



User Guide

Version 6.0

April 2016

Table of Contents

Welcome to InterMapper	9
About InterMapper	11
What's New in InterMapper®6.0?	11
Software License Agreement	12
InterMapper and Section 508	14
Getting Started	17
Installing and Launching InterMapper	17
Registering Your Software	21
InterMapper Control Center	25
Automatic Notifications of Updates	28
Installing InterMapper Flows	31
InterMapper Quick Tour	32
Using InterMapper	36
Try out the Demo Maps	39
The Map Window	41
The Map List Window	46
The Device List Window	48
Layer 2 View	51
Understanding the Layer 2 View	52
InterMapper User Preferences	53
Creating Maps	57
Using Auto-Discover	59
Adding Devices Manually	65
Set Probe Window	66
Adding Networks to the Map	68
Scanning A Network	70
Creating Sub-maps	71
Creating Probe Groups	74
Using Helper Applications	78
Using Double-Click Actions	83
Saving Your Map	85
The Map Settings Window	86
Quick Reference - Editing Your Map	95
Configuring PowerShell For Use With InterMapper	97

Arranging Your Map	99
Icons and Images on Maps	101
Adding Background Images To Your Map	104
Editing Labels	106
Dynamic Label and Alert Text	108
Using the Arrange Commands	114
Other Tips for Arranging Your Maps	119
Connecting Devices to Switch Ports	121
e Copying Subnet Ovals	123
Adding Unmanaged Hubs and Switches to a Map	124
Hiding and Un-hiding Detail	128
Notifiers and Alerts	129
Working With Notifiers	131
Attaching a Notifiers to Devices and Interfaces	133
Using Vantage Points	136
Configuring Notifiers	139
Configuring a Sound Notifier	142
Configuring an E-Mail Notifier	144
Using Group Notifiers	146
Configuring a Pager Notifier to use an Analogue Modem	147
Sending SMS/Text Alerts to a Cell Phone	151
Notification Using a Numeric Pager	153
Configuring a Page Notifier to Send a Page Using SNPP (Network)	155
Configuring an SMS Notifier	157
Command-line Notifiers	160
Example Notification from a Command Line Program	162
Interfaces & Notifiers	164
WinPopup (Windows Only)	165
Configuring a Syslog Notifier	166
Notification by SNMP Trap	167
AutoMate Notifier	169
PowerShell Notifier	173
The Dartware MIB	177
Monitoring Your Network	180

Understanding the Map	181
Viewing Status Windows	185
The Info Window	188
The Device Info Window	189
The Network Info Window	193
Interfaces Window	195
About Packet Loss	200
Acknowledging Device & Link Problems	202
Outage Alarms on Interfaces	206
Setting Thresholds	208
Setting Traffic Indicators	215
Sending Feedback	216
Creating Charts	219
Using Charts	220
Chart Menus	223
Chart Options	226
Chart Log Files	232
Purging Chart Data	233
Log Windows	234
The Event Log	235
Event Log Messages	236
The Outages Log	246
Debug Logs	247
Server Settings	249
Server Information Panels	251
Server Preference Panels	253
SNMP Preferences	254
Log File Preferences	257
DNS/WINS Settings	262
E-Mail Preferences	264
Default Map Colors	265
Default Device and Network Preferences	267
Default Device Thresholds	269
Default Server Interface Thresholds	270
Chart Defaults	271

Retention Policies	274
NT Services & WMI	276
Server Configuration Panels	277
Configuring a Firewall	278
Controlling Access to Your Server	280
The Remote Server	282
Reports Server	285
The Web Server	289
The Telnet Server	291
AutoMate	293
Layer 2 Features	294
Enabled Maps	296
Users and Groups	298
Access Control Examples	303
Controlling Access to a Map	305
Map Backup	307
Notifier List	308
SSL Certificates	310
InterMapper Flows™	315
The Flows Window	316
Top Hosts Tab	323
Top Ports Tab	327
Top VLANs Tab	330
Top Sessions Tab	332
Supported Exporters	333
InterMapper Flows Settings	334
Using the Layer 2 View	343
Overview	343
Viewing Layer 2 Information	343
Understanding the Layer 2 View	344
The Filter Pane	345
Understanding and Using the Endpoints Pane	347
Understanding and Using the Connections Pane	348
Understanding Layer 2 Flags	350
Understanding Fuzzy Devices	352

Mapping With Layer 2	353
InterMapper Reports	354
Creating A Report	355
Selecting Source Data	359
Creating and Using Data Filters	364
Choosing a Report Style	366
Managing and Printing Your Reports	370
Switching to Edit Mode	370
Using InterMapper RemoteAccess	373
Command and Menu Reference	374
File Menu	375
Edit Menu	380
View Menu	384
Monitor Menu	387
Insert Menu	404
Format Menu	411
Window Menu	425
Help Menu	430
InterMapper Menus	434
Context Menus	435
Keyboard Shortcuts	436
Keyboard Navigation	437
Probe Reference	438
Probe Reference Index	442
Basic	448
SNMP	451
Miscellaneous	461
Network Devices	466
PowerShell	479
Probe Groups	484
Servers-Proprietary	485
Servers-Standard	505
WMI	536
Wireless	549
Experimental	593
About Packet-Based Probes	596

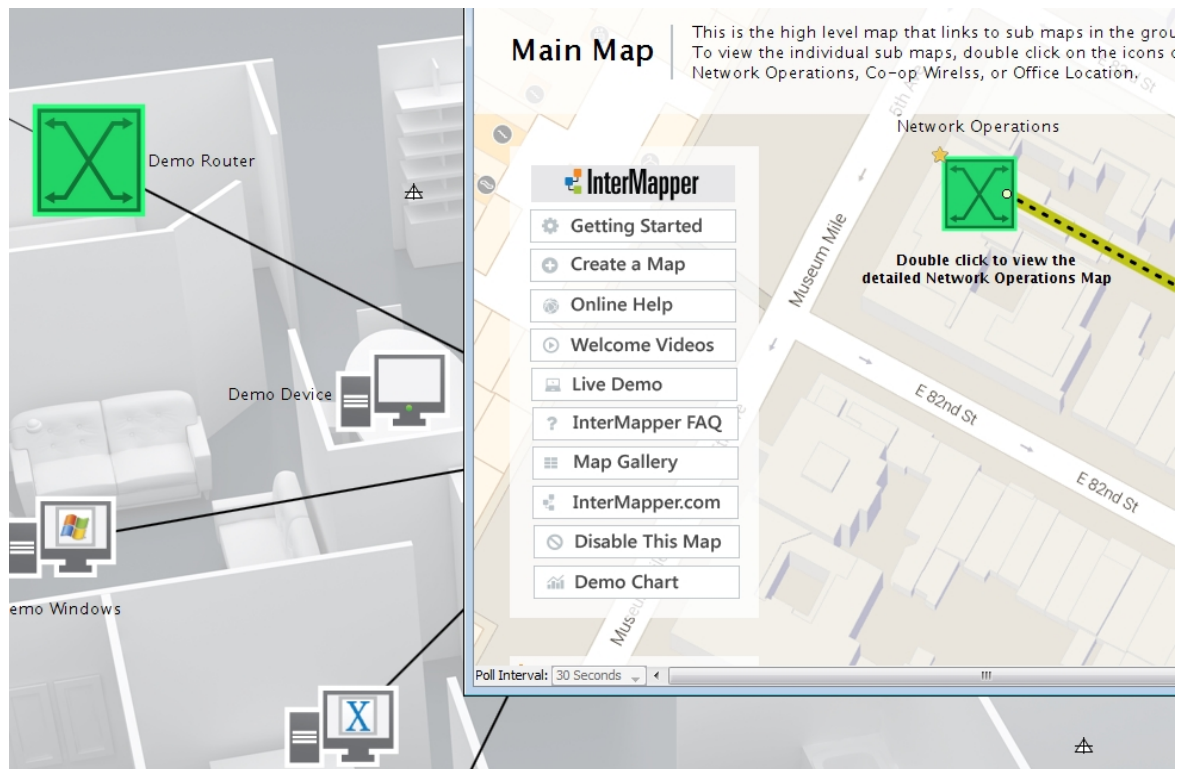
About SNMP Versions	598
Command-Line Probes	600
Monitoring NT Services with the Windows NT Services Probe	601
Cisco IP SLA Probe	605
Big Brother Probes	607
Troubleshooting Network and Server Probes	608
Using InterMapper DataCenter	613
Configuring InterMapper DataCenter	613
Using an Existing Database	615
About Retention Policies	618
Configuring InterMapper Database Logging Preferences	619
Reviewing Database Disk Usage	620
Configuring Automatic Database Backups	621
Performing Maintenance Tasks	622
Using the InterMapper Authentication Server	623
Data Collecting and Reporting	626
InterMapper Files and Folders	628
Making Backups	631
The InterMapper Settings Folder	632
InterMapper DataCenter Folder	634
Importing and Exporting Maps	635
Exporting Data From Maps	635
Importing Data	637
Using Geographic Coordinates	640
Exporting Information to Google Earth	644
Advanced Data Importing	649
Introduction - The Directive Line	649
Device Attributes	656
Vertex Attributes	667
Interface Attributes	670
Map Attributes	675
Notifier Attributes	678
Notifier Rules Attributes	679
User Attributes	681
Retention Policy Attributes	682

About D-Sets	684
The IMProbe URL Specification	687
Using the Web Server	689
The Home Page	691
The Error and Full Pages	695
The Outages Web Page	698
The Device List Web Page	699
Viewing a Chart	701
Telnet Server Command Reference	702
Command-line Options	710
Command-line Options for InterMapper	710
Command-line Options for RemoteAccess	711
Using InterMapper With Splunk	715
Troubleshooting InterMapper	719
Troubleshooting InterMapper RemoteAccess	724
Troubleshooting InterMapper DataCenter	725
About IP Addresses	726
Quick Intro to IPv6 Address Formatting	729
About DNS	730
SNMP Information	731
About WINS Names	735
InterMapper FAQs	736
InterMapper Flows FAQs	739
Cross-platform Questions	740
Index	742

Chapter 1

Welcome to InterMapper

InterMapper Server and Network Monitoring



InterMapper is a network monitoring and alerting program. It continually tests routers, servers, hubs, and other computer devices that are attached to your network. If InterMapper detects a failure, it sends notifications to one or more individuals via sounds, e-mail, pagers, SMS text, or by running a program to correct the problem.

Use this manual to learn about how to get InterMapper up and running quickly, and to get detailed information about specific features of the program.

InterMapper has several components that work together to help you understand what's happening on your network:

[InterMapper \(Pg 36\)](#)

The core functionality of the product that gathers data about your network, and provides polling, alerting, notifications about its operation.

[InterMapper Flows \(Pg 315\)](#)

Uses NetFlow, sFlow and J-Flow data to provide detailed information about the kinds of data flowing through the network.

[InterMapper DataCenter \(Pg 626\)](#)

Several additional components that enhance InterMapper. Includes access to external authentication servers and a PostgreSQL database.

[InterMapper RemoteAccess \(Pg 373\)](#)

A GUI application that allows you to view and configure your InterMapper system from any location.

In addition, you can customize InterMapper's operation in a number of ways. The [Developer Guide/Software Development Kit](#) is described separately.

Please give us comments at the address listed below. Thanks!

[HelpSystems LLC](#)

[InterMapper Feedback](#)

About InterMapper

What's New in InterMapper®6.0?

InterMapper 6.0 includes a number new features and enhancements. Here's a summary...

Link and Interface Monitoring Enhancements

InterMapper 6.0 includes a large number of enhancements that allow much more precise monitoring of links and interfaces. Among these enhancements:

- Set thresholds for an individual interface for Link Utilization, Interface Errors, and Interface Discards.
- Set default interface thresholds for a server, map, or device.
- Send alerts when thresholds are reached.
- View and acknowledge status for individual interfaces.
- View status of links with new visual indicators.
- View Statistics in a new tab of the Interfaces window.

Changes to System Requirements

System requirements for InterMapper are now maintained only online. Please see the [System Requirements page](#) on the HelpSystems website.

Documents versions:

- InterMapper & InterMapper RemoteAccess: 6.0
- Document Built: 4/11/2016 10:11 AM

Software License Agreement

PERMANENT LICENSE AGREEMENT

BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE PRODUCT ("Product"), YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT ("Agreement"), UNDERSTAND IT, AND AGREE TO BE BOUND BY IT.*

LICENSE

Upon receipt of payment for the Product (which includes the software and accompanying documentation), the Company grants the licensing party identified in the applicable final quote, purchase order or invoice ("Customer") a perpetual, limited, non-exclusive, non-transferable license to use the Product solely on the system or partition specified in the Customer's order and solely for the Customer's internal business purposes, and subject to all the terms and conditions of this Agreement.

The Customer shall not:

- i. transfer the Product to another system or partition without the Company's written consent;
- ii. permit any third party access to the Product, including, but not limited to, external hosting or third party IT outsourcing vendors, without obtaining prior written consent to such an arrangement from the Company;
- iii. reverse engineer, translate, disassemble, decompile, sell, rent, assign, lease, manufacture, adapt, create derivative works from, or otherwise modify or distribute the Product or any part thereof;
- iv. copy, in whole or in part, the Product with the exception of one copy of the Product for backup or archival purposes;
- v. delete any copyright, trademark, patent, or other notices of proprietary rights of the Company as they appear anywhere in or on the Product.

The Company reserves all rights, title, interest, ownership, and proprietary rights in and to the Product, including but not limited to, all copies of the Product and any patent rights, copyrights, trademark rights, trade secret rights, and any other intellectual property rights. The Product is protected both by United States law and international treaty provisions.

The Product is provided "AS IS" WITHOUT WARRANTY, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE COMPANY DOES NOT WARRANT THAT THE PRODUCT WILL MEET THE CUSTOMER'S REQUIREMENTS, OPERATE IN COMBINATION WITH OTHER SOFTWARE, OR BE UNINTERRUPTED OR ERROR-FREE. In no event shall the Company be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages arising out of the use of or inability to use the Product even if the Company has been advised of the possibility of such damages. In no event shall the Company's total liability to the Customer exceed the amount of any license fee paid by the Customer to the Company for the Product. The foregoing limitations shall apply even if the remedy fails of its essential purpose.

The Company may terminate this Agreement immediately if the Customer fails to comply with any provision of this Agreement or if the Customer ceases to carry on its present business or becomes insolvent, makes a general assignment for the benefit of creditors, or is involved in a bankruptcy or receivership proceeding. The Company's right to terminate this Agreement is in addition to and not in limitation of any other available remedies. Upon termination, the Customer agrees to destroy the original and all copies of the Product in its possession or control. This Agreement and any dispute arising from or relating to it shall be governed by and construed and enforced in accordance with Minnesota law, without reference to conflicts of laws principles. Any legal action or proceeding shall be instituted in a state or federal court in Hennepin County, Minnesota, USA. This Agreement constitutes the complete agreement between the parties and supersedes all prior or contemporaneous agreements or representations, written or oral, concerning the subject matter of this Agreement including any purchase order or ordering document. This Agreement may not be modified or amended except in writing and when signed.

The Company, wholly owned by Help/Systems, LLC, may assign any or all of its rights under this Agreement at any time without notice.

**Note to customers outside the U.S.: You also agree to be bound by any additional license terms and conditions presented to you by the authorized Company distributor from whom you purchased the Product ("additional license terms"). The additional license terms are incorporated in this Agreement to the extent they do not explicitly conflict with any of the terms set forth above.*

MAINTENANCE

The Customer may purchase maintenance for the Product by payment of a maintenance fee as set forth by the then current software product price list. Maintenance includes the following benefits:

- Refinements and corrections of the Product as they become available, provided these improvements are not separately priced and marketed by the Company.
- Enhancements to interface the Product with new versions.
- The right to temporarily copy and use the Product on a different system located at a hot site.
- Unlimited technical support via e-mail.

Training services must be used within 6 months of being invoiced and all fees are nonrefundable.

InterMapper and Section 508

Voluntary Product Accessibility Template

The table below outlines InterMapper and InterMapper RemoteAccess (collectively called "InterMapper" below, unless otherwise specified) accessibility features in the context of the Section 508 standards. This document is not intended to be a certification of compliance.

The document contains subsets of the Electronic and Information Technology Accessibility Standards as published in 36 CFR Part 1194 and provides an analysis of InterMapper as compared to these standards.

Section 1194.21 Software Applications and Operating Systems - Detail

Criteria	Supporting Features	InterMapper & RemoteAccess
Keyboard Access (a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.	Supports with exceptions.	Some functions, including arranging devices on the map and displaying status windows are not accessible via keyboard commands.
Accessibility Features (b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	Supports. InterMapper does not disable accessibility features.	X
On-screen focus and tracking (c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes.	Supports with exceptions. InterMapper provides on-screen indication of current focus that moves among interactive interface	Focus is not programmatically exposed in InterMapper

	elements as the input focus changes.	
Information about user interface elements (d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element, the information conveyed by the image must also be available in text.	Supports with Exceptions. InterMapper provides "status windows" that describe the state of items on a map, however these status windows are not available to Assistive Technology.	X
Consistent meaning of images (e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	Supports. The InterMapper user interface consistently uses bitmap images to display device status.	X
Availability of textual information (f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.	Supports.	X
Contrast and color settings (g) Applications shall not override user selected contrast and color selections and other individual display attributes.	Supports. InterMapper does not override user selected contrast and color settings when they are available in the operating system.	X
Animation (h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	Does not support.	InterMapper has animated traffic flows that have no presentation mode that is available to Assistive Technology.
Color Coding	Supports.	X

(i) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

Variety of color selections

(j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.

Supports. Inter- X
Mapper allows
users to cus-
tomize the con-
trast and color
settings of the
text and back-
ground of their
document to a
wide range of
colors supported
by their system.

Flash or blink frequency

(k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.

Supports. InterMapper uses
a 1 Hz (or
slower) blinking
icon to indicate
an outage.

Interaction with electronic forms

(l) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

Not Applicable. N/A
InterMapper
does not have
electronic forms
capabilities.

Chapter 2

Getting Started

Installing and Launching InterMapper

[Get a copy of InterMapper](#), then install it as described below.

When you install InterMapper, the installer also includes [InterMapper DataCenter \(Pg 613\)](#) and [InterMapper Flows \(Pg 315\)](#). During the trial period, all three are available. Once the trial license expires, you need a license to run InterMapper Flows, and the correct InterMapper license to run InterMapper DataCenter.

When you launch InterMapper the first time, a Welcome page appears. Use the shortcuts on the Welcome page to get you quickly to area of InterMapper that will best get you started.



InterMapper Welcome page

- **Create a new map** - opens the New Map window. After naming your map, you can start the Autodiscovery process to scan your network for devices. All discovered devices get placed on your new map. Find out more about this process in [Using Auto-discover. \(Pg 59\)](#)
- **Try out the Demo maps** - opens a Demo map as described below.
- **Get help** - opens the Getting Started page on the InterMapper website.

To prevent the Welcome window from appearing:

- Click **Do not show this window again** and click **Continue to Map List**.

Using the Demo Maps

No matter which platform you're using, a set of demo maps becomes available when installation is complete and the program is launched. Watch them operate, and experiment with them to see how InterMapper operates. For additional information, see [With Try Out the Demo Maps \(Pg 39\)](#).

Installing on Different Platforms



Note: although many of the features described in this manual are similar between the MacOS, Windows, and Unix/Linux platforms, there are a few differences. We recommend you read the Readme file installed with your version.

MacOS X

1. Double-click the *.dmg* file to mount it.
2. Double-click the InterMapper.pkg icon for the installer and follow the instructions. The *InterMapper* application starts running when installation is complete.

Windows

- Double-click the InstallShield icon for the installer and follow the instructions. The *InterMapper* application starts running when installation is complete.

Unix or Linux

- If you're using **Unix** or **Linux**, then read the accompanying **ReadMe** (also found on the download page) to get instructions for installing on your particular platform.

About the Trial Version

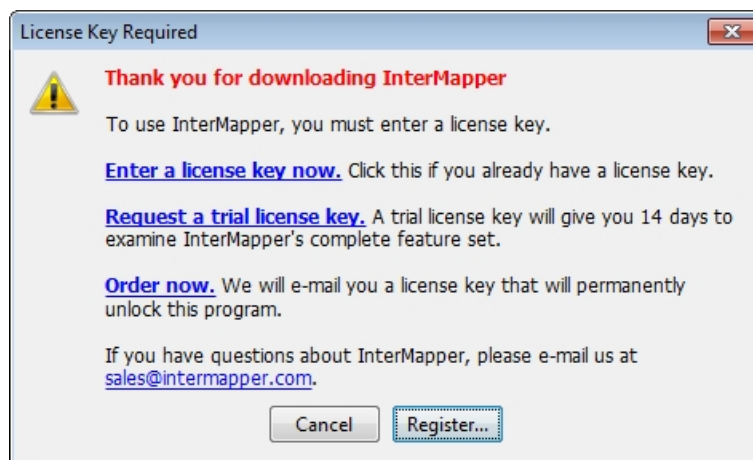
The downloadable version of InterMapper requires a license key to operate. You can [request a free license key](#) to get full functionality for 14 days, including printing and opening saved maps.

If you already have a license key (because you purchased the software or you received a trial key), click

Enter a license key

now or the **Register** button in the License Key Required window. You can then enter your name and serial number. For details about entering your evaluation (or any other) serial number, you can read the [Registering your software \(Pg 21\)](#) page.

If you don't have a license key, click the **Request a trial license key** link in the window shown above. A form appears, allowing you to enter some information, and request a trial license key. When you click Send Request, a license key appears in the text box. It allows you to use InterMapper to monitor a limited number of devices for 14 days. Click Register to activate the key.



Once you've seen the demo, see [Using InterMapper \(Pg 36\)](#) to guide you as you try out InterMapper's features.

About License Keys

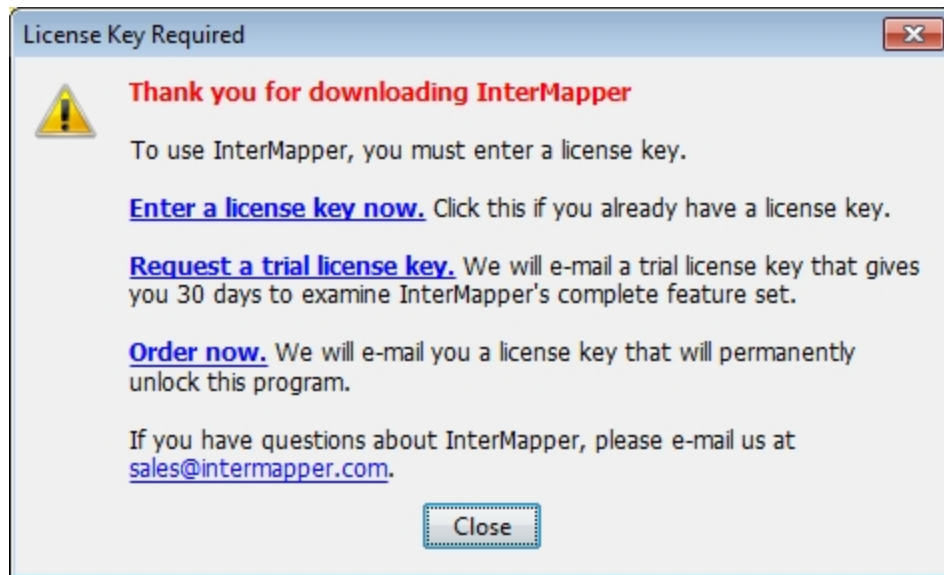
When you purchase InterMapper, we will send you a license key that unlocks the software permanently. The license key is associated with a specific piece of hardware, so it will allow InterMapper to run only on a particular machine.

A full license - sent to those who purchase the software - never times out. Once registered, the application will run forever on that machine. If you want to run InterMapper on a different machine, you will need to request a new license key for that machine.

InterMapper also supports trial license keys, which allow you to run InterMapper for a certain number of days before it requires a new key. This gives you an opportunity to try the program without obligation. When a license key expires, InterMapper simply ceases to operate. It *never* deletes or alters files on your hard drive.

Registering Your Software

When you install and run InterMapper, the following window appears:

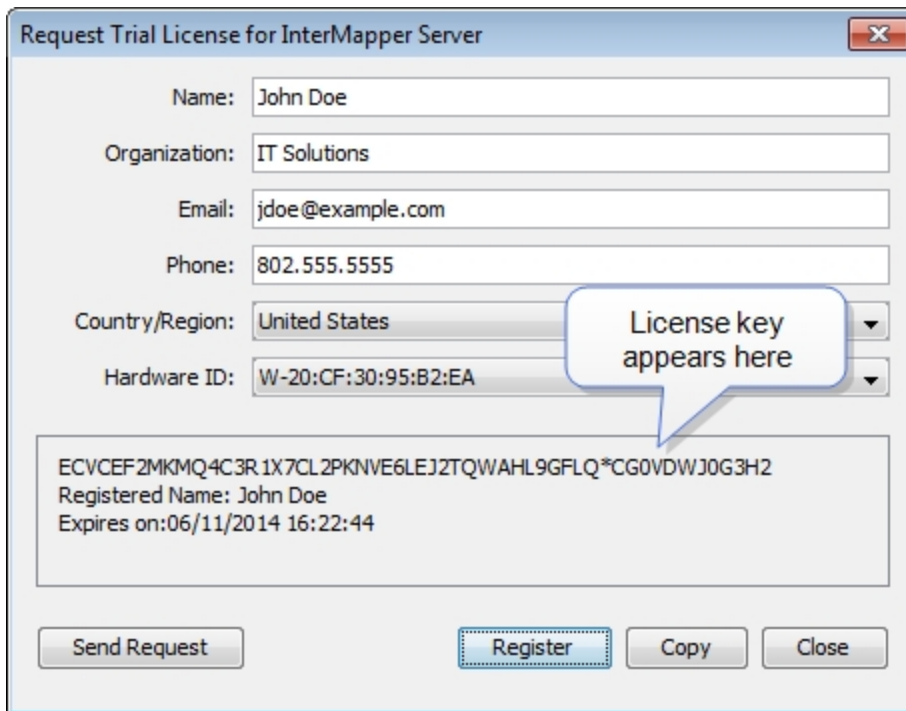


- **Enter license key now** - if you already have a key, click to paste it now.
- **Request a trial license key** - if you don't have a key, click to request one. The Request Trial License window appears as shown below.
- **Order now** - Allows you to purchase the produce.

Requesting a Trial License

To request a trial license:

- When you click ***Request a trial license key***, the Request Trial License window appears as shown below:



Request Trial License for InterMapper Server

Name: John Doe

Organization: IT Solutions

Email: jdoe@example.com

Phone: 802.555.5555

Country/Region: United States

Hardware ID: W-20:CF:30:95:B2:EA

License key appears here

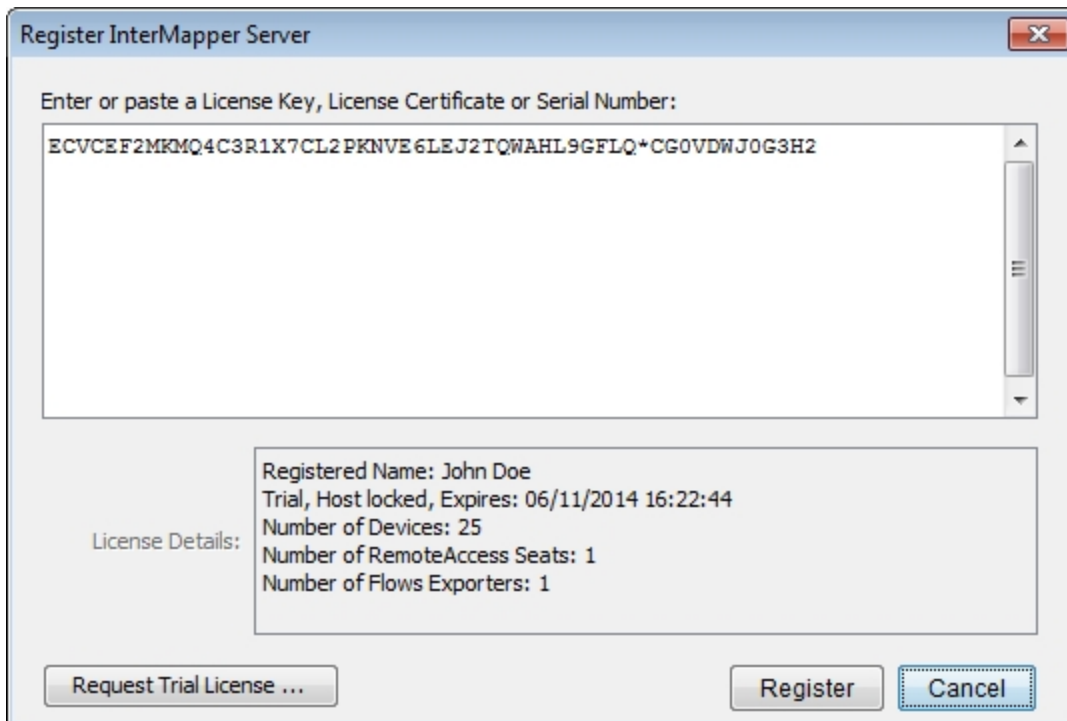
ECVCEF2MKMQ4C3R1X7CL2PKNVE6LEJ2TQWAHL9GFLQ*CG0VDWJ0G3H2

Registered Name: John Doe

Expires on: 06/11/2014 16:22:44

Send Request Register Copy Close

1. Click **Send Request**. InterMapper contacts HelpSystems and retrieves a trial key. The new key appears in the area shown above.
2. Click **Register**. The Register InterMapper window appears as shown:



Register InterMapper Server

Enter or paste a License Key, License Certificate or Serial Number:

ECVCEF2MKMQ4C3R1X7CL2PKNVE6LEJ2TQWAHL9GFLQ*CG0VDWJ0G3H2

License Details:

Registered Name: John Doe

Trial, Host locked, Expires: 06/11/2014 16:22:44

Number of Devices: 25

Number of RemoteAccess Seats: 1

Number of Flows Exporters: 1

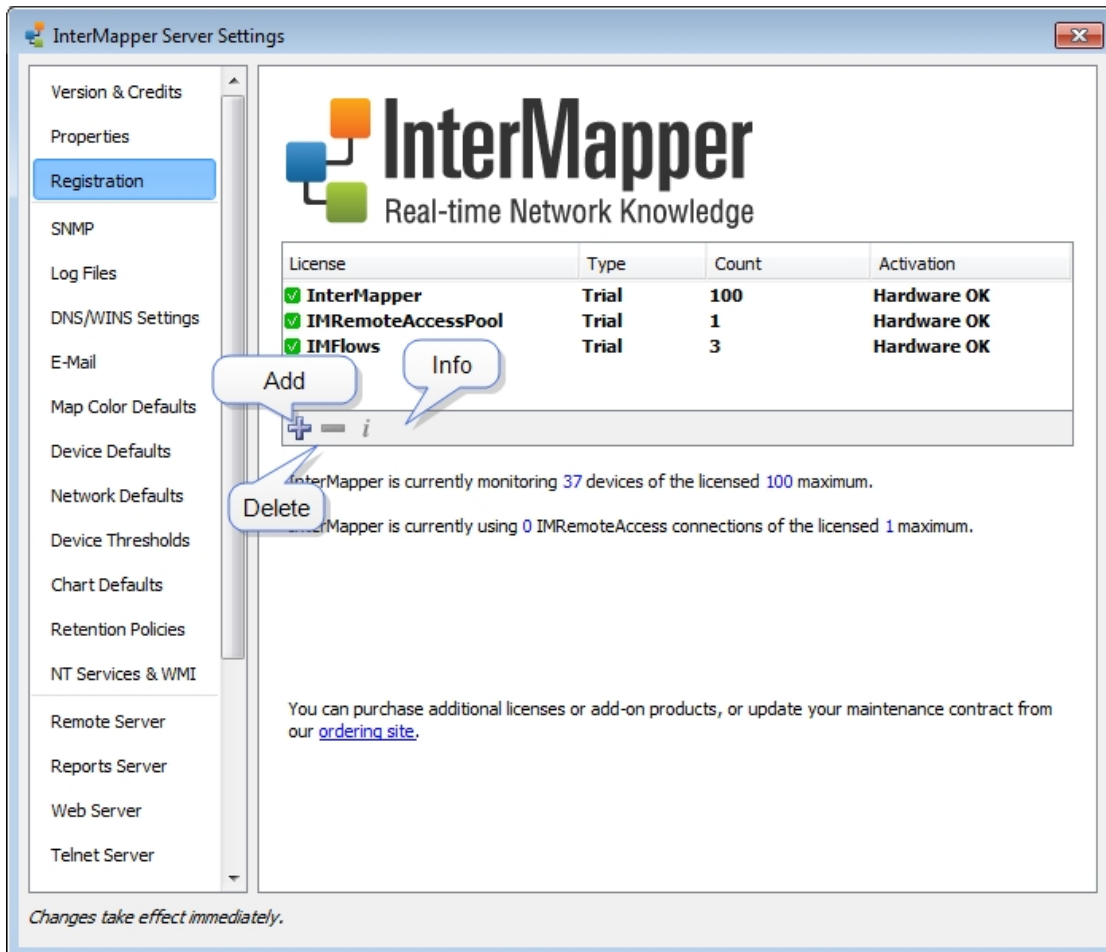
Request Trial License ... Register Cancel

The license shows the registered name, type of license, and the number of devices and other licenses associated with this key.

3. Click Register. The license key is registered as shown.

Entering Multiple Licenses

You can enter multiple serial numbers to unlock additional InterMapper functionality. The **Registration** pane in InterMapper Server Settings window shows the licenses that are currently installed.



Multiple licenses in InterMapper RemoteAccess

Use these options, available from the Registration pane, to add, delete or view information about a license or serial number:

- Click **+** to add a new license or serial number.
- Click **-** to remove the selected license or serial number.
- Click **i** to view detailed information about the selected license or serial number.

InterMapper Control Center

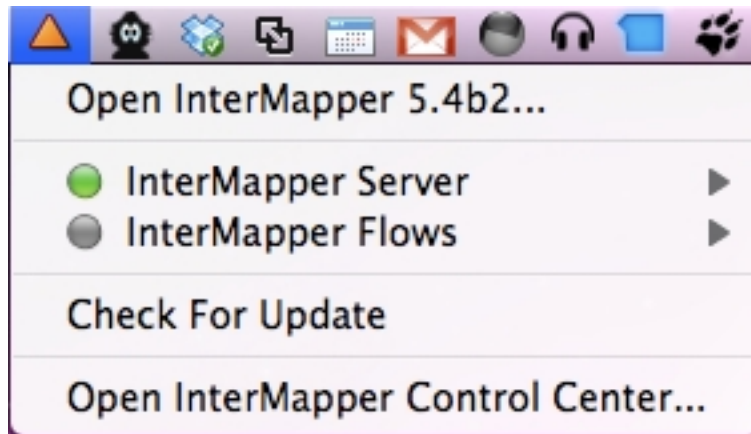
On MacOS X, InterMapper installs a Menu Bar Application that gives a summary of InterMapper's status, and allows you to start and stop the InterMapper daemon.

On Windows, InterMapper installs an icon in System Tray (lower right corner) that does much the same thing. It also uses presents a window to indicate an interesting change in InterMapper's state.

The System Tray Icon and Menu Bar Application are available only on the machine hosting the InterMapper Server.

On MacOS X

The menu bar application has an icon that reflects the most serious state of InterMapper. When the server is not running at all, the InterMapper program icon appears. The icon will be green, yellow, orange or red, depending on the severity when the server is running.



The menu bar application can also:

- Open the InterMapper application
- Start or Stop the InterMapper server daemon
- Open the InterMapper Control Center
- Check for software updates

The InterMapper Server Status window shows the server name and version, as well as the current state of the InterMapper server. This window also allows you to start or stop the InterMapper server, or open InterMapper.

On Windows

The InterMapper Control Center application is available on supported Windows systems (Pg 1).

It has the same function of the MacOS X application, but is called from the Window System Tray (lower right corner of the screen).

You can do the following from the InterMapper Control Center:

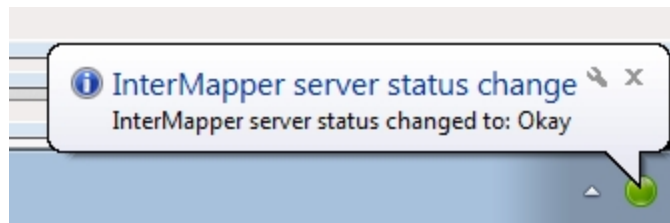
- Choose whether the Windows balloons appear when map status changes.
- Start or stop the InterMapper or Flows services.
- Open the InterMapper application.
- Choose whether to check for software updates automatically.
- Check for software updates manually.

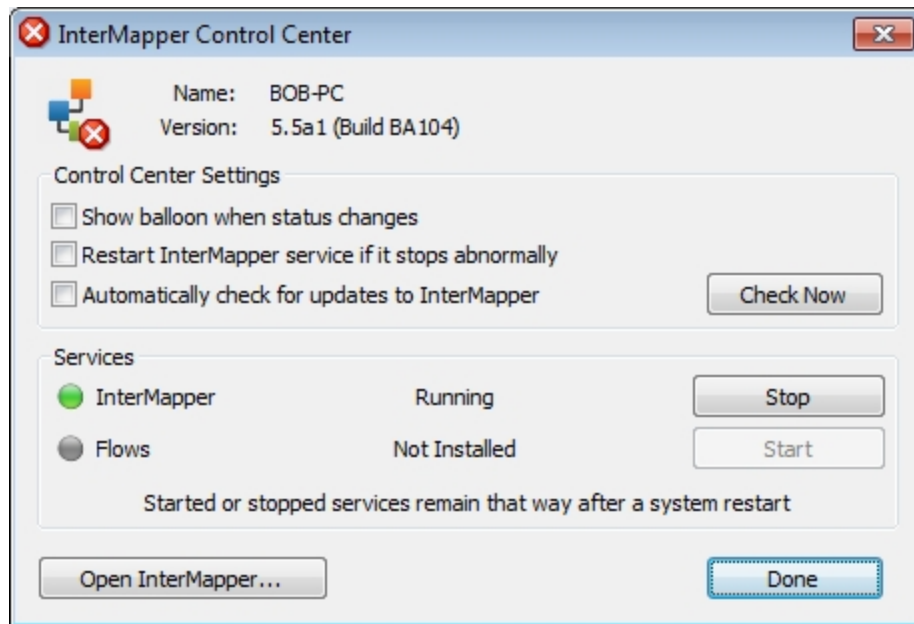
You can do most of these same functions from the context menu that appears when you right-click the InterMapper status icon.

Note: When you stop or start a service from the InterMapper Control Center, that states of those services are maintained when you restart the machine.

To open the InterMapper Control Center:

- Right-click the InterMapper Control Center icon in the Windows System Tray and choose **Show InterMapper Control Center**.





Automatic Notifications of Updates

InterMapper can automatically check to see if a new version is available for download. This check is performed at startup and again every 24 hours.

If the check has never been run before, InterMapper presents a dialog you can use to disable the automatic checking before it takes place. At any time, you can disable the feature, either by choosing Preferences from the Edit menu, then choosing the Behavior->Version Updates pane, or by opening the InterMapper Control Center. When a new version is available, a message appears, including a link to the new version

When you first start up a Windows version of InterMapper, a message asks you would like InterMapper to check for new versions. This is the only time it will ask this question. If you answer yes, the check is performed at startup and again every 24 hours.

To enable or disable this feature:

1. Open InterMapper Control Center
2. Select or clear the "Automatically check for updates to InterMapper" check box.

Upon detecting that a newer version of the software is available, a dialog box appears, indicating that a newer version is available, and asking if you would like to download the new version.

- Click "Yes" to launch a browser with the URL to the new version.

Using Growl for Update Notifications (Macintosh Only)

Growl is a notification system for Mac OS X. It provides a central mechanism for controlling and customizing the delivery of notification messages from Mac OS X applications.

Growl is a free download from: <http://growl.info>

How Notifications Appear When Growl is Running

When Growl is available, InterMapper Control Center uses it to display notification messages instead of using the default "yellow tooltip window". If Growl is running when InterMapper Control Center starts up, Growl notifications are used automatically. If you install Growl after InterMapper Control Center is already running, you must open the InterMapper Control Center settings window before Growl is detected and used.

Growl provides a number of features not available through InterMapper Control Center's built-in message window.

1. Growl has a plugin system that supports customizable "look-and-feel". As a result, Growl notifications look much better, and feel more natural than InterMapper's yellow window.
2. Most Growl plugins are customizable. You can configure the appearance of the notification, including text size and color.

3. You can choose which InterMapper notification messages you want to see, or alter the appearance of specific messages to match their importance. For example, you can set up DOWN and CRITICAL notifications to display in large red text, and ignore all other notifications.
4. You can specify that any or all InterMapper notifications are "sticky", each remaining on screen until you explicitly click it.
5. There are many more options. For example, you can choose to have Growl speak notification messages or email them to you.

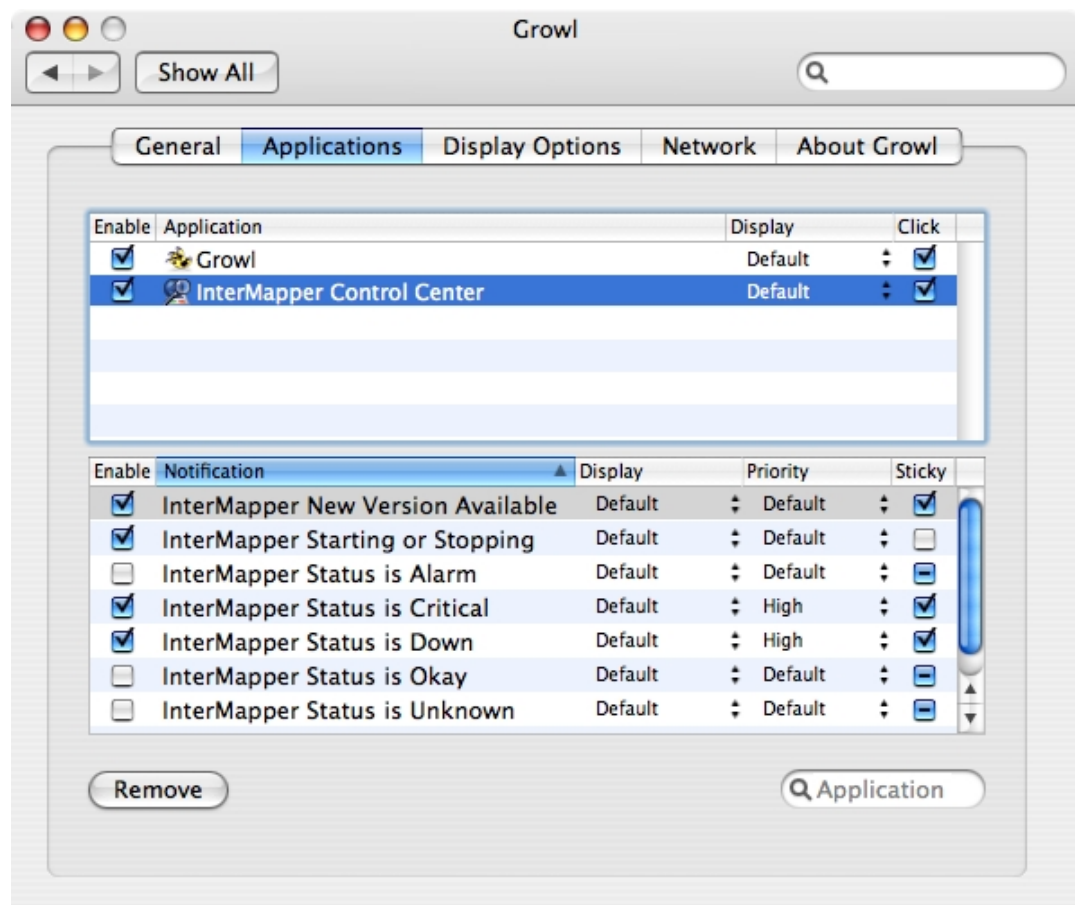
To test Growl messages:

1. Open the InterMapper Control Center window.
2. Select the "Show messages when InterMapper Server status changes" checkbox.

Note: Neither Growl nor InterMapper's built-in status window is used if this checkbox is not checked.

Growl Control

Use Growl's System Preference panel to configure Growl's behavior.



Growl provides control over the following InterMapper notifications:

- InterMapper New Version Available
- InterMapper Starting or Stopping
- InterMapper Status is Down
- InterMapper Status is Critical
- InterMapper Status is Alarm
- InterMapper Status is Warning
- InterMapper Status is Okay
- InterMapper Status is Unknown

You can individually enable or disable any of these messages. You can also specify different plugins for different messages or specify that certain messages require you to click on them to dismiss them (the "sticky" option).

By default, Growl support is automatically enabled in InterMapper Control Center if Growl is available. If you have Growl installed, but you do **not** want InterMapper to use it, disable it using the following command-line:

```
defaults write com.dartware.InterMapperMenu DWGrowlDisabledKey 1
```

After executing the command, you must reopen the InterMapper Control Center Settings window for this change to take effect.

Installing InterMapper Flows

You must follow several steps before you can begin analyzing your Flows data.

- InterMapper Flows is installed automatically with InterMapper. See [Installing and Launching InterMapper \(Pg 17\)](#) for more information.
- If you are running a trial version, InterMapper Flows is fully operational. Once the trial expires, an InterMapper Flows license is required.
- Be sure to **remove any firewalls** on the selected UDP ports for NetFlow (default is 2055).
- *Note:* The InterMapper Flows service/daemon may not start up if another program is using port 2055 (or whatever port you have designated for netflow packets). You should stop/uninstall any other netflow packages on the system.
- You must also **configure one or more Flows exporters** to send data to the InterMapper Flows server. InterMapper Flows automatically detects the exporters and begins collecting their data. Many switches and routers can be configured to export Flows data. There are also several software-based Flows exporters available, including nProbe, SoftFlowd, and ProQueSys.

InterMapper Quick Tour

Ten things to try with InterMapper when you're first checking it out. Learn how to create maps, make them attractive, send alerts, make charts, etc.

This page lists ten things you can try with InterMapper to get more familiar with it. You can also refer to the [InterMapper User Guide](#) for more information.

1. **Try Out The Demo Maps** When you install InterMapper for the first time, a set of demo maps is installed. On the Welcome page, click **Try Out The Demo Maps** and take a couple minutes to try the steps listed in the text you'll see there. When finished, you can click **Disable This Map**. You can disable the demo map from the Enabled Maps pane of the Server Settings window.
2. **Building Maps** There are several ways to create maps—autodiscovery, entering addresses manually, and importing a file. Before you proceed, you may want to download the [Hands-on Examples](#) because it has some files for the following steps. Things to try:
 - **Autodiscovery** InterMapper can scan a network to find devices
 - Create a new map by choosing **File > New map...** Give it a name (*Local Network*) and click Next.
 - Check the Autodiscovery button in the window, then click Next. You'll see the Autodiscover window.
 - Enter a starting point address (the default value is fine) and click OK.
 - Autodiscovery will begin. Let it complete, or click Cancel in the top of the map when you've discovered enough.
 - **Manual Entry** You can also add devices manually by typing or pasting a list of DNS names or IP addresses into the window that appears.
 - Create a new map, give it the name "North America" and click **Next >**. Check the Manual Entry button, then click **Next >**. You'll see the Add Device(s)... window.
 - Type **www.helpsystems.com** and **www.example.com** and click Add. Note that they appear as devices (rectangles) and turn green a few moments afterward. (InterMapper is already testing them.)
 - You can add a background image to make the map look better. Drag the *NorthAmerica.jpg* from the Hands-on Extras folder to map window and it will appear as the map's background.
 - Choose **Window > Zoom window** to resize the map to the image.
 - Drag the rectangles to the desired location on the background map.
 - **Create top-level map** InterMapper can have top-level maps that indicate the most serious condition of a sub-map. We'll add icons for the *Local Network* and the *Unalakleet* sub-maps to the North America

map.

- Open the North America map and position it and the Map List so you can see both windows.
- Drag the icon for *Unalakleet* from the Map List into North America map.
- Drag the icon for the *Local Network* map in a similar way.
- Drill down by double-clicking the *Local Network* icon on the top-level North America map. You'll see the *Local Network* map open up.

3. **Making Attractive Maps** There are a number of techniques for making the maps look more attractive, or to convey more information. Things to try:

- **Drag items around** to match the way you think of your network. Lines between devices "rubberband" to preserve the interconnections.
- **Add a background image** to position devices as you like. Simply drag a PNG, JPEG, or GIF image into the map window to add it, or choose **Edit > Map Settings...**
- **Select different icons and shapes for devices** Choose **Format > Icon...** to pick new icons for the devices.
- **Change labels on devices** The label is the text that appears in/next to the icon on the map. To edit a device's label, choose **Format > Label...** or Ctl/Cmd-L.
- **Arrange devices on the map** Use different options in the **Format > Arrange...** menu .
- **Align command** The **Format > Align** (Ctl/Cmd-Shift-K) command aligns items vertically and/or horizontally.
- **Add a link between devices** Select two devices, then **Insert > Add link** (Ctl/Cmd-E)
- **Connect multiple devices to a point** Select the devices, then choose the context menu **Attach to...** Lines will rubberband, and stick to the object you next click.

4. **Probes for Various Servers** In addition to simply pinging them, InterMapper can monitor dozens of different devices and display their special characteristics. Right/control-click, or **Monitor > Set Probe...** to select the probe for one or multiple selected devices. Things to try:

- **Automatic** This probe uses either Pings or SNMP queries to monitor the device. If the device speaks SNMP, InterMapper will use the SNMP Traffic probe to query the device. If not, InterMapper will ping the device and report if it ever goes down.
- **SNMP Traffic** The SNMP Traffic probe monitors traffic on routers, switches, etc. It works with nearly all network gear from different vendors.
- **Network Devices** There are many probes for monitoring various other equipment, such as Cisco, Apple, APC and other UPS vendors, and other equipment.

- **Servers-Standard** Standards-based servers, such as mail, web, LDAP, Radius, DNS, etc.
 - **Servers-Proprietary** Vendor-specific probes for Apple, Barracuda, Big Brother, FileMaker, Lotus, and many others.
 - **Miscellaneous** Nagios, legacy probes, etc. along with other bundles of probes for wireless and other gear.
5. **Alerts and Notifications** InterMapper can put a device into one of five states: OK, Critical, Warning, Alarm, Down. Each time the device goes into a new state, InterMapper can trigger a notification/alert.
- **Create Notifiers** Notifiers are like a robot that watches a device and performs some action to send an alert when it changes state. Choose **Edit > Server Settings** and scroll to the Notifier List at the bottom. Add an e-mail notifier for yourself.
 - **Examine various notification types** Mail, pager (analog modem and SNPP), command line, trap, group, syslog.
 - **Look at schedule** Alerts will only be triggered during the selected schedule, otherwise they are ignored.
 - Finally, **Attach a notifier to a device** To attach a notifier, choose **Monitor > Notifiers window** and check the boxes for the states that should trigger a notification.
6. **Acknowledgement** After alerts/notifications have been sent, you probably want to set those problems aside so you can detect new ones. Acknowledging a device turns its icon blue (to indicate that it has been acknowledged). The device is still down, but its blue color shows that someone has taken responsibility for it. Acknowledging also helps you know *who's* working on the problem. Each time you ack a device, there's an opportunity to enter an ack message, that is written to the Event log. This contains the login name of the person who ack'd it.
- **Monitor > Acknowledge...** (Ctl/Cmd-') This does three things:
 1. It stops subsequent repeated notifications.
 2. The text of the message is written to the Event Log file, along with the name and IP address of the person who did it.
 3. The icon stops blinking, and turns blue, to indicate that it's acknowledged, and someone's working on it.
 - **Basic acknowledgement** Only for duration of that state
 - **Timed** For the next n minutes, hours, or days
 - **Indefinite** Until cancelled
7. **Dependencies** InterMapper will suppress notifications if it can tell that a device is unreachable because of another failure. InterMapper supports automatic dependencies—it follows the links from the *vantage point* through the map to the failed device. If there's an outage on that path, InterMapper won't send notifications for the dependent device.
- **Automatic** InterMapper follows the links from the Vantage Point.
 - **Set the Vantage Point** - only one per map
8. **Charts** View the history of selected variables.

- **Open a status window for a device.**
 - **Tear off window** by dragging outside.
 - **Click an underlined value** to create new chart.
 - **Drag another underlined link** to add it to an existing chart.
9. **Edit > Server Settings** The server settings shows the preferences for a server.
- **Per server** Use the **Edit > Server Settings...**
10. **InterMapper RemoteAccess** Allows you to have all this fun, but from anywhere on the Internet
- **Connects to multiple servers** at remote locations
 - **Works through firewall** at client/remote site. You pick the port.
 - **SSL Encryption** is the default. You can install your own SSL certificate.

Chapter 3

Using InterMapper

You experience InterMapper through the [Map List Window \(Pg 46\)](#), where you view a list of available maps. When you open a map, it appears in a [Map Window \(Pg 41\)](#).

If you are using [InterMapper RemoteAccess \(Pg 373\)](#), you may be viewing more than one map list in the Map List window; one for each server.

You can customize InterMapper by defining [Helper Applications \(Pg 78\)](#) and by specifying what actions should be taken when you [double-click an object on a map \(Pg 83\)](#). You can also set [user preferences \(Pg 53\)](#) for InterMapper and InterMapper RemoteAccess.

Creating Maps

Use this section to find out how to [start your map \(Pg 57\)](#), to [use Autodiscovery \(Pg 59\)](#) to find and map each device on your network, and to [add devices \(Pg 65\)](#) and [networks \(Pg 68\)](#) manually. Once you are familiar with what maps are and how you can use them, you can add devices to your map by [importing them \(Pg 637\)](#), and can [export data from maps \(Pg 635\)](#) for use in spreadsheets and databases.

You can even [place a physical map image in the background \(Pg 104\)](#) of your map, and [use geographic coordinates \(Pg 640\)](#) as you import to place devices automatically at specific locations in relation to the background image.

Use InterMapper's [different probe types \(Pg 66\)](#) to query your devices in specialized ways to give you more accurate information about the states of those devices.

As you become more familiar with what InterMapper can do, you can [add networks \(Pg 68\)](#) and [scan them \(Pg 70\)](#). You can [create sub-maps \(Pg 71\)](#), allowing you to view large networks through an overview map, "drilling down" to see more detail as needed.

Arranging Your Map

Once you have created your map, you may want to [rearrange devices into logical groups \(Pg 99\)](#), [change the appearance of devices \(Pg 101\)](#), change the [device labels \(Pg 106\)](#), or [add text \(Pg 409\)](#) or a [background image \(Pg 104\)](#). For maps with large switches, you may want to [hide some detail \(Pg 128\)](#). For tips on arranging your map, see [Arranging Tips \(Pg 119\)](#).

Notifiers and Alerts

You can [set up devices to alert you to problems \(Pg 129\)](#) in a number of ways. When a device goes the specified state, a notifier is triggered, and alerts you to the problem.

You can [create your own notifiers \(Pg 131\)](#) and [configure them \(Pg 139\)](#) to send an [E-mail message \(Pg 144\)](#), page (through a modem or [network \(Pg 155\)](#)), [send a text message \(Pg 151\)](#) to a cell phone, or [execute a script or system command \(Pg 160\)](#). You can also [open a WinPopup window \(Pg 165\)](#) on a Windows machine, [send an entry to a Syslog server \(Pg 166\)](#), or [send an SNMP trap \(Pg 167\)](#).

You can attach notifiers in a number of ways:

- For each map, you can [define a default set \(Pg 86\)](#) of notifiers to be attached to a device.
- You can [attach one or more notifiers \(Pg 133\)](#) to one or more specific devices.
- You can create [groups of notifiers \(Pg 146\)](#) and assign them to a device all at once.
- You can [attach a notifier to one or more interfaces \(Pg 164\)](#) on a device.

If a device goes down, and other devices are attached to that device, you can [set a Vantage Point \(Pg 136\)](#). InterMapper can then determine that the attached devices are dependent on the down device, and will not send notifications for those devices.

Monitoring Your Network

InterMapper begins polling devices as soon as you create your map. A great deal of information is immediately available by viewing the [Status window \(Pg 185\)](#) for a device, network, or link. You also view and edit a device or network's information from its [Info window \(Pg 188\)](#). For routers, switches, or other devices with interfaces, you can view status or other information about specific ports through the [Interfaces window \(Pg 195\)](#).

You can set thresholds for a number of statistics:

- For devices, you can set thresholds for [packet loss \(Pg 200\)](#) or [network traffic \(Pg 208\)](#), and InterMapper alerts you when a behavior is out of range.
- For links, you can set thresholds Error, Link Utilization, and Interface Discards.
- You can set default thresholds the server, a map, or a device.

You can [create charts \(Pg 219\)](#) that graph one or more data values associated with a device. You can also [view a detailed Event log \(Pg 235\)](#) and [Outage log \(Pg 246\)](#) to help you troubleshoot problems accurately. You can even [create new log files \(Pg 257\)](#) for logging specific data.

If a device or link goes down, you can [acknowledge the problem \(Pg 202\)](#), which prevents InterMapper from continuing to send notifications. There are several options for acknowledging problems that allow you to control the resumption of notifications after acknowledgment.

You can [collect data from devices](#) (Pg 626) and save it in the [InterMapper Database](#) (Pg 615), through the InterMapper DataCenter. The data can then be retrieved for use in reporting and analysis. You can [set policies](#) (Pg 618) to specify how much data is retained and how long it is retained.

Server Settings

Use the [Server Settings panel](#) (Pg 249) to view [information about InterMapper](#) (Pg 251), to [set preferences](#) (Pg 253), and to [configure](#) (Pg 277) InterMapper's [Remote](#) (Pg 282), [Web](#) (Pg 289), [Telnet](#) (Pg 291), and [Authentication](#) (Pg 623) servers. You can also maintain InterMapper's [firewall](#) (Pg 278) and [user](#) (Pg 298) list, [enable and disable](#) (Pg 296) or [control access to maps](#) (Pg 305), and [create notifiers](#) (Pg 308).

InterMapper Reference

Use the InterMapper Reference to view comprehensive lists of [menu commands](#) (Pg 374), details about the available [device probes](#) (Pg 438), [file and folder locations](#) (Pg 628), and learn [advanced data import and export techniques](#) (Pg 649). You can also learn how to use and customize the [InterMapper web server](#) (Pg 689), and how to use the [InterMapper Telnet server](#) (Pg 702).

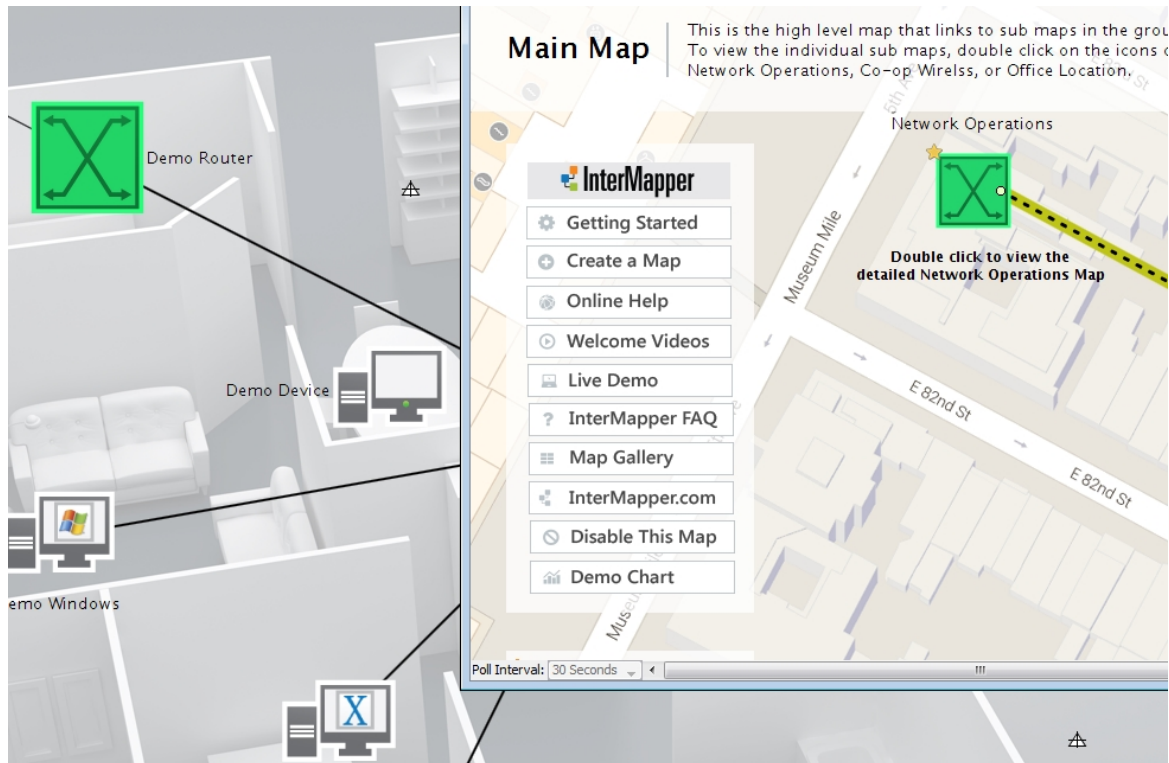
Troubleshooting InterMapper

Use the Troubleshooting section to help you learn about [IP addresses](#) (Pg 726), [Domain Name Servers](#) (Pg 730), [SNMP](#) (Pg 731), [WINS Names](#) (Pg 735), and view a number of frequently-asked questions.

Try out the Demo Maps

The first time InterMapper launches, it will open a Demo Map file that shows simulated network activity: outages, high traffic, and other problems that you'd see in a real network. (Although not as frequently, we hope...)

The image below shows a portion of an example map with a number of devices (rectangles) connected by various kinds of links (lines).



Here are some tips to help you understand the various items on the map:

- Devices are displayed in **green** to indicate that the device is up and running.
- Devices that are down **blink red** when InterMapper cannot communicate with them.
- **Click and hold** a device to see a status window of detailed information and outage history, or **Right/Ctrl-click** it and choose **Status Window** from the dropdown menu.
- You can **tear off** these status windows to keep them open by dragging the mouse outside their boundary.
- You'll hear **sounds** to indicate that there have been failures. (InterMapper can send e-mail or pages, too!) To silence these alarms, choose **Preferences...** from the **Edit** menu, click the **Sounds** subcategory of the **Behavior** category and clear the **Play sound notifications** check box.
- Lines (*links*) show **dotted lines** (*ants*) when traffic exceeds a threshold
- Links get a **yellow or orange background** when traffic exceeds 50% or 90%, respectively.
- **Circles at the ends of links** (they look like raindrops in puddles) indicate errors that have been detected by the interface.

- **Circles close to the device** indicate receive errors.
- **Circles close to the network** indicate transmit errors.
- **Click and hold on a link** to see a status window of port/interface information and traffic statistics, or **Right/Ctrl-click** it and choose **Status Window** from the dropdown menu.

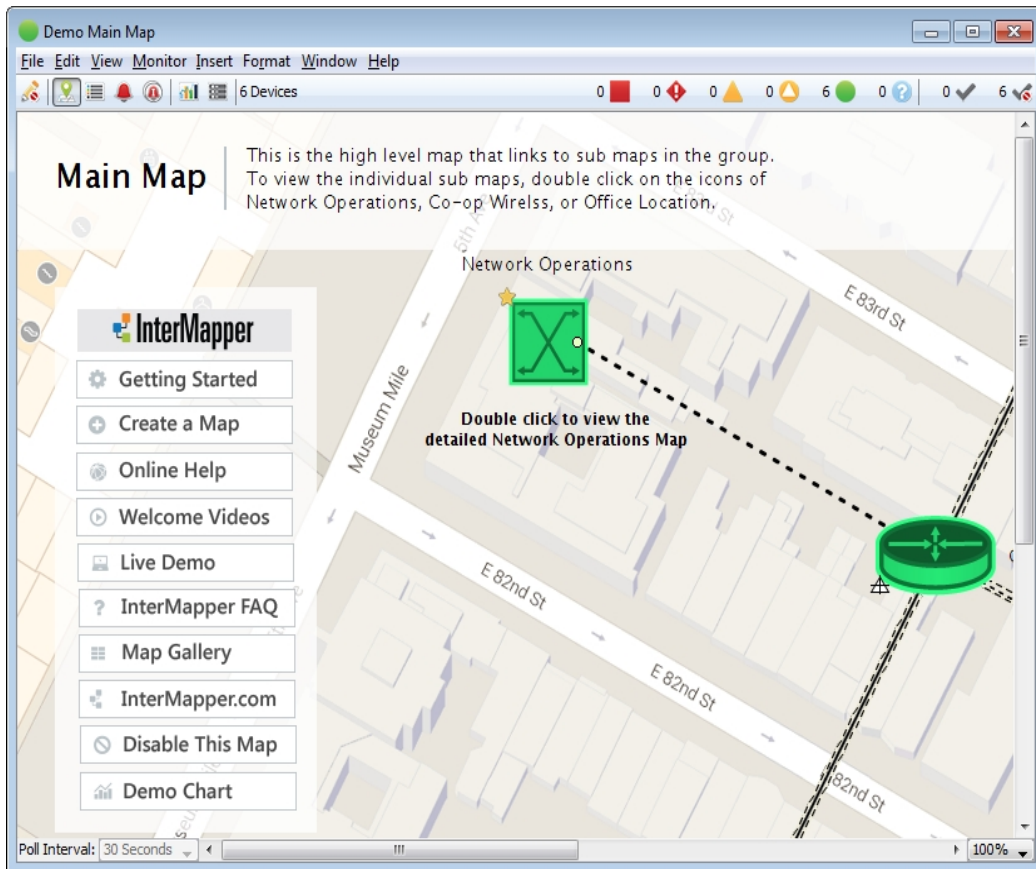
In addition, there are other things you may note on the map as it operates:

- Some devices become dim from time to time. That's because they're being *shadowed* by another failure on the map. We also say that those shadowed devices *depend* on all the devices on the path to it. InterMapper can automatically detect this state and will avoid notifying the network manager about outages if the dependent devices are unreachable because of the other failure.
- On several of the demo maps, a star appears on a device. That means that it's the *Vantage Point* for "shadowing". InterMapper will suppress notifications for a device if it's not possible to reach the device from the Vantage Point without going through a failed device. (It's in the "shadow" of a failed device.)

The Map Window

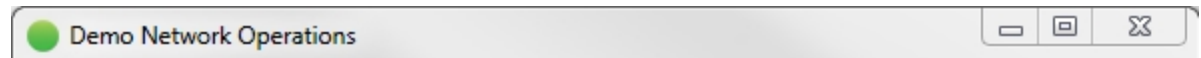
You view any map in a Map window. Below is one of the example maps installed with InterMapper.

For an in-depth explanation of the elements that appear in the map window, what they mean, and how to use them, see [Monitoring Your Network \(Pg 180\)](#).



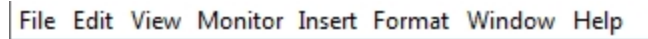
The Title Bar

The Title bar shows the map's title, its state, and has standard controls for zooming, minimizing, and closing the window.



The Menu Bar

The Menu bar contains the map's menus.



For a complete reference for each menu, see the [Command/Menu Reference \(Pg 374\)](#).

The Toolbar

The Toolbar contains buttons to toggle the map's edit mode and to switch from one view to another.



Switching Between Monitor Mode and Edit Mode

- Click the Lock button at the left end of the tool bar to switch the map between Monitor mode and Edit mode:



In Monitor mode - The map is not editable, and status windows appear when you click and hold a device, link, or network.



In Edit mode - The map is editable. Status windows can be opened with menu commands.

Tip: Press tab to switch between Monitor and Edit modes.

Switching Views in the Map Window

Click one of these buttons to switch to a different Map Window view.



Map view

Shows the map graphically, showing devices, networks, and their inter-connections.



List view

Shows the devices on the map as a list, with columns for the device's status, name, address, probe type, and current and previous condition.

- Click a column heading to sort by that column.
- Click again to sort in reverse order.
- Use the **Columns** submenu available from the View menu to choose the columns you want to view.
- Right-click a column heading to choose the columns you want to view, and to choose a column to sort by.

- Drag items from one map to another. The source map must be in List view. The target map must be editable, but can be in another view.

It is convenient to sort by Status so the most serious conditions appear at the top of the list.

Note: You can also view a global list of devices.

To view a global device list:

- With a server selected in the map list, choose **Device List** from the Map List window's Window menu. A list of all devices on the selected server appears.



Device Notifiers view

This view lets you see which notifiers are attached to each device on a map. Another way to think of it is as a "responsibilities" view - what devices apply to a certain notifier.

- Select a particular notifier from the dropdown menu; you can see the checkboxes for all its recipients.
- To set a value for all devices, hold **Alt** or **Option**, and set a value. The value you changes to the selected value for the entire column. This works on all check boxes, as well as on the **Delay**, **Repeat**, and **Count** columns.



Link Notifiers view

This view lets you see which notifiers are attached to interfaces on a map.

Attach notifiers to interfaces in exactly the same way as in the Device Notifiers view.



Chart view

Shows the list of charts for the map.

- Expand the tree to view a chart's datasets.
- Double-click a chart name to open the chart.
- Right-click the Chart List button to open a particular chart without switching the view.
- Right-click a chart to:
 - Show the chart
 - Rename the chart
 - Delete the chart
- Right-click a dataset to:
 - Show the chart containing that instance of the dataset
 - Show the device generating the dataset
 - Raise the status window for the device generating the dataset
 - Rename the dataset
 - Remove the dataset
 - Export data from the dataset
 - Delete data from the dataset



Dataset view

This view shows the datasets available for charting and data collection in

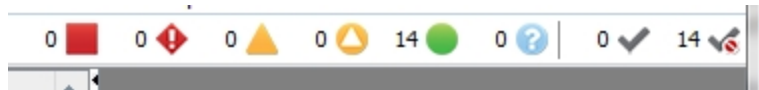
this map. With the map in edit mode, you can choose a retention policy for any dataset.

Shows the following:

- A list of devices on the current map.
- The dataset name, type, and current retention policy and variable for a selected device whose check box is selected.
- Any available interfaces and the available datasets associated with them.

The Map Legend

The Map legend to the right of the toolbar shows the different states of the map and the number of devices in each state. It also acts as a filter in list view.



Badge	Color	Meaning
	Red (Flashing)	Down - No response has been received from the device within the specified timeout period.
	Red (Solid)	Critical - The specified threshold for critical state has been met
	Orange	Alarm - The specified threshold for alarm state has been met.
	Yellow	Warning - The specified threshold for warning state has been met.
	Green	Up - The device is working below the specified thresholds.
	Gray	Unknown - The device is not being polled, so its state is unknown.
	Purple	Searching - The device is searching for adjacent routers (during auto-discovery) or is tracking down unnumbered interfaces.
		Acknowledge - Timed or Indefinite - The device's problem has been acknowledged and notifications are being suppressed, either indefinitely, or for a specified period of time.
		Acknowledge - Basic - The device's problem has been acknowledged, and notifications are being suppressed until the device comes back up, at which time the checkmark is cleared.
		List Acknowledged Devices - (Filter button) List all devices that have been acknowledged.
		List Un-Acknowledged Devices - (Filter button) List all devices that have not been acknowledged.

- Click a legend icon to view a list of devices that currently in that state.
- Click the icon again to go back to the previous view.
- Shift-click icons to view devices in more than one state.

Example: Shift-click the Alarm and Warning icons to see any devices in either of those states.

- Click one of the Acknowledge Filter buttons (to the right of the legend) to list only acknowledged or un-acknowledged devices.

Note: The filter buttons work in concert with the legend icons - clicking a Filter button shows only the devices in the selected state that are acknowledged or un-acknowledged. It is possible to click a filter button and see no devices.

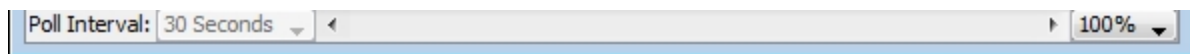
The Map Area

The Map area is the "canvas" on which you create your map. To get started, take a look at [Creating Maps](#). It is full of information about [starting your map \(Pg 57\)](#). The Creating Maps section is full of information for [creating \(Pg 57\)](#), [arranging \(Pg 99\)](#), and making your map look [just the way you want \(Pg 99\)](#) it to look. You'll also find a quick reference of [editing shortcuts \(Pg 95\)](#).

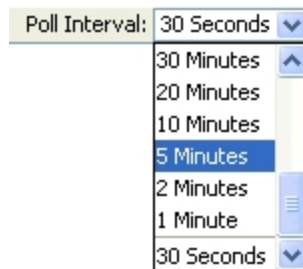
For an in-depth explanation of the elements that appear in the map window, what they mean, and how to use them, see [Monitoring Your Network \(Pg 180\)](#).

The Status Bar

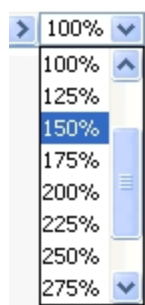
The Status bar contains controls for switching in and out of map edit mode, setting the polling interval, and zooming the map.



The **Poll Interval** drop-down menu sets the polling interval for the map.



The **Map Zoom** drop-down menu sets the zoom factor for the map. If you choose **Auto**, the map zooms automatically when you resize the window.



The Map List Window

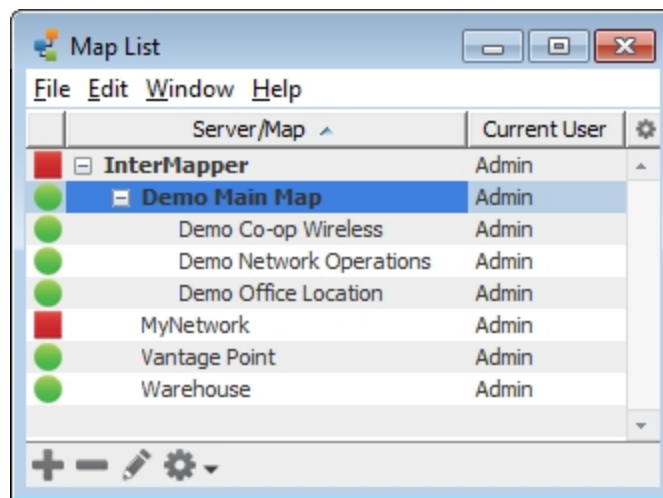
Use the Map List window as the primary interface to InterMapper.

- With InterMapper, you can control all aspects of the InterMapper server running on your local machine. You can also disable a map by right-clicking it and choosing **Disable Map**.
- With InterMapper RemoteAccess, you can access multiple InterMapper Servers from the same machine. If you have administrator access, you can edit all server settings on a remote server. You can also disable a map by right-clicking it and choosing **Disable Map**.

The menu items available in the File menu differ slightly between InterMapper and InterMapper RemoteAccess. For more information, see the [File Menu \(Pg 375\)](#) reference.

The Map List Window

Use the Map List window to view a list of maps. If you have InterMapper RemoteAccess, you can also view a list of other available InterMapper servers, to log into one or more servers, and to view a list of maps currently running on each server.



The Map List Window

Using the Map List Window

Here are a few tips for getting the most out of the Map List window:

- A green map name indicates that the map's window is open.
- Position the mouse cursor over a map in the list to view its DNS Name and/or IP address, and the port on which it's listening for InterMapper RemoteAccess connections.
- Right-click (or Ctrl-click) a map to choose commands from the context menu.
- Use the Quick Menus, described below, to perform map-related commands and operations.

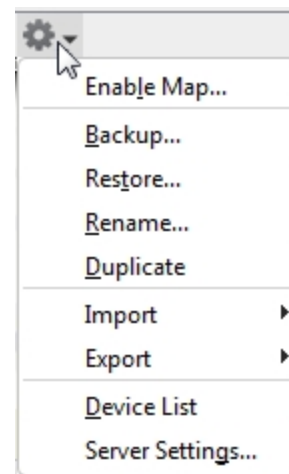
Quick Menus

Use the quick menus at the bottom of the map list window to access frequently used functions.

- Click the **Add** menu to add a map or server.
- Select a map and click the **Delete (-)** button to remove the map from the Map Window.
Note: that this does not actually delete the map; it simply disables it.
- Select a server, then click the **Info** button to view or change info about a server.



- Use the **Tools** menu to perform a number of map-related operations. You can enable and disable maps, backup, restore, or duplicate a map. You can also import or export maps and data files, as well as open the Server Settings window...



Arranging your Maps into Folders

You can arrange your maps into folders as shown above, using the Server Configuration>Enabled Maps pane of the Server Settings window. For more information, see [Enabled Maps \(Pg 297\)](#).

Viewing the Global Device List

From the Map List window, you can view a list of all devices on a particular server.

To view a global device list:

- With a server selected in the map list, choose **Device List** from the Map List window's Window menu. A list of all devices on the selected server appears.

The Device List Window

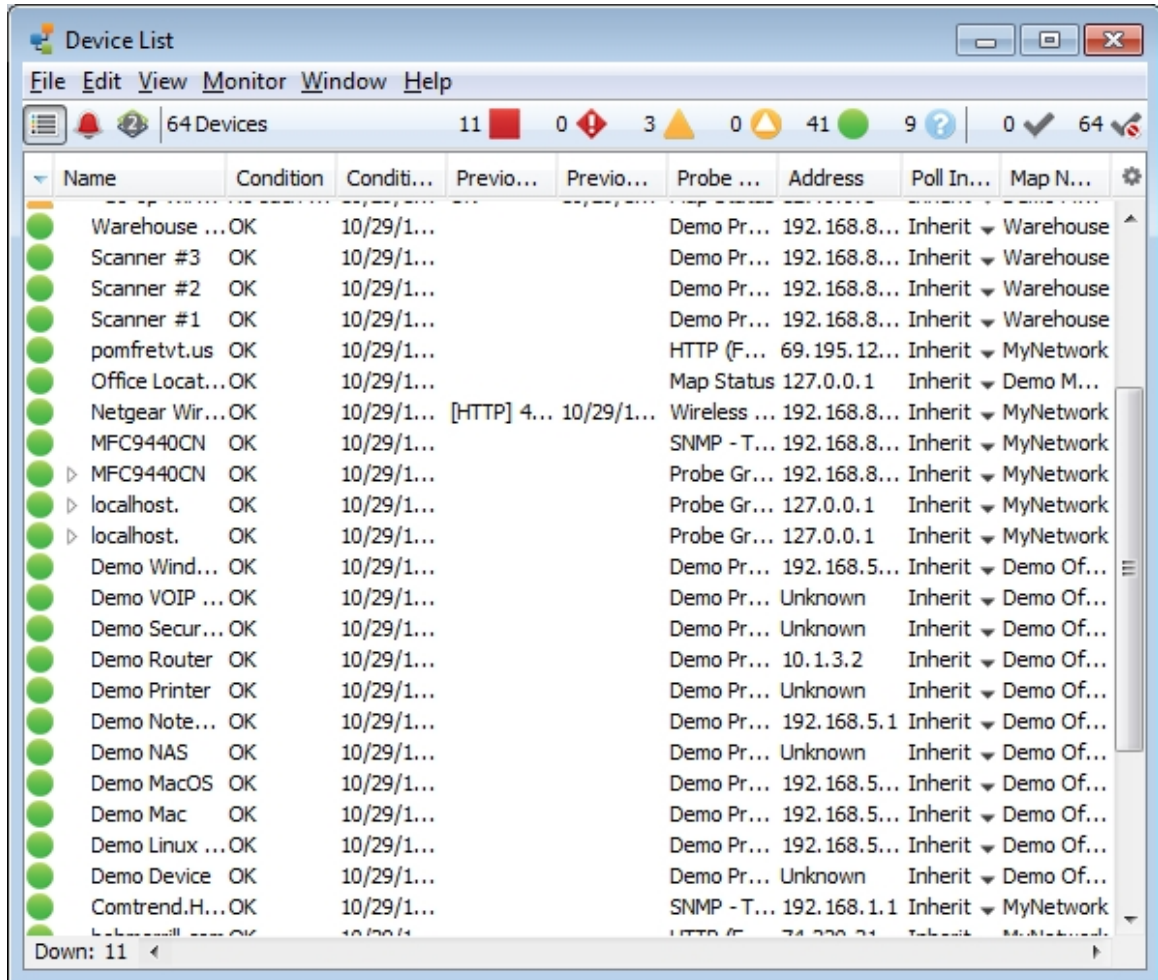
Use the device list window to view

- a global list of devices
- a list of notifiers
- a list of Layer 2 devices.

List View



Use the Device List view to see a global list of devices used in all of the maps on the InterMapper Server.



The Device list view

Device List Columns

Status:	The device's state. The icon's color matches its color in the map.
Name:	The first line of the device's name as shown on the map
Condition:	The most severe (i.e. worst) status for the device
Date:	Shows when the device entered its current state
Previous con-	The device's status before it entered the current state

dition:

Date & Time: Shows when the device entered the previous condition

Probe Type: Shows the probe type for the device

Address: Shows the network address of the device

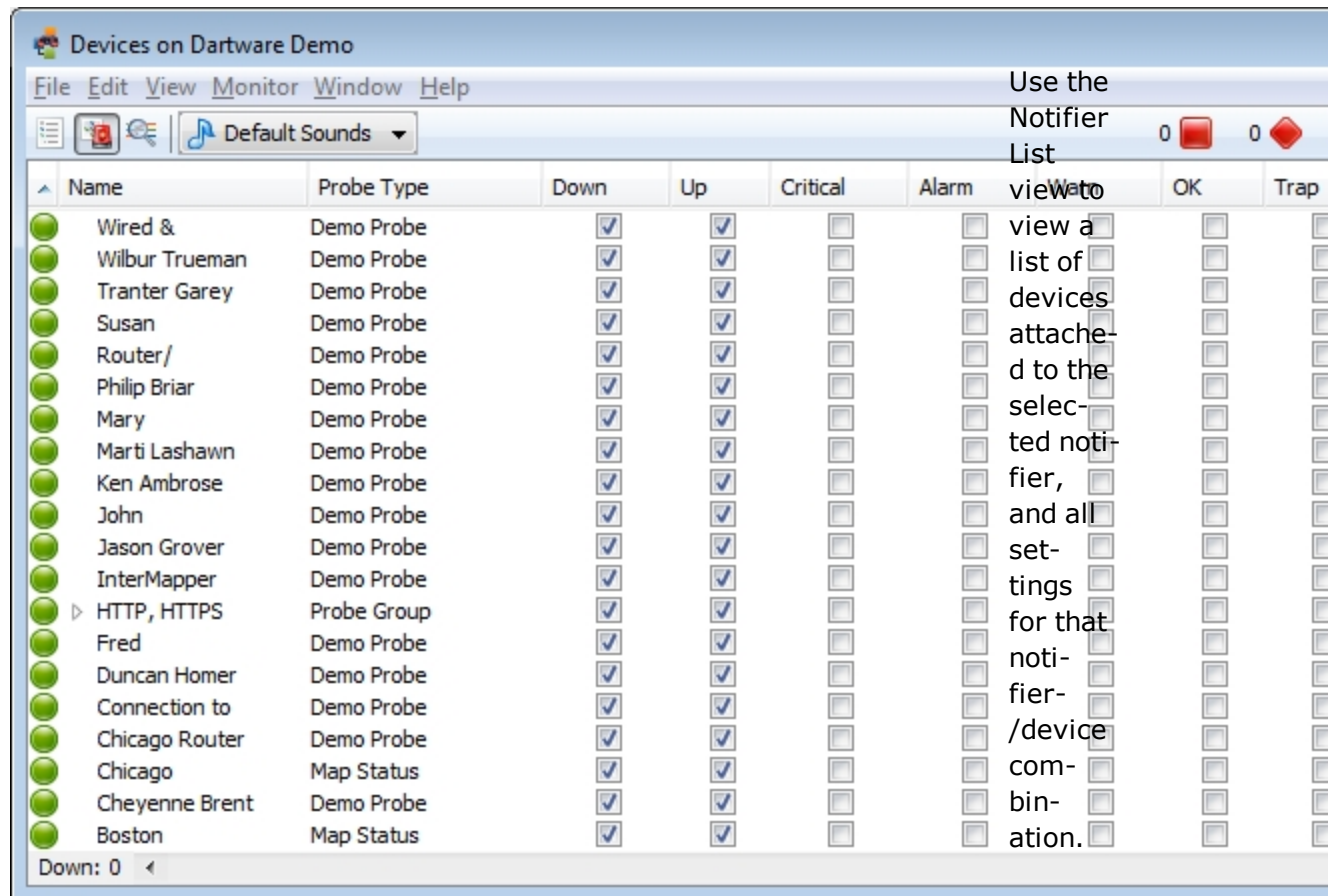
Map Name: The name of the map in which the device appears

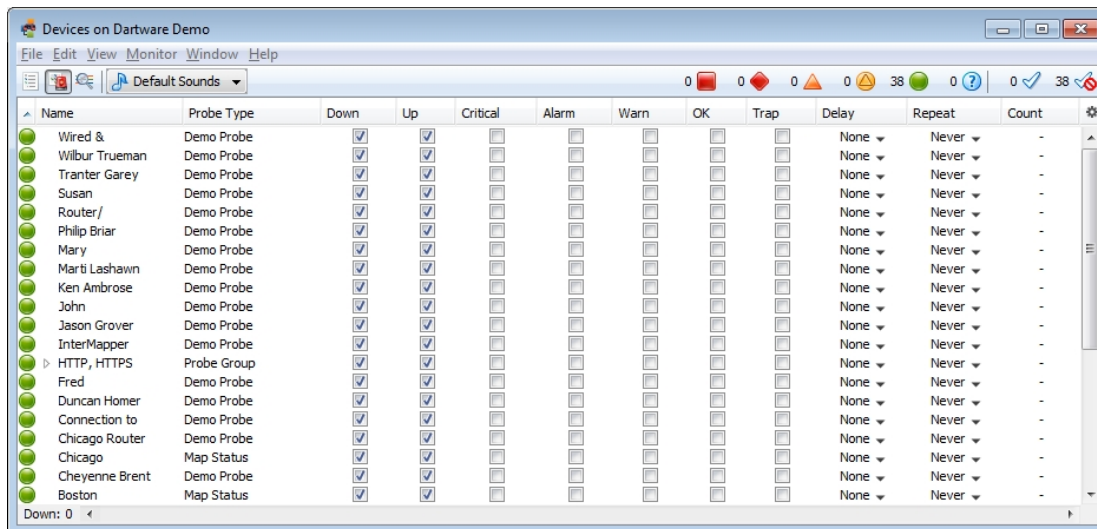
Manipulating the Device List

There are a number of ways to interact with the Device List:

- Double-click an entry in the Device List to switch to the proper map, and highlights the particular device with zooming rectangles.
- Sort the list by clicking a column heading. Click again to re-sort in the opposite order.
- Resize columns by dragging the separator between the columns to the proper size.
- Re-order the columns by dragging a column to a new position in the Device List window.

Notifier View





The Notifier list view

Using the Notifier List view, you can quickly attach a notifier to a device or check to see which devices are attached to a given notifier. You can set delay and repeat parameters to control escalation of a problem.

- Choose a notifier from the dropdown menu.
- Select or clear the check boxes for the devices states at which you want to trigger an alert.
- Set delay, repeat, and repeat count settings for the device as needed.

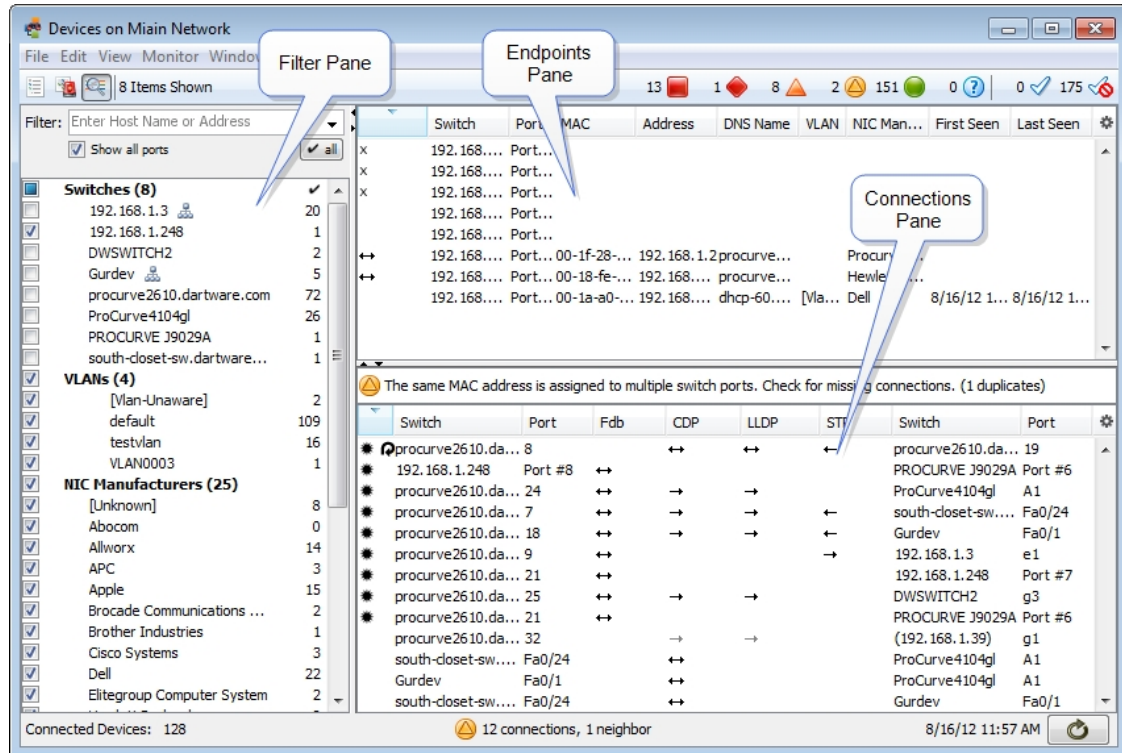
Layer 2 View



Use the Layer 2 List view to view a list of switches, VLANs and NIC manufacturers, with a list of devices connected to each.

For more detailed information on the Layer 2 view, see [The Layer 2 View](#).

The Layer 2 View

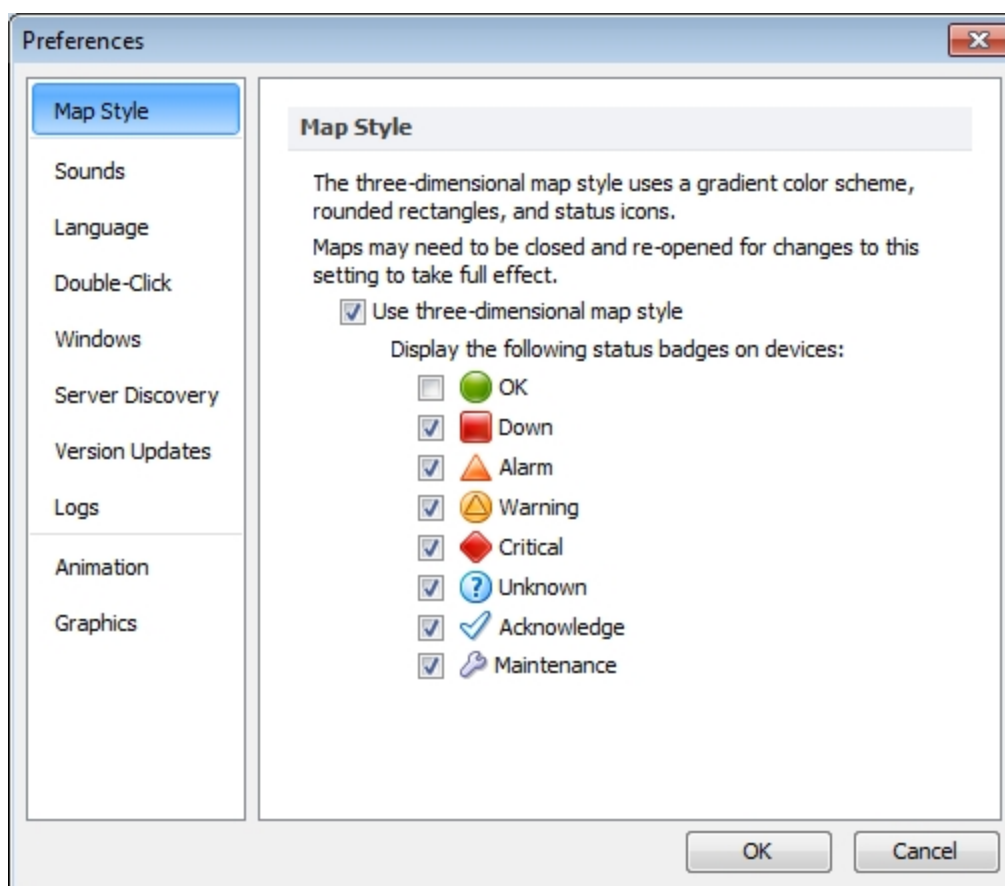


Understanding the Layer 2 View

The Layer 2 View contains three main panes:

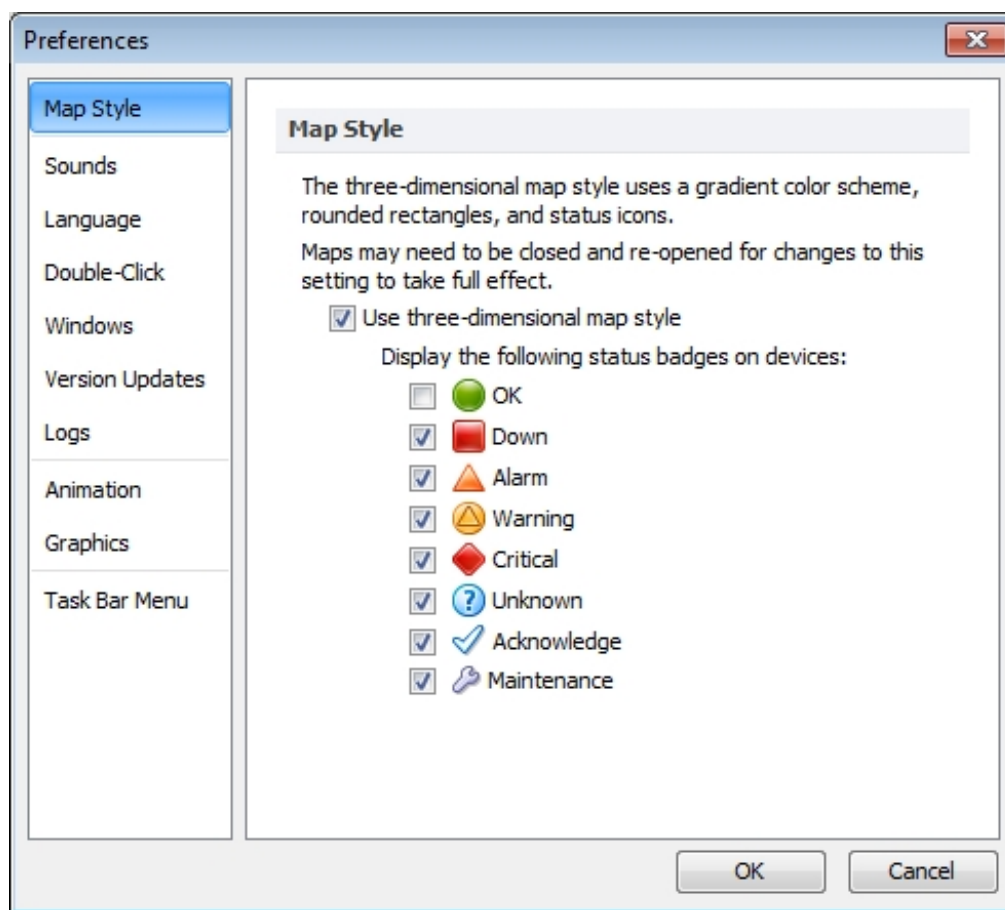
- The **Endpoints pane (Pg 347)** - the upper right pane lists all switch ports and the devices connected to them. It contains only those ports and devices that match the filter criteria in the Filter pane.
- The **Filter pane (Pg 345)** - the left pane provides criteria for showing or hiding endpoints based on their presence on a particular switch, VLAN, or the endpoint's manufacturer. lists available switches, the VLANs in which they appear, and manufacturers of network interface cards of the devices connected to them. Use the check boxes to select or hide endpoints in the Endpoints pane, and type additional criteria to help select the endpoints you want to view.
- The **Connections pane (Pg 348)** - the lower right pane provides details about switch-to-switch connections.

InterMapper User Preferences



*InterMapper
RemoteAccess*

Use
the



InterMapper

Pr-

ferences command, available from the Edit menu, to set user preferences for the InterMapper user interface. These settings affect only the copy of the InterMapper or InterMapper RemoteAccess you are running - it does not affect other users' settings.

To view and edit InterMapper's preferences:

1. From the Edit menu, choose **Preferences...** The Preferences window appears.
2. In the left pane, click the name of settings you want to change. If necessary, expand a section to view the more settings. The selected settings panel appears in the right pane.

Map Style

Use the Map Style panel to set your preference for the style in which your maps are displayed.

- **Use three-dimensional map style** - (checked by default) Check this box to use the current three-dimensional display style, with gradient colors, rounded

rectangles, and status icons.

- **Display the following status badges on devices** - select or clear the checkboxes for the badges you want to appear on devices. By default, the Ok badge is not checked, but all other badges are checked.

Sounds

Use this panel to enable or disable sound notifications. Select or clear the **Play sound notifications** check box to turn sounds on or off.

Language

Use this panel to specify the language you InterMapper to use in its user interface.

To change the language from the system default, choose your language from the Language Options dropdown menu. All available language options are listed.

Note: You must restart InterMapper or InterMapper RemoteAccess after changing this option.

Double-Click

Use this panel to specify a default action to take for a device or network that doesn't have an action assigned. Use the **Action** dropdown menu to choose from these options:

- **Helper App...** - Choose a helper application to launch.
- **Open URL...** - Enter a URL in the **Action** text box.
- **Built In...** - Choose an InterMapper menu command from the menu tree. By default, the Info window opens.

Windows

Use this panel to specify whether charts and status windows are hidden when a map becomes inactive. You can also reset the state of "Ignored" windows.

- **Hide charts and status windows when Map is inactive** - Click to select this check box to hide charts and status windows for any map that is not the active window. If the box is not checked, any open charts and status windows remain open.
- **Reset Ignored Windows** - a number of alert messages provide the option not to show the message again. Click this button to reset the state of all Ignored windows.

Server Discovery (InterMapper RemoteAccess Only)

Use this panel to specify whether or not to search for InterMapper servers on the local LAN.

- **Discover InterMapper Servers on the LAN** - Click to select this check box if you want InterMapper RemoteAccess to search for InterMapper Servers on the local LAN.

Version Updates

Use this panel to enable or disable the Automatic Update function by selecting or clearing the **Automatically check for updates** box and select **Daily**, **Weekly**, or **Monthly** from the dropdown menu. This function is also available from the [InterMapper Control Center](#) (Pg 25). To check for updates immediately, use the **Check Now** button on the InterMapper Control Center.

Logs

Use this panel to control the amount of information saved in the server log and whether to save it to disk.

- **Log Line Count** - Specify the number of lines of the server log that appear in Debug, Event or Outages Log window. This can reduce the amount of memory required to display a log window.
- **Client Debug Log** - Select the **Store Client Debug Log on disk** check box to save the debug log to your local disk.

Animation

Use this panel to specify your preference for animation settings. Faster animation looks better, but may use more CPU power than you would like, if you are running a slower CPU or have some very large maps.

- Select or clear the **Display Animations** check box to turn animations off or on. (They are off by default.) This turns off traffic indicators (ants) and transition effects (scale changes, scrolling to found devices, effects when windows opening or closing, etc.)
- **Animation rate** - Choose an animation rate by moving the slider left for slower rates or right for higher ones. The selected rate appears in the upper right above the slider.

Graphics

Use this panel to control the way graphics are rendered.

Use the **Anti-aliasing** controls to smooth the jagged look of diagonal and curved lines. Some users find that anti-aliased text or lines are blurry or fuzzy. Select or clear the check boxes to apply anti-aliasing to text or graphics.

Note: The Anti-aliasing settings are "hints" to help the graphics system render the graphics. The settings may be ignored by some systems.

Use the **Image Scaling** slider to choose level of quality to use when viewing maps at a zoom level other than 100%. The algorithm you choose may affect application performance.

Task Bar Menu (InterMapper only)

Use this panel to specify whether to show a task bar icon for the InterMapper Control Center.

- **Show status in task bar** - Select this checkbox to show the status icon in the task bar (Windows) or menu bar (Mac).

Chapter 4

Creating Maps

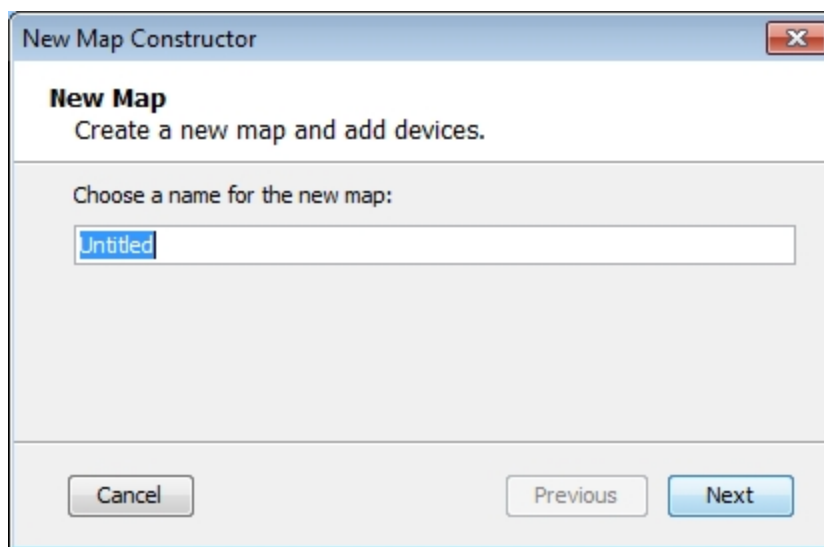
Starting Your Map

When you launch *InterMapper*, a Map List window appears. It contains several demo maps, which show examples of network maps, and contains brief descriptions of the elements appearing on the maps. Double-click a map to open it.

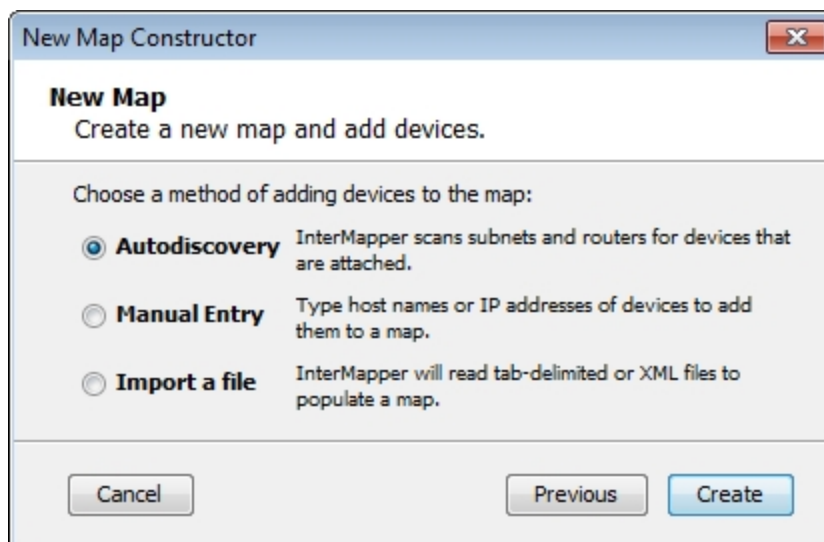
After you have explored the demo maps, you are ready to use the Auto-discover function to create your first map.

Creating a New Map

To create a new map, choose **New Map...** from the File Menu. The New Map Constructor window appears:



Enter a map name, and click **Next >**. The second page of the New Map Constructor appears.



- **Autodiscovery** - InterMapper's Auto-discover function automatically scans your network, looking for network devices to add to your map. It uses several heuristic techniques (including SNMP probes, ICMP echo packets, and DNS and NBP queries) to discover all the devices that are present. It then places those devices on a map.
- **Manual Entry** - Type or paste a list of host names or IP addresses for the devices you want to add to the map.
- **Import a file** - Specify a tab-delimited, CSV, or XML import file. For more information, see [Importing Data Into Maps \(Pg 637\)](#).

For information on using the Auto-discover function, see [Using Auto-discover \(Pg 59\)](#).

Importing Data into a Map

You can also create a map by importing data in a text file. For more information, see [Importing Data Into Maps \(Pg 637\)](#).

InterMapper Labels

InterMapper places a label on each device it finds. By default, it uses the device's full DNS name. Networks are labeled with both an IP address and the number of bits in the subnet mask (indicating the network range). For example, the network labeled 192.168.1.0/24 indicates that the IP devices are in subnet 192.168.1.0, with a subnet mask of 24 bits (255.255.255.0).

Note: You can change the label that appears for each device using the **Label...** command, available from the [Format menu \(Pg 411\)](#).

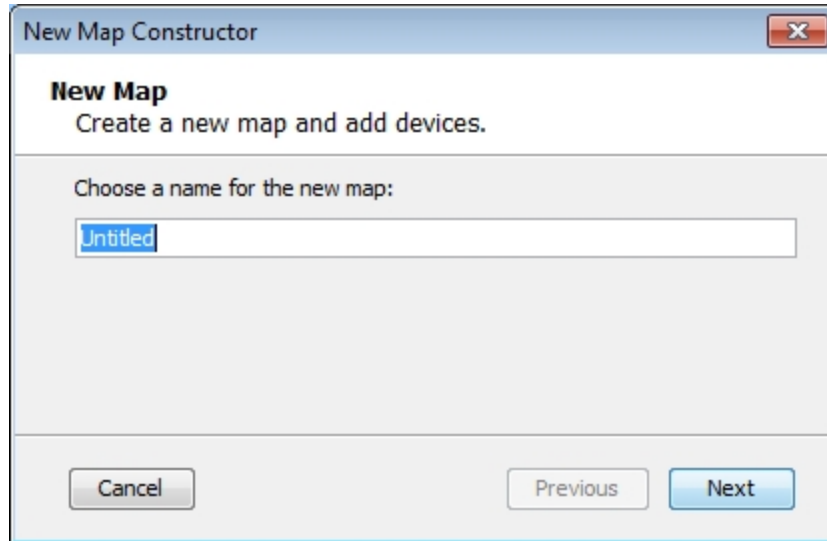
Using Auto-Discover

You can use Auto-Discover to create a new map. If your network contains Layer 2-enabled switches, you can also use Layer 2 information to increase the accuracy of a map's representation of your network topology. For more information, see [Mapping With Layer 2 \(Pg 353\)](#).

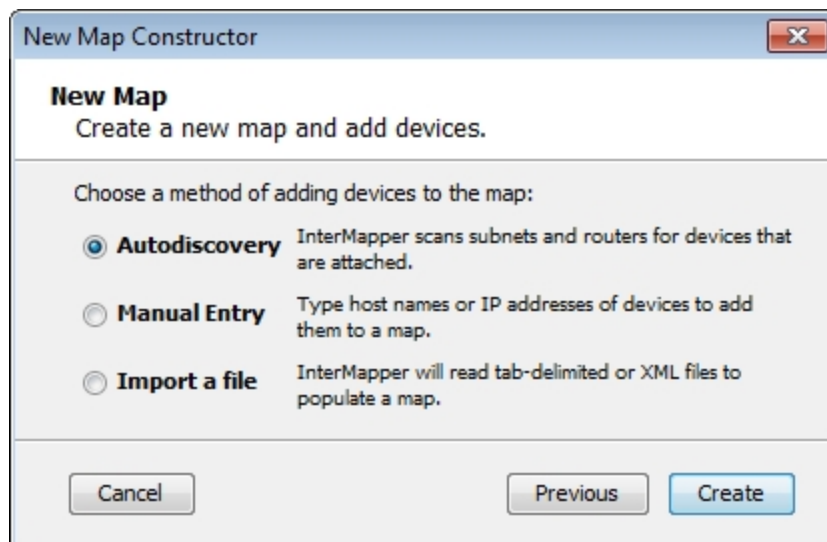
For existing maps, you will need to use the [manual technique \(Pg 353\)](#) for converting the map. For new maps you create with Auto-Discovery, use the [automatic technique \(Pg 353\)](#).

To Auto-Discover to create an initial network map:

1. From the File menu, choose **New...** The New Map Constructor window appears.
2. Enter a map name and click **Next**.



3. Click to choose **Auto-discovery**, then click **Create**. The Auto-matic Device Discovery window appears, as shown below.



4. Enter a host name or IP address you want to use as the starting point for auto-discovery.

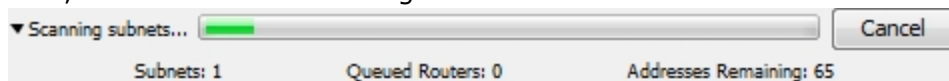
A name is suggested for you. It is the DNS name or IP address of a router, or if there's no

router, the computer InterMapper is running on. Use the default value, or enter any of the following:

- A DNS name
- An IP address (if you want to create a map of another part of a network.)

If you enter the name or address of an SNMP-speaking router, InterMapper draws interconnections to other routers in the network more quickly.

5. If you have SNMP-speaking devices in your network, specify an [SNMP Community \(Pg 731\)](#) string.
6. Select your Discovery Options, as explained in [The Auto-Discovery Window \(Pg 61\)](#) below.
7. Click the **Filter** button to set a filter for the discovery.
8. Click **OK** to start the Auto-discovery process. A Discovery Status bar appears as shown. The status bar shows progress statistics for subnets, queued routers, and addresses remaining to be scanned:



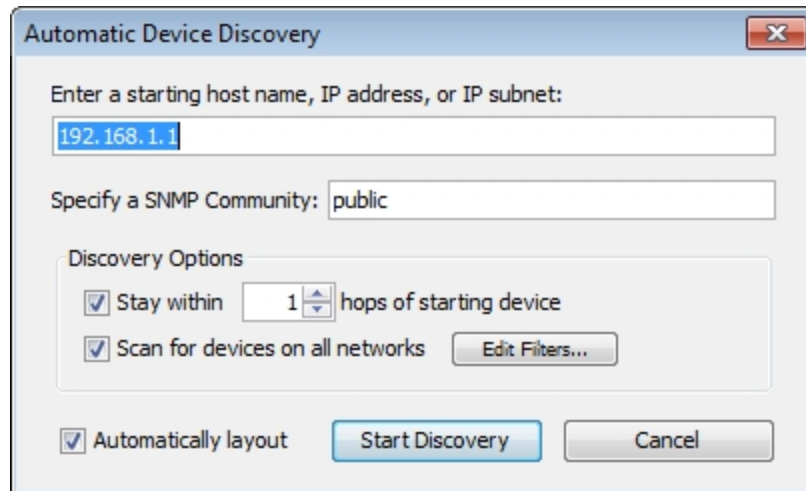
9. As the network is scanned, discovered devices appear in the current map (or in a list if you have cleared the **Automatically Layout** check box.) When InterMapper has found all the devices within the specified subnet, the Discovery Status bar disappears.



Click the Map View button near the upper left corner of the Map window to view your network as a map, showing devices and networks as icons, with the interconnections between them.

To stop the Auto-discover process:

- Click the **Cancel** button. The discovery process is stopped, and no new devices or networks are added. All devices added before you stopped the process remain in the list.



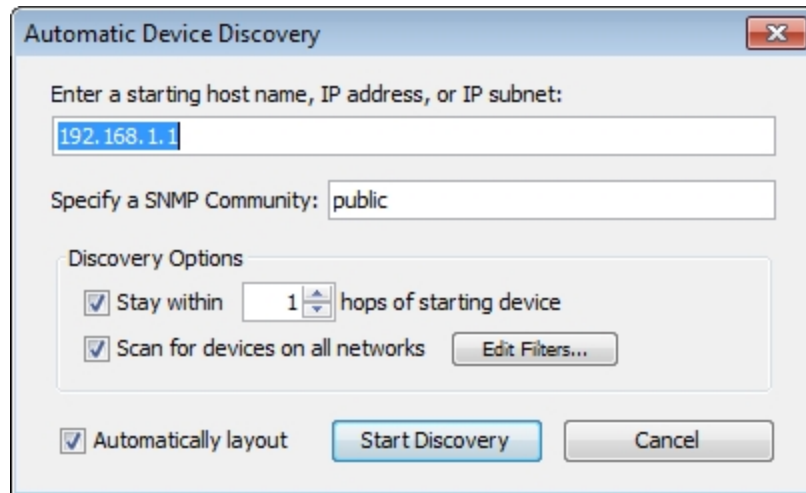
The Automatic Device Discovery Window

You control the starting point, the [SNMP Community string \(Pg 731\)](#), the breadth of the network search, and the kinds of devices that are automatically added to the map using this window.

- **Starting host name** -

The [DNS name \(Pg 730\)](#), [IP address \(Pg 726\)](#), or [WINS name \(Pg 735\)](#) of a device to use as a starting point for the auto-discovery.

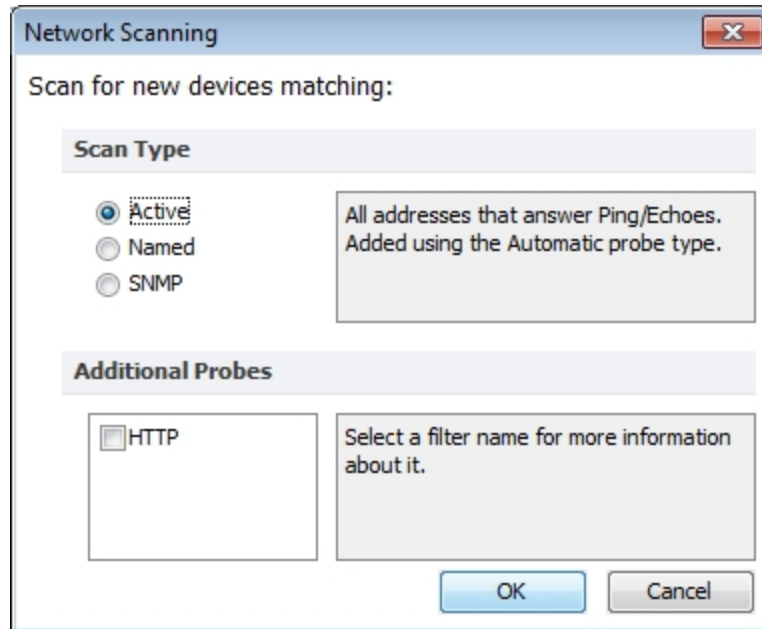
- Specify an SNMP community - The SNMP Read-only community string to be used to interrogate all devices. (InterMapper attempts to read SNMP information using the specified community string. It is set to 'public' by default.)
- **Stay within *NN* hops of starting device** - Stops autodiscovery after InterMapper has searched the specified number of hops from the starting device.
- **Scan for devices on all networks** - Specify which kinds of devices should be automatically added to the map. Click to check this box, or click **Edit Filters...** to open the Network Scanning window.
- Click **Automatically layout** to let InterMapper layout the map automatically.
- Click **Start Discovery** to initiate a scan of the specified host.



The Network Filter Dialog

Check the filters you want to use to add devices to the map:

- **Active** - InterMapper performs a complete IP address scan for each network. A device is added for each IP address that responds.
- **Named** - Each IP address in the subnet is looked up in the DNS. If a corresponding name is present, the device is added to the map.
- **SNMP** - InterMapper sends an SNMP GetRequest to each address in the range. Any device that responds is added to the map and uses the SNMP Basic Traffic probe. If the device does not respond to SNMP, the probe is set to Ping/Echo.
- **HTTP** - If the device responds to an HTTP request, an HTTP probe is added to the device (along with SNMP Basic Traffic or Ping/Echo probe), and the device becomes a [probe group](#).



What Happens During Autodiscovery?

During autodiscovery, InterMapper attempts to discover all devices on a network, based on the IP address and SNMP string provided. It does this by querying the router and ARP tables. Then, using any scan filters specified in the Network Scanning window, it scans all attached subnets, mapping all devices it finds, until it reaches the hop count specified in the **Discovery Options** section of the Automatic Device Discovery window. It then performs the following processes concurrently and iteratively until the specified limits are reached:

- If InterMapper discovers an SNMP-speaking router, it attempts to discover what interfaces the router has, and what other routers are connected to those interfaces. InterMapper then queries each of the discovered routers for their connected networks, and begins autodiscovery on each network.
- For each network or subnet discovered, InterMapper pings every address on that subnet to find more active or named devices.
- When InterMapper finds a device, it uses several techniques to characterize it. For example, it sends SNMP queries (with the specified SNMP community strings) to determine what kind of device is present.

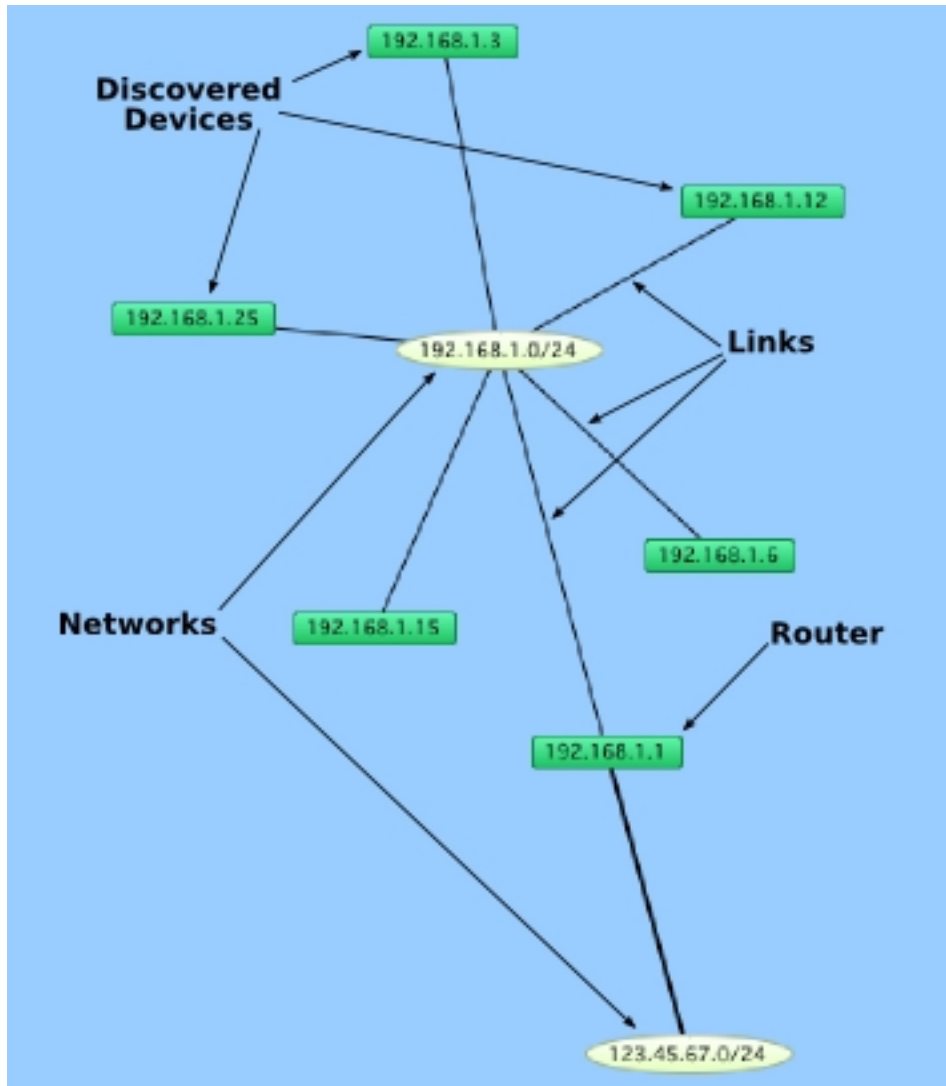
Warning: *In autodiscovery mode, InterMapper may ping or query every device address on a subnet. If your network has an intrusion detection system, autodiscovery may trigger your intrusion alarms. Be sure to check with the network manager before using this feature.*

Note: *It may take a long time to do autodiscovery on a large subnet (a Class A or B subnet). InterMapper limits its autodiscovery queries to two per second so that it doesn't overload any networks and thus it takes about 32,000 seconds (a shade under 10 hours) to scan that class B subnet (with 65,535 addresses) completely.*

To create your maps more quickly, you can type or paste one or more host [DNS names \(Pg 730\)](#), [IP addresses \(Pg 726\)](#), or [WINS names \(Pg 735\)](#) into the Add Devices... window (Insert menu). (WINS names must be preceded by "\\".) InterMapper immediately adds them to the map and connects them to the proper network.

You can also import a list of devices from a text file. For more information, see [Importing Data Into Maps \(Pg 637\)](#) .

Below is a typical map after autodiscovery has finished.



Autodiscovered devices and networks. Routers are interconnected by links to networks.

Adding Devices Manually

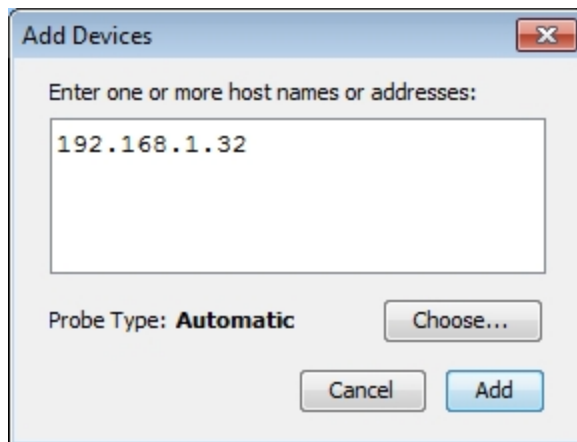
Add devices to your map manually using the **Device...** command, available from the Insert menu or the **Add Device(s)...** command, available from the context menu

To add devices manually:

1. Make sure the map is in Edit mode.
2. From the Insert menu, choose Device..., or Right/Ctrl-click in the window and choose **Add Device(s)...** from the context menu. The Add Devices window appears, as shown below.
3. Enter the device names and/or addresses as shown below.
4. The device(s) will be monitored with the indicated probe. To select a different probe type, click **Choose...** and select a probe as described in [Select Probe Window \(Pg 66\)](#).
5. Click **Add**. All devices entered are added to the map.

Note: If you enter a DNS name, the device is added to your map only if a DNS entry can be found.

- **Enter one or more host names or addresses** - Enter individual host names or addresses or paste a list of DNS names, IP addresses, or WINS names into this window. Entries must be separated by commas or by whitespace characters, such as spaces, tabs, or carriage returns. You can copy a list of host names and addresses from a text file or from a traceroute program. You can also use [WINS names \(Pg 735\)](#) (preceded by "\\"). For each entry that responds, a device is added to the map.



Add Device(s) window.

- **Probe Type** - Shows the type of probe currently assigned to the device. Click **Choose...** to open the Select Probe window and choose a different probe.
- Click **Add** to add the devices to the map.

Note: If any of the device names cannot be resolved (if a device name is not configured in your domain name system server) or if a device cannot be tested with the selected probe, don't worry; you'll get a chance to correct the entry.

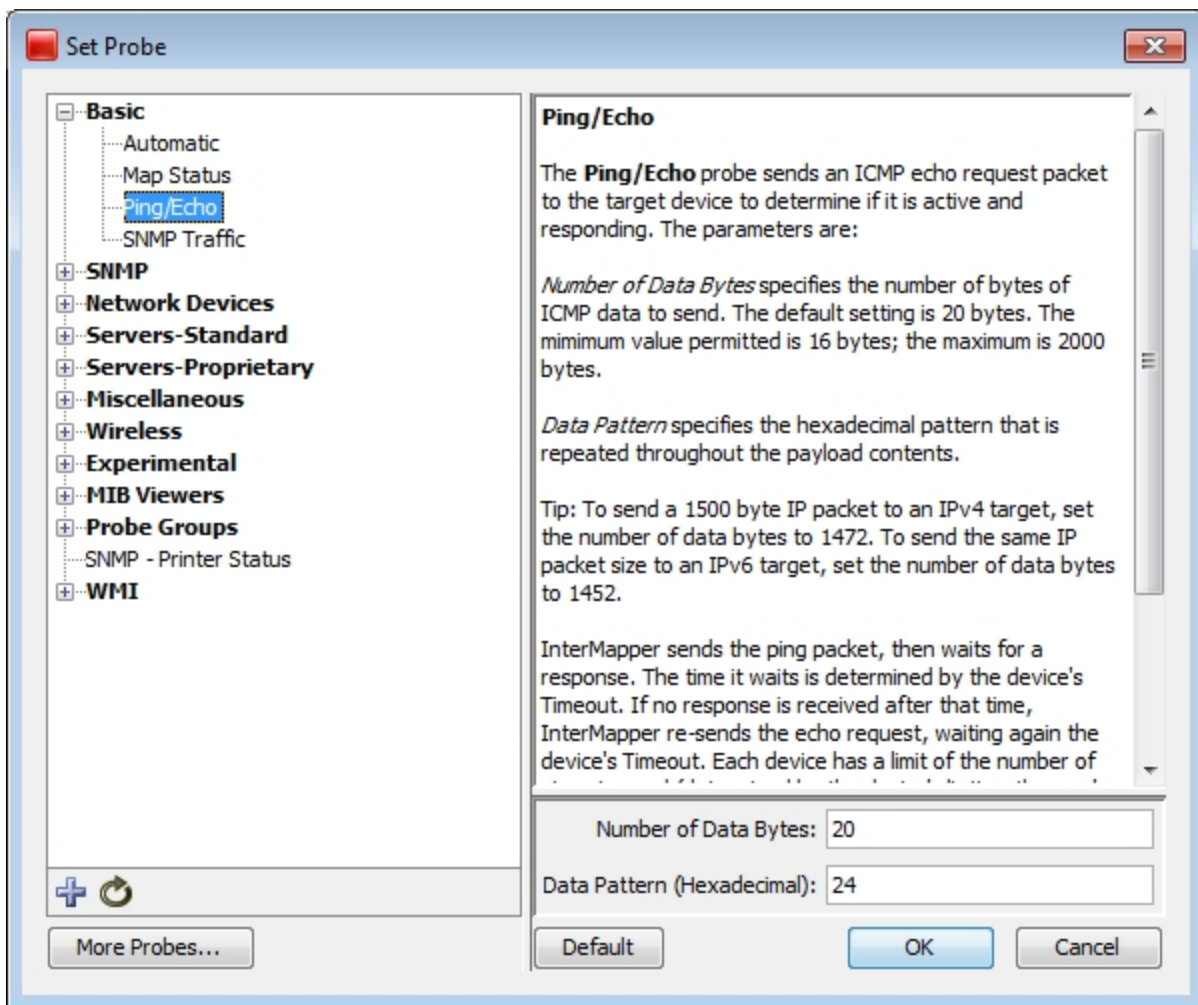
IPv6 Note: To ensure that when possible, host names are resolved to IPv6 addresses rather than IPv4 addresses, enclose the host name in square brackets ([]) as shown in the example.

Set Probe Window

Use the **Set Probe** command, available from the Monitor menu, the device's context menu, or by clicking **Choose...** in the Add Device(s) window, to view the Select Probe window. From this window you can choose and configure the probe for the selected devices.

- The left pane contains a hierarchical list of probes, divided into sections and subsections.
- The right pane shows the description and configuration options for the selected probe.

For a comprehensive list of probes with descriptions, see the [Probe Reference \(Pg 438\)](#).



To choose and configure a probe:

1. **Choose a section** - In the left pane, click plus (+) to expand the section and subsections to view the probes. Click minus (-) to collapse an expanded section or subsection.

2. **Choose a probe** - In the left pane, click a probe within a section or sub-section to select it. The description and options for the probe appear in the right pane.
3. **Set the probe's options** - In the right pane, enter or select the options you want to use with the selected probe. These options vary, depending on the probe. Click **Default** to reset the probe's options to the default settings.
4. Click **OK** to choose the probe.

Additional actions available from the Set Probe window:



Import a probe - click this button and select from a standard file dialog to import a probe file.



Reload probe list - click this button to reload the list of probes found in the InterMapper Settings/Probes folder.

More Probes... Click this button to launch your browser and view a list of probes contributed by InterMapper users.

Adding Networks to the Map

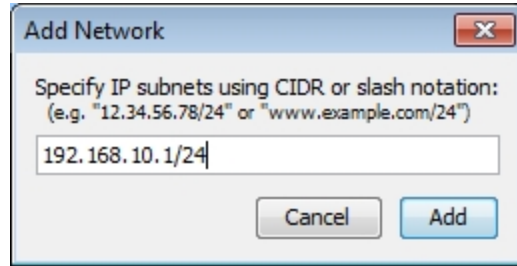
InterMapper uses "network ovals" to represent a "subnet" - a range of IP addresses. It uses these networks as graphical connecting points for all the devices on the subnet. When InterMapper places an SNMP-speaking device on a map, it automatically adds a network for each of its interfaces.

You can also add new networks manually.

To add a new network:

1. From the Insert menu, choose **Network...** An Add Network window appears, as shown below.
2. Enter the IP subnet information or range and click **OK**. For more information on IP addresses and subnets, see [About IP \(Pg 726\)](#).

The network is added to the map as an oval, labeled with the network information you entered. Any devices that belong to that subnet are automatically connected to the new network.



Add Subnet... window.

Enter an IP subnet (in the form x.x.x.x/yy).

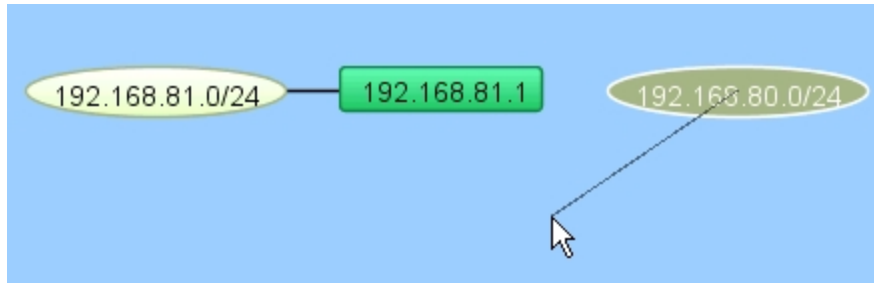
Note: Adding a subnet does not automatically initiate the discovery process. To scan the new network, right-click the new network oval and choose Scan Network... For more information, see [Scanning a Network \(Pg 70\)](#).

Adding and Removing Links

InterMapper may not connect devices to the proper network in every case. In such a case, you can make the connection manually.

To add a link manually:

1. Make sure the map is in [Edit mode \(Pg 180\)](#).
2. Right/Ctrl-click one of the objects you want to link to another.
3. From the menu that appears, click **Attach To**. A line appears, connecting the selected object to your mouse cursor, as shown:



4. Click the object you want to connect to. A link is created between the two objects:



Note: Once a manual connection has been established, InterMapper remembers it. You can drag manually-connected items around the map, and they work just like those links InterMapper has created automatically.

To remove a manually-connected link:

1. Make sure the map is in [Edit mode \(Pg 180\)](#).
2. Right/Ctrl-click the link and choose **Remove**. The link disappears.

Scanning A Network

InterMapper can scan an IP address range to discover all the devices on that network. It then adds those discovered devices to the map, and connects them to the proper network.

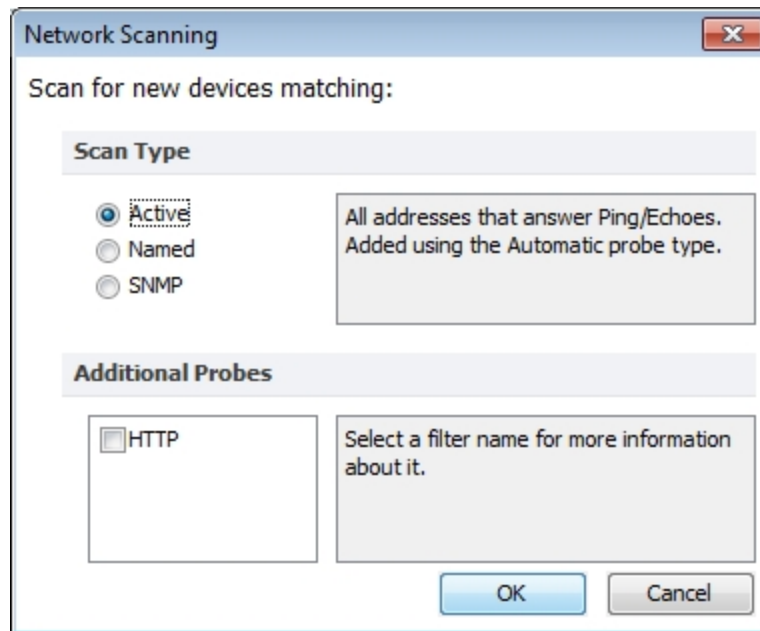
To scan a network:

1. Click to select a network oval, then click the Insert menu.

or

Right-click the network oval.

2. Choose **Scan Network...** The Network Scanning window appears, as shown below.
3. Choose a **Scan Type**.
4. In the **Additional Probes** box, choose whether you want an HTTP probe added to the device (converting it to a probe group) when a response to an HTTP request is received.
5. Click **OK**. The network oval turns purple, and remains that way until scanning is complete, at which time the color changes to the default network color.

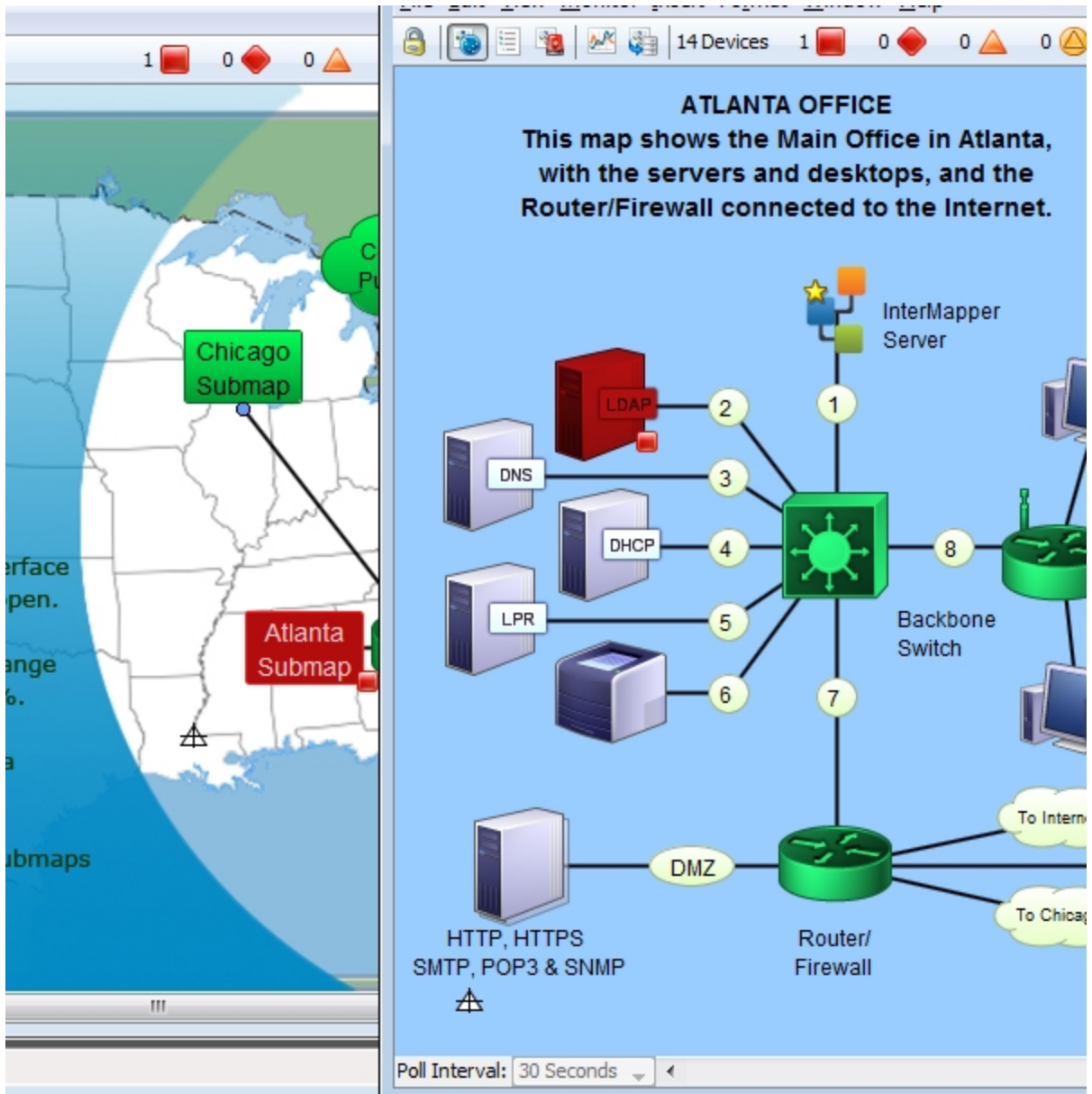


The Network Scanning window

Creating Sub-maps

Another way to hide detail is to create a top-level map that gives an overview of many individual maps. Each icon on the top-level map shows the status of another map (a "sub-map"). The color of the icon indicates the most serious condition (the "worst thing") on its sub-map. These sub-maps can be on the local computer, or could even be on another InterMapper server.

The example below shows the Atlanta map that opens when you double-click the Atlanta icon on the National map. Notice that on the National map, the Atlanta icon is "down". The Atlanta map shows that the LDAP server is the reason.



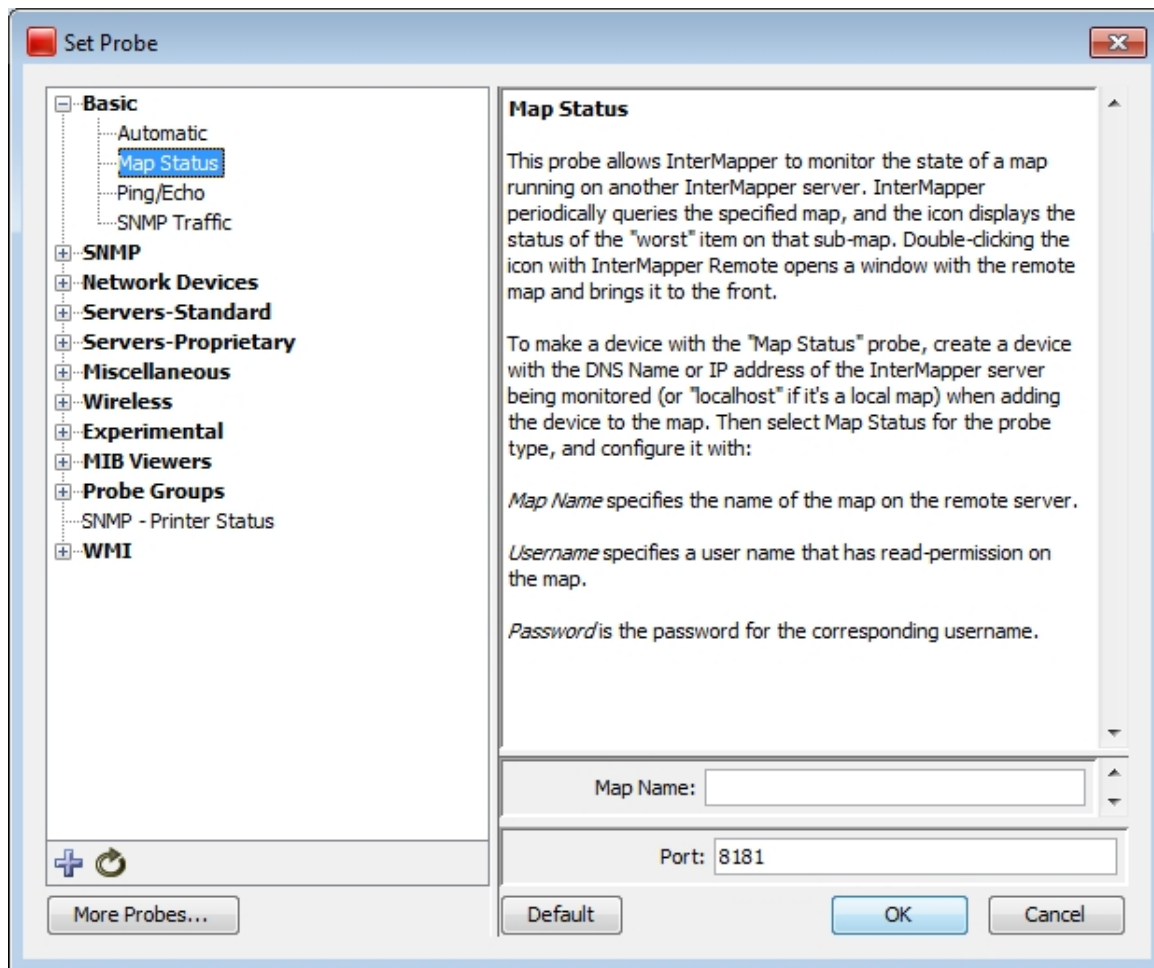
Creating a Sub-Map

Use the Map Status probe to create an icon that represents a sub-map. To do this, you add a device with the address of the InterMapper server on which the map is running, (127.0.0.1 if it's on the local computer) with a Probe Type of **Map Status**.

The color of the icon for a map item using a Map Status probe indicates the most serious condition (the "worst thing") on sub-map.

To add a sub-map item to a map:

1. The easiest way to add a submap is to drag the desired map from the Map List window to the map. In certain special cases, the Set Probe window appears, with the Map Status Probe selected.
2. Click **OK** to accept the default settings. A new device is added, using the current map and user account information.



The Map Status probe configuration window.

To add a sub-map manually:

1. From the Insert menu, choose **Device...**
2. Enter the [IP address \(Pg 726\)](#), [DNS name \(Pg 730\)](#), or [WINS name \(Pg 735\)](#) (preceded by "\\") of the InterMapper server that contains the sub-map. Sub-maps may be running on the local InterMapper server (use the address *127.0.0.1*), or enter the address of InterMapper running at a customer site, at a branch office, or at an international office.
3. Specify the **Port** to connect to (default is 8181).
4. Select **Map Status** from the Basic category.
5. Enter the **Map Name** to be monitored.

Note: if your map is nested in a sub-folder, you must enter the full path to the map. For example, *"/MySubFolder/MyMap.map"*. If you add the submap by dragging it into the map from the Map List window, the path is entered automatically.

6. Enter the **User Name** and **Password** of an account on that server. This account must have read-access to the map.
7. Click **OK**. The new icon appears on the map, and its color reflects the state of everything on the sub-map.

To view the sub-map (to "drill down" into it)

- Double-click the sub-map's icon. The map opens, and you can see and modify (if you have been granted permission) the settings on the sub-map.

Best Practices When Using Sub-maps

Try to follow these best practices when setting up a map status probe:

- Use a username with minimum amount of privilege (read-only). Never set up a map status probe using a username that has administrative privileges.
- Use only one username per server for map status probes. InterMapper has a limit of 2 user logins per connection. If map status probes monitoring maps on a server are configured using more than one username, you may need to explicitly logout from the map status probe login before you can access a map status probe that uses a different username.

For example, let's assume you have access to map status probes on server S, and that we have MapB and MapC on server S that you don't have access to. When you double click a map status probe for MapB, the InterMapper client will log you in as user B (you are logged in twice on server S). You will not be able to open MapC before you log off the connection to MapB. This restriction is only for one server, if you are using map status probes to monitor maps on multiple InterMapper servers, you can use a different username for each server.

Creating Probe Groups

Overview

Use a probe group to include multiple probes targeting the same IP address into a single icon on a map. A probe group shows the worst status among the probes in the group. A probe group counts as a single device against your license count.

Note: Only those devices that reference the same IP address can be added to a group.

About the Control Probe

Each probe group can contain a control probe. Setting a control probe affects the probe group as follows:

- When a control probe is defined, no notifications for the other probes in the group are sent if the control probe is down.
- The group's interfaces match those of the control probe.

When you create a group containing an SNMP probe, a "control probe" is automatically determined for the group. This is the first SNMP probe detected, and can be changed. If there are no SNMP probes in the group, no control probe is defined. See [Setting a probe group's control probe \(Pg 77\)](#) below.

How grouped devices are probed

Here are some important facts about how devices are probed after grouping.

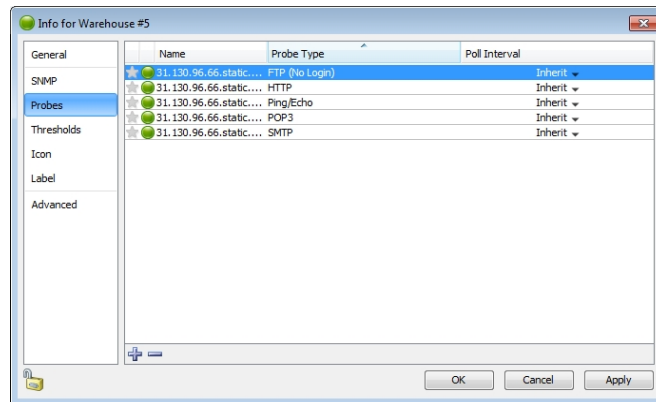
- **Each member probe is polled at its own rate, with its own settings.** The settings in place when the device is added to a probe group are used, including poll rate, attached notifiers, and probe parameters. You can edit the settings for any probe - see [Editing Settings for a Probe Within a Probe Group \(Pg 76\)](#).
- **The device icon's state reflects the most serious condition of its member probes.** When the state of one of the member probes becomes the most serious state, the device icon's state changes to reflect it.
- **By attaching a notifier to the device,** you can get notifications whenever any probe in the group has a problem.
- **By attaching a notifier to a member of the group,** you can get notifications when that member probe has a problem
- **If the control probe is down,** no notifications are sent for any other member of the group.
- **Interface information is shown** based on the selected control probe.

Use the **Group** command to create a probe group from a set of selected devices.

To create a probe group:

1. With the map editable, select the devices you want to group. All devices must use the same IP address.
2. From the Insert menu, choose **Group**. The selected devices are replaced by a single device icon.

When you double-click the resulting device icon, the grouped probes appear in a list in the group's Info window.



Warehouse #5
66.96.130.31
Ping/Echo

Warehouse #5
66.96.130.31
POP3

Warehouse #5
66.96.130.31
SMTP

Warehouse #5
66.96.130.31
FTP (No Login)

Before grouping

Warehouse #5

After grouping

Note: When you group a selection of probes, the resulting group uses the first line of the first device as its label. You can change the label before or after grouping.

Creating one or more empty Probe Groups

You can create an empty probe group, then add probes to the group as needed.

To create an empty probe group:

1. From the Insert menu, choose **Empty Probe Group...** The Add Probe Group (s) dialog appears.
2. For each probe group you want to add, enter a host name or IP address.
3. Click **Add**. A probe group icon appears for each host name or address you entered.

Adding devices to a probe group

You can add probes to a group in several ways:

- Add an existing device to a group.
- Add a new device to a group
- From the list view, drag and drop a device into a group.

To add an existing device to a probe group:

1. Select the group and the devices you want to add to it.
2. Choose **Group** from the Insert menu. If all selected devices use the same IP address or host name, the selected devices are added to the existing probe group.

To add a new device to a probe group:

1. From the probe group's Info window, click the **plus (+)** button. The Set Probe window appears.
2. Choose the probe you want to use, set its parameters, then click **OK**. The probe is added to the group.

You can remove one or more probes from a group.

To remove probes from a group:

1. Double-click a probe group. The probe group's Info window appears.
2. In the Info window, select the probes you want to remove from the group. Use Shift-click to add contiguous probes to your selection, or Control-click to add or remove discontinuous probes from your selection.
3. Click the **minus (-)** button. The selected probes are removed from the probe group, and appear as separate devices in the map.

From the List view, you can also drag a probe out of a probe group.

Editing Settings for a Probe Within a Probe Group

Each probe in a probe group can be polled at its own rate, can have its own settings, and can be edited while part of the group.

To edit a probe's setting within a group:

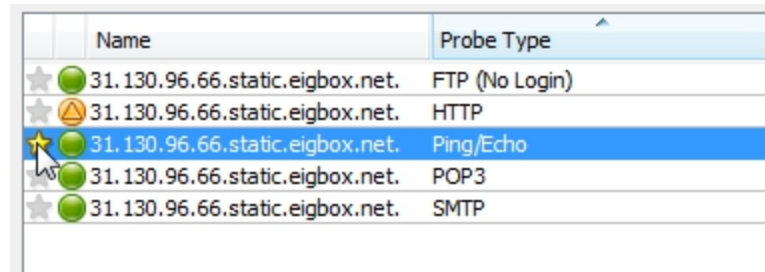
1. Double-click the probe group's device icon. The Info window opens, showing the list of probes in the group.
2. Double-click to open the Info window for the selected probe, or right-click-/Ctrl-click the probe, and choose an option from the context menu.

Setting a probe group's control probe

You can set the control probe for a probe group. If the control probe is down, no notifications are sent for any other member of the group, and the group's interfaces match those of the control probe.

To set the control probe for a group:

1. With the map editable, double-click the probe group icon. The Info window appears.
2. Click **Probes** in the left panel. The probes in the group appears.
3. In the left column of the probe list, click the star icon for the probe you want to use as the control probe. The color of the star changes to indicate that the probe is the control probe.



	Name	Probe Type
★	31.130.96.66.static.eigbox.net.	FTP (No Login)
★	31.130.96.66.static.eigbox.net.	HTTP
★	31.130.96.66.static.eigbox.net.	Ping/Echo
★	31.130.96.66.static.eigbox.net.	POP3
★	31.130.96.66.static.eigbox.net.	SMTP

Setting the control probe

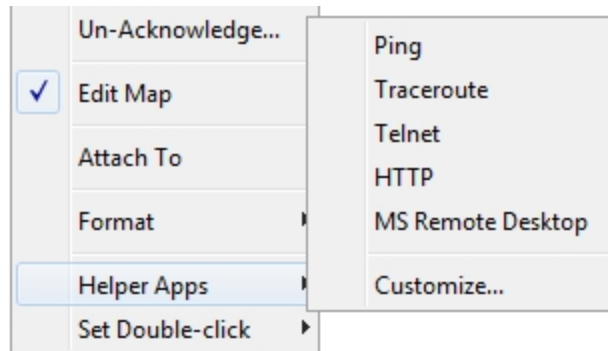
Using Helper Applications

You can use helper applications to get information for creating maps or to troubleshoot problems. These programs are available through a [Context menu](#) (Pg 435).

To invoke a helper program:

1. Control-click or right-click on a device.
2. Select one of the helper applications to launch it using the device as its target.

For example, the 'Ping' helper application invokes the system's ping utility: generally `/sbin/ping` on Unix, Linux or MacOS X, or `ping` on Windows. Including a URL as the helper application will invoke the system's tool configured to handle the URL.



The Helper apps context menu

Notes:

- You can specify the same helper application for several devices at the same time if more than one device is selected. The helper app is invoked for each selected device.
- The helper application that is invoked is platform-dependent: generally, InterMapper will open a terminal program and issue a command to run the helper.
- You can choose to invoke a Helper Application by double-clicking a device. See [Using Double-Click Actions](#) (Pg 83) for more information.

Editing Helper Applications

Use the Helper Applications Customize window to modify the built-in helper applications, and add new ones.

To view the Helper Applications Customize window:

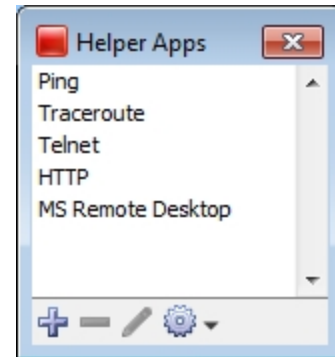
1. Right/control-click a device. A drop-down menu appears.
2. From the Helper Applications submenu, choose **Customize...**

or

- From the Monitor menu's Helper Apps submenu, choose **Customize...**

The **Helper Apps** window appears.

This window shows the list of built-in helper apps and any user-added helper applications. To add, edit, or remove a helper application, see *Adding or Editing Helper Apps* below. It also describes the *Launcher*, a platform-specific tool used to launch a helper app.



Adding or Editing Helper Apps

To add a new helper application:

- In the Helper Apps window, click the Plus-button (+). The Create Helper App window appears, showing default values for the new helper.

To edit an existing helper:

- In the Helper Apps window, click the helper you want to edit.
- Click the Pencil tool. The Edit window appears, showing the current values for the selected helper.

Create Helper App

Please enter the title InterMapper should use for this helper application:

Title (\${TITLE}):

The Command Line, Path, and Arguments will automatically have single backslashes (\) escaped.

InterMapper will run this helper application by issuing the following command. The variables (in \${...}) will be substituted with the specified values.

Command Line:

Enter the Path and Arguments that should replace the \${PATH} and \${ARGS} variables on the command line above. Note that \${TITLE}, \${LABEL}, \${DEVICENAME}, \${ADDRESS}, and \${PORT} may also be used on the command line.

Path (\${PATH}):

Arguments (\${ARGS}):

☐ \${ADDRESS} is a list of addresses

Input:

Enter values as follows:

- **Title** is the human-readable name that appears on the Helper Applications sub-menu.
- **Path** is the full file path name for the helper application
- **Arguments** that will be passed along to the helper application.

Finally, the **Command Line** is the actual string that will be invoked. You can configure this string using the \${TITLE}, \${PATH}, \${ARGS}, and \${LAUNCHER} macros that will be substituted when the command is invoked. In addition, you may use the \${ADDRESS}, \${PORT}, \${LABEL}, or \${DEVICENAME} macro.

Removing a Helper Application

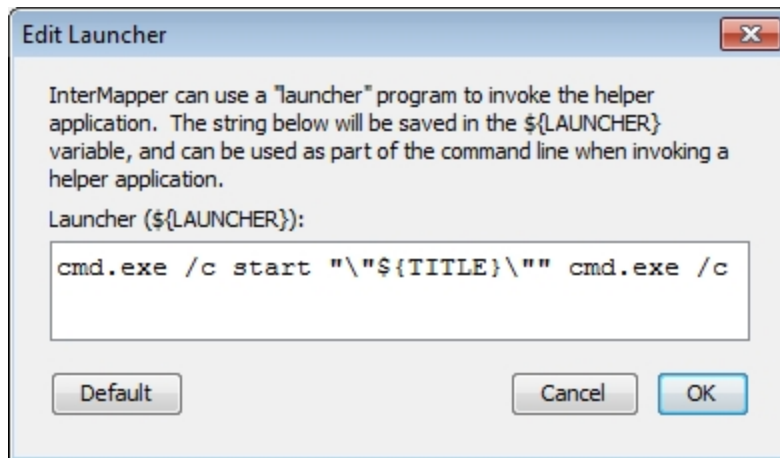
You can remove any helper application definition you have created. Built-in helper apps cannot be removed.

To remove a helper app definition:

1. In the Helper Apps window, click the helper you want to remove.
2. Click **Remove...**

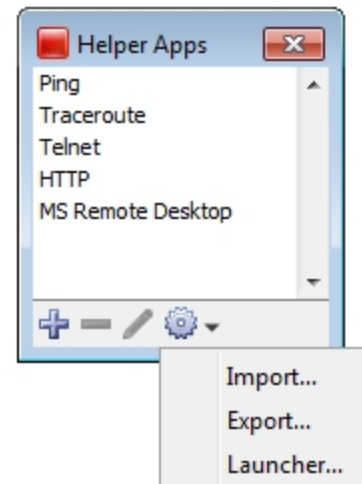
The Launcher

The *Launcher* is a platform-specific program that allows you to invoke another program from InterMapper.



To open the Launcher window:

1. From the Helper Apps window, click the Tools button. The Tools menu appears.
2. Choose Launcher from the Tools menu. The Launcher window appears.



Exporting and Importing Helper Application Definitions

You can export your current Helper Application settings and import them to another instance of InterMapper.

To export the current Helper Applications definitions:

1. From the Helper Apps window's Tools menu, choose **Export...** A standard file dialog appears.
2. Specify a file name and location, and click **Save**.

To import Helper Application definitions from a file:

1. From the Helper Apps window's Tools menu, choose **Import...** A standard file dialog appears.
2. Navigate to the Helper Apps definitions file you want to use, and double-click it or click it and click **Open**. The Helper Apps definitions are replaced with the definitions in the selected file.

How does the Launcher invoke an application?

The method of launching an application is platform-dependent.

- On Windows, InterMapper uses a command shell.
- On OSX, InterMapper opens a Terminal window.
- On Unix/Linux, InterMapper invokes the shell.

Using Default Values

For each platform, there is a default value for each built-in helper app. You can reset a helper app to its default values.

To reset a helper app to its default values:

- Click the **Default** button. The launcher string is reset to the default value for that platform.

Note: You don't have to use the launcher for any helper, but it's often the easiest way to invoke another program on your computer.

Using Double-Click Actions

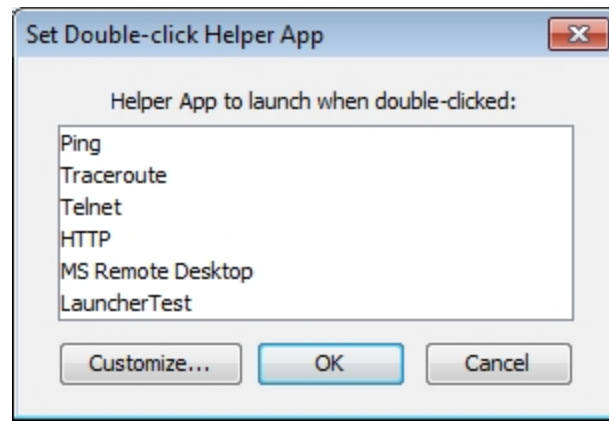
InterMapper defines *Double-click Actions* that it will perform when a device is double-clicked. Many probes have a pre-defined double-click action, but this can be overridden.



To change a double-click action, right-click on the device, and select the proper choice from the sub-menu:

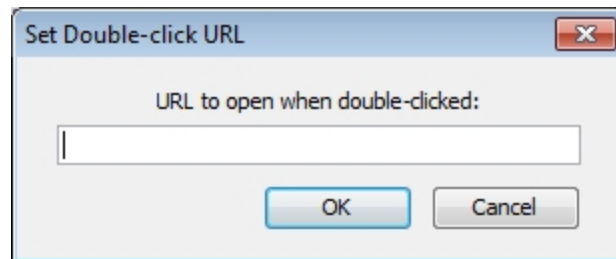
Helper App

Double-clicking will invoke a specified [helper application \(Pg 78\)](#). This helper application runs on the same machine as the InterMapper client. Select the helper application from the current list of helpers.



URL

You may supply a URL (http, ftp, telnet, etc.) and InterMapper will invoke it when the device is double-clicked. Enter a URL to be invoked when the device is double-clicked. You may use the following macros: `${address}`, `${port}`.



Enter a URL you want to use when the icon double-clicked. The default browser is launched with the specified URL.

