pathSolutions™

# PathSolutions

# Network Monitor

# V4.0

PathSolutions, Inc.
PO Box 64427
Sunnyvale, CA 94088-4427
www.PathSolutions.com

# Document and Software Copyrights

PathSolutions Inc. reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to, typographical, arithmetic, or listing errors.

# Trademarks

PathSolutions, Network Weather Report, Network Prescription, and PathSolutions' Network Monitor are Trademarks of PathSolutions, Inc. in the United States and/or other countries.

# Version Information

Network Monitor
Version: 4.0
Revision: 4817
Date: November 17, 2009

# Company Information

PathSolutions
PO Box 64427
Sunnyvale, CA 94088-4427
www.PathSolutions.com
Support@PathSolutions.com
Sales@PathSolutions.com
(408) 748-1777 (main)
(408) 748-1666 (fax)

# Contents

# Preface

Most network devices are constantly collecting statistics relating to the health of each interface. Network engineers rarely have the budget, time, and resources to access this wealth of information, and very few products exist that can help engineers detect and analyze problems before they affect users.

PathSolutions' Network Monitor was created to help provide this information (collected by switches, routers, servers, and other network devices) in an easy to use format, to help identify the root cause of network problems, and maintain maximum network performance.

## *Audience*

Network administrators with various levels of expertise can benefit from PathSolutions' Network Monitor, as the product offers not only a rapid view of network health, but also in-depth analysis of specific issues.

To install and use PathSolutions' Network Monitor, a network administrator should be able to set up a managed switch with an IP address and an SNMP read-only community string.

## *Conventions*

The following conventions are used in this manual:

*Italic*
Used for emphasis and to signify the first use of a glossary term.

`Courier`
Used for URLs, host names, email addresses, registry entries, and other system definitions.

**Note:** Notes are called out to inform you of specific information that is relevant to the configuration or operation of PathSolutions' Network Monitor. Notes may occasionally be used to describe best practices for using the system.

## *Technical Support*

For technical support: Support@PathSolutions.com
(408) 748-1777 select 1 for technical support

# Overview

PathSolutions' Network Monitor is designed to disclose network weaknesses that cause data and VoIP stability issues.  By monitoring all network interfaces for utilization, packet loss, and errors, it becomes easy to determine exactly where network faults exist.

PathSolutions' Network Monitor goes one step further by providing insight into the specific error or issue that is causing degradation so a rapid resolution can be applied.

Continuous monitoring of all interfaces provides the ability to generate alerts if any interface degrades below a level that will support VoIP services.

PathSolutions' Network Monitor also maintains a history of utilization and errors on all interfaces so you can troubleshoot VoIP and network problems after they occur.

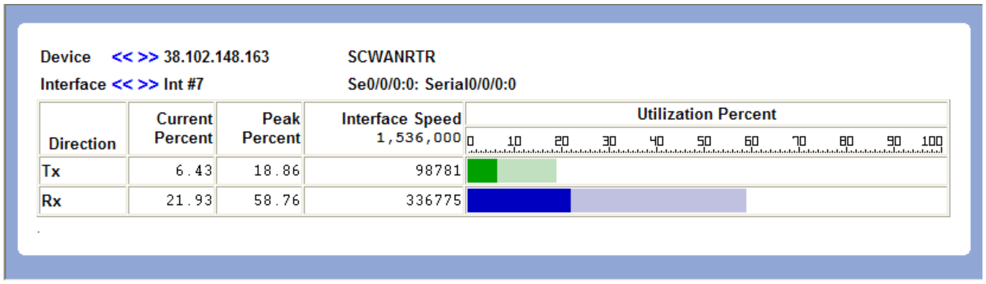
All network devices that support SNMP can be queried for link status and health information

# Standard Features

PathSolutions' Network Monitor is a Windows 2000/2003/2008/XP service that uses SNMP to monitor statistics and utilization for each interface on your switches. If data-link errors or utilization rates rise above a settable threshold, you can use the generated web pages to help you determine the source of the network problems. This will help you to maintain a healthy network.

## *Immediate Current Utilization of any Link*

Easily view the current utilization of any monitored network link from a web browser or PocketPC. No need to set up a packet analyzer or analyzer port on your switch just to see what's happening on an interface.



Device << >> 38.102.148.163 SCWANRTR
Interface << >> Int #7 Se0/0/0:0: Serial0/0/0:0

| Direction | Current Percent | Peak Percent | Interface Speed<br>1,536,000 | Utilization Percent<br>0 10 20 30 40 50 60 70 80 90 100 |
|---|---|---|---|---|
| Tx | 6.43 | 18.86 | 98781 | |
| Rx | 21.93 | 58.76 | 336775 | |

A high-water mark is kept so you can track the peak utilization of a link over time.

## *Daily Network Weather Reports™*

Every day, a report will be emailed to you outlining the health of your network. This helps you to keep track of the general level of errors and overall utilization of your network.

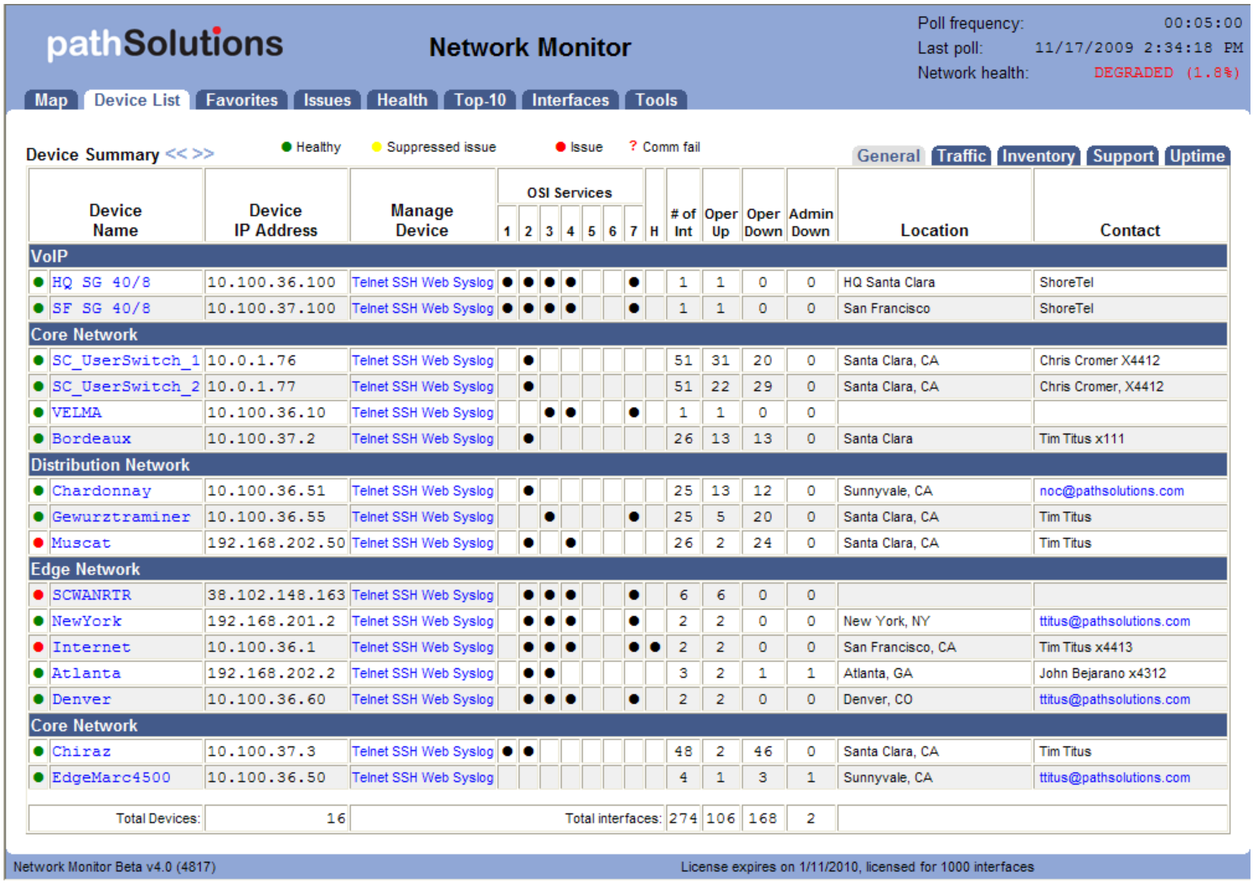
- Keep track of utilization rates on your Internet links and other WAN links to determine if you need to add bandwidth.
- Maintain an active reminder of available interfaces (never get stuck running out of switch interfaces as you continue to add workstations to your network).
- Network Weather Reports can be fully customized.
- Easy to Understand Web-based Statistics
- PathSolutions' Network Monitor collects statistics and displays them in an easy to disseminate format via web pages.
- Web-based statistics viewing allows you to check on the health of your network from any browser

## *Quick Setup with the Built-in Webserver*

PathSolutions' Network Monitor's built-in web server helps to speed up installation so more time can be spent analyzing errors rather than configuring the system.

## *Web-Based Monitoring*

The web pages allow you to quickly locate the interfaces that have high error rates or high utilization rates.



Network Monitor

Poll frequency: 00:05:00
Last poll: 11/17/2009 2:34:18 PM
Network health: DEGRADED (1.8%)

Device Summary << >>

🟢 Healthy 🟡 Suppressed issue 🔴 Issue ? Comm fail

| Device Name | | Device IP Address | Manage Device | OSI Services | | | | | | | | # of Int | Oper Up | Oper Down | Admin Down | Location | Contact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | H | | | | | | |
| VoIP | | | | | | | | | | | | | | | | | |
| 🟢 | HQ SG 40/8 | 10.100.36.100 | Telnet SSH Web Syslog | ● | ● | ● | ● | | | ● | | 1 | 1 | 0 | 0 | HQ Santa Clara | ShoreTel |
| 🟢 | SF SG 40/8 | 10.100.37.100 | Telnet SSH Web Syslog | ● | ● | ● | ● | | | ● | | 1 | 1 | 0 | 0 | San Francisco | ShoreTel |
| Core Network | | | | | | | | | | | | | | | | | |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Telnet SSH Web Syslog | | ● | | | | | | | 51 | 31 | 20 | 0 | Santa Clara, CA | Chris Cromer X4412 |
| 🟢 | SC_UserSwitch_2 | 10.0.1.77 | Telnet SSH Web Syslog | | ● | | | | | | | 51 | 22 | 29 | 0 | Santa Clara, CA | Chris Cromer, X4412 |
| 🟢 | VELMA | 10.100.36.10 | Telnet SSH Web Syslog | | | ● | ● | | | ● | | 1 | 1 | 0 | 0 | | |
| 🟢 | Bordeaux | 10.100.37.2 | Telnet SSH Web Syslog | | ● | | | | | | | 26 | 13 | 13 | 0 | Santa Clara | Tim Titus x111 |
| Distribution Network | | | | | | | | | | | | | | | | | |
| 🟢 | Chardonnay | 10.100.36.51 | Telnet SSH Web Syslog | | ● | | | | | | | 25 | 13 | 12 | 0 | Sunnyvale, CA | noc@pathsolutions.com |
| 🟢 | Gewurztraminer | 10.100.36.55 | Telnet SSH Web Syslog | | | ● | | | | ● | | 25 | 5 | 20 | 0 | Santa Clara, CA | Tim Titus |
| 🔴 | Muscat | 192.168.202.50 | Telnet SSH Web Syslog | | ● | | ● | | | | | 26 | 2 | 24 | 0 | Santa Clara, CA | Tim Titus |
| Edge Network | | | | | | | | | | | | | | | | | |
| 🔴 | SCWANRTR | 38.102.148.163 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 6 | 6 | 0 | 0 | | |
| 🟢 | NewYork | 192.168.201.2 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 2 | 2 | 0 | 0 | New York, NY | ttitus@pathsolutions.com |
| 🔴 | Internet | 10.100.36.1 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | ● | 2 | 2 | 0 | 0 | San Francisco, CA | Tim Titus x4413 |
| 🟢 | Atlanta | 192.168.202.2 | Telnet SSH Web Syslog | | ● | ● | | | | | | 3 | 2 | 1 | 1 | Atlanta, GA | John Bejarano x4312 |
| 🟢 | Denver | 10.100.36.60 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 2 | 2 | 0 | 0 | Denver, CO | ttitus@pathsolutions.com |
| Core Network | | | | | | | | | | | | | | | | | |
| 🟢 | Chiraz | 10.100.37.3 | Telnet SSH Web Syslog | ● | ● | | | | | | | 48 | 2 | 46 | 0 | Santa Clara, CA | Tim Titus |
| 🟢 | EdgeMarc4500 | 10.100.36.50 | Telnet SSH Web Syslog | | | | | | | | | 4 | 1 | 3 | 1 | Sunnyvale, CA | ttitus@pathsolutions.com |
| Total Devices: | | 16 | Total interfaces: | | | | | | | | | 274 | 106 | 168 | 2 | | |

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

PathSolutions' Network Monitor web pages can be viewed from any standard browser, anywhere on your intranet.

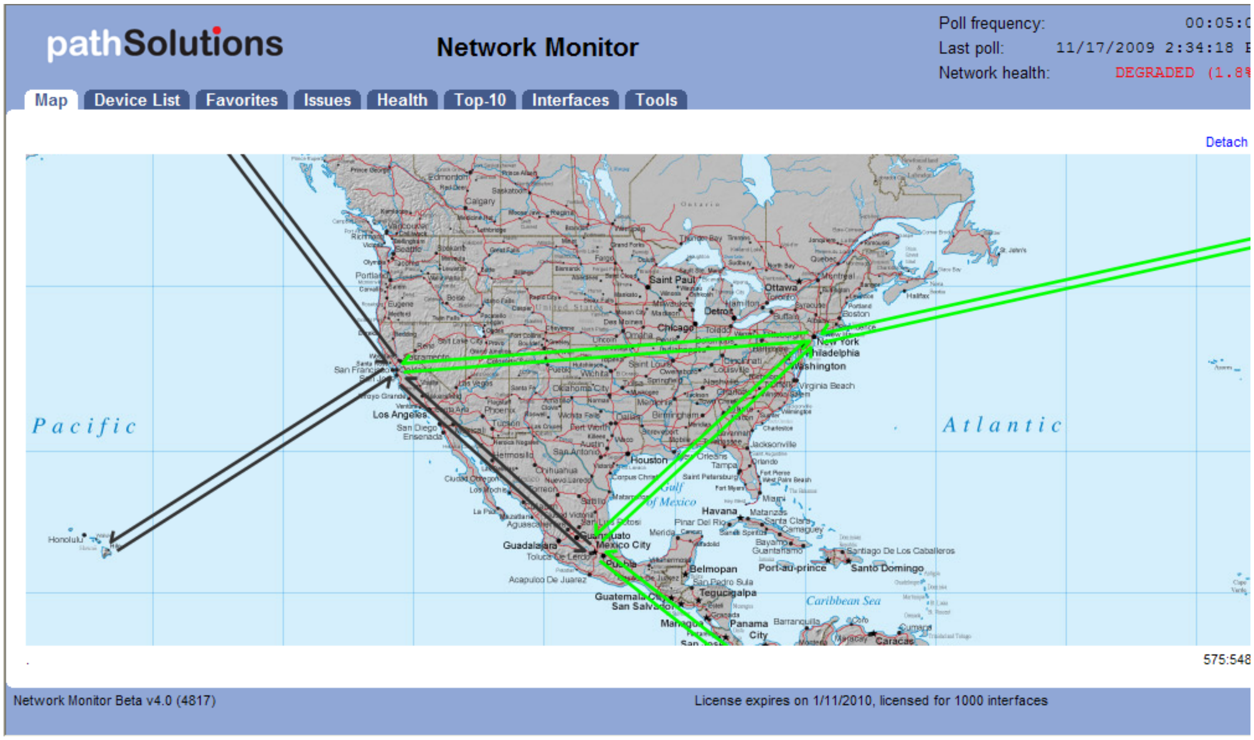
Errors and utilization information is collected for each interface and is presented in a format that allows you to easily determine the source of the problem.

## *Analysis Engine*

The errors are analyzed by an analysis engine that helps to guide you to possible solutions to the problems with each specific interface.  This gives the Network Prescription™ the ability to diagnose the root cause of the problem without having to utilize additional tools or combine datasets from multiple locations.

## *Network Map*

PathSolutions' Network Monitor includes a dynamically updating network map with a click and drag user interface. This capability gives you an "eagle's eye" view of what your network is doing right now.



Poll frequency: 00:05:0

Last poll: 11/17/2009 2:34:18 P

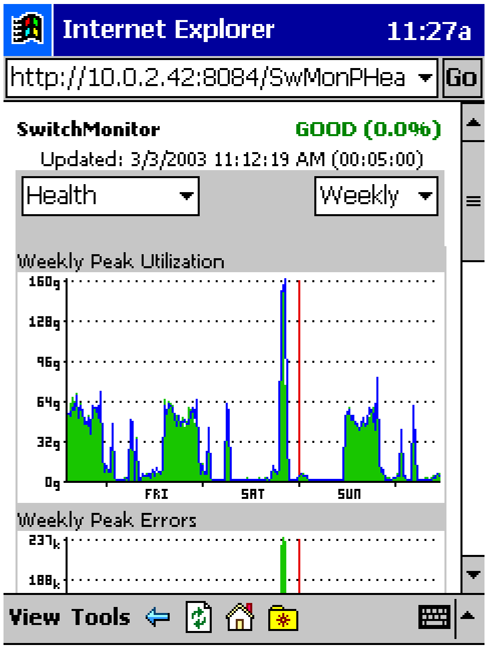
Network health: DEGRADED (1.8%

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

## PocketPC Monitoring

Custom web pages have been created for Microsoft's PocketPC. This allows for a very handy solution, as PocketPCs can be used with wireless Ethernet cards as a portable hand-held network monitoring system.



SwitchMonitor GOOD (0.0%)

Updated: 3/3/2003 11:12:19 AM (00:05:00)

Health ▾ Weekly ▾

## Quick and Easy Installation and Configuration

The initial installation and configuration can be completed in under ten minutes for virtually any sized network with the Quick Config Wizard. This wizard will automatically scan your network and configure PathSolutions' Network Monitor to monitor all of the interfaces that are discovered.

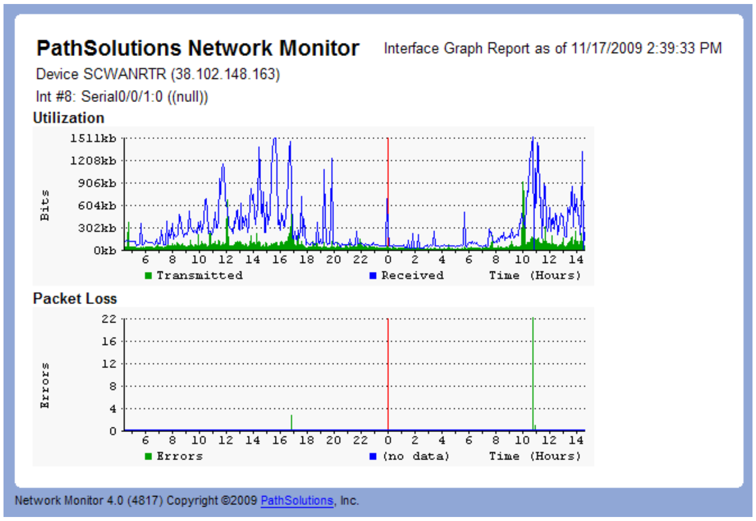
## No Desktop Security Concerns

Running as a Windows 2000/2003/XP service, PathSolutions' Network Monitor provides benefits over console based monitoring tools:

- No need to remain logged in to the console for monitoring to occur
- Desktop resources (desktop real estate and system tray space) on the console are not used

## Rapid Re-Configuration when your Network Changes

When your network changes, and devices are added or removed, you can rapidly update your configuration using the Quick Config Wizard. It will detect new interfaces and include them in your configuration, and start monitoring again.



PathSolutions Network Monitor Interface Graph Report as of 11/17/2009 2:39:33 PM

Device SCWANRTR (38.102.148.163)

Int #8: Serial0/0/1:0 ((null))

Network Monitor 4.0 (4817) Copyright ©2009 PathSolutions, Inc.

## Advanced Email Reporting

Email templates are included for devices, interfaces, and overall health monitoring. Templates can be easily modified to include a variety of data elements.

## Emailed Graphs

Graphs for any interface or device can be included in emailed reports.

## Parent/Child Relationships for Outage Alerting

Parent-Child relationships can be established for each device so alerts are not generated for devices located behind other devices. This insures that you receive outage alerts for only the specific device that went down and not all devices behind that device.

# VoIP Features

When the VoIP module is enabled, additional features become available:

## *Phones Tab*

PathSolutions' VoIP Monitor makes it easy to discover where all of your VoIP phones are connected to the network. The Phones tab shows each phone and the health of the connection to the network.

## *Call Path*

The Call Path feature displays health and configuration information of every link involved in a call from a starting IP address to an ending IP address. This provides unprecedented visibility into any problems that previously occurred on all involved links.

## *Current utilization Call Path*

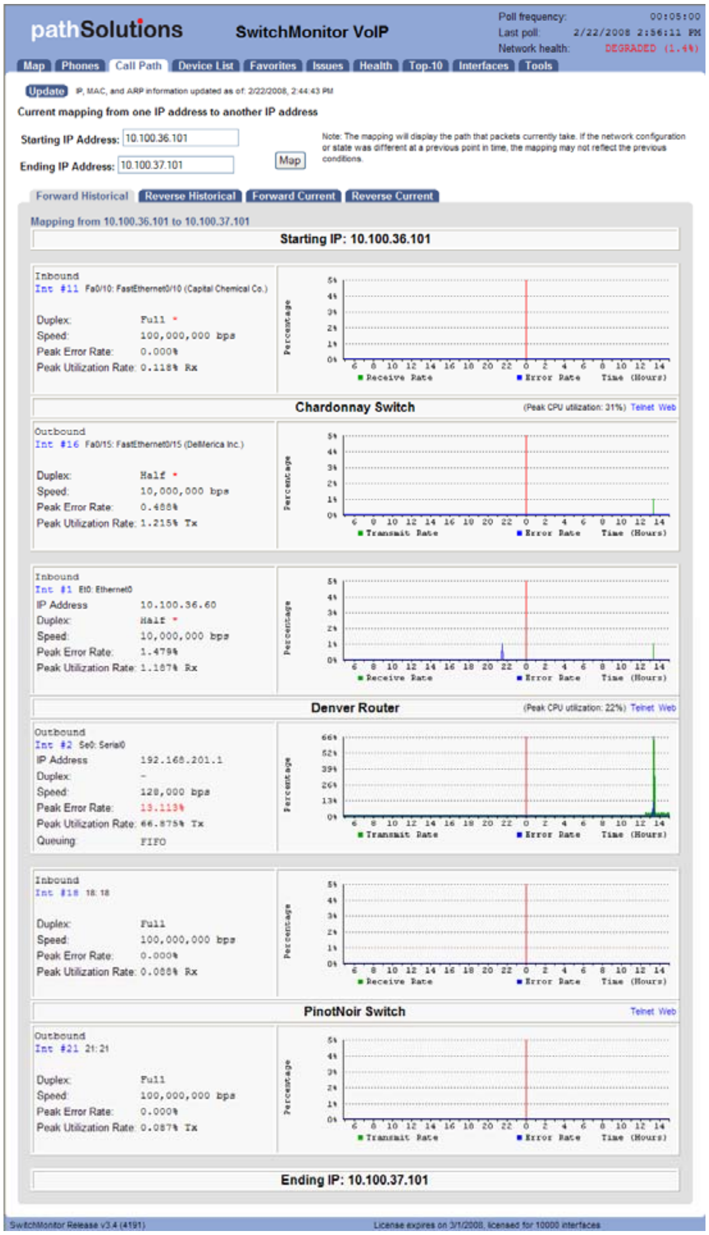
PathSolutions' VoIP Monitor also permits viewing the current utilization of all links between two IP addresses.

Solving call-in-progress problems is now easy because you have visibility into real-time usage information of all involved links.

## *Device Latency, Jitter, Loss, and MOS Score*

PathSolutions' VoIP Monitor is able to provide visibility into the latency, jitter, packet loss, and MOS score for any monitored device.

With this feature, you can monitor network devices that are in remote offices and have continuous visibility into the capabilities of the connection to that office.



Poll frequency: 00:05:00
Last poll: 2/22/2008 2:56:11 PM
Network health: DEGRADED (1.4%)

IP, MAC, and ARP information updated as of: 2/22/2008, 2:44:43 PM

Current mapping from one IP address to another IP address

Starting IP Address: 10.100.36.101
Ending IP Address: 10.100.37.101

Note: The mapping will display the path that packets currently take. If the network configuration or state was different at a previous point in time, the mapping may not reflect the previous conditions.

Mapping from 10.100.36.101 to 10.100.37.101

Starting IP: 10.100.36.101

Inbound
Int #11 Fa0/10: FastEthernet0/10 (Capital Chemical Co.)
Duplex: Full *
Speed: 100,000,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 0.118% Rx

Chardonnay Switch (Peak CPU utilization: 31%)

Outbound
Int #16 Fa0/15: FastEthernet0/15 (DelMerica Inc.)
Duplex: Half *
Speed: 10,000,000 bps
Peak Error Rate: 0.488%
Peak Utilization Rate: 1.215% Tx

Inbound
Int #1 Et0: Ethernet0
IP Address 10.100.36.60
Duplex: Half *
Speed: 10,000,000 bps
Peak Error Rate: 1.479%
Peak Utilization Rate: 1.187% Rx

Denver Router (Peak CPU utilization: 22%)

Outbound
Int #2 Se0: Serial0
IP Address 192.168.201.1
Duplex: -
Speed: 128,000 bps
Peak Error Rate: 13.113%
Peak Utilization Rate: 66.875% Tx
Queuing: FIFO

Inbound
Int #18 18: 18
Duplex: Full
Speed: 100,000,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 0.088% Rx

PinotNoir Switch

Outbound
Int #21 21: 21
Duplex: Full
Speed: 100,000,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 0.087% Tx

Ending IP: 10.100.37.101

SwitchMonitor Release v3.4 (4191)
License expires on 3/1/2008, licensed for 10000 interfaces

## *VoIP Tools*

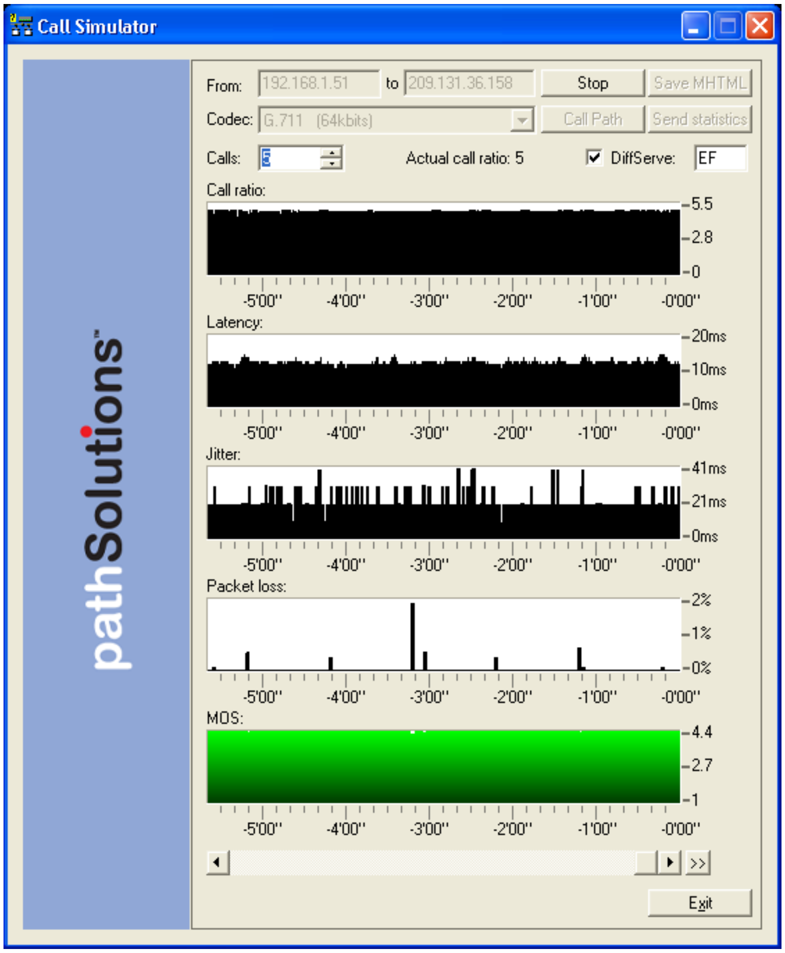
Network Address Translation can cause one-way voice problems. PathSolutions' VoIP Monitor provides a unique tool to help determine if NAT is occurring.

# VoIP Assessment Features

When the VoIP assessment module is added to PathSolutions' VoIP Monitor, additional features become available:

## *Call Simulator*

A Call Simulator is provided to help assess the capability of your network. Various numbers of calls can be simulated and the performance of the network can be evaluated during the simulation.



Call Simulator

From: 192.168.1.51 to 209.131.36.158

Codec: G.711 (64kbits)

Calls: 5 Actual call ratio: 5 ☑ DiffServe: EF

## *Assessment Tab*

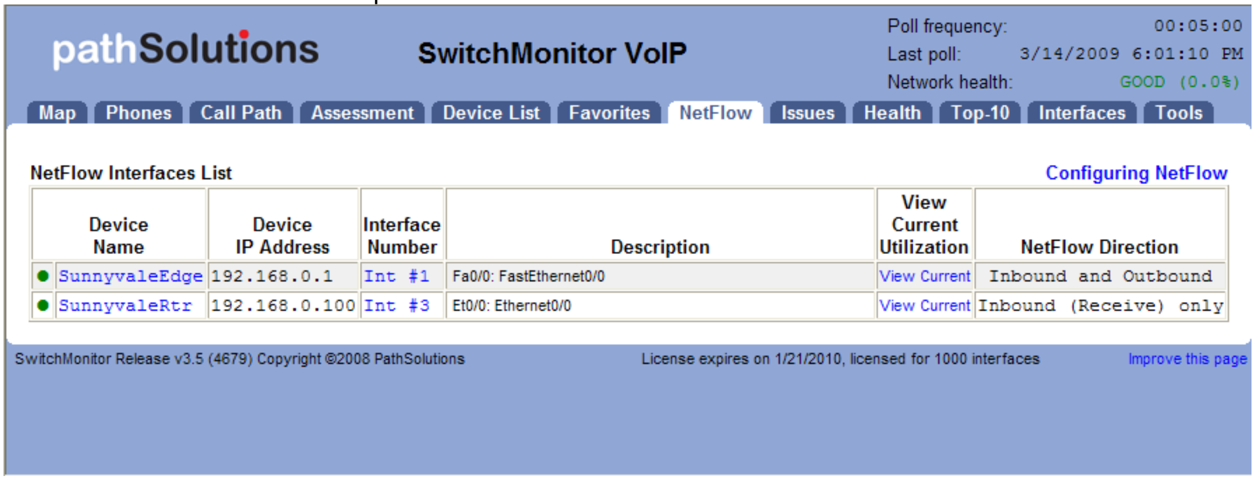
PathSolutions' VoIP Monitor with the assessment module also gives you the ability to acutely analyze your bandwidth constrained links and their QoS configuration on the Assessment tab.

# NetFlow Features

When the NetFlow module is added to PathSolutions Network Monitor, additional features become available:

## *NetFlow Tab*

PathSolutions' Network Monitor with the NetFlow module gives you the ability to instantly know who is using your bandwidth and what they are doing.  This feature is available on any Cisco device with NetFlow enabled to track the top flows.



Poll frequency: 00:05:00
Last poll: 3/14/2009 6:01:10 PM
Network health: GOOD (0.0%)

NetFlow Interfaces List

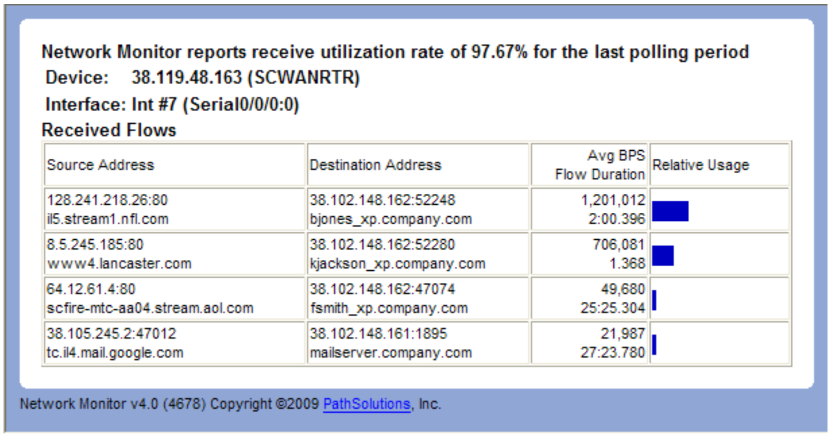
| Device Name | Device IP Address | Interface Number | Description | View Current Utilization | NetFlow Direction |
|---|---|---|---|---|---|
| ● SunnyvaleEdge | 192.168.0.1 | Int #1 | Fa0/0: FastEthernet0/0 | View Current | Inbound and Outbound |
| ● SunnyvaleRtr | 192.168.0.100 | Int #3 | Et0/0: Ethernet0/0 | View Current | Inbound (Receive) only |

SwitchMonitor Release v3.5 (4679) Copyright ©2008 PathSolutions

License expires on 1/21/2010, licensed for 1000 interfaces

## *NetFlow High Utilization Alerts*

If a utilization alert is sent for an interface that has NetFlow enabled, the utilization alert will include the top flows and reverse DNS information so it's easy to determine what's causing the high utilization condition.



Network Monitor reports receive utilization rate of 97.67% for the last polling period

Device: 38.119.48.163 (SCWANRTR)

Interface: Int #7 (Serial0/0/0:0)

Received Flows

| Source Address | Destination Address | Avg BPS<br>Flow Duration | Relative Usage |
|---|---|---|---|
| 128.241.218.26:80<br>il5.stream1.nfl.com | 38.102.148.162:52248<br>bjones_xp.company.com | 1,201,012<br>2:00.396 | ▇▇▇ |
| 8.5.245.185:80<br>www4.lancaster.com | 38.102.148.162:52280<br>kjackson_xp.company.com | 706,081<br>1.368 | ▇▇ |
| 64.12.61.4:80<br>scfire-mtc-aa04.stream.aol.com | 38.102.148.162:47074<br>fsmith_xp.company.com | 49,680<br>25:25.304 | ▏ |
| 38.105.245.2:47012<br>tc.il4.mail.google.com | 38.102.148.161:1895<br>mailserver.company.com | 21,987<br>27:23.780 | ▏ |

Network Monitor v4.0 (4678) Copyright ©2009 PathSolutions, Inc.

# Requirements

The PathSolutions' Network Monitor service installs on a Windows (2000/2003/XP) server (or workstation acting as a server), and can be viewed from web browsers on the network. The following are requirements for the server, and the client web browser.

## *Server Requirements*

The system requirements may be low, depending on the size of your network. As your network grows, you may need to increase the base system requirements.

### Small Network Server Requirements

For networks with less than 1,000 total interfaces, the following hardware requirements are required:

- ✓ Pentium 200 MHz processor or faster
- ✓ 40 MB of free disk space
- ✓ 256 MB of RAM for the service (512 MB RAM minimum for the server)
- ✓ 100 MBPS Network Interface Card
- ✓ Operating systems: Windows 2000 Server/Advanced Server

  Windows 2000 Professional
  Windows XP Professional
  Windows Server 2003
  Windows Server 2008

### Medium Network Server Requirements

For networks with more than 1,000 interfaces, but less than 10,000 interfaces, the following hardware requirements are suggested:

- ✓ Pentium 800 MHz processor or faster
- ✓ 1 GB of free disk space
- ✓ 1 GB of RAM for the service (2 GB RAM minimum for the server)
- ✓ 100 MBPS Network Interface Card
- ✓ Operating systems: Windows 2000 Server/Advanced Server

  Windows 2000 Professional
  Windows XP Professional
  Windows Server 2003
  Windows Server 2008

### Large Network Server Requirements

For networks with more than 10,000 interfaces, the following hardware requirements are suggested:

- ✓ Pentium 1 GHz processor or faster
- ✓ 10 GB of free disk space
- ✓ 3 GB of RAM for the service (4 GB RAM minimum for the server)
- ✓ 100 MBPS Network Interface Card, configured for full-duplex operation
- ✓ 15,000k rpm hard drive
- ✓ Operating systems: Windows 2000 Advanced Server

  Windows Server 2003
  Windows Server 2008

## Web Browser Minimum Client Requirements

The client requirements are as follows:

- ✓ Internet Explorer v6.0 or later
- ✓ 64 MB of RAM
- ✓ 100 MBPS Network Interface Card
- ✓ Pentium 200 MHz processor or faster

## PocketPC Browser Minimum Client Requirements

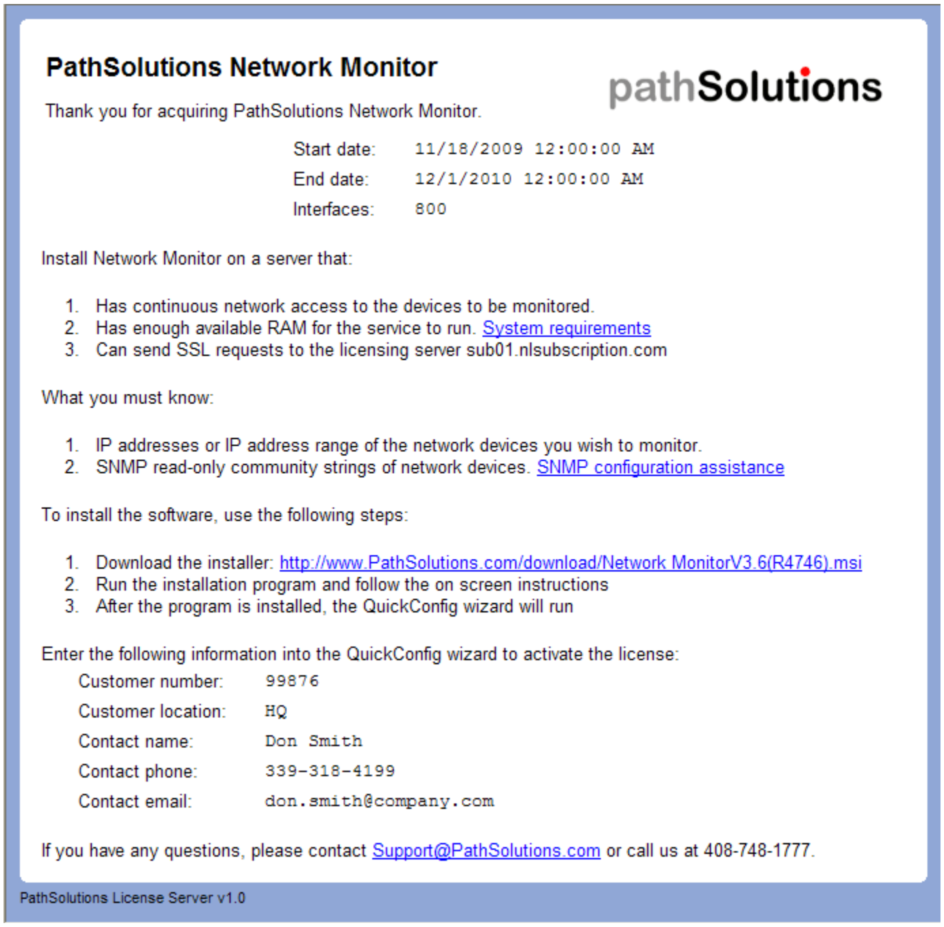
The PocketPC client requirements are as follows:

- ✓ Microsoft PocketPC or later
- ✓ Pocket IE
- ✓ Any IP Network connection (wireless recommended)

# Installation

Installation and configuration of PathSolutions' Network Monitor takes less than 30 minutes for most networks.

You must have a valid PathSolutions' Network Monitor license to use the software. This will usually arrive in the form of an email from PathSolutions:



**PathSolutions Network Monitor**

Thank you for acquiring PathSolutions Network Monitor.

Start date: 11/18/2009 12:00:00 AM
End date: 12/1/2010 12:00:00 AM
Interfaces: 800

Install Network Monitor on a server that:

1. Has continuous network access to the devices to be monitored.
2. Has enough available RAM for the service to run. System requirements
3. Can send SSL requests to the licensing server sub01.nlsubscription.com

What you must know:

1. IP addresses or IP address range of the network devices you wish to monitor.
2. SNMP read-only community strings of network devices. SNMP configuration assistance

To install the software, use the following steps:

1. Download the installer: http://www.PathSolutions.com/download/Network MonitorV3.6(R4746).msi
2. Run the installation program and follow the on screen instructions
3. After the program is installed, the QuickConfig wizard will run

Enter the following information into the QuickConfig wizard to activate the license:

Customer number: 99876
Customer location: HQ
Contact name: Don Smith
Contact phone: 339-318-4199
Contact email: don.smith@company.com

If you have any questions, please contact Support@PathSolutions.com or call us at 408-748-1777.

PathSolutions License Server v1.0

License information can be obtained from your PathSolutions reseller, or directly from PathSolutions.

PathSolutions license support: 1-877-748-1777
Support@PathSolutions.com

To set up PathSolutions' Network Monitor on your machine, use the provided link in the email to download the latest version from the PathSolutions website.

PathSolutions' Network Monitor should be installed on a server or workstation that has a permanent connection to the network.

Double-click on the installation program and follow the instructions on the screen.  The Quick Config Wizard will auto-configure PathSolutions' Network Monitor for your network and begin monitoring in just a few minutes.

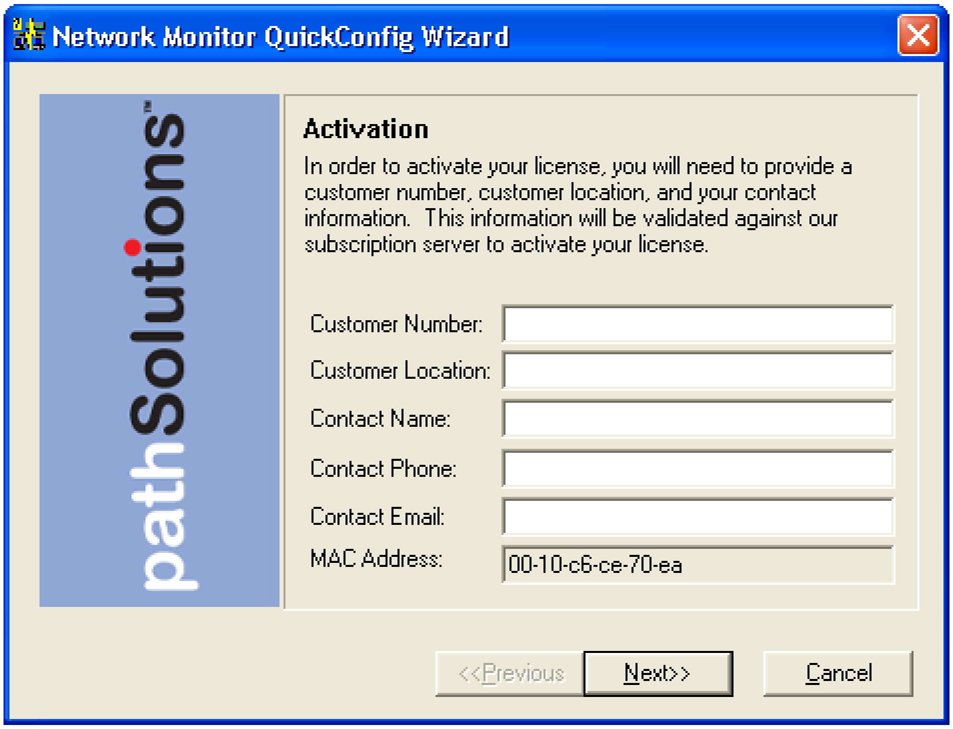
The QuickConfig Wizard has six steps:

Step 1: Activation
Step 2: Switch Configurations
Step 3: Network Address Ranges
Step 4: SNMP Community Strings
Step 5: Issue Thresholds
Step 6: Emailed Reports

After installation is complete, PathSolutions' Network Monitor will scan your network for devices and begin monitoring.

### *Step 1: Activation*

The first step will ask you to enter your subscription information to activate the subscription.



**Activation**

In order to activate your license, you will need to provide a customer number, customer location, and your contact information.  This information will be validated against our subscription server to activate your license.

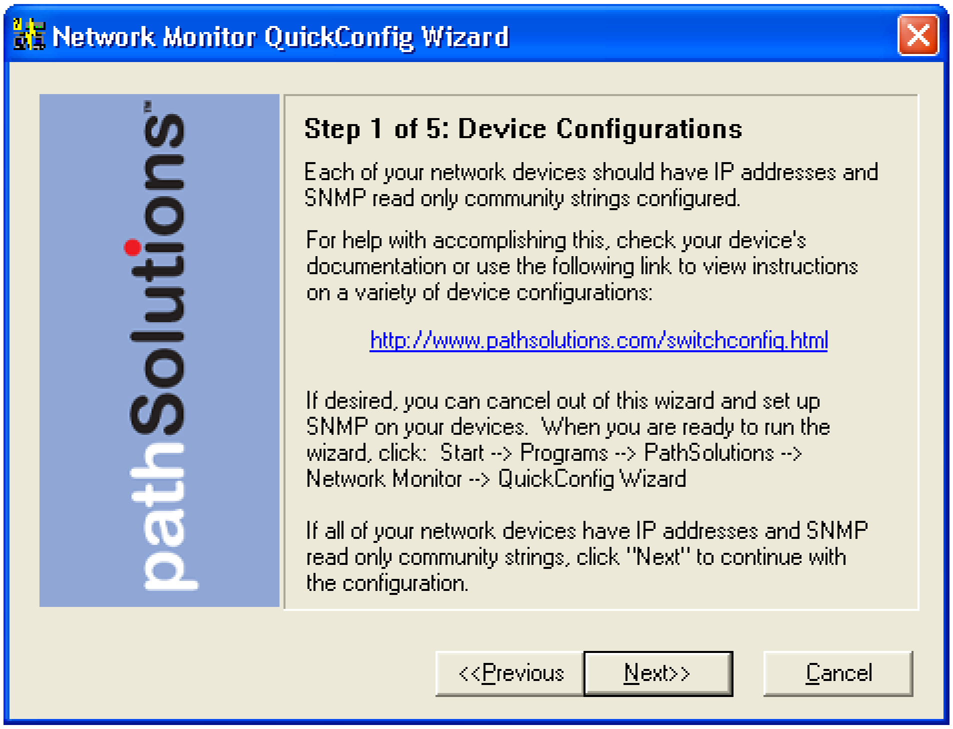
| | |
|---|---|
| Customer Number: | |
| Customer Location: | |
| Contact Name: | |
| Contact Phone: | |
| Contact Email: | |
| MAC Address: | 00-10-c6-ce-70-ea |

Enter all fields from your subscription email.

**Note:** Customer Number and Customer Location fields are case sensitive. These fields must be entered exactly as they are specified in the subscription email.

### *Step 2: Switch Configurations*

The second step will ask you to make sure that your network switches have IP addresses and SNMP read only community strings configured:



**Step 1 of 5: Device Configurations**

Each of your network devices should have IP addresses and SNMP read only community strings configured.

