
WhatsUp Gold

User's Guide

Software Version 5

Ipswitch, Inc.

The information in this document is subject to change without notice and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. assumes no liability for damages resulting from the use of the information contained in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of that license.

Copyright © 1995-2000 by Ipswitch, Inc. All rights reserved. IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective companies.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transferred without the express prior written consent of Ipswitch, Inc.

Printing History

March 1997	First edition.
December 1997	Second edition.
April 1999	Third edition.
September 1999	Fourth edition.
March 2000	Fifth edition.

Contents

Preface	ix
What This Package Includes	ix
The Ipswitch Products	ix
Chapter 1: Introduction	1
What is WhatsUp Gold?	1
Mapping the Network	1
How It Works	3
Getting Information from the Network Map	3
Getting Status for a Device	4
Reporting	4
What's New in Version 5.0?	5
System Requirements	6
Upgrading	6
Installation	7
Trying WhatsUp Gold on Your Network	8
Creating a New Network Map	8
Adding a File Server	9
Initiating Monitoring	11
Running WhatsUp Gold as an NT Service	11
Setting Up to Run as an NT Service	11
Starting and Stopping the NT Service	12
Chapter 2: Creating Network Maps	13
Creating a Network Map	13
Discover and Map Network Devices	14
Mapping a Hierarchical Network	17
Using SmartScan	17
Results of the SmartScan	20
Mapping a Flat Network	21
Results of the Scan	23
Using the Scan WinNet Tool	25
Loading a Hosts File	25
Traceroute Mapping	26
Manually Drawing a Map	26
Reading a Network Map	27
Tips for Making a Map Easier to Read	27
Device Properties	28
The Polling Method	28
Defining General Properties	29
Setting Up Monitoring	31

Using the Right Mouse Menu	33
Adding a Command to the Right Mouse Menu	34
Program Variables	34
Custom Device Types	35
Creating a Custom Device Type	35
Changing the Double-Click Action for a Custom Device	38
Running a script or program for custom devices	38
Using the Custom Device on a Map	39
Scanning and Mapping a Custom Device	39
Changing the Standard Device Icons	40
Creating a Subnet	41
Setting Map Polling Properties	42
Setting the Map Display	44
Setting Map Colors	45
Editing a Network Map	46
Getting In and Out of Edit Mode	47
Draw Toolbar	47
Edit Toolbar	47
Keeping Tools Active	48
Drawing	48
Changing Item Properties	48
Attached Lines	48
Creating Text Captions	49
Arranging the Toolbars	50
Saving and Naming a Network Map	51
Saving a Context	51
Chapter 3: Setting Up Notifications	53
Defining Notifications	54
Defining System Notifications	54
Sound Notifications	55
WinPopups	55
Defining Pager Notifications	56
Defining Beeper Notifications	58
Defining E-mail Notifications	60
Defining Group Notifications	61
Notification Message Variables	63
Testing Beeper, Pager, and E-mail Notifications	64
Defining Program Notifications	64
Setting Up a Voice Modem	65
Defining Voice Notifications	66
Assigning Notifications to Devices	69
Using the Alerts Tab	69

Assigning a Notification	72
Editing Notifications	75
Assigning Notifications Globally	75
Chapter 4: Monitoring Services	79
Monitoring Standard TCP/IP Services	81
Monitoring Custom Services	83
Defining a Custom TCP/IP Service	83
Using Rules Expressions	86
Rules Expressions Text and Quantifiers Tables	87
Testing a Rules Expression	88
Summary of Service Monitoring Requirements	88
Custom Services API	89
Chapter 5: Working from the Console	91
Opening Network Maps	91
Starting and Stopping Polling	91
To Initiate Automatic Polling	92
To Stop Automatic Polling	92
To Check a Device	92
Reading the Network Map	93
Receiving Alarms	93
Receiving Notifications	94
Acknowledging Alerts	94
Using the Status Tab	94
Using the Status Window	96
Viewing and Changing Dependencies	96
Setting “Up” and “Down” Dependencies	98
Viewing the Polling Statistics	98
Viewing Active Notifications	100
Using the Mini Status View	100
Chapter 6: Logs and Reports	103
Logging and Reporting Events	104
Types of Events Logged	104
Changing How Events Are Logged	105
Viewing the Event Log	107
Creating an Event Report	107
Debug Log Information	109
Using the Command Line for Event Reports	109
Basic Command Syntax	109
Examples	110
Return Codes	110
Logging and Reporting Polling Statistics	111

The Polling Statistics	111
Changing Statistics Logging	112
Viewing the Statistics Log	112
Creating Reports on Polling Statistics	113
Exporting Raw Data	114
Statistics Report Legend	115
Using the Command Line for Statistics Reports	115
Basic Command Syntax	115
Examples	116
Return Codes	116
Creating Performance Graphs	117
Graph Options	117
Creating a Graph	118
Using Search Expressions	120
Sample Performance Graphs	121
Viewing, Printing, and Exporting Performance Graphs	122
Using the Command Line for Performance Graphs	123
Basic Command Syntax	124
Examples	125
Sending Recurring Status Reports	125
Chapter 7: Working from a Web Browser	129
Setting Up the WhatsUp Gold Web Server	129
Customizing Your WhatsUp Gold Web Site	130
Making Maps Available for Web Viewing	132
Setting Web Server Access	133
Default User Accounts for the Web Server	133
Setting Up User Accounts for the Web Server	133
Setting Web Access by IP Address	136
Logging On to the Web Server	138
WhatsUp Gold Web Display	139
WhatsUp Gold Web Functions	141
Chapter 8: Monitoring SNMP Devices	143
SNMP Implementation in WhatsUp Gold	143
SNMP Overview	144
Management Information Base (MIB)	145
Security	146
SNMP Agent or Manager	147
SNMP Operations	147
SNMP Traps	147
Setting Up the MIB Identifiers	148
Viewing SNMP Objects	149
Graphing SNMP Values	152

Starting the SNMP Graphing Utility	153
Adding, Editing, and Deleting SNMP Objects	153
Viewing Item Values	155
Editing Item Properties	156
Deleting Items from the Graph	157
Saving and Opening Graph Files	157
Editing Graph Properties	158
Receiving SNMP Traps	159
Setting Up Notifications for Traps	160
Viewing Trap Log Entries	162
Monitoring SNMP Service	162
Chapter 9: Using Network Tools	163
Using Format, Copy, and Print Functions	164
Printing Results	164
Displaying Device Information (Info Tool)	165
Checking a Web Address (HTML Tool)	166
Synchronizing Time (Time Tool)	167
Verifying Connectivity (Ping Tool)	170
Tracing a Route (TraceRoute Tool)	171
Finding Host and Name Server (Lookup Tool)	174
Getting Information About Users (Finger Tool)	176
Getting Owner Information (Whois Tool)	177
Searching Directories (LDAP Tool)	178
Viewing Quotations (Quote Tool)	180
Scanning Your Network (Scan Tool)	180
Viewing and Graphing SNMP Values (SNMP Tool)	180
Displaying Network Information (WinNet Tool)	181
Testing Data Speed (Throughput Tool)	181
Viewing Local System Information	183

Preface

WhatsUp Gold is a graphical network monitoring system designed for multi-protocol networks. WhatsUp Gold monitors your critical devices and services and initiates visual and audible alarms when there's a problem. In addition, WhatsUp Gold can notify you remotely by beeper, alphanumeric pager, e-mail, or telephone. WhatsUp Gold runs on Windows 2000, Windows NT, Windows 98, or Windows 95 on the Intel platforms.

What This Package Includes

WhatsUp Gold includes the following:

- WhatsUp Gold CD
 - License agreement
 - This manual, the *WhatsUp Gold User's Guide*
-

The Ipswitch Products

Other Ipswitch products include:

- **WS_FTP™ Pro FTP Client**

WS_FTP Pro provides two powerful Windows interfaces for connecting to remote hosts and transferring files. WS_FTP Pro includes the Find Utility, Scripting Utility, and Synchronize Utility.
- **WS_FTP Server**

WS_FTP Server is a full-featured FTP server for Windows NT systems. WS_FTP Server lets you create FTP sites that make files and folders on your PC available to other users. WS_FTP Server offers many features not found in most commercial servers today, including automatic resumption of interrupted transfers.
- **IMail Server**

IMail Server is an electronic mail server system based on Internet standards.

IMail Server provides Simple Mail Transfer Protocol (SMTP) for sending and receiving mail over the Internet or over an internal TCP/IP network. It supports any mail client that uses the Post Office Protocol, Version 3 (POP3) or Internet Message Access Protocol (IMAP4). Web Messaging lets users access their mail from any web browser; users do not need to have a mail client. IMail Server runs on Windows NT or Windows 2000 on the Intel platform.

- **WS_Ping ProPack™**

WS_Ping ProPack is the ultimate network information tool. It provides everything you need to help track down network problems and to get information about users, hosts, and networks on the Internet or on your intranet. Tools include Info, Time, HTML, Ping, Traceroute, Lookup, Finger, Whois, LDAP, Quote, Scan, SNMP, WinNet, and Throughput. WS_Ping ProPack runs on Windows NT, Windows 2000, Windows 98, or Windows 95 on the Intel platforms.

Chapter 1: Introduction

This chapter describes the basic operation of WhatsUp Gold and lists both standard and new features. In addition, you will find system requirements, upgrading and installation instructions, a quick “try it” procedure, and the procedure for running WhatsUp Gold as an NT service.

Note

For updated information since this manual was printed, see the Release Notes, *WhatsUpG.txt*.

What is WhatsUp Gold?

WhatsUp Gold is an easy-to-use tool for monitoring TCP/IP, NetBIOS, and IPX networks. WhatsUp Gold initiates both visible and audible alarms when monitored devices and system services go down. WhatsUp Gold can also notify you of problems by digital beeper, alphanumeric pager, e-mail, or voice message. WhatsUp Gold provides a web interface so you can view network status from a web browser on any computer on the Internet. You can configure WhatsUp Gold and start monitoring your network without any special training.

Mapping the Network

WhatsUp Gold can map your network in several different ways, including an automatic “discover and map” capability that can scan files and the Windows network. You can also create a network map by scanning for SNMP information, scanning a range of IP addresses, loading a hosts file, scanning a Windows network, or drawing it.

The WhatsUp Gold scan methods:

- Poll devices on the network to which your computer is connected
- Identify any TCP/IP, NetBIOS, or IPX devices
- Create a network map with an icon for each device (workstations, servers, hosts, bridges, routers, LAN boxes, hubs, printers). Each device is associated with a specific address.

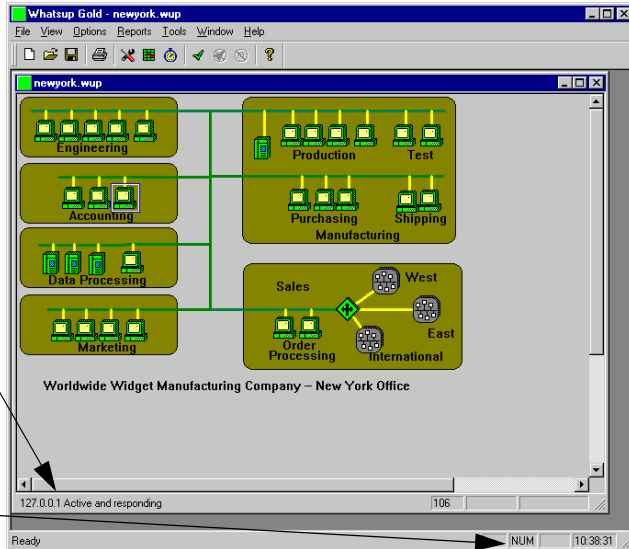
Note

To scan and poll IPX devices, you must have Microsoft NWLink IPX/SPX Compatible Transport installed and running on the system on which WhatsUp Gold is installed. For more information, see “System Requirements” on page 6.

When you open the network map window, WhatsUp Gold automatically begins monitoring the network.

When you place the cursor over a device icon, the status bar at the bottom of the map window shows the device name, address, and a brief status description, including the status of any services being monitored.

The status bar at the bottom of the WhatsUp Gold window displays the polling status and a timer that counts down the time between polls.



Note

Unless you have the express permission of the owners of particular devices, do not monitor host systems, workstations, or other devices that you do not control.

WhatsUp Gold is in either Monitor Mode or Edit Mode. Monitor Mode is the mode in which WhatsUp Gold polls the network. Edit Mode is the mode in which you make changes to the map; you can use Edit Mode to refine the network map, add devices, draw connecting lines, and convert icons to a different icon type. For more information, see “Manually Drawing a Map” on page 26.

How It Works

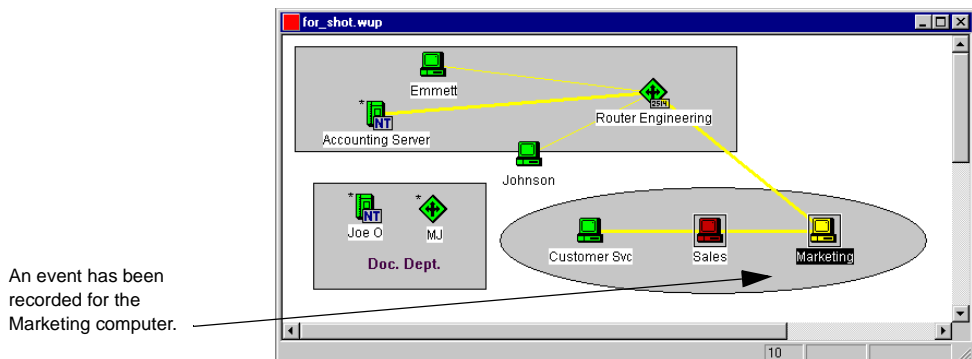
Once you have created or loaded a network map, you can set WhatsUp Gold to continuously monitor the network, or you can initiate a single “poll” of the network. One poll of the network involves checking each monitored device in the network map. Each “check” consists of WhatsUp Gold sending a poll request to a device and tracking the response.

For each monitored device, you can choose from a set of options in the device properties to determine how the device is monitored and define what action to take if the device does not respond to a check.

On each TCP/IP device in your network map, you can determine which services are running on that device (such as HTTP, SMTP, POP3, DNS) and you can select those services you want to monitor; WhatsUp Gold monitors a service by communicating with the default port that the service runs on.

Getting Information from the Network Map

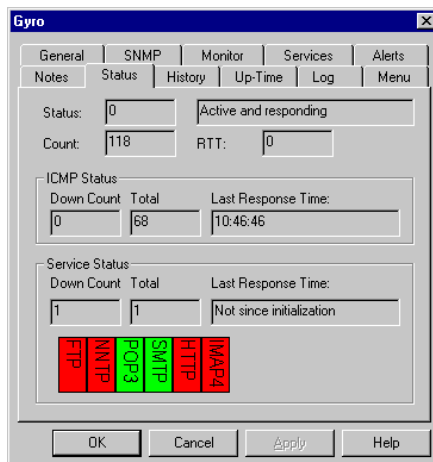
In Monitor Mode, the map gives graphic indication of potential and actual problems on your network. If an event occurs such as a device going down, the name of the device becomes inverted on the map.



In addition, colors indicate the status of the various devices. By default, devices that respond to polls are displayed in green, those that have missed one poll are light green, those that have missed two polls are yellow, and those that are not accessible (or have not responded to four polls) are red. (You can change the default colors.)

Getting Status for a Device

In Monitor Mode, you can display up-to-the-minute status information about a device by double-clicking the device icon to display the device properties, and then clicking the **Status** tab.



In addition, you can define notification actions (such as sending a message to a pager or e-mail account) for a device or a range of devices.

Reporting

WhatsUp Gold logs two types of data: changes in network status (called events), such as a device going down; and, polling statistics for each device.

From this logged data, WhatsUp Gold can create several reports and graphs that show the status of your network in different ways. From the **Reports** menu, you can create the following:

Event Reports. Show device up and down events, service up and down events, and WhatsUp Gold events such as map open and close.

Statistics Reports. Show the accumulated polling statistics by device.

Performance Graphs. Show devices by best or worst performance based on aggregated polling statistics.

Recurring Reports. Show network status (count and names of devices that are up, and those that are down) and send as a pager, e-mail, or beeper message.

What's New in Version 5.0?

Version 5 of WhatsUp Gold offers many new capabilities:

- **SmartScan Using SNMP** (on the **Tools** -> **Import** menu) discovers and maps devices by reading SNMP data on your network's default router. This scan method creates maps that reflect your network's hierarchy, with separate maps for various levels of subnetworks.
- SmartScan and Scan can now be started from the Discover and Map wizard (available by selecting **File** -> **New**).
- You can create **Performance Graphs** (from the **Reports** menu) that plot the accumulated polling statistics for selected maps and devices. The Performance Graphs can show aggregate data, such as the devices with the best and worst availability, or the devices with the highest and lowest average response time, and the best and worst days of the week for network performance.
- You can now jump to the parent map from a subnet map (in the subnet map, right-click and select **View parent map** from the pop-up menu). You can also set or change the parent map in the Map properties for the subnet map (right-click in the subnet map and select **Map properties** from the pop-up menu).
- Ability to display maps with icons in the web interface.
- SmartScan and Scan can identify devices that are SNMP manageable and record SNMP information in the **SNMP** tab in device properties. This information can be useful when querying a device with the SNMP tool.
- The **Change SNMP Communities** tool (on the **Tools** menu) lets you do a global change of Read and Write community names in your map.
- You can edit or replace the standard icons used to display devices on a map. For more information, see "Changing the Standard Device Icons" on page 40.
- You can set the Map Display properties to apply to all new maps and the **Map Properties** (on the **File** menu) have been reorganized.

System Requirements

WhatsUp Gold requires the following system resources:

- An Intel 386, 486, or Pentium Family processor or equivalent
- Windows NT 4.0 or greater, Windows 2000, Windows 98, or Windows 95
- A TCP/IP protocol stack. Supported stacks include those from Microsoft (Windows NT, 2000, 98, 95)
- If you want to install the Performance Graphs capability, you need to first install Microsoft's Open Database Connectivity (ODBC) interface and the ODBC text driver.

WhatsUp Gold sets up the statistics data, from which graphs are created, as an ODBC database.

ODBC is installed as part of Microsoft Office 97, or you can obtain the ODBC files from Microsoft's web site at: www.microsoft.com/Data/mdac2.htm.

You do not need to set up the ODBC data source. If the WhatsUp Gold installation procedure finds ODBC on your computer, it automatically sets up the data source (DSN) for Performance Graphs. The data source is *wugstats.log* (in the WhatsUp directory) and uses the Microsoft .txt database format.

- To scan and poll IPX devices, Microsoft's NWLink IPX/SPX Compatible Transport must be installed and running on the system on which WhatsUp Gold is installed. You can add this transport using the Control Panel Network applet. (In the "Select Network Protocol" dialog box, select **Microsoft** and **IPX/SPX-compatible Protocol** and follow the online instructions.)

Upgrading

If you are upgrading from a previous version of WhatsUp Gold or WhatsUp, you should note the following:

- Be sure that WhatsUp Gold has completely shut down before upgrading. If you exit WhatsUp Gold during a poll, it may take up to 30 seconds for the application to be removed from memory. Until then, WhatsUp Gold appears in the Windows task list.

- Back up your network maps (*.db* for WhatsUp and *.wup* for WhatsUp Gold). When you open a WhatsUp file in WhatsUp Gold, it is automatically converted to the *.wup* format and saved with a *.wup* extension. Note that *.wup* maps saved in Version 5.0 cannot be used in previous versions of WhatsUp Gold.
- During installation, WhatsUp Gold will compare its own *mib.txt* and *traps.txt* files with any already present. If there is a difference, it asks if you want to overwrite your old *mib.txt* and *traps.txt* files; answer **No** if you have customized WhatsUp Gold to recognize vendor-provided SNMP objects.

Note

All defined notifications are stored in a file *ipnotify.ini*. This file is shared by other Ipswitch products and is therefore not deleted or replaced when you uninstall or upgrade WhatsUp Gold. Furthermore, if you ever move WhatsUp Gold to a new system, you will need to manually copy the *ipnotify.ini* file to the Windows or NT directory of the new system.

Installation

To install or upgrade WhatsUp Gold:

- 1 Do one of the following:
 - If you purchased a WhatsUp Gold CD-ROM, insert the CD-ROM in a drive. If the installation program does not run automatically, then click **Start**, select **Run**, and then enter the CD path followed by `AutoRun.exe`. For example:
`d:\AutoRun.exe`
 - If you downloaded WhatsUp Gold from the Internet, run the downloaded application, *wugold.exe*.
- 2 To view a demo of WhatsUp Gold, open the map named *world.wup*.

WhatsUp Gold uses Microsoft's Open Database Connectivity (ODBC) interface and the ODBC text driver to create performance graphs.

If the installation program finds ODBC installed on your computer, it automatically installs the Performance Graphs capability and sets up the ODBC data source to use for creating graphs.

If the installation program does not find ODBC, it asks if you want to continue the installation. If you want to use the Performance Graphs, we recommend that you:

- 1 Click **No** to cancel the installation.
- 2 Install ODBC (for ODBC information see “System Requirements” on page 6).
- 3 Restart the WhatsUp Gold installation program.

Trying WhatsUp Gold on Your Network

The following procedures let you try out WhatsUp Gold. They take you through starting a simple network map, adding a file server, and editing the map.

Creating a New Network Map

To create a new network map:

- 1 Select **New** from the **File** menu.
- 2 Select **Create a blank map** and click **Finish**.

WhatsUp Gold displays a blank map.

Edit Mode button

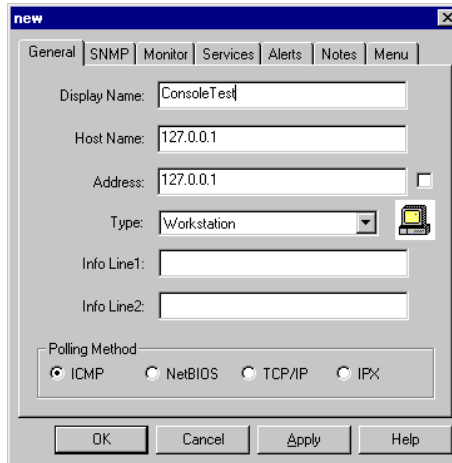


Add Workstation
button



- 3 Click the **Edit Mode** button in the main toolbar. WhatsUp Gold displays the **Edit Mode** toolbars.
- 4 Click the **Add Workstation** button in the Edit Toolbar, and then click the map to create an icon for the workstation.

- 5 Double-click the icon you just created to view device properties.



- 6 On the **General** tab, enter the information as shown. Set the **Display Name** to *ConsoleTest* or whatever name you would like for the WhatsUp Gold console (the system on which WhatsUp Gold is installed).

Set the **Address** to 127.0.0.1, which is the default. (This is the local “loopback” network address; it is the address you use to monitor your own system *from* your system.)

- 7 Click the **Monitor** tab and select **Monitor This Device**.
- 8 Click the **Alerts** tab and select **Enable alerts** and **Enable Sound**.
- 9 Click **OK**.

Adding a File Server

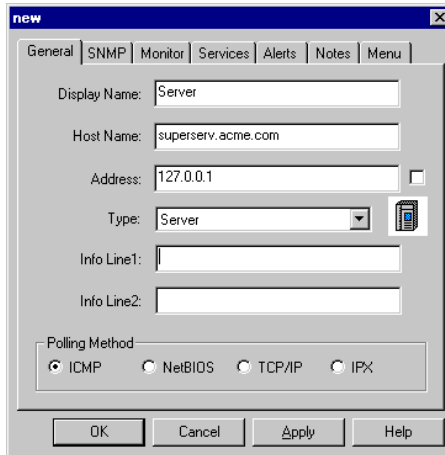
To create an icon for one of your file servers:

Add Server tool



- 1 Click the **Add Server** tool in the Edit Toolbar, and then click the desired location on the map to create the icon.

- 2 Double-click the icon you just created to view its properties.



- 3 On the **General** tab, set the **Display Name** to *Server*.
- 4 Set the **Address** to the IP address, or set the **Host Name** text box to the name of a system on your network. (Note: If you use a name, the network stack must be able to resolve it from a local hosts file or by looking it up on a Domain Name Server, a server that lists host names and their IP addresses. This name is looked up whenever the map is loaded.) Then, click **Apply**.
- 5 Click the **Monitor** tab; make sure **Monitor This Device** is selected.
- 6 Click the **Alerts** tab, select **Enable alerts** and **Enable Sound**, and then click **OK**.
- 7 Save the map by selecting **Save As** from the **File** menu. Save the map with the name of *MyTestMap.wup*.

Initiating Monitoring

You are now ready to start monitoring your little network of two items.

Edit Mode button



1 Click the **Edit Mode** button to exit Edit Mode and return to Monitor Mode.

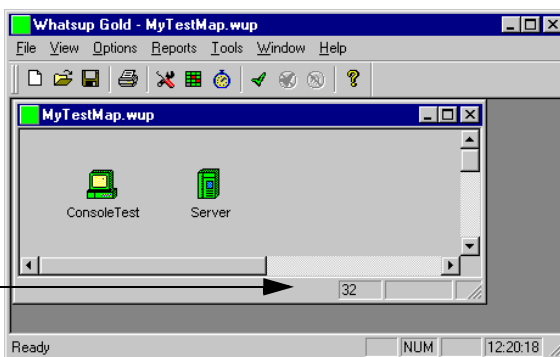
Check button



2 Click the **Check** button to poll the network.

Your screen should look something like this.

Number of seconds to start of next automatic poll.



Running WhatsUp Gold as an NT Service

WhatsUp Gold can run as a system service on Windows NT 4.0 or later. When running as a service, WhatsUp Gold uses only the web interface as its user interface. To use less memory, no map windows are opened on the WhatsUp Gold NT console.

Running WhatsUp Gold as an NT service allows you to log off the NT console, thus providing an extra level of security; the service can run completely hidden. As with any NT service, you can set WhatsUp Gold to restart whenever Windows NT is rebooted.

Setting Up to Run as an NT Service

We recommend that you create your network maps using WhatsUp Gold in normal operating mode on the Windows NT console. Once your maps are created, select any desired program options (from the **Options** menu, select **Program**). These options will be in effect during operation as an NT service.

On the **Startup** tab in the program options, you can specify multiple maps to load at startup in the **Map Names** box by specifying the names of the maps, separated by commas. Additional maps can be subsequently loaded and unloaded using the web interface, provided the maps are in the directory specified in the **Directory** box. Note that the “contexts” capability, which lets you save a particular configuration of WhatsUp Gold windows, cannot be used when operating WhatsUp Gold as an NT service.

Set any of the web server options (select **Web Server** from the **Options** menu). Turn on the **Enable Web Server** option on the **Web** tab. For more information about web server options, see “Chapter 7: Working from a Web Browser” on page 129.

If you set up any permissions or other web configuration parameters (set on the **Web** and **Web Users** tabs) while running WhatsUp Gold in normal operating mode on the NT console, you may need to stop and restart the NT service mode (see section below).

On the **Web Users** tab, if you select **Automatically save changes from web interface**, you will be able to change user options from the web interface.

Starting and Stopping the NT Service

Your WhatsUp Gold installation includes an executable file named *wugsvc.exe* for the purpose of installing, removing, starting, and stopping the WhatsUp Gold NT service.

To install and start WhatsUp Gold as an NT service, enter the following command at the Command Prompt:

```
wugsvc -install
```

To remove WhatsUp Gold as an NT service, enter the following command at the Command Prompt:

```
wugsvc -remove
```

Note that these two commands don’t install or remove WhatsUp Gold; they merely install and remove the NT service capability.

Chapter 2: Creating Network Maps

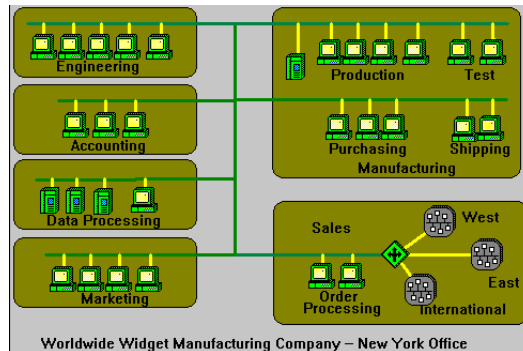
With WhatsUp Gold, you can use one of the automatic methods to quickly create a map of your network; then you can start monitoring your network immediately, using the default properties that WhatsUp Gold assigned to the map and the individual network devices.

However, you'll probably want to customize WhatsUp Gold so it polls your network in exactly the way that best suits your needs. This chapter describes how to do the following steps to create your map:

- 1 Create a network map using one or more WhatsUp tools or techniques.
- 2 View and edit the default properties for network devices (hosts, servers, etc.).
- 3 View and edit the default map properties.
- 4 Use Edit Mode to visually organize your network map.

Creating a Network Map

The network map is a graphical representation of the devices in a network. The following shows a typical network map.



Network devices can be workstations, hosts, servers, routers, bridges, hubs, LAN boxes, printers, subnetworks (“subnets”), or custom host types.

WhatsUp Gold provides several methods and tools to create a network map and add devices to it:

- Discover and Map - automatically discovers the devices on your network by using a variety of information sources. A wizard steps you through the process and lets you select the “discover” methods.

Note

SmartScan, Scan, Load hosts file, and Scan WinNet can be run as part of the Discover and Map capability or on their own.

- SmartScan - locates devices by reading SNMP information on your network. This is the best way to discover and map a hierarchical network because it creates subnetwork maps and links them to the parent map.
- Scan - locates devices within a range of IP addresses.
- Scan WinNet - scans your Windows network for devices.
- Load hosts file - uses the hosts file on your system.
- Traceroute tool - maps routers between your local host and a remote host.
- Edit Toolbar - provides tools you can use to manually add devices to a network map.

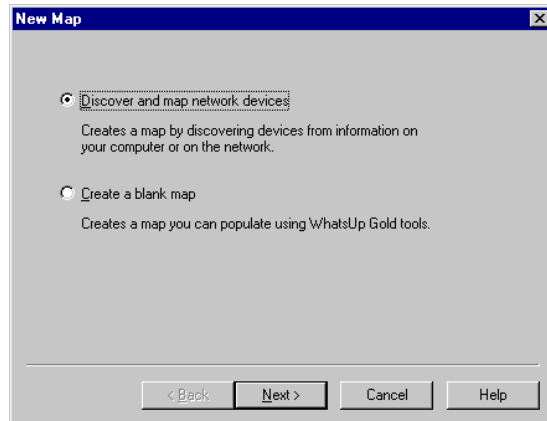
You can use any combination of WhatsUp Gold methods and tools to create a network map. Each of these methods and tools is described in the following sections.

Discover and Map Network Devices

The Discover and Map capability creates a map from information on your computer — or on the network to which your computer is connected — by reading network files and identifying devices listed in the files. These files can include a hosts file, the Windows registry, and Windows network information. Discover and Map can also find devices by reading SNMP information on the network or by scanning a range of IP addresses.

To use the Discover and Map capability:

- 1 From the **File** menu, select **New** to view the following dialog box.



- 2 Select **Discover and map network devices**, and then click **Next**. The Discover Devices screen appears.



- 3 Select the parameters you want to use to create the map.

Intelligently scan network with SNMP. Reads SNMP information on your default router to identify devices on your network and also identifies and maps subnets within your network. Use this option to map a hierarchical network, if your network is SNMP enabled. The Discover Devices wizard will display additional options for scanning with SNMP. If you select this option, you cannot select **Discover devices with ICMP**.

Discover devices with ICMP. Scans a range of IP addresses and maps the devices that respond to a message sent via the Internet Control Message Protocol (ICMP). Use this option to map a single network that does not contain subnets (all devices will be displayed on one map). The Discover Devices wizard will display additional options for the scan. If you select this option, you cannot select **Intelligently scan network with SNMP**.

Import devices from registry. Reads the Windows registry to find devices that are referenced in the TCP/IP, Microsoft Internet Explorer, or Netscape Navigator configurations, then automatically adds the devices to the map.

Import devices from hosts file. Reads the hosts file on the local system and creates an icon for each network device.

Discover devices from Network Neighborhood. If your computer is connected to a Microsoft Windows network, WhatsUp Gold scans the network and creates an icon for each device it finds. (This can take a few minutes, depending on the size of your network.)

- 4 Click the **Next** button. An information screen appears. Click **Finish** to start the Discover and Map process. Depending on the Discover options you selected, WhatsUp Gold does the following:
 - If you selected **Intelligently scan network with SNMP**, displays the “SmartScan” dialog box with default values filled in. Click **Start** to proceed. To change the default values; see “Mapping a Hierarchical Network” on page 17.
 - If you selected **Discover devices with ICMP**, displays the “Scan” dialog box with default values filled in. Click **Start** to proceed. To change the default values; see “Mapping a Flat Network” on page 21 for more information.
 - Reads the network files and creates icons for any devices it finds.
- 5 From the **File** menu, select **Save** or **Save As** to save the map.
- 6 See “Tips for Making a Map Easier to Read” on page 27.

Mapping a Hierarchical Network

If your network has a router with an SNMP agent, SmartScan is a powerful way to discover and map your network, as it can create maps and subnet maps that reflect your network's hierarchy. SmartScan discovers and maps devices by reading SNMP data on a device (preferably a router) in your network. Based on the information it finds, SmartScan will continue to scan your network until it has mapped all devices.

To make sure you scan only those devices in your own network, you can use the **Depth** and **Limit scan to IP address of root device** options. Also, the scan will stop if it comes to a network for which it does not know the **Community** name.

Note

Do not scan devices on someone else's network without their permission!

You can also enable the scan so that it discovers a custom device type and creates a custom icon for the device. For information on how to do this, see "Custom Device Types" on page 35.

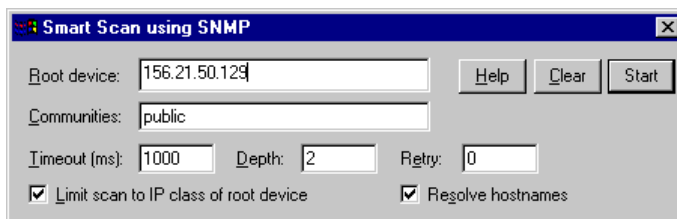
Using SmartScan

SmartScan maps and displays the devices according to your network's hierarchy. If your network is divided into subnets, SmartScan creates a parent map of the top-level network and also creates a map for each subnet. The parent map will show links to its subnets, and any subnet map can have links to lower-level subnets.

To discover and map devices on your network using SmartScan:

- 1 If you are not already in the "SmartScan using SNMP" dialog box, you can start a scan in either of the following ways:
 - To create a new map, select **New Map** from the **File** menu. In the New Map, select the **Discover and Map Network Devices** option on the first screen and select **Intelligently scan network with SNMP** on the next screen. Click **Next**, then click **Finish** to complete the wizard.
 - To add devices to an existing map or a blank map, select the map, then select **Import -> SmartScan** from the **Tools** menu.

The “SmartScan Using SNMP” dialog box appears. WhatsUp Gold enters default values in this dialog box from information it finds on your local machine.



- 2 Enter or change the **Root device**. This is the host name or IP address of an SNMP-enabled device in your network. In most cases, it uses the default router specified in the Windows registry on the local machine. You can change the entry box to a different device on your network.
- 3 Enter or change the SNMP Read **Communities** used in your network. These community names are a type of password; the scan needs to know these names to read SNMP data on your network. Separate each community name with a comma.

The order in which you enter community names is important because it could increase the scan time per device. The scan checks a device for the first community name, then the second, and so on. If the first name matches the device's community name, the scan moves on to the next device. So you should list the most widely-used community name first.
- 4 Optionally, enter or change the **Timeout** value. This is the number of milliseconds (ms) after which the scan stops trying to do an SNMP query or ping a device.
- 5 Optionally, enter or change the **Depth** value to set the levels of your network that you want to scan. The default value of 2 means that the scan discovers and creates a parent map of your top-level network and any of its subnets. If a subnet itself has a subnet, you would have to enter a Depth of 3 to make the scan go to that level.
- 6 Optionally, enter or change the **Retry** value. This is the number of times to re-try to discover a device at a given IP address, if the initial attempt fails. We recommend setting this to zero, particularly if you are using multiple **Communities**.

- 7 **Limit scan to IP class of root device** is turned on by default. This option limits the scan to the network class defined by the IP address of the **Root device**. If the IP address is within the network class (class A, B, or C network) of the root device, the scan proceeds; otherwise, the scan skips to the next IP address.

Note that the **Communities** and **Depth** settings further limit the scan.
- 8 Optionally, turn on **Resolve hostnames** if you want to display the host name (rather than the IP address) as the device label in the map. Note that this requires “looking up” the host name associated with each IP address and thus it can take longer to complete the scan.
- 9 Click **Start** to start the scan. When the scan starts, the **Start** button toggles to **Stop**. Click **Stop** at any time to end the scan. When the scan is complete, the Stop button toggles back to **Start**.
- 10 Click **Exit** to close the “SmartScan” dialog box.
- 11 From the **File** menu, select **Save** or **Save As** to save the map.
- 12 See “Tips for Making a Map Easier to Read” on page 27.

