

SolarWinds Toolset

Administrator Guide

Copyright© 1995-2007 SolarWinds, all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds. All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft® and Windows 2000® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Toolset Administrator Guide 08.17.2007 Version 9.1

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	1.866.530.8100 www.solarwinds.com
Technical Support	www.solarwinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
<i>Italics</i>	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1 value2	Exclusive command parameters where only one of the options can be specified

SolarWinds Toolset Documentation Library

The following documents are included in the SolarWinds Toolset documentation library:

Document	Purpose
Administrator Guide	Provides installation, migration, and step-by-step procedures and conceptual information.
QuickStart Guide	Provides installation, setup, and common scenarios for which Toolset provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com .

Contents

<i>About SolarWinds</i>	<i>iii</i>
<i>Contacting SolarWinds</i>	<i>iii</i>
<i>Conventions</i>	<i>iii</i>
<i>SolarWinds Toolset Documentation Library</i>	<i>iv</i>

Chapter 1

Introduction and Installing	1
<i>Editions</i>	<i>1</i>
<i>Requirements</i>	<i>3</i>
<i>Installing Toolset</i>	<i>4</i>
<i>Upgrading Toolset</i>	<i>5</i>
<i>Backing Up or Migrating Your Toolset Implementation</i>	<i>6</i>
<i>Software License Key</i>	<i>7</i>
<i>Understanding the Launchpad</i>	<i>8</i>
<i>Managing the Shared Credentials Database</i>	<i>8</i>
<i>Reviewing Local ARP, DNS, IP Configuration, and Route Information</i>	<i>10</i>
<i>Launching the Command Prompt</i>	<i>10</i>
<i>Renaming Toolset Launchpad Groups</i>	<i>11</i>
<i>Reordering Toolset Launchpad Groups</i>	<i>11</i>
<i>Creating and Populating Launchpad Groups</i>	<i>11</i>
<i>Modifying Launchpad Startup Behavior</i>	<i>12</i>
<i>Viewing Version Information and Finding Help</i>	<i>12</i>

Chapter 2

Introducing the Tools	13
<i>Cisco-Specific Network Tools</i>	<i>13</i>
<i>IP Address Management Tools</i>	<i>15</i>
<i>Network Discovery Tools</i>	<i>16</i>
<i>Network Monitoring Tools</i>	<i>18</i>
<i>Ping and Network Diagnostics Tools</i>	<i>19</i>
<i>Security Tools</i>	<i>21</i>
<i>SNMP Tools</i>	<i>22</i>

Chapter 3

Cisco-Specific Network Tools.....	25
Compare Running vs. Startup Configs	25
Launching the Shared Credentials Database.....	27
Config Downloader.....	28
Getting Started.....	28
Launching the Shared Credentials Database.....	29
Advanced Options	30
Config Downloader Menus	31
Config Uploader	31
Getting Started.....	32
Example Configuration Files.....	33
Launching the Shared Credentials Database.....	35
Config Upload Menus	36
Resetting an Enable Secret Password Using SNMP	36
Config Viewer	37
Downloading a Config from a Cisco Router or Switch	37
Automatic Archiving of Downloaded Configuration Files.....	38
Comparing Two Configurations	39
Decrypting Passwords.....	39
Launching the Shared Credentials Database.....	40
Config Viewer Menus.....	41
Troubleshooting Config Viewer	44
CPU Gauge.....	44
Monitoring a Device	44
Saving a gauge setup	45
Loading a gauge	45
CPU Gauge Skins.....	45
IP Network Browser	46
Getting Started.....	46
IP Network Browser Menus	48
Printing Discovery Results.....	51
Modifying IP Network Browser Settings	52
IP Network Browser Configuration Wizard	53
Saving the Discovery in HTML	54
Exporting the Discovery as a Text File	54
IP Network Browser Command Line Operation.....	55
Customizing the Tools Menus	56

Customizing the MIBs Menu	57
Walking a Network from One Subnet to Another	58
NetFlow Configurator	58
NetFlow Realtime	59
Capturing NetFlow Data	59
Storing NetFlow Data	60
Analyzing NetFlow Data	61
Defining Applications and Modifying Port Definitions	62
Router Password Decryption	63
Proxy Ping	63
Modifying PING Settings	64
Router CPU Load	64
Getting Started	64
Setting Polling Options, Notification, and Logging	65
Immediately Polling Monitored Routers	66
Setting All Routers to a Specific Poll Interval	66
Viewing Peak Load High-Water Marks	66
Resetting High-Water Marks	66
Printing CPU Loads	67
Saving Loaded Routers	67
Loading a Saved Router List	67
Deleting All Monitored Routers	67
Troubleshooting Router CPU Load	68
TFTP Server	68
Configuring Your TFTP Server	69

Chapter 4

IP Address Management Tools	71
Advanced Subnet Calculator	71
Looking Up Address Details	72
Classful Subnet Calculator	73
CIDR Calculator	74
Subnet Addresses	76
Exporting, Printing, and Copying Calculations	76
DHCP Scope Monitor	77
Modifying DHCP Scope Monitor Settings	77
Interpreting DHCP Scope Monitor Results	78
Rescanning DHCP Scopes	78

Exporting, Printing, and Copying DHCP Scope Results	79
Discovering a List of Used IP Addresses	79
DNS and Who Is Resolver	80
Specifying WhoIs Servers.....	80
Viewing a Cache of Resolved Names	81
Exporting, Printing, and Copying Results	81
DNS Analyzer.....	82
Getting Started.....	82
Viewing Discovered DNS Details	82
Viewing Packet Details	82
DNS Analyzer Menus	83
Adding Root DNS Servers.....	88
Modifying DNS Query Timeout.....	88
Deciding Whether to Lookup DNS Server Addresses.....	88
Understanding Colors in DNS Analyzer	89
Analysis Examples.....	90
Setting a Node as the Root and Rescanning	92
DNS Audit.....	92
Starting an Audit	92
Filtering Results	93
Exporting, Printing, and Copying Calculations	93
Interpreting DNS Audit Results.....	94
IP Address Management.....	94
Scanning a Subnet	94
Modifying the Subnet Name, Mask, and Scan Frequency	95
Filtering	96
Manually Changing the Status of an IP Address.....	97
Modifying SNMP Credentials and Enabling SNMP Discovery	97
Modifying ICMP Scan Settings	98
Automatically Publish Discovered Information in HTML.....	98
Manually Scanning a Subnet.....	99
Refreshing a Subnet IP Address List.....	99
Exporting, Printing, and Copying Subnet Scans.....	99
Sharing the IP Address Management Database	100
Ping Sweep	101
Exporting, Printing, and Copying Sweeps	101
Ping Sweep Settings.....	102
Modifying ICMP Ping Settings	103
Publishing to the Web.....	104

Chapter 5

Network Discovery Tools.....	105
DNS Audit.....	105
Starting an Audit.....	106
Filtering Results.....	106
Exporting, Printing, and Copying Calculations.....	106
Interpreting DNS Audit Results.....	107
IP Address Management.....	108
Scanning a Subnet.....	108
Modifying the Subnet Name, Mask, and Scan Frequency.....	109
Filtering.....	109
Manually Changing the Status of an IP Address.....	110
Modifying SNMP Credentials and Enabling SNMP Discovery.....	110
Modifying ICMP Scan Settings.....	111
Automatically Publish Discovered Information in HTML.....	111
Manually Scanning a Subnet.....	112
Refreshing a Subnet IP Address List.....	112
Exporting, Printing, and Copying Calculations.....	113
Sharing the IP Address Management Database.....	114
IP Network Browser.....	115
Getting Started.....	115
IP Network Browser Menus.....	117
Printing Discovery Results.....	120
Modifying IP Network Browser Settings.....	121
IP Network Browser Configuration Wizard.....	122
Saving the Discovery in HTML.....	123
Exporting the Discovery as a Text File.....	123
IP Network Browser Command Line Operation.....	124
Customizing the Tools Menus.....	125
Customizing the MIBs Menu.....	126
Walking a Network from One Subnet to Another.....	127
IP Network Browser Frequently Asked Questions.....	127
MAC Address Discovery.....	128
Searching Results Data.....	128
Exporting, Printing, and Copying Discovered Results.....	129
Modifying MAC Address Discovery Settings.....	129
Network Sonar.....	130
Completing the Discover Wizard.....	130
Modifying Network Sonar Discovery Preferences.....	131
Network Sonar Menus.....	134

<i>Network Sonar Toolbars</i>	137
<i>Exporting, Printing, and Copying Data</i>	139
<i>Limiting Discovery to a Single Class B or C Network</i>	139
<i>Ping Sweep</i>	140
<i>Exporting, Printing, and Copying Sweeps</i>	140
<i>Ping Sweep Settings</i>	141
<i>Modifying ICMP Ping Settings</i>	142
<i>Publishing to the Web</i>	143
<i>Port Scanner</i>	143
<i>Exporting, Printing, and Copying Scan Results</i>	144
<i>Publishing to the Web</i>	144
<i>Port Scanner Options and Settings</i>	144
<i>Rescanning Ports on a Particular Address</i>	145
<i>SNMP Sweep</i>	146
<i>Exporting, Printing, and Copying Sweeps</i>	146
<i>Publishing to the Web</i>	147
<i>Clearing Sweep Results</i>	147
<i>Modifying SNMP Sweep Settings</i>	147
<i>Subnet List</i>	149
<i>Modifying SNMP Options for Subnet List</i>	150
<i>Exporting, Printing, and Copying Subnet List Results</i>	150
<i>Publishing to the Web</i>	151
<i>Switch Port Mapper</i>	152
<i>Selecting What You Want Reported</i>	152
<i>Modifying SNMP Settings</i>	153
<i>Mapping Switch and Hub Ports</i>	154
<i>Exporting, Printing, and Copying Mappings</i>	155
<i>Publishing to the Web</i>	156

Chapter 6

Network Monitoring Tools	157
<i>Advanced CPU Load</i>	157
<i>Adding Your First Devices</i>	158
<i>Modifying Advanced CPU Load Settings</i>	159
<i>Monitoring Multi-Processor Devices</i>	160
<i>Viewing Running Processes on the Target Device</i>	160
<i>Viewing Client Session on the Target Device</i>	161
<i>Viewing Running Services on the Target Device</i>	161
<i>Viewing Installed Software on the Target Device</i>	161

<i>Viewing Historical Graphs</i>	<i>162</i>
<i>Modifying Displayed Columns</i>	<i>162</i>
Bandwidth Gauges	162
<i>Creating a Gauge</i>	<i>162</i>
<i>Launching the Shared Credentials Database</i>	<i>164</i>
<i>Bandwidth Gauges Menus</i>	<i>165</i>
<i>Modifying Settings and the Publishing of Gauges</i>	<i>166</i>
<i>Context Menus</i>	<i>168</i>
<i>Saving and Loading a Set of Gauges</i>	<i>169</i>
CPU Gauge	170
<i>Monitoring a Device</i>	<i>170</i>
<i>Saving a gauge setup</i>	<i>170</i>
<i>Loading a gauge</i>	<i>171</i>
<i>CPU Gauge Skins</i>	<i>171</i>
Network Monitor	171
<i>Adding Devices to Monitor</i>	<i>171</i>
<i>Importing into Network Monitor</i>	<i>172</i>
<i>Configuring Network Monitor Settings</i>	<i>175</i>
<i>Exporting and Printing Node Lists and Event Details</i>	<i>178</i>
<i>Publishing to the Web</i>	<i>178</i>
<i>Viewing and Modifying Node Details</i>	<i>179</i>
<i>Deleting and Undeleting Nodes</i>	<i>180</i>
<i>Viewing Node-Specific Events</i>	<i>180</i>
<i>Viewing the Event Monitor</i>	<i>180</i>
<i>Viewing Event Details</i>	<i>181</i>
<i>Searching Past Events</i>	<i>181</i>
<i>Exporting Events</i>	<i>182</i>
<i>Running Database Maintenance Immediately</i>	<i>182</i>
<i>Modifying the Look and Feel of Network Monitor</i>	<i>182</i>
<i>Running Response Time Charts</i>	<i>182</i>
Network Performance Monitor	185
<i>What Network Performance Monitor Offers</i>	<i>185</i>
<i>Starting Toolset Network Performance Monitor</i>	<i>186</i>
<i>Adding Nodes and Interfaces</i>	<i>186</i>
<i>Modifying System Settings</i>	<i>189</i>
<i>Modifying Advanced Settings</i>	<i>191</i>
<i>Viewing Node Data and Modifying Node Properties</i>	<i>194</i>
<i>Viewing Interface Data and Modifying Interface Properties</i>	<i>196</i>
<i>Viewing Volume Details and Modifying Volume Properties</i>	<i>199</i>
<i>Polling on Demand</i>	<i>200</i>
<i>Rediscovering on Demand</i>	<i>201</i>
<i>Understanding and Acknowledging Events</i>	<i>202</i>

<i>Understanding Views</i>	204
<i>Viewing Charts</i>	207
<i>Understanding Alerts</i>	208
<i>Creating an Alert</i>	209
<i>Testing an Alert Action</i>	210
<i>Editing an Alert</i>	211
<i>Copying an Alert</i>	211
<i>Viewing Current Alerts</i>	211
<i>Disabling an Alert</i>	212
<i>Deleting an Alert</i>	212
<i>Understanding Alert Suppression</i>	212
<i>Dependent Node Alert Suppression Example</i>	215
<i>Failure of Load Balancing Alert Suppression Example</i>	216
Realtime Interface Monitor	217
<i>Beginning to Monitor Interfaces on Your Device</i>	218
<i>Modifying Statistics Update Intervals</i>	219
<i>Enabling Synchronous SNMP Queries</i>	219
<i>Customizing Statistics Groups</i>	219
<i>Exporting, Printing, and Copying Statistics</i>	220
<i>Publishing to the Web</i>	221
<i>Automatically Publish Discovered Information in HTML</i>	221
Router CPU Load	221
<i>Getting Started</i>	221
<i>Setting Polling Options, Notification, and Logging</i>	222
<i>Immediately Polling Monitored Routers</i>	223
<i>Setting All Routers to a Specific Poll Interval</i>	223
<i>Viewing Peak Load High-Water Marks</i>	223
<i>Resetting High-Water Marks</i>	224
<i>Printing CPU Loads</i>	224
<i>Saving Loaded Routers</i>	224
<i>Loading a Saved Router List</i>	224
<i>Deleting All Monitored Routers</i>	224
<i>Troubleshooting Router CPU Load</i>	225
SNMP Realtime Graph	225
<i>Graphing an OID Value</i>	226
<i>Modifying Polling Settings</i>	227
<i>Changing the Columns in the OID Table</i>	227
<i>Calculating Counter Rollovers</i>	228
<i>Customizing Graphs and Automatically Generating HTML</i>	228
<i>Viewing Raw Data</i>	230
<i>Exporting, Copying, and SNMP Graph Results</i>	230
<i>Publishing SNMP Graph Results in HTML</i>	231

Zooming	231
Customizing the OID	231
Syslog Server	232
Selecting Message Properties	232
Designating the Number of Messages to Display	233
Clearing Messages from the Display	233
Filtering Accepted Messages	233
Sending Syslog Messages	234
Searching the Syslog Server Database	234
Deleting Old Syslog Messages from the Database	234
Emptying the Syslog Server Database	235
Exporting, Printing, and Copying Messages	235
Watch It	236
Changing the audible alerts	236
Minimizing Watch IT	237

Chapter 7

Ping and Diagnostic Tools	239
DNS Analyzer	239
Getting Started	239
Viewing Discovered DNS Details	239
Viewing Packet Details	240
DNS Analyzer Menus	240
Adding Root DNS Servers	245
Modifying DNS Query Timeout	245
Deciding Whether to Lookup DNS Server Addresses	246
Understanding Colors in DNS Analyzer	246
Analysis Examples	247
Setting a Node as the Root and Rescanning	249
Enhanced PING	249
Logging Your Statistics	250
Exporting Results	251
Saving and Loading Profiles	252
Printing Results	252
Resetting Statistics	252
Customizing the Graph	253
Modifying Enhanced Ping Settings	254
Zooming in on an area of the chart	254

- Ping 255
 - Exporting, Printing, and Copying Sweeps 255
 - Modifying Ping Settings 256
- Ping Sweep 257
 - Exporting, Printing, and Copying Sweeps 257
 - Ping Sweep Settings..... 258
 - Modifying ICMP Ping Settings 259
 - Publishing to the Web..... 260
- Proxy Ping 260
 - Modifying PING Settings..... 260
- Send Page..... 261
 - Send Page Settings 261
- Spam Blacklist..... 261
 - Spam Blacklist Menus 263
 - Spam Blacklist Toolbar 265
 - Spam Blacklist Settings 266
 - Exporting Spam Blacklist Results..... 266
 - Hints and Tips..... 267
- TraceRoute..... 267
 - Modifying TraceRoute Settings 268
 - Launching the Shared Credentials Database..... 271
 - Starting Concurrent Traces..... 272
 - Exporting, Printing, and Copying TraceRoute Results 272
 - Publishing to the Web..... 272
- Wake-On-LAN..... 273
 - Getting Started..... 273
 - Configuring Your PC to Support Wake-On-LAN..... 273
 - Enabling Directed Broadcasts on your Network..... 274
 - Wake-On-LAN Settings 275
- WAN Killer 275

Chapter 8

- Security Tools..... 277**
- Edit Dictionaries 277
 - Dictionary Editor Menus..... 278
 - Mutating a Dictionary..... 279

Importing a List of Words	279
Hints and Tips	279
Port Scanner	280
Exporting, Printing, and Copying Sweeps.....	280
Ping Sweep Settings	281
Modifying ICMP Ping Settings.....	282
Publishing to the Web	283
Remote TCP Session Reset.....	283
Remote TCP Session Reset Menus	283
Remote TCP Session Reset Toolbar	285
Remote TCP Session Reset Settings	285
Exporting from Remote TCP Session Reset.....	286
Remote TCP Session Reset Frequently Asked Questions.....	286
Router Password Decryption.....	286
Router Password Decryption Frequently Asked Questions.....	287
SNMP Brute Force Attack	288
SNMP Brute Force Attack Settings.....	288
SNMP Brute Force Attack Frequently Asked Questions.....	289
SNMP Dictionary Attack	289
SNMP Dictionary Attack Menus	290
SNMP Dictionary Attack Toolbar.....	292
SNMP Dictionary Attack Settings.....	293
Exporting from SNMP Dictionary Attack	294
Discovering All the Devices on Your Network.....	295
 Chapter 9	
SNMP Tools.....	297
SNMP MIB Browser.....	297
Browsing a MIB Tree.....	298
Exporting, Printing, and Copying MIB Data	300
Launching the Shared Credentials Database	301
Bookmarking Frequently Used MIBs.....	302
Viewing a List of MIBs in the Database	302
Running the SNMP Set Tool.....	302
Modifying SNMP MIB Browser Settings.....	303
Searching the MIB Tree	304

- MIB Viewer..... 304
 - Guidelines and Examples..... 305
 - Exporting, Printing, and Copying Values..... 306
- MIB Walk..... 307
 - Exporting, Printing, and Copying Values..... 307
- SNMP Trap Editor..... 308
 - Viewing Example Traps..... 309
 - Sending a Trap..... 309
 - Exporting, Printing, and Copying Values..... 309
 - Copying an Existing Trap Template to the Trap Editor 310
- SNMP Trap Receiver 310
 - Configuring Settings 311
 - Sending Test Traps 311
 - Exporting, Printing, and Copying Values..... 312
- Update System MIB 312

Chapter 1

Introduction and Installing

The SolarWinds Toolset provides the tools you need as a network engineer or network consultant to get your job done. Toolset includes best-of-breed solutions that work simply and precisely, providing the diagnostic, performance, and bandwidth measurements you want, without extraneous, unnecessary features. SolarWinds was founded by network professionals and continues to design tools for the network professional by listening to and enlisting the help of network professionals.

This document contains information for the tools contained in all toolset editions.

Editions

The Toolset comes in different editions that include different tools. The following table provides an easily scanned breakdown of editions and the tools included in each.

Tool	Standard Edition	Engineer's Edition
Advanced CPU Load		X
Advanced Subnet Calculator	X	X
Bandwidth Gauges	X	X
CPU Gauges		X
Compare Configs		X
Config Editor/Viewer		X
Config Uploader		X
Config Downloader		X
DHCP Scope Monitor		X
DNS Audit		X
DNS Analyzer		X
DNS/Whois Resolver	X	X
Edit Dictionaries		X
Enhanced PING	X	X

Tool	Standard Edition	Engineer's Edition
IP Address Management		X
IP Network Browser-Standard	X	
IP Network Browser-Professional		X
MAC Address Discovery		X
MIB Browser		X
MIB Updates System Fields		X
MIB Walk		X
MIB Viewer		X
NetFlow Configurator	X	X
NetFlow Realtime		X
Network Monitor		X
Network Performance Monitor		X
Network Sonar		X
PING	X	X
PING Sweep	X	X
Proxy PING		X
Port Scanner		X
Realtime Interface Monitor		X
Remote TCP Reset		X
Router CPU Load	X	X
Router Password Decryption		X
Router Security Check (unavailable in evaluation versions)		X
SNMP Brute Force Attack		X
SNMP Dictionary Attack		X
SNMP Graph		X
SNMP Sweep		X
SNMP Trap Editor		X
SNMP Trap Receiver		X

Tool	Standard Edition	Engineer's Edition
Spam Blacklist		X
Subnet List	X	X
Switch Port Mapper		X
Syslog Server		X
TFTP Server	X	X
Trace Route	X	X
Wake-on-LAN	X	X
WAN Killer		X
Watch It!	X	X

Requirements

The computer on which you install SolarWinds Toolset must meet or exceed the following requirements:

Software/Hardware	Requirements
Operating System	One of the following 32-bit operating systems is required: - Windows 2003 SP1 and later - Windows 2000 SP4 or later - Windows XP SP2 or later - Windows Vista Business and Ultimate Editions (IPv4 mode only) Note: 64-bit operating systems are currently unsupported.
CPU Speed	500MHz or faster
Memory	128MB or greater
Hard Drive Space	640MB or more
Window Account	Install requires an account with administrator privileges
Network	Must be accessible from the computer on which the Toolset is installed to successfully use any network tools

Software/Hardware	Requirements
.Net Framework	Version 2 or later
Database	Syslog Server additional component, used to capture and decode syslog messages sent from network devices, can support any of the following databases: • SQL 2000 Sp4 MSDE, Standard, or Enterprise • SQL 2005 Express, Standard, or Enterprise

Note: Microsoft Vista has implemented a layer of security (user account control (UAC)) that ensures hostile programs cannot run unnoticed with administrator privileges. When installing Toolset or running Toolset applications, consider the following notes:

- You may be prompted for administrator credentials
- You may be prompted to allow the application access to the computer.

This is expected behavior.

Installing Toolset

Installing Toolset is extremely simple. These applications do not require the complications of server-client architecture, the implementation of agents, or complicated script generation. The goal of Toolset has always been ease of use combined with powerful results. Before beginning the setup program, ensure your computer meets or exceeds the requirements to run Toolset. For more information, see “Requirements” on page 3.

To install Toolset:

1. Log on with an administrator account to the computer on which you want to install SolarWinds Toolset.
2. **If you downloaded the product from the SolarWinds website,** navigate to your download location and launch the executable. The setup program has either an exe or msi extension.
3. **If you received physical media,** navigate the autorun and launch the setup program.
4. Review the Welcome text, and then click **Next**.
5. Accept the license agreement on the License Agreement window, and then click **Next**. If you do not agree to the license agreement, click Cancel to exit the setup program.

6. Specify the appropriate information on the Customer Information window, and then click **Next**. On this window, you can select whether the Toolset is installed to the currently logged on user account profile or made available to any user account with access to this computer.
7. Browse to a file system folder where you want to install the Toolset program files, and then click **Next**. The default location is \Program Files\SolarWinds.
8. Click **Install** on the Ready to Install the Program window. Before you click install on this window, nothing has been modified on your computer. If you want to change anything you designated before this window, click **Back**.
9. Review the Setup Status window as Toolset installs.
10. Click **Finish** on the Wizard Complete window.
11. Provide the appropriate information on the Install Software License Key window, and then click **Continue**. You need a customer ID and password to successfully install the key. For more information, see “Software License Key” on page 7.

Upgrading Toolset

To upgrade to the current version of SolarWinds Toolset, find the upgrade path that matches your implementation in the following list:

- Upgrade Toolset from Engineer’s Toolset version 8 to Engineer’s Toolset version 9.1 can be done in place -- no manual uninstall required and no data lost.
- Upgrade Toolset from Standard Toolset version 8 to Standard Toolset version 9.1 can be done in place -- no manual uninstall required and no data lost.
- Upgrade Toolset version 9 to version 9.1 can be done in place (Standard to Standard, Engineer’s to Engineer’s, Evaluation to Evaluation) – no manual uninstall required and no data lost.
- Upgrade Toolset from Standard Toolset to Engineer’s Toolset requires uninstalling the Standard version and installing the Engineer’s version.
- Upgrade Toolset from an evaluation version to a licensed version of Toolset requires uninstalling the evaluation version and installing the licensed version.
- Downgrade Toolset from Engineer’s Toolset, including the evaluation version, to Standard Toolset requires uninstalling the Engineer’s version and installing the Standard version.

If you have determined that you need to uninstall before installing the newest version of Toolset, complete the following procedure.

To uninstall before upgrading toolset and keep your previously collected data:

1. Copy the files you want to preserve to a folder on your desktop. For more information about the files to copy, see “Backing Up or Migrating Your Toolset Implementation” on page 6.
2. Uninstall your older version of Toolset.
3. Install the new version of Toolset.
4. Copy the data files from the folder on your desktop to the new installation location. For more information about the files you will be copying, see “Backing Up or Migrating Your Toolset Implementation” on page 6.

Backing Up or Migrating Your Toolset Implementation

To back up your Toolset implementation after installing the newest version or to migrate your Toolset configuration and data files to another server, the following files should be considered integral to your success. Ensure you are installing the same version of Toolset as what was installed on the computer from which you copy these files. If you cannot find a file, you have not run the associated program. You can safely skip the file.

Files to backup or move	Purpose
*.BandwidthGauges	Bandwidth gauge settings files
Bandwidth-Monitor.cfg, dictionaries.cfg, DNS.cfg, IP-BrowserWeb.cfg, Network-Monitor.cfg, PortScan.cfg, SWDiscovery.cfg, SWNetPerfMon.cfg, TraceRoute.cfg, Watchit.cfg	Configuration settings files
*.IPDB	IP address management database
*.mdb	Syslog database
*.SNMP-Graph	SNMP Realtime graphs
*.SDB	Network Sonar databases

Software License Key

After installing the program, the Toolset setup program displays the licensing window. Complete the following procedure to enable a software license key.

To enable a software license key:

1. ***If the computer on which you installed Toolset is connected to the Internet and not behind a proxy server,*** enter the requested information on the Install Software License Key window, and then click Continue.

Note: The SolarWinds license registration server immediately issue a license key that enables Toolset.
2. ***If the computer on which you are installing Toolset is not connected to the Internet,*** you cannot authenticate to the SolarWinds license registration server. Complete the following procedure:
 - a. Click **Skip This and Enter Software License Key Now** on the Install Software License Key window.
 - b. Using another computer that is connected to the Internet, log in to the customer area of the SolarWinds website at www.solarwinds.com/keys.
 - c. Click **Software Keys** from the Customer Area menu.
 - d. Select the product for which you need a key, and follow the instructions on the page to obtain a key.
 - e. Enter the key in the **Enter Software License Key** field on the Toolset computer.
3. Click **Continue** to complete your Software License Key installation.

Understanding the Launchpad

The SolarWinds Toolset Launchpad provides more than a convenient way to launch the tools. You can use the launchpad to complete a number of tasks:

- Launch the tools
- Manage the Shared Credentials Database
- Review ARP, DNS, IP configuration, and Route information for your computer
- Launch the command prompt
- Rename and reorder the Toolset Launchpad groups
- Modify Startup behavior
- Access Information about your version, the Administrator Guide, the Community Site and Forums, and Online Support.

Managing the Shared Credentials Database

The shared credentials database can be accessed and edited directly from the launchpad or from the tools that currently use the database, including the Cisco Config tools, NetFlow Realtime, and Toolset Network Performance Monitor.

To manage the Shared Credentials Database:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Settings** in the left navigation pane.
3. Click **Manage** in the right pane.
4. ***If you want to add a credential set and the device support SNMP version 1 or version 2***, complete the following procedure:
 - a. Click **Add**.
 - b. Click **Community string**, and then type the appropriate community string.
 - c. Click **OK**.

5. ***If you want to add a credential set and the device supports SNMP version 3***, complete the following procedure:
 - a. Click **Add**.
 - b. Specify the appropriate information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
6. ***If you want to modify a credential set***, complete the following procedure.
 - a. Click the credentials you want to modify.
 - b. Click **Modify**.
 - c. Specify the appropriate information, and then click **OK**.
7. ***If you want to delete a credential set***, complete the following procedure.
 - a. Click the credentials you want to delete.
 - b. Click **Delete**.
 - c. Click **Yes** to confirm you want to delete the credentials.
8. ***If you want to associate your credentials with a device or disassociate credentials from a device***, complete the following procedure:
 - a. Click the credential you want to associate with the device.
 - b. Click **Devices**.

- c. If you want to associate a device, click **Add**, select a device from the list, and then click **OK**.

Note: You must have added the device through one of the tools for the device to be listed in the Devices for Association window.

- d. If you want to disassociate a device, select the device, and then click **Remove**.
- e. Click **OK**.

Reviewing Local ARP, DNS, IP Configuration, and Route Information

The launchpad provides a single place for viewing your host ARP, DNS, IP configuration, and route information.

To view this information:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Host Network Info** in the left navigation pane.
3. Click the information you want to view on the menu in the right pane:
 - ARP Info
 - DNS Info
 - IP Configuration
 - Route Info

Launching the Command Prompt

If you see something you need to check or correct while reviewing your host network information, the launchpad also provides the ability to launch the Command Prompt.

To launch the Command Prompt:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Host Network Info** in the left navigation pane.
3. Click **CMD Prompt** on the menu in the right pane.

Renaming Toolset Launchpad Groups

Should it be necessary for you to rename the groupings found in the left navigation pane, it is easy to do so.

To rename a grouping, double-click the group name in the left pane, and then type the new name.

Reordering Toolset Launchpad Groups

You can change the order in which Toolset Launchpad groups appear in the left navigation pane. For example, you can place your more frequently used toolset tool groups at the top of the launchpad.

To reorder Toolset Launchpad groups:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Settings** in the left navigation pane.
3. Click **Tabs** on the menu in the right pane.
4. Select the group you want to move, and then use the Move Up and Move Down buttons to change group location.

Creating and Populating Launchpad Groups

You can create new tool groups and populate them with the current toolset shortcuts provided in other tool groups. For example, you can place your more frequently used toolset tools in a **Commonly Used** group, and then use the ability to reorder your groups to move the group to the top of the launchpad.

To reorder Toolset Launchpad groups:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Settings** in the left navigation pane.
3. Click **Tabs** on the menu in the right pane.
4. Click **Add**, and then specify the name of your new tool group.
5. Click **OK** on the Add Group Status window.
6. Select the group in the left navigation pane that contains the tools you want to copy into the new group.
7. Drag and drop shortcuts from the selected group into the new group.

Modifying Launchpad Startup Behavior

You stop the Toolset Launchpad from being added to the system tray or automatically launch the launchpad when Windows starts.

To modify current launchpad behavior:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Settings** in the left navigation pane.
3. Click **General** on the menu in the right pane.
4. Check the appropriate checkbox in the Startup settings section of the right pane:
 - Run Toolset Launchpad when Windows starts up
 - Add Toolset Launchpad to the Windows System Tray

Viewing Version Information and Finding Help

The launchpad provides a convenient place to find your version information, access the Help, connect with other SolarWinds Toolset users on the forum, and connect to the SolarWinds website.

To find version information and Help:

1. Launch the Toolset Launchpad from the Start menu or the system tray icon.
2. Click **Help** in the left navigation pane.
3. Click the appropriate option in the right pane:
 - Software Version
 - Admin Guide
 - Community Site and Forum
 - Online Support

Chapter 2

Introducing the Tools

The following sections provide brief overviews of each of the tools included with Toolset.

Cisco-Specific Network Tools

Because SolarWinds recognizes the popularity of Cisco routers and switches, a number of tools have been designed specifically for these devices.

Compare Running vs. Startup Configs

Allows you to compare the Running and Startup (in NVRAM) configs on a Cisco router. Uncommitted changes to non-volatile memory can be easily discovered using this tool.

Config Downloader

Allows you to download a configuration file from a Cisco router to your computer.

Config Uploader

Allows you to upload a new or modified configuration file to a Cisco router. You can also change any Cisco configuration parameter using SNMP.

Config Viewer

Allows you to view the running configuration and create an archive for future reference. Config Viewer can also decrypt passwords and compare changes between routers or archived configuration files.

CPU Gauge

Allows you to monitor the real-time CPU load for a Cisco router.

IP Network Browser

Allows you to scan an IP subnet and display the responding devices on the subnet. IP Network Browser also provides details about each interface, including the following:

- Frame relay DLCIs
- Internetwork operating system (IOS) levels
- Flash memory
- Hub ports, if applicable
- Installed cards
- Routes
- ARP table

NetFlow Configurator

Allows you to use a wizard-driven interface to remotely configure NetFlow on your version 5 NetFlow-capable routers.

NetFlow Realtime

Allows you to capture exported NetFlow data from NetFlow enabled Cisco routers and switches, displaying detailed traffic information in realtime.

Password Decryption

Allows you to decrypt the enable password for a Cisco router.

Proxy PING

Allows you to initiate a PING test from any remote Cisco router to any SNMP enabled device. The results are calculated based on packets sent from the Cisco router directly to the other remote device.

Router CPU Load

Allows you to monitor the realtime CPU load on multiple Cisco routers at the same time. Load is displayed as a compact horizontal bar, allowing you to monitor many routers with the minimal amount of wasted real estate. Alerts can trigger when defined thresholds are exceeded.

TFTP Server

Allows you to transmit and receive multiple files concurrently without errors. SolarWinds TFTP Server is one of the only multi-threaded TFTP servers that also provide advanced security features.

IP Address Management Tools

IP addresses management is already complex, and, coupled with the growth rate of many companies, it is often difficult to eliminate current errors, much less match and remove addresses on decommissioned equipment. The IP address management tools from SolarWinds were designed to help alleviate the overhead, providing speed and ease of use to make address management quick and simple.

Advanced Subnet Calculator

Allows you to execute realtime DNS and PING test, while making subnet creation and network worksheet generation simple and easy.

DHCP Scope Monitor

Allows you to monitor DHCP (Dynamic Host Configuration Protocol) scopes and quickly locate scopes low on addresses. This tool displays the number of dynamically assigned and currently unassigned IP addresses for each scope.

DNS and Who Is Resolver

Allows you to determine who owns or controls a domain name, network, or IP address, while also offering forward and reverse DNS look-ups.

DNS Analyzer

Allows you to graphically display the hierarchy of DNS Resource records, including name server, CName, and pointer. The resulting DNS structure diagram makes it easy to see the relationships between multiple name servers and target IP addresses. Redirections from one Name Server to another are also displayed.

DNS Audit

Allows you to scan individual IP addresses or a range and perform forward and reverse lookups, providing quick identification of reverse DNS errors. The tool supports both DNS and WINS resolution.

IP Address Management

Allows you to monitor IP addresses within multiple subnets on your network and report on their usage. You can also use the tool to pre-allocate IP addresses.

Ping Sweep

Allows you IP network discovery using PING sweeps across an entire range of IP Addresses or Subnet. Ping Sweep displays IP addresses in use and not in use. The tool also provides reverse DNS lookup for discovered address.

Network Discovery Tools

The Network Discovery tools, some of the first tools developed by SolarWinds, help you discover a broad range of network issues. You can successfully discover something as large as the entire enterprise of nodes and networks, using Network Sonar, and troubleshooting something as specific as a reverse DNS error, using DNS Audit. The network discovery engine embedded in IP Network Browser and Network Sonar is one to the fastest, most extensive discovery engines on the market.

DNS Audit

Allows you to scan individual IP addresses or a range and perform forward and reverse lookups, providing quick identification of reverse DNS errors. The tool supports both DNS and WINS resolution.

IP Address Management

Allows you to monitor IP addresses within multiple subnets on your network and report on their usage. You can also use the tool to pre-allocate IP addresses.

IP Network Browser

Allows you to perform detailed network discovery with one of the fastest, most thorough, interactive TCP/IP network browsers available, and then displays the results in an easily understand format.

MAC Address Discovery

Allows you to map IP addresses to the MAC or physical interface addresses.

Network Sonar

Allows you to discover your network using one of the fastest, most comprehensive ICMP, SNMP, and DNS discovery engines available. Network Sonar also provides the ability to generate a detailed discovery database of your network, available in Microsoft Access format, if desired.

Ping Sweep

Allows you IP network discovery using PING sweeps across an entire range of IP addresses or subnet. Ping Sweep displays IP addresses in use and not in use. The tool also provides reverse DNS lookup for discovered address.

Port Scanner

Allows you to remotely discover the status of IP ports on an IP address or address range. You can limit the ports to scan by specifying a Quick List of port numbers or selecting ports from a list that includes their common uses.

SNMP Sweep

Allows you to scan an IP address range for responding devices, and then discovers device details using SNMP.

Subnet List

Allows you to quickly discover all subnets and masks on a network

Switch Port Mapper

Allows you to remotely discover details about each port and the devices connected to each port on your switches and hubs. Switch Port Mapper also discovers the MAC address, IP address, and hostname of connected devices.

Network Monitoring Tools

Network Monitoring is a critical component of a complete Network Management Toolset. With the SolarWinds Toolset you receive several tools that provide the ability to monitor everything from single port traffic to the response time and availability of every server in your network. Numerous tools in the SolarWinds Toolsets also provide graphical reporting and trend analysis capabilities.

Advanced CPU Load

Allows you to monitor your network device CPU utilization using SNMP, and then provides both realtime and historical views of utilization. This one tool allows you to monitor router, switch, and server CPU utilization.

Bandwidth Gauges

Allows you to view a set of gauges monitoring realtime transmit and receive traffic for any port, interface, or device. For convenience, you can create device or port groupings, saving them as profiles for repeat viewing.

CPU Gauge

Allows you to see the real-time CPU load for a Windows Server or Cisco router or switch.

Network Monitor

Allows you to monitor hundreds of nodes concurrently and provide visual alert indicators, audible alarms, send e-mail messages and pages when devices fail to respond. Network Monitor also generates historical response time charts.

Network Performance Monitor

Allows you to track network latency, packet loss, traffic and bandwidth usage, and many other network statistics in realtime. Taking advantage of SNMP, Network Performance Monitor can report when a node reboots or an interface goes down and alert you when a router reboots, a server fails, an interface goes down, bandwidth traffic exceeds a set threshold, or network latency increases, among other events.

Realtime Interface Monitor

Allows you to display numerous statistics from routers and switches simultaneously, such as, interface and port status, time of last change, current transmit and receive traffic rates, interface percent utilization, duplex settings, collisions, alignment errors, runts, and giants.

Response Time Charts

Allows you to display historical data collected by Network Monitor.

Router CPU Load

Allows you to view realtime CPU load for Cisco routers arranged in a set of bar graphs. You can simultaneously view the load on one or many routers, and you can define threshold-based alerts.

SNMP Graph

Allows you to monitor and graph the statistics from any MIB OID that responds to SNMP. With SNMP Graph, you can monitor numerous elements concurrently and graphically display their performance.

Syslog Server

Allows you to listen for incoming Syslog messages on UDP port 514 and decodes the messages for logging purposes.

Watch It

Allows for immediate notification when a router, circuit, or server goes down or becomes unreachable.

Ping and Network Diagnostics Tools

The following is a brief overview of the Ping & Diagnostic tools available in the Toolset:

DNS Analyzer

Allows you to graphically display the hierarchy of DNS Resource records, including name server, CName, and pointer. The resulting DNS structure diagram makes it easy to see the relationships between multiple name servers and target IP addresses. Redirections from one Name Server to another are also displayed.

Enhanced Ping

Allows you to view and monitor realtime graphs of response times and packet loss from multiple devices concurrently. The graphing utility allows you to format the results to accommodate a large range of presentations.

Ping

Allows you to collect a running average of response time and packet loss, as well as current response times. The packet size, delay between PINGs, ICMP timeout, and time-to-live (TTL) can be set. The PING tool can also export statistics to text or rtf or print reports.

Ping Sweep

Allows IP network discovery using PING sweeps across an entire range of IP addresses or subnet. Ping Sweep displays IP addresses in use and not in use. The tool also provides reverse DNS lookup for discovered address.

Proxy PING

Allows you to initiate a PING test from any remote Cisco router to any SNMP enabled device. The results are calculated based on packets sent from the Cisco router directly to the other remote device.

Send Page

Allows you to quickly and easily send a text email or page without a locally installed email client.

Spam Blacklist

Allows you to test the IP addresses of your mail servers and verify they have not been blacklisted. By verifying your blacklist status, you can ensure mail sent from your systems successfully reaches the appropriate destination.

Trace Route

Allows you to run a trace routes across the network and displays the response time per device and DNS name by device.

Wake-On-LAN

Allows on-demand transmission of a *magic* packet to a remote device or server to switch on that device, assuming the NIC card or motherboard has been configured to support Wake-on-LAN (WoL).

WAN Killer

Allows you to generate traffic over a wide area network (WAN) connection. Set the circuit bandwidth and the load percentage desired and WAN Killer generates random traffic to meet that percentage. Transmitted packet size can also be adjusted.

Security Tools

The following is a brief overview of the Security tools available in the Toolset:

Edit Dictionaries

Allows you to change the dictionaries used with SNMP Dictionary Attack or import new dictionaries.

Port Scanner

Allows you to remotely discover the status of IP ports on devices. You can specify a range of IP addresses to be included in the scan, and then scan either by specifying a list of port numbers or selecting ports from a list that includes their commonly used purpose.

Remote TCP Session Reset

Allows you to remotely display all active sessions on a terminal server, router, dial-in server, or access server and easily reset any session.

Router Password Decryption

Allows you to decrypt the enable password for a Cisco router.

Security Check

Allows you to check your Cisco Catalyst or router security through emulating an attack and attempting to determine the read-only or read-write SNMP community strings. You can use this tool to decide whether the Cisco IOS needs to be upgraded.

SNMP Brute Force Attack

Allows you to remotely determine an SNMP read-only or read-write community string by trying every possible combination of letters and numbers. This tool can be customized to only try certain character sets or certain length community strings. The attack speed can also be customized.

By using this tool you accept the license agreement and agree to only run this application on networks under your management.

SNMP Dictionary Attack

Allows you to aggressively attack your network using dictionary based attacks on SNMP enabled devices. The SNMP Dictionary Attack application was written for companies who want to ensure their SNMP community strings are secure. Included with the SNMP Dictionary Attack are many pre-loaded dictionaries common to the hacker community, a dictionary permutation editor to morph the dictionaries, and the ability to import your own dictionaries.

By using this tool you accept the license agreement and agree to only run this application on networks under your management.

SNMP Tools

With this group of tools, you can view MIB values a number of different ways. You can browse through different MIB values on a device, display all MIB values, or display specific values.

SNMP MIB Browser

Allows you to walk MIB trees, view MIB tables, search MIBs, remotely modify SNMP values, among other functions, using the extensive MIB database from SolarWinds. The MIB database contains over 1,000 MIBs and over 100,000 public and vendor private OIDs.

SNMP MIB Viewer

Allows you to view any OID or table in the extensive SolarWinds MIB database. The SNMP MIB Viewer provides quicker retrieval of frequently used MIBs than SNMP MIB Browser.

SNMP MIB Walk

Allows you to generate a table of all MIBs and OIDs supported on a specific device by walking the SNMP tree for a target device.

SNMP Trap Editor

Allows you to modify SNMP trap templates used by the SolarWinds Network Management Tools. You can create SNMP traps of almost any structure, including the ability to mimic traps generated by network hardware.

SNMP Trap Receiver

Allows you to receive and display SNMP traps sent from network management applications, network devices, or servers. Consider using this tool to analyze the format of a trap and to verify trap sources are correctly configured and functioning.