For help with accomplishing this, check your device's documentation or use the following link to view instructions on a variety of device configurations:

http://www.pathsolutions.com/switchconfig.html

If desired, you can cancel out of this wizard and set up SNMP on your devices. When you are ready to run the wizard, click: Start --> Programs --> PathSolutions --> Network Monitor --> QuickConfig Wizard

If all of your network devices have IP addresses and SNMP read only community strings, click "Next" to continue with the configuration.

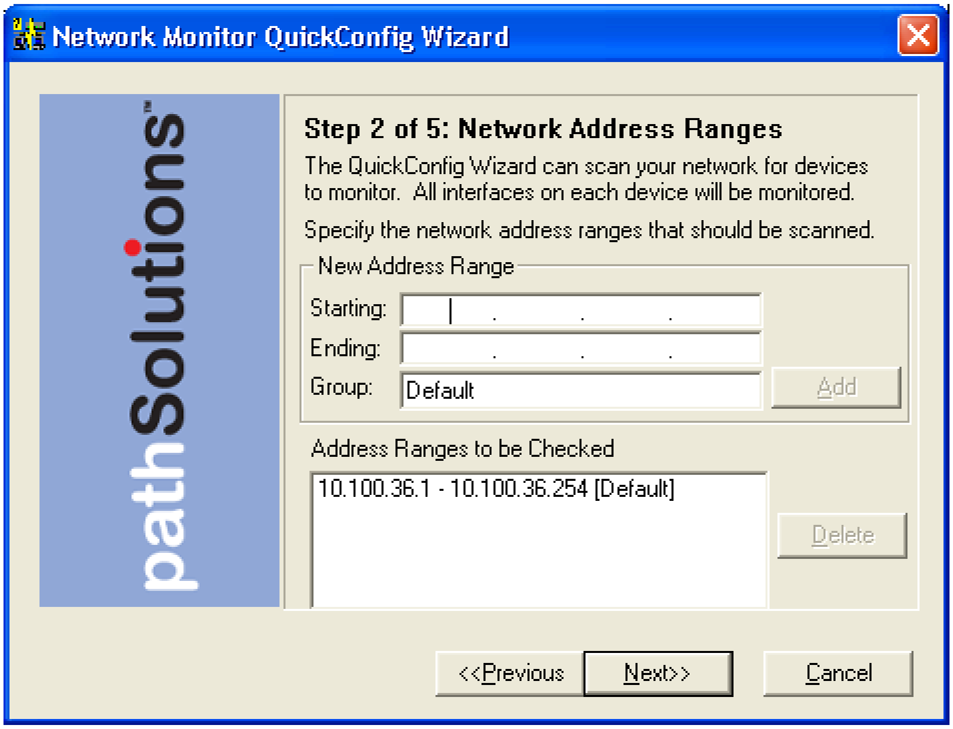
If you need assistance setting up IP addresses and SNMP read only community strings (passwords), click on the provided link, or refer to Appendix B.

**Note:** It is strongly recommended to not use "public" or "private" as the SNMP community strings, as they constitute easily guessable passwords.

Once all of your switches are configured with IP addresses and SNMP read only community strings, click "Next" to continue.

### *Step 3: Network Address Ranges*

The third step allows you to specify the network range or ranges that should be scanned to discover network devices such as switches and routers.



Step 2 of 5: Network Address Ranges

The QuickConfig Wizard can scan your network for devices to monitor. All interfaces on each device will be monitored.

Specify the network address ranges that should be scanned.

New Address Range

Starting: . . .

Ending: . . .

Group: Default

Address Ranges to be Checked

10.100.36.1 - 10.100.36.254 [Default]

Enter a starting IP address and an ending IP address for each network range that should be scanned. A group name can be assigned to each IP address range that is added.

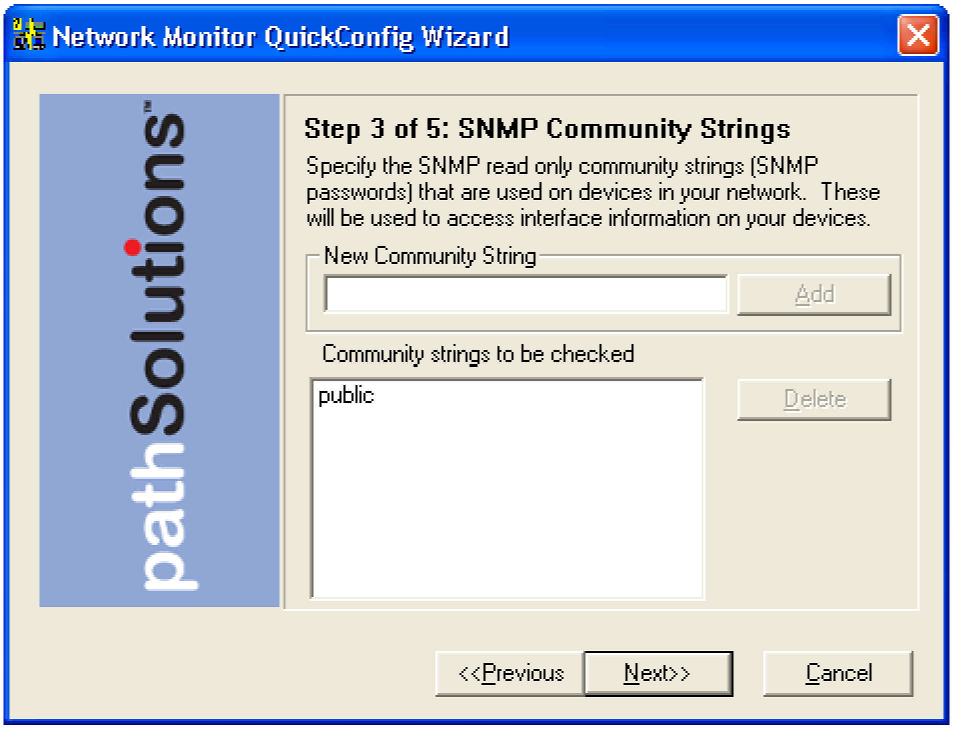
**Note:** Run the Quick Config Wizard once with just a couple of subnets and notice the results. Then you can re-run the Quick Config Wizard and add successive subnets.

**Note:** The list of what PathSolutions' Network Monitor discovers can be examined and adjusted with the PathSolutions' Network Monitor Configuration Tool.

Click "Next" to continue.

### *Step 4: SNMP Community Strings*

The fourth step allows you to select what SNMP read only community strings should be used with this scan.



Step 3 of 5: SNMP Community Strings

Specify the SNMP read only community strings (SNMP passwords) that are used on devices in your network. These will be used to access interface information on your devices.

New Community String

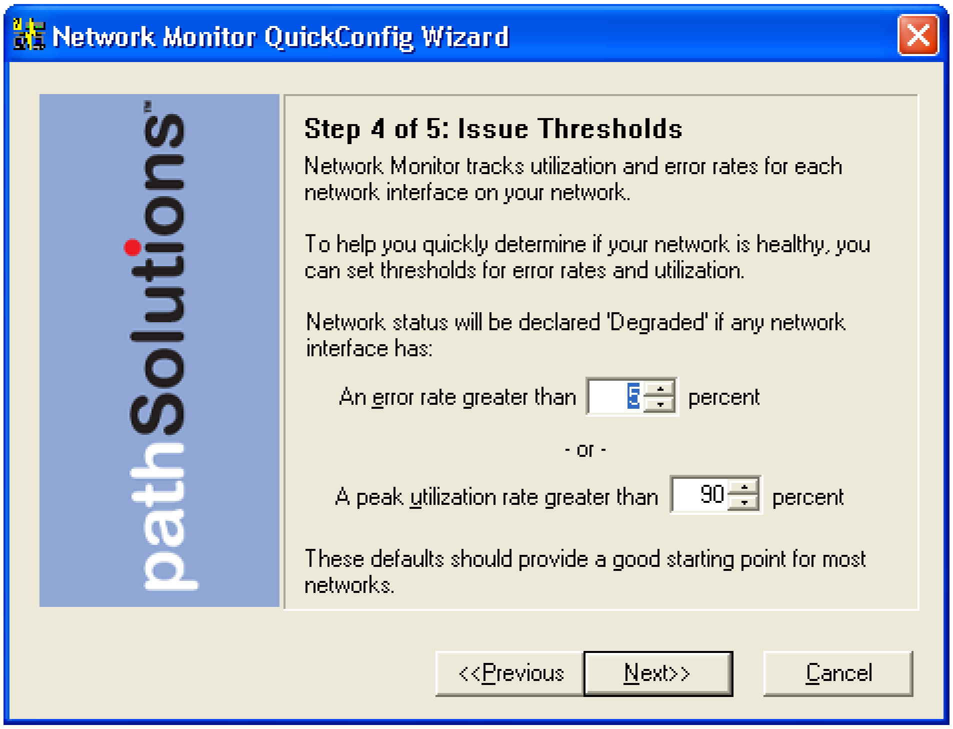
Community strings to be checked

public

Enter all of the SNMP read-only community strings that are used in your network to help ensure that network devices are correctly identified.
Click "Next" to continue.

### *Step 5: Issue Thresholds*

The fourth step will ask what thresholds to use for determining if your network is healthy or not:



**Step 4 of 5: Issue Thresholds**

Network Monitor tracks utilization and error rates for each network interface on your network.

To help you quickly determine if your network is healthy, you can set thresholds for error rates and utilization.

Network status will be declared 'Degraded' if any network interface has:

An error rate greater than 5 percent

- or -

A peak utilization rate greater than 90 percent

These defaults should provide a good starting point for most networks.

If an interface has an error rate higher than 10%, network status will be changed to 'Degraded'.

If an interface has a peak utilization rate (transmitted or received) over 80%, network status will be changed to 'Degraded'.

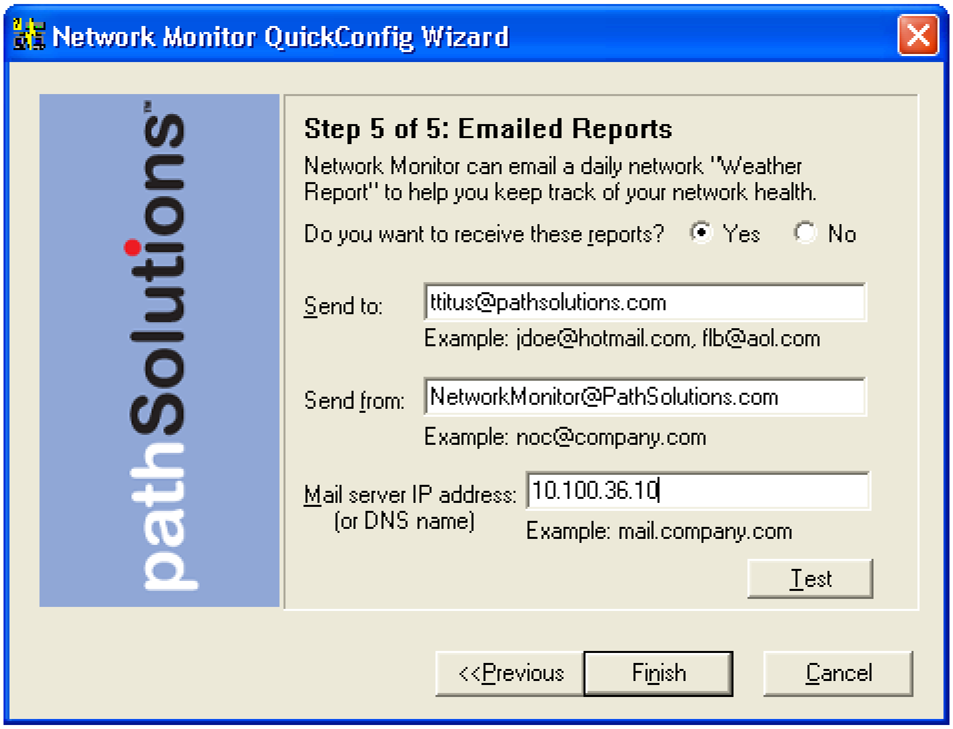
These numbers can be adjusted to suit your specific network environment, and your tolerance for errors.

The default values are 10% error rate, and 80% peak utilization rate.

Click "Next" to continue.

### Step 6: Emailed Reports

The sixth step will ask if you want to receive daily emailed network 'Weather Reports':



**Step 5 of 5: Emailed Reports**

Network Monitor can email a daily network "Weather Report" to help you keep track of your network health.

Do you want to receive these reports? ● Yes ○ No

Send to: ttitus@pathsolutions.com

Example: jdoe@hotmail.com, flb@aol.com

Send from: NetworkMonitor@PathSolutions.com

Example: noc@company.com

Mail server IP address: (or DNS name) 10.100.36.10

Example: mail.company.com

Enter the Internet SMTP email addresses that should receive the daily report. You can enter multiple email addresses by using a semicolon, comma or space character between each email address.

Enter the email address that these messages should be sent from (make sure to use an Internet SMTP email address -- e.g. bob@company.com). If the email address does not exist, the email will bounce back to the "Send from" user's mailbox.

You will need to enter the IP address or DNS hostname of your SMTP mail server address. This mail server should allow SMTP forwarding if you intend to send to individuals at other domain names. See the appendix for additional information on SMTP email forwarding.

After entering this information, you can click "Test" to send a test email. If there is a problem sending an email, you will be presented with detailed information how to resolve the problem.

Click "Finish" to complete the wizard.

After clicking "Finish", the wizard will scan the network ranges for network devices that support SNMP. The monitoring service will be started, and you will be presented with a web page displaying which devices are being monitored.

That is all that is necessary to install and configure the program. You should be able to immediately analyze errors on your network.

The network Weather Report emails are sent out at midnight local time, detailing the status of your network for the previous day.

# Re-Configuring when your Network Changes

If you have new interfaces on your network, or want to quickly remove old devices from the configuration, you can re-run the Quick Config Wizard to scan your network and determine what changes have occurred.

To re-run the Quick Config Wizard, click on "Start", choose "Programs", then "PathSolutions", and "PathSolutions’ Network Monitor", and "Quick Config Wizard".

You don't have to change any configurations already set with the Quick Config Wizard.  Just click "Next" to every screen and the network will be scanned for new interfaces.

# Automatic Re-Configuration

The Quick Config wizard can be run in automatic mode from a scheduled task if it is desired for new devices to be automatically discovered on a regular basis.

```
MonitorWizard.exe /a
```

When run in automatic mode, the program will not ask any questions but will scan the previous IP address ranges and use the previous SNMP community strings and add any new devices to the service. The service will then be stopped and then re-started to have the new devices added.

To change what IP address ranges and SNMP community strings are used in the automatic scan, edit the wizard.ini file:

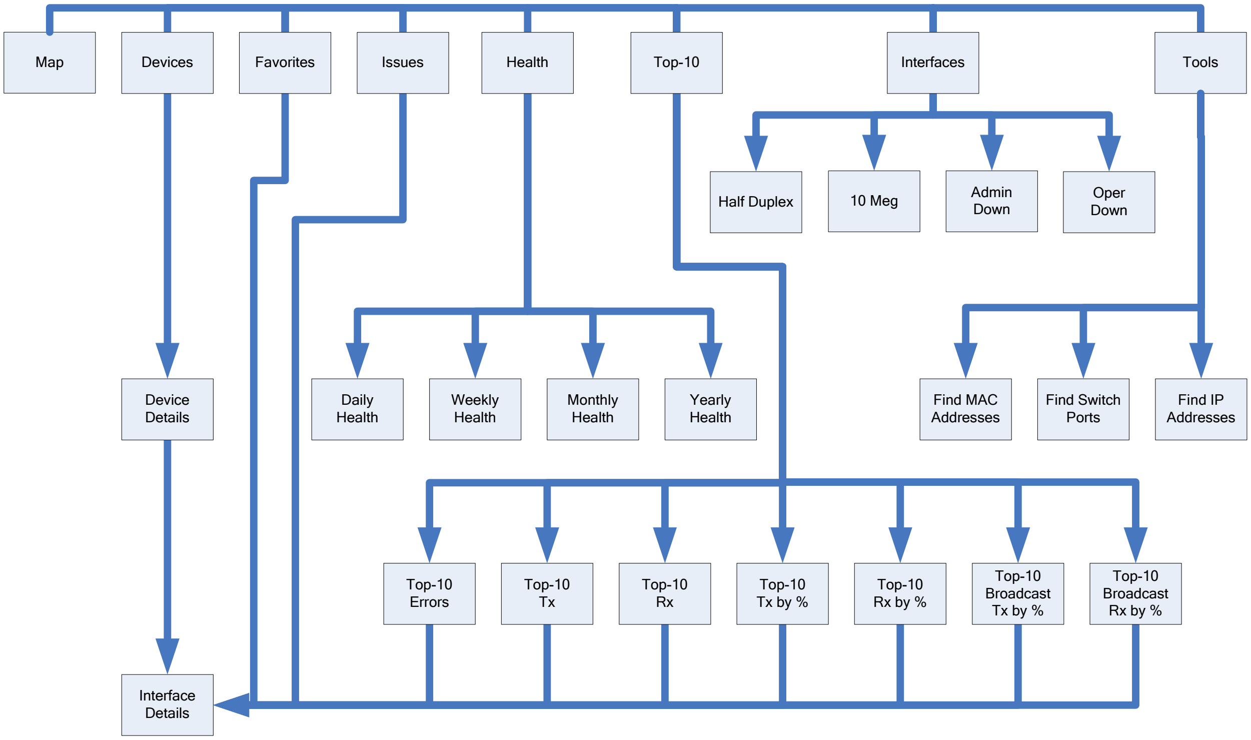
```
/#10.100.36.1 - 10.100.36.254 [Default]/
/#10.100.37.1 - 10.100.37.254 [Default]/
/#192.168.201.1 - 192.168.201.10 [Edge Network]/
/#192.168.202.1 - 192.168.202.10 [Edge Network]/
/public/
```

Make sure all slashes ‘/’ and pound signs ‘#’ are maintained.

# Using the Web Interface

## Navigation Map

The PathSolutions' Network Monitor web layout is easy to follow, and easy to navigate between switches and interfaces.



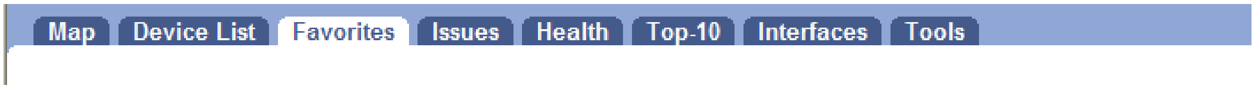
The top row of the navigation map includes a number of tabs that define different areas of the product.

## Web Page Headers

At the top of each web page, general information is displayed: Polling Frequency, Last Poll Time, and Network Health.

## Tabs

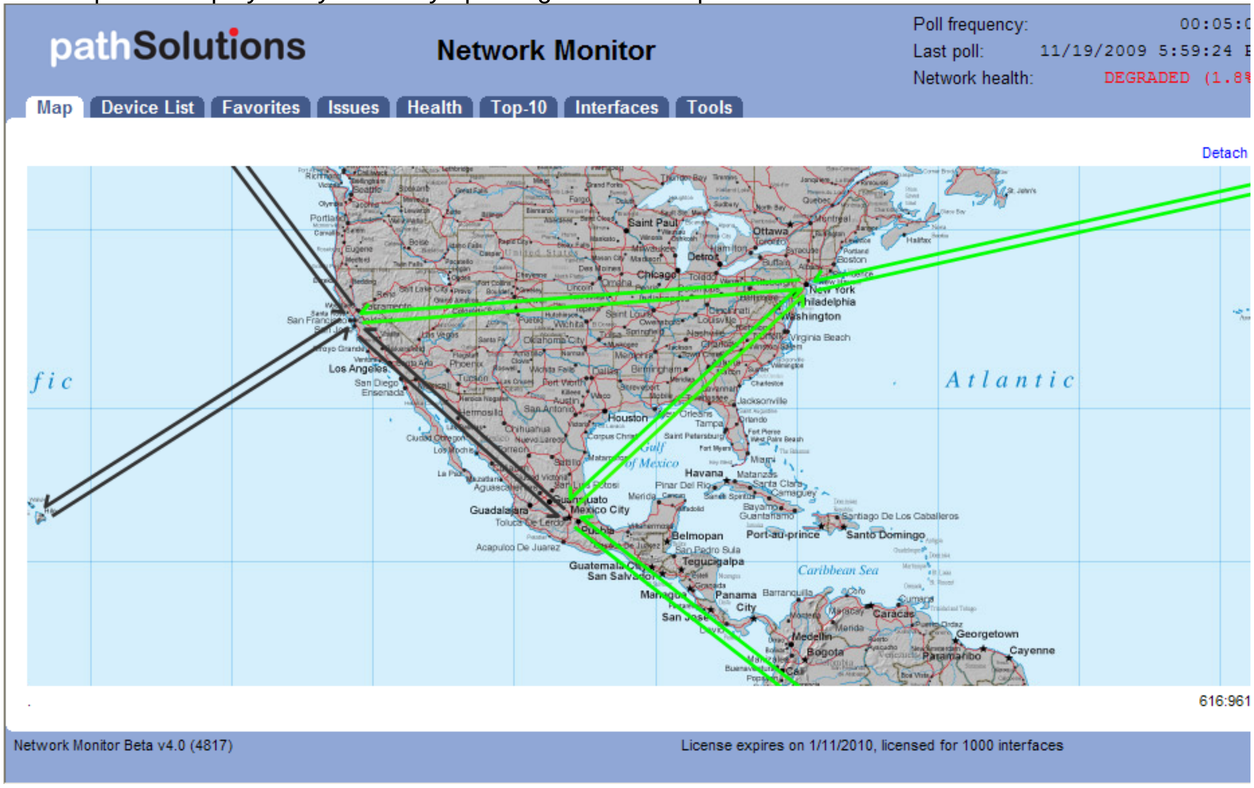
Navigating using the web interface is accomplished by using the tabs at the top of the web page:



Each tab covers a specific area relating to the health of your network.

## Map

The Map view displays a dynamically updating network map.



Network Monitor

Poll frequency: 00:05:0

Last poll: 11/19/2009 5:59:24 P

Network health: DEGRADED (1.8%

616:961

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

Links can be added to this map via the configuration tool. To pinpoint locations for adding lines, use the X,Y coordinates indicated in the lower right corner of the web page.

To pan around the map, simply click and drag anywhere on the background of the map.

Click on any line to display a daily graph for the monitored interface.

You can use the “Detach” link in the upper right corner to open a detached view of the network map for full page viewing.

Legend

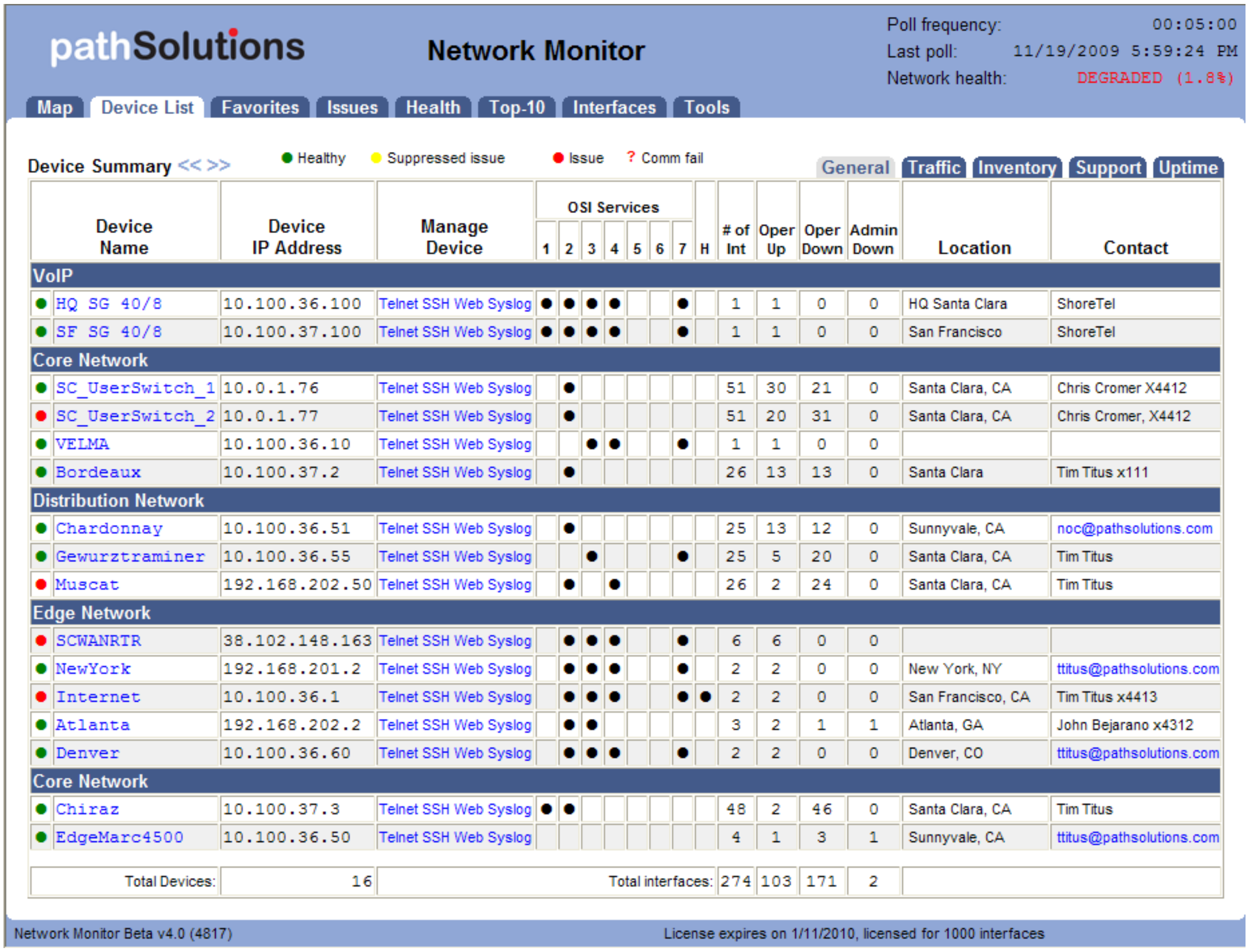
| Line Color | Description |
|---|---|
| Green | <10% utilized |
| Yellow | ~50% utilized |
| Red | >90% utilized |
| Black | Interface is down |
| White | Communication failure (could not read interface status) |

## *Device List*

The Device List view shows you a list of your monitored network devices and information about each.

### General Sub-tab

The “General” sub-tab allows you to manage the device as well as learn about the device capabilities.



pathSolutions Network Monitor

Poll frequency: 00:05:00
Last poll: 11/19/2009 5:59:24 PM
Network health: DEGRADED (1.8%)

Device Summary << >>   🟢 Healthy   🟡 Suppressed issue   🔴 Issue   ? Comm fail

| | Device Name | Device IP Address | Manage Device | OSI Services | | | | | | | | # of Int | Oper Up | Oper Down | Admin Down | Location | Contact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | H | | | | | | |
| VoIP | | | | | | | | | | | | | | | | | |
| 🟢 | HQ SG 40/8 | 10.100.36.100 | Telnet SSH Web Syslog | ● | ● | ● | ● | | | ● | | 1 | 1 | 0 | 0 | HQ Santa Clara | ShoreTel |
| 🟢 | SF SG 40/8 | 10.100.37.100 | Telnet SSH Web Syslog | ● | ● | ● | ● | | | ● | | 1 | 1 | 0 | 0 | San Francisco | ShoreTel |
| Core Network | | | | | | | | | | | | | | | | | |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Telnet SSH Web Syslog | | ● | | | | | | | 51 | 30 | 21 | 0 | Santa Clara, CA | Chris Cromer X4412 |
| 🔴 | SC_UserSwitch_2 | 10.0.1.77 | Telnet SSH Web Syslog | | ● | | | | | | | 51 | 20 | 31 | 0 | Santa Clara, CA | Chris Cromer, X4412 |
| 🟢 | VELMA | 10.100.36.10 | Telnet SSH Web Syslog | | | ● | ● | | | ● | | 1 | 1 | 0 | 0 | | |
| 🟢 | Bordeaux | 10.100.37.2 | Telnet SSH Web Syslog | | ● | | | | | | | 26 | 13 | 13 | 0 | Santa Clara | Tim Titus x111 |
| Distribution Network | | | | | | | | | | | | | | | | | |
| 🟢 | Chardonnay | 10.100.36.51 | Telnet SSH Web Syslog | | ● | | | | | | | 25 | 13 | 12 | 0 | Sunnyvale, CA | noc@pathsolutions.com |
| 🟢 | Gewurztraminer | 10.100.36.55 | Telnet SSH Web Syslog | | | ● | | | | ● | | 25 | 5 | 20 | 0 | Santa Clara, CA | Tim Titus |
| 🔴 | Muscat | 192.168.202.50 | Telnet SSH Web Syslog | | ● | | ● | | | | | 26 | 2 | 24 | 0 | Santa Clara, CA | Tim Titus |
| Edge Network | | | | | | | | | | | | | | | | | |
| 🔴 | SCWANRTR | 38.102.148.163 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 6 | 6 | 0 | 0 | | |
| 🟢 | NewYork | 192.168.201.2 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 2 | 2 | 0 | 0 | New York, NY | ttitus@pathsolutions.com |
| 🔴 | Internet | 10.100.36.1 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | ● | 2 | 2 | 0 | 0 | San Francisco, CA | Tim Titus x4413 |
| 🟢 | Atlanta | 192.168.202.2 | Telnet SSH Web Syslog | | ● | ● | | | | | | 3 | 2 | 1 | 1 | Atlanta, GA | John Bejarano x4312 |
| 🟢 | Denver | 10.100.36.60 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 2 | 2 | 0 | 0 | Denver, CO | ttitus@pathsolutions.com |
| Core Network | | | | | | | | | | | | | | | | | |
| 🟢 | Chiraz | 10.100.37.3 | Telnet SSH Web Syslog | ● | ● | | | | | | | 48 | 2 | 46 | 0 | Santa Clara, CA | Tim Titus |
| 🟢 | EdgeMarc4500 | 10.100.36.50 | Telnet SSH Web Syslog | | | | | | | | | 4 | 1 | 3 | 1 | Sunnyvale, CA | ttitus@pathsolutions.com |
| | Total Devices: | 16 | Total interfaces: | | | | | | | | | 274 | 103 | 171 | 2 | | |

Network Monitor Beta v4.0 (4817)   License expires on 1/11/2010, licensed for 1000 interfaces

The first column includes a red or green status indicator. If a device has an interface that is degraded (utilization or error rate is higher than the configured threshold), the status for the device will be red.

The name of the device (programmed into the switch as the system name, hostname, or sysName) is displayed in the second column. To change this, you should login to the device and change the device’s internal name (hostname) or "sysName". Refer to the device manufacturer’s documentation to determine how to change this information.

If you click on the device name, it will link to a summary of the device, listing all of the interfaces that exist on the device, along with detailed information about the device. Refer to the "Interface Summary" section for more information about this page.

The managed IP address of the device is listed in the third column.

The fourth column includes links to telnet and web into the device, as well as the syslog information received from the device.

The fifth column includes information relating to the OSI services that the device provides. A layer-2 switch would display as providing OSI layer 2 services. A router would display as providing layer 2 and layer 3 services.

The sixth column displays the total number of interfaces on the device.

The seventh column displays the total number of operationally shut down interfaces on the device. These interfaces are not in-use, and will have an inactive link light.

The eighth column displays the total number of administratively shut down interfaces on the device. These interfaces have been manually disabled by the network administrator and will not function if a node is connected to the interface.

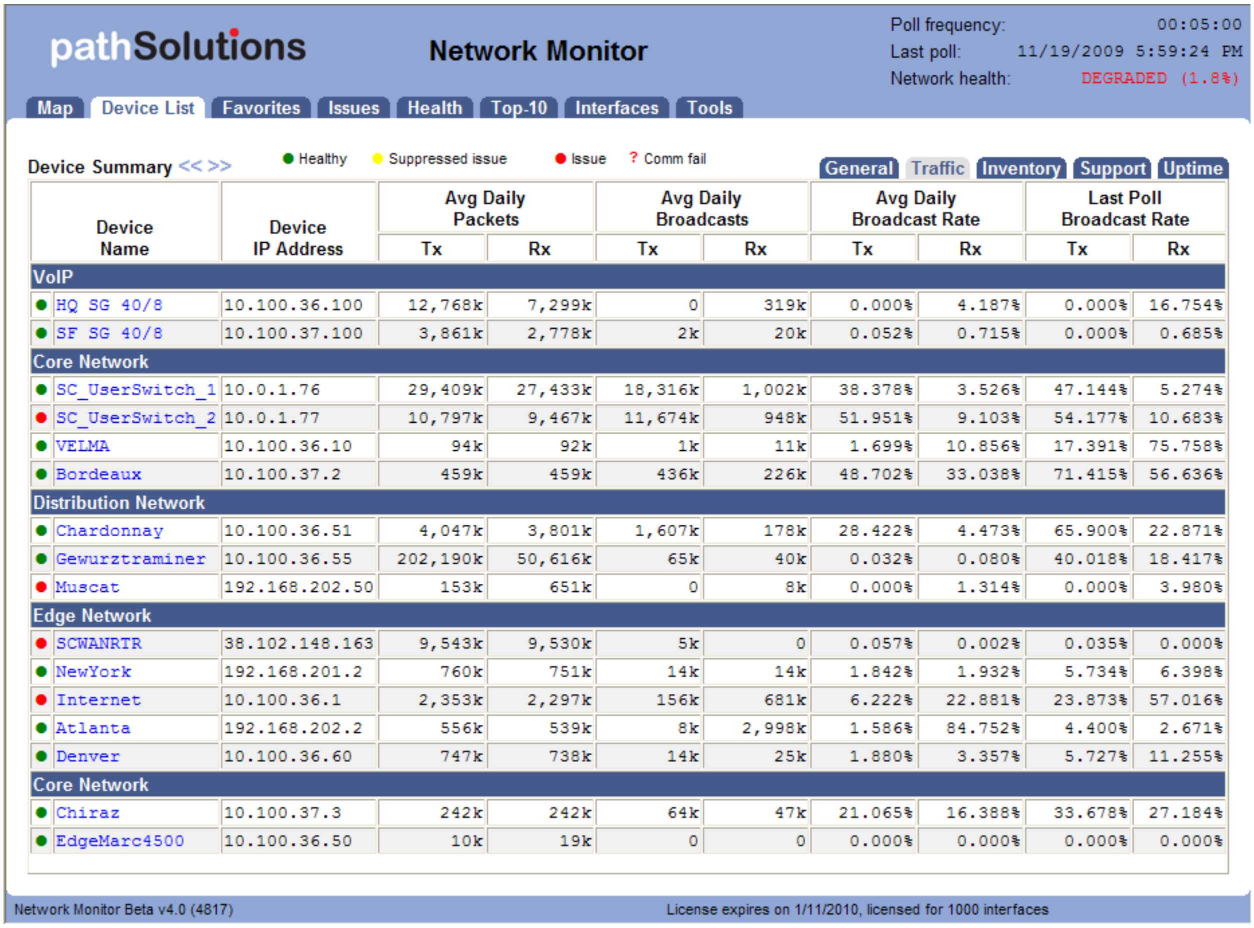
The ninth column of information displays the location of the device. This information is configured on the switch as the location or "sysLocation" of the device. Refer to the device manufacturer's documentation to determine how to change this information.

The tenth column of information displays the contact for the device. This information is configured on the device as the contact or "sysContact" of the switch. Refer to the device manufacturer's documentation to determine how to change this information.

**Note:** If PathSolutions' Network Monitor reads an email address in the sysContact field, it will create a web link to the email address.

## Traffic Sub-tab

The “Traffic” sub-tab displays information about the device’s packets and broadcasts seen:



Poll frequency: 00:05:00
Last poll: 11/19/2009 5:59:24 PM
Network health: DEGRADED (1.8%)

Device Summary

| | Device Name | Device IP Address | Avg Daily Packets | | Avg Daily Broadcasts | | Avg Daily Broadcast Rate | | Last Poll Broadcast Rate | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx |
| VoIP | | | | | | | | | | |
| ● | HQ SG 40/8 | 10.100.36.100 | 12,768k | 7,299k | 0 | 319k | 0.000% | 4.187% | 0.000% | 16.754% |
| ● | SF SG 40/8 | 10.100.37.100 | 3,861k | 2,778k | 2k | 20k | 0.052% | 0.715% | 0.000% | 0.685% |
| Core Network | | | | | | | | | | |
| ● | SC_UserSwitch_1 | 10.0.1.76 | 29,409k | 27,433k | 18,316k | 1,002k | 38.378% | 3.526% | 47.144% | 5.274% |
| ● | SC_UserSwitch_2 | 10.0.1.77 | 10,797k | 9,467k | 11,674k | 948k | 51.951% | 9.103% | 54.177% | 10.683% |
| ● | VELMA | 10.100.36.10 | 94k | 92k | 1k | 11k | 1.699% | 10.856% | 17.391% | 75.758% |
| ● | Bordeaux | 10.100.37.2 | 459k | 459k | 436k | 226k | 48.702% | 33.038% | 71.415% | 56.636% |
| Distribution Network | | | | | | | | | | |
| ● | Chardonnay | 10.100.36.51 | 4,047k | 3,801k | 1,607k | 178k | 28.422% | 4.473% | 65.900% | 22.871% |
| ● | Gewurztraminer | 10.100.36.55 | 202,190k | 50,616k | 65k | 40k | 0.032% | 0.080% | 40.018% | 18.417% |
| ● | Muscat | 192.168.202.50 | 153k | 651k | 0 | 8k | 0.000% | 1.314% | 0.000% | 3.980% |
| Edge Network | | | | | | | | | | |
| ● | SCWANRTR | 38.102.148.163 | 9,543k | 9,530k | 5k | 0 | 0.057% | 0.002% | 0.035% | 0.000% |
| ● | NewYork | 192.168.201.2 | 760k | 751k | 14k | 14k | 1.842% | 1.932% | 5.734% | 6.398% |
| ● | Internet | 10.100.36.1 | 2,353k | 2,297k | 156k | 681k | 6.222% | 22.881% | 23.873% | 57.016% |
| ● | Atlanta | 192.168.202.2 | 556k | 539k | 8k | 2,998k | 1.586% | 84.752% | 4.400% | 2.671% |
| ● | Denver | 10.100.36.60 | 747k | 738k | 14k | 25k | 1.880% | 3.357% | 5.727% | 11.255% |
| Core Network | | | | | | | | | | |
| ● | Chiraz | 10.100.37.3 | 242k | 242k | 64k | 47k | 21.065% | 16.388% | 33.678% | 27.184% |
| ● | EdgeMarc4500 | 10.100.36.50 | 10k | 19k | 0 | 0 | 0.000% | 0.000% | 0.000% | 0.000% |

Network Monitor Beta v4.0 (4817)

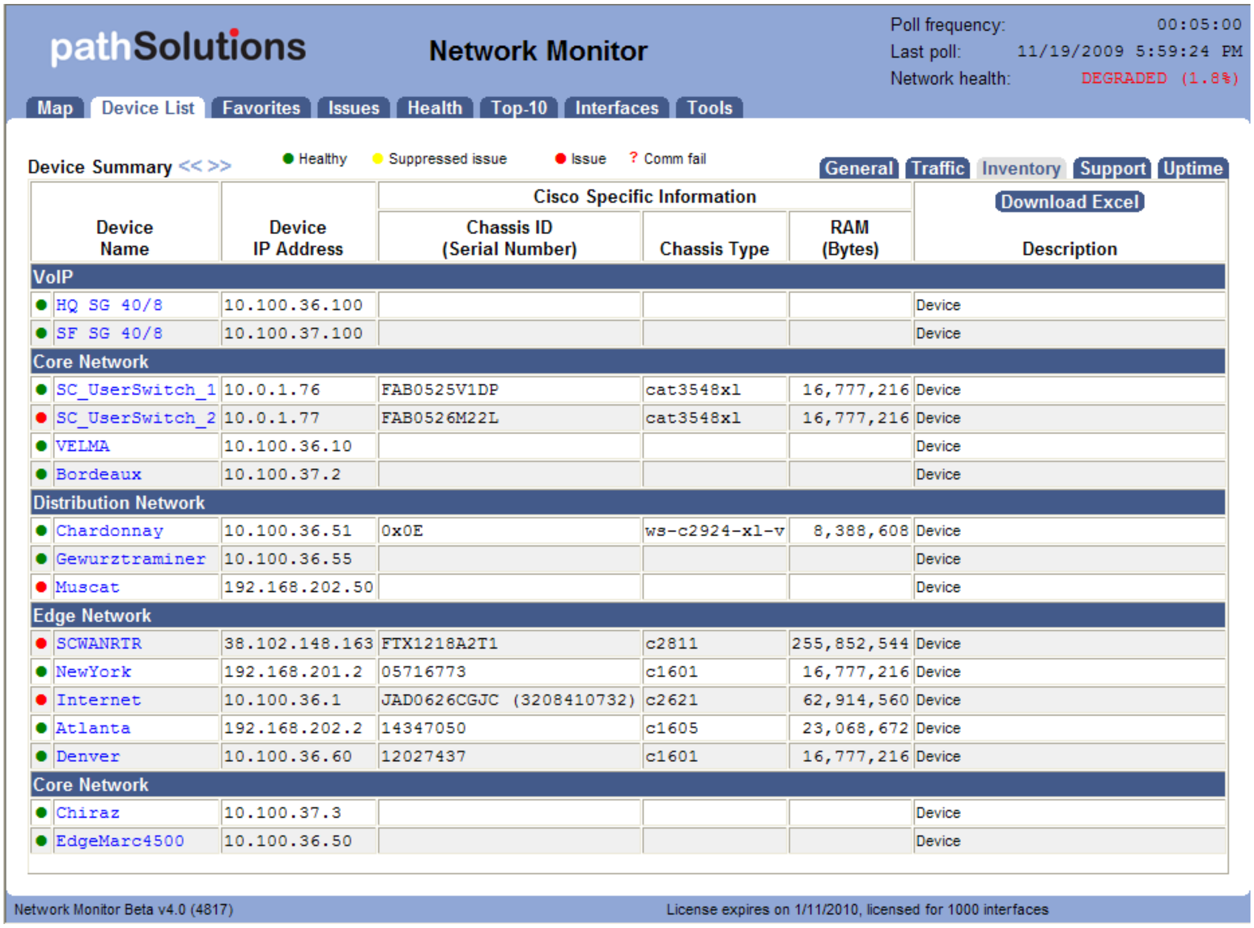
License expires on 1/11/2010, licensed for 1000 interfaces

This permits you to determine the average daily broadcast rate and compare it to the last poll broadcast rate to help identify devices that are transmitting or receiving a high level of broadcasts.

**Note:** If a device is transmitting a high percentage of broadcasts, it is more likely that one of its interfaces is receiving a high percentage of broadcasts from one of its ports, and then transmitting those broadcasts to all interfaces on the device. Click on the device and look for interfaces that are receiving a high broadcast rate to determine the device that is broadcasting.

## Inventory Sub-tab

The “Inventory” tab shows information about the device’s internal information:



Poll frequency: 00:05:00
Last poll: 11/19/2009 5:59:24 PM
Network health: DEGRADED (1.8%)

Device Summary

🟢 Healthy 🟡 Suppressed issue 🔴 Issue ? Comm fail

| | Device Name | Device IP Address | Cisco Specific Information | | | Description |
|---|---|---|---|---|---|---|
| | | | Chassis ID (Serial Number) | Chassis Type | RAM (Bytes) | |
| **VoIP** | | | | | | |
| 🟢 | HQ SG 40/8 | 10.100.36.100 | | | | Device |
| 🟢 | SF SG 40/8 | 10.100.37.100 | | | | Device |
| **Core Network** | | | | | | |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | FAB0525V1DP | cat3548xl | 16,777,216 | Device |
| 🔴 | SC_UserSwitch_2 | 10.0.1.77 | FAB0526M22L | cat3548xl | 16,777,216 | Device |
| 🟢 | VELMA | 10.100.36.10 | | | | Device |
| 🟢 | Bordeaux | 10.100.37.2 | | | | Device |
| **Distribution Network** | | | | | | |
| 🟢 | Chardonnay | 10.100.36.51 | 0x0E | ws-c2924-xl-v | 8,388,608 | Device |
| 🟢 | Gewurztraminer | 10.100.36.55 | | | | Device |
| 🔴 | Muscat | 192.168.202.50 | | | | Device |
| **Edge Network** | | | | | | |
| 🔴 | SCWANRTR | 38.102.148.163 | FTX1218A2T1 | c2811 | 255,852,544 | Device |
| 🟢 | NewYork | 192.168.201.2 | 05716773 | c1601 | 16,777,216 | Device |
| 🔴 | Internet | 10.100.36.1 | JAD0626CGJC (3208410732) | c2621 | 62,914,560 | Device |
| 🟢 | Atlanta | 192.168.202.2 | 14347050 | c1605 | 23,068,672 | Device |
| 🟢 | Denver | 10.100.36.60 | 12027437 | c1601 | 16,777,216 | Device |
| **Core Network** | | | | | | |
| 🟢 | Chiraz | 10.100.37.3 | | | | Device |
| 🟢 | EdgeMarc4500 | 10.100.36.50 | | | | Device |

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

If there are Cisco devices on the network, the serial number, chassis type, and installed RAM will be displayed in the first three columns.

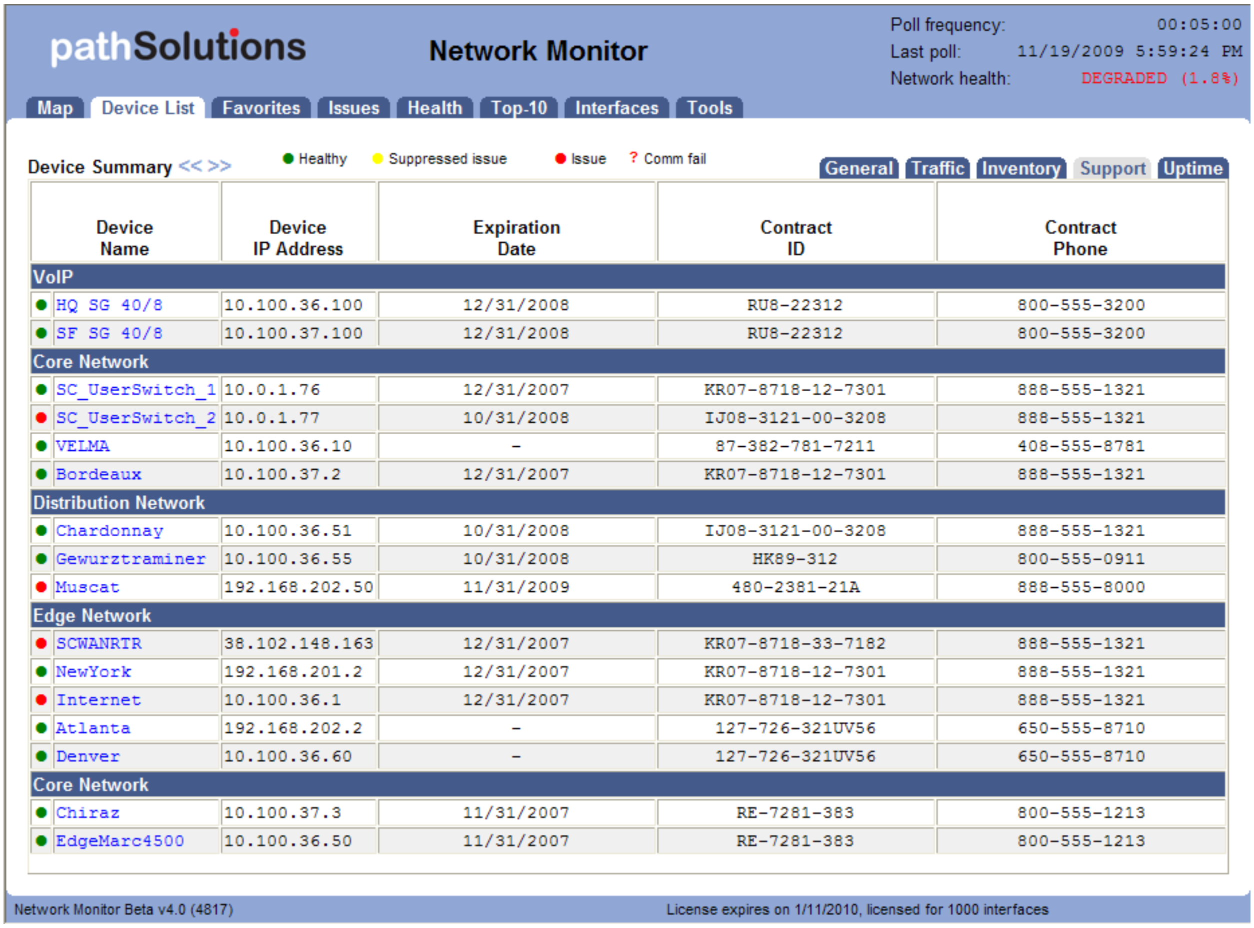
If there are no Cisco devices on the network, the internal system description will display in the first column.