Opening an InterMapper map

To open another InterMapper map, use this URL format:

```
intermapper://Host:Port/MapName
```

- **Host** is the address or DNS name of the InterMapper server hosting the map . Use \$SAMEHOST\$ to get to a map on the same InterMapper server.
- **Port** is the port for the specified InterMapper server
- **MapName** is the name of the map, URL-escaped (%20 for a space, %3D for a slash,etc)

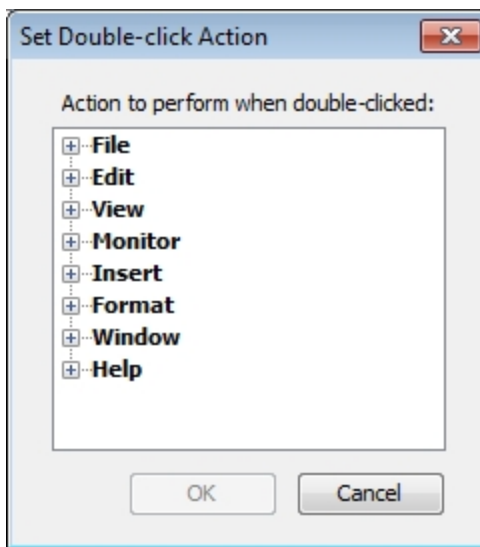
Example

The Example.com demonstration submaps have links back to the Example.com parent map that look like this:

```
intermapper://$SAMEHOST$:8181/Example.com%20National%20Map
```

Built In

InterMapper can invoke nearly any of the menu commands as a result of a double-click. Select the desired item from the hierarchy of menu items.



Saving Your Map

Each time you make the map editable, a backup of the map is created automatically. You can revert to the backup version by choosing **Revert...** from the Edit menu.

When you make a change to a map, the change is saved immediately, automatically, every minute or so.

Making a backup of your map

If for some reason you want to make changes to your map, but you want to be able to get back to your original version if necessary, you can make a backup of your map.

When you make a backup file, it stores references to your original chart data. If you decide to restore a previous version, your chart data remains available.

To make a backup:

1. From the File menu, choose **Backup...** The Backup Map window appears, showing a list of previous backups of the current map.
2. In the **Backup Name** box, enter the name you want to use for the backup file.
3. Click **OK**. A backup of the current map is created.

Note: Backups are stored in the InterMapper Settings/Maps (Backups) folder.

Restoring a previous version of your map

Use the **Restore...** command, available from the File menu, to restore a previous version of a map.

To restore a previous version:

1. From the File Menu, choose **Restore...** The Restore from Backup window appears, showing a list of previous backups of the map.
2. Click the backup you want to use to restore the map.
3. Click **Restore**. The map is restored to the backup version.

Backup Types

InterMapper creates the following backup types:

- **Manual** - the backup was created using the Backup... command.
- **Automatic** - the backup was created automatically by a change in a Layer 2-enabled map.
- **Scheduled** - the backup was created automatically, based on a schedule defined in the Map Backup panel of the Server Settings window.

The Map Settings Window

Use the Map Settings window to specify colors for the map, to specify a background image, and to specify default thresholds and notifiers. Any changes you make are saved with the map, and do not affect any other maps.

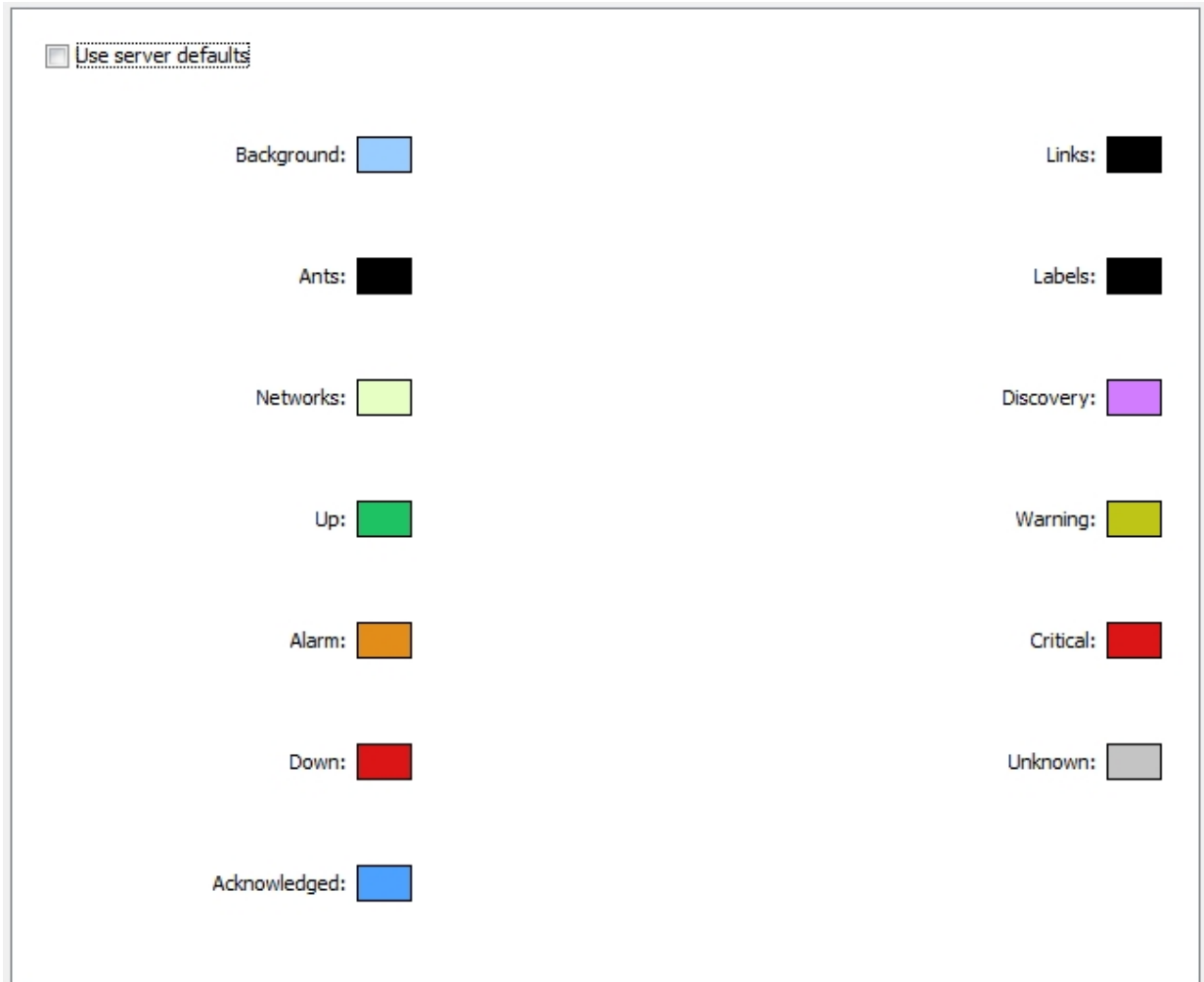
To view the Map Settings Window:

1. Make sure the map is in [Edit mode \(Pg 180\)](#).
2. From the Edit menu, choose **Map Settings...** The Map Settings Window appears. In the left pane is a menu. In the right pane are the settings for the selected section of the menu.

Colors
Background
Device Thresholds
Interface Thresholds
Traffic Indicators
Default Notifiers
Retention Policy
Layer 2 Features

*Left pane of the
Map Settings Window*

Setting a Map's Colors



☐ Use server defaults

Background:

Ants:

Networks:

Up:

Alarm:

Down:

Acknowledged:

Links:

Labels:

Discovery:

Warning:

Critical:

Unknown:

The Colors pane of the Map Settings Window

To view and edit the colors for the current map:

From the Appearance section of the Map Settings window, choose **Colors...** The current colors for the map appear.

InterMapper has a default color scheme that is controlled by the [default map colors \(Pg 265\)](#) window. This color scheme applies to all new maps, and to those maps for which the **Use server defaults** box is checked.

For an explanation of each color you can change, see [Colors you can change \(Pg 266\)](#), which explains the meaning of each default color.

To use a set of colors different from the global color scheme:

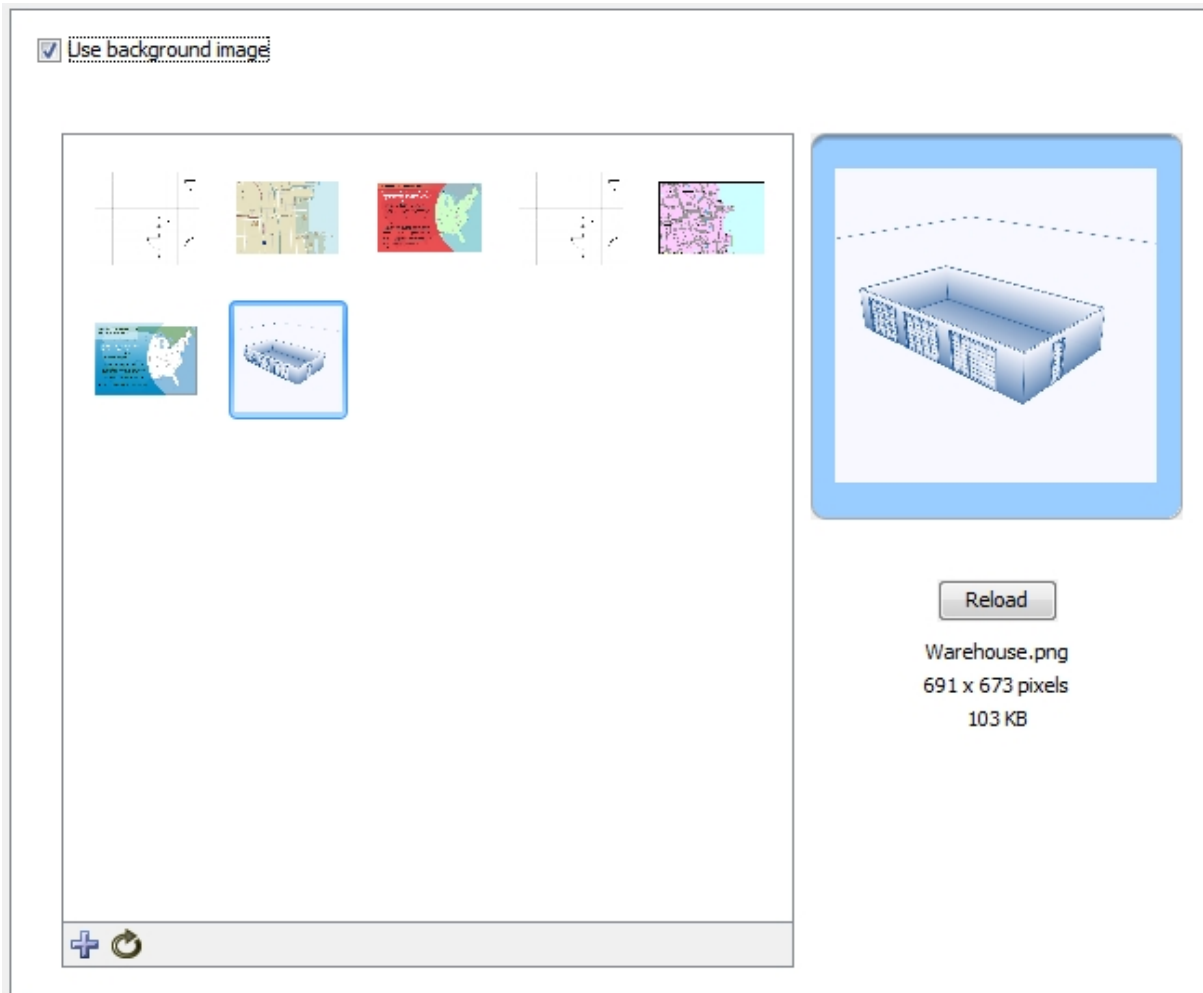
1. Clear the **Use server defaults** box.
2. Click the color box for the first color you want to change. The Color Picker window appears.

3. Click to choose a color, then click **OK**. The new color appears in the color box you clicked.
4. Repeat steps 2 and 3 for each color you want to change.
5. Click **OK**.

To restore the current map to the default color settings:

1. Click to select the **Use server defaults** check box.
2. Click **OK**. The map uses the default colors. The colors you defined are still saved with the map.

Adding a Background Image



Background Image pane of the Map Settings Window

You can define a background image for any map. The background image appears behind the map contents - the devices, icons, and links on the map.

You might use a background image containing a floor plan of an office, and move the items on the map to show the locations of each device in the office. You might use an image containing street map of a city or topographic map of a county or state.

For more information, see [Background Images \(Pg 104\)](#).

Setting a Map's Default Device Thresholds

Set thresholds to alert you to network problems.

☒ Use Server defaults

Down Thresholds

Number of lost packets (1 - 10):

Other Thresholds

	Warning	Alarm	Critical	
Interface errors:	<input type="text" value="2"/>	<input type="text" value="10"/>	<input type="text" value="20"/>	per minute
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/>	of last 100
Response Time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/>	msec

The Device pane of the Map Settings Window

InterMapper can provide warnings or alerts when interface errors, packet loss, or round-trip times get too high. You can set default thresholds for all of these metrics from the Map Settings window.

- **Use Server Defaults** - check this box to override the map settings and use the server default settings.
- **Down Thresholds** - Enter the number of lost packets required to generate a Down state.
- **Other Thresholds** - For each metric, in each column enter a value required to generate the a Warning, Alarm, or Critical state.

Setting a Map's Default Interface Thresholds

Use the Interface Thresholds pane of the Map Settings window to set Error, Link Utilization and Discard thresholds for a specific map. These settings are applied to interfaces on each new device added to the map.

To create map-specific interface thresholds:

1. Clear the **Use server defaults** check box for the threshold type you want to make specific to this map.
2. Set the thresholds for the selected threshold type, as shown below.
3. Click OK.

Note: You can also set thresholds for an individual link. For more information, see XXX.

Set interface thresholds to alert you to network problems.

Error Thresholds

☒ Use server defaults

	Warning	Alarm	Critical	
Rx Errors (Received):	<input type="text" value="10"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	per minute
Tx Errors (Transmitted):	<input type="text" value="10"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	per minute
Total Errors (Rx + Tx):	<input type="text" value="10"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	per minute

Utilization Thresholds

☒ Use server defaults

	Warning	Alarm	Critical	
Rx Utilization (Received):	<input type="text" value="75"/>	<input type="text" value="85"/>	<input type="text" value="95"/>	%
Tx Utilization (Transmitted):	<input type="text" value="75"/>	<input type="text" value="85"/>	<input type="text" value="95"/>	%
Total Utilization (Rx + Tx):	<input type="text" value="75"/>	<input type="text" value="85"/>	<input type="text" value="95"/>	%

Discard Thresholds

☒ Use server defaults

	Warning	Alarm	Critical	
Rx Discards (Received):	<input type="text" value="15"/>	<input type="text" value="25"/>	<input type="text" value="35"/>	per minute
Tx Discards (Transmitted):	<input type="text" value="15"/>	<input type="text" value="25"/>	<input type="text" value="35"/>	per minute
Total Discards (Rx + Tx):	<input type="text" value="15"/>	<input type="text" value="25"/>	<input type="text" value="35"/>	per minute

The Interface Thresholds pane of the Map Settings Window

Controlling a Map's Traffic Indicators

Use traffic indicators to help you view network activity on a map. You can set the traffic levels at which "moving ants" appear to show you the level and direction of activity on a particular link.

Set traffic thresholds to highlight network activity. Moving ants indicate the direction and magnitude of network traffic.

When the rate goes above these values, alter the display:

Frames Per Second:	<input type="text" value="10"/>	- . . . Some traffic
Frames Per Second:	<input type="text" value="100"/> High traffic
Average bytes per frame:	<input type="text" value="200"/>	---- Large frames
Errors per minute:	<input type="text" value="10"/>	☉ Trouble

The Traffic Indicators pane of the Map Settings Window

You can set the following values to control the appearance of traffic indicators:

- **Traffic units** - choose bytes or frames per second from a dropdown menu. This unit is used for traffic thresholds.
- **Some traffic** - enter the number (of bytes or frames per second) that represents some traffic.
- **High traffic** - enter the number (of bytes or frames per second) that represents high traffic.
- **Large Frames** - enter the number of bytes per frame that represents a large frame.
- **Errors per minute** - enter the number of errors per minute that represents a clear sign of trouble.

To set the default values for traffic indicators:

1. In an editable map, choose **Map Settings** from the Edit menu. The Map Settings window appears.
2. In the left pane, click **Traffic Indicators**. The current traffic indicator settings for the map appear in the right pane.
3. Enter the settings you want to change, and click **OK**. The map uses the new settings.

Note: Traffic indicators are part of InterMapper's "Animation" feature set. By default, animations are not turned on because they may require additional CPU resources. You can turn them on from the Animation Settings pane of the [Preferences window](#) (Pg 53).

Specifying a Map's Default Notifiers

Notifier Name	Down	Up	Critical	Alarm	Warn	OK	Trap	Delay	
Day Sounds	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	▲
Alternate Sounds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Command Line No...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Email Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Jack - Page	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Jack - SMS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
My AutoMate Task	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
PowerShell-Local-dir	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
SplunkLog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Uli - Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Uli - SMS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Write To Screen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	

The Default Notifiers pane of the Map Settings Window

Use the Map Settings window to specify the notifiers you want to attach to new devices in this map by default.

To specify the default notifiers for the current map:

- For each map state, select the check box for each notifier you want to attach to that state. For more information, see [Working With Notifiers \(Pg 131\)](#).

To edit the available notifiers:

- Click **Edit Notifiers...** The Notifier List pane of the Server Settings window appears, showing the available notifiers. For more information, see [Working With Notifiers \(Pg 131\)](#).

Resetting the Default Notifier

If you have changed the default notifier, or have edited its settings, you can reset all of the devices on the map to have the current default notifier or updated settings.

To reset the default notifier or its settings for all devices on the map:

- Click **Reset All**. All devices on the map now use the current version of the default notifier.

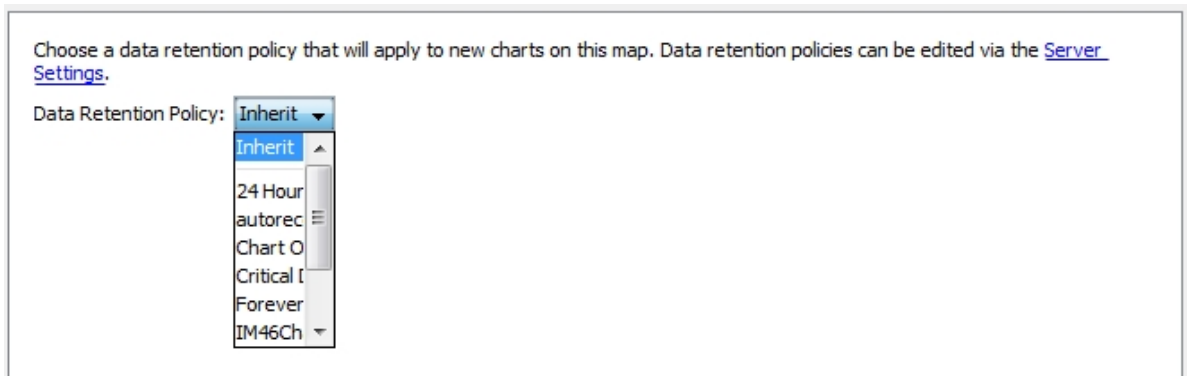
Specifying a Map's Default Data Retention Policy

If you are using InterMapper Database to collect device and network data, you can specify a default retention policy for a map. This setting overrides any default policy set in the Server Settings window.

Use the Map Settings window to specify the Retention Policy you want to use with new devices in this map. Data Retention Policies are defined from the [Retention Policy pane \(Pg 274\)](#) of the Server Settings window.

Settings your map's Retention Policies

Use the Retention Policy panel to choose the retention policy to be applied to new devices added to the map.



- **Data Retention Policy** - Choose a retention policy from the dropdown menu.

Setting your map's Layer 2 features

Use the Layer 2 Settings panel to turn on Layer 2 features for a map and to choose how Layer 2 connections should appear.

Notes:

- To use the Layer 2 features, you must enable Layer 2 collection in the [Layer 2 Features](#) pane of the Server Settings window.
- One option allows InterMapper to make changes to the map based on Layer 2 data. This can cause significant changes to your map. Help/Systems recommends that you back up the map before activating Layer 2 features.

Layer 2 features can be enabled for any map. You can control the discovery process via the [Server Settings](#).

☒ **Enable Layer 2 features for this map**

The Layer 2 mapping feature can visually arrange the connections on the map to reflect the most recent topology. This feature is experimental and can cause significant changes to your map. Backup this map before enabling this feature.

☒ Automatically change this map to show Layer 2 connections

You can customize the appearance of your map when the Layer 2 connections are refreshed to show more or fewer details.

☒ Show interfaces when a connection is made

☒ Hide interfaces that have nothing connected

☒ Hide propVirtual interfaces

Change Now

Use data from:
12/13/11 10:32 AM

- **Enable Layer 2 features for this map** - select this check box to turn on Layer 2 mapping for this map.
- **Change Now** - click this button to initiate the visual arrangement of connections on the map to reflect the most recent topology using Layer 2 data.
- **Automatically change this map to show Layer 2 connections** - select this box to allow InterMapper to edit the map automatically to show Layer 2 connections.
- **Show interfaces when a connection is made** - select this box to show Layer 2 interfaces when a connection is made.
- **Hide interfaces that have nothing connected** - select this box to limit the interfaces shown to those that have something connected to them.
- **Hide propVirtual interfaces** - select this box to hide interfaces whose ifType is propVirtual.

Quick Reference - Editing Your Map

This is a quick overview of editing the map. Also see [Arranging the Map \(Pg 99\)](#).

Note:

- Right-click (Windows/Unix) = Command-click (Mac)
- Alt-click (Windows/Unix) = Option-click (Mac)

To make changes to the map:

- Press **Tab**, or
- Right-click in the map and choose **Edit Map**. or
- Click on the lock in the upper left-hand corner to unlock the map for editing.
- With a map editable, drag items from another map's List View window to copy them to the new map.

To move an object on a map:

- Select and drag it.

To change the shape or label characteristics of an object:

- Select the node and choose the appropriate command from the Format menu.

To resize a wire-shaped network:

- Click and drag the end points.

To select a node and its adjacent nodes:

- Alt-click on an object. Continuing to Alt-click continues to select adjacent items.

To select the devices at each end of a link:

- Alt-click on the link.

To re-center the map:

- Control-click the background of the map. The point you click is centered in the map window.

To scroll the contents of the map:

- Control-drag the background of the map. The window scrolls the map contents within the map window.
- Press Alt+[arrow key] (or Option+[arrow key], Mac) scrolls the map in the direction of the arrow.

To zoom in or out:

- Ctr+Alt+drag (Ctrl+Option+drag on Mac) to select an area of the map to zoom into.
- Ctrl+scrollwheel (Cmd+scrollwheel on Mac) to zoom in or out.

Summary of selection tricks:

- **To select multiple items** - Shift-click.
- **To select adjacent items** - Alt-click. Alt-click again to select the items adjacent to those items.
- **To select all routers, networks or various other groups of items** - From the Edit menu, choose the appropriate command from the **Select Other** sub-menu.

Configuring PowerShell For Use With InterMapper

Before you can use PowerShell probes or notifiers, you need to configure the InterMapper machine and any target machines to allow connections. There are many options, and an exhaustive tutorial is beyond the scope of this topic.

Chris Hoffman has written an [excellent overview to using PowerShell](#) on remote computers.

Note: This topic assumes you know how to launch PowerShell, and that the InterMapper machine and the machines you want to connect to are running Microsoft Windows.

Enabling PowerShell Remoting

To enable PowerShell remoting, open a PowerShell window, and run the following command (also known as a "*cmdlet*") on all the machines you want to connect to:

```
Enable-PSRemoting -Force
```

The command starts the WinRM service, configures it to start automatically, and creates a firewall rule that permits incoming connections. The `-Force` attribute accepts the default settings.

Notes:

- You must be logged in as an administrator to execute these commands.
- If both the local and remote computers are in a domain, you need to enable PowerShell Remoting only on remote machines.
- If the local and remote computers are not in a domain, enabling remoting on the local machine is recommended; among other things, it allows you to access and modify TrustedHosts, which is required in order to connect to a remote computer.

Configuring TrustedHosts

Note: The configuration of TrustedHosts can result in security vulnerabilities. If you are not well-versed in security issues, you may want to consult an expert.

TrustedHosts is a list of trusted resources for your computer. The TrustedHosts list consists of a comma-separated list of computer names, IP addresses, and fully-qualified domain names. For a given computer, only administrators can change the TrustedHosts list.

Before you can connect to a remote computer, your TrustedHosts list must contain the IP address of that computer.

If your computers are not on a domain, you need to configure the TrustedHosts setting on the InterMapper server for all the computers you want to connect to.

Execute these commands, providing an IP address, or use wildcards to specify an IP range (see below). Separate entries with commas.

Setting the Value of TrustedHosts

The following is a sample command that sets values in TrustedHosts.

```
Set-Item wsman:\localhost\client\trustedhosts [IP  
address],[IP address], ...  
Restart-Service WinRM
```

Using Wildcards When Configuring TrustedHosts

When configuring TrustedHosts, PowerShell accepts only a single asterisk (*) for a wild card.

These are not allowed:

```
...\trustedhosts *.*.*.*, 192.168.*.*
```

These are allowed:

```
...\trustedhosts *, 192.*, 192.168.*
```

Testing the Connection

To test the configuration, execute this command:

```
Test-WsMan [COMPUTER]
```

A successful test shows a several lines of information. The last line is most interesting, as it shows the version of Windows Management (WsMan) running on the target machine.

Executing a Command

You are now ready to try a command. To determine the versions of PowerShell and several other related systems, try this command:

```
Invoke-Command -ComputerName [Target Computer] -ScriptB-  
lock { $PSVersionTable } -credential [UserName]
```

This returns a list of versions of PowerShell, WsMan, and several other systems.

If the command above works successfully, you are ready to try running PowerShell probes and notifiers.

Chapter 5

Arranging Your Map

Once you've added all the devices to the map, you can arrange them to suit your ideas about the network.

Default Appearance of Devices and Networks

By default, *InterMapper* displays *devices* as rectangles in its map. These devices are connected by *links* - straight lines of differing thickness to indicate the kind of link - to *networks*, which are represented as ovals.



Possible Arrangement Approaches

You can use *InterMapper's* layout tools to arrange your maps in ways that are most useful to you.

One strategy:

1. Find one or more *clusters* of related items and move them close together.
2. Once you have created clusters, you can move them to different parts of the map.
For example, an Ethernet or FDDI backbone with its attached routers might make a good cluster. Similarly, a central router or switch with its attached networks might serve as a cluster.
3. If networks or ports are not important for a map, hide them from the [Inter-faces Window \(Pg 195\)](#).
4. See [Using the Arrange Commands \(Pg 114\)](#) for more information about using the commands from the Format menu.
5. For other information related to arranging your maps, see [Arranging Tips \(Pg 119\)](#).

Enhancing Your Map's Appearance

InterMapper has many tools for enhancing your map's appearance. These include:

- **Setting Custom Icons:** InterMapper comes with a set of icons derived from Cisco's Icon Library. Use these industry standard icons, or import your own PNG, GIF, or JPEG images. For more information, see [Custom Icons \(Pg 101\)](#).
- **Setting a Map Background:** You can use a graphic as a "background" to the map. The devices being monitored will appear above this background image. For more information on using background images, see [Background Images \(Pg 104\)](#).
- **Adding text objects:** You can add text objects your map to label groups of objects, or simply to provide information to the viewer. For more information, see [Text... \(Pg 409\)](#) in the Insert menu reference topic.
- **Importing Device Descriptions:** InterMapper allows you to import descriptions of the devices on a map directly from a tab-delimited file. This

simplifies the creation of a new map, and makes it easy to add new devices as your network grows. For more information, see [Importing Data Into Maps \(Pg 637\)](#).

- **Setting the Geographic Coordinates of the Map:** InterMapper allows you to indicate the latitude and longitude for *benchmarks* - known positions on the map. If, for example, you are using an actual geographic map as a background image, you can use geographic coordinates to place a device in the correct location on the map. For more information, see [Using Geographic Coordinates \(Pg 640\)](#).

Setting a Map Background

Create a new map, and then save it. You can scan your own map, or obtain an image that covers the right area from one of the sites listed in [Using Geographic Coordinates \(Pg 640\)](#). InterMapper can use PNG, GIF, or JPEG image files as backgrounds for maps. You can obtain suitable images by scanning or creating your own maps, or use one of the many map sites listed in [Sources of Maps \(Pg 643\)](#).

To add a background image to a map, simply drag the image file into the map window. It will be added to the map and become visible.

Setting the Geographic Coordinates of a Map

If you use a geographic map for a background, you can associate specific points on the map with geographic coordinates (latitude and longitude) by adding **benchmarks**. For more information, see [Using Geographic Coordinates \(Pg 640\)](#). Once you have specified the coordinates, you can specify geographic coordinates for devices as you import them to the map, and they are automatically placed at the correct location.

Icons and Images on Maps

InterMapper can display devices on a map in one of several *shapes*. The default shape is a rectangle, with the device's *Label* inside. InterMapper can also display an oval, a wire (a straight line), a cloud, a text object which can be used as a legend on a map, or as an icon.

A large number of built-in icons are provided with InterMapper. It is also very straightforward to import your own icons.

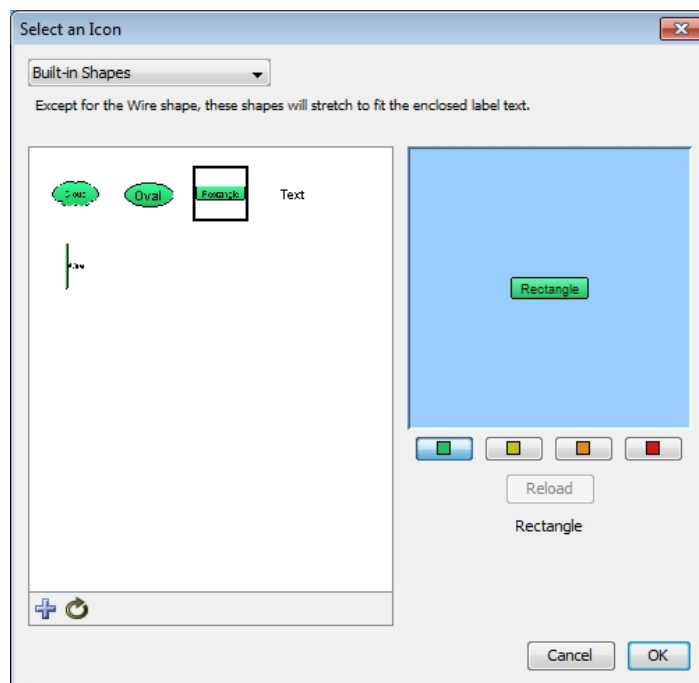
Setting an Object's Icon

To set an icon, select one or more items on the map, then choose **Format > Icon...** This opens the Select an Icon window. This window has several components:

- A drop-down menu lists collections of icons called *Icon Sets*. There are several built-in icon sets, including *Traditional* and *Default icons* sets, and various Cisco-themed icon sets..
- A scrolling list on the left shows icons from the selected icon set. These icons appear at a uniform size in the list. Click one of these icons to use it for the selected device(s) on the map.

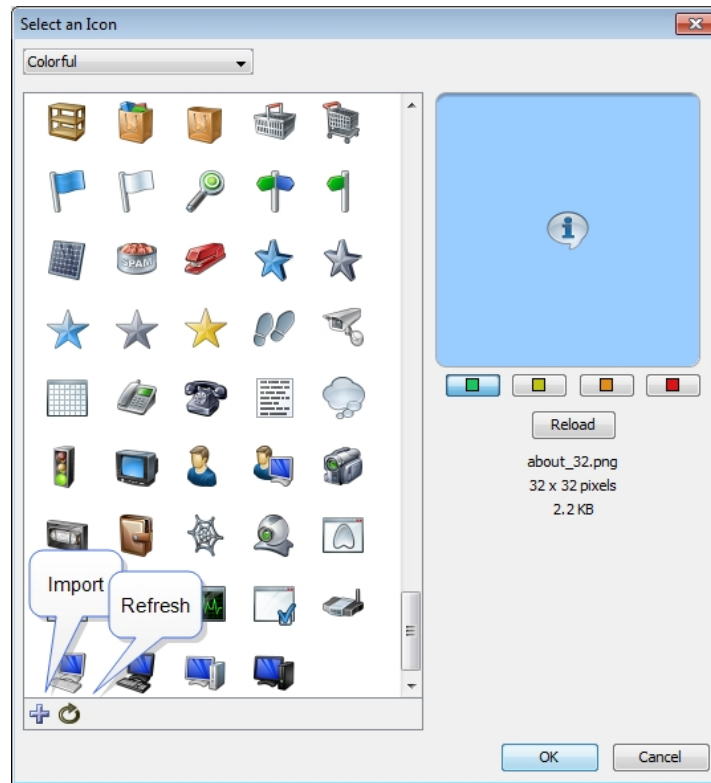
Note: Grayscale custom icons appear shaded with the color of a device when it is in the UP state (the default is green.)

- A preview pane of the icon, showing the selected icon in the size it will appear on the map.
- Color preview buttons. The green, yellow, orange, and red buttons correspond to the different device states. Click a colored button to view the icon's appearance when it is in the indicated state.



Select an Icon window - Built-in Shapes

- Below the **Reload** button is Information about the icon: its filename, dimensions, and file size.
- Click the **Refresh** button (as shown) to force InterMapper to reload the image, perhaps after modification in an image editing program.
- Click the **Import** button (as shown) to import an icon or a folder of icons into InterMapper. These icons are sent to the *InterMapper Settings > Custom Icons* folder on the InterMapper server.
- Click the **Refresh** button to refresh the list of icons.
- Drag an image file to the window to import it into the current icon-set.
- Drag a folder of image files to the window to create a new icon-set, importing the image files in the folder to the new icon-set.
- If the Icon Size slider appears, use it to select the icon's size.



Select an Icon window - Default Icons

Icon Coloring According to the Device Status

InterMapper colors the icon depending on its status. When in the **Up** status, the icon retains its normal color. (Grayscale icons are tinted green.)

If the icon goes to a warning, alarm, or down status (yellow, orange, or red, respectively) Inter-

Mapper shows a grayscale version, tinted to match the device's state.



Clicking the color preview buttons changes the color to show how the icon appears on the map in a given status.

Creating Custom Icon Files

Icons files can be saved in one of several common graphic formats:

- Portable Network Graphics (PNG) - recommended - works with all operating systems and platforms.
- Joint Photographic Experts Group (JPEG) - works with all operating systems and platforms.
- Graphic Interchange Format (GIF) - works with all operating systems and platforms.

Other graphics file formats may work for you, but aren't guaranteed to appear properly on all platforms.

The recommended file format is a PNG file, saved at 72 pixels per inch, with 256 colors. You should use transparency for the area surrounding the icon, so the background color shows through properly.

If the icon's filename has a suffix of "_###" where "###" is a number representing the size in pixels, the icons are grouped automatically, and the icon size slider appears.

Placing arbitrary icons and images in maps

Any icon or image can be placed in a map. Before you can place an image in a map, you must import it as an icon.

To place an image or icon in a map:

1. If the image has not yet been imported as an icon, import it now.
2. From the Insert menu, choose **Icon...** The Select an Icon window appears.
3. Choose the icon or image you want to insert and click **OK**. The icon or image appears in the map.
4. Move the icon or image to a desired location on the map.

Note: When you place an icon on a map, a network oval is added to the map, and the icon assigned to it. You can edit the network as you would any other network, changing the icon or label, or adding a comment or subnet list.

Adding Background Images To Your Map

You can place a background image on a map so that it appears behind the devices, icons, and links on the map. All image [file formats supported for custom icons](#) (Pg 103) can be used.

- You might use a background image containing a floor plan of an office, and move the items on the map to show the locations of each device in the office.
- You might use an image containing a street map of a city or topographic map of a county or state.

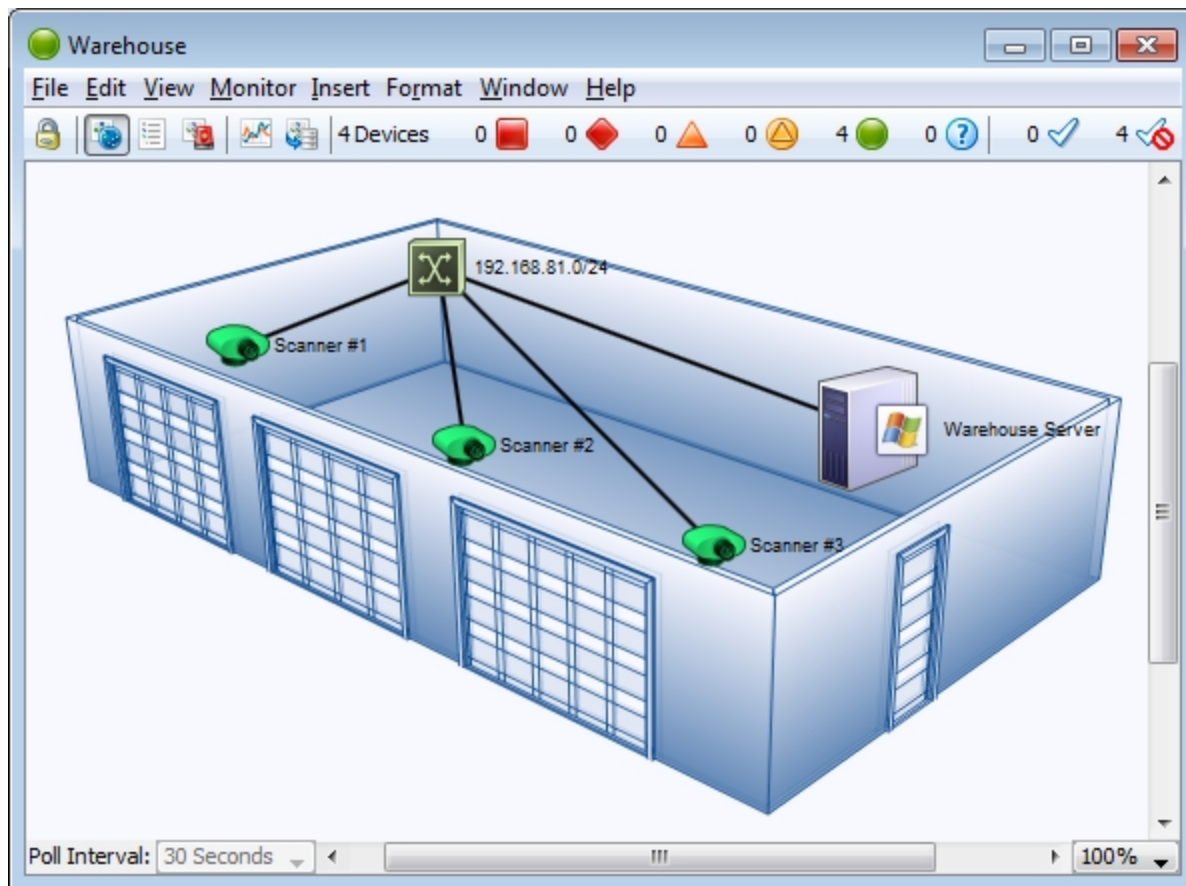
The figure below shows a map after placing an image in the background.

To place a background image in your map:

- Drag an image file from a desktop folder to the map window.

or

1. From the Appearance section of the [Map Settings](#) (Pg 86) window, available from the Edit menu, choose **Background**. The Background pane appears, showing the current background image, if there is one.
2. Click to select **Use background image**.



Map with background image.

Tips for Using Background Images

Image size

The background image retains its height and width, and is not scaled (stretched or shrunk) when you resize the window. If the background image is smaller than the current window size, the image will be centered in the map, and the map's background color will show around the edges. If a large image is placed, its dimensions determine the full size of the window.

Image contrast and brightness

Contrasty images may make it difficult to see the devices and links against the background. To make the image more suitable as a background image, you may use a graphics program to increase the brightness and/or decrease its contrast before placing it in a map. We regularly use GraphicConverter, an inexpensive shareware graphics program from <http://www.lemkesoft.com>, to do this task. It has a Brightness/Contrast adjustment facility to simplify this task.

Be aware of image file size

Large images consume large amounts of memory and slow InterMapper's redrawing of the window, especially when viewed over a remote connection. You should balance the image quality against the size of the map. Larger maps may look better, but they may consume large amounts of memory.

Note: Use of a compressed image file format such as JPG does not necessarily translate into less memory use.

Use contrast and compression to reduce image file size

Decreasing contrast can decrease the size of an image, so that decreasing the contrast as described above may help decrease the size of the background image as well. Use compressed formats, such as JPG and GIF, to further decrease the overall size of the image file.

Editing Labels

Use the **Label...** command, available from the Format menu (Cmd/Ctrl-L) to edit the labels for the selected map objects. You can edit the label for a single device or network from the Device or Network Info window.

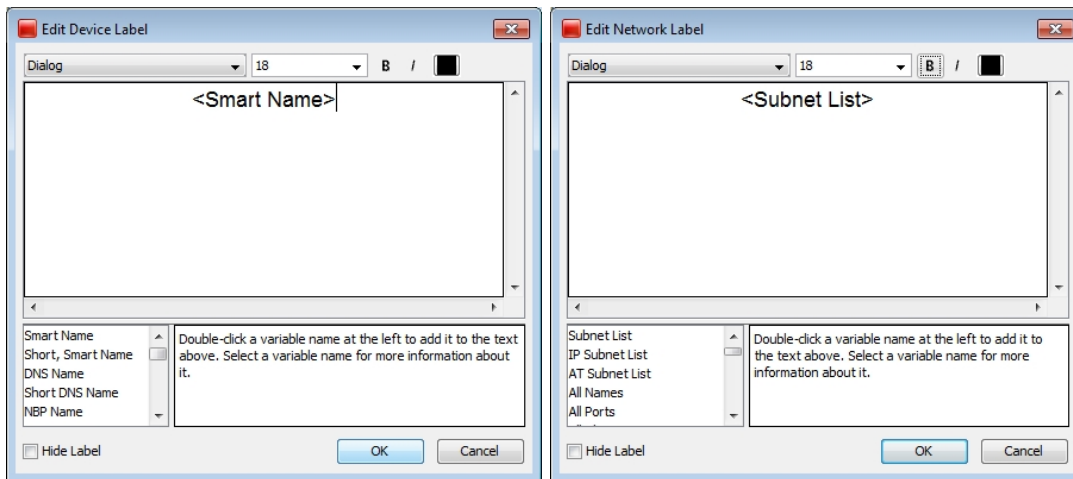
Every item on a map has its own descriptive label. InterMapper creates a default label showing the device's full DNS name or IP address(es).

To edit a map object's label:

1. Make sure the map is in [Edit mode](#) (Pg 180).
2. Select one or more map objects.
3. From the Format menu, choose **Label...** (Cmd/Ctrl-L).
Depending on the object you select, the Edit Device Label dialog or the Edit Network Label dialog appears, as shown below.
4. Enter label data as follows:
 - Enter text in the Label dialog's text box.
 - Double-click on any variable names in the list at the lower-left to insert that value into the item's label.
 - Select **Hide Label** if desired. (See below.)

For example, the device in the Edit Device Label window uses the short, smart name (the leftmost part of the full domain name). The network shown in the Edit Network Label window has a static (unchanging) label of "Our ISP", and a list of all the subnets in the network shown on the next line.

Note: You can also use InterMapper variables and Javascript to insert information dynamically into a device label. For more information, see [Dynamic Label & Alert Text](#) (Pg 108).



The Edit Device Label window

The Edit Network Label window

Hiding a Device or Network Label

In some cases you may not want a label to show at all.

You can hide the label for any device or network unless the icon is set to:

- Rectangle
- Oval
- Cloud
- Text

To hide the label for a device or network:

1. From the Format menu, choose **Icon...** The Select an Icon window appears.
2. Choose an icon other than one mentioned above and click **OK**. The icon appears for the selected device or network.
3. From the Monitor menu, choose **Label...** The Edit Device Label or Edit Network Label window appears.
4. Select the **Hide Label** check box and click **OK**. The label for the selected device or network disappears.

Dynamic Label and Alert Text

When you edit a device label, notifier title, or notifier message, you can use a number of techniques to control the resulting text dynamically.

Showing Parameter or Variable values in a Device Label

When editing a device label, you can show probe parameters, probe variables, and device export attributes in the label.

- **Probe parameters** - any field in the selected probe's Set Probe pane, specified in the [<parameters> section](#) of the probe.
- **Probe variables** - variables defined in the probe. In SNMP probes, specified in the [<snmp-device-variables> section](#) of the probe.
- **Device attributes** - any [attribute of a device \(Pg 656\)](#) exported using [the Data File... command \(Pg 635\)](#) (available from the File menu's Export sub-menu.)

The syntax is:

```
{param:<name of parameter, variable, or attribute>}
```

For example, to show the connect time in a device label corresponding to a TCP probe, your label might look like this:

```
<Smart Name>  
Time to establish connection: ${param:_connect} msec.
```

Notice, there is no space after the param: and the name of the variable. (The underscore is part of the variable name. Most names do not have the underscore.) Any variable that can be shown in the `<snmp-device-display>`, `<script-output>`, or `<command-display>` section of the probe can be used in a label using this syntax. You can show a parameter of the Basic OID probe just as well:

```
Getting data from: ${param:Object ID}
```

You can show device export fields like this:

```
Belongs to map: ${param:MapName}
```

Using JavaScript in a Device Label or Notifier

You can also use JavaScript in a device label or notifier. Use this to collect information, process it programatically, and include the results in the label or notifier. The syntax in a label looks like this:

```
<? write( "Hello World" + "\n"); ?>
```

The markers `<?` and `?>` indicate the beginning and end of the JavaScript.

Variables and Scope in JavaScript

Important: JavaScript in labels and notifiers runs in the global scope within InterMapper. If you declare a variable within the global scope, rather than within a function, the variable is accessible for reading and writing by JavaScript running in any other device label within InterMapper. This may produce unexpected results if you attempt to run the same script in multiple devices.

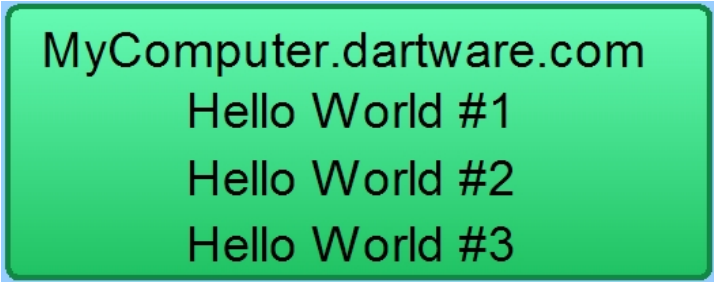
JavaScript functions are supported, and you can store values within devices and notifiers; these are remembered between polls. These techniques are recommended when you need to protect a variable from being overwritten. Setting variables in devices is described in [Remembering Values from One Poll to the Next \(Pg 111\)](#).

Example: Simple Scripted Label

Here is a little more complex, although silly, JavaScript label:

```
<Smart Name>
<?
  for (var i=1; i<=3; i++) {
    writeln( "Hello World #" + i);
  }
?>
```

The displayed label for the above would be something like this:



MyComputer.dartware.com
Hello World #1
Hello World #2
Hello World #3

The write and writeln functions

Two functions are used to write output to the label:

- The function `write` sends its output to the label without a line break.
- The function `writeln` sends its output to the label, and appends line break at the end, so you do not need to explicitly append the `"\n"` in your JavaScript code.

Accessing Probe Parameters

Use JavaScript to access probe parameters using the following syntax:

```
<? writeln( "Getting data from: " + self.get( "Object ID")); ?>
```

The `self` object refers to the device whose label you are setting. The `self` object is always available when using JavaScript to generate a label. Use the same syntax to get access to a probe variable as well:

```
<?
  var connTime = self.get( " connect");
  writeln( "Time to establish connection: " + connTime);
?>
```

JavaScript Error Handling

If you misspell the name of your variable, (by using `"_conect"` in the previous example) the label looks like this:

Time to establish connection: BAD ARG, see debug log

If you look in the debug log, you see the following message:

```
12:15:46 JS> [Device: map 'Exporting Fields', device 'nitro.dart-ware.com.', probe 'SNMP Traffic']:BAD ARG: There is no variable called '_conect'. It should be the name of a probe variable without '$' or curly braces.
```

The error message tells you the map, device, and probe in which the error occurred, and details about what caused the problem.

A JavaScript syntax error results in a label like this:

JS EXCEPTION, see debug log

The debug log contains the exception message, but give details about the syntax problem.

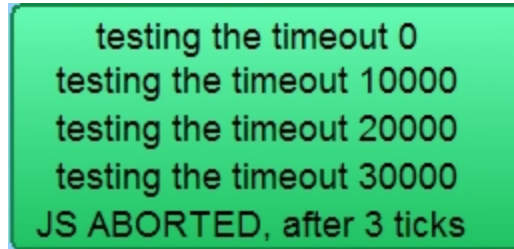
Execution Time Limit

The execution time of a script is limited to between 50 and 100 msec. This is a prevents the script from monopolizing the CPU. This is more than adequate time to produce a complex label or notifier output.

Here is a way to demonstrate the timeout:

```
<?
for (var i = 0; i < 1000000; i++) {
  if(i%10000 == 0) {
    writeln( "testing the timeout " + i);
  }
}
?>
```

The label would look something like this:



testing the timeout 0
testing the timeout 10000
testing the timeout 20000
testing the timeout 30000
JS ABORTED, after 3 ticks

Three ticks is approximately 50 msec.

Remembering Values from One Poll to the Next

Sometimes it is useful to retain the value of a variable from execution of the JavaScript to the next.

There are two different techniques you can use to achieve this:

- **JavaScript Global Variables** - Any JavaScript variable declared at global scope is retained from one execution of JavaScript to the next. The variable is visible regardless of which device is running the script. The variable is also visible regardless whether the JavaScript is running to generate label text or a notifier's text. Keep this in mind when using the same script for more than one device - you may find yourself overwriting a global variable unexpectedly.
- **Device JavaScript Variables** - A piece of data can be stored in a device. An advantage of these variables over global variables is that each device can have the same named variable but the value will be different for each device. You use `self.get(...)` and `self.set(...)` to read and write this data. The name of the variable must be different than any probe parameter or probe variable.

Example: Storing a Value With a Device

To read the value stored in the device's variable "MyInformation" into myinfo:

```
var myinfo = self.get( "MyInformation" );
```

To write the value of myinfo out to the device's variable "MyInformation":

```
storedinfo = self.set( "MyInformation", myinfo );
```

The function `self.set(...)` actually returns the value that is being stored. If the value cannot be saved, (for instance, if you try to save to an existing probe parameter or probe variable) the returned value is the actual value of the parameter or variable, not the one you tried to save.

Example: An Incrementing Counter

Here is a way to implement a counter that increments each time the label is drawn. Note that the first time the script runs, the counter variable does not yet exist.

This script below gets the value of "Count", displays it, increments it, and saves it. The first time the script runs, `self.get()` returns the string "BAD ARG, see debug log". Since JavaScript cannot turn this value into a number, you can use the JavaScript `isNaN()` function to determine that `n` is NaN (Not a Number), and thus has not been initialized.

```
<?
var n = Number( self.get( "Count" ));
if (isNaN(n)) n = 0;
writeln( "Count is " + n);
n++;
self.set("Count", n);
?>
```

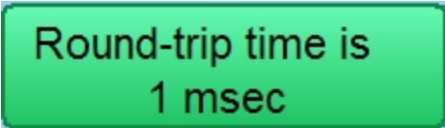
A similar technique would also work for JavaScript global variables as well.

Accessing Device Attributes

You can also use JavaScript to access device attributes. The syntax is different than for accessing probe parameters and variables. It still uses the `self` object, but the attribute names are simply properties of the `self` object. The syntax looks like this:

```
<?
var rtt = self.RoundTripTime;
writeln( "Round-trip time is \n" + rtt + " msec");
?>
```

The above JavaScript reads the last round-trip time into `rtt`, and displays it:



Round-trip time is
1 msec

If you misspell a device attribute, the error shows up as a JavaScript syntax error because the misspelling is not JavaScript data, but actual language syntax. You would see "JS EXCEPTION, see debug log" in the label, and a detailed explanation in the debug log.

Any device attribute can be used in a label. For a list of device attributes, see [Device Attributes \(Pg 656\)](#).

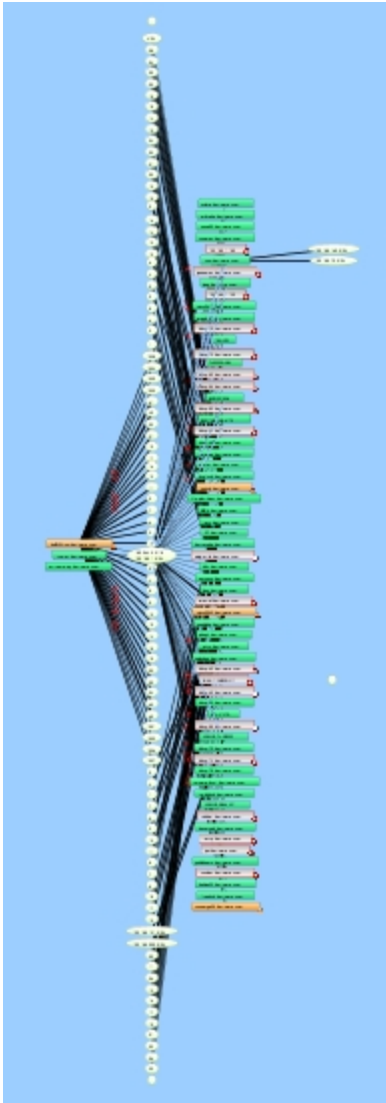
Accessing Interface Attributes

Devices connect to networks through interfaces. Each device has a property called `interfaces`. In JavaScript, this property appears as an array of Interface objects. The example below lists all down interfaces:

```
<?
var downInterfaces = 0;
for (var i =0; i < self.interfaces.length; i++) {
  var ifc = self.interfaces[i];
  if ((ifc.Enabled == "TRUE") && (ifc.Status == "down")) {
    downInterfaces++;
    write( ifc.Index + ". ");
    write(ifc.Alias.length > 0 ? ifc.Alias : ifc.Name );
    writeln( " : " + ifc.Status);
  }
}
writeln();
writeln(downInterfaces + "/" + self.interfaces.length + " interfaces
down");
?>
```

Any interface attribute can be used in a label. For a list of interface attributes, see [Interface Attributes \(Pg 670\)](#).

Using the Arrange Commands



Use the ***Organic***, ***Tree***, ***Cycle***, ***Bus***, ***Star***, and ***Grid*** commands available from the Format menu's ***Arrange*** submenu to rearrange and organize the selected elements automatically.

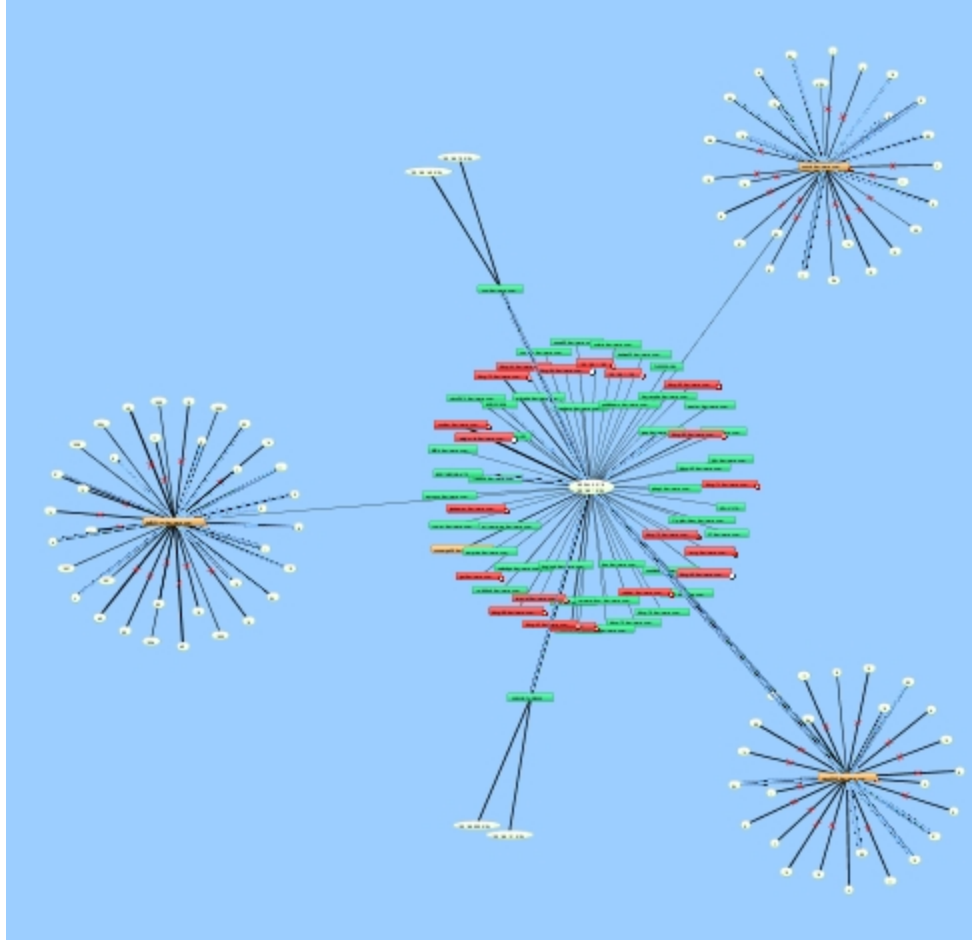
Note: If no objects are selected, ***Organic***, ***Tree***, and ***Grid*** operate on all map objects, or on any selected objects. For ***Star*** and ***Bus***, you must have at least one object selected. For ***Cycle*** and ***Grid***, you must have at least two objects selected.

Using the Organic Command

Use the Organic command, available from the Format menu's Arrange submenu, to arrange the objects on a map so that crossed lines are minimized, and objects are not overlaid on each other. This is the method used to arrange devices during auto-discovery.

To the right is a complex map. Notice that there are many overlapping links.

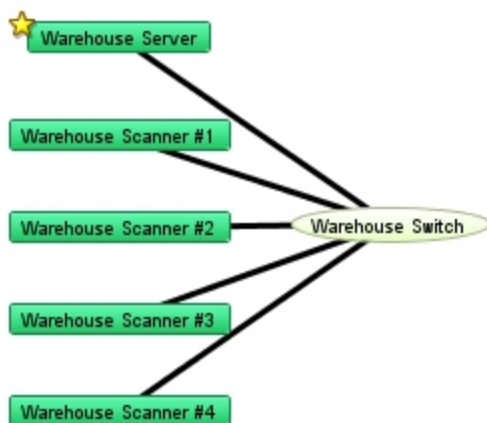
Here is the same map after applying the Organic command.



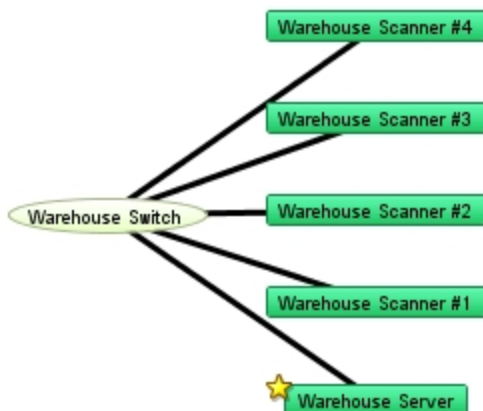
Using the Tree Commands

Use the **Tree** command to arrange the current selection in a tree. A sub-menu controls whether the tree structure should be drawn to the **right**, **down**, **left**, or **up**.

Arrange items in a tree structure. Choose which direction the branches of the tree should go. Shown below are **Tree > left** and **Tree > right**.



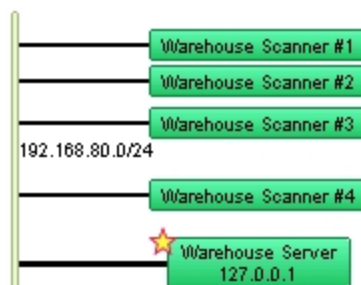
Tree > left



Tree > right

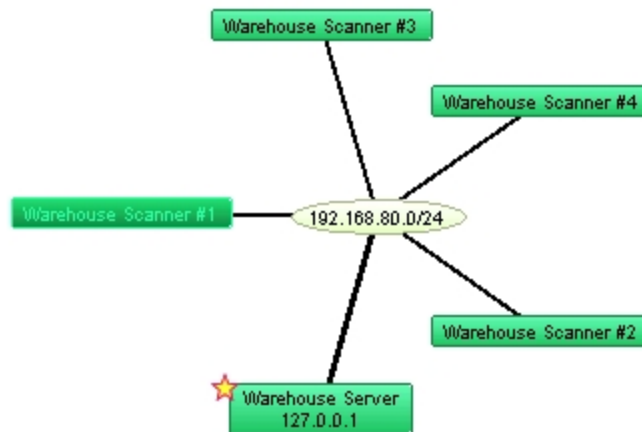
Using the Bus command

The network oval in the center of the cluster above represents an Ethernet segment that interconnects several devices in an office. To make it a cluster, use the **Bus** command from the **Arrange** submenu.



Using the Star Command

The **Star** command arranges connected items in a circle around the selected item, similar to the Organic command.



Using the Grid Command

Use the Grid command to arrange connected items in a grid.

To use the grid command:

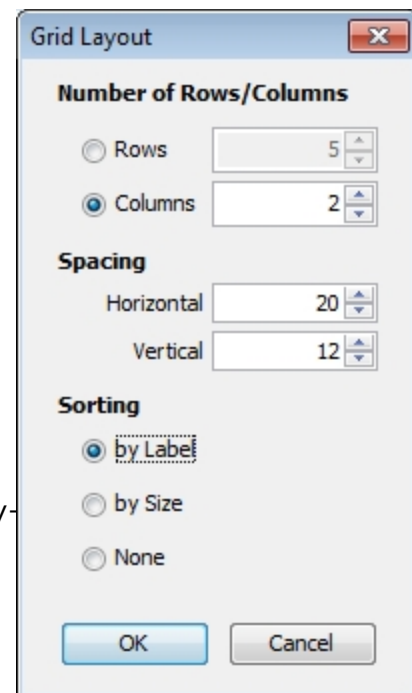
1. Select the devices you want to arrange in a grid.
2. From the Format menu's Arrange submenu, choose Grid... The Grid Layout dialog appears.
3. Choose your parameters as appropriate.
4. Click OK. The devices are arranged as specified.

Note: Sorting by **None** moves the selected devices to form a grid relative to the upper-left icon in the selection.

The example below shows the result of the Grid layout command after selecting only the devices in Star example above.



2-column grid layout



Using the Cycle Command

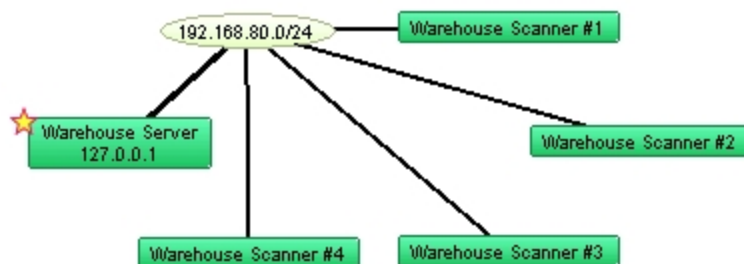
Note: The Cycle command is deprecated. We recommend you Organic command for initial map layouts.

Use the **Cycle** command to spread out the items in the map, and make the relationships more clear. The **Cycle** command moves all devices and networks near the edge of the window as shown below.

To use the Cycle command on all map objects:

1. From the Edit's Select menu, choose **Select All** (Cmd-A).
All objects in the map are selected.
2. From the Format menu's Arrange submenu, choose **Cycle**.
The objects are evenly distributed around the map as shown below.

The **Cycle** command moves all devices and networks near the edge of the window as shown below.



Results of the Cycle command.

Other Tips for Arranging Your Maps

Having formed a bus or star cluster, drag it to the edge of the window. This allows you to see the interconnections of the remaining devices. Create other clusters as required.

Once you have identified and arranged the clusters, use the following tips to fine-tune your map:

- **Move one or more items around the window** - Drag them to a new position. Use shift-click to add or remove items from the current selection before dragging.
- **Automatically select connected items - *Alt/Option-click*** an object to select all the leaves connected to it. (A leaf is an object that has no other connections.) A second ***Alt/Option-click*** selects all the objects (leaves and non-leaves) connected to the current selection.
Subsequent ***Alt/option-clicks*** continue to expand the selection, choosing first the leaves, then the non-leaves that are attached to the current set of selected objects.
- **Use the *Format* menu commands** to affect *placement* of items in the map. In addition to the **Cycle**, **Bus**, and **Star** commands described above, use these menu commands to change the orientations or sizes of the items in the map.
 - Align...** modify the alignment of items
 - Rotate...** rotate the selected items around their center
 - Scale...** increase or decrease the separation of the selected items
- Use these **Format** menu commands to affect the *appearance* of individual items:
 - Icon:** change the item's shape to a rectangle, oval, wire, cloud, text, or other icon
 - Label:** modify a text label for an item in the map
 - Label position:** change the location of a text label relative to its item
- Right-click (or Ctrl-click) to set the Font, text Size and text Style from the context menu for all selected items.
- If networks or ports are not important for a map, hide them from the [Interfaces Window \(Pg 195\)](#).
- See [Editing Labels for Devices and Networks \(Pg 106\)](#) and [Connecting Devices to Switch Ports \(Pg 121\)](#) for more tips on arranging the map.
- InterMapper periodically scans routers and switches and displays newly discovered interfaces. If you delete the interface/oval from the map, InterMapper rediscovers it and displays it again. You can hide them from the [Interfaces Window \(Pg 195\)](#). For more information, see [Hiding and Un-hiding Detail \(Pg 128\)](#).
- If you use a switch's VLAN capabilities to segment your network, you may want to show which equipment is connected to each VLAN segment. Do this by manually dragging device links to the proper port to indicate the correct con-

nection point. See *Connecting Devices to Switch Ports* in the [Switches](#) (Pg 121).

- If the layout of the network as discovered doesn't match your conceptual network layout, you can copy a network oval and move device links to the new network oval. For more information, see [Copying Network Ovals](#) (Pg 123).

Connecting Devices to Switch Ports

Here are some tips for handling switches in your map.

Hiding Inactive Ports

Auto-discovered switches have all their ports shown in a map. This can add clutter, and can make it difficult to see the real structure of the map. In addition, an inactive (i.e., unused) switch port will cause the switch itself to be placed in alarm.

Note: You can also convert your map to Layer 2. Using Layer 2 information, your map is automatically updated to match the topology represented by the switch's Layer 2 information. For more information, see [Mapping with Layer 2 \(Pg 353\)](#).

Use the Interfaces window to select and remove these switch ports.

To hide switch ports:

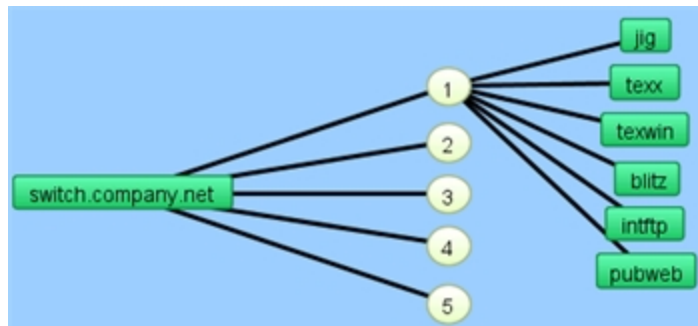
1. With the map editable, right-click/CTRL-click the switch and choose Interfaces Window. The Interfaces window appears, showing the switch's available interfaces.
2. Select or clear the checkboxes to enable or disable switch ports. The disabled interfaces disappear from the map.

Connecting Devices to Switch Ports

InterMapper does not connect devices to the proper port of a switch. Instead, it connects all the devices of a subnet to the first switch port it discovers (usually the port with ifIndex=1).

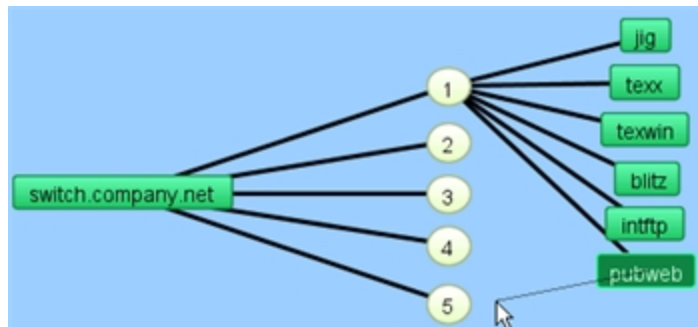
You can manually move a device's link to the proper port by dragging the link from the central oval (labeled "192.168.1.0/24" in the figures below) to the proper port, as shown below:

1. The map before making changes. The switch's ports are shown by the numbered ovals. (Make sure the map is in [Edit mode \(Pg 180\)](#).)



2. Click a link and drag it. A line appears, and follows the cursor.

Note: You can drag links only *from* a network.



3. Drag the link to the desired port. The link disconnects from the original network oval and remains connected to the new. Note that the port's oval now contains two port numbers: that of the switch (7) and the port number of the device (2).



Tip: When moving links to the proper ports on a switch, it's sometimes easier to change the port labels to display the port's number.

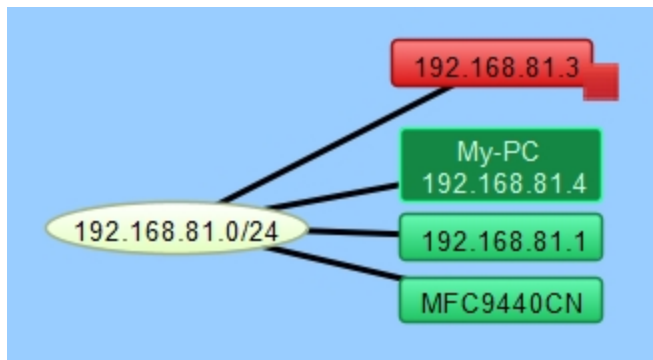
e Copying Subnet Ovals

After discovering all your devices, you may find that the map layout does not match your concept for a logical layout of your network.

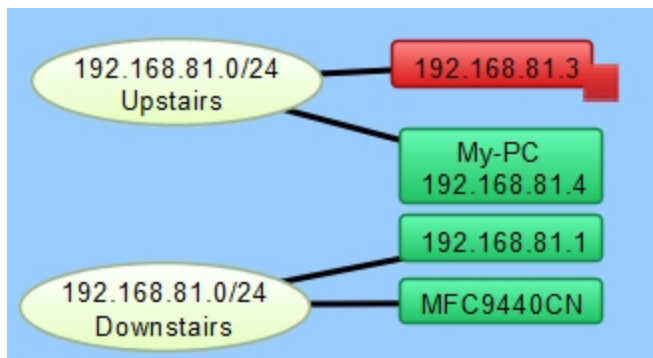
You can make a copy of a subnet oval and reconnect your devices to it. This allows you to create visual arrangements that more closely match your concept of a logical map layout.

To copy a subnet oval and connect to it:

1. With the map editable, click to select the subnet oval you want to copy.
2. From the Edit menu, choose **Copy**.
3. From the Edit menu, choose **Paste**. The copy of the subnet oval appears on the map.
4. Move the subnet oval to preferred location.
5. From the Format menu, choose **Label...** or press **Ctrl/Cmd+click**. The Edit Network Label window appears.
6. Add a meaningful label to distinguish it from original label. For more information, see [Editing Labels](#) (Pg 106)
7. For each device you want to connect to the new oval, drag the link from the old oval to the new oval. The device is connected to the new oval.



Before copy



After copy, two links moved, labels updated

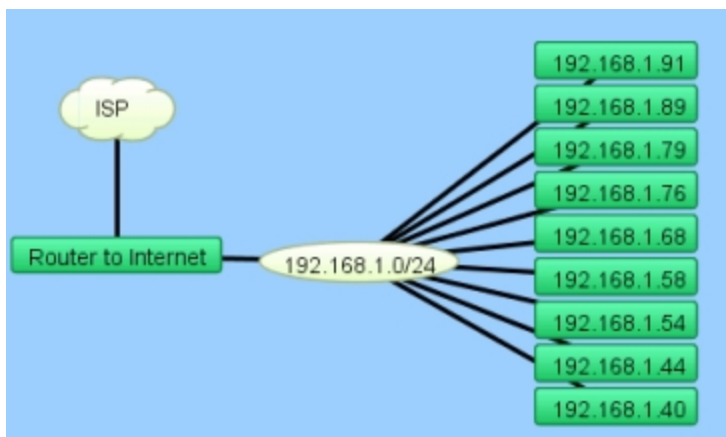
Adding Unmanaged Hubs and Switches to a Map

InterMapper cannot automatically discover or monitor unmanaged switches and hubs (so-called 'dumb' devices) since they have no IP address. However, there is a workaround that allows you to represent them on an InterMapper map.

To do this, you can create a placeholder icon, and then manually drag the links from the appropriate devices to this new icon. Although InterMapper cannot test or monitor this "fake" equipment, it will appear on the map and display the inter-connections of your network as a tool to diagnose problems.

Here is a step-by-step description of the process. Note that this description works equally well for either switches or hubs.

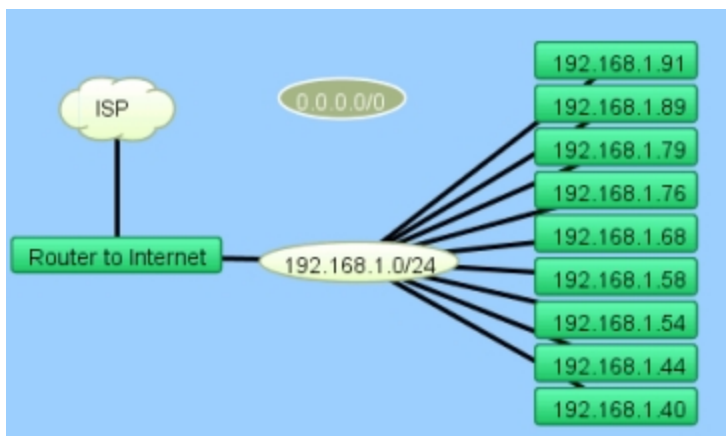
In the starting map, notice that InterMapper has automatically connected a number of devices to the network oval labeled "192.168.1.0/24". We happen to know that the top three devices --IP addresses 192.168.1.91, .89, and .79-- are in fact, connected to a dumb (e.g., unmanaged) hub on the floor above. This page shows how to create a placeholder icon to represent the hub and connect those three devices to it.



The problem

The top three devices - IP addresses 192.168.1.91, .89, and .79 - are in fact, connected to a dumb (e.g., unmanaged) hub upstairs.

We want to create a placeholder icon that represents the hub, and then move the connections for those devices to the placeholder.



Step 1: Create a placeholder to represent your hub

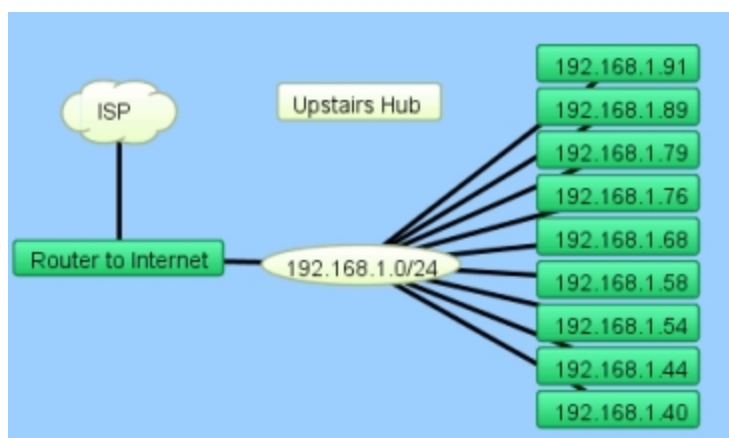
The first step is to create a new (empty) network.

To create the new network:

1. From the Insert menu, choose **Net-work...**

2. Enter a subnet number that's the same as the device's current subnet (oval) as shown in [Adding Networks to a Map \(Pg 68\)](#).

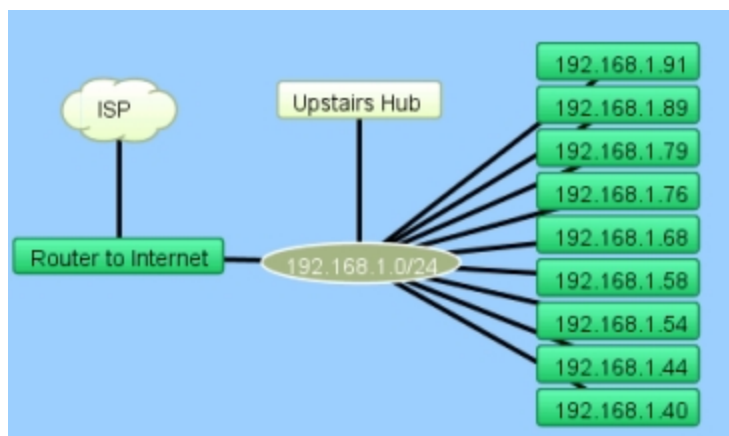
The new network appears as an oval, with the subnet number you entered (not "0.0.0.0/0", as shown in this example).



Step 2: Tidy up

Tidy up the appearance of the item:

1. Move the new network up a little bit
2. Change its shape to a rectangle using the **Icon...** command from the Format menu.
3. Change its name to "Upstairs Hub" using the **Label (Cmd-L)** from the Format menu.



Step 3: Connect the hub to the network

Connect this new rectangle to the oval below.

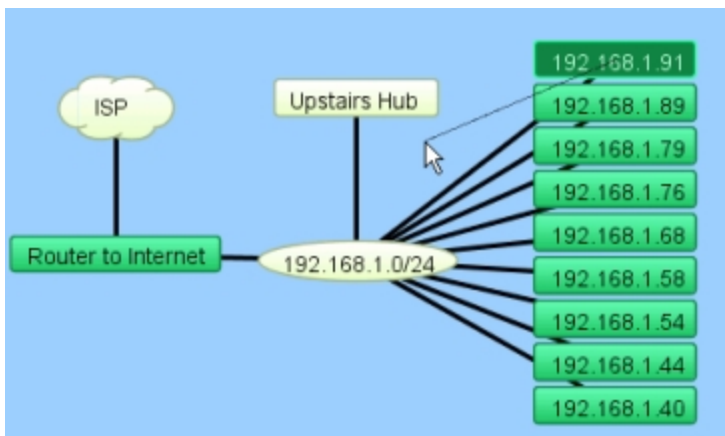
To connect the "hub" to the network:

1. Click to select the new rectangle.
2. From the Insert menu, choose **Link**. A line

Attach To from the device's context menu.

3. Click the network oval below the rectangle. The "hub" is connected to the network

A line appears, connecting the two items together. This line persists as you move the items around your map.



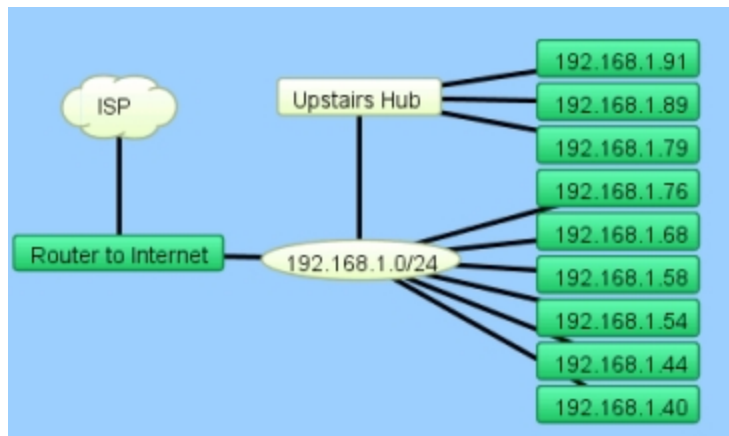
Step 4: Connect the devices to the "hub"

Drag each of the links for the three devices from the oval to the new rectangle.

To connect the devices to the "hub":

1. Click on a link (line) for the first device, and drag it toward the "Upstairs Hub" rectangle.
2. Let go of the mouse when it's over the rectangle.

The line "sticks" to the new rectangle. Do this for all three links.



The result

Your map should look like this after dragging the three links from the oval to the "fake" hub.

Hiding and Un-hiding Detail

It is easy to create maps with more detail than you may want to see, especially if your network contains one or more switches. This is because InterMapper periodically scans routers and switches and displays newly discovered interfaces. If you delete a network oval from the map, InterMapper no longer polls the associated interfaces.

- Use the Delete command to delete one or more networks. Select the networks you don't want to see, then choose **Delete** from the Edit menu, or press the Delete key. InterMapper does not poll interfaces for deleted networks.
- [Create sub-maps \(Pg 71\)](#) - If you want to hide detail, but still want to monitor its state, and view it occasionally, you can create separate maps containing the detail you want to hide, then make a new map with devices which use the [Map Status probe \(Pg 448\)](#). Each device represents a "sub-map." .
- Use the [Interfaces window \(Pg 195\)](#) to hide or show interfaces. When you hide an interface, it is no longer polled, and alerts are not sent.

Chapter 6

Notifiers and Alerts

InterMapper can send many different kinds of notifications to alert the network manager of problems in the network. An entire map can be configured to use a default notifier (or set of notifiers), and then individual devices can have customized notifiers.

What is a Notifier?

Think of a notifier as a little "robot" that watches the state of one or more devices, and performs a specified action when the device changes to a certain state. The action is called a notification.

You can attach notifiers to a device, and then specify which states (down, up, warning, alarm, critical) should trigger the notifier. When a device changes to that state, the notifier triggers, and *InterMapper* sends the notification.

For example, you can create a notifier that sends an e-mail message. You then attach that notifier to a device. You might also specify that it should be triggered when the device goes down or comes back up. When the device goes into either of those states, the e-mail would be sent.

Notifier Types

There are several types of notifiers; each uses a different method to send a notification:

- [E-mail \(Pg 144\)](#) - sends an e-mail
- [Alphanumeric Pager \(Pg 147\)](#) - sends a page through a dial-up modem using the TAP protocol.
- [Network Paging \(Pg 155\)](#) - sends a page across the Internet using the Simple Network Paging Protocol (SNPP).
- [SMS Alert \(Pg 157\)](#) - sends a text message to a cell phone via SMS.
- [Sound \(Pg 142\)](#) - plays a sound associated with the state of the device.
- [SNMP Trap \(Pg 167\)](#) - sends an SNMP trap to the specified trap receiver
- [Syslog \(Pg 166\)](#) - sends a message to a syslog server
- [WinPopup \(Pg 165\)](#) (Windows only) - sends a message to the specified user. The message appears in a separate window.
- [Command Line \(Pg 160\)](#) - executes a command on the *InterMapper* host machine.
- [Group \(Pg 146\)](#) - sends notifications to a group of existing notifiers.
- [PowerShell \(Pg 173\)](#) - executes a PowerShell command or script on the *InterMapper* host machine or a remote Windows machine.
- [AutoMate \(Pg 169\)](#) - executes a task created with HelpSystems' AutoMate software..

What You Can Do With Notifiers

- The **Notifier List** (Available from the Server Configuration section of the Server Settings window) is a library of notifiers you have created.

- You [create a notifier \(Pg 131\)](#) from the Notifier List, the Default Notifiers dialog, or the Notifiers window.
- You [configure the notifier \(Pg 139\)](#), then [test it \(Pg 141\)](#) to make sure it's working properly.
- You [attach a notifier \(Pg 133\)](#) to a device using the Attach Notifier dialog.
- You [remove a notifier \(Pg 131\)](#) using the Notifier List.
- You [define a set of default notifiers \(Pg 132\)](#) using the Default Notifiers dialog. When you add a new device to a map, the default notifier set is attached to the new device automatically. (You can also create and attach notifiers to individual items.)
- You attach notifiers only to devices, not to networks.

Parts of a Notifier

Notifier Name	This is a human-readable description of the notifier. It's useful to include the type and recipient in the name, e.g., "Network Techs via email" or "Syslog to Main Logger"
Notifier Type	There are many notifier types - e-mail, sounds, traps, etc. - as listed above. Each notifier you create will cause some kind of notification or alert, depending on its parameters.
Notifier Parameters	The parameters of a notifier indicate the recipient or the action to be performed. Parameters can specify an e-mail address, a sound file to play, the address of a syslog or trap server, a pager account, or a script or program to run. Each notifier type determines its parameters.
Notifier Schedule	Each notifier has a schedule associated with it. The schedule specifies the days of the week, and the hours of each day during which a notifier should send notifications. If the event happens outside the schedule, no notification will be sent.

About the Notifier List

The Notifier list is a library of notifiers that you can attach to different devices on your map. It is available from the Server Settings window. You create, configure, edit, remove, and disable notifiers from the Notifier list. Once you have created and configured the notifiers you want to use, you can attach them to devices.

Occasionally, you may be about to attach a Notifier, and discover that you need to create a new one before you can attach it. You can quickly open the Notifier list from the Notifiers window, and create a new notifier.

How Notifications Get Sent

When an event occurs, for example, when a device changes to a new state (Up to Down, Warning to Alarm, Alarm to OK) InterMapper triggers the attached notifiers that apply to that new state. The notifier then sends a notification, as defined in its parameters, to the specified target users as defined by the notifier schedule.

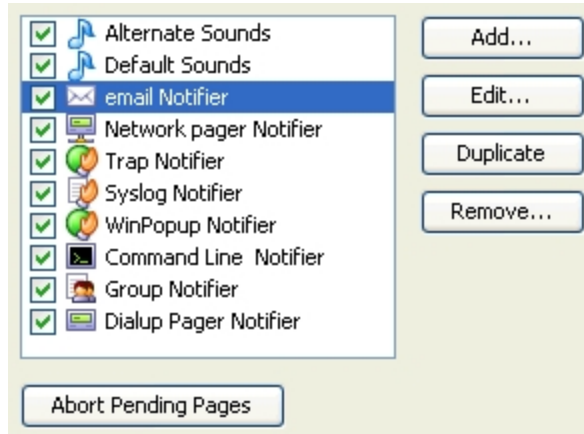
Working With Notifiers

You create and configure notifiers in the Notifier list. You attach notifiers to devices in the Notifiers window.

Using the Notifier List

Use the Notifier List to view a list of all notifiers defined for all open maps. You can also use the Notifier List window to:

- Add new notifiers
- Edit existing notifiers
- Copy existing notifiers
- Remove a notifier
- Activate or deactivate a notifier



Notifier List window. The Default Sounds are built-in.

To view the Notifier List:

- From the Server Settings window's Server Configuration section, choose **Notifier List**. The Notifier List appears.

To add a notifier:

1. Click **+**. The Configure Notifier window appears.
2. Configure the notifier and click **OK**.

To edit an existing notifier:

1. Click to select the notifier you want to edit.
2. Click **Edit...** The Configure Notifier window appears, showing the current configuration of the selected notifier.
3. Edit the notifier's configuration, and click **OK**.

To make a copy of an existing notifier:

1. Click to select the notifier you want to copy.
2. Click **Duplicate**. The Configure Notifier window appears, showing the current configuration of the selected notifier.
3. Edit the notifier's configuration, and click **OK**.

To remove a notifier:

1. Click to select the notifier you want to remove.
2. Click **Remove...** A confirmation dialog appears.
3. Click **Remove**. The selected notifier disappears from the Notifier List.

To activate or deactivate a notifier:

- Select or clear the check box to the left of the notifier's name in the notifier list. When deactivated, the notifier never triggers. This is useful for vacation periods or other times when you don't want the notifier to be used.

Defining Default Notifiers

You can create one or more notifiers that, by default, are attached to every new device you create. When the status of the device changes to a specified state, the notifier sends a notification automatically.

InterMapper ships with one default notifier, called "Default Sounds." It plays a default sound when a device goes down, and another sound when the device comes back up.

To create a set of default notifiers:

1. From the Edit menu, choose **Map Settings...** The Map Settings window appears.
2. In the left pane, click **Default Notifiers...** The Default Notifiers pane appears, showing a list of defined notifiers, with a column containing a check box for each possible device state.
3. For each notifier you want to attach to new devices on the map, select the check box for each state you want to trigger that notifier.
4. When finished, close the click **OK**. The specified notifiers are automatically attached to each new device added to your map.
5. To attach the default notifier set to all the devices on the map, click **Reset All**. Any attached notifiers are removed, and replaced with the default notifier set.

Note: Changing default notifiers does not change notifiers already attached to existing devices; it applies only to newly added devices. To attach the default notifier set to all devices on the map, click **Reset All**. Any attached notifiers are removed, and replaced with the default notifier set.

To change all notifiers on a map:

- Select all items on the map, then open the Notifiers window from the Monitor menu. Any changes you make apply to all selected map items.

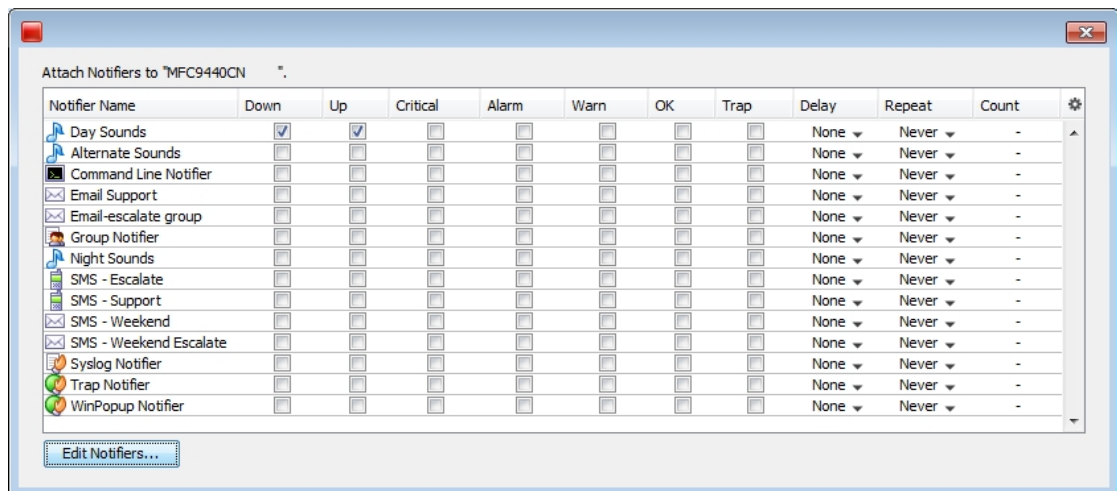
Attaching a Notifiers to Devices and Interfaces

Attaching Notifiers to Devices

You can attach one or more notifiers to any device. For each notifier, you can choose which states trigger a notification to be sent. For example, a particular device might have a notifier send an e-mail when a device goes down, but can have a second notifier that plays sounds when the same device goes down, comes up, or enters an alarm state. You might also send an e-mail to an on-site system administrator during the day, and to a different administrator outside business hours.

To attach a notifier to a device:

1. Select one or more devices.
2. From the Monitor menu, choose **Notifiers Window**. The Notifier Settings window appears, containing the notifiers currently attached to the selected item as shown below.
3. Select or clear the check boxes for the device states you want to trigger the notifier. A notification is sent when the device's state changes to any of the selected states.



Attach Notifier window

Notes:

- You can create a new notifier from the Notifier Settings window. The "Edit Notifiers..." button is a shortcut to the Notifier List in the Server Settings page.
- You can also attach notifiers to devices from the Device Notifiers list view of the Map window.

Attaching Notifiers to Interfaces

You can also attach notifiers to a device's interfaces, so that alerts are sent for a link when that link goes down.

To attach a notifier to one or more interfaces:

1. Select the device containing the interfaces you want to attach notifiers to.
2. View the Interfaces window, either from the Monitor menu or from the device's context menu. The Interfaces window appears, showing the device's interfaces .
3. Select the interfaces you want to attach notifiers to, using Click, Shift-click, and Ctrl-click. Use Ctrl-A to select all of the device's interfaces.
4. Right-click (or Ctrl-click) one of the selected interfaces and choose
5. **Notifiers Window** from the context menu. The Notifier Settings window appears, containing the notifiers currently attached to the selected interfaces.
6. Choose the notifier you want to attach from the dropdown menu.
7. Select or clear the check boxes for the device states you want to trigger the notifier. Set **Delay**, **Repeat**, and **Count** values as appropriate. A notification is sent when any of the interfaces' states change to one of the selected states.

Note: You can also attach notifiers to interfaces from the **Link Notifiers list** view of the Map window.

Resetting Devices to the Default Notifier

If you change the default notifier or any of its settings after attaching it to devices , you can reset all of the devices in a map to use the new notifier or settings:

1. With the map window open for the map you want to reset, choose **Map Settings...** from the Edit menu. The Map Settings window appears.
2. In the left pane, click **Default Notifiers**. A list of notifiers appears.
3. From the Context menu (Right-click/Ctrl-click one of the devices) or from the Monitor menu, choose **Notifiers Window**. The Notifiers window appears as shown below.
4. Click **Reset All**. The selected devices are now attached to the default notifier.

Using the Delay, Repeat, and Count parameters

For each notifier, you can specify **Delay**, **Repeat**, and **Count** parameters. These parameters can be used to control how quickly and how frequently notifications are sent. For example, to avoid unnecessary pages you might configure a notifier to wait until a device has been down for two minutes before sending the first page. You might also choose to re-send a notifier every 10 minutes forever. Notifications are sent until the count is reached, or the device has been acknowledged.

How Delayed Notifiers work

InterMapper maintains a queue of notifications to be sent. When a DOWN, WARN, ALARM or CRITICAL event happens, InterMapper places a notification in the queue, and sets its "time to be sent" according to the delay. (UP, OK and Trap notifications are never delayed.)

When an UP or OK event occurs, InterMapper first searches the notification queue for the corresponding down, warn, or alarm notification. If it's there, InterMapper removes both the DOWN (or Warn or Alarm) notification and UP (OK) event and won't send either one. If not, then InterMapper sends the UP/OK notification straight away.

Notification Escalation

You can use notifiers to implement a problem escalation system by creating two or more notifiers for a device. The first notifier can fire quickly to alert someone immediately. A second notifier can be delayed for a period of time, perhaps 30 minutes or an hour, before notifying a second person. If the problem remains when the second notifier's delay time is reached, the second notification is sent. As soon as a problem is acknowledged, no further notifications are sent, even if the outage lasts a long time.

Using Vantage Points

InterMapper can block or suppress notifications for devices that are "behind" or "shadowed by" another failed device. This helps you avoid receiving dozens (or hundreds) of notifications for devices that don't respond because there is a router or link down between InterMapper and that device.

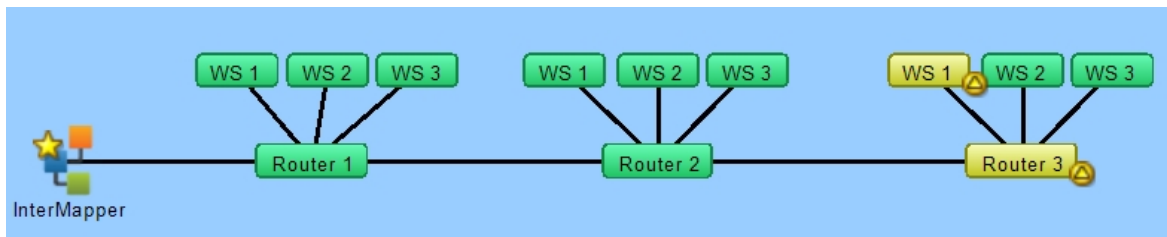
When one device is dependent on another, you can use this dependency to suppress the notifications for devices that depend on the failed device.

There's no need to set the dependencies manually between devices on a map. Instead, InterMapper follows the links that are already part of the map.

To enable dependencies, you [set a Vantage Point \(Pg 137\)](#). The Vantage Point indicates the position from which InterMapper views the network. You usually set the Vantage Point on the actual device where InterMapper is running. Once you've set the Vantage Point, InterMapper can determine which devices are dependent on which other devices.

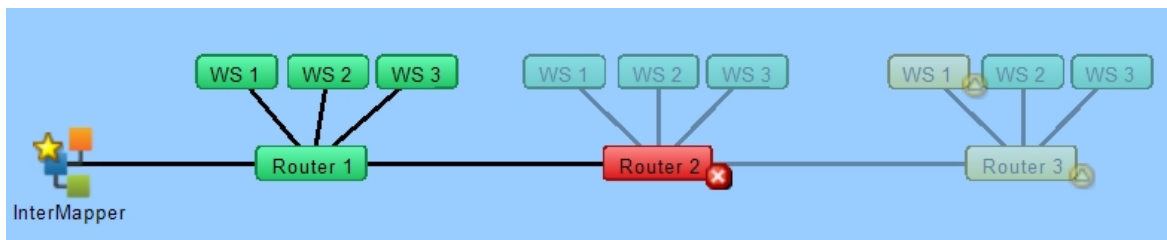
Example 1: All devices are up

The example below shows a map with several interconnected routers. The yellow star on the InterMapper icon shows that it is the map's vantage point.



Example 2: One device is down, shows dependent devices

In this example, Router2 has failed. InterMapper will send the normal notifications for Router2, but it will suppress notifications for any of the devices that depend on it. Those dependent devices' icons are dimmed on the map to show they're being shadowed by the failure.



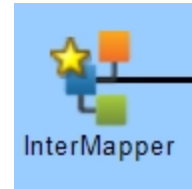
Setting a Vantage Point

To set a map's Vantage Point:

1. Make the map editable.
2. Select the device or network you want to use as the Vantage Point.
3. From the Monitor menu's Set Info submenu, choose **Set Vantage Point**.

or

- When the map is editable, right-click (or Ctrl-click) a device or network, then choose **Set Vantage Point** from the context menu's Set Info submenu.



*A Vantage Point.
Notice the star
on the item.*

A small star appears next to the item, as shown here.

Moving and Removing a Vantage Point

You may remove a Vantage Point or move it to a new item.

To move a Vantage Point to a new item:

- Set the Vantage Point to the new item as described above.

To remove a Vantage Point:

1. Select the item to which the Vantage Point is currently assigned.
2. From the Monitor menu's Set Info submenu, choose **Remove Vantage Point**.

or

- Control-click the item to which the Vantage Point is currently assigned, then choose **Remove Vantage Point** from the dropdown menu's Set Info submenu.

A star next to the item disappears, and no Vantage Point is set. Notifications are sent for all map items.

How Vantage Points Work

When a device goes down (when no response has been received from it), dependencies are used to determine whether to suppress the notification.

Starting at the Vantage Point, InterMapper follows the links toward the device in question. If the only path to that device passes through a device, a link, or an interface that's already down, InterMapper knows that the device is shadowed, dims its icon, and suppresses the notifications.

If there is no failure along the path, or if there is no path at all (functional or not) to the device, InterMapper allows the notification to go through.

Even though a device is shadowed (and its notifications are suppressed), InterMapper continually probes the device to show its status.

One Vantage Point Per Map

You can define only one Vantage Point per map. Even if a map does not show the machine on which the server is running, you can use the Vantage Point to indicate the communication path from the InterMapper server to the devices on the map.

This allows InterMapper to know which devices are inaccessible if a switch or router goes down.

Managing Notifications for Dependent Devices

If a device fails but has not yet been polled, it is possible for notifications for dependent devices to be sent even though the failed device is responsible for the failure. This can result in a number of unnecessary and inaccurate alerts being sent.

In this situation, configure the notifiers for the dependent devices to have a delay that is longer than a single polling cycle of the device on which they depend. In this setup, the dependent devices do not send an alert if the device on which they depend goes down. An alert is sent only for the failed device.

Configuring Notifiers

A notifier has four attributes:

- A *notifier name*.
- The *type* of notification to send
- A *schedule* of hours during which the notification should be sent
- A set of *parameters* determined by the notification type. This is the information required to allow the notification to be sent. For example, an E-mail notifier requires a valid E-mail address.

To configure a notifier:

1. Enter a notifier *name* in the **Name** box.
2. In the **Notifier Type** dropdown menu, choose a notifier type.
3. In the Configuration panel, enter configuration information for the selected notifier type.
4. In the **Scheduled Hours** panel, choose the hours during which the notifier is active.
5. Click **Test Notifier Configuration** to send a test notification.

Note: The Test Notifier Configuration button checks to make sure that the notifier is configured correctly and that a notification is placed in the queue. The notification can fail to be delivered, even when the notifier is configured correctly.

6. Close the Configure Notifier window.

The Configure Notifier window.

- Use the left side of the window to choose the *type* of notification, and to set the notifier parameters.
- Use the right side of the window edit the *schedule* during which the notification can be sent.

When you select the type of notifier from the **Notifier Type** dropdown menu, the left pane changes to show the parameters required for the selected notifier type.

Removing a Notifier

You can remove a notifier from the Notifier List window.

To remove a notifier:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears, with a list of settings in the left pane.
2. From the Server Configuration section of the settings list, choose **Notifier List**. The Notifier List window appears.
3. Click to select the notifier you want to remove.
4. Click **Remove...** A confirmation dialog appears.
5. Click **Yes**. The selected notifier disappears from the Notifier List.

Configure Notifier Window Reference

Name

Enter a name in the Name box. The name can be any can be any descriptive text string.

Tip: If the notifier is active only at certain times of the day or week, you may want to include a description of the time period as well. For example, you could assign names like "Weekend Pager" and "Second Shift Pager" to notifiers that had those time schedules.

Notifier Type

From the Configure Notifier window's **Notifier Type** dropdown menu, choose a notifier type. For more information, see [Notifier Types \(Pg 129\)](#) at the top of this topic.

Scheduled Hours

Select a range of hours during which this notification should be sent.

- Active hours are shown in gray.
- Inactive hours are shown in white.

To set a range of hours:

- Click and drag across a range of hours.
- Click and drag across all blocks to invert the selection.

To add or remove hours from the schedule:

- Click an individual cell to make it active or inactive.

To activate or deactivate all hours in the schedule:

- Double-click the **Active Hours** legend to activate all hours in the schedule.
- Double-click the **Inactive Hours** legend to de-activate all hours in the schedule.

To edit the message sent with the notification:

- Click **Edit Message...** The [E-mail Notification page \(Pg 129\)](#) shows the editing interface.

Note: You can also use InterMapper variables and Javascript to insert information dynamically into a notifier message or subject. For more information, see [Dynamic Label & Alert Text \(Pg 108\)](#).

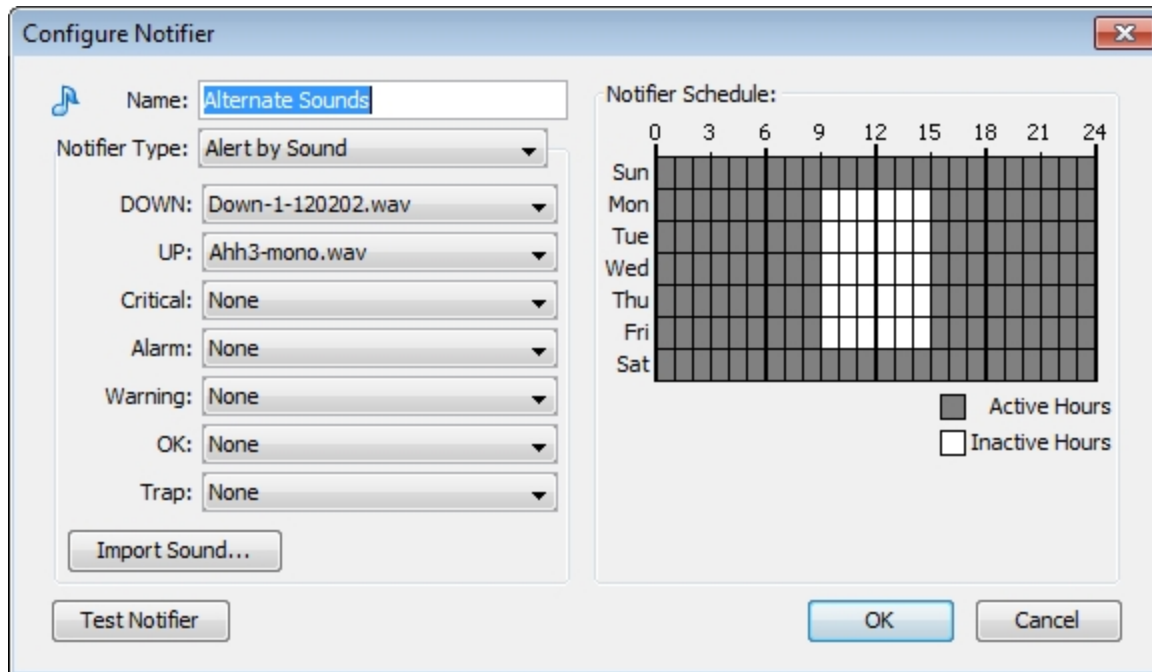
Test Notifier

- In the Configure Notifier window, click **Test Notifier**. The notification is sent immediately, with the state defined as "Test."

Once you have created notifiers, you may attach them to all devices (the default notifier is used for all new devices) or to one or more devices.

Configuring a Sound Notifier

A sound notifier plays a sound whenever a device enters a new state. For each state, you can assign a different sound.



The Configure Notifier window for Sound notifier type. For each device state, you can select a different sound.

To configure a sound notifier:

1. Create or edit the notifier you want to configure.
2. In the **Notifier Type** dropdown menu, choose **Alert by Sound** if it is not already chosen. The Sound Notifier configuration panel appears as shown in above.
3. For each state, use the **Sound Name** dropdown menu to choose the sound you want to play when the device changes to that state. If you do not want sounds to play for certain states, set those states to **None**. The states are described below.
4. If the sound you want to use for a particular state does not appear, click **Import Sound...** to import a sound file containing the sound you want to use.

Notes:

- On Windows machines, the available sounds are located in the *InterMapper Settings/Sounds* folder.
- On Mac OS X machines, the available sounds include any system sounds or the sound files in */System/Library/Sounds* folder, as well as those in the */InterMapper Settings/Sounds* folder.
- Supported sound file formats: .WAV, .AIF, and .AU.
- InterMapper RemoteAccess must download each sound file from the InterMapper server, but once it is downloaded it is cached on the remote machine.

Bear in mind that large sound files may affect system performance for remote users.

- Sounds are queued up for playing. One sound does not start until the previously queued sound is completely finished playing. Relatively short sound files are recommended.

Device States

- **Up** - Plays a sound when a device responds normally after being down.
- **Down** - Plays a sound when a device goes down (fails to respond to InterMapper's queries.)
- **Critical** - Plays a sound when a device enters Critical state.
- **Alarm** - Plays a sound when a device enters Alarm state.
- **Warning** - Plays a sound when a device enters Warning state.
- **OK** - Plays a sound when a device is no longer in critical, alarm, or warning state.
- **Trap** - Plays a sound when InterMapper receives an SNMP trap from the device.

InterMapper's default sound notifiers are as follows:

- **Down** - plays the *Klaxon* sound
- **Up** - plays the *Yahoo* sound
- All other states are set to **None**.

What you can do with sounds

You can use sounds in many different ways to help give you audible indicators the condition of your network. Here are two possible uses for sound notifiers.

- **Create different sound sets for different times of day, or for different days** - create different sound notifiers, each having a different notifier schedule. This can be helpful if you need to, for example, use certain notification sounds during working hours in a busy office, and have louder, more easily distinguishable sounds outside working hours, when you are working away from your computer.
- **Create different sound sets for certain devices** - create sound notifiers for certain kinds of devices, and use different sounds. You can tell without looking if, for example, a certain machine or router goes down. It is also useful if you been having trouble with a particular device.

Sound files must be placed in the InterMapper Settings/Sounds folder before they can be made available in the Server Configuration Notifier List panel of the Server Settings window.

Configuring an E-Mail Notifier

Use an e-mail notifier to send an e-mail message to one or more recipients. The e-mail message can provide detailed information about the device that triggered the notifier. The example below shows the Configure Notifier window for the E-mail notifier type.

The screenshot shows the 'Configure Notifier' dialog box. On the left, there is a 'Name' field with 'Jack - Email', a 'Notifier Type' dropdown menu set to 'Electronic Mail (SMTP)', and an 'Addresses' text area containing 'jack@example.com'. A note states: 'The outgoing SMTP server and sender must be set in the E-Mail pane of the Server Settings before e-mail can be sent.' Below the addresses is an 'Edit Message...' button. On the right, the 'Notifier Schedule' section features a grid for days of the week (Sun-Sat) and hours (0-24). The grid shows active hours (shaded) from 0 to 24 for all days. A legend indicates 'Active Hours' (shaded square) and 'Inactive Hours' (white square). At the bottom are 'Test Notifier', 'OK', and 'Cancel' buttons.

Configuring an e-mail notifier.

To configure an e-mail notifier:

1. In the Configure Notifier window, choose "Electronic mail (SMTP)" from the **Notifier Type** drop-down menu.
2. In the **Address** box, enter the e-mail address you want to receive the notification. You can enter multiple addresses, separated by commas, spaces, tabs, newlines, or carriage returns.

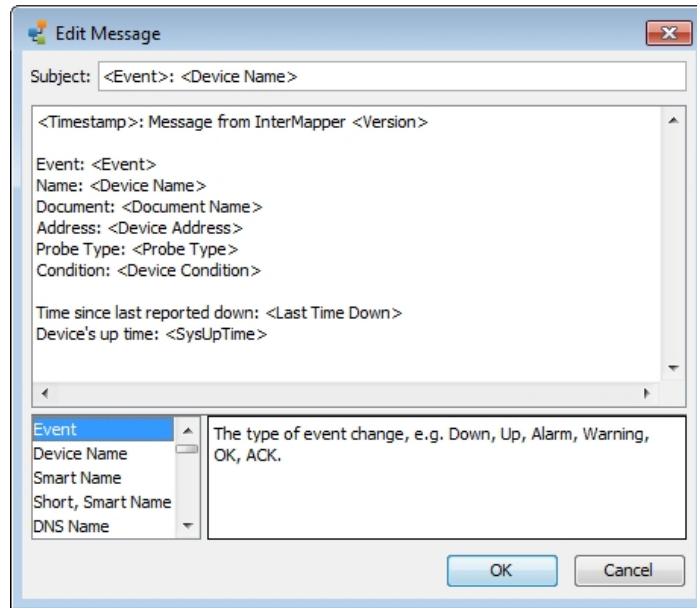
Note: E-mail is sent using an outgoing SMTP mail server. Before InterMapper can send e-mail notifications, you must specify the SMTP host you want to use for sending e-mail notifications. For more information on how to specify your outgoing SMTP mail server (and a backup server) see [E-mail Preferences \(Pg 264\)](#).

Editing the Text of an E-mail Notification Message

Edit E-mail Message window, showing the default e-mail message.

An E-mail notifier sends a text message that describes the failure.

Use the Edit Message window to edit the message sent by the notifier. The example below shows the Edit E-mail Message window containing the default e-mail message. The list at the lower left contains variables you can substitute in the text.



Double-click an item to insert it into the message text. When the notification is sent, the inserted item is replaced with its current value in the message text.

Subject :

```
<Event>:
<Device Name>
```

Message:

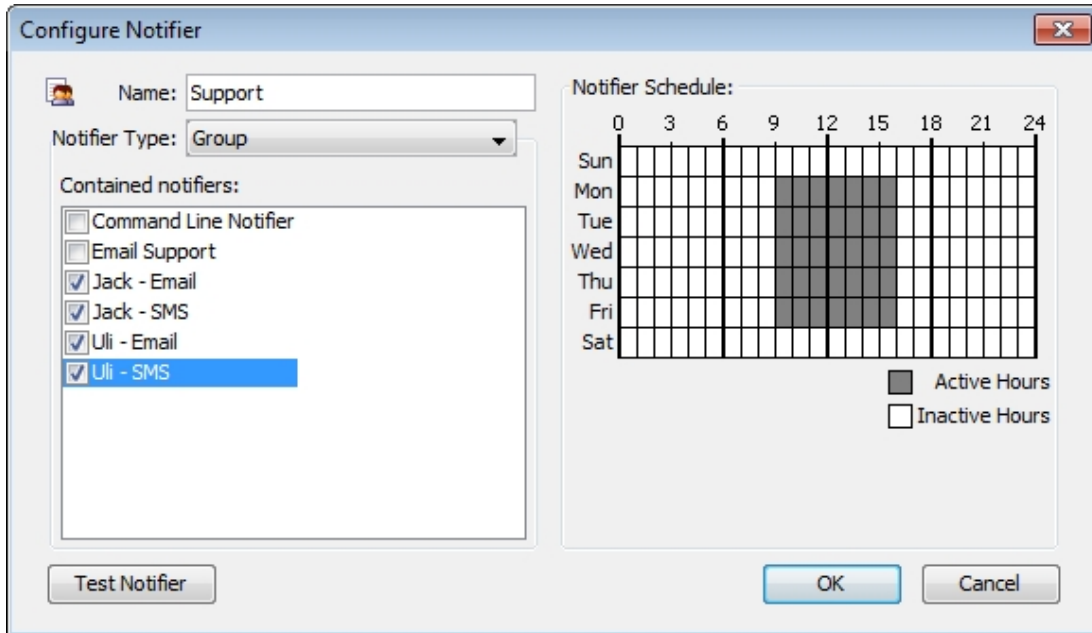
```
<Timestamp>:
  Message from InterMapper <Version>
Event: <Event>
Name: <Device Name>
Document: <Document Name>
Address: <Device Address>
Probe Type: <Probe Type>
Condition: <Device Condition>
Time since last
  reported down: <Last Down>
Device's up time: <SysUpTime>
```

Note: You can also use InterMapper variables and Javascript to insert information dynamically into a notifier's subject or message text. For more information, see [Dynamic Label & Alert Text \(Pg 108\)](#).

Using Group Notifiers

InterMapper can group notifiers together so that a transition to a particular device state sends multiple notifiers, even of different types, for that event.

To create a Group notifier, select **Group** from the **Notifier Type** dropdown menu. A set of currently-defined notifiers appears, with a check box next to each. To create the group notifier, check the appropriate boxes in the list.



The "Configure Notifier" dialog box is shown. It has a title bar with a close button. The "Name" field contains "Support". The "Notifier Type" dropdown is set to "Group". Under "Contained notifiers:", there is a list with checkboxes: "Command Line Notifier" (unchecked), "Email Support" (unchecked), "Jack - Email" (checked), "Jack - SMS" (checked), "Uli - Email" (checked), and "Uli - SMS" (checked and highlighted). The "Notifier Schedule:" section shows a 24x7 grid. The grid has columns for hours (0, 3, 6, 9, 12, 15, 18, 21, 24) and rows for days (Sun, Mon, Tue, Wed, Thu, Fri, Sat). A legend indicates that shaded squares represent "Active Hours" and white squares represent "Inactive Hours". In the grid, the hours 9 through 18 are shaded for all days of the week. At the bottom, there are buttons for "Test Notifier", "OK", and "Cancel".

How it works

When the Group notifier is invoked, InterMapper first checks the time schedule. If the time is applicable, InterMapper invokes each of the checked notifiers. They in turn check their schedules, and send the notification if desired.

Notes:

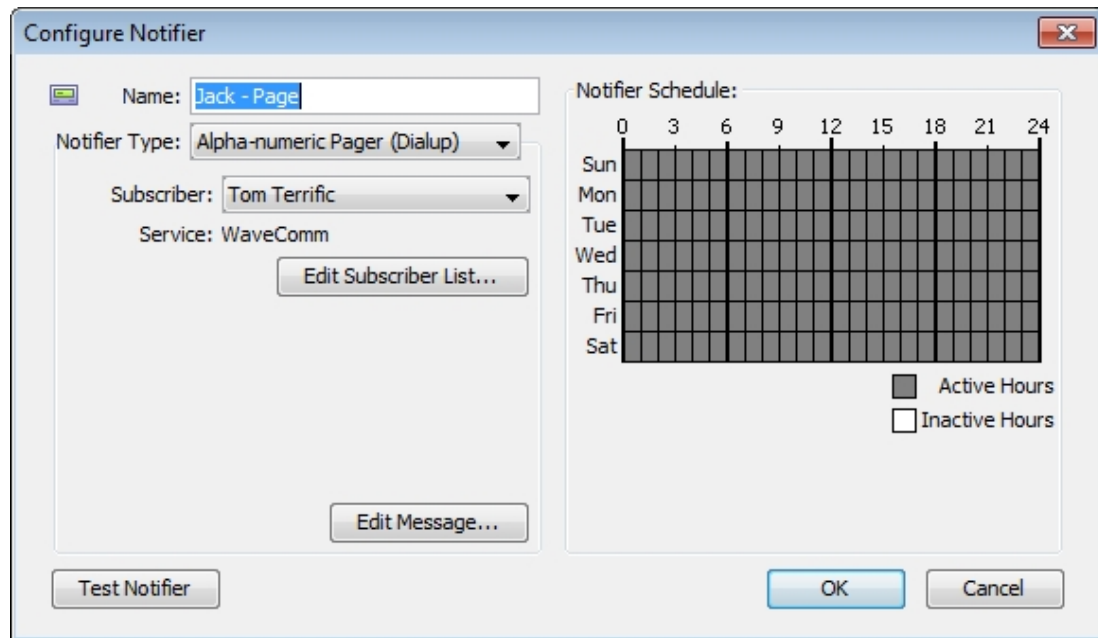
- It is normal for a group notifier's schedule to be 24 x 7, so that the underlying notifiers will govern when they are sent.
- When attaching a group notifier to a device, leave its component notifiers' boxes unchecked. Otherwise, duplicate notifications are sent (once for the group and again for the component).

Configuring a Pager Notifier to use an Analogue Modem

InterMapper uses TAP, the Telelocator Alphanumeric Protocol, with an internal or external analogue modem to connect to a page service, and to deliver a notification.

To use the built-in support for paging via analogue modems:

1. [Create a new notifier \(Pg 131\)](#).
2. From the **Notifier Type** dropdown menu, select *Alpha-numeric Pager (Dial-up)*. The example below shows the Configure Notifier window with the Alpha-numeric Pager (Dial-up) type.
3. From the **Subscriber** dropdown menu, choose a subscriber, or choose **Edit List...** to add or edit paging services or subscribers.
4. Click **Edit Message...** to edit the message that is sent to the pager. (See warning below)
5. In the **Notifier Schedule** panel, choose the hours during which the page will be sent.
6. When finished, click **OK**.



A notification that uses the built-in modem paging facilities. The page will be sent to the person specified by the Subscriber menu.

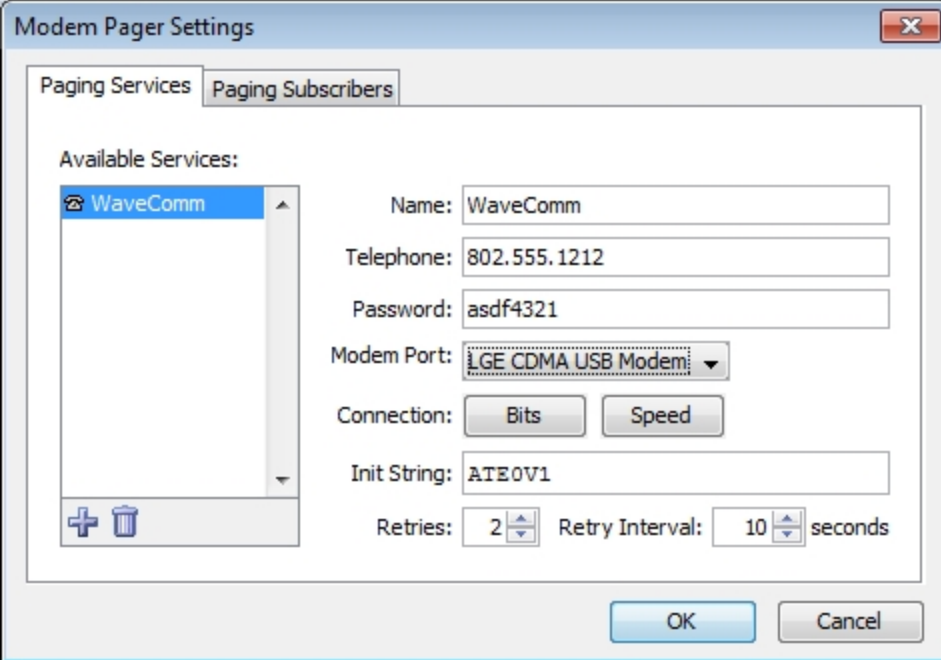
Warning: Many paging services limit the length of a message. Sending a longer message can cause multiple pages per event, and can considerably increase your pager bill.

Setting up Paging Services and Subscribers

Before you can use the paging options, you need to:

- Set up one or more paging services.
- Set up one or more subscribers for that service.

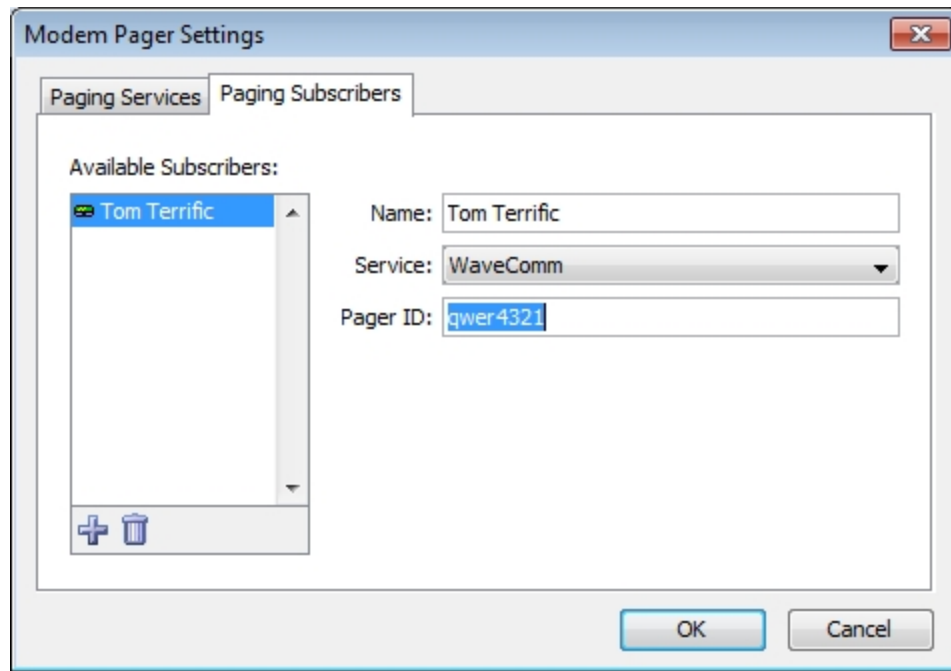
The window above assumes that you have already configured InterMapper for your pager service.

The image shows a Windows-style dialog box titled "Modem Pager Settings". It has two tabs: "Paging Services" (selected) and "Paging Subscribers". Under "Available Services:", there is a list box containing "WaveComm" with a plus icon at the bottom. To the right of the list box are several input fields: "Name:" with "WaveComm", "Telephone:" with "802.555.1212", "Password:" with "asdf4321", "Modem Port:" with a dropdown menu showing "LGE CDMA USB Modem", "Connection:" with "Bits" and "Speed" buttons, "Init String:" with "ATE0V1", "Retries:" with a spinner set to "2", and "Retry Interval:" with a spinner set to "10" followed by the text "seconds". At the bottom right are "OK" and "Cancel" buttons.

Entering information about a service

To add or edit paging services:

1. Choose **Edit List...** from the **Subscriber** drop-down menu. The Paging Settings window appears.
2. Click the **Paging Services** tab. A list of paging services appears, if any are defined.
3. Click a service to edit, or click **Add**. The information for the paging service appears.
4. Enter dialup information in the boxes provided. Use the information about your paging service to enter the service name, telephone number, and password, the port to which your modem is attached, and the modem configuration.
5. In the **Bits** dropdown menu, choose values appropriate to your modem. Open the menu repeatedly to set the data bits, stop bits, and parity. By default, the values are set to 7 data bits, 1 stop bit, and Even parity.
6. In the **Retries** box, set the number of times you would like the page to be sent if it fails. The default is 2.
7. In the **Retry Interval** box, set the number of seconds to wait between retries. The default is 10 seconds.
8. When finished, click **Done**.



Entering information about a subscriber

To add or edit paging subscribers:

1. Choose **Edit List...** from the **Subscriber** drop-down menu. The Paging Settings window appears.
2. Click the **Paging Subscribers** tab. A list of paging subscribers appears, if any are defined.
3. Click a service to edit, or click **Add**. The information for the paging service appears.
4. In the **Name** box, enter the name of the person you want to receive the page.
5. From the **Service** dropdown menu, choose the user's Paging Service. If the user's paging service doesn't appear, you need to create it as described above.
6. In the **Pager ID** box, enter the person's pager ID. (This may be different from the Service phone number that you entered when creating the user's Paging Service definition above.)
7. When finished, click **Done**.

Paging Log File

The paging log file is a special file which will receive logging of all paging traffic and messages, including the details of the modem commands and text written and read. The information in this log may help you or InterMapper Technical Support to troubleshoot paging if it is not working correctly.

To start logging this traffic, use the Log Files server settings panel to create a log file named Paging (The log file name will be "Paging<date>.txt") Logging will continue until the log file is removed through the Log Files panel.

Modem Compatibility

With Mac OSX

InterMapper has been tested with Mac OSX using various built-in modems, an external USB modem (MultiTech MT5634ZBA-USB), and an older external modem connected via a KeySpan Twin Serial adapter (using KeySpan's current OSX driver) on a beige G3. With the KeySpan serial adapter, InterMapper lists both serial ports in the Modem Page Settings dialog and you are responsible for choosing the correct one.

With Windows and Unix

A number of modems have been tested with InterMapper. While we cannot guarantee that a particular modem works, we believe that most modems that support V.34 or a later specification will work well.

Sending SMS/Text Alerts to a Cell Phone

InterMapper can send SMS or text message alerts to a cell phone, mobile phone, or wireless phone. These notifications will be sent using an analogue modem to dial a TAP paging terminal at your wireless provider.

Note: The methods described below depend on an analogue modem dialing a TAP service or a cell phone. You can also use a cell modem to send SMS message directly to another cell phone. For more information, see [Configuring an SMS Notifier \(Pg 157\)](#). This may be preferable at this point.

There are several methods for sending alerts to a mobile phone.

TAP - the Telelocator Alphanumeric Protocol

InterMapper can send SMS or Text Messages using TAP, the Telelocator Alphanumeric Protocol, with an internal or external analogue modem. It will connect to a paging service and deliver a notification or alert to your cell phone

Using TAP to Send a Message

If your paging service provides a TAP paging terminal that forwards pages as SMS or text messages to your wireless phone, you can follow the instructions below to configure InterMapper to send alerts to your phone.

1. Add a new Notifier. To do this, click **Add** in the Server Settings>Notifiers List window. The Configure Notifier window appears.
2. From the **Notifier Type** drop-down list, choose **Alpha-numeric Pager (Dialup)**.
3. Click **Edit Subscriber List**.
4. Add a new paging service. To do this, click **Add** button in the Paging Services tab. Enter the name of the service, the phone number to dial (including any numbers you may need to access an outside line), and a password, if required. Use the default values for **data bits**, **stop bits**, **parity** and **speed** unless your paging service has provided you with different values.
5. Add a new subscriber. To do this, click **Add** button in the Paging Subscribers tab. Enter the **subscriber name**, then select the paging service you created in step 4 from the drop-down list. Enter the subscriber's cell phone number in the **Pager ID** field.
6. When you have finished adding the new paging service and subscriber, click **OK** to return to the Configure Notifier window.
7. Click **Edit Message** if you want to change the data included with the text message. Edit the message, then click **OK** when finished.
8. Edit the notifier schedule, if required.
9. Click **Test Notifier** to confirm that the message can be sent and received.
10. When finished, click **OK**.

Note: This procedure has been tested using Verizon's TAP access to their SMS/Text Message system. The access number is 866-823-0501. Other cell providers may offer a gateway to their text/SMS message service.

Sending a Message if TAP is Not Available

If your cell phone provider does not provide a TAP interface for text messages, you can use an e-mail-based service to deliver the message. You should contact your cell phone provider for details on sending alerts and notifications via e-mail. **Note:** Remember that sending an alert through e-mail fails if your connection to the Internet is down. See below for a low-tech workaround.

Workaround for When Your Internet Connection Is Down

If your Internet connection is down, but your cell phone provider doesn't offer access to their text/SMS message system via an analogue modem, you can still get notified about problems. Simply create a new Alpha-numeric Pager (Dialup) notifier and enter the cell phone number as the paging service number. It dials the phone directly. There won't be any voice or text/SMS message, but the CallerID will let the recipient know that it's InterMapper calling.

Troubleshooting SMS/Text Alerts

If you encounter any problems, InterMapper can create a log file that shows the details of the paging mechanism. This is useful to review or send to tech support. To do this:

- Open the Server Settings>Log Files window and click **Add** to create a new log file. Name the log file 'paging' and click **OK**.
- Test your notifier again from the Configure Notifier window. The paging.txt file contains detailed logging for the test notification. You can find the paging.txt file in the InterMapper Settings>InterMapper Logs folder on the server. If the information contained in the paging log isn't helpful to you, please send the file with a description of the problem to support@intermapper.com.

Notification Using a Numeric Pager

You can configure InterMapper to use alphanumeric modem paging to send messages to numeric pagers.

To send numeric pages, follow these three basic steps:

1. Create a new paging service.
2. Create one or more paging subscribers to receive the numeric pages.
3. Edit the notification message as you normally would. Any non-numeric characters are removed.

Step 1: Create a new paging service:

1. From the Edit menu, choose **Server Settings...**
2. In the Server Settings window, click to choose **Notifier List**.
3. Click **Add...** to create a new notifier.
4. From the **Notifier Type** dropdown menu, choose **Alpha-numeric Pager (Dialup)**.
5. From **Subscriber** dropdown menu, choose **Edit List...** The Modem Pager Settings window appears.
6. In the **Paging Services** tab, click **Add**. A New Service appears in the Paging Services list, and an information form for the new service appears at the right.
7. In the **Name** box, enter a name for the new service.
8. Leave the service telephone number blank. (This is what tells InterMapper to do numeric paging instead of alpha-numeric paging.)
9. Data bits, stop bits, parity, and baud rate are irrelevant and may be set to anything legal.
10. Leave the modem init string at the default, ATE0V1.
11. Choose the desired modem. You may create more than one such service, if you want.

Step 2: Create one or more paging subscribers:

12. Click the **Paging Subscribers** tab and create the paging subscriber(s) who will use numeric paging.
13. Set the service field to use the service created in the steps above.
14. Set the pager id to be the phone number used to dial the pager. To the pager id/phone number, append enough of your modem's pause characters (for most modems, this is a comma) to make sure that InterMapper waits until the call has been answered and any introductory message played to send the tones with the numeric message. This varies from service to service.

Step 3: Edit the message as you normally would:

When creating a notifier based on numeric pager subscribers, edit the message as you normally would, using the InterMapper macros if you so desire. When the page is sent, all non-numeric characters will be removed. So, the message:

DOWN: 192.168.1.132

becomes

1921681132

Future versions of InterMapper may contain new macros to provide numeric codes for common events.

Paging Log File

The paging log file is a special file which receives logging of all paging traffic and messages, including the details of the modem commands and text written and read. The information in this log may help you or InterMapper Technical Support to troubleshoot paging if it is not working correctly.

To start logging this traffic, use the **Log Files** panel of the Server Settings window to create a log file named **Paging** (The log file name will be "Paging<date>.txt") Logging continues until the log file is removed through the Log Files panel.

Configuring a Page Notifier to Send a Page Using SNPP (Network)

Use InterMapper's Simple Network Paging Protocol (SNPP) feature to send pages over a network. Using this protocol, pages can be sent quickly and reliably, without the use of an analogue modem or a separate telephone line.

To configure:

1. [Create a new notifier \(Pg 131\)](#).
2. From the **Notifier Type** dropdown menu, select *Alpha-numeric Pager (Network)*. The example below shows the Configure Notifier window with the Alpha-numeric Pager (Network) type.
3. In the **Pager ID** box, enter the ID of the pager you wish to call.
4. In the **SNPP Server** box, enter the IP address or domain name of the SNPP Server.
5. If you want to use a port other than the default SNPP port, enter it in the **SNPP Port** box.

Contact your pager provider for IP address, domain name, and SNPP port information.

6. Click **Edit Message...** to edit the message that is sent to the pager.
7. In the **Notifier Schedule** panel, choose the hours during which the page will be sent.
8. When finished, click **OK**.

Note: InterMapper may not be able to reach your SNPP-based paging service via the Internet if your WAN circuits or routers are down. Be sure that you have a

backup notification mechanism for failures to critical services. See the workaround in [Alerts Via Cell Phone \(Pg 152\)](#) for a possible approach.

Configuring an SMS Notifier

Use an SMS notifier to send a text message directly to a cell phone using a cellular (GSM or CDMA) modem.

Note: To state the obvious, the modem used to send SMS messages must be able to connect to a cellular network. If there is no coverage at the location of the SMS modem, the server will not be able to send the notification.

Configure Notifier

Name:

Notifier Type:

Recipient:

Modem: Server Cell Modem

Notifier Schedule:

	0	3	6	9	12	15	18	21	24
Sun									
Mon									
Tue									
Wed									
Thu									
Fri									
Sat									

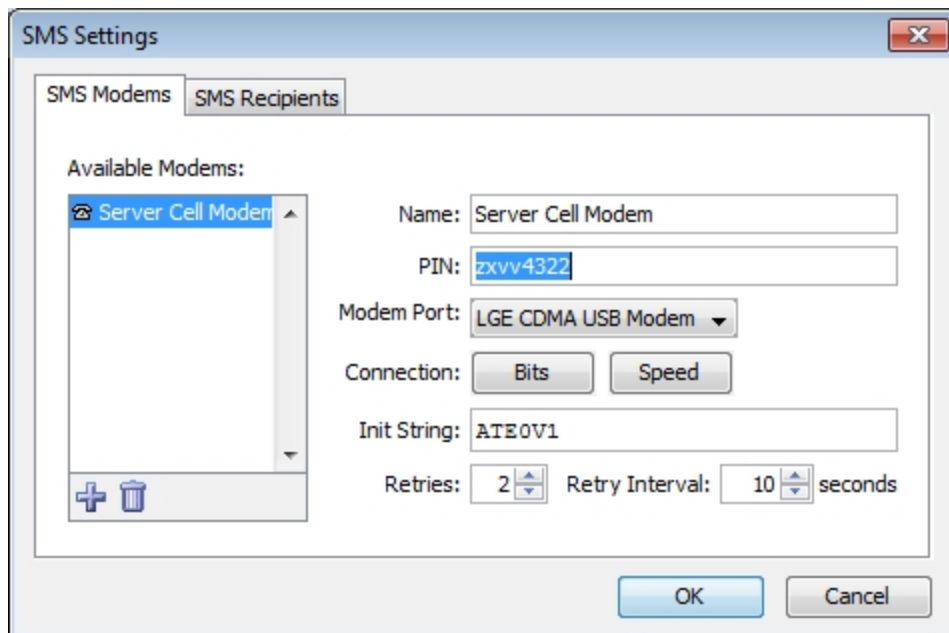
☒ Active Hours
☐ Inactive Hours

To configure an SMS notifier:

1. In the Configure Notifier window, choose "SMS" from the **Notifier Type** drop-down menu.
2. In the **Recipient** box, choose the recipient from the dropdown menu. If there are no recipients in the list, click **Edit Recipient List...** to configure connection to an SMS modem and to add and configure SMS recipients. See [Adding and Removing SMS Modems \(Pg 158\)](#) and [Adding and Removing SMS Recipients \(Pg 159\)](#), below.
3. If you want to edit the message, click **Edit Message...** For more information on editing messages, see [Editing the Text of an E-mail Notification Message \(Pg 145\)](#).

Adding and Removing SMS Modems

Before you can send SMS messages, you must set up at least one SMS modem through which SMS messages are sent.



To add an SMS modem:

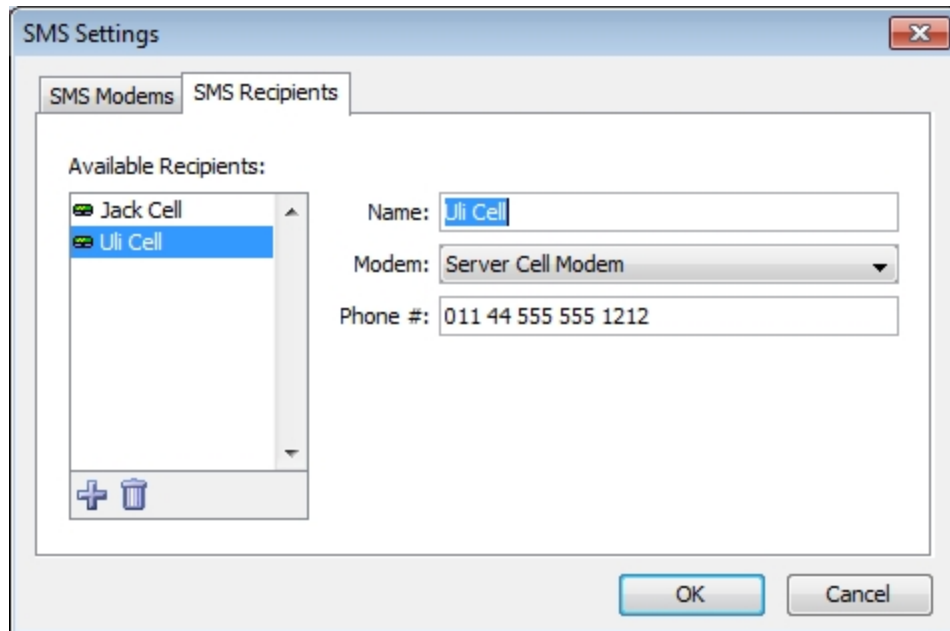
1. From the Configure Notifier window, with SMS selected as the Notifier Type, click **Edit Recipient List...** The SMS Settings window appears.
2. In the SMS window, click the **SMS Modems** tab. A list of available modems appears on the left.
3. Click **Add**. A new modem configuration form appears.
4. Enter a **Name** and **PIN**, choose a **Modem Port**, connection **Bits** and **Speed**, and enter a modem initialization string in the **Init String** box.

Note: Not all cell carriers require a PIN.

5. If you want to change the default retry specifications, set the **Retries** and **Retry Interval** values.
6. When finished, click **OK**. The specified modems appear in the recipient's **Modem** dropdown menu.

Adding and Removing SMS Recipients

Before you can send SMS messages, you must set up at least one SMS recipient to receive the message.



To add an SMS recipient:

1. From the Configure Notifier window, with SMS selected as the Notifier Type, click **Edit Recipient List...** The SMS Settings window appears.
2. In the SMS window, click the **SMS Recipients** tab. A list of available recipients appears on the left.
3. Click **Add**. A new recipient configuration form appears.
4. Enter a **Name**, choose a **Modem**, and enter the number of the recipient's phone in the **Phone #** box.
5. When finished, click **OK**. The specified recipients appear in the notifier's dropdown menu. The recipient's specified modem appears when you choose the recipient from the notifier's **Recipient** dropdown menu.

Command-line Notifiers

Use a command-line notifier specify a command (executable, shell script, batch file, etc.) to be executed as a notification.

To configure a Command Line notifier:

1. In the Configure Notifier window, choose "Command Line" from the **Notifier Type** drop-down menu.
2. In the **Command** box, enter the command to be executed. Include any arguments, exactly as you would type them on the command line.
3. Click **Test Notifier** to send a test notification.

Configuring the Command Line notifier

The screenshot shows the 'Configure Notifier' window. On the left, the 'Name' field contains 'Reset Power'. Below it, the 'Notifier Type' dropdown menu is set to 'Command Line'. The 'Command' text area contains the text 'reset-power 192.168.2.54'. To the right of the command field is an 'Edit Message...' button. On the right side of the window is the 'Notifier Schedule' section. It features a grid with days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) on the vertical axis and hours (0, 3, 6, 9, 12, 24) on the horizontal axis. The grid cells are shaded grey, indicating 'Active Hours'. A legend below the grid shows a grey square for 'Active Hours' and a white square for 'Inactive Hours'. At the bottom of the window are four buttons: 'Test Notifier', 'Edit Message...', 'OK', and 'Cancel'.

Command text box

Specify the executable you wish to run, including any arguments. Note that you need to specify the exact name, including any extensions such as .exe or .cmd.

If you want the message generated by InterMapper to be included in the command, place the text `${MESSAGE}` where you would like the message to go.

To include the message escaped for use in an HTTP query string, use `${ESCAPED_MESSAGE}` instead. You are responsible for supplying quotes if it is necessary.

Note: InterMapper allows an expanded command line (that is, the command line with the path added and the message inserted) up to 65535 characters, but you may find that your host platform limits the command-line size to only 255 characters. Windows users, to work around this limitation try converting your command-line script to a PowerShell script and use a [PowerShell notifier](#) (Pg 173).

Use `${STRIPPED_MESSAGE}` to strip the message of any punctuation that might cause trouble for the command-line notifier.

Use `${URLESCAPE}` to escape the message for use as a URL.

Note: The command box must refer to an executable which resides in the *Tools* subdirectory of the *InterMapper Settings* directory, or a subdirectory thereof. No other executables may be referred to. However, the executables in this directory may be links, shortcuts, or aliases to an executable elsewhere; they will be resolved and executed.

See the [Examples page \(Pg 162\)](#) for an example of a command line notifier.

Example Notification from a Command Line Program

An interesting tool for notifications that we've found is iPing (<http://www.iping.com/>). This tool gives you several ways of generating by computer a notification that iPing will read to the recipient over the phone. You can use this tool in any version of InterMapper by making an email notifier where the email address is ping.<yourAccountName>@iping.com.

However, iPing also has an API, one method of which allows more control over how the notification is carried out. This method, putnotification, is invoked via http. With a command-line tool like "curl" and InterMapper's command-line notifiers, you can create a powerful and tailored iPing notifier for InterMapper.

Implementing an iPing Notifier

The curl utility is already available on many Unix systems. If it is not available on yours, or if you are using Windows, you can find out more about it and download a copy from <http://curl.haxx.se/>. You can find out more about the putnotification API method for iPing from <http://www.iping.com/ipingv2/PutNotification.aspx>. The rest of this command-line notifier tutorial assumes that curl is installed and that you have an iPing account.

First, make sure that curl or an alias or soft link to it is in the Tools directory on the InterMapper server. The Tools directory is a subdirectory of the InterMapper Settings directory. If you do not have a Tools directory, you will need to create one. For security reasons, only executables in this directory may be executed as notifiers.

Open the Server Settings dialog box and click on the **Notifier List** entry. Click on the **Add...** button and choose a type of **Command Line**. Give it a name.

In the "Command" field, enter the iPing notification command you want to use. A simple example to send a message to a phone number immediately would be:

```
curl
"https://www.iping.com/services/iping.asp?method_name=putnotification
&user_name=testdriver
&password=12345
&phone_number=8448675309
&notification_dt=now
&msg_text_body=${ESCAPED_MESSAGE}"
```

Note: All the text above should be on a single line, with no blank spaces in the URL.

The parameters to the iPing message are:

- **method_name** must be "putnotification"
- **user_name** the name of your iPing account
- **password** the password of your iPing account
- **phone_number** the phone number to dial
- **notification_dt** Valid notification date/time (see the iPing documentation) or

"now"

- **msg_text_body** The text of the message to be spoken.

Note 1: The `msg_text_body` must be in a form suitable for inclusion in a URL. In particular, the text should not contain spaces, ampersands (&), question marks (?) or a number of other characters. InterMapper provides two macros that make it easy to enter the text:

- **\${URLESCAPE: xxxxx}** This macro returns a string that contains the text ("xxxxx") with all the URL special characters escaped properly.
- **\${ESCAPED_MESSAGE}** This macro is a special case facility that performs the URL escaping function on the notifier's `${MESSAGE}` string, as entered by the user. Click the "Edit Message" button to modify the default message. The default message is fairly short, as is appropriate for command-line notifications.

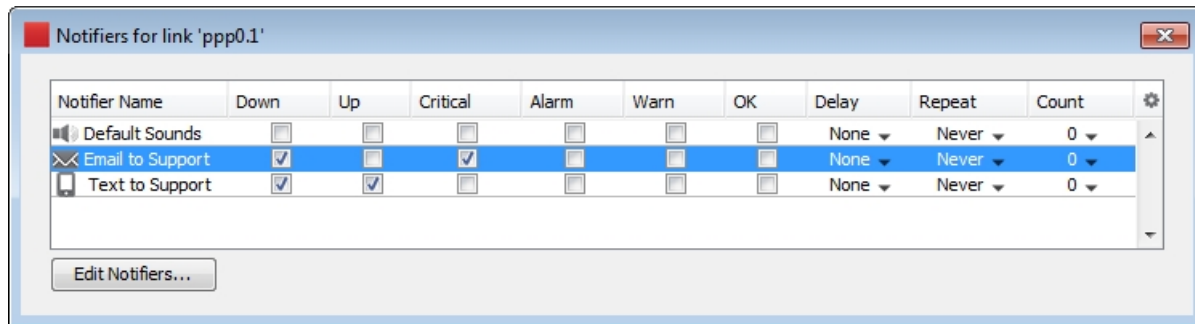
Note 2: The `curl` command generally exits with a code of zero. This avoids InterMapper log messages warning of unsuccessful notifications.

Interfaces & Notifiers

You can attach one or more notifiers to one or more interfaces. When the link status changes for any of the interfaces, an alert can be sent.

To attach a notifier to an interface:

1. [View the Interfaces window](#) (Pg 195) for the device containing the interfaces you want alerts from. The Interfaces window appears, showing all interfaces for the selected device.
2. Click the row containing the interface you want to attach notifiers to. The row is highlighted. Select additional rows using Ctrl+click or Shift-click.
3. Right-click (or Ctrl-click) the selected row, and choose **Notifiers Window...** The Notifiers window, showing the notifiers currently attached to the selected interface(s).
4. For each notifier, select or clear check boxes for status levels. Alerts are sent from the selected notifiers when a link status changes to the selected status.



Notifiers Window for a link

WinPopup (Windows Only)

When the device's status triggers a notification, a WinPopup message is sent to the designated person.

Note: Windows Messenger Service is not supported in Windows operating systems beyond Windows XP, so the WinPopup notifier works only when both the server and the target user or server are running Windows 2003 server or Windows XP.

Configure Notifier

Name:

Notifier Type:

User Name or Server:

Notifier Schedule:

	0	3	6	9	12	15	18	21	24
Sun									
Mon									
Tue									
Wed									
Thu									
Fri									
Sat									

☒ Active Hours
☐ Inactive Hours

To configure:

1. In the **User Name** or **Server:** text box, enter the user name or server name of the person to contact.
2. Click **Edit Message...** to edit the message that will be sent.
3. In the **Notifier Schedule** panel, choose the hours during which the page is sent.
4. When finished, click **OK**.

Configuring a Syslog Notifier

Syslog is a mechanism for recording information about significant events into a log file. It originated on Unix hosts which wrote the information to a local file (the *system log* file). This was later enhanced to write the data across a network to a server that collects the entries.

InterMapper can send a syslog message as a notification. That is, when an event occurs, InterMapper can write the data to a specified syslog server on the network.

The screenshot shows the 'Configure Notifier' dialog box. It has a title bar with a close button. Inside, there's a 'Name' field with 'Syslog-Emergency'. Below it is a 'Notifier Type' dropdown set to 'Syslog'. Then, 'Send syslog messages to:' is a text field with 'syslog.example.com'. Below that are 'Facility:' (dropdown, 'local0') and 'Severity:' (dropdown, 'emergency'). An 'Edit Message...' button is at the bottom of this section. To the right is a 'Notifier Schedule' section with a grid. The grid has columns for hours (0, 3, 6, 9, 12, 24) and rows for days (Sun, Mon, Tue, Wed, Thu, Fri, Sat). The grid cells are mostly shaded grey, representing 'Active Hours'. A legend at the bottom right of the grid shows a grey square for 'Active Hours' and a white square for 'Inactive Hours'. At the bottom of the dialog are three buttons: 'Test Notifier', 'OK', and 'Cancel'.

Send syslog messages to: - the IP address or DNS name of the syslog server that should receive the message

Facility: - The syslog server administrator may specify that messages from a particular source be tagged with a certain facility code. Select the facility requested by your administrator.

Severity: - Syslog messages can be tagged with a severity, so that the syslog files can be scanned for entries with different priority. Set the desired severity to

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

Edit message... - You may enter the format of the syslog message. See [Editing the text of an E-mail Notification Message \(Pg 145\)](#), where this process is described. Newline characters will be converted to spaces, so the message will appear as a single line. Syslog messages will contain "InterMapper" as the syslog tag.

Notification by SNMP Trap

An *SNMP trap* is an unsolicited SNMP message that is sent to another device. Traps are sent to convey the data immediately, instead of waiting for that device to be polled at some future time.

InterMapper sends a SNMP Trap as a notification when a device goes into a particular state.

Configuring a Trap Notifier. Enter the IP Address or DNS name for the device to receive the trap, along with the SNMP Trap Community String.

In the notification Schedule window, select "SNMP Trap" from the dropdown menu, and fill in the IP address or DNS name of the device to receive the trap, and the SNMP Trap Community string.

InterMapper sends six pieces of information in the trap. All are encoded as OCTET STRING. This information is also available in ASN.1 format. in the [Dartware MIB \(Pg 177\)](#).

Timestamp: The current date and time, as a string in the format:
MM/DD HH:MM:SS

Message: DOWN, UP, ALARM, WARN, OK, or TRAP (See the [Dartware MIB \(Pg 177\)](#).)

Device name: The devices DNS name, as a string

Condition: The condition of the device, as it would be printed in the log file.

Device Address: The address of the device the triggered the notifier.

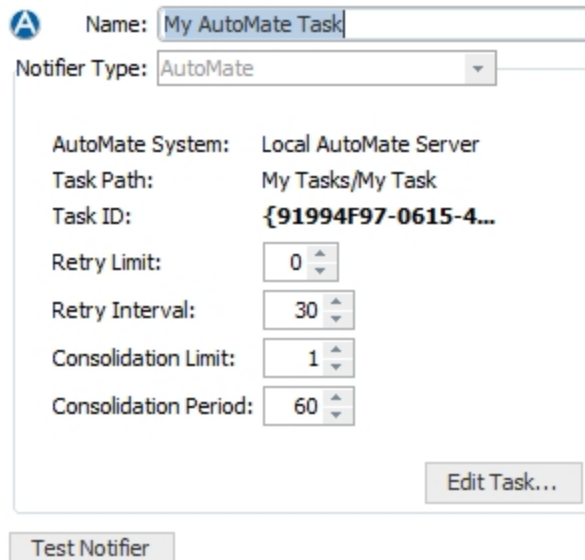
Probe Type: The type of probe that triggered the notifier

InterMapper's traps contain the following MIB variables, taken from the Dartware MIB (described in detail in [The Dartware MIB \(Pg 177\)](#)):

```
intermapperTimestamp = 1.3.6.1.4.1.6306.2.1.1.0  
intermapperMessage = 1.3.6.1.4.1.6306.2.1.2.0  
intermapperDeviceName = 1.3.6.1.4.1.6306.2.1.3.0  
intermapperCondition = 1.3.6.1.4.1.6306.2.1.4.0
```

AutoMate Notifier

Use the Automate Notifier to run an Automate task when specified conditions are met.



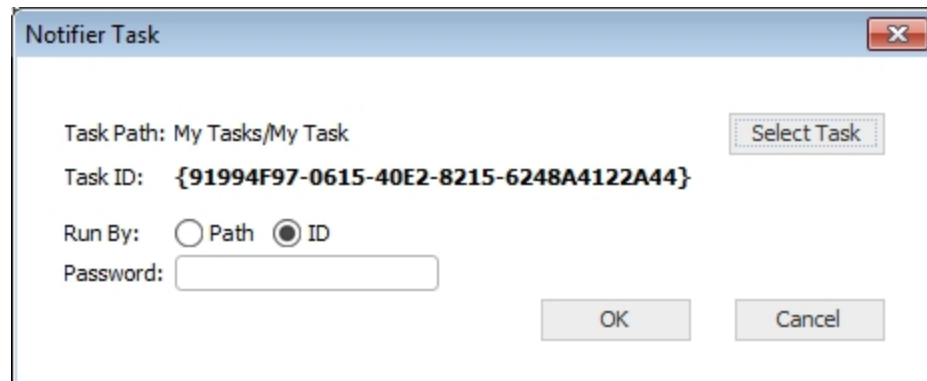
The screenshot shows the 'AutoMate Notifier' configuration window. It has a title bar with a blue 'A' icon. The 'Name' field is 'My AutoMate Task'. The 'Notifier Type' dropdown is set to 'AutoMate'. Below this, the 'AutoMate System' is 'Local AutoMate Server', 'Task Path' is 'My Tasks/My Task', and 'Task ID' is '{91994F97-0615-4...}'. There are spinners for 'Retry Limit' (0), 'Retry Interval' (30), 'Consolidation Limit' (1), and 'Consolidation Period' (60). An 'Edit Task...' button is at the bottom right of the configuration area. Below the configuration area is a 'Test Notifier' button.

Connecting to the AutoMate Server

Before you can create an AutoMate notifier, you need to enable the connection to an AutoMate Server. The AutoMate Server must be running on the same machine as the InterMapper Server. For more information see the section on configuring [AutoMate](#) (Pg 293) in the Server Settings.

To configure an AutoMate notifier:

1. From the Notifier Type dropdown menu, choose **AutoMate**. The AutoMate Notifier configuration window appears.
2. Click **Edit Task...** The Notifier Task window appears:



The screenshot shows the 'Notifier Task' configuration window. It has a title bar with a blue background and a red 'X' button. The 'Task Path' is 'My Tasks/My Task' and the 'Task ID' is '{91994F97-0615-40E2-8215-6248A4122A44}'. There is a 'Select Task' button to the right of the Task ID. The 'Run By' section has two radio buttons: 'Path' (unselected) and 'ID' (selected). There is a 'Password' field below the radio buttons. At the bottom right are 'OK' and 'Cancel' buttons.

3. Click **Select Task...** to select from a list of available tasks.

4. In the **Run By** section, choose whether to execute the task by **Path** or **ID**. HelpSystems recommends that you select **ID**, because it reduces the traffic between InterMapper and AutoMate.
5. Enter a **Password** if one is required by the AutoMate task's security configuration.
6. Click **OK**. The task is selected.
7. Set **Retry** and **Consolidation** settings as described below and click **Test** to run the notifier and execute the task.

Note: If a task is disabled in AutoMate, the task still appears in the available task list, but will not run when the notifier is triggered.

Retry and Consolidation Settings

Use the Retry and Consolidation settings to specify when to run or retry a task.

- **Retry limit** - Enter the number of times the task will be re-attempted upon failure. By default, the value is 0, and the task is not re-tried.
- **Retry interval** - Enter the number of seconds between retries.
- **Consolidation limit** - Enter the maximum number of notifications sent before the task is executed. If it is set to 1, a task is executed each time the notification is sent. If it is greater than 1, the task is executed when the number of notifications reaches the Consolidation limit or the Consolidation period is reached.
- **Consolidation period** - Enter the number of seconds to wait for additional notifications before running the task, when the Consolidation limit is non-zero. Once a notification has been sent by the notifier, the task is run when either the Consolidation limit or the Consolidation period is reached.

Note: An AutoMate notifier is not run again until the selected AutoMate task is complete.

Accessing InterMapper Variables in an AutoMate Task

When an AutoMate notifier is run, InterMapper writes data about the triggering device to a CSV file, and grants the AutoMate task access to it. Through this file, AutoMate can access InterMapper variables, which can be used by the task in a wide variety of ways.

In order for AutoMate to access this data from an AutoMate task, the task should include these steps:

1. Wait for exclusive access to InterMapper's CSV file. (A timeout value of 30 seconds is recommended.)
2. Read the CSV file into a dataset.
3. Iterate over the rows of the dataset, gathering the data you need.
4. Delete the CSV file.

A sample task that completes these steps is supplied with InterMapper. The file, called `NotifierTest.aml` can be found at:

```
%Installation Folder%\InterMapper\docs\samples\automate\
```

To run the test task:

1. Drag this file into the AutoMate Task Administrator.
2. Create an Automate notifier.
3. Select the the task to be run by the Automate notifier. The task presents a dialog that displays received values for all of the parameters listed above. Edit the task in the visual editor to see how to access each parameter.

In the AutoMate task editor, you can access these parameters with this syntax:

```
%PARAMETERS.[InterMapper variable name]%
```

Here is a list of available parameters:

- **Notifier:** %PARAMETERS.NOTIFIER% - the name of the notifier.
- **Event:** %PARAMETERS.EVENT% - the type of event that triggered the notifier. (Down, Up, Alarm, Warning, etc.)
- **Name:** %PARAMETERS.NAME% - the first line of the device label.
- **ProbeGroup:** %PARAMETERS.PROBEGROUP% - the name of the probe group (if any) to which the probe that triggered the notifier belongs.
- **MemberProbe:** %PARAMETERS.MEMBERPROBE% - the name of the member probe that triggered the notifier (if the probe is a member of a probe group.)
- **Address:** %PARAMETERS.ADDRESS% - the address of the device.
- **Status:** %PARAMETERS.STATUS% - the status of the device and whether it has been acknowledged.
- **Condition:** %PARAMETERS.CONDITION% - the condition of the device.
- **Previous condition:** %PARAMETERS.PREVCONDITION% - the previous condition of the device.
- **Probe is:** %PARAMETERS.PROBE% - the probe type used for polling.
- **MAC address:** %PARAMETERS.MACADDRESS% - the MAC address of the interface associated with the device's address, if the MAC address can be found using SNMP.
- **SysUptime:** %PARAMETERS.SYSUPTIME% - the amount of time the system has been up.
- **Last down:** %PARAMETERS.LASTDOWN% - the last time the system went down.
- **Time:** %PARAMETERS.TIME% - the time the notifier ran the task.
- **Document:** %PARAMETERS.DOCUMENT% - the name of the document.
- **InterMapper version:** %PARAMETERS.VERSION% - the InterMapper version that was running when the notifier was triggered.
- **SysContact:** %PARAMETERS.SYSCONTACT% - the name of the person responsible for the device (if available).
- **SysLocation:** %PARAMETERS.SYSLOCATION% - the location of the device.
- **Comment:** %PARAMETERS.COMMENT% - a user-defined comment (if any) for the device.
- **Counts** - the total number of devices whose status matches the each of the four specified states below.
 - down:** %PARAMETERS.DOWNCOUNT%
 - critical:** %PARAMETERS.CRITCOUNT%
 - alarm:** %PARAMETERS.ALRMCOUNT%
 - warn:** %PARAMETERS.WARNCOUNT%

- **Acknowledge message:** %PARAMETERS.ACKMESSAGE% - the message entered when the device was last acknowledged
- **Send Counts** - the number of times this notifier has been triggered, and the maximum number that will be sent.
send count: %PARAMETERS.SENDCOUNT%
max: %PARAMETERS.MAXSEND COUNT%
- **Map ID:** %PARAMETERS.MAPID% - the internal InterMapper ID of the map containing the device that triggered the notifier.
- **Device IMID:** %PARAMETERS.DEVICEIMID% - the internal InterMapper ID of the device that triggered the notifier.
- **Param:** %PARAMETERS.PARAM% - the parameters sent to the task.
- **Nickname:** %PARAMETERS.NICKNAME% - also called the "Smart Name". The device's DNS name, SNMP SysName, or address, tried in that order.
- **Shortened nickname:** %PARAMETERS.SHORTNICKNAME% - also called the "Short, Smart Name". The first part of the device's DNS name, SNMP SysName, or address, tried in that order.
- **Persist name:** %PARAMETERS.PERSISTNAME% - the device's domain name.
- **Short name:** %PARAMETERS.SHORTNAME% - the first label of the device's domain name.
- **SystDescr:** %PARAMETERS.SYSDSCR% - the description of the device and its software as reported by the `sysDescr` variable.
- **SysName:** %PARAMETERS.SYSNAME% - the name of the device as reported by the `sysName` variable.
- **Enterprise ID:** %PARAMETERS.ENTERPRISEID% - the enterprise ID of the device as reported by the `EnterpriseID` variable.
- **Enterprise serial:** %PARAMETERS.ENTSERIALNUM% - the serial number of the device as reported by the `EntSerialNum` variable.
- **Enterprise manuf name:** %PARAMETERS.ENTMFGNAME% - the manufacturer name of the device as reported by the `EntMfgName` variable.
- **Enterprise model name:** %PARAMETERS.ENTMODELNAME% - the model name of the device as reported by the `EntModelName` variable.
- **Context:** %PARAMETERS.CONTEXT% - an internal context description (could include IMID of the device, alarm point, current time, notifier type, notifier IMID, event time, event status, send count).
- **Port Name** - %PARAMETERS.IFPORTNAME% - the name of the port that triggered the notifier.
- **Port Number** - %PARAMETERS.IFPORTNUM% - the number of the interface that triggered the notifier.
- **Interface Name** - %PARAMETERS.IFNAME% - the name of the interface that triggered the notifier.
- **Interface Index** - %PARAMETERS.IFINDEX% - the index of the interface that triggered the notifier.