Note

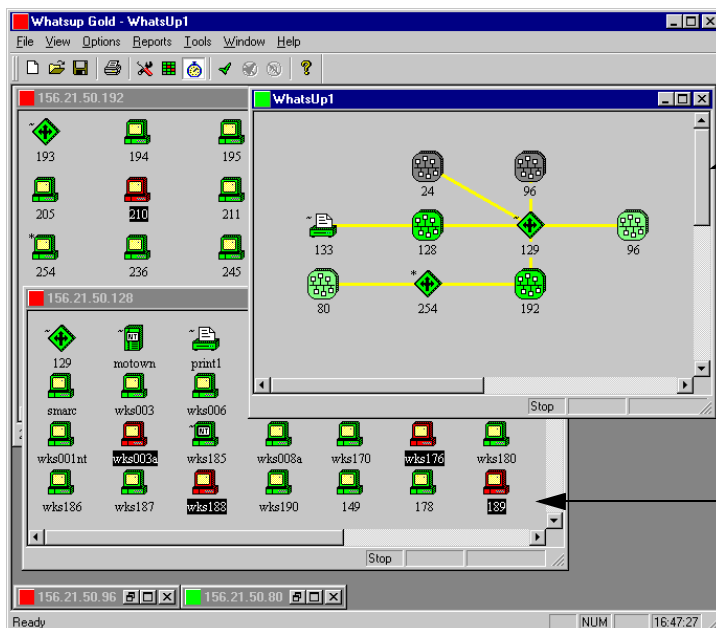
The default settings limit the scan to your network. WhatsUp Gold provides control over these settings so that you can further limit or change the scan to reflect your unique network topology.

Note

Never try to discover and map devices on a network that is not owned by your organization!

Results of the SmartScan

SmartScan creates a map hierarchy that reflects your network and its subnets. It creates a separate map for each subnet and creates a parent map with links to the subnets.



Parent map shows status of subnets. To open a subnet map, double-click its icon.

Subnet map shows devices in the sub-network's range of IP addresses.

Note

A map created by SmartScan may show other networks connected to your network as a gray subnet icon. This means the scan was unable to map the devices in that subnet because the scan settings would not allow it.

Mapping a Flat Network

If you have one network with no subnets, or you want to create subnets manually, you can use the Scan tool.

The Scan tool automatically detects the network devices *within a specified range* of IP addresses and creates a single map. You specify a range of IP addresses to be scanned, and WhatsUp Gold polls each address in the range. If WhatsUp Gold finds an active network device in the range, it creates an icon for the device.

You can also enable the scan so that it discovers a custom device type and creates a custom icon for the device. For information on how to do this, see “Custom Device Types” on page 35.

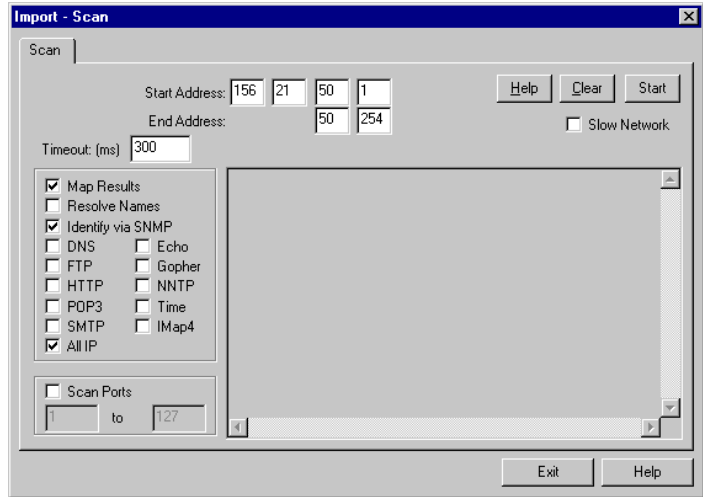
A scan can also identify the network services (such as FTP, HTTP, SMTP) on each network device.

If you want to view the results of a scan before creating the map, turn off **Map results**. When you are ready to create the map, you can turn it back on and run the scan again.

To start a scan:

- 1 Select an existing map or create a new map window.
 - To create a new map, select **New Map** from the File menu. In the New Map wizard, select the **Discover and Map Network Devices** option on the first screen and select **Discover devices with ICMP** on the next screen. Click **Next**, then click **Finish** to complete the wizard.
 - To add devices to an existing map, select the map, then select **Import -> Scan IP** from the Tools menu.

The following dialog box appears.



- 2 Enter a range of network addresses to scan. Your current network is used as the default range.

The scan works consecutively from the last number of the **Start Address** through the last number in the **End Address**. For example, if you enter 245.245.1.50 as the **Start Address** and 245.245.10.60 as the **End Address**, the scan only scans from 50 to 60 in each of the networks from 245.245.1 through 245.245.10.

- 3 Set the scanning options.

Map Results. When this option is checked, the scan creates an icon for each device that it finds. Use this option when creating a map. This option is checked by default.

Resolve Names. When this option is checked, the scan displays the host name for each device and uses the host name (rather than the IP address) as the device label in the map (if **Map results** is checked.) Note that this requires “looking up” the host name associated with the given IP address and thus it can take longer to complete the scan.

Identify via SNMP. When this option is checked, if the scan finds an SNMP object identifier for a device, it uses the identifier to check for a custom device type (in the *hosttype.ini* file). If a custom device type is associated with the identifier, the icon for

that type is used in the map. The scan also checks the **SNMP Manageable** option in the device's SNMP tab, and adds the SNMP object identifier to the SNMP tab.

Timeout. Enter the timeout in milliseconds (ms). If a device does not respond to the scan within this time, the scan continues on to the next IP address. The Timeout should be set to 300 ms or greater. For maximum scanning speed, set Timeout to 300 ms and turn off **Resolve Names**.

DNS, Echo, FTP, Gopher, HTTP, IMAP4, NNTP, POP3, SMTP, Time. Select the services you want to scan for, and WhatsUp Gold will scan each active network device in the IP address range for the selected services. However, note that scanning network devices for these services can significantly increase the time it takes to complete a scan.

All IP. When **All IP** is selected, the scan finds all the devices in the specified range of IP addresses. If **All IP** is *not* selected, the scan finds only those devices that are running one of the selected services. For example, if you want to map only the devices that are running SMTP, you turn off **All IP** and turn on **SMTP**.

Scan Ports. Make sure this is *not* selected when creating a map. See the Scan tool help topic for other uses of this tool.

4 Click **Start**.

The **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the scan. Wait at least three seconds for the system to respond to a **Stop** request.

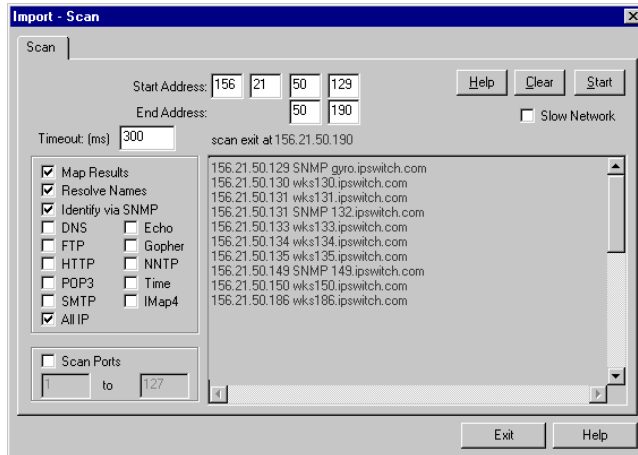
5 Click **Exit** to close the dialog box.

6 From the **File** menu, select **Save** or **Save As** to save the map.

7 See “Tips for Making a Map Easier to Read” on page 27.

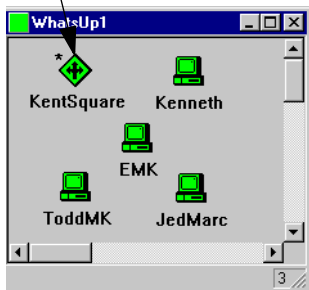
Results of the Scan

When you use the Scan tool as described above, WhatsUp Gold scans the range of IP addresses. For each active IP address it finds, it lists the address. It also lists the host name if **Resolve Names** is turned on.

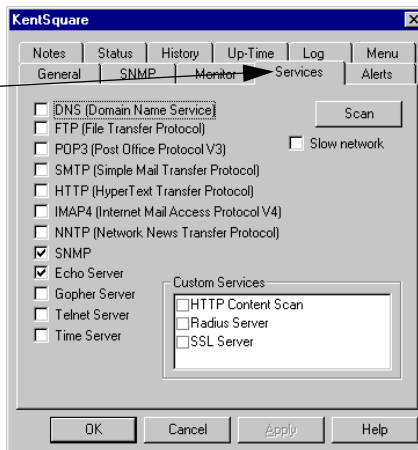


If **Map Results** is selected, WhatsUp Gold creates an icon on the active map for each device it finds. If you scan for particular services, the devices running those services will have those services checked on the device properties **Services** tab.

On the map, devices that have an SNMP service running are flagged with an asterisk or tilde.



Double-click the device icon to view the Services tab.



(Under the right conditions, the Scan can also recognize custom device types. For more information, see “Scanning and Mapping a Custom Device” on page 39.)

Using the Scan WinNet Tool

The Scan WinNet tool creates a map by scanning the Windows network to which your computer is connected, and finding the other devices on the network. It creates an icon for each device that it finds on the network.

To start a Scan WinNet:

- 1 Select an existing map or create a new map window.

To select an existing map, select **Open** from the **File** menu and enter the map file name; the devices found on the Windows network will be added to this map.

To create a new map, select **New** from the **File** menu. Select **Create a blank map**, and then click **Finish**.

- 2 From the **Tools** menu, select **Import -> Scan WinNet**.

WhatsUp Gold scans your Windows network and creates an icon on the map for each device that it finds. Note that this scan can take a few minutes to complete depending on the size of your network.

Note

The Scan WinNet tool will also find NetWare devices.

- 3 From the **File** menu, select **Save** or **Save As** to save the map.
- 4 See “Tips for Making a Map Easier to Read” on page 27.

Loading a Hosts File

You can load a hosts file (which lists device names and their associated IP addresses) and WhatsUp Gold creates an icon for each device listed in the file.

- 1 Select an existing map or create a new map window.

To select a map, select **Open** from the **File** menu and enter a map file name; the devices in the hosts file are added to this map.

To create a new map, select **New** from the **File** menu. Select **Create a blank map**, and then click **Finish**.

- 2 From the **Tools** menu, select **Import -> Hosts File**. The “Browse” dialog box appears.
- 3 Locate the hosts file and click **OK**. WhatsUp Gold reads the hosts file and creates an icon for each network device it finds.
- 4 From the **File** menu, select **Save** or **Save As** to save the map.
- 5 See “Tips for Making a Map Easier to Read” on page 27.

Traceroute Mapping

The Traceroute tool lets you map the network devices (usually routers) that comprise the route of an IP packet from your local host to a remote Internet host. WhatsUp Gold displays an icon for each router and shows the connections from router to router.

For information on how to use the Traceroute tool, see “Tracing a Route (TraceRoute Tool)” on page 171.

Manually Drawing a Map

You can create network devices manually by using Edit Mode.

- 1 Select an existing map or create a new map window.
To select an existing map, select **Open** from the **File** menu and enter the map file name.
To create a new map, select **New** from the **File** menu. Select **Create empty map**, and then click **Finish**.
- 2 In the main toolbar, click the Edit Mode button. The editing toolbars appear.
- 3 Use the drawing tools to create network devices. For more information, see “Editing a Network Map” on page 46.
- 4 From the **File** menu, select **Save** or **Save As** to save the map.
- 5 See “Tips for Making a Map Easier to Read” on page 27.

Edit Mode button



Reading a Network Map

When WhatsUp Gold is in Monitor Mode, it polls the active network maps. The icons on the map indicate the status of the various network devices. As explained in the previous chapter, when an event occurs (such as a device going down or a trap is received) the name of the device becomes inverted on the map. In addition, the colors of the device icons also indicate certain events as explained in “Getting Information from the Network Map” on page 3.

The indicators on the map are not the only way of getting status information about your network. The **Status** tab of the device properties also gives information about an individual device, and the Event Log lists all events for all open maps; both are covered in “Chapter 5: Working from the Console” on page 91.

In addition, you can get information by defining and activating notifications which are sent when particular events occur; for more information, see the following chapter.

Tips for Making a Map Easier to Read

If you have a large number of devices in your network and you used Discover and Map, SmartScan, Scan IP, or Scan WinNet to create a network map, the first version of the map may be a bit difficult to read. Use the tips below for making your map more readable.

- Select **Map Properties** from the **File** menu, click the Display tab, and then select **Clip Names**. You can also try the **Wrap Names** option to see if that makes the device names easier to read.
- Enter or modify the properties of the network devices. For starters, you might want to turn off monitoring for those network devices that you don’t need to monitor right away.

To do this, double-click the device icon to view the device properties; then click the **Monitor** tab and make sure **Monitor This Device** is turned off.

Edit Mode button



- Click the Edit Mode button and then drag device icons to new locations. For more information on organizing devices using shapes and lines, see “Editing a Network Map” on page 46.
- If the map contains overlapping icons, you can automatically arrange the icons on a map by selecting **Arrange Icons** from the

View menu. This feature arranges all icons on the current map in equally spaced rows starting in the top left corner. Do not use **Arrange Icons** if you have already set up the map the way you want it to appear.

- To change a device's icon, right-click it and select **Item Properties** from the pop-up menu. Click the **General** tab, then select a new **Type**.

Device Properties

WhatsUp Gold needs basic information about a device in order to monitor it. When you create a map using any of the “discover and map” tools, WhatsUp Gold automatically determines the device's display name, host name, and IP address. This section describes why you might edit the default device properties that WhatsUp Gold assigns.

The Polling Method

By default, WhatsUp Gold uses the ICMP polling method for TCP/IP devices, IPX for IPX devices, and NetBIOS for NetBIOS devices. You can change the default polling method at the bottom of the **General** tab of the device properties.

- **ICMP** sends packets (echo requests) to a device and tracks the responses.
- **TCP/IP** can be used to monitor a service on a device that does not allow ICMP packets (as in the case of some firewalls). The **TCP/IP** setting uses either TCP or UDP to poll the service. To use this method of monitoring a device, at least one service must be monitored on that device (selected on the **Services** tab of the device properties).
- **NetBIOS** is the polling method to use for Windows networks.
- **IPX** is the polling method for Novell NetWare networks.

Note

To scan and poll IPX devices, the system on which WhatsUp Gold is installed must have Microsoft NWLink IPX/SPX Compatible Transport installed and running. For more information, see “System Requirements” on page 6.

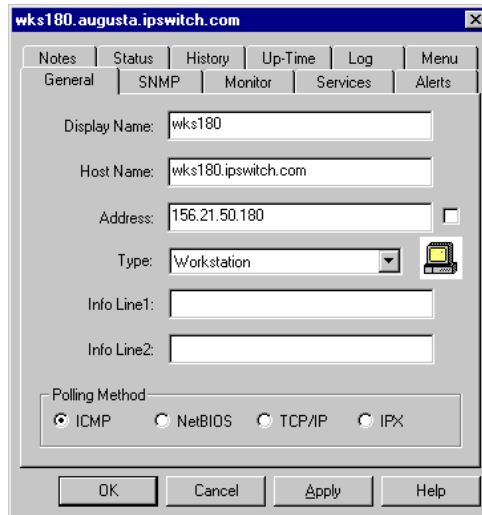
If the polling method for a device is NetBIOS or IPX, you will *not* be able to monitor TCP/IP services on this device.

Defining General Properties

On the **General** tab, you can make any changes to general properties, change the icon type for the device, and set the method WhatsUp Gold uses to poll the device.

To view or change device properties:

- 1 Right-click the device and select **Item Properties** from the pop-up menu. Click the **General** tab.



- 2 In the **Display Name** text box, enter a name. This is the name displayed on the network map.
- 3 **Host Name.** If the polling method is ICMP or TCP/IP, enter either the host name here or the IP address in Step 4. If you enter a host name, it must be a name that can be resolved to an IP

address. In other words, the host name must be in your system's host file or in your network's DNS server.

If the polling method is NetBIOS or IPX, you *must* enter a valid NetBIOS or IPX name.

- 4 In the **Address** text box, enter a valid IP address.

If the polling method is ICMP or TCP/IP and you entered a **Host Name** in Step 3, you can leave this blank and WhatsUp Gold will use the **Host Name** to look up the IP address.

Check the box next to the **Address** text box only if you want WhatsUp Gold to look up the IP address *each time* it checks this device. (This is useful if you use DHCP to assign IP addresses dynamically, but note that if you use this feature for a large number of devices, the name lookups put a heavy load on the DNS server.)

If the polling method is NetBIOS or IPX, leave the address blank; WhatsUp Gold displays the hardware Ethernet address of the device *after* it completes one poll.

- 5 In the **Type** box, select the desired device type from the drop-down list. This selection determines which icon is displayed on the network map. Note that the subnet icon is a special type that is used to link a subnet map to a parent map. For more information, see "Creating a Subnet" on page 41.
- 6 In the **Info Line 1** and **Info Line 2** text boxes, enter any additional information about this device. This information can be included in notification messages. For example, you can enter a "point of contact" for a device or location. This information is also displayed on the Host Summary page in the web interface.
- 7 Under **Polling Method**, select the method to use for polling this device. For detailed information, see "The Polling Method" on page 28.
- 8 Click **Apply** to apply your changes. Click **OK** to apply the changes and exit the dialog box.

Setting Up Monitoring

You use the **Monitor** tab to turn monitoring on or off for a device, to specify how often to check the device, the number of seconds to wait for a response, and any up or down dependencies.

- 1 In the device properties, click the **Monitor** tab.



- 2 Make sure **Monitor This Device** is selected.
- 3 In the **Poll Frequency** text box, enter a value to determine how often this device should be checked. The **Poll Frequency** determines if this device is checked on every poll (value = 1), every second poll (value = 2), every third poll (value = 3), and so on. The default value is every poll (1), but you can use this property to poll a particular device less frequently.
- 4 In the **Timeout** text box, enter the number of seconds to wait for a response from a monitored device.

You can enter a value from 1 to 20 seconds. The default value is 5 seconds. This timeout should be set to the smallest possible value. For a local network, a timeout of 2 seconds is usually sufficient. For a long-distance (or slow-path) network, this timeout may need to be as high as 10 seconds.

Note

For information on setting the default **Poll Frequency** and **Timeout** for all devices in the map, see “Setting Map Polling Properties” on page 42.

- 5 Set the **Time Period** options to specify when you want to monitor this device. Click the **Change** button to change the default setting of 7 days a week, 24 hours a day.

Select the **Day of Week** options: **7 days a week** is the default. You can clear the **7 days a week** option and then select the specific days of the week that you want to monitor this device.

Select one of the three **Time of Day** options: Use **24 hours a day** to monitor all day. Use **Between** to set the start and end time for monitoring. Use **Not between** to set the hours that monitoring is turned off.

Note

When using **Between** and **Not Between**, the start time must be less than the end time. To set the period between an AM time and a PM time, you must use the 24 hour clock (0000 to 2400) or use the options together to set the hours.

Click **OK** to save your changes and exit the dialog box.

- 6 (Optional) To draw an attached line from this device to another device, select a device from the **Connected to item** drop-down list. (Attached lines move when you move the device icon.) For information about using attached lines, see “Attached Lines” on page 48.
- 7 To make this device an “up dependency” for another device (meaning it gets checked only if the other device is up), select the other device from the **Check only if up item** list.
- 8 To make this device a “down dependency” for another device (meaning it gets checked only if the other device is down), select the other device from the **Check only if down item** list.
- 9 Click **Apply** to apply your changes. Click **OK** to apply the changes and exit the dialog box.

Using the Right Mouse Menu



Select a device and then click the right mouse button to display the device pop-up menu. When you're in Edit Mode, the menu looks similar to the image to the left; in Monitor Mode, the menu has fewer commands. You can add menu commands that start applications. To do so, see "Adding a Command to the Right Mouse Menu" on page 34.

The default menu commands on the right mouse menu (in Edit Mode) are the following:

New lets you add devices to the map.

Edit lets you cut, copy, paste, and delete.

Item Properties shows you the device properties.

Check now does an immediate poll of the device and will show any change in status via a color change. It provides a way to do a quick check without checking all other devices in the map and without waiting for the map poll timer to count down to zero.

Connect calls *telnet.exe* or whatever program specified in the **Telnet program** box on the **Programs and SNMP** tab of **Program Options**.

Ping runs the Ping tool to send an ICMP echo request to the device.

Traceroute runs the Traceroute tool to show the network path used to reach a specified TCP/IP address.

Browse. If this device is running a web server on port 80, this command launches the default web browser and finds the web site.

SNMP starts the SNMP tool using the device's IP address. This command appears only if the **SNMP Manageable** option (on the SNMP tab) is turned on.

Attach to draws an attached line from the selected device to the next object you click. For information about using attached lines, see "Attached Lines" on page 48.

Disconnect disconnects any attached lines that originate from the selected device.

Move to Top. If the selected item is a drawn shape, such as a rectangle or circle, this command moves it in front of all other drawn shapes.

Move to Bottom. If the selected item is a drawn shape, such as a rectangle or circle, this command moves it behind all other drawn shapes.

Adding a Command to the Right Mouse Menu

You can add commands that start applications to the menu that appears when you right-click a device; you create these commands using the **Menu** tab of the device properties.

To add an item to the right mouse menu:

- 1 Double-click a device to display its properties and click the **Menu** tab.
- 2 In the **Menu Item** box, type the command name as you want it to appear on the right mouse menu.
- 3 In the **Command Line** box, enter the path and program name you want to start when you choose this command. You can enter the name of any executable program, or you can use one of the following values:
 - [telnet] - calls telnet.exe
 - [ping] - calls the Ping tool
 - [trace] - calls the Traceroute tool
 - [browse] – starts the default browser using the IP address as the URL
- 4 Following the program name, you can use variables to pass parameters to the specified program. See the following section for a list of program variables you can use.

Program Variables

In WhatsUp Gold, you can call an external program:

- From the right mouse menu when you right-click a device (See “Adding a Command to the Right Mouse Menu” above.)
- By double-clicking a custom device icon (See “Creating a Custom Device Type” on page 35.)

You can pass parameters to the specified program by using the variables in the following table. The specific variables you use and the order in which you use them depends on the program you are calling.

Variable	Returns
%1	Info Line 1 from the General tab of device properties
%2	Info Line 2 from the General tab of device properties
%a	IP Address from the General tab of device properties
%l (lower case L)	Display Name from the General tab of device properties
%n	Host Name from the General tab of device properties
%O	Valid only for custom device types with an SNMP identifier. Returns SNMP Object identifier (from the View -> Device Types dialog box) or "unknown" if SNMP Object is blank.
%R	SNMP Read Community from SNMP tab of device properties
%T	Device Type from the General tab of device properties.
%W	SNMP Write Community from SNMP tab of device properties

Custom Device Types

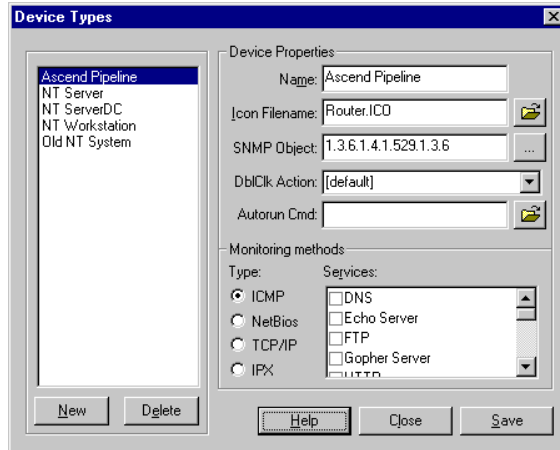
You can create custom device types to use in a map. You can supply your own icon for these custom devices, and set them up so that they are automatically mapped when you use the SmartScan or Scan tools.

Creating a Custom Device Type

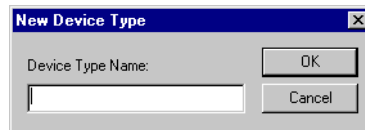
The Edit Toolbar provides tools that let you add a workstation, host, server, router, bridge, hub, LAN box, subnet, or custom devices to your network map.

To create a custom device type:

- 1 If you want the SmartScan or Scan tools to use a special icon when it finds this custom device, make sure you add vendor-provided identifiers to the MIB tree, see “Setting Up the MIB Identifiers” on page 148
- 2 Select **Device Types** from the **View** menu.



- 3 Click **New**.



- 4 Enter a name for the new device type and click **OK**.
- 5 In the **Icon Filename** box, enter the name of an icon (.ico) file that:
 - Has a depth of 16 colors
 - Is exactly 32 pixels tall and 32 pixels wide
 - Has a black border surrounded by white. The first four pixels in the top left corner must be unused to accommodate the way the icon flood fills. These pixels cannot be black.
 - Has transparent pixels within the black border that WhatsUp Gold can use to display status colors

Examples of suitable .ico files can be found in your WhatsUp Gold directory

- 6 (Optional) In the **SNMP Object** text box, enter an SNMP object identifier that corresponds to a vendor device type; this is usually found in the “private -> enterprises” section of the MIB tree, under the vendor name. Click the Browse button next to the text box to browse the MIB tree for the appropriate SNMP object.

SmartScan and Scan will map custom devices using the SNMP identifiers to locate the specified icons. To scan for custom devices, you must also enter the proper **Community** name and, if you use the Scan tool, turn on **Identify via SNMP** (as described in “Scanning and Mapping a Custom Device” on page 39).

You can use multiple identifiers. For example, suppose a manufacturer named Acme makes three devices: the Acme 4500, the Acme 4501, and the Acme 4502. You could define one custom device type to represent any Acme device in the 4500 series; in the **SNMP Object** box, you would enter the three SNMP identifiers for the Acme 4500, 4501, and 4502. A scan will use the icon for any of the three devices. Separate multiple SNMP object identifiers by semi-colons. The last number in the identifier can be an asterisk, a range using hyphens, or contain multiples separated by commas. For example:

1.3.6.1.4.1.311.1.1.3.1.3

1.3.6.1.4.1.311.1.1.3.1.3;1.3.6.1.4.1.311.1.1.3.1.4

1.3.6.1.4.1.311.1.1.3.1.3,4

1.3.6.1.4.1.311.1.1.3.1.1,3-4

1.3.6.1.4.1.311.1.1.3.1.*

Note

Custom device types are stored in the *hosttype.ini* file. WhatsUp Gold uses the device icon for the first object identifier it finds in *hosttype.ini*. Thus, if a device type “Cisco 3xxx” (1.3.6.1.4.1.9.1.32-37) appears before “Cisco 3204” (1.3.6.1.4.1.9.1.37), WhatsUp Gold uses the “Cisco 3xxx” icon for the “Cisco 3204” device.

- 7 In the **DbIClk Action** box, select the desired action. For more information, see “Changing the Double-Click Action for a Custom Device” below.
- 8 In the **Autorun Cmd** box, enter a script or program name. For more information, see “Running a script or program for custom devices” below.
- 9 Select the **Type** (polling method) of the device. For more information, see “The Polling Method” on page 28. If the **Type** is **TCP/IP**, select whatever **Services** you want to monitor by default when you create a device of this type.
- 10 Click **Save** to save the new device type.

Changing the Double-Click Action for a Custom Device

To change the action that occurs when you double-click a custom device’s icon:

- Select a preconfigured action from the list:
 - [default] - opens the device properties
 - [snmp] - starts the SNMP tool
 - [telnet] - calls telnet.exe
 - [ping] – starts the Ping tool
 - [trace] – starts the Traceroute tool
 - [browse] – starts the default browser using the IP address
- Alternatively, enter a program name in the **DbIClk Action** text box. For example, to start WS_FTP Pro, you would enter: *ftp95pro.exe*. Enter appropriate variables to pass parameters to the specified program. See “Program Variables” on page 34.

Running a script or program for custom devices

You can set a program to run automatically whenever a scan (SmartScan or Scan) maps a custom device.

- 1 Enter a script or program name in the **Autorun Cmd** text box.
- 2 You can enter the same values and variables described above for “changing the double-click action.”

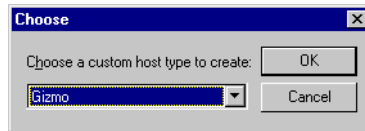
Using the Custom Device on a Map

To use the custom device type on a network map:

Custom device tool



- 1 Click the custom device tool in the Edit Toolbar.
- 2 Click the map location where you want to add the custom device type. You see the following dialog box.



- 3 Choose the custom device type from the drop down list.
- 4 Click **OK**. The custom device icon appears where you clicked.

Scanning and Mapping a Custom Device

If you want the a scan (SmartScan or Scan) to identify a custom device type, such as a Cisco 4000 router, and use a custom icon for the device, you can do the following:

- 1 Define a custom device type. Make sure you enter the appropriate identifier in the **SNMP Object** text box in the “Device Types” dialog box.
- 2 If you are using the Scan tool:
 - Select the **Identify via SNMP** and **Map results** option.
 - Start a scan of the appropriate IP addresses.
 - When prompted, enter the SNMP Read Community name assigned to your network. You can enter multiple communities, separated by a comma (.). The scan checks SNMP communities in the order that they are specified.
- 3 If you are using SmartScan, enter the network’s **Community** name and start the scan. You can enter multiple community names, separated by a comma (.). The scan checks SNMP communities in the order that they are specified.

If any of these conditions are *not* met, the scan will use one of the WhatsUp Gold standard device icons for the custom device.

Changing the Standard Device Icons

You can edit or replace the standard icons used to represent device types (workstation, host, router, etc.). If you replace a standard icon, you must use the same file name for the new file. For example, to replace the router.ico icon, you need to call the new file router.ico.

The standard icons are internal to the WhatsUp Gold program, but we have made the icon files available in the WhatsUp Gold directory. You can use these icon files as a starting point for creating your own icons. After creating or editing an icon, you need to select **Options -> Reload Icons** so that the new icon replaces the standard icon in the internal part of WhatsUp Gold.

You can use the following icon files as a starting point: bridge.ico, host.ico, hub.ico, lanbox.ico, printer.ico, router.ico, server.ico, workstn.ico

To change one of the standard icons:

- 1 Open one of the icon files (.ico) in an icon editor program. You cannot use a bitmap editor.
- 2 Make your changes to the icon (.ico) file. The icon file must have the following characteristics:
 - Has a depth of 16 colors
 - Is exactly 32 pixels tall and 32 pixels wide
 - Has a black border surrounded by white. The first four pixels in the top left corner must be unused to accommodate the way the icon flood fills. These pixels cannot be black. Everything outside of the black border will be transparent.
 - Has transparent pixels somewhere within the black border that WhatsUp Gold can use to display status colors

Examples of suitable .ico files can be found in your WhatsUp Gold directory.

- 3 Save your changes to a file with the same name as the icon you want to replace, and overwrite the icon file in your WhatsUp Gold top directory. For example, make changes to the workstn.ico file, then save your changes as workstn.ico in the WhatsUp Gold top directory.
- 4 Select **Program** from the Options menu. In the **Startup** tab, turn on the **Use external device icons** option.
- 5 Select **Reload Icons** from the Options menu.

WhatsUp Gold replaces the internal .ico files with the .ico files in the WhatsUp Gold top directory.

Creating a Subnet

The Subnet feature of WhatsUp Gold allows you to create separate maps for different segments of your network, yet maintain a connection between the maps. If you already have a parent network map, you can create a second network map for a particular network segment and then link it to the parent map; this makes the second map a “subnet” of the parent map.

Note

If you have a hierarchical network that uses SNMP, subnet maps can be created automatically by using SmartScan. For more information see, “Mapping a Hierarchical Network” on page 17.

WhatsUp Gold can simultaneously monitor the parent network map and any subnet maps. When a device or service goes down in a subnet map, the subnet icon on the parent map changes color to indicate that there’s a problem in the subnet. The subnet icon in the parent network map will have the color of the highest priority alarm that occurs in the subnet map. For example, if a device in the subnet does not respond to four polls, the subnet icon is red.

To create a subnet map (assuming you already have a parent map):

- 1 Create a new map and add the devices for the subnet. You can use any of the methods for creating a network map described in the previous section. You can also copy and paste devices from an existing map.

Edit Mode button



Add Subnet tool



- 2 Save the new map.
- 3 Open the parent map or, if it's already open, make it active.
- 4 Click the **Edit Mode** button to view the editing toolbars.
- 5 Click the **Add Subnet** tool and then click the parent map where you want to create the subnet icon.
- 6 Double-click the subnet icon to display its properties and click the **General** tab.
- 7 In the **Display Name** box, enter the file name of the subnet map, *not* the Map Title. This must be the name of the *.wup* file without the file extension. For example, if the subnet map file is named *SubnetA.wup*, you enter *SubnetA* here.
- 8 Click **Apply** to save your changes. On the **Monitor** tab, make sure **Monitor This Item** is selected.

When you open a network map, WhatsUp Gold can also open any associated subnet maps and start monitoring them. (From the **View** menu, select **Program Options** -> **Startup**, and then enable the **Auto Load Subnets** option.)

If a subnet map window is not opened, you can right-click the subnet icon and select **Load Subnet** from the menu to open it.

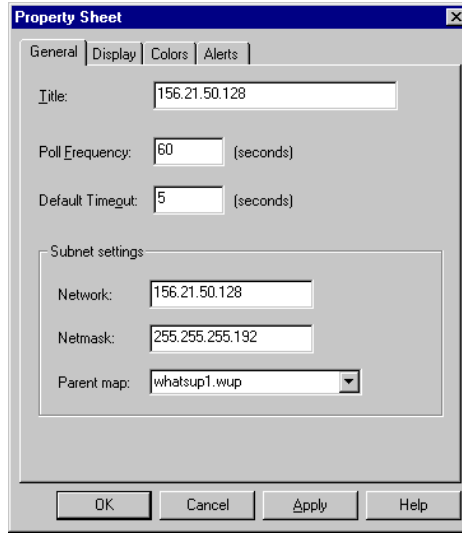
If a subnet map is opened but is hidden behind other windows, you can right-click the subnet icon and select **View Subnet** from the menu to bring the subnet map to the top.

From within a subnet map, you can open its parent map by right-clicking and selecting **View parent map**, or by selecting **Parent map** from the **Window** menu.

Setting Map Polling Properties

You can set the polling properties for each parent network map and subnet map.

Open the map window for the network map, then select **Map Properties** from the **File** menu. Or, right-click an *empty* area of the map to display the right mouse menu and then select **Map Properties**. Click the **General** tab.



Title. This title is used to identify a network map on the Map Window and when accessed from a web browser. You should be careful about changing the Title because it is also used to report information in the Event and Statistics logs. Polling statistics are saved in the [title.wui] file. The Status, Dependencies, Statistics, and Notifications Windows display information per map and use the Title.

Poll Frequency. This is the number of seconds between the start of a poll of the map. You can enter a value in the range 10 through 3600. The status line of each Map Window displays a timer that counts down from this number to zero before starting each poll. The timer continues to count down *during* polls: if the previous poll is not complete when the timer reaches zero, a new poll is not started.

Default timeout. This is the number of seconds to wait for a response from a polled device. This default value is assigned to new devices when they are added to the map.

Subnet Settings. The main purpose of these settings is to set a parent map for the current map. If you created the map using SmartScan, then each subnet map will already have an entry for the Parent map. To change the Parent map, select any of the maps shown in the drop-down list. This list shows all open maps.

To view a subnet's parent map, right-click on the map, and select **View parent map**, or select **Parent map** from the **Windows** menu.

This tab also shows the **Network** and **Netmask** settings for the network segment that this subnet map represents. These settings provide the default address settings for the Scan tool, if it is started when this map is active.

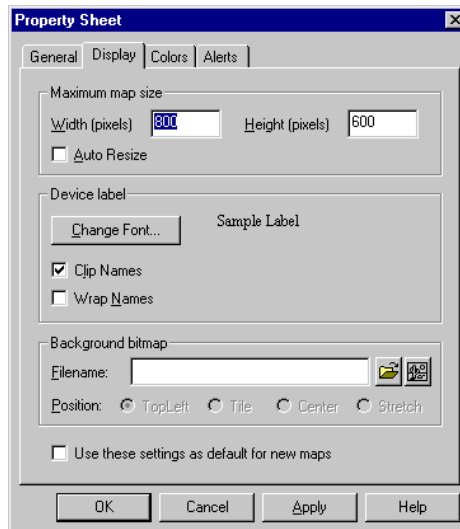
Network. Shows the starting IP address for this network segment.

Netmask. Shows the netmask for this network segment. The netmask defines how to read the IP address to identify subnets and devices.

Setting the Map Display

You can set the polling properties for each parent network map and subnet map.

Open the map window for the network map, then select **Map Properties** from the **File** menu. Or, right-click an *empty* area of the map to display the right mouse menu and then select **Map Properties**. Click the **Display** tab.



Maximum map size. Specifies the maximum map **Width** and **Height** in pixels. The default setting is 800 by 600.

In Edit Mode, these settings appear as a dotted line in the Map Window. When **Auto Resize** is turned on, the map shrinks to fit the display window, if necessary. If the display window is large enough to

accommodate the map, the map is not resized. (This option applies to the map window in Monitor Mode only, it does not affect Edit Mode.)

Device label. Specifies the font used for the device's display name. Click the **Change Font** button to open the standard Windows font selection dialog box. Select the font properties you want to use and click **OK**. The "Sample Label" shows the new font selection.

When **Clip Names** is turned on, the display names for devices are terminated at the first space or period in the name, thus shortening the display name. When **Wrap Names** is turned on, long display names are wrapped at every space or period in the name.

Background Bitmap and Position. Allows you to specify a bitmap (*.bmp*) image file to be used as a background for the WhatsUp Gold map. This could be a floor plan, a geographical map (city, state, or country), or any bitmap image that you want. Click the browse button to look for a file; click the paint tool button to open Microsoft Paint.

You can position the bitmap to completely fill the map background (**Stretch**), or place it within the map using the **TopLeft**, **Center**, or **Tile** settings. Note that the color depth of the bitmap must be equal to, or less than, the color depth of the screen.