Update System MIB

Allows you to easily update system information for SNMP devices, including system name, location, and contact. Consider using this tool to update information for network printers, hubs, and terminal servers.

Chapter 3

Cisco-Specific Network Tools

The following sections provide detailed information about the Cisco tools included in the Toolsets.

- “Compare Running vs. Startup Configs” on page 25
- “Config Downloader” on page 28
- “Config Uploader” on page 31
- “Config Viewer” on page 37
- “CPU Gauge” on page 44
- “IP Network Browser” on page 46
- “NetFlow Realtime” on page 59
- “Router Password Decryption” on page 63
- “Proxy Ping” on page 63
- “Router CPU Load” on page 64
- “TFTP Server” on page 68

Compare Running vs. Startup Configs

Use this tool to compare the running and startup (in NVRAM) configs of a Cisco router. If changes were made to the configuration but not committed to non-volatile memory, you can detect differences between the two configurations. Always compare running and startup configs before rebooting a router.

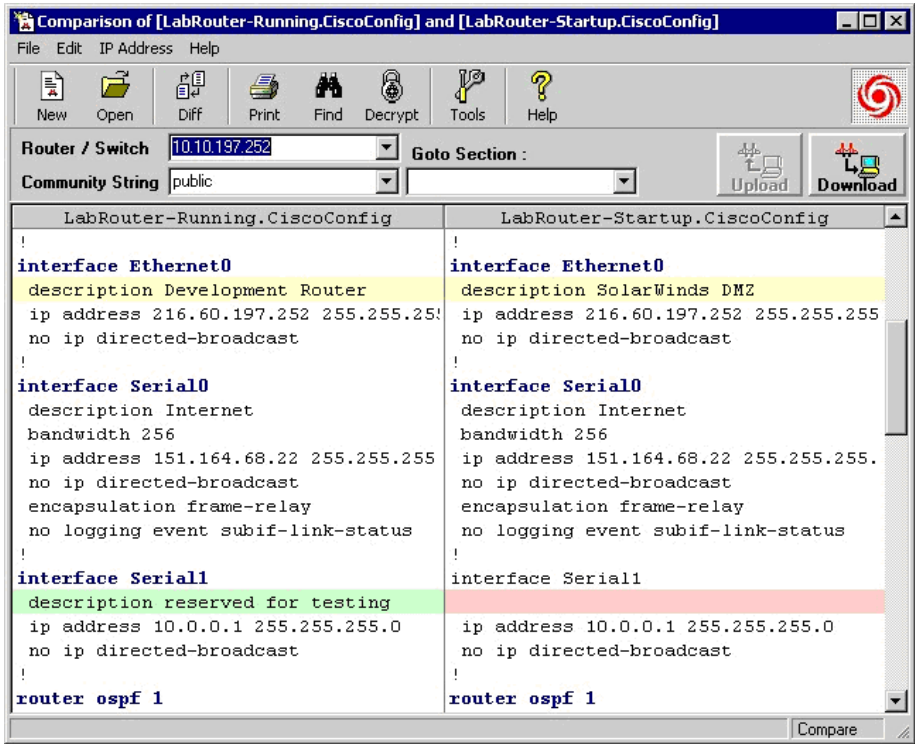
To compare the currently running config with the startup config:

1. Click **Select Device**, and then specify the IP address or hostname of the device.
2. Select whether you want to use a community string or SNMP version 3 credentials.
3. If you want to test the credentials, click **Test**.
4. Click **OK**.
5. *If prompted*, specify whether you want to store the credentials you specified in the shared credentials database.

6. Click **Compare Configs**.

When downloading a configuration file, the SolarWinds TFTP Server starts automatically if necessary. If the TFTP Server is running, an icon is displayed in the Windows System Tray. To see the TFTP Server log, click the icon and click **Status** on the TFTP Server menu. The TFTP Server log will display any errors that occurred while transferring the configuration files.

After downloading both configurations, the comparison is displayed in the Config Editor/Viewer.



Notes:

- Ensure your access list does not block SNMP queries.
- Cisco routers stop responding to SNMP queries while they are requesting a file from a TFTP Server. They also stop responding to SNMP while sending files to a TFTP Server. If you instruct a Cisco router to upload or download a new configuration file and it cannot for some reason, the action is attempted numerous times – repeating up to a minute. During this time, the router will stop responding to SNMP queries. You have to wait until the previous router action times out, and then try again.

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.
 - a. *If you want to add a community string*, click Community string and then type the string.
 - b. *If you want to add SNMP version 3 credentials*, click SNMP Version 3, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Config Downloader

The SolarWinds Config Download tool is used to download the configuration files from a Cisco router or switch. With Config Download you can specify the target directory in which to save the config files (configs). The config download tool lets you download configs quickly and archive them for later use. You do not need to view the downloaded config each time. In order to use the config download tool, you need the SNMP read-write community string for the router or switch that you are downloading changes from. You will also need a TFTP Server for the router or switch to communicate with. You can use SolarWinds TFTP Server or any other TFTP Server.

Some of the uses for the Config Downloader include:

- Shutting down an interface
- Resetting or changing a login or enable password
- Changing banners
- Modifying access lists
- Modifying any other configuration setting

Getting Started

The Config Download sends instructions to a router or switch via SNMP. This is why the SNMP read-write community string for the target router or switch is needed. The router/switch then transmits the configuration file to the target directory using the TFTP Server specified.

To download a configuration from a router or switch:

1. Click **Select Router**, and then specify the IP address or hostname of the device.
2. Select whether you want to use a community string or SNMP version 3 credentials.
3. If you want to test the credentials, click **Test**.
4. Click **OK**.

5. **If prompted**, specify whether you want to store the credentials you specified in the shared credentials database.
6. Click **Copy Config from Router/Switch to PC**.

Notes:

- Ensure your access list does not block SNMP queries.
- Cisco routers stop responding to SNMP queries while they are requesting a file from a TFTP Server. They also stop responding to SNMP while sending files to a TFTP Server. If you instruct a Cisco router to upload or download a new configuration file and it cannot for some reason, the action is attempted numerous times – repeating up to a minute. During this time, the router will stop responding to SNMP queries. You have to wait until the previous router action times out, and then try again.

The new configuration file is simply a text file with any set of commands that you would like to merge with the running configuration. For more information on Cisco command syntax and valid commands for your router or switch visit Cisco. For more information about configuration files, see “Example Configuration Files” on page 33.

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.

- a. **If you want to add a community string**, click Community string and then type the string.
- b. **If you want to add SNMP version 3 credentials**, click SNMP Version 3, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Advanced Options

The advanced options may be turned on or off by clicking **Advanced Options** or **No Advanced Options**. The advanced options default is to place the downloaded Config file in the default system directory and to use the TFTP Server configured for the workstation. When the Advanced Options are selected the following features are available:

View Config File After Downloading

If this checkbox is selected, the config download will automatically launch the SolarWinds Config Viewer and display the downloaded config file.

Save Config to

This window allows you to either directly enter the desired directory name in which to archive the downloaded config file or by using the browse (...) button you may browse your directory structure and select the desired folder.

TFTP Server Address

A specific TFTP Server may be selected by entering the IP Address of the TFTP Server.

Status Window

This window is used to display the status of the download as it progresses.

Config Downloader Menus

The following Menus are available in the Config Download tool:

Edit**Shared Credentials Database**

Allows you to add credentials and associate credentials with devices. This database can be accessed by numerous tools within the toolset.

Router Menu**Ping Router**

Ping the IP address entered in the "IP Address or Hostname" text box.

Telnet

Telnets to the address entered in the "IP Address or Hostname" text box.

IP Network Browser

Browses the address entered in the "IP Address or Hostname" text box using SolarWinds IP Network Browser.

Config Uploader

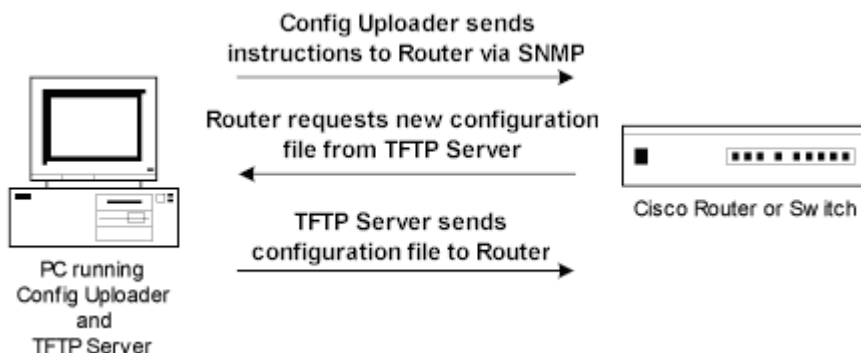
The SolarWinds Config Uploader is used to upload configuration changes into a Cisco router or switch. Config Uploader can be used to change an entire config or just one or two parameters. In order to use the Config Uploader, you will need the SNMP read-write community string for the router or switch that you are uploading changes into. You will also need the SolarWinds TFTP Server for the router or switch to communicate with.

Some of the uses for the Config Uploader are:

- Shutdown an interface
- Reset/change a login or enable password
- Change banners
- Modify access lists
- Modify any other configuration setting

Getting Started

The Config Uploader sends instructions to a Cisco router or switch via SNMP. This is why the Cisco Upload tool requires the SNMP read-write community string for the target router or switch. The device then requests the new configuration file from the TFTP Server and merges the new configuration file with the running configuration. You can also have the Config Uploader write the new configuration changes to non-volatile RAM by checking **Write to NVRAM also**.



To upload a configuration change to a Cisco router or switch:

1. Create the new configuration file
2. Place the new configuration file in the TFTP Server's root directory.
The new configuration should be placed in the root directory of the TFTP Server.
3. Click **Select Router**, and then specify the IP address or hostname of the device.
4. Select whether you want to use a community string or SNMP version 3 credentials.
5. If you want to test the credentials, click **Test**.

6. Click **OK**.
7. **If prompted**, specify whether you want to store the credentials you specified in the shared credentials database.
8. Click **Copy Config from PC to Router/Switch**.

Notes:

- Ensure your access list does not block SNMP queries.
- Devices must support the writeNet MIB to support this tool.
- Cisco routers stop responding to SNMP queries while they are requesting a file from a TFTP Server. They also stop responding to SNMP while sending files to a TFTP Server. If you instruct a Cisco router to upload or download a new configuration file and it cannot for some reason, the action is attempted numerous times – repeating up to a minute. During this time, the router will stop responding to SNMP queries. You have to wait until the previous router action times out, and then try again.

Example Configuration Files

Configuration files are text files containing commands you want to merge with the running configuration. There are no special rules for naming this file. You may give it any filename you choose. The following examples illustrate some common configuration changes.

Shutdown Interface Ethernet0/2

```
interface Ethernet0/2
shutdown
```

Replace the Logon Banner

```
banner motd $
Internet-Gateway
Cisco 7200
Support Number: 800-555-1212
Contract Number: A34511-23
Serial Number: 123456789
$
```

Reset the Enable Password to “New*Password”

```
enable password New*Password
```

Note: You can change an enable secret password the same way.

Change All Buffer Settings

```
buffers small
```

```
permanent 500
```

```
buffers small max-free 1000
```

```
buffers small min-free 150
```

```
buffers middle permanent 500
```

```
buffers middle max-free 1000
```

```
buffers middle min-free 150
```

```
buffers big permanent 200
```

```
buffers big max-free 400
```

```
buffers big min-free 150
```

```
buffers verybig permanent 150
```

```
buffers verybig max-free 300
```

```
buffers verybig min-free 50
```

```
buffers large permanent 100
```

```
buffers large max-free 200
```

```
buffers large min-free 50
```

```
buffers huge permanent 50
```

```
buffers huge max-free 100
```

```
buffers huge min-free 10
```

Note: By creating a single configuration file with all the new buffer settings and then upload the change to all your routers using Config Uploader, you can easily avoid any typing errors.

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.
 - a. *If you want to add a community string*, click Community string and then type the string.
 - b. *If you want to add SNMP version 3 credentials*, click SNMP Version 3, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Config Upload Menus

The following Menus are available in the Config Upload tool:

Edit

Shared Credentials Database

Allows you to add credentials and associate credentials with devices. This database can be accessed by numerous tools within the toolset.

Router Menu

Ping Router

Pings the IP address typed in the **IP Address or Hostname** field.

Telnet

Telnets to the address typed in the **IP Address or Hostname** field.

IP Network Browser

Browses the address typed in the **IP Address or Hostname** field using SolarWinds IP Network Browser.

Verify Community String

Verifies the community string typed in the **Community String** field matches the read-write community string for the address typed in the **IP Address or Hostname** field. You can use this menu selection to make sure you are using the correct community string.

Resetting an Enable Secret Password Using SNMP

The SolarWinds Config Uploader can easily reset any login or enable password on a Cisco router or switch. You do not need to know the password, just the router/switch's SNMP read-write community string.

1. Create a text file with a single line containing the new password and copy it to the TFTP Server root directory. This text file provides a set of configuration commands you want to merge with the running configuration. This is simply a text file. You may give it any filename you choose.
2. The following example text resets the enable password to "New*Password".

```
enable password New*Password
```

This will change the enable password even if it has been set using the type 5 "secret" method.

3. If you need to reset the login passwords for the vty (telnet) terminals, use the following example text:

```
line vty 0 4
password New*Password
login
```

4. Start the TFTP Server on your PC.
5. Ensure the text file is in the root directory of the TFTP Server.
6. Type the device address, community string, and the TFTP server IP address into the Config Uploader and click **Copy Config from PC to Router/Switch**.

Note: In this example, Config Uploader did not write to non-volatile memory. If you restart or reboot the router, the enable secret password resets back to the previous password, prior to the changes. Write the changes to non-volatile memory, if you want to ensure the router retains the new password after a restart.

Config Viewer

You can use the SolarWinds Config Viewer in many ways:

- Download configurations from Cisco routers and switches
- Compare date-based configurations of Cisco routers and switches
- Upload configurations to Cisco routers and switches
- Back up configurations
- Print configurations
- View and make changes to running router and switch configurations

Downloading a Config from a Cisco Router or Switch

Config Viewer makes it easy to download configs from your devices.

To download a Cisco configuration:

1. Click **Select Router**, and then specify the IP address or hostname of the device.
2. Select whether you want to use a community string or SNMP version 3 credentials.
3. If you want to test the credentials, click **Test**.
4. Click **OK**.

5. **If prompted**, specify whether you want to store the credentials you specified in the shared credentials database.
6. Click **Download**.
7. Select the config you want to download, currently running config or the start-up config in the routers memory.

Notes:

- When downloading a configuration file, the Config Viewer will automatically start the SolarWinds TFTP Server, if necessary. When running, the TFTP Server icon is displayed in the Windows system tray.
- To see the TFTP Server log, click on the icon, and then click **Status** on the TFTP Server menu. The TFTP Server log displays any errors that occur during configuration file transfer.
- Ensure your access list does not block SNMP queries.
- Cisco routers stop responding to SNMP queries while they are requesting a file from a TFTP Server. They also stop responding to SNMP while sending files to a TFTP Server. If you instruct a Cisco router to upload or download a new configuration file and it cannot for some reason, the action is attempted numerous times – repeating up to a minute. During this time, the router will stop responding to SNMP queries. You have to wait until the previous router action times out, and then try again.

Automatic Archiving of Downloaded Configuration Files

The Config Viewer creates an archive of each configuration file as it is downloaded. Archived config files are saved in subdirectories of the install directory. These subdirectories are named using a date-stamp using the following syntax: *mm-dd-yyyy*. When a configuration is downloaded, a copy is placed in the archive directory. Automatic archiving makes it easy to compare an older configuration with a current configuration to review changes. For more information about specifying the directory used as the root for archive directories, see “Preferences” on page 42.

Comparing Two Configurations

SolarWinds Config Viewer allows you to compare text-based configurations. You can compare the configurations of different routers or switches or compare an older version with the current configuration.

To compare two files:

1. Click **File > Compare Two Files**.
2. Provide the path to each file.

Note: Config Viewer shows compared files side by side with changes highlighted in yellow. Red designates missing lines. Green highlights added lines.

3. *If you want to print the comparisons*, click **File > Print**.

Decrypting Passwords

SolarWinds Config Viewer can decrypt Cisco type 7 passwords. The password decryption feature is used quite often with AS5200 (and other Cisco access servers) devices. The Config Viewer can download the configuration and decrypt all the login passwords in a manner of seconds. This is quite useful when converting AS5200 logins to TACACS or RADIUS.

To decrypt all type 7 passwords in a configuration file:

Click **Edit > Decrypt Passwords**.

Config Viewer searches and decrypts all type 7 passwords, highlighting them in green.

For more information about resetting type 7 or secret type 5 passwords, see the following sections:

- Reset the Enable Password to "New*Password" on page 34
- Resetting an Enable Secret Password Using SNMP on page 36

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.
 - a. *If you want to add a community string*, click Community string and then type the string.
 - b. *If you want to add SNMP version 3 credentials*, click SNMP Version 3, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Config Viewer Menus

The following options are available through Config Viewer menus:

Edit

Shared Credentials Database

Allows you to add credentials and associate credentials with devices. This database can be accessed by numerous tools within the toolset.

File Menu

New Config File

Saves a configuration file with a different name.

Open Config File

Loads a configuration file from disk.

Save

Saves the currently displayed configuration file. This does NOT write the configuration back to the router or switch. To upload a configuration to a Cisco router or switch, see “Config Uploader” on page 31.

Save As

Saves the currently displayed configuration as a new file name.

Close

Closes the current configuration file.

Compare Two Config Files

Compares two configuration files and displays the differences in a side-by-side view.

Compare Startup vs. Running Configs

Compares the current Running config file with the Startup config file in the Cisco routers memory.

Print

Prints the current configuration.

Print Preview

Allows you to preview the print before printing. When comparing configuration files, if the compared files split between two pages, decreasing the width of the Config Viewer window will make the comparison stay on one page.

Preferences

Downloading Configs

From the Preferences window you can change the default location to which downloaded Config files are saved. This window is accessed by selecting "File" then "Preferences..." from the menu.

Fonts and Colors

The Fonts and Colors setting allows you to adjust the default font size at which the downloaded Config files are displayed. The differences between two (2) config files are highlighted in RED, GREEN and YELLOW. These colors normally appear as pastel but can be changed to absolute Green, Red and Yellow.

TFTP Server Address

Specifies whether to use the local IP address as your TFTP server address or a different IP address.

Exit

Exits the Config Viewer.

Edit Menu

Undo Typing

Selecting "Undo" will reverse the last editing change to the configuration file.

Copy Selection

Copies the currently highlighted text to the windows clipboard.

Copy All

Copies the entire Config of the current file to the Windows Clipboard.

Cut

Deletes the currently highlighted text and puts it on the windows clipboard.

Paste

Pastes the contents of the windows clipboard into the current configuration file.

Delete

Deletes the currently highlighted text.

Find

Allows you to search for a particular string in the configuration file.

Decrypt Passwords

Scans the current file for all type 7 passwords and decrypts them. The decrypted password will be highlighted in green.

IP Address Menu

To use the IP Address menu, first highlight any IP address or subnet within the current configuration file.

Ping

PINGS the currently highlighted IP address.

Traceroute

Traces the route to the selected node.

Telnet

Telnets to the currently highlighted IP address. To use a different telnet program, see the Frequently Asked Questions.

IP Network Browser

Browses the currently highlighted IP address or subnet using SolarWinds IP Network Browser.

Troubleshooting Config Viewer

Consider the following notes to help troubleshoot any issues you encounter. Ensure you have also reviewed the notes following the download procedure. For more information, see “Downloading a Config from a Cisco Router or Switch” on page 37.

Ensure the TFTP Server setting is correct

Select File > Preferences, and then ensure the TFTP Server Address settings are correct. You may need to restart the Config Viewer after making these changes.

Ensure the device supports the writeNet MIB

Config Viewer uses the writeNet MIB, so devices that do not support this MIB do not support the tool.

CPU Gauge

The SolarWinds CPU Gauge monitors CPU load on routers, switches, and Windows 2000 and later computers. The CPU Gauge utilizes SNMP to communicate with the remote device, displaying the received results in an easily consumed graphical gauge. The following sections pertain to the default CPU Gauge skin.

Monitoring a Device

Complete following procedure to select a device to monitor.

To monitor a device:

1. Click on the button in the top right corner of the tool.
2. Click **Setup Gauge**.
3. Provide the IP address and the read or read/write community string for the device.
4. Click **OK**.

The left of the CPU Gauge provides the following statistics:

- Maximum load since monitoring began displayed in red
- Minimum load since monitoring began displayed in green

Current CPU Load is also displayed in the center of the gauge

Notes:

- Ensure your access list does not block SNMP queries.
- Ensure you use a valid read or read-write community string.

Saving a gauge setup

Complete the following procedure to save a loaded gauge.

To save a gauge:

1. Click on the button in the top right corner of the tool.
2. Click **Save Gauge**.
3. Provide a name for the configured gauge, and then click **Save**.

Loading a gauge

Complete the following procedure to load a saved gauge.

To load a gauge:

1. Click on the button in the top right corner of the tool.
2. Click **Load Gauge**.
3. Select the gauge you want to load, and then click **Open**.

CPU Gauge Skins

CPU Gauge ships with a number of different skins.

To change the skin of this utility:

1. Click the five vertical lines next to the title of the tool.
2. Select the new skin you want to use.

IP Network Browser

SolarWinds IP Network Browser is an interactive network discovery tool. IP Network Browser can scan a subnet and show the details about the devices on the subnet. Each IP address is sent a PING. For each responding address, IP Network Browser attempts to gather more information. It does this using SNMP (Simple Network Management Protocol). An SNMP agent must be active on the remote devices in order for IP Network Browser to gather details about the device.

The SolarWinds IP Network Browser is not specific to Cisco devices. It can discover any device with an IP address. If the device has an SNMP agent and the correct SNMP community string is included in the IP Network Browser Settings, IP Network Browser discovers a great deal about the device.

IP Network Browser inherently understands hundreds of types of devices and will discover different details about each. For example: User Accounts, Shares, and Running Services are discovered about Windows workstations and servers. For Cisco routers, the tool discovers IOS levels, the cards in each slot, flash memory details, interface details, frame relay DLCIs and their statuses, among other information.

You do not need to specify the SNMP community string for each device. Simply enter a list of community strings used on your network. IP Network Browser will determine the correct one for each device. For more information about entering SNMP community strings, see “Modifying IP Network Browser Settings” on page 52.

Getting Started

The first time you run IP Network Browser, a configuration wizard guides you through setting up the tool. Before completing the wizard, ensure you have the read or read-write community string and that an access list on your router is not blocking SNMP access.

To complete the configuration wizard:

1. Review the welcome window, and then click **Next**.
2. Provide a list of SNMP community strings you want to use to access devices on your network. Ensure you arrange the list so the most common SNMP community strings are listed first. Click **Next**.
3. Click the appropriate connection type, and then click **Next**.
4. Review the final window, and then click **Finished** to launch the tool.

To scan a subnet:

1. Type an IP address in the **Subnet Address** field.
2. Type the subnet mask in the **Subnet Mask** field, and then click **Scan Subnet**.

Note: You do not have to enter the exact network address. IP Network Browser is intelligent, and will calculate the correct subnet address based on the Subnet Mask. For example: if you enter 10.0.23.100 as the Subnet Address and 255.255.255.192 as the Subnet Mask, IP Network Browser will calculate the correct subnet. 10.0.23.64/255.255.255.192. For this example, IP Network Browser will scan from 10.0.23.65 to 10.0.23.126.

To scan a single device:

1. Type a hostname or IP address in the **Hostname or IP Address** field.
2. Click **Scan Device**.

Note: **Scan a Single Device** and **Scan an IP Address Range** are not available in the Standard Edition.

To scan an IP range:

1. Type the beginning IP address in the **Beginning IP Address** field.
2. Type the final IP address of the range in the **Ending IP Address** field, and then click **Scan Address Range**.

Notes:

- When scanning a range of IP addresses, there is a good chance you may scan a network or broadcast address. When you scan a broadcast address, any device (or all devices) on the subnet may respond. The discovery information may be a mix from many different devices.
- The **Scan a Single Device** and **Scan an IP Address Range** options are not available in the Standard Edition.

IP Network Browser Menus

File Menu

New Subnet Window

Displays another IP Network Browser window.

Export Wizard

Exports the results from IP Network Browser.

Print Preview

Displays a preview of exactly what the print out would look like.

Print

Prints the current results.

IP Network Browser Settings

Displays the IP Network Browser Settings dialog box.

Configuration Wizard

Displays the Configuration Wizard that was run the first time you launched IP Network Browser.

Exit

Closes the IP Network Browser window.

Edit Menu**Copy Selected**

Copies the highlighted item to the Windows clipboard.

Copy Selected Tree

Copies the highlighted item and ALL children in the tree under that item to the Windows clipboard.

Nodes Menu**Expand and Discover details for selected Node**

Expands all discovery trees for the selected node. To expand all trees or selected trees for ALL nodes, use the "Expand and Discover details for All Nodes..." menu selection from the Discovery Menu.

Note: If you see a message stating that the ActiveX component can't create object, a component of your SolarWinds Toolset has been deleted or moved. Reinstall the toolset. Your existing license will still work and you will NOT need to re-register.

Collapse all Nodes

This selection collapses all expanded trees.

Refresh Node Details

Deletes all discovered information for the selected Node. Expand the discovery trees to rediscover the details about the node.

Delete Selected Node

Removes the selected node from the list. To remove all nodes of a specific type, use the

Tools Menu

You can customize the list of Tools by editing the Tools.Menu file. This file and other customization files are located in the IP-Network-Browser directory one level below the SolarWinds Toolset installation directory. For more information, see "Customizing the Tools Menus" on page 56.

Ping

PINGS the selected node or IP address.

Web Browser

Opens the default web browser with the selected node or IP address as the target URL.

View Config File

Downloads the configuration from a Cisco router or Switch. This selection only works when the selected node is a Cisco device.

Telnet

Telnets to the selected node or IP address. IP Network Browser references a program named `telnet.exe`. Windows searches the directories defined by the `PATH` environment variable for the first occurrence of `telnet.exe`. If you would like to launch a different telnet program, you have two options:

- Edit the `PATH` environment variable and enter the location before `C:\Windows\System32`. You may also need to rename your telnet program to `telnet.exe`.
- Edit the `tools.menu` file. For more information, see “Customizing the Tools Menus” on page 56.

Traceroute

Traces the route to the selected node or IP address.

MIBs Menu

The list of MIB (Management Information Base) entries is dependant on the type of node currently selected. For example, a different set of MIBs will be listed on the MIBs menu for Cisco devices than when selecting a Windows Server. A working knowledge of SNMP and MIBs is needed in order to customize the MIBs menus. For more information, see “Customizing the MIBs Menu” on page 57.

Discovery Menu

Stop Discovery

Stops all scanning and detail discovery in the current window.

Rescan Subnet/Range

Rescans the current subnet or IP address range. The devices already discovered are not deleted. This simply adds any newly discovered devices to the current list.

Expand and Discover details for selected Node

Expands all discovery trees for the selected node.

Expand and Discover details for all Nodes

Allows you to select which groups of discovered information you wish to display. Only the selected items will be expanded. This function is particularly useful in discovering specific items across many nodes.

Filter node list

This selection allows you to filter for specific types of nodes and display only those selected. You can remove all nodes except certain types, or you can select which types of devices to remove from the discovery window.

Collapse all Nodes

This selection collapses all expanded trees.

Clear List

Deletes all nodes from the results window.

Subnet Menu

Scan Selected Subnet

Opens a new IP Network Browser window to scan the selected subnet. This selection only works when a subnet is selected from the results window.

View Menu

Toolbar

Shows or hides the toolbar at the top of the window.

Status Bar

Shows or hides the status bar at the bottom of the window.

Printing Discovery Results

You must first discover node details and expand the corresponding tree item to include details in the printed version of the discovery. For example, if you have discovered a Windows Server and would like the user accounts included in the printout, you must first expand the accounts tree so the account details will be discovered.

To print discover results:

1. Click **File > Print**.
2. Check the nodes you want to printed, and then click **Next**.

3. Check the discovery groups you would like included in the report, and then click **Next**. Discovery groups include accounts, routes, shares, and other information discovered through SNMP. Your discovery results may not include all the groups. Results depend on the discovered device type and what it supports.
4. Specify whether to include the SNMP community strings in the printed version, and then click **Print**.

Modifying IP Network Browser Settings

A number of settings can be adjusted to ensure IP Network Browser locates as many devices as possible within your network.

To change product settings:

1. Click **File > IP Network Browser Settings**.
2. ***If you want to modify the community strings tried when contacting devices***, click the Community Strings tab.
 - To add a community string, type the community string you want to add in the New Community String field, and then click **Add**.
 - To remove a community string, click the community string, and then click **Delete**.
 - To change the order in which community strings are attempted, select the community string and then click the up or down arrow.
3. ***If you want to modify the number of PINGs sent during the discovery mode or change the delay between Pings***, click the Discovery tab. ICMP PINGs are used to initially discover a responding node. If you are connecting over dialup or another slow connection, the wait and delay can be increased for better discovery and to limit traffic generated by the tool.

Warning: The number of PINGs per node should always be set to 2 or more, especially when scanning networks using Cisco routers. If the target IP address is not in the ARP cache of the Cisco router, the router will throw away the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never make it to the subnet of the target IP address. In this situation, the second PING will be the one the target IP address responds to.

4. ***If you want to modify the wait period before timing out change the PING time to live for a packet***, click the ICMP tab.
 - The PING timeout is the number of milliseconds to wait for a reply before assuming that the target IP address is not responding.
 - The packet time-to-live is the number of hops you will except while navigating to the specified IP address. With a setting of 32, your PING test could pass through up to 32 different routers on its way to the remote IP address before being thrown away by the network. Normally you would set this to 32 hops.
5. ***If you want to modify the community strings tried when contacting devices***, click the SNMP tab.
 - The packet timeout designates the number of milliseconds to wait for an SNMP reply before assuming the packet was lost and retrying. You can set this around 600 milliseconds, the internal SNMP logic of the tool automatically adjust when it notices dropped packets.
 - Query attempts defines how many times to retry an SNMP query before giving up. Set this to at least 2, to ensure one retry.

IP Network Browser Configuration Wizard

The configuration wizard helps you setup some basic configurations for the tool.

To complete the configuration wizard:

1. Review the welcome window, and then click **Next**.
2. Provide a list of SNMP community strings you want to use to access devices on your network. Ensure you arrange the list so the most common SNMP community strings are listed first. Click **Next**.
3. Click the appropriate connection type, and then click **Next**. If you select dialup, IP Network Browser adjusts ICMP timeouts and wait periods accordingly.
4. Review the final window, and then click **Finished** to launch the tool.

Saving the Discovery in HTML

The Engineer's Edition of IP Network Browser can save the current discovered information as an HTML page that can be published to your web server. You must first discover node details and expand the corresponding tree items to include details in the HTML version of the discovery. For example, if you have discovered a Windows Server and would like the user accounts included in the saved file, you must first expand the accounts tree so the account details will be discovered.

To save a discovery in HTML:

1. Click **File > Publish to Web**.
2. Check the nodes you want to include, and then click **Next**.
3. Check the discovery groups you would like included in the report, and then click **Next**. Discovery groups include accounts, routes, shares, and other information discovered through SNMP. Your discovery results may not include all the groups. Results depend on the discovered device type and what it supports.
4. Specify whether to include the SNMP community strings, and then click **Publish**.

When viewing the HTML in your browser, a blue plus (+) indicates a selection can be expanded to view additional detail. If a node does not have additional detail, ensure it was fully expanded and discovered prior to saving to HTML. The saved page does not perform discovery, it displays what was previously discovered.

Exporting the Discovery as a Text File

You can also export discovered results to a text file. You must first discover node details and expand the corresponding tree items to include details in the text version of the discovery. For example, if you have discovered a Windows Server and would like the user accounts included in the text file, you must first expand the accounts tree so the account details will be discovered.

To save a discovery in HTML:

1. Click **File > Export Wizard**.
2. Check the nodes you want to include, and then click **Next**.

3. Check the discovery groups you would like included in the report, and then click **Next**. Discovery groups include accounts, routes, shares, and other information discovered through SNMP. Your discovery results may not include all the groups. Results depend on the discovered device type and what it supports.
4. Specify whether to include the SNMP community strings, and then click **Export**.

Network Sonar can discover your network and create a Microsoft Access database. For more information, see “Network Sonar” on page 130.

IP Network Browser Command Line Operation

It is possible to launch the IP Network Browser directly from the command line. You must add the path to IP Network Browser in the PATH system variable or specify the full path when running the program from the command line.

Syntax

```
IP-Network-Browser HostIP [subnet/mask | startip-endip]
```

Where:

Hostip

IP address of a single machine

subnet/mask

Subnet address and mask separated by a "/"

startip-endip

An IP address range separated by a "-"

Examples

- Scan or discover a single device:
IP-Network-Browser 10.23.1.1
- Scan or discover an entire subnet:
IP-Network-Browser 10.23.1.1/255.255.255.0
- Scan or discover a range of IP addresses:
IP-Network-Browser 10.23.1.1-10.23.50.255

Customizing the Tools Menus

You can add new tools to the Tools menu by editing the Tools.Menu file. This file and other customizable files are located in the IP-Network-Browser directory in the SolarWinds Toolset installation directory.

The Tools.Menu file is a text file and can be edited from Notepad. The default Tools.Menu file is listed below.

```
#

# Tools Menu for IP Network Browser

#

#

#

# Macros that can be used with any command are:

#

# ${IP} IP address of the node

# ${Target} Node Name

# ${SysObjectID} Unique System OID for the node

# ${Community} SNMP community string for the node

#

#

&Telnet ... : telnet.exe ${IP}

Trace&Route ... : traceroute.exe ${IP}
```

To change the Telnet command:

Replace the current tool with the following entry: &Telnet ... :
C:\Program Files\MyFavoriteTools\mytelnet.exe \${IP}

To add a command called SSH:

Add the following entry on an empty line: &ssh ... : ssh.exe \${IP}
\${Community}

To add menu-dividing lines:

Enter a single hyphen (-) on a line alone.

Customizing the MIBs Menu

You can add new MIB references to the MIBs menu by editing the .MibsMenu files. These files and other customizable files are located in the IP-Network-Browser directory in the SolarWinds Toolset installation directory.

The *.MibsMenu files are text files that can be edited using Notepad. The filenames of the MibsMenu files are simply the vendor or machine specific sysObjectID followed by .MibsMenu. The sysObjectID can be discovered for a specific device by using IP Network Browser to discover it, and then expanding the **System MIB** section of the tree. You can also use SolarWinds MIB Browser to find or discover new MIB references.

```
# MIBs Menu for IP Network Browser

#

# Generic SNMP Devices

#

# Syntax for each line is ...

#

# Menu item : MIB table or tree

# &MAC Addresses of Interfaces ... : ifPhysAddress
&Running Software ... : hrSWRunTable
Installed &Software ... : hrSWInstalledTable
-

&IP Statistics ... : ipInReceives & Next 16
&ICMP Statistics ... : ICMP
&SNMP Statistics ... : SNMP

&TCP Statistics ... : tcpRtoAlgorithm & Next 11 & tcpInErrs &
tcpOutRsts

&UDP Statistics ... : udpInDatagrams & Next 3
-

RMON &Ethernet Statistics ... : etherStatsTable
RMON &Token Ring Statistics ... : tokenRingMLStatsTable
```

-

&Frame Relay Statistics ... : frCircuitTable

&BGP Peer Table ... : bgpPeerTable

Walking a Network from One Subnet to Another

If you right-click a selected subnet, you can zoom to the next subnet and scan it. IP Network Browser opens a new window and begins scanning the subnet in the new window.

NetFlow Configurator

The SolarWinds NetFlow Configurator provides a simple, wizard-driven tool to remotely configure your NetFlow-capable Cisco routers. At this time, support for version 5 of NetFlow is provided.

Notes:

- NetFlow Configurator uses SNMP to change the running config of the NetFlow-capable device. If your device cannot be updated using SNMP, it does not support the OID 1.3.6.1.4.1.9.9.387.1.2.1.1, then NetFlow Configurator cannot update the NetFlow configuration of the device.
- The following Cisco IOS versions support the configuration of NetFlow using SNMP:
 - o 12.4(10) or later
 - o 12.4(10)T or later
 - o 12.2S or later

To configure your NetFlow-capable Cisco router:

1. Open NetFlow Configurator from the **SolarWinds Engineer's Toolset > Cisco Tools** program menu.
2. Specify the hostname or IP address of the NetFlow device you want to configure.
3. Select the version of SNMP you want to use when communicating with this device. The community string or SNMP version 3 credentials you provide must have read-write access to the device.
4. Click the **Next**.
5. Ensure the Device Info section of the window provides the appropriate device information. That is, ensure you are modifying the correct device.

6. Specify the appropriate information in the Device NetFlow Configuration section of the window, and then click **Apply**.

- Provide the IP addresses and ports of the host you want the device to target with exported NetFlow data in the **Export to host** fields. NetFlow data can be exported to 2 different collection points.
- Select the ingress (incoming relative to the device) and egress (outgoing relative to the device) interface traffic you want to monitor. If you are using the NetFlow Configurator to setup NetFlow on a router for use with Orion NetFlow Traffic Analyzer, only the ingress traffic should be monitored.

Note: All information about all NetFlow data flowing through the device is exported to the specified hosts. Exported data is not confined to traffic generated or received on specific interfaces.

7. If you want to configure another router or switch, click **Configure another device**. Otherwise, click **Exit**.

NetFlow Realtime

NetFlow Realtime provides a granular view of your network traffic. Using this tool you can see the last 5 to 60 minutes of flow data broken out by applications, conversation, domains, endpoints, and protocols. You can use NetFlow Realtime to explore exactly how your bandwidth is being used and by whom.

Capturing NetFlow Data

Before you can begin analyzing data exported by your NetFlow enabled routers and switches, you need to capture the flows. Ensure you complete the following tasks before attempting to monitor data with NetFlow Realtime:

- Modify the configuration of your NetFlow device to ensure it is exporting NetFlow data. Due to the large number of different routers and switches that can export NetFlow data, consult your Cisco device documentation as to how to enable NetFlow data export. A technical reference is available on the SolarWinds website that provides guidance. For more information, see www.solarwinds.net/support/documentation.aspx and review the *Enabling NetFlow and NetFlow Data Export on Cisco Catalyst Switches* technical reference.
- Ensure you know the port on which to listen for NetFlow data. This port is part of the configuration of the NetFlow device.
- Ensure you know the IP address or hostname of the NetFlow device.
- Ensure you know the community string or SNMP version 3 credentials.

To begin capturing your NetFlow data:

1. Open NetFlow Realtime from the **SolarWinds Engineer's Toolset > Cisco Tools** program menu.
2. Specify the port on which your NetFlow device is exporting data in the **Listen on port** field.
3. Click the **Add Device** icon () , and then specify the following information on the NetFlow Device Credentials window.
 - IP address or hostname of the NetFlow device
 - Community string or SNMP version 3 credentials.
4. Click **Test**, and then review the Credentials Test window.
5. Make any necessary adjustments to your values on the NetFlow Device Credentials window, and then click **OK**.

Note: If NetFlow Realtime is able to see NetFlow data, a green check mark is displayed in the Sending NetFlow column of the NetFlow Analyzer user interface.

Storing NetFlow Data

NetFlow Realtime stores up to 60 minutes of captured NetFlow data in Microsoft Access-readable capture files. You can modify the location of capture files by changing the path displayed in the **Capture file** field of the NetFlow Realtime user interface.

Analyzing NetFlow Data

NetFlow Realtime offers up to 60 minutes of traffic to analyze, grouped in a number of different ways:

Applications

Allows you to see all the traffic passing through the specific based on the application. Applications use specific ports to send data. This mapping between port, application, and traffic is used to create the specific data points. Depending on the Top XX value, the number of applications listed in the tree changes. Clicking the top node, **Applications**, provides an inclusive graph.

Conversations

Allows you to see traffic based on source and destination IP, source and destination port, and the protocol used. These 5 data points grouped together and matched create a single conversation. For example, a conversation between 1.1.10.10 and google.com is defined by 1.1.10.10, google.com, port 80 (HTTP) on both IP addresses, and the TCP protocol. Clicking an IP address in the tree provides a view of all the other IP addresses or domains with which this IP address is communication. Clicking the top node, **Conversations**, provides an inclusive graph of your highest traffic conversations.

Domains

Allows you to see all traffic in a domain. The domain consists of all IP addresses that were resolvable, using reverse DNS, to that domain. Clicking a domain or IP address in the tree provides a view of all the other domains or IP addresses with which this domain is communication. Clicking the top node, **Domains**, provides an inclusive graph of all the domains on which traffic is being detected.

Endpoints

Allows you to select specific IP addresses (hosts) and view all the data transmitted and received by that host. Clicking the top node, **Endpoints**, provides an inclusive graph. This view does not separate data by application (port) or protocol, but provides an overview of your highest traffic producers.

Protocols

Allows you to see all the traffic that matches a specific protocol, for example, TCP or UDP. Clicking a specific protocol provides a view of the individual applications the protocol to traverse the specified interface. Clicking the top node, **Protocols**, provides an inclusive graph of all traffic produced split into protocols.

To view the data collected in easily analyzed graphs:

1. Click the interface through which NetFlow data is flowing and you want to analyze, and then click **Start Flow Capture**.
2. Review the information displayed in the analysis graphs.

Notes:

- The tree view can be expanded to reveal individual applications, conversations, domains, endpoints, and protocols. The tree views are dynamic and change based on time period and the selected Top ## number.
- The refresh rate is in seconds.

Defining Applications and Modifying Port Definitions

NetFlow Realtime uses the port utilized by an application to define the application.

To modify the definition of a port or define an unknown port:

1. Click the interface through which NetFlow data is flowing and you want to analyze, and then click **Start Flow Capture**.
2. Click **Tools > Application Mappings**.
3. To add a new Application definition:
 - a. Click the Add Application () icon.
 - b. Provide the appropriate information on the Add new window, and then click **OK**.
 - c. Ensure the spreadsheet of applications, protocols, and ports is correct, and then click **OK**.
4. To edit the definition of a port or Application:
 - a. Click the Edit Application () icon.
 - b. Modify the appropriate fields on the Edit window, and then click **OK**.
 - c. Ensure the spreadsheet of applications, protocols, and ports is correct, and then click **OK**.

Router Password Decryption

Router Password Decryption can decrypt Cisco type 7 passwords. Type 7 passwords are commonly used for terminal and enable logins on Cisco routers and switches. You must have the encrypted password string in order to decrypt the password. The encrypted string is normally taken from a printed Cisco configuration or by downloading the configuration directly from the router or switch.

To decrypt an encrypted password string:

Type or copy and paste the encrypted type 7 password string, and then click **Decrypt**.

For more information on how to reset an enable secret password, see “Resetting an Enable Secret Password Using SNMP” on page 36.

Notes:

- Type 5 secret passwords use a one-way hash algorithm and cannot be decrypted. However, they can be reset. You can reset a type 5 secret password using SolarWinds Cisco Config Uploader. It resets the password via SNMP. All you need is the SNMP read-write community string. For more information, see “Config Uploader” on page 31.
- If you need to decrypt numerous passwords, use SolarWinds Cisco Config Viewer. It can find all the passwords in a configuration file and decrypt them. This is convenient when converting a Cisco AS5200 to use TACACS or RADIUS. For more information, see “Config Viewer” on page 37.

Proxy Ping

With Proxy Ping, you can initiate a PING test from any remote Cisco router. The ICMP PING results are calculated based upon packets sent from the Cisco router directly to the other remote device.

To initiate a Proxy PING:

1. Specify the following information in the appropriate fields:
 - Hostname or IP address of the proxy Cisco router
 - Read-write community string for the router
 - Hostname or IP address of the target device to be PINGed
2. Click **PING via Proxy** to start the test.

3. To restart the test after reviewing the results, click **PING via Proxy** again.

Modifying PING Settings

You can modify the characteristics of the ICMP PINGS Proxy Ping sends.