The last column will display the PathSolutions’ Network Monitor configured description. This description can be changed in the Configuration Tool.

An Excel spreadsheet with additional information can be downloaded by clicking on the “Download Excel” button.

## Support Sub-tab

The “Support” tab will display support contract information for each monitored device:



Poll frequency: 00:05:00
Last poll: 11/19/2009 5:59:24 PM
Network health: DEGRADED (1.8%)

● Healthy ● Suppressed issue ● Issue ? Comm fail

| Device Name | Device IP Address | Expiration Date | Contract ID | Contract Phone |
|---|---|---|---|---|
| VoIP | | | | |
| ● HQ SG 40/8 | 10.100.36.100 | 12/31/2008 | RU8-22312 | 800-555-3200 |
| ● SF SG 40/8 | 10.100.37.100 | 12/31/2008 | RU8-22312 | 800-555-3200 |
| Core Network | | | | |
| ● SC_UserSwitch_1 | 10.0.1.76 | 12/31/2007 | KR07-8718-12-7301 | 888-555-1321 |
| ● SC_UserSwitch_2 | 10.0.1.77 | 10/31/2008 | IJ08-3121-00-3208 | 888-555-1321 |
| ● VELMA | 10.100.36.10 | - | 87-382-781-7211 | 408-555-8781 |
| ● Bordeaux | 10.100.37.2 | 12/31/2007 | KR07-8718-12-7301 | 888-555-1321 |
| Distribution Network | | | | |
| ● Chardonnay | 10.100.36.51 | 10/31/2008 | IJ08-3121-00-3208 | 888-555-1321 |
| ● Gewurztraminer | 10.100.36.55 | 10/31/2008 | HK89-312 | 800-555-0911 |
| ● Muscat | 192.168.202.50 | 11/31/2009 | 480-2381-21A | 888-555-8000 |
| Edge Network | | | | |
| ● SCWANRTR | 38.102.148.163 | 12/31/2007 | KR07-8718-33-7182 | 888-555-1321 |
| ● NewYork | 192.168.201.2 | 12/31/2007 | KR07-8718-12-7301 | 888-555-1321 |
| ● Internet | 10.100.36.1 | 12/31/2007 | KR07-8718-12-7301 | 888-555-1321 |
| ● Atlanta | 192.168.202.2 | - | 127-726-321UV56 | 650-555-8710 |
| ● Denver | 10.100.36.60 | - | 127-726-321UV56 | 650-555-8710 |
| Core Network | | | | |
| ● Chiraz | 10.100.37.3 | 11/31/2007 | RE-7281-383 | 800-555-1213 |
| ● EdgeMarc4500 | 10.100.36.50 | 11/31/2007 | RE-7281-383 | 800-555-1213 |

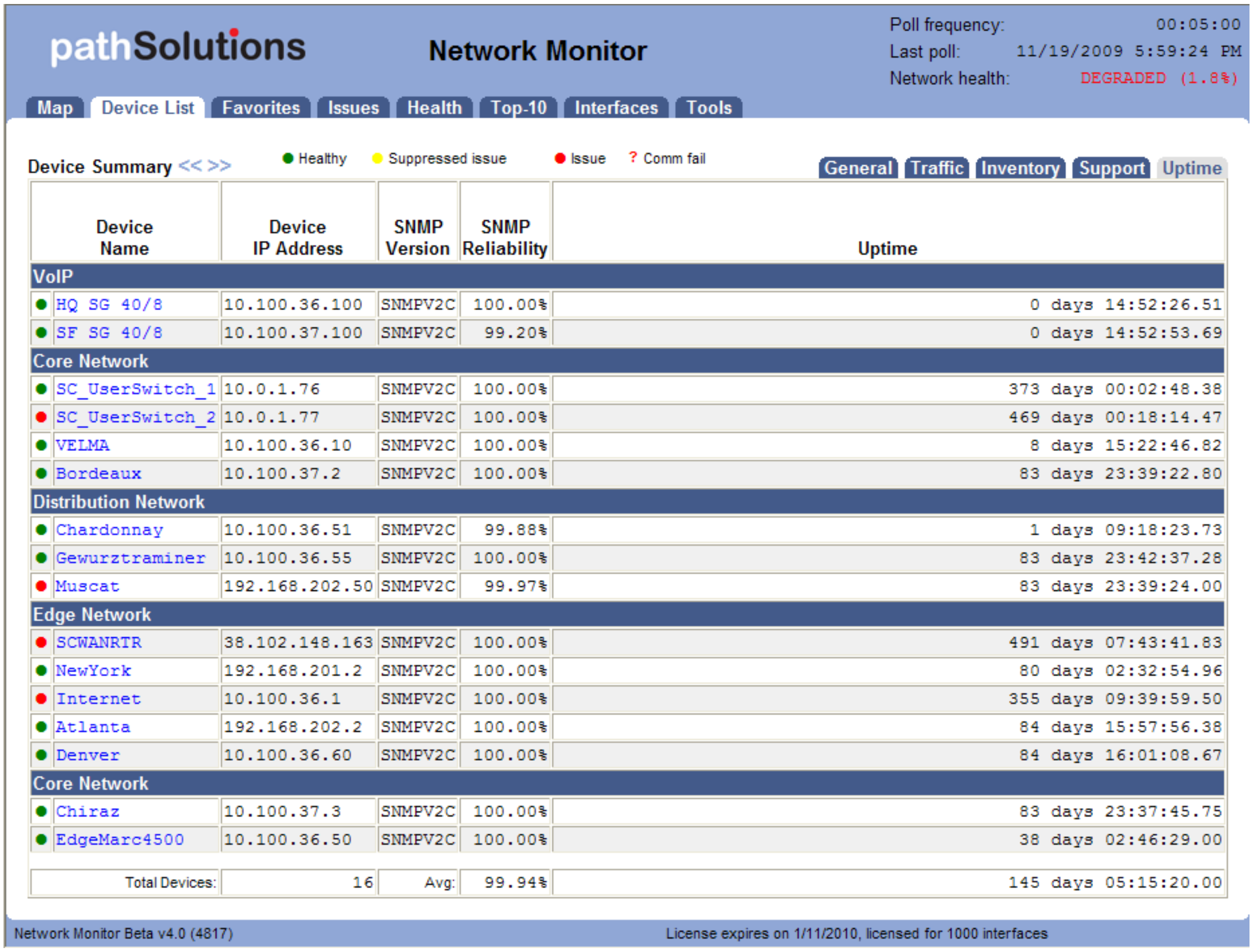
Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

This information can be entered via the Configuration Tool.

The system will send an email if any of the support contracts are within 30 days of expiration to help make sure support contracts don’t lapse.

## Uptime Sub-tab

The “Uptime” tab displays information on the device current status:



Poll frequency: 00:05:00
Last poll: 11/19/2009 5:59:24 PM
Network health: DEGRADED (1.8%)

Device Summary << >>   🟢 Healthy   🟡 Suppressed issue   🔴 Issue   ? Comm fail

| | Device Name | Device IP Address | SNMP Version | SNMP Reliability | Uptime |
|---|---|---|---|---|---|
| VoIP | | | | | |
| 🟢 | HQ SG 40/8 | 10.100.36.100 | SNMPV2C | 100.00% | 0 days 14:52:26.51 |
| 🟢 | SF SG 40/8 | 10.100.37.100 | SNMPV2C | 99.20% | 0 days 14:52:53.69 |
| Core Network | | | | | |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | SNMPV2C | 100.00% | 373 days 00:02:48.38 |
| 🔴 | SC_UserSwitch_2 | 10.0.1.77 | SNMPV2C | 100.00% | 469 days 00:18:14.47 |
| 🟢 | VELMA | 10.100.36.10 | SNMPV2C | 100.00% | 8 days 15:22:46.82 |
| 🟢 | Bordeaux | 10.100.37.2 | SNMPV2C | 100.00% | 83 days 23:39:22.80 |
| Distribution Network | | | | | |
| 🟢 | Chardonnay | 10.100.36.51 | SNMPV2C | 99.88% | 1 days 09:18:23.73 |
| 🟢 | Gewurztraminer | 10.100.36.55 | SNMPV2C | 100.00% | 83 days 23:42:37.28 |
| 🔴 | Muscat | 192.168.202.50 | SNMPV2C | 99.97% | 83 days 23:39:24.00 |
| Edge Network | | | | | |
| 🔴 | SCWANRTR | 38.102.148.163 | SNMPV2C | 100.00% | 491 days 07:43:41.83 |
| 🟢 | NewYork | 192.168.201.2 | SNMPV2C | 100.00% | 80 days 02:32:54.96 |
| 🔴 | Internet | 10.100.36.1 | SNMPV2C | 100.00% | 355 days 09:39:59.50 |
| 🟢 | Atlanta | 192.168.202.2 | SNMPV2C | 100.00% | 84 days 15:57:56.38 |
| 🟢 | Denver | 10.100.36.60 | SNMPV2C | 100.00% | 84 days 16:01:08.67 |
| Core Network | | | | | |
| 🟢 | Chiraz | 10.100.37.3 | SNMPV2C | 100.00% | 83 days 23:37:45.75 |
| 🟢 | EdgeMarc4500 | 10.100.36.50 | SNMPV2C | 100.00% | 38 days 02:46:29.00 |
| | Total Devices: | 16 | Avg: | 99.94% | 145 days 05:15:20.00 |

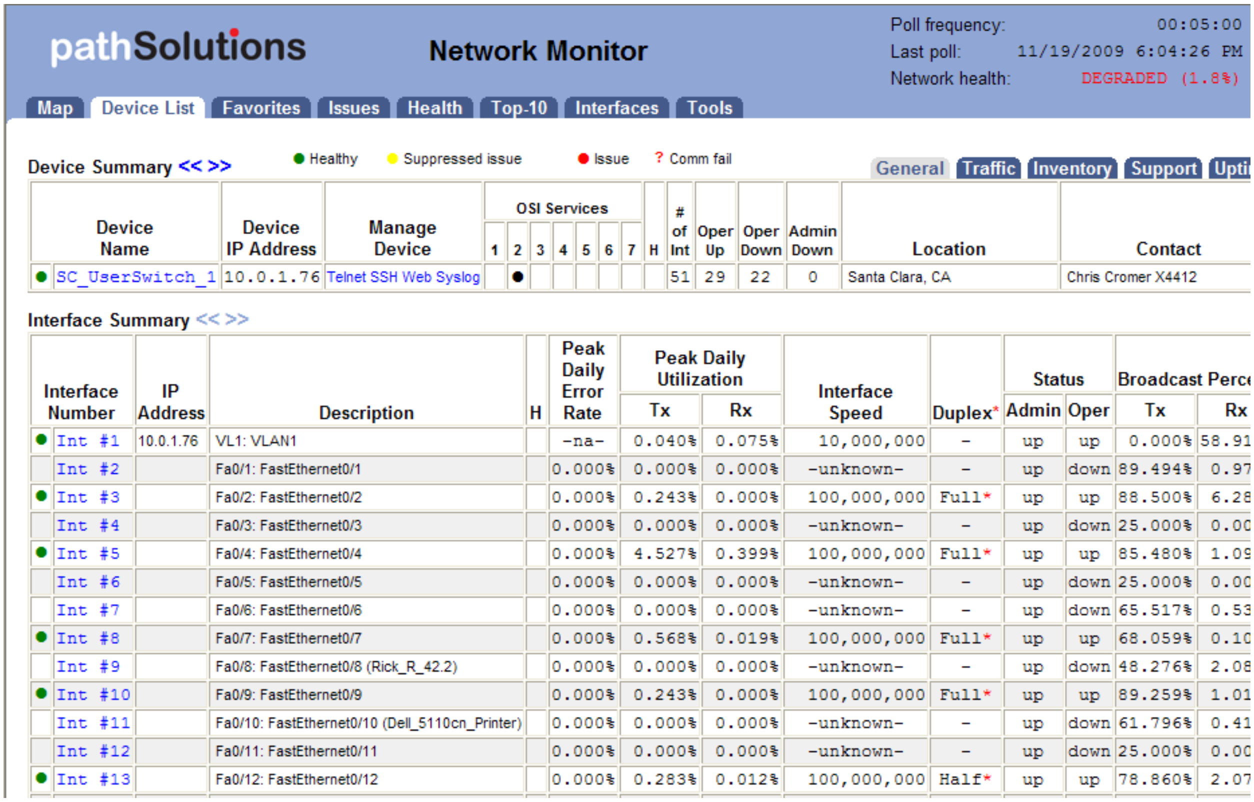
Network Monitor Beta v4.0 (4817)   License expires on 1/11/2010, licensed for 1000 interfaces

The version of SNMP that is being used to communicate with the device along with the reliability of communication with the device is displayed.

The uptime (as reported by the device) is also displayed, along with an average uptime of all devices. This can help track when a device was last rebooted.

## *Interface Summary*

If you click on a device name, it will display the Interface Summary for that device:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:04:26 PM
Network health: DEGRADED (1.8%)

Device Summary << >>

| | Device Name | Device IP Address | Manage Device | OSI Services | | | | | | | | # of Int | Oper Up | Oper Down | Admin Down | Location | Contact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | H | | | | | | |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Telnet SSH Web Syslog | | ● | | | | | | | 51 | 29 | 22 | 0 | Santa Clara, CA | Chris Cromer X4412 |

Interface Summary << >>

| | Interface Number | IP Address | Description | H | Peak Daily Error Rate | Peak Daily Utilization | | Interface Speed | Duplex* | Status | | Broadcast Perce | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx | | | Admin | Oper | Tx | Rx |
| ● | Int #1 | 10.0.1.76 | VL1: VLAN1 | | -na- | 0.040% | 0.075% | 10,000,000 | - | up | up | 0.000% | 58.91 |
| | Int #2 | | Fa0/1: FastEthernet0/1 | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 89.494% | 0.97 |
| ● | Int #3 | | Fa0/2: FastEthernet0/2 | | 0.000% | 0.243% | 0.000% | 100,000,000 | Full* | up | up | 88.500% | 6.28 |
| | Int #4 | | Fa0/3: FastEthernet0/3 | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 25.000% | 0.00 |
| ● | Int #5 | | Fa0/4: FastEthernet0/4 | | 0.000% | 4.527% | 0.399% | 100,000,000 | Full* | up | up | 85.480% | 1.09 |
| | Int #6 | | Fa0/5: FastEthernet0/5 | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 25.000% | 0.00 |
| | Int #7 | | Fa0/6: FastEthernet0/6 | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 65.517% | 0.53 |
| ● | Int #8 | | Fa0/7: FastEthernet0/7 | | 0.000% | 0.568% | 0.019% | 100,000,000 | Full* | up | up | 68.059% | 0.10 |
| | Int #9 | | Fa0/8: FastEthernet0/8 (Rick_R_42.2) | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 48.276% | 2.08 |
| ● | Int #10 | | Fa0/9: FastEthernet0/9 | | 0.000% | 0.243% | 0.000% | 100,000,000 | Full* | up | up | 89.259% | 1.01 |
| | Int #11 | | Fa0/10: FastEthernet0/10 (Dell_5110cn_Printer) | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 61.796% | 0.41 |
| | Int #12 | | Fa0/11: FastEthernet0/11 | | 0.000% | 0.000% | 0.000% | -unknown- | - | up | down | 25.000% | 0.00 |
| ● | Int #13 | | Fa0/12: FastEthernet0/12 | | 0.000% | 0.283% | 0.012% | 100,000,000 | Half* | up | up | 78.860% | 2.07 |

The Interface Summary will list the specific switch information that you selected, and a table showing all of the interfaces on the switch.

### Interface Summary Fields

The interface summary table includes the following fields:

The first column includes a red or green status indicator. If an interface is degraded (utilization or error rate is higher than the configured threshold), the status for the interface will be red, and the Error Rate, or Utilization Rate will be marked in red.

**Note:** If the status indicator is a blank, then the interface is operationally shut down, and is not relevant.

The second column is the interface number on the device. Each device manufacturer will create a unique number for each interface. You can use this interface number to correlate physical interfaces on the switch. Clicking on the interface number will display the "Interface Details" page. Refer to the "Interface Details" section for more information about this page.

The third column is the IP address associated with the interface (if any). Routers will generally have an IP address assigned to each interface, whereas switches may only have an IP address associated with the management interface. If multiple IP addresses are associated with an interface, it will appear on the tooltip if you hover over the IP address field.

The fourth column is the interface description. This information is provided by the device as a way of describing the interface. It may contain information on the type of interface, or the interface identifier used on the device.

The fifth column is the error rate of the interface. The error rate is calculated as a combination of all inbound and outbound errors on the interface, compared to the number of packets that have passed through the interface.

If the error rate is above the error threshold, it will be displayed in red.

**Note:** There are some devices that do not report error information correctly, and can lead you to believe that there are faults on interfaces that actually are functioning correctly. If you perceive errors on an interface that are abnormal, contact the device manufacturer to attempt to determine more about its SNMP reporting capabilities.

The sixth column is daily peak utilization transmitted data. This statistic reports the maximum transmitted utilization on the interface (as a percentage of bandwidth) that was seen over the past 24 hour period.

If this statistic is over the utilization threshold, it will be displayed in red.

**Note:** If PathSolutions' Network Monitor is unable to read the correct interface speed from the device, this number may not be accurate.

The seventh column is daily peak utilization received data. This statistic reports the maximum received utilization on the interface (as a percentage of bandwidth) that was seen over the past 24 hour period.

If this statistic is over the utilization threshold, it will be displayed in red.

**Note:** If PathSolutions' Network Monitor is unable to read the correct interface speed from the device, this number may not be accurate.

The eighth column is interface speed, rated in bits per second. If the interface is operationally shut down, or the device does not report a valid speed, then the speed is listed as "Unknown".

The ninth column shows the duplex status of the interface. Duplex information cannot easily be determined from different switch manufacturers, so this field is calculated based on the presence or absence of collisions. If there are any collisions on the interface, then the interface must be half-duplex. If there are no collisions on the interface, then the interface may be full-duplex, or it may be a half-duplex interface that has not yet received any collisions.

The tenth column shows the administrative status of the interface. If the network administrator has configured this interface to be shut down, it will be listed as "down" in this column.

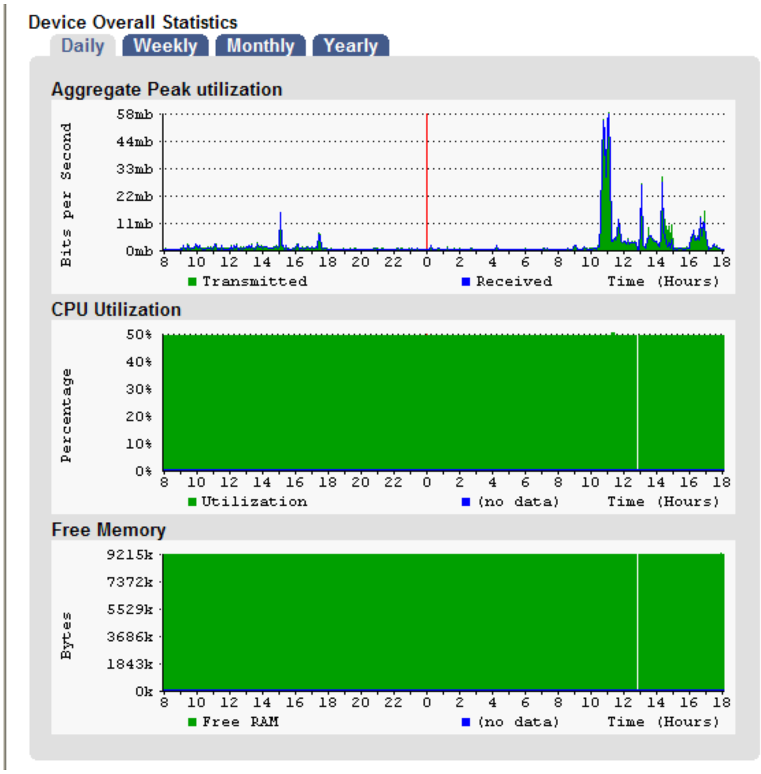
The eleventh column shows the operational status of the interface. If the interface has a node connected, and there is a link light present, the interface will be listed as "up".

The twelfth column shows the percent of transmitted traffic that are broadcasts as seen on this interface.

The thirteenth column shows the percent of received traffic that are broadcasts as seen on this interface.

## Device Overall Statistics

Below the interface listing is a view of the overall statistics for the device:



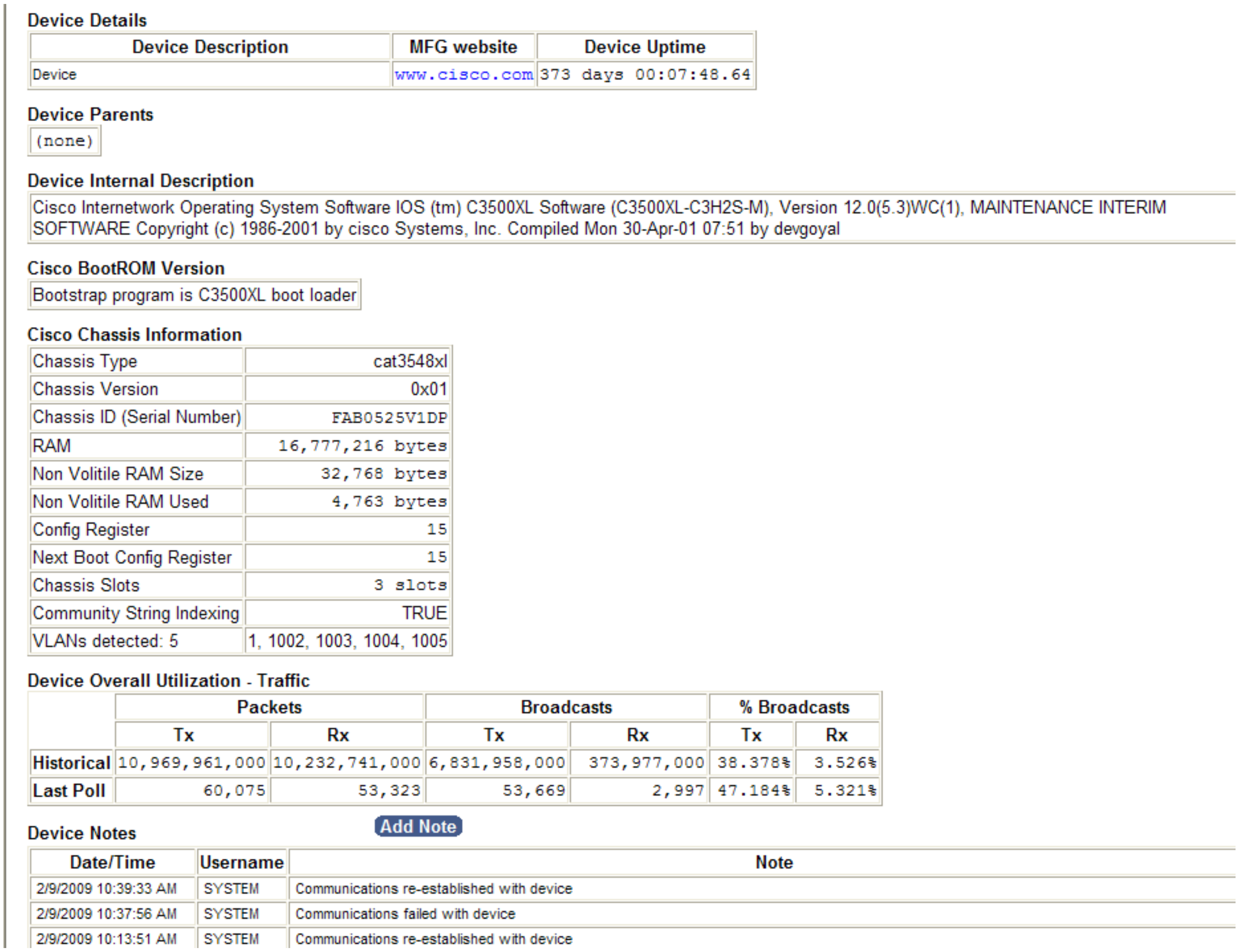
You can view the daily, weekly, monthly, or yearly information for the aggregate utilization for the device.

This is valuable for determining when the device is passing more or less traffic. This equates to a graph showing how much work was performed by the device over time, and is useful for determining when to schedule downtime for the device.

If the device is a Cisco router or switch, the CPU utilization and Free RAM is also displayed.

## Device Details

Below the Device Overall Statistics is information about the device:



**Device Details**

| Device Description | MFG website | Device Uptime |
|---|---|---|
| Device | www.cisco.com | 373 days 00:07:48.64 |

**Device Parents**

(none)

**Device Internal Description**

Cisco Internetwork Operating System Software IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE Copyright (c) 1986-2001 by cisco Systems, Inc. Compiled Mon 30-Apr-01 07:51 by devgoyal

**Cisco BootROM Version**

Bootstrap program is C3500XL boot loader

**Cisco Chassis Information**

| | |
|---|---|
| Chassis Type | cat3548xl |
| Chassis Version | 0x01 |
| Chassis ID (Serial Number) | FAB0525V1DP |
| RAM | 16,777,216 bytes |
| Non Volitile RAM Size | 32,768 bytes |
| Non Volitile RAM Used | 4,763 bytes |
| Config Register | 15 |
| Next Boot Config Register | 15 |
| Chassis Slots | 3 slots |
| Community String Indexing | TRUE |
| VLANs detected: 5 | 1, 1002, 1003, 1004, 1005 |

**Device Overall Utilization - Traffic**

| | Packets | | Broadcasts | | % Broadcasts | |
|---|---|---|---|---|---|---|
| | Tx | Rx | Tx | Rx | Tx | Rx |
| Historical | 10,969,961,000 | 10,232,741,000 | 6,831,958,000 | 373,977,000 | 38.378% | 3.526% |
| Last Poll | 60,075 | 53,323 | 53,669 | 2,997 | 47.184% | 5.321% |

**Device Notes**

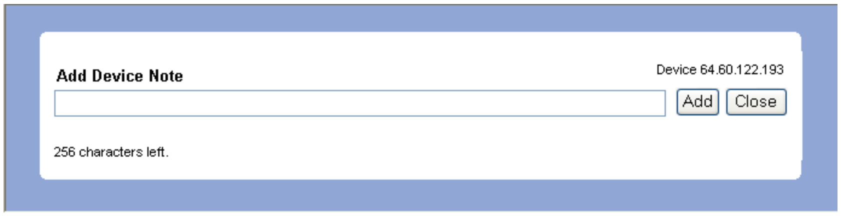
| Date/Time | Username | Note |
|---|---|---|
| 2/9/2009 10:39:33 AM | SYSTEM | Communications re-established with device |
| 2/9/2009 10:37:56 AM | SYSTEM | Communications failed with device |
| 2/9/2009 10:13:51 AM | SYSTEM | Communications re-established with device |

From this section, you can track the device's uptime (as reported by the device), as well as internal information about the device.

**Note:** If the device is a Cisco switch or router, then additional internal device information is displayed.

## Device Notes

Notes can be added to a device so you can track when you performed work on a device:



Add Device Note

Device 64.60.122.193

256 characters left.

---

**Note:** If you have authentication turned on, then the Username field will use the logged in user who entered the note.

---

**Note:** The notes are stored in comma separated values (CSV) format in the following directory:

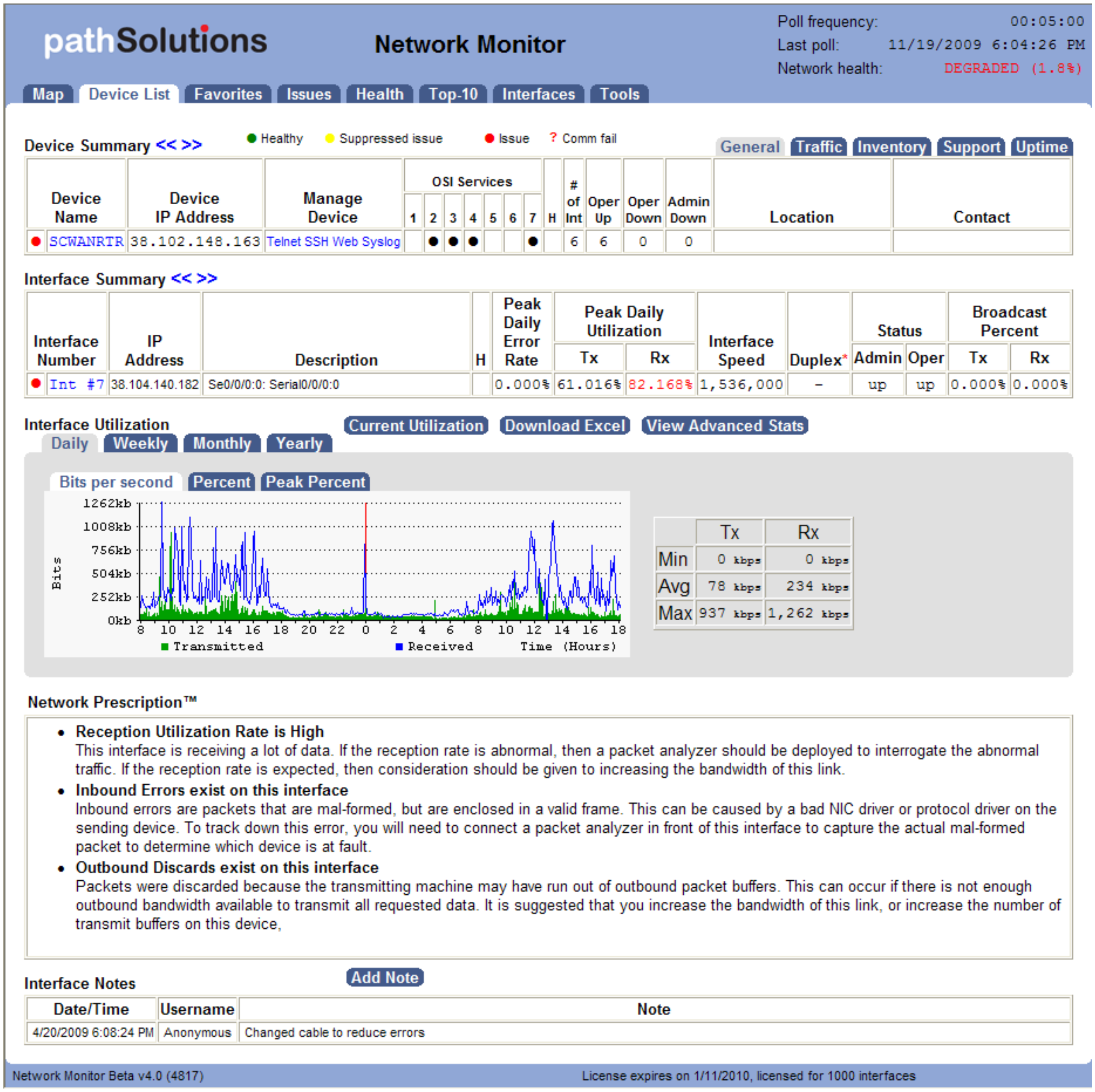
```
C:\Program Files\PathSolutions\Network Monitor\Notes
```

You can edit the files with any text editor like Notepad, or use Excel to open the file in CSV format.

The filename for device notes is the IP address of the device. For example, the notes for device 10.100.36.10 would be stored in filename 10.100.36.10.csv.

### *Interface Details*

If you click on an interface number, you will see details about that specific interface:



Network Monitor

Poll frequency: 00:05:00
Last poll: 11/19/2009 6:04:26 PM
Network health: DEGRADED (1.8%)

Device Summary << >>

● Healthy ● Suppressed issue ● Issue ? Comm fail

| | Device Name | Device IP Address | Manage Device | OSI Services | | | | | | | H | # of Int | Oper Up | Oper Down | Admin Down | Location | Contact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | | | | | | | |
| ● | SCWANRTR | 38.102.148.163 | Telnet SSH Web Syslog | | ● | ● | ● | | | ● | | 6 | 6 | 0 | 0 | | |

Interface Summary << >>

| | Interface Number | IP Address | Description | H | Peak Daily Error Rate | Peak Daily Utilization | | Interface Speed | Duplex* | Status | | Broadcast Percent | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx | | | Admin | Oper | Tx | Rx |
| ● | Int #7 | 38.104.140.182 | Se0/0/0:0: Serial0/0/0:0 | | 0.000% | 61.016% | 82.168% | 1,536,000 | - | up | up | 0.000% | 0.000% |

Interface Utilization

| | Tx | Rx |
|---|---|---|
| Min | 0 kbps | 0 kbps |
| Avg | 78 kbps | 234 kbps |
| Max | 937 kbps | 1,262 kbps |

Network Prescription™

- **Reception Utilization Rate is High**
  This interface is receiving a lot of data. If the reception rate is abnormal, then a packet analyzer should be deployed to interrogate the abnormal traffic. If the reception rate is expected, then consideration should be given to increasing the bandwidth of this link.
- **Inbound Errors exist on this interface**
  Inbound errors are packets that are mal-formed, but are enclosed in a valid frame. This can be caused by a bad NIC driver or protocol driver on the sending device. To track down this error, you will need to connect a packet analyzer in front of this interface to capture the actual mal-formed packet to determine which device is at fault.
- **Outbound Discards exist on this interface**
  Packets were discarded because the transmitting machine may have run out of outbound packet buffers. This can occur if there is not enough outbound bandwidth available to transmit all requested data. It is suggested that you increase the bandwidth of this link, or increase the number of transmit buffers on this device,

Interface Notes

| Date/Time | Username | Note |
|---|---|---|
| 4/20/2009 6:08:24 PM | Anonymous | Changed cable to reduce errors |

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

From this page, you can view all information about an interface’s performance.

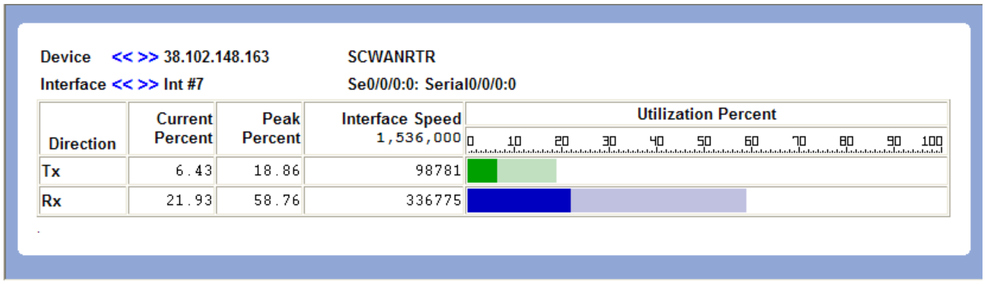
## Utilization Graphs

The utilization graphs provide historical utilization of an interface in Daily, Weekly, Monthly, and Yearly views.

You can view the information in bits per second, percent utilization, or peak percent utilization.

## Current Utilization Information

If you want to view the current utilization of this interface, click on "Current Utilization".  You'll get a window that will display the immediate current utilization on the interface:



Device << >> 38.102.148.163 SCWANRTR

Interface << >> Int #7 Se0/0/0:0: Serial0/0/0:0

| Direction | Current Percent | Peak Percent | Interface Speed 1,536,000 | Utilization Percent |
|---|---|---|---|---|
| Tx | 6.43 | 18.86 | 98781 | |
| Rx | 21.93 | 58.76 | 336775 | |

You can open as many of these current utilization windows as you would like.  This permits you to do detailed bandwidth studies of any monitored interface on the system.

A high-water mark is maintained so you can determine the highest utilization point that occurred since the window was opened.

The current utilization page is updated every 5 seconds.

## Exporting Utilization Graph Data for an Interface

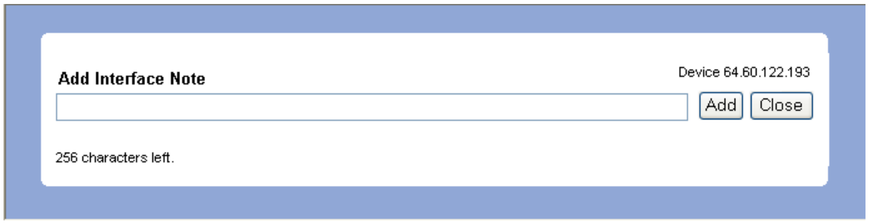
The "Download CSV utilization" allows you to download all of the graph data into a CSV (Comma Separated Values) file for charting & graphing with a spreadsheet.

## Network Prescription

Below the graph is the Network Prescription for the interface.  This is an analysis of any problems that exist on the interface, including errors and utilization.

## Interface Notes

Notes can be added to an interface so you can track when you performed work on an interface:



**Note:** If you have authentication turned on, then the Username field will use the logged in user who entered the note.

**Note:** The notes are stored in comma separated values (CSV) format in the following directory:

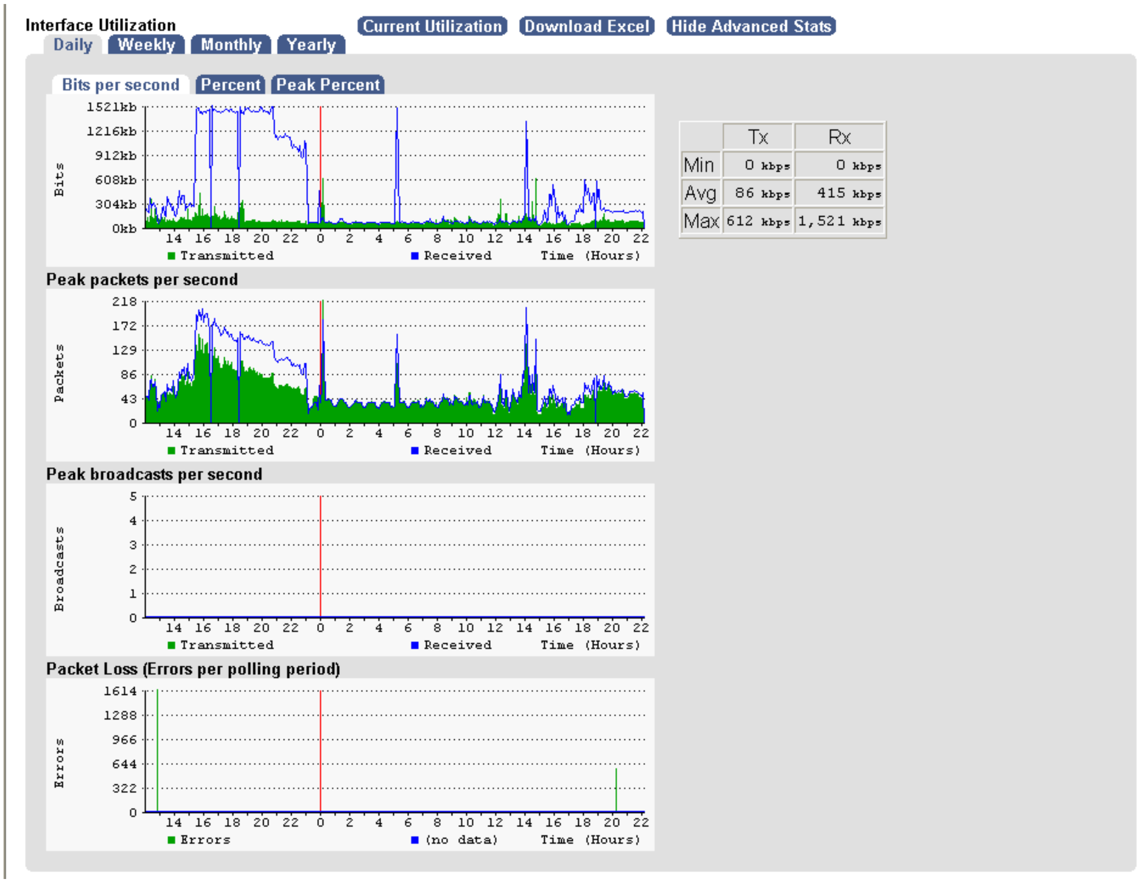
```
C:\Program Files\PathSolutions\Network Monitor\Notes
```

You can edit the files with any text editor like Notepad, or use Excel to open the file in CSV format.

The filename for interface notes is the IP address of the device, then a hyphen '-', followed by the interface number. For example, the notes for device 10.100.36.10 interface #36 would be stored in filename 10.100.36.10-36.csv.

## Advanced Interface Statistics

If you click on the “View Advanced Stats” button, you will be presented with additional graphs showing packets per second, broadcasts per second, and errors over time:

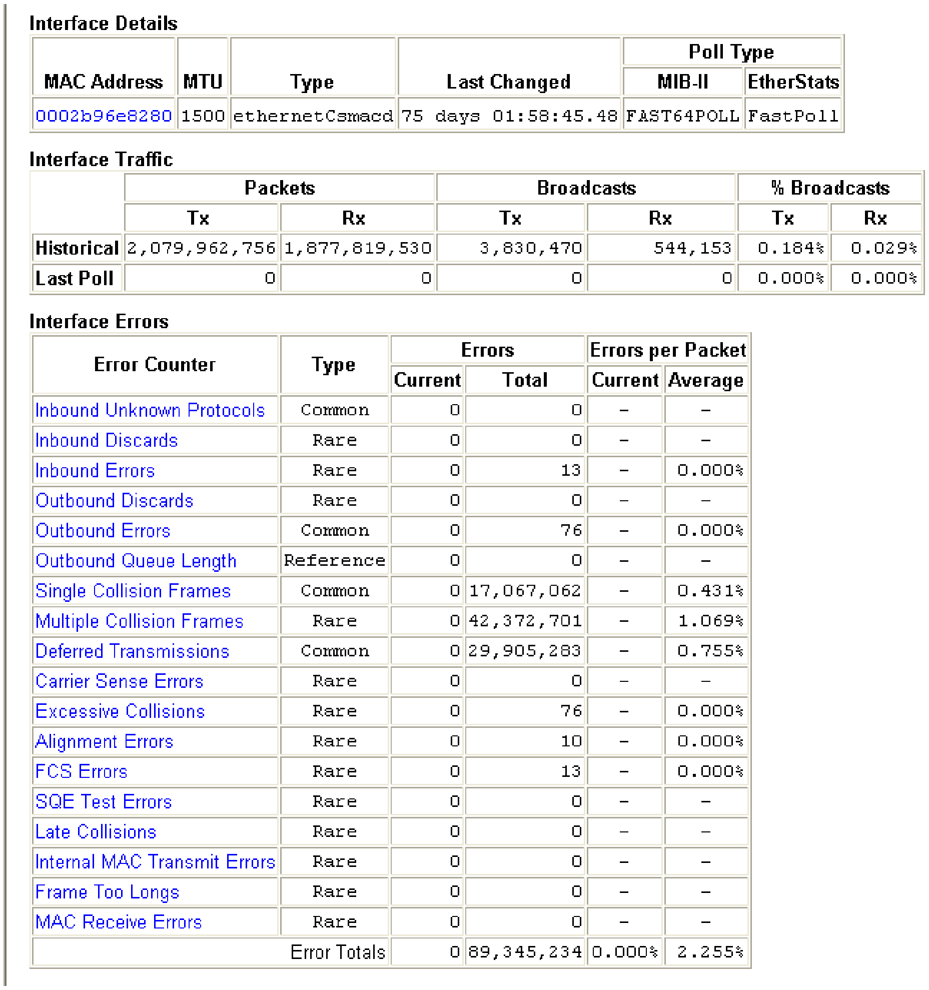


| | Tx | Rx |
|---|---|---|
| Min | 0 kbps | 0 kbps |
| Avg | 86 kbps | 415 kbps |
| Max | 612 kbps | 1,521 kbps |

The information displayed is useful for determining timing of broadcast storms or unusual packet activity.

You can also determine when packet loss occurred on the interface to help correlate with network events. It is useful to determine if packet loss occurred along with high utilization levels or if the loss was independent from utilization events.

Additional interface information is displayed below the graphs:



Interface Details

| MAC Address | MTU | Type | Last Changed | Poll Type | |
|---|---|---|---|---|---|
| | | | | MIB-II | EtherStats |
| 0002b96e8280 | 1500 | ethernetCsmacd | 75 days 01:58:45.48 | FAST64POLL | FastPoll |

Interface Traffic

| | Packets | | Broadcasts | | % Broadcasts | |
|---|---|---|---|---|---|---|
| | Tx | Rx | Tx | Rx | Tx | Rx |
| Historical | 2,079,962,756 | 1,877,819,530 | 3,830,470 | 544,153 | 0.184% | 0.029% |
| Last Poll | 0 | 0 | 0 | 0 | 0.000% | 0.000% |

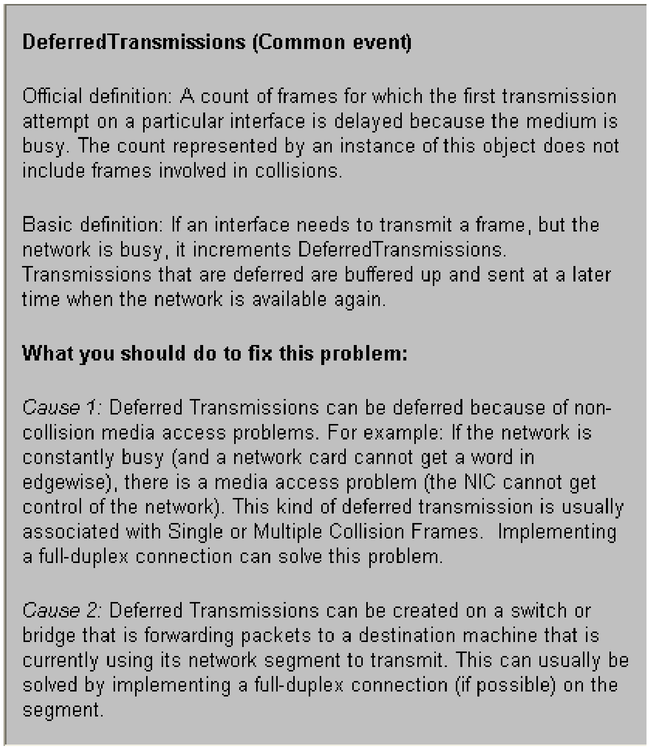
Interface Errors

| Error Counter | Type | Errors | | Errors per Packet | |
|---|---|---|---|---|---|
| | | Current | Total | Current | Average |
| Inbound Unknown Protocols | Common | 0 | 0 | - | - |
| Inbound Discards | Rare | 0 | 0 | - | - |
| Inbound Errors | Rare | 0 | 13 | - | 0.000% |
| Outbound Discards | Rare | 0 | 0 | - | - |
| Outbound Errors | Common | 0 | 76 | - | 0.000% |
| Outbound Queue Length | Reference | 0 | 0 | - | - |
| Single Collision Frames | Common | 0 | 17,067,062 | - | 0.431% |
| Multiple Collision Frames | Rare | 0 | 42,372,701 | - | 1.069% |
| Deferred Transmissions | Common | 0 | 29,905,283 | - | 0.755% |
| Carrier Sense Errors | Rare | 0 | 0 | - | - |
| Excessive Collisions | Rare | 0 | 76 | - | 0.000% |
| Alignment Errors | Rare | 0 | 10 | - | 0.000% |
| FCS Errors | Rare | 0 | 13 | - | 0.000% |
| SQE Test Errors | Rare | 0 | 0 | - | - |
| Late Collisions | Rare | 0 | 0 | - | - |
| Internal MAC Transmit Errors | Rare | 0 | 0 | - | - |
| Frame Too Longs | Rare | 0 | 0 | - | - |
| MAC Receive Errors | Rare | 0 | 0 | - | - |
| | Error Totals | 0 | 89,345,234 | 0.000% | 2.255% |

This includes information of when the interface last changed status, as well as historical and last poll packet and broadcast information.