Use these settings as default for new map. If this option is turned on, WhatsUp Gold applies the settings for these map properties to all new maps that you create.

Setting Map Colors

For each network map, you can change the default colors for alerts and for the various parts of the map window. To change map colors:

- 1 Select **Map Properties** from the **File** menu, and click the **Colors** tab.
- 2 Select an item in the list box and click the desired color.

Responding. This is the color that indicates that a device is responding to polls. The default is solid bright green.

Note that if you change the "Responding" color, you won't see the change until you are in Monitor Mode and WhatsUp Gold completes the next poll.

Lost 1 pkt. The color that indicates that a device has not responded to one poll. The default is solid light green.

Lost 2 pkts. The color that indicates that a device has not responded on two consecutive polls. The default is solid yellow.

Lost 3 pkts. The color that indicates that a device has not responded on three consecutive polls. The default is solid yellow.

Lost 4-7 pkts. The color that indicates that a device has not responded on four to seven polls. The default is solid light red.

Lost 8+ pkts. The color that indicates that a device has not responded on eight or more polls or has a network error. The default is solid dark red.

Service down. The color that indicates that a service is down on a device. The default is solid purple.

Inactive. The color that indicates a device that is not being monitored. The default is solid dark grey.

Background. The color of the map window background. The default is solid light grey.

Text. The color for drawn text. The default is solid black.

Attach lines. The color for attached lines. The default is solid yellow.

Note

The default color for freehand (unattached) lines is black; you can change this using the color toolbar.

Editing a Network Map

You use Edit Mode to move device icons around in the map window. When you're in Edit Mode, you can use tools to:

- Add and delete device icons
- Cut, copy, and paste device icons and drawn objects
- Draw, color, and size graphic shapes to visually organize network elements

Getting In and Out of Edit Mode

Edit Mode button

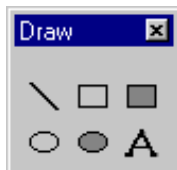


To access Edit Mode, make sure the map that you want to edit is active, then click the Edit Mode button in the main toolbar. The editing toolbars appear.

Note

WhatsUp Gold stops polling the network when you're in Edit Mode.

Draw Toolbar



Use the Draw Toolbar to add free (unattached) lines, rectangles, filled rectangles, ellipses, filled ellipses, and text blocks to your map.

Edit Toolbar

Use the Edit Toolbar to create device icons and to select, move, cut, copy, and paste device icons and drawing objects.

The select tool is the default active tool. When the select tool is active, you can drag any map object to a new location.



When the display tool is active, you can click a device icon to view and modify its properties.

Add workstation

Add server

Add bridge

Add LAN box

Add printer

Add host

Add router

Add hub

Add subnet

Add custom device. For more information, see "Creating a Custom Device Type" on page 35.

Edit Mode button



To exit Edit Mode and return to Monitor Mode, click the **Edit Mode** button again. The toolbars disappear.

Keeping Tools Active

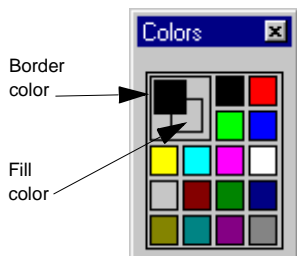
When you're in Edit Mode, you click a tool to use it. By default, the tool stays active for one operation. If you want the tool to remain active until you decide to change it, select **Keep Buttons Down** from the **Options** menu.

Drawing

To draw a shape, such as a rectangle, ellipse, filled rectangle, or filled ellipse, click the appropriate tool, and then drag to create the shape.

The shape uses the active border color, as shown in the illustration to the left. Filled objects use the active fill color.

To change the border color, click the left mouse button on any color. To change the fill color, click the right mouse button on any color.

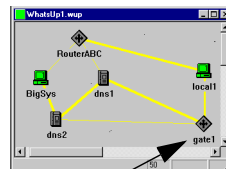
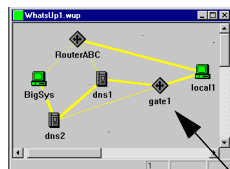


Changing Item Properties

To change the line width or color of a drawn object, select the object, and then select **Item Properties** from the pop-up menu.

Attached Lines

In addition to the freehand lines that behave like any other drawn object, you can also use *attached* lines.



When you move an icon that has attached lines, the attached ends of the lines move with it.

You can attach a device to up to five other devices or drawn objects. The primary connection (the last connection made) is represented by a line that is two pixels wide. Any secondary connections (all other connections) are shown as lines that are one pixel wide.

To attach one device to another:

- 1 Right-click the device icon you want to draw an attached line *from*; this displays the right mouse menu.

- 2 Select **Attach to**. The cursor changes to a line character.
- 3 Click the item *to which* you want to attach the device.

Or, to set only the primary connection:

- 1 Double click a device icon to display its properties.
- 2 Click the **Monitor** tab.
- 3 In the **Connected to item** drop-down list, select the primary device to attach to.

To disconnect any attached lines that originate from the selected device:

- 1 Right-click the device.
- 2 Select **Disconnect** from the right mouse menu.

Or, to disconnect only the primary connection:

- 1 Double click a device to display its properties.
- 2 Select the **Monitor** tab.
- 3 In the **Connected to item** drop-down list, select **None**.

Creating Text Captions

You can use text captions to further identify a network map or segments of a map. Text is available in many fonts, sizes, text effects, and colors.

In addition, you can specify an opaque background for the text block, which is also available with a choice of colors. Text blocks can be rotated a full 360 degrees (if you select a TrueType font) to address special text labeling requirements.

To add text to the network map:

- 1 Select the border color in the Color Toolbar.
- 2 In the Draw Toolbar, click the Text tool.
- 3 Place the cursor where you want to locate the text and click. The Sample Text and its properties dialog box appear.
- 4 In the **Text** box, replace *Sample Text* with the desired text.
- 5 Set the color, font, or rotation options as appropriate.

Foreground. Click **Change Color** to select another color.

Text tool



Opaque. Select this to set the text against a background color.

Background. If **Opaque** is selected, the background color is used. You can click **Change Color** to select another color.

Change Font. Click **Change Font** to change the font of the text.

Rotation. Enter a number from 0 to 360 to represent the degrees to rotate the text. You must be using one of the TrueType fonts in order to rotate text.

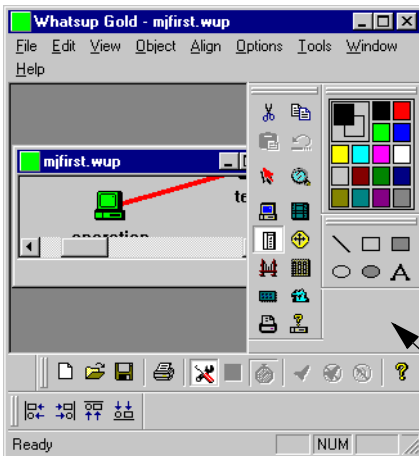
Note

Even after you rotate text, the text retains its original anchor points. To select rotated text, click an original anchor point.

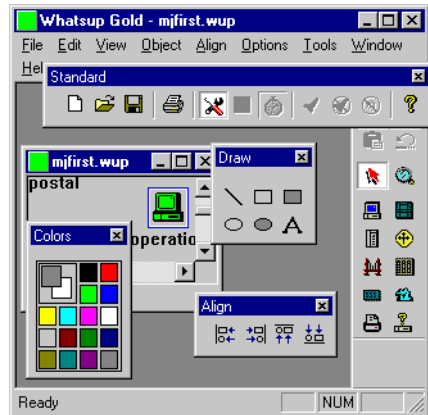
6 Click **OK**.

Arranging the Toolbars

In Edit Mode, you can arrange the five WhatsUp Gold toolbars any number of ways, on or off a gray toolbar backdrop.



Toolbar backdrop



To make a toolbar float in its own window, drag the double gray lines at the top of the toolbar to an area *off* the toolbar backdrop. To move a free-floating toolbar onto the toolbar backdrop, drag its title bar to the toolbar backdrop; to use the toolbar backdrop if it's not visible, double-click a toolbar's title bar.

You can also reshape the Standard Toolbar by grabbing a side and drag to the desired shape.

Saving and Naming a Network Map

If you save a new map by selecting **Save** from the **File** menu, the map file is saved with a default name. The first default file name assigned by WhatsUp Gold is *WhatsUp.wup*, and subsequent maps saved this way are named *WhatsUp1.wup*, *WhatsUp2.wup* ... *WhatsUpn.wup*.

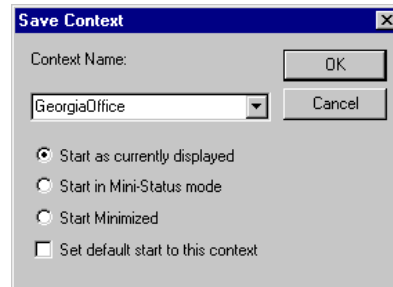
To save a map with your own name, use the **Save As** command.

Saving a Context

You can use the Save Context function to save the window setup and locations that you have selected for monitoring a network. For example, if you regularly use a view where you have a Map Window, Tree Window, and Status Window open, you can save this view as a “context” so that you can later open the context without having to restart the Tree and Status Windows. You can use the Save Context function to save several different views of the network.

To save a context:

- 1 From the **File** menu, select **Save Context**. The following dialog box appears.



- 2 In the **Context Name** box, enter a unique name for the context.
- 3 Select one of the following start options:

Start as currently displayed. When you open the context, it will be displayed as shown in the current display, with current window locations.

Start in Mini Status mode. When you open the context, it will be displayed in Mini Status mode. Mini Status mode provides a simple listing of the network elements (in place of the main window) and is designed to save screen space. For more information, see “Using the Mini Status View” on page 100.

Start Minimized. When you open the context, it will be displayed as an icon (minimized).

- 4 Optionally, check the **Set default start to this context** option if you want this context to open whenever you start WhatsUp Gold.
- 5 Click **OK** to save your changes.

To open a context:

- 1 From the File menu, select **Open Context**. The “Open Context” dialog box appears.
- 2 Select a context name from the drop-down list.
- 3 Click **OK** to open the context.

Chapter 3: Setting Up Notifications

When an event occurs on your network, WhatsUp Gold performs several different actions. WhatsUp Gold:

- Records the event in the Event Log (described in “Logging and Reporting Events” on page 104)
- Updates the device properties Status and Log tabs
- Changes the appearance of the device icon on a map (as described in “Reading the Network Map” on page 93)
- Optionally, sends a notification (as described in this chapter)

WhatsUp Gold can send a notification in several ways; it can:

- Sound an alarm
- Activate a beeper
- Send a message to a pager
- Send an e-mail message
- Send a pre-recorded message to a telephone (only in Windows 95, 98, and only if you have a voice modem installed)
- Display a WinPopup on a Windows NT system
- Send a group of notifications that includes any of the above types

You can also set up a “recurring report” to use a beeper, pager, or e-mail message to send a network status report at a specified time interval. See “Sending Recurring Status Reports” on page 125.

Setting up notifications involves two steps:

- 1 You first need to *define* the notifications that you want to use, such as activating a network administrator’s beeper or sending e-mail to an individual. This section describes how to do this.
- 2 Then, you *assign* a notification to a particular device, selected devices, or all devices.

For information on assigning notifications to a device, see “Assigning Notifications to Devices” on page 69. For information on assigning notifications for selected devices or for all devices, see “Assigning Notifications Globally” on page 75.

Defining Notifications

You define the different types of notifications using the Notifications Editor. You can access the Notifications Editor in one of two ways:

- From the **View** menu, select **Notifications**.
- Open the device properties, click the **Alerts** tab, and select **Enable Alerts** and **Enable Notifications**. Then click the **Notifications Editor** button.

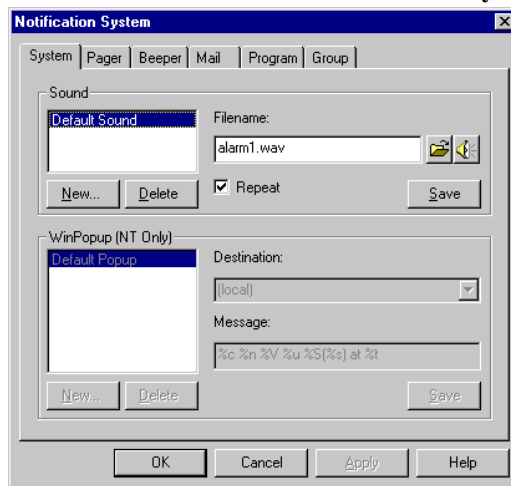
Note

Any notifications you define are stored in a file named *ipnotify.ini* in your Windows or NT directory. This file is shared by other Ipswitch products and is therefore not deleted or replaced when you uninstall or upgrade WhatsUp Gold. Furthermore, if you ever move WhatsUp Gold to a new system, you will need to manually copy the *ipnotify.ini* file to the Windows or NT directory of the new system.

Defining System Notifications

System notifications are of two types: sound notifications and WinPopups. A sound notification sounds an alarm when a device goes down or comes back up. WinPopup notifications display a message in the WinPopup window on particular Windows NT systems.

Select **View** -> **Notifications** and click the **System** tab.



Sound Notifications


Note

To play the alarm sounds, you must have a sound card and speakers installed on your system. Also, do not enable sounds if you plan to run WhatsUp Gold as an NT service.

To define a sound notification:

- 1 Click **New**, enter a unique name, and click **OK**. The new notification name appears in the list box.
- 2 In the **Filename** text box, enter the name of the *.wav* file to be played when this notification is triggered. (Click the **Browse** button to the right of the file name to select a *.wav* file.)
- 3 Optionally, select **Repeat** to play the sound continuously until the **Quiet** button is clicked.
- 4 Click **Save** to save the new notification.

Browse 

Invoke Sound Recorder 

WinPopups

A WinPopup notification displays a message in the WinPopup window on either:

- A single Windows NT system. (You can define one WinPopup notification for each system on which you want to display the message.)
- All Windows NT systems in a local domain.

To define a WinPopup notification (on Windows NT systems only):

- 1 Click **New**, enter a name for the notification, and click **OK**.
- 2 In the **Destination** text box, select a host name or domain name from the drop-down list. Note that, in the drop-down list, domain names are marked with an asterisk (*).
- 3 In the **Message** text box, enter a text message plus any of the variables described in “Notification Message Variables” on page 63. (You can use these to add status information.)
- 4 Click **Save** to save the new notification.

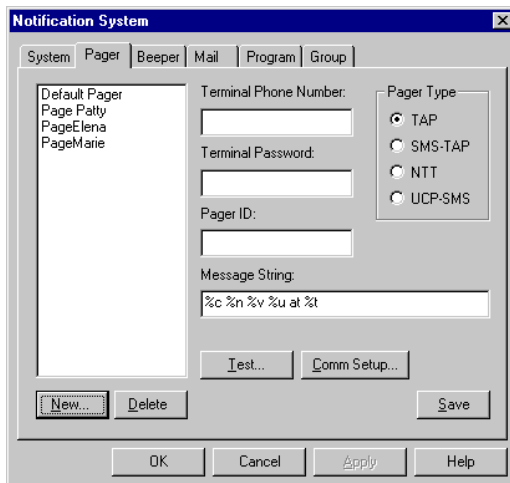
Defining Pager Notifications

You can define a pager notification to send an alphanumeric message to a pager when a device does not respond.

WhatsUp Gold supports PageNet and other TAP (Telocator Alphanumeric input Protocol) pager services, as well as SMS-TAP, NTT, and UCP-SMS pager services.

To define a pager notification:

- 1 In the “Notification System” dialog box, click the **Pager** tab.



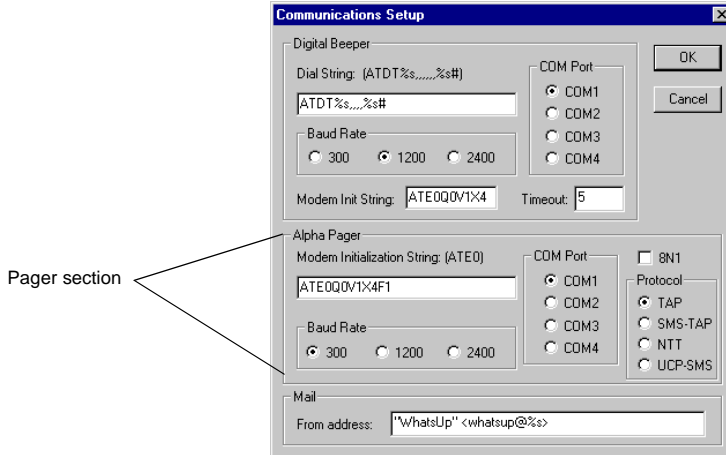
- 2 Click **New** and enter a unique name to identify the pager notification, for example, *Page Bob*. Click **OK**. The new notification name appears in the list box.
- 3 In the **Pager Type** section, select the type of pager service that you are using.

Note

Get the **Pager Type**, **Terminal Phone Number** and **Password**, and **Pager ID** from your service provider.

- 4 In the **Terminal Phone Number** box, enter the phone number to dial. If required, enter the pager password in the **Terminal Password** box. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers, for example: (617) 555-5555.

- 5 In the **Pager ID** box, enter the pager identification number.
- 6 In the **Message String** box, enter a text message plus any of the variables described in “Notification Message Variables” on page 63. Use these to add status information to the notification.
- 7 Click **Comm Setup** to view the following dialog box.



- 8 In the **Alpha Pager** section of the dialog box, enter:

Modem Initialization String (ATE0). The default string is ATE0. This string should contain the modem commands for “Command Echo Off.”

Baud Rate. Select the speed (measured in bits per second) at which the serial port will communicate with the modem.

COM Port. Select the port to which your modem is attached.

8N1. The TAP protocol requires the 7E1 setting for communications, but if your pager uses 8N1, you can select this option.

Protocol. Select the protocol used by your pager service.

When you have entered the information, click **OK** to save your changes and exit the “Communications Setup” dialog box.

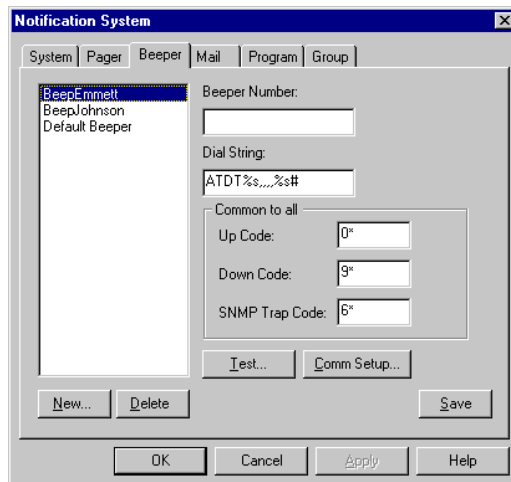
- 9 On the **Pager** tab, click **Save** to save the new notification.

Defining Beeper Notifications

A beeper notification activates a beeper when a device does not respond to polling.

To create a beeper notification:

- 1 Select **View -> Notifications** and click the **Beeper** tab.



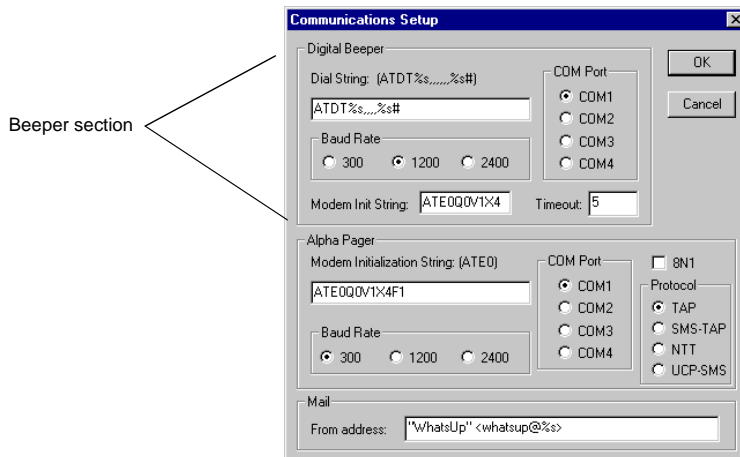
- 2 Click **New** and enter a unique name to identify the beeper notification, for example, *Beep Bob*. Click **OK**. The new notification name appears in the list box.
- 3 In the **Beeper Number** box, enter the phone number to dial. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers, for example: (617) 555-5555.
- 4 In the **Dial String** box, the default is `ATDT%s,,, %s#`. WhatsUp Gold replaces the first `%s` with the phone number and the second `%s` with the Up, Down, or SNMP Trap code. Most modems and beepers support the use of '#' to terminate the message and '*' to print out a dash.

A comma (,) provides a one second pause. Commas are used to give the beeper service time to pick up. If the code is dialed too soon, you can increase the number of commas in the dial string; you can decrease the number of commas if the modem waits too long.

- 5 In the **Common to all** section, the **Up Code** specifies the characters sent to the beeper to indicate that the device has come back up after being down (the default value is 0*). The **Down Code** specifies the code sent to indicate the device is down (the default value is 9*). The **SNMP Trap Code** specifies the code sent to indicate that an SNMP trap has been received for the device. You can use the asterisk (*) character to separate the code from a subsequent message.

When sent to the beeper, the **Up** or **Down Code** is followed by the **Item digital code** that indicates which device the notification is for. (The **Item digital code** is specified in the “Add/Edit Notifications” dialog box when you assign a beeper notification to a particular device. For more information, see “Assigning Notifications to Devices” on page 69.)

- 6 Click **Comm Setup** to view the following dialog box.



- 7 Enter the following information in the **Digital Beeper** section of the dialog box:

Dial String. This is the default dial string for beeper notifications.

Baud Rate. Select the speed (bits per second) at which the serial port will communicate with the modem.

COM Port. Select the port to which your modem is attached.

Modem Init String. The default string is ATE0Q0V1X4. This string should include the modem commands for “Command Echo Off” (E0), “Result Codes On” (Q0), “Verbal Results” (V1), and “Extended Status” (X4).

Timeout. The timeout value determines how long the system waits, after sending the last character, before it hangs up the phone (if a transition is not recognized).

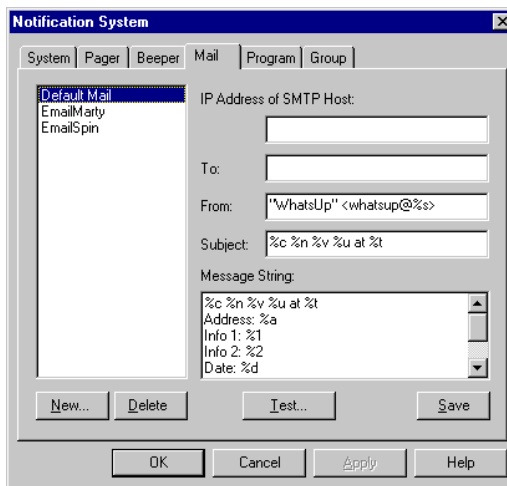
When you have entered the information, click **OK** to save your changes and exit the “Communications Setup” dialog box.

- 8 On the **Beeper** tab, click **Save** to save the new notification.

Defining E-mail Notifications

An e-mail notification sends a message to an e-mail address when a device does not respond.

- 1 Select **View -> Notifications** and click the **Mail** tab.



- 2 Click **New** and enter a unique name to identify the e-mail notification, for example, Mail to Netadmin. Click **OK**.
- 3 In the **IP Address of SMTP Host** box, enter the IP address of your e-mail server (SMTP mail host).
- 4 In the **To** box, enter one or more e-mail addresses that are accepted by the SMTP server. Separate each address with a comma. The addresses should not contain brackets, braces, quotes, or parentheses.

- 5 The **From** address defines the sender of an e-mail notification as: <what.sup@%s>, where %s is converted by WhatsUp Gold to the local host name. You may need to change this address to be a valid user on your e-mail (SMTP) server. If you *do* change the address, be sure to keep the angle brackets (<>) in place.
- 6 In the **Subject** box, enter a text message and/or any of the notification variables described in “Notification Message Variables” on page 63. You can use these variables to add status information to the notification.
- 7 In the **Message String** box, enter text messages plus any of the notification variables described in “Notification Message Variables” on page 63. You can use these variables to add status information to the notification.
- 8 Click **Save** to save the new notification.

Defining Group Notifications

A group notification includes multiple pager, beeper, e-mail, or voice notifications. Each group notification can be set up to “Notify All” (send all its member notifications at once) or “Notify First” (send one member notification at a time until one is successfully sent).

Example A. One group notification might be named *SeriousProblem* and it might include the following four pager notifications:

- PageTodd 24 hours a day on Monday, Wednesday, or Friday
- PageElena 24 hours a day on Tuesday or Thursday
- PageKenny 24 hours a day on Saturday or Sunday
- PageManager 24hours a day, 7 days a week

Example B. A group notification could try a series of beeper and e-mail notifications until one is successfully sent. For example, suppose you have a group notification named *Operations*; its members are:

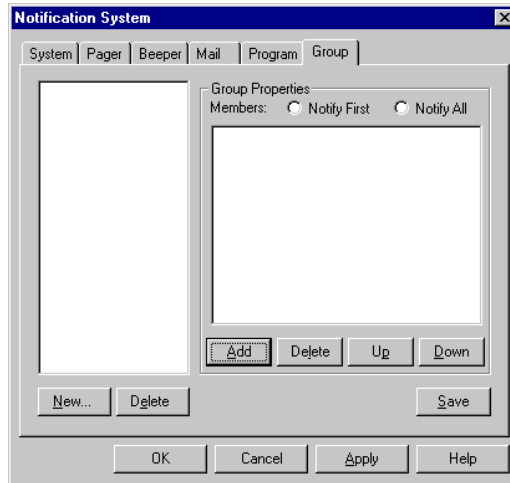
- *BeepJed*
- *EmailJed*
- *BeepHeidi*
- *EmailHeidi*
- *BeepFaith*
- *EmailFaith*

In this case, WhatsUp Gold would try to beep Jed first, but if this beeper message is *not* sent successfully, it then tries to e-mail Jed.

If the e-mail to Jed is also not successfully sent, WhatsUp Gold next tries to beep Heidi. Now, lets suppose the beeper message to Heidi *is* sent successfully; in this case, WhatsUp Gold will not attempt to send any more notifications in the *Operations* group.

To define a group notification:

- 1 Select **View** -> **Notifications** and click the **Group** tab.



- 2 Click the **New** button, enter a name for the group, and click **OK**.
- 3 Add each member notification to the group by clicking the **Add** button to view the “Add/Edit Notification” dialog box shown on page 72. The appearance of this dialog box varies slightly depending on the notification that is selected in the drop-down list at the top of the dialog box.

As described in the steps on page 72, select a member notification from the drop-down list, set the options for the selected notification including **Trigger** and **Time Period**, and then click **OK**. Repeat for each notification in the group.
- 4 (Optional) To send the member notifications one at a time until one of them is sent successfully, select **Notify First**, and then use the **Up** and **Down** buttons to sequence the list of members.
- 5 Click the **Save** button.

Notification Message Variables

In notification messages, you can use the following variables to encode information about a device.

Variable case sensitive	Returns	Notifications in which it's valid			
		Mail	(System) WinPopup	Pager	Beeper
%1	Info line 1 (from General tab)	✓	✓	✓	
%2	Info line 2 (from General tab)	✓	✓	✓	
%a	IP Address (from General tab)	✓	✓	✓	
%c	Same as %T, returns the device type. Use %T; %c was used in previous versions.	✓	✓	✓	
%C	Item digital code in "Add/Edit" dialog box.				✓
%d	Current date (mm/dd/yyyy)	✓	✓	✓	
%h	Host Name (from General tab)	✓	✓	✓	
%L	The Event Log file, <i>whatsupg.log</i> (or %Lnn where nn = last nn lines of the log file)	✓			
%n	Display Name (from General tab)	✓	✓	✓	
%N	Notes and SNMP trap text. (Notes are from the device properties Notes tab. If the event is an SNMP trap, the full SNMP trap text is appended to the notes.)	✓	✓		
%O	SNMP Object identifier. (Valid only for a custom device type) This is the word "unknown" if SNMP Object box is blank.)	✓	✓		
%R	SNMP Read Community (from the SNMP tab)	✓	✓		
%s	Winsock error code	✓	✓	✓	
%S	WhatsUp Gold status (such as "timed out" or "did not respond")	✓	✓	✓	
%t	Current time (hh:mm:ss)	✓	✓	✓	
%T	Custom device Type (from General tab) See the Note below.	✓	✓		
%u	The word "UP" or "DOWN"	✓	✓	✓	
%v	Names of down services	✓	✓	✓	
%V	Names of down services, followed by the word "services"	✓	✓		
%W	SNMP Write Community (from the SNMP tab)	✓	✓		

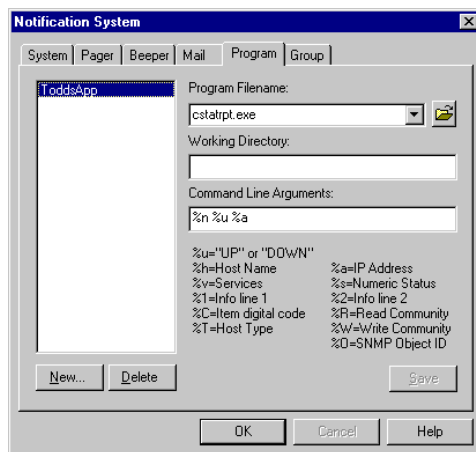
Testing Beeper, Pager, and E-mail Notifications

To test a beeper, pager, or e-mail notification, select it in the Notification Editor and click the **Test** button. WhatsUp Gold runs a test and responds with a Succeeded or Failed message. You can open the Debug Log (**View -> Logs -> Debug Log**) to see the conversation.

Defining Program Notifications

A program notification starts an application when a device goes down or comes back up.

- 1 Select **View -> Notifications** and click the **Program** tab.



- 2 Click **New**, enter a name to identify the program notification, and click **OK**. The new notification name appears in the list box.
- 3 In the **Program Filename** box, enter the executable name of the application you want to start or browse for a file.
- 4 (Optional) In the **Working Directory** box, specify a directory where the working files for the application are stored.
- 5 In **Command Line Arguments**, enter any of the variables described in “Notification Message Variables” on page 63. The defaults are the display name (%n), up or down status (%u), and IP address (%a).
- 6 Click **Save** to save the new notification.

Setting Up a Voice Modem

To use voice notifications, you must install a supported voice modem and the Unimodem/V drivers on the system on which WhatsUp Gold is installed. WhatsUp Gold has been tested with the *US Robotics Sportster Voice 33.6 Faxmodem with Personal Voice Mail* and with the *Diamond 3500* voice modem.

Note

At the time this manual was published, the Unimodem/V drivers were supported on Windows 95 and 98 only. Therefore, you cannot use voice notifications on Windows NT.

To install the driver and voice modem:

- 1 Download the Unimodem/V driver, *unimodv.exe*, from Microsoft. Copy it to an empty directory and run it to extract several files. See the *readme.txt* for installation instructions.
- 2 If your voice modem is not directly supported by Unimodem/V, go to your modem manufacturer's web site and locate the Unimodem/V support files and *.wav* driver. Copy the proper *.inf* files into your `\windows\inf` directory, open the Windows Explorer to the directory, select the files, and select **Install** from the right mouse menu (or read the vendor's instructions).
- 3 If the WhatsUp Gold *.wav* files are compatible with your modem, you can use them. If they're not compatible, or you want to change the message, you can record new files. The suggested default setting for recording is: PCM 8,000 Hz, 16 bit, Mono.

Wave files needed for voice notifications are:

Default <i>.wav</i> file	Message
isdown.wav	"... is down."
isup.wav	"... is now reachable."
svcdown.wav	"a service is down on ..."
svcup.wav	"the service is now up on ..."
ahost.wav	"a host ..."
pressone.wav	"WhatsUp has a message for you. Press 1 for the message."

- 4 Set the *.wav* files on the **Voice** tab to point to the *.wav* files that you create.

For more information, see the following section, “Defining Voice Notifications.”

- 5 Make sure your serial port has a COM driver.

You can check this in the Control Panel by selecting **System** -> **Device Manager** -> **Ports** -> (modem’s COM port).

If you do not have all of the above installed (voice modem, Unimodem/V drivers, and a COM driver), you will not see the **Voice** tab in the “Notifications Editor” dialog box.

Defining Voice Notifications

After setting up the voice modem (see previous section), you can define voice notifications to send a voice message to a telephone or answering machine when a device goes down or comes back up.

You can use the default *.wav* files included with WhatsUp Gold to send a message, or you can record your own *.wav* files.

When a voice notification is triggered, WhatsUp calls the specified telephone number and plays the initial message.

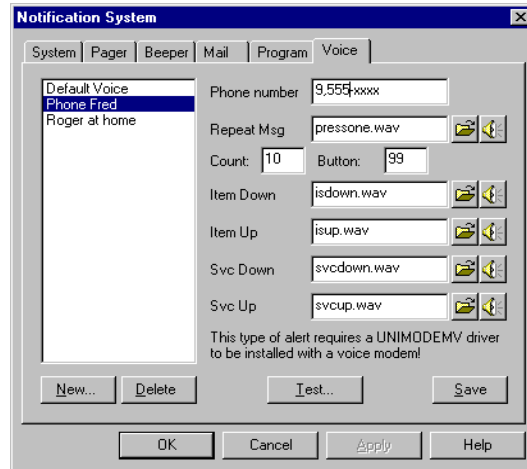
The default initial message (*pressone.wav*) is “WhatsUp has a message for you. Press one for the message.” When you press 1 on the phone, one of the up or down messages will play, such as “A host is down.”

If you want to include the device name in the message (for example, “Gyro is down”), you can record a *.wav* file of a particular device name and enter the *.wav* file name in the “Add Notifications” dialog box when you add the voice notification to that device.

For more information, see “Assigning Notifications to Devices” on page 69.

To create a voice notification:

- 1 Select **View -> Notifications** and click the **Voice** tab.



If you do not have a voice modem, Unimodem/V drivers, and a COM driver installed, you will not see the **Voice** tab in the “Notifications Editor” dialog box.

- 2 Click **New** and enter a unique name to identify the voice notification, for example, “Phone Fred.” The new notification name appears in the list box.
- 3 In the **Phone number** box, enter the phone number to dial. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers, for example: (617) 555-5555.
- 4 In the **Repeat Msg** box, enter or select the sound (.wav) file that will be played as the initial voice message to tell the recipient that they have received a message from WhatsUp Gold. The default message (*pressone.wav*) is “WhatsUp has a message for you. Press 1 for the message.” When the recipient presses 1 on the phone, one of the status messages will be played.

Browse 

Invoke Sound Recorder 

Click **Browse** to select a .wav file. Click the **Invoke Sound Recorder** button to open the .wav file in the Sound Recorder. You can play the sound file or edit it to create a different sound. For more information on Sound Recorder, see the Sound Recorder **Help**.

- 5 In the **Count** text box, enter the number of times to play the initial message (specified in the **Repeat Msg** box) before timing out (if the message is not acknowledged).
- 6 In the **Button** text box, enter the number on the telephone that the recipient presses to get the status message.

The default message (specified in the **Repeat Msg** box) tells the recipient to press 1 to receive the status message. You can set this number to 99 to make it accept any number pressed on the telephone.

Note

If voice mail or an answering machine answers the phone, the voice notification will not get beyond the initial *.wav* file specified in the **Repeat Msg** box.

- 7 Optionally, enter or select the sound (*.wav*) file that will be played for any of the status messages. The default status messages are:

Property	Default <i>.wav</i> file	Message
Item Down	<i>isdown.wav</i>	"... is down."
Item Up	<i>isup.wav</i>	"... is now reachable."
Svc Down	<i>svcdown.wav</i>	"a service is down on ..."
Svc Up	<i>svcup.wav</i>	"the service is now up on ..."
Wave file (in Alerts)	<i>ahost.wav</i>	"a host ..."

Browse 

Invoke Sound Recorder 

Click the **Browse** button to select a *.wav* file. Click the **Invoke Sound Recorder** button to open the *.wav* file in the Sound Recorder. You can play the sound file or edit it to create a different sound. For information on recording and editing sound files, select an item from the Sound Recorder's **Help** menu.

- 8 Click **Save** to save the new notification.

Assigning Notifications to Devices

WhatsUp can notify you when:

- A device is down
- A service on a device is down
- An SNMP trap has been received for a device

In order to receive a notification for one of these events, you need to *define* the notifications you want to use. Then, once you have defined the notifications, you *assign* them to the appropriate device(s). These can be individual devices, selected devices, or all devices in a particular network map.

This section describes how to assign notifications to *individual* devices. For information about assigning notifications globally (to *selected* devices or to *all* devices in a map), see “Assigning Notifications Globally” on page 75.

Note

Global notifications (assigned to selected or all devices using Map Properties) override notifications assigned to individual devices. Therefore, assign notifications globally *before* you assign them to individual devices.