PowerShell Notifier

Use the Powershell notifier to execute a PowerShell script when a device meets specified conditions.

Note: Before you can run a PowerShell Notifier, you must [configure PowerShell to work with InterMapper \(Pg 97\)](#) on the local machine and any target machines you want to access with PowerShell. Use PowerShell probes to test the connectivity.

To configure a PowerShell notifier:

1. Enter a notifier **Name**.
2. From the Notifier Type dropdown menu, choose **PowerShell**. The PowerShell Notifier configuration window appears as shown below.
3. Choose whether you want to execute the script on the local machine (localhost) or a remote machine.
4. In the **PowerShell arguments** box, enter the arguments you want to use define how the PowerShell process executes. See below for more information.
5. In the **PowerShell command text** box, enter the command you want to execute. See below for more information.

PowerShell Notifier Settings

- **Execution** - Choose how the script or command is executed:
 - Local** - the PowerShell command text is executed on the local machine.
 - Alerting Device** - Powershell uses the selected **Authentication** method to connect to the machine that triggered the alert, and executes the specified command text.
 - Other Device** - Powershell uses the selected **Authentication** method to connect to the machine specified in the **ComputerName** box, and executes the specified command text.
- **User** - For **Local** execution, leave this blank unless you want to pass credentials to your script, (for example, to use Get-WmiObject). For **Remote** execution, use the credentials of a valid administrator on the remote computer. For networks that do not use a domain controller, a notifier must be created for each unique administrator.
- **Password** - enter the password associated with the supplied user name.
- **PowerShell Arguments** - enter the arguments to be passed to the PowerShell command. These are command line arguments used when launching PowerShell; they control how PowerShell executes, and are not sent to your PowerShell script.
- **PowerShell Command Text** - enter the text of the command to be executed. These are the commands that PowerShell runs when the notifier is triggered.

Notes:

- The **PowerShell Command Text** box is limited to 255 characters. Typically it is used to execute an existing script in a file.

- Parameters to the command are passed through STDIN, and thus are not bound by the character limit. If you encounter the limit, you can use message variables as arguments, including sending the entire contents of the notifier message as an argument ("\${MESSAGE}"). If you choose to use one of these variables, be sure to enclose it in quotes, in case it contains whitespace.
- Relative paths to PowerShell scripts must be relative to the InterMapper Settings\Tools folder.
- You can create additional folders hierarchy within the Tools folder if you find it useful.
- In the Command Text box, the path to the Tools folder is `"/yourscript.ps1"`. PowerShell also accepts a backslash, but it must be escaped: `".\\yourscript.ps1."`
- Signed scripts must be run from the InterMapper Settings\Tools folder or in a folder it contains.

Available Variables

You can use many InterMapper variables, including `${address}`, `${User}`, `${Password*}`, as well as any of the other information available to Command-Line notifiers.

Choosing an Execution Method

Three methods of execution are available. Each one determines how the script will be executed, and what device it is executed on.

- **Local** - the PowerShell command text is executed on the local machine.
- **Alerting Device** - Powershell uses the selected **Authentication** method to connect to the machine that triggered the alert, and executes the specified command text.
- **Other Device** - Powershell uses the selected **Authentication** method to connect to the machine specified in the **ComputerName** box, and executes the specified command text.

Default Command Text

When you choose an execution method, the **PowerShell command text** box is preloaded an appropriate command.

Here are the defaults for each execution method:

- **Local**

```
./MyPowerShellNotifier.ps1 "${MESSAGE}"
```

- **Alerting Device**

```
Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList  
"${MESSAGE}"
```

- **Other Device**

```
Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList
"${MESSAGE}"
```

Change the name of the **.ps1** script and change or add parameters as needed.

Execution: Local Device

The specified command text is executed on the local machine.

The screenshot shows the configuration window for a PowerShell Notifier. The 'Name' field is 'MyPowerShellNotifier-local'. The 'Type' is 'PowerShell'. Under 'Execution', the 'Local' radio button is selected. The 'User' is 'Fred', 'Password' is masked with dots, 'ComputerName' is '\${address}', and 'Authentication' is 'Default'. The 'PowerShell arguments' field contains '-ExecutionPolicy RemoteSigned -NoProfile'. The 'PowerShell command text' field contains './MyPowerShellNotifier.ps1 "\${MESSAGE}"'. There is an 'Edit Message...' button at the bottom right.

Execution: Alerting Device

The specified command text is executed on the machine that triggered the alert.

The screenshot shows the configuration window for a PowerShell Notifier. The 'Name' field is 'MyPowerShellNotifier-Alerting'. The 'Type' is 'PowerShell'. Under 'Execution', the 'Alerting Device' radio button is selected. The 'User' is 'Fred', 'Password' is masked with dots, 'ComputerName' is '\${address}', and 'Authentication' is 'Default'. The 'PowerShell arguments' field contains '-ExecutionPolicy RemoteSigned -NoProfile'. The 'PowerShell command text' field contains 'Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList'. There is an 'Edit Message...' button at the bottom right.

Execution: Other Device

The specified command text is executed on the machine specified in the **ComputerName** box.

The screenshot shows a configuration window for a PowerShell Notifier. At the top, the 'Name' field is set to 'MyPowerShellNotifier-Other'. Below it, the 'Type' is set to 'PowerShell'. Under the 'Execution' section, three radio buttons are present: 'Local', 'Alerting Device', and 'Other Device', with 'Other Device' being selected. The 'User' field contains 'Fred', the 'Password' field is masked with dots, and the 'ComputerName' field contains '\${address}'. The 'Authentication' dropdown is set to 'Default'. Below these fields, there are two text boxes: 'PowerShell arguments:' containing '-ExecutionPolicy RemoteSigned -NoProfile' and 'PowerShell command text:' containing 'Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList'. An 'Edit Message...' button is located at the bottom right of the configuration area.

Name: MyPowerShellNotifier-Other

Type: PowerShell

Execution: ☐ Local ☐ Alerting Device ☒ Other Device

User: Fred

Password: ••••••

ComputerName: \${address}

Authentication: Default

PowerShell arguments:
-ExecutionPolicy RemoteSigned -NoProfile

PowerShell command text:
Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList

Edit Message...

The Dartware MIB

HelpSystems, LLC has registered the Enterprise 6306 for its own SNMP variables.
The remainder of this page shows the Dartware MIB in ASN.1 notation.

```

-- *****
-- DARTWARE-MIB for InterMapper and other products
--
-- May 2007
--
-- Copyright© HelpSystems, LLC
-- All rights reserved.
-- *****

DARTWARE-MIB DEFINITIONS ::= BEGIN

    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, enterprises
            FROM SNMPv2-SMI
        DisplayString
            FROM SNMPv2-TC;

    dartware MODULE-IDENTITY
        LAST-UPDATED "200507270000Z"
        ORGANIZATION "Dartware, LLC"
        CONTACT-INFO "Dartware, LLC
            Customer Service

            Postal: PO Box 130
            Hanover, NH 03755-0130
            USA

            Tel: +1 603 643-9600

            E-mail: support@dartware.com"

        DESCRIPTION
            "This MIB module defines objects for SNMP traps sent by Inter-
            Mapper."

        REVISION "200705300000Z"
        DESCRIPTION
            "Updated descriptions to show timestamp format, correct strings
            for intermapperMessage."

        REVISION "200512150000Z"
        DESCRIPTION
            "Added intermapperDeviceAddress and intermapperProbeType."

        REVISION "200507270000Z"
        DESCRIPTION
            "First version of MIB in SMIV2."

        ::= { enterprises 6306 }

    notify    OBJECT IDENTIFIER ::= { dartware 2 }

```

```
intermapper OBJECT IDENTIFIER ::= { notify 1 }

intermapperTimestamp OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The current date and time, as a string, in the format 'mm/dd
hh:mm:ss'."
    ::= { intermapper 1 }

intermapperMessage OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The type of event - Down, Up, Critical, Alarm, Warning, OK,
or Trap - as a string."
    ::= { intermapper 2 }

intermapperDeviceName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The (first line of the) label of the device as shown on a
map, as a string."
    ::= { intermapper 3 }

intermapperCondition OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The condition of the device, as it would be printed in the
log file."
    ::= { intermapper 4 }

intermapperDeviceAddress OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The device's network address, as a string."
    ::= { intermapper 5 }

intermapperProbeType OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
```

```
DESCRIPTION
    "The device's probe type, as a human-readable string."
 ::= { intermapper 6 }

-- For SMIV2, map the TRAP-TYPE macro to the
-- corresponding NOTIFICATION-TYPE macro:
--
-- intermapperTrap TRAP-TYPE
--     ENTERPRISE    dartware
--     VARIABLES     { intermapperTimestamp, intermapperMessage,
--                     intermapperDeviceName, intermapperCondition }
--     DESCRIPTION
--         "The SNMP trap that is generated by InterMapper as a
notification option."
--     ::= 1

intermapperNotifications OBJECT IDENTIFIER ::= { intermapper 0 }

intermapperTrap NOTIFICATION-TYPE
    OBJECTS { intermapperTimestamp, intermapperMessage,
              intermapperDeviceName, intermapperCondition,
              intermapperDeviceAddress, intermapperProbeType }
    STATUS current
    DESCRIPTION
        "The SNMP trap that is generated by InterMapper as a noti-
fication option."
    ::= { intermapperNotifications 1 }

END
```

Chapter 7

Monitoring Your Network

Once you have arranged your map, you can switch it to monitor mode. You may already have noticed that devices were changing colors while you were arranging the map. This shows that *InterMapper* was already polling devices, even as you were editing the map's layout.

Making the Map Editable

To change a map between Monitor mode and Edit mode:

- Click the lock button at the left end of the toolbar in the Map window, or press **Tab** as a keyboard shortcut. The tool switches between locked and unlocked as shown.

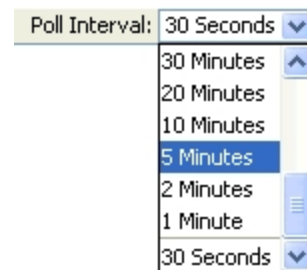
Changing the Poll Interval

The **Poll Interval** drop-down menu sets the polling interval for the map.

To change the Poll Interval:

- Choose a value from the **Poll Interval** drop-down menu.

Note: You can also change the poll interval for one or more individual devices, using the [Set Poll Interval](#) (Pg 400) command, available from the Monitor menu. The map's poll interval value affects only those devices that are using the default poll interval.



Zooming In On the Map

The Map Zoom drop-down menu sets the zoom factor for the map. If you choose **Auto**, the map zooms automatically when you resize the window.

To change the Map Zoom setting:

- Choose a value from the **Map Zoom** drop-down menu.



Understanding the Map

InterMapper provides visual cues to help you understand the states of the devices on your map quickly. Here is a summary of the visual indicators available in your map:

- [Color Codes](#) (Pg 181)
- [Status Badges](#) (Pg 181)
- [Dotted lines \(or "moving ants"\)](#) (Pg 182)
- [Boxes and Ovals \(or "bubbles"\)](#) (Pg 182)
- [Line Styles](#) (Pg 183)
- [Link States](#) (Pg 183)

Color Codes

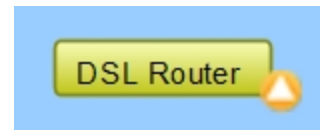
Devices turn different colors depending on the magnitude of the problem detected. Links may be "haloed" with yellow or orange as utilization reaches 50 and 90 percent respectively. These are coupled with status badges, described below.












These are the default color assignments. You can redefine the colors from the [Server Settings](#) (Pg 265) window.

Status Badges

InterMapper uses status badges as additional visual cues to increase the ease with which you can determine the status of one among many device or links.

Note: You can specify which badges you want appear on devices from the [InterMapper User Preferences](#) window.



Badge	Color	Meaning
	Red (Flashing)	Down - No response has been received from the device or interface within the specified timeout period.
	Red (Solid)	Critical - The specified threshold for critical state has been met
	Orange	Alarm - The specified threshold for alarm state has been met.
	Yellow	Warning - The specified threshold for warning state has been met.
	Green	Up - The device is working below the specified thresholds.
	Gray	Unknown - The device is not being polled, so its state is unknown.
	Purple	Searching - The device is searching for adjacent routers (during auto-discovery) or is tracking down unnumbered interfaces.
	Clock	Acknowledge - Timed - The device or link's problem has been acknowledged and notifications are being suppressed for a specified period of time.
	Wrench	Acknowledge - Timed or Indefinite - The device or link's problem has been acknowledged and notifications are being suppressed indefinitely.
	Check mark (devices)	Acknowledge - Basic - The device or link's problem has been acknowledged, and notifications are being suppressed until the device or link comes back up, at which time the check mark or X is cleared.
	Blue X (links)	

Dotted lines (or "moving ants")

InterMapper draws dotted lines ("ants") next to a link to indicate that its current traffic flow is above a user-settable threshold value. Use the **Thresholds>Traffic** panel of the Map Settings window, available from the **Edit** menu, to change the settings and to view a legend of the different varieties of ants. You see the ants only in Monitor mode (as opposed to Edit mode.) To toggle between the two modes, click lock in the upper left corner or press **Tab**.

InterMapper regularly polls all the visible interfaces for packets, bytes, errors and discards.

Note: InterMapper uses SNMP to query the MIB of SNMP-enabled equipment to compute and display the traffic processed by each interface. Traffic indication appears only for SNMP-enabled devices.










Boxes and ovals (or "bubbles")

The *boxes* represent the physical equipment of your network. The *ovals* represent the networks which link the routers together. The numbers in the bubbles are "network identifiers". For IP networks, the number is the network and the subnet portion of the IP addresses of all devices on it. For example, "192.0.16.0/24" is a network where IP addresses are in the range 192.0.16.0-192.0.16.254, and the subnet mask has 24 bits (it is a Class C network.) This is described in detail in the [Subnet Mask \(Pg 727\)](#) FAQ.

Click and hold on a router or network to see a status window with information about that item. (This only works in "browse" mode -- press **Tab**, or click the lock in the upper left corner to lock it).


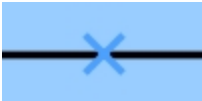
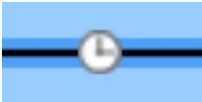

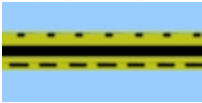
Line styles

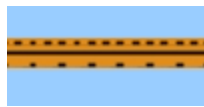
The style of the line corresponds to the type of interface.

	10 Mbit Ethernet
	100 Mbit Ethernet or FDDI
	Serial line - T3 Speed
	Serial line - T1 Speed
	Serial line - 56 K or other
	Frame-Relay Interface Type
	ATM Interface Type
	LocalTalk Interface Type
	Any type not specifically represented

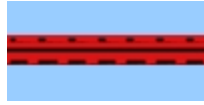
As with the networks and devices, you can click and hold a link to see a Status window, containing information about the interface type and traffic statistics.

Link States

Badge	State	Meaning
	Red X	Link Down - No response has been received from the interface within the specified timeout period.
	Blue X	Basic Acknowledge - The link is down, and has been set to Basic Acknowledge
	Clock, Blue link	Timed Acknowledge - The link is down, and has been set to Timed Acknowledge
	Wrench, Blue link	Indefinite Acknowledge - The link is down, and has been set to Indefinite Acknowledge (Maintenance)
	Yellow link	Warning - The link is working, but has reached one of the specified warning thresholds

**Orange link**

Alarm - The link is working, but has reached one of the specified alarm thresholds

**Red link**

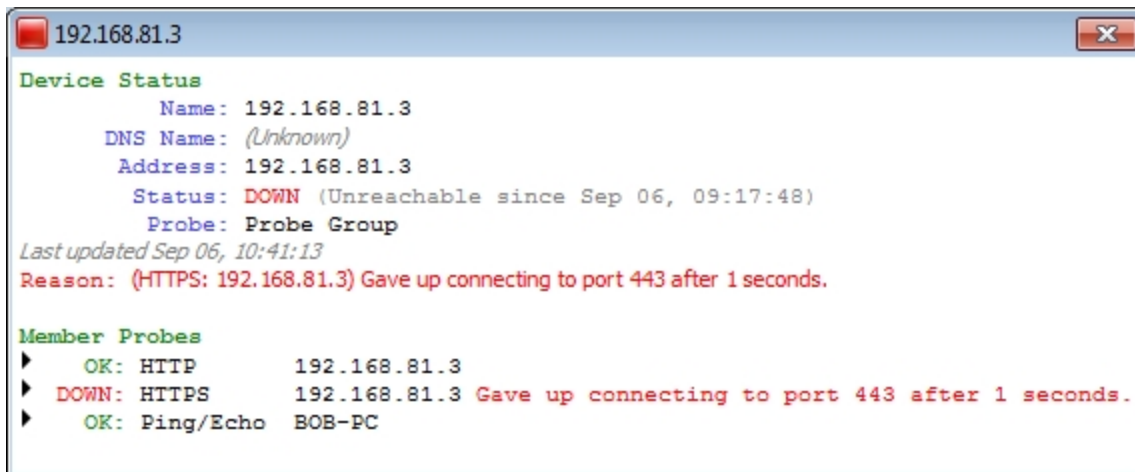
Critical- The link is working, but has reached one of the specified critical thresholds

**Red X in circle**

Admin Down- the device has responded saying that the interface's `ifAdmin` status is set to **Down**.

Viewing Status Windows

InterMapper shows detailed status about any item on a map (a device, a network, or a link) in a Status window, as shown in the Device Status window below.



To view device, network, or link status:

1. Make sure your map is in Monitor mode (click the lock at the upper left of map window to lock the map, or press the **Tab** key.)
2. Click and hold a device, network, or link on the map, or right-click the device, network, or link, then choose **Status Window**. The Status window for the selected device appears.
3. Release the mouse button to hide the Status window.

To keep a Status window open:

1. Make sure your map is in Monitor mode.
2. Click and hold the device, network, or link on the map.
3. Drag to a new location. As you drag, the cursor (Windows) or a transparent window appears.
4. Release the mouse. You have "torn" the window off; it remains open, located where you released the mouse.

Customizing a Status Window

If you are using a custom TCP or SNMP probe, you can override the default contents of a Status window. For more information, see *Custom Probes* and *Customizing Status Windows* in the [Developer Guide](#).

Device Status Window

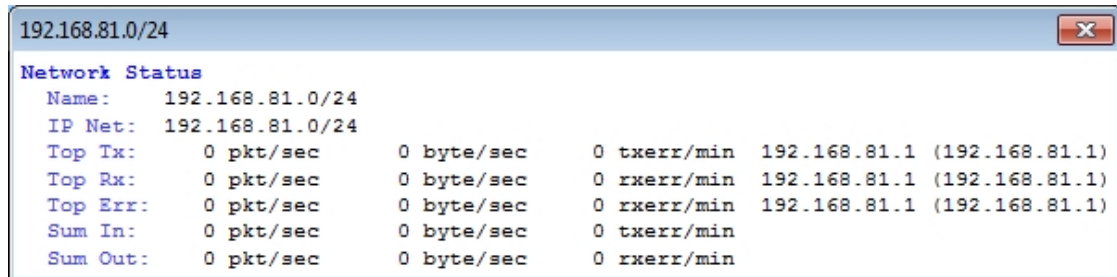
- Click and hold the mouse on a device to open its *device status* window, or right-click the device and choose **Status Window**.
- Click and drag to tear the window off and leave it open.
- Click the underlined Reset link to set Packet Loss to zero. This also resets the device's availability measurement.

Note: The map must be in Edit mode to reset the Packet Loss value.

The window shows the device name, network address, device status, the probe used to poll it, up-time (i.e., SNMP sysUptime, if available), availability (the percentage of the time the device was available based on the number of packets lost while testing), round-trip time (in msec), and spanning tree status (if available).

When the device reports a problem, the reason for the most important error is shown in red at the bottom of the Status window.

Network Status Window



- Click and hold the mouse on a network oval to open its *network status* window, or right-click the network and choose **Status Window..**
- Click and drag to tear the window off and leave it open.

The *network status* window shows the network's IP address and subnet mask, (if available) and information about the amount of traffic flowing on that network segment. This data comes from all the SNMP devices attached to that network oval.

- **Top Tx** - tells which device is transmitting the most data
- **Top Rx** - tells which device is receiving the most data
- **Top Err** - tells which device is reporting the highest error rate for the link
- **Sum In/Sum Out** - the sum of all the transmitters and receivers connected to that network.

Note: The traffic statistic shown are only for devices connected to this network that speak SNMP: Ping/Echo, or TCP-based devices (such as HTTP, FTP, etc. probes) do not have this information and are ignored when computing the sums and maximums displayed in the Status Window.

Link Status Window

- Click and hold the mouse on a link, or right click the link and choose **Status Window**. to open its *link status* window.
- Click and drag to tear the window off and leave it open.

The *link status* window shows the link's interface name and description, its type (10 or 100 Mbps, 1.5 Mbps T-1, etc.), its status and up-time, its IP and MAC addresses (when available), traffic statistics (transmitted from and received by the interface), and the time since the last poll.

Backbone Switch: 29	
Interface Status (ifindex = 29)	
Device Name:	Backbone Switch
Description:	29
Type:	100 MBit ethernetCsmacd (MTU=1500)
Status:	up
SNMP Note: ifLastChange.29 >= sysUpTime.0	
MAC Address:	00-1F-28-9B-2C-63
VLAN:	1
Interface Statistics	
Utilization:	0.19 % (of 100 MBit FD bandwidth)
Percent Err:	0.0 % (14221 pkts w/o error)
Transmit Statistics (0.19 % utilization)	
Pkt/Second:	212 (85.6 % multicast)
Byte/Second:	24358 (194864 bps)
Err/Minute:	0 (0 errors)
Disc/Minute:	0 (0 discards)
Percent Err:	0.0 % (12938 pkts w/o error)
Receive Statistics (0.02 % utilization)	
Pkt/Second:	21 (2.26 % multicast)
Byte/Second:	2054 (16437 bps)
Err/Minute:	0 (0 errors)
Disc/Minute:	0 (0 discards)
Percent Err:	0.0 % (1283 pkts w/o error)
Last updated Sep 06, 10:49:01; sample: 1 minute, 0 seconds.	

Tip: Certain devices do not report their link speed accurately in their SNMP responses. This causes InterMapper to report a value which is not actually correct. To work around this, switch the map to Edit mode, then right-click the link and choose **Set Link Speed...** The Set Link Speed window appears, allowing you to set Transmit and Receive speeds.

The Info Window

Use the Info Window, available from the Monitor menu or a device or network context menu, to view and edit information about a selected device or network.

The appearance and content of an info window varies, depending on whether the selected object is a device or network.

- For details on viewing and editing device info, see [The Device Info Window \(Pg 189\)](#).
- For details on viewing and editing network info, see [The Network Info Window \(Pg 193\)](#).

To open an info window:

Click the device or network whose info you want to view and do one of the following:

- Press **Ctrl/Cmd-I** to open the info window.
- From the Monitor menu, choose **Info Window**.

Alternatively, right-click the device or network and choose **Info Window**.

Once the window is open:

- Click the lock icon (lower left) to change the map to Edit mode.
- Click a info section on the left to view or edit that info type.
- Click **Apply** to save your changes.
- Click **OK** to save your changes and close the Info window.

The Device Info Window

Use the Device Info window to view and edit information about a device.

The screenshot shows a window titled "Info for W" with a left sidebar containing tabs: General, SNMP, Probes, Thresholds, Icon, Label, and Advanced. The "General" tab is selected. The main area contains the following fields and sections:

- Address:** 192.168.81.2
- Host Name:** (empty text field)
- Don't change address or name:** (dropdown menu)
- Use as Map's Vantage Point:** (checkbox, currently unchecked)
- Database Information:**
 - IMID:** device.1.5.27
 - Kind:** Unspecified (dropdown menu)
 - Retention Policy:** 24 Hours (dropdown menu)
- Geographical Location:**
 - Latitude:** (empty text field)
 - Longitude:** (empty text field)
- Comment:** (empty text area)

Callouts in the image provide additional context:

- "Select info to edit" points to the left sidebar tabs.
- "Edit info here" points to the main content area.
- "Set this device as the map's vantage point" points to the "Use as Map's Vantage Point" checkbox.
- "Click to change to Edit mode" points to a lock icon at the bottom left.

At the bottom right, there are three buttons: OK, Cancel, and Apply.

To use the device window:

- Click a section on the left to edit that info type.
- Edit the info as described below.
- Click **Apply** to save your changes.
- Click **OK** to save your changes and close the Info window.

General Pane

Use the Device Info window's General pane to edit general information about the device.

Editing General Info

- **Address** - view or edit the device address. This is the address that is used when the device is polled.
- **Host Name** - view or edit the device's host name. This is the host name that is used to resolve the address
- **Resolve** - choose **address to set name**, **name to set address**, or **neither**.
- Select **Use as Map's Vantage Point** to use this network as the map's [Vantage Point \(Pg 136\)](#).
- **IMID** - view InterMappers internal device ID. (This info is read-only.)
- **Kind** - choose from the dropdown menu to specify the type of device.
- **Retention Policy** - choose a Retention Policy to specify how data for this device is saved.
- **Latitude** - set the device's latitude.
- **Longitude** - set the device's longitude.
- **Comment** - enter text in the **Comment** box to add a comment to the device.

SNMP Pane

Use the Info window's SNMP pane to view available SNMP information. This is a read-only pane, so there are no options to edit.

Probes Pane

Use the Device Info window's Probes pane to view and edit the device's probes.

Editing Probe Info

From the Probes pane, you can add and remove probes, and edit a probe's information.

To edit a probe's information:

1. Make the map editable by clicking the Lock icon at lower left.
2. To change the probe, right-click (or Control-click) the probe you want to edit, and choose **Set Probe...** from the context menu. The Set Probe window appears.
3. Choose the probe you want to use and edit the settings as needed.
4. Click **OK** to close the Set Probe window.

To add a probe:

1. Click the plus icon (+) at the bottom of the Probes pane. The Set Probe window appears.
2. Click to choose a probe from the probe list on the left.
3. Edit the probe settings as needed.
4. Click **OK** to close the Set Probe window.

Note: When you add a probe, the device becomes a probe group.

Thresholds Pane

Use the Device Info window's Thresholds pane to view and edit threshold settings for the device.

Editing Threshold Info

1. Open the Info window for the device you want to edit.
2. Make sure the map is in Edit mode.
3. Click **Thresholds** to view the Thresholds pane.
4. Select the **Ignore Outages** check box to suppress alerts for the device when it goes down or comes up.

Note: The **Ignore Outages** check box suppresses alerts only with respect to outages, not to other state changes, thresholds, or to any alerts triggers by probes attached to the device. This is useful if a device such as a laptop or mobile device goes up or down (or leaves the network completely) as part of its normal operation.

5. Clear the **Use Map Defaults** check box.
6. Enter new values in the boxes you want to change.
7. Click Apply to activate the changes without closing the window or **OK** to activate and close the window. The selected device uses the new values.

Icon Pane

Use the Device Info window's Icon pane to change the icon for the device.

Editing Icon Info

To change the device's icon:

1. From the dropdown menu at the top of the pane, choose an icon set.
2. Scroll through the set and choose an icon. You can see what it looks like by clicking on it. You can see what it looks like in different states by clicking the colored buttons below the preview area.
3. When you have found an icon you want to use, click **Apply** to activate the icon without closing the window or **OK** to activate the icon and close the window.

Label Pane

Use the Device Info window's Label pane to edit the device's label.

Editing a Label

A label can contain any combination of text, variables, and JavaScript. For detailed information on editing labels see [Editing Labels \(Pg 106\)](#) and [Dynamic Label and Alert Text \(Pg 108\)](#).

Advanced Pane

Use the Advanced pane to choose the mapping behavior of a device, and whether to collect Layer 2 information.

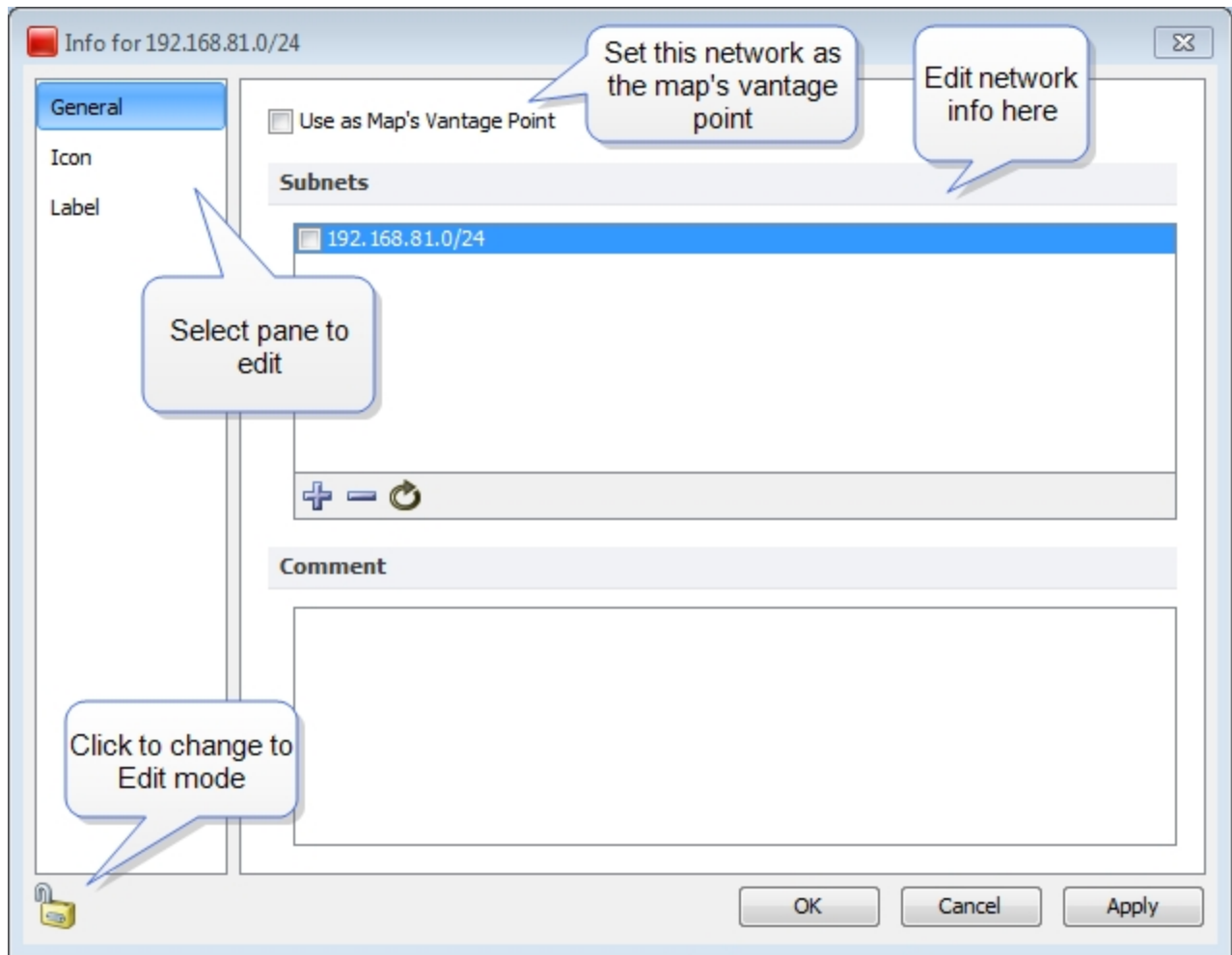
Mapping Behavior

- **Determine network information for each port separately** - use this option when mapping Routers.
- **Propagate all network number information from one port to all ports** - use this option when mapping switches.
- **Do not propagate network information about the ports** - use this option when mapping hubs and end systems.

Layer 2

- **Poll this address for Layer 2 information** - clear this box to prevent this device's IP address from being polled for Layer 2 information. This is equivalent to the **Remove switch from Layer 2 database** command, available when you right-click a switch in the [Layer 2 view's Filter pane](#).
- **Allow Layer 2 connection** - clear this box to prevent InterMapper from making a connection from this device to other devices on the map using Layer 2 information.

The Network Info Window



General Pane

Use the General pane to view a list of subnets that appear on the map, to control which subnets appear, to add and remove subnets, to set the network as the map's Vantage Point, or to add a comment.

- **Add a subnet** - Click plus (+) at the bottom of the General pane to add a subnet.
- **Remove a subnet** - Select a subnet from the Subnets list, and click minus (-) at the bottom of the General pane to remove the subnet from the list and the map.
- **Add a Comment** - enter text in the **Comment** box to add a comment to the network.
- Click **Use as Map's Vantage Point** to use this network as the map's [Vantage Point](#) (Pg 136).
- After making a change, click **Apply** to save the change without closing the Info window. Click **OK** to save the change and close the Info window.

Icon Pane

Use the Network Info window's Icon pane to change the icon that appears on the map for the selected network.

The Icon pane operates exactly as the [Device Info window's Icon pane \(Pg 191\)](#).

Label Pane

Use the Network Info window's Label pane to edit the network's label.

The Label pane operates exactly as the [Device Info window's Label pane \(Pg 191\)](#).

Interfaces Window

InterMapper can show the interfaces of a particular router or switch. This is convenient for viewing the specifics of those interfaces (for example, the Name or ifAlias assigned to each individual port) or for viewing the status of the port.

To view the Interfaces window:

1. Right-click the router or switch for which you want to view the Interfaces Window.
2. From the context menu, choose **Interfaces Window**.

or

- From the Monitor menu, choose **Interfaces Window**.

Note: You may open as many interfaces windows as you like. Each window is updated at the device's poll interval.

The Interfaces Window - Info View

Show	Status	Index	Name	ifAlias	Description	Type	TX Speed	RX Speed	VLAN	Ignore Errors	Ignore Discards	Ignore Utilization
<input checked="" type="checkbox"/>		1	Et1		eth1	ether...	100 M	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		2	Et2		eth2	ether...	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		3	Et3		eth3	ether...	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		4	Et4		eth4	ether...	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		5	ppp0.1		ppp0.1	ppp	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		6	dsl0		dsl0	adsl	700 k	3.36 M	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		7	ATM0		atm0	atm	3.36 M	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Interfaces window - Info View

The Interfaces window displays one row for each port or interface on the device. It shows the following information in columns:

- **Show/Hide Checkbox** - When checked this interface will be visible on the map. Unchecking this box will hide the interface.
- **Status** - The status of the interface as determined by ifAdminStatus and ifOperStatus
 - If the interface has been acknowledged as down indefinitely, a wrench icon appears in this column.
 - If a timed acknowledgement is used, a clock icon appears.
- **Index** - The ifIndex of the interface.
- **Name** - The name assigned to the interface.
- **ifAlias** - The ifAlias assigned to the interface.
- **Description** - The description assigned to the interface.
- **Type** - The type of the interface, as defined in MIB-II.
- **TX Speed** - The Transmit Speed reported by the interface, in bits per second.
- **RX Speed** - User-settable value that is used when InterMapper computes the utilization of the receive side of the interface. If the value is not set, InterMapper uses the TX Speed for the calculation. This is useful when the transmit

and receive speeds are different (for example, in asymmetric DSL links). You can change both the RX Speed and TX speed using the **Set Link Speed...** command, described below.

- **VLAN** - Contains the VLAN ID that has been assigned to the interface (if any).
- **Ignore Errors** - Select or clear this box to choose whether to ignore interface errors.
- **Ignore Discards** - Select or clear this box to choose whether to ignore interface discards.
- **Ignore Utilization** - Select or clear this box to choose whether to ignore interface errors.
- **Display unnumbered interfaces** - Select or clear this box to choose whether to see all the unnumbered interfaces on a switch. By default, *Inter-Mapper* does not display unnumbered interfaces.
- **Allow periodic reprobe** - Select or clear this box to choose whether or not a device is to be automatically reprobbed every 12 hours.

Note: The **Display unnumbered interfaces** and **Allow periodic reprobe** functions are also available from Interfaces menu's Behavior... dialog box, available from both the Monitor menu and context menu. The setting applies a device or to all selected devices.

The Interfaces Window - Statistics View

Status	Index	Name	Total Utilization %	Total Errors/min	Total Discards/min	Tx Utilization %	Tx Errors/min	Tx Discards/min	Rx Utilization %	Rx Err
●	1	Et1	0.01	0	0	0.01	0	0	0.0	
●	2	Et2	0.0	0	0	0.0	0	0	0.0	
●	3	Et3	0.0	0	0	0.0	0	0	0.0	
■	4	Et4	0.0	0	0	0.0	0	0	0.0	
●	5	ppp0.1	0.0	0	0	0.0	0	0	0.0	
●	6	dsl0	0.03	0	0	0.03	0	0	0.0	
✕	7	AT0	0.03	0	0	0.03	0	0	0.0	

☐ Display unnumbered interfaces
 ☒ Allow Periodic Reprobe

Interfaces window - Statistics view

Use the Statistics view of the Interfaces window to see various statistics for all interfaces on a device:

- **Status** - The status of the interface as determined by `ifAdminStatus` and `ifOperStatus`
 - If the interface has been acknowledged as down indefinitely, a wrench icon appears in this column.
 - If a timed acknowledgement is used, a clock icon appears.
- **Index** - The `ifIndex` of the interface.
- **Name** - The name assigned to the interface.
- **Total Utilization %, Errors/min, Discards/min** - the sum of TX and RX utilization, error, and discard statistics for a link.
- **TX and RX Utilization %, Errors/min, Discards/min** - statistics for TX and RX utilization, errors, and discards for the link.

- **Display unnumbered interfaces** - Select or clear this box to choose whether to see all the unnumbered interfaces on a switch. By default, *InterMapper* does not display unnumbered interfaces.
- **Allow periodic reprobe** - Select or clear this box to choose whether or not a device is to be automatically reprobbed every 12 hours.

Hiding and Deleting Interfaces

You can hide interfaces, or you can delete them.

To hide an interface:

- Clear the check box next to the interface. If you hide an interface, a network associated that interface disappears from the map, and remains that way. The interface is no longer polled, and data is no longer collected.

To delete an interface:

- Click the line for the interface you want to delete and press **Delete**.

or

- Right-click the interface line and choose Delete from the context menu.

Hiding vs. Deleting an Interface

Use the following information to help you decide whether you want to hide or delete an interface:

- **Probe rediscovery** - When you *hide* the interface, it does not reappear unless you "unhide" it. When you *delete* an interface, InterMapper rediscovered it and displays it again the next time it re-probes the device unless you clear the **Allow periodic reprobe** check box.
- **Data Collection** - When you *hide* the interface, data collection stops. It starts when you re-enable it. When you *delete* an interface, data collection resumes when the interface is rediscovered.
- **Polling** - When you *hide* the interface, polling for that interface stops. It starts when you re-enable it. When you *delete* an interface, it is polled, and thus reappears when rediscovered.
- **Layer 2 Discovery** - When you *hide* the interface, Layer 2 discovery for that interface stops. It starts when you re-enable it. When you *delete* an interface, the interface is rediscovered, and Layer 2 information is collected.

Acknowledging Down Interfaces

You can acknowledge one or more down interfaces from the Interfaces window.

To acknowledge down interfaces:

1. In the Interfaces window, select the rows for the interfaces you want to acknowledge.
2. Right-click one of the selected interfaces and choose Acknowledge... The Acknowledge window appears.
3. Create an acknowledgement as described in [Acknowledging Device Problems](#).

Copying Data from the Interfaces Window

You can copy data from the Interfaces window for use in spreadsheet or other application.

To copy data from the Interfaces window:

1. Select the rows you want to copy. Shift-click to select contiguous rows, Ctrl-click to select non-contiguous rows.
2. Press **Ctrl/Cmd-C**. The selected rows are copied to the clipboard in tab-delimited format.

Setting the Data Retention Policy for an Interface

You can set the retention policy for an interface from the Interfaces window.

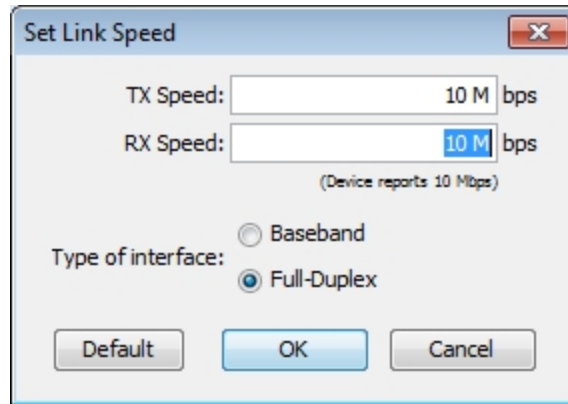
To set the retention policy for a particular interface:

1. Right-click the interface and choose **Set Data Retention** from the context menu.
The Set Retention Policy window appears.
2. Choose a retention policy from the **Data Retention Policy** dropdown menu.
Data is collected as specified by the selected policy.

Setting the Link Speed

With the map editable, use the Set Link Speed window to set the TX Speed and RX Speed for a particular interface. There are two ways to open the Set Link Speed window:

- Right-click the link, and choose **Set Link Speed...** from the context menu.
- From the Interfaces Window, right-click the Interface whose speed you want to set, and choose **Set Link Speed...** from the context menu.



The following units are permitted:

- K (Kilo), M (Mega), G (Giga), T (Tera), P (Peta)

These are all valid values:

- 1000000
- 1000 K
- 1M

Note: The **RX Speed** box is disabled when **Type of interface** is set to **Baseband**.

About Packet Loss

InterMapper has the ability to monitor both long-term and short-term packet loss. These are useful for detecting problems in your network.

Long term Packet Loss is measured from the time InterMapper starts testing a device. InterMapper computes this from the total number of pings or SNMP queries sent, and the fraction of those that fail to respond.

Long-term Packet Loss

The Long-term Packet Loss is displayed in the device's Status Window, along with the total number of packets sent and responses received. It is possible to reset this value using the **Reset** link in the device's Status Window.

Short-term Packet Loss

InterMapper measures Short-term Packet Loss by counting the number of lost packets in the last 100 sent. To do this, each device retains the history of the last 100 packets sent/received.

The short-term packet loss is displayed in the device's Status Window as a percentage of the number of dropped packets in the last 100. This value can be reset via the **Reset** link in the Status Window(which resets all the device's statistics), or by selecting one or more devices and choosing **Monitor -> Reset Short-term Packet Loss**.

Packet Loss Notifiers

InterMapper can send alerts/notifiers when the short term packet loss statistics exceed certain thresholds. That is, when short term packet loss exceeds a warning, alarm, or critical threshold, the device will turn to the appropriate color and InterMapper will send the appropriate alert. These thresholds can be set in several places:

- **Server Settings** - Device Thresholds apply to all devices on all maps
- **Map Settings** - Device Thresholds apply to all the devices on a particular map, overriding the Server Settings value.
- **Individual device - Set Thresholds...** sets the thresholds for that particular device, overriding the map-wide or server-wide settings.

To disable alerts/notifications for high packet loss, set the packet loss thresholds to 100%.

Ignoring lost packets during outages

When a device goes down, InterMapper stops updating the packet loss history (both short and long term) for the duration of the outage. This prevents the packet loss statistics from continuing to increase during an outage. (If InterMapper continued to count lost packets while a device was down, the statistics would incorrectly indicate there was high packet loss when it was likely the problem was something else.)

In addition, InterMapper ignores the packets lost when determining that a device has gone down. For example, the default is that three successive lost packets will indicate that the device is down (no longer responding). However, these three dropped packets would be shown (incorrectly) as a 3% packet loss. Consequently, InterMapper removes those dropped packets from the history, so that it shows an accurate accounting.

When the device subsequently responds (after the problem has been corrected), InterMapper begins counting successful and lost packet responses again.

Acknowledging Device & Link Problems

Use the Acknowledge command, available from the Monitor Menu, to acknowledge failures or problems in the network. When you acknowledge a problem, the Inter-Mapper program does the following:

- Changes the device's icon or link color to blue to show that the problem has been acknowledged.
- Stops further notifications of the problem, either for the duration of this outage, or for a specified time period.
- Writes any comment you enter into to the Event Log file, along with the name and IP address of the user who acknowledged the problem.
- Displays the comment in the device or link's Status Window.

Why are Acknowledgment useful?

Acknowledgments allow the network administrator to see the state of the network, as well as the responses that have been made to the current set of problems.

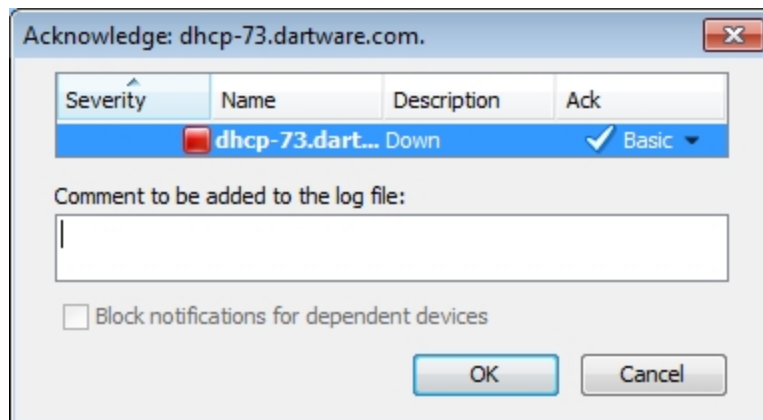
Use Acknowledgements to:

- **Indicate that someone has taken responsibility for a problem** - Because acknowledging a problem turns the affected device's icon blue, it's easy to see that someone is aware of (and is presumably working on) the problem.
- **Emphasize new problems** - The normal color of icons on a map should be green (operating correctly) or blue (having trouble, but being worked on.) When a new problem occurs, the affected devices' color are red, orange or yellow, depending on the severity. This makes it easy to see where new troubles lie. After acknowledgment, these devices will also be blue.
- **Suppress notification for a problem device** - When a device has been acknowledged, no further notifications are sent.
- **Provide information about the problem and its management** - Enter a comment to convey information about the failure, and/or the corrective action.

Acknowledging a problem

To acknowledge a problem with a device:

1. For devices, click or Right-click (or Ctrl-click) the device(s) you want to acknowledge. For interfaces, Right-click (or Ctrl-click) the



link.

2. From the Monitor menu or Context menu, choose **Acknowledge...** (Cmd-' or Ctrl-'). The Acknowledge window appears.
3. If you want keep the device or link in Acknowledgment mode for a specific period of time, or for an indefinite period, choose **Indefinite** or **Timed...** in the **Ack** column.
4. If you want to suppress notifications for devices that depend on this device, click to select the **Block notifications for dependent devices** check box.
5. Enter a comment, then click **Acknowledge**. The selected device's icon changes to blue, and your comment is written to the Event Log file. Notifications are cancelled for the selected device for the duration of this outage.

Basic, Timed and Indefinite Acknowledgments

InterMapper offers three kinds of acknowledgments for devices:

Basic

The device or link is acknowledged, and notifications are suppressed until it gets better or worse. The device icon or link turns blue to indicate that someone has taken responsibility for it, and that no further notifications will be sent.

As soon as the device or link state changes to any other status, its acknowledge status is automatically cleared, and notifications resume. From then on, notifications are sent for any subsequent failures.



Down, with Basic Acknowledgment



Link, with Basic Acknowledgment

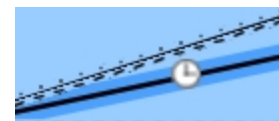
Timed

The device or link is acknowledged, and notifications suppressed for the specified period of time. In this case, the state of the device is OK.

The icon or link turns blue if it's not okay, and the clock badge appears to show that notifications are blocked for the specified time.



Up, with Timed Acknowledgment



Link, with Timed Acknowledgment

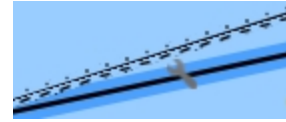
Indefinite

The device or link remains acknowledged until the operator *unacknowledges* it.

As with the **Timed** acknowledgment, the icon turns blue and the wrench badge appears to remind the operator that notifications are suppressed. In this case, the device is DOWN.



Down, with Indefinite Acknowledgment



Link, with Indefinite Acknowledgement

Notes:

- When you acknowledge an interface outage, the interface's link turns blue, rather than the device itself, and an X, wrench, or clock appears on the link, depending on whether it is a Basic, Indefinite, or Timed Acknowledgment.
- With timed and indefinite acknowledge, you can acknowledge a device even when it is up and okay (i.e., green). This is useful if you know that there may be future outages (for example, planned maintenance) with the device, and you want to avoid extraneous notifications. You cannot do this with Basic Acknowledge.
- The presence of the wrench badge is a safety measure. When you scan the map visually, the wrench indicates devices whose notifications are currently being blocked.

Acknowledgements and Dependencies

When you acknowledge a device, use the **Block notifications for dependent devices** check box to specify whether the acknowledged device should be considered in finding dependencies. Checking the box suppresses notifications for any device "on the other side" of the device being acknowledged.

To suppress notifications for all devices that are dependent on the selected device:

- Check the **Block notifications for dependent devices** box. Notifications are suppressed for any device that depends on the selected device.

For more information on dependencies and dependent devices, see [Using Notification Dependencies \(Pg 136\)](#).

Unacknowledging a Device or Link

Use the Unacknowledge command to restore the device to its current notification state.

To remove the acknowledgment for a device:

1. Click to select the device, or choose multiple devices.
2. From the Monitor menu, choose **Un-Acknowledge**. The selected devices are returned to their current notification states, and their notifications are no longer suppressed.

To remove the acknowledgment for a link:

1. Right-click (or Ctrl-click) the link. A context menu appears.
2. From the context menu, choose ***Un-Acknowledge***. The selected link is returned to its current notification state, and notifications for the link are no longer suppressed.

Outage Alarms on Interfaces

InterMapper treats an outage on each device interface as a separate alert event. By default, each time an interface goes down, the affected interface gets a red "X", and alarm notifications for that interface are triggered.

Choosing Alarm Behavior for Interfaces

Use the the **Set devices to Alarm status on down link** check box, available from the [Device Thresholds pane](#) (Pg 269) of the Server Settings window to control the behavior of alarms when an interface goes down.

You can:

- Trigger alarms for individual interfaces
- Trigger an alarm for the device when any interface goes down.

Acknowledging Interface Outages

You can right-click an affected interface's link, and select "Acknowledge". The interface link gets a blue "X", and no further notifications for that interface are sent. InterMapper also writes a line in the Event Log file for these events. The format of the Event Log entries is:

```
09/30 14:03:32 link DOWN : [1] switch.example.com - 1
...
09/30 14:03:49 link ACK : [1] switch.example.com - 1
```

If another interface subsequently goes down, the same process repeats:

- The link gets a red "X".
- An entry is written to the Event Log file
- Notifications are sent
- You can acknowledge the new interface

If two interfaces go down at the same time, a set of alarm notifications is sent for each interface. No further notifications are sent.

Once acknowledged, a link's Status Window show the interface's status as **ACK (down)**.

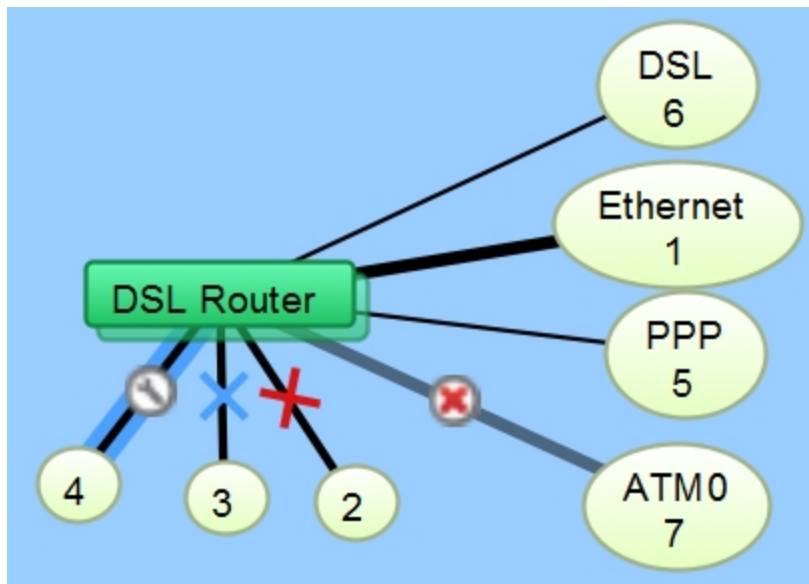
You can acknowledge and unacknowledge multiple interfaces from the device's Interfaces window.

To acknowledge multiple interfaces:

1. Click to select the device.
2. From the Monitor menu, or from the context menu using Right-click (or Ctrl-click), choose Window... from the Interfaces submenu. The interfaces window appears.
3. Click to select one of the interfaces you want to acknowledge.
4. Shift-click or Ctrl-click to choose more interfaces to acknowledge.

5. Right-click (or Ctrl-click) and choose **Acknowledge...** from the context menu.

You can **Un-acknowledge...** one or more links using Right-click (or Ctrl-click) in the same way you acknowledge. This replaces the blue "X" with a red one, and re-enables any repeated notifications for that device.



Various Link States

Note: The red "x" in a circle in the image above shows a link whose status as supplied by the router is `ifAdminDown`. To see all of the available states for devices and links, see [Understanding the Map \(Pg 181\)](#).

Two Approaches for Down Interfaces

- **Acknowledge the interface** as described above. This is good for outages on operational interfaces that are expected to return to service in the near future.
- **Hide the interface** - If you know that an interface will be down for a long time, you can hide it. This tells InterMapper not to monitor its status and removes it from the map to minimize clutter. To show or hide an interface, open the device's Interfaces Window and select or clear the check box in the left column.

Setting Thresholds

You can set a number of thresholds in InterMapper:

- **Devices** - set thresholds for lost packets, interface errors, and short-term packet loss.
- **Interfaces** - set thresholds for interface errors, link utilization, and interface discards.

You can set thresholds as follows:

- **Individual thresholds** for devices and interfaces
- **Server Defaults** for device and interface thresholds
- **Map Defaults** for device and interface thresholds

Device Thresholds

For devices, you can set thresholds for:

- **Number of lost packets** - specify a number of lost packets between 1 and 10 required to set a device to a down state.
- **Interface errors** - specify the number of interface errors-per-minute required to set a device to warning, alarm or critical state.
- **Short-term packet loss** - specify a number of packets out of the last 100 required to set a device to warning, alarm, or critical state. This metric is applicable only to packet-based probes. This statistic can be viewed from the device's status window.
- **Response Time** - specify a response time in milliseconds required to set a device to warning, alarm, or critical state. This statistic can be viewed from the device's status window.

Interface Thresholds

For interfaces, you can set Warning, Alarm, and Critical thresholds for:

- **Errors** - **Rx Errors (Received)** per minute, **Tx Errors (Transmitted)** per minute, and **Total Errors (Rx + Tx)** per minute.
- **Link Utilization** - **Rx Utilization (Received)** percentage, **Tx Utilization (Transmitted)** percentage, and **Total Utilization (Rx + Tx)** percentage.
- **Discards** - **Rx Discards (Received)** per minute, **Tx Discards (Transmitted)** per minute, and **Total Discards (Rx + Tx)** per minute.

As stated above, these statistics can be seen in the device's status window.

Setting Thresholds for Individual Devices

Use the Monitor menu or the device's context menu to set thresholds for a device.

To set thresholds for a device:

1. Right-click (or Ctrl-click) the device and choose **Info Window...** or click to select the device, then choose **Info Window...** from the Monitor menu. The device's Info window appears.
2. In the left pane, click **Thresholds**. The Thresholds panel appears in the right pane.
3. Clear the **Use Map Defaults** check box.
4. Set the thresholds as needed and click **OK**. New thresholds are used to determine the device's status starting with the next poll.

Setting Thresholds for Individual links

There are several ways to set thresholds for interface links:

- Set thresholds for each link separately, using the interface link's context menu.
- Set thresholds for all of the device's links at once, using the device's context menu.
- Set thresholds for some, but not all, of the device's links using the Interfaces window. In this case, use the Interfaces window to select the interfaces whose links you want to set, then use the context menu to set them all at once.

Set Thresholds for a Link

1. Right-click (or Ctrl-click) the link and choose **Interfaces > [the threshold set you want to set]** from the context menu. The link's selected Threshold window appears.
2. Set the thresholds as needed and click **OK**. New thresholds are used to determine the link's status starting with the next poll.

Set Thresholds for All of a Device's Links

1. Right-click (or Ctrl-click) the device and choose **Interfaces > [the threshold set you want to set]** from the context menu
or
Click to select the device, and choose **Interfaces > [the threshold set you want to set]** from the Monitor menu. The selected device's Interface Threshold window appears.
2. Set the thresholds as needed and click **OK**. New thresholds are used to determine the status of all the device's links starting with the next poll.

Set Thresholds for Some of a Device's Links

You can set thresholds for some (but not all) of a device's links. You can also use this method to set thresholds for an individual link.

1. Right-click (or Ctrl-click) the device and choose **Interfaces > Window...** from the context menu. The selected device's Interfaces window appears.

- Click to select the first interface you want to set. The interface line is selected.
- Shift-click (for contiguous lines) or Control-click (for non-contiguous lines) to select additional interfaces you want to set.
- Right-click (or Ctrl-click) the selected interfaces and choose **Interfaces > [the threshold set you want to set]** from the context menu. The Thresholds window appears, showing the values that are common among the links. Any values that are not the same show <mixed>.
- Set the thresholds as needed and click **OK**. New thresholds are used to determine the status of the selected links starting with the next poll.

Viewing and Resolving Conflicts in Threshold Settings

You can set thresholds for several links at once. If you have already set thresholds for one of the links, then select multiple links and open the thresholds window, the conflicting are shown as <<mixed>> as shown:

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	<<mixed>>	<<mixed>>	<<mixed>>	%
Total Utilization (Rx + Tx):	75	85	95	%

Thresholds window showing mixed values

The image above shows that the **Tx Utilization** threshold for one or more of the selected interfaces is different from the others. You can resolve the issue by making the settings the same for the selected interfaces. Hover your mouse over the conflicting value to see the value of the parent device's threshold setting.

Sending Alerts Based On Link Status

Use the same techniques as above to attach notifiers to links, sending alerts based on the status of one, some, or all links on a device.

Attaching a Notifier to a link

- Right-click (or Ctrl-click) the link and choose **Interfaces > Notifiers window** from the context menu. The link's Notifiers window appears, showing a

list of notifiers, with check boxes for each of the link's status levels. If any notifiers are attached to the link, check boxes are selected.

2. Click status level check boxes to indicate which notifiers should be run. When finished, closed the window. Alerts are sent as specified when link thresholds reach the status associated with a notifier's checked box.

Attach a notifier to some or all links on a device

1. Right-click (or Ctrl-click) the device and choose **Interface > Window...** from the device's context menu. The device's Interfaces window appears.
2. Select the interfaces for the links you want to attach notifiers to. Press Ctrl-A (or Cmd-A) to select all. Click a line, then Shift-click or Ctrl-click as described above to select additional interfaces. Then Right-click (or Ctrl-click) and choose **Notifiers Window** from the context menu.
3. If notifiers are attached to any of the device's links, status check boxes are filled for certain status levels.
4. Click status level check boxes to indicate which notifiers should be run. When finished, closed the window. Alerts are sent as specified when thresholds reach the status associated with a notifier's checked box.

Setting Default Thresholds

Set default thresholds for a server or a map. Default thresholds set for a server are applied by default. You can override those settings, and use default thresholds for a map instead. You can also override those thresholds for an individual device or interface.

You can set default device and traffic thresholds for a map. Use the Map Settings window, available from the Edit menu, to set default thresholds.

Setting Default Device Thresholds

Use the **Device Thresholds** section of the Map Settings window to set default device thresholds for a map so that errors for all devices are reported at the same levels.

Set thresholds to alert you to network problems.

☒ Use Server defaults

Down Thresholds

Number of lost packets (1 - 10):

Other Thresholds

	Warning	Alarm	Critical	
Interface errors:	<input type="text" value="2"/>	<input type="text" value="10"/>	<input type="text" value="20"/>	per minute
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/>	of last 100
Response Time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/>	msec

To set the default device thresholds for a map:

1. In an editable map, choose **Map Settings** from the Edit menu. The Map Settings window appears.
2. In the left pane, click **Device**. The default thresholds for the map appear in the right pane.
3. Enter the settings you want to change, and click **OK**. The map uses the new threshold settings.

Setting Default Interface Thresholds

For devices that have multiple interfaces, such as switches and routers, you can also set thresholds for individual interfaces.

Use the **Traffic** section of the Map Settings window to set traffic thresholds for a map. You cannot set traffic thresholds for a specific device.

You can set default interface thresholds for the server, or for an individual map.

- To set defaults for the server, choose **Interface Thresholds** in the Server Settings window.
- To set defaults for the map, choose **Interface Thresholds** in the Map Settings window.

You can set any of the following thresholds:

- **Error thresholds** - set thresholds for Rx Errors (Received), Tx Errors (Transmitted), and Total Errors (Rx + Tx).
- **Utilization thresholds** - set thresholds for Rx Utilization (Received), Tx Utilization (Transmitted), and Total Utilization (Rx + Tx).
- **Discard thresholds** - set thresholds for Rx Discards (Received), Tx Discards (Transmitted), and Total Discards (Rx + Tx).

Setting Thresholds for a Specific Device

You can set device thresholds for a specific device, with different values than the default map settings. You cannot set traffic thresholds for a specific network or link. You do this from the Info window.

Note: When setting thresholds for a probe group, you can set the thresholds only for an individual probe, or use the Map's default settings. For more information, see [Setting Thresholds for Probe Groups \(Pg 213\)](#) below.

Note: Only SNMP probes have thresholds for all three parameters (response time, packet loss and interface errors); a ping/UDP-based probe monitors only response time and packet loss, and a TCP probe monitors only response time.

To set the device thresholds for a specific device:

1. With the map in Edit mode, right-click a device and choose **Info window**, or choose **Info window** from the Monitor menu. The Info window appears.
2. In the left pane of the Info window, click **Thresholds**. The Thresholds pane appears.
3. Clear the **Use Map Defaults** check box.
4. If you want to suppress alerts for the device when it goes down, select the **Ignore Outages** check box.

Note: The **Ignore Outages** check box suppresses alerts only with respect to outages, not to other state changes, thresholds, or to any alerts triggers by probes attached to the device. This is useful if a device such as a laptop or mobile device goes up or down (or leaves the network completely) as part of its normal operation.

5. Enter new values in the boxes you want to change, and click **OK** or **Apply**. The selected device uses the new values.

Setting Thresholds for Probe Groups

When setting thresholds for a probe group, you can set the thresholds only for an individual probe, or use the Map's default settings.

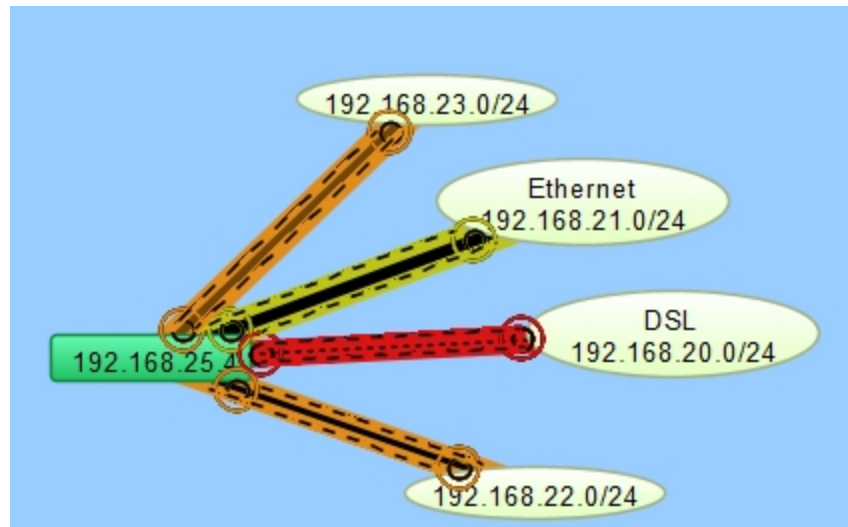
To set thresholds for a probe group:

1. Double-click a probe group. The Info window for the probe group appears.
2. In the left pane of the Info window, click **Probes**. A list of probes in the probe group appears.

3. Right-click (or Ctrl-click) the probe for which you want to set thresholds, and choose **Info Window**. The Info window for the selected probe appears.
4. In the left pane, click **Thresholds**. The threshold settings for the selected probe appear.
5. Clear the **Use Map Defaults** box, then set the thresholds as needed and click **OK**. The thresholds for the selected probe are set.
6. Continue setting thresholds for each probe as needed, then click **OK** in the probe group's Info window.

Setting Traffic Indicators

Use traffic indicators to help you view network activity on a map. You can set the traffic levels at which "moving ants" appear to show you the level and direction of activity on a particular link.



Use the **Traffic** section of the [Map Settings window \(Pg 91\)](#) to turn on and configure traffic indicators for a map. You cannot set traffic indicators for a specific device or link.

Note: Traffic indicators are part of InterMapper's "Animation" feature set. By default, animations are not turned on, as they do require some additional CPU resources. You can turn them on from the Animation Settings pane of the [Preferences window \(Pg 53\)](#).

Sending Feedback

Use the **Send Feedback...** and **Send a Screenshot...** commands, available from the Help menu, to send comments or report bugs. You can also use the Send Feedback window to [submit updates for an existing ticket](#).

Note: If the window appears automatically, you have encountered a client-side bug. (A bug on the server is not visible from the client.) If you have selected the **Automatically E-mail InterMapper bug reports** check box in the Server Preferences > E-mail panel, the server sends bug reports to InterMapper Support when an error is encountered by the InterMapper Server.

To send feedback:

1. From the Help menu choose **Send Feedback...**
The Send Feedback window appears.
2. Enter or edit contact information as needed, and enter a **Subject** for the feedback. This should be a short description of the comment or bug. If you are updating an existing support ticket, you can simply enter the ticket number, and the content of

your feedback submission is added to that ticket. See [To Update an Existing Support Ticket](#) for more information.

Send Feedback

Thank you for sending this information. Please tell us what you wanted to happen, what actually happened, what steps we could take to reproduce it, and any other information you think might be relevant. You will receive an acknowledgement from our tracking system.

After submitting this information, you will be given a chance to quit the program or continue using the application.

Contact Information

Name: Tom Terrific Phone: 603-555-1212

Email: tom.terrific@example.com

Ticket: 113225 Subject:

☐ Include screenshot

Summary System Files Logs

Steps to Reproduce

Here's an update - I was able to reproduce the problem reliably with the following steps:

1. Open a map.
2. (etc.)

Submit Cancel

3. If you are reporting a bug, enter the steps required to reproduce the bug or condition into the **Steps to Reproduce** box. If you are making a comment or suggestion, enter it in the box.
4. If you want to include a screenshot, click **Include screenshot**.
5. To include additional information, click the **System**, **Files**, or **Logs** tab. See additional information below.
6. When ready, click **Submit**.

To send feedback with a screenshot:

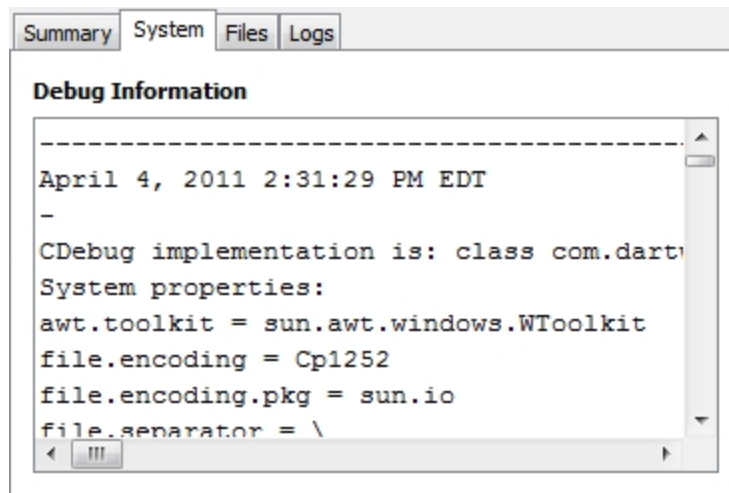
- From the Help menu choose **Send a Screenshot...** The Send Feedback window appears, with a note that a screenshot is included. Enter information as appropriate as described above.

To update an existing support ticket:

1. From the Help menu choose **Send Feedback...** The Send Feedback window appears.
2. Enter the ticket number in the **Ticket** box.
3. Enter additional information in the **Summary** tab, attach additional files on the **Files** tab, or and send additional logs on the **Logs** tab.

System Tab

Use the System tab to view and edit the Debug information that gets sent with the report.



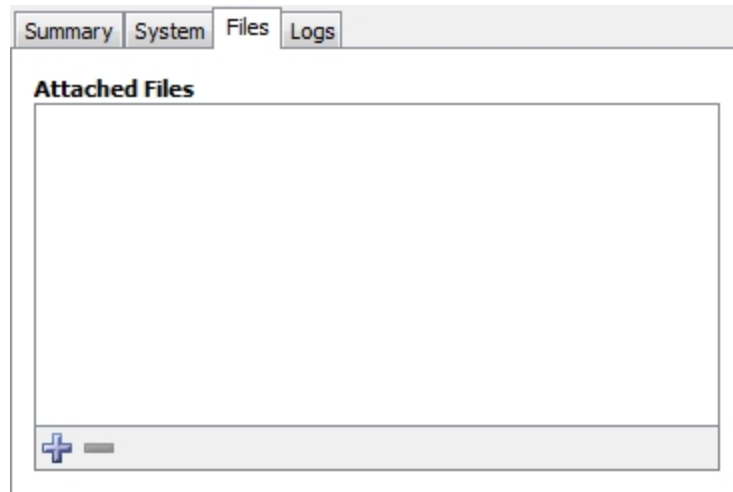
The screenshot shows a web form with four tabs: Summary, System (selected), Files, and Logs. The 'System' tab is active, displaying a text area titled 'Debug Information'. The text area contains the following information:

```
-----  
April 4, 2011 2:31:29 PM EDT  
-  
CDebug implementation is: class com.dart  
System properties:  
awt.toolkit = sun.awt.windows.WToolkit  
file.encoding = Cp1252  
file.encoding.pkg = sun.io  
file.separator = \
```

Files Tab

Use the Files tab to include files with the report.

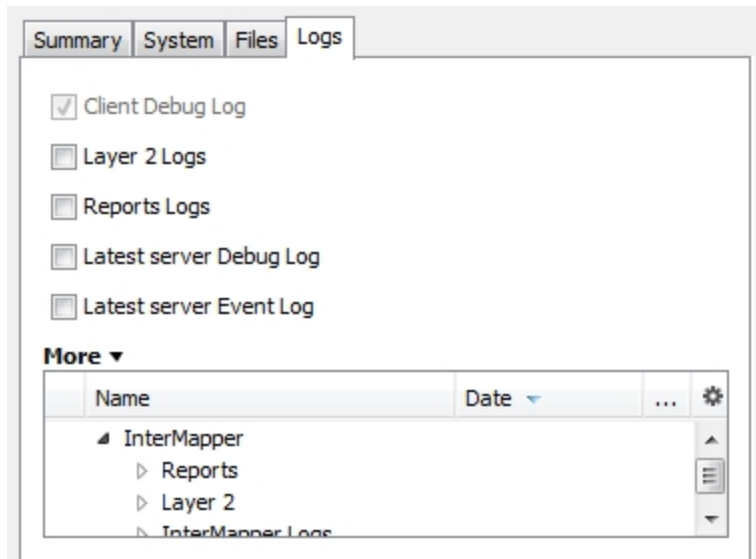
- Click the **Add file** button (plus icon) to add a file to send. The path to the file appears in the Attached Files list.
- To remove a file from the list, click to select a file line in the Attached Files list, and click the **Remove selected file** button (minus icon).



Logs Tab

Use the Logs tab to choose the log files you want to include with the report.

- Select or clear the check boxes to choose the log files you want to send.
- Expand the More list to view additional log files you can choose to send.

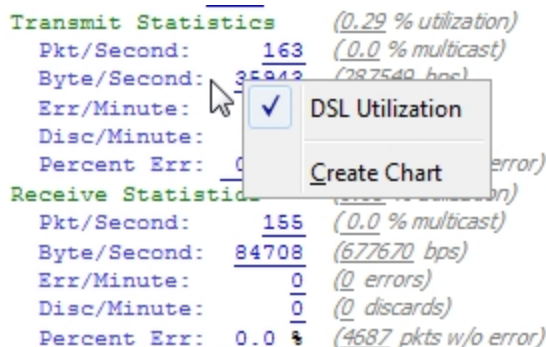


Creating Charts

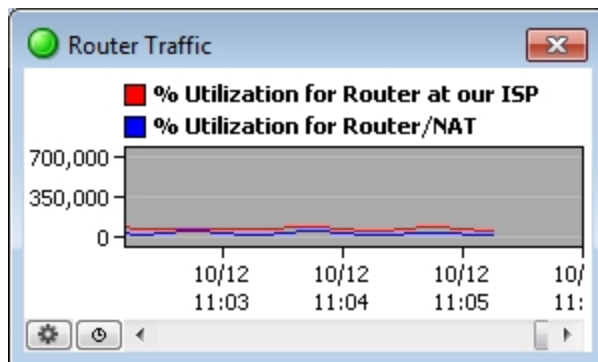
InterMapper charts display the history of one or more variables. This information can also be saved to a log file for further analysis.

To create a chart:

1. Open one of the status windows as described in [Viewing Status Windows \(Pg 185\)](#).
2. Tear the status window off to create a new window.
3. Click on any of the underlined values. If the underlined value appears any existing charts, a list of charts appears, along with a Create Chart option.



4. Click **Create Chart**. A new chart appears.
5. To add more variables to the chart, drag their underlined values to the chart. The example below shows a typical chart.



A chart showing two traces.

For more information about charts, see [Using Charts. \(Pg 220\)](#)

Using Charts

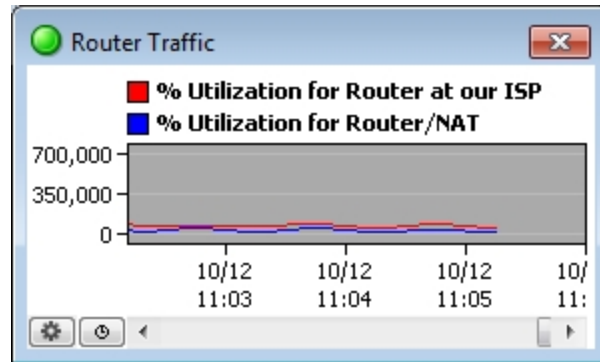
InterMapper displays historical information in a *chart*. Charts can hold an unlimited number of datasets for an unlimited time period. These data can also be written to a tab-delimited text file.

A chart is a persistent window that belongs to a particular map. All the data that is displayed in a chart must come from devices or links of that map.

The figure on the right shows a chart with two variables. You can control its labels, axes, options, and time intervals, as described in the pages of this section.

You use the options available from the [Charts Menu \(Pg 223\)](#) to view and hide charts.

You use the options available from the [Chart Options \(Pg 226\)](#) menu to view and edit the parameters which control content and appearance of each chart.



A chart showing two datasets.

You can also specify the file that logs the chart's data, and control options for creating new chart log files. For more information, see [Chart Log Files \(Pg 232\)](#).

Below is a Quick Start guide for using charts.


Viewing and Hiding Charts

You view and hide charts using the Charts command in the View menu or by selecting options from the [Charts menu at the bottom left of the chart's window](#). (Pg 223).


To show an existing chart:

- From the Windows menu, choose the chart you want to view by selecting it from the **Charts** submenu.

or

- Click the  button in the tool bar to view a list of charts associated with the map. Double-click a chart to view it.

or

- Right/Ctrl-click the  button in the tool bar to view a dropdown menu of charts associated with the map without changing to the Chart List view. Choose a list from the dropdown menu.

or

- Right/Ctrl-click a chart in Chart List view and choose **Show Chart**.

To hide a chart:

- Click the chart's close box. The chart is hidden, but the chart's data is preserved, and continues to be collected.

To scroll the chart:

- Drag the chart's background to scroll the chart right or left.

Creating and Adding Datasets to Charts

To create a chart:

1. Open one of the status windows as described in [Viewing Status Windows \(Pg 185\)](#).
2. Tear the status window off to create a new window.
3. Click on any of the underlined values. If the underlined value appears any existing charts, a list of charts appears, along with a Create Chart option.
4. Click **Create Chart**. A new chart appears.

To add a dataset to an existing chart:

1. Open a Status window.
2. Drag an underlined value (blue or grey) from a status window into the chart. The variable is added to the chart.

Note: To see what device a dataset belongs to, right-click (or Ctrl-click) the dataset's legend in the Chart window, and choose **Show Device**. If you are viewing the Map window in Map view, the device is highlighted momentarily. In List view, the device is selected in the list.

Editing Charts

Edit the parameters that control a chart's content and appearance from the [Chart Options window \(Pg 226\)](#), available from the [Chart menu \(Pg 223\)](#).

Deleting Charts

Use the **Delete Chart...** command, available from the [Chart menu \(Pg 223\)](#) to delete a Chart.

Chart Menus

InterMapper provides three menus you can use to view and edit charts.

The Charts Menu

Use the Charts menu to view and hide charts.

To show all charts:

From the Charts submenu of the Windows menu, choose **Show Charts**. All defined charts for the current map appear.

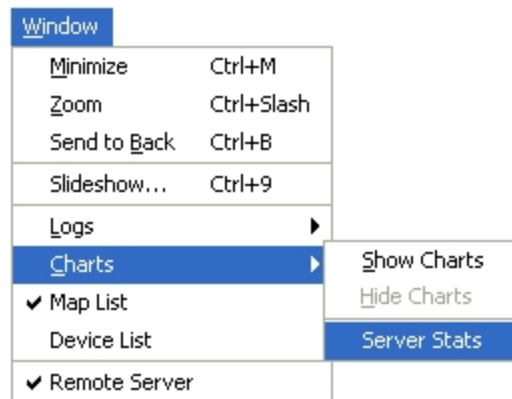
To hide all charts:

From the Charts submenu of the Windows menu, choose **Hide Charts**. All defined charts for the current map disappear.

To view an individual chart:

From the Charts submenu of the Windows menu, choose the chart you want to show. When the chart is visible, a checkmark appears in the submenu next to the chart name, as shown at the right.

Note: From the Charts list window, select one or more charts, then right/Ctrl-click a selected chart line and choose **Show Chart**.



The Charts menu

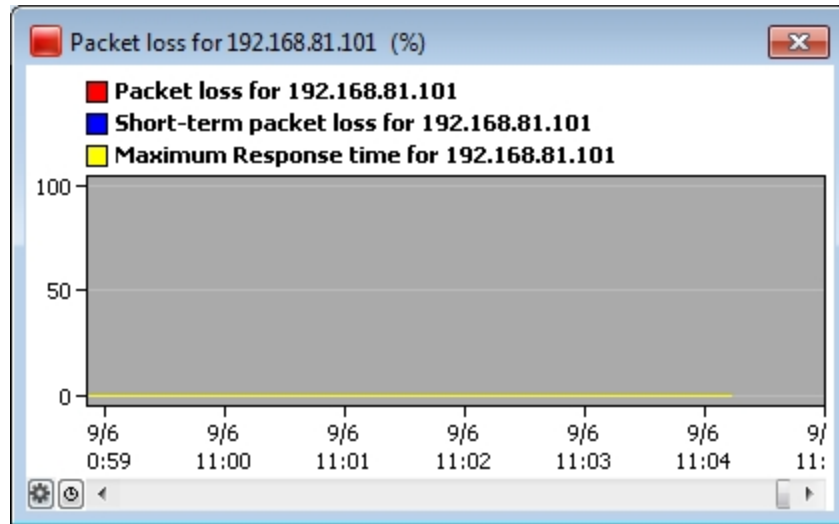
The Chart Menu

To view the Chart menu:

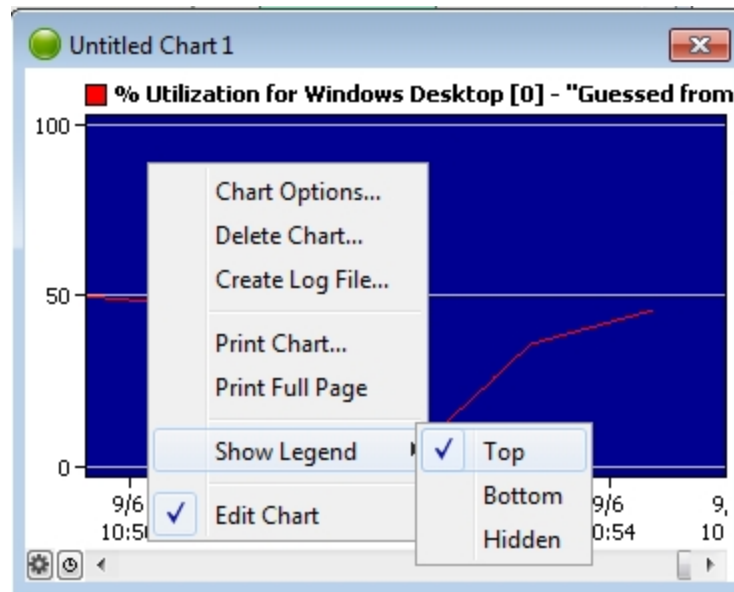
- Click the icon in the lower left to access the Chart dropdown menu.

or

- Right/Ctrl-click in the chart's data area.



The Chart dropdown menu appears.



The Chart dropdown menu.

Chart Options... - Choose this option to view and edit parameters for the current chart. For more information, see [Chart Options \(Pg 226\)](#).

Delete Chart - Choose this option to delete the current chart and its data.

Log File... - Choose this option to create a log file to receive the data for the current chart.

Show Legend - Choose an option from the **Show Legend** submenu to place the chart's legend at the top, bottom, or to hide the legend completely.

Edit Chart - If the map is not in edit mode, this is the only option available. Choose this option to edit the chart and view the Chart dropdown menu.

The Time Interval Menu

Use the Time Interval dropdown menu, located next to the Chart dropdown menu icon at the lower left corner of the Chart window to set the time between the tick marks on the chart's horizontal axis.



Chart Options

Use the Chart Options window to view and edit the parameters that define a chart's appearance and content.

The Chart Options window is available from the [Chart menu \(Pg 223\)](#), or by right-clicking within the chart window.

Applying Changes In the Chart Options Window

Use the Apply button to apply changes to a chart. Here are some things you should know about using the Apply button:

- Click **Apply** to apply changes you have made on any of the tabs, without closing the Chart Options window.
- Click **Cancel** to undo any changes you've made and applied.
- Click **OK** to apply any changes and close the window.
- Close the window to save any changes you've already applied.

Setting the Chart Title

The chart's title appears in the Charts menu and in the chart's title bar. Enter a title in the **Title** box.

Vertical Axis Tab

The screenshot shows the 'Chart Options' dialog box with the 'Vertical Axis' tab selected. The 'Title' field contains 'Packet loss for 192.168.81.101 (%)'. The 'Label' field is empty. The 'Prefix' dropdown is set to an empty state. The 'Upper Bounds' field is '100' and the 'Lower Bounds' field is '0'. The 'Auto-adjust' checkbox is checked. The 'Dividers' spinner is set to '3' and the 'Sub-Dividers' spinner is set to '0'. The 'Scale' section has 'Linear' selected with a radio button and 'Logarithmic' unselected. At the bottom are 'Apply', 'OK', and 'Cancel' buttons.

Vertical Axis Tab parameters

- **Label** - Enter a label for the vertical axis of the chart.
- **Prefix** - Select a prefix for the data displayed in the chart. InterMapper automatically scales the values to match this prefix, and inserts the prefix into the vertical axis label. (example: "volts" would become "μ-volts").
- **Upper Bounds, Lower Bounds** - Enter values to control the vertical scale of the chart. The range of values depends on the variable being monitored.
- **Auto-adjust** - Select or clear the **Auto-adjust** check box to choose whether to allow InterMapper to adjust the scale of the chart automatically. If the **Auto-adjust** check box is checked, the upper and/or lower bounds are adjusted automatically so that data points are always displayed, no matter how much they increase or decrease.
- **Dividers, Sub-Dividers** - Click the up- and down-arrows or enter a number of dividing lines to set the number of horizontal dividers and to set the number of sub-dividers you want to appear between the dividers.

Example: To divide a chart into 10 parts, you'll need eleven dividers. You can do either of the following:

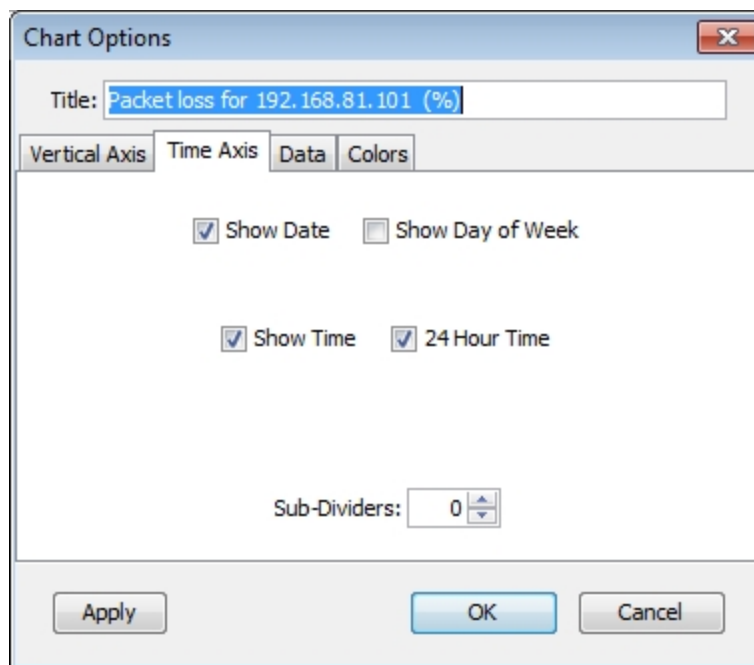
- Set the number of dividers to 11, with no sub-dividers.
- Set the number of dividers to 3, and the sub-dividers between each divider to 4.

- **Scale** - Click to choose **Linear** or **Logarithmic**. scaling of the displayed values. When you choose **Logarithmic** scaling, you can set the Y-axis labels to powers of 10 by setting the desired upper bound and lower bounds, then adjusting the number of dividers to match. A lower bound of zero is converted to 1.

Example: To create a log scale with labels of 3000, 300, 30, and 3:

- Set the upper bound to 3000
- Set the lower bound to 3
- Set the number of dividers to 4

Time Axis Tab

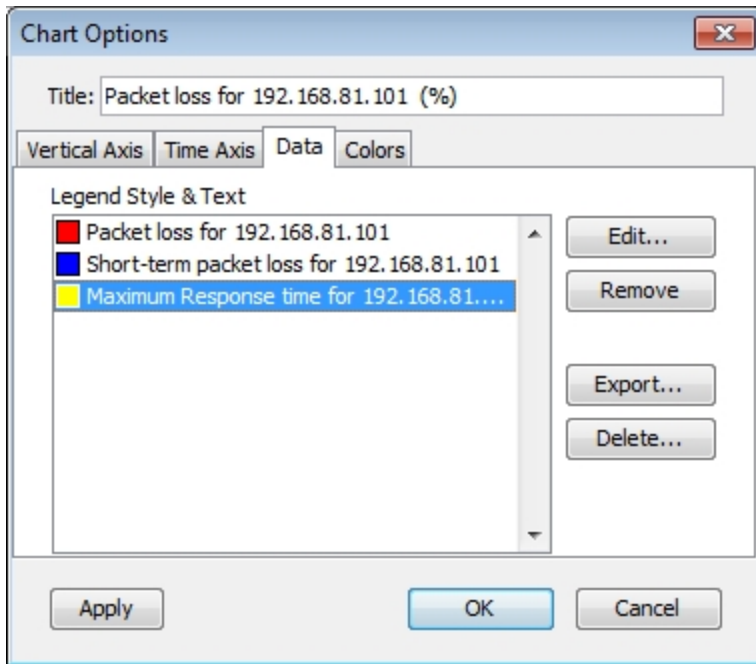


Time Axis Tab parameters

- **Show Date, Show Day of Week, Show Time, 24 Hour Time** - Check or clear these boxes to specify which labels appear on a chart's horizontal axis by default.
- **Sub-Dividers** - Click the up- and down-arrows to specify the number of unlabeled vertical sub-dividers to draw between data points.

Data Tab

The Data tab shows a lists of datasets used in the current chart. Use the Data tab of the Chart Options window to export a dataset, to remove it from the chart, or to edit the appearance of a dataset's legend.



The Data tab of the Chart Options window

To remove a dataset from the chart:

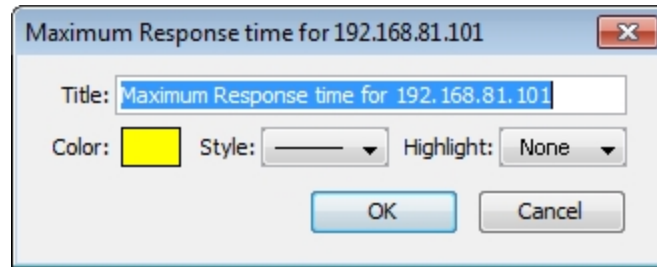
1. In the list of datasets, click the dataset you want to remove from the chart.
2. Click **Remove**. The dataset disappears from the list.

To export a dataset:

1. In the list of datasets, click the dataset you want to export.
2. Click **Export**. A standard file dialog appears.
3. Enter a filename, choose a location, and click **Save**. A tab-delimited text file is created, with one data value per line.

To edit the appearance of the legend for a dataset:

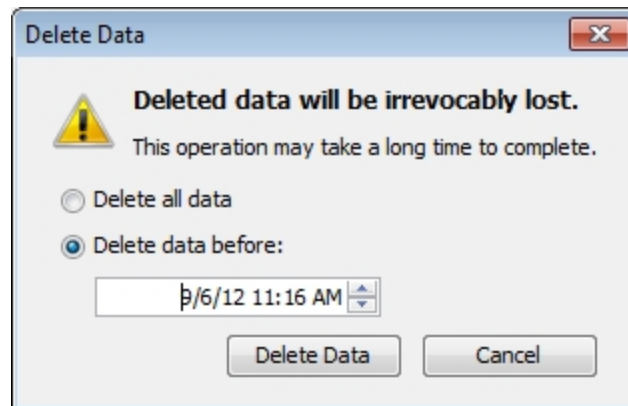
In the list of datasets, double-click the data for the set whose legend you want to edit. The edit window for the dataset's legend appears:



1. Click the **Color** rectangle and choose a color for the dataset.
2. Choose a line style for the dataset from the **Style** drop-down menu.
3. Choose a highlight icon for the dataset from the **Highlight** drop-down menu.
4. Edit the chart's title in the **Title** text box.
5. Click **OK** to save your changes.

To delete a range of data from a dataset:

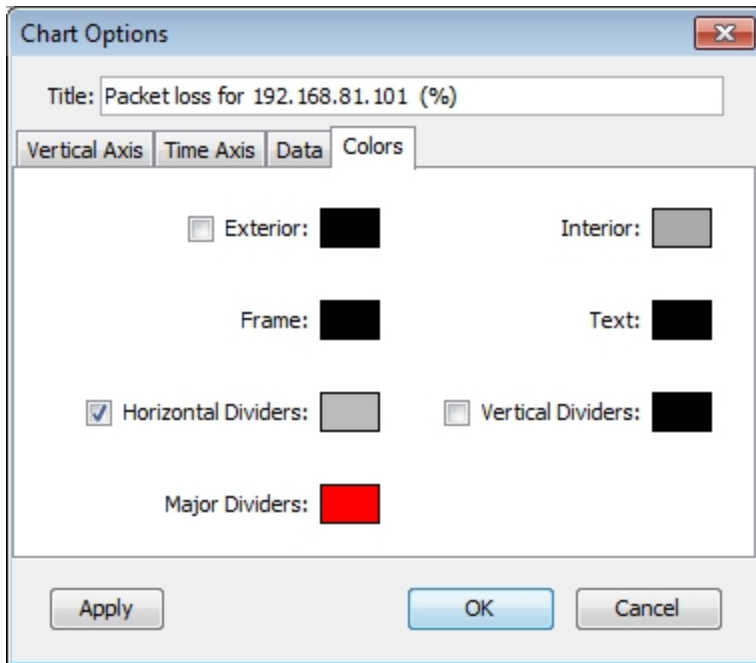
1. In the list of datasets, click to select the dataset containing the data you want to delete.
2. Click **Delete...** The Delete Data window for the dataset appears.



3. Set the date and time. Data before this date and time are deleted from the dataset.
4. Click **OK**. The specified data is deleted from the dataset.

Colors Tab

Use the Colors tab of the Chart Options window to define the colors for various parts of the chart.



- **Exterior** - Click to set the color of the chart's background, outside the data area. Click the check box to use the color.
- **Interior** - Click to set the background color for the data area of the chart.
- **Frame** - Click to set the line color for the frame of the data area.
- **Text** - Click to set the color for the chart's text.
- **Horizontal Dividers** - Click to set the line color for the chart's horizontal dividers. Click the check box to use the color.
- **Vertical Dividers** - Click to set the line color for the chart's vertical dividers. Click the check box to use the color.

To change a color:

- Click a color box in the window above to set the color. Use the system color picker to select a new color.

Chart Log Files

InterMapper can write chart data to a tab-delimited text file. You can specify separate log files for each chart, or you can send the data from several charts to a single log file.

To specify a log file to receive chart data:

1. From the [Chart dropdown menu \(Pg 223\)](#), select **Log file...** The Create Log File window appears, as shown at right.
2. In the **Log File Name** box, enter the name of the new log file.
3. Set the preferences for the new log file using a window similar to the example at the right. For more details creating log files, see [Log Files \(Pg 257\)](#). When finished, click **OK**.

Each line of the tab-delimited file contains a date and time stamp and the current values of the variables defined by the chart.

Specifying a chart log file

To stop logging data to a log file:

1. From the Server Settings window, choose the [Log Files \(Pg 257\)](#) panel of the Server Preferences section. The Log Files panel appears.
2. Click to select the file for which you want to stop logging data.
3. Click **Remove**. The file disappears from the list, and chart data is no longer written to that file.

Purging Chart Data

Use a command line to purge the data stored with charts. You can purge all chart data, or you can specify a number of days of data you want to retain.

Note: before running the purge command, HelpSystems recommends that you back up the InterMapper Settings folder (especially the Chart Data folder.)

To purge chart data:

1. Stop the InterMapper server.
2. Execute the purge command.
3. Start the InterMapper server.

Stopping and starting the InterMapper Server varies depending on your platform.

Purge Command Syntax

For Mac, Unix, and Linux, the command includes the location of the InterMapper daemon configuration file. Here's the syntax those platforms:

```
/usr/local/bin/intermapperd -f /usr/local/etc/intermapperd.conf --  
chart-purge [# of days]
```

For Windows, here is the syntax:

```
"C:\Program Files\InterMapper\InterMapper.exe" --chart-purge [# of  
days]
```

#of days specifies the number of days of chart data to retain, while purging the rest.

Purging all Chart Data

To purge all chart data, use a **# of days** value of 0.

Purge Notes

- **Server must not be running** - The InterMapper Server must not be running when you executed the command.
- **Enabled maps only** - Only charts from devices on enabled maps are purged.
- **Administrative rights and write-access** - You must have administrative rights, and write-access to the InterMapper Settings folder.

Log Windows

InterMapper writes information about interesting events into [log files \(Pg 257\)](#). These streams of information can be viewed in the Log window. This allows you to review log files without the need for an external text editor.

These three logs are pre-defined:

[The Event log \(Pg 235\)](#)

Use this log to view all events generated during the monitoring of devices. It includes events in which a device changes state, reasons for alarm notifications, and many other events.

[The Outages log \(Pg 246\)](#)

Use this log to view a list of devices and networks that have been down, and the times that they came back up.

[The Debug log \(Pg 247\)](#)

Use this log to view a list of detailed debug messages that may be useful for debugging *InterMapper*.

You create and control the preferences for log files from the Log Files panel of the Server Settings window. For more information on creating, viewing, and controlling the events that appear in log files, see [Server Preferences - Log Files. \(Pg 257\)](#)

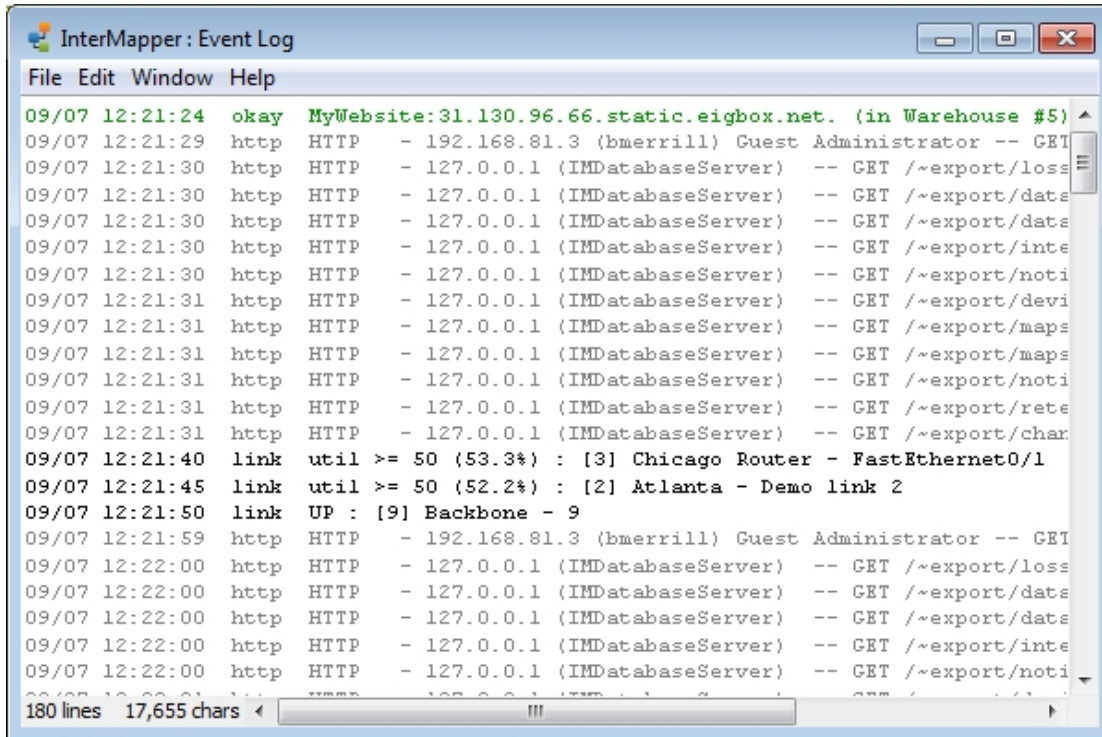
Note: Debug log and Event log are encoded in UTF-8 format. To edit those files, your text editor must support UTF-8 encoding in order to view foreign characters correctly.

The Event Log

InterMapper writes information about interesting events into *event logs*. These streams of information are written to log files on-disk, and can be viewed in one of the Log windows. The Event Log is a pre-defined log file which serves as a default "catch-all" log file.

To open the Event Log window:

- From the Windows Menu, choose **Event Log** from the Logs submenu. The Event Log window appears, as shown below.



The main Event Log window. It can show information about device ups and downs, high traffic on links, web, telnet, and InterMapper RemoteAccess server connections, as well as error messages.

As entries are written to the Event Log file, (stored in the InterMapper Settings/InterMapper Logs" folder) they are also placed at the bottom of this window.

If the window is scrolled to the very bottom of the Event Log, it scrolls automatically as new events are appended to the log.

Event Log Messages

All event log messages have one of these two formats:

Message Format - Devices

<timestamp> <tag> <fullname>:: <message>

The <tag>s are:

```
"UP ": <message> = "(Was down for <duration:3>)"
"DOWN": <message> = "(Was up for <duration:3>)"
"okay": <message> = <threshold-condition>
"warn": <message> = <threshold-condition>
"alm": <message> = <threshold-condition>
"ACK ": <message> = <acknowledge-message>
"UNAC": <message> = ""
"TRAP": <message> = <trap-message>
```

where the <duration:3> can be one of:

- "[0-9]+ seconds?"
- "[0-9]+ minutes?, [0-9]+ seconds?"
- "[0-9]+ hours?, [0-9]+ minutes?, [0-9]+ seconds?"
- "[0-9]+ days?, [0-9]+ hours?, [0-9]+ minutes?"

Message Format - All Other Events

```
<timestamp> <tag> <message>
```


Summary of Log Messages

This page lists all log messages that InterMapper writes to a log, with a description of each. Items shown in *italics* are variable names that are substituted with the proper value when the log message is created.

Note: Debug messages are not documented by Help/Systems, because they are subject to change, and do not follow a specified format.

General Messages

These messages describe InterMapper's actions as it starts up, enables and disables servers, and opens and closes the map files. These messages always go to the Event Log window.

**** Starting *appName*

InterMapper is starting up. This entry contains the program's version number

**** Quitting *appName*

The InterMapper application is quitting.

**** Opening map *docName*

The named map is being opened.

**** Closing map *docName*

The named map is being closed.

http Starting web server on port *portnumber*

InterMapper is starting its web server on port *portnumber*

http Stopping web server on port *portnumber*

InterMapper is stopping the web server

imrm Starting Remote server on port *portnumber*

InterMapper is starting its InterMapper RemoteAccess server on port *portnumber*

imrm Stopping Remote server on port *portnumber*

InterMapper is stopping the InterMapper RemoteAccess server

tlnt Starting telnet server on port *portnumber*

InterMapper is starting its Telnet server on port *portnumber*

tlnt Stopping telnet server on port *portnumber*

InterMapper is stopping the Telnet server

Start-up error: Could not open *porttype* port *portnumber*.

InterMapper could not open the specified port during startup

Error sending udp packet. (Err = *errNumber*)

InterMapper received an error attempting to send a UDP packet

DNS-Related Messages

**** Address Change: "www" changed from x.x.x.x to y.y.y.y. (DNS z.z.z.z)

The Device named www changed its IP address from x.x.x.x to y.y.y.y according to the DNS server at z.z.z.z

**** No IP address for "www". (DNS z.z.z.z)

InterMapper was not able to determine an IP address for the device named www from the DNS server at z.z.z.z

**** Name Change: "w.w.w.w" changed from "xxx" to "yyy". (DNS z.z.z.z)

The IP address w.w.w.w changed its DNS name from xxx to yyy according to the DNS server at z.z.z.z

**** No domain name for x.x.x.x. (DNS z.z.z.z)

InterMapper was not able to determine a DNS name for x.x.x.x from the DNS server at z.z.z.z

**** "No response from DNS x.x.x.x when resolving 'yyy' to an address.

The DNS server at x.x.x.x did not respond when attempting to resolve the DNS name yyy to an address.

**** "No response from DNS x.x.x.x when resolving 'y.y.y.y' to a name.

The DNS server at x.x.x.x did not respond when resolving the address y.y.y.y to a name.

dbug "DNS packet with bad format from y.y.y.y"

InterMapper received a DNS response with an invalid format.

dbug "Error ### while processing DNS reply from y.y.y.y"

InterMapper received an error while processing a DNS response.

**** Connected to > InterMapper DataCenter at 127.0.0.1

InterMapper connected successfully to InterMapper DataCenter

**** Disconnected from > InterMapper DataCenter at 127.0.0.1

InterMapper was disconnected from InterMapper DataCenter

Probe File Error Messages

These messages describe problems with the Custom Probe files. Many of them are self-explanatory.

```
debug "MyProbe: Can't match "MyProbe"", cFileName, lineStr
```

```
debug "xxxx: Invalid Probe ID."
```

The probe xxxx contains an invalid ID (i.e., the package is not a valid string)

```
debug "MyProbe: Invalid Probe Name.", cFileName
```

```
debug "MyProbe: Invalid Probe Human Name.", cFileName
```

```
debug "MyProbe: Probe definition does not contain a valid <description> section.",  
cFileName
```

```
debug "MyProbe: Probe definition does not contain a valid <snmp-device-vari-  
ables> section.", cFileName
```

```
debug "xxxx: Probe definition does not contain a valid <snmp-device-display> sec-  
tion."
```

The xxxx probe file does not contain a valid <snmp-device-display> section.

```
debug "MyProbe: Probe definition does not contain a valid end tag for <MyProbe>.",  
cFileName, endTagStr
```

Telnet Server Messages

**** x.x.x.x denied access to tcp server.

An attempt to connect to the Telnet server from address x.x.x.x was refused.

tlnt TELNET - x.x.x.x denied access.

An attempt to connect to the Telnet server from address x.x.x.x was refused.

tlnt TELNET - x.x.x.x denied access because there are too many connections.

An attempt to connect to the Telnet server from address x.x.x.x was refused because there were too many connections already established.

tlnt TELNET - Accepted connection from x.x.x.x

A user at x.x.x.x successfully connected to the Telnet server.

tlnt TELNET - Accepted user connection from x.x.x.x

Telnet server accepted a user connection from x.x.x.x

tlnt TELNET - x.x.x.x authenticated as "username".

The Telnet server accepted a connection from an authenticated user, "username"

tlnt TELNET - Closed connection from x.x.x.x

The user at address x.x.x.x disconnected from the Telnet server.

Trap-Related Messages

trap "y.y.y.y (not on map) :: text-msg"

InterMapper received a trap from device y.y.y.y containing the *text-msg*

trap "An error occurred while processing a SNMP trap from y.y.y.y. (err = ###)"

InterMapper encountered an error processing a trap from y.y.y.y

Notification Messages

ntfy "Silenced e-mail notification to "username"."

InterMapper suppressed an e-mail notification to the listed user because of the Snooze Alarm

ERR! "Failed to send e-mail notification to "username" for "message: devicename" event. Check e-mail configuration. (err = ###)"

InterMapper was unable to send an e-mail notification to the named person because of the error code ###

ntfy "Sent e-mail notification to "username" for "message: devicename" event. (n of m)"

InterMapper sent an e-mail notification as indicated. The "n of m" indicates that the n'th repeated message has been sent

ntfy "Silenced pager message notification to "username"."

InterMapper suppressed a page to the listed user because of the Snooze Alarm

ERR! "Failed to send pager notification to "username" for "message: devicename". (err = ###)"

InterMapper was unable to send a page to the named person because of the error code ###

ntfy "Sent pager message notification to "MyProbe" for "MyProbe: MyProbe".", itsUserName, eventMesg, deviceName

**** "Silenced sound notification to "MyProbe".", itsUserName

ERR! "Failed to send sound notification to "MyProbe". (err = %d)", itsUserName, err

ntfy "Silenced SNMP trap notification to "MyProbe".", itsUserName

ERR! "Failed to send SNMP trap notification to "MyProbe" for "MyProbe: MyProbe". (err = %d)", itsUserName, eventMesg, deviceName, err

ntfy "Sent SNMP trap notification to "MyProbe" for "MyProbe: MyProbe".", itsUserName, eventMesg, deviceName

ERR! "Failed to send e-mail notification to MyProbe. Check user configuration.", itsUserName

ERR! "Failed to send pager notification to MyProbe. (err = %d)", itsUserName, err

**** "Silenced all notifications until MyProbe.", timeStr

ERR! "SMTP Failure: Can't connect to "MyProbe". Error = %d", itsMailServer, err

ERR! "SMTP Failure: Server connection to "MyProbe" idle for more than 4 minutes. Disconnecting...", itsMailServer

ERR! "SMTP Failure: Server "MyProbe" won't accept mail from MyProbe. (Reply = %d)", itsMailServer, reversePath, replyCode

ERR! "SMTP Failure: Server "MyProbe" rejected recipient MyProbe. (Reply = %d)", itsMailServer, emailAddr, replyCode

ERR! "SMTP Failure: Server "MyProbe" failed when sending mailto MyProbe. Mail not sent. (%s Reply = %d)", itsMailServer, emailAddr, cmdName, replyCode

Web Server Messages

http HTTP - *address (user) authLevel -- commandargument*

InterMapper received a *command* request for *argument* from *address*

http HTTP - ERROR: JPEG compression failed. Compressed length = xxx. (Error = yyy)

InterMapper got an error code of yyy when attempting to compress the JPEG image whose length is yyy bytes.

http HTTP - ERROR: JPEG compression failed. Can't obtain/lock PixMap

InterMapper was unable to compress a JPEG image because it was already compressing an image. If this problem persists, quit InterMapper and relaunch it.

http HTTP - ERROR: JPEG compression failed. Can't create graphics offscreen. (Error = yyy)/dt>

InterMapper received the yyy error code when attempting to compress a JPEG image.

http HTTP - ERROR: PNG compression failed because there is not enough memory. (yyy K available)

InterMapper failed to compress a PNG

http "HTTP - ERROR: PNG compression failed. (Error = ###)"

InterMapper received an OS error ### when attempting to compress the PNG image

http "HTTP - y.y.y.y -- Unknown HTTP Version: xxx"

InterMapper received an unknown version - xxx - in an HTTP request from y.y.y.y

http "HTTP - y.y.y.y -- Missing HTTP Version."

No HTTP version was included in the HTTP request from y.y.y.y

http "HTTP - y.y.y.y -- Unknown HTTP Command: xxxx"

An HTTP request from y.y.y.y contained an unknown "xxxx" command

http "HTTP - y.y.y.y -- Disconnected before response was sent."

The HTTP client at y.y.y.y disconnected before InterMapper had sent the entire response

http "HTTP - ERROR: Unable to create ### x ### JPEG image. (Error = err)"

InterMapper received an *err* OS error code when attempting to generate a ### x ### JPEG image.

http "HTTP - ERROR: Unable to create ### x ### PNG image. (Error = err)"

InterMapper received an *err* OS error code when attempting to generate a ### x ### PNG image.

link "msg (util%) : [ifIndex] device-name - ifDescr"

Logged to the event log when the utilization crosses some threshold. 'msg' is a message of the form "util < nn" or "util >= nn" where 'nn' is the threshold. The actual link utilization follows in parentheses. 'ifIndex', 'device-name', and 'ifDescr' identify the individual interface.

debug "device-name UTIL[ifIndex]=util? type: upTimeNow=nn, upTimePrev=nn;inOctetNow=nn, inOctetPrev=nn; outOctetNow=nn, outOctetPrev=nn; bps-s=nn

Logged to the event log when the interface utilization calculated is greater than 110%. In general, a value greater than 100% indicates an erroneous value for one of the inputs; this log message prints out all the inputs to the calculation for later analysis. device-name and ifIndex indicate the interface, util is the utilization percentage, type indicates the type of calculation: FullDuplex or Baseband. The other numbers are the values of sysUpTime.0, ifInOctets, ifOutOctets, and ifSpeed.

debug Saved backup copy of *mapname* in "InterMapper Settings:Old Maps" folder.

InterMapper saved a copy of the original file (*mapname*) in the Old Maps folder before saving a version of the file in a newer format. This allows you to retrieve the earlier file and use it with an older copy of InterMapper.

debug An error occurred while attempting to save backup copy of *mapname*

InterMapper was not able to create a backup copy of the named map

debug Can't locate backup folder to save backup copy of *mapname*

InterMapper couldn't locate or create the InterMapper Settings:Old Maps folder.

debug Device '*devicename*' was using non-existent probe '*probename*', now set to non-polling.

The named device was set to be probed with a non-existent probe type. It has been set to "non-polling", and will no longer be probed.

InterMapper RemoteAccess Server Messages

imrn "Accepted user connection from y.y.y.y."

An InterMapper RemoteAccess user connected in from y.y.y.y

imrn "Closed connection from y.y.y.y."

InterMapper closed the connection to the Remote client at address y.y.y.y

imrn "y.y.y.y denied access."

The InterMapper RemoteAccess client at y.y.y.y was denied access

imrn "y.y.y.y denied; too many connections."

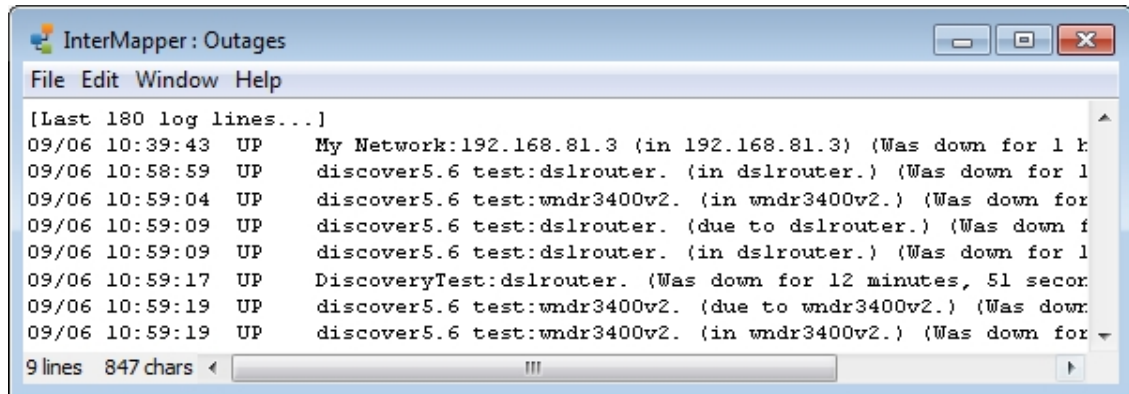
InterMapper denied access to an InterMapper RemoteAccess client because it already had too many connections operating.

The Outages Log

InterMapper summarizes outages that have occurred in the **Outages Log**. An *outage* is defined as a device that has gone from the UP state to the DOWN state, and then returned to the UP state. InterMapper tracks the start and end time of the outage, and computes the duration. Each time a device goes DOWN and then comes back UP, an entry is placed in the Outages log.

To open the Outages Log window:

- From the Windows Menu, choose **Outages** from the Logs submenu. The Event Log window appears, as shown below.



The Outages window shows the start and end time and the duration of outages.

The controls in the Outages Log window are identical to those of the other [Event Log \(Pg 235\)](#) windows, and are described on that page.

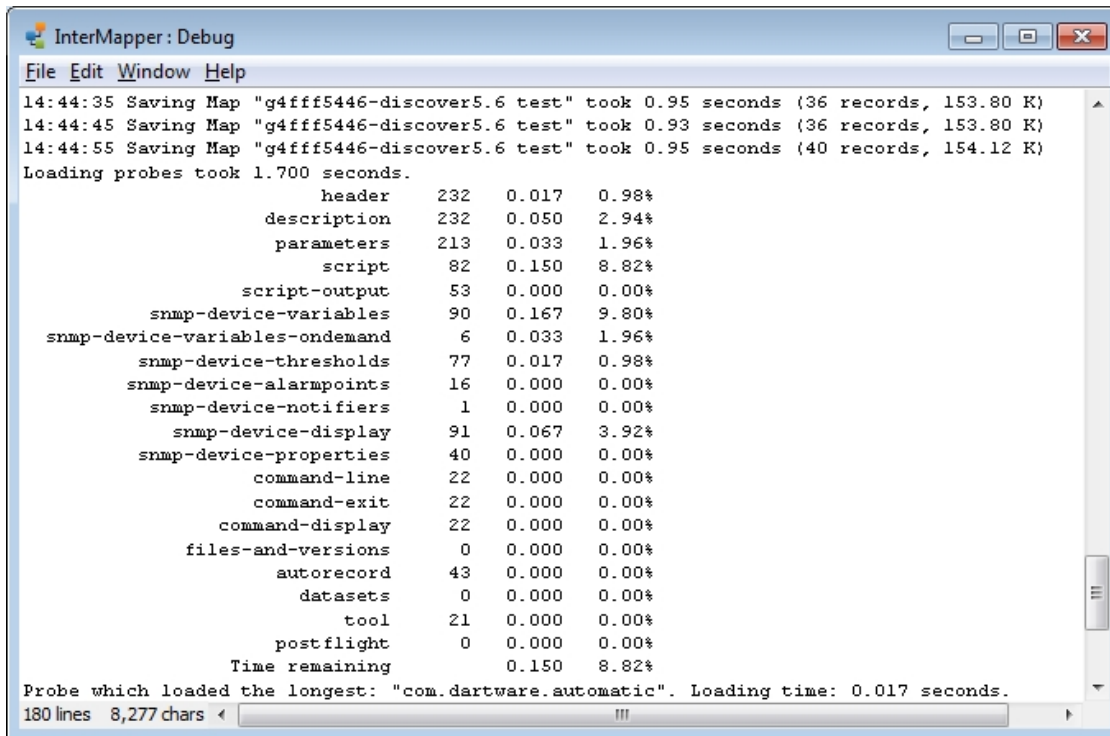
Debug Logs

InterMapper maintains two debug logs:

- **The Server Debug Log** - available from the Window menu's Logs submenu.
- **The Client Debug Log** - available from the Help menu's Diagnostics submenu.

Server Debug Log

The Server Debug Log contains details of the InterMapper Server's operations that can be valuable for troubleshooting various configuration problems. It stores messages generated by the server.



```
InterMapper: Debug
File Edit Window Help
14:44:35 Saving Map "g4fff5446-discover5.6 test" took 0.95 seconds (36 records, 153.80 K)
14:44:45 Saving Map "g4fff5446-discover5.6 test" took 0.93 seconds (36 records, 153.80 K)
14:44:55 Saving Map "g4fff5446-discover5.6 test" took 0.95 seconds (40 records, 154.12 K)
Loading probes took 1.700 seconds.
      header      232    0.017    0.98%
      description  232    0.050    2.94%
      parameters   213    0.033    1.96%
      script        82    0.150    8.82%
      script-output  53    0.000    0.00%
      snmp-device-variables  90    0.167    9.80%
      snmp-device-variables-ondemand    6    0.033    1.96%
      snmp-device-thresholds    77    0.017    0.98%
      snmp-device-alarmpoints    16    0.000    0.00%
      snmp-device-notifiers     1    0.000    0.00%
      snmp-device-display    91    0.067    3.92%
      snmp-device-properties    40    0.000    0.00%
      command-line    22    0.000    0.00%
      command-exit    22    0.000    0.00%
      command-display    22    0.000    0.00%
      files-and-versions    0    0.000    0.00%
      autorecord     43    0.000    0.00%
      datasets        0    0.000    0.00%
      tool            21    0.000    0.00%
      postflight      0    0.000    0.00%
      Time remaining    0.150    8.82%
Probe which loaded the longest: "com.dartware.automatic". Loading time: 0.017 seconds.
180 lines 8,277 chars
```

Some examples of information that is stored:

- A series of messages generated when the server is started or stopped.
- A message when a map is opened or saved.
- A series of messages when probes are reloaded.
- Most messages contain an indicator of how long a particular operation took.

To open the Debug Log window:

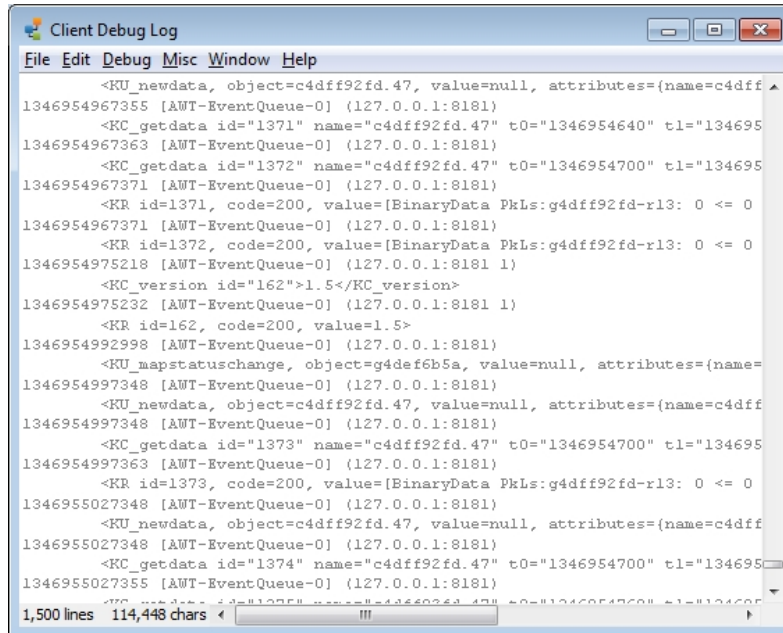
- From the Window menu's Logs submenu, choose **Client Debug Log**.

Client Debug Log

The Client Debug Log shows details of InterMapper's operations that can be valuable for debugging problems with the program. If you have trouble with InterMapper, the support staff may ask you to [Send Feedback \(Pg 216\)](#). The Send Feedback form sends the Client Log by default.

The Client Debug Log Window

The Client Log Window shows the contents of the Client Log.



To open the Client Debug window:

- From the Help menu's Diagnostics submenu, choose **Client Debug Log**.

Macintosh: Command + Option + Shift + Z

Windows: Control + Alt + Shift + Z

Linux/Unix: Control + Alt + Shift + Z

The Client Debug Log window opens, and **Debug** and **Misc** menus appear in the menu bar at the top of the window.

In general, Help/Systems does not document the information shown in the Client Debug Log window, because its messages will change from version to version.

Note: Opening the Client Debug Log window creates two new menus. Certain of the items in these menus are designed to test InterMapper's crash recovery facilities. Certain others may exercise portions of the program that may crash.

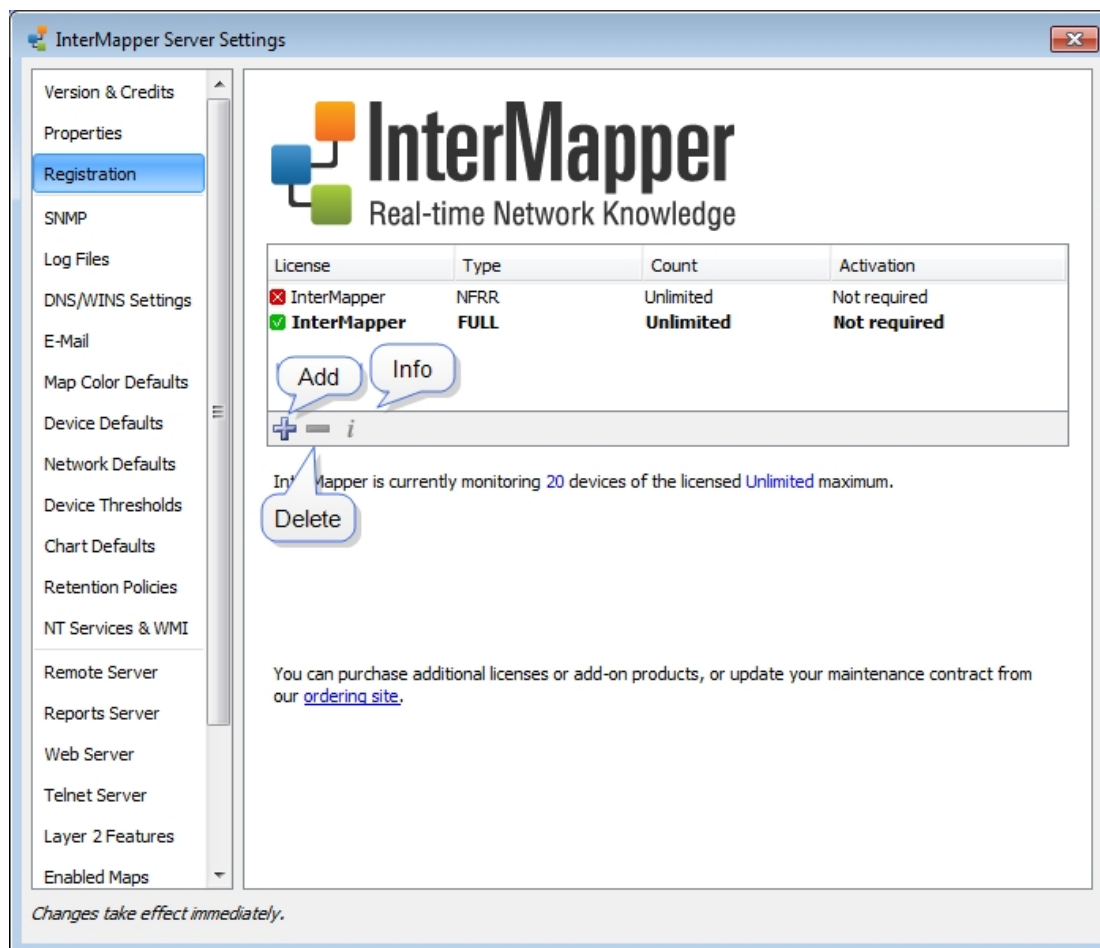
Chapter 8

Server Settings

Use the Server Settings window to view and edit the settings of an InterMapper server. You must have administrator privileges to access the Server Settings window.

The Server Settings documentation in this manual is divided into three topics:

- [Server Information Panels \(Pg 251\)](#) - view information about the InterMapper version. View and edit the server name and software licenses.
- [Server Preferences Panels \(Pg 253\)](#) - set defaults and other preferences for your server.
- [Server Configuration Panels \(Pg 277\)](#) - set up the web, telnet, Reports, and InterMapper Remote servers, enable and disable maps, create users and groups and set up map access, define notifiers, and set up an SSL certificate for the InterMapper server.



Use the Server Preferences section of the Server Settings window to view and edit default InterMapper's server settings.

To view and edit InterMapper server settings:

1. From the Edit menu, choose ***Server Settings...***. The Server Settings window appears, showing three sections of settings on the left. On the right is a panel in which the selected settings appear.
2. Click the subsection for the settings you want to edit. The selected settings appear in the right panel.

Server Information Panels

Use the Server Information panels of the Server Settings window to view and edit information about the current version of InterMapper and your system.

InterMapper Version & Credits

Use the Version & Credits panel to view the following information.

Version	View the version of InterMapper software currently running.
Built On	View the date on which the InterMapper software was built.

Properties

Use the Properties panel to view information about the InterMapper host system. You can also set the server name from this panel:

Server Name	View and set the name of the machine on which InterMapper is running. This name appears in the Map List window.
Hardware ID	View the hardware ID of the machine InterMapper is licensed and running on.
<OS type> System Version	The type of operating system and version number.
<OS type> Running Time	The length of time the operating system has been running.
Server Running Time	The length of time the InterMapper Server has been running.
Network Interfaces	Lists network interfaces available on the machine on which InterMapper is installed.

Registration

Use the Registration panel to view information about your monitored devices, to view a list of licensed products, and to add new licenses for software.

License List	Shows a list of licenses and add-on products.
Monitoring information	The number of monitored devices and your licensed monitoring limit are shown below the InterMapper logo. Note: Some InterMapper licenses specify a number of devices you can monitor. Demo probes do not reduce the number of devices available for monitoring.

Server Preference Panels

Use the following panels of the Server Settings window to set global preferences for the selected server.

In the left pane of the Server Settings window, click a button to view and edit its settings, as follows:

- [SNMP](#) (Pg 254)
- [Log Files](#) (Pg 257)
- [DNS/WINS settings](#) (Pg 262)
- [E-Mail](#) (Pg 264)
- [Map Default Colors](#) (Pg 265)
- [Device Defaults](#)
- [Network Defaults](#) (Pg 267)
- [Chart Defaults](#) (Pg 271).
- [Device Thresholds](#) (Pg 269).
- [NT Services & WMI](#) (Pg 276)

Note: You can also set preferences for a particular map using the **Map Settings** panel, available from the Edit menu. For more information, see [Map Settings](#) (Pg 86).

SNMP Preferences

Use the SNMP subsection of the Server Preferences section to set the default SNMP settings for each SNMP access method. These settings are used for all new devices.

About SNMP Versions

InterMapper can retrieve data from devices using SNMP version 1, version 2c, or version 3. Each of these can access the same SNMP information, but through different means:

- **SNMPv1** was the original version, and provided a simple means for retrieving data. Security was provided through *community strings* that acted like a password to allow or deny access to the information. The Read-Only community string gave permission to the requester to read data; the Read-Write community string gave permission to modify data. All data transmissions (including the community string) were sent "in the clear", that is, unencrypted.
- **SNMPv2c** provided additional, more efficient methods to request data, and added new data types (such as 64-bit counters) so that the monitoring system could get more accurate data. SNMPv2c is like SNMPv1 in that it uses the same community string system, and transmits data in the clear.
- **SNMPv3** provides the same data retrieval facilities as SNMPv2c, with additional security. There is a secure method of providing authentication information (so the device knows whether to respond to the query or not), as well as a privacy function that encrypts the entire transmission so that eavesdroppers cannot discern the data.

What is an SNMP Community String?

The SNMP Read-only Community string is like a user id or password that allows access to a router's or other device's statistics. InterMapper sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply ignores the request and does not respond.

Note: SNMP Community strings are used only by devices which support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

Community String Types

There are actually three community strings for SNMPv1-v2c-speaking devices:

- **SNMP Read-only community string** - enables a remote device to retrieve "read-only" information from a device. InterMapper uses this information from devices on its maps.
- **SNMP Read-Write community string** - used in requests for information from a device and to modify settings on that device. InterMapper does not use the read-write community string, since it never attempts to modify any settings on its devices.

- **SNMP Trap community string** - included when a device sends SNMP Traps to InterMapper. InterMapper accepts any SNMP Trap community string.

By convention, most SNMPv1-v2c equipment ships from the factory with a read-only community string set to "public". It is standard practice for network managers to change all the community strings so that outsiders cannot see information about the internal network. (In addition, network managers may employ firewalls to block any SNMP traffic to ports 161 and 162 on the internal network.)

SNMP Server Settings Pane

InterMapper remembers the default settings for each of the various SNMP access methods. These are set in the **Server Settings>SNMP** preference pane.

These options control how InterMapper interacts using the Simple Network Management Protocol (SNMP).

This pane allows you to specify the following:

- **SNMP Version** - Select the default *Setting the default SNMP preferences* SNMP version to be used for new devices in autodiscovery. InterMapper will attempt to use the selected version when it discovers a new device. If it gets a response, it will continue to use that version. If that fails, then it will simply ping the device.
- **SNMPv1-2c Community** - If the selected SNMP Version is either SNMPv1 or SNMPv2c, InterMapper will use this community string to attempt to communicate with the device.
- **SNMPv3 Authentication** - If the selected SNMP version is SNMPv3, InterMapper will use the specified authentication method (SHA, MD5, or None) with the indicated password on the right to authenticate with the device.
- **User Name** - The SNMPv3 user name to be used for authentication and privacy.
- **Privacy** - When using SNMPv3, the privacy method (DES, AES, or None) will be used with the encryption password on the right.

- **Listen for SNMP Traps on UDP Port 162** - Check this box if you want InterMapper to listen for SNMP traps sent from devices to the standard port 162.
- **Also listen for SNMP traps on UDP port** - InterMapper can listen for traps on a second, non-standard port (in addition to port 162). Check this box and enter the port number in the text box. Traps received on this alternate port are handled in the same manner as those received on port 162.
- **Verbose trap logging** - Check this box to instruct InterMapper to display the full OID and contents for all varbinds of a trap, instead of simply the varbind contents.

Setting SNMP Preferences for Specific Devices

The panel shown above sets the default SNMP preferences that InterMapper uses when querying devices. You can also set SNMP preferences for individual devices on your map using the **Set Community...** (SNMPv1-v2c) or **Set Probe...** (all three SNMP versions) commands, available from the Monitor menu. You can set various parameters for one or more devices at a time, by selecting the devices you want to change before executing the command.

Log File Preferences

InterMapper writes information to log files about various events. Use the log files to review the events surrounding a particular problem, helping you to troubleshoot the problem more effectively.

To view an existing log file:

- Choose the file you want to view from the Logs submenu of the Windows menu.

To view and edit the preferences for log files:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
2. Click **Log Files**. A list of log files appears in the right panel, showing the current Log File preferences for the selected log file.

Setting Preferences for Log Files

Log File Options + Add New Log

Name	Rotate Interval
Debug	Daily at 00:00
Event Log	Daily at 00:00
Outages	Daily at 00:00
Paging	Daily at 00:00
SMS	Daily at 00:00

Log File Name: <date>.txt

Start New Log File: Once a Day

Every day at 00:00

☒ Delete log files after 7 days

☐ Also send messages to syslog server

IP Address:

Facility: local0

Severity: emergency

✕ Delete this Log

This log file records low-level information as InterMapper runs. This information is often useful in tracing program operation. To see the Debug Window, choose Window->Logs->Debug in any open map window.

The Log File preferences pane shows a list of currently defined log files with properties for the selected file.

- **To see a brief explanation of the function of a log file,** click the log file in the list. The explanation appears in the lower panel of the Preferences pane.
- **To add a log file,** click **Add New Log**. The [Log File Preferences \(Pg 259\)](#) for the new log file appear.
- **To edit a log file definition,** click to select a log file definition. The properties for the selected log file appear. The [Log File Preferences \(Pg 259\)](#) for the selected log file appear.
- **To delete a log file,** click to select a log file definition, then click **Delete this Log**. The log file definition disappears from the list.

Note: The Debug Log, Event Log and Outages Log cannot be deleted.

Log File Preferences

The example above typical log file preferences. It shows the names of the log files, and their rotation intervals.

To add a new log file:

1. Click **Add New Log**. The [Log File preferences \(Pg 259\)](#) for the new log file appear.
2. [Set the log file preferences \(Pg 259\)](#) as described below.

To edit preferences for an existing log file:

1. Click to select the log file. The [Log File preferences \(Pg 259\)](#) for the selected log file appear.
2. [Set the log file preferences \(Pg 259\)](#) as described below.

Setting Log File Preferences

Log File Name - Set the filename (actually the prefix) for the log file. You can enter up to 14 characters (see [Log File Naming and File Format \(Pg 261\)](#) below.) The file is given a .TXT extension, and can be edited with any text editor.

Start New Log File - Use these settings to specify how often and at what point in a log cycle the current log file is closed and a new one is opened. This allows you to break the log files into convenient sizes and/or time epochs. Choose from these options:

- Never
- Once daily
- Twice daily
- Once weekly
- Twice weekly

Delete log files after ___ days/weeks - Check this box to force InterMapper to delete old log files automatically after a certain date.

Note: Each time InterMapper starts a new log file, it checks to see if any log files should be deleted. On platforms where the file creation date is available, it is used to determine whether a log file should be deleted. If the creation date is not available, the file's last modification date is used.

Also send messages to syslog server

Click this checkbox to specify that all log file entries be sent to a syslog server. Set the values for:

- **IP Address** - enter an IP address for the syslog server.
- **Facility** - choose a value to match your local system conventions.
- **Severity** - choose a value to match your local system conventions.

Redirecting Log Entries

By default, all entries go to the built-in Event Log file. You can redirect streams of log entries from InterMapper's Remote Server, Web Server, or Telnet server to a particular log file (and syslog server). This can be useful, for example, for sending all web access events one file, and all outage events to a different file.

To redirect a log entry stream:

1. Create a new log file definition for the file you want to receive the log entries, as described above.
2. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
3. In the left panel of the Server Settings window, click to choose the server (Remote, Web, or Telnet) whose log entries you want to send to a different log file. The panel for the selected server appears.
4. In the **Send Log File Entries to** menu, choose the log file you created to receive the log entries. All log file entries for the selected server are redirected to the new log file.

Log File Naming and File Format

Log files are saved in text format in the *InterMapper Settings:InterMapper Logs* folder. Each file has a user-defined prefix that describes its function, and ends with a suffix of *.yyyymmddhhmm.txt*, where the suffix is the (four-digit) year, month, day, hour and minute when the file was created. The prefix can be up to 14 characters in length.

Log File Sources

Log information comes from several sources, including:

- Up and down entries for the devices being logged
- Hits on the built-in web server
- Connections to the InterMapper RemoteAccess and Telnet server
- InterMapper's own internal status and error messages

Three built-in log files are always present, and cannot be deleted:

- The **Event Log** file - when you first launch InterMapper, the Event log file receives all entries from all sources. You can divert certain streams to other log files.
- The **Outages** file - contains entries that describe the start and end times of outages, as well as their duration. This stream of entries cannot be redirected to any other log file.
- The **Debug** file - displays certain debugging information, as described in [The Debug Window \(Pg 247\)](#).

DNS/WINS Settings

Use the DNS/WINS Settings section to specify the DNS server(s) and WINS server(s) that InterMapper uses. InterMapper uses your current DNS servers as its default.

InterMapper can use one or more Domain Name Service servers (DNS) to convert DNS names to addresses and back. InterMapper checks the listed DNS server(s) at regular intervals to make sure that the DNS name and IP address for a device match.

When you start InterMapper on a MacOS X or Windows machine, the DNS servers specified by the current network configuration are used. On Unix machines, you must enter one or more DNS server addresses manually.

The DNS addresses are optional: if the preference is empty, InterMapper does not attempt to make DNS <-> IP address conversions.

For example, when InterMapper polls a device that has a name assigned, it looks up the corresponding IP address in the DNS. If the resulting address has changed since the device was added to a map, InterMapper logs an error message.

InterMapper will use the Domain Name Servers listed below to look up device names and IP addresses.

Comma-separated list of DNS server addresses:

192.168.81.1

Search Domain:

Minimum interval between DNS checks: 5 Minutes

☒ Use WINS name resolution

InterMapper will use the WINS Servers listed below to look up device names and IP addresses.

Comma-separated list of WINS server addresses:

☒ Use broadcast if lookup fails

WINS Scope:

DNS/WINS Settings pane.

Setting DNS Monitor Preferences

Set DNS Monitor preferences as follows:

- **Comma-separated list of Domain Name Server addresses** - Enter a list of Domain Name Server addresses, separated by commas.
- **Search Domain** - Enter a name to append to a partial domain name to make a fully-qualified domain name.
- **Minimum interval between DNS checks** - Set this value to the amount of time to wait between successive queries for a host. Use a larger value to reduce the number of times the DNS is checked.

Setting WINS Preferences

You can specify one or more WINS servers that InterMapper will use for WINS lookups. InterMapper can also fall back to broadcast lookups for WINS/NetBIOS name lookups. Unless instructed by your network administrator, you should usually leave the WINS Scope blank.

- **Use WINS name resolution** - Check this box to allow InterMapper to use the specified WINS servers to look up device names and addresses.
- **Comma-separated list of WINS server addresses** - Enter a list of addresses, separated by commas.
- **Use broadcast if lookup fails** - Check this box to allow InterMapper to use broadcast lookups for WINS/NetBIOS lookups if the WINS lookup fails.
- **WINS Scope** - Enter a WINS Scope. This should only be necessary if instructed by your network administrator.

E-Mail Preferences

Use this panel to enter the information required to send e-mail notifications.

InterMapper sends e-mail notifications to these SMTP servers using the sender information specified.

Primary SMTP	Host:	<input type="text"/>	Port:	<input type="text"/>
	User:	<input type="text"/>		
	Password:	<input type="text"/>		
Back-up SMTP	Host:	<input type="text"/>	Port:	<input type="text"/>
	User:	<input type="text"/>		
	Password:	<input type="text"/>		

The From: line and Errors-To: line of the message will be set to the values below.

From address:	<input type="text"/>
Errors to:	<input type="text"/>

☐ Automatically e-mail InterMapper crash reports

Send crash reports to:

Configuration for sending e-mail notifications.

Setting E-mail Preferences














- **Primary SMTP** - Enter the Host name. If your SMTP server requires authentication, enter a User, Password, and Port for the primary SMTP host. Port 25 is typically used for outgoing E-mail servers.
- **Back-up SMTP** - Enter the Host name. If your SMTP server requires authentication, enter a User, Password, and Port for the back-up SMTP host. If unsuccessful sending through the primary host, InterMapper attempts to deliver e-mail messages through the Back-up host.
Notes: InterMapper supports the PLAIN and CRAM-MD5 authentication commands. You can use different E-mail accounts and passwords for the primary and back-up SMTP servers.
- **From address** - Enter the E-mail address you want to appear as the *From:* line of the message.
- **Errors to** - Enter the address you want to use in the *Errors-To:* line of the message. Bounce messages are returned to this address.
- **Automatically e-mail InterMapper bug reports** - Check this box to allow InterMapper to send reports of errors and bugs to the staff at Help/Systems automatically.
 - **Send bug reports to** - Enter the E-mail address you want to use when sending bug reports.

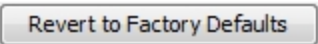
Default Map Colors

When InterMapper creates a new map, it uses a set of default colors for the items and features on the map. Use the Map Colors preferences to set the default colors for a map.

Use the Default Map Colors preference to view and edit the default colors for all map items and features.

Click a color below to change the default color of the corresponding map feature.

Background: 	Links: 
Ants: 	Labels: 
Networks: 	Discovery: 
Up: 	Warning: 
Alarm: 	Critical: 
Down: 	Unknown: 
Acknowledged: 	



The Map Color Defaults subsection of the Server Preferences section of the Server Settings window. Click any of the colors to open the Color Picker and select a different color for that device/link.

To view and edit the Default Map Colors preference:

- From the Server Preferences section of the Server Settings window, click **Map Color Defaults**. The Map Color Defaults preferences appear in the right pane.

Colors you can change

The following colors can be defined.

- **Background** - Set the map's background color. This is overridden by a background image.
- **Ants** - Set the color of the traffic flow indicators that appear on a link. These are often referred to as "marching ants." Traffic flow indicators only appear in links to SNMP devices.
- **Networks** - Set the default color of network ovals.
- **Up** - Set the color of devices that are in the "Up" state.
- **Alarm** - Set the color of devices that are in "Alarm" state.
- **Down** - Set the color of devices that are in the "Down" state.
- **Acknowledged** - Set the color of devices that have gone down and the outage has been acknowledged.
- **Links** - Set the color of links, the connections between devices, networks, or interfaces.
- **Labels** - Set the default color of device and network labels.
- **Discovery** - Set the color of a network that is the target of the discovery process.
- **Warning** - Set the color of devices that are in the "Warning" state.
- **Critical** - Set the color of devices that are in the "Critical" state.
- **Unknown** - Set the color of devices that are in an "Unknown" state.

To change a map color:

1. Click in that feature's box. The Color Picker appears.
2. Click to choose the desired color.
3. Click **OK**.

Note: Changing the default colors changes the colors assigned to an existing map only if **Use server defaults** is checked in the map's settings (it is checked by default). Change an individual map's colors from the [Map Settings \(Pg 86\)](#) window.

Default Device and Network Preferences

When devices and networks are first added to the map, InterMapper shows devices as rectangles and networks as ovals.

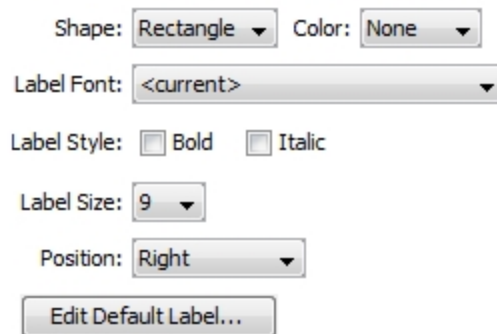
Use the Device Defaults and Network Defaults Preferences to change the default appearance of devices and networks.

Note: The Device Defaults and Network Defaults Preferences are identical in appearance and function. One affects the default appearance of devices, while the other affects the default appearance of networks.

Device Defaults

The defaults for devices are shown below:

New Devices on a map will have the appearance specified below.



Shape: Rectangle Color: None

Label Font: <current>

Label Style: ☐ Bold ☐ Italic

Label Size: 9

Position: Right

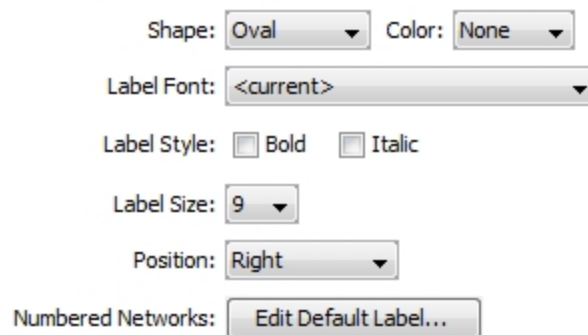
Edit Default Label...

The Device Defaults Panel

Network Defaults

The defaults for a network are shown below:

New Networks on a map will have the appearance specified below.



Shape: Oval Color: None

Label Font: <current>

Label Style: ☐ Bold ☐ Italic

Label Size: 9

Position: Right

Numbered Networks: Edit Default Label...

The Network Defaults Panel

Setting Default Device and Default Network parameters

To view and edit the default Device and Network parameters:

1. From the Map List window, click to select any map on the server whose settings you want to edit.
2. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
3. In the Server Preferences section, click the Device Defaults or Network Defaults subsection. The default settings for the selected subsection appear.
4. Edit the preferences as described below.
5. When finished, click **OK**.

Shape Choose a default shape for the device or network from the dropdown menu.

Color Choose a default color for the device or network from the dropdown menu.

Label Font Choose a default font for the device or network's label.

Label Size Choose a default font size for the device or network's label.

Position Choose a default position for the label text, relative to the device or network icon.

Note: The **Position** parameter affects only *Wire* and *Icon* shapes.

Edit Label... Set default labels for numbered and unnumbered networks, as described in [Editing \(Pg 106\)](#) [Labels \(Pg 106\)](#).

Default Device Thresholds

You can set default device thresholds any new device added to a map.

Note: Only SNMP probes have thresholds for all three parameters (round-trip time, packet loss and interface errors); a ping/UDP-based probe monitors only round-trip time and packet loss, and a TCP probe monitors only round-trip time.

For more information on device thresholds, see [Setting Error and Traffic Thresholds \(Pg 208\)](#).

Set device thresholds to alert you to network problems.

Down Thresholds			
Number of lost packets (1 - 10):		<input type="text" value="3"/>	
Other Thresholds			
	Warning	Alarm	Critical
Interface SNMP errors:	<input type="text" value="2"/>	<input type="text" value="10"/>	<input type="text" value="20"/> per minute
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/> of last 100
Response time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/> msec
<input type="checkbox"/> Set devices to Alarm status on down link			

The Default Device Thresholds Panel

Choosing Alarm Behavior for Interfaces

Use the the **Set devices to Alarm status on down link** check box to control the behavior of alarms when an interface goes down.

To choose your preferred behavior:

- **Trigger an alarm for the device** when any interface goes down - select the check box.
- **Trigger an alarm for an individual interface** when an it goes down - clear the check box.

Default Server Interface Thresholds

You can set default thresholds for interfaces on any new device added to a map.

For more information on interface thresholds, see [Setting Error and Traffic Thresholds \(Pg 208\)](#).

Set interface thresholds to alert you to network problems.

Error Thresholds

	Warning	Alarm	Critical	
Rx Errors (Received):	<input type="text" value="10"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	per minute
Tx Errors (Transmitted):	<input type="text" value="10"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	per minute
Total Errors (Rx + Tx):	<input type="text" value="10"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	per minute

Utilization Thresholds

	Warning	Alarm	Critical	
Rx Utilization (Received):	<input type="text" value="75"/>	<input type="text" value="85"/>	<input type="text" value="95"/>	%
Tx Utilization (Transmitted):	<input type="text" value="75"/>	<input type="text" value="85"/>	<input type="text" value="95"/>	%
Total Utilization (Rx + Tx):	<input type="text" value="75"/>	<input type="text" value="85"/>	<input type="text" value="95"/>	%

Discard Thresholds

	Warning	Alarm	Critical	
Rx Discards (Received):	<input type="text" value="15"/>	<input type="text" value="25"/>	<input type="text" value="35"/>	per minute
Tx Discards (Transmitted):	<input type="text" value="15"/>	<input type="text" value="25"/>	<input type="text" value="35"/>	per minute
Total Discards (Rx + Tx):	<input type="text" value="15"/>	<input type="text" value="25"/>	<input type="text" value="35"/>	per minute

The Default Interface Thresholds Panel

Chart Defaults

Charts (see [Creating Charts \(Pg 219\)](#) and [Using Charts \(Pg 219\)](#)) can show historical data for values received from one or more devices. Use the Chart Defaults panel of the Server Preferences section of the Server Settings window to view and edit the default settings for a newly-created chart.

To view and edit Chart Default preferences:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears, showing the list of available settings. On the right is a panel in which the selected settings appear.
2. Click **Chart Defaults**. The Chart Defaults panel appears in the right panel of the Server Settings window.

Axes Tab

Use the Axes Tab of the Chart Defaults panel to define the appearance and behavior of newly-created charts.

Upper Bounds, Lower Bounds -

Enter values to control the vertical scale of the chart. The range of values depends on the variable being monitored.

Auto-adjust -

Select or clear the **Auto-adjust** check box to choose whether to allow Inter-Mapper to adjust the scale of the chart automatically. If the **Auto-adjust** check box is checked, the upper and/or

lower bounds are adjusted automatically so that data points are always displayed, no matter how much they increase or decrease.

Dividers, Sub-Dividers - Click the up- and down-arrows or enter a number of dividing lines to set the number of horizontal dividers and to set the number of

The Axes Tab

sub-dividers you want to appear between the dividers. Example: Set the number of dividers to 3. Set the number of sub-dividers to 4. This gives a total of 11 dividers. (Three dividers - top, bottom, and center, with four dividers between each. Eight sub-dividers and three dividers.)

Show Date, Show Day of Week, Show Time, 24 Hour Time - Click to select or clear these check boxes to specify which labels appear on a chart's horizontal axis by default.

Default Interval - Use the drop-down menu to choose a default interval between time stamps on the X-axis (horizontal) of new charts. Shorter intervals show finer detail, longer intervals show a longer history.

Note: Because InterMapper saves all the data points, there is no limit to the amount of memory needed to save a chart. Choosing a longer time interval does not save memory - all the data points are saved.

Sub-Dividers - Click the up- and down-arrows to specify the number of vertical sub-dividers to draw between data points.

Data Tab

Use the Data Tab of the Chart Defaults panel to choose line and data point styles.



The Data Tab

Use the Data tab to control the way in which data appears in the chart.

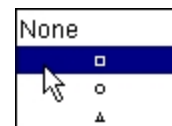
Style

Use the **Line Style** menu to choose a line thickness for the default line.

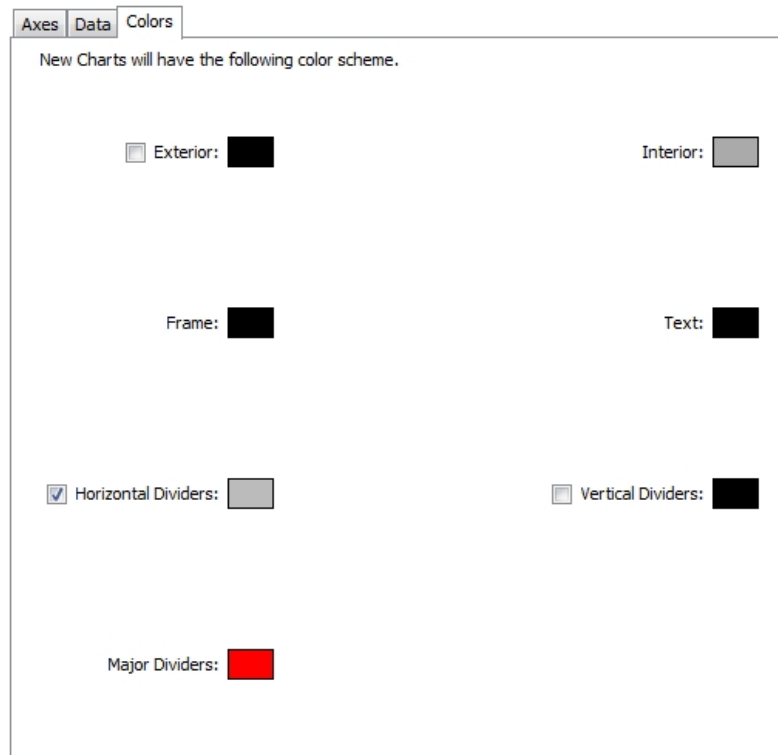


Highlight

Use the **High-light** menu to choose the icon to be drawn at the end of each line segment.



Colors Tab



The screenshot shows a dialog box with three tabs: 'Axes', 'Data', and 'Colors'. The 'Colors' tab is selected. Below the tabs, a text label reads 'New Charts will have the following color scheme.' The dialog contains several color selection options, each with a label and a color box:

- ☐ Exterior: [Black color box]
- Interior: [Light Gray color box]
- Frame: [Black color box]
- Text: [Black color box]
- ☒ Horizontal Dividers: [Light Gray color box]
- ☐ Vertical Dividers: [Black color box]
- Major Dividers: [Red color box]

Use the Colors tab to set the default colors for charts.

To change a color:

Click a color box to set the color. A color-selection window appears.

For more information on colors and how they are used, see the [Colors Tab \(Pg 231\)](#) section of Chart Options.

The Colors Tab

Retention Policies

Use the Retention Policies pane to create and edit retention policies that can be used to specify how data is stored for a particular device or map.

Data Retention Policies affect how much data is stored for charts and reports.

Unless otherwise specified, InterMapper will apply this Data Retention Policy to data when first added to a chart.

Data Retention Policy for new Charts: 24 Hours ▼

Name	Original	5 Min.	Hourly	Daily	Chart Data
24 Hours	1 Day	1 Day	1 Day	1 Day	Forever
autorecord	1 Day	1 Month	1 Week	355 Days	Forever
Chart Only	None	None	None	None	Forever
Critical Data	1 Day	2 Months	355 Days	Forever	Forever
Forever	Forever	Forever	Forever	Forever	Forever
IM46Charts	Forever	Forever	Forever	Forever	Forever
None	None	None	None	None	None
Server Default	1 Day	2 Weeks	6 Months	1,775 Days	Forever
SLA Data	1 Day	2 Months	6 Months	355 Days	Forever

Add - Delete - Edit

+ - ✎

The Retention Policies pane

Each row shows a Retention Policy, and its setting for retaining Original, 5-minute, Hourly, and Daily data from devices, as well as data from Charts.

Using the Retention Policies Pane

- **Default Retention Policy for new Charts** - choose a policy to apply by default.
- **Policy list** - click to select the policy you want to delete or edit.
- **Add Policy** - click **+** to add a new policy.
- **Delete Policy** - click to select the policy you want to delete, then click **-**.
- **Edit Policy** - click to select the policy you want to edit, then click the Pencil tool.

Creating and Editing a Retention Policy

About Retention Policies

You can use data retention policies to consolidate raw data, reducing the amount of data stored. Data retention policies control how often and how much data is averaged and reduced.

A data retention policy can be applied to a specific map, to one or more devices or interfaces on a map, to an individual dataset, or to all maps on an InterMapper Server. Policies also affect the way InterMapper stores chart data.

Creating Retention Policies

Use the Create Retention Policy window to define a new retention policy. The same window is used for editing an existing policy.

To create a retention policy:

1. Click the plus icon to open the Create Retention Policy window.
2. Enter a policy name.
3. Specify how long you want to keep **original data**, **5-Minute**, **Hourly**, and **Daily** samples.
4. Select a **Server Storage type**:
 - **Forever** - all charted or exported values are saved to a local disk file.
 - **None** - data is polled, but is not saved for charting or exporting.

To edit a retention policy:

1. In the Retention Policies pane, click the retention policy you want to edit.
2. Click the Pencil tool. The Edit Policy window for the selected policy appears.

NT Services & WMI

InterMapper can monitor and send notifications for NT Services running on another computer. InterMapper uses the Service Control Manager facilities of the underlying Windows host to communicate with a remote computer to track the state of its services.

Notes:

- You must be running the InterMapper server on a Windows computer to use this capability.
- The InterMapper server computer must be able to log onto the target Windows computer *as a service*. For more information, see [Authentication for NT Services Probe \(Pg 601\)](#) in the topic, "Monitoring NT Services with the Windows NT Services Probe".
- If a command-line probe contains the NTCREDENTIALS flag, InterMapper runs the probe as the user specified here.

Use the NT Services panel of the Server Preferences section to set the User and Password for the machine. If you are running InterMapper Server on a Windows machine, this allows InterMapper to build a list of services the machine is running.

Please enter the username and password of an account with Administrator privileges on the InterMapper machine.

Administrator privileges are necessary in order that the NT Services and WMI probes be able to establish connections to the target machines.

InterMapper is not currently running under an administrator account; it will use the username and password you supply to elevate its privileges each time it needs to poll an NT Services or WMI device.

User:
Password:

NT Services & WMI panel

Server Configuration Panels

InterMapper provides three built-in servers you can use to view and retrieve information about the status of the network from remote computers. Each server's built-in firewall must be configured before it can be used. By default, each server's firewall is set up so that access is denied.

Use the Server Configuration panels of the Server Settings window to view and edit settings for the built-in servers, to manage users and groups, to control map access, and to manage a list of [notifiers/alerts \(Pg 131\)](#).