All error counters are displayed so you can determine the exact error type that occurred on the interface.

If you click on an error type, you will receive the official definition of the error, as well as what should be done to resolve the error:



**DeferredTransmissions (Common event)**

Official definition: A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.

Basic definition: If an interface needs to transmit a frame, but the network is busy, it increments DeferredTransmissions. Transmissions that are deferred are buffered up and sent at a later time when the network is available again.

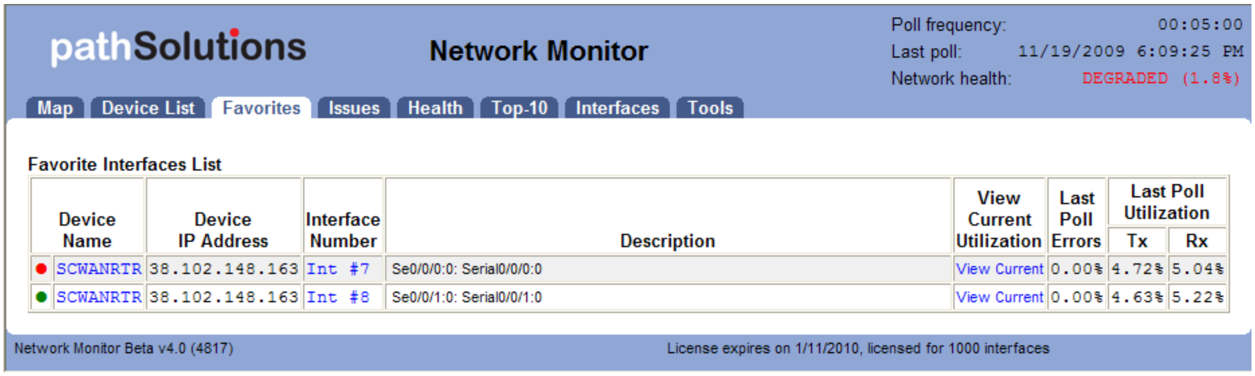
**What you should do to fix this problem:**

*Cause 1:* Deferred Transmissions can be deferred because of non-collision media access problems. For example: If the network is constantly busy (and a network card cannot get a word in edgewise), there is a media access problem (the NIC cannot get control of the network). This kind of deferred transmission is usually associated with Single or Multiple Collision Frames. Implementing a full-duplex connection can solve this problem.

*Cause 2:* Deferred Transmissions can be created on a switch or bridge that is forwarding packets to a destination machine that is currently using its network segment to transmit. This can usually be solved by implementing a full-duplex connection (if possible) on the segment.

## *Favorites Page*

If you have specific interfaces that you want to group together to view from one page, they can be added to the favorites page:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Favorite Interfaces List

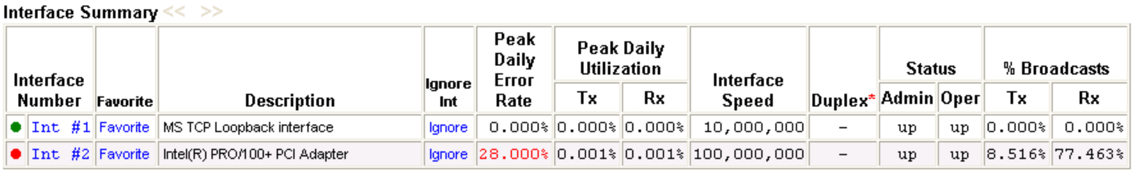
| | Device Name | Device IP Address | Interface Number | Description | View Current Utilization | Last Poll Errors | Last Poll Utilization | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | Tx | Rx |
| ● | SCWANRTR | 38.102.148.163 | Int #7 | Se0/0/0:0: Serial0/0/0:0 | View Current | 0.00% | 4.72% | 5.04% |
| ● | SCWANRTR | 38.102.148.163 | Int #8 | Se0/0/1:0: Serial0/0/1:0 | View Current | 0.00% | 4.63% | 5.22% |

Network Monitor Beta v4.0 (4817)
License expires on 1/11/2010, licensed for 1000 interfaces

This page displays the most recent utilization that was seen during the last polling period of all favorite interfaces.

### Adding an Interface to the Favorites List

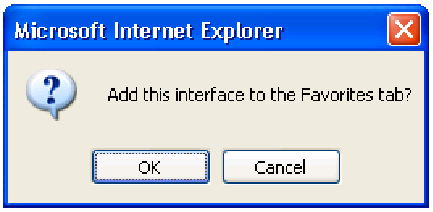
To add an interface to the favorites list, just click “Favorite” on an interface when the web interface is in configuration mode:



Interface Summary << >>

| | Interface Number | Favorite | Description | Ignore Int | Peak Daily Error Rate | Peak Daily Utilization | | Interface Speed | Duplex* | Status | | % Broadcasts | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx | | | Admin | Oper | Tx | Rx |
| ● | Int #1 | Favorite | MS TCP Loopback interface | Ignore | 0.000% | 0.000% | 0.000% | 10,000,000 | – | up | up | 0.000% | 0.000% |
| ● | Int #2 | Favorite | Intel(R) PRO/100+ PCI Adapter | Ignore | 28.000% | 0.001% | 0.001% | 100,000,000 | – | up | up | 8.516% | 77.463% |

You will be presented with a dialog confirming your selection:



Add this interface to the Favorites tab?

Click “OK” to add the interface to the favorites tab, or Cancel if you do not want to do so.

### Removing an Interface from the Favorites List

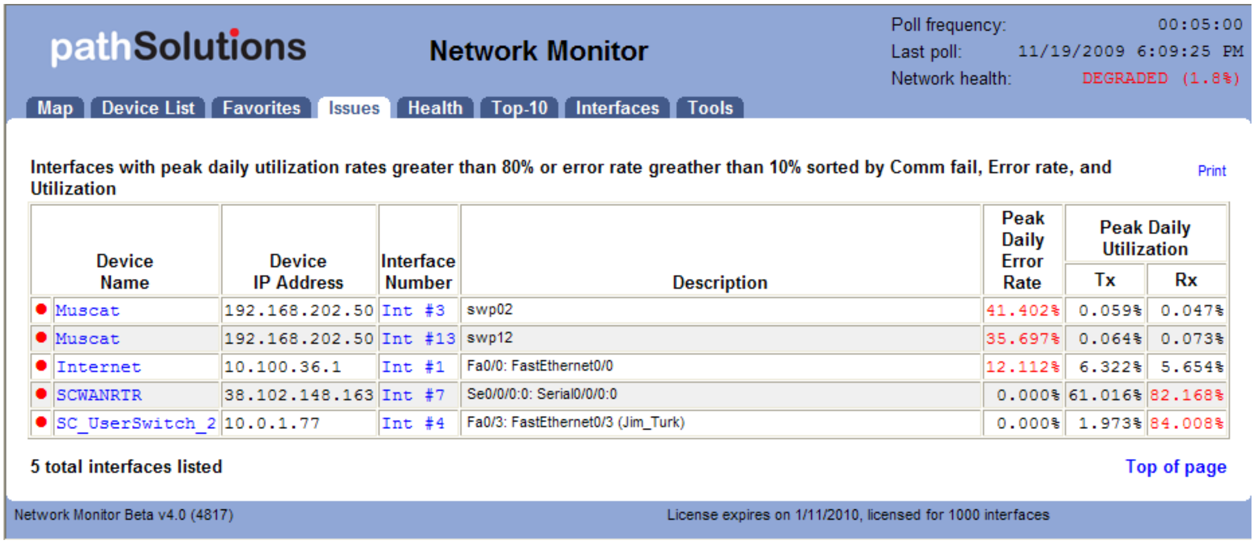
To remove an interface from the Favorites List you must edit the following file with a text editor:

```
C:\Program Files\PathSolutions\Network Monitor\Favorites.cfg
```

Locate the IP address and interface number in the file and then delete it and Save the file. You do not need to stop and restart the service after changing this file.

## *Issues*

Interfaces that have peak utilization rates or error rates that are over the threshold will be listed under the "Issues" tab:



Network Monitor

Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Interfaces with peak daily utilization rates greater than 80% or error rate greather than 10% sorted by Comm fail, Error rate, and Utilization

| Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|
| | | | | | Tx | Rx |
| ● Muscat | 192.168.202.50 | Int #3 | swp02 | 41.402% | 0.059% | 0.047% |
| ● Muscat | 192.168.202.50 | Int #13 | swp12 | 35.697% | 0.064% | 0.073% |
| ● Internet | 10.100.36.1 | Int #1 | Fa0/0: FastEthernet0/0 | 12.112% | 6.322% | 5.654% |
| ● SCWANRTR | 38.102.148.163 | Int #7 | Se0/0/0:0: Serial0/0/0:0 | 0.000% | 61.016% | 82.168% |
| ● SC_UserSwitch_2 | 10.0.1.77 | Int #4 | Fa0/3: FastEthernet0/3 (Jim_Turk) | 0.000% | 1.973% | 84.008% |

5 total interfaces listed

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

The threshold levels are displayed at the top of this table for reference.

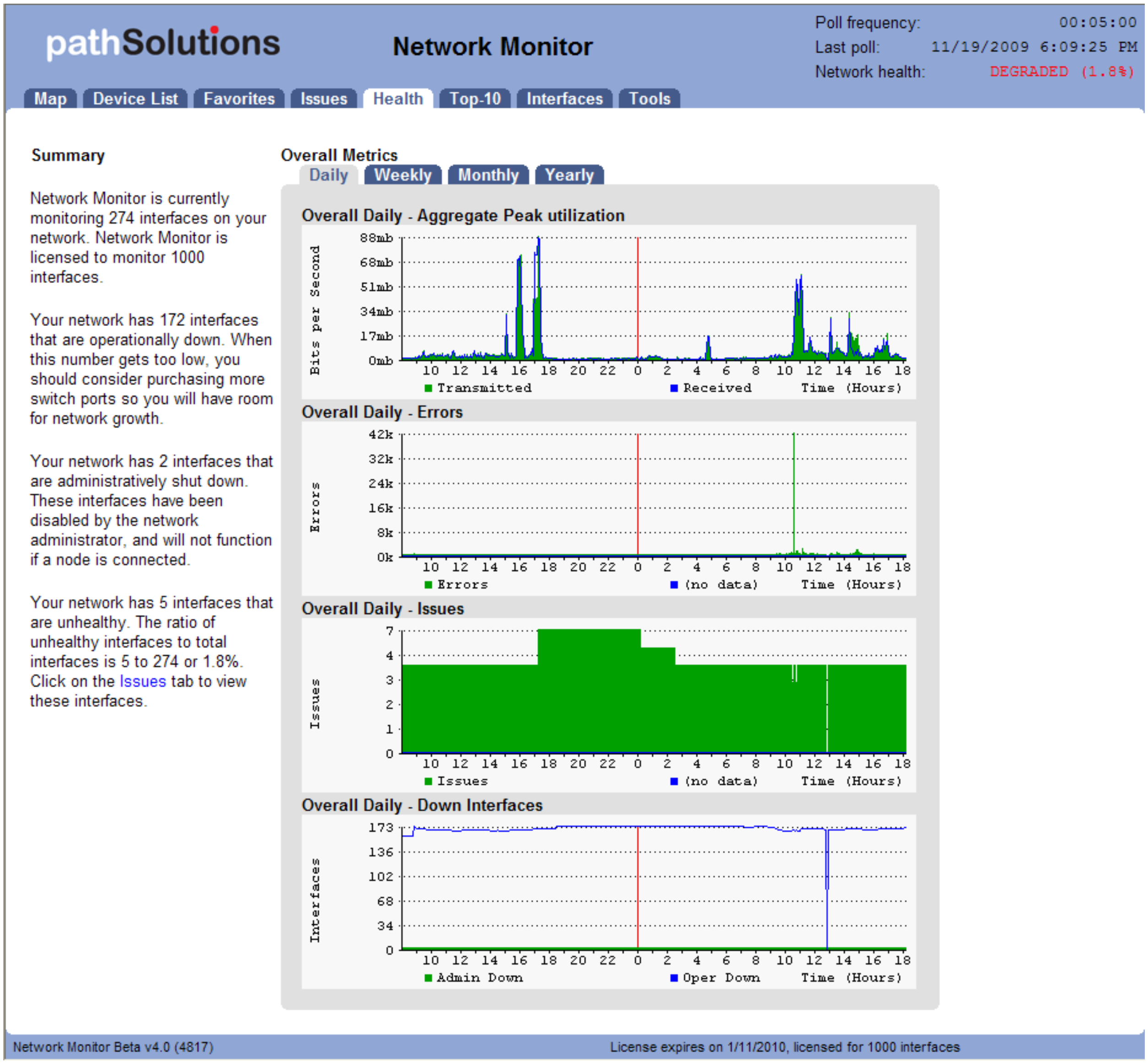
If the error rate or peak utilization rate is over the threshold, it will be displayed in red for easy determination of the interface problem.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

**Note:** Interfaces that have been over threshold sometime in the past 24 hours are listed. Interfaces will roll off of the issues list if it is under the error rate and utilization rate for a full 24 hours

## *Health*

Overall network health information can be viewed on the Health tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

**Summary**

Network Monitor is currently monitoring 274 interfaces on your network. Network Monitor is licensed to monitor 1000 interfaces.

Your network has 172 interfaces that are operationally down. When this number gets too low, you should consider purchasing more switch ports so you will have room for network growth.

Your network has 2 interfaces that are administratively shut down. These interfaces have been disabled by the network administrator, and will not function if a node is connected.

Your network has 5 interfaces that are unhealthy. The ratio of unhealthy interfaces to total interfaces is 5 to 274 or 1.8%. Click on the Issues tab to view these interfaces.

**Overall Metrics**

**Overall Daily - Aggregate Peak utilization**

**Overall Daily - Errors**

**Overall Daily - Issues**

**Overall Daily - Down Interfaces**

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

The summary section includes information about interfaces and their status.

The Overall Metrics section includes Daily, Weekly, Monthly, and Yearly information on:

*Overall Utilization* -- This is a summation of all traffic on all interfaces. This provides you with an understanding of when your network is most heavily utilized.

*Overall Errors* -- This is a summation of all network errors on all interfaces. This provides you with an understanding of when your network has the most overall errors.
*Overall Issues* -- This graph tracks the number of issues that exist on your network. This can help you to track how healthy your network is over time.

*Overall Down Interfaces* -- This graph tracks the number of operationally shut down and administratively shut down interfaces on your network. As you add nodes, the number of operationally shut down interfaces will drop. As you remove nodes, the number of operationally shut down interfaces will rise.

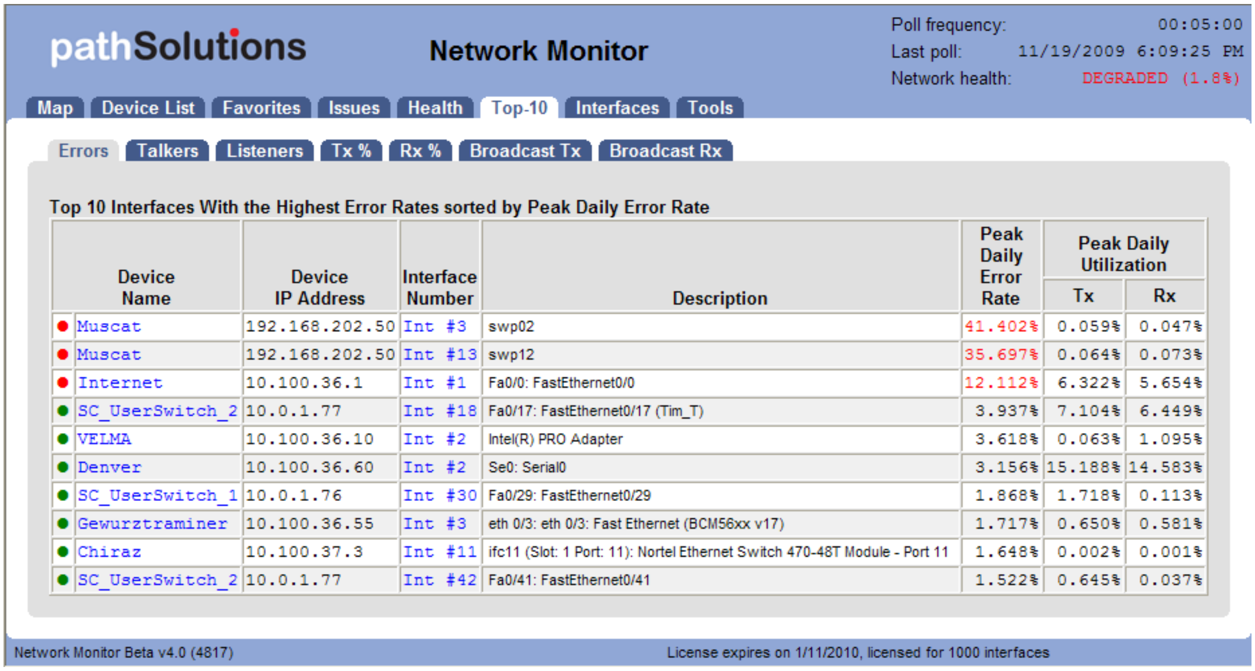
**Note:** The Overall Down Interfaces graph is useful to track when people connect and disconnect from your network. If you have users with laptops who connect every Monday and Tuesday, you should see the effect on this graph. Likewise, if you have a policy to power down all desktops on the weekend, you should see that policy in effect here.

## *Top 10*

The top 10 section provides you with overall network information for all monitored interfaces. This section is handy for determining what is occurring on the network regarding errors, utilization, and broadcast levels..

### Top Errors

The top 10 interfaces with the highest error rates are listed under the "Top Stats" tab, in the "Top Errors" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Error Rates sorted by Peak Daily Error Rate

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx |
| ● | Muscat | 192.168.202.50 | Int #3 | swp02 | 41.402% | 0.059% | 0.047% |
| ● | Muscat | 192.168.202.50 | Int #13 | swp12 | 35.697% | 0.064% | 0.073% |
| ● | Internet | 10.100.36.1 | Int #1 | Fa0/0: FastEthernet0/0 | 12.112% | 6.322% | 5.654% |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 3.937% | 7.104% | 6.449% |
| ● | VELMA | 10.100.36.10 | Int #2 | Intel(R) PRO Adapter | 3.618% | 0.063% | 1.095% |
| ● | Denver | 10.100.36.60 | Int #2 | Se0: Serial0 | 3.156% | 15.188% | 14.583% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #30 | Fa0/29: FastEthernet0/29 | 1.868% | 1.718% | 0.113% |
| ● | Gewurztraminer | 10.100.36.55 | Int #3 | eth 0/3: eth 0/3: Fast Ethernet (BCM56xx v17) | 1.717% | 0.650% | 0.581% |
| ● | Chiraz | 10.100.37.3 | Int #11 | ifc11 (Slot: 1 Port: 11): Nortel Ethernet Switch 470-48T Module - Port 11 | 1.648% | 0.002% | 0.001% |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #42 | Fa0/41: FastEthernet0/41 | 1.522% | 0.645% | 0.037% |

Network Monitor Beta v4.0 (4817)

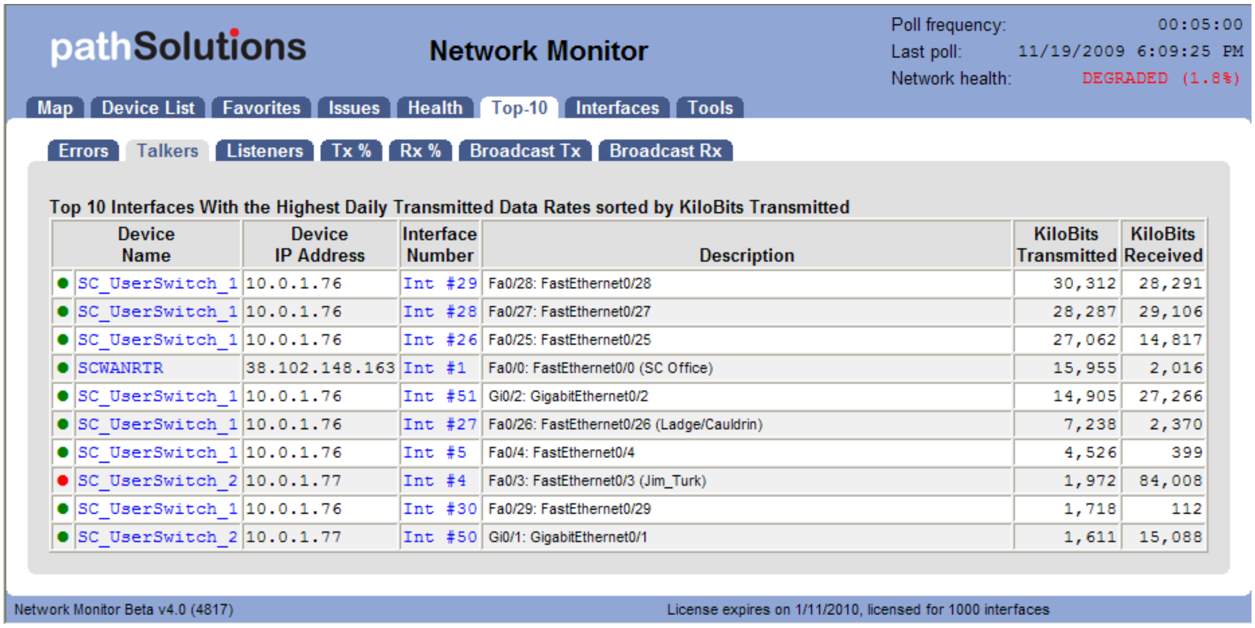
License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see what interfaces have errors that are approaching the error threshold.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

## Top Talkers

The top 10 interfaces with the most data transmitted are listed under the "Top Talkers" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Daily Transmitted Data Rates sorted by KiloBits Transmitted

| | Device Name | Device IP Address | Interface Number | Description | KiloBits Transmitted | KiloBits Received |
|---|---|---|---|---|---|---|
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #29 | Fa0/28: FastEthernet0/28 | 30,312 | 28,291 |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #28 | Fa0/27: FastEthernet0/27 | 28,287 | 29,106 |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #26 | Fa0/25: FastEthernet0/25 | 27,062 | 14,817 |
| ● | SCWANRTR | 38.102.148.163 | Int #1 | Fa0/0: FastEthernet0/0 (SC Office) | 15,955 | 2,016 |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #51 | Gi0/2: GigabitEthernet0/2 | 14,905 | 27,266 |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #27 | Fa0/26: FastEthernet0/26 (Ladge/Cauldrin) | 7,238 | 2,370 |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #5 | Fa0/4: FastEthernet0/4 | 4,526 | 399 |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #4 | Fa0/3: FastEthernet0/3 (Jim_Turk) | 1,972 | 84,008 |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #30 | Fa0/29: FastEthernet0/29 | 1,718 | 112 |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #50 | Gi0/1: GigabitEthernet0/1 | 1,611 | 15,088 |

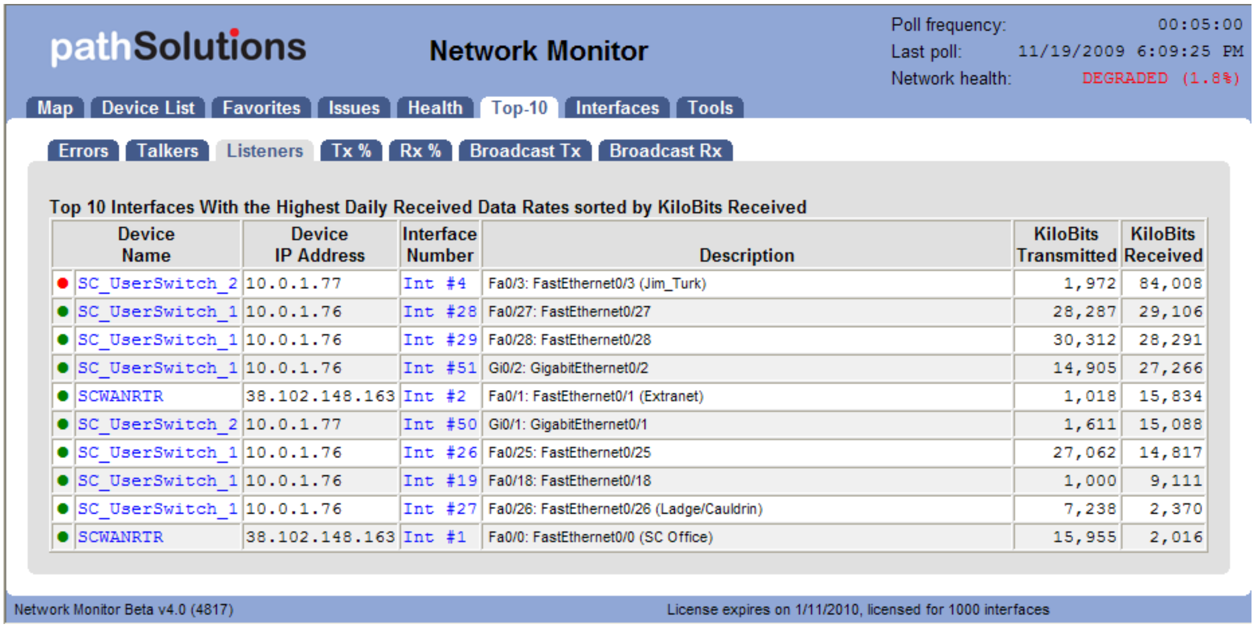
Network Monitor Beta v4.0 (4817)
License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see what interfaces physically transmit the most data regardless of interface speed.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

## Top Listeners

The top 10 interfaces with the most data received are listed under the "Top Listeners" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Daily Received Data Rates sorted by KiloBits Received

| | Device Name | Device IP Address | Interface Number | Description | KiloBits Transmitted | KiloBits Received |
|---|---|---|---|---|---|---|
| 🔴 | SC_UserSwitch_2 | 10.0.1.77 | Int #4 | Fa0/3: FastEthernet0/3 (Jim_Turk) | 1,972 | 84,008 |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Int #28 | Fa0/27: FastEthernet0/27 | 28,287 | 29,106 |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Int #29 | Fa0/28: FastEthernet0/28 | 30,312 | 28,291 |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Int #51 | Gi0/2: GigabitEthernet0/2 | 14,905 | 27,266 |
| 🟢 | SCWANRTR | 38.102.148.163 | Int #2 | Fa0/1: FastEthernet0/1 (Extranet) | 1,018 | 15,834 |
| 🟢 | SC_UserSwitch_2 | 10.0.1.77 | Int #50 | Gi0/1: GigabitEthernet0/1 | 1,611 | 15,088 |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Int #26 | Fa0/25: FastEthernet0/25 | 27,062 | 14,817 |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Int #19 | Fa0/18: FastEthernet0/18 | 1,000 | 9,111 |
| 🟢 | SC_UserSwitch_1 | 10.0.1.76 | Int #27 | Fa0/26: FastEthernet0/26 (Ladge/Cauldrin) | 7,238 | 2,370 |
| 🟢 | SCWANRTR | 38.102.148.163 | Int #1 | Fa0/0: FastEthernet0/0 (SC Office) | 15,955 | 2,016 |

Network Monitor Beta v4.0 (4817)

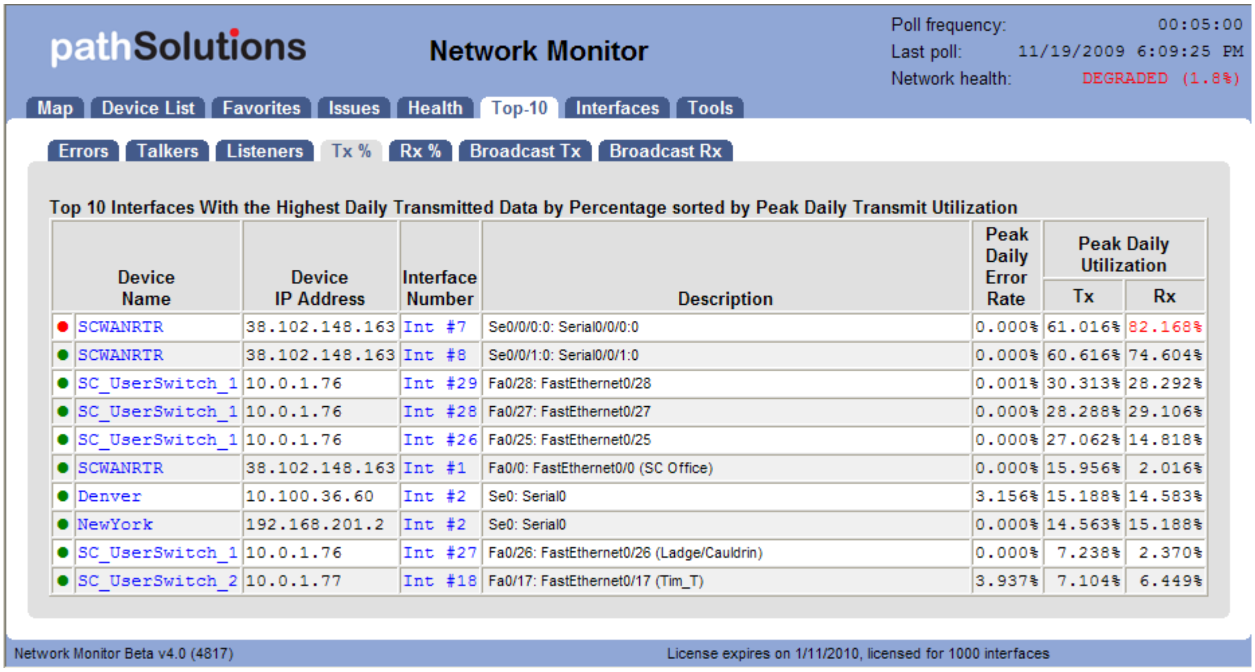
License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see what interfaces physically receive the most data regardless of interface speed.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

## Top Transmitters by Percent

The top 10 interfaces with the most data transmitted by percentage can be viewed under the "Top Tx %" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Daily Transmitted Data by Percentage sorted by Peak Daily Transmit Utilization

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx |
| ● | SCWANRTR | 38.102.148.163 | Int #7 | Se0/0/0:0: Serial0/0/0:0 | 0.000% | 61.016% | 82.168% |
| ● | SCWANRTR | 38.102.148.163 | Int #8 | Se0/0/1:0: Serial0/0/1:0 | 0.000% | 60.616% | 74.604% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #29 | Fa0/28: FastEthernet0/28 | 0.001% | 30.313% | 28.292% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #28 | Fa0/27: FastEthernet0/27 | 0.000% | 28.288% | 29.106% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #26 | Fa0/25: FastEthernet0/25 | 0.000% | 27.062% | 14.818% |
| ● | SCWANRTR | 38.102.148.163 | Int #1 | Fa0/0: FastEthernet0/0 (SC Office) | 0.000% | 15.956% | 2.016% |
| ● | Denver | 10.100.36.60 | Int #2 | Se0: Serial0 | 3.156% | 15.188% | 14.583% |
| ● | NewYork | 192.168.201.2 | Int #2 | Se0: Serial0 | 0.000% | 14.563% | 15.188% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #27 | Fa0/26: FastEthernet0/26 (Ladge/Cauldrin) | 0.000% | 7.238% | 2.370% |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 3.937% | 7.104% | 6.449% |

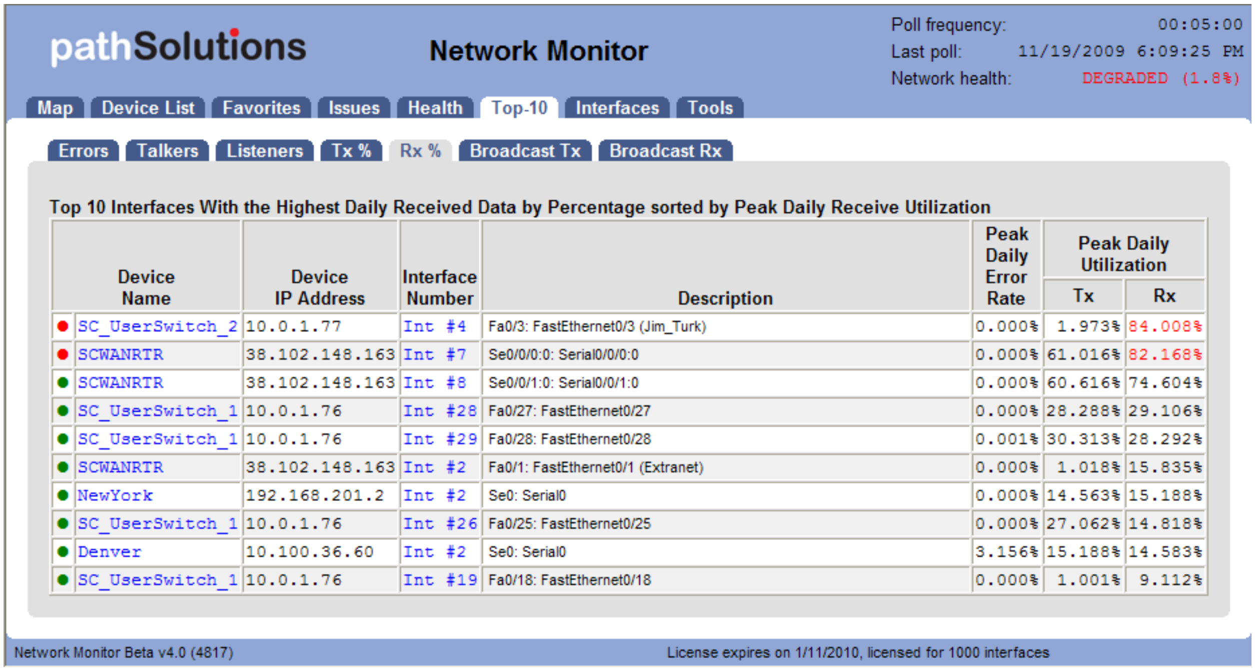
Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see which interfaces have transmitted data rates that are the highest by percentage utilization.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

## Top Receivers by Percent

The top 10 interfaces with the most data received by percentage are listed under the "Top Rx %" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Daily Received Data by Percentage sorted by Peak Daily Receive Utilization

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #4 | Fa0/3: FastEthernet0/3 (Jim_Turk) | 0.000% | 1.973% | 84.008% |
| ● | SCWANRTR | 38.102.148.163 | Int #7 | Se0/0/0:0: Serial0/0/0:0 | 0.000% | 61.016% | 82.168% |
| ● | SCWANRTR | 38.102.148.163 | Int #8 | Se0/0/1:0: Serial0/0/1:0 | 0.000% | 60.616% | 74.604% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #28 | Fa0/27: FastEthernet0/27 | 0.000% | 28.288% | 29.106% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #29 | Fa0/28: FastEthernet0/28 | 0.001% | 30.313% | 28.292% |
| ● | SCWANRTR | 38.102.148.163 | Int #2 | Fa0/1: FastEthernet0/1 (Extranet) | 0.000% | 1.018% | 15.835% |
| ● | NewYork | 192.168.201.2 | Int #2 | Se0: Serial0 | 0.000% | 14.563% | 15.188% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #26 | Fa0/25: FastEthernet0/25 | 0.000% | 27.062% | 14.818% |
| ● | Denver | 10.100.36.60 | Int #2 | Se0: Serial0 | 3.156% | 15.188% | 14.583% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #19 | Fa0/18: FastEthernet0/18 | 0.000% | 1.001% | 9.112% |

Network Monitor Beta v4.0 (4817)

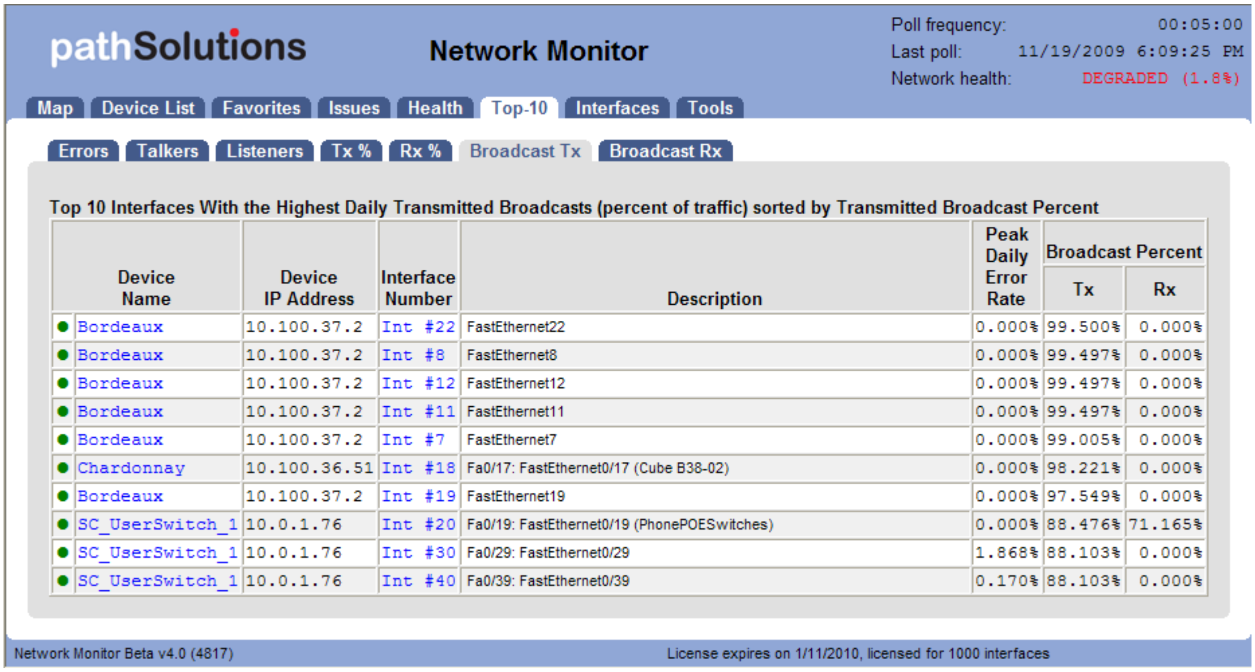
License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see which interfaces have received data rates that are the highest by percentage utilization.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

## Top Transmitted Broadcast by Percent

The top 10 interfaces with the most broadcasts transmitted by percentage are listed under the "Top Broadcast Tx %" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Daily Transmitted Broadcasts (percent of traffic) sorted by Transmitted Broadcast Percent

| Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Broadcast Percent | |
|---|---|---|---|---|---|---|
| | | | | | Tx | Rx |
| ● Bordeaux | 10.100.37.2 | Int #22 | FastEthernet22 | 0.000% | 99.500% | 0.000% |
| ● Bordeaux | 10.100.37.2 | Int #8 | FastEthernet8 | 0.000% | 99.497% | 0.000% |
| ● Bordeaux | 10.100.37.2 | Int #12 | FastEthernet12 | 0.000% | 99.497% | 0.000% |
| ● Bordeaux | 10.100.37.2 | Int #11 | FastEthernet11 | 0.000% | 99.497% | 0.000% |
| ● Bordeaux | 10.100.37.2 | Int #7 | FastEthernet7 | 0.000% | 99.005% | 0.000% |
| ● Chardonnay | 10.100.36.51 | Int #18 | Fa0/17: FastEthernet0/17 (Cube B38-02) | 0.000% | 98.221% | 0.000% |
| ● Bordeaux | 10.100.37.2 | Int #19 | FastEthernet19 | 0.000% | 97.549% | 0.000% |
| ● SC_UserSwitch_1 | 10.0.1.76 | Int #20 | Fa0/19: FastEthernet0/19 (PhonePOESwitches) | 0.000% | 88.476% | 71.165% |
| ● SC_UserSwitch_1 | 10.0.1.76 | Int #30 | Fa0/29: FastEthernet0/29 | 1.868% | 88.103% | 0.000% |
| ● SC_UserSwitch_1 | 10.0.1.76 | Int #40 | Fa0/39: FastEthernet0/39 | 0.170% | 88.103% | 0.000% |

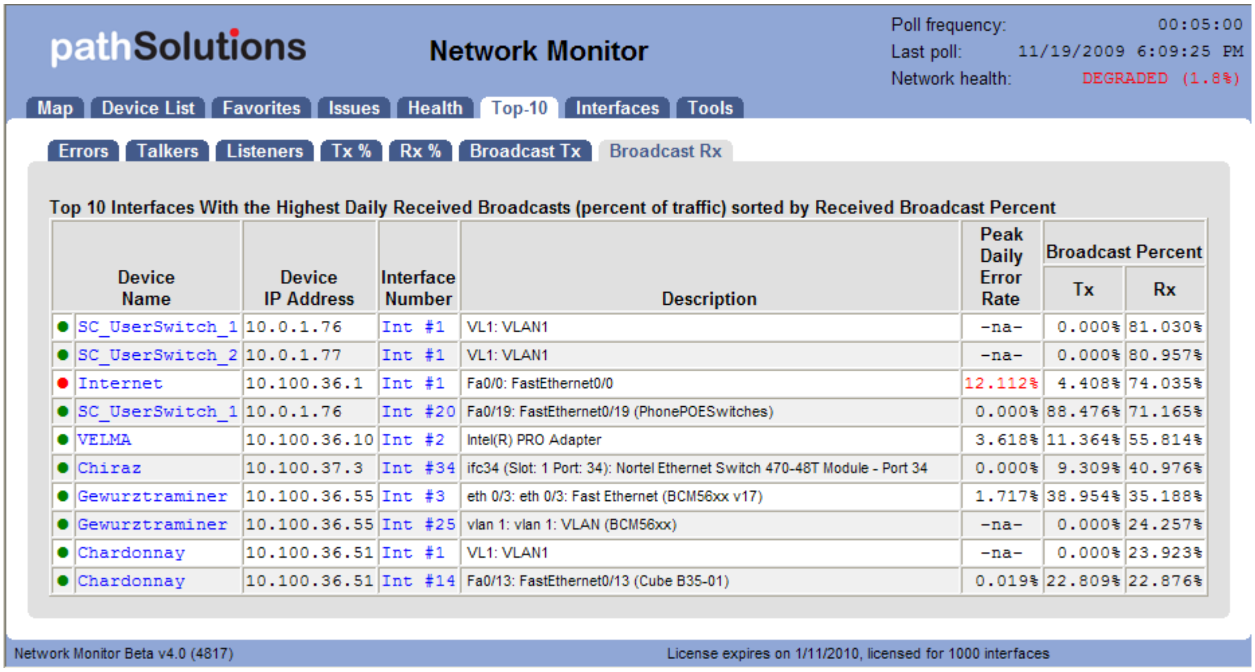
Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see what interfaces have transmitted the most broadcasts.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

### Top Received Broadcast by Percent

The top 10 interfaces with the most broadcasts received by percentage are listed under the "Top Broadcast Rx %" sub-tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Top 10 Interfaces With the Highest Daily Received Broadcasts (percent of traffic) sorted by Received Broadcast Percent

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Broadcast Percent | |
|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #1 | VL1: VLAN1 | -na- | 0.000% | 81.030% |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #1 | VL1: VLAN1 | -na- | 0.000% | 80.957% |
| ● | Internet | 10.100.36.1 | Int #1 | Fa0/0: FastEthernet0/0 | 12.112% | 4.408% | 74.035% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #20 | Fa0/19: FastEthernet0/19 (PhonePOESwitches) | 0.000% | 88.476% | 71.165% |
| ● | VELMA | 10.100.36.10 | Int #2 | Intel(R) PRO Adapter | 3.618% | 11.364% | 55.814% |
| ● | Chiraz | 10.100.37.3 | Int #34 | ifc34 (Slot: 1 Port: 34): Nortel Ethernet Switch 470-48T Module - Port 34 | 0.000% | 9.309% | 40.976% |
| ● | Gewurztraminer | 10.100.36.55 | Int #3 | eth 0/3: eth 0/3: Fast Ethernet (BCM56xx v17) | 1.717% | 38.954% | 35.188% |
| ● | Gewurztraminer | 10.100.36.55 | Int #25 | vlan 1: vlan 1: VLAN (BCM56xx) | -na- | 0.000% | 24.257% |
| ● | Chardonnay | 10.100.36.51 | Int #1 | VL1: VLAN1 | -na- | 0.000% | 23.923% |
| ● | Chardonnay | 10.100.36.51 | Int #14 | Fa0/13: FastEthernet0/13 (Cube B35-01) | 0.019% | 22.809% | 22.876% |

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

This tab allows you to see what interfaces have received the most broadcasts.

**Note:** This information is used to determine if a device is transmitting a lot of broadcasts on the network (and your network devices are receiving them). If you have an interface that is receiving a high level of broadcasts, investigate the device that is connected to it to determine why it is transmitting a lot of broadcasts.