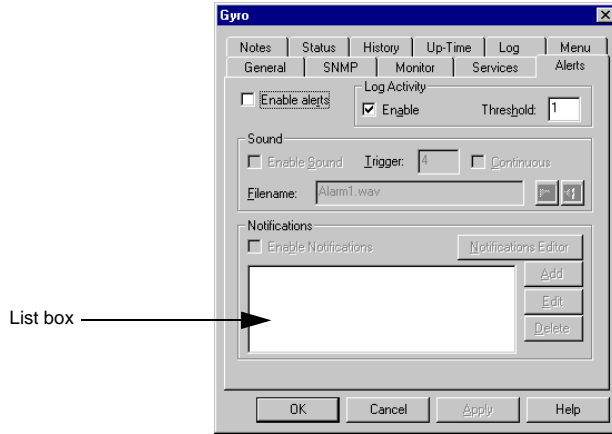
Using the Alerts Tab

You use the **Alerts** tab to:

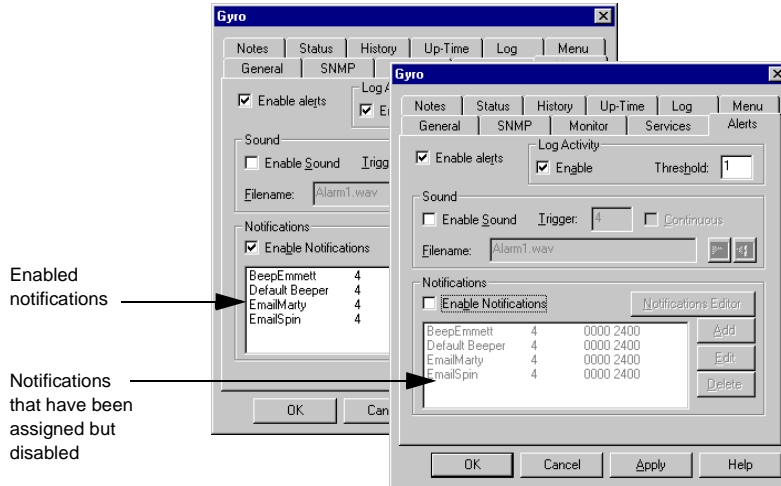
- Enable logging
- Enable an alarm sound
- Assign notifications and/or enable notifications

To use the **Alerts** tab:

- 1 Double-click the device to view the device properties, and then click the **Alerts** tab. If alerts are not enabled and no notifications are assigned, the **Alerts** tab is similar to the following:



If notifications have been assigned to the device, they appear in the list box. If the notifications are enabled, they appear in a black font, but if they were assigned and subsequently disabled, they appear in gray. Each device can have up to 10 notifications.



- 2 Make sure **Enable Alerts** is selected.
- 3 If you want to log “UP” and “DOWN” events for this device, under **Log Activity**, make sure **Enable** is turned on. (These entries can be viewed on the **Log** tab of the device properties.)

- To change the number of consecutive missed polls that generate a “DOWN” or “UP” event, change the value in the **Threshold** box.

The **Threshold** default value is 1, which means that every missed poll is logged; this setting gives you the most complete information about your network: when any device (or a monitored service on a device) misses one poll, it is logged as “DOWN” or “SVCDOWN.”

If you have a device on your network that routinely misses just one poll, you may feel that you are getting too many “DOWN” or “UP” messages in the Event Log. In this type of situation, you can set the **Threshold** to a higher number such as 2, 3, or 4.

However, if you have assigned notifications to this device and want to make sure, for clarity’s sake, that a “DOWN” or “UP” event for this device is recorded in the Event Log *before* any alerts or notifications are recorded, make sure the **Threshold** value is *less than or equal to* the **Trigger** value of any notifications assigned to this device.

- In the **Sound** section of the **Alerts** tab, select **Enable Sound** to sound an alarm (a specified .wav file) when the device fails.

Note

To play the alarm sounds, you must have a sound card and speakers installed on your system. Also, do not enable sounds if you plan to run WhatsUp Gold as an NT service.

Trigger. Enter the number of missed polls after which the alarm will be sounded. The default value is 4. See the information above about the relationship of the **Trigger** and **Threshold** values.

Continuous. Select this to sound the alarm until it is manually turned off (by clicking the **Quiet** button in the main toolbar).

Filename. Enter or select the sound (.wav) file that will be played when the device goes down. WhatsUp Gold provides three .wav files: *alarm1.wav*, *alarm2.wav*, *alarm3.wav*.

Click the **Browse** button to browse the directories and select a .wav file. Click the **Invoke Sound Recorder** button to open the .wav file in the Sound Recorder. You can play the sound file or

Quiet



Browse



Invoke Sound Recorder



edit it to create a different sound. For information on using Sound Recorder, see the Sound Recorder **Help**.

- 6 (Optional) In the **Notifications** section of the **Alerts** tab, select **Enable Notifications** to activate this section of the **Alerts** tab.

To delete a notification, select the notification in the list box and click **Delete**.

To edit a notification, see “Editing Notifications” on page 75.

To assign a notification to this device, see below.

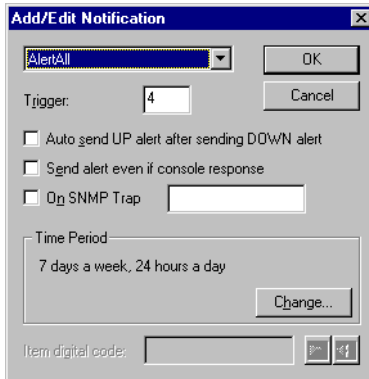
Assigning a Notification

Note

Before you can assign a notification to a device, you must define the notification. For more information, see “Defining Notifications” on page 54.

To assign a notification, you add it to the list box on the **Alerts** tab (if **Enable alerts** and **Enable Notifications** are selected):

- 1 On the **Alerts** tab, click the **Add** button to view the “Add/Edit Notifications” dialog box. The appearance of this dialog box varies slightly depending on the notification that is selected in the drop-down list at the top of the dialog box.



- 2 Select a defined notification, such as **Default Beeper** or **Default Pager**, from the drop-down list. All your defined notifications are available from this list.

- 3 Enter a **Trigger**. After this number of consecutive failed checks, WhatsUp Gold sends the notification. We recommend that this number be at least 4.
- 4 (Optional) Select **Auto send UP alert after sending DOWN alert** to send the notification when the device(s) comes back up after a down notification. This option is active for all notifications except sounds.

Quiet

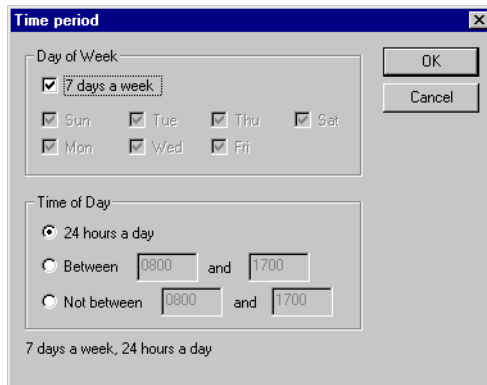


- 5 Select **Send alert even if console response** to send active notifications for the device(s) even if the alarm has been turned off on the WhatsUp Gold console by clicking the **Quiet** button in the main toolbar. (Clicking the **Quiet** button normally prevents further processing of the notifications associated with an event.)
- 6 Select **On SNMP Trap** to trigger a notification when an SNMP trap is received for the device(s). When this option is enabled, and the edit box to the right of it is empty, the specified notification will be sent when *any* SNMP trap is received for the device. If the edit box contains a trap number or numbers, notification is sent only if a trap with the specified number is received. Separate multiple entries in the text box with a comma.

You can enter a number for one of the six standard traps. If you are unsure of a number, view the Events Log (after enabling traps) to see what number is associated with a particular trap.

For more information on SNMP traps, see “Chapter 8: Monitoring SNMP Devices” on page 143.

- 7 Under **Time Period**, click **Change** to change the default setting of 7 days a week, 24 hours a day.



Select the **Day of Week** options: **7 days a week** is the default. You can clear the **7 days a week** option and then select the specific days of the week that you want to receive notifications from this device.

Select one of the three **Time of Day** options: Use **24 hours a day** to monitor all day. Use **Between** to set the start and end time for monitoring. Use **Not between** to set the hours that monitoring is turned off.

Note

When using **Between** and **Not Between**, the start time must be less than the end time. To set a period between an AM time and a PM time, you must use the 24 hour clock (0000 to 2400) or use the options together to set the hours.

- 8 If you are assigning a beeper notification, the **Item digital code** option is available. The **Item digital code** is a unique numeric code that identifies the device, for example, the IP address. This code is sent to the beeper following an “Up” or “Down” code.

Note

You can use an asterisk (*) character to separate numbers in an IP address. The asterisk displays as a dash (-) in numeric beepers. The period character (.) is not allowed in this box.

- 9 If you are assigning a voice notification, the **Wave file** text box is available. You can use this box to specify a *.wav* file that identifies the device that’s down.

To do this, record a *.wav* file for the device; for example, the recording could say “Gyro” for a device named Gyro. When the device goes down, the voice message will be “Gyro is down.” The default value in this box is [auto]; this looks for the file *display_name.wav* (for example, *gyro.wav*). If the file is not found, it plays the file *ahost.wav*, which says “a host,” as in “A host is down.”

Editing Notifications

You can edit:

- The way a notification works with a particular device
- The basic definition of a notification

To edit the way the notification works with this device, select the notification on the device properties **Alerts** tab and click the **Edit** button to see the “Add/Edit” dialog box shown on page 72. The steps below the illustration describe each of the values in this dialog box.

To edit the notification *definition*, you use the Notifications Editor. You can access the Notifications Editor in one of two ways:

- From the **View** menu, select **Notifications**.
- If you are on the **Alerts** tab of device properties, select **Enable alerts** and **Enable Notifications**. Then click the **Notifications Editor** button.

Note

If you are editing notifications from the **Alerts** tab, you must click **Save** to apply your changes.

Assigning Notifications Globally

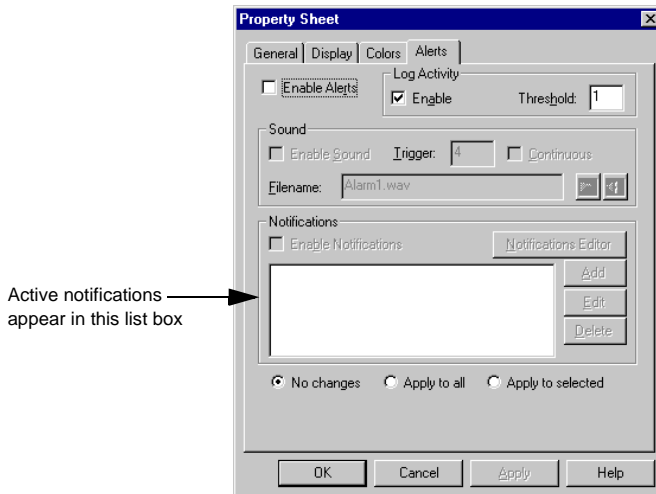
You can assign notifications globally by using the **Alerts** tab of the Map Properties. Using this tab, you can assign notifications to all devices in the map, or to just the selected devices.

Note

Notifications assigned globally (on the **Alerts** tab of Map Properties) *replace* notifications assigned to individual devices. Because of this, you should assign global notifications *before* you assign notifications for individual devices.

To assign a notification to selected devices in a network map, or to all devices in a map:

- 1 Open the network map.
- 2 (Optional) If you want to assign notifications to less than all the devices on the map, select those devices to which you want to assign the notification.
- 3 From the **File** menu, select **Map Properties** and then click the **Alerts** tab.



The notifications that appear in the list box in the **Notifications** section are the active notifications for the selected device(s).

- 4 Make sure **Enable Alerts** is selected.
- 5 If you want to log “UP” and “DOWN” events for this device, under **Log Activity**, make sure **Enable** is turned on. (These entries can be viewed on the **Log** tab of the device properties.)
- 6 To change the number of missed polls that generate a “DOWN” or “UP” event in the log, change the value in the **Threshold** box.

The **Threshold** default value is 1, which means that every missed poll is logged; this setting gives you the most complete information about your network: when any device (or a monitored service on a device) misses one poll, it is logged as “DOWN” or “SVCDOWN.”

If you have a device on your network that routinely misses just one poll, you may feel that you are getting too many “DOWN” or “UP” messages in the Event Log. In this type of situation, you can set the **Threshold** to a higher number such as 2, 3, or 4.

However, if you have assigned notifications to this device and want to make sure, for clarity’s sake, that a “DOWN” or “UP” event for this device is recorded in the Event Log *before* any alerts or notifications are recorded, make sure the **Threshold** value is *less than or equal to* the **Trigger** value of any notifications assigned to this device.

- 7 (Optional) In the **Sound** section of the **Alerts** tab, select **Enable Sound**, and then assign or change the sound alarm.

Note

To play the alarm sounds, you must have a sound card and speakers installed on your system. Also, do not enable sounds if you plan to run WhatsUp Gold as an NT service.

Trigger. Enter the number of consecutive missed polls after which the alarm will be sounded. The default value is 4.

Continuous. Select this option to sound the alarm until it is manually turned off (by clicking the **Quiet** button in the main toolbar).



Filename. Enter or select the sound (.wav) file that will be played when the devices go down. WhatsUp Gold provides three .wav files: *alarm1.wav*, *alarm2.wav*, *alarm3.wav*.



Click the **Browse** button to browse the directories and select a .wav file. Click the **Invoke Sound Recorder** button to open the .wav file in the Sound Recorder. You can play the sound file or edit it to create a different sound. For information on using Sound Recorder, see the Sound Recorder **Help**.

- 8 In the **Notifications** section of the **Alerts** tab, select **Enable** to activate this section of the **Alerts** tab.
- 9 Do one of the following:
To add notifications to the list box, see “Assigning a Notification” on page 72.

To edit a notification, see “Editing Notifications” on page 75.

To delete a notification, select it and click **Delete**.

Note

When deleting notifications, make sure you have selected **Apply to all** or **Apply to selected** before you click the **Apply** button.

- 10 Do one of the following:
 - Select **Apply to all**.
 - Select **Apply to selected**.
- 11 Click **Apply** to apply your changes. Click **OK** to apply your changes and exit the “Map Properties” dialog box.

Chapter 4: Monitoring Services

When WhatsUp Gold checks a device, it also checks each service you have selected to monitor on the **Service** tab of the device properties.

WhatsUp Gold can monitor:

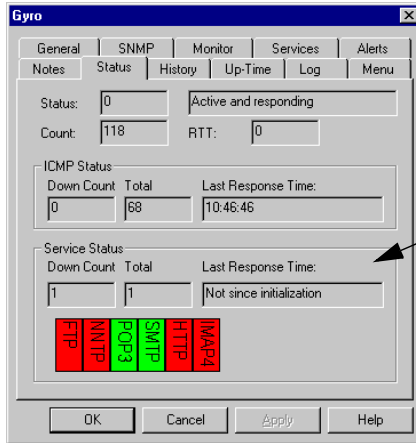
- Standard TCP/IP services
- Nonstandard TCP/IP services such as those that use nonstandard port numbers (for example: Radius or IRC)
- Any other services (such as NT system services) that can be checked by a custom, user-defined module using Microsoft's Component Object Model interface. See "Custom Services API" on page 89.

When a monitored service misses a poll, you have several ways of knowing about it:

- An event is automatically recorded in the Event Log and on the **Log** tab of the device properties.
- The **Status** tab of device properties is automatically updated.
- The device icon on the network map automatically changes color to purple (provided you are using the default colors).
- (Optional) A notification is sent. (This happens if a notification is assigned to the device on which the service is running.)

Note

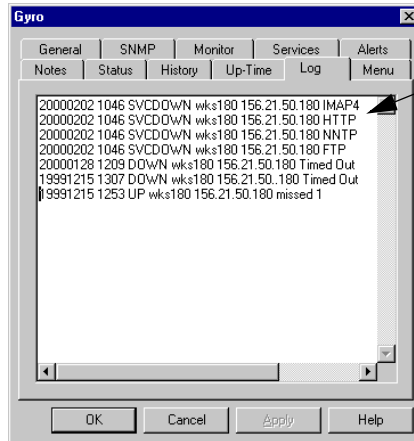
Using WhatsUp Gold to monitor a service that is logged by another application may increase the size of that application's log files by generating entries to those files. Also, the other application may view the WhatsUp Gold checks as failed connections; this could negatively impact statistics generated from the other application's log files.



Device **Status** tab shows service status.

Note

To reduce the load on your network, we recommend you monitor only the most critical services, and not every service on a device.



Device **Log** tab shows services down.

Monitoring Standard TCP/IP Services

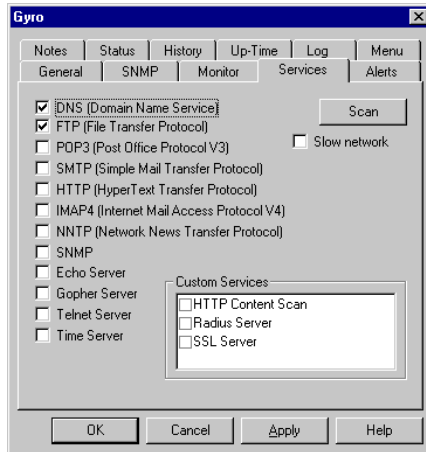
Standard TCP/IP services include DNS, FTP, POP3, SMTP, HTTP, IMAP4, NNTP, SNMP, Echo, Gopher, Telnet, and Time. You can scan a device to see which of these standard services are running on it.

To scan a device to see what services are running:

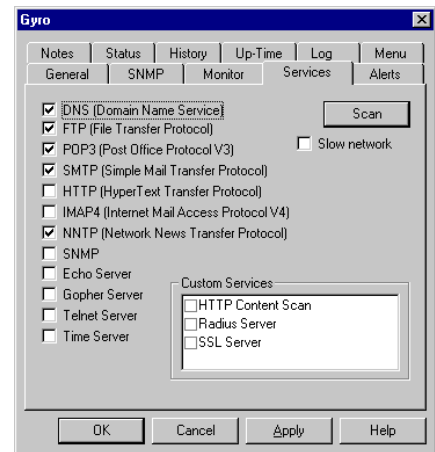
- 1 Double-click the device to view its properties
- 2 Click the **Services** tab.
- 3 Click the **Scan** button.

Any services found are turned on (check mark is displayed) for monitoring.

The Services tab before clicking the Scan button shows two services being monitored.



After clicking the Scan button, the tab shows three additional services running on the device.



By default, WhatsUp Gold monitors services using ICMP packets, but if you want to monitor a service on a device that does not allow ICMP packets, you need to change the **ICMP** setting to **TCP** on the **General** tab of the device properties.

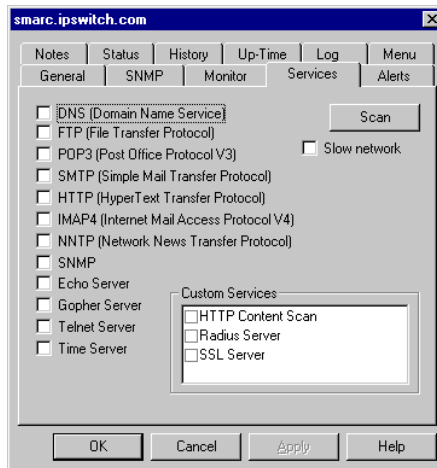
Note

The **TCP** setting uses either TCP or UDP to poll the service. To use this method of monitoring a device, at least one service must be monitored on that device.

Services can be monitored only on a device that has ICMP or TCP selected as the polling method (on the **General** tab of the device properties). In other words, if you have selected IPX or NetBIOS as the polling method for the device, you cannot monitor the TCP/IP services on that device.

You indicate what TCP/IP services you want to monitor on the **Services** tab of the device properties.

- 1 Double click a device to view its properties. Click the **Monitor** tab and select **Monitor This Device**.
- 2 Click the **Services** tab.



- 3 Select the services you want to monitor.

You can click the **Scan** button on the **Services** tab to scan the device and see which of the standard services are running on it: WhatsUp Gold selects all active services it finds.

- 4 Click **Apply** to save changes.

Monitoring Custom Services

You can also monitor “custom” services. Custom services include:

- TCP/IP services that are not listed on the **Services** tab (such as Radius or IRC)
- TCP/IP services that use a nonstandard port number

You can define an unlimited number of TCP/IP custom services; these become dynamic, sharable objects that can be monitored on any device on any network map.

WhatsUp Gold is shipped with custom services already defined for you:

- HTTP Content Scan
- Radius Server (Remote Authentication and Dial-In User Service)
- SSL Server

You can define additional TCP services. For example, you may want to monitor an IRC (Internet Relay Chat) service, a Lotus Notes server, a Microsoft SQL server, or a Microsoft Exchange service.

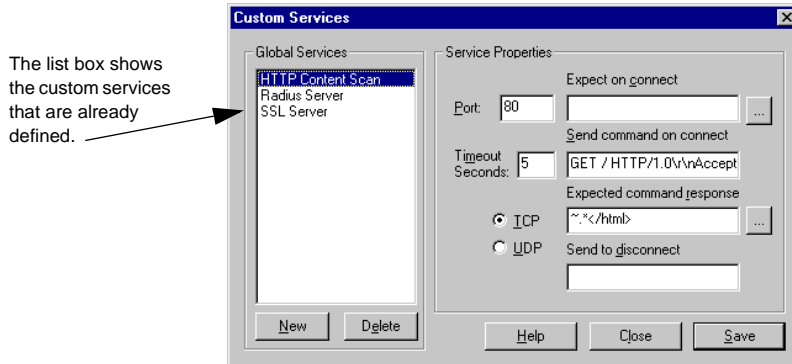
Defining a Custom TCP/IP Service

The monitoring of a service always involves a protocol handshake and can also include some additional information exchange between WhatsUp Gold and the service. You can search the response from the service for an exact match of a particular text string, or you can use rules expressions to analyze the response for a more generic text pattern.

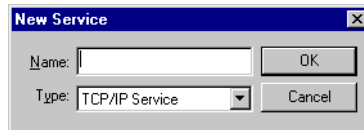
For example, if you are looking for *any* error message, and you know that all possible error messages have the word “fail” in common, you can use a rule expression to look for just the word “fail.” Or, you can create a rule expression that looks for any number of possible error messages. (You can search for “this,” “that,” or “the other.”).

To define a custom TCP/IP service:

- 1 Select **Custom Services** from the **View** menu. You see the following dialog box.



- 2 Click the **New** button.



- 3 Select **TCP/IP Service** from the **Type** drop-down list.
- 4 In the **Name** text box, enter a unique name for the service. This name will be displayed as a selectable option on the **Services** tab of the device properties. Click **OK** to return to the “Custom Services” dialog box shown above. The name you entered for the new service now appears in the **Global Services** list box.
- 5 In the **Global Services** list, select the name you just entered.
- 6 In the **Port** text box, enter the TCP or UDP port that you wish to monitor. For example, 6667 is the standard port for IRC.
- 7 In the **Timeout Seconds** text box, set the timeout for the service status, in seconds. Note that this is different than the timeout used for polling a device.
- 8 Select the **TCP** or **UDP** network type.
- 9 In the **Expect on connect** text box, enter a text string or a rule expression that you expect the remote service to send back to you on connect. For information on composing a rule expression, see “Using Rules Expressions” on page 86.

- 10 In the **Send command on connect** text box, enter the command to send to the service's port.

Examples:

For IRC, the command is

```
Version\r\n
```

For HTTP, the command is:

```
GET /Access/myprogs/dbstat.qry HTTP/1.0\r\nAccept:
*/*\r\nUser-Agent: Ipswitch_Whatsup/5.0\r\n\r\n
```

(This is for a cgi program named *dbstat.qry* located in */Access/myprogs/*; this program performs a status check of a database.)

- 11 In the **Expected command response** text box, enter text or a rule expression that represents the expected response to the send command. For example, for IRC, this is

```
:irc
```

For the HTTP example above, you might scan for an approximate match by using:

```
.*(successful|success|ok)
```

You can enter a customized string that you have set up on the service to tell you that everything is OK. For more information, “Using Rules Expressions” below.

- 12 In the **Send to disconnect** text box, enter a command string to disconnect from the service properly. For most TCP/IP servers, the string `QUIT\r\n` is proper. If a command string is not specified, the connection is closed by sending a FIN packet and then an RST packet.
- 13 Click **Save**.

Note

You *must* click the **Save** button to save the custom service.

Using Rules Expressions

The rule expression syntax is:

search_text *quantifier*

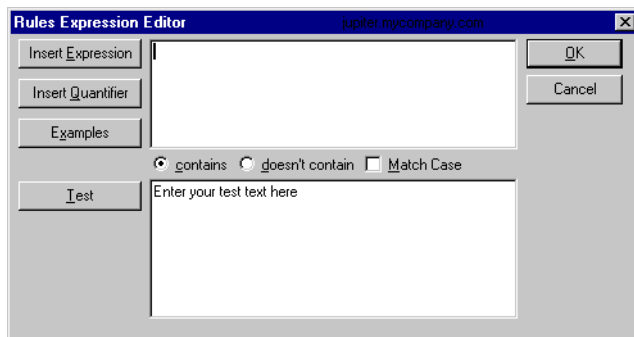
Note that *search_text* can be any combination of literal text and the text patterns shown below.

To create a rule expression:

Browse button



- 1 In the “Custom Services” dialog box shown on page 84, click the Browse button next to **Expect on connect** or **Expected command response** to view the Rules Expression Editor.



- 2 Select the **contains** option to look for messages that contain the search string; select **doesn't contain** to look for messages that do *not* contain the search string.
- 3 Select **Match Case** to search for text that matches the case of the search string; to ignore case, make sure **Match Case** is *not* selected.
- 4 Enter the expected text by doing one or more of the following:
 - Type the literal text that you want to search for. For example, if you want to find the word *fail*, type *f a i l*.
 - Type the text and quantifiers you want to search for; See “Rules Expressions Text and Quantifiers Tables” on page 87.
 - Click **Insert Expression** or **Insert Quantifier** to insert a generic form of a text pattern or a quantifier. Then edit the inserted expression. See “Rules Expressions Text and Quantifiers Tables” below.
- 5 Click **OK** to save the rule.

Rules Expressions Text and Quantifiers Tables

Text Pattern	Expression
Any character	.
Any of the values separated by vertical bars within the parentheses; the vertical bar represents "or"	
Any word character (a-z, A-Z, 0-9)	\w
Any non-word character	\W
Any digit (0-9)	\d
Any non-digit	\D
Any white space (spaces and/or tabs and/or carriage returns)	\s
Any non-white space	\S
Any punctuation character (any character other than \w or \s)	\p
Any non-punctuation character	\P
Binary value	%nnn where nnn is a number between 0 and 255

Quantifier	Expression
Zero or more	*
One or more	+
Exactly n	{n}
At least n1, but not more than n2 (where n1 and n2 are numbers)	{n1,n2}

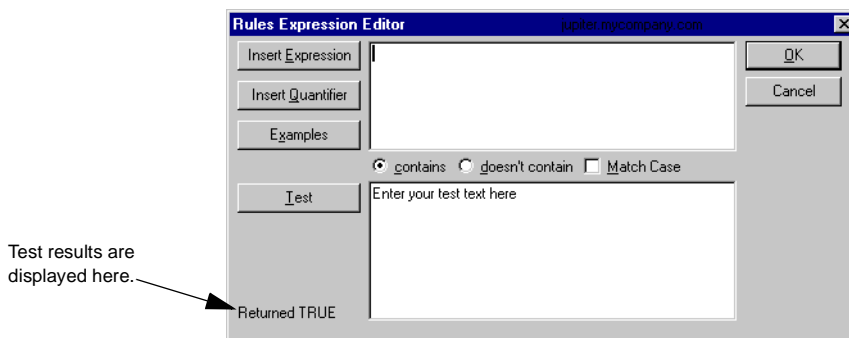
Note: As shown above, the following characters have special meaning in a rule:

{ } () | * + , . : %

If you want to use one of these characters in a search string, precede it with a backslash. For example, to search for a plus sign, enter \+ in the search string.

Testing a Rules Expression

To test a rule expression, you use the Rules Expression Editor.



Browse button



1 If the Rules Expression Editor is not visible, select **Custom Services** from the **View** menu. Then, select the rule you want to test. Click the Browse button next to the rule to view the Rules Expression Editor.

2 In the lower text box of the Rules Expression Editor, copy a message that meets your intended search criteria and click **Test**.

If the rule expression does what you intended it to, **Returned TRUE** is displayed. If the rule expression *doesn't* test true, **Returned FALSE** is displayed. Edit the rule expression and test again. For a long or complex rule expression, we recommend you test one part of it at a time.

Summary of Service Monitoring Requirements

When you want to monitor services (either standard or custom), you need to make the following changes to the device properties:

- Turn on **Monitor This Device** on the **Monitor** tab of the device properties
- Use the **Service** tab of the device properties to select the services to monitor on the device.

Custom Services API

WhatsUp Gold provides a COM interface to allow experienced COM program developers to create customized service checks that “plug in” to WhatsUp Gold. In fact, the TCP/IP Service monitoring capability of WhatsUp Gold is implemented as a plug-in module that uses WhatsUp Gold’s COM interface.

You can also visit our web site and download other plug-ins such as an NT Service Monitor Plug-In and an SNMP Threshold Plug-In. Any other plug-in modules we make available in the future will also be listed on our web site.

To write your own plug-in modules, see the *wugapi.h* file that was installed with WhatsUp Gold.

Note

All pertinent information regarding the implementation of the COM interface is provided in the *wugapi.h* file that is automatically installed in the WUG program directory. The information in this file is for experienced COM program developers to use to extend the monitoring capabilities of WhatsUp Gold. It is beyond the scope of this document to provide any guidance on writing COM applications.

Chapter 5: Working from the Console

WhatsUp Gold has two interfaces: the console and the web interface. The WhatsUp Gold console is the system on which WhatsUp Gold is installed.

This chapter describes how to use the console to start and stop polling of the devices in your network map and how to display network status. “Chapter 7: Working from a Web Browser” tells you how to use WhatsUp Gold from the web interface.

Opening Network Maps

In order for WhatsUp Gold to monitor a network, you need to have the network map open. You can open previously-defined maps [**File --> Open**] or create a new network map [**File --> New**]. For detailed information on creating a network map, see “Chapter 2: Creating Network Maps” on page 13.

You can open multiple map windows and WhatsUp Gold can monitor the network maps simultaneously. If you open a map that contains subnets, the subnet maps will also open.

For any device that you do not want to poll, you can turn off **Monitor This Item** on the **Monitor** tab of the device properties. (The icon for any device that is not being actively monitored is displayed in dark gray by default.)

Starting and Stopping Polling

When you open a network map, Whatsup Gold immediately starts automatic polling — it polls the devices continuously, starting each new pass after a specified time interval. If a map contains subnet maps, WhatsUp Gold also opens the subnet maps and starts polling. You can stop and start automatic polling at any time.

You can also start a single check of the network, in which case WhatsUp Gold makes a single pass through the devices in the active network map, polling each device.

To Initiate Automatic Polling

When you open a network map, Whatsup Gold immediately starts automatic polling on the map and any associated subnet maps.

To change the default settings for automatic polling, choose **Map Properties** from the **File** menu. The map properties appear. On the **General** tab, set the number of seconds you want between checks (**Poll Frequency**), the number of seconds to wait before timeout (**Default Timeout**), and any other options you may want to change.

If polling is stopped, you can restart automatic polling of currently active devices by clicking the **Stopwatch** button in the main toolbar. WhatsUp Gold checks each device and tracks the responses. After waiting the time set in the **Poll Frequency**, it makes a second polling pass through the devices and continues polling until you stop polling by clicking on the **Stopwatch** button again or by closing the map window.

Stopwatch button



WhatsUp Gold polls the devices in the order in which they were created in the network map. To view or change the polling sequence, select **Dependencies Window** from the **Windows** menu. For more information, see “Viewing and Changing Dependencies” on page 96.

To Stop Automatic Polling

To temporarily stop automatic polling, click the **Stopwatch** button in the main toolbar. To resume polling, click **Stopwatch** again.

Note

If you exit WhatsUp Gold during a poll, it may take up to 30 seconds for WhatsUp Gold to remove itself from memory. Until it is removed from memory, WhatsUp Gold appears in the Windows task list (when you press Ctrl+Alt+Del).

To Check a Device

To do an immediate poll of a device, right-click a device and select **Check now** from the pop-up menu.

Reading the Network Map

By default, the following conventions are used in the map window to indicate the status of a device or service:

- Inverted device name — an event has been recorded for the device. For more information, see “Types of Events Logged” on page 104.
- Green device icon — the device is “up” (responding to polling)
- Light green icon — the device has missed at least one polling request
- Yellow icon — the device has missed two polling requests
- Red icon — the device is “down” (It is not accessible or has not responded to four consecutive polling requests)
- Purple icon — a standard service on the device is down

You can change the default colors in the map properties, as described in the [Map Color Properties](#) topic in [Help](#).

You can quickly display a brief status message by moving the cursor over a device icon. In the status bar of the map window, a message displays the device’s host name, IP address, and current status or service status.

WhatsUp Gold displays a count-down timer on the right side of the status bar of the map window. The timer is set to the **Map Poll Frequency (File -> Map Properties)** and counts down to one between each poll. WhatsUp Gold resets this timer after each poll.

Receiving Alarms

If sound is enabled (on the **Alerts** tab of device properties), an alarm sounds when a device fails to respond to four (the default) consecutive polling requests. To play the alarm, you must have a sound card installed on your system. You can set the number of failed poll requests that triggers a sound alert.

Quiet button



To turn off a sound alarm, click the **Quiet** button in the main toolbar, or select **Stop Alarm** from the **Tools** menu.

Receiving Notifications

Enabled notifications are sent when:

- The device fails to respond to the specified number of polling requests
- A monitored service goes down
- An SNMP trap is received for a device

To view the active notifications for a network map, select **Notifications Window** from the **Windows** menu. For more information, see “Viewing Active Notifications” on page 100.

Acknowledging Alerts

To acknowledge alerts, select **Acknowledge** from the **Tools** menu. **Acknowledge** is active only when there are unacknowledged alerts. Clicking it acknowledges alerts and prevents any pending alerts from being sent.

Using the Status Tab

To display status information associated with any of the displayed devices (active or inactive), double click the device to view its properties. Click the **Status** tab to display current status information.

The screenshot shows the 'Gyro' dialog box with the 'Status' tab selected. The dialog has a title bar with 'Gyro' and a close button. Below the title bar are several tabs: 'General', 'SNMP', 'Monitor', 'Services', 'Alerts', 'Notes', 'Status', 'History', 'Up-Time', 'Log', and 'Menu'. The 'Status' tab is active, displaying the following information:

Status:	0	Active and responding
Count:	118	RTT: 0
ICMP Status		
Down Count	Total	Last Response Time:
0	68	10:46:46
Service Status		
Down Count	Total	Last Response Time:
1	1	Not since initialization

At the bottom of the dialog, there are five colored buttons representing different services: FTP (red), NNTP (green), POP3 (green), SMTP (green), and HTTP (red). Below these buttons are four standard dialog buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

The **Status** tab displays the status of packets sent by WhatsUp Gold to poll this device and a current status message. These status numbers are measured from the last time the device's counters were cleared.

Status. Current status of the device. A zero status code indicates the device is up. A numeric status code above 10000 is a Winsock error code. The text for the error message is also displayed.

Count. Total number of times this device was polled.

RTT. Round Trip Time (RTT) is the time (in milliseconds) that it took the last packet sent to arrive at the device and return.

The **Status** tab shows the following three items for the Device (ICMP) Status and Service Status:

Down Count. Count of how many polls have passed since the device or service last responded.

Total. Total count of how many polls occurred where the device or service did not respond since the counter was last cleared, WhatsUp Gold started, or since the device was added to the map.

Last Response Time. Time of day (in *hours:minutes:seconds*) of the last response.

The services graph at the bottom of the dialog box shows the status of any services being monitored on the device (as specified on the **Services** tab). Services cannot be monitored if NetBIOS or IPX is the selected polling method. A service is green if it is up, red if it is down.

You can also display the following status information from within a device's properties:

- Click the **History** tab to display a graph of the round trip times of the device over the last 30 polls. Red vertical bars indicate the device was not responding.
- Click the **Up-Time** tab to display a pie chart that shows the percentage of successful polls for the total poll count.
- Click the **Log** tab to display any service or device "up" or "down" events for this device. On the **Alerts** tab, you can enable logging for the device (select **Enable** in the **Log Activity** section).

Using the Status Window

The Status Window shows a list of all the devices in the currently active map and displays the status using the same colors used on the map. It also shows the status of any services being monitored.

From the **Window** menu, select **Status Window**.



You can monitor the network through the Status Window. You may need to expand the Status Window in order to read the service status information.

Poll button



In the main toolbar, click the **Poll** button to start a single check of each device in the Status Window. Click the **Stopwatch** button to start automatic polling of each device.

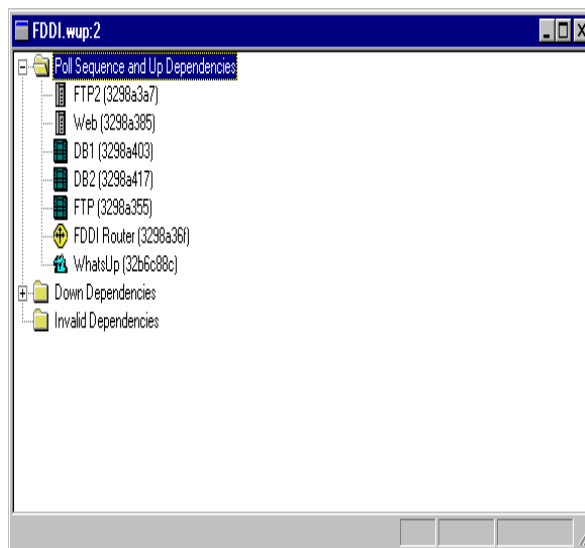
You can double click a device in the Status window to display the device properties.

Viewing and Changing Dependencies

By default, WhatsUp Gold polls devices in the order that they were added to the map. In the Dependencies Window, you can view and change the polling sequence and a device's dependency on other devices.