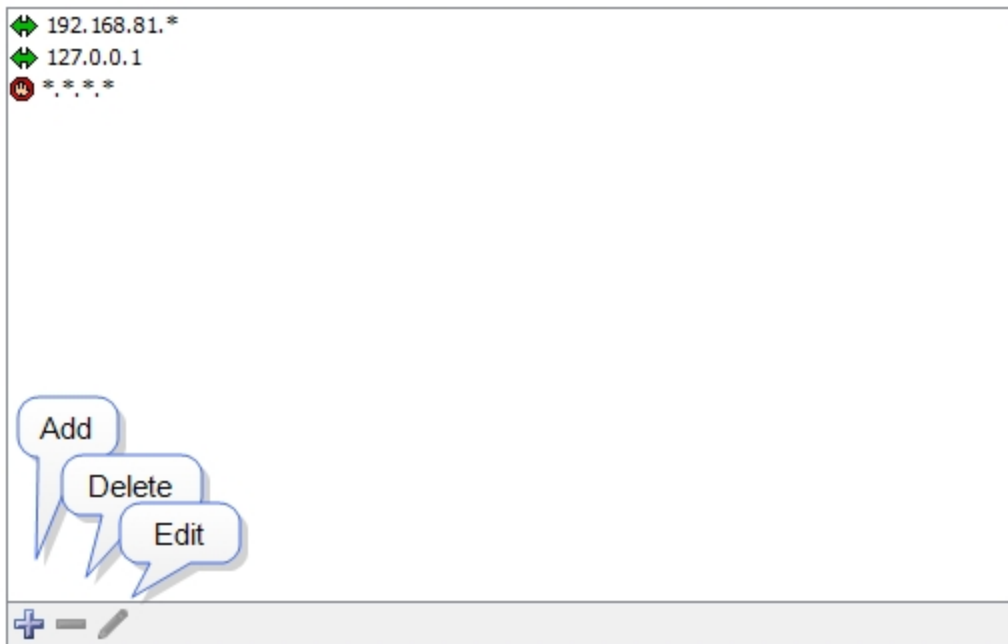
In the left pane of the Server Settings window, click the button for the settings you want to edit, as follows:

- [Remote Server \(Pg 282\)](#) - Start, stop, or edit settings for the InterMapper RemoteAccess server.
- [Reports Server \(Pg 285\)](#) - Start stop, or edit settings for the InterMapper Reports Server.
- [Web Server \(Pg 289\)](#) - Start, stop, or edit settings for the InterMapper web server.
- [Telnet Server \(Pg 291\)](#) - Start, stop, or edit settings for the InterMapper Telnet server.
- [Layer 2 Features \(Pg 294\)](#) - Turn on Layer 2 discovery for your server.
- [Enabled Maps \(Pg 296\)](#) - View a list of available maps, enable or disable maps, and import or export maps.
- [Users \(Pg 298\)](#) - View, Add, and Edit users and groups, and control access for users and groups.
- [Map Access \(Pg 305\)](#) - Control access by any user or group to any map through the web server or remote server.
- [Map Backup \(Pg 307\)](#) - Enable automatic map backups and create a schedule for backing them up.
- [Notifier List \(Pg 308\)](#) - View, add, copy, edit and remove notifiers.
- [SSL Certificate \(Pg 310\)](#) - Create new Certificate Signing Requests (CSR) and upload new certificates to the InterMapper server.

For more information on configuring your servers, see [Server Access Control \(Pg 280\)](#). It tells how to set a server's port, discusses encryption and when to use it, and describes how to configure a server's built-in firewall's list of IP addresses.

Configuring a Firewall

For each built-in server, the Firewall list shows all the addresses that are allowed to connect or are blocked:



- If an incoming address matches an *Allow* address (or range), the connection is allowed.
- If the incoming address matches a *Deny* address, the connection is dropped.
- Firewall definitions are checked against the incoming address in the order in which they appear.

Changing the order of a firewall definition

Firewall definitions are applied in the order in which they appear. You can change the order of the definitions after you have created them.

To move a firewall definition to a different position in the list:

- Click and drag the firewall definition to the new position.

Entering Address Ranges

You can enter addresses in the access control list in three different formats:

- **Fully-specified IP addresses**
Example: 192.168.1.10
- **Address ranges**
Example: 192.168.1.1-31. This specifies any device in the range 192.168.1.1 to 192.168.1.31.
- **Addresses with a "*" wildcard** Each wildcard corresponds to a range of 0-255.
Example: 192.168.1.* (equivalent to 192.168.1.1-255)
Example: 192.168.*.* (Class B range)
Example: *.*.*.* ("all addresses")

Tip: To deny access to certain addresses, add them at the top of the list and set the **Access** attribute to "Deny".

For a description of the Access Control process and the rules InterMapper uses to determine whether a user should be allowed to connect to an InterMapper server, see [Controlling Access to Your Server \(Pg 280\)](#).

Controlling Access to Your Server

You can configure the firewalls of InterMapper's built-in servers to accept or deny connections from a client based on its IP address. You can also require a user name and password. Once accepted, a connection is associated with a user name that is used to determine which maps and permissions are available. For some examples of typical access control setups, see [Access Control Examples \(Pg 303\)](#).

Notes:

- You can also control access through the [InterMapper Authentication Server \(Pg 623\)](#), which connects to an external authentication server such as Radius, LDAP, or ActiveDirectory to authenticate a user. For more information, see [Authentication Server \(Pg 623\)](#).
- Any firewall that is protecting the machine that is running InterMapper must be configured to allow access to the ports specified for remote access. This includes the port specified for use by the web server.

The Access Control Process

When a user attempts to connect to one of the InterMapper servers, the request goes through these steps:

1. **The client's IP address is checked against the list of firewall definitions.** If the address matches a DENY address in the firewall list, or if the address fails to match an ALLOW address, the connection is dropped with a "not allowed" response.
2. **The client's IP address is checked against the list of Automatic Login addresses.**

If the client's IP address matches an Automatic Login address, the connection is accepted and is assigned the user name associated with that Automatic Login.

3. If the client's IP address does not match an Automatic Login address, the connection is accepted and authentication by a username and password begins, as follows:
 - a. **Web server** - issues a "401 Unauthorized" response, which forces the web browser to request a username/password from the user.
 - b. **Telnet server** - prompts for a username and password.
 - c. **Remote server** - proceeds after the InterMapper RemoteAccess client requests and supplies a username and password.
4. **The username and password are verified against InterMapper's built-in authentication database.** If they match, the connection is assigned the user name. Otherwise, the connection is dropped with a "not allowed" response. When using the Remote and Telnet servers, an error message appears, saying that the user name is not allowed. When using the Web server, a web page appears, saying that the user is not allowed access.
5. **The users is checked for membership in a Special Group.** These special groups give broader access:
 - **Administrators Group**
If the user is a member of the Administrators group, the connection is

given full (read/write) access to every map and setting.

- **FullWebAccess Group**

If you have created a group named *FullWebAccess*, all members of that group are given full access to all maps through the web server. As with all web access rights, this is a read-only view. This membership also overrides any individual map access settings.

FullWebAccess members can also acknowledge down devices.

- **FullTelnetAccess Group**

If you have created a group named *FullTelnetAccess*, all members of that group are given full access to the Telnet server.

- **FullLogAccess Group**

If you have created a group named *FullLogAccess*, all members of that group are given full access to all log files.

6. **The user is granted access to maps.** Once a connection has a user name associated with it, InterMapper then checks to see which information is available for that user. Access to individual maps can be granted using the "Map Access" server setting (see [Map Access \(Pg 305\)](#) for more info).

If a user is not in the Administrators, FullWebAccess, or FullTelnetAccess group, and has no access to an individual map, the connection is dropped with a "not allowed" response, since the user has no options for access.

The Remote Server

InterMapper's Remote Server allows a user to configure and edit maps on an InterMapper installation from a remote computer. To allow these changes, the Remote Server accepts connections from the InterMapper or InterMapper RemoteAccess application, running on a different computer. For more information about InterMapper RemoteAccess, see the [InterMapper Remote](#) web site.

InterMapper always listens for remote connections on its localhost interface, 127.0.0.1. This allows a user to run a copy of the InterMapper RemoteAccess application on the machine that is running InterMapper. For security, InterMapper refuses all Remote Server connections from non-localhost addresses by default to prevent unauthorized configuration.




You can configure InterMapper to accept connections from remote computers, giving varying degrees of access by IP address or by username and password.




Unlike the Telnet and Web servers, you cannot start or stop the Remote Server. You configure the Remote Server using the Remote Server settings panel of the Server Configuration section, found in the Server Settings window.

Remote Server Listening On Port 8181 [Secure]

Listen for connections on TCP port:

Access Control List to Remote Server based on IP Address:

	192.168.81.*
	127.0.0.1
	*,*,*,*

Show Connected Clients

Send log file entries to:

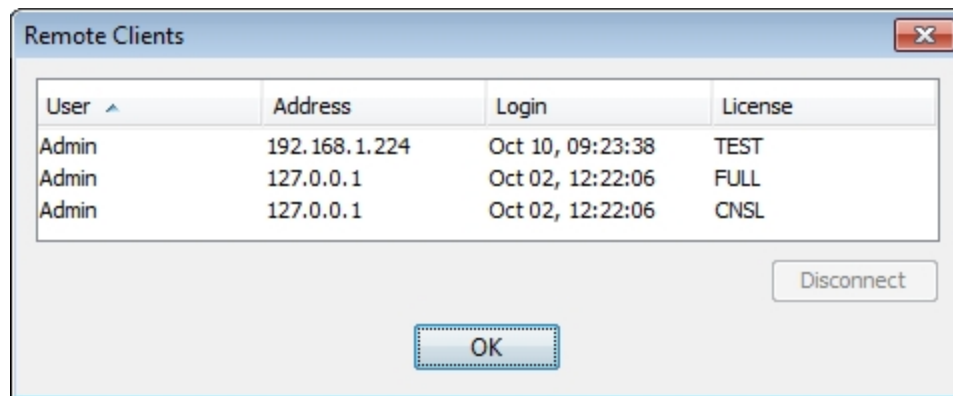
To configure the Remote Server:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
2. In the Server Configuration section, click **Remote Server**. The Remote Server panel appears.
 - Enter a TCP port number, or use the default value.
 - To configure access to the Remote Server, click the Plus icon to add addresses to the Remote Server firewall.
 - To remove an entry, click the entry, then click the Minus icon.
 - To edit an entry, click then entry, then click the Pencil tool.
 - To see a list of clients connected to the server, click **Show Connected Clients**. (See below)
 - If you want entries from this server to be sent to a different log file, choose a log file from the **Send log file entries to** dropdown menu. For more information on log files, see [Log Files \(Pg 257\)](#).

Note: The Server Settings window is available only to users who have administrator privileges.

Showing Connected Clients

Click Show Connected Clients to view a list of InterMapper clients connected to the server. The Remote Clients window appears, showing the connected user's name, IP address, time of login and type of license.



The screenshot shows a window titled "Remote Clients" with a close button (X) in the top right corner. Inside the window is a table with four columns: "User", "Address", "Login", and "License". There are three rows of data. Below the table is a "Disconnect" button, and at the bottom center is an "OK" button.

User ^	Address	Login	License
Admin	192.168.1.224	Oct 10, 09:23:38	TEST
Admin	127.0.0.1	Oct 02, 12:22:06	FULL
Admin	127.0.0.1	Oct 02, 12:22:06	CNSL

Additional Information

For more information on configuring your Remote Server, see [Server Access Control \(Pg 280\)](#). It describes how to set your Remote Server's port, discusses encryption and when to use it, and describes how to configure the built-in firewall's list of IP addresses.

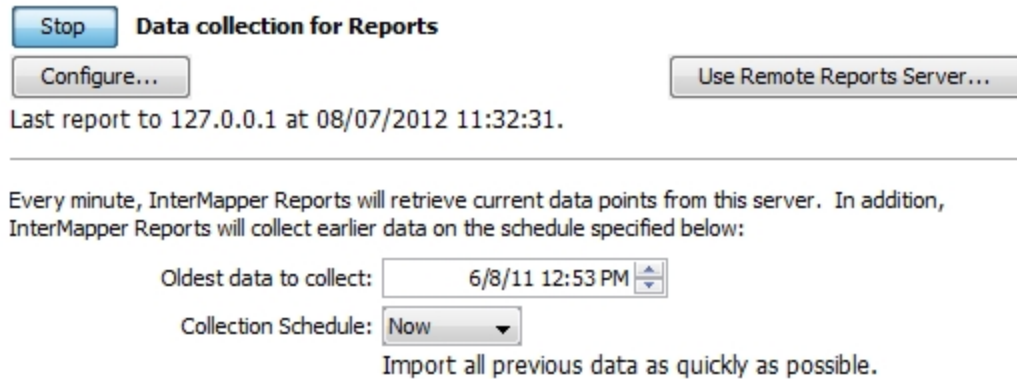
For more information on configuring your built-in servers' firewalls, see [Configuring a Firewall \(Pg 278\)](#).

For more information on users and groups, see [Users and Groups \(Pg 298\)](#). It describes how to set up users and groups, and how you specify who may use the Remote Server. It also discusses administrator access to the Remote Server.

For more information on setting permissions for a particular map, see [Controlling Access to a Map \(Pg 305\)](#). It describes how to set up unique access controls (by username) for an individual map.

Reports Server

The Reports Server stores data in a database for use in reports. Use the Reports Server panel, available from the Server Configuration section of the Server Settings panel, to specify the amount of data you want to store in the database.



Stop **Data collection for Reports**

Configure... **Use Remote Reports Server...**

Last report to 127.0.0.1 at 08/07/2012 11:32:31.

Every minute, InterMapper Reports will retrieve current data points from this server. In addition, InterMapper Reports will collect earlier data on the schedule specified below:

Oldest data to collect: 6/8/11 12:53 PM

Collection Schedule: Now

Import all previous data as quickly as possible.

InterMapper Reports Server Configuration pane

Setting up the Reports Server

If InterMapper DataCenter is running on the same host machine as InterMapper Server, the Reports Server is automatically configured, and you can start collecting data as soon as you start it.

If InterMapper DataCenter is installed on another host machine, you need to configure InterMapper to use that server.

To open InterMapper DataCenter and configure the Reports Server:

- Click **Configure...** For more about configuring the Reports Server, see [Configuring InterMapper DataCenter](#) for more information.

Starting Data Collection

You can start and stop collection of data on the Reports Server.

To start or stop collecting InterMapper data:

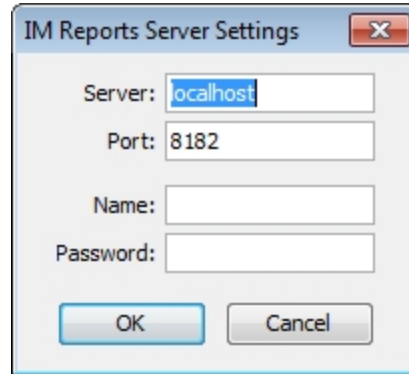
- Click **Start (Data collection for Reports)**.
- Click **Stop** to stop data collection.

Specifying an InterMapper Reports Server connection

If InterMapper DataCenter is running on a different host than the InterMapper Server, you must also specify the server, port, and an account login for the database you want InterMapper to use.

To configure the InterMapper Reports Server connection:

- From the Reports Server panel of the Server Settings window, click **Use Remote Reports Server...** and enter the information in the dialog InterMapper Reports Server Settings window as shown.



The image shows a dialog box titled "IM Reports Server Settings" with a close button (X) in the top right corner. It contains four input fields: "Server:" with the text "localhost", "Port:" with the text "8182", "Name:" which is empty, and "Password:" which is empty. At the bottom, there are two buttons: "OK" and "Cancel".

Collecting Current Data

Every minute, InterMapper Reports Server sends a request for a certain number of rows of current data to insert into the database. The request contains a start and end time, where the start time is the oldest data desired, and the end time is the newest (generally, the present time).

The response from InterMapper Server contains the rows to insert into the database, as well as the time of the next row to request. InterMapper Reports Server uses this information to update its notion of the current time, and the subsequent requests use that time.

The number of rows in the request is automatically adjusted so that the insertion process uses approximately half of the (one minute) time interval. Typically, 500 rows are requested for events and 25,000 rows are requested for data points.

If the time of the next row in the response is less than the requested end time, InterMapper Reports Server can tell that there is more data available.

Collecting Pre-Existing Data

In parallel, InterMapper Reports Server retrieves old (historical) data by working backwards (from newer to oldest), requesting data from the InterMapper Server. It does this by making requests for a set of data rows *older* than a particular time.

The InterMapper Server responds with those rows, and InterMapper Reports Server inserts them and updates the time of the next (oldest) row. Subsequent requests start at this time, and retrieve still older data rows.

Use the **Collection Profile** dropdown menu to specify the rate at which InterMapper Reports Server requests the historical data:

- **Now** - attempts to retrieve the historical data as fast as possible. It uses most of the remainder of the one-minute time interval (the time left after retrieving the current data) to request historical data. InterMapper Reports Server adjusts the number of rows in its request so that it will finish inserting in time to start the next current data request.
- **Gradually** - retrieves historical data between every other polls for current data.
- **Nightly** - only retrieves historical data between the hours of 1AM and 3AM. During this time period, it uses the "Now" profile.
- **Weekend** - retrieves historical data between the hours of 01:00 and 23:00 on Saturday and Sunday. During this time period, it uses the "Now" profile.
- **Never** - does not retrieve historical data at all.

What Data Gets Collected?

Certain variables for probes are recorded automatically when data is collected from a device by InterMapper Reports Server. You can also specify other variables you want to record when data for a device is stored.

For all probes, the following data is recorded:

- response time (in msec)
- long-term packet loss (%)
- input byte rates for all visible interfaces.
- output byte rates for all visible interfaces.

For built-in probes, Help/Systems has selected values that make sense to record for each probe.

For custom probes, you can specify which variables should be recorded. The syntax for this is described in *Recording Probe Data* in the Developer Guide.

The Web Server

InterMapper can act as a web server, publishing most of the information available from the InterMapper application.

Note: Before InterMapper will allow web connections, you must configure the web preferences as described in [Configuring a Firewall \(Pg 278\)](#). You must also make sure that any other firewalls protecting the InterMapper machine allow traffic to the port specified below.

You start, stop, and configure the Web Server from the Web Server panel, in the Server Configuration section of the Server Settings window, as shown below.

The screenshot shows the 'Web Server' configuration panel. At the top, there is a 'Stop' button and the title 'Web Server Listening On Port 80'. Below this, the URL is set to 'http://192.168.81.3:80'. A text field for 'Listen for connections on TCP port:' contains the value '80'. There is an unchecked checkbox for 'Use a secure protocol (SSLv3/TLS)'. A section titled 'Access Control List to Web Server based on IP Address:' contains a list with two entries: '192.168.81.*' with a green double-headed arrow icon, and '*.*.*.*' with a red 'X' icon. At the bottom of the list are icons for adding (+), removing (-), and editing (pencil). Below the list is a dropdown menu for 'Send log file entries to:' with 'Event Log' selected.

Stop **Web Server Listening On Port 80**

URL: <http://192.168.81.3:80>

Listen for connections on TCP port: 80

☐ Use a secure protocol (SSLv3/TLS)

Access Control List to Web Server based on IP Address:

- 192.168.81.*
- *.*.*.*

Send log file entries to: Event Log

Note: When configuring the InterMapper web server on a machine where IIS is also installed, do not use the default port 80. IIS uses port 80 by default, and this will prevent the InterMapper web server from starting.

To start, stop or configure the Web Server:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
2. In the Server Configuration section, click **Web Server**. The Web Server panel appears.
 - To start the Web Server, click **Start**.
 - To stop the Web Server when it is running, click **Stop**.
 - Enter a TCP port number, or use the default value.
 - To use a secure protocol, check the **Use a secure protocol (SSLv3/TLS)** box.
 - To configure access to the Web Server, click **Add...** to add addresses to the Web Server firewall. For more information on configuring firewalls, see [Configuring a Firewall \(Pg 278\)](#).
 - From the **Send log file entries to:** menu, choose a log file to which you want to send log entries.

Note: The Server Settings window is available only to users who have administrator privileges.

For more information on configuring your Web Server, see [Server Access Control \(Pg 280\)](#). It describes how to set your Web Server's port, discusses encryption and when to use it, and describes how to configure the built-in firewall's list of IP addresses.

For more information on users and groups, see [Users and Groups \(Pg 298\)](#). It describes how to set up users and groups, and how you specify who may use the Web Server. It also discusses administrator access to the Web Server.

For more information on setting permissions for a particular map, see [Controlling Access to a Map \(Pg 305\)](#). It describes how to set up unique access controls (by username) for an individual map.

Connecting to the Web Server

Once you have started the Web Server, a URL appears below the Web Server's **Stop** button. Click the URL, or enter the URL in a web browser. If the Web Server is configured correctly, the InterMapper Web Server's home page appears in your browser window.

The Telnet Server

InterMapper provides a telnet service that gives basic information about the devices being monitored as well as detailed information about the InterMapper server itself. Before InterMapper accepts Telnet connections, you must configure the Telnet Server firewall preferences as described in [Configuring a Firewall \(Pg 278\)](#).


You start, stop, and configure the firewall for the Telnet Server from the Telnet Server settings panel, in the Server Configuration section of the Server Settings window, as shown below:


Telnet Server Off




URL: *inactive*

Listen for connections on TCP port:

Access Control List to Telnet Server based on IP Address:

 192.168.1.*

 *.*.*.*

Send log file entries to:

To start, stop or configure the Telnet Server:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
2. In the Server Configuration section, click **Telnet Server**. The Telnet Server panel appears.
 - To start the Telnet Server, click **Start**.
 - To stop the Telnet Server when it is running, click **Stop**.
 - Enter a TCP port number, or use the default value.
 - To configure access to the Telnet Server, click **Add...** to add addresses to the Telnet Server firewall.

Note: The Server Settings window is available only to users who have administrator privileges.

For more information on configuring your Telnet Server, see [Server Access Control \(Pg 280\)](#). It describes how to set your Telnet Server's port, discusses encryption and when to use it, and describes how to configure the built-in firewall's list of IP addresses.

For more information on users and groups, see [Users and Groups \(Pg 298\)](#). It describes how to set up users and groups, and how you specify who may use the Telnet Server. It also discusses administrator access to the Telnet Server.

AutoMate

Use the AutoMate pane of the Server Settings window to enable and configure a connection to a local version of the AutoMate application.

AutoMate System

Name: Local AutoMate Server ☒ Enabled
 Host: localhost Port: 10011
 Password:
 Polling Interval: 0

Server System Tasks

	Event	Task	
<input type="checkbox"/>	Server startup		▲
<input type="checkbox"/>	Log file rotation		
<input type="checkbox"/>	Map backup comp...		
			▼

Name - Shows the name of the selected AutoMate server

Enabled - Select this box to allow InterMapper to request execution of AutoMate tasks on behalf of InterMapper's AutoMate notifiers to trigger AutoMate and Server System tasks.

Host - Currently, the AutoMate server must be running on the same machine as InterMapper Server.

Port - The port to use to connect to the AutoMate server.

Password - The default task password, if one is not supplied during task selection.

Polling Interval - The number of seconds to be used when polling the AutoMate server to check the status of a task. When set to zero, the polling interval increases over the length of time the task has been running.

Server System Tasks - Select the boxes for the system events you want to run AutoMate tasks. These include InterMapper system startup, completion of a scheduled map backup, and log file rotation.

Layer 2 Features

Use the Layer 2 Features panel to enable Layer 2 features and specify how you want to use them.

The Layer 2 features collect information about the connectivity of your ethernet switches. This information can be used to produce more complete maps.


☒ Enable Layer 2 features on this server [1 Maps Enabled](#)

Collect detailed information from SNMP devices on specific maps and use this information to calculate the Layer 2 topology of the network:

Last Updated: 12/13/11 10:32 AM

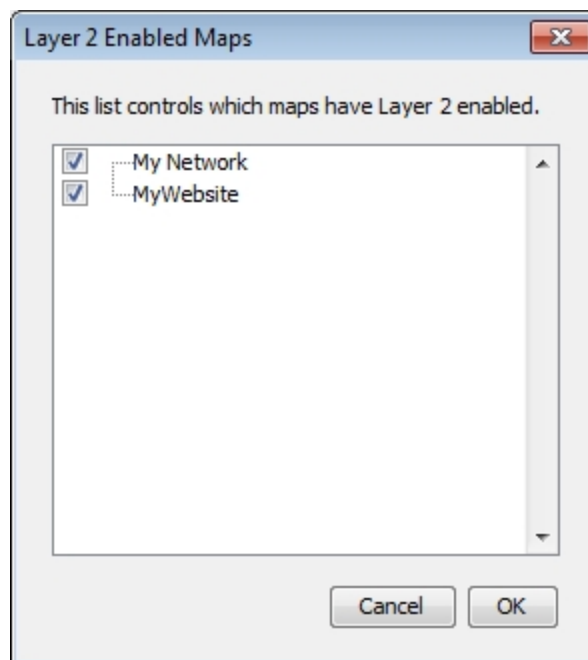
☒ Collect complete information about all devices on the network

☐ Limit Layer 2 discovery to CDP and LLDP only

 The selected option uses switch forwarding tables in conjunction with CDP, LLDP and other SNMP information to determine the connections between switches. On large networks, you may notice high CPU utilization on your switches and routers when the discovery process is running. We recommend that you use this option sparingly until you have determined how your devices respond.

Click to enable maps for Layer 2

- **Enable Layer 2 features on this server** - select this check box to turn on Layer 2 features.
- **[NN] Maps Enabled** - Click this link to choose the maps for which Layer 2 is enabled. The Layer 2 Enabled Maps window appears as shown below.



Note: In order to use the Layer 2 features in your map, *after* enabling Layer 2 features in the Server Settings window, you must enable them in the [Map Settings window](#) for each map that contains Layer 2 devices.

Discovery Options

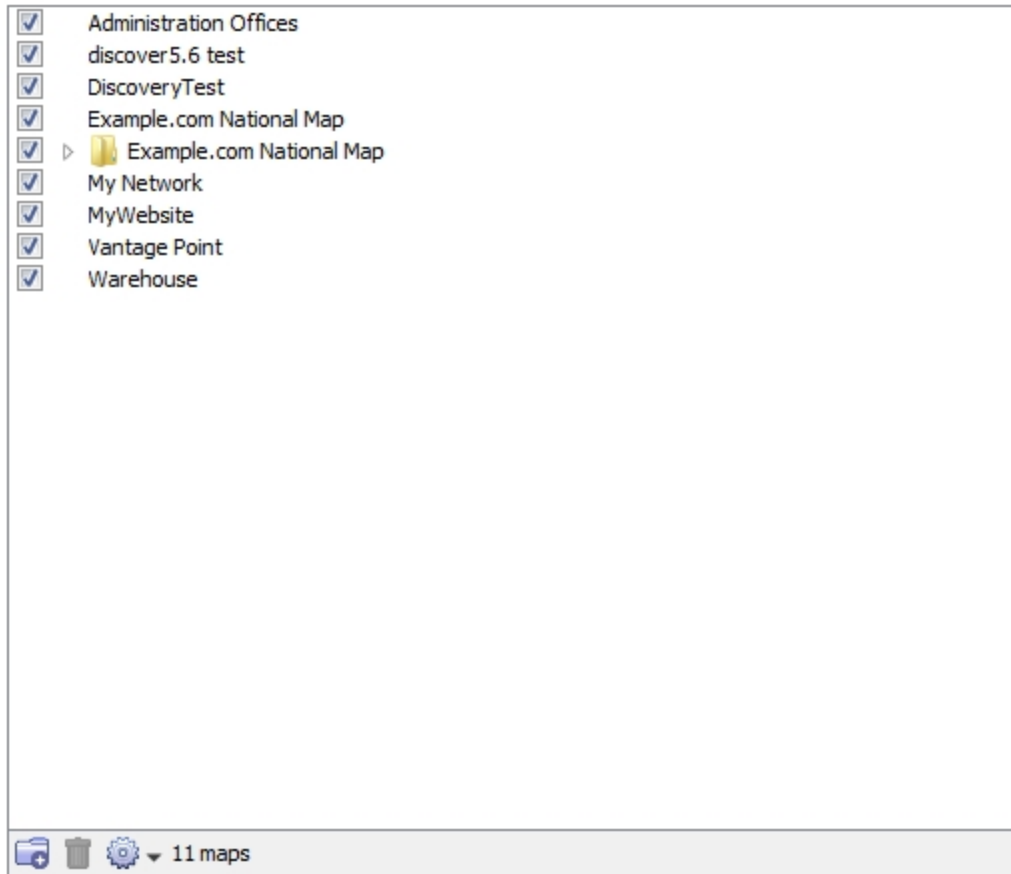
- **Layer 2 discovery period** - select a discovery period from the dropdown menu to specify how often to initiate discovery requests. Choose **Manually** to collect Layer 2 information only when you choose.
- **Now** - click the Now button to perform a discovery and collect Layer 2 data immediately.
- **Collect complete information about devices on the network** - select this option to collect detailed information from SNMP devices. This may place significant CPU load on your switches and routers during discovery.
- **Limit Layer 2 discovery to CDP and LLDP only** - select this option to request only CDP and LLDP information from Layer 2 devices. This option reduces the CPU load on your switches during the discovery process. It has the effect of limiting discovery only to switches.

Enabled Maps

Use the Enabled Maps panel of the Server Settings window to enable and disable maps, to remove maps, to organize them into folders, and to import and export them.

Select a check box to enable a map; clear the box to disable it.

Use the tools below to create folders, or to delete or perform other operations on selected maps. Drag maps into or out of folders.



- **Checked maps** - these maps are active. InterMapper actively polls everything on the map.
- **Unchecked maps** - these maps are not "active". InterMapper does not poll the devices on those maps.

The Enabled Maps panel lists available maps and shows which ones are enabled. From the Enabled Maps panel, you can do the following:

- **Enable or Disable a map.** Click the check box to the left of a map in the list to enable or disable it.
- **Import a map.** Click **Import...** to import data into InterMapper.
- **Export a map.** Click **Export...** to save the current map as an InterMapper map file on your local machine.
- **Duplicate a map.** Click to select a map, then click **Duplicate** to create a copy of it.

- **Remove a map.** Click to select a map, then click **Remove**. A confirmation window appears.
Note: When you remove a map, it is placed in the *Maps (Deleted)* folder.
- **Create a new Folder.** Click a map at the level you want to create the folder, then click **New Folder**. (see below)

Organizing Maps into Folders

From the Enabled Maps panel, you can create folders, and use them to organize your maps. This organization then appears in the Map List window.

To organize maps into folders:

1. If you want to create a folder in the top level of the map list, click any map at the top level, and click **New Folder**. A folder appears, with the name "Untitled". To create a folder within a folder, click the folder in which you want to create the new folder.
2. Enter a name for the new folder and press *Enter*. The folder's name changes to the specified name, and the folder moves to the correct alphabetic location in the list.
3. Drag maps into the folder.

Note: When you create a folder with the same name as a map at the same hierarchical level, a folder appears. Once the folder is created, when you double-click the folder in the Map List window, the map opens.

Map File Locations

Maps are stored in the following locations:

- Enabled maps are stored in the "InterMapper Settings/Maps/<version>/Enabled" folder.
- Disabled maps are kept in the "InterMapper Settings/Maps/<version>/Disabled" folder.
- When you delete a map, it is not discarded, but is placed in the "InterMapper Settings/Maps/Deleted" folder.

Note: While it is possible to place maps in the Maps folder using the file system, this is not recommended. If the server is running when you place the files in the folder, the map(s) are ignored and an error is logged when you go to the Server Configuration>Enabled Maps panel of the Server Settings window. Use the Enabled Maps panel's **Import Map** button to add maps to the Maps folder.

Users and Groups

Use the Users panel of the Server Settings window to [add](#) (Pg 300) and [edit](#) (Pg 301) users and [groups](#) (Pg 301), to [assign users to groups](#) (Pg 301), and to assign privileges and access to maps.

Note: The Server Settings window is available only to users who have administration privileges.

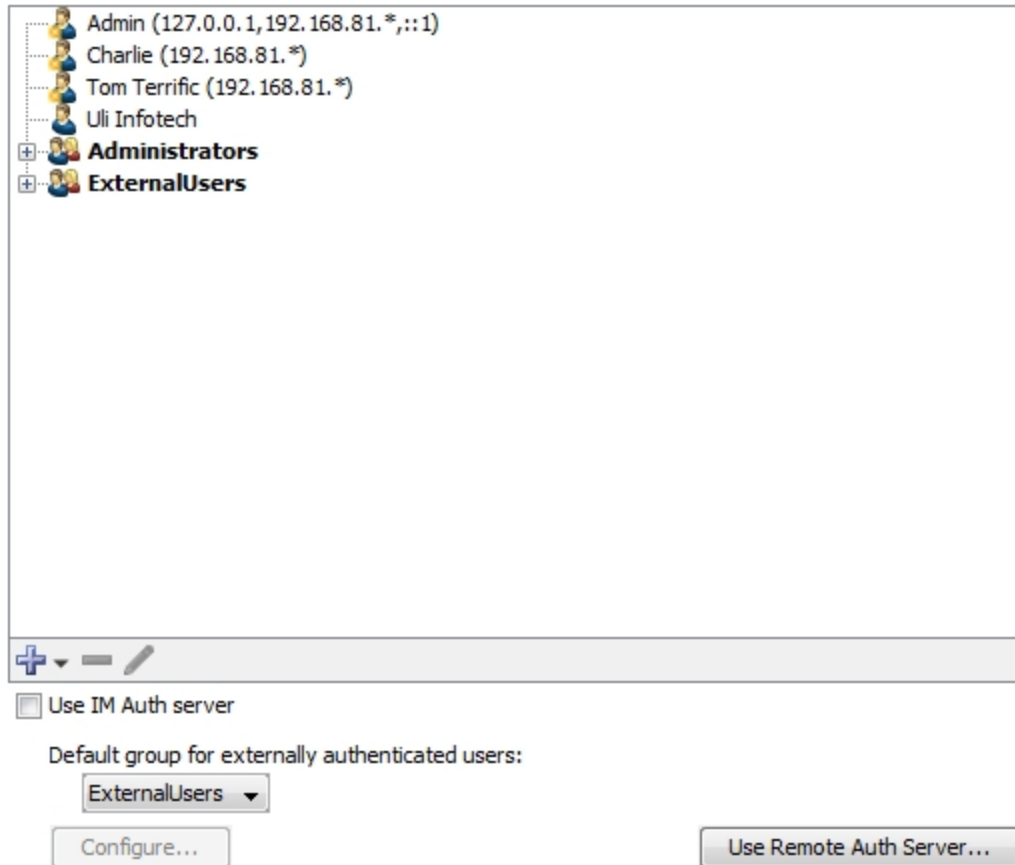
The Users Panel

Use the Users panel to maintain the list of users and groups allowed to access the various servers.

- To add a user, click **New User....**
- To add a group, click **New Group...**
- To remove a user or group, click to select the user or group, then click **Remove.**
- To edit a user or group's information, click to select the user or group, then click **Edit...**
- To use the [InterMapper Authentication server](#), select the **Use IM Auth Server** check box. Click **Configure...** to open the [InterMapper DataCenter](#) to set up the IMAuth Server.
- To use an Authentication Server on another computer, click Use **Remote Auth Server...**
- Choose a **Default group for externally authenticated users** from the dropdown menu.

The example below shows a typical user and group configuration in the Users panel of the Server Settings window.

This list shows the users and groups on the server.
Drag a user to a group to add it.



Setting up Users and Groups

What are Users and Groups?

- **User**
An individual identified by a user name and password, or identified automatically from a clients' IP address or range.
- **Group**
A collection of users. A group can be given permissions to access certain servers or maps, and may be given different levels of access for a server or map.

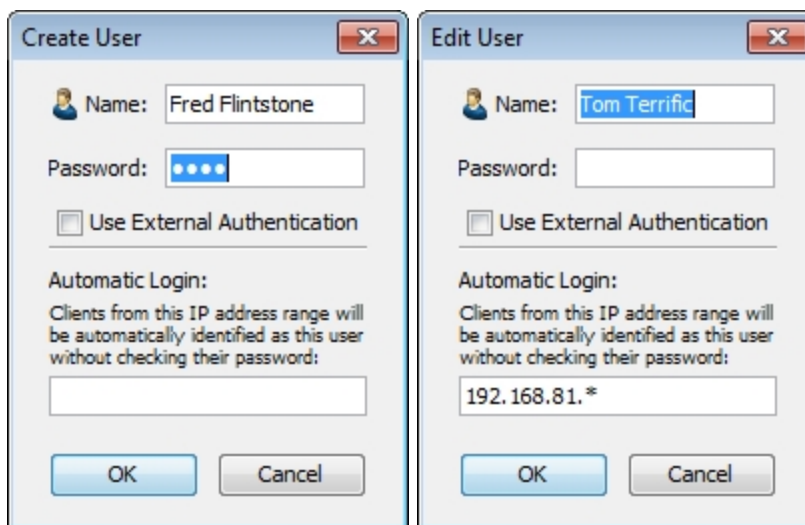
Creating a New User

To create a new user:

1. Click the **+** button and choose **Add User...** The User Information dialog appears, as shown in the two examples below.
2. Enter the name and password for the new user in the **Name** and **Password** text boxes.
or
Omit the password and enter an IP address range in the **Automatic Login** text box.
or
Select the **Use External Authentication** check box, and enter the user-name used by the external authentication server. No password is necessary; authentication is performed by the external authentication server.

How Automatic Login Works

- If a connection arrives from an address that matches the Automatic Login address, the person is automatically logged in as the specified user.
- If you supply both the password and automatic-login address, the person is logged in automatically from the specified address, but must supply a password when connecting from other addresses.
- Automatic-login addresses should be unique between users; the resulting Login name is not guaranteed if two automatic-login addresses are the same.
- For more information see [Controlling Access To Your Server \(Pg 280\)](#).



Creating a new user

These two examples show two different users. 'Fred Flintstone' must log in with a name and password, and 'Tom Terrific' is automatically identified when connecting from IP address 192.168.*.*.

Editing User Information

To edit the information about a user:

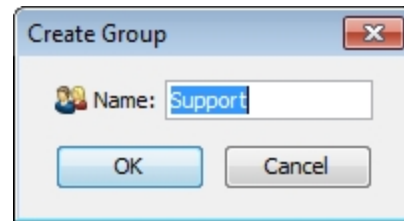
1. In the user list, click to select the user you want to edit.
2. Click **Edit...** or double-click the user entry. The User Information dialog appears, containing information for the selected user.

Managing Users and Groups

A group is a collection of users, all of whom have the same set of permissions.

To create a new group:

1. Click the **+** button and choose **Add Group...** The Group Information dialog appears, as shown above.
2. Enter the name of the new group.
3. Click **OK**. The new group appears in the User list.



New group window. Enter the name of the new group in this window.

Adding and Removing Group Members

To view the users in a group:

Click the plus sign (+) to the left of the group to expand it.

To add a user to a group:

Click and drag the user's entry to the group entry. The user appears in the list of users for that group.

To remove a user from a group:

1. Expand the group list to view the users in the group.
2. Click the entry for the user you want to remove, and click the **Remove** button. A confirmation dialog appears.
3. Click **OK**. The user is removed from the group.

Note: When you remove a user from a group, the user definition is removed only from the group, not from the user list. To remove a user completely from the list and all groups, see [Removing Users and Groups \(Pg 302\)](#) below.

Removing Users and Groups

To delete a user or group completely:

1. Click to select the user you want to remove.
2. Click the **Remove** button. A confirmation dialog appears.
3. Click **OK** to confirm. The user or group entry is removed from the list.

Note: The **Administrators** group is a special group that is always present, and cannot be removed.

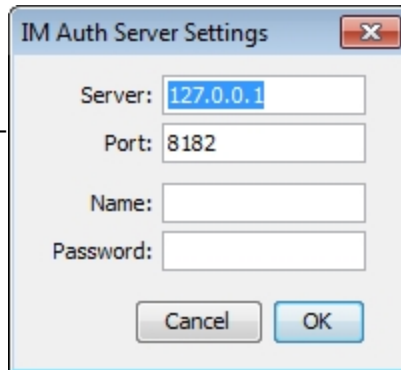
Note: The **FullWebAccess** group is a special group you define. If present, its members can view all web pages, and can acknowledge devices through the web server.

Note: The **FullLogAccess** group is a special group you define. If present, its members can view all log files.

Note: The **FullTelnetAccess** group is a special group you define. If present, its members have full access to the Telnet server.

Configuring the InterMapper Authentication Server

Click the **Use Remote Auth Server...** button to connect to an InterMapper Authentication Server installed on a different machine from InterMapper. For more information, see [Authentication Server \(Pg 623\)](#).

A screenshot of a dialog box titled "IM Auth Server Settings". It contains four input fields: "Server:" with the value "127.0.0.1", "Port:" with the value "8182", "Name:" which is empty, and "Password:" which is empty. At the bottom are "Cancel" and "OK" buttons.

Note: If the InterMapper Authentication Server is installed on the same machine as InterMapper, you need only check the **Use IM Auth Server** check box. The default server and port are used, and there is no need to enter a name or password.

Importing Users and Groups

Use the Import button to upload a file containing data for users and groups. For information on importing data, see [Importing Data \(Pg 637\)](#). For information on the User/Group data structure, see [User Attributes \(Pg 681\)](#).

Access Control Examples

Here are some typical access control configurations that might be used in different settings:

Allow connections from anywhere (no authentication)

1. From the Server Settings window, click a server (Remote Server, Web Server, or Telnet Server). A list of firewall entries appears in the right pane.
2. Add a firewall definition and set it to "Allow *.*.*.*."
3. From the [Users panel \(Pg 298\)](#), create a Guest account with an Automatic Login address of "*.*.*.*".

Note 1: This is a very open setting. Be sure that you actually intend to allow anyone to connect. This configuration might be reasonable if InterMapper were running behind a firewall, and thus not visible outside your organization.

Note 2: The IP wildcard example above works with 32-bit IPv4 address. InterMapper now supports 128-bit IPv6 addresses. Wildcard characters are not currently supported for IPv6 addresses.

Allow connections from anywhere, but with authentication

1. Define your user names and passwords as described in [Users and Groups \(Pg 298\)](#).
2. From the Server Settings window, click **Remote Server**. A list of firewall entries appears in the right pane.
3. Add a firewall definition and set it to "Allow *.*.*.*."

Anyone that connects is required to provide a username/password.

Allow web connections to see all maps

1. Define a group named **FullWebAccess**.
2. Add users to that group.

The users in the group can view all web pages, and can acknowledge down devices.

Allow people from known addresses to connect without entering a password

This is called an *automatic-login* user.

1. Create a new user with the desired name.
2. Leave the **Password** box empty.
3. Enter the desired IP address in the **Automatic Login** box.

All connections from that IP address or range are automatically connected, and are assigned the specified user name.

Allow a non-administrator user to see the log files

1. Define a group named FullLogAccess.
2. Add users to that group.

The users in the group can view all the log files.

Allow an automatic-login user name to connect from elsewhere by entering a password

- Create an [automatic-login user](#) (Pg 303) as described above, but enter a password.

When connecting from an IP address *within* the range specified for automatic login, the user is automatically connected and assigned the specified user name.

When connecting from an IP address *outside* the range specified for automatic login, the user is prompted for a user name and password.

Deny all connections from certain addresses or sites

You can prohibit connections from certain sites.

1. From the Server Settings window, click **Remote Server**. A list of firewall entries appears in the right pane.
2. Click **Add...** The Firewall Definition dialog appears.
3. In the **IP Address** box, enter an IP address or [IP address range](#) (Pg 278).
4. From the **Access** dropdown menu, choose **Deny**.
5. Click **OK**.

All connections from the specified IP address or range are denied.

Give a single user access to a specific map

1. From the Users tab, [create a new user](#) (Pg 278).
2. From the Maps tab, set the user's permissions for the Web and Remote servers.

These permissions are tested only if the user fails to match the global IP address test and/or username and password

Controlling Access to a Map

You can use the Map Access panel of the Server Settings window to authorize access to a map to one or more users or groups.

Note: All individuals in the Administrators group have access to all maps.

The Map Access Panel

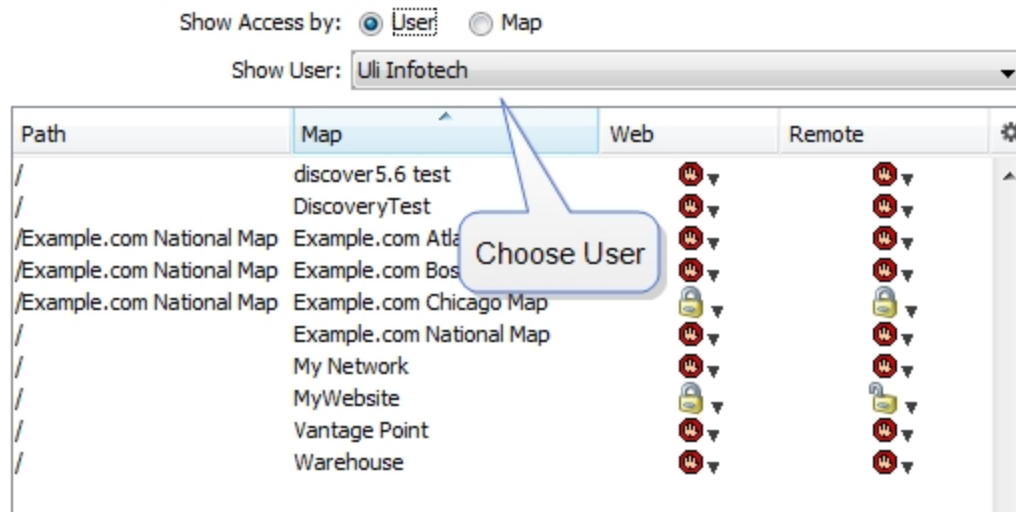
InterMapper lets you control the access rights to each map in two ways:

- **Control access by user** - View each user's rights to a particular map
- **Control access by map** - View each map's access rights for a particular user

The top example shows the list sorted per-user: it shows the rights that Crabby Appleton has for each of the maps. The bottom example shows the list sorted per-map: that is, it shows what access each user has to the Current Wireless Probes map.

Controlling Map Access by User

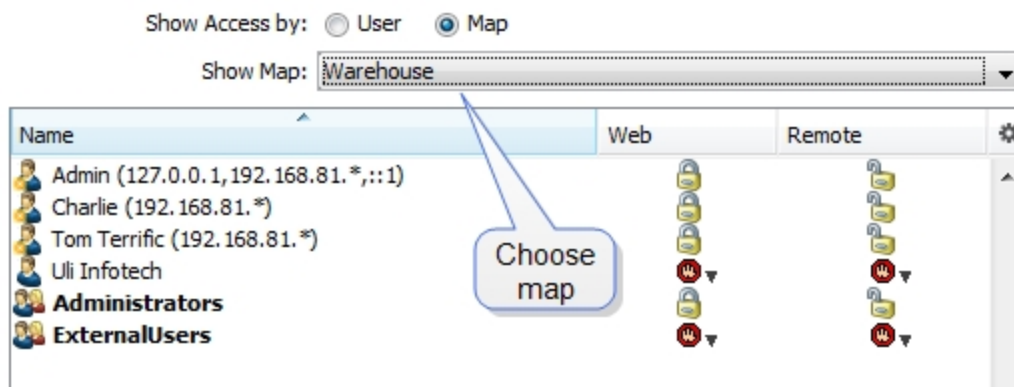
Choose **Show Access by: User** to control each map's access by a specific user through the Web and Remote servers.



- To set a user's access for any open map, choose the user from the **Show User** dropdown menu.
- To allow access to the selected map through the Web server, click the icon in the **Web** column for the user or group whose access permissions you want to set, then select a permission level.
- To allow access to the selected map through the Remote server, click the icon in the **Remote** column for the user or group whose access permissions you want to set, then select a permission level.

Controlling User Access by Map




Choose **Show Access by: Map** to control each user's access to a specific map through the Web and Remote servers.



- To set access control parameters for any open map, choose that map from the **Map Name** dropdown menu.
- To allow access to the selected map through the Web server, click the icon in the **Web** column for the user or group whose access permissions you want to set, then select a permission level.
- To allow access to the selected map through the Remote server, click the icon in the **Remote** column for the user or group whose access permissions you want to set, then select a permission level.

Map Access Permission Levels

Select a map's Web and Remote server access permission levels for each user or group as described below:

-  **No Access** Deny access to this map.
-  **Read-Only Access** Allow the user to view the map, but do not allow changes. (Access to the web server is always read-only.)
-  **Read-Write Access** Allow the user to view and edit the map.

Map Backup

Use the Map Backup panel of the Server Settings window to configure scheduled backups of your maps.


Define a schedule for automatic backup of all enabled maps.

☒ Enable scheduled backups

Days:

- ☐ All
- ☐ Sunday
- ☒ Monday
- ☐ Tuesday
- ☒ Wednesday
- ☐ Thursday
- ☒ Friday
- ☐ Saturday

Start time: 09:30 

Maximum backups: 2 

To schedule map backups:

1. Select the **Enable scheduled backups** check box.
2. Select the **Days** on which you want to schedule backups.
3. Set a **Start time** for the backup.
4. Specify a number of **Maximum backups**.

Scheduled backups appear in the Backup and Restore windows as "Scheduled". For more information, see [Backup...](#) section of the File Menu reference topic.

Notifier List

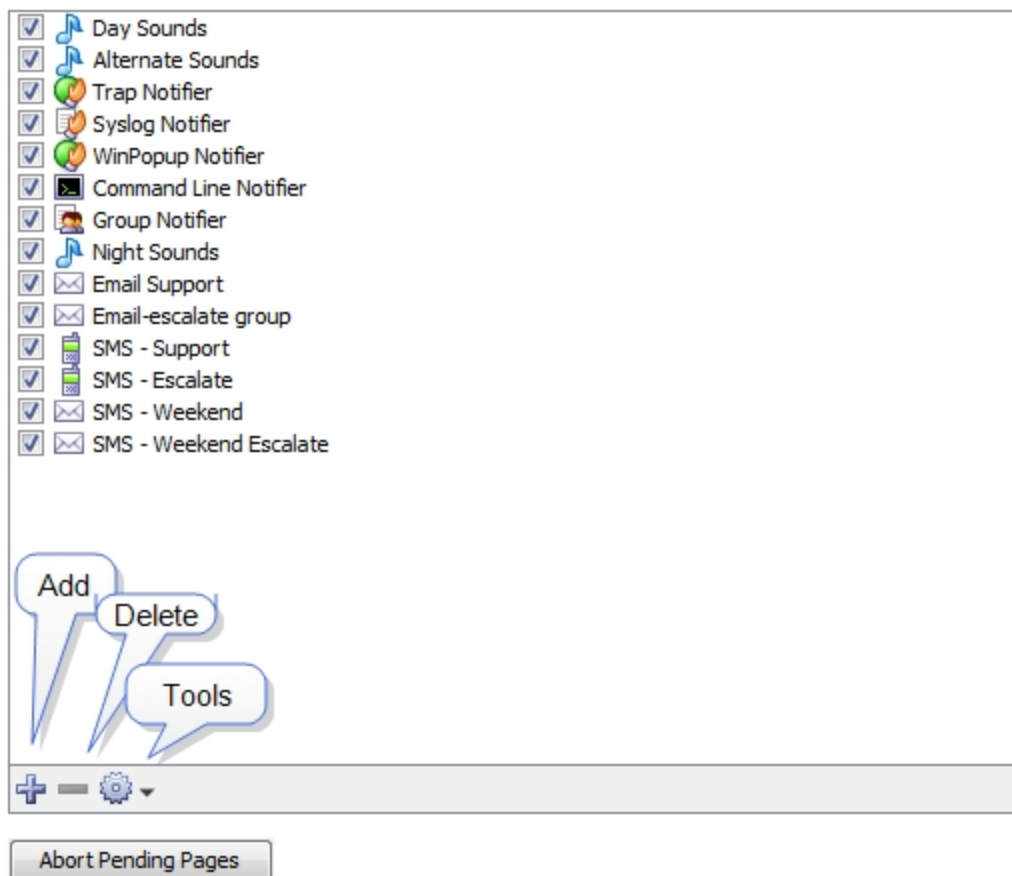
Use the Notifier List section of the Server Settings window to add, edit, copy and delete notifiers. For more information, see [Using Notifiers \(Pg 131\)](#).

To view and edit the Notifier List:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears, showing three sections on the left, each containing a list of available settings. On the right is a panel in which the selected settings appear.
2. Click **Notifier List**. A list of notifiers appears in the right panel of the Server Settings window.



A notifier sends an alert when the notifier is triggered by an attached device.

Uncheck a notifier to deactivate it for all devices (e.g., during vacation periods).



Notifier List Panel

From the Notifier List panel, you can do the following:

- **Add a notifier.** Click  The Configure Notifier window appears. For detailed information on configuring notifiers see [Configuring a Notifier \(Pg 131\)](#).
- **Edit an existing notifier.** Click to select the notifier you want to edit, then choose **Edit...** from the Tools dropdown menu. The Configure Notifier window appears, showing the current settings for the selected notifier.
- **Duplicate a notifier.** Click to select the notifier you want to duplicate, then choose **Duplicate** from the Tools menu. The Configure Notifier window appears, showing the current settings of the selected notifier, but with the name "<selected notifier> Copy."
- **Delete a notifier.** Click to select a notifier, then click minus (). A confirmation window appears.
- **Abort Pending Pages.** All messages sent to pagers still in process are terminated as soon possible, and any pages waiting to be sent are deleted. This affects only pages sent to Dialup Pagers; it has no affect on SNPP pages or other notifiers.

SSL Certificates

InterMapper's web and remote servers can employ a certificate to encrypt the data going between the server and clients. This assures that the client has connected to the actual server, and not another server acting as an impostor.

InterMapper ships with a certificate signed by Help/Systems Inc. This will work; the data is encrypted. But it's not using strong encryption (that is, it's easily broken) and web browsers using HTTPS connections will give a warning that there is a problem with the certificate, and that the data might be intercepted in transit.

To get stronger encryption and verification that the server is authentic, you can create and install your own SSL certificate. This is a three-step process:

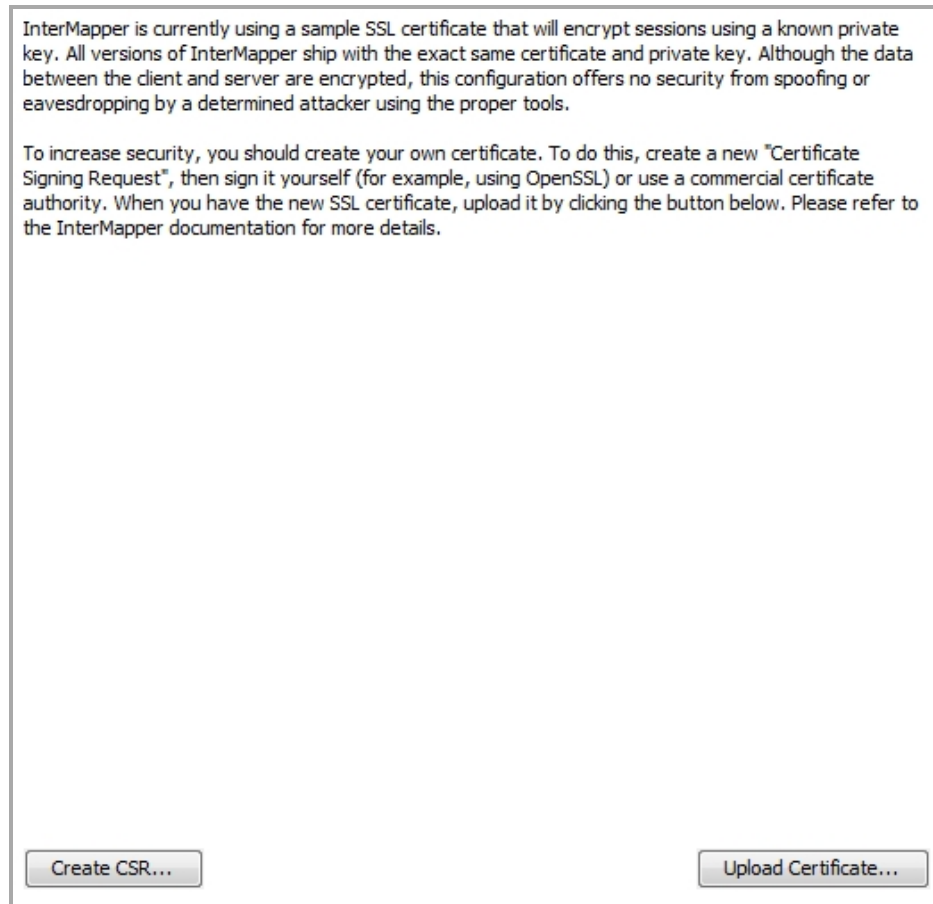
1. Create a Certificate Signing Request (CSR). The CSR contains all the information needed to identify the computer. InterMapper has a built-in function for collecting this information and building the certificate.
2. Sign the CSR. Signing is a process where an authority verifies the information in the certificate.
3. Upload the signed certificate into InterMapper to make it operational.

In either case, you must first create a Certificate Signing Request (CSR), which is a file that you can create using InterMapper. You then sign the CSR yourself, or send it to a commercial Certificate Authority to sign.

Use the SSL Certificate panel, available from the Server Configuration section of the Server Settings window to create a Certificate Signing Request, and to upload a signed certificate to the InterMapper server.

The remainder of this topic describes the three separate steps in detail.

The SSL Certificate Panel



Step 1: Create a Certificate Signing Request

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
2. In the Server Configuration section, click **SSL Certificate**. The SSL Certificate panel appears.
3. Click **Create new CSR...** The Certificate Signing Request window appears, as shown below.
4. Enter the required information as described below, and click **OK**. A 1,024-bit private key is generated for your computer, and the information is then used to create the Certificate Signing Request. The key and a copy of the CSR are saved in the *InterMapper Settings:Certificates* folder, and a standard Save File dialog appears.

You are being asked to save a copy of the CSR (with a filename of the FullyQualifiedDomainName.csr) on your disk. We recommend you save this on the desktop so it's easy to find when you create a signed certificate. After you have requested a signed certificate, you can discard this file.

5. Click **Save**. The new certificate is saved in the specified location.

Enter the following information for your Certificate Signing Request:

- **Common Name**
Enter your *full* DNS name or IP address of your server. If possible, it should include your domain name.
- **Organization**
Enter the name of your organization.
- **Organizational Unit**
If applicable, enter the name of an organizational unit within your organization, such as a department or division name.
- **Country**
Enter a two-letter abbreviation for your country
- **State or Province**
Enter a state or province name or abbreviation
- **City or Locality**
Enter a descriptive location of the server.
- **Make new private key**
The first time you generate a CSR, this box is dimmed. On subsequent uses, select this check box to create a new private key. Leave it unchecked to use the same private key.
- **Key Size**
Choose 1024 or 2048 bits.
- **Digest Type**
Choose SHA1 or SHA2. SHA1 is the default value.
- **Digest Size**
If you choose SHA2, choose 256 or 512 bits.

The Certificate Signing Request window.

When you click the OK button, InterMapper generates a private key for your computer, then use the information entered above to create the Certificate Signing Request. InterMapper will save following files in the *InterMapper Settings:Certificates* folder:

- **SSLCertificateKeyFile** contains your private key
- **Pending.csr** the Certificate Signing Request (CSR) file

You will also be asked to save another copy of the CSR (with a filename of the *FullyQualifiedDomainName.csr*) on your disk. We recommend you save this on the

desktop so it's easy to find when you are ready to create a signed certificate. You may discard this file after you have requested a signed certificate.

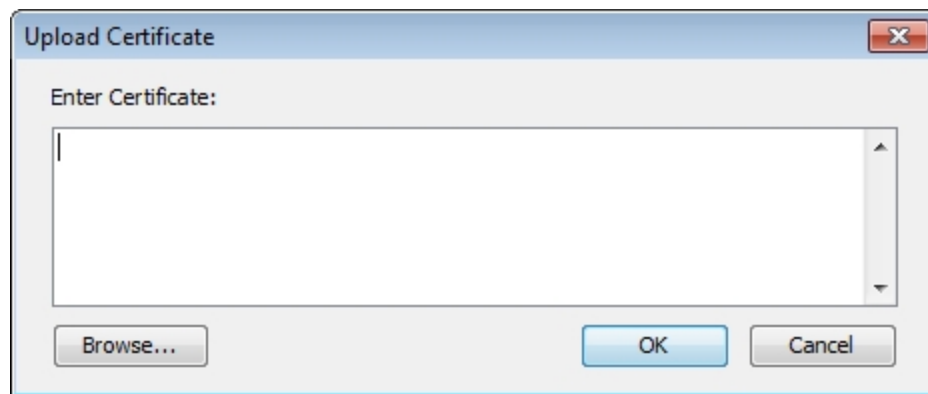
Step 2: Sign the Certificate

Once you have a CSR file, you must have it signed. There are two ways to do this:

1. You can use the OpenSSL software (available from <http://www.openssl.org>) or use the Windows CA to sign this CSR. This will create a self-signed certificate that you can easily use within your own organization.
2. You can send the CSR to any of several commercial certificate authorities, such as InstantSSL (<http://www.instantssl.com>), Verisign (<http://www.verisign.com/products/site/index.html>), or Thawte (<http://www.thawte.com>). These companies return a signed certificate that is globally-recognizable as authentic.

Step 3: Uploading the Signed Certificate

After the certificate has been signed, you can upload it using **Upload new Certificate...** Either copy and paste the text of the certificate into this window, or click **Browse...** and locate the certificate file on your hard drive.



At the conclusion of this, the InterMapper Settings:Certificates folder contains files named:

- **SSLCertificateKeyFile** contains your private key, created above.
- **SSLCertificateFile** contains your signed certificate (the file from Verisign, InstantSSL, or OpenSSL.) Be sure to remove any suffix (such as ".pem") from the file name.
- **SSLCACertificateFile** contains the public certificate chain of the signing CA's (in order).

Stop the affected server from the Server Settings window, and then start it again. These certificates are then used for HTTPS and InterMapper Remote client connections if the SSL/TLS boxes are checked in the respective server settings.

Using an externally generated CSR and Private Key

If you use a different application from InterMapper to create your Certificate Signing Request (CSR), InterMapper will not have access to the private key used to create the CSR. To upload your certificate with the private key, create one text file containing the signed certificate, the private key, and the CA's public certificate chain (if included), and use the "Upload new certificate..." button to upload this combined file.

Technical Notes

The design for this scheme is based on the SSL section of the Apache Mod-SSL `httpd.conf` file.

1. For InstantSSL, the `SSLCACertificateFile` is the same as the `ca-bundle` file, described in http://www.instantssl.com/ssl-certificate-support/cert_installation/
2. If there is no `SSLCertificateKeyFile`, InterMapper will look for the private key in `SSLCertificateFile`.
3. InterMapper will always load the additional CA certificates, if they exist, from `SSLCertificateFile` first, then it will check `SSLCACertificateFile` if it exists.
4. You can set up the configuration so one file, named `SSLCertificateFile`, contains everything. The file must contain a key, certification, and trust chain in that order, or the certificate is not imported properly.
5. InterMapper will convert CR's to LF's in the file data before loading it. There's no need to worry about CR-LF translation issues.

Chapter 9

InterMapper Flows™

InterMapper has always made it easy to see heavy traffic at a glance. Its charts show when traffic peaks, but not what it's used for.

InterMapper Flows™ is a feature of InterMapper that allows you to get deeper insight into the traffic on your network. It is a Flows analyzer that works with NetFlow, sFlow, JFlow, and cFlow, and can show the following:

- Top talkers and listeners
- Top protocols in use
- Top conversations and sessions
- Detailed session information to identify particular machines

How InterMapper Flows Works With InterMapper



InterMapper Flows collects and stores Flows data from any device that supports its collection (Flows Exporter). For information on supported devices, see [Supported Exporters \(Pg 333\)](#) You can choose the available exporters from which you want to collect data. For more information, see [Flows Settings - Exporters Tab \(Pg 334\)](#).

The Flows Window

Use the Flows window to view and analyze traffic at a very detailed level. InterMapper Flows acts as a NetFlow/sFlow collector; the Flows window provides a view of Flows data collected from supported hardware and software exporters.

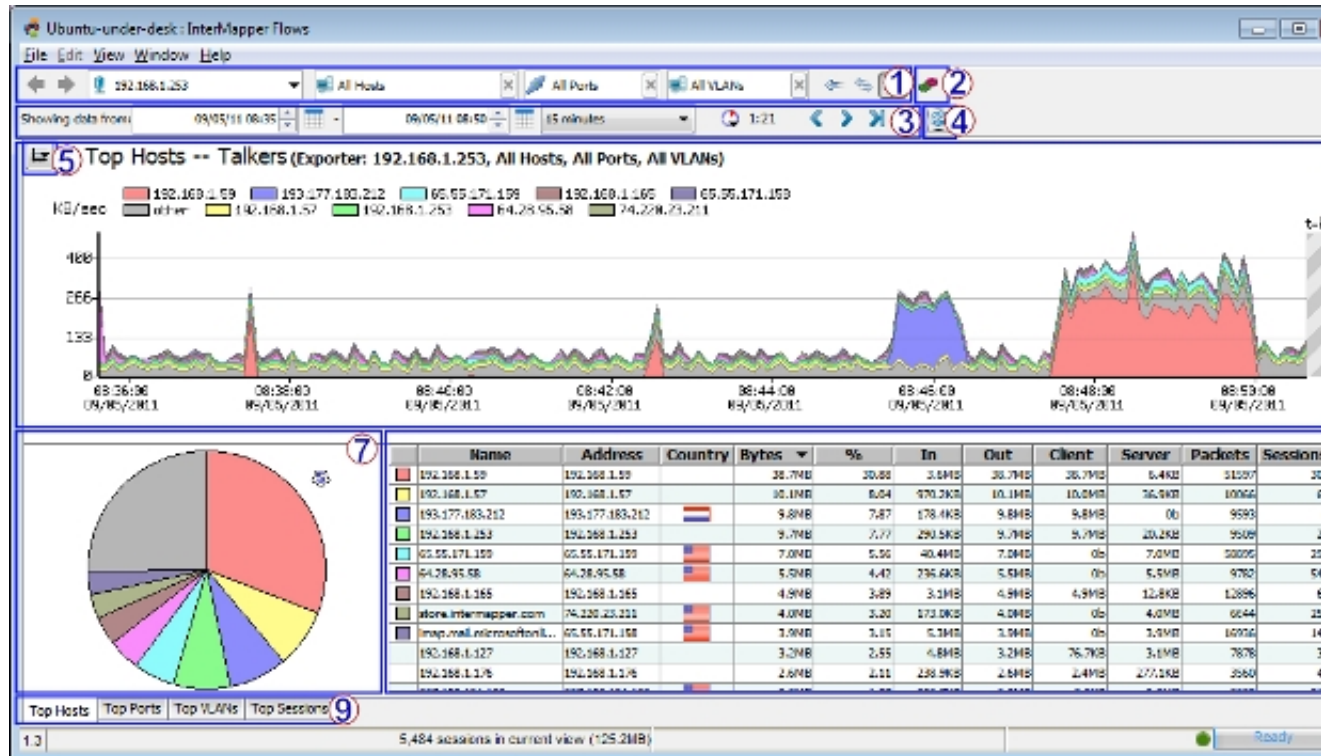


To open the Flows window:

- To see network traffic data from any device, **Right-click** or **ctrl-click** a device that shows an exporter badge and choose **Flows Window**.
Note: The Exporter badge appears for any device that is set up to be a Flows exporters. For more information, see [Flows Settings - Exporters Tab \(Pg 334\)](#).
- To see the traffic through an exporter's interface, **Right-click** or **ctrl-click** a link and choose **Flows Window** from the **Show In** submenu.

Understanding the Flows window

Use the Flows window to view Flows data in a number of ways.



When you first open the Flows window, the Hosts tab is selected.

- **1: Filter tools** (Pg 319) - select the subset of Flows data you want to view.
- **2: InterMapper Flows Settings** (Pg 334) - view and edit InterMapper Flows settings.
- **3: Time Range Selection tools** (Pg 321) - select and navigate Flows data over a specified period.
- **4: Refresh button** (Pg 321) - click to refresh the current view of Flows data.
- **5: Set Graph Scale** - choose a scale to use for viewing data in the Stack Chart.
- **6: Stack Chart** - view current Host, Port, or VLAN data in a stacked area chart.
- **7: Hosts, Ports, or VLANs pie chart** - view current Host, Port, or VLAN data as a percentage of total data flow in a pie chart.
- **8: Hosts, Ports, or VLANs list table** - view details about a specific host, port, or VLAN.
- **9: Page Selection tabs** - Click a tab to choose a Flows window page. (see below.)

Click a tab to choose one of these Flows window pages:

- [Top Hosts tab \(Pg 323\)](#) - view a list of top talkers, listeners, or both, with stack and pie charts showing the relative activity of each.
- [Top Ports tab \(Pg 327\)](#) - view a list of ports with the highest activity, with stack and pie charts showing the relative activity of each.
- [Top VLANs tab](#) - view a list of VLANs with the highest activity, with stack and pie charts showing the relative activity of each.
- [Top Sessions tab \(Pg 332\)](#) - view a list of sessions, with start and end IP addresses and the start and end time of each session.

Flow Type Icons

When collecting data from both NetFlow and sFlow exporters, you can tell at a glance what kind of exporter the data is coming from.



NetFlow



Data

This icon is shown when viewing data from a NetFlow exporter. Depending on the version, the icon shows a 1, 5, 7, or 9.



sFlow Data

This icon is shown when viewing data from an sFlow exporter.



J-Flow, CFlow

These exporters implement a Flows format that is identical to NetFlow v5, so they appear as NetFlow v5 in the Flows window.

Filter Tools

Use the filter tools to view a subset of the data, selecting from available exporters, talkers, listeners, ports or sessions collected by InterMapper Flows.



**Previous/
Next view**

Click the left arrow to view the current tab with a previous set of filters. If you have clicked a previous set of filters, click the right arrow to view the current tab with the next set of filters in the view history.



Exporter

Choose a different exporter from the dropdown menu to view traffic from that exporter. You can also choose a specific interface on an exporter from the dropdown menu.



Host

Enter an IP address or subnet (x.x.x.x/#) to view traffic from that host or subnet or choose from the dropdown menu. Enter an exclamation point (!) to exclude the specified host.



Port

Enter a port from the dropdown menu to view traffic from that port or choose from the dropdown menu. Enter an exclamation point (!) to exclude the specified port.



VLAN

Enter a VLAN number in the box to show Flows activity for only that VLAN. Enter an exclamation point (!) to exclude the specified VLAN.



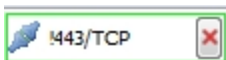
**Talkers/
Both/
Listeners**

Click the left arrow to view Top Listeners (receivers) only, the right arrow to view Top Talkers (senders) only, and the button with both arrows to view Top Hosts by the total traffic sent and received by each host.

Context Menu

Right-click or Ctrl-click an area of host activity in the Stack chart, Pie chart, or list and choose from the context menu. The menu changes depending on which area of the window you right-click.

Get more detail in the [Top Hosts](#)



**Exclude
Host/Port/VLAN**

(Pg 323), [Top Ports \(Pg 327\)](#), or [Top Sessions \(Pg 332\)](#) tab.

Enter an exclamation point (!) to negate a filter, or right-click (Ctrl-click) a host, port or VLAN in the pie chart or graph and choose ***Exclude***.

Negated filters are shown with green border.

Time Range Selection

Use the time range selection controls to view and select a range of time for which you want to view.



To select a time range:

- Select by dragging across an area of the stack chart.
- For precise control, enter times in the Showing data from Start and End time fields.
- Click the calendar icon to set a Start or End date.
- Use the dropdown menu to choose a preset time range. When you change this value, the current End time is preserved.
- Use the time navigation controls shown below to jump back or forward by the amount shown in the time range dropdown menu or jump to now.



Back in Time

Click the left arrow to view the previous page of data. The amount of data shown is determined by the current setting of the time range dropdown menu.



Forward in Time

Click the right arrow to view the next page of data. The amount of data shown is determined by the current setting of the time range dropdown menu.



Forward to Now

Click the Now button to view the latest data. The amount of data shown is determined by the current setting of the time range dropdown menu.



Zoom Out

Click the Zoom Out button to reset the time range to the most recent setting in the Time Range dropdown menu.



Refresh

Click the Refresh button to view the most recent data, based on the setting of the time range dropdown menu.



Auto-refresh Interval

Choose a refresh interval from the Auto-refresh dropdown menu.

Time until refresh

The time to the right of the Auto-refresh Interval button indicates the time until the next refresh of the window.

Reports and Settings



**Save
Report**

Click this button to save the report to disk. A standard file dialog appears. The report is saved in PDF format, and contains the Top Hosts, Top Ports, and Top Sessions tabs.



**Print
Report**

Click this button to print a report using the current time range and filter settings. A standard print dialog appears.



**Open
Settings
Dialog**

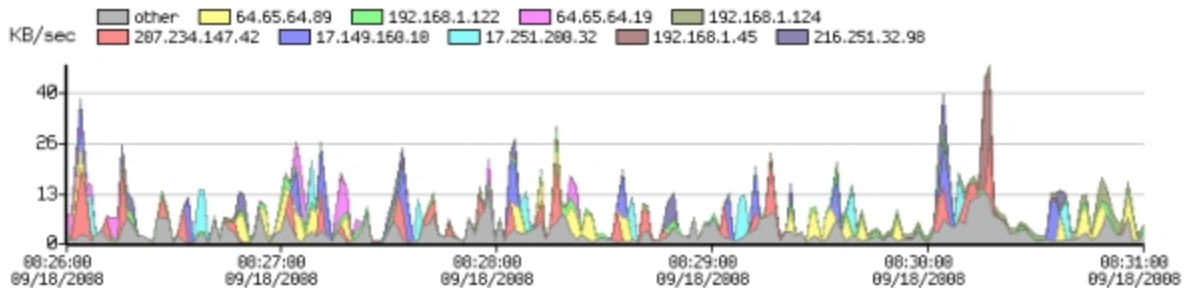
Click this button to open the InterMapper Flows Settings dialog. For more information, see the [InterMapper Flows Settings \(Pg 334\)](#) topic.

Top Hosts Tab

- Click the **Top Hosts** tab (or type **Ctrl-1**) to view a list of top talkers, listeners, or both, with stack and pie charts showing the relative activity of each.

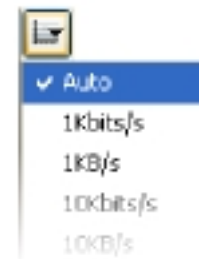
The Stack Chart

Use the Top Hosts tab's Stack chart to view the relative activity of different hosts over time. Each host's activity is stacked with the others, with the top host on the bottom of the stack. Here's a typical stack chart:



The legend above the chart shows the top hosts for the data you are currently viewing.

- Click a legend (above the Stack chart) to select the corresponding line in the Host list.
- Mouse over an area of the Stack chart to view the host address for that activity.
- Click an area of the stack chart to select the corresponding line in the Host list.
- Click and drag to select a region of the chart to reset the time range to that area of the Stack chart.
- Click the **Set Graph Scale** button to set the vertical scale for the Stack chart. Choose **Auto** to normalize the scale to the displayed data, or select a scale between 1Kbits/second and 10GBytes/second.
- Right-click an area of the Stack chart and choose from the context menu as described below.



The Pie Chart

Use the Pie chart to view the relative activity of each top host in proportion to the others.















- Click a pie segment to select the corresponding line in the Host list.
- Mouse over a pie segment to view the host address for that segment.
- Right-click an area of the Pie chart and choose from the context menu as described below.



The Host List

Use the Host List to view detailed statistics about a particular host. Below is a typical host list, which shows the top 25 hosts.

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click an unselected row to select it.
- Shift-click an unselected row to select all rows between that row and the currently selected row.
- Control-click a row to select or de-select it.
- Right-click a line or IP address from the Host list, and choose from the context menu as described below.

Legend	Hostname	Address	Country	Bytes	%	In	Out	Client	Server
	207-234-147-42.ptr.example.com	207.234.147.42		385.5K	13.03	41.7KB	385.5K	3.9KB	381.6KB
	example.net	64.65.64.89		343.3K	11.61	35.2KB	343.3K	0b	343.3KB
	nwk-www.example.com	17.149.160.10		267.7KB	9.05	12.9KB	267.7KB	0b	267.7KB
	dhcp-122.dartware.com	192.168.1.122		223.0KB	7.54	1.1MB	223.0KB	217.5KB	5.5KB
	cup-www.example.com	17.251.200.32		189.9KB	6.42	8.1KB	189.9KB	0b	189.9K
	vws.example.net	64.65.64.19		142.3K	4.81	17.2KB	142.3K	0b	142.3KB
	nitro.dartware.com	192.168.1.45		141.1KB	4.77	670.4KB	141.1KB	74.2KB	66.9KB
	dhcp-124.dartware.com	192.168.1.124		125.1KB	4.23	76.6KB	125.1KB	83.9KB	41.2KB
	host-ing.example.com	216.251.32.98		115.8KB	3.91	8.5KB	115.8KB	0b	115.8KB
	eclair.example.net	64.65.64.64		98.1KB	3.32	18.8KB	98.1KB	0b	98.1KB
	out-going02.example.net	64.65.64.125		69.2KB	2.34	26.0KB	69.2KB	0b	69.2KB
	192.168.1.12	192.168.1.12		63.3KB	2.14	67.8KB	63.3KB	25.5KB	37.8KB
	<up to 25 rows>								
	Other	Other		396.5KB	13.40	555.8KB	396.5KB	118.5KB	278.0KB

- **Legend** - The top 10 hosts are indicated with color legends. The report shows the top 25 hosts or ports, but places the "Other" category at the bottom of the list, as it shows total traffic for the remaining hosts or ports not shown in the

previous 24 rows.

- **Hostname** - Contains the host name of the talker or listener.
- **Address** - Contains the IP address of the talker or listener.
- **Country** - Contains a flag indicating the country in which the host name or IP address originates.
- **Bytes** - The volume of traffic (in bytes/kbytes/mbytes) for a particular row in the specified time interval.
- **%** - The percentage of traffic attributed to this host during the specified time interval.
- **In** - The number of bytes received by the host's IP address.
- **Out** - The number of bytes sent from the host IP address.
- **Client** - The number of bytes transmitted when the host was acting as a client (for example, sending a request to another server.)
- **Server** - The number of bytes transmitted when the host was acting as a server (for instance, when responding to a request from a client.)

Note: InterMapper Flows uses heuristic rules to determine which host is operating as a client or server:

- It has a built-in list of common server ports. If the port matches an entry in the list, it is treated as a server.
 - If there is no match with a common host port, the lower-numbered port is treated as a server.
- **Packets** - The number of packets sent or received by this host.
 - **Sessions** - The number of sessions including this host.

Context Menu - Top Hosts tab

Right-click or CTRL-click (Mac) on the Stack chart, Pie chart, or Host list, and choose from the Context menu as follows:

Stack chart:

- **Select On [host]** - include only traffic from the selected host.
- **Exclude [host]** - exclude traffic from the selected host.
- **Center on this** - centers the stack chart on the selected point in the timeline.

Pie chart:

- **Select On [host]** - include only traffic from the selected host.
- **Exclude [host]** - exclude traffic from the selected host.

Hosts List:

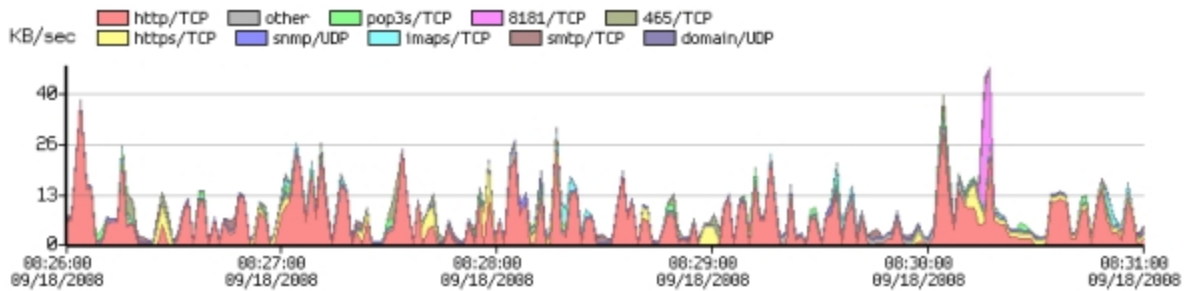
- **Select All** - select all rows of the table
- **Filter on selected host** - include only traffic to or from the selected host
- **Exclude selected host** - exclude traffic from the selected row
- **Copy selected rows** - copy the fields from the selected table rows to the clipboard
- **Copy IP address** - copy only the IP address from the selected row to the clipboard
- **Whois Lookup** - see the Whois description for the selected host.

Top Ports Tab

- Click the **Top Ports** tab (or type **Ctrl-2**) to view a list of ports with the highest activity, with stack and pie charts showing the relative activity of each.

The Stack Chart

Use the Top Ports tab's Stack chart to view the relative activity of different ports over time. Each port's activity is stacked with the others, with the top port on the bottom of the graph. Here's a typical stack chart:

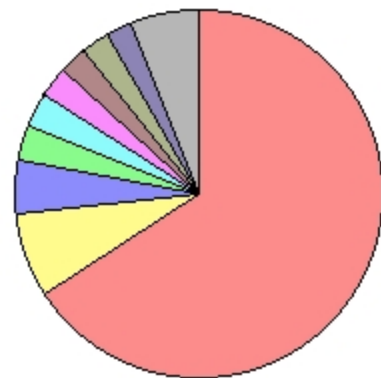


- Click a legend above the Stack chart to select the corresponding line in the Port list.
- Mouse over an area of the Stack chart to view port information for that activity.
- Click an area of the stack chart to select the corresponding line in the Port list.
- Click and drag to select a region of the chart to reset the time range to that area of the Stack chart.
- Click the **Set Graph Scale** button to set the vertical scale for the Stack chart. Choose **Auto** to normalize the scale to the displayed data, or select a scale between 1Kbits/second and 10GBytes/second.
- Right-click an area of the Stack chart and choose from the context menu as described below.

The Pie Chart

Use the Pie chart to view the relative activity of each top port in proportion to the others.

- Click a pie segment to select the corresponding line in the Ports list.
- Mouse over a pie segment to view the port corresponding to that segment.
- Double-click a segment of the pie chart to set a filter allowing you to view data only for the selected port.
- Right-click or Ctrl-click a point in the timeline and choose **Center on This** from













the context menu to bring a particular point in the Stack chart to the center of the timeline.

- Double-click a pie segment, or right-click or Ctrl-click a segment and choose **Select on Port/Protocol [Service or Port number]** from the context menu to set a filter for that port.
- Right-click an area of the Stack chart and choose from the context menu as described below.

The Ports List

Use the Ports List to view detailed data about the top 25 ports.

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click an unselected row to select it.
- Shift-click an unselected row to select all rows between that row and the currently selected row.
- Control-click a row to select or de-select it.
- Right-click or Ctrl-click a row and choose **Select All** to select all rows.
- Right-click a selected row and choose **Copy Selected Rows** to copy the currently selected set of rows to the clipboard in tab-delimited format.

Legend	Service	Protocol	Port	Bytes	%
	HTTP	TCP	80	1.9MB	65.76
	HTTPS	TCP	443	223.8KB	7.57
	SNMP	UDP	161	134.8KB	4.56
	POP3S	TCP	995	92.8KB	3.14
	IMAPS	TCP	993	89.6KB	3.03
	8181	TCP	8181	78.3KB	2.65
	SMTP	TCP	25	74.0KB	2.50
	465	TCP	465	72.2KB	2.44
	DOMAIN	UDP	53	68.8KB	2.33
	1278	UDP	1278	41.6KB	1.40
	ICMP	ICMP		22.7KB	0.77
	1220/TCP	TCP	1220	17.1KB	0.58
	106/TCP	TCP	106	11.6KB	0.39
< up to 25 rows >					
	OTHER	IP		13.4KB	0.45

- **Legend** - The top 10 ports are indicated with colored legends. The report shows the top 25 ports, but places the "Other" category at the bottom of the list, as it shows total traffic for the remaining ports not shown in the previous 24 rows.
- **Service** - Contains the name of the server associated with the port.
- **Protocol** - Contains the protocol (TCP/UDP/GRE/ICMP) associated with the port.
- **Port** - The port number
- **Bytes** - the volume of traffic (in bytes/kbytes/mbytes) for a particular row in the specified time interval.

- **%** - the percentage of that traffic for the specified port in the specified time interval.

Context Menu - Top Ports tab

Right-click or CTRL-click (Mac) on the Stack chart, Pie chart, or Ports list, and choose from the Context menu as follows:

Stack chart:

- **Select On [port]** - include only traffic from the selected port.
- **Exclude [port]** - exclude traffic from the selected port.
- **Center on this** - centers the stack chart on the selected point in the timeline.

Pie chart:

- **Select On [port]** - include only traffic from the selected port.
- **Exclude [port]** - exclude traffic from the selected port.

Ports List:

- **Select All** - select all rows of the table
- **Filter on selected port** - include only traffic to or from the selected port
- **Exclude selected port** - exclude traffic from the selected row
- **Copy selected rows** - copy the fields from the selected table rows to the clipboard
- **Copy IP address** - copy only the IP address from the selected row to the clipboard
- **Whois Lookup** - see the Whois description for the selected port.

Top VLANs Tab

Click the **Top VLANs** tab (or type **Ctrl-3**) to view a list of VLANs with the highest activity, with stack and pie charts showing the relative activity of each.

The Pie Chart

Use the Pie chart to view the relative activity of each top VLAN in proportion to the others.











- Click a pie segment to select the corresponding line in the VLAN list.
- Mouse over a pie segment to view the percentage of traffic for that VLAN.
- Right-click an area of the Pie chart and choose from the context menu as described below.



The VLAN List

Use the VLAN List to view detailed statistics about a particular VLAN.

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click an unselected row to select it.
- Shift-click an unselected row to select all rows between that row and the currently selected row.
- Control-click a row to select or de-select it.
- Right-click a line in the VLAN list, and choose from the context menu as described below.

Legend	VLAN	Bytes	%
	0	385.5K	13.03
	1	343.3K	11.61
	2	267.7K	9.05
	3	223.0K	7.54
	4	189.9K	6.42
	5	142.3K	4.81
	6	141.1K	4.77
	7	125.1K	4.23
	8	115.8K	3.91
	9	98.1K	3.32
	10	69.2K	2.34
	11	63.3K	2.14
<up to 25 rows>			
	Other	396.5KB	13.40

- **Legend** - The top 10 VLANs are indicated with color legends. The report shows the top 25 VLANs, but places the "Other" category at the bottom of the list, as it shows total traffic for the remaining VLANs not shown in the previous 24 rows.
- **VLAN** - Contains the number of the VLAN.
- **Bytes** - The volume of traffic (in bytes/kbytes/mbytes) for a particular row in the specified time interval.
- **%** - The percentage of traffic attributed to this VLAN during the specified time interval.

Context Menu - Top Hosts tab

Right-click or CTRL-click (Mac) on the Stack chart, Pie chart, or Host list, and choose from the Context menu as follows:

Stack chart:

- **Select On VLAN [NN]** - include only traffic from the selected host.
- **Exclude VLAN [NN]** - exclude traffic from the selected host.
- **Center On This** - centers the stack chart on the selected point in the timeline.

Pie chart:

- **Select On VLAN [NN]** - include only traffic from the selected host.
- **Exclude VLAN [NN]** - exclude traffic from the selected host.

VLANs List:

- **Filter on selected VLAN** - include only traffic to or from the selected VLAN.
- **Exclude selected VLAN** - exclude traffic from the selected row.
- **Select All** - select all rows of the table.
- **Copy selected rows** - copy the fields from the selected table rows to the clipboard.

Top Sessions Tab

- Click the **Top Sessions** tab (or type **Ctrl-4**) to view a list of sessions, with client and server IP addresses and the start and end time of each session.

Use the Top Sessions tab to view detailed data about sessions with the greatest amount of traffic.

- **Client** - The IP address or host name of client in the session.
- **Server** - The IP address or host name of the server to which the session is connected.
- **Service** - The service being used during the session.
- **Total Bytes** - The total number of bytes sent and received during this session.
- **Client Port** - The port number used by the session's client.
- **Server Port** - The port number used by the session's server.
- **Protocol** - The protocol (TCP/UDP/GER/ICMP) used during the session.
- **Client Packets** - The total number of packets sent by the client during this session.
- **Client Bytes** - The total number of bytes sent by the client during this session.
- **Server Packets** - The total number of packets sent by the server during this session.
- **Server Bytes** - The total number of bytes sent by the server during this session.
- **Start Time** - The session's start time. If the session started before the start of the time range currently being viewed, the start time is shown in a different color.
- **Last Update** - The time of the last packet sent or received during the session. If the session ended before the start of the time range currently being viewed, the Last Update time is shown in a different color.
- **Exporter** - The IP address of the exporter that recorded the session.
- **In** - The index of the device interface through which the client packets entered.
- **Out** - The index of the device interface through which the server packets entered.
- **VLAN In** - The number of the VLAN used for incoming packets.
- **VLAN Out** - The number of the VLAN used for outgoing packets.

Sorting the Sessions List

You can sort the Sessions list by any column.

To sort the Sessions list:

- Click a column heading to sort by that column.
- Click again to reverse the sort.

Supported Exporters

NetFlow: InterMapper Flows handles NetFlow v1, v5, v7, and v9 exports from routers and switches from Cisco and other NetFlow-compatible vendors as well as a number of software exporters.

sFlow: InterMapper Flows handles sFlow versions 2, 4, and 5, including MIB Enterprise numbers 4300 and 14706 from equipment from HP, Extreme, Foundry, Force10, and others.

J-Flow, CFlow: Identical to NetFlow v5, implemented by different vendors. The NetVlow v5 icon appears when using these exporters

Using InterMapper Flows with sFlow

sFlow provides information about the traffic through the network, including the sender and recipient of the traffic flows and the protocols used.

To configure InterMapper Flows to receive the sFlow data, you must first enable sFlow export on the router or switch. Most modern gear uses SNMP to enable/disable sFlow export, as described in the [sFlow specification](#).

InterMapper Flows lets you specify the exporter(s) that should send data.

To add an sFlow exporter:

1. Open the Flows Settings window, and click the Exporters tab.
2. Set the sFlow port (default is 6343) at the bottom of the window.
3. Click the **Add sFlow exporter** button. The Enter sFlow Information window appears.
4. Enter the IP address of the exporter, the SNMP read/write community string, choose the IP address for the collector, choose a sampling rate, and click OK. InterMapper Flows configures the selected exporter (via SNMP) to send sFlow records to the specified collector. The exporter appears in the Exporters list in a few moments.

InterMapper Flows Settings

Use the Flows Settings window to view and edit settings for InterMapper Flows.

To open the Flows Settings window:

- Click the Settings icon in the top-right corner of the Flows window:

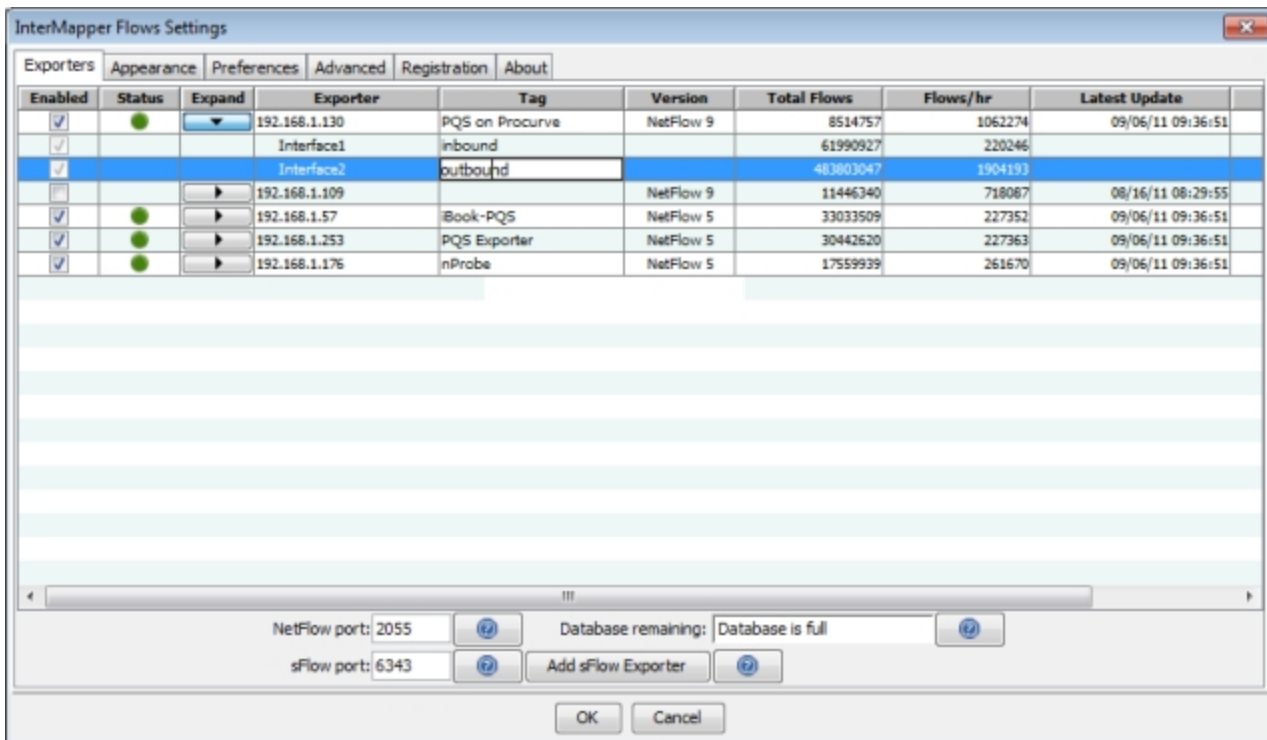


The following tabs are available in the Settings window:

- Use the [Exporters \(Pg 334\)](#) tab to choose which exporters you want to collect from.
- Use the [Appearance \(Pg 337\)](#) tab to select a coloring theme for protocols and hosts.
- Use the [Preferences \(Pg 338\)](#) tab to set parameters that control behavior of InterMapper Flows.
- Use the [Advanced \(Pg 339\)](#) tab to set performance-related parameters, the path to your database, and a database size.
- Use the [Registration \(Pg 341\)](#) tab to view information about your current InterMapper Flows license, and to enter a new license key.
- Use the [About \(Pg 342\)](#) tab to view version information about InterMapper Flows and its components.

Exporters tab

Use the Exporters tab to select the exporters from which you want to collect data.



Choosing and Adding Exporters

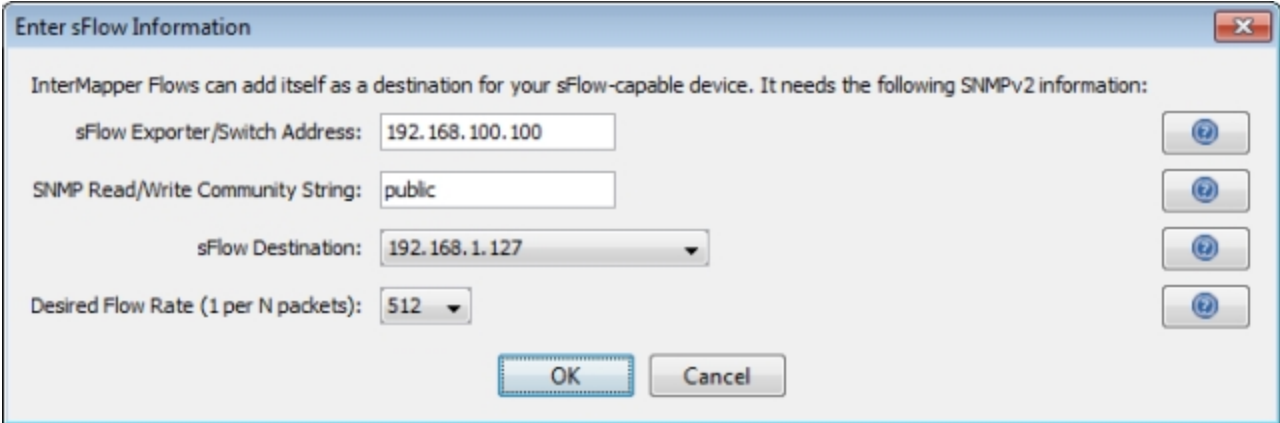
The Exporters tab lists all available exporters.

To choose exporters:

- To enable or disable collection and analysis of data from an exporter, select or clear the **Enabled** check for an exporter.

Note: NetFlow exporters appear in the list automatically if they are properly configured. The exporter must be configured to send data to InterMapper Flows.

- To add an sFlow exporter, click **Add sFlow Exporter**. The Enter sFlow Information window appears as shown below. Enter information about the exporter, then click OK. InterMapper Flows sends SNMP commands to the exporter to turn on sFlow.



Enter information as follows:

- **sFlow Exporter/Switch Address** - enter the address of an SNMPv2-capable sFlow exporter.
- **SNMP Read/Write Community String** - enter the community string for the exporter.
- **sFlow Destination** - the address of the InterMapper Flows collector. Your server may have multiple network devices, each with its own IP address. InterMapper Flows makes its best guess as to which IP address should be listed as your sFlow collector, but it may guess wrong. If the exporter isn't registered correctly, try a different IP address.
- **Desired Flow Rate (1 per N packets)** - ask the exporter to send an sFlow update every **N** packets. The exporter may not be able to honor this request, so InterMapper Flows keeps track of the actual update rate as well.

Additional Columns:

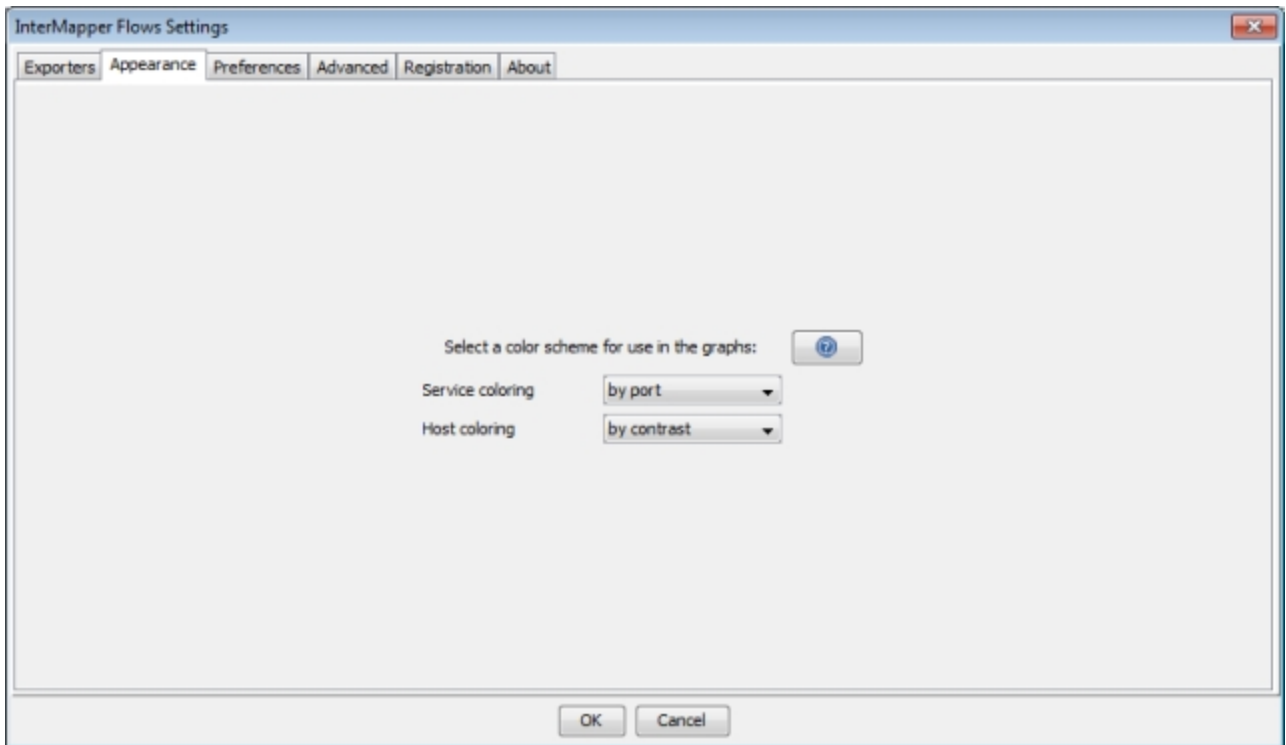
- **Expand** - click the right-pointing arrow to expand an exporter to view information for all available interfaces. Click the down-pointing arrow to collapse the exporter's interface lines.
- **Tag** - double-click to edit the tag for any exporter or interface. Tags appear in the Exporter/Interface selection dropdown in the Flows window. InterMapper Flows fills in these tags, if available, from every device.
- **Version** - shows the NetFlow or sFlow version used by the exporter.
- **Total Flows** - total number of Flow records exported.
- **Flows/hr** - average flows-per-hour from this exporter.
- **Latest Update** - the date and time of the last update from this exporter.
- **First Report** - the date and time of the first report from this exporter.

Additional Boxes:

- **NetFlow port** - InterMapper Flows listens for NetFlow v1, v5, v7, and v9 on this port. 2055 is the default port, but ports 9555 and 9995 are sometimes used.
- **Database remaining** - each exporter has an estimated flow rate, updated the last time it reported. The combined rate is used to calculate an estimated database capacity.
- **sFlow port** - InterMapper Flows listens for sFlow on this port. The default port is 6343. This must be different from the NetFlow port. Make sure that this port is not firewalled from any of your exporters.
- **Add sFlow Exporter button** - click this button to add an sFlow exporter. The Enter sFlow Information window appears.

Appearance tab

Use the Appearance tab to choose the coloring scheme used to color charts in the Flows window.

**Choose color schemes as follows:**

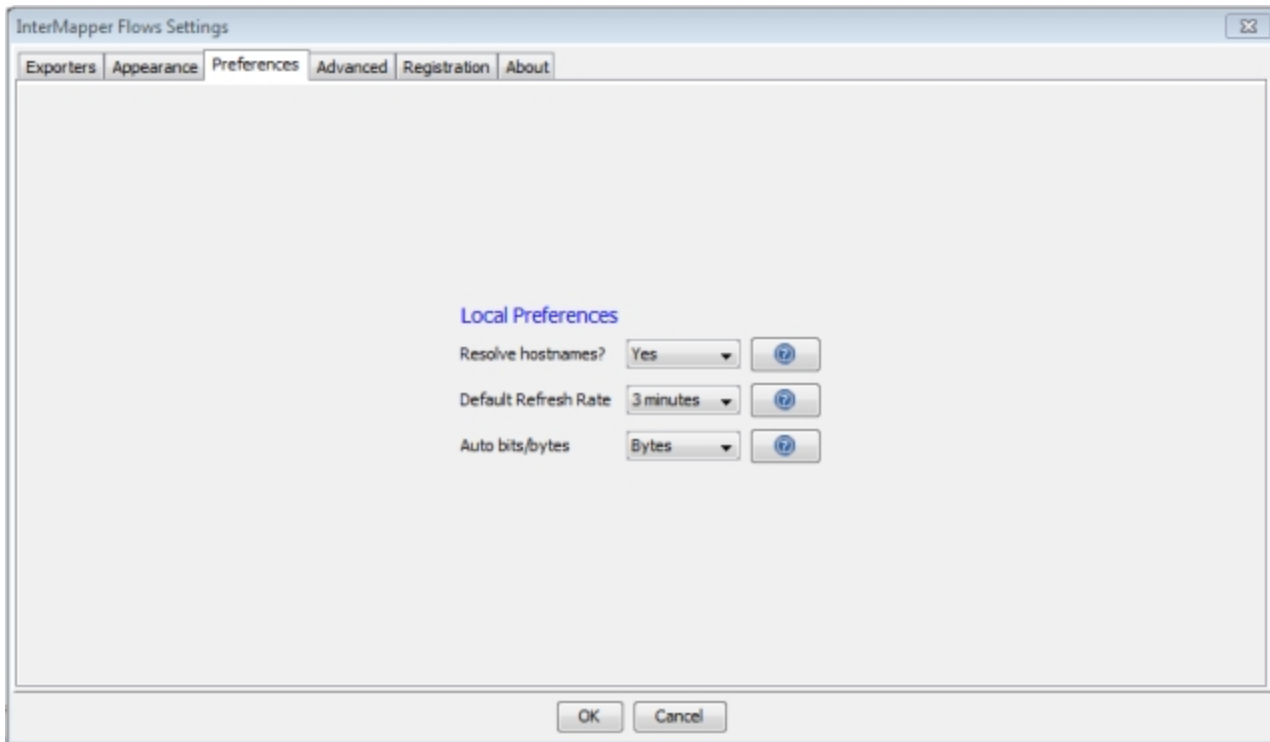
- **Service coloring** - choose a scheme to use for Services.
- **Host coloring** - choose a scheme to use for Hosts.

Two different color scheme strategies are used for charts and graphs:

- **By port or host** - colors are fixed for each port or host. This means the color for a port or host is the same in every chart in which that port or host appears. Because of the limited number of colors, it is possible for two adjacent hosts in a chart to have the same color.
- **By contrast** - chart colors are assigned in the same order for each chart. This provides greater contrast, but a single host or port might be colored differently in each chart, or in the same chart at different times.

Preferences Tab

Use the Preferences Tab to set local preferences for InterMapper Flows.

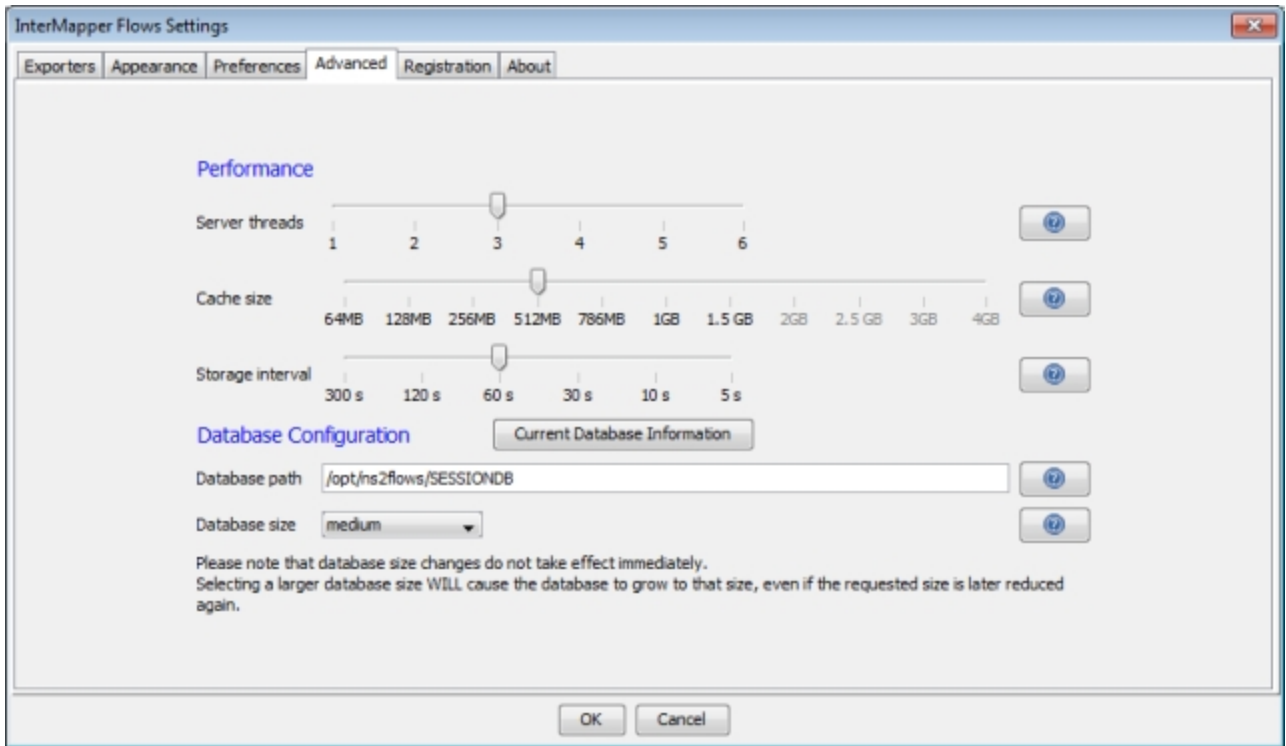


Local Preferences

- **Resolve hostnames?** - choose **Yes** to resolve IP addresses to show host names. Choose **No** to display only IP addresses. This can improve performance and security.
- **Default Refresh Rate** - choose a default refresh rate for a new Flows window. To override this setting in any Flows window, choose a different refresh rate from the Auto-update dropdown menu.
- **Auto bits/bytes** - choose a default display setting of **Bits** or **Bytes** for any new Flows window. To override this setting, choose a different setting from the Graph Scale dropdown menu at the upper left of the Stack Chart.

Advanced tab

Use the Advanced tab to set performance- and database-related parameters.

**Performance settings**

- **Server threads** - the number of available query threads to start. In practice, this number can be quite small. It is the number of concurrent requests that InterMapper Flows will handle without queuing requests. A good rule of thumb for this value is the number of processors in the server, plus 1. For example, a quad-core server might use 5 threads.
- **Cache size** - the size of the memory session cache. Session records are written to disk regularly, but to speed up queries (for graphs and tables) a number of them are cached in memory. It is safe to set this close to the memory capacity of the server.

Notes:

- Larger values for the session cache will increase server startup/restart times as records are loaded from disk.
- A cache larger than 1.5Gb requires a 64-bit processor.

- **Storage interval** - the number of seconds between disk commits. Committing more often may decrease performance by using physical media more often. Committing less often requires more session cache to avoid losing data.

Database Configuration settings

- **Database path** - specify a path to an existing directory. The server must have read/write access to this directory.

Note: If you change the database path, the existing database is not copied to the new location, however, you can do this manually while the service is not running. The old database is not deleted.

- **Database size** - available sizes as shown below (calculated from the current flow rate):

Size	# Session Records	Size on disk
tiny	3000	~400 KB
small	~8 million	~1000 MB
medium	80 million	~10 GB
large	800 million	~100 GB
very large	2 billion	~256 GB

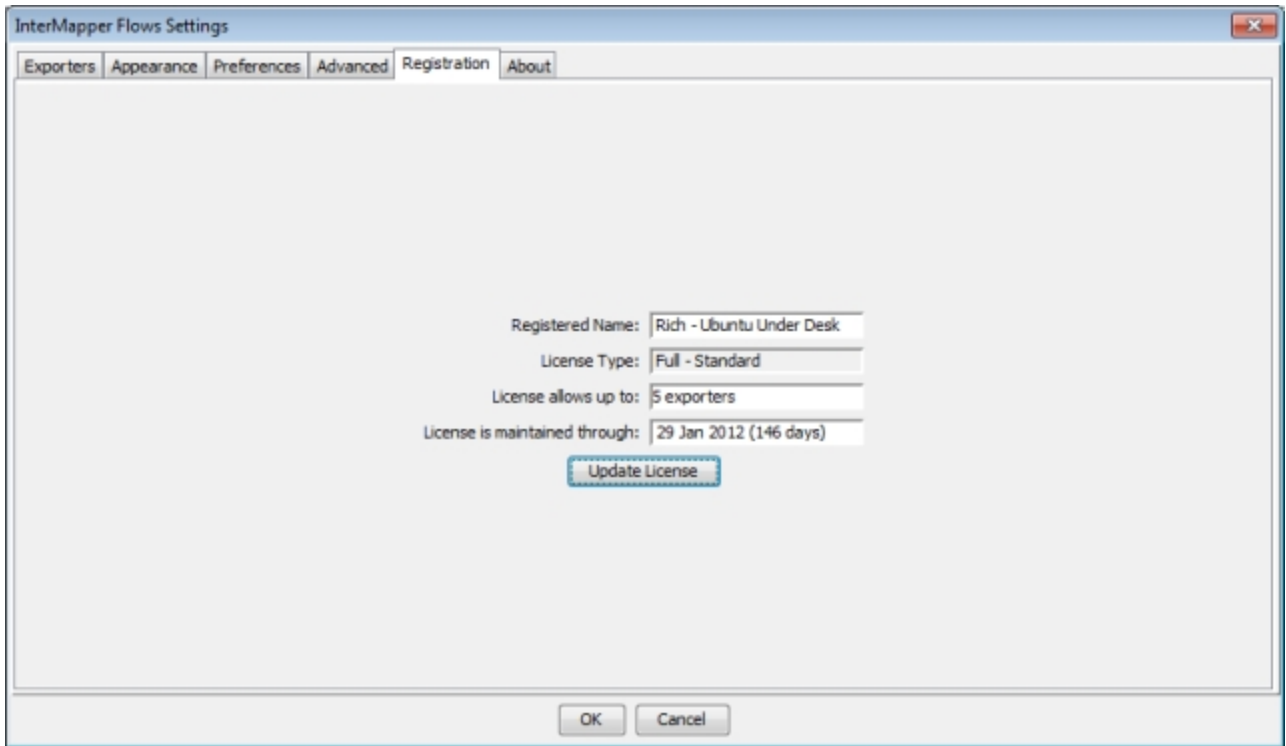
Note: Resizing a database may be a gradual process. Growing a database simply allocates more space for session records, while shrinking a database takes longer, as records are cropped over time.

- **Current Database Information** button - shows the maximum size of the database, the number of records in the database, and the number of days over which those records have been collected.



Registration tab

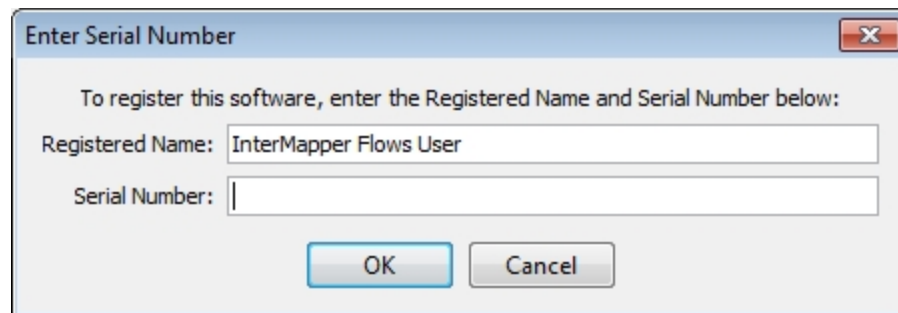
Use the Registration tab to enter or update your license key.



The screenshot shows the 'InterMapper Flows Settings' dialog box with the 'Registration' tab selected. The dialog has tabs for 'Exporters', 'Appearance', 'Preferences', 'Advanced', 'Registration', and 'About'. The 'Registration' tab contains the following fields and buttons:

- Registered Name: Rich - Ubuntu Under Desk
- License Type: Full - Standard
- License allows up to: 5 exporters
- License is maintained through: 29 Jan 2012 (146 days)
- Update License button
- OK and Cancel buttons at the bottom

- **Registered Name** - the name to which the software is registered.
- **License Type** - Demo, Evaluation, NFR (Not for resale), Test, or Full.
- **License allows up to** - the number of allowed exporters.
- **License operates through** - for evaluation, demo and NFR serial numbers, this is the last day of operation for InterMapper Flows. For purchased licenses, the end date for the maintenance contract is shown.
- **Update License** button - click to enter a user name and serial number for your copy of InterMapper Flows. The Enter Serial Number dialog appears:



The screenshot shows the 'Enter Serial Number' dialog box. It contains the following text and fields:

To register this software, enter the Registered Name and Serial Number below:

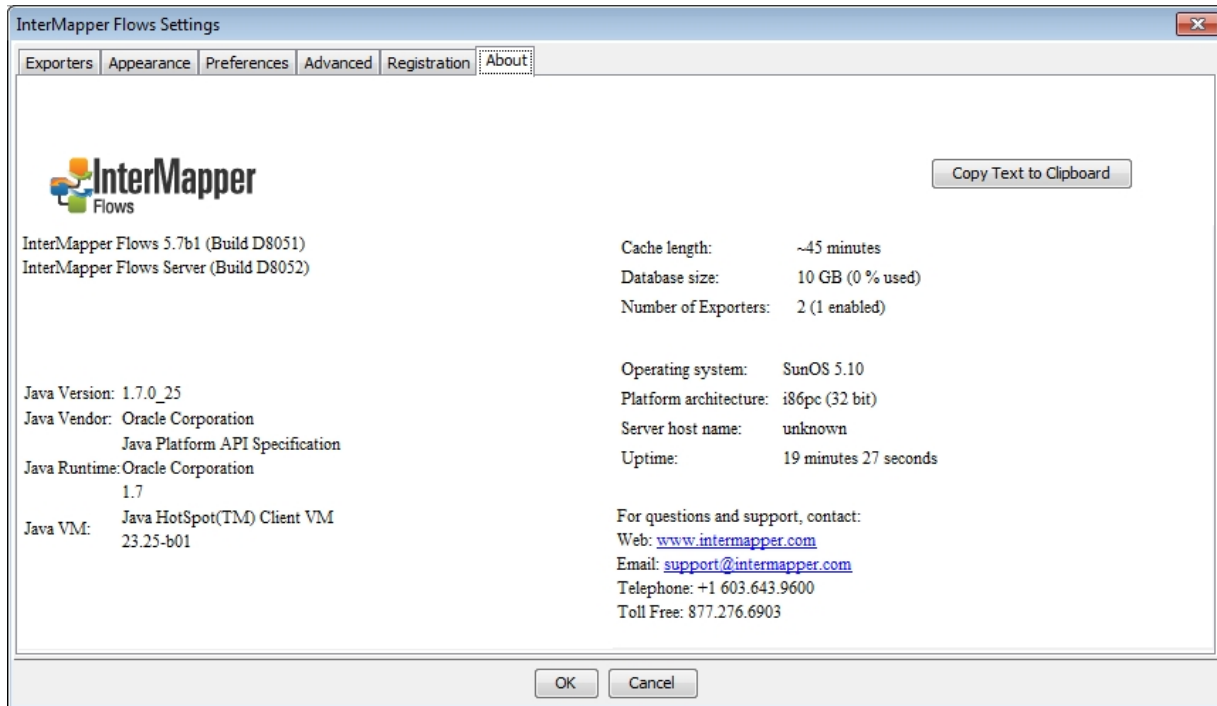
Registered Name: InterMapper Flows User

Serial Number:

OK and Cancel buttons are at the bottom.

About tab

Use the About tab to view information about InterMapper Flows and the platform on which it is running. Click **Copy to Clipboard** to copy detailed information about the configuration of InterMapper Flows to the clipboard for pasting into another document. This is useful when corresponding with technical support.



Using the Layer 2 View

Overview

Use the Layer 2 view of the Device List window to view information about your switches and what's connected to them. With the Layer 2 view, you can answer questions like:

- What switch port is this computer connected to?
- What computers are connected to that switch port?
- How are these two switches connected?

What Layer 2 Processing Does

InterMapper periodically scans all the switches on maps where Layer 2 is enabled (see the [Layer 2 Features pane \(Pg 86\)](#) of the Map Settings window). It collects information regarding which devices are attached to which ports, what other switches are present, and places the resulting information into the Endpoints pane.

InterMapper Layer 2 uses device MAC addresses to identify devices. It looks through the forwarding databases of the switches to identify the ports where devices connect. The Layer 2 process also looks through ARP tables and other sources of data to map the MAC addresses to IP addresses, to collect DNS names, VLANs, and other information, locating each device as precisely as it can.

When Layer 2 passes the connection information back to the map, automatically showing the connection of each device on the map to the proper port on the switch.

In order to use InterMapper's Layer 2 features, you must:

1. Enable [Layer 2 features](#) in the Server Settings window.
2. Enable them in the [Map Settings window](#) for any map containing switches you want to include during Layer 2 discovery.

To use the Layer 2 connection information to make connections on the map automatically, select ***Automatically change this map to show Layer 2 connections*** in the Layer 2 Features pane of the Map Settings window.

Note: The Layer 2 View is disabled when:

- Layer 2 features are not enabled.
- The user is not an administrator.
- The user is not a member of the FullLayer2Access group.

Viewing Layer 2 Information

Layer 2 information is shown in a "sub-view" of the global Device List Window, available from the Window menu.

To open the Layer 2 view:

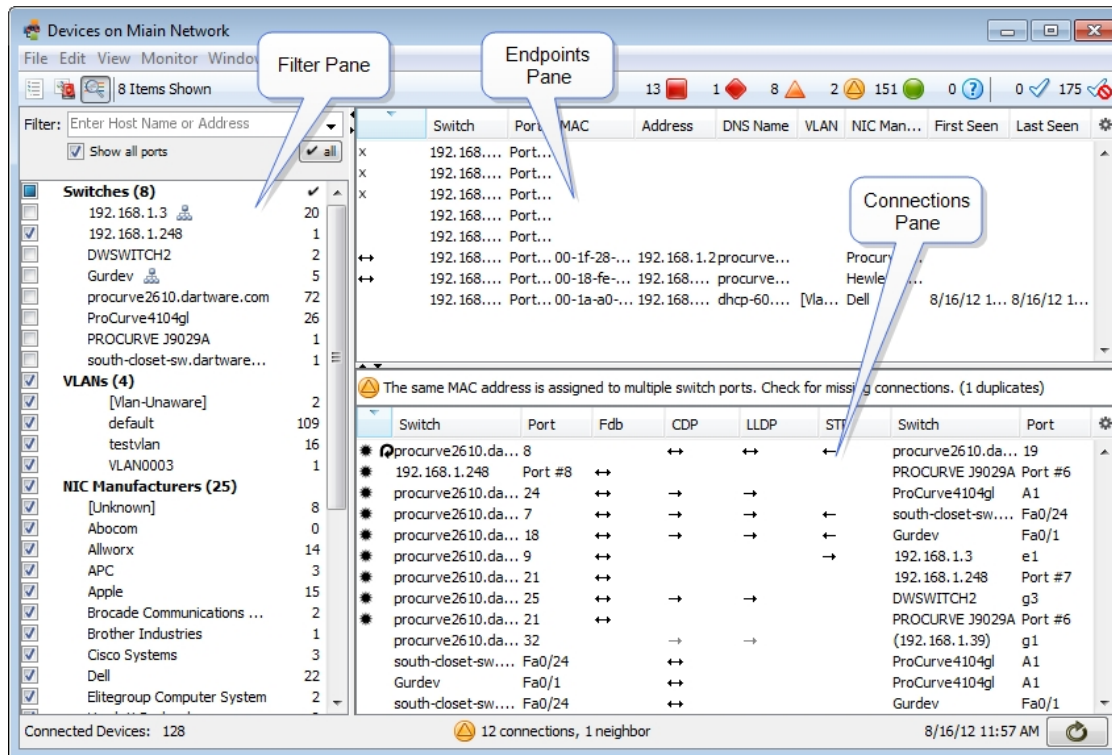
1. From the Window menu, choose Device List. The Device List window opens.
2. In the Device List window, click the Layer 2 view button, as shown at right. The Layer 2 window appears.



Alternatively, you can:

- Right-click a device on a map and choose **Show in Layer 2** from the context menu.
- Select a device on a map and choose **Show in Layer 2** from the Monitor menu.

The Layer 2 View



Understanding the Layer 2 View

The Layer 2 View contains three main panes:

- The **Endpoints pane (Pg 347)** - the upper right pane lists all switch ports and the devices connected to them. It contains only those ports and devices that match the filter criteria in the Filter pane.
- The **Filter pane (Pg 345)** - the left pane provides criteria for showing or hiding endpoints based on their presence on a particular switch, VLAN, or the endpoint's manufacturer. lists available switches, the VLANs in which they appear, and manufacturers of network interface cards of the devices connected to them. Use the check boxes to select or hide endpoints in the Endpoints pane, and type additional criteria to help select the endpoints you want to view.
- The **Connections pane (Pg 348)** - the lower right pane provides details about switch-to-switch connections.

The Filter Pane

Use the Filter pane to limit the endpoints you want to view in the Endpoints pane. Choose a combination of switch, VLAN and NIC Manufacturer to select the devices you want to view.

The **Switches** section lists each switch by name, and shows the number of endpoints attached to that switch.

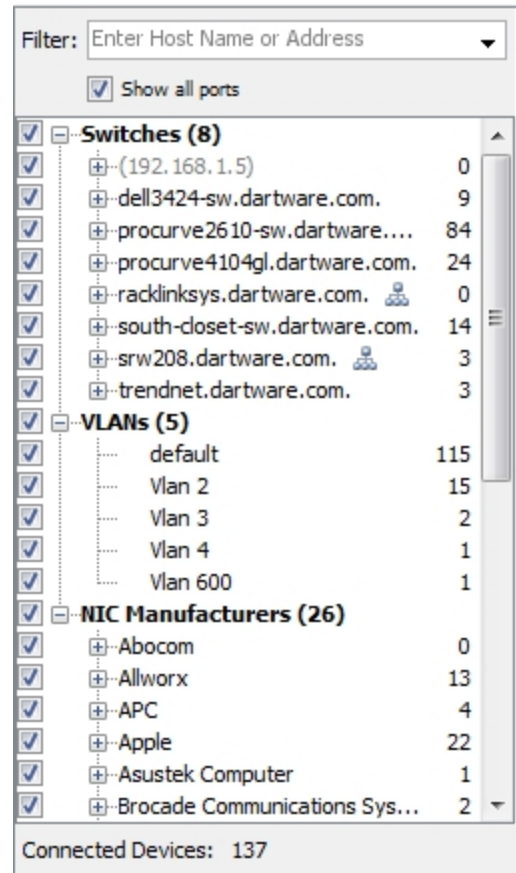
The **VLANs** section lists all VLANs and the number of endpoints on each.

The **NIC Manufacturers** section lists all unique NIC Manufacturers connected to devices.

The right column of the Filter Pane shows a count of endpoints present for each of the criteria. See [Understanding Endpoint Counts \(Pg 346\)](#) for more information.

Use these methods to control the filter criteria:

- By default, all check boxes are selected.
- Select or clear check boxes to get the combination of switch, VLAN, and NIC Manufacturer that matches the devices you want to view.
- Double-click a check box to select it and clear all other check boxes in the section.
- Expand the Switch tree to view and select switch ports.
- Right-click a switch and choose **Remove switch from Layer 2 database** to prevent the switch from being polled for Layer 2 information. This is equivalent to the **Poll this address for Layer 2 information** check box, available in the [Set Behavior window](#).
- Expand the VLANs tree to view and select VLANs.
- Expand the NIC Manufacturer tree to view and select NIC models from those available.
- Select or clear the **Show all ports** box to show or hide the ports to which in the Endpoints pane to which nothing is connected.
- Use the Filter Control (see below) for additional control of the set of rows that are displayed in the Endpoints pane.






- The Filter box provides significant additional filtering capability. Enter a host-name or address in the **Filter box** to limit the devices shown in the Endpoints pane. See [Using the Filter Box \(Pg 347\)](#) below for many more options.
- Certain flags appear next to entries. See [Understanding Layer 2 Flags \(Pg 350\)](#).
- A switch that appears in grey and in parentheses indicates that the switch was previously detected, but is no longer on a Layer 2-enabled map.

Understanding Endpoint Counts

The right column of the Filter pane shows the number of Endpoint devices (specifically, the number of distinct MAC addresses) for each of the filter criteria.

- An SNMP-enabled managed switch or hub appears as zero endpoints, since it is not considered an endpoint.
- A single endpoint (host, workstation, server, router, etc.) will show as one endpoint.
- If an unmanaged hub or switch is present, or if the switch is not present on a Layer 2-enabled map, the endpoint count reflects the number of endpoints detected "out that port". In some cases, this may be a very large number of endpoints.

The number of endpoints indicated in the Filters panel often exceeds the number of entries in the Endpoints pane. This discrepancy occurs because the Endpoints panel often displays multiple entries for the same MAC address. Multiple entries appear in the following cases:

- **Multi-homed devices** - devices with multiple IP addresses that use a single MAC address. The flag at right appears. 
- **Interior devices** - devices attached to an unmanaged switch or hub that is placed between two managed switches. InterMapper's Layer 2 algorithm cannot show the correct switch port (because it's unmanaged), so it indicates the device as an "interior" device – between two managed switches. Interior devices are indicated with left or right arrows as shown at right.  

When you select the **Show All Ports** box, the Endpoints pane also shows:

- All ports, whether a device is connected or not
- Ports that are connected to other switches. (Normally these are hidden because switches are not considered endpoints.)
- Fuzzy devices (any device whose connection point cannot be completely determined.)

For more information, see [Understanding Layer 2 Flags \(Pg 350\)](#).

Using the Filter Box

Use the Filter box, located at the top of the Device Filter pane, to limit the devices you see in the Endpoints pane.

- Enter a host name or address to view only devices connected to that domain or address.
- From the Filter dropdown menu, select or clear **Endpoints Only** to include or exclude entries for ports with switches, unknown devices, and devices identified as "fuzzy" (see [Understanding Fuzzy Devices \(Pg 352\)](#).)
- In the Map or List view, select a device, then choose **in Layer 2** from the **Show** submenu, available from the Monitor menu and the context menu, to view that device's connections in the Layer 2 View.
- If the value is in double-quotes, list all endpoints where the value is part of the NIC Manufacturer. (e.g. "App" will match "Apple", "Appliance", etc.)
- If the value is an IPv4 CIDR block, list all endpoints with IP addresses in that CIDR block. (For example, enter "192.168.1.1/24")
- If the value is decimal digits separated by periods, or just digits, treat it as an IPv4 address. There are three forms:
 - a. **192.168** matches any IP address that begins with 192.168
 - b. **.1** matches any IP address that ends with .1
 - c. **10** matches any IP address that begins with 10. (no period necessary).
- If the value is hexadecimal and separated by dashes, treat it as a MAC address. Search for endpoints with the MAC address or MAC address substring. (e.g. "00-00-0c", "00-00-d7-00-10-ab")
- If the value starts with an alphabetical character, resolve the host name to an IPv4 address and filter on that IP address.
- If the value starts with '#', process the specified debug command (e.g. "#help")

Understanding and Using the Endpoints Pane

The Layer 2 view's Endpoints pane lists all *endpoint* devices (servers, workstations, and routers) and the switch ports they are connected to. It does *not* include managed switches, which are not considered to be endpoints.

The columns of the Endpoints pane are:

- **Flags** - flags that give detailed information about the port or device. See [Layer 2 Flags \(Pg 350\)](#) for more information.
- **Switch and Port** - describe a particular switch port
- **MAC and Address** - contain the MAC address and the IP Address of the device.
- **DNS** - the DNS name of the device (if known).
- **VLAN** - the VLAN(s) supported by this port.
- **NIC Manufacturer** - the manufacturer of the Network Interface Card (NIC), derived from the MAC address.
- **First Seen** - the time the device was first detected during a Layer 2 scan.
- **Last Seen** - the most recent time the device was detected during a Layer 2 scan.

- **Present** - two numbers, separated by "/". The first is the number of times this device was seen during a scan, the second is the total number of scans.
- **ifAlias** - the ifAlias taken from the Switch and Port (if available).

	Switch	Port	MAC	Address	DNS Name	VLAN	NIC ...	First Seen	Last Seen	
↔	procurve4104gl.dartware.com.	A1	00-12-0e-...	192.168.1...	trendnet...		Abocom			
🏠	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.63	dhcp-63.d...	Vlan 600	Apple	10/20/11 ...	10/20/11 ...	
🏠	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.63	dhcp-63.d...	default	Apple	10/20/11 ...	10/20/11 ...	
🏠	procurve4104gl.dartware.com.	D9	00-50-56-...			default	VMware	7/25/11 6...	7/25/11 1...	
🏠	procurve4104gl.dartware.com.	B10	00-50-56-...	192.168.1...	dhcp-122...	default	VMware	10/19/11 ...	10/19/11 ...	
✖	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.68	dhcp-68.d...	Vlan 600	Apple	10/20/11 ...	10/20/11 ...	
✖	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.68	dhcp-68.d...	default	Apple	10/20/11 ...	10/20/11 ...	
	procurve4104gl.dartware.com.	D18	00-50-56-...	192.168.1...	dhcp-118...	default	VMware	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D7	00-50-56-...	192.168.1...	solaris.dar...	default	VMware	7/22/11 6...	10/20/11 ...	
	procurve4104gl.dartware.com.	D2	00-50-56-...	192.168.1...	aurorax-s...	default	VMware	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D1	00-17-f2-0...	192.168.1...	cswmac.d...	default	Apple	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D1	00-11-11-...	192.168.1...	cswvmwar...	default	Intel	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D1	00-0c-29-...	192.168.1...	csw2k8...	default	VMware	8/16/11 4...	10/20/11 ...	
	procurve4104gl.dartware.com.	B17	00-50-56-...	192.168.1...	supportw2...	default	VMware	7/22/11 6...	10/20/11 ...	
	procurve4104gl.dartware.com.	B14	00-0c-29-f...	192.168.1...	aurora-ms...	default	VMware	6/24/11 2...	10/20/11 ...	

Controlling what you see in the Endpoints Pane

- In the Filter pane, click various combinations of Switch, VLAN, and NIC Manufacture to control the rows that appear in the Endpoints pane.
- In the Endpoints pane, click a column heading to sort by that column. Click again to reverse the sort.
- Click the sprocket at the right end of the Endpoints pane's column heading bar to add to or remove columns from the Endpoints Pane.
- By default, the Endpoints pane shows endpoints only - it hides ports connected to other switches, ports with no devices attached (regardless of whether they are up or down) or devices marked as "fuzzy." Select the Show All Ports box near the top of the [Filter pane \(Pg 345\)](#) to show all ports.

Using Layer 2 Information to Update Map Connections

In addition to this tabular view, InterMapper can pass the connection information back into the Map view, automatically showing the connection of each device on the map to the proper port on the switch. This simplifies the creation and arrangement of your maps; all you need to do is tidy up the map. Turn this feature on from the Layer 2 Features pane of the [Map Settings \(Pg 94\)](#) window.

Understanding and Using the Connections Pane

The Layer 2 Connections pane lists all switches, the switches they are connected to, and the ports through which they are connected. This information is derived from the switch's forwarding tables, as well as information available through Cisco Delivery Protocol (CDP), Link Layer Delivery Protocol (LLDP), and Spanning Tree Protocol (STP).

	Switch	Port	VLAN	Fdb	CDP	LLDP	STP	Switch	Port	
✱	procurve2610-sw.dart...	7	default	↔	→	→	←	south-closet-sw.dar...	Fa0/24	▲
✱	procurve2610-sw.dart...	8			↔	↔	←	procurve2610-sw.d...	19	
✱	procurve2610-sw.dart...	9	default	↔			←	dell3424-sw.dartwar...	e1	☰
	procurve2610-sw.dart...	9			→	→		procurve4104gl.dart...	A1	
	procurve2610-sw.dart...	18			→	→		(192.168.1.35)	Fa0/1	
✱	procurve2610-sw.dart...	28	default	↔				srw208.dartware.com.	e6	
✱	dell3424-sw.dartware....	e4	default	↔				procurve4104gl.dart...	A1	▼

The Connections Pane

Connections Pane Columns

- **Switch and Port** - each row shows two switches and two ports. These switches are known to be connected by the specified ports.
- **VLAN** - The VLAN(s) that are present on the connection between the switches.
- **Fdb** - (Forwarding database)
 - A **two-headed arrow** means that both switches' forwarding databases have entries for each other. ↔
 - A **single-headed arrow** points toward the switch that is in the other switch's Fdb; there is no corresponding entry in the reverse direction. →
- **CDP and LLDP** - (Cisco Discovery Protocol and Link Layer Discovery Protocol)
 - A **two-headed arrow** indicates that both switches hear the other's protocol advertisements. ↔
 - A **single-headed arrow** points to the switch that receives the protocol advertisements from the other. →

Note: Some CDP/LLDP-aware switches may turn off advertisements on certain ports. This affects the arrows.
- **STP** - (Spanning Tree Protocol)
 - A **single-headed arrow** points away from the root of the spanning tree. →
 - A **two-headed arrow** indicates that the path for some spanning trees (such as certain VLANs) goes one way, while the path for other spanning trees goes the other way. If there are loops between these two switches, the port closest to the root may be in a blocking state. ↔

Using the Connections Pane

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click the sprocket icon at the right end of the column heading bar to choose the columns that appear in the list.

Understanding Layer 2 Flags

The meanings of flags in the Layer 2 view depend the pane in which they appear.

Flags in Device Filter and Endpoints panes

In the Filter and Endpoints panes, flags indicate the following:

- ↔ **Switch-to-Switch connection** - Connected to another switch
- ← **Interior device** - The device is attached to a hub or switch that is connected or between ports of two managed switches. The left or right arrow points away → from the spanning tree root.
- ✕ **Down** - This port is not operating.
- 🏠 **Multi-homed device** - A single MAC address has multiple IP addresses. Each IP addresses is shown as a separate row in the Endpoints pane.
- 👤 **Ghost** - Port is not active, and the endpoint (device with this MAC address) has not been seen elsewhere in the network. It was last seen on the indicated switch port.
- ↔ **Not present on Map** - Port is connected to a managed switch, but that switch is not present on a Layer 2-enabled map.
- ← **Fuzzy** - The Layer 2 process cannot determine the exact port where the or device is attached. See [Understanding Fuzzy Devices \(Pg 352\)](#) below.
-
- or
- ↓
- 📄 **Duplicate MAC address detected** - The Layer 2 process has found the same MAC address on two separate switch ports.
- ✖ **IP conflict** - The Layer 2 process has found the same IP address on two separate switch ports.
- 👤 **Spanning tree root** - This switch is the root of the spanning tree.
- 🔄 **Loop** - a port is connected to another port on the same switch.
- 📶 **Wireless (assigned manually)** - a port or VLAN has been tagged as Wireless. The Wireless flag appears next to the port in the Filters and Endpoints panes. See [Manual Tagging \(Pg 352\)](#) below.
- 💻 **Virtual machine (assigned manually)** - All NICs from this manufacturer with this OUI (organizationally unique identifier) are virtual machines. The Virtual Machine flag appears next to the OUI and any endpoints that use NICs with that OUI. See [Manual Tagging \(Pg 352\)](#) below.

Flags in the Connections pane

The following flags may be present in the Flags column of the Connections pane.

- ✱ **Confirmed connection** - (will be exported to map).
- ← **Not present on Map** - Port is connected to a device that is not present on a
→ Layer 2-enabled map.
- ↻ **Loop** - Indicates a direct port-to-port connection on this switch

- ↔ Both ends see each other's CDP/LLDP advertisements.
- ← The left end of the connection sees the right end's CDP/LLDP advertisements.
- The right end of the connection sees the left end's CDP/LLDP advertisements.
- Connected to a device that is not present on any map.
- ✱ Confirmed connection (will be exported to map).

STP column: In the STP column of the Connections Pane, arrows indicate the direction of travel of STP bridge information.

- ← Right switch is the left switch's path to root for one or more of the left switch's spanning trees. (Right switch's port may be in blocking state, if there are loops.)
- Left switch is the right switch's path to root for one or more of the right switches' spanning trees. (Left switch's port may be in blocking state, if there are loops.)
- ↔ Right switch is left switch's path to root for one or more spanning trees and left switch is right switch's path to root for other spanning trees. (Either switch's port may be in blocking state for one or more spanning trees, if there are loops.)

Understanding Fuzzy Devices

A device with a MAC address whose location in the Layer 2 topology cannot be completely determined is considered a "fuzzy" device by InterMapper.

Fuzzy devices are quite common, and can occur for a number of reasons. The Layer 2 engine attempts to collect information from all the switches nearly simultaneously. However, some time can elapse between the times that two switches finishes collecting Layer 2 information. During this time period, a MAC address collected from one switch may "age out" of another switch. Alternatively, a device may connect to the network during Layer 2 collection, so its MAC address is reported in one switch's forwarding tables, but not in the edge switch (due to the difference in scan times for the two switches).



Devices may be classified as fuzzy due to bugs in certain switch models. For example, Help/Systems has a small managed desktop switch that doesn't report its complete forwarding table via SNMP. The extra un-reported devices appear as fuzzy, because the upstream switch reports the MAC address, but the downstream switch never reports them (even though the switch is otherwise perfectly functional.)

Fuzzy devices are distinct from *Interior* devices. A fuzzy device appears to be in the middle of the network (between two switches) because InterMapper doesn't have complete information. An interior device appears to be in the middle of the network because there is actually another switch or hub located there, but it's not part of the Layer 2 information.

Manual Tagging

For certain kinds of connections, you may want to tag a port or endpoint device so you can see easily what kind of device it is.

Here are some tagging options:

-  Wireless (assigned manually) - Right-click a switch port or VLAN in the Filters pane and select **as Wireless** from the Tag submenu. The Wireless icon appears next to the port or VLAN.
-  Virtual machine (assigned manually) - Right-click a port in the NIC manufacturer's section of the Filters pane (one that is associated with a virtual machine), and select **as Virtual Machine** from the Tag submenu. The Virtual Machine icon appears next to the OUI and any endpoints that use NICs with that OUI.

Mapping With Layer 2

You can use Layer 2 to create maps that accurately reflect your network's topology. There are several ways to do this - two methods are detailed here.

Converting an Existing Map to use Layer 2

For maps with a relatively small number of devices, you can convert the map directly so that it uses Layer 2 features to configure the map. You can also create a new map and use Layer 2 information to add the switches and devices.

To convert an existing map to Layer 2:

1. Open the map you want to convert and make it editable.
2. From the Map Settings window's Layer 2 Features pane, select the **Enable Layer 2 features for this map** check box.
3. From the Window menu, choose **Device List**, and choose **Layer 2** from the View menu or click the **Layer 2 View** icon. The Layer 2 window appears, showing your available Layer 2 devices.
4. In the Layer 2 view, click the **Refresh** button at the lower right corner of the window.
5. From the Map Settings window's Layer 2 Features pane, click **Change Now**. Any Layer 2 connections are broken and reconnected using Layer 2 information.
6. Select all devices and choose **Organic** from the Format menu's Arrange submenu. The map now uses Layer 2 information to connect the devices on the map.

To create a new map using Layer 2 information:

1. Create a new empty map and make it editable.
2. From the Window menu, choose **Device List**, and choose **Layer 2** from the View menu or click the **Layer 2 View** icon. The Layer 2 window appears, showing your available Layer 2 devices.
3. In the Layer 2 view, click the **Refresh** button at the lower right corner of the window.
4. In the Connections pane, select the lines for the switches you want to map and choose **Copy** from the Edit menu.
5. Paste into your new map. In a few moments the switches appear on your map.
6. From the Map Settings window's Layer 2 Features pane, select the **Enable Layer 2 features for this map** check box.
7. Click **Change Now**. The switches on the map are connected as defined by Layer 2 information. This represents your network's switch backbone.
8. From the Layer 2 window's Endpoints pane, select all endpoints, copy them, and paste them into your map.
9. From the Map Settings window's Layer 2 Features pane, click **Change Now**. The devices are connected as defined by Layer 2 information.
10. Although optional, you may find it helpful to select all devices and choose **Organic** from the Format menu's Arrange submenu.

InterMapper Reports

Overview

Use the InterMapper Reports server to create, view, print and save reports that use data collected from InterMapper servers.

InterMapper Reports is a module of [InterMapper DataCenter \(Pg 613\)](#). Use your favorite browser to use InterMapper Reports to create your reports.

Note: Before you can use it, you must start the InterMapper Reports Server. This allows InterMapper to send data to the Reports Server where it is collected in a database.

To start collecting data:

1. From the Server Settings window, choose **Reports Server**. The Reports Server pane appears.
2. From the Reports Server pane, click **Start**. The Configure button becomes active.

To view the Reports Server interface:

- From any InterMapper map, right-click a device and choose **Reports...** from the **Show in** submenu. A browser page launches and the InterMapper Reports window appears.

Creating A Report

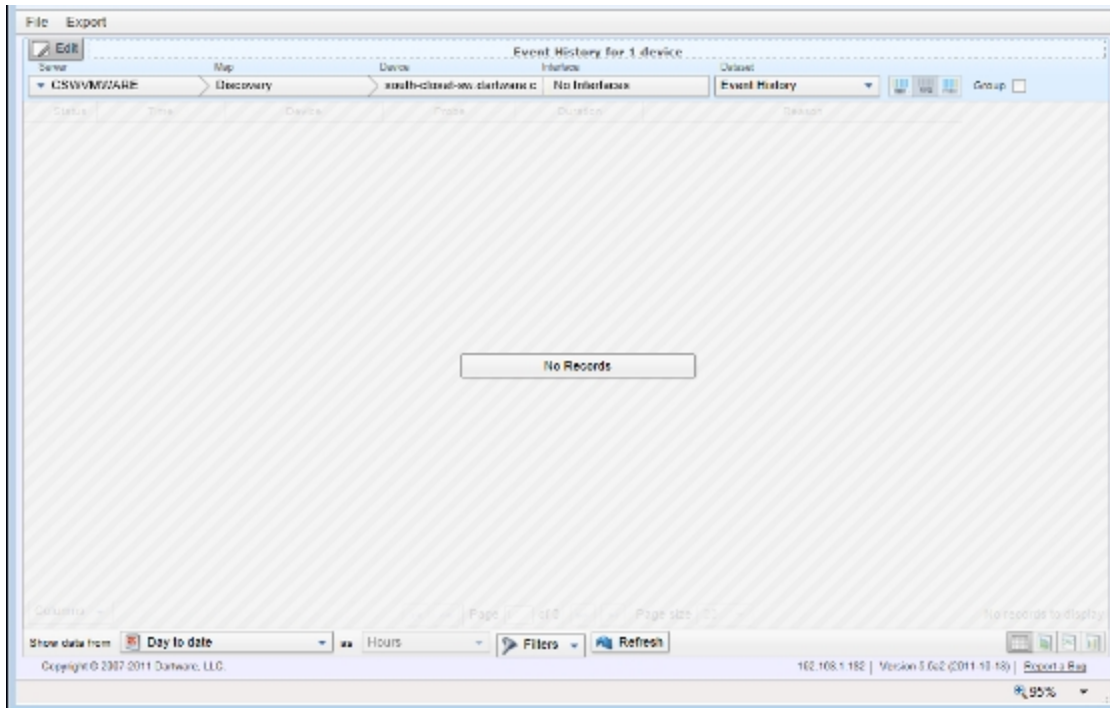
Use the Reports Server web UI to create, save, load, link, or print a report.

You can open the InterMapper Reports window from an InterMapper map.

Opening the Reports Window

To open the InterMapper Reports window:

1. Select a device in an InterMapper map window.
2. Right-click the device and from the Context menu, choose **Reports**. The InterMapper Reports window appears in a new browser window as shown below.



InterMapper Reports window in View mode

Two other ways you can also open the Reports window:

- Use this URL:

[https://\[InterMapper Server address\]:8182/~imreports/](https://[InterMapper Server address]:8182/~imreports/)

- From the Server Settings window, view the Reports Server pane, and click Configure, log in to the InterMapper DataCenter, and click **View Reports** in the InterMapper Reports box.

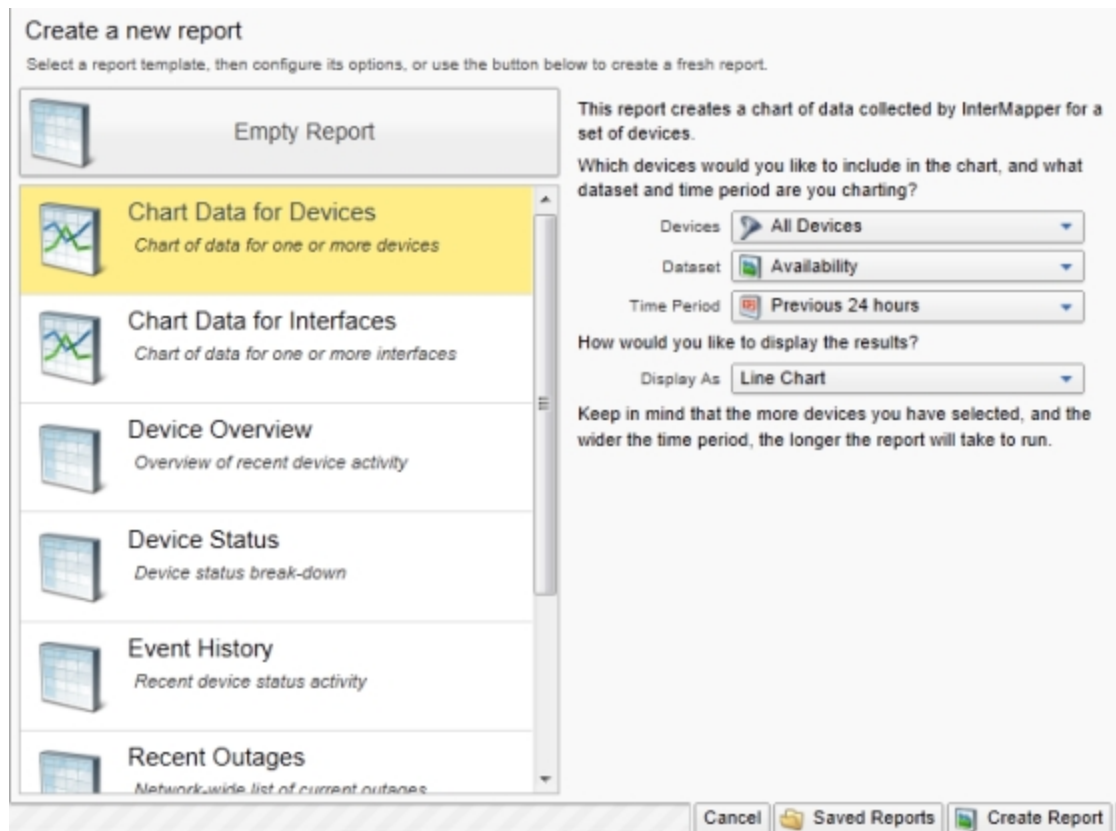
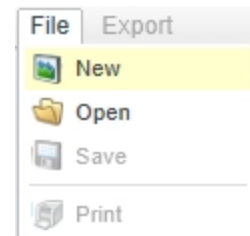
Creating a New Report

There are several ways to create a report:

- **From the Map Window** - open the Reports window after selecting one or more devices or interfaces.
- **From a template** - a number of pre-configured templates are available.
- **From scratch** - using an empty template. Select your own devices or interfaces, the data you want to show from each, any calculations you want to apply, a report period and interval, and the way in which the data is shown.

To create a new report from a template:

1. If you haven't stored any reports, you can start with a template.
2. From the Report window's File menu (shown at right,) choose **New**. The Templates list appears, as shown below.
3. Click to choose a template from the left side of the list. A set of parameters for that template appears on the right. You can also click **Saved Reports** to view a list of reports that have already been saved.
4. Choose from the template's available parameters.
5. Click Create Report. The report loads with the selected parameters.



The Templates List

Report types

Report templates fall into two general categories:



Graph - Can be used with datasets that contain only numeric data.

Three display options are available in a Graph report:

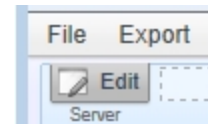
- **Area** - a line chart with the area below the line filled.
- **Line** - a line chart with a dot at each data point.
- **Bar** - a bar chart.



Table - a tabular report, containing columns and rows.

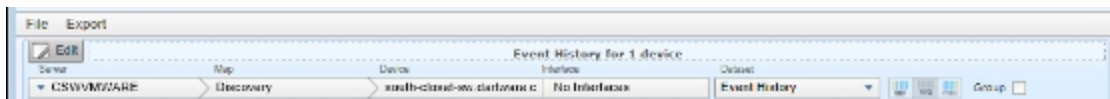
To create a new report from the Empty Report template:

1. If you choose the Empty Report template, you can create a report from scratch. You can also recall an existing report to use as a starting point.
2. Click **Edit**, located just below the File and Export menus. The Reports window changes to Edit mode. (The **Edit** button toggles the report in and out of Edit mode.)



Editing a Report

The image below shows the controls you can use to fine-tune your report definition.



InterMapper Reports window in Edit mode

Once in Edit mode, you need to answer some or all of these questions (in the areas shown above), depending on your requirements for this report:

- **Which devices?** Select the devices you want to include in the report. Select from the available **Servers**, **Maps** and **Devices**. If network interface data available for any of the selected devices, select one or more Interfaces.
- **Which data?** Choose from available Datasets. A number of datasets, including *Details* and *Event History*, are standard for all devices, other datasets are based on data available from your device selection.

Note: Currently, only one dataset can be included in a report.

- **Calculations?** If you have selected a Dataset other than Details and Event History, such as Response Time, you can choose from some basic calculation options. Choose **Min**, **Avg**, or **Max** to specify how the results are displayed.

Min shows the only lowest values for the dataset.

Avg averages the results (most commonly used).

Max shows only the highest values in the dataset.

The Group checkbox allows devices in your selection to be grouped as one dataset in the results.

- **Period of time?** Choose a start date or date range. (Not active when Detail dataset is selected.) For other datasets, common date selections are available. When specifying a date range, the calendar indicates whether data is available from the selected date range (grayed for no data, black for data)
- **Interval?** Specifies data interval, which controls the density of the data over time.

Note: Event History and Details datasets do not use Interval.

- **Report Type?** Choose how the dataset results are displayed. By default, a Tabular report (list) is shown. When the selected dataset contains numeric values, you can also choose Area, Line or Bar chart. For Event History and Details, only a tabular view is available.

Additional Report-editing Features

Use a number of other controls to customize your report further:

- Click the **title** to edit it.
- For tabular reports, **click a column heading** to sort by that column; click again to reverse the sort. The sort order is saved with the report.
- To change the order of tabular report columns, **drag a column heading** to move the column to the right or left.
- To save the report, click **Save** from the Report window's File menu, give the report a name, and click **Save Report**.

Opening a Saved Report

You can save any number of reports, then open, view or print them at a later time. For more information, see [Managing and Printing Your Reports \(Pg 370\)](#).

Selecting Source Data

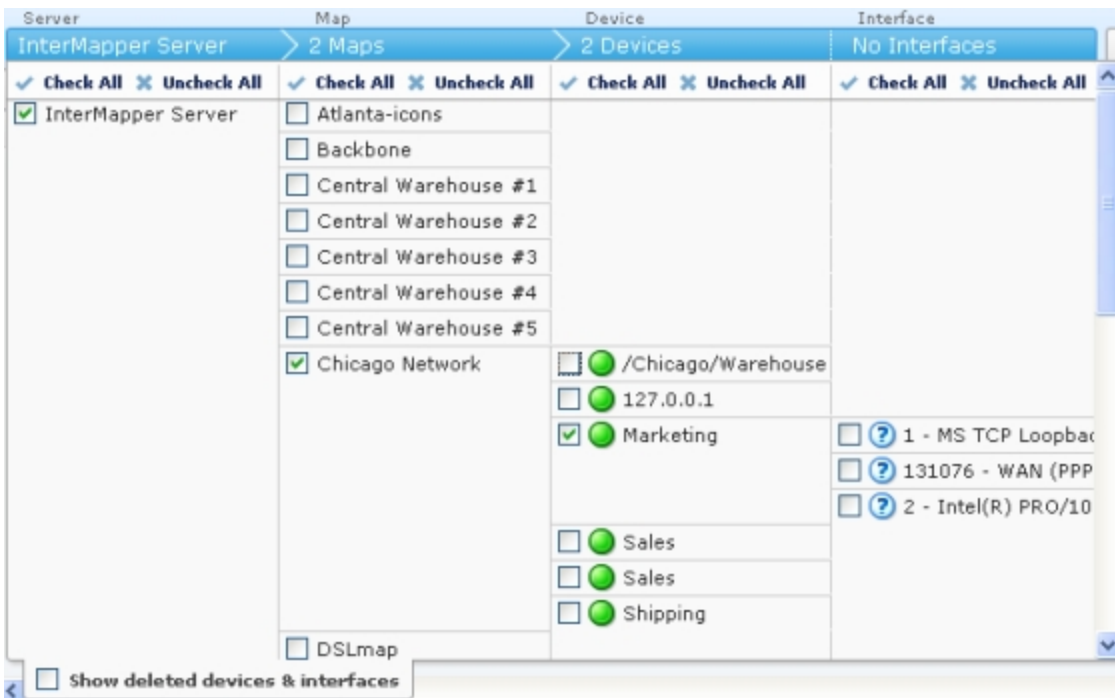
When creating a report, you first need to choose the devices or interfaces for which data is included in the report.

Use the data source selection bar to select the devices or interfaces for your report.

Server	Map	Device	Interface
InterMapper Server	scan test	192.168.81.1	No Interfaces

To select data sources:

- Click anywhere in the source selection bar shown above. A selection tree appears, as shown below.



- Select or clear the check boxes for the devices or interfaces whose source data you want to include in the report.
- Select the **Show deleted devices & interfaces** check box to include devices or interfaces that have been deleted.
- Click the **Select All** or **Unselect All** to select or unselect all devices or interfaces in a column.
- When finished selecting, click the source selection bar. The selection tree disappears, and the selected data appears.

Note: If you select a large amount of data over a large time range, it may take a few moments or longer for the data to appear. This depends on a number of variables - the speed of reports server CPU, the amount of data, the time units selected.

Selecting a Dataset

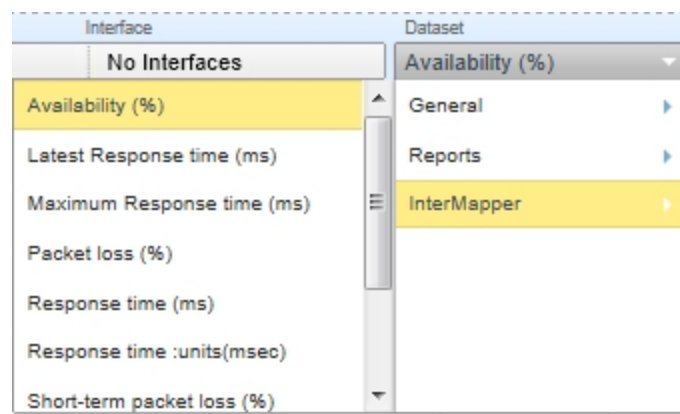
To create graphs, you need to select a dataset that contains numeric values. The datasets available depend on which devices are selected, the probes used to monitor those devices, what datasets are recorded through those probes, and whether those datasets are being exported to the Reports Server database.

A dataset is available when retention policy for the selected device is not set to **None** and one of the following is true:

- For devices, response time or short-term packet loss are always stored.
- For interfaces, incoming or outgoing bytes/second are always stored.
- If the dataset is specified in the probe to be 'autorecord'.
- If a chart was created from the dataset by clicking it in the Status window or dragging it from the Status window to an existing chart.

To select a dataset:

- From the Dataset drop-down menu, near the right of the device selection controls, choose a dataset. Assuming you are still in Table view, a list of values appears.



Selecting Data Grouping



Grouping by time

In most cases, the selected time scale causes each data point to represent a group of raw samples. Use the data grouping buttons to specify how you want the group of samples represented by a graph data point to be displayed.

To select data grouping for each time period:

- Click **Min** to display the minimum value from the group of samples during a data point's time period.
- Click **Avg** to take the average value from the group of samples during a data point's time period.
- Click **Max** to display the maximum value from the group of samples during a data point's time period.

Grouping by device or interface

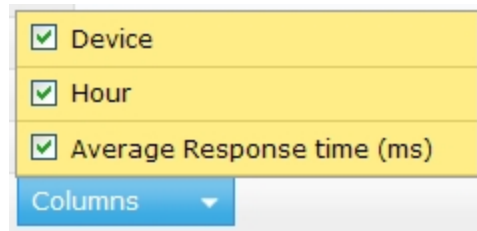
When multiple devices or interfaces are selected, each device or interface's dataset appears as a line or bar on the graph. The Group check box allows you to group the datasets from multiple devices or interfaces into a single dataset that shows the minimum, average or maximum value for all devices in the group over the selected time period.

To view devices or interfaces as one dataset:

- Select the **Group** check box.

