helpsystems

Intermapper User Guide
Intermapper
6.3

Copyright Terms and Conditions

Table of Contents

Welcome to Intermapper

Intermapper Server and Network Monitoring
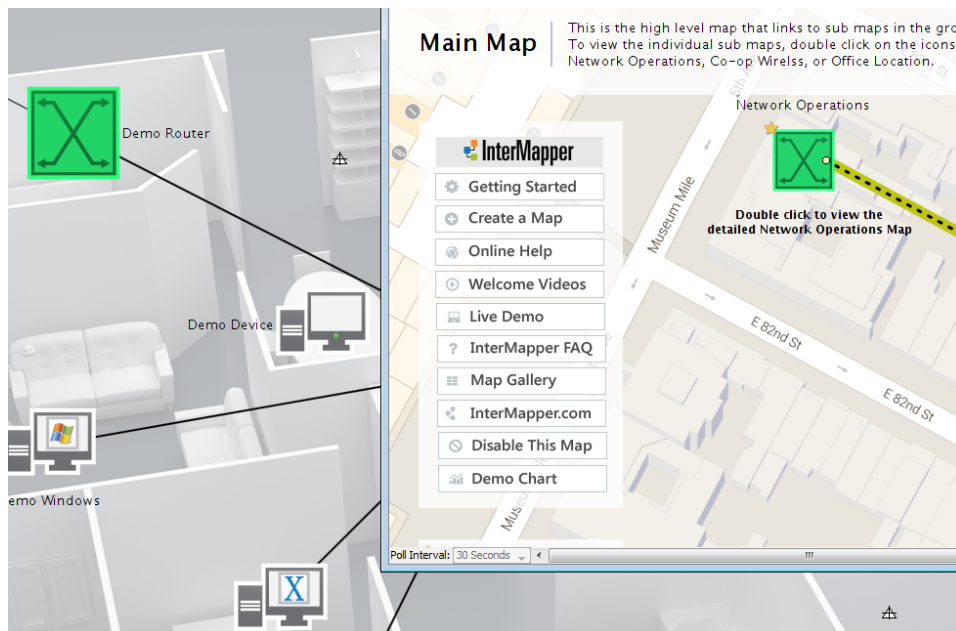
Intermapper is a network monitoring and alerting program. It continually tests routers, servers, hubs, and other computer devices that are attached to your network. If Intermapper detects a failure, it sends notifications to one or more individuals via sounds, e-mail, pagers, SMS text, or by running 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](#)

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

[Intermapper Flows](#)

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

[Intermapper Data Center](#)

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

[Intermapper Remote Access](#)

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 [IntermapperDeveloper Guide](#) is described separately.

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

[HelpSystems LLC](#)
[Intermapper Feedback](#)

6.3 | 201902051022 | February 2019

About Intermapper

What's New in Intermapper® 6.3?

Intermapper 6.3 includes a number new features and enhancements. Here's a summary...

Integration of Intermapper with Insite

HelpSystemsInsite provides a mobile-friendly, single pane window for HelpSystems software and streamlines software deployment. For more information, see [the HelpSystems website](#).

Intermapper for Insite allows you to connect to and monitor one or more Intermapper servers. In version 6.3 you do the following through Insite:

- **Add Connection** - add a network connection from Insite to one or more Intermapper servers.
- **Home** - view a list of connected Intermapper servers, with summary info about each connection.
- **Dashboard** - Add widgets to view various information about the devices on an Intermapper server, as well as the server itself. Create widgets to view:
  - The Device List
  - A Device Status Summary
  - Device Status over time
  - Server Resource Statistics over time.

  Select from a variety of chart styles.

> **NOTE:** For each Intermapper server you want to monitor through Insite, you need to do the following:
>
> - Enable the Intermapper Server's web server (in Server Settings > Web Server.)
> - Enter the Intermapper server's IP address and credentials in the Insite **Add Connection** pane.

System Requirements

> **NOTE:** If you are upgrading from 6.2 or earlier, HelpSystems recommends that you back up your chart data before running 6.3. Chart data is located in the Chart Data folder, found in the Intermapper Settings folder.

System requirements for Intermapper are now maintained only online. Please see the System Requirements page on the HelpSystems website.

License Agreement

HelpSystems, LLC SOFTWARE LICENSE AND SERVICES AGREEMENT

This software license and service agreement ("Agreement") is made by and between HelpSystems LLC (HelpSystems) and the entity on whose behalf such individual accepts this Agreement ("Client") formed by installing or updating the Software. Please read all the terms and conditions set forth in this Agreement before accepting this Agreement. By installing or updating the Software Client her by agrees to, and agrees to be bound by, the terms and conditions set forth in this Agreement, and represents to HelpSystems that it is authorized to do so. If you do not agree to all the terms of this Agreement or if you do not have the authority to bind the Company or organization on whose behalf you are accepting this Agreement, do not install or update the Software.

SECTION 1.   Definitions.

 For the purposes of this Agreement, the following terms have the meanings set forth below:

> 1.   **"Additional Services"** shall mean implementation or integration services; training services; programming or coding services; data conversion services;

or on-site consultation, other than those services provided by Maintenance defined in Section 1.9, provided by HelpSystems at the request of the Client.

1.2   **"Authorized Device"** shall mean a server, partition, computer, or any other virtual or otherwise emulated hardware system controlled or owned by Client and sanctioned by HelpSystems.

1.3   **"Authorized User"** shall mean a designated person or number of persons who are granted access to the Software by HelpSystems.

1.4   **"Confidential Information"** means any material, data, or information in whatever form or media of a party to this Agreement that is provided or disclosed to the other, and shall include, the Services rendered by HelpSystems to Client, the Software licensed by HelpSystems to Client, financial and operational information, and other matter relating to the operation of HelpSystems' or Client's business, including information relating to actual or potential customers, accounting, finance or tax information and pricing information.

1.5   **"Invoice"** shall mean any statement of charges issued by HelpSystems for Software, Maintenance, or Services.

1.6   **"Effective Date"** shall mean the date the Client accepts this Agreement.

1.7   **"Functional Specifications"** shall mean those system and operational requirements set forth in the Software Documentation to which the Software shall conform.

1.8   **"License Fees"** shall mean the fees paid to HelpSystems for the right to use the version of the Software which is current at the time of the Effective Date. All fees are non-refundable.

1.9   **"Maintenance"** shall mean providing the Client with (a) access to HelpSystems' technical assistance; (b) access to HelpSystems' self-service utilities; and (c) access to updates, and enhancements of the Software.

1.10   **"Maintenance Fees"** shall mean the fees paid to HelpSystems for Maintenance. All fees are non-refundable.

1.11   **"Maintenance Period"** shall mean the period of time that HelpSystems will provide Maintenance. The initial Maintenance Period shall commence and expire on the dates indicated on the Invoice. The Maintenance Period may be renewed by the Client in accordance with Section 7.

1.12   **"Services"** shall mean collectively any Maintenance and Additional Services provided by HelpSystems.

1.13 **"Software"** shall mean the products delivered to Client under the terms of this Agreement, including all updates, add-ons, and enhancements created by HelpSystems for those products.

1.14 **"Software Documentation"** shall mean any tutorials, technical publications, and materials supplied with the Software which include system requirements for implementation and operation of the Software as wellas the Functional Specifications of the Software.

SECTION 2. Scope and Term of Agreement.

This Agreement sets forth the terms and conditions under which HelpSystems shall license the Software and provide Maintenance and Services to Client. This Agreement shall remain in effect unless and until terminated by HelpSystems or Client in accordance with Section 10.

SECTION 3.   Software License.

3.1 Subject to the terms and provisions of this Agreement, as well as the payment of License Fees, HelpSystems hereby grants to Client, or an Authorized User of the Client, a non-exclusive, non-transferable, and non-assignable license to use the version of the Software which is current at the time of the Effective Date for Client's internal business purposes. The license covers the version of the Software which is current at the time of the Effective Date and any available Software Documentation.

3.2 Client may install or otherwise utilize the Software on an Authorized Device. The Software may not be moved to another device. If the Client desires to move the Software to another device, the Client shall secure the prior approval of HelpSystems, which may be granted subject to an additional fee.   Client shall not alter, modify, adapt, reverse engineer, decompile, disassemble, or create derivative works from the Software, nor take any other action intended to reproduce the source code of the Software or any part thereof without the prior written consent of HelpSystems. The Client shall not remove any copyright or proprietary rights notices from the Software and shall reproduce all such notices on any copies made in accordance with this Section 3.2.

3.3 Client may be allowed to transfer its right to use the Software provided (a) Client is in receipt of the prior written consent of HelpSystems, which may be withheld by HelpSystems in HelpSystems' sole discretion; (b) Client has paid any additional fee which HelpSystems may charge Client at HelpSystems' sole discretion; and (c) Client transfers the most recent production release of the Software, including any and all updates to the Software. Any transfer of Client's right to use the Software made in violation of the terms and provisions of this Section 3.3 shall constitute a breach of this Agreement.

3.4   Client agrees that the Software will not be shipped, transferred, or exported into any country or used inany manner prohibited by the United States Export Administration Act, or any other export laws, restrictions, or regulations.

SECTION 4.   Software Delivery and Installation.

4.1   Upon payment of the License Fee, HelpSystems shall make the version of the Software which is current at the time of the Effective Date available to Client along with a valid license key. Whether by providing an electronic download, physical distribution, or any other form of conveyance, the software shall be deemed delivered once it is made available to Client. The Client may also access and utilize any Software Documentation related to the Software delivered under the terms of this agreement.

4.2   Client shall be responsible for installation of the Software on an Authorized Device that meets the requirements for operation of the Software as identified in the Software Documentation.

SECTION 5.   Nondisclosure of Confidential Information.

5.1   HelpSystems and Client agree that the party receiving Confidential Information shall exercise the same degree of care and protection with respect to the Confidential Information of the party disclosing the Confidential Information that it would exercise with respect to its own Confidential Information and shall not directly or indirectly disclose, copy, distribute, republish, or allow any third party to have access to any Confidential Information of the disclosing party, without the prior written consent of the disclosing party, except the receiving party may disclose Confidential Information on a need-to-know basis, to employees, agents or representatives of the receiving party who are informed by the receiving party of the confidential nature of the Confidential Information and the obligations of the receiving party under this Agreement or in accordance with a judicial or other governmental order, but only if the receiving party promptly notifies the disclosing party of the order and complies with any applicable protective or similar order. The receiving party will cause its employees, agents and representatives to comply with the provisions of this Section 5.1.

5.2   HelpSystems and Client agree that the party receiving Confidential Information will promptly notify the disclosing party of any unauthorized use or disclosure of Confidential Information, or any other breach of this Agreement; and assist the disclosing party in every reasonable way to retrieve any Confidential Information that was used or disclosed by the receiving party or an employee, agent and representative of the receiving party without the disclosing party's specific prior written authorization and to mitigate the harm caused by the unauthorized use or disclosure.

5.3 HelpSystems and Client agree that the party receiving Confidential Information will not breach Section 5.1 or Section 5.2 by using or disclosing Confidential Information if the receiving party demonstrates that the information used or disclosed (a) is generally available to the public other than as a result of a disclosure by the receiving party or an employee, agent and representative of the receiving party; (b) was received by the receiving party from a third party without any limitations on use or disclosure; or (c) was independently developed by the receiving party without use of the Confidential Information.

5.4 HelpSystems and Client agree that upon the request of the party disclosing Confidential Information, the receiving party will (a) promptly return to the disclosing party all materials furnished by the disclosing party containing Confidential Information, together with all copies and summaries of Confidential Information in the possession or under the control of the receiving party, and provide written certification that all such Confidential Information has been returned to the disclosing party, or (b) promptly destroy all materials furnished by the disclosing party containing Confidential Information, together with all copies and summaries of Confidential Information in the possession or under the control of the receiving party, and provide written certification that all such Confidential Information has been destroyed by the receiving party.

5.5 HelpSystems and Client acknowledge and agree that the remedies available at law for any breach of this Agreement will, by their nature, be inadequate. Accordingly, each party may obtain injunctive relief or other equitable relief to restrain a breach or threatened breach of this Agreement or to specifically enforce this Agreement, without proving that any monetary damages have been sustained.

SECTION 6. Software Ownership Rights; Intellectual Property Rights and Intellectual Property Rights Indemnification by HelpSystems.

6.1 Client acknowledges and agrees that the Software and Software Documentation, and all intellectual property rights therein, are (a) the sole and exclusive property of HelpSystems; (b)protected by United States Copyright Law; and (c) the Software is a trade secret of HelpSystems. Except to the limited extent required for Client to use the Software pursuant to the license granted in Section 3.1, nothing in this Agreement will be deemed to grant, by implication, estoppel or otherwise, a license in any existing or future intellectual property of HelpSystems. No title or ownership rights to the Software are transferred to Client by this Agreement, but shall remain with HelpSystems. All rights not expressly granted by HelpSystems with respect to the Software under this Agreement are reserved by HelpSystems.

6.2 HelpSystems shall defend at its own expense any action against Client brought by a third party to the extent that the action is based upon a claim that the Software

directly infringes any copyright filed in the United States or misappropriates any trade secret recognized as such under the Uniform Trade Secrets Act, and HelpSystems will pay those costs and damages finally awarded against Client in any such action that are specifically attributable to such claim or those costs and damages agreed to in a monetary settlement of such action. HelpSystems obligations under this Section 6.2 are conditioned on (a) Client notifying HelpSystems within ten (10) days of notice of such action, (b) Client giving HelpSystems sole control of the defense thereof and any related settlement negotiations, and (c) Client cooperating with HelpSystems in such defense (including, without limitation, by making available to HelpSystems all documents and materials in Client's possession or control that are relevant to the infringement or misappropriation claims, and by making Client's personnel available to testify or consult with HelpSystems or its attorneys in connection with said defense). If the Software becomes, or in HelpSystems' opinion is likely to become, the subject of an infringement or misappropriate claim, HelpSystems may, at its option and expense, either (i) procure for Client the right to continue using the Software; (ii) replace or modify the Software so that it becomes non- infringing, or (iii) terminate Client's right to use the Software and give Client a refund or credit of the amounts actually paid by Client to HelpSystems for the Software less a reasonable allowance for the period of time Client has used the Software. HelpSystems will have no obligation with respect to any infringement or misappropriation claim based upon (1) any use of the Software not in accordance with the Agreement or for purposes not intended by HelpSystems; (2) any use of the Software in combination with other products, equipment, software, or data not supplied by HelpSystems; (3) any use of any release of the Software other than the most current release made available to Client; or (4) any modification of the Software made by any person other than HelpSystems. This Section 6.2 states HelpSystems' entire liability and Client's sole and exclusive remedy for infringement and misappropriation claims and actions.

SECTION 7.   Maintenance and Additional Services.

 7.1   During the Maintenance Period HelpSystems will provide Client with Maintenance. HelpSystems' continuing obligation to provide Maintenance is contingent on payment in full of the Maintenance Fees by Client to HelpSystems. HelpSystems maintenance agreements automatically renew for successive twelve (12) month periods unless Client provides written notice of its election to not renew sixty (60) days in advance of the renewal date. HelpSystems may allow Client to pay the annual maintenance fee by credit card (HelpSystems uses a PCI compliant third party system) and, with your agreement, HelpSystems can annually automatically charge the Client credit card upon the renewal date. Within the sixty (60) day period prior to the expiration of the Maintenance Period, HelpSystems shall send Client an Invoice for Maintenance Fees for the next Maintenance Period. The Maintenance

Fees charged to Client for the next Maintenance Period are subject to change in HelpSystems' sole discretion. Client's payment of the Maintenance Fee in response to an Invoice for Maintenance prior to the expiration date of the then current Maintenance Period, will extend the Maintenance Period until the new expiration date indicated on HelpSystems' Invoice for Maintenance. Client's failure to pay the Maintenance Fees prior to the expiration date of the then current Maintenance Period shall constitute Client's election to allow the Maintenance Period to expire without further notice from HelpSystems. If the Maintenance Period is allowed to expire, HelpSystems may condition any subsequent reinstatement of the Maintenance Period on payment by Client to HelpSystems of an additional fee set by HelpSystems in HelpSystems' sole discretion.

7.2   The Maintenance provided by HelpSystems during the Maintenance Period specifically and expressly does <u>NOT</u> include any Additional Services as defined in Section 1.1. Should Client require Additional Services, those Additional Services may be available subject to the payment of fees by Client to HelpSystems and as otherwise agreed to in writing by HelpSystems and Client.

7.3   In the event HelpSystems incurs any liability to Client, including but not limited to a credit balance and whether arising from this Agreement or otherwise, HelpSystems may, without notice to Client, set-off the amount of such liability against any liability of Client to HelpSystems, including but not limited to Maintenance Fees to be paid by Client to HelpSystems for Maintenance pursuant to Section 7.1.

SECTION 8.   <u>Limited Warranty and Warranty Disclaimer</u>.

8.1   HelpSystems warrants that (a) the Software shall substantially conform to the Functional Specifications and(b) that the Software Documentation shall be substantially free of errors. This warranty shall extend for ninety (90) days from delivery of the Software as set forth in Section 4.1. In the event of any breach of the warranty set forth in this Section 8.1, HelpSystems' sole and exclusive responsibility, andthe Client's sole and exclusive remedy, shall be for HelpSystems to correct or replace, at no additional charge to Client, any portion of the Software found to be defective; provided, however, that if within a commercially reasonable period HelpSystems neither corrects nor replaces the defective Software, then Client's sole and exclusive remedy shall be to receive direct damages not to exceed the License Fees paid to HelpSystems. HelpSystems does not warrant that the operation of the Software will be uninterrupted or error free or that the Software will meet the Client's operational requirements. HelpSystems is not responsible for errors or defects in the Software caused by changes in or to the operating characteristics of the Client's computer hardware or operating systems made after delivery of the Software as set forth in Section 4.1 or errors or defects in the Software caused by

the interaction of the Software with third party programs or applications. The warranty set forth in this Section 8.1 shall be void as to Software where noncompliance is caused or related to (a) the acts or omissions of non-HelpSystems personnel, agents, or third parties; (b) any alternations or modifications made to the Software by Client, its personnel or agents; (c) use of the Software other than in the operating environment specified in the Software Documentation; or (d) coding, information, or specifications created or provided by the Client.

8.2 HelpSystems warrants that any Services provided by HelpSystems pursuant to this Agreement shall be performed in accordance with the prevailing professional standards of the software industry. In the event of any breach of the warranty set forth in this Section 8.2, HelpSystems' sole and exclusive responsibility, and the Client's sole and exclusive remedy, shall be for HelpSystems to correct, at no additional charge to Client, any portion of the Services found not to meet prevailing professional standards of the software industry; provided, however, that if within a commercially reasonable period HelpSystems fails to correct the Services found not to meet prevailing professional standards of the software industry, then Client's sole and exclusive remedy shall be to receive direct damages not to exceed the fees paid to HelpSystems for the Services.

8.3 In the event of any breach of any provisions of this Agreement other than the warranties set forth in this Agreement, Client's sole and exclusive remedy shall be to receive direct damages not to exceed the License Fee.

8.4 EXCEPT AS SET FORTH IN THIS SECTION 8, HELPSYSTEMS MAKES NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES, OR THEIR CONDITION, MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE OR USE BY CLIENT. HELPSYSTEMS FURNISHES THE ABOVE WARRANTIES IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

SECTION 9. Limitation of Liability.

9.1 HELPSYSTEMS SHALL NOT BE LIABLE FOR ANY (a) SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS, ARISING FROM OR RELATED TO A BREACH OF THIS AGREEMENT OR THE OPERATION OR USE OF THE SOFTWARE OR SERVICES INCLUDING SUCH DAMAGES, WITHOUT LIMITATION, AS DAMAGES ARISING FROM LOSS OF DATA OR PROGRAMMING, LOSS OF REVENUE OR PROFITS, FAILURE TO REALIZE SAVINGS OR OTHER BENEFITS, DAMAGE TO EQUIPMENT, AND CLAIMS AGAINST CUSTOMER BY ANY THIRD PARTY, EVEN IF HELPSYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (b) DAMAGES (REGARDLESS OF THEIR NATURE) FOR ANY DELAY OR FAILURE BY

HELPSYSTEMS TO PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT DUE TO ANY CAUSE BEYOND HELPSYSTEMS' REASONABLE CONTROL; OR (c) CLAIMS MADE A SUBJECT OF A LEGAL PROCEEDING AGAINST HELPSYSTEMS MORE THAN ONE (1) YEAR AFTER ANY SUCH CAUSE OF ACTION FIRST AROSE.

9.2   NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT, BUT EXCLUDING ANY CLAIMS FOR INDEMNIFICATION UNDER SECTION 6, HELPSYSTEMS' LIABILITY UNDER THIS AGREEMENT, WHETHER UNDER CONTRACT LAW, TORT LAW, WARRANTY, OR OTHERWISE SHALL BE LIMITED TO DIRECT DAMAGES NOT TO EXCEED THE AMOUNTS ACTUALLY RECEIVED BY HELPSYSTEMS UNDER THIS AGREEMENT.

SECTION 10.   Termination.

10.1   HelpSystems shall have the right to terminate this Agreement if (a) Client fails to pay any fees that are due, other than for Maintenance, within ten (10) days after receiving written notice of such obligation from HelpSystems; (b) Client breaches any provision of this Agreement and fails to remedy such breach within thirty (30) days after receiving written notice of such breach; or (c) a proceeding is instituted by or against Client seeking to adjudicate it bankrupt or insolvent, or seeking liquidation, winding up, reorganization, arrangement, adjustment, protection, relief or composition of it or its debts under any law relating to bankruptcy, insolvency or reorganization or relief of debtors, or seeking an entry of an order for relief or the appointment of a receiver, trustee or other similar official for it or any substantial part of its property or taking any action to authorize any of the foregoing or similar actions by or against Client.

10.2   Client shall have the right to terminate this Agreement if (a) HelpSystems breaches any provision of this Agreement and fails to remedy such breach within thirty (30) days after receiving written notice of such breach; or (b) a proceeding is instituted by or against HelpSystems seeking to adjudicate it bankrupt or insolvent, or seeking liquidation, winding up, reorganization, arrangement, adjustment, protection, relief or composition of it or its debts under any law relating to bankruptcy, insolvency or reorganization or relief of debtors, or seeking an entry of an order for relief or the appointment of a receiver, trustee or other similar official for it or any substantial part of its property or taking any action to authorize any of the foregoing or similar actions by or against HelpSystems.

10.3   Upon any termination of this Agreement, Client shall make no further use of the Software and shall either return to HelpSystems or destroy originals and all copies of the Software and Software Documentation. Client shall supply a written affidavit executed by an officer of Client to HelpSystems certifying that it no longer possesses any embodiments of the Software or Software Documentation. No refunds or credits will be due Client.

SECTION 11.   Governing Law; Venue.

HelpSystems and Client agree that this Agreement shall be governed by and construed in accordance with the laws of the State of Minnesota without regard to conflict of laws principles. Any action or proceeding seeking to enforce any provisions of, or based on any right or claim arising out of this Agreement will be brought against HelpSystems or Client in Hennepin County Circuit Court of the State of Minnesota or, subject to applicable jurisdictional requirements in the United States District Court of the District of Minnesota, and HelpSystems and Client consent to the jurisdiction of such courts (and of the appropriate appellate courts) in any such action or proceeding and waives any objection to such venue.

SECTION 12.   Waiver.

HelpSystems and Client agree that this Agreement may not be changed or modified, nor may any provision hereof be waived, except as agreed to in writing by HelpSystems and Client.

SECTION 13.   Severability.

If any provision of this Agreement is found to be illegal, invalid, or unenforceable, that provision shall not affect the validity or enforceability of this Agreement as a whole, and this Agreement shall then be construed in all respects as if such invalid or unenforceable provision was omitted.

CLIENT ACKNOWLEDGES THAT CLIENT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. CLIENT FURTHER AGREES THAT THE AGREEMENT IS A COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN HELPSYSTEMS AND CLIENT AND THAT IT SUPERSEDES ALL PRIOR AND CONTEMPORANEOUS AGREEMENTS, NEGOTIATIONS, DISCUSSIONS, AND PROPOSALS, ORAL OR WRITTEN, AND ANY AND ALL OTHER COMMUNICATIONS RELATING TO THE SUBJECT MATTERS OF THE AGREEMENT.

Trademark, Copyright, and Licenses

- Trademark and Copyright Information
- Third Party Packages
- Acknowledgements
- Babel
- DNS-SD
- freetype
- gd library

- [Genshi](#)
- [IJG JPEG](#)
- [jQuery](#)
- [jQuery-JSON](#)
- [ldaptor](#)
- [libcrypto and libssl](#)
- [libpng](#)
- [libsnmp](#)
- [miglayout](#)
- [postgresql](#)
- [psycopg](#)
- [pyASN.1](#)
- [pycrypto](#)
- [pyopenssl](#)
- [pyparsing](#)
- [pyrad](#)
- [python](#)
- [spidermonkey](#)
- [sqlite](#)
- [twisted](#)
- [zlib](#)
- [zopeinterface](#)

Trademark and Copyright Information

```
Intermapper™ is a registered trademark of Help/Systems, LLC.
Intermapper RemoteAccess™,
Intermapper DataCenter™, Intermapper Auth Server™, MacPing™,
and SNMP
Watcher™ are trademarks of HelpSystems LLC. Intermapper,
Intermapper RemoteAccess,
Intermapper Data Center, Intermapper Auth Server, MacPing,
and SNMP Watcher are copyright
 (c)HelpSystems, LLC. All rights reserved.

This manual documents Intermapper 6.3, and was last updated
in February 2019.
```

```
Help/Systems, LLC.
6455 City West Parkway
Eden Prairie, MN 55344
Phone: +1 952-933-0609
Toll Free: 1-800-328-1000
http://www.helpsystems.com
```

Third Party Packages

```
Other programs mentioned in this manual are trademarked and
copyrighted by their
respective owners. The _Third Party Licenses_ page gives the
full text of each of the
licenses below.

Certain sounds copyright  Ambrosia Software, Inc. Used with
Permission.

This product includes cryptographic software written by Eric
Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL
Project for use in the OpenSSL
toolkit. (http://www.openssl.org).

The libpng library is copyright  2004, 2006-2009 Glenn
Randers-Pehrson.

This software is based in part on the work of the Independent
JPEG Group.

Portions of this software are copyright  2006 The FreeType
Project (www.freetype.org).

Ldaptor: Copyright (C) 2002  Tommi Virtanen, Matthew W.
Lefkowitz

pyopenssl and psycopg are made available under the GPL.

Python 2.6: Copyright (c) 2001-2009 Python Software
Foundation;
All Rights Reserved.
```

```
pycrypto is available under a free usage license. Thanks to
A.M. Kuchling at
http://www.amk.ca.

PostgresSQL Database Management System: Portions copyright
(c) 1996-2008, PostgreSQL
Global Development Group; Portions Copyright (c) 1994, The
Regents of the University of
California

Zope is made available under the Zope Public License (ZPL)
Version 2.1.
twisted: Copyright (c) 2001-2008 Allen Short, Andrew
Bennetts,
Apple Computer, Inc., Benjamin Bruheim, Bob Ippolito,
Canonical Limited,
Christopher Armstrong, David Reid, Donovan Preston, Eric
Mangold,
Itamar Shtull-Trauring, James Knight, Jason A. Mobarak, Jean-
Paul Calderone,
Jonathan Lange, Jonathan D. Simms, Jürgen Hermann, Kevin
Turner,
Mary Gardiner, Matthew Lefkowitz, Massachusetts Institute of
Technology,
Moshe Zadka, Paul Swartz, Pavel Pergamenshchik, Ralph Meijer,
Sean Riley,
Software Freedom Conservancy, Travis B. Hartwell, Thomas
Herve, Eyal Lotem,
Antoine Pitrou, Andy Gayton.

pyrad: Copyright 2002-2007 Wichert Akkerman. All rights
reserved. Copyright 2007 Simplon. All rights reserved.

pyparsing: Copyright (c) 2003-2006  Paul T. McGuire

pyASN.1: Copyright (c) 2005, 2006 Ilya Etingof
<ilya@glas.net>, all rights reserved.
```

Acknowledgements

```
Portions of this Help/Systems,LLC Software may utilize the
following copyrighted,
open source material (OSS), the use of which is hereby
```

```
acknowledged.
```

Babel

```
Copyright (C) 2007 Edgewall Software
All rights reserved.
Redistribution and use in source and binary forms, with or
without modification, are
permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above
copyright notice, this list of
conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above
copyright notice, this list
of conditions and the following disclaimer in the
documentation and/or other materials
provided with the distribution.
3. The name of the author may not be used to endorse or
promote products derived from
this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE AUTHOR BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA,
OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```

dns_sd

```
DNS-SD
(http://developer.apple.com/opensource/internet/bonjour.html)
```

```
[dns_sd.h, dnssd_clientstub.c, dnssd_ipc.c from
mDNSResponder-107.6]

To accommodate license compatibility with the widest possible
range
of client code licenses, the shared library code, which is
linked
at runtime into the same address space as the client using
it, is
licensed under the terms of the "Three-Clause BSD License".

*
* Copyright (c) 2003-2004, Apple Computer, Inc. All rights
reserved.
*
* Redistribution and use in source and binary forms, with or
without
* modification, are permitted provided that the following
conditions are met:
*
* 1.  Redistributions of source code must retain the above
copyright notice,
*     this list of conditions and the following disclaimer.
* 2.  Redistributions in binary form must reproduce the
above copyright notice,
*     this list of conditions and the following disclaimer
in the documentation
*     and/or other materials provided with the distribution.
* 3.  Neither the name of Apple Computer, Inc. ("Apple") nor
the names of its
*     contributors may be used to endorse or promote
products derived from this
*     software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS
"AS IS" AND ANY
* EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE
* DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE
LIABLE FOR ANY
* DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
```

```
CONSEQUENTIAL DAMAGES
* (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
OF THE USE OF THIS
* SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
*
```

freetype

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~

FreeType2 Library by The FreeType Project
(http://www.freetype.org)



  """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
""""""""""""""""""
      Portions of this software are copyright ^(c) 2006 The
FreeType
      Project (www.freetype.org). All rights reserved.


  """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
""""""""""""""""""

                    The FreeType Project LICENSE
                    ----------------------------

                           2006-Jan-27

                    Copyright 1996-2002, 2006 by
            David Turner, Robert Wilhelm, and Werner Lemberg
```

```
    Introduction
    ============


    The FreeType  Project is distributed in  several archive
packages;
    some of them may contain, in addition to the FreeType
font engine,
    various tools and  contributions which rely on, or
relate to, the
    FreeType Project.

    This  license applies  to all  files found  in such
packages, and
    which do not  fall under their own explicit  license.
The license
    affects  thus  the  FreeType   font  engine,  the  test
programs,
    documentation and makefiles, at the very least.

    This  license   was   inspired  by  the  BSD,   Artistic,
 and  IJG
    (Independent JPEG  Group) licenses, which  all encourage
inclusion
    and  use of  free  software in  commercial  and freeware
 products
    alike.  As a consequence, its main points are that:

     o We don't promise that this software works. However,
we will be
        interested in any kind of bug reports. (`as is'
distribution)

     o You can  use this software for whatever you  want, in
parts or
        full form, without having to pay us. (`royalty-free'
usage)

     o You may not pretend that  you wrote this software.
If you use
        it, or  only parts of it,  in a program,  you must
acknowledge
        somewhere  in  your  documentation  that  you  have
used  the
        FreeType code. (`credits')
```

```
     We  specifically  permit  and  encourage  the  inclusion
 of  this
     software, with  or without modifications,  in commercial
products.
     We  disclaim  all warranties  covering  The  FreeType
Project  and
     assume no liability related to The FreeType Project.


     Finally,  many  people  asked  us  for  a  preferred
form  for  a
     credit/disclaimer to use in compliance with this
license.  We thus
     encourage you to use the following text:

      """
      Portions of this software are copyright ^(c) <year> The
FreeType
      Project (www.freetype.org).  All rights reserved.
      """

     Please replace <year> with the value from the FreeType
version you
     actually use.


   Legal Terms
   ===========

   0. Definitions
   --------------

   Throughout this license,  the terms `package', `FreeType
Project',
   and  `FreeType  archive' refer  to  the  set  of files
originally
   distributed  by the  authors  (David Turner,  Robert
Wilhelm,  and
   Werner Lemberg) as the `FreeType Project', be they named
as alpha,
   beta or final release.

    `You' refers to  the licensee, or person using  the
```

```
project, where
      `using' is a generic term including compiling the
project's source
      code as  well as linking it  to form a  `program' or
`executable'.
      This  program is  referred to  as  `a program  using the
 FreeType
      engine'.

      This  license applies  to all  files distributed  in
the original
      FreeType  Project,   including  all  source   code,
binaries  and
      documentation,  unless  otherwise  stated   in  the
file  in  its
      original, unmodified form as  distributed in the
original archive.
      If you are  unsure whether or not a particular  file is
covered by
      this license, you must contact us to verify this.

      The FreeType  Project is copyright (C) 1996-2000  by
David Turner,
      Robert Wilhelm, and Werner Lemberg.  All rights reserved
except as
      specified below.

   1. No Warranty
   --------------

      THE FREETYPE PROJECT  IS PROVIDED `AS IS' WITHOUT
WARRANTY OF ANY
      KIND, EITHER  EXPRESS OR IMPLIED,  INCLUDING, BUT NOT
LIMITED TO,
      WARRANTIES  OF  MERCHANTABILITY   AND  FITNESS  FOR  A
PARTICULAR
      PURPOSE.  IN NO EVENT WILL ANY OF THE AUTHORS OR
COPYRIGHT HOLDERS
      BE LIABLE  FOR ANY DAMAGES CAUSED  BY THE USE OR  THE
INABILITY TO
      USE, OF THE FREETYPE PROJECT.

   2. Redistribution
   -----------------
```

```
      This  license  grants  a  worldwide, royalty-free,
perpetual  and
      irrevocable right  and license to use,  execute,
perform, compile,
      display,  copy,  create  derivative  works   of,
distribute  and
      sublicense the  FreeType Project (in  both source and
object code
      forms)  and  derivative works  thereof  for  any
purpose; and  to
      authorize others  to exercise  some or all  of the
rights granted
      herein, subject to the following conditions:

       o Redistribution of  source code  must retain this
license file
        (`FTL.TXT') unaltered; any  additions, deletions or
changes to
        the original  files must be clearly  indicated in
accompanying
        documentation.   The   copyright   notices   of   the
unaltered,
        original  files must  be  preserved in  all  copies
of  source
        files.

      o Redistribution in binary form must provide a
disclaimer  that
        states  that  the software is based in part of the
work of the
        FreeType Team,  in  the  distribution  documentation.
 We also
        encourage you to put an URL to the FreeType web page
in  your
        documentation, though this isn't mandatory.

      These conditions  apply to any  software derived from or
 based on
      the FreeType Project,  not just the unmodified files.
If you use
      our work, you  must acknowledge us.  However, no  fee
need be paid
      to us.
```

```
   3. Advertising
   --------------

      Neither the  FreeType authors and  contributors nor you
shall use
      the name of the  other for commercial, advertising, or
promotional
      purposes without specific prior written permission.

      We suggest,  but do not require, that  you use one or
more of the
      following phrases to refer  to this software in your
documentation
      or advertising  materials: `FreeType Project',
`FreeType Engine',
      `FreeType library', or `FreeType Distribution'.

      As  you have  not signed  this license,  you are  not
required to
      accept  it.   However,  as  the FreeType  Project  is
copyrighted
      material, only  this license, or  another one contracted
 with the
      authors, grants you  the right to use, distribute,  and
modify it.
      Therefore,  by  using,  distributing,  or modifying  the
 FreeType
      Project, you indicate that you understand and accept all
the terms
      of this license.

   4. Contacts
   -----------

      There are two mailing lists related to FreeType:

       o freetype@nongnu.org

         Discusses general use and applications of FreeType,
as well as
         future and  wanted additions to the  library and
distribution.
         If  you are looking  for support,  start in  this
```

```
list  if you
       haven't found anything to help you in the
documentation.

      o freetype-devel@nongnu.org

      Discusses bugs,  as well  as engine internals,
design issues,
      specific licenses, porting, etc.

   Our home page can be found at

    http://www.freetype.org
```

gd library

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~

gd: A graphics library for fast image creation
(http://www.boutell.com/gd)

    Portions copyright 1994, 1995, 1996, 1997, 1998, 1999,
2000, 2001,
    2002 by Cold Spring Harbor Laboratory. Funded under
Grant
    P41-RR02188 by the National Institutes of Health.

    Portions copyright 1996, 1997, 1998, 1999, 2000, 2001,
2002 by
    Boutell.Com, Inc.

    Portions relating to GD2 format copyright 1999, 2000,
2001, 2002
    Philip Warner.

    Portions relating to PNG copyright 1999, 2000, 2001,
2002 Greg
    Roelofs.

    Portions relating to gdttf.c copyright 1999, 2000, 2001,
2002 John
```

```
      Ellson (ellson@lucent.com).

      Portions relating to gdft.c copyright 2001, 2002 John
Ellson
      (ellson@lucent.com).

      Portions relating to JPEG and to color quantization
copyright 2000,
      2001, 2002, Doug Becker and copyright (C) 1994, 1995,
1996, 1997,
      1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This
software is
      based in part on the work of the Independent JPEG Group.
See the
      file README-JPEG.TXT for more information.

      Portions relating to WBMP copyright 2000, 2001, 2002
Maurice
      Szmurlo and Johan Van den Brande.

      Permission has been granted to copy, distribute and
modify gd in
      any context without fee, including a commercial
application,
      provided that this notice is present in user-accessible
supporting
      documentation.

      This does not affect your ownership of the derived work
itself, and
      the intent is to assure proper credit for the authors of
gd, not to
      interfere with your productive use of gd. If you have
questions,
      ask. "Derived works" includes all programs that utilize
the
      library. Credit must be given in user-accessible
documentation.

      This software is provided "AS IS." The copyright holders
disclaim
      all warranties, either express or implied, including but
not
      limited to implied warranties of merchantability and
```

```
fitness for a
      particular purpose, with respect to this code and
accompanying
      documentation.

      Although their code does not appear in gd, the authors
wish to thank
      David Koblas, David Rowley, and Hutchison Avenue
Software Corporation
      for their prior contributions.
```

Genshi

```
Copyright (C) 2007 Edgewall Software
All rights reserved.
Redistribution and use in source and binary forms, with or
without modification, are permitted provided that the
following conditions are met:
1. Redistributions of source code must retain the above
copyright notice, this list of conditions and the following
disclaimer.
2. Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following
disclaimer in the documentation and/or other materials
provided with the distribution.
3. The name of the author may not be used to endorse or
promote products derived from this software without
specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE AUTHOR BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS
OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY
OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR
```

```
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

IJG JPEG

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~

The Independent JPEG Group's JPEG software
(http://www.ijg.org)



  """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
""""""""""""""""
     This software is based in part on the work of the
Independent JPEG Group.


  """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
""""""""""""""""

   --- LEGAL ISSUES Section Snipped from README file ---

   In plain English:

   1. We don't promise that this software works.  (But if you
find any bugs,
      please let us know!)
   2. You can use this software for whatever you want.  You
don't have to pay us.
   3. You may not pretend that you wrote this software.  If
you use it in a
      program, you must acknowledge somewhere in your
documentation that
      you've used the IJG code.

   In legalese:

   The authors make NO WARRANTY or representation, either
express or implied,
   with respect to this software, its quality, accuracy,
merchantability, or
```

```
    fitness for a particular purpose.   This software is
provided "AS IS", and you,
    its user, assume the entire risk as to its quality and
accuracy.

    This software is copyright (C) 1991-2009, Thomas G. Lane,
Guido Vollbeding.
    All Rights Reserved except as specified below.

    Permission is hereby granted to use, copy, modify, and
distribute this
    software (or portions thereof) for any purpose, without
fee, subject to these
    conditions:
    (1) If any part of the source code for this software is
distributed, then this
    README file must be included, with this copyright and no-
warranty notice
    unaltered; and any additions, deletions, or changes to the
original files
    must be clearly indicated in accompanying documentation.
    (2) If only executable code is distributed, then the
accompanying
    documentation must state that "this software is based in
part on the work of
    the Independent JPEG Group".
    (3) Permission for use of this software is granted only if
the user accepts
    full responsibility for any undesirable consequences; the
authors accept
    NO LIABILITY for damages of any kind.

    These conditions apply to any software derived from or
based on the IJG code,
    not just to the unmodified library.  If you use our work,
you ought to
    acknowledge us.

    Permission is NOT granted for the use of any IJG author's
name or company name
    in advertising or publicity relating to this software or
products derived from
    it.  This software may be referred to only as "the
Independent JPEG Group's
```

```
    software".

    We specifically permit and encourage the use of this
software as the basis of
    commercial products, provided that all warranty or
liability claims are
    assumed by the product vendor.



    ansi2knr.c is included in this distribution by permission
of L. Peter Deutsch,
    sole proprietor of its copyright holder, Aladdin
Enterprises of Menlo Park, CA.
    ansi2knr.c is NOT covered by the above copyright and
conditions, but instead
    by the usual distribution terms of the Free Software
Foundation; principally,
    that you must include source code if you redistribute it.
(See the file
    ansi2knr.c for full details.)  However, since ansi2knr.c
is not needed as part
    of any program generated from the IJG code, this does not
limit you more than
    the foregoing paragraphs do.

    The Unix configuration script "configure" was produced
with GNU Autoconf.
    It is copyright by the Free Software Foundation but is
freely distributable.
    The same holds for its supporting scripts (config.guess,
config.sub,
    ltconfig, ltmain.sh).  Another support script, install-sh,
is copyright
    by M.I.T. but is also freely distributable.

    The IJG distribution formerly included code to read and
write GIF files.
    To avoid entanglement with the Unisys LZW patent, GIF
reading support has
    been removed altogether, and the GIF writer has been
simplified to produce
    "uncompressed GIFs".  This technique does not use the LZW
algorithm; the
    resulting GIF files are larger than usual, but are
```

```
readable by all standard
   GIF decoders.

   We are required to state that
      "The Graphics Interchange Format(c) is the Copyright
property of
      CompuServe Incorporated.  GIF(sm) is a Service Mark
property of
      CompuServe Incorporated."

   --- End Snippet ---
```

jQuery

```
Copyright (c) 2009 John Resig, http://jquery.com/
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the Software
without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute,
sublicense, and/or sell copies of the Software, and
to permit persons to whom the Software is furnished to do so,
subject to the following conditions:
The above copyright notice and this permission notice shall
be included in all copies or substantial portions
of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY
KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR
COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN
AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT
OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

jQuery-JSON

```
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the Software
without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute,
sublicense, and/or sell copies of the Software, and
to permit persons to whom the Software is furnished to do so,
subject to the following conditions:
The above copyright notice and this permission notice shall
be included in all copies or substantial portions
of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY
KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR
COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN
AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT
OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

ldaptor

```
ldaptor is released under the GNU Lesser General Public
License.
```

libcrypto and libssl

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~

libcrypto and libssl (OpenSSL) http://www.openssl.org



  """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
""""""""""""""""
    This product includes software developed by the OpenSSL
```

```
Project
    for use in the OpenSSL Toolkit (http://www.openssl.org/)
    This product includes cryptographic software written by
Eric Young
    (eay@cryptsoft.com)
    This product includes software written by Tim Hudson
(tjh@cryptsoft.com)


 """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
"""""""""""""""""

     OpenSSL License
     ---------------

   /*
================================================================
=======
    * Copyright (c) 1998-2008 The OpenSSL Project.  All
rights reserved.
    *
    * Redistribution and use in source and binary forms, with
or without
    * modification, are permitted provided that the following
conditions
    * are met:
    *
    * 1. Redistributions of source code must retain the above
copyright
    *    notice, this list of conditions and the following
disclaimer.
    *
    * 2. Redistributions in binary form must reproduce the
above copyright
    *    notice, this list of conditions and the following
disclaimer in
    *    the documentation and/or other materials provided
with the
    *    distribution.
    *
    * 3. All advertising materials mentioning features or use
of this
    *    software must display the following acknowledgment:
    *    "This product includes software developed by the
```

```
OpenSSL Project
     *      for use in the OpenSSL Toolkit.
(http://www.openssl.org/)"
     *
     * 4. The names "OpenSSL Toolkit" and "OpenSSL Project"
must not be
used to
     *      endorse or promote products derived from this
software without
     *      prior written permission. For written permission,
please contact
     *      openssl-core@openssl.org.
     *
     * 5. Products derived from this software may not be
called "OpenSSL"
     *      nor may "OpenSSL" appear in their names without
prior written
     *      permission of the OpenSSL Project.
     *
     * 6. Redistributions of any form whatsoever must retain
the following
     *      acknowledgment:
     *      "This product includes software developed by the
OpenSSL Project
     *      for use in the OpenSSL Toolkit
(http://www.openssl.org/)"
     *
     * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS
IS'' AND ANY
     * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE
     * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
     * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL
PROJECT OR
     * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL,
     * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT
     * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES;
     * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
     * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
```

```
IN CONTRACT,
    * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE)
    * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED
    * OF THE POSSIBILITY OF SUCH DAMAGE.
    *
===============================================================
=======
    *
    * This product includes cryptographic software written by
Eric Young
    * (eay@cryptsoft.com).  This product includes software
written by Tim
    * Hudson (tjh@cryptsoft.com).
    *
    */

    Original SSLeay License
    -----------------------

  /* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
   * All rights reserved.
   *
   * This package is an SSL implementation written
   * by Eric Young (eay@cryptsoft.com).
   * The implementation was written so as to conform with
Netscapes SSL.
   *
   * This library is free for commercial and non-commercial
use as long as
   * the following conditions are aheared to.  The following
conditions
   * apply to all code found in this distribution, be it the
RC4, RSA,
   * lhash, DES, etc., code; not just the SSL code.  The SSL
documentation
   * included with this distribution is covered by the same
copyright terms
   * except that the holder is Tim Hudson
(tjh@cryptsoft.com).
   *
   * Copyright remains Eric Young's, and as such any
Copyright notices in
```

```
    * the code are not to be removed.
    * If this package is used in a product, Eric Young should
be given attribution
    * as the author of the parts of the library used.
    * This can be in the form of a textual message at program
startup or
    * in documentation (online or textual) provided with the
package.
    *
    * Redistribution and use in source and binary forms, with
or without
    * modification, are permitted provided that the following
conditions
    * are met:
    * 1. Redistributions of source code must retain the
copyright
    *    notice, this list of conditions and the following
disclaimer.
    * 2. Redistributions in binary form must reproduce the
above copyright
    *    notice, this list of conditions and the following
disclaimer in the
    *    documentation and/or other materials provided with
the distribution.
    * 3. All advertising materials mentioning features or use
of this software
    *    must display the following acknowledgement:
    *    "This product includes cryptographic software
written by
    *     Eric Young (eay@cryptsoft.com)"
    *    The word 'cryptographic' can be left out if the
rouines from the library
    *    being used are not cryptographic related :-).
    * 4. If you include any Windows specific code (or a
derivative thereof) from
    *    the apps directory (application code) you must
include an
acknowledgement:
    *    "This product includes software written by Tim
Hudson
(tjh@cryptsoft.com)"
    *
    * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
    * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
```

```
LIMITED TO, THE
     * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
     * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR
CONTRIBUTORS BE LIABLE
     * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL
     * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
     * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
     * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
IN CONTRACT, STRICT
     * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY
     * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
     * SUCH DAMAGE.
     *
     * The licence and distribution terms for any publically
available version or
     * derivative of this code cannot be changed.  i.e. this
code cannot simply be
     * copied and put under another distribution licence
     * [including the GNU Public Licence.]
     */
```

libpng

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~

libpng (http://www.libpng.org/pub/png/libpng.html)



  """""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
""""""""""""""""
     libpng version 1.2.40 - September 10, 2009
      Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson
      Copyright (c) 1996-1997 Andreas Dilger
      Copyright (c) 1995-1996 Guy Eric Schalnat, Group 42,
```

```
Inc.


    """"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
    """"""""""""""""


    /*
     * COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:
     *
     * If you modify libpng you may insert additional notices
immediately following
     * this sentence.
     *
     * libpng versions 1.2.6, August 15, 2004, through 1.2.40,
September 10, 2009, are
     * Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson,
and are
     * distributed according to the same disclaimer and
license as libpng-1.2.5
     * with the following individual added to the list of
Contributing Authors:
     *
     *    Cosmin Truta
     *
     * libpng versions 1.0.7, July 1, 2000, through 1.2.5,
October 3, 2002, are
     * Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are
     * distributed according to the same disclaimer and
license as libpng-1.0.6
     * with the following individuals added to the list of
Contributing Authors:
     *
     *    Simon-Pierre Cadieux
     *    Eric S. Raymond
     *    Gilles Vollant
     *
     * and with the following additions to the disclaimer:
     *
     *    There is no warranty against interference with your
enjoyment of the
     *    library or against infringement.  There is no
warranty that our
     *    efforts or the library will fulfill any of your
particular purposes
```

```
     *     or needs.  This library is provided with all faults,
and the entire
     *     risk of satisfactory quality, performance, accuracy,
and effort is with
     *     the user.
     *
     * libpng versions 0.97, January 1998, through 1.0.6,
March 20, 2000, are
     * Copyright (c) 1998, 1999, 2000 Glenn Randers-Pehrson,
and are
     * distributed according to the same disclaimer and
license as libpng-0.96,
     * with the following individuals added to the list of
Contributing Authors:
     *
     *     Tom Lane
     *     Glenn Randers-Pehrson
     *     Willem van Schaik
     *
     * libpng versions 0.89, June 1996, through 0.96, May
1997, are
     * Copyright (c) 1996, 1997 Andreas Dilger
     * Distributed according to the same disclaimer and
license as libpng-0.88,
     * with the following individuals added to the list of
Contributing Authors:
     *
     *     John Bowler
     *     Kevin Bracey
     *     Sam Bushell
     *     Magnus Holmgren
     *     Greg Roelofs
     *     Tom Tanner
     *
     * libpng versions 0.5, May 1995, through 0.88, January
1996, are
     * Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42,
Inc.
     *
     * For the purposes of this copyright and license,
"Contributing Authors"
     * is defined as the following set of individuals:
     *
     *     Andreas Dilger
```

```
    *     Dave Martindale
    *     Guy Eric Schalnat
    *     Paul Schmidt
    *     Tim Wegner
    *
    * The PNG Reference Library is supplied "AS IS".  The
Contributing Authors
    * and Group 42, Inc. disclaim all warranties, expressed
or implied,
    * including, without limitation, the warranties of
merchantability and of
    * fitness for any purpose.  The Contributing Authors and
Group 42, Inc.
    * assume no liability for direct, indirect, incidental,
special, exemplary,
    * or consequential damages, which may result from the use
of the PNG
    * Reference Library, even if advised of the possibility
of such damage.
    *
    * Permission is hereby granted to use, copy, modify, and
distribute this
    * source code, or portions hereof, for any purpose,
without fee, subject
    * to the following restrictions:
    *
    * 1. The origin of this source code must not be
misrepresented.
    *
    * 2. Altered versions must be plainly marked as such and
    * must not be misrepresented as being the original
source.
    *
    * 3. This Copyright notice may not be removed or altered
from
    *     any source or altered source distribution.
    *
    * The Contributing Authors and Group 42, Inc.
specifically permit, without
    * fee, and encourage the use of this source code as a
component to
    * supporting the PNG file format in commercial products.
If you use this
    * source code in a product, acknowledgment is not
```

```
required but would be
    * appreciated.
    */
```

libsnmp

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~

libsnmp from Net-SNMP

   Various copyrights apply to this package, listed in
various separate parts
   below.  Please make sure that you read all the parts.

   ---- Part 1: CMU/UCD copyright notice: (BSD like) -----


         Copyright 1989, 1991, 1992 by Carnegie Mellon
University

          Derivative Work - 1996, 1998-2000
   Copyright 1996, 1998-2000 The Regents of the University of
California

              All Rights Reserved

   Permission to use, copy, modify and distribute this
software and its
   documentation for any purpose and without fee is hereby
granted,
   provided that the above copyright notice appears in all
copies and
   that both that copyright notice and this permission notice
appear in
   supporting documentation, and that the name of CMU and The
Regents of
   the University of California not be used in advertising or
publicity
   pertaining to distribution of the software without
specific written
   permission.

   CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
```

```
DISCLAIM ALL
    WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL
IMPLIED
    WARRANTIES OF MERCHANTABILITY AND FITNESS.  IN NO EVENT
SHALL CMU OR
    THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR
ANY SPECIAL,
    INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING
    FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF
    CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN
    CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.


    ---- Part 2: Networks Associates Technology, Inc copyright
notice (BSD) -----

    Copyright (c) 2001-2003, Networks Associates Technology,
Inc
    All rights reserved.

    Redistribution and use in source and binary forms, with or
without
    modification, are permitted provided that the following
conditions are met:

    *  Redistributions of source code must retain the above
copyright notice,
       this list of conditions and the following disclaimer.

    *  Redistributions in binary form must reproduce the above
copyright
       notice, this list of conditions and the following
disclaimer in the
       documentation and/or other materials provided with the
distribution.

    *  Neither the name of the Networks Associates Technology,
Inc nor the
       names of its contributors may be used to endorse or
promote
       products derived from this software without specific
```

```
prior written
      permission.

   THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS ``AS
   IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
NOT LIMITED TO,
   THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR
   PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR
   CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL,
   EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO,
   PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS;
   OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
OF LIABILITY,
   WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR
   OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF
   ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

   ---- Part 3: Cambridge Broadband Ltd. copyright notice
(BSD) -----

   Portions of this code are copyright (c) 2001-2003,
Cambridge Broadband Ltd.
   All rights reserved.

   Redistribution and use in source and binary forms, with or
without
   modification, are permitted provided that the following
conditions are met:

   *  Redistributions of source code must retain the above
copyright notice,
      this list of conditions and the following disclaimer.

   *  Redistributions in binary form must reproduce the above
copyright
      notice, this list of conditions and the following
```

```
disclaimer in the
      documentation and/or other materials provided with the
distribution.

   *  The name of Cambridge Broadband Ltd. may not be used to
endorse or
      promote products derived from this software without
specific prior
      written permission.

   THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS
IS'' AND ANY
   EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
   IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
   PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
HOLDER BE
   LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR
   CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF
   SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR
   BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
   WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE
   OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN
   IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.


   ---- Part 4: Sun Microsystems, Inc. copyright notice (BSD)
-----

   Copyright ^(c) 2003 Sun Microsystems, Inc., 4150 Network
Circle, Santa Clara,
   California 95054, U.S.A. All rights reserved.

   Use is subject to license terms below.

   This distribution may include materials developed by third
parties.
```

```
    Sun, Sun Microsystems, the Sun logo and Solaris are
trademarks or registered
    trademarks of Sun Microsystems, Inc. in the U.S. and other
countries.

    Redistribution and use in source and binary forms, with or
without
    modification, are permitted provided that the following
conditions are met:

    *  Redistributions of source code must retain the above
copyright notice,
       this list of conditions and the following disclaimer.

    *  Redistributions in binary form must reproduce the above
copyright
       notice, this list of conditions and the following
disclaimer in the
       documentation and/or other materials provided with the
distribution.

    *  Neither the name of the Sun Microsystems, Inc. nor the
       names of its contributors may be used to endorse or
promote
       products derived from this software without specific
prior written
       permission.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS ``AS
    IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
NOT LIMITED TO,
    THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR
    PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR
    CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL,
    EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO,
    PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS;
    OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
```

```
OF LIABILITY,
    WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR
    OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF
    ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

    ---- Part 5: Sparta, Inc copyright notice (BSD) -----

    Copyright (c) 2003-2008, Sparta, Inc
    All rights reserved.

    Redistribution and use in source and binary forms, with or
without
    modification, are permitted provided that the following
conditions are met:

    *  Redistributions of source code must retain the above
copyright notice,
       this list of conditions and the following disclaimer.

    *  Redistributions in binary form must reproduce the above
copyright
       notice, this list of conditions and the following
disclaimer in the
       documentation and/or other materials provided with the
distribution.

    *  Neither the name of Sparta, Inc nor the names of its
contributors may
       be used to endorse or promote products derived from
this software
       without specific prior written permission.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS ``AS
    IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
NOT LIMITED TO,
    THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR
    PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR
    CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL,
```

```
    EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO,
    PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS;
    OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
OF LIABILITY,
    WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR
    OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF
    ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

    ---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

    Copyright (c) 2004, Cisco, Inc and Information Network
    Center of Beijing University of Posts and
Telecommunications.
    All rights reserved.

    Redistribution and use in source and binary forms, with or
without
    modification, are permitted provided that the following
conditions are met:

    *  Redistributions of source code must retain the above
copyright notice,
        this list of conditions and the following disclaimer.

    *  Redistributions in binary form must reproduce the above
copyright
        notice, this list of conditions and the following
disclaimer in the
        documentation and/or other materials provided with the
distribution.

    *  Neither the name of Cisco, Inc, Beijing University of
Posts and
        Telecommunications, nor the names of their contributors
may
        be used to endorse or promote products derived from
this software
        without specific prior written permission.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
```

```
CONTRIBUTORS ``AS
    IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
NOT LIMITED TO,
    THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR
    PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR
    CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL,
    EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO,
    PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS;
    OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
OF LIABILITY,
    WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR
    OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF
    ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

    ---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright
notice (BSD) -----

    Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
    oss@fabasoft.com
    Author: Bernhard Penz <bernhard.penz@fabasoft.com>

    Redistribution and use in source and binary forms, with or
without
    modification, are permitted provided that the following
conditions are met:

    *  Redistributions of source code must retain the above
copyright notice,
       this list of conditions and the following disclaimer.

    *  Redistributions in binary form must reproduce the above
copyright
       notice, this list of conditions and the following
disclaimer in the
       documentation and/or other materials provided with the
distribution.
```

```
    *   The name of Fabasoft R&D Software GmbH & Co KG or any
of its subsidiaries,
       brand or product names may not be used to endorse or
promote products
       derived from this software without specific prior
written permission.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS
IS'' AND ANY
    EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
    IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
    PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
HOLDER BE
    LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR
    CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF
    SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR
    BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
    WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE
    OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN
    IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

miglayout

```
Copyright (c) 2004, Mikael Grev, MiG InfoCom AB. (miglayout
(at) miginfocom (dot) com)
All rights reserved.

Redistribution and use in source and binary forms, with or
without modification, are permitted
provided that the following conditions are met:
Redistributions of source code must retain the above
copyright notice, this list of conditions
and the following disclaimer.
Redistributions in binary form must reproduce the above
```

```
copyright notice, this list of conditions
and the following disclaimer in the documentation and/or
other materials provided with the
distribution. Neither the name of the MiG InfoCom AB nor the
names of its contributors may be
used to endorse or promote products derived from this
software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER
OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY
OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

postgresql

```
PostgreSQL Database Management System
(formerly known as Postgres, then as Postgres95)

Portions Copyright (c) 1996-2006, PostgreSQL Global
Development Group

Portions Copyright (c) 1994, The Regents of the University of
California

Permission to use, copy, modify, and distribute this software
and its
```

```
documentation for any purpose, without fee, and without a
written agreement
is hereby granted, provided that the above copyright notice
and this
paragraph and the following two paragraphs appear in all
copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO
ANY PARTY FOR
DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL
DAMAGES, INCLUDING
LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS
DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN
ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY
WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE.  THE SOFTWARE PROVIDED
HEREUNDER IS
ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO
OBLIGATIONS TO
PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.
```

psycopg

```
psycopg and the GPL
===================

psycopg is free software; you can redistribute it and/or
modify
it under the terms of the GNU General Public License as
published by
the Free Software Foundation; either version 2 of the
License, or
(at your option) any later version. See file COPYING for
details.

As a special exception, specific permission is granted for
the GPLed
```

```
code in this distribution to be linked to OpenSSL and
PostgreSQL libpq
without invoking GPL clause 2(b).

Note that the GPL was chosen to avoid proprietary adapters
based on
psycopg code. Using psycopg in a proprietary product (even
bundling
psycopg with the proprietary product) is fine as long as:

 1. psycopg is called from Python only using only the
provided API
     (i.e., no linking with C code and no C modules based on
it); and

 2. all the other points of the GPL are respected (you offer
a copy
     of psycopg's source code, and so on.)

Alternative licenses
=====================

If you prefer you can use the Zope Database Adapter
ZPsycopgDA (i.e.,
every file inside the ZPsycopgDA directory) user the ZPL
license as
published on the Zope web site,
http://www.zope.org/Resources/ZPL.

Also, the following BSD-like license applies (at your option)
to the
files following the pattern psycopg/adapter*.{h,c} and
psycopg/microprotocol*.{h,c}:

 Permission is granted to anyone to use this software for any
purpose,
 including commercial applications, and to alter it and
redistribute it
 freely, subject to the following restrictions:

 1. The origin of this software must not be misrepresented;
you must not
     claim that you wrote the original software. If you use
this
```

```
      software in a product, an acknowledgment in the product
documentation
      would be appreciated but is not required.

 2. Altered source versions must be plainly marked as such,
and must not
      be misrepresented as being the original software.

 3. This notice may not be removed or altered from any source
distribution.

psycopg is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty
of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

Proprietary licenses
====================

A non-exclusive license is available for companies that want
to include
psycopg in their proprietary products without respecting the
spirit of the
GPL. The price of the license is one day of development done
by the author,
at the consulting fee he applies to his usual customers at
the day of the
request.
```

pyASN.1

```
Copyright (c) 2005, 2006 Ilya Etingof <ilya@glas.net>, all
rights reserved.

THIS
SOFTWARE IS NOT FAULT TOLERANT AND SHOULD NOT BE USED IN ANY
SITUATION
ENDANGERING HUMAN
LIFE OR PROPERTY.

Redistribution and use in source and binary forms, with or
without
```

```
modification, are permitted provided that the following
conditions are met:

   *
Redistributions of source code must retain the above
copyright notice,
     this list of
conditions and the following disclaimer.

   * Redistributions in binary form must
reproduce the above copyright notice,
     this list of conditions and the following
disclaimer in the documentation
     and/or other materials provided with the
distribution.

   * The name of the authors may not be used to endorse or
promote
products
     derived from this software without specific prior written
permission.

THIS
SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS ``AS IS''
AND ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL
THE REGENTS OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR
TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF
THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

pycrypto

```
===============================================================
======
Distribute and use freely; there are no restrictions on
further
dissemination and usage except those imposed by the laws of
your
country of residence.  This software is provided "as is"
without
warranty of fitness for use or suitability for any purpose,
express
or implied. Use at your own risk or not at all.

===============================================================
======

Incorporating the code into commercial products is permitted;
you do
not have to make source available or contribute your changes
back
(though that would be nice).