You can set or change a dependency so that certain devices get polled only if another device that they are connected to is up or down. For example, you may want to poll intervening routers only if the end point cannot be reached. An easy way to set this up is to use the Traceroute tool (see page 171) to automatically map a path to an address and tell it to **Set Dependencies**. Look at the result in the Dependencies Window after doing this.

From the **Window** menu, select **Dependencies Window**.



The Dependencies Window shows the network as a hierarchical tree showing the polling sequence and user-defined up and down dependencies. The value in the parenthesis after the name is an item identifier to resolve ambiguous device names.

Poll Sequence and Up Dependencies. Devices are listed in the order they are polled. If a device is “up dependent” on the device above it, it is indented. You can drag a device within the branch to change the polling order of the device.

To change the polling sequence, do one of the following:

- In the **Poll Sequence and Up Dependencies** list, drag a device to a different location in the Poll Sequence list.
- Right-click a device and use the popup menu.
- Select a device and use the Arrange menu.

The following commands appear on the popup and **Arrange** menus:

Move to Start of Poll. Make the device the first device to be polled.

Move to Earlier in Poll. Move the device up one position in the order.

Move to End of Poll. Make the device the last device to be polled.

Move to Later in Poll. Move the device down one position in the polling order.

Setting “Up” and “Down” Dependencies

You can set any of the devices in the map to have an “up” or “down” dependency on another device in the map. An “up dependency” means that the device is checked only if another specified device is up. A “down dependency” means that the device gets checked only if the other device is down.

Dependencies are shown in the **Up Dependencies** and **Down Dependencies** lists by their location and indentation. If a device is dependent on another device, it is indented below the other device.

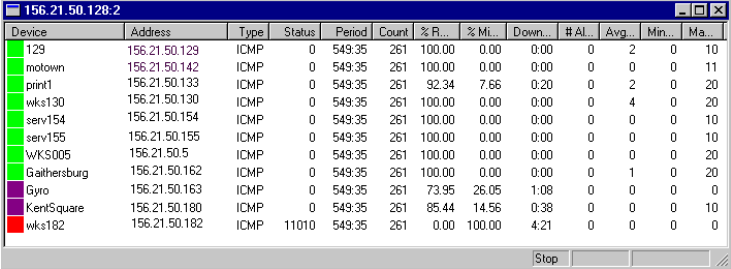
To set an up or down dependency:

- 1 In the **Up Dependencies** or **Down Dependencies** list, move the device that you want to have a dependency so that it appears just below the device it will depend on.
- 2 Right-click the device that you want to have the dependency.
- 3 Select **Depend on Prior Item** from the right-mouse menu.

Viewing the Polling Statistics

WhatsUp Gold provides easy access to the polling statistics for the active map. From the **Windows** menu, select **Statistics Window** to view the accumulated statistics for each device in the active network map.

The polling statistics are retained when you close or open network maps. Each map has an associated *.wui* file. Polling statistics are logged in the *map_name.wui* file.



Device	Address	Type	Status	Period	Count	% R...	% Mi...	Down...	# Al...	Avg...	Min...	Ma...
129	156.21.50.129	ICMP	0	549:35	261	100.00	0.00	0.00	0	2	0	10
motown	156.21.50.142	ICMP	0	549:35	261	100.00	0.00	0.00	0	0	0	11
print1	156.21.50.133	ICMP	0	549:35	261	92.34	7.66	0.20	0	2	0	20
wks130	156.21.50.130	ICMP	0	549:35	261	100.00	0.00	0.00	0	4	0	20
serv154	156.21.50.154	ICMP	0	549:35	261	100.00	0.00	0.00	0	0	0	10
serv155	156.21.50.155	ICMP	0	549:35	261	100.00	0.00	0.00	0	0	0	10
WKS5005	156.21.50.5	ICMP	0	549:35	261	100.00	0.00	0.00	0	0	0	20
Gaithersburg	156.21.50.162	ICMP	0	549:35	261	100.00	0.00	0.00	0	1	0	20
Gyro	156.21.50.163	ICMP	0	549:35	261	73.95	26.05	1.08	0	0	0	0
KentSquare	156.21.50.180	ICMP	0	549:35	261	85.44	14.56	0.38	0	0	0	10
wks182	156.21.50.182	ICMP	11010	549:35	261	0.00	100.00	4.21	0	0	0	0

The Statistics Window lists all of the devices in the network map and shows the following statistics for each device:

Device. The device name.

Address. Device address (if the polling method is ICMP or TCP/IP).

Type. The polling method (ICMP, TCP, NetBIOS, or IPX) set on the **General** tab in the device properties.

Status. The device's last read status. A zero status indicates the device is up. Any other value indicates an error. If it is a TCP/IP device, you may see a status code above 10000, a Winsock error code. To view a reported error, click the **Status** tab of the device properties.

For each device, the Statistics Window also shows the counters described below. These values are cumulative until you reset them for a map in one of two ways:

- Using the **Reset Counters** command on the **Tools** menu (*available only when the Statistics Window is open*)
- Using the **Reset Counters** function in the web interface

The counters shown in this window are not the same as those shown in the Statistics Log. Counters in the Statistics Window are cumulative per device. Counters in the Statistics Log are written per device at an interval determined by the setting on the **Statistics Generation** tab (**Options -> Program Options**).

Period. The time (in *hours:minutes*) since the counters were last cleared.

Count. The number of times the device has been polled since last cleared.

% Responded. Of the total number of polls to the device, the percent that responded.

% Missed. Of the total number of polls to the device, the percent that failed.

Down Time. The total down time (in *hours:minutes*) for this device. This is calculated by multiplying the number of missed polls by the Map Poll Frequency. For example, if the device misses 7 polls, and the poll frequency is once per minute, the down time will be 7 minutes.

Alerts. The number of alerts that have occurred for the device.

AvgRTT. Average round trip time (RTT) of the last polls sent.

MinRTT. Minimum RTT of polls sent to the device.

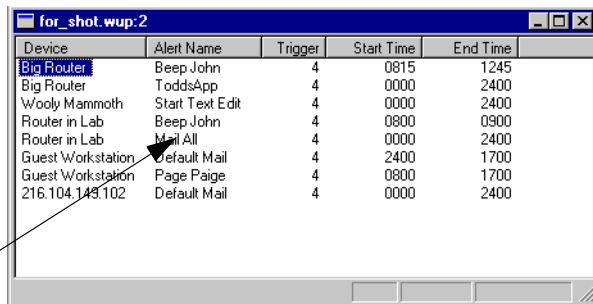
MaxRTT. Maximum RTT of polls sent to the device.

You can click any of the column headings to toggle the sort between ascending and descending.

Viewing Active Notifications

You can view the notifications enabled for the active network map. From the **Window** menu, select **Notifications Window**.

Double-click a device name to view the Alerts tab of the device properties. →



The screenshot shows a window titled "for_shot.wup:2" containing a table of notifications. The table has five columns: Device, Alert Name, Trigger, Start Time, and End Time. The data is grouped by device. An arrow points from the text "Double-click a device name to view the Alerts tab of the device properties." to the "Big Router" entry. Another arrow points from the text "Double-click an Alert Name to view the Notifications Editor." to the "Mail All" alert name.

Device	Alert Name	Trigger	Start Time	End Time
Big Router	Beep John	4	0815	1245
Big Router	ToddsApp	4	0000	2400
Wooly Mammoth	Start Text Edit	4	0000	2400
Router in Lab	Beep John	4	0800	0900
Router in Lab	Mail All	4	0000	2400
Guest Workstation	Default Mail	4	2400	1700
Guest Workstation	Page Paige	4	0800	1700
216.104.149.102	Default Mail	4	0000	2400

Double-click an Alert Name to view the Notifications Editor.

The notifications are grouped by device. Click a column heading to toggle the sort between ascending and descending order.

Using the Mini Status View

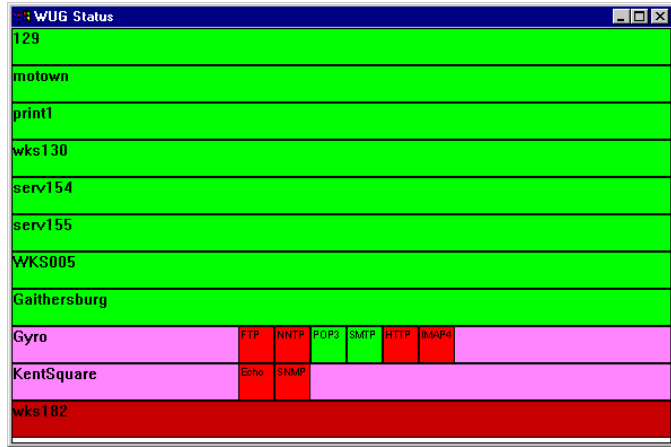
The Mini Status view is a small profile window that you can use to monitor network status in place of the map window. The Mini Status view lists all devices in the currently active maps and displays status using the same colors used in the map window.

From the **View** menu, select **Mini Status**. The WhatsUp Gold main window is closed and the Mini Status view appears.

Each open map is listed in a separate column. Any services being monitored on a device are shown.

Click the Mini Status view to silence an alarm.

Double-click the Mini Status view to close it and go back to the map window.



The screenshot shows a window titled "WUG Status" with a list of maps and their monitored services. The maps are listed in a column, and the services are listed in a row below each map. The services are color-coded: red for failed, green for successful, and yellow for warning.

Map	FTP	NTP	POP3	SMTP	HTTP	IMAP4
129						
motown						
print1						
wks130						
serv154						
serv155						
WKS005						
Gaithersburg						
Gyro	Failed	Failed	Warning	Warning	Failed	Failed
KentSquare	Failed	Failed				
wks182	Failed	Failed	Failed	Failed	Failed	Failed

Chapter 6: Logs and Reports

WhatsUp Gold logs two types of data:

- **Events** — Events are changes to network status, such as a device going down or a device coming back up. Events are recorded in the Event Log (*whatsupg.log*), which provides a history of what has occurred on the network. In addition, the Debug Log window provides a view of events as they occur.
- **Polling statistics** — Polling statistics are the accumulated round trip times (RTT) of polls sent to a device. These statistics measure the availability and performance of a device. Polling statistics are recorded in the Statistics Log (*wugstats.log*).

From this logged data, WhatsUp Gold can create several reports and graphs that show the status of your network in different ways. From the **Reports** menu, you can create the following:

Event Reports. Show device up and down events, service up and down events, and WhatsUp Gold events such as map open and close. You can print this report or create a tab-delimited file from it.

Statistics Reports. Show round trip times and percentage of missed polls based on the accumulated polling statistics for each device. You can print this report or create a tab-delimited file from it.

Performance Graphs. Show devices by best or worst performance based on aggregated polling statistics, and shows graphs for each device.

Recurring Reports. Show network status (count and names of devices that are up, count and names of devices that are down, and the most recent lines from the Event Log). Recurring reports are sent as a pager, e-mail, or beeper message at a specified time interval.

This chapter describes how to use the WhatsUp Gold logs and reports. They are available from the console and from the web interface.

Note

Performance graphs are not available from the web interface, but can be exported to HTML format (for more information, see see “Using the Command Line for Performance Graphs” on page 123.).

Logging and Reporting Events

WhatsUp Gold logs events in the Event Log (*whatsupg.log*) and lets you create reports based on the event data.

WhatsUp Gold automatically logs application-level events (such as opening or closing a map) and device-specific events (such as a device or service down) for devices that have **Log Activity** enabled on the Alerts tab. After WhatsUp Gold logs sufficient event data, you can generate reports on the data or save the data in a tab-delimited format that can be imported to another application.

The following sections describe the types of events logged, how you can modify event logging, and how you can generate reports on the events.

Types of Events Logged

WhatsUp Gold records events in the log (*whatsupg.log*) as they occur. WhatsUp Gold logs the following types of events for any open maps:

- Map changes — includes map open and close and changes to the map configuration.
- SNMP traps — logs SNMP trap server start or stop and any SNMP traps received for a device.
- Device changes — for devices that have **Log Activity** enabled on the Alerts tab, WhatsUp Gold logs an up or down alert for a device or a service and missed polls for a device. When a device comes back up, it logs the total number of missed polls and the total down time.
- Notifications — all notifications that get sent are logged.
- Acknowledged Alerts — logs an event when you select **Tools** -> **Acknowledge** (to clear all alerts) on the console or click **Acknowledge** in the web interface.
- Access table lockout events — occurs when a web access attempt is denied, for example, due to settings on the **Web Access** tab of **Program Options**. The log entry also shows the IP address of the host that attempted to log on to the web server.
- NT Service events — any up or down events resulting from checking an NT Service.

Changing How Events Are Logged

The application-level events (such as opening or closing a map) are logged automatically. For device-specific events, you can specify:

- Whether the up or down events for a device are logged
- The number of polls missed (**Threshold**) before a “DOWN” or “SVSDOWN” event is recorded for a device or for a monitored service on a device

To change how events are logged for a single device:

- 1 Double-click the device to display its properties.
- 2 Click the **Alerts** tab.
- 3 To log “UP” and “DOWN” events for this device, under **Log Activity**, make sure **Enable** is turned on. (These entries can be viewed on the **Log** tab of the device properties.)
- 4 To change the number of missed polls that generate a “DOWN” or “UP” event, change the value in the **Threshold** box.

The **Threshold** default value is 1, which means that every missed poll is logged; this setting gives you the most complete information about your network: when a device (or a monitored service on the device) misses one poll, it is logged as “DOWN” or “SVCDOWN.”

If you have a device on your network that routinely misses just one poll, you may feel that you are getting too many “Down” or “Up” messages in the Event Log. In this type of situation, you can set the **Threshold** to a higher number such as 2, 3, or 4.

However, if you have assigned notifications to this device and want to make sure, for clarity’s sake, that a “Down” or “Up” event for this device is recorded in the Event Log *before* any alerts or notifications are recorded, make sure the **Threshold** value is *less than or equal to* the **Trigger** value of any notifications assigned to this device.

- 5 Click **Apply** to save your changes.

To change how events are logged for all devices or multiple selected devices:

- 1 (Optional) To change how events are logged for some number of devices in the map, select the devices.
- 2 Select **Map Properties** from the **File** menu.
- 3 Click the **Alerts** tab.
- 4 If you want to log “UP” and “DOWN” events for the selected devices (or for all devices), under **Log Activity**, make sure **Enable** is turned on.
- 5 To log events for the selected devices (or for all devices), make sure **Enable** is turned on under **Log Activity**.
- 6 To change the number of missed polls that generate a “DOWN” or “UP” event, change the value in the **Threshold** box.

The **Threshold** default value is 1, which means that every missed poll is logged; this setting gives you the most complete information about your network: when any device (or a monitored service on a device) misses one poll, it is logged as “DOWN” or “SVCDOWN.”

If you have a device on your network that routinely misses just one poll, you may feel that you are getting too many “DOWN” or “UP” messages in the Event Log. In this type of situation, you can set the **Threshold** to a higher number such as 2, 3, or 4.

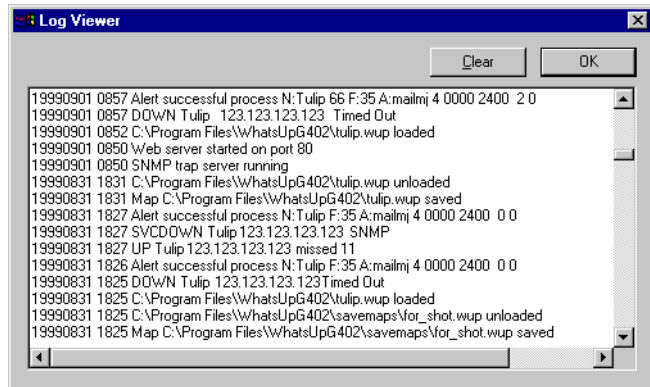
However, if you have assigned notifications to this device and want to make sure, for clarity’s sake, that a “DOWN” or “UP” event for this device is recorded in the Event Log *before* any alerts or notifications are recorded, make sure the **Threshold** value is *less than or equal to* the **Trigger** value of any notifications assigned to this device.

- 7 Select **Apply to all** or **Apply to selected**. (**Apply to selected** is available only if one or more devices are selected.)

Viewing the Event Log

The Event Log provides a history of the events that occur for any network maps that are open. For a description of the events that get logged, see “Types of Events Logged” on page 104.

To view the event information, select **Logs -> Event Log** from the **View** menu. The following screen shows an example:



The Event Log shows the date and time an event occurred, the type of event, and other pertinent information depending on the type of event.

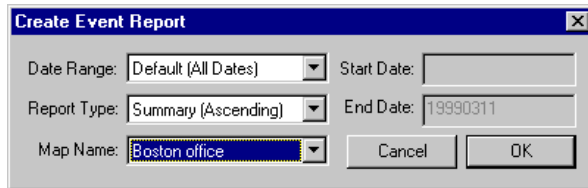
The Event Log holds the event data for *all* of your WhatsUp Gold maps. It holds data starting with either the date you first started monitoring a map or the date you last cleared the log.

Creating an Event Report

After WhatsUp Gold has been monitoring a map long enough to generate event data, you can create reports based on the event data. For a description of the events that get logged, see “Types of Events Logged” on page 104. If you want to change how events get logged, see “Changing How Events Are Logged” on page 105.

To create an Event Report:

- 1 From the **Reports** menu, select **Event Report**. The Create Event Report dialog box appears.



- 2 Select the **Date Range** for the report.

When you select an option, the **Start Date** and **End Date** are shown.

The default includes all days since you started monitoring the map, or since the event data was last cleared by clicking **Clear** in the Event Log or by clearing the log from the web interface.

Select **Custom** if you want to enter a **Start Date** and **End Date** for the report. Enter dates in the format *yyyymmdd*, for example: 19990308.

- 3 Select the **Report Type**.

Summary. Reports total service and device down time for each device and sorts by device name in **Ascending** or **Descending** order. You can also sort by **Worst First** order, which means the device with the most down time is shown first.

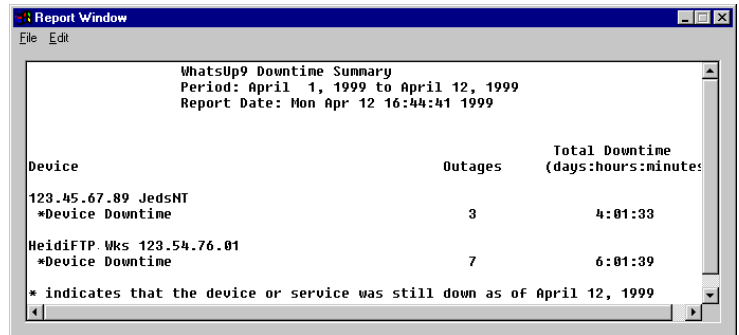
Detail. Reports all up and down events for each device. For each device down event, the elapsed down time is reported. The report sorts devices by device name in **Ascending** or **Descending** order. You can also sort by **Worst First** order, which means the device with the most down time is shown first.

In addition, the Detail report shows the following events: map configuration changes, acknowledge alerts events, NT service restarts, and access table lockouts. For more information about these events, see “Types of Events Logged” on page 104.

Raw Data. Exports the data from the Event Log to a tab-delimited file that can be imported to another application. The data is sorted by date and time in ascending order.

- 4 Select the **Map Name** of the map for which you want a report.
- 5 Click **OK** to generate the report.

WhatsUp Gold generates the specified report and displays it in the Report Window. From the Report Window, you can save the data to a file, print it, or copy data to another application.



If you get the message “insufficient data,” it’s possible that you have not monitored the map long enough to generate event data.

Debug Log Information

All actions, such as poll requests and service checks performed by WhatsUp Gold, are shown in the Debug Log window. The Debug Log is a real-time log that displays WhatsUp Gold events as they occur. To view the log, select **Logs -> Debug Logs** from the **View** menu.

Using the Command Line for Event Reports

Wugrpt.exe is a utility that can generate reports from the Event Log (*whatsupg.log*) data. You can invoke *wugrpt* from the Windows Command Prompt (MS-DOS prompt). By default, the report is displayed in the Command Prompt or MS-DOS window.

Basic Command Syntax

```
wugrpt -mmapname [-syyyymmdd] [-eyyyymmdd] [-llogfile]
[-osortmode] [-rreport] [-tmaptitle]
```

Note

You must use the *-m* argument to specify the name of the WhatsUp Gold map to use for the report. All other arguments are optional.

Argument	Explanation
<code>-mmapname</code>	The mapname must include the full path. The path and name must be enclosed in quotes. For example, <code>wugrpt -m"C:\pgms\whatsup\network1.wup"</code>
<code>-syyyymmdd</code>	Use <code>-s</code> to specify the start date for the report. The default is the oldest date in the log.
<code>-eyyyymmdd</code>	Use <code>-e</code> to specify the end date for the report. The default is the most recent date in the log.
<code>-llogfile</code>	Use <code>-l</code> to specify an alternate log file. The default is <code>whatsupg.log</code> .
<code>-osortmode</code>	Use <code>-o</code> to specify one of the sort modes: <i>Ascend</i> sorts by device name in ascending order (this is the default value); <i>Descend</i> sorts by device name in descending order; <i>Score</i> sorts by the device's "score," which is determined by the sum of polls missed. <i>Score</i> sorts from highest to lowest value.
<code>-rreport</code>	Use <code>-r</code> to specify one of the report types: <i>Detail</i> generates a report by device for all events for the selected map in the specified period. <i>Summary</i> generates a report by device for any down or up events in the selected map in the specified period. <i>Export</i> generates a tab delimited file of the raw data.
<code>-tmaptitle</code>	Use <code>-t</code> to specify the title to use at the top of the report. The default title is the map name.
<code>-?</code>	Use <code>-?</code> to see a summary of argument options.

Examples

The following examples create Event Reports for the *Boston1* map:

```
wugrpt -m"C:\Program Files\whatsup\Boston1.wup"
```

Generates a detail report for all days in the log (uses defaults).

```
wugrpt -m"C:\Program Files\whatsup\Boston1.wup"
-s19990301 -e19990131
```

Generates a detail report for one month of log data.

Return Codes

Wugrpt returns 1 if it performed at least one of the requested operations; it returns 0 if it failed.

Logging and Reporting Polling Statistics

WhatsUp Gold lets you log and report on polling statistics to provide a picture of how your network is performing over a selected time interval.

WhatsUp Gold can log polling statistics for each device in an open map. After WhatsUp Gold logs sufficient polling data, you can generate reports on the data, create performance graphs, or save the data to a tab-delimited file that can be imported to another application.

The following sections describe the polling statistics, how you can change statistics logging, and how you can generate reports from the statistics. For information on performance graphs, see “Creating Performance Graphs” on page 117.

The Polling Statistics

WhatsUp Gold writes values for the polling statistics to the Statistics Log (*wugstats.log*). By default, the statistics data is saved to the log every hour, but you can change this interval.

WhatsUp Gold can log the following polling statistics for each device in an open map:

Average RTT. The average Round Trip Time (RTT) for polls to the device. This average is taken over the interval you specify for statistics generation (**Options -> Program -> Statistics Generation**). The default value is one hour.

Maximum RTT. The highest RTT recorded for the device during the statistics interval (default is one hour).

Minimum RTT. The lowest RTT recorded during the statistics interval (default is one hour).

Percentage of missed polls. The average percentage of missed polls during the statistics interval (default is one hour).

Note that the counters shown in the Statistics Log are not the same as those shown in the Statistics Window. Counters in the Statistics Window are cumulative per device. Counters in the Statistics Log are written per device at an interval determined by the setting on the **Statistics Generation** tab of program options.

Changing Statistics Logging

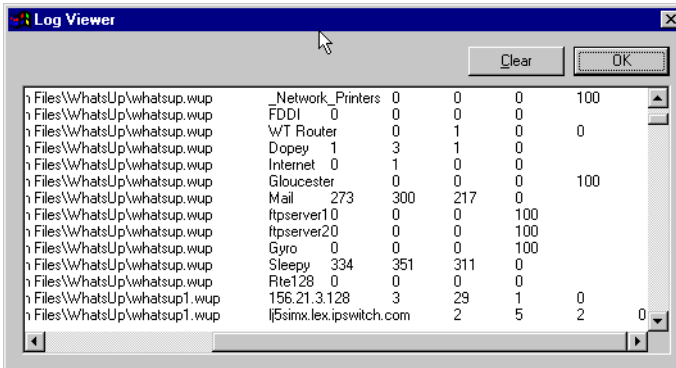
You can set how often you want polling data written to the Statistics log (*wugstats.log*). By default, statistics are written every hour.

To set how often to update the Statistics log:

- 1 From the **Options** menu, select **Program** and click the **Statistics Generation** tab.
- 2 Change the value for hours. You can set this value from 0 to 254 hours. To turn off statistics logging, set the value to zero.
- 3 Optionally, click **Update Now** to write current statistics to the log and reset the counters for each statistic.
- 4 Optionally, click **Clear** to set the statistics counters to zero.

Viewing the Statistics Log

To view the log, select **Logs -> Statistics Log** from the **View** menu. The Log Viewer appears. The following screen shows an example:



The screenshot shows a window titled "Log Viewer" with a "Clear" button and an "OK" button. The window contains a table with the following data:

h Files\WhatsUp\whatsup.wup	_Network_Printers	0	0	0	100
h Files\WhatsUp\whatsup.wup	FDDI	0	0	0	0
h Files\WhatsUp\whatsup.wup	WT Router	0	1	0	0
h Files\WhatsUp\whatsup.wup	Dopey	1	3	1	0
h Files\WhatsUp\whatsup.wup	Internet	0	1	0	0
h Files\WhatsUp\whatsup.wup	Gloucester	0	0	0	100
h Files\WhatsUp\whatsup.wup	Mail	273	300	217	0
h Files\WhatsUp\whatsup.wup	ftpserver10	0	0	0	100
h Files\WhatsUp\whatsup.wup	ftpserver20	0	0	0	100
h Files\WhatsUp\whatsup.wup	Gyro	0	0	0	100
h Files\WhatsUp\whatsup.wup	Sleepy	334	351	311	0
h Files\WhatsUp\whatsup.wup	Rite128	0	0	0	0
h Files\WhatsUp\whatsup1.wup	156.21.3.128	3	23	1	0
h Files\WhatsUp\whatsup1.wup	l5simx.lex.ipswitch.com	2	5	2	0

The Statistics Log shows the following information: the date and time the statistics were recorded, map name, host name, average RTT, maximum RTT, minimum RTT, and percent missed. For a description of these statistics, see “The Polling Statistics” on page 111.

The Statistics Log holds the polling data for all of your WhatsUp Gold maps. It holds data starting with either the date you first started monitoring a map, or the date you last cleared the log.

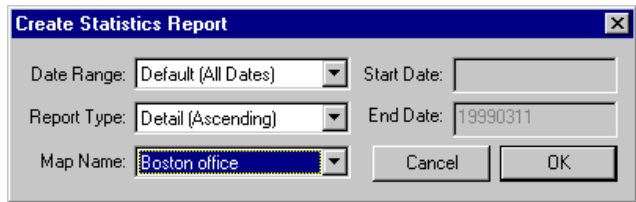
If you use the default time interval of one hour for generating statistics (on the **Statistics Generation** tab of program options), you will see entries for each device recorded one hour apart.

Creating Reports on Polling Statistics

After WhatsUp Gold has monitored a map long enough to generate statistics data, you can create reports based on the statistics.

To create a statistics report:

- 1 From the **Reports** menu, select **Statistics Report**. The Create Statistics Report dialog box appears.
- 2 Select the **Date Range** for the report.



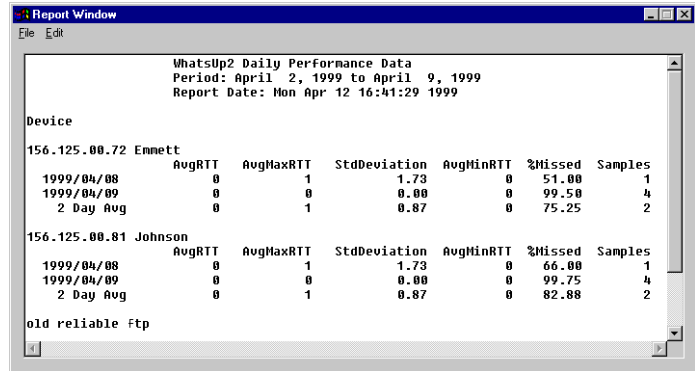
When you select an option, the **Start Date** and **End Date** are shown.

The default includes all days since either the date you started monitoring the map or the date since the statistics were last cleared.

Select **Custom** if you want to enter a **Start Date** and **End Date** for the report. Enter dates in the format *yyyymmdd*, for example: 19991208.

- 3 Select the **Report Type**.
 - Detail.** Report polling statistics for each device and sort by device name in Ascending or Descending order. The reported statistics are calculated from data in the Statistics Log. For definitions of the reported statistics, see “Statistics Report Legend” on page 115.
 - Raw Data.** Save the data from the Statistics Log to a tab-delimited format that can be imported by another application. The data is sorted by device polling order. See “Exporting Raw Data” on page 114.
- 4 Select the **Map Name** of the map for which you want a report.
- 5 Click **OK** to generate the report.

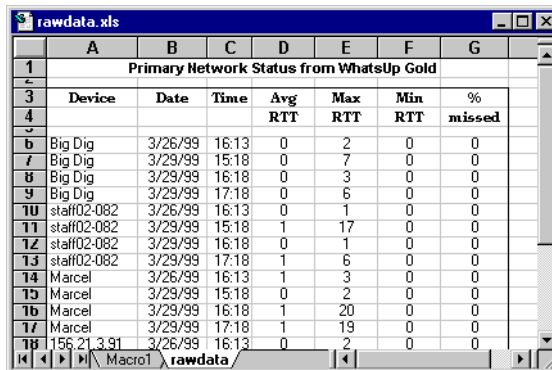
WhatsUp Gold generates the specified report and displays it in the report window. From the report window, you can save the data to a file, print it, or copy data to another application.



If you get the message “insufficient data,” it’s possible that you have not monitored the map long enough to generate polling statistics.

Exporting Raw Data

As mentioned above, you can create a raw data file of the Statistics Report. The tab-delimited raw data file can be imported by another application, for example by a spreadsheet application.



Statistics Report Legend

The values in the statistics report are calculated from the data in the Statistics Log (*wugstats.log*). When you create a statistics report, WhatsUp Gold calculates the average daily values for each device in the selected map; the average daily values are based on the number of data samples in the Statistics Log. Thus, the report shows:

Sample. Number (n) of data samples used to calculate the averages. If you use the default for statistics generation (one hour), then if the map was monitored for all 24 hours of the day, you will have 24 samples.

Average RTT. The arithmetic mean of n samples of Round Trip Time (RTT).

Average Maximum RTT. The arithmetic mean of n samples of Maximum RTT.

Average Standard Deviation. The standard deviation of the RTT values.

Average Minimum RTT. The arithmetic mean of n samples of Minimum RTT.

Average Percentage of Missed Polls. The arithmetic mean of n samples of the percentage of missed polls.

Using the Command Line for Statistics Reports

Wugstat.exe is a WhatsUp Gold utility used to generate reports from WhatsUp Gold Statistics Log (*wugstats.log*) data.

You can invoke *wugstat* from the Command Prompt or MS-DOS prompt. You must invoke *wugstat* with the *-mmapname* argument. All other arguments are optional. By default, the report is displayed in the Command Prompt or MS-DOS window.

Basic Command Syntax

```
wugstat -mmapname [-syyyymmdd] [-eyyyyymmdd] [-llogfile]
[-osortmode] [-rreport] [-tmaptitle]
```

Note

You must use the `-m` argument to specify the name of the WhatsUp Gold map to use for the report. All other arguments are optional.

Argument	Explanation
<code>-mmapname</code>	The mapname must include the full path. The path and name must be enclosed in quotes. For example, <code>wugrpt -m"C:\pgms\whatsup\network1.wup"</code>
<code>-syyyymmdd</code>	Use <code>-s</code> to specify the start date for the report. The default is the oldest date in the log.
<code>-eyyyyymmdd</code>	Use <code>-e</code> to specify the end date for the report. The default is the most recent date in the log.
<code>-logfile</code>	Use <code>-l</code> to specify an alternate log file. The default is <code>wugstats.log</code> .
<code>-osortmode</code>	Use <code>-o</code> to specify one of the sort modes: <i>Ascend</i> sorts by device name in ascending order (this is the default value); <i>Descend</i> sorts by device name in descending order.
<code>-rreport</code>	Use <code>-r</code> to specify one of the report types: <i>Detail</i> generates a detailed report that lists AvgRTT, MaxRTT, MinRTT, and % Missed Polls by device; <i>Export</i> generates a tab delimited file of the raw data.
<code>-tmaptitle</code>	Use <code>-t</code> to specify the title to use at the top of the report. The default title is the map name.
<code>-?</code>	Use <code>-?</code> to see a summary of argument options.

Examples

The following examples create statistics reports for the *Boston1* map:

```
wugstat -m"C:\Program Files\whatsup\Boston1.wup"
```

Generates a detail report for all days in the log (uses defaults).

```
wugstat -m"C:\Program Files\whatsup\Boston1.wup"  
-s19990301 -e19990131
```

Generates a detail report for one month of log data.

Return Codes

Wugstat returns 1 if it performed at least one of the requested operations; it returns 0 if it failed.

Creating Performance Graphs

You can graph the polling statistics that WhatsUp Gold accumulates for the devices on your network. The graphs show performance for a device by plotting the average time it takes a device to respond to a poll, known as the round trip time (RTT). In addition, the Performance Graphs can show aggregate data, such as the devices with the best and worst availability, or the devices with the highest and lowest average missed polls, and the best and worst days of the week for network performance.

High values for response time (RTT) indicate poor performance, low values indicate good performance, and low values for missed polls indicate high availability.

Graphs are based on data in the *wugstats.log*. For information about this log, see “Logging and Reporting Polling Statistics” on page 111.

Note

If **Performance Graphs** in the **Reports** menu is grayed out, you need to install Microsoft's ODBC and the ODBC text driver. To install ODBC, see see “System Requirements” on page 6.

Graph Options

When you create a Performance Graph, you can choose:

- the time interval for which you want to see statistics: daily, weekly, monthly, or all observations in the log
- in some cases, the graph format: bar chart or area chart
- how you want to sort the data: by device name; in ascending or descending order
- which maps and which devices to include in a graph

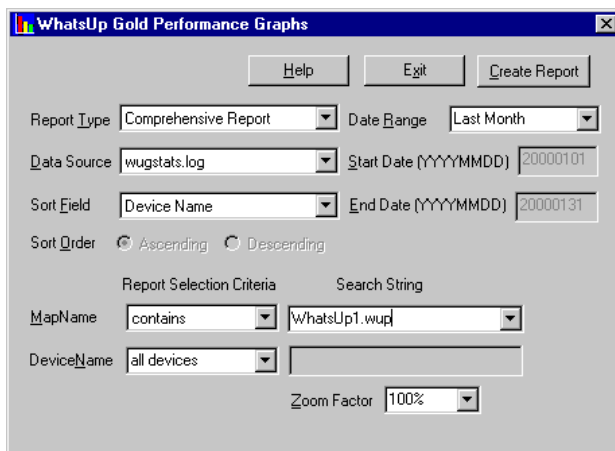
All graphs show both aggregate performance data for the selected time period and the data for each device.

Creating a Graph

To create a graph:

- 1 Start the Performance Graphs tool by doing one of the following:
 - From the **Reports** menu, select **Performance Graphs**.
 - From the **Start** menu, select **WhatsUp -> WhatsUp Gold -> WhatsUp Gold Performance Graphs**.

The WhatsUp Gold Performance Graphs dialog box appears.



- 2 Select the **Report Type** to set which performance data you will view and the format of the graph. To see examples of graphs, see “Sample Performance Graphs” on page 121.

Comprehensive Report. Shows devices by average response time for the selected period. This includes slowest devices; slowest dates for overall response time (all devices); and slowest days of the week for overall response time (all devices). Within the report, you can select a device to show its own graph.

Daily (Line Chart). Shows the aggregated Average, Maximum, and Minimum RTT values for the selected devices by date recorded. Within the report, you can select a device to show its own graph.

Day of the Week (Area Chart or Bar Chart). Shows the aggregated Average, Maximum, and Minimum RTT values for the selected devices by the day of the week. For example, the

averages for Monday, the averages for Tuesday, etc. This graph can be shown as an Area Chart or Bar Chart. Within the report, you can select a device to show its own graph.

Monthly (Area Chart or Bar Chart). Shows the aggregated Average, Maximum, and Minimum RTT values for the selected devices by month. For example, the averages for January, the averages for February, etc. This graph can be shown as an Area Chart or Bar Chart. Within the report, you can select a device to show its own graph.

Daily Text Report. Shows a daily average for the each of the statistics per device. You can select the devices and the period for which you want to display data.

Availability Report. Shows the availability of devices based on average missed polls. This includes the best and worst availability over the selected period; best and worst dates for overall availability (all devices); best days of the week for overall availability (all devices). Within the report, you can select a device to show its own graph.

- 3 Select the **Date Range** for the report. When you select an option, the **Start Date** and **End Date** are shown.

The default includes all days since you started monitoring the map, or since the statistics were last cleared by clicking **Clear** in the Statistics Log or by clearing the log from the web interface.

Select **Custom** if to enter a **Start** and **End Date** for the report. Enter dates in the format `yyyymmdd`, for example: 20000208.

- 4 The **Data Source** box shows `wugstats.log` as the default value. Current statistics are always logged to `wugstats.log`. To archive statistics, you can copy the current statistics to a different file name — as long as the file is in the WhatsUp top directory and its name starts with `wugstats`, it will appear in the **Data Source** drop-down list.
- 5 The **Sort Field** box shows that the performance data is sorted by the device name, in alphabetical order. You can select to sort in **Ascending** or **Descending** order for all reports (except the Comprehensive Report).
- 6 Enter the Report Selection Criteria to determine which maps and which devices to include in the graph.