To modify Proxy Ping settings:

1. Click File > Settings.
2. Specify the appropriate settings:
 - Number of PINGS -- the number of ICMP PINGS to process before the results and averages are calculated
 - Packet Size -- the size of the ICMP Packet sent from the remote proxy router
 - Inter-Packet Delay -- the delay between each PING transmission

Router CPU Load

Router CPU Load monitors the CPU load on Cisco routers in realtime. Each router is shown as a horizontal bar comprised of the current load and the high-water mark. Router CPU Load also provides the ability to generate popup alert messages whenever router load goes over a user-defined point and the ability to print the current load for all routers.

Getting Started

You can add numerous routers to your Router CPU Load user interface.

To monitor CPU load:

1. Click **Bar > Add New CPU Load Bar**.
2. Type the router IP address in the Target Router field.
3. Type the read-only or read-write community string for the router in the **Community String** field.
4. Select a poll time:
 - An average load over the last 5 minutes
 - An average load over the last minute
 - Realtime allows you to select a polling time from 1 to 60 seconds.
5. Select the name you want displayed for the monitored router:

- The SysName of the router
- A name you specify

Setting Polling Options, Notification, and Logging

Polling options setup the following options and features:

- Caution and warning levels for detected CPU loads
- SNMP timeout and number of attempts
- Notification types
- Logging

To modify options:

1. Click **Option > Polling Options**.
2. Click the Polling tab, and then select thresholds for the caution (yellow) and warning (red) levels. When the CPU load surpasses the value, the bar changes color.
3. Click the SNMP tab, and then specify the following values:
 - Select the number of milliseconds the tool should wait for an SNMP reply before assuming the packet was lost and trying again.
 - Select the number of times the tool should retry an SNMP query before giving up. This should normally be set to 2.
4. Click the Notification tab, and then check the notifications you want when the router exceeds the thresholds set on the Polling tab:
 - Check **Popup on alarm** to restore the tool from minimized mode when a threshold is exceeded
 - Check **Beep on alarm** to generate a system beep when a threshold is exceeded
 - Check **Open Notification window on alarm** to specify messages for exceeding caution and warning thresholds
5. Click the Logging tab, and then check Logging Enabled to specify a text log file and an interval at which to log CPU load on monitored routers.

Immediately Polling Monitored Routers

If you need the current status of your monitored routers, you can collect current state by immediately polling.

To immediately poll routers:

Click **Bar > Poll all routers now**, or right-click the bar that corresponds to the router you want to immediately poll and click **Poll**.

Setting All Routers to a Specific Poll Interval

You can quickly set all monitored routers to be polled at the same interval.

To set all monitored routers to the same polling interval:

Click one of the following options:

- **Bar > Set all bars to 5 minute decaying average**
- **Bar > Set all bars to 1 minute decaying average**
- **Bar > Set all bars to realtime**

For more information, see “Getting Started” on page 64.

Viewing Peak Load High-Water Marks

To view the high-water peak, peak load of a specific monitored router, mouse over the bar. A tooltip provides the exact time-date stamp and peak percentage of the high-water mark.

Resetting High-Water Marks

Router CPU Load provides at-a-glance high-water or max polled value markers within the monitored router bar. When you have corrected an issue, consider resetting your high-water marks to see how changes made affect your maximum CPU loads.

To reset high-water marks:

Click **Bar > Reset peak markers**.

Printing CPU Loads

You can print current CPU loads, if necessary. Printouts include the current load and the high-water marks, including the date and time of the peaks.

To print current CPU loads:

Click **File > Print**.

Saving Loaded Routers

After loading a number of routers you want to monitor frequently, consider saving the loaded information as a unique profile.

To save a loaded router profile:

Click **File > Save Profile** and then name and save the router profile.

Loading a Saved Router List

If you have taken advantage of the ability to save profiles, complete the following procedure to load your saved profiles.

To load a router profile:

Click **File > Load Profile**, and then select the router profile your want to load.

Deleting All Monitored Routers

If you need to delete the routers you have added to the Router CPU Load tool, complete the following procedure.

To delete all currently monitored routers from the tool:

Click **Bar > Delete all bars**.

Troubleshooting Router CPU Load

If you get an error message like "xxx does not support the Cisco AvgBusy MIB or is not responding to SNMP polls", then you probably need to reconfigure your router. Add the following lines to your Cisco router configuration file:

```
snmp-server community public R0
```

```
snmp-server community secret RW
```

These lines enable SNMP on your router. Of course you will want to put your own read/write community string in place of *secret*.

If SNMP is already configured on your router, look for a line in the configuration file similar to this:

```
snmp-server community public R0 60
```

The 60 at the end of this line is referring to an access list.

You need to do one of the following:

- Add your Router CPU Load tool computer IP address to the access list
- Add your entire range of internal IP addresses
- Remove the access list entirely

Ensure you do not have a firewall between you and your router that blocks SNMP.

TFTP Server

Numerous network devices, including routers, switches, hubs, X-terminals, printers, and terminal server devices, need a TFTP server to load initial configuration, IOS files, and transfer configuration file updates. SolarWinds TFTP Server was written to transmit and receive multiple configuration files at the same time using multiple connections.

Note: A TFTP Server is not an FTP server. TFTP and FTP are different protocols. You cannot connect to a TFTP server with an FTP client.

Configuring Your TFTP Server

The TFTP server runs as a service, but some basic configuration may be necessary to ensure the TFTP server behaves in a way that works best within your environment. Complete the following procedure to setup your server.

To configure your TFTP server:

1. Click File > Configure.
2. Click the General tab, and then specify whether to start the server.
3. *If you want the TFTP server to start with the computer*, check **Automatically start TFTP Server when computer starts**.
4. *If you want the TFTP server to appear in the task tray*, check **Add TFTP Server to Windows task tray**.
5. Specify a directory to use as the root directory of the TFTP server. Files received by the TFTP server are saved here. Files to be sent by the TFTP server must be first copied to this directory.
6. Click the Security tab, and select what actions you want to allow the TFTP server to do. For example, click **Receive files** if you want to restrict the server to only receiving files.
7. *If you want to restrict TFTP server functions to a specific IP address range*, click **Add** and then specify the beginning and ending IP addresses of the range. Then, click **OK**.
8. Click **OK**.

Note: TFTP protocol has no innate security. There are no passwords or authentication. SolarWinds TFTP Server adds security by allowing you to limit the server's functionality and specify a range of IP addresses from which to accept requests.

Chapter 4

IP Address Management Tools

IP addresses management is already complex, and, coupled with the growth rate of many companies, it is often difficult to eliminate current errors, much less match and remove addresses on decommissioned equipment. The IP address management tools from SolarWinds were designed to help alleviate the overhead, providing speed and ease of use to make address management quick and simple.

- “Advanced Subnet Calculator” on page 71
- “DHCP Scope Monitor” on page 77
- “DNS and Who Is Resolver” on page 80
- “DNS Analyzer” on page 82
- “DNS Audit” on page 92
- “IP Address Management” on page 94
- “Ping Sweep” on page 101

Advanced Subnet Calculator

SolarWinds Advanced Subnet Calculator assists you in calculating subnet masks and IP address management. This includes many powerful features, including the following:

- Able to break down the IP Address
- Performs DNS Resolution
- Offers classful subnet calculations
- Offers classless (CIDR) subnet calculations
- Provides a complete report of subnet addresses based on calculations

Looking Up Address Details

From the Address Details tab, you can execute forward and reverse DNS lookups, ping IP addresses, and convert them to hex and binary.

IP Address

Enter an IP address and click **Lookup Hostname** to lookup the DNS name of the IP address. The tool also PINGS the target and calculates the response time.

Hostname

Enter a Hostname and click **Lookup IP Address** to lookup the IP address. The tool also PINGS the target and calculates the response time.

Response Time

Provides the response time for the IP address or hostname.

Hex

Provides the hex equivalent of the IP address.

Binary

Provides the binary equivalent of the IP address.

Address Owner / Info

Provides a complete DNS Resolution of the owner of the IP address and bit template.

Copying to the Windows clipboard

Click **Copy Details** copy the current information to the Windows clipboard. Exporting is also available from the File menu. For more information, see “Exporting, Printing, and Copying Calculations” on page 76.

Classful Subnet Calculator

From the Classful Subnet Calculator tab, you can generate a list of subnets based on a number of different parameters. The classful approach to masking is the most common and is achieved by adhering to the standard classes:

- Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000
- Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000
- Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

The following information is calculated after entering an IP address:

- Subnet
- Mask
- Inverse mask
- Subnet size
- Host range
- Broadcast

IP Address

The IP address you specify is used as a base address when calculating subnets. Click **Generate Subnets** to calculate a list of subnets.

Subnet Mask

The subnet mask used when generating a list of subnets. The subnet mask automatically adjusts when you change any other parameters.

Mask Bits

Number of network (or mask) bits used when generating a subnet list. The number of mask bits automatically adjusts when you change any other parameters.

Host Bits

Number of host bits used when generating a list of subnets. The number of host bits automatically adjusts when you change any other parameters.

Number of Subnets

Number of subnets that can be generated based on the subnet mask. The number of subnets automatically adjusts when you change any other parameters.

Hosts per Subnet

Number of hosts within each subnet, based on the subnet mask. The number of hosts automatically adjusts when you change any other parameters.

Subnet Bit Mask

Mask template for the current subnet mask.

Copying to the Windows clipboard

Click **Copy Details** to copy the current subnet information to the Windows clipboard. Click **Copy Subnets** to copy the list of subnets to the Windows clipboard. Exporting is also available from the File menu. For more information, see “Exporting, Printing, and Copying Calculations” on page 76.

CIDR Calculator

Classless Inter Domain Routing (CIDR) provides a less wasteful way to allocate and specify IP addresses used in inter-domain routing more flexibly than with the original system of classful IP address assignment. As a result, the number of available addresses has been greatly increased. CIDR is now the routing system used by virtually all gateway hosts on the backbone network of the Internet. Many small companies also benefit from CIDR in that 4 class C's can be grouped into one subnet to provide over 1000 IP addresses.

IP Address

Provide an IP address to act as the base address when calculating subnets. Click **Generate Subnets** to calculate a list of subnets.

Subnet Mask

The subnet mask used when generating a list of subnets. The subnet mask will automatically be adjusted when you change any of the other parameters.

Mask Bits

Number of network (or mask) bits used when generating a list of subnets. The number of mask bits will automatically be adjusted when you change any of the other parameters.

Host Bits

Number of host bits used when generating a list of subnets. The number of host bits will automatically be adjusted when you change any of the other parameters.

Number of Subnets

Number of subnets that can be generated based on the subnet mask. The number of subnets will automatically be adjusted when you change any of the other parameters.

Hosts per Subnet

Number of hosts within each subnet based on the subnet mask. The number of hosts will automatically be adjusted when you change any of the other parameters.

Subnet Bit Mask

Mask template for the current subnet mask.

Copying to the Windows clipboard

Click **Copy Details** to copy the current subnet information to the Windows clipboard. Click **Copy Subnets** to copy the list of subnets to the Windows clipboard. Exporting is also available from the File menu. For more information, see “Exporting, Printing, and Copying Calculations” on page 76.

Subnet Addresses

The Subnet Addresses tab helps you generate a worksheet of IP addresses for any subnet. Notes for each IP address can be added in the Notes column. These notes are printed or exported when the list of IP addresses is printed or exported.

IP Address

Enter an IP address here. This IP address will be used the subnet address when generating a list of IP addresses. Click Generate Addresses to generate a list of IP addresses for the subnet.

Subnet Mask

The subnet mask used when generating a list of IP addresses.

Copying to the Windows clipboard

Click **Copy** to copy the list of IP addresses to the Windows clipboard. Exporting is also available from the File menu. For more information, see “Exporting, Printing, and Copying Calculations” on page 76.

Exporting, Printing, and Copying Calculations

After calculating information, the Advanced Subnet Calculator allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print calculated information.

Exporting Calculations

To export calculations on any tab of the product:

Click **File > Export**, and then select the type of export.

Copying Calculations

To copy the displayed data:

Click **Edit**, and then select the information to copy. The selection changes based on the tab you view.

Printing Calculations

To print displayed data:

Click **File > Print**.

DHCP Scope Monitor

The Dynamic Host Configuration Protocol (DHCP) Monitor Scope polls DHCP servers to extract IP scopes and highlight scopes low on addresses. The number of dynamically assigned and unassigned IP Addresses for each scope is displayed. You can use DHCP Monitor to show which scopes within your environment are running out of IP Addresses.

To add a DHCP Scope to the list of monitored scopes:

1. Click **Scope > Add DHCP Scope**.
2. Specify the IP address or hostname and the SNMP community string on the Add DHCP Scope window, and then click **OK**. You can add numerous DHCP servers to the tool, simultaneously monitoring numerous scopes.

Note: This tool supports DHCP scopes only on Windows NT, Windows 2000, and Windows 2003 servers and monitors scopes using SNMP. SNMP must be installed on the DHCP server.

Modifying DHCP Scope Monitor Settings

The settings used by DHCP Scope Monitor can be modified to reflect your environment and network needs.

To modify polling intervals, the alert level, and community strings:

1. Click **Settings** on the toolbar.
2. Click the Polling tab, and then adjust the polling interval.
3. Click the Alerts tab, and then adjust the time at which to consider IP address scope critically low. This setting marks the DHCP Scope, Scope name, and Available columns red when the number of IP addresses drops below the selected threshold.
4. Click the Community Strings tab, and then select the DHCP servers you want to monitor.
5. Click **OK**, when you have completed your changes.

Interpreting DHCP Scope Monitor Results

DHCP Scope Monitor displays several details about each DHCP Scope:

- DHCP Scope provides the subnet address of the scope.
- Scope Name provides an editable field, allowing you to specify a name for each scope. Double-click on the cell you wish to edit, and then type the name for each scope.
- Size display the total number of IP addresses defined for each scope.
- Leased provides the total number of used IP addresses.
- Available provides the total number of unused IP addresses.
- Server provides the server name.
- Status provides the date and time of the last poll and any error messages.

Note: Fields in red specify that the scope has dropped below your alert level.

Rescanning DHCP Scopes

You can refresh the DHCP scopes of a specific DHCP server or all monitored DHCP servers.

To rescan the entire range of DHCP scopes:

Click **Scope > Poll All DHCP Scopes Now**.

To refresh a single DHCP scope:

Select the scope, and then click **Scope > Poll Selected DHCP Scope**.

Exporting, Printing, and Copying DHCP Scope Results

After discovering scopes, you can transfer that information to other tools through exporting and copy and paste capabilities. You can also print results.

Exporting Calculations

To export calculations on any tab of the product:

Click **File > Export**, and then select the type of export.

Copying Calculations

To copy the displayed data:

Click **Edit**, and then select whether you want to copy all the results or just those results you select.

Printing Calculations

To print displayed data:

Click **File > Print**. Check the fields you want to include in your printout.

Discovering a List of Used IP Addresses

The DHCP Scope Monitor displays the number of addresses used and available. You cannot learn the used and available addresses directly from the DHCP Server. However, you can use SolarWinds Ping Sweep to scan the subnet. Ping Sweep shows the addresses in use. For more information, see “Ping Sweep” on page 101.

DNS and Who Is Resolver

SolarWinds DNS Resolver retrieves information about domain names and IP addresses and displays as much information as can be found about the specified hostname or address.

To begin resolving domain names or IP addresses:

1. **If you want to find the IP address of a host or domain**, type any of the following in the **Hostname** field:

- Hostname, for example, Server-4 or `www.solarwinds.net`
- URL, for example, `http://solarwinds.net`
- Email address, for example, `sales@solarwinds.net`
- Domain name, for example, `yahoo.com`

Click **Lookup Address** to retrieve information about the hostname or URL.

2. If you want to find the hostname or domain of a specific IP or network address, type any of the following in the **IP Address** field:

- IP address, for example, `206.67.58.195`
- Network address, for example, `206.67.58.0`

Click **Lookup Hostname** to retrieve the hostname and other details about the address.

Specifying WhoIs Servers

You can allow the tool to select a WhoIs server automatically or designate a specific server to use.

To modify the WhoIs server used by DNS Resolver:

1. Click **File > Settings**.
2. Uncheck **Automatically determine the correct WhoIs Servers**, and then type the IP address or hostname of the server you want to use or select the WhoIs server from the list.
3. Click **OK**.

Viewing a Cache of Resolved Names

You can directly access a cache of all the hostnames and IP addresses resolved by the tool. When a hostname or IP address is resolved, the DNS Resolver creates an HTML file containing all the discovered results and stores it in the DNS-Cache directory.

To view a cache of resolved names:

1. Navigate to your installation directory.
2. Locate the DNS-Cache directory, and then use your browser to view the HTML file named using your search parameter.

Note: Since the DNS-Cache directory is cleared when the program is closed, you should copy the files into another directory if you need to save them.

Exporting, Printing, and Copying Results

After resolving hostnames and addresses, you can transfer that information to other tools through exporting and copy and paste capabilities. You can also print results.

Exporting Calculations

To export calculations on any tab of the product:

Click **File > Export**, and then select the type of export.

Copying Calculations

To copy the displayed data:

Click **Edit > Copy**.

Printing Calculations

To print displayed data:

Click **File > Print**.

DNS Analyzer

You can use the DNS Analyzer tool to visually display the hierarchy of DNS resource records, including name server, CName, and pointer. The relationships between multiple Name servers and target IP addresses are easy to distinguish using the DNS structure diagram. Redirections from one Name server to another are also shown.

Getting Started

DNS Analyzer queries your DNS servers and graphically represents the results.

To begin querying your DNS servers and generate your graphical analysis:

Type the appropriate information in the **Hostname, URL, or E-Mail address** field, and then click **Draw DNS Structure**.

Viewing Discovered DNS Details

You can view details about each node in the discovered structure.

To view the details pane:

Select the server you want more information about, and then click **Details** . The Details pane is displayed on the right side of the screen.

The Details pane provides the following information:

- Server details
- Question sent to the server
- Record type asked for
- Parent node details
- Records returned

Viewing Packet Details

You can view details about the packet sent between servers directly from the DNS diagram.

To view packet details:

Right-click on a link between nodes, and then click **Packet Details**.

DNS Analyzer Menus

File Menu

New Diagram

Clears the existing diagram

Open Diagram

Opens a previously saved diagram

Save

Saves the current diagram

Save As

Saves the current diagram to a new file

Export Diagram

Allows you to select an export format for the diagram

Send Diagram to

Allows you to select from a list of media type to which to send the diagram

Publish to Web

Exports the results to an HTML file

Print Setup

Opens the Print Setup dialog

Print Preview

Previews the results exactly the same as it would appear when printed

Print

Prints the current diagram

Settings

Opens the Settings dialog

Exit

Closes the DNS Analyzer

Edit Menu

Copy as Bitmap

Copies the diagram as a bitmap to the Windows clipboard

Copy as Metafile

Copies the diagram as a Metafile to the Windows clipboard

Select All

Selects every object in the diagram

Delete Selected

Deletes the selected objects from the diagram

Hide

Hides the selected objects from the diagram

UnHide All

Returns all of the hidden objects to the diagram

Diagram Menu

Select

Allows you to select objects in the diagram

Pan

Allows you to pan the screen in all directions by clicking and dragging the mouse

Interactive Zoom

Allows you to zoom in and out by clicking and dragging the mouse up and down

Marquee Zoom

Allows you to select a zoom area by clicking and dragging the mouse around a specific area

Refresh

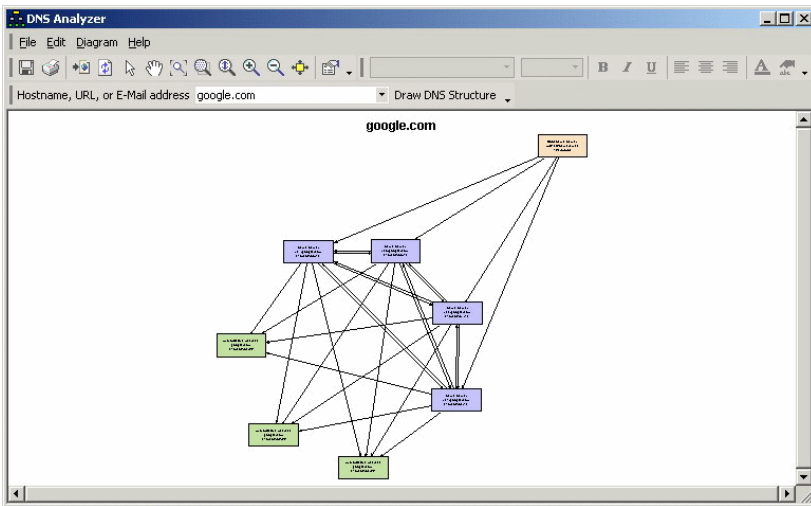
Rescans and redraws the current diagram

Zoom

Provides a number of different preset zoom options.

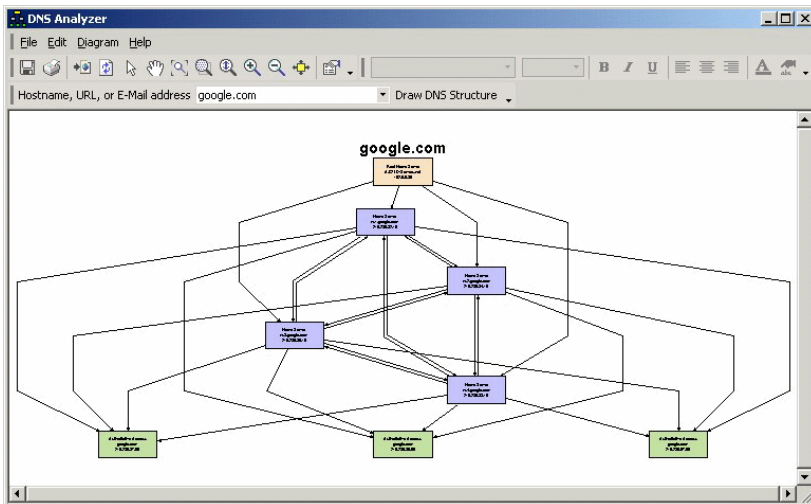
Auto Arrange – Circular

Rearranges the diagram in a circular pattern.



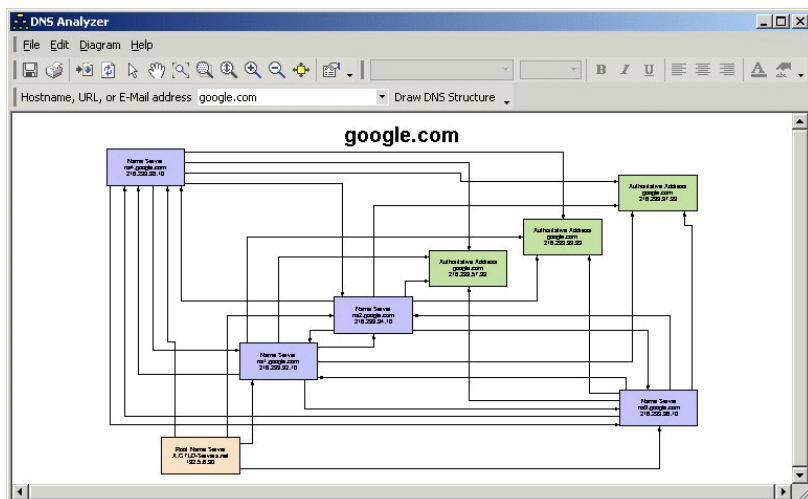
Auto Arrange – Hierarchical

Rearranges the diagram in a hierarchical pattern.



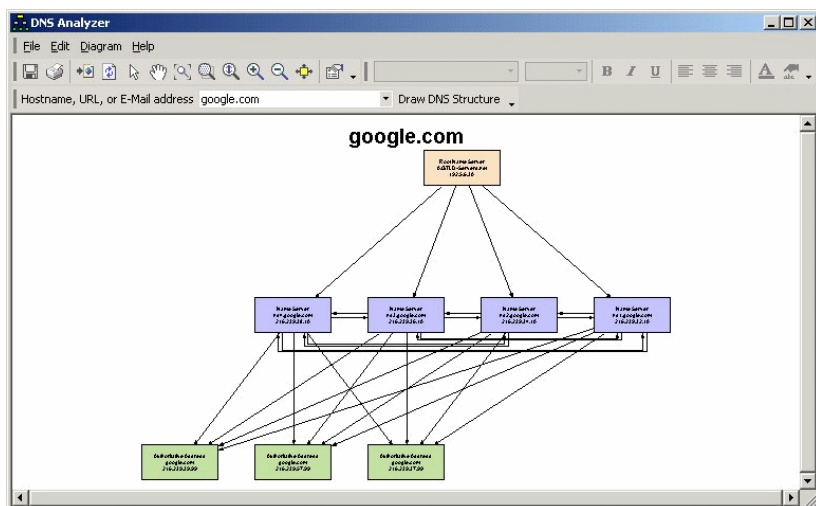
Auto Arrange – Orthogonal

Rearranges the diagram in an orthogonal pattern.



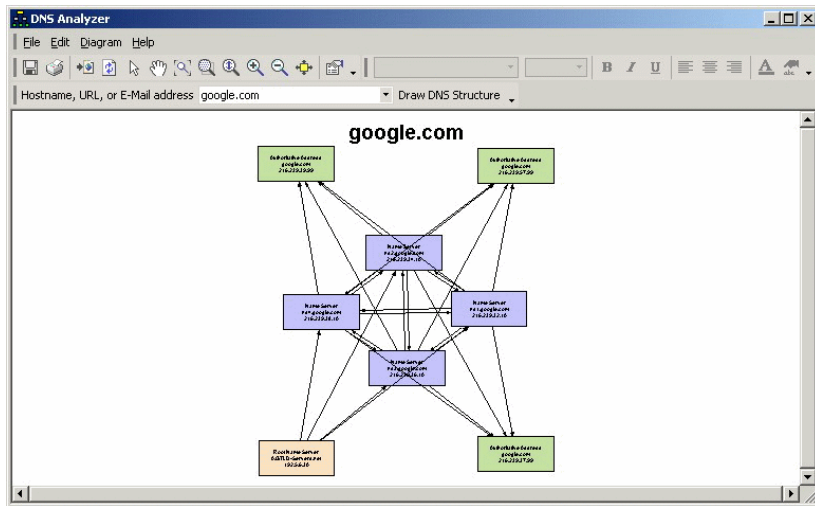
Auto Arrange – Tree

Rearranges the diagram in a tree pattern.



Auto Arrange – Symmetrical

Rearranges the diagram in a symmetrical pattern.



Auto Arrange - Reorganize

Redraws the diagram in the selected Auto Arrange style.

Auto Arrange - Auto Arrange Properties

Opens the Layout Properties dialog.

Auto Arrange - Arrange Labels

Automatically adjusts the label positions in the diagram.

Show Details

Opens the Details pane.

Adding Root DNS Servers

You can add root DNS servers to DNS Analyzer. Root name servers field requests for the root namespace domain and then direct further requests to the top-level domains. You can find a listing of root name servers at root-servers.org.

To modify the list of root name servers:

1. Click **File > Settings**, and then click the Root DNS Servers tab.
2. Type the name of the root name server you want to add in the **Add Name Server to List** field, and then click **Add Server**.
3. Click **OK**.

Modifying DNS Query Timeout

Depending on your network and bandwidth limitations, you may need to adjust the DNS query timeout.

To change the DNS query timeout:

1. Click **File > Settings**, and then click the Details tab.
2. Adjust the DNS Query Timeout scroll bar, and then click **OK**.

Deciding Whether to Lookup DNS Server Addresses

DNS servers may not always provide both the name and the address when providing information about other DNS servers. You can force another DNS lookup to retrieve the missing information, or you can accept the provided name or address.

To skip the resolution of names provided without addresses:

1. Click **File > Settings**, and then click the Details tab.
2. Check **Do Not Resolve Suggested Name Servers without Addresses**, and then click **OK**.

Understanding Colors in DNS Analyzer

Understanding the colors used in DNS Analyzer is integral to understanding your graphical DNS analysis. Consult the following table for a list of colors, designations, and definitions.

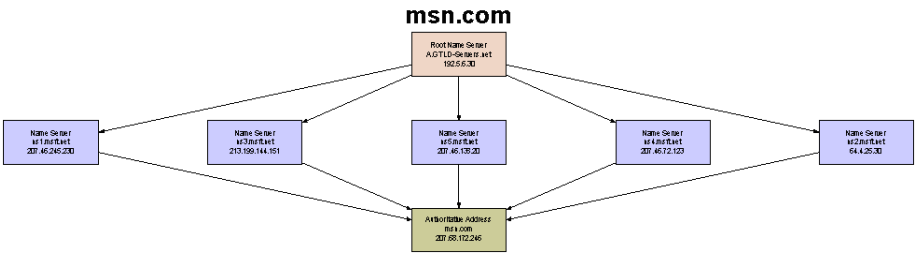
Color	Object	Definition
 Peach	Root Name Server	Represents the Root Name servers used to start the chain of queries. These are the first name servers queried during a DNS Analysis. You may change the Root Name servers in the settings dialog.
 Purple	Name Server	Represents a non-Top Level Domain name server which was referred to us by another name server.
 Yellow	CName	Represents a record returned from a Name Server that indicates that the target Hostname that we are querying for is really an alias for another Hostname.
 Aqua	MX Record	Represents a record returned from a Name Server indicating the hostname of the computer that is designated to receive Email traffic.
 Gold	Global Top Level Domain Servers (GTLD)	Represents Name Servers which are known to be at the top level of the internet naming system (DNS). GTLD Servers are typically used as the Root Name Server for DNS Analysis.
 Green	Authoritative Address	Represents a record returned from a Name Server containing the Authoritative IP Address for the request hostname. Authoritative indicates that the Name Server is the authority for the queried domain.
 Blue	Address	Represents a record returned from a Name Server containing an IP Address for the queried hostname. These record types are returned by Name Servers which have previously queried other Name Servers for the address, and have cached the answer.
 Red	Error	Represents an error during the Analysis. If a Name server fails to respond in the designated timeout period, an error node will be drawn with the description "Timeout". Other errors may include "Name Error", which indicates that the queried hostname does not exist.

Analysis Examples

The following examples illustrate common output for DNS Analyzer and a short description of the output.

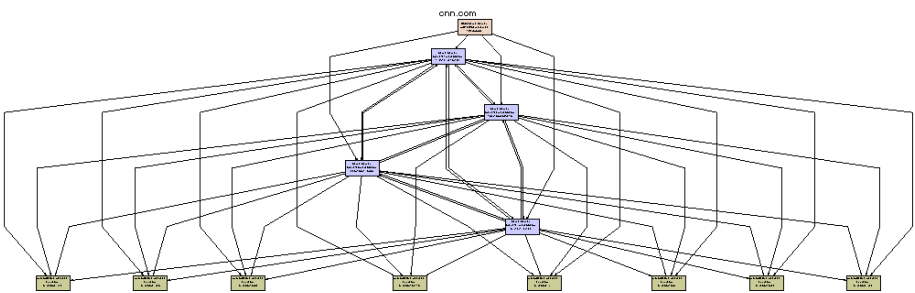
Example 1

The root name server is GTLD. The additional name servers are ns1.msft.net, ns3.msft.net, ns5.msft.net, ns4.msft.net, ns2.msft.net. All name servers point to one authoritative server. Msn.com does not appear to have any DNS issues.



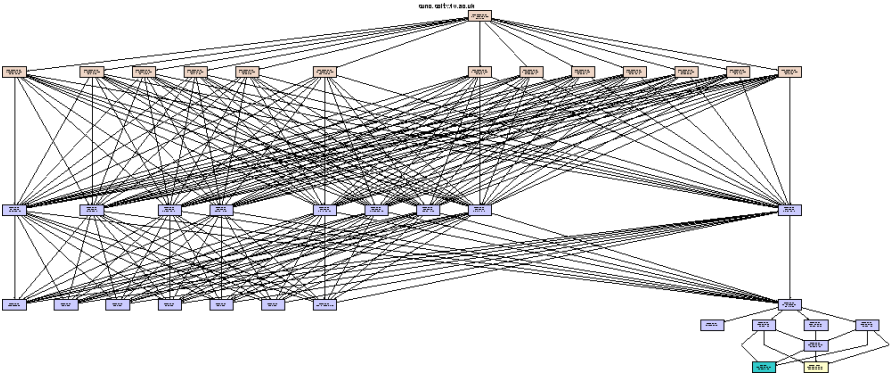
Example 2

The root name server is GTLD. The additional name servers are ns1.msft.net, ns3.msft.net, ns4.msft.net, and ns2.msft.net. All name servers point the authoritative servers. In this example, the DNS is hosted from 8 different servers.



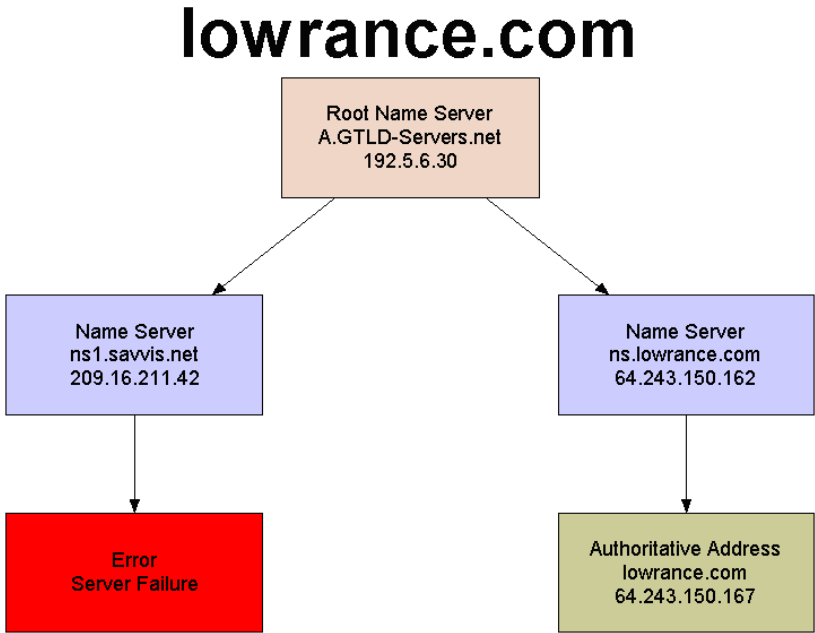
Example 3

There are 14 root name servers listed and 22 name servers. A non-authoritative address is found and an alias. The address is non-authoritative because it comes from the cache of the name server.



Example 4

In this example, there is an error reported from one of the Name Servers. This represents a time out issue.



Setting a Node as the Root and Rescanning

DNS Analyzer allows you to set a discovered node as the root of your DNS analysis, and then rescan and recreate your diagram.

To set a discovered node as your root:

Right-click the node you want as your root, and then click **Set node as Root and ReQuery**.

DNS Audit

The DNS Audit tool helps you locate DNS database errors by scanning a range of IP Addresses and performing reverse DNS lookups for each address. If DNS Audit receives a DNS response for an address, it then attempts a forward DNS lookup to verify that the forward lookup resolves to the originally scanned IP address.

Any errors found during the scan are highlighted. You can also filter the results to show the reverse DNS errors, the IP addresses that did not resolve or forward DNS errors.

Starting an Audit

To begin a DNS audit of an IP range, complete the following procedure.

To start an audit:

1. Type the beginning address of an IP range in the Starting IP Address field.
2. Type the ending address of an IP range in the Ending IP Address field.
3. Click Scan.

Notes:

- If DNS Audit finds forward or reverse DNS records with more than one response, it will list them all.
- DNS Audit uses the DNS and WINS servers already configured on your PC.
- If multiple domain names are assigned to a single IP address or there are multiple IP addresses assigned to a single domain name, DNS Audit will only show them when you run DNS Audit on Windows 2000.

Filtering Results

A number of filters are available, including the ability to limit results to the following:

- Addresses with reverse DNS responses
- Addresses that do not respond to reverse DNS
- Addresses with DNS errors

To filter results:

Click **Filter**, and then select the type of filter you want to apply.

Exporting, Printing, and Copying Calculations

After running an audit, the DNS Audit tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered information:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the displayed data:

Click **Edit**, and then select the information to copy.

Printing Calculations

To print displayed data:

Click **File > Print**, and then select the information you want to print.

Interpreting DNS Audit Results

Consider the following list when interpreting DNS Audit results:

- The first column of the user interface provides the scanned IP address
- The Reverse Resolve column provides the DNS name, if the IP address resolves using reverse DNS
- The Reverse Resolve column contains red text <no reverse DNS response> if a response is not received
- The Forward Resolve column contains nothing if reverse resolution fails (forward resolution is not attempted)
- The Forward Resolve column contains <did not resolve> if there was a failure of the forward resolution attempt
- The Forward Resolve column contains a red IP address if the forward resolution to an IP address is different than the originally scanned IP address

IP Address Management

SolarWinds IP Address Management can be used to actively monitor which IP addresses are in use on your network across multiple subnets. It can also be used to pre-allocate IP addresses.

Scanning a Subnet

You can quickly get started by scanning a network subnet.

To scan a subnet:

1. Click **Subnets > New**.
2. Type a recognizable name for the subnet. This name is used in the navigation tree on the left of the user interface and as the window name in the right pane.

3. Type an IP address in the subnet you want to scan.
4. Type the subnet mask, and then click **OK**.

The following information is reported for each IP address:

- IP address status, for example, Available, Used, or Reserved for future use
- DNS name
- Days since the last response, that is, how long ago was the last usage
- Machine type, provided if the target device supports SNMP
- System Name (if target device supports SNMP)
- Location (if target device supports SNMP)
- Response Time
- Comments (you can add your own comments for each address)

Notes:

- You do not need to leave IP Address Management running. Many customers run the tool only when assigning IP addresses. They scan the subnet to update the current IP address details just before they assign an IP address.
- If you do leave the tool running, IP Address Management has a better chance of picking up every used IP address. If you leave IP Address Management running, any devices that were powered off during the initial scan are retrieved when the device is powered up.

Modifying the Subnet Name, Mask, and Scan Frequency

You can change the name used to identify a subnet within the IP Address Management tool, modify the subnet mask, and change the automatic scan frequency.

To modify subnet details:

1. Click the subnet you want to modify in the left pane.
2. Click **Subnets > Details**.
3. Type an easily recognized name in the **Subnet Name** field.

4. Type the mask you want to use when scanning the subnet. If you change this setting, ensure you rescan the subnet.
5. Adjust the slider to adjust the frequency with which the IP Address Management tool should scan the subnet for IP addresses in use.

Note: You can also specify that this subnet be excluded from the automatic publishing of discovered IP addresses. For more information, see “Automatically Publish Discovered Information in HTML” on page 98.

Filtering

The addresses within each subnet can be filtered to display the following discovered addresses:

All addresses in the subnet

Provides a list of all addresses listed in IP address order.

Used addresses in the subnet

Provides a list of only the IP addresses that have responded to an IP Address Management scan. These IP addresses are currently in use and should not be used when assigning addresses to new devices.

Reserved addresses in the subnet

Displays the IP addresses that you have marked as reserved for future use. You should Reserve an IP address when assigning it to a device. You can reserve an IP address by clicking the IP address and pressing R on the keyboard or by right-clicking on the IP address and selecting **Reserved**.

Available addresses in the subnet

Displays IP addresses that have never responded and are marked available. These addresses can be assigned to new devices.

To filter your discovered subnet list:

Click **View**, and then select the filter you want to use.

- All Addresses
- Used Addresses
- Reserved Addresses
- Available Addresses

Manually Changing the Status of an IP Address

If you know the status of an IP address and it is not properly reflected in your IP address scan, you can manually update the status of the address. You may need to manually update address information for a number of reasons, including the following:

A particular device was down at the time of the scan

A device has been recently decommissioned

To manually change the status of an IP address:

Click **Edit**, and then click the appropriate option.

- Mark Selected Addresses as Reserved
- Mark Selected Addresses as Used
- Mark Selected Addresses as Available

Modifying SNMP Credentials and Enabling SNMP Discovery

You do not need SNMP credentials to use the product to find used or available IP addresses. If you want to discover the type of device using the IP address, specify SNMP credentials. You can create a list of SNMP credentials, including SNMP v3 credentials, to use when querying your subnets.

To add SNMP credentials:

1. Click **File > Network/Scanner Settings**.
2. Check **Enable SNMP Discovery** on the Credentials tab.
3. Click **Add**.
4. Specify the appropriate information on the Add Credentials window and then click **OK**.
5. Arrange the order of the community strings using **Move Up** and **Move Down**. Access is attempted using the community strings in the order displayed. Often used credentials should be higher in the list to speed discovery.
6. Click **OK**.

Modifying ICMP Scan Settings

Initial contact with devices is attempted using ICMP. Depending on your network, you may modify your scanning settings to expand or shorten delays between pings and the timeout.

To modify ICMP ping settings:

1. Click **File > Network/Scanner Settings**.
2. Click the Preferences tab, and then specify the appropriate values in the Scanning grouping of the window.

Notes:

- Number of pings should be set to 2 or more, especially when scanning networks using Cisco routers. If the target IP address is not in the ARP cache of a Cisco router, the router discards the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never arrive at the subnet of the target IP address. In this situation, the Cisco router responds to the second PING.
- On slow connections, consider allowing more time between pings and expanding the timeout period.

3. Click **OK**.

Automatically Publish Discovered Information in HTML

The IP Address Management tool allows you to automatically generate an HTML file that contains the information you select on a timed schedule. For example, you can save this report to your inetpub root directory and provide an automatically refreshing list of used and free IP addresses on your website.

To enable automatic HTML publishing:

1. Click **File > Network/Scanner Settings**.
2. Click the Preferences tab, and then check **Enable auto-publish to web**.
3. Specify the directory to which you want the HTML files saved. The files will use the subnet address as the name of the published HTML file.
4. Specify the publishing interval in the **Auto-publish every** field.

5. Click the appropriate option:
 - Publish all IP Addresses
 - Publish only Reserved, Used, or IP Addresses with comments
6. Click **OK**.

Excluding a Subnet from Automatic Publishing

If you want to exclude a specific subnet from inclusion in the published HTML file, complete the following task.

To exclude a subnet:

1. Click **Subnets > Details**.
2. Check **Exclude this subnet when Auto-Publishing to the Web** on the Subnet Details window, and then click **OK**.

Manually Scanning a Subnet

To manually scan a subnet:

Select the subnet in the left pane, and then click **Subnets > Scan Now**.

Refreshing a Subnet IP Address List

To refresh the list of IP addresses found during a scan:

Select the subnet in the left pane, and then click **Refresh**. Refreshing a subnet does not rescan the subnet. This action only repopulates the table from the database.

Exporting, Printing, and Copying Subnet Scans

After running a subnet scan, the IP Address Management tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered information:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the displayed data:

Click **Edit > Copy**.

Printing Calculations

To print displayed data:

Click **File > Print**, and then select the information you want to print.

Sharing the IP Address Management Database

When you create a new IP Address Management database, you can select a shared location to save the new database. If you select a shared server, any computer in your network with the SolarWinds IP Address Management tool installed can access, view, and update this data.

If you have an existing database that you want to move to a shared server, complete the following task.

Moving a database to a shared location:

1. Copy the IP-Address-Management .IPDB file from the SolarWinds directory where you installed the executables to the shared server where you want the database to reside. The default installation directory is \Program Files\SolarWinds\Engineer's Toolset.
2. Open the SolarWinds IP Address Management tool with which you want to load this database.
3. Click **File > Open IP Address Management Database**, and then browse to and select the IP-Address-Management.IPDB on your shared server.

Note: This database becomes your default until you change to a different database.

Ping Sweep

Ping Sweep can scan a range of IP addresses and show which IP addresses are in use and which ones are currently free. Ping Sweep can also look up the DNS name for each IP address using your configured DNS and WINS servers. Ping Sweep performs a fast ICMP sweep of your IP address range and presents the results in an easy to use worksheet.

To start using Ping Sweep:

1. Specify a beginning IP address for the range to sweep.
2. Specify an ending IP address for the range.
3. Select the type of addresses to return.
 - Responding IP addresses
 - Non-Responding IP addresses
 - All IP addresses
4. Click **Scan**.

Note: If you need to automate collection of IP address status and device type, consider using the IP Address Management. For more information, see “IP Address Management” on page 94.