--amk
    (www.amk.ca)
```

pyopenssl

```
pyopenssl  is released under the GNU Lesser General Public
License.
```

pyparsing

```
# Copyright (c) 2003-2006  Paul T. McGuire
#
# Permission is hereby granted, free of charge, to any person
obtaining
# a copy of this software and associated documentation files
(the
# "Software"), to deal in the Software without restriction,
```

```
including
# without limitation the rights to use, copy, modify, merge,
publish,
# distribute, sublicense, and/or sell copies of the Software,
and to
# permit persons to whom the Software is furnished to do so,
subject to
# the following conditions:
#
# The above copyright notice and this permission notice shall
be
# included in all copies or substantial portions of the
Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY
KIND,
# EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
WARRANTIES OF
# MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT.
# IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY
# CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT,
# TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

pyrad

```
Copyright 2002-2006 Wichert Akkerman. All rights reserved.

All rights reserved.

Redistribution and use in source and binary forms, with or
without
modification, are permitted provided that the following
conditions
are met:

1. Redistributions of source code must retain the above
copyright
    notice, this list of conditions and the following
```

```
disclaimer.
2. Redistributions in binary form must reproduce the above
copyright
    notice, this list of conditions and the following
disclaimer in the
    documentation and/or other materials provided with the
distribution.
3. Neither the name of the University nor the names of its
contributors
    may be used to endorse or promote products derived from
this software
    without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS
``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR
CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
SUCH DAMAGE.
```

pysqlite

```
Copyright (c) 2004 Gerhard Häring

This software is provided 'as-is', without any express or
implied warranty. In
no event will the authors be held liable for any damages
arising from the use
of this software.
```

```
Permission is granted to anyone to use this software for any
purpose,
including commercial applications, and to alter it and
redistribute it freely,
subject to the following restrictions:

    1. The origin of this software must not be
misrepresented; you must not
        claim that you wrote the original software. If you use
this software in
        a product, an acknowledgment in the product
documentation would be
        appreciated but is not required.

    2. Altered source versions must be plainly marked as
such, and must not be
        misrepresented as being the original software.

    3. This notice may not be removed or altered from any
source distribution.
```

python

```
A. HISTORY OF THE SOFTWARE
==========================

Python was created in the early 1990s by Guido van Rossum at
Stichting
Mathematisch Centrum (CWI, see http://www.cwi.nl) in the
Netherlands
as a successor of a language called ABC.  Guido remains
Python's
principal author, although it includes many contributions
from others.

In 1995, Guido continued his work on Python at the
Corporation for
National Research Initiatives (CNRI, see
http://www.cnri.reston.va.us)
in Reston, Virginia where he released several versions of the
software.
```

```
In May 2000, Guido and the Python core development team moved
to
BeOpen.com to form the BeOpen PythonLabs team.  In October of
the same
year, the PythonLabs team moved to Digital Creations (now
Zope
Corporation, see http://www.zope.com).  In 2001, the Python
Software
Foundation (PSF, see http://www.python.org/psf/) was formed,
a
non-profit organization created specifically to own Python-
related
Intellectual Property.  Zope Corporation is a sponsoring
member of
the PSF.

All Python releases are Open Source (see
http://www.opensource.org for
the Open Source Definition).  Historically, most, but not
all, Python
releases have also been GPL-compatible; the table below
summarizes
the various releases.

    Release            Derived      Year          Owner        GPL-
                       from
compatible? (1)

    0.9.0 thru 1.2                  1991-1995     CWI          yes
    1.3 thru 1.5.2   1.2            1995-1999     CNRI         yes
    1.6              1.5.2          2000          CNRI         no
    2.0              1.6            2000          BeOpen.com   no
    1.6.1            1.6            2001          CNRI         yes
(2)
    2.1              2.0+1.6.1      2001          PSF          no
    2.0.1            2.0+1.6.1      2001          PSF          yes
    2.1.1            2.1+2.0.1      2001          PSF          yes
    2.2              2.1.1          2001          PSF          yes
    2.1.2            2.1.1          2002          PSF          yes
    2.1.3            2.1.2          2002          PSF          yes
    2.2.1            2.2            2002          PSF          yes
    2.2.2            2.2.1          2002          PSF          yes
    2.2.3            2.2.2          2003          PSF          yes
    2.3              2.2.2          2002-2003     PSF          yes
```

```
     2.3.1               2.3        2002-2003   PSF          yes
     2.3.2               2.3.1      2002-2003   PSF          yes
     2.3.3               2.3.2      2002-2003   PSF          yes
     2.3.4               2.3.3      2004        PSF          yes
     2.3.5               2.3.4      2005        PSF          yes
     2.4                 2.3        2004        PSF          yes
     2.4.1               2.4.1      2005        PSF          yes
     2.4.2               2.4.1      2005        PSF          yes
     2.4.3               2.4.2      2006        PSF          yes
     2.4.4               2.4.3      2006        PSF          yes
     2.5                 2.4        2006        PSF          yes


Footnotes:

(1) GPL-compatible doesn't mean that we're distributing
Python under
    the GPL.  All Python licenses, unlike the GPL, let you
distribute
    a modified version without making your changes open
source.  The
    GPL-compatible licenses make it possible to combine
Python with
    other software that is released under the GPL; the others
don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-
compatible,
    because its license has a choice of law clause.
According to
    CNRI, however, Stallman's lawyer has told CNRI's lawyer
that 1.6.1
    is "not incompatible" with the GPL.


Thanks to the many outside volunteers who have worked under
Guido's
direction to make these releases possible.



B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING
PYTHON


================================================================
==
```

```
PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
--------------------------------------------

1. This LICENSE AGREEMENT is between the Python Software
Foundation
("PSF"), and the Individual or Organization ("Licensee")
accessing
and
otherwise using this software ("Python") in source or binary
form and
its associated documentation.

2. Subject to the terms and conditions of this License
Agreement, PSF
hereby grants Licensee a nonexclusive, royalty-free, world-
wide
license to reproduce, analyze, test, perform and/or display
publicly,
prepare derivative works, distribute, and otherwise use
Python
alone or in any derivative version, provided, however, that
PSF's
License Agreement and PSF's notice of copyright, i.e.,
"Copyright (c)
2001, 2002, 2003, 2004, 2005, 2006 Python Software
Foundation; All Rights
Reserved" are retained in Python alone or in any derivative
version
prepared by Licensee.

3. In the event Licensee prepares a derivative work that is
based on
or incorporates Python or any part thereof, and wants to make
the derivative work available to others as provided herein,
then
Licensee hereby agrees to include in any such work a brief
summary of
the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS"
basis.  PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS
OR
IMPLIED.  BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO
AND
```

```
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY
OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF
PYTHON
FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS
AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING
PYTHON,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY
THEREOF.

6. This License Agreement will automatically terminate upon a
material
breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to
create any
relationship of agency, partnership, or joint venture between
PSF and
Licensee.  This License Agreement does not grant permission
to use PSF
trademarks or trade name in a trademark sense to endorse or
promote
products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee
agrees to be bound by the terms and conditions of this
License
Agreement.


BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0
-------------------------------------------

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"),
having an
office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the
Individual or Organization ("Licensee") accessing and
otherwise using
```

```
this software in source or binary form and its associated
documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python
License
Agreement, BeOpen hereby grants Licensee a non-exclusive,
royalty-free, world-wide license to reproduce, analyze, test,
perform
and/or display publicly, prepare derivative works,
distribute, and
otherwise use the Software alone or in any derivative
version,
provided, however, that the BeOpen Python License is retained
in the
Software, alone or in any derivative version prepared by
Licensee.

3. BeOpen is making the Software available to Licensee on an
"AS IS"
basis.  BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES,
EXPRESS OR
IMPLIED.  BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES
NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY
OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE
WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS
OF THE
SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL
DAMAGES OR LOSS
AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE,
OR ANY
DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY
THEREOF.

5. This License Agreement will automatically terminate upon a
material
breach of its terms and conditions.

6. This License Agreement shall be governed by and
interpreted in all
```

```
respects by the law of the State of California, excluding
conflict of
law provisions.  Nothing in this License Agreement shall be
deemed to
create any relationship of agency, partnership, or joint
venture
between BeOpen and Licensee.  This License Agreement does not
grant
permission to use BeOpen trademarks or trade names in a
trademark
sense to endorse or promote products or services of Licensee,
or any
third party.  As an exception, the "BeOpen Python" logos
available at
http://www.pythonlabs.com/logos.html may be used according to
the
permissions granted on that web page.

7. By copying, installing or otherwise using the software,
Licensee
agrees to be bound by the terms and conditions of this
License
Agreement.


CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
---------------------------------------

1. This LICENSE AGREEMENT is between the Corporation for
National
Research Initiatives, having an office at 1895 Preston White
Drive,
Reston, VA 20191 ("CNRI"), and the Individual or Organization
("Licensee") accessing and otherwise using Python 1.6.1
software in
source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License
Agreement, CNRI
hereby grants Licensee a nonexclusive, royalty-free, world-
wide
license to reproduce, analyze, test, perform and/or display
publicly,
prepare derivative works, distribute, and otherwise use
```

```
Python 1.6.1
alone or in any derivative version, provided, however, that
CNRI's
License Agreement and CNRI's notice of copyright, i.e.,
"Copyright (c)
1995-2001 Corporation for National Research Initiatives; All
Rights
Reserved" are retained in Python 1.6.1 alone or in any
derivative
version prepared by Licensee.  Alternately, in lieu of CNRI's
License
Agreement, Licensee may substitute the following text
(omitting the
quotes): "Python 1.6.1 is made available subject to the terms
and
conditions in CNRI's License Agreement.  This Agreement
together with
Python 1.6.1 may be located on the Internet using the
following
unique, persistent identifier (known as a handle):
1895.22/1013.  This
Agreement may also be obtained from a proxy server on the
Internet
using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is
based on
or incorporates Python 1.6.1 or any part thereof, and wants
to make
the derivative work available to others as provided herein,
then
Licensee hereby agrees to include in any such work a brief
summary of
the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an
"AS IS"
basis.  CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS
OR
IMPLIED.  BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES
NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY
OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1
```

```
WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF
PYTHON
1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES
OR LOSS AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING
PYTHON 1.6.1,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY
THEREOF.

6. This License Agreement will automatically terminate upon a
material
breach of its terms and conditions.

7. This License Agreement shall be governed by the federal
intellectual property law of the United States, including
without
limitation the federal copyright law, and, to the extent such
U.S. federal law does not apply, by the law of the
Commonwealth of
Virginia, excluding Virginia's conflict of law provisions.
Notwithstanding the foregoing, with regard to derivative
works based
on Python 1.6.1 that incorporate non-separable material that
was
previously distributed under the GNU General Public License
(GPL), the
law of the Commonwealth of Virginia shall govern this License
Agreement only as to issues arising under or with respect to
Paragraphs 4, 5, and 7 of this License Agreement.  Nothing in
this
License Agreement shall be deemed to create any relationship
of
agency, partnership, or joint venture between CNRI and
Licensee.  This
License Agreement does not grant permission to use CNRI
trademarks or
trade name in a trademark sense to endorse or promote
products or
services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by
```

```
copying,
installing or otherwise using Python 1.6.1, Licensee agrees
to be
bound by the terms and conditions of this License Agreement.

        ACCEPT


CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2
--------------------------------------------------------

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum
Amsterdam,
The Netherlands.  All rights reserved.

Permission to use, copy, modify, and distribute this software
and its
documentation for any purpose and without fee is hereby
granted,
provided that the above copyright notice appear in all copies
and that
both that copyright notice and this permission notice appear
in
supporting documentation, and that the name of Stichting
Mathematisch
Centrum or CWI not be used in advertising or publicity
pertaining to
distribution of the software without specific, written prior
permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH
REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE
LIABLE
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY
DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,
ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.
```

spidermonkey

The Mozilla Foundation provides overall support for various open source software
projects. SpiderMonkey is the code-name for Mozilla's open source C implementation
of JavaScript. In some Help/Systems Inc. products, Help/Systems Inc.uses a modified
version of the open source SpiderMonkey code. Use of that source is subject
to the Mozilla Public License Version 1.1 (the License). You may obtain a copy
of the License on the Mozilla website or in the download files. Visit the Mozilla website
for more details about SpiderMonkey and how to download the source to it.
In compliance with the requirements of the License, Help/Systems Inc. makes the
modified version of the source code available for download: spidermonkey.zip.

sqlite

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~

sqlite (www.sqlite.org)

    The original author of SQLite has dedicated the code to
the public
    domain. Anyone is free to copy, modify, publish, use,
compile, sell,
    or distribute the original SQLite code, either in source
code form
    or as a compiled binary, for any purpose, commercial or
    non-commercial, and by any means.
```

twisted

```
Copyright (c) 2001-2008
Allen Short
Andrew Bennetts
Apple Computer, Inc.
Benjamin Bruheim
Bob Ippolito
Canonical Limited
Christopher Armstrong
David Reid
Donovan Preston
Eric Mangold
Itamar Shtull-Trauring
James Knight
Jason A. Mobarak
Jean-Paul Calderone
Jonathan Lange
Jonathan D. Simms
Jürgen Hermann
Kevin Turner
Mary Gardiner
Matthew Lefkowitz
Massachusetts Institute of Technology
Moshe Zadka
Paul Swartz
Pavel Pergamenshchik
Ralph Meijer
Sean Riley
Software Freedom Conservancy
Travis B. Hartwell
Thomas Herve
Eyal Lotem
Antoine Pitrou
Andy Gayton

Permission is hereby granted, free of charge, to any person
obtaining
a copy of this software and associated documentation files
(the
"Software"), to deal in the Software without restriction,
including
without limitation the rights to use, copy, modify, merge,
```

```
publish,
distribute, sublicense, and/or sell copies of the Software,
and to
permit persons to whom the Software is furnished to do so,
subject to
the following conditions:

The above copyright notice and this permission notice shall
be
included in all copies or substantial portions of the
Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY
KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN
AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

zlib

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~

zlib (www.zlib.net)

   (C) 1995-2004 Jean-loup Gailly and Mark Adler

   This software is provided 'as-is', without any express or
implied
   warranty.  In no event will the authors be held liable for
any damages
   arising from the use of this software.

   Permission is granted to anyone to use this software for
any purpose,
```

```
  including commercial applications, and to alter it and
redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented;
you must not
     claim that you wrote the original software. If you use
this software
     in a product, an acknowledgment in the product
documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such,
and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any
source distribution.


  Jean-loup Gailly        Mark Adler
  jloup@gzip.org          madler@alumni.caltech.edu
```

zopeinterface

```
Zope Public License (ZPL) Version 2.1

A copyright notice accompanies this license document that
identifies
the copyright holders.

This license has been certified as open source. It has also
been
designated as GPL compatible by the Free Software Foundation
(FSF).

Redistribution and use in source and binary forms, with or
without
modification, are permitted provided that the following
conditions are
met:

   1. Redistributions in source code must retain the
accompanying
   copyright notice, this list of conditions, and the
```

```
following
   disclaimer.

   2. Redistributions in binary form must reproduce the
accompanying
   copyright notice, this list of conditions, and the
following
   disclaimer in the documentation and/or other materials
provided with
   the distribution.

   3. Names of the copyright holders must not be used to
endorse or
   promote products derived from this software without prior
written
   permission from the copyright holders.

   4. The right to distribute this software or to use it for
any
   purpose does not give you the right to use Servicemarks
(sm) or
   Trademarks ™ of the copyright holders. Use of them is
covered by
   separate agreement with the copyright holders.

   5. If any files are modified, you must cause the modified
files to
   carry prominent notices stating that you changed the files
and the
   date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS ``AS IS''
AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDERS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
```

```
PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF
THE POSSIBILITY OF SUCH DAMAGE.
```

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 elements as the input focus changes.	Focus is not programmatically exposed in Intermapper
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 (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.	Supports.	X

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. Intermapper allows users to customize the contrast and color settings of the text and background of their document to a wide range of colors supported by their system.	X
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. Intermapper does not have electronic forms capabilities.	N/A

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 and Intermapper Flows. During the trial period, all three are available. Once the trial license expires, you need a license to run Intermapper or Flows.

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.
- **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 works. For additional information, see Try Out the Demo Maps.

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. See the Readme file installed with your version for complete installation instructions.

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 30 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 page.
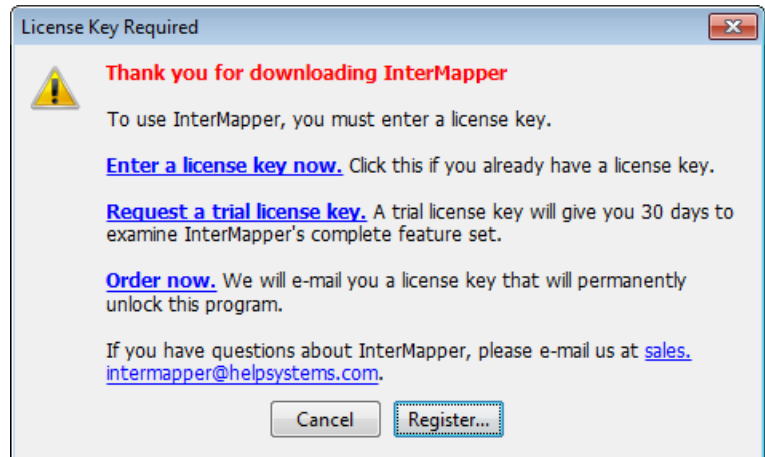
If you don't have a license key, click the *Request a trial license key* link in the window shown above. A form appears, allowing you to enter some information, and request a trial license key. When you click Send Request, a license key appears in the text box. It allows you to use Intermapper to monitor a limited number of devices for 30 days. Click Register to activate the key.

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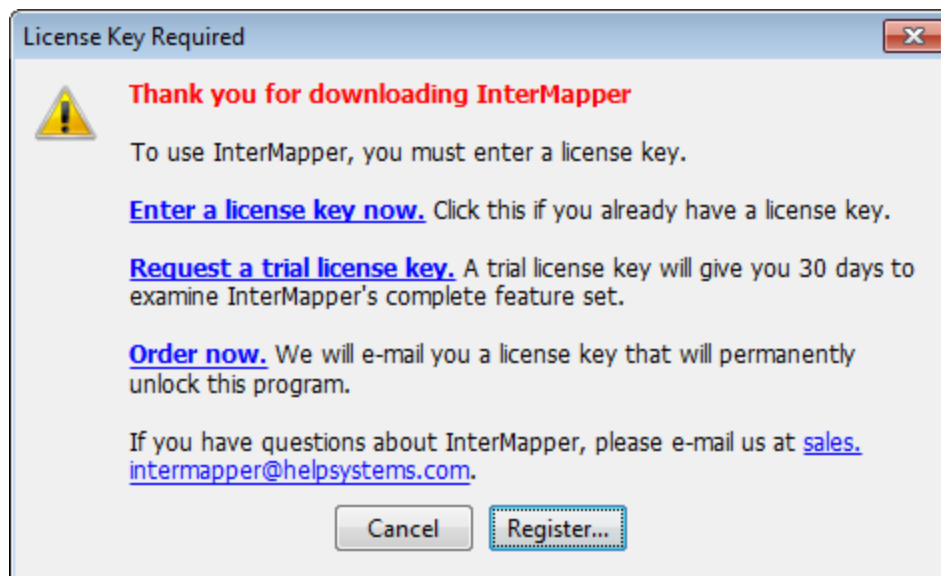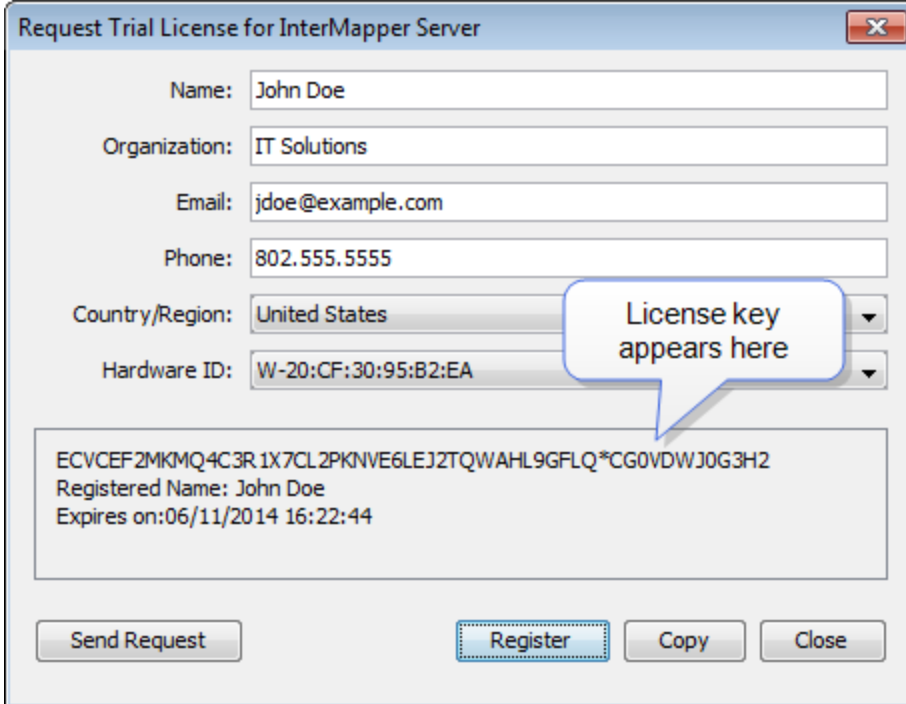
- **Enter license key now** - if you already have a key, click to paste it now.
- **Request a trial license key** - if you don't have a key, click to request one. The Request Trial License window appears as shown below.
- **Order now** - Allows you to purchase the produce.

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:
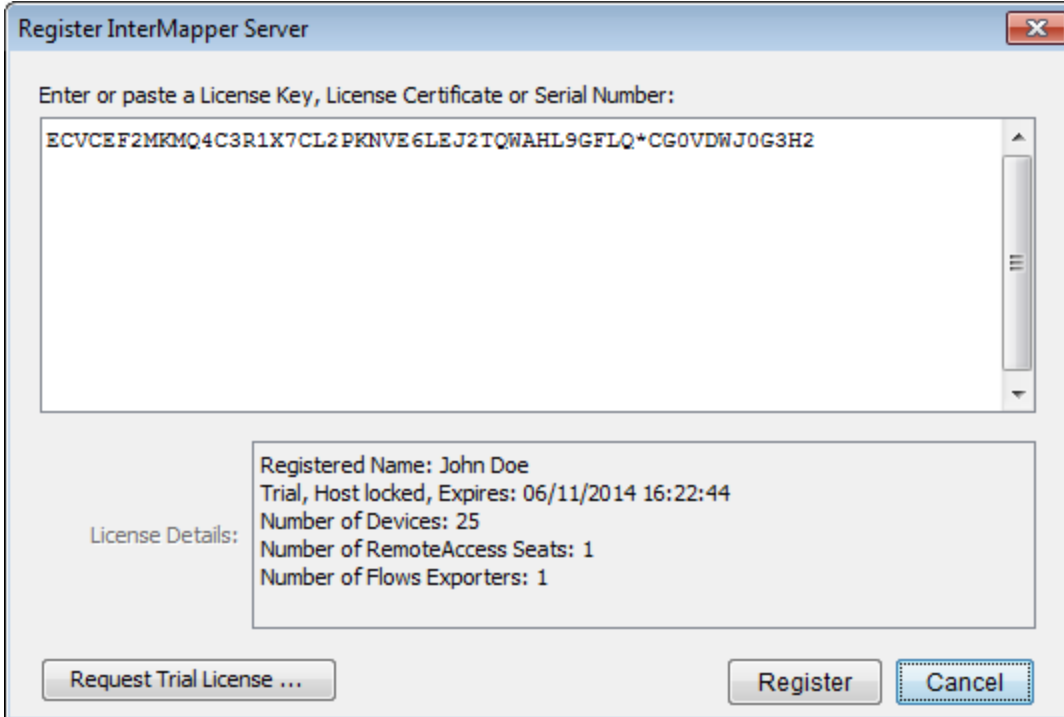
1. Click *Send Request*. Intermapper contacts HelpSystems and retrieves a trial key. The new key appears in the area shown above.

2. Click *Register*. The Register Intermapper window appears as shown:

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.
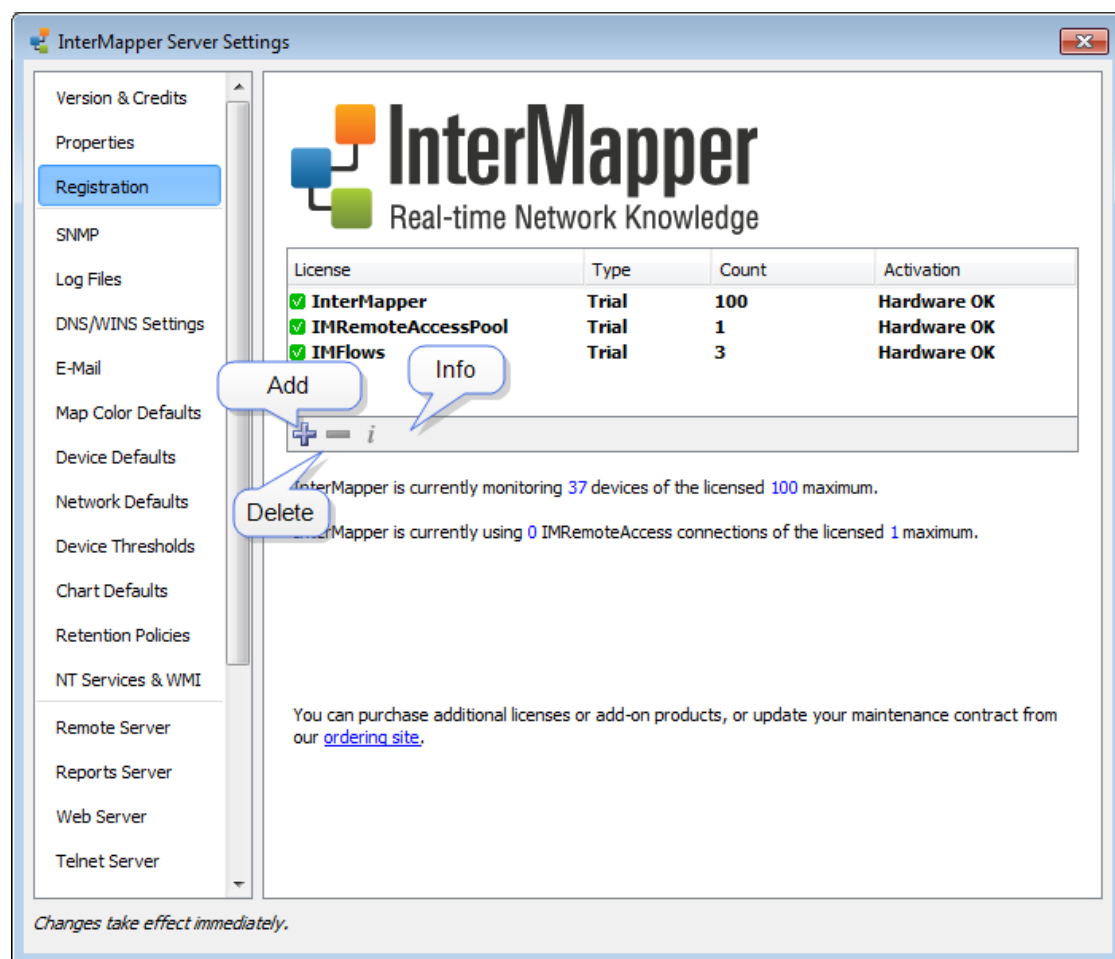
Multiple licenses in Intermapper RemoteAccess

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

Use the Intermapper Control Center to start and stop the Intermapper and Flows servers, as well as do some other basic configuration.

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

On Windows, Intermapper installs an icon in System Tray (lower right corner) that allows the same functions. Click the icon to open the Intermapper Control Center, or right-click it to view a menu similar to the Mac OS X menubar application. You can also view Intermapper's status from either the menu or the Control Center window.

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.
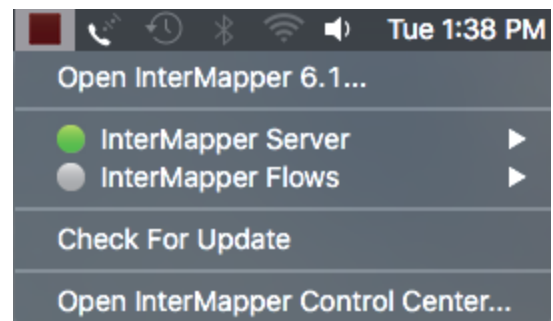
On Windows

- Right-click the system tray icon to view the menu shown above.
- Click the system tray icon to view the Intermapper Control Center, shown below.

The Intermapper Control Center application is available on supported Windows systems.

It has the same function of the MacOS X application, but is called from the Window System Tray (lower right corner of the screen).
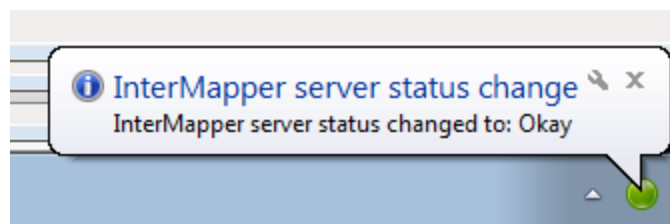
You can do the following from the Intermapper Control Center:

- 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:

- From the Intermapper menu , choose *Open Intermapper Control Center...* The Intermapper Control Center window appears.
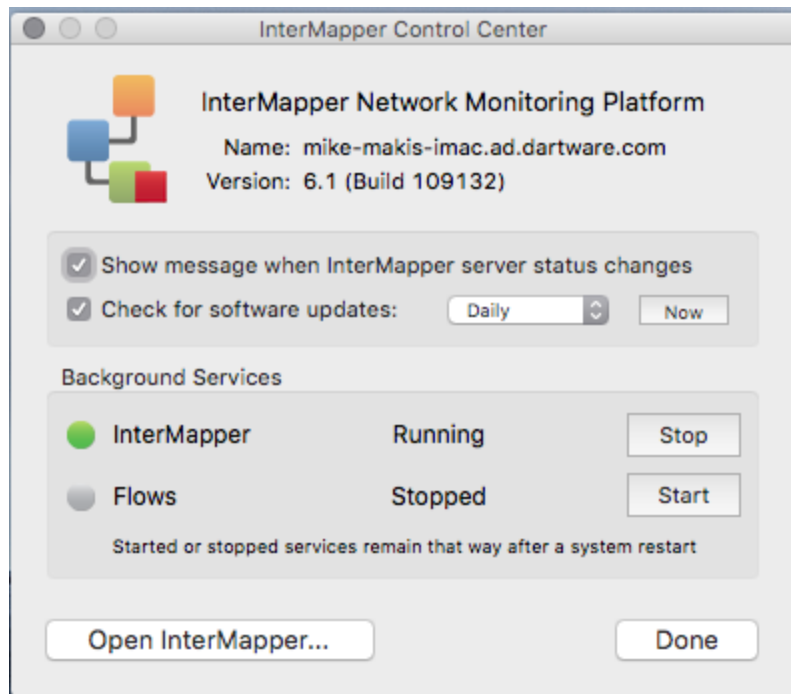
- Right-click the Intermapper Control Center icon in the Windows System Tray and choose *Show Intermapper Control Center*. The Intermapper Control Center window appears.
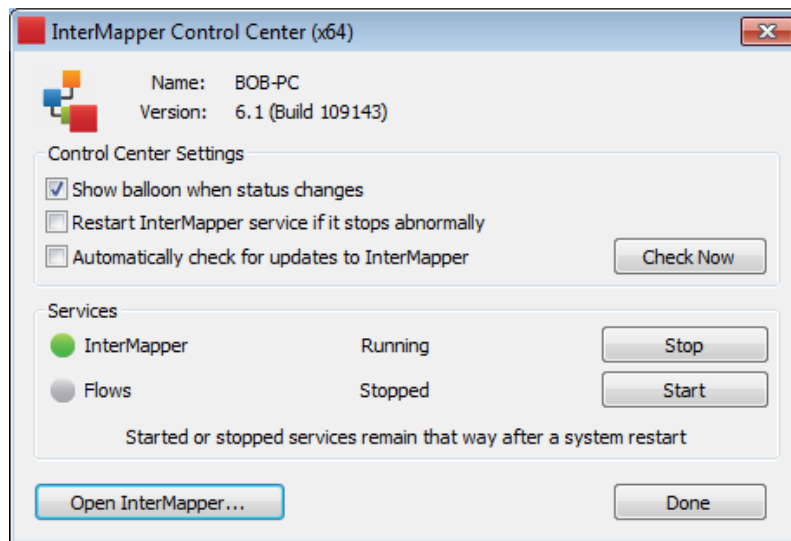
Automatic Notifications of Updates

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.

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 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 thing 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. You can also specify a range of addresses to scan.
     - 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 > Device Notifiers** 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.

Using Intermapper

You experience Intermapper through the Map List Window, where you view a list of available maps. when you open a map, it appears in a Map Window.

If you are using Intermapper RemoteAccess, 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 and by specifying what actions should be taken when you double-click an object on a map. You can also set user preferences for InterMapper and InterMapper RemoteAccess.

Creating Maps

Use this section to find out how to start your map, to use Autodiscovery to find and map each device on your network, and to add devices and networks 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, and can export data from maps for use in spreadsheets and databases.

You can even place a physical map image in the background of your map, and use geographic coordinates as you import to place devices automatically at specific locations in relation to the background image.

Use InterMapper's different probe types 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 and scan them. You can create sub-maps, 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, change the appearance of devices, change the device labels, or add text or a background image. For maps with large switches, you may want to hide some detail. For tips on arranging your map, see Arranging Tips.

Notifiers and Alerts

You can set up devices to alert you to problems 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 and configure them to send an E-mail message, page (through a modem or network), send a text message to a cell phone, or execute a script or

system command. You can also open a WinPopup window on a Windows machine, send an entry to a Syslog server, or send an SNMP trap.

You can attach notifiers in a number of ways:

- For each map, you can define a default set of notifiers to be attached to a device.
- You can attach one or more notifiers to one or more specific devices.
- You can create groups of notifiers and assign them to a device all at once.
- You can attach a notifier to one or more interfaces on a device.

If a device goes down, and other devices are attached to that device, you can set a Vantage Point. 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 for a device, network, or link. You also view and edit a device or network's information from its Info window. For routers, switches, or other devices with interfaces, you can view status or other information about specific ports through the Interfaces window.

You can set thresholds for a number of statistics:

- For devices, you can set thresholds for packet loss or network traffic, 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 that graph one or more data values associated with a device. You can also view a detailed Event log and Outage log to help you troubleshoot problems accurately. You can even create new log files for logging specific data.

If a device or link goes down, you can acknowledge the problem, 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 and save it in the InterMapper Database, through the InterMapper DataCenter. The data can then be retrieved for use in reporting and analysis. You can set policies to specify how much data is retained and how long it is retained.

Server Settings

Use the Server Settings panel to view information about InterMapper, to set preferences, and to configure InterMapper's Remote, Web, Telnet, and Authentication servers. You can also maintain InterMapper's firewall and user list, enable and disable or control access to maps, and create notifiers.

InterMapper Reference

Use the InterMapper Reference to view comprehensive lists of menu commands, details about the available device probes, file and folder locations, and learn advanced data import and export techniques. You can also learn how to use and customize the InterMapper web server, and how to use the InterMapper Telnet server.

Troubleshooting InterMapper

Use the Troubleshooting section to help you learn about IP addresses, Domain Name Servers, SNMP, WINS Names, and view a number of frequently-asked questions.

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. 674).

For information on using the Auto-discover function, see Using Auto-discover (Pg. 132).

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. 674).

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. 437).

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. 674).

For information on using the Auto-discover function, see Using Auto-discover (Pg. 132).

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. 674).

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. 437).

Using Auto-Discover

You can use Auto-Discover to create a new map. Auto-Discover scans your network and creates an IP-based, Layer 3 view of the map.

> **NOTE:** 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 once the devices have been discovered.
>
> For more information, see Mapping With Layer 2.

For existing maps, you will need to use the manual technique for converting the map. For new maps you create with Auto-Discovery, use the automatic technique.

To Auto-Discover to create an initial network map:

1. From the File menu, choose **New...** The New Map Con-structor window appears.

2. Enter a map name and click *Next*.

3. C
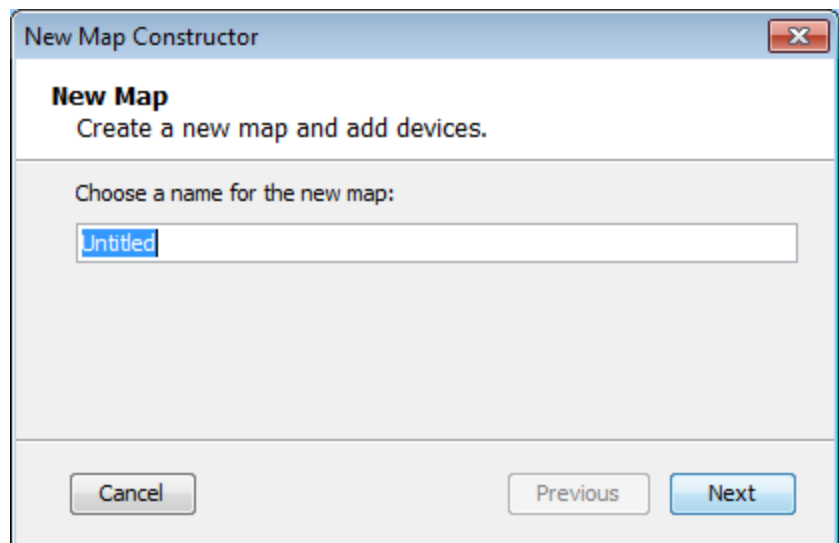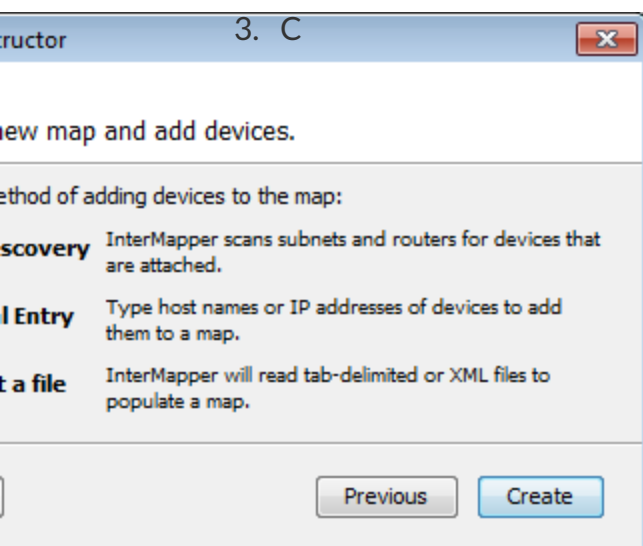
Create. The Automatic Device Discovery window appears, as shown below.

4. In the *Enter a starting host name, or IP address* box, enter the 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 would like to discover a range of addresses, rather than all addresses, enter them in the *Enter an IP address range to discover* box. Use hyphens, wildcards, and CIDR slash notation to specify an IP address range. For more information, see Entering an IP Address Range.

6. If you have SNMP-speaking devices in your network, enter an SNMP Community (Pg. 772) string in the *Specify an SNMP Community* box.

7. Select your *Discovery Options*, as explained in The Auto-Discovery Window (Pg. 134) below.

8. Click the *Filter* button to set a filter for the discovery.

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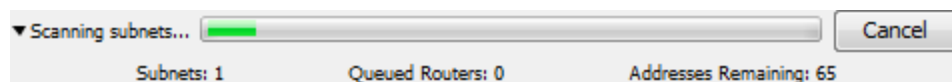
10. As the network is scanned, discovered devices appear in the current map (or in a list if you have cleared the *Automatically Layout* check box.) When *Intermapper* has found all the devices within the specified subnet, the Discovery Status bar disappears.

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.
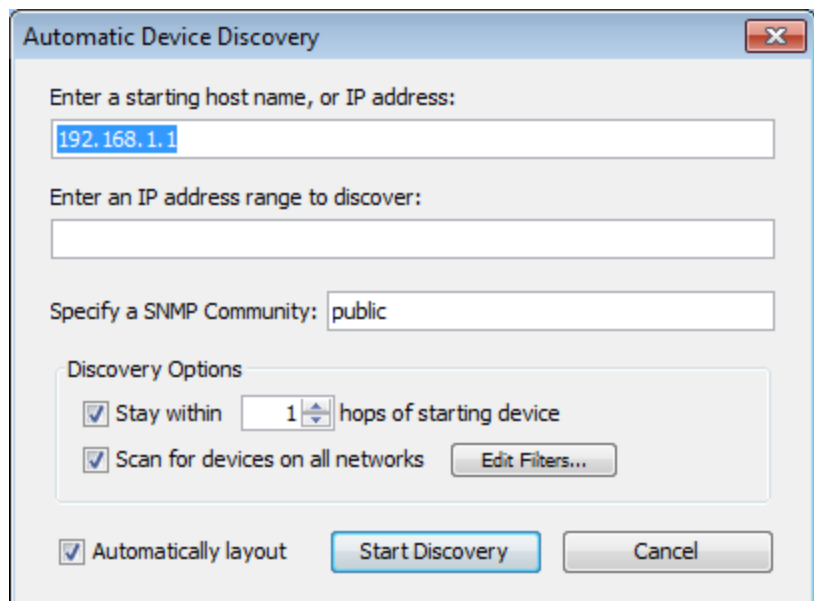
The Automatic Device Discovery Window

You control the starting point, the SNMP Community string (Pg. 772), 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. 770), IP address (Pg. 766), or WINS name (Pg. 776) of a device to use as a starting point for the auto-discovery.

- **IP Address Range** - Use hyphens, wildcards, and CIDR slash notation to specify an IP address range. For more information, see

- 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.
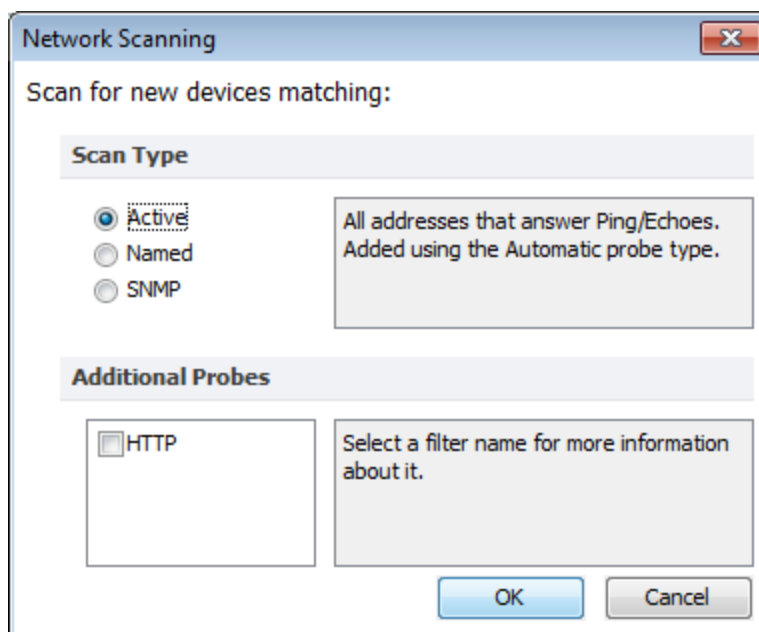
What Happens During Autodiscovery?

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. 770), IP addresses (Pg. 766), IP address ranges, or WINS names (Pg. 776) 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. 674) .

Below is a typical map after autodiscovery has finished.
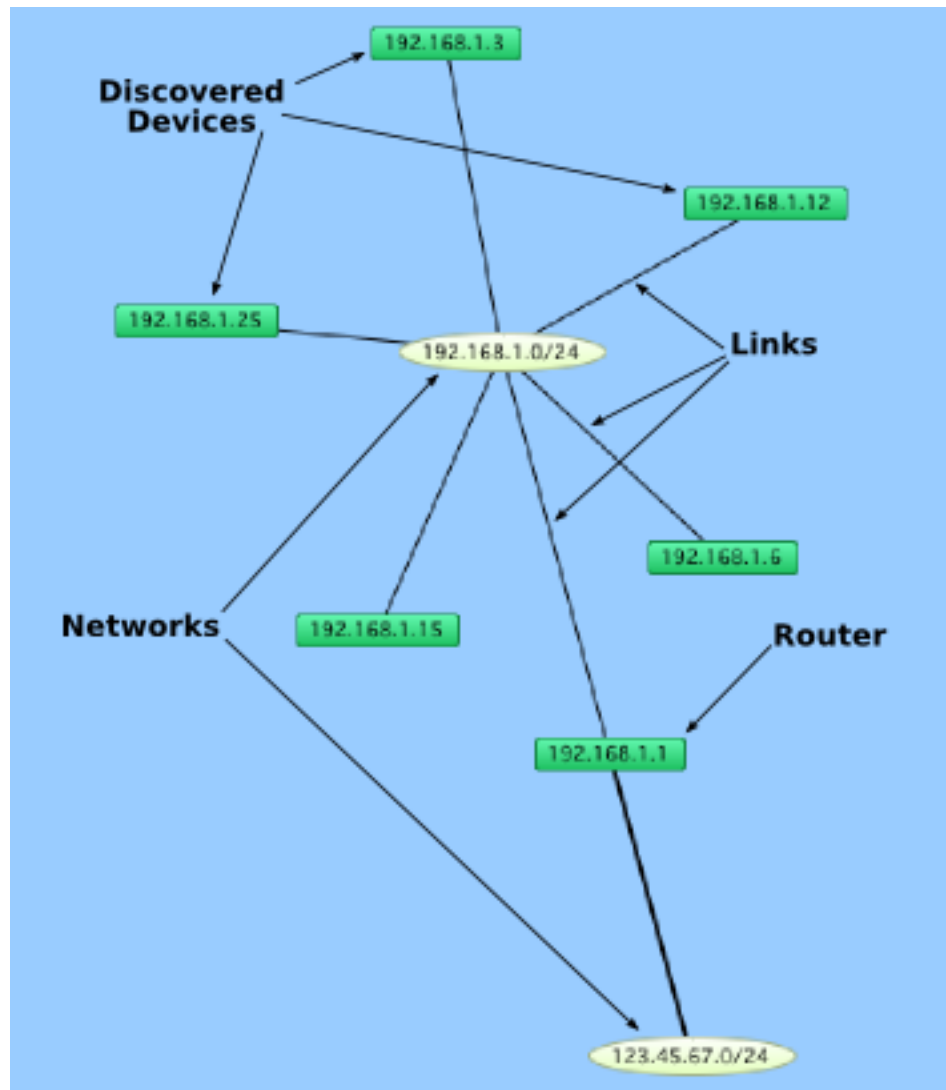
*Autodiscovered devices and networks. Routers
are interconnected by links to networks.*

Entering an IP Address Range

You can enter IP address ranges in several ways, depending on what you need to do. These ranges are useful for configuring access in the InterMapper firewall, as well as for autodiscovery.

Characters you can use

- Use *hyphens (-)* to separate high and low values
- Use *wildcards (*)* to indicate a full range of values.
- Use *slashes (/)* to enter a range in [CIDR](#) notation.

Examples

- **Address range using hyphens**
  Example: `192.168.1.1-31` - specifies any device in the range `192.168.1.1` to `192.168.1.31`.
  Example `192.168.1-10.1-10` - specifies in subnets `192.168.1.*` to `192.168.10.*`, and finds addresses between 1 and 10 within each subnet.

- **Address range using "*" wildcards**
  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"`)

- **Address range using wildcards and hyphens**
  Example: `192.168.1-10.*` - finds 255 addresses in each of 10 subnets.
  Example: `192.168.*.1` - finds address #1 in each of 255 subnets.

- **Address range using [CIDR](#) ("slash") notation** which defines length in bits, often referred to as "prefix length" or "prefix bits"
  Example: `192.168.0.0/24` - (equivalent to `192.168.0.*` Class C)
  Example: `192.168.0.0/16` - (equivalent to `192.168.*.*` Class B)
  Example: `192.168.1.128/25` - (equivalent to `192.168.1.128-255`)
  Example: `example.com/24` - the last 255 addresses at example.com (Class C)
  Example: `example.com/25` - 126 addresses beginning with either 1 or 129, depending on the value of the last octet of example.com's IP address.

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.

139).

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. 776) (preceded by "\\"). For each entry that responds, a device is added to the map.
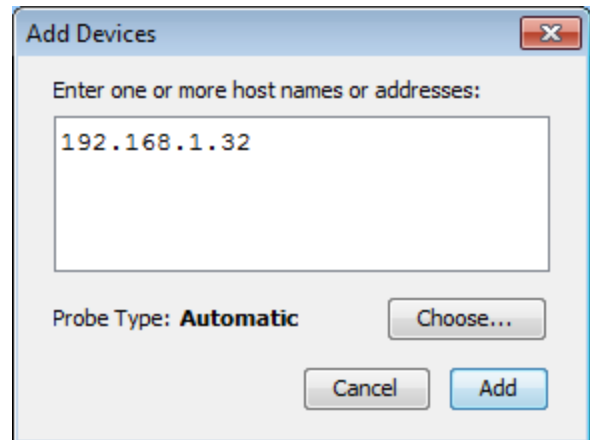
Add Device(s) window.

- **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.

> **NOTE: IPv6** To ensure that when possible, host names are resolved to IPv6 addresses rather than IPv4 addresses, enclose the host name in `[square brackets]`. For example, `[myserver.example.com]`.

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. 461).
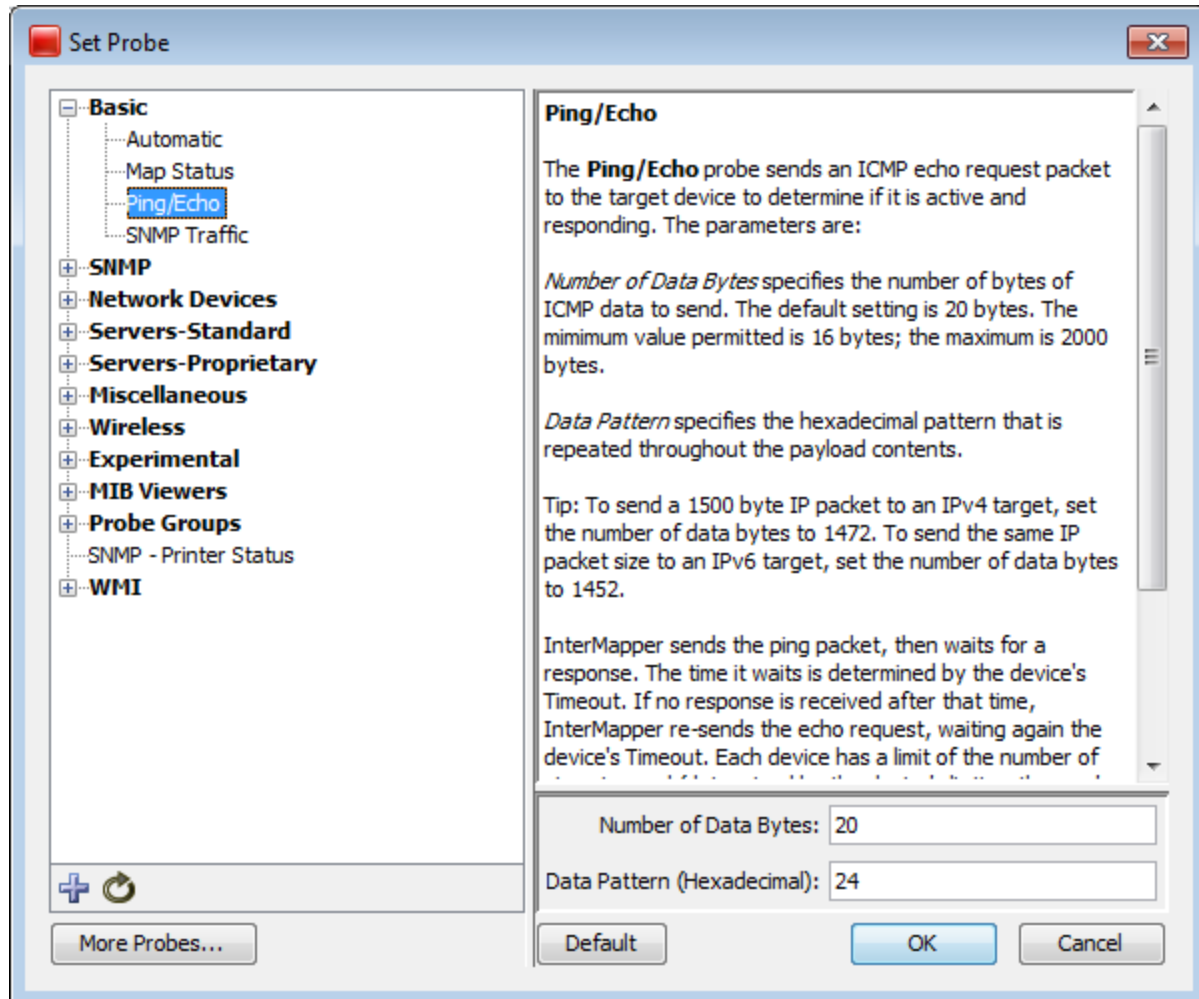
To choose and configure a probe:

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 subsection 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. 766).
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.
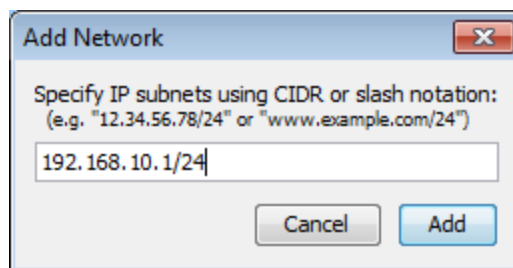
Add Subnet... window.
Enter an IP subnet (in the form x.x.x.x/yy).

> **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. 142).

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. 238).

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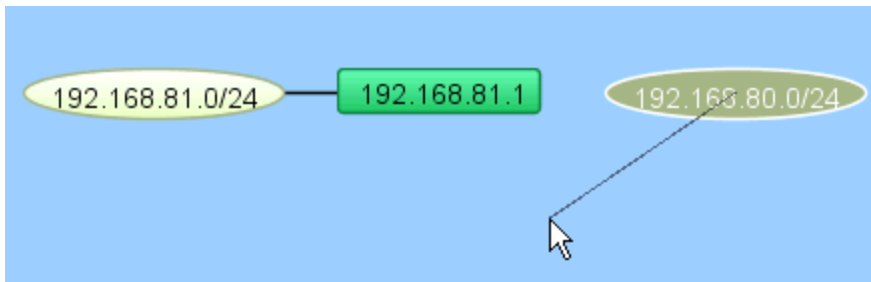
4. Click the object you want to connect to. A link is created between the two objects:

> **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. 238).

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.
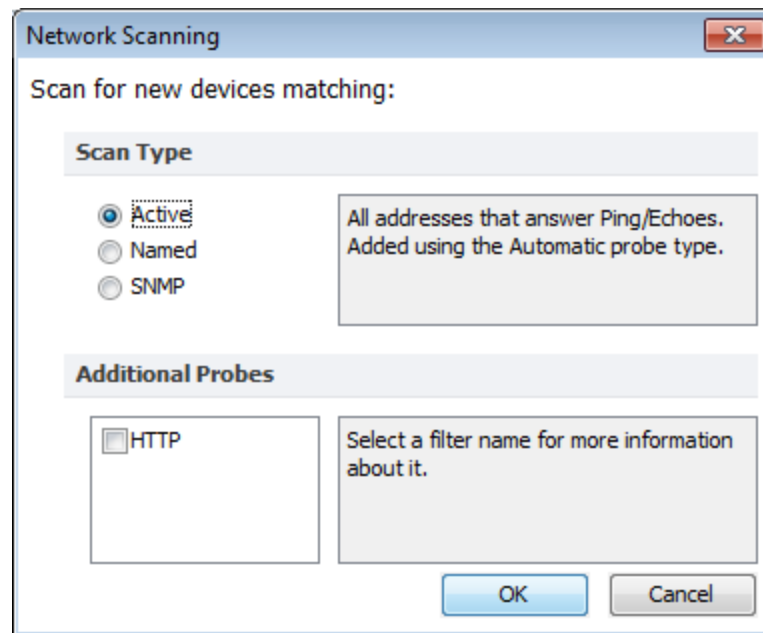
The Network Scanning window

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.
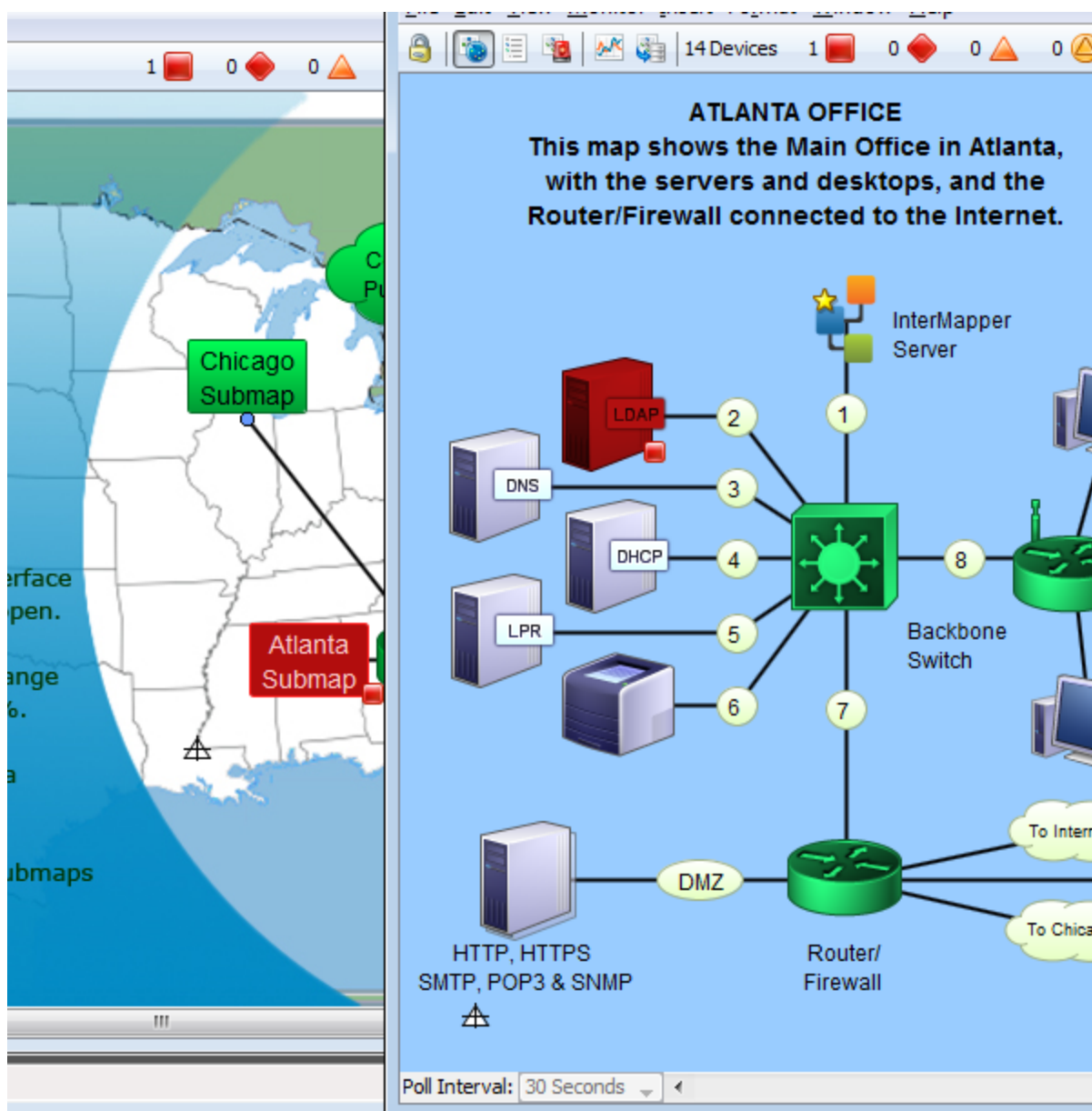
Creating a Sub-Map

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.
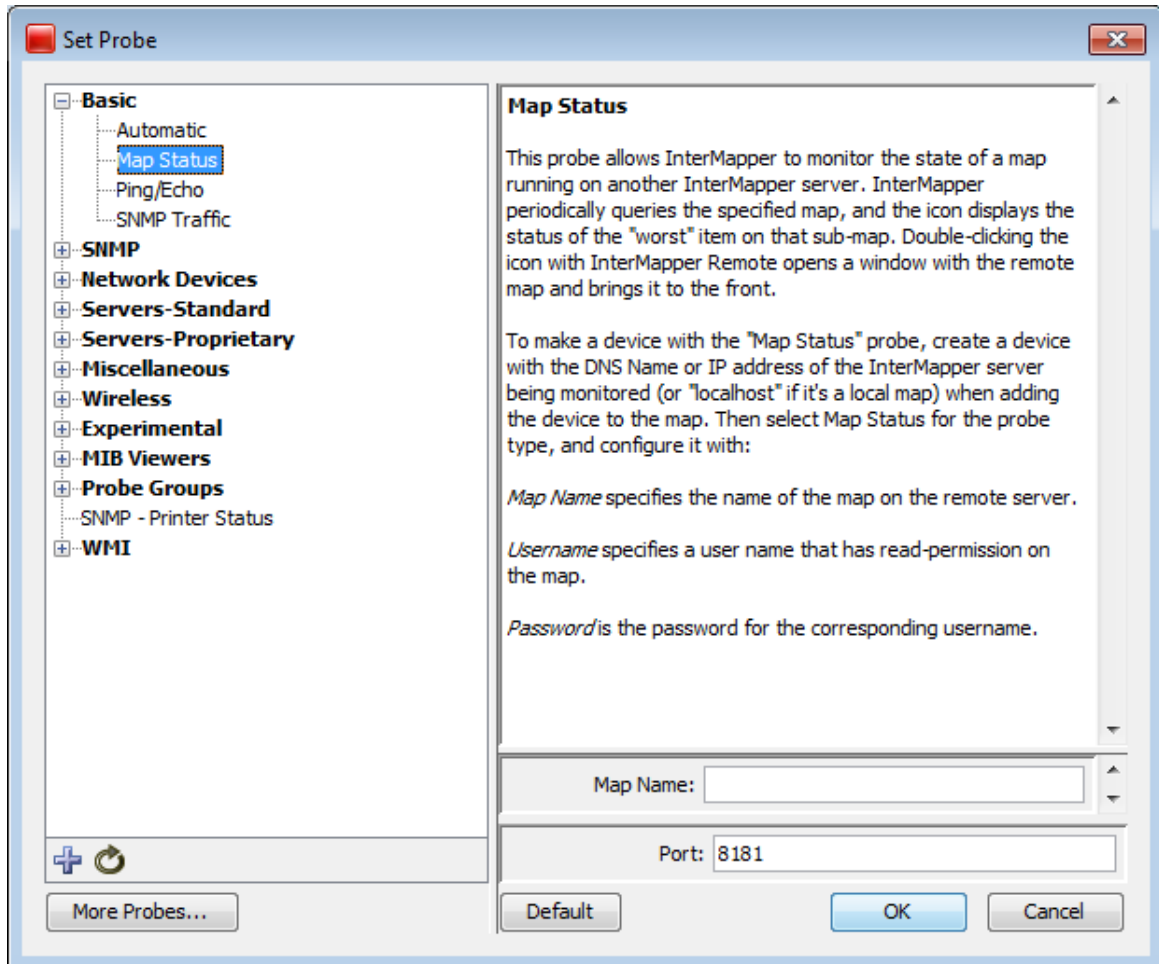
The Map Status probe configuration window.

To add a sub-map manually:

1. From the Insert menu, choose **Device...**

2. Enter the IP address (Pg. 766), DNS name (Pg. 770), or WINS name (Pg. 776) (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. 150) 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.
- **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.
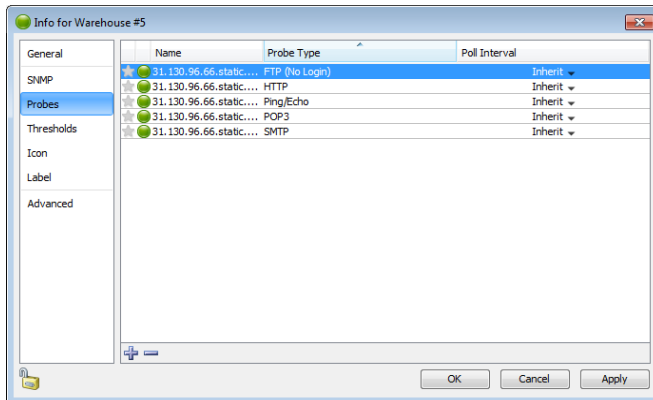
Before grouping

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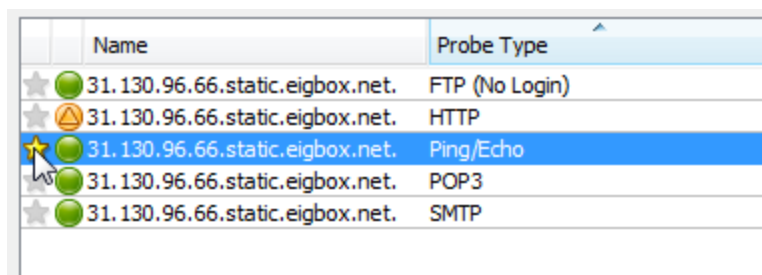
1. Double-click the probe group's device icon. The Info window opens, showing the list of probes in the group.
2. Double-click to open the Info window for the selected probe, or right-click/Ctrl-click the probe, and choose an option from the context menu.

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.

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.

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

The Helper apps context menu

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.

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](#) 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.
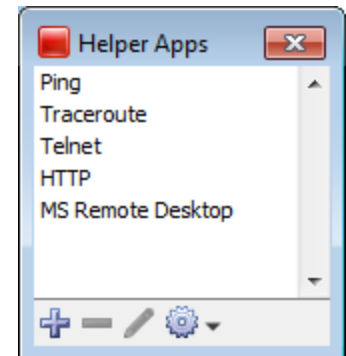
Adding or Editing Helper Apps

To add a new helper application:

- In the Helper Apps window, click the Plusbutton (**+**). 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.

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 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. F

   r

   o

   m
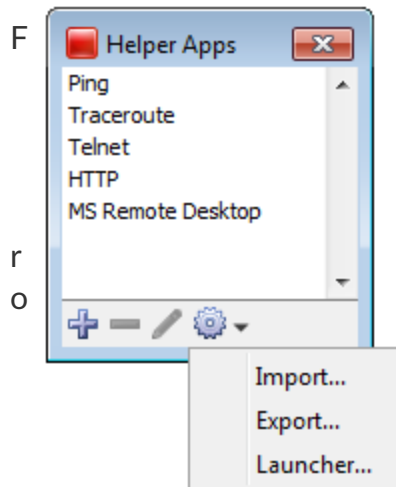
    the Helper Apps window, click the Tools button. The Tools menu appears.

2. Choose Launcher from the Tools menu. The Launcher window appears.
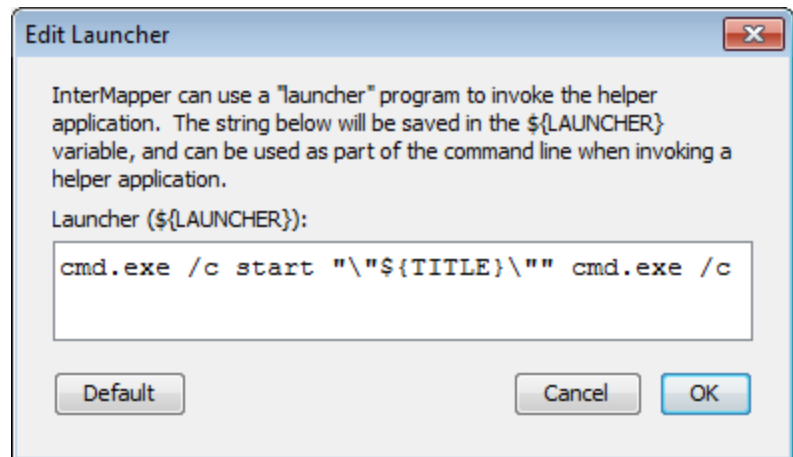
Exporting and Importing Helper Application Definitions

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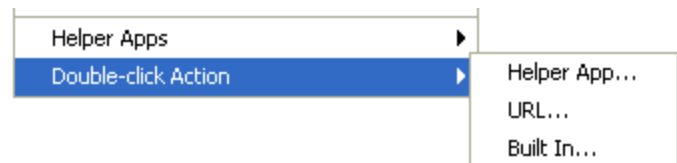
To change a double-click action, right-click on the device, and select the proper choice from the sub-menu:

Helper App

Double-clicking will invoke a specified helper application. This helper application runs on the same machine as the Intermapper client. Select the helper application from the current list of helpers.
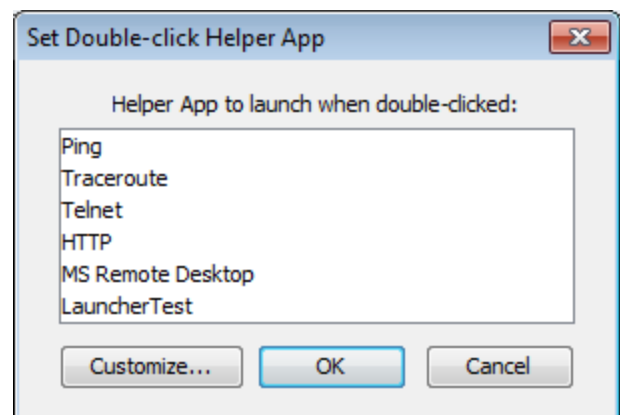
URL

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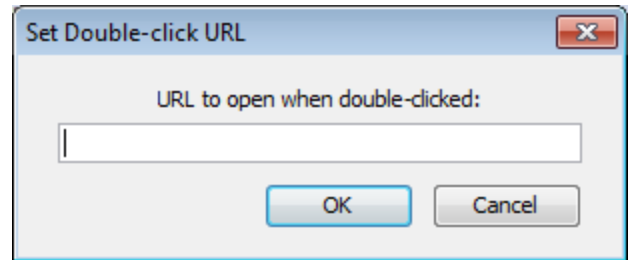
Enter a URL you want to use when the icon double-clicked. The default browser is launched with the specified URL.

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.
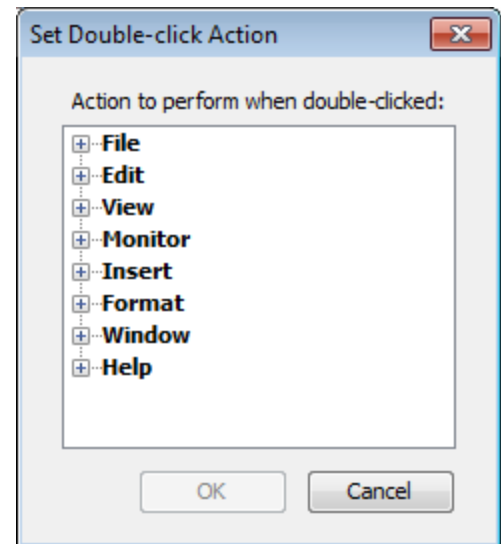
Making a backup of your map

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.
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.

Left pane of the Map Settings Window

Setting a Map's Colors
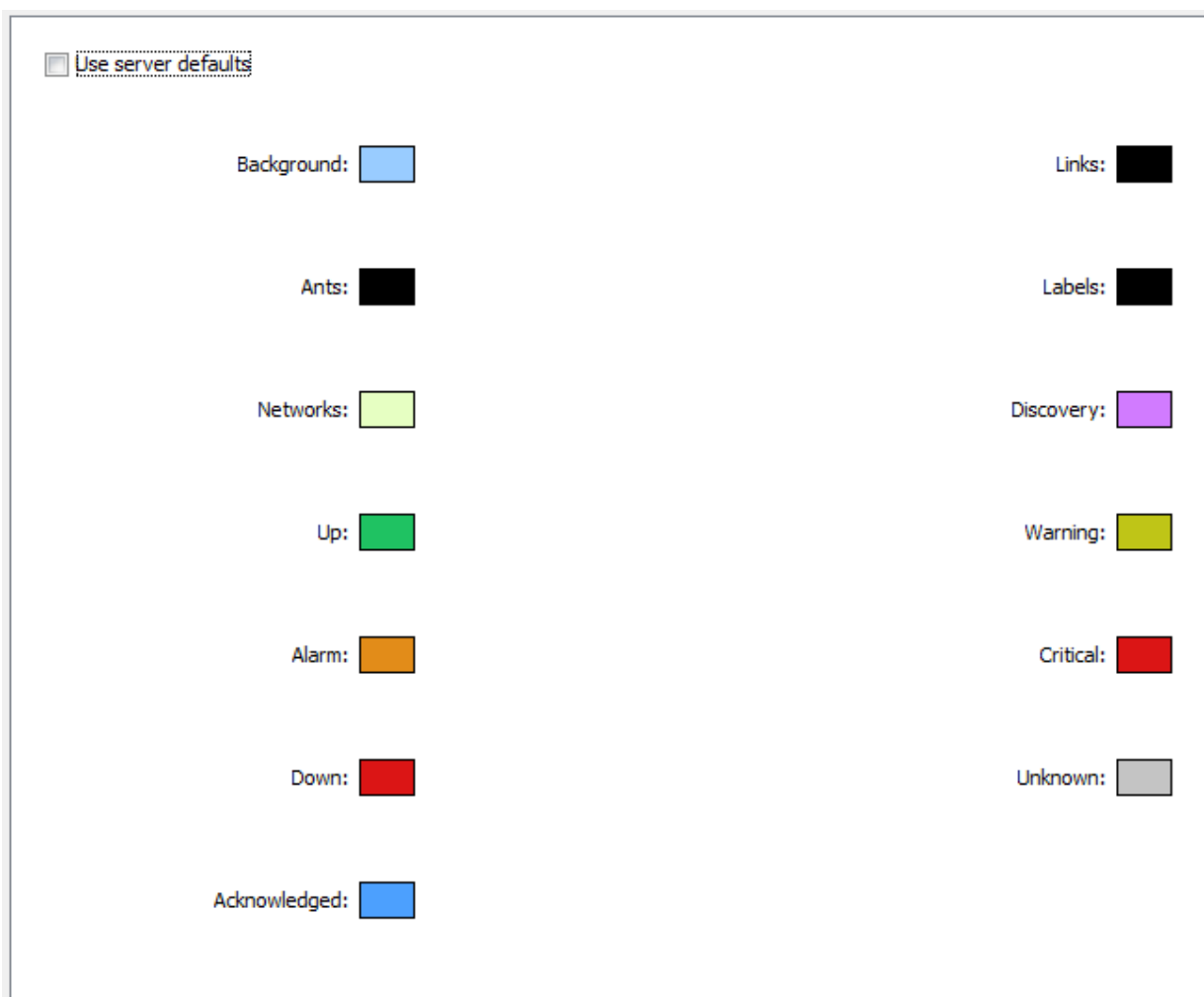
The Colors pane of the Map Settings Window

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 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, 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
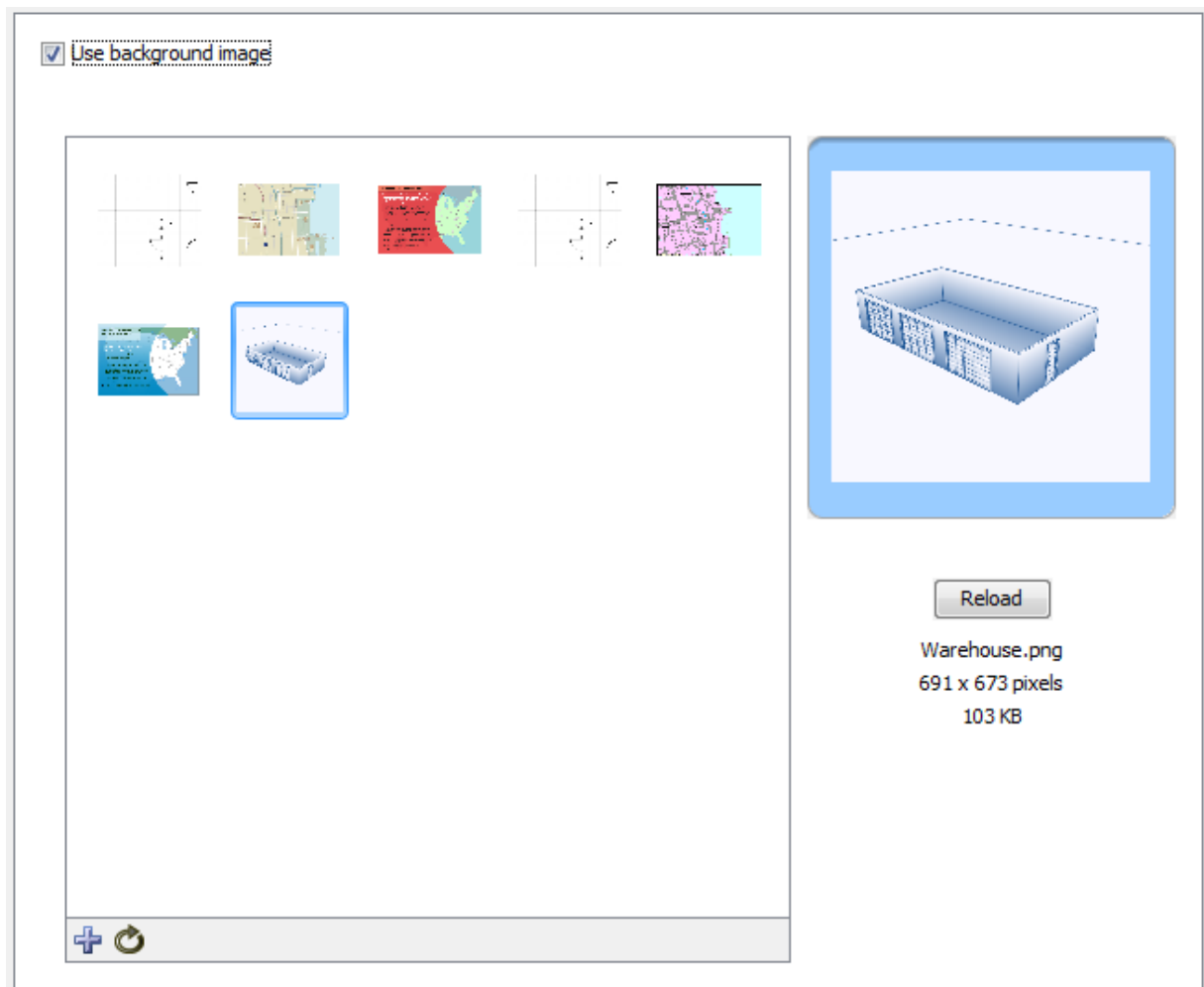
Background Image pane of the Map Settings Window

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.

Setting a Map's Default Device Thresholds

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 *Setting Thresholds for Individual links*.

Set interface thresholds to alert you to network problems.

Error Thresholds

☑ Use server 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

Utilization Thresholds

☑ Use server defaults

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

Discard Thresholds

☑ Use server defaults

	Warning	Alarm	Critical	
Rx Discards (Received):	15	25	35	per minute
Tx Discards (Transmitted):	15	25	35	per minute
Total Discards (Rx + Tx):	15	25	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: ▼	10	· · · · Some traffic
Frames Per Second:	100	········ High traffic
Average bytes per frame:	200	- - - - Large frames
Critical Errors: #####	◎	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.
- **Critical Errors** - this threshold is set in the Interface Thresholds panel.

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](#).

Specifying a Map's Default Notifiers

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 Configuring a Notifier.

- To **choose all notifiers at once**, Alt-click or Cmd-click (Mac) a check box in any column. All boxes are selected or cleared in that column. You can also use **Alt-click** to set **Delay** and **Repeat** to the same value for all notifiers.

To edit a notifier:

1. Click the row of the notifier you want to edit. The notifier row is highlighted and the **Edit Notifiers...** button is enabled.

2. Click *Edit Notifiers...* The Configure Notifier window for the selected notifier appears. For more information, see [Working With Notifiers](#).

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](#) 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.
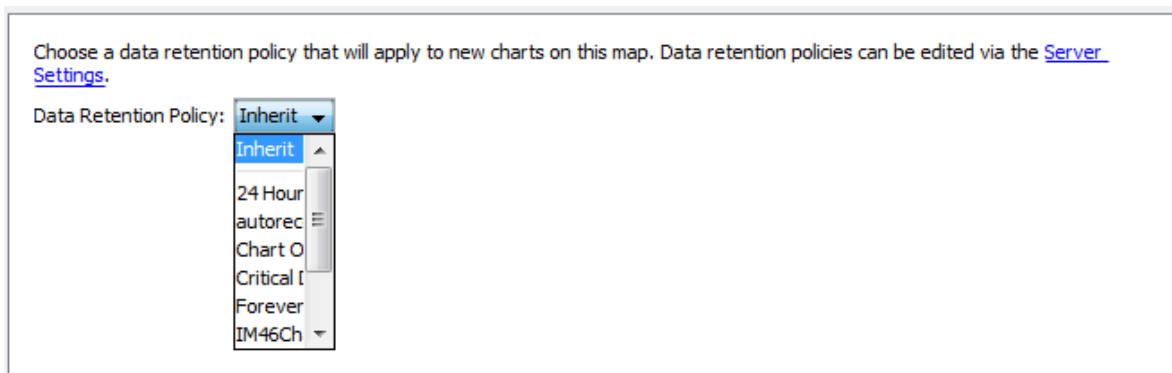
- **Data Retention Policy** - Choose a retention policy from the dropdown menu.

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.

- **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 .

> **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.

> **NOTE:**
> - 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] -ScriptBlock {
$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.

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 Interfaces Window.
4. See Using the Arrange Commands (Pg. 184) for more information about using the commands from the Format menu.
5. For other information related to arranging your maps, see Arranging Tips (Pg. 188).

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. 171).
- **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. 174).

- **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. 436) 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. 674).
- **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. 677).

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. 677). 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. 680).

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. 677). 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.
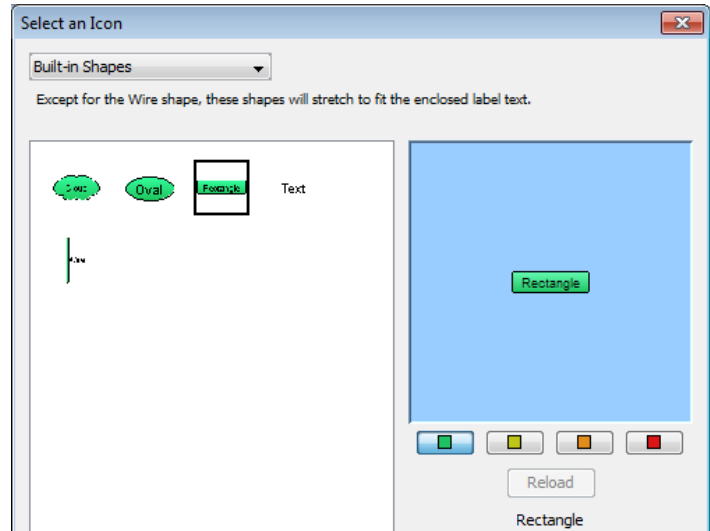
> **NOTE:** Grayscale custom icons appear shaded with the color of a device when it is in the UP state (the default is green.)

Select an Icon Window — Built-in Shapes

- 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.

- 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.

Select an Icon window - Default 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.

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) InterMapper 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. 173) 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. 157)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*.
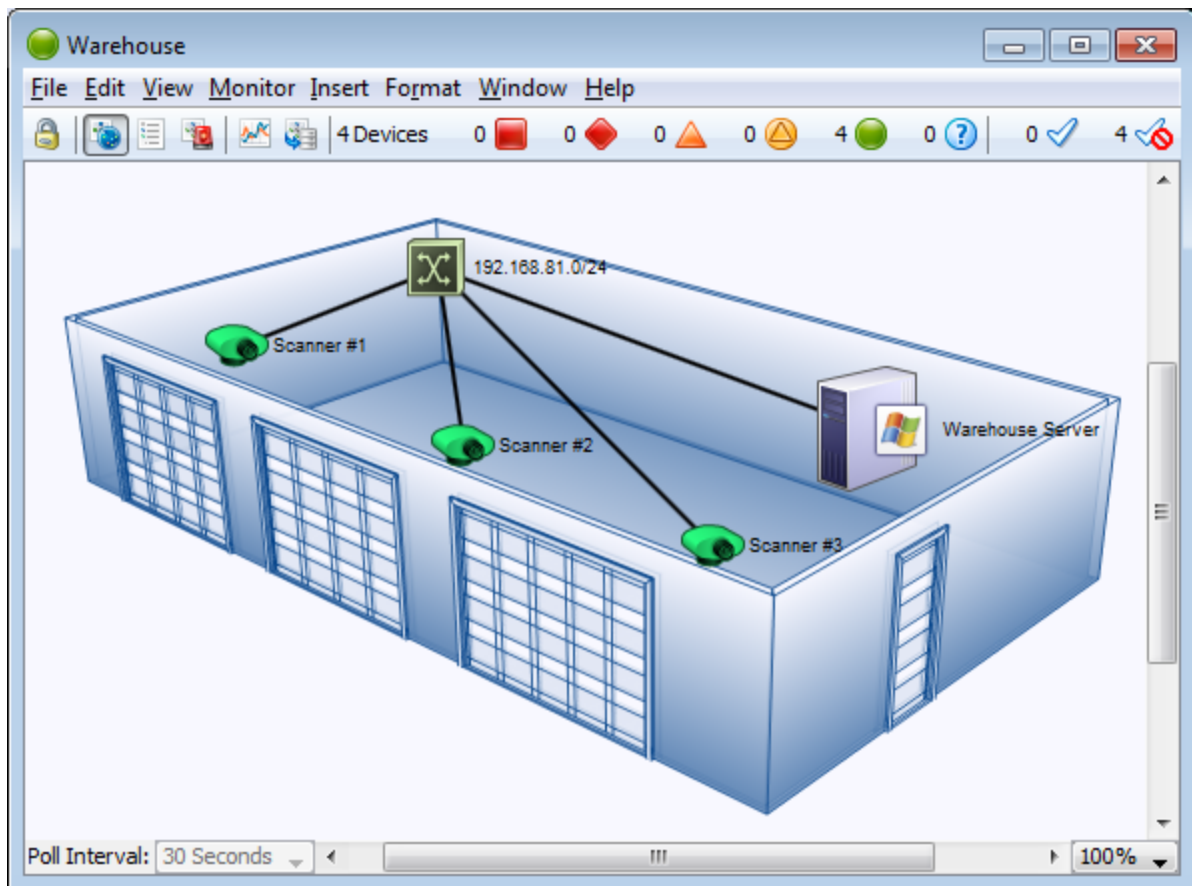
Map with background image.

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. 238).
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.
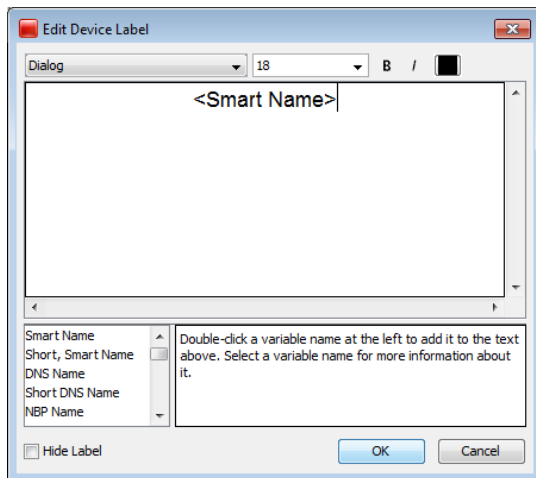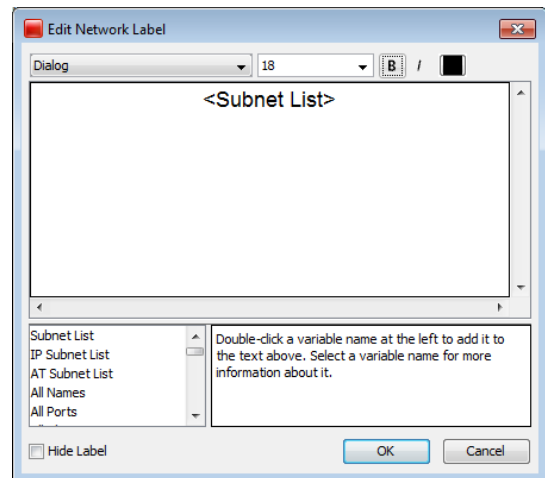
The Edit Device Label window   *The Edit Network Label window*

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 exported using the *Data File...* command (available from the File menu's Export submenu.)

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](#).

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:

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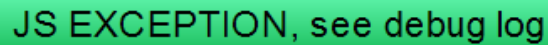
If you look in the debug log, you see the following message:

```
12:15:46 JS> [Device: map 'Exporting Fields', device
'nitro.dartware.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:

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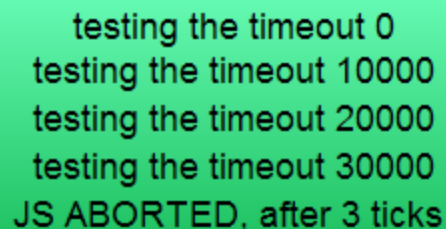
Execution Time Limit

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:

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);
?>
```
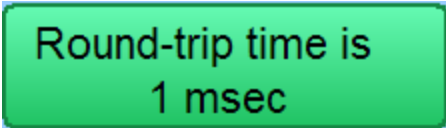
A similar technique would also work for JavaScript global variables as well.

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:

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.

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](#).

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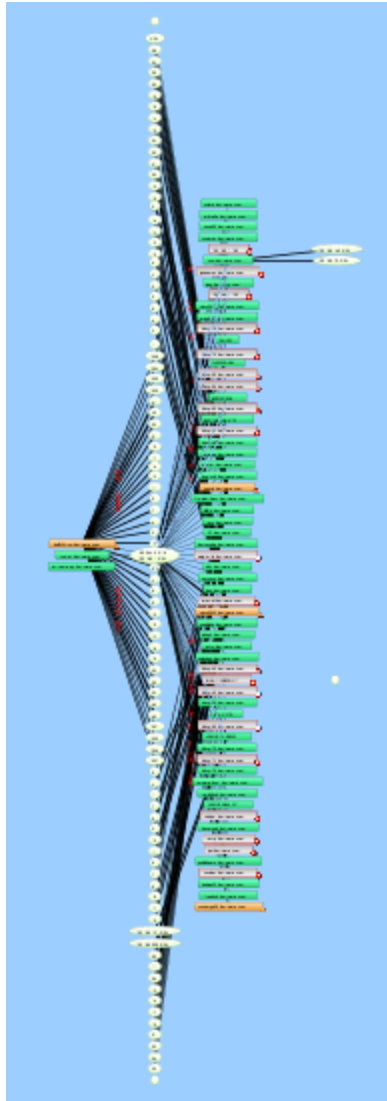
Use the *Organic*, *Tree*, *Cycle*, *Bus* , *Star*, and *Grid* commands available from the Format menu's *Arrange* submenu to rearrange and organize the selected elements automatically.

> **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.
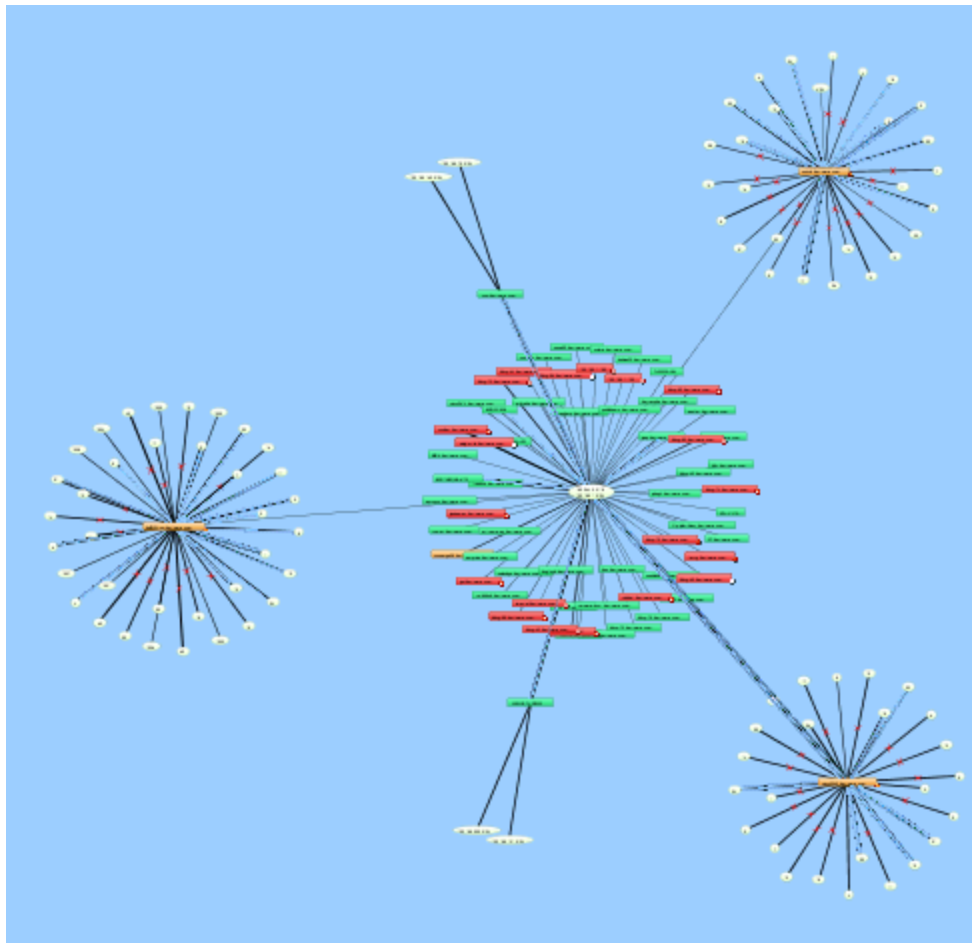
Using the Tree Commands

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*.
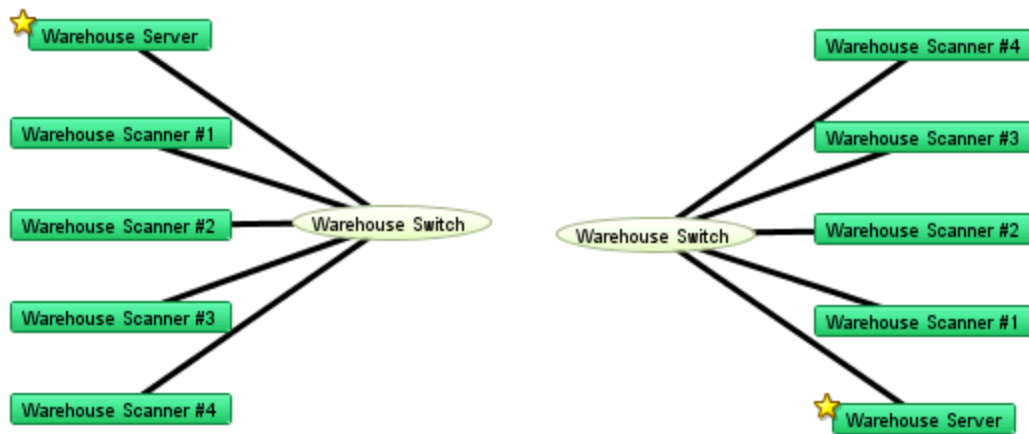
Tree > left　　　　　　　　**Tree > right**

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.
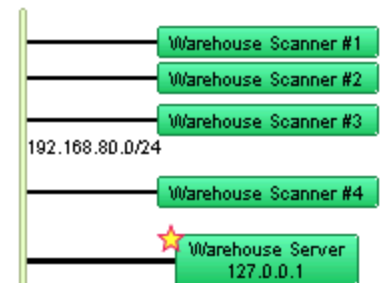
Using the Star Command

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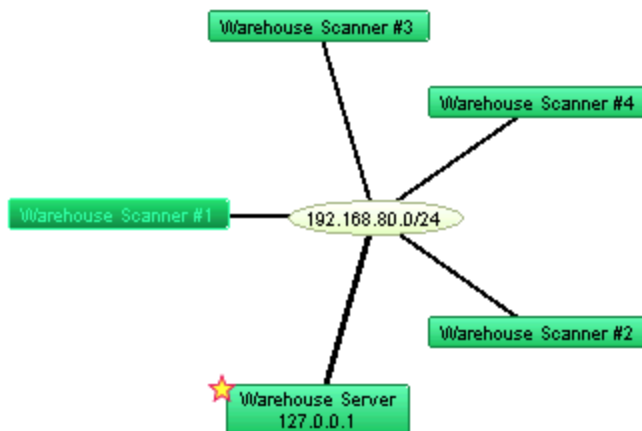
Using the Grid Command

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.
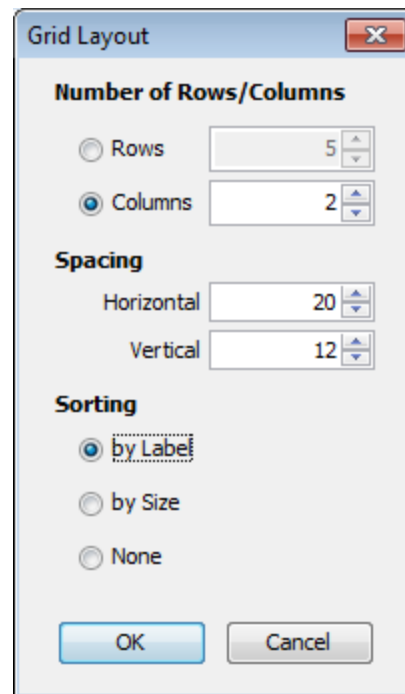
2-column grid layout

Using the Cycle Command

> **NOTE:** The Cycle command is deprecated. We recommend you Organic command for intial 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.
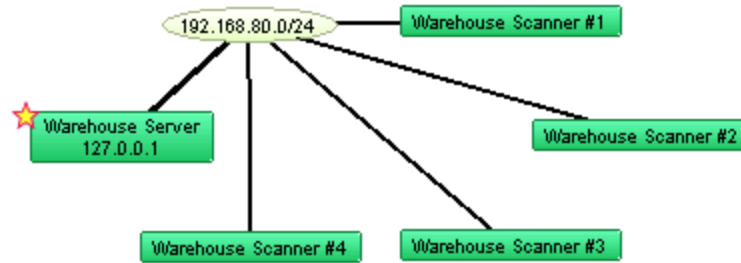
Results of the Cycle command.

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.

- See Editing Labels for Devices and Networks and Connecting Devices to Switch Ports 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. For more information, see Hiding and Un-hiding Detail .

- 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 connection point. See *Connecting Devices to Switch Ports* in the Switches .

- 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*.

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.

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 "switch.company.net" 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. 238).)
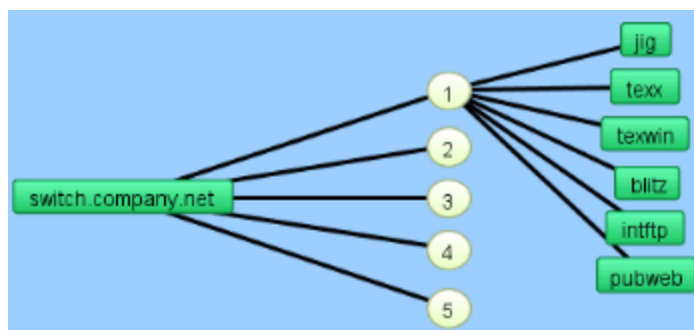
2. Click a link and drag it. A line appears, and follows the cursor.
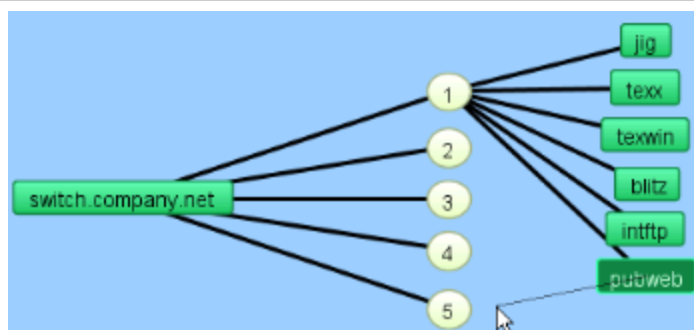
NOTE: You can drag links only from a network.

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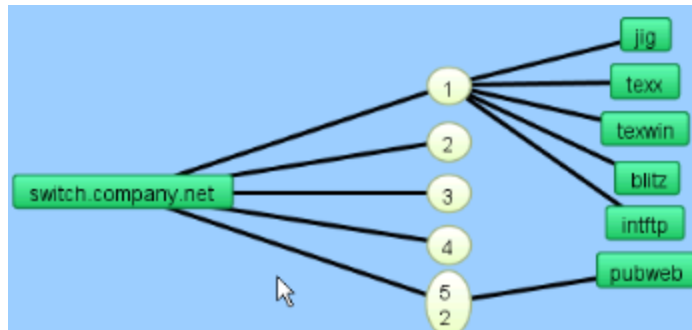
Tip: When moving links to the proper ports on a switch, it's sometimes easier to change the port labels to display the port's number.

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](#)
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.
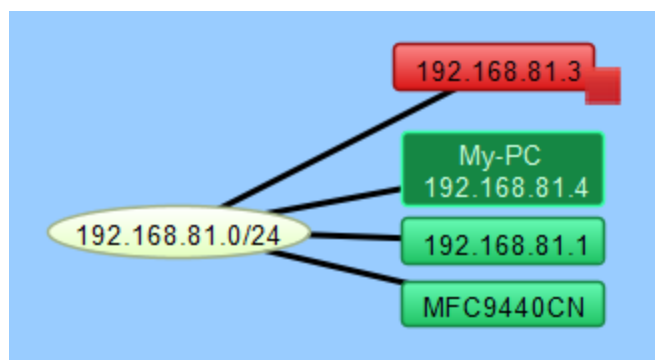
Before copy
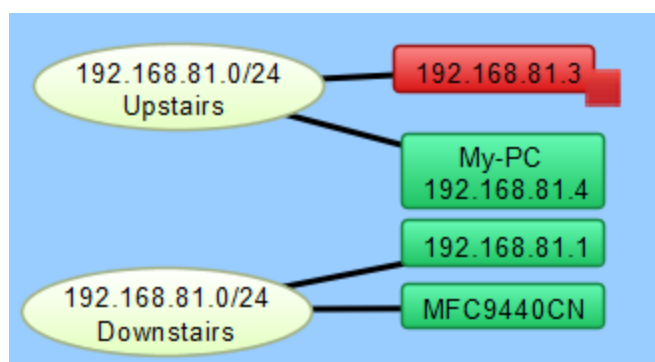
After copy, two links moved, labels updated

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 interconnections 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.
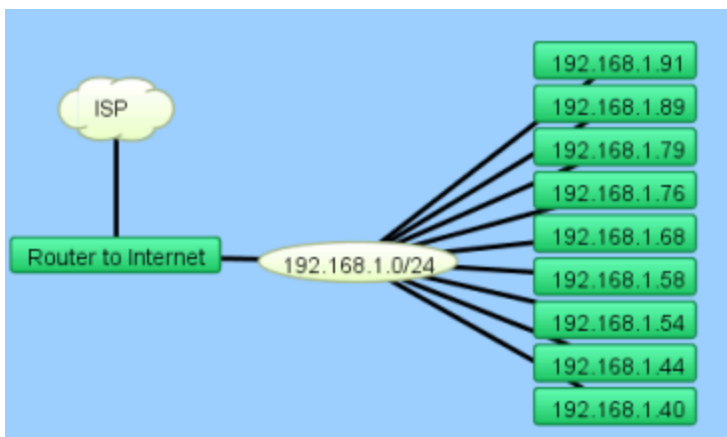
The problem

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.
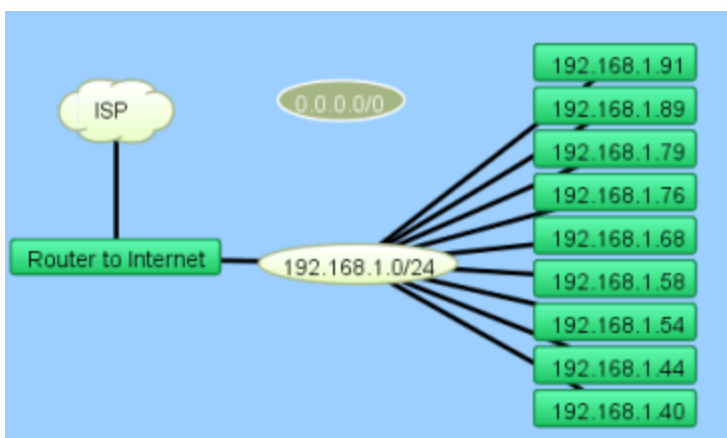
Step 1: Create a placeholder to represent your hub

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

To create the new network:

1. From the Insert menu, choose **Network...**

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. 141).

    The new network appears as an oval, with the subnet number you entered (not "0.0.0.0/0", as shown in this example).
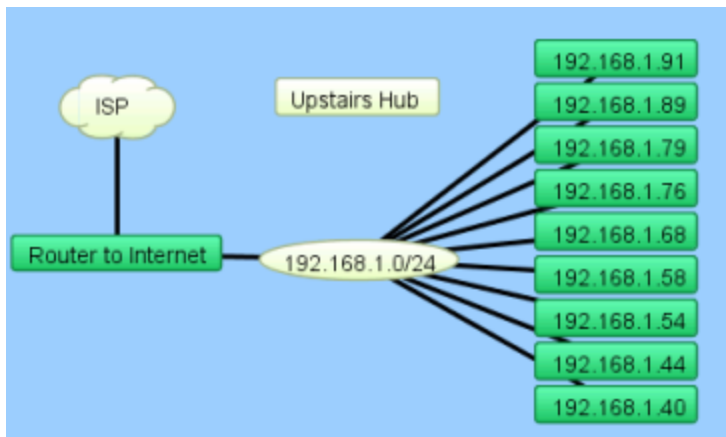
Step 2: Tidy up

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.
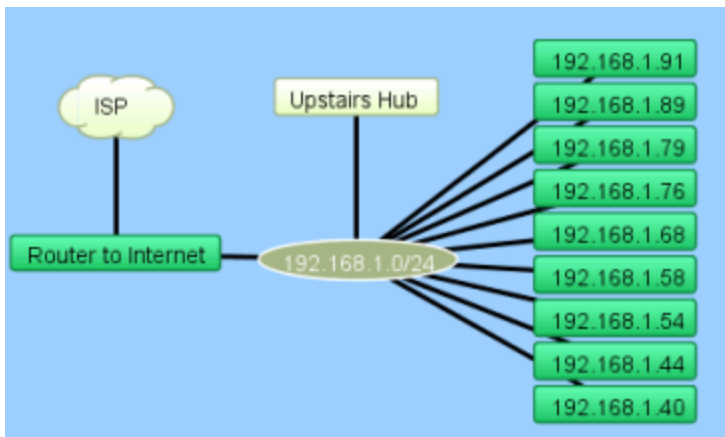
Step 3: Connect the hub to the network

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 appears, connected on one end to the rectangle, and to your mouse cursor on the other. You can also right-click one of the selected devices and choose *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.
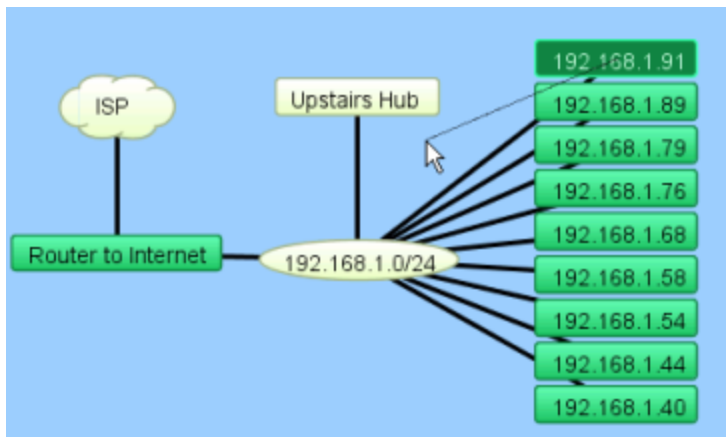
Step 4: Connect the devices to the "hub"

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.
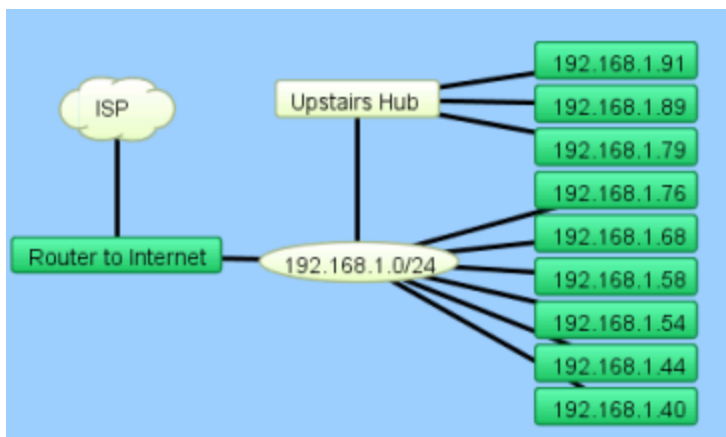
The result

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** - 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. Each device represents a "sub-map." .

- Use the Interfaces window to hide or show interfaces. When you hide an interface, it is no longer polled, and alerts are not sent.

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** - sends an e-mail
- **Alphanumeric Pager** - sends a page through a dial-up modem using the TAP protocol.
- **Network Paging** - sends a page across the Internet using the Simple Network Paging Protocol (SNPP).
- **SMS Alert** - sends a text message to a cell phone via SMS.
- **Sound** - plays a sound associated with the state of the device.
- **SNMP Trap** - sends an SNMP trap to the specified trap receiver
- **Syslog** - sends a message to a syslog server
- **WinPopup** (Windows only) - sends a message to the specified user. The message appears in a separate window.
- **Command Line** - executes a command on the Intermapper host machine.
- **Group** - sends notifications to a group of existing notifiers.
- **PowerShell** - executes a PowerShell command or script on the Intermapper host machine or a remote Windows machine.
- *AutoMate* - 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](#) from the [Notifier List](#) pane, available in the **Server Settings** window.
- You [configure the notifier](#), then [test it](#) to make sure it's working properly.
- You [attach a notifier](#) to a device using the Attach Notifier dialog.
- You [remove a notifier](#) using the Notifier List.
- You [define a set of default notifiers](#) 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 Device Notifiers or Link Notifiers view of the map window. Choose **Edit Notifiers...** from the Notifier dropdown menu in the tool bar as shown below.
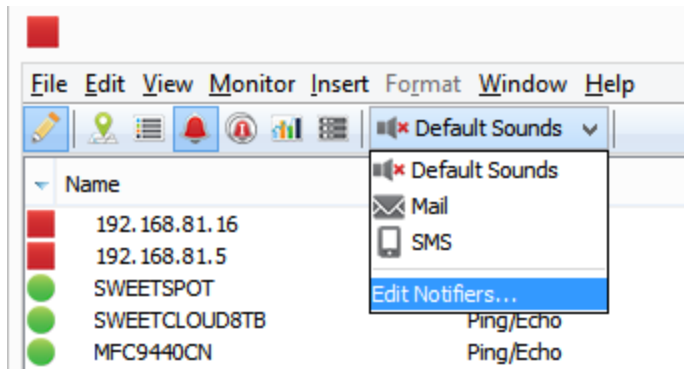
How Notifications Get Sent

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 pane, available from the Server Settings window. You attach notifiers to devices in the Device 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
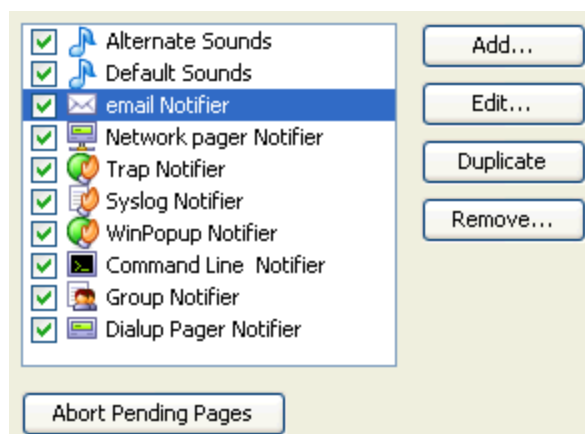
Notifier List window. The Default Sounds are built-in.

To view the Notifier List:

- From the Server Settings window 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 Device Notifiers window from the Monitor menu, or Alt-click or Cmd-click (Mac) the context menu. Any changes you make apply to all selected map items.

Attaching a Notifier to a Device or Interface

Attaching a Notifier to a Device

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 *Device Notifiers* or right-click a device in the Map or Device List view of the Map window. The **Notifiers for device(s)** window appears, showing which notifiers are currently attached to the selected items as shown below.

3. In each notifier row, 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 for that notifier.
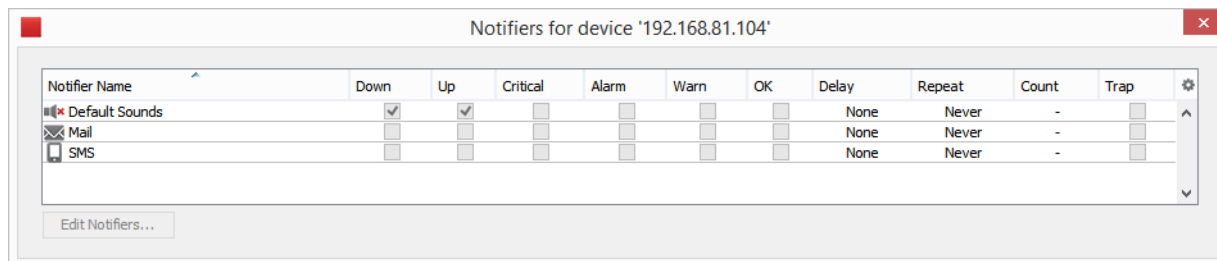
Device Notifier window

> **NOTE:**
> - **Configure a notifier** - Click a row to select a notifier, then click **Edit Notifiers....**. The Configure Notifier window appears.
> - Attach all notifiers to selected devices, Alt-click or Cmd-click (Mac) a check box in the status column you want to use. All check boxes in the column are toggled to the same state. Alt-click or Cmd-click (Mac) a **Delay** or **Repeat** dropdown menu and choose a value to set all rows to that value.

Attaching a Notifier to an Interface

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's **Interfaces** submenu, or from the device's context menu's **Interfaces** submenu. 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 (Mac) one of the selected interfaces and choose *Notifiers Window* from the context menu's **Interfaces** submenu. The **Notifiers for link** window appears, showing which of the available notifiers and the status they use to attach to the selected interfaces .
5. 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, showing the default attachment settings used when a new device is added.

3.

4. Click *Reset All*. The Confirm Notifier Reset dialog appears.
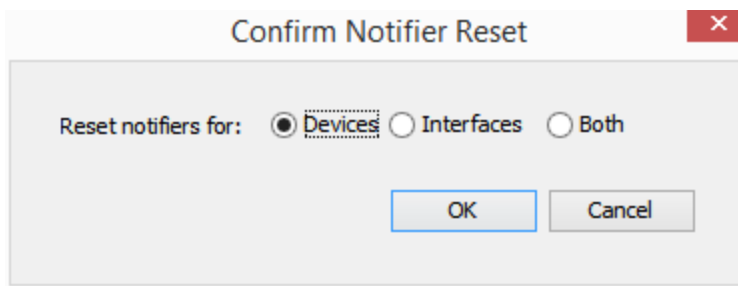
5. Click to reset notifiers for **Devices**, **Interfaces**, or **Both**, then click **OK**. All devices on the map are set to the default notifier settings.

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 quicky 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. 206). 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.
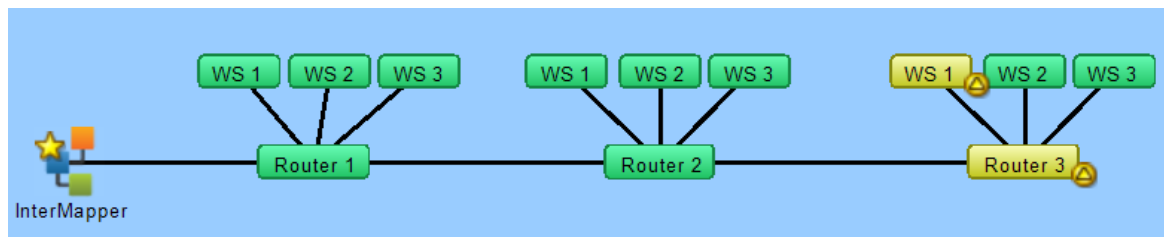
Example 2: One device is down, shows dependent devices

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.
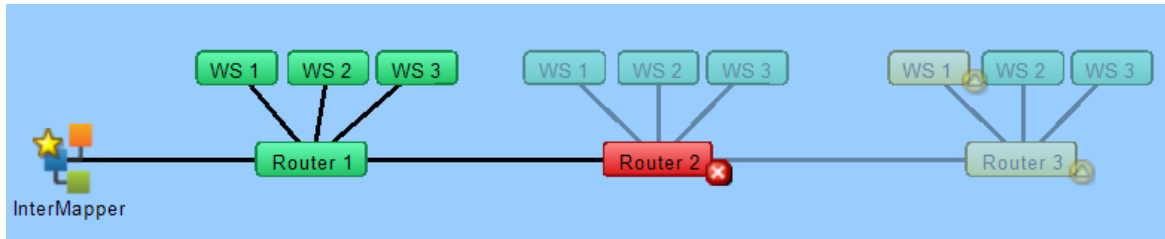
Setting a Vantage Point

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* .

A Vantage Point. Notice the star on the item.

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 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.
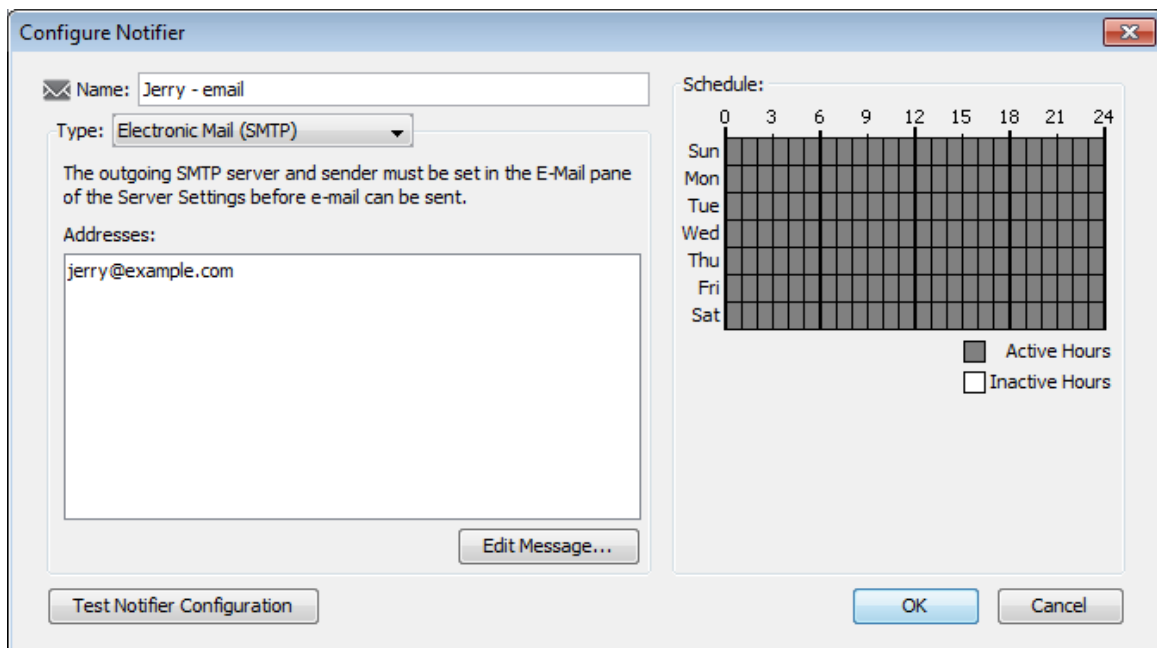
The Configure Notifier window.

- 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. 198) 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. 198)](#) 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](#).

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 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.
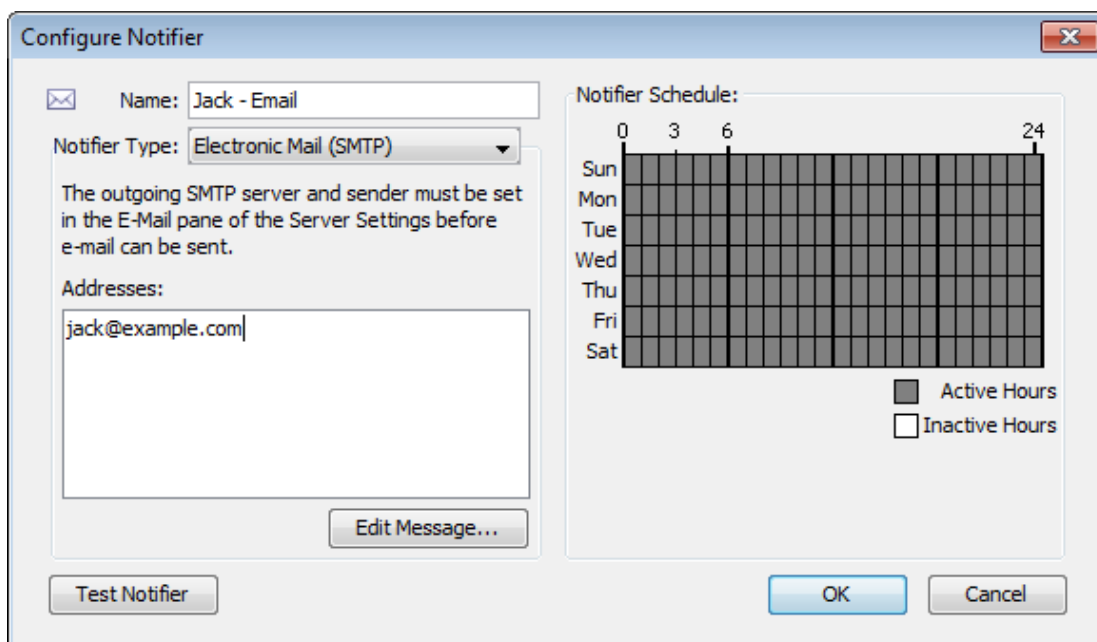
Configuring an e-mail notifier.

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. 305).

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.
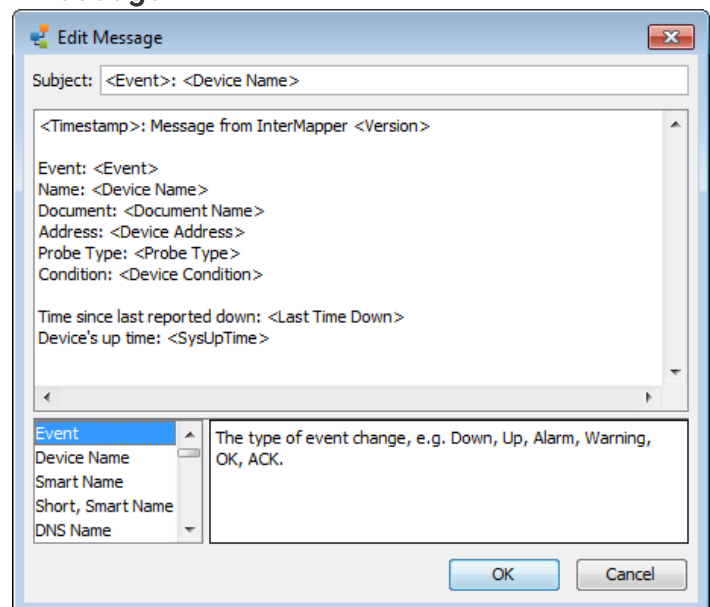
Subject :

```
<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](#).

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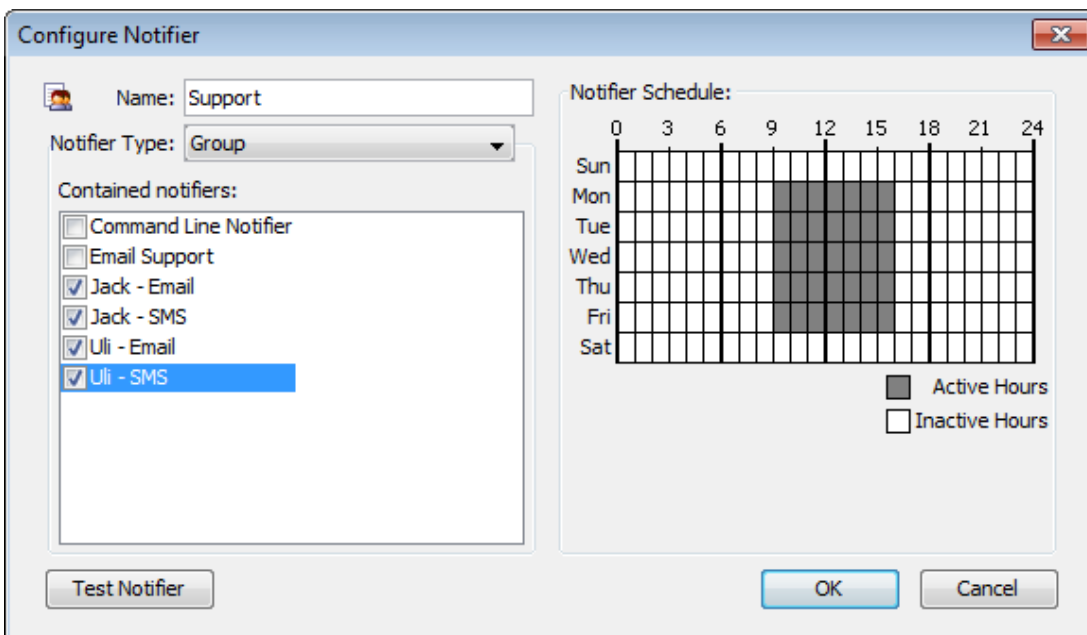
How it works
When the Group notifier is invoked, Intermapper first checks the time schedule. If the time is applicable, Intermapper invokes each of the checked notifiers. They in turn check their schedules, and send the notification if desired.

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).

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](). 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.

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. 201).
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. 214) 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 able to send the notification.
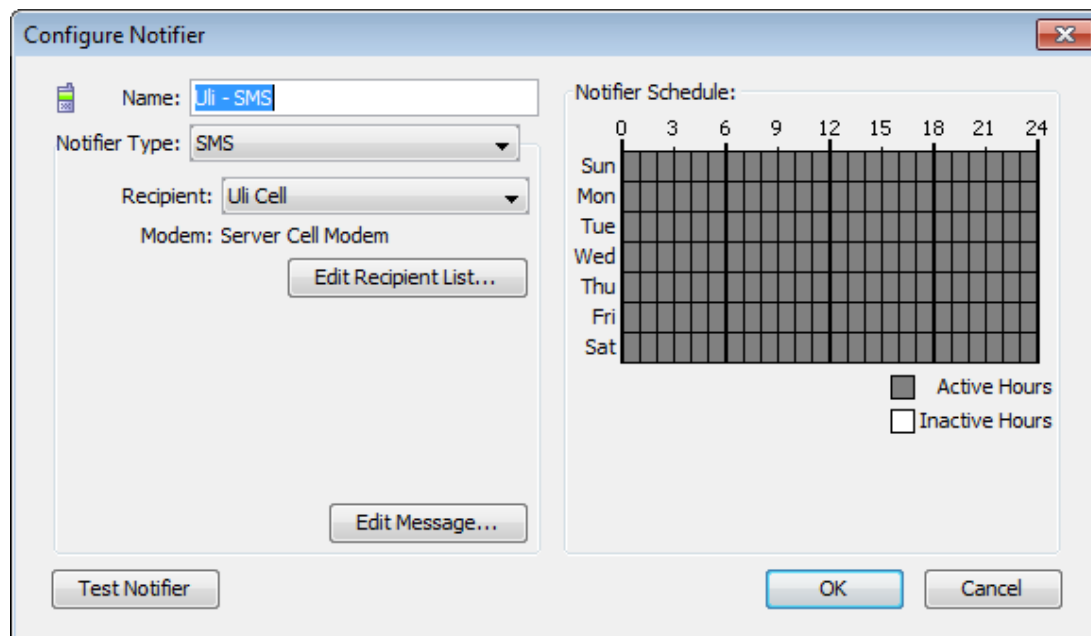
To configure an SMS notifier:

1. In the Configure Notifier window, choose "SMS" from the *Notifier Type* dropdown 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. 217) and Adding and Removing SMS Recipients (Pg. 218), 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. 211).