Selecting Columns (Table view)

In Table view, regardless of the selected dataset, use the **Columns** selector to choose the columns to show in the report.



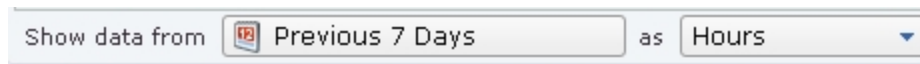
Using the Page Controls

Use the page controls to choose the page of data you want to view.



- Click the left and right arrow buttons to move to the start or end of the report or to move to the previous or next page.
- Type in a page number to move to that page.
- Use the dropdown selector to specify the number of results are shown on a page.

Selecting a Data Range



You can limit the amount of data from the dataset that is displayed in the report. In selecting a data range, you select data over a time range, and control the density of that data over the specified range. You do this using the **Show Data From** controls at the bottom of the window. Select a range of data by date, and specify the units to use (hours, days, weeks, months, etc.). Learn more about data range selection options in Data Range Options, below.

Data Range Options

Previous

Select a data in a range of time previous to today.

Previous	24 hours
... to Date	7 days
Specific date	30 days
All dates before	365 days
All dates after	
Date range	

Previous 7 Days as Hours Filters

...to Date

Select all data from beginning of the most recent day, week, month, or year.

The time units vary with your selection.

Previous	Day
... to Date	Week
Specific date	Month
All dates before	Year
All dates after	
Date range	

Previous 7 Days as Hours Filters

Specific date

Select data for a specific date.

Previous	December 2010
... to Date	
Specific date	
All dates before	
All dates after	
Date range	

Previous 7 Days as Hours Filter

All dates before

Select all data before the specified date.

Previous	December 2010
... to Date	
Specific date	
All dates before	
All dates after	
Date range	

Previous 7 Days as Hours Filter

All dates after

Select all data after the specified date.

Previous	December 2010
... to Date	
Specific date	
All dates before	
All dates after	
Date range	

Previous 7 Days as Hours Filter

Date Range

Select data from the specified range of dates.

Previous

... to Date

Specific date

All dates before

All dates after

Date range

Previous 7 Days

December 2010

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

December 2010

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Specifying Time Units

In addition to selecting a range of data over time, you can specify the units used to display the data.

Of course, the data units selected affect the time it takes to display the report. (Displaying data every 5 minutes over a year, for example, represents a large amount of data.)

Newest Value

5-Minute

Hours

Days

Weeks

Months

Combined

Days

Creating and Using Data Filters

You can limit the amount of data, or select specific subsets within a dataset, using Filters.

To create a filter:

- Click the Filters button. A new filter control appears.

Filter Options

Filters generally have three parts:

- **Data field** - the default value is Any Field.
- **Comparison operator** - the default value is Matches.
- **Comparison value** - no default value

The available values for comparison operators depend on the type of data field selected.

Data field options

This menu lists all the available fields in the dataset.



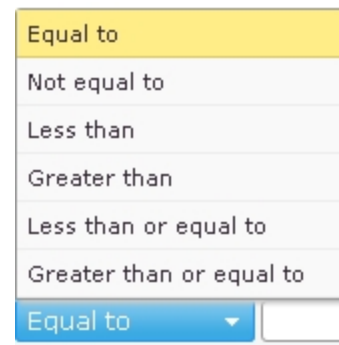
Comparison operators (non-numeric fields)

When comparing values in non-numeric fields, a simple boolean comparison operator is available.



Comparison operators (numeric fields)

When comparing numeric values, a number of comparison operators are available.



Multi-part Filters

You can create filters with more than one set of filter criteria.



The screenshot shows a user interface for creating multi-part filters. It consists of a light blue horizontal bar containing three filter criteria sets. Each set is a small box with a dropdown menu for 'Any Field', a dropdown menu for 'Matches', an empty text input field, and a small 'x' button to remove the criterion. A small blue square with a white plus sign is located to the right of the third criterion set, indicating where to click to add more criteria.

To add a filter to an existing filter set:

- Click the Plus button.



To remove a filter from an existing filter set:

- Click the X button.



Choosing a Report Style

Four report styles available:

- **Table** - a list-style report with rows and columns.
- **Area** - a line chart with the area below the line filled.
- **Line** - a line chart.
- **Bar** - a standard bar chart.

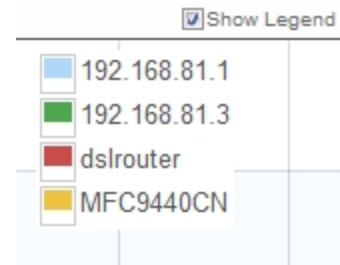
To choose a report style:

- Click one of the report style tabs in the lower right of the window to choose a report style.

Note: Area, Line, and Bar styles are available only for datasets with numeric values.

Showing or Hiding the Legend

For Area, Line, and Bar styles, select or clear the **Show Legend** check box to show or hide the legend, as shown at right.



Viewing Data Point Values

In Area, Line and Bar styles, mouse over a data point to see its value.

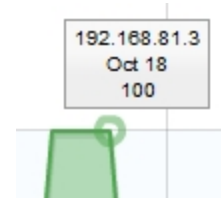

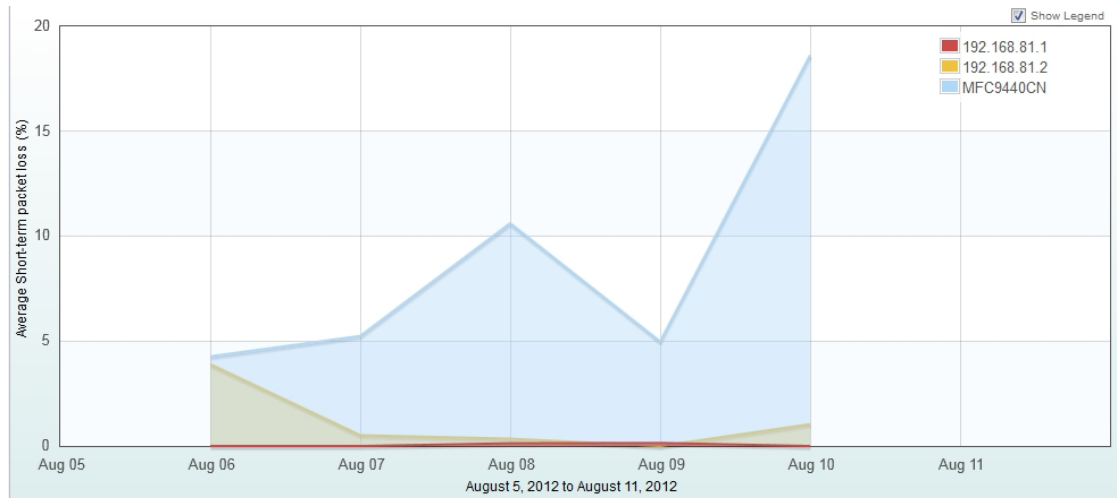


Table Report

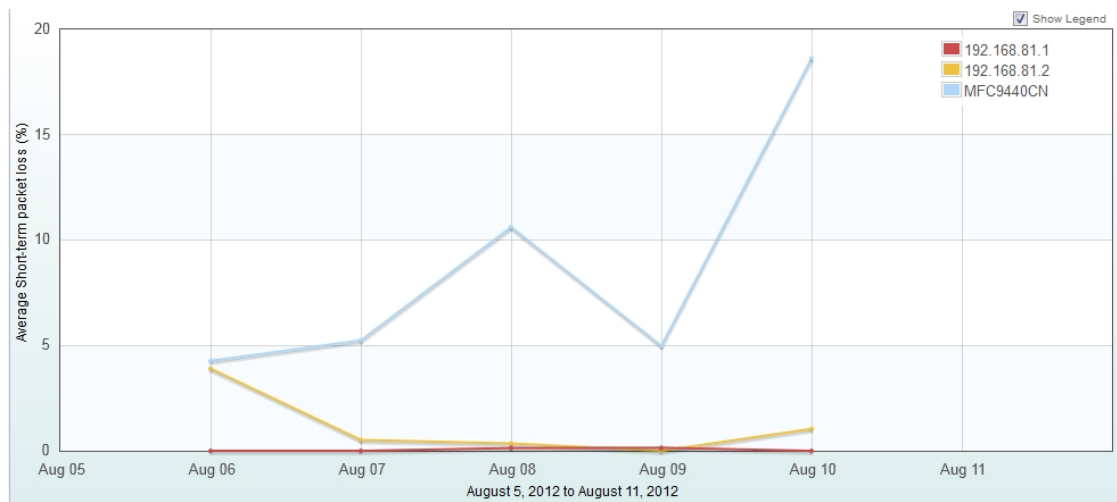


	Map	Device 	Days	Average Short-term packet loss (%)
1	My Network	192.168.81.1	2012-08-06 00:00:00	0.00
2	My Network	192.168.81.1	2012-08-07 00:00:00	0.00
3	My Network	192.168.81.1	2012-08-08 00:00:00	0.13
4	My Network	192.168.81.1	2012-08-09 00:00:00	0.15
5	My Network	192.168.81.1	2012-08-10 00:00:00	0.00
6	My Network	192.168.81.2	2012-08-06 00:00:00	3.90
7	My Network	192.168.81.2	2012-08-07 00:00:00	0.52
8	My Network	192.168.81.2	2012-08-08 00:00:00	0.35
9	My Network	192.168.81.2	2012-08-09 00:00:00	0.00
10	My Network	192.168.81.2	2012-08-10 00:00:00	1.04
11	My Network	MFC9440CN	2012-08-06 00:00:00	4.28
12	My Network	MFC9440CN	2012-08-07 00:00:00	5.24
13	My Network	MFC9440CN	2012-08-08 00:00:00	10.62
14	My Network	MFC9440CN	2012-08-09 00:00:00	4.99
15	My Network	MFC9440CN	2012-08-10 00:00:00	18.63

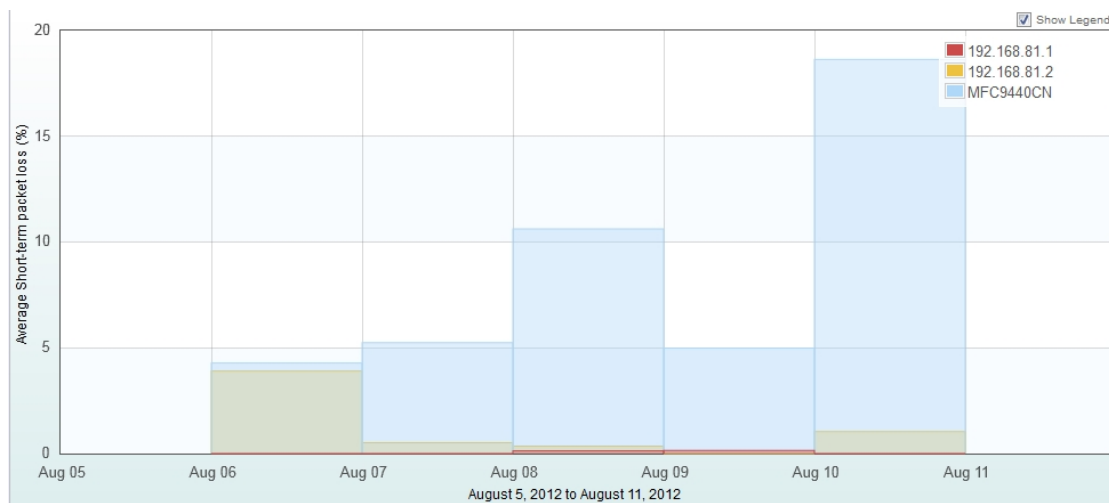
Area Report



Line Report

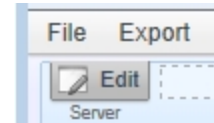


Column Report

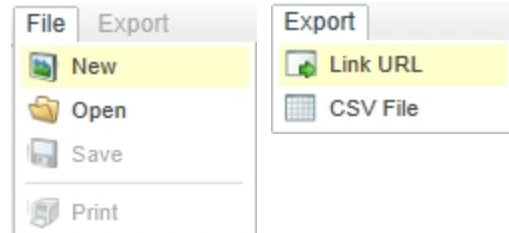


Managing and Printing Your Reports

Use the Edit button to switch between Edit and View modes.



Use the File and Export menus to create new reports, to Load, Save, to get a Link URL for distribution or to Export a report to a CSV file.

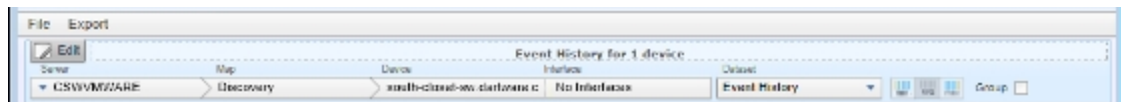


Switching to Edit Mode

To edit a report, you must be in Edit mode.

To switch to Edit mode:

- Click the **Edit** button. The Edit controls appear as shown below. Click again to switch back to View mode.



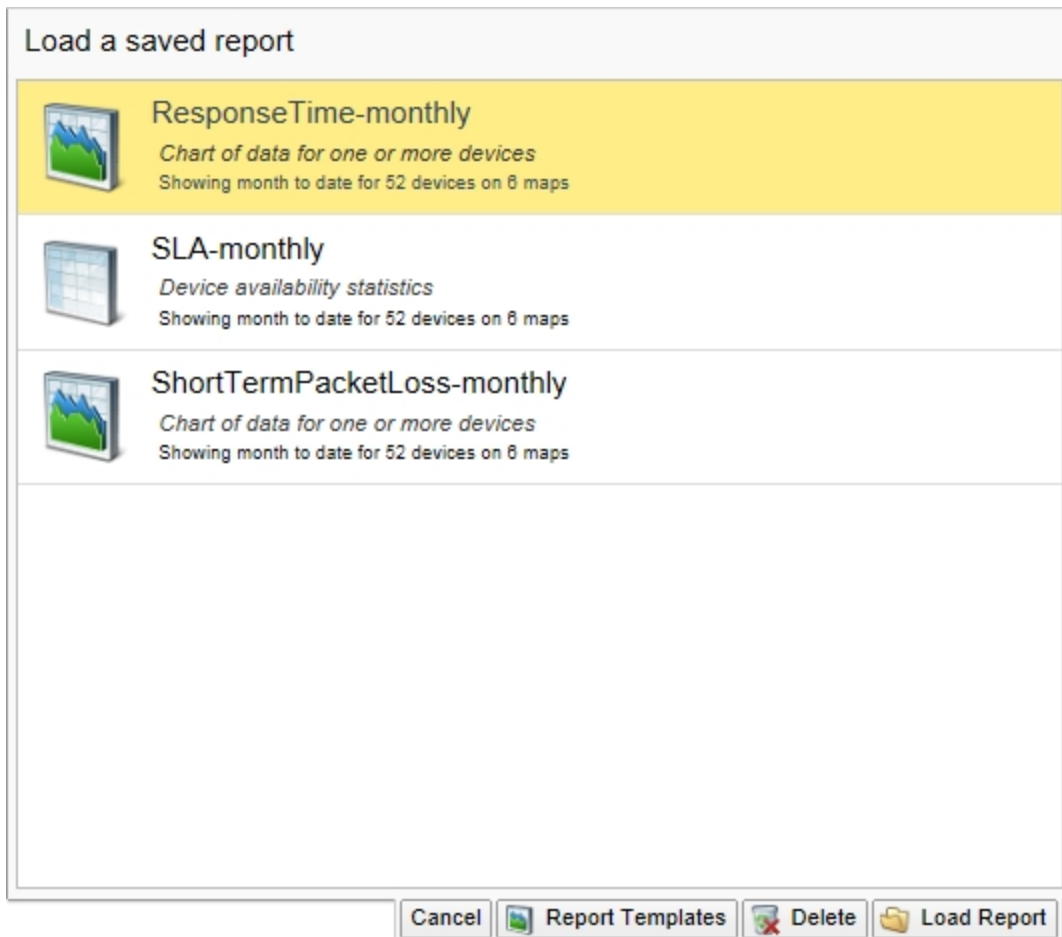
Reports window in Edit mode

Loading a Saved Report

You can save any number of reports, then open, view or print them at a later time.

To open a saved report:

1. From the Report window's File menu, choose **Open**. A list of saved reports appears, as shown below. Each report shows a summary of selected parameters.
2. Click the report you want to load, then click **Load Report**. To create a new report instead, click **Report Templates** to view available templates.



The Saved Reports list

Deleting a Saved Report

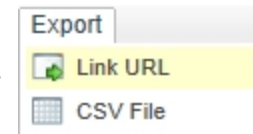
You can delete a saved report from the Saved Reports list.

To delete a saved report:

1. From the Report window's File menu, choose **Open**. A list of saved reports appears, as shown above.
2. Click the report you want to delete, then click **Delete**. A Confirm window appears.
3. Click **OK**. The selected report is removed from the list.

Exporting and Linking to a Report

Use the Report window's Export menu to obtain a URL for distribution, or to export the report data in a CSV file.



To get the URL to a report:

1. After viewing the report, choose **Link URL** from the Report window's Export menu. The Link URL box appears as shown.



2. Copy the URL and paste it into an email, document, or other container you want to use to distribute it.
3. Click **Cancel** to close the Link URL box.
4. To protect the URL from being changed, select **Lock against changes**.

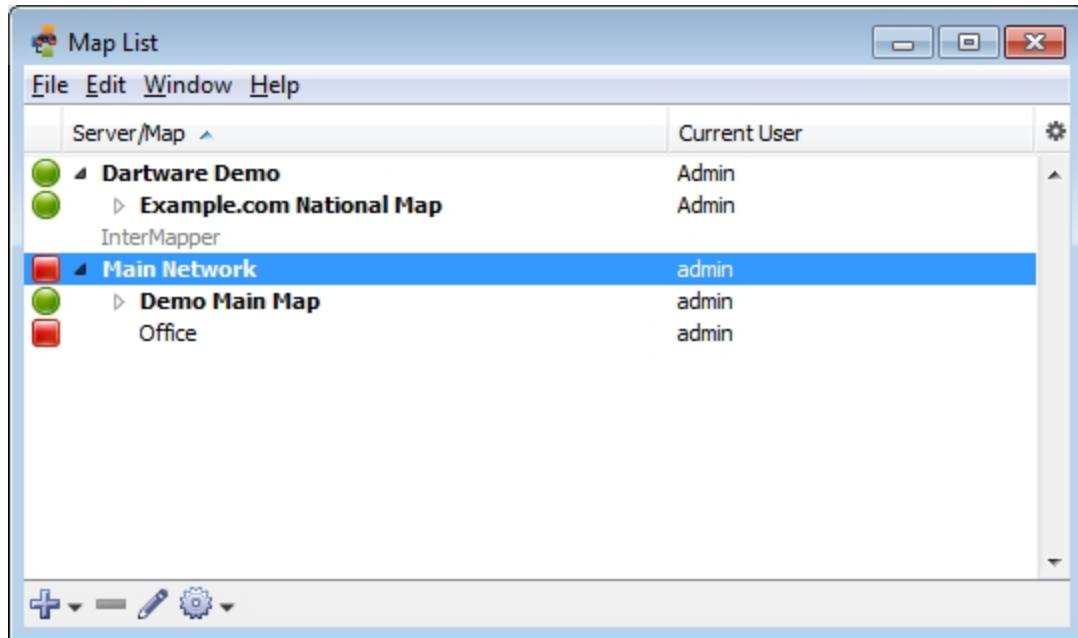
To export a CSV file:

1. After viewing the report, choose **CSV File** from the Report window's Export menu. The result depends on your browser, but a file save action is initiated.
2. Choose a location for the file, and click **Save** (again, the actual name depends on your browser.) A CSV file is saved to the specified location.

Chapter 12

Using InterMapper RemoteAccess

InterMapper can make its maps available to people who are away from the server. They can use a program called [InterMapper RemoteAccess](#) to view and configure the server.



InterMapper RemoteAccess's Map List window

InterMapper RemoteAccess is capable of configuring every aspect of InterMapper. For more information about enabling the Remote server, and a description of how to set up access permissions per-map or by IP address, see [The Remote Server \(Pg 282\)](#).

InterMapper RemoteAccess is also accessible through a [command-line interface](#).

Note to Windows users: By default, XP, Vista, and Windows 7 have significant firewalling turned on. You need to create exceptions ("poke holes") in the firewall in order to use the remote server, web server, telnet server, or DataCenter server as well as to monitor SNMP traps. For detailed information, see [Using InterMapper with Windows XP SP2 and Vista](#) in the InterMapper Knowledgebase.

Command and Menu Reference

This chapter describes each of the menu commands in detail. Each topic listed below contains a summary of the commands available from each menu.

File Menu (Pg 375)

Use the File menu to execute commands for opening, closing, and saving maps, for printing windows, and for quitting InterMapper. You can also import and export maps from the File menu.

Edit Menu (Pg 380)

Use the Edit menu to execute commands for copying and pasting data as well as commands for selecting and hiding items in maps.

View Menu (Pg 384)

Use the View menu to change the way in which you view a map. The View menu is available only from a map window.

Monitor Menu (Pg 387)

Use the Monitor menu to re-probe one or more devices on a map, to edit information about one or more devices, and to open various windows related to map items. The Monitor menu is available only from a map window.

Insert Menu (Pg 404)

Use the Insert menu to insert devices, networks, links, text blocks or icons, and to group or un-group probes. You can also initiate the Auto-discovery process or scan a network, or set a benchmark for use with geographic coordinates. The Insert menu is enabled only when the Map Editor is active and when you are viewing a map window.

Format Menu (Pg 411)

Use the Format menu to format and arrange items on the map. The Format menu is enabled only when you are viewing a map window, the Map Editor is active, and you have one or more map items selected. The Format menu is available only from a map window.

Window Menu (Pg 425)

Use the Window menu to execute commands for controlling the view of the current map, for viewing Log files, and for bringing open windows to the front.

Help Menu (Pg 430)

Use the Help menu to view the on-line help system, to view information about InterMapper, and to report bugs or send screenshots to Help/Systems.

InterMapper and IM RemoteAccess Menus (Pg 434)

Macintosh OSX adds an InterMapper menu or IM RemoteAccess menu. These menus contain menu items that normally appear in other menus on other platforms.

Context Menus (Pg 435)

Context menus are implemented through the InterMapper user interface. These menus allow you to choose options that are available only for and related to specific objects in the window.

Keyboard Shortcuts (Pg 436)

Certain menu items have keyboard shortcuts. The topics listed above contain the keyboard shortcuts available in the listed menus. For more information on keyboard shortcuts and how they relate to different platforms, see [Keyboard Shortcuts \(Pg 436\)](#).

File Menu

Use the File menu to create new maps, open existing maps, and to save maps that you have edited. You can also import and export maps, and can set up and print maps. The table below shows the commands available from the File menu, and which commands are available from the Map or Map List window.

Note: Use shortcuts with Control key (Windows) or Command key (Macintosh.)

IMRA = Map List window, InterMapper RemoteAccess

IM = Map List window, InterMapper

Map = Map window

Command	Description
New Map (Pg 377)	Creates a new map.
Open Recent (submenu) (Pg 377)	Choose a recently-opened map from this submenu.
Close (Pg 377)	Closes the current window.
Backup... (Pg 377)	Backs up the current map.
Restore... (Pg 378)	Restores the current map from a backup.
Rename... (Pg 378)	Renames the selected map.
Duplicate... (Pg 378)	Makes a copy of the selected map.
Disable... (Pg 378)	If you have administrator privileges, use this command to disable the current map (Map Window) or the selected map (Map List window.)
Import (submenu) (Pg 378)	Choose from these submenu commands: <ul style="list-style-type: none"> • Map... - Copies a map file saved on the InterMapper RemoteAccess machine to the InterMapper server and makes it available. (Use the Export... command to save the file on the InterMapper RemoteAccess machine.) • Data File... - Creates maps or updates devices from a tab-delimited import file. For more information, see Importing Data Into Maps (Pg 637). • Probe... - Imports custom probe files to your server. • MIB... - Imports an SNMP MIB file for a specific device or family of devices.
Export (submenu) (Pg 379)	Choose from these submenu commands: <ul style="list-style-type: none"> • Map... - Save a copy of a server's map to the InterMapper RemoteAccess machine. • Data File... - Save a file containing selected data from a map in Tab-delimited, CSV, HTML, or XML format. • Image... - Save a PNG image of the selected map.

Server (submenu)

Choose from these submenu commands:

- **Log In...** - Log into an InterMapper server.
- **Log Out** - Log out of an InterMapper server.
- **Info** - View (**IM**) and change (**IMRA**) server name, address and port info.

Page Setup... (Pg 379)
Print... (Pg 379)

Opens the standard Page Setup dialog. (**Map**)
Prints the current window on the currently selected printer. (**Map**)

Print Single Page...

Prints a single page of a map in the current view.
(**Map**)

Exit/Quit (Pg 379)

Exits the application.

Note: On Macintosh, this command is available from the [InterMapper or IM RemoteAccess menu](#).

New Map

Creates a new empty map. See the [Autodiscovery \(Pg 406\)](#) menu command for details about creating a map automatically.

Open Recent (submenu)

Choose a recently-opened map from a submenu.

Close

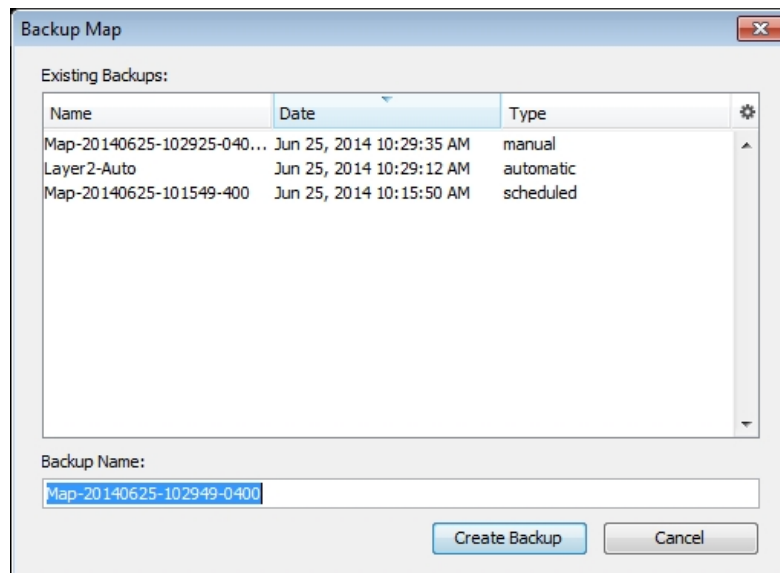
Closes the current window.

Note: Closing a map window does not stop the map's devices from being polled or from sending notifications. To prevent a map from being polled, disable the map in the Enabled Maps section of the [Server Settings window \(Pg 277\)](#).

Backup...

Makes a snapshot backup of the current map.

The Backup Map window shows a list of previous backups of the selected map. Enter a name for the backup or accept the default name, then click **OK**.



Backup Types

InterMapper creates the following backup types:

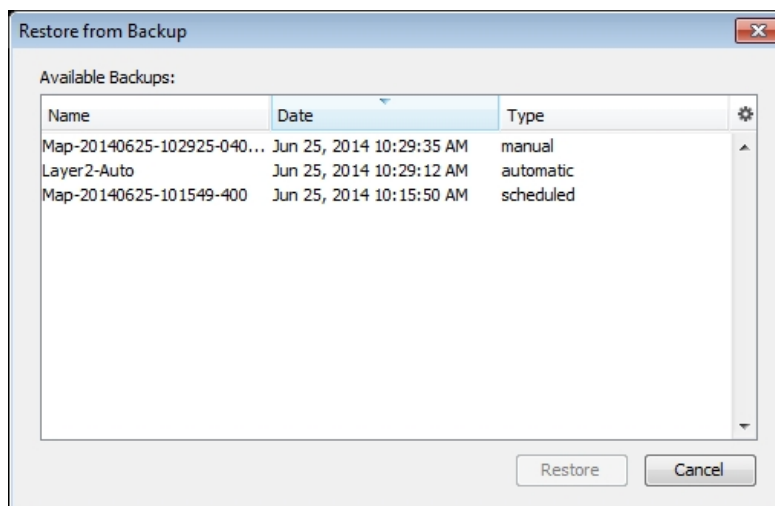
- **Manual** - the backup was created using the Backup... command.
- **Automatic** - the backup was created automatically by enabling Layer 2 in a map and clicking **Change Now**.
- **Scheduled** - the backup was created automatically, based on a schedule defined in the Map Backup panel of the Server Settings window.

Restore...

Restores from a previous backup of a map.

The Restore Map window shows a list of previous backups. Click the backup you want to restore, then click **OK**.

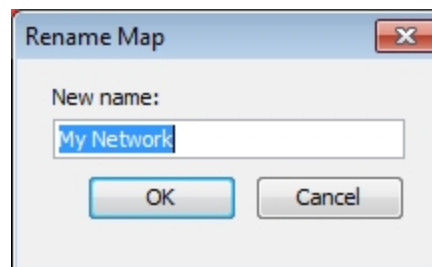
See Backup... (above) for information on backup types.



Rename...

Renames the selected map.

Enter a new name for the selected map, then click **OK**.



Duplicate...

Makes a copy of the selected map.

Disable...

If you have administrator privileges, use this command to disable the current map (Map Window) or the selected map (Map List window.) A confirmation dialog appears.

Import (submenu)

Use the Import submenu to choose from the available Import commands:

Data File...

Use the **Import > Map...** command to import a map from a tab-delimited, comma-delimited, or XML file. For more information, see [Importing Data Into Maps \(Pg 637\)](#).

InterMapper Map...

Copies a map file saved on the InterMapper RemoteAccess machine to the InterMapper server and makes it available. (Use the Export... command to save the file on the InterMapper RemoteAccess machine.)

Probes...

Imports custom probe files to your server. For more information, see the InterMapper [Developer Guide](#).

MIB...

Imports an SNMP MIB file for a specific device or family of devices. You can use the MIB file information to enhance the formatting of the displayed data. For example, certain views (especially in log files and the SNMP Table views) use the MIB data to display numeric values as the human-readable strings.

Export Map...

Use the Export Map... command to save a copy of your map on your local machine or network drive. This is an easy way to copy a map from one server to another. After you export the map file, you can then import it to a different server. You can also export a tab-delimited file for use in a spreadsheet or database.

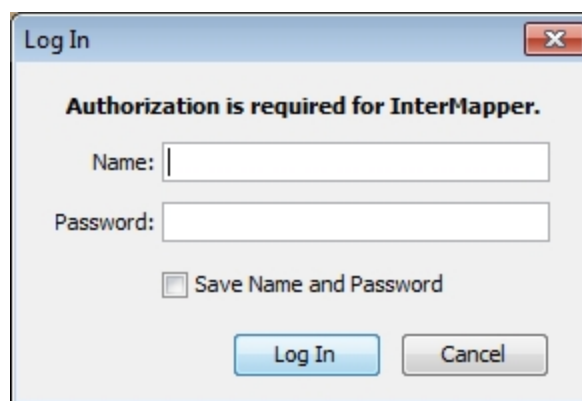
For more information, see [Exporting Data From Maps \(Pg 635\)](#).

Server (submenu)**Log In...**

In the Map List window, click the server you want to log into, then choose **Log In...** from the File menu. An authentication window appears:

Enter a **Name** and **Password**. If you want to save the Name and Password, click to select **Save Name and Password**.

Note: SASL authentication is used for logins.

**Log Out**

In the Map List window, click a map on the server you want to log out from, then choose **Log Out**. You are disconnected from the selected server.

Note: Open windows for any maps on the selected server remain open after you log out, but the maps are dimmed to indicate that they are no longer active.

Page Setup...

Opens a standard Page Setup dialog.

Print...

Prints the current window on the currently selected printer. This operation uses as many pages as necessary to print the entire map or window contents.

Exit/Quit

Exits the application.

Edit Menu

The Edit menu contains standard editing commands, as well as various commands for selecting and finding items.

Menu Command	Description
Undo (Pg 381)	(Map Window only) Most operations in <i>InterMapper</i> can be undone. Undo is multiple levels.
Redo (Pg 381)	(Map Window only) Available after you execute the Undo command. Restores the state of the map before the Undo command was executed.
Revert... (Pg 381)	(Map Window only) Restores the state of the map as it was when you last opened it for editing.
Cut (Pg 381)	Cut the selected items to the clipboard.
Copy (Pg 381)	Copy the selected items to the clipboard.
Paste (Pg 381)	Paste the contents of the clipboard to the current window.
Delete (Pg 381)	Removes the selected items from the map. Caution: This operation cannot be undone.
Select (submenu) (Pg 381)	Choose from a variety of commands to select objects in a variety of ways. (Map Window only)
Select All (Pg 382)	(Map List Window only) Select all maps and servers.
Find (submenu) (Pg 382)	<ul style="list-style-type: none">• Find (Pg 382) - Opens the Find window. Enter a text string to search for.• Find Next (Pg 382) - Search for the next occurrence of the last defined text string.• Find Device... (Pg 382) - Search for a device in a map on a connected server.
Map Settings... (Pg 382)	Opens the Map Settings window.
Server Settings... (Pg 383)	Opens the Server Settings window.
Preferences... (Pg 383)	Opens the Preferences window for the InterMapper client application or InterMapper RemoteAccess client application. Note: On Macintosh, this command is available from the InterMapper or IM RemoteAccess menu .

Undo

Reverses the previous operation. Most operations in *InterMapper* can be undone. Undo is multiple levels.

Redo

Re-performs the previous undo operation. Any operation that has been undone can be redone.

Note: The Undo/Redo function is sequential; if you undo multiple operations, then perform a different operation, all the operations you undid are gone.

Revert

Restores the state of the current map to its last state when it was last enabled for editing.

Cut

Cuts the selected items to the clipboard.

Copy

Copies the selected items to the clipboard.

Paste

Pastes the contents of the clipboard to the current window.

Delete

Removes the selected items from the current window.

Select (submenu)

Choose any of these options from the **Select** submenu.

- **Select All** - Selects all map items.
- **Select Adjacent** - Selects all map objects connected to the current selection. The first time you choose the command, all leaves are selected (a leaf is an object that has no other connections.) Choose the command a second time to select all other objects connected to the selected object. Continue choosing the command to continue expanding the selection, first selecting the leaves, then the others objects

Note: If you select a device connected to a network, then choose **Select Adjacent**, the network is selected, but none of the other devices connected to the network is selected. To select a network and its adjacent devices, select the network first, then choose **Select Adjacent**.

- **All devices** - Select all devices, but not links or networks
- **DOWN devices** - Select only the devices that are currently marked as down.
- **UP devices** - Select only the devices that are currently marked as up.
- **All networks** - Select all networks, but not the attached devices.
- **DOWN Interfaces** - Select all interfaces currently marked as down.

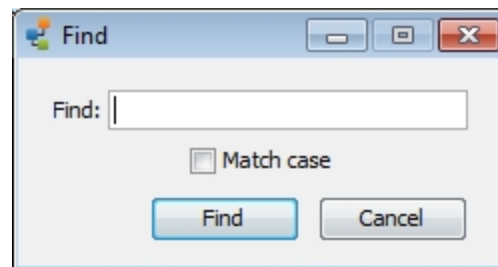
- **Networks with...** - Select all networks with the specified number of attached devices.
- **Unselected** - Invert the selection. Un-selects all selected items; selects all un-selected items.

Select All

(Map List Window) Selects all maps and servers.

Find...

Find the first object containing the specified text in the current map. The device is highlighted when it is found.



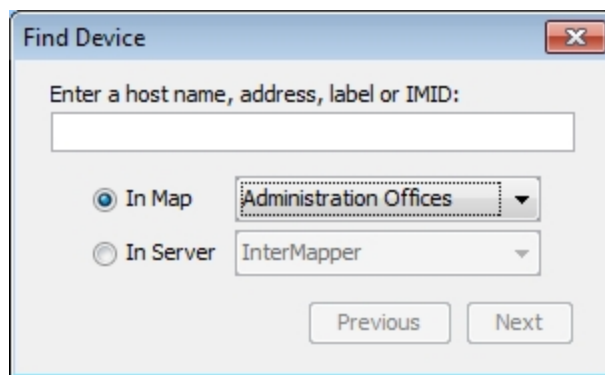
The Find window

Find Next

Finds the next item in the current map that matches the previously specified text string.

Find Device...

Find the a device on the specified map or server. You can enter a host name, address, or IMID. This could be useful to help you determine, for example, the device from which a dataset in the database came.



The Find Device window

Map Settings...

Use the Map Settings... command to view and edit an individual map's color settings, specify a background image, and view and edit the list of default notifiers for the map. See [Map Settings \(Pg 86\)](#) for more information. This command is available only in Edit mode.

Server Settings...

Use the Server Settings command to open the Server Settings window. Use the Server Settings window to view server information, and to view and edit all server preferences and settings. You can control the settings of the built-in Web, InterMapper RemoteAccess, and Telnet servers. See [Server Settings \(Pg 249\)](#) for more information.

Preferences...

Use the Preferences... command to open the Preferences window to set preferences for the InterMapper client application or for InterMapper RemoteAccess. These settings affect only the copy of the application you are running.

View Menu

Use the View menu in the Map window to specify how you want to look at a map. The view menu is available only from the map window.

Menu Command	Description
Map (Pg 384)	View as a map, with graphic objects representing devices, networks and links.
List (Pg 384)	View as a list of devices.
Device Notifiers (Pg 385)	View as a list of devices, each showing the states for which the selected notifier sends notifications.
Link Notifiers (Pg 385)	View as a list of interfaces, each showing the states for which the selected notifier sends notifications.
Charts (Pg 385)	View a list of charts associated with the map.
Datasets (Pg 385)	Select from a list of devices to view a list of datasets available for those devices.
Actual Size (Pg 385)	In Map view, set the zoom level to 100%.
Zoom In (Pg 385)	In Map view, zoom in.
Zoom Out (Pg 385)	In Map view, zoom out.
Sort (submenu) (Pg 385)	In any list view, choose from a list of columns to sort the list by. Note: You can also sort the list by clicking a column heading. Click again to reverse the sort.
Columns (submenu) (Pg 385)	Choose the columns you want to show in any list view.
Filter (submenu) (Pg 385)	Choose to view only those objects with the selected state.
Expand All (Pg 386)	In List view, expands all hierarchical items in the Map and Device List windows.
Collapse All (Pg 386)	In List view, collapses all hierarchical items in the Map and Device List windows.
Show/Hide Toolbar (Pg 386)	(Map List Window only) Choose to show or hide the toolbar.
Edit Map (Pg 386)	Toggles between Map Edit mode and Monitor mode.

Map

Keyboard Shortcut: Ctrl+1

View as a map, with graphic objects representing devices, networks and links.

List

Keyboard Shortcut: Ctrl+2

View as a list of devices, networks, and links.

Device Notifiers

Keyboard Shortcut: Ctrl+3

View as a list of devices, each showing the states for which the selected notifier sends notifications.

Link Notifiers

Keyboard Shortcut: Ctrl+4

View as a list of interfaces, each showing the states for which the selected notifier sends notifications.

Charts

Keyboard Shortcut: Ctrl+5

View a list of charts associated with the map.

Datasets

Keyboard Shortcut: Ctrl+6

Select from a list of devices to view a list of datasets available for those devices.

Actual Size

Keyboard Shortcut: Ctrl+0

In Map view, set the zoom level to 100%.

Zoom In

Keyboard Shortcut: Ctrl+Up Arrow

Zoom Out

Keyboard Shortcut: Ctrl+Down Arrow

Sort (submenu)

From the **Sort** submenu, choose a column by which you want to sort the list. Choose it again to reverse the sort order. Not available in Map view.

Note: You can also click the column heading to sort by that column, and click it again to reverse the sort order.

Columns

From the **Columns** submenu, select or clear the check mark for a column to show or hide the column. Not available in Map view.

Filter (submenu)

Choose to view only those objects with the selected state. Filter devices with the selected state to view only those that are acknowledged or unacknowledged.

Expand All

Expands all hierarchical items in the Map List or Device List window.

Collapse All

Collapses all hierarchical items in the Map List or Device List window.

Show/Hide Toolbar

Choose to show or hide the toolbar.

Edit Map

Select this menu item, click the lock icon at the upper left of the map, or press the **Tab** key.

Toggles the map between *Editing mode* (where the map may be rearranged, edited, and changed) and *Monitoring mode* (where the map is uneditable, but displays the current state of the network.) The menu item has a check mark when map editing is enabled.

Note: Many users can use InterMapper RemoteAccess to connect to an InterMapper server at the same time. At any given time, however, only one user may edit a map. If you try to change a map to Edit mode while it is being edited by another user, a message appears. You can choose to interrupt the other user's editing session, at which time you gain the right to edit the map.

Monitor Menu

Use the Monitor menu to re-probe one or more devices on a map, to edit information about one or more devices, and to open various windows related to map items. The Monitor menu is available only from a Map window.

Menu Command	Description
<u>Reprobe/Reprobe Selection (Pg 389)</u>	Reprobe: If no device is selected, re-poll all devices on the map. Reprobe Selection: Re-poll the selected device (s).
<u>Acknowledge (Pg 389)</u>	Use this command to acknowledge a failure. This stops an icon's flashing, and deactivates recurring notifications.
<u>Un-Acknowledge (Pg 390)</u>	Use this command to remove an acknowledgement from the selected device, and to reactivate notifications.
<u>Info Window (Pg 390)</u>	Open the Info Window for the selected device or network.
<u>Status Window (Pg 391)</u>	Opens the Status window for the selected device, network, or link.
<u>Interfaces > Window... (Pg 392)</u>	Opens the Interfaces window for the selected device.
<u>Interfaces > Error Thresholds... (Pg 392)</u>	Opens the Error Thresholds dialog. Set error thresholds for one or more interfaces.
<u>Interfaces > Utilization Thresholds... (Pg 393)</u>	Opens the Utilization Thresholds dialog. Set thresholds for utilization of one or more links.
<u>Interfaces > Discard Thresholds... (Pg 393)</u>	Opens the Discard Thresholds dialog. Set packet discard thresholds for an interface.
<u>Interfaces > Behavior... (Pg 394)</u>	Opens a device's Behavior dialog. Specify whether to allow periodic reprobes, and whether to display unnumbered interfaces.
<u>Notifiers Window (Pg 394)</u>	Opens the Notifiers window, and shows a list of notifiers for the selected device.
<u>SNMPWalk... (Pg 396)</u>	Opens the SNMPWalk dialog.
<u>Flows Window (Pg 397)</u>	Opens the Flows Window if you have installed the InterMapper Flows add-on.
<u>Show in Layer 2 (Pg</u>	Opens the Device List window in Layer 2 view, and

344)	shows connections to the selected device.
<u>Set Info > Set Address... (Pg 397)</u>	Set the IP address or name for the selected device.
<u>Set Info > Set Comment... (Pg 399)</u>	Enter a comment about the selected device(s).
<u>Set Info > Set Community... (Pg 399)</u>	Set the SNMP community string for the selected devices.
<u>Set Info > Set Data Retention... (Pg 399)</u>	Select a Data Retention policy to use when storing data to the InterMapper Database.
<u>Set Info > Set Double-click (submenu) (Pg 403)</u>	Define the action to be taken when you double-click the selected device.
<u>Set Info > Set Kind... (Pg 400)</u>	Set the device kind you want to use when storing data to the InterMapper Database.
<u>Set Info > Set Latitude & Longitude... (Pg 400)</u>	Set the latitude and longitude for the selected devices.
<u>Set Poll Interval... (Pg 400)</u>	Set the poll interval for the selected devices.
<u>Set Info > Set Probe... (Pg 401)</u>	Set the probe to be used with the selected devices.
<u>Set Info > Set Thresholds... (Pg 402)</u>	Set the criteria for sending notifications that a device is down, in alarm, or in warning. These settings apply to all devices on the map.
<u>Set Info > Set Vantage Point (Pg 402)</u>	Set the selected device as the vantage point from which InterMapper views all other devices on the map.
<u>Reset Short-term Packet Loss (Pg 403)</u>	Resets the accumulated value of short-term packet loss.
<u>Helper Apps (submenu) (Pg 403)</u>	Launch a helper application or customize the list of applications.

Reprobe/Reprobe Selection

Re-poll the selected device(s). This is useful for retrieving the status of a device or detecting that it has returned to service.

- **If a single device is selected**, it is polled as soon as possible.
- **If many devices are selected**, they are moved to the head of the poll queue so they will be polled as soon as possible.
- **If no devices are selected**, all devices in the map are moved to the head of the poll queue, and are polled as soon as possible.

Acknowledge

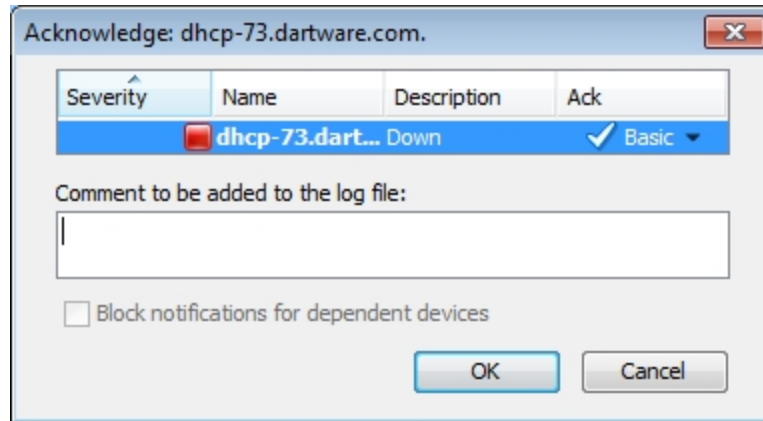
When Inter-Mapper detects a problem with a device, the device's icon changes to yellow, orange, or red. This serves to attract attention to the failure, but can be dis-

tracting after corrective action has been initiated. It also masks further failures: if several items on a map are already in alarm, it's hard to notice new problems.

Use the Acknowledgement command to indicate that the network administrator is aware of a problem, and may have initiated corrective action. Acknowledging an alarm turns the device's icon blue, and also stops repeated notifications for that device.

For a complete description of the Acknowledgements window, see [Acknowledging Device Problems \(Pg 202\)](#).

Note: Another feature - dependencies - is useful for controlling the number of notifications you receive when there are failures of central equipment. See [Using Notification Dependencies \(Pg 136\)](#) for more information.



The Acknowledge Message Window. Data typed here is entered into the InterMapper log file, as well as appearing in the device's Information window.

Un-Acknowledge

Use this command to restore the flashing icon for a device that has been acknowledged in error, or which needs further attention. Un-acknowledging a device reactivates recurring notifications.

Info Window

The screenshot shows a window titled "Info for W" with a sidebar on the left containing buttons for "General", "SNMP", "Probes", "Thresholds", "Icon", "Label", and "Advanced". The "General" tab is selected. The main area contains the following fields and sections:

- Address:** 192.168.81.2
- Host Name:** (empty text field)
- Don't change address or name:** (dropdown menu)
- Use as Map's Vantage Point:** (checkbox, currently unchecked)
- Database Information:**
 - IMID:** device.1.5.27
 - Kind:** Unspecified (dropdown menu)
 - Retention Policy:** 24 Hours (dropdown menu)
- Geographical Location:**
 - Latitude:** (empty text field)
 - Longitude:** (empty text field)
- Comment:** (empty text area)

Callouts in the image provide additional instructions:

- "Select info to edit" points to the sidebar buttons.
- "Edit info here" points to the main content area.
- "Set this device as the map's vantage point" points to the "Use as Map's Vantage Point" checkbox.
- "Click to change to Edit mode" points to a lock icon at the bottom left.

At the bottom right, there are three buttons: "OK", "Cancel", and "Apply".

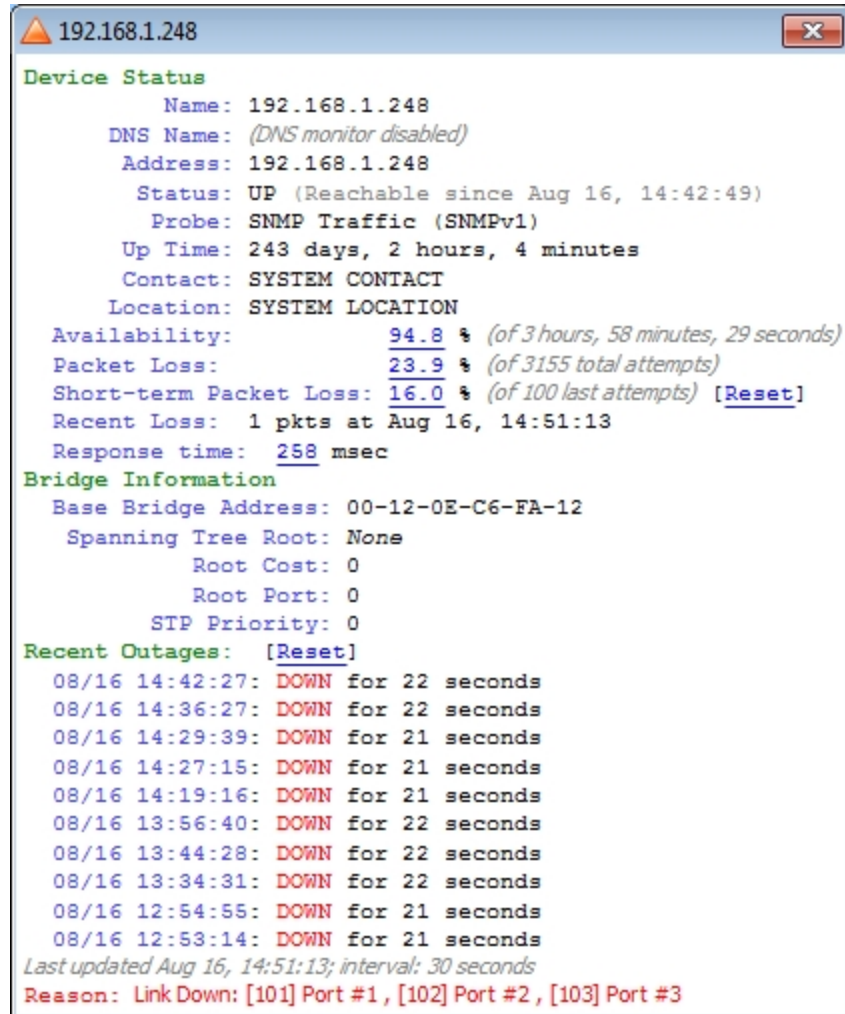
Use the [Info window \(Pg 185\)](#) command to view information about the selected device or network.

- Click the lock icon to change to Edit mode.
- Click a button at left to view that Info pane.

Status Window

Open the [Status window \(Pg 185\)](#) for the selected device. This command is active in Map Edit mode, which is useful for creating charts.

The example below shows a Device Status window. Status windows are also available for networks and links. For examples, see [Status windows \(Pg 185\)](#).



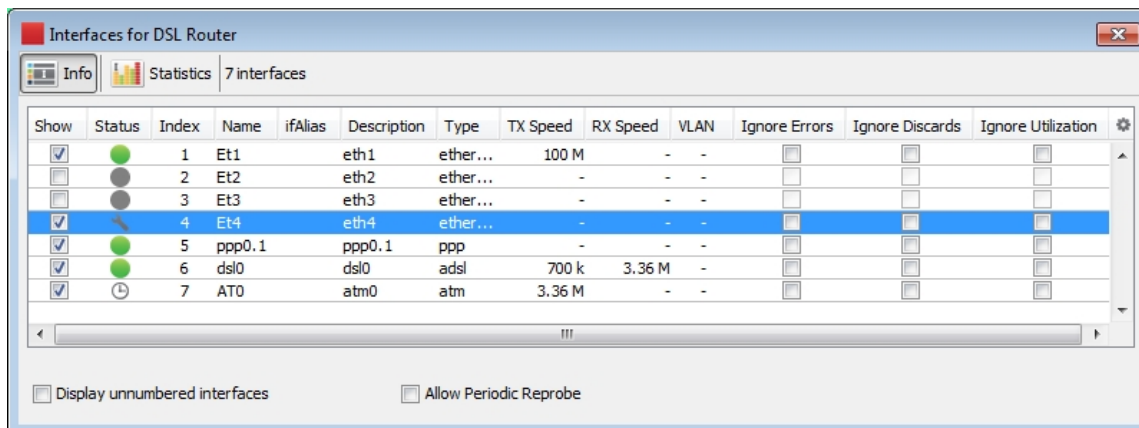
Status window

Interfaces Window

Open the [Interfaces window](#) (Pg 195) for the selected device.

Info View

Use the Info view of the Interfaces window to view the status of interfaces for the selected device, to hide or show them, to specify mapping behavior, and to choose what thresholds to ignore. You can also access the Interfaces submenu for one or more interfaces.

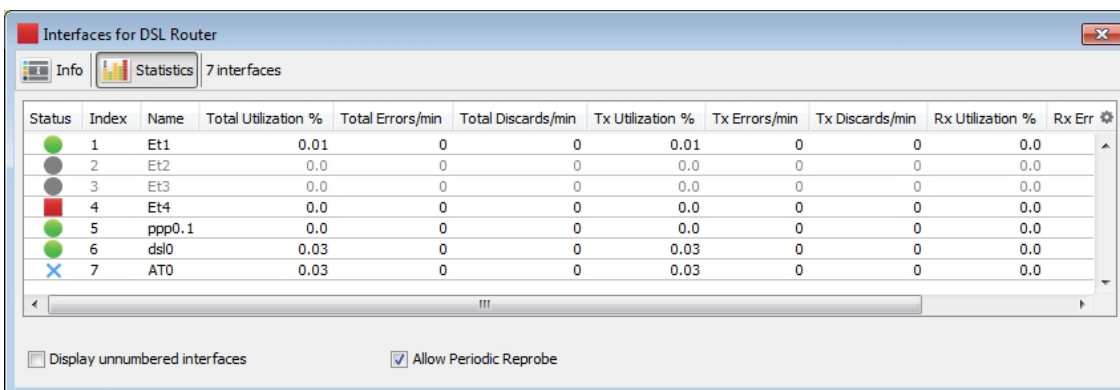


Interfaces window - Info View

For more information, see [Interfaces window](#) (Pg 195).

Statistics View

Use the Statistics view of the Interfaces window to see various statistics for all interfaces on a device.



Interfaces window - Statistics view

For more information, see [Interfaces window](#) (Pg 195).

Error Thresholds Window

Use the Error Thresholds window to override map defaults and set thresholds for link errors on the selected devices. For more information, see [Setting Thresholds](#) (Pg 208).

Link Error Thresholds for Device 'DSL Router'

Set interface thresholds to alert you to network problems.

Error Thresholds

☒ Use map defaults

	Warning	Alarm	Critical	
Rx Errors (Received):	10	20	30	per minute
Tx Errors (Transmitted):	10	20	30	per minute
Total Errors (Rx + Tx):	10	20	30	per minute

OK Cancel

Utilization Thresholds Window

Use the Utilization Thresholds window to override map defaults and set thresholds for link utilization on the selected devices. For more information, see [Setting Thresholds \(Pg 208\)](#).

Link Utilization Thresholds for Device 'DSL Router'

Set interface thresholds to alert you to network problems.

Utilization Thresholds

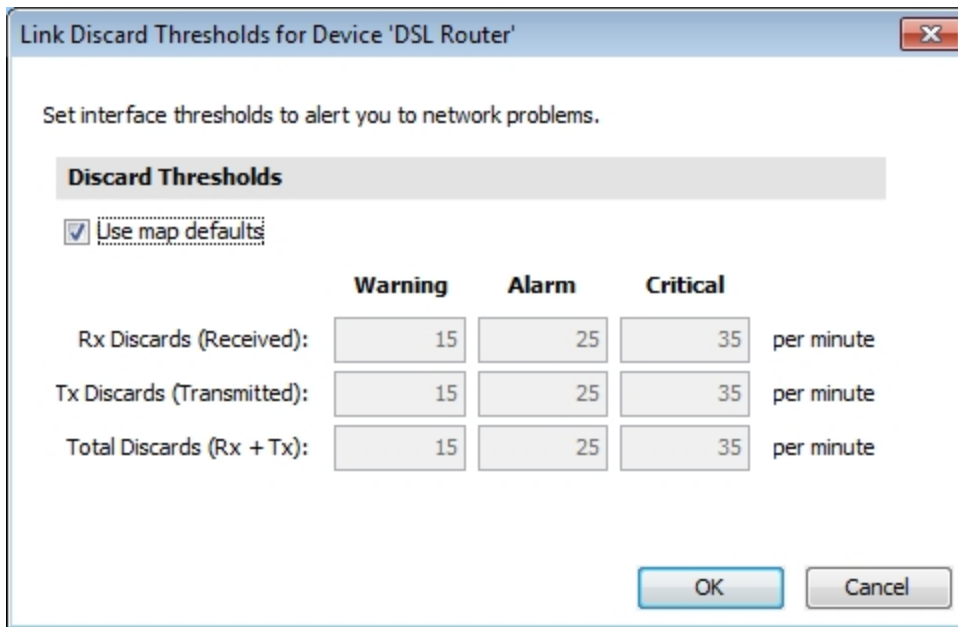
☒ Use map defaults

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

OK Cancel

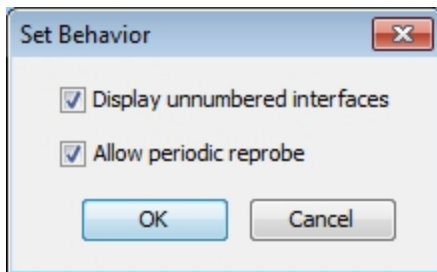
Discard Thresholds Window

Use the Discard Thresholds window to override map defaults and set thresholds for discarded packets on the selected devices. For more information, see [Setting Thresholds \(Pg 208\)](#).



Behavior Window

Use the Behavior window to set the display and polling behavior of the selected devices. This window is also available from the context menu; the options are also available from the [Interfaces window](#) (Pg 392).



Notifiers Window

Open the Notifiers window for the selected device.

Attach Notifiers to "MFC9440CN".

Notifier Name	Down	Up	Critical	Alarm	Warn	OK	Trap	Delay	Repeat	Count	
Day Sounds	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	▲
Alternate Sounds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Command Line Notifier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Email Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Email-escalate group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Group Notifier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Night Sounds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
SMS - Escalate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
SMS - Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
SMS - Weekend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
SMS - Weekend Escalate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Syslog Notifier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
Trap Notifier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	
WinPopup Notifier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▾	Never ▾	-	▼

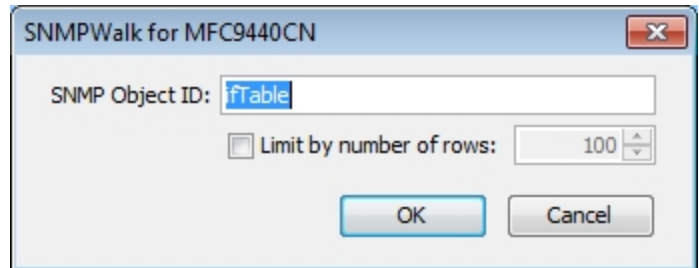
Edit Notifiers...

Notifiers window

SNMPWalk

Use the SNMPWalk com-
mand to execute an
SNMPWalk on the specified
SNMP-enabled device.
Enter a numeric or textual
OID.

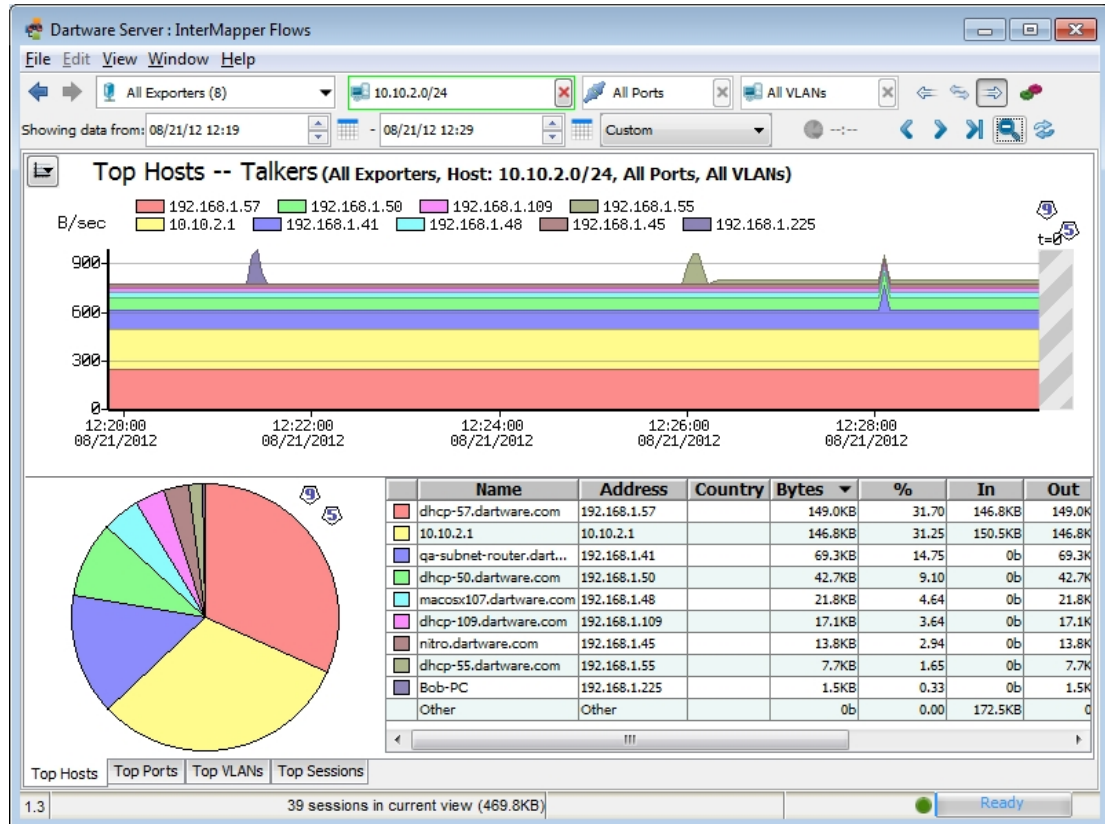
The window below shows
the output of an SNMPWalk
command with ifTable as
the specified OID.



The SNMPWalk dialog

ifTable			
ifTable at 192.168.81.102			
This data collected on: 8/16/12 3:00 PM			
Refresh			
OID	Name	Type	Value
1.3.6.1.2.1.2.2.1.1.1	RFC1213-MIB::ifIndex.1	Integer	1
1.3.6.1.2.1.2.2.1.1.2	RFC1213-MIB::ifIndex.2	Integer	2
1.3.6.1.2.1.2.2.1.2.1	RFC1213-MIB::ifDescr.1	OctetS...	NC-6500h
1.3.6.1.2.1.2.2.1.2.2	RFC1213-MIB::ifDescr.2	OctetS...	SoftwareLoopBack
1.3.6.1.2.1.2.2.1.3.1	RFC1213-MIB::ifType.1	Integer	7
1.3.6.1.2.1.2.2.1.3.2	RFC1213-MIB::ifType.2	Integer	24
1.3.6.1.2.1.2.2.1.4.1	RFC1213-MIB::ifMtu.1	Integer	1500
1.3.6.1.2.1.2.2.1.4.2	RFC1213-MIB::ifMtu.2	Integer	1500
1.3.6.1.2.1.2.2.1.5.1	RFC1213-MIB::ifSpeed.1	Gauge	10000000
1.3.6.1.2.1.2.2.1.5.2	RFC1213-MIB::ifSpeed.2	Gauge	0
1.3.6.1.2.1.2.2.1.6.1	RFC1213-MIB::ifPhysAddress.1	OctetS...	
1.3.6.1.2.1.2.2.1.6.2	RFC1213-MIB::ifPhysAddress.2	OctetS...	
1.3.6.1.2.1.2.2.1.7.1	RFC1213-MIB::ifAdminStatus.1	Integer	1
1.3.6.1.2.1.2.2.1.7.2	RFC1213-MIB::ifAdminStatus.2	Integer	1
1.3.6.1.2.1.2.2.1.8.1	RFC1213-MIB::ifOperStatus.1	Integer	1
1.3.6.1.2.1.2.2.1.8.2	RFC1213-MIB::ifOperStatus.2	Integer	1
1.3.6.1.2.1.2.2.1.9.1	RFC1213-MIB::ifLastChange.1	Timeticks	490
1.3.6.1.2.1.2.2.1.9.2	RFC1213-MIB::ifLastChange.2	Timeticks	0
1.3.6.1.2.1.2.2.1.10.1	RFC1213-MIB::ifInOctets.1	Counter	70754371
1.3.6.1.2.1.2.2.1.10.2	RFC1213-MIB::ifInOctets.2	Counter	0
1.3.6.1.2.1.2.2.1.11.1	RFC1213-MIB::ifInUcastPkts.1	Counter	63900
1.3.6.1.2.1.2.2.1.11.2	RFC1213-MIB::ifInUcastPkts.2	Counter	0
1.3.6.1.2.1.2.2.1.12.1	RFC1213-MIB::ifInNUcastPkts.1	Counter	190013
1.3.6.1.2.1.2.2.1.12.2	RFC1213-MIB::ifInNUcastPkts.2	Counter	0
1.3.6.1.2.1.2.2.1.13.1	RFC1213-MIB::ifInDiscards.1	Counter	0
1.3.6.1.2.1.2.2.1.13.2	RFC1213-MIB::ifInDiscards.2	Counter	0
1.3.6.1.2.1.2.2.1.14.1	RFC1213-MIB::ifInErrors.1	Counter	0

Flows Window



If you have installed the InterMapper Flows add-on, opens the Flows Window, which shows InterMapper Flows information. For documentation about InterMapper Flows, please see [InterMapper Flows \(Pg 315\)](#).

Show in Layer 2

Use the Show in Layer 2 command to open the Device List window in Layer 2 view, and view the connections to the selected devices.

Reports...

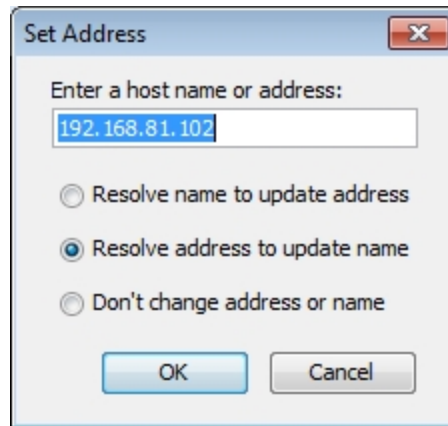
Use the Reports command to open the Reports UI in a browser window. Use the Reports window to create, load, edit, and save reports.

Set Address...

Enter a host name or address - Enter a DNS name or IP address here. InterMapper uses this address to probe the device.

Resolve Name to Update Address - InterMapper queries the DNS for the given name, and uses the result to change the address it uses to poll the device.

Resolve Address to Update Name - keeps the specified IP address fixed, but may update the name from the DNS server if one is found.

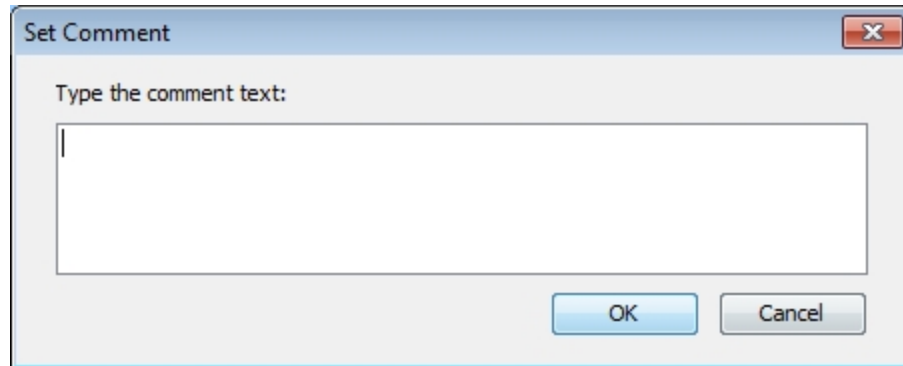


Set Comment...

The comment is seen in the device's status window. Sets the comment for all the selected devices.

(See the Device Status window for details on the comment field.)

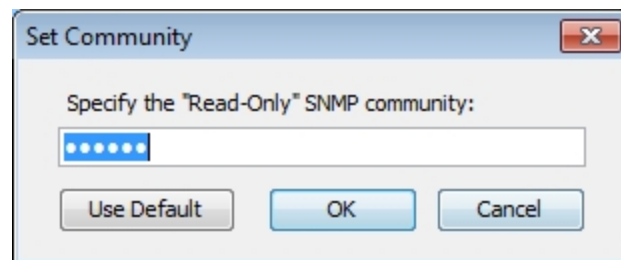
This information is saved as part of the map. Use the Comment field to save the model and serial number for a device, telephone numbers, circuit numbers, or other information related to the item.

A dialog box titled "Set Comment" with a close button (X) in the top right corner. It contains a text input field with the placeholder text "Type the comment text:". Below the input field are two buttons: "OK" and "Cancel".

Set Community...

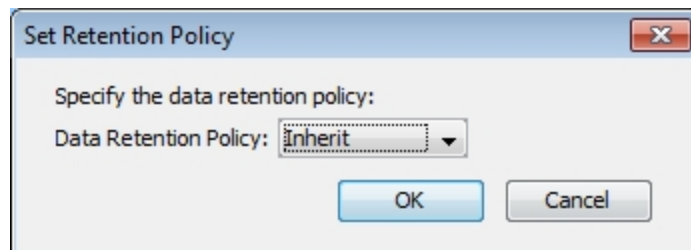
Sets the [read-only community string \(Pg 731\)](#) for all selected devices.

The default community string for most SNMP devices is "public".

A dialog box titled "Set Community" with a close button (X) in the top right corner. It contains a text input field with the placeholder text "Specify the 'Read-Only' SNMP community:". Below the input field are three buttons: "Use Default", "OK", and "Cancel".

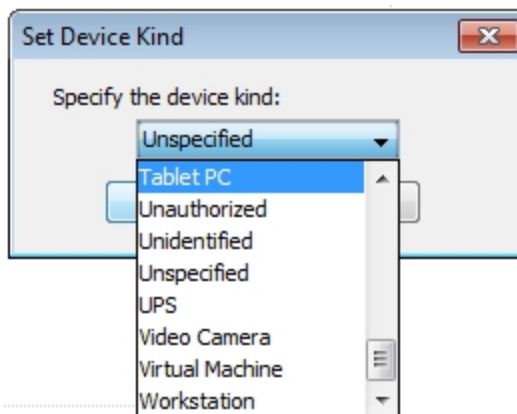
Set Data Retention...

Selects the Data Retention Policy to use when storing data to the InterMapper Database. Data Retention Policies are defined using the InterMapper Database Settings page of the DataCenter Administration Panel.

A dialog box titled "Set Retention Policy" with a close button (X) in the top right corner. It contains a dropdown menu with the placeholder text "Specify the data retention policy:". Below the dropdown menu is a button labeled "OK" and a button labeled "Cancel".

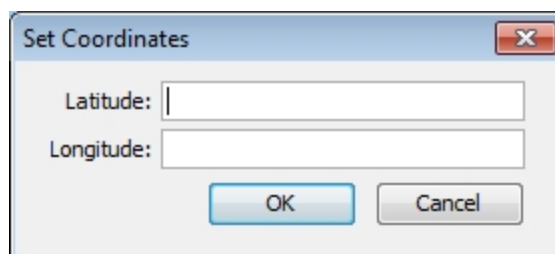
Set Kind

For each device whose data is stored in the InterMapper Database, you can set a device kind. This can be useful during data reporting or analysis. Use the Set Device Kind dialog to choose the device kind you want to store with the device data.



Set Latitude & Longitude

Enter valid latitude and longitude values in the text boxes and click **OK**. The device is moved to the appropriate location in the map, based on existing benchmarks.

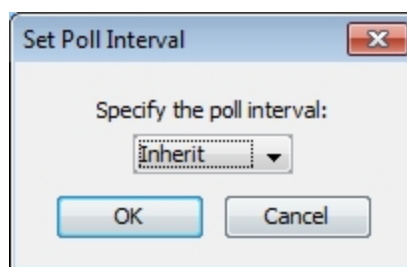


Set Poll Interval

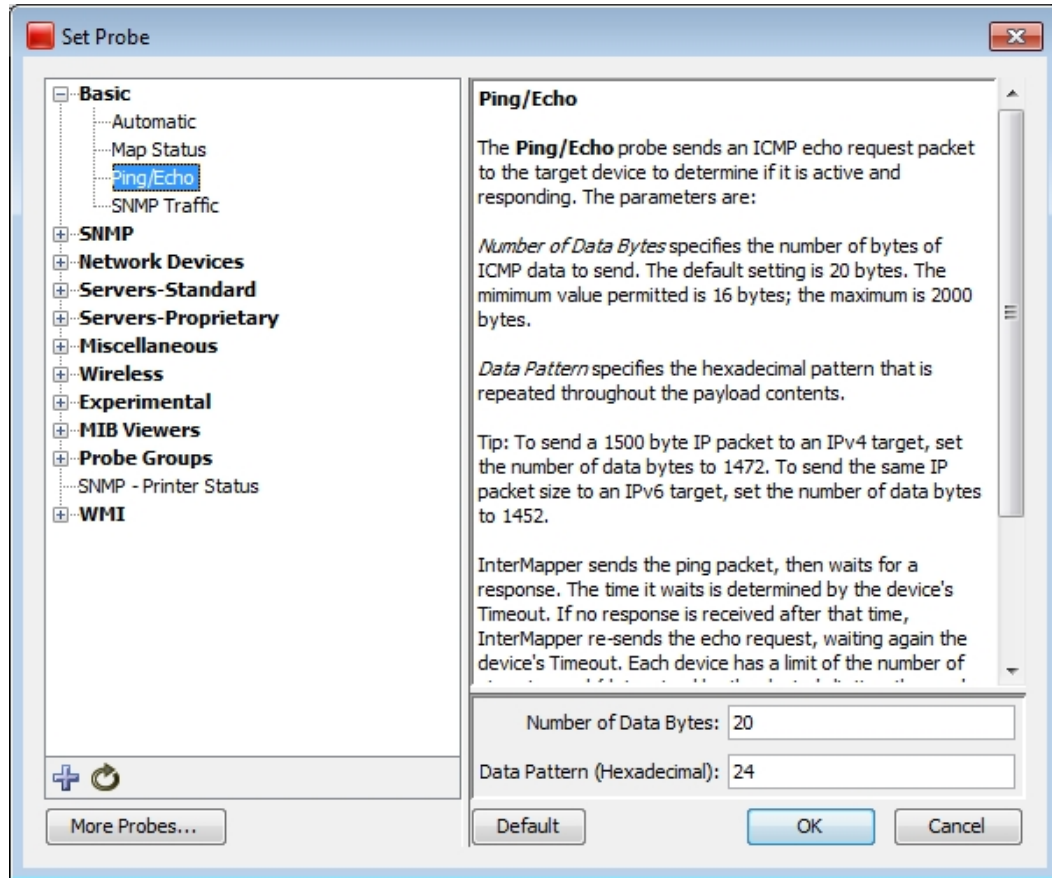
Choose from this dropdown menu to set the poll interval for selected devices. This interval is independent of and takes priority over the map's poll interval.

If the device's poll interval is set to "Default", the map's poll interval is used.

If a map is set to "No polling" the device poll intervals are ignored, and no devices are polled for that map.



Set Probe...



Opens the Probe Picker window.

Sets the probe used to query the selected device and the probe's parameters, if applicable. See [Probe Reference \(Pg 439\)](#) for details on the available InterMapper probes. See Custom Probes for information on creating your own InterMapper probes.

- Click plus (+) in the left pane to expand a probe group.
- Click minus (-) in the left pane to collapse a probe group.
- Click a probe in the left pane to choose the probe. Information about the probe and controls for setting any available parameters appear in the right frame.
- Click **Default** to set the probe back to default setting for that probe type.

Set Thresholds

Device Thresholds for Web Server

Set thresholds to alert you to network problems.

☐ Ignore outages

☒ Use Map defaults

Down Thresholds

Specify the timeout in seconds (1-9600): 3

Number of lost packets (1 - 10): 3

Other Thresholds

	Warning	Alarm	Critical	
Short-term packet loss:	2	5	20	of last 100
Response Time:	1000	5000	20000	msec

OK Cancel

Device Threshold window.

Set the criteria for sending a notification that a device is *down*, in an *alarm* state, or in a *warning* state. These settings apply to all the devices on the map.

- **Down:** This is the most serious condition. It means the device is no longer responding to probes. Specify the number of packets that may be lost before declaring the device down.
- **Critical:** This is the most serious condition in which responses are still being received. Specify the number of interface errors (per minute) allowed before marking the device as critical.
- **Alarm:** This is next most serious condition. Specify the number of interface errors (per minute) allowed before marking the device in alarm.
- **Warning:** The least serious error state. Specify the number of interface errors (per minute) allowed before showing the device in warning.

Set Vantage Point

Set the selected device as the Vantage Point from which InterMapper views all other devices on the map. If a device (such as a router or switch) between the Vantage Point and other devices fails, notifications are sent only for the failed device. The other devices are in the "shadow" of the failed device, and appear dimmed on the map.

The Vantage Point specifies InterMapper's virtual point of presence - as if the InterMapper server were directly connected to that item. When the Vantage Point is set on a device, a star appears next to the icon, as shown.



A Vantage Point icon.

The Vantage Point is used in conjunction with InterMapper's Notification Dependencies, which suppress notifications for devices that are assumed to be down because some other failure hides or shadows them. For full details, see [Notification Dependencies \(Pg 136\)](#).

Reset Short-term Packet Loss

InterMapper counts the number of dropped packets out of the last 100. This applies to all packets sent to the device (networks and links are not involved).

The Short-term packet loss is displayed in the device's Status Window as a percentage of the number of dropped packets in the last 100. Use this command to reset the current value to zero.

Helper Apps

Select a device, then choose from this submenu to launch a helper application, or choose customize to configure your helper applications.

Set Double-click

Select one or more map items, then choose from this submenu to specify what action is taken when any of the items is double-clicked. Use double-click actions to launch an Helper Application, URL, or Menu item.

For more information on Double-Click actions, see [Using Double-Click Actions \(Pg 83\)](#).

Insert Menu

Use the Insert menu to insert devices, networks, links, and blocks of text to your map, and to initiate the Auto-discovery and network-scanning processes.

The Insert menu is available only in the Map window, and is active only when the Map Editor is on.

Menu Command	Description
<u>Device...</u> (Pg 404)	Add one or more devices to a map.
<u>Network...</u> (Pg 405)	Add a network (oval) to the map.
<u>Link</u> (Pg 406)	Connect two devices with a link.
<u>Auto-Discover...</u> (Pg 406)	Scan a network to find network devices such as routers, hosts, switches, hubs, servers, workstations, and place them on the map. Specify a starting address and the kinds of devices InterMapper finds and limit the breadth of the search.
<u>Scan Networks...</u> (Pg 407)	Scan a network to find network devices such as routers, hosts, switches, hubs, servers, workstations, and place them on the map. Limit the types of devices InterMapper looks for. This command is available only when a network is selected, but the Filter dialog is also available from the Automatic Device Discovery dialog.
<u>Empty Probe Group...</u> (Pg 409)	Insert one or more empty probe groups in the map.
<u>Text...</u> (Pg 409)	Adds an object to the map containing the specified text.
<u>Icon...</u> (Pg 409)	Insert an icon into a map.
<u>Map Benchmark</u> (Pg 410)	Insert a benchmark to define the latitude and longitude of a point on the map.
<u>Group</u> (Pg 410)	Group two or more selected devices into a probe group. Devices must have the same IP address.
<u>Un-Group</u> (Pg 410)	Remove all probes from the selected probe group, and create a single device for each probe.

Device...

Add a new device to a map. *InterMapper* links the newly-added device(s) to networks already in the map. This example shows the **Add Devices** window.

To add a device:

1. Enter the one or more device names or addresses into the window.

Enter the names manually or paste from some other source. The names must be separated with commas or whitespace

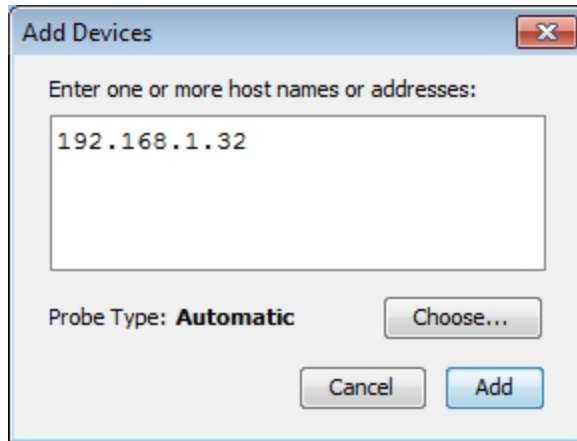
(spaces, tabs, or returns). The list of host names or IP addresses can be copied from a text file, from a traceroute program, or from other source of names and/or addresses. To resolve a domain name to an IPv6 address, enclose it in [square brackets] as shown in the example.

2. Select a probe type.

Automatic uses SNMP or ICMP Echo for IP devices.

You can also choose from a list of probes for web servers, mail servers, or any of the other probes shown in the dropdown menu. See [Probe Reference \(Pg 438\)](#) for a complete list of the built-in probes.

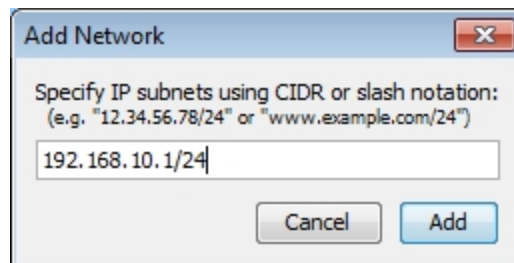
3. Enter a port number (if applicable to the probe).
4. Enter an SNMP Community string (if applicable).
5. Click **OK**.



Add Device(s) window.

Network...

Add a network (oval) to the map. This is useful when *InterMapper* does not automatically detect the network because no SNMP-speaking



Add Network... window. Enter an IP address range.

devices are present.

The window shown appears. Enter the IPaddress. (For a discussion of how IP network information is represented, along with a discussion of the "/24" etc notation, see [Subnet Mask FAQ. \(Pg 727\)](#))

After you click **OK**, you will see a new network oval on the map representing that subnet. You can connect devices to this network by dragging their links as described in [Adding and Removing Links \(Pg 69\)](#).

Link

Use the Link command to add a link manually where none exists. This can be useful when a link is not added during the auto-discovery process, or when you want to use links to specify that certain devices are dependent upon other devices. For more information on dependencies, see [Using Notification Dependencies \(Pg 136\)](#).

To add a link manually:

1. Select two devices or networks. (The menu command is available only when two items are selected.) You can use Shift-click, Control-click, or you can click and drag to draw a box around the items you want to select.
2. From the Insert menu, choose **Link**. A link appears between the selected items. The link is permanently attached, and remains connected when you move the items.

To remove a manually-added link:

- Right-click the link and choose **Remove**. The link is removed.

Auto-Discover...

Use the Auto-Discover command to open the Automatic Device Discovery window. Using this command you can automatically find network devices such as routers, hosts, switches, hubs, servers, workstations, and place them on the map. Specify the kinds of devices InterMapper finds and the breadth of its search.



The Automatic Device Discovery window.

InterMapper uses a *starting address* and then scans for additional devices. By default, InterMapper starts with its router's address or its own [IP address \(Pg 726\)](#). You may, however, enter a different address or [DNS name \(Pg 730\)](#) or [WINS name \(Pg 735\)](#) (preceded by "\\") as a starting point. If InterMapper finds SNMP-speaking routers with connections on other networks, it searches those networks, hop-by-hop, finding more devices (and possibly more routers) until the specified hop limit is reached.

The **Autodiscovery** window shown above allows you to specify the starting address as well as specifying other options for the autodiscovery process.

Enter a starting host name, IP address, or IP subnet - Enter the name or address of a device that InterMapper should use to begin the autodiscovery process.

Specify a SNMP Community - Enter an *additional* SNMP Read-only community string to be used to interrogate all devices. (InterMapper always attempts to read SNMP information using the default 'public' community string. For more information, see [SNMP Frequently-asked Questions \(Pg 731\)](#).)

Stay within ___ hops of starting device - Stops autodiscovery after InterMapper has searched the specified number of hops from the starting device.

Scan for devices on all networks - See [Scan Network... \(Pg 407\)](#) below.

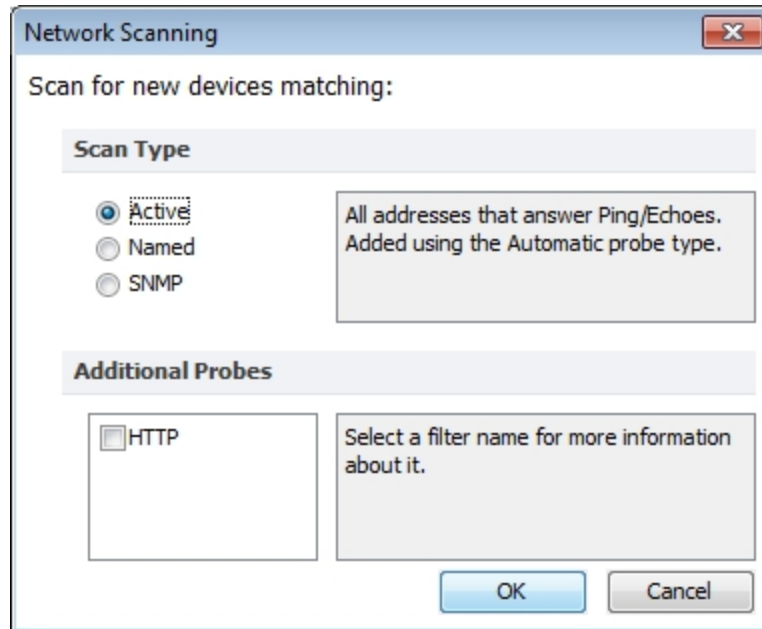
Edit Filters... - Click this button to open the Network Scanning window. See [Scan Network... \(Pg 407\)](#) below.

Automatically Layout - Select this box to have the map laid out automatically (using the Organic layout.)

Scan Networks...

The auto-discovery process also allows you to select which kinds of devices are to be added to the map. InterMapper applies a set of *filters* to the discovered devices. Only those that match the checked filters will be added to the map.

Click the **Edit Filter...** button, shown in the Automatic Device Discovery window above, or choose **Scan Networks...** from the Insert menu to open the **Network Scanning** window



The Network Scanning dialog. Check a box to seek the associated device.

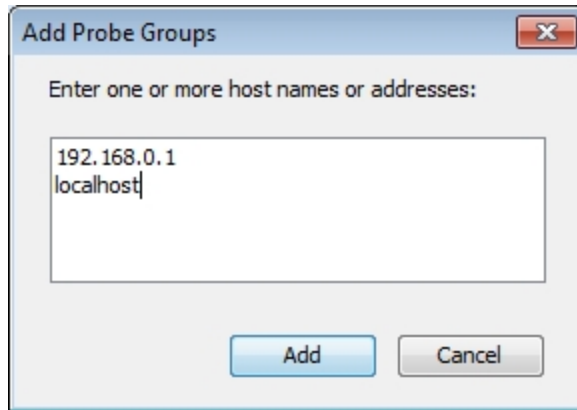
Choose from these options:

- **Active** forces a complete IP address scan for each network. InterMapper sends an ICMP Ping request to each IP address in the subnet range.
- **Named** Each IP address in the subnet is looked up in the DNS. If a corresponding name is present, the device is added to the map
- **SNMP** InterMapper sends a SNMP GetRequest to each address in the range. Devices that respond are added to the map.
- **Additional Probes** With the **HTTP** box selected, an HTTP probe is added if an HTTP response is received, and the device becomes a probe group.

Note: It is possible to choose options that result in InterMapper's attempting to discover everything on a network. On a small or medium-sized network, this might be a reasonable approach. On large networks, InterMapper may discover far too many devices to make a workable map.

Empty Probe Group...

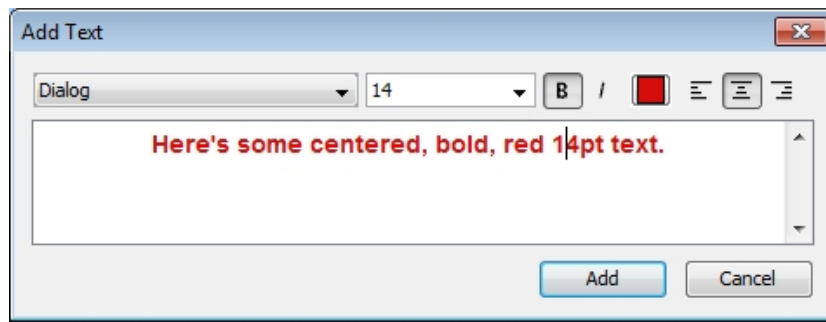
Enter one or more addresses or domain names in the Add Probe Groups text box and click **Add**. An empty probe group is added for each name or address.



Text...

Use the **Text...** command to place a block of text on a map at the location you choose.

To add a text object to a map:



Add Text window. Enter text in the text box.

Use the text formatting controls to format the text.

1. From the Insert menu, choose **Text...**. The Add Text window appears.
2. Enter the text you want to add to your map.
3. Use the formatting controls to format the text.
4. Click **OK**. A text object appears on the map.
5. Drag the text object to move it to the desired location.

Icon...

Use the **Icon** command to add an icon to a map. An icon inserted using this method is not associated with any device or network; it is simply a graphic element added to the map.

To add an icon to a map:

1. With the map editable, choose **Icon...** from the Insert menu. The Select an Icon window appears.
2. Choose an icon, and click **OK**. The icon appears in the map.

Map Benchmark

Use the **Map Benchmark** command to define the latitude and longitude of a point on a map. This is useful if you are placing devices on the map using geographic coordinates. Each device is located on the map in relation to the map's benchmarks.

Group

Use the Group command to create a probe group, a single device containing multiple probes. In order for the command to work, all selected devices must use the same IP address.

To create a probe group:

1. Select the devices you want to group. All selected devices must have the same IP address.
2. From the Insert menu, choose **Group**. The selected devices are "collapsed" into a single device, containing a probe for each selected device.

Note: A probe group counts as one device against your device count.

Un-Group

Use the Un-Group command to "explode" a probe group into individual devices.

To un-group a probe group:

1. Select the group you want to un-group.
2. From the Insert menu, choose **Un-Group**. The probe group is replaced by individual devices, each configured with one of the probes from the original group.

Note: Each device counts as one device against your device count.

Format Menu

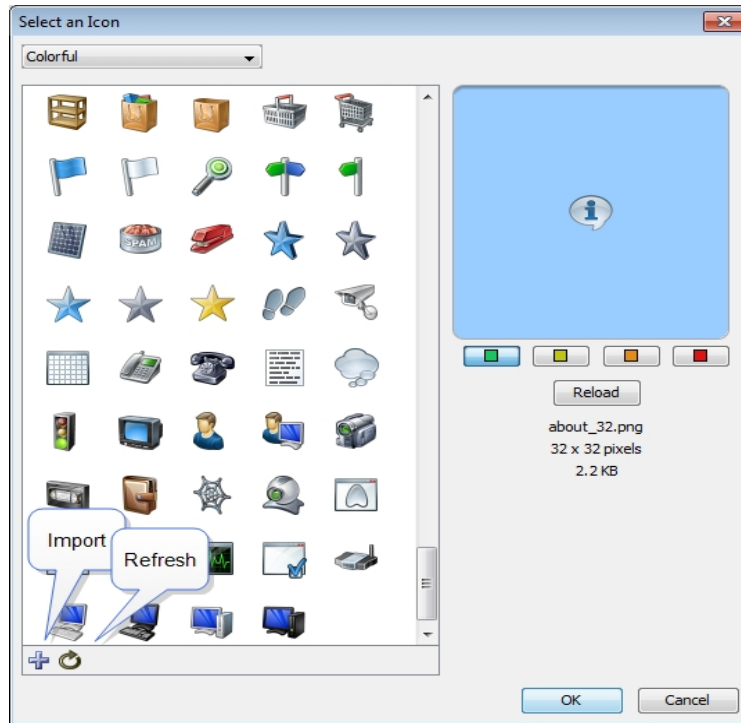
The **Format** menu contains commands that affect the appearance of individual items in the map. Items can be either devices (routers, servers, hosts, etc.) or networks (drawn as ovals, by default.)

Menu Command	Description
<u>Icon...</u> (Pg 412)	Choose an icon for the selected items.
<u>Label...</u> (Pg 414)	Modifies the label of one or more items from the map. Devices and networks have text labels that identify the item. These labels may be generated automatically from information gathered from the device, or contain static text that you enter.
<u>Label Position (submenu)</u> (Pg 418)	Change the position of the label relative to an item.
<u>Align...</u> (Pg 419)	Align the selected objects to each other.
<u>Rotate...</u> (Pg 419)	Rotate the positions of the selected objects in relation to each other.
<u>Scale...</u> (Pg 420)	Scale the positions of the selected items in relation to each other.
<u>Arrange (submenu)</u> (Pg 420)	Rearrange the selected items into a cycle, bus, or star.
<u>Context menu</u> (Pg 423)	Set the Font, Size, and Style of the selected devices from the context menu

Icon

Use the **Icon** command to select an icon for a device or network as it appears on your map. The Select an Icon window appears.

- Click an icon from those displayed in the left box. It appears in pre-view box on the right.
- Click **OK** to assign the icon to the selected devices or networks.
- From the drop-down menu at the top of the window, choose a group of icons. The Built-in Shapes are shown below.
- Click **Import...** to import an image as an icon.
- When viewing groups of icons other than Built-in Shapes, click Reload to refresh the icon list in the left box.
- Drag an image to the window to import it as an icon.
- Drag a folder of images to the window to import the contents as a new icon group.

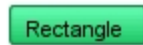


For more information, see [Custom Icons \(Pg 101\)](#).

Built-in Shapes

Use the icons in the **Built-in Shapes** icon group.

Note: Except for the **Wire** icon, all Built-in Shapes stretch to enclose the specified label text.



Rectangle and Oval

Rectangles and Ovals contain the text label within them.

Rectangle is the default shape for a device.
Oval is the default shape for a network.



Wire

The Wire item is drawn as a straight line. Connections to the wire are drawn at right angles to the wire if possible.

- Drag the ends of the wire to resize it or change its orientation (angle).
- Choose from the **Label Position** sub-menu to position the label at one of nine positions.



Cloud

Cloud items contain the text label within them.



Text

The font, style, and color are controlled by the other choices in the Format menu. The border of the item appears only when the item is selected.



Icon

Choose from a set of default icons or create your own. See [Custom Icons \(Pg 101\)](#) to learn more about adding icons to *InterMapper's* set.

Label

Each item in your map has a label. Use the **Label...** command from the Format menu to edit labels for the selected items.

Default Labels

- **Device** - its Smart Name.
- **Network**- IP address or range.

The Edit Device Label window

The example below shows the window for editing an item's label.

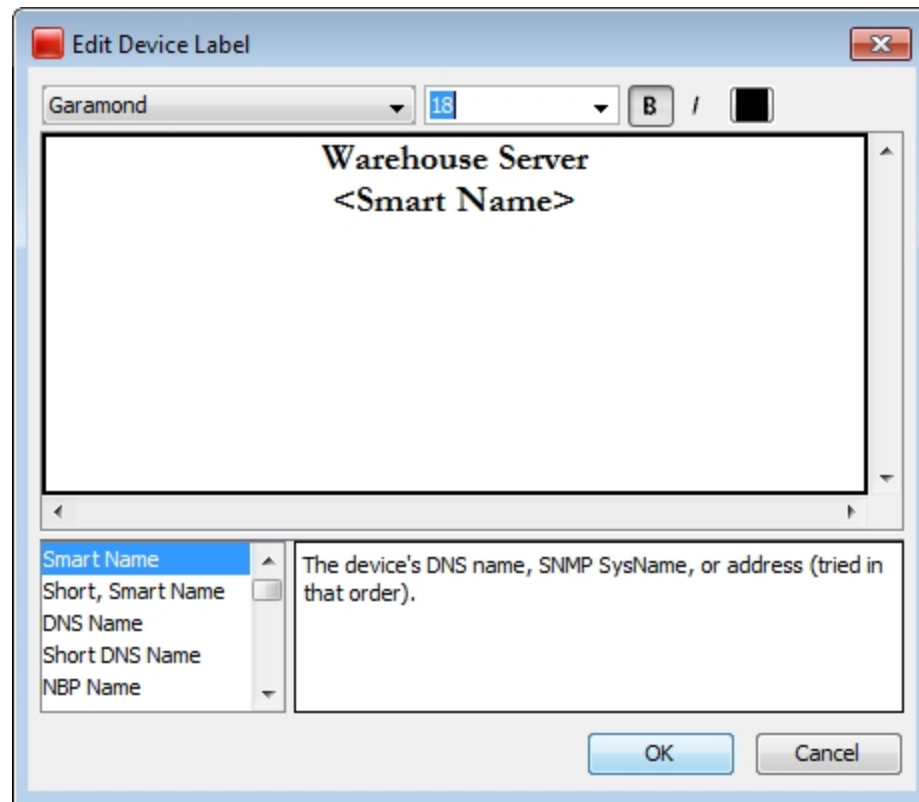
- **Top pane** - lists the label as it will be displayed.
The entries in <...> are *variables* which are filled in with the values from the particular device or network.
Press **Enter** to move text or variables to a new line.
- **Lower-left pane** - displays a list of variables that may be used in the top pane; the lower-right pane shows the definition of each variable

To insert a variable into the item's label:

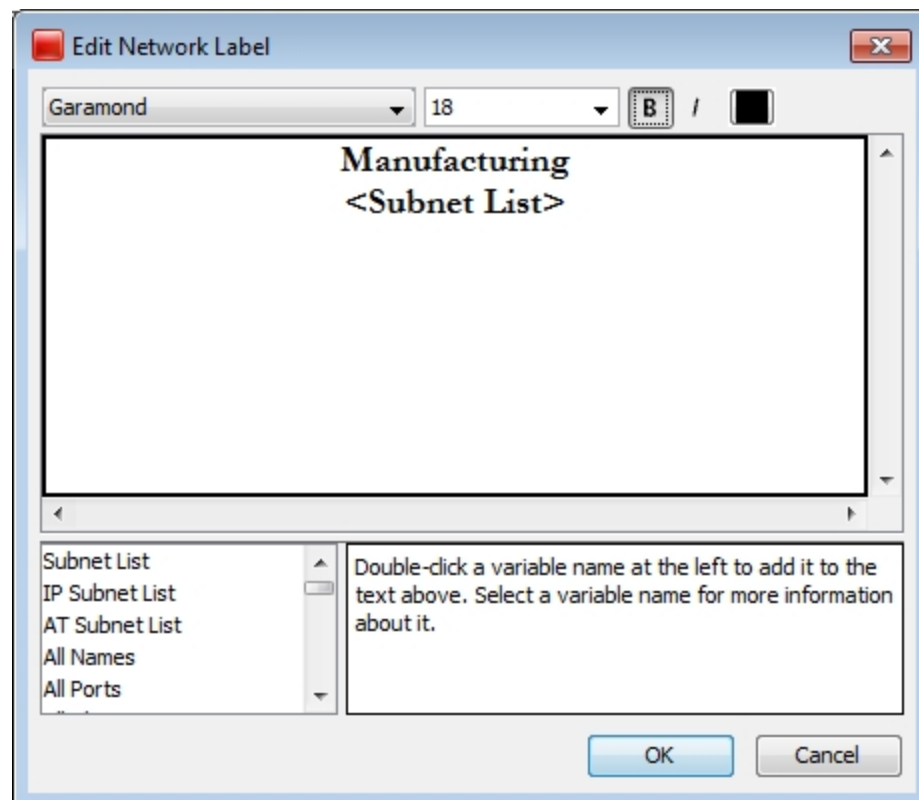
In the top pane, place your cursor where you want to place the variable.

In the Lower-left pane, double-click variable you want to insert. The variable appears in the top pane, enclosed in <...>.

Tip: To move text or a variable to a new line, place the cursor where you want the new line to start and press **Enter**.



Editing a Device label.



Editing a Network Label.

Label Variables

Use label variables to help you see the item information you consider most important.

Device Variables

Smart Name (default)	The device's DNS name, SNMP SysName, or IP address, tried in that order.
Short, Smart Name	The leftmost part (up to the first ".") of the device's Smart Name (except for IP addresses).
DNS Name	The full DNS name for the device (not the sysName or IP Address).
Short DNS Name	The first part of the device's DNS Name.
NBP Name	The device's Name Binding Protocol name.
SNMP SysName	The name of the device as reported by the 'sysName' variable.
SNMP SysDescr	The hardware and software information reported in the 'sysDescr' variable.
SNMP SysContact	The contact person as reported by the 'sysContact' variable.
SNMP SysLocation	The location of the device as reported by the 'sysLocation' variable.
SNMP EnterpriseID	The enterprise ID of the device as reported by the 'EnterpriseID' variable.
SNMP EntSerialNum	The serial number of the device as reported by the 'EntSerialNum' variable.
SNMP EntMfgName	The manufacturer name of the device as reported by the 'EntMfgName' variable.
SNMP EntModelName	The model name of the device as reported by the 'EntModelName' variable.
Address	The network address of the device.
MAC Address	The device's MAC Address. If the device has multiple interfaces, this field contains the MAC Address associated with the device's main IP Address (the same address as the address field).
Probe Type	The probe type used to test the device.
Comment	The comments associated with the device in its "Get Info" window.
TCP Port	The TCP port number that is being monitored, if the device is using a TCP-based probe type.

WINS/NetBIOS Name The device's WINS/NetBIOS name.

Network Variables

Subnet List (default)	A list of the subnets on the network.
IP Subnet List	A list of IP subnets on the network.
AT Subnet List	A list of AppleTalk subnets on the network.
All Names	List of interface names (for devices that have them), one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
All Ports	List of the device's ifIndex attached to the network, one per line.
All Aliases	List of interface aliases (for devices that have them), one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
All Descriptions	List of port descriptions attached to the network, one per line.
All Device-Names	List of 'device-label: interface-name' attached to the network, one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
All Device-Ports	List of 'device-label: ifIndex' attached to the network, one per line.
All Device-Aliases	List of 'device-label: interface-alias' attached to the network, one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
All Device-Descriptions	List of 'device-label: port-description' attached to the network, one per line.
Switch Names	List of only switch's interface names (for devices that have them), one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
Switch Ports	List of only switch's ifIndex attached to the network, one per line.
Switch Aliases	List of only switch's interface alias (for devices that have them), one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
Switch Descriptions	List of only switch's port descriptions attached to the network, one per line.

Switch Device-Names	List of only switch's 'device-label: interface-name' attached to the network, one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
Switch Device-Ports	List of only switch's 'device-label: ifIndex' attached to the network, one per line.
Switch Device-Aliases	List of only switch's 'device-label: interface-alias' attached to the network, one per line. Devices that do not use SNMPv2c or SNMPv3 will not be shown.
Switch Device-Descriptions	List of only switch's 'device-label: port-description' attached to the network, one per line.
Port Address	List of all numbered interfaces, one per line.
IP 3rd Octet	List of IP subnets on the network, one per line. Subnets are identified by their 3rd octet only.
VLAN	List of VLAN IDs on the network, one per line.
Port List	List of 'device-label: ifIndex' attached to the network, one per line.
Interface Name	List of the interface names (for devices that have them), one per line. Devices that do not use SNMPv2c or SNMPv3 are not shown.
Port Number	List of device's ifIndex attached to the network, one per line.
Interface Alias	List of interface alias (for devices that have them), one per line. Devices that do not use SNMPv2c or SNMPv3 are not shown.
Port Name	List of port descriptions attached to the network, one per line.

Label Position

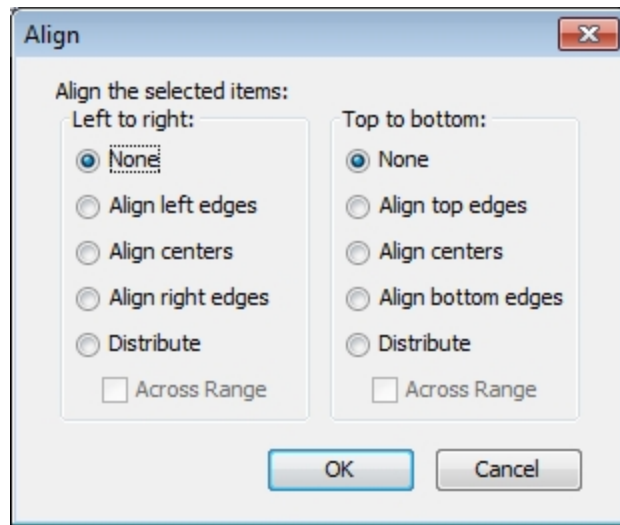
Choose from these nine positions:

- Top Left, Top, Top Right
- Left, Center, Right
- Bottom Left, Bottom, and Bottom Right

Note: The label position affects only *Wire* and *Icon* shapes.

Align

Align the selected items relative to each other. The **Align ...** buttons work like other drawing programs.



Changing alignment of selected items in a map.

1. Select the items you want to align.
2. From the Format menu, choose **Align...** The Set Alignment dialog appears.
3. Choose horizontal (left to right) and vertical (top to bottom) alignment options and click **OK**. The selected items are aligned as specified.

Distribute:

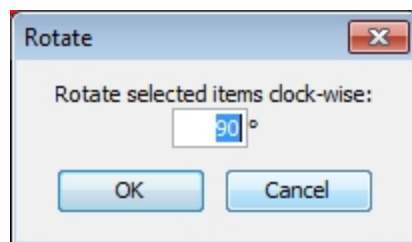
The Distribute option spaces the devices evenly.

Check the **Across range** box to distribute the items evenly in the space that the items occupy.

Clear the **Across range** box to draw the items with a small amount of space between the icons.

The example at left shows the options for aligning items.

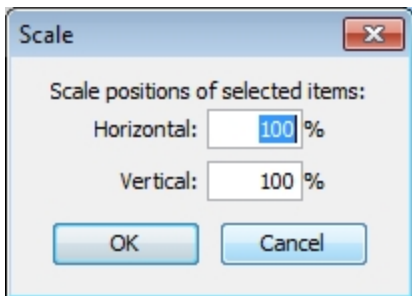
Rotate



Rotate the selected items (but not their icons or text labels) by the specified number of degrees.

Rotate the positions (but not the text or icons) of the selected items as a group. Items are rotated clockwise by the number of degrees specified. The example at left shows the window for rotating items.

Scale



Change the relative spacing of the selected items. This is useful after arranging items in a star to increase or decrease the diameter of the circle. The example at left shows the interface.

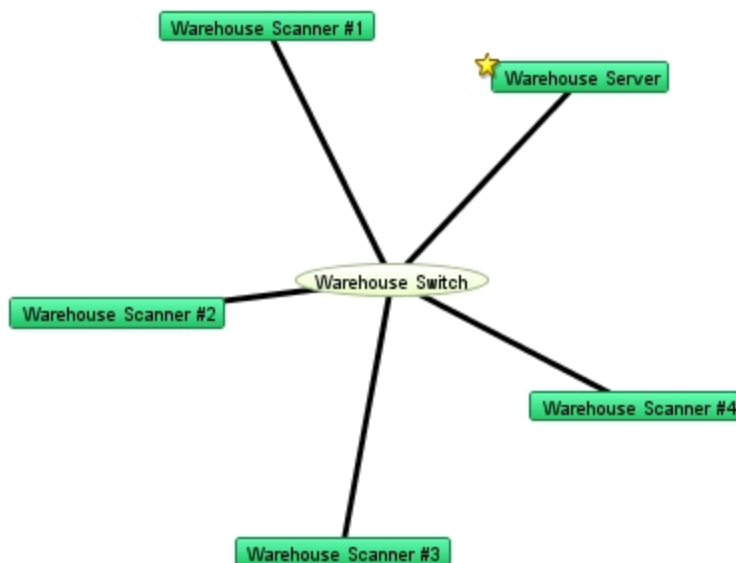
Scaling item positions. Specify the amount (percentage) to change the positions both vertically and horizontally.

Arrange (submenu)

If no objects are selected, Organic and Tree commands work on all objects on a map. For Star and Bus, you must select at least one object. For Cycle, you must select at least two object. All commands will work on two or more objects.

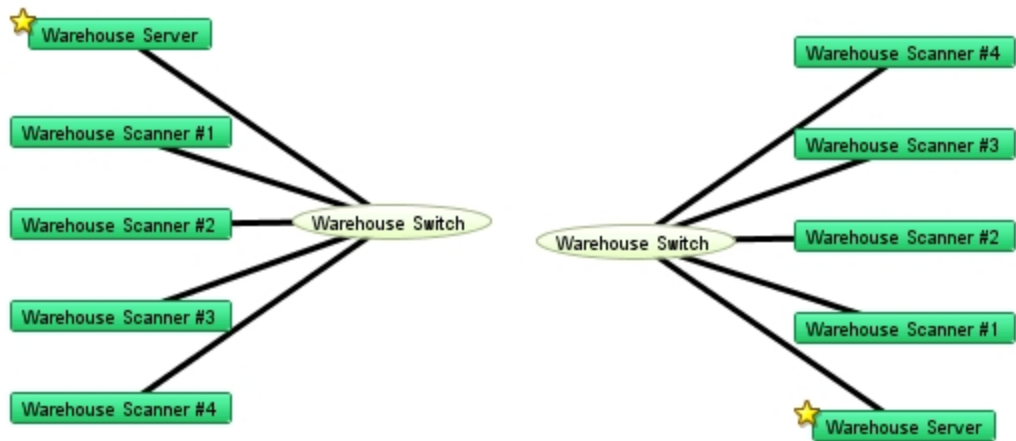
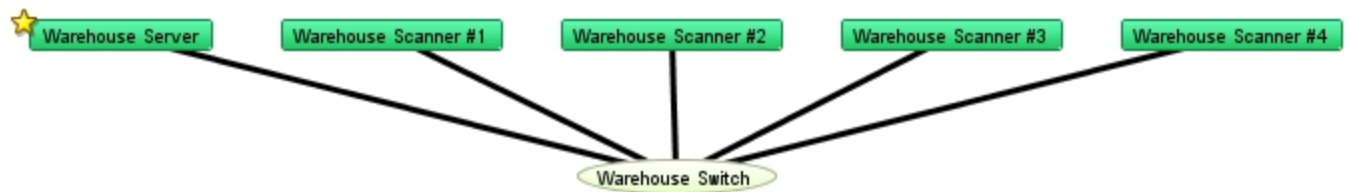
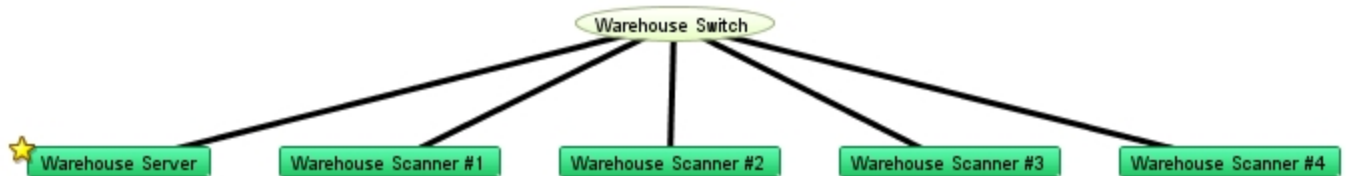
Organic

Arrange items with a minimum number of crossed links and overlaid objects.



Tree

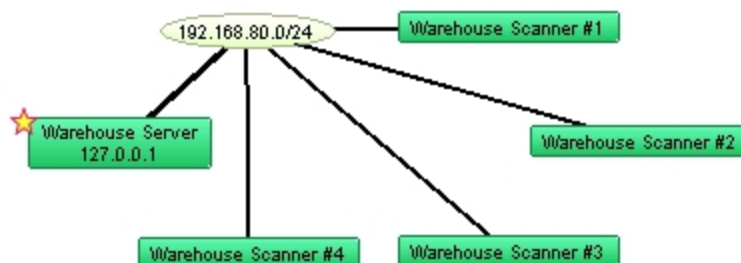
Arrange items in a tree structure. Choose which direction the branches of the tree should go.

**Tree - left****Tree - right****Tree - up****Tree - down**

Cycle

Move the selected items into an oval around the edge of the window. This allows you to see the interconnections between the devices of your network more easily. The Cycle example in

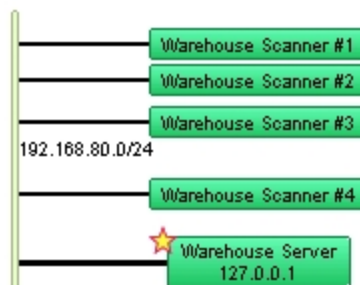
[Using the Arrange Commands](#) (Pg 118) illustrates the Cycle command's action.



Bus

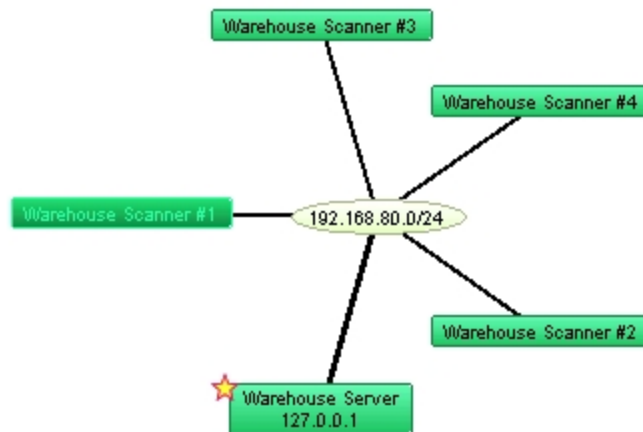
Arrange items into a vertical column, changing the item that connects them into a vertical *bus* shape. This might represent a group of devices connected by an Ethernet or other broadcast medium. The Bus example in [Using the Arrange Commands](#) (Pg 116) illustrates the Bus command's action.

Note: The **Bus** command affects only items that are connected to networks.



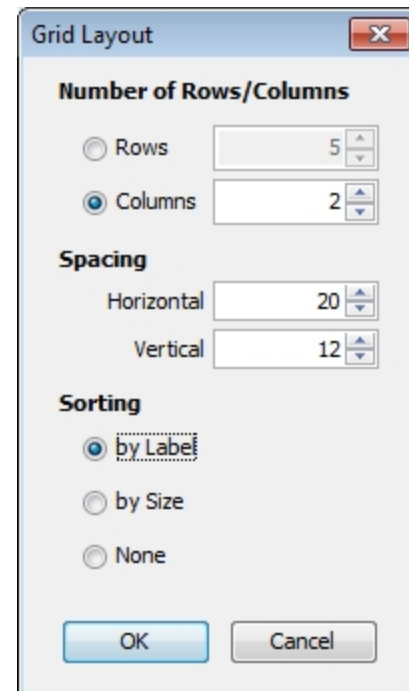
Star

Arrange items so they surround a network or device that connects them. The devices are spaced equally around the circumference of a circle. The Star example in [Using the Arrange Commands \(Pg 116\)](#) illustrates the Star command's action.



Grid

Arrange items to form a grid, with the specified number of columns or rows. Sort by Label, Size, or None. If sorting by None, the grid is created relative to the upper-left icon in the selection.



Features available only from the Context Menu

Font, Size, and Style

You can change the attributes for each label in your map.

- Choose from Font, Size or Style from the context menu to change the label's font, font size, and font style.

Note: The Font, Size, and Style attributes affect all labels in the selected objects. The Color attribute affects the text color only when the shape is set to Text. These functions are also available from the Edit Device Label... dialog.

Window Menu

The Window menu lists all open maps at the bottom of the menu. You can also change certain aspects of window appearance, and can access other InterMapper windows.

Menu Command	Description
Minimize (Pg 426)	Minimize the frontmost window.
Zoom (Pg 426)	Choose the Zoom command to expand (or contract) the frontmost window to the size necessary to show all devices, or to the maximum size of its current screen, if all items cannot be shown at the same time. If the Toolbar is shown, the minimum window width is the width of the toolbar.
Send to Back (Pg 426)	Send the front-most window to the back.
Slideshow... (Pg 426)	Rotate between open map windows.
Logs (Pg 427)	Choose from a submenu of log files to view a history of events, outages, the Debug log, or custom logs you set up yourself.
Charts (submenu) (Pg 428)	Choose from a submenu of defined charts. Note: In the Charts window, a Show Chart context menu item has the same effect.
Map List (Pg 428)	Open the Map List window, or bring it to the front.
Device List (Pg 429)	Open the Device List window.

Minimize

Minimizes the frontmost InterMapper window.

Zoom

Choose the **Zoom** command to expand the frontmost window to the largest size necessary to show all devices, or to the maximum size of its current screen, if all items cannot be shown at the same time.

- Choose **Zoom** again to return the window to its original size.

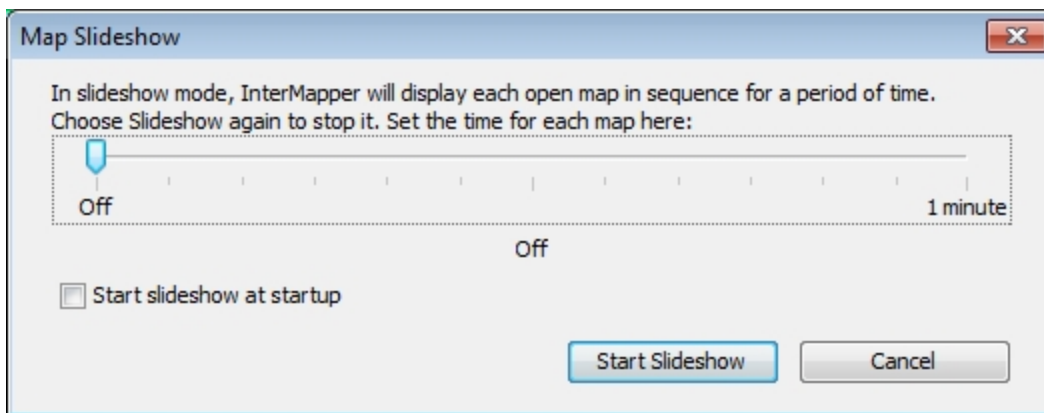
Send to Back

Use the **Send to Back** command to send the front-most window to the back.

Floating windows associated with that window, such as Status windows, are hidden.

Slideshow...

Use the **Slideshow...** command to rotate the open map windows at a specified rate.

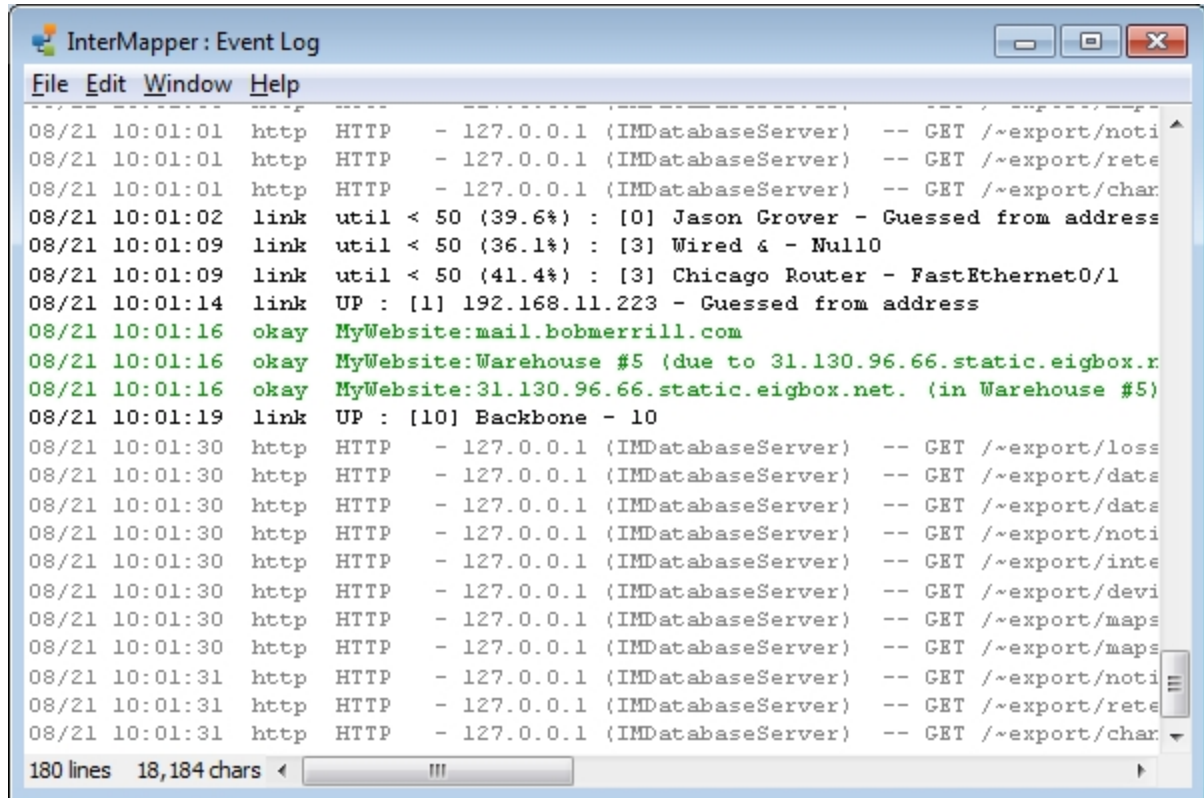


- From the Window menu, choose **Slideshow...**, and choose the amount of time each map should be shown.
- Choose **Slideshow** again to stop the slide show.

Logs

Use the **Logs** selection from the Window menu to choose from a submenu of log files. You can view a history of events, outages, connections to the web and remote servers, or custom logs you set up yourself.

Here is a typical Event Log window.



Event Log window.

Each time a device changes state, an entry is made in an event log window. In addition, *InterMapper* logs messages for the following events:

- Acknowledgements (including the text entered by the operator)
- Maps opening and closing
- Program startup
- DNS errors
- Errors when sending a notification
- Receipt of an SNMP trap

For more information, see the Overview of [Information and Log Windows \(Pg 234\)](#).

Charts

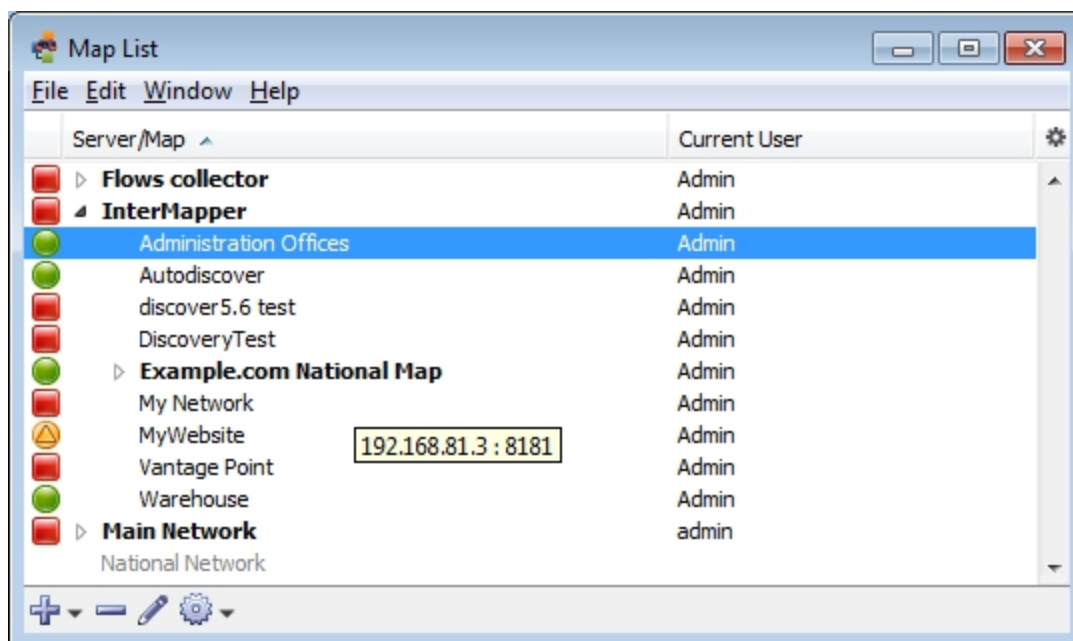


Choose from a submenu listing all available charts for the current map window

- Select and clear the check mark on individual charts from the submenu to show or hide them.
- Choose **Show Charts** to show all charts.
- Choose **Hide Charts** to hide all charts.

Map List

Use the Map List command to open the Map List window or bring it to the front.



Device List

Use the **Device List** command to view the Device List window, which shows a global device list. InterMapper keeps a server-wide list of all the devices that are being monitored on all enabled maps that the current logged-in user can see.

Name	Condition	Condition ...	Previous C...	Previous Ti...	Probe Type	Address	Poll Inter...	Map Name
wndr3400v2.	Down	8/21/12 9:0...		8/21/12 9:0...	Probe Group	192.168.0.47	Inherit	discover5.6 ...
Router 2	Down	8/21/12 9:0...		8/21/12 9:0...	Ping/Echo	192.168.81.101	Inherit	Vantage Point
dslrouter.	Down	8/21/12 9:0...		8/21/12 9:0...	Ping/Echo	192.168.0.1	Inherit	DiscoveryTest
dslrouter.	Down	8/21/12 9:0...		8/21/12 9:0...	Probe Group	192.168.0.1	Inherit	discover5.6 ...
192.168.81.101	Down	8/21/12 9:0...		8/21/12 9:0...	Probe Group	192.168.81.101	Inherit	My Network
192.168.81.101	Down	8/21/12 9:0...		8/21/12 9:0...	Ping/Echo	192.168.81.101	Inherit	DiscoveryTest
192.168.81.4	Down	8/21/12 9:0...		8/21/12 9:0...	Ping/Echo	192.168.81.4	Inherit	DiscoveryTest
192.168.81.2	Down	8/21/12 9:0...		8/21/12 9:0...	Probe Group	192.168.81.2	Inherit	My Network
Router 3	Short-term P...	8/21/12 10:...	Short-term P...	8/21/12 10:...	Ping/Echo	192.168.81.2	Inherit	Vantage Point
192.168.81.2	Short-term P...	8/21/12 10:...	Short-term P...	8/21/12 10:...	Ping/Echo	192.168.81.2	Inherit	My Network
192.168.81.2	Short-term P...	8/21/12 10:...	Short-term P...	8/21/12 10:...	Ping/Echo	192.168.81.2	Inherit	DiscoveryTest
192.168.81.2	Short-term P...	8/21/12 10:...	Short-term P...	8/21/12 10:...	Ping/Echo	192.168.81.2	Inherit	DiscoveryTest
Web Server	Short-term P...	8/21/12 10:...	Short-term P...	8/21/12 10:...	Ping/Echo	192.168.81.2	Inherit	My Network
WS 3	OK	8/21/12 9:0...			Ping/Echo	192.168.81.1	Inherit	Vantage Point
WS 3	OK	8/21/12 9:0...			Ping/Echo	192.168.81.1	Inherit	Vantage Point
WS 3	OK	8/21/12 9:0...			Ping/Echo	192.168.81.1	Inherit	Vantage Point
WS 2	OK	8/21/12 9:0...			Ping/Echo	192.168.81.1	Inherit	Vantage Point
WS 2	OK	8/21/12 9:0...			Ping/Echo	192.168.81.1	Inherit	Vantage Point
WS 2	OK	8/21/12 9:0...			Ping/Echo	192.168.81.1	Inherit	Vantage Point
WS 1	OK	8/21/12 9:0...			Ping/Echo	192.168.81.102	Inherit	Vantage Point

The Device list window.

For more information, see [The Device List Window](#).

Help Menu

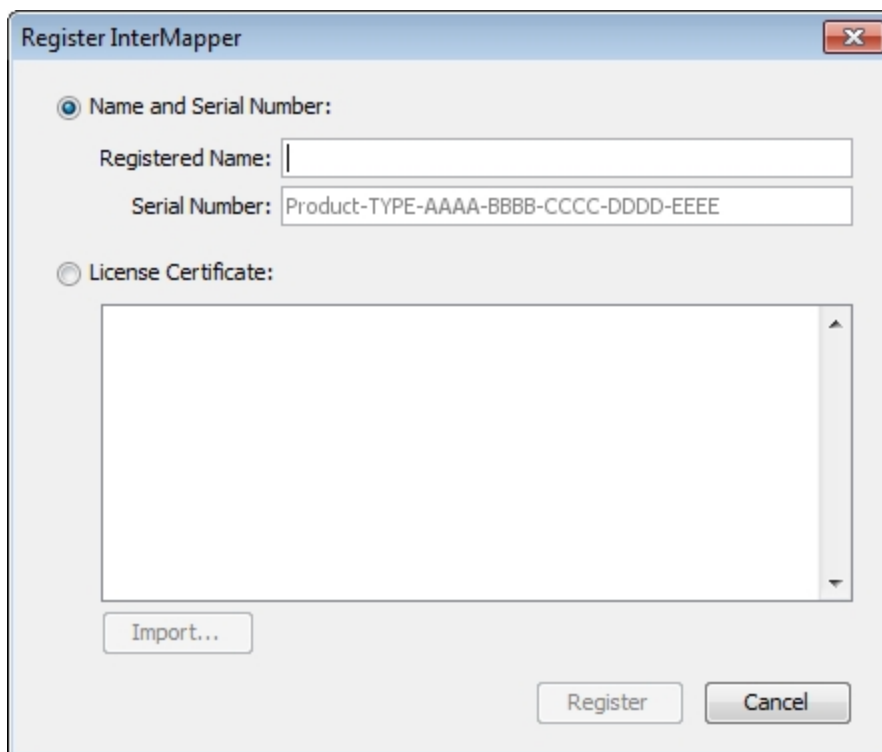
Use the Help menu to view the on-line help system.

Menu Command	Description
About InterMapper	Opens the InterMapper software information page. Note: On Macintosh, this command is available from the InterMapper or IM RemoteAccess menu .
Register InterMapper..., Register InterMapper RemoteAccess (Pg 431)	Opens the InterMapper or InterMapper RemoteAccess registration window.
InterMapper Help, InterMapper RemoteAccess Help	Opens the InterMapper help system.
Send Feedback... (Pg 216)	Opens the Send Feedback window.
Send a Screenshot... (Pg 216)	Opens the Send Feedback window with a screenshot attached.
Diagnostics (submenu) (Pg 431)	Choose from a number of diagnostic commands, described below.

About InterMapper

Opens the InterMapper software information page. View information about the software and its contributors, as well as viewing information about memory use, platform, operating system and current Java version.

Register InterMapper, Register InterMapper RemoteAccess



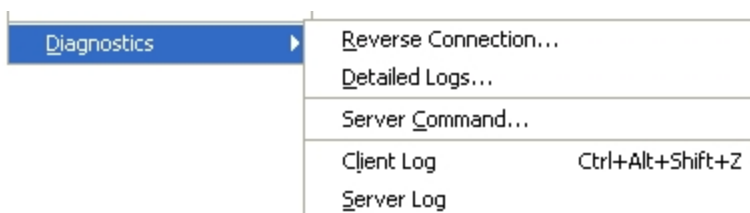
The dialog box titled "Register InterMapper" has a close button (X) in the top right corner. It contains two radio buttons: "Name and Serial Number:" (selected) and "License Certificate:". Under "Name and Serial Number:", there are two text fields: "Registered Name:" (empty) and "Serial Number:" (containing "Product-TYPE-AAAA-BBBB-CCCC-DDDD-EEEE"). Under "License Certificate:", there is a large empty text area with a vertical scrollbar. At the bottom, there are three buttons: "Import...", "Register", and "Cancel".

(InterMapper Only)

Opens the Register InterMapper (or InterMapper RemoteAccess) window. This is the same window displayed when you click Add... from the Registration pane, found in the Server Information section of the Server Settings window.

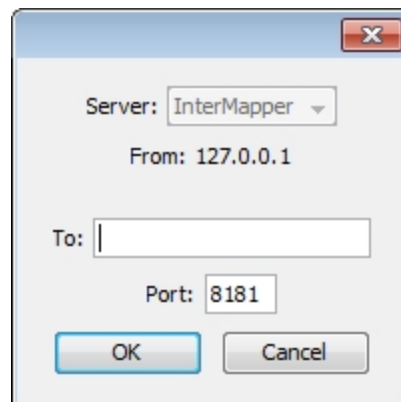
Diagnostics (submenu)

Use the diagnostics menu to create a Reverse Connection to a server for troubleshooting, to view Detailed Logs, to execute a server command, or to view the Client or Server log.



Reverse Connection...

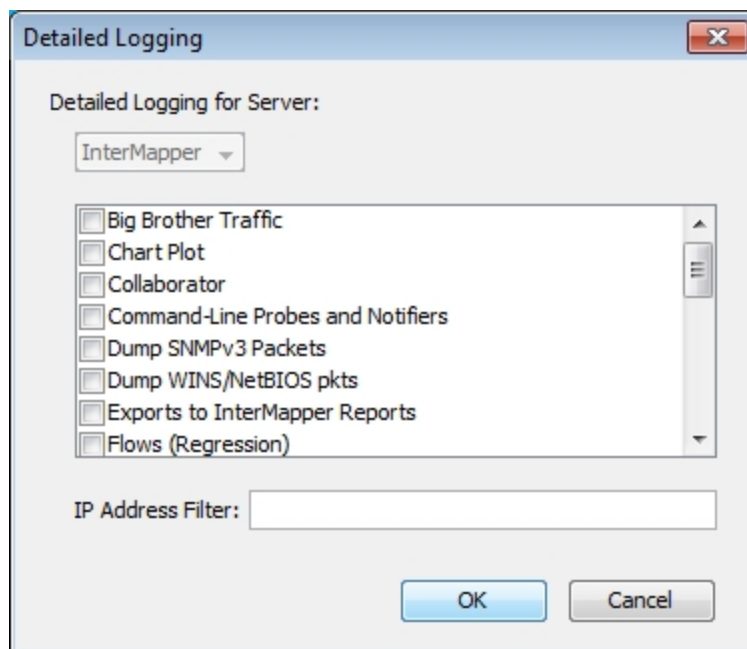
Use the Reverse Connection command to initiate a reverse connection from your InterMapper server to a copy of InterMapper RemoteAccess client for troubleshooting purposes. This is frequently used to allow tech support personnel to view a customer's server. Using a reverse connection, the customer can instruct their server to connect out to another InterMapper RemoteAccess without changing any firewall configurations.



Detailed Logs...

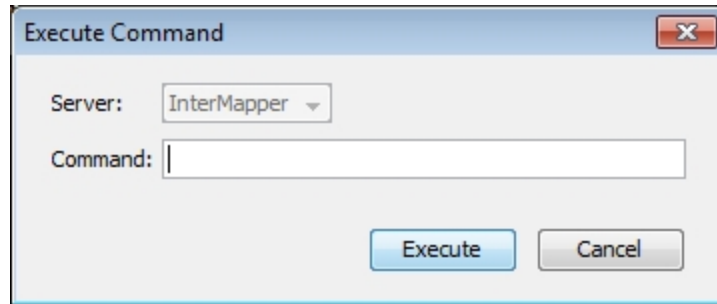
Use the Detailed Logs command to toggle detailed logging for a variety of different InterMapper events. Choose the type of event for which you want detailed logging to be displayed. The detailed information is sent to the server's Debug Log file. Enter an IP address in the Filter field to limit the the logged information to a particular IP address.

When detailed logging is on, a significant quantity of data can be logged in a relatively short period. To conserve server disk space, use this feature only when needed for troubleshooting.



Server Command...

InterMapper RemoteAccess can instruct a server to execute certain commands, and to display the output in the Debug Log file. The major command is **snmpwalk**; it and other commands are described in the [Developer Guide](#).

**Client Log**

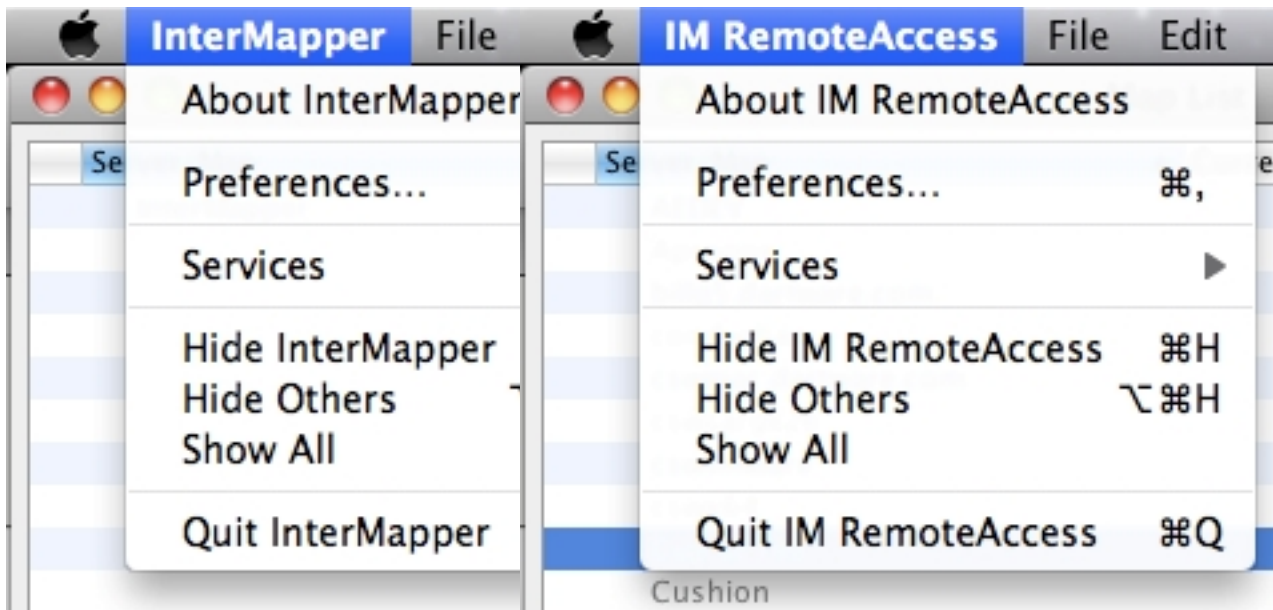
Use this command to open the Client Log window, which contains the messages sent between the client and the InterMapper server. This information can often be useful for debugging InterMapper problems.

Server Log

Use this command to open the Debug log file for the server. It can also be opened from the Window>Logs>Debug menu.

InterMapper Menus

Macintosh OSX adds an InterMapper menu or IM RemoteAccess menu. These menus contain menu items that normally appear in other menus on other platforms.



InterMapper menu

InterMapper RemoteAccess menu

The **About**, **Preferences...**, and **Quit** menu items appear in these menus on Macintosh systems.

For information on these features, see the menu reference topics as follows:

- About InterMapper, About IM RemoteAccess: [Help menu](#)
- Preferences: [Edit menu](#)
- Quit: [File menu](#)

Context Menus

Use a context menu to choose options available for a particular device, network, link, map, window or other screen object. The options available in a context menu change depending on the object you are using to activate the context menu.

To execute a command from a context menu:

1. **Right/Ctrl-click** the object for which you want to activate the context menu. The context menu appears.
2. Click to choose a command from the context menu. Commands appropriate to the selected object and current context appear.

Keyboard Shortcuts

InterMapper runs on multiple platforms. Since different platforms have different modifier keys, (keys that change the function or meaning of another key) the keyboard shortcuts vary slightly from one platform to another.

General Rules

The primary difference is between Macintosh and Windows machines. Use the following rules, depending on your platform:

To choose a menu item using the keyboard:

Macintosh: *Commandkey*

Windows, Unix, Linux: *Control key*

To choose an item from a context menu:

Macintosh: *Control-click* (hold **Control**, click with the mouse)

Windows, Unix, Linux: *Right-click*

Finding Menu Item Shortcuts

Each menu item that has a shortcut shows the key required for the shortcut in the menu.

Keyboard Navigation

You can use the keyboard to speed up a number of operations. See [Keyboard Navigation \(Pg 437\)](#) for a complete set of navigation keystrokes.

Other Shortcuts

A number of other shortcuts are available to help you work efficiently. See [Quick Reference - Editing Your Map \(Pg 95\)](#) for additional selection and scrolling techniques.

Keyboard Navigation



Scroll the view

(in Browse mode)



Micro-adjust the position of the selected item

(in Edit mode)



Scroll the view in Edit mode.

Alt or Option <arrow key> (in Edit mode)

Home

Scroll to Upper Left

End

Scroll to Lower Right

Page Up

Scroll one page up

Page Down

Scroll one page down

Tab

Toggle between Browse and Edit Mode

Cmd/Ctrl + Click

Center map

Cmd/Ctrl + Drag

Scroll map in any direction

Cmd/Ctrl + Scroll Wheel

Zoom in or out dynamically

Cmd/Ctrl + Option + Drag


Zoom in on selected rectangle

Cmd/Ctrl + Up


Zoom In

Cmd/Ctrl + Down

Zoom Out

Cmd/Ctrl + 


View Icons

Cmd/Ctrl + 

View List

Cmd/Ctrl + 

View Notifiers

Cmd/Ctrl + 

View Charts



(Numeric Keypad)

Zoom In



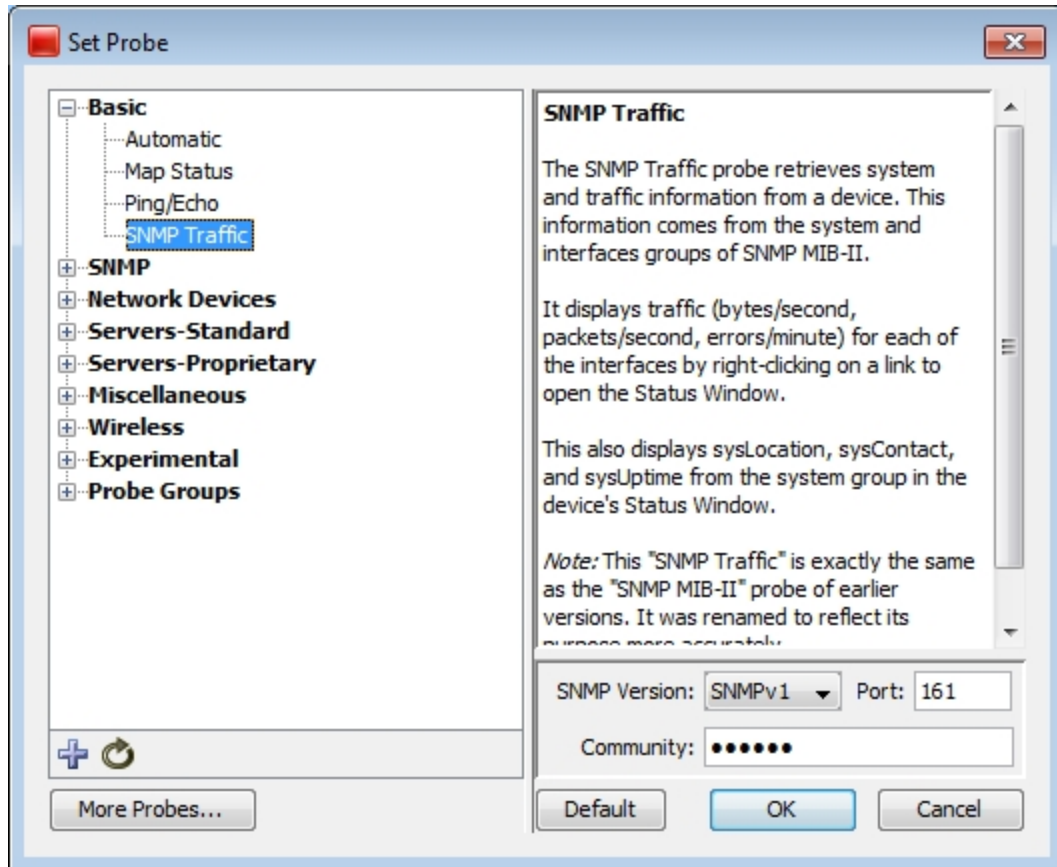
(Numeric Keypad)

Zoom Out

Chapter 13

Probe Reference

Use the Probe Picker window to choose the probe you want to use to query the device.



Set Probe Window

Using the Probe Selection Window

- Click plus (+) in the left pane to expand a probe group.
- Click minus (-) in the left pane to collapse a probe group.
- Click a probe in the left pane to choose the probe. Information about the probe and controls for setting any available parameters appear in the right frame.
- Click **Default** to set the probe back to default setting for that probe type.

About the Probes

InterMapper comes with a large number of built-in probes. For a full index and detailed descriptions of built-in probes, see the [Probe Index \(Pg 442\)](#).

- [Basic Probes \(Pg 448\)](#) - use the Basic probes to cover the majority of your needs for probing devices.
- [SNMP Probes \(Pg 451\)](#) - use the SNMP probes to perform a wide variety of queries on SNMP devices.
- [Network Devices \(Pg 466\)](#) - Use the network device probes to query network devices, such as routers, switches and UPS units.
- [PowerShell Probes \(Pg 479\)](#) - Use these probes to get information from Windows machines using PowerShell scripts.
- [Servers-Standard \(Pg 505\)](#) - use these probes to query various devices using one of many Standard protocols.
- [Servers-Proprietary \(Pg 485\)](#) - use these probes to query various devices using one of many Proprietary protocols.
- [Miscellaneous Probes \(Pg 461\)](#) - use these probes for a variety of uses. You can find the Demo, Non-Polling, and TCP Check probes. You can also find the Legacy probes (included to support older maps) and the template for developing Nagios and Command-line probes.
- [Wireless Probes \(Pg 549\)](#) - Use these probes to get vendor-specific information from a number of wireless devices.
- [WMI Probes \(Pg 536\)](#) - If InterMapper is installed on a Windows machine, use these probes to get detailed information from Windows workstations through the Windows Management Instrumentation (WMI) interface.

Packet-based probes

Probes such as "Ping/Echo", "SNMP Traffic", "NNTP" and "RADIUS" send UDP packets to the device being tested and await a correctly formatted response.

- For more information on packet-based probes, see [About Packet-based Probes \(Pg 596\)](#) and [Network Device Probes \(Pg 466\)](#).

Probe timeout period

The timeout period for waiting is configured by choosing **Set Timeout** from the Set Probe Info submenu. If no response is received within the timeout period, InterMapper tries again by sending another request packet. This process is repeated until either a response is received, or the number of requests sent exceeds the "Number of Lost Packets" threshold set for the map (a default of 3).

Response packet integrity

All packet-based probes check the integrity of the response they receive, and some can set the status of the device (*Alarm*, *Warning*, or *OK*) based on the severity of a problem.

TCP-based probes

Probes like "HTTP", "SMTP", and "LDAP" and others test the ability of a server to accept a TCP connection on a specific listening port, and to respond to a scripted interchange.

- For more information on TCP-based probes see [Server Probes - Standard \(Pg 505\)](#).

What happens in a TCP-based interchange

1. InterMapper first attempts to connect to the specified port at the device's address.
2. If this connection attempt fails, InterMapper shows the device in the DOWN state.

If InterMapper successfully connects to the listening port, InterMapper sends protocol-specific commands through the TCP connection to test the server's responses and compare them to expected values.

3. InterMapper changes the status of the device (e.g. ALARM, WARNING, OKAY, DOWN) if an error condition is detected, or if the execution of InterMapper's probe is interrupted for any reason.
4. If InterMapper doesn't receive a proper response for 60 seconds, or if the TCP connection is lost while waiting for a response, the InterMapper probe will set status of the device to the proper condition.

Miscellaneous Probes

InterMapper has several "miscellaneous probes", described briefly below. They are described in detail in [Miscellaneous Probes \(Pg 461\)](#).

- **Demo probe** - Use this probe to create demonstration maps, which simulate a network and its activity.
- **Legacy probes** - These probes that have been superseded by other probes. They are included to support older maps.
- **Nagios** - Use the Nagios probe type to select plugins from the Nagios monitoring system. InterMapper can use these plugins to test devices. For more details, see the Nagios Plugins page in the [Developer Guide](#).
- **Non-polling probe** - Choose this probe so that the selected device is not probed.
- **Prototype SNMP probe** - Use this probe as the basis for creating custom SNMP probes.
- **TCP Check probe** - Use this probe to monitor the number of TCP connections to an SNMP-enabled device and to send an alarm when a specified number of connections is exceeded.

Troubleshooting PowerShell Probes

If you are having trouble getting PowerShell probes to work, you can look in the Debug Log information.

Each time a PowerShell probe is chosen or its parameters change, a connectivity test is run. If the test is successful, the probe runs at the next polling interval. For the connectivity test, and for each time a PowerShell probe runs, two entries are created:

- One entry shows the input string sent to `stdin`.
- A second entry shows the variables returned by the probe, enclosed in "`\{...\code>", followed by the string assigned to stdout.`

Probe Reference Index

Basic [view \(Pg 448\)](#)

- [Basic > Automatic](#) (Pg 448)
- [Basic > Map Status](#) (Pg 448)
- [Basic > Ping/Echo](#) (Pg 449)
- [Basic > SNMP Traffic](#) (Pg 449)

Experimental [view \(Pg 593\)](#)

- [Experimental > Flow Exporter Status](#) (Pg 593)
- [Experimental > InterMapper](#) (Pg 593)
- [Experimental > sFlow v1.2](#) (Pg 594)
- [Experimental > sFlow Vers. 1.3](#) (Pg 595)

Miscellaneous [view \(Pg 461\)](#)

- [Miscellaneous > Demo Probe](#) (Pg 461)
- [Miscellaneous > Legacy > Basic OID \(v2c\)](#) (Pg 461)
- [Miscellaneous > Legacy > Cisco \(v2c\)](#) (Pg 462)
- [Miscellaneous > Legacy > SNMP v2c](#) (Pg 462)
- [Miscellaneous > Nagios > Nagios Plugin](#) (Pg 463)
- [Miscellaneous > Non Polling](#) (Pg 463)
- [Miscellaneous > Prototype SNMP Probe](#) (Pg 464)
- [Miscellaneous > TCP Check](#) (Pg 465)

Network Devices [view \(Pg 466\)](#)

- [Network Devices > Apple > Apple AirPort \(Extreme\)](#) (Pg 466)
- [Network Devices > Apple > Apple AirPort \(Graphite\)](#) (Pg 467)
- [Network Devices > Cisco > Cisco IP SLA Jitter](#) (Pg 467)
- [Network Devices > Cisco > Cisco N5000 with FEX Traffic](#) (Pg 469)
- [Network Devices > Cisco > Cisco Old CPU MIB](#) (Pg 469)
- [Network Devices > Cisco > Cisco Process and Memory Pool](#) (Pg 470)
- [Network Devices > Cisco > Cisco Aironet](#) (Pg 470)
- [Network Devices > Juniper > Netscreen VPN](#) (Pg 471)
- [Network Devices > Karlnet Wireless](#) (Pg 471)
- [Network Devices > UPS > APC UPS AP961x](#) (Pg 471)
- [Network Devices > UPS > APC UPS](#) (Pg 472)
- [Network Devices > UPS > BestPower UPS](#) (Pg 473)
- [Network Devices > UPS > Exide UPS](#) (Pg 474)
- [Network Devices > UPS > Liebert UPS OpenComms](#) (Pg 474)
- [Network Devices > UPS > Liebert UPS Series 300](#) (Pg 475)
- [Network Devices > UPS > Liebert UPS](#) (Pg 476)
- [Network Devices > UPS > Standard UPS \(RFC1628\)](#) (Pg 476)
- [Network Devices > UPS > TrippLite UPS](#) (Pg 477)
- [Network Devices > UPS > Victron UPS](#) (Pg 477)

PowerShell [view \(Pg 479\)](#)

- [PowerShell > Disk Space](#) (Pg 479)
- [PowerShell > Remoting > Disk Space \(Signed\)](#) (Pg 480)

- [PowerShell > Remoting > Disk Space \(Pg 481\)](#)
- [PowerShell > Remoting > Installed Software \(Pg 481\)](#)
- [PowerShell > Remoting > Process Count \(Pg 482\)](#)

Probe Groups [view \(Pg 484\)](#)

- [Probe Groups > Probe Group \(Pg 484\)](#)

SNMP [view \(Pg 451\)](#)

- [SNMP > Basic OID \(Pg 451\)](#)
- [SNMP > Comparison \(Pg 451\)](#)
- [SNMP > High Threshold \(Pg 452\)](#)
- [SNMP > Low Threshold \(Pg 453\)](#)
- [SNMP > Range Threshold \(Pg 453\)](#)
- [SNMP > Restricted Interface \(Pg 454\)](#)
- [SNMP > Single OID Viewer \(Pg 454\)](#)
- [SNMP > SNMP High PPS \(Pg 455\)](#)
- [SNMP > SNMP High Traffic \(Pg 455\)](#)
- [SNMP > SNMP High Util \(Pg 455\)](#)
- [SNMP > String Comparison \(Pg 456\)](#)
- [SNMP > Table Viewer \(Pg 457\)](#)
- [SNMP > Trap Viewer \(Pg 458\)](#)

Servers Proprietary [view \(Pg 485\)](#)

- [Servers Proprietary > 4D Server \(Pg 485\)](#)
- [Servers Proprietary > Apache > \(Pg 486\)](#)
- [Servers Proprietary > Apple > AppleShareIP \(Pg 486\)](#)
- [Servers Proprietary > Apple > OS X Server > AFP \(Pg 487\)](#)
- [Servers Proprietary > Apple > OS X Server > FTP \(Pg 487\)](#)
- [Servers Proprietary > Apple > OS X Server > Info \(Pg 488\)](#)
- [Servers Proprietary > Apple > OS X Server > NAT \(Pg 488\)](#)
- [Servers Proprietary > Apple > OS X Server > Print \(Pg 488\)](#)
- [Servers Proprietary > Apple > OS X Server > QTSS \(Pg 489\)](#)
- [Servers Proprietary > Apple > OS X Server > Web \(Pg 489\)](#)
- [Servers Proprietary > Apple > RTMP \(Pg 490\)](#)
- [Servers Proprietary > Apple > Xserve > Xserve G4 \(Pg 490\)](#)
- [Servers Proprietary > Apple > Xserve > Xserve G5 \(Pg 491\)](#)
- [Servers Proprietary > Apple > Xserve > Xserve RAID \(Pg 492\)](#)
- [Servers Proprietary > Apple > Xserve > Xserve Tiger \(PPC\) \(Pg 492\)](#)
- [Servers Proprietary > Barracuda > Barracuda HTTP \(Pg 493\)](#)
- [Servers Proprietary > Barracuda > Barracuda HTTPS \(Pg 495\)](#)
- [Servers Proprietary > Big Brother Probe \(Pg 498\)](#)
- [Servers Proprietary > BlitzWatch \(Pg 498\)](#)
- [Servers Proprietary > Citrix Server \(Pg 498\)](#)
- [Servers Proprietary > Dartware > DataCenter > IMAuth \(Pg 499\)](#)
- [Servers Proprietary > Dartware > DataCenter > IMDatabase \(Pg 499\)](#)
- [Servers Proprietary > DND Protocol \(Pg 499\)](#)
- [Servers Proprietary > FileMaker Pro \(Pg 500\)](#)
- [Servers Proprietary > FirstClass Server \(Pg 500\)](#)
- [Servers Proprietary > KeyServer \(Pg 500\)](#)
- [Servers Proprietary > Lotus Notes \(Pg 501\)](#)

- [Servers Proprietary > MeetingMaker \(Pg 501\)](#)
- [Servers Proprietary > Microsoft > DHCP Lease Check \(Pg 501\)](#)
- [Servers Proprietary > Microsoft > NT Services \(Pg 502\)](#)
- [Servers Proprietary > Microsoft > SQL Server Query \(Pg 502\)](#)
- [Servers Proprietary > Nagios NRPE \(Pg 503\)](#)

Servers Standard [view \(Pg 505\)](#)

- [Servers Standard > Basic TCP \(Blocked\) \(Pg 506\)](#)
- [Servers Standard > Basic TCP \(Pg 506\)](#)
- [Servers Standard > Custom TCP \(Pg 506\)](#)
- [Servers Standard > CVS Server \(Pg 507\)](#)
- [Servers Standard > DHCPv4/BOOTP \(Pg 507\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(A\) Address \(Pg 508\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(MX\) Mail Server \(Pg 509\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(NS\) Name Server \(Pg 510\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(PTR\) Reverse Lookup \(Pg 510\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(TXT\) Text Record \(Pg 511\)](#)
- [Servers Standard > FTP > FTP \(Login\) \(Pg 512\)](#)
- [Servers Standard > FTP > FTP \(No Login\) \(Pg 512\)](#)
- [Servers Standard > Gopher \(Pg 513\)](#)
- [Servers Standard > Host Resources \(Pg 513\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Don't Match\) \(Pg 514\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Follow Redirects\) \(Pg 515\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Post\) \(Pg 515\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Proxy\) \(Pg 516\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Redirect\) \(Pg 517\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Pg 518\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Follow Redirects\) \(Pg 518\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Post\) \(Pg 519\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Redirect\) \(Pg 520\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(SSLv3\) \(Pg 521\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Pg 522\)](#)
- [Servers Standard > IPMI v2.0 \(Pg 522\)](#)
- [Servers Standard > IRC \(Pg 523\)](#)
- [Servers Standard > LDAP > LDAP SSL \(Pg 523\)](#)
- [Servers Standard > LDAP > LDAP \(Pg 524\)](#)
- [Servers Standard > LPR \(Pg 524\)](#)
- [Servers Standard > Mail > IMAP4 SSL \(Pg 525\)](#)
- [Servers Standard > Mail > IMAP4 \(Pg 525\)](#)
- [Servers Standard > Mail > POP3 SSL \(Pg 525\)](#)
- [Servers Standard > Mail > POP3 \(Pg 526\)](#)
- [Servers Standard > Mail > Roundtrip IMAP \(Pg 526\)](#)
- [Servers Standard > Mail > Roundtrip POP \(Pg 527\)](#)
- [Servers Standard > Mail > SMTP TLS \(Pg 528\)](#)
- [Servers Standard > Mail > SMTP \(Pg 528\)](#)
- [Servers Standard > Multimedia > Multicast Listener \(Pg 529\)](#)
- [Servers Standard > Multimedia > RTSP \(Pg 529\)](#)
- [Servers Standard > Network Time \(Pg 530\)](#)

- [Servers Standard > NNTP \(Pg 530\)](#)
- [Servers Standard > RADIUS \(Pg 530\)](#)
- [Servers Standard > SIP over UDP \(Pg 531\)](#)
- [Servers Standard > SNPP \(Pg 531\)](#)
- [Servers Standard > SSH \(Pg 532\)](#)
- [Servers Standard > Subversion > SVN \(Apache\) \(Pg 532\)](#)
- [Servers Standard > Subversion > SVN \(Svnserve\) \(Pg 533\)](#)
- [Servers Standard > Telnet \(Pg 534\)](#)
- [Servers Standard > VNC Server \(Pg 534\)](#)

Splunk [view](#)

- [Splunk > Layer 2 Output](#)

WMI [view \(Pg 536\)](#)

- [WMI > WMI CPU Utilization \(Pg 536\)](#)
- [WMI > WMI Disk Available \(Pg 537\)](#)
- [WMI > WMI Disk Fragmentation Analysis \(Pg 537\)](#)
- [WMI > WMI Event Log \(Pg 538\)](#)
- [WMI > WMI File Check \(Pg 539\)](#)
- [WMI > WMI Folder Check \(Pg 540\)](#)
- [WMI > WMI Free Memory \(Pg 540\)](#)
- [WMI > WMI Installed Software \(Pg 541\)](#)
- [WMI > WMI Logged on Users \(Pg 542\)](#)
- [WMI > WMI MExchange 2007 Hub Transport Server \(Pg 542\)](#)
- [WMI > WMI MExchange 2007 Mailbox Server \(Pg 543\)](#)
- [WMI > WMI Network Utilization \(Pg 543\)](#)
- [WMI > WMI Process Monitor \(Pg 544\)](#)
- [WMI > WMI Service Monitor \(Pg 545\)](#)
- [WMI > WMI SQL Server 2008 Service Monitor \(Pg 545\)](#)
- [WMI > WMI System Accessibility \(Pg 546\)](#)
- [WMI > WMI System Information \(Pg 547\)](#)
- [WMI > WMI Top Processes \(Pg 547\)](#)

Wireless [view \(Pg 549\)](#)

- [Wireless > Alvarion > Alvarion B 14 & B 28 \(BU\) \(Pg 550\)](#)
- [Wireless > Alvarion > Alvarion B 14 & B 28 \(RB\) \(Pg 551\)](#)
- [Wireless > Alvarion > BreezeACCESS \(AU\) \(Pg 551\)](#)
- [Wireless > Alvarion > BreezeACCESS \(SU\) \(Pg 552\)](#)
- [Wireless > Alvarion > BreezeACCESS LB \(Pg 552\)](#)
- [Wireless > Alvarion > BreezeACCESS VL \(AU\) \(Pg 553\)](#)
- [Wireless > Alvarion > BreezeACCESS VL \(SU\) \(Pg 553\)](#)
- [Wireless > Atmel > Atmel AT76C510 \(Pg 554\)](#)
- [Wireless > Basic > IEEE 802.11 \(Pg 555\)](#)
- [Wireless > Basic > SNMP for Wireless \(Pg 555\)](#)
- [Wireless > Canopy > Canopy \(AP\) \(Pg 555\)](#)
- [Wireless > Canopy > Canopy \(SM\) \(Pg 556\)](#)
- [Wireless > Canopy > Canopy Backhaul \(45 Mbps/FW 5830\) \(Pg 557\)](#)
- [Wireless > Canopy > Canopy Backhaul \(60 Mbp/FW 5840\) \(Pg 557\)](#)
- [Wireless > Canopy > Canopy Backhaul \(Master\) \(Pg 558\)](#)
- [Wireless > Canopy > Canopy Backhaul \(Slave\) \(Pg 558\)](#)

- [Wireless > Canopy > Canopy CMM Micro \(Pg 559\)](#)
- [Wireless > CB3 > CB3 Bridge \(Pg 559\)](#)
- [Wireless > CB3 > CB3 Deluxe Bridge \(Pg 559\)](#)
- [Wireless > Inscope Data > AirEther AB54 Series AP \(AP Mode\) \(Pg 560\)](#)
- [Wireless > Inscope Data > AirEther AB54 Series AP \(Bridge Mode\) \(Pg 560\)](#)
- [Wireless > Inscope Data > AirEther AB54 Series AP \(Client Mode\) \(Pg 561\)](#)
- [Wireless > Inscope Data > AirEther AB54 Series AP \(Repeater Mode\) \(Pg 561\)](#)
- [Wireless > Inscope Data > AirEther CB54 Series Client \(Pg 562\)](#)
- [Wireless > MikroTik > MT Radio Uplink \(Pg 562\)](#)
- [Wireless > MikroTik > MT Routerboard \(Pg 563\)](#)
- [Wireless > MikroTik > MT Software Only \(Pg 564\)](#)
- [Wireless > MikroTik > WDS Bridge \(Pg 564\)](#)
- [Wireless > Motorola > PTP 400 Series Bridge \(Pg 565\)](#)
- [Wireless > Motorola > PTP 600 Series Bridge \(Pg 566\)](#)
- [Wireless > Orthogon > Gemini \(Pg 566\)](#)
- [Wireless > Orthogon > Spectra \(Pg 567\)](#)
- [Wireless > Other > HTTP \(Pg 567\)](#)
- [Wireless > Proxim > Proxim AP 2000 \(Pg 568\)](#)
- [Wireless > Proxim > Proxim AP 4000 \(Pg 569\)](#)
- [Wireless > Proxim > Proxim AP 600 \(Pg 569\)](#)
- [Wireless > Proxim > Proxim AP 700 \(Pg 570\)](#)
- [Wireless > Proxim > Proxim LAN Access Point \(Pg 570\)](#)
- [Wireless > Proxim > Tsunami GX \(Pg 571\)](#)
- [Wireless > Proxim > Tsunami MP.11 BSU \(Pg 572\)](#)
- [Wireless > Proxim > Tsunami MP.11 SU \(Pg 572\)](#)
- [Wireless > Redline > AN50 \(Pg 573\)](#)
- [Wireless > smartBridges > airBridge \(Pg 574\)](#)
- [Wireless > smartBridges > airClient Nexus PRO total \(Pg 574\)](#)
- [Wireless > smartBridges > airClient Nexus \(Pg 575\)](#)
- [Wireless > smartBridges > airHaul Nexus PRO total \(Pg 575\)](#)
- [Wireless > smartBridges > airHaul Nexus \(Pg 576\)](#)
- [Wireless > smartBridges > airHaul2 Nexus PRO \(Pg 577\)](#)
- [Wireless > smartBridges > airPoint Nexus PRO total \(Pg 577\)](#)
- [Wireless > smartBridges > airPoint Nexus \(Pg 578\)](#)
- [Wireless > smartBridges > airPoint \(Pg 578\)](#)
- [Wireless > smartBridges > airPoint2 Nexus PRO \(Pg 579\)](#)
- [Wireless > Trango > Trango M2400S \(AP\) \(Pg 580\)](#)
- [Wireless > Trango > Trango M5800S \(Pg 580\)](#)
- [Wireless > Trango > Trango M5830S \(SU\) \(Pg 581\)](#)
- [Wireless > Trango > Trango M5830S \(Pg 581\)](#)
- [Wireless > Trango > Trango M900S \(AP\) \(Pg 582\)](#)
- [Wireless > Trango > Trango P5830S \(master\) \(Pg 583\)](#)
- [Wireless > Trango > Trango P5830S \(remote\) \(Pg 583\)](#)
- [Wireless > Tranzeo > Sixth Generation AP \(Pg 584\)](#)
- [Wireless > Tranzeo > Sixth Generation CPE \(Pg 584\)](#)
- [Wireless > Tranzeo > Sixth Generation PxP \(Pg 585\)](#)
- [Wireless > Tranzeo > Tranzeo \(AP\) \(Pg 585\)](#)
- [Wireless > Tranzeo > Tranzeo \(PXP\) \(Pg 586\)](#)
- [Wireless > Tranzeo > Tranzeo \(SAI\) \(Pg 587\)](#)
- [Wireless > Tranzeo > Tranzeo 58XX Series Backhaul \(Pg 587\)](#)

- [Wireless > Tranzeo > Tranzeo AP 5A \(44R\) \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo AP 5A \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo Classic \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 200 \(1.77.R\) \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 200 \(Pg 589\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 5A \(44R\) \(Pg 589\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 5A \(Pg 590\)](#)
- [Wireless > Tranzeo > Tranzeo TR CPE \(Pg 590\)](#)
- [Wireless > WaveRider > CCU \(Pg 590\)](#)
- [Wireless > WaveRider > EUM \(Pg 591\)](#)

Basic

- [Basic > Automatic \(Pg 448\)](#)
- [Basic > Map Status \(Pg 448\)](#)
- [Basic > Ping/Echo \(Pg 449\)](#)
- [Basic > SNMP Traffic \(Pg 449\)](#)

[To Probe Index \(Pg 442\)](#)

Basic > Automatic

Automatic

This probe checks whether the device responds to SNMP. If it doesn't, the probe is set to Ping/Echo.