The default values graph performance data for all maps and all devices for which there is data in *wugstats.log*. You can change the criteria to graph performance data for any combination of maps and devices.

MapName. Use *All maps* to graph all data. To choose from a list of your maps, select contains, and then select a map name from the **Search String** box. You can also select the search expression (such as contains, is like), and then enter the search text (such as a map name or partial map name) in the **Search String** box. (See “Using Search Expressions” below.)

DeviceName. Select **All devices** or select the search expression (such as contains, is like), and then enter the search text (such as a device name or partial device name) in the box to the right. (See “Using Search Expressions” below.)

- 7 Use **Zoom Factor** to change the view size of the report.
- 8 Click **Create Report**. You may have to wait a few seconds for the report to appear, depending on the number of devices included in the report. For examples of graphs, see “Sample Performance Graphs” on page 121.

Using Search Expressions

When setting which maps and devices to include in a report, you can specify a search expression accompanied by search text.

The following table lists the search expressions you can use:

all maps or all devices	Include all maps or all devices
contains	Include maps (or devices) that contain the search string; or select a map from the drop-down list in the Search String box
does not contain	Exclude maps (or devices) that contain the search string
is like	Include maps (or devices) that match characters in the search string: ? = one character; * = many characters
starts with	Include maps (or devices) that start with the search text
does not start with	Exclude maps (or devices) that start with the search text

Search String. To enter the **Search String**, enter the literal text that you want to search for. For example, if you want to report on a device named wks120, type: `wks120`

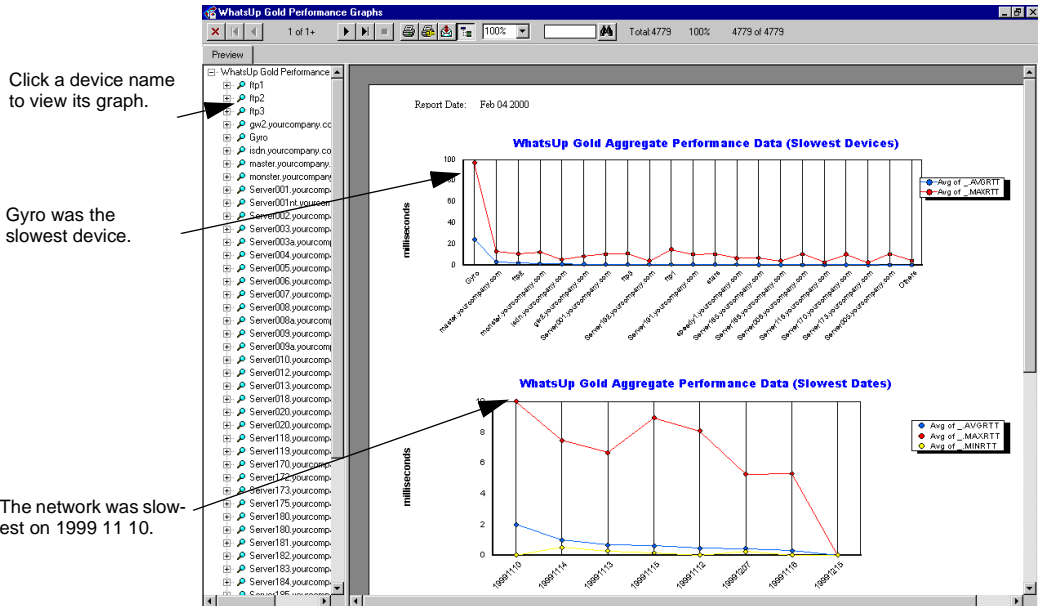
If you use the *is like* expression, you can use `?` or `*` in the **Search String**. For example:

`wks?` - finds wks1, wks 2, wks9; but does not find wks10, wks11, wks120

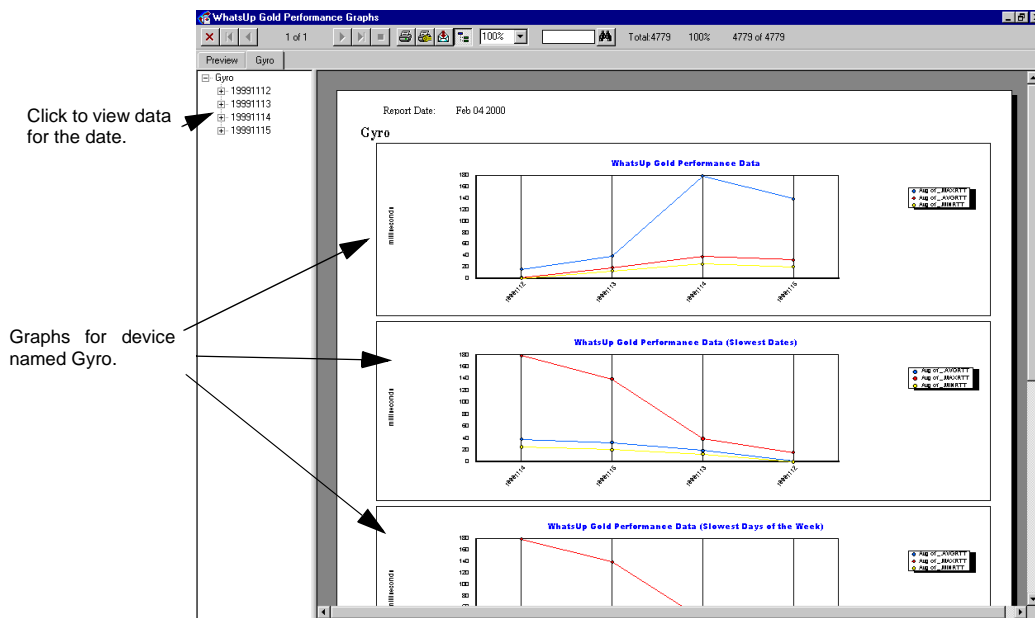
`wks*` - finds wks1, wks10,wks120

Sample Performance Graphs

The following example shows a Comprehensive Report for all devices in a map.



You can click a device name in the left panel to see the graph for that device, as shown in the following example.



Viewing, Printing, and Exporting Performance Graphs

When you create a performance graph, it appears in the graph viewer. If there are graphs of the aggregated values for all devices, these graphs appear on the first pages of the report. The remaining pages of the report show graphs of individual devices. The exception is the Daily Text Report, which shows formatted text and does not contain graphs.

Device list. The left frame of the report viewer lists the devices in the report, by host name or IP address. To display the graph for a device, click on a device in the left frame.

Tool Bar. Use the buttons in the tool bar to navigate or print the report, export report data to another format, or change the report display.



Printing Graphs

To print a graph, click the **Print** icon in the tool bar and enter your print options. To change the default printer, click the **Print Setup** icon in the toolbar.

Exporting Graphs

You can export the currently displayed graph to a variety of formats, including HTML. To export a graph:

- 1 Click the **Export** icon in the toolbar. The Export dialog box appears.
- 2 Select a **Format**. Select HTML, text, RTF, or a specific application's format.
- 3 Select a **Destination**.
- 4 Click **OK**.

You can view the exported graph in a tool that supports the selected format.

Using the Command Line for Performance Graphs

Cstatrpt.exe is a utility that can generate graphs from the Statistics Log (wugstats.log) data. You can invoke *cstatrpt* from the Windows Command Prompt (MS-DOS prompt). By default, the report is displayed in the Performance Graphs interface. The -x (for Export) argument is the only non-interactive mode (meaning no dialog boxes are displayed). The -x option creates a Performance Graph in HTML format, which you can display in a browser.

Basic Command Syntax

```
cstattrpt [-mmapname] [-ddevicename] [-Ddateopt][-syyyymmdd] [-eyyyymmdd] [-llogfile] [-osortmode] [-rreport] [-x]
```

Argument	Explanation
<i>-mmapname</i>	The mapname must include the full path. For example, wugrpt -mC:\pgms\whatsup\network1.wup You can enter a complete map name, or enter a partial name. For example, -mnetwork will include network1, network2, network3, etc.
<i>-ddevicename</i>	Use -d to specify the name of a device on which to base the report. You can enter a complete device name, or a partial name to include all devices that match the partial name. For example -dWKS will include WKS1, WKS2, WKS3, etc.
<i>-Ddateopt</i>	Use -D to specify a recurring time period: wtd - Current week to date lastw - Last week mtd - Month to date lastm - Last month
<i>-syyyymmdd</i>	Use -s to specify the start date for the report. The default is the oldest date in the log.
<i>-eyyyymmdd</i>	Use -e to specify the end date for the report. The default is the most recent date in the log.
<i>-llogfile</i>	Use -l to specify an alternate log file. The default is <i>wugstats.log</i> .
<i>-osortmode</i>	Use -o to specify one of the sort modes: <i>Ascend</i> sorts by device name in ascending order (this is the default value); <i>Descend</i> sorts by device name in descending order.
<i>-rreport</i>	Use -r to specify one of the report types: Wugstatal.rpt - Comprehensive Report Wugstatdaily.rpt - Daily (Line Chart) Wugstatdow.rpt - Day of the Week (Area Chart) Wugstatdowbar.rpt - Day of the Week (Bar Chart) Wugstatmoy.rpt - Monthly (Area Chart) Wugstatmoybar.rpt - Monthly (Bar Chart) Wugstatdailytext.rpt - Daily Text Report Wugstatavail.rpt - Availability Report
<i>-x</i>	Use -x to export the report specified by -r to an HTML file, without running the graphical user interface. The exported file(s) is placed in the Web\reporttype folder under the WhatsUp top directory.
<i>-?</i>	Use -? to see a summary of argument options.

Examples

The following examples create performance graphs for the Boston1 map:

Example 1.

```
cstatrpt -mC:\ProgramFiles\  
                                whatsup\Boston1.wup
```

generates a Comprehensive report for all devices in the Boston1 map for all days in the log (uses defaults, except for the map name).

Example 2.

```
cstatrpt -mC:\Program Files\whatsup\  
        Boston1.wup -rwugstatdaily.rpt -Dlastm -x
```

generates a daily report for all devices in the Boston1 map using the last month of log data, and exports the graphs to HTML format (does not display the Performance Graphs interface).

Sending Recurring Status Reports

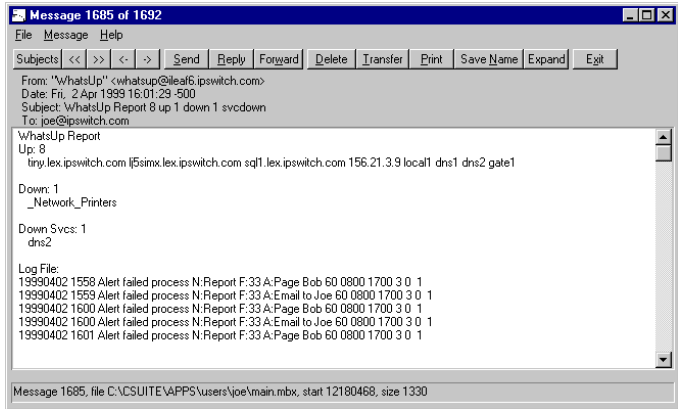
WhatsUp Gold can send a recurring network status report as a beeper, pager, or e-mail message.

The Recurring Report provides snapshot of your network status and can include:

- The count and names of devices that are up
- The count and names of devices that are down
- Names of devices that have a service down
- The most recent lines from the Event Log

You can set options to send the report at a specified interval. This report lets you receive up-to-date status reports at a remote site, so you can be assured the network is running smoothly, or so you can be quickly apprised of any problems.

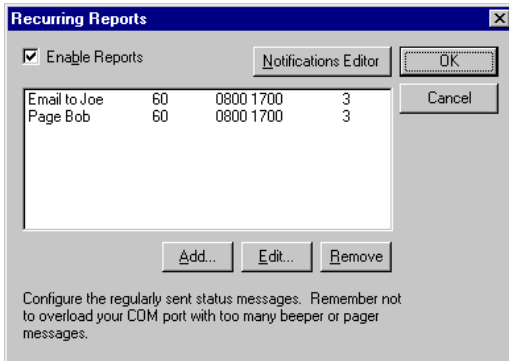
The following example shows a Recurring Report sent via e-mail:



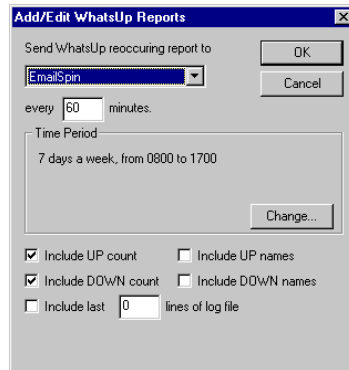
To set up a Recurring Report:

- 1 From the **Reports** menu, select **Recurring Reports**. The Recurring Reports dialog box appears.
- 2 Select **Enable Reports**.

You see the following dialog box:



- 3 Click **Add**. The Add/Edit WhatsUp Reports dialog box appears.



- 4 Select a notification from the drop-down list.

For example, if you defined a notification that sends e-mail to the network administrator, you can select that notification from the drop-down list. For information on defining a notification, see “Chapter 3: Setting Up Notifications” on page 53.

- 5 Enter how often (in minutes) you want to send the report.
- 6 Select the **Time Period** when you would like to receive the report. Click **Change** to change the default setting of 7 days a week, 24 hours a day.

Select the **Day of Week** options: **7 days a week** is the default. You can clear the **7 days a week** option and then select the specific days of the week.

Select one of the three **Time of Day** options:

- Use **24 hours a day** to set the period to all day.
- Use **Between** to set the start and end time.
- Use **Not between** to set the hours that reporting is turned off.

Note

When using **Between** and **Not Between**, the start time must be less than the end time. To set a period between an AM time and a PM time, you must use the 24 hour clock (0000 to 2400) or use the options together to set the hours.

To receive a report at a specific time every day, enter the start time and the time plus one minute as the end time. For example, enter 0600 and 0601 in the boxes for the *Not between* option.

- 7 Check any other options you want to use. You can use the following options for pager and e-mail notifications, but not for beeper notifications.

Include UP count. Report the number of up devices.

Include UP names. Report the names of the up devices.

Include DOWN count. Report the number of down devices.

Include DOWN names. Report the names of the down devices.

For mail notifications, you can also specify the following option:

Include last n lines of log file. Check the box and enter the number of lines from the Event Log (the most recently recorded lines) that you want to include in the report.

For beeper notifications, you must use the following option to send a report message:

Message format. You can begin the message with 99 (or any numeric character) to identify to the beeper user that this is a message from WhatsUp Gold. The message must contain three %u characters, which denote the following: the first %u = number of up devices, the second %u = number of down devices, the third %u = number of up devices that have services down.

No other message variables (% characters) are allowed. You can use an asterisk (*), which prints on most beepers as a dash (-) to separate characters in the message. An example of the beeper message is: 99*%u*%u*%u*

- 8 Click **OK** to save the new notification and close the Add/Edit WhatsUp Reports dialog box.

The new notification appears in the Recurring Reports dialog box.

- 9 Click **OK** to save the changes and close the dialog box.

Chapter 7: Working from a Web Browser

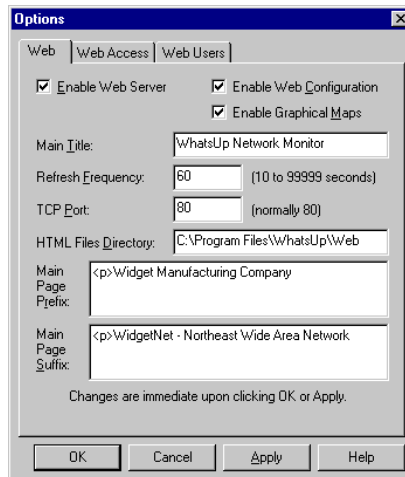
This chapter describes how to set up the WhatsUp Gold web server and use a web browser to access mapping, monitoring, and notification functions from a remote computer.

Setting Up the WhatsUp Gold Web Server

WhatsUp Gold provides a web server that lets you use any web browser on any computer on the Internet to view the status of your network and change WhatsUp Gold settings. You can enable/disable the web server and set access to this server through the web properties. If you run WhatsUp Gold as a Windows NT service (see “Running WhatsUp Gold as an NT Service” on page 11), the web browser will be your primary interface.

To set up the web server:

- 1 From the **Options** menu, select **Web Server**, and click the **Web** tab to display the setup properties.



- 2 Make sure the **Enable Web Server** option is checked.
- 3 If you want web users to be able to change WhatsUp Gold settings from the web interface, make sure **Enable Web Configuration** is checked.

You can set access for each web user account (see “Setting Web Access” in this chapter). If **Enable Web Configuration** is not checked, the web users cannot change any WhatsUp Gold settings; they can use only the view functions.

- 4 There are two formats for displaying maps in a web browser: Graphical maps, which use JPEG format to display the same icons and colors as maps on the console; or a Text listing of devices in a map. To view the Graphical maps, turn on **Enable Graphical Maps**.

- 5 Enter or change any of the setup information.

Main Title. The title displayed on the main web page (“Top View”) for the WhatsUp Gold web site. You can enter any text for the title.

Refresh Frequency. The number of seconds between updates to the WhatsUp Gold display on the web site. You can set the refresh rate in the range from 10 to 99999 seconds.

TCP Port. The default is port 80, which is the standard TCP/IP port for a web (HTTP) server. If you already have a web server running on this system, set the port number in this box to another port number (for example, 8000).

- 6 Click **Apply** to apply changes immediately.

You can add your own web pages and add information to the main page (“Top View”) by using the **HTML Files Directory**, **Main Page Prefix** and **Main Page Suffix** options. You can also use the WhatsUp Gold web server to serve your own web pages. See ‘Customizing Your WhatsUp Gold Web Site’ below.

Customizing Your WhatsUp Gold Web Site

You can customize your WhatsUp Gold web site as follows:

- Add your own web pages to the site.
- Display information at the top or bottom of the main page (“Top View”), which appears after a successful logon.

To do either of these customizations:

- 1 From the **Options** menu, select **Web Server** to display the setup properties.

- 2 Use the following options to add information to the web site.

HTML Files Directory. If you want the WhatsUp Gold web server to serve your own web pages, you can add any HTML files to this directory. The default is the *\Web* subdirectory of the directory in which you installed WhatsUp Gold. If you use a different directory, you need to specify the full path to the directory in this text box. Subdirectories to this directory are also supported.

Note

The Help files for the web interface (*.htm) are installed in the *\Web* directory. If you change the default HTML Files Directory, you should move the Help files into the new directory.

To open a web page, in your browser's address field, enter the host name of the system on which WhatsUp Gold is installed, and the file name for the web page. For example, assuming the web server is running on the default HTTP port 80, you might enter:

http://gyro.ipswitch.com/whatsup/webdir/page1.htm.

Note

Do not place a file named *default.htm* in this directory because WhatsUp Gold uses this name to activate the web server.

Main Page Prefix. Enter a message to be displayed at the top of the main web page ("Top View"). You can enter up to 100 characters of plain text and/or HTML code in this edit box. The HTML begin and end tags (<HTML> and </HTML>) are automatically added to any HTML code you enter.

Right-click in this edit box to access the standard Windows cut, copy, paste, and delete functions.

Main Page Suffix. Enter a message to be displayed at the bottom of the main web page ("Top View"). You can enter up to 100 characters of plain text and/or HTML code in this edit box. The HTML begin and end tags (<HTML> and </HTML>) are automatically added to any HTML code you enter.

Right-click in this edit box to access the standard Windows cut, copy, paste, and delete functions.

Note

Within the Main Page Prefix or Suffix, you can create a link to other web pages, such as a page that lists phone contacts for network operations. These additional web pages must be stored in the HTML Files Directory.

- 3 Click **OK** to apply your changes. The changes take effect immediately.

The following example shows the main web page with prefix and suffix information displayed:

Main Title → **WidgetNet Network Monitor**

Main Page Prefix → Widget Manufacturing Company

Map	Items Up	Items Down	Services Down	
Schenectady	6	1	0	Setmap
Boston office	12	0	0	New Map
London Office	25	0	0	Load Map
Worldwide Widget	9	1	0	Unload Map

Main Page Suffix → WidgetNet - Northeast Wide Area Network

1999/04/05 15:01

Making Maps Available for Web Viewing

Any network maps that are open in WhatsUp Gold can be viewed from a web browser. In addition, web users with **Configure program** permission can load any maps in the map directory on the system where WhatsUp Gold is installed. There are two ways to set the map directory:

- From the WhatsUp Gold console, select **Program** from the **Options** menu, click the **Startup** tab to display the Startup options. In the **Directory** box, enter the full path for the directory that contains the network maps.
- From a web browser, log on to the WhatsUp Gold web server. The web site main page (“Top View”) appears. Select **Settings** to display the program settings. In the **Startup Map Directory** box, enter the path for the directory that contains the network maps.

You must restart WhatsUp Gold for the change to take effect.

Setting Web Server Access

There are two ways that you can set access to the web server. You can use either one or both together:

- Require a user ID and password to view page on the WhatsUp Gold web site. This includes setting the pages and functions that the user can access.
- Specify an IP address or set of IP addresses that are either granted access to the web site or are denied access.

Default User Accounts for the Web Server

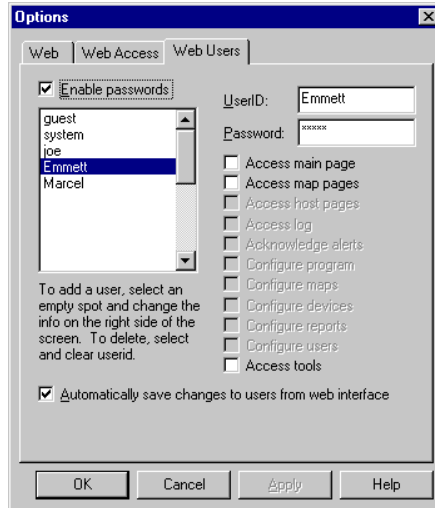
WhatsUp Gold provides two default user IDs for accessing the web server:

- The user ID *system* with password *system* has full access to WhatsUp Gold pages and functions, with the exception that they cannot set up or change web user accounts.
- The user ID *guest* with no password has access to all WhatsUp Gold pages but cannot change any WhatsUp Gold settings. If a user enters any user ID with no password, they will be logged on to the *guest* account. If you do not want users to access the web server in this way, then you should disable the permissions for the *guest* account.

Setting Up User Accounts for the Web Server

You can add up to 20 user accounts for web access to WhatsUp Gold and you can assign different levels of access to each user.

- 1 From the **Options** menu, select **Web Server** and click the **Web Users** tab to display the user access properties.



- 2 Select the **Enable passwords** option (make sure it is checked). If this option is not selected, web users can log on without specifying a password.
- 3 Click an empty slot in the list of users, then enter a user ID and password for the new account.

The first slot is always the default *guest* account, which does not require a password. You cannot remove this account, but you can change the permissions assigned to the account.
- 4 Select the WhatsUp Gold web pages and the web functions that you want the user to have.

Note

For more information about the WhatsUp Gold views and functions available from the web server, see “WhatsUp Gold Web Display” on page 139

Access main page. The user can view a list of active maps with Items Up, Items Down, and Services Down reported for each map. When this option is not checked, you cannot assign the **Configure program**, **Configure reports**, or **Configure users** functions to a user.

Access map pages. The user can click a map title (in the main page or “Top View”) to view the network map in a table format. The user can also view a summary of polling statistics and services for the map. When this option is not selected, you cannot give the user access to the device pages or logs, or to the **Configure maps** or **Configure hosts** functions.

Access host pages. The user can click a device name (in the map page) to view a detailed summary of activity for that device. When this option is not selected, you cannot give the user access to the **Configure hosts** function.

Access log. The user can view the log of WhatsUp Gold events.

Acknowledge alerts. Lets the user acknowledge a change and stop further alerts for the device(s).

Configure programs. Lets the user change program settings, create a new map, load and unload maps, and create, edit, and assign notifications.

Configure maps. Lets the user change map settings, reset counters for all devices, and add and remove devices.

Configure devices. Lets the user change host settings; reset counters for individual devices; configure service monitoring; and add, edit, and remove alerts.

Configure reports. Lets the user add, edit, and delete report notifications.

Configure users. Lets the user add, edit, and delete web user accounts.

Access tools. Lets the user access and use the Ping and Traceroute tools.

- 5 If you want changes made from the web interface (by any web users) to be saved in the WhatsUp Gold application, select **Automatically save changes to users from web interface**. If this option is not selected, any changes made from the web interface will last only for the duration of the web session.
- 6 Click **Apply** to save your changes.

When a user opens the WhatsUp Gold web pages, they will be prompted to enter the logon user ID and password before they can view the pages.

Note

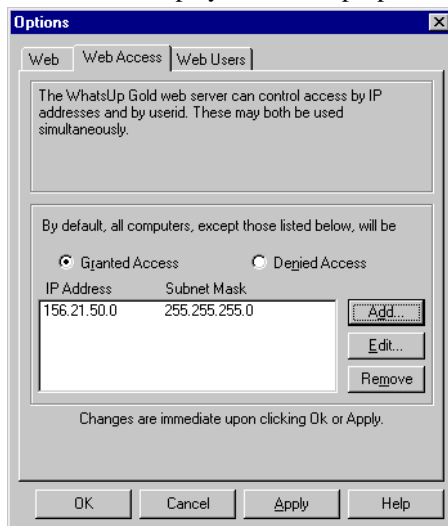
You can disable access to the configuration functions for all WhatsUp Gold web users, thus overriding the settings for each individual user. To do this, from the **Option** menu, select **Web Server**, click the **Web** tab, and then turn off the **Enable Web Configuration** option.

Setting Web Access by IP Address

You can specify a list of IP addresses to be granted or denied access to the WhatsUp Gold web pages.

To deny access to a specific computer or group of computers:

- 1 From the **Options** menu, select **Web Server** and click the **Web Access** tab to display the access properties.



- 2 Select **Granted Access**.
- 3 Click **Add**. The "Deny Access On" dialog box appears.
- 4 In the **IP Address** box, enter the IP address of the computer to be denied access to the WhatsUp Gold site.

To deny access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you enter 156.21.50.0 and a subnet mask of 255.255.255.0, all IP addresses in the range 156.21.50.1 through 156.21.1.254 will be denied access.

- 5 Click **OK** to add the IP address(es) to the list. Access will be granted to all computers except those listed.
- 6 On the **Web Access** tab, click **Apply** to save the changes.

To grant access to a specific computer or group of computers:

- 1 On the **Web Access** tab, select **Denied Access**.
- 2 Click **Add**. The “Grant Access On” dialog box appears.
- 3 In the **IP Address** box, enter the IP address of the computer to be granted access to the WhatsUp Gold site.

To grant access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you enter 156.21.50.0 and a subnet mask of 255.255.255.0, all IP addresses in the range 156.21.50.1 through 156.21.50.254 will be granted access.

- 4 Click **OK** to add the IP address(es) to the list. Access will be denied to all computers except those listed.
- 5 On the **Web Access** tab, click **Apply** to save the changes.

If the **Enable passwords** option (on the **Web Users** tab) is selected, when a user logs on from a valid IP address, they are prompted to enter the logon user ID and password before they can view the specified pages.

On the **Web Access** tab, to edit a web access address, select the IP address in the list, then click **Edit** to display properties, and then enter any changes. To remove an address from either list, select the address and click **Remove**.

Logging On to the Web Server

The web server is assigned a web address that can be used to open the WhatsUp Gold web page from any browser. This web address consists of the host name of the system on which WhatsUp Gold is installed, and the web server port number. The default port number is 80.

To log on to the web server:

- 1 Open any browser on your network and enter your WhatsUp Gold web address in the **Address (or URL:)** box. For example, if your WhatsUp Gold system is named *monitor1.ipswitch.com*, then the web address will be: `http://monitor1.ipswitch.com:80`

Note

You can save your WhatsUp Gold web address as a “favorite” or “bookmark” site in your browser.

After connecting, the logon dialog box appears.

- 2 Enter the user ID and password for your WhatsUp Gold web account. You may not have to enter a password, depending on how your WhatsUp Gold administrator set up access to the web server.

The main page (“Top View”) for the WhatsUp Gold web server appears. You can use the views and functions provided to your web user account.

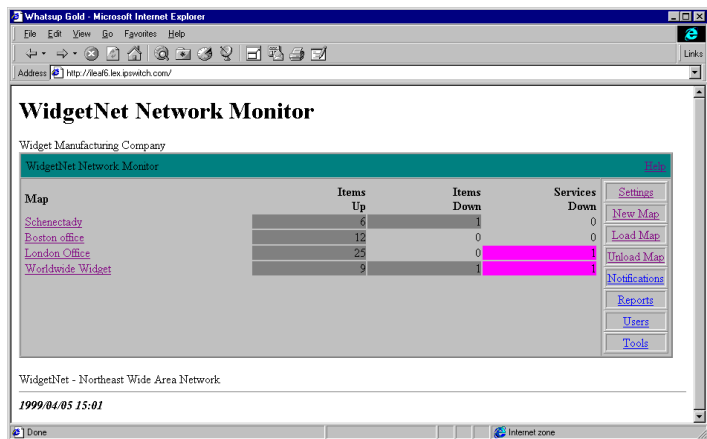
If your attempt to connect to the web server is denied, make sure the following have been done:

- Your WhatsUp Gold administrator has set up access to the web server for you.
- The **Enable Web Server** option in **Options -> Web Server -> Web** is selected.
- Your computer’s IP address is allowed access on the **Web Access** tab (**Options -> Web Server -> Web Access**).

WhatsUp Gold Web Display

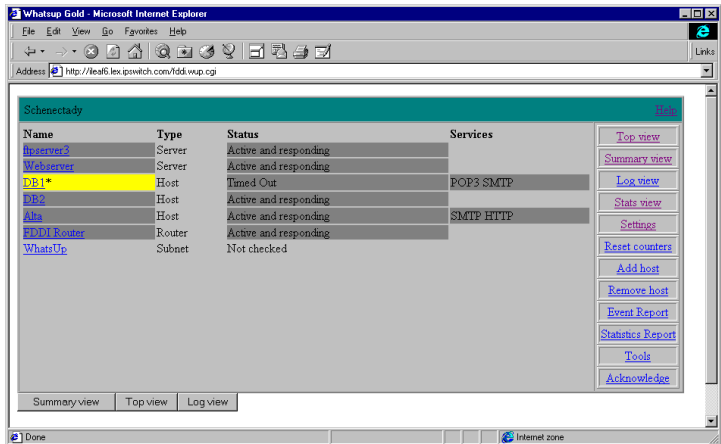
After logging on to the WhatsUp Gold web site, you can use the following web pages (depending on your permissions): Top View page, Map View pages, Device View pages, Summary View pages, and the Events Log. This section briefly describes the views available from a web browser. Refer to the WhatsUp Gold web monitor's help system for detailed information.

Top View. The Top View page is displayed after you log on. It lists each active network map by map title (the title is set in Map Properties). You can click a map title to display the map page for that network.

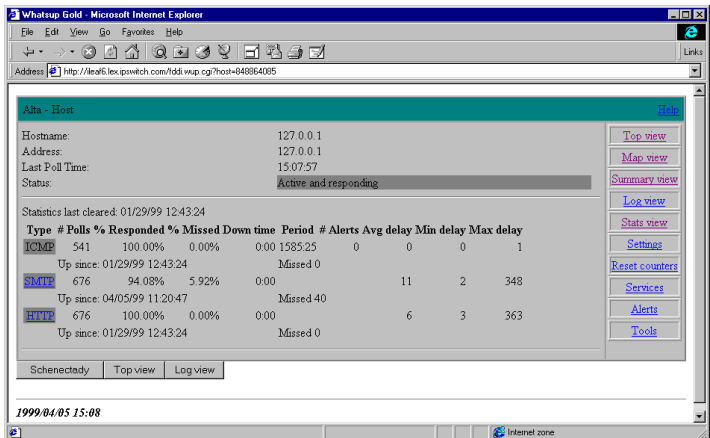


Map View. Click a map name in the Top View to display the Map View. There are two formats for displaying maps in a web browser: Graphical maps, which use the same icons and colors as maps on the console; or a Text listing of devices in a map. To view the Graphical maps, turn on **Enable Graphical Maps** in the **Web** tab.

Any services being monitored on a device are shown. The Map View will show any alerts that occur for devices in the map and will play an audible alarm (if your computer has a sound card). You can click Acknowledge to acknowledge the alert and turn off an alarm.



Device View. Click any device in the list to show its Device View. The Device View lists the host name, IP address, and polling statistics for the device. The polling statistics are the same as those displayed in the Statistics Window in the WhatsUp Gold application.



Summary View. The Summary View lists all devices in the selected network map and shows the polling statistics for each device.

Name	Type	# Polls	% Responded	% Missed	Down time	Period	# Alerts	Avg delay	Min delay	Max delay
192.168.1.1	ICMP	546	100.00%	0.00%	0:00	1585:27	0	0	0	1
192.168.1.2	ICMP	546	100.00%	0.00%	0:00	1585:27	0	0	0	1
192.168.1.3	ICMP	546	0.73%	99.27%	9:02	1585:27	0	0	9999	0
192.168.1.4	POP3	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.5	SMTP	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.6	ICMP	542	100.00%	0.00%	0:00	1585:26	0	0	0	1
192.168.1.7	ICMP	542	100.00%	0.00%	0:00	1585:26	0	0	0	1
192.168.1.8	SMTP	677	94.09%	5.91%	0:00	0:00	11	2	348	0
192.168.1.9	SMTP	677	100.00%	0.00%	0:00	0:00	6	3	363	0
192.168.1.10	ICMP	542	99.82%	0.18%	0:01	1585:26	0	0	0	1
192.168.1.11	ICMP	37	2.70%	97.30%	0:36	10901:46	0	0	0	0
192.168.1.12	DNS	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.13	FTP	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.14	SSH	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.15	SMTP	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.16	Time	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.17	Time	0	100.00%	0.00%	0:00	0:00	0	0	0	0
192.168.1.18	SNMP	0	100.00%	0.00%	0:00	0:00	0	0	0	0

Log View. You can click the **Log View** button to view the **Event Log page**. The Event Log page shows all events that have been logged for the devices in a network map.

WhatsUp Gold Web Functions

This section briefly describes the WhatsUp Gold functions available from a web browser. Refer to the WhatsUp Gold web monitor's help system for detailed information.

The functions available to each user are determined by the permissions granted to the user account. For information on setting up web accounts, see "Setting Up User Accounts for the Web Server" on page 133

Configure program. Configure the startup settings for WhatsUp Gold and the display settings for the WhatsUp Gold web pages.

Configure maps. Change settings for a selected map, such as map title, poll timer, and timeout.

Configure devices. Change the settings for a device, such as the display name, host name, IP address, polling frequency, polling schedule, and up and down dependencies.

Configure reports. Configure the recurring network status report. This report provides a snapshot of your network's status (including Up and Down devices and down services) and can be sent via e-mail, pager, or beeper notification.

Configure users. Add, remove, and change WhatsUp Gold web user accounts.

Acknowledge alerts. Acknowledge a reported change (alert) and stop any further alerts for the change.

Access tools. Use the Ping, Trace, Lookup, and Scan tools. These tools operate from the system on which the WhatsUp Gold application is installed. For example, when you do a "trace" from the web interface, you are tracing the route from the WhatsUp Gold system to a remote system.

Chapter 8: Monitoring SNMP Devices

The Simple Network Management Protocol (SNMP) is an Internet standard that allows management data on different network devices to be read and monitored by an application. You can use WhatsUp Gold to view and monitor SNMP objects on any device that implements an SNMP agent.

This chapter describes how WhatsUp Gold implements SNMP, how to view and monitor SNMP values for a networked device, and how WhatsUp Gold can receive unsolicited messages (known as traps) from an SNMP device.

SNMP Implementation in WhatsUp Gold

This section provides an overview of the SNMP monitoring functions available in WhatsUp Gold. It assumes you are familiar with the SNMP standard and Management Information Base (MIB) for SNMP objects. For background information on SNMP and the MIB, see “SNMP Overview” below.

WhatsUp Gold provides limited monitoring of devices that support SNMP. WhatsUp Gold supports the current Internet standards: SNMP Version 1 and MIB II. You can make custom extensions to MIB II to add vendor-provided SNMP objects. For more information, see “Setting Up the MIB Identifiers” on page 148.

Note

WhatsUp Gold does not let you change the value of an SNMP object on a device and does not provide SNMP manager functions.

Use WhatsUp Gold to do the following types of SNMP monitoring:

- View SNMP information on a device.
You can use the SNMP tool (**Net Tools** from the **View** menu, then click the **SNMP** tab) to view information for a device.
- Graph selected SNMP values.
You can graph the SNMP values by using the SNMP Graphing Utility (**Start -> Programs -> WhatsUp Gold -> SNMP Graph Utility** or select **SNMP Graph Utility** from **Tools** menu).

- Receive traps from SNMP devices.

A trap is sent when the status of a device changes. Traps are unsolicited messages, such as a router indicating one of its interfaces went down or a printer indicating it is out of paper.

WhatsUp Gold records traps on the device properties **Log** tab and in the Event Log (provided logging is enabled on the **Alerts** tab in device properties). You can also set WhatsUp Gold to send a notification (via pager, beeper, e-mail, or voice) when a trap is received.

When a trap is recorded for a device, that device's display name will be inverted on the network map (as happens with any change in status). You can then check the **Log** tab in the device properties for the trap information.

- Monitor whether SNMP is running on a device.