Exporting, Printing, and Copying Sweeps

After running a sweep, Ping Sweep allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Hint: If the results table is split horizontally between two pages, decreasing the width of the Ping Sweep window will make the table stay on one page.

Ping Sweep Settings

Ping Sweep provides a number of global settings that control default behaviors:

- For what type of IP addresses to scan
 - o Responding - limit the scan to show addresses in use
 - o Non-responsive - limit the scan to show addresses not in use
 - o Display both
- Do you want to perform DNS and WINS lookups
- When and if you want to play sounds

To change default settings:

1. Click **Edit > Settings**.
2. Click the Scanner tab, and then specify the appropriate information.
3. Click **OK**.

Modifying ICMP Ping Settings

At the core of Ping Sweep is the ability to field ICMP communications. Depending on your network topology and speed, you may need to modify the ICMP Ping settings used by Ping Sweep.

To modify the ICMP Ping settings:

1. Click **Edit > Settings**.
2. Click the Network tab, and then specify the appropriate information.

Delay between PINGs

Allows you to modify the time to wait before sending PING communication to each node. You can use this setting to limit traffic generated by Ping Sweep for slower connections.

PING Timeout

Allows you to adjust the amount of time that Ping Sweep waits for a response from a target IP address. If the target does not respond within the timeout and does not respond to any other PING attempts, it is assumed to be down.

PINGs transmitted per node

Allows you to control the number of PING attempts to send each address during a scan. When scanning networks containing Cisco routers, set this number above two (2). If the target IP address is not in the ARP cache of a Cisco router, the router discards the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never arrive at the subnet of the target IP address. In this situation, the Cisco router responds to the second PING.

Packet Time-To-Live

The Packet Time-to-Live is the number of different locations you accept during the route to the IP address. A setting of 32 means your PING test could pass through up to 32 different routers on the way to the remote IP address before being thrown away by the network. Normally, you set this to 32 hops.

3. Click **OK**.

Publishing to the Web

Ping Sweep results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Chapter 5

Network Discovery Tools

The Network Discovery tools, some of the first tools developed by SolarWinds, help you discover a broad range of network issues. You can successfully discover something as large as the entire enterprise of nodes and networks, using Network Sonar, and troubleshooting something as specific as a reverse DNS error, using DNS Audit. The network discovery engine embedded in IP Network Browser and Network Sonar is one to the fastest, most extensive discovery engines on the market.

- “DNS Audit” on page 105
- “IP Address Management” on page 108
- “IP Network Browser” on page 115
- “MAC Address Discovery” on page 128
- “Network Sonar” on page 130
- “Ping Sweep” on page 140
- “Port Scanner” on page 143
- “SNMP Sweep” on page 146
- “Subnet List” on page 149
- “Switch Port Mapper” on page 152

DNS Audit

The DNS Audit tool helps you locate DNS database errors by scanning a range of IP Addresses and performing reverse DNS lookups for each address. If DNS Audit receives a DNS response for an address, it then attempts a forward DNS lookup to verify that the forward lookup resolves to the originally scanned IP address.

Any errors found during the scan are highlighted. You can also filter the results to show the reverse DNS errors, the IP addresses that did not resolve or forward DNS errors.

Starting an Audit

To begin a DNS audit of an IP range, complete the following procedure.

To start an audit:

1. Type the beginning address of an IP range in the Starting IP Address field.
2. Type the ending address of an IP range in the Ending IP Address field.
3. Click Scan.

Notes:

- If DNS Audit finds forward or reverse DNS records with more than one response, it will list them all.
- DNS Audit uses the DNS and WINS servers already configured on your PC.
- If multiple domain names are assigned to a single IP address or there are multiple IP addresses assigned to a single domain name, DNS Audit will only show them when you run DNS Audit on Windows 2000.

Filtering Results

A number of filters are available, including the ability to limit results to the following:

- Addresses with reverse DNS responses
- Addresses that do not respond to reverse DNS
- Addresses with DNS errors

To filter results:

Click **Filter**, and then select the type of filter you want to apply.

Exporting, Printing, and Copying Calculations

After running an audit, the DNS Audit tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered information:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the displayed data:

Click **Edit**, and then select the information to copy.

Printing Calculations

To print displayed data:

Click **File > Print**, and then select the information you want to print.

Interpreting DNS Audit Results

Consider the following list when interpreting DNS Audit results:

- The first column of the user interface provides the scanned IP address
- The Reverse Resolve column provides the DNS name, if the IP address resolves using reverse DNS
- The Reverse Resolve column contains red text <no reverse DNS response> if a response is not received
- The Forward Resolve column contains nothing if reverse resolution fails (forward resolution is not attempted)
- The Forward Resolve column contains <did not resolve> if there was a failure of the forward resolution attempt
- The Forward Resolve column contains a red IP address if the forward resolution to an IP address is different than the originally scanned IP address

IP Address Management

SolarWinds IP Address Management can be used to actively monitor which IP addresses are in use on your network across multiple subnets. It can also be used to pre-allocate IP addresses.

Scanning a Subnet

You can quickly get started by scanning a network subnet.

To scan a subnet:

1. Click **Subnets > New**.
2. Type a recognizable name for the subnet. This name is used in the navigation tree on the left of the user interface and as the window name in the right pane.
3. Type an IP address in the subnet you want to scan.
4. Type the subnet mask, and then click **OK**.

The following information is reported for each IP address:

- IP address status, for example, Available, Used, or Reserved for future use
- DNS name
- Days since the last response, that is, how long ago was the last usage
- Machine type, provided if the target device supports SNMP
- System Name (if target device supports SNMP)
- Location (if target device supports SNMP)
- Response Time
- Comments (you can add you own comments for each address)

Notes:

- You do not need to leave IP Address Management running. Many customers run the tool only when assigning IP addresses. They scan the subnet to update the current IP address details just before they assign an IP address.
- If you do leave the tool running, IP Address Management has a better chance of picking up every used IP address. If you leave IP Address Management running, any devices that were powered off during the initial scan are retrieved when the device is powered up.

Modifying the Subnet Name, Mask, and Scan Frequency

You can change the name used to identify a subnet within the IP Address Management tool, modify the subnet mask, and change the automatic scan frequency.

To modify subnet details:

1. Click the subnet you want to modify in the left pane.
2. Click **Subnets > Details**.
3. Type an easily recognized name in the **Subnet Name** field.
4. Type the mask you want to use when scanning the subnet. If you change this setting, ensure you rescan the subnet.
5. Adjust the slider to adjust the frequency with which the IP Address Management tool should scan the subnet for IP addresses in use.

Note: You can also specify that this subnet be excluded from the automatic publishing of discovered IP addresses. For more information, see “Automatically Publish Discovered Information in HTML” on page 98.

Filtering

The addresses within each subnet can be filtered to display the following discovered addresses:

All addresses in the subnet

Provides a list of all addresses listed in IP address order.

Used addresses in the subnet

Provides a list of only the IP addresses that have responded to an IP Address Management scan. These IP addresses are currently in use and should not be used when assigning addresses to new devices.

Reserved addresses in the subnet

Displays the IP addresses that you have marked as reserved for future use. You should Reserve an IP address when assigning it to a device. You can reserve an IP address by clicking the IP address and pressing R on the keyboard or by right-clicking on the IP address and selecting **Reserved**.

Available addresses in the subnet

Displays IP addresses that have never responded and are marked available. These addresses can be assigned to new devices.

To filter your discovered subnet list:

Click **View**, and then select the filter you want to use.

- All Addresses
- Used Addresses
- Reserved Addresses
- Available Addresses

Manually Changing the Status of an IP Address

If you know the status of an IP address and it is not properly reflected in your IP address scan, you can manually update the status of the address. You may need to manually update address information for a number of reasons, including the following:

- A particular device was down at the time of the scan
- A device has been recently decommissioned

To manually change the status of an IP address:

Click **Edit**, and then click the appropriate option.

- Mark Selected Addresses as Reserved
- Mark Selected Addresses as Used
- Mark Selected Addresses as Available

Modifying SNMP Credentials and Enabling SNMP Discovery

You do not need SNMP credentials to use the product to find used or available IP addresses. If you want to discover the type of device using the IP address, specify SNMP credentials. You can create a list of SNMP credentials, including SNMP v3 credentials, to use when querying your subnets.

To add SNMP credentials:

1. Click **File > Network/Scanner Settings**.
2. Check **Enable SNMP Discovery** on the Credentials tab.
3. Click **Add**.

4. Specify the appropriate information on the Add Credentials window and then click **OK**.
5. Arrange the order of the community strings using **Move Up** and **Move Down**. Access is attempted using the community strings in the order displayed. Often used credentials should be higher in the list to speed discovery.
6. Click **OK**.

Modifying ICMP Scan Settings

Initial contact with devices is attempted using ICMP. Depending on your network, you may modify your scanning settings to expand or shorten delays between pings and the timeout.

To modify ICMP ping settings:

1. Click **File > Network/Scanner Settings**.
2. Click the Preferences tab, and then specify the appropriate values in the Scanning grouping of the window.

Notes:

- Number of pings should be set to 2 or more, especially when scanning networks using Cisco routers. If the target IP address is not in the ARP cache of a Cisco router, the router discards the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never arrive at the subnet of the target IP address. In this situation, the Cisco router responds to the second PING.
- On slow connections, consider allowing more time between pings and expanding the timeout period.

3. Click **OK**.

Automatically Publish Discovered Information in HTML

The IP Address Management tool allows you to automatically generate an HTML file that contains the information you select on a timed schedule. For example, you can save this report to your inetpub root directory and provide an automatically refreshing list of used and free IP addresses on your website.

To enable automatic HTML publishing:

1. Click **File > Network/Scanner Settings**.
2. Click the Preferences tab, and then check **Enable auto-publish to web**.

3. Specify the directory to which you want the HTML files saved. The files will use the subnet address as the name of the published HTML file.
4. Specify the publishing interval in the **Auto-publish every** field.
5. Click the appropriate option:
 - Publish all IP Addresses
 - Publish only Reserved, Used, or IP Addresses with comments
6. Click **OK**.

Excluding a Subnet from Automatic Publishing

If you want to exclude a specific subnet from inclusion in the published HTML file, complete the following task.

To exclude a subnet:

1. Click **Subnets > Details**.
2. Check **Exclude this subnet when Auto-Publishing to the Web** on the Subnet Details window, and then click **OK**.

Manually Scanning a Subnet

To manually scan a subnet:

Select the subnet in the left pane, and then click **Subnets > Scan Now**.

Refreshing a Subnet IP Address List

To refresh the list of IP addresses found during a scan:

Select the subnet in the left pane, and then click **Refresh**. Refreshing a subnet does not rescan the subnet. This action only repopulates the table from the database.

Exporting, Printing, and Copying Calculations

After running a subnet scan, the IP Address Management tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered information:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the displayed data:

Click **Edit > Copy**.

Printing Calculations

To print displayed data:

Click **File > Print**, and then select the information you want to print.

Sharing the IP Address Management Database

When you create a new IP Address Management database, you can select a shared location to save the new database. If you select a shared server, any computer in your network with the SolarWinds IP Address Management tool installed can access, view, and update this data.

If you have an existing database that you want to move to a shared server, complete the following task.

Moving a database to a shared location:

1. Copy the IP-Address-Management .IPDB file from the SolarWinds directory where you installed the executables to the shared server where you want the database to reside. The default installation directory is \Program Files\SolarWinds\Engineer's Toolset.
2. Open the SolarWinds IP Address Management tool with which you want to load this database.
3. Click **File > Open IP Address Management Database**, and then browse to and select the IP-Address-Management.IPDB on your shared server.

Note: This database becomes your default until you change to a different database.

IP Network Browser

SolarWinds IP Network Browser is an interactive network discovery tool. IP Network Browser can scan a subnet and show the details about the devices on the subnet. Each IP address is sent a PING. For each responding address, IP Network Browser attempts to gather more information. It does this using SNMP (Simple Network Management Protocol). An SNMP agent must be active on the remote devices in order for IP Network Browser to gather details about the device.

The SolarWinds IP Network Browser is not specific to Cisco devices. It can discover any device with an IP address. If the device has an SNMP agent and the correct SNMP community string is included in the IP Network Browser Settings, IP Network Browser discovers a great deal about the device.

IP Network Browser inherently understands hundreds of types of devices and will discover different details about each. For example: User Accounts, Shares, and Running Services are discovered about Windows workstations and servers. For Cisco routers, the tool discovers IOS levels, the cards in each slot, flash memory details, interface details, frame relay DLCIs and their statuses, among other information.

You do not need to specify the SNMP community string for each device. Simply enter a list of community strings used on your network. IP Network Browser will determine the correct one for each device. For more information about entering SNMP community strings, see “Modifying IP Network Browser Settings” on page 52.

Getting Started

The first time you run IP Network Browser, a configuration wizard guides you through setting up the tool. Before completing the wizard, ensure you have the read or read-write community string and that an access list on your router is not blocking SNMP access.

To complete the configuration wizard:

1. Review the welcome window, and then click **Next**.
2. Provide a list of SNMP community strings you want to use to access devices on your network. Ensure you arrange the list so the most common SNMP community strings are listed first. Click **Next**.
3. Click the appropriate connection type, and then click **Next**.
4. Review the final window, and then click **Finished** to launch the tool.

To scan a subnet:

1. Type an IP address in the **Subnet Address** field.
2. Type the subnet mask in the **Subnet Mask** field, and then click **Scan Subnet**.

Note: You do not have to enter the exact network address. IP Network Browser is intelligent, and will calculate the correct subnet address based on the Subnet Mask. For example: if you enter 10.0.23.100 as the Subnet Address and 255.255.255.192 as the Subnet Mask, IP Network Browser will calculate the correct subnet. 10.0.23.64/255.255.255.192. For this example, IP Network Browser will scan from 10.0.23.65 to 10.0.23.126.

To scan a single device:

1. Type a hostname or IP address in the **Hostname or IP Address** field.
2. Click **Scan Device**.

Note: **Scan a Single Device** and **Scan an IP Address Range** are not available in the Standard Edition.

To scan an IP range:

1. Type the beginning IP address in the **Beginning IP Address** field.
2. Type the final IP address of the range in the **Ending IP Address** field, and then click **Scan Address Range**.

Notes:

- When scanning a range of IP addresses, there is a good chance you may scan a network or broadcast address. When you scan a broadcast address, any device (or all devices) on the subnet may respond. The discovery information may be a mix from many different devices.
- The **Scan a Single Device** and **Scan an IP Address Range** options are not available in the Standard Edition.

IP Network Browser Menus

File Menu

New Subnet Window

Displays another IP Network Browser window.

Export Wizard

Exports the results from IP Network Browser.

Print Preview

Displays a preview of exactly what the print out would look like.

Print

Prints the current results.

IP Network Browser Settings

Displays the IP Network Browser Settings dialog box.

Configuration Wizard

Displays the Configuration Wizard that was run the first time you launched IP Network Browser.

Exit

Closes the IP Network Browser window.

Edit Menu

Copy Selected

Copies the highlighted item to the Windows clipboard.

Copy Selected Tree

Copies the highlighted item and ALL children in the tree under that item to the Windows clipboard.

Nodes Menu

Expand and Discover details for selected Node

Expands all discovery trees for the selected node. To expand all trees or selected trees for ALL nodes, use the "Expand and Discover details for All Nodes..." menu selection from the Discovery Menu.

Note: If you see a message stating that the ActiveX component can't create object, a component of your SolarWinds Toolset has been deleted or moved. Reinstall the toolset. Your existing license will still work and you will NOT need to re-register.

Collapse all Nodes

This selection collapses all expanded trees.

Refresh Node Details

Deletes all discovered information for the selected Node. Expand the discovery trees to rediscover the details about the node.

Delete Selected Node

Removes the selected node from the list. To remove all nodes of a specific type, use the

Tools Menu

You can customize the list of Tools by editing the Tools.Menu file. This file and other customization files are located in the IP-Network-Browser directory one level below the SolarWinds Toolset installation directory. For more information, see "Customizing the Tools Menus" on page 56.

Ping

PINGS the selected node or IP address.

Web Browser

Opens the default web browser with the selected node or IP address as the target URL.

View Config File

Downloads the configuration from a Cisco router or Switch. This selection only works when the selected node is a Cisco device.

Telnet

Telnets to the selected node or IP address. IP Network Browser references a program named `telnet.exe`. Windows searches the directories defined by the PATH environment variable for the first occurrence of `telnet.exe`. If you would like to launch a different telnet program, you have two options:

- Edit the PATH environment variable and enter the location before `C:\Windows\System32`. You may also need to rename your telnet program to `telnet.exe`.
- Edit the `tools.menu` file. For more information, see “Customizing the Tools Menus” on page 56.

Traceroute

Traces the route to the selected node or IP address.

MIBs Menu

The list of MIB (Management Information Base) entries is dependant on the type of node currently selected. For example, a different set of MIBs will be listed on the MIBs menu for Cisco devices than when selecting a Windows Server. A working knowledge of SNMP and MIBs is needed in order to customize the MIBs menus. For more information, see “Customizing the MIBs Menu” on page 57.

Discovery Menu**Stop Discovery**

Stops all scanning and detail discovery in the current window.

Rescan Subnet/Range

Rescans the current subnet or IP address range. The devices already discovered are not deleted. This simply adds any newly discovered devices to the current list.

Expand and Discover details for selected Node

Expands all discovery trees for the selected node.

Expand and Discover details for all Nodes

Allows you to select which groups of discovered information you wish to display. Only the selected items will be expanded. This function is particularly useful in discovering specific items across many nodes.

Filter node list

This selection allows you to filter for specific types of nodes and display only those selected. You can remove all nodes except certain types, or you can select which types of devices to remove from the discovery window.

Collapse all Nodes

This selection collapses all expanded trees.

Clear List

Deletes all nodes from the results window.

Subnet Menu

Scan Selected Subnet

Opens a new IP Network Browser window to scan the selected subnet. This selection only works when a subnet is selected from the results window.

View Menu

Toolbar

Shows or hides the toolbar at the top of the window.

Status Bar

Shows or hides the status bar at the bottom of the window.

Printing Discovery Results

You must first discover node details and expand the corresponding tree item to include details in the printed version of the discovery. For example, if you have discovered a Windows Server and would like the user accounts included in the printout, you must first expand the accounts tree so the account details will be discovered.

To print discover results:

1. Click **File > Print**.
2. Check the nodes you want to printed, and then click **Next**.

3. Check the discovery groups you would like included in the report, and then click **Next**. Discovery groups include accounts, routes, shares, and other information discovered through SNMP. Your discovery results may not include all the groups. Results depend on the discovered device type and what it supports.
4. Specify whether to include the SNMP community strings in the printed version, and then click **Print**.

Modifying IP Network Browser Settings

A number of settings can be adjusted to ensure IP Network Browser locates as many devices as possible within your network.

To change product settings:

1. Click **File > IP Network Browser Settings**.
2. ***If you want to modify the community strings tried when contacting devices***, click the Community Strings tab.
 - To add a community string, type the community string you want to add in the New Community String field, and then click **Add**.
 - To remove a community string, click the community string, and then click **Delete**.
 - To change the order in which community strings are attempted, select the community string and then click the up or down arrow.
3. ***If you want to modify the number of PINGs sent during the discovery mode or change the delay between Pings***, click the Discovery tab. ICMP PINGs are used to initially discover a responding node. If you are connecting over dialup or another slow connection, the wait and delay can be increased for better discovery and to limit traffic generated by the tool.

Warning: The number of PINGs per node should always be set to 2 or more, especially when scanning networks using Cisco routers. If the target IP address is not in the ARP cache of the Cisco router, the router will throw away the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never make it to the subnet of the target IP address. In this situation, the second PING will be the one the target IP address responds to.

4. If you want to modify the wait period before timing out change the PING time to live for a packet, click the ICMP tab.

- The PING timeout is the number of milliseconds to wait for a reply before assuming that the target IP address is not responding.
- The packet time-to-live is the number of hops you will except while navigating to the specified IP address. With a setting of 32, your PING test could pass through up to 32 different routers on its way to the remote IP address before being thrown away by the network. Normally you would set this to 32 hops.

5. If you want to modify the community strings tried when contacting devices, click the SNMP tab.

- The packet timeout designates the number of milliseconds to wait for an SNMP reply before assuming the packet was lost and retrying. You can set this around 600 milliseconds, the internal SNMP logic of the tool automatically adjust when it notices dropped packets.
- Query attempts specifies how many times to retry an SNMP query before giving up. Set this to at least 2, to ensure one retry.

IP Network Browser Configuration Wizard

The configuration wizard helps you setup some basic configurations for the tool.

To complete the configuration wizard:

1. Review the welcome window, and then click **Next**.
2. Provide a list of SNMP community strings you want to use to access devices on your network. Ensure you arrange the list so the most common SNMP community strings are listed first. Click **Next**.
3. Click the appropriate connection type, and then click **Next**. If you select dialup, IP Network Browser adjusts ICMP timeouts and wait periods accordingly.
4. Review the final window, and then click **Finished** to launch the tool.

Saving the Discovery in HTML

The Engineer's Edition of IP Network Browser can save the current discovered information as an HTML page that can be published to your web server. You must first discover node details and expand the corresponding tree items to include details in the HTML version of the discovery. For example, if you have discovered a Windows Server and would like the user accounts included in the saved file, you must first expand the accounts tree so the account details will be discovered.

To save a discovery in HTML:

1. Click **File > Publish to Web**.
2. Check the nodes you want to include, and then click **Next**.
3. Check the discovery groups you would like included in the report, and then click **Next**. Discovery groups include accounts, routes, shares, and other information discovered through SNMP. Your discovery results may not include all the groups. Results depend on the discovered device type and what it supports.
4. Specify whether to include the SNMP community strings, and then click **Publish**.

When viewing the HTML in your browser, a blue plus (+) indicates a selection can be expanded to view additional detail. If a node does not have additional detail, ensure it was fully expanded and discovered prior to saving to HTML. The saved page does not perform discovery, it displays what was previously discovered.

Exporting the Discovery as a Text File

You can also export discovered results to a text file. You must first discover node details and expand the corresponding tree items to include details in the text version of the discovery. For example, if you have discovered a Windows Server and would like the user accounts included in the text file, you must first expand the accounts tree so the account details will be discovered.

To save a discovery in HTML:

1. Click **File > Export Wizard**.
2. Check the nodes you want to include, and then click **Next**.

3. Check the discovery groups you would like included in the report, and then click **Next**. Discovery groups include accounts, routes, shares, and other information discovered through SNMP. Your discovery results may not include all the groups. Results depend on the discovered device type and what it supports.
4. Specify whether to include the SNMP community strings, and then click **Export**.

Network Sonar can discover your network and create a Microsoft Access database. For more information, see “Network Sonar” on page 130.

IP Network Browser Command Line Operation

It is possible to launch the IP Network Browser directly from the command line. You must add the path to IP Network Browser in the PATH system variable or specify the full path when running the program from the command line.

Syntax

```
IP-Network-Browser HostIP [subnet/mask | startip-endip]
```

Where:

Hostip

IP address of a single machine

subnet/mask

Subnet address and mask separated by a "/"

startip-endip

An IP address range separated by a "-"

Examples

- Scan or discover a single device:
IP-Network-Browser 10.23.1.1
- Scan or discover an entire subnet:
IP-Network-Browser 10.23.1.1/255.255.255.0
- Scan or discover a range of IP addresses:
IP-Network-Browser 10.23.1.1-10.23.50.255

Customizing the Tools Menus

You can add new tools to the Tools menu by editing the `Tools.Menu` file. This file and other customizable files are located in the `IP-Network-Browser` directory in the SolarWinds Toolset installation directory.

The `Tools.Menu` file is a text file and can be edited from Notepad. The default `Tools.Menu` file is listed below.

```
#
# Tools Menu for IP Network Browser
#
#
#
# Macros that can be used with any command are:
#
# ${IP} IP address of the node
# ${Target} Node Name
# ${SysObjectID} Unique System OID for the node
# ${Community} SNMP community string for the node
#
#
&Telnet ... : telnet.exe ${IP}

Trace&Route ... : traceroute.exe ${IP}
```

To changing the Telnet command:

Replace the current tool with the following entry: `&Telnet ... :`
`C:\Program Files\MyFavoriteTools\mytelnet.exe ${IP}`

To add a command called SSL:

Add the following entry on an empty line: `&ssl ... : ssl.exe ${IP}`
`${Community}`

To add menu-dividing lines:

Enter a single hyphen (-) on a line alone.

Customizing the MIBs Menu

You can add new MIB references to the MIBs menu by editing the .MibsMenu files. These files and other customizable files are located in the IP-Network-Browser directory in the SolarWinds Toolset installation directory.

The *.MibsMenu files are text files that can be edited using Notepad. The filenames of the MibsMenu files are simply the vendor or machine specific sysObjectID followed by .MibsMenu. The sysObjectID can be discovered for a specific device by using IP Network Browser to discover it, and then expanding the **System MIB** section of the tree. You can also use SolarWinds MIB Browser to find or discover new MIB references.

```
# MIBs Menu for IP Network Browser

#

# Generic SNMP Devices

#

# Syntax for each line is ...

#

# Menu item : MIB table or tree

# &MAC Addresses of Interfaces ... : ifPhysAddress

&Running Software ... : hrSWRunTable

Installed &Software ... : hrSWInstalledTable

-

&IP Statistics ... : ipInReceives & Next 16

&ICMP Statistics ... : ICMP

&SNMP Statistics ... : SNMP

&TCP Statistics ... : tcpRtoAlgorithm & Next 11 & tcpInErrs &
tcpOutRsts

&UDP Statistics ... : udpInDatagrams & Next 3

-

RMON &Ethernet Statistics ... : etherStatsTable

RMON &Token Ring Statistics ... : tokenRingMLStatsTable
```

-

&Frame Relay Statistics ... : frCircuitTable

&BGP Peer Table ... : bgpPeerTable

Walking a Network from One Subnet to Another

If you right-click a selected subnet, you can zoom to the next subnet and scan it. IP Network Browser opens a new window and begins scanning the subnet in the new window.

IP Network Browser Frequently Asked Questions

How do I create a Community Sting?

For Cisco routers there is a brief overview on the Cisco web page (www.cisco.com). If you have a different router, please refer to that manufacturer's home page for specific instructions on how to configure and change Community Strings.

Is IP Network Browser specific to Cisco devices only, or can it be used to discover details about any device?

The SolarWinds IP Network Browser is not specific to Cisco devices. It can discover any device with an IP address. If the device has an SNMP agent and the correct SNMP community string is included in the IP Network Browser Settings, IP Network Browser discovers a great deal more about the device.

IP Network Browser inherently understands hundreds of types of devices and will discover different details about each. For example: User Accounts, Shares, and Running Services are discovered about Windows workstations and servers. For Cisco routers, the tool discovers IOS levels, the cards in each slot, flash memory details, interface details, frame relay DLCIs and their statuses, among other information.

When expanding the results I get a message saying: "ActiveX component can't create object"

This occurs if a component of your SolarWinds tools has been deleted or moved. This is easily resolved by re-installing the toolset. Your existing license will still work and you will NOT need to re-register.

I cannot seem to download a Cisco configuration file. What am I doing wrong?

- Are you using the read-write community string?
Click **Router > Verify Community String** and ensure you have the read-write community string.
- Ensure an access control list (ACL) on the router is not blocking SNMP queries.

For more information, see “Troubleshooting Config Viewer” on page 44.

MAC Address Discovery

The MAC Address Discovery tool can discover the MAC addresses, hardware manufacturer, IP address, and hostnames of the devices connected to your local.

If you want to discover the MAC addresses of devices connected to remote subnets, either run the tool on a laptop you can plug into the remote subnets or consider using Network Sonar and the Switch Port Mapper. For more information, see “Network Sonar” on page 130 and “Switch Port Mapper” on page 152.

To start your discovery:

1. Select the local subnet from the Local Subnet list. If your computer is attached to one subnet, only one choice is provided in the list.
2. Click **Discover MAC Addresses**.

Searching Results Data

You can search for a value in the results set returned by the MAC Address Discovery tool.

1. Click Edit > Find.
2. Specify the text string you want to find.
3. Specify the appropriate search option:
 - From the top
 - From the current position down
 - From the current position up
4. Click **Find Next**.

Exporting, Printing, and Copying Discovered Results

After running a discovery, the MAC Address Discovery tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Discovery Results

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Discovery Results

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire result set to the clipboard or a selected IP address.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Modifying MAC Address Discovery Settings

You can configure the type of data provided in the discovery settings by adding data columns and specifying how to format MAC addresses. You can also adjust the ICMP Ping settings to reflect your network speed.

To adjust MAC Address Discovery settings:

1. Click **File > Settings**.
2. Click the Columns tab, and then select the columns you want to display in your discover results. Use up and down arrows to change the left to right order of the selected columns.
3. Click the MAC Addresses tab, and then specify the notation you want to use. Dotted notation offers an easier to read value separated by periods (.).
4. Click the Network tab, and then specify the ICMP values you want to use when pinging devices in the local subnet. Fast connections can use shorter timeout and delay settings.

Network Sonar

SolarWinds Network Sonar is a high performance network discovery tool, allowing you to build a database of the structure and devices on a TCP/IP network.

Completing the Discover Wizard

The Network Discovery Wizard walks you through discovering your network.

To start the wizard:

1. Click **File > Network Discovery Wizard**.
2. *If you are creating a new database*, click **Create a New Discovery Database**, and then complete the following steps.
 - a. Type a name and then select the type of database you want to create in the **Save as type** field:
 - Sonar Database
 - Access Database
 - b. Click **Save**.
3. *If you want to use a previously created database*, click **Open an Existing Database**, select your database, and then click **OK**.
4. Click **Next**.
5. Type your SNMP community strings into the **Add** field, and then click **Add**.

Note: The more community strings you add, the longer Network Sonar may take to discover your network. Ensure the most frequently used community strings appear first in the list. Use the arrows to arrange the order of the strings.
6. Click **Next**.
7. Click **Specify a Seed Router and Discover Network Topology**. A seed router is any router in your network. A server, switch, or workstation that supports SNMP can also be used. Though for best results, use a core router.
8. Type an IP address or hostname in the Hostname or IP address, and then click **Add**.

9. Click **Discover Network Topology**.

Note: Discovering the network topology may take a few minutes. If a small number of subnets are missing from the list, Network Sonar can pick them up during the network discovery. If entire networks are missing, rerun the topology discovery using a seed router in the missing network. Click **Previous** to get back to the Discover subnets from a seed router window.

10. Click **OK** on the Network Topology window, and then click **Next**.

11. Check the subnets you want to include, and then click **Next**.

Note: If you are planning on discovering a portion of the Internet, such as a national or local ISP network, add the networks or subnets manually and set limits on the discovery. If you do specify desired subnets, Network Sonar may attempt to discover the entire Internet.

12. Click **Start Discovery**. The faster you set the discovery slider, the more traffic generated. If you are discovering a network across a dial-up line or low bandwidth circuits, increasing the discovery speed will also increase the chances of congestion and dropped packets.

You can stop the discovery at any time. The next time you start it, it will simply begin where it left off.

Modifying Network Sonar Discovery Preferences

A number of preferences can be changed to better discover and scan your network.

To modify Network Sonar preferences:

1. Click **Discovery > Preferences**.
2. Click **Discovery Performance**, and then adjust the following settings:

Network Connection

This slider will adjust the speed of the network discovery. The discovery speed can be set from slow dial-up lines up to a high speed LAN. Network Sonar will also automatically adjust the speed of the discovery if needed.

Network Congestion

This slider will adjust the default timeouts and retries for Network Sonar. Most of the time, set this to **Normal**. Network Sonar will also automatically adapt the network discovery if it begins to encounter problems or congestion in part of the network.

3. Click **Community Strings**, and then add and adjust community strings.

Note: The more community strings you add, the potentially longer the network discovery will take. Arrange the most commonly used community strings at the top of the list.

4. Click Automatic Subnet Selection, and then adjust the appropriate setting:

During a network discovery, Network Sonar may find subnets that it does not already have in its database. Network Sonar will always add the new subnet to the Discovery Database, but it will include it in the active discovery based on these settings.

Exclude the new subnet from the network discovery

Select "Exclude" if you do not want any new subnets found during the discovery to be automatically scanned as part of the discovery. Network Sonar will still add the subnet to the database, just not scan it. You can always select the subnet later and resume the discovery to scan it.

Use this option if you are scanning part of the Internet (an ISP for example). You do not want Network Sonar to automatically include any new subnets in the active discovery. If it did, it would attempt to discover the entire Internet.

Include the new subnet in the network discovery

Select "Include" if you would like new subnets found during the discovery to be automatically scanned as part of the discovery. This is useful when scanning a corporate Intranet to ensure Network Sonar scans every subnet.

Include the Subnet if it is smaller than

Set the size of the subnets that should be automatically included. Adjust the slider to change subnet mask size. All subnets smaller than this setting will be included in the active discovery.

5. Click **Ping Sweeps**, and then adjust the appropriate settings:

Delay between PINGs

The time in milliseconds to wait before sending PINGs to each node. This setting is used to arbitrarily slow down the network discovery. This is important on dial-up lines or to limit the amount of traffic generated by Network Sonar. Normally, you would not adjust this slider. Network Sonar will make any adjustments when needed.

PINGs transmitted per node

This setting is used to control how many PINGs should be sent to each IP address during scanning. Normally, this should be set to 2 or more.

This is very important when scanning networks using Cisco routers. If the target IP address is not in a Cisco router's ARP cache, then the router will throw away the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never even make it to the subnet of the target IP address. In this situation, the second PING will be the one the target IP address responds to.

6. Click **ICMP**, and then adjust the appropriate settings:

PING Timeout

This setting is the number of milliseconds Network Sonar should wait for a reply before assuming that the target IP address is not responding.

Packet Time-To-Live

The Packet Time-To-Live is the number of "hops" you will expect in trip to the specified IP address. With a setting of 32, your PING test could pass through up to 32 different routers on the way to the remote IP address before being thrown away by the network. Normally you would set this to 32 hops.

7. Click **SNMP**, and then adjust the appropriate settings:

Packet Timeout

This setting is the number of milliseconds Network Sonar should wait for an SNMP reply before assuming the packet was lost and trying again. This setting should normally be set around 600 milliseconds.

Query Attempts

This setting is the number of times Network Sonar should retry an SNMP query before giving up. This should normally be set to 2.

Network Sonar Menus

File Menu

Because Network Sonar continuously saves the information it discovers to the current discovery database, there is no save option.

Network Discovery Wizard

Displays the Network Discovery Wizard. The Network Discovery Wizard will walk you through setting up a network discovery.

New Database

Creates a new Sonar Discovery Database. The new database will be empty.

Open Database

Opens a previous Sonar Discovery Database.

Close Database

Closes the current Discovery Database.

Clear Database

Clears the current Discovery Database. All Networks, Subnets, Nodes, etc are removed from the database. Any discovery settings or tuning will not be removed. Only the information discovered about a network will be cleared.

Export Wizard

Displays the Export Wizard that dialog box. For more details see Exporting from Network Sonar.

Recent Discovery Database list

The list of recently used databases will be displayed on the "File" menu. Select one of the databases to open it.

Exit

Stops the current discovery (if active) and closes the Network Sonar windows.

Edit Menu

The Edit menu is only visible when a Chart Window is active. Click **Analysis > Charts** to display a Chart Window.

Copy Metafile to Clipboard

Copies the current chart to the Windows clipboard as a Windows metafile. Windows metafiles are a special graphics format that can be scaled without pixilation.

Copy Bitmap to Clipboard

Copies the current chart to the Windows clipboard as a Windows bitmap.

This copies a bitmap of the current chart at exactly the same size of the current chart. You can make the window large or smaller before you copy the bitmap to adjust the bitmap's size.

Chart Menu

The "Chart" menu is only visible when a Chart Window is active. Select "Charts..." from the "Analysis" menu to display a Chart Window.

Style Menu

Select from "Pie Chart" or "Bar Chart" for the current chart.

Font Size Menu

Select the size of the text on the current chart.

Customize Chart

Launches the Chart Customization dialog box.

Discovery Menu

Discover Network Topology from Seed Routers

Displays the Network Topology Discovery dialog box.

Select Subnets to include in Discovery

Displays the subnet selection window.

Start Network Discovery

Starts or resumes a network discovery.

Devices Discovered

Displays the current list of devices that have been discovered. You can watch this list during a network discovery to see what types of devices are being discovered.

Target Devices

Displays the Target Devices window. The Target Devices window allows you to tell the Discovery Engine to only look for certain types of devices.

Preferences

Displays the Discovery Preferences dialog box. This dialog box allows you to customize and tune the network discovery.

Subnets Menu

The Subnets menu is only visible when the Select Subnets Window is active. To activate the Subnets menu, click **Discover > Select Subnets to Include in the Discovery**.

Add Subnet

Allows you to manually add a subnet to the subnet list.

Select Subnets based on Mask

Selects subnets to include in the discovery based on their subnet mask.

Select Subnets based on Address

Selects subnets to include in the discovery based on their address.

Unselect All Subnets

Unselects all subnets for inclusion in the network discovery.

Subnet Auto-Selection Preferences

Displays the Subnet Auto-Selection settings from the Preferences dialog box.

Analysis Menu

Routers

Displays the list of nodes on the network configured as routers. A device is considered a router if it is configured for IP forwarding or routing. PCs or servers may appear in this list if they are configured for IP forwarding, even though they may not actually be routing packets.

Statistics

Displays the Network Statistics window.

Query Database

Displays the Database Query window.

Charts

Displays the Sonar Charts window.

Machine Types

Displays the Database Query window with a list of machine types discovered.

Network Sonar Toolbars

Main Toolbar

Wizard

Displays the Network Discovery Wizard.

New

Creates a new discovery database.

Open

Opens an existing discovery database.

Help

Opens the Toolset help.

Discovery Toolbar

Select the Discovery group from the left toolbar to display the Discovery Toolbar.

Discovery Wizard

Displays the Network Discovery Wizard.

Discovery Topology

Displays the Network Topology Discovery dialog box.

Select Subnets

Displays the list of Networks and Subnets. You can select which subnets to include in the discovery.

Start Discovery

Starts or Resumes a network discovery. During a discovery, this item Stops or Pauses a network discovery.

Devices Discovered

Displays a list of discovered devices. You can watch this list during discovery to see what kinds of devices are being found.

Preferences

Displays the Discovery Settings and Preferences dialog box. For more information, see “Modifying Network Sonar Discovery Preferences” on page 131.

Analysis Toolbar

Select the Analysis group from the left toolbar to display the Analysis Toolbar.

Routers

Displays the devices that are configured as routers (IP forwarding).

Statistics

Displays statistics about the network discovery.

Query Database

Performs various searches on the Discovery Database.

Charts

Display discovered statistics on a chart.

Machine Types

Displays a list of discovered devices.

Export Wizard

Opens the Export Wizard.

Exporting, Printing, and Copying Data

After running a discovery, Network Sonar allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Charts

To copy the results:

Click **Edit > Copy Bitmap to Clipboard** or **Edit > Copy Metafile to Clipboard**.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Limiting Discovery to a Single Class B or C Network

The following steps illustrate one method of scanning a single class B or C network only. Step two tells the Discovery Engine to ignore any subnets outside of the initial network.

To limit your discovery to a single class B or C network:

1. Add the class B or C network manually.
2. Exclude all new subnets from the discovery.
3. Add the SNMP community strings for your network.
4. Start the network discovery.

Ping Sweep

Ping Sweep can scan a range of IP addresses and show which IP addresses are in use and which ones are currently free. Ping Sweep can also look up the DNS name for each IP address using your configured DNS and WINS servers. Ping Sweep performs a fast ICMP sweep of your IP address range and presents the results in an easy to use worksheet.

To start using Ping Sweep:

1. Specify a beginning IP address for the range to sweep.
2. Specify an ending IP address for the range.
3. Select the type of addresses to return.
 - Responding IP addresses
 - Non-Responding IP addresses
 - All IP addresses
4. Click **Scan**.

Note: If you need to automate collection of IP address status and device type, consider using the IP Address Management. For more information, see “IP Address Management” on page 94.

Exporting, Printing, and Copying Sweeps

After running a sweep, Ping Sweep allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Hint: If the results table is split horizontally between two pages, decreasing the width of the Ping Sweep window will make the table stay on one page.

Ping Sweep Settings

Ping Sweep provides a number of global settings that control default behaviors:

- For what type of IP addresses to scan
 - o Responding - limit the scan to show addresses in use
 - o Non-responsive - limit the scan to show addresses not in use
 - o Display both
- Do you want to perform DNS and WINS lookups
- When and if you want to play sounds

To change default settings:

1. Click **Edit > Settings**.
2. Click the Scanner tab, and then specify the appropriate information.
3. Click **OK**.

Modifying ICMP Ping Settings

At the core of Ping Sweep is the ability to field ICMP communications. Depending on your network topology and speed, you may need to modify the ICMP Ping settings used by Ping Sweep.

To modify the ICMP Ping settings:

1. Click **Edit > Settings**.
2. Click the Network tab, and then specify the appropriate information.

Delay between PINGs

Allows you to modify the time to wait before sending PING communication to each node. You can use this setting to limit traffic generated by Ping Sweep for slower connections.

PING Timeout

Allows you to adjust the amount of time that Ping Sweep waits for a response from a target IP address. If the target does not respond within the timeout and does not respond to any other PING attempts, it is assumed to be down.

PINGs transmitted per node

Allows you to control the number of PING attempts to send each address during a scan. When scanning networks containing Cisco routers, set this number above two (2). If the target IP address is not in the ARP cache of a Cisco router, the router discards the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never arrive at the subnet of the target IP address. In this situation, the Cisco router responds to the second PING.

Packet Time-To-Live

The Packet Time-to-Live is the number of different locations you accept during the route to the IP address. A setting of 32 means your PING test could pass through up to 32 different routers on the way to the remote IP address before being thrown away by the network. Normally, you set this to 32 hops.

3. Click **OK**.

Publishing to the Web

Ping Sweep results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Port Scanner

The Port Scanner tool remotely discovers the status of TCP ports on devices. You can specify a range of IP addresses to include in the scan, and then scan a Quick List of port numbers or manually select the ports from a list that includes their common purposes.

To begin scanning ports:

1. Type the beginning and ending IP addresses of the computers whose ports you want to scan.
2. *If you want to use a Quick List for your scan*, check **Use Quick List instead of Settings**, and then type a list of ports or select a predefined Quick List in the **Port Range** field.

Note: Type port lists separated by commas for individual ports or separated by hyphens to cover a range of values.

3. *If you want to select ports from a list which includes common port definitions*, complete the following procedure:
 - a. Click **Settings**.
 - b. Check the ports you want to scan in the Available Ports list.
 - c. *If you want to redefine or add a new port*, type the port and a description in the Add New Port window grouping, and then click **Add New**.
 - d. If you want to delete a port, select the port, and then click **Delete**.
 - e. If you want to change the sort or filter the window to show only those ports already selected, check the appropriate field.
 - f. Click **OK**.
4. Click **Scan**.

Exporting, Printing, and Copying Scan Results

After running a port scan, the Port Scanner tool allows you to transfer scan results to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Scan Results

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Scan Results

To copy the scan results:

Click **Edit > Copy**, and then specify whether you want to copy the entire result set to the clipboard or a selected value.

Printing Scan Results

To print scan results:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

Port Scanner results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Port Scanner Options and Settings

A number of settings are configurable within the Port Scanner tool.

To configure your settings:

1. Click **File > Settings**.
2. Click the Ports tab, and then specify the ports you want to scan. For more information, see “Port Scanner” on page 143.

3. Click the Display & Sound Settings tab, and then check the options you want to enable. To improve performance, disable the sound options.
4. Click the Time & Performance tab, and then specify the appropriate settings. Timeout and scan spacing can be set low (fast) for LANs and newer computers. If you receive numerous No Reply messages, consider increasing these settings.
5. Click the Grid Settings tab, and then specify the options you want to enable. For more information about a setting, click **Explain**.

Rescanning Ports on a Particular Address

Rescanning can be quickly accomplished by right-clicking an individual IP address and then selecting one of the following options:

Set to Rescan This Address (same ports)

Sets the starting and ending IP address range to the current address without modifying port selections.

Set to Rescan This Address (all ports)

Sets the starting and ending IP address range to the current address and activates the Quick List option with all ports specified.