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.
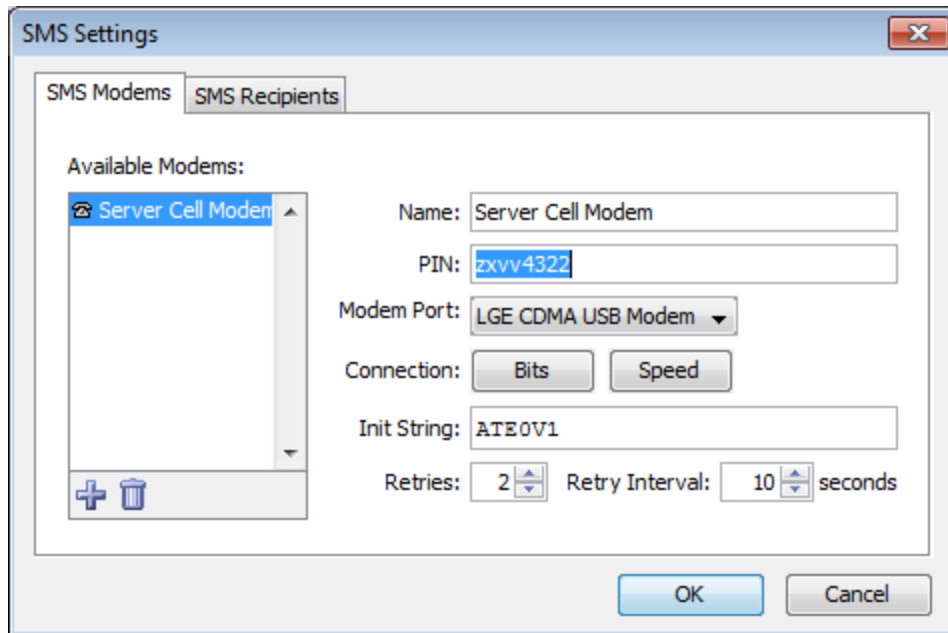
To add an SMS modem:

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.
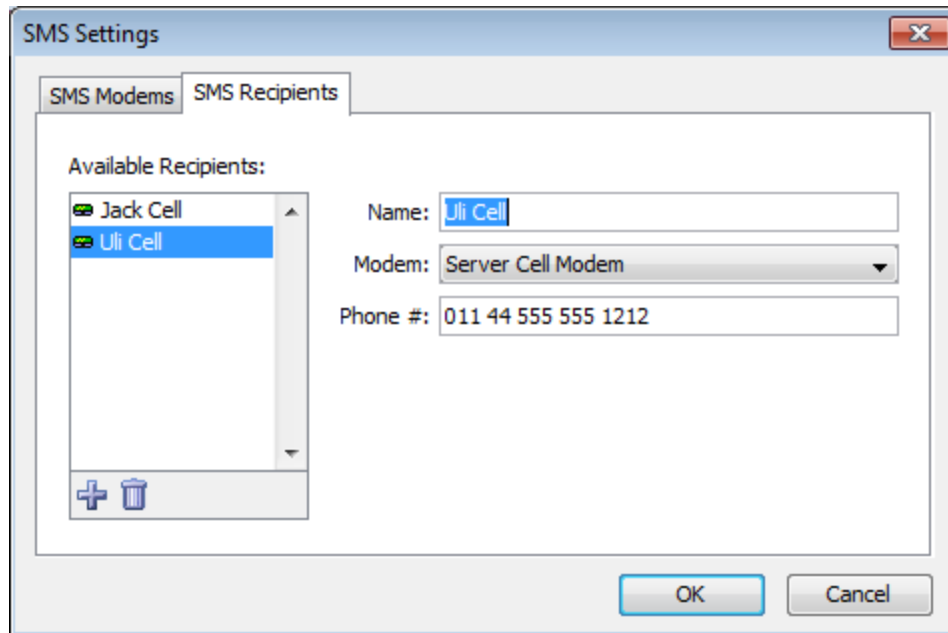
To add an SMS recipient:

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

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.

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. 220) for an example of a command line notifier.

Example Notification from a Command Line Program

Here is a simple example of a command line notifier. This notifier does the following:

1. Calls a python script located in the Intermapper Settings\Tools folder.
2. Passes the script two parameters:
    - The notification message, using the ${MESSAGE} macro.
    - A filename for a log file
3. The script opens the specified file, (also located in the Tools folder) and appends the message text to it.

Log.py Script

Place this script in the Tools folder in a text file named `log.py`:

```python
import sys
# options are: message logfile
if __name__ == '__main__':
    f = open(sys.argv[2], 'a+')
    f.write(sys.argv[1]+'\n')
    f.close()
```

Configuring the Command-Line Notifier

Configure a new notifier as follows:

1. Create a new notifier.
2. Set the **Type** to **Command Line**.
3. Enter this text in the Command box:
    `${PYTHON} log.py "${MESSAGE}" test.log`
4. Edit the message and schedule as needed.
5. Click Test Notifier Configuration.
6. Attach the notifier to one or more devices as described in Attaching_A_Notifier.htm.

When the notifier runs, a file named `test.log` is created in the Tools folder. Message text is appended to to the log file.

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 Link Notifiers window](#) for the interface you want alerts from.
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 (Mac) the selected row, and choose *Notifiers Window...* from the **Interfaces** submenu. The *Notifiers for link(s)* window appears, 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.
5. Alt-click or Cmd-click (Mac) a check box or choose a value from the dropdown in the **Delay** or **Repeat** column to set the notifiers for all links to the same value.
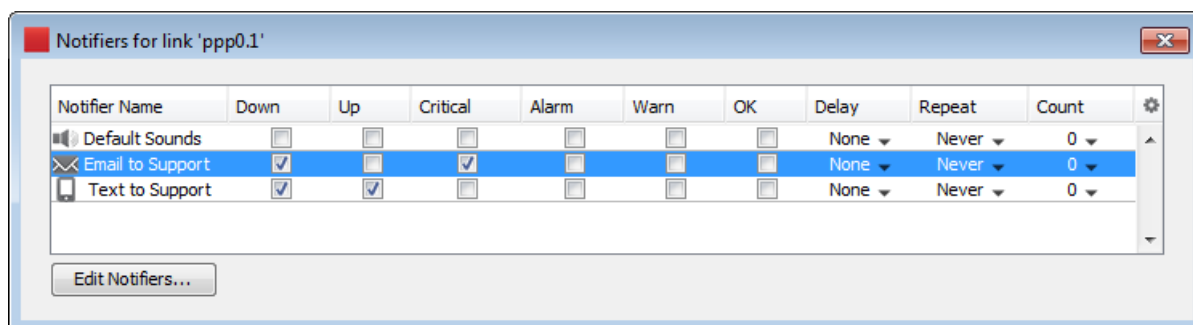
Notifiers Window for a link

WinPopup (Windows Only)

When the devices 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.

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.

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. 211)](#), 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. 233).
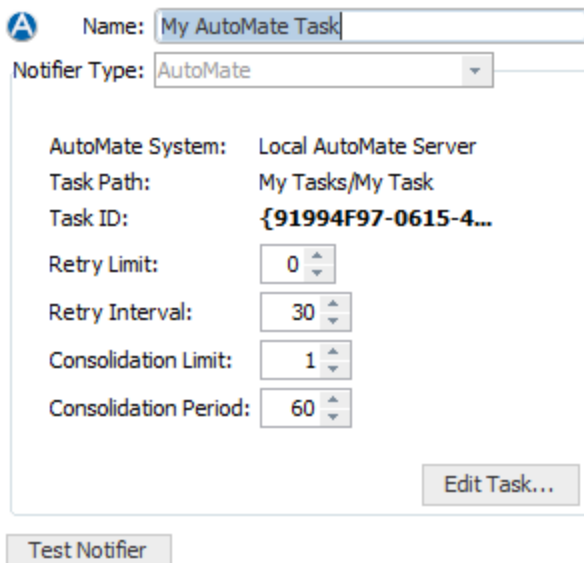
Timestamp:	The current date and time, as a string in the format: MM/DD HH:MM:SS
Message:	DOWN, UP, ALARM, WARN, OK, or TRAP (See the Dartware MIB (Pg. 233).)
Device name:	The devices DNS name, as a string
Condition:	The condition of the device, as it would be printed in the log file.
Device Address:	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. 233)):

```
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.

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 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:

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 notifer.
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.MAXSENDCOUNT%
- **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.SYSDESCR% - 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](#) 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.

Execution: Alerting Device

The specified command text is executed on the machine that triggered the alert.

Execution: Other Device

The specified command text is executed on the machine specified in the *ComputerName* box.

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
InterMapper."

    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
notification option."
     ::= { intermapperNotifications 1 }



END
```

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. 427) command, available from the Monitor menu. The map's poll interval value affects only those devices that are using the default poll interval.
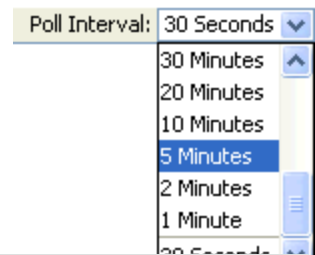
Zooming In On the Map

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.
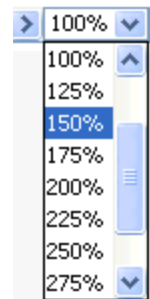
Understanding the Map

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
- Status Badges
- Dotted lines (or "moving ants")
- Boxes and Ovals (or "bubbles")
- Line Styles
- Link States

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 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.
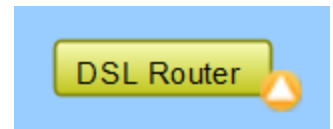
> **NOTE:** You can specify which badges you want appear on devices from the Intermapper User Preferences window.

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.
1.0/2	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) Blue X (links)	**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.

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 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).
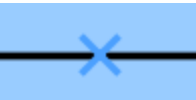
Line styles
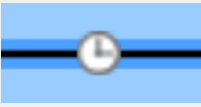
The style of the line corresponds to the type of interface.

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.
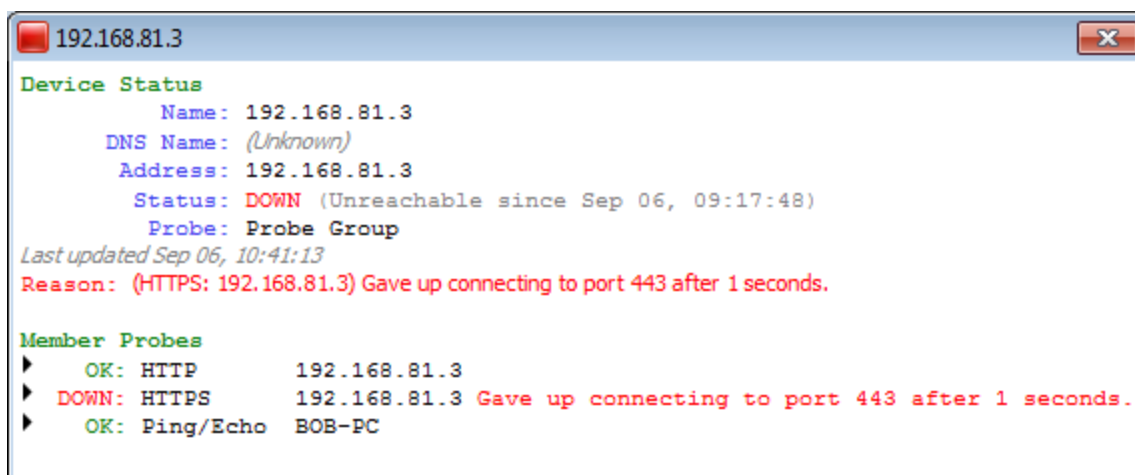
To view device, network, or link status:

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 and 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

```
192.168.81.0/24                                                    [x]
Network Status
  Name:      192.168.81.0/24
  IP Net:  192.168.81.0/24
  Top Tx:      0 pkt/sec      0 byte/sec      0 txerr/min  192.168.81.1 (192.168.81.1)
  Top Rx:      0 pkt/sec      0 byte/sec      0 rxerr/min  192.168.81.1 (192.168.81.1)
  Top Err:     0 pkt/sec      0 byte/sec      0 rxerr/min  192.168.81.1 (192.168.81.1)
  Sum In:      0 pkt/sec      0 byte/sec      0 txerr/min
  Sum Out:     0 pkt/sec      0 byte/sec      0 rxerr/min
```
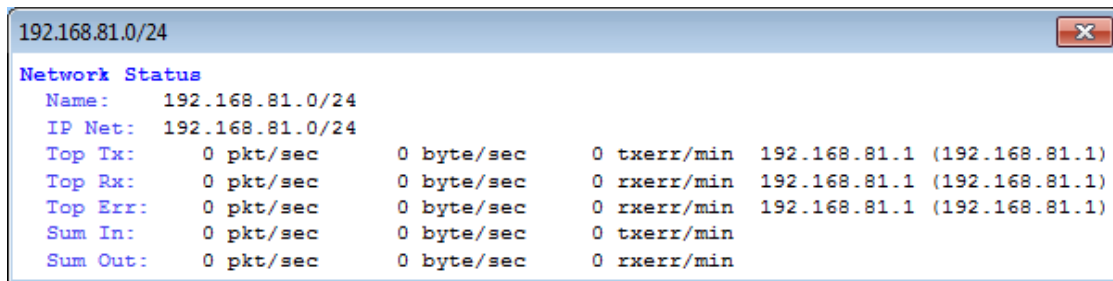
- Click and hold the mouse on a network oval to open its *network status* window, or right-click the network and choose **Status Window**..

- 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.
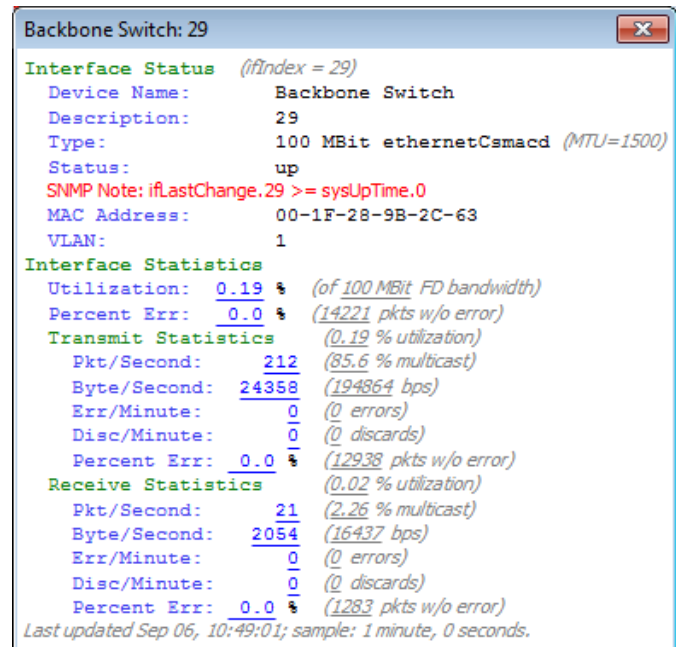
Tip: Certain devices do not report their link speed accurately in their SNMP responses. This causes Intermapper to report a value which is not actually correct. To work around this, switch the map to Edit mode, then right-click the link and choose *Set Link Speed...* The Set Link Speed window appears, 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](#).
- For details on viewing and editing network info, see [The Network Info Window](#).

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.

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](#).

- **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 and Dynamic Label and Alert Text.

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
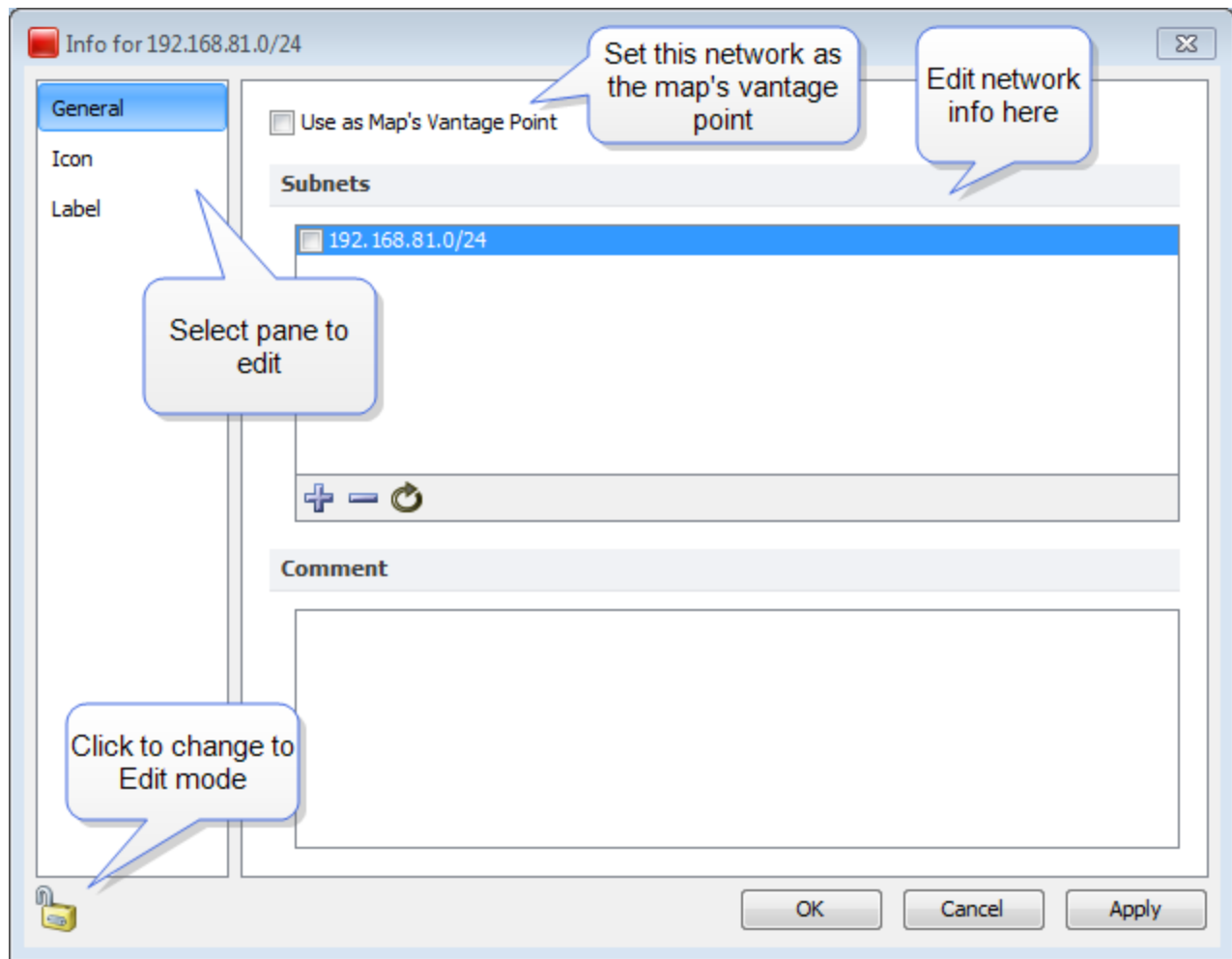
General Pane

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.
- 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](#).

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](#).

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
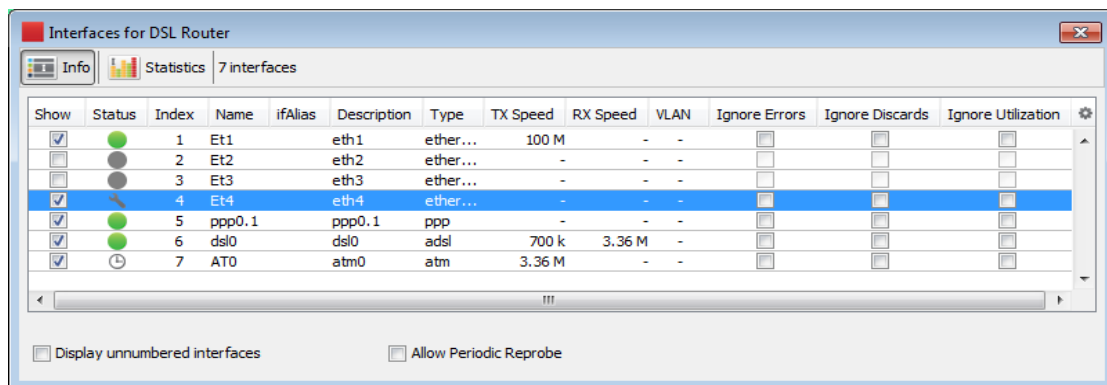
Interfaces window - Info View

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, 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 reprobed every 12 hours.
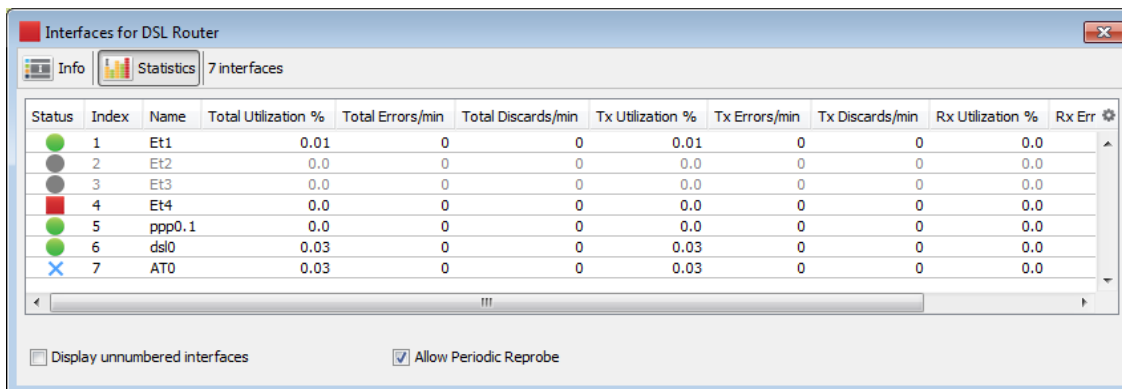
Notes:

- 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.

- These two controls interact with each other. The *Display unnumbered interfaces* box determines whether an unnumbered interface is ignored during a periodic or manual reprobe. The Interfaces Window does not change when you uncheck this box until the next reprobe. This applies to a periodic reprobe described above and to a manual reprobe.

The Interfaces Window - Statistics View

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 reprobed 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 rediscovers 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.
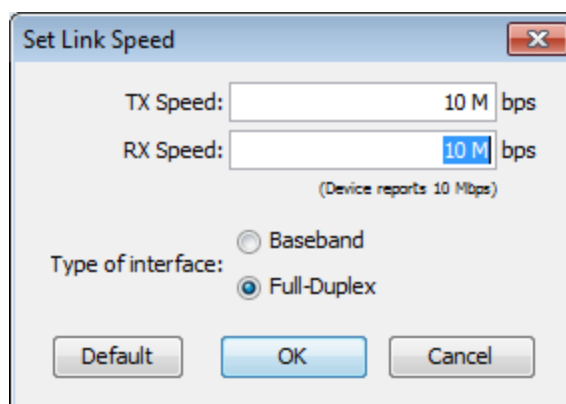
The following units are permitted:

- 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*.

The Detection Map

Use the Detection map to view devices that have recently been discovered on your network, and to add those devices to a map.

> **NOTE:** Before you can use the New Devices map, you must enable New Device Detection from the <u>server settings window</u>.

The Detection map shows all devices that have been discovered through Scheduled Auto-Discovery or through the Flows server. The Detection map differs from all other maps in the following ways:

- It shows only devices that are not on other maps.
- All devices are non-polling by default.
- When you attach a notifier, you don't attach it directly to a device. You choose whether to trigger an alert when a new device is discovered, and the source by which it is discovered (Scheduled Auto-Discovery or Flows server.)

For more information, see <u>Using the Detection Map</u>.

Using The Detection Map

Use the Detection Map to view all newly detected devices, and to move those devices onto maps.

Overview

Devices appear on the Detection Map from two sources:

- **Scheduled Auto-discovery** - if scheduled Auto-discovery is enabled, any device that responds to a ping from Intermapper appears on the Detection Map. The Detection Map is updated only when a scheduled Auto-discovery runs.

- **Flows Server discovery** - if Flows Server discovery is enabled and the Flows server is connected to a correctly configured Flows exporter, devices that show any activity appear on the Detection Map. The Flows Server runs continuously.

Moving Devices to a Map

When a new device appears on the Detection Map, you can move it to an existing map.

To move one or more new devices to an existing map:

1. Select the devices you want to move. If you want to move only one device, you can skip this step.
2. Right click the device(s)s and choose the map you want to move them to from the *Move to* submenu. The selected devices move to the specified map.

> **NOTE:** The devices on the Detection Map use the Non-polling probe. Once you move a device, select the probes appropriate to the device.

Getting an Alert When a New Device is Added

Any notifier can be attached to the Detection map. Most notifiers are attached to devices, networks, or interfaces, and are triggered based changes in their states. For devices that appear on a Detection map, you specify whether to trigger a notifier based on the source of the detection:

- **The Flows Server** - the notifier is triggered whenever the Flows Server reports a new device.
- **Scheduled Auto-Discovery** - the notifier is triggered when a device is discovered through Scheduled Auto-Discovery.

Deleting Devices from the Detection Map

In some cases you may never want to monitor a particular device.

To delete devices from the Detection map:

1. Click the pencil icon to make the map editable.
2. Select the devices you want to delete.
3. Press Delete. The selected devices disappear from Detection map.

> **NOTE:** The devices may reappear at some point, depending on how you have configured New Device Detection:

- **Scheduled Auto-discovery** - if you delete a device that was detected through scheduled Auto-discovery, the device re-appears when a new Auto-discovery cycle runs if the device is discovered during that cycle.
- **Flows Server discovery** - if you delete a device that was detected through the Flows Server, the device re-appears only when the Flows Server is restarted and activity is detected from the device.

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 Intermapper 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 (Mac) the device(s) you want to acknowledge.
   For interfaces, Right-click or Ctrl-click (Mac) the link.

2. From the Monitor menu or Context menu, choose *Acknowledge...* . 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.
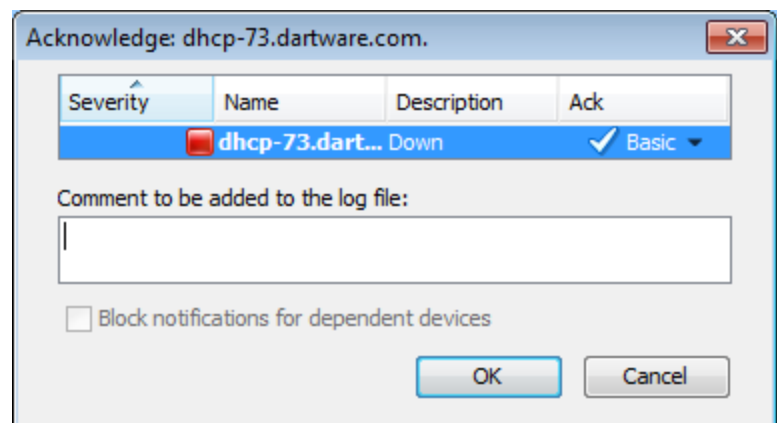
Basic, Timed and Indefinite Acknowledgments
Intermapper offers three kinds of acknowledgments for devices:

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 Acknowledgement* *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*
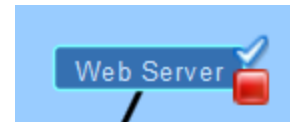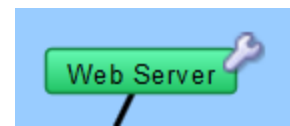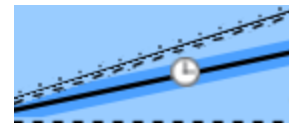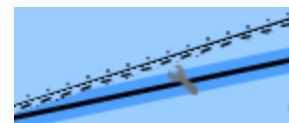
Notes:

- 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. 205).

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 (Mac) 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 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 (Mac), 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 (Mac) and choose *Acknowledge...* from the context menu.

You can *Un-acknowledge...* one or more links using Right-click or Ctrl-click (Mac) in the same way you acknowledge. This replaces the blue "X" with a red one, and re-enables any repeated notifications for that device.
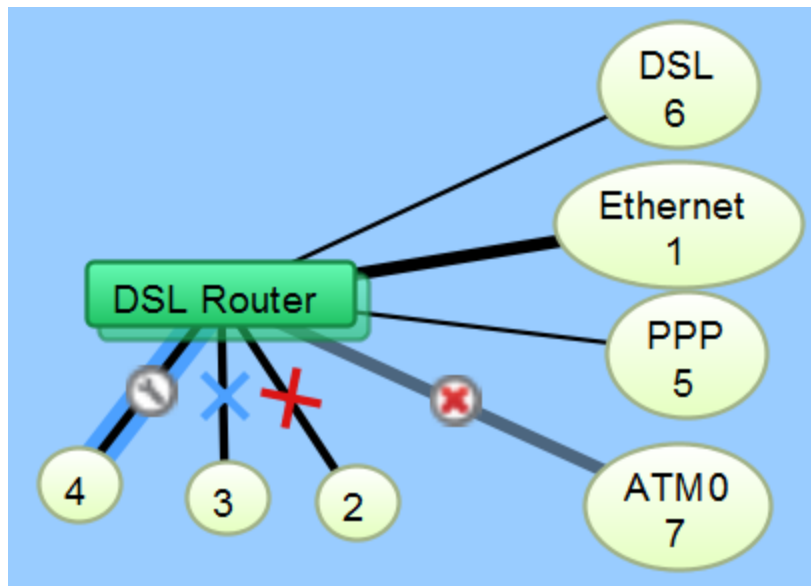
Various Link States

> 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.

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 (Mac)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 (Mac)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 (Mac)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 (Mac)the device and choose *Interfaces > Window...* from the context menu. The selected device's Interfaces window appears.

2. Click to select the first interface you want to set. The interface line is selected.

3. Shift-click (for contiguous lines) or Control-click (for non-contiguous lines) to select additional interfaces you want to set.

4. Right-click or Ctrl-click (Mac)the 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>`.

5. 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:

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

1. Right-click or Ctrl-click (Mac)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 (Mac)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 (Mac) 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.

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.
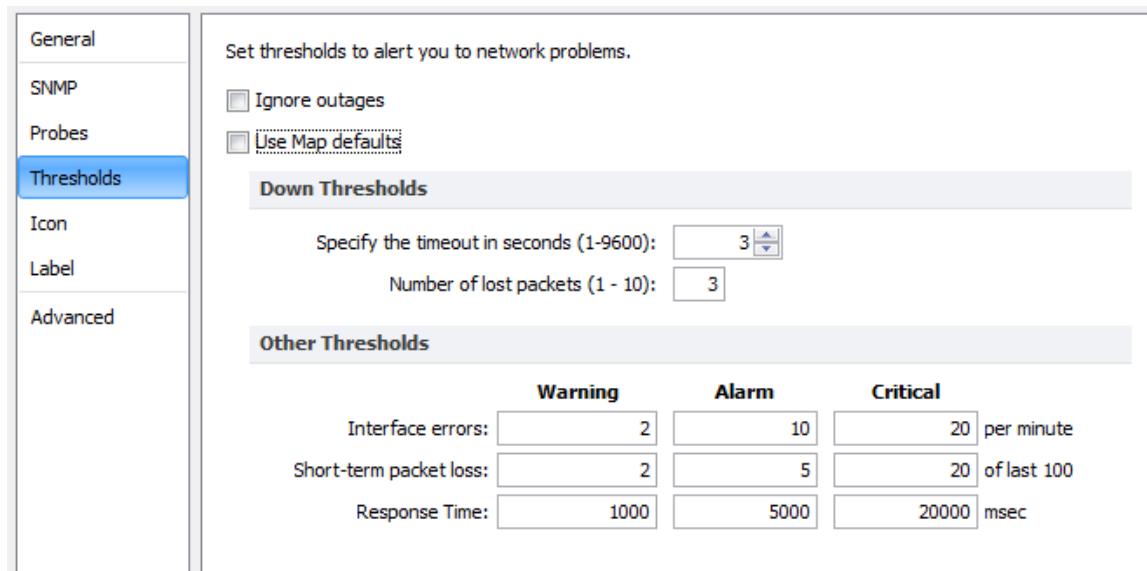
You can set any of the following thresholds:

- **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*Setting Thresholds for Probe Groups* 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 (Mac) 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](#) to turn on and configure traffic indicators for a map. You cannot set traffic indicators for a specific device or link.
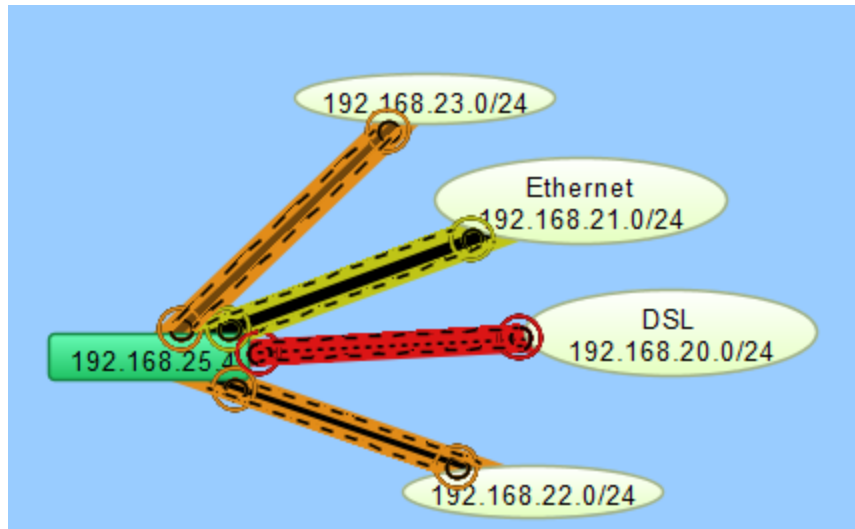
NOTE: Traffic indicators are part of Intermapper's "Animation" feature set. By default, animations are not turned on, as they do require some additional CPU resources. You can turn them on from the Animation Settings pane of the [Preferences window](#).

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.

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.

Files Tab
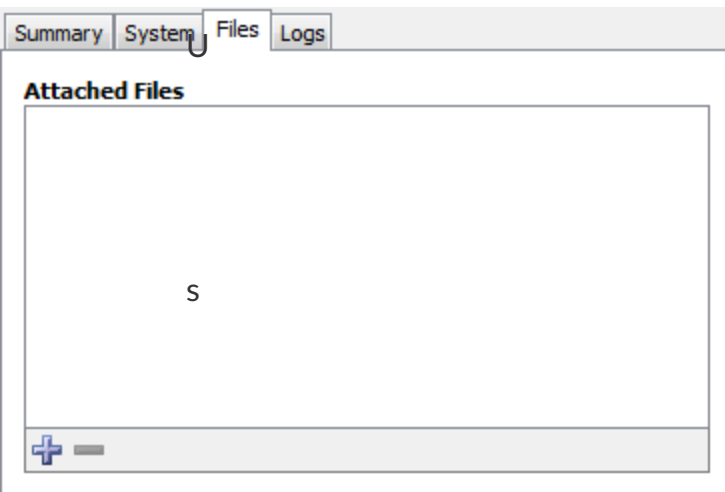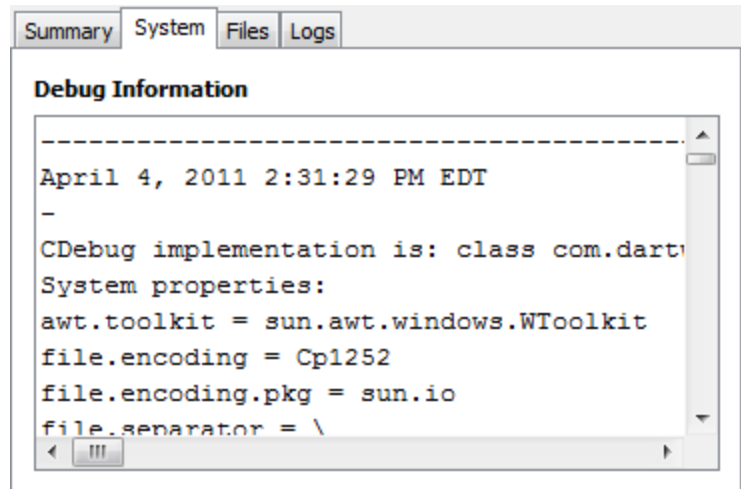
s

e
 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.
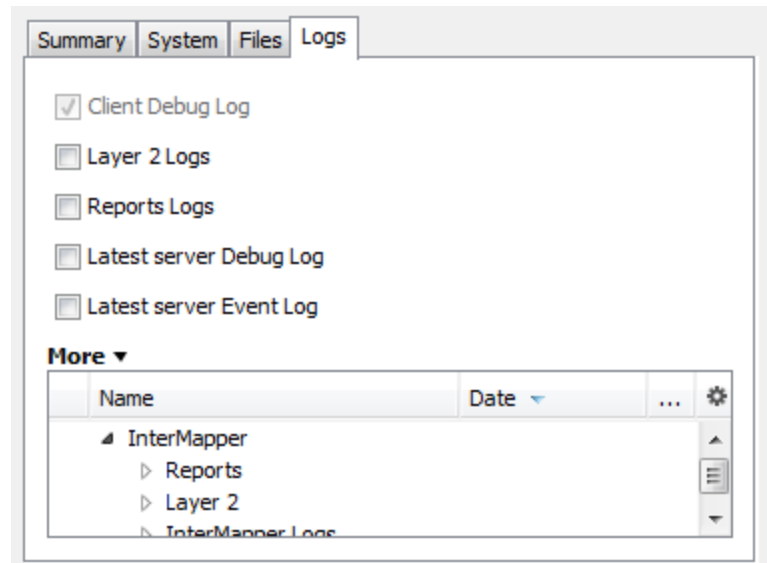
Creating Charts

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. 242)](#).

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.
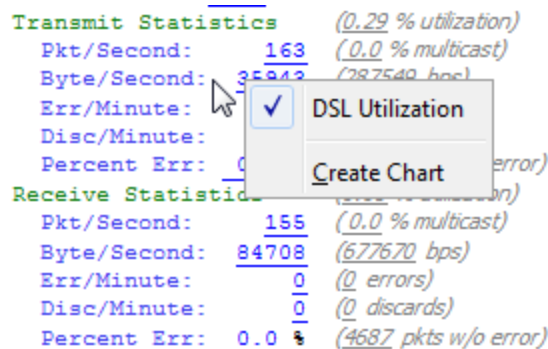
4. Click *Create Chart*. A new chart appears.

5. To add more variables to the chart, drag their underlined values to the chart. The example below shows a typical chart.
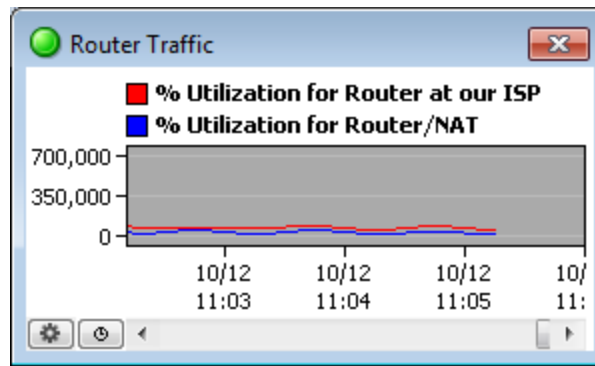
A chart showing two traces.

For more information about charts, see Using Charts. (Pg. 276)

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. 278) to view and hide charts.

You use the options available from the Chart Options menu to view and edit the parameters which control content and appearance of each chart.
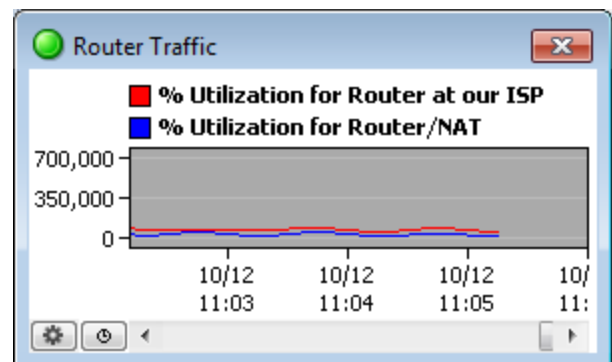
A chart showing two datasets.

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. 280).

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. 278).

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 [icon] 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 [icon] 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 <u>Viewing Status Windows</u> (Pg. 242).
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, available from the Chart menu (Pg. 278).

Deleting Charts

Use the *Delete Chart...* command, available from the Chart menu (Pg. 278) 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.

The Charts menu

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.
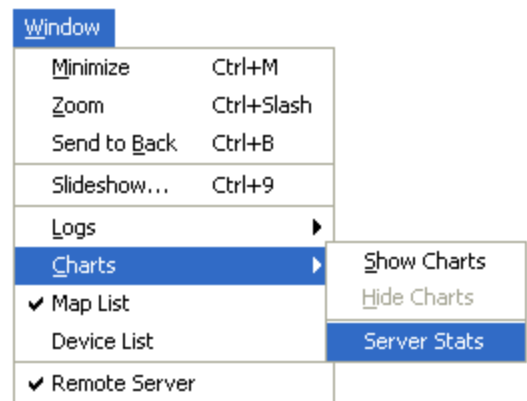
> **NOTE:** From the Charts list window, select one or more charts, then right/Ctrl-click a selected chart line and choose *Show Chart*.

The 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.
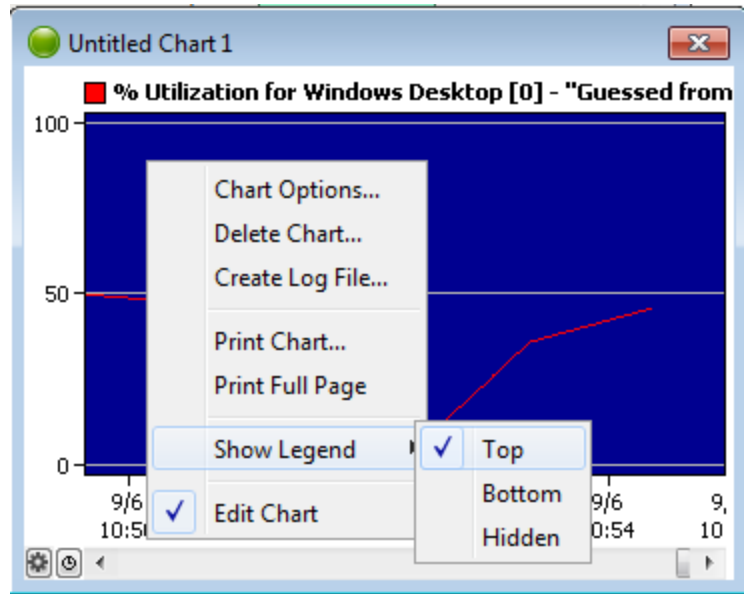
The Chart dropdown menu.

Chart Options... - Choose this option to view and edit parameters for the current chart. For more information, see Chart Options.

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 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. 278), 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. 299). When finished, click **OK**.

Specifying a chart log file

Each line of the tab-delimited file contains a date and time stamp and the current values of the variables defined by the chart.

To stop logging data to a log file:

1. From the Server Settings window, choose the Log Files (Pg. 299) 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 Linux and OS X, the command includes the location of the Intermapper daemon configuration file. Here's the syntax those platforms (see note below):

```
/usr/local/bin/intermapperd -f
/usr/local/etc/intermapperd.conf --chart-purge [# of days]
```

For Windows, use this syntax (see note below):

```
"C:\Program Files\InterMapper\InterMapper.exe" --chart-purge
[# of days]
```

The most recent **#of days** of chart data is retained; the rest is purged.

> **NOTE:** Both of the commands above require administrative privileges.
>
> - For Windows, open the `cmd` window using **Windows menu > Windows System > Command Prompt > Misc > Run as Administrator**, or similar, depending on your operating system and how you access the `cmd` window.
> - For Linux or OS X, the command should either be prefaced with `sudo`, or specified to be run as root.

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 execute 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.
- For Windows, open the `cmd` window using **Windows menu > Windows System > Command Prompt > Misc > Run as Administrator**, or similar, depending on your operating system and how you access the `cmd` window.
- For Linux or OS X, the command should either be prefaced with `sudo`, or specified to be run as root.
- If you have a large number of datasets with a substantial amount of accumulated data, the purge could take several hours to complete.

Log Windows

Intermapper writes information about interesting events into *log files* (Pg. 299). 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. 283)

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. 292)

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

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. 299)

> **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.
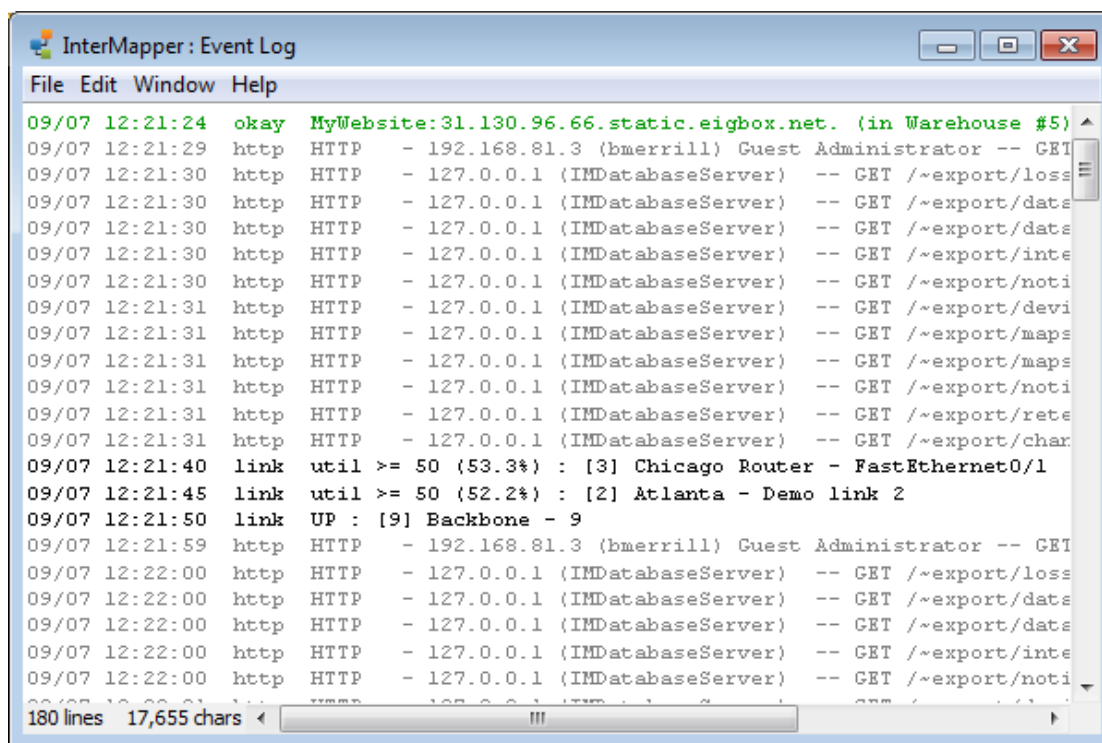
The main Event Log window. It can show information about device ups and downs, high traffic on links, web, telnet, and InterMapper RemoteAccess server connections, as well as error messages.

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>
    "alrm": <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*

imrmStopping 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 yyyy 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.

dbug "MyProbe: Can't match "MyProbe"", cFileName, lineStr

dbug "xxxx: Invalid Probe ID."

The probe xxxx contains an invalid ID (i.e., the package is not a valid string)

dbug "MyProbe: Invalid Probe Name.", cFileName

dbug "MyProbe: Invalid Probe Human Name.", cFileName

dbug "MyProbe: Probe definition does not contain a valid <description> section.", cFileName

dbug "MyProbe: Probe definition does not contain a valid <snmp-device-variables> section.", cFileName

dbug "xxxx: Probe definition does not contain a valid <snmp-device-display> section."

The xxxx probe file does not contain a valid <snmp-device-display> section.

dbug "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.

dbug "device-name UTIL[ifIndex]=util? type: upTimeNow=nn, upTimePrev=nn;inOctetNow=nn, inOctetPrev=nn; outOctetNow=nn, outOctetPrev=nn; bps=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.

dbug 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.

dbug An error occurred while attempting to save backup copy of *mapname*

InterMapper was not able to create a backup copy of the named map

dbug Can't locate backup folder to save backup copy of *mapname*

InterMapper couldn't locate or create the InterMapper Settings:Old Maps folder.

dbug 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.
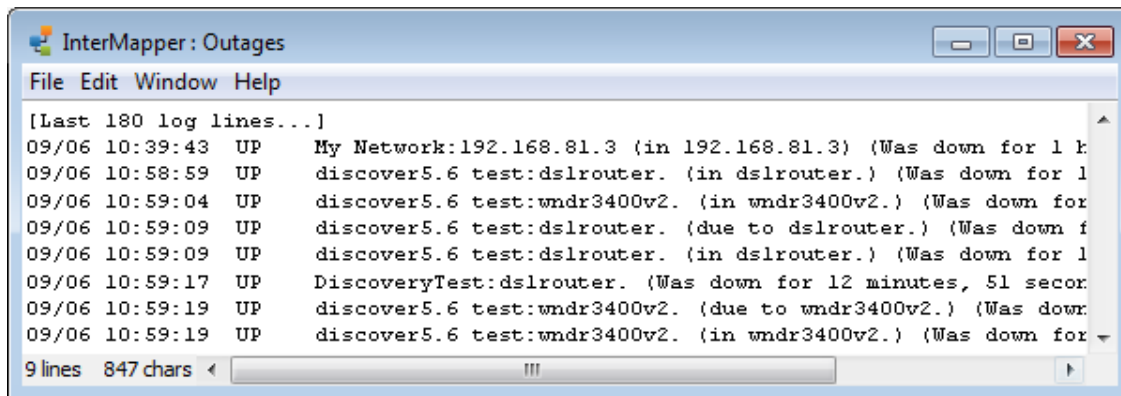
The Outages window shows the start and end time and the duration of outages.

The controls in the Outages Log window are identical to those of the other Event Log (Pg. 283) windows, and are described on that page.

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. 295) - view information about the Intermapper version. View and edit the server name and software licenses.
- Server Preferences Panels (Pg. 296) - set defaults and other preferences for your server.
- Server Configuration Panels (Pg. 318) - 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.
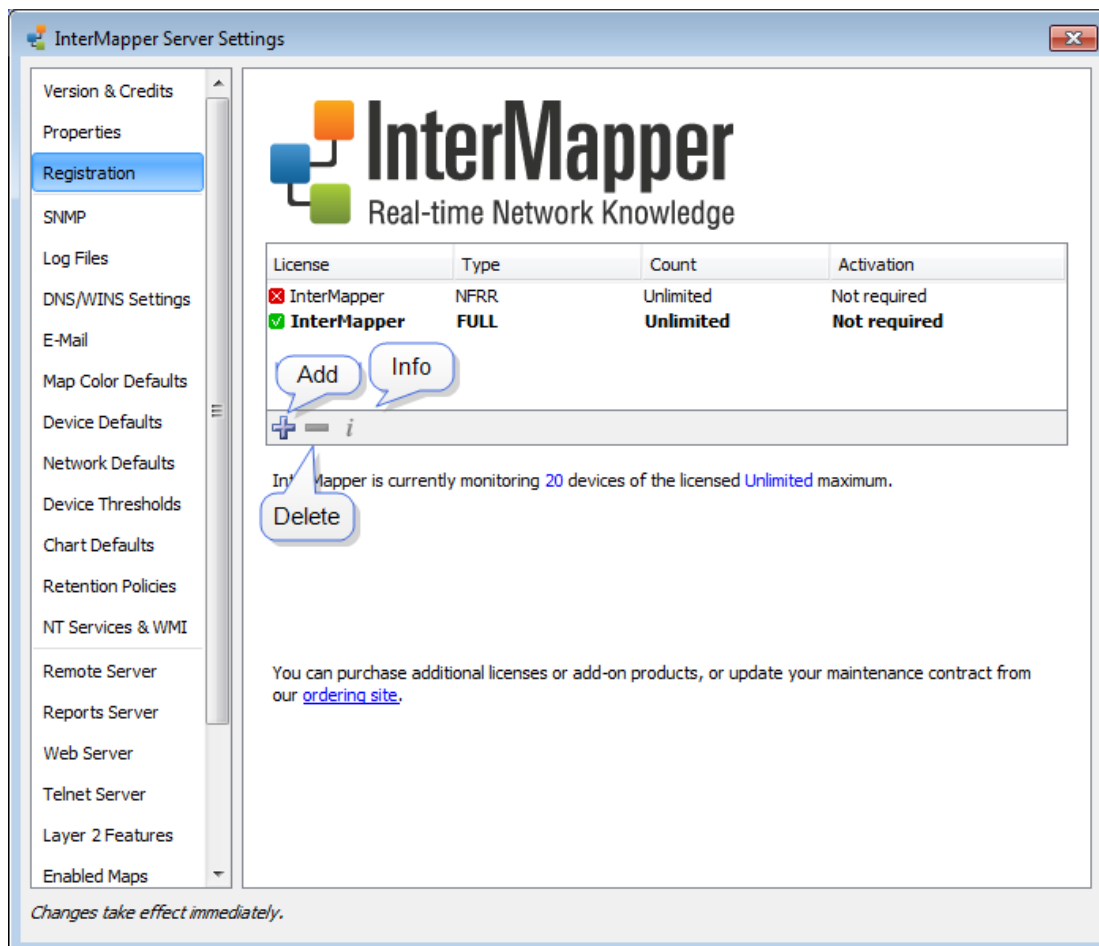
Use the Server Preferences section of the Server Settings window to view and edit default Intermapper's server settings.

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 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. 296)
- [Log Files](#) (Pg. 299)
- [DNS/WINS settings](#) (Pg. 303)
- [E-Mail](#) (Pg. 305)
- [Map Default Colors](#) (Pg. 306)
- [Device Defaults](#)
- [Network Defaults](#) (Pg. 308)
- [Chart Defaults](#) (Pg. 311).
- [Device Thresholds](#) (Pg. 310).
- [NT Services & WMI](#) (Pg. 316)

> **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. 157).

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:
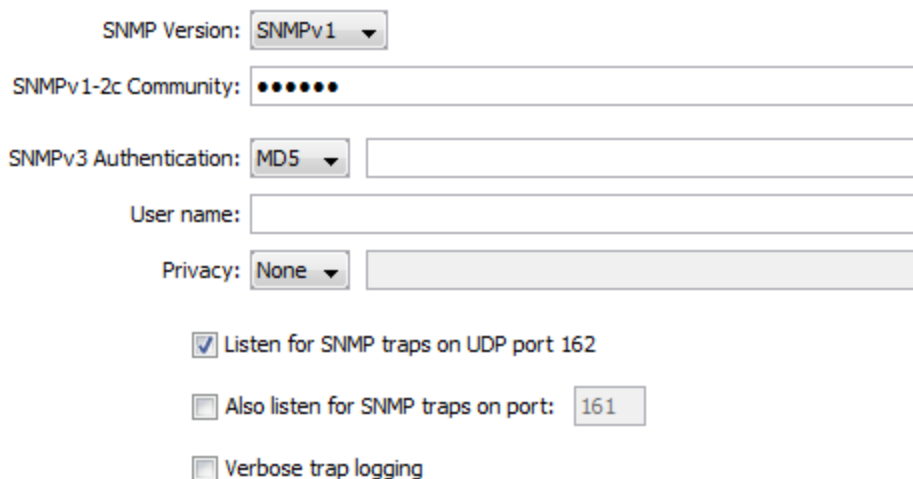
- **SNMP Read-only community string** - enables a remote device to retrieve "read-only" information from a device. Intermapper uses this information from devices on its maps.

- **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).

SNMP Version:	SNMPv1 ▾
SNMPv1-2c Community:	●●●●●
SNMPv3 Authentication:	MD5 ▾
User name:	
Privacy:	None ▾

☑ Listen for SNMP traps on UDP port 162

☐ Also listen for SNMP traps on port: 161

☐ Verbose trap logging

This pane allows you to specify the following:

- **SNMP Version** - Select the default SNMP   *Setting the default SNMP preferences* 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

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. 301) 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. 301) 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. 301) for the new log file appear.
2. Set the log file preferences   (Pg. 301) as described below.

To edit preferences for an existing log file:

1. Click to select the log file. The Log File preferences (Pg. 301) for the selected log file appear.
2. Set the log file preferences (Pg. 301) 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. 302) 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](#).

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.

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 uses 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: █

Revert to Factory Defaults

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. 157) 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:

The Device Defaults Panel

Network Defaults

The defaults for a network are shown below:

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. 176) Labels (Pg. 176).

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.

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. 264).

Set interface thresholds to alert you to network problems.

Error Thresholds

	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

Utilization Thresholds

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

Discard Thresholds

	Warning	Alarm	Critical	
Rx Discards (Received):	15	25	35	per minute
Tx Discards (Transmitted):	15	25	35	per minute
Total Discards (Rx + Tx):	15	25	35	per minute

The Default Interface Thresholds Panel

Chart Defaults

Charts (see Creating Charts (Pg. 275) and Using Charts (Pg. 275)) 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 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

The Axes Tab

to set the number of horizontal dividers and to set the number of 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 subdividers 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 *Highlight* menu to choose the icon to be drawn at the end of each line segment.
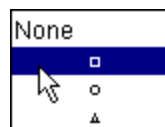
Colors Tab

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 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, the 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*:

- **None** - data is polled, but is not saved for charting or exporting.

- **Limited** - data is retained for the specified period. Enter a number and choose **day**, **week**, **month**, or **year**.

> **NOTE:** Up to 24 hours of additional data may be retained until the next time data is purged.

- **Forever** - all charted or exported values are saved to a local disk file.

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. 639) 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. 200).

In the left pane of the Server Settings window, click the button for the settings you want to edit, as follows:

- **Remote Server (Pg. 322)** - Start, stop, or edit settings for the Intermapper RemoteAccess server.
- **Reports Server (Pg. 325)** - Start stop, or edit settings for the Intermapper Reports Server.
- **Web Server (Pg. 327)** - Start, stop, or edit settings for the Intermapper web server.
- **Telnet Server (Pg. 329)** - Start, stop, or edit settings for the Intermapper Telnet server.
- **Layer 2 Features (Pg. 332)** - Turn on Layer 2 discovery for your server.
- **Enabled Maps (Pg. 333)** - View a list of available maps, enable or disable maps, and import or export maps.
- **Users** - View, Add, and Edit users and groups, and control access for users and groups.
- **Map Access (Pg. 336)** - Control access by any user or group to any map through the web server or remote server.
- **Map Backup** - Enable automatic map backups and create a schedule for backing them up.
- **Notifier List (Pg. 338)** - View, add, copy, edit and remove notifiers.
- **SSL Certificate (Pg. 340)** - 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. 321). 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.

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. 200).

In the left pane of the Server Settings window, click the button for the settings you want to edit, as follows:

- **Remote Server (Pg. 322)** - Start, stop, or edit settings for the Intermapper RemoteAccess server.
- **Reports Server (Pg. 325)** - Start stop, or edit settings for the Intermapper Reports Server.
- **Web Server (Pg. 327)** - Start, stop, or edit settings for the Intermapper web server.
- **Telnet Server (Pg. 329)** - Start, stop, or edit settings for the Intermapper Telnet server.
- **Layer 2 Features (Pg. 332)** - Turn on Layer 2 discovery for your server.
- **Enabled Maps (Pg. 333)** - View a list of available maps, enable or disable maps, and import or export maps.
- **Users** - View, Add, and Edit users and groups, and control access for users and groups.
- **Map Access (Pg. 336)** - Control access by any user or group to any map through the web server or remote server.
- **Map Backup** - Enable automatic map backups and create a schedule for backing them up.
- **Notifier List (Pg. 338)** - View, add, copy, edit and remove notifiers.
- **SSL Certificate (Pg. 340)** - 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. 321). 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:
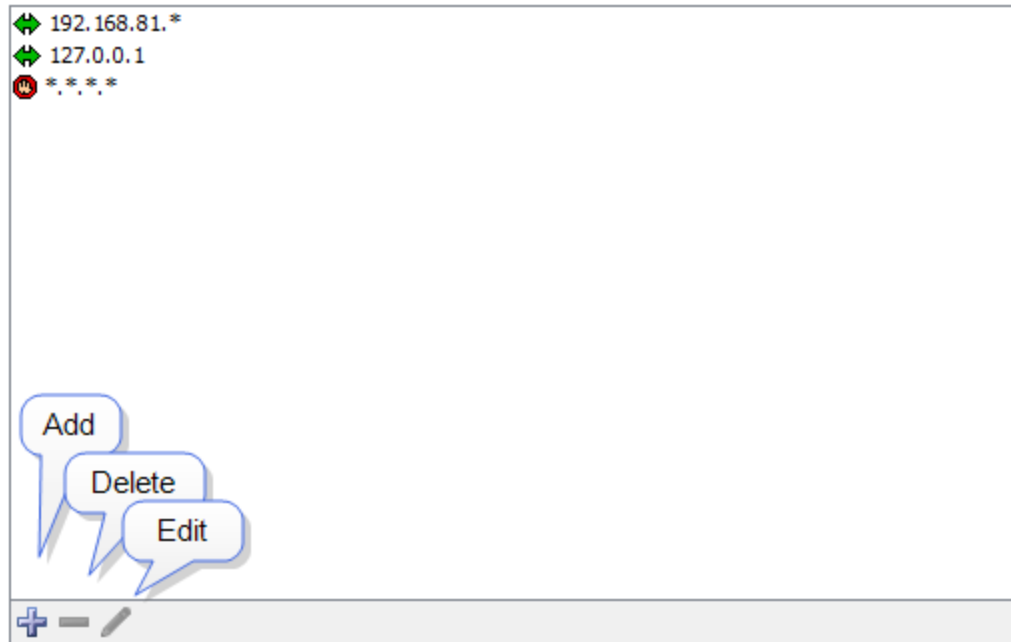
- If an incoming address matches an *Allow* address (or range), the connection is allowed.

- 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 Addresses and Ranges

You can enter addresses in the access control list or you can enter address ranges. For more information, see Entering an IP Address Range.

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.

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.

Notes:

- You can also control access through the InterMapper Authentication Server (Pg. 660), which connects to an external authentication server such as Radius, LDAP, or ActiveDirectory to authenticate a user. For more information, see Authentication Server (Pg. 660).

- 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](#) 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: 8181

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: Event Log ▾

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. 299).

> 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.
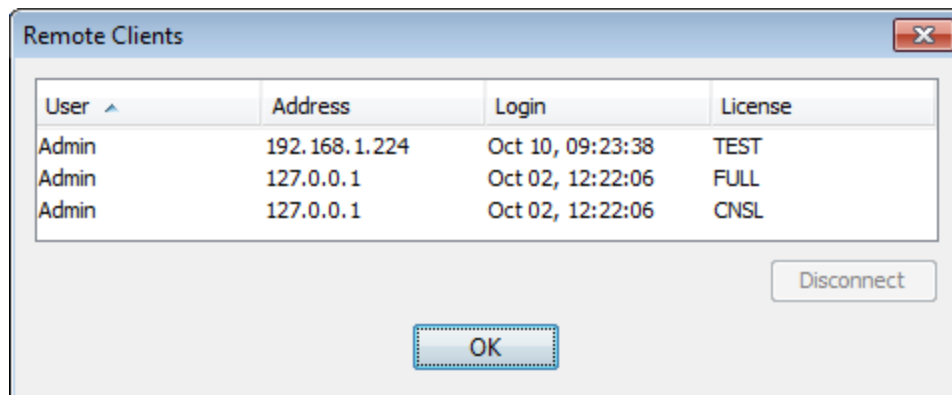
Additional Information

For more information on configuring your Remote Server, see Server Access Control (Pg. 321). 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. 319).

For more information on users and groups, see Users and Groups. 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. 336). 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.

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:
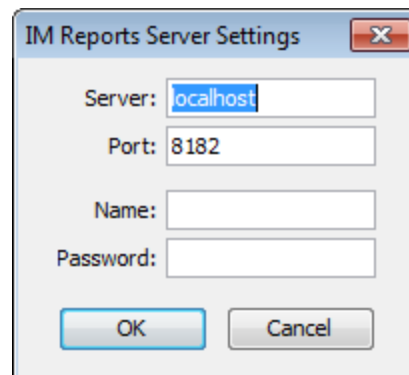
- Click *Start (Data collection for Reports)* .
- Click *Stop* to stop data collection.

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.

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. 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.

> **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. 319).

- 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. 321). 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. 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. 336). 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.

Setting the Default Refresh Interval
Use the **Default Refresh** dropdown, located in the upper-right corner of the Web Server Settings pane to set the refresh rate that a web page uses by default.

- When you change the value on a web page, the new value is remembered for you for that page.

- Each web page has its own value.

- The value is remembered for the page even if you navigate to it with a link.

- The value is remembered for the page if a link opens it in a new tab or 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. 319).

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:

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. 321). 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. You can also see a variety of options for specifying IP address in Entering an IP Address Range.

For more information on users and groups, see Users and Groups. 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

Version: 11

Name: Local AutoMate Server ☑ Enabled

Host: localhost Port: 11011

Password: •••••

Polling Interval: 0

[Test]

Server System Tasks

	Event	Task	⚙
☐	Server startup		
☐	Log file rotation		
☐	Map backup comp...		