How it works:

InterMapper sends a SNMP GetNextRequest for the sysName, sysObjectID, and sysServices OIDs (1.3.6.1.2.1.1.5.5, 1.3.6.1.2.1.1.5.2, and 1.3.6.1.2.1.1.5.7, respectively) using the specified SNMP Read-only community string. Upon receiving a valid SNMP response, InterMapper sets the device's probe to SNMP. If not, the Ping/Echo probe is used.

Filename: `com.dartware.automatic`
Version: `1.7`

[Back to Top](#)

Basic > Map Status

Map Status

This probe allows InterMapper to monitor the state of a map running on an InterMapper server. InterMapper periodically queries the specified map, and sets the device status to the status of the "worst" item on that map. Double-click the device to view specified map.

The easiest way to use this probe is to drag a map from the Map List onto another editable map. You can also create a device using the DNS Name or IP address of the InterMapper server containing the map, or "localhost" for a local map. Then set the following:

Map Name - The name of the map on the remote server.

Username - A user name that has read-permission on the map.

Password - The password for the specified user.

Filename: `com.dartware.map.status`
Version: `1.8`

[Back to Top](#)

Basic > Ping/Echo

Ping/Echo

This probe sends an ICMP echo request packet to the target device to determine if it is active and responding.

Number of Data Bytes - The number of bytes of ICMP data to send. By default, 20 bytes of data is sent. The minimum value is 16 bytes; the maximum is 2000 bytes.

Data Pattern - The hexadecimal pattern repeated throughout the payload contents.

Tip: *To send a 1500-byte IP packet to an IPv4 target, set the number of data bytes to 1472. To send the same IP packet size to an IPv6 target, set the number of data bytes to 1452.*

InterMapper sends the ping packet, then waits for a response. The device's specified Timeout value is used to determine the amount of time the probe waits for a response. If no response is received within the specified time, InterMapper re-sends the echo request, waiting again the device's Timeout. When the probe reaches the device's limit of the number of pings to send (as determined by the device or map's limit), without receiving a response, the device status is set to DOWN.

By default, the number of echo requests is three, and the default timeout is three seconds. Thus it can take up to nine seconds to set a device status to DOWN.

Filename: `com.dartware.ping`
Version: `2.0`

[Back to Top](#)

Basic > SNMP Traffic

SNMP Traffic

This probe retrieves system and traffic information from an SNMP-enabled device. This information comes from the system and interfaces groups of SNMP MIB-II.

It shows traffic (bytes/second, packets/second, errors/minute) for each interface. Right-click a link to open the interface's Status Window.

The probe also shows sysLocation, sysContact, and sysUptime from the system group in the device's Status Window.

Note: *This is exactly the same probe as the "SNMP MIB-II" probe found in earlier versions of InterMapper. It was renamed to reflect its purpose more accurately.*

Filename: `com.dartware.snmp`
Version: `1.7`

[Back to Top](#)

SNMP

- [SNMP > Basic OID](#) (Pg 451)
- [SNMP > Comparison](#) (Pg 451)
- [SNMP > High Threshold](#) (Pg 452)
- [SNMP > Low Threshold](#) (Pg 453)
- [SNMP > Range Threshold](#) (Pg 453)
- [SNMP > Restricted Interface](#) (Pg 454)
- [SNMP > Single OID Viewer](#) (Pg 454)
- [SNMP > SNMP High PPS](#) (Pg 455)
- [SNMP > SNMP High Traffic](#) (Pg 455)
- [SNMP > SNMP High Util](#) (Pg 455)
- [SNMP > String Comparison](#) (Pg 456)
- [SNMP > Table Viewer](#) (Pg 457)
- [SNMP > Trap Viewer](#) (Pg 458)

[To Probe Index](#) (Pg 442)

SNMP > Basic OID

Basic OID

This probe lets you monitor a single, user-defined MIB variable.

Object Name - optional - The name of the value that you want to monitor. This parameter value is used only for display in the popup window and chart legend.

Object ID - The object identifier (OID) of the value that you want to monitor. To retrieve the value of a MIB variable that is not in a table, the OID must end with ".0" (e.g. "1.3.6.1.2.1.1.1.0").

This probe retrieves a lot of SNMP information from the device, including the MIB-II system group and the interfaces table. If you just want to monitor a single SNMP variable, use the SNMP/Single OID probe.

Filename: `com.dartware.snmp.basic`
Version: `0.7`

[Back to Top](#)

SNMP > Comparison

Comparison

This probe retrieves a single SNMP MIB variable, compares it to a specified value, and uses the result to set the device's status. It also displays the value in the Status Window.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Test - Choose whether to set the status to ALARM if the device is **Equal** or **NotEqual** to the Value parameter.

Value - The value to compare against.

Severity - The status to use if the comparison fails.

Legend - A text string used to identify the variable in the status window and any strip charts. If left blank, the variable's name or OID is used.

Units - optional - A text string that is displayed next to the value in the Status Window, intended for use as a unit of measure (packets/sec, degrees, etc.)

Tag - A short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: com.dartware.snmp.oidcomparison.txt
Version: 1.11

[Back to Top](#)

SNMP > High Threshold

High Threshold

This probe retrieves a single SNMP MIB variable and compares it to the specified thresholds below. If the value goes above any of the specified thresholds, the device changes to the specified state.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Critical, Alarm, and Warning - the threshold to be used for comparison for each severity. Thresholds may be positive or negative numbers.

Legend - a text string used to identify the variable in the status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status Window. Usually used for units of measure (packets/sec, degrees, etc.)

Tag - A short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: com.dartware.snmp.oidhigh.txt
Version: 1.6

[Back to Top](#)

SNMP > Low Threshold

Low Threshold

This probe retrieves a single SNMP MIB variable and compares it to the specified thresholds below. If the value goes below any of the specified thresholds, the device changes to the specified state.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Critical, Alarm, and Warning - the threshold to be used for comparison for each severity. Thresholds may be positive or negative numbers.

Legend - a text string used to identify the variable in the status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status Window. Usually used for units of measure (packets/sec, degrees, etc.)

Tag - A short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: com.dartware.snmp.oidlow.txt

Version: 1.6

[Back to Top](#)

SNMP > Range Threshold

Range Threshold

This probe retrieves a single SNMP MIB variable and compares it to the specified thresholds. If the value goes outside the specified range, the device changes to the corresponding state.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Critical, Alarm, and Warning - the threshold to be used for comparison for each severity. Thresholds may be positive or negative numbers.

Legend - a text string used to identify the variable in the status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status Window. Usually used for units of measure (packets/sec, degrees, etc.)

Tag - A short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidrange.txt`
Version: `1.7`

[Back to Top](#)

SNMP > Restricted Interface

Restricted Interface

This probe is identical to the Basic SNMP Traffic probe, except that it restricts the visible interfaces to those that match the specified Interface Description.

Parameters

Interface Description - specifies the interfaces to display. Any interface with a value of *ifDescr* that matches this pattern is visible on the map. Non-matching interfaces are hidden.

Filename: `com.dartware.snmp.restrictedint.txt`
Version: `0.2`

[Back to Top](#)

SNMP > Single OID Viewer

Single OID Viewer

This probe retrieves a single SNMP MIB variable and displays it in the device's Status Window.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Legend - a text string used to identify the variable in the status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status Window. Usually used for units of measure (packets/sec, degrees, etc.)

Tag - A short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: com.dartware.snmp.oidsingle.txt
Version: 1.5

[Back to Top](#)

SNMP > SNMP High PPS

SNMP - High PPS

*This probe monitors the ifInPackets and ifOutPackets statistics of the specified device interface, and sets the state of the device to **Alarm** or **Warning** when the packet rate (in packets/second) exceeds specified thresholds. It sets the state to **Down** if the interface's ifOperStatus is not equal to 1 (Up).*

Parameters

Port Number - the ifIndex of the port to monitor.

Warn Threshold and Alarm Threshold - threshold values in packets-per-second.

Filename: com.dartware.snmp.pps.txt
Version: 0.6

[Back to Top](#)

SNMP > SNMP High Traffic

SNMP - High Traffic

*This probe monitors the ifInOctets and ifOutOctets traffic statistics of a particular interface on the device, and sets the device to **Alarm** or **Warning** when the traffic exceeds specified thresholds. It sets the device's state to **Down** if the interface's ifOperStatus is not equal to 1 (up).*

Parameters

Port Number - The ifIndex of the port to monitor.

Warn Threshold and Alarm Threshold - Thresholds in bytes per second.

Filename: com.dartware.snmp.traffic.txt
Version: 0.4

[Back to Top](#)

SNMP > SNMP High Util

SNMP - High Util

This probe monitors the utilization of ifInOctets and ifOutOctets traffic statistics of a particular interface on the device, and sets the device to

Alarm or **Warning** when the traffic exceeds specified utilization thresholds. It sets the device's state to **Down** if the interface's ifOper-Status is not equal to 1 (up)

Parameters

Port Number - The ifIndex of the port to monitor.

Warn Threshold and Alarm Threshold - Threshold, specified as a percentage of bandwidth utilization.

Filename: `com.dartware.snmp.traffic-util.txt`
Version: `0.3`

[Back to Top](#)

SNMP > String Comparison

String Comparison

This probe retrieves a single SNMP MIB variable, compares it to a specified value, and sets the device's severity based on the comparison. It also displays the value in the Status Window.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Test - choose whether the device is equal to the Value parameter or not.

Value - the value to compare with the MIB variable's value.

Severity - choose severity level to use if the value does not match the specified value.

Legend - a text string used to identify the variable in the status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status Window. Usually used for units of measure (packets/sec, degrees, etc.)

Tag - A short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidstrcomparison.txt`
Version: `1.9`

[Back to Top](#)

SNMP > Table Viewer**Table Viewer**

This probe shows the contents of several useful tables from common SNMP MIBs. It retrieves its data by walking the SNMP data values in the tables.

- **ifTable** - The "Interfaces" table gives information about the physical and logical interfaces of the device. It shows the following columns: *ifIndex*, *ifDescr*, *ifType*, *ifSpeed*, *ifPhysAddress*, *ifOperStatus*, and *ifAdminStatus*. It is defined in MIB-II (RFC-1213) and updated in the IF-MIB.
- **ifXTable** - The "Extended Interfaces" table defined in IF-MIB. It adds the *ifName* and *ifAlias* fields/columns to those shown in *ifTable* above.
- **Traffic Counters** - Shows traffic counters *ifInOctets* and *ifOutOctets* from the MIB-II *ifTable*, and the *ifHCInOctets* and *ifHCOctets* from the IF-MIB. To determine the traffic rate, refresh the window and compare two separate readings. The difference divided by the time between the refreshes (in seconds) is the number of bytes/second.
- **tcpConnTable** - Shows information about any present connections: Variables include *tcpConnLocalAddress*, *tcpConnLocalPort*, *tcpConnRemAddress*, and *tcpConnRemPort*. It is defined in MIB-II.
- **udpTable** - Shows information about any present UDP listeners: Variables include *udpLocalAddress*, *udpLocalPort*. It is defined in MIB-II.
- **ipAddrTable** - Shows the IP address/mask/broadcast address for each interface. Includes *ipAdEntAddr*, *ipAdEntIfIndex*, *ipAdEntNetMask*, *ipAdEntBcastAddr*, and *ipAdEntReasmMaxSize*. It is defined in RFC-1213, and updated in the IP-MIB.
- **ipRouteTable** - This table (currently deprecated) comes from RFC-1213 (MIB-II).
- **ipCidrRouteTable** and **ipForwardTable** - These tables come from the IP-FORWARD-MIB, and show information about CIDR multi-path IP Routes. Note: the *ipForwardTable* obsoletes the *ipRouteTable* of MIB-II, and is in turn obsoleted by the *ipCidrRouteTable*.
- **ipNetToMediaTable** - The "Net Address-to-Media Address" table (also known as the "ARP Table") shows these fields/columns: *ipNetToMediaIfIndex*, *ipNetToMediaNetAddress*, *ipNetToMediaPhysAddress*, and *ipNetToMediaType*. It is defined in RFC-1213.
- **dot1dTpFdbTable** - The "Bridge MIB" (RFC1493) shows the forwarding database for transparent bridges.

A link to each table appears in the Status Window. Click the link to see the contents of the table on the selected device.

This probe requires that you first import these MIBs: [RFC1213-MIB \(MIB-II\)](#), [Bridge MIB \(rfc1493\)](#), [IP-MIB \(rfc2011\)](#), [IF-MIB \(rfc2863\)](#), and [IP-FORWARD-MIB \(rfc2096\)](#). These are all bundled together in a [single zip archive](#).

Parameters

None.

<p>Filename: <code>com.dartware.snmp.tableviewer.txt</code> Version: <code>1.9</code></p>
--

[Back to Top](#)

SNMP > Trap Viewer

Trap Viewer

This probe listens for trap packets and displays the contents of a trap in the Status Window. It does not actively poll the device, and takes no action based on the contents of the trap.

All variables parsed from the trap packet appear in the device's Status Window. You can use this probe as a prototype for making your own trap probes.

How the Trap Viewer Probe Works

When a trap arrives, the probe parses the trap to retrieve the values from the trap's header, along with the first ten items in its Varbind List. Each value is assigned to a variable for use by the probe; each is also shown in the Status Window.

To see how this probe works, you can configure your equipment to send traps to InterMapper, or use the `net-snmp snmptrap` command. Either way, the Status Window shows the values present in any traps that arrive.

For more information on the `snmptrap` command, see the `net-snmp` documentation for the [trap tutorial](#) and the [snmptrap command](#). The remainder of this note shows how to send a trap with variables from the Dartware MIB:

SNMPv1 Traps

- a) Add a device to a map with the IP address 192.168.56.78
- b) Set it to use this probe
- c) Issue the `snmptrap` command below from the command line (it should all be on one line):

```
snmptrap -v 1 -c commString localhost
1.3.6.1.4.1.6306.192.168.56.78 6 123 4567890
1.3.6.1.4.1.6306.2.1.1.0 s "05/08 23:26:35"
1.3.6.1.4.1.6306.2.1.2.0 s Critical
1.3.6.1.4.1.6306.2.1.3.0 s "Big Router"
1.3.6.1.4.1.6306.2.1.4.0 s "Critical: High Traffic"
1.3.6.1.4.1.6306.2.1.5.0 s "127.0.0.1"
1.3.6.1.4.1.6306.2.1.6.0 s "SNMP Traffic Probe"
```

SNMPv2c Traps

- a) Add a device to the map with an IP address of localhost
- b) Set it to use this probe
- c) Issue the `snmptrap` command below from the command line (it should all be on one line)

```
snmptrap -v 2c -c commString localhost
4567890 1.3.6.1.4.1.6306
1.3.6.1.4.1.6306.192.168.56.78 6 123 4567890
1.3.6.1.4.1.6306.2.1.1.0 s "05/08 13:26:35"
1.3.6.1.4.1.6306.2.1.2.0 s Critical
1.3.6.1.4.1.6306.2.1.3.0 s "Big Router"
1.3.6.1.4.1.6306.2.1.4.0 s "Critical: High Traffic"
1.3.6.1.4.1.6306.2.1.5.0 s "127.0.0.1"
1.3.6.1.4.1.6306.2.1.6.0 s "SNMP Traffic Probe"
```

Notes:

- This probe file contains the lines above in a single-line format suitable for copying and pasting.
- The parameters in this probe are unused, but could be used to set thresholds for various alarms.

Parameters

MinValue - Unused

MaxValue - Unused

Filename: `com.dartware.snmp.trapdisplay.txt`
Version: `2.3`

[Back to Top](#)

Miscellaneous

- [Miscellaneous > Demo Probe \(Pg 461\)](#)
- [Miscellaneous > Legacy > Basic OID \(v2c\) \(Pg 461\)](#)
- [Miscellaneous > Legacy > Cisco \(v2c\) \(Pg 462\)](#)
- [Miscellaneous > Legacy > SNMP v2c \(Pg 462\)](#)
- [Miscellaneous > Nagios > Nagios Plugin \(Pg 463\)](#)
- [Miscellaneous > Non Polling \(Pg 463\)](#)
- [Miscellaneous > Prototype SNMP Probe \(Pg 464\)](#)
- [Miscellaneous > TCP Check \(Pg 465\)](#)

[To Probe Index \(Pg 442\)](#)

Miscellaneous > Demo Probe

Demo Probe

Use this probe to build a demo map. The probe generates random data for the traffic on all its links, giving you something to look at. All data are chartable, and can be used to demonstrate strip charts or data collection.

The probe also toggles the device state between UP/OK and Down when you reprobe the device manually. This makes it easy to see what happens when a device goes down, especially for manual dependencies.

For simple maps, the parameters can be set to zero. To create complicated, heavily-interconnected demonstration maps, try setting the Link Count and Loop % parameters to 10 and 50, respectively.

Link Count - sets the number of interfaces to create when adding the device to the map.

Loop % - sets the percentage of links that should connect themselves to subnets already present on the map.

Filename: `com.dartware.demo`
Version: `1.6`

[Back to Top](#)

Miscellaneous > Legacy > Basic OID (v2c)

Basic OID (v2c)

This is a legacy probe, provided for compatibility with InterMapper Traditional and older versions of InterMapper (< 4.4). Use the Basic OID probe, setting the SNMP version to SNMP v2.

This probe lets you monitor a single, user-defined MIB variable. It uses SNMPv2c.

Object Name - optional - The name of the value that you want to monitor. It appears in the Status window and in a chart legend.

Object ID - The object identifier (OID) of the value that you want to monitor. To retrieve the value of a MIB variable that is not in a table, the OID must end with ".0" (e.g. "1.3.6.1.2.1.1.1.0").

Filename: `com.dartware.snmpv2c.basic`

Version: `1.5`

[Back to Top](#)

Miscellaneous > Legacy > Cisco (v2c)

Cisco (v2c)

This is a legacy probe, provided for compatibility with InterMapper Traditional and older versions of InterMapper (< 4.4). Use the Cisco - Process and Memory Pool probe instead and set the probe's SNMP version to SNMP v2 in the Probe Info window.

This probe monitors the CPU and Memory utilization of a Cisco router using SNMPv2c.

Parameters

*CPU Busy - Alarm - specifies the **Alarm** threshold for CPU utilization as a percentage. If the average CPU usage over a 1 minute interval exceeds this threshold, the device is set to Alarm state.*

*CPU Busy - Warning - specifies the **Warning** threshold for CPU utilization. If the average CPU usage over a 1 minute interval exceeds this threshold, the device is set to Warning state.*

*Low Memory - Alarm - specifies the **Alarm** threshold for the amount of free memory remaining (in bytes). If the free memory drops below this threshold, the device is set to Alarm state.*

*Low Memory - Warning - specifies the **Warning** threshold for the amount of free memory remaining (in bytes). If the free memory drops below this threshold, the device is set to Warning state.*

Filename: `com.dartware.snmpv2c.cisco`

Version: `1.11`

[Back to Top](#)

Miscellaneous > Legacy > SNMP v2c

SNMP v2c

This is a legacy probe, provided for compatibility with InterMapper Traditional and older versions of InterMapper (< 4.4). Use the SNMP Traffic probe, setting the SNMP version to SNMP v2.

The SNMP v2c probe retrieves MIB-II information from the device. This includes sysLocation, sysContact, and sysUptime from the system group, and traffic (bytes/second, packets/second, errors/minute) for each interface.

It uses the 64-bit counters for interface traffic statistics. This provides accurate information (without rollover) on very high speed links.

Filename: `com.dartware.snmpv2c`
Version: `1.6`

[Back to Top](#)

Miscellaneous > Nagios > Nagios Plugin

Nagios Plugin

This probe lets you specify a Nagios plugin. InterMapper invokes the plugin and uses the exit value to set the condition of the device. It uses the performance data returned by the plugin to create a nice display of chartable data.

Plugin - Should contain the same command line (including arguments) you would use to test the plugin manually.

Note: If you enter `${ADDRESS}` it is replaced with the device's IP address; `${PORT}` is replaced by the port specified for the probe.

This probe expects the plugin to be located in the InterMapper Settings/Tools directory.

Nagios and the Nagios logo are registered trademarks of Ethan Galstad. For more information, see <http://www.nagios.org>

Parameters

Plugin - enter the Nagios command string. You can use the `${ADDRESS}` and `${PORT}`, as mentioned above.

Filename: `com.dartware.nagios.template`
Version: `1.8`

[Back to Top](#)

Miscellaneous > Non Polling

Non-Polling

This probe does not cause any action to occur. It can be used as a placeholder for a device; it does not count against the InterMapper device count.

Filename: `com.dartware.nonpolling`

Version: `1.5`

[Back to Top](#)

Miscellaneous > Prototype SNMP Probe

Prototype SNMP Probe

This probe demonstrates an InterMapper SNMP probe. Many of these features are described in [Creating Your Own Probes](#), in the [Developer Guide](#). If you have questions about this probe, [please contact us](#).

This probe probably isn't useful for production work, but provides examples of techniques available in custom SNMP probes.

The probe demonstrates how to retrieve SNMP values from a device by specifying their OIDs and how to display those values in the device's Status Window.

*The probe also provides thresholds that set the device into **Alarm** or **Warning** state.*

*In this example, the device goes into **Alarm** or **Warning** state if it has been rebooted recently (controlled by the `RebootAlarm` and `RebootWarn` parameters - two and three minutes, by default) or if there aren't as many interfaces in the `ifTable` as specified (in the `ExpectedInterfaces` parameter.)*

This probe also demonstrates:

- **CALCULATION variables** - converts from centi-seconds (hundredths of a second) to seconds.
- **Formatting of the Status Window** - in the `<snmp-device-display>` section.
- **IMML** also allows you to create a link to a URL, using the `\U2-2=http://xxxx\` notation shown in the `<snmp-device-display>` section.

Parameters

RebootAlarm - set the device to **Alarm** if the `sysUptime` is less than the specified value in minutes.

RebootWarn - set the device to **Warning** if the `sysUptime` is less than the specified value in minutes.

ExpectedInterfaces - set the device to **Warning** if the `ifNumber` is greater than or equal to this value.

Filename: `com.dartware.snmp.prototype.txt`

Version: `1.4`

[Back to Top](#)

Miscellaneous > TCP Check

TCP Check

This probe generates an alarm if the count of TCP connections exceeds a specified number. It can be used to detect people telnetting into a box that shouldn't have connections, such as a router that might be attacked from outside your network).

*It retrieves the device's tcpCurrEstab variable and compares it. If the number of established TCP connections exceeds the value specified in Allowed TCP Connections, the device is set to **Alarm** state.*

Parameters

Allowed TCP Connections - The maximum number of TCP connections allowed.

<i>Filename:</i> <code>com.dartware.snmp.tcpcheck</code> <i>Version:</i> <code>1.6</code>
--

[Back to Top](#)

Network Devices

- [Network Devices > Apple > Apple AirPort \(Extreme\) \(Pg 466\)](#)
- [Network Devices > Apple > Apple AirPort \(Graphite\) \(Pg 467\)](#)
- [Network Devices > Cisco > Cisco IP SLA Jitter \(Pg 467\)](#)
- [Network Devices > Cisco > Cisco N5000 with FEX Traffic \(Pg 469\)](#)
- [Network Devices > Cisco > Cisco Old CPU MIB \(Pg 469\)](#)
- [Network Devices > Cisco > Cisco Process and Memory Pool \(Pg 470\)](#)
- [Network Devices > Cisco > Cisco Aironet \(Pg 470\)](#)
- [Network Devices > Juniper > Netscreen VPN \(Pg 471\)](#)
- [Network Devices > Karlnet Wireless \(Pg 471\)](#)
- [Network Devices > UPS > APC UPS AP961x \(Pg 471\)](#)
- [Network Devices > UPS > APC UPS \(Pg 472\)](#)
- [Network Devices > UPS > BestPower UPS \(Pg 473\)](#)
- [Network Devices > UPS > Exide UPS \(Pg 474\)](#)
- [Network Devices > UPS > Liebert UPS OpenComms \(Pg 474\)](#)
- [Network Devices > UPS > Liebert UPS Series 300 \(Pg 475\)](#)
- [Network Devices > UPS > Liebert UPS \(Pg 476\)](#)
- [Network Devices > UPS > Standard UPS \(RFC1628\) \(Pg 476\)](#)
- [Network Devices > UPS > TrippLite UPS \(Pg 477\)](#)
- [Network Devices > UPS > Victron UPS \(Pg 477\)](#)

[To Probe Index \(Pg 442\)](#)

Network Devices > Apple > Apple AirPort (Extreme)

Apple AirPort (Extreme)

This probe monitors the custom MIB in an Apple AirPort Extreme Base Station. This probe monitors the number of clients using the base station, and lists each with its signal strength.

The first version of AirPort Extreme was round; subsequent versions are square. There is one important difference between them:

- *The original round version does not return complete information to clients using the community string "public". To retrieve complete information from the original round version, you must set the community string to the AirPort Extreme's password.*
- *Subsequent versions have a settable SNMP community string. To use this probe on these versions, you must supply the SNMP community string as set in the AirPort Extreme.*

Parameters

None.

<i>Filename:</i> <code>com.dartware.snmp.airport.ext</code> <i>Version:</i> <code>1.6</code>

[Back to Top](#)

Network Devices > Apple > Apple AirPort (Graphite)

Apple AirPort (Graphite)

This probe monitors the custom MIB in an Apple AirPort Base Station (v1 = Graphite) using SNMPv1. This probe monitors the number of clients using the base station and lists each one with its signal strength.

Parameters

Read/Write Community - Use the AirPort Base Stations's password.

An SNMP set-request is sent, instructing the AirPort Base Station to discover its clients periodically and test the signal strength of each.

Filename: `com.dartware.snmp.airport`
Version: `1.8`

[Back to Top](#)

Network Devices > Cisco > Cisco IP SLA Jitter

Cisco - IP SLA Jitter

This probe extracts jitter test data from a Cisco IP SLA agent that is running on a Cisco router or switch. Typically these jitter tests are used to measure jitter, latency, and packet loss for VoIP and video conferencing applications.

Parameters

SNMP Index - The value used when configuring the IP SLA agent in the Cisco switch or router using the "ip sla monitor" command (see example below). This value identifies the jitter test, and is the SNMP index used by Intermapper to probe the device. To probe for different instances of jitter tests on a single Cisco switch or router, create separate devices on your Intermapper map, each using a different SNMP Index.

Latency Alarm Threshold - The ALARM threshold for latency in milliseconds. If Average Latency value exceeds this threshold, the device enters ALARM state.

Latency Warning Threshold The WARNING threshold for latency in milliseconds. If the Average Latency value exceeds this threshold, the device enters WARNING state.

Jitter Alarm Threshold - The ALARM threshold for Jitter. If the Average Jitter value exceeds this threshold, the device enters ALARM state.

Jitter Warning Threshold - The WARNING threshold for Jitter. If the Average Jitter value exceeds this threshold, the device enters WARNING state.

Packet Loss Alarm Threshold - The ALARM threshold for Packet Loss. If the Percent Packet Loss value exceeds this threshold, the device enters ALARM state.

Example

Example IOS commands for configuring an IP SLA jitter test to run on a Cisco router or switch:

```
ip sla monitor 250
type jitter dest-ipaddr w.w.w.w dest-port 50505 source-ipaddr x.x.x.x
num-packets 2000 interval 20
request-data-size 256
owner yyyy
tag zzzz
exit
```

In the above example specifies "250" as the SNMP index. This can be any value as long as it is unique. "w.w.w.w" is the IP address of the remote IP SLA responder. "x.x.x.x" is the local IP address of this IP SLA agent. "yyyy" is any text information identifying the owner of the test (e.g., name of network service provider). "zzzz" is any text information identifying this particular test.

To schedule the IP SLA test to run forever:

```
ip sla monitor schedule 66 life forever start-time now
```

To start the IP SLA responder on the remote IP SLA responder:

```
ip sla monitor responder
```

In the above IOS commands, the jitter test does not specify a codec type, so ICPIF and MOS scores are not available. If the test is modified to include a codec type then minor revisions are required to this SNMP probe. Also, some routers and switches may not support the MIB variables for ICPIF and MOS scores - this depends on the IOS train.

More information about configuring Cisco IP SLA is available on the www.cisco.com site.

<i>Filename:</i> com.dartware.snmp.cisco-ip-sla.txt <i>Version:</i> 2.4
--

[Back to Top](#)

Network Devices > Cisco > Cisco N5000 with FEX Traffic

Cisco - N5000 with FEX Traffic

This probe provides Basic SNMP Traffic probe functionality for the Nexus 5000 with Fiber Extender (FEX). The standard SNMP Traffic probe does not show the Fiber Extender's interfaces, so this probe incorporates special logic to retrieve that information.

This probe requires InterMapper Server version 5.6.6 or newer, which uses the special logic described above; otherwise, the speeds displayed for high speed interfaces are not shown correctly.

Parameters

None.

<p><i>Filename:</i> <code>com.dartware.snmp.cisco.n5kfex.traffic.txt</code> <i>Version:</i> <code>1.1</code></p>
--

[Back to Top](#)

Network Devices > Cisco > Cisco Old CPU MIB

Cisco - Old CPU MIB

This probe monitors the CPU and Memory utilization of a Cisco router.

Parameters

CPU Busy - Alarm - The ALARM threshold for CPU utilization in Per Cent. If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters ALARM state.

CPU Busy - Warning - The WARNING threshold for CPU utilization in Per Cent. If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters WARNING state.

Low Memory - Alarm - The ALARM threshold for the amount of free memory remaining (in bytes). If free memory drops below this threshold, the device enters ALARM state.

Low Memory - Warning - The WARNING threshold for the amount of free memory remaining (in bytes). If free memory drops below this threshold, the device enters WARNING state.

<p><i>Filename:</i> <code>com.dartware.snmp.cisco</code> <i>Version:</i> <code>1.9</code></p>

[Back to Top](#)

Network Devices > Cisco > Cisco Process and Memory Pool***Cisco - Process and Memory Pool***

This probe monitors the CPU and Memory utilization in a Cisco router. It uses variables from CISCO-MEMORY-POOL-MIB and CISCO-PROCESS-MIB.

Parameters

CPU Busy - Alarm - The ALARM threshold for CPU utilization in Per Cent. If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters ALARM state.

CPU Busy - Warning - The WARNING threshold for CPU utilization in Per Cent. If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters WARNING state.

Low Memory - Alarm - The ALARM threshold for the amount of free memory remaining (in bytes). If the free memory drops below this threshold, the device enters ALARM state.

Low Memory - Warning - The WARNING threshold for the amount of free memory remaining (in bytes). If the free memory drops below this threshold, the device enters WARNING state.

<i>Filename:</i> <code>com.dartware.snmp.cisconewmib</code> <i>Version:</i> <code>1.9</code>

[Back to Top](#)

Network Devices > Cisco > Cisco Aironet***Cisco Aironet***

This probe uses SNMPv1 to monitor the custom MIB in a Cisco Aironet Wireless Access Point. It monitors the number of clients using the base station and lists each client with its signal strength.

The alarm and warning thresholds must be greater than zero, or they are ignored.

Parameters

Number of Active Stations alarm - Set the threshold at which the device goes into ALARM state.

Number of Active Stations warning - Set the threshold at which the device goes into WARNING state.

<i>Filename:</i> <code>com.dartware.snmp.aironet</code> <i>Version:</i> <code>1.6</code>

[Back to Top](#)

Network Devices > Juniper > Netscreen VPN

Netscreen VPN

This probe monitors the status of VPN Tunnels in a Netscreen Firewall. It uses the `nsVpnMonTable` to monitor the Netscreen's active tunnels. Each active tunnel is treated and mapped as a separate interface.

Some statistics may be available only if the monitoring status for the tunnel as reported by `nsVpnMonMonState` is on.

Parameters

None.

Filename: `com.dartware.snmp.netscreen.txt`
Version: `1.2`

[Back to Top](#)

Network Devices > Karlnet Wireless

Karlnet Wireless

This probe monitors the custom MIB in a Karlnet Wiress Base Station using SNMPv1. It monitors the number of clients using the base station and lists each, along with its signal strength.

This probe sends SNMP set-requests to the Karlnet Base Station, causing it to discover and test the signal strength of each client. For the set-requests to work, enter the read/write community string for the base station.

Parameters

Read/Write Community - SNMP Read/Write community string.

Filename: `com.dartware.snmp.karlnet`
Version: `1.6`

[Back to Top](#)

Network Devices > UPS > APC UPS AP961x

APC UPS - AP961x

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

*(1 of 2) **APC UPS MIB** [... enterprises.apc.products.hardware.ups / ... 1.3.6.1.4.1.318.1.1.1]*

(2 of 2) **APC Environmental Monitoring MIB** [... enterprises.apc.products.hardware.environmentalMonitor / ... 1.3.6.1.4.1.318.1.1.10]

B. Displayed Values

UPS: model, firmware, status, (battery: capacity, time remaining, temperature, replacement status), (output: load percent, volts, amps, frequency), (input: volts, voltage range over last minute, frequency, last input failure).

Environmental Monitor: probe name, number of probes, current temperature & humidity, high & low threshold configurations.

C. Alarms

(1 of 3) If unit goes onto battery or goes off-line.

(2 of 3) If battery needs replacement.

(3 of 3) If the UPS' internal temperature/humidity threshold is exceeded (must also be enabled).

D. Warnings

(1 of 1) If unit goes onto "Smart Trim" or "Smart Boost"

Parameters

None.

<p><i>Filename:</i> com.dartware.ups.apc-ap961x.txt</p> <p><i>Version:</i> 3.5</p>
--

[Back to Top](#)

Network Devices > UPS > APC UPS

APC UPS

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

*(1 of 1) **APC UPS MIB** [... enterprises.apc.products.hardware.ups / ... 1.3.6.1.4.1.318.1.1.1]*

B. Displayed Values

UPS: model, firmware, status, (battery: capacity, time remaining, temperature, replacement status), (output: load percent, volts, amps, frequency), (input: volts, voltage range over last minute, frequency, last input failure).

C. Alarms

(1 of 3) If unit goes onto battery or goes off-line.

(2 of 3) If battery needs replacement.

(3 of 3) If the battery temperature exceeds user-specified thresholds (see "Parameters" below).

D. Warnings

(1 of 2) If unit goes onto "Smart Trim" or "Smart Boost"

(2 of 2) If the battery temperature exceeds user-specified thresholds (see "Parameters" below).

Parameters

(1 of 5) Units of Temperature (C / F): Determines how the following thresholds are interpreted.

(2 of 5) Alarm Threshold - Low Temp: Threshold for alarm state (see above).

(3 of 5) Warning Threshold - Low Temp: Threshold for alarm state (see above).

(4 of 5) Warning Threshold - High Temp: Threshold for warning state (see above).

(5 of 5) Alarm Threshold - High Temp: Threshold for warning state (see above).

Filename: `com.dartware.ups.apc.txt`
Version: `3.5`

[Back to Top](#)

Network Devices > UPS > BestPower UPS

BestPower UPS

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

(1 of 1) **BestPower MIB** [... enterprises.bestPower.bestLink / ... 1.2947.1]

B. Displayed Values

vendor, model, firmware version, VA Rating, time on battery, time remaining, (input & output: voltage, current, frequency), output power, internal temperature.

C. Alarms & Warnings

(1 of 2) Warning: If UPS loses AC power.

(2 of 2) *Alarm: If minutes of battery life remaining is less than specified threshold.*

Parameters

(1 of 1) *BatteryRemainingAlarm: Threshold for alarm state (see above).*

Filename: `com.dartware.ups.bestpower.txt`
Version: `2.11`

[Back to Top](#)

Network Devices > UPS > Exide UPS

Exide UPS

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

(1 of 2) **UPS MIB (RFC 1628)** [... `mib-2.upsMIB` / ... 1.33]

(2 of 2) **Exide XUPS MIB** [... `enterprises.powerware` / ... 1.534]

B. Displayed Values

vendor, model, software version, firmware version, output source, battery status, battery voltage, battery current, (three input lines: Hz, volts, amps, kWatts), (three output lines: Hz, volts, amps, kWatts, output load percent)

C. Alarms

(1 of 1) *If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).*

Parameters

None.

Filename: `shef.ac.uk.ups.exide.txt`
Version: `2.12`

[Back to Top](#)

Network Devices > UPS > Liebert UPS OpenComms

Liebert UPS - OpenComms

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

(1 of 2) **UPS MIB (RFC 1628)** [... `mib-2.upsMIB` / ... 1.33]

(2 of 2) **Liebert Global Products MIB** [... enterprises.emerson.liebertCorp.liebertGlobalProducts / ... 1.476.1.42]

B. Displayed Values

vendor, model, software version, firmware version, output source, battery status, battery voltage, battery current, (three input lines: Hz, volts, amps, kWatts), (three output lines: Hz, volts, amps, kWatts, output load percent); (temperatures: battery, ambient)

C. Alarms

(1 of 1) If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).

Parameters

None.

<p>Filename: com.dartware.ups.liebert-opencomms.txt Version: 2.13</p>

[Back to Top](#)

Network Devices > UPS > Liebert UPS Series 300

Liebert UPS - Series 300

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

(1 of 1) **LIEBERT-SERIES-300-UPS-MIB** [... enterprises.emerson.liebertCorp.liebertUps.luExtensions.luCore / ... 1.476.1.1.1.1] and [... luExtensions.luUPStationS / ... 1.2]

B. Displayed Values

vendor, model, software version, firmware version, output load (%), battery voltage, battery current, (three input, output, and bypass phases: voltage, current),(frequencies: input, output, bypass)

C. Alarms

(1 of 1) If the device is reporting any alarms. (The MIB includes a comprehensive list of alarms).

Parameters

None.

<p>Filename: com.dartware.ups.liebert-series300.txt Version: 2.7</p>
--

[Back to Top](#)

Network Devices > UPS > Liebert UPS**Liebert UPS**

NOTE: This probe is meant to aid Dartware's development of probes for the Liebert product line.

- 1) Check other probes to see if one exists for your Liebert UPS device.
- 2) If not, select this probe.
- 3) Open the status window and "Copy All" (right/option click on the window)
- 4) "Paste" into an email and [send the info to us](#).
- 5) We'll try to develop a probe for your device as soon as possible.

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

(1 of 1) **Liebert UPS MIB** [... enterprises.emerson.liebertCorp.liebertUps / ... 1.476.1.1]

B. Displayed Values

MIB, vendor, model, & software version

Parameters

None.

<p><i>Filename:</i> com.dartware.ups.liebert-ups.txt</p> <p><i>Version:</i> 2.7</p>

[Back to Top](#)

Network Devices > UPS > Standard UPS (RFC1628)**Standard UPS (RFC1628)****A. Probed MIB(s)**

This probe works best with devices which have implemented the listed MIB(s).

(1 of 1) **UPS MIB (RFC 1628)** [... mib-2.upsMIB / ... 1.33]

B. Displayed Values

vendor, model, software version, firmware version, output source, battery status, battery voltage, battery current, (three input lines: Hz, volts, amps, kWatts), (three output lines: Hz, volts, amps, kWatts, output load percent)

C. Alarms

(1 of 1) *Alarm: If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).*

(2 of 2) *Alarm: If the battery temp exceeds a user-defined threshold.*

Parameters

UserHighBatteryTemperatureAlarm - Threshold for alarm state (see above). This alarm is disabled when the threshold is set to "0" (default).

Filename: `com.dartware.ups.standard.txt`
Version: `3.5`

[Back to Top](#)

Network Devices > UPS > TrippLite UPS

TrippLite UPS

A. Probed MIB(s)

This probe works best with devices which have implemented the listed MIB(s).

(1 of 2) **UPS MIB (RFC 1628)** [... `mib-2.upsMIB` / ... 1.33]

(2 of 2) **TrippUPS MIB** [... `enterprises.tripplite.trippUPS.trippUpsEnvironment` / 1.850.0.3]

B. Displayed Values

vendor, model, software version, firmware version, output source, battery status, battery voltage, battery current, (three input lines: Hz, volts, amps, kWatts), (three output lines: Hz, volts, amps, kWatts, output load percent); ambient temperature, ambient humidity

C. Alarms

(1 of 1) *If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).*

Parameters

None.

Filename: `com.dartware.ups.tripplite.txt`
Version: `2.12`

[Back to Top](#)

Network Devices > UPS > Victron UPS

Victron UPS

This probe monitors important values in the Victron UPS.

Parameters

UPS Battery Status - Alarm - ALARM threshold for Battery Status.

- *If the value is 2, the UPS working normally.*
- *If the value is 1, the UPS is on bypass, the device enters Alarm state.*

*UPS Battery Remaining - Warning - WARNING threshold for the estimated battery time remaining. If the Battery Remaining is less than this threshold, the device is set to **Warning**.*

*UPS Battery low Voltage - Warning - WARNING threshold for the min. battery voltage. If the Battery voltage is less than this threshold, the device is set to **Warning**.*

*Low Input Voltage line [1,2, or 3] - Alarm - ALARM threshold for the minimum specified input voltage on phase 1, 2, or 3. If the input voltage drops below this threshold, the device is set to **Alarm**.*

*Low Output Voltage line [1,2, or 3] - Alarm - ALARM threshold for the minimum specified output voltage on phase 1, 2, or 3. If the output voltage drops below this threshold, the device is set to **Alarm**.*

<i>Filename:</i> <code>de.medianet.freinet.ups.victron.txt</code> <i>Version:</i> <code>3.0</code>

[Back to Top](#)

PowerShell

- [PowerShell > Disk Space \(Pg 479\)](#)
- [PowerShell > Remoting > Disk Space \(Signed\) \(Pg 480\)](#)
- [PowerShell > Remoting > Disk Space \(Pg 481\)](#)
- [PowerShell > Remoting > Installed Software \(Pg 481\)](#)
- [PowerShell > Remoting > Process Count \(Pg 482\)](#)

[To Probe Index \(Pg 442\)](#)

PowerShell > Disk Space

Disk Space

This probe uses PowerShell to retrieve the disk space available on a drive on the target host. It uses WMI's ability to retrieve information from a remote host instead of PowerShell's remoting capability. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the Warning, Alarm and Critical parameters you set.

Parameters

Drive - set to "All" to list all Local hard drives on the host. Enter a list of comma-separated drive letters with colons. Drives can be listed regardless of whether they are local or not. Zero-sized drives, such as empty cd-roms, are not listed. The first drive failing the warning or critical criteria test is cited in the reason.

Warning, Alarm, Critical, Down (%) - enter a threshold for the percentage of disk space that changes the device's state to the specified alarm level.

User - may be a local user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank if authentication is not required, such as when the target is the localhost.

Password - enter a password for the specified user.

Timeout (sec) - enter a number of seconds to wait for a response from the target host.

PowerShell Version - Choose the version of PowerShell running on the InterMapper Server's host. (Note: This is not the target device's host.)

InterMapper invokes the WindowsWmiFreeDiskSpace.ps1 companion script, placed in the Tools folder of the InterMapper Settings folder when probe is loaded. It uses the exit value to set the condition of the device, and uses the performance data returned by the script to create a display of chartable data.

<p>Filename: <code>com.helpsystems.powershell.wmi.diskspace.txt</code></p> <p>Version: <code>1.0</code></p>

[Back to Top](#)

PowerShell > Remoting > Disk Space (Signed)

Disk Space (Signed)

This probe requires a companion script that must be signed and placed in the \InterMapper Setting\Tools folder before it can be run.

This probe uses PowerShell to determine the disk space available on a drive on the target host. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the Warning and Critical parameters you set. The target host must be running PowerShell with Remoting enabled.

Parameters

Drive - set to "All" to list all Local hard drives on the host. Use a list of comma-separated drive letters with colons. Drives can be listed regardless of whether they are local or not. Zero-sized drives (i.e. an empty cd-rom) are not listed. The first drive failing the warning or critical criteria test is cited in the reason.

Warning, Alarm, Critical, Down (%) - enter a threshold for the percentage of disk space that changes the device's state to the specified alarm level.

User - may be a local user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank if authentication is not required, such as when the target is the localhost.

Password - enter a password for the specified user.

Timeout (sec) - enter a number of seconds to wait for a response from the target host.

PowerShell Version - Choose the version of PowerShell running on the InterMapper Server's host. (Note: This is not the target device's host.)

InterMapper attempts to invoke the WindowsRemotingFreeDiskSpace.signed.ps1 companion script after setting ExecutionPolicy to "AllSigned". If InterMapper is installed in the default location, this script is available in the C:\Program Files\InterMapper\docs\samples\powershell folder. It must be copied to the Tools folder, and signed before it can be run. It uses the exit value to set the condition of the device and the performance data returned by the script to create a display of the results.

Filename:

`com.helpsystems.powershell.remote.diskspace.sign.txt`

Version: 1.0

[Back to Top](#)

PowerShell > Remoting > Disk Space

Disk Space

This probe uses PowerShell to determine the disk space available on a drive on the target host. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the Warning and Critical parameters you set. The target host must be running PowerShell with Remoting enabled.

Parameters

Drive - set to "All" to list all Local hard drives on the host. Use a list of comma-separated drive letters with colons. Drives can be listed regardless of whether they are local or not. Zero-sized drives (i.e. an empty cd-rom) are not listed. The first drive failing the warning or critical criteria test is cited in the reason.

Warning, Alarm, Critical, Down (%) - enter a threshold for the percentage of disk space that changes the device's state to the specified alarm level.

User - may be a local user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank if authentication is not required, such as when the target is the localhost.

Password - enter a password for the specified user.

Timeout (sec) - enter a number of seconds to wait for a response from the target host.

PowerShell Version - Choose the version of PowerShell running on the InterMapper Server's host. (Note: This is not the target device's host.)

InterMapper invokes the WindowsRemotingFreeDiskSpace.ps1 companion script, placed in the Tools folder of the InterMapper Settings folder when probe is loaded. It uses the exit value to set the condition of the device, and uses the performance data returned by the script to create a display of chartable data.

Filename: `com.helpsystems.powershell.remote.diskspace.txt`
Version: `1.0`

[Back to Top](#)

PowerShell > Remoting > Installed Software

Installed Software

*This probe uses PowerShell to provide a listing of installed software, installed updates, or both. This probe requires that **PowerShell 2.0** or later be installed, and PowerShell remoting must be enabled and*

configured to use this probe. This probe uses the registry, not WMI objects

Parameters

Software - Choose whether to list installed software, software updates, or both.

User - may be a local user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank if authentication is not required, such as when the target is the localhost.

Password - enter a password for the specified user.

Authentication - choose a type of authentication you want PowerShell to use to connect to the target host.

Timeout (sec) - enter a number of seconds to wait for a response from the target host.

PowerShell Version - Choose the version of PowerShell running on the InterMapper Server's host. (Note: This is not the target device's host.)

InterMapper invokes the included ApplicationList.ps1 companion script in InterMapper Settings/Tools.

Filename:

com.helpsystems.powershell.remote.installedSoftware.txt

Version: 1.0

[Back to Top](#)

PowerShell > Remoting > Process Count**Process Count**

This probe uses PowerShell's remoting capabilities and Get-Process object to retrieve the number of instances of a given process currently executing on the target host.

Parameters

ProcessName - enter the name of the process you want to monitor.

User - may be a local user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank if authentication is not required, such as when the target is the localhost.

Password - enter a password for the specified user.

Timeout (sec) - enter a number of seconds to wait for a response from the target host.

PowerShell Version - Choose the version of PowerShell running on the InterMapper Server's host. (Note: This is not the target device's host.)

InterMapper invokes the ProcessCount.ps1 companion script, placed in the Tools folder of the InterMapper Settings folder when probe is loaded.

Filename:

`com.helpsystems.powershell.remote.processcount.txt`

Version: 1.0

[Back to Top](#)

Probe Groups

- [Probe Groups > Probe Group \(Pg 484\)](#)

[To Probe Index \(Pg 442\)](#)

Probe Groups > Probe Group

Probe Group

This probe creates an empty probe group. Once you have created a device using this probe, you can select the new probe group device and other devices and choose Insert->Group to place those devices into the single probe group. Find out more about probe groups in the User Guide at <http://intermapper.com/go.php?to=intermapper.probegroups>.

Parameters

None.

<i>Filename:</i> <code>com.dartware.probegroup.txt</code> <i>Version:</i> <code>0.4</code>

[Back to Top](#)

Servers-Proprietary

- [Servers Proprietary > 4D Server](#) (Pg 485)
- [Servers Proprietary > Apache >](#) (Pg 486)
- [Servers Proprietary > Apple > AppleShareIP](#) (Pg 486)
- [Servers Proprietary > Apple > OS X Server > AFP](#) (Pg 487)
- [Servers Proprietary > Apple > OS X Server > FTP](#) (Pg 487)
- [Servers Proprietary > Apple > OS X Server > Info](#) (Pg 488)
- [Servers Proprietary > Apple > OS X Server > NAT](#) (Pg 488)
- [Servers Proprietary > Apple > OS X Server > Print](#) (Pg 488)
- [Servers Proprietary > Apple > OS X Server > QTSS](#) (Pg 489)
- [Servers Proprietary > Apple > OS X Server > Web](#) (Pg 489)
- [Servers Proprietary > Apple > RTMP](#) (Pg 490)
- [Servers Proprietary > Apple > Xserve > Xserve G4](#) (Pg 490)
- [Servers Proprietary > Apple > Xserve > Xserve G5](#) (Pg 491)
- [Servers Proprietary > Apple > Xserve > Xserve RAID](#) (Pg 492)
- [Servers Proprietary > Apple > Xserve > Xserve Tiger \(PPC\)](#) (Pg 492)
- [Servers Proprietary > Barracuda > Barracuda HTTP](#) (Pg 493)
- [Servers Proprietary > Barracuda > Barracuda HTTPS](#) (Pg 495)
- [Servers Proprietary > Big Brother Probe](#) (Pg 498)
- [Servers Proprietary > BlitzWatch](#) (Pg 498)
- [Servers Proprietary > Citrix Server](#) (Pg 498)
- [Servers Proprietary > Dartware > DataCenter > IMAuth](#) (Pg 499)
- [Servers Proprietary > Dartware > DataCenter > IMDatabase](#) (Pg 499)
- [Servers Proprietary > DND Protocol](#) (Pg 499)
- [Servers Proprietary > FileMaker Pro](#) (Pg 500)
- [Servers Proprietary > FirstClass Server](#) (Pg 500)
- [Servers Proprietary > KeyServer](#) (Pg 500)
- [Servers Proprietary > Lotus Notes](#) (Pg 501)
- [Servers Proprietary > MeetingMaker](#) (Pg 501)
- [Servers Proprietary > Microsoft > DHCP Lease Check](#) (Pg 501)
- [Servers Proprietary > Microsoft > NT Services](#) (Pg 502)
- [Servers Proprietary > Microsoft > SQL Server Query](#) (Pg 502)
- [Servers Proprietary > Nagios NRPE](#) (Pg 503)

[To Probe Index](#) (Pg 442)

Servers Proprietary > 4D Server

4D Server

This probe attempts to connect to a 4D server listening on port 19813. If the response contains the database name, the probe exits with OKAY status; if not, the result is WARN. If no response arrives within timeout, the probe exits with a WARN status.

<p><i>Filename:</i> <code>com.dartware.tcp.4D</code> <i>Version:</i> <code>1.5</code></p>

[Back to Top](#)

Servers Proprietary > Apache >

This probe monitors an Apache Web Server with the Apache Status module enabled (mod_status). The Apache Status module allows a server administrator to find out how well an Apache server is performing. This probe reads output of provided by the Status module that presents the current server statistics, using the ?auto parameter.

To enable status reports for this probe, add this code to the httpd.conf file on the target server:

```
<Location /server-status>
```

```
SetHandler server-status
```

```
Order Deny,Allow
```

```
Deny from all
```

```
Allow from InterMapper-Address
```

```
</Location>
```

This probe supports the Apache ExtendedStatus directive, if enabled.

Parameters

Host Name - Name of the host server

URL Path - Path to the server status page

User ID - Server administrator username

Password - Administrator password

Filename: com.dartware.tcp.apache.txt

Version: 1.1

[Back to Top](#)

Servers Proprietary > Apple > AppleShareIP**AppleShareIP**

The file-sharing protocol used by Apple computers over TCP/IP. The default TCP port number for AppleShareIP connections is port 548.

*This TCP probe connects to the AppleShareIP port and issues a "Get Server Info" request. If the the probe does not receive the expected response, the device's status is set to **Down**.*

This probe sends a request; it does not actually create an AppleShare session.

Filename: `com.dartware.tcp.appleshareip`
Version: `1.5`

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > AFP

AFP

This TCP probe queries a [Mac OS X Server](#) installation for various details about its Apple File Sharing using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *The implementation of this probe uses OpenSSL on MacOS X.*

Filename: `com.dartware.tcp.osxserver.afp.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > FTP

FTP

This TCP probe queries a [Mac OS X Server](#) installation for various details about its FTP Server using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *This probe uses OpenSSL on MacOS X.*

Filename: `com.dartware.tcp.osxserver.ftp.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > Info**Info**

This TCP probe queries a [Mac OS X Server](#) installation for various details using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *The implementation of this probe uses OpenSSL on MacOS X.*

<i>Filename:</i> <code>com.dartware.tcp.osxserver.info.txt</code> <i>Version:</i> <code>1.0</code>

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > NAT**NAT**

This TCP probe queries a [Mac OS X Server](#) installation for various details about its NAT service using the Server Admin port and protocol.

A request for status information is made via an HTTPS post to the Server Admin port. The server responds with XML data that is then parsed by the probe.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *The implementation of this probe uses OpenSSL on MacOS X.*

<i>Filename:</i> <code>com.dartware.tcp.osxserver.nat.txt</code> <i>Version:</i> <code>1.0</code>
--

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > Print**Print**

This TCP probe queries a [Mac OS X Server](#) installation for various details about its Print Server using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *The implementation of this probe uses OpenSSL on MacOS X.*

Filename: `com.dartware.tcp.osxserver.print.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > QTSS

QTSS

This TCP probe queries a [Mac OS X Server](#) installation for various details about its QuickTime Streaming Server using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *The implementation of this probe uses OpenSSL on MacOS X.*

Filename: `com.dartware.tcp.osxserver.qtss.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > OS X Server > Web

Web

This TCP probe queries a [Mac OS X Server](#) installation for various details about its Web Server using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

Note: *The implementation of this probe uses OpenSSL on MacOS X.*

Filename: `com.dartware.tcp.osxserver.web.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > RTMP

RTMP

This probe sends an AppleTalk RTMP RDR Request query of type 3, and waits for a RTMP response.

Filename: `com.dartware.rtmp`
Version: `1.5`

[Back to Top](#)

Servers Proprietary > Apple > Xserve > Xserve G4

Xserve G4

This TCP probe queries an Xserve G4 for various details using the Server Monitor port and protocol.

This probe will monitor Xserve G4s running Mac OS X 10.3.9 and earlier. For Xserves running 10.4 or later, please choose the Xserve Tiger probe.

A request for status information is made via an HTTPS post to the Server Monitor port. The server responds with XML data that is then parsed by the probe.

User is the name of any user on the specified server.

Password is the password for the user specified in User.

OS Version specifies the version of Mac OS X Server that is running on the Xserve.

The remaining options allow you to display or ignore the corresponding data. These options correspond to the tabs in the Server Monitor application on Mac OS X Server.

Info is general information about the server, such as amount of RAM and OS name and version.

Drives is information about the various drives installed on the server. This information includes the manufacturer, model, and capacity of each drive.

Power is information pertaining to the power supply.

Network information includes the hardware address, IP address, traffic information, and type of each interface.

Temperature is the ambient temperature of the server.

Blowers is information on the speed of the server's cooling fans.

Security monitors the state of the security lock and the enclosure.

Note: The implementation of this probe uses OpenSSL on MacOSX.

Filename: com.dartware.tcp.xserve.details

Version: 1.0

[Back to Top](#)

Servers Proprietary > Apple > Xserve > Xserve G5

Xserve G5

This TCP probe queries an [Xserve G5](#) for various details using the Server Monitor port and protocol.

Sends a request for status information via an HTTPS post to the Server Monitor port and parses an XML response.

Parameters

User - the name of any user on the specified server.

Password - the password for the specified user.

The remaining options let you display or ignore data in the response. These options correspond to tabs in the Server Monitor application on Mac OS X Server.

Info - general information about the server, such as amount of RAM, and OS name, and version.

Drives - information about the drives installed on the server. Includes the manufacturer, model, and capacity of each drive.

Power - information about the power supply.

Network - Includes the hardware address, IP address, traffic information, and type of each interface.

Temperature - the ambient temperature of the server.

Blowers - information on the speed of the server's cooling fans.

Security - the state of the security lock and the enclosure.

Note: *The implementation of this probe uses OpenSSL on MacOSX.*

Filename: `com.dartware.tcp.xserve.g5.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > Xserve > Xserve RAID

Xserve RAID

This TCP probe queries an [Xserve RAID](#) for various details using the RAID Admin port and protocol.

Sends a request to an Xserve Raid via an HTTPS post via a series of HTTP POSTs and parses an XML responses.

Parameters

Password - the RAID administrator's monitoring password.

Filename: `com.dartware.tcp.xserve.raid.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Apple > Xserve > Xserve Tiger (PPC)

Xserve Tiger (PPC)

This probe queries an [Xserve](#) running Mac OS X 10.4 using the Server Monitor port and protocol. Because of this, the probe requires an administrator's name and password in order to access the information. Due to significant hardware differences, there are separate probes for G4 Xserves, G5 Xserves, and Intel Xserves.

Apple has pre-configured several thresholds for various properties, such as temperatures, blower speeds, and power supply values. The Server Monitor protocol specifies when any of these thresholds are exceeded and the error message and status are reflected by this probe.

Sends a request for status information via an HTTPS post to the Server Monitor port and parses an XML response.

Parameters

User - the name of any user on the specified server.

Password - the password for the specified user.

The remaining options let you display or ignore data in the response. These options correspond to tabs in the Server Monitor application on Mac OS X Server.

Info - general information about the server, such as amount of RAM, and OS name, and version.

Drives - information about the drives installed on the server. Includes the manufacturer, model, and capacity of each drive.

Power - information about the power supply.

Network - Includes the hardware address, IP address, traffic information, and type of each interface.

Temperature - the ambient temperature of the server.

Blowers - information on the speed of the server's cooling fans.

Security - the state of the security lock and the enclosure.

Note: The implementation of this probe uses OpenSSL on MacOSX.

Filename: `com.dartware.tcp.xserve.tiger.txt`
Version: `1.0`

[Back to Top](#)

Servers Proprietary > Barracuda > Barracuda HTTP

Barracuda HTTP

This TCP probe queries a [Barracuda Spam Firewall](#) for various performance statistics.

The BASIC->Status page of the Administrators interface is retrieved via HTTP.

Parameters

User - Firewall administrator name.

Password - Firewall administrator password.

Port - Firewall's Web Interface HTTP Port as set on the BASIC->Administration page.

Thresholds

Set thresholds as follows:

In/Out Queue Size - The returned value should normally be less than 100. An In or Out Queue value that consistently exceeds 100 for more than 30 minutes **may** indicate a problem that needs attention.

Note: The returned value may rise temporarily, then go back down after 10 or 15 minutes.

- For the Inbound Queue, this is normal behavior, but can also be the result of an orchestrated attack. The Barracuda attempts to read as many messages as it can, which results in a slower processing rate,

which in turn increases the number of messages in the queue.

- For the Outbound Queue, an increase usually indicates that the destination server is unavailable or the local DNS is not functioning properly.

Recommended settings:

- A value exceeding 100 for more than 15 minutes should result in a **Warning**.
- A value exceeding 500 for more than 30 minutes should result in an **Alarm**.

Average Latency - The average time, in seconds, to receive, process and deliver the last 30 messages. The value should normally be below 50 seconds. If the latency consistently exceeds 50 seconds for more than 30 minutes **may** indicate a problem that needs attention. Sometimes the value will rise temporarily and then go back down after 10 or 15 minutes. This is normal behavior.

Recommended settings:

- A value exceeding 50 seconds for more than 15 minutes should result in a **Warning**.
- A value exceeding 150 seconds for more than 30 minutes should result in an **Alarm**.

Last Message - The time, in minutes, since the last message was received. For a busy machine, this value should normally be less than 5 minutes. A value consistently exceeding 20 minutes for more than 30 minutes **may** indicate a problem that needs attention. Sometimes the value will rise temporarily and then go back down after 2 or 3 minutes. This is normal behavior.

Recommended settings:

- A value exceeding 15 minutes should result in a **Warning**.
- A value exceeding 30 minutes should result in an **Alarm**.

CPU 1/CPU 2 Fan Speed - Should be between 3,000 and 5,000 (RPM)

Recommended settings:

- A value for either CPU fan that falls below 2500 should result in a **Warning**.
- A value for either CPU fan that falls below 500 should result in an **Alarm**.

Firmware Storage - Typical value (in percent) is 60 - 80%. A value above 80% usually means that a debug file needs to be deleted. This can be done on a non-emergency basis.

Recommended settings:

- A value above 80% should result in a **Warning**.
- A value above 90% should result in an **Alarm**.

Mail/Log Storage - Typical value (in percent) is 1 - 70%.

Recommended settings:

- A value above 70% should result in a **Warning**.
- A value above 80% should result in an **Alarm**.

*System Load - The system's load (in percent.) During normal operation, this value can vary wildly, anywhere between 1 and 100%. A value that remains at 100% for more than 2 hours **may** indicate a problem that needs attention. The value may rise temporarily, then go back down after 2 or 3 minutes. This is normal behavior.*

Recommended settings:

- A value above 80% for more than 1 hour should result in a **Warning**.
- A value above 90% for more than 3 hours should result in an **Alarm**.

CPU Temperature - Should be between 40 and 70 degrees C

Recommended settings:

- A value above 70 degrees C for more than 30 minutes should result in a **Warning**.
- A value above 80 degrees C for more than 1 hour should result in an **Alarm**.

Filename: `com.dartware.tcp.barracuda.http.txt`
Version: `3.1`

[Back to Top](#)

Servers Proprietary > Barracuda > Barracuda HTTPS

Barracuda HTTPS

This TCP probe queries a [Barracuda Spam Firewall](#) for various performance statistics.

The BASIC->Status page of the Administrators interface is retrieved via HTTPS.

Parameters

User - Firewall administrator name.

Password - Firewall administrator password.

Port - Firewall's Web Interface HTTP Port as set on the BASIC->Administration page.

Thresholds

Set thresholds as follows:

In/Out Queue Size - The returned value should normally be less than 100. An In or Out Queue value that consistently exceeds 100 for more than 30 minutes **may** indicate a problem that needs attention.

Note: The returned value may rise temporarily, then go back down after 10 or 15 minutes.

- For the Inbound Queue, this is normal behavior, but can also be the result of an orchestrated attack. The Barracuda attempts to read as many messages as it can, which results in a slower processing rate, which in turn increases the number of messages in the queue.
- For the Outbound Queue, an increase usually indicates that the destination server is unavailable or the local DNS is not functioning properly.

Recommended settings:

- A value exceeding 100 for more than 15 minutes should result in a **Warning**.
- A value exceeding 500 for more than 30 minutes should result in an **Alarm**.

Average Latency - The average time, in seconds, to receive, process and deliver the last 30 messages. The value should normally be below 50 seconds. If the latency consistently exceeds 50 seconds for more than 30 minutes **may** indicate a problem that needs attention. Sometimes the value will rise temporarily and then go back down after 10 or 15 minutes. This is normal behavior.

Recommended settings:

- A value exceeding 50 seconds for more than 15 minutes should result in a **Warning**.
- A value exceeding 150 seconds for more than 30 minutes should result in an **Alarm**.

Last Message - The time, in minutes, since the last message was received. For a busy machine, this value should normally be less than 5 minutes. A value consistently exceeding 20 minutes for more than 30 minutes **may** indicate a problem that needs attention. Sometimes the value will rise temporarily and then go back down after 2 or 3 minutes. This is normal behavior.

Recommended settings:

- A value exceeding 15 minutes should result in a **Warning**.
- A value exceeding 30 minutes should result in an **Alarm**.

CPU 1/CPU 2 Fan Speed - Should be between 3,000 and 5,000 (RPM)

Recommended settings:

- A value for either CPU fan that falls below 2500 should result in a **Warning**.
- A value for either CPU fan that falls below 500 should result in an **Alarm**.

Firmware Storage - Typical value (in percent) is 60 - 80%. A value above 80% usually means that a debug file needs to be deleted. This can be done on a non-emergency basis.

Recommended settings:

- A value above 80% should result in a **Warning**.
- A value above 90% should result in an **Alarm**.

Mail/Log Storage - Typical value (in percent) is 1 - 70%.

Recommended settings:

- A value above 70% should result in a **Warning**.
- A value above 80% should result in an **Alarm**.

*System Load - The system's load (in percent.) During normal operation, this value can vary wildly, anywhere between 1 and 100%. A value that remains at 100% for more than 2 hours **may** indicate a problem that needs attention. The value may rise temporarily, then go back down after 2 or 3 minutes. This is normal behavior.*

Recommended settings:

- A value above 80% for more than 1 hour should result in a **Warning**.
- A value above 90% for more than 3 hours should result in an **Alarm**.

CPU Temperature - Should be between 40 and 70 degrees C

Recommended settings:

- A value above 70 degrees C for more than 30 minutes should result in a **Warning**.
- A value above 80 degrees C for more than 1 hour should result in an **Alarm**.

<i>Filename:</i> <code>com.dartware.tcp.barracuda.https.txt</code> <i>Version:</i> 3.1

[Back to Top](#)

Servers Proprietary > Big Brother Probe

Big Brother Probe

This probe lets you use InterMapper as a Big Brother "BBDISPLAY" to collect information sent by Big Brother clients.

Purple Time - sets the number of minutes to wait without a report before indicating a problem. In an actual Big Brother server, this is thirty minutes; Big Brother shows a device as purple if it goes this long without a report from the device. This probe shows it as DOWN.

Filename: `com.dartware.bigbrother`
Version: `1.6`

[Back to Top](#)

Servers Proprietary > BlitzWatch

BlitzWatch

This probe monitors the performance of a BlitzMail server.

BlitzMail is a TCP/IP-based client-server electronic mail system developed at Dartmouth College. In the BlitzMail system, all mail and mail preferences are stored on one or more BlitzMail servers, giving a user access to email from anywhere.

This probe provides a simple view into the current state of a single BlitzMail server, showing simultaneous user count, CPU utilization, and disk transfer statistics.

Filename: `com.dartware.blitzwatch`
Version: `1.5`

[Back to Top](#)

Servers Proprietary > Citrix Server

Citrix Server

This probe connects to a Citrix server, using default port 1494. It checks for the presence of the string "ICA" in the response, which indicates that the Citrix server is running.

*This probe sets the device to **Alarm** if:*

- a disconnect is received unexpectedly.*
- doesn't receive a response within 30 seconds after connecting*
- the response doesn't contain the string "ICA"*

Parameters

None.

Filename: `com.dartware.tcp.citrix.txt`
Version: `1.2`

[Back to Top](#)

Servers Proprietary > Dartware > DataCenter > IMAuth

IMAuth

This TCP probe queries an [InterMapper DataCenter](#) server to verify that IMAuth is configured and running on that server. This only works with InterMapper DataCenter 5.1 or later.

Parameters

User - the DataCenter admin user's name.

Password - the DataCenter admin user's password.

Port - the port the DataCenter server listens on.

Filename: `com.dartware.tcp.imauth`
Version: `0.4`

[Back to Top](#)

Servers Proprietary > Dartware > DataCenter > IMDatabase

IMDatabase

This TCP probe queries an [InterMapper DataCenter](#) server to verify that IMDatabase is configured and running on that server. This will only work when run against InterMapper DataCenter 5.1 or later.

Parameters

User - the DataCenter admin user's name.

Password - the DataCenter admin user's password.

Port - the port the DataCenter server listens on.

Filename: `com.dartware.tcp.imdatabase`
Version: `0.4`

[Back to Top](#)

Servers Proprietary > DND Protocol

DND Protocol

The protocol used to lookup directory entries and validation information in a DND server. The DND is a centralized authentication/directory ser-

vice developed at Dartmouth College. The default TCP port number for DND connections is port 902.

Name - the name to look up in the DND.

Filename: `com.dartware.tcp.dnd`
Version: `1.6`

[Back to Top](#)

Servers Proprietary > FileMaker Pro

FileMaker Pro

This probe attempts to connect to a Filemaker Pro database server. By default, the port is 5003. If successful, device status is set to **Okay**.

Filename: `com.dartware.tcp.filemaker`
Version: `1.6`

[Back to Top](#)

Servers Proprietary > FirstClass Server

FirstClass Server

This probe connects to a FirstClass mail server. It sends two carriage returns, and expects to receive a banner; the default contains "FirstClass System". By default, it listens on port 510.

Filename: `com.dartware.tcp.firstclass`
Version: `1.6`

[Back to Top](#)

Servers Proprietary > KeyServer

KeyServer

This probe tests the operation of Sassafras Software's KeyServer via TCP/IP. [KeyServer](#) is a software license management tool for Windows, Macintosh and thin-client based computers.

The probe sends a proprietary status request to the KeyServer -- a full description is available from [Sassafras Software](#). By default, the server accepts UDP requests on port 19283.

KeyServer is a registered trademark of Sassafras Software.

Filename: `com.dartware.keyserver`
Version: `1.6`

[Back to Top](#)

Servers Proprietary > Lotus Notes

Lotus Notes

Lotus Notes uses Port 1352 for its Remote Procedure Call and Notes Replication.

This probe simply establishes a connection to the indicated port, which presumably is a Lotus Notes server. If the connection is successful, the device's status is set to OK; otherwise, its status is DOWN.

Filename: `com.dartware.tcp.lotusnotes`
Version: `1.4`

[Back to Top](#)

Servers Proprietary > MeetingMaker

MeetingMaker

The MeetingMaker server listens on port 649. This probe attempts to connect and exits with OKAY status if it succeeds.

Filename: `com.dartware.tcp.meetingmaker`
Version: `1.4`

[Back to Top](#)

Servers Proprietary > Microsoft > DHCP Lease Check

DHCP Lease Check

This probe monitors the count of free DHCP leases on a Microsoft DHCP server. If the count goes below the specified thresholds, the device enters ALARM or WARNING state.

The check is specific to a scope.

Parameters

Scope - The DHCP scope to check (e.g., "192.168.1.0").

Free Lease Warning - The number of remaining leases at which the device enters WARNING state.

Free Lease Alarm - The number of free leases remaining at which the device enters ALARM state.

Free Lease Critical - The number of free leases remaining at which the device enters CRITICAL state.

View the DHCP scope table - Click to view a list of available scopes, along with information about in-use lease, free lease, and pending offers.

Filename: `com.dartware.snmp.dhcpcheck.txt`
Version: `0.4`

[Back to Top](#)

Servers Proprietary > Microsoft > NT Services

NT Services

This probe monitors the state of one or more services on a Windows-based machine, Windows NT 4.0 and newer. InterMapper uses the Service Control Manager (SCM) to retrieve the information about the specified services. This probe works only if the InterMapper server is running on a Windows computer.

Services to Monitor - The list of services to be monitored. In the status window, services with green icons are currently running; those with red icons are stopped.

InterMapper monitors services whose boxes are checked. For a single machine, choose from all the services on the machine. For multiple machines, choose from those services common to all of the machines.

Username - The name of an administrative user on the machine being probed. InterMapper uses this username to log into the target machine to query the Service Control Manager.

Password - The password for the specified user.

If Username and Password are left blank, the user credentials under which InterMapper is running will be used.

Note: *In order for this probe to operate, InterMapper must be running as an administrative user, or you must supply an administrator username and password for in the NT Services panel in Server Settings. This allows InterMapper to elevate its privileges temporarily.*

Filename: `com.dartware.ntsvcs.std`
Version: `1.8`

[Back to Top](#)

Servers Proprietary > Microsoft > SQL Server Query

SQL Server Query

This probe establishes an ADO (ActiveX Data Object) connection to a Microsoft SQL Server running on the target host. It issues the specified

query and displays the returned fields. If no records are returned, the device status is set to Critical.

Parameters

Query - contains the SQL query to send. It should be enclosed in double-quotes. Using the "TOP" keyword in your query improve the response to the query. You may want to specify specific columns in your query and include a "WHERE" or an "ORDER BY" clause.

Rows and Columns - let you limit the output of your query. Enter the number of "Columns" and the number of "Rows" records of the query you want to view.

Instance - specifies the SQL Server instance on the target host the query is sent to. If you wish to query the default server instance, leave this field blank.

Database - specifies the database on the target instance to query.

User - can be an SQL Server user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank to use integrated authentication. The specified user must have dbreader privileges to the database.

Timeout (sec) - allows you to override the device's specified timeout.

InterMapper invokes the `sql_query.vbs` script, included with this probe.

Filename: `com.dartware.cmd.sql_query.txt`
Version: `1.4`

[Back to Top](#)

Servers Proprietary > Nagios NRPE

Nagios NRPE

The NRPE ("Nagios Remote Plugin Executor") protocol defines a way to execute Nagios plugins on remote machines. After you install a Nagios NRPE daemon and one or more Nagios plugins on a remote machine, InterMapper uses the following procedure to retrieve the status of that machine.

- *Establish an encrypted SSL/TLS connection to the remote NRPE daemon*
- *Request that a specific Nagios plugin be executed*
- *Receive the response from the plugin*
- *Parse the response and display the state of that machine.*

The NRPE daemon uses a configuration file (`nrpe.cfg`) that has command definition entries in this form:

```
command[check_swap]=/usr/local/nagios/libexec/check_swap -  
w 20% -c 10%
```

When the NRPE daemon receives a request to run the "check_swap" plugin, it issues the command above.

Parameters

Nagios Plugin - tells which plugin to execute. It must match one of the command definitions in the `nrpe.cfg` file (the text within square brackets [...]). To test the connection from InterMapper to the NRPE daemon, set *Nagios Plugin* to the value "`_NRPE_CHECK`".

For information about installing an NRPE daemon, see the [NRPE Documentation](http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf) (at <http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf>), especially the section on Remote Host Configuration. Nagios and the Nagios logo are registered trademarks of Ethan Galstad. For more information, see <http://www.nagios.org>.

<p><i>Filename:</i> <code>com.dartware.tcp.nrpe.txt</code> <i>Version:</i> <code>1.2</code></p>

[Back to Top](#)

Servers-Standard

- [Servers Standard > Basic TCP \(Blocked\) \(Pg 506\)](#)
- [Servers Standard > Basic TCP \(Pg 506\)](#)
- [Servers Standard > Custom TCP \(Pg 506\)](#)
- [Servers Standard > CVS Server \(Pg 507\)](#)
- [Servers Standard > DHCPv4/BOOTP \(Pg 507\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(A\) Address \(Pg 508\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(MX\) Mail Server \(Pg 509\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(NS\) Name Server \(Pg 510\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(PTR\) Reverse Lookup \(Pg 510\)](#)
- [Servers Standard > Domain Name \(DNS\) > DNS: \(TXT\) Text Record \(Pg 511\)](#)
- [Servers Standard > FTP > FTP \(Login\) \(Pg 512\)](#)
- [Servers Standard > FTP > FTP \(No Login\) \(Pg 512\)](#)
- [Servers Standard > Gopher \(Pg 513\)](#)
- [Servers Standard > Host Resources \(Pg 513\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Don't Match\) \(Pg 514\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Follow Redirects\) \(Pg 515\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Post\) \(Pg 515\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Proxy\) \(Pg 516\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Redirect\) \(Pg 517\)](#)
- [Servers Standard > HTTP & HTTPS > HTTP \(Pg 518\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Follow Redirects\) \(Pg 518\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Post\) \(Pg 519\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Redirect\) \(Pg 520\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(SSLv3\) \(Pg 521\)](#)
- [Servers Standard > HTTP & HTTPS > HTTPS \(Pg 522\)](#)
- [Servers Standard > IPMI v2.0 \(Pg 522\)](#)
- [Servers Standard > IRC \(Pg 523\)](#)
- [Servers Standard > LDAP > LDAP SSL \(Pg 523\)](#)
- [Servers Standard > LDAP > LDAP \(Pg 524\)](#)
- [Servers Standard > LPR \(Pg 524\)](#)
- [Servers Standard > Mail > IMAP4 SSL \(Pg 525\)](#)
- [Servers Standard > Mail > IMAP4 \(Pg 525\)](#)
- [Servers Standard > Mail > POP3 SSL \(Pg 525\)](#)
- [Servers Standard > Mail > POP3 \(Pg 526\)](#)
- [Servers Standard > Mail > Roundtrip IMAP \(Pg 526\)](#)
- [Servers Standard > Mail > Roundtrip POP \(Pg 527\)](#)
- [Servers Standard > Mail > SMTP TLS \(Pg 528\)](#)
- [Servers Standard > Mail > SMTP \(Pg 528\)](#)
- [Servers Standard > Multimedia > Multicast Listener \(Pg 529\)](#)
- [Servers Standard > Multimedia > RTSP \(Pg 529\)](#)
- [Servers Standard > Network Time \(Pg 530\)](#)
- [Servers Standard > NNTP \(Pg 530\)](#)
- [Servers Standard > RADIUS \(Pg 530\)](#)
- [Servers Standard > SIP over UDP \(Pg 531\)](#)
- [Servers Standard > SNPP \(Pg 531\)](#)
- [Servers Standard > SSH \(Pg 532\)](#)
- [Servers Standard > Subversion > SVN \(Apache\) \(Pg 532\)](#)
- [Servers Standard > Subversion > SVN \(Svnserve\) \(Pg 533\)](#)

- [Servers Standard > Telnet \(Pg 534\)](#)
- [Servers Standard > VNC Server \(Pg 534\)](#)

[To Probe Index \(Pg 442\)](#)

Servers Standard > Basic TCP (Blocked)

Basic TCP (Blocked)

*This basic TCP probe tests that a TCP port is **not** accepting connections. This probe may be used to test that a firewall is working properly, or that a particular TCP service is never operating on an important machine.*

*If the specified port accepts the TCP connection, the device state is set to the selected state. Otherwise, the device status is set to **OKAY**.*

*Failure Status - The device status upon successful connection. The default state is **DOWN**.*

Filename: `com.dartware.tcp.blocked`
Version: `1.5`

[Back to Top](#)

Servers Standard > Basic TCP

Basic TCP

*This basic TCP probe tests whether a TCP port accepts connections. If the specified port fails to accept the TCP connection within sixty seconds, the device state is set to **Down**.*

Filename: `com.dartware.tcp.basic`
Version: `1.5`

[Back to Top](#)

Servers Standard > Custom TCP

Custom TCP

This probe sends the specified string over a TCP connection, and sets the status of the device based on the response. Six parameters control the operation of this probe:

String to send - The initial string sent to the device via TCP. This could be a command which indicates what to test, or a combination of a command and a password. The string is sent on its own line, terminated by a CR-LF.

*Seconds to wait - The number of seconds to wait for a response. If no response is received within the specified number of seconds, the device's status is set to **Down**.*

OK Response - The substring to match the device's "ok response". If it matches the first line received, the device is reported to have a status of OK.

*WARN Response - The substring to match the device's **Warning** response.*

*ALRM Response - The substring to match the device's **Alarm** response.*

*CRIT Response - The substring to match the device's **Critical** response.*

*DOWN Response - The substring to match the device's **Down** response.*

*If InterMapper cannot connect to the specified TCP port, the device's status is set to **Down**.*

Filename: com.dartware.tcp.custom

Version: 1.9

[Back to Top](#)

Servers Standard > CVS Server

CVS Server

This probe tests a CVS server by connecting to the specified port and authentication strings as shown below. By default, the port is 2401.

BEGIN AUTH REQUEST<lf>

CVSROOT_Path<lf>

Username<lf>

Scrambled_password<lf>

END AUTH REQUEST<lf>\p

If the response is "I LOVE YOU", then the authentication succeeded.

If the response is "I HATE YOU", then either the authentication failed or the path to CVSROOT is incorrect.

Filename: com.dartware.tcp.cvs

Version: 1.6

[Back to Top](#)

Servers Standard > DHCPv4/BOOTP

DHCPv4/BOOTP

DHCP is the protocol used by IP clients to obtain an IPv4 address and other parameters for using TCP/IP. Depending on your setup, this probe may work only if your computer is already using an IP address acquired using BOOTP or DHCP.

Note: On Mac OS X, this probe will only work if no DHCP, Bootp, or PPP interfaces are enabled.

The probe sends DHCP-INFORM requests to test the DHCP mechanism for an IP subnet.

BOOTP Relay Address - the IP address to which all DHCP requests are addressed. Normal BOOTP/DHCP requests are broadcast to the local subnet (255.255.255.255), where they are picked up by the BOOTP agent in a router and relayed to the BOOTP/DHCP server. If this parameter is left blank, InterMapper sends the DHCP requests directly to the device's IP address.

DHCP Client ID - an optional parameter included with the DHCP-INFORM request that can be used to identify the DHCP client as InterMapper. If this parameter is blank, InterMapper does not include the DHCP Client ID option in its DHCP probe.

DHCP Subnet Mask - an optional parameter that specifies the expected value of the subnet mask returned by the DHCP server. If this parameter is blank, InterMapper accepts any subnet mask value.

DHCP Router Address - an optional parameter that specifies the expected value of the router address returned by the DHCP server. If this parameter is blank, InterMapper accepts any router address value.

DHCP Message Type - the type of DHCP message to send. Typically, you should use DHCP-INFORM, since this type will not cause the DHCP server to allocate an IP address. A DHCP server may respond to a DHCP-DISCOVER request by leasing an IP address which will never be used.

Hardware Address - an optional parameter that specifies the MAC address of the network interface used to send the DHCP request.

Request Seconds - an optional parameter that specifies the number of seconds to claim we have been sending DHCP requests. Certain DHCP servers (such as the one supplied with OS X 10.5 with the default settings) do not respond until the client claims to have been trying for at least 10 seconds.

<i>Filename:</i> com.dartware.dhcp <i>Version:</i> 2.0

[Back to Top](#)

Servers Standard > Domain Name (DNS) > DNS: (A) Address

DNS: (A) Address

DNS is the protocol used by TCP/IP network clients to translate Internet names into IP addresses, as defined in [RFC 1034](#) and [RFC 1035](#). This

probe sends a DNS request to look up the IP address for a specified domain name.

Domain Name - the fully qualified domain name you are attempting to resolve.

IP Address - optional parameter specifies an IP address the domain name should resolve to. If this parameter is not blank, InterMapper reports the status specified in Failure Status if one of the returned IP addresses doesn't match this address.

*Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is **True**, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of **False**.*

Failure Status - the device status InterMapper should report when the IP address in a DNS response doesn't match the specified IP Address parameter. By default, an IP address mismatch sets the device to Alarm. (Down is reserved for complete lack of response by the DNS server.)

Filename: `com.dartware.dns`
Version: `1.8`

[Back to Top](#)

Servers Standard > Domain Name (DNS) > DNS: (MX) Mail Server

DNS: (MX) Mail Server

The protocol used by TCP/IP network clients to translate Internet names into Mail servers, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the mail server for a specified domain name.

Domain Name - the fully qualified domain name to be resolved.

Mail Server - optional - specify a mail server the domain name should resolve to. If this parameter is non-empty, and one of the returned mail servers doesn't match the one provided, a status as specified in Failure Status is returned.

*Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is **True**, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of **False**.*

*Failure Status - specifies the device status returned when the DNS response returns a mail server that doesn't match the specified Mail Server. You can choose **Down**, **Alarm** or **Warning**. By default, mail server mismatches return an **Alarm** condition; **Down** is reserved for when the DNS server fails to respond at all.*

Filename: `com.dartware.dns.mx`

Version: 1.1

[Back to Top](#)

Servers Standard > Domain Name (DNS) > DNS: (NS) Name Server

DNS: (NS) Name Server

The protocol used by TCP/IP network clients to translate Internet names into name servers, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the name server for a specified domain name. CNAME records are accepted if no NS records are present in the response.

Domain Name - the fully qualified domain name to be resolved.

Name Server - optional - specify the name server the domain name should resolve to. If this parameter is non-empty, and one of the returned name servers doesn't match the one provided, a status as specified in Failure Status is returned.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is **True**, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of **False**.

Failure Status - specifies the device status returned when the DNS response returns a name server that doesn't match the specified Name Server. You can choose **Down**, **Alarm** or **Warning**. By default, name server mismatches return an **Alarm** condition; **Down** is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.ns`

Version: 1.1

[Back to Top](#)

Servers Standard > Domain Name (DNS) > DNS: (PTR) Reverse Lookup

DNS: (PTR) Reverse Lookup

The protocol used by TCP/IP network clients to translate IP addresses into Internet names, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the domain name for a specified IP address. Both PTR and CNAME records are accepted in the response.

Parameters

IP Address - the fully qualified IP address to be resolved.

Domain Name - optional - specify a domain name the IP address should resolve to. If this parameter is non-empty, and one of the returned domain names doesn't match the one provided, a status as specified in *Failure Status* is returned.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is **True**, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of **False**.

Failure Status - specifies the device status returned when the DNS response returns a domain name that doesn't match the specified Domain Name. You can choose **Down**, **Alarm** or **Warning**. By default, mail server mismatches return an **Alarm** condition; **Down** is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.ptr`
Version: `1.2`

[Back to Top](#)

Servers Standard > Domain Name (DNS) > DNS: (TXT) Text Record

DNS: (TXT) Text Record

The protocol used by TCP/IP network clients to translate Internet names into Text records, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the text record for a specified domain name.

Parameters

Domain Name - the fully qualified domain name to be resolved.

Text Substring - optional - specify a substring of a text record the domain name should resolve to. If this parameter is non-empty, and one of the returned text records doesn't contain the substring provided, the device's condition is set as specified in *Failure Status*.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is **True**, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of **False**.

Failure Status - specifies the device status returned when the DNS response text record in a DNS response doesn't contain the specified Text Substring. You can choose **Down**, **Alarm** or **Warning**. By default, mail server mismatches return an **Alarm** condition; **Down** is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.txt`
Version: `1.2`

[Back to Top](#)

Servers Standard > FTP > FTP (Login)

FTP (Login)

The standard protocol for transferring files on TCP/IP internets, as defined in [RFC 959](#). The default TCP port number for FTP control connections is port 21.

This TCP probe connects to the FTP server's control port (21). It then logs in using the specified User ID and Password and issues a NOOP command. If the connection is successful, the probe issues the QUIT command and sets the status to **Okay**.

Parameters

User ID - the account name used to login to the FTP server.

Password - the account password used to verify the User ID's identity.

Note: If the probe queries the FTP server often, and at regular intervals, the FTP server's log files contain a succession of "Login" and "Logout" log lines.

Filename: <code>com.dartware.tcp.ftp.login</code> Version: <code>1.9</code>
--

[Back to Top](#)

Servers Standard > FTP > FTP (No Login)

FTP (No Login)

The standard protocol for transferring files on TCP/IP internets, as defined in [RFC 959](#). The default TCP port number for FTP control connections is port 21.

This TCP script connects to the FTP server's control port (21). It then issues a NOOP command without logging in. If the connection is successful, the probe issues the QUIT command and sets the status to **Okay**.

Note: Use this script if you are going to be probing the FTP server frequently. Unlike the FTP (login) probe, this probe does generate numerous entries in your FTP logs.

Parameters

None.

Filename: <code>com.dartware.tcp.ftp.nologin</code> Version: <code>1.9</code>
--

[Back to Top](#)

Servers Standard > Gopher

Gopher

The document search and retrieval protocol described in [RFC 1436](#). The default TCP port number for Gopher connections is port 70.

This script connects to a Gopher server and sends the specified Selector string. By default, the Selector string is empty; the Gopher server returns top level information as a sequence of lines. This script simply checks that data is returned by the gopher server; it does not validate the data's contents.

Selector string - the string sent to the Gopher server. By default, this string is empty.

Filename: `com.dartware.tcp.gopher`
Version: `1.6`

[Back to Top](#)

Servers Standard > Host Resources

Host Resources

This probe uses SNMP to monitor elements of the Host Resources MIB of the target device.

Parameters

Processor Load Alarm % - Specifies the threshold, as a percentage of processor load, to enter ALARM state.

Processor Load Warning % - Specifies the threshold, as a percentage of processor load, to enter state.

Disk Usage Alarm % - Specifies the threshold, as a percentage of disk usage, to enter ALARM state.

Disk Usage Warning % - Specifies the threshold, as a percentage of disk usage, to enter WARNING state.

Memory Usage Alarm % - Specifies the threshold, as a percentage of memory usage, to enter ALARM state.

Memory Usage Warning % - Specifies the threshold, as a percentage of memory usage, to enter WARNING state.

One-minute Load Average Alarm - Specifies the one-minute load average value to enter ALARM state.

One-minute Load Average Warning - Specifies the one-minute load average value to enter WARNING state.

Five-minute Load Average Alarm - Specifies the five-minute load average value to enter ALARM state.

Five-minute Load Average Warning - Specifies the five-minute load average value to enter WARNING state.

Fifteen-minute Load Average Alarm - Specifies the fifteen-minute load average value to enter ALARM state.

Fifteen-minute Load Average Warning - Specifies the fifteen-minute load average value to enter WARNING state.

Ignore storage table indices After the device is polled, select the storage table entries you want to ignore. The selected entries do not cause alarms or warnings and are not be displayed in the Status window.

Filename: `com.dartware.snmp.hrmib`
Version: `1.13`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTP (Don't Match)

HTTP (Don't Match)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML. If the string is present, then the device goes to a warning state.

Host Name - the domain name of the web server (e.g. "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test. Only enter an IP address or domain name; do not add "http://".

URL Path - the full path of the desired file on the web server (e.g. "/index.html"). This can be empty to get to the root page of the site.

String to detect - a string NOT expected in HTTP server's response. If the string is present, the device goes to a Warning severity.

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

Filename: `com.dartware.tcp.http-nomatch.txt`
Version: `2.5`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTP (Follow Redirects)

HTTP (Follow Redirects)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML. This probe will follow a limited number of page redirects to the same HTTP server.

Parameters

Host Name - the domain name of the web server (Example: "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test. You must enter a valid Host Name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add "http://".

URL Path - the full path of the desired file on the web server (Example: "/index.html"). This can be empty to request the root page of the site.

String to verify - a string to verify in the HTTP server's response. For example, if you are retrieving a web page, you could search for "<HTML" or "<P>" to verify that the data is HTML. If the string is not found, the device goes into **Alarm**.

User ID - the user name typed into the web browser's password dialog. Leave this blank unless you want to test a web page that requires authentication.

Password - the password for the web browser's dialog. Leave this blank unless you want to test a web page that requires authentication.

Redirect Limit - the maximum number of redirects to follow.

Filename: com.dartware.tcp.http.follow
Version: 1.3

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTP (Post)

HTTP (Post)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you post form results to a specific web CGI and verify that the POST operation worked.

Parameters

Host Name - the domain name of the web server (e.g. "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test. Only enter an IP address or domain name; do not add "http://".

URL Path - the full path to the desired CGI on the web server (e.g. "/index.cgi"). This can be empty to get to the root page of the site.

Form Data - the encoded data sent in the body of the POST message.

String to verify - a string expected in HTTP server's response. For example, if you post form data that is designed to generate an error, you might search for "sorry" or "could not be processed" to verify that the CGI is properly rejecting the data. If this string is not found, the device goes into alarm.

Filename: com.dartware.tcp.http.cgi.post
Version: 2.8

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTP (Proxy)**HTTP (Proxy)**

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you test that a web server can be accessed using a remote proxy server as an intermediary. For example, this probe can check if your web server is accessible from some remote location on the Internet.

Parameters

Host Name - the domain name of the web server (example: "www.intermapper.com"). This is the host name part of the URL that you want to test.

Note: The host name is likely to be different from that of the actual device on the map. If the host name is not specified, the probe assumes it is included in the URL Path, and no adjustment to the path is made.

URL Path - the relative URI of the desired file on the web server (e.g. "/index.html"). This can be empty to get to the root page of the site. If Host Name is empty, this should contain the absolute URI.

Proxy User ID - your user ID for the proxy server. Leave this field blank if no authentication is required to use the proxy server.

Proxy Password - your password for the proxy server. Leave this field blank if no authentication is required to use the proxy server.

String to verify - a string expected in HTTP server's response. For example, if you are retrieving a web page, you might search for "<HTML" or "<P>" to verify that the data is HTML. If this string is not found, the device goes into alarm.

User Agent - the string that identifies this InterMapper client probe to the proxy web server. Some proxy servers block traffic at the proxy based on the User-Agent identity. This parameter lets you override InterMapper's default User-Agent setting. Leave this parameter blank to send a User-Agent string of "InterMapper/version", where version is the current version number of InterMapper.

Filename: `com.dartware.tcp.http.proxy`
Version: `2.12`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTP (Redirect)

HTTP (Redirect)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you test that a web server is redirecting certain URL's to a specific URL.

Parameters

Host Name - the domain name of the web server (e.g. "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test.

URL Path - the full path of the desired file on the web server (e.g. "/index.html"). This can be empty to get to the root page of the site.

Redirect URL - the complete URL that the given URL Path is redirected to. The URL should begin with "http://".

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter if you want to test a web page that requires authentication.

Filename: `com.dartware.tcp.http.redirect`
Version: `1.15`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTP

HTTP

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML.

Parameters

Host Name - the domain name of the web server (e.g. "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test. Only add an IP address or domain name; do not add "http://".

URL Path - the full path of the desired file on the web server (e.g. "/index.html"). This can be empty to get to the root page of the site.

String to verify - the string to verify in the data returned by the HTTP server. For example, if you are retrieving a web page, you might search for "<HTML" or "<P>" to verify that the data is HTML. If this string is not found, the device will go into alarm.

User ID - the user name typed into the web browser's password dialog. The default is to leave this blank. You should set this parameter if you want to test a web page that requires authentication.

Password - the password for the web browser's dialog. The default is to leave this blank. Set this parameter if you want to test a web page that requires authentication.

Filename: `com.dartware.tcp.http`
Version: `2.12`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTPS (Follow Redirects)

HTTPS (Follow Redirects)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTPS connections is port 443.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML. This probe will follow a limited number of page redirects to the same HTTPS server.

Parameters

*Host Name - the domain name of the web server (Example: "www.in-
termapper.com"). This can be derived from the host name part of the
URL that you want to test. You must enter a valid Host Name to test a
web server that implements a virtual host. Add only an IP address or
domain name; do not add "http://".*

*URL Path - the full path of the desired file on the web server (Example:
"/index.html"). This can be empty to get to the root page of the site.*

*String to verify - a string to verify in the server's response. For example,
if you are retrieving a web page, you could search for "<HTML" or "<P>"
to verify that the data is HTML. If the string is not found, the device goes
into **Alarm**.*

*User ID - the user name typed into the web browser's password dialog.
Set this parameter to test a web page that requires authentication.*

*Password - the password for the web browser's dialog. Set this para-
meter to test a web page that requires authentication.*

Redirect Limit - the maximum number of redirects to follow.

Filename: `com.dartware.tcp.https.follow`
Version: `1.2`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTPS (Post)

HTTPS (Post)

*The protocol used for secure transfer of web pages on the World Wide
Web. The default TCP port number for HTTPS connections is port 443.*

*This TCP probe lets you post form results to a specific web CGI over a
secure connection and verify that the POST operation worked.*

Parameters

*Host Name - the domain name of the web server (Example: "www.in-
termapper.com"). This can be derived from the host name part of the
URL that you want to test. You must enter a valid Host Name to test a
web server that implements a virtual host. Add only an IP address or
domain name; do not add "http://".*

*URL Path - the full path to the desired CGI on the web server (e.g. "/in-
dex.cgi"). This can be empty to get to the root page of the site.*

Form Data - the encoded data sent in the body of the POST message.

String to verify - a string to verify in the server's response. For example, if you post form data that is designed to generate an error response, you might search for "sorry" or "could not be processed" to verify that the CGI is properly rejecting the data. If the string is not found, the device goes into **Alarm**.

Note: The implementation of this probe uses OpenSSL on MacOSX.

Filename: com.dartware.tcp.https.cgi.post
Version: 1.14

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTPS (Redirect)

HTTPS (Redirect)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you test that a web server is redirecting certain URL's to a specific URL.

Parameters

Host Name - the domain name of the web server (Example: "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test. You must enter a valid Host Name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add "http://".

URL Path - the full path of the desired file on the web server (Example: "/index.html"). This can be empty to get to the root page of the site.

Redirect URL - the complete URL that the given URL Path is redirected to. The URL should begin with "https://".

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

Filename: com.dartware.tcp.https.redirect.txt
Version: 1.5

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTPS (SSLv3)

HTTPS (SSLv3)

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

This probe establishes a secure connection to a web server, downloads a specific web page, and scans it for a specific string of HTML. Unlike the default HTTPS probe, this probe does not attempt to auto-negotiate a TLSv1 connection, making it compatible with some older application servers.

This probe lets you establish a secure connection to a web server, download a specific web page, and scan it for a specific string of HTML. Unlike the default HTTPS probe, this probe will not attempt to auto-negotiate a TLSv1 connection, making it compatible with some older application servers.

Parameters

Host Name - the domain name of the web server (Example: "www.intermapper.com"). This can be derived from the host name part of the URL that you want to test. You must enter a valid Host Name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add "http://".

URL Path - the full path of the desired file on the web server (Example: "/index.html"). This can be empty to get to the root page of the site.

*String to verify - a string to verify in the server's response. For example, if you are retrieving a web page, you could search for "<HTML" or "<P>" to verify that the data is HTML. If the string is not found, the device goes into **Alarm**.*

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

Note: *The implementation of this probe uses OpenSSL on MacOSX.*

Filename: `com.dartware.tcp.https.notls.txt`
Version: `1.4`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTPS**HTTPS**

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

This probe establishes a secure connection to a web server, downloads a specific web page, and scans it for a specific string of HTML.

Host Name - the domain name of the web server (e.g. "www.in-termapper.com"). Use the host name part of the URL that you want to test. You must enter a valid "Host Name" to test web servers which implement virtual hosts.

URL Path - the full path of the desired file on the web server (e.g. "/index.html"). This can be empty to get to the root page of the site.

String to verify - a string expected in the HTTP server's response. For example, if you are retrieving a web page, you might search for "<HTML" or "<P>" to verify that the data is HTML. If this string is not found, the device goes into Alarm.

User ID - the login user name. Set this parameter to test a web page that requires authentication.

Password - the login password. Set this parameter to test a web page that requires authentication.

Filename: `com.dartware.tcp.https`
Version: `2.8`

[Back to Top](#)

Servers Standard > IPMI v2.0**IPMI v2.0**

This probe implements version 2.0 of the Intelligent Platform Management Interface (IPMI) over a LAN. It sends UDP-based RMCP+ packets to a Baseboard Management Controller (BMC) located within a server or workstation. The BMC is hardware which permits network-based management of the computer even when it is turned off, i.e. "lights-out management".

Parameters

User - required - An administrator-level user name to the BMC.

Password - required - The password for the specified user.

Dialect - The variant of the IPMI protocol. There are subtle differences in implementations of IPMI in various products.

- To use this probe with an Apple XServe 2008 or earlier, set the "Dialect" parameter to "XServe".
- For Dell Servers, the Apple XServe 2009, and any other product set the "Dialect" parameter to "Other".

This probe supports one-key, non-anonymous logins only. Internally, it uses RAKP-HMAC-SHA1 and AES-CBS-128 for authentication and confidentiality, respectively. The firewall configuration of the BMC must permit UDP packets from InterMapper.

Filename: `com.dartware.ipmi.txt`
Version: `1.2`

[Back to Top](#)

Servers Standard > IRC

IRC

This probe tests whether InterMapper can register a connection with an IRC server. This probe establishes a connection to the IRC server and issues the "PASS", "NICK", and "USER" commands. It verifies that the IRC server returns a particular string, in its welcome message, for example.

Password is the connection password. This parameter is passed using the "PASS" command.

Nickname gives the connection a nickname. This parameter is passed using the "NICK" command.

Username specifies the username, hostname, servername and realname of the new user. Typically, the hostname and servername are ignored for client connections. The realname must be prefixed with a ':'.

String to verify is a string to verify in the data returned by the IRC server. For example, you might check for a string returned in the IRC server's welcome message.

Filename: `com.dartware.tcp.irc`
Version: `1.6`

[Back to Top](#)

Servers Standard > LDAP > LDAP SSL

LDAP-SSL

The protocol used to access directories supporting the X.500 models, as described in [RFC 2251](#).

This probe connects to the LDAP server and binds using the designated Bind Name. If a Bind Password is provided, this password is sent as clear text to authenticate the probe.

Once logged in, the probe sends a SearchRequest for Field to Match searching for an equality match of Name to Lookup, and counts the number of LDAP records returned.

If the Search Base field is specified, this value is used as the base of the search. Otherwise, the Bind Name is used for the Base DN.

Filename: `com.dartware.tcp.ldap.ssl`
Version: `1.9`

[Back to Top](#)

Servers Standard > LDAP > LDAP

LDAP

The protocol used to access directories supporting the X.500 models, as described in [RFC 2251](#).

This probe connects to the LDAP server and binds using the designated Bind Name. If a Bind Password is provided, this password is sent as clear text to authenticate the probe.

Once logged in, the probe sends a SearchRequest for Field to Match searching for an equality match of Name to Lookup, and counts the number of LDAP records returned.

If the Search Base field is specified, this value is used as the base of the search. Otherwise, the Bind Name is used for the Base DN.

Filename: `com.dartware.tcp.ldap`
Version: `1.9`

[Back to Top](#)

Servers Standard > LPR

LPR

The print server protocol used to print over a TCP/IP network, as defined in [RFC 1179](#). The default TCP port number for LPR connections is port 515.

Filename: `com.dartware.tcp.lpr`
Version: `1.7`

[Back to Top](#)

Servers Standard > Mail > IMAP4 SSL

IMAP4-SSL

The protocol used for accessing and manipulating email messages on a server, as defined in [RFC 2060](#). This probe tests a secure connection to the IMAP server. The default TCP port number for secure IMAP connections is port 993.

This TCP script connects to the IMAP4 server and issues a CAPABILITY command, a NOOP command, and finally terminates with a LOGOUT command. The script checks the server's response to the CAPABILITY command to verify that the server supports IMAP4 or IMAP4rev1.

Filename: `com.dartware.tcp.imap4.ssl`
Version: `1.7`

[Back to Top](#)

Servers Standard > Mail > IMAP4

IMAP4

The protocol used for accessing and manipulating email messages on a server, as defined in [RFC 2060](#). The default TCP port number for IMAP4 connections is port 143.

This TCP script connects to the IMAP4 server and issues a CAPABILITY command, a NOOP command, and finally terminates with a LOGOUT command. The script checks the server's response to the CAPABILITY command to verify that the server supports IMAP4 or IMAP4rev1.

Filename: `com.dartware.tcp.imap4`
Version: `1.7`

[Back to Top](#)

Servers Standard > Mail > POP3 SSL

POP3-SSL

The protocol used to access email messages from a central maildrop server, as defined in [RFC 1939](#). The default TCP port number for POP3-SSL connections is port 995.

If the "User Name" parameter is left empty, this probe verifies that the server send "+OK" as its initial greeting, then immediately sends the QUIT command.

Parameters

User Name - if left empty, the probe verifies that the server sends "+OK" as its initial greeting, then immediately sends the QUIT

*command. If specified, the probe attempts to use the specified Password to login to the POP3 server. If the login fails , the device is set to **Warning**.*

*Use APOP if supported - By default, the probe uses the APOP command to authenticate the user if the server supports it. To authenticate via USER and PASS commands for a particular user, set this parameter to **False**.*

Note: *If APOP is not supported by the server, the Use APOP if supported option has no effect.*

Filename: `com.dartware.tcp.pop3.ssl`
Version: `2.7`

[Back to Top](#)

Servers Standard > Mail > POP3

POP3

The protocol used to access email messages from a central maildrop server, as defined in [RFC 1939](#). The default TCP port number for POP3 connections is port 110.

If the "User Name" parameter is left empty, this probe verifies that the server send "+OK" as its initial greeting, then immediately sends the QUIT command.

If a "User Name" parameter is specified, this probe will attempt login to the POP3 server using the specified password. If the probe fails to authenticate, the device will be marked in "warning".

By default, this probe will use the APOP command to authenticate the user if the the APOP command is supported by the server. To authenticate via USER and PASS commands for a particular user, set the "Use APOP if supported" parameter to False.

- The "Use APOP if supported" option has no effect if APOP is not supported by the server.*

Filename: `com.dartware.tcp.pop3`
Version: `2.6`

[Back to Top](#)

Servers Standard > Mail > Roundtrip IMAP

Roundtrip-IMAP

This probe tests an IMAP server and measures the time it takes to send a message (via SMTP) and retrieve it (via IMAP). It sends a short message to the specified SMTP server, and continually attempts to retrieve the

message via IMAP from the device being tested. The probe alerts if the server fails to respond properly or the round-trip time exceeds the specified timeout.

Parameters

SMTP Server - The server to receive the SMTP message. If left blank, the device being tested is used as the target.

SMTP User and SMTP Password - optional - The user name and password to be used when sending the message. Leave blank if not required.

Email To - The e-mail address to which the message is sent.

Email From - The From: address in the message.

IMAP User and IMAP Password - The user name and password used to log into the IMAP server to retrieve the message.

Timeout - Measured in seconds.

Filename: `com.dartware.email.imap.txt`
Version: `1.4`

[Back to Top](#)

Servers Standard > Mail > Roundtrip POP

Roundtrip-POP

This probe tests a POP server and measures the time it takes to send a message (via SMTP) and retrieve it (via POP). It sends a short message to the specified SMTP server, and continually attempts to retrieve the message via POP from the device being tested. The probe alerts if the server fails to respond properly or the round-trip time exceeds the specified timeout.

Parameters

SMTP Server - The server to receive the SMTP message. If left blank, the device being tested is used as the target..

SMTP User and SMTP Password - optional - The user name and password to be used for sending the message. Leave blank if not required.

Email To - The e-mail address to which the message is sent.

Email From - The From: address in the message.

POP User and POP Password - The user name and password used to log into the POP server to retrieve the message.

Timeout - Measured in seconds.

Filename: `com.dartware.email.pop.txt`
Version: `1.4`

[Back to Top](#)

Servers Standard > Mail > SMTP TLS

SMTP-TLS

The standard protocol used to transfer electronic mail on the Internet, as defined in [RFC 821](#). This probe tests a secure connection to the SMTP server. The default TCP port number for secure SMTP connections is port 25.

This probe tries to verify that a specified email address exists on the SMTP server, using the VRFY command. It connects to the SMTP server, introduces itself using the HELO command, then issues a VRFY command for the specified email address. When it has received a response, the script sends the QUIT command before closing its connection to the server.

Email Address is the name or email address that we are attempting to verify.

Filename: `com.dartware.tcp.smtp.tls`
Version: `1.8`

[Back to Top](#)

Servers Standard > Mail > SMTP

SMTP

The standard protocol used to transfer electronic mail on the Internet, as defined in [RFC 821](#). The default TCP port number for SMTP connections is port 25.

This probe tries to verify that a specified email address exists on the SMTP server, using the VRFY command. It connects to the SMTP server, introduces itself using the HELO command, then issues a VRFY command for the specified email address. When it has received a response, the script sends the QUIT command before closing its connection to the server.

Email Address is the name or email address that we are attempting to verify.

Filename: `com.dartware.tcp.smtp`
Version: `2.0`

[Back to Top](#)

Servers Standard > Multimedia > Multicast Listener

Multicast Listener

This probe lets you listen for UDP packets directed to a specific UDP port. If you specify a multicast IP address, InterMapper will listen for packets directed to that multicast address. This probe will change the device status to the DOWN if a packet isn't received within specified number of seconds (the default is 10 seconds).

The Multicast Listener probe can be used to verify that a multicast source is broadcasting, for example, a live QuickTime broadcaster.

This probe does not inject any traffic into the network; it is passive only.

Multicast IP Address is the optional multicast IP address to listen on.

Seconds to wait is the maximum number of seconds to wait between packets. If a packet is not received within the specified number of seconds, the device's status is set to DOWN. The "Seconds to wait" timer is reset every time a packet is received.

Verify Source Address lets you specify whether the probe should only count packets from the IP address of the targeted device.

Filename: `com.dartware.udplistener`
Version: `2.0`

[Back to Top](#)

Servers Standard > Multimedia > RTSP

RTSP

The protocol used to control real-time streams, defined in [RFC 2326](#) and [RFC 1889](#). The default TCP port number for RTSP connections is port 554.

This TCP probe lets you check that the server is up and responding.

*The specifics of the commands that the probe must send to the server vary somewhat depending upon the version of RFC2326 that the server implements. If the server you're monitoring implements RFC2326bis-02 or later, then set **RFC2326bis-02 or later** to "Yes". If you're not sure, leave it set to "No". If the device goes into warning with the reason set to "[RTSP] Unexpected response to PLAY command. (RTSP/1.0 460 Only Aggregate Option Allowed)", then set it to "Yes".*

Filename: `com.dartware.tcp.rtsp`
Version: `2.1`

[Back to Top](#)

Servers Standard > Network Time

Network Time

The protocol used to synchronize time between computers, defined in [RFC 1119](#).

This probe sends a client-mode current-time request to the NTP server. By default, NTP requests are sent to UDP port 123.

Filename: `com.dartware.ntp`
Version: `1.5`

[Back to Top](#)

Servers Standard > NNTP

NNTP

The protocol used to read network news on TCP/IP Internets, as defined in [RFC 977](#). The default TCP port number for NNTP connections is port 119.

This script connects to the news server and uses the GROUP command to ask for information about a specific newsgroup name. The script then issues the QUIT command to tell the server it is closing the connection.

Newsgroup is the name of the newsgroup that you want to verify.

Filename: `com.dartware.tcp.nntp`
Version: `1.6`

[Back to Top](#)

Servers Standard > RADIUS

RADIUS

The protocol used by remote access servers to authenticate dial-in users, as defined in [RFC 2138](#). This probe tests a RADIUS server by sending an Access-Request packet to authenticate a specific user name and password. Before you can use this probe with a particular RADIUS server, you must add the InterMapper computer's IP address to the RADIUS server and choose a "shared secret" for it. The "shared secret" is used by the RADIUS protocol to encrypt passwords in RADIUS requests. A RADIUS server does not answer access-requests from a client it doesn't recognize.

The official port number for RADIUS is 1812. Some RADIUS servers, however, use port number 1645 for historical reasons.

Shared Secret - InterMapper's unique password into the RADIUS server. Since it is used for authentication, the same value must be configured in the RADIUS server as well.

User Name - The user name to be used for InterMapper's authentication.

Password - The password for the specified user name. The password is not sent in the clear; it is encrypted using the shared secret.

Filename: `com.dartware.radius`
Version: `1.8`

[Back to Top](#)

Servers Standard > SIP over UDP

SIP over UDP

The protocol used to set up voice communications for Voice-over-IP (VOIP), as described in [RFC 3261](#). This probe sends a SIP request in a single UDP packet and checks for a valid SIP response.

By default, this probe sends an OPTIONS command to the target device. However, some VOIP systems do not answer un-authenticated OPTIONS requests. For these devices, change the command to REGISTER.

Parameters

URI - The SIP uniform resource identifier in the request.

Command - The SIP command to send in the request.

Filename: `com.dartware.sip.txt`
Version: `1.1`

[Back to Top](#)

Servers Standard > SNPP

SNPP

This protocol transfers pager information across the Internet, as defined in [RFC 1861](#). The default TCP port number for SMTP connections is port 444.

This SNPP probe verifies that an SNPP server is working by connecting to it and issuing a PAGE <pagerid> command. If it receives a valid response code, the probe issues a QUIT command and exits, setting device status to **OK**.

If an "Invalid Pager ID" response is received, the probe issues a QUIT command and exits, setting device status to **Alarm**.

*If no connection was made, or if an unexpected response is received, device status is set to **Down**.*

Parameters

PagerID - your Pager ID on the specified SNPP server.

Filename: `com.dartware.tcp.snpp`
Version: `1.6`

[Back to Top](#)

Servers Standard > SSH**SSH**

The protocol used for secure remote login. The default TCP port number for SSH connections is port 22.

This probe opens a TCP connection to the specified port and looks for the identification string that indicates an SSH server as specified in [RFC 4253](#).

Parameters

*Require SSH 2.0 - If set to **true** and the server doesn't require SSH 2.0, the device is set to **Alarm**.*

Filename: `com.dartware.tcp.ssh.txt`
Version: `1.4`

[Back to Top](#)

Servers Standard > Subversion > SVN (Apache)**SVN (Apache)**

This probe tests a Subversion server running as an Apache module. The subversion module lets Apache function as a WebDAV/DeltaV server. Since the server responds normally to HTTP GET requests, testing whether it is up is the same as performing an HTTP GET request and checking to ensure the location was found.

Parameters

Host Name - the domain name of the subversion server (e.g. "svn.-collab.net"). Include only the IP address or domain name; do not include "http://".

URL Path - the path to the repository. The first and last characters must be a '/'.

User ID - the user name used for authentication by the subversion server, if required.

Password - the password used for authentication by the subversion server, if required.

Subversion is a version control system intended as a replacement for CVS. The software is released under an Apache/BSD style open-source license. The project can be found at <http://subversion.tigris.org>.

Filename: `com.dartware.tcp.svn.apache`
Version: `1.1`

[Back to Top](#)

Servers Standard > Subversion > SVN (Svnserve)

SVN (Svnserve)

This probe tests a stand-alone svnserve Subversion server. It connects to the svnserve using its default port 3690. The server returns a response to indicate it is running. If a repository location is specified, the probe then tries to connect to that repository. If a username is specified, the probe tries to authenticate using CRAM-MD5, otherwise it connects anonymously.

Parameters

Repository - the subversion repository path (e.g. "svn/experimental"). It should not begin with a '/'.

User ID - the user name used for authentication by the subversion server, if required.

Password - the password used for authentication by the subversion server, if required.

Subversion is a version control system intended as a replacement for CVS. The software is released under an Apache/BSD style open-source license. The project can be found at <http://subversion.tigris.org>.

A description of the custom protocol used by svnserve can be found at http://svn.collab.net/repos/svn/trunk/subversion/libsvn_ra_svn/-protocol.

Filename: `com.dartware.tcp.svn.svnserve`
Version: `1.1`

[Back to Top](#)

Servers Standard > Telnet

Telnet

The protocol used for terminal-to-terminal communication and distributed computation as described in [RFC 854](#). The default TCP port number for Telnet connections is port 23.

This probe lets you Telnet to a device, login with a name and password, and optionally enter a command. This probe is specifically designed to reject any Telnet options proffered by the Telnet server; the TCP connection always remains in the base "network virtual terminal" state. This probe lets you enter data at up to three prompts.

Intro String to Match is a string to match in the welcome banner sent by the Telnet server when you first connect. Leave this parameter blank if you want to match anything in the welcome banner.

First Prompt is the string to match in the first prompt. (e.g. "Login:")

Reply #1 is your reply to the first prompt. (i.e. your response to the "Login:" prompt)

Second Prompt is the string to match in the second prompt. (e.g. "Password:") If this parameter is empty, the probe ignores the prompt string and it does not send its reply.

Reply #2 is your reply to the second prompt. (i.e. your response to the "Password:" prompt.)

Third Prompt is the string to match in the third prompt. If this parameter is empty, the probe ignores the prompt string and its reply.

Reply #3 is your reply to the third prompt.

Filename: `com.dartware.tcp.telnet`
Version: `1.7`

[Back to Top](#)

Servers Standard > VNC Server

VNC Server

Attempt to connect to a VNC Server. VNC uses RFB (Remote Frame Buffer) protocol for communication between clients and server. The probe waits to receive a "RFB ###.###" string. If it arrives, the VNC server is assumed to be up and the probe simply disconnects.

The Virtual Network Computer (VNC) protocol was originally designed at AT&T Labs in Cambridge. There are many implementations: the developers now support it from the RealVNC site at <http://www.realvnc.com/>.

Filename: `com.dartware.tcp.vnc`
Version: `1.7`

[Back to Top](#)

WMI

- [WMI > WMI CPU Utilization \(Pg 536\)](#)
- [WMI > WMI Disk Available \(Pg 537\)](#)
- [WMI > WMI Disk Fragmentation Analysis \(Pg 537\)](#)
- [WMI > WMI Event Log \(Pg 538\)](#)
- [WMI > WMI File Check \(Pg 539\)](#)
- [WMI > WMI Folder Check \(Pg 540\)](#)
- [WMI > WMI Free Memory \(Pg 540\)](#)
- [WMI > WMI Installed Software \(Pg 541\)](#)
- [WMI > WMI Logged on Users \(Pg 542\)](#)
- [WMI > WMI MExchange 2007 Hub Transport Server \(Pg 542\)](#)
- [WMI > WMI MExchange 2007 Mailbox Server \(Pg 543\)](#)
- [WMI > WMI Network Utilization \(Pg 543\)](#)
- [WMI > WMI Process Monitor \(Pg 544\)](#)
- [WMI > WMI Service Monitor \(Pg 545\)](#)
- [WMI > WMI SQL Server 2008 Service Monitor \(Pg 545\)](#)
- [WMI > WMI System Accessibility \(Pg 546\)](#)
- [WMI > WMI System Information \(Pg 547\)](#)
- [WMI > WMI Top Processes \(Pg 547\)](#)

[To Probe Index \(Pg 442\)](#)

WMI > WMI CPU Utilization

WMI CPU Utilization

This probe uses WMI to retrieve the percentage of time that a processor uses to execute a non-idle thread on the target host. Specifically, it queries the PercentProcessorTime property of the Win32_PerfFormattedData_PerfOS_Processor class and compares it against the Warning and Critical parameters you set.

The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

Single Warning, Single Critical, Total Warning, and Total Critical - the device's condition is set by comparing each processor against the specified Single percentages, and the total CPU utilization against the specified Total percentages. You can leave any of these values blank.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `cpu_util.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the

device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.cpu_utilization.txt`
Version: `1.11`

[Back to Top](#)

WMI > WMI Disk Available

WMI Disk Available

This probe uses WMI to determine the disk space available on the specified drive(s) on the target host. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the specified values. The target host must be running Windows 2000 or later.

Parameters

Drive - May be set to "All" to check disk space on all of the host machine's local hard drives. Enter a list of comma-separated drive names (including the colon). These drives will be listed regardless of whether they are local hard drives. Zero-sized drives, such as an empty cd-rom, are not listed. The first drive with space that is less than the specified values is cited in the reason.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

InterMapper invokes the `disk_avail.vbs` companion script included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.disk_available.txt`
Version: `1.10`

[Back to Top](#)

WMI > WMI Disk Fragmentation Analysis

WMI Disk Fragmentation Analysis

*This probe uses WMI to analyze disk fragmentation on a drive on the target host. Specifically, it calls the DefragAnalysis method of the Win32_Volume class and reports pertinent statistics from the analysis. If the drive needs to be defragmented, the device is set to **Warning**. The target host must be running Windows Vista, Windows Server 2003 or later.*

Parameters

Drive - the drive letter assigned to the local disk to be analyzed, including the colon but without backslashes.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `defrag_analysis.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.defrag_analysis.txt`
Version: 1.10

[Back to Top](#)

WMI > WMI Event Log

WMI Event Log

This probe uses WMI to retrieve entries from the Event Logs on the target host. Specifically, it queries the Win32_NTLogEvent class, limiting the search with the parameters you set. If matching events are found, a critical status is returned. The target host must be running Windows 2000 or later.

Parameters

Log File - contains a comma-separated list of the logs to be searched. At least one Log File is required.

Event Codes - a comma-separated list of event codes to search. To select all codes, leave this parameter blank.

Event Types - a comma-separated list; can include event type names or corresponding numerical values. Names and values can be intermixed. Limits the selection to events of the specified types.

Hours, Minutes, and Seconds - combine to define how far back in the event log to search. The specified values are subtracted from the current time and used to select events, based on when they were written to the log.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `event_log.vbs` companion script included with this probe.

Filename: `com.dartware.wmi.event_log.txt`
Version: `1.12`

[Back to Top](#)

WMI > WMI File Check

WMI File Check

This probe uses WMI to retrieve information about files on the target host. Specifically, it queries the `CIM_DataFile` class, limiting the search with the parameters you set. The target host must be running Windows 2000 or later.

Parameters

Path - the location of the files to be checked. Include the drive, and enclose the path in double-quotes if it contains spaces.

File - the filename and extension of the file you wish to check. The path is prepended to filename during the final query. To check all files that met the specified Size or time criteria, leave this parameter blank. You may also use a list of comma-separated filenames.

Wildcards (?)* may be used in the filename. When using wildcards, be sure to specify the *Path* parameter. Otherwise, the query could take an inordinate amount of time. At least one of *File* or *Path* must be set.

Size - the minimum filesize in bytes. Any file larger than this value is listed.

Hours, Minutes and Seconds - specify how recently the file was changed in order to be listed, based on the file's `LastModified` value. At least one of these parameters must be set.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is `localhost`), leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `file_chk.vbs` companion script, included with the probe. It lists the files which meet the specified criteria, and uses the exit value to set the condition of the device.

Filename: `com.dartware.wmi.file_check.txt`
Version: `1.10`

[Back to Top](#)

WMI > WMI Folder Check

WMI Folder Check

This probe uses WMI to retrieve information about a folder on the target host. Specifically, it queries the Win32_Directory and CIM_DataFile classes to walk the directory tree, accumulating file and folder counts and the total of file sizes. It also notes the most recently modified file in the tree. The target host must be running Windows 2000 or later.

Parameters

Path - specifies the folder at the top of the tree you want to check. It should include the drive, and should be enclosed in double-quotes if it contains spaces.

Warning and Critical - set thresholds for the number of folders, the number of files, and the total of the file sizes.

User - may be a local user on the target host, or can take the form domain\user for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the folder_chk.vbs companion script, included with the probe. The script compares the number of files, folders, and the total size against your criteria to set the condition of the device.

Filename: com.dartware.wmi.folder_check.txt
Version: 1.12

[Back to Top](#)

WMI > WMI Free Memory

WMI Free Memory

This probe uses WMI to retrieve the amount of physical memory available to processes running on the target host, in megabytes. Specifically, it queries the TotalPhysicalMemory property of the Win32_ComputerSystem class. It also queries the FreePhysicalMemory property of the Win32_OperatingSystem class and compares it against specified thresholds. The target host must be running Windows 2000 or later.

Parameters

Warning and Critical - specify thresholds in megabytes for which the device condition is set to the specified state.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `free_mem.vbs` companion script, included with the probe. The script uses the `exit` value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.free_memory.txt`
Version: 1.9

[Back to Top](#)

WMI > WMI Installed Software

WMI Installed Software

This probe uses WMI to retrieve information about software installed on the target host. Specifically, it queries the Win32_Product class for information about products installed using Windows Installer. It also queries Win32_OperatingSystem and displays the operating system name, version and service pack level.

The target host must be running Windows XP, Windows Server 2003 or later. On Windows Server 2003, the Win32_Product class isn't always installed by default. You can install the "WMI Windows Installer Provider" component under "Management and Monitoring Tools" in "Add/Remove Windows Components".

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `installed_software.vbs` companion script included with this probe.

Filename: `com.dartware.wmi.installed_software.txt`
Version: 1.6

[Back to Top](#)

WMI > WMI Logged on Users

WMI Logged-on Users

This probe uses WMI to retrieve information about users logged on to the target host. Specifically, it queries the LogonType and StartTime properties of the Win32_LogonSession class, limiting the selection to those in the comma-separated list of numeric Logon Types you set in the Type parameter. It queries instances of the Win32_LoggedOnUser class, matches the LogonID and extracts the user's name and domain from the path of the Win32_Account. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `log_users.vbs` companion script, included with this probe.

Filename: `com.dartware.wmi.logged-on_users.txt`
Version: `1.12`

[Back to Top](#)

WMI > WMI MExchange 2007 Hub Transport Server

WMI MExchange 2007 Hub Transport Server

This probe uses WMI to retrieve performance information about the delivery queues on a MS Exchange 2007 Hub Transport Server. Specifically, it queries the Win32_PerfFormattedData_MSExchangeTransportQueues_MSExchangeTransportQueues class to collect a variety of queue statistics and then compares them to the criteria you set. The default criteria for warning and critical conditions are taken from the Microsoft TechNet article [Monitoring Hub Transport Servers](#).

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `ex07_transport.vbs` companion script included with this probe. It uses the exit value to set the condition of the device.

Filename: `com.dartware.wmi.ex07_transport_server.txt`
Version: 1.5

[Back to Top](#)

WMI > WMI MExchange 2007 Mailbox Server

WMI MExchange 2007 Mailbox Server

This probe uses WMI to retrieve performance information about the delivery queues on a MS Exchange 2007 Mailbox Server. Specifically, it queries the `Win32_PerfFormattedData_MExchangeIS_MExchangeIS`, `Win32_PerfFormattedData_MExchangeIS_MExchangeISMailbox`, `Win32_PerfFormattedData_MExchangeIS_MExchangeISPublic`, `Win32_PerfFormattedData_MExchangeSearchIndices_MExchangeSearchIndices` classes to collect a variety of statistics and then compares them to the criteria you set. The default criteria for warning and critical conditions are taken from the Microsoft TechNet article [Monitoring Mailbox Servers](#).

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `ex07_mailbox.vbs` companion script included with this probe. It uses the script's exit value to set the condition of the device.

Filename: `com.dartware.wmi.ex07_mailbox_server.txt`
Version: 1.5

[Back to Top](#)

WMI > WMI Network Utilization

WMI Network Utilization

This probe uses WMI to retrieve the network utilization on an interface on the target host. Specifically, it queries the `BytesTotalPersec`, `CurrentBandwidth`, `OutputQueueLength` and `PacketsReceivedErrors` properties of the `Win32_PerfFormattedData_Tcpip_NetworkInterface` class. It compares `OutputQueueLength` against the Warning and Critical para-

meters you set. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

The interface may be selected by IP Address, MAC Address, or Index. When specifying a MAC address, use colons, hyphens or no separators. The interface name is queried from the Win32_NetworkAdapterConfiguration class and used to query data from the Win32_PerfFormattedData_Tcpip_NetworkInterface class.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `net_util.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.net_utilization.txt`
Version: 1.11

[Back to Top](#)

WMI > WMI Process Monitor

WMI Process Monitor

This probe uses WMI to retrieve information about processes running on the target host. Specifically, it queries the `PercentProcessorTime` property of the `Win32_PerfFormattedData_PerfProc_Process` class and compares it against the specified parameters. Any of the specified processes not found are listed, and the status is set to Critical. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

Process - a comma-separated list of process names to check. Extensions are not included in the process names. Names containing spaces or other special characters should be enclosed in quotes. If more than one process matches the name, all matching processes are listed.

Warning and Critical - specify thresholds (in percent) for which the device condition is set to the specified state.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `proc_mon.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It also uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.process_monitor.txt`
Version: `1.12`

[Back to Top](#)

WMI > WMI Service Monitor

WMI Service Monitor

This probe uses WMI to retrieve the state of services running on the target host by querying the `Win32_Service` class. Any specified services not found are listed, and the status is set to Critical. The target host must be running Windows 2000 or later.

Parameters

Service - a comma-separated list of service names to be checked.

Note: *Service names should not be confused with the service's Display Name, shown in the Services tool. Check the Properties for the service to find the actual service name. Names containing spaces or other special characters should be enclosed in quotes.*

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `serv_mon.vbs` companion script, included with the probe. The script's exit value is used to set the condition of the device.

Filename: `com.dartware.wmi.service_monitor.txt`
Version: `1.13`

[Back to Top](#)

WMI > WMI SQL Server 2008 Service Monitor

WMI SQL Server 2008 Service Monitor

This probe uses WMI to retrieve the state of Microsoft SQL Server 2008 services running on the target host by querying the `Win32_Service` class.

The states of the selected services are listed, and if any are not running, the status of the device is set to Critical. The target host must be running Windows 2000 or later.

Parameters

Services - select or clear checkboxes to select the services which you want to monitor.

Instance - the SQL Server instance you wish to monitor on the target host. To monitor the default instance, leave this parameter blank.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `sql2k8_serv_mon.vbs` companion script, included with this probe. It uses the script's exit value to set the condition of the device.

<i>Filename:</i> <code>com.dartware.wmi.sql2k8_service_monitor.txt</code> <i>Version:</i> 1.5
--

[Back to Top](#)

WMI > WMI System Accessibility

WMI System Accessibility

This probe uses WMI to test accessibility of a target device from the monitored host. Specifically, it uses the `Win32_PingStatus` class to test the connectivity and returns a chartable response time. If the target cannot be pinged, the status is set to critical and a discontinuity is inserted in the chart data. The target host must be running Windows XP, Windows Server 2003 or later.

Additional information about the monitored host is queried from the `Win32_NetworkAdapterConfiguration` and `Win32_NTDomain` classes and displayed in the status window.

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `sys_access.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It also uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.system_accessibility.txt`
Version: `1.10`

[Back to Top](#)

WMI > WMI System Information

WMI System Information

This probe uses WMI to collect a variety of information about the monitored host including hardware and operating system details. The target host must be running Windows 2000 or later.

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `system_info.vbs` companion script, included with the probe.

Filename: `com.dartware.wmi.system_infomation.txt`
Version: `1.9`

[Back to Top](#)

WMI > WMI Top Processes

WMI Top Processes

This probe uses WMI to retrieve information about CPU utilization and processes running on the target host. Specifically, it queries the `PercentProcessorTime` property of the `Win32_PerfFormattedData_PerfOS_Processor` class and compares it against the specified thresholds. It queries the `PercentProcessorTime` property of the `Win32_PerfFormattedData_PerfProc_Process` class and lists up to five processes using the most CPU time. Because there is a time lapse between collecting the CPU data and the process data, the reported values do not add up exactly. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

Warning and Critical - set a value in percent to use as the threshold to set the device to this condition.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

InterMapper invokes the `top_cpu.vbs` companion script, included with the probe. The probe uses script's the exit value to set the condition of the device. It also uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.top_process.txt`
Version: `1.11`

[Back to Top](#)

Wireless

- [Wireless > Alvarion > Alvarion B 14 & B 28 \(BU\) \(Pg 550\)](#)
- [Wireless > Alvarion > Alvarion B 14 & B 28 \(RB\) \(Pg 551\)](#)
- [Wireless > Alvarion > BreezeACCESS \(AU\) \(Pg 551\)](#)
- [Wireless > Alvarion > BreezeACCESS \(SU\) \(Pg 552\)](#)
- [Wireless > Alvarion > BreezeACCESS LB \(Pg 552\)](#)
- [Wireless > Alvarion > BreezeACCESS VL \(AU\) \(Pg 553\)](#)
- [Wireless > Alvarion > BreezeACCESS VL \(SU\) \(Pg 553\)](#)
- [Wireless > Atmel > Atmel AT76C510 \(Pg 554\)](#)
- [Wireless > Basic > IEEE 802.11 \(Pg 555\)](#)
- [Wireless > Basic > SNMP for Wireless \(Pg 555\)](#)
- [Wireless > Canopy > Canopy \(AP\) \(Pg 555\)](#)
- [Wireless > Canopy > Canopy \(SM\) \(Pg 556\)](#)
- [Wireless > Canopy > Canopy Backhaul \(45 Mbps/FW 5830\) \(Pg 557\)](#)
- [Wireless > Canopy > Canopy Backhaul \(60 Mbp/FW 5840\) \(Pg 557\)](#)
- [Wireless > Canopy > Canopy Backhaul \(Master\) \(Pg 558\)](#)
- [Wireless > Canopy > Canopy Backhaul \(Slave\) \(Pg 558\)](#)
- [Wireless > Canopy > Canopy CMM Micro \(Pg 559\)](#)
- [Wireless > CB3 > CB3 Bridge \(Pg 559\)](#)
- [Wireless > CB3 > CB3 Deluxe Bridge \(Pg 559\)](#)
- [Wireless > Inscape Data > AirEther AB54 Series AP \(AP Mode\) \(Pg 560\)](#)
- [Wireless > Inscape Data > AirEther AB54 Series AP \(Bridge Mode\) \(Pg 560\)](#)
- [Wireless > Inscape Data > AirEther AB54 Series AP \(Client Mode\) \(Pg 561\)](#)
- [Wireless > Inscape Data > AirEther AB54 Series AP \(Repeater Mode\) \(Pg 561\)](#)
- [Wireless > Inscape Data > AirEther CB54 Series Client \(Pg 562\)](#)
- [Wireless > MikroTik > MT Radio Uplink \(Pg 562\)](#)
- [Wireless > MikroTik > MT Routerboard \(Pg 563\)](#)
- [Wireless > MikroTik > MT Software Only \(Pg 564\)](#)
- [Wireless > MikroTik > WDS Bridge \(Pg 564\)](#)
- [Wireless > Motorola > PTP 400 Series Bridge \(Pg 565\)](#)
- [Wireless > Motorola > PTP 600 Series Bridge \(Pg 566\)](#)
- [Wireless > Orthogon > Gemini \(Pg 566\)](#)
- [Wireless > Orthogon > Spectra \(Pg 567\)](#)
- [Wireless > Other > HTTP \(Pg 567\)](#)
- [Wireless > Proxim > Proxim AP 2000 \(Pg 568\)](#)
- [Wireless > Proxim > Proxim AP 4000 \(Pg 569\)](#)
- [Wireless > Proxim > Proxim AP 600 \(Pg 569\)](#)
- [Wireless > Proxim > Proxim AP 700 \(Pg 570\)](#)
- [Wireless > Proxim > Proxim LAN Access Point \(Pg 570\)](#)
- [Wireless > Proxim > Tsunami GX \(Pg 571\)](#)
- [Wireless > Proxim > Tsunami MP.11 BSU \(Pg 572\)](#)
- [Wireless > Proxim > Tsunami MP.11 SU \(Pg 572\)](#)
- [Wireless > Redline > AN50 \(Pg 573\)](#)
- [Wireless > smartBridges > airBridge \(Pg 574\)](#)
- [Wireless > smartBridges > airClient Nexus PRO total \(Pg 574\)](#)
- [Wireless > smartBridges > airClient Nexus \(Pg 575\)](#)
- [Wireless > smartBridges > airHaul Nexus PRO total \(Pg 575\)](#)
- [Wireless > smartBridges > airHaul Nexus \(Pg 576\)](#)
- [Wireless > smartBridges > airHaul2 Nexus PRO \(Pg 577\)](#)
- [Wireless > smartBridges > airPoint Nexus PRO total \(Pg 577\)](#)

- [Wireless > smartBridges > airPoint Nexus \(Pg 578\)](#)
- [Wireless > smartBridges > airPoint \(Pg 578\)](#)
- [Wireless > smartBridges > airPoint2 Nexus PRO \(Pg 579\)](#)
- [Wireless > Trango > Trango M2400S \(AP\) \(Pg 580\)](#)
- [Wireless > Trango > Trango M5800S \(Pg 580\)](#)
- [Wireless > Trango > Trango M5830S \(SU\) \(Pg 581\)](#)
- [Wireless > Trango > Trango M5830S \(Pg 581\)](#)
- [Wireless > Trango > Trango M900S \(AP\) \(Pg 582\)](#)
- [Wireless > Trango > Trango P5830S \(master\) \(Pg 583\)](#)
- [Wireless > Trango > Trango P5830S \(remote\) \(Pg 583\)](#)
- [Wireless > Tranzeo > Sixth Generation AP \(Pg 584\)](#)
- [Wireless > Tranzeo > Sixth Generation CPE \(Pg 584\)](#)
- [Wireless > Tranzeo > Sixth Generation PxP \(Pg 585\)](#)
- [Wireless > Tranzeo > Tranzeo \(AP\) \(Pg 585\)](#)
- [Wireless > Tranzeo > Tranzeo \(PXP\) \(Pg 586\)](#)
- [Wireless > Tranzeo > Tranzeo \(SAI\) \(Pg 587\)](#)
- [Wireless > Tranzeo > Tranzeo 58XX Series Backhaul \(Pg 587\)](#)
- [Wireless > Tranzeo > Tranzeo AP 5A \(44R\) \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo AP 5A \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo Classic \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 200 \(1.77.R\) \(Pg 588\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 200 \(Pg 589\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 5A \(44R\) \(Pg 589\)](#)
- [Wireless > Tranzeo > Tranzeo CPE 5A \(Pg 590\)](#)
- [Wireless > Tranzeo > Tranzeo TR CPE \(Pg 590\)](#)
- [Wireless > WaveRider > CCU \(Pg 590\)](#)
- [Wireless > WaveRider > EUM \(Pg 591\)](#)

[To Probe Index \(Pg 442\)](#)

Wireless > Alvarion > Alvarion B 14 & B 28 (BU)

Alvarion B-14 & B-28 (BU)

This probe monitors an [Alvarion](#) B-14 or B-28 base unit (BU). It retrieves and displays the radio band, operating frequency, and slave association. It will go into an alarm when no slave is associated, and when the operating frequency doesn't match the configured frequency. Traffic information is available for the ethernet and radio interfaces. (To show the ethernet interface, we recommend using the "Display unnumbered interfaces" behavior.)

Parameters

None.

<p>Filename: <code>com.dartware.wrls.alvarion.b14.master.txt</code> Version: <code>0.5</code></p>

[Back to Top](#)

Wireless > Alvarion > Alvarion B 14 & B 28 (RB)

Alvarion B-14 & B-28 (RB)

This probe monitors an [Alvarion](#) B-14 or B-28 remote bridge (RB) unit. It retrieves and displays the radio band, operating frequency, average received signal to noise ratio, and the MAC address of the associated base unit (BU). It will go into alarm or warning states based on user-defined parameters for a low signal to noise ratio or high traffic on a specified interface.

Parameters

Avg Receive SNR too low alarm, Avg Receive SNR low warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

High Traffic Interface Number - enter the number of the interface for which you want to monitor traffic.

Filename: `com.dartware.wrls.alvarion.b14.slave.txt`
Version: `0.5`

[Back to Top](#)

Wireless > Alvarion > BreezeACCESS (AU)

BreezeACCESS (AU)

This probe monitors a BreezeCom or [Alvarion](#) BreezeACCESS 2.4 Ghz or 900 MHz access unit (AU). It retrieves and displays the operating radio band of the unit, and the number of client associations since the last reset. Traffic information is available for the ethernet and radio interfaces. (To show the ethernet interface, we recommend using the "Display unnumbered interfaces" behavior.)

Parameters

Retransmitted Fragments too high alarm, Retransmitted Fragments high warning,

Dropped Frames too high alarm, Dropped Frames high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

High Traffic Interface Number - enter the number of the interface for which you want to monitor traffic.

Filename: com.dartware.wrls.alvarionbaau.txt
Version: 1.7

[Back to Top](#)

Wireless > Alvarion > BreezeACCESS (SU)

BreezeACCESS (SU)

This probe monitors a BreezeCom or [Alvarion](#) BreezeACCESS 2.4 Ghz or 900 MHz subscriber unit (SU). It retrieves and displays the radio band, average power (in dBm or RSSI), and the MAC address of the associated AU. For a 900 MHz unit, it will also display the radio frequency. The probe will go into alarm or warning states based on user-definable parameters for low signal power or high incoming traffic on a specified interface.

Parameters

Average Power too low alarm, Average Power low warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

High Traffic Interface Number - enter the number of the interface for which you want to monitor traffic.

Filename: com.dartware.wrls.alvarionbasu.txt
Version: 1.7

[Back to Top](#)

Wireless > Alvarion > BreezeACCESS LB

BreezeACCESS LB

This probe is meant to probe an [Alvarion](#) BreezeACCESS LB radio, acting as either AP or an SU. It retrieves and displays a number traffic and radio related variables. It will go into alarm or warning states based on user-defined parameters.

Parameters

Expected Operating Frequency - Enter a frequency.

*SNR too low alarm, SNR low warning - enter thresholds for **Warning** and **Alarm**.*

Filename: com.dartware.wrls.alvarionbalb.txt
Version: 0.16

[Back to Top](#)

Wireless > Alvarion > BreezeACCESS VL (AU)

BreezeACCESS VL (AU)

This probe monitors an [Alvarion](#) BreezeACCESS VL access unit (AU). It retrieves and displays the radio band, operating frequency, and number of clients. It will go into an alarm or warning based on user defined parameters for high and low numbers of clients (SUs), and when the operating frequency doesn't match the configured frequency. Traffic information is available for the ethernet and radio interfaces. (To show the ethernet interface, we recommend using the "Display unnumbered interfaces" behavior.)

Parameters

*Current SU Count too high alarm, Current SU Count high warning,
Current SU Count too low alarm, Current SU Count low warning*

- enter thresholds for **Warning** and **Alarm**.

Filename: `com.dartware.wrls.alvarionbavlau.txt`
Version: 1.7

[Back to Top](#)

Wireless > Alvarion > BreezeACCESS VL (SU)

BreezeACCESS VL (SU)

This probe monitors an [Alvarion](#) BreezeACCESS VL subscriber unit (SU). It retrieves and displays the radio band, operating frequency, average received signal to noise ratio, and the MAC address of the associated access unit (AU). It will go into alarm or warning states based on user-defined parameters for a low signal to noise ratio or high traffic on a specified interface.

Parameters

*Avg Receive SNR too low alarm, Avg Receive SNR low warning,
High Traffic Bytes alarm, High Traffic Bytes warning*

- enter thresholds for **Warning** and **Alarm**.

High Traffic Interface Number - enter the number of the interface for which you want to monitor traffic.

Filename: `com.dartware.wrls.alvarionbavlsu.txt`
Version: 1.7

[Back to Top](#)

Wireless > Atmel > Atmel AT76C510**Atmel AT76C510**

This probe monitors devices based on the Atmel AT76C510 chip. Please refer to your device's technical specification to find out the chip type. Sample devices based on AT76C510 chip are as follows: Belkin F5D6130, D-Link DWL 900AP (rev. 1), Netgear ME102, and Linksys WAP11 (ver < 2).

It retrieves and displays information from the AT76C510 MIB using SNMP v1. Depending on the bridge's operating mode this probe will display different information.

If device is operating as a wireless client or a wireless repeater, the probe will display information about the connection to the parent access point (ESSID, SSID, channel, RSSI, link quality).

If the device is operating as a wireless bridge (either point-to-point or point-to-multipoint), the probe will display the list of authorized MAC addresses.

If the operating mode is a wireless repeater or access point, the probe will monitor the number of clients and list each one with its RSSI/link quality.

It retrieves and displays a number of traffic (bytes received/transmitted) and physical variables (name, MAC address, firmware revision).

This probe may not return complete information to SNMPv1 clients using the community string "public". To fully utilize this probe, you must set the community string to the one with the correct permissions.

Parameters

Number of clients warning, Maximum number of clients,

Too many failed packets/sec, Too many retry packets/sec

- enter thresholds for **Warning** and **Alarm**.

Link to Device Management Tool - enter the URL to the web manager for this device.

<i>Filename: com.dartware.wrls.AT76C510.txt</i> <i>Version: 1.5</i>
--

[Back to Top](#)

Wireless > Basic > IEEE 802.11

IEEE 802.11

This probe monitors 802.11 counters from a wireless device that supports the IEEE802dot11-MIB.

Parameters

Interface index - enter an interface for the wireless device.

*Tx Failed frames/sec, Tx Retry frames/sec, Rx FCS err fragments/sec, and ACK failures/sec - enter thresholds for **Warning** and **Alarm**.*

Filename: com.dartware.wrls.80211counters.txt
Version: 0.2

[Back to Top](#)

Wireless > Basic > SNMP for Wireless

SNMP for Wireless

(Previously titled "Wireless - Generic (SNMP MIB-II)")

This is a general probe for monitoring wireless gear for which there is no specific InterMapper probe, but that supports SNMP MIB-2. This probe will gather general traffic information, network connections, etc. It also adds an alarm when traffic on a user-selected interface reaches specified levels.

Parameters

Wireless interface number - the interface number of the device.

*High Traffic Bytes alarm, High Traffic Bytes warning - enter thresholds for **Warning** and **Alarm**.*

Filename: com.dartware.wrls.generic.txt
Version: 1.4

[Back to Top](#)

Wireless > Canopy > Canopy (AP)

Canopy (AP)

This probe monitors a Canopy wireless access point (AP), including basic information, traffic information, and the number of clients associated. It places the device into alarm or warning when the number of clients exceeds the user-defined thresholds.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

Too many clients alarm, Many clients warning,

Too few clients alarm, Few clients warning

- enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.canopyap.txt

Version: 1.9

[Back to Top](#)

Wireless > Canopy > Canopy (SM)**Canopy (SM)**

This probe monitors a Canopy wireless service module (SM).

This probe retrieves and displays a number of variables. It will place the device in alarm or warning states based on user-defined thresholds for high re-registration count, low RSSI, high Jitter, long Round Trip delay, and low Power Level, and give an alarm if the unit is not registered.

Note that the 2x jitter thresholds will only be used when the SM is operating in 2x/2x mode.

To disable any of the thresholds, set their values to 0.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

RSSI too low alarm, RSSI low warning,

Jitter too high alarm, Jitter high warning,

Jitter (2x) too high alarm, Jitter (2x) high warning,

Round Trip too long alarm, Round Trip long warning,

Power Level too low alarm, Power Level low warning,

Session count alarm, Session count warning,

Reg count alarm, Reg count warning,

Re-reg count alarm, Re-reg count warning

- enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.canopysm.builtin.txt

Version: 1.6

[Back to Top](#)

Wireless > Canopy > Canopy Backhaul (45 Mbps/FW 5830)

Canopy Backhaul (45 Mbps/FW 5830)

This probe monitors a Canopy 45Mbps Backhaul radio with firmware 5830 or older, acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation and speed mode, current and maximum transmit power, receive power, vector error, link loss, and signal-to-noise ratio. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, link loss, and signal-to-noise ratio.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning,

SNR too low alarm, SNR low warning

- *select or enter thresholds for **Warning** and **Alarm**.*

<i>Filename: com.dartware.wrls.canopy.backhaul45old.txt</i> <i>Version: 1.7</i>
--

[Back to Top](#)

Wireless > Canopy > Canopy Backhaul (60 Mbp/FW 5840)

Canopy Backhaul (60 Mbp/FW 5840)

This probe monitors a Canopy 60Mbps Backhaul radio with firmware 5840 or later, acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation and speed mode, current and maximum transmit power, receive power, vector error, and link loss. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, and link loss.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

*Rx Power too low alarm, Rx Power low warning,
Vector Error too high alarm, Vector Error high warning,
Link Loss too high alarm, Link Loss high warning*

- select or enter thresholds for **Warning** and **Alarm**.

*Filename: com.dartware.wrls.canopy.backhaul45.txt
Version: 1.9*

[Back to Top](#)

Wireless > Canopy > Canopy Backhaul (Master)

Canopy Backhaul (Master)

This probe monitors a Canopy wireless backhaul master unit, including wireless network and link information. It will give a warning if no slave is associated.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

None.

*Filename: com.dartware.wrls.canopybhm.txt
Version: 1.4*

[Back to Top](#)

Wireless > Canopy > Canopy Backhaul (Slave)

Canopy Backhaul (Slave)

This probe monitors a Canopy wireless backhaul slave unit. It retrieves and displays a number of variables. It will place the device in alarm or warning states based on user-defined thresholds for low RSSI, high Jitter, long Round Trip delay, and low Power Level, and give an alarm if the unit is not registered.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

*RSSI too low alarm, RSSI low warning,
Jitter too high alarm, Jitter high warning,
Round Trip too long alarm, Round Trip long warning,*

Power Level too low alarm, Power Level low warning

- enter thresholds for **Warning** and **Alarm**.

Filename: `com.dartware.wrls.canopybhs.txt`
Version: `1.4`

[Back to Top](#)

Wireless > Canopy > Canopy CMM Micro

Canopy CMM-Micro

This probe monitors a Canopy CMM-Micro. The device only supports basic SNMP v2c MIBs, no device-specific enterprise information is available.

Parameters

None.

Filename: `com.dartware.wrls.canopy.cmmmicro.txt`
Version: `0.5`

[Back to Top](#)

Wireless > CB3 > CB3 Bridge

CB3 Bridge

This TCP probe queries a CB3 wireless bridge via a HTTP GET request.

Parameters

User - the username to use when logging in.

Password - the password for the User specified above.

Port - the CB3's web interface HTTP port.

*Quality Warning, Quality Alarm - enter thresholds (in percent) for **Warning** and **Alarm**.*

Filename: `com.dartware.wrls.cb3.old.txt`
Version: `1.2`

[Back to Top](#)

Wireless > CB3 > CB3 Deluxe Bridge

CB3 Deluxe Bridge

This TCP probe queries a CB3 Deluxe wireless bridge via a HTTP GET request.

Parameters

User - the username to use when logging in.

Password - the password for the User specified above.

Port - the CB3's web interface HTTP port.

Quality Warning - the value (as a percentage) that the communications quality must fall below for the device to go into the WARN state.

Quality Alarm - the value (as a percentage) that the communications quality must fall below for the device to go into the ALARM state.

Filename: `com.dartware.wrls.cb3.txt`

Version: 1.5

[Back to Top](#)

Wireless > Inscape Data > AirEther AB54 Series AP (AP Mode)

AirEther AB54 Series AP (AP Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, AB54E Pro Multifunctional AP in Access Point Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Port - the Web interface's HTTP port.

RSSI Warning <, *RSSI Alarm* <,

Too Many Stations Warning >, *Too Many Stations Alarm* >,

Too Few Stations Warning <, *Too Few Stations Alarm* <

- enter thresholds for **Warning** and **Alarm**.

Filename: `com.dartware.wrls.inscape.ab54.ap.txt`

Version: 1.1

[Back to Top](#)

Wireless > Inscape Data > AirEther AB54 Series AP (Bridge Mode)

AirEther AB54 Series AP (Bridge Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, AB54E Pro Multifunctional AP in Point to Point or Point to Multipoint Bridge Mode.

Parameters

User is the name of the administrator.

Password is the password for the administrator.

Port is the Web interface's HTTP port.

*RSSI Warning <, RSSI Alarm < - enter thresholds for **Warning** and **Alarm**.*

Filename: com.dartware.wrls.inscape.ab54.bridge.txt
Version: 1.1

[Back to Top](#)

Wireless > Inscape Data > AirEther AB54 Series AP (Client Mode)

AirEther AB54 Series AP (Client Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, and AB54E Pro Multifunctional AP in Client Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Signal Strength Warning - the warning threshold for low signal strength %.

Signal Strength Alarm - the alarm threshold for low signal strength %.

Link Quality Warning - the warning threshold for low link quality %.

Link Quality Alarm - the alarm threshold for low link quality %.

Expected BSSID - the expected BSSID. This value will be ignored if blank.

Port - the Web interface's HTTP port.

Filename: com.dartware.wrls.inscape.ab54.client.txt
Version: 1.1

[Back to Top](#)

Wireless > Inscape Data > AirEther AB54 Series AP (Repeater Mode)

AirEther AB54 Series AP (Repeater Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, AB54E Pro Multifunctional AP in Repeater Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

RSSI Warning <, RSSI Alarm <,

*Too Many Stations Warning >, Too Many Stations Alarm >,
Too Few Stations Warning <, Too Few Stations Alarm <*

- enter thresholds for **Warning** and **Alarm**.

Port - the Web interface's HTTP port.

*Filename: com.dartware.wrls.inscape.ab54.repeater.txt
Version: 1.1*

[Back to Top](#)

Wireless > Inscape Data > AirEther CB54 Series Client

AirEther CB54 Series Client

This probe monitors [Inscape Data](#)'s CB54, CB54E, and CB5418 wireless client device.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Signal Strength Warning - the warning threshold for low signal strength %.