Click **Scan** to start the port scan.

SNMP Sweep

SNMP Sweep scan a range of IP addresses and show which IP addresses are in use. SNMP Sweep also provides the following information:

- DNS name
- System Name
- Location
- Contact
- Last Reboot
- System Description

Note: SNMP must be enabled on the device.

To begin a sweep:

1. Type the beginning and ending addresses of the IP address range you want to scan.
2. Click **Scan**.

Note: If a computer is configured for IP forwarding, it is considered capable of routing. The computer may not actually be routing packets, but it can function as a router. This includes Windows-, Unix-, and Linux-based computers running IP forwarding services and daemons.

If you want information about both addresses in use and not in use, consider using Ping Sweep or IP Address Management. For more information, see “Ping Sweep” on page 140 and “IP Address Management” on page 108.

Exporting, Printing, and Copying Sweeps

After running a sweep, SNMP Sweep allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Sweep Results

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Sweep Results

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Sweep Results

To print results:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

SNMP Sweep results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Clearing Sweep Results

When you are finished with the information returned by SNMP Sweep.

To delete the results of a sweep:

Click **Edit > Clear List**.

Modifying SNMP Sweep Settings

When requesting values, such as the description and machine type values, SNMP Sweep uses SNMP community strings to request this information. You can specify community strings, ICMP configuration values, SNMP configuration values, reverse lookup, and whether to play sounds during the sweep.

To modify SNMP Sweep settings:

1. Click **File > Settings**.
2. Click the **Community Strings** tab, and then specify the community strings you want to use when polling your subnet. Ensure the most commonly used community strings are listed first. Click a community string and move it higher in the list or lower using the up and down arrows.

3. Click the ICMP tab, and then specify the appropriate values:

PING Timeout

Designates the maximum amount of time in milliseconds that SNMP Sweep will wait for a response from a target IP address. If a target IP address does not respond within the number of milliseconds set here, SNMP Sweep will assume it is down.

Packet Time-To-Live

Designates the number of hops you will accept along the way to an IP address. With a setting of 32, a packet could pass through up to 32 different routers on its way to the remote IP address before being thrown away by the network. Normally you would set this to 32 hops.

Delay between PINGs

Designates the time in milliseconds to wait before sending PINGs to each node. This setting is used to arbitrarily slow down SNMP Sweep. This is important on dial-up lines or to limit the amount of traffic generated by SNMP Sweep.

PINGs transmitted per node

Designates how many PINGs should be sent to each IP address during scanning. Set this to 2 or more when scanning networks containing Cisco routers. If the target IP address is not in the ARP cache of a Cisco router, then the router will throw away the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never make it to the subnet of the target IP address. In this situation, the second PING will be the one the target IP address responds to.

- Click the SNMP tab, and then specify the appropriate values:

Packet Timeout

Designates the number of milliseconds SNMP Sweep should wait for an SNMP reply before assuming the packet was lost and trying again.

Query Attempts

Designates the number of times SNMP Sweep should retry an SNMP query before giving up. This should normally be 2 or more.

- Click the Scanner tab, and then specify the appropriate values:

Reverse addresses via DNS / WINS

Check this field to attempt DNS / WINS reverse lookups for the name of each IP address. SNMP Sweep automatically uses the DNS and WINS servers configured on the computer running SNMP Sweep.

Play sounds during scan

Check this field to play a sound each time SNMP Sweep finds a device.

Subnet List

The Subnet List tool builds a list of network subnets by scanning route tables on a seed router. The target router must have SNMP enabled, and you must know the SNMP community string.

To immediately begin retrieving subnet lists for your network:

- Provide the hostname or IP address of the router or server and the SNMP community string for a core router.
- Click **Retrieve Subnets**.

Note: Subnet List creates subnet lists by scanning route tables. If subnets have been summarized into a summary route on the router you are scanning, Subnet List cannot discover all your subnets. Direct the tool to a different router, one that does not have routes summarized.

Modifying SNMP Options for Subnet List

Depending on your network infrastructure, you may need to increase the wait time for SNMP timeout or increase the number of SNMP query attempts. Conversely, if your network speed is optimal, you may be able to shorten the SNMP timeout.

To modify SNMP settings:

1. Click **File > Settings**.
2. Adjust the settings to reflect your network environment:

Packet Timeout

This setting is the number of milliseconds Subnet List should wait for an SNMP reply before assuming the packet was lost and trying again.

Query Attempts

Designates the number of times Subnet List should retry an SNMP query before considering the device down. Set this to 2 or more.

Exporting, Printing, and Copying Subnet List Results

After querying your router, Subnet List allows you to transfer the discovered subnets to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Subnet List Results

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Subnet List Results

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire result set to the clipboard or a selected IP address.

Printing Subnet List Results

To print results:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

Subnet List results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Switch Port Mapper

The Switch Port Mapper tool remotely discovers the devices connected to each port on a switch or hub. Additionally, Switch Port Mapper discovers the MAC address, IP Address, and Hostname of connected devices, as well as details about each port.

Selecting What You Want Reported

Before running Switch Port Mapper, consider looking through the information that can be returned by a successful map of your hub or switch. Consider the following list of information that can be returned:

- Index of the interface
- Interface description
- Interface name
- Interface alias
- Type of switch interface as icon
- Type of switch/hub interface
- Admin status of port as text
- Admin status of port as icon
- Up/Down status of port as text
- Up/Down status of port as icon
- Port speed
- Maximum transmission unit for the interface
- MAC address of the switch port
- MAC addresses of connected devices
- IP address of connected MAC addresses
- DNS/NetBIOS lookup of IP addresses
- Interface duplex
- Date/Time of last interface status change
- Reason for last interface change (Cisco IOS)
- Hardware type (Cisco IOS)
- Time last packet was received on this port (Cisco IOS)

- Time elapsed since the last packet was received (Cisco IOS)
- Time last packet was transmitted on this port (Cisco IOS)
- Time elapsed since the last packet was transmitted on this port (Cisco IOS)
- Last time of packet send or receive (Cisco IOS)
- 5 minute receive rate (Cisco IOS)
- 5 minute transmit rate (Cisco IOS)
- 5 minute receive packet rate (Cisco IOS)
- 5 minute transmit packet rate (Cisco IOS)

Modifying SNMP Settings

Modify the SNMP settings if your network can handle faster SNMP polling or if you notice that information is not being reported, slow the polling. You can also disable SNMP v2 packets, disabling Get Bulk requests. The modifications you make are globally applied to all hubs and switches and routers used by Switch Port Mapper.

To modify the SNMP Settings:

1. Click **File > Settings**, and then click the SNMP tab.
2. Modify the settings to fit your environment, and then click OK.
 - SNMP Timeout is used to configure the amount of time that the Switch Port Mapper waits for a response after querying a device
 - SNMP Retries is used to configure the number of times Switch Port Mapper retries statistics collection
 - Disabling SNMP V2 support forces Switch Port Mapper to use SNMP V1 packets, reducing the speed at which statistics are gathered.

Mapping Switch and Hub Ports

Port mapping is done by discovering and correlating port information to MAC address and IP address information. The MAC and IP address information is discovered through a router or server directly connected to the same subnet as the switch or hub.

Switches and hubs that support the BRIDGE-MIB can be mapped. If you are not sure if your device supports the BRIDGE-MIB, try to use the tool. Many devices support this MIB. Device details for Switches and Hubs that do not support BRIDGE-MIB cannot be discovered.

Note: Using the Ping Sweep tool to sweep the subnet before running Switch Port Mapper improves the details of the mapping by pre-loading the ARP table of the router. For more information, see “Ping Sweep” on page 101.

To map your switch or hub:

1. Click **Select Switch**, and then provide the SNMP community string or SNMP v3 credential information on the Switch/Hub Credentials window.

Note: If you want to map a device with VLANs configured, specify the community string in the following format: *communityString@VLAN#*. For example, to scan VLAN 2 using the public community string, type *public@VLAN2*.

2. Click **Test** to ensure you specified valid credentials.
3. Click **OK**.
4. Click **Select Router**, and then provide the SNMP community string or SNMP v3 credential information on the Router/Switch Credentials window. This is the router or server to which the hub or switch is connected. This device is used to gather MAC and IP addresses to correlate with the hub or switch port information.
5. Click **Test** to ensure you specified valid credentials.

6. Click **OK**.
7. Click **Map Ports**.

Notes:

- If the IP address or hostname is not returned for a device, it is possible the device does not appear within the ARP table of the router or server you specified. The tool will be unable to correlate the MAC address to an IP address and hostname. The ARP entry for this device may have expired or the device may be off.
- If you see multiple devices connected to the same port, a hub is probably connected to the switch and multiple devices directly connected to the hub.
- If you want to launch Realtime Interface Monitor using the switch or hub as your target device, click **Real Time**.

Exporting, Printing, and Copying Mappings

After generating a port mapping, Switch Port Mapper allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Mappings

To export port mapping results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Mappings

To copy the port mapping results:

Click **Edit > Copy**, and then specify whether you want to copy the entirety of the mapping results to the clipboard or a selection.

Printing Calculations

To print port mapping results:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

Port mapping results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Chapter 6

Network Monitoring Tools

The following sections provide detailed information about the Network Monitoring tools included with the Toolset.

- “Advanced CPU Load” on page 157
- “Bandwidth Gauges” on page 162
- “CPU Gauge” on page 170
- “Network Monitor” on page 171
- “Network Performance Monitor” on page 185
- “Realtime Interface Monitor” on page 217
- “Router CPU Load” on page 221
- “SNMP Realtime Graph” on page 225
- “Syslog Server” on page 232
- “Watch It” on page 236

Advanced CPU Load

The Advanced CPU Load tool uses SNMP to monitor network device CPU utilization and provides both real-time and historical views of this data. Using the tool, you can monitor the processor utilization of your routers, switches, servers, and other SNMP enabled network devices. In addition to monitoring CPU utilization you can monitor response time, running processes, uptime, errors, and several other statistics.

Note: If your device does not support the Host-Resources-MIB, some information may not be able to be gathered.

Adding Your First Devices

The Advanced CPU Load tool requires a database to store the statistics you gather. The database allows you to keep load statistics and mine that data for trending. Before you can add your first devices to the Advanced CPU Load tool, you create your database.

To add your first devices:

1. Click **File > New CPU-Load Database**.
2. Provide a name and location for your database, and then click **OK**.
3. Click **Devices > Add Device**.
4. Specify the IP address or hostname of the device you want to monitor and the SNMP community string. If you want to be able to update information, such as the location or contact for a device, ensure you supply the read-write community string for your device. Information you can modify is displayed in blue.

Note: Changing the IP address changes the device you are monitoring, it does not change the IP address of the target device.

5. Click **OK**.

Modifying Advanced CPU Load Settings

By modifying your Advanced CPU Load settings, you can change the following global configuration information:

- Change SNMP polling intervals, timeout, and retries
- Add columns to display when polling devices for CPU load, including current load, time-date stamp of last reboot, time-date stamp of next poll, number of processors, SNMP community string, system contact, description, location, name, and OID.
- Statistics retention and database write frequency

To modify your configuration:

1. Click **File > Settings**.
2. Click the SNMP Polling tab, and then specify the appropriate values:

CPU Load Poll Interval

Allows you to specify the amount of time the tool waits between polling devices for current CPU load statistics.

SNMP Timeout

Allows you to configure the amount of time the tool waits for a response after querying for status.

SNMP Retries

Allows you to configure the number of times the tool tries to collect statistics from a device.

3. Click the Display Columns tab, and then specify the columns you want to add to the main monitoring window. All data is collected at every poll. Changing this setting only changes what is displayed. Use the up and down arrows to modify the column order.

4. Click the Database Archive tab, and then specify the appropriate information:

Statistics Retention

Allows you to designate how long statistics are kept in the database. You can keep statistic up to 1500 days for trend analysis and historical purposes.

Log Current CPU Load to Database every

Allows you to specify how often the database is updated with the current CPU load information.

Note: The Advanced CPU Load database is a standard Microsoft Access database and can be accessed for custom queries and reports.

Monitoring Multi-Processor Devices

The Advanced CPU Load tool monitors multiple processor devices and keeps CPU specific loads separate.

To display the number of processors that the device has and the load on a per processor basis:

1. Click **Devices > % Load on each Processor**.
2. If you want to refresh the displayed information, click **Edit > Refresh Entire List**.
3. Close the display by clicking **File > Exit**.

Viewing Running Processes on the Target Device

When monitoring CPU loads, you can also view the processes running on a device. This can help you determine what is taxing your systems.

To view the running processes on a device:

1. Click **Devices > Processes Running**.
2. If you want to refresh the displayed information, click **Edit > Refresh Entire List**.
3. Close the display by clicking **File > Exit**.

Viewing Client Session on the Target Device

When monitoring CPU loads, you can also view the client sessions open on a device. This can help you determine what is taxing your systems.

To view the open sessions on a device:

1. Click **Devices > Client Sessions**.
2. If you want to refresh the displayed information, click **Edit > Refresh Entire List**.
3. Close the display by clicking **File > Exit**.

Viewing Running Services on the Target Device

When monitoring CPU loads, you can also view the services currently running on a device. This can help you diagnose CPU load spikes.

To view the running services on a device:

1. Click **Devices > Services**.
2. If you want to refresh the displayed information, click **Edit > Refresh Entire List**.
3. Close the display by clicking **File > Exit**.

Viewing Installed Software on the Target Device

When monitoring CPU loads, you can also view the software currently installed on a device. This can help you diagnose CPU load spikes.

To view the running services on a device:

1. Click **Devices > Software Packages**.
2. If you want to refresh the displayed information, click **Edit > Refresh Entire List**.
3. Close the display by clicking **File > Exit**.

Viewing Historical Graphs

You can view a graph of the data captured about your devices derived from the database created while monitoring CPU loads. This graph allows you to perform trend analysis and can be modified to display specific time periods, allowing a clear view of before and after upgrade performance.

To view historical graphs:

1. Click **Devices > Historical Graph**.
2. Change time periods by clicking **Period**, and then clicking the desired period, including a custom period.

Modifying Displayed Columns

A quick and easy way to change the column order of the data displayed is to drag-and-drop columns in their location you want them. You can also right-click a column head and select or deselect the columns to display.

Bandwidth Gauges

Bandwidth Gauges provides realtime traffic monitoring. The tool monitors the utilization, the amount of data being received and transmitted, of any remote network device, using SNMP to communicate and gather traffic statistics. Gauges display transmit and receive traffic in bits per second or transmit and receive percent utilization for each interface or port.

Creating a Gauge

Bandwidth Gauges are simple to setup. As long you have enabled SNMP communication on your devices and your devices support MIB-II, you can monitor their bandwidth usage with the Bandwidth Gauges tool.

To create a gauge:

1. Click **Gauges > New Gauge**.
2. Specify the IP address or hostname of the device.
3. Select whether you want to use a community string or SNMP version 3 credentials.
4. ***If you want to test the credentials***, click **Test**.
5. Click **Next**.
6. ***If prompted***, specify whether you want to store the credentials you specified in the shared credentials database.
7. Select one of the discovered interfaces or ports, and then click **Next**.

8. Ensure the automatically discovered speed is correct, or specify your own speeds. Different speeds can be specified for transmit and receive. The tool uses the port speeds to calculate percent utilization of the interface and define the upper scale of the gauge.
9. Select whether to use 64-bit or 32-bit traffic counters.
10. Click **Finish**. The gauge will take a baseline, and then immediately start monitoring usage.

Notes:

- You can select any interface or sub-interface of a frame-relay to monitor.
- The number of gauges is governed by the memory of the Toolset computer.
- Realtime utilization is based on the number of octets transmitted/received through an interface over the last few seconds. Bandwidth gauge polls the remote interface about every fifteen (15) seconds by default and calculates average bits per second since the last poll.

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.
 - a. *If you want to add a community string*, click Community string and then type the string.
 - b. *If you want to add SNMP version 3 credentials*, click SNMP Version 3, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Bandwidth Gauges Menus

File Menu

Load Gauges

Load a set of gauges from a previously save file. This file has the extension .BandwidthGauges and it created by selecting Save or Save As from the File menu.

Save

Saves the current set of gauges as a *.BandwidthGauges file. This file can be reloaded later by selecting Load Gauges from the File menu.

Save As

Saves the current set of gauges as a *.BandwidthGauges file with a new filename. This file can be reloaded later by selecting Load Gauges from the File menu.

Close

Closes all gauges currently displayed.

Publish to Web

Saves the gauges as an HTML file and gauge images to the specified location. This location could be part of a web site.

New Window

Opens another instance of the Bandwidth Gauges in a new window.

Settings

Opens the Settings dialog window.

Exit

Exits the program. You should save your gauges before exiting if you want to reload them without having to add them one at a time.

Edit

Shared Credentials Database

Allows you to add credentials and associate credentials with devices. This database can be accessed by numerous tools within the toolset.

Gauges Menu

New Gauge

Adds a new gauge to the list.

Refresh

Polls all devices and the updates the associated gauges. Some devices, including Windows servers, update the traffic statistics in their SNMP Agent every 15 or 20 seconds. If the device is polled more frequently than the remote SNMP Agent is updated, the gauges may show 0 bps, and then show the correct values a few seconds later. If you notice the gauges changing from 0 bps to a higher value, you may need to increase the poll interval. Double-click on a gauge to adjust its poll interval.

Modifying Settings and the Publishing of Gauges

Click **File > Settings** to adjust the following information:

- Layout
- Transparency
- Gauge styles
- Data table inclusion
- Networking details, including refresh rate, SNMP timeout and retry attempts
- Automatically publishing gauges as HTML

Layout Tab

Number of Columns

Sets the maximum number of gauges to be displayed in each row. When a new gauge is added, a new row will be created if the current row is already displaying the maximum number of gauges.

Reposition Gauges

Use the up and down arrows to arrange the display order of the gauges.

Transparency Tab

Switch to transparent mode after a few seconds

When this option is enabled, moving the mouse cursor away from the Bandwidth Gauges window will activate the transparent mode. When the gauges are transparent, mouse clicks will be passed to the workspace (applications running behind the gauges) instead of to the gauges. To exit transparent mode, place the mouse cursor over the Bandwidth Gauges title bar.

Transparent Slider

Adjust the slider to change the transparency opacity. To make the gauges more prominent, increase the percentage, decrease it to make the gauges more transparent.

Keep Bandwidth Gauges on top of other windows

Check this option to show Bandwidth Gauges on top of all windows even when working in another application.

Note: When Switch to transparent mode after a few seconds is enabled, the Bandwidth Gauges will always be placed on top of other windows.

Gauge Styles Tab

Style of Gauge

There are over thirty different gauge styles to choose from. Changing the Style in the Bandwidth Gauges Settings dialog only changes the default style. Click the “Apply to All” button to change the current gauges to the selected style.

Double-click on a gauge to modify the settings for a single set of gauges.

Data Table Tab

Show a data table below Gauges

Check this to set the default data table for all gauges. When a new gauge is added, it will contain a data table with the Selected Statistics shown here. Click **Apply to All** to add a data table to the gauges currently displayed.

Double-click on a gauge to modify the settings for a single set of gauges.

Network Tab

These sliders are used to adjust polling frequency, timeout, and to adjust how often the gauges are displayed. The “Apply to All” button applies the Update Gauges every XX seconds to all gauges currently displayed.

Note: Some devices, including Windows servers, only update the traffic statistics in their SNMP Agent every 15 or 20 seconds. If the device is polled more frequently than the remote SNMP Agent is updated, the gauges may show 0 bps, and then show the correct values a few seconds later. If you notice the gauges changing from 0 bps to a higher value, you may need to increase the poll interval. Double-click on a gauge to adjust its poll interval.

Auto-Publish

Auto-Publish these Gauges to a Web

When this is selected, an HTML file will be created every few seconds. The Web Page Title will be displayed on the title bar of the web browser and as the title of the web page. Adjust the slider at the bottom of the window to change how often the HTML file is updated.

Context Menus

Right click on any gauge to display a context menu for that gauge.

Copy

Right-clicking on a gauge and selecting Copy will copy an image of that gauge to the clipboard. Alternately, when right-clicking on the data table and selecting Copy will copy the data table text to the clipboard.

Delete Selected Gauge

Deletes the gauge from the current display.

New Gauge

Opens the New Traffic Gauges dialog to add a new gauge to the current display.

Reset

Clears the historical statistics and starts a new baseline for the selected gauge.

Refresh

Polls the selected device and the updates the gauges. Some devices, including Windows servers, only update their MIBs every 15 or 20 seconds. If the device is polled more frequently than the MIB is updated, zero values will be reported.

Data Table

Displays the data table if not currently shown. If a data table is already displayed, it will be removed.

Historical Chart

Displays a brief history of the selected gauge in a chart format.

Historical Statistics

Displays a brief history of the selected gauge in a table format.

Properties

Opens the Gauge Properties dialog for the selected gauge.

Note: Any value adjusted in this dialog will only apply to the selected gauge. To change values for all gauges, use the Bandwidth Gauges Settings dialog.

Saving and Loading a Set of Gauges

Once you have a set of gauges defined, you can save their configuration as a file that can be loaded at anytime.

To save a set of gauges:

1. Click **File > Save Gauges**.
2. Specify a name for the configuration file, and then click **Save**.

To reload a set of gauges:

1. Click **File > Load Gauges**.
2. Navigate to the configuration file, and then click **Open**.

CPU Gauge

The SolarWinds CPU Gauge monitors CPU load on routers, switches, and Windows 2000 and later computers. The CPU Gauge utilizes SNMP to communicate with the remote device, displaying the received results in an easily consumed graphical gauge. The following sections pertain to the default CPU Gauge skin.

Monitoring a Device

Complete following procedure to select a device to monitor.

To monitor a device:

1. Click on the button in the top right corner of the tool.
2. Click **Setup Gauge**.
3. Provide the IP address and the read or read/write community string for the device.
4. Click **OK**.

Notes:

- Ensure your access list does not block SNMP queries.
- Ensure you are using the correct read or read-write community string.

The left of the CPU Gauge provides the following statistics:

- Maximum load since monitoring began displayed in red
- Minimum load since monitoring began displayed in green

Current CPU Load is also displayed in the center of the gauge

Saving a gauge setup

Complete the following procedure to save a loaded gauge.

To save a gauge:

1. Click on the button in the top right corner of the tool.
2. Click **Save Gauge**.
3. Provide a name for the configured gauge, and then click **Save**.

Loading a gauge

Complete the following procedure to load a saved gauge.

To load a gauge:

1. Click on the button in the top right corner of the tool.
2. Click **Load Gauge**.
3. Select the gauge you want to load, and then click **Open**.

CPU Gauge Skins

CPU Gauge ships with a number of different skins.

To change the skin of this utility:

1. Click the five vertical lines next to the title of the tool.
2. Select the new skin you want to use.

Network Monitor

The Network Monitor tool can monitor hundreds of devices, keeping track of response time and packet loss. Network Monitor can also notify you when a device stops responding.

Note: If you need to monitor interface traffic and errors also, use the Network Performance Monitor tool.

Adding Devices to Monitor

As long as you can use ICMP to ping a device, you can monitor that device with the Network Monitor tool. Network Monitor monitors hundreds of devices, referred to as nodes, providing a simple up/down/warning status along with response and packet loss. If you do not want to add nodes to Network Monitor individually, you can import nodes. For more information, see “Importing into Network Monitor” on page 172.

To add a node:

1. Click **Nodes > New Node**.
2. Type the node hostname or IP address on the Add Node window, and then click **OK**.

3. Ensure the correct information is provided on the Node Details window:
 - If you want to send an email or page, check **Send E-Mail/Page notifications for events on this node**. You will need to configure your SMTP settings to receive email and page alerts. For more information, see “Configuring Network Monitor Settings” on page 175.
 - Poll interval is the frequency with which the node is polled using ICMP.
 - Fast poll interval is the frequency with which the node is polled when packet loss occurs. If the device does not respond during the fast poll interval, it is considered down. While in the fast poll interval, it is considered in a warning state.
4. Click the Icons & Sounds tab, and then specify any customizations to the node icons and sounds used for Active, Warning, and Inactive states.
5. Click **Close**.

Importing into Network Monitor

A number of file formats are supported for importing IP address lists into Network Monitor.

To import addresses into Network Monitor:

1. Click **File > Import**, and then select the format of the file to import:
 - Import from a Network Sonar Database
 - Import from a Comma Delimited File
 - Import from a Tab Delimited File
 - Import from a Microsoft Access Database
2. Select the nodes that should be imported into Network Monitor, and then click **OK**.

Import from a Network Sonar Database

If you have discovered your network using Network Sonar, then you can import the discovery results directly into Network Monitor. For more information, see “Network Sonar” on page 130.

Import from a Comma Delimited File

When creating a comma delimited file, also referred to as a CSV or comma separated value file, each field is separated by a comma. For Network Monitor, ensure the first field is the IP address and the second field is the node name. The following example was created with Ping Sweep, leaving response time out of the report. For more information about Ping Sweep, see “Ping Sweep” on page 101.

```
# Exported from PingSweep

"IP Address", "DNS Lookup"

10.45.19.1, Admin.SolarWinds.Net
10.45.19.2, www.NovtekVideo.com
10.45.19.3, PerfMan.SolarWinds.Net
10.45.19.4, F3.SolarWinds.Net
10.45.19.5, Development.SolarWinds.Net
10.45.19.6, ww2.SolarWinds.Net
10.45.19.7,
10.45.19.8,
10.45.19.9,
10.45.19.10,
10.45.19.11,
10.45.19.12,
10.45.19.13,
10.45.19.14,
10.45.19.15,
10.45.19.16,
10.45.19.17,
10.45.19.18,
10.45.19.19,
10.45.19.20, WebDev.SolarWinds.Net
```

Import from a Tab Delimited File

Each field in this file format is separated by a tab. The first field is the IP address and the second field is the node name. The following example was created with Ping Sweep, leaving response time out of the report. For more information about Ping Sweep, see “Ping Sweep” on page 101.

Exported from PingSweep

IP Address	DNS Lookup
216.60.197.200	ww2.SolarWinds.Net
216.60.197.201	Admin.SolarWinds.Net
216.60.197.202	www.NovtekVideo.com
216.60.197.203	PerfMan.SolarWinds.Net
216.60.197.204	Family.SolarWinds.Net
216.60.197.205	Development.SolarWinds.Net
216.60.197.206	www.RCC4Jesus.org
216.60.197.207	
216.60.197.208	
216.60.197.209	
216.60.197.210	
216.60.197.211	
216.60.197.212	
216.60.197.213	
216.60.197.214	
216.60.197.215	
216.60.197.216	
216.60.197.217	
216.60.197.218	
216.60.197.219	
216.60.197.220	WebDev.SolarWinds.Net

Import from a Microsoft Access Database

This import method reads directly from a Microsoft Access database. You will be prompted for the table within the Access database that contains the nodes to import.

Network Monitor will attempt to determine which field contains the IP addresses. If it cannot determine which field contains the IP addresses, then you will be prompted to select the field. You will also be prompted for the field that contains the name of each node.

Configuring Network Monitor Settings

Before you can receive email or page alerts based on node events, you need to configure your Network Monitor settings. These settings control the following configuration options:

- Who to notify and for what events
- Message contents for node down, node warning, node up events
- Network Monitor database maintenance
- SMTP mail setup
- Polling intervals
- Icon and sound settings
- ICMP ping timeout and included data

To configure Network Monitor settings:

1. Click **File > Settings**.
2. Click the Event Notification tab, and then specify the appropriate information:

E-Mail / Pager Recipient

Type the email and pager addresses, separated with commas, you want to notify when events occur. Network Monitor sends the events to all E-Mail / Pager addresses entered here.

From E-Mail Account

Provide the name and reply address information for notifications sent by Network Monitor. Many pagers display the reply address as the name of the person who sent the page.

Event Types to send notification on

Select the events for which you want notification.

Note: You must turn on event notification for each node from which you want to receive notification. For more information, see “Viewing and Modifying Node Details” on page 179 and “Viewing Event Details” on page 181.

3. Click the Messages tab, and then complete the following procedure:
 - a. Click the event type you want to customize, and then type a subject line.
 - b. Type a custom message you want to use for this event. The following macros can be used in message bodies:
 - %NODENAME – name of device
 - %DATE – date of event
 - %TIME – time of event
 - c. Repeat this procedure for each event type you want to customize.
4. Click the Database Size tab, and then specify the appropriate information:

Nightly Database Maintenance

Specify a time when maintenance should be performed.

Response Time Summarization

Specify when granular response time statistics are summarized into hourly averages and when hourly averages can be summarized into daily averages.

Event Archiving

Specify when old events can be deleted

5. Click the SMTP Gateway tab. You must have an SMTP server configured for Network Monitor to send email and page notifications. Specify the appropriate information:

SMTP Gateway

Provide the IP address or hostname of the SMTP server you want to use for email and pager notification.

Retry attempts

Use the slider to select how many times an email or page will be attempted.

Show status

The E-Mail Notification Service can display a status box whenever a message is sent to the SMTP server. The status window shows you the interaction between the notification service and the SMTP server, including any errors that occur.

6. Click the Polling tab, and then specify the appropriate information:

Poll Interval.

Poll interval is the frequency with which the node is polled using ICMP for response time and packet loss.

Fast Poll Interval

Fast poll interval is the frequency with which the node is polled when packet loss occurs. If the device does not respond during the fast poll interval, it is considered down. While in the fast poll interval, it is considered in a warning state.

7. Click the Icons & Sounds tab, and then specify then complete the following procedure:
 - a. ***If you want to change the default icons***, click **Change Default Icons**, select an icon, and then click **OK**.
 - b. ***If you want to change the default alarms***, click the event for which you want to modify the alarm, select a sound, and then click **OK**.
 - c. ***If you want to mute the alarms***, check Mute next to the event you want to mute.
8. Click the ICMP tab, and then change the ICMP timeout to reflect your network speed and the data included with the packet. High-latency networks such as frame-relay or satellite networks can require longer ICMP timeouts.

Exporting and Printing Node Lists and Event Details

While monitoring a device, Network Monitor allows you to transfer node lists and event details to other tools through exporting and printing.

Exporting Node Lists and Event Details

To export a node lists or event details:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Printing Node Lists and Event Details

To print a node list or event details:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

Network Monitor node lists and event details can be published to a static HTML page containing all the statistics for a specific statistics group.

To save a node list to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

To save event details to an HTML page:

1. Click **File > Export to HTML File** or **Export to MHTML File**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Viewing and Modifying Node Details

You can change the following attributes of a node:

- Name
 - IP address
 - Polling intervals
 - Associated icons and sounds
1. Click the node, and then click **Nodes > Node Details**.
 2. Review the information about the node, click refresh to update response time and packet loss.
 3. Ensure the correct information is provided on the Node Details window:
 - If you want to send an email or page, check **Send E-Mail/Page notifications for events on this node**. You will need to configure your SMTP settings to receive email and page alerts. For more information, see “Configuring Network Monitor Settings” on page 175.
 - Poll interval is the frequency with which the node is polled using ICMP.
 - Fast poll interval is the frequency with which the node is polled when packet loss occurs. If the device does not respond during the fast poll interval, it is considered down. While in the fast poll interval, it is considered in a warning state.
 4. Click the Icons & Sounds tab, and then specify any customizations to the node icons and sounds used for Active, Warning, and Inactive states.
 5. Click **Close**.

Deleting and Undeleting Nodes

If you no longer need to monitor a device, you can remove the node from Network Monitor.

To remove a node:

Click the unnecessary node, and then click **Nodes > Delete Node**.

If you mistakenly delete a node, you can restore the last deleted node, including all statistics for the node.

To undelete a node:

Click **Nodes > Undo Delete**.

Viewing Node-Specific Events

You can display the events for a specific node.

To view node-specific events:

1. Click the appropriate node.
2. Click **Nodes > Node Details**.
3. Clicking **Node > Events for this Node**.

Viewing the Event Monitor

The Event Monitor provides an excellent overview of all current, uncleared Network Monitor events. As new events occur, they are added to the Event Monitor window. As events are cleared, they are removed from the Event Monitor.

The Event Monitor is not constrained by the Network Monitor window and can be left open while the Network Monitor is minimized. This allows you to remain apprised of your events without having the full application restored at all times.

To start the Event Monitor:

1. Click **Events > Event Monitor**.
2. *If you want to clear events from the Event Monitor*, click the X.

Viewing Event Details

The Event Details window provides a detailed view of the current network events. As new events occur, they are added to the Event Details window. As events are cleared, they are removed from the Event Details window.

Unlike the Event Monitor, individual event detail is provided for each event. They are not summarized and grouped by the event type.

To view event details:

1. Click **Events > Event Details**.
2. ***If you want to clear events from the Event Monitor***, click the X next to the event you want to clear.
3. If you want to clear an entire category of events, click Events on the Current Network Monitor Events window and then select the category of events you want to clear:
 - Clear selected events
 - Clear informational events
 - Clear node up events
 - Clear node down events
 - Clear all events

Note: Cleared events are still stored in the database and can be searched. For more information, see “Searching Past Events” on page 181.

Searching Past Events

Cleared events are still available for viewing, searching, and exporting from the database.

To search past events:

1. Click **Events > Event Details**.
2. Click **Events > Past Events**.
3. ***If you want to view all events during a specific time period***, specify a start and end date, and then click **Search**.

4. ***If you want to view all uncleared events for a specific node***, specify the node, and then click **Search**.
5. ***If you want to view all uncleared events of a specific category***, specify the category, and then click **Search**.

Note: You can select dates, nodes, and categories together. After each change, ensure you click **Search**.

Exporting Events

The current set of events and past events can be exported in a number of file formats. For more information, see “Exporting and Printing Node Lists and Event Details” on page 178.

Running Database Maintenance Immediately

If your database is getting overly large or you are running low on disk space and want to immediately run database maintenance, complete the following procedure.

To immediately run database maintenance:

Click **File > Run Nightly Database Maintenance Now**.

The settings for database maintenance you configured will be executed immediately. For more information, see “Configuring Network Monitor Settings” on page 175.

Modifying the Look and Feel of Network Monitor

You can change the icons and sounds used within the tool. For more information about how to change these items, see “Configuring Network Monitor Settings” on page 175.

Running Response Time Charts

The Response Time Charts tool is an integral part of SolarWinds Network Monitor. In order to display response time charts, you must first add a device to monitor in Network Monitor. You may not see any information in Response Time Charts for 15 or 20 minutes after you add the device to Network Monitor. Response Time Charts displays historical response time and packet loss charts. Realtime charts of response times can be configured in the Enhanced Ping tool. For more information, see “Enhanced PING” on page 249.

Launching Response Time Charts

Response time charts provide you a historical overview of response time for the selected node.

To launch a response time historical chart for a node:

1. Click the node you want to chart.
2. Click **Nodes > Response Time Chart**.
3. ***If you want to change the time period***, click **Period** and then select the period you want to display:
 - Today
 - This week
 - This month
 - Last 30 days
 - Last 3 months
 - Last 12 months
 - This year
 - Custom period

Note: The custom period option allows you to specify the bounds of the time period and the sample rate to display.

4. ***If you want to view a table of the response times***, click **Chart > Response Time Table**.
5. ***If you want to increase or decrease the sample rate of the data***, click **Chart > More Detail** or **Chart > Less Detail**. When you select less detail, individual response times are averaged together.
6. ***If you want to customize the chart***, click **Edit > Customize Chart**, and then tab through the available customization options.
7. ***If you want to copy the chart***, click **Edit > Copy Bitmap** or **Edit > Copy Metafile**.
8. ***If you want to print the chart***, click **File > Print**.
9. ***If you want to Export the chart***, click **File > Export** and then select the target export type.

10. If you want to load a new chart of another node, click **File > Build New Chart** and then select the node and click **OK**.

Notes:

- If no chart is displayed, you do not have enough response time information in the database for the selected node. If you recently added the node, you need to wait 15 to 20 minutes for Network Monitor to accumulate data and add it to the database.
- Network Monitor will only add response time details to the database when it is running. If you exit Network Monitor, response times cannot be added to the database. Your response time chart will have a section or sections missing.

Network Performance Monitor

The Toolset Network Performance Monitor is a realtime network monitor able to track network latency, packet loss, traffic and bandwidth usage, node and interfaces status, and other critical data points.

What Network Performance Monitor Offers

Toolset Network Performance Monitor provides two different levels of monitoring:

Devices that support SNMP

Can be monitored for network latency and packet loss, provide traffic statistics, and supply detailed management information.

Devices that do not support SNMP

Can provide network latency and packet loss information.

Toolset Network Performance Monitor provides an ideal solution for the following needs:

- Monitoring the bandwidth utilization of your WAN circuits
- Isolating traffic bottlenecks within your network
- Graphing realtime results
- Identifying high traffic nodes
- Building customized reports
- Alerting on any of over 150 network properties
- Posting charts and reports on the web using the HTML Publish feature

Notes:

- While Engineer's Toolset provides detailed statistics collection for analysis, troubleshooting, and diagnostics, the embedded database is not intended for long-term monitoring of networks with more than 500 network elements and has a 2GB limit on stored data.

If you have a larger network and/or require data retention longer than 30 days, we highly recommend upgrading to Orion Network Performance Monitor (Orion NPM). Orion NPM is the perfect complement to Toolset's realtime network analysis and diagnostic capabilities. Orion NPM provides support for thousands of interfaces, virtually unlimited storage using a Microsoft SQL database backend, and includes a web-based interface to allow you and your entire team access to network availability and both realtime and historical statistics.

- Devices do not need to be on the same network.

Starting Toolset Network Performance Monitor

Toolset Network Performance Monitor provides an easily navigated, Windows explorer-like interface with a tree view in the left pane and a results view in the right.

To start Network Performance Monitor:

Click **Network Performance Monitor** in the Network Monitoring program folder.

Adding Nodes and Interfaces

A node is defined as any device with an IP address. Network Performance Monitor nodes typically include routers, switches, e-mail servers, application servers, and workstations. Nodes do not need to be on the same network, though they must be reachable from the computer on which you install Network Performance Monitor.

To add nodes or interfaces:

1. Click **Nodes > Add Node**. If you are adding an interface, click **Interfaces > Add Interface**.
2. Type or select the device name or IP address, and then click **Next**. If you want to support dynamic IP address assignment, check **Device uses a dynamic IP address (DHCP or BOOTP)**.
3. *If the device support SNMP version 1 or version 2*, click **Community string**, and then type the appropriate community string. If you specify a community string that has not been saved before, you are asked if you would like to save the credentials. Select yes to make the community string available in other tools that support the shared credentials database. If you want to be able to shutdown an interface remotely, you must provide a read/write community string.

4. If the device supports SNMP version 3, complete the following procedure:

- a.** Select a credential set from the list, or click **Add** to create a new credential set and save it in the shared credentials database.
- b.** If you are adding a new credential set, specify the appropriate information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.

Note: If you want to be able to shutdown an interface remotely, you must provide read/write credentials.

5. **If the device does not support SNMP**, click **Device does not support SNMP**. You can monitor latency, packet loss, and availability of a node without SNMP support.
6. Select the appropriate options on the Resource window, and then click **OK** to add your selections to the database and begin monitoring. If you have provided valid SNMP credentials, you can select CPU and memory utilization resource monitoring, volume, disk-based virtual and physical memory utilization, and interface traffic and error charting. If your device does not support SNMP or you do not have the appropriate credentials, the device is added to the left pane without displaying the Resource window.

Resource	What is Monitored
CPU	CPU load as percentage of capacity
Memory	Memory and buffer utilization as total usage and percentage of capacity
Volume	Memory and buffer utilization as total usage and percentage of capacity
Interface	Bandwidth utilization, percentage of capacity, errors and discards, and total bytes transferred

Modifying System Settings

System settings allow you to specify how your data is stored, how often data is collapsed, how often objects are polled and rediscovered, how often statistics are collected from objects, the behavior of charts, the timeout and retry intervals for ICMP and SNMP communications, and the appearance of the tree view.

To modify your system settings:

1. Click **File > Network Performance Monitor Settings**.
2. Specify the appropriate information on the Database tab:
 - Nightly database maintenance runs at the specified time. Maintenance uses the values specified in Statistics Summarization to compact and delete data.
 - Statistics summarization provides 4 customizable retention periods:
 - o Raw data retention
 - o Hourly data retention
 - o Daily data retention
 - o Event retention

Notes:

- While Engineer's Toolset provides detailed statistics collection for analysis, troubleshooting, and diagnostics, the embedded database is not intended for long-term monitoring of networks with more than 500 network elements and has a 2GB limit on stored data.

If you have a larger network and/or require data retention longer than 30 days, we highly recommend upgrading to Orion Network Performance Monitor (Orion NPM). Orion NPM is the perfect complement to Toolset's realtime network analysis and diagnostic capabilities. Orion NPM provides support for thousands of interfaces, virtually unlimited storage using a Microsoft SQL database backend, and includes a web-based interface to allow you and your entire team access to network availability and both realtime and historical statistics.

- You can run database maintenance immediately by clicking **Run Database Maintenance Now**.

3. Specify the appropriate information on the Polling tab. Polling determines availability, status, network latency, and packet loss and is normally done more frequently than statistics collection. Intervals apply to all objects added after your changes. If you want to overwrite the current polling intervals for your nodes, click **Apply these settings to All**.
4. Specify the rediscovery interval before leaving the Polling tab. Rediscovery validates the identity of monitored nodes, interfaces, and volumes and automatically adjusts for most changes in this information.
5. Specify the appropriate information on the Statistics tab. Statistics collection retrieves data from your device, interface traffic and errors, volume, and CPU usage. If you want to overwrite the current statistics collection intervals for your nodes, click **Apply these settings to All**.

Note: Statistics represent summaries, peaks, and averages collected over a period of time. Statistics do not represent only the activity occurring at the time of the collection, but are calculated values summarizing total activity since the last collection.

6. Specify the appropriate information on the Charts tab:
 - Specify whether to print charts in color or monochrome using differentiating symbols.
 - Specify the default font size.
 - Specify whether to automatically refresh charts.
7. Specify the ICMP and SNMP timeout intervals on the Network tab. You can also specify the SNMP retry number. Adjust these intervals to take advantage of a fast network or account for a slower network connection. For more information, see “Understanding ICMP Settings” on page 190 and “Understanding SNMP Settings” on page 191.
8. Specify your icon choices for nodes, interfaces, and volumes on the Node Tree tab.

Understanding ICMP Settings

The ICMP Timeout is the maximum amount of time (in milliseconds) Network Performance Monitor waits for a response from an IP address. Adjust this value to the minimum practical value possible in order to maximize performance. A good starting point is twice the maximum PING time across your network. A few days or weeks of observing your network response times will give you a good idea of what a practical minimum should be.

If no response is received, NPM changes the status of the node to a warning state. If the device remains unresponsive during the node warning interval, the node status changes to down. For more information about node warning intervals, see “Modifying Advanced Settings” on page 191.

You can edit ICMP packet content to make their sources identifiable or to adjust their size. The data payload size can vary from zero (0) to 200 bytes. Some network devices consider ICMP packets with data in the payload suspicious. Try adjusting the packet size to be less than 10 bytes or remove the data from the payload of the packet.

Note: When adjusting ICMP payload data, a byte counter is provided above the Data Portion text box.

Understanding SNMP Settings

The SNMP Timeout setting determines the number of milliseconds the Network Performance Monitor application waits for a reply before assuming the packet was lost and trying again. This setting should normally be set to twice the maximum PING time to any device you are monitoring. After observing the unique behavior of your network, you can adjust these values to the lowest time possible to assure responsiveness from an active device.

Modifying Advanced Settings

Advanced Network Performance Monitor Settings allow you to decide how to deal with the following actions:

- When to baseline your nodes and interfaces
- How to calculate availability
- How long a node remains in a warning state
- How to calculate values after a monitored counter rolls over
- Whether to automatically take XML snap shots of monitored object status and details.

Default values are selected for all of these options that work for most networks. Ensure you understand the implications of changing any of the values you decide to modify.

To modify advanced settings:

1. Click **File > Advanced Settings**.
2. Specify the appropriate information on the Baseline Calculation tab. For more information, see “Understanding Baseline Calculation” on page 192.
3. Specify the appropriate information on the Availability Calculation tab. For more information, see “Understanding Availability Calculation” on page 192.