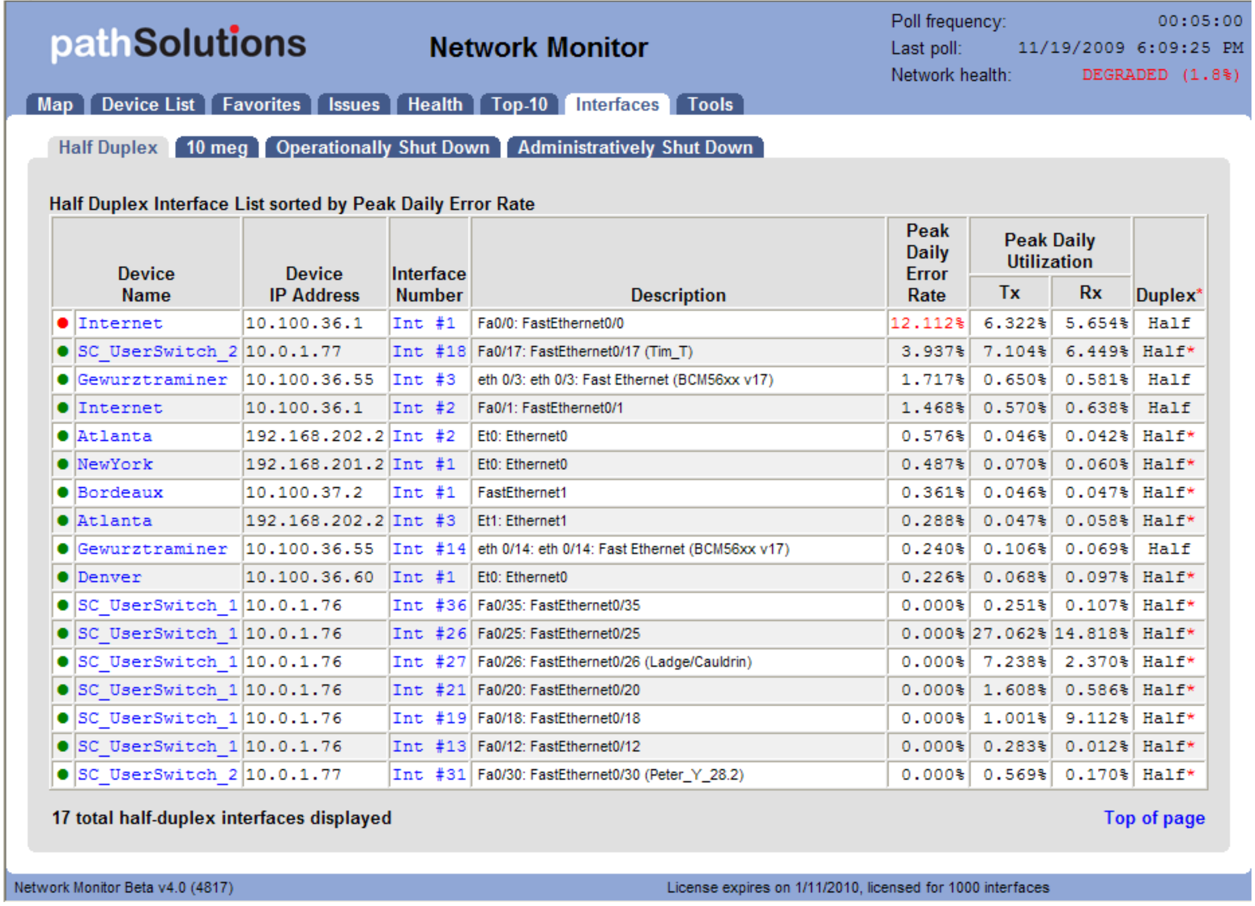
You can click on the interface number to jump to the interface details page and view the utilization and error information.

## *Interfaces Tab*

This section identifies interfaces with specific conditions.

### Half Duplex Interface Report

Interfaces that are configured for half-duplex or are showing collision counters are displayed on this report:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:09:25 PM
Network health: DEGRADED (1.8%)

Half Duplex Interface List sorted by Peak Daily Error Rate

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | | Duplex* |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx | |
| ● | Internet | 10.100.36.1 | Int #1 | Fa0/0: FastEthernet0/0 | 12.112% | 6.322% | 5.654% | Half |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 3.937% | 7.104% | 6.449% | Half* |
| ● | Gewurztraminer | 10.100.36.55 | Int #3 | eth 0/3: eth 0/3: Fast Ethernet (BCM56xx v17) | 1.717% | 0.650% | 0.581% | Half |
| ● | Internet | 10.100.36.1 | Int #2 | Fa0/1: FastEthernet0/1 | 1.468% | 0.570% | 0.638% | Half |
| ● | Atlanta | 192.168.202.2 | Int #2 | Et0: Ethernet0 | 0.576% | 0.046% | 0.042% | Half* |
| ● | NewYork | 192.168.201.2 | Int #1 | Et0: Ethernet0 | 0.487% | 0.070% | 0.060% | Half* |
| ● | Bordeaux | 10.100.37.2 | Int #1 | FastEthernet1 | 0.361% | 0.046% | 0.047% | Half* |
| ● | Atlanta | 192.168.202.2 | Int #3 | Et1: Ethernet1 | 0.288% | 0.047% | 0.058% | Half* |
| ● | Gewurztraminer | 10.100.36.55 | Int #14 | eth 0/14: eth 0/14: Fast Ethernet (BCM56xx v17) | 0.240% | 0.106% | 0.069% | Half |
| ● | Denver | 10.100.36.60 | Int #1 | Et0: Ethernet0 | 0.226% | 0.068% | 0.097% | Half* |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #36 | Fa0/35: FastEthernet0/35 | 0.000% | 0.251% | 0.107% | Half* |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #26 | Fa0/25: FastEthernet0/25 | 0.000% | 27.062% | 14.818% | Half* |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #27 | Fa0/26: FastEthernet0/26 (Ladge/Cauldrin) | 0.000% | 7.238% | 2.370% | Half* |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #21 | Fa0/20: FastEthernet0/20 | 0.000% | 1.608% | 0.586% | Half* |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #19 | Fa0/18: FastEthernet0/18 | 0.000% | 1.001% | 9.112% | Half* |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #13 | Fa0/12: FastEthernet0/12 | 0.000% | 0.283% | 0.012% | Half* |
| ● | SC_UserSwitch_2 | 10.0.1.77 | Int #31 | Fa0/30: FastEthernet0/30 (Peter_Y_28.2) | 0.000% | 0.569% | 0.170% | Half* |

17 total half-duplex interfaces displayed

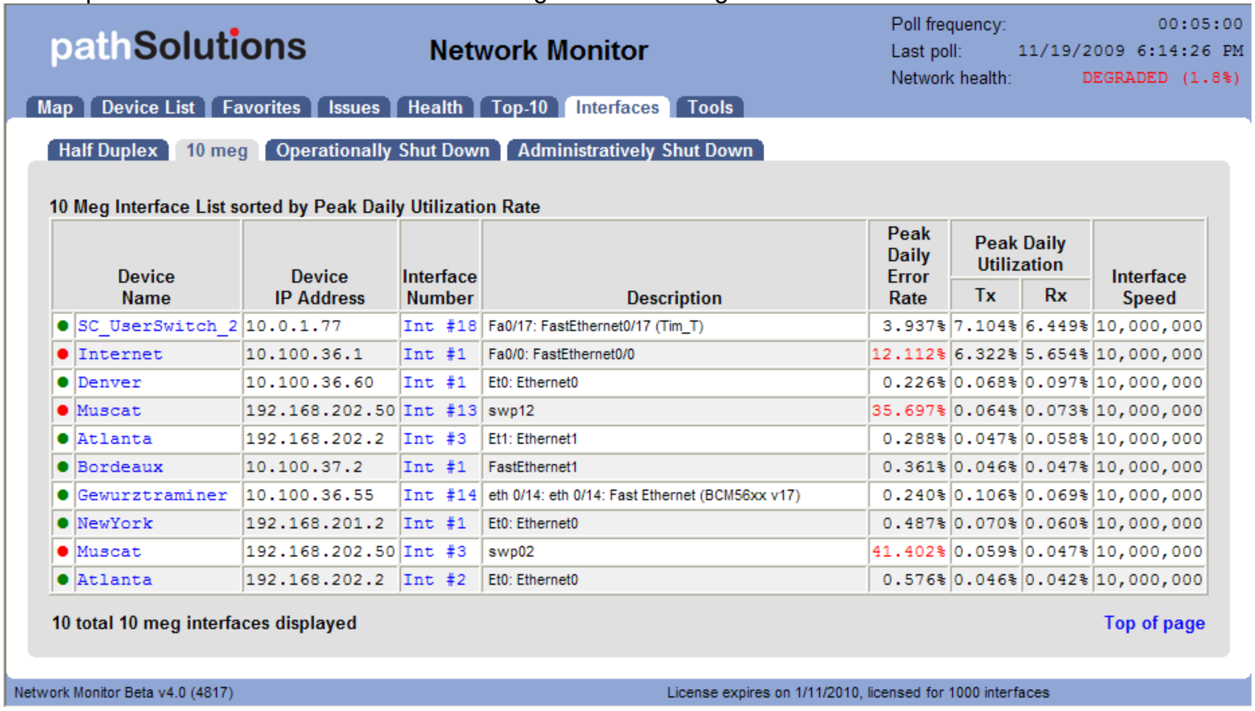
Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

With modern switched networks, no interfaces should be configured for half-duplex or creating collisions on the network.  This report discloses all interfaces that are either configured for half-duplex operation, or have collision error counters.

## 10Meg Interface Report

This report shows all interfaces that are configured for 10meg Ethernet:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:14:26 PM
Network health: DEGRADED (1.8%)

10 Meg Interface List sorted by Peak Daily Utilization Rate

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | | Interface Speed |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx | |
| 🟢 | SC_UserSwitch_2 | 10.0.1.77 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 3.937% | 7.104% | 6.449% | 10,000,000 |
| 🔴 | Internet | 10.100.36.1 | Int #1 | Fa0/0: FastEthernet0/0 | 12.112% | 6.322% | 5.654% | 10,000,000 |
| 🟢 | Denver | 10.100.36.60 | Int #1 | Et0: Ethernet0 | 0.226% | 0.068% | 0.097% | 10,000,000 |
| 🔴 | Muscat | 192.168.202.50 | Int #13 | swp12 | 35.697% | 0.064% | 0.073% | 10,000,000 |
| 🟢 | Atlanta | 192.168.202.2 | Int #3 | Et1: Ethernet1 | 0.288% | 0.047% | 0.058% | 10,000,000 |
| 🟢 | Bordeaux | 10.100.37.2 | Int #1 | FastEthernet1 | 0.361% | 0.046% | 0.047% | 10,000,000 |
| 🟢 | Gewurztraminer | 10.100.36.55 | Int #14 | eth 0/14: eth 0/14: Fast Ethernet (BCM56xx v17) | 0.240% | 0.106% | 0.069% | 10,000,000 |
| 🟢 | NewYork | 192.168.201.2 | Int #1 | Et0: Ethernet0 | 0.487% | 0.070% | 0.060% | 10,000,000 |
| 🔴 | Muscat | 192.168.202.50 | Int #3 | swp02 | 41.402% | 0.059% | 0.047% | 10,000,000 |
| 🟢 | Atlanta | 192.168.202.2 | Int #2 | Et0: Ethernet0 | 0.576% | 0.046% | 0.042% | 10,000,000 |

10 total 10 meg interfaces displayed

Network Monitor Beta v4.0 (4817)

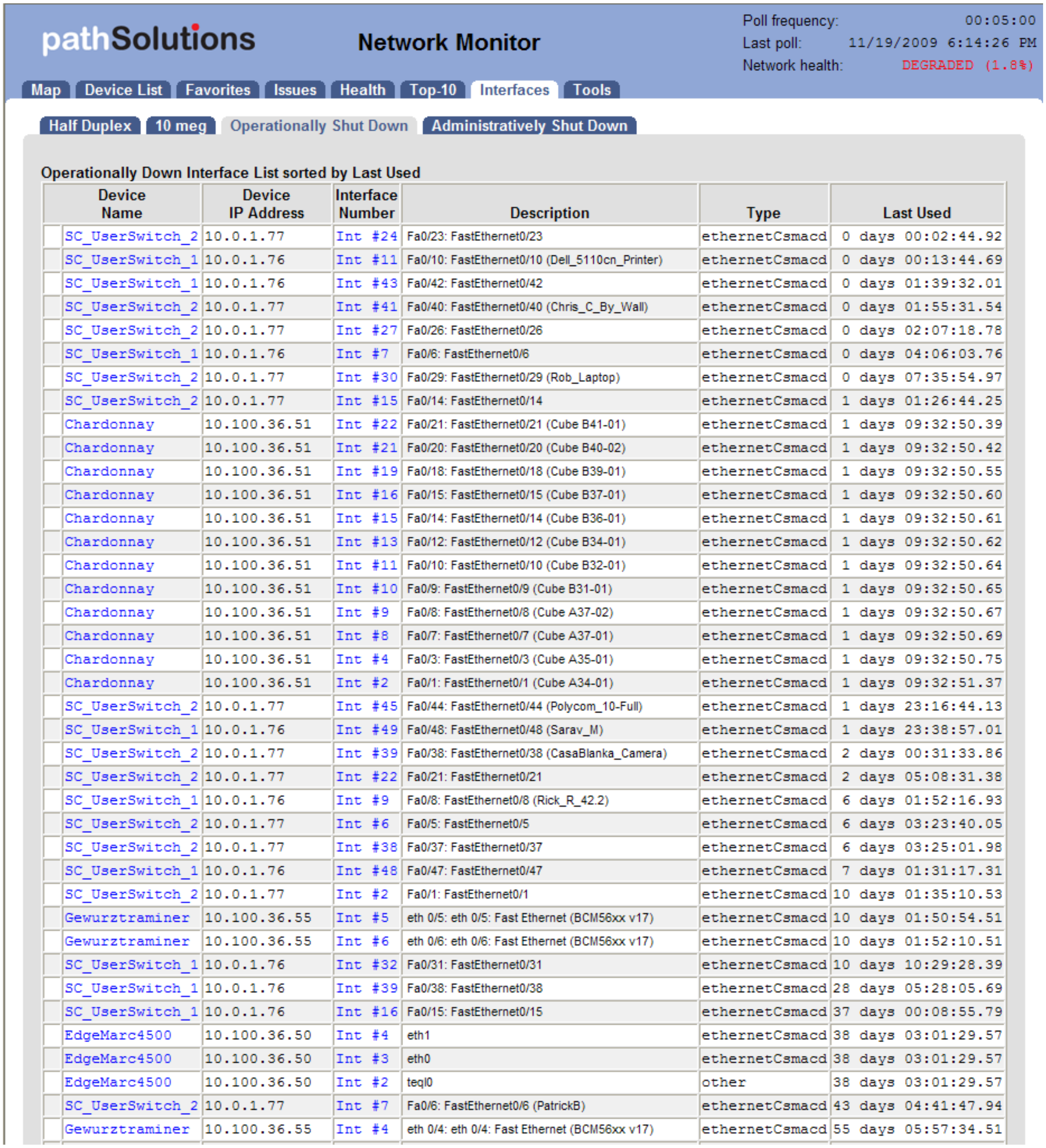
License expires on 1/11/2010, licensed for 1000 interfaces

Since virtually all network adapters that have been sold in the past 10 years are both 10meg and 100meg capable, this report discloses interfaces that are configured for 10meg. Network performance can be generally improved by changing these adapters to use 100meg speeds instead of 10meg.

Note: Even if a network link has low utilization, it can still benefit from upgrading to 100meg, as the latency to stream small chunks of data across a 10meg link can be reduced significantly by increasing the bandwidth ten-fold.

### Operationally Shut Down Interface Report

Operationally shut down interfaces are listed under the "Operationally Shut Down" tab:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:14:26 PM
Network health: DEGRADED (1.8%)

Operationally Down Interface List sorted by Last Used

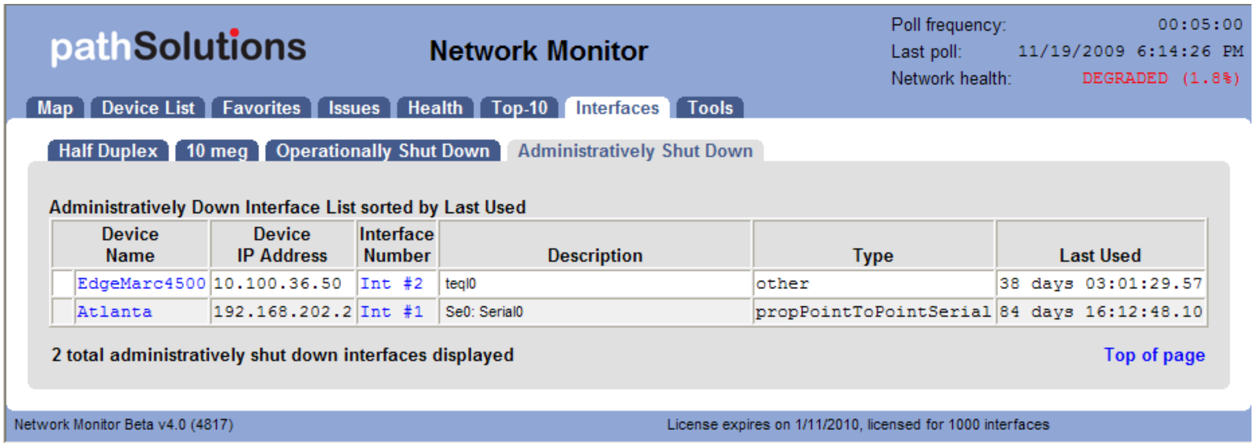
| | Device Name | Device IP Address | Interface Number | Description | Type | Last Used |
|---|---|---|---|---|---|---|
| | SC_UserSwitch_2 | 10.0.1.77 | Int #24 | Fa0/23: FastEthernet0/23 | ethernetCsmacd | 0 days 00:02:44.92 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #11 | Fa0/10: FastEthernet0/10 (Dell_5110cn_Printer) | ethernetCsmacd | 0 days 00:13:44.69 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #43 | Fa0/42: FastEthernet0/42 | ethernetCsmacd | 0 days 01:39:32.01 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #41 | Fa0/40: FastEthernet0/40 (Chris_C_By_Wall) | ethernetCsmacd | 0 days 01:55:31.54 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #27 | Fa0/26: FastEthernet0/26 | ethernetCsmacd | 0 days 02:07:18.78 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #7 | Fa0/6: FastEthernet0/6 | ethernetCsmacd | 0 days 04:06:03.76 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #30 | Fa0/29: FastEthernet0/29 (Rob_Laptop) | ethernetCsmacd | 0 days 07:35:54.97 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #15 | Fa0/14: FastEthernet0/14 | ethernetCsmacd | 1 days 01:26:44.25 |
| | Chardonnay | 10.100.36.51 | Int #22 | Fa0/21: FastEthernet0/21 (Cube B41-01) | ethernetCsmacd | 1 days 09:32:50.39 |
| | Chardonnay | 10.100.36.51 | Int #21 | Fa0/20: FastEthernet0/20 (Cube B40-02) | ethernetCsmacd | 1 days 09:32:50.42 |
| | Chardonnay | 10.100.36.51 | Int #19 | Fa0/18: FastEthernet0/18 (Cube B39-01) | ethernetCsmacd | 1 days 09:32:50.55 |
| | Chardonnay | 10.100.36.51 | Int #16 | Fa0/15: FastEthernet0/15 (Cube B37-01) | ethernetCsmacd | 1 days 09:32:50.60 |
| | Chardonnay | 10.100.36.51 | Int #15 | Fa0/14: FastEthernet0/14 (Cube B36-01) | ethernetCsmacd | 1 days 09:32:50.61 |
| | Chardonnay | 10.100.36.51 | Int #13 | Fa0/12: FastEthernet0/12 (Cube B34-01) | ethernetCsmacd | 1 days 09:32:50.62 |
| | Chardonnay | 10.100.36.51 | Int #11 | Fa0/10: FastEthernet0/10 (Cube B32-01) | ethernetCsmacd | 1 days 09:32:50.64 |
| | Chardonnay | 10.100.36.51 | Int #10 | Fa0/9: FastEthernet0/9 (Cube B31-01) | ethernetCsmacd | 1 days 09:32:50.65 |
| | Chardonnay | 10.100.36.51 | Int #9 | Fa0/8: FastEthernet0/8 (Cube A37-02) | ethernetCsmacd | 1 days 09:32:50.67 |
| | Chardonnay | 10.100.36.51 | Int #8 | Fa0/7: FastEthernet0/7 (Cube A37-01) | ethernetCsmacd | 1 days 09:32:50.69 |
| | Chardonnay | 10.100.36.51 | Int #4 | Fa0/3: FastEthernet0/3 (Cube A35-01) | ethernetCsmacd | 1 days 09:32:50.75 |
| | Chardonnay | 10.100.36.51 | Int #2 | Fa0/1: FastEthernet0/1 (Cube A34-01) | ethernetCsmacd | 1 days 09:32:51.37 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #45 | Fa0/44: FastEthernet0/44 (Polycom_10-Full) | ethernetCsmacd | 1 days 23:16:44.13 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #49 | Fa0/48: FastEthernet0/48 (Sarav_M) | ethernetCsmacd | 1 days 23:38:57.01 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #39 | Fa0/38: FastEthernet0/38 (CasaBlanka_Camera) | ethernetCsmacd | 2 days 00:31:33.86 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #22 | Fa0/21: FastEthernet0/21 | ethernetCsmacd | 2 days 05:08:31.38 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #9 | Fa0/8: FastEthernet0/8 (Rick_R_42.2) | ethernetCsmacd | 6 days 01:52:16.93 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #6 | Fa0/5: FastEthernet0/5 | ethernetCsmacd | 6 days 03:23:40.05 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #38 | Fa0/37: FastEthernet0/37 | ethernetCsmacd | 6 days 03:25:01.98 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #48 | Fa0/47: FastEthernet0/47 | ethernetCsmacd | 7 days 01:31:17.31 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #2 | Fa0/1: FastEthernet0/1 | ethernetCsmacd | 10 days 01:35:10.53 |
| | Gewurztraminer | 10.100.36.55 | Int #5 | eth 0/5: eth 0/5: Fast Ethernet (BCM56xx v17) | ethernetCsmacd | 10 days 01:50:54.51 |
| | Gewurztraminer | 10.100.36.55 | Int #6 | eth 0/6: eth 0/6: Fast Ethernet (BCM56xx v17) | ethernetCsmacd | 10 days 01:52:10.51 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #32 | Fa0/31: FastEthernet0/31 | ethernetCsmacd | 10 days 10:29:28.39 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #39 | Fa0/38: FastEthernet0/38 | ethernetCsmacd | 28 days 05:28:05.69 |
| | SC_UserSwitch_1 | 10.0.1.76 | Int #16 | Fa0/15: FastEthernet0/15 | ethernetCsmacd | 37 days 00:08:55.79 |
| | EdgeMarc4500 | 10.100.36.50 | Int #4 | eth1 | ethernetCsmacd | 38 days 03:01:29.57 |
| | EdgeMarc4500 | 10.100.36.50 | Int #3 | eth0 | ethernetCsmacd | 38 days 03:01:29.57 |
| | EdgeMarc4500 | 10.100.36.50 | Int #2 | teql0 | other | 38 days 03:01:29.57 |
| | SC_UserSwitch_2 | 10.0.1.77 | Int #7 | Fa0/6: FastEthernet0/6 (PatrickB) | ethernetCsmacd | 43 days 04:41:47.94 |
| | Gewurztraminer | 10.100.36.55 | Int #4 | eth 0/4: eth 0/4: Fast Ethernet (BCM56xx v17) | ethernetCsmacd | 55 days 05:57:34.51 |

This list displays all available (operationally shut down) interfaces on your network, including:

- Switch name
- Interface number
- Interface description
- Interface speed
- Interface type
- Interface last used time

### Administratively Shut Down Interface Report

Administratively shut down interfaces are listed under the "Administratively Shut Down" tab:



pathSolutions
Network Monitor
Poll frequency: 00:05:00
Last poll: 11/19/2009 6:14:26 PM
Network health: DEGRADED (1.8%)
Map
Device List
Favorites
Issues
Health
Top-10
Interfaces
Tools
Half Duplex
10 meg
Operationally Shut Down
Administratively Shut Down

Administratively Down Interface List sorted by Last Used

| Device Name | Device IP Address | Interface Number | Description | Type | Last Used |
|---|---|---|---|---|---|
| EdgeMarc4500 | 10.100.36.50 | Int #2 | teql0 | other | 38 days 03:01:29.57 |
| Atlanta | 192.168.202.2 | Int #1 | Se0: Serial0 | propPointToPointSerial | 84 days 16:12:48.10 |

2 total administratively shut down interfaces displayed

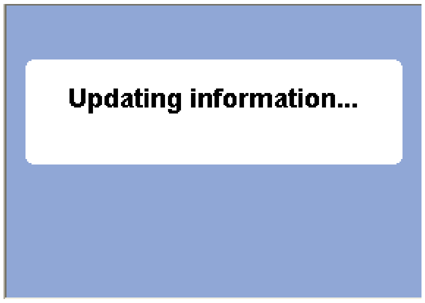
Top of page
Network Monitor Beta v4.0 (4817)
License expires on 1/11/2010, licensed for 1000 interfaces

This list displays interfaces that have been administratively shut down, and will not function unless the interface is brought online.

## *Tools*

Tools are provided to help locate IP addresses and MAC addresses on your network.

Before using any of the tools, you should click on the “Update” button to collect the Bridge table and ARP cache information from your network.



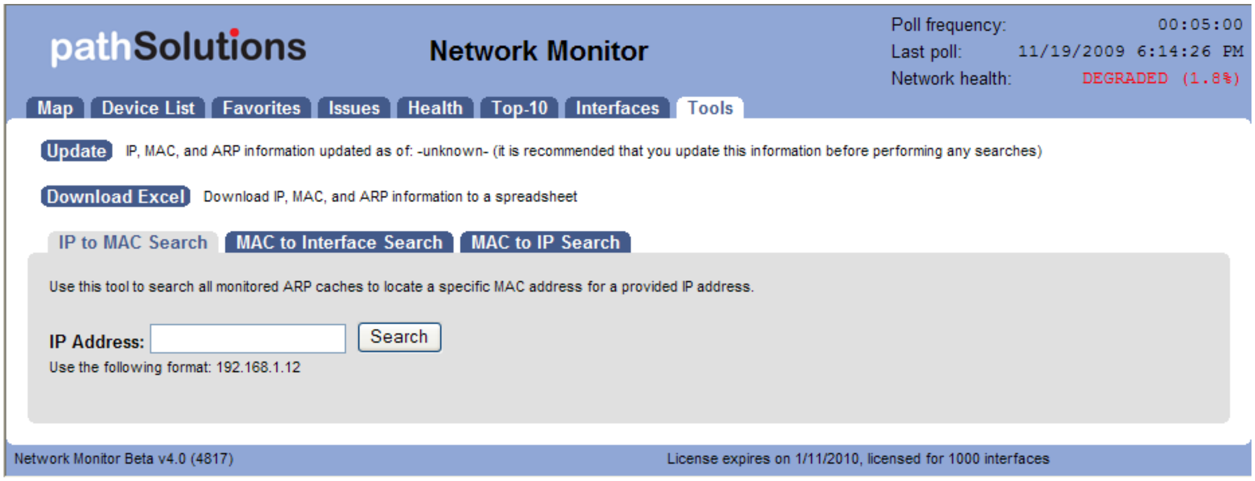
Updating information...

This process may take more than 10 minutes depending on the size of your network and the number of monitored devices.

After the update is complete, you can choose to download the information to an Excel spreadsheet, or perform queries against the information.

## Finding a MAC address for an IP address

Determining what MAC address goes with an IP address is easy if your computer is on the same subnet as the device, but can prove to be difficult if you have many subnets.



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:14:26 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: -unknown- (it is recommended that you update this information before performing any searches)

Download IP, MAC, and ARP information to a spreadsheet

Use this tool to search all monitored ARP caches to locate a specific MAC address for a provided IP address.

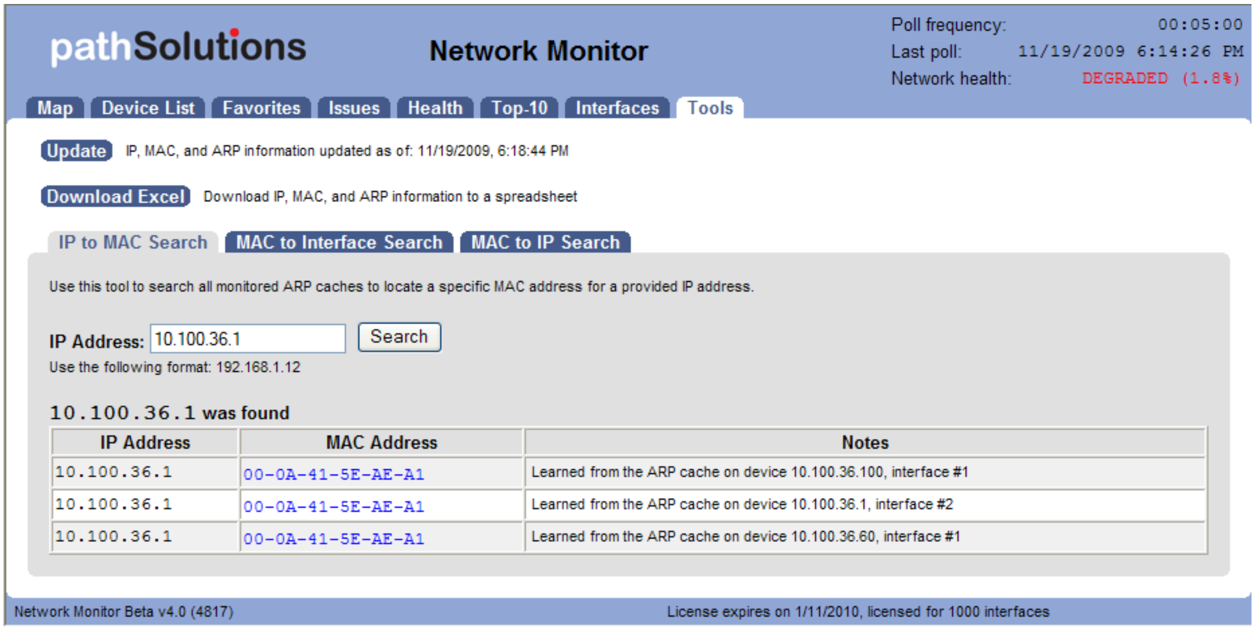
IP Address:

Use the following format: 192.168.1.12

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

From the IP to MAC search screen, enter the IP address that you want to find and click “Search”.

If the IP address was discovered in any monitored device’s ARP cache, it will be displayed along with the device where it was discovered:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:14:26 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:18:44 PM

Download IP, MAC, and ARP information to a spreadsheet

Use this tool to search all monitored ARP caches to locate a specific MAC address for a provided IP address.

IP Address: 10.100.36.1

Use the following format: 192.168.1.12

10.100.36.1 was found

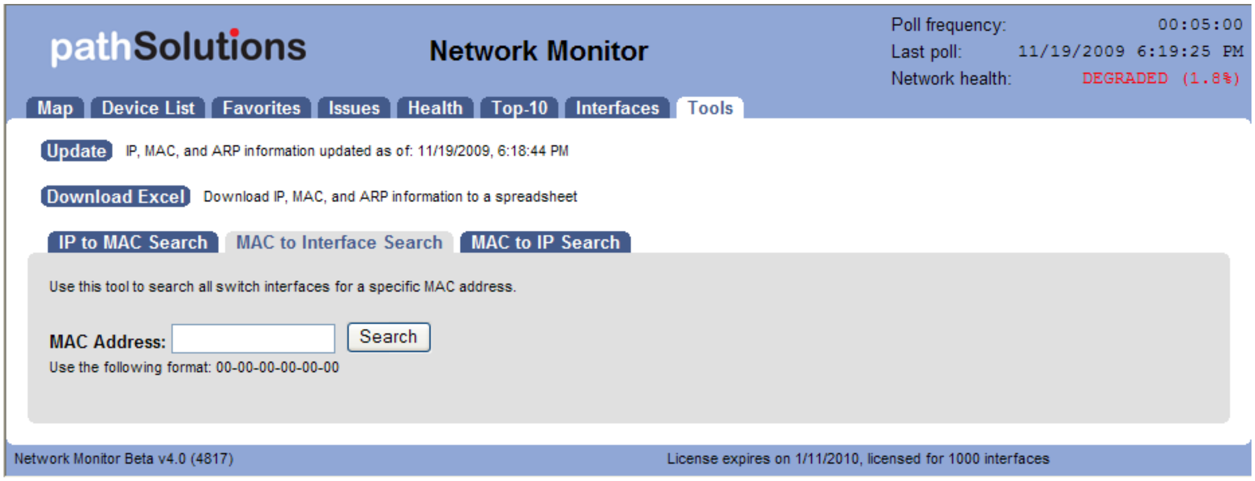
| IP Address | MAC Address | Notes |
|---|---|---|
| 10.100.36.1 | 00-0A-41-5E-AE-A1 | Learned from the ARP cache on device 10.100.36.100, interface #1 |
| 10.100.36.1 | 00-0A-41-5E-AE-A1 | Learned from the ARP cache on device 10.100.36.1, interface #2 |
| 10.100.36.1 | 00-0A-41-5E-AE-A1 | Learned from the ARP cache on device 10.100.36.60, interface #1 |

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

The MAC address will be displayed along with the device and interface where the MAC address was found in the device’s ARP cache.

### Finding a MAC address on a Switch Interface

Locating where a MAC address exists on a switch port can be difficult if you have a lot of switches to query.  This can easily be done on the MAC to Interface Search screen:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:19:25 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:18:44 PM

Download IP, MAC, and ARP information to a spreadsheet

Use this tool to search all switch interfaces for a specific MAC address.

MAC Address:

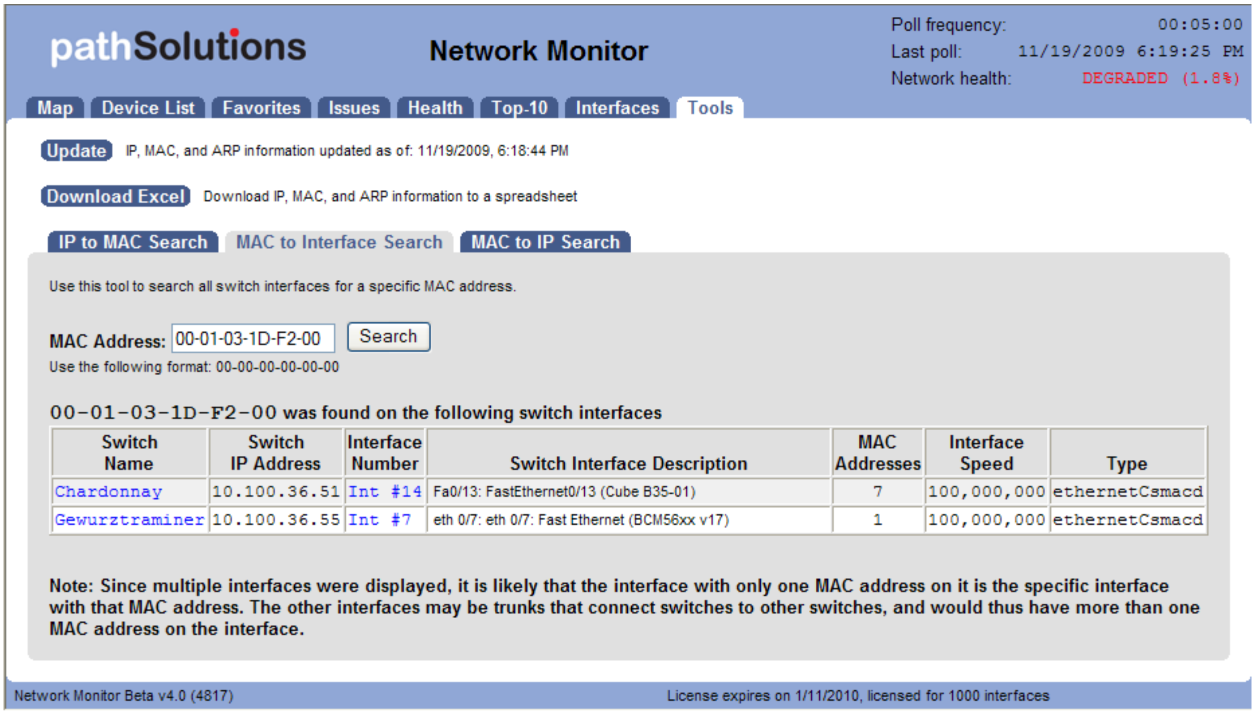
Use the following format: 00-00-00-00-00-00

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

Enter the MAC address that you want to search for and click “Search”.

If the MAC address is found on a switch, you should see the following:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:19:25 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:18:44 PM

Download IP, MAC, and ARP information to a spreadsheet

Use this tool to search all switch interfaces for a specific MAC address.

MAC Address: 00-01-03-1D-F2-00

Use the following format: 00-00-00-00-00-00

00-01-03-1D-F2-00 was found on the following switch interfaces

| Switch Name | Switch IP Address | Interface Number | Switch Interface Description | MAC Addresses | Interface Speed | Type |
|---|---|---|---|---|---|---|
| Chardonnay | 10.100.36.51 | Int #14 | Fa0/13: FastEthernet0/13 (Cube B35-01) | 7 | 100,000,000 | ethernetCsmacd |
| Gewurztraminer | 10.100.36.55 | Int #7 | eth 0/7: eth 0/7: Fast Ethernet (BCM56xx v17) | 1 | 100,000,000 | ethernetCsmacd |

**Note: Since multiple interfaces were displayed, it is likely that the interface with only one MAC address on it is the specific interface with that MAC address. The other interfaces may be trunks that connect switches to other switches, and would thus have more than one MAC address on the interface.**

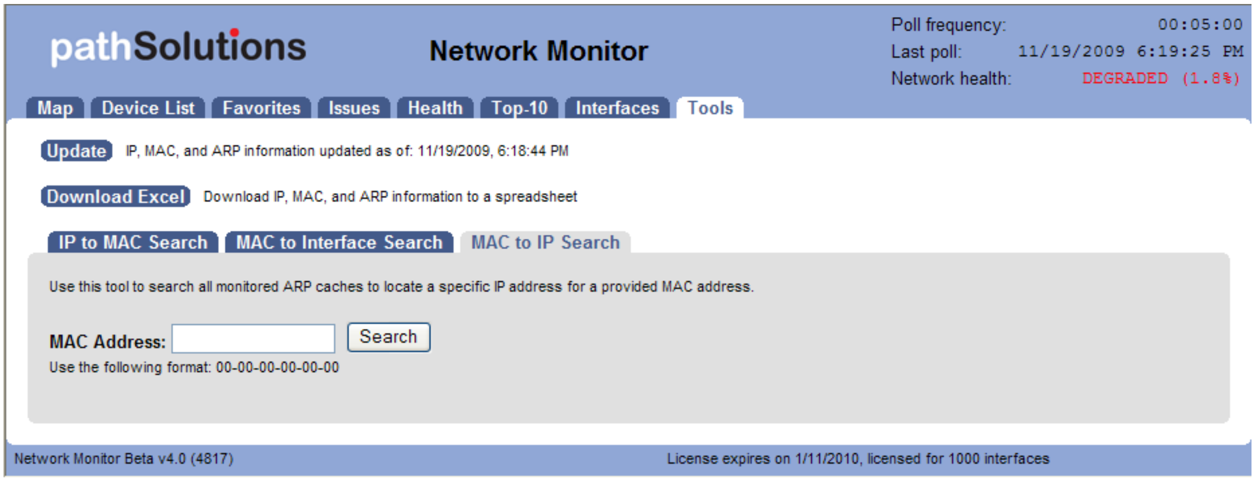
Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

Notice that the MAC address was discovered on more than one interface.  The “MAC Addresses” column will help you to determine how many MAC addresses exist on an interface.  This is useful for determining if an interface is a switch to switch trunk (more than one MAC address would exist on the link), or if the interface only has one MAC address connected (interface where the device is physically connected).

## Converting a MAC address to an IP address

If you have a MAC address and want to know what IP address it is associated with, use this tool:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:19:25 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:18:44 PM

Download IP, MAC, and ARP information to a spreadsheet

Use this tool to search all monitored ARP caches to locate a specific IP address for a provided MAC address.

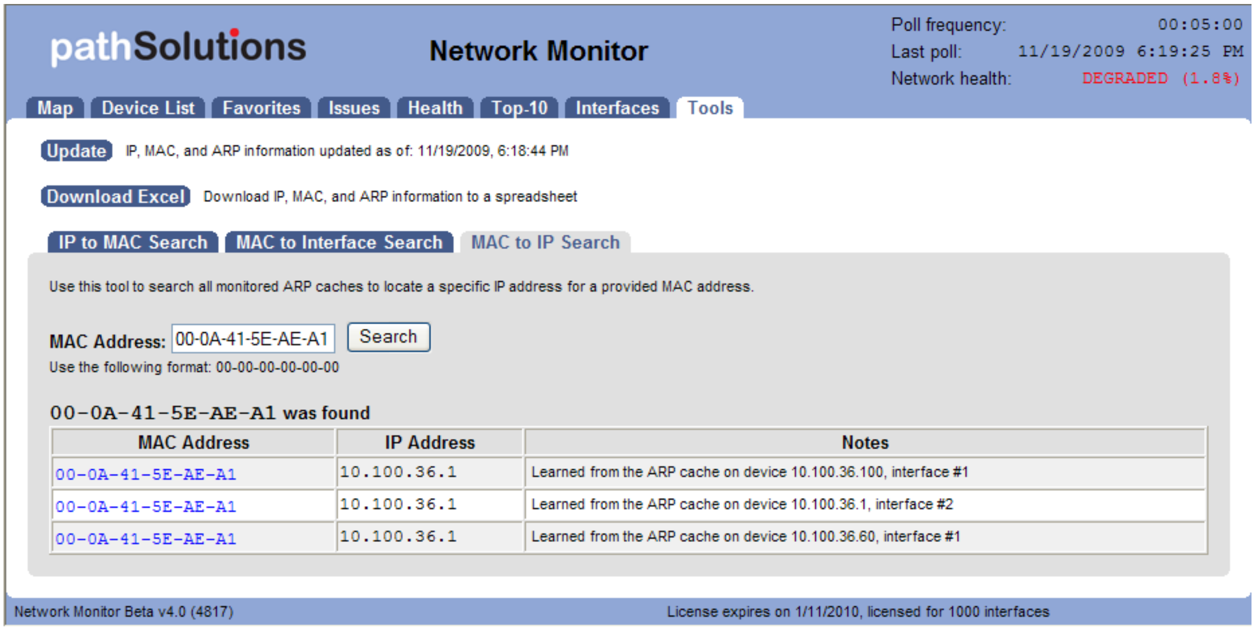
MAC Address:

Use the following format: 00-00-00-00-00-00

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

Enter the MAC address and click “Search”.

You should see the resulting IP address for the MAC address if it was found in any of the monitored devices’ ARP caches:



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:19:25 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:18:44 PM

Download IP, MAC, and ARP information to a spreadsheet

Use this tool to search all monitored ARP caches to locate a specific IP address for a provided MAC address.

MAC Address: 00-0A-41-5E-AE-A1

Use the following format: 00-00-00-00-00-00

00-0A-41-5E-AE-A1 was found

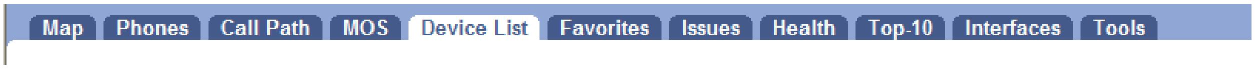
| MAC Address | IP Address | Notes |
|---|---|---|
| 00-0A-41-5E-AE-A1 | 10.100.36.1 | Learned from the ARP cache on device 10.100.36.100, interface #1 |
| 00-0A-41-5E-AE-A1 | 10.100.36.1 | Learned from the ARP cache on device 10.100.36.1, interface #2 |
| 00-0A-41-5E-AE-A1 | 10.100.36.1 | Learned from the ARP cache on device 10.100.36.60, interface #1 |

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

The IP address will be displayed along with the device and interface where the IP address was found in the device’s ARP cache.

# PathSolutions' VoIP Monitor Features

When running PathSolutions' VoIP Monitor, additional tabs are available:



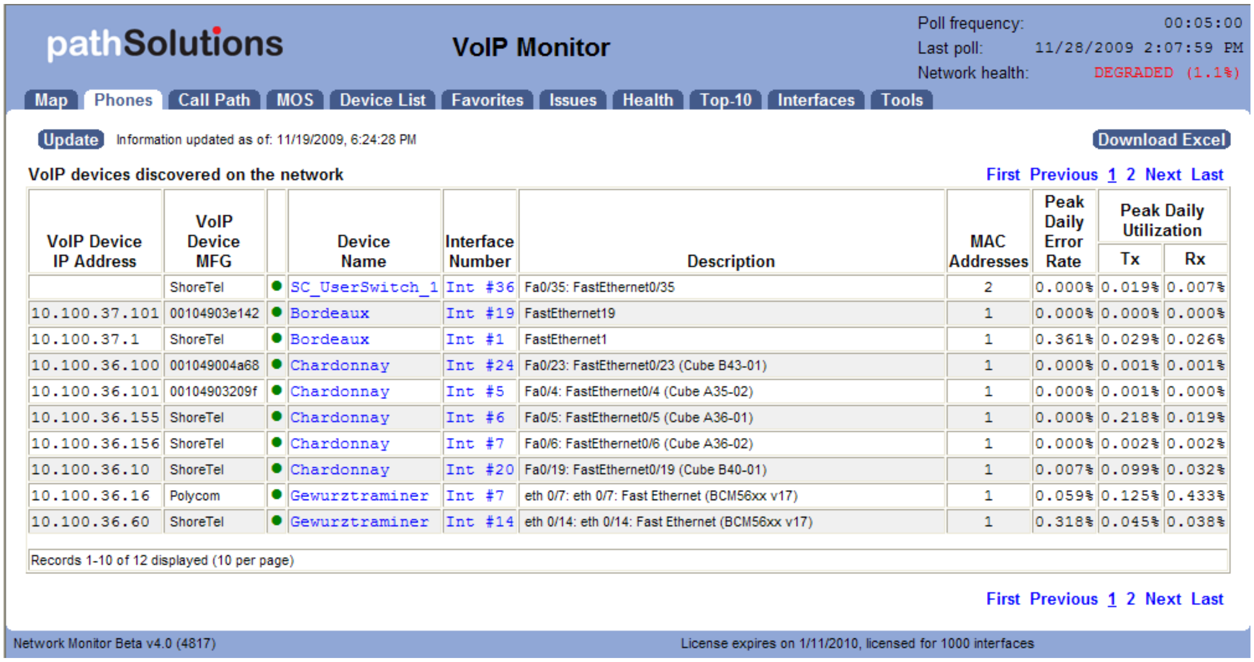
These tabs are only available when licensed for PathSolutions' VoIP Monitor.

## *Phones Tab*

The Phones tab lists the location of all VoIP phones in your network.  This is detected by looking for the MAC address prefixes that VoIP phones use.

To learn the current location of phones, click the "Update" button to collect the bridge tables and ARP cache information.