Signal Strength Alarm - the alarm threshold for low signal strength %.

Link Quality Warning - the warning threshold for low link quality %.

Link Quality Alarm - the alarm threshold for low link quality %.

Expected BSSID - the expected BSSID. This value will be ignored if blank.

Port - the Web interface's HTTP port.

*Filename: com.dartware.wrls.inscape.cb54.client.txt
Version: 1.1*

[Back to Top](#)

Wireless > MikroTik > MT Radio Uplink

MT Radio Uplink

This probe monitors a MikroTik router and its radio uplink interface. For the AP it monitors general SNMP interface and traffic information, as well as device utilization (CPU, Disk, Memory loads). For the radio uplink interface it monitors name & ssid, frequency, tx/rx rates, strength, and BSSID.

You must manually specify the OID index of the wireless uplink interface. Using Telnet: 1) Login, 2) Enter "interface wireless print oid", 3) The interface index is the last digit of the OIDs, 4) Type this number into the "Wireless Interface" field below.

This probe will raise an alarm in the following situations:

- *High Use -- for CPU, Disk, or Memory loads exceeds 90% (default setting of parameter).*

This probe is part of the InterMapper Wireless Probe Bundle, and requires InterMapper 4.2.1 or later.

Parameters

High Use Threshold - Percentage of use to trigger alarm

Wireless Interface - OID of the wireless uplink interface

<i>Filename: com.dartware.wrls.mt-1radio.txt</i> <i>Version: 1.14</i>
--

[Back to Top](#)

Wireless > MikroTik > MT Routerboard

MT Routerboard

This probe monitors a MikroTik Routerboard (wireless access point). It monitors the general SNMP interface and traffic information, device utilization (CPU Load, Disk use, and Memory use in percent), and the device's "health" (internal voltages and temperatures).

This probe will raise an alarm in the following situations:

- *High Use -- CPU Load, Disk use, or Memory use exceeding 90%.*
- *Unsafe Temperatures -- Safe ranges of -20°C to 50°C for Board & Sensor temps., -20°C to 70°C for CPU temp.*
- *Unsafe Voltages -- Safe deviation of +/- 5% for 12V & 5V, +/- 3% for 3.3V and Core Voltage (either 1.8V or 2.0V).*

This probe is part of the InterMapper Wireless Probe Bundle, and requires InterMapper 4.2.1 or later.

Parameters

High Use Threshold - Percentage of use to trigger alarm

High and Low Temperature thresholds - Enter temperature values (C) to trigger alarms, or keep the default values.

High & Low voltage thresholds - enter voltage values to trigger alarms, or keep the default values.

```
Filename: com.dartware.wrls.mt-routerboard.txt  
Version: 1.6
```

[Back to Top](#)

Wireless > MikroTik > MT Software Only

MT Software Only

This probe monitors any device that uses MikroTik software (a wireless access point), but does not monitor its wireless interfaces. It monitors general SNMP interface and traffic information and device utilization: CPU Load, Disk use, and Memory use (in percent).

This probe will raise an alarm in the following situations:

- *High Use -- CPU Load, Disk use, or Memory use exceeds 90%.*

This probe is part of the InterMapper Wireless Probe Bundle, and requires InterMapper 4.2.1 or later.

Parameters

High Use Threshold - Percentage of use to trigger alarm.

```
Filename: com.dartware.wrls.mt-0radio.txt  
Version: 1.5
```

[Back to Top](#)

Wireless > MikroTik > WDS Bridge

WDS Bridge

This probe monitors a MikroTik router in WDS Bridge mode. The probe monitors the Ethernet traffic information, as well as device utilization (CPU, Disk, Memory loads). The probe also displays the signal strength and tx/rx rates of the wireless link.

You must specify both the MAC address of the other AP, as well as the ifIndex of the wireless interface. The MAC address must be entered as six decimal numbers separated by "."

To determine the ifIndex of the wireless interface, Telnet to the radio, then:

- 1) *Log into the router*
- 2) *Enter `interface wireless print oid`*
- 3) *The interface index is the last digit of the OIDs*
- 4) *Type this number into the "Wireless Interface" field below.*

This probe will raise an alarm if the CPU, Disk, or Memory loads exceeds the High Use Threshold.

Parameters

Associated AP MAC Adrs - the MAC address of Access Point to which the router is connected.

Wireless Interface - the index of the interface

*High Use Threshold (%) - the usage threshold to trigger **Alarm**.*

Filename: `com.dartware.wrls.mikrotik-wds.txt`
Version: `1.3`

[Back to Top](#)

Wireless > Motorola > PTP 400 Series Bridge

PTP 400 Series Bridge

This probe monitors a Motorola PTP400 point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, and link loss. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, and link loss.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- *select modes and enter thresholds for **Warning** and **Alarm**.*

Filename: `com.dartware.wrls.motorola.ptp400.txt`
Version: `1.2`

[Back to Top](#)

Wireless > Motorola > PTP 600 Series Bridge**PTP 600 Series Bridge**

This probe monitors a Motorola PTP600 point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, link loss, and signal-to-noise ratio. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, link loss, and signal-to-noise ratio.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- *select modes and enter thresholds for **Warning** and **Alarm**.*

Filename: com.dartware.wrls.motorola.ptp600.txt

Version: 0.8

[Back to Top](#)

Wireless > Orthogon > Gemini**Gemini**

This probe monitors an Orthogon Systems Gemini point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, and link loss. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, and link loss.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- select and enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.orthogon.gemini.txt
Version: 1.8

[Back to Top](#)

Wireless > Orthogon > Spectra

Spectra

This probe monitors an Orthogon Systems Spectra point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, link loss, and signal-to-noise ratio. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, link loss, and signal-to-noise ratio.

Parameters

*Tx Modulation Mode Alarm, Tx Modulation Mode Warning,
Rx Modulation Mode Alarm, Rx Modulation Mode Warning,
Rx Power too low alarm, Rx Power low warning,
Vector Error too high alarm, Vector Error high warning,
Link Loss too high alarm, Link Loss high warning*

- select and enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.orthogon.spectra.txt
Version: 0.8

[Back to Top](#)

Wireless > Other > HTTP

HTTP

This probe tests an HTTP server by downloading a specific web page and scanning it for a specific string of HTML.

Parameters

URL Path - the full path of the desired file on the web server (e.g. "/index.html"). The first character must be a '/

String to verify - a string to verify in the server's response. For example, if you are retrieving a web page, you might search for "<HTML>" or "<P>" to verify that the data is HTML, or look for a unique string that is present only in the specified page.

User ID - the user name you would type into the web browser's authentication dialog. It is blank by default. Set this parameter to test a web page that requires authentication.

Password - the password you would type into the web browser's authentication dialog. It is blank by default. Set this parameter to test a web page that requires authentication.

```
Filename: com.dartware.wrls.http.txt  
Version: 1.5
```

[Back to Top](#)

Wireless > Proxim > Proxim AP 2000

Proxim AP-2000

This probe monitors [Proxim](#) AP-2000 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set Show station statistics to **true**.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- enter thresholds for **Warning** and **Alarm**.

Show wireless if settings - choose whether to show wireless interface settings.

Show security settings - choose whether to show security settings.

Show station statistics - choose whether to show statistics.

```
Filename: com.dartware.wrls.proximap2000.txt  
Version: 1.4
```

[Back to Top](#)

Wireless > Proxim > Proxim AP 4000

Proxim AP-4000

This probe monitors [Proxim](#) AP-4000 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set Show station statistics to **true**.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- enter thresholds for **Warning** and **Alarm**.

Show wireless if settings - choose whether to show wireless interface settings.

Show security settings - choose whether to show security settings.

Show station statistics - choose whether to show statistics.

Filename: `com.dartware.wrls.proximap4000.txt`
Version: 1.4

[Back to Top](#)

Wireless > Proxim > Proxim AP 600

Proxim AP-600

This probe monitors [Proxim](#) AP-600 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set Show station statistics to **true**.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- enter thresholds for **Warning** and **Alarm**.

Show wireless if settings - choose whether to show wireless interface settings.

Show security settings - choose whether to show security settings.

Show station statistics - choose whether to show statistics.

Filename: `com.dartware.wrls.proximap600.txt`

Version: 1.3

[Back to Top](#)

Wireless > Proxim > Proxim AP 700

Proxim AP-700

This probe monitors [Proxim](#) AP-700 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set Show station statistics to **true**.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- enter thresholds for **Warning** and **Alarm**.

Show wireless if settings - choose whether to show wireless interface settings.

Show security settings - choose whether to show security settings.

Show station statistics - choose whether to show statistics.

Filename: `com.dartware.wrls.proximap700.txt`

Version: 1.4

[Back to Top](#)

Wireless > Proxim > Proxim LAN Access Point

Proxim LAN Access Point

This probe monitors [Proxim](#) LAN access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set Show station statistics to **true**.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Many clients warning, Too many clients alarm,
FCS errors/sec high warning, FCS errors/sec too high alarm,
Failures/sec high warning, Failures/sec too high alarm,
Retries/sec high warning, Retries/sec too high alarm,
Show wireless if settings[true,false], Show security settings[true,false]

- enter thresholds for **Warning** and **Alarm**.

Show station statistics - choose whether to show statistics for this device.

Filename: com.dartware.wrls.proximap.txt
Version: 1.4

[Back to Top](#)

Wireless > Proxim > Tsunami GX

Tsunami GX

This probe monitors a Proxim Tsunami GX (GX 32 and GX 90).

This probe sets the device to **Alarm** if the status of either of the device's external inputs is in alarm. It also monitors the device's RFU status, IDU and RFU temperatures, RFU cable status, IDU fan status, IDU synthesizer status, RFU power status, RFU summary/minor relay status, AIS injection status, link status, and the number of errors/sec.

The temperature warning and alarm threshold are used only if the Use custom temperature threshold checkbox is selected.

Parameters

Use custom temperature threshold - check this to set your own temperature thresholds.

Temperature warning, Temperature alarm,
Errors/sec warning, Errors/sec alarm, Severe errors/sec alarm

- enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.proxim4.txt
Version: 0.4

[Back to Top](#)

Wireless > Proxim > Tsunami MP.11 BSU

Tsunami MP.11 BSU

This probe monitors [Proxim](#) Tsunami MP.11 Base Station Unit (BSU).
This probe can be used to monitor all MP.11 models, including 2411, 2454-R, 5054, and 5054-R.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Many subscribers warning, Too many subscribers alarm,
Signal dBm too low alarm, Signal dBm low warning,
Noise dBm too high alarm, Noise dBm high warning,
Send retries pct high warning, Send retries pct too high alarm,
Send failures pct high warning, Send failures pct too high alarm,
Receive retries pct high warning, Receive retries pct too high alarm,
Receive failures pct high warning, Receive failures pct too high alarm,
FCS errors/sec high warning, FCS errors/sec too high alarm,
Failures/sec high warning, Failures/sec too high alarm,
Retries/sec high warning, Retries/sec too high alarm

- enter thresholds for **Warning** and **Alarm**.

Show wireless if settings - select to show interface settings.

Show SU statistics - select to show Subscriber Unit statistics.

Filename: com.dartware.wrls.proximtmpbsu.txt
Version: 1.2

[Back to Top](#)

Wireless > Proxim > Tsunami MP.11 SU

Tsunami MP.11 SU

This probe monitors [Proxim](#) Tsunami MP.11 Subscriber Unit (SU/RSU).
This probe can be used to monitor all MP.11 models, including 2411, 2454-R, 5054, and 5054-R.

Note: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the InterMapper server.

Parameters

Signal dBm too low alarm, Signal dBm low warning,
Noise dBm too high alarm, Noise dBm high warning,
Send retries pct high warning, Send retries pct too high alarm,
Send failures pct high warning, Send failures pct too high alarm,
Receive retries pct high warning, Receive retries pct too high alarm,
Receive failures pct high warning, Receive failures pct too high alarm,
FCS errors/sec high warning, FCS errors/sec too high alarm,
Failures/sec high warning, Failures/sec too high alarm,
Retries/sec high warning, Retries/sec too high alarm

- enter thresholds for **Warning** and **Alarm**.

Show wireless if settings - select to show interface settings.

Filename: `com.dartware.wrls.proximtprsu.txt`
Version: `1.3`

[Back to Top](#)

Wireless > Redline > AN50

AN50

This probe is meant to probe a [Redline](#) AN50 point-to-point radio, acting as either a master or slave. It retrieves and displays a number of critical statistics for the radio, and gives alarms if it goes out of user-specified thresholds. The probe retrieves:

Average RF Rx signal strength, Average RF SNR, Signaling Burst Rate, Operating frequency, Radio Link Status and compares them to the thresholds below.

Parameters

Avg. Rx Signal strength too low alarm, Avg. Rx Signal strength low warning,
Avg. SNR too low alarm, Avg. SNR low warning,
Expected Uncoded Burst Rate, Expected Operating Frequency,
Active Links too high alarm, Active Links high warning,
Active Links too low alarm, Active Links low warning

- enter thresholds for **Warning** and **Alarm**.

Filename: `com.dartware.wrls.redlinean50.txt`
Version: 1.3

[Back to Top](#)

Wireless > smartBridges > airBridge

airBridge

This probe monitors a [smartBridges](#) airBridge device. It retrieves and displays a number of traffic (bytes received/transmitted) and physical variables (name, MAC address).

Note: Install InterMapper on a machine where you don't plan to run smartBridges simpleMonitor. To run both InterMapper and smartBridges' simpleMonitor on the same machine, disable trap processing in InterMapper.

Parameters

RSSI % low warning, RSSI % too low alarm,

Too many failed packets/sec, Too many retry packets/sec

- enter thresholds for **Warning** and **Alarm**.

Link to Device Management Tool - the URL for the device's web manager.

Filename: `com.dartware.wrls.airbridge.txt`
Version: 1.5

[Back to Top](#)

Wireless > smartBridges > airClient Nexus PRO total

airClient Nexus PRO total

This probe monitors a [smartBridges](#) airClient Nexus PRO total device. It retrieves and displays general device information, remote device information,

wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm

Tx retries (%) high warning Tx retries (%) too high alarm

Tx failed (%) high warning, Tx failed (%) too high alarm

Frame errors (%) high warning, Frame errors (%) too high alarm

ACK failures/min high warning, ACK failures/min too high alarm

Aborted frames/min high warning, Aborted frames/min too high alarm

RTS errors (%) high warning, RTS errors (%) too high alarm

- enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.airclientnexuspro.txt
Version: 0.5

[Back to Top](#)

Wireless > smartBridges > airClient Nexus

airClient Nexus

This probe monitors a [smartBridges](#) airClient Nexus device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm

Tx retries (%) high warning, Tx retries (%) too high alarm

Tx failed (%) high warning, Tx failed (%) too high alarm

Frame errors (%) high warning, Frame errors (%) too high alarm

ACK failures/min high warning, ACK failures/min too high alarm

Aborted frames/min high warning, Aborted frames/min too high alarm

RTS errors (%) high warning, RTS errors (%) too high alarm:

*- enter thresholds for **Warning** and **Alarm**.*

Filename: com.dartware.wrls.airclientnexus.txt
Version: 0.5

[Back to Top](#)

Wireless > smartBridges > airHaul Nexus PRO total

airHaul Nexus PRO total

This probe monitors a [smartBridges](#) airHaul Nexus PRO total device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

*Tx retries (%) high warning, Tx retries (%) too high alarm,
 Tx failed (%) high warning, Tx failed (%) too high alarm,
 Frame errors (%) high warning, Frame errors (%) too high alarm,
 ACK failures/min high warning, ACK failures/min too high alarm,
 Aborted frames/min high warning, Aborted frames/min too high alarm,
 RTS errors (%) high warning, RTS errors (%) too high alarm*

- enter thresholds for **Warning** and **Alarm**.

*Filename: com.dartware.wrls.airhaulnexuspro.txt
 Version: 0.5*

[Back to Top](#)

Wireless > smartBridges > airHaul Nexus

airHaul Nexus

This probe monitors a [smartBridges](#) airHaul Nexus device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

*RSSI (dBm) low warning, RSSI (dBm) too low alarm,
 Tx retries (%) high warning, Tx retries (%) too high alarm,
 Tx failed (%) high warning, Tx failed (%) too high alarm,
 Frame errors (%) high warning, Frame errors (%) too high alarm,
 ACK failures/min high warning, ACK failures/min too high alarm,
 Aborted frames/min high warning, Aborted frames/min too high alarm,
 RTS errors (%) high warning, RTS errors (%) too high alarm*

- enter thresholds for **Warning** and **Alarm**.

*Filename: com.dartware.wrls.airhaulnexus.txt
 Version: 0.5*

[Back to Top](#)

Wireless > smartBridges > airHaul2 Nexus PRO

airHaul2 Nexus PRO

This probe monitors a [smartBridges](#) airHaul2 Nexus PRO device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Radio to monitor - choose a radio interface to monitor.

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

Aborted frames/min high warning, Aborted frames/min too high alarm,

RTS errors (%) high warning, RTS errors (%) too high alarm

- enter thresholds for **Warning** and **Alarm**.

Filename: com.dartware.wrls.airhaul2nexuspro.txt
Version: 0.5

[Back to Top](#)

Wireless > smartBridges > airPoint Nexus PRO total

airPoint Nexus PRO total

This probe monitors a [smartBridges](#) airPoint Nexus PRO total device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Many clients warning, Too many clients alarm,

Many WDS clients warning, Too many WDS clients alarm,

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

*Aborted frames/min high warning, Aborted frames/min too high alarm,
RTS errors (%) high warning, RTS errors (%) too high alarm*

- enter thresholds for **Warning** and **Alarm**.

*Filename: com.dartware.wrls.airpointnexuspro.txt
Version: 0.5*

[Back to Top](#)

Wireless > smartBridges > airPoint Nexus

airPoint Nexus

This probe monitors a [smartBridges](#) airPoint Nexus device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

*Many clients warning, Too many clients alarm,
Many WDS clients warning, Too many WDS clients alarm,
RSSI (dBm) low warning, RSSI (dBm) too low alarm,
Tx retries (%) high warning, Tx retries (%) too high alarm,
Tx failed (%) high warning, Tx failed (%) too high alarm,
Frame errors (%) high warning, Frame errors (%) too high alarm,
ACK failures/min high warning, ACK failures/min too high alarm,
Aborted frames/min high warning, Aborted frames/min too high alarm,
RTS errors (%) high warning, RTS errors (%) too high alarm*

- enter thresholds for **Warning** and **Alarm**.

*Filename: com.dartware.wrls.airpointnexus.txt
Version: 0.5*

[Back to Top](#)

Wireless > smartBridges > airPoint

airPoint

This probe monitors a [smartBridges](#) airPoint device. It retrieves and displays information from the AT76C510 MIB using SNMP v1. Depending on the bridge's operating mode this probe will display different information.

If device is operating as a wireless client or a wireless repeater, the probe will display information about the connection to the parent access point (ESSID, SSID, channel, RSSI, link quality).

If the device is operating as a wireless bridge (either point-to-point or point-to-multipoint), the probe will display the list of authorized MAC addresses.

If the operating mode is a wireless repeater or access point, the probe will monitor the number of clients and list each one with its RSSI/link quality.

It retrieves and displays a number of traffic (bytes received/transmitted) and physical variables (name, MAC address, firmware revision).

This probe may not return complete information to SNMPv1 clients using the community string "public". To fully utilize this probe, you must set the community string to the one with the correct permissions.

Note: *Install InterMapper on a machine where you don't plan to run smartBridges simpleMonitor. To run both InterMapper and smartBridges' simpleMonitor on the same machine, disable trap processing in InterMapper.*

Parameters

Number of clients warning, Maximum number of clients,

Too many failed packets/sec, Too many retry packets/sec

- *enter thresholds for **Warning** and **Alarm**.*

Link to Device Management Tool - enter the URL to the web manager for this device.

Filename: com.dartware.wrls.airpoint.txt
Version: 1.5

[Back to Top](#)

Wireless > smartBridges > airPoint2 Nexus PRO

airPoint2 Nexus PRO

This probe monitors a [smartBridges](#) airPoint2 Nexus PRO device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Radio to monitor - choose a radio interface to monitor.

Many clients warning, Too many clients alarm,

Many WDS clients warning, Too many WDS clients alarm,

*RSSI (dBm) low warning, RSSI (dBm) too low alarm,
 Tx retries (%) high warning, Tx retries (%) too high alarm,
 Tx failed (%) high warning, Tx failed (%) too high alarm,
 Frame errors (%) high warning, Frame errors (%) too high alarm,
 ACK failures/min high warning, ACK failures/min too high alarm,
 Aborted frames/min high warning, Aborted frames/min too high alarm,
 RTS errors (%) high warning, RTS errors (%) too high alarm,*

- enter thresholds for **Warning** and **Alarm**.

*Filename: com.dartware.wrls.airpoint2nexuspro.txt
 Version: 0.5*

[Back to Top](#)

Wireless > Trango > Trango M2400S (AP)

Trango M2400S (AP)

This probe monitors a [Trango](#) M2400S access point (AP). It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, expected antenna mode, and expected channel. (This probe calculates counters without using sysUpTime, which isn't available. MIB-2 traffic and interface information is also unavailable.)

Parameters

*Tx power too low alarm, Tx power low warning - enter thresholds for **Warning** and **Alarm**.*

Expected Channel - enter the expected channel number.

Expected Antenna - choose an antenna mode.

*Filename: com.dartware.wrls.trango2400.txt
 Version: 1.1*

[Back to Top](#)

Wireless > Trango > Trango M5800S

Trango M5800S

This probe monitors a [Trango](#) 5800S access point, 5800-AP-60, or 5830-AP-60.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined

parameters for transmit power, number of subscriber unit clients, channel number, incoming traffic on the radio interface, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Parameters

Tx power too low alarm, Tx power low warning,

Too many client alarm, Many client warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

High Traffic Bytes alarm, High Traffic Bytes warning,

- enter thresholds for **Warning** and **Alarm**.

Expected Channel enter the expected channel number.

Filename: `com.dartware.wrls.trango10.txt`
Version: `1.4`

[Back to Top](#)

Wireless > Trango > Trango M5830S (SU)

Trango M5830S (SU)

This probe monitors a [Trango M5830S SU](#) Subscriber Unit.

You must enter the password for the subscriber unit to retrieve the information.

Note: *Occasionally, this Subscriber Unit reports extremely high data rates. These rates - in the range of millions of kbps - are seen both by this probe and in the Web interface. To keep the strip charts accurate, we recommend you turn off the Auto-adjust feature for the chart.*

Parameters

Password - the password for the Subscriber Unit.

Filename: `com.dartware.wrls.trango.M5830SSU.txt`
Version: `1.2`

[Back to Top](#)

Wireless > Trango > Trango M5830S

Trango M5830S

This probe monitors a [Trango M5830S](#) access point.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, number of subscriber unit clients, channel number, incoming traffic on the radio interface, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Parameters

Tx power too low alarm, Tx power low warning,

Too many client alarm, Many client warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

High Traffic Bytes alarm, High Traffic Bytes warning,

- enter thresholds for **Warning** and **Alarm**.

Expected Channel enter the expected channel number.

Filename: com.dartware.wrls.trango20.txt
Version: 1.4

[Back to Top](#)

Wireless > Trango > Trango M900S (AP)**Trango M900S (AP)**

This probe monitors a [Trango](#) M900S access point (AP). It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, expected antenna mode, and expected channel. (This probe calculates counters without using sysUpTime, which isn't available. MIB-2 traffic and interface information is also unavailable.)

Parameters

*Tx power too low alarm, Tx power low warning - enter thresholds for **Warning** and **Alarm**.*

Expected Channel - enter the expected channel number.

Expected Antenna - choose an antenna mode.

Filename: com.dartware.wrls.trango900.txt
Version: 1.4

[Back to Top](#)

Wireless > Trango > Trango P5830S (master)

Trango P5830S (master)

This probe monitors a [Trango](#) P5830S master unit.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, expected active channel number, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Tx power too low alarm, Tx power low warning,

RSSI too low alarm, RSSI low warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

RF High Traffic Bytes alarm, RF High Traffic Bytes warning,

Eth High Traffic Bytes alarm, Eth High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

Expected Channel - enter expected channel number.

<p>Filename: <code>com.dartware.wrls.trangoP5830SMU.txt</code> Version: 1.5</p>

[Back to Top](#)

Wireless > Trango > Trango P5830S (remote)

Trango P5830S (remote)

This probe monitors a [Trango](#) P5830S remote unit with firmware version 1.11 (040930) or later.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, incoming traffic on the radio interface, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Parameters

Tx power too low alarm, Tx power low warning,

RSSI too low alarm, RSSI low warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

RF High Traffic Bytes alarm, RF High Traffic Bytes warning,

Eth High Traffic Bytes alarm, Eth High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

Filename: `com.dartware.wrls.trangoP5830SRU.txt`
Version: 1.7

[Back to Top](#)

Wireless > Tranzeo > Sixth Generation AP

Sixth Generation AP

This probe monitors the sixth generation Access Point (AP) from [Tranzeo](#). This series includes AP for the following models: 5A, 5Aplus, 6600, 6500, 6000, 4900, CPQ, CPQplus.

This probe is part of the InterMapper Wireless Probe Bundle, and requires InterMapper 4.3 or later. Tranzeo is a trademark of Tranzeo Wireless Technologies, Inc.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.gen6ap.txt`
Version: 1.0

[Back to Top](#)

Wireless > Tranzeo > Sixth Generation CPE

Sixth Generation CPE

This probe monitors the sixth generation Customer Premise Equipment (CPE) from [Tranzeo](#). This series includes models 5A, 5Aplus, 6600, 6500, 6000, 4900, CPQ, CPQplus, running firmware version 2.0.11 or later.

The probe monitors the received signal strength and compares it to the warning and alarm thresholds below.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - enter thresholds for signal strength

Filename: `com.dartware.wrls.tranzeo.gen6cpe.txt`
Version: 1.2

[Back to Top](#)

Wireless > Tranzeo > Sixth Generation PxP

Sixth Generation PxP

This probe monitors the sixth generation point-to-point (PxP) equipment from [Tranzeo](#). This series includes models 5A, 5Aplus, 6600, 6500, 6000, 4900, CPQ, CPQplus, running firmware version 2.0.11 or later.

The probe monitors the received signal strength and compares it to the warning and alarm thresholds below.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - enter thresholds for signal strength

Filename: com.dartware.wrls.tranzeo.gen6pxp.txt

Version: 1.1

[Back to Top](#)

Wireless > Tranzeo > Tranzeo (AP)

Tranzeo (AP)

This probe monitors a [Tranzeo](#) 1000, 2000, 3000, 400, or 4000-series all in one device used as an Access Point (AP).

It retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for Received Signal level, Expected versus actual Station Channel, and incoming traffic on the radio interface, and gives an alarm when the wireless or ethernet links are reported down.

Supported Models: TR-410, TR-420, TR-430, TR-440, TR-450, TR-4115, TR-4215, TR-4315, TR-4415, TR-4118, TR-4218, TR-4318, TR-4418, TR-4500, and TR-4519. This probe will also support TR-1000, TR-1100, TR-1200, TR-1300, TR-2015, TR-2115, TR-2215, TR-2315, TR-3015, TR-3115, TR-3215, TR-3315, TR-2018, TR-2118, TR-2218, and TR-2318 model radios with firmware version 3.4.31.

Parameters

Received Signal Level too low alarm, Received Signal Level low warning,

No Buffer Packets too high alarm, No Buffer Packets high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

Expected Channel - enter the number of the expected channel.

Filename: com.dartware.wrls.tranzeoap.txt

Version: 1.3

[Back to Top](#)

Wireless > Tranzeo > Tranzeo (PXP)

Tranzeo (PXP)

This probe is meant to probe a [Tranzeo](#) 1000, 2000, 3000, 400, and 4000-series all in one device used as a PXP (bridge), or as an SAI (station) in router mode.

The probe retrieves and displays a number of variables for basic, ethernet, wireless, and bridge information. It will go into alarm and warning states based on user-defined parameters for Received Signal level, Expected versus actual Station Channel, and incoming traffic on the radio interface, as well as into alarm when the wireless or ethernet links are reported down.

Supported Models: TR-410, TR-420, TR-430, TR-440, TR-450, TR-4115, TR-4215, TR-4315, TR-4415, TR-4118, TR-4218, TR-4318, TR-4418, TR-4500, and TR-4519. This probe will also support TR-1000, TR-1100, TR-1200, TR-1300, TR-2015, TR-2115, TR-2215, TR-2315, TR-3015, TR-3115, TR-3215, TR-3315, TR-2018, TR-2118, TR-2218, and TR-2318 model radios with firmware version 3.4.31.

Parameters

Received Signal Level too low alarm, Received Signal Level low warning,

No Buffer Packets too high alarm, No Buffer Packets high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

Expected Channel - the number of the expected channel.

Filename: com.dartware.wrls.tranzeopxp.txt

Version: 1.3

[Back to Top](#)

Wireless > Tranzeo > Tranzeo (SAI)

Tranzeo (SAI)

This probe is meant to probe a [Tranzeo](#) 1000, 2000, 3000, 400, and 4000-series all in one device used as an SAI (station).

The probe retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for Received Signal level, Expected versus actual Station Channel, and incoming traffic on the radio interface, as well as into alarm when the wireless or ethernet links are reported down.

Supported Models: TR-410, TR-420, TR-430, TR-440, TR-450, TR-4115, TR-4215, TR-4315, TR-4415, TR-4118, TR-4218, TR-4318, TR-4418, TR-4500, and TR-4519. This probe will also support TR-1000, TR-1100, TR-1200, TR-1300, TR-2015, TR-2115, TR-2215, TR-2315, TR-3015, TR-3115, TR-3215, TR-3315, TR-2018, TR-2118, TR-2218, and TR-2318 model radios with firmware version 3.4.31.

Parameters

Received Signal Level too low alarm, Received Signal Level low warning,

No Buffer Packets too high alarm, No Buffer Packets high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

Expected Channel - the number of the expected channel.

Filename: `com.dartware.wrls.tranzeosai.txt`
Version: `1.3`

[Back to Top](#)

Wireless > Tranzeo > Tranzeo 58XX Series Backhaul

Tranzeo 58XX Series Backhaul

This probe is meant to monitor a [Tranzeo](#) 58XX Series Backhaul.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.58xx.backhaul.txt`
Version: `1.5`

[Back to Top](#)

Wireless > Tranzeo > Tranzeo AP 5A (44R)**Tranzeo AP-5A (44R)**

This probe is meant to monitor a [Tranzeo](#) TR-AP.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.ap.5A.44r.txt`
Version: `1.4`

[Back to Top](#)

Wireless > Tranzeo > Tranzeo AP 5A**Tranzeo AP-5A**

This probe is meant to monitor a [Tranzeo](#) TR-AP.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.ap.5A.txt`
Version: `1.4`

[Back to Top](#)

Wireless > Tranzeo > Tranzeo Classic**Tranzeo Classic**

This probe is meant to monitor a [Tranzeo](#) Classic.

Parameters

Password - the administrative password.

Filename: `com.dartware.wrls.tranzeo.classic.txt`
Version: `1.4`

[Back to Top](#)

Wireless > Tranzeo > Tranzeo CPE 200 (1.77.R)**Tranzeo CPE-200 (1.77.R)**

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Quality Warning, Quality Alarm,

Signal Warning, Signal Alarm

- enter thresholds for **Warning** and **Alarm** for Quality and Signal Strength.

Filename: com.dartware.wrls.tranzeo.cpe.200.177R.txt
Version: 1.4

[Back to Top](#)

Wireless > Tranzeo > Tranzeo CPE 200

Tranzeo CPE-200

This probe monitors a [Tranzeo](#) TR-CPE 200. It has thresholds for alarms and warnings if the signal level gets too low.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - enter thresholds for signal strength

Filename: com.dartware.wrls.tranzeo.cpe.200.txt
Version: 1.7

[Back to Top](#)

Wireless > Tranzeo > Tranzeo CPE 5A (44R)

Tranzeo CPE-5A (44R)

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - enter thresholds for signal strength

Filename: com.dartware.wrls.tranzeo.cpe.5A.44r.txt
Version: 1.5

[Back to Top](#)

Wireless > Tranzeo > Tranzeo CPE 5A**Tranzeo CPE-5A**

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - enter thresholds for signal strength

Filename: `com.dartware.wrls.tranzeo.cpe.5A.txt`
Version: `1.4`

[Back to Top](#)

Wireless > Tranzeo > Tranzeo TR CPE**Tranzeo TR-CPE**

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

It will give a warning at a user-definable threshold for low signal, and an alarm when signal strength is "poor". You will need to enter as parameters your web admin username and password, as well as the SSID of the connection you want information on.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

SSID - the SSID of the connection you want to view.

Warning Threshold - enter a threshold for Signal Strength.

Filename: `com.dartware.wrls.tranzeocpe.txt`
Version: `1.3`

[Back to Top](#)

Wireless > WaveRider > CCU**CCU**

This probe monitors a WaveRider CCU (access point). It retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined

parameters for radio frequency, percentage of payloads not needing a retry, percentage of payloads sent as broadcast, percentage of payloads discarded, percentage of payloads "Rx PER", percentage of payloads with HCRC errors, "Rx No-Match" errors, and high traffic incoming on the wireless interface. It will also go into an alarm based on the global status indicator.

Parameters

Expected Frequency - the expected frequency

No Retry percentage too low alarm, No Retry percentage low warning,

Broadcast percentage too high alarm, Broadcast percentage high warning,

Discard percentage too high alarm, Discard percentage high warning,

Rx PER percentage too high alarm, Rx PER percentage high warning,

HCRC percentage too high alarm, HCRC percentage high warning,

Rx No-Match too high alarm, Rx No-Match high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter **Warning** and **Alarm** thresholds.

Filename: com.dartware.wrls.waveriderccu.txt

Version: 1.1

[Back to Top](#)

Wireless > WaveRider > EUM

EUM

This probe monitors a WaveRider EUM (subscriber unit). It retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for radio frequency, percentage of payloads not needing a retry, percentage of payloads discarded, RSSI value, signal strength rating, and high traffic incoming on the wireless interface. It will also go into an alarm based on the global status indicator.

Parameters

RSSI too low alarm, RSSI low warning,

Signal rating too high alarm, Signal rating high warning,

SNR too low alarm, SNR low warning,

No Retry percentage too low alarm, No Retry percentage low warning,

Tx Discard percentage too high alarm, Tx Discard percentage high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- enter thresholds for **Warning** and **Alarm**.

<p><i>Filename:</i> <code>com.dartware.wrls.waveridereum.txt</code> <i>Version:</i> <code>1.2</code></p>
--

[Back to Top](#)

Experimental

- [Experimental > Flow Exporter Status \(Pg 593\)](#)
- [Experimental > InterMapper \(Pg 593\)](#)
- [Experimental > sFlow v1.2 \(Pg 594\)](#)
- [Experimental > sFlow Vers. 1.3 \(Pg 595\)](#)

[To Probe Index \(Pg 442\)](#)

Experimental > Flow Exporter Status

Flow Exporter Status

This probe monitors a Flow Exporter and reports statistics about Flow activity. It does this by retrieving information from the InterMapper Flows server.

The normal state of the device is UP/OKAY. There are two error conditions:

- *If the monitored device does not appear to be a Flow Exporter (it is not listed by InterMapper Flows), the status of the device is set to CRITICAL.*
- *If the InterMapper Flows server has received no flow records during a poll interval, the status of the device is set to DOWN.*

Parameters

None.

<i>Filename:</i> <code>com.dartware.flow.exporter.txt</code> <i>Version:</i> <code>1.3</code>
--

[Back to Top](#)

Experimental > InterMapper

InterMapper

This probe monitors the status of the InterMapper polling engine. With the default setting, this probe displays the results of 500 loops through the polling engine. To measure activity at a finer-grain, decrease the value of the Loops parameter. A value of '1' updates the statistics on every pass through the main run loop.

The "Main Loop" frequency is the number of times that InterMapper performs the main loop each second. The theoretical maximum loop frequency is 66.667 loops per second, based on the current yield value of 15 msec. If it falls below 10 or even 5 loops per second, InterMapper may report false outages.

This probe also reports polling rate as a percentage of the maximum loops per second. This is a measure of how much additional processing

occurs per loop. This percentage will never be 100%. It should, however, level out and remain steady over time.

On Unix systems, this probe reports Context Switches Per Loop (CSPL). This is another measure of the overhead of InterMapper's processing as it runs on your system. Fewer context switches per loop is better (ideal = 0), since context switches carry overhead. A server with thousands of devices and hundreds of mays may well have a CSPL greater than 2 during normal operation. (This value is not available on Windows systems, and is always set to -1.)

InterMapper tracks the number of bytes sent out the main UDP polling socket. Bytes/Loop is the average bytes sent per loop, averaged over the last batch of N loops. Bytes Peak is the maximum number of bytes sent in a *single* polling loop. (In the current implementation, the peak bytes is checked on every loop, but only resets to 0 when you change the # loops parameter; ie peak bytes is not the peak bytes of the last batch of N loops.)

Parameters

Loops - the number of loops to perform before updating statistics.

<p>Filename: <code>com.dartware.tcp.intermapper.txt</code> Version: <code>0.11</code></p>

[Back to Top](#)

Experimental > sFlow v1.2

sFlow v1.2

This probe's Status Window shows the sFlow version, address, and address type of the sFlow exporter. It uses the [sFlow MIB version 1.2](#), with the Enterprise Number 4300 to retrieve statistics for sFlow versions 2 and 4.

It also shows the sFlowTable, as an on-demand table. It lists all devices receiving the sFlow records. (To view this on-demand table, you must import [the SFLOW-MIB version 1.2](#).)

Parameters

Version_HiWarn - sFlow version expected. If the exporter version does not match this version, the device is set to a **Warning** state.

<p>Filename: <code>com.dartware.sflowv1.2.txt</code> Version: <code>1.2</code></p>
--

[Back to Top](#)

Experimental > sFlow Vers. 1.3

sFlow Vers. 1.3

This probe's Status Window shows the sFlow version, address, and address type of the sFlow exporter. It uses the [sFlow MIB version 1.3](#), with the Enterprise Number 14706 for sFlow version 5.

It also shows the sFlow Receiver Table as an on-demand table. It lists all devices receiving the sFlow records. (To view this on-demand table, you must import [the SFLOW-MIB version 1.3](#).)

Parameters

sFlow version - Enter the version of sFlow to use.

<i>Filename:</i> <code>com.dartware.sflow.v1.3.txt</code> <i>Version:</i> <code>1.3</code>

[Back to Top](#)

About Packet-Based Probes

Packet-based Test Procedure

Whenever InterMapper tests a packet-based device, it uses the following procedure:

1. InterMapper sends the appropriate probe packet (ping, SNMP get-request, DNS query, etc.)
2. InterMapper waits the timeout interval specified for the particular device.
3. If a response arrives, InterMapper examines its contents and sets the device status based on that response
4. However, if no response arrives, InterMapper sends another probe packet
5. The above procedure is repeated until a response arrives or the specified number of probes has been sent
6. If no response has arrived after the final timeout, InterMapper sets the device status to Down.
7. In any event, the device is scheduled to be tested again at a time set by the map's (or the device's) poll interval.

The default timeout is three seconds, with a default probe count of three seconds. Consequently, InterMapper will take nine seconds to declare a device is down (three probes, waiting three seconds each). Both the timeout and the number of probes can be set for each device.

This often gives rise to 21 second or 51 second outages. What's happening here is that the device fails to respond to one set of probes (for example, after nine seconds), but responds immediately at the next poll 30 or 60 seconds later. This gives an outage duration to be $(30-9=21)$ seconds or $(60-9=51)$ seconds.

Shared Polling in Ping/Echo and SNMP Probes

You may have created different maps that poll the same device. For Ping/Echo and SNMP probes (built-in or custom), InterMapper polls a device only once if it is considered to be the same device, and shares the response among all the maps that poll that device.

This happens automatically, and there are no user-controllable parameters.

In order for two mapped devices to be considered the same and share the results of a single probe, the following characteristics of the mapped device must be identical:

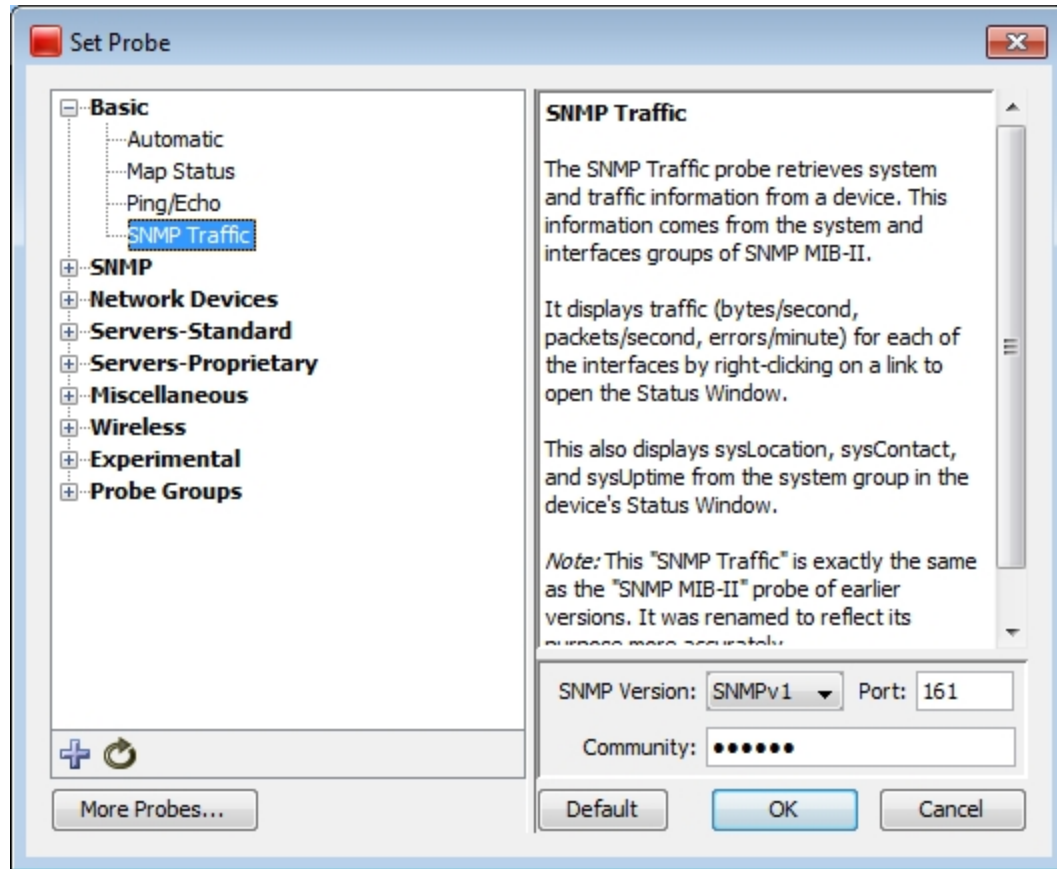
- Probe Type
- Address
- Port
- Poll Interval
- Timeout
- Max tries
- Display Unnumbered Interfaces, Ignore Discards, Ignore Errors, Allow Periodic Reprobe
- SNMP Version and read-only community string

- Number, name, and value of probe parameters
- SNMPv3 authentication information

For SNMP probes, the following flags in the probe file must be identical. (this is nearly always the case, as it is implied by the probe type, but is still checked explicitly):

- MINIMAL
- NOLINKS
- LINKCRITICAL

About SNMP Versions



Using SNMP Version 1, 2c, and 3 in Probes

All SNMP-based probes can use one of version 1, 2c, or 3, at the user's choice. The Probe Configuration window allows you to specify the SNMP version at the same time you set all the other parameters for the probe.

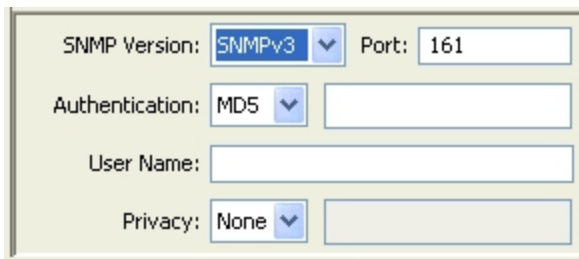
The lower part of the Probe Configuration window displays the SNMP version information. Select the version from the SNMP Version dropdown.

- Selecting SNMPv1 or SNMPv2c will show a field to enter the SNMP Read-only community string.



- Selecting SNMPv3 changes the lower half of the probe configuration window to let you specify all the authentication and privacy parameters. The initial settings show the default settings taken from the Server Settings > SNMP pane.

See the [SNMP Preferences \(Pg 254\)](#) page for more details.



The image shows a dialog box titled "SNMP Preferences". It contains four rows of controls:

- SNMP Version: A dropdown menu with "SNMPv3" selected.
- Port: A text box containing "161".
- Authentication: A dropdown menu with "MD5" selected, followed by an empty text box.
- User Name: An empty text box.
- Privacy: A dropdown menu with "None" selected, followed by an empty text box.

Note: Certain equipment requires SNMPv2 or SNMPv3, and probes can be built to force that selection. If you try to set the SNMP version lower than the probe can support, you will receive an error message.

Command-Line Probes

Command-line probes execute a command as a command-line on supported platforms. They usually call custom executables on the target machine.

Command Line Probes

Use the Command Line probe to execute a user-written program or script to test a device. The result code returned from the program sets the device's condition. When you create a custom command line probe, you usually start with the Nagios Plugin probe.

For more information, see *Command Line Probes* in the [Developer Guide](#).

Monitoring NT Services with the Windows NT Services Probe

InterMapper can monitor and send notifications for NT Services running on another computer. InterMapper uses the Service Control Manager facilities of the underlying Windows host to communicate with a remote computer to track the state of its services.

Note: This NT Services monitoring is only available if the InterMapper server is running on a Windows XP, or 2003 computer. You cannot use this facility if you're using a Macintosh or Unix/Linux computer to host the InterMapper server.

The NT Services

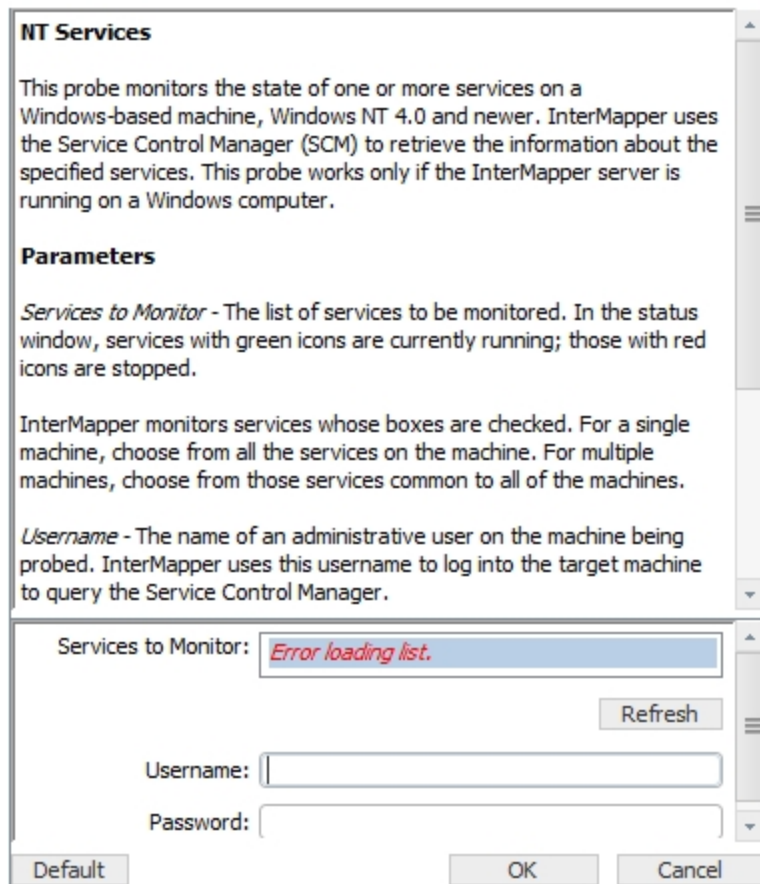
configuration window displays the full list of services that are running on a remote host. You can check off one or many services to monitor; InterMapper will then give an alert if any of them fails. The parameters to the probe are:

- A list of **NT services** on the target machine. This list has red and green marks to indicate whether the service is currently running. Checking the box for the service will cause InterMapper to send an alert if that service ever stops running.
- The **Username** and **Password** required to log onto the target machine.

Authentication for NT Services Probe

The NT Services probe opens the Service Control Manager (SCM) on the target machine; hence, some authentication is required before this can happen. There are several ways to do this.

1. **Using built-in username and password:** InterMapper has the built-in ability to solicit from you a username and password for authentication. When you



NT Services Preferences Panel

choose the NT Services probe, it will prompt you for a username and password before attempting to connect to the target machine. If you have not used one of the methods below, fill in a username and password at that point and click OK. This will be all you need to do for authentication; the username and password will be saved.

Note: For this to work, InterMapper must be running as an administrator, as only administrators are empowered to make the required network connections. You can do this in one of two ways:

- The first way is by adjusting the account under which InterMapper is run. InterMapper is normally installed under the LocalSystem account, which does not have administrator privileges. To change the account under which it runs, follow this procedure: Go into the SCM and stop the InterMapper service if it is running. Right-click and choose "Properties". Choose the "Log On" tab. Under "Log On As...", click the radio button next to "This account:", and click "Browse..." to list the accounts; choose an account with administrator privileges. Fill in the password for the account in "Password:" and "Confirm Password:". Click "OK".
- The second way is to let InterMapper be an administrator when it needs to be by supplying it with an administrator's username and password, so that it can elevate its privileges when it needs to. You can do this using the NT Services item in the Server Settings list. **Note:** In either scheme, the administrator you supply must have been given the "Logon as a service" right in the local security policy of the machine you are monitoring.

2. **The NET USE command:** Another way to authenticate is to use the NET USE command to create a connection between the host machine and the target. For instance, to monitor the services on a host at 192.168.1.140, enter the following:

```
NET USE \\192.168.1.140\ipc$ /USER:Administrator
```

You will be prompted for the password, and the connection will be made. (If you have done this, when prompted for a username and password for NT Services by InterMapper, you can leave them blank and click OK.)

Note: You must use the IP address and not the network name for the machine. That is important, as the Windows OS will not see the DNS name or the domain name as being the same as 192.168.1.140 when checking the connections, and will not recognize that there is a connection when InterMapper tries to query the services by IP address, returning an "access denied" error instead.

3. **Synchronizing Users:** A third way to authenticate is to make sure that the user and password under which the InterMapper service is running exists on the target machine as well.

When InterMapper is first installed, it is installed running under the user "LocalSystem", as most services are. It is necessary to create a new user on

your machine; let's name it *InterMapper* and give it a password. Make sure it is a member of Administrators. (If you already have a username and password that exist on all machines that are to be targeted by the NT Services probe as well as the InterMapper host and which has Administrator permissions everywhere, you can skip the previous step and substitute it for *InterMapper* in the following.)

Go into the SCM and stop the InterMapper service if it is running. Right-click and choose "Properties". Choose the "Log On" tab. Under "Log On As...", click the radio button next to "This account:", and click "Browse..." to list the accounts; choose *InterMapper*. Fill in the password for the account in "Password:" and "Confirm Password:". Click "OK".

On the target machine, create a new user, also named *InterMapper*, with the same password, and also a member of Administrators.

Start InterMapper from the SCM on the original machine. You should now be able to use NT Services probes. (When prompted for a username and password for NT Services by InterMapper, you can leave them blank and click OK.)

A Note on Error Messages

InterMapper may encounter authentication errors when attempting to connect. Here is a list of the messages and ways you might work around them:

- **Error attempting to elevate privileges.** InterMapper is not running as an administrator, and thus needs to elevate its privileges in order to be able to execute the NT Services probe. It could not do so. Make sure a correct username and password for the InterMapper host machine have been supplied in the NT Services panel of the Server Settings dialog. Make sure the user given has the right to log on as a service in your Local Security Policy. If host machine is Windows Server 2003 or newer, make sure the user has the right to impersonate another user.
- **Could not establish Windows Networking connection to probe target.** When a username and password have been supplied for the target machine, InterMapper attempts to use them to create a connection between the host and the probe target. This attempt failed for some reason. Will be followed by more specific error information. See below.
- **Could not open SCM on probe target.** InterMapper could not open the Service Control Manager on the target machine. Will be followed by more specific error information. See below.

The following errors might be appended to the messages above:

- **Access is denied.** Make sure InterMapper is running as an administrator, or that an administrator username and password have been provided in the NT Services panel in the Server Settings dialog. Make sure a valid administrator username and password have been supplied for the probe target. If the probe target is running Windows XP, make sure that "Simple Networking" is turned off.
- **The network name cannot be found.** and **The network path was not found.** The device you have specified does not appear to exist on the network. If you are sure that it does, make sure it is a Windows machine with File and Print Sharing turned on, and that any firewall has exceptions for File and Print Sharing.
- **An extended error has occurred.** A network-specific error has occurred. It should be followed by more information about the nature of the error. You may need to consult your network administrator.
- **The specified network password is incorrect.** The password you supplied doesn't match the username.
- **No network provider accepted the given network path.** and **The network is not present or not started.** No network is present, or a component of the network has not been started. Consult your network administrator.
- **The RPC server is unavailable.** Make sure that probe target is a Windows machine with File and Print Sharing turned on, and that any firewall has exceptions for File and Print Sharing.

Cisco IP SLA Probe

IP SLA uses active traffic monitoring - the generation of traffic in a continuous, reliable, and predictable manner - for measuring network performance edge-to-edge over a network. The traffic generated simulates network applications like VoIP and video conferencing, and collects network performance information in real time. The information collected includes data about jitter (interpacket delay variance), latency, and packet loss.

Cisco IP SLA is supported on most IOS-based Cisco routers and switches. IP SLA was previously known as Service Assurance Agent (SAA).

You can easily configure your Cisco routers and switches to be IP SLA agents or IP SLA responders. An agent initiates IP SLA tests to a remote responder. A particular agent can have multiple IP SLA tests running to many remote responders. A particular router or switch can be both an agent and a responder. For each IP SLA test that has been configured the agent collects edge-to-edge network performance information and stores it in the Cisco RTTMON MIB.

The InterMapper IP SLA Probe

```

Jitter Test UBC<->UNBC
Device Status
  Name: Jitter Test UBC<->UNBC
  DNS Name: (Unknown)
  SysName: LFSC01-97
  Address: 10.10.2.29
  Status: UP
  Protocol: SNMP - Cisco SAA Jitter Probe (port 161)
  Up Time: 13 days, 17 hours, 45 minutes
  Contact: netadmins@example.com
  Availability: 100 % (of 3 days, 20 hours, 9 minutes)
  Packet Loss: 0.14 % (of 11079 total attempts) [Reset]
  Recent Loss: 1 pkts at Oct 31, 20:43:06
  Round-trip time: 7 msec
Cisco IP SLA Jitter Test Information
Probe version: Feb.1, 2007 IP SLA Agent 1min Avg CPU Busy:1%
Alarm and Warning Thresholds:
  Latency Alarm:150ms, Latency Warning:100ms
  Jitter Alarm:30ms, Jitter Warning:20ms
  Packet Loss Alarm:1%
Jitter Test Parameters:
  Send 50 1024-byte packets spaced 20ms apart every 60 seconds
  SNMP index:59
Latest Round Trip Test Results:
  Number of Round Trips:50, Min:15ms, Max:16ms, Sum:776ms, Avg:16ms
  SD Packets Lost:0, DS Packets Lost:0
  Out of Sequence:0, Late Arrival:0
  % Packet Loss:0%, Total Packets Lost:0
Latest Jitter Test Results:
  SD +Jitter Values #:2, Min:1ms, Max:1ms, Sum:2ms, Avg:1ms
  SD -Jitter Values #:2, Min:1ms, Max:1ms, Sum:2ms, Avg:1ms
  DS +Jitter Values #:4, Min:1ms, Max:1ms, Sum:4ms, Avg:1ms
  DS -Jitter Values #:3, Min:1ms, Max:1ms, Sum:3ms, Avg:1ms
  Average Jitter Value:0ms, Total Jitter:11ms, Max Jitter:1ms
Latest Latency Test Results:
  SD Packets Sent #:50, Min:8ms, Max:9ms, Sum:403ms, Avg:8ms
  DS Packets Rcvd #:50, Min:7ms, Max:8ms, Sum:373ms, Avg:7ms
  Average Latency:8ms, Max Latency:9ms
60min Accumulated Test Results:
  60min Max Round Trip Time:17ms
  60min Total SD Packets Lost:0, Total DS Packets Lost:0
  60min Max SD +Jitter Value:1ms, -Jitter, Value:1ms
  60min Max DS +Jitter Value:2ms, -Jitter, Value:2ms
Last updated Nov 01, 09:58:41; interval: 1 minute, 0 seconds

```

IP SLA Jitter probe output in Status window

The InterMapper Cisco IP SLA Jitter probe uses SNMP to collect the information from the RTTMON MIB in the agent, allowing you to alarm jitter, latency, and packet loss, and to chart these values. You can [download a .zip](#) of the probe.

The InterMapper Cisco *IP SLA Probe* is particularly useful for monitoring and measuring QoS for VoIP and video conferencing applications. However, it is useful in many other contexts including:

- Service level agreement monitoring, measurement, and verification.
- IP network health assessment
- Troubleshooting of network operation

Documentation

An [IP SLA Probe User Guide](#) describes how to set up the IP SLA testing between two Cisco routers/switches and how to configure the InterMapper probe to monitor the values.

This page shows a sample Status Window for the probe. You can also see a [screen-shot with several graphs from a live installation](#).

Extensive documentation about IP SLA and how to configure IP SLA is available on the [Cisco web site](#).

Big Brother Probes

InterMapper can act as a Big Brother server. [Big Brother](#) is a popular network monitoring tool that allows you to create scripts ("clients") that run on remote systems and send status reports back to the Big Brother server. This allows a network manager to test additional kinds of network devices, either by writing scripts or using some of the many [scripts that are already available](#).

When you specify a device to be tested with a Big Brother probe, InterMapper's built-in Big Brother server listens for messages coming from a Big Brother client on the corresponding machine.

To configure Big Brother probe, you need to set two parameters:

- **Port** - The default port is 1984, but you may choose a different port. If you choose a different port, make sure that the Big Brother client on the corresponding machine is also configured for the same port.
- **Purple Time** - This is the number of minutes to wait without a report before indicating a problem. In an actual Big Brother server, this is thirty minutes; Big Brother shows a device as purple if it goes this long without reports from the device. InterMapper shows it as DOWN (blinking red).

In order for InterMapper to receive Big Brother messages from the remote client, it must be configured correctly. In particular, the client must be configured so that its BBDISPLAY is set to the IP address of the machine where InterMapper is running.

The Big Brother states will be mapped to InterMapper states as shown in the table below:

Big Brother State	InterMapper Status
Okay (green)	Okay (green)
Attention (yellow)	Warning (yellow)
Trouble (red)	Critical (red)

At the moment, the only messages that InterMapper will process and represent are "status" (and "combo") messages.

Note that the Big Brother server for a given port will not start until at least one device has been configured for that port. Similarly, once the last device for that port has been removed, the server for that port will shut down.

For more information about Big Brother, check the Big Brother web site at <http://www.bb4.com/download.html>. "Big Brother System and Network Monitor" is a trademark of BB4 Technologies, Inc. There's a good description of the Big Brother message format at: http://www.bb4.org/bb/help/help/Status_Message_Format.htm. You can also look through a large set of [Big Brother clients](#) that can be downloaded freely.

Troubleshooting Network and Server Probes

- [How do I change the protocol that a device is being polled with? \(Pg 608\)](#)
- [What MIB variables does InterMapper poll? \(Pg 608\)](#)
- [How Does InterMapper Compute Traffic Statistics? \(Pg 610\)](#)
- [How Does InterMapper Compute Utilization for a Link? \(Pg 610\)](#)
- [How Does InterMapper Compute Errors for a Link? \(Pg 610\)](#)
- [Why can't I get a DHCP probe on OSX to work? \(Pg 611\)](#)
- [If I look at the traffic on a link, wait five seconds, and look again, the traffic rates are the same. Shouldn't these numbers be updated? \(Pg 612\)](#)
- [How does InterMapper compute byte and packet rates? \(Pg 612\)](#)
- [How does InterMapper compute time intervals? \(Pg 612\)](#)

How do I change the protocol that InterMapper polls with?

1. Click to select the device you want to change.
2. From the Monitor menu, choose **Info Window**
3. Choose a new probe type from the **Probe Type** dropdown menu. If parameters are required, a parameters window appears for the selected probe type.
4. Enter parameters if necessary, and click **OK**. The device is polled using the new probe type.

For more information, see [Status Windows](#) (Pg 185).

What MIB variables does InterMapper poll?

Anytime InterMapper displays traffic for a link, (using the [SNMP Traffic Probe \(Pg 449\)](#), for example) it polls the following variables:

SNMPv1

When you set the **SNMP Version** to SNMPv1, the following variables are queried:

MIB Variable	OID	SNMP Version
ifInOctets	1.3.6.1.2.1.2.2.1.10	SNMPv1
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	SNMPv1
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	SNMPv1
ifOutOctets	1.3.6.1.2.1.2.2.1.16	SNMPv1
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	SNMPv1
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	SNMPv1

InterMapper examines these two variables to decide whether an interface is up or down:

MIB Variable	OID	SNMP Version
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	SNMPv1
ifOperStatus	1.3.6.1.2.1.2.2.1.8	SNMPv1

InterMapper examines these variables to detect error conditions:

MIB Variable	OID	SNMP Version
ifInDiscards	1.3.6.1.2.1.2.2.1.13	SNMPv1
ifInErrors	1.3.6.1.2.1.2.2.1.14	SNMPv1
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	SNMPv1
ifOutErrors	1.3.6.1.2.1.2.2.1.20	SNMPv1

SNMPv2c

When you set the **SNMP Version** to SNMPv2c, the following variables are queried:

This variable set is used on an initial scan of the device.

MIB Variable	OID	SNMP Version
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv1
ifType	1.3.6.1.2.1.2.2.1.3	SNMPv1
ifMTU	1.3.6.1.2.1.2.2.1.4	SNMPv1
ifSpeed	1.3.6.1.2.1.2.2.1.5	SNMPv1
ifPhysAddress	1.3.6.1.2.1.2.2.1.6	SNMPv1
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	SNMPv1
ifOperStatus	1.3.6.1.2.1.2.2.1.8	SNMPv1
ifName	1.3.6.1.2.1.31.1.1.1.1	SNMPv2c
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15	SNMPv2c
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16	SNMPv2c
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17	SNMPv2c
ifAlias	1.3.6.1.2.1.31.1.1.1.18	SNMPv2c

This variable set is polled to display statistics for the device's operation.

MIB Variable	OID	SNMP Version
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	SNMPv1
ifOperStatus	1.3.6.1.2.1.2.2.1.8	SNMPv1
ifLastChange	1.3.6.1.2.1.2.2.1.9	SNMPv1
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	SNMPv1
ifInErrors	1.3.6.1.2.1.2.2.1.14	SNMPv1
ifInDiscards	1.3.6.1.2.1.2.2.1.13	SNMPv1
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	SNMPv1
ifOutErrors	1.3.6.1.2.1.2.2.1.20	SNMPv1
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	SNMPv1
sysUpTime	1.3.6.1.2.1.1.3	SNMPv1
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	SNMPv2c
ifHCOctets	1.3.6.1.2.1.31.1.1.1.10	SNMPv2c

ifInMulticastPkts 1.3.6.1.2.1.31.1.1.1.2 SNMPv2c
ifInBroadcastPkts 1.3.6.1.2.1.31.1.1.1.3 SNMPv2c
ifOutMulticastPkts 1.3.6.1.2.1.31.1.1.1.4 SNMPv2c
ifOutBroadcastPkts 1.3.6.1.2.1.31.1.1.1.5 SNMPv2c

Note: In the SNMPv2c, the input and output MulticastPkts and BroadcastPkts MIB variables replace NUcastPkts variables of the SNMPv1 probe, which are deprecated. HCOctets replace the regular Octets counters. Pkts and errors still use the MIB-II 32 bit counters.

How Does InterMapper Compute Traffic Statistics?

InterMapper uses `ifInOctets` and `ifOutOctets` to compute the Receive and Transmit bytes/second values, respectively.

The Receive and Transmit packets/second numbers are computed using the sum of the (`ifInUcastPkts` + `ifInNUcastPkts`) and (`ifOutUcastPkts` + `ifOutNUcastPkts`) respectively.

How Does InterMapper Compute Utilization for a Link?

InterMapper queries a device at specified intervals, and requests a number of SNMP MIB variables. To compute utilization, InterMapper does the following:

1. It queries `ifInOctets` (and `ifOutOctets`) and the `sysUpTime` and `ifSpeed` variables.
2. It subtracts the octet counts from successive samples, and divides by the difference in the `sysUpTime` samples to compute a byte/second rate.
3. It divides the result by the `ifSpeed` variable to compute a percentage of the link's capacity/bandwidth. (If the user has overridden the `ifSpeed` variable, InterMapper uses the user-entered value.)
4. If a network is using a shared baseband link (such as Ethernet, wireless, etc.) InterMapper compares the sum of the transmitted and received bytes/second against the link speed to get the utilization.
 If it's a full-duplex link (such as a frame relay, T-1 or T3, ATM, etc.) then InterMapper compares the higher of the transmitted or received data rate against the link speed.

How Does InterMapper Compute Errors for a Link?

Q: A customer writes,

"I see the Received Discards/Minute and Percent Err values for an ATM AAL5 interface are non-zero and I would like to know which variables were used, and what calculation was used to arrive at these numbers.

"We are also graphing the Percent Err: value. This figure is showing errors and my Cisco support folks wanted to know which MIB variables go into the calculation of this percentage and how they are combined to create this number."

A: The Percent Err values were computed as follows:

The one-way percent errors under the Receive section are computed by totalling { ifInUcastPkts, ifInNUcastPkts, ifInErrors, ifInDiscards } as follows:

```
PERCENT ERROR = totalErrors / totalPkts;
```

where:

```
totalErrors = dErrs + dDis and  
totalPkts = dUcast + dNUcast + totalErrors
```

and:

```
dUcast = ifCurrStats.inUcastPkts - ifPrevStats.inUcastPkts  
dNUcast = ifCurrStats.inNUcastPkts - ifPrevStats.inNUcastPkts  
dErrs = ifCurrStats.inErrors - ifPrevStats.inErrors  
dDis = ifCurrStats.inDiscards - ifPrevStats.inDiscards
```

Note: Either of 'dErrs' or 'dDis' may be forced to zero if you have "IgnoreInterface Errors" or "Ignore Interface Discards" checked.

The one-way percent errors for outgoing traffic are similarly computed from the { ifOutUcastPkts, ifOutNUcastPkts, ifOutErrors, ifOutDiscards } statistics.

The two-way Percent error number (just below Utilization on the Interface information menu) is the probability given both one-way error percentages that a packet will be lost making the round-trip across the link and back. If the probability of successful transmission is T and the probability of successful receipt is R (and assuming the act of transmission and receive are relatively independent), then the probability of a successful round-trip is T * R. The probability of error is (1 - T*R).

T and R are computed from the complement of the one-way percent errors above.

Why can't I get a DHCP probe on OSX to work?

When running InterMapper on Mac OS X, you need to disable DHCP and PPP and assign a manually assigned static address to the computer running InterMapper.

To disable DHCP and PPP for all interfaces:

1. Open the Network settings in the System Preferences... application.
2. Choose "Network Port Configurations" from the Show: menu.
3. Disable any ports that have been configured to use DHCP or PPP, even if nothing is plugged into them and they aren't currently being used.
4. If DHCP or PPP is enabled on any interface of your machine, the process "configd" will open UDP port 68, and prevent InterMapper from using it. You can use the Terminal application to test if configd has port 68 open. Type 'sudo

`lsof -i | grep bootpc` and press return. If configd is listed, you still have DHCP running.

5. If InterMapper still marks the device as down after making these changes, you may need to use a DHCP Message Type of "DHCP-Discover" instead of the default "DHCP-Inform". This setting can be toggled in the DHCP/Bootp probe parameters dialog.

If I look at the traffic on a link, wait five seconds, and look again, the traffic rates are the same. Shouldn't these numbers be updated?

The traffic statistics are samples: the numbers do not change until after InterMapper probes the device again.

How does InterMapper compute byte and packet rates?

SNMP only supplies counts of bytes, packets, or errors, etc. that have passed through or occurred in an interface. These counts increment "forever" (or until the counter rolls over to zero like a car's odometer).

During each poll, InterMapper collects the total traffic and computes the difference with the total traffic from the previous poll. It then divides by the amount of time that has passed to compute the rate (per second or per minute).

Technical note: Even when a counter rolls over (e.g., from 999 to 000), InterMapper will compute the traffic rates accurately. Let's say the two successive samples are 995 and 003. InterMapper subtracts the previous count (995) from the new count (003), assumes that the "003" is actually "1003", and gets the proper difference of 8. Although the counters in the SNMP MIB variable are binary numbers, the same arithmetic principles hold. Thus InterMapper can compute these rates accurately.

How does InterMapper compute time intervals?

To compute the elapsed time accurately, InterMapper uses the `sysUpTime` variable of the device as a timestamp to calculate the time that has elapsed between subsequent two polls. The time elapsed should roughly correspond to the poll interval; however, it is possible for polls to be delayed occasionally so using the change in `sysUpTime` to measure the elapsed time is more accurate.

Chapter 14

Using InterMapper DataCenter

Configuring InterMapper DataCenter

InterMapper DataCenter is installed automatically when you install InterMapper.

Note: Unless you want to do one of the following, you do not to take any of the steps described in this topic:

- If you want to install and run InterMapper DataCenter from another machine.
- If you want to specify an outgoing email server for error and bug reporting.
- If you want to change the logging setup.

To open the InterMapper DataCenter web UI:

- From the Reports Server pane of InterMapper's Server Settings window, click **Configure...**
- Go to this URL:

<https://127.0.0.1:8182/>

Note: If this is a fresh installation, InterMapper DataCenter automatically generates an SSL certificate, used to encrypt communication with your browser and the InterMapper server. Because a new certificate is generated for every installation, the certificate cannot be signed by a recognized certificate authority. As a result, your browser may display a message alerting you to an invalid certificate. To avoid seeing the message in the future, choose the option to continue, and tell your browser to add the certificate to its list of trusted certificates. In some browsers, including Firefox, you may need to click a link on the warning page and use a separate pane to add an exception for the certificate.

You can replace the generated certificate with one of your own by visiting the Services List. Click the Change Settings link for the InterMapper DataCenter Daemon, once initial setup is complete.

Setting the Password for the Admin Account

Before you can use InterMapper DataCenter from another machine, you must set the password for the InterMapper DataCenter admin account.

To set the password for the InterMapper DataCenter admin account:

1. Click the **Settings** tab.
2. In the **Username** box, enter a username. The default username is "admin".
3. In the **Password** box, enter a password.
4. In the **Confirm Password** box, re-enter the password.
5. Click **Save Settings** at the bottom of the page.

Note: By default, you can log in to InterMapper DataCenter from the machine it is installed on without any authentication. You can choose to force authentication even on the local machine by unchecking the **Skip authentication for local connections** box, and creating a password as described above.

If you are planning to use an existing database, you are now ready to [configure it \(Pg 615\)](#). If you are planning to use [InterMapper Authentication Server \(Pg 623\)](#), you are also ready to configure it now.

Setting Up InterMapper DataCenter Logging and Event Collection

InterMapper DataCenter can log status information, connection attempts by InterMapper servers, and error information obtained when connecting to directory services. InterMapper DataCenter logs to a file called *log/imdc.log* within the IMDC install folder. For the location of the log file for your platform, see [InterMapper Files and Folders \(Pg 628\)](#).

To set the logging level:

1. Click the **Log** button in the upper-left corner of the page. The Log Viewer appears.
2. From the **Logging Level** dropdown menu, choose the level you want to use.
3. Click **Save**. The InterMapper DataCenter installation is complete.

Setting up InterMapper DataCenter's Error Reporting

InterMapper DataCenter can report problems and send bug reports to InterMapper Support. To do this, you need to specify one or more SMTP hosts and user information.

To set up error reporting:

1. In the InterMapper DataCenter section of the InterMapper DataCenter home page, click the **Settings** tab. The DataCenter Settings page appears.
2. In the Primary SMTP section of the Error Reporting section, enter a **Host**, **Port** (if different from the default), a valid **Username** and **Password** for the email account you want to use to send messages, and a **From** address for the messages. Enter (optional) SMTP settings for a secondary SMTP host.
3. To send an E-mail notification when an error occurs in InterMapper DataCenter, click to select the **On errors, send E-mail to** check box.
4. To send an email notification to Help/Systems when an error occurs, click to select the **Automatically E-mail bug reports to Help/Systems** check box.
5. To test your SMTP connection, click **Send Test E-mail**. A test email message is sent to the specified address.

Using an Existing Database

InterMapper makes it easy to install and run InterMapper Reports Server using the built-in PostgreSQL database. The database is installed, configured, and registered automatically. To use InterMapper Reports Server, you need only to start the server so that InterMapper reports to it.

If you prefer, you can use another instance of a PostgreSQL database, running on the same machine or on another machine. See [Configuring the Database](#) below.

Configuring the Database

Use this section only if you want to use an existing PostgreSQL database, regardless of whether it is running on the same machine as InterMapper or on a different machine.



InterMapper Database

Status: **not yet configured**

Click **Configure** to set up the connection to the database.

[Configure](#)

Use the InterMapper Database section of the InterMapper DataCenter Administration Panel to configure the InterMapper Database used by the Reports Server.

Configuring a New Installation

When configuring a new installation, follow these steps.

- **Step 1: Choose and configure database to connect to**, or use the default Built-in database.
- **Step 2: Register your InterMapper Server** with the InterMapper Reports server.

Step 1: Database Configuration

- A. Choose whether to use the Built-in database, or to connect to an existing external (PostgreSQL) database.
- B. If you choose to use the **Built-in** database, an *intermapper* account is created automatically for InterMapper to use, so you can click **Continue** without adding any additional accounts. You have the option to create one or more user accounts when the database is installed.

(You'll need an additional user account if you want to use pgAdmin, Perl, PHP, Crystal Reports, or some other method to retrieve information from InterMapper Reports Server. If you wish, you can add them later.)

- C. If you choose to use an existing database, enter a **Host**, **Port**, **Database Name**, **Database Username**, and **Database Password** in the appropriate boxes and click **Continue**. You are finished with Step 1.

Note: The user you specify must have, at minimum, CREATE, TEMPORARY,

and CONNECT privileges in order for InterMapper to log data to the database.

- D. If you want to add users, click **Add** to add a user. An unnamed user appears in the User List at left.
- E. Enter a user name in the **Username** box.
- F. Enter a password in the **Password** box and in the **Confirm Password** box.
- G. Select or clear the **Write Access** check box to choose whether a user can make changes to tables (as through pgAdmin).
- H. By default, users can access the database only from the same host as it is running on. Select or clear the **Remote Login** check box to choose whether to grant a user access from any machine on the network.
- I. To create more users, repeat steps D through H.

Step 2: Register your InterMapper Server with the InterMapper Database server

- A. If InterMapper Reports detects an InterMapper server running on the same machine, you are given the option to register that server to export data to the InterMapper Reports Server.
 - 1. Click **Register Server**. The existing server is registered with InterMapper Reports Server, and you are presented with the option of registering additional servers.
 - 2. Click **Instructions**, and follow the instructions for each InterMapper server you want to register.
 - 3. Click **Finish**. The InterMapper DataCenter home page appears, showing that the InterMapper Reports Server is running.

If InterMapper Reports Server is installed on a different machine, you'll need to register your InterMapper server(s) manually. Click **Register Server Manually**.

- B. In InterMapper, view the Server Configuration > Reports Server pane of the Server Settings panel, click **Start**. InterMapper begins sending data to InterMapper DataCenter.

Changing Settings After Installation

InterMapper DataCenter is installed automatically when you install InterMapper. Once you have configured InterMapper Database, you can change settings as needed from the InterMapper DataCenter Administration Panel.

To change the settings in the InterMapper Database:

- From the InterMapper DataCenter's Home page, click ***Change Settings*** in the InterMapper Database box. The InterMapper Database Settings Page appears.

To view the InterMapper Database log:

- In the InterMapper Database section of the DataCenter Administration Panel, click the ***Log*** tab. The InterMapper Database log page appears.

About Retention Policies

You can use data retention policies to average raw data, reducing the amount of data stored. Data retention policies control how often and how much data is averaged, and reduced.

A data retention policy can be applied to a specific map, to one or more devices or interfaces on a map, to an individual dataset, or to all maps on an InterMapper Server. Policies also affect the way InterMapper stores chart data.

Using Data Retention Policies

Use the Retention Policies pane of the Server Preferences section of the Server Settings window to create and edit retention policies that can be used to specify how data is stored for a particular device or map. For more information, see [Retention Policies \(Pg 274\)](#).

Configuring InterMapper Database Logging Preferences

Use the InterMapper DataCenter's Log tab to view recent log entries, to set the level of logging you want to the InterMapper Database to use, and to set preferences for the Log tab.

To change the settings of the Service Log File page:

- Make the changes you want, and click **Save Settings**.

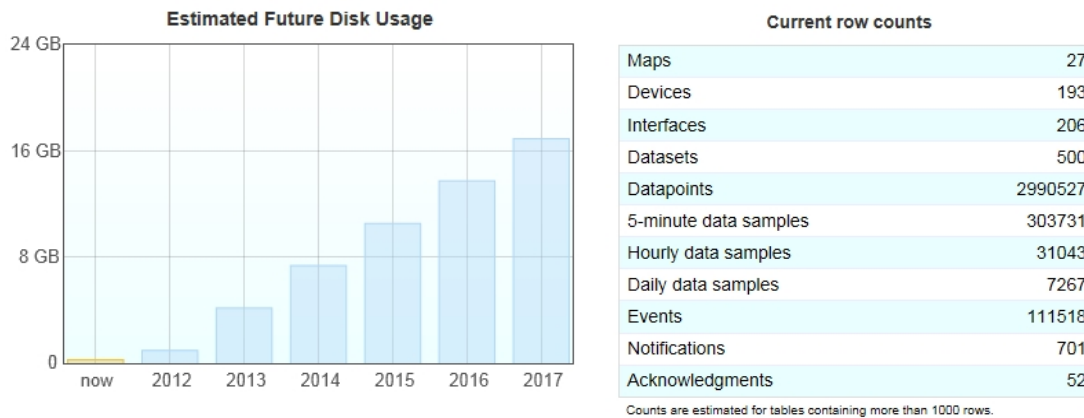
Log levels Explained

From the Logging Level dropdown menu, choose the logging level you want to use, as follows:

- **Full Debug** - Log minor details such as values read from configuration files and chunks of data arriving as part of directory responses.
- **Connections** (default) - Log authentication attempts, connections by the InterMapper server, and outgoing data.
- **Information** -Log web admin panel logins, changes to configuration and scheduled server tasks.
- **Errors Only** - Log only serious errors, indications of future errors, and possible security problems.

Reviewing Database Disk Usage

You can view disk usage statistics from the InterMapper Database's Overview page. The following statistics are available:



How Statistics are Calculated

- Estimated future disk usage is calculated based on the number of devices, datasets, and how retention policies are configured.
- With the exception of **Datapoints**, each row count corresponds to a specific database table, and indicates the number of records in that table. For tables with more than 1000 rows, the value is estimated.
- **Datapoints** is an estimated value.

To view database disk usage statistics:

- From the InterMapper DataCenter's **Home** tab, click **Overview**. The Overview page appears, showing disk usage statistics.

Configuring Automatic Database Backups

InterMapper Database can automatically create back-ups of its built-in database. Please keep in mind that creating a backup can consume a lot of disk space, and takes time to complete.

To set up automatic backups:

1. From the InterMapper Database Settings page, click **Automatic Backups**. The Automatic Database Backups page appears.
2. Set the period you want to use for backing up. You do backups daily or weekly.
3. For daily backups, set the time you want the backup to start. For weekly backups, set the day and time.
4. Specify the maximum number of backups you want to store. Once this number of backups is reached, the oldest backup is deleted each time a new one is created.
5. Click **Save Settings**. The backup settings are saved, and backups are created according to the specified schedule.

Creating an unscheduled backup

You can create a backup at any time.

To create a backup:

- Click **Create Backup**. A new backup file is created immediately. The backup starts immediately. When finished, the backup file is listed in the **Available Backups** box.

Restoring a previous backup

You can restore a previous backup.

1. In the **Available Backups** box, click the backup file you want to restore.
2. Click **Restore**. Data from the selected backup is restored to the InterMapper Database.

Viewing backup progress and canceling backups

When a backup is underway, you can view its progress from the Automatic Database Backups page. You can also cancel a backup while it is under way.

To view backup progress or cancel a backup:

- While the backup is under way, go to the Automatic Database Backups page. The progress bar appears.
- Click **Abort** to cancel the current backup.

Performing Maintenance Tasks

Use the Maintenance Tasks page to perform these maintenance tasks.

- **Pause Operations** - Sometimes it can be useful to pause import, without stopping the database entirely. This allows you to manually re-cluster or re-index tables, or avoid errors when the InterMapper Server goes down for maintenance. Specify the interval for which you want to pause, then click **Pause Operations**. A Resume Operations button and countdown clock appear. To resume operations at any time, click **Resume Operations**.
- **Data to Delete** - Data retention policies are the recommended way to free disk space on a per-dataset basis. You can also delete data or events across all devices, or you can delete data for deleted devices and interfaces. Please be aware that this operation is permanent and cannot be undone. Specify which data you want to delete (raw data, data samples, events, or data from deleted devices), and a time period over which you want to delete them, then click **Delete**.
- **Apply Retention Policies** and **Reclaim Disk Space** - Retention policies are applied daily, and a maintenance task runs once each week to reclaim unused disk space. You can run both of these tasks manually using these buttons. Both operations can take from a few minutes to a few hours to complete, depending on the size of your database. See [About Automatic Maintenance Tasks](#) below for more information.

About Automatic Maintenance Tasks

Two tasks are run automatically to clear out data that is beyond its retention policy expiration, and to reclaim unused disk space.

- **Daily task** - runs at 1AM local time each day. It applies retention policies, then uses the PostgreSQL VACUUM command to mark free space for re-use by the database. This is a relatively low-impact process, and does not pause database operations. It does not release disk space for reuse by the operating system.
- **Weekly task** - runs at 1AM local time each Sunday. It uses the PostgreSQL CLUSTER command, and pauses database operations while it runs. This task frees up unused database space, making it available to the operating system.

After you have run one of these tasks, the Disk Usage table shows the freed disk space as available.

Using the InterMapper Authentication Server

Use the InterMapper Authentication Server to authenticate InterMapper users through an external authentication directory.

Overview

The InterMapper Authentication Server (IMAuth) is a component of the InterMapper DataCenter (IMDC) add-on package. It lets an InterMapper server authenticate users against an external authentication directory. IMAuth supports LDAP, RADIUS, ActiveDirectory, IAS, Kerberos, and DND directories.

IMAuth acts as an intermediary between an InterMapper server and the directory. If an authentication request comes in from a user whose password is not in InterMapper's local user database, the InterMapper server forwards that request to IMAuth. IMAuth translates and passes the request to the directory server, and forwards any responses it receives back to the InterMapper server. In addition, a new user entry is created in the local database, configured for external authentication and assigned to a default group you will have specified for users created this way.

IMAuth is not a replacement for InterMapper's local user database. You may continue to keep some user passwords in InterMapper's local user database for local authentication while requiring others to be authenticated via IMAuth. For each user, you must choose one method or the other.

Select the "Use External Authentication" check box in the **Edit User** or **Create User** dialog to indicate that the user should be authenticated via IMAuth, in which case you should not supply a password. For more information on creating and editing users, see [Users and Groups \(Pg 298\)](#).

Installing the Authentication server

InterMapper Authentication Server runs as a component of InterMapper DataCenter and is installed automatically when you install InterMapper. On Windows and MacOS X, IMDC is installed automatically alongside InterMapper. On other platforms, you need to download and install IMDC separately.

Configuring and connecting to your directory

You need to configure the InterMapper Authentication Server to talk to your directory server. This is done from InterMapper DataCenter's web administration page. To do this, start IMAuth Server as described above, then open a web browser and navigate to: <https://localhost:8182>. You can also click **Configure...** in the Reports Server pane of the Server Settings window.

1. Configure the connection to your authentication directory (LDAP, Radius, ActiveDirectory, Microsoft IAS, Kerberos v5, DND).
2. Configure the connection that an InterMapper server uses to connect to IMAuth.
3. Configure InterMapper to connect to IMAuth.

Tips and Hints for Various Authentication/Directory Servers***RADIUS / IAS***

IMAuth acts as a RADIUS client, and so it must be added to the clients section of your RADIUS configuration file or, for Microsoft IAS, the clients section of the IAS configuration pane. You are asked to specify a *secret*, and must then enter exactly the same secret in the IMAuth RADIUS settings.

LDAP

If you encounter any problems, first try un-checking the *Use SSL* option, or choose *Whenever Necessary* for the *Use Plaintext* option in the IMAuth LDAP settings. If this works, it means your server wasn't built to include SSL or SASL DIGEST-MD5 password encryption. You'll need to either stay with the lower IMAuth security settings, or upgrade your LDAP server.

Another thing to look at is the LDAP Base DN specified in the IMAuth LDAP settings. This tells IMAuth where in your LDAP directory the user entries are located. This depends on how your directory was set up, but usually takes the form:

`ou=people,dc=example,dc=com`, where *example* and *com* correspond to the domain name your directory was set up with. IMAuth takes the Base DN and attaches the user's name; for example:

`cn=Jane,cn=Smith,ou=people,dc=example,dc=com`.

ActiveDirectory

ActiveDirectory is based on LDAP, but differs slightly in its default configuration. If you are encountering problems with these ActiveDirectory versions, try un-checking the *Use SSL* option or choosing *Whenever Necessary* for the *Use Plaintext* option in the IMAuth LDAP settings. The Base DN for an ActiveDirectory server will almost always be: `cn=Users,dc=example,dc=com` where *example* and *com* are replaced by the name of the Windows Domain that ActiveDirectory is serving.

Since ActiveDirectory is built around the idea of domains rather than single servers, the username you use to authenticate must have your domain name attached to it. For example, if your normal Windows logon name is *janesmith* and your domain is *example.com*, the username you give when accessing a map with InterMapper or InterMapper RemoteAccess is *janesmith@example.com*.

Almost all ActiveDirectory versions support SSL. If you have provided your own certificate, choosing the *Whenever Necessary* option for the *Use Plaintext* field in the IMAuth LDAP settings doesn't have much impact on your security. If you really do need the additional encryption, you must perform these steps:

1. Log in to your server as an administrator, and start the *Active Directory Users and Computers* panel.
2. Open the properties for each user who needs to authenticate, and switch to the *Account* tab.
3. Under *Account options*, check the *Store password using reversible encryption* box.

Note: Windows cannot apply the change immediately, so you must get that

user to log on to the Windows domain as normal (by signing on to their machine, for example) before the change becomes active.

In this case you might again need to use a different username. Instead of the usual login name, you may need to use the user's full name. For example, instead of *janesmith* you would use *Jane M. Smith*.

When setting up IMAuth, it's a good idea to try the normal login name, the login name with your domain attached, and the user's full name, to see which login your ActiveDirectory server accepts.

Kerberos

For a good introduction to Kerberos, see the following Knowledgebase article:

- [Using Kerberos with InterMapper](#)
- [Supported Kerberos encryption modes](#)

Problems encountered when using Kerberos are usually caused by misconfiguring the InterMapper Authentication Server, or by the values used when creating the `imauth` service account.

- **Kerberos Domain** - The name, of the Kerberos authentication realm. It is typically all uppercase (Example: `INTERMAPPER.COM`). On Windows, it is almost always the same as the ActiveDirectory domain's name, but upper-cased.
- **KeyServer Address** - The full domain name of the Kerberos key server. On Windows, even on complex networks with multiple ActiveDirectory nodes, only one acts as the Key Distribution Center. The **KeyServer Address** value must match the machine's name *exactly*. For example, if the machine is registered on the network as `ad.intermapper.com`, the **KeyServer Address** must be `'ad.intermapper.com'`; entering the IP address of the machine, or just `'ad'`, causes authentication failures.
- **Service Principal** - The service principal name associated with IMAuth on the domain. This is typically the service name (`imauth`) followed by a forward slash and then the Kerberos key server's full domain name. For example, on Windows, assuming you follow the instructions in the Knowledgebase link above, and created an ActiveDirectory service account called `'imauth'`, the Service Principal value would be `'imauth/ad.intermapper.com'`. This user account *must also be active* in ActiveDirectory; disabling the account is a common mistake that causes authentication failures.

Data Collecting and Reporting

Use the InterMapper Reports Server to collect data you can use for analysis and to create custom reports.

InterMapper Reports Server is a module of InterMapper DataCenter. [InterMapper DataCenter \(Pg 613\)](#) is installed automatically when you install InterMapper Server on Windows and Mac OS. It is a separate download on other platforms.

Use the Reports Server panel, available from the Server Configuration section of the Server Settings panel, to start and stop collecting data. You can also configure InterMapper to connect to a remote database server, and specify the intervals at which data is stored. For more information, see [Reports Server \(Pg 285\)](#).

Collecting Data for a Device or Interface

You can collect data for any device in any map. Use the Set Data Retention command, available from the Monitor menu or the device or interface's **Set Info** context menu to specify how long the data from the device or interface is retained, and at what resolution.

The default server-wide Data Retention Policy is **24 Hours** (except for devices and interfaces associated with charts created in 4.6 or earlier). You can also create and select a different retention policy as the server-wide default policy:

- For all *maps*, choose **Inherit** to use the specified server-wide default policy, as set in the Server Settings window. You can also specify a default Data Retention policy for a map that is different from the server's default policy.
- For all *devices*, choose **Inherit** to use the specified map-wide default policy, as set in the Map Settings window. You can also specify a default Data Retention policy for a device that is different from the map's default policy.
- For all *interfaces*, choose **Inherit** to use the specified device policy, as set in the Device Info window. You can also specify a default Data Retention policy for an interface that is different from the device's policy.
- For devices and interfaces associated with charts created in 4.6, the default Data Retention policy is **IM46Charts**.
- If you do none of the above, the default server-wide policy is applied automatically.

Note: Data Retention Policies are applied individually, not in sequence. For example, specifying an hourly data expiration of two days now causes hourly samples to be deleted after two days, instead of two days plus the raw and custom expirations.

Retention Policies in Status and Info Windows

A device or interface's current Retention Policy is shown in the Status and Info windows. In the Status window, the information appears as follows:

```
Retention Policy: PolicyName, [Not] Exportable
```

- **Policy** - the policy name as created in InterMapper Reports Server.
- **Exportable/Not Exportable**
 - **Exportable** appears if the parameters of the policy are such that they cause data to be exported to the database.
 - **Not Exportable** appears if the parameters of the policy are such that they will not cause data to be exported to the database (the None policy, for instance).

Getting Data From the Database

The Reports Server is the easiest way to get data from the Reports Server database, but you can use your own method for retrieving data from the InterMapper Database using SQL queries. There are several example reports written for Crystal Reports and OpenRPT, as well as several perl scripts available. For more information, see *Retrieving Data From the InterMapper Reports Server* in the Developer Guide.

Chapter 15

InterMapper Files and Folders

InterMapper saves its files in specific folders. In particular, the following file and folders have special locations:

- **The InterMapper application folder** - If applicable, it contains the actual InterMapper Application.
- **The InterMapper RemoteAccess application folder** - If applicable, it contains the actual InterMapper Application.
- **The InterMapper Settings folder** - Contains all InterMapper server settings file as well as several folders containing various information used by InterMapper. For detailed information its contents, see [InterMapper Settings \(Pg 632\)](#).
- **The InterMapper DataCenter folder** - contains the data storage for all installed components of InterMapper DataCenter, as well as a number of other files. For detailed information on the contents of the InterMapper DataCenter folder, see [InterMapper DataCenter Folder \(Pg 634\)](#).
- **The InterMapper Flows folder** - contains data storage for Flows data as well as a number of other files.

File Locations

The locations of these files and folders differ slightly between operating systems as described below.

InterMapper Application Folder

OS	Location of InterMapper Application files
<i>Windows 32 & 64-bit</i>	C:\Program Files\InterMapper or specified location.
<i>Mac OS X</i>	Binary files (intermapperd, intermapperauthd) are placed in /usr/local/bin, unless a different location was chosen at installation.
<i>Linux</i>	Binary files (intermapperd, intermapperauthd) are placed in /usr/local/bin, unless a different location was chosen at installation.

InterMapper Settings Folder

For detailed information on the contents of the InterMapper Settings folder, see [InterMapper Settings \(Pg 632\)](#).

OS	Location of InterMapper Settings files
<i>Windows</i>	C:\ProgramData\InterMapper\InterMapper Settings or specified location.
<i>Mac OS X</i>	As specified in /etc/intermapperd.conf (Usually /Library/Application Support/InterMapper Settings/)
<i>Linux</i>	As specified in intermapperd.conf (Usually /var/local/InterMapper_Settings/)

InterMapper RemoteAccess Application Folder

OS	Location of InterMapper RemoteAccess files
<i>Windows 32-bit</i>	C:\Program Files\InterMapper RemoteAccess
<i>Windows 64-bit</i>	C:\Program Files (x86)\InterMapper RemoteAccess
<i>Mac OS X</i>	Drag and drop to location of your choice.
<i>Linux</i>	Installed at location where .bin file is run.

InterMapper DataCenter Folder

For detailed information on the contents of the InterMapper DataCenter folder, see [InterMapper DataCenter Folder \(Pg 634\)](#).

OS	Location of InterMapper DataCenter files
<i>Windows 32 and 64-bit</i>	C:\Program Files\intermapper\dwf
<i>Mac OS X and Linux</i>	/usr/local/imdc

InterMapper Flows Folder

OS	Location of InterMapper Flows files
<i>Windows 32 & 64 bit</i>	<ul style="list-style-type: none">• (Flows files) C:\Program Files\InterMapper\flows• (Database) C:\ProgramData\InterMapper\InterMapper Settings\Flows\SESSIONDB
<i>Mac OS X</i>	<ul style="list-style-type: none">• (Flows configuration files) /Library/Application Support/InterMapper Settings/Flows• (Database) /Library/Application Support/InterMapper Settings/Flows/SESSIONDB• (Logs) /Library/Application Support/InterMapper Logs/flows-stderr.txt, flows-stdout.txt, flows.log
<i>Linux</i>	<ul style="list-style-type: none">• (Flows files) /var/local/InterMapper_Settings/Flows• (Database) /var/local/InterMapper_Settings/Flows/SESSIONDB/

Making Backups

InterMapper saves its state the *InterMapper Settings* folder.

As described in [InterMapper Files and Folders](#), the InterMapper Settings folder is in different locations, depending on whether it is installed in Windows or Unix/Linux/Mac OS X.

To backup InterMapper on any of these systems,

- Back up the *InterMapper Settings* folder.

Note: When making backups of the InterMapper Settings folder on Windows installations, it is important to stop the InterMapper Server before making a backup, or make sure that your backup mechanism allows files to be accessible by InterMapper simultaneously. Opening certain types of chart or log files can cause them to be inaccessible to InterMapper, causing the InterMapper Server to stop abruptly.

Retaining Copies of Maps in Older Formats

A new version of InterMapper can use a file data structure which is different from previous versions. To preserve the ability to "go back" to an earlier version, InterMapper creates a copy of the current maps when you install a new version of InterMapper, named with the new version number. This becomes the copy that contains active maps.

The old maps are moved to a folder named with the previous version number. If you need to revert to an earlier version of InterMapper, you can get your original maps from the folder whose name corresponds with the version you want to run. In subsequent releases, the folder that corresponds to the current version is used automatically.

The InterMapper Settings Folder

The InterMapper Settings folder contains all the settings, preferences, and configuration of InterMapper. The location of this folder varies, depending on your platform. For more information, see [Files and Folders \(Pg 628\)](#).

The InterMapper Settings folder contains the following items:

- **Certificates folder** - Contains certificates used by secure servers to verify that they are the InterMapper servers they claim to be. Also contains key files and pending certificate signing requests.
- **Chart Data folder** - Contains the saved data of charts. When InterMapper starts up, it reads the data from these files to restore the charts' history.
- **Custom Icons folder** - Contains custom icons you add to maps to enhance InterMapper's built-in icon set. See [Custom Icons \(Pg 101\)](#) for details about making and adding custom icons.
- **InterMapper Logs folder** - Contains text files that log events that InterMapper has detected.
- **InterMapper Prefs file** - Contains the current settings of all InterMapper preferences.
- **Maps folder** - Contains maps saved from InterMapper. All maps in this folder are opened automatically when you start InterMapper.
 - **[Version Number] folder** - For each version of InterMapper that has been installed, (starting with 5.4) a new folder is created for each version. Maps from a previous version are copied into the new folder, which becomes the active maps folder. The folder for each new version contains a Disabled folder and a Deleted folder.
 - **Enabled folder** - Contains maps that have been disabled by removing the check mark in the Map Files panel of the Server Settings window.
 - **Disabled folder** - Contains maps that have been disabled by removing the check mark in the Map Files panel of the Server Settings window.
 - **Deleted folder** - Contains maps that have been removed using the Map Files panel of the Server Settings window.
 - **Backups folder** - Contains backups created using the Backup command.
- **MIB Files folder** - Contains SNMP MIB files that ship with the product, or have been added using the **Import > MIB...** command. InterMapper parses the MIB files in this folder and uses the information to convert between variable names and OIDs.
- **Probes folder** - Contains built-in and custom probes. Probes are text files that add functionality to InterMapper so that it can test new devices. See Customizing InterMapper's Probes for details about creating and customizing probes.

Note: Built-in probes are stored in a ZIP archive named *Built-inProbes.zip*. To view or modify a built-in probe, you'll need to unzip the archive. InterMapper scans the archive as well as the unzipped contents

of the folder. If a built-in probe's filename matches an unzipped version, the probe's version number, then the last-modified date, is used to determine which probe is the most recent. If you are developing or modifying a built-in probe, be sure to advance the version number to be sure that InterMapper uses the modified version.

- **Sounds folder** - Add .aiff, .wav, and other sound files to this folder to make them available for InterMapper notifications. For more information on sounds and how to use them, see [Configuring a Sound Notifier \(Pg 142\)](#)
- **Web Pages folder** - Contains the template and target files that describe the web pages that the InterMapper server displays. See Customizing Web Pages for details about customizing these pages.
- **InterMapper User List folder** - Previous versions of InterMapper kept the user list in a separate file. Now, these user and group settings have been incorporated into the *InterMapper Prefs* file. You may leave this file in place without affecting InterMapper's operation.
- **Tools folder** - Contains executable files (or aliases/links/shortcuts to them) that will be used as command-line probes or notifiers.
- **Fonts folder** - (optional) Contains TrueType fonts used by the web server.

Note: On Windows machines, the Windows font directory is also available, giving access to all available TrueType fonts installed on the machine. On Macs, InterMapper looks in */Library/Fonts* and */System/Library/Fonts*, as well as in the */InterMapper Settings/Fonts* folder.

- **Temporary folder** - When files are uploaded, they are initially uploaded and saved into this directory until the upload is complete. At that point, they are moved into a more appropriate directory. If something goes wrong, and an upload is interrupted, a file may remain in the "Temporary" directory.

When you exit InterMapper, it leaves the files in the Temporary directory alone, so debugging information can be collected. When InterMapper starts up, it checks the Temporary directory, and deletes all files in it. Therefore, InterMapper users should not rely on the contents of the Temporary directory remaining long, and should not park files there.

InterMapper DataCenter Folder

The InterMapper DataCenter folder, named `dwf` on Windows systems and `imdc` on Mac/Linux/Unix systems, contains a number of folders related to InterMapper DataCenter and its components. The folder location depends on the operating system. For more information, see [InterMapper Files and Folders \(Pg 628\)](#).

Folders common to all platforms

All platforms contain the following folders:

- **config** - Contains the database storage, including configuration information for InterMapper DataCenter and its components.
- **core** - Contains InterMapper-distributed versions of PostgreSQL and Python, as well as license information about third-party products used or distributed.
- **imauth** - Contains python objects, HTML, text, etc., for the InterMapper Auth Server component.
- **imdatabase** - Contains python objects, HTML, text, etc., for the InterMapper Database component.
- **imdc** - Contains python objects, HTML, text, etc., common to all IMDC components and for the InterMapper DataCenter setup, configuration, etc.
- **imreports** - Contains python objects, HTML, text, etc., for the InterMapper Reports component.
- **log** - Contains logs for all InterMapper DataCenter components.

Platform-specific folders

Mac OS

The Mac platform also contains:

sbin - This contains a script used by `launchctl` to start and stop the InterMapper DataCenter daemon.

Linux/Unix

The Linux/Unix platform also contains:

sbin - This contains a script used by the platform's load daemon to start and stop the InterMapper DataCenter daemon, as well as assorted other scripts.

Chapter 16

Importing and Exporting Maps

Exporting Data From Maps

InterMapper exports data about the devices on its maps. This makes it possible to use the map data in a number of ways, for example:

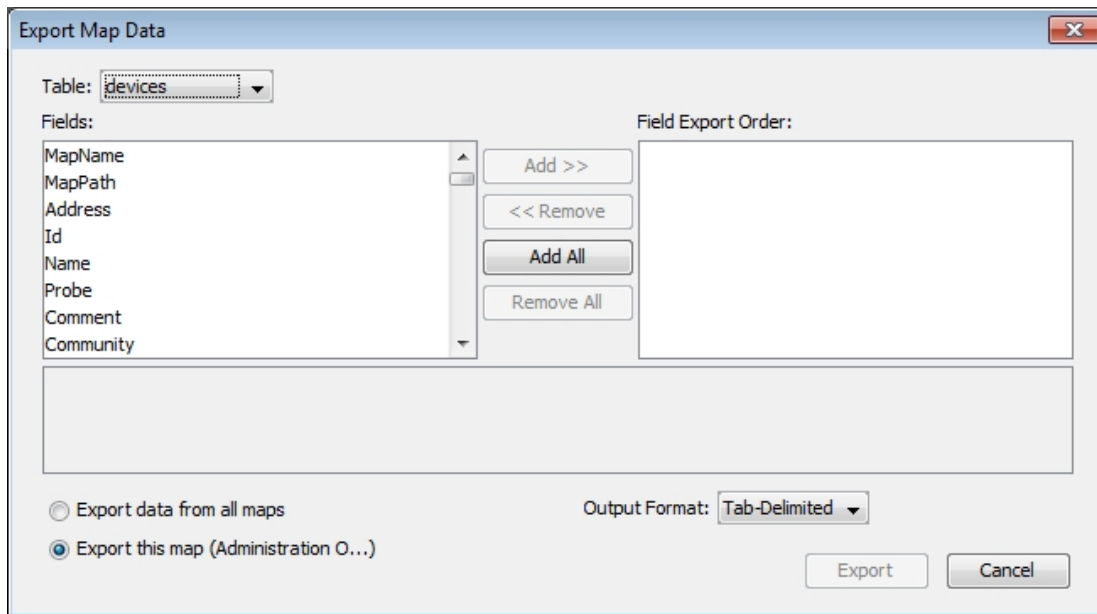
- To review the map's configuration to check for consistency
- To edit the map data using some external tool, and then re-import it (using the [Import Command \(Pg 637\)](#)) back into the map, updating the affected devices.
- To use the configuration in some down-stream application

You can export data for *all maps*, for *the current map*, or only for *selected items in the current map*.

Note: You can automate the exporting of map data by sending commands to InterMapper RemoteAccess through its command-line interface or through the HTTP API. This allows you to interact with InterMapper through your own scripts. For more information, see [Command-line options for RemoteAccess](#), (in this manual) as well as *InterMapper HTTP API* in the [Developer Guide](#).

Types of data you can export

Map	Save a copy of the map from the server on which it's running to a file on a local computer. A standard File Save dialog appears.
Data file	<p>Save a text file containing information about a map in one of these formats:</p> <ul style="list-style-type: none">• Tab-delimited - creates a text file with all field data separated by tab characters.• CSV - creates a text file with all field data separated by commas.• HTML - creates a text file containing field data in HTML tables.• XML - creates a text file containing field data in XML format.
Image file	<p>A standard File Save dialog appears.</p> <p>Save a PNG image of the current map. A standard File Save dialog appears.</p>



The Export Map Data window.

To export map data:

1. From the File menu's Export submenu, choose **Data File...** The Export Map Data window appears as shown below.
2. From the **Table** drop-down menu, choose **devices** (device attributes), **vertices** (appearance attributes), **maps**, **notifiers**, **users**, or **schema** (output file attributes).
3. From the **Fields** box, click to choose the fields you want to export. *Shift-click* to select a contiguous series, or *Ctrl-click* to choose non-contiguous fields.
4. Click **Add>>**. The selected fields appear in the **Field Export Order** box. If you want to export all fields, click **Add All**.
5. In the **Field Export Order** box, drag the field names up or down to set the order you want the fields to appear in the export file.
6. Click to choose **Export data from all maps** or **Export this map**.
7. If you want to export data only for the selected items on the map, click **Only export selected items**.
8. From the **Output format** drop-down menu, choose **Tab-delimited**, **CSV**, **HTML**, or **XML**. For information on these formats, see the table above.
9. Click **Export**. A standard File Save dialog appears.
10. Choose a name and location for the export file, and click **Save**. The export file is saved in the specified location.

Importing Data

InterMapper can import data from a text file to update information about devices on a map, or information about Users or Groups. This is useful for:

- New customers who want to import the devices/probe types from their current monitoring system (or information that's already present in a spreadsheet or other format) into InterMapper.
- Customers who make frequent updates to existing devices on maps.
- Customers who frequently add new devices to maps. They want to enter information about new customers to a database, then export the new device information to a file that can be bulk-imported into InterMapper.
- Customers who want to make systematic changes to their maps. They can export the InterMapper map as, say, tab-delimited data, then edit columns in a spreadsheet/database, then re-import, letting InterMapper merge the new information onto the existing devices. This is useful for wholesale label changes, switching IP addresses, etc.
- Customers who want to import a list of users from another source for authentication purposes.

To import data:

1. Create an import file as described in [Creating an Import File \(Pg 638\)](#).
2. In the Map List window, click to select the server to which you want to import map data, or open a map on that server.

Note: The import file contains the name of the map. If the map does not exist, it is created automatically.

3. From the File menu's **Import...** submenu, choose **Data File...** A standard file dialog appears.
4. Select the file you want to import and click **Open**. If the map data is valid, devices are added or updated on the specified maps as appropriate. If the specified map does not exist, one is created automatically.

Note: You can automate the importing of map data by sending commands to InterMapper RemoteAccess through its command-line interface or through the HTTP API. This allows you to interact with InterMapper through your own scripts. For more information, see [Command-line options for RemoteAccess](#), (in this manual) as well as *InterMapper HTTP API* in the [Developer Guide](#).

When importing data in Tab/CSV/XML formats, foreign characters must be presented in the same way as the output of the **Export** command:

- Characters with values less than 255 can be imported directly.
- Character values greater than 255 must be escaped using the standard XML format (`&#[character code]`).

Creating An Import File

Since a missing tab can cause errors in an import by causing data to be imported into the wrong fields, creating a file from scratch in a text editor is relatively error-prone. The following methods are recommended for creating import files quickly and accurately:

- [Export a map \(Pg 635\)](#), then edit the file.
- [Use a spreadsheet application \(Pg 639\)](#) such as Excel to create a tab-delimited file.
- Generate a file algorithmically from a database. This may be useful if you plan to update maps regularly.

An import file is text file, formatted as follows:

- **The first line of the file specifies the format of the following lines** - it specifies the file format ("tab" in the example below), the table to be filled ("devices") and the order of the fields. Three fields must be specified: MapName, Address, and Probe; the remaining fields are optional.
- **Remaining lines contain the data for the devices you want to import** - Each device occupies a single line, and the data columns are separated by tabs (a "tab-delimited" file.) Each column corresponds to a field in the **fields** specification of Line 1.

Line 1 - specifying the format for the import file data

The first line of the file determines the method you are going to use for importing, and can provide you with a significant amount of control over how devices are imported. There are two different methods you can use for importing; each uses a different format for the first line of the file:

- **Spreadsheet-style import** - This technique is used only for adding new devices to a map. The first line of the file contains the column names associated with the data in the remaining lines. This is the recommended method. Once you have created this file, it is easy to change the first line to a Directive line.
- **Directive line** - This method gives you a large amount of control over the import process. In addition to inserting new devices, you can update specific attributes of existing devices, change their appearance or location, and delete them. This technique is documented in [Advanced Data Importing \(Pg 649\)](#) in the References section.

Notes:

- For either style of importing, data is set only in those fields whose **Access** value is specified as "READ-WRITE" in the *Device Attributes* and *Vertex Attributes* topics, found in the [Advanced Data Importing \(Pg 649\)](#) in the References section.
- Text files should be encoded in UTF8 format.
- Characters with values less than 255 can be imported directly.
- Character values greater than 255 must be escaped using the standard XML format (`&#[character code]`).

Spreadsheet-style Import file

The recommended format for creating an import file is a spreadsheet style format, in which the first line contains tab-separated column names that correspond to the remaining rows:

```
LabelTemplate MapName Address
Machine1 Map1 192.0.0.1
Machine2 Map1 192.0.0.2
```

This is the equivalent of the following directive line, as explained below:

```
# format=tab table=devices fields=LabelTemplate,MapName,Address insert=LabelTemplate,MapName,Address
Machine1 Map1 192.0.0.1
Machine2 Map1 192.0.0.2
```

Notes:

- If you have created a spreadsheet-style import file, you can easily change it to a *Directive line-based* file for updating the map.
- You can include columns in your import file from both the Device and Vertices tables. InterMapper automatically applies the Vertex attributes appropriately.

The columns are imported in the order specified. The last value specified takes precedence over previous values in the same line. Because of this, Help/Systems recommends that you use only one of the following columns when importing. If more than one of these is specified, and there are conflicts, the last column's values are used:

- **Address**
- **DNSName**
- **IMProbe**

For a complete list of device attributes and corresponding field names, see *Device Attributes* in [Advanced Data Importing \(Pg 649\)](#) in the References section.

The Directive-Line

Using the Directive Line technique, in addition to inserting new devices, you can update specific attributes of existing devices, change their appearance or location, and delete them. This technique is documented in [Advanced Data Importing \(Pg 649\)](#) in the References section.

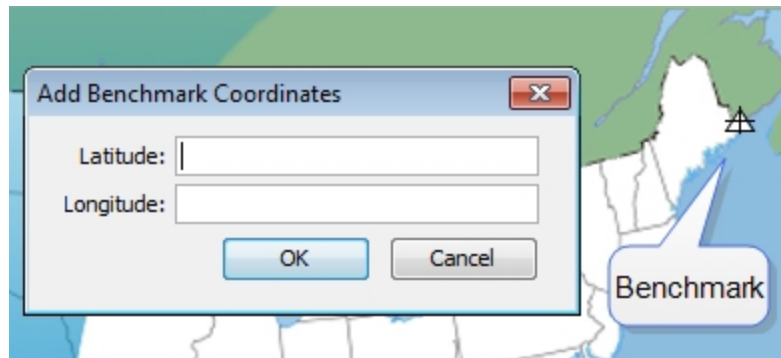
Using Geographic Coordinates

You can use geographic Latitude and Longitude coordinates to place devices on your map. This can be useful if you have many devices at different locations. The procedure is relatively simple:

1. Create a new map on which you want to place the devices.
2. Obtain a map image you want to use as the background for the map. You can scan your own map to create the image, or get one from one of the sites listed below. InterMapper can import image files in PNG, JPEG, or GIF format.
3. Set the image as the background for your map as described in [Background Images \(Pg 104\)](#).
4. Set *benchmarks* in the map as described below. This sets the relationship between your map image and real geographic coordinates.
5. Create a text file containing a list of your devices with their IP addresses and Latitude and Longitude coordinates. You can specify many other parameters for each device within this file as well. For more information, see [Importing Data Into Maps \(Pg 637\)](#). A sample data file is shown below, containing geographic coordinates.
6. Import the text file. The devices appear at the correct location on the map.

Setting Benchmarks in Your Map

A *benchmark* is an icon on a map that specifies the latitude and longitude of that point. InterMapper uses the benchmarks to determine the proper location for icons on the map.



To place a benchmark on a map:

1. Right-click (CTRL-click) a known location (on for which you know the actual latitude and longitude) in the map's background image and choose **Add benchmark...** The Add Benchmark Coordinates window appears.
2. Enter the latitude and longitude for the point. A small triangular icon appears to represent the benchmark. InterMapper supports multiple formats for latitude and longitude. (See below)
3. Follow steps 1 and 2 to enter a second benchmark to complete the geographic information. Your map is now ready for you to import devices with specified geographic coordinates.

To remove a benchmark on a map:

- Right-click (CTRL-click) an existing benchmark, choose **Remove benchmark...** The benchmark disappears from the map.

To remove both benchmarks from a map:

- Right-click (CTRL-click) anywhere in the map's background image and choose **Clear benchmarks...** Both benchmarks disappear from the map.

Accepted Geographic Coordinate Formats

InterMapper supports a wide variety of formats for entering geographic coordinates. Any coordinate can be entered as follows:

- - Decimal degrees: 43.692 or 72.272
- - Degrees, minutes, seconds: 43:16:34.56
- - Degrees with decimal minutes: 43:23.341
- - Use 'W' and 'S' suffixes as alternatives to negative values.

Sample accepted formats:

- [+|-]dd.dd:mm.mm:ss.ss
- [+|-]dd.dd:mm.mm
- [+|-]dd.dd
- [+|-]dd.dd mm.mm ss.ss
- [+|-]dd.dd mm.mm

Allowable suffixes:

- s, n, e, w, S, N, E, W.

Acceptable Data Elements (in order)

- an optional negative sign
- a real number
- anything except letters, digits, -, or .
- a real number
- anything except letters, digits, -, or .
- a real number
- an optional ending directional notation (N, S, E, W, n, s, e, w (depends on the field)) or " (e.g. in the case of 43° 16' 23")

Importing Devices with Geographic Coordinates

You can create a tab-delimited file with information about the devices to be added to the map. This information can include any of following fields: Name, IP Address, DNS name, port, type of device, SNMP community string, latitude, longitude, and many other fields. Fields left unspecified are filled with default values. For more information, see [Importing Data Into Maps \(Pg 637\)](#).

An import file is formatted as follows:

- **Line 1 specifies the format of the following lines** - it specifies the file format ("tab" in the example below), the table to be filled ("devices") and the order of the fields. Three fields must be specified: MapName, Address, and Probe: the remainder are optional.
- **Remaining lines contain the data for the devices you want to import** - Each device occupies a single line, and the data columns are separated by tabs (a "tab-delimited" file.) Each column corresponds to a field in the *fields* specification of Line 1.

In this example import file, there are five fields to import. InterMapper places these items on the map named "MapA", using the address specified to create HTTP probes. They are placed at the indicated latitude and longitude.

```
# format=tab table=devices field-  
s=MapName,Address,Probe,Latitude,Longitude  
MapA 192.168.2.100 http 43.3 -72.0  
MapA 192.168.2.101 http 43.9 -72.3  
MapA 192.168.2.102 http 43.8 -72.8  
MapA 192.168.2.103 http 43.0 -72.4  
MapA 192.168.2.104 http 43.2 -72.3  
MapA 192.168.2.105 http 43.6 -72.2
```

Sources of Maps

There are a huge number of mapping services available through the web. Here are several that we have found useful:

Web-based Service	Description
<u>Google Image Search</u>	http://www.Google.com/imghp?hl=en&tab=wi&ie=UTF-8&q= Search their Images section for the word "map" plus the name of the country, province, state, etc. you need. Free.
<u>Maporama</u>	http://www.maporama.com Attractive street maps with different styles and coloring that are good for backgrounds. Large maps available. Free.
<u>Mapblast</u>	http://www.mapblast.com Another site showing street maps suitable for backgrounds. Large maps available. Free.
<u>National Atlas</u>	http://www.nationalatlas.gov A source of national and state maps. Free.
<u>ter-raserver.com</u>	http://www.teraserver.com Aerial photographs. Clever interactive latitude and longitude indicator using mouse rollover. 1 m/px resolution.
<u>Microsoft Research Maps</u>	http://msrmaps.com/ USGS Aerial photos, and topo maps to 1 m resolution. Clicking shows latitude and longitude of the clicked point. Also allows large, medium, and small maps. Free.
<u>US Census Bureau</u>	http://www.census.gov/geo/www/maps Construct a map from Census data as well as street, political, river/water data. Free.
<u>Yahoo! Listing of Mapping Resources</u>	http://dir.ya-hoo.com/Science/Geography/Cartography/Maps/Interactive/ Yahoo! Search for interactive maps. Lists many interesting mapping sites. Free.
<u>dmoz Open Directory</u>	http://dmoz.org/Science/Social_Sciences/Geography/Geographic_Information_Systems/ Links to many Geographic Information Systems sites. Free.
<u>Geocode.com</u>	http://www.geocode.com/ An inexpensive geocoding service that converts street addresses to latitude and longitude.
<u>Radio Mobile</u>	http://www.cplus.org/rmw/english1.html Software that predicts the performance of a radio system based on topographic maps. Free.

Exporting Information to Google Earth

InterMapper exports the following information so that Google Earth can place devices in the proper location. This information is exported as a .KML file compatible with Google Earth.

Each InterMapper map appears as a place in the left pane of Google earth. Items are shown as follows:

- **Devices** are represented by their status badges (green, yellow, orange, red circle icons)
- **Network ovals** are shown as small circles.
- **Links** between devices are shown as lines connecting the icons.
- **A Status window** for each of the above items displayed when you click the item.

To be displayed in Google Earth, a device must have geographic information; devices that do not have geographic information are not displayed at all.

Geographic coordinates may be set in two ways:

- **Explicitly** - by using **Set Latitude and Longitude...** for each device. You can set latitude and longitude values for many devices at once by [importing a text file containing the correct information \(Pg 642\)](#).
- **Implicitly** - When benchmarks are placed on a map, the device's latitude and longitude are inferred from the x/y position on the map, relative to the established benchmarks. Use the Insert menu's **Map Benchmark...** (Pg 640). to add benchmarks. Use of benchmarks is inherently less precise than using explicit coordinates.

In the case where both explicitly set coordinates and benchmarks are used, InterMapper uses the explicit coordinates and ignores the benchmarks.

How it works

- **Google Earth requests information from the InterMapper server using HTTP.** Consequently, the InterMapper web server interface must be enabled in the Server Settings.
- **The Google Earth connection uses the same authentication method as the web interface;** you must have appropriate web access permissions for any map you wish to view in Google Earth. (Google Earth will prompt you for the username and password.)
- **Google Earth does not need to be installed on the InterMapper server,** though its machine must have appropriate access permissions established in the InterMapper web server firewall.
- **Google Earth uses a "Network Link"** with a URL that Google Earth uses to request information from InterMapper.

How to use it

The easiest way to get the URL is through the InterMapper web interface.

1. Download and install Google Earth.
2. From the Server Configuration section of the Server Settings window, click **Web Server**. The Web Server settings pane appears in the right pane.
3. Make sure the web server is running, then click the URL to launch a browser with the InterMapper Web interface.
4. In the InterMapper web interface, click **Map List**. A list of maps on your server appears.
5. Click the link to a map that contains latitude/longitude information, either implicitly or explicitly. The map appears in the browser.
6. At the bottom of the map, click **View this map in Google Earth**. This is a link to the map's .KML file, a data file used by Google Earth. Assuming Google Earth has been installed properly, your browser offers to use Google Earth to open the file.

If everything is set up properly, the status badges for your devices hover over the surface of the Earth in appropriate locations.

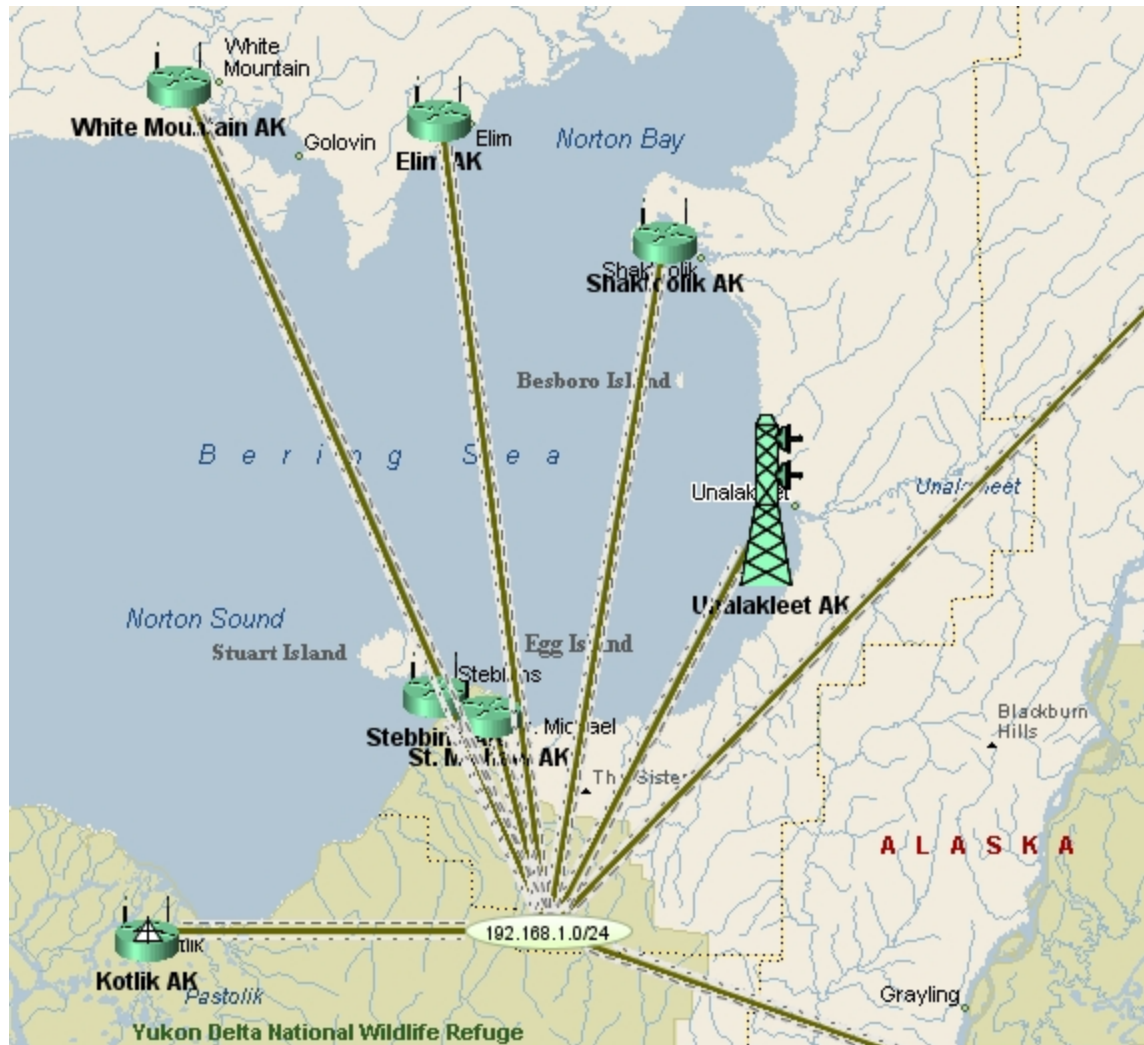
To view a device's status window:

- Click the device's badge. The device's Status Window appears in the Google Earth window.

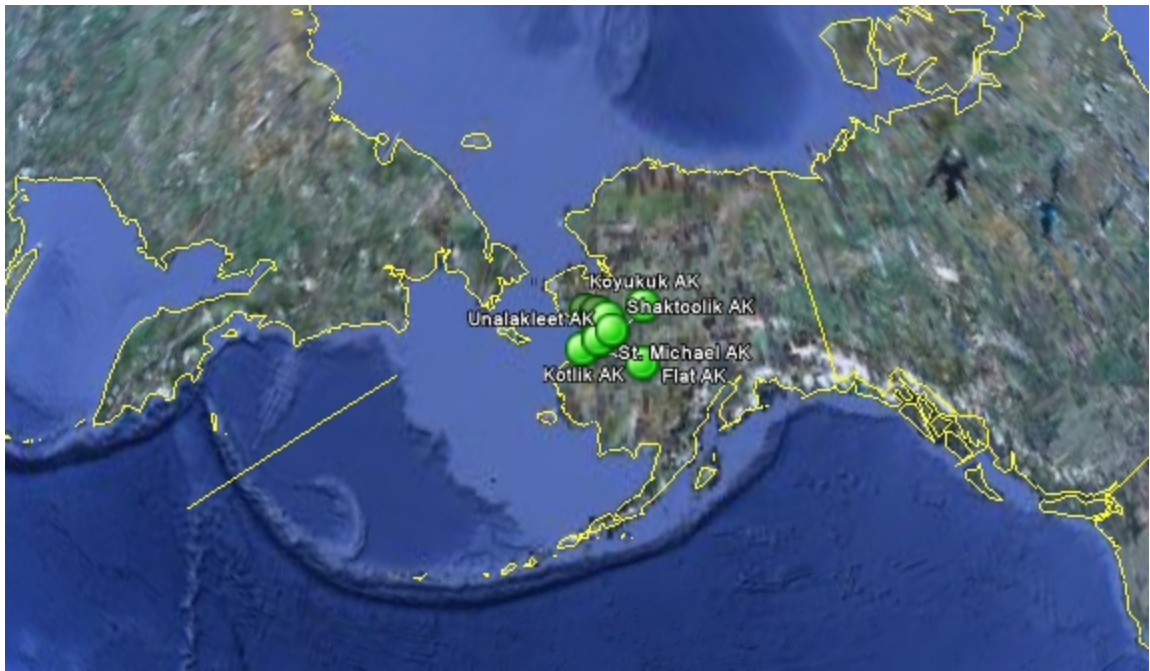
The map refreshes automatically every 5 minutes.

What you see

The images below show the original map, the mapped devices displayed from two different zoom levels, and the status window for one of the devices.



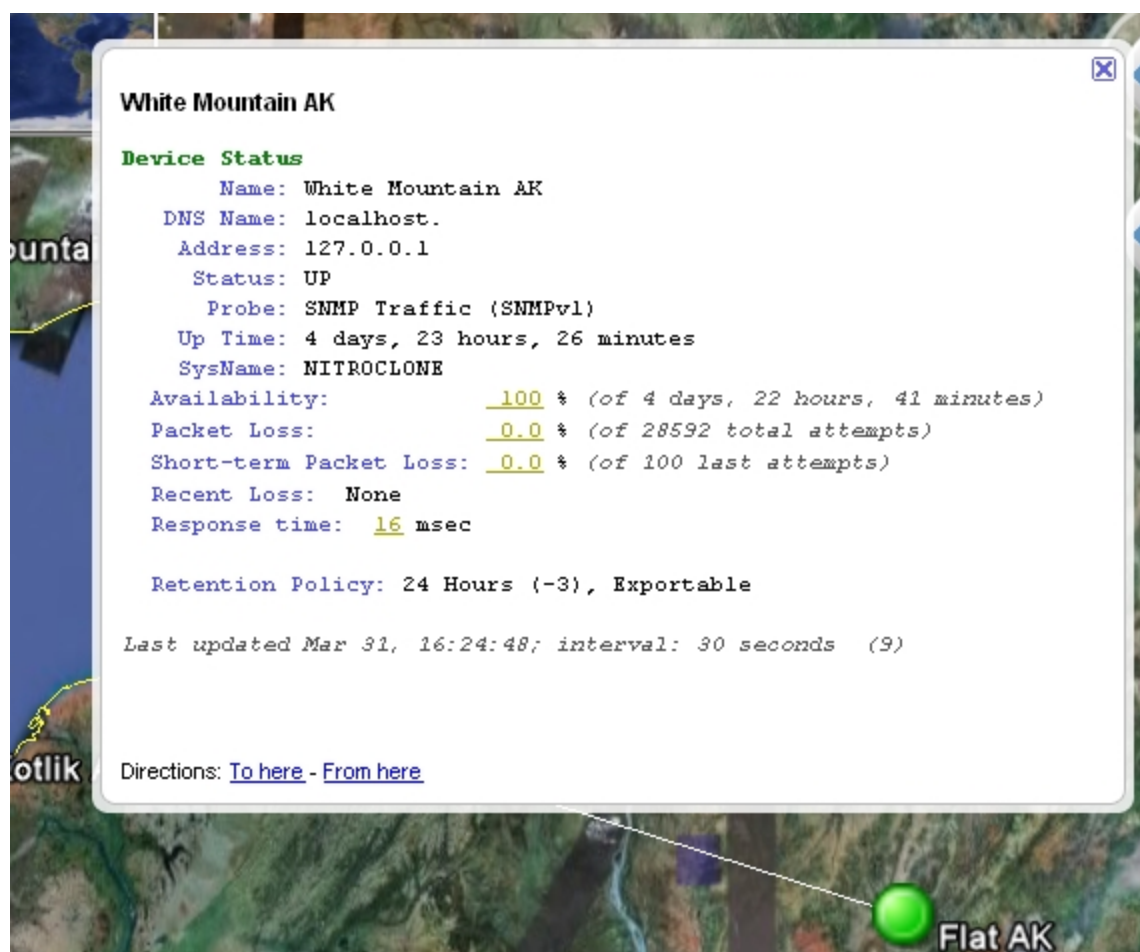
Original map in InterMapper



Wide view in Google Earth



Closer view in Google Earth



Status window in Google Earth

Chapter 17

Advanced Data Importing

Introduction - The Directive Line

If you need more control over the import process, you can use the Directive line technique instead of a spreadsheet-style import file. In addition to inserting new devices, you can update specific attributes of existing devices, change their appearance or location, and delete them.

Note: You can automate the importing of map data by sending commands to InterMapper RemoteAccess through its command-line interface. This allows you to interact with InterMapper through your own scripts. For more information, see *Using the Command Line Interface* in the [Developer Guide](#).

The first line, known as the **directive** line, is formatted as in this example:

```
# format=tab table=devices fields=id,name,address modify=address match=id
```

Each of the elements below is separated by a tab:

- The first line must begin with pound/hash sign ("#").
- The *table=devices* parameter specifies which table the data should be imported into.

Valid choices are detailed in [Data types \(Pg 655\)](#), below.

Notes:

- You can generate a list of fields and descriptions for any data type by exporting the **Schema** table. For more information, see [Exporting Data From Maps \(Pg 635\)](#).
- You can include columns in your import file from both the Device and Vertices tables. InterMapper automatically applies the Vertex attributes appropriately to the vertex linked to the indicated device.
- The *fields=id,name,address* parameter identifies the order of the data in the columns. In this example, there are three columns for the device's ID, name, and address.
- The *modify* and *match* parameters combine to specify which device attributes to change, and which device attributes to use to verify that the correct device has been found.

Directive Format/Options
Parameter

Format Supported file formats:

- **tab** - tab-delimited
- **csv** - comma-separated
- **xml** - XML format (see an exported file for the format)

Example:

```
format=tab
```

Table Available values for the `table` directive are listed in [Data types \(Pg 655\)](#), below.

Examples:

```
table=devices  
table=vertices
```

Modify Comma-separated list of field names. Use this parameter to specify which of the columns you want to update. You can combine this with the optional **Match** parameter.

Note: If there is no **Match** parameter, the **ID** field is used to find matches. If no **ID** field exists, the import fails.

Example:

```
modify=ID,MapName,Address,Latitude,Longitude
```

Match Comma-separated list of field names. Use this parameter to specify which of the columns you want to use to determine whether to modify device values.

If no **Match** parameter is included, the **ID** field is used to find matches.

If no **ID** field is included in the file, the import fails.

Example:

```
match=MapName,Address
```

Insert Comma-separated list of field names. Use this parameter to specify the fields you want to set when creating the

You must include a combination of at least two fields whose Access attribute is "CREATE" (MapPath, Address, DNSName, IMProbe, MapID). To see the valid combinations, see [Device Attributes \(Pg 656\)](#). When no valid MapPath is included, one is created for you, named "Untitled 1".

Once the device is created using one or more of these fields, InterMapper attempts to set the values of the remaining fields specified in the Insert parameter to the values in the corresponding columns.

Insert fields are evaluated from left to right. If, for example, you specify an Address, DNSName, and IMProbe in that order, the Address is set, and the DNSName is resolved to it, and remaining fields are set from the IMProbe parameter.

Examples:

```
Insert=MapPath,Address,Name,Latitude,Longitude
```

(The example above creates devices in the specified maps with the specified addresses, names, latitude, and longitude)

Delete

Comma-separated list of field names. Use this parameter to specify which of the columns you want to use to determine whether a device should be deleted.

Example:

```
delete=MapName,Probe
```

(The example above would delete all devices in the specified maps that use the specified probes)

Group

Comma-separated list of field names.

Behaves exactly like the Insert directive, except when it encounters a device to be inserted as a probe group. Devices immediately following the probe group with the same address (and not a probe group) are added to the group.

When another probe group is encountered, the previous group is ended, and subsequent entries are added to the new group.

Note: If the InterMapper server cannot resolve the DNS name, a probe group is added by IP address. This may prevent subsequent entries from being added to the probe

group.

Examples:

```
group=  
=MapName,MapPath,A-  
ddress,Name,Latitude,Longitude
```


Remaining lines - specifying the data

The remaining lines of the file contain the data as specified in the **fields** definition described above. Each column is separated by a tab, and columns must appear in the order specified in the **fields** definition (for directive line imports) or must correspond to the field names specified in the first line of the file (spreadsheet-style imports).

Available values for the `table` directive are listed in [Data types \(Pg 655\)](#), below.

Import File Example

Below is an example of an Import file. This file specifies itself as a tab-delimited file containing a list of devices. All devices are going into the map named "MapA", and each device definition contains Address, Probe, Latitude, and Longitude columns.

```
# format=tab table=devices field-
s=MapName,Address,Probe,Latitude,Longitude
MapA 192.168.2.100 http 43.3 -72.0
MapA 192.168.2.101 http 43.9 -72.3
MapA 192.168.2.102 http 43.8 -72.8
MapA 192.168.2.103 http 43.0 -72.4
MapA 192.168.2.104 http 43.2 -72.3
MapA 192.168.2.105 http 43.6 -72.2
```

Note: The example above creates the devices and assigns probes, but does not set the parameters for the probes. The most efficient way to do this is using the [IMProbe URL](#) (Pg 687). It lets you specify the SNMP community string, the probe by file name, and any parameters needed.

Creating Probe Groups

Use the `group` directive to create a device and add probes to it as a group. The following example adds six devices, with the last one having a probe group. Groups are created in order - probes are added to the group until the IP address changes.

Note: Like the example above, this one creates the devices and assigns probes, but does not set the parameters for the probes. The most efficient way to create and configure a probe group is to use the [IMProbe URL](#) (Pg 687). It lets you specify the SNMP community string, the probe by file name, and any parameters needed.

```
# format=tab table=devices field-
s=MapName,Address,Probe,Latitude,Longitude
group=MapName,Address,Probe,Latitude,Longitude
MapA 192.168.2.100 http 43.3 -72.0
MapA 192.168.2.101 http 43.9 -72.3
MapA 192.168.2.102 http 43.8 -72.8
MapA 192.168.2.103 http 43.0 -72.4
MapA 192.168.2.104 http 43.2 -72.3
MapA 192.168.2.105 group 43.6 -72.2
MapA 192.168.2.105 http 43.6 -72.2
MapA 192.168.2.105 snmp 43.6 -72.2
```

Automatic Placement of Devices

If your map contains no benchmarks (as described in [Using Geographic Coordinates \(Pg 640\)](#)) latitude and longitude fields are ignored. You can place devices at specific locations using the XCoordinate and YCoordinate fields (described in the [Vertex Attributes \(Pg 667\)](#)). X and Y coordinates are calculated from the upper left.

If the map contains benchmarks to specify geographic coordinates, InterMapper uses them to place devices at the proper location in the map.

Note: In order for InterMapper to place devices accurately using geographic coordinates, two benchmarks must be specified before you import or update the devices. If you have imported the devices to the map before specifying the benchmarks, you can create an export file containing the MapPath, ID, Latitude and Longitude, then re-import the file after specifying your benchmarks. The devices are moved to the appropriate locations on the map.

How InterMapper Inserts Devices

InterMapper places new devices in horizontal rows across the top of the specified map. If either X/Y coordinates or geographic coordinates are specified for the device, InterMapper places it at the specified location on the map.

How InterMapper Handles Errors and Defaults

InterMapper strives to use sensible defaults. The import file needs only a server name, map path, and either an IP address or DNS Name for a new device. InterMapper uses its default settings for other values and parameters.

Note: If the InterMapper server cannot resolve the DNS name, the device is added by IP address.

The import process recovers sensibly from faulty, ill-formatted, or inconsistent input values. An invalid format for an IP address, for example, cannot succeed, and is reported as an error. Most other data is passed along so the device can be added to the map with appropriate defaults. The InterMapper Event Log file contains a line for each newly added device, along with indication of success or error.

If the attribute name in the header of the imported file is not recognized as a valid attribute, InterMapper displays an error message and ignores the contents of that column.

When the import is finished, a summary is written to the Event Log file.

Notes:

- Every InterMapper server maintains a unique identifier (the "id") for each of its devices on each map. This makes it a convenient value for matching updated information to an existing device.
- InterMapper defines a new *IMProbe* URL that completely specifies all the parameters of an InterMapper Probe. This IMProbe: URL is defined in [The IMProbe URL \(Pg 687\)](#).

Data types

For each table for which data can be imported or exported, a data type is defined. For information on the different data types, and what information is readable, writable, or both, see the Attributes topic for each data type as linked below.

```
table=[data type]
```

- **devices** - imports data specific to devices. See the [Device Attributes \(Pg 656\)](#) table.
- **vertices** - You can also control other aspects of a device in a map, such as the device's color, label, shape, or font. The `vertices` type imports data specific to the appearance of devices. See the [Vertex Attributes \(Pg 667\)](#) table.
- **interfaces** - imports data specific to the switch and router interfaces. See the [Interface Attributes \(Pg 670\)](#) table.
- **maps** - imports data specific to maps. See the [Map Attributes \(Pg 675\)](#) table.
- **notifiers** - imports data to describe notifiers. See the [Notifier Attributes \(Pg 678\)](#) table.
- **notifierrules** - imports data to describe how a notifier is applied. See the [Notifier Rules Attributes table. \(Pg 679\)](#)
- **users** - imports user account information. See the [User Attributes \(Pg 681\)](#) table.
- **retentionpolicies** - imports user account information. See the [Retention Policy Attributes \(Pg 682\)](#) table

Device Attributes

Device attributes are supported as described in the table below. At minimum, **MapName** and **Address** are required. To create a device by importing, the following is required:

- One of **MapPath** or **MapID**
- One of **Address**, **DNSName**, or **NetBIOSName**

For any attribute that is not in the file, a default value is used. For example, if no probe is specified, the **Automatic** probe is used.

Use these attributes with the following table specification in line 1:

```
table=device
```

Notes:

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus(+) can be updated during import.
- Fields with the Access attribute of "SENSITIVE" can only be imported by an administrator over a secure SSL connection.
- The columns are imported in the order specified. The last value specified takes precedence over previous values in the same line. Because of this, Help/Systems recommends that you use only one the following columns when importing: **Address**, **DNSName**, **IMProbe**. If more than one of these is specified, and there are conflicts, the last column's values are used.

Device Attributes

Field Name	Description
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the map containing the device.
MapPath	Type: TEXT Access: READ-ONLY Attributes: CREATE Description: Full path of the map containing the device, including the name of the map.
Address +	Type: ADDRESS Access: READ-WRITE Attributes: CREATE Description: The IP or AppleTalk address of the device that is probed by InterMapper. The IP address is represented in dotted-decimal notation, e.g. 'a.b.c.d'.

	The AppleTalk address is represented in slash notation, e.g. 'a/b'.
Id	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique, persistent identifier for this device instance. The id will be unique across all maps on a single InterMapper server.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: The name of the device. The name is the first non-empty line in a device's label on a map.
Probe +	Type: TEXT Access: READ-WRITE Attributes: none Description: The human-readable name of the InterMapper probe.
Comment +	Type: TEXT Access: READ-WRITE Attributes: none Description: The comment associated with the device.
Community +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The SNMP community of the device.
DisplayIfUnNumbered +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is set to display unnumbered interfaces.
DNSName +	Type: TEXT Access: READ-WRITE Attributes: CREATE Description: The fully-qualified DNS name of the device.

IgnoreIfAppleTalk +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore AppleTalk interface information.
IgnoreIfDiscards +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore interface discards.
IgnoreIfErrors +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore interface errors.
IgnoreOutages +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore outages.
AllowPeriodicReprobe +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to allow periodic reprobe.
IMProbe *+	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE,CREATE Description: A special URL representation describing the Inter-Mapper probe and its parameters, e.g. improbe://address:port/...
Latitude +	Type: TEXT Access: READ-WRITE Attributes: none Description: The latitude of the device. The value will be a double within the range [-90..90] or empty string

	if the device does not have this attribute set.
Longitude +	Type: TEXT Access: READ-WRITE Attributes: none Description: The longitude of the device. The value will be a double within the range [-180..180] or empty string if the device does not have this attribute set.
LastTimeDown	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The time when the device last went down. Value is 0 if device has not gone down since we started monitoring it.
LastTimeSysUp	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The time when the device last came up (ie rebooted), based on the value of sysUpTime. The value is 0 if unknown.
LastTimeUp	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The time when the device status last transitioned from DOWN to UP. Value is 0 if this has not happened since we started monitoring.
MACAddress	Type: TEXT Access: READ-ONLY Attributes: none Description: The device's MAC Address. If the device has multiple interfaces, this field will contain the MAC Address associated with the device's main IP Address (the same address in the address field).
MapAs +	Type: TEXT Access: READ-WRITE Attributes: none Description: Value is one of { ROUTER , SWITCH , HUB, END

	SYSTEM }
MapId	Type: TEXT Access: READ-ONLY Attributes: CREATE Description: The unique Id of the map file containing the device.
MaxTries +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The maximum number of attempts to reach the device, typically indicates the maximum number of packets to send during each poll, for packet-based probes.
NetBIOSName +	Type: TEXT Access: READ-WRITE Attributes: CREATE Description: The NetBIOS/WINS name of the device.
PctLoss	Type: DOUBLE Access: READ-ONLY Attributes: none Description: The percent loss (# packets lost/total # packets sent).
ShortTermPctLoss	Type: DOUBLE Access: READ-ONLY Attributes: none Description: The short-term percent loss (# packets lost/# packets sent).
Availability	Type: DOUBLE Access: READ-ONLY Attributes: none Description: The percent availability (time up/time monitored).
PollInterval +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The poll interval of the device, in seconds. Value is 0 if non-polling.

Port +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The UDP or TCP port number. If the port number is not applicable, this value is always 0. (e.g. for ICMP)
Resolve +	Type: TEXT Access: READ-WRITE Attributes: none Description: Value is one of { name , addr , none }.
RoundTripTime	Type: INTEGER Access: READ-ONLY Attributes: none Description: The last round-trip time in milliseconds, if known.
SNMPv3AuthPassword +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The device's SNMPv3 authentication password.
SNMPv3AuthProtocol +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMPv3 authentication protocol (MD5, SHA, None).
SNMPv3PrivPassword +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The device's SNMPv3 privacy password.
SNMPv3PrivProtocol +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMPv3 privacy protocol (DES, None).
SNMPv3UserName +	Type: TEXT Access: READ-WRITE Attributes: none

	Description: The device's SNMPv3 user name.
SNMPVersion +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMP version (SNMPv1, SNMPv2c, or SNMPv3).
Status	Type: TEXT Access: READ-ONLY Attributes: none Description: The status of the device. The value is one of { 'UP', 'DOWN', 'UNKNOWN' }.
StatusLevel	Type: TEXT Access: READ-ONLY Attributes: none Description: The status level of the device. The value is one of { 'Unknown', 'OK', 'Warning, Acked', 'Warning', 'Alarm, Acked', 'Alarm', 'Critical', 'Critical, Acked', 'Down', 'Down, Acked' }.
StatusLevelReason	Type: TEXT Access: READ-ONLY Attributes: none Description: The reason the device has its status level.
SysDescr	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysDescr.
SysName	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysName.
SysContact	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysContact.

SysLocation	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysLocation.
SysObjectID	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The value of sysObjectID.
TimeOut +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The timeout of the device, in seconds. Value is 0 if not-applicable to the probe.
IMID	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: Identifier of the device in the IMID format.
Type	Type: TEXT Access: READ-ONLY Attributes: none Description: One of { none, other, snmp, tcp, udp, icmp, cmd, bigbro, ntsvcs }. These values have been updated in 5.0 to match the values used by the database in the probekind field of the devices table.
ProbeXML	Type: TEXT Access: READ-ONLY Attributes: SENSITIVE Description: XML dataset DTD, type='probe'.
SNMPVersionInt	Type: INTEGER Access: READ-ONLY Attributes: none Description: 1, 2, 3 - SNMP versions. 0 for non-SNMP.
SysServices	Type: INTEGER Access: READ-ONLY Attributes: none

	Description: 16-bits integer.
EntSerialNum	Type: TEXT Access: READ-ONLY Attributes: none Description: SnmpAdminString (entPhysicalSerialNum of chassis).
EntMfgName	Type: TEXT Access: READ-ONLY Attributes: none Description: SnmpAdminString (entPhysicalMfgName of chassis).
EntModelName	Type: TEXT Access: READ-ONLY Attributes: none Description: SnmpAdminString (entPhysicalModelName of chassis).
DataRetentionPolicy	Type: INTEGER Access: READ-ONLY Attributes: none Description: Data retention policy for IM Database
CustomerNameReference	Type: TEXT Access: READ-ONLY Attributes: none Description: Customer-supplied device name reference, for linking to an external database.
EnterpriseID	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysEnterpriseID.
DeviceKind	Type: TEXT Access: READ-ONLY Attributes: none Description: User-specified device type.
SysUpTime	Type: TEXT

	Access: READ-ONLY Attributes: none Description: System uptime.
LastModified	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: Timestamp of last modification to this device.
Parent	Type: TEXT Access: READ-ONLY Attributes: none Description: Device ID of the parent probe group; this device's id if this device is a probe group; 0 if the device is not part of a probe group.
Acknowledge +	Type: TEXT Access: READ-WRITE Attributes: none Description: The acknowledgement state of the device; one of { 'None', 'Basic', 'Maintenance' }. The Ack-Message field must also be set to import this field. Indefinite maintenance will be set if AckExpiration is missing and state is set to 'Maintenance'.
AckMessage +	Type: TEXT Access: READ-WRITE Attributes: none Description: The message associated with the acknowledge state. If Acknowledge is not set and an Ack-Message is supplied, Acknowledge will be set to 'Basic'.
AckExpiration +	Type: TEXT Access: READ-WRITE Attributes: none Description: The absolute time when the timed acknowledgement expires, if any. The AckMessage field must also be set to import this field. Acknowledge will be set to 'Maintenance' if not supplied.
AckTimer	Type: TEXT

	Access: READ-ONLY Attributes: none Description: The time in seconds remaining until the timed acknowledgement expires, if any.
VertexId	Type: TEXT Access: READ-ONLY Attributes: none Description: The Vertex Id of the vertex associated with the device. Matches the VertexId of the corresponding vertex in the vertices table.
Layer2	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if layer2 mapping is enabled for this device.

Vertex Attributes

Use the `vertices` data type to control the appearance of devices in your map, such as the device's color, label, shape, or font.

Use these attributes with the following table specification in line 1:

```
table=vertices
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus(+) can be updated during import.

Field Name	Description
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the map file containing the vertex.
Id	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique, persistent identifier for this vertex instance. The id will be unique across all maps on a single InterMapper server.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: The name of the vertex. The name is the first non-empty line in a device or network's label on a map.
Color +	Type: TEXT Access: READ-WRITE Attributes: none Description: Color (valid names: white, black, red, orange, yellow, blue, green, brown)
FontName +	Type: TEXT Access: READ-WRITE Attributes: none Description: Font name, eg. Bodoni MT
FontSize +	Type: INTEGER Access: READ-WRITE

	Attributes: none Description: Font size in points.
FontStyle +	Type: TEXT Access: READ-WRITE Attributes: none Description: Font style (bold, italic, plain)
Label	Type: TEXT Access: READ-ONLY Attributes: none Description: Vertex label.
LabelPosition +	Type: TEXT Access: READ-WRITE Attributes: none Description: Label position. Valid values are topleft, top, topright, left, center, right, bottomleft, bottom, bottomright
LabelTemplate +	Type: TEXT Access: READ-WRITE Attributes: none Description: Vertex label template.
LabelVisible +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the vertex label is visible (only used when the device is represented by an icon)
MapId	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique Id of the map file containing the vertex.
Origin +	Type: TEXT Access: READ-WRITE Attributes: none Description: The origin determines whether the vertex coordinates are relative to the center or one of the sides of the vertex. Valid values: center, top, left, right, botom, topleft, topright, bottomright, bottomleft.

Shape +	Type: TEXT Access: READ-WRITE Attributes: none Description: Vertex shape (rect, oval, wire, cloud, text, or icon name).
VantagePoint +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the vertex is a vantage point of the graph
XCoordinate +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Horizontal map coordinate, the positive direction is to the right.
YCoordinate +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Vertical map coordinate, the positive direction is to the bottom.
VertexId	Type: TEXT Access: READ-ONLY Attributes: none Description: The Vertex Id of the vertex. Corresponds to the device with a matching VertexID in the devices table.

Interface Attributes

The `interfaces` data type imports data specific to the switch and router interfaces.

Use these attributes with the following table specification in line 1:

```
table=interfaces
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus(+) can be updated during import.

Interface Attributes

Field Name	Description
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: The name of the map to which the interface belongs.
InterfaceID	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique persistent identifier for this interface instance.
DeviceID	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique persistent identifier for the adjacent device.
NetworkID	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique persistent identifier for the adjacent network.
Index	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface index (i.e. <code>ifIndex</code>) of the interface.
IntegerIndex	Type: TEXT

	Access: READ-ONLY Attributes: none Description: The interface index (i.e. ifIndex) of the interface, as an integer.
Description	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface description (i.e. ifDescr).
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface name (i.e. ifName).
Alias	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface alias (i.e. ifAlias).
PhysAddress	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The interface's data-link layer address (i.e. ifPhysAddr) .
Type	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface type as a human-readable string (i.e. ifType).
MTU	Type: INTEGER Access: READ-ONLY Attributes: none Description: The interface MTU (i.e. ifMTU).
Address	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The interface's first network-layer address.

SubnetMask	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The subnet mask associated with "Address".
SubnetList	Type: TEXT Access: READ-ONLY Attributes: none Description: A comma-separated list of addresses/masks on this interface.
SubnetPrefixList	Type: TEXT Access: READ-ONLY Attributes: none Description: A comma-separated list of addresses/prefixes on this interface.
Speed	Type: INTEGER Access: READ-ONLY Attributes: none Description: The interface's speed in bits per second. (Derived from preferred speed and reported speed.)
PreferredSpeed +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The preferred speed of the interface as set by the customer.
ReportedSpeed	Type: INTEGER Access: READ-ONLY Attributes: none Description: The speed of the interface as reported by the interface.
LastChange	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The timestamp when the interface last changed status.
Status	Type: TEXT

	Access: READ-ONLY Attributes: none Description: The status of the interface (e.g. UP, DOWN, or ADMIN-DOWN).
Enabled +	Type: TEXT Access: READ-WRITE Attributes: none Description: Flag which indicates whether the interface is enabled or not.
MapId	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique persistent identifier for the map to which the interface belongs.
IMID	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: Identifier of the interface in the IMID format.
TypeInt	Type: INTEGER Access: READ-ONLY Attributes: none Description: The interface type as a number.
RecvSpeed +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Unsigned 64-bit integer. 0 means baseband; speed in Speed.
StatusInt	Type: INTEGER Access: READ-ONLY Attributes: none Description: The status of the interface as integer. Values correspond to {UP, DOWN, ADMIN-DOWN, DOWN but locally acked}.
CustomerNameReference	Type: TEXT Access: READ-ONLY

	Attributes: none Description: Customer-supplied name, for referencing an external database.
DataRetentionPolicy	Type: INTEGER Access: READ-ONLY Attributes: none Description: Database data retention policy.
Duplex	Type: TEXT Access: READ-ONLY Attributes: none Description: Interface Duplex status.
VLANs	Type: TEXT Access: READ-ONLY Attributes: none Description: Comma-separated list of this interface's VLANs.
NatVLAN +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Native VLAN. Signed integer (0-4093). 0 means none.

Map Attributes

The `maps` directive contains data to describe maps. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=maps
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus(+) can be updated during import.

Field Name	Description
MapId	Type: TEXT Access: READ-ONLY Attributes: none Description: A unique, persistent identifier for this map instance.
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the map.
MapPath	Type: TEXT Access: READ-ONLY Attributes: none Description: Full path of the map, including the name of the map.
Status	Type: TEXT Access: READ-ONLY Attributes: none Description: Status of the map (e.g. down, critical, alarm, warning, okay).
DeviceCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in the map.
NetworkCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of networks in the map.

InterfaceCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of interfaces in the map.
DownCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices that are down.
CriticalCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in critical status.
AlarmCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in alarm status.
WarningCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in warning status.
OkayCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of okay devices.
DataRetentionPolicy	Type: INTEGER Access: READ-ONLY Attributes: none Description: Database retention policy.
IMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the map in the IMID format.
Enabled	Type: BOOLEAN Access: READ-ONLY

	Attributes: none Description: True if the map is currently running.
Layer2	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if the map is enabled for layer 2 polling.

Notifier Attributes

The `notifiers` data type contains data to describe notifiers. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=notifiers
```

Field Name	Description
IMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the notifier in the IMID format.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: Human readable, one-line name.
NotifierXML	Type: TEXT Access: READ-ONLY Attributes: none Description: XML dset DTD, type='notifier'.
enabled	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if the notifier is enabled.

Notifier Rules Attributes

The `notifierrules` data type contains data to describe how a notifier is applied. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=notifierrules
```

Field Name	Description
NotifierIMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the notifier in the IMID format.
EscalationIMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the escalation in the IMID format.
Down	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of DOWN events.
Up	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of UP events.
Critical	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of CRITICAL events.
Alarm	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of ALARM events.
Warning	Type: BOOLEAN Access: READ-ONLY

	Attributes: none Description: True if user is notified of WARNING events.
Okay	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of OKAY events.
Trap	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of TRAP events.
Delay	Type: INTEGER Access: READ-ONLY Attributes: none Description: Notification delay.
Repeat	Type: INTEGER Access: READ-ONLY Attributes: none Description: Notification repeat.
Count	Type: INTEGER Access: READ-ONLY Attributes: none Description: Notification count.

User Attributes

The `users` data type imports user account information.