4. Specify the appropriate information on the Node Warning Interval tab. For more information, see “Understanding the Node Warning Interval” on page 192.
5. Specify the appropriate information on the Counter Rollover tab. For more information, see “Calculating Counter Rollovers” on page 193.
6. Specify the appropriate information on the XML Snapshots tab. For more information, see “Taking XML Snapshots” on page 193.
7. Click **OK**.

Understanding Baseline Calculation

When Toolset Network Performance Monitor starts, current data is unavailable for your network. Toolset Network Performance Monitor creates a baseline. All Resources are polled right away, and, as soon as the first poll completes, the network is polled again. These two result sets are used to create statistics providing an immediate view of network performance.

Baseline calculation requires a great deal of data gathering and data computation that can affect the performance of the Toolset Network Performance Monitor host and polled router. If you do not need statistics immediately upon starting Toolset Network Performance Monitor, click **Disable Baseline Calculation at Startup** on the Baseline Calculation tab.

Understanding Availability Calculation

Toolset Network Performance Monitor provides two methods for calculating device availability. The default method uses the status of the node, up or down. As long as the device responds to a ping within the warning interval, Toolset Network Performance Monitor considers the node up. For more information about the node warning interval, see “Understanding the Node Warning Interval” on page 192.

The other method offered bases node availability on packet loss percentage. Unless you need packet loss percentage based availability calculations, it is recommended that you retain the default method for availability calculation.

Understanding the Node Warning Interval

Devices drop packets and fail to respond to polling for many reasons. When a device fails to respond, Toolset Network Performance Monitor changes the status from Up to Warning. The node warning interval allows you to specify how long a device can remain in a Warning state before it is considered unreachable or Down. While a node is in the Warning state, the service performs fast polling, pinging the device every 3 minutes, to quickly detect any change in node status.

If you see erroneous events or receive false alerts for down nodes, it is possible that the application is detecting intermittent packet loss within the network. If you do not want to diagnose the cause of the network flutter, consider setting the node warning interval to a higher value.

Calculating Counter Rollovers

Depending on the monitored device type and your Toolset Network Performance Monitor settings, statistical information may be derived from 32-bit counters. These counters offer a maximum value of 2 to the 32nd power (4,294,967,296). You can decide how Toolset Network Performance Monitor compensates when a 32-bit counter reaches maximum capacity and rolls over to zero. The default method detects a counter rollover and ignores the zeroed value. Instead, a new sample is scheduled in 20 seconds. This method can cause slightly skewed total bytes transferred numbers.

The more advanced method, which produces skewed numbers when manual counter resets occur, detects a counter rollover and uses the following calculation to correct for the rollover to zero: $\text{currentValue} + (\text{maximumCounterValue} - \text{lastCounterValue})$. If manual counter resets are rare, this method produces the most accurate results.

Toolset Network Performance Monitor can and does gather statistics from the 64-bit counters on network devices, if available. These counters have a capacity of 2 to the 64th power (18,446,744,073,709,551,616). While Toolset Network Performance Monitor fully supports the use of 64-bit counters, the implementation of these high capacity counters by some hardware vendors exhibit erratic behavior. If you notice peculiar results when using these counters, disable the use of 64-bit counters for the device and contact the hardware manufacturer.

You can enable and disable 64-bit counter use on the Node Details window. For more information, see “Viewing Node Data and Modifying Node Properties” on page 194.

Taking XML Snapshots

Toolset Network Performance Monitor can save periodic XML files of gathered data. This XML Snapshot can be used by other programs, most commonly web applications, to display information about selected devices or interfaces at a chosen point in time.

Warning: Generating XML snapshots causes intensive CPU usage. Leave this option disabled unless you use the XML Snapshots.

Viewing Node Data and Modifying Node Properties

The Node Details window contains a live view of data from the node, including the following information:

- Object specific information, type, sub-type, and node ID
- IP Address
- SNMPv2 only
- Community string
- Node, System, and Reverse DNS name
- Vendor
- SysObject ID
- Node and machine type
- Description
- Location and contact information, if set on the device
- Last boot time-date stamp
- IOS information, if applicable
- Status information (up, warning, down)
- Polling information, including interval, next expected, and fast polling interval
- Statistics collection and rediscovery interval
- 64-bit counter state
- Response time information, including current, average, maximum, minimum
- Packet loss
- CPU utilization
- RAM, total, used, and percent used
- Buffer information

The following information can be updated:

- Name
- IP address
- Dynamic IP address designation

- SNMP community string
- 64-bit counter allowance
- Node status polling
- Node statistics collection

To view or modify node properties:

1. Select the node in the tree pane, and then click **Nodes > Node Details**.
2. Review the information presented on the Details window.
3. If you want to modify any of the properties, do so, and then click **Apply Changes**.

Notes:

- Changing the name of a node only affects the way the node is identified on charts and graphs within Toolset Network Performance Monitor. It does not impact the device on the network.
- Changes made in this window affect only the node being viewed.
- While Toolset Network Performance Monitor fully supports the use of 64-bit counters, the implementation of these high capacity counters by some hardware vendors exhibit erratic behavior. If you notice peculiar results when using these counters, disable the use of 64-bit counters for the device and contact the hardware manufacturer.
- Change the IP address or community string only if they change on your network.

Unmanaging a Device

If you need to perform maintenance on a device, you can set a maintenance window in which Toolset Network Performance Monitor stops polling the device, does not create events about the device, and does not trigger alerts. All interface and volume statistics cease to be collected. When the time specified is reached, Toolset Network Performance Monitor begins normal polling of the device again.

To unmanage a device:

1. Select the node in the tree pane, and then click **Nodes > Node Details**.
2. Click **UnManage**.
3. Specify the appropriate time-date stamp in the following format: *mm/dd/yyyy hh:mm:ss AM|PM*. Then, click OK. Toolset Network Performance Monitor immediately stops managing the node.

Note: Unmanaging is not granular. You cannot specify an interface or a volume; the entire node must be unmanaged.

Viewing Interface Data and Modifying Interface Properties

The Interface Details window contains a live view of data from the interface, including the following information:

- Object specific information, type, sub-type, node ID, interface ID, and name
- Interface index (ifIndex)
- Interface name, ifName, and alias
- Interface type
- Interface description
- Interface type (numerical)
- 64-bit counter state
- MAC address
- MTU
- Port speed
- Status, operations status, administrative status
- Actively responding to SNMP
- Last change time-date stamp

- Polling information, including interval and next expected poll
- Statistics collection and rediscovery interval
- Transmit and receive bandwidth setting, actual bits per second, utilization percentage, packets, average packet size, unicast and multicast packets
- Peak received and peak transmitted, including time
- Transit and receive errors and discards

The following information can be updated:

- Name
- Transmit bandwidth maximum
- Receive bandwidth maximum
- Interface status polling
- Interface statistics collection

Note: Each Interface on a managed device must have a unique name. Some switches name all interfaces *Ethernet*. For Toolset Network Performance Monitor to collect traffic and error statistics on each interface, you must assign unique names.

To view or modify interface properties:

1. Navigate to and then select the interface in the tree pane
2. Click **Interfaces > Interface Details**.
3. Review the information presented on the Details window.

Note: An interface index (ifIndex) of zero indicates that the interface is no longer present on the node

4. If you want to modify any of the properties, do so, and then click **Apply Changes**.

Notes:

- Changing the name of an interface only affects the way the interface is identified on charts and graphs within Toolset Network Performance Monitor. It does not impact the device on the network.
- Changes made in this window affect only the interface being viewed.
- Transmit and receive bandwidth are used to calculate percent utilization and trigger alerts. For more information about how to use and modify these values, see “Understanding Transmit and Receive Bandwidth Values” on page 198.

Understanding Transmit and Receive Bandwidth Values

Transmit and Receive Bandwidth values govern percent utilization calculations. Toolset Network Performance Monitor sets these values when the interface is added and does not dynamically update them. Because you may want to set these values lower than the actual bandwidth full dedication or because you may want to set the values independently for asymmetric circuits (ADSL or CATV interfaces, for example, with different upstream and downstream data rates), these values are manually customizable.

During customer circuit monitoring, consider setting thresholds that reflect allowed and allowable transmit and receive bandwidth settings. For example, a customer may have a 10 Mbps connection (via Ethernet), but may only be paying for 512 Kbps with overcharges when they exceed the 512k limit. You can set the Transmit and Receive Bandwidth settings to 512000 and display Percent Utilization charts for the circuit in terms of 512 Kbps.

Enabling and Disabling Interfaces

If you have provided a read-write SNMP community string or an SNMP version 3 account with the appropriate permissions at the node level, you can remotely enable and disable interfaces from the Toolset Network Performance Monitor console.

To enable a disabled interface or disable an enabled interface:

1. Navigate to and then select the interface in the tree pane, and then click **Interfaces**.
2. Click the appropriate action on the Interfaces menu.
 - Administratively Shutdown Interface
 - Administratively Enable Interface

Note: Ensure you do not disabling the interface you are using to connect to the device.

Viewing Volume Details and Modifying Volume Properties

The Volume Details window contains a live view of data from the volume, including the following information:

- Object specific information, type, sub-type, node ID, volume ID, and name
- Volume index and description
- Volume type
- Status
- Actively responding to SNMP
- Last change time-date stamp
- Polling information, including interval and next expected poll
- Statistics collection and rediscovery interval
- Volume size, bytes used, and bytes available
- Volume errors

The name of the volume can be updated on this window.

To view or modify volume properties:

1. Navigate to and then right-click the volume in the tree pane.
2. Click **Volume Details**.
3. Review the information presented on the Details window.
4. If you want to modify the name of the volume, do so, and then click **Apply Changes**.

Notes:

- Changing the name of a volume only affects the way the volume is identified on charts and graphs within Toolset Network Performance Monitor. It does not impact the mounted device.
- Changes made in this window affect only the volume being viewed.

Polling on Demand

You can manually pole any of the following objects:

- Nodes
- Interfaces
- Volumes

Polling requests whatever information can be requested from the object. If the object has SNMP communication enabled, the manual poll will pull statistics. If not, the manual poll will use ICMP communication and return only those values. You can see the immediate results of a manual poll on the details window of the object you poll. For more information, see the following sections:

- “Viewing Node Data and Modifying Node Properties” on page 194
- “Viewing Interface Data and Modifying Interface Properties” on page 196
- “Viewing Volume Details and Modifying Volume Properties” on page 199

To poll a node:

1. Select the node in the tree pane.
2. Click **Nodes > Node Details**.
3. Click **Poll**.

To poll an interface:

1. Navigate to and then select the interface in the tree pane.
2. Click **Interfaces > Interface Details**.
3. Click **Poll**.

To poll a volume:

1. Navigate to the volume in the tree pane, and then right-click the volume you want to poll.
2. Click **Volume Details**.
3. Click **Poll**.

Rediscovering on Demand

Rediscovery of an object allows you to verify and update identity information. For example, the name or IP address of a node.

You can manually rediscover any of the following objects:

- Nodes
- Interfaces
- Volumes

To Rediscover a node:

1. Select the node in the tree pane.
2. Click **Nodes > Node Details**.
3. Click **Rediscover**.

To poll an interface:

1. Navigate to and then select the interface in the tree pane.
2. Click **Interfaces > Interface Details**.
3. Click **Rediscover**.

To poll a volume:

1. Navigate to the volume in the tree pane, and then right-click the volume you want to poll.
2. Click **Volume Details**.
3. Click **Rediscover**.

Understanding and Acknowledging Events

An event is defined as any change to the state of a monitored object or an action in response to a state change. Review the following list to better understand the type of events you can expect. This list is not inclusive of all possible events.

Node events

Down, Up, Warning, Deleted, Added, Unmanaged, Manage, Rebooted, and Changed

Interface events

Down, Up, Shutdown, Enabled, Unknown, Added, Deleted, Remapped, and Changed

Volume events

Remapped, Changed, Added, Deleted, Disappeared, and Reappeared

Monitoring

Started and Stopped

Failover

Failover and Failback

Alert

Triggered and Reset

Viewing a Detailed Log of Unacknowledged Events

Toolset Network Performance Monitor provides a detailed list of current unacknowledged events that includes the time-date stamp, the type, and the full text of the event.

To view unacknowledged events:

1. Click **Events > Event Details**.
2. Ensure **Current Events** is depressed in the lower left of the Events window.

Acknowledging Events

Acknowledging an event removes it from the default event window (Current Events) and from the event summary. It is not removed from the event database. For more information about viewing all the events in the database, see “Viewing a Detailed Log of All Events or Events during a Specific Period” on page 203.

To acknowledge events:

1. If you want to acknowledge a single event, click the icon (X) in the Ack column of the Current Events window.
2. If you want to acknowledge multiple events, complete the following procedure:
 - a. Select multiple events using CTRL+Click or Shift+Click.
 - b. Right-click a selected event, and then click **Clear Selected Events**.
3. If you want to acknowledge events by type, right-click within the Current Events window, and then click one of the following options:
 - Clear All Events
 - Clear Informational Events
 - Clear Node Up Events
 - Clear Node Down Events

Viewing a Detailed Log of All Events or Events during a Specific Period

Acknowledging an event removes it from the Current Events window, but it does not remove the event from the SolarWinds Network Performance Manager database.

To view events in the database:

1. Click **Events > Event Details**.
2. Click **Past Events** in the lower left of the Events window.
3. Specify the time period for which you want to display events.
4. Specify the event categories you want to display.
5. Specify the network objects for which you want to display events.
6. Click **Search**, and then review the events.

Note: SolarWinds Network Performance Manager keeps events in the database for the number of days specified on the Database tab of the Network Performance Monitor Settings window. For more information, see “Modifying System Settings” on page 189.

Viewing a Summary of Logged Events

Toolset Network Performance Monitor provides a summary view of all currently unacknowledged events. This view is not constrained to the Toolset Network Performance Monitor window and does not minimize with the Toolset Network Performance Monitor window, allowing you to keep your eye on your network events as you continue to work on other issues.

To launch the Network Events Summary:

Click **Events > Event Monitor**.

Note: To acknowledge an entire category of events, click the acknowledge icon (x).

Understanding Views

Views provide a number of ways to analyze your realtime data. A view consists of network object information provided in an easily scanned table that reflects the most recently collected data. Toolset Network Performance Monitor provides over 20 predefined views created with the help of network engineers in the field. If you do not find a view that meets your needs, you can quickly and easily create custom views.

Predefined views provide the appropriate data about all the objects that match the purpose of the view. For example, you will not find CPU load information in the interface errors and discards view, just as you will not find errors and discard information in the CPU load table. Consider the following list of predefined views:

- Buffer Errors this Hour
- Buffer Errors Today
- CPU Load
- Current Packets per Second
- Current Packet Size
- Current Traffic
- Errors and Discards this Hour
- Errors and Discards Today
- Fast Polling Status for all Nodes
- Interface Bandwidth Settings
- Interface Polling Intervals

- Interface Status
- Interfaces
- IOS Image and Version
- Maximum Traffic Load
- Memory Utilization
- Node Polling Intervals
- Node Status
- Nodes View
- Percent Utilization
- Response Time
- SNMP Community Strings
- Volumes

Viewing Realtime Data

Views provide a valuable, easily scanned, table-based view of your network objects.

To display a view:

1. Click **View > Display View**, and then select the view you want to display.
2. ***If you want to rearrange the column in a view***, drag and drop the column to the desired location.
3. ***If you want to sort on a specific column***, click the column heading.
4. ***If you want to take action on an object displayed in a view***, right-click the object and select an available action.

Creating Views

Creating new views provides you with an easy way to get the information you need displayed in a dynamic and easily consumable format.

To create a new view:

1. Click **View > New View**.
2. Type the name of the new view in the **View name** field.
3. Check the properties you want displayed in your view, and then click **OK**.

Printing Views

You can print entire views or selectively include columns.

To print a view:

1. Arrange the columns and sort the view as you expect to print it.
2. Click **File > Print**.
3. Check the columns you want to include, and then click **OK**.

Exporting View Data

You can export view data in a number of other formats:

- Comma-Delimited Text
- Plain Text
- HTML
- MHTML
- Excel
- Image

To export a view:

1. Arrange the columns and sort the view as you expect to export it.
2. Click **File > Export**.
3. Check the columns you want to include, and then click **OK**.

Note: Export to Excel Spreadsheet saves an XLS file. Export Directly to Microsoft Excel saves and then opens the file in Microsoft Excel.

Viewing Charts

Toolset Network Performance Monitor provides a number of charts for viewing both object-wide summaries and specific object statistics.

To view a chart:

1. Navigate to the appropriate location in the tree pane. For example, to view a summary chart, expand **Summary Charts**. To view a chart for a specific SNMP enabled node, expand the node, and then expand the category of the property, for example, expand **CPU Load and Memory Use**.
2. Click the chart you want to view.

Notes:

- You can zoom into a section of a chart by drawing a bounding box around the area of interest.
- To ensure the most up-to-date data is reflected in the chart, click **Autorefresh** (). Autorefresh also returns the chart to the default state.
- Select or specify a time period by clicking the appropriate tab below the chart. Click **Custom Period** to specify a time period not included as a tab.
- If your chart contains data generated prior to data summarization, you will see a single value for minimum, maximum, and average values. After summarization, this data is available as two distinct values.

Customizing Charts

Numerous chart customizations are available to ensure your charts display what you want in the detail you want.

To customize a chart:

1. Open the chart you want to customize, and then click **Custom** in the toolbar.
2. Specify the customizations you want on the different tabs, and then click **OK**. For example, you can change the number of places beyond the decimal point to display in the Numeric Precision grouping of the General tab.

Exporting Charts

You can export charts in a number of different formats.

To export a chart:

1. Open the chart you want to customize, and then click **Custom** in the toolbar.
2. Click **Export**.
3. Specify the appropriate format, destination, and size, and then click **Export**.

Adding Value Tables to Charts

You can add a table of data along the bottom of the chart by clicking **Table** in the toolbar. The values displayed in the table depend on the viewed chart. For example, adding the table to a Min/Max Average CPU Load provides a table of minimum CPU load, maximum CPU load, and average CPU load. Values in the table are aligned with the time displayed at the bottom of the chart.

Understanding Alerts

Toolset Network Performance Monitor generates alerts for network events you want to monitor. You can customize alerts in many ways:

- Notify different people on different days
- Notify at different times of the day
- Notify different people for different events
- Notify using any combination of times, events, and people

You can set alerts to notify people or other monitoring programs using several different modes:

- Send an e-mail or page
- Play a sound on the NPM machine
- Log details to a file
- Log details to the Windows Event Log
- Send a Syslog message
- Execute an external program
- Execute a Visual Basic script

- E-mail a web page
- Change the value of a interface or node property
- Play a text to speech output
- Send a Windows Net Message (net send)
- Dial a Paging or SMS Service
- Send an SNMP trap
- Post a URL to a web server

Creating an Alert

Complete the following procedure to create an alert based on events in your network.

To create an alert:

1. Click **Alerts > Configure Alerts**, and then click **New Alert** on the Configure Alerts window.
2. Type the name of the alert you want to create, and then check **Enable this Alert**.
3. Click Property to Monitor, and then check the property you want to monitor. You can alert on only one property at a time.
4. Click Monitored Network Objects, and then check the appropriate monitored object.
5. Click Alert Trigger, and then specify the appropriate trigger and reset values. Values are based on the property you choose to monitor. For example, if you check **IP Address** for a node, there are no selectable alert triggers. Toolset Network Performance Monitor notifies you when the IP address changes. If you check **Received bits per second** for an interface, you can select a threshold and another threshold at which the alert resets.
Note: When an Alert triggers, the trigger action is not repeated until the reset condition has been satisfied.
6. Click Time of Day, and then specify the time when the alert should trigger, including days of the week.
7. Click Alert Suppression, and then specify the appropriate alert suppression settings. Selecting one of the suppression options provides the ability to add conditions under which alerts are suppressed.

8. Click **Actions**, and then click **Add Alert Action** and add the actions you want to trigger for this alert, for example, sending a page. The **Actions** tab allows multiple actions for a single alert. Depending on the action selected, Toolset Network Performance Monitor prompts you for more information. For example, when configuring an email alert, you are prompted for the email addresses, the email address to use in the **From** field, the SMTP server address and port, the message, and the reset message.

Notes:

- Some pager systems require a valid reply address in order for the page to complete.
- To suppress the e-mail for either the alert trigger or reset condition, remove the text from the subject and message fields on the corresponding tab.
- When emailing a website link, you must specify the URL for the website and any required user ID and password in the corresponding trigger and reset tabs.

Testing an Alert Action

You can test alert actions to ensure appropriate configuration.

To test an alert:

1. Click **Alerts > Configure Alerts**, and then click **Test Alert** on the **Configure Alerts** window.
2. Select the network object on which you want to trigger the alert.
3. Select the alert you want to test, and then click **Test Alert Trigger** or **Test Alert Reset**.
4. Review the **Alert Error Log** and modify the alert actions, if necessary.

Note: To edit a tested alert, you can double-click on the alert name in the display.

Editing an Alert

After creating alerts, editing to correct alert action issues or to update time periods or any other property is a simple task.

To edit an alert:

1. Click **Alerts > Configure Alerts**, and then select the alert you want to edit on the Configure Alerts window.
2. Click **Edit Alert**, and then update the property you want to modify.
3. Click **OK**, when you have updated the alert appropriately.

Copying an Alert

After configuring an alert the way you want it to behave, consider using it as a template for other alerts. For example, you might not want to have an alert fire during work hours. To create this alert, you already had to create all of the suppression, alerting, and reset features and exclude the 9 to 5 weekday time period. Using the ability to copy this alert, you can easily change only the Time of Day tab to update and include the entire weekend. You might also consider creating disabled template alerts that contain working email alerts, to avoid having to enter the SNMP information over and over. Or, you might want to notify a different individual on different days. All of these scenarios can take advantage of copying an alert.

To copy an alert:

1. Click **Alerts > Configure Alerts**, and then select the alert you want to edit on the Configure Alerts window.
2. Click **Copy Alert**, and then update the properties you want to modify.
3. Click **OK** to save the copy of your new alert.

Viewing Current Alerts

The Active Alerts window provides an easily sorted table view of your current alerts, that is, alerts that have not met reset conditions.

To view current alerts:

1. Click **Alerts > Active Alerts**.
2. Select a category by which you want to group alerts, either Type of Alert or Node.

Note: Clicking a column head causes the alerts to be sorted by that column.

Disabling an Alert

When trouble shooting a device, it is easy to disable an individual alert or all alerts, especially if the actions become cumbersome.

To disable an individual alert:

Click **Alerts > Configure Alerts**, and then uncheck the alert you want to disable.

To disable all alerts:

Click **Alerts > Configure Alerts**, and then check **Temporarily Disable all Actions for All Alerts**.

Note: Alerts continue to be recorded in the log and displayed in the Active Alerts window.

Deleting an Alert

Deleting an alert permanently removes it from the system. If you want to retain the configuration, consider disabling the alert instead of deleting it entirely.

To delete an alert:

Click **Alerts > Configure Alerts**, and then click **Delete**.

Understanding Alert Suppression

Error conditions in a network can trigger multiple alerts from a single event. Likewise, some network issues may not need to trigger an alert if they occur alone, but should if present with other conditions. Alert suppression allows you to create conditions that take into account complex situations, and alert you with the information you need to determine the root cause of the problem.

By design, alert suppression is not configured by default. Before enabling alert suppression, review the following guidelines:

- Give considerable thought to each scenario and the ways in which alert-triggering events can occur
- Work with a diagram of your network
- Extensively test any scenario to which you apply suppression.

Proceed with caution when configuring the alert suppression. It is possible to suppress important alerts on the status of your network.

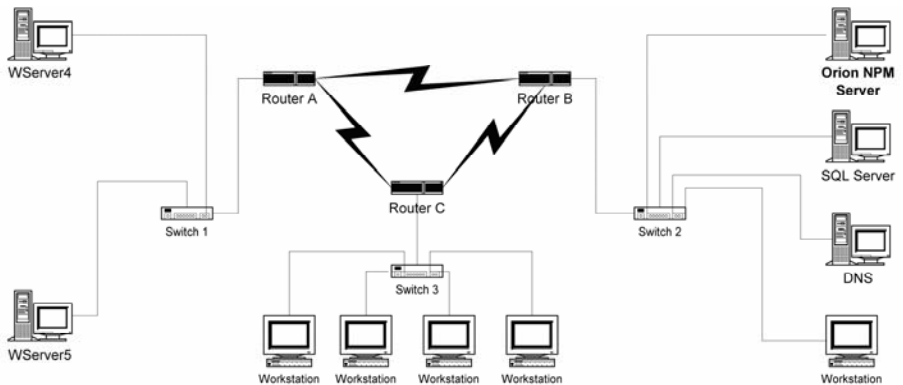
There are two choices for activating Alert Suppression:

- Suppress the alert if *any* of one or more conditions exist
- Suppress the alert if *all* of two or more conditions exist

Review the following scenarios for help with understanding when to create alert suppression rules. The location of the Toolset Network Performance Monitor computer is integral to these examples.

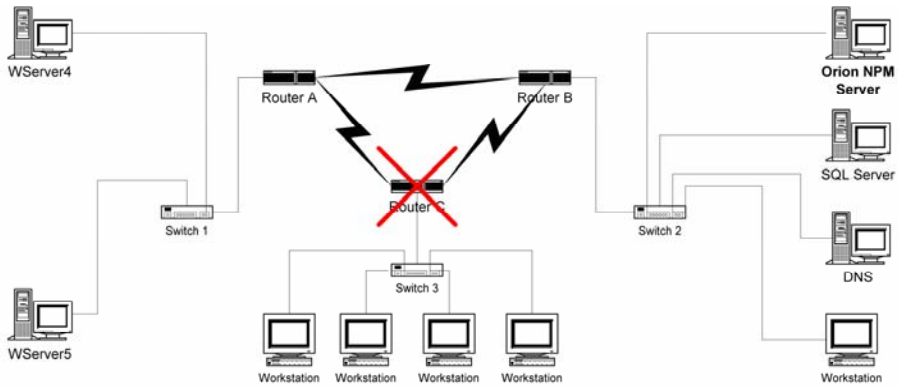
Failure of Redundant Servers

Review the following diagram. Both WServers—are identical in order to provide failover, redundancy, and load balancing. If WServer4 fails and the other is still functioning, you may want to be alerted immediately during business hours, but not paged in the middle of the night. In this case, configure the alert for the failure of one WServer to be suppressed unless the other also fails.



Apparent Failure of Dependent Nodes Downstream of a Failed Device

In the following diagram, dependencies exist among devices. If Router C fails, Switch 3 and all four Workstations become unreachable by NPM. You want to know that the Workstations have failed, but only if Router C and Switch 3 have not failed. Configure the alerts for failure of the Workstations to depend on Router C and Switch 3 being operational.

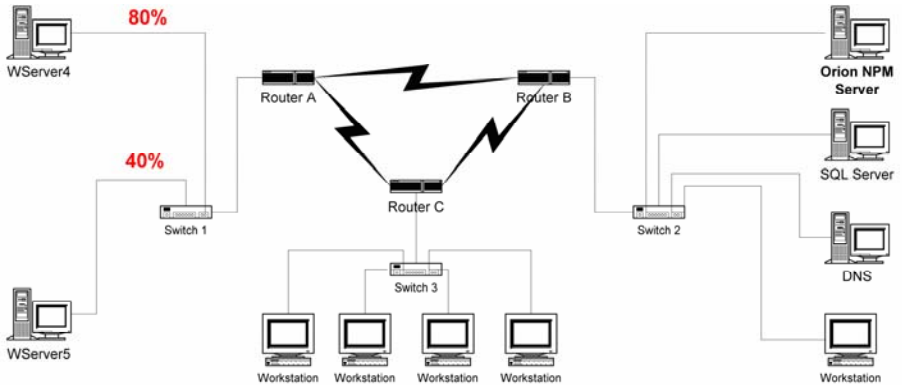


Failure of a Network Link when a Redundant Link Remains Functional

In reference to the previous diagram, during some hours, you may want to be notified of the failure of the link between Router B and Router C only if the alternative link through Router A is also down.

Failure of Load Balancing between Devices

If you configured your network to balance traffic across your web servers, consider configuring an alert that notifies you of very high CPU utilization only if one or more is experiencing much lower usage.



Note: The suppression of Alerts does not preclude knowledge of critical events. Network events will still be logged in the database whether or not alert suppression is enabled.

Dependent Node Alert Suppression Example

Within this example, an assumption is made that you have configured an alert which notifies you when nodes on a subnet go down. In this specific case, you configured an alert to notify you when workstations on a segment of your network on the other side of a particular router are unavailable. You only want to be alerted to Node failures if the router is still operational.

Note: The router should not be included in the group of monitored objects. The failure of the router is the trigger for suppressing the alert. Create another alert to be notified of the failure of the router

To configure dependent node alert suppression:

1. Configure an alert that triggers on failure of devices downstream of the router that serves the subnet (a Node Down Alert). Downstream is relative to the location of the computer running Toolset Network Performance Monitor.
2. Click **Suppress this Alert if ANY of the selected Suppressions are Active** on the Alert Suppression tab.
3. Click **Add**.
4. Select the property you want to monitor, in this example, **Node Status**. You can select only one property per suppression condition.

5. Click the Network Object tab, and then select the router between NPM and the subnet for which you have configured the Node Down Alert. The object types available on the Network Object tab depend upon the choice you have made on the Properties to Monitor dialog. If you had chosen to monitor an interface-related property, you would see a list of available Interfaces. Since you chose a node-related property, Toolset Network Performance Monitor presents a list of nodes.
6. Click the Suppression Trigger tab, and then check **Down**, **Warning**, and **Unknown** from the list and click **OK**.
7. Check the newly created suppression condition. Suppressions are not turned on automatically.
8. If you want to add another condition, repeat this procedure starting with **Step 3**.

Failure of Load Balancing Alert Suppression Example

If you have multiple servers configured to load balance your website, knowing that load sharing is not performing as it should is very important to site stability. Within this example, an assumption is made that you want to be alerted when the CPU load on two servers exceeds 80 percent, but only if one shows a CPU load of 40 percent or less. The alert is suppressed if the second server reports greater than 40 percent utilization.

You will need to configure two alerts, one for each server. These alerts are identical, except for the servers monitored.

To configure load balancing alert suppression:

1. Click **Alerts > Configure Alerts**, and then click **New Alert** on the Configure Alerts window.
2. Type a name for your alert in the **Name of Alert** field.
3. Click the Property to Monitor tab, and then check **% CPU Utilization** in the Node Statistics section of the tree.
4. Click the Monitored Network Objects tab, and then check the server you want to monitor.
5. Click the Alert Trigger tab, and then enter the percentage you want for Alert and Reset triggers. Type 80 percent to follow the scenario.
6. Click the Time of Day tab, and then select time of day parameters, if necessary.
7. Click the Alert Suppression tab, and then click **Suppress this Alert if ANY of the selected Suppressions are Active**.
8. Click **Add**.

9. Check **% CPU Utilization** on the Property to Monitor tab.
10. Click the Network Object tab, and then check the second server of the load balanced pair.
11. Click the Suppression Trigger tab, and then select **Greater Than** and type 40 in the text-entry field
12. Click **OK**.
13. Check the newly created suppression condition to activate it.
14. Repeat the procedure, but reverse the server choices made at **Steps 4 and 10**.

Realtime Interface Monitor

The Realtime Interface Monitor simultaneously displays numerous statistics from routers and switches. You can select from over 30 statistics grouping which include over 400 standard and proprietary statistics. Consider the wealth of information provided in the following list of statistics groups:

- Traffic
- Interface/Port status
- Broadcast/Multicast
- Errors/Discards
- Interface/Port configuration
- Time data was last Received/Transmitted
- ARP cache
- Ethernet statistics
- Ethernet collisions
- Token ring statistics
- ATM AAL5 traffic
- Frame relay configuration
- Frame relay traffic
- DS1 line status
- DS1 last 15 minutes snapshot
- ADSL configuration
- AppleTalk configuration

- 802.11 access point configuration
- 802.11 access point power levels
- 802.11 frame rates
- 802.11 access point last client
- 802.11 access point antennas
- Wireless clients (Cisco APs)
- Wireless access point SSID (Cisco APs)
- Wireless bridges and repeaters (Cisco APs)
- ISDN line configuration
- Traffic rates (Cisco only)
- Queue errors (Cisco only)
- Slow vs. Fast switching
- Protocols (Cisco only)
- IGRP settings
- Cisco discover protocol

All of these groups contain statistics specific to the grouping and baseline the statistics, when appropriate. For example, in the Traffic grouping, the receive and transmit percent utilization statistics need a baseline before they can be displayed. Baselining is automatic. Updates to statistics occur every 30 seconds, by default.

Beginning to Monitor Interfaces on Your Device

Realtime monitoring requires an SNMP community string. If you want to modify an interface, for example, enable or disable an interface, you need to provide a read-write community string or SNMP v3 credentials.

To begin monitoring interfaces:

1. Click **Select device**.
2. Specify the appropriate information on the Device Credentials window, and then click **OK**.
3. Click **Monitor**.
4. Select the statistics you want to view from the Statistics Group list.

Modifying Statistics Update Intervals

If you want to extend or shorten the statistics update intervals, keep in mind that shortening the interval causes more traffic and more load on your monitored devices.

To modify statistics update intervals:

1. Click **File > Settings**.
2. Click the General tab, and then adjust the slider in the Statistics Update Interval grouping.
3. Click **OK**.

Enabling Synchronous SNMP Queries

You can improve the performance over a WAN and improve the refresh rate of the data provided on the Realtime Interface Monitor window by allowing synchronous SNMP queries. Though, this may also cause increased CPU load on some routers and switches.

To enable synchronous SNMP queries:

1. Click **File > Settings**.
2. Click the General tab, and then check **Execute Synchronous SNMP Queries to the Target Device**.
3. Click **OK**.

Customizing Statistics Groups

Realtime Interface Monitor allows you to create your own statistics groups, providing you with the ability to create a single view that encapsulates all the information you know you want to see most often. This also limits the load imposed on your device by switching between statistics groupings.

To create or edit a statistics group:

1. Click **File > Settings**.
2. Click the Statistics Groups tab

3. If you want to modify an existing statistics group, complete the following procedure:
 - a. Select the group you want to modify, and then click **Edit Selected Statistics Group**.
 - b. Check the statistics you want to add to the group in the left pane.
 - c. Click **OK**.
4. If you want to create a new statistics group, complete the following procedure:
 - a. Type a name in the New Statistics Group field, and then click **Add Group**.
 - b. Check the statistics you want to add to the group in the left pane.
 - c. Click **OK**.
5. Click **OK**.

Note: Renaming, Deleting, and Resetting groups to their defaults can also be accomplished on the tab.

Exporting, Printing, and Copying Statistics

While monitoring a device, Realtime Interface Monitor allows you to transfer statistics to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Statistics

To export statistics group results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Statistics

To copy the statistics:

Click **Edit > Copy**. If you want to copy all the statistics, consider clicking **Edit > Select All** before copying the statistics.

Printing Statistics

To print statistics group results:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

Realtime Interface Monitor statistics can be published to a static HTML page containing all the statistics for a specific statistics group.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Automatically Publish Discovered Information in HTML

The Realtime Interface Monitor tool allows you to automatically generate an HTML file that contains the monitored statistics on a timed schedule. For example, you can save this report to your inetpub root directory and provide an automatically refreshing list of statistics on your website.

To enable automatic HTML publishing:

1. Click **File > Settings**.
2. Click the Auto-Publish tab, and then check **Enable Auto-Publishing to the Web**.
3. Specify the name and directory to which you want HTML files saved.
4. Specify the publishing interval.
5. Click **OK**.

Router CPU Load

Router CPU Load monitors the CPU load on Cisco routers in realtime. Each router is shown as a horizontal bar comprised of the current load and the high-water mark. Router CPU Load also provides the ability to generate popup alert messages whenever router load goes over a user-defined point and the ability to print the current load for all routers.

Getting Started

You can add numerous routers to your Router CPU Load user interface.

To monitor CPU load:

1. Click **Bar > Add New CPU Load Bar**.
2. Type the router IP address in the Target Router field.

3. Type the read-only or read-write community string for the router in the Community String field.
4. Select a poll time:
 - An average load over the last 5 minutes
 - An average load over the last minute
 - Realtime allows you to select a polling time from 1 to 60 seconds.
5. Select the name you want displayed for the monitored router:
 - The SysName of the router
 - A name you specify

Setting Polling Options, Notification, and Logging

Polling options setup the following options and features:

- Caution and warning levels for detected CPU loads
- SNMP timeout and number of attempts
- Notification types
- Logging

To modify options:

1. Click **Option > Polling Options**.
2. Click the Polling tab, and then select thresholds for the caution (yellow) and warning (red) levels. When the CPU load surpasses the value, the bar changes color.
3. Click the SNMP tab, and then specify the following values:
 - Select the number of milliseconds the tool should wait for an SNMP reply before assuming the packet was lost and trying again.
 - Select the number of times the tool should retry an SNMP query before giving up. This should normally be set to 2.

4. Click the Notification tab, and then check the notifications you want when the router exceeds the thresholds set on the Polling tab:
 - Check **Popup on alarm** to restore the tool from minimized mode when a threshold is exceeded
 - Check **Beep on alarm** to generate a system beep when a threshold is exceeded
 - Check Open Notification window on alarm to specify messages for exceeding caution and warning thresholds
5. Click the Logging tab, and then check Logging Enabled to specify a text log file and an interval at which to log CPU load on monitored routers.

Immediately Polling Monitored Routers

If you need the current status of your monitored routers, you can collect current state by immediately polling.

To immediately poll routers:

Click **Bar > Poll all routers now**, or right-click the bar that corresponds to the router you want to immediately poll and click **Poll**.

Setting All Routers to a Specific Poll Interval

You can quickly set all monitored routers to be polled at the same interval.

To set all monitored routers to the same polling interval:

Click one of the following options:

- Bar > Set all bars to 5 minute decaying average
- Bar > Set all bars to 1 minute decaying average
- Bar > Set all bars to realtime

For more information, see “Getting Started” on page 64.

Viewing Peak Load High-Water Marks

To view the high-water peak, peak load of a specific monitored router, mouse over the bar. A tooltip provides the exact time-date stamp and peak percentage of the high-water mark.

Resetting High-Water Marks

Router CPU Load provides at-a-glance high-water or max polled value markers within the monitored router bar. When you have corrected an issue, consider resetting your high-water marks to see how changes made affect your maximum CPU loads.

To reset high-water marks:

Click **Bar > Reset peak markers**.

Printing CPU Loads

You can print current CPU loads, if necessary. Printouts include the current load and the high-water marks, including the date and time of the peaks.

To print current CPU loads:

Click **File > Print**.

Saving Loaded Routers

After loading a number of routers you want to monitor frequently, consider saving the loaded information as a unique profile.

To save a loaded router profile:

Click **File > Save Profile**, and then name and save the router profile.

Loading a Saved Router List

If you have taken advantage of the ability to save profiles, complete the following procedure to load your saved profiles.

To load a router profile:

Click **File > Load Profile**, and then select the router profile you want to load.

Deleting All Monitored Routers

If you need to delete the routers you have added to the Router CPU Load tool, complete the following procedure.

To delete all currently monitored routers from the tool:

Click **Bar > Delete all bars**.

Troubleshooting Router CPU Load

If you get an error message like "xxx does not support the Cisco AvgBusy MIB or is not responding to SNMP polls", then you probably need to reconfigure your router. Add the following lines to your Cisco router configuration file:

```
snmp-server community public RO
snmp-server community secret RW
```

These lines enable SNMP on your router. Of course you will want to put your own read/write community string in place of *secret*.

If SNMP is already configured on your router, look for a line in the configuration file similar to this:

```
snmp-server community public RO 60
```

The 60 at the end of this line is referring to an access list.

You need to do one of the following:

- Add your Router CPU Load tool computer IP address to the access list
- Add your entire range of internal IP addresses
- Remove the access list entirely

Ensure you do not have a firewall between you and your router that blocks SNMP.

SNMP Realtime Graph

SNMP Realtime Graph provides realtime data collection and graphing, allowing you to graph data from any management information base (MIB). By selecting the device and the desired OID (Object ID), you can monitor a number of parameters, including:

- Traffic
- CPU processor load
- Voltage on a power plant
- Unique user per web server
- Temperature
- VoIP Traffic

If you can access a device using SNMP, the SNMP Graph tool allows you to graphically monitor and view the statistics of that OID. The monitored SNMP OID can be from a standard MIB or a proprietary vendor MIB.

Graphing an OID Value

SNMP Graph is one of the most powerful and flexible monitoring tool available. It is hardware independent and capable of graphically displaying statistics from any device that supports SNMP and has a valid MIB OID. This tool uses the extensive MIB database of thousands of standard and vendor MIBs, but can also monitor SNMP variables that are NOT in the SolarWinds MIB database.

To begin seeing your OID values in a rich, graphical representation, complete the following procedure.

To start graphing your values:

1. Click Graph > Add MIB to Graph.
2. Provide the appropriate information on the New SNMP MIB variable to Graph window:
 - IP address or hostname (this device must support SNMP)
 - SNMP community string (read or read-write)
 - SNMP MIB variable to monitor
 - o Type the name of the MIB, for example, RFC1213-MIB:ifInOctets
 - o Type the OID of the MIB to monitor, for example, 1.3.5.1.2.1.2.2.1.10
 - o Click **MIB Browser** and select a MIB from the tree
 - o Click **MIB Browser** and then click **Search MIB Tree**: search by OID, name, or description
 - Units and calculation
3. ***If more than one index is found***, check the indexes you want to graph, and then click **OK**.

4. Wait as the tool establishes a baseline. This can take up to a minute.

Notes:

- Monitored OID elements display in a table below the graph, while the realtime results display in the graph. If different types of data were selected, multiple axes will be displayed on the left.
- SNMP Graph has the ability to monitor dissimilar data at the same time on a single chart. For example, you can monitor router CPU processor load in percent utilization on the same chart as traffic in bits per second. You can also monitor the number of unique users on a web server at the same time you monitor total traffic downloaded or response time.

Modifying Polling Settings

Polling interval settings help you ensure you receive the information you need, even when connected over less than optimal conditions. You can increase the polling interval and retries when conditions are poor and decrease the interval and retries during optimal bandwidth conditions.

To modify polling settings:

1. Click **File > Settings**.
2. Click the SNMP Polling tab, and then adjust the interval, timeout, and retries settings.

Note: Normally the timeout setting should be set at 2500 milliseconds and the retries at 2 attempts. If you are monitoring a very remote device, over 20 hops away, you may need to increase the timeout delay or retry frequency to overcome network delays.

Changing the Columns in the OID Table

Below the graph created when monitoring an OID, SNMP Graph displays a chart of the current element statistics. You can modify the realtime data shown in this table.

To change OID table columns:

1. Click **File > Settings**.
2. Click the Displayed Columns tab, and then modify the list of included columns. The up and down arrows can be used to modify column order from left to right.

Calculating Counter Rollovers

Depending on the monitored device and OID, statistical information may be derived from 32-bit counters. These counters offer a maximum value of 2 to the 32nd power (4,294,967,296). You can decide how Toolset Network Performance Monitor compensates when a 32-bit counter reaches maximum capacity and rolls over to zero. The default method detects a counter rollover and ignores the zeroed value. Instead, a new sample is scheduled in 20 seconds. This method can cause slightly skewed total bytes transferred numbers.

The more advanced method, which produces skewed numbers when manual counter resets occur, detects a counter rollover and uses the following calculation to correct for the rollover to zero: $\text{currentValue} + (\text{maximumCounterValue} - \text{lastCounterValue})$. If manual counter resets are rare, this method produces the most accurate results.

To modify counter rollover behavior:

1. Click **File > Settings**.
2. Click the Counter Rollover tab, and then select a counter rollover method.

Customizing Graphs and Automatically Generating HTML

SNMP Graph offers a wide variety of customization options for your graph. Any changes made to the graph displayed locally are automatically applied to the HTML generated when utilizing the publish to web option.

To customize the look and feel of your graph:

1. Click **Graph > Customize Graph Style**.
2. Specify the changes you want to make on the appropriate tabs.

Titles

Allows you to automatically or manually create a title for the graph. You can enter a main title as well as a subtitle. The footer section allows you to place text at the bottom of the page. Use | separators to create columns. For example, typing South Central NOC|USGS|Trigger Counter in the Main Title field generates a left-aligned South Central NOC, center-aligned USGS, and right-aligned Trigger Counter.