In a few moments, you should see the phones in your environment along with the switch ports where they are connected:



Poll frequency: 00:05:00
Last poll: 11/28/2009 2:07:59 PM
Network health: DEGRADED (1.1%)

Information updated as of: 11/19/2009, 6:24:28 PM

VoIP devices discovered on the network

| VoIP Device IP Address | VoIP Device MFG | | Device Name | Interface Number | Description | MAC Addresses | Peak Daily Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Tx | Rx |
| | ShoreTel | ● | SC_UserSwitch_1 | Int #36 | Fa0/35: FastEthernet0/35 | 2 | 0.000% | 0.019% | 0.007% |
| 10.100.37.101 | 00104903e142 | ● | Bordeaux | Int #19 | FastEthernet19 | 1 | 0.000% | 0.000% | 0.000% |
| 10.100.37.1 | ShoreTel | ● | Bordeaux | Int #1 | FastEthernet1 | 1 | 0.361% | 0.029% | 0.026% |
| 10.100.36.100 | 001049004a68 | ● | Chardonnay | Int #24 | Fa0/23: FastEthernet0/23 (Cube B43-01) | 1 | 0.000% | 0.001% | 0.001% |
| 10.100.36.101 | 00104903209f | ● | Chardonnay | Int #5 | Fa0/4: FastEthernet0/4 (Cube A35-02) | 1 | 0.000% | 0.001% | 0.000% |
| 10.100.36.155 | ShoreTel | ● | Chardonnay | Int #6 | Fa0/5: FastEthernet0/5 (Cube A36-01) | 1 | 0.000% | 0.218% | 0.019% |
| 10.100.36.156 | ShoreTel | ● | Chardonnay | Int #7 | Fa0/6: FastEthernet0/6 (Cube A36-02) | 1 | 0.000% | 0.002% | 0.002% |
| 10.100.36.10 | ShoreTel | ● | Chardonnay | Int #20 | Fa0/19: FastEthernet0/19 (Cube B40-01) | 1 | 0.007% | 0.099% | 0.032% |
| 10.100.36.16 | Polycom | ● | Gewurztraminer | Int #7 | eth 0/7: eth 0/7: Fast Ethernet (BCM56xx v17) | 1 | 0.059% | 0.125% | 0.433% |
| 10.100.36.60 | ShoreTel | ● | Gewurztraminer | Int #14 | eth 0/14: eth 0/14: Fast Ethernet (BCM56xx v17) | 1 | 0.318% | 0.045% | 0.038% |

Records 1-10 of 12 displayed (10 per page)

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

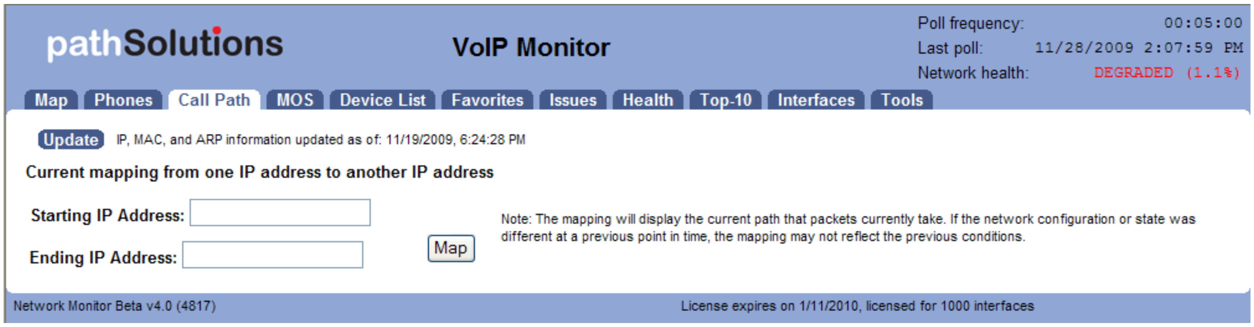
If you notice that there is more than one MAC address on the interface, that would indicate that a PC is hooked up to the phone.

The error rates and utilization rates are shown for each switch interface to inform you of the health of these connections.

**Note:** If you have VoIP phones that are not showing up in the list, you can add device manufacturer OUIs (Organizationally Unique Identifier) to the OUIFilter.cfg file.  Look in Appendix G for additional information on this.

## *Call Path Tab*

The Call Path tab permits you to view the health of all links between two IP addresses.



Poll frequency: 00:05:00
Last poll: 11/28/2009 2:07:59 PM
Network health: DEGRADED (1.1%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:24:28 PM

Current mapping from one IP address to another IP address

Starting IP Address:

Ending IP Address:

Note: The mapping will display the current path that packets currently take. If the network configuration or state was different at a previous point in time, the mapping may not reflect the previous conditions.

Network Monitor Beta v4.0 (4817)

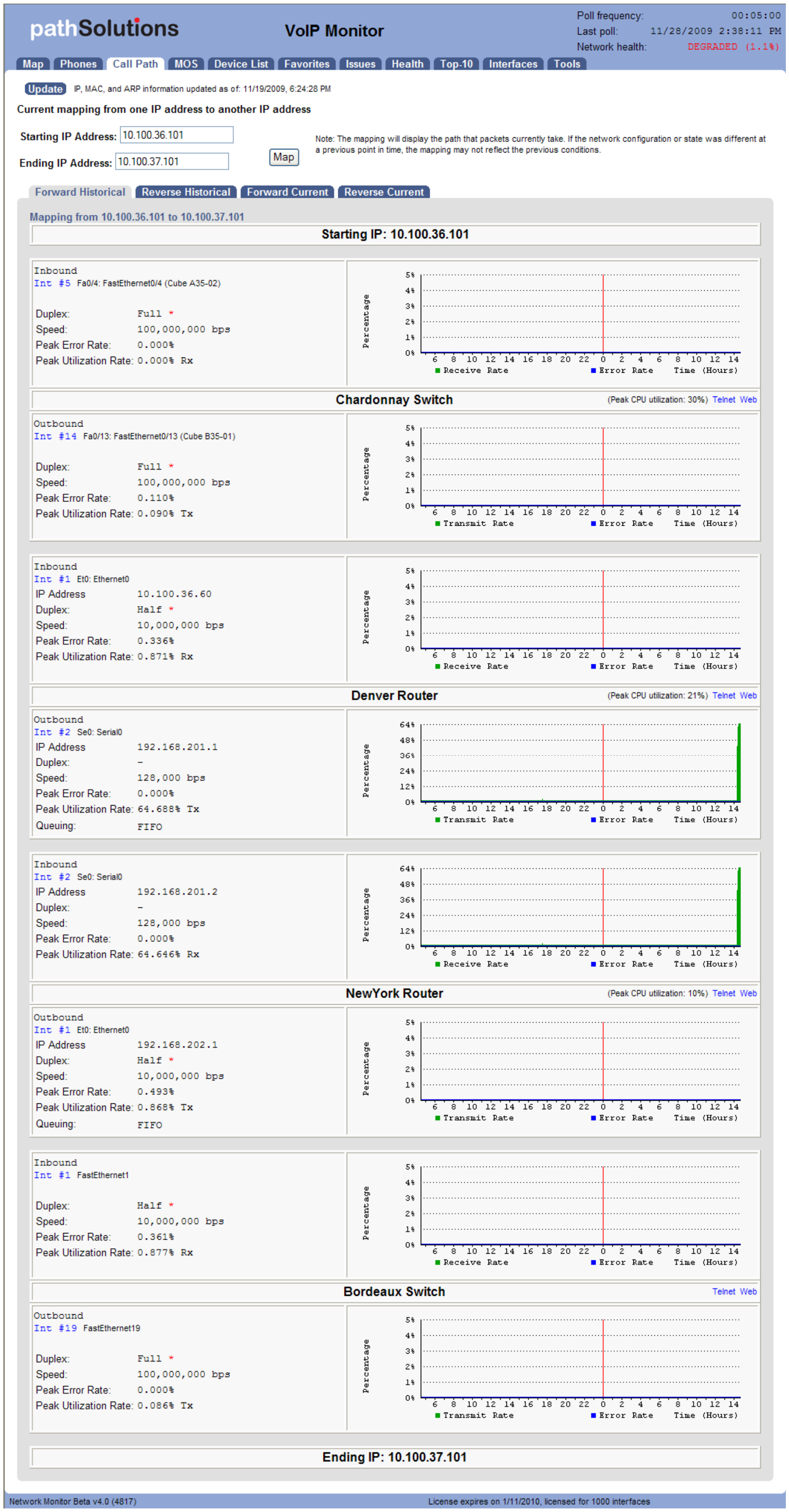
License expires on 1/11/2010, licensed for 1000 interfaces

Before mapping a call, click on the “Update” button to make sure that the bridge tables and ARP cache information is current.

**Note:** The mapping will display the current path that packets take. If the network configuration or state was different at a previous point in time, this mapping may not reflect the previous conditions.

Enter the starting IP address where you want the mapping to start and the ending IP address where the packets would be destined. Click the “Map” button to initiate the mapping.

You should see:



VoIP Monitor

Poll frequency: 00:05:00
Last poll: 11/28/2009 2:38:11 PM
Network health: DEGRADED (1.1%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:24:28 PM

**Current mapping from one IP address to another IP address**

Starting IP Address: 10.100.36.101
Ending IP Address: 10.100.37.101

Note: The mapping will display the path that packets currently take. If the network configuration or state was different at a previous point in time, the mapping may not reflect the previous conditions.

Mapping from 10.100.36.101 to 10.100.37.101

**Starting IP: 10.100.36.101**

Inbound
Int #5 Fa0/4: FastEthernet0/4 (Cube A35-02)
Duplex: Full *
Speed: 100,000,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 0.000% Rx

**Chardonnay Switch** (Peak CPU utilization: 30%) Telnet Web

Outbound
Int #14 Fa0/13: FastEthernet0/13 (Cube B35-01)
Duplex: Full *
Speed: 100,000,000 bps
Peak Error Rate: 0.110%
Peak Utilization Rate: 0.090% Tx

Inbound
Int #1 Et0: Ethernet0
IP Address 10.100.36.60
Duplex: Half *
Speed: 10,000,000 bps
Peak Error Rate: 0.336%
Peak Utilization Rate: 0.871% Rx

**Denver Router** (Peak CPU utilization: 21%) Telnet Web

Outbound
Int #2 Se0: Serial0
IP Address 192.168.201.1
Duplex: -
Speed: 128,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 64.688% Tx
Queuing: FIFO

Inbound
Int #2 Se0: Serial0
IP Address 192.168.201.2
Duplex: -
Speed: 128,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 64.646% Rx

**NewYork Router** (Peak CPU utilization: 10%) Telnet Web

Outbound
Int #1 Et0: Ethernet0
IP Address 192.168.202.1
Duplex: Half *
Speed: 10,000,000 bps
Peak Error Rate: 0.493%
Peak Utilization Rate: 0.868% Tx
Queuing: FIFO

Inbound
Int #1 FastEthernet1
Duplex: Half *
Speed: 10,000,000 bps
Peak Error Rate: 0.361%
Peak Utilization Rate: 0.877% Rx

**Bordeaux Switch** Telnet Web

Outbound
Int #19 FastEthernet19
Duplex: Full *
Speed: 100,000,000 bps
Peak Error Rate: 0.000%
Peak Utilization Rate: 0.086% Tx

**Ending IP: 10.100.37.101**

Network Monitor Beta v4.0 (4817)
License expires on 1/11/2010, licensed for 1000 interfaces

This will perform a one-way path mapping from the starting IP address to the ending IP address. It is a one-way view of how packets would flow from the starting IP to the ending IP. To view how packets would return, you should click on “Reverse Historical”, as the reverse path may be different than the outbound path if asymmetric routing is occurring.

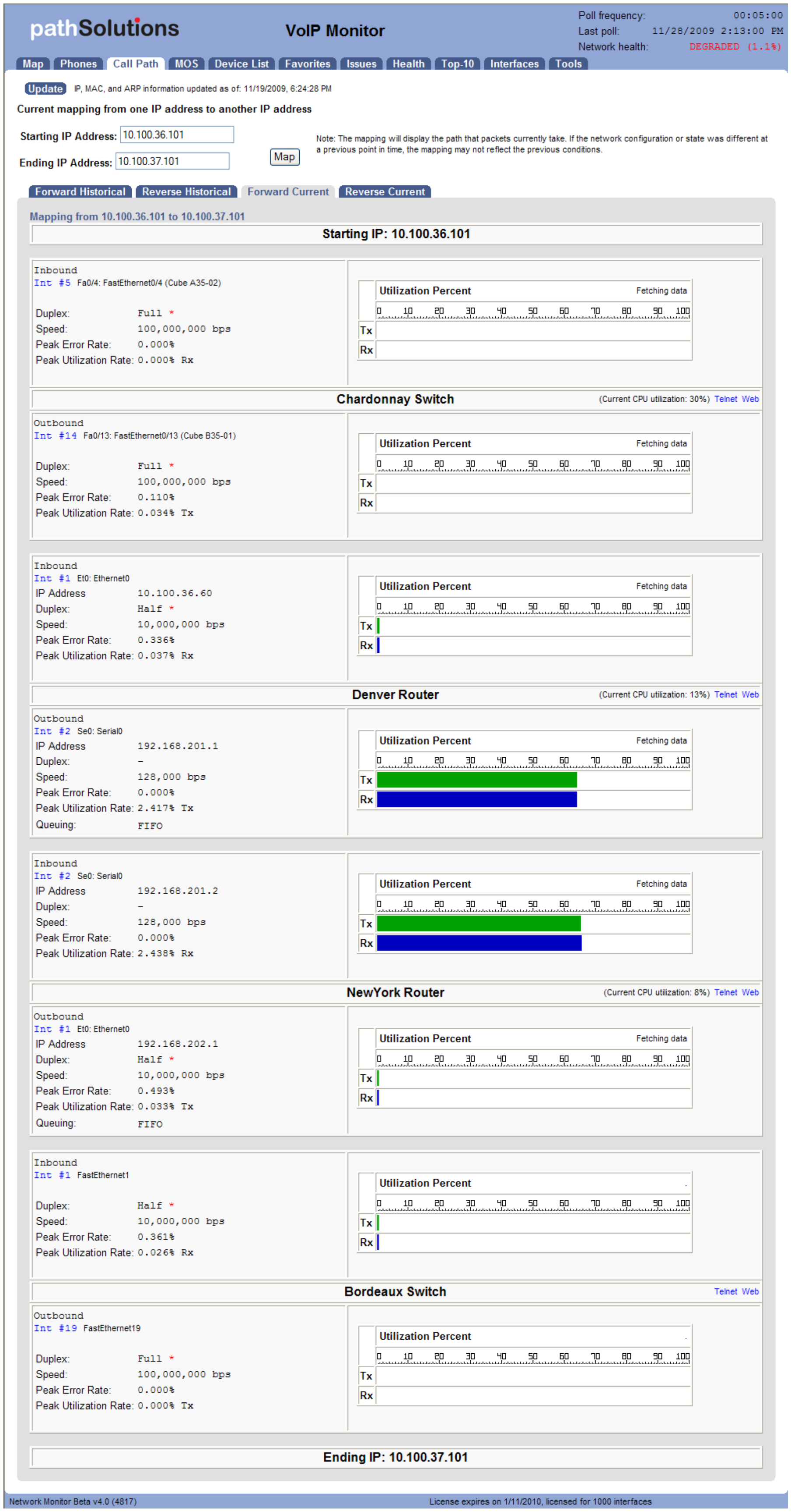
Each interface will display the historical percent utilization (received for inbound interfaces and transmit for outbound interfaces) along with the error rate.

You can also view the duplex setting of each interface to make sure that each outbound interface matches the duplex setting on the inbound interface.

On outbound Cisco router interfaces, the Queuing configuration of the interface is also shown to aid in determining if QoS is configured properly on the interface.

You can view current utilization for all of these links by clicking “Forward Current”.

You should see:



Poll frequency: 00:05:00
Last poll: 11/28/2009 2:13:00 PM
Network health: DEGRADED (1.1%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:24:28 PM

Current mapping from one IP address to another IP address

Starting IP Address: 10.100.36.101
Ending IP Address: 10.100.37.101

Note: The mapping will display the path that packets currently take. If the network configuration or state was different at a previous point in time, the mapping may not reflect the previous conditions.

Mapping from 10.100.36.101 to 10.100.37.101

**Starting IP: 10.100.36.101**

```
Inbound
Int #5  Fa0/4: FastEthernet0/4 (Cube A35-02)

Duplex:                Full *
Speed:                 100,000,000 bps
Peak Error Rate:       0.000%
Peak Utilization Rate: 0.000% Rx
```

**Chardonnay Switch** (Current CPU utilization: 30%) Telnet Web

```
Outbound
Int #14  Fa0/13: FastEthernet0/13 (Cube B35-01)

Duplex:                Full *
Speed:                 100,000,000 bps
Peak Error Rate:       0.110%
Peak Utilization Rate: 0.034% Tx
```

```
Inbound
Int #1  Et0: Ethernet0
IP Address             10.100.36.60
Duplex:                Half *
Speed:                 10,000,000 bps
Peak Error Rate:       0.336%
Peak Utilization Rate: 0.037% Rx
```

**Denver Router** (Current CPU utilization: 13%) Telnet Web

```
Outbound
Int #2  Se0: Serial0
IP Address             192.168.201.1
Duplex:                -
Speed:                 128,000 bps
Peak Error Rate:       0.000%
Peak Utilization Rate: 2.417% Tx
Queuing:               FIFO
```

```
Inbound
Int #2  Se0: Serial0
IP Address             192.168.201.2
Duplex:                -
Speed:                 128,000 bps
Peak Error Rate:       0.000%
Peak Utilization Rate: 2.438% Rx
```

**NewYork Router** (Current CPU utilization: 8%) Telnet Web

```
Outbound
Int #1  Et0: Ethernet0
IP Address             192.168.202.1
Duplex:                Half *
Speed:                 10,000,000 bps
Peak Error Rate:       0.493%
Peak Utilization Rate: 0.033% Tx
Queuing:               FIFO
```

```
Inbound
Int #1  FastEthernet1

Duplex:                Half *
Speed:                 10,000,000 bps
Peak Error Rate:       0.361%
Peak Utilization Rate: 0.026% Rx
```

**Bordeaux Switch** Telnet Web

```
Outbound
Int #19  FastEthernet19

Duplex:                Full *
Speed:                 100,000,000 bps
Peak Error Rate:       0.000%
Peak Utilization Rate: 0.000% Tx
```

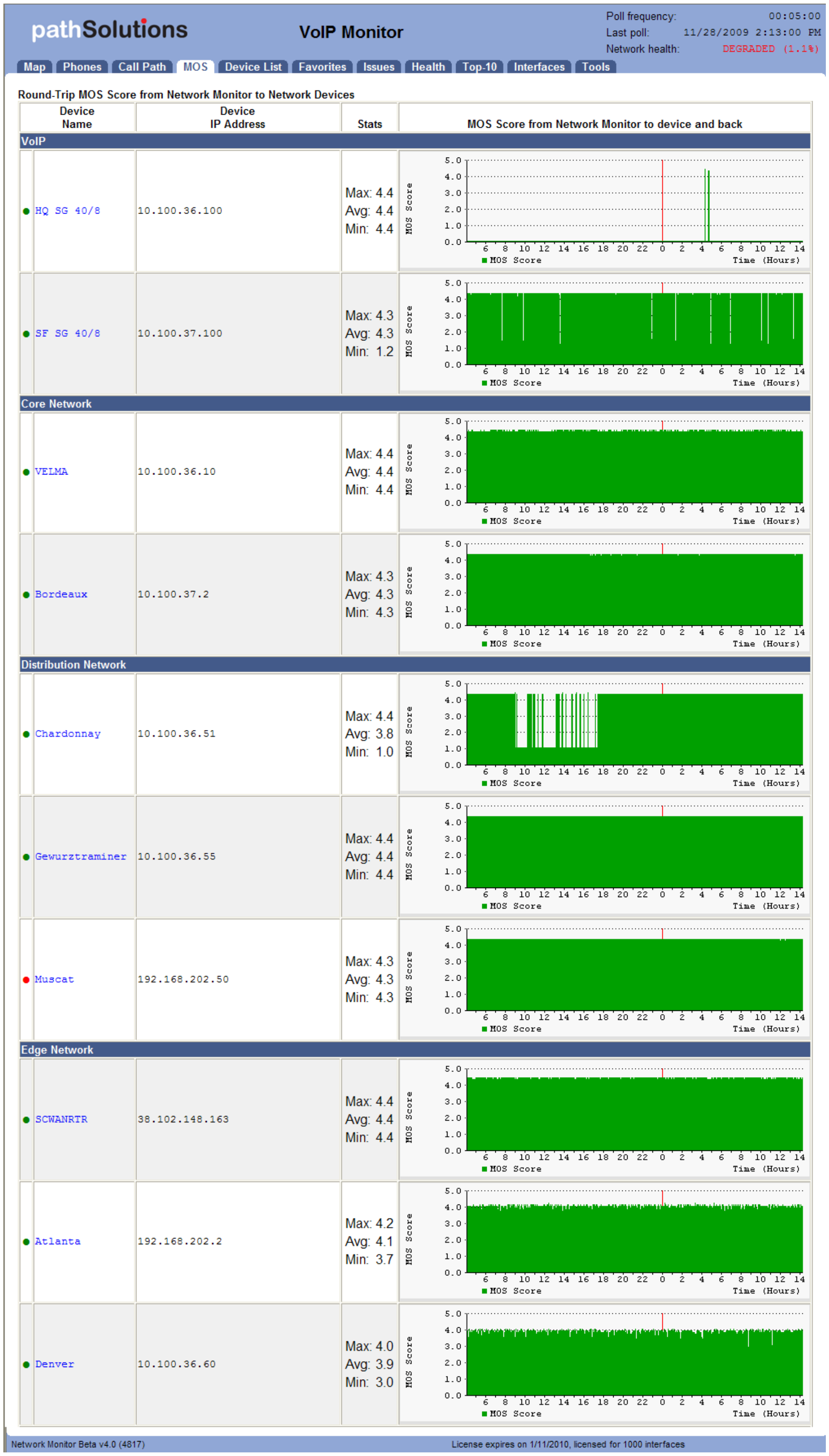
**Ending IP: 10.100.37.101**

Network Monitor Beta v4.0 (4817)    License expires on 1/11/2010, licensed for 1000 interfaces

The current utilization will update every 10 seconds.

## MOS Tab

The MOS tab displays the MOS graphs for each monitored device on the network:



Poll frequency: 00:05:00
Last poll: 11/28/2009 2:13:00 PM
Network health: DEGRADED (1.1%)

Round-Trip MOS Score from Network Monitor to Network Devices

| Device Name | Device IP Address | Stats | MOS Score from Network Monitor to device and back |
|---|---|---|---|
| **VoIP** | | | |
| ● HQ SG 40/8 | 10.100.36.100 | Max: 4.4<br>Avg: 4.4<br>Min: 4.4 | |
| ● SF SG 40/8 | 10.100.37.100 | Max: 4.3<br>Avg: 4.3<br>Min: 1.2 | |
| **Core Network** | | | |
| ● VELMA | 10.100.36.10 | Max: 4.4<br>Avg: 4.4<br>Min: 4.4 | |
| ● Bordeaux | 10.100.37.2 | Max: 4.3<br>Avg: 4.3<br>Min: 4.3 | |
| **Distribution Network** | | | |
| ● Chardonnay | 10.100.36.51 | Max: 4.4<br>Avg: 3.8<br>Min: 1.0 | |
| ● Gewurztraminer | 10.100.36.55 | Max: 4.4<br>Avg: 4.4<br>Min: 4.4 | |
| ● Muscat | 192.168.202.50 | Max: 4.3<br>Avg: 4.3<br>Min: 4.3 | |
| **Edge Network** | | | |
| ● SCWANRTR | 38.102.148.163 | Max: 4.4<br>Avg: 4.4<br>Min: 4.4 | |
| ● Atlanta | 192.168.202.2 | Max: 4.2<br>Avg: 4.1<br>Min: 3.7 | |
| ● Denver | 10.100.36.60 | Max: 4.0<br>Avg: 3.9<br>Min: 3.0 | |

Network Monitor Beta v4.0 (4817)

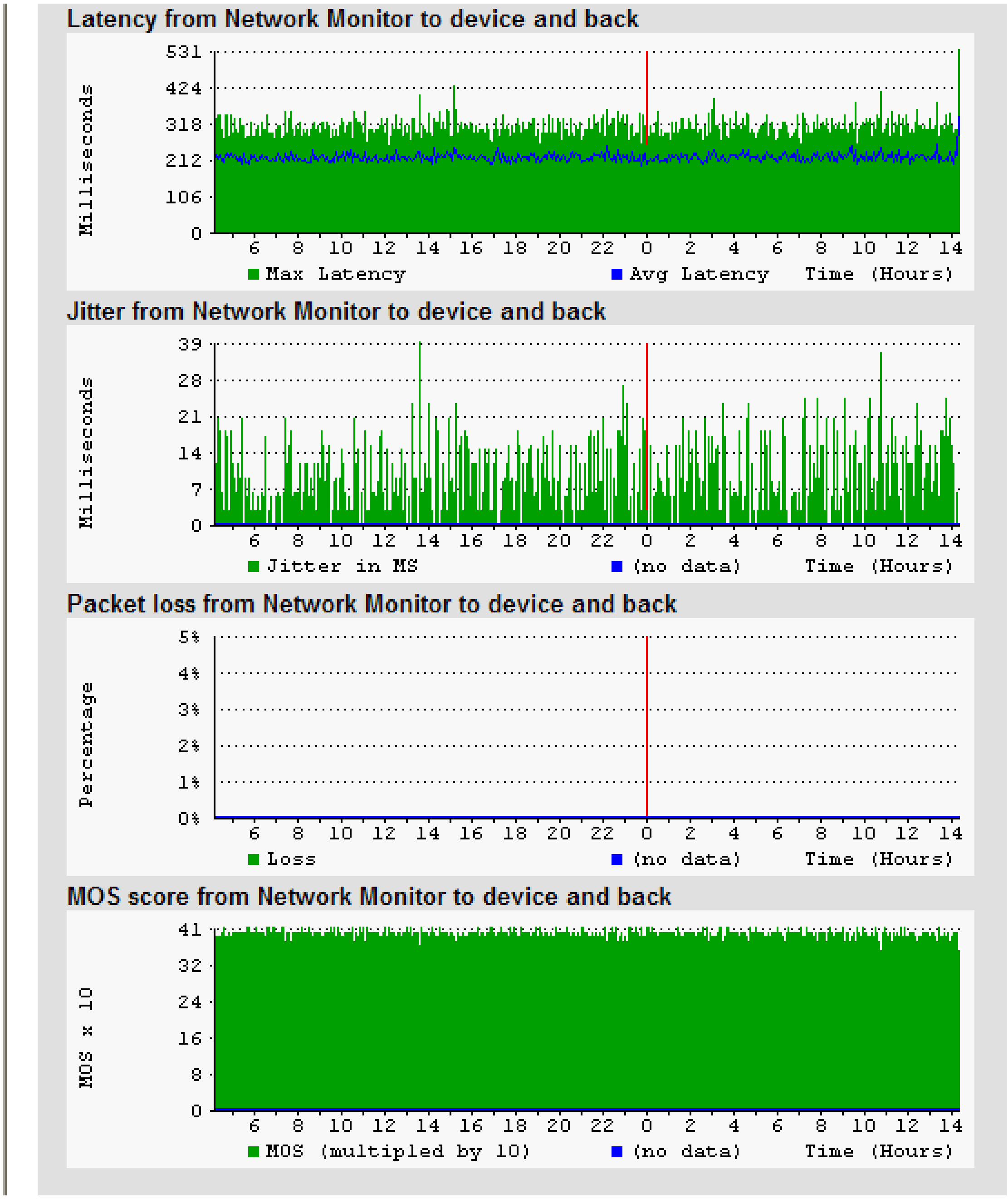
License expires on 1/11/2010, licensed for 1000 interfaces

### *Device Latency, Jitter, Loss, and MOS scores*

During its communications with each monitored device, PathSolutions' Network Monitor tracks the peak and average latency, as well as the jitter, packet loss and MOS score.

This creates the ability to monitor devices across a WAN or the Internet and know how stable the connection is.

This information is available below the Aggregate Peak utilization (and CPU and memory graphs if it is a Cisco device) on the device page:



Latency from Network Monitor to device and back

Jitter from Network Monitor to device and back

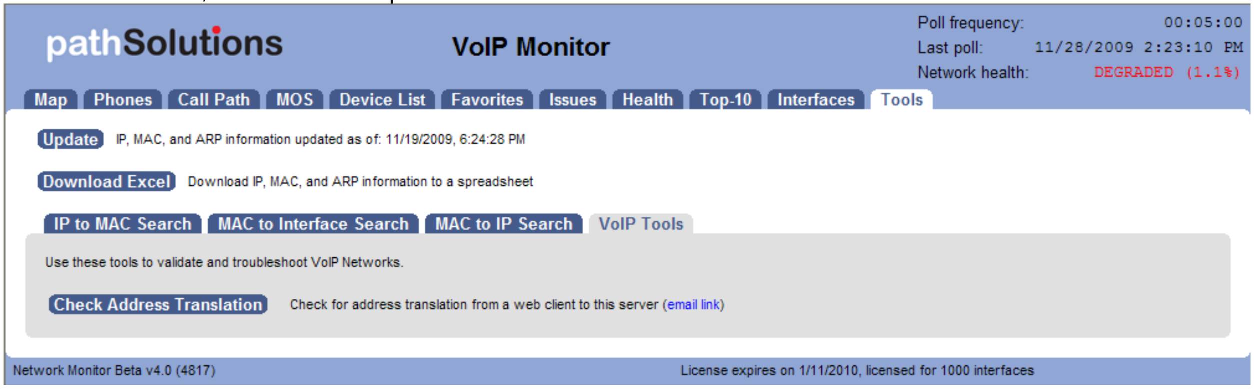
Packet loss from Network Monitor to device and back

MOS score from Network Monitor to device and back

MOS score is displayed as MOS x 10. Thus, the graph above shows a MOS of 42. This would be read as MOS of 4.2.

## *VoIP Tools*

On the Tools tab, an additional option is available: VoIP Tools.



IP, MAC, and ARP information updated as of: 11/19/2009, 6:24:28 PM

Download IP, MAC, and ARP information to a spreadsheet

Use these tools to validate and troubleshoot VoIP Networks.

Check for address translation from a web client to this server (email link)

Network Monitor Beta v4.0 (4817)

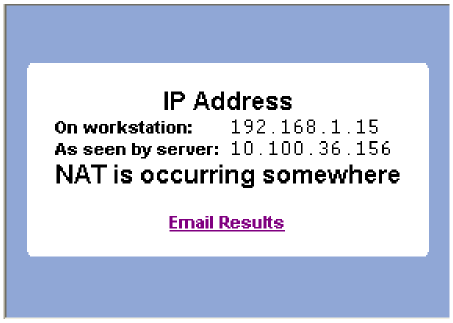
License expires on 1/11/2010, licensed for 1000 interfaces

### Check for NAT

Network Address Translation can cause one-way audio problems in a VoIP network. Being able to quickly ascertain if NAT is being performed is an important capability.

Simply click on the provided link to determine if NAT is occurring between your computer and the PathSolutions' Network Monitor server.

You should see:



IP Address

On workstation: 192.168.1.15

As seen by server: 10.100.36.156

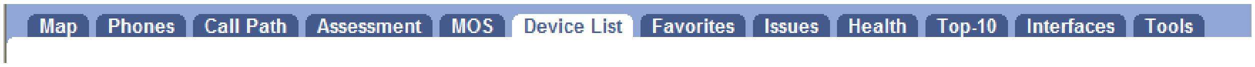
NAT is occurring somewhere

**Note**: This tool runs a small Java applet. The browser where this is executed must be able to run a Java v1.1 applet.

This tool is intended to be run by users on remote computers. It is recommended to use the "email link" button on the VoIP Tools tab to send a link to the end user who should run this check. The end user can then click on "Email Results" to send the results back to you for evaluation.

# PathSolutions' Network Monitor VoIP Assessment Features

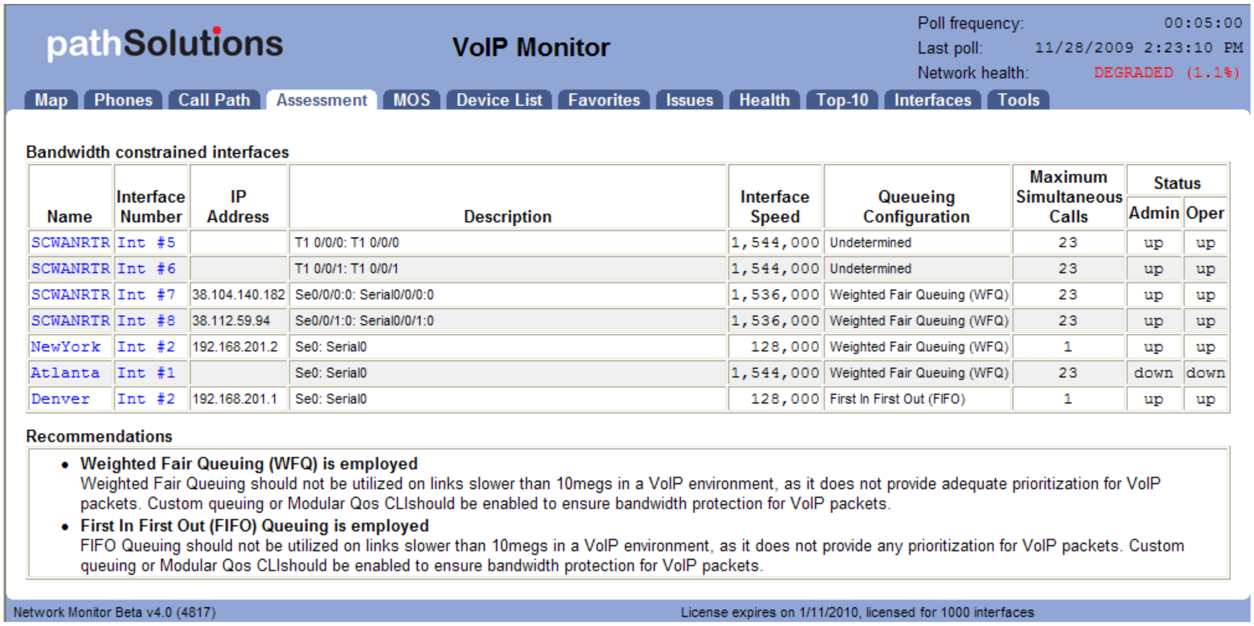
When running PathSolutions' Network Monitor VoIP Assessment, there will be one additional "Assessment" tab available:



This tab is only available when running PathSolutions' Network Monitor VoIP Assessment.

## Assessment Tab

The Assessment tab lists any interface that is below 10mbps on the network along with their queuing configuration and status.



Poll frequency: 00:05:00
Last poll: 11/28/2009 2:23:10 PM
Network health: DEGRADED (1.1%)

Bandwidth constrained interfaces

| Name | Interface Number | IP Address | Description | Interface Speed | Queueing Configuration | Maximum Simultaneous Calls | Status | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | Admin | Oper |
| SCWANRTR | Int #5 | | T1 0/0/0: T1 0/0/0 | 1,544,000 | Undetermined | 23 | up | up |
| SCWANRTR | Int #6 | | T1 0/0/1: T1 0/0/1 | 1,544,000 | Undetermined | 23 | up | up |
| SCWANRTR | Int #7 | 38.104.140.182 | Se0/0/0:0: Serial0/0/0:0 | 1,536,000 | Weighted Fair Queuing (WFQ) | 23 | up | up |
| SCWANRTR | Int #8 | 38.112.59.94 | Se0/0/1:0: Serial0/0/1:0 | 1,536,000 | Weighted Fair Queuing (WFQ) | 23 | up | up |
| NewYork | Int #2 | 192.168.201.2 | Se0: Serial0 | 128,000 | Weighted Fair Queuing (WFQ) | 1 | up | up |
| Atlanta | Int #1 | | Se0: Serial0 | 1,544,000 | Weighted Fair Queuing (WFQ) | 23 | down | down |
| Denver | Int #2 | 192.168.201.1 | Se0: Serial0 | 128,000 | First In First Out (FIFO) | 1 | up | up |

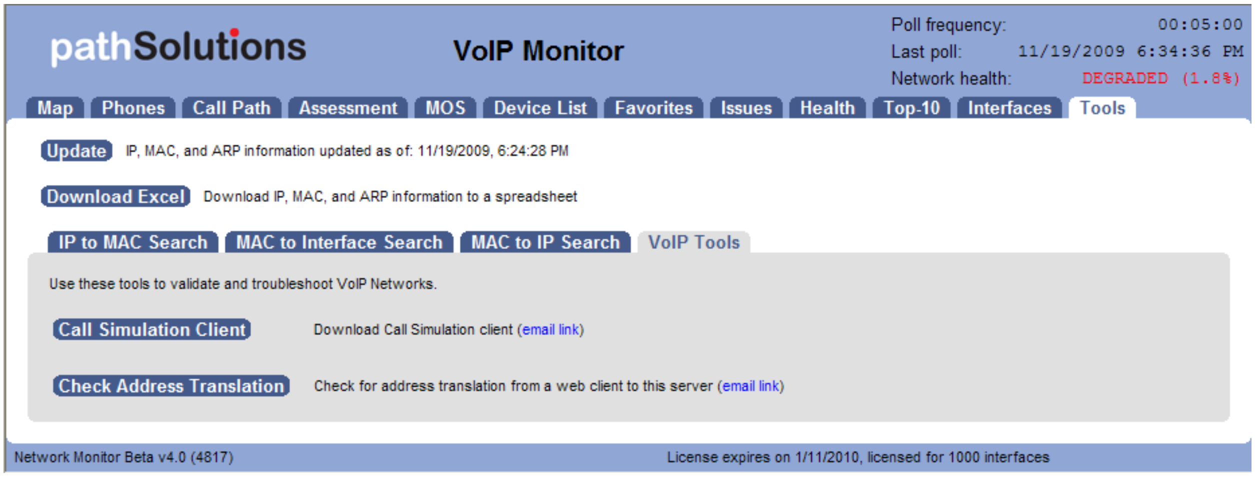
Recommendations

- **Weighted Fair Queuing (WFQ) is employed**
  Weighted Fair Queuing should not be utilized on links slower than 10megs in a VoIP environment, as it does not provide adequate prioritization for VoIP packets. Custom queuing or Modular Qos CLIshould be enabled to ensure bandwidth protection for VoIP packets.
- **First In First Out (FIFO) Queuing is employed**
  FIFO Queuing should not be utilized on links slower than 10megs in a VoIP environment, as it does not provide any prioritization for VoIP packets. Custom queuing or Modular Qos CLIshould be enabled to ensure bandwidth protection for VoIP packets.

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

## VoIP Tools

On the Tools tab, an additional option is available under the VoIP Tools tab.



Poll frequency: 00:05:00
Last poll: 11/19/2009 6:34:36 PM
Network health: DEGRADED (1.8%)

IP, MAC, and ARP information updated as of: 11/19/2009, 6:24:28 PM

Download IP, MAC, and ARP information to a spreadsheet

Use these tools to validate and troubleshoot VoIP Networks.

Download Call Simulation client (email link)

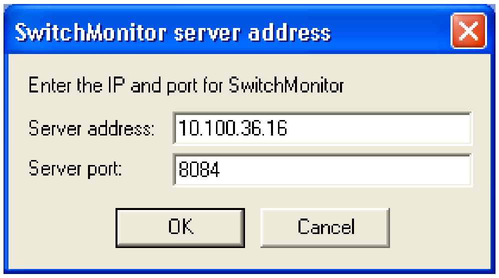
Check for address translation from a web client to this server (email link)

Network Monitor Beta v4.0 (4817) License expires on 1/11/2010, licensed for 1000 interfaces

## Call Simulator

The Call Simulator is a program that is run on a computer where you would like to test a VoIP call. It will send VoIP formatted ICMP ping packets to any IP address endpoint. This permits you to simulate a VoIP phone call to any remote IP address without having to set up software on the remote IP endpoint.

When the Call Simulator is initially run on a computer, it will ask for the IP address and port number for the PathSolutions' Network Monitor server. This is done for licensing as well as to seed the program with the server and port for performing call path mappings:



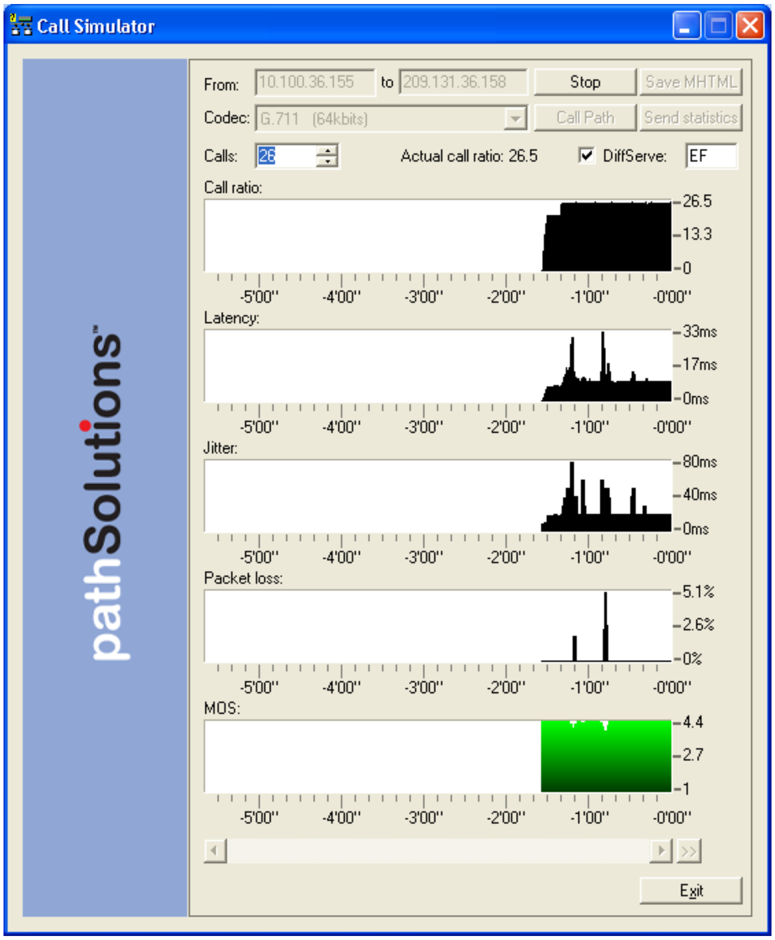
SwitchMonitor server address

Enter the IP and port for SwitchMonitor

Server address: 10.100.36.16

Server port: 8084

Once it runs, you can then enter the IP address of the remote device and choose the codec to simulate. Then click "Start" to start the simulation:



Call Simulator

From: 10.100.36.155 to 209.131.36.158

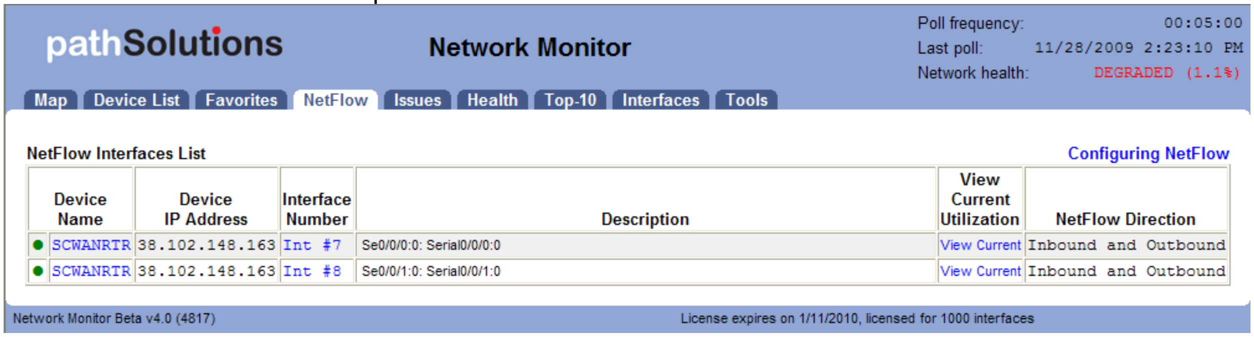
Codec: G.711 (64kbits)

Calls: 26 Actual call ratio: 26.5 ☑ DiffServe: EF

# Finding Who’s Using the Network and What they are Doing

## *NetFlow Tab*

PathSolutions’ Network Monitor with the NetFlow module gives you the ability to instantly know who is using your bandwidth and what they are doing. This feature is available on any Cisco device with NetFlow enabled to track the top flows.



Network Monitor

Poll frequency: 00:05:00
Last poll: 11/28/2009 2:23:10 PM
Network health: DEGRADED (1.1%)

NetFlow Interfaces List

Configuring NetFlow

| | Device Name | Device IP Address | Interface Number | Description | View Current Utilization | NetFlow Direction |
|---|---|---|---|---|---|---|
| ● | SCWANRTR | 38.102.148.163 | Int #7 | Se0/0/0:0: Serial0/0/0:0 | View Current | Inbound and Outbound |
| ● | SCWANRTR | 38.102.148.163 | Int #8 | Se0/0/1:0: Serial0/0/1:0 | View Current | Inbound and Outbound |

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

The NetFlow tab will show all of the interfaces on the network that are configured for NetFlow.

## *Configuring NetFlow on a Cisco router*

A router must support the CISCO-NETFLOW-MIB to be able to be configured for NetFlow Top Talkers queries. The Top Talkers feature was incorporated into the following IOS versions:

| |
|---|
| IOS 12.2(25)S |
| IOS 12.3(11)T |
| IOS 12.2(27)SBC |

If you are running later versions of IOS, the CISCO-NETFLOW-MIB and Top Talkers feature should be available.

### Configuration

Telnet to the router and use the following CLI commands to configure the router for NetFlow Top Talkers:

Router Configuration

```
1.  enable
2.  configure terminal
3.  ip flow-top-talkers
4.  top 50                  ← Increase by 25 for each additional interface monitored
5.  sort by bytes
6.  cache-timeout 5000
7.  end
```

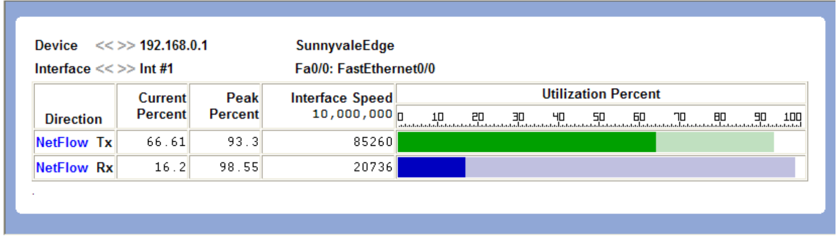
Interface Configuration

```
1.  enable
2.  configure terminal
3.  interface FastEthernet0/0
4.  ip flow ingress
5.  ip flow egress
6.  exit
```

Remember to save your router configuration

## Viewing Current Utilization on a NetFlow Interface

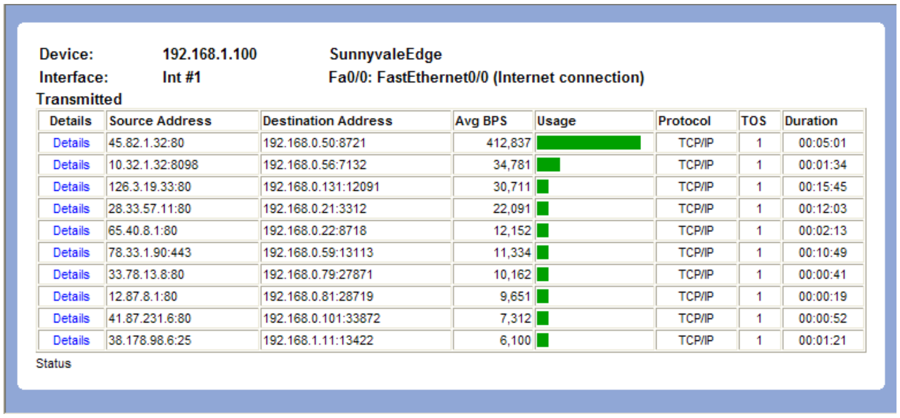
Current utilization can be viewed on a NetFlow configured interface just like any other interface:



Device << >> 192.168.0.1 SunnyvaleEdge
Interface << >> Int #1 Fa0/0: FastEthernet0/0

| Direction | Current Percent | Peak Percent | Interface Speed 10,000,000 | Utilization Percent |
|---|---|---|---|---|
| NetFlow Tx | 66.61 | 93.3 | 85260 | 🟩 |
| NetFlow Rx | 16.2 | 98.55 | 20736 | 🟦 |

If high utilization is detected in a specific direction, you can click on the "NetFlow" link to the left of the Tx or Rx indication to view the flows that are currently traversing the router:



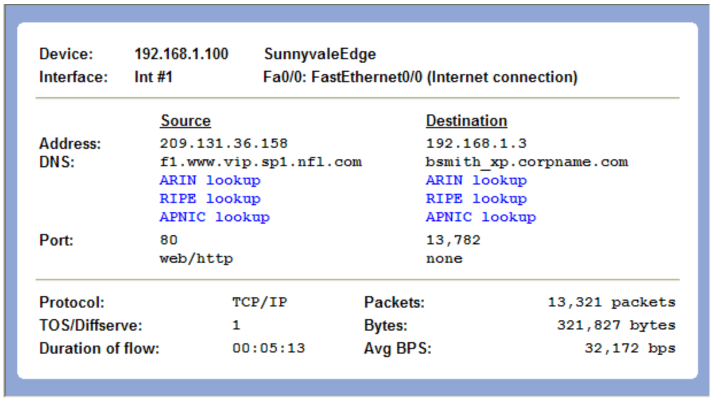
Device: 192.168.1.100 SunnyvaleEdge
Interface: Int #1 Fa0/0: FastEthernet0/0 (Internet connection)
Transmitted

| Details | Source Address | Destination Address | Avg BPS | Usage | Protocol | TOS | Duration |
|---|---|---|---|---|---|---|---|
| Details | 45.82.1.32:80 | 192.168.0.50:8721 | 412,837 | 🟩 | TCP/IP | 1 | 00:05:01 |
| Details | 10.32.1.32:8098 | 192.168.0.56:7132 | 34,781 | 🟩 | TCP/IP | 1 | 00:01:34 |
| Details | 126.3.19.33:80 | 192.168.0.131:12091 | 30,711 | 🟩 | TCP/IP | 1 | 00:15:45 |
| Details | 28.33.57.11:80 | 192.168.0.21:3312 | 22,091 | 🟩 | TCP/IP | 1 | 00:12:03 |
| Details | 65.40.8.1:80 | 192.168.0.22:8718 | 12,152 | 🟩 | TCP/IP | 1 | 00:02:13 |
| Details | 78.33.1.90:443 | 192.168.0.59:13113 | 11,334 | 🟩 | TCP/IP | 1 | 00:10:49 |
| Details | 33.78.13.8:80 | 192.168.0.79:27871 | 10,162 | 🟩 | TCP/IP | 1 | 00:00:41 |
| Details | 12.87.8.1:80 | 192.168.0.81:28719 | 9,651 | 🟩 | TCP/IP | 1 | 00:00:19 |
| Details | 41.87.231.6:80 | 192.168.0.101:33872 | 7,312 | 🟩 | TCP/IP | 1 | 00:00:52 |
| Details | 38.178.98.6:25 | 192.168.1.11:13422 | 6,100 | 🟩 | TCP/IP | 1 | 00:01:21 |

Status

The flow summary will show the IP addresses, Average Bits Per Second, Relative usage, Protocol, Type of Service, and Duration of flow.