Version - Enter the version of the selected AutoMate server

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 Intermappers 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.

- **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.
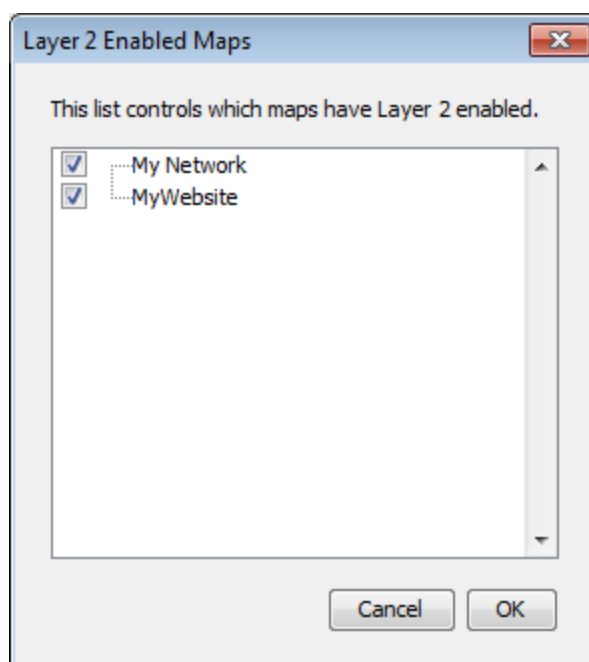
NOTE: In order to use the Layer 2 features in your map, *after* enabling Layer 2 features in the Server Settings window, you must enable them in the Map Settings window for each map that contains Layer 2 devices.

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.

```
☑      Administration Offices
☑      discover5.6 test
☑      DiscoveryTest
☑      Example.com National Map
☑   ▷  📁  Example.com National Map
☑      My Network
☑      MyWebsite
☑      Vantage Point
☑      Warehouse
```

🗀 🗑 ⚙ ▾ 11 maps
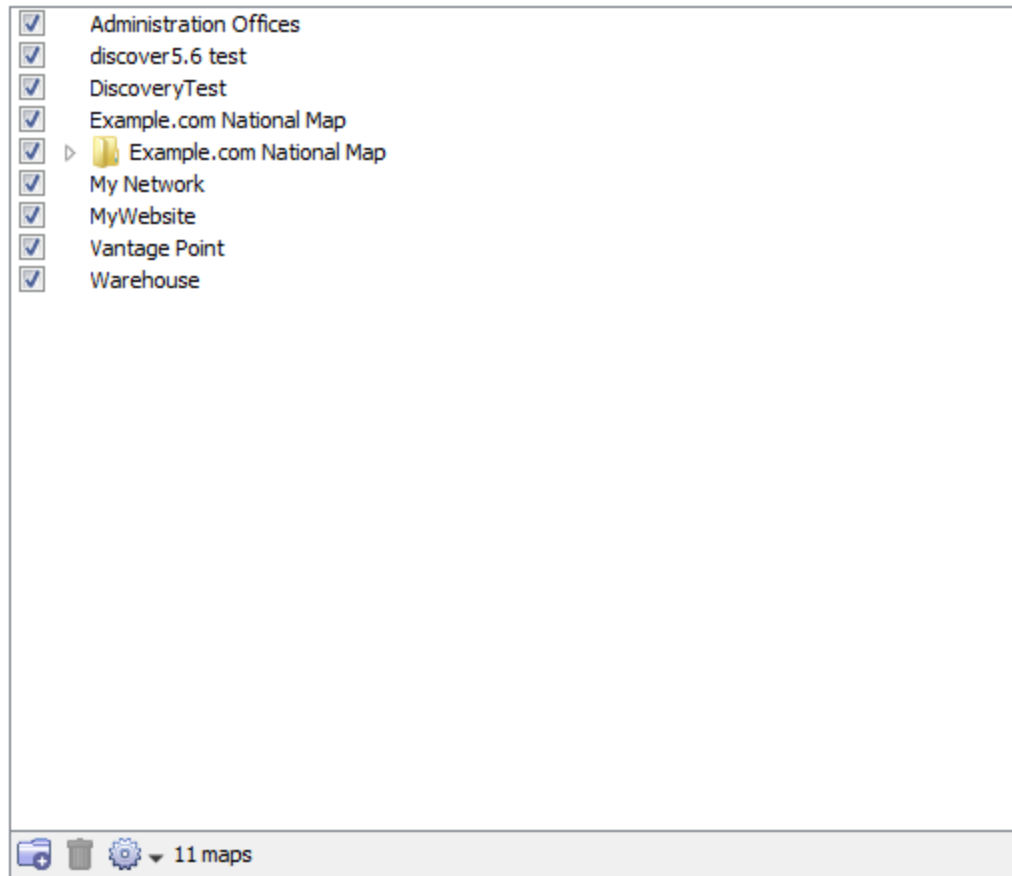
- **Checked maps** - these maps are active. Intermapper actively polls everything on the map.
- **Unchecked maps** - these maps are not "active". Intermapper does not poll the devices on those maps.

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.

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.
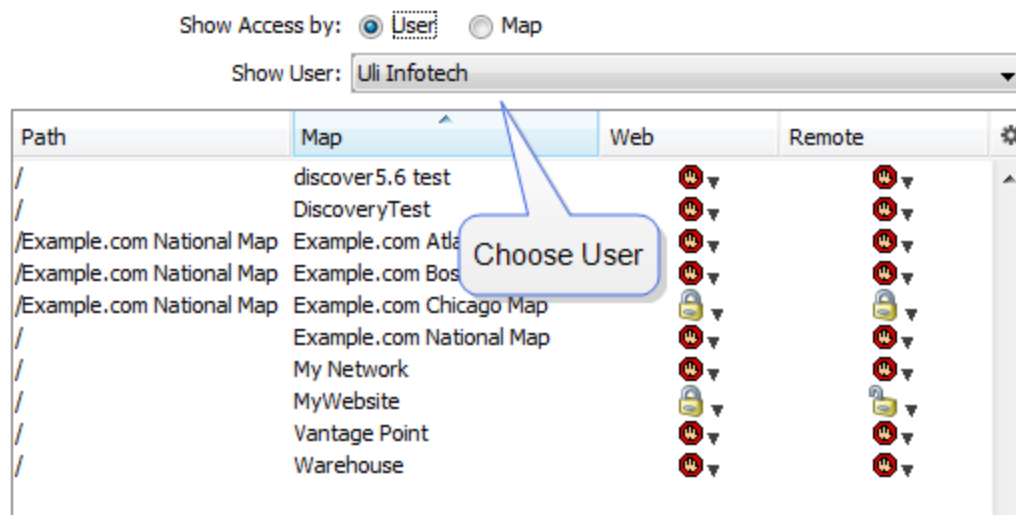
- To **set a user's access for any open map**, choose the user from the *Show User* dropdown menu.
- To **allow access to the selected map through the Web server**, click the icon in the *Web* column for the user or group whose access permissions you want to set, then select a permission level.
- To **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.

- To **set access for all maps at once**, Alt-click or Cmd-click (Mac) the Web or Remote dropdown for any map in the window. When you choose from the menu, the value in the selected column is set to the same value for all maps.

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.
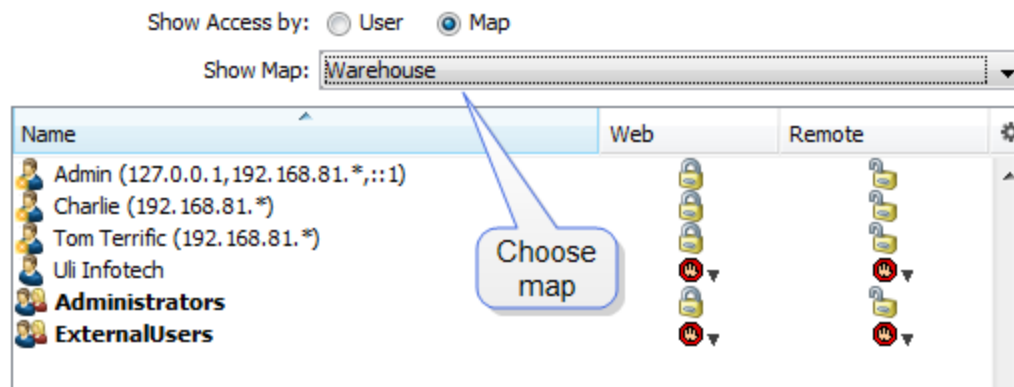
- To **set access control parameters for any open map**, choose that map from the *Map Name* dropdown menu.

- 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.

- To **set access to the selected map for all users at once**, Alt-click or Cmd-click (Mac) the Web or Remote dropdown for any user in the window. When you choose from the menu, the value in the selected column is set to the same value for all users.

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.

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. 200).

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.
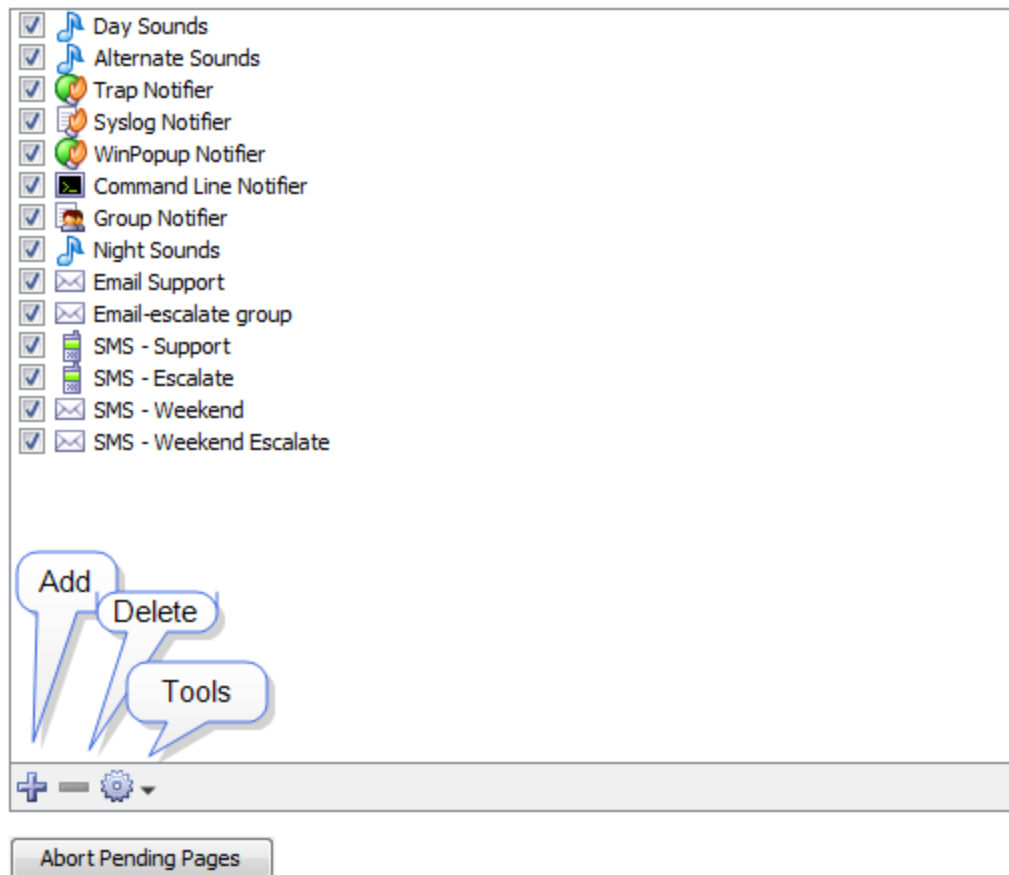
Notifier List Panel

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. 200).

- **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

InterMapper is currently using a sample SSL certificate that will encrypt sessions using a known private key. All versions of InterMapper ship with the exact same certificate and private key. Although the data between the client and server are encrypted, this configuration offers no security from spoofing or eavesdropping by a determined attacker using the proper tools.

To increase security, you should create your own certificate. To do this, create a new "Certificate Signing Request", then sign it yourself (for example, using OpenSSL) or use a commercial certificate authority. When you have the new SSL certificate, upload it by clicking the button below. Please refer to the InterMapper documentation for more details.

Create CSR...

Upload Certificate...

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.
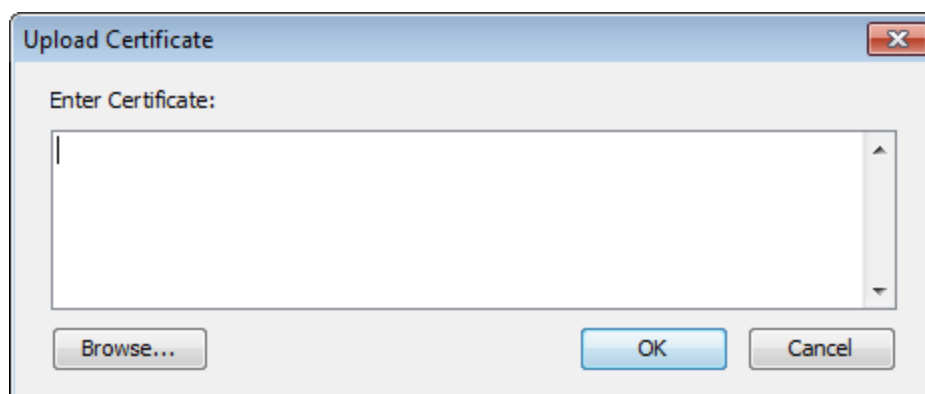
At the conclusion of this, the InterMapper Settings:Certificates folder contains files named:

- **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.

Configuring New Device Detection

Use the New Device Detection panel to enable and configure new device detection.

New Device Detection through InterMapper Flows Server

New Device Detection can be done through InterMapper Flows server with no Flows license.

Flows server is not running. New Device Detection will take effect when Flows server starts.

☐ Run New Device Detection with Flows server

     ☐ Turn off Flows data collection

New Device Detection through Scheduled Auto-Discovery

New Device Detection can be also done through Scheduled Auto-Discovery.

☐ Run New Device Detection with Scheduled Auto-Discovery

- Run New Device Detection with Flows server - check this box to use the Flows server for new device detection.
- Turn off Flows data collection -
- Run New Device Detection with Scheduled Auto-Discovery - check this box to use the Flows server for new device detection.

Methods of New Device Detection

Choose two different methods of device detection:

1. Use Intermapper Flows server - queries a Flows exporter to find new devices.
2. Use Scheduled Auto-Discovery - the Intermapper server performs Auto-Discovery as scheduled, searching only for new devices.

Which Method(s) Should I Use?

The two methods described above are not mutually exclusive. You can use both methods at the same time. Each has its advantages and disadvantages:

Using the Flows Server for Detecting New Devices

- When enabled, new device detection runs continuously. (It cannot be scheduled.)
- A Flows license is not required, but you must set up a Flows exporter to use this feature.
- This method detects devices that actively generate network traffic, and so could discover devices that might otherwise be missed by Auto-Discovery.

Using the Scheduled Auto-Discovery for Detecting New Devices

- When enabled, uses the same methods as regular Auto-Discovery, but queries only IP addresses that are not already on in the device list.

- You can use this method to schedule discovery of new devices to run as often as every half hour. This method may put additional load on the Intermapper server, so you have the option to schedule discovery for off-peak periods such as nights and weekends.

- This method actively probes devices, so may discover devices that are not generating network traffic and thus are not discovered using the Flows server.

The Detection Map

As soon as you enable either method method, a new map appears in the map list, named *DetectionMap*. All new devices (ones that do not currently appear in the Device List) appear in this map. Once discovered, you can move these devices to other maps. For more information, see [Using The Detection Map](#)

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
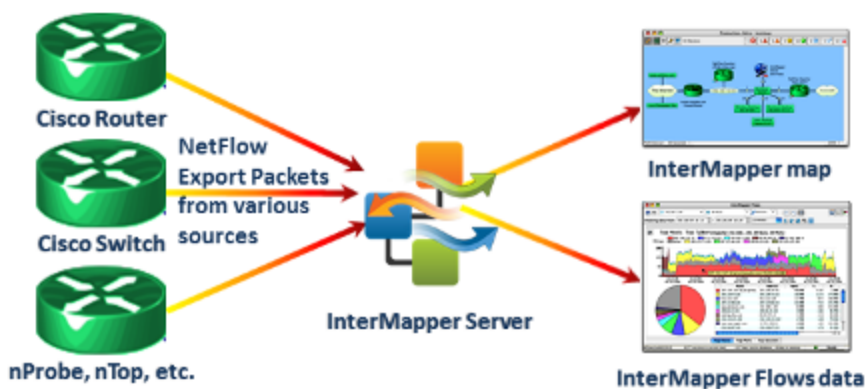
Intermapper Flows collects and stores Flows data from any device that supports its collection (Flows Exporter). For information on supported devices, see Supported Exporters You can choose the available exporters from which you want to collect data. For more information, see Flows Settings - Exporters Tab.

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:

- **See all Flows data** - *right-click* or *ctrl-click* a server in the Map List window and choose *Flows Window*. This is an unfiltered view of your Flows data; no filters are set.

- **See Flows data for a specific exporter's interface** - *right-click* or *ctrl-click* a link on a device that shows an exporter device badge and choose *Show In > Flows Window*. The Exporters filter is set to the selected exporter.

> **NOTE:** The Exporter badge appears for any device that appears in the list of Flows exporters. For more information, see Flows Settings - Exporters Tab

- **See all Flows data for a device** - *right-click* or *ctrl-click* a device and choose *Show In > Flows Window*. The Device filter is set to the selected device. If the device has the same IP address as an exporter, that exporter is selected in the Exporters filter and you are viewing data only for that exporter.

For more information on filters, see Filter Tools below.

Understanding the Flows window

Use the Flows window to view Flows data in a number of ways.
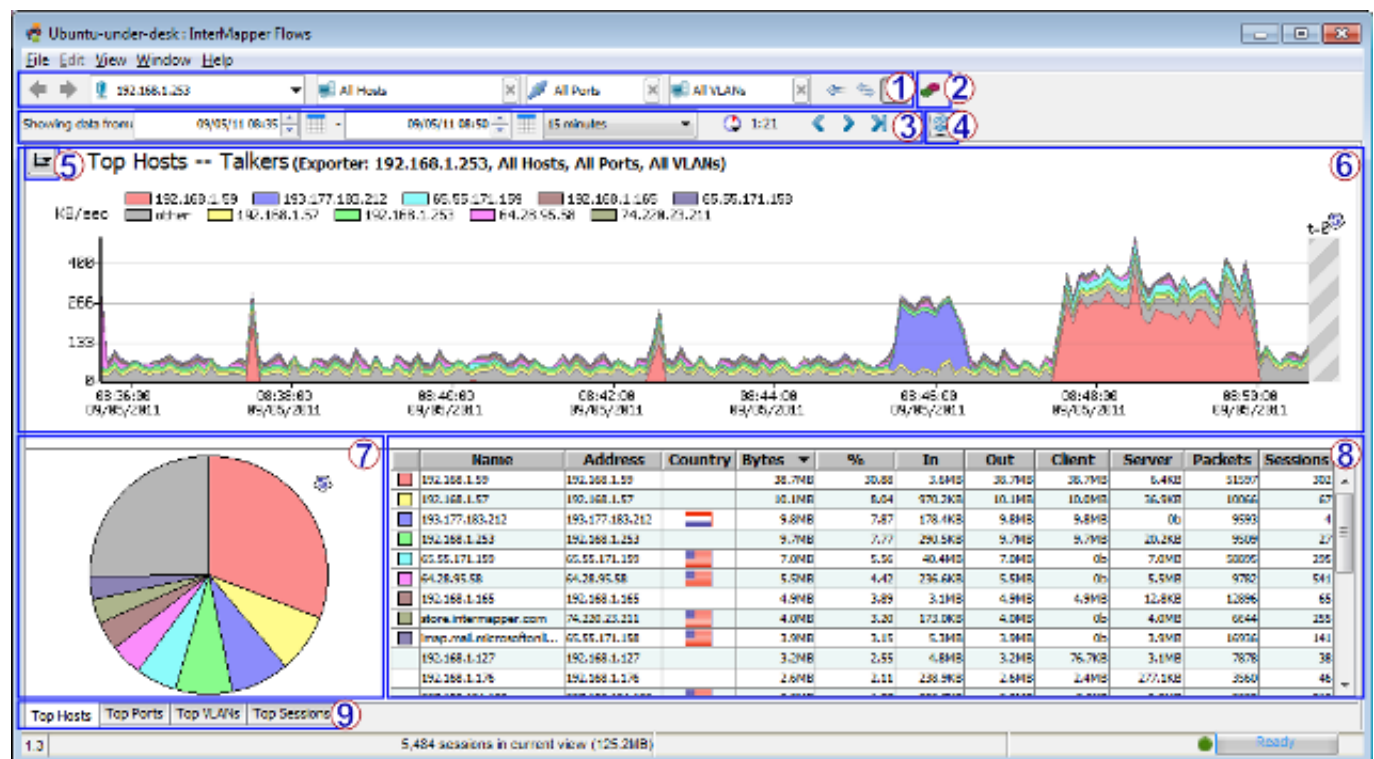
When you first open the Flows window, the Hosts tab is selected.

- **1: Filter tools** - select the subset of Flows data you want to view.
- **2: Intermapper Flows Settings** - view and edit Intermapper Flows settings.
- **3: Time Range Selection tools** - select and navigate Flows data over a specified period.
- **4: Refresh button** - 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** - view a list of top talkers, listeners, or both, with stack and pie charts showing the relative activity of each.
- **Top Ports tab** - 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** - 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.
All Exporters (7)	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.
All Hosts	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.
All Ports	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.
All VLANs	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, Top Ports, or Top Sessions tab.
443/TCP	**Exclude Host/Port/VLAN**	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.
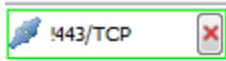
Time Range Selection

Use the time range selection controls to view and select a range of time for which you want to view.

Showing data from: 12/17/09 08:23 - 12/17/09 08:38   15 minutes

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...		Choose this command from the File menu to save a PDF report to disk. A standard file dialog appears. The report contains the Top Hosts, Top Ports, and Top Sessions tabs.
Print...		Choose this command from the File menu 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 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:
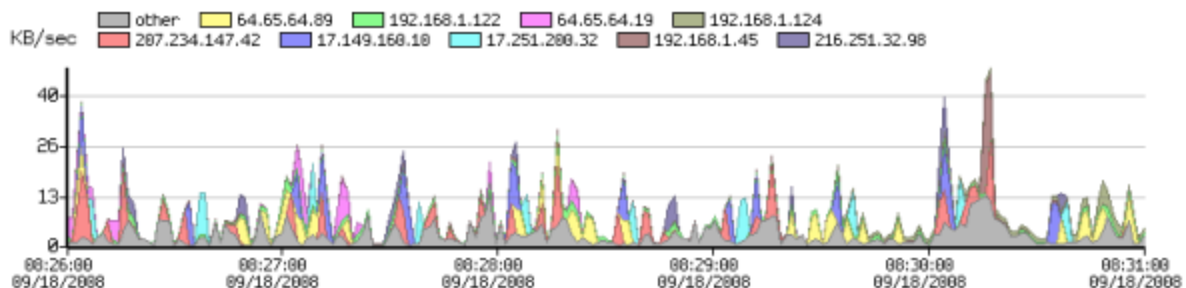
The legend above the chart shows the top hosts for the data you are currently viewing.

- 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.
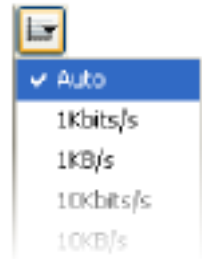
The Pie Chart

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		385.5 KB	13.03	41.7 KB	385.5 K	3.9K B	381.6 KB
	example.net	64.65.64.89		343.3 K	11.61	35.2 KB	343.3 KB	0b	343.3 KB
	nwk-www.example.com	17.149.160.10		267.7 KB	9.05	12.9 KB	267.7 KB	0b	267.7 KB
	dhcp-122.dartware.com	192.168.1.122	🇺🇸	223.0 KB	7.54	1.1M B	223.0 KB	217.5 KB	5.5K B
	cup-www.example.com	17.251.200.32		189.9 KB	6.42	8.1K B	189.9 KB	0b	189.9 K
	vws.example.net	64.65.64.19		142.3 K	4.81	17.2 KB	142.3 KB	0b	142.3 KB
	nitro.dartware.com	192.168.1.45	🇺🇸	141.1 KB	4.77	670.4 KB	141.1 KB	74.2 KB	66.9 KB
	dhcp-124.dartware.com	192.168.1.124	🇺🇸	125.1 KB	4.23	76.6 KB	125.1 KB	83.9 KB	41.2 KB
	hosting.example.com	216.251.32.98		115.8 KB	3.91	8.5K B	115.8 KB	0b	115.8 KB
	eclair.example.net	64.65.64.64		98.1 KB	3.32	18.8 KB	98.1 KB	0b	98.1 KB
	outgoing02.example.net	64.65.64.125		69.2 KB	2.34	26.0 KB	69.2 KB	0b	69.2 KB
	192.168.1.12	192.168.1.12	🇺🇸	63.3 KB	2.14	67.8 KB	63.3 KB	25.5 KB	37.8 KB
	<up to 25 rows>								
	Other	Other		396.5 KB	13.40	555.8 KB	396.5 KB	118.5 KB	278.0 KB

- **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:
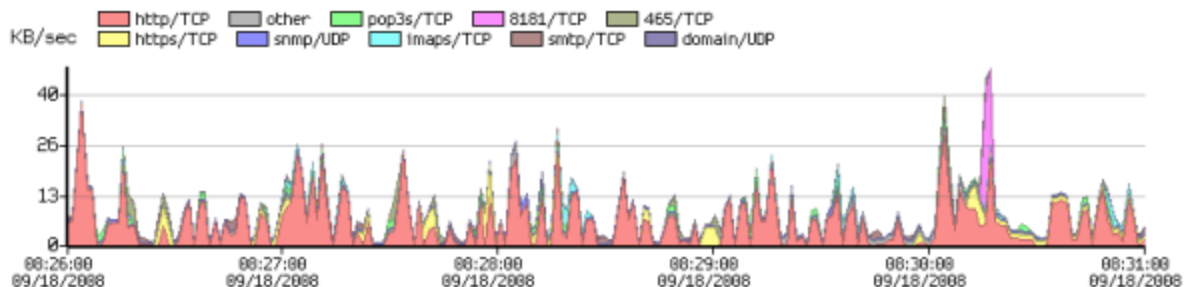
- Click a legend above the Stack chart to select the corresponding line in the Port list.
- Mouse over an area of the Stack chart to view port information for that activity.
- Click an area of the stack chart to select the corresponding line in the Port list.
- Click and drag to select a region of the 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.
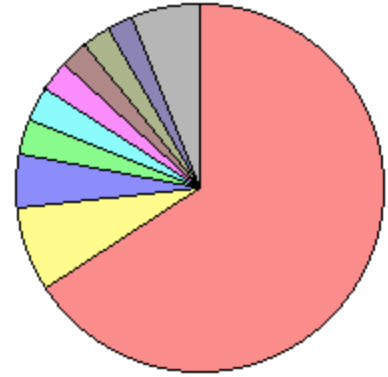
- Click a pie segment to select the corresponding line in the Ports list.

- 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

	VLAN	Bytes	%
	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* tab to choose which exporters you want to collect from.
- Use the *Appearance* tab to select a coloring theme for protocols and hosts.
- Use the *Preferences* tab to set parameters that control behavior of Intermapper Flows.
- Use the *Advanced* tab to set performance-related parameters, the path to your database, and a database size.

Exporters tab

Use the Exporters tab to select the exporters from which you want to collect data.

InterMapper Flows Settings

Enabled	Status	Expand	Exporter	Tag	Version	Total Flows	Flows/hr	Latest Update
✔	●	▶	10.65.49.38		NetFlow 9	257327	264	02/09/18 11:01:1
✔	●		10.65.49.12		SFlow 5	240860	54	02/09/18 11:02:2
✔	⚠	▶	10.65.48.100		NetFlow 9	1671767	18956314	12/04/17 16:47:0
✔	●	▶	0:0:0:0:0:0:0:1		NetFlow 9	227125	914	02/09/18 11:02:4

NetFlow port: 2055   ⑦   Database remaining: ~2 hours   ⑦
sFlow port: 6343   ⑦   Add sFlow Exporter   ⑦

OK   Cancel

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 ad 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.
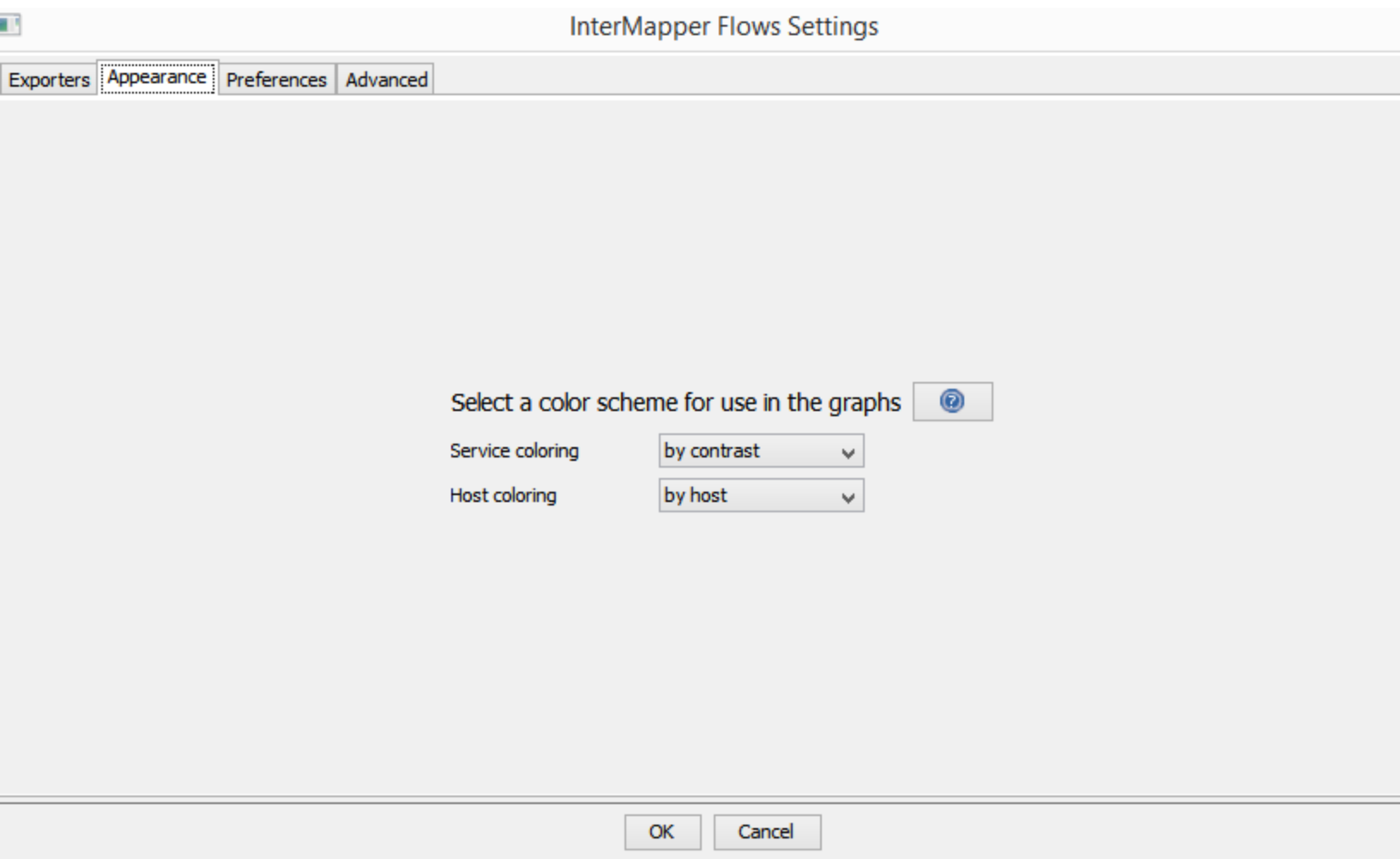
Choose color schemes as follows:

- **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.
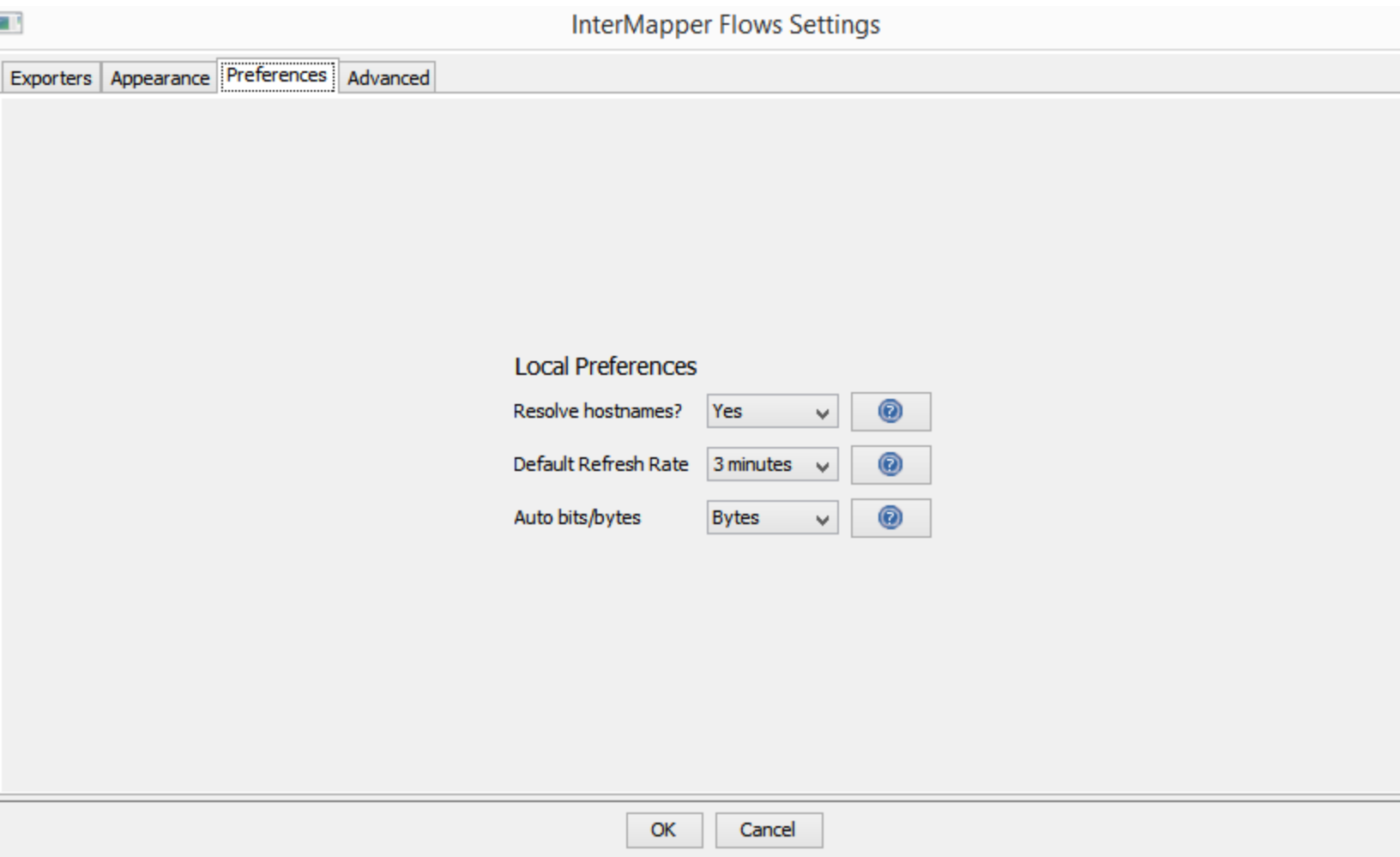
Local Preferences

- **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.

InterMapper Flows Settings

| Exporters | Appearance | Preferences | Advanced |

Performance

Server threads
1   2   3   4   5   6

Cache size
64MB   128MB   256MB   512MB   786MB   1GB   1.5GB   2GB   2.5GB   3GB   4GB

Storage interval
300 s   120 s   60 s   30 s   10 s   5 s

Database Configuration

Current Database Information

Database path   L:\ProgramData\InterMapper\InterMapper Settings\Flows\SESSIONDB

Database size   medium

Please note that database size changes do not take effect immediately.
Selecting a larger database size WILL cause the database to grow to that size, even if the requested size is later
reduced again.

OK   Cancel

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.

> **NOTE:** - 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.

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 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
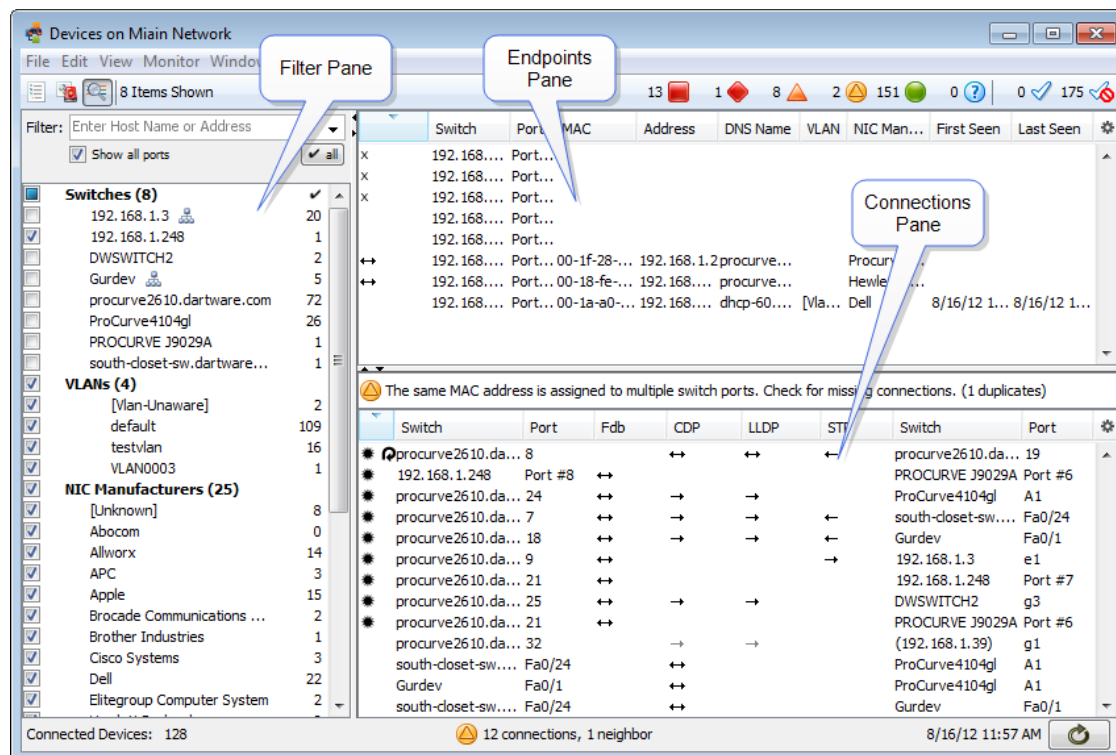
Understanding the Layer 2 View

The Layer 2 View contains three main panes:

- The **Endpoints pane** - 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** - 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** - 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 for more information.

Use these methods to control the filter criteria:

Filter:	Enter Host Name or Address	
☑ Show all ports		
☑ ⊟ **Switches (8)**		
☑	⊞ (192.168.1.5)	0
☑	⊞ dell3424-sw.dartware.com.	9
☑	⊞ procurve2610-sw.dartware....	84
☑	⊞ procurve4104gl.dartware.com.	24
☑	⊞ racklinksys.dartware.com.	0
☑	⊞ south-closet-sw.dartware.com.	14
☑	⊞ srw208.dartware.com.	3
☑	⊞ trendnet.dartware.com.	3
☑ ⊟ **VLANs (5)**		
☑	default	115
☑	Vlan 2	15
☑	Vlan 3	2
☑	Vlan 4	1
☑	Vlan 600	1
☑ ⊟ **NIC Manufacturers (26)**		
☑	⊞ Abocom	0
☑	⊞ Allworx	13
☑	⊞ APC	4
☑	⊞ Apple	22
☑	⊞ Asustek Computer	1
☑	⊞ Brocade Communications Sys...	2
Connected Devices: 137		

- 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 addtional filtering capability. Enter a hostname or address in the *Filter box* to limit the devices shown in the Endpoints pane. See [Using the Filter Box](#) below for many more options.
- Certain flags appear next to entries. See [Understanding Layer 2 Flags](#).
- 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.

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.)

- 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 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 detecting 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....	csww2k8....	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 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 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

---

← or → **Interior device** - The device is attached to a hub or switch that is connected between ports of two managed switches. The left or right arrow points away from the spanning tree root.

ˣ **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.

← or → or ↓ **Fuzzy** - The Layer 2 process cannot determine the exact port where the device is attached. See [Understanding Fuzzy Devices](#) below.

▢ **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](#) 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](#) 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).

← or → **Not present on Map** - Port is connected to a device that is not present on a Layer 2-enabled map.

Ω **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.

> **NOTE:** Layer 2 mapping can only display information returned from a Layer 2 scan.For example, if a switch's `dot1dTpFdbTable` (BRIDGE-MIB) is missing or sparsely populated, the Layer 2 scan may fail to return the connections, so they can't be shown.

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](#). 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.
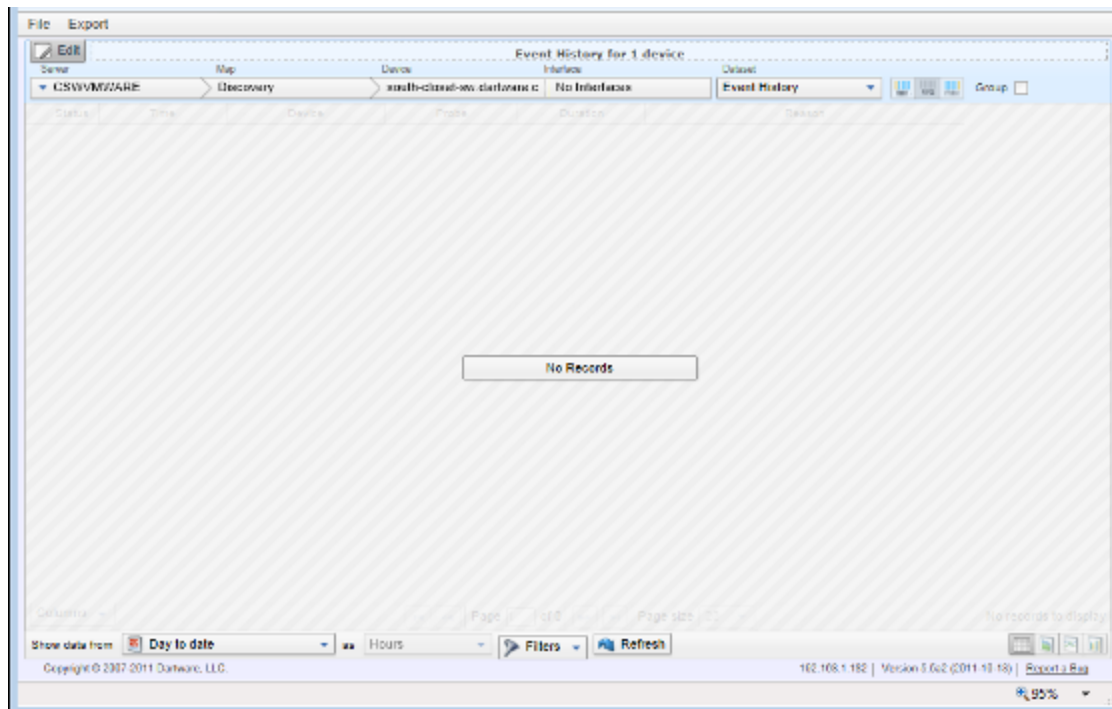
Intermapper Reports window in View mode

Two other ways you can also open the Reports window:

- Use this URL:

    https://[InterMapper Server address]:8182/~imreports/

- 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.
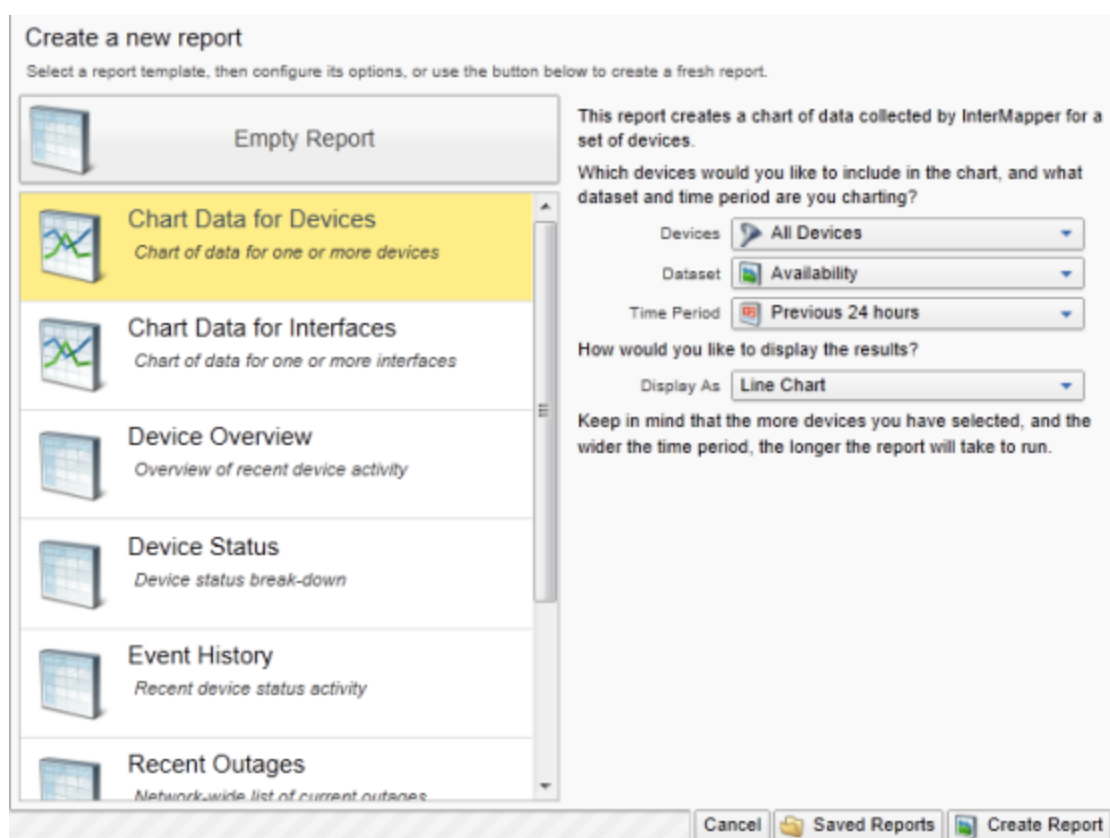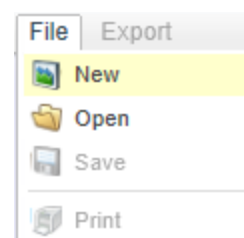
The Templates List

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.)
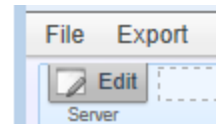
Editing a Report

The image below shows the controls you can use to fine-tune your report definition.
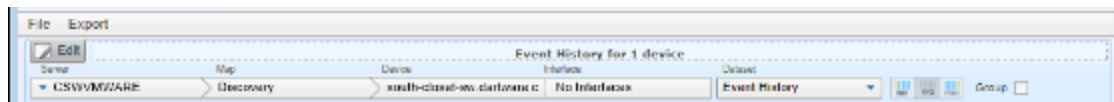
Intermapper Reports window in Edit mode

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.

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.

To select data sources:

- Click anywhere in the source selection bar shown above. A selection tree appears, as shown below.
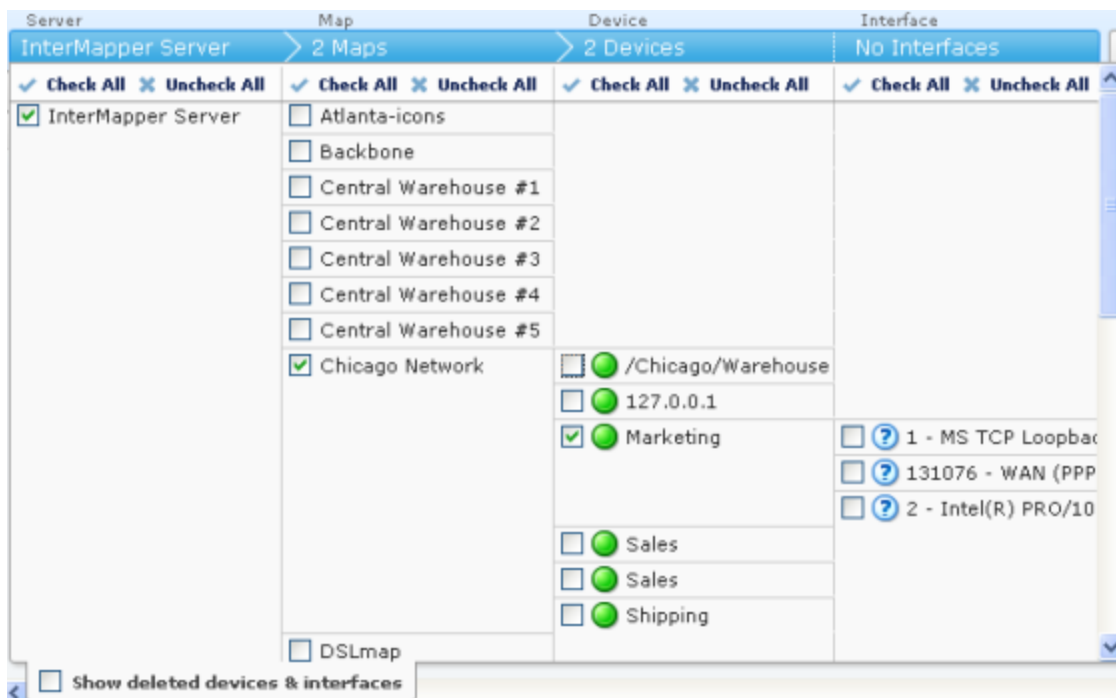
- Select or clear the check boxes for the devices or interfaces whose source data you want to include in the report.

- 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 dropdown menu, near the right of the device selection controls, choose a dataset.
  Assuming you are still in Table view, a list of values appears.
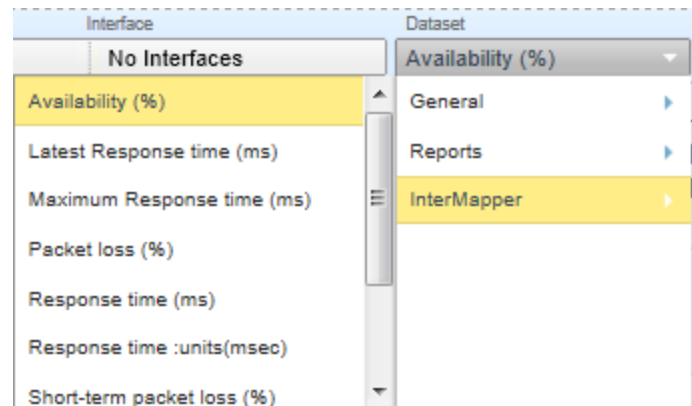
Selecting Data Grouping

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.
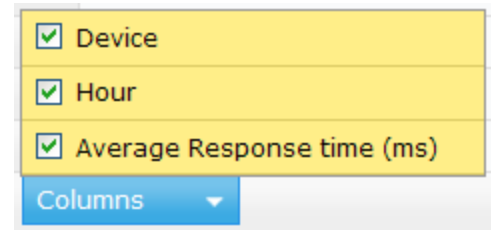
Using the Page Controls

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
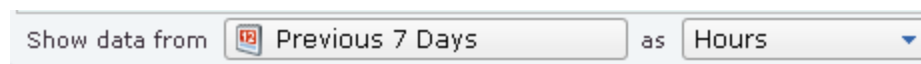
You can limit the amount of data from the dataset that is displayed in the report. In selecting a data range, you select data over a time range, and control the density of that data over the specified range. You do this using the *Show Data From* controls at the bottom of the window. Select a range of 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.

...to Date

Select all data from beginning of the most recent day, week, month, or year.

The time units vary with your selection.

Specific date

Select data for a specific date.

All dates before

Select all data before the specified date.

All dates after

Select all data after the specified date.
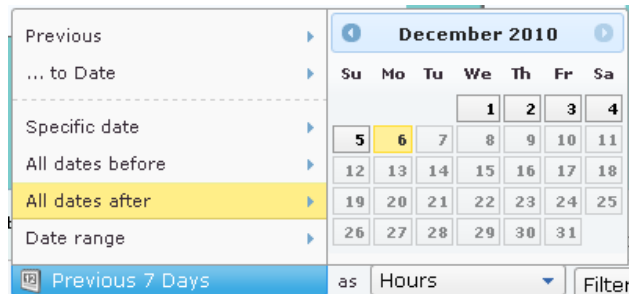
Date Range

Select data from the specified range of dates.

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.)

Creating and Using Data Filters

You can limit the amount of data, or select specific subsets within a dataset, using Filters.
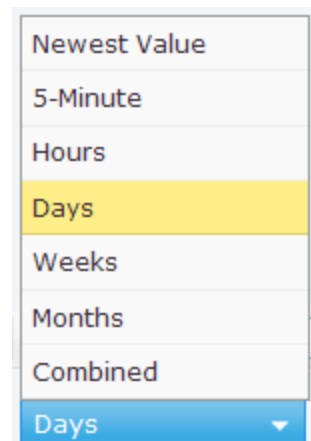
To create a filter:

- 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.
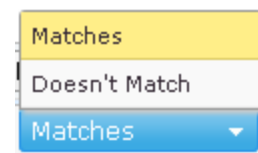
Comparison operators
(numeric fields)

When comparing numeric values, a number of comparison operators are available.
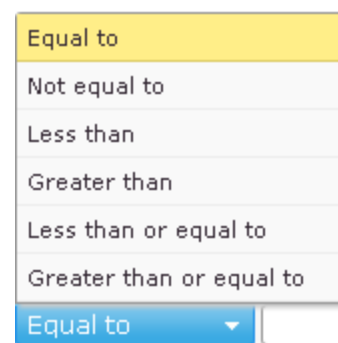
Multi-part Filters

You can create filters with more than one set of filter criteria.

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.
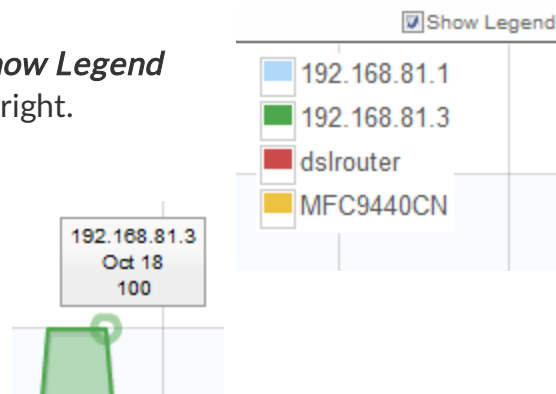
Table Report

	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
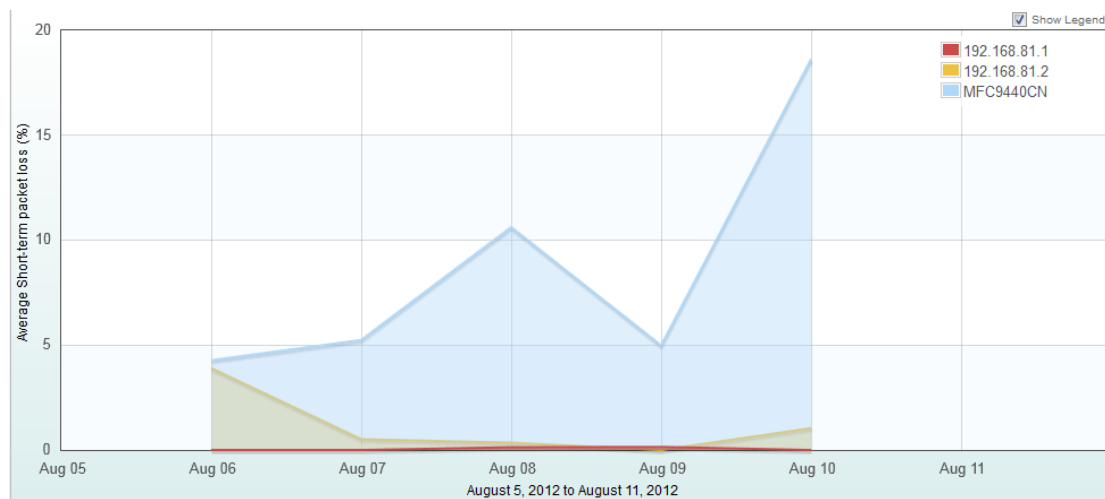
Line Report
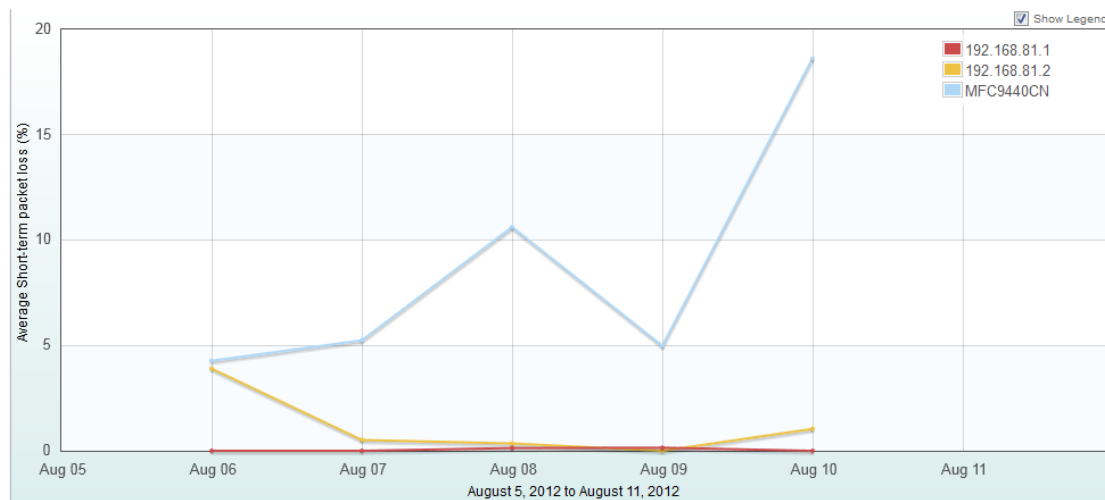
Column Report
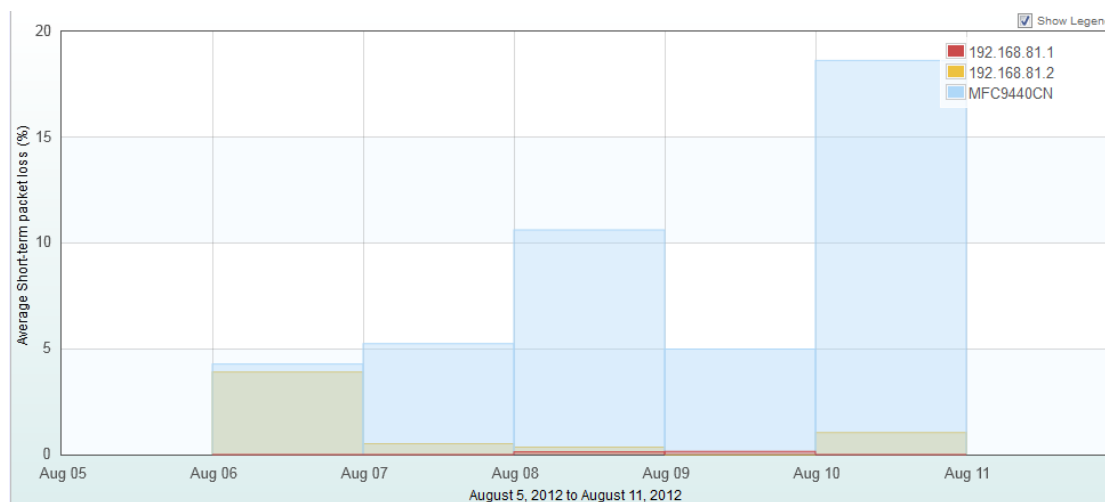
Managing and Printing Your Reports

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.
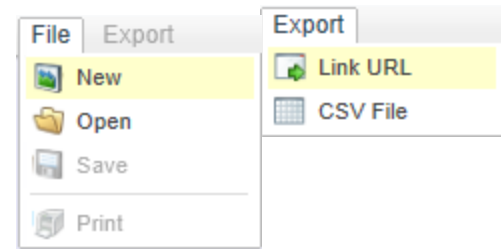
Switching to Edit Mode

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.
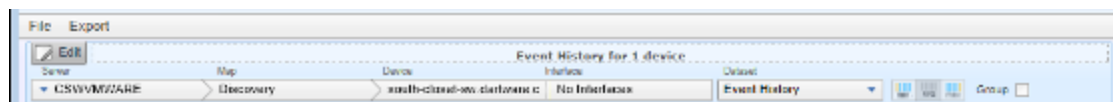
Reports window in Edit mode

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.
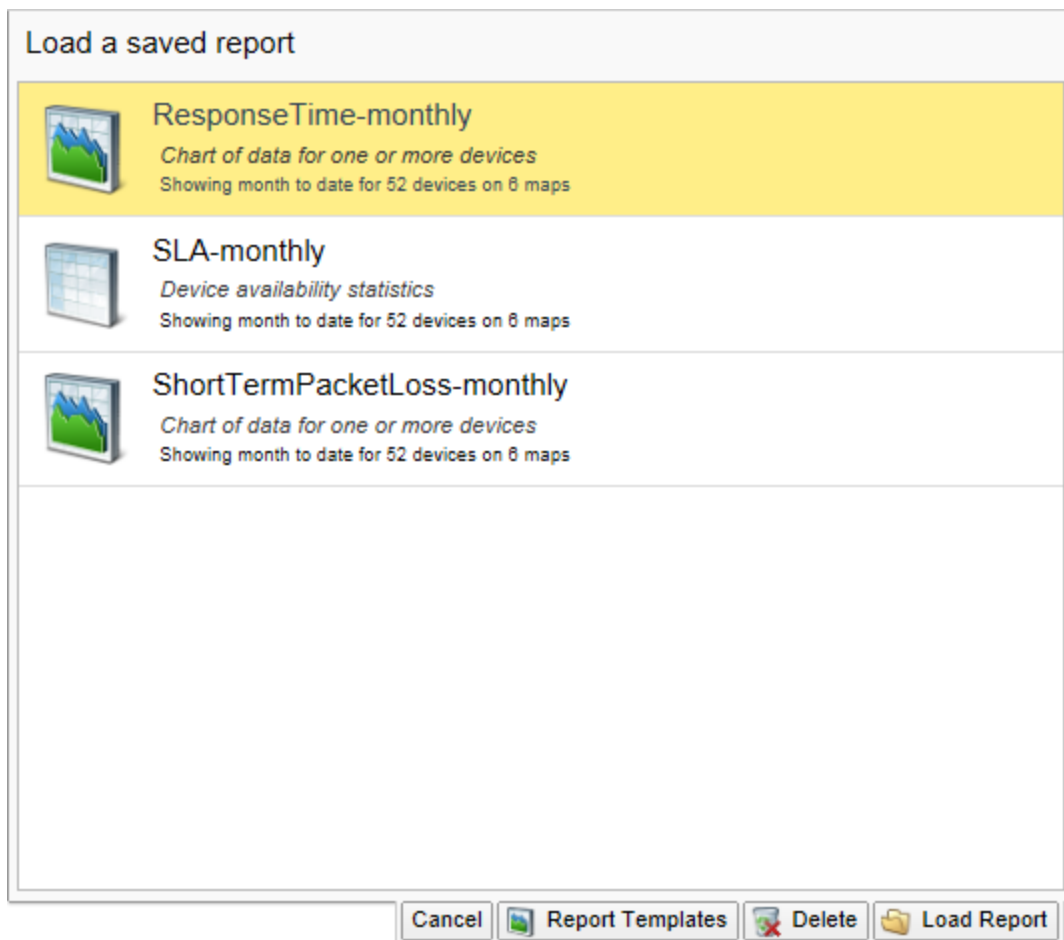
The Saved Reports list

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:
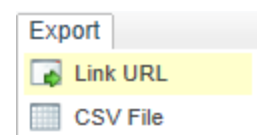
1. After viewing the report, choose **Link URL** from the Report window's Export menu. The Link URL box appears as shown.