Style

Allows you to disable the table displayed at the bottom of the page. You can also specify the number of decimal points to be displayed. Data is always stored at the highest level of detail but can be displayed at only two decimal points. You can also use the slide bar at the bottom of this window to display the number of data points to be displayed when in Zoom mode.

Axis

Allows you to color-code axis to make it easier to identify which data corresponds to which axis. This window can also be used to change one monitored attribute from a line graph to an area or ribbon graph. Many customers find it useful to use trend lines when reviewing data for trending purposes.

The default is to display the data as Overlap Axis. This means dissimilar elements are displayed on the same chart, for example, BPS and Processor Load. Uncheck this box to view data on two separate charts, one above the other.

OIDs

Allows you to modify the line color, line style, and description of the element being graphed.

Polling

Allows you to log realtime data to a comma-delimited text file. Adjust the slider to select the frequency with which to collect the data.

Auto-Publish

Allows you to automatically create and publish charts to an HTML web page in realtime. If you save this file to your web server, you can view the results of the SNMP Graph from any browser.

Colors

Allows you to create templates for displaying your results. You can customize any template or create your own profile of colors and backgrounds for SNMP Graphs.

Fonts

Provides the ability to increase or decrease the default font size used by the graph.

Viewing Raw Data

Raw data is collected and viewable at anytime. This data is the exact data collected from the counter being monitored.

To view raw data:

1. Click **Graph > View Raw Data**.
2. Review the table of data.

Exporting, Copying, and SNMP Graph Results

You can transfer graphs and data to other tools through exporting and copy and paste capabilities. You can also print monitored information.

Exporting Graphs and Data

To export graphs and data:

1. *If you want to export the graph image*, click **File > Export Graph**, and then select the type of export.
2. *If you want to export the data*, click **File > Export Data**, select the type of export, and then check the information you want to export.
3. Specify the name and path for the exported information.

Copying Graphs and Data

To copy graphs and data:

If you want to copy graphs, click **Edit > Copy as Bitmap** or **Edit > Copy as Windows MetaFile**.

If you want to copy raw data, click **Edit > Copy Raw Data**.

Printing Graphs

To print graphs:

Click **File > Print**.

Publishing SNMP Graph Results in HTML

If you want to generate an HTML page of your SNMP Graph results, you have two options.

- To create an automatically refreshing page, see “Customizing Graphs and Automatically Generating HTML” on page 228.
- To create a single static page, click **File > Export to Web**, and then specify the name and directory for your file.

Zooming

You can use the left mouse button to zoom in on any section of a graph. While holding the left mouse button, drag the cursor to the left or right. When you release the mouse button the tool will automatically "zoom" into this area of the chart. You can use the slider bar at the bottom of the chart to advance forward or backward in time on the chart. This feature is fully interactive and the tool will continue to collect and log data while you are zoomed into the results. Right-click and select **Zoom Back Out** to return to normal viewing.

Customizing the OID

During monitoring, you can customize the OID, updating units, calculations, the IP address, among other options.

To customize a monitored OID:

1. Click Graph > Customize Graph Style.
2. Click the OIDs tab, and then select the OID you want to customize.
3. Click the ellipses (...) next to the IP address or hostname.
4. Specify the changes you want to make on the Customize OID window. For example, you can update the community string.

Note: The **Units** field accepts functions. For example, the ifOutOctets.1 OID collects data in octets, but you can display the results in bps by entering the formula `bits=*8` in the **Units** field. This calculation takes the OID data in octets and multiplies it by 8 to show data in bits per second. To view the results in nibbles, change the formula to `nibbles=*2`, as one octet equals two nibbles.

Syslog Server

The Syslog Server listens for incoming Syslog messages on UDP port 514, decodes the messages for logging purposes, and stores the messages in a local database. If you have active maintenance and wish to report to a SQL database instead of Access, login to the SolarWinds website and go to Additional Components.

Though originally used specifically on UNIX systems for application, network, and operating system logging, numerous network devices can also generate Syslog messages. For details on enabling Syslog message on a particular device, refer to the vendor's documentation.

When a Syslog message is received, the Syslog Server adds the message to the Syslog database and displays the message.

Selecting Message Properties

Syslog Monitor allows you to modify a number of general properties, including the following:

- Display messages as they arrive
- Play a sound when a message is received
- Wordwrap messages
- Select the properties to display of the message itself.

To modify any of these properties:

1. Click **File > Settings**.
2. Click the General tab, and then select the options you want to enable or disable.
3. Click the Display Columns tab, and select the properties you want to display about Syslog messages.

Note: Modifying the properties viewed does not change what is stored in the database. The entire message is stored.

4. Click **OK**.

Designating the Number of Messages to Display

You can specify how many rows to display in the user interface. This does not limit the number of messages you save in your database.

To limit the number of displayed messages:

1. Click **File > Settings**.
2. Click the Display Rows tab, and select the number of rows to display in the user interface.
3. Click **OK**.

Clearing Messages from the Display

You can delete single messages from the user interface by clicking the **X** icon located to the far left of the message.

If you want to delete selected displayed messages, select the messages you want to delete, and then click **Edit > Clear Selected Messages**.

If you want to delete all displayed messages, click **Edit > Clear All Messages**.

Filtering Accepted Messages

If you only want to accept specific messages from devices sending Syslog messages, you can limit the messages accepted.

To filter the messages accepted by the Syslog Server tool:

1. Click **File > Settings**.
2. Click the Priority Filter tab, and then check the priorities you want to accept. For example, check **Emergency**.
3. Click the Facility Filter tab, and then check the facilities described within the message you want to accept. For example, check **user-level message**.
4. Click **OK**.

Sending Syslog Messages

You can use the tool to send Syslog messages to another Syslog server. This feature is commonly used to add messages manually to a remote Syslog database for testing reasons, during system upgrades, and while troubleshooting a network problem, among other reasons.

To send a Syslog message:

1. Click **Edit > Send Syslog Message**.
2. Type the hostname or IP address of the message target in the Target Hostname or IP Address field.
3. Select a facility from the list.
4. Select a priority from the list.
5. Type your message, and then click **Send**. Your message is sent on UDP port 514.

Searching the Syslog Server Database

To find older messages, messages that have been cleared from the display, or messages that are outside the row limit of the display, you can search the database. You can also use this functionality to display all the messages from a specific source, a specific priority or facility, among other uses.

To search the database:

1. Click **Edit > Search Syslog Database**.
2. Specify the information for which you want to search, and then click **Search**.

Note: You can use the asterisk (*) wildcard within search strings. For example, typing *bob* in the **Containing the following text** field finds all messages that contain bob.

Deleting Old Syslog Messages from the Database

The Syslog Server tool allows you to set an archival time after which messages are deleted from the database.

To set an archival time:

1. Click **File > Settings**.
2. Click the General tab, and then specify a time in the Database Archival grouping after which you want to delete data from your database.

Emptying the Syslog Server Database

It is possible to completely empty the Syslog Server database. If you are running out of file space, or you have received a large influx of messages that have no value, you may consider emptying the database.

To delete everything in the database:

Click **File > Purge Syslog Database**, and then confirm that you want to delete all the data.

Exporting, Printing, and Copying Messages

You can transfer messages to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Displayed Messages

To export messages:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Messages

To copy the messages:

Click **Edit > Copy**. If you want to copy all the statistics, consider clicking **Edit > Select All** before copying the statistics.

Printing Messages

To print messages:

Click **File > Print**, and then select the information you want to print.

Watch It

Watch It is an up-down network monitor. It can monitor numerous device-types, including the following:

- Servers
- Routers
- Websites
- Workstations

Watch It notifies you when network response time begins to degrade or when a device is down. Sounds can be played whenever a device drops packets, stops responding, and when a down device becomes active again.

To begin monitoring devices:

1. Specify the hostname or IP address of the device you want to monitor.
2. Click **Add Node**.
3. Click **OK** when you have added all the devices you want to monitor.

Notes:

- If Watch It is currently running, click **+/-** to add or remove devices.
- To reveal the Watch It user interface, mouse over the row of lights displayed on the right side of your desktop.
- Double-click any device to check the current response time.
- The response time of each device is monitored. When response time begins to deteriorate or the device begins dropping packets, the light beside the device turns yellow. The light turns red if the device stops responding.

Changing the audible alerts

Each time a device changes state, starts dropping packets, or response time degrades an audible alarm can be played.

To change audible alerts:

1. Mouse over the Watch It user interface.
2. Click **+/-**.
3. Select the device you want to modify.

4. Click the state for which you want to modify the sound. For example, click **Warning**.
5. Select a new sound, and then click **OK**.
6. Click **OK** on the Watch It Settings window.

Minimizing Watch IT

Click on the left corner of the UI and then select **Place Watch It in System Tray** to minimize Watch It to the system tray. While in the system tray, Watch It provides a single LED.

- Green light - all devices are responding
- Yellow light - one or more devices are dropping packets or response time is degrading
- Red light - one or more devices have stopped responding.

Chapter 7

Ping and Diagnostic Tools

The following sections provide detailed information about the Ping and Diagnostic tools included with the Toolset.

- “DNS Analyzer” on page 239
- “Enhanced PING” on page 249
- “Ping” on page 255
- “Ping Sweep” on page 257
- “Proxy Ping” on page 260
- “Send Page” on page 261
- “Spam Blacklist” on page 261
- “TraceRoute” on page 267
- “Wake-On-LAN” on page 273
- “WAN Killer” on page 275

DNS Analyzer

You can use the DNS Analyzer tool to visually display the hierarchy of DNS resource records, including name server, CName, and pointer. The relationships between multiple Name servers and target IP addresses are easy to distinguish using the DNS structure diagram. Redirections from one Name server to another are also shown.

Getting Started

DNS Analyzer queries your DNS servers and graphically represents the results.

To begin querying your DNS servers and generate your graphical analysis:

Type the appropriate information in the **Hostname, URL, or E-Mail address** field, and then click **Draw DNS Structure**.

Viewing Discovered DNS Details

You can view details about each node in the discovered structure.

To view the details pane:

Select the server you want more information about, and then click **Details** (🔍). The Details pane is displayed on the right side of the screen.

The Details pane provides the following information:

- Server details
- Question sent to the server
- Record type asked for
- Parent node details
- Records returned

Viewing Packet Details

You can view details about the packet sent between servers directly from the DNS diagram.

To view packet details:

Right-click on a link between nodes, and then click **Packet Details**.

DNS Analyzer Menus

File Menu

New Diagram

Clears the existing diagram

Open Diagram

Opens a previously saved diagram

Save

Saves the current diagram

Save As

Saves the current diagram to a new file

Export Diagram

Allows you to select an export format for the diagram

Send Diagram to

Allows you to select from a list of media type to which to send the diagram

Publish to Web

Exports the results to an HTML file

Print Setup

Opens the Print Setup dialog

Print Preview

Previews the results exactly the same as it would appear when printed

Print

Prints the current diagram

Settings

Opens the Settings dialog

Exit

Closes the DNS Analyzer

Edit Menu**Copy as Bitmap**

Copies the diagram as a bitmap to the Windows clipboard

Copy as Metafile

Copies the diagram as a Metafile to the Windows clipboard

Select All

Selects every object in the diagram

Delete Selected

Deletes the selected objects from the diagram

Hide

Hides the selected objects from the diagram

UnHide All

Returns all of the hidden objects to the diagram

Diagram Menu

Select

Allows you to select objects in the diagram

Pan

Allows you to pan the screen in all directions by clicking and dragging the mouse

Interactive Zoom

Allows you to zoom in and out by clicking and dragging the mouse up and down

Marquee Zoom

Allows you to select a zoom area by clicking and dragging the mouse around a specific area

Refresh

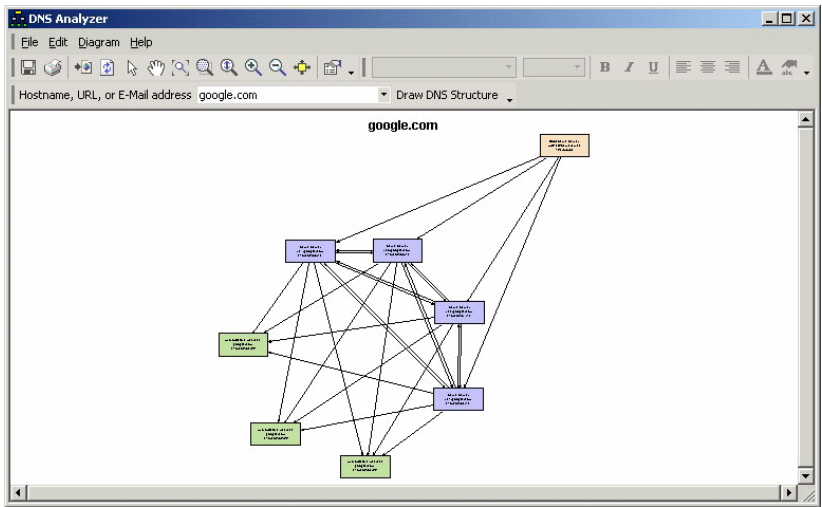
Rescans and redraws the current diagram

Zoom

Provides a number of different preset zoom options.

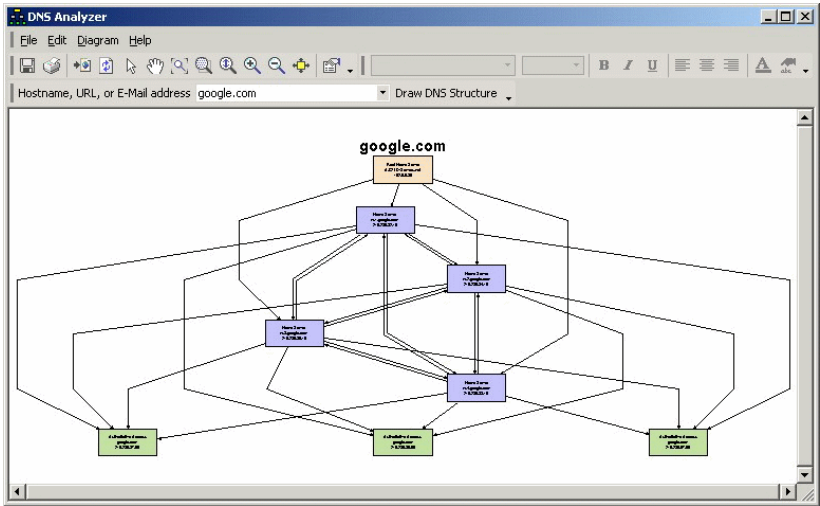
Auto Arrange – Circular

Rearranges the diagram in a circular pattern.



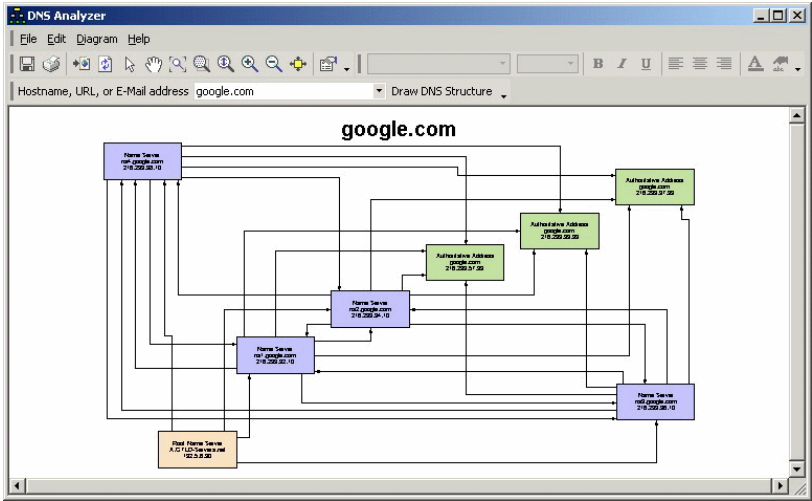
Auto Arrange – Hierarchical

Rearranges the diagram in a hierarchical pattern.



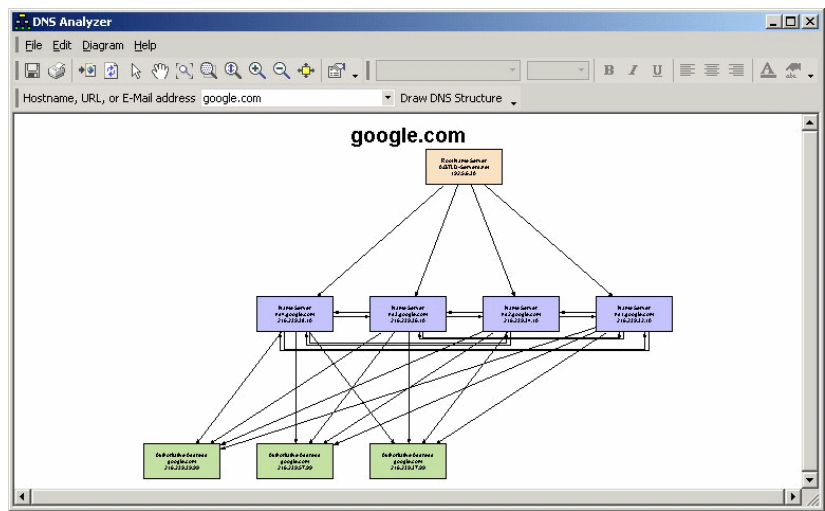
Auto Arrange – Orthogonal

Rearranges the diagram in an orthogonal pattern.



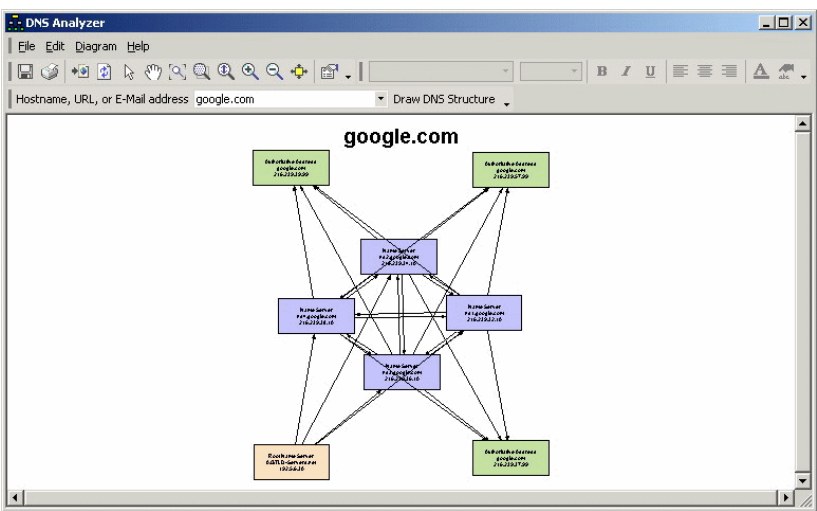
Auto Arrange – Tree

Rearranges the diagram in a tree pattern.



Auto Arrange – Symmetrical

Rearranges the diagram in a symmetrical pattern.



Auto Arrange - Reorganize

Redraws the diagram in the selected Auto Arrange style.

Auto Arrange - Auto Arrange Properties

Opens the Layout Properties dialog.

Auto Arrange - Arrange Labels

Automatically adjusts the label positions in the diagram.

Show Details

Opens the Details pane.

Adding Root DNS Servers

You can add root DNS servers to DNS Analyzer. Root name servers field requests for the root namespace domain and then direct further requests to the top-level domains. You can find a listing of root name servers at root-servers.org.

To modify the list of root name servers:

1. Click **File > Settings**, and then click the Root DNS Servers tab.
2. Type the name of the root name server you want to add in the **Add Name Server to List** field, and then click **Add Server**.
3. Click **OK**.

Modifying DNS Query Timeout

Depending on your network and bandwidth limitations, you may need to adjust the DNS query timeout.

To change the DNS query timeout:

1. Click **File > Settings**, and then click the Details tab.
2. Adjust the DNS Query Timeout scroll bar, and then click **OK**.

Deciding Whether to Lookup DNS Server Addresses

DNS servers may not always provide both the name and the address when providing information about other DNS servers. You can force another DNS lookup to retrieve the missing information, or you can accept the provided name or address.

To skip the resolution of names provided without addresses:

- 1. Click **File > Settings**, and then click the Details tab.
- 2. Check **Do Not Resolve Suggested Name Servers without Addresses**, and then click **OK**.

Understanding Colors in DNS Analyzer

Understanding the colors used in DNS Analyzer is integral to understanding your graphical DNS analysis. Consult the following table for a list of colors, designations, and definitions.

Color	Object	Definition
 Peach	Root Name Server	Represents the Root Name servers used to start the chain of queries. These are the first name servers queried during a DNS Analysis. You may change the Root Name servers in the settings dialog.
 Purple	Name Server	Represents a non-Top Level Domain name server which was referred to us by another name server.
 Yellow	CName	Represents a record returned from a Name Server that indicates that the target Hostname that we are querying for is really an alias for another Hostname.
 Aqua	MX Record	Represents a record returned from a Name Server indicating the hostname of the computer that is designated to receive Email traffic.
 Gold	Global Top Level Domain Servers (GTLD)	Represents Name Servers which are known to be at the top level of the internet naming system (DNS). GTLD Servers are typically used as the Root Name Server for DNS Analysis.
 Green	Authoritative Address	Represents a record returned from a Name Server containing the Authoritative IP Address for the request hostname. Authoritative indicates that the Name Server is the authority for the queried domain.

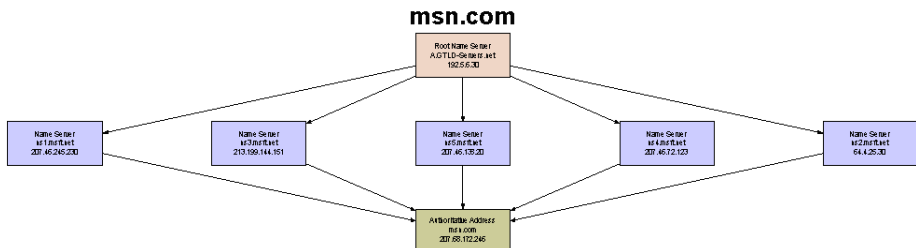
Color	Object	Definition
 Blue	Address	Represents a record returned from a Name Server containing an IP Address for the queried hostname. These record types are returned by Name Servers which have previously queried other Name Servers for the address, and have cached the answer.
 Red	Error	Represents an error during the Analysis. If a Name server fails to respond in the designated timeout period, an error node will be drawn with the description "Timeout". Other errors may include "Name Error", which indicates that the queried hostname does not exist.

Analysis Examples

The following examples illustrate common output for DNS Analyzer and a short description of the output.

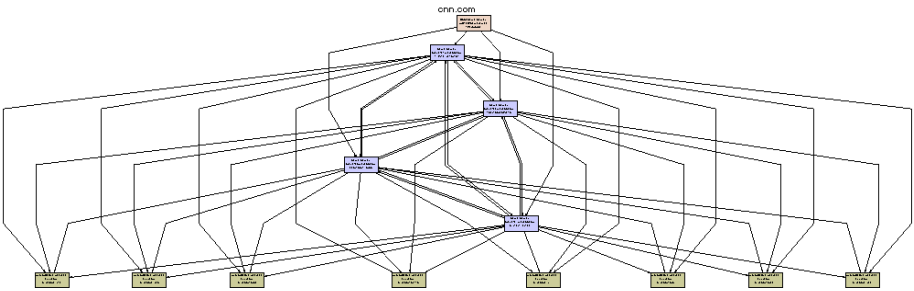
Example 1

The root name server is GTLD. The additional name servers are ns1.msft.net, ns3.msft.net, ns5.msft.net, ns4.msft.net, ns2.msft.net. All name servers point to one authoritative server. Msn.com does not appear to have any DNS issues.



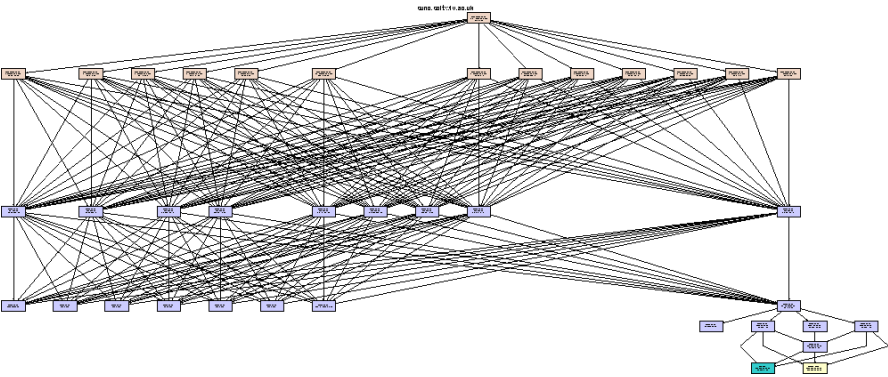
Example 2

The root name server is GTLD. The additional name servers are ns1.msft.net, ns3.msft.net, ns4.msft.net, and ns2.msft.net. All name servers point the authoritative servers. In this example, the DNS is hosted from 8 different servers.



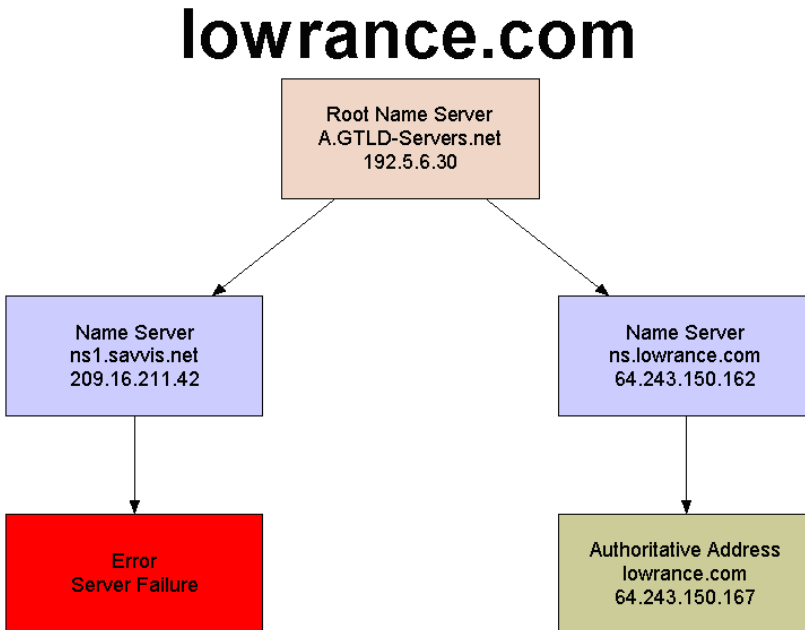
Example 3

There are 14 root name servers listed and 22 name servers. A non-authoritative address is found and an alias. The address is non-authoritative because it comes from the cache of the name server.



Example 4

In this example, there is an error reported from one of the Name Servers. This represents a time out issue.

**Setting a Node as the Root and Rescanning**

DNS Analyzer allows you to set a discovered node as the root of your DNS analysis, and then rescan and recreate your diagram.

To set a discovered node as your root:

Right-click the node you want as your root, and then click **Set node as Root and ReQuery**.

Enhanced PING

Enhanced Ping can be used to continuously monitor a number of servers, routers, workstations, or other devices and continually show real-time response time.

To immediately begin pinging multiple devices:

1. Click **Nodes > Edit Nodes**.
2. Type the name of the node you want to ping, and then click **Add Node**.

3. Repeat **Step 2** until you have added all the devices you want to monitor with the Enhanced PING tool.
4. Click **OK**.

Logging Your Statistics

The Enhanced Ping tool can log response times as they are collected. The log file is a plain text file. A new line will be added to the log file each time Enhanced Ping checks the response time of each node.

To log to a file:

1. Click **Nodes > Settings**, and then click the Logging tab.
2. Check **Enable logging of ICMP responses**, and then specify a destination and file name for the file in the **Log File** field.

Exporting Results

Using the export wizard, you are provided with a number of export options:

- Export in any of the following formats:
 - o Windows Metafile
 - o BMP
 - o JPG
 - o PNG
 - o Text only
- Export to any of the following destinations:
 - o Clipboard
 - o File
 - o Printer
- Export the object using the following width and height dimensions:
 - o No specific size
 - o Millimeters
 - o Inches
 - o Points

To export your results:

1. Click **File > Export Wizard**.
2. Specify the appropriate values, and then click **Export**.

Saving and Loading Profiles

To save time, especially if you often monitor the same set of devices with the Enhanced Ping tool, save your profile. This will ensure you can quickly load the profile and immediately start monitoring, instead of building a device list each time you start the tool.

To save a profile:

Click **File > Save Profile** or **File > Save Profile As**. If you have not previously saved this profile, you are prompted to provide a name and destination for the profile.

To load a profile:

1. Click **File > Load Profile**.
2. Select the profile you want to load, and then click **Open**.

Printing Results

To print your current graph, click **File > Print**.

Resetting Statistics

You can clear and recalculate the high and low response time statistics for all nodes by completing the following procedure.

To reset high and low statistics:

Click **Nodes > Reset High/Low Statistics**.

If you want to clear all the data and restart monitoring, complete the following procedure.

To reset all statistics:

Click **Nodes > Reset All Statistics**.

Customizing the Graph

There are a number of quick changes you can make to the look of your chart. You can simply select a different chart type:

- Step Chart
- Ribbon Chart
- Area Chart
- Vertical Bar Chart
- Horizontal Bar

To change the chart type:

Click **Chart**, and then select the chart type you want to view.

To add a response time table:

Click **Chart > Response Time Table** to add a table of response times at the bottom of the chart.

To select a different color palette for your chart:

Click **Chart > Palette**, and then select a color scheme.

To modify the colors used in the foreground and background of the chart and to designate your statistics:

Click **Chart > Set Colors**.

To view a full set of the customization options:

Click **Chart > Customize**, and then modify the chart.

Modifying Enhanced Ping Settings

Enhanced Ping allows you to modify ICMP polling intervals, ICMP timeout, packet time-to-live, and the data size and contents of the actual ICMP packet.

To modify settings:

1. Click Nodes > Settings.
2. Click on the Polling tab, and then specify the appropriate values:

Poll Interval

Allows you to change how often to check the response time of each node.

ICMP Timeout

Designates the amount of time to wait for a PING response before assuming the IP address is no longer responding. If you expect devices to respond quickly and would like any delays over 300 milliseconds to be flagged as a problem, then set the PING Timeout to 300 milliseconds. Enhanced Ping will assume PING responses taking longer than 300 milliseconds as lost.

Packet Time-To-Live

Allows you to specify the number of hops you allow during a trip to the specified IP address. With a setting of 32, your test could pass through 32 different routers before being thrown away by the network.

3. Click on the Packet Size tab, and then specify the appropriate values:

Data portion of ICMP packet

Allows you to specify the actual data included in the ICMP packet. You can type additional text in the window to increase the packet size or delete text to reduce the packet size. Most PING tests require only a small amount of data.

Zooming in on an area of the chart

Draw a box around any area of the chart to zoom in on it. When you zoom in, a scroll bar will appear on the bottom of the chart that allows you to scroll the chart right or left to display more data. Select "Zoom Out" from the "Chart" menu to return to the full view.

Ping

The Ping tool provides an alternative to the operating system PING utility. Ping sends ICMP packets to a target IP address and measures the response time and packet loss.

To ping a device:

Type the hostname or IP address in the appropriate field, and click the **PING**.

Exporting, Printing, and Copying Sweeps

After running a ping test, the Ping tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export results:

Click **File > Export**, and then specify the name and path for the exported information.

Copying Calculations

To copy the results:

Click **Edit > Copy**, this copies the entire result set to the clipboard. If you want to limit what is copied, select what you want to copy, and then click **Edit > Copy**.

Printing Calculations

To print results:

Click **File > Print**.

Modifying Ping Settings

Ping settings allow you to set the timeout, time-to-live, delay, and data portion of the ICMP packet sent to the target device. You can also specify whether Ping plays sounds while working.

To modify these settings:

Click **File > Settings**, and then specify the appropriate values:

PING Timeout

Designates the maximum amount of time in milliseconds that PING will wait for a response from the target IP address. If the target IP address does not respond within the number of milliseconds set here, PING will assume it is down.

Packet Time-To-Live

Designates the number of hops you allow along the way to the specified address. With a setting of 32, your PING test could pass through up to 32 different routers on the way to the remote address before being thrown away by the network.

Delay Between PINGs

Designates the time in milliseconds between each successive PING to the target address. Setting this value very low will send a constant stream of Pings to the target IP address.

Play sounds while PINGing

Plays a sound on each response. A different sound will play for a good response as opposed to a bad response.

Data portion of ICMP packet

Allows you to specify the actual data included in the ICMP packet. You can type additional text in the window to increase the packet size or delete text to reduce the packet size. For most PING tests only a small amount of data is needed.

Ping Sweep

Ping Sweep can scan a range of IP addresses and show which IP addresses are in use and which ones are currently free. Ping Sweep can also look up the DNS name for each IP address using your configured DNS and WINS servers. Ping Sweep performs a fast ICMP sweep of your IP address range and presents the results in an easy to use worksheet.

To start using Ping Sweep:

1. Specify a beginning IP address for the range to sweep.
2. Specify an ending IP address for the range.
3. Select the type of addresses to return.
 - Responding IP addresses
 - Non-Responding IP addresses
 - All IP addresses
4. Click **Scan**.

Note: If you need to automate collection of IP address status and device type, consider using the IP Address Management. For more information, see “IP Address Management” on page 94.

Exporting, Printing, and Copying Sweeps

After running a sweep, Ping Sweep allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Hint: If the results table is split horizontally between two pages, decreasing the width of the Ping Sweep window will make the table stay on one page.

Ping Sweep Settings

Ping Sweep provides a number of global settings that control default behaviors:

- For what type of IP addresses to scan
 - o Responding - limit the scan to show addresses in use
 - o Non-responsive - limit the scan to show addresses not in use
 - o Display both
- Do you want to perform DNS and WINS lookups
- When and if you want to play sounds

To change default settings:

1. Click **Edit > Settings**.
2. Click the Scanner tab, and then specify the appropriate information.
3. Click **OK**.

Modifying ICMP Ping Settings

At the core of Ping Sweep is the ability to field ICMP communications. Depending on your network topology and speed, you may need to modify the ICMP Ping settings used by Ping Sweep.

To modify the ICMP Ping settings:

1. Click **Edit > Settings**.
2. Click the Network tab, and then specify the appropriate information.

Delay between PINGs

Allows you to modify the time to wait before sending PING communication to each node. You can use this setting to limit traffic generated by Ping Sweep for slower connections.

PING Timeout

Allows you to adjust the amount of time that Ping Sweep waits for a response from a target IP address. If the target does not respond within the timeout and does not respond to any other PING attempts, it is assumed to be down.

PINGs transmitted per node

Allows you to control the number of PING attempts to send each address during a scan. When scanning networks containing Cisco routers, set this number above two (2). If the target IP address is not in the ARP cache of a Cisco router, the router discards the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never arrive at the subnet of the target IP address. In this situation, the Cisco router responds to the second PING.

Packet Time-To-Live

The Packet Time-to-Live is the number of different locations you accept during the route to the IP address. A setting of 32 means your PING test could pass through up to 32 different routers on the way to the remote IP address before being thrown away by the network. Normally, you set this to 32 hops.

3. Click **OK**.

Publishing to the Web

Ping Sweep results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Proxy Ping

With Proxy Ping, you can initiate a PING test from any remote Cisco router. The ICMP PING results are calculated based upon packets sent from the Cisco router directly to the other remote device.

To initiate a Proxy PING:

1. Specify the following information in the appropriate fields:
 - Hostname or IP address of the proxy Cisco router
 - Read-write community string for the router
 - Hostname or IP address of the target device to be PINGed
2. Click **PING via Proxy** to start the test.
3. To restart the test after reviewing the results, click **PING via Proxy** again.

Modifying PING Settings

You can modify the characteristics of the ICMP PINGs Proxy Ping sends.

To modify Proxy Ping settings:

1. Click **File > Settings**.
2. Specify the appropriate settings:
 - Number of PINGs -- the number of ICMP PINGs to process before the results and averages are calculated
 - Packet Size -- the size of the ICMP Packet sent from the remote proxy router
 - Inter-Packet Delay -- the delay between each PING transmission

Send Page

SolarWinds Send Page is a convenient way to quickly send an E-Mail or Page. Send Page uses the E-Mail gateway setup within SolarWinds Network Monitor. For more information, see “Network Monitor” on page 171.

To send an E-Mail or page:

1. Type the required information in the **To**, **From**, and **Subject** fields.
2. Type the message you want to send in the text box, and then click **OK**.

Send Page Settings

To change Send Page settings:

1. Click **File > Settings**.
2. *If you want to change the gateway server*, edit the **E-Mail Gateway** field.
3. *If you want to see the status of the email server when sending messages*, check **Show E-Mail server status when sending E-Mail**.
4. *If you want to log all communications with the E-Mail gateway*, check **Debugging enabled**. The log file name is EMail-Notification-debug.log and is located in the \SolarWinds directory.
5. Adjust the **Retries** slider to set the amount of retries you want send page to attempt when sending a message fails.
6. *If you want to test the settings*, click **Test Gateway**.
7. Click **Apply Changes**.

Spam Blacklist

DNS blacklists or spam blacklists are popular tools used by e-mail administrators to help block reception of unsolicited e-mails into their mail systems. A DNS blacklist server maintains a database of IP addresses which have been sources of SPAM. The idea is if an IP address has sent SPAM in the past, it will be likely to send more SPAM in the future. By configuring mail servers to consult DNS blacklists before accepting an email message, e-mail administrators can block a large percentage of incoming SPAM.

SolarWinds Spam Blacklist allows you to test the IP addresses of your mail servers and verify the mail servers have not been blacklisted. By verifying your blacklist status, you can be sure other mail system which also use blacklist servers will not be blocking mail from your mail system.

One problem that could be detected by monitoring blacklist servers would be when one of your end users receives a Trojan Horse virus which uses the corporate mail servers to send SPAM or copies of itself on to other email systems. As a result of the mass mailing caused by the virus, your corporate mail server becomes blacklisted. Other business partners begin to block your mail because of your blacklist status. You need to know that you have been blacklisted so you can track down the reason why, fix the problem, and then send a request to the blacklist administrator that your address range be removed from the blacklist.

Another use for the SolarWinds Spam Blacklist checker is for determining which blacklist servers would work best on your corporate mail server. You can test the source IP addresses of recently received SPAM and determine which DNS blacklist servers most accurately block the SPAM. Conversely, you could also see which blacklist servers are needlessly blocking IP addresses of mail servers you need to receive mail from.

To scan DNS blacklist servers:

- 1. Click File > New Address List.**
- 2. Click Edit > Add Addresses.**
- 3. Type the IP address or hostname of the servers you want to add to the list. Press the Enter key after each server to add additional servers.**

Note: You can enter domain names (xyz.com), hostnames, and IP addresses.

- 4. Click OK.**
- 5. Click Address > Start Blacklist Scan.**

To remove your servers from a blacklist:

If your servers have been added to a blacklist, can contact the blacklist administrator for instructions about getting your addresses removed from the list. Many times there are instructions for doing this on the blacklist server website.

To report a server that is sending SPAM:

You can forward the email to a blacklist server to be added to their list. Most blacklist servers will post where to send these emails on their websites. You could also create your own blacklist and add the IP to this list.

Spam Blacklist Menus**File Menu****New Address List**

Starts a new, blank address list

Open Address List

Opens an existing address list

Save

Saves the current address list

Save As

Saves the current address list to a new file

Close

Closes the current address list and returns to the Quick Start page

Export to HTML

Exports the results to an HTML file

Export to Plain Text file

Exports the results to a text file

Export to Comma Delimited File

Exports the results to a comma delimited file (.CSV)

Export to Excel Spreadsheet

Exports the results to an Excel spreadsheet file

Export Directly to Microsoft Excel

Exports the results to an Excel spreadsheet and then opens the spreadsheet in Excel

Export to PDF

Exports the results to a PDF file

Send to 3 ½ Floppy (A)

Sends the results to the floppy drive in a format of your choice

Send to Desktop (create shortcut)

Sends the results to the Windows Desktop in a format of your choice

Send to Mail Recipient (as Attachment)

Sends the results to an email recipient in a format of your choice as an attachment

Send to Mail Recipient

Sends the results to an email recipient in a format of your choice

Send to My Documents

Sends the results to the My Documents folder for the current Windows user in a format of your choice

Publish to Web

Exports the results to an HTML file.

Print Preview

Previews the results exactly the same as it would appear when printed

Print

Prints the scan results

Settings

Opens the Settings dialog

Exit

Closes Spam Blacklist

Edit Menu**Add Address**

Opens the Add New Addresses dialog

Delete

Deletes the selected address from the list

Copy

Copies the selected text to the Windows clipboard

Select All

Selects all values in the current results page

Address Menu**Start Blacklist Scan**

Begins a new scan of the current address list

Stop Blacklist Scan

Aborts the active blacklist scan

Spam Blacklist Toolbar**Main Toolbar****Open Address List**

Opens an existing address list

Save

Saves the current address list

Print

Prints the scan results

Print Preview

Previews the results exactly the same as it would appear when printed

Add Address

Opens the Add New Addresses dialog

Copy

Copies the selected text to the Windows clipboard

Delete

Deletes the selected address from the list

Settings

Opens the Settings dialog

Scan Blacklists

Begins a new scan of the current address list.

Stop Scanning

Aborts the active Blacklist scan.

Spam Blacklist Settings

A number of settings can be adjusted to ensure Spam Blacklist operates the way you want.

To change the Spam Blacklist settings:

1. Click **File > Settings**.
2. Select the address tree auto expansion level you want, and then adjust the **Maximum Concurrent Queries** slider to fit your computer and network capabilities.
3. Click the Blacklist Servers tab, and then check the servers you want to use during a scan.
4. If you want to add additional servers to the list, click **Add**, provide the required server information, and then click **OK**.

Exporting Spam Blacklist Results

The Spam Blacklist tool includes a powerful export engine for exporting the results into different file formats.

To export Spam Blacklist results:

1. Perform a blacklist scan.
2. Click **File > Export**, and then select a format.

3. Select which fields to include in the export.
4. Specify a path and a file name, and then click **Save**.

Hints and Tips

The following list includes some helpful hints and tips for Spam Blacklist.

Color-Coded Addresses

When adding addresses to the list, addresses that cannot be resolved will be highlighted in red. Addresses that are successfully resolved appear in green.

Right-Click Functionality

When right-clicking on a server in the Blacklist Servers tab of the Settings dialog, you are presented with additional options to add, edit, or delete servers.

Expand/Collapse All at the Same Level

If you press and hold the Ctrl button while clicking on the + or - buttons, everything at that same level will expand/collapse.

TraceRoute

The TraceRoute tool shows you the path network traffic takes from your PC to a target server or device and displays SNMP information about the devices it discovers. TraceRoute adds realtime response time and packet loss information as a constantly refreshing bar graph and can often determine the type of machine over many hops through the public network.

Once a route is learned, the SolarWinds TraceRoute will remember the route and details about it. Since the routes are remembered, TraceRoute can show you route and failing devices whenever part of the network is down. Each hop in the selected path is traced and processed concurrently.

Note: Ensure you review the settings, the TraceRoute tool allows you to collect more than basic PING time, but also advanced information like system OID, community string, location, and other valuable information. For more information, see “Modifying TraceRoute Settings” on page 268.

To start using TraceRoute:

Type the hostname or IP address you want to trace in the appropriate field, and then click **Trace**.

Modifying TraceRoute Settings

A number of settings allow you to gather more detailed information during your TraceRoute calculations.

To modify your TraceRoute settings:

1. Click **File > TraceRoute Settings**.
2. Click the credentials tab, and, if you want to attempt to collect SNMP values from route devices, then complete the following procedure:
 - a. Click **Enable SNMP Discovery**.
 - b. *If you want to add a community string*, click **Community string** and then type the string.
 - c. *If you want to add SNMP version 3 credentials*, click **SNMP Version 3**, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.