To see details of a specific flow, click on the "Details" link for any flow. You will see the following:



Device: 192.168.1.100 SunnyvaleEdge
Interface: Int #1 Fa0/0: FastEthernet0/0 (Internet connection)

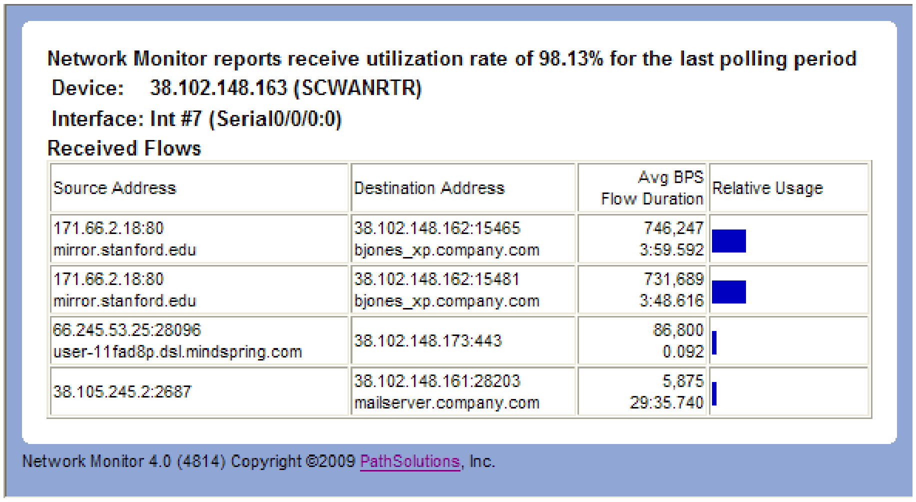
| | Source | Destination |
|---|---|---|
| Address: | 209.131.36.158 | 192.168.1.3 |
| DNS: | f1.www.vip.sp1.nfl.com<br>ARIN lookup<br>RIPE lookup<br>APNIC lookup | bsmith_xp.corpname.com<br>ARIN lookup<br>RIPE lookup<br>APNIC lookup |
| Port: | 80<br>web/http | 13,782<br>none |

| | | | |
|---|---|---|---|
| Protocol: | TCP/IP | Packets: | 13,321 packets |
| TOS/Diffserve: | 1 | Bytes: | 321,827 bytes |
| Duration of flow: | 00:05:13 | Avg BPS: | 32,172 bps |

The flow details will provide reverse DNS information (if available) and lookups for ARIN, RIPE, and APNIC as well as the ports used for the flow.

## NetFlow High Utilization Alerts

If a utilization alert is sent for an interface that has NetFlow enabled, the utilization alert will automatically include the top flows and reverse DNS information so it's easy to determine what's causing the high utilization condition:



**Network Monitor reports receive utilization rate of 98.13% for the last polling period**

**Device: 38.102.148.163 (SCWANRTR)**

**Interface: Int #7 (Serial0/0/0:0)**

**Received Flows**

| Source Address | Destination Address | Avg BPS<br>Flow Duration | Relative Usage |
|---|---|---|---|
| 171.66.2.18:80<br>mirror.stanford.edu | 38.102.148.162:15465<br>bjones_xp.company.com | 746,247<br>3:59.592 | ■ |
| 171.66.2.18:80<br>mirror.stanford.edu | 38.102.148.162:15481<br>bjones_xp.company.com | 731,689<br>3:48.616 | ■ |
| 66.245.53.25:28096<br>user-11fad8p.dsl.mindspring.com | 38.102.148.173:443 | 86,800<br>0.092 | ▏ |
| 38.105.245.2:2687 | 38.102.148.161:28203<br>mailserver.company.com | 5,875<br>29:35.740 | ▏ |

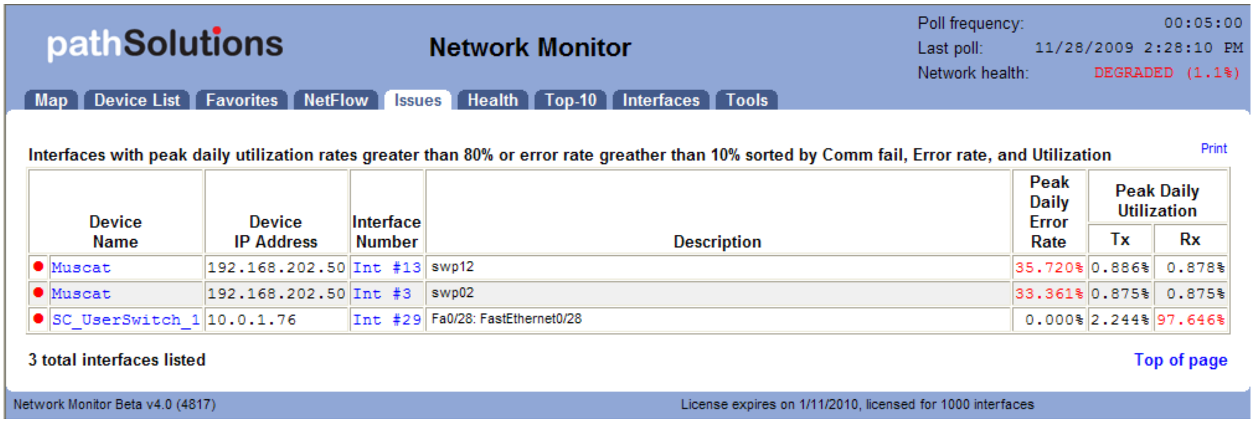
Network Monitor 4.0 (4814) Copyright ©2009 PathSolutions, Inc.

Note: If reverse DNS information is not shown for local IP addresses, it means there is no reverse DNS entry in your DNS server for that address. In many cases, your local DNS server can be configured to automatically create reverse entries for local desktop computers and servers.

# Fixing Problems on your Network

## *Improving Network Health*

Network health can be improved by working on the issues listed in the “Issues” list:



Poll frequency: 00:05:00
Last poll: 11/28/2009 2:28:10 PM
Network health: DEGRADED (1.1%)

Interfaces with peak daily utilization rates greater than 80% or error rate greather than 10% sorted by Comm fail, Error rate, and Utilization

| | Device Name | Device IP Address | Interface Number | Description | Peak Daily Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|---|
| | | | | | | Tx | Rx |
| ● | Muscat | 192.168.202.50 | Int #13 | swp12 | 35.720% | 0.886% | 0.878% |
| ● | Muscat | 192.168.202.50 | Int #3 | swp02 | 33.361% | 0.875% | 0.875% |
| ● | SC_UserSwitch_1 | 10.0.1.76 | Int #29 | Fa0/28: FastEthernet0/28 | 0.000% | 2.244% | 97.646% |

3 total interfaces listed

Network Monitor Beta v4.0 (4817)

License expires on 1/11/2010, licensed for 1000 interfaces

Click on the interface number to get details on the source of the problem.

If you have a bandwidth problem, you may want to upgrade the interface to a faster speed (upgrade 10mbps to 100mbps, or 100mbps to gigabit), and/or configure the link for full duplex. You may have errors associated with a bandwidth problem (like collisions), so it is recommended to solve bandwidth problems first.

After resolving bandwidth problems, you will want to focus on reducing the error rate on the interface (if this is a problem). Use the error analysis section for suggestions of a course of action. It may recommend replacing cables or network cards, depending on the types of errors that occur.

Additional troubleshooting information exists for each specific error. You can receive the online help by clicking on the specific error name.

Once you have implemented a fix, you should have a gradual reduction of the error rate on this interface. You may choose to immediately reset the counters on the interface so the program will start calculating error rates with a clean slate. Refer to your switch's documentation for information on how to clear interface statistics.

**Note:** Some switch manufacturers only allow clearing statistics for the entire switch, not a specific interface.

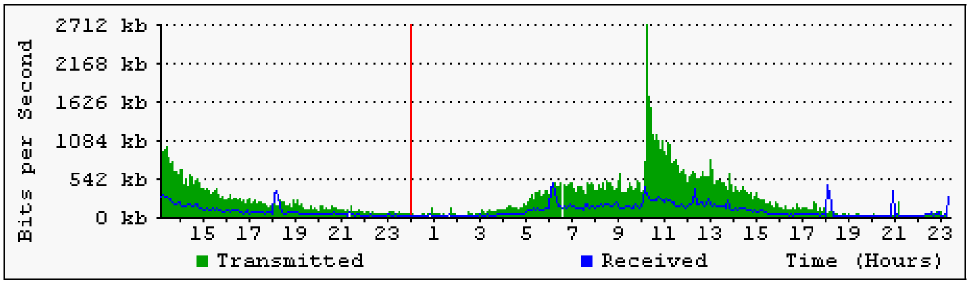
**Note:** If a switch manufacturer does not offer a method of clearing statistics, you will have to reboot the switch (or perhaps just the management module) to clear out old statistics.

The telnet link can be used to quickly connect to the switch and check duplex and switch configuration.

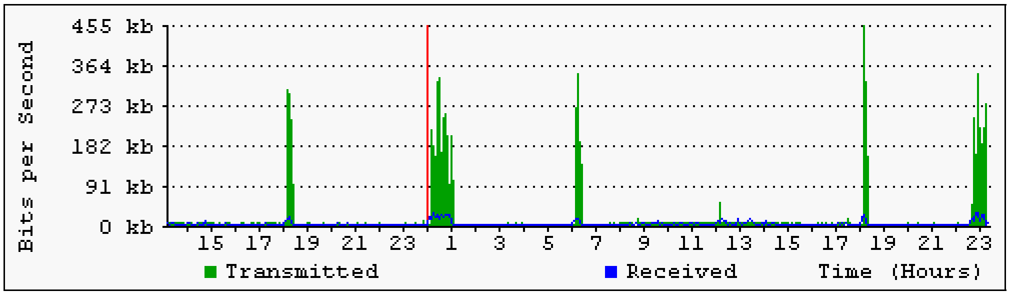
### *Finding Anomalous Traffic*

If you notice strange traffic on one interface, you can use System Monitor to locate the source of the traffic.

Consider the following graph:



At approximately 18:15 (6:15pm) yesterday, roughly 300k of data was received. The same amount of traffic was received at 06:15 (6:15am) this morning, and 18:15 this evening. With this traffic pattern in mind, we can quickly click on the interface arrows to find the interface that transmitted that quantity of traffic during those times:



Once you have found the interface, you can determine what is connected to the interface and look into the purpose of the traffic.

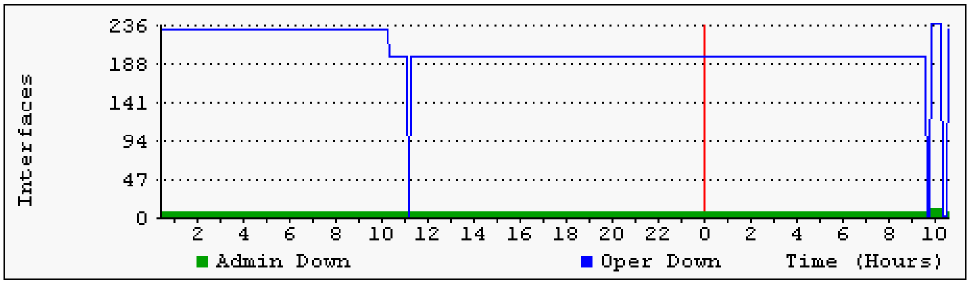
The benefit of this feature is that you do not have to be in front of a packet analyzer at the time the traffic is transmitted to determine the source of the traffic.

Click on the left and right interface arrows to view the other interfaces on the switch, looking for a similar traffic pattern at the same timeframe.

If determining the source and destination of the traffic is not enough to narrow down the cause, the next step would be to connect a network analyzer to that interface to try to determine the purpose of the traffic.

### Determining Laptop Usage

Laptops add and drop from the network on a regular basis. To track their usage patterns, select the Health tab and look at the bottom graph “Down Interfaces”:



Notice that the number of "Operationally Down" interfaces decreases as users connect to the network and increases as users disconnect.

### Planning for Network Growth

Making sure that you always have free network ports available for growth is important. Use the Health tab “Down Interfaces” to determine overall port availability.
When the number of operationally shut down ports gets too low, additional switch ports should be acquired.

### Scheduling Server Outages

Determining the timeframe to schedule server outages can be tricky without System Monitor. Choose the interface that connects to the server and view the daily, weekly, and monthly graphs to determine when network utilization for this server is lowest. The user community should be comfortable with the decision, as there is no documented usage during that period.

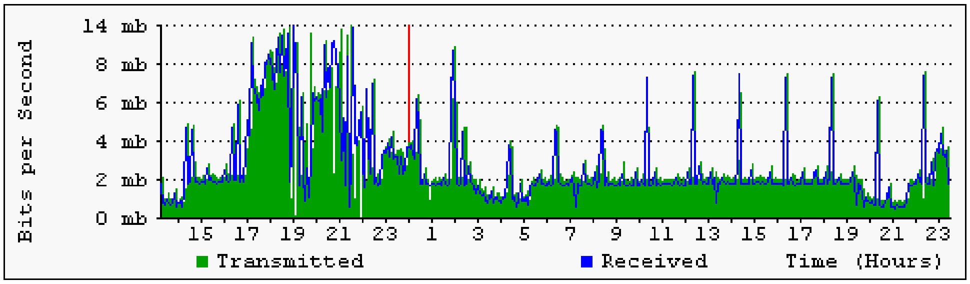
### Scheduling Switch & Router Outages

Scheduling switch outages are easy as well. Choose the switch details and view the daily, weekly, and monthly graphs to determine when overall switch utilization is lowest.

### Daily Overall Utilization Tracking

View the daily overall utilization on the Health tab to determine if the utilization meets with your expectation of usage.

Consider the following daily overall utilization graph:

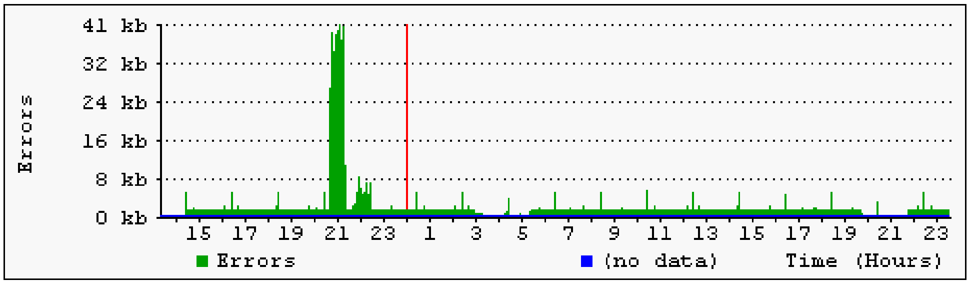


This graph shows a lot of data being transmitted on the previous day starting at 17:00 hours (5:00pm). This timeframe may correspond with backup jobs that are set to execute during that timeframe.
The graph also shows spikes roughly every two hours throughout the day. This may also correspond with scheduled activities on the network.

## Daily Overall Error Tracking

View the daily overall errors to determine if the level of errors meets with your expectation of error distribution.

Consider the following daily overall error graph:



This graph shows that there were a lot of errors around 21:00 hours (9:00pm). If you are aware of a process that runs at that time, you may choose to investigate the interface of the machine that executes the process.

## Performing Proactive Analysis

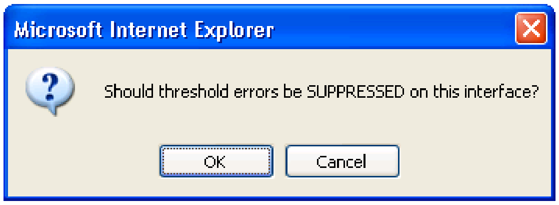
You can be proactive by using the "Top Errors" tab to locate interfaces that have error rates that are increasing. Reducing these error rates will help prevent them from becoming issues.

The "Top Talkers" and "Top Listeners" tabs can be used to watch which interfaces may become bandwidth bottlenecks.

## Error Resolution

Some device manufacturers may improperly report error information, making it impossible to clear certain errors. The device manufacturer should be able to provide a new version of their device software to report errors correctly.

You can tell PathSolutions' Network Monitor to suppress errors on interfaces by clicking on the status indicator. You should be presented with the following dialog:

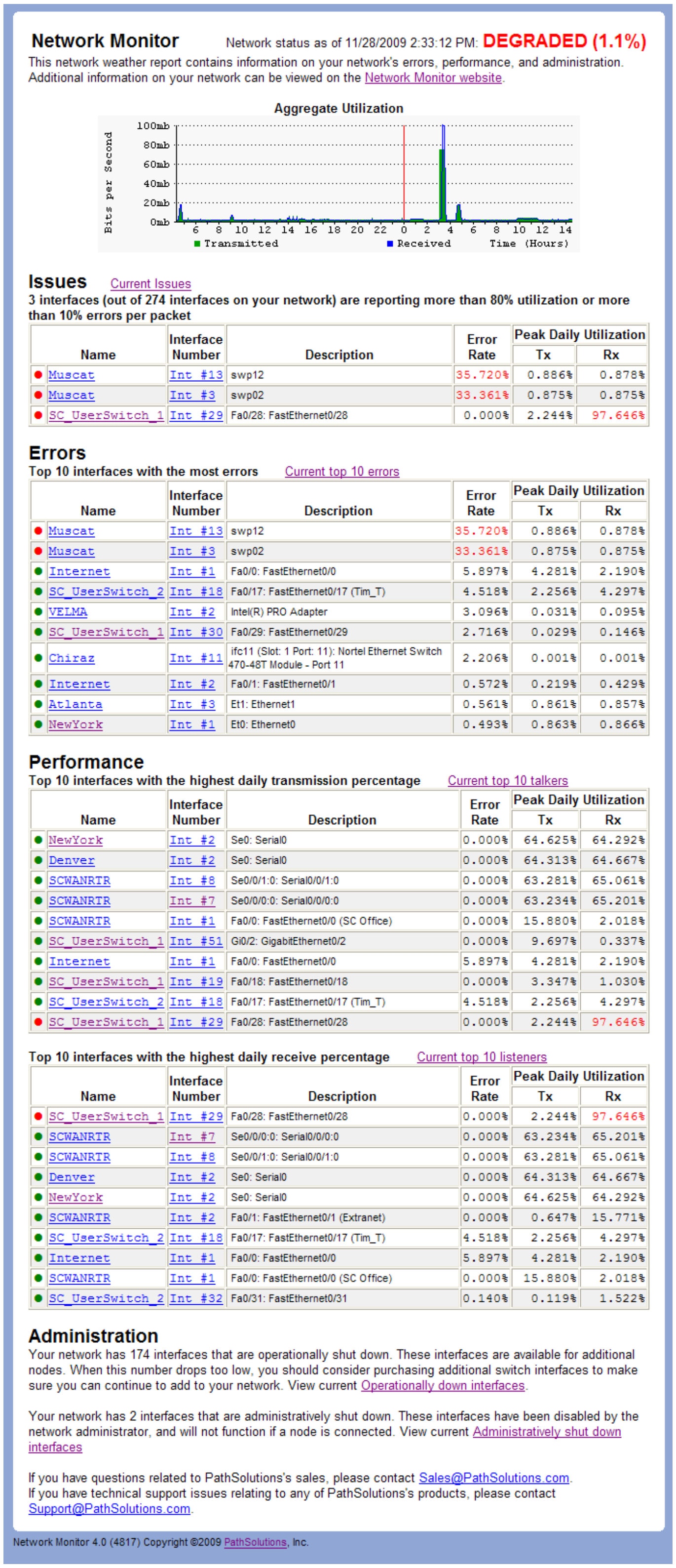


Should threshold errors be SUPPRESSED on this interface?

You can un-suppress errors on an interface by clicking on its status indicator again.

# Using the Network Weather Report

The network Weather Report is sent by the service every night at midnight. An example of a weather report with interfaces that are degraded is as follows:



**Network Monitor** Network status as of 11/28/2009 2:33:12 PM: **DEGRADED (1.1%)**

This network weather report contains information on your network's errors, performance, and administration. Additional information on your network can be viewed on the Network Monitor website.

**Aggregate Utilization**

## Issues

Current Issues

3 interfaces (out of 274 interfaces on your network) are reporting more than 80% utilization or more than 10% errors per packet

| | Name | Interface Number | Description | Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|
| | | | | | Tx | Rx |
| ● | Muscat | Int #13 | swp12 | 35.720% | 0.886% | 0.878% |
| ● | Muscat | Int #3 | swp02 | 33.361% | 0.875% | 0.875% |
| ● | SC_UserSwitch_1 | Int #29 | Fa0/28: FastEthernet0/28 | 0.000% | 2.244% | 97.646% |

## Errors

Top 10 interfaces with the most errors Current top 10 errors

| | Name | Interface Number | Description | Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|
| | | | | | Tx | Rx |
| ● | Muscat | Int #13 | swp12 | 35.720% | 0.886% | 0.878% |
| ● | Muscat | Int #3 | swp02 | 33.361% | 0.875% | 0.875% |
| ● | Internet | Int #1 | Fa0/0: FastEthernet0/0 | 5.897% | 4.281% | 2.190% |
| ● | SC_UserSwitch_2 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 4.518% | 2.256% | 4.297% |
| ● | VELMA | Int #2 | Intel(R) PRO Adapter | 3.096% | 0.031% | 0.095% |
| ● | SC_UserSwitch_1 | Int #30 | Fa0/29: FastEthernet0/29 | 2.716% | 0.029% | 0.146% |
| ● | Chiraz | Int #11 | ifc11 (Slot: 1 Port: 11): Nortel Ethernet Switch 470-48T Module - Port 11 | 2.206% | 0.001% | 0.001% |
| ● | Internet | Int #2 | Fa0/1: FastEthernet0/1 | 0.572% | 0.219% | 0.429% |
| ● | Atlanta | Int #3 | Et1: Ethernet1 | 0.561% | 0.861% | 0.857% |
| ● | NewYork | Int #1 | Et0: Ethernet0 | 0.493% | 0.863% | 0.866% |

## Performance

Top 10 interfaces with the highest daily transmission percentage Current top 10 talkers

| | Name | Interface Number | Description | Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|
| | | | | | Tx | Rx |
| ● | NewYork | Int #2 | Se0: Serial0 | 0.000% | 64.625% | 64.292% |
| ● | Denver | Int #2 | Se0: Serial0 | 0.000% | 64.313% | 64.667% |
| ● | SCWANRTR | Int #8 | Se0/0/1:0: Serial0/0/1:0 | 0.000% | 63.281% | 65.061% |
| ● | SCWANRTR | Int #7 | Se0/0/0:0: Serial0/0/0:0 | 0.000% | 63.234% | 65.201% |
| ● | SCWANRTR | Int #1 | Fa0/0: FastEthernet0/0 (SC Office) | 0.000% | 15.880% | 2.018% |
| ● | SC_UserSwitch_1 | Int #51 | Gi0/2: GigabitEthernet0/2 | 0.000% | 9.697% | 0.337% |
| ● | Internet | Int #1 | Fa0/0: FastEthernet0/0 | 5.897% | 4.281% | 2.190% |
| ● | SC_UserSwitch_1 | Int #19 | Fa0/18: FastEthernet0/18 | 0.000% | 3.347% | 1.030% |
| ● | SC_UserSwitch_2 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 4.518% | 2.256% | 4.297% |
| ● | SC_UserSwitch_1 | Int #29 | Fa0/28: FastEthernet0/28 | 0.000% | 2.244% | 97.646% |

Top 10 interfaces with the highest daily receive percentage Current top 10 listeners

| | Name | Interface Number | Description | Error Rate | Peak Daily Utilization | |
|---|---|---|---|---|---|---|
| | | | | | Tx | Rx |
| ● | SC_UserSwitch_1 | Int #29 | Fa0/28: FastEthernet0/28 | 0.000% | 2.244% | 97.646% |
| ● | SCWANRTR | Int #7 | Se0/0/0:0: Serial0/0/0:0 | 0.000% | 63.234% | 65.201% |
| ● | SCWANRTR | Int #8 | Se0/0/1:0: Serial0/0/1:0 | 0.000% | 63.281% | 65.061% |
| ● | Denver | Int #2 | Se0: Serial0 | 0.000% | 64.313% | 64.667% |
| ● | NewYork | Int #2 | Se0: Serial0 | 0.000% | 64.625% | 64.292% |
| ● | SCWANRTR | Int #2 | Fa0/1: FastEthernet0/1 (Extranet) | 0.000% | 0.647% | 15.771% |
| ● | SC_UserSwitch_2 | Int #18 | Fa0/17: FastEthernet0/17 (Tim_T) | 4.518% | 2.256% | 4.297% |
| ● | Internet | Int #1 | Fa0/0: FastEthernet0/0 | 5.897% | 4.281% | 2.190% |
| ● | SCWANRTR | Int #1 | Fa0/0: FastEthernet0/0 (SC Office) | 0.000% | 15.880% | 2.018% |
| ● | SC_UserSwitch_2 | Int #32 | Fa0/31: FastEthernet0/31 | 0.140% | 0.119% | 1.522% |

## Administration

Your network has 174 interfaces that are operationally shut down. These interfaces are available for additional nodes. When this number drops too low, you should consider purchasing additional switch interfaces to make sure you can continue to add to your network. View current Operationally down interfaces.

Your network has 2 interfaces that are administratively shut down. These interfaces have been disabled by the network administrator, and will not function if a node is connected. View current Administratively shut down interfaces

If you have questions related to PathSolutions's sales, please contact Sales@PathSolutions.com.
If you have technical support issues relating to any of PathSolutions's products, please contact Support@PathSolutions.com.

Network Monitor 4.0 (4817) Copyright ©2009 PathSolutions, Inc.

The default report includes information regarding the health of the network, a section on errors, a section on performance, and administrative information.

All links on the report will link to the product website so you can rapidly check information and work on resolving problems on a daily basis.

It is recommended that you archive these reports in an email folder for future reference.

The network's overall status is displayed in color (red for "Degraded", green for "Good") at the top of the report.

If the overall network status is "Degraded", then a table listing the interfaces with issues will be displayed.

The "Errors" section will list the top 10 interfaces with the most errors.

The "Performance" section will list the top 10 talkers and top 10 listeners.

The "Administration" section will include the number of interfaces that are operationally shut down and administratively shut down.

Network Weather Reports can be customized to include your company logo, or other text. Refer to page 92 (Configuring Email) for information on configuring the report.

**Note:** The Network Weather Report has an attached text file that can be used to display the same data, except without HTML formatting.

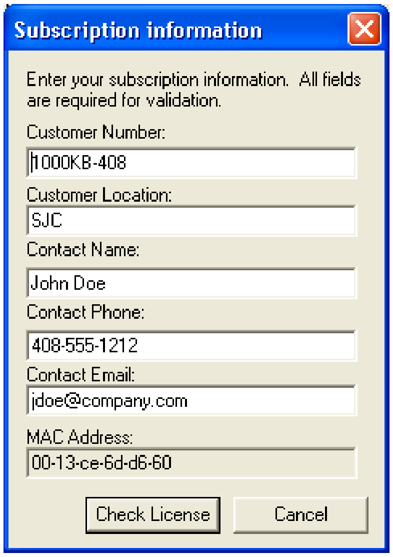
# Using the Configuration Tool

The Configuration Tool is used to change the general configuration options of the product, as well as add or remove devices from monitoring.

## *Running the System Monitor Configuration Tool*

To run the PathSolutions' Network Monitor Configuration Tool, select "Start", choose "Programs", point to "PathSolutions", then choose "PathSolutions' Network Monitor", and select "Config Tool".

If you have not yet entered your subscription information, you may be presented with the following dialog upon starting the program:



Enter your subscription information. All fields are required for validation.

Customer Number: 1000KB-408

Customer Location: SJC

Contact Name: John Doe

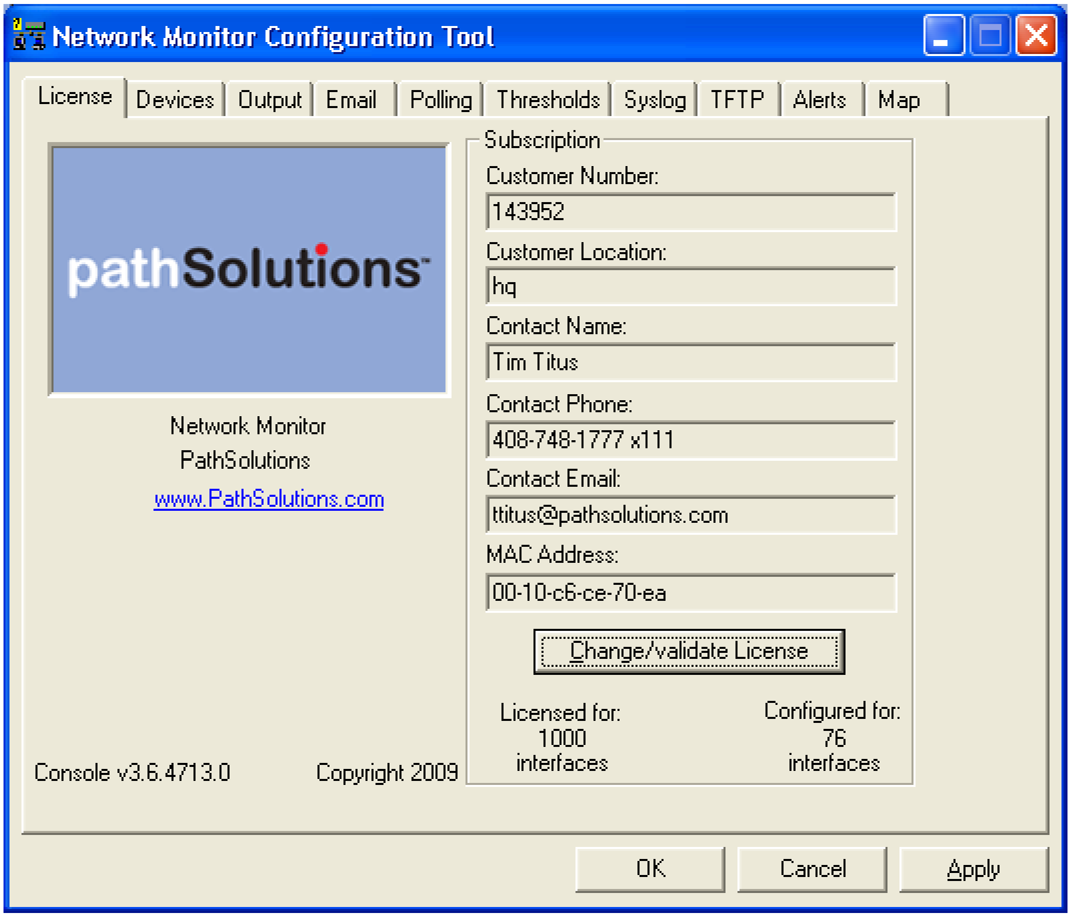
Contact Phone: 408-555-1212

Contact Email: jdoe@company.com

MAC Address: 00-13-ce-6d-d6-60

Enter your subscription information and then click “Check License” to validate the license and continue.

You should see the PathSolutions' Network Monitor Configuration Tool license window:



Subscription

Customer Number: 143952

Customer Location: hq

Contact Name: Tim Titus

Contact Phone: 408-748-1777 x111

Contact Email: ttitus@pathsolutions.com

MAC Address: 00-10-c6-ce-70-ea

Licensed for: 1000 interfaces

Configured for: 76 interfaces

Network Monitor
PathSolutions
www.PathSolutions.com

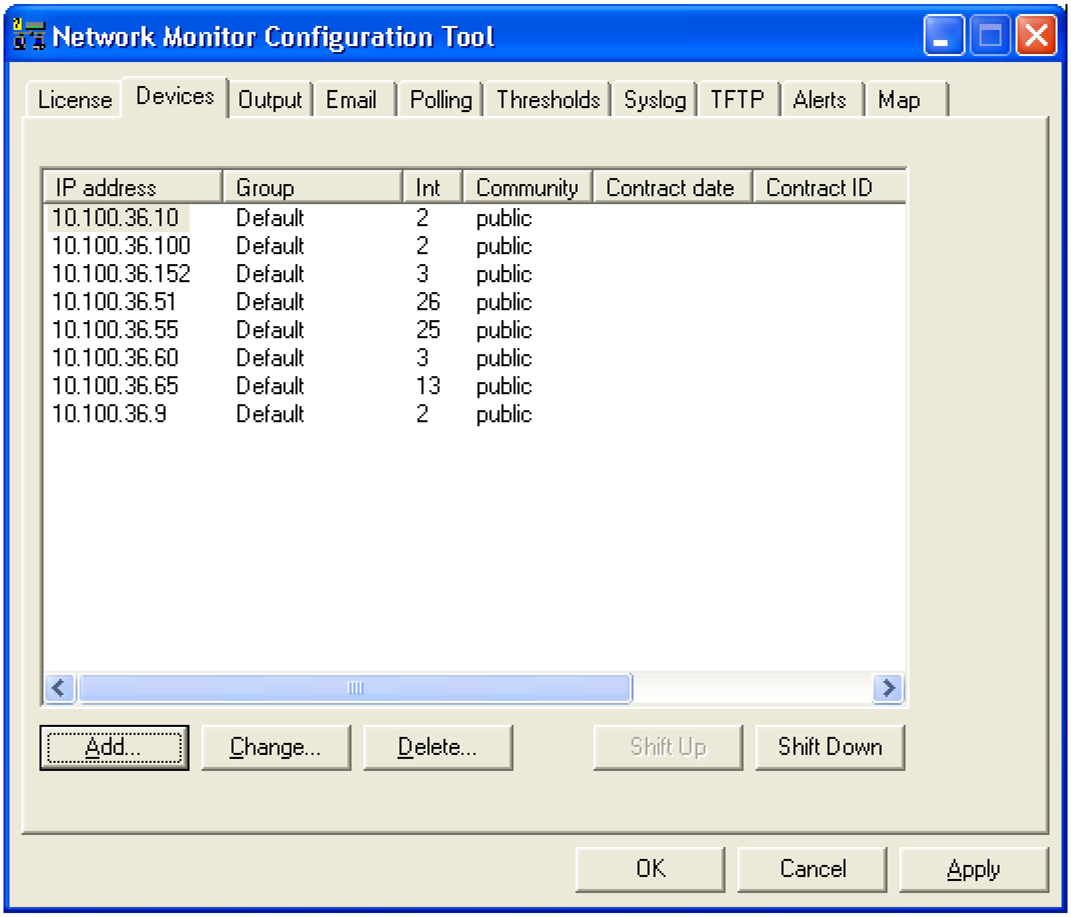
Console v3.6.4713.0

Copyright 2009

You can use this page to verify your subscription information, and determine how many interfaces are currently being monitored.

### *Adding or Removing Devices*

When you select the “Devices” tab, you will see the list of currently monitored devices:



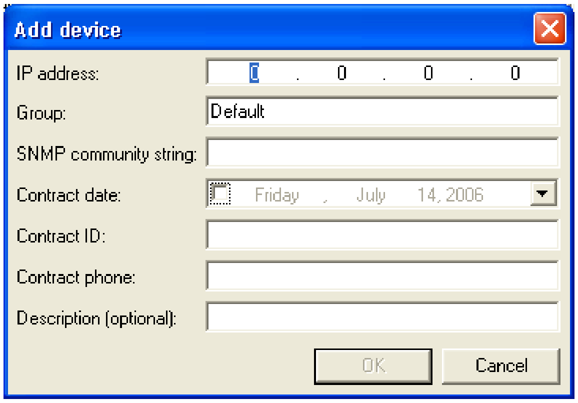
| IP address | Group | Int | Community | Contract date | Contract ID |
|---|---|---|---|---|---|
| 10.100.36.10 | Default | 2 | public | | |
| 10.100.36.100 | Default | 2 | public | | |
| 10.100.36.152 | Default | 3 | public | | |
| 10.100.36.51 | Default | 26 | public | | |
| 10.100.36.55 | Default | 25 | public | | |
| 10.100.36.60 | Default | 3 | public | | |
| 10.100.36.65 | Default | 13 | public | | |
| 10.100.36.9 | Default | 2 | public | | |

You can sort the list (and thus sort the order that the devices are displayed on the web pages) by clicking on a column header.

To move switches up or down in the listing click on the switch and then click " Shift Up" or " Shift Down".

## Adding Devices

To add a device, click "Add". You will see the "Add device" dialog:



IP address: 0 . 0 . 0 . 0

Group: Default

SNMP community string:

Contract date: □ Friday , July 14, 2006

Contract ID:

Contract phone:

Description (optional):

Enter the IP address and SNMP read-only community string for the device. If desired, you can also add a description and support contract information for the device.

Click "OK" to add the device, and the system will present you with a blank dialog box so you can enter another device.

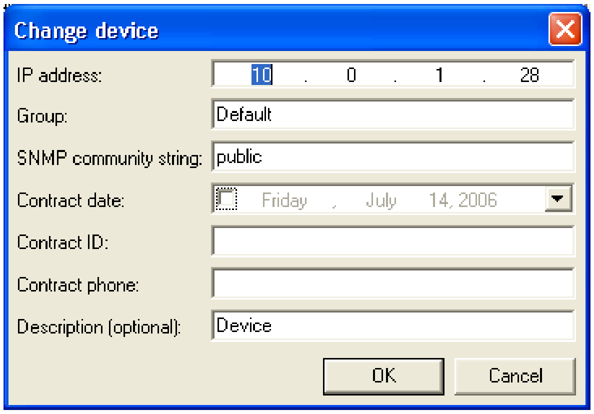
Click "Cancel" on a blank dialog box to close the dialog and stop adding devices.

**Note:** All interfaces for each switch are monitored by default. You can ignore individual interfaces from being monitored on the web interface.

## Changing Device Information

To modify a device, double-click on an existing device IP address, or select the device's IP address and then click on "Change".

You will be presented with the Change Device dialog:



IP address: 10 . 0 . 1 . 28

Group: Default

SNMP community string: public

Contract date: □ Friday , July 14, 2006

Contract ID:

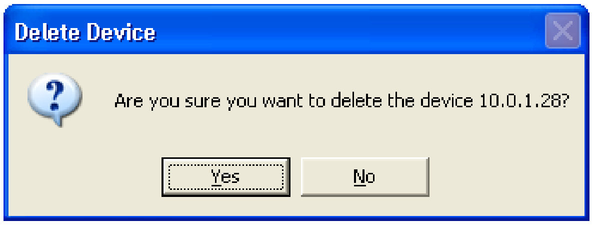
Contract phone:

Description (optional): Device

The only required fields for a device are the IP address and SNMP community string fields. All other fields are optional.

### Deleting Devices

To delete a device, click on the device and then click "Delete". You will see the "Delete device" dialog:

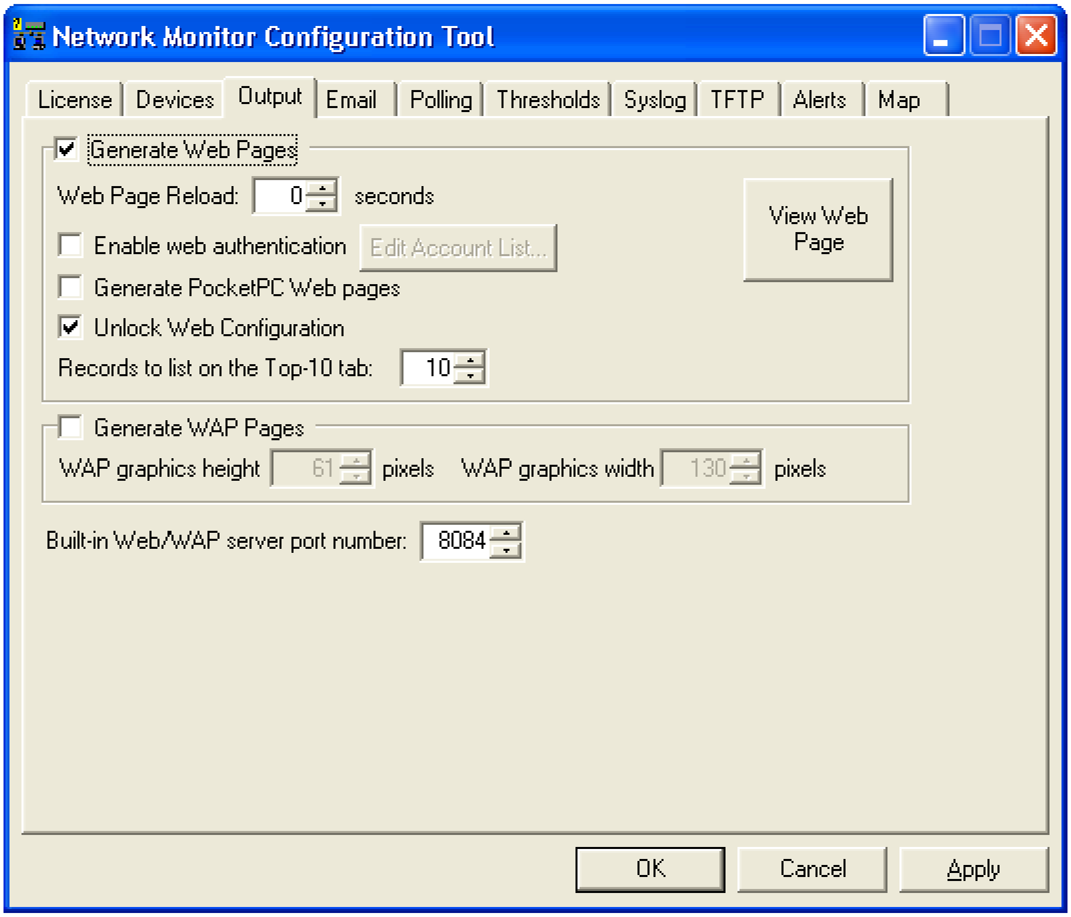


Are you sure you want to delete the device 10.0.1.28?

**Note:** Deleting a device from monitoring will not delete the previously collected graph data. You can add the device back to monitoring and it will continue to use the same data file for graph data storage.

## *Configuring Output*

Select the "Output" tab.  You should see the PathSolutions' Network Monitor Configuration Tool output configuration window:



☑ Generate Web Pages

Web Page Reload: 0 seconds

☐ Enable web authentication

☐ Generate PocketPC Web pages

☑ Unlock Web Configuration

Records to list on the Top-10 tab: 10

☐ Generate WAP Pages

WAP graphics height 61 pixels WAP graphics width 130 pixels

Built-in Web/WAP server port number: 8084

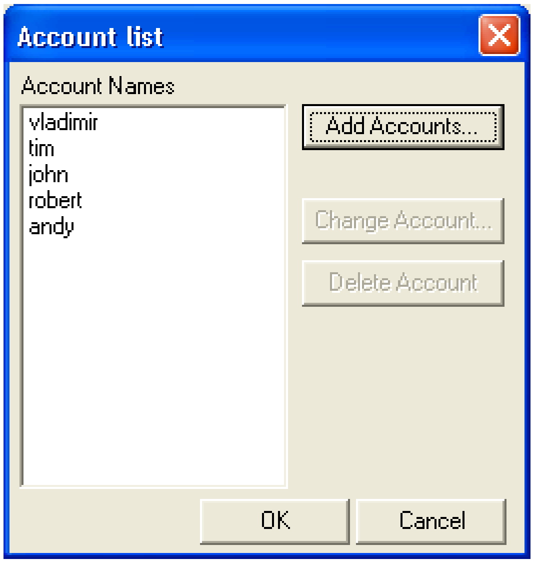
### Web Pages

Check the "Generate Web Pages" box if you desire web pages to be generated by PathSolutions' Network Monitor.

If a web browser opens web pages generated by PathSolutions' Network Monitor, the browser will be instructed to re-load the page every 120 seconds (default).  You can change this web reload value to any timeframe you desire.  If you want to be aware of updated web pages more frequently, lower this number.  Be aware that if you lower the number too low, your computer will spend all of its time re-loading the web page.  Network traffic may increase, and your computer's CPU will suffer.

You can quickly view the web page by clicking on "View Web Page".

If you want to employ account security so passwords are required to view the web pages, check the box "Enable web authentication" and click on the button "Edit Account List" to create accounts. You should see the "Account List" dialog:



From this dialog, you can add accounts by clicking on the "Add Accounts" button, change account names and passwords, or delete accounts.

If you want custom web pages created for PocketPC browsers, check the "Generate PocketPC Web pages" checkbox.

If the web configuration is locked, and you want to unlock it, check the box “Unlock Web Configuration.

## WAP Pages

Check the box if you want WAP pages to be generated by System Monitor.

The WAP graphics files that are generated can be re-sized to perfectly fit your cell phone or PDA’s display. Use the height and width adjustments to define how large or small the graphs should be.

**Note:** You may need to adjust your firewall settings to permit your WAP enabled cell phone to browse from the Internet into your PathSolutions’ Network Monitor server.