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.

Using Intermapper Remote Access

Intermapper can make its maps available to people who are away from the server. They can use a program called Intermapper Remote Access to view and configure the server.
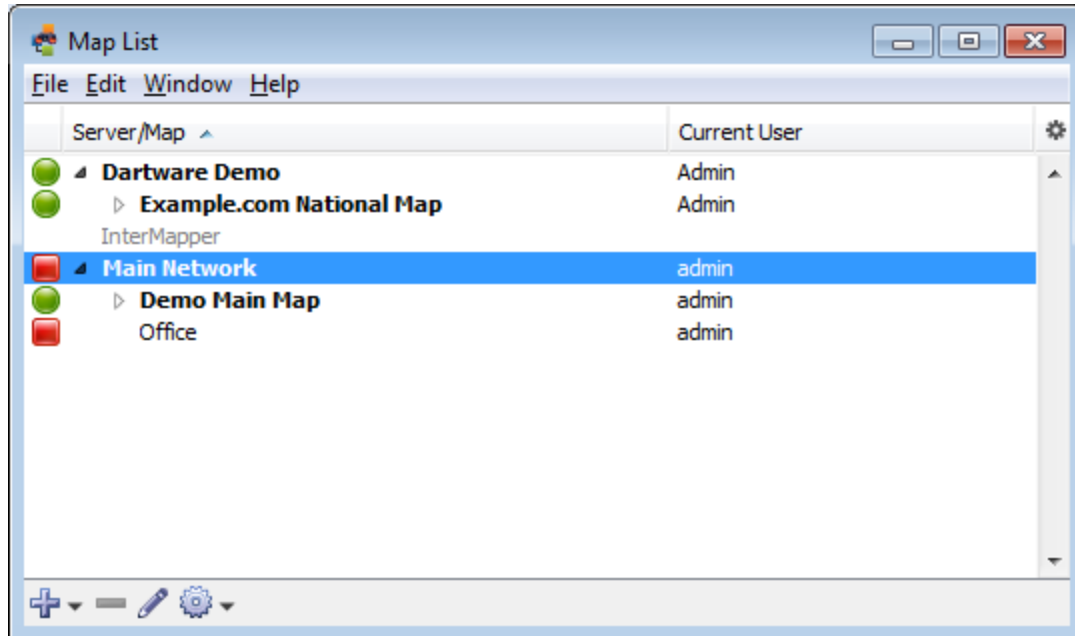
Intermapper Remote Access Map List window

Intermapper Remote Access 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.

InterMapper RemoteAccess is also accessible through a command-line interface.

Note to Windows users: By default, Windows has 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.

Intermapper Reference

Use the Intermapper Reference section to get detailed information about Intermapper components:

- **Command/Menu Reference** - view a list of menu items for each menu and the purpose of each.
- **Probe Reference** - view an overview of the Set Probe window, a list of probes with a description of each, a number of topics about packet-based, SNMP, Command-Line, and other specialized probes, and a topic on troubleshooting.
- **Using Intermapper Data Center** - learn how to configure and use the data center.
- **Files and Folders** - get information about default locations of various files and folders for different platforms and how to control locations.

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. 402)

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. 407)

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. 411)

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. 414)

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. 430)

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. 437)

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. 449)

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. 454)

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. 457)

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. 458)

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. 458)

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. 458).

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	Creates a new map.
Save...	Save a PDF report to disk. (**Flows**)
Open Recent (submenu)	Choose a recently-opened map from this submenu.
Close	Closes the current window.
Backup...	Backs up the current map.
Restore...	Restores the current map from a backup.
Rename...	Renames the selected map.

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.)
Import (submenu)	Choose from these submenu commands:

- **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.
- **Probe...** - Imports custom probe files to your server.
- **MIB...** - Imports an SNMP MIB file for a specific device or family of devices.

Export (submenu)	Choose from these submenu commands:

- **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...	Opens the standard Page Setup dialog. (**Map**)
Print...	Prints the current window on the currently selected printer. (**Map**)
	Prints a report using the current time range and filter settings. (**Flows**)

Print Single Page...	Prints a single page of a map in the current view. (**Map**)
Exit/Quit	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 menu command for details about creating a map automatically.

Save...

Saves a PDF report to disk. A standard file dialog appears. The report contains the Top Hosts, Top Ports, and Top Sessions tabs.

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.

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.
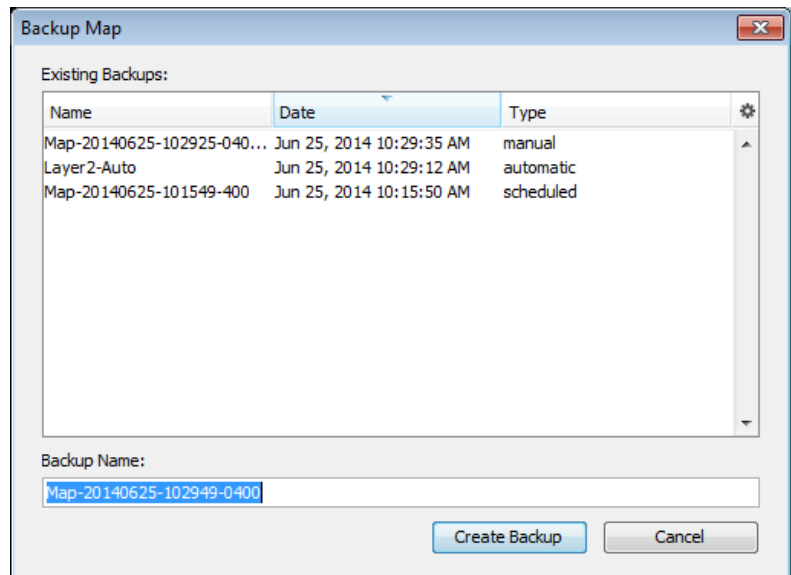
Restore…

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, the click *OK*.

See Backup… (above) for information on backup types.
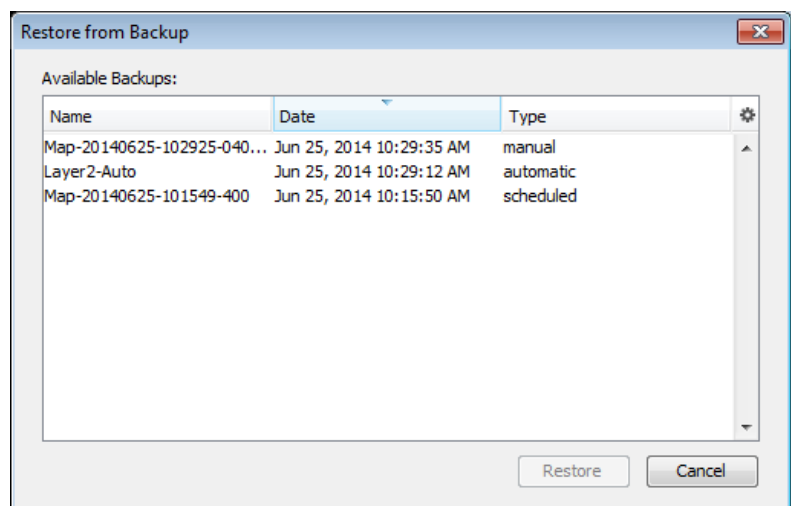
Rename…

Renames the
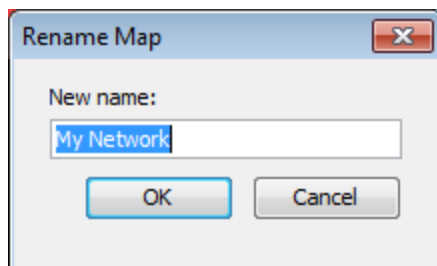
selected map.

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.

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.

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*.
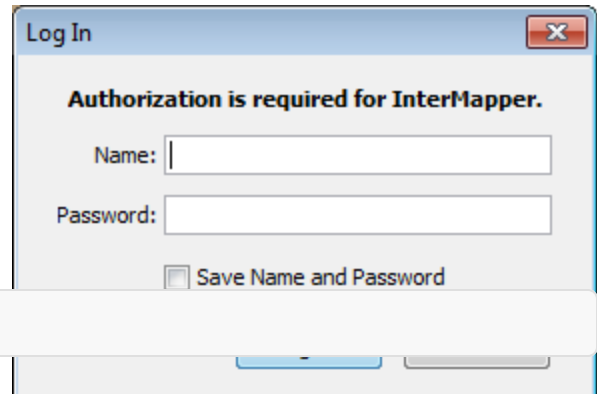
> **NOTE:** SASL authentication is used for logins.

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...

From a map, this command 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.

From the Flows window, this command prints a report using the Flows window's current time range and filter settings.

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. 409)	(Map Window only) Most operations in Intermapper can be undone. Undo is multiple levels.

Redo (Pg. 409)	(Map Window only) Available after you execute the Undo command. Restores the state of the map before the Undo command was executed.
Revert... (Pg. 409)	(Map Window only) Restores the state of the map as it was when you last opened it for editing.
Cut (Pg. 409)	Cut the selected items to the clipboard.
Copy (Pg. 409)	Copy the selected items to the clipboard.
Paste (Pg. 409)	Paste the contents of the clipboard to the current window.
Delete (Pg. 409)	Removes the selected items from the map. **Caution:** This operation cannot be undone.
Select (submenu) (Pg. 409)	Choose from a variety of commands to select objects in a variety of ways. (Map Window only)
Select All (Pg. 410)	(Map List Window only) Select all maps and servers.
Find (submenu) (Pg. 410)	• **Find** (Pg. 410) - Opens the Find window. Enter a text string to search for. • **Find Next** (Pg. 410) - Search for the next occurrence of the last defined text string. • **Find Device...** (Pg. 410) - Search for a device in a map on a connected server.
Map Settings... (Pg. 410)	Opens the Map Settings window.
Server Settings... (Pg. 411)	Opens the Server Settings window.
Preferences... (Pg. 411)	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 other 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.

Find Next

Finds the next item in the current map that matches the previously specified text string.
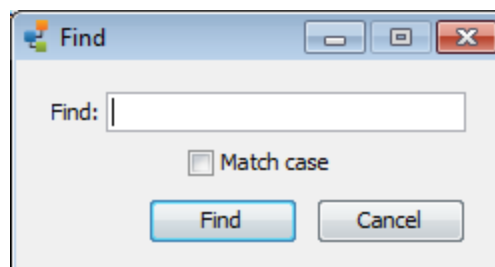
The Find window

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.
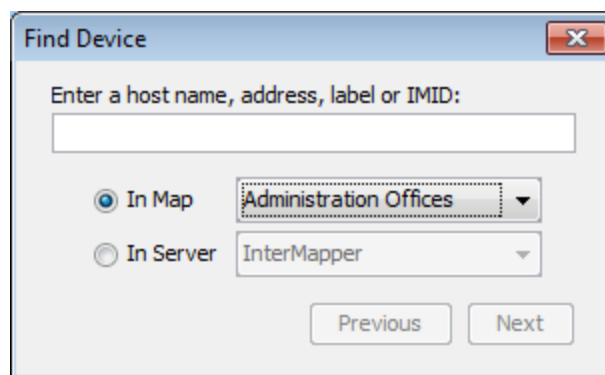
Map Settings...

Use the Map Settings... command to view and edit an individual map's color settings, specify

The Find Device window

a background image, and view and edit the list of default notifiers for the map. See Map Settings (Pg. 157) 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. 293) 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	View as a map, with graphic objects representing devices, networks and links.
List	View as a list of devices.
Device Notifiers	View as a list of devices, each showing the states for which the selected notifier sends notifications.
Link Notifiers	View as a list of interfaces, each showing the states for which the selected notifier sends notifications.
Charts	View a list of charts associated with the map.
Datasets	Select from a list of devices to view a list of datasets available for those devices.
Actual Size	In Map view, set the zoom level to 100%.
Zoom In	In Map view, zoom in.
Zoom Out	In Map view, zoom out.

Sort (submenu)	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)	Choose the columns you want to show in any list view.
Filter (submenu)	Choose to view only those objects with the selected state.
Expand All	In List view, expands all hierarchical items in the Map and Device List windows.
Collapse All	In List view, collapses all hierarchical items in the Map and Device List windows.
Show/Hide Toolbar	(Map List Window only) Choose to show or hide the toolbar.
Edit Map	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
Reprobe/Reprobe Selection	**Reprobe:** If no device is selected, re-poll all devices on the map. **Reprobe Selection:** Re-poll the selected device(s).
Acknowledge	Use this command to acknowledge a failure. This stops an icon's flashing, and deactivates recurring notifications.
Un-Acknowledge	Use this command to remove an acknowledgement from the selected device, and to reactivate notifications.
Info Window	Open the Info Window for the selected device or network.

Status Window	Opens the Status window for the selected device, network, or link.
Interfaces > Window...	Opens the Interfaces window for the selected device.
Interfaces > Error Thresholds...	Opens the Error Thresholds dialog. Set error thresholds for one or more interfaces.
Interfaces > Utilization Thresholds...	Opens the Utilization Thresholds dialog. Set thresholds for utilization of one or more links.
Interfaces > Discard Thresholds...	Opens the Discard Thresholds dialog. Set packet discard thresholds for an interface.
Interfaces > Behavior...	Opens a device's Behavior dialog. Specify whether to allow periodic reprobes, and whether to display unnumbered interfaces.
Device Notifiers Window	Opens the Device Notifiers window, and shows a list of notifiers for the selected device.
SNMPWalk...	Opens the SNMPWalk dialog.
Flows Window	Opens the Flows Window if Intermapper Flows is running.
Show in Layer 2 (Pg. 371)	Opens the Device List window in Layer 2 view, and shows connections to the selected device.
Set Info > Set Address...	Set the IP address or name for the selected device.
Set Info > Set Comment...	Enter a comment about the selected device(s).
Set Info > Set Community...	Set the SNMP community string for the selected devices.
Set Info > Set Data Retention...	Select a Data Retention policy to use when storing data to the Intermapper Database.
Set Info > Set Double-click (submenu)	Define the action to be taken when you double-click the selected device.
Set Info > Set Kind...	Set the device kind you want to use when storing data to the Intermapper Database.
Set Info > Set Latitude & Longitude...	Set the latitude and longitude for the selected devices.
Set Poll Interval...	Set the poll interval for the selected devices.

Set Info > Set Probe... (Pg. 428)	Set the probe to be used with the selected devices.
Set Info > Set Thresholds...	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.
Set Info > Set Vantage Point	Set the selected device as the vantage point from which Intermapper views all other devices on the map.
Reset Short-term Packet Loss	Resets the accumulated value of short-term packet loss.
Helper Apps (submenu)	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 Intermapper 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 distracting 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.
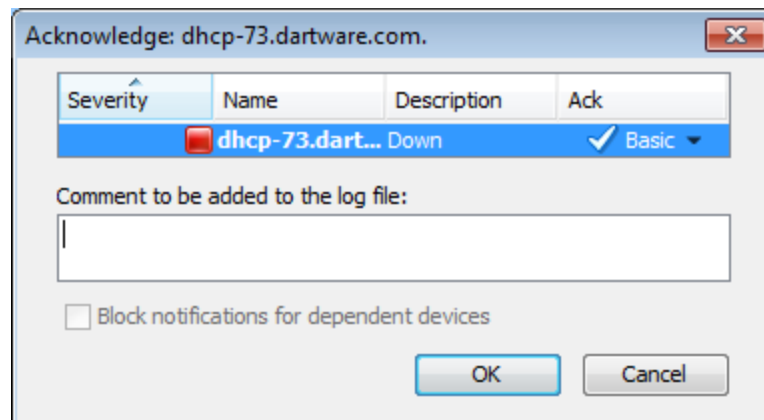
The Acknowledge Message Window. Data typed here is entered into the Intermapper log file, as well as appearing in the device's Information window.

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.

> **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 for more information.

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
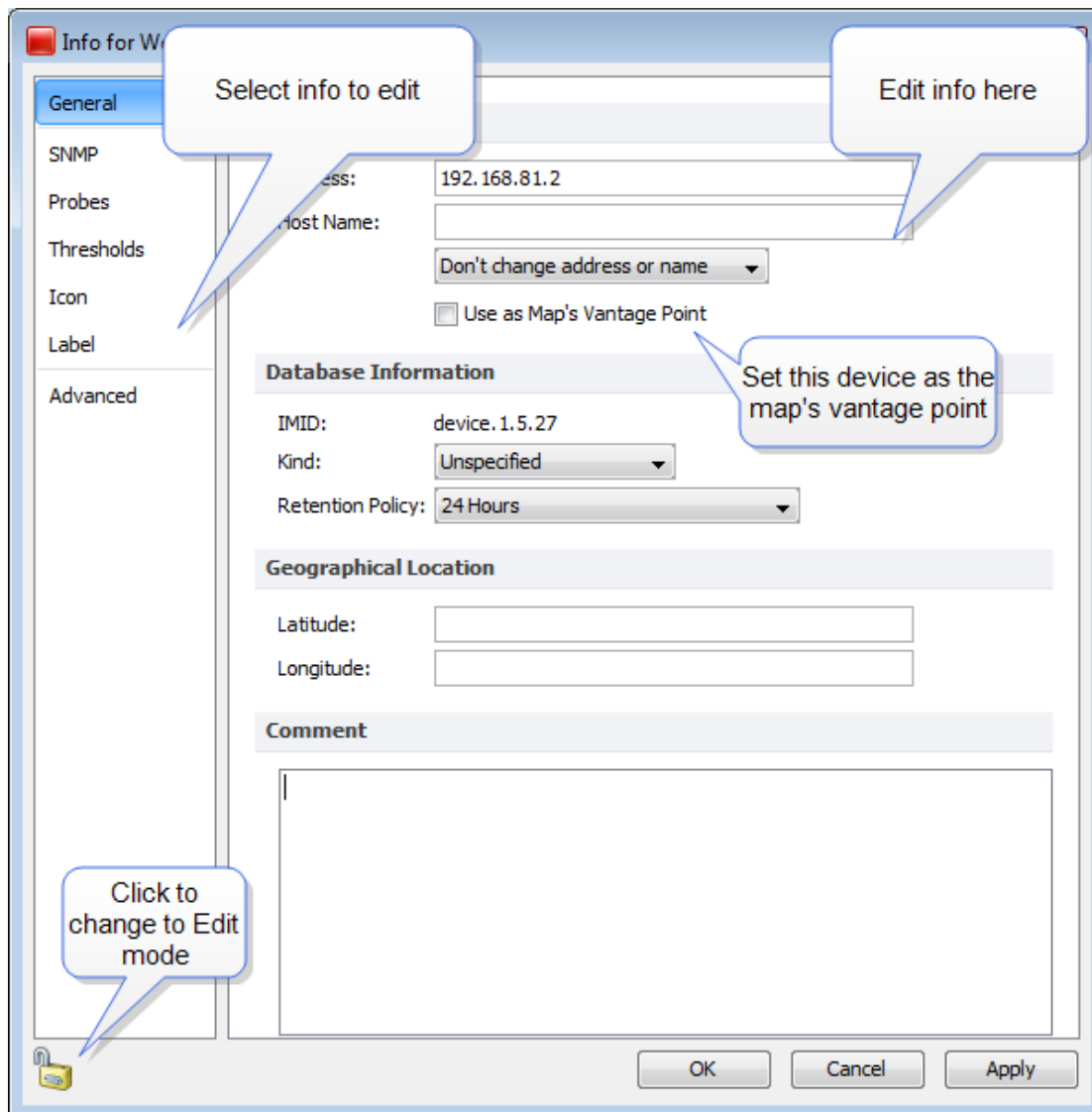
Use the Info window command to view information about the selected device or network.

- 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 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.
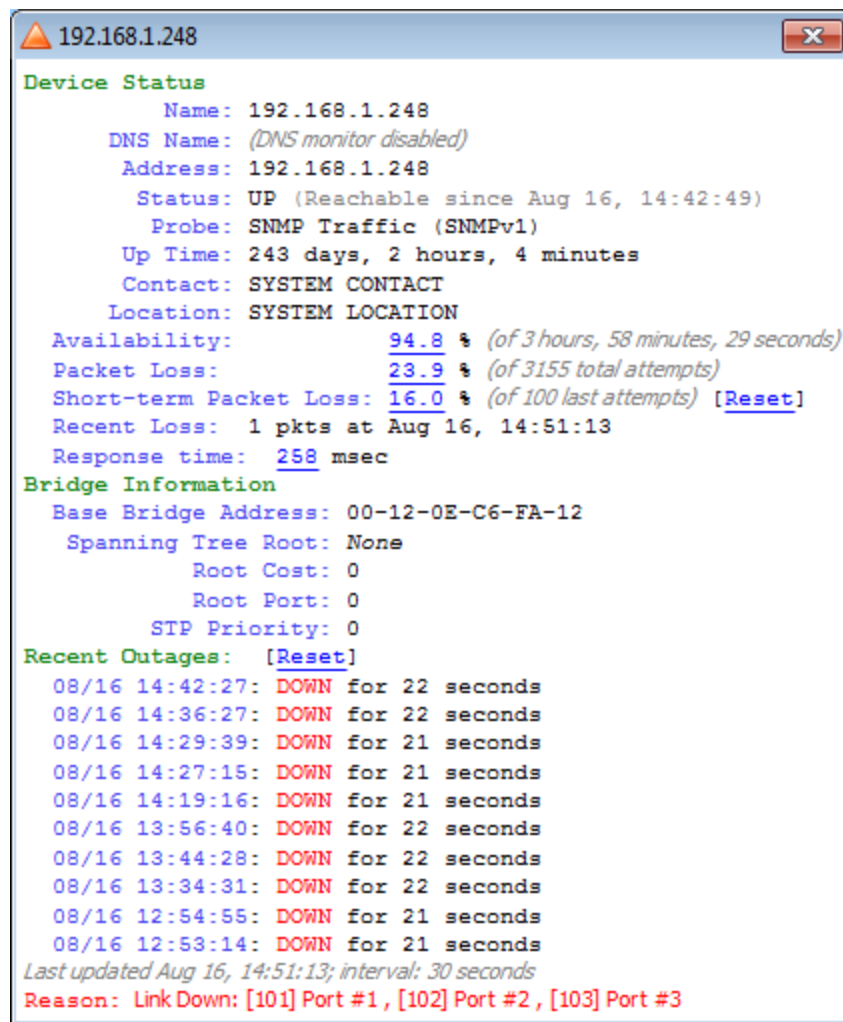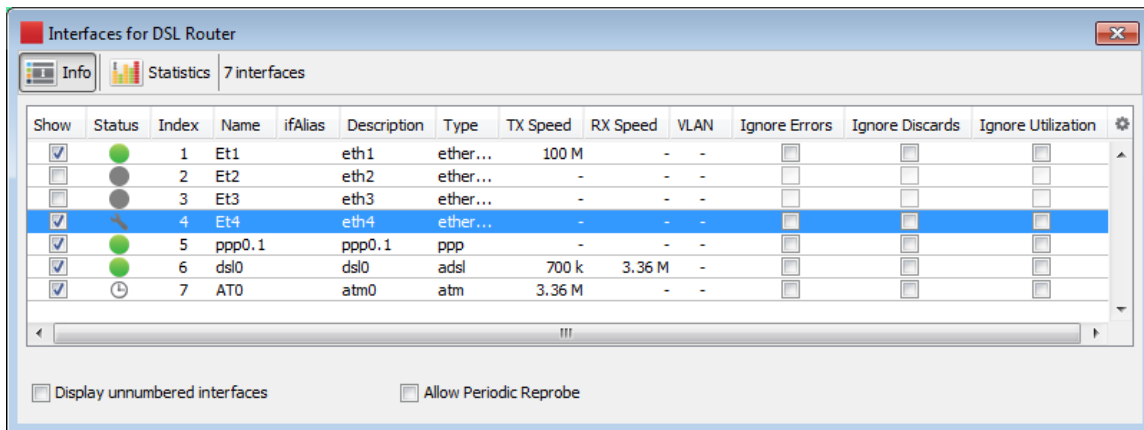
Status window

Interfaces Window

Open the Interfaces window 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.

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.

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.

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.

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.
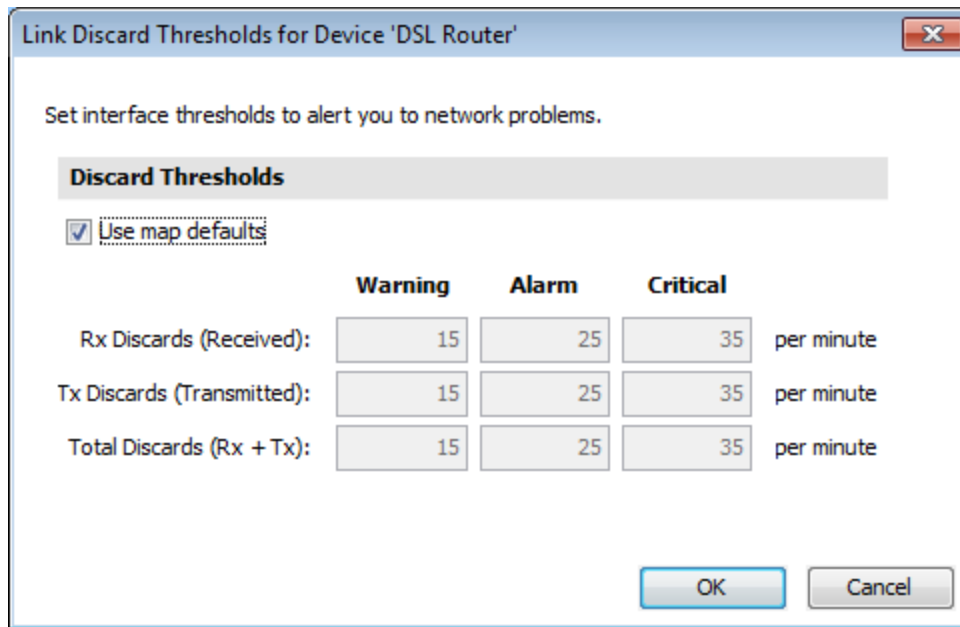
Behavior Window

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.
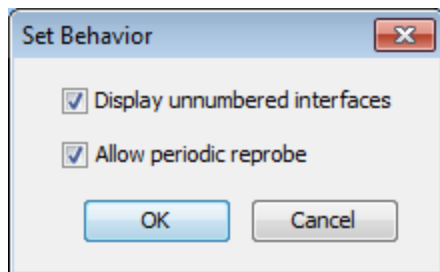
Notifiers Window

Open the Notifiers window for the selected device.
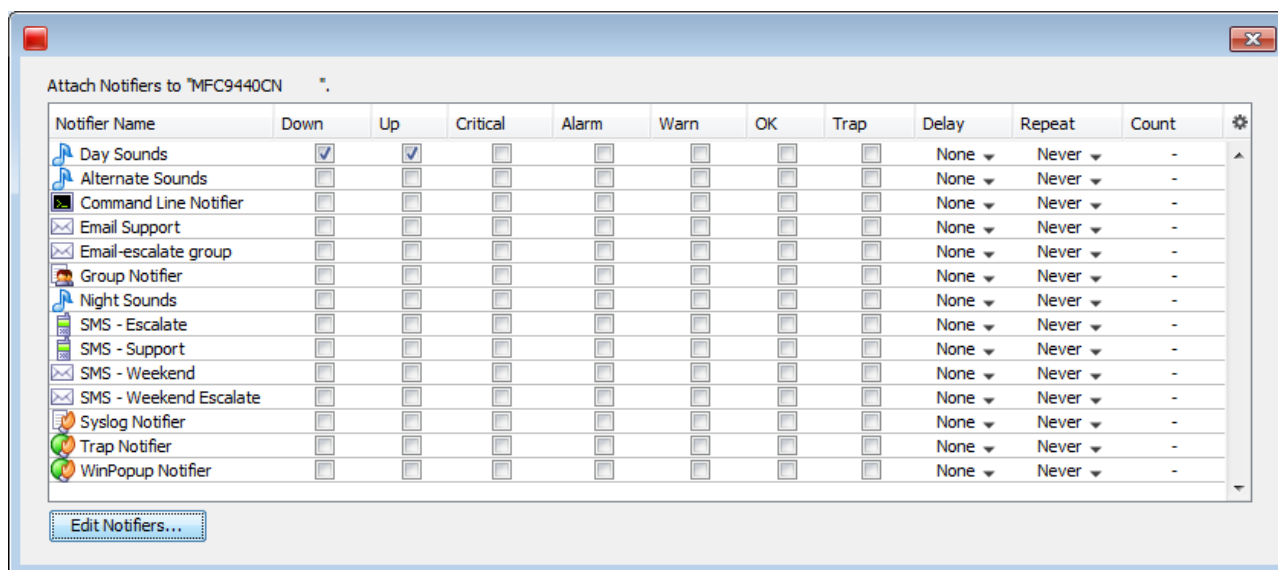
Notifiers window

SNMPWalk

Use the SNMPWalk command 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

Flows Window

If Intermapper Flows is running, opens the Flows Window, which shows Intermapper Flows information. For documentation about Intermapper Flows, please see [Intermapper Flows](#).

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…
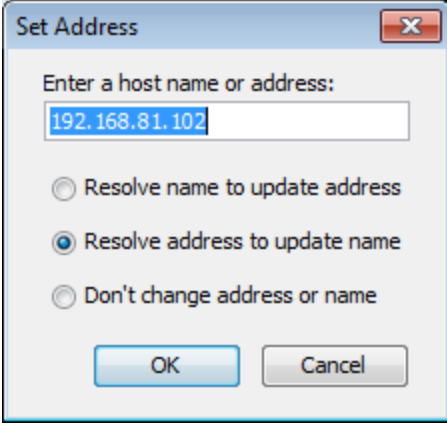
Use the Reports command to open the Reports UI in a browser window. Use the Reports window to create, load, edit, and save reports.

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.
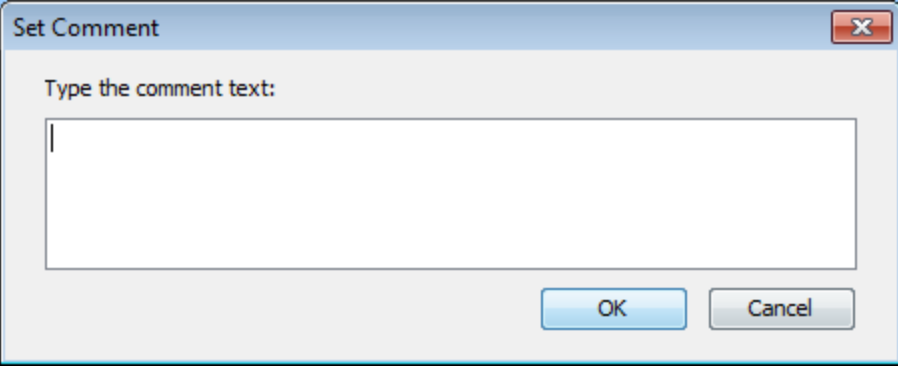
Resolve Address to Update Name - keeps the specified IP address fixed, but may update the name from the DNS server if one is found.

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.)
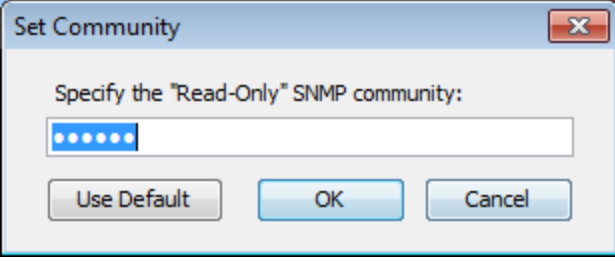
This information is saved as part of the map. Use the Comment field to save the model and serial number for a device, telephone numbers, circuit numbers, or other information related to the item.

Set Community...

Sets the [read-only community string](#) for all selected devices.
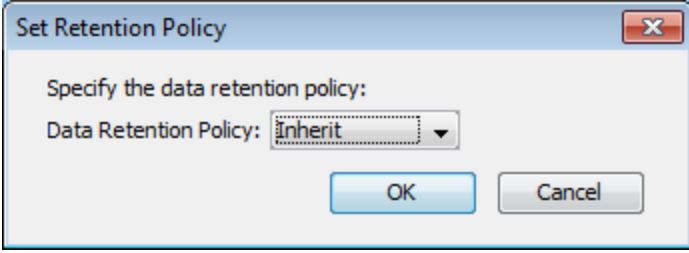
The default community string for most SNMP devices is "public".

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.

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.
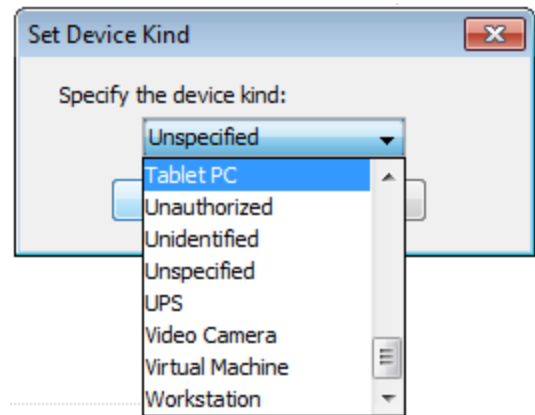
Set Latitude & Longitude

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.
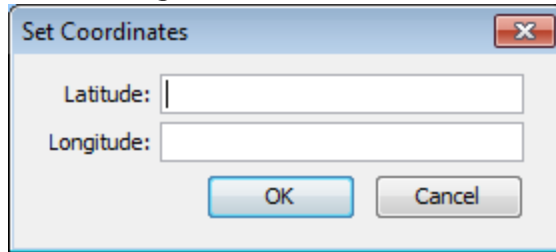
Set Poll Interval

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.
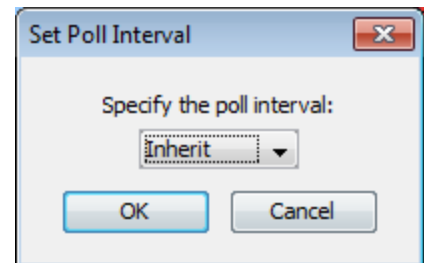
Set Probe...
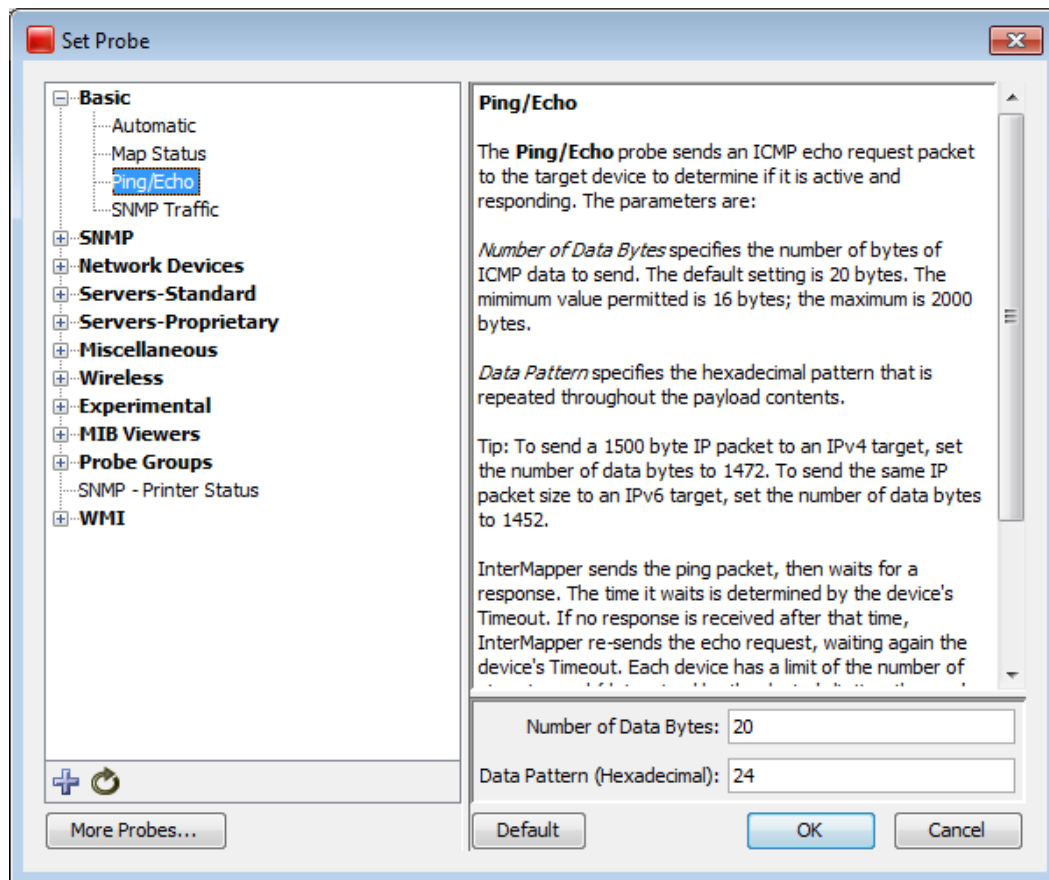
Opens the Probe Picker window.

Sets the probe used to query the selected device and the probe's parameters, if applicable. See Probe Reference 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 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.

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.

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.

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
Device... (Pg. 431)	Add one or more devices to a map.
Network... (Pg. 432)	Add a network (oval) to the map.
Link (Pg. 433)	Connect two devices with a link.

Auto-Discover... (Pg. 433)	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.
Scan Networks... (Pg. 434)	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.
Empty Probe Group... (Pg. 436)	Insert one or more empty probe groups in the map.
Text... (Pg. 436)	Adds an object to the map containing the specified text.
Icon...	Insert an icon into a map.
Map Benchmark*Map Benchmark*	Insert a benchmark to define the latitude and longitude of a point on the map.
Group	Group two or more selected devices into a probe group. Devices must have the same IP address.
Un-Group	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.
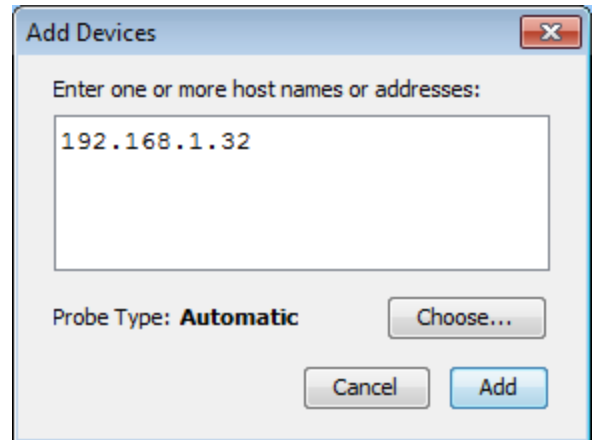
Add Device(s) window.

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. 461) 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*.

Network...

Add a network (oval) to the map. This is useful when Intermapper does not automatically detect the network because no SNMP-speaking devices are present.
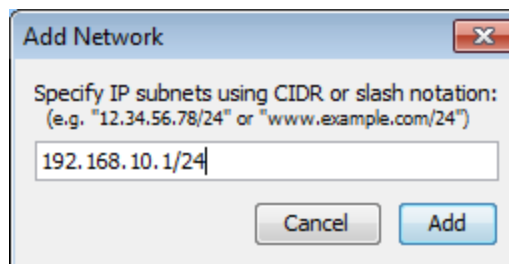
Add Network... window. Enter an IP address range.

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. 768))

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. 141).

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. 205).

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
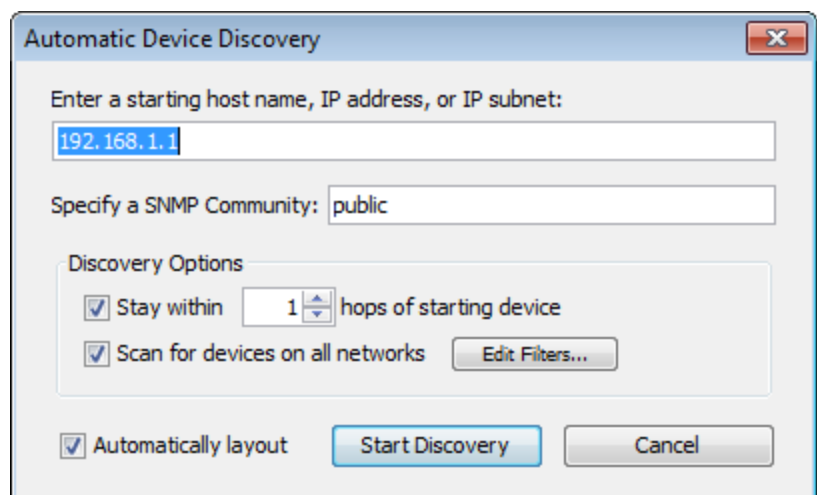
address (Pg. 766). You may, however, enter a different address or DNS name (Pg. 770) or WINS name (Pg. 776) (preceded by "\\") as a starting point. If Intermapper finds SNMP-speaking routers with connections on other networks, it searches those networks, hop-by-hop, finding more devices (and possibly 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. 771).)

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. 434)* below.

Edit Filters... - Click this button to open the Network Scanning window. See Scan Network... 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

Choose from these options:

*The Network Scanning dialog. Check a box to seek
the associated device.*

- **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.
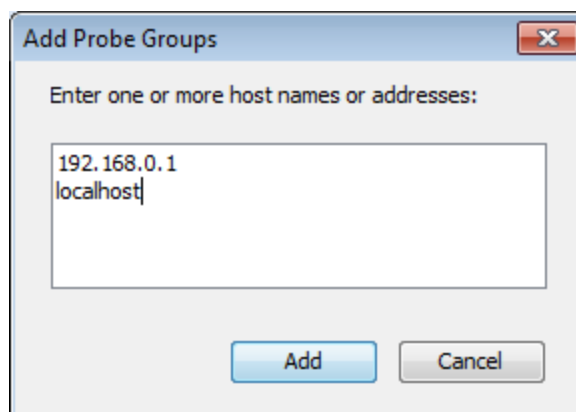
Text...
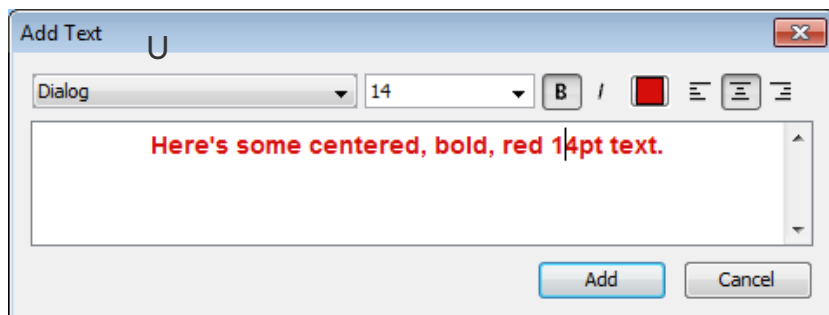
Add Text window. Enter text in the text box.
Use the text formatting controls to format the text.

s
e 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:

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

[Icon... (Pg. 438)](#)	Choose an icon for the selected items.
[Label... (Pg. 439)](#)	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.
[Label Position (submenu) (Pg. 444)](#)	Change the position of the label relative to an item.
[Align... (Pg. 444)](#)	Align the selected objects to each other.
[Rotate... (Pg. 445)](#)	Rotate the positions of the selected objects in relation to each other.
[Scale... (Pg. 446)](#)	Scale the positions of the selected items in relation to each other.
[Arrange (submenu) (Pg. 446)](#)	Rearrange the selected items into a cycle, bus, or star.
[Context menu (Pg. 449)](#)	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 preview 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.
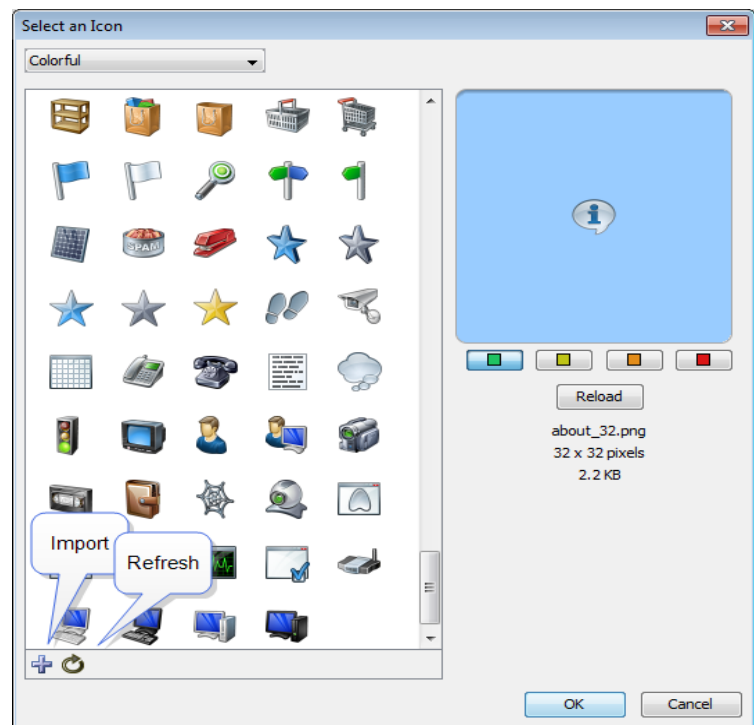
- Click *Import...* to import an image as an icon.
- When viewing groups of icons other than Built-in Shapes, click Reload to refresh the icon list in the left box.
- Drag an image to the window to import it as an icon.
- Drag a folder of images to the window to import the contents as a new icon group.

For more information, see Custom Icons (Pg. 171).

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	**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	**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* submenu to position the label at one of nine positions.
Cloud	**Cloud**	Cloud items contain the text label within them.
Text	**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	**Icon**	Choose from a set of default icons or create your own. See Custom Icons (Pg. 171) 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*.
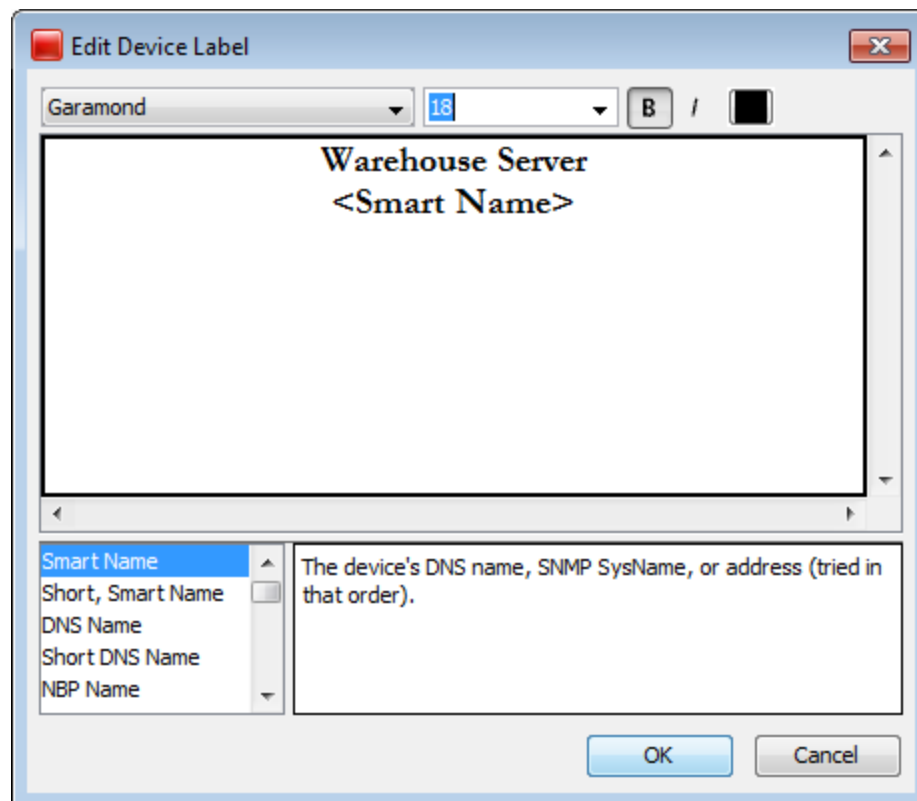
Editing a Device label.
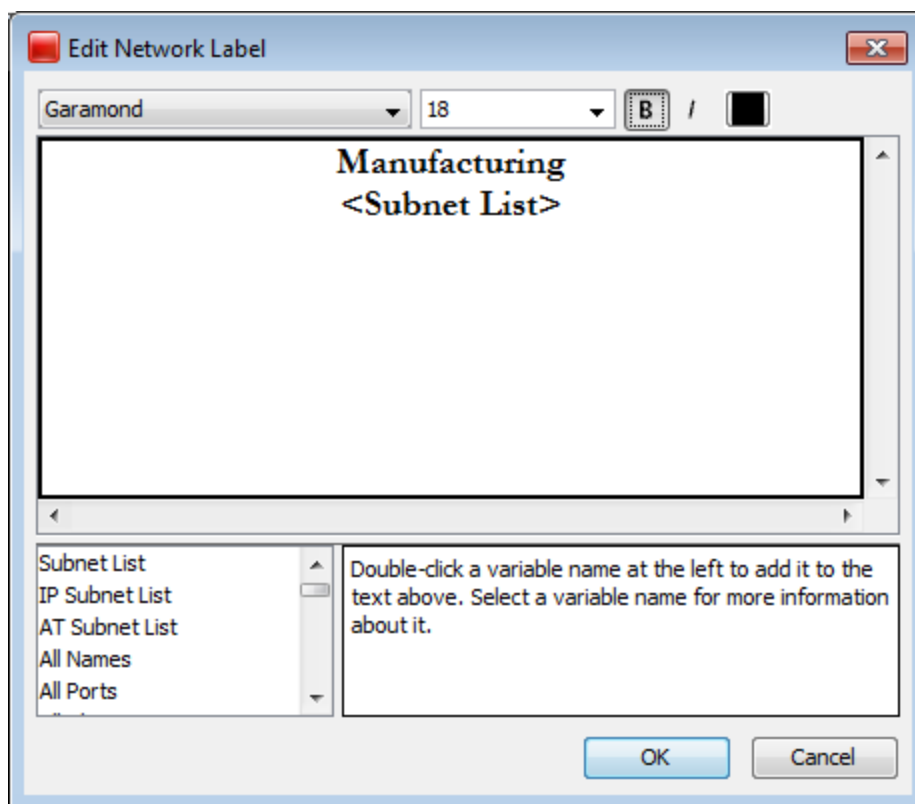
Editing a Network Label.

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.
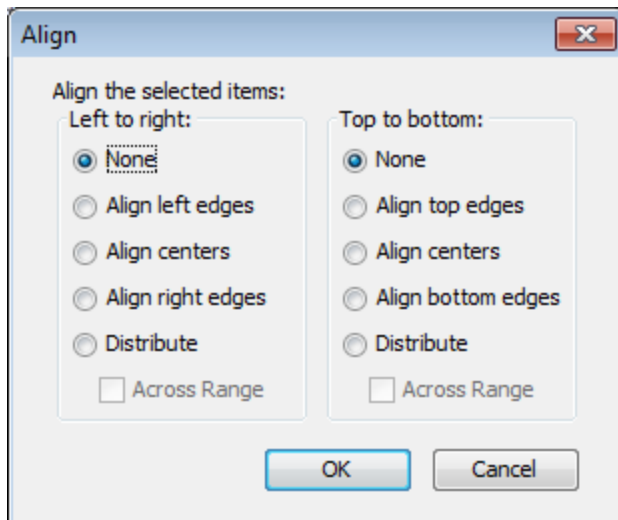
Changing alignment of selected items in a map.

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
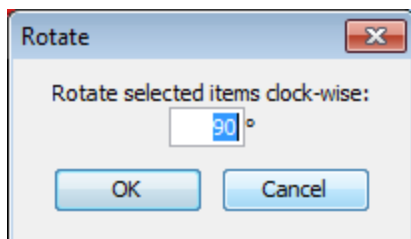
Rotate the selected items (but not their icons or text labels) by the specified number of degrees.

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
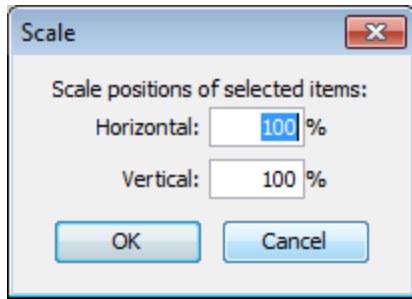
Change the relative spacing of the selected items. This is useful after arranging items in a star to increase or decrease the diameter of the circle. The example at left shows the interface.

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
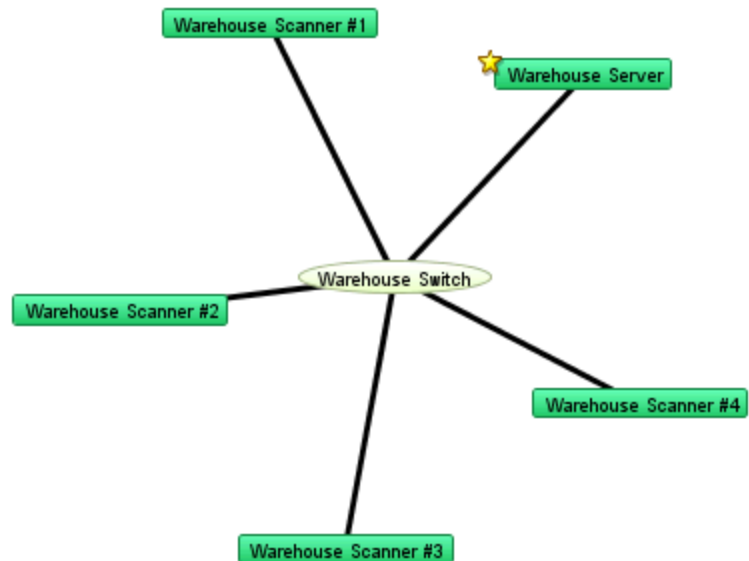
Arrange items in a tree structure. Choose which direction the branches of the tree should go.
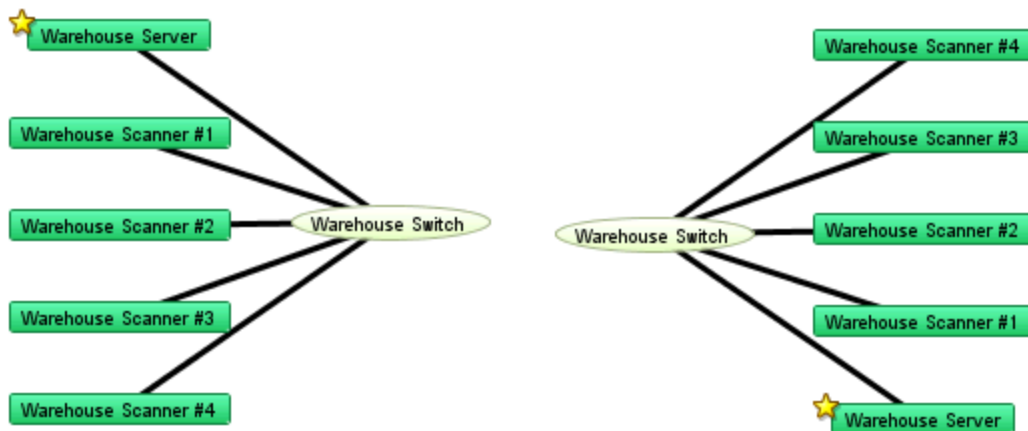
Tree - left   **Tree - right**
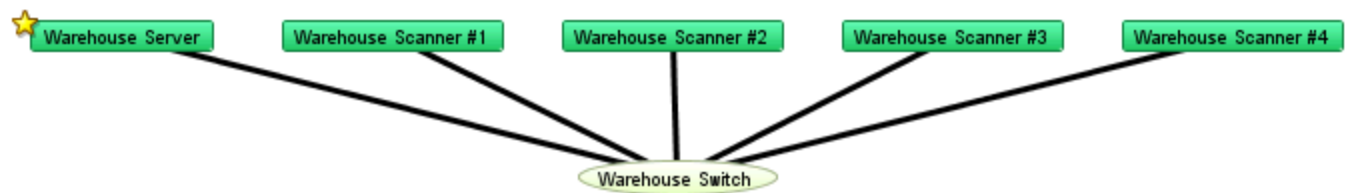
Tree - up
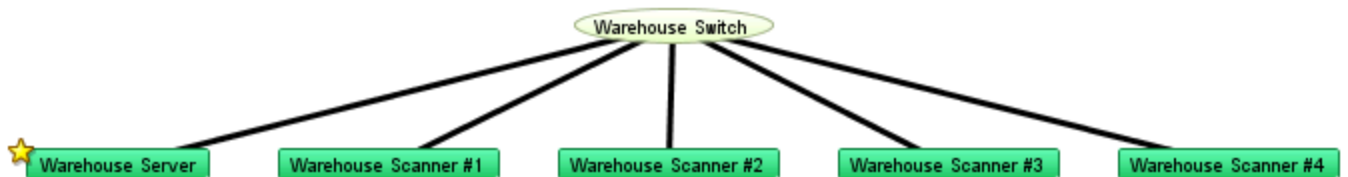
Tree - down

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. 187) 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. 186) illustrates the Bus command's action.
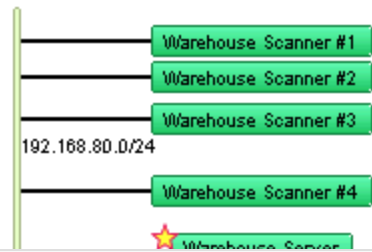
> **NOTE:** The **Bus** command affects only items that are connected to networks.

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. 186) illustrates the Star command's action.
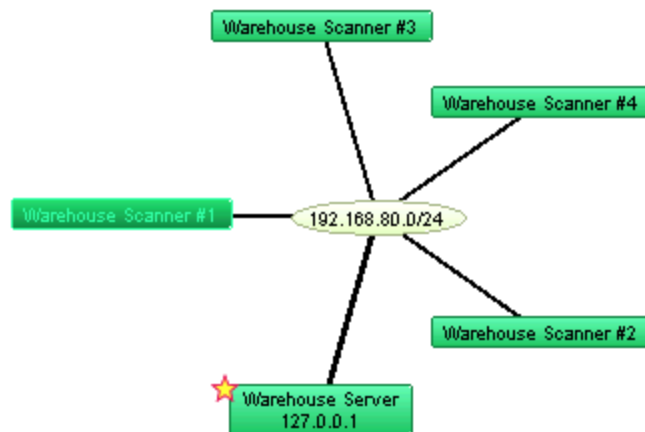
Grid

Arrange items to form a grid, with the
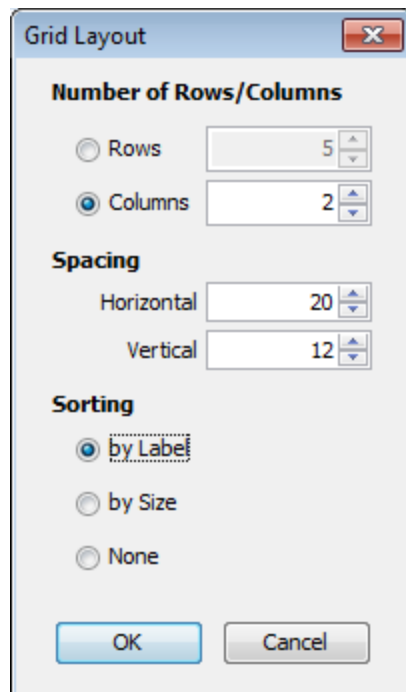
specified number of columns or rows. Sort by Label, Size, or None. If sorting by None, the grid is created relative to the upper-left icon in the selection.

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. 450)	Minimize the frontmost window.
Zoom (Pg. 450)	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. 450)	Send the front-most window to the back.

[Slideshow... (Pg. 450)](#)	Rotate between open map windows.
[Logs (Pg. 451)](#)	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. 452)](#)	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. 452)](#)	Open the Map List window, or bring it to the front.
[Device List (Pg. 453)](#)	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.
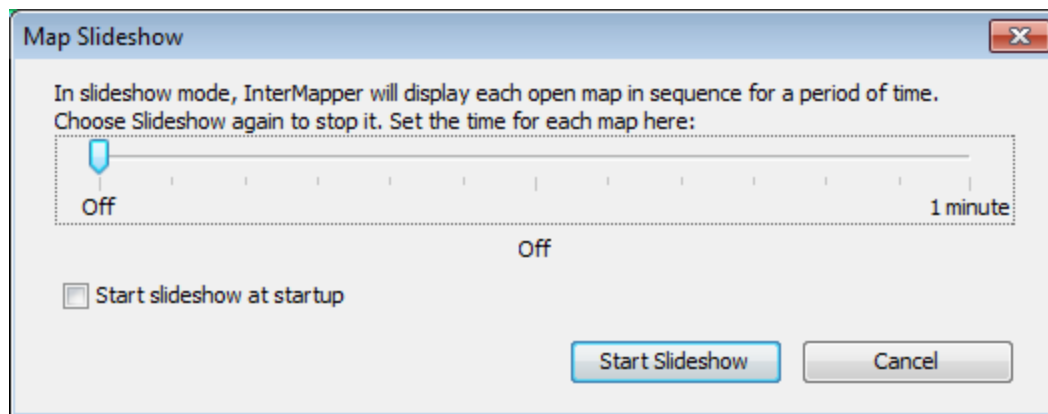
- From the Window menu, choose *Slideshow...*, and choose the amount of time each map should be shown.

- 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.
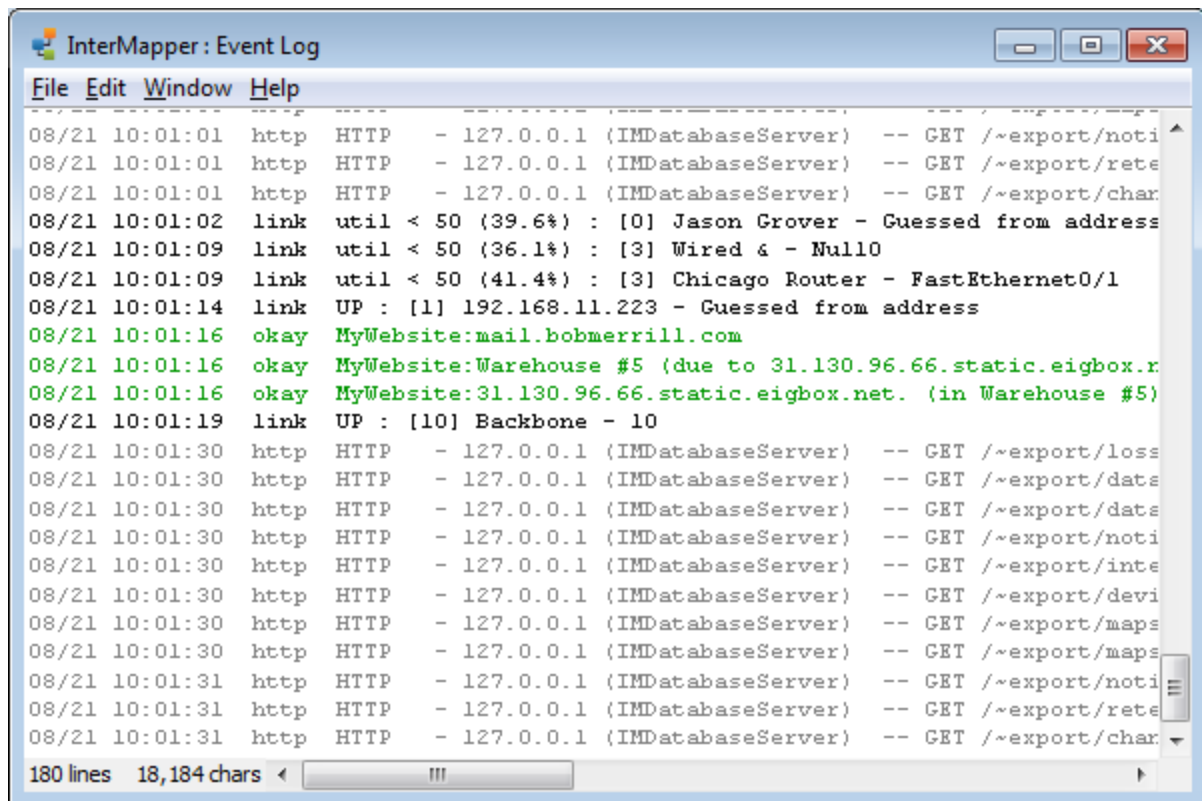
Event Log window.