3. Click the Preferences tab, and then specify the appropriate information:

ICMP Timeout

The ICMP Timeout is the maximum amount of time in milliseconds that Trace Route will wait for a response from the target IP address. If the target IP address does not respond within the number of milliseconds set here, Trace Route will assume it is down.

SNMP Timeout

This setting is the number of milliseconds the TraceRoute should wait for an SNMP reply before assuming the packet was lost and try again.

SNMP Retry

This setting is the number of times TraceRoute should retry an SNMP query before giving up. This should normally be set at two (2).

Maximum Hops

The maximum number of hops (routers) that Trace Route will trace a network path through. This setting is normally set to 32 hops. Setting this too high will slow down Trace Route and will also generate needless network traffic.

Play sounds during trace

Selecting this option instructs Trace Route to play sounds for each successful hop. Trace Route will also play a sound whenever a router stops responding.

4. Click the Cache tab, and then specify the appropriate information:

Cache DNS Information for

Allows you to set the number of days to retain cached information.

Clear DNS Cache now

The SolarWinds TraceRoute remembers the reverse DNS names of all traces executed. If you trace to a node successfully on Monday and the same Trace fails on Tuesday, the TraceRoute will display the DNS Name of the next hop even though the hop never responded. The Clear DNS Cache feature allows you to reset this cache. You may wish to clear this cache if you are using a portable workstation initiating a trace from a new starting point.

Clear Trace Cache now

The Clear Trace Cache feature allows you to reset this cache. You may wish to clear this cache if you are using a portable workstation initiating a trace from a new starting point.

5. Click the Results tab, and then specify the fields you want to include in your main TraceRoute window. Many fields depend on the target of the hop responding to the SNMP credentials you provide on the Credentials tab.

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.
 - a. *If you want to add a community string*, click **Community string** and then type the string.
 - b. *If you want to add SNMP version 3 credentials*, click **SNMP Version 3**, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Starting Concurrent Traces

You can start more than one trace at a time, leaving the first open to continue to analyze the data.

To start another trace:

Click **File > New TraceRoute Window**.

Exporting, Printing, and Copying TraceRoute Results

After collecting data, the TraceRoute tool allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire TraceRoute output to the clipboard or the selected information.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Publishing to the Web

TraceRoute results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Wake-On-LAN

The Wake-on-LAN utility allows you to power on a PC remotely. This is accomplished by the generation of a “magic packet” to remotely power on PCs attached to networks. When the remote network adapter hears a magic packet created for the unique MAC address of the device, the network adapter alerts the computer to power on. If Wake on LAN has been enabled in the BIOS settings, the system will power on as if the power button had been pressed. To accomplish this you will first need to ensure your PC is configured to accept a Wake-on-LAN remote command. You must also identify the IP address and MAC address of the remote device. When the device shuts down, the network interface card (NIC card) is still receiving power, and keeps listening on the network for a magic packet to arrive.

Getting Started

To get started, launch the Wake-On-LAN tool and enter the MAC Address and IP Address of the PC you want to Wake-Up. The MAC Address and IP Address can be determined opening a command prompt and typing the command `ipconfig /all` or on older system by typing the command `winipcfg`. You must use the correct target MAC and IP address to be able to remotely locate and 'turn-on' a specific computer. The Remote Wake-On-LAN tool will then send a series of Magic Packets to the target PC in an attempt to Power-On the device.

To wake a remote computer:

1. Type the MAC and IP address of the device you want to wake in to the appropriate fields.
2. Click **Wake Up PC**.
3. Click **OK** on the window indicating the packets were sent.

Configuring Your PC to Support Wake-On-LAN

Most computers will have Wake-on-LAN disabled by default. The exact procedure for enabling Wake-on-LAN will be different with each computer manufacturer.

To enable Wake-On-LAN support in BIOS:

1. Enter the BIOS settings screen during the computer's power-on self-test.
Note: F1, INS, or DEL keys are usually pressed to enter the BIOS settings.
2. Within the BIOS screen, navigate to the Power Settings.

3. Within the Power Settings screen look for settings related to “Power Up Control,” and then enable settings related to Power Up on PCI card, LAN, or Network.
4. Save and exit the BIOS settings.

Some Windows operating system drivers can enable the Wake ON LAN features of network adapters without having to access the BIOS settings.

To enable Wake-On-LAN support in Windows,

1. Access the properties of the network adapter.
2. Click the Power Management tab, and then check **Allow this device to bring the computer out of standby**.

Some computers with older PCI busses will not respond to a Wake Up signal via the PCI bus. For Wake-on-LAN to work on these computers, a WoL cable must be installed between the Network Card and the Motherboard. Because this requires opening the computer case, we recommend contacting your PC manufacturer for specific instructions.

Enabling Directed Broadcasts on your Network

If you are going to be sending WOL packets from remote networks, the routers must be configured to allow directed broadcasts. This must be done for two reasons. The first is since the PC is asleep it will not have an IP address and will not respond to ARPs from the router so only a local subnet IP broadcast packet is going to be transmitted on the segment without an ARP. Secondly, if there is a layer two switch between the router and the PC, which is true for most networks today, the switch does not know to which port the PC is physically connected. Only a layer two broadcast packet will be sent out all switch ports. All IP broadcast packets are addressed to the broadcast MAC address.

A Cisco router has IP broadcast packets enabled by default. If IP broadcast packets have been disabled, the interface configuration will have the line `no ip directed-broadcast`. If IP broadcasts are enabled, the line `no ip directed-broadcast` will not be present.

Wake-On-LAN Settings

A number of settings can be adjusted to ensure Wake-on-LAN operates properly on your network.

To change the Wake-on-LAN Settings:

1. Click **File > Settings**.
2. From the Network Settings tab, you can specify the number of retries per packet to send as well as the duration between each packet.

Note: These parameters are used to send the “magic packet” to power-on the remote PC. If you are attempting to “wake-up” a very remote PC (over 14 hops away) you may find it necessary to increase the number of retries as well as the inter-packet delay.
3. Click the Auto-Calc Broadcast Addresses tab.
4. Adjust the slider bar to select the mask appropriate for your network.
5. Click the Auto-Monitor tab.
6. ***If you want to disable the Auto-Monitor feature that automatically notifies you when the remote PC finishes its Boot-up procedure, uncheck the check box.***
7. Click **OK**.

WAN Killer

WAN Killer is a Wide Area Network traffic generator. You can adjust the packet size, the bandwidth of the circuit, and the percentage of the bandwidth you want to load with randomly generated random.

To start generating traffic:

1. Specify the access point or wireless router hostname or IP address. This is the address to which traffic will be sent.
2. Specify the port to which traffic is to be sent and the protocol to use. For example, type `7 echo - tcp` to designate TCP traffic on port 7.

Notes:

- You can enter any number, but the remote device may disconnect before any random data is sent. For example, if you select port 80 http on a remote web server and start WAN Killer, the remote machine may close or reject the session before any random data is sent.
 - Use port 7 to generate traffic going both ways. When data is sent to port 7 (echo), all traffic that is received by the target device will be sent back to WAN Killer. This will generate a load in both directions.
 - Use port 9 (discard) to generate one-way traffic. Port 9 discards all data when received.
3. Specify the size of the packet you want to send. WAN Killer always attempts to send the percent of bandwidth selected, setting the packet size higher generates less packets. Setting a smaller packet size generates more packets.
 4. Specify the size of WAN circuit in Kbps (kilobits per second).
 5. Specify the traffic percent of the total bandwidth you want WAN Killer to generate.
 6. Click **Start**.

Note: It may take WAN Killer up to 30 seconds to adjust to the Windows Operating System, IP stack, and network. WAN Killer will continually make adjustments in order to send the percentage load specified.

7. ***If you want to adjust packet gap***, uncheck **Automatic inter-packet gap adjustment**.

Note: WAN Killer automatically adjusts the inter-packet gap to maintain the specified load. If you choose to adjust the clock factor manually, ensure you make small incremental changes. Increasing the clock factor will generate more traffic. Decreasing it will reduce the amount of traffic.

8. ***If you want to suspend data generation***, click **Pause**.
9. ***If you want to stop data generation***, click **Stop**.

Chapter 8

Security Tools

The following sections provide detailed information about the Security tools included with Toolset.

- “Edit Dictionaries” on page 277
- “Port Scanner” on page 280
- “Remote TCP Session Reset” on page 283
- “Router Password Decryption” on page 286
- “SNMP Brute Force Attack” on page 288
- “SNMP Dictionary Attack” on page 289

Edit Dictionaries

The Dictionary Editor is used to build a database of words to be used during an SNMP or password attack. The dictionary database is normally used by SolarWinds SNMP Dictionary Attack, but you can also be used it with other programs. The database of dictionaries is a Microsoft Access database.

- A new dictionary can be created by importing a list of words.
- The words in a dictionary can be permuted.
- Dictionaries can also be exported into plain text files.

To view a dictionary, click **Dictionaries > Show Dictionary**, and then click the dictionary you want to see.

Dictionary Editor Menus

File Menu

Import Dictionary

Imports a list of words into an existing or new dictionary

Export Dictionary

Exports a dictionary into a text file

Exit

Closes Dictionary Editor

Dictionaries Menu

New Dictionary

Creates a new, empty dictionary

Copy Dictionary

Copies the word list from one dictionary to another

Clear Dictionary

Deletes all words from a dictionary

Delete Dictionary

Deletes the dictionary from the database

Show Dictionary

Displays the words in a dictionary

Remove Duplicates

Scans a dictionary for duplicate words and removes them

Mutate Dictionary

Displays the Mutate Dictionary dialog box. For more information, see “Mutating a Dictionary” on page 279.

Mutating a Dictionary

Mutating a dictionary is the process of mutating each word slightly. For example, changing all the words to upper case, capitalizing them, or converting individual characters.

To mutate a dictionary:

1. Click **Dictionaries > Mutate Dictionary**, and then click the dictionary you want to alter.
2. Select one or more mutations to apply, and then click **OK**.
3. Select a dictionary to place the new words in, and then click **OK**.

Notes:

- Words will be taken from one dictionary, mutated, and then stored in the target dictionary.
- The source and target dictionary may be the same. Also, you can perform many mutations on a single dictionary. You are not limited to a single mutation.

Importing a List of Words

Word lists can be imported in the dictionary database using a text file.

To import a list of words:

1. Click **File > Import Dictionary**.
2. Choose to import the list to a new or existing database.

Note: When importing words into a new dictionary, you will need to give the dictionary a unique name and description.

3. Browse to the text file containing the list of words you wish to add, and then click **Open**.

Note: The list of words should be in a plain text file with one word per line.

Hints and Tips

Editing the list of words in a dictionary

The easiest way to edit the words in a dictionary is to export it to a plain text file and load it into WordPad or Notepad. After you have edited the dictionary, import it back into the dictionary database. For more information, see “Importing a List of Words” on page 279.

Port Scanner

Ping Sweep can scan a range of IP addresses and show which IP addresses are in use and which ones are currently free. Ping Sweep can also look up the DNS name for each IP address using your configured DNS and WINS servers. Ping Sweep performs a fast ICMP sweep of your IP address range and presents the results in an easy to use worksheet.

To start using Ping Sweep:

1. Specify a beginning IP address for the range to sweep.
2. Specify an ending IP address for the range.
3. Select the type of addresses to return.
 - Responding IP addresses
 - Non-Responding IP addresses
 - All IP addresses
4. Click **Scan**.

Note: If you need to automate collection of IP address status and device type, consider using the IP Address Management. For more information, see “IP Address Management” on page 94.

Exporting, Printing, and Copying Sweeps

After running a sweep, Ping Sweep allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Calculations

To export discovered results:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Calculations

To copy the results:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Hint: If the results table is split horizontally between two pages, decreasing the width of the Ping Sweep window will make the table stay on one page.

Ping Sweep Settings

Ping Sweep provides a number of global settings that control default behaviors:

- For what type of IP addresses to scan
 - o Responding - limit the scan to show addresses in use
 - o Non-responsive - limit the scan to show addresses not in use
 - o Display both
- Do you want to perform DNS and WINS lookups
- When and if you want to play sounds

To change default settings:

1. Click **Edit > Settings**.
2. Click the Scanner tab, and then specify the appropriate information.
3. Click **OK**.

Modifying ICMP Ping Settings

At the core of Ping Sweep is the ability to field ICMP communications. Depending on your network topology and speed, you may need to modify the ICMP Ping settings used by Ping Sweep.

To modify the ICMP Ping settings:

1. Click **Edit > Settings**.
2. Click the Network tab, and then specify the appropriate information.

Delay between PINGs

Allows you to modify the time to wait before sending PING communication to each node. You can use this setting to limit traffic generated by Ping Sweep for slower connections.

PING Timeout

Allows you to adjust the amount of time that Ping Sweep waits for a response from a target IP address. If the target does not respond within the timeout and does not respond to any other PING attempts, it is assumed to be down.

PINGs transmitted per node

Allows you to control the number of PING attempts to send each address during a scan. When scanning networks containing Cisco routers, set this number above two (2). If the target IP address is not in the ARP cache of a Cisco router, the router discards the ICMP query (PING) while it requests the MAC address of the target IP. The first PING will never arrive at the subnet of the target IP address. In this situation, the Cisco router responds to the second PING.

Packet Time-To-Live

The Packet Time-to-Live is the number of different locations you accept during the route to the IP address. A setting of 32 means your PING test could pass through up to 32 different routers on the way to the remote IP address before being thrown away by the network. Normally, you set this to 32 hops.

3. Click **OK**.

Publishing to the Web

Ping Sweep results can be published to a static HTML page containing all the discovered results.

To save results to an HTML page:

1. Click **File > Publish to Web**.
2. Select the fields you want to include, and then click **OK**.
3. Name and choose a location for the file, and then click **Save**.

Remote TCP Session Reset

This security tool can remotely display all active sessions on a terminal server, router, dial-in server, access server, etc. You can also easily reset any TCP session remotely.

To display a list of TCP sessions connected to a remote device:

1. Type the hostname or IP address in the **Router, Switch or Server Name / IP** field.
2. Type the SNMP community string for the remote device in the **Read-Write Community String** field.

To reset a remote TCP session:

1. Connect to the remote device using the steps listed above.
2. Select the session from the list and then click **Session > Break Selected Sessions**.

Note: You can not reset a TCP session unless you are using the SNMP read-write community string.

Remote TCP Session Reset Menus

File Menu

Export to Comma Delimited File

Exports the results to a comma delimited file (.CSV)

Export to Plain Text file

Exports the results to a text file

Export to HTML

Exports the results to an HTML file

Export to Excel Spreadsheet

Exports the results to an Excel spreadsheet file

Export Directly to Microsoft Excel

Exports the results to an Excel spreadsheet and then opens the spreadsheet in Excel

Publish to Web

Exports the results to an HTML file

Print

Prints the scan results

Print Preview

Previews the results exactly the same as it would appear when printed

Note: If the results table is split horizontally between two pages, decreasing the width of the Remote TCP Session Reset window will make the table stay on one page.

Exit

Closes Remote TCP Session Reset

Edit Menu

Copy

Copies the currently selected TCP sessions to the Windows clipboard

Copy All

Copies all the TCP sessions to the Windows clipboard

Session Menu

Break Selected Sessions

Resets the currently selected TCP sessions

Note: You can only break a TCP session if you use the SNMP read-write community string. A read-only community string will display the list of TCP sessions, but not reset them.

Remote TCP Session Reset Toolbar

Export

Exports the list of TCP sessions

Send To

Sends the list of TCP sessions to a specified location or E-Mail message

Print

Prints the list of TCP sessions

Refresh

Refreshes the list of TCP sessions by connecting to it again

Auto Off

Turns Auto-Update on/off.

Break

Breaks the selected TCP session. You can only break a TCP session if you use the SNMP read-write community string.

Settings

Opens the Settings window.

Help

Displays the SolarWinds Toolset Page Help.

Remote TCP Session Reset Settings

A number of settings can be adjusted to ensure Remote TCP Session Reset operates the way you want.

To change the Remote TCP Session Reset settings:

1. Click **File > Settings**.
2. Adjust the **Auto Refresh Rate** slider to establish how often the statistics will refresh when Auto Update is enabled.
3. Click the Advanced tab.
4. If you want to force Remote TCP Session Reset to use SNMP V1 packets, check **Disable SNMP V2 Support**.

Note: Disabling SNMP V2 support greatly reduces the speed at which statistics can be gathered.

Exporting from Remote TCP Session Reset

The Remote TCP Session Reset tool includes a powerful export engine for exporting the results into different file formats.

To export a list of TCP sessions:

1. Connect to the remote device.
2. Click **File > Export**, and then select a format.
3. Select which fields to include in the export.
4. Specify a path and a file name, and then click **Save**.

Remote TCP Session Reset Frequently Asked Questions

When I click 'Break', nothing happens. Why?

Are you using the SNMP read-write community string? You can display a list of TCP sessions using the read-only community string, but not break them.

Router Password Decryption

Router Password Decryption can decrypt Cisco type 7 passwords. Type 7 passwords are commonly used for terminal and enable logins on Cisco routers and switches. You must have the encrypted password string in order to decrypt the password. The encrypted string is normally taken from a printed Cisco configuration or by downloading the configuration directly from the router or switch.

To decrypt an encrypted password string:

Type or copy and paste the encrypted type 7 password string, and then click **Decrypt**.

For more information on how to reset an enable secret password, see "Resetting an Enable Secret Password Using SNMP" on page 36.

Router Password Decryption Frequently Asked Questions

Where do I find the encrypted password?

From a Cisco router or switch configuration file. You can extract the password from a saved or printed configuration file. You can also download the current configuration directly from the router or switch without knowing the password. All you need is the read-write SNMP community string.

Can Router Password Decryption decrypt type 5 secret passwords?

No. Type 5 secret passwords use a one-way hash algorithm and cannot be decrypted. However, they can be reset. You can reset a type 5 secret password using SolarWinds Cisco Config Uploader. It resets the password via SNMP. All you need is the SNMP read-write community string. For more information, see “Config Uploader” on page 31.

How can I decrypt dozens of passwords at once?

Use SolarWinds Cisco Config Viewer. It can find all the passwords in a configuration file and decrypt all of them at once. This is convenient when converting a Cisco AS5200 to use TACACS or RADIUS. For more information, see “Config Viewer” on page 37.

SNMP Brute Force Attack

SNMP Brute Force Attack attacks an IP address with SNMP queries to attempt to determine the SNMP read-only and read-write community strings. It does this by trying every possible community string. You can specify the character set to build words from as well as the maximum length of the community strings to try.

To SNMP Brute Force Attack a device:

1. Type the IP address of the device you want to attack and then click **Attack**.
2. If you want to change the attack speed, adjust the **Attach Speed** slider.

Note: If you attack too fast, the network or the target device may begin dropping packets. The "Packet Drops" line can be a good indicator that packets are being dropped. But the "Packet Drop" line only increments when SNMP Brute Force Attack knows it definitely dropping packets. Packets may still be discarded without SNMP Brute Force Attack detecting it.

3. *If you want to stop the pause the attack*, click **Pause**.

Note: After pausing, clicking **Attack** will resume where SNMP Brute Force Attack was paused.

SNMP Brute Force Attack Settings

A number of settings can be adjusted to ensure SNMP Brute Force Attack operates properly on your network.

To change the SNMP Brute Force Attack Settings:

1. Click **File > Settings**.
2. *If you want to stop the attack when a Read/Only community string is found*, check **Stop searching after Read/Only string is found**.
3. *If you want to change the length of community strings attempted by SNMP Brute Force Attack*, adjust the **Try community strings up to xx characters long** slider.
4. Click the **Character Set** tab, and then select the character set you want SNMP Brute Force Attack to use to build the community strings or type a custom set of characters.
5. Click the **Community Strings** tab.
6. *If you want to use a starting community string*, type the string in the **Starting Community String** field.

7. Select **Rotate from right to left** or **Rotate from left to right** to establish the progression the attack engine builds the community strings.
8. Click the **SNMP** tab.
9. Adjust the **Packet Timeout** slider to set the number of milliseconds the attack engine should wait for a SNMP reply before assuming the packet was lost.
10. Adjust the **Query Attempts** slider to set the number of times the attack engine should retry a SNMP query before giving up.
11. Click **OK**.

SNMP Brute Force Attack Frequently Asked Questions

How do I attack a device using a predefined list of community strings?

Use SolarWinds SNMP Dictionary Attack instead. For more information, see “SNMP Dictionary Attack” on page 289.

SNMP Dictionary Attack

SNMP Dictionary Attack attacks a set of IP addresses with SNMP queries to attempt to determine the SNMP community strings using a dictionary of community strings. You can use one of the dictionaries provide by SolarWinds, or import your own. You can also mutate a dictionary. For more information, see “Edit Dictionaries” on page 277.

To attack a set of IP addresses using a dictionary:

1. Click **File > New Database**.
2. Select a path and type a name for your new database, and then click **Save**.
3. **If you want to add IP addresses manually**, complete the following task.
 - a. Click **Edit > Add IP Addresses**.
 - b. Type the IP address and click **Add** for each device you want to add.
 - c. Click **OK**.

4. **If you want to import a list of IP addresses**, complete the following procedure.
 - a. Click **File > Import IP Addresses** and then select the file type you want to import.

Note: You can use SolarWinds Ping Sweep or SolarWinds Network Sonar to generate a list of IP addresses. For more information about Ping Sweep, see “Ping Sweep” on page 140. For more information about Network Sonar, see “Network Sonar” on page 130.
 - b. Browse to the file you want to import, and then click **Open**.
 - c. Follow the onscreen instructions to complete the import process.
5. Click **Edit > Dictionary**.
6. Select the dictionary to use during the attack, and then click **OK**.

Note: You can also edit, mutate, or create new dictionaries using the SolarWinds Dictionary Editor. For more information, see “Edit Dictionaries” on page 277.
7. Click **Run > Start SNMP Attack**.

SNMP Dictionary Attack Menus

File Menu

New Database

Creates a new Attack database

Open Database

Loads an existing Attack database

Close Database

Closes the current database

Import IP Addresses

Imports a list of IP addresses to attack

Export to Comma Delimited File

Exports the results to a comma delimited file (.CSV)

Export to Plain Text file

Exports the results to a text file

Export to HTML

Exports the results to an HTML file

Export to Excel Spreadsheet

Exports the results to an Excel spreadsheet

Export Directly to Microsoft Excel

Exports the results to an Excel spreadsheet and then opens the spreadsheet in Excel. You must have Excel installed for this to work

Publish to Web

Exports the results to an HTML file

Print

Prints the scan results

Print Preview

Previews the results exactly the same as it would appear when printed

Note: If the results table is split horizontally between two pages, decreasing the width of the SNMP Dictionary Attack window will make the table stay on one page.

Exit

Closes SNMP Dictionary Attack

Edit Menu**Add IP Addresses**

Manually adds IP addresses one at a time

Copy

Copies the highlighted results to the Windows clipboard

Delete

Deletes the selected IP addresses from the attack database

Mark all IP Addresses as Not Complete

Resets all IP addresses in the attack database to "Not Complete"

Note: The addresses will be attacked again during the next dictionary attack

Select All

Highlights all IP addresses in the list

Dictionary

Specifies which dictionary to use during the attack

Settings

Displays the SNMP Dictionary Attack settings dialog box

Run Menu

Start / Stop SNMP Attack

Starts or stops the Attack

Filter Menu

All Nodes

Displays all IP addresses in the Attack database

Addresses that did not respond to PINGs

Displays only the IP addresses that do not respond

Addresses that the community string could not be determined

Displays only the IP addresses that the SNMP attack was unsuccessful at determining the community string

Successful Attacks

Displays only the IP addresses that the SNMP attack was successful

SNMP Dictionary Attack Toolbar

New

Creates a new Attack database

Open

Opens an existing Attack database

Print

Prints the current view

Import

Imports a list of IP addresses to attack

Export

Export the results to a specified file format

Dictionary

Specifies the dictionary to use during the attack

Settings

Displays the Settings dialog box

Start

Starts the attack using the selected dictionary

Stop

Stops the current attack

SNMP Dictionary Attack Settings

A number of settings can be adjusted to ensure SNMP Dictionary Attack operates properly on your network.

To change the SNMP Dictionary Attack Settings:

1. Click **File > Settings**.
2. Adjust the **Scanner Performance** slider to adjust the speed of the attack.
3. Click the SNMP tab.
4. Adjust the **Packet Timeout** slider to set the number of milliseconds the attack engine should wait for a SNMP reply before assuming the packet was lost and trying again.
5. Adjust the Query Attempts to set the number of times the attack engine should retry a SNMP query before giving up.
6. Click **OK**.

Exporting from SNMP Dictionary Attack

SNMP Dictionary Attack can export the list of IP addresses into a number of file formats. When you export from SNMP Dictionary Attack, a dialog box allows you to select the information that should be included in the exported file.

Comma Delimited File

This format is suitable for importing into other programs, spreadsheets or databases. Each field is separated by a comma. Comment lines begin with a pound (#) character. Fields with spaces or special characters will be enclosed in quotation marks.

Plain Text File

When exporting to a Plain Text File, SNMP Dictionary Attack simply dumps the output to a text file without any special formatting. Each field is separated by a tab.

HTML File

The HTML export method creates an HTML file in the same format as the SNMP Dictionary Attack table.

Excel Spreadsheet

This export method creates a Microsoft Excel spreadsheet and exports the results to it. Microsoft Excel must be installed on your machine in order for this export method to work.

Direct to Microsoft Excel

This export method creates a Microsoft Excel spreadsheet, exports the results to it, and then opens the spreadsheet within Excel. Microsoft Excel must be installed on your machine in order for this export method to work.

Publish to the Web

Publishes a static HTML page of all DNS Audit results.

Discovering All the Devices on Your Network

Use SolarWinds Network Sonar. Network Sonar will build a database of all devices on a network. You can import the list of IP addresses into SNMP Dictionary Force Attack directly from the Sonar database. For more information about Network Sonar, see “Network Sonar” on page 130.

You could also use Ping Sweep to build a list of IP addresses. After scanning an IP address range with Ping Sweep, export the IP addresses to a Comma Delimited file. You can then import the file into SNMP Dictionary Force Attack. For more information about Ping Sweep, see “Ping Sweep” on page 140.

Chapter 9

SNMP Tools

With this group of tools, you can view MIB values a number of different ways. You can browse through different MIB values on a device, display all MIB values, or display specific values.

- “SNMP MIB Browser” on page 297
- “MIB Viewer” on page 304
- “MIB Walk” on page 307
- “SNMP Trap Editor” on page 308
- “SNMP Trap Receiver” on page 310
- “Update System MIB” on page 312

SNMP MIB Browser

The MIB Browser utilizes SolarWinds extensive MIB (Management Information Base) database of over a thousand standard and proprietary MIBs. A MIB Browser is a core fundamental tool for network engineers. It allows an engineer to query a remote device for software and hardware configurations via SNMP. It also allows an engineer to make changes to the remote device. The remote device could be a router, switch, hub, server, firewall, or any other device that supports SNMP.

The most critical part of any MIB Browser is the number of standard and proprietary MIBs it supports. Without the correct MIBs, the data collected from a remote device is difficult to interpret and use. SolarWinds MIB Browser is shipped with over 250,000 precompiled unique OIDs from hundreds of standard and vendor MIBs – the largest collection in the industry. SolarWinds engineers continually update the MIB database with the latest MIBs. Updates to the MIB database are available periodically to SolarWinds subscription customers.

Another common use for a MIB Browser is to find out what MIBs and OIDs are supported on a particular device. The SolarWinds MIB Browser allows an engineer to easily walk any MIB Tree (even if the MIB tree is not in the SolarWinds database) and determine what MIBs a particular piece of hardware supports. This is important when determining the SNMP OIDs from which to collect statistics or to monitor. The SolarWinds MIB Browser automatically analyzes the results from each SNMP query and displays the information in a readable form.

The query results windows are also customizable. An engineer can select the type of information to be displayed for each SNMP query. OIDs, defining MIB, access (read-only, read-write, no-access), OID status (standard, deprecated, obsolete), raw value, cooked value, English description, and other properties can be displayed while querying a remote device. For more information, see “Modifying SNMP MIB Browser Settings” on page 303.

Browsing a MIB Tree

Complete the following procedure to begin browsing the MIB tree.

To browse the MIB tree for a specific device:

1. Click Select a Device.
2. Select or type a hostname or IP address in the Device or IP address field.
3. ***If the device support SNMP version 1 or version 2***, click **Community string**, and then type the appropriate community string. If you specify a community string that has not been saved before, you are asked if you would like to save the credentials. Select yes to make the community string available in other tools that support the shared credentials database. If you want to remotely update values discovered by the MIB Browser, ensure you specify a read-write community string.

4. **If the device supports SNMP version 3**, complete the following procedure:
- a. Select a credential set from the list, or click **Add** to create a new credential set and save it in the shared credentials database.
 - b. If you are adding a new credential set, specify the appropriate information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.

If you want to remotely update values discovered by the MIB Browser, ensure you specify credentials with read-write access.

5. Select an OID from the MIB Tree on the left.

6. *If you are not sure which OID to select*, complete the following procedure to view a number of useful values:
- Expand **iso > org > dod > internet > mgmt > mib-2**.
 - Click **system**.
 - Click **Get Tree** to walk the system tree. All the values in blue are read-write and can be changed remotely, if you are using the SNMP read-write community string. Click on the field and start typing, or use the drop down menus within each field. For example, the drop down menu shows all of the possible values in a readable format, with the numeric value in parenthesis, for `ifAdminStatus` and allows you to easily shutdown the interface remotely. The MIB Browser allows this for any MIB, not just the few examples shown here.

Note: You can right-click on any SNMP value and select "Details..." from the popup menu to get more information about it.

Exporting, Printing, and Copying MIB Data

After finding the MIB and OID you need, MIB Browser allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting

To export discovered results:

- Click **File > Export**, and then select the type of export.
- Check the information you want to export.
- Specify the name and path for the exported information.

Copying Charts

To copy the results:

Click **Edit > Copy**. If you want to copy all displayed information, ensure you select **Edit > Select All** before copying.

Printing Calculations

To print results:

Click **File > Print**, and then select the information you want to print.

Launching the Shared Credentials Database

The shared credentials database allows you to quickly load credentials between different tools in the toolset.

To launch the shared credentials database:

1. Click **Edit > Shared Credentials Database**.
2. Click **Add**, and then complete the following procedure to enter a new set of credentials.
 - a. *If you want to add a community string*, click Community string and then type the string.
 - b. *If you want to add SNMP version 3 credentials*, click SNMP Version 3, and then specify the following information:
 - Credential set – the name that represents the credentials you specify on the Add Credentials window. This name is displayed in the SNMP Version 3 list in Toolset tools that support the shared credentials database.
 - Context – a named designation, similar to a group or domain name, to which the user name belongs. Context is mandatory if it has been defined for the object being managed.
 - User name – the name of the user with access to the device.
 - Authentication type – the authentication type you want to use when logging on to the device, for example, MD5.
 - Authentication password/key – the password or key that corresponds to the authentication selected.
 - Encryption type – the encryption used when communicating with the device, for example, DES (56bit) or AES (128bit) encryption.
 - Encryption password/key – the password or key that corresponds to the encryption selected.
3. Click a set of credentials, and then click **Modify** to change the stored information.
4. Click the credentials and then **Devices** to specify the hostname or IP address of a device to associate with the selected credentials.

Bookmarking Frequently Used MIBs

Much like you can bookmark common sites in a web browser, you can bookmark commonly searched for OIDs.

To bookmark an OID:

1. Locate the OID in the browser.
2. Click the OID, and then click **Bookmarks > Bookmark Selected OID**.
3. *If you want to organize your bookmarks*, click **Manage Bookmarks**.

Note: You can organize and delete saved bookmarks on the Manage Bookmarks window.

Viewing a List of MIBs in the Database

If you would like to view a list of all the MIBs in the database, the Manage MIBs in Database option allows you to do this. Always search for a MIB in the MIB database before sending a MIB inclusion request to SolarWinds.

To view a list of MIBs in the database:

1. Click MIBs, and then click Manage MIBs in Database.
2. Review the list in the results pane.

Running the SNMP Set Tool

The MIB Browser provides two different methods for updating OID values. You can browse the tree and change values displayed in the results pane. Or, you can use the SNMP Set tool. The SNMP Set tool provides another way to update SNMP OID values.

To run the SNMP Set tool:

1. Click Tools > SNMP Set.
2. Select or type the target device IP address or hostname in the appropriate field.
3. Enter the OID and OID values to set.

Note: You can gather the current value by clicking **Get Current Value**.

4. Click SNMP Set when you have made the appropriate modifications.

Modifying SNMP MIB Browser Settings

You can change a number of default settings in the MIB Browser:

- You may want to specify different fields to reveal in the results pane. By doing so, you can change the fields that are copied, exported, and printed.
- You can optimize SNMP performance by modifying network settings.
- You can change the look and feel of the product by modifying the advanced settings.

To modify settings:

1. Click **File > Settings**.
2. Click the General tab, and then select the fields you want to include in the results pane.
3. Click the Network tab, and then modify the SNMP settings, including:
 - Timeout
 - Retries
 - Request size
 - Remote port

Note: Disabling SNMP V2 support forces Remote TCP Session Reset to use SNMP V1 packets reducing the speed at which statistics are gathered.

4. Click the Advanced tab, and then select the user interface you want to use and whether to reveal OIDs in the MIB tree.

Searching the MIB Tree

The MIB Browser incorporates a powerful MIB Tree OID search capability. This search capability allows you to search for a specific OID, OID name pattern, or keyword in the descriptions.

To search the MIB Tree:

1. Click Tools > Search MIB Tree.
2. Select the appropriate tab:
 - Search by OID
 - Search by Name
 - Search Descriptions
3. You can use asterisks (*) as a wildcard character. For example, system* finds all OIDs that start with system, and *number finds all OIDs that end with number.
4. Type the search criteria, and then click Search.
5. Click Show in MIB Tree to view the OID in the MIB tree.
6. ***If you want to copy or print the OID information you find***, click the appropriate button.

Note: When using the description tab, the first 500 OIDs that match the pattern will be displayed. Click the OID to display details about it.

MIB Viewer

The MIB Viewer tool queries the extensive MIB database to display any OID or Table. It provides a quicker method of retrieving frequently used MIBs than the MIB Browser, though it does not provide browsing of the MIB tree. For more information, see “SNMP MIB Browser” on page 297.

To view an OID or table:

1. Type the hostname or IP address of the target device. MIB Viewer directly queries the device for supported MIBs.
2. Provide an SNMP community string. If you want to modify values, ensure you provide the read-write community string.

3. Provide an OID or table name or enter an entire MIB tree. The MIB Viewer tool analyzes your input and determines the best way to format the results. You can also concatenate MIBs by placing an ampersand '&' between them. The MIB Viewer downloads each OID and MIB tree in the order you enter them. For more information, see “Guidelines and Examples” on page 305.

Note: OID values in blue are read-write and can be changed, if you supplied a read-write community string. Click the value and type a new value, or use the list to select a value.

4. *If you want to view details about a selected OID, including the numerical OID and description, click **View > Details**.*

Guidelines and Examples

Review the following table for examples of valid input for the **MIB Table to download** field.

MIB Table to download field	Description
RFC1213-MIB:system	MIB-II system tree
1.3.6.1.2.1.1	Numeric OID equivalent to RFC1213-MIB:system
hrSWRunTable	Running software from the Host-Resources MIB
ipInReceives & next 16	IP Statistics
ICMP	ICMP statistics from RFC-1213
tcpRtoAlgorithm & Next 11 & tcpInErrs & tcpOutRsts	TCP Statistics
etherStatsTable	RMON Ethernet Statistics
frCircuitTable	Frame Relay circuits
bgpPeerTable	BGP peer table
ifPhysAddress	MAC addresses for all interfaces on a device
hrSWInstalledTable	Installed software
OLD-CISCO-MEMORY-MIB:freeMem & Next 39 & bufferHgSize & Next 7	Cisco Buffers

MIB Table to download field	Description
cdpCacheTable	Cisco Discovery Protocol table
tcpConnTable	TCP connection table

Notes:

- You can add Next *x*, where *x* represents the number of OIDs to return. The Cisco Buffers in the previous table of examples provides an excellent example of the Next *x* syntax.
- Each OID can be fully qualified with the MIB Name, a colon, and the OID name. Or, you can provide only the MIB tree.

For common OID names that could exist in multiple MIBs, include the MIB Name when specifying the value. For example, system exists in RFC1213-MIB, HP-UNIX, INTEL-GEN-MIB, and the Apple Macintosh MIB, therefore specify the MIB when retrieving the value: RFC1213-MIB:system or HP-UNIX:system or INTEL-GEN-MIB:system.

Valid formats for the OID name are provided in the following table:

MIBName:OIDName	RFC1213-MIB:system	OLD-CISCO-MEMORY-MIB:freeMem
Numeric OID	1.3.6.1.2.1.1	1.3.6.1.4.1.9.9.27.1.1.2
OIDName	tcpConnTable	cdpCacheTable

Exporting, Printing, and Copying Values

After retrieving MIB values, MIB View allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Results

To export OID values:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Results

To copy OID values:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Results

To print OID values:

Click **File > Print**, and then select the information you want to print.

MIB Walk

The MIB Walk tool walks the SNMP tree for a target device and pulls the value of each OID in the supported MIBs (Management Information Base). Use the MIB Walk tool to find out what MIBs and OIDs are supported on a particular device. MIB Walk uses the SolarWinds MIB database to determine the common, human readable, name for each OID and the MIB to which it belongs. SNMP communication must be enabled on the device. To walk the MIBs, you can use either the read-only or the read-write community string.

To walk the MIBs on a device:

1. Specify the hostname or IP address for the device.
2. Specify the SNMP community string.
3. Select the SNMP tree to walk:
 - Standard starts the SNMP walk from 1.3.6.1.2
 - Private starts the SNMP walk from 1.3.6.1.4
4. Click **Walk**.

Exporting, Printing, and Copying Values

After retrieving MIB values, MIB Walk allows you to transfer that information to other tools through exporting and copy and paste capabilities. You can also print discovered information.

Exporting Results

To export values:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Results

To copy values:

Click **Edit > Copy**, and then specify whether you want to copy the entire sweep to the clipboard or a selected IP address.

Printing Results

To print values:

Click **File > Print**, and then select the information you want to print.

SNMP Trap Editor

The Trap Editor tool can be used to modify SNMP Trap templates used by the SolarWinds Network Management Tools. By using the Trap Editor you can create SNMP Traps of almost any structure, including mimicking traps generated by network hardware. If you are using a network management solution, consider the ease with which you can now mimic critical alerts sent to that solution, ensuring it responds correctly when receiving such an alert.

To begin building an SNMP Trap:

1. Click **File > New Trap**. The two OIDs required for an SNMP v2 Trap are provided whenever you create a new trap, they are: SysUptime (1.3.6.1.2.1.1.3.0) and TrapOID (1.3.6.1.6.3.1.1.4.1.0).
2. Click **Trap > Add OID**.
3. Click browse (...) next to the blank OID column, select an OID, and then click **OK**.
4. Select the data type from the list in the Data Type column. Click the cell to enable the list.
5. *If you need to edit the value of the data type*, click the empty value cell and type the value. If you select an OID for the data type, you can browse for the OID.
6. *If you want to duplicate a selected OID to a new row*, click **Edit > Duplicate**.
7. *If you want to delete a selected OID*, click **Edit > Delete**.
8. *If you want to copy a selected OID to the clipboard*, click **Edit > Copy**.
9. *If you want to select all values*, click **Edit > Select All**.

10. *If you want to Add a new row*, click **Trap > Add OID**.
11. *If you want to move a highlighted row up or down*, click **Trap > Shift Up** or **Trap > Shift Down**.

Viewing Example Traps

If you would like to view an example of a trap created with the SNMP Trap editor, or use an example as a foundation to build your own traps, complete the following procedure.

To view example traps:

1. Click **File > Open Trap**.
2. Select one of the following example traps:
 - Example1.trap
 - Orion-Detailed-Alert.trap
 - Orion-Generic-Alert.trap
3. Click **OK**.

Sending a Trap

You can test your trap template by sending your newly created trap to a receiver. If you do not want to send the trap to a production piece of equipment, consider sending the trap to the Trap Receiver tool. For more information, see “SNMP Trap Receiver” on page 310.

To send a trap:

1. Click **Trap > Send Trap**.
2. Specify the hostname or IP address and the community string of the device to which you want to send the trap.
3. Click **Send**.

Exporting, Printing, and Copying Values

After receiving traps, Trap Receiver allows you to transfer trap information to other tools through exporting and copy and paste capabilities. You can also print trap information.

Exporting Traps

To export trap values:

1. Click **File > Export**, and then select the type of export.

2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Traps

To copy trap values:

Click **Edit > Copy**. If you want to copy all displayed values, click **Edit > Select All**, and then click **Edit > Copy**.

Printing Results

To print values:

Click **File > Print**, and then select the information you want to print.

Copying an Existing Trap Template to the Trap Editor

Send a trap from the device you want to mimic to the SNMP Trap Receiver, and then save the trap to the folder C:\Program Files\SolarWinds\Common. You can now open this trap template with SNMP Trap Editor. For more information, see “SNMP Trap Receiver” on page 310.

SNMP Trap Receiver

SNMP Traps are network health notifications sent on UDP port 162. The SNMP Trap Receiver tool receives and displays SNMP Traps sent from any of the following:

- Network management applications
- Network devices
- Servers

You can use the tool to analyze the format of the trap and to verify that a trap source is configured and functioning properly.

The SNMP Trap Receiver adds a powerful diagnostic tool to your arsenal. Trap Receiver ensures your network management solutions are properly configured to accept traps sent by your devices. The format of the trap is dictated by the device sending the trap. For more assistance with interpreting the Trap Details, refer to the documentation for the device sending the traps.

Once you have launched the SNMP Trap Receiver you are ready to start receiving and displaying traps. No configuration changes need to be made in order for the application to begin collecting traps.

Configuring Settings

You can customize the Trap Receiver in the following ways:

- Decode or show the raw data of trap OIDs
- Filter from what IP addresses, subnets, or address ranges you accept traps
- Filter what SNMP community strings to accept
- Log traps to a file

To configure your Trap Receiver Settings:

1. Click **File > Settings**.
2. Click the General tab, and then specify whether to decode trap OIDs. If you are analyzing a trap to ensure its capture by your network management solution, ensure you view results both ways. Not all network solutions decode trap OIDs. This setting is applied to traps received after it is configured.
3. Click the Device Filter tab, and then add the addresses from which you want to accept.
4. Click the Community Filter tab, and then add the community strings from which you want to accept traps.
5. Click the Logging tab, and then provide the path and name for your log file.
6. Click **OK**.

Sending Test Traps

To ensure the trap receiver is able to receive traps or to ensure another instance of a trap receiver is able to receive traps, Trap Receiver can send an SNMP trap to an IP address.

To send a test trap:

1. Click **Traps > Send Test Trap**.
2. Provide the IP address or hostname and the community string used to access the target trap receiver.
3. Click **Send**.

Exporting, Printing, and Copying Values

After receiving traps, Trap Receiver allows you to transfer trap information to other tools through exporting and copy and paste capabilities. You can also print trap information.

Exporting Traps

To export trap values:

1. Click **File > Export**, and then select the type of export.
2. Check the information you want to export.
3. Specify the name and path for the exported information.

Copying Traps

To copy trap values:

Click **Edit > Copy**. If you want to copy all displayed values, click **Edit > Select All**, and then click **Edit > Copy**.

Printing Results

To print values:

Click **File > Print**, and then select the information you want to print.

Update System MIB

Update System MIB is a convenient way to remotely change the System Name, Location, and Contact for a device. Update System MIB uses the SNMP read-write community string to make the changes.

You can use this tool to quickly and easily set the system information for Network Printers, terminal servers, X-terminals, hubs, UPS devices, and many other devices.

To update system information:

1. Specify the hostname or IP address of the device.
2. Specify the read-write community string of the device. You must provide the read-write community string or the update will fail.
3. Click **Retrieve Details**.
4. Specify the new name for the device in the System Name field.
5. Specify a new location.
6. Specify a new contact.

7. Click **Update Details.****Notes:**

- Ensure you specify the previous name assigned, if you do not want to update the information.
- If the update fails, the target device may not allow changes to the system information remotely.