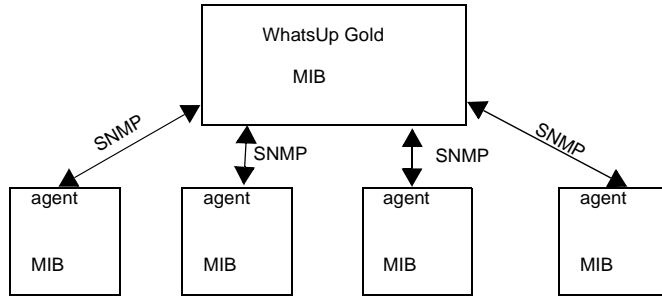
You can select SNMP on the device properties **Services** tab and monitor it just as you can monitor any service. Again, this only checks to see if SNMP is running on the device; no SNMP management is involved.

The following sections describe how to use each of these capabilities.

SNMP Overview

The Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a networked device (a host, gateway, server, etc.). A monitoring or management application on the remote user's system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device can provide information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the Management Information Base (MIB). The MIB defines the SNMP objects that can be managed and the format for each object.



The SNMP protocol, together with the MIB, provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. For a detailed description of SNMP, see Request for Comments (RFC) 1157. For a description of the MIB, see RFC 1213.

Note

The Internet Engineering Task Force (IETF) publishes Requests for Comments (RFCs) for all Internet standards. Each RFC provides a detailed description of the particular standard. View RFCs online at <http://info.internet.isi.edu/in-notes/rfc/>.

Management Information Base (MIB)

The MIB contains the essential objects that make up the “management information” for the device. The Internet TCP/IP MIB, commonly referred to as MIB-II, defines the network objects to be managed for a TCP/IP network and provides a standard format for each object.

This section provides a brief description of the MIB. For a detailed description of the MIB, see RFC 1213.

The MIB is defined as an “object tree” divided into logically related groups of objects. For example, MIB-II contains the following groups of objects:

- system — contains general information about the device, for example: sysDescr (description), sysContact (person responsible), and sysName (device name).

- interfaces — contains information about network interfaces, such as Ethernet adapters, or point-to-point links; for example: ifDescr (name), ifOperStatus (status), ifPhysAddress (physical address), ifInOctets, and ifOutOctets (number of octets received and sent by the interface).
- ip — contains information about the processing of IP packets, such as routing table information: ipRouteDest (the destination), and ipRouteNextHop (the next hop of the route entry).
- Other groups provide information about the operation of a specific protocol, for example, tcp, udp, icmp, snmp, and egp.
- The enterprises group contains vendor specific objects that are extensions to the MIB.

The MIB provides an extensible design to which both public and private objects can be added.

Each object in the MIB has a numeric object identifier and a text name. For example, the system group contains an object named sysDescr, which provides a description of the device. The sysDescr object has the following object identifier:

```
iso   org   dod   internet  mgmt   mib   system  sysDescr
 1     3     6     1         2     1     1       1
```

This object identifier would be 1.3.6.1.2.1.1.1 to which is appended an instance sub-identifier of 0. That is, 1.3.6.1.2.1.1.1.0 identifies the one and only instance of sysDescr.

You will find all of the MIB-II objects (for TCP/IP networks) under the MIB node of tree (so all these objects will have an identifier that starts with 1.3.6.1.2.1).

Security

Limited security is provided for access to a device's data by use of a community profile. The network administrator can assign a community name within the SNMP agent, or manager, on a device. The network management application can access data on the device only if it knows the community name.

Most SNMP agent software (on the device) also let you specify the IP addresses from which the agent will accept requests.

SNMP Agent or Manager

SNMP agent or manager software must be installed and enabled on any devices from which you want to receive SNMP information. Windows NT, Windows 2000, 98, and 95 provide an SNMP agent. Network systems manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

SNMP Operations

An SNMP application can read values for the SNMP objects (for monitoring of devices) and some applications can also change the variables (to provide remote management of devices). Basic SNMP operations include:

- Get — gets a specified SNMP object for a device
- Get next — gets the next object in a table or list
- Set — sets the value of an SNMP object on a device
- Trap — sends a message about an event (that occurs on the device) to the management application

The SNMP agent software on a device listens on port 161 for requests from an SNMP application. The SNMP agent and application communicate using UDP. Trap messages, which are unsolicited messages from a device, are sent to port 162.

If an SNMP application makes a request for information about a device but an SNMP agent is not enabled on the device, the UDP packets are discarded.

SNMP Traps

The SNMP standard provides a limited number of unsolicited messages (called traps) that are sent from a device to an SNMP application. These messages can be sent by the SNMP agent on the device to notify an SNMP application of a change in status.

There are six standard traps which you can receive from any SNMP agent and there can also be enterprise specific traps for a device, which are defined by the device vendor.

Traps are numbered as follows:

Trap #	Trap type	Description
0	Cold start	The device is rebooting itself and may change its configuration or the SNMP agent's configuration.
1	Warm start	The device is rebooting itself but neither the device's nor the SNMP agent's configuration will change.
2	Link down	One of the communication links for the device is down.
3	Link up	One of the communication links for the device is back up.
4	Authorization failure	The device has received a protocol message that is not properly authenticated.
5	EGP neighbor loss	An EGP neighbor for which the device is an EGP peer is down and the peer relationship no longer exists.
6	Enterprise specific traps	The SNMP specification lets vendors define enterprise specific traps, for example a trap that occurs on a particular vendor's router. Enterprise specific traps should be added to the MIB on the device and on the management application.

Setting Up the MIB Identifiers

WhatsUp Gold uses two reference files (*mib.txt* and *traps.txt*) to refer to MIB identifiers. The reference files are used by WhatsUp Gold to display the MIB object tree when you browse for an object name/ identifier using the SNMP tool.

As shipped with WhatsUp Gold, these reference files contain the SNMP objects defined in the MIB-II standard, including the six standard SNMP traps.

If your network includes devices from a vendor who also provides RFC-compliant MIB files, you can update these reference files to include the MIB and trap information from the vendor's files; to do this, you run the MIB Extractor.

The WhatsUp Gold "MIB Extractor" (a command line program named *mibextra.exe*) updates the MIB and trap information that WhatsUp Gold references when it converts SNMP object and trap identifiers into object and trap names, and vice versa.

To run the MIB extractor:

- 1 Collect your vendor-provided MIB files into a single directory
- 2 At the command prompt, enter:

```
mibextra directoryname\filename
```

where *filename* is the name of the vendor-provided file.

The MIB Extractor reads the current contents of *mib.txt* and *traps.txt*, processes the vendor-provided MIB files, and rewrites *mib.txt* and *traps.txt*.

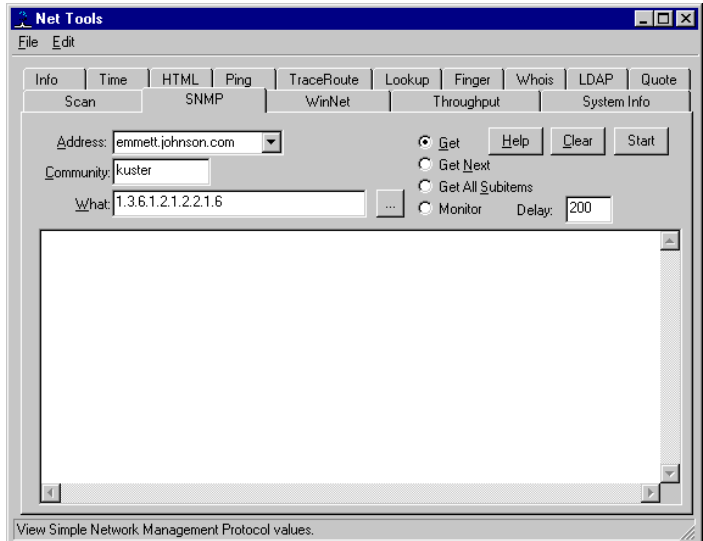
Note

If the MIB Extractor returns a "failed to open file" error, the MIB file you are using has dependencies. These "dependency" files are listed in the Import section of the vendor's mib file. You should check all of the MIB files for dependencies.

Viewing SNMP Objects

The SNMP tool lets you view information on a remote device that has an SNMP agent. To view SNMP information:

- 1 From the **Tools** menu, select **Net Tools**, and click the **SNMP** tab to display the SNMP options.

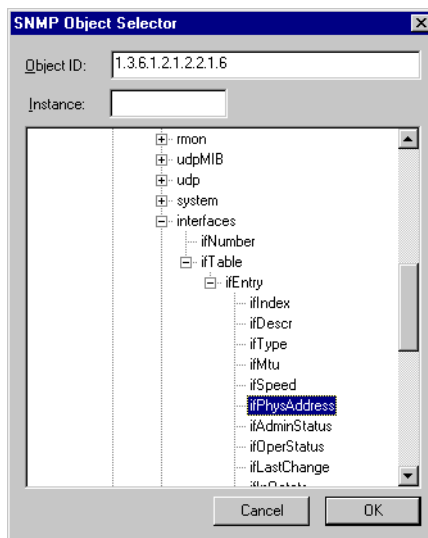


- 2 In the **Address** box, enter the host name or IP address of the device for which you want to view SNMP objects, or select one from the drop-down list.
- 3 If necessary, change the text in the **Community** box. The default string is “public.”

SNMP (Version 1) as a protocol does not support security. Security is implemented within the SNMP manager itself (on the device) by specifying the IP addresses from which it will accept requests. However, simple security can be implemented by use of the community string.

The default string (*public*) will work for most SNMP hosts unless the administrator has specifically removed public and replaced it with a string of his/her own. If you know a device is manageable via SNMP and “public” doesn’t work, you will have to talk to the owner of that device to get a community name that will work.

- 4 In the **What** box, type an SNMP object name or identifier to retrieve, or click the button next to the **What** box to displays the MIB tree view of the SNMP objects.



Each SNMP object has a name and numeric identifier. For example, in the “system” group, the network object named *SysDescr* with object identifier 1.3.6.1.2.1.1.1 contains a description of the device.

An object can have one or more instances, depending on the configuration of the monitored device. For example, a device can have two network adapters, in which case there will be two instances of the *ifPhysAddress* object, which has object identifier 1.3.6.1.2.1.2.2.1.6. In this case, you need to specify an instance number at the end of the object identifier (such as 1.3.6.1.2.1.2.2.1.6.1). If you do not specify an instance number, it defaults to zero. For more information on SNMP objects, see the “SNMP Background” section of this chapter.

Note

Entering **sysInfo* in the **What** box returns most of the “system” identification objects.

- 5 Select one of the radio buttons:

Get. If you know the object name or identifier, you can enter it in the **What** box and use the **Get** option. For example, on a Windows NT system, a **Get** request for *ifPhysAddress.2* returns the network adapter address. If it is a wrong name or number, you will not get any information back. If there is more than one instance of the object, you need to enter the specific instance.

Get Next. Use **Get Next** to get the next object instance from a table or list within the SNMP agent on the device. You can determine the values to use in the **What** box by what is returned using **Get Next**. You should use this option with most of the items that are in the MIB.

Get All Subitems. This option returns any subitems of the named item.

Monitor. Starts the SNMP Graphing Utility and graphs the network object specified in the **What** box. For more information on graphing, see “Graphing SNMP Values” on page 152.

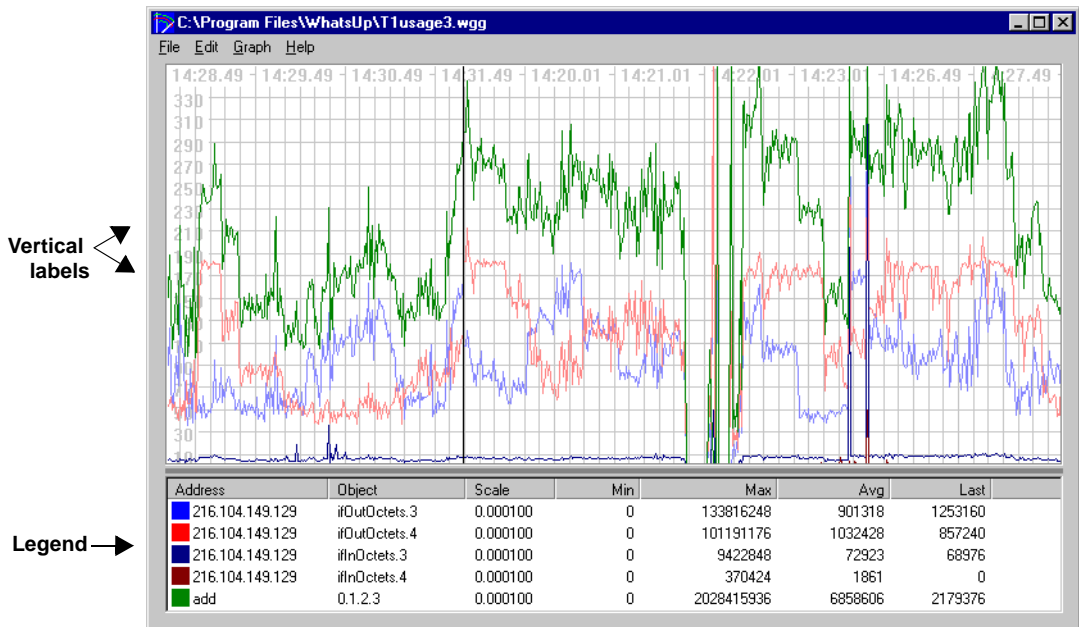
- 6 (Optional) Change the **Delay** setting from the default of 1000 milliseconds. This value tells the SNMP tool how long to wait for a response to an SNMP request before reporting a timeout.
- 7 Click **Start** to retrieve the SNMP information.

Any information found for the object is shown in the results window.

Graphing SNMP Values

Some of the SNMP objects are best monitored by displaying their changing values in a graph. WhatsUp Gold's SNMP Graphing Utility lets you select one or more SNMP objects and show a real-time graph of their values. You can also save a particular graph and later open the graph to resume graphing the SNMP objects.

The main window of the SNMP Graphing Utility shows a line graph for each SNMP object added to the graph.



Up to 20 SNMP objects can be active on the graph. You can set the color and line width to distinguish each graphed object.

By default, the SNMP Graphing Utility graphs the *change between* each reported value of the SNMP object. You can set the utility to graph only the reported values for an object. For more information, see “Adding, Editing, and Deleting SNMP Objects” on page 153

Starting the SNMP Graphing Utility

To start the SNMP Graphing Utility, do one of the following:

- Select **SNMP Graph Utility** from the **Tools** menu; or from the **Start** menu, select **Programs -> WhatsUp Gold -> WhatsUp Gold SNMP Graph Utility**.

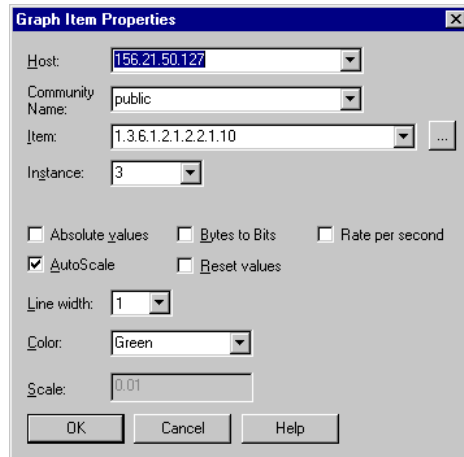
The utility starts the default graph file (*graph.wgg*) that shows the time elapsed between SNMP values reported, which is determined by the Interval specified in **Graph -> Properties**.

- From the SNMP tool (**Tools -> Net Tools -> SNMP**), enter an SNMP object identifier in the **What** box, select **Monitor**, and then click **Start**. The WhatsUp Gold Graphing Utility appears and begins real-time graphing of the selected SNMP object.

Adding, Editing, and Deleting SNMP Objects

To add an SNMP object to the graph:

- 1 From the **Edit** menu, select **Add Item -> SNMP Item**. The Graph Item Properties appear:



- 2 In the **Host** box, enter the host name or IP address of the device for which you want to graph SNMP objects, or select one from the drop-down list.
- 3 If necessary, change the string in the **Community Name** box. The default string is “public.”

The default (*public*) will work for most SNMP hosts unless the administrator has specifically removed “public” and replaced it with a string of their own. If you know a device is manageable via SNMP and public doesn’t work, you will have to talk to the owner of that device to get a community name that will work.

- 4 Enter the **Item** and **Instance** numbers to specify the SNMP object that you want to graph. (Use the Browse button to the right of the Item box to view the MIB tree and select an object. When you select an object in the MIB tree, its object identifier is entered in the **Item** box.)

For background information on item and instance numbers, see “SNMP Overview” on page 144. To customize the MIB tree to include vendor-provided objects that are specific to your enterprise, see “Setting Up the MIB Identifiers” on page 148.

- 5 Set the item graphing options:

Absolute values. When checked, graphs the reported values of an SNMP object rather than graphing the change between the last reported value and the current value (default method). You probably want to turn off **Absolute values** when graphing a counter, such as ifOutOctets; otherwise, the graphed values may be difficult to read.

AutoScale. When checked, the graph scale for the SNMP object is determined by the graphing utility. This is a relative scale that is calculated to make the graph fit into the vertical scale. If you turn off this option, the **Scale** option becomes active and you can enter a value to scale the graph.

Bytes to bits. When checked, multiplies the value reported for the SNMP object by 8 to approximate the count in bits. This option can be used with SNMP objects that are counters, for example if you want to know the baud rate while monitoring a T1 router port, you want (ifOutOctets * 8) to give you a value close to the real baud rate.

Reset values. When checked, clears the values for the selected SNMP object when you exit the dialog box. You can clear the values for all SNMP objects on the graph by selecting **Clear** from the **Edit** menu.

Line width. Sets the width of the line that represents the selected SNMP object.

Color. Sets the color of the line that represents the selected SNMP object.

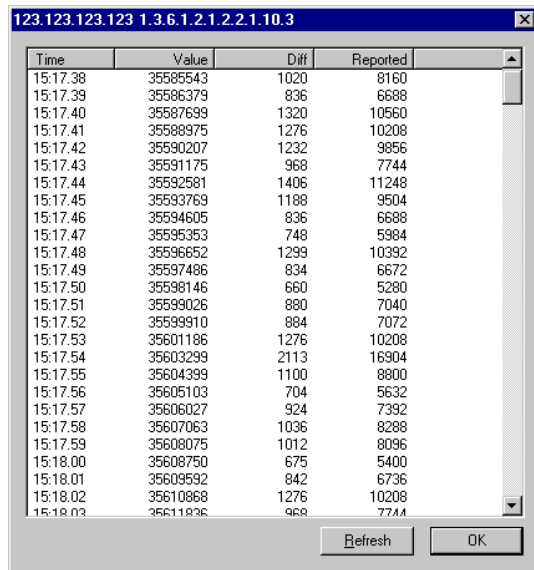
Scale. When **AutoScale** is turned off, you can enter a fixed value in this text box to determine the scale of the graph. You may want to try different values in this box until you find a scale that is useful.

Rate per second. When checked, calculates the average change per second in the values reported for the SNMP object, and then graphs the result. To calculate this average, it takes the difference between the latest reported value and the previously reported value, then divides by the number of seconds between reported values. This option is useful when the graph **Interval** (in Graph Options) is different than one second. You cannot use this option with the **Absolute values** option.

6 Click **OK** to add the SNMP object to the graph.

Viewing Item Values

You can view the raw data used to generate the graph for an SNMP item. Select the graph item in the Legend, then select **View Item Values** from the **Edit** menu.



Time	Value	Diff	Reported
15:17.38	35585543	1020	8160
15:17.39	35586379	836	6688
15:17.40	35587699	1320	10560
15:17.41	35588975	1276	10208
15:17.42	35590207	1232	9856
15:17.43	35591175	968	7744
15:17.44	35592581	1406	11248
15:17.45	35593769	1188	9504
15:17.46	35594605	836	6688
15:17.47	35595353	748	5984
15:17.48	35596652	1299	10392
15:17.49	35597486	834	6672
15:17.50	35598146	660	5280
15:17.51	35599026	880	7040
15:17.52	35599910	884	7072
15:17.53	35601186	1276	10208
15:17.54	35603299	2113	16904
15:17.55	35604399	1100	8800
15:17.56	35605103	704	5632
15:17.57	35606027	924	7392
15:17.58	35607063	1036	8288
15:17.59	35608075	1012	8096
15:18.00	35608750	675	5400
15:18.01	35609592	842	6736
15:18.02	35610868	1276	10208
15:18.03	35611836	968	7744

The “View Item Values” window shows the following data for the SNMP object:

Title bar. Shows the IP address of the selected host and the object identifier for the SNMP object.

Time. Time the value was reported.

Value. The absolute value reported by the SNMP object.

Diff. This is the difference between the reported value and the previously reported value. (Note that this value may not make sense if the graph is at a “wrap” point.)

Reported. This is the actual value used in the graph. This value depends on the setting in the graph item's properties, which can be set in one of the following dialog boxes: Graph Item Properties, Graph Accumulator Properties, Graph Timer Properties. If the item is set to report **Absolute value**, this value will be equal to the absolute value. If set to report **Bytes to bits**, this value will be the absolute value multiplied by 8. If set to report **Rate per second**, this value will be the difference between the last two reported absolute values divided by the time difference (**Time Diff**). If both **Bytes to bits** and **Rate per second** are selected, the reported value will be equal to the difference between the last two reported absolute values multiplied by 8, then divided by the time difference (**Time Diff**).

Time Diff. This is the difference (in milliseconds) between the time the last value was reported and the time the previous value was reported.

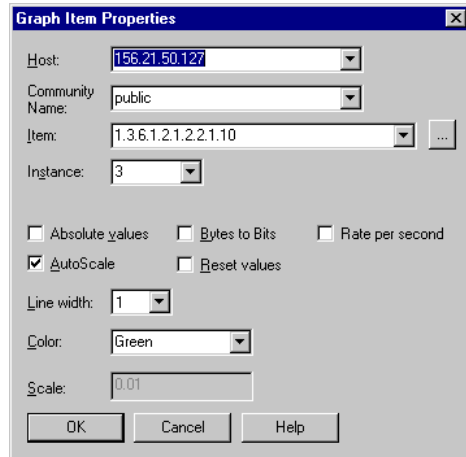
Click **Refresh** to update the displayed values.

Editing Item Properties

To edit a graph item’s properties:

- 1 To select the item to edit, do one of the following:
 - In the graph legend, double click the item you want to modify.
 - In the graph legend, click the item you want to modify, and then select **Item Properties** from the **Edit** menu.
 - In the graph legend, right-click the item you want to modify, and select **Properties** from the right-mouse menu.

The following dialog box appears.



- 2 Make any changes to the properties and click **OK** to save them and exit the dialog box.

Deleting Items from the Graph

You can delete an item from the graph at any time. In the graph legend, do one of the following:

- 1 Click the item you want to delete, and then select **Delete Item** from the **Edit** menu.
- 2 Right-click the item you want to delete and then select **Delete** from the right mouse menu.

Saving and Opening Graph Files

You can save a graph to a file and it will save the selected graph items and options. Data values are not saved. You can later reopen the graph file and resume real-time graphing of the saved SNMP items.

WhatsUp Gold SNMP graph files use the extension *.wgg*.

To save a graph:

- 1 From the **File** menu, select **Save Graph**. The “Save As” dialog box appears.
- 2 In the **File** name box, enter a file name with a *.wgg* extension.
- 3 Click **Save** to save the graph objects.

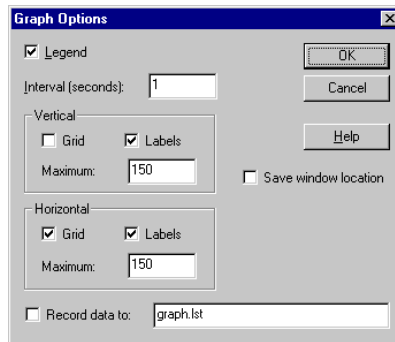
To open a saved graph:

- 1 From the **File** menu, select **Open Graph**. The “Open” dialog box appears.
- 2 Select a graph file name (with a *.wgg extension*) and click **Open**.

Editing Graph Properties

Use the “Graph Options” dialog box to set the layout of the graph window, the interval (or frequency) for recording values for the SNMP objects, and whether you want to record the data to a file.

To view the properties, select **Properties** from the **Graph** menu:



Legend. When checked, the Legend appears at the bottom of the graph window. The Legend displays each graphed SNMP object and its associated device, as well as any accumulator items.

Interval (seconds). Sets the time interval at which the graph records values.

Vertical (y-axis). When **Grid** is checked, displays lines across the graph to help you read the vertical graph. When **Labels** is checked, values are displayed next to the y-axis. The **Maximum** determines the highest value on the y-axis scale, as well as the internal values. This value cannot exceed 1500.

Horizontal (x-axis). When **Grid** is checked, displays lines across the graph to help you read the x-axis values. When **Labels** is checked, values are displayed next to the x-axis. The **Maximum** determines the highest value on the x-axis, as well as the internal values. This value cannot exceed 1500.

Save Window Location. When checked, saves the position of the Graph Window so that it always opens in the same location on your screen.

Record data to. If you want to save graph data, check this box and enter a file name. Whenever the graph is running, the SNMP values will be appended to this file. The file is saved in the WhatsUp Gold directory. The file format is tab-delimited and can be imported to a spreadsheet application.

File Format:

```
Date [tab] time [tab] first item value [tab] second item value [tab]
...
```

For example, a graph with four items would show the date and time plus the four values recorded at that time. The heading shows the IP address and SNMP object identifier for each graph item.

```
DateTime[156.21.50.12]:1.3.6.1.2.1.5.2.2.12.50.1102:1.3.6.1.2.1.2.2.1.10.4[156.21.
[156.21.50.12]:1.3.6.1.2.1.2.2.1.16.4
11/03/199911:07:34103782671006689712990
11/03/199911:07:35169587431031456766866
11/03/199911:07:3620678156873944783968
```

Receiving SNMP Traps

WhatsUp Gold has an internal SNMP trap handler, which when enabled, listens for and accepts SNMP traps that are addressed to it. A trap is sent when the status of a device changes. Traps are unsolicited messages, such as a router indicating one of its interfaces went down or a printer indicating it is out of paper.

When a trap arrives from a device, WhatsUp Gold inverts the device's display name on the network map to show a status change and records the trap information in the device's **Log** tab and in the Event Log.

You can also set up WhatsUp Gold to send a notification message (via pager, beeper, e-mail, or voice) when a trap is received for a device.

To receive traps in WhatsUp Gold, you need to do the following:

- 1 On each physical device that will be monitored, set the SNMP agent to send traps to WhatsUp Gold. This *cannot* be done from WhatsUp Gold.
- 2 If you have vendor-provided devices, run the MIB Extractor as described in "Setting Up the MIB Identifiers" on page 148.

Enable the SNMP Trap Handler. (Select **Options** -> **Program**, click the Programs and SNMP tab, turn on **Enable SNMP Trap Handler**, and then click **Apply**.)

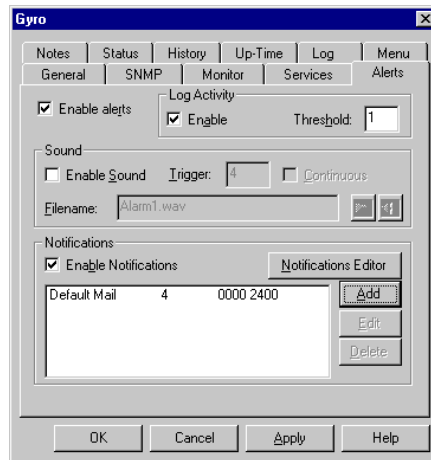
- 3 Set up any notifications for traps as described in the following section.

Setting Up Notifications for Traps

You can set up WhatsUp Gold to send a notification when an SNMP trap is received for a device. You can specify that the notification is sent when any trap message is received or when a specified trap number(s) is received. For background information about SNMP traps and trap numbers, see “SNMP Traps” on page 147.

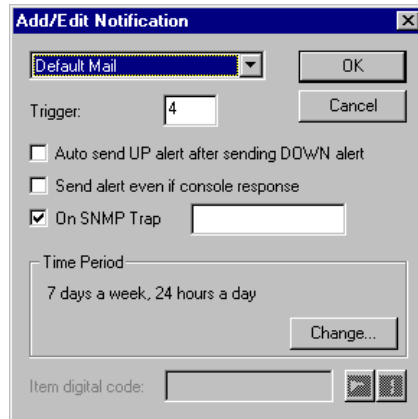
To set up a notification for a trap message:

- 1 Double-click the device and click the **Alerts** tab.



- 2 Turn on **Enable Alerts** and **Enable Notifications**.
- 3 In the **Notifications** section, click **Add**.

The “Add/Edit Notifications” dialog box appears.



- 4 From the drop-down list, select the notification you want to send when this device receives a trap message.

You can create new notifications and make them available in the drop-down list. See the “Defining Notifications” section in Chapter 5 for the step-by-step procedure.

- 5 Turn on the **On SNMP Trap** option.

When this option is enabled, and the edit box to the right of it is empty, the specified notification will be sent when *any* trap is received for the device. If the edit box contains a trap number or numbers, notification is sent only if a trap with the specified number is received. Separate multiple entries in the text box with a comma.

You can enter a number for one of the six standard traps, or you can enter a number for a vendor-provided trap. If you are unsure of a trap number, you can view the Event Log (after enabling traps) to see what number is associated with a particular trap.

Note that the notification of the SNMP trap is sent as soon as the trap arrives: the **Trigger** value is ignored. The trap text can be included in mail notifications if you use the %N variable. For more information, see “Notification Message Variables” on page 63.

Note

A notification will also be sent if the device misses the number of polls specified in the **Trigger** box. If you want to be notified *only* of an SNMP trap, you can set the **Trigger** to 9999.

- 6 Set the **Time Period** in which you want the notification to be active.
- 7 Click **OK** to save your changes. The notification is added to the device's list of notifications.
- 8 In the **Alerts** tab, click **OK** to save changes and exit the dialog box.

Viewing Trap Log Entries

SNMP traps are logged regardless of whether or not you have enabled log activity for the device.

To view trap information for a device, view the device properties and click the **Log** tab.

To view trap information for all devices, select **SNMP Trap Log** from the **View** menu.

Monitoring SNMP Service

To monitor whether SNMP is running on a device:

- 1 Double click the device to display its properties.
- 2 Click the **Services** tab to display services properties.
- 3 Check the **SNMP** service. Use the default (*public*) in the **Community** box unless your system administrator has set a different community.
- 4 Click **Apply** to apply your changes. Click **OK** to apply the changes and exit the dialog box.

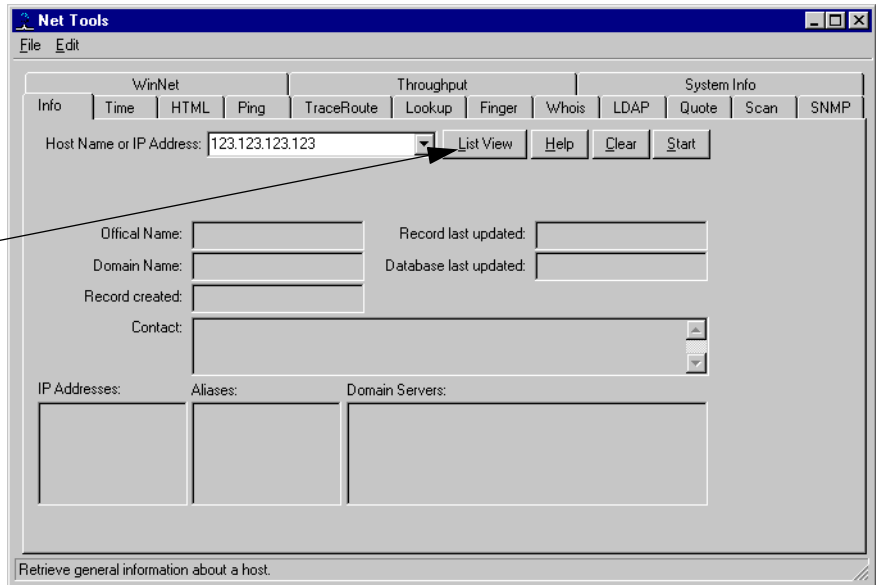
If SNMP service is being monitored on a device, an asterisk (*) is displayed next to the device icon in the map.

Chapter 9: Using Network Tools

WhatsUp Gold includes a versatile set of tools that let you search for and display information about organizations, networks, computers, or people on a network.

When you select **Net Tools** from the **Tools** menu, you see the following tabbed dialog box:

The Info, Ping, Traceroute, and Throughput tools have a button that toggles between "List View" (list format) and "Report View" (textual format).



Each tab contains the parameters and results area for one tool. The tools include:

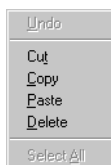
- Info — Display a summary of device information.
- Time — Synchronize your computer's clock with a remote time server.
- HTML — Query a web address.
- Ping — Verify connectivity to a host.
- TraceRoute — Trace and view the route to an Internet host.
- Lookup — Query Internet domain name servers for information about hosts and name servers.
- Finger — Display information about users on a host.

- Whois — Display information from the network information center about Internet domain ownership and Internet groups.
- LDAP — Search directories for names and information.
- Quote — View quotations from a quote server.
- Scan — Scan a range of IP addresses to create a network map. For information on using this tool, see “Chapter 2: Creating Network Maps” on page 13.
- SNMP — View and graph Simple Network Management Protocol values for a device. For information on using this tool, see “Chapter 8: Monitoring SNMP Devices” on page 143.
- WinNet — View Windows Network domains, hosts, and workstations.
- Throughput — Test data throughput on the connection between your computer and a remote computer.
- System Info — View information about your local system.

Using Format, Copy, and Print Functions

You can use the standard Windows cut, copy, and paste functions in all the tools and you can cut, copy, and paste between the tools as well as between a tool and any Windows application.

In general, to cut, copy, or paste data in a text box or in a display window, you can click the right mouse button to display the pop-up menu.



However, the right mouse menu is not available when you are using the Report View of the Ping, TraceRoute, and Throughput tools; use the **Edit** menu instead. Furthermore, when using the Info tool, you can select and copy text only when displaying results in the List View.

Printing Results

You can print the results displayed by any of the tools. Within a tool’s tab, display the results of a query, and then select **Print** from the **File** menu to view the standard Windows print setup dialog box.

Displaying Device Information (Info Tool)

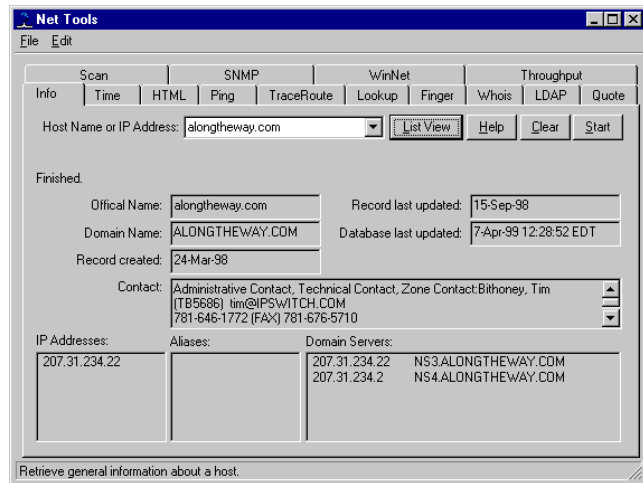
The Info tool displays a summary of information about a network host or device, including the official host name, IP address, and contact information (from the Whois database). An Info request on a host name also polls (pings) the host to verify connectivity.

The Info tool provides a quick way to get host information – it runs Lookup and Whois queries on the specified host and also pings the host to check its availability.

To send an Info query:

- 1 From the **Tools** menu, select **Net Tools** and click the **Info** tab to display the Info options.
- 2 In the **Host name or IP Address** box, enter the name or address of a host you want to query. This must be a fully qualified host name or address (for example: whitehouse.gov)
- 3 Click the **Start** button.

The results of the query appear in the window.



During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Checking a Web Address (HTML Tool)

The HTML tool's primary purpose is to help developers debug their web sites. The HTML tool sends a "get" or "head" request to a specified web address (URL) and returns full header information (including cookies) and also returns the page data (raw or formatted HTML code).

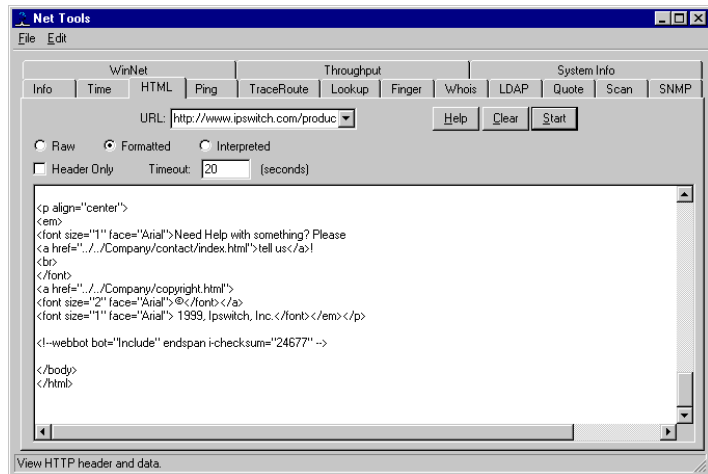
To query a web address:

- 1 From the **Tools** menu, select **Net Tools** and click the **HTML** tab to display the HTML options.
- 2 In the **URL** (Uniform Resource Locator) box, enter the web address of the web page you want to query.

This must be a specific web site file (for example: `http://host name/page/`). A slash (/) is required at the end of the URL.