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. 282).

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.
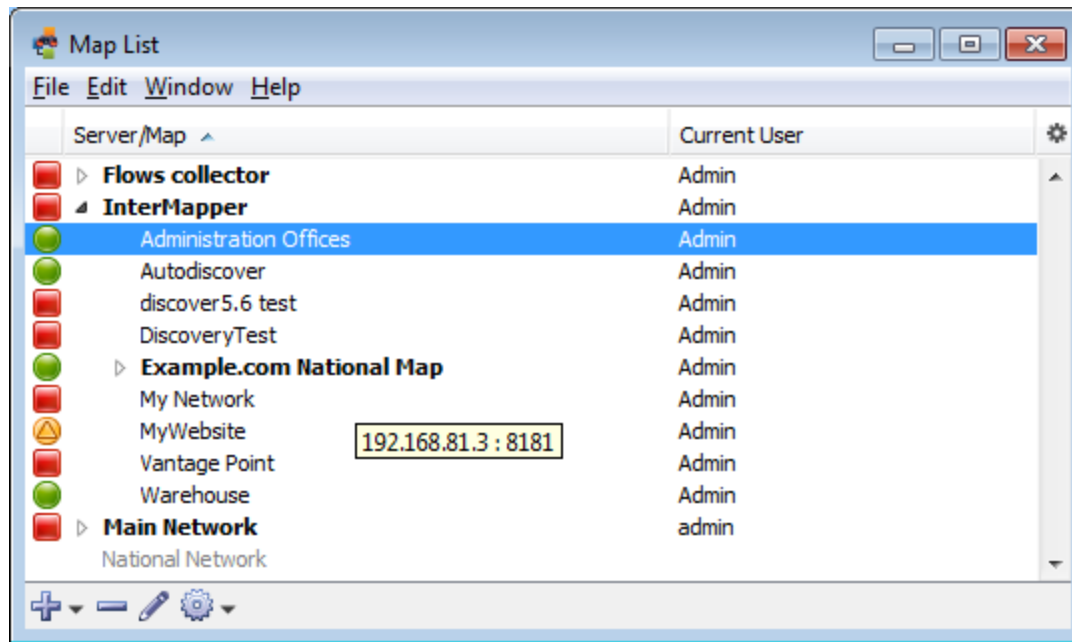
Device List

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.
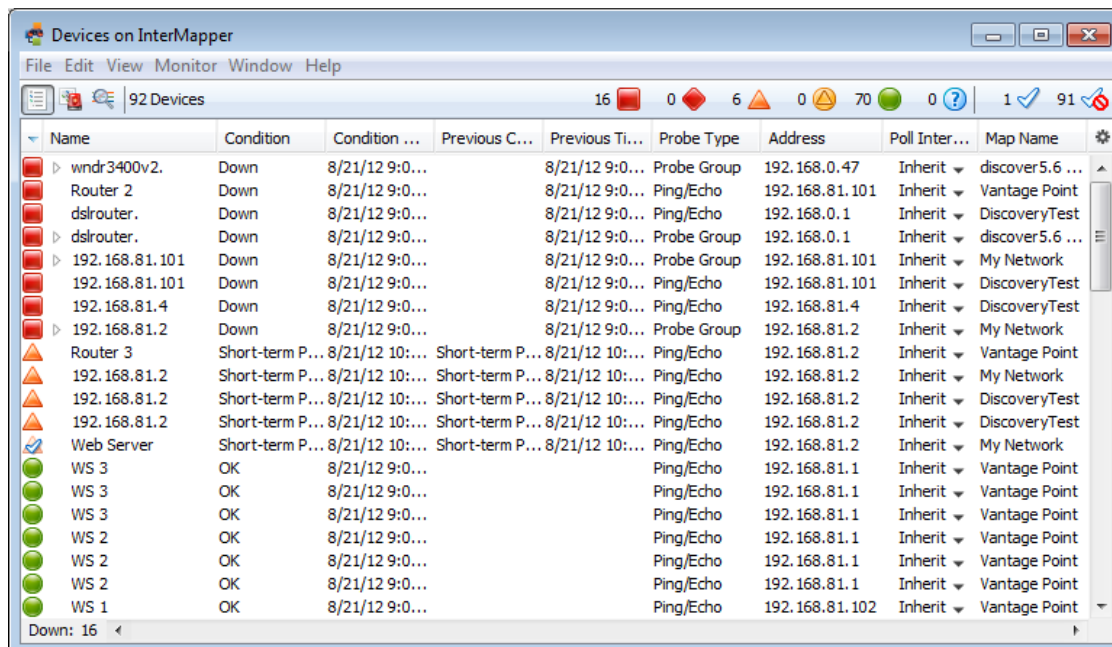
The Device list window.

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	Opens the InterMapper or InterMapper RemoteAccess registration window.
InterMapper Help, InterMapper RemoteAccess Help	Opens the InterMapper help system.
Send Feedback...	Opens the Send Feedback window.
Send a Screenshot...	Opens the Send Feedback window with a screenshot attached.
Diagnostics (submenu)	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
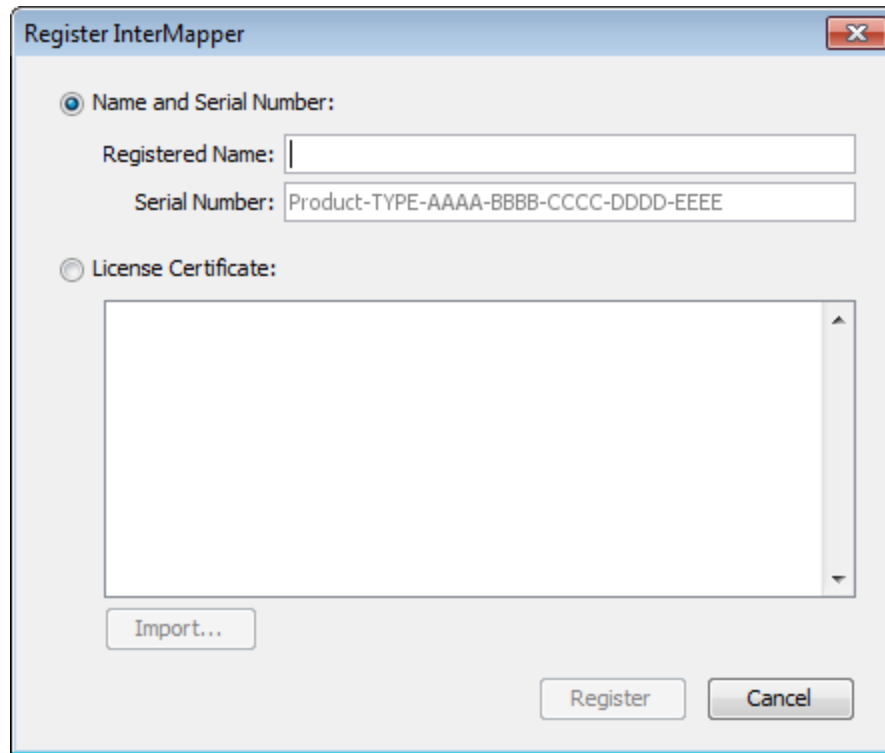
(InterMapper Only)

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.
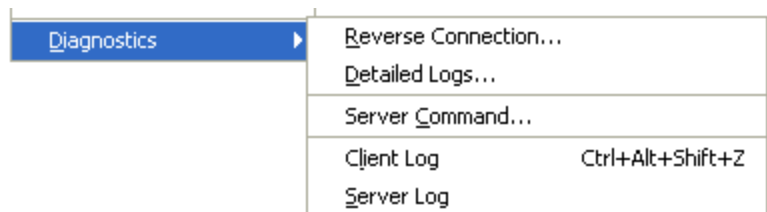
Reverse Connection...

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.
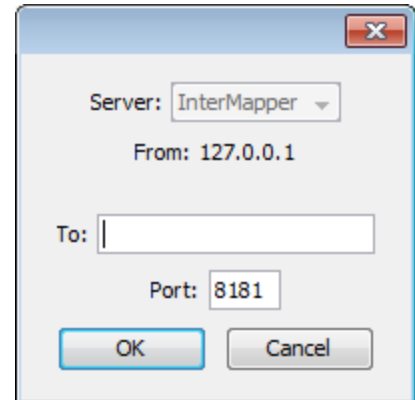
Detailed Logs...

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.
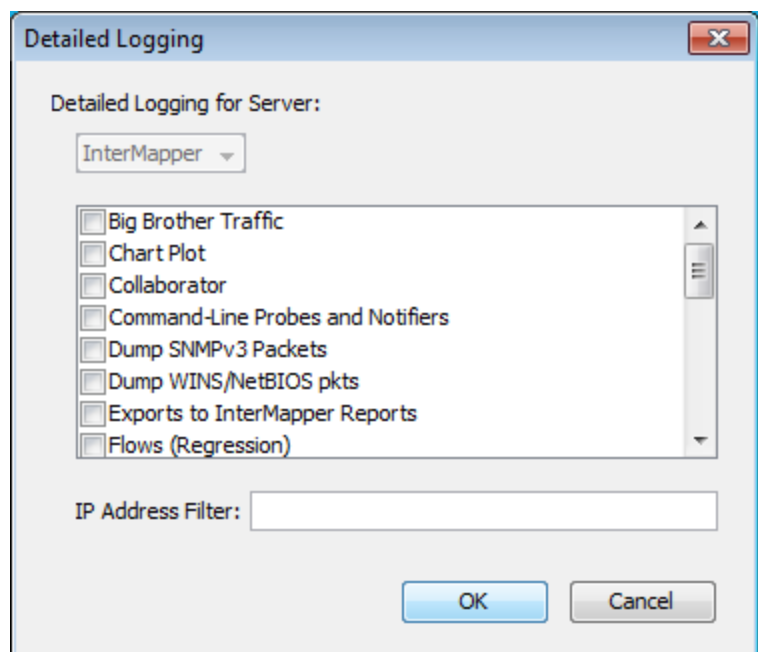
Server Command...

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.
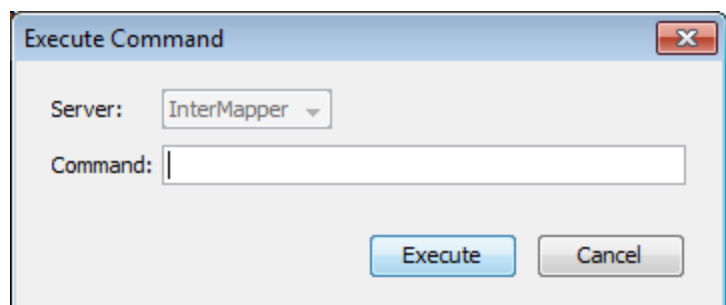
Client Log

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.
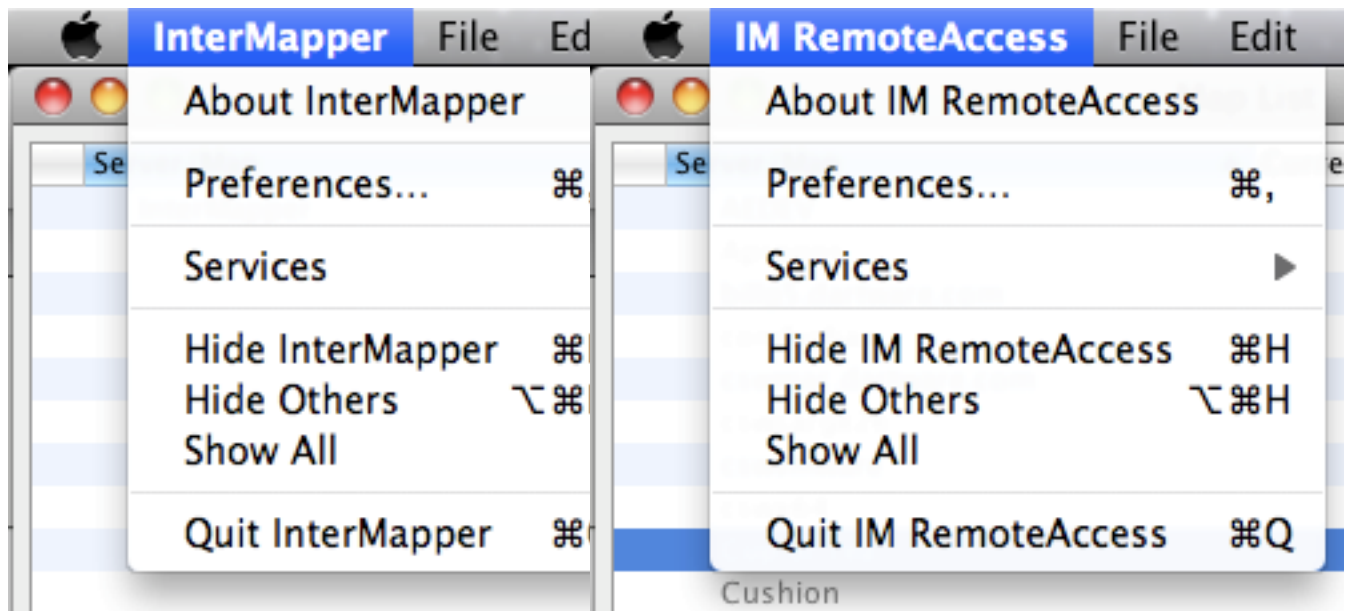
| *Intermapper menu* | *Intermapper RemoteAccess menu* |

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:	*Command* key
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. 459) 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. 165) for additional selection and scrolling techniques.

Keyboard Navigation

← ↑ → ↓ **(in Browse mode)**	Scroll the view
← ↑ → ↓ **(in Edit mode)**	Micro-adjust the position of the selected item
← ↑ → ↓ **Alt** or **Option <arrow key>** **(in Edit mode)**	Scroll the view 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 + 1	View Icons
Cmd/Ctrl + 2	View List

Cmd/Ctrl + **3**		View Notifiers
Cmd/Ctrl + **4**		View Charts
+ (Numeric Keypad)		Zoom In
− (Numeric Keypad)		Zoom Out

Probe Reference

Use the Probe Picker window to choose the probe you want to use to query the device.
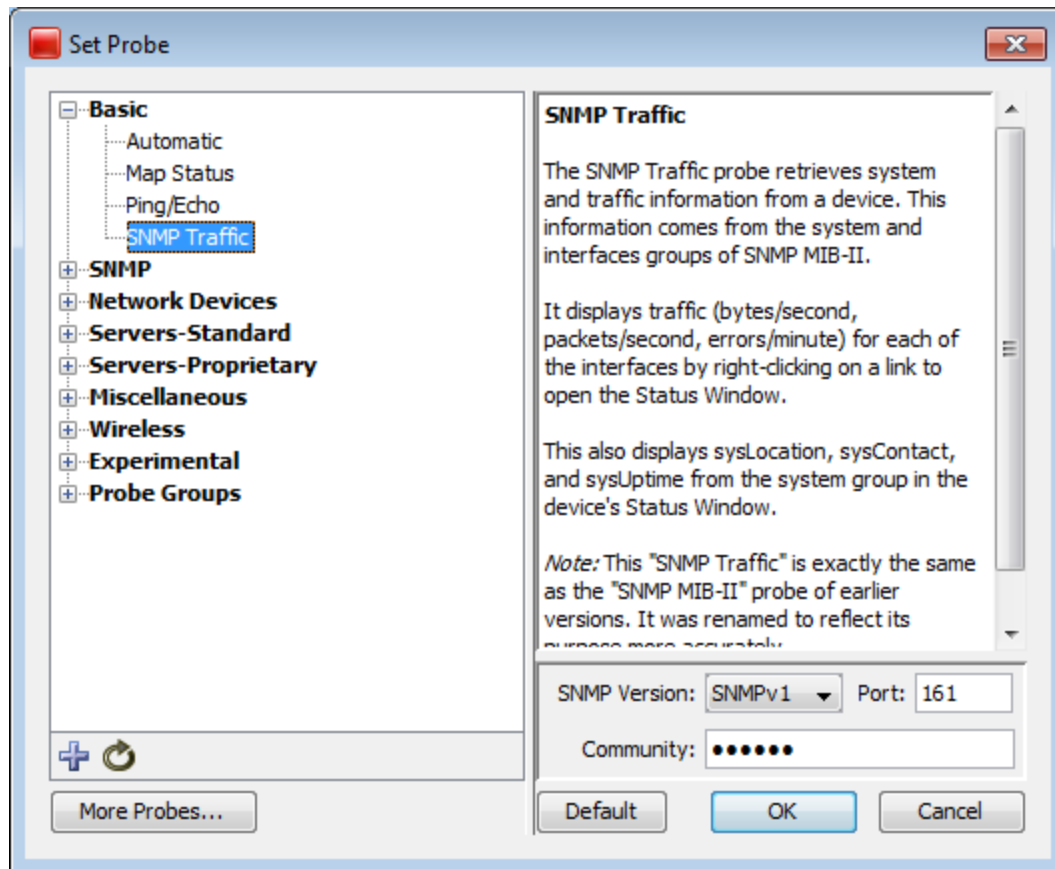
Set Probe Window

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. 464).

- **Basic Probes (Pg. 474)** - use the Basic probes to cover the majority of your needs for probing devices.
- **SNMP Probes (Pg. 476)**- use the SNMP probes to perform a wide variety of queries on SNMP devices.
- **Network Devices (Pg. 491)** - Use the network device probes to query network devices, such as routers, switches and UPS units.
- **PowerShell Probes** - Use these probes to get information from Windows machines using PowerShell scripts.
- **Servers-Standard (Pg. 537)** - use these probes to query various devices using one of many Standard protocols.
- **Servers-Proprietary (Pg. 515)** - use these probes to query various devices using one of many Proprietary protocols.
- **Miscellaneous Probes (Pg. 486)** - 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. 586)** - Use these probes to get vendor-specific information from a number of wireless devices.
- **WMI Probes (Pg. 572)** - 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. 635) and Network Device Probes (Pg. 491).

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. 537).

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. 486).

- **Demo probe** - Use this probe to create demonstration maps, which simulate a network and its activity.
- **Legacy probes** - These probes that have been superceded 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 "\{...}", followed by the string assigned to `stdout`.

Probe Reference Index

Basic [view*Basic*](#)

- [Basic > Automatic](#)*Basic > Automatic*
- [Basic > Map Status](#)*Basic > Map Status*
- [Basic > Ping/Echo](#)*Basic > Ping/Echo*
- [Basic > SNMP Traffic](#)*Basic > SNMP Traffic*

Experimental [view*Experimental*](#)

- [Experimental > Flow Exporter Status](#)*Experimental > Flow Exporter Status*
- [Experimental > InterMapper](#)*Experimental > InterMapper*
- [Experimental > sFlow v1.2](#)*Experimental > sFlow v1.2*
- [Experimental > sFlow Vers. 1.3](#)*Experimental > sFlow Vers. 1.3*

Miscellaneous [view*Miscellaneous*](#)

- [Miscellaneous > Demo Probe](#)*Miscellaneous > Demo Probe*
- [Miscellaneous > Legacy > Basic OID (v2c)](#)*Miscellaneous > Legacy > Basic OID (v2c)*
- [Miscellaneous > Legacy > Cisco (v2c)](#)*Miscellaneous > Legacy > Cisco (v2c)*
- [Miscellaneous > Legacy > SNMP v2c](#)*Miscellaneous > Legacy > SNMP v2c*
- [Miscellaneous > Nagios > Nagios Plugin](#)*Miscellaneous > Nagios > Nagios Plugin*

- Miscellaneous > Non Polling*Miscellaneous > Non Polling*
- Miscellaneous > Prototype SNMP Probe*Miscellaneous > Prototype SNMP Probe*
- Miscellaneous > TCP Check*Miscellaneous > TCP Check*

Network Devices   view*Network Devices*

- Network Devices > Apple > Apple AirPort (Extreme)*Network Devices > Apple > Apple AirPort (Extreme)*
- Network Devices > Apple > Apple AirPort (Graphite)*Network Devices > Apple > Apple AirPort (Graphite)*
- Network Devices > Cisco > Cisco IP SLA Jitter*Network Devices > Cisco > Cisco IP SLA Jitter*
- Network Devices > Cisco > Cisco N5000 with FEX Traffic*Network Devices > Cisco > Cisco N5000 with FEX Traffic*
- Network Devices > Cisco > Cisco Old CPU MIB*Network Devices > Cisco > Cisco Old CPU MIB*
- Network Devices > Cisco > Cisco Process and Memory Pool*Network Devices > Cisco > Cisco Process and Memory Pool*
- Network Devices > Cisco > Cisco Aironet*Network Devices > Cisco > Cisco Aironet*
- Network Devices > Cisco > Cisco ASA Firewall*Network Devices > Cisco > Cisco ASA Firewall*
- Network Devices > Cisco > Cisco Catalyst Switch*Network Devices > Cisco > Cisco Catalyst Switch*
- Network Devices > Cisco > Cisco Firepower Threat Defence ASA*Network Devices > Cisco > Cisco Firepower Threat Defence ASA*
- Network Devices > Cisco > Cisco WLC*Network Devices > Cisco > Cisco WLC*
- Network Devices > Juniper > Netscreen VPN*Network Devices > Juniper > Netscreen VPN*
- Network Devices > Karlnet Wireless*Network Devices > Karlnet Wireless*
- Network Devices > UPS > APC UPS AP961x*Network Devices > UPS > APC UPS AP961x*
- Network Devices > UPS > APC UPS*Network Devices > UPS > APC UPS*
- Network Devices > UPS > BestPower UPS*Network Devices > UPS > BestPower UPS*
- Network Devices > UPS > Exide UPS*Network Devices > UPS > Exide UPS*
- Network Devices > UPS > Liebert UPS EXM*Network Devices > UPS > Liebert UPS EXM*

- Network Devices > UPS > Liebert UPS OpenComms*Network Devices > UPS > Liebert UPS OpenComms*
- Network Devices > UPS > Liebert UPS Series 300*Network Devices > UPS > Liebert UPS Series 300*
- Network Devices > UPS > Liebert UPS*Network Devices > UPS > Liebert UPS*
- Network Devices > UPS > Standard UPS (RFC1628)*Network Devices > UPS > Standard UPS (RFC1628)*
- Network Devices > UPS > TrippLite UPS*Network Devices > UPS > TrippLite UPS*
- Network Devices > UPS > Victron UPS*Network Devices > UPS > Victron UPS*

PowerShell view*PowerShell*

- PowerShell > Disk Space*PowerShell > Disk Space*
- PowerShell > Remoting > Disk Space (Signed)*PowerShell > Remoting > Disk Space (Signed)*
- PowerShell > Remoting > Disk Space*PowerShell > Remoting > Disk Space*
- PowerShell > Remoting > Installed Software*PowerShell > Remoting > Installed Software*
- PowerShell > Remoting > Process Count*PowerShell > Remoting > Process Count*

Probe Groups view*Probe Groups*

- Probe Groups > Probe Group*Probe Groups > Probe Group*

SNMP view*SNMP*

- SNMP > Basic OID*SNMP > Basic OID*
- SNMP > Comparison*SNMP > Comparison*
- SNMP > High Threshold*SNMP > High Threshold*
- SNMP > Low Threshold*SNMP > Low Threshold*
- SNMP > Range Threshold*SNMP > Range Threshold*
- SNMP > Restricted Interface*SNMP > Restricted Interface*
- SNMP > Single OID Viewer*SNMP > Single OID Viewer*
- SNMP > SNMP High PPS*SNMP > SNMP High PPS*
- SNMP > SNMPv1 High Traffic*SNMP > SNMPv1 High Traffic*
- SNMP > SNMPv1 High Util*SNMP > SNMPv1 High Util*
- SNMP > String Comparison*SNMP > String Comparison*
- SNMP > Table Viewer*SNMP > Table Viewer*
- SNMP > Trap Viewer*SNMP > Trap Viewer*

Servers Proprietary view*Servers-Proprietary*

- Servers Proprietary > 4D Server*Servers Proprietary > 4D Server*
- Servers Proprietary > Apache > *Servers Proprietary > Apache >*
- Servers Proprietary > Apple > AppleShareIP*Servers Proprietary > Apple > AppleShareIP*
- Servers Proprietary > Apple > OS X Server > AFP*Servers Proprietary > Apple > OS X Server > AFP*
- Servers Proprietary > Apple > OS X Server > FTP*Servers Proprietary > Apple > OS X Server > FTP*
- Servers Proprietary > Apple > OS X Server > Info*Servers Proprietary > Apple > OS X Server > Info*
- Servers Proprietary > Apple > OS X Server > NAT*Servers Proprietary > Apple > OS X Server > NAT*
- Servers Proprietary > Apple > OS X Server > Print*Servers Proprietary > Apple > OS X Server > Print*
- Servers Proprietary > Apple > OS X Server > QTSS*Servers Proprietary > Apple > OS X Server > QTSS*
- Servers Proprietary > Apple > OS X Server > Web*Servers Proprietary > Apple > OS X Server > Web*
- Servers Proprietary > Apple > RTMP*Servers Proprietary > Apple > RTMP*
- Servers Proprietary > Apple > Xserve > Xserve G4*Servers Proprietary > Apple > Xserve > Xserve G4*
- Servers Proprietary > Apple > Xserve > Xserve G5*Servers Proprietary > Apple > Xserve > Xserve G5*
- Servers Proprietary > Apple > Xserve > Xserve RAID*Servers Proprietary > Apple > Xserve > Xserve RAID*
- Servers Proprietary > Apple > Xserve > Xserve Tiger (PPC)*Servers Proprietary > Apple > Xserve > Xserve Tiger (PPC)*
- Servers Proprietary > Barracuda > Barracuda HTTP*Servers Proprietary > Barracuda > Barracuda HTTP*
- Servers Proprietary > Barracuda > Barracuda HTTPS*Servers Proprietary > Barracuda > Barracuda HTTPS*
- Servers Proprietary > Big Brother Probe*Servers Proprietary > Big Brother Probe*
- Servers Proprietary > BlitzWatch*Servers Proprietary > BlitzWatch*
- Servers Proprietary > Citrix Server*Servers Proprietary > Citrix Server*

- Servers Proprietary > Dartware > DataCenter > IMAuth*Servers Proprietary > Dartware > DataCenter > IMAuth*
- Servers Proprietary > Dartware > DataCenter > IMDatabase*Servers Proprietary > Dartware > DataCenter > IMDatabase*
- Servers Proprietary > DND Protocol*Servers Proprietary > DND Protocol*
- Servers Proprietary > FileMaker Pro*Servers Proprietary > FileMaker Pro*
- Servers Proprietary > FirstClass Server*Servers Proprietary > FirstClass Server*
- Servers Proprietary > KeyServer*Servers Proprietary > KeyServer*
- Servers Proprietary > Lotus Notes*Servers Proprietary > Lotus Notes*
- Servers Proprietary > MeetingMaker*Servers Proprietary > MeetingMaker*
- Servers Proprietary > Microsoft > DHCP Lease Check*Servers Proprietary > Microsoft > DHCP Lease Check*
- Servers Proprietary > Microsoft > NT Services*Servers Proprietary > Microsoft > NT Services*
- Servers Proprietary > Microsoft > SQL Server Query*Servers Proprietary > Microsoft > SQL Server Query*
- Servers Proprietary > Nagios NRPE*Servers Proprietary > Nagios NRPE*

Servers Standard view*Servers-Standard*

- Servers Standard > Basic TCP (Blocked)*Servers Standard > Basic TCP (Blocked)*
- Servers Standard > Basic TCP*Servers Standard > Basic TCP*
- Servers Standard > Custom TCP*Servers Standard > Custom TCP*
- Servers Standard > CVS Server*Servers Standard > CVS Server*
- Servers Standard > DHCPv4/BOOTP*Servers Standard > DHCPv4/BOOTP*
- Servers Standard > Domain Name (DNS) > DNS: (A) Address*Servers Standard > Domain Name (DNS) > DNS: (A) Address*
- Servers Standard > Domain Name (DNS) > DNS: (MX) Mail Server*Servers Standard > Domain Name (DNS) > DNS: (MX) Mail Server*
- Servers Standard > Domain Name (DNS) > DNS: (NS) Name Server*Servers Standard > Domain Name (DNS) > DNS: (NS) Name Server*
- Servers Standard > Domain Name (DNS) > DNS: (PTR) Reverse Lookup*Servers Standard > Domain Name (DNS) > DNS: (PTR) Reverse Lookup*
- Servers Standard > Domain Name (DNS) > DNS: (TXT) Text Record*Servers Standard > Domain Name (DNS) > DNS: (TXT) Text Record*
- Servers Standard > FTP > FTP (Login)*Servers Standard > FTP > FTP (Login)*
- Servers Standard > FTP > FTP (No Login)*Servers Standard > FTP > FTP (No Login)*

- Servers Standard > Gopher*Servers Standard > Gopher*

- Servers Standard > Host Resources*Servers Standard > Host Resources*

- Servers Standard > HTTP & HTTPS > HTTP (Don't Match)*Servers Standard > HTTP & HTTPS > HTTP (Don't Match)*

- Servers Standard > HTTP & HTTPS > HTTP (Follow Redirects)*Servers Standard > HTTP & HTTPS > HTTP (Follow Redirects)*

- Servers Standard > HTTP & HTTPS > HTTP (Post)*Servers Standard > HTTP & HTTPS > HTTP (Post)*

- Servers Standard > HTTP & HTTPS > HTTP (Proxy)*Servers Standard > HTTP & HTTPS > HTTP (Proxy)*

- Servers Standard > HTTP & HTTPS > HTTP (Redirect)*Servers Standard > HTTP & HTTPS > HTTP (Redirect)*

- Servers Standard > HTTP & HTTPS > HTTP*Servers Standard > HTTP & HTTPS > HTTP*

- Servers Standard > HTTP & HTTPS > HTTPS TLSv1.0*Servers Standard > HTTP & HTTPS > HTTPS TLSv1.0*

- Servers Standard > HTTP & HTTPS > HTTPS (Follow Redirects)*Servers Standard > HTTP & HTTPS > HTTPS (Follow Redirects)*

- Servers Standard > HTTP & HTTPS > HTTPS (Post)*Servers Standard > HTTP & HTTPS > HTTPS (Post)*

- Servers Standard > HTTP & HTTPS > HTTPS (Redirect)*Servers Standard > HTTP & HTTPS > HTTPS (Redirect)*

- Servers Standard > HTTP & HTTPS > HTTPS (SSLv3)*Servers Standard > HTTP & HTTPS > HTTPS (SSLv3)*

- Servers Standard > HTTP & HTTPS > HTTPS*Servers Standard > HTTP & HTTPS > HTTPS*

- Servers Standard > IPMI v2.0*Servers Standard > IPMI v2.0*

- Servers Standard > IRC*Servers Standard > IRC*

- Servers Standard > LDAP > LDAP SSL*Servers Standard > LDAP > LDAP SSL*

- Servers Standard > LDAP > LDAP*Servers Standard > LDAP > LDAP*

- Servers Standard > LPR*Servers Standard > LPR*

- Servers Standard > Mail > IMAP4 SSL*Servers Standard > Mail > IMAP4 SSL*

- Servers Standard > Mail > IMAP4*Servers Standard > Mail > IMAP4*

- Servers Standard > Mail > POP3 SSL*Servers Standard > Mail > POP3 SSL*

- Servers Standard > Mail > POP3*Servers Standard > Mail > POP3*

- Servers Standard > Mail > Roundtrip IMAP*Servers Standard > Mail > Roundtrip IMAP*

- Servers Standard > Mail > Roundtrip POP*Servers Standard > Mail > Roundtrip POP*

- [Servers Standard > Mail > SMTP TLS](#)*Servers Standard > Mail > SMTP TLS*

- [Servers Standard > Mail > SMTP](#)*Servers Standard > Mail > SMTP*

- [Servers Standard > Multimedia > Multicast Listener](#)*Servers Standard > Multimedia > Multicast Listener*

- [Servers Standard > Multimedia > RTSP](#)*Servers Standard > Multimedia > RTSP*

- [Servers Standard > Network Time](#)*Servers Standard > Network Time*

- [Servers Standard > NNTP](#)*Servers Standard > NNTP*

- [Servers Standard > RADIUS](#)*Servers Standard > RADIUS*

- [Servers Standard > SIP over UDP](#)*Servers Standard > SIP over UDP*

- [Servers Standard > SNPP](#)*Servers Standard > SNPP*

- [Servers Standard > SSH](#)*Servers Standard > SSH*

- [Servers Standard > Subversion > SVN (Apache)](#)*Servers Standard > Subversion > SVN (Apache)*

- [Servers Standard > Subversion > SVN (Svnserve)](#)*Servers Standard > Subversion > SVN (Svnserve)*

- [Servers Standard > Telnet](#)*Servers Standard > Telnet*

- [Servers Standard > VNC Server](#)*Servers Standard > VNC Server*

Splunk [view](#)

- [Splunk > Layer 2 Output](#)

WMI [view](#)*WMI*

- [WMI > WMI CPU Utilization](#)*WMI > WMI CPU Utilization*

- [WMI > WMI Disk Available](#)*WMI > WMI Disk Available*

- [WMI > WMI Disk Fragmentation Analysis](#)*WMI > WMI Disk Fragmentation Analysis*

- [WMI > WMI Event Log](#)*WMI > WMI Event Log*

- [WMI > WMI File Check](#)*WMI > WMI File Check*

- [WMI > WMI Folder Check](#)*WMI > WMI Folder Check*

- [WMI > WMI Free Memory](#)*WMI > WMI Free Memory*

- [WMI > WMI Installed Software](#)*WMI > WMI Installed Software*

- [WMI > WMI Logged on Users](#)*WMI > WMI Logged on Users*

- [WMI > WMI MSExchange 2007 Hub Transport Server](#)*WMI > WMI MSExchange 2007 Hub Transport Server*

- [WMI > WMI MSExchange 2007 Mailbox Server](#)*WMI > WMI MSExchange 2007 Mailbox Server*

- WMI > WMI Network Utilization*WMI > WMI Network Utilization*

- WMI > WMI Process Monitor*WMI > WMI Process Monitor*

- WMI > WMI Service Monitor*WMI > WMI Service Monitor*

- WMI > WMI SQL Server 2008 Service Monitor*WMI > WMI SQL Server 2008 Service Monitor*

- WMI > WMI System Accessibility*WMI > WMI System Accessibility*

- WMI > WMI System Information*WMI > WMI System Information*

- WMI > WMI Top Processes*WMI > WMI Top Processes*

Wireless   view*Wireless*

- Wireless > Alvarion > Alvarion B 14 & B 28 (BU)*Wireless > Alvarion > Alvarion B 14 & B 28 (BU)*

- Wireless > Alvarion > Alvarion B 14 & B 28 (RB)*Wireless > Alvarion > Alvarion B 14 & B 28 (RB)*

- Wireless > Alvarion > BreezeACCESS (AU)*Wireless > Alvarion > BreezeACCESS (AU)*

- Wireless > Alvarion > BreezeACCESS (SU)*Wireless > Alvarion > BreezeACCESS (SU)*

- Wireless > Alvarion > BreezeACCESS LB*Wireless > Alvarion > BreezeACCESS LB*

- Wireless > Alvarion > BreezeACCESS VL (AU)*Wireless > Alvarion > BreezeACCESS VL (AU)*

- Wireless > Alvarion > BreezeACCESS VL (SU)*Wireless > Alvarion > BreezeACCESS VL (SU)*

- Wireless > Atmel > Atmel AT76C510*Wireless > Atmel > Atmel AT76C510*

- Wireless > Basic > IEEE 802.11*Wireless > Basic > IEEE 802.11*

- Wireless > Basic > SNMP for Wireless*Wireless > Basic > SNMP for Wireless*

- Wireless > Canopy > Canopy (AP)*Wireless > Canopy > Canopy (AP)*

- Wireless > Canopy > Canopy (SM)*Wireless > Canopy > Canopy (SM)*

- Wireless > Canopy > Canopy Backhaul (45 Mbps/FW 5830)*Wireless > Canopy > Canopy Backhaul (45 Mbps/FW 5830)*

- Wireless > Canopy > Canopy Backhaul (60 Mbp/FW 5840)*Wireless > Canopy > Canopy Backhaul (60 Mbp/FW 5840)*

- Wireless > Canopy > Canopy Backhaul (Master)*Wireless > Canopy > Canopy Backhaul (Master)*

- Wireless > Canopy > Canopy Backhaul (Slave)*Wireless > Canopy > Canopy Backhaul (Slave)*

- Wireless > Canopy > Canopy CMM Micro*Wireless > Canopy > Canopy CMM Micro*

- Wireless > CB3 > CB3 Bridge*Wireless > CB3 > CB3 Bridge*

- Wireless > CB3 > CB3 Deluxe Bridge*Wireless > CB3 > CB3 Deluxe Bridge*
- Wireless > Inscape Data > AirEther AB54 Series AP (AP Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (AP Mode)*
- Wireless > Inscape Data > AirEther AB54 Series AP (Bridge Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (Bridge Mode)*
- Wireless > Inscape Data > AirEther AB54 Series AP (Client Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (Client Mode)*
- Wireless > Inscape Data > AirEther AB54 Series AP (Repeater Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (Repeater Mode)*
- Wireless > Inscape Data > AirEther CB54 Series Client*Wireless > Inscape Data > AirEther CB54 Series Client*
- Wireless > MikroTik > MT Radio Uplink*Wireless > MikroTik > MT Radio Uplink*
- Wireless > MikroTik > MT Routerboard*Wireless > MikroTik > MT Routerboard*
- Wireless > MikroTik > MT Software Only*Wireless > MikroTik > MT Software Only*
- Wireless > MikroTik > WDS Bridge*Wireless > MikroTik > WDS Bridge*
- Wireless > Motorola > PTP 400 Series Bridge*Wireless > Motorola > PTP 400 Series Bridge*
- Wireless > Motorola > PTP 600 Series Bridge*Wireless > Motorola > PTP 600 Series Bridge*
- Wireless > Orthogon > Gemini*Wireless > Orthogon > Gemini*
- Wireless > Orthogon > Spectra*Wireless > Orthogon > Spectra*
- Wireless > Other > HTTP*Wireless > Other > HTTP*
- Wireless > Proxim > Proxim AP 2000*Wireless > Proxim > Proxim AP 2000*
- Wireless > Proxim > Proxim AP 4000*Wireless > Proxim > Proxim AP 4000*
- Wireless > Proxim > Proxim AP 600*Wireless > Proxim > Proxim AP 600*
- Wireless > Proxim > Proxim AP 700*Wireless > Proxim > Proxim AP 700*
- Wireless > Proxim > Proxim LAN Access Point*Wireless > Proxim > Proxim LAN Access Point*
- Wireless > Proxim > Tsunami GX*Wireless > Proxim > Tsunami GX*
- Wireless > Proxim > Tsunami MP.11 BSU*Wireless > Proxim > Tsunami MP.11 BSU*
- Wireless > Proxim > Tsunami MP.11 SU*Wireless > Proxim > Tsunami MP.11 SU*
- Wireless > Redline > AN50*Wireless > Redline > AN50*
- Wireless > smartBridges > airBridge*Wireless > smartBridges > airBridge*
- Wireless > smartBridges > airClient Nexus PRO total*Wireless > smartBridges > airClient Nexus PRO total*

- [Wireless > smartBridges > airClient Nexus](#)*Wireless > smartBridges > airClient Nexus*
- [Wireless > smartBridges > airHaul Nexus PRO total](#)*Wireless > smartBridges > airHaul Nexus PRO total*
- [Wireless > smartBridges > airHaul Nexus](#)*Wireless > smartBridges > airHaul Nexus*
- [Wireless > smartBridges > airHaul2 Nexus PRO](#)*Wireless > smartBridges > airHaul2 Nexus PRO*
- [Wireless > smartBridges > airPoint Nexus PRO total](#)*Wireless > smartBridges > airPoint Nexus PRO total*
- [Wireless > smartBridges > airPoint Nexus](#)*Wireless > smartBridges > airPoint Nexus*
- [Wireless > smartBridges > airPoint](#)*Wireless > smartBridges > airPoint*
- [Wireless > smartBridges > airPoint2 Nexus PRO](#)*Wireless > smartBridges > airPoint2 Nexus PRO*
- [Wireless > Trango > Trango M2400S (AP)](#)*Wireless > Trango > Trango M2400S (AP)*
- [Wireless > Trango > Trango M5800S](#)*Wireless > Trango > Trango M5800S*
- [Wireless > Trango > Trango M5830S (SU)](#)*Wireless > Trango > Trango M5830S (SU)*
- [Wireless > Trango > Trango M5830S](#)*Wireless > Trango > Trango M5830S*
- [Wireless > Trango > Trango M900S (AP)](#)*Wireless > Trango > Trango M900S (AP)*
- [Wireless > Trango > Trango P5830S (master)](#)*Wireless > Trango > Trango P5830S (master)*
- [Wireless > Trango > Trango P5830S (remote)](#)*Wireless > Trango > Trango P5830S (remote)*
- [Wireless > Tranzeo > Sixth Generation AP](#)*Wireless > Tranzeo > Sixth Generation AP*
- [Wireless > Tranzeo > Sixth Generation CPE](#)*Wireless > Tranzeo > Sixth Generation CPE*
- [Wireless > Tranzeo > Sixth Generation PxP](#)*Wireless > Tranzeo > Sixth Generation PxP*
- [Wireless > Tranzeo > Tranzeo (AP)](#)*Wireless > Tranzeo > Tranzeo (AP)*
- [Wireless > Tranzeo > Tranzeo (PXP)](#)*Wireless > Tranzeo > Tranzeo (PXP)*
- [Wireless > Tranzeo > Tranzeo (SAI)](#)*Wireless > Tranzeo > Tranzeo (SAI)*
- [Wireless > Tranzeo > Tranzeo 58XX Series Backhaul](#)*Wireless > Tranzeo > Tranzeo 58XX Series Backhaul*
- [Wireless > Tranzeo > Tranzeo AP 5A (44R)](#)*Wireless > Tranzeo > Tranzeo AP 5A (44R)*
- [Wireless > Tranzeo > Tranzeo AP 5A](#)*Wireless > Tranzeo > Tranzeo AP 5A*
- [Wireless > Tranzeo > Tranzeo Classic](#)*Wireless > Tranzeo > Tranzeo Classic*
- [Wireless > Tranzeo > Tranzeo CPE 200 (1.77.R)](#)*Wireless > Tranzeo > Tranzeo CPE 200 (1.77.R)*

- [Wireless > Tranzeo > Tranzeo CPE 200](#)*Wireless > Tranzeo > Tranzeo CPE 200*
- [Wireless > Tranzeo > Tranzeo CPE 5A (44R)](#)*Wireless > Tranzeo > Tranzeo CPE 5A (44R)*
- [Wireless > Tranzeo > Tranzeo CPE 5A](#)*Wireless > Tranzeo > Tranzeo CPE 5A*
- [Wireless > Tranzeo > Tranzeo TR CPE](#)*Wireless > Tranzeo > Tranzeo TR CPE*
- [Wireless > WaveRider > CCU](#)*Wireless > WaveRider > CCU*
- [Wireless > WaveRider > EUM](#)*Wireless > WaveRider > EUM*

Basic

- [Basic > Automatic](#)*Basic > Automatic*
- [Basic > Map Status](#)*Basic > Map Status*
- [Basic > Ping/Echo](#)*Basic > Ping/Echo*
- [Basic > SNMP Traffic](#)*Basic > SNMP Traffic*

  [To Probe Index](#)*Probe Reference Index*

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 mimimum 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 determined 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`

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`

SNMP

- SNMP > Basic OID*SNMP > Basic OID*
- SNMP > Comparison*SNMP > Comparison*
- SNMP > High Threshold*SNMP > High Threshold*
- SNMP > Low Threshold*SNMP > Low Threshold*
- SNMP > Range Threshold*SNMP > Range Threshold*
- SNMP > Restricted Interface*SNMP > Restricted Interface*
- SNMP > Single OID Viewer*SNMP > Single OID Viewer*
- SNMP > SNMP High PPS*SNMP > SNMP High PPS*
- SNMP > SNMPv1 High Traffic*SNMP > SNMPv1 High Traffic*
- SNMP > SNMPv1 High Util*SNMP > SNMPv1 High Util*
- SNMP > String Comparison*SNMP > String Comparison*
- SNMP > Table Viewer*SNMP > Table Viewer*
- SNMP > Trap Viewer*SNMP > Trap Viewer*

To Probe Index*Probe Reference Index*

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 > SNMPv1 High Traffic

SNMPv1 - 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 > SNMPv1 High Util

SNMPv1 - 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 ifOperStatus 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 *ifHCOutOctets* 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.

Parameters

None.

Filename: `com.dartware.snmp.tableviewer.txt`
Version: `1.10`

[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 retireve 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"

> **NOTE:** 1 - This probe file contains the lines above in a single-line format suitable for copying and pasting.

> **NOTE:** 2 - 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: `2.4`

[Back to Top](#)

Miscellaneous

- [Miscellaneous > Demo Probe](#)*Miscellaneous > Demo Probe*
- [Miscellaneous > Legacy > Basic OID (v2c)](#)*Miscellaneous > Legacy > Basic OID (v2c)*
- [Miscellaneous > Legacy > Cisco (v2c)](#)*Miscellaneous > Legacy > Cisco (v2c)*
- [Miscellaneous > Legacy > SNMP v2c](#)*Miscellaneous > Legacy > SNMP v2c*
- [Miscellaneous > Nagios > Nagios Plugin](#)*Miscellaneous > Nagios > Nagios Plugin*
- [Miscellaneous > Non Polling](#)*Miscellaneous > Non Polling*
- [Miscellaneous > Prototype SNMP Probe](#)*Miscellaneous > Prototype SNMP Probe*
- [Miscellaneous > TCP Check](#)*Miscellaneous > TCP Check*

  [To Probe Index](#)*Probe Reference Index*

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.

Parameters

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: `1.7`

[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.

Parameters

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: `1.6`

[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 MIB-II 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.

Additional Parameters

None.

Filename: `com.dartware.snmpv2c`
Version: `1.7`

[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=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.

Filename: `com.dartware.snmp.tcpcheck`
Version: `1.6`

[Back to Top](#)

Network Devices

- [Network Devices > Apple > Apple AirPort (Extreme)](#)*Network Devices > Apple > Apple AirPort (Extreme)*

- [Network Devices > Apple > Apple AirPort (Graphite)](#)*Network Devices > Apple > Apple AirPort (Graphite)*

- [Network Devices > Cisco > Cisco IP SLA Jitter](#)*Network Devices > Cisco > Cisco IP SLA Jitter*

- [Network Devices > Cisco > Cisco N5000 with FEX Traffic](#)*Network Devices > Cisco > Cisco N5000 with FEX Traffic*

- [Network Devices > Cisco > Cisco Old CPU MIB](#)*Network Devices > Cisco > Cisco Old CPU MIB*

- [Network Devices > Cisco > Cisco Process and Memory Pool](#)*Network Devices > Cisco > Cisco Process and Memory Pool*

- [Network Devices > Cisco > Cisco Aironet](#)*Network Devices > Cisco > Cisco Aironet*

- [Network Devices > Cisco > Cisco ASA Firewall](#)*Network Devices > Cisco > Cisco ASA Firewall*

- [Network Devices > Cisco > Cisco Catalyst Switch](#)*Network Devices > Cisco > Cisco Catalyst Switch*

- [Network Devices > Cisco > Cisco Firepower Threat Defence ASA](#)*Network Devices > Cisco > Cisco Firepower Threat Defence ASA*

- [Network Devices > Cisco > Cisco WLC](#)*Network Devices > Cisco > Cisco WLC*

- [Network Devices > Juniper > Netscreen VPN](#)*Network Devices > Juniper > Netscreen VPN*

- [Network Devices > Karlnet Wireless](#)*Network Devices > Karlnet Wireless*

- [Network Devices > UPS > APC UPS AP961x](#)*Network Devices > UPS > APC UPS AP961x*

- [Network Devices > UPS > APC UPS](#)*Network Devices > UPS > APC UPS*

- [Network Devices > UPS > BestPower UPS](#)*Network Devices > UPS > BestPower UPS*

- [Network Devices > UPS > Exide UPS](#)*Network Devices > UPS > Exide UPS*

- [Network Devices > UPS > Liebert UPS EXM](#)*Network Devices > UPS > Liebert UPS EXM*

- [Network Devices > UPS > Liebert UPS OpenComms](#)*Network Devices > UPS > Liebert UPS OpenComms*

- [Network Devices > UPS > Liebert UPS Series 300](#)*Network Devices > UPS > Liebert UPS Series 300*

- [Network Devices > UPS > Liebert UPS](#)*Network Devices > UPS > Liebert UPS*

- [Network Devices > UPS > Standard UPS (RFC1628)](#)*Network Devices > UPS > Standard UPS (RFC1628)*
- [Network Devices > UPS > TrippLite UPS](#)*Network Devices > UPS > TrippLite UPS*
- [Network Devices > UPS > Victron UPS](#)*Network Devices > UPS > Victron UPS*

[To Probe Index](#)*Probe Reference Index*

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.

Filename: `com.dartware.snmp.airport.ext`
 Version: `1.6`

[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.

Filename: `com.dartware.snmp.cisco-ip-sla.txt`
 Version: `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.

Filename: `com.dartware.snmp.cisco.n5kfex.traffic.txt`
Version: `1.1`

[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.

Filename: `com.dartware.snmp.cisco`
Version: `1.9`

[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.

Filename: `com.dartware.snmp.cisconewmib`
 Version: `1.9`

[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.

Filename: `com.dartware.snmp.aironet`
 Version: `1.6`

[Back to Top](#)

Network Devices > Cisco > Cisco ASA Firewall

Cisco ASA Firewall
This probe monitors a Cisco ASA firewall or security context.

It monitors the CPU utilization, memory utilization, active connections, connections per second, primary unit status, and secondary unit status.

It will generate an ALARM if:

-*CPU % busy* averaged over 1 minute exceeds a threshold

-*Active connections* exceeds a threshold

-*Connections per second* averaged over 1 minute exceeds a threshold

-*Primary unit status* is abnormal

-*Secondary unit status* is abnormal

Parameters

CPU Utilization Threshold - enter a percentage of CPU usage required to generate an ALARM.

Active Connections Alarm Threshold - enter a maximum number of active connections required to generate an ALARM.

Connections Per Second Alarm Threshold - enter a maximum number of connections per second required to generate an ALARM.

Filename: `com.helpsystems.snmp.cisco.asa.firewall`
Version: `1.0`

[Back to Top](#)

Network Devices > Cisco > Cisco Catalyst Switch

Cisco Catalyst Switch

This probe monitors the following Cisco Catalyst switches:

- a fixed configuration Cisco Catalyst switch
- a modular Cisco Catalyst switch
- an entire stack of Cisco Catalyst switches

It has been tested with Catalyst 2960, Catalyst 3560, Catalyst 3750, Catalyst 3750X, and Catalyst 3850 switches.

The probe will generate a warning or alarm alert if:

-the % CPU utilization over a 1 minute interval exceeds a threshold

-the free memory remaining in bytes falls below a threshold

-the state of a switch is abnormal

-the outlet exhaust temperature of a switch exceeds normal operational limits

-a fan malfunctions or fails

-a power supply malfunctions or fails

-the stack ring is not redundant

Warning and alarm alerts can be turned on or off by adjusting the probe parameters. They are on by default.

Important Notes:

(1) When you restart the Intermapper server or add a new Catalyst switch to a map it takes several poll cycles for the probe to collect and display information about the switch or switch stack in the Device Status window. The more switches in a stack the longer it will take to display the information. Also, newer switches like the Catalyst 3850 with fast SNMP processing will display information twice as fast as older switches.

(2) Catalyst 3750X IOS Release 12.2(55) has a bug where SNMP does not return information for 'Fan 2' for the second and subsequent switches in the stack. This affects the "#Fan" column in the Device Status window. The '#Fan' column will indicate only 1 fan is installed, when there may actually be 2. Upgrading to IOS Release 12.2(58) or later will fix the problem.

(3) Please report bugs and enhancement requests to Help Systems so that this probe can be enhanced and kept up to date.

Parameters

- *CPU Busy - Warning Threshold* - the threshold in CPU usage (percent) required to place the device in **Warning** status.
- *CPU Busy - Alarm Threshold* - the threshold in CPU usage (percent) required to place the device in **Alarm** status.
- *Free Memory - Warning Threshold* - the threshold (in bytes) of memory remaining required to place the device in **Warning** status.
- *Free Memory - Alarm Threshold* - the threshold (in bytes) of memory remaining required to place the device in **Alarm** status.
- *CPU Warnings[On,Off]* - Set to **Off** to prevent **Warning** status notifications for CPU usage above the specified threshold. Defaults to **On**.
- *CPU Alarms[On,Off]* - Set to **Off** to prevent **Alarm** status notifications for CPU usage above the specified threshold. Defaults to **On**.
- *Memory Warnings[On,Off]* - Set to **Off** to prevent **Warning** status notifications for remaining memory below the specified threshold. Defaults to **On**.

- *Memory Alarms[On,Off]* - Set to **Off** to prevent **Alarm** status notifications for remaining memory below the specified threshold. Defaults to **On**.
- *State Alarms[On,Off]* - Set to **Off** to prevent monitoring the Cisco switch states. Defaults to **On**.
- *PS Warnings[On,Off]* - Set to **Off** to prevent **Warning**s for power supply issues. Defaults to **On**.
- *PS Alarms[On,Off]* - Set to **Off** to prevent **Alarm**s for power supply issues. Defaults to **On**.
- *Fan Warnings[On,Off]* - Set to **Off** to prevent **Warning**s for fan issues. Defaults to **On**.
- *Fan Alarms[On,Off]* - Set to **Off** to prevent **Alarm**s for fan issues. Defaults to **On**.
- *Temperature Warnings[On,Off]* - Set to **Off** to prevent **Warning**s for temperature issues. Defaults to **On**.
- *Temperature Alarms[On,Off]* - Set to **Off** to prevent **Alarm**s for temperature issues. Defaults to **On**.
- *Stack Alarms[On,Off]* - Set to **Off** to prevent **Alarm**s when the stack ring is not redundant. Defaults to **On**.

Filename: `com.helpsystems.snmp.catalystswitch`
Version: `1.0`

[Back to Top](#)

Network Devices > Cisco > Cisco Firepower Threat Defence ASA

Cisco Firepower Threat Defence ASA
This probe monitors a Cisco Firepower Threat Defence ASA.

It monitors CPU utilization, system memory utilization, active connections, and connection setups.

The probe generates an ALARM if:

- *% CPU Busy (5 min)* exceeds a threshold

- *% System Memory Used* exceeds a threshold

- *% Active Connections Used* exceeds a threshold

- *Connections/Sec (5 min)* exceeds a threshold

- *Connections Denied (1 min)* exceeds a threshold

Set a threshold to 0 to suppress the alarm for that threshold.

Parameters

CPU Utilization Alarm Threshold - the percentage of CPU usage required to generate an ALARM.

System Memory Used Alarm Threshold - the percentage of system memory usage required to generate an ALARM.

Active Connections Alarm Threshold - the maximum number of active connections required to generate an ALARM.

Connections Per Second Alarm Threshold - the maximum number of connections per second required to generate an ALARM.

Denied Connections Per Minute Alarm Threshold - the maximum number of denied connections per minute required to generate an ALARM.

Notes:

- You cannot poll consolidated data for Firepower Threat Defense clusters. Each individual Firepower Threat Defense device is polled separately using its Local IP address and appears on the Intermapper map. For example, if your cluster has two Firepower Threat Defense devices, two devices appear on the Intermapper map.

- This probe monitors only the ASA part of the Firepower Threat Defence Device. The IPS (snort) and DDOS (radware) parts cannot be monitored.

Filename:
`com.helpsystems.snmp.cisco.firepowerthreatdefence.asa`
 Version: `1.0`

[Back to Top](#)

Network Devices > Cisco > Cisco WLC

Cisco WLC
This probe monitors a Cisco WLC (Wireless LAN Controller).

It will generate an ALARM if:

-*Memory Utilization* exceeds a threshold

-*CPU Utilization* exceeds a threshold

-*Internal Temperature* exceeds a threshold

-*Power Supply Status* is FAIL

-*Connected Clients* exceeds a threshold

Parameters

Memory Threshold - enter a memory usage value (in Mb) required to generate an ALARM. Enter 0 to suppress Memory Utilization alarms.

CPU Utilization Threshold - enter a percentage of CPU usage required to generate an ALARM. Enter 0 to suppress CPU Utilization alarms.

Internal Temperature Threshold - enter an internal temperature (in degrees Celsius) required to generate an ALARM. Enter 0 to suppress Internal Temperature alarms.

Connected Clients Threshold - enter a maximum number of connected clients required to generate an ALARM. Enter 0 to suppress Connected Clients alarms.

> **NOTE:** 1 - This probe has been tested with several models of Cisco WLC including the 3504, 5508, and 8540 models. It should work with other models but has not been tested. Monitoring of power supplies and SSO Sync Status is release dependent.

> **NOTE:** 2 - This probe monitors a Cisco WLC for up to 16 WLAN SSIDs. If you need to monitor more than 16 WLAN SSIDS you will need to modify the probe.

Filename: `com.helpsystems.snmp.cisco.wlc`
 Version: `1.1`

[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

This probe works best with devices which have implemented the following MIB (s):

- *APC UPS MIB* - [... enterprises.apc.products.hardware.ups / ... 1.3.6.1.4.1.318.1.1.1]
- *APC Environmental Monitoring MIB* - [... enterprises.apc.products.hardware.environmentalMonitor / ... 1.3.6.1.4.1.318.1.1.10]

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
- *Enviromental Monitor* - probe name, number of probes, current temperature & humidity, high & low threshold configurations.

Alarms

- If unit goes onto battery or goes off-line.
- If battery needs replacement.
- If the UPS' internal temperature/humidity threshold is exceeded (must also be enabled).

Warnings

- If unit goes onto "Smart Trim" or "Smart Boost"

Parameters

None.

Filename: `com.dartware.ups.apc-ap961x.txt`
Version: `3.6`

[Back to Top](#)

Network Devices > UPS > APC UPS

APC UPS
Use this probe with APC UPS devices.

This probe works best with devices which have implemented the following MIB (s):

- APC UPS MIB - [... enterprises.apc.products.hardware.ups / ... 1.3.6.1.4.1.318.1.1.1]

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

Alarms

- If unit goes onto battery or goes off-line.
- If battery needs replacement.
- If the battery temperature exceeds user-specified thresholds (see "Parameters" below).

Warnings

- If unit goes onto "Smart Trim" or "Smart Boost"
- If the battery temperature exceeds user-specified thresholds (see "Parameters" below).

Parameters

- *Units of Temperature (C / F)* - Determines how the following thresholds are interpreted.
- *Alarm Threshold - Low Temp*: Threshold for alarm state (see above).
- *Warning Threshold - Low Temp* - Threshold for alarm state (see above).
- *Warning Threshold - High Temp* - Threshold for warning state (see above).
- *Alarm Threshold - High Temp* - Threshold for warning state (see above).

Filename: `com.dartware.ups.apc.txt`
Version: `3.6`

[Back to Top](#)

Network Devices > UPS > BestPower UPS

BestPower UPS
Use this probe with BestPower UPS devices.

This probe works best with devices which have implemented the following MIB (s):

- BestPower MIB - [... enterprises.bestPower.bestLink / ... 1.2947.1]

Displayed Values

vendor, model, firmware version, VA Rating, time on battery, time remaining, (*input & output:* voltage, current, frequency), output power, internal temperature.

Alarms

- Warning: If UPS loses AC power.
- Alarm: If minutes of battery life remaining is less than specified threshold.

Parameters

- *BatteryRemainingAlarm* - Threshold for alarm state (see above).

Filename: `com.dartware.ups.bestpower.txt`
Version: `2.12`

[Back to Top](#)

Network Devices > UPS > Exide UPS

Exide UPS

Use this probe with Exide UPS devices.

This probe works best with devices which have implemented the following MIB:

- UPS MIB (RFC 1628) [... mib-2.upsMIB / ... 1.33]
- Exide XUPS MIB [... enterprises.powerware / ... 1.534]

Displayed Values

- *UPS* - vendor, model, software version, firmware version
- *Battery* - output source, battery status, battery voltage, battery current
- *Input* - Hz, volts, amps, kWatts
- *Output* - Hz, volts, amps, kWatts, output load percent

Displayed Values

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 EXM

Liebert UPS - EXM

Use this probe with the Liebert EXM Power System line of UPS devices.

This probe works best with devices which have implemented the following MIB:

- Liebert UPS MIB - [... enterprises.emerson.liebertCorp.liebertUps / ... 1.476.1.1]

Displayed Values

MIB, vendor, model, & software version

Parameters

None.

Filename: `com.dartware.ups.liebert-exm.txt`
Version: `1.2`

[Back to Top](#)

Network Devices > UPS > Liebert UPS OpenComms

Liebert UPS - OpenComms

Use this probe with Liebert UPS equipped with an OpenComms Network Management Card.

This probe works best with devices which have implemented the following MIB(s):

- *UPS MIB (RFC 1628)* - [… mib-2.upsMIB / … 1.33]
- *Liebert Global Products MIB* - [… enterprises.emerson.liebertCorp.liebertGlobalProducts / … 1.476.1.42]

Displayed Values

- *UPS* - vendor, model, software version, firmware version
- *Battery* - output source, battery status, battery voltage, battery current
- *Input* - Hz, volts, amps, kWatts
- *Output* - Hz, volts, amps, kWatts, output load percent
- *Temperature* - battery, ambient

Alarms

If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).

Parameters

None.

Filename: `com.dartware.ups.liebert-opencomms.txt`
Version: `2.13`

[Back to Top](#)

Network Devices > UPS > Liebert UPS Series 300

Liebert UPS - Series 300

Use this probe with the Liebert Series 300 line of UPS devices.

This probe works best with devices which have implemented the following MIB:

- LIEBERT-SERIES-300-UPS-MIB\p\ [...
enterprises.emerson.liebertCorp.liebertUps.luExtensions.luCore / ...
1.476.1.1.1.1] and [... luExtensions.luUPStationS / ... 1.2]

Displayed Values

- *UPS* - vendor, model, software version, firmware version
- *Battery* - output load (%), battery status, battery voltage, battery current
- *three input, output, and bypass phases:* voltage, current
- *frequencies:* input, output, bypass

Alarms

If the device is reporting any alarms. (The MIB includes a comprehensive list of alarms).

Parameters

None.

Filename: `com.dartware.ups.liebert-series300.txt`
 Version: `2.9`

[Back to Top](#)

Network Devices > UPS > Liebert UPS

Liebert UPS

This probe is meant to aid Dartware's development of probes for the Liebert product line.

Check other probes to see if one exists for your Liebert UPS device.

If not, select this probe, copy the contents of the status window, and email it to support.intermapper@helpsystems.com. We'll try to develop a probe for your device as soon as we can.

This probe works best with devices which have implemented the following MIB:

- Liebert UPS MIB - [... enterprises.emerson.liebertCorp.liebertUps / ...
1.476.1.1]

Displayed Values

MIB, vendor, model, & software version

Parameters

None.

Filename: `com.dartware.ups.liebert-ups.txt`
Version: `2.10`

[Back to Top](#)

Network Devices > UPS > Standard UPS (RFC1628)

Standard UPS (RFC1628)
Use this probe with UPS devices.

This probe works best with devices which have implemented the following MIB:

- UPS MIB (RFC 1628) [... mib-2.upsMIB / ... 1.33]

Displayed Values

- *UPS* - vendor, model, software version, firmware version
- *Battery* - output source, battery status, battery voltage, battery current
- *Input* - Hz, volts, amps, kWatts
- *Output* - Hz, volts, amps, kWatts, output load percent

Alarms

- Alarm: If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).
- 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: `3.6`

[Back to Top](#)

Network Devices > UPS > TrippLite UPS

TrippLite UPS
Use this probe with TrippLite UPS devices.