Use these attributes with the following table specification in line 1:

```
table=users
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus(+) can be updated during import.

Field Name	Description
Id	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique, persistent identifier for this user.
Name *+	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE,CREATE Description: Login name of the user.
Password +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: If the user is to be validated locally, the user's password.
Guest +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The user's autologin properties.
External +	Type: BOOLEAN Access: READ-WRITE Attributes: SENSITIVE Description: Indicates user is to be validated by an auth server.
Groups +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: Comma-separated list of groups to which to add user. (Will not remove users from groups not in list.)

Retention Policy Attributes

The `retentionpolicies` data type contains data to describe retention policies. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=retentionpolicies
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus(+) can be updated during import.

Field Name	Description
IMID	Type: TEXT Access: READ-ONLY Attributes: none Description: IMID of the retention policy.
RetentionPolicyID	Type: INTEGER Access: READ-ONLY Attributes: none Description: Identifier of the retention policy.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the retention policy.
ServerStorageType	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long chart data is retained by the server; 0 = No data retained, -1 = data retained forever, -2 = data retained in memory only.
RawExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long raw chart data is retained by the database in days; -1 = forever.
FiveExpiration	Type: INTEGER Access: READ-ONLY Attributes: none

	Description: How long five-minute sample data is retained by the data-base in days; -1 = forever.
HourlyExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long hourly sample chart data is retained by the database in days; -1 = forever.
DailyExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long daily sample chart data is retained by the data-base in days; -1 = forever.

About D-Sets

When you export data, you can export a generic set of information about a probe or notifier. This information is in XML format, contained in an export field in the following export tables:

- ProbeXML - If this field is included in the export, a D-set is included for each selected device on the map.
- NotifierXML - If this field is included in the export, a D-set is included for each active notifier associated with the map.

ProbeXML D-set

This D-set contains information about a specific probe. Depending upon the probe type, it may have more or fewer <d> clauses. Here is an example:

```
<dset type='probe' hashcode='abcdef'>
  <d name='probe'>com.dartware.snmp</d>
  <d name='snmp ver'>SNMPv3</d> // present only for snmp probes
  <d name='address'>192.168.1.23</d>
  <d name='username'>MyName</d> // present only for snmp v3
  <d name='auth protocol'>MD5</d> // present only for snmp v3
  <d name='auth_passwd'>somePwd</d> // present only for snmp v3
  <d name='priv_protocol'>DES</d> // present only for snmp v3
  <d name='priv_passwd'>somePwd2</d> // present only for snmp v3
  <d name='community'>public</d> // present only for snmp_v1 and
snmp v2c probes
  <d name='port'>80</d>
  <d name='interval'>30</d>
  <d name='timeout'>3</d>
  <d name='tries'>3</d>
  <d type='param' name='Disk Usage Warning %'>75</d>
  <d type='param' name='Memory Usage Alarm %'>90</d>
  <d type='param' ... </d>
</dset>
```

NotifierXML D-set

This D-set contains information about a specific notifier. Depending upon the notifier type, it may have more or fewer <d> clauses. Here are some examples:

```
<dset type='notifier'>
  <d name='method'>smtpmail</d>
  <d type='param' name='email addr'>abc@dd.com</d>
  <d type='param' name='subject'>This is a subject</d>
  <d type='param' name='message'>This is a message.</d>
</dset>
```

```
<dset 'notifier'>
  <d name='method'>audible</d>
  <d type='param' name='down_sound'>name of the sound (as
string)</d>
  <d type='param' name='up_sound'></d>
  <d type='param' name='crit_sound'></d>
```



```
<d type='param' name='alarm_sound'></d>
<d type='param' name='warn_sound'></d>
<d type='param' name='ok_sound'></d>
<d type='param' name='trap_sound'></d>
<d type='param' name='down_vol'>3</d>
<d type='param' name='up_vol'>2</d>
<d type='param' name='crit_vol'>1</d>
<d type='param' name='alarm_vol'>1</d>
<d type='param' name='warn_vol'>1</d>
<d type='param' name='ok_vol'>1</d>
<d type='param' name='trap_vol'>5</d>
</dset>
```

```
<dset type='notifier'>
  <d name='method'>snmptrap</d>
  <d type='param' name='address'></d>
  <d type='param' name='community'></d>
</dset>
```

```
<dset type='notifier'>
  <d name='method'>snpppager</d>
  <d type='param' name='pager_id'></d>
  <d type='param' name='message'></d>
</dset>
```

```
<dset type='notifier'>
  <d name='method'>modempager</d>
  <d type='param' name='pager_id'></d>
  <d type='param' name='message'></d>
</dset>
```

```
<dset type='notifier'>
  <d name='method'>winpopup</d>
  <d type='param' name='popup_id'></d>
  <d type='param' name='message'></d>
</dset>
```

```
<dset type='notifier'>
  <d name='method'>cmdline</d>
  <d type='param' name='cmdline'></d>
  <d type='param' name='success'></d>
  <d type='param' name='message'></d>
</dset>
```

```
<dset type='notifier'>
  <d name='method'>syslog</d>
  <d type='param' name='address'></d>
  <d type='param' name='facility'></d>
```

```
<d type='param' name='severity'></d>  
<d type='param' name='message'></d>  
</dset>
```

```
<dset type='notifier'>  
  <d name='method'>group</d>  
  <d type='param' name='id_list'></d>  
</dset>
```

The IMProbe URL Specification

InterMapper defines a URL format for specifying all the parameters for a probe in a single string. This makes it straightforward to import information about a probe into InterMapper from a text file.

When you export data from InterMapper, you can include the IMProbe field in the export file. The IMProbe field contains the IMProbe URL, which in turn contains all configuration information for a probe in URL-encoded format. You can use the IMProbe URL to change the parameters of probes editing the parameters of the URL, and then importing the URL into the map.

For example, you could change the username and password for all of your HTTP probes in all maps at once by:

1. Exporting the data, including the MapName, Address, and Id, and IMProbe fields for all maps.
2. Finding and replacing the username and password parameters in each URL.
3. Re-importing the text file.

The URL format specifies the information necessary to define a probe using the IMProbe scheme:

```
URL: 'improbe://' [community '@'] address [ ':' port ] '/' probe  
['?' parameters]
```

Note: 'improbe://' is case-sensitive, and must be lower-case.

The minimal information required for an IMProbe URL is the Address information, Probe type, and Authentication information.

- Address information
 - DNS name
 - IP address
 - port number (optional)
- Probe type
 - canonical probe name
 - probe-specific parameters (optional)
- Authentication information
 - SNMP community name (optional)

The `probe` may be a canonical InterMapper probe name specified in full, ie. `com.dartware.radius`, `com.dartware.http.redirect`, or a unique probe suffix may be specified, ie. `radius`, `http.redirect`.

The `parameters` are the parameters for the probe, encoded as for a GET request. To make it simpler to create IMProbe URL's manually, the matching of parameter names is simplified. Before matching parameter names, the parameter names are converted to lower-case, and any spaces and underscores are removed. For a parameter named `Shared Secret`, this means that IMProbe parameters

`shared_secret` and `shared_secret` will match and provide values.

If the `parameters` section contains a parameter name that is not defined for the probe, the parameter is ignored. If a probe parameter is left out of the IMProbe URL, it is set to its default value from the probe file.

Examples

Both of the IMProbe URLs below specify that the host `netopia.example.com` should be tested with the built-in Ping probe:

```
improbe://netopia.example.com/com.dartware.ping
improbe://netopia.example.com/ping
```

Both these URLs test a RADIUS server at `netopia.example.com`, with a shared secret of 'secret', a user name of 'im', and a password of 'pw'. The "Shared Secret" parameter can be written multiple ways:

```
improbe://netopia.example.com/com.dartware.radius?shared_secret-
t=secret&user_name=im&password=pw
improbe://netopia.example.com/radius?sharedsecret=secret&username=im&password=pw
```

The URLs below specifies the SNMP probe, testing a device at `192.168.1.1`, using the community string of 'public'. The second URL a test against port 1611 instead of the default port 161 used in the first URL:

```
improbe://public@192.168.1.1/com.dartware.snmp
improbe://public@192.168.1.1:1611/snmp
```

Encoding Special Characters

The IMProbe URL format uses the Common Internet Scheme Syntax as specified in section 3.1 of RFC 1738. The following characters are illegal and must be encoded with `%hh`:

```
00-1F, 7F, 80-FF
```

The following characters are also considered unsafe and should be encoded with `%hh`:

```
< > " # %
```

The following characters are reserved for special purposes and should not appear unencoded except when used as delimiters in the URL:

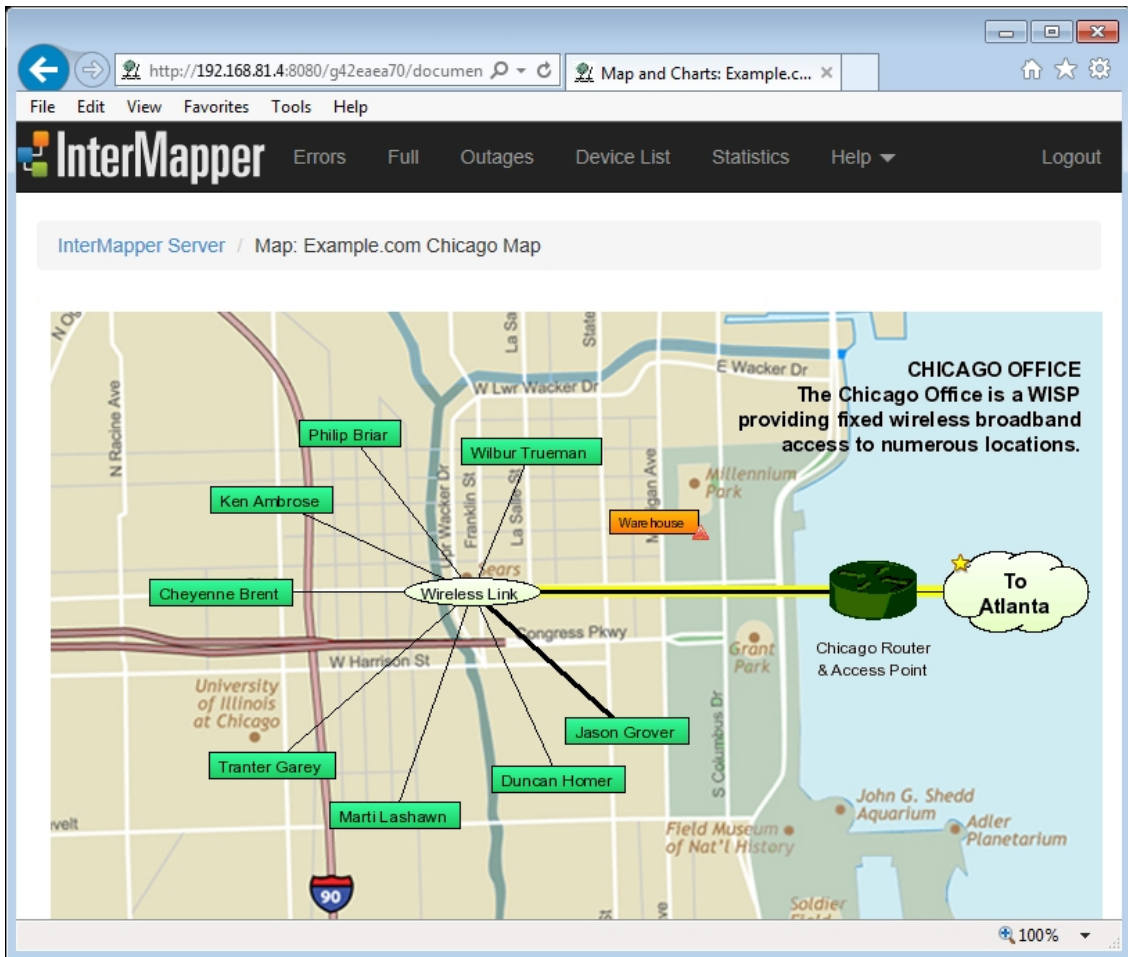
```
 ; / ? : @ = &
```

Chapter 18

Using the Web Server

Each page that InterMapper serves contains the same controls at the top. The example below shows an InterMapper map as it appears in a web page.

Note: To access the web server remotely, (that is, from a different machine connected to the network) you must configure the InterMapper firewall to permit the connection. You must also configure any other firewalls protecting the machine that is running InterMapper to allow traffic to the specified port. For more information, see [The Web Server \(Pg 289\)](#) in the Server Settings section.



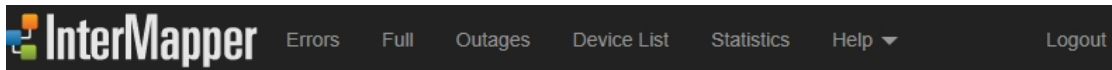
A typical InterMapper web page. the "Example.com" Chicago map.

The InterMapper web page typically has three parts:

- The *header*, which shows the map name or other title and a navigation bar for going to other pages. This is usually the same for every page.
- The *content* of the page, which varies, depending on which page is selected.
- The *footer* of the page, which shows the time the page was created.

InterMapper Web Page Navigation

Use the menu at the top of the InterMapper Web Page to access the available features of the web page. The example above shows a web page for a particular map. The image below shows the InterMapper Web Server menu, found at the top of each page.



Click any of the menu items at the top of the page to view the page. Here is a brief description of each page:

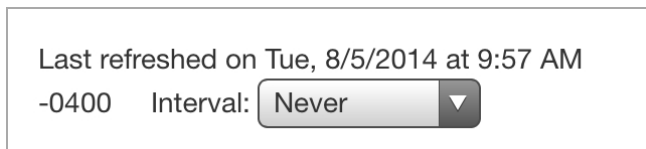
- **Home Page** - Click the InterMapper logo to return to the Home page. View a list of open maps and the charts associated with those maps. Mouse over a map link to see a preview of a map. Click the link to view the map.
- **Error** - View a list of InterMapper errors.
- **Full** - View a list of devices and networks associated with all open maps.
- **Outages** - View a list of current outages (devices and networks that are currently down) and previous outages (devices and networks that failed in the past, but have returned to service).
- **Device List** - View a list of devices and networks associated with all open maps.
- **Statistics** - View information about the current version of InterMapper under which the Web Server is running.
- **Help (menu)** - Choose from a menu of options that allow you to get information about the InterMapper Web client and the current version of InterMapper. View and download files in the InterMapper Settings folder, view the User and Developer Guides, and connect to the InterMapper Telnet server.

Setting the Interval for Reloading the Web Page

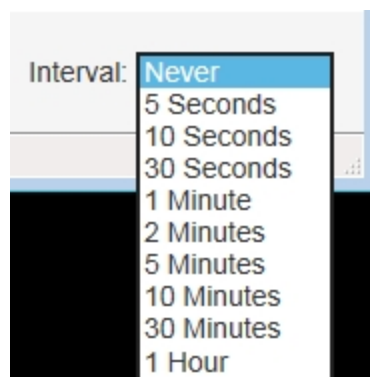
InterMapper pages can be set to refresh at a specified interval. This keeps the web page's information up-to-date.

To set the Reload interval:

- From the **Interval** dropdown menu, choose a reload interval. The web browser refreshes the page at the specified interval.



Interval Menu on iPhone



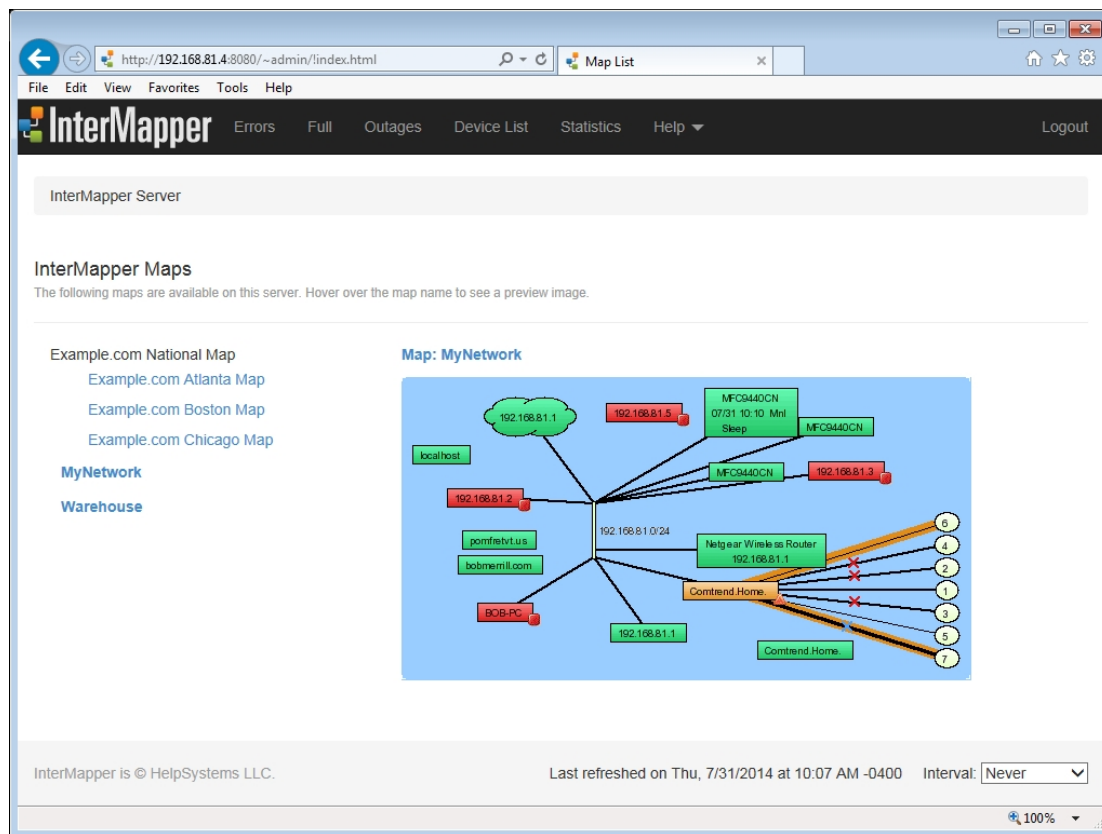
Interval Menu on Computer

Customizing Web Pages

InterMapper's web page appearance is controlled by template files. For more information, see *Customizing Web Pages* in the [Developer Guide](#).

The Home Page

Use the Home page to view a list of open maps and the charts associated with those maps.



The InterMapper Web Server Home page.

- **Mouse over a map link** to see a preview of a map.
- **Click the link** to view the map.

Once you are viewing a map:

- **Click any link, device, or network** on a map to view detailed information about that item.
- **Click a chart link below the map** if any charts have been created for this map. See [The Chart Web Page \(Pg 701\)](#) for more information.
- View the map in Google Earth by clicking the link in **Links to other pages**.

Note: A map on a web page is actually a "snapshot" image of the current state of the map at the time you request the page. The map image is static, so you need to refresh the page to see changes in the map state. You can use the **Interval** drop-down menu button to select the page's refresh interval.

Viewing Information for a Link, Device, or Network

Click any link, device, or network to view detailed information about that item. This is the same information that appears in a Status window. Here are typical displays:

Device Status

Device Information

```
Name:      router.company.net.
DNS Name:  router.company.net.
Address:   192.168.1.1
Status:    UP
Protocol:  Ping/Echo
Up Time:   n/a
Availability: 100% (of 1 hour, 29 minutes, 12 seconds)
Packet Loss: 0.0% (of 143 total attempts) [Reset]
Recent Loss: None
Last updated Jun 23, 12:16:42; interval: 30 seconds
```

Typical Device Status.

Network Status

Network Information

```
Name: 192.168.1.0/24
IP Net: 192.168.1.0/24 (255.255.255.0)
Sum In: 2 pkt/sec 548 byte/sec 0 error/min
Sum Out: 3 pkt/sec 316 byte/sec 0 error/min
```

Comment:

```
This is the network in the office.
It has an IP address of 192.168.1.0, and a subnet mask of
255.255.255.0.
```

Typical Network Status.

Link Status

Interface Information (*ifIndex = 1*)
Device Name:router.company.net.
Description:EN1
Type:10 MBit ethernetCsmacd (*MTU=1500*)
Status:UP for 4 days, 13 hours
Address:192.168.1.1 (255.255.255.0)
MAC Address:00-00-C5-76-E2-EC

Interface Statistics
Utilization:0.01% (*of 10 MBit bandwidth*)
Percent Err:0.0% (*59 pkts w/o error*)
Transmit Statistics (*0.01% utilization*)
Pkt/Second:0 (*5.88% multicast*)
Byte/Second:73 (*590 bps*)
Err/Minute:0 (*0 errors*)
Disc/Minute:0 (*0 discards*)
Percent Err:0.0% (*17 pkts w/o error*)
Receive Statistics (*0.01% utilization*)
Pkt/Second:1 (*59.5% multicast*)
Byte/Second:93 (*748 bps*)
Err/Minute:0 (*0 errors*)
Disc/Minute:0 (*0 discards*)
Percent Err:0.0% (*42 pkts w/o error*)
Last updated Jun 23, 12:21:02; sample: 37.94 seconds.

Typical Link Status.

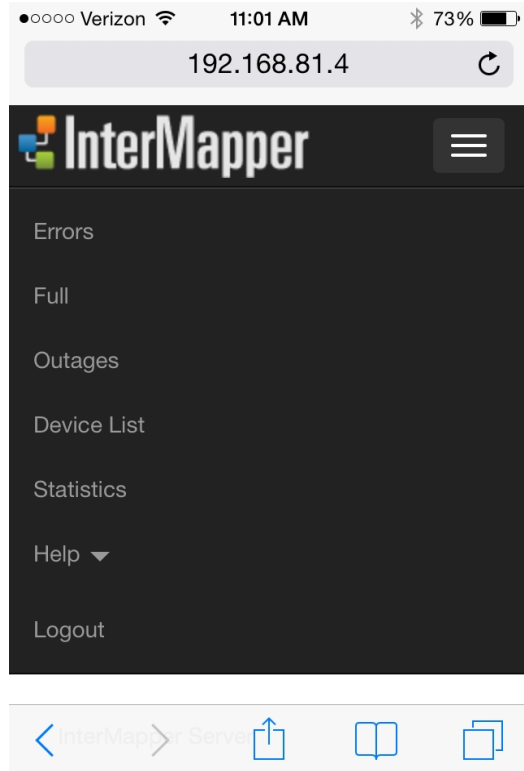
Map Status

When you click a Map Status item, the map associated with that device appears, rather than an information window.

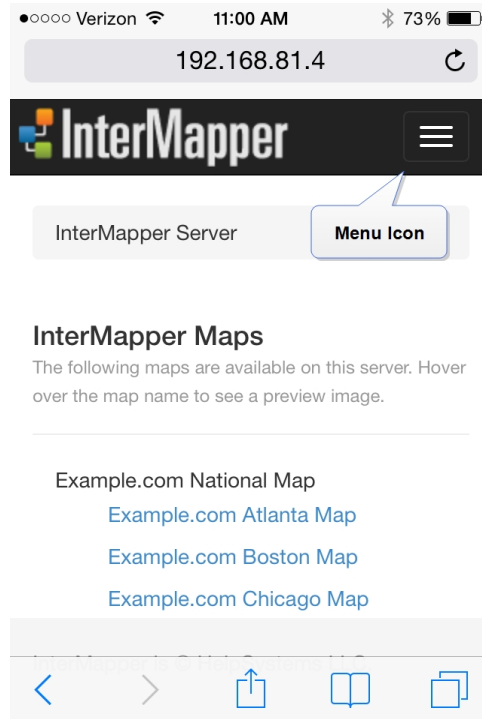
Using InterMapper Web Server on Mobile Devices

The InterMapper Web Server supports viewing on mobile devices.

Tap the menu icon (shown at right) to view the web server menu, shown below.



Web Server menu on an iPhone



The Error and Full Pages

Use the **Error Page** to view devices, networks, and links that are down, or in alarm or warning states.

- **If you are an InterMapper administrator**, this page appears by default when you first connect your browser to the InterMapper web server.
- **If you are not an administrator**, the Error page is available only if you are a member of the "FullWebAccess" group.
- **By default** you are directed to the first map (alphabetically) in the map list to which you have access.

Use the **Full Page** to view all devices, networks, and links being monitored by InterMapper, not just those with problems.

Both the Error and Full web pages have the same format, shown below.

- Click a link in the left column of either page to view detailed information about the link, device, or network.

The [Home Page \(Pg 691\)](#) topic shows typical Device and Network Status.

The screenshot shows the InterMapper web interface. The browser address bar displays 'http://192.168.81.4:8080/~admin/error_screen.html'. The page title is 'InterMapper Devices in Error'. The navigation bar includes links for 'Errors', 'Full', 'Outages', 'Device List', 'Statistics', and 'Help'. The main content area is titled 'InterMapper Server / Errors' and 'Devices and Links with Errors'. It shows a summary: 'Jul 29 11:17:06 34 nodes, 1 down, 70 links, 1 down, 1075 pk/s, 120686 K by/s'. Below this is a table of devices and links.

Device	Stat	SysUpTime (Down Since)	Avail	Loss	RTT	Probe	Address
Warehouse	ALRM		100.0	0.0	0	Map	127.0.0.1
192.168.11.222	DOWN	07/29 11:16 AM	99.3	3.2	0	Demo	192.168.11.222

Link	Prt	Stat	TPkt	TBytes	TErr	TDis	RPkt	RBytes	RErr	RDis	Util	Segment
Wired &	3	up	16	62277	1*	0	16	62277	1*	0	33.2%	to
John	1	up	18	0	1*	0	18	0	1*	0	0.0%	192.168.1.0/24
Susan	5	up	11	1602	1*	0	11	1602	1*	0	22.9%	192.168.1.0/24
Chicago Router	7	up	18	35342	2*	0	18	35342	2*	0	37.7%	To
Duncan Homer	1	up	31	0	6*	0	31	0	6*	0	0.0%	Wireless Link
Ken Ambrose	1	up	29	0	4*	0	29	0	4*	0	0.0%	Wireless Link
Philip Briar	1	up	14	0	2*	0	14	0	2*	0	0.0%	Wireless Link
Wilbur Trueman	1	up	19	0	2*	0	19	0	2*	0	0.0%	Wireless Link
Jason Grover	0	up	22	5596766	4*	0	22	5596766	4*	0	44.8%	Wireless Link
Jason Grover	0	up	22	5596766	4*	0	22	5596766	4*	0	44.8%	Wireless Link

The InterMapper Errors page

Device	Stat	SysUpTime (Down Since)	Avail	Loss	RTT	Probe	Address
Wired &	UP		100.0	0.0	0	Demo	10.1.3.2
Fred	UP		100.0	0.0	0	Demo	192.168.5.172
Mary	UP		100.0	0.0	0	Demo	192.168.5.1
John	UP		100.0	0.0	0	Demo	192.168.5.171
Susan	UP		100.0	0.0	0	Demo	192.168.5.171
Chicago Router	UP		100.0	0.0	0	Demo	10.1.2.2
Duncan Homer	UP		100.0	0.0	0	Demo	192.168.4.174
Marti Lashawn	UP		100.0	0.0	0	Demo	192.168.4.177
Tranter Garey	UP		96.9	3.2	0	Demo	192.168.4.172
Cheyenne Brent	UP		93.9	3.3	0	Demo	192.168.4.175
Ken Ambrose	UP		100.0	0.0	0	Demo	192.168.4.173
Philip Briar	UP		100.0	0.0	0	Demo	192.168.4.178
Wilbur Trueman	UP		96.9	3.2	0	Demo	192.168.4.176
Jason Grover	UP		100.0	0.0	0	Demo	192.168.4.171
Warehouse	UP		100.0	0.0	0	Map	127.0.0.1
Router/	UP		100.0	0.0	0	Demo	192.168.1.2

The InterMapper Full page.

Viewing the Summary Information

The top line shows a summary of items being monitored in all open maps. They are, in order:

- **date** and **time** the page was generated
- **number of nodes** being monitored
- **number of devices** currently shown as down
- **number of links** being monitored
- **number of links** currently shown as down
- **total packets per second** entering the network
- **total bytes per second** entering the network

Viewing Device Status

The first detailed section of the page shows *devices* that are down, or are in alarm or warning states. The Device section shows:

- **Device** - device name (click the link for more information)
- **Stat** - device status
- **SysUptime** - device uptime
- **Avail** - availability
- **Loss** - packet loss
- **RTT** - round-trip time
- **Probe** - probe type
- **Address** - network address

Viewing Networks and Link Status

The second detailed section of the page shows *networks* and *links* that are down, or are in alarm or warning states. The Link section shows:

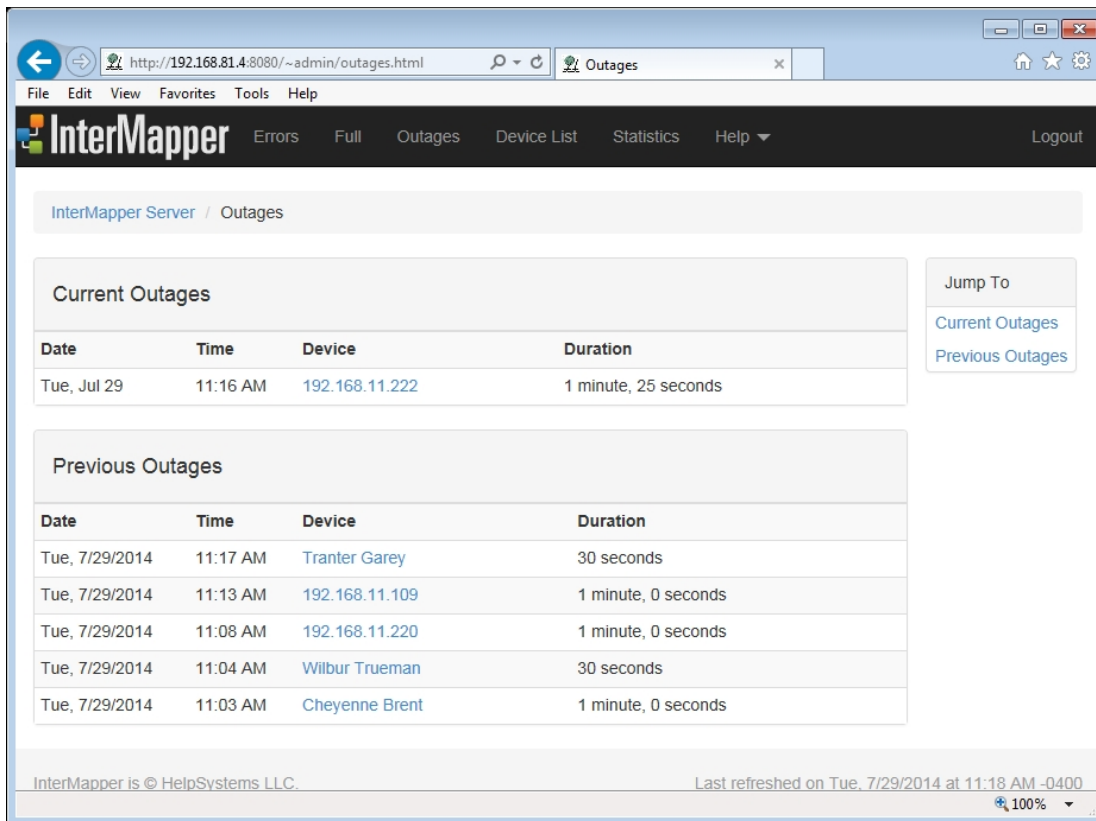
- **Link** - device name (click the link for more information)
- **Prt** - device port number
- **Stat** - device status
- **TPkt, TBytes, TErr, TDis** - transmit information (transmitted packets and bytes per second, transmit errors and discards per minute)
- **RPkt, RBytes, RErr, RDis** - receive information (received packets and bytes per second, received errors and discards per minute)
- **Util** - network utilization
- **Segment** - segment name (if any)

The Outages Web Page

Use the Outages web page to view a history of outages, as shown below.

- Click an active link on the Outages Web page to view detailed information as described in the [Map Web Page](#) topic.

The Outages web page lists up to 10 outages for each device.



The screenshot shows the InterMapper web interface. The browser address bar displays `http://192.168.81.4:8080/~admin/outages.html`. The page title is "Outages". The navigation bar includes links for "Errors", "Full", "Outages", "Device List", "Statistics", and "Help", along with a "Logout" button. The main content area is titled "InterMapper Server / Outages". It features two tables: "Current Outages" and "Previous Outages". The "Current Outages" table has one row showing an outage on Tue, Jul 29 at 11:16 AM for device 192.168.11.222, lasting 1 minute and 25 seconds. The "Previous Outages" table lists five past outages from Tue, 7/29/2014, with durations ranging from 30 seconds to 1 minute. A "Jump To" sidebar on the right contains links for "Current Outages" and "Previous Outages". The footer indicates "InterMapper is © HelpSystems LLC." and "Last refreshed on Tue, 7/29/2014 at 11:18 AM -0400".

Date	Time	Device	Duration
Tue, Jul 29	11:16 AM	192.168.11.222	1 minute, 25 seconds

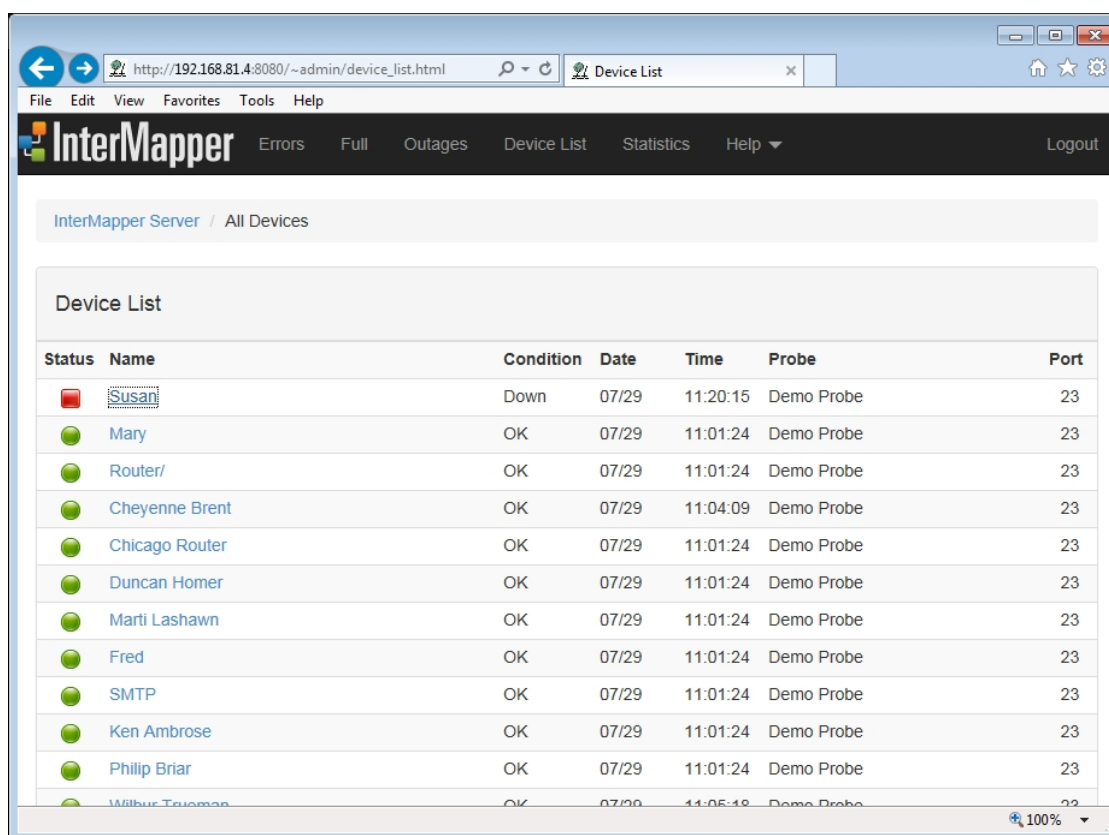
Date	Time	Device	Duration
Tue, 7/29/2014	11:17 AM	Tranter Garey	30 seconds
Tue, 7/29/2014	11:13 AM	192.168.11.109	1 minute, 0 seconds
Tue, 7/29/2014	11:08 AM	192.168.11.220	1 minute, 0 seconds
Tue, 7/29/2014	11:04 AM	Wilbur Trueman	30 seconds
Tue, 7/29/2014	11:03 AM	Cheyenne Brent	1 minute, 0 seconds

The InterMapper Outages web page.

The Device List Web Page













Use the Device List web page to view a list of devices appearing in all open maps. The list shows each device's status, name, condition, and date and time of the last change in status.

- Click a link to view detailed information about a device. The example below shows a typical Device List web page.



InterMapper Server / All Devices

Device List

Status	Name	Condition	Date	Time	Probe	Port
	Susan	Down	07/29	11:20:15	Demo Probe	23
	Mary	OK	07/29	11:01:24	Demo Probe	23
	Router/	OK	07/29	11:01:24	Demo Probe	23
	Cheyenne Brent	OK	07/29	11:04:09	Demo Probe	23
	Chicago Router	OK	07/29	11:01:24	Demo Probe	23
	Duncan Homer	OK	07/29	11:01:24	Demo Probe	23
	Marti Lashawn	OK	07/29	11:01:24	Demo Probe	23
	Fred	OK	07/29	11:01:24	Demo Probe	23
	SMTP	OK	07/29	11:01:24	Demo Probe	23
	Ken Ambrose	OK	07/29	11:01:24	Demo Probe	23
	Philip Briar	OK	07/29	11:01:24	Demo Probe	23
	Wilbur Truman	OK	07/29	11:05:18	Demo Probe	23

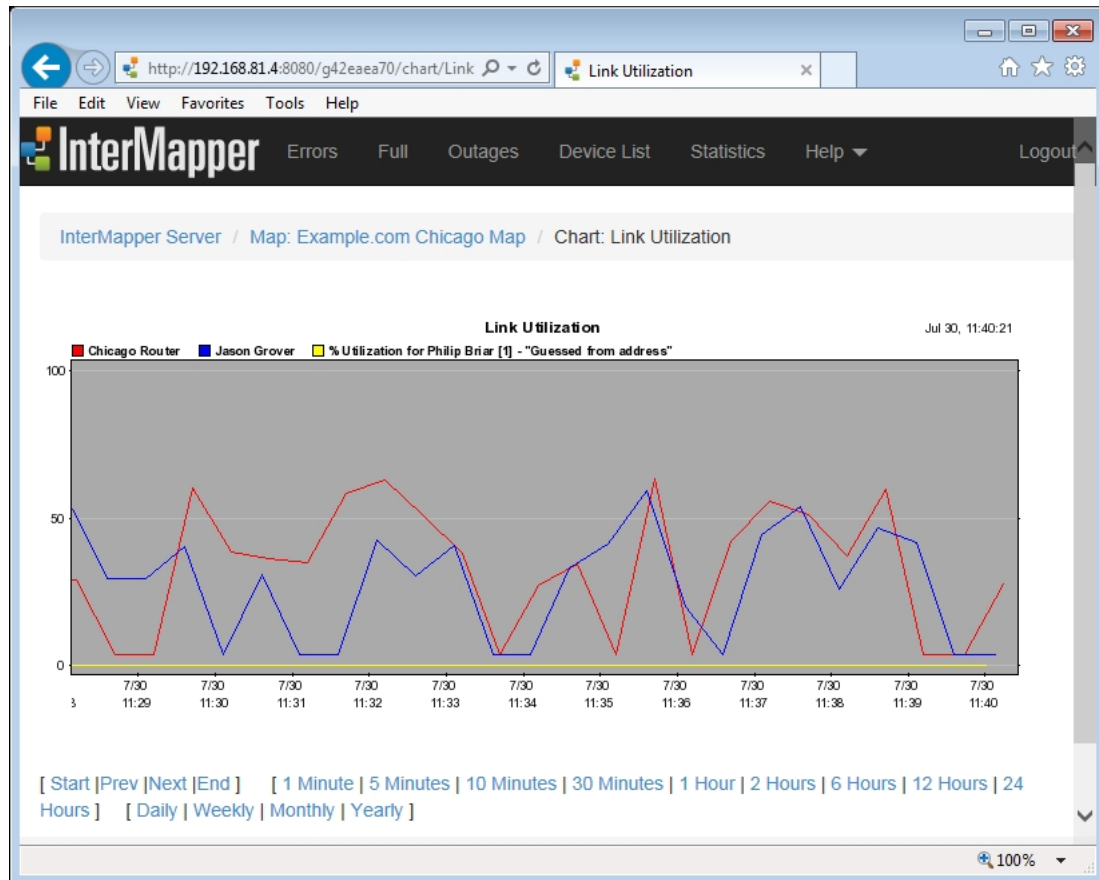
Web Device List. This shows the status of all the devices InterMapper is monitoring, sorted by severity of their status.

Viewing a Chart

Use the Chart web page to view the selected chart.

When view a map's page, a list of the charts associated with the map appears. The list appears only if charts have been created.

- Click on a chart name to view the chart.
- Click the **Start**, **Prev**, **Next** or **End** links to show different parts of the history.
- Click the links below the chart to choose the period you want to view.



A typical chart

Chapter 19

Telnet Server Command Reference

The Telnet Server uses a text-based command-line interface to provide information about devices and networks in maps that are open in InterMapper.

Here is summary of the features and functions available from the Telnet Server, as shown through the server's help system. For each command listed below, click [\[details \]](#) to view the server help for that command:

```
Welcome to the InterMapper [version #] operations interface.  
Enter 'help' for command list.  
> help  
=====
```

ERROR

- Shows a report of all devices and links that exceed some threshold. This report is updated every minute. For detailed information about the fields and columns of this report, type "help error". This is the default command when you connect. [\[details \]](#) (Pg 704) (Abbreviations: "E", "ERR")

FULL

- Shows a report of all devices and links being monitored. [\[details \]](#) (Pg 704) (Abbreviations: "F")

NODE <name-prefix>

- Shows a report of the named device using the same format as the "ERROR" report. This report is updated every time InterMapper polls the device. [\[details \]](#) (Pg 704) (Abbreviations: "N")

BUS <name-prefix>

- Shows a report of the named network or segment using the same format as the "ERROR" report. This report is updated every minute. [\[details \]](#) (Pg 704) (Abbreviations: "B")

DOWN- Lists all devices that are down. The same functionality is also provided by the ERRORS command. [\[details \]](#) (Pg 705)

LDOWN- Lists all interfaces (ie links) that are down. The same functionality is

also provided by the ERRORS command. [\[details \]](#) (Pg 707)

LOG []
- Displays the last entries from the event log window and continuously displays new log lines. [\[details \]](#) (Pg 707)

KALI [<conn> ["compress" | "kill"]]
- Displays list of Kali connections and allows you to debug them. [\[details \]](#) (Pg 706)

KALID
- Displays a list of the maps, log, lists, and other shared resources open by each Remote connection. [\[details \]](#) (Pg 707)

HELP [<topic>]
- Without a parameter, the help command displays this help text. If you include the name of the command as the parameter, it displays detailed information about the format of the report generated by it. [\[details \]](#) (Pg 706)

QUIT- End the telnet session and disconnect. [\[details \]](#) (Pg 707)

RELOAD
- Closes all map files and reopens them. This command is only implemented in the server/daemon version of InterMapper. [\[details \]](#) (Pg 708)

REMOTE <hostname> [<port>]
- Initiates a remote connection with a client at hostname, listening on <port>, rather than the usual procedure of a client initiating a connection with the server.
This is useful when the server is behind a firewall. InterMapper Support may occasionally ask you to do this in order to let us take a look at your system without requiring you to adjust your firewall. If the port is not specified, it is assumed to be 8181.

DETAILS < "net" | "graph" | "collaborator" | "smtp" | "probe" >
 - Toggles detailed logging to the debug log for the indicated class of events. InterMapper Support may occasionally ask you to do this in order to provide us with more detailed information about what is happening when you run InterMapper.

SERVER <server> < "start" | "stop" | "status" > [<port>] ["secure"
]
 - Start, stop or change one of the three servers: Web, Telnet or Remote. [\[details \]](#) (Pg 708)

TELNET
 - Displays a list of current connections to the Telnet server. [\[details \]](#) (Pg 708)

USERS [<UID>] - Displays a list of users with user IDs. Include the user ID to delete the user.

WEB
 - Displays a list of current connections to the Web server. [\[details \]](#) (Pg 709)

Command Details

> **help error**
 The ERROR, FULL, NODE, and BUS commands emit a report with three parts:
 (1) a status line summarizing the condition of the entire network
 (2) a node report
 (3) a link report.

Example:

```
Jul 31 11:11:58  2 nodes,   1 down,   8 links,   0 down,  461 pk/s,
                141 K by/s
```

Name	Stat	SysUpTime	Probe	Address
egg-1	DOWN	0+00:00:00	ICMP	127.110.13.210

Name	Prt	Stat	TPkt	TBytes	TErr	TDis	RPkt	RBytes	RErr	RDis
Util										
Segment										
egg-1	1	UP	46	13790	0	0	67	10152	12*	0
1% 127.0.13.0/24										
egg-1	2	UP	78	8330	0	0	586	144524	14*	0
12% 127.0.14.0/24										

(1) THE STATUS LINE
 Jul 31 11:11:58 2 nodes, 1 down, 8 links, 0 down, 461 pk/s,
 141 K by/s
 In order, these fields are:

- the date and time of the report
- the total number of devices
- the number of devices which are down
- the total number of links
- the number of links which are down
- the sum of pkts per second transmitted on all links
- the sum of bytes per second transmitted on all links

(2) NODE REPORT

```
Name          Stat  SysUpTime    Probe  Address
```

The columns are:

- Name - the name of the device
- Stat - the status of the device (UP, DOWN, or ACK)
- SysUpTime - the number of days + hh:mm:ss that the device has been running
- Probe - the type of probe used to check the device
- Address - the address of the device (where the probes are sent)

(3) LINK REPORT

```
Name          Prt  Stat  TPkt  TBytes  TErr  TDis  RPkt  RBytes  RErr  RDis
Util
Segment
```

The columns are:

- Name - the name of the device
- Prt - the interface number
- Stat - the status of the interface (UP, DOWN, or ACK)
- TPkt - the number of pkts per second transmitted on this interface
- TBytes - the number of bytes per second transmitted on this interface
- TErr - the number of packets per minute lost due to errors
- TDis - the number of packets per minute dropped due to resource limitations
- RPkt - the number of pkts per second received on this interface
- RBytes - the number of bytes per second received on this interface
- RErr - the number of packets per minute received with an error
- RDis - the number of packets per minute dropped due to resource limitations
- Util - the percentage utilization of the interface
- Segment - the name of the network or segment attached to this interface

The * following a value indicates that the value is above the threshold. This is useful because it tells you why the link is being displayed as part of the error report.

> help down

The DOWN command lists all devices which currently have the 'DOWN' or 'DOWN-ACK' status.

Each line of the DOWN list has the format:

```
mm/dd hh:mm:ss  DOWN      <Device-Name>
```

For devices which are acknowledged down, the following format is used:

```
mm/dd hh:mm:ss DOWN-ACK <Device-Name>
```

> **help**

HELP [<topic>]

- Without a parameter, the help command displays this help text. If you include the name of the command as the parameter, it displays detailed information about the format of the report generated by it.

> **help kali**

KALI [["compress" | "kill"]]

Displays a list of current InterMapper RemoteAccess connections and allows you to monitor them.

When you enter "KALI" without any arguments, the response is a list of the current InterMapper RemoteAccess connections in the form:

ID	USER	REMOTE ADDRESS	IN	OUT	LOGING
366a58	<listener>	<server-port 8181>	0	0	-
485d58	Guest	198.115.166.18:58619	20339	177408	Oct 02, 15:51:12
2d18b8	<listener>	<server-port 8181>	0	0	-

The second and third columns identify the user and their source IP address. The two users marked "<listener>" are the server's two pending listening connections for port 8181.

The first column of output is the identifier for the connection. To monitor an existing connection, type "KALI <conn>" where <conn> is a connection ID.

To monitor the next new connection to the server, use "next" for the connection ID; i.e. type "KALI NEXT".

Monitoring a remote connection turns off compression for the data stream; this

makes it easier to see the actual traffic. To leave compression enabled when

while monitoring, include the "compress" option; i.e. type "KALI <conn> COMPRESS".

To forcibly disconnect an existing connection, type "KALI <conn> KILL".

This command will terminate the remote connection and release its resources on the server.

> help kalid

Displays a list of the maps, log, lists, and other shared resources open by each Remote connection.

Here is some sample output:

```
+ CKaliOpenMapList [2d6008] user='Guest' [ADMIN]
- [485d58] Guest@198.115.166.18:58619
+ CKaliOpenLogList [351cd8] addr='198.115.166.18' user='Guest'
[ADMIN]
- [485d58] Guest@198.115.166.18:58619
+ CKaliOpenSoundSetList [351d68]
- [485d58] Guest@198.115.166.18:58619
```

This indicates that the remote connection [485d58] is responsible for an "open map list", an "open log list", and an "open sound list". Essentially, this means that client will be notified of any changes to those lists. If this user had opened a map, you would see them registered for that "open map"; i.e. they would be notified of any changes.

Multiple connections may be registered for the same resource, the output above only shows the server state with one connection.

> help ldown

The LDOWN command lists all interfaces which currently have the 'DOWN' status. The LDOWN report does not include interfaces which are hidden and therefore not being polled. Each line has the following format:

```
mm/dd hh:mm:ss DOWN <Device-Name>:<ifIndex>:<ifDescr>
<ifIndex> is the index of the interface in the interface table,
and <ifDescr> is a description of the interface.
```

> help log

Displays the last <num-lines> entries from the event log window and continuously displays new log lines. The format of the LOG output is exactly the same as the format of the "Event Log" window of the InterMapper program.

> help quit

QUIT
- End the telnet session and disconnect.

> help reload

RELOAD

Closes all map files and reopens them. This command is only implemented in the server/daemon version of InterMapper.

This command is for experimental purposes. You should avoid using it; it may go away in future versions.

> help server

```
SERVER <server> < "start" | "stop" | "status" > [ <port> ] [ "secure" ]
```

Start, stop or change one of the three servers: Web, Telnet or Remote.

To start a server on the same or different port number (with SSL/TLS disabled), type:

```
server <server> start <port>
```

To start the server with SSL/TLS enabled, type:

```
server <server> start <port> secure
```

In both cases, <server> must be one of "web", "telnet" or "remote".

To stop a server, type:

```
server <server> stop
```

Note: You cannot stop the Telnet server using the SERVER command. However, you can restart the telnet server on a different port number. When you do this, your own telnet connection will be disconnected immediately.

To receive a quick status report on all three servers, type "server status".

This command combines the output of the "web", "telnet" and "kali" commands.

> help telnet

TELNET

Displays a list of current connections to the Telnet server.

```
ID USER REMOTE ADDRESS IN OUT LOGIN@
404c28 <listener> <server-port 23> 0 0 -
3f63a8 Guest 192.168.1.21:49176 0 0 -
2d60e8 <listener> <server-port 23> 0 0 -
```


This command is similar in output to the KALI command. It lists the source and login ID of any existing telnet connections. However, unlike the KALI command, you cannot monitor or terminate telnet connections using the TELNET command; you can only receive a status report.

Note: The IN, OUT, and LOGIN@ stats are not implemented for the TELNET command.

> **help web**

WEB

Displays a list of current connections to the Web server. The web server normally does not allow HTTP connections to linger, so the list of current connections should never grow very large.

ID	USER	REMOTE ADDRESS	IN	OUT	LOGIN@
38af68	<listener>	<server-port 80>	0	0	-
35f518	<listener>	<server-port 80>	0	0	-
478478	<listener>	<server-port 80>	0	0	-
39f308	<listener>	<server-port 80>	0	0	-
473e98	<listener>	<server-port 80>	0	0	-
481bb8	<listener>	<server-port 80>	0	0	-

This command is similar in output to the KALI command. It lists the source and login ID of any existing web connections. Since the web server has to deal with the possibility of many simultaneous hits, the number of reserve pending listeners is larger than for the other server.

Unlike the KALI command, you cannot monitor or terminate web connections using the WEB command; you can only receive a status report.

Note: The IN, OUT, and LOGIN@ stats are not implemented for the WEB command.

Chapter 20

Command-line Options

Command-line Options for InterMapper

A number of command-line options are available for use with InterMapper.

Usage:

```
intermapperd [OPTIONS] (Mac OS/Linux*)  
intermapper.exe [OPTIONS] (Windows)
```

*For Mac OS and Linux, you may need to use the full path to the executable (/usr/local/bin/intermapperd) in order for some options to work correctly.

Argument	Description
-h -? --help	Display this help text and exit.
-v --version	Print the version number.
-f <file>	Use the specified configuration file.
-A <user-addr>	Add the specified 'user[:pass]@address' to the access list. Extended options: -u --user <name> Run as this user. (Overrides 'User' directive) --group <name> Run as this group. (Overrides 'Group' directive)
-u --user <name>	Run as this user. (Overrides 'User' directive)
--group <name>	Run as this group. (Overrides 'Group' directive)
--settings <path>	Specify path to 'InterMapper Settings' directory. (Overrides 'SettingsFolder' directive)
--fonts <path>	Specify path to 'Font' directory. (Overrides 'FontFolder' directive)
--listen <address>	Listen only on the interface with the specified IPv4 address. Disable IPv6.
--port <port>	Listen for remote connections on the specified TCP port.
--no-daemonize	Do not fork and disassociate from the controlling terminal.
--no-ipv6	Disable IPv6 support.
--no-ssl	Disable SSL for remote connections.
--test-only	Run tests and exit.
-d --debug	Enable debug mode; don't disassociate from controlling terminal.
--printconfig	Print the daemon's configuration.
--getenv <var>	Get the value of <var> in the InterMapper environment.

<code>--setenv <var>=<val></code>	Set the value of <var> to <val> in the InterMapper environment.
<code>--wrap <filename></code>	Wrap the probe bundle defined by the bundle header at <filename>.
<code>--output <filename></code>	Put output of wrap operation in file at <filename>.
<code>--suppress-avail</code>	Suppress the 'availability' statistic in device status windows.
<code>--verify-permissions</code>	Check the permissions of all files in the 'InterMapper Settings' directory.
<code>--check-upgrade <date></code>	Check the release manufacture <date> against the maintenance contract date.
<code>--detail <log></code>	Turn on detailed logging for the type indicated by <log>.
<code>--ciphers <all default list></code>	Show supported SSL ciphers.
<code>--chart-purge <days></code>	Purge chart data to maximum <days> history.

Command-line Options for RemoteAccess

You can call InterMapper RemoteAccess from a command line, and control a significant number of functions. This can be useful for automating the updating of maps, or for various testing purposes.

InterMapper RemoteAccess currently supports the following command-line arguments:

Argument	Description
<code>-host --host <HOST></code>	connect to the specified HOST
<code>-port --port <PORT></code>	connect to the specified PORT on HOST (defaults to 8181)
<code>-map --map <MAP_NAME></code>	load the specified map(s) from HOST (separate map names with ":")
<code>-import --import <FILE_NAME></code>	import the specified file (use - for stdin)
<code>-importmap --importmap <FILE_NAME></code>	import the specified map.
<code>-export --export <EXPORT-SPEC></code>	export the specified data to stdout.
<code>-exportmap --exportmap <MAP_ID></code>	Note: Data for all maps is exported. export the specified map Note: The easiest way to get the map ID is to look in the Maps folder in the InterMapper Settings folder. Each map name has a prefix that begins with "g". The text between the "g" and the hyphen ("-") is the Map ID.
<code>-f --file <FILE_NAME></code>	open the specified shortcut file
<code>-d --debug <DEBUG_CONFIG_FILE></code>	use the specified configuration file to configure debugging output

-D<name>=<value>	set a system property
-user --user <USER>	log in as USER
-pass --pass <PASSWORD>	log in as USER with PASSWORD
-ignore-cert-check	accept all server SSL certificates without prompting
-agree-to-license	accept the End User License Agreement
-version --version	print product version
-env --env	print out system properties
-test --test [TIMEOUT]	test the connection - automatically quit after TIMEOUT seconds
-h -? --help	print this help message

Windows Users

The syntax for Windows users is essentially the same as the Linux/Unix examples below, except that the command line requires the full Windows path to InterMapper's Java installation (rather than any other installations of Java that might exist on the machine.) The following example sets the working directory to the .jar file, then invokes java with the .jar file:

```
cd "[jar file location]"
"C:\Program Files\InterMapper\java\bin\java" -jar \[jar file name].-
jar
```

Remember to use this approach for all of the examples below, replacing `java` with the full path to the InterMapper Java installation.

Examples for Import commands

To import to a specified server, IM Remote is invoked as follows:

```
java -jar <jar-file> --host <intermapper-server> [--user <username>
--pass <password>] --import <import-file>
```

The example below reads imported data from `newdata.tab`.

```
java -jar intermapper_remoteaccess.jar --host big.dartware.com --
user admin --pass adminpw --import newdata.tab
```

The example below reads imported data from `stdin`.

```
java -jar intermapper_remoteaccess.jar --host big.dartware.com --
user admin --pass adminpw --import -
```

The `stdin` form of the `--import` option allows Unix users to create self-contained executable files that import stuff:

```
#!/usr/bin/java
-jar intermapper_remoteaccess.jar --host big.dartware.com --import -
#import blah blah
  blah
blah blah
  blah
blah blah
  blah
```

One use for this would be to automate testing of InterMapper Server.

Examples for Export commands

To export from a specified server, IM Remote is invoked as follows:

```
java -jar <jar-file> --host <intermapper-server> [--user <username>
--pass <password>] \
--export "format=<output-type> table=<table-name> fields=<field-
list>
```

The example below writes exported data to `stdout`.

```
java -jar intermapper_remoteaccess.jar --host big.dartware.com --user
admin --pass adminpw --export "format=tab table=devices fields=*"
```

Using InterMapper With Splunk

InterMapper works with Splunk by sending syslog entries in a specific format when an InterMapper device changes state. An add-on application in Splunk allows you to analyze and view various events through an InterMapper-specific dashboard.

Use the information below to connect InterMapper to Splunk.

System Requirements

To use Splunk with InterMapper, you need:

- A local or remote installation of Splunk Enterprise.
- The InterMapper web server must be running.
- The Splunk machine must have access to the InterMapper server.
- A syslog notifier that sends information to Splunk must be attached to all devices you want to track with Splunk.

Installation Overview

In order to use Splunk and InterMapper together, you need to do the following:

1. Prepare InterMapper. This includes enabling the Web server, adding a syslog notifier for Splunk, and setting the syslog message for compatibility with Splunk.
2. Set up InterMapper to send syslog notifications to Splunk.
3. Install the InterMapper App for Splunk.

Preparing InterMapper for use with Splunk

Before you can use Splunk with InterMapper, you have to set up InterMapper to allow Splunk to access it. The steps are as follows:

Step 1: Enable the Web server

Before you can use Splunk, you need to enable the InterMapper web server.

To enable the web server:

1. From the Edit menu, choose **Server Settings...** The Server Settings window appears.
2. In the left pane of the Server Settings window, click **Web Server**. The Web Server configuration panel appears.
3. In the Web Server configuration panel, click **Start**.
Note: You can choose to run the web server on a different port, but will need to enter that port in the Splunk application when you set it up.
4. Add an access control list entry to allow web server access by the Splunk host machine. Access is based on IP address.
5. Add one or more access control list entries to allow web server access by any users of the Splunk application. Access is based on IP address or address range.

Step 2: Add a Splunk user

You need to add a user account to InterMapper that Splunk can use to log in to the InterMapper server.

To add a user:

1. In the left pane of the Server Settings window, click **Users**. The Users panel appears.
2. Click the **+** button and choose **Add User...** The User Information dialog appears.
3. In the **Name** box, enter a user name for the Splunk Server.
4. In the **Automatic Login** text box, enter the IP address of the Splunk server.
5. Click **OK**. The Splunk Server user appears in the user list.
6. Drag the Splunk Server user to the Administrators group. The Splunk Server user requires elevated privileges to export details about InterMapper maps.

Step 3: Add a syslog notifier for Splunk

Splunk acts as a syslog server. You need to create a syslog notifier that InterMapper can use to send syslog entries to Splunk.

To create a syslog notifier:

1. From the Server Settings window, click **Notifier List**. The list of existing notifiers appears.
2. Click the **+** button. The Configure Notifier window appears.
3. Give the notifier a name, such as "SplunkLog".
4. From the Notifier Type dropdown menu, choose **Syslog**.
5. Enter the Splunk server's IP address in the **Send syslog message to** box.
6. Click Edit Message, then edit the syslog message as follows:

```
timestamp="<Timestamp>" map name="<Document Name>" notification
level="<Event>" device host="<Device Name>" device ip="<Device
Address>" probe_type="<Probe Type>" probe_message="<Device Condi-
tion>"
```

Note: The message above must be on one line.

This format allows Splunk to extract syslog data and make it available in Splunk.

Step 4: Attach the notifier to all devices

Once you have created the Splunk notifier, you need to attach it to all devices in InterMapper.

To attach a notifier to all devices:

1. From InterMapper's Window menu, choose **Device List**. The Device List window appears, showing a list of devices.
2. Click the **Notifier View** button near the left end of the window's toolbar. A set of checkboxes appears for each device.
3. From the dropdown menu just to the right of the View selection buttons, choose the Splunk syslog notifier you just created.
4. For each state you want to record in Splunk, hold **Alt** and click a check box in the column for that state. All check boxes are selected.
5. Recommended settings for Delay, Repeat time, and Count:

Delay = none
Repeat time = 5 minutes
Count = infinite

Hold **Alt**, click the dropdown menu for each column, then release the **Alt** key and choose the value from the dropdown menu. It is set for each device in the list.

Notes:

- Set your Splunk notifier to be attached to new devices by default from the **Default Notifiers** panel of the Map Settings window.
- To send data to Splunk for only a single map, you can view devices in the map's Notifier View and attach only the devices in that map to the Splunk notifier.

Step 5: To send Layer 2 information

To send Layer 2 information to Splunk you must do the following:

- Set up InterMapper to collect Layer 2 information. See the InterMapper User Guide for more information.
- Add a device to any InterMapper map, and apply the Splunk > Layer 2 Output probe to it. Otherwise, use the information below to locate and upload the probe.

Note: *One and only one* device using this probe should exist on an InterMapper server. Running multiple instances of this probe uses InterMapper server resources unnecessarily, with no benefit to the InterMapper App for Splunk.

The probe is located in the Splunk install directory (%SPUNK_HOME%) at:

```
%SPUNK_HOME%\etc\apps\InterMapper\default
```

Probe file name: `com.dartware.layer2`

The probe sends switch port data in CSV format to Splunk; the data is then interpreted and indexed in Splunk.

Step 6: Get Notifications Into Splunk

Assuming a clear network route between InterMapper and Splunk, and that you are running Splunk as `root`, indexing of syslog data by Splunk begins nearly immediately.

To verify that Splunk is receiving InterMapper data:

- Do a search in Splunk on `sourcetype=intermapper`.

Step 7: Installing the InterMapper App for Splunk

The InterMapper App for Splunk automatically configures Splunk to receive and interpret syslog data from InterMapper.

In order for Splunk to present collected data in an InterMapper-specific way, you need to install the InterMapper App for Splunk.

To install the InterMapper App for Splunk:

1. From Splunk's **Apps** menu (in the Web UI), choose **Find More Apps...** The Browse More Apps page appears.
2. Enter "InterMapper" in the search box, and click the Search button or press **Enter**. The InterMapper App for Splunk appears.
3. Click the **Read More** link. The description page for the InterMapper App for Splunk appears.
4. Click **Download**, log into your Splunk account, and save the file in a location accessible to your browser.
5. From the Web UI or your Splunk installation, choose **Manage Apps...** from the Apps menu. The Apps Manager page appears, showing all currently installed Splunk Apps.
6. Click **Install App from File**. The Upload an App page appears.
7. In the File box, click **Browse**, and navigate to the App file you downloaded.
8. If you have installed a previous version, click to select **Upgrade App**.
9. Click **Upload**. The app is installed. You will be asked to restart your Splunk server.
10. Click **OK** to restart your Splunk server.
11. From the Apps menu, choose **InterMapper**. A configuration notice appears.
12. Follow the links to the Configuration page.
13. Enter the IP address and port of the InterMapper web server in the form "[address]:[port]", and the name of a default map, and click **Save**.
14. After a few moments, the InterMapper page appears with the default map.

Chapter 21

Troubleshooting InterMapper

- [How do I change the community string? \(Pg 719\)](#)
- [How do I monitor a fixed IP address? \(Pg 719\)](#)
- [I still can't make my router talk... \(Pg 719\)](#)
- [My switches are always orange and showing lots of errors \(or discards\). Why? \(Pg 720\)](#)
- [What does it mean when InterMapper says a "subnet mask is discontinuous"? \(Pg 720\)](#)
- [Why do network labels sometimes have a "/2*"? \(Pg 721\)](#)
- [Why won't a device connect to the proper subnet oval? \(Pg 721\)](#)
- [There are two separate network ovals on my map where there should only be one... \(Pg 721\)](#)
- [Some network ovals have more than one IP network number... \(Pg 721\)](#)
- [Does InterMapper support unnumbered IP links? \(Pg 722\)](#)
- [What does it mean when a Status Window shows "\[ifIndex not in ifTable\]" ? \(Pg 722\)](#)
- [How can I find out how many devices I'm monitoring with InterMapper. Do I have to count all the boxes on each map? \(Pg 722\)](#)
- [I get an error message: "This InterMapper Server already appears to be associated with the InterMapper Database. Existing UUID is associated with a different URL". \(Pg 725\)](#)

How do I change the community string?

You can open the **Show Info** window on a device as described in the [Monitor menu \(Pg 390\)](#) reference topic.

To set the community string:

1. Select the devices for which you want to change the community string.
2. From the Monitor menu, choose **Set Community**. The Set Community window appears.
3. Enter a Community string and click **OK**.

Use this procedure to set the Read-Only community string for one or more devices at once.

How do I monitor a fixed IP address?

In the **Add Device...** dialog, enter an IP address in dotted-decimal notation .

IP addresses discovered using the IP discovery feature are fixed by default.

I still can't make my router talk...

If you still can't make the router work with InterMapper, try the following:

- From the Help Menu's Diagnostics submenu choose **Server Log**, or from the Window menu's Logs submenu, choose **Debug**. Look for any messages

related to that device.

- Let us know. Send E-Mail to support@intermapper.com with information about the type of device and the trouble you're having.

My switches are always orange and showing lots of errors (or discards). Why?

We frequently hear of devices that appear to have high levels of discards and/or errors. They are usually orange on the map, and the status window shows a message like this:

```
Reason: Discards = 738: [1] sc0
```

The most likely reason that InterMapper shows a high rate of discards from a device is that the device is actually reporting these errors. It's common that when InterMapper reports errors (from its SNMP queries), the manufacturers' own monitoring tools will report zero errors. (It's also normal that the affected devices are operating normally, without problems, in this state.)

Experiments and Workarounds:

1. Use the vendor's own network monitoring tool (by telnetting in, using a web browser, etc.) to see if errors are being reported through the native management interface. It's possible that there actually *is* a problem.
2. This may be a bug in the SNMP implementation of the device. You can check with your vendor to see if there's a firmware upgrade that addresses the problem.
3. To test InterMapper's accuracy, use another SNMP console to check out the particular MIB variables for the device. InterMapper monitors the `ifInDiscards` and `ifInErrors` MIB variables (and the corresponding `ifOutxxxx` variables) listed on the [Network and Server Probes \(Pg 608\)](#) page to compute its error & discard figures.

You can monitor these same variables with your SNMP Console to see if the same errors are reported there.

4. Run a ping test through the device that's reporting the errors.
 - If packets are actually being discarded, you'll see a higher than normal packet rate of dropped packets.
 - If packets aren't being dropped, it's another clue that the values reported by SNMP are incorrect.
5. As a workaround, if you've satisfied yourself that the error reports are bogus, you can instruct InterMapper to ignore the discards and/or errors. To do this, Get Info on the affected device and check the "Ignore Interface Errors" or "Ignore Interface Discards" box as desired.

What does it mean when InterMapper says a "subnet mask is discontinuous"?

In usual network configurations, a device's subnet mask contains one bits in the left side of the number, and zero bits on the right. InterMapper can then use the convention that a subnet mask is described as the number of bits in the subnet mask, and uses the notation of "/24" to indicate a subnet mask of 24 one-bits, or "255.255.255.0". For more details, see the [IP Addressing FAQ. \(Pg 727\)](#)

A subnet mask that has zero bits interspersed with the one bits in the left half of the value is often a configuration error. InterMapper points this out when you click and hold on a link: the status window resembles the figure at the right.

Normally, the address line contains the IP address and the subnet mask. This example shows a device whose IP address and subnet mask are set to the same value. This error is shown in the status window.

Why do network labels sometimes have a "/2*"?

This is another indication that there's a problem with the subnet mask. The figure at the right shows the network oval with a discontinuous subnet mask. The /2* indicates that the subnet mask has zero bits in the left half; clicking on the link will give a status window similar to the one above.

This example comes from an HP printer that has a bug in its SNMP implementation. The subnet mask of the printer is actually configured properly, and the printer is working. However, the SNMP software in the printer is reporting the incorrect value (it's reporting the IP address) for the subnet mask. Help/Systems has reported this to HP.

There are two separate network ovals on my map where I only expect one...

Examine the network's Status window to determine whether the subnet masks are the same in both ovals. If the subnet masks are different, one of the devices connected to the oval with the "wrong" subnet mask probably has a misconfigured subnet mask. (Look for the device that is being polled with SNMP.)

Note: For devices polled with ICMP echoes, InterMapper tries to guess whether it should draw a link to the network that contains the IP address. If both network ovals look equally good, it may draw a link to the "wrong" one, or alternate between them.

Some network ovals have more than one IP network number...

It's possible for a router or host to have two or more configured IP addresses for a particular interface. This form of secondary IP addressing can be common if your addressing is in transition. Rather than bringing everything to a halt to change IP addresses, a network administrator will support two IP subnets on the same logical wire. All the devices in the subnet can then have their IP addresses changed at their leisure, rather than forcing everyone to change them all at once. When all the

addresses have changed, the administrator usually gets rid of the old network number.

It's also possible that InterMapper is only reporting what it knows, and the information it is using is incomplete. This may be true of multi-point network technologies (like frame-relay clouds). If you find a situation where InterMapper is reporting multiple networks on a logical network and you know it's wrong, please send us email (support@intermapper.com) so we can figure out a way to make InterMapper's depictions more accurate.

We would also like to hear about a network with multiple IP network numbers where InterMapper does not show them correctly.

Does InterMapper support unnumbered IP links?

Yes.

To display unnumbered links:

1. From the Monitor menu, choose **Set Behavior...** The Set Behavior window appears.
2. Select the **Display unnumbered interfaces** check box.
3. Click **OK**. Unnumbered interfaces are now shown.

For more information, see the [Set Behavior \(Pg 387\)](#) window reference section of the Monitor Menu reference topic.

What does it mean when a Status Window shows **[[ifIndex not in ifTable]]** ?

It is a normal situation for VLANs. InterMapper first traverses the ipAddrTable which maps IP addresses to ifIndex entries. If the ipAddrTable looks like:

```
ifIndex 1 --> 192.168.1.1/24
ifIndex 2 --> 192.168.2.1/24
ifIndex 3 --> 192.168.3.1/24
```

And the ifTable looks like:

```
ifIndex 1 --> Ethernet 10/100
ifIndex 3 --> Ethernet 10/100
```

Then the interface description for ifIndex 2 will be listed as "[[Not in ifTable]]".

How can I find out how many devices I'm monitoring with InterMapper. Do I have to count all the boxes on each map?

The Server Information pane of the Server Settings window shows the number of devices you are monitoring.

I discovered a multi-protocol router (TCP/IP & AppleTalk) using TCP/IP, but I could not go back and change the protocol to RTMP?

This problem is related to having only one "target" address for each device, even though InterMapper knows the addresses of the other ports. When a device is

discovered using TCP/IP, it gets added with a target address in IP. You can't switch to use RTMP because that's an AppleTalk-only protocol.

Troubleshooting InterMapper RemoteAccess

Where do I find debugging information for InterMapper RemoteAccess

Unix Systems (including MacOS X)

Sending a SIGQUIT message to InterMapper RemoteAccess will result in a full thread dump. If you launched InterMapper RemoteAccess via the command line (e.g., `java -jar <InterMapper RemoteAccess>`), `Ctrl-\` to stdin will also work.

To send a SIGQUIT message, type the following in a terminal window (pid is the process id for InterMapper RemoteAccess):

```
kill -QUIT pid
```

The thread dump will be sent to stderr. On MacOS X, this is always the Console, unless you are running from the Terminal.

Windows Systems

If you have launched InterMapper RemoteAccess from the command line (e.g., `java -jar <InterMapper RemoteAccess>`) press `Ctrl-Break` in the Command Prompt to force the stack trace.

The stack trace always goes to stderr.

On Windows, this is the equivalent of `/dev/null` unless you are running from a Command Prompt or have redirected stdout/stderr to a file via the Debug Window's Redirect System Output... menu item.

Troubleshooting InterMapper DataCenter

- [I get an error message: "This InterMapper Server already appears to be associated with the InterMapper Database. Existing UUID is associated with a different URL". \(Pg 725\)](#)

I get an error message: "This InterMapper Server already appears to be associated with the InterMapper Database. Existing UUID is associated with a different URL"

Because multiple InterMapper installations can report to a single InterMapper Database, when InterMapper registers with InterMapper Database, it supplies a UUID to uniquely identify it. The InterMapper Database makes note of the URL and other characteristics of the server and associates them with the UUID. If InterMapper Database receives the same UUID from a different URL, it generates the error above. This may happen, for instance, if you copy your server settings from one copy of InterMapper to another, or move InterMapper to a new host or IP address. Your choices are to:

- **Cancel** - Stop the registration of the server
- **Force** - Force the UUID to be associated with the new URL.
- **Regenerate** - Have InterMapper generate a new UUID.

If you are certain that the installation of InterMapper which has generated this error is the same installation that was associated with the UUID previously, or if you know it should replace it, you can choose "Force".

If this is a different installation of InterMapper, choose "Regenerate".

Note: *It is important to pay attention to this error; map ids, device ids, etc., are only unique within a given server; if you associate a completely different installation of InterMapper with an existing UUID, the information about maps, etc. on the old server will be replaced or updated by information from the new server. When that occurs, datapoints from completely different datasets may be associated as if they were from one dataset.*

About IP Addresses

Note: InterMapper now supports 128-bit IPv6 addresses. Most of the information in this topic is still relevant and accurate. In addition, you can enter an IPv6 address anywhere in InterMapper that you can enter a 32-bit IPv4 address.

- [What is an IP address? How do I get one? \(Pg 726\)](#)
- [How do computers send data through the Internet? \(Pg 726\)](#)
- [What is a subnet? Why do I care? \(Pg 726\)](#)
- [What does the "/24" mean? How does that relate to my subnet mask? \(Pg 727\)](#)
- [What is a "private IP address range"? \(Pg 728\)](#)

What is an IP address? How do I get one?

An IP address ("Internet Protocol address") is a number that represents a single unique computer on the Internet. IP addresses are similar to telephone numbers, in that each computer (or telephone) must have its own unique IP address (telephone number.) Like telephones, there's a directory system - called the Domain Name System, or "DNS" - that can convert a name such as "www.apple.com" into a corresponding numeric IP address.

32-bit IPv4 Addresses are written as a sequence of four numbers separated by ".", like this: 208.123.246.35. Each of the four numbers in the IP address can take the value between 0 and 255.

InterMapper now supports 128-bit IPv6 addresses.

Every computer on the Internet must have a unique IP address. ISPs purchase large blocks of consecutive IP addresses, and then allocate smaller ranges of these addresses to their customers. Thus, a particular company might be assigned all the 254 IP addresses in the range 208.123.246.1 to 208.123.246.254. (The addresses ".0" and ".255" are not usually assigned.) Companies then assign the IP address to individual computers within the organization.

How do computers send data through the Internet?

Computers send information through the Internet by dividing the data to send into small chunks ("packets") and transmitting them to the other device. All this happens without your doing anything - the web browser, e-mail program, etc. all take care of these low level details.

When your computer wants to send to another computer, it creates the packet, then places the other computer's address in the *destination address* of the packet, places its own address in the *source address* of the packet, and then sends the packet off, either directly to the destination computer, or to a nearby router that takes responsibility for routing the packet.

There's an analogy with the post office here. Packets are like envelopes, with destination addresses and return addresses. Routers are like post offices: they check the destination address and have the responsibility for delivering the packet to the final destination computer or to another router that's closer to the destination.

What is a subnet? Why do I care?

A *subnet* is a range of IP addresses. The special attribute of a subnet is that all the computers within the subnet (a "sub-network") can talk directly to each other, and don't need a router to communicate.

As mentioned above, your computer delivers a packet directly to the destination computer or sends it to the router for ultimate delivery.

But how does your computer know whether the packet's destination is within its subnet? The answer is that your computer uses the subnet mask to determine the members of the subnet.

The chart below associates the number of IP addresses in a subnet to the subnet mask. For example, the subnet mask "255.255.255.0" represents 254 consecutive IP addresses. If your computer's IP and the destination computer's IP addresses are in the same subnet address range, then they can send packets directly to each other. If they're not in the same range, then they must send their data through a router for delivery.

What does the "/24" mean? How does that relate to my subnet mask?

InterMapper uses a shorthand notation to represent an IP subnet's information. The number in the "/xx" shorthand stands for the number of bits (technically, bits set to one) in the subnet mask. The convention is always to start at the left end of the 32-bit (IPv4) subnet mask. The table below shows the correspondence between the "/xx" notation and the actual numeric representation.

Subnet Mask	# of Addresses	Subnet Mask	# of Addresses
/1 128.0.0.0	2.1 billion	/17 255.255.128.0	32,766
/2 192.0.0.0	1 billion	/18 255.255.192.0	16,382
/3 224.0.0.0	536 million	/19 255.255.224.0	8,190
/4 240.0.0.0	268 million	/20 255.255.240.0	4,094
/5 248.0.0.0	134 million	/21 255.255.248.0	2,046
/6 252.0.0.0	67 million	/22 255.255.252.0	1,022
/7 254.0.0.0	34 million	/23 255.255.254.0	510
/8 255.0.0.0	17 million (<i>Class A</i>)	/24 255.255.255.0	254 (<i>Class C</i>)
/9 255.128.0.0	8.4 million	/25 255.255.255.128	126
/10 255.192.0.0	4.2 million	/26 255.255.255.192	62
/11 255.224.0.0	2.1 million	/27 255.255.255.224	30
/12 255.240.0.0	1 million	/28 255.255.255.240	14
/13 255.248.0.0	524 thousand	/29 255.255.255.248	6
/14 255.252.0.0	262 thousand	/30 255.255.255.252	2
/15 255.254.0.0	131 thousand	/31 255.255.255.254	RFC 3021
/16 255.255.0.0	65,534 (<i>Class B</i>)	/32 255.255.255.255	Loopback address

What is a "private IP address range"?

The Internet Assigned Numbers Authority (IANA) has reserved several blocks of IP addresses that an organization may assign for its own private internet. These blocks are defined in RFC 1918 (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>).

From the RFC:

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

We will refer to the first block as "24-bit block", the second as "20-bit block", and to the third as "16-bit" block. Note that (in pre-CIDR notation) the first block is nothing but a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 256 contiguous class C network numbers.

Quick Intro to IPv6 Address Formatting

This table gives the major forms of IPv6 addresses. The most important/common are **Localhost** (::1), **Global Unicast** (usually starting with "200x"), and **Link-Local Unicast** (starting with "FE80").

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA (*)	1111 110	FC00::/7
Global Unicast (**)	001	2000::/3
IPv4-Mapped	00...0:1111 1111:IPv4	::FFFF:IPv4/128
Site-Local Unicast (***)	1111 1110 11	FECO::/10
IPv4-compatible (***)	00...0 (96 bits)	::IPv4/128

* Unique Local Address (ULA) is an IPv6 unicast address that is generated to be unique in a local context. It is highly likely to be unique globally.

** Global Unicast address are all currently being assigned with a 2000::/3 prefix. Other three-bit prefixes are reserved for future use.

*** Site-Local Unicast and IPv4-compatible prefixes are deprecated. Use ULA and IPv4-mapped addresses, respectively.

About DNS

- [What resolver does InterMapper OSX use for its DNS? \(Pg 730\)](#)
- [InterMapper sometimes won't show a device's DNS name... \(Pg 730\)](#)
- [What is a FQDN? \(Pg 730\)](#)

What resolver does InterMapper OSX use for its DNS?

InterMapper uses two different DNS resolvers. When you add a device using the **Add Device...** command, InterMapper uses the system's resolver, configured in the OSX Network settings panel. When you use the "DNS Check" feature, InterMapper does its own DNS operations, via UDP packets, to the domain name servers listed in the DNS Monitor Preferences panel. InterMapper's built-in domain name resolver assumes that the domain name is fully-qualified. The interval for verifying the domain name is determined by the TTL in each DNS response (with the minimum interval specified in the DNS Monitor preferences panel).

When you discover devices, InterMapper initially looks up the FQDN name from the IP address (address --> name), then it settles down to monitoring the domain name (name --> address). InterMapper's built-in DNS resolver doesn't handle partially-qualified or invalid domain names; they fail to resolve.

InterMapper sometimes won't show a device's DNS name...

From the Edit menu, you can choose the Set Info submenu, then choose **Set Address...** to change the DNS option for each affected device from **Resolve name to address** to **Resolve address to name**. With this setting InterMapper always resolves the address to a name, and you don't see errors with names that aren't fully-qualified domain names.

What is a FQDN?

This is an acronym for a "Fully-Qualified Domain Name." Within an organization, it's convenient to refer to a computer by the first part of its name, knowing that "everyone" will know that the remainder is the same as the other computers in the organization. Thus, you may speak of "sneezy" and "dopey", knowing that they're really two computers at "seven-dwarves.org".

To identify a computer uniquely, you need the FQDN, such as "sneezy.seven-dwarves.org." Most user software can add a "search domain" to a partially-qualified domain name, adding the missing part of the FQDN. Some DNS servers require the FQDN to work properly with InterMapper. It's always best to enter the full domain name.

Tip: Even though you enter a FQDN when specifying a computer, you can use the *Short, Smart Name* when [constructing a label for a device \(Pg 414\)](#).

Tip: Technically, a FQDN requires a "." at the end. Just as the search domain is tacked onto the end of a partial domain name, most user software adds the trailing "."

SNMP Information

- [What is SNMP? \(Pg 731\)](#)
- [What is the 'Read-only Community String'? \(Pg 731\)](#)
- [Why can't I get SNMP information from a device? \(Pg 732\)](#)
- [How can InterMapper query a particular MIB variable? \(Pg 732\)](#)
- [Do all tables have an index? \(Pg 733\)](#)
- [Where can I read more information about SNMP? \(Pg 734\)](#)
- [How do I interpret an unknown enterprise number? \(Pg 734\)](#)
- [Is there a way to scan a network for all SNMP devices? \(Pg 734\)](#)

What is SNMP?

SNMP stands for the Simple Network Management Protocol. At its heart, SNMP is a set of rules that allows a computer to get statistics from another computer across the Internet.

Computers keep track of various statistics that measure what they're doing. For example, routers can keep track of the number of bytes, packets, and errors that were transmitted and received on each interface (port). Web servers might keep a tally of the number of hits they have received. Other kinds of equipment have configuration information that's available through SNMP.

Each of these pieces of information (packet statistics, page hits, configuration) is kept in a database described by a *Management Information Base* (a *MIB* in SNMP parlance.) There are a many different MIBs, describing many different aspects of a computer's operation.

The various values that can be retrieved from a MIB are called *MIB variables*. These variables are defined in the MIB for a device. Each MIB variable is named by an *Object Identifier* (OID), which usually has a name in the form of numbers separated by periods ("."), like this: 1.3.6.1.xxxx.x.x.x.x...

For example, the MIB-II (pronounced, "MIB two") has a variable that indicates the number of interfaces (ports) in a router. It's called the "ifNumber", and its OID is 1.3.6.1.2.1.2.1.0

InterMapper can query a device for the MIB variables and display the results. When a device receives a SNMP Get-Request for this ifNumber OID, it responds with the count of interfaces.

Note: The trailing ".0" in the example above is technically part of the OID. Although you will often see OIDs written without it, InterMapper requires that it be present wherever you enter an OID.

What is the 'Read-only Community String'?

The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. Most network vendors ship their equipment with a default password of "public". (This is the so-called "default public community string".) Many network administrators will change the community string to keep intruders from getting information about the

network setup. This is a good idea. Even if it's only read-access, SNMP can divulge a lot of information about the network that could be used to compromise it.

If there's a "read-only community string", you might expect that there is a "Write community string". You'd be correct. There is also a SNMP Set-Request, which is a command to set certain SNMP MIB variables (e.g., certain OIDs) to a specified value. These writes are protected by the write community string (which should *never* be set to 'public!'). Many SNMP-speaking devices also have IP address filters that ignore requests (read and write) unless the source address is on an access list.

There's also a SNMP Trap, which is an unsolicited message from a device to an SNMP console (for example, InterMapper) that the device is in an interesting state. Traps might indicate power-up or link-up/down conditions temperatures exceeding certain thresholds, high traffic, etc. Traps provide an immediate notification for an event that might otherwise be discovered only during occasional polling.

Why can't I get SNMP information from a device?

InterMapper requires that SNMP be available and configured to display traffic information. The most common cause of not being able to see traffic is that you haven't entered the SNMP Read-only community string. (This is like a password that controls whether another computer can retrieve SNMP information.)

In order of simplest to most complex, here is a list of reasons that InterMapper might not get SNMP information from a device:

- **Wrong DNS name/IP address** - (not likely, but we have to mention it)
- **No connectivity** - Can you ping the device from InterMapper?
- **No SNMP agent on the device** - Many devices or computers have optional SNMP capabilities that must be installed separately.
- **Is the SNMP agent disabled?** - Many devices allow you to disable the SNMP capability totally, or from certain ports.
- **If the SNMP agent is based on net-snmp or UCD-snmp package** - be sure that the configuration file specifically lists InterMapper's IP address/sub-net as an allowed client
- **In a custom probe, have you specified the OID properly?** - (See the [OID Format FAQ \(Pg 732\)](#) for details.)
- **Wrong Community string** - (have you tried 'public' ?)
- **Access lists: does the equipment only allow SNMP access from certain addresses?**
- **Firewalls: does a firewall block the SNMP port between your Mac and the equipment?**
- **Bugs in the SNMP agent on the equipment** - InterMapper uses SNMP Get-Next-Requests in several places. We've seen certain equipment that fails when queried this way.

If you're sure that you've checked all these things and you still can't get SNMP information, please get back to us at support@intermapper.com. We may have some tricks up our sleeves. (Or we may wind up learning something!)

How can InterMapper query a particular MIB variable?

There are two kinds of MIB variables: scalar values and table entries.

- **Scalars** have a single value, such as the interface number shown above. For example, the `ifNumber` MIB variable of a router is a single number that represents the total number of its interfaces (ports).
- **Table values**, on the other hand, provide the same pieces of information for different items, such as the traffic for each of a router's ports, or information about each of the TCP connections in a device.

InterMapper can read and display both scalar variables and table variables in its custom SNMP probes.

Scalar values must have a ".0" suffix in their OIDs. For example, the OID for `ifNumber` in MIB-II is often written as "1.3.6.1.2.1.2.1". In custom probe files, it should be represented as "1.3.6.1.2.1.2.1.0". (This ".0" is technically part of the OID - it's convenient not to write it, though.)

Table variables are generally suffixed with the index of the row. (This isn't always true: see the note below). For example, the Cisco Environment Monitoring MIB defines two variables for the input air temperature and input voltage as the first rows in each of these tables:

```
ciscoEnvMonTemperatureStatusValue 1.3.6.1.4.1.9.9.13.1.3.1.3
ciscoEnvMonVoltageStatusValue 1.3.6.1.4.1.9.9.13.1.2.1.3
```

If you add a suffix ".1" to each of these, you'll get the value of the first row; add ".2" to as a suffix, you'll get the second row, etc.

Do all tables have an index?

As noted above, some tables don't have a separate index column. These rows are named (their OIDs are specified by) data in the row. For example, the OID for `tcpConnState` row, the status of a particular TCP connection is "1.3.6.1.2.1.6.13.1.1". Its index is the source and destination IP address and port (all four values) which are appended to the `tcpConnState` OID. Thus, the full OID for the state of a TCP connection from 9.8.7.6 port 543 to 123.45.67.89 port 8765 would be:

```
1.3.6.1.2.1.6.13.1.1.9.8.7.6.543.123.45.67.89.8765
```

Where can I read more information about SNMP?

Here's a great site to start learning about MIBs and all the cool things you can do with them:

<http://www.snmpworld.com/>

Another is:

<http://netman.cit.buffalo.edu/>

A periodic newsletter, *The Simple Times*, is online at:

<http://www.simple-times.org/>

A great site pointing to various snmp products:

<http://www.simpleweb.org/>

How do I interpret an unknown enterprise number?

Q: My error log file shows the following lines:

```
14/02 15:13:07 TRAP CITRIX1:: coldStart14/02 15:13:07 TRAP
CITRIX1:: linkUp, ifIndex = 114/02 15:13:07 TRAP CITRIX1::
linkUp, ifIndex = 1677721914/02 15:14:07 TRAP CITRIX1::
1.3.6.1.4.1.3845.3.1.1 (8) { <no variables> }
```

Can you tell me what that SNMP ID is? (1.3.6.1.4.1.3845.3.1.1 (8))

A: The "1.3.6.1.4.1..." prefix of the OID indicates that the trap is from a private enterprise MIB. You can find out what enterprise by downloading the Enterprise Numbers RFC from:

<http://www.iana.org/assignments/enterprise-numbers>

Reading through the file indicates this:

```
3845 Citrix Systems Keith Turnbull
      keitht@citrix.com
```

You should contact the Citrix company (or read their MIB) to find out the exact interpretation of the trap's OID.

Is there a way to scan a network for all SNMP devices?

InterMapper will do a very good job of finding SNMP-speaking devices if you know the devices' SNMP Read-only Community string. Detailed instructions for scanning a subnet are available from the network scanning page. Be sure to set the default SNMP Read-only Community String as shown in the [SNMP Preferences](#). (Pg 254)

InterMapper may not be able to find a device for [any of these reasons](#). (Pg 732)

About WINS Names

Microsoft's Windows Internet Naming Service (WINS) is a name resolution service that resolves computer names to Internet Protocol (IP) address. Using WINS, the computer name can be resolved to a specific IP address.

InterMapper uses WINS names as follows:

- InterMapper (all platforms) queries devices for a NetBIOS (WINS) name. This name is used as the device's smart name if the DNS name is unknown or contains the word "DHCP".
- When adding a device that is in the same LAN as InterMapper server, you can use the device's NetBIOS/WINS name. To cause a name to be treated as a WINS name, place "\\" in front of the name when adding a device. The name is not looked up in the DNS.

Note: InterMapper does not use the WINS server - it only resolves local device names.

InterMapper FAQs

How can I stop the InterMapper server from polling for a while?

The easiest way to stop InterMapper's polling for a while is to disable all the maps. To do this:

1. Open the Server Settings... window
2. Click the Enabled Maps tab.
3. Uncheck all the maps. They will no longer be polled or tested.

Alternatively, you can disable maps individually from the Map List by right-clicking on a map in the list and selecting the 'Disable' command.

How can I stop the InterMapper server? How can I restart it?

On MacOS X, InterMapper installs a Menu Bar Application that gives a summary of InterMapper's status, and allows you to start and stop the InterMapper daemon.

On Windows, InterMapper installs an icon in System Tray (lower right corner) that does much the same thing.

On all Unix/Linux installations, InterMapper installs a script to control the server daemon.

We recommend you read the Readme file on the [Downloads page](#) for information specific to your version.

How can I move InterMapper from one server to another?

The recommended way to move InterMapper to another server is to follow these steps:

1. Install InterMapper on the new server, and stop the InterMapper service/daemon when installation is complete.
2. Stop the InterMapper service/daemon on the old server and copy your InterMapper Settings folder to the new platform, replacing the one created when you installed InterMapper on the new server.
3. On the new server, start the InterMapper service/daemon.

The default location for the InterMapper Settings folder depends upon the platform where installed:

- Windows: C:\Program Files\InterMapper\InterMapper Settings
- Mac OS X: /Library/Application Support/InterMapper Settings
- UNIX/Linux: \$HOME/InterMapper_Settings/, where \$HOME is the home directory for the specified user InterMapper is running under.

Note: If you are migrating from Mac OS X PowerPC to Mac Intel, Windows or any other Intel-based system, please contact support@intermapper.com prior to installing on the new platform. Additional steps are necessary in order to preserve the historical chart data when migrating between these platforms.

How can I uninstall the InterMapper server?

Each version of InterMapper comes with its own uninstaller. Find the original distribution file (or retrieve the current version from <http://www.intermapper.com/files>) and use its uninstall feature.

I get an "intermapperd dead but subsys locked" error message when I get InterMapper status by typing "/etc/init.d/intermapperd status". What does this mean?

The message "intermapperd dead but subsys locked" means that intermapperd is not running; the daemon has either crashed or was sent an explicit kill command by the root user. Furthermore, the InterMapper lock file `/var/lock/subsys/intermapperd` exists when intermapperd isn't running.

To restart InterMapper, log on to the system as root and type:

```
/etc/init.d/intermapperd restart
```

You may also clear the lock file by typing:

```
rm /var/lock/subsys/intermapperd
```

but this isn't required because the restart command does this.

Why do I have trouble with Telnet using my Windows terminal program?

Q: When I use HyperTerminal to telnet into InterMapper's server, I don't see character echoes. Why not?

A: Two commonly-available Windows telnet clients, HyperTerminal and the command-line telnet client, do not work correctly with InterMapper in their default configuration. Neither of them do local echoing by default, and both refuse to turn it on when asked to do so by the InterMapper server.

Therefore, neither of these clients work out-of-the-box with InterMapper, so you need to turn on local echoing yourself.

Turning On Local Echoing in HyperTerminal

With your InterMapper session loaded, choose File->Properties. Click the Settings tab. Click the ASCII Setup... button. Check the box labelled "Echo typed characters locally". When connecting to earlier versions of InterMapper, you should also check the box labelled "Send line ends with line feeds". Later versions of InterMapper do not require this (although it won't hurt.) Click Ok to close the ASCII Setup dialog, then click Ok to put away the Properties dialog. Remember to save your session to make the new settings permanent.

Turning On Local Echoing with Built-in Telnet Client

Start your telnet session with InterMapper. Press Ctrl+] to enable the client to process setup commands. Type "SET LOCAL_ECHO" and press Enter to turn on local echoing. Press Enter again to return to your session. I'm not aware of any way to save this setting for future sessions, so you'll need to do this each time.

Putty - Another Choice

One free Windows telnet client we have had good luck with is Putty. Putty is available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Putty requires no configuration to work correctly with InterMapper. You may find this nicer to use than either of the built-in options that come with Windows.

On an Xserve, can I use the serial port for paging?

You can use the built-in serial port to drive an external modem that can in turn send page notifications. To do this, you must disable the getty process that's usually listening on that port.

On the Xserve, open this file:

```
/System/Library/StartupItems/SerialTerminalSupport
```

At about line 72 is:

```
ENABLE_SERIAL_TERMINAL=$TRUE
```

Change this to:

```
ENABLE_SERIAL_TERMINAL=$FALSE
```

Re-init the system, and there should be no getty and InterMapper will get to the modem just fine. (Thanks to Charlie Winchcombe for this tip.)

InterMapper Flows FAQs

When the InterMapper Flows server is restarting and reloading the sessions, the Flows Window displays the number of records loaded so far vs. the total number of sessions. Sometimes the first number is larger than the second. What's going on?

The NetSAW server estimates the number of flows it will load into its cache, based on the flowrate that's learned from the actual records in the DB. Since this estimate is never perfect, you'll sometimes notice that the actual number of records exceeds the estimated records. Other times it'll fall short and finish early.

Is there any additional information available for troubleshooting or debugging a problem with InterMapper Flows?

InterMapper can provide some debug information via the Telnet server. To do this, turn on the Telnet server in the InterMapper Settings. Then telnet to the InterMapper server and use the "flows" command to list the exporters that InterMapper knows about. Use the "ext" command to check that InterMapper has its own connection to the IMFlows server.

You can copy/paste the output of these two commands into a bug report (Help - > Report a Bug...).

In the directory in which InterMapper Flows is installed, (see the Readme file in the installation package for a file location) there is a log file named "ns2-flows.log". The server logs significant information in this file. If you feel the file is getting too large, you can delete it safely.

Does InterMapper Flows work on LAN links? On WAN Links?

Yes, InterMapper Flows will work on any link where there's an "exporter" (the router/switch) to keep track of the traffic statistics. Many kinds of Cisco equipment can export flow records that summarizes the data flowing through that device.

How much bandwidth will NetFlow consume? How frequent is the traffic flow?

A quick answer is "not much". According to Cisco reference documents, NetFlow consumes 5 to 10 percent of your network bandwidth, depending on your configuration. In Help/Systems' experience, it is often much less. The switch/router summarizes the flow information, and typically will send an update about the flows it has seen every 60 or 120 seconds (this is configurable).

It is easy to set up your Cisco gear to send flow records, so you can see the effect on the traffic. You can find a brief document that describes the commands at:

http://dartware.com/support/tech_notes/imflows/netflowconfig.html

Does IM Flow act as collector at each location so that the central server can pull the data from each collector and correlate the same?

No. In our first release, all the flow records must be sent to one InterMapper Flows machine (the "collector"). You can have multiple exporters sending flow records to the single collector, though.

Cross-platform Questions

These questions relate to the differences between the implementations on various platforms.

- [How can I move from Traditional to the service/daemon version on Windows/Unix/Linux? \(Pg 740\)](#)
- [How can I keep InterMapper from polling for a while? \(Pg 741\)](#)
- [How can I stop the InterMapper server? \(Pg 741\)](#)
- [How can I remove the InterMapper server completely? \(Pg 741\)](#)

How can I move from Traditional to the service/daemon version on Windows/Unix/Linux?

The recommended way to upgrade to InterMapper on another platform is to follow these steps:

1. Set up InterMapper on the other platform, configuring the preferences anew as well as your notification settings.
2. Copy your map files to the "InterMapper Settings/Maps (Disabled)" folder on the new platform. (If you wish, you can also use InterMapper RemoteAccess to "import" them onto the new server.)
3. On the new platform, open the Server Settings window and "enable" the maps that you want to run.
4. Go through your maps and re-attach notifications to devices; these connections were lost in the transfer.

It is also possible to copy your InterMapper Settings folder and maps directly from one platform to another. This will preserve the attached notifiers for devices in your maps, but the procedure is slightly more complicated:

If you are running InterMapper "traditional" on a pre-Mac OS X system (ie Mac OS 9.2 or earlier), you will need to convert your preferences file ("InterMapper Prefs"). The easiest way to do this is to run InterMapper on Mac OS X -- start up the program and quit it -- InterMapper will fix up the file so it is cross-platform.

If you have any icon files in your "Custom Icons" folder, you will need to convert these to "data-fork" based resource files. You can use the [Custom Icon Conversion Script \(Pg 740\)](#) on a MacOS X computer to convert the file format. If that's not convenient, then send a note to support@intermapper.com. We will do the conversion and return the new file to you.

You must double-check your modem pager settings on the new platform; the location of the modem device stored in the preferences file will be completely different.

All of the other files should transfer without any problems.

How can I use custom icons from my Mac Classic installation on OSX?

There is a droplet that converts resource-based icons (used by the Classic/MacOS 8-9 versions) to a "data-fork" version that works on OS X. You can retrieve the droplet from: http://www.intermapper.com/binaries/Convert_Custom_Icon_File.sit

Drag your icon files onto this droplet program, and they will be converted to a form usable by the MacOS X version of InterMapper. Drag the resulting files to the */Library/Application Support/InterMapper Settings/Custom Icons* folder.

How can I stop the InterMapper server from polling for a while?

The easiest way to stop InterMapper's polling for a while is to disable all the maps. To do this:

1. Open the **Server Settings...** window
2. Click the **Enabled Maps** tab.
3. Uncheck all the maps. They will no longer be polled or tested.

How can I stop the InterMapper server? How can I restart it?

When using the Traditional InterMapper on MacOS X, simply quit the application. That will stop the polling. If you're using one of the server-based InterMapper versions (on OSX, Windows, or Unix/Linux), you'll need to stop the InterMapper service/daemon separately from InterMapper or InterMapper RemoteAccess.

On Windows installations, use InterMapper Control Center to start, stop, or restart the InterMapper service.

On all Unix/Linux/MacOSX installations, InterMapper installs a script to control the server daemon. The script should be invoked with one of these commands:

- **start** - start the daemon
- **stop** - stop the daemon
- **restart** - stop and restart the daemon
- **status** - check the status of the daemon

This script will be installed in different directories, depending on the operating system.

- **MacOS X:** */Library/StartupItems/InterMapperServer/InterMapperServer command*
- **Most versions of Linux:** */etc/init.d/intermapperd command*
- **FreeBSD:** */usr/local/etc/rc.d/intermapperd.sh command*

How can I uninstall the InterMapper server?

Each server-based version of InterMapper comes with its own uninstaller. Find the original distribution file (or retrieve the current version) and use its uninstall feature.

Index

1

16-bit 728

2

20-bit 728

24-bit 728

24 Hour Time 228, 272

3

32-bit subnet 727

6

64-bit 254

A

About DNS 730

About InterMapper 430

About IP Addresses 726

About Packet-Based Probes 596

About Serial Numbers 20

About SNMP Versions 254, 598

About WINS Names 735

Access 179, 223, 237, 278, 280, 282,
290, 292, 298, 303, 305, 638,
650, 656

Chart dropdown menu 223

Controlling 280, 305

InterMapper RemoteAccess 237

Remote Server 282

set 279

tcp 240

Telnet 280, 302

Telnet Server 291

Web Server 289

Access Control 278

Access Control Examples 303

Access Control Process 280

ACK 202, 206, 236, 705

Acknowledgements 202, 389, 427

Acknowledge-message 236

Acknowledge Message
Window 389

Acknowledge window 203

Acknowledgements window 389,
430

Acknowledging 202, 206

Device Problems 202

remove 204

Use 387

Action 55

Action dropdown menu 53

Active Hours 140

Add All 635

Add Benchmark Coordinates win-
dow 640

Add Device 62, 65-66, 405, 719,
730

Add Devices window 65

Add Network 124

Add Subnet 68

Add Text window 409

Adding 21, 65, 68, 71, 79, 88, 104,
124, 131, 147, 153, 162, 222,
257, 282, 289, 291, 303, 308,
632, 635, 640

Background Image 88

Background Images To Your
Map 104

- dataset 222
- Devices Manually 65
- firewall 303
- Networks 68
- submap 72
- Unmanaged Hubs 124
- Adding Datasets 222
 - Charts 220
- Addr 704
- ADDRESS 80
- Address Change 238
- Address Ranges 278
 - Entering 278
- Addresses 63, 71, 129, 144, 282, 290, 292, 638, 640, 651, 656, 687, 702, 726, 730
 - InterMapper 71
 - Remote Server firewall 283
 - Resolve 730
 - SNMP-speaking 60
 - syslog 129
 - Telnet Server firewall 292
 - Web Server firewall 290
- Admin 714
- ADMIN 707
- Administrator 280, 302, 305, 602
 - Administrator's username 602
 - Administrators Group 280
- Adminpw 714
- Advance Data Importing 639
- AES 255
- AIF 142
- Aiff 633
- Alarm 44, 89, 130, 133, 143, 167, 179, 182, 206, 439
 - OK 130
 - Warning 129
- Alert 142
- Align 411
- ALLOW 278, 280, 303
 - automatic-login 303
 - matches 278
- Alpha-numeric Pager 147, 153, 155
 - Configure Notifier window 155
- Alrm 236
- Alt-click 95
- Alt/Option-click 119
- Analogue Modem 147
- Anti-aliasing 54
- ants 39, 56, 182
- Apache Mod-SSL httpd.conf file 310
- API 162
- App 78
- Appearance 87, 104
- AppleTalk
 - AppleTalk-only 722
 - AppleTalk Name Binding Protocol 416
 - AppleTalk subnets 417
- Apply 638, 649
 - Vertex 638
- AppName 237

- Apps 78
 - ARGS 80
 - Arrange Commands 114
 - Arrange submenu 118
 - Arranging 99
 - Arranging Your Maps 119
 - ASN.1 167, 177
 - AT Subnet List 417
 - ATE0V1 153
 - ATM 610
 - ATM AAL5 610
 - Attach 129, 133
 - Attach Notifier dialog 130
 - Attach To 125
 - Notifier 129, 133
 - Attribute 727
 - subnet 726
 - AU 142
 - Auth 280, 298, 681-682
 - Authentication 687
 - Authentication Server 298, 623
 - AuthLevel 243
 - Auto 45, 180
 - Auto-adjust 227, 271
 - Auto-Discover 57, 59, 404
 - stop 60
 - Auto-discovery 60, 374, 404
 - initiate 374, 404
 - Autodiscovered 64, 121
 - Autodiscovery 58, 61, 255, 407
 - Autodiscovery window 404
 - During 63
 - Automatic-login 300, 303
 - Allow 303
 - called 303
 - automatic-login user 304
 - Automatic Device Discovery dialog 59
 - Automatic Device Discovery window 61, 407
 - Automatic Login 280, 300, 303
 - matches 280, 300
 - Automatic Placement 654
 - Axes Tab 271
-
- B**
-
- Back-up 264
 - Back-up SMTP 264
 - Background 86, 104
 - Background Image 88
 - Background Images To Your Map 104
 - Backup Map window 85, 377
 - Backup Name 85
 - Backups 85, 631
 - Baseband 244, 610
 - Basic Acknowledge 204
 - Basic, Timed 203
 - BB4 Technologies 607
 - BBDISPLAY 607
 - BEGIN IMPORTS 177

Behaviour 730
Benchmarks 640
 Setting 640
Big Brother Probes 607
Big Brother State 607
Big Brother System 607
Big.dartware.com 714
Bits 148
Block 203, 726
 Check 203
 IP 726
 select 203
Both 641
Bottom 418
 Bottom Left 418
 Bottom Right 418
Bound 227
Bps 244, 693
Brightness/Contrast 105
BroadcastPkts MIB 610
Browse 310, 602
Built-in Shapes 101, 412
 Built-in Shapes icon 411
Built In 55, 84
Built On 251
Bus 114, 119, 411, 702
By/s 704
Byte/Second 610, 693
 compute 608
Bytes Per Second 86

Bytes/second 610

C

Can't obtain/lock QPixmap 236
Capacity/bandwidth 610
Census 643
Certificate 310
Certificate Authority 310
 Certificate Signing Request window 312
 Certificate Signing Requests 277, 310
Certificate Signing Request window 312
CFileName 239
Changes 106, 132, 180, 389, 687, 730
 DNS 730
 Edit 387
 Labels 106
 Map Zoom 180
 Poll Interval 180
 specified 132
 username 687
Characteristics 95
Chart 701
 Chart Data 632
 Chart Defaults 271
 Chart Log Files 232
 Chart Menus 223, 226
 Chart Options 224, 226, 273
 Chart Options window 226
 Chart Title 226

Chart window 225	Cmd 160, 203
Charts popup 221	Cmd-A 118
Charts submenu 220, 223	Cmd-L 125
Chart Defaults 271	Cmd/Ctrl-L 106
Chart dropdown menu 223	CmdName 242
Chart dropdown menu icon 223	Cmd-line 711
Chart Menu 223	Color-selection window 273
Charts 219-220	Color Picker 265
Adding Datasets 222	Color Picker window 87
Creating 219	Colors 86, 231, 273, 411
Deleting 222	Colors Tab 231, 273
Editing 222	Com.dartware.http.redirect 687
Cisco 610	Com.dartware.radius 687
Cisco's Icon Library 99	Comma-delimited 378
Cisco Environment Monitoring MIB 731	Comma-separated list 263, 650
Cis-	Domain Name Server 263
coEn-	WINS 262
vMonTemperatureStatusValue	Command 160, 162, 374, 380, 384, 387, 404, 425, 430, 702
ciscoEnvMonVoltageStatusValue 731	Command-line 439
Citrix 734	Command-line Notifiers 160
CKaliOpenLogList 707	Command-Line Probes 600
CKaliOpenMapList 707	Command + Option 247
CKaliOpenSoundSetList 707	Command Details 704
Class 63, 183	Command key 375
Classic/MacOS 8-9 740	Command Line 80, 160, 162, 600
Client 431	Command Line Interface 649
Client Log 247	Command Line Probes 600
Client Log window 248, 433	Command Line Program 162
Client window 248	Configuring 160
	Comment 388

- Common Internet Scheme
 - Syntax 688
- Common Name 312
- Community 719, 731
 - Community String Types 254
 - string 731
- Compress 243, 703
 - JPEG 243
 - PNG 243
- Compute 608
 - byte/second 610
- Configd 611
- Configuration 139
- Configure Notifier 139
 - Configure Notifier window 131, 139, 142, 144, 147, 155, 160, 309
 - Configure Notifier Window Reference 140
- Configure Notifier window 131, 309
- Configuring 139, 142, 144, 147, 155, 160, 166, 278, 290
 - Command Line 160
 - e-mail 144
 - E-Mail Notifier 144
 - Firewall 278
 - firewalls 290
 - Notifier 139
 - Page Notifier 155
 - Pager Notifier 147
 - Sound Notifier 142
 - Syslog Notifier 166
- Confirm Password 602
- Connecting 121, 278, 290
 - Devices 121
 - InterMapper 279
 - Web Server 289
- Connecting Devices 119
 - Switch Ports 119
- Context Menus 435
- Contrasty 105
- Control 280, 305, 436
 - Access 280, 305
 - Map Access 305
 - User Access 306
- Control key 375
- Copy 244, 308, 311, 375, 432
 - CSR 310
 - InterMapper 53, 237
 - InterMapper RemoteAccess 430
 - mapname 244
 - Retaining 631
- Count 134
- CPU 56
- CR's 314
 - LF's 314
- CR-LF 314
- CRAM-MD5 264
- Create 57, 59, 71, 102, 219, 237, 300, 303, 310, 375, 431, 638, 650
 - An Import File 638
 - Certificate Signing Request 310

Charts 219
CSR 310
Custom Icon Files 103
Guest 303
New Map 57
New User 298
Reverse Connection 431
Sub-maps 71
Create Log File window 232
Critical 89, 134, 143
Cross-platform Questions 740
CSR 277, 310
 copy 311
 create 310
 CSR file 313
 generate 311
 send 310
CSV 58, 635
Ctrl 203
Ctrl-click 636, 640
Current Wireless Probes 305
Currently-defined 146
 set 146
Custom Icons 99, 101, 632
 Custom Icon Files 103
 Setting 99
Custom Probe 185, 239
Customize 79, 185, 689
 Status Window 185

Cycle 114, 119, 411
 Cycle Command 118
 illustrated 411
 result of 114

D

D<name 712
Daemon 25, 740
 start 740
 stop 740
Dartware
 DARTWARE-MIB
 DEFINITIONS 179
 Dartware MIB 167, 177
 Dartware OBJECT IDENTIFIER 177
Data 58, 227, 271
 Importing 58
 Use 226, 271
Data File 375
Data From Maps 635
 Exporting 635
Data Into Maps 637
 Importing 637
Data Retention 388
Data Tab 229, 272
Dataset 222
 add 222
Date & Time 49
Date/time 162
Days/weeks 260
Dbug 238
DDis 611

- Debug 234, 248, 425, 432
 - InterMapper 430
- Debug file 257
- Debug Log file 432
- DEBUG_CONFIG_FILE 711
- Debugging 248
- Default 54, 67, 438, 655
 - Default Appearance 99
 - Default button 78
 - Default Device 267
 - Setting 268
 - Default Device Thresholds 211
 - Setting 208
 - Default Icons 102
 - Default Map Colors 265
 - edit 265
 - Default Network 268
 - Default Notifiers 92, 132
 - Default Notifiers dialog 130
 - Default Notifiers window 132
 - Defining 132
 - Default Sounds 131
 - Default Thresholds 208
 - Setting 208
 - Default Traffic Thresholds
 - Setting 208
 - Labels 414
- Default Notifiers window 132
- Defaults 711
 - 8181 711
- Define SNMPv1 Traps 179
- Defining 132
 - Default Notifiers 132
- Delay 134
- Delayed Notifiers 134
- Delete 24, 128, 230
 - interface/oval 119, 128
- Delete Chart 224
- Delete Data window 230
- Deleting
 - Charts 222
- Demo 18, 39, 439
 - Demo Map file 39
 - open 39
 - find 439
 - Try out 39
- DENY 278, 280, 304
 - matches 278, 280
- Dependencies 204
- DErrs 611
- DES 254
- Describing 78
 - Launcher 79
- DESCRIPTION 179
- Detail 128
 - Hiding 128
- Detailed Logs 431
- DETAILS 704
- Determine 238
 - DNS 238

- IP 237
- Developer Guide 168, 185, 433, 440, 600, 637, 690
- Developing 439
 - Nagios 439
- Device 72, 88, 99, 121, 202, 236, 267, 411, 638, 640, 649, 695
 - Automatic Placement 654
 - Connecting 121
 - Default Appearance 99
 - Editing 415
 - Importing 640
 - Unacknowledging 204
- Device-Name 705
- Device Address 145
- Device Attributes 638, 656
- Device Condition 145
- Device Defaults 267
- Device Defaults Panel 267
- Device Descriptions 99
 - Importing 99
- Device Kind 388
- Device List 425, 690, 699
 - Manipulating 50
 - Use 426, 699
- Device List Columns 48
- Device List Web Page 699
- Device List window 425
 - Open 425
- Device Name 145, 693
- Device Problems 202
 - Acknowledging 202
- Device States 143
- Device Status 103, 692
 - Coloring According 103
- Device Status window 185, 399, 608
- Device Threshold window 402
- Device Thresholds window 208
- Device Variables 416
- Device. Add Device 404
- Device/link 265
- Device?InterMapper 731
- Devicename 241
- Devices - Adding Manually 65
- Devices/probe 637
- DHCP 608, 735
 - DHCP-Discover 612
 - DHCP-Inform 612
 - DHCP Message Type 612
 - DHCP/Bootp 612
- Diagnostics menu 247-248
- Dialup 153
- Directive 638, 649
 - Directive Line 638
 - Directive Line Technique
 - Importing 638
 - Directive Parameter 650
- Directive Line 649
- Disable 296, 732
 - SNMP 731

- Disc/Minute 693
- Disconnected 240
- Discontiguous subnet 719
- Discovery Options 63
- Discovery Status bar 59
- Display 124, 722
 - interconnections 124
 - Select 719
- Distribute Command 411
- Dividers, Sub-Dividers 227, 271
- DNS 58, 60, 65, 106, 166-167, 179, 238, 260, 262, 312, 398, 407, 416, 427, 596, 602, 642, 687, 726, 730, 735
 - change 730
 - determine 238
 - DNS-Related Messages 238
 - DNS Check 730
 - DNS Monitor Preferences 263, 730
 - Setting 262
 - DNS Monitor prefs 730
 - DNS Name 416, 655, 692
 - DNS x.x.x.x 238
 - DNS z.z.z.z 238
 - DNS/WINS Settings 262
 - Use 262
 - DNSName 639, 650, 656
 - enter 65, 388
 - monitoring 730
 - processing 238
 - see 602
 - specify 262
- DNUcast 611
- DocName 237
- Document Name 145
- Domain Name
 - Domain Name Server 263
 - Comma-separated list 263
 - Domain Name Service 262
 - Domain Name System 726
 - called 726
- Double-click Actions 83, 387
- Down 89, 129, 133, 154, 167, 179, 206, 236, 246, 388, 440, 596, 702
 - generate 89
 - set 388
- DOWN-ACK 705
- DOWN list 705
- Down Thresholds 89
- Downloadable 19
- Downloading 734
 - Enterprise Numbers RFC 731
- Drag 119, 278
 - firewall 278
- Dropdown menu 43, 78, 400
- Dt 239
- DUcast 611
- Duplicate 131, 309

E

- E-mail 9, 39, 129, 133, 139, 144, 241, 248, 264, 726
 - Configuring 144
 - enter 144, 264
 - outgoing 264
 - send 129, 133, 144, 264
 - specify 129
 - Use 144
 - E-mail Notification Message 144
 - E-Mail Notifier 144
 - Configuring 144
 - E-Mail Preferences 264
 - Setting 264
 - Echo 404
 - Edit 42, 65, 79, 106, 131, 145, 180, 186, 188, 211, 220, 257, 265, 268, 277, 298, 308, 384, 387
 - change 389
 - Charts 220
 - Default Map Colors 265
 - Device 411
 - Helper Applications 78
 - Label 414
 - Labels 106
 - Network Label 415
 - Notifier List 308
 - Text 145
 - User Information 300-301
 - Edit Chart 225
 - Edit Default Notifiers 132
 - Edit Device Label dialog 106
 - Edit Device Label window 106
 - Edit E-mail Message window 145
 - shows 144
 - Edit Label 268
 - Edit List 147, 153
 - Edit Map 95, 384
 - Edit menu 39, 86, 99, 104, 106, 118, 132, 140, 153, 211, 250, 253, 257, 268, 271, 283, 290, 292, 308, 311, 374, 380, 730
 - From 730
 - Use 374
 - Edit Message 141, 147, 155, 162, 165
 - Edit Network Label dialog 106
 - Edit Network Label window 106
 - Edit Notifiers 92, 133
 - Edit window 80
 - Editing Helper Apps 79
 - Editing Your Map 95
 - Electronic 144
 - Email 130, 162
 - making 162
 - EmailAddr 242
 - Enabled Maps 296, 375, 741
 - Enabling 373
 - Remote 373
 - Encoding 688
 - Special Characters 688
 - Encrypted 310
-

- End 179, 703, 726
 - 32-bit subnet 727
 - EndTagStr 239
 - telnet 702
- Enhancing 99
 - Your Map's Appearance 99
- Enter 55, 65, 68, 73, 83, 89, 125, 144, 155, 162, 167, 202, 226, 262, 264, 271, 278, 283, 290, 292, 300, 303, 377, 388, 405, 411, 432, 598, 719, 730-731
 - Address Ranges 278
 - Community 719
 - DNS 65, 398
 - e-mail 144, 264
 - FQDN 730
 - Host 264
 - ID 155
 - IP 155, 299, 303, 404, 430
 - IP Address 167
 - IP subnet 68
 - iPing 162
 - list 262
 - Map Name 73
 - Multiple Licenses 24
 - Name 375
 - OID 731
 - SNMP Community 405
 - SNMP Read-only 598, 731
 - subnet 125
 - TCP 283, 290, 292
 - URL 55, 83, 290
 - User 264
 - User Name 73
 - WINS Scope 263
- Enter dialup 148
- Enterprise 6306 177
- Enterprise Numbers RFC 731
 - downloading 734
- Env 712
- ERR 237
- Err/Minute 693
- Error 208, 237, 695, 702
 - Setting 208
- Error Page 695
- Error/min 692
- ERRORS 702
- Errors-per-minute 208
- Errors-To 264
- ErrorThe ERROR 702
- ESCAPED_MESSAGE 160
- Ethernet 99, 116, 422, 610
 - represent 116
- Ethernet 10/100 722
- Evaluation Serial Number 19
 - Request 19
- Event 146, 257
- Event Log 235, 703
- Event Log file 202, 235, 260, 655
- Event Log Messages 236
- Event Log window 235, 237, 427
 - open 235

- EventLog file 206
 - EventMesg 241
 - Example Notification 162
 - Excel 638
 - Exe 160
 - Execute 380, 604
 - NT Services 601
 - Undo 380
 - Exit/Quit 376
 - Expand
 - frontmost window 425
 - Preference 271
 - Server Settings 296, 308
 - Expand/contract
 - frontmost window 425
 - Experiments 720
 - Export 711
 - EXPORT-SPEC 711
 - Export Map 375
 - Export Map Data window 636
 - Export submenu 636
 - Exporting 226, 296, 379, 635, 649
 - Data From Maps 635
 - Schema 649
 - Exterior - Click 226
-
- F**
-
- FDDI 99
 - Field Export Order 635
 - Fields 636
 - File Format 261
 - File Menu 46, 57, 59, 85, 374-375
 - File Save dialog 635
 - FILE_NAME 711
 - Filter 407, 432
 - Find Next 380
 - Find window 380
 - Finding 436, 438, 719, 734
 - Demo 439
 - Legacy 439
 - Menu Item Shortcuts 436
 - SNMP-speaking 732
 - Firewall 277-278, 280, 303, 432, 732
 - Add 303
 - Configuring 278
 - drag 278
 - move 278
 - Firewall's list 277-278, 280, 283, 290, 292
 - IP 277, 282, 290, 292
 - Firewall Definition dialog 304
 - Firewalls 255, 280, 283, 290, 732
 - configuring 290
 - InterMapper's 280
 - FoldersInterMapper saves its files 628
 - Font, Size 423
 - Format 101, 114, 411
 - Format menu 95, 99, 106, 119, 125, 374, 411
 - Format/Options 650
-

FQDN 730
 enter 730
 require 730
FreeBSD 741
Frontmost window 425
FTP 83, 186
FULL 695, 702
Full Pages 695
 Use 695
FullDuplex 244
FullLogAccess 281, 302, 304
Fullname 236
FullTelnetAccess 281, 302
FullTelnetAccess Group 281
FullWebAccess 281, 302-303
FullWebAccess Group 281
Fully-qualified 263, 730
Fully-Qualified Domain Name 730
Fully-specified IP 278
FullyQualifiedDomainName.csr 311
Function 26
 MacOS 25

G

General Messages 237
General Rules 436
Generate 89, 311
 1,024-bit 311
 CSR 310
 Down 89
 Warning 89

Geocoding 643
Geographic Coordinates 100, 640
 Setting 99
Geographic Information
 Systems 643
Get 608, 687
 DHCP 608
Get-Next-Requests 732
Get Info 411, 720
GIF 99, 103, 105, 640
GraphicConverter 105
Graphics 54
Graphing 610
 Percent Err 610
Grayscale 101
Grep bootpc 611
Group 146, 298
Group Information dialog 298
Group notifiers together so 146
Guest 303
 create 303

H

Handle 78
 URL 78
HCOctets 610
Help 247-248, 702
Help Menu 374, 430
 Use 374, 430
Helper App 55, 83
Helper Applications 78
 Editing 79

Removing 81	ICMP 58, 721
Helper Applications Customize window 79	ICMP Echo 405
Use 78	ICMP Ping 408
view 79	Icon Sets 101
Helper Applications submenu 79	Icon Size 102
Helper apps 78, 388	Icon window 101, 412
Helper Apps submenu 79	Icons 412
Helper Apps window 80	Icons on Maps 101
HelpNo 702	Id 147, 155, 238, 649, 687, 702
Hide 185	ID,MapName,Address,Latitude,Longitude 650
Status window 185	Id,name,address 649
Hide Charts 223	Id/phone 153
Hide Selection	IfAdminStatus 195-196, 608-609
Use 128	IfAlias 195, 609
Hiding 121, 128	IfAlias The ifAlias 195
Detail 128	IfConnectorPresent 609
Inactive Ports 121	IfCurrStats.inDiscards 611
Hiding Charts 221	IfCurrStats.inErrors 611
Highlight 230	IfCurrStats.inNUcastPkts 611
Highlight popup	IfCurrStats.inUcastPkts 611
Use 271	IfDescr 244, 609, 707
Horizontal Dividers 227	IfHCInOctets 609
Host 25, 264, 601	IfHCOctets 609
Enter 264	IfHighSpeed 609
InterMapper 601	IfInBroadcastPkts 610
InterMapper Server 25	IfIndex 121, 195-196, 244, 693, 707, 722, 734
HOST 711	IfInDiscards 609, 611, 720
HTML 635	IfInErrors 609, 611
	IfInErrors MIB 719

I

IANA 728

- IfInMulticastPkts 610
- IfInNUcastPkts 608, 610
- IfInOctets 244, 608, 610
- IfInUcastPkts 608-610
- IfLastChange 609
- IfMTU 609
- IfName 609
- IfNumber MIB 731
- IfNumber OID 731
- IfOperStatus 195-196, 608-609
- IfOutBroadcastPkts 610
- IfOutDiscards 609, 611
- IfOutErrors 609, 611
- IfOutMulticastPkts 610
- IfOutNUcastPkts 608, 610
- IfOutOctets 244, 608, 610
- IfOutUcastPkts 608-610
- IfOutxxxx 720
- IfPhysAddress 609
- IfPrevStats.inDiscards 611
- IfPrevStats.inErrors 611
- IfPrevStats.inNUcastPkts 611
- IfPrevStats.inUcastPkts 611
- IfPromiscuousMode 609
- IfSpeed 195, 244, 609-610
- IfTable 719
- IfType 609
- Ignore Interface Discards 611, 719
- Ignore Interface Errors 720
- IgnoreInterface Errors 611
- IM 375, 687
- IM-Remote.jar 714
- Im&password 688
- Image 375, 640
- Implementations 740
- Implementing 162
 - iPing Notifier 162
- Import 58, 296, 375, 412, 637-638, 640, 687, 711
 - Data 58
 - Data Into Maps 637
 - Device Descriptions 99
 - Devices 640
 - SNMP MIB file 375
 - URL 687
- Import button 101
- Import file 649
- Import File Example 653
- Import Sound 142
- Import submenu 378
- IMProbe 651, 656, 687
 - include 687
- IMProbe URL 655, 687
 - contains 687
 - use 687
- IMProbe URL Specification 687
- IMRA 375
- Inactive Hours 140
- Inactive Ports 121
 - Hiding 121

- Includes 21, 57, 78, 687
 - IMProbe 687
 - MapName 687
 - SNMP 58
 - URL 78
- Indefinite Acknowledgements 203
- Info - View 375
- Info window 55, 188, 387, 608
 - Use 188
- Information 102, 695
 - Viewing 692, 696
- Information window 389
- Init 153
- InOctetPrev 244
- Insert 649
- Insert menu 65, 68, 70, 73, 99, 124, 374, 404
- InstallShield icon 19
- InstantSSL 313
- Interconnections 42, 60, 119, 124, 422
 - display 124
 - see 119, 412
- Interface 610
 - Utilization 608
- Interface Attributes 670
- Interface Information 693
- Interface Statistics 693
- Interface/oval 119, 128
 - delete 128
- Interfaces window 195, 206, 387
 - Opens 387
 - view 195
- InterMapper's Remote Server 282, 724
- InterMapper Control Center 25, 53
- InterMapper Control Center application 25
- InterMapper Control Center icon 26
- InterMapper daemon 25
 - stop 25
- InterMapper Errors 695-696
- InterMapper Event Log file 655
- InterMapper Files 628
- InterMapper Handles Errors 655
- InterMapper Help 430
- InterMapper icon 136
- InterMapper Inserts Devices 654
- InterMapper Labels 58
- InterMapper Logs 257, 632
- InterMapper Map 378
- InterMapper menu 55
- Intermapper OBJECT IDENTIFIER 177
- InterMapper on Mac OS 740
- InterMapper on MacOS 741
- InterMapper OSX 730
- InterMapper Outages 698
- InterMapper Preferences 249
- InterMapper Prefs 740
- InterMapper Prefs file 632

- InterMapper Probe 655
- InterMapper Remote 310, 711
- InterMapper RemoteAccess 46, 142, 162, 235, 237, 261, 277, 280, 282, 373, 375, 380, 386, 430, 635, 637, 706, 724
 - access 237
 - copy 432
 - stopping 237
 - Troubleshooting 724
- InterMapper RemoteAccess's Map List window 373
- InterMapper RemoteAccess application 282
- InterMapper RemoteAccess Help 430
- InterMapper Server 9, 25, 46, 251, 276, 714
 - hosting 25
 - running 276
 - testing 711
- InterMapper Server Preferences Overview 253
- InterMapper Server Status window 25
- InterMapper Servers window 637
- InterMapper service/daemon 740
- InterMapper Settings 102, 161-162, 236, 261, 312, 628, 631-632, 740
 - create 237
 - state 631
 - subdirectory 162
 - Tools subdirectory 160
- InterMapper Settings Folder 632
- InterMapper Settings/InterMapper Logs 235
- InterMapper Settings/Maps 85, 297, 740
- InterMapper Settings/Sounds 142
- InterMapper Status 607
- InterMapper Telnet 277, 689
- InterMapper Telnet-based Interface 9
- InterMapper Tray window 26
- InterMapper User List 633
- InterMapper User Preferences 53
- InterMapper Version 251
- InterMapper Web Page 689
- InterMapper Web Page Navigation 690
- InterMapper Web Server 290
- InterMapper Web Server menu 690
- InterMapper.pkg icon 19
- Intermapperauthd 628
- IntermapperCondition 168, 179
- Intermapperd 628
- IntermapperDeviceName 168, 179
- IntermapperMessage 168, 179
- IntermapperTimestamp 168, 179
- IntermapperTrap 179
- Internet 129, 155, 726, 731
- Internet Assigned Numbers Authority 728
- Internet Protocol 726, 735
- Interval 690
 - Setting 690

Invalid Probe Human Name 239

Invalid Probe ID 239

Invalid Probe Name 239

IP 57, 60, 65, 68, 70, 106, 124, 155,
166-167, 182, 186, 202, 237,
260, 262, 277, 280, 282, 290,
292, 299, 303, 310, 373, 387,
404, 411, 430, 602, 607, 637,
640, 649, 687, 692, 707, 726,
730-731, 735

assign 726

blocks 726

contains 721

corresponding 262

determine 238

Enter 155, 300, 303, 405, 432

firewall's list 277, 283, 290, 292

ICMP Echo 405

reporting 720

scan 70

set 607

Set 388

switching 637

use 601

IP Address 167, 303, 416, 726

IP Net 692

IP subnet 68, 407, 727

IP Subnet List 417

IP subnets 417, 721

IpAddrTable 722

IPing 162

IPing Notifier 162

Implementing 162

ISPs 726

Item

Alt/Option-click 119

ItsMailServer 242

ItsUserName 241

J

Java Version 430

Joint Photographic Experts
Group 103

JPEG 99, 103, 243, 640

JPG 105

K

Kali 237, 703

KALI NEXT 706

Kali Starting KALI 237

Kali Stopping KALI 237

KalidDisplays 702

Keyboard Shortcuts 436

KeySpan Twin Serial 150

KILL 703

Klaxon 143

L

Label 58, 101, 106, 124, 227, 411,
414

Changing 106

Editing 106

Select 106

Label Font 268

Label Position 411

- Label Position submenu 411
- Label Size 268
- Label Variables 416
- LAN 735
- Last Down 145
- Latitude 640, 650
- Launcher 79
- Launching InterMapper 17
- LDAP 439
- LDOWN 702
- LF's 314
 - CR's 314
- Library/Application Support/InterMapper Settings/Custom Icons 740
- License List 252
- Line 638, 642, 702
 - Directive 638
 - DOWN list 705
- Line Style 271
- Linear 228
- LineStr 239
- Link 69, 124, 404, 608, 695, 697
- Link-up/down 732
- LINK REPORT 704
- Link Status 693
- Link Status Window 187
- LinkUp 734
- Linux 78, 436, 628-630, 740
- Linux/Unix 248
- Listen 256
 - SNMP 254
 - SNMP Traps 255
- Lists 384, 702
 - kalidDisplays 702
- Local Security Policy 602
- Localhost 282
- Locality 312
- LocalSystem 602
- Locations 628
- LOG 703
- Log Entries 260
 - Redirecting 260
- Log File 150, 154, 224, 232, 234, 257
 - Paging 147, 153
- Log File Name 232, 260
- Log File Parameters 259
 - Setting 257
- Log File Preferences 232
- Log File Sources 261
- Log In 376
- Log Messages 236
- Log On 601
- Log Out 376
- Logarithmic 228
- Login 300, 303
- Logins 379
- Logon 602
- Logs 235, 257, 374-375, 425
 - Preferences 257

viewing 374
Logs submenu 235, 246, 257
Long-term Packet Loss 200
Longitude 388, 640, 650
Loopback 727
Lost Packets 439
Lower-left 414
Lower Bounds 227, 271

M

Mac 187, 732
MAC Address 693
Mac OS 142, 611, 628-630
Mac OSX 150
Macintosh 436, 601
MacOS 25, 78, 262
 function 26
 InterMapper 262
MacPing
 find 719
Mailto MyProbe 242
Main Logger 130
 Syslog 129
Management Information Base 731
Managing 301
 Users 298
Manual Entry 58
Manually-connected 69
 remove 69

Map 41, 53, 57, 68, 99, 124, 180,
 181, 208, 296, 303, 305, 375,
 631, 635, 640, 649, 691
 Switches 124
 Understanding 181
Map's Colors 87, 266
 Setting 86
Map's Default Device Thresholds 89
 Setting 86
Map's Default Notifiers 92
 Specifying 92
Map's Default Traffic Thresholds 91
 Setting 86
Map Access 281, 305
 Controlling 305
Map Access Panel 305
Map Access Permission Levels 306
Map Area 45
Map Attributes 675
Map Background 99
 Setting 99
Map Benchmark 404
Map Data 637
Map Edit 384, 391
Map Editable 180
 Making 180
Map Editor 181, 374, 404
Map Files 296, 632
Map Legend 44
Map List 425, 690
Map List window 46, 71, 251, 268,

- 375, 380, 384, 425
- Open 425
- Map Name 49, 73, 306
- Map Settings 86, 132, 211, 253, 380
- Map Settings Window 86, 132, 182, 211, 380
- Map Status 72, 693
 - Probe Type 72
- Map Status item 693
- Map Status Probe 72
- Map View button 60
- Map Web Page 691
- Map window 41, 60, 180, 380, 384, 387, 404
- Map Zoom 45, 180
- MAP_NAME 711
- MapName 244, 638, 642, 650, 687
- MapName,Address 650
- MapName,Address,Name,Latitude,Longitude 651
- MapName,Probe 651
- Maps
 - Deleted 632
 - Disabled 632
 - Enabled 632
- Maps, Free 640
- Matches 278, 280, 300, 601, 650
 - Allow 278
 - Automatic Login 280, 300
 - DENY 278, 280
 - username 601
- Mbps 187
- MD5 255
- Menu Bar 42
- Menu Bar Application 25
- Menu Command 411
- Menu Item Shortcuts 436
 - Finding 436
- Menu Reference Overview 374
- MESSAGE 160, 162
- Message Editor window 145
 - Use 144
- Message Format 236
- MIB 168, 182, 375, 608, 731
 - SNMP-enabled 182
 - use 375
- MIB-II 195, 731
- MIB-II 32 610
- MIB file 375
- Microsoft's Windows Internet Naming Service 735
- Misc 248
- Miscellaneous Probes 440
- Misconfigured subnet 721
- Missing HTTP Version 243
- Modem Compatibility 150
- Modem Page Settings dialog 150
- Modem Pager Settings window 153
- Monitor 41, 79, 180, 185, 384, 601, 730
 - DNS 730
 - Network 180

- NT Services 601
 - Monitor menu 66, 131, 133, 137, 188, 195, 202, 213, 374, 387, 608, 719
 - Move 137, 278
 - firewall 278
 - Vantage Point 136
 - Msec 186
 - Msg 240
 - MTU 693
 - Multicast 693
 - MulticastPkts 610
 - Multiple Licenses 24
 - MultiTech MT5634ZBA-USB 150
 - MyProbe 239
-
- N**
-
- Nagios 439
 - developing 439
 - Nagios Plugins 440
 - Nagios Template 600
 - Name 139, 148, 153, 155, 195, 236, 299, 375, 735
 - Enter 377
 - Internet Protocol 735
 - SNPP Server 155
 - Name, IP Address 642
 - Name,MapName,Address 639
 - NBP 58
 - NBP Name 416
 - Net-snmp 732
 - NET USE 602
 - NetBIOS 735
 - NetBIOS/WINS 735
 - Netmask
 - InterMapper 251
 - Netopia.example.com 688
 - Network 68, 70, 99, 106, 180, 267, 608, 695
 - Adding 68
 - Monitoring 180
 - Open 611
 - Scanning 70
 - Troubleshooting 608
 - Network-specific 604
 - Network Defaults 267
 - Network Defaults Panel 267
 - Network Defaults Preferences 267
 - Network Filter Dialog 62
 - Network Info Window 193
 - Network Label 415
 - Editing 415
 - Network Monitor 607
 - Network Monitoring 9
 - Network Preferences 267
 - Network Scanning dialog 408
 - Network Scanning window 61, 70, 404
 - Network Status 692
 - Network Status Window 186
 - Network Techs 130
 - Network Variables 417
 - Network. Add Network 404
-

- New 59
 - New Group 298
 - New Map 57, 375
 - Creating 57
 - New Map Constructor window 57, 59
 - New Service 153
 - New User 298
 - Creating 300
 - Newdata.tab 714
 - Newline 166
 - NNTP 439
 - NODE 702
 - NODE REPORT 704
 - Non-localhost 282
 - Non-Polling Probe 440
 - Notification 167
 - Notification Escalation 135
 - Notification Messages 241
 - Notification Using 153
 - Numeric Pager 153
 - Notification_dt Valid 162
 - Notifier 129, 133, 139, 384
 - attach 129, 133
 - Configuring 139
 - Parts 130
 - Removing 140
 - Notifier List 92, 129, 131, 133, 140, 153, 162, 308
 - edit 308
 - open 130
 - Use 131, 308
 - view 131
 - Notifier List window 131, 140
 - use 131
 - Notifier Name 130
 - Notifier Parameters 130
 - Notifier Schedule 130, 147, 155, 165
 - Notifier Settings window 133-134
 - Notifier Type 129, 139, 142, 144, 147, 155, 160
 - Notifier Type dropdown menu 146, 153
 - Notifiers window 130-131, 133-134, 387
 - open 131, 387
 - Notifiers/Alerts 129
 - Overview 129
 - NT 601
 - NT Services 276, 601, 740
 - choose 601
 - execute 604
 - Monitoring 601
 - open 601
 - NT Services item 602
 - NT Services Probe 601
 - Ntfy 241
 - NUcastPkts 609
 - Num-lines 707
 - Numeric Pager 153
 - Notification Using 153
-
- O**
-
- OBJECT IDENTIFIER 179, 731
-

- OCTET STRING 167
 - Octets 609
 - Offscreen 243
 - OID 256, 608, 731
 - enter 731
 - ifNumber 731
 - part 731
 - specified 732
 - tcpConnState 733
 - OK 60, 67-68, 70, 72, 85, 88, 101, 130-131, 134, 143, 147, 155, 165, 167, 179, 230, 232, 266, 268, 301, 304, 310, 377, 400, 405, 412, 439, 601, 608, 719
 - Alarm 130
 - OKAY 440
 - Old Maps 244
 - Older Formats 631
 - Only SNMP 213
 - Open Recent 375
 - Open Status Window 185
 - Open URL 55
 - OpenSSL 313
 - Organizational Unit 312
 - OS 237, 251, 740
 - OSX 82, 150, 608
 - OSX Network 730
 - Other Thresholds 89
 - Other Tips 119
 - Arranging Your Maps 119
 - Outage Alarms on Interfaces 206
 - Outages 246, 698
 - Outages file 257
 - Outages Log 246
 - Outages Log window 246
 - Outages Web Page 698
 - Outages window 246
 - Outgoing 144, 264
 - E-mail 264
 - SMTP 144
 - OutOctetNow 244
 - OutOctetPrev 244
 - Output 636
 - Oval 411
-
- P**
-
- Packet-based Test Procedure 596
 - Packet Loss 186, 200, 692
 - reset 186
 - Page Notifier 155
 - Configuring 155
 - Page Setup 376
 - Page Setup dialog 376
 - Page Using SNPP 155
 - Pager ID 149, 155
 - Pager Notifier 147
 - Configuring 147
 - Pager Settings window 147
 - Paging 147, 153
 - Log File 150, 154
 - Paging Services 147, 153
 - shows 147
 - Paging Services list 153
-

- Paging Settings window 148
- Paging Subscribers 147, 153
 - shows 147
- Paging<date>.txt 150, 154
- Partially-qualified 730
- Password 73, 264, 276, 299, 303, 379, 601
- PASSWORD 712
- PATH 80
- Pem 313
- Pending.csr 312
 - Certificate Signing Request 310
- Percent 610
- Percent Err 610, 693
 - graphing 610
- PERCENT ERROR 611
- Ping 78, 688
- Ping.<y-ourAccountName>@iping.com 162
- Ping/Echo 186, 439, 692
- Ping/UDP-based 213
- Pk/s 704
- Pkt/Second 693
- Pkts 609, 704
 - number 704
 - sum 702
- PLAIN 264
- Platform-dependent 78
- Platform-specific 79
- Plugins 440
- PNG 99, 103, 243, 375, 635, 640
 - compress 243
 - Save 375, 635
- PNG file 103
- Poll Interval 45, 180
 - Changing 180
- Popup 611
- PORT 73, 80, 264, 711
 - Specify 73
- Port Number 416
- PORT on HOST 711
- Port/interface 40, 195
- Portable Network Graphics 103
- Portnumber 237
- Porttype 237
- Position 268
- Possible Arrangement Approaches 99
- Pound/hash 649
- Powers 228
- PPP 611
- Pre-CIDR 728
- Pre-Mac OS 740
- Preferences 53, 253-254, 257, 265, 267, 271, 380
 - Logging 259
 - Setting 257
 - Use 53, 253
- Preferences window 53, 265, 380
- Prefix 227
- Primary SMTP 264
- Print 375

Print Sharing 604
 Print Single Page 376
 Privacy 254
 Private Address Space 728
 Private Key 311
 Probe 375
 Probe Configuration window 598
 Probe File Error Messages 239
 Probe Picker window 401, 438
 Probe Reference Overview 438
 Probe timeout 439
 Probe Type 49, 65, 72, 145, 416, 608
 Map Status 72
 Probename 244
 Probes 439, 598, 638, 642, 651, 687, 705
 running 705
 Processing 238
 DNS 238
 SNMP 239
 Program Files 628
 Prompts 280, 601
 Properties 602
 Proprietary 439
 Protocol-specific 440
 Province 312
 Prt 697, 704
 Purple Oval 181
 Putnotification 162
 Putnotification API 162
 Pw 688

Pw improbe 687

Q

Quick Reference 95
 Quick Start 220
 QUIT 703
 QuitNo 702
 Quitting 237, 247, 374
 appName 237
 InterMapper 374

R

RADIUS 439, 687
 RBytes 697, 704
 RDis 697, 704
 Read 46
 READ-ONLY 254, 719
 set 719
 Read-Only Access 306
 Read-only Community String 731
 READ-WRITE 254, 638
 Read-Write Access 306
 Read/write 280
 ReadMe 19
 Receive Statistics 693
 Received Discards/Minute 610
 see 608
 Recent Loss 692
 Recently-opened 375
 Choose 375
 Redirect 260
 Log Entries 260

- Reference 638
- Register button 21
- Registering 21
- Relaunch 243
- Reload 412, 690-691
- Reload button 101
- Remote 237, 280, 303, 305, 373, 706, 724
 - enabling 373
- REMOTE 703
- Remote Server 282, 303
 - access 282
 - stop 282
- Remote Server firewall 283
- Remove 69, 79, 131, 137, 140, 204, 229, 232, 258, 296, 298, 309, 406, 641
 - acknowledgement 202
 - Helper Application 78
 - manually-connected 69
 - Notifier 139
 - Users 298
 - Vantage Point 136
- Remove button 298
- Remove Vantage Point 137
- Removing Group Members 301
- Removing Links 69
- Rename 375
- Repeat 134
- Replacing 687
 - username 687
- Reply 238
- ReplyCode 242
- Report 720
- Reprobe 387
- Reprobe/Reprobe Selection 387
- Request 19, 280
 - Evaluation Serial Number 19
 - username/password 280
- RErr 697, 704
- Reset 186
 - Packet Loss 186
- Resolve 730
 - address 730
 - Update Address 398
 - Update Name 398
- Responsibilities 43
- Restore 85, 375
- Restore Map window 378
- Retaining 631
 - Copies 631
- Reverse Connection 431
- ReversePath 242
- Revert 85
 - choosing 85
- RFC 727
 - RFC 1738 688
 - RFC 1918 728
- River/water 643
- Round-Trip Time 208
- RPC 604

RPkt 697, 704
 Running 21, 251, 276, 282, 601, 611, 705
 InterMapper 251, 276, 282, 601, 608
 InterMapper Server 276
 Probe 704
 Windows NT 601
 Running Time 251

S

SASL 379
 Save 85, 229, 311, 375, 635
 PNG 375, 635
 Your Map 85
 Save File dialog 311
 Save Name 379
 Sbin/ping on Unix 78
 Scale 227
 Scan Network 407
 Scanning 70, 734
 IP 70
 Network 70
 subnet 732
 Schedule window 167
 Scheduled Hours 139
 Schema 649
 exporting 649
 SCM 601
 Screenshot 430
 Send 374, 430
 Search Domain 263

Secret&user_name 688
 Secret&username 688
 Segment 697
 Select 86, 101, 106, 121, 203, 255, 380, 411, 598, 719
 Block 203
 Display 722
 Icon window 101, 412
 Label 106
 SNMPv1 598
 SNMPv3 598
 Use 86
 Select Adjacent 381
 Select All 118, 380
 Select Map Status 71
 Select Other 96
 Select Other submenu 121
 Select Probe Window 65-66
 Select submenu 380
 Send 129, 133, 144, 155, 166, 264, 283, 290, 310, 425, 430
 Back 425
 CSR 310
 e-mail 129, 133, 144, 241, 264
 mailto MyProbe 242
 Page Using SNPP 155
 Screenshot 430
 SNMP 129
 syslog 166
 Use 426
 Send E-Mail 720

- Send Log File Entries 260
- Send syslog 166
- SENSITIVE 656
- Server 165, 431, 628
- Server "MyProbe" 242
- Server Command 431
- Server Configuration 140, 260, 277, 282, 289, 291, 310
- Server Configuration Overview 277
- Server Information 251, 722
- Server Information Overview 251
- Server Messages 240
- Server Name 251
- Server Preferences 232, 271, 276
- Server Probes 608
- Server Probes - Proprietary 160, 162, 185, 236, 310, 438, 640, 687
- Server Running Time 251
- Server Settings 133, 140, 153, 249, 257, 268, 271, 282, 289, 291, 296, 308, 310, 380, 598, 740
 - Open 740
 - Use 381
- Server Settings dialog 162, 604
- Server Settings list 602
- Server Settings window 21, 86, 130-131, 140, 153, 232, 234, 249, 251, 253, 257, 265, 267, 271, 277, 282, 289, 291, 296, 298, 303, 305, 308, 310, 375, 380, 632, 722, 740
 - Disable 375
 - open 740
 - Use 249, 381
- Server Settings Window
 - Overview 249
- Server Settings>SNMP 255
- Service 147, 740
- Service Control Manager 276, 601
 - opens 601
- Service/daemon 740
- Set 86, 99, 101, 136, 142, 146, 208, 226, 254, 257, 262, 264, 268, 276, 279, 388, 607, 640, 690, 719, 727, 730
 - Access 278
 - Benchmarks 640
 - Chart Title 226
 - Custom Icons 99
 - Default Device 267
 - Default Device Thresholds 211
 - Default Thresholds 208
 - DNS Monitor Preferences 263
 - DOWN 388
 - E-mail Preferences 264
 - Error Thresholds 208
 - Geographic Coordinates 100
 - Interval 690
 - IP 387, 607
 - Log File Parameters 259
 - Map's Colors 87
 - Map's Default Device Thresholds 89
 - Map's Default Traffic Thresholds 91

Map Background 99	Set Thresholds 208, 402
Notifiers 146	Set Timeout 439
Object's Icon 101	Set Timeout window 387
Preferences 257	Set Vantage Point 137, 388
Read-Only 719	Settable 596
Reload 690	Settings/user/IMRemote 724
SNMP 388	SHA 255
SNMP Community 254	Shared Secret 687
SNMP Preferences 254	Shared%20secret 687
Text 411	Shared_secret 688
Thresholds 208	Sharedsecret 687
User 276	Shift 248
Vantage Point 136	Shift-click 96, 406
WINS Preferences 263	Short 730
Y-axis 228	Short-term Packet Loss 200
Set Address 388, 730	Short DNS Name 416
Set Alignment dialog 419	Short, Smart Name 416
Set Behavior 722	Show Charts 223
Set Behavior window 719	Show Client Log 433
Set button 689, 691	Show Date 228, 272
Set Comment 388	Show Day 228, 272
Set Community 256, 388, 719	Week 228, 272
Set Community window 719	Show Info Window 188, 719
Set DNS Monitor 263	Show InterMapper Control Center 26
Set Info submenu 66, 256, 730	Show Legend 224
Set Latitude/Longitude 387	Show Legend submenu 223
Set Poll Interval 400	Show Server Log 433
Set Probe 66, 256, 388	Show Time 228, 271
Set Probe Info submenu 439	Show User 305
Set Probe window 72	Show/Hide Checkbox 195

- Show/Hide Toolbar 384
- Showing 65, 71, 139, 145, 147, 155, 177, 380, 404, 610, 689, 702
 - Add Device 405
 - Chicago 71
 - Configure Notifier window 139, 147, 155
 - Dartware MIB 177
 - Edit E-mail Message window 145
 - InterMapper 689
 - InterMapper Web Server menu 690
 - Paging Services 147
 - Paging Subscribers 147
- Signed Certificate 310
 - Uploading 313
- Silenced 241
- Silenced e-mail 241
- Silenced SNMP 241
- Simple Network Management Protocol 731
- Simple Network Paging Protocol 129
- Simple Networking 604
- SIZE 179
- Slideshow 425
- Smart Name 416, 730
- SMTP 144, 264, 439
 - outgoing 144
 - specify 144
- SMTP Failure 242
- SNMP 58, 60, 129, 143, 167, 177, 182, 185, 239, 254, 388, 405, 427, 439, 596, 598, 642, 687, 731
 - AirPort If 404
 - disable 732
 - If 60
 - including 58
 - listen 256
 - processing 238
 - sends 129
 - Set 388
 - specify 60, 598
 - Use 254, 438
- Snmp-device-display 239
- Snmp-device-variables 239
- SNMP-enabled 182, 440
 - MIB 182
- SNMP-speaking 60, 68, 406, 732
 - address 60
 - finding 734
- SNMP Community 254, 405
 - Enter 405
 - setting 254
 - Specify 404
- SNMP Community String 254
- SNMP Console 720
- SNMP Get-Next-Requests 732
- SNMP Get-Request 731
- SNMP GetRequest 62, 408
- SNMP ID 734
- SNMP Information 731
- SNMP MIB 610, 732

- SNMP MIB-II 439
- SNMP MIB file 375
 - Imports 375
- SNMP Preferences 254
 - Setting 254
- SNMP Read-only 254, 407, 598, 731
 - enter 598, 731
- SNMP Read-only Community 254, 731
- SNMP Read-Only Community String 731
- SNMP Read-Write 254
- SNMP Server Settings Pane 255
- SNMP Set-Request 732
- SNMP SysContact 416
- SNMP SysDescr 416
- SNMP SysLocation 416
- SNMP SysName 416
- SNMP sysUptime 186
- SNMP Table 379
- SNMP Trap 167, 255, 732
 - InterMapper 254
 - Listen 256
- SNMP Trap Community 167
- SNMP Trap Community String 167
- SNMP Version 254
- SNMP Version dropdown 598
- SNMP Watcher 720, 731
- SNMPv1 254, 598, 610
 - Selecting 598
- SNMPv1-2c Community 255
- SNMPv1-v2c 254
- SNMPv1-v2c-speaking 254
 - strings 254
- SNMPv2 598
- SNMPv2c 254, 598
- SNMPv3 254, 598
 - Selecting 598
- SNMPv3 Authentication 255
- Snmpwalk 433
- Snooze Alarm 241
- SNPP 129, 155
- SNPP-based 155
- SNPP Port 155
- SNPP Server 155
- Sort submenu 384
- Sound 142
 - Configure Notifier window 142
- Sound Name 142
- Sound Notifier 142
 - Configuring 142
- Special Characters 688
 - Encoding 688
- Special Group 280
- Specific Device 212, 215, 256
- Specific folders 628
- Specifying 57, 59, 71, 92, 129, 144, 262, 407, 653, 731
 - Address 649
 - DNS 262
 - e-mail 129
 - Map's Default Notifiers 92

- OID 731
- Port 73
- SMTP 144
- SNMP 60, 598
- SNMP Community 405
- Spreadsheet-style Import file 639, 649
- Spreadsheet/database 637
- Ss DOWN 702
- Ss DOWN-ACK 702
- SSL 310
- SSL Certificates 310
- SSL/TLS 313
- SSLCACertificateFile 313
- SSLCertificateFile 313
- SSLCertificateKeyFile 312
- SSLv3/TLS 290
- Star 114, 119, 411
 - command - using 114
 - illustrated 411
- Start 57, 237, 289, 291, 740
 - appName 237
 - daemon 740
 - Telnet Server 291
 - Web Server 289
 - Your Map 57
- Start InterMapper 603
- Start New Log File 260
- Stat 697, 704
- State 25, 142, 631
 - InterMapper 25
 - InterMapper Settings 631
 - None 142
 - State/color 206
 - Status 179, 195, 426
 - Status Bar 45
 - Status window 183, 185, 202, 206, 387, 722
 - Customizing 185
 - hide 185
 - Open 387
 - Viewing 185
- Stdin 711
- Stdout 711
- Stop 25, 60, 237, 282, 289, 291, 740
 - Auto-discovery 60, 404
 - daemon 740
 - InterMapper 25, 601
 - InterMapper daemon 25
 - InterMapper RemoteAccess 237
 - Remote Server 282
 - Telnet 237
 - Telnet Server 291
 - Web Server 289
- Strings 254, 731
 - COMMUNITY 731
 - SNMPv1-v2c-speaking 254
- STRIPPED_MESSAGE 160
- Style 230
- Style submenus 411
- Sub-Dividers 227, 271

Sub-maps 71	Sum In/Sum Out 186
Creating 71	Sum Out 692
Subdirectory 161-162	Summary Information 696
InterMapper Settings 162	Suspend Sounds 39
Submap 72	Switch Ports 119, 121
add 72	Connecting Devices 119
Submenu 223, 375, 380, 384, 388, 425, 430, 637	Switches 124, 637
Submit Bug Report window 430	IP 637
Subnet 58, 60, 68, 106, 121, 125, 183, 185, 406, 692, 719, 726, 732	Map 124
attribute 727	Synchronizing 602
Enter 125	Users 602
indicate 721	SysContact 416
scanning 734	SysDescr 416
see 720	SysLocation 416
subnet 726	Syslog 129, 166, 260
uses 727	address 130
value 720	Main Logger 130
Subnet 192.168.1.0 57	send 166
Subnet List 417	Syslog Notifier 166
Subnet Mask 726	Configuring 166
Subnets 63, 68, 106, 417	Syslog Server 260
Subscriber 147	SysName 416
Subscriber dropdown menu 153	System Preferences 611
Subscriber menu 147	System Tray icon 25
sudo Isof 611	System Version 251
Sum 702	System/Library/Sounds 142
pkts 704	SysUpTime 145, 609-610, 697, 704
Sum In 692	SysUpTime.0 244
	<hr/> T <hr/>
	Tab-Delimited TEXT File 375

- Tab key 384
- TAP 129, 147
- Task Bar Menu 56
- TBytes 697, 704
- TCP 185, 213, 240, 283, 290, 292, 416, 439, 733
 - accept 439
 - access 237
 - Enter 283, 290, 292
 - number 439
- TCP-based 186, 416, 439
- TCP Check 439
- TCP Port 416
- TcpConnState OID 731
- TDis 697, 704
- Telelocator Alphanumeric Protocol 147
- Telnet 83, 235, 237, 261, 280, 282, 291, 302, 383, 702
 - access 280, 298
 - End 703
 - stopping 237
- Telnet Server 291, 702
 - access 292
 - start 291
 - stop 291
 - use 292
- Telnet Server Command Reference 702
- Telnet Server firewall 292
 - addresses 292
- Telnet Server Messages 240
- Telnetting 720
- Terminal application 611
- Terminal window 82
- TErr 697, 704
- Test IP 719
- Test Notifier 139, 160
- Tests 139
- TEXT 54, 145, 229, 404, 411
 - Editing 145
 - Use 404
- Text-msg 240
- Thawte 313
- The ImProbe URL 687
- The Simple Times 734
- Threshold-condition 236
- Thresholds 208
 - Setting 208
- Thresholds>Device 211
- Thresholds>Traffic 182, 212, 215
- Time Axis Tab 228
- Time Interval 272
- Time Interval dropdown menu 225
- Time Interval Menu 225
- Timed acknowledgement 202
- TimeOut 439, 596
 - Set 388
- Timestamp 145, 167, 236, 612
- TimeStr 241
- Title Bar 42

TInt TELNET 240
 TInt Starting telnet 237
 TInt Stopping telnet 237
Tools 162
Tools->Folder Options 601
Tools subdirectory 160
 InterMapper Settings 161
Top 412
Top Err 186
Top Left 418
Top Right 418
Top Rx 186
Top Tx 186
TotalErrors 611
TotalPkts 611
TPkt 697, 704
Traceroute 65, 405
Traditional 101
 service/daemon 740
 Traditional InterMapper on
 MacOS 741
Traffic 91
Traffic Thresholds 208
Transition 146
 particular device state sends mul-
 tiple notifiers 146
Transmit bytes/second 608
Transmit packets/second 610
Transmit Statistics 693
TRAP 134, 167, 179, 236
Trap-Related Messages 240
Trap - Plays 142
Trap Notification Schedule 167
Troubleshooting 608, 719, 724
 InterMapper 719
 InterMapper RemoteAccess 724
 Network 608
TTL 730
TXT 260
Typical Device Information 692
Typical Network 692
Typical Network Information 692

U

UCD-snmp 732
UDP 256, 439, 611, 730
UDP Port 162 Check 254
Un-Acknowledge 204-205, 387
Un-hiding Detail 128
UNAC 236
Unacknowledge 203, 206
Undo 380
Undo/Redo 381
Unencoded 688
Unencrypted 254
Uninstall 741
Uninstaller 741
Unix 150, 162, 166, 262, 714, 740
 Unix/Linux 82, 601, 740
 Unix/Linux/Mac OS 631
 Unix/Linux/MacOSX 741
Unknown HTTP Command 243

- Unknown HTTP Version 243
- Unmanaged Hubs 124
 - Adding 124
- Unselected - Invert 380
- UP/OK 134
- Update Address 398
 - Resolve Name 398
- Update Name 398
 - Resolve Address 398
- Upgrade 740
- Uploading 313
 - Signed Certificate 310
- Upper Bounds 227, 271
- Uptime 697
- UpTimeNow 244
- UpTimePrev 244
- URL 55, 78, 83, 162, 290, 655, 687
 - Enter 55, 83, 290
 - handle 78
 - importing 687
 - Including 78
 - performs 163
- URL-encoded 687
- URLESCAPE 161, 163
- USB 150
- User 264, 276, 298, 303, 305, 601
 - enter 264
 - Managing 301
 - Removing 301
 - set 276
 - Synchronizing 602
- USER 712
- User-settable 182
- User Access 306
 - Controlling 305
- User Information 300-301
 - Editing 301
- User Information dialog 301
- User list 301
- User Name 73, 165, 255
 - Enter 73
- User-
 - home/Library/Preferences/InterMapper
 - Remote 724
- Username 240, 280, 282, 290, 601, 687
 - change 687
 - match 604
 - prompted 602
 - prompts 280
 - replacing 687
 - supplies 280
- Username/password 254, 280, 303
 - provide 303
 - request 280
- Users Panel 298
- USGS Aerial 643
- Using 114, 649, 689
 - Arrange Commands 114
 - Command Line Interface 649
 - Web Server 689

Using Auto-discover 59

Using Background Images 105

 Tips 105

Using Charts 220

Using Default Values 82

Using Double-Click Actions 83

Using Geographic Coordinates 640, 654

Using Group Notifiers

 InterMapper 146

Using Helper Applications 78

Using InterMapper

 RemoteAccess 373

Using Notification Dependencies 136

Using SNMP Version 598

Using WINS 735

Usr/bin/java 714

Usr/local/bin 628

Util 244, 697

Utilization 608

 Interface 610

V

V.34 150

Value 237, 720

 subnet 719

 sysUpTime.0 244

Vantage Point 40, 136, 388

 move 137

 Removing 137

 set 136

Varbind 256

Varbinds 256

Verisign 313

Version 145, 251

 Use 251

Vertex 638, 667

 applies 639, 649

 Use 667

Vertex Attributes 638, 667

Vertical Axis Tab 227

Vertical Dividers 231

Vertices 639, 649

View 66, 79, 86, 131, 185, 195, 223, 305, 374, 430, 691, 695

 Chart dropdown menu 223

 Chart menu 223

 Client 431

 Helper Applications Customize window 79

 Information 695

 Interfaces window 195

 Log 374

 Map Settings Window 86

 Notifier List 131

 Select Probe window 66

 Status Windows 185

 Summary Information 696

View as

 Map 384

View Menu 374, 384

 Use 374, 384

VLAN 119

Vlans 722

W

WAN 155

WARN 134, 167, 179

Warning 44, 89, 129, 133, 143, 182, 439

 Alarm 130

 generate 89

WAV 142, 633

Web 280, 282, 303, 305, 383

Web-based Service 643

Web Device List 700

Web Page 633, 689

 Customizing 690

 Reloading 690

Web Server's Stop button 289

Web Server firewall 290

 addresses 290

Web Server Messages 243

Web Servers 104, 289, 689

 access 290

 Connecting 290

 start 289

 stop 289

 use 290

 Using 689

Week 228, 272

 Show Day 228, 272

Weekend Pager 139

Whitespace 65, 405

Wildcards 278

Window

 Edit Device Label 414

Window System Tray 26

Window>Logs submenu 247

Window>Logs>Debug menu 433

Windows 25, 59, 68, 78, 142, 150, 162, 262, 276, 404, 411, 436, 601, 631, 702, 740

Windows 2003 25

Windows CA 313

Windows menu 221, 223, 235, 246, 257, 374, 425

 Charts submenu 223

 Logs submenu 257

 Use 374

Windows Networking 604

Windows NT 601

 running 601

Windows NT Services Probe 601

Windows NT/2000/XP 373, 741

Windows Only 165

Windows OS 601

Windows popup window 25

Windows Server 2003 604

Windows XP 25

 running 601

Windows, Unix 436

WINDOWS/Profiles/user/IMRemote 724

Windows/Unix 95

Windows/Unix/Linux 740

WinPopup 165

WINS 61, 65, 262, 735

Comma-separated list 263

use 262, 735

WINS Preferences 263

Setting 262

WINS Scope 263

Enter 262

leave 263

WINS/NetBIOS 263

Wire 268, 413

Wire icon 411

Wire item 413

Wrong Community 732

Wrong DNS name/IP 732

X

X-axis 272

XCoordinate 654

XML 58, 635

XML file 378

XP 601

XP Home

running 601

Y

Y-axis 228

YCoordinate 654

Z

Zoom 180, 425

Choose 425

In On 180