- 3 Select the format for displaying the page data: Select **Raw** to display page data with embedded HTML code. Select **Formatted** to display the page data with carriage returns inserted. Select **Interpreted** to display the page as viewed in a browser. Select **Header only** if you want to display the HTML header for the page, without downloading the full contents of the page.
- 4 Click the **Start** button.

The results of the query appear in the window.



During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Synchronizing Time (Time Tool)

The Time tool lets you synchronize your local system's clock with the clock of a remote time server. Remote time servers provide a constantly updated time of day reading (in hours, minutes, and seconds) and the date (year, month, day). The Time tool provides predefined entries for some publicly available time servers. You can also query your own or other time servers.

Note

The Time tool uses the Time protocol specified in RFC 868.

Using the Time tool, you can also:

- Synchronize your local clock on demand
- Interrogate multiple time of day servers simultaneously and display the difference (in seconds) between the remote time server and the local system time.
- Adjust the displayed time of a remote time server by setting an offset (plus or minus hours) from GMT.
- Sort the display (for multiple time servers) by column (Server Name, Time, Difference, Offset, and Error Code).

To synchronize your local system's clock with a remote time server:

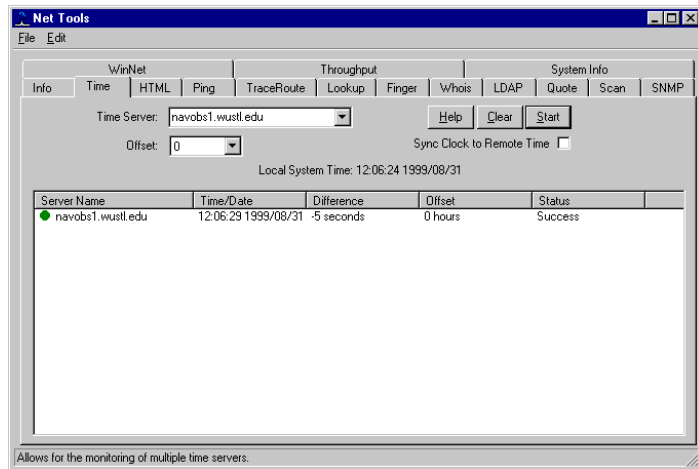
- 1 From the **Tools** menu, select **Net Tools** and click the **Time** tab to display Time options.
- 2 In the **Time Server** box, type the host name or IP Address (for example, xfiles-jr.esa.lanl.gov, navobs1.wustl.edu, wwwvb.isi.edu) of the remote time server you want to query. The drop-down list shows the previous host names or IP addresses you have queried.
- 3 Click the **Synch Clock to Remote Time** option (make sure it is checked). Your local system's date and clock time is always displayed above the results area.

- 4 Optionally, use the **Offset** box to adjust the displayed time of a remote time server by an offset (plus or minus hours) from GMT.
- 5 Click the **Start** button.

A connection is established with the remote time server and the server name and current time are reported in the display window. The reported time is constantly updated until you do one of the following:

- Click **Clear** to clear the display.
- Select the time server in the display, and then select **Remove** from the right-mouse menu.

The display window also shows the time difference between your local system's clock and the time server's clock, any time offset you specified, and any error codes reported. (If Time reports an error code, try another time server from the list.)



During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

To sort values in a column in ascending order, click the column heading. To reverse the sort order, click again.

To interrogate multiple time servers:

One at a time, enter or select the time server's host name or IP address in the **Time Server** box and then click **Start**. Each time server you select is displayed on a separate line.

To update the time reported by the server now:

Right-click the time server in the Server Name column to display the pop-up menu, and then select **Update Time from Server**.

To synchronize the local clock with the time server now:

Right-click the time server in the Server Name column to display the pop-up menu, and then select **Sync Clock To Remote Time**.

To suspend polls to a time server:

Right-click the time server in the Server Name column to display the pop-up menu, and then select **Stop Monitoring This Item**. To restart monitoring, right-click on the server and select **Start Monitoring This Item**.

To suspend polls to all time servers:

Right-click any time server in the Server Name column to display the pop-up menu, and then select **Stop Monitoring All Items**. To restart monitoring, right-click on any server and select **Start Monitoring All Items**.

To remove a time server from the list of servers:

Right-click the time server in the Server Name column to display the pop-up menu, and then select **Remove**.

To change the offset (to account for time zone differences):

- 1 Click the time server in the Server Name column or select a server from the Time Server drop-down list.
- 2 In the **Offset** drop-down list, select the desired offset.
- 3 Click **Start**.

Verifying Connectivity (Ping Tool)

The Ping tool is a network diagnostic tool used to verify connectivity to a particular system on your network. Ping sends an ICMP “echo request” in the form of a data packet to a remote host and displays the results for each “echo reply”. This exchange is referred to as “pinging.” The Ping command also displays the time for a response to arrive in milliseconds (this will vary depending on network load) and debugging information about the network interface. You can have multiple instances of the Ping tool active simultaneously.

To ping a host:

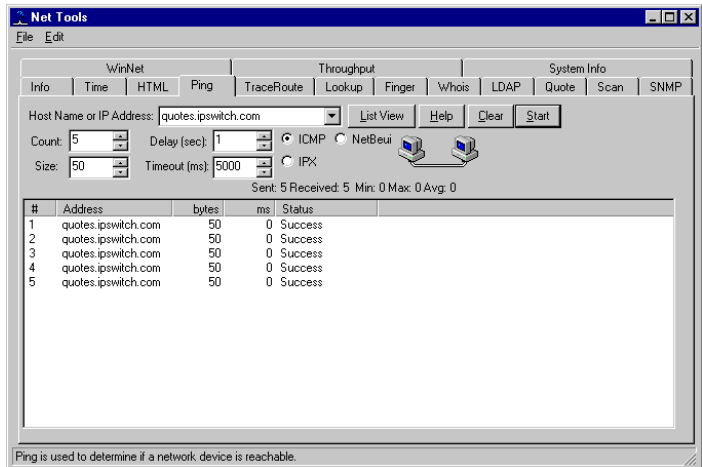
- 1 From the **Tools** menu, select **Net Tools** and click the **Ping** tab to display ping options.
- 2 In the **Host name or IP Address** box, type a host name or IP Address (for example, internic.net).
- 3 Select the protocol to use for pinging depending on the type of host selected. Use **ICMP** for TCP/IP hosts, **IPX** for Novell NetWare hosts, or **NetBEUI** for Windows network hosts.

Note

To ping an IPX device, Microsoft’s NWLink IPX/SPX Compatible Transport must be installed and running on the WhatsUp Gold system. For more information, see “System Requirements” on page 6.

- 4 Set any of the options you want to use:
 - Count.** The number of data packets sent by the ping command.
 - Delay (sec).** Number of seconds to wait between sending a ping.
 - Size.** The length in bytes of each packet sent by the ping command.
 - Timeout (ms).** The ping will fail if the host does not respond after this number of milliseconds.
- 5 Click the **Start** button.

The Ping tool sends an echo request and waits for the echo reply. If the ping was successful, summary lines are displayed in the Ping tab, indicating the result of the ping.



If the reply is not received within the timeout value, the ping fails. This means there has been a failure at one of several points from your PC to the remote host. The host may not be functioning and therefore is unable to respond, a network or gateway in the path from the user may not be working, or the host may not implement the service you are requesting.

During the ping, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the ping. Click **Clear** to erase the results from the display window.

Tracing a Route (TraceRoute Tool)

The Traceroute tool lets you trace and view the actual route an IP packet follows from the local host to another host on the Internet. Response times are displayed in milliseconds and will vary depending on network load. TraceRoute is useful for finding potential trouble spots on large and complex networks that are connected together by routers.

The results of a traceroute can be mapped to a network map.

To initiate a traceroute search, do the following:

- 1 From the **Tools** menu, select **Net Tools** and click the **TraceRoute** tab to display the traceroute options.
- 2 In the **Host Name or IP Address** text box, enter a host name or IP address for the remote host — this is the host to which you want to trace the route.

The drop-down list shows the previous host names or IP addresses for which you've done a traceroute.

- 3 Set any of the options you want to use.

Maximum Hopcount. The maximum number of hops to trace before ending the traceroute. When an IP packet passes from one host to another, it is referred to as one hop.

Map Results. When this option is enabled, when you launch a trace to a host, WhatsUp Gold draws a map of the route, displaying an icon for each router and showing the connections from router to router until it reaches the host.

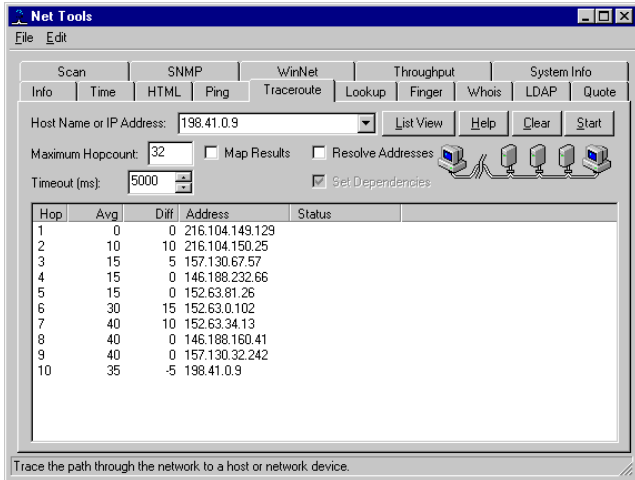
Resolve Addresses. When enabled, the host names of each router along the route will be displayed along with the IP addresses. When disabled, only the IP addresses are shown. Showing the host names will add time to the traceroute as it requires that the IP addresses be resolved.

Set Dependencies. This option is available when **Map Results** is turned on. When enabled, it will set each router found by the traceroute as an “up” dependency on the previous router in the route. This means that when polling, if a router is down, WhatsUp Gold will not poll routers further along the route to a host.

Timeout. The TraceRoute will fail if the device does not respond after this number of milliseconds.

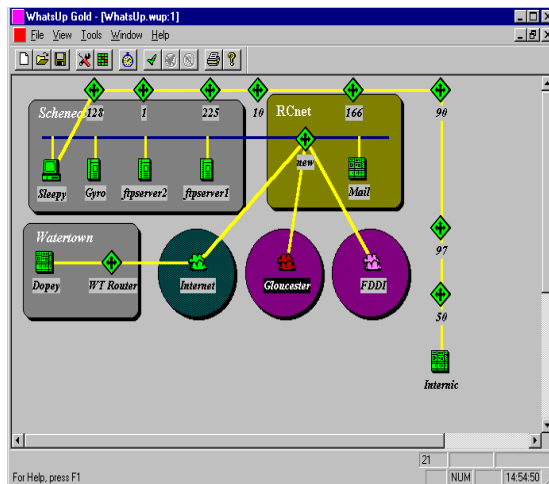
- 4 Click the **Start** button.

The results of the TraceRoute search are displayed in the results area.



During the trace, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the trace. Click **Clear** to erase the results from the display window.

If the **Map Results** option is enabled, WhatsUp Gold draws a map of the route. It adds icons for any devices (such as routers) that are not already in the map. The following example shows the map of the route from Sleepy (the local host) through each router along the path to the Internic's host.



Finding Host and Name Server (Lookup Tool)

The Lookup tool lets you query Internet domain name servers for information about hosts and name servers. You can use Lookup to:

- Find the IP address from a name or a name from an IP address
- List just the name and Internet address of a host or domain
- Query the name server for information about various hosts and domains
- List hosts in a domain

To initiate a Lookup query:

- 1 From the **Tools** menu, select **Net Tools** and click the **Lookup** tab to display lookup options.
- 2 In the **Name or IP Address** text box, enter a host name or IP address of the device or domain name server you want to look up.
- 3 Set any of the options you want to use.

DNS Server. Enter the IP address of the domain name server you want to query or select *[stack]* from the drop-down list to use the network stack in your operating system.

Note

When you select the *[stack]* option, Lookup uses the Winsock stack lookup routines. If you specify a server, Lookup creates and interprets its own DNS packets and does not use the Winsock stack routines.

Query Type. Select a type from the drop-down list.

The query types are:

Type	Returns the following information:
A	The host's Internet address
ALL	All information
CNAME	Alias names for the host
HINFO	The CPU type and operating system type of the host
MX	The host that acts as the mail exchanger
NS	The name server for the named zone

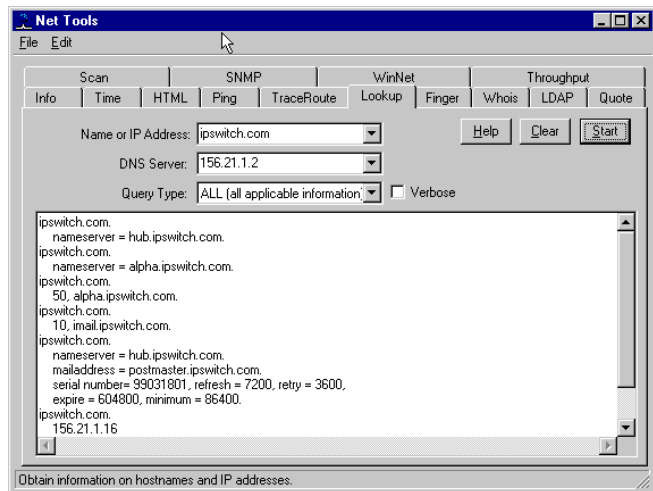
PTR	The host name, if the query is an Internet address; otherwise, a pointer to other data
SOA	The domain's "start of authority" information, which indicates the name server and additional administrative information
ZONE	The zone listing for the domain, which defines the domains for which the name server is the primary name server and lists registered host in the domain

Note

If you use the network stack, you can only do name-to-address lookups (A) or address-to-name lookups (PTR). If you specify a DNS server, you can use all of the query types.

The **Verbose** option is useful only when you specify a DNS server. When enabled, you can see the information that comes back from the DNS server.

- 4 Click **Start**. The information returned by the lookup query appears in the results area.



During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Getting Information About Users (Finger Tool)

The Finger tool lets you identify and display information about all users on a network host. This information can include a display of current users on the host (their user IDs and user names), and for each user — the home directory, log in time, idle times, office location, last time they received mail, and last time they read mail. The exact data returned by a Finger query depends on what the source (the Finger server) has chosen to provide.

A Finger request will also display any information contained in the file *.plan* or the file *.project* in the user's home directory. These files are often used as a simple way to distribute information.

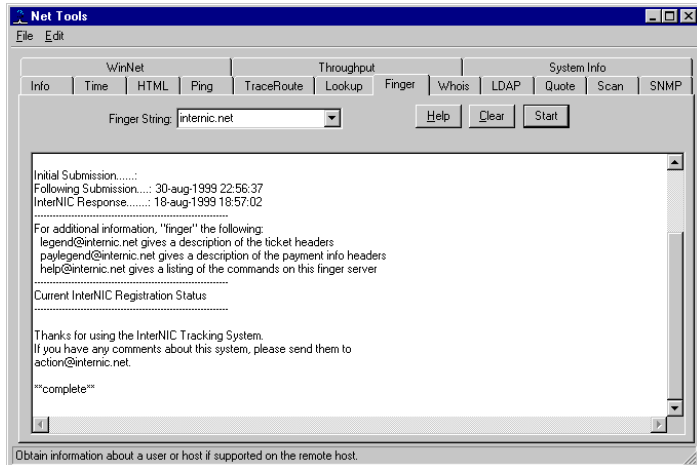
If the specified host does not have a Finger server, the Finger client displays the message: `Connection not made`

To initiate a Finger query, do the following:

- 1 From the **Tools** menu, select **Net Tools**, and click the **Finger** tab to display Finger options.
- 2 In the **Finger String** text box, enter a host name or IP address.

The drop-down list shows the previous host names or IP addresses for which you sent a Finger request.

- 3 Click the **Start** button. The Finger client contacts the host's Finger server. The results of the query appear in the window.



During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Getting Owner Information (Whois Tool)

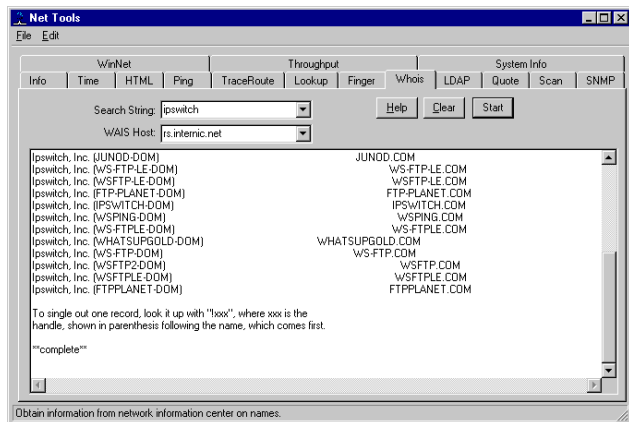
The Whois tool, like Finger, is an Internet directory service. Whois provides information about who owns an Internet host or domain and who you can contact regarding that host or domain. A Whois request displays a contact name, mailing address, telephone number, and network mailbox for all users and organizations who are registered with the Network Information Center (NIC) database.

Note

The current host server for the Network Information Center (NIC) is *rs.internic.net*. You can send a Whois query to this host to display information on using services that the NIC provides.

To initiate a Whois query, do the following:

- 1 From the **Tools** menu, select **Net Tools**, and click the **Whois** tab.
- 2 In the **Search String** text box, enter a search string. If you know the name or handle of an organization, enter it here.
- 3 In the **WAIS Host** text box, enter a host name or user name.
- 4 Click the **Start** button. The Whois client contacts that host's Whois server. The results of the query appear in the window.



During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Searching Directories (LDAP Tool)

Lightweight Directory Access Protocol (LDAP) is an Internet standard for accessing directory information stored on a server. It permits an LDAP-enabled client to search for and view information stored in an LDAP directory on another computer. LDAP is a subset of the x.500 directory access protocol.

The LDAP tool lets you view information on a remote computer that has an LDAP server. Most LDAP servers will let you view e-mail addresses and users' full names, and many servers will provide information such as the user's organization name, division or department name, and postal address. In addition, any LDAP server can contain its own customized set of attributes or data.

To view LDAP information:

- 1 From the **Tools** menu, select **Net Tools**, and click the **LDAP** tab to display the LDAP options.
- 2 Define a query for LDAP information.

Use the three text entry boxes at the top of the LDAP tab to specify a query for LDAP information.

In the first text box, enter the LDAP attribute that you want to display, or select an attribute from the drop-down list. If you want to display all the entries for the selected attribute (for example, you want to display all mail addresses), you can ignore the other two text boxes.

If you want to further narrow your search to display specific entries, you can use the second and third text boxes. In the second text box, you can select one of the following:

contains	the text (in the third box) is part of the entry
is	the text is the exact name of the entry
is like	the text is a near match for the entry (not supported by all LDAP servers)

Then, in the last text box, you can enter criteria (such as a name) to display only those entries that meet the search criteria. For example, to search an LDAP directory for information about a company named Acme, you could enter it as follows:

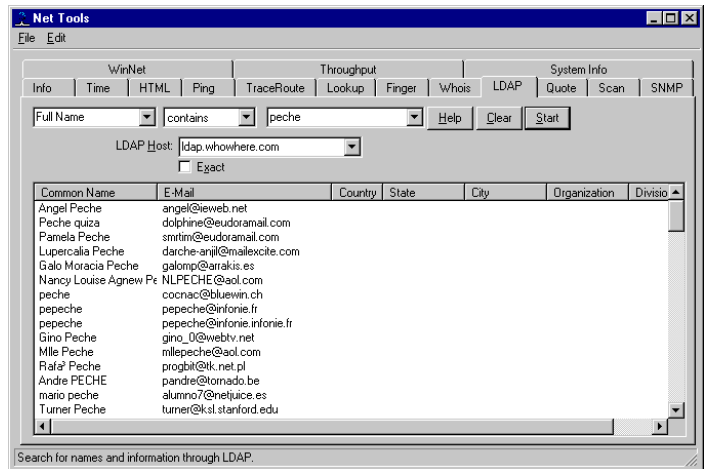


- 3 In the **LDAP Host** box, enter the name of the host that you want to query.

This must be a fully qualified host name (for example, mail.acme.com). From the drop-down list, you can select some of the more widely-used LDAP directories. Your previous LDAP entries are also shown in the drop-down list.

- 4 Click the **Start** button.

Any LDAP information that meets the specified search criteria is displayed.



Note

If there are too many responses to your query, most LDAP servers will not return anything. You'll need to further define your search criteria.

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Viewing Quotations (Quote Tool)

The Quote client lets you view information on a remote host that supports a Quote server. Quote servers often display a “quote of the day.” For example, if you connect to the Ipswitch quote server, you may see a quote like the following:

“It was as true as taxes is. And nothing’s truer than them.”
Charles Dickens (1812-1870)

To view Quotes:

- 1 From the **Tools** menu, select **Net Tools**, and click the **Quote** tab to display the Quote options.

This must be a fully qualified host name (for example: *quotes.ipswitch.com*).

- 2 In the **Quote server** box, enter the name of a host that contains the quote server.
- 3 Click the **Start** button.

The results of the query appear in the window.

During the query, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the query. Click **Clear** to erase the results from the display window.

Scanning Your Network (Scan Tool)

The Scan tool lets you scan a range of IP addresses to create a map of the devices in your network. For more information, see “Chapter 2: Creating Network Maps” on page 13.

Viewing and Graphing SNMP Values (SNMP Tool)

The SNMP tool lets you view and graph Simple Network Management Protocol values for a device. The device must be SNMP enabled. For information on using this tool, see “Chapter 8: Monitoring SNMP Devices” on page 143.

Displaying Network Information (WinNet Tool)

The WinNet tool scans your local network and displays the names of Windows network resources (domains, hosts, or shared resources). Note that resources on the Windows network use NetBEUI (Windows NetBIOS) names which may or may not correspond to Internet host or domain names. You can use the drop-down list to select the items for which you want to scan. In addition, you can enter the NetBEUI name of a Windows resource on your network and view information about that resource.

- 1 From the **Tools** menu, select **Net Tools**, and click the **WinNet** tab.
- 2 In the **Network Items** text box, select the type of network items that you want to display from the drop-down list. You can select from the following item types:

networks — show all networks (groups of domains)

domains — show all domains (groups of servers)

servers — show all devices running the Server service

shares — show all shared devices, such as printers

all — show all the above types of items

- 3 Click the **Start** button.

WhatsUp Gold scans your local network and displays the name and address of the specified items.

During the scan, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the scan. Click **Clear** to erase the results from the display window.

Testing Data Speed (Throughput Tool)

Throughput is a diagnostic tool that lets you test the data speed on a connection with a remote host. It sends a specified number of IP packets, in a range of packet sizes, to a specified remote computer and calculates the average data speed over the communications link.

To test throughput on a connection:

- 1 From the **Tools** menu, select **Net Tools** and click the **Throughput** tab.

2 In the **Hostname or IP Address box**, type a host name or IP Address (for example, internic.net).

3 Set any of the options you want to use:

Packet Count. The number of data packets sent.

Timeout (ms). The time, in milliseconds, that the tool will wait for a response.

Packet Size. The maximum length in bytes of the largest packet sent. To accurately determine throughput, use the largest packet size that works consistently without timing out.

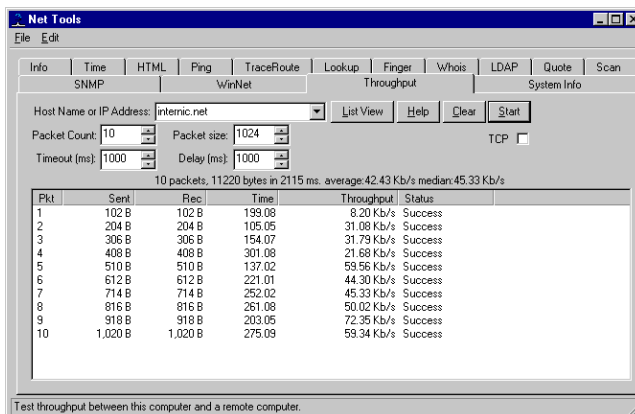
Delay (ms). Number of milliseconds to wait between packets.

TCP. Normally, ICMP packets are sent, but if this is selected, TCP checks are sent through the echo port (port 7), which must be running on the remote system. Throughput is more accurate if this option is not used.

4 Click the **Start** button.

The Throughput tool sends the specified number of data packets, in a range of packet sizes. For each data packet sent, Throughput shows the number of packets sent, the number received by the remote host, and the average time it took to receive a response (in milliseconds).

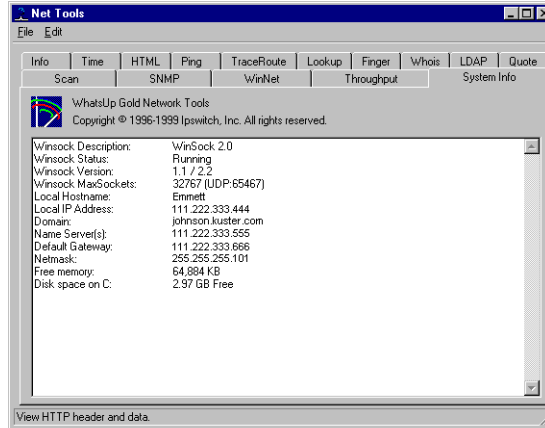
The data speed (in kilobytes per second or whatever measure is appropriate) on the connection is calculated; this is the “throughput.” This will vary depending on the system you are checking and the size of data packets.



During the test, the **Start** button toggles to **Stop**. You can click **Stop** at any time to stop the test. Click **Clear** to erase the results from the display window.

Viewing Local System Information

WhatsUp provides a quick means of getting information about your local system. To view local system information, select **Net Tools** from the **Tools** menu and click the **System Info** tab.



This tab displays information about your local system; WhatsUp Gold gets this information from the Windows Registry.

If your local system has multiple network adapters, System Info will display information from all of the adapters — you will see multiple IP addresses and netmasks.

Note

If you are using DHCP (Dynamic Host Configuration Protocol), the host name, IP address, domain, name server, gateway, and netmask information are dynamically assigned and the Windows registry is not updated. Therefore, the values you see in this tab (under Local Hostname, Local IP Address, Domain, Name Server, Default Gateway, and Netmask) may be incorrect or you may see zero values in place of the IP address and netmask.

Numerics

127.0.0.1 9
7E1 57
8N1 57

A

acknowledging alerts
 from console 94, 104, 108
 from web interface 142
add-ins 89
alarm colors 45, 93
alarms 93
 sounding 54
 sounds 55, 71, 77
 turning off 93, 104, 108
 turning off sound 73, 77
alerts
 acknowledging from
 console 94, 104, 108
 acknowledging from web
 interface 142
API for creating customized
 service checks 89
applications
 starting 34
arguments for programs 34
asterisk 24, 37, 55, 59, 74,
 128, 162
attached lines
 disconnecting 49
 drawing 48
autorun program or script 38

B

background 45
baud rate
 beeper 59
 pager 57
beeper notifications 58
binary value
 searching for 87
bitmap 45
bridges See devices.

C

captions 49
cgi program 85
checking
 definition 3
colors
 device status 3, 45, 93
 map 45
 setting 45
COM extensibility 89
COM interface 89
COM Port 59
Comm (Communications)
 Setup
 beeper 59
 pager 57
command line
 creating Events Reports
 with 109
 creating performance
 graphs 123
 creating Statistics Reports
 with 115
commands on right mouse
 menu 34
communities See SNMP.
context 12, 51, 52
custom
 devices 35
 services 89

D

db files 7
Debug Log 109
default gateway 183
deleting notifications 78
dependencies 31, 98
 setting 32
Dependencies Window 96
depth (of network) 18
devices 1
 addresses 1
 alerts 69

 custom 35
 general properties of 29
 global notifications 75
 icons 40
 IPX 1
 monitoring 31
 monitoring services on 81
 names 27, 29
 root 18
 status 94
 types 1
DHCP 30, 183
dial string 59
disconnecting attached lines 49
Discover and Map 14, 27, 28
disk space, amount of free 183
display name 29
DNS See Domain Name
 Server.
Domain Name Server 10, 23,
 30
domain, local 55, 183
drawing
 shapes and lines 47
 text 49
DSN 6

E

Echo 23
Edit Mode 27, 44, 47
 creating a map 26
 definition 2
e-mail notifications 60
error codes (Winsock) 95, 99
Ethernet 30
Event Log 107
 changing 105
 creating report from 107
 exporting data from 108
 referencing in recurring
 reports 128
 types of events 104
 viewing 107

Event Report 109
Exchange service 83
exporting data 108, 113
exporting performance graphs
123
extensibility 89

F

features
new 5
flat networks 21
free disk space 183
free memory 183
FTP 23

G

gateway, default 183
global notifications 75
Gopher 23
graphs
performance 5, 117
performance, exporting
123
SNMP values 152
group notifications 61

H

hierarchical networks 15, 17,
20, 41, 43
host name 30
host name of local system 183
hosts See devices.
hosts file
importing devices from
16, 25
specifying 26
hosttype.ini 37
HTTP 23
HTTP Content Scan 83

I

ICMP
network scan 21

ICMP packets 28
ICMP requests 3
icons
changing standard 40
custom device 36, 39
names 27
IMail Server ix
IMap4 23
importing devices 16
installation 7
upgrades 6
insufficient data 114
Internet Relay Chat 84
IP Address of local system 183
IP addresses 23, 30
scanning a range of 22
separating numbers in 74

IP packet 171
ipnotify.ini file 7, 54
Ipswitch
products ix
IPX 28, 30
IPX devices 29
polling 28
scanning 28
IRC service 84
monitoring 83
Item digital code 59, 74

L

labels 49
LANbox See devices.
lines
attached See attached
lines
free (unattached) 47
List Window 98
Log tab 70, 76, 105
logs See Debug Log, Event
Log, Statistics Log.
loopback network address 9

M

Management Information Base
See MIB.
manufacturer-provided SNMP
objects 148
maps 1
alarms 93
colors 45
creating 13
drawing 26
Scan tool 21
Scan WinNet tool 25
SmartScan 14, 41
Traceroute 26
hierarchical 17, 20, 41, 43
icons, changing 40
monitoring 93
naming 51
parent map 17, 20, 41, 43
poll frequency 43
properties 42
saving 51
subnets 17, 20, 41, 43
titles 43
members (of group
notifications) 62
memory, amount of free 183
Menu tab 34
menu, right mouse 34
MIB
description 145
object identifiers 148
MIB II 143
mib.txt file 148
mibextra.exe 148
Microsoft Exchange service 83
Microsoft NWLink IPX/SPX
Compatible Transport 6
Microsoft Open Database
Connectivity See ODBC.
Microsoft SQL server 83
Mini Status mode 52
Mini Status view 100

- modems 60
 - drivers 65
 - initialization string 57
 - setting up 65
- Modes, Monitor and Edit 2
- Monitor Mode 27
 - definition 2
- monitoring
 - enabling/disabling 91
 - establishing the active maps 91
 - HTTP Content Scan 83
 - IRC 83
 - Microsoft Exchange 83
 - network maps 93
 - network type 28
 - polling frequency 31
 - Radius service 83
 - services 3
 - setting up 31
 - SQL service 83
 - SSL service 83
 - using a web browser 129
 - using Dependencies Window 96
 - using map window 93
 - using Mini Status view 100
 - using Notifications Window 100
 - using Statistics Window 98
 - using Status Window 96
- N**
- name server 183
- naming
 - contexts 51
 - devices 45
 - icons 40
 - maps 51
- NetBIOS 28, 30
- netmask 44, 183
- NetWare IPX 28
- network class 19
- network devices See devices.
- network elements See devices.
- network maps See maps.
- Network Neighborhood
 - discovering devices from 16
- network status report 125
- network type 28
- networks
 - flat 21
 - hierarchical 17
 - subnets 18
- NNTP 23
- notifications
 - adding to list box 72
 - assigning globally 75
 - assigning to devices 69
 - beeper 58
 - defining 54
 - editing 75
 - e-mail 60
 - global 75
 - group 61
 - how WhatsUp Gold stores 7, 54
 - moving to another system 7, 54
 - overriding 75
 - pager 56
 - program 64
 - properties 69
 - receiving 94
 - setting globally 75
 - sharing among Ipswitch applications 7, 54
 - sound 55
 - system 54
 - threshold 76
 - upgrading 7, 54
 - variables in 63
 - viewing active 94
 - voice 66
 - WinPopup 55
- Notifications Window 100
- Novell IPX See IPX.
- Novell NetWare networks 28
- NT service (WhatsUp Gold as) 11, 55, 77
 - starting and stopping 12
- NTT 56
- NWLink IPX/SPX Compatible Transport 29
- O**
- object identifiers See SNMP.
- ODBC 6, 7
- P**
- PageNet 56
- pager notifications 56
- parameters for programs 34
- parent map 5, 17, 20, 41, 43
- performance graphs 117
 - exporting 123
 - samples 121
- phone number
 - beeper 58
 - modem 67
 - pager 56
 - voice notification 67
- plug-ins 89
- polling
 - automatic 92
 - definition 3
 - dependencies 31
 - frequency 31, 43
 - ICMP requests 3
 - methods 28
 - setting dependencies 98
 - starting and stopping 91
 - statistics 98, 111
 - stopping automatic 92
 - time of day 32
 - timeout 31

POP3 23
 port 3, 23
 primary connection 49
 printers See devices.
 program
 arguments 34
 notifications 64
 parameters 34
 running automatically 38
 starting 34, 64
 variables 34
 properties
 devices 29
 display name 29
 drawn objects 48
 host name 30
 IP address 30
 maps 42
 protocols supported 28

Q

Quiet button 73, 77

R

Radius service 83
 recording wav files 65, 74
 recurring report 125
 registry See Windows registry.
 Remote Authentication and
 Dial-In User Service 83
 reports
 event 107
 recurring 125
 statistics 111
 using command line to
 create 109, 115
 requirements (system) 6
 response time See round trip
 time.
 right mouse menu 33, 34
 root device 18, 19
 rotating
 text captions 50

round trip time 95, 117
 routers See devices.
 RTT See round trip time.
 rules expressions
 search text 86
 text patterns 87

S

Scan IP 27
 Scan IP tool See Scan tool.
 Scan tool 21, 44
 custom icons 39
 Scan WinNet tool 27
 creating maps with 25
 scanning a network using
 SmartScan 17
 scanning the Windows network
 25
 script
 running automatically 38
 search expressions 120
 services 3
 custom 89
 how they are monitored 3
 monitoring 81
 properties 81
 status 95
 Simple Network Management
 Protocol See SNMP.
 SmartScan 5, 14, 16, 17, 20,
 27, 39, 41, 43
 SMS-TA 56
 SMTP 23
 mail host 60
 SNMP
 communities 5, 18
 concepts 144
 manageable devices 23,
 33
 manager 143
 MIB II 143
 monitoring whether
 SNMP is running 162

network scan 15
 object identifiers 22, 37,
 148
 objects 144, 145, 148,
 149, 152, 153
 overview 143, 144
 traps 59, 69, 73, 94, 148,
 162
 sound notification 54
 sounds
 quieting alarm 71, 77, 93
 recording 65, 74
 turning off alarm 71, 77,
 93
 SQL server 83
 SSL server 83
 starting applications 34
 starting programs 34
 statistics See polling statistics.
 Statistics Log 111
 changing 112
 exporting data from 113
 viewing 112
 Statistics Reports 111
 Statistics Window 98
 status
 device 94
 message 93
 network element 94
 report 125
 services 95
 viewing 96
 Status Window 96
 subnet maps 17, 41, 43
 loading 42
 viewing 42
 subnets 17, 20, 21, 41, 43
 system information 183
 system notifications 54
 system requirements 6
 systems See devices.

T

- TAP 56, 57
- TCP/IP 3, 6, 28
- telnet 33
- testing
 - installation 8
- text captions
 - creating 49
- threshold 71, 76, 77, 105, 106
- tilde 24
- time period 32, 73
- Time server 23
- timeout
 - beeper 60
 - polling 31, 43
 - Scan tool 23
 - SmartScan 18
- tips
 - making a map easier to read 27
- toolbars
 - arranging 50
- Traceroute tool 171
- Trap Log 162
- traps.txt file 148
- trigger 62, 71, 73, 77, 105, 106
- trigger and SNMP traps 161
- turning off sound alarms 73, 77

U

- UCP-SMS 56
- UDP 84
- Unimodem V 65
- upgrading 6
 - keeping old notifications 7, 54
- user accounts 133
- user-defined devices See devices, custom
- user-defined services See services, custom.

V

- variables
 - in notification messages 63
 - program 34
- vendor-provided SNMP objects 148
- voice modem
 - setting up 65
- voice notifications 66
 - adding 74

W

- Web pages
 - customizing 130
 - functions 141
 - HTML Files Directory 131
 - Main Page Prefix 131
 - Main Page Suffix 131
 - main page title 130
 - refresh frequency 130
 - TCP Port 130
 - Top View title 130
 - views 139
- Web server
 - access by IP address 133, 136
 - customizing 130
 - functions 141
 - logging on 138
 - making maps available 132
 - setting up 129
 - user accounts 133
 - views 139
- Windows registry
 - importing devices from 16
- WinNet tool 181
 - creating maps with 25
- WinPopup notifications 54
- Winsock errors 95, 99
- Winsock information 183

- WS_FTP Find Utility ix
- WS_FTP Pro (FTP Client) ix
- WS_FTP Scripting Utility ix
- WS_FTP Server ix
- WS_FTP Synchronize Utility ix
- WS_Ping ProPack x
 - wugapi.h file 89
 - wugrpt.exe 109
 - wugstat.exe 115
 - wugstats.log 117

Z

- zero status code 95