This probe works best with devices which have implemented the following MIB:

- UPS MIB (RFC 1628) [... mib-2.upsMIB / ... 1.33]
- TrippUPS MIB [... enterprises.tripplite.trippUPS.trippUpsEnvironment / 1.850.0.3]

Displayed Values

- *UPS* - vendor, model, software version, firmware version
- *Battery* - output source, battery status, battery voltage, battery current
- *Input* - Hz, volts, amps, kWatts
- *Output* - Hz, volts, amps, kWatts, output load percent
- *Environment* - ambient temperature, ambient humidity

Alarms

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: `2.13`

[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 mininmum 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 mininmum specified output voltage on phase 1, 2, or 3. If the output voltage drops below this threshold, the device is set to **Alarm**.

Filename: `de.medianet.freinet.ups.victron.txt`
 Version: `3.1`

[Back to Top](#)

PowerShell

- [PowerShell > Disk Space](#)*PowerShell > Disk Space*
- [PowerShell > Remoting > Disk Space (Signed)](#)*PowerShell > Remoting > Disk Space (Signed)*
- [PowerShell > Remoting > Disk Space](#)*PowerShell > Remoting > Disk Space*
- [PowerShell > Remoting > Installed Software](#)*PowerShell > Remoting > Installed Software*
- [PowerShell > Remoting > Process Count](#)*PowerShell > Remoting > Process Count*

  [To Probe Index](#)*Probe Reference Index*

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.

Filename: `com.helpsystems.powershell.wmi.diskspace.txt`
Version: `1.0`

[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](#)*Probe Groups > Probe Group*

  [To Probe Index](#)*Probe Reference Index*

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.

Filename: `com.dartware.probegroup.txt`
 Version: `0.4`

[Back to Top](#)

Servers-Proprietary

- [Servers Proprietary > 4D Server](#)*Servers Proprietary > 4D Server*
- [Servers Proprietary > Apache >](#) *Servers Proprietary > Apache >*
- [Servers Proprietary > Apple > AppleShareIP](#)*Servers Proprietary > Apple > AppleShareIP*
- [Servers Proprietary > Apple > OS X Server > AFP](#)*Servers Proprietary > Apple > OS X Server > AFP*
- [Servers Proprietary > Apple > OS X Server > FTP](#)*Servers Proprietary > Apple > OS X Server > FTP*
- [Servers Proprietary > Apple > OS X Server > Info](#)*Servers Proprietary > Apple > OS X Server > Info*
- [Servers Proprietary > Apple > OS X Server > NAT](#)*Servers Proprietary > Apple > OS X Server > NAT*
- [Servers Proprietary > Apple > OS X Server > Print](#)*Servers Proprietary > Apple > OS X Server > Print*
- [Servers Proprietary > Apple > OS X Server > QTSS](#)*Servers Proprietary > Apple > OS X Server > QTSS*
- [Servers Proprietary > Apple > OS X Server > Web](#)*Servers Proprietary > Apple > OS X Server > Web*
- [Servers Proprietary > Apple > RTMP](#)*Servers Proprietary > Apple > RTMP*
- [Servers Proprietary > Apple > Xserve > Xserve G4](#)*Servers Proprietary > Apple > Xserve > Xserve G4*
- [Servers Proprietary > Apple > Xserve > Xserve G5](#)*Servers Proprietary > Apple > Xserve > Xserve G5*
- [Servers Proprietary > Apple > Xserve > Xserve RAID](#)*Servers Proprietary > Apple > Xserve > Xserve RAID*
- [Servers Proprietary > Apple > Xserve > Xserve Tiger (PPC)](#)*Servers Proprietary > Apple > Xserve > Xserve Tiger (PPC)*
- [Servers Proprietary > Barracuda > Barracuda HTTP](#)*Servers Proprietary > Barracuda > Barracuda HTTP*

- [Servers Proprietary > Barracuda > Barracuda HTTPS](#)*Servers Proprietary > Barracuda > Barracuda HTTPS*
- [Servers Proprietary > Big Brother Probe](#)*Servers Proprietary > Big Brother Probe*
- [Servers Proprietary > BlitzWatch](#)*Servers Proprietary > BlitzWatch*
- [Servers Proprietary > Citrix Server](#)*Servers Proprietary > Citrix Server*
- [Servers Proprietary > Dartware > DataCenter > IMAuth](#)*Servers Proprietary > Dartware > DataCenter > IMAuth*
- [Servers Proprietary > Dartware > DataCenter > IMDatabase](#)*Servers Proprietary > Dartware > DataCenter > IMDatabase*
- [Servers Proprietary > DND Protocol](#)*Servers Proprietary > DND Protocol*
- [Servers Proprietary > FileMaker Pro](#)*Servers Proprietary > FileMaker Pro*
- [Servers Proprietary > FirstClass Server](#)*Servers Proprietary > FirstClass Server*
- [Servers Proprietary > KeyServer](#)*Servers Proprietary > KeyServer*
- [Servers Proprietary > Lotus Notes](#)*Servers Proprietary > Lotus Notes*
- [Servers Proprietary > MeetingMaker](#)*Servers Proprietary > MeetingMaker*
- [Servers Proprietary > Microsoft > DHCP Lease Check](#)*Servers Proprietary > Microsoft > DHCP Lease Check*
- [Servers Proprietary > Microsoft > NT Services](#)*Servers Proprietary > Microsoft > NT Services*
- [Servers Proprietary > Microsoft > SQL Server Query](#)*Servers Proprietary > Microsoft > SQL Server Query*
- [Servers Proprietary > Nagios NRPE](#)*Servers Proprietary > Nagios NRPE*

  [To Probe Index](#)*Probe Reference Index*

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.

Parameters

database name - the name of an existing database on the 4D server.

timeout - the number of seconds to wait for a response before returning a WARN status.

Filename: `com.dartware.tcp.4D`
Version: `1.6`

[Back to Top](#)

Servers Proprietary > Apache >

This probes 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.

Parameters

None.

Filename: `com.dartware.tcp.appleshareip`
 Version: `1.6`

[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.

Filename: `com.dartware.tcp.osxserver.info.txt`
 Version: `1.0`

[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.

Filename: `com.dartware.tcp.osxserver.nat.txt`
Version: `1.0`

[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.

Note: 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.

Parameters

User - the name of any user on the specified server.

Password - the password for the user specified in *User*.

OS Version - 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 - general information about the server, such as amount of RAM and OS name and version.

Drives - 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 - the ambient temperature of the server.

Blowers - information on the speed of the server's cooling fans.

Security - monitors the state of the security lock and the enclosure.

> **NOTE:** 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 administrators 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**.

Filename: `com.dartware.tcp.barracuda.https.txt`
Version: `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.

Parameters

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: `1.7`

[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.

Parameters

None.

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 service
developed at Dartmouth College. The default TCP port number for DND
connections is port 902.

Parameters

Name - the name to look up in the DND.

Filename: `com.dartware.tcp.dnd`
Version: `1.7`

[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**.

Parameters

None.

Filename: `com.dartware.tcp.filemaker`
 Version: `1.7`

[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.

Parameters

banner - the banner text you expect to receive from the FirstClass server.

Filename: `com.dartware.tcp.firstclass`
 Version: `1.7`

[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.

Parameters

None.

Filename: `com.dartware.keyserver`
 Version: `1.7`

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.

Parameters

None.

Filename: `com.dartware.tcp.lotusnotes`
Version: `1.5`

Servers Proprietary > MeetingMaker

MeetingMaker

The MeetingMaker server listens on port 649. This probe attempts to connect and exits with OKAY status if it succeeds.

Parameters

None.

Filename: `com.dartware.tcp.meetingmaker`
Version: `1.5`

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.

Parameters

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 adminsitrator 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: `1.9`

[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 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](#) (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.](#)

Filename: `com.dartware.tcp.nrpe.txt`
 Version: `1.2`

[Back to Top](#)

Servers-Standard

- [Servers Standard > Basic TCP (Blocked)](#)*Servers Standard > Basic TCP (Blocked)*
- [Servers Standard > Basic TCP](#)*Servers Standard > Basic TCP*
- [Servers Standard > Custom TCP](#)*Servers Standard > Custom TCP*

- Servers Standard > CVS Server*Servers Standard > CVS Server*
- Servers Standard > DHCPv4/BOOTP*Servers Standard > DHCPv4/BOOTP*
- Servers Standard > Domain Name (DNS) > DNS: (A) Address*Servers Standard > Domain Name (DNS) > DNS: (A) Address*
- Servers Standard > Domain Name (DNS) > DNS: (MX) Mail Server*Servers Standard > Domain Name (DNS) > DNS: (MX) Mail Server*
- Servers Standard > Domain Name (DNS) > DNS: (NS) Name Server*Servers Standard > Domain Name (DNS) > DNS: (NS) Name Server*
- Servers Standard > Domain Name (DNS) > DNS: (PTR) Reverse Lookup*Servers Standard > Domain Name (DNS) > DNS: (PTR) Reverse Lookup*
- Servers Standard > Domain Name (DNS) > DNS: (TXT) Text Record*Servers Standard > Domain Name (DNS) > DNS: (TXT) Text Record*
- Servers Standard > FTP > FTP (Login)*Servers Standard > FTP > FTP (Login)*
- Servers Standard > FTP > FTP (No Login)*Servers Standard > FTP > FTP (No Login)*
- Servers Standard > Gopher*Servers Standard > Gopher*
- Servers Standard > Host Resources*Servers Standard > Host Resources*
- Servers Standard > HTTP & HTTPS > HTTP (Don't Match)*Servers Standard > HTTP & HTTPS > HTTP (Don't Match)*
- Servers Standard > HTTP & HTTPS > HTTP (Follow Redirects)*Servers Standard > HTTP & HTTPS > HTTP (Follow Redirects)*
- Servers Standard > HTTP & HTTPS > HTTP (Post)*Servers Standard > HTTP & HTTPS > HTTP (Post)*
- Servers Standard > HTTP & HTTPS > HTTP (Proxy)*Servers Standard > HTTP & HTTPS > HTTP (Proxy)*
- Servers Standard > HTTP & HTTPS > HTTP (Redirect)*Servers Standard > HTTP & HTTPS > HTTP (Redirect)*
- Servers Standard > HTTP & HTTPS > HTTP*Servers Standard > HTTP & HTTPS > HTTP*
- Servers Standard > HTTP & HTTPS > HTTPS TLSv1.0*Servers Standard > HTTP & HTTPS > HTTPS TLSv1.0*
- Servers Standard > HTTP & HTTPS > HTTPS (Follow Redirects)*Servers Standard > HTTP & HTTPS > HTTPS (Follow Redirects)*
- Servers Standard > HTTP & HTTPS > HTTPS (Post)*Servers Standard > HTTP & HTTPS > HTTPS (Post)*
- Servers Standard > HTTP & HTTPS > HTTPS (Redirect)*Servers Standard > HTTP & HTTPS > HTTPS (Redirect)*

- Servers Standard > HTTP & HTTPS > HTTPS (SSLv3)*Servers Standard > HTTP & HTTPS > HTTPS (SSLv3)*

- Servers Standard > HTTP & HTTPS > HTTPS*Servers Standard > HTTP & HTTPS > HTTPS*

- Servers Standard > IPMI v2.0*Servers Standard > IPMI v2.0*

- Servers Standard > IRC*Servers Standard > IRC*

- Servers Standard > LDAP > LDAP SSL*Servers Standard > LDAP > LDAP SSL*

- Servers Standard > LDAP > LDAP*Servers Standard > LDAP > LDAP*

- Servers Standard > LPR*Servers Standard > LPR*

- Servers Standard > Mail > IMAP4 SSL*Servers Standard > Mail > IMAP4 SSL*

- Servers Standard > Mail > IMAP4*Servers Standard > Mail > IMAP4*

- Servers Standard > Mail > POP3 SSL*Servers Standard > Mail > POP3 SSL*

- Servers Standard > Mail > POP3*Servers Standard > Mail > POP3*

- Servers Standard > Mail > Roundtrip IMAP*Servers Standard > Mail > Roundtrip IMAP*

- Servers Standard > Mail > Roundtrip POP*Servers Standard > Mail > Roundtrip POP*

- Servers Standard > Mail > SMTP TLS*Servers Standard > Mail > SMTP TLS*

- Servers Standard > Mail > SMTP*Servers Standard > Mail > SMTP*

- Servers Standard > Multimedia > Multicast Listener*Servers Standard > Multimedia > Multicast Listener*

- Servers Standard > Multimedia > RTSP*Servers Standard > Multimedia > RTSP*

- Servers Standard > Network Time*Servers Standard > Network Time*

- Servers Standard > NNTP*Servers Standard > NNTP*

- Servers Standard > RADIUS*Servers Standard > RADIUS*

- Servers Standard > SIP over UDP*Servers Standard > SIP over UDP*

- Servers Standard > SNPP*Servers Standard > SNPP*

- Servers Standard > SSH*Servers Standard > SSH*

- Servers Standard > Subversion > SVN (Apache)*Servers Standard > Subversion > SVN (Apache)*

- Servers Standard > Subversion > SVN (Svnserve)*Servers Standard > Subversion > SVN (Svnserve)*

- Servers Standard > Telnet*Servers Standard > Telnet*

- Servers Standard > VNC Server*Servers Standard > VNC Server*

   To Probe Index*Probe Reference Index*

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**.

Parameters

Failure Status - The device status upon successful connection. The default state is **DOWN**.

Filename: `com.dartware.tcp.blocked`
 Version: `1.6`

[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**.

Parameters

None.

Filename: `com.dartware.tcp.basic`
 Version: `1.6`

[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:

Parameters

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.\p\

Parameters

CVSROOT_path - path to the CVS server

Username - Username for the CVS server

Password - Password used with Username

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.

Parameters

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.

Filename: `com.dartware.dhcp`
 Version: `2.1`

[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.

Parameters

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: `1.9`

[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.

Parameters

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: `1.2`

[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.

Parameters

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: `1.2`

[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: `com.dartware.tcp.ftp.login`
 Version: `1.9`

[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: `com.dartware.tcp.ftp.nologin`
 Version: `1.9`

[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.

Parameters

Selector string - the string sent to the Gopher server. By default, this string is empty.

Filename: `com.dartware.tcp.gopher`
Version: `1.7`

[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)

Use this probe to search for a string that should not 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.

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 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: `2.13`

[Back to Top](#)

Servers Standard > HTTP & HTTPS > HTTPS TLSv1.0

HTTPS-TLSv1.0

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.

Parameters

Host Name - the domain name of the web server (e.g. "www.intermapper.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-tlsv10.txt`
 Version: `2.10`

[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.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.

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.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 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 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: `1.5`

[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.

Parameters

Host Name - the domain name of the web server (e.g. "www.intermapper.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: `2.9`

[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.

Parameters

Password - the connection password. This parameter is passed using the "PASS" command.

Nickname - the connection nickname. This parameter is passed using the "NICK" command.

Username - 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 - 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 through a secure connection, and binds using the designated *Bind Name* and *Bind Password* (if specified.)

Parameters

Bind Name - The LDAP name to be authenticated

Bind Password - The password to be used with the *Bind Name*. It is sent as clear text to authenticate the probe.

Field to Match - 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.

Search Base - If 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: `1.10`

[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* and *Bind Password* (if specified.)

Parameters

Bind Name - The LDAP name to be authenticated

Bind Password - The password to be used with the *Bind Name*. It is sent as clear text to authenticate the probe.

Field to Match - 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.

Search Base - If 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: `1.10`

[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.

Parameters

Queue Name - specify a queue name if applicable to your printer.

Filename: `com.dartware.tcp.lpr`
 Version: `1.8`

[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.

Parameters

None.

Filename: `com.dartware.tcp.imap4.ssl`
 Version: `1.8`

[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.

Parameters

None.

Filename: `com.dartware.tcp.imap4`
 Version: `1.8`

[Back to Top](#)

Servers Standard > Mail > POP3 SSL

POP3-SSL
The protocol uses PO3 over SSL 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.

Parameters

User Name - POP3 account user name. If left empty, this probe verifies that the server sends "+OK" as its initial greeting, then immediately sends the QUIT command.

Password - POP3 account password. If *User Name* is specified, this probe attempts to login to the POP3 server using the specified password. If the probe fails to authenticate, the device will be marked in "warning".

Use APOP if supported - By default, this probe uses the APOP command to authenticate the user if 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.

> **NOTE:** The "Use APOP if supported" option has no effect if APOP is not supported by the server.

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.

Parameters

User Name - POP3 account user name. If left empty, this probe verifies that the server sends "+OK" as its initial greeting, then immediately sends the QUIT command.

Password - POP3 account password. If *User Name* is specified, this probe attempts to login to the POP3 server using the specified password. If the probe fails to authenticate, the device will be marked in "warning".

Use APOP if supported - By default, this probe uses the APOP command to authenticate the user if 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.

> **NOTE:** The "Use APOP if supported" option has no effect if APOP is not supported by the server.

Filename: `com.dartware.tcp.pop3`
Version: `2.7`

[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.

Parameters

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.

Parameters

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 is passive; it only listens, and does not inject any traffic into the network.

Parameters

Multicast IP Address - (optional) multicast IP address to listen on.

Seconds to wait - 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 - specify whether the probe should count packets only from the IP address of the targeted device.

Filename: `com.dartware.udplistener`
 Version: `2.1`

[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".

Parameters

Movie Name - the name of the media you want to use to test server status

Seconds to play - the number of seconds to play the media before returning a status

RFC2326bis-02 or later - specify whether the server implements RFC2326bis

Filename: `com.dartware.tcp.rtsp`
Version: `2.2`

[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.

Parameters

None.

Filename: `com.dartware.ntp`
Version: `1.6`

[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.

Parameters

Newsgroup - the name of the newsgroup that you want to verify.

Filename: `com.dartware.tcp.nntp`
Version: `1.7`

[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.

Parameters

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: `1.9`

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.

If the probe times out while trying to match a "string-to-match" field, returns a **Down** status

> **NOTE:** The "string-to-match" fields accept regular expressions.

Parameters

Intro String to Match - 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 - the string to match in the first prompt. (e.g. "Login:")

Reply #1 - your reply to the first prompt. (i.e. your response to the "Login:" prompt)

Second Prompt - 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 - your reply to the second prompt. (i.e. your response to the "Password:" prompt.)

Third Prompt - the string to match in the third prompt. If this parameter is empty, the probe ignores the prompt string and its reply.

Reply #3 - your reply to the third prompt.

Final String to Match - The final string to match. This could be a response to a command you entered in the previous step.

Filename: `com.dartware.tcp.telnet`
 Version: `1.9`

[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/.

Parameters

None.

Filename: `com.dartware.tcp.vnc`
 Version: `1.8`

[Back to Top](#)

WMI

- [WMI > WMI CPU Utilization](#)*WMI > WMI CPU Utilization*
- [WMI > WMI Disk Available](#)*WMI > WMI Disk Available*
- [WMI > WMI Disk Fragmentation Analysis](#)*WMI > WMI Disk Fragmentation Analysis*
- [WMI > WMI Event Log](#)*WMI > WMI Event Log*

- [WMI > WMI File Check](#)*WMI > WMI File Check*

- [WMI > WMI Folder Check](#)*WMI > WMI Folder Check*

- [WMI > WMI Free Memory](#)*WMI > WMI Free Memory*

- [WMI > WMI Installed Software](#)*WMI > WMI Installed Software*

- [WMI > WMI Logged on Users](#)*WMI > WMI Logged on Users*

- [WMI > WMI MSExchange 2007 Hub Transport Server](#)*WMI > WMI MSExchange 2007 Hub Transport Server*

- [WMI > WMI MSExchange 2007 Mailbox Server](#)*WMI > WMI MSExchange 2007 Mailbox Server*

- [WMI > WMI Network Utilization](#)*WMI > WMI Network Utilization*

- [WMI > WMI Process Monitor](#)*WMI > WMI Process Monitor*

- [WMI > WMI Service Monitor](#)*WMI > WMI Service Monitor*

- [WMI > WMI SQL Server 2008 Service Monitor](#)*WMI > WMI SQL Server 2008 Service Monitor*

- [WMI > WMI System Accessibility](#)*WMI > WMI System Accessibility*

- [WMI > WMI System Information](#)*WMI > WMI System Information*

- [WMI > WMI Top Processes](#)*WMI > WMI Top Processes*

  [To Probe Index](#)*Probe Reference Index*

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: `1.13`

[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: `1.12`

[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 anaylsis. 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: `1.12`

[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: `1.14`

[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: `1.12`

[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: `1.14`

[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: `1.11`

[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_sofware.vbs` companion script included with this probe.

Filename: `com.dartware.wmi.installed_software.txt`
 Version: `1.8`

[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: `1.14`

WMI > WMI MSExchange 2007 Hub Transport Server

WMI MSExchange 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: `1.7`

WMI > WMI MSExchange 2007 Mailbox Server

WMI MSExchange 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_MSExchangeIS_MSExchangeIS, Win32_ PerfFormattedData_MSExchangeIS_MSExchangeISMailbox, Win32_ PerfFormattedData_MSExchangeIS_MSExchangeISPublic, Win32_ PerfFormattedData_MSExchangeSearchIndices_MSExchangeSearchIndices 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: `1.7`

[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 parameters 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 specifiying 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: `1.13`

[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: `1.14`

[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: `1.15`

[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.

Filename: `com.dartware.wmi.sql2k8_service_monitor.txt`
 Version: `1.7`

[Back to Top](#)

WMI > WMI System Accessibility

WMI System Accessibility
This probe uses WMI to test accessibilty 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: `1.12`

[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: `1.11`

[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: `1.13`

[Back to Top](#)

Wireless

- [Wireless > Alvarion > Alvarion B 14 & B 28 (BU)](#)*Wireless > Alvarion > Alvarion B 14 & B 28 (BU)*
- [Wireless > Alvarion > Alvarion B 14 & B 28 (RB)](#)*Wireless > Alvarion > Alvarion B 14 & B 28 (RB)*
- [Wireless > Alvarion > BreezeACCESS (AU)](#)*Wireless > Alvarion > BreezeACCESS (AU)*
- [Wireless > Alvarion > BreezeACCESS (SU)](#)*Wireless > Alvarion > BreezeACCESS (SU)*
- [Wireless > Alvarion > BreezeACCESS LB](#)*Wireless > Alvarion > BreezeACCESS LB*
- [Wireless > Alvarion > BreezeACCESS VL (AU)](#)*Wireless > Alvarion > BreezeACCESS VL (AU)*
- [Wireless > Alvarion > BreezeACCESS VL (SU)](#)*Wireless > Alvarion > BreezeACCESS VL (SU)*
- [Wireless > Atmel > Atmel AT76C510](#)*Wireless > Atmel > Atmel AT76C510*
- [Wireless > Basic > IEEE 802.11](#)*Wireless > Basic > IEEE 802.11*
- [Wireless > Basic > SNMP for Wireless](#)*Wireless > Basic > SNMP for Wireless*
- [Wireless > Canopy > Canopy (AP)](#)*Wireless > Canopy > Canopy (AP)*
- [Wireless > Canopy > Canopy (SM)](#)*Wireless > Canopy > Canopy (SM)*
- [Wireless > Canopy > Canopy Backhaul (45 Mbps/FW 5830)](#)*Wireless > Canopy > Canopy Backhaul (45 Mbps/FW 5830)*
- [Wireless > Canopy > Canopy Backhaul (60 Mbp/FW 5840)](#)*Wireless > Canopy > Canopy Backhaul (60 Mbp/FW 5840)*
- [Wireless > Canopy > Canopy Backhaul (Master)](#)*Wireless > Canopy > Canopy Backhaul (Master)*
- [Wireless > Canopy > Canopy Backhaul (Slave)](#)*Wireless > Canopy > Canopy Backhaul (Slave)*

- Wireless > Canopy > Canopy CMM Micro*Wireless > Canopy > Canopy CMM Micro*

- Wireless > CB3 > CB3 Bridge*Wireless > CB3 > CB3 Bridge*

- Wireless > CB3 > CB3 Deluxe Bridge*Wireless > CB3 > CB3 Deluxe Bridge*

- Wireless > Inscape Data > AirEther AB54 Series AP (AP Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (AP Mode)*

- Wireless > Inscape Data > AirEther AB54 Series AP (Bridge Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (Bridge Mode)*

- Wireless > Inscape Data > AirEther AB54 Series AP (Client Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (Client Mode)*

- Wireless > Inscape Data > AirEther AB54 Series AP (Repeater Mode)*Wireless > Inscape Data > AirEther AB54 Series AP (Repeater Mode)*

- Wireless > Inscape Data > AirEther CB54 Series Client*Wireless > Inscape Data > AirEther CB54 Series Client*

- Wireless > MikroTik > MT Radio Uplink*Wireless > MikroTik > MT Radio Uplink*

- Wireless > MikroTik > MT Routerboard*Wireless > MikroTik > MT Routerboard*

- Wireless > MikroTik > MT Software Only*Wireless > MikroTik > MT Software Only*

- Wireless > MikroTik > WDS Bridge*Wireless > MikroTik > WDS Bridge*

- Wireless > Motorola > PTP 400 Series Bridge*Wireless > Motorola > PTP 400 Series Bridge*

- Wireless > Motorola > PTP 600 Series Bridge*Wireless > Motorola > PTP 600 Series Bridge*

- Wireless > Orthogon > Gemini*Wireless > Orthogon > Gemini*

- Wireless > Orthogon > Spectra*Wireless > Orthogon > Spectra*

- Wireless > Other > HTTP*Wireless > Other > HTTP*

- Wireless > Proxim > Proxim AP 2000*Wireless > Proxim > Proxim AP 2000*

- Wireless > Proxim > Proxim AP 4000*Wireless > Proxim > Proxim AP 4000*

- Wireless > Proxim > Proxim AP 600*Wireless > Proxim > Proxim AP 600*

- Wireless > Proxim > Proxim AP 700*Wireless > Proxim > Proxim AP 700*

- Wireless > Proxim > Proxim LAN Access Point*Wireless > Proxim > Proxim LAN Access Point*

- Wireless > Proxim > Tsunami GX*Wireless > Proxim > Tsunami GX*

- Wireless > Proxim > Tsunami MP.11 BSU*Wireless > Proxim > Tsunami MP.11 BSU*

- Wireless > Proxim > Tsunami MP.11 SU*Wireless > Proxim > Tsunami MP.11 SU*

- Wireless > Redline > AN50*Wireless > Redline > AN50*

- Wireless > smartBridges > airBridge*Wireless > smartBridges > airBridge*

- Wireless > smartBridges > airClient Nexus PRO total*Wireless > smartBridges > airClient Nexus PRO total*

- Wireless > smartBridges > airClient Nexus*Wireless > smartBridges > airClient Nexus*

- Wireless > smartBridges > airHaul Nexus PRO total*Wireless > smartBridges > airHaul Nexus PRO total*

- Wireless > smartBridges > airHaul Nexus*Wireless > smartBridges > airHaul Nexus*

- Wireless > smartBridges > airHaul2 Nexus PRO*Wireless > smartBridges > airHaul2 Nexus PRO*

- Wireless > smartBridges > airPoint Nexus PRO total*Wireless > smartBridges > airPoint Nexus PRO total*

- Wireless > smartBridges > airPoint Nexus*Wireless > smartBridges > airPoint Nexus*

- Wireless > smartBridges > airPoint*Wireless > smartBridges > airPoint*

- Wireless > smartBridges > airPoint2 Nexus PRO*Wireless > smartBridges > airPoint2 Nexus PRO*

- Wireless > Trango > Trango M2400S (AP)*Wireless > Trango > Trango M2400S (AP)*

- Wireless > Trango > Trango M5800S*Wireless > Trango > Trango M5800S*

- Wireless > Trango > Trango M5830S (SU)*Wireless > Trango > Trango M5830S (SU)*

- Wireless > Trango > Trango M5830S*Wireless > Trango > Trango M5830S*

- Wireless > Trango > Trango M900S (AP)*Wireless > Trango > Trango M900S (AP)*

- Wireless > Trango > Trango P5830S (master)*Wireless > Trango > Trango P5830S (master)*

- Wireless > Trango > Trango P5830S (remote)*Wireless > Trango > Trango P5830S (remote)*

- Wireless > Tranzeo > Sixth Generation AP*Wireless > Tranzeo > Sixth Generation AP*

- Wireless > Tranzeo > Sixth Generation CPE*Wireless > Tranzeo > Sixth Generation CPE*

- Wireless > Tranzeo > Sixth Generation PxP*Wireless > Tranzeo > Sixth Generation PxP*

- Wireless > Tranzeo > Tranzeo (AP)*Wireless > Tranzeo > Tranzeo (AP)*

- Wireless > Tranzeo > Tranzeo (PXP)*Wireless > Tranzeo > Tranzeo (PXP)*

- Wireless > Tranzeo > Tranzeo (SAI)*Wireless > Tranzeo > Tranzeo (SAI)*

- Wireless > Tranzeo > Tranzeo 58XX Series Backhaul*Wireless > Tranzeo > Tranzeo 58XX Series Backhaul*

- Wireless > Tranzeo > Tranzeo AP 5A (44R)*Wireless > Tranzeo > Tranzeo AP 5A (44R)*

- Wireless > Tranzeo > Tranzeo AP 5A*Wireless > Tranzeo > Tranzeo AP 5A*

- [Wireless > Tranzeo > Tranzeo Classic](#)*Wireless > Tranzeo > Tranzeo Classic*

- [Wireless > Tranzeo > Tranzeo CPE 200 (1.77.R)](#)*Wireless > Tranzeo > Tranzeo CPE 200 (1.77.R)*

- [Wireless > Tranzeo > Tranzeo CPE 200](#)*Wireless > Tranzeo > Tranzeo CPE 200*

- [Wireless > Tranzeo > Tranzeo CPE 5A (44R)](#)*Wireless > Tranzeo > Tranzeo CPE 5A (44R)*

- [Wireless > Tranzeo > Tranzeo CPE 5A](#)*Wireless > Tranzeo > Tranzeo CPE 5A*

- [Wireless > Tranzeo > Tranzeo TR CPE](#)*Wireless > Tranzeo > Tranzeo TR CPE*

- [Wireless > WaveRider > CCU](#)*Wireless > WaveRider > CCU*

- [Wireless > WaveRider > EUM](#)*Wireless > WaveRider > EUM*

  [To Probe Index](#)*Probe Reference Index*

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.

Filename: `com.dartware.wrls.alvarion.b14.master.txt`
 Version: `0.5`

[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 brige'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.

Filename: `com.dartware.wrls.AT76C510.txt`
Version: `1.5`

[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`

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`

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**.

Filename: `com.dartware.wrls.canopy.backhaul45old.txt`
Version: `1.7`

[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

Filename: `com.dartware.wrls.mt-1radio.txt`
Version: `1.14`

[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 this 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 this 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.proximg4.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.proximtmprsu.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.

Filename: `com.dartware.wrls.trangoP5830SMU.txt`
Version: `1.5`

[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 frequencey

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**.

Filename: `com.dartware.wrls.waveridereum.txt`
 Version: `1.2`

Experimental

- [Experimental > Flow Exporter Status](#)*Experimental > Flow Exporter Status*
- [Experimental > InterMapper](#)*Experimental > InterMapper*
- [Experimental > sFlow v1.2](#)*Experimental > sFlow v1.2*
- [Experimental > sFlow Vers. 1.3](#)*Experimental > sFlow Vers. 1.3*

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.

Filename: `com.dartware.flow.exporter.txt`
 Version: `1.3`

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 alway 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.

Filename: `com.dartware.tcp.intermapper.txt`
 Version: `0.11`

[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.

Filename: `com.dartware.sflowv1.2.txt`
 Version: `1.2`

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.

Filename: `com.dartware.sflow.v1.3.txt`
 Version: `1.3`

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
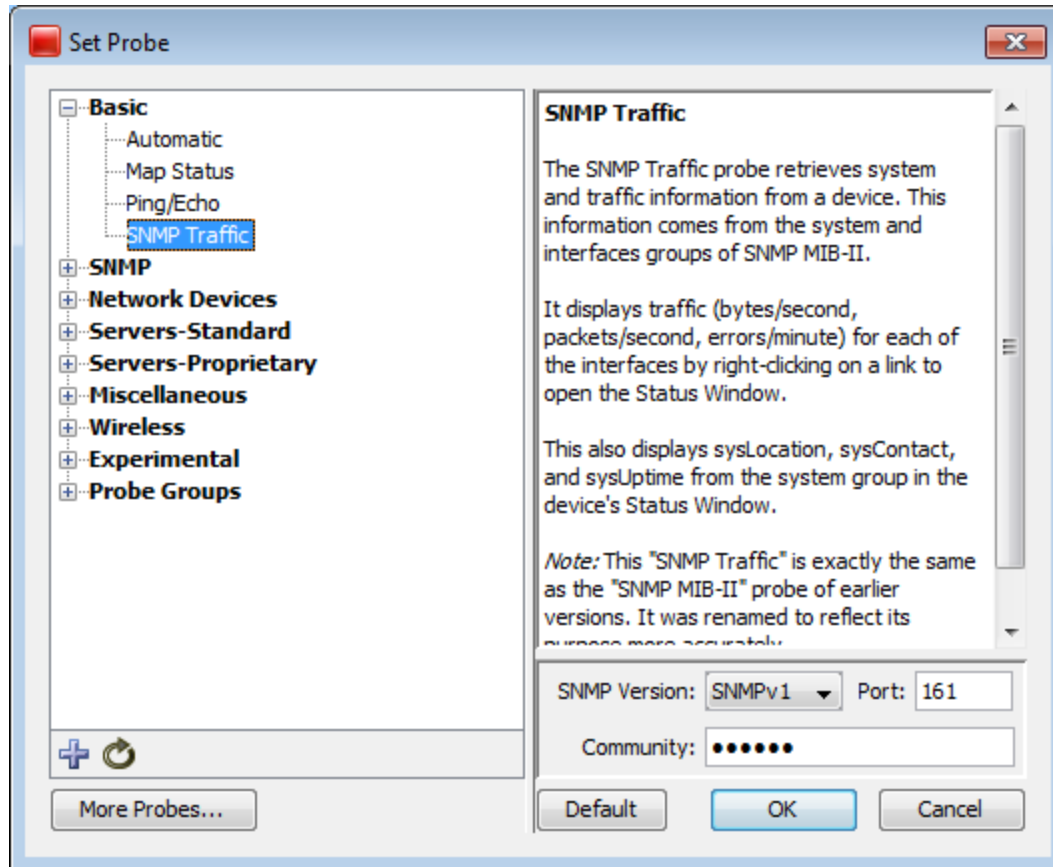
Using SNMP Version 1, 2c, and 3 in Probes
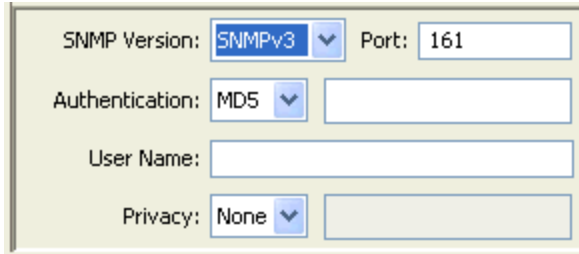
All SNMP-based probes can use one of version 1, 2c, or 3, at the user's choice. The Probe Configuration window allows you to specify the SNMP version at the same time you set all the other parameters for the probe.

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.
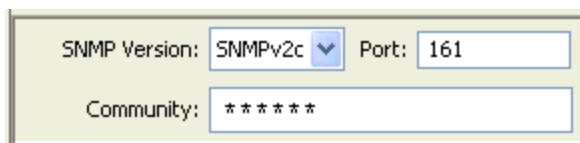
- Selecting SNMPv3 changes the lower half of the probe configuration window to let you specify all the authentication and privacy parameters. The initial settings show the default settings taken from the Server Settings > SNMP pane. See the SNMP Preferences (Pg. 296) page for more details.

> **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.

NT Services Preferences Panel

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 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

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 screenshot 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 has been 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 by using some of the many scripts that are already available.

> NOTE: Big Brother was created by two developers who later joined Quest Software, continuing to work on the product. In 2012, Quest Software was purchased by Dell. (Source: Wikipedia.)

All available support information about Big Brother provided by Dell can be found at Dell's Big Brother page. Dell does not appear to provide client binaries, but you may be able to find them at one of the software distribution sites. A lot of additional information, including potential sources of binaries and source code, is at the Wikipedia link above.

Using the Big Brother Probe

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 processes and represents are "status" (and "combo") messages.

> NOTE: The Big Brother server for a given port does 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 shuts down.

Troubleshooting Network and Server Probes

- How do I change the protocol that a device is being polled with?
- What MIB variables does Intermapper poll?
- How Does Intermapper Compute Traffic Statistics?
- How Does Intermapper Compute Utilization for a Link?
- How Does Intermapper Compute Errors for a Link?
- Why can't I get a DHCP probe on OSX to work?
- 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?
- How does Intermapper compute byte and packet rates?
- How does Intermapper compute time intervals?

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.

What MIB variables does Intermapper poll?

Anytime Intermapper displays traffic for a link, (using the SNMP Traffic Probe, 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
ifHCOutOctets	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.

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. 654). If you are planning to use Intermapper Authentication Server (Pg. 660), 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.

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.

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.

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:

Estimated Future Disk Usage

Current row counts	
Maps	27
Devices	193
Interfaces	206
Datasets	500
Datapoints	2990527
5-minute data samples	303731
Hourly data samples	31043
Daily data samples	7267
Events	111518
Notifications	701
Acknowledgments	52

Counts are estimated for tables containing more than 1000 rows.
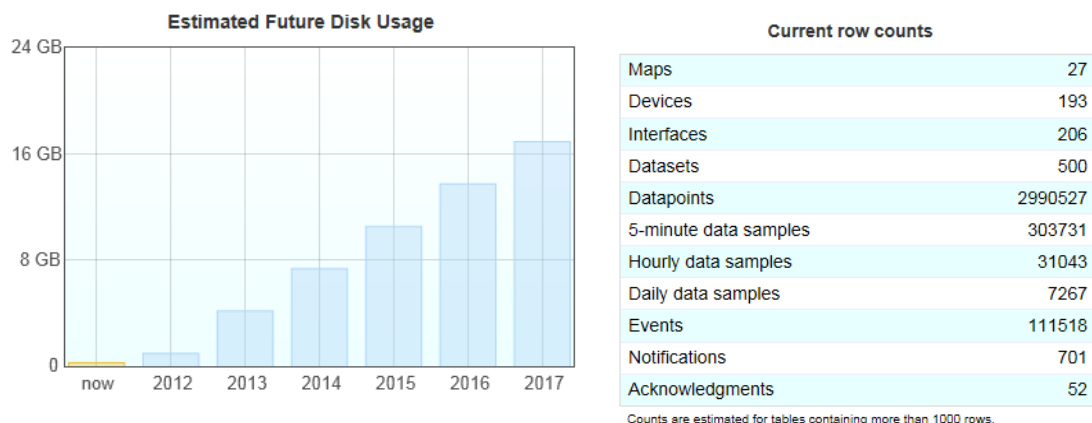
How Statistics are Calculated

- 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 date 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.

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. 652) 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. 325).

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.

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. 668)](#).
- **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](#).
- **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
Windows 32 & 64-bit	`C:\Program Files\InterMapper` or specified location.
Mac OS X	Binary files (`intermapperd`, `intermapperauthd`) are placed in `/usr/local/bin`, unless a different location was chosen at installation.
Linux	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](#).

OS	Location of Intermapper Settings files
Windows	`C:\ProgramData\InterMapper\InterMapper Settings` or specified location.
Mac OS X	As specified in `/etc/intermapperd.conf` (Usually `/Library/Application Support/InterMapper Settings/`)
Linux	As specified in `intermapperd.conf` (Usually `/var/local/InterMapper_Settings/`)

Intermapper RemoteAccess Application Folder

OS	Location of Intermapper RemoteAccess files
Windows 32-bit	`C:\Program Files\InterMapper RemoteAccess`
Windows 64-bit	`C:\Program Files (x86)\InterMapper RemoteAccess`
Mac OS X	Drag and drop to location of your choice.
Linux	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](#).

OS	Location of Intermapper DataCenter files
Windows 32 and 64-bit	`C:\Program Files\intermapper\dwf`
Mac OS X and Linux	`/usr/local/imdc`

Intermapper Flows Folder

OS	Location of Intermapper Flows files

Windows 32 & 64 bit	• (Flows files)
	`C:\Program Files\InterMapper\flows`
	• (Database)
	`C:\ProgramData\InterMapper\InterMapper Settings\Flows\SESSIONDB`

Mac OS X	• (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`

Linux	• (Flows files)
	`/var/local/InterMapper_Settings/Flows`
	• (Database)
	`/var/local/InterMapper_ Settings/Flows/SESSIONDB/`

Making Backups

Intermapper saves its state the in 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. 665).

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. 171) 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 BuiltinProbes.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 teh 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](#)

- **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](#).

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.

Overview

Use Intermapper's import and export features when you need to manage, create or update maps, devices, users. Intermapper includes a rich set of features for controlling both import and export of data.

You can automate imports and exports through Intermapper's command-line interface, and you can even create data layers for maps that use geographic coordinates suitable for viewing in Google Earth.

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. 674)) 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   Save a text file containing information about a map in one of
                                 these formats:

- **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.

A standard File Save dialog appears.

Image file   Save a PNG image of the current map. A standard File Save
                                 dialog appears.
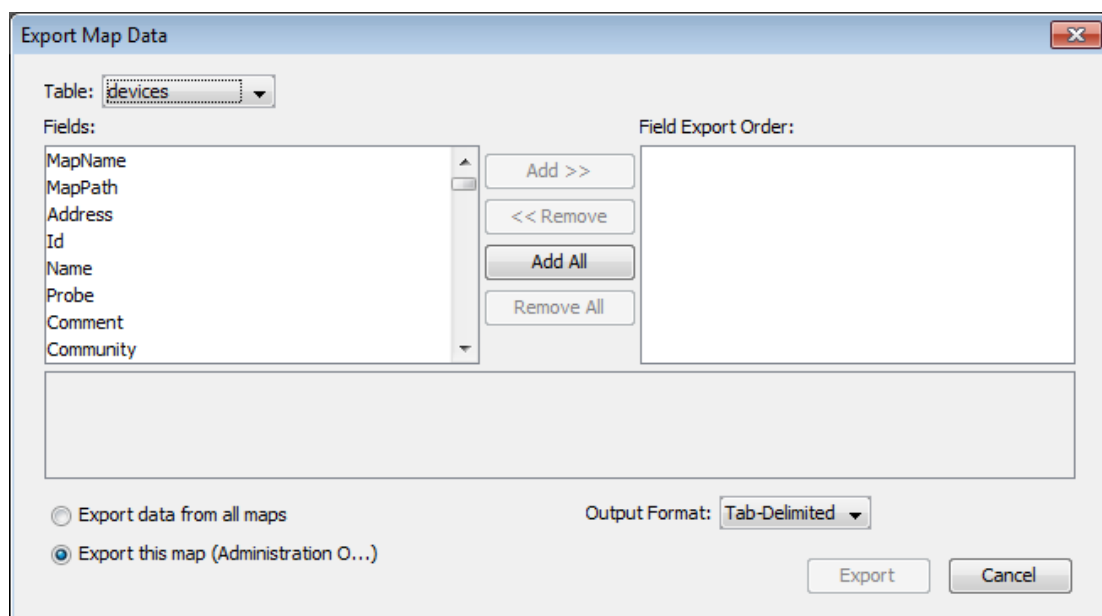
The Export Map Data window.

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. Some reasons you might want to import data:

- you want to import the devices/probe types from another monitoring system (or information that's already present in a spreadsheet or other format) into Intermapper.

- You make frequent updates to existing devices on maps.

- You frequently add new devices to maps. For example, you might 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.

- You want to make systematic changes to your maps. You can export the Intermapper map as tab-delimited data, edit columns in a spreadsheet or 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.

- You 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. 676).

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

> **NOTE:** Command-line options for RemoteAccess

> **NOTE:** , (in this manual) as well as InterMapper HTTP API in the

> **NOTE:** Developer Guide

> **NOTE:** .

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:

- , then edit the file.
- 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. 686)](#) 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 in [Advanced Data Importing (Pg. 686)](#) 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 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. 686)*](#) *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. 686)*](#) *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. 174)](#).

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. 674). 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:
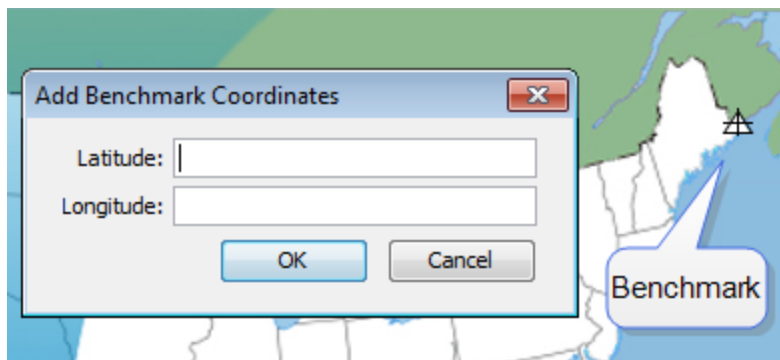
1. Right-click (CTRL-click) a known location (on for which you know the actual latitude and longitude) in the map's background image and choose **Add benchmark...** The Add Benchmark Coordinates window appears.

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. 674).

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
fields=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
Google Image Search	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.
Maporama	http://www.maporama.com Attractive street maps with different styles and coloring that are good for backgrounds. Large maps available. Free.
Mapblast	http://www.mapblast.com Another site showing street maps suitable for backgrounds. Large maps available. Free.
National Atlas	http://www.nationalatlas.gov A source of national and state maps. Free.
terraserver.com	http://www.terraserver.com Aerial photographs. Clever interactive latitude and longitude indicator using mouse rollover. 1 m/px resolution.
Microsoft Research Maps	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.

US Census Bureau	http://www.census.gov/geo/www/maps Construct a map from Census data as well as street, political, river/water data. Free.
Yahoo! Listing of Map Resources	http://dir.yahoo.com/Science/Geography/Cartography/Maps/Interactive/ Yahoo! Search for interactive maps. Lists many interesting mapping sites. Free.
dmoz Open Directory	http://dmoz.org/Science/Social_Sciences/Geography/Geographic_Information_Systems/ Links to many Geographic Information Systems sites. Free.
Geocode.com	http://www.geocode.com/ An inexpensive geocoding service that converts street addresses to latitude and longitude.
Radio Mobile	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. 679).
- **Implicitly** - When benchmarks are 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. 678). 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
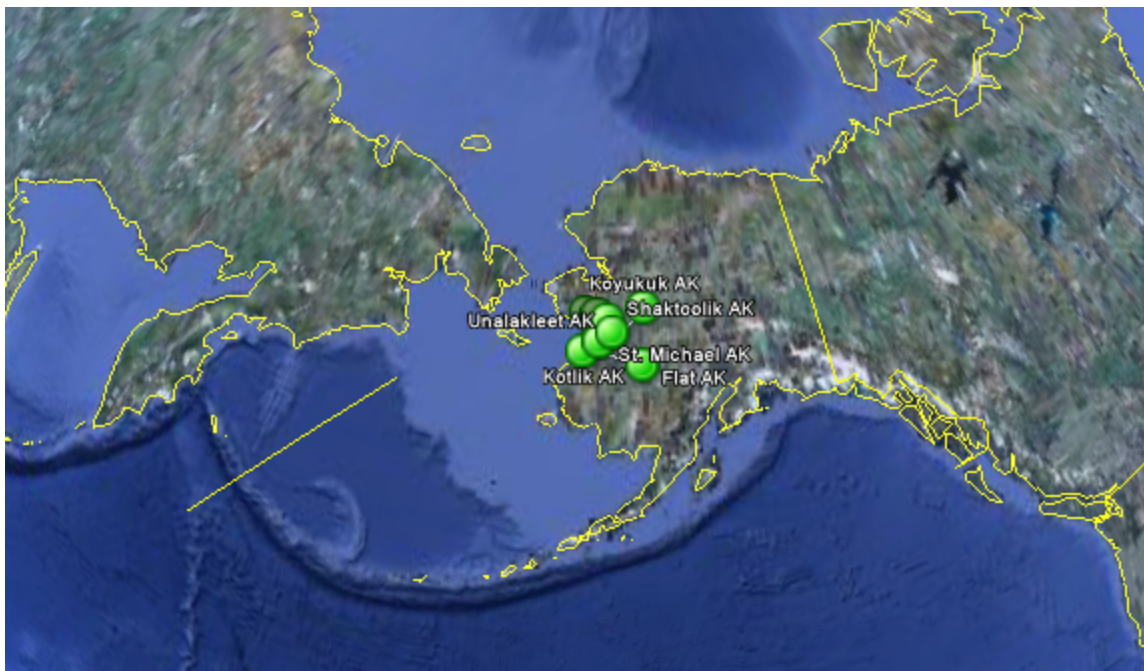
Wide view in Google Earth
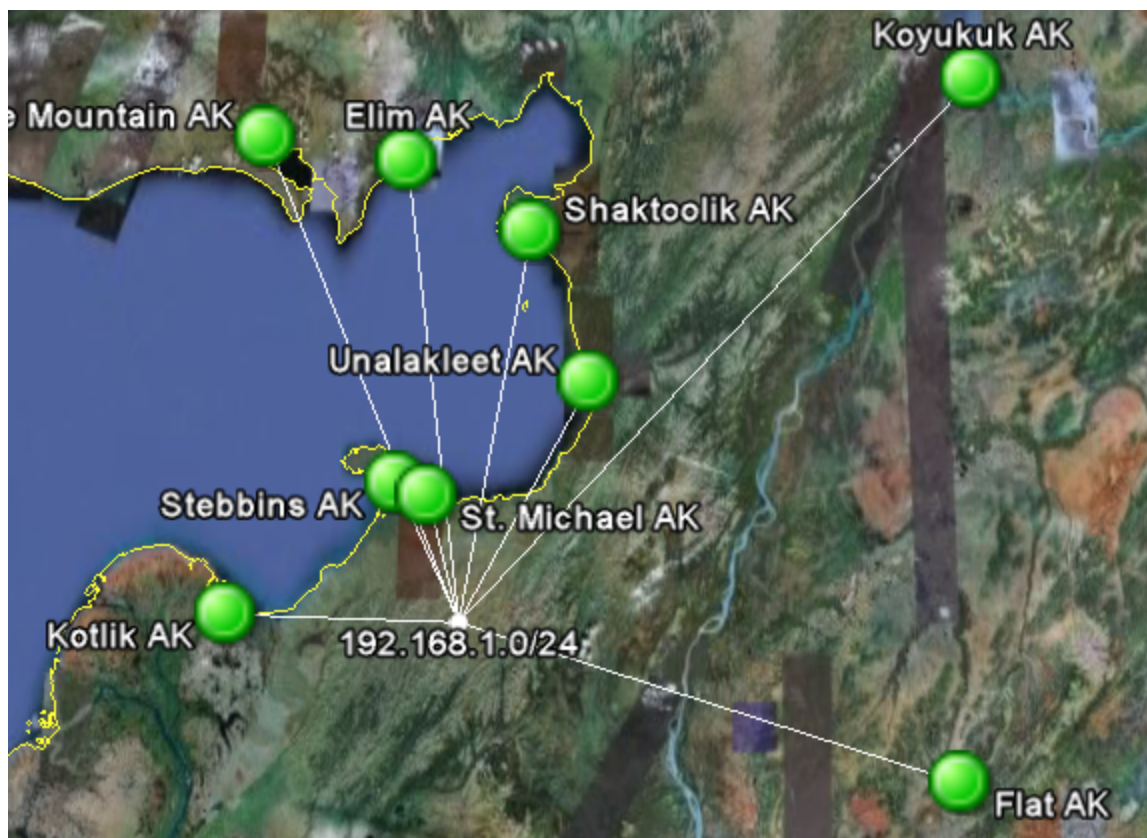
Closer view in Google Earth
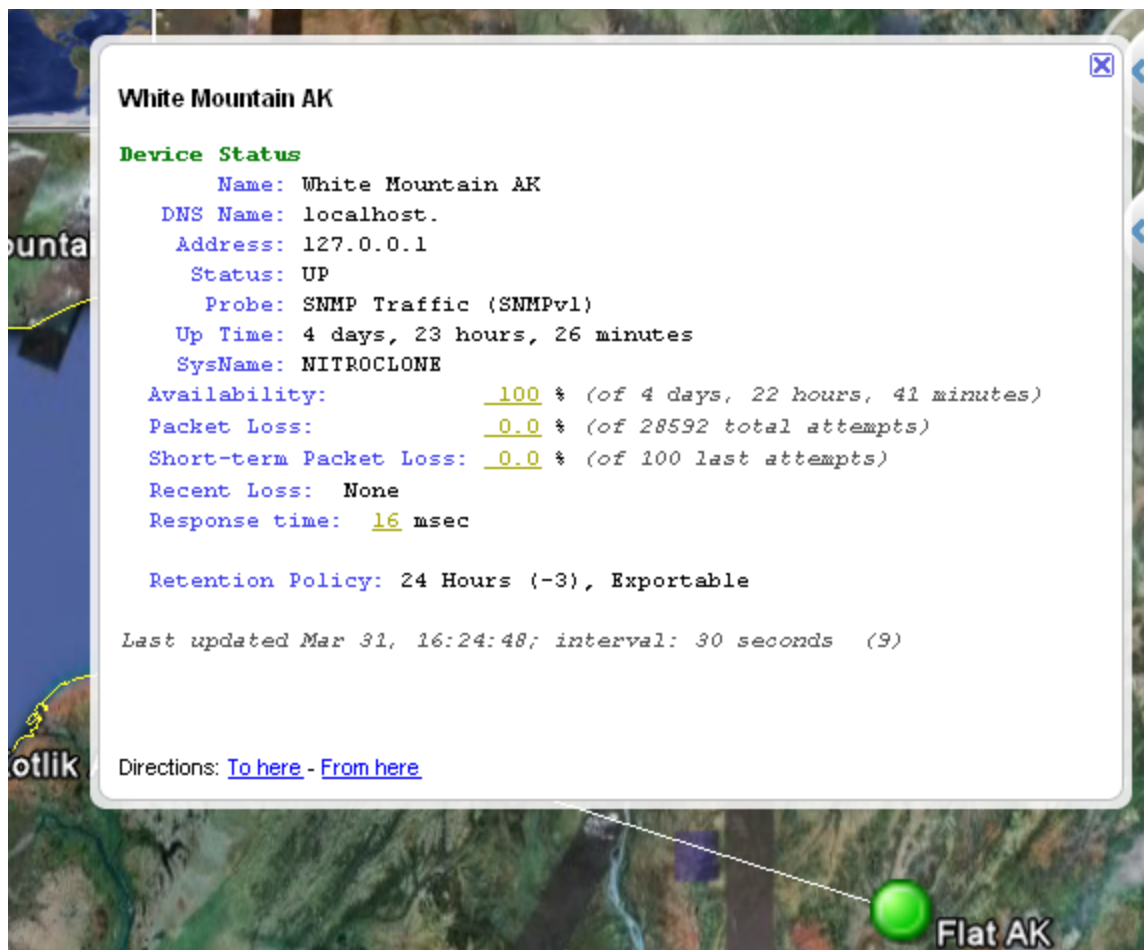
Status window in Google Earth

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:** **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. 691), 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. 672).
    - 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 Parameter	Format/Options
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. 691)](#), 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 device.
	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. 692)](#). 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,Address,Name,Latitude,Longit
ude
``` |

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 , 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
fields=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. 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. It lets you specify the SNMP community string, the probe by file name, and any parameters needed.

```
# format=tab table=devices
fields=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) 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. 703)). 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. 721)*.

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. 692)](#) 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. 703)](#) table.
- **interfaces** - imports data specific to the switch and router interfaces. See the [Interface Attributes (Pg. 706)](#) table.
- **maps** - imports data specific to maps. See the [Map Attributes (Pg. 711)](#) table.
- **notifiers** - imports data to describe notifiers. See the [Notifier Attributes (Pg. 713)](#) table.
- **notifierrules** - imports data to describe how a notifier is applied. See the [Notifier Rules Attributes table. (Pg. 714)](#)
- **users** - imports user account information. See the [User Attributes (Pg. 716)](#) table.
- **retentionpolicies**- imports user account information. See the [Retention Policy Attributes (Pg. 717)](#) 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 Intermapper 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 AckMessage 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 AckMessage 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. ifIndex) 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, persistant 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 database 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 database 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%20secret`, `sharedsecret` 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=secret&user_name=im&password=pw

improbe://netopia.example.com/radius?sharedsecret=secret&user
name=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 (now deprecated) and in compliance with current RFC 3986. 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:

```
;  /   ?  :   @   =   &
```

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 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.

Last refreshed on Tue, 8/5/2014 at 9:57 AM
-0400   Interval: Never

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. 734) 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* dropdown 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% (of10 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. 726) topic shows typical Device and Network Status.

The Intermapper Errors page

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 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.

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

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. 738)(Abbreviations:
  "E", "ERR")

FULL
-     Shows a report of all devices and links being monitored.
[details] (Pg. 738) (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. 738) (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. 738)(Abbreviations: "B")

DOWN-   Lists all devices that are down. The same functionality is also provided
      by the ERRORS command. [details] (Pg. 740)

LDOWN-   Lists all interfaces (ie links) that are down. The same functionality is
    also provided by the ERRORS command.   [details] (Pg. 742)

LOG [   ]
-    Displays the last entries from the event log window and continuously
    displays new log lines. [details] (Pg. 743)

KALI [<conn> ["compress" | "kill"]]
- Displays list of Kali connections and allows you to debug them. [details] (Pg. 741)

KALID
- Displays a list of the maps, log, lists, and other shared resources open by each
   Remote connection.
   [details] (Pg. 742)

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. 740)

QUIT-   End the telnet session and disconnect. [details] (Pg. 743)

RELOAD
- Closes all map files and reopens them. This command is only implemented in the
   server/daemon version of Intermapper. [details] (Pg. 743)

 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. 743)

TELNET
- Displays a list of current connections to the Telnet
server. [details] (Pg. 744)

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. 744)

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
    LOGIN@
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.
```

Configuring Intermapper Server Using a Command-Line

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 InterMappe renvironment.
--setenv <var>=<val>	Set the value of <var> to <val> in the Intermapper environment.
--wrap <filename>	Wrap the probe bundle defined by the bundle header at <filename>.
--output <filename>	Put output of wrap operation in file at <filename>.
--suppress-avail	Suppress the 'availability' statistic in device status windows.
--verify-permissions	Check the permissions of all files in the 'Intermapper Settings' directory.
--check-upgrade <date>	Check the release manufacture <date>against the maintenance contract date.
--detail <log>	Turn on detailed logging for the type indicated by <log>.
--ciphers <all|default|list>	Show supported SSL ciphers.
--chart-purge <days>	Purge chart data to maximum <days> history. **NOTE:** If you have a large amount of chart data, using this option to purge chart data may take a significant amount of time. If you start Intermapper with this option, monitoring may be affected adversely until the purge is completed.

Configuring Intermapper Server Using a Command-Line

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 InterMappe renvironment.

--setenv <var>=<val>	Set the value of <var> to <val> in the Intermapper environment.
--wrap <filename>	Wrap the probe bundle defined by the bundle header at <filename>.
--output <filename>	Put output of wrap operation in file at <filename>.
--suppress-avail	Suppress the 'availability' statistic in device status windows.
--verify-permissions	Check the permissions of all files in the 'Intermapper Settings' directory.
--check-upgrade <date>	Check the release manufacture <date>against the maintenance contract date.
--detail <log>	Turn on detailed logging for the type indicated by <log>.
--ciphers <all|default|list>	Show supported SSL ciphers.
--chart-purge <days>	Purge chart data to maximum <days> history.

> **NOTE:** If you have a large amount of chart data, using this option to purge chart data may take a significant amount of time. If you start Intermapper with this option, monitoring may be affected adversely until the purge is completed.

Command-Line Options for Intermapper Clients

Two client applications are available for Intermapper:

- **Intermapper client** runs on the same machine as Intermapper Server, so it has a limited set of command-line arguments.
- **Intermapper Remote Access client** runs on any machine, and connects to multiple Intermapper servers, so it has a larger set of options.

Usage:

```
java -jar [jar file] [Options]
```

- For Intermapper client, the jar file name is `intermapper.jar`.
- For Intermapper Remote Access, the jar file name is `intermapper_ remoteaccess.jar`.

- Depending on your installation, you may need to change your working directory, supply the full path to the jar file, or both. See *Windows Users* (Pg. 751), below.

You can call Intermapper Remote Access 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.

> **NOTE:** The examples below assume the Intermapper server is running on the host you are connecting to.

Intermapper clients support the following command-line arguments:

> **NOTE:**
> - **IMRA:** applies to Intermapper Remote Access client only
> - **Both:** applies to both Intermapper and Intermapper Remote Access clients

Argument	Client	Description
-host --host <HOST>	IMRA	connect to the specified HOST
-port --port <PORT>	Both	connect to the specified PORT on HOST (defaults to 8181)
-map --map <MAP_NAME>	Both	load the specified map(s) from HOST. For multiple maps, use one "--map" option per map
-import --import <FILE_NAME>	Both	import the specified file (use - for stdin)
-importmap --importmap <FILE_NAME>	Both	import the specified map.
-export --export <EXPORT-SPEC>		export the specified data to stdout. **Note:** Data for all maps is exported.

-exportmap --exportmap <MAP_ID>	Both	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.
-f --file <FILE_NAME>	Both	open the specified shortcut file
-d --debug <DEBUG_CONFIG_FILE>	Both	use the specified configuration file to configure debugging output
-D<name>=<value>	Both	set a system property
-user --user <USER>	IMRA	log in as USER
-pass --pass <PASSWORD>	IMRA	log in as USER with PASSWORD
-ignore-cert-check	IMRA	accept all server SSL certificates without prompting
-agree-to-license	Both	accept the End User License Agreement
-version --version	Both	print product version
-env --env	Both	print out system properties
-test --test [TIMEOUT]	Both	test the connection - automatically quit after TIMEOUT seconds
-h -? --help	Both	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 may require that the working directory must be set to the Intermapper installation folder, or Java jar file must include the full Windows path.

The following example sets the working directory to the Intermapper Server installation folder, invokes java with the .jar file, and opens the MyNetwork1 and MyNetwork2 maps.

```
cd "C:\Program Files\InterMapper"
java -jar "intermapper.jar" --map MyNetwork1 --map MyNetwork2
```

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.helpsystems.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 Condition>" device_imid="<Device-IMID>"
```

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 unneccessarily, with no benefit to the Intermapper App for Splunk.

The probe is located in the Splunk install directory (`%SPUNK_HOME%`) at:

`%SPLUNK_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.

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 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 "ns2flows.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.

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. 766)
- How do computers send data through the Internet? (Pg. 767)
- What is a subnet? Why do I care? (Pg. 767)
- What does the "/24" mean? How does that relate to my subnet mask? (Pg. 768)
- What is a "private IP address range"? (Pg. 768)

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 *(Class A)*	**/24**	255.255.255.0	254 *(Class C)*
/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 *(Class B)*	**/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/r fc1918.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 "FF80").

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. 770)
- [Intermapper sometimes won't show a device's DNS name...](#) (Pg. 770)
- [What is a FQDN?](#) (Pg. 770)

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. 439).

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?

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.

Management Information Base (MIB)

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.

MIB Variables and OIDs (Object Identifiers)

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.

Enterprise Numbers and OIDs

You may notice that most OIDs start with 1.3.1.6.1.x. If the 6th number is 4, the OID is generated by a private enterprise. The 7th number is the Enterprise number, assigned to the organization by the IANA as defined here:

http://www.iana.org/assignments/enterprise-numbers

The remaining numbers are generated by and under the control of the registered enterprise.

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/subnet as an allowed client
- **In a custom probe, have you specified the OID properly?** - (See the [OID Format FAQ (Pg. 773)](#) 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?

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. 296)

Intermapper may not be able to find a device for any of these reasons. (Pg. 773)

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.

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. 776)
- How can I keep Intermapper from polling for a while? (Pg. 777)
- How can I stop the Intermapper server? (Pg. 778)
- How can I remove the Intermapper server completely? (Pg. 778)

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. 777) 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.

Troubleshooting Intermapper

How do I change the community string?

You can open the *Show Info* window on a device as described in the [Monitor menu (Pg. 418)](#) 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. 646) 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 discontiguous"?

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. 768)

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 discontiguous 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. 422) 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. 785)

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.

Index