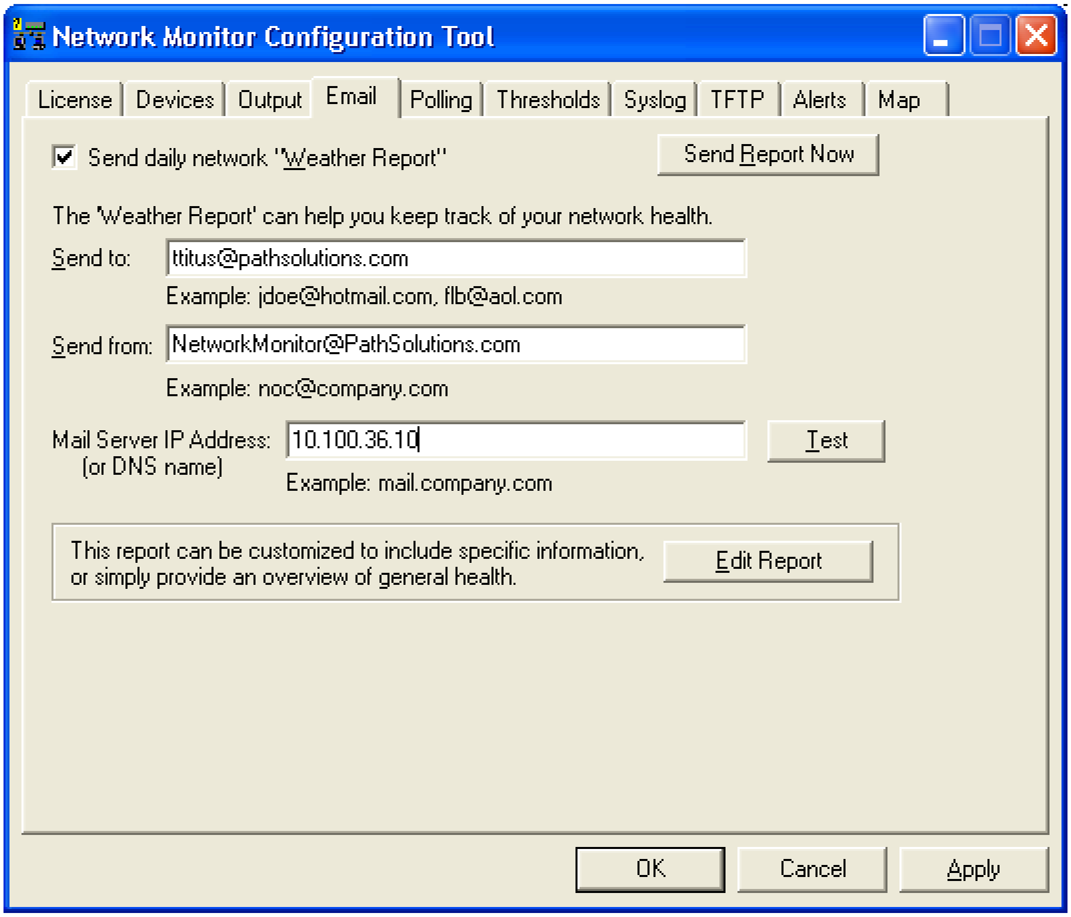
## Built-in Web/WAP Server Port Number

If you are using the integrated Web server to serve pages, you can specify the port that the program should use. You should choose a port that is unused on your system, or the service may not be able to use that port.

If you select a port and then apply the changes by clicking on "Apply" or "OK", and the server does not respond on that port, check the application event log to determine if there may be a port conflict.

### *Configuring Email*

Select the "Email" tab.  You should see the PathSolutions' Network Monitor Configuration Tool email configuration window:



☑ Send daily network "Weather Report"

The 'Weather Report' can help you keep track of your network health.

Send to: ttitus@pathsolutions.com

Example: jdoe@hotmail.com, flb@aol.com

Send from: NetworkMonitor@PathSolutions.com

Example: noc@company.com

Mail Server IP Address: (or DNS name) 10.100.36.10

Example: mail.company.com

This report can be customized to include specific information, or simply provide an overview of general health.

This dialog allows you to change information relating to the network "Weather Report".
If you want to receive a daily network Weather Report, check the Send daily Network Weather Report box.

You must enter an Internet SMTP email address that the report should be sent from, and an Internet SMTP email address that the report should be sent to.

If you want reports to be sent to multiple users on the network, enter the user names here separated by a semicolon, comma, or space.

You must also enter your SMTP relay server IP address.  This address can be your SMTP mail Internet gateway server's IP address (depending on your mail server configuration).  If you are uncertain, check with your email server administrator. Appendix B contains additional information on SMTP relay server configuration.

Click "Test" to send a test email to all users listed.

If you want to modify the network Weather Report, click "Edit Report".  You will be able to modify the default report to include your company logo, custom information, or shrink the email to display only the information you are interested in.

**Note:** The report uses MIME encoding to allow email readers to respect the content as HTML formatted content. If you need assistance with modifying this report, and do not understand MIME encoding, refer to the IETF's RFC1521 (www.ietf.org) or contact PathSolutions technical support for assistance.

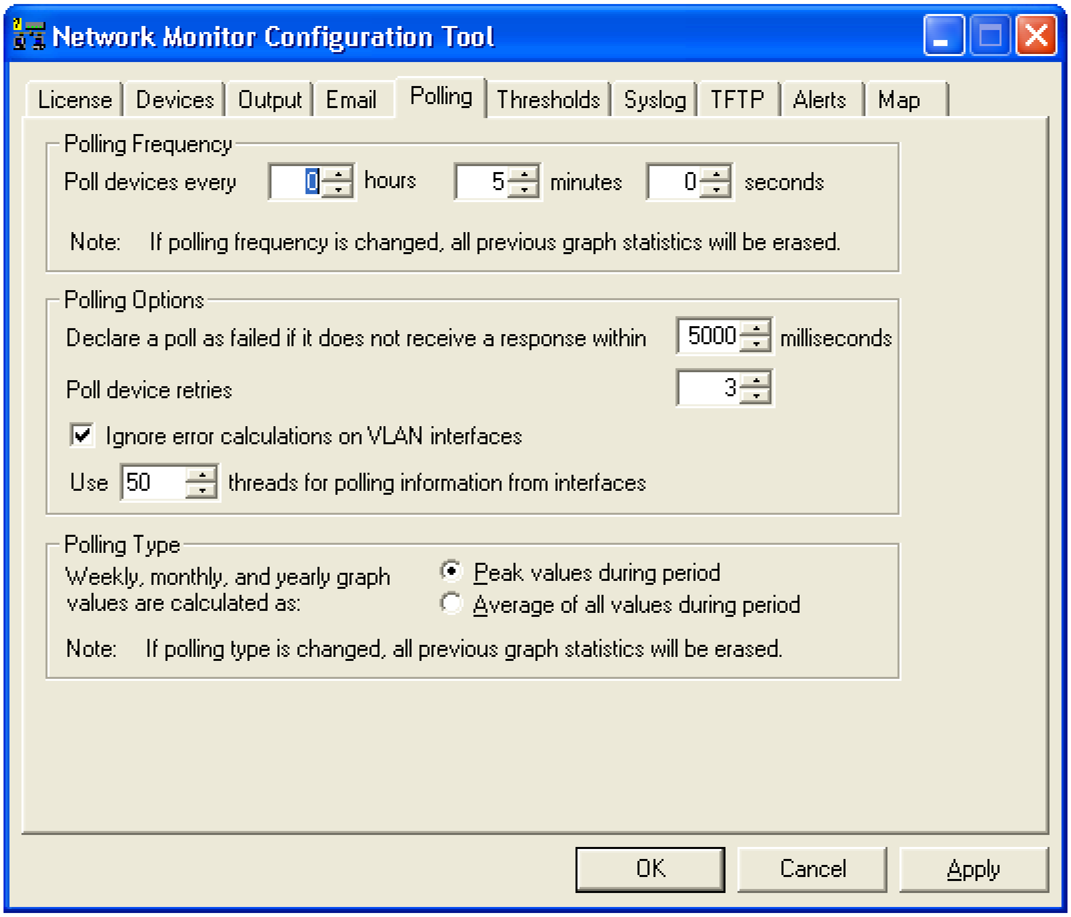
The following objects can be included in the report:

| | |
|---|---|
| %% | This will output a single "%" sign |
| %DATE% | Current date |
| %TIME% | Current time |
| %URL-HOME% | URL to the System Monitor home page |
| %URL-GRAPHICS% | URL pointer to the graphics directory (this can be re-directed to an Internet location) |
| %ISSUES% | Text table showing the interfaces that are currently over the utilization rate or over the error rate |
| %ISSUES*% | HTML table showing the interfaces that are currently over the utilization rate or over the error rate |
| %STATUS-ERR% | Error rate threshold |
| %STATUS-UTIL% | Utilization rate threshold |
| %STATUS-RESULT% | Current status: Good or Degraded |
| %STATUS-COLOR% | HTML color green if the status is Good, or the HTML color red if the status is Degraded |
| %IFSTATUS-GOOD% | If the current status is 'Good', then the text following will be parsed and displayed up until %ENDIF% |
| %IFSTATUS-DEGRADED% | If the current status is 'Degraded', then the text following will be parsed and displayed up until %ENDIF% |
| %TOPCOUNT% | Number of interfaces that are configured to be displayed in the 'Top X' lists (Top 10 Errors, etc.) |
| %TOPERRORS% | Text table showing the interfaces that have the highest error rates |
| %TOPERRORS*% | HTML table showing the interfaces that have the highest error rates |
| %URL-TOPERRORS% | URL pointer to the current top errors web page |
| %TOPTALKERS% | Text table showing the interfaces that have the highest transmission rates |
| %TOPTALKERS*% | HTML table showing the interfaces that have the highest transmission rates |
| %URL-TOPTALKERS% | URL pointer to the current top talkers web page |
| %TOPLISTENERS% | Text table showing the interfaces that have the highest reception rates |
| %TOPLISTENERS*% | HTML table showing the interfaces that have the highest reception rates |
| %URL-TOPLISTENERS% | URL pointer to the current top listeners web page |
| %ADMINDOWN% | Text table showing the interfaces that are currently administratively shut down |
| %ADMINDOWN*% | HTML table showing the interfaces that are currently administratively shut down |
| %ADMINDOWN#% | Total number of administratively shut down interfaces |
| %URL-ADMINDOWN% | URL pointer to the current admin down web page |
| %OPERDOWN% | Text table showing the interfaces that are currently operationally shut down |
| %OPERDOWN*% | HTML table showing the interfaces that are currently operationally shut down |
| %OPERDOWN#% | Total number of operationally shut down interfaces |
| %URL-OPERDOWN% | URL pointer to the current oper down web page |

**Note:** Do NOT put a period "." on its own line anywhere in this file.

## *Configuring Polling Behavior*

Select the "Polling" tab. You should see the PathSolutions' Network Monitor Configuration Tool polling configuration window:



Polling Frequency

Poll devices every 0 hours 5 minutes 0 seconds

Note: If polling frequency is changed, all previous graph statistics will be erased.

Polling Options

Declare a poll as failed if it does not receive a response within 5000 milliseconds

Poll device retries 3

☑ Ignore error calculations on VLAN interfaces

Use 50 threads for polling information from interfaces

Polling Type

Weekly, monthly, and yearly graph values are calculated as:

● Peak values during period
○ Average of all values during period

Note: If polling type is changed, all previous graph statistics will be erased.

PathSolutions' Network Monitor is very 'network friendly', and makes every attempt to prevent flooding the network with requests. One minimum sized SNMP packet is sent per interface.

### Configuring the Polling Frequency

You will want to select how often the program should poll each interface.

The default is 5 minutes. Less frequent polls will decrease the traffic on your network, however it will not provide you with as granular information on utilization and error rates.

**Note:** If you change the polling frequency, all historical utilization information (daily, weekly, monthly, and yearly graphs) will be erased when you click "OK", or "Apply".

**Note:** It is very important to make sure you do not poll your devices too often, as this can add to network overhead. In general, you should poll your interfaces every 5 minutes.

### Failed Poll Option

PathSolutions' Network Monitor will need to know how long to wait for a response before declaring an individual poll as failed. The default is 3000ms (3 seconds). If you have a network that has extremely high latencies, you may choose to increase this number. If you want PathSolutions' Network Monitor to declare a device as failed if it does not respond within a smaller response window you can adjust this number down.

### VLAN Interfaces

For some switch manufacturers, VLAN interfaces report anomalous errors.  If you do not want the error rate of VLAN interfaces calculated, check this box.  The VLAN interface will still be listed, but it will not become an “issue” listed under the “Issues” tab.

### Polling Threads

PathSolutions’ Network Monitor uses 20 threads for polling devices for SNMP information.  If you have a faster computer, you may choose to increase this number.  If you have a slower computer, and PathSolutions’ Network Monitor is utilizing 100% of the system’s CPU during a polling cycle, you may get better performance by reducing this number.  This will cause less thread overhead in the system.

### Polling Type

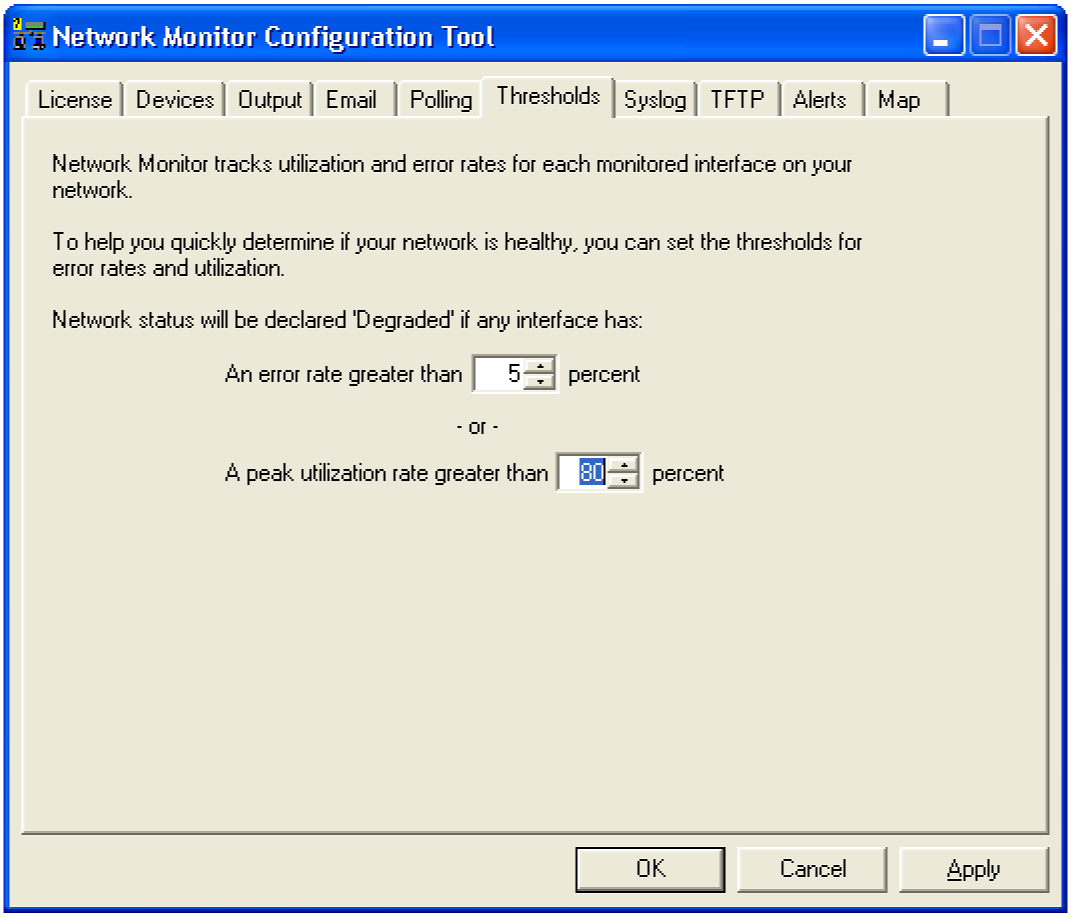
The daily polling information is summarized to the weekly graph, and the weekly graph is summarized to the monthly graph, and the yearly graph is summarized to the yearly graph.
The mechanism used for summarization can be configured to maintain the average utilization during the period, or the peak values during the period.

Typically, knowing how often an interface reached peak utilization is more valuable than averaging, as the average utilization information loses its granularity through the averaging process.

**Note:** If you change the polling frequency, all historical utilization information (daily, weekly, monthly, and yearly graphs) will be erased when you click “OK”, or “Apply”.

### *Configuring Thresholds*

Select the "Thresholds" tab.  You should see the System Monitor Configuration Tool thresholds configuration window:



Network Monitor tracks utilization and error rates for each monitored interface on your network.

To help you quickly determine if your network is healthy, you can set the thresholds for error rates and utilization.

Network status will be declared 'Degraded' if any interface has:

An error rate greater than 5 percent

- or -

A peak utilization rate greater than 80 percent

If an interface has an error rate higher than 10%, network status will be changed to 'Degraded'.

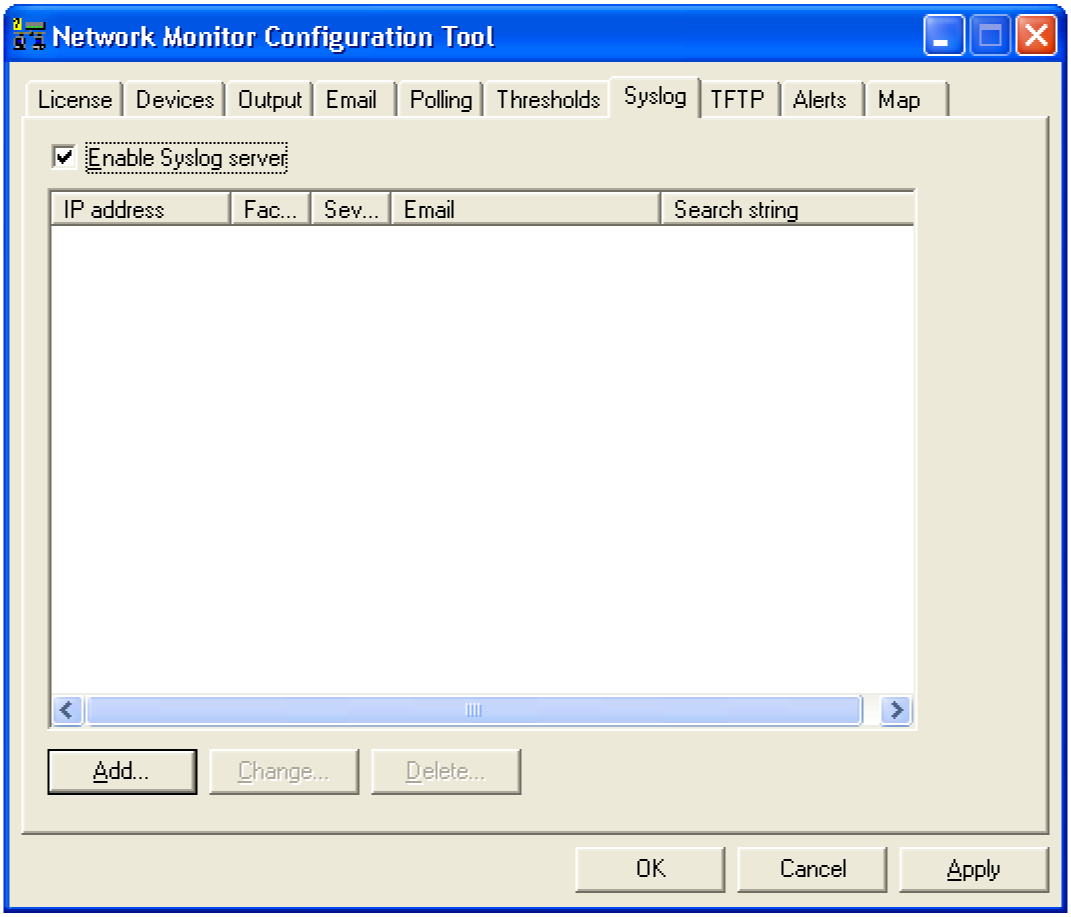
If an interface has a peak utilization rate (transmitted or received) over 80%, network status will be changed to 'Degraded'.

These numbers can be adjusted to suit your specific network environment, and your tolerance for errors.

When you are finished making changes, click "OK" to apply changes and exit the configuration tool.

## Enabling the Syslog Server

The system has a built in syslog server to receive and organize syslog messages received from network devices:



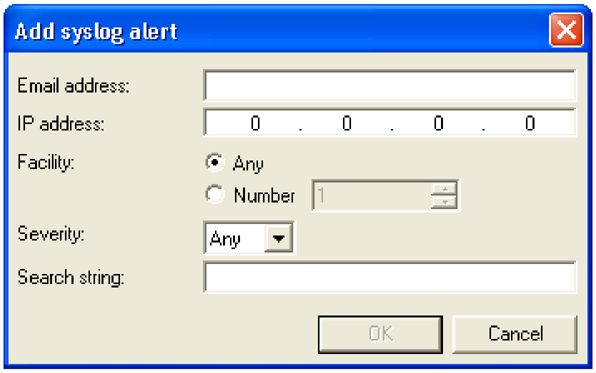
☑ Enable Syslog server

To enable the syslog server, check the box "Enable Syslog Server".

Syslog messages will be captured and be visible from the web pages. Click on the "Syslog" link to the right of "Telnet" and "Web" to view the received syslog messages from each device.

**Note:** You will have to configure each of your network devices to send their syslog messages to the PathSolutions' Network Monitor server.

You can add alerting for syslog messages by clicking on the "Add" button. You should see the following dialog:



Email address:

IP address: 0 . 0 . 0 . 0

Facility: ● Any ○ Number 1

Severity: Any

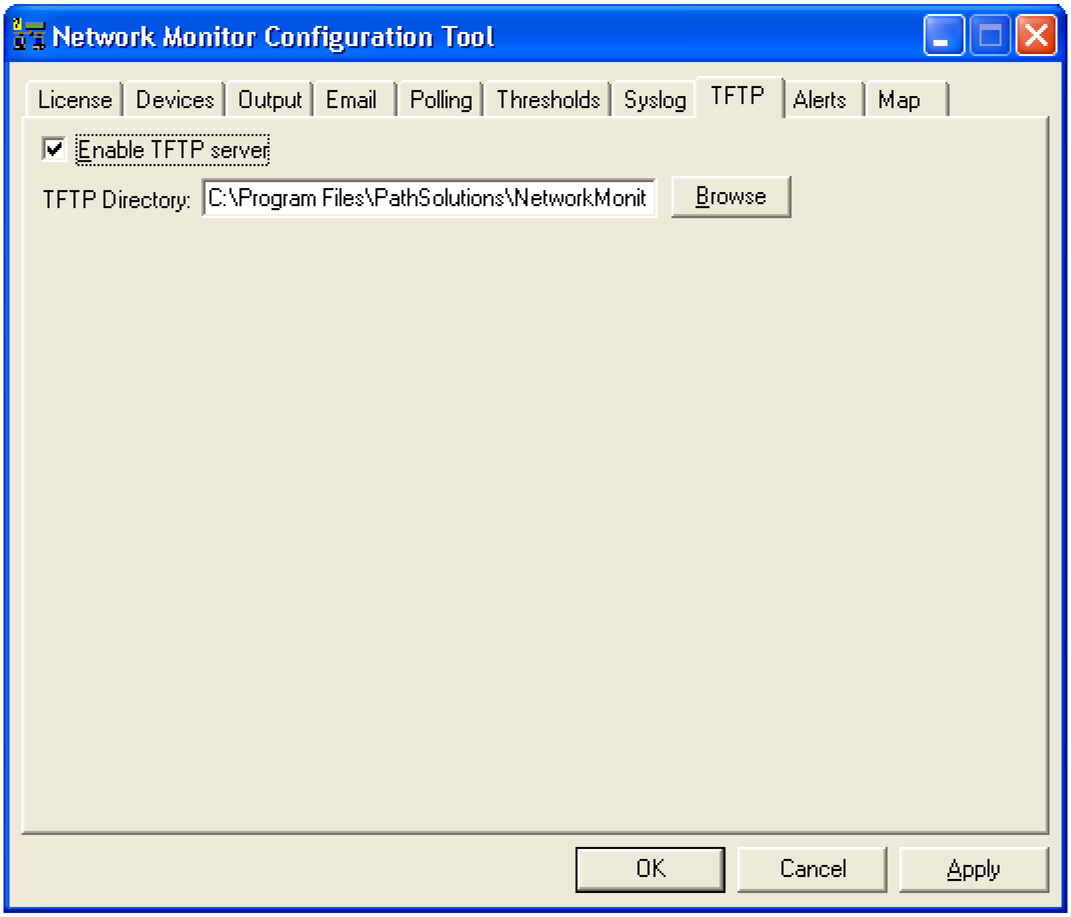
Search string:

Enter the email address that should receive the alert, the IP address where the syslog message should come from, and the facility number (or Any if it could be any facility number).

You will also need to enter a search string that should match the received message. For example, to generate an alert if an interface changes status, you would want to enter “changed status to”. This would generate an alert if the following message arrived: “Interface Fa0/2 changed status to down”

### *Enabling the TFTP Server*

The system can receive TFTP files from network devices via the built-in TFTP server:



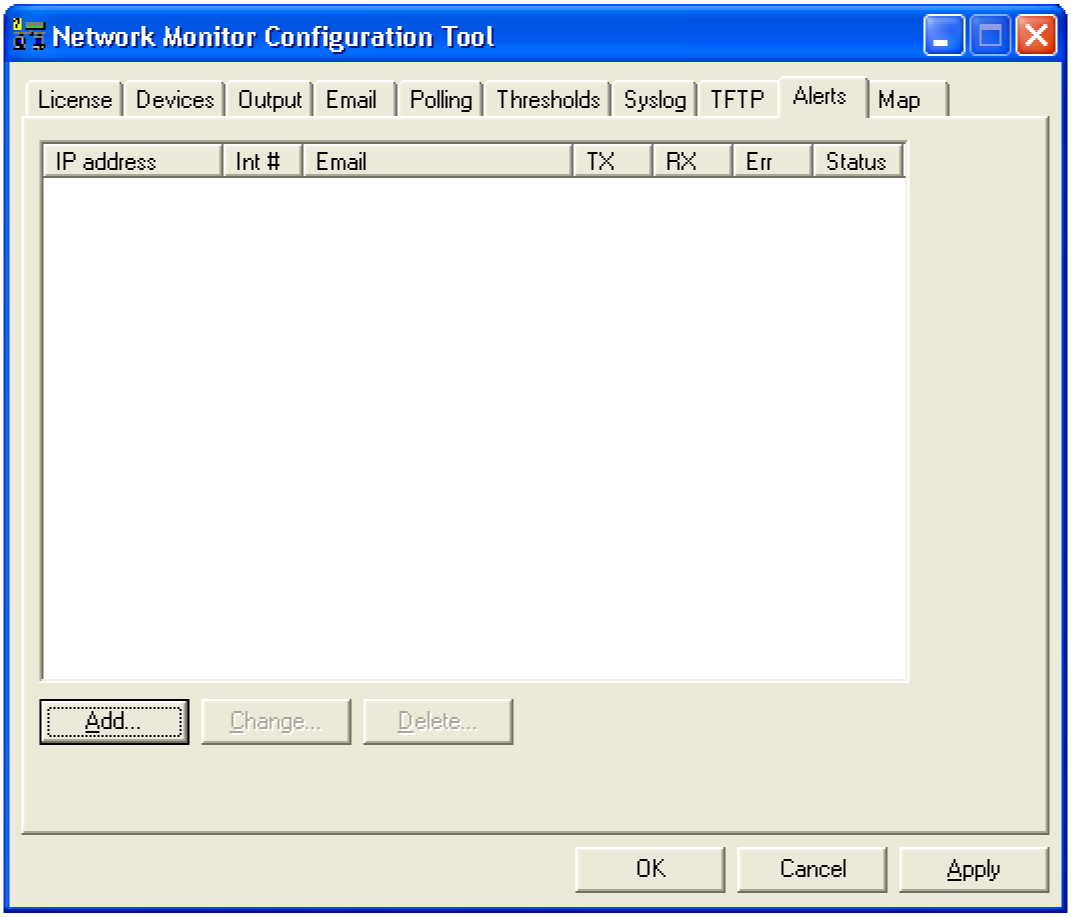
☑ Enable TFTP server

TFTP Directory: C:\Program Files\PathSolutions\NetworkMonit

You can enter a different directory where the TFTP files are saved/retrieved from if desired.

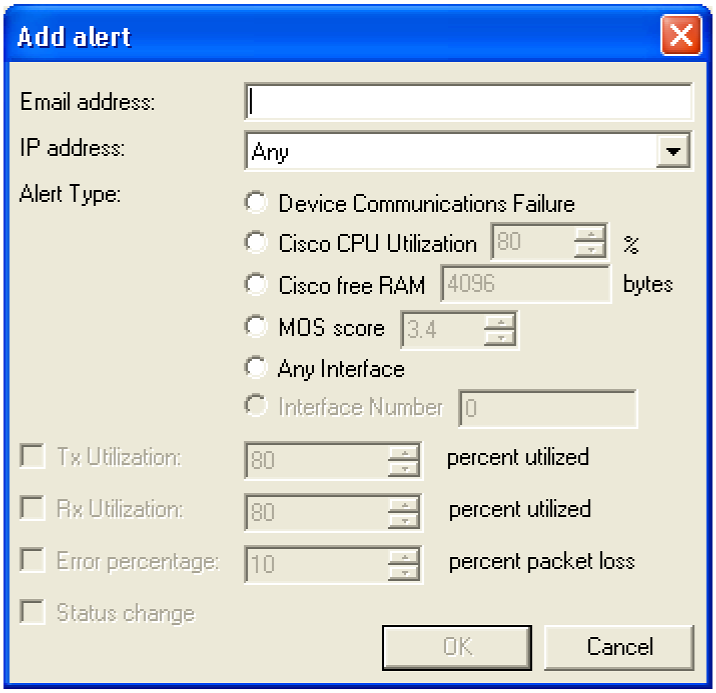
### *Enabling Alerting*

The system can generate alerts if interfaces change status or exceed set levels of utilization or errors:



You can add alerting for interfaces by clicking on the “Add” button.

You should see the following dialog:



Add alert

Email address:

IP address: Any

Alert Type:

○ Device Communications Failure

○ Cisco CPU Utilization 80 %

○ Cisco free RAM 4096 bytes

○ MOS score 3.4

○ Any Interface

○ Interface Number 0

□ Tx Utilization: 80 percent utilized

□ Rx Utilization: 80 percent utilized

□ Error percentage: 10 percent packet loss

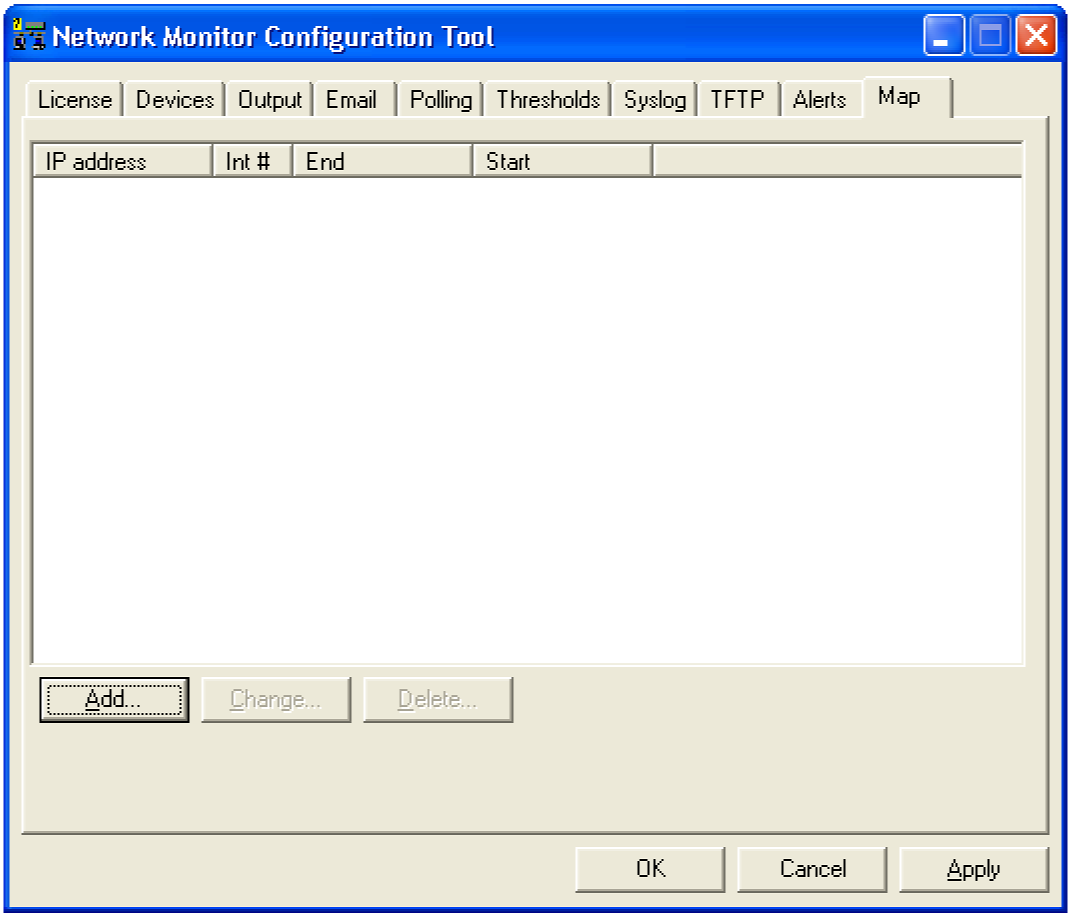
□ Status change

Enter the email address that should receive the alert, the IP address of the device and the interface number. Enter Comm Fail if you want to receive an alert if the device cannot be communicated with, or “Any” if you want to receive the alert if any interface on the device exceeds the threshold.

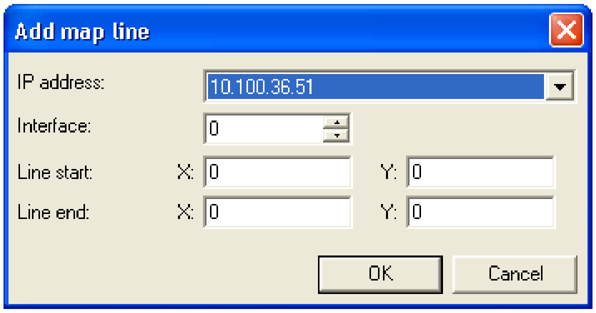
You should check the box for Utilization, Error percentage, or status change if you want these variables to trigger an alert or not.

### Configuring the Network Map

The system can generate alerts if interfaces change status or exceed set levels of utilization or errors:



To add a line, click “Add”.  You should get the add map line dialog:



IP address: 10.100.36.51

Interface: 0

Line start: X: 0 Y: 0

Line end: X: 0 Y: 0

Choose the IP address of the device and then enter the interface number that should be updated.  Then enter the line start X and Y coordinate and the line end X and Y coordinate.

# Sending Emailed Reports

Reports can be emailed to users whenever desired, or on regular schedules.

To set up a report to be sent, create a text file with Notepad or other text editor. This file should contain four fields, separated by at least one <TAB> character:

```
;Email Address    Template File                Device       Interface
;---------------- ---------------------------- ------------ ---------
jdoe@company.com  IntMailDetailDaily.txt       192.168.1.1  1
jdoe@company.com  IntMailSummartyDaily.txt     192.168.6.12 14
jdoe@company.com  SystemMailDaily.txt          /            /
```

The first field is the Email address where the report should be sent.

The second field is the email template file to use to send the report. Templates can be found in the "MailTemplates" subdirectory.

The third field references a monitored device. This field may or may not be required depending on the template used. If a system-wide report is used, it does not need a specific device to be referenced, and a slash '/' should be used instead.

The fourth field references a specific interface on the specified device. If the report is a system-wide report, or a device report, no interface needs to be specified and a slash '/' can be used instead.

Save this file with any filename that ends in ".cfg" in the "ReportSend" subdirectory and the report(s) will be sent during the next polling period and the file deleted.

**Note:** It's valuable to save this file in an alternate directory first and then copy it to the "ReportSend" directory when you want it to be sent.

**Note:** This process can be automated via the Windows Task manager to schedule reports to be sent on a regular basis.

**Note:** All files in the "ReportSend" directory with the extension .cfg will be processed and deleted every poll period.

# Creating Email Report Templates

Existing email report templates are located in the "MailTemplates" directory.

They can be edited with a text editor and copied to create new templates. The format of the templates includes standard MIME encapsulation headers and definitions for multipart messages (HTML and embedded graphics).

PathSolutions' Network Monitor will pre-process the template and add data elements using the %ELEMENT% replacement strings.

Available replacement strings are as follows:

| | |
|---|---|
| %% | Prints percent sign |
| %DATE% | Prints current date |
| %TIME% | Prints current time |
| %COMMENT-START% | Starts a comment area that won't be sent in the email |
| %COMMENT-END% | Ends a comment area |
| %CUSTOMERNUMBER% | Prints the licensed customer number |
| %CUSTOMERLOCATION% | Prints the licensed customer location |
| %LICENSEDINTERFACES% | Prints the licensed interface count |
| %LICENSEEXPIRATION% | Prints the license expiration |
| %RESELLERNUMBER% | Prints the reseller number |
| %INTERFACES% | Prints the number of monitored interfaces |
| %VERSION% | Prints the version of the program |
| %REVISION% | Prints the revision of the program |
| %PRODNUMBER% | Prints the product license number |
| %PRODNAME% | Prints the product name |
| %COMPANYNAME% | Prints the company name |
| %EMAILADDRESS% | Prints the email address(es) that this email will be sent to |
| %LICENSEDAYSLEFT% | Prints the number of licensed days remaining |
| %URL-HOME% | Prints the full URL to the home page |
| %URL-HEALTH% | Prints the full URL to the health page |
| %URL-GRAPHICS% | Prints the full URL to the graphics directory |
| %URL-FAVORITES% | Prints the full URL to the favorites page |
| %FAVORITES% | Prints a text table of favorite interfaces |
| %FAVORITES*% | Prints an HTML table of favorite interfaces |
| %ISSUES% | Prints a text table of current issues |
| %ISSUES*% | Prints an HTML table of current issues |
| %ISSUES#% | Prints the current number of issues |
| %URL-ISSUES% | Prints the full URL to the issues page |
| %STATUS-PERCENT% | Prints the current health percentage |
| %STATUS-ERR% | Prints the configured error threshold level |
| %STATUS-UTIL% | Prints the configured utilization threshold level |
| %STATUS-RESULT% | Prints "Good" or "Degraded" depending if there are any issues |
| %STATUS-COLOR% | Prints "#008000" or "#FF0000" depending if there are any issues |
| %IFSTATUS-GOOD% | Prints the following if there are no issues |
| %IFSTATUS-DEGRADED% | Prints the following if there are issues |
| %ENDIF% | Ends a conditional IFSTATUS section |
| %IFDEVICE-CISCO% | Prints the following if it is a Cisco device |
| %ENDIF-CISCO% | Ends conditional for Cisco device |
| %IFLICENSE-VOIP% | Prints the following if the system is licensed for VoIP |
| %ENDIF-VOIP% | Ends conditional for VoIP License |
| %TOPCOUNT% | Prints the number of interfaces configured for the Top list |
| %TOPERRORS% | Prints a text table of top interfaces with errors |
| %TOPERRORS*% | Prints an HTML table of top interfaces with errors |
| %URL-TOPERRORS% | Prints the full URL to the top errors page |
| %TOPTALKERS% | Prints a text table of top talkers |
| %TOPTALKERS*% | Prints an HTML table of top talkers |
| %URL-TOPTALKERS% | Prints the full URL to the top talkers page |
| %TOPLISTENERS% | Prints a text table of top listeners |
| %TOPLISTENERS*% | Prints an HTML table of top listeners |
| %URL-TOPLISTENERS% | Prints the full URL to the top listeners page |
| %ADMINDOWN% | Prints a text table of admin down interfaces |
| %ADMINDOWN*% | Prints an HTML table of admin down interfaces |
| %ADMINDOWN#% | Prints the number of admin down interfaces |
| %URL-ADMINDOWN% | Prints the full URL to the admin down page |
| %OPERDOWN% | Prints a text table of oper down interfaces |
| %OPERDOWN*% | Prints an HTML table of oper down interfaces |

| | |
|---|---|
| %OPERDOWN#% | Prints the number of oper down interfaces |
| %URL-OPERDOWN% | Prints the full URL to the oper down page |
| %POLLDELAY% | Prints the current configured poll delay |
| %SAVESTATSTICKCOUNT% | Prints the number of ticks (ms) required during the last poll to save statistics to disk |
| %SAVESTATSTICKCOUNTAVG% | Prints the average number of ticks (ms) required to save statistics to disk |
| %POLLTICKCOUNT% | Prints the number of ticks (ms) required during the last poll to collect SNMP information from all devices |
| %POLLTICKCOUNTAVG% | Prints the average number of ticks (ms) required to collect SNMP information from all devices |
| %ANALYZETICKCOUNT% | Prints the number of ticks (ms) required during the last poll to analyze all data |
| %ANALYZETICKCOUNTAVG% | Prints the average number of ticks (ms) required to analyze all data |
| %OUTPUTTICKCOUNT% | Prints the number of ticks (ms) required during the last poll to write output information |
| %OUTPUTTICKCOUNTAVG% | Prints the average number of ticks (ms) required to write output information |
| %POLLHOURS% | Prints the configured poll delay hours |
| %POLLMINUTES% | Prints the configured poll delay minutes |
| %POLLSECONDS% | Prints the configured poll delay seconds |
| %POLLFAILSECONDS% | Prints the number of seconds that the last poll failed by |
| %POLLFAILTABLE% | Prints the text version of the poll fail table |
| %POLLFAILTABLE*% | Prints the HTML version of the poll fail table |
| %SYSTEM-DAILY-UTIL% | Prints base64 encoding of the daily aggregate utilization graph |
| %SYSTEM-DAILY-ERRORS% | Prints base64 encoding of the daily overall errors graph |
| %SYSTEM-DAILY-ISSUES% | Prints base64 encoding of the daily overall issues graph |
| %SYSTEM-DAILY-INTERFACES% | Prints base64 encoding of the daily interfaces graph |
| %SYSTEM-WEEKLY-UTIL% | Prints base64 encoding of the weekly aggregate utilization graph |
| %SYSTEM-WEEKLY-UTIL% | Prints base64 encoding of the weekly overall errors graph |
| %SYSTEM-WEEKLY-ISSUES% | Prints base64 encoding of the weekly overall issues graph |
| %SYSTEM-WEEKLY-INTERFACES% | Prints base64 encoding of the weekly interfaces graph |
| %SYSTEM-MONTHLY-UTIL% | Prints base64 encoding of the monthly aggregate utilization graph |
| %SYSTEM-MONTHLY-ERRORS% | Prints base64 encoding of the monthly overall errors graph |
| %SYSTEM-MONTHLY-ISSUES% | Prints base64 encoding of the monthly overall issues graph |
| %SYSTEM-MONTHLY-INTERFACES% | Prints base64 encoding of the monthly interfaces graph |
| %SYSTEM-YEARLY-UTIL% | Prints base64 encoding of the yearly aggregate utilization graph |
| %SYSTEM-YEARLY-ERRORS% | Prints base64 encoding of the yearly overall errors graph |
| %SYSTEM-YEARLY-ISSUES% | Prints base64 encoding of the yearly overall issues graph |
| %SYSTEM-YEARLY-INTERFACES% | Prints base64 encoding of the yearly interfaces graph |
| %URL-DEVICE% | Prints the full URL to the specified device page |
| %DEVICE-NUMBER% | Prints the device number |
| %DEVICE-AGENT% | Prints the device agent (IP address) |
| %DEVICE-GROUP% | Prints the configured group for the device |
| %DEVICE-CONTRACT-DATE% | Prints the configured device service contract date |
| %DEVICE-CONTRACT-ID% | Prints the configured device ID number associated with the service contract |
| %DEVICE-CONTRACT-PHONE% | Prints the configured device service contract phone number |
| %DEVICE-DESCRIPTION% | Prints the configured device description |
| %DEVICE-INTERFACES% | Prints the number of interfaces for the device |
| %DEVICE-ADMINDOWN% | Prints the number of admin down interfaces on the device |
| %DEVICE-OPERDOWN% | Prints the number of oper down interfaces on the device |
| %DEVICE-INT-DESCRIPTION% | Prints the device internal description (sysDescr) |
| %DEVICE-LOCATION% | Prints the device configured location (sysLocation) |
| %DEVICE-CONTACT% | Prints the device configured contact (sysContact) |
| %DEVICE-NAME% | Prints the device configured name (sysName) |
| %DEVICE-SERIALNO% | Prints the device serial number (Cisco IOS only) |
| %DEVICE-CPU% | Prints the device current CPU utilization graph (Cisco IOS only) |
| %DEVICE-RAM% | Prints the device current RAM utilization graph (Cisco IOS only) |
| %DEVICE-DAILY-UTIL% | Prints base64 encoding of the daily device overall utilization graph |
| %DEVICE-DAILY-CPU% | Prints base64 encoding of the daily CPU utilization graph (Cisco IOS only) |
| %DEVICE-DAILY-RAM% | Prints base64 encoding of the daily RAM utilization graph (Cisco IOS only) |
| %DEVICE-DAILY-LATENCY% | Prints base64 encoding of the daily latency graph (VoIP only) |
| %DEVICE-DAILY-JITTER% | Prints base64 encoding of the daily jitter graph (VoIP only) |
| %DEVICE-DAILY-LOSS% | Prints base64 encoding of the daily loss graph (VoIP only) |
| %DEVICE-DAILY-MOS% | Prints base64 encoding of the daily MOS graph (VoIP only) |
| %DEVICE-WEEKLY-UTIL% | Prints base64 encoding of the weekly device overall utilization graph |
| %DEVICE-WEEKLY-CPU% | Prints base64 encoding of the weekly CPU utilization graph (Cisco IOS only) |
| %DEVICE-WEEKLY-RAM% | Prints base64 encoding of the weekly RAM utilization graph (Cisco IOS only) |
| %DEVICE-WEEKLY-LATENCY% | Prints base64 encoding of the weekly latency graph (VoIP only) |
| %DEVICE-WEEKLY-JITTER% | Prints base64 encoding of the weekly jitter graph (VoIP only) |
| %DEVICE-WEEKLY-LOSS% | Prints base64 encoding of the weekly loss graph (VoIP only) |
| %DEVICE-WEEKLY-MOS% | Prints base64 encoding of the weekly MOS graph (VoIP only) |
| %DEVICE-MONTHLY-UTIL% | Prints base64 encoding of the monthly device overall utilization graph |
| %DEVICE-MONTHLY-CPU% | Prints base64 encoding of the monthly CPU utilization graph (Cisco IOS only) |
| %DEVICE-MONTHLY-RAM% | Prints base64 encoding of the monthly RAM utilization graph (Cisco IOS only) |
| %DEVICE-MONTHLY-LATENCY% | Prints base64 encoding of the monthly latency graph (VoIP only) |
| %DEVICE-MONTHLY-JITTER% | Prints base64 encoding of the monthly jitter graph (VoIP only) |
| %DEVICE-MONTHLY-LOSS% | Prints base64 encoding of the monthly loss graph (VoIP only) |

| | |
|---|---|
| %DEVICE-MONTHLY-MOS% | Prints base64 encoding of the monthly MOS graph (VoIP only) |
| %DEVICE-YEARLY-UTIL% | Prints base64 encoding of the yearly device overall utilization graph |
| %DEVICE-YEARLY-CPU% | Prints base64 encoding of the yearly CPU utilization graph (Cisco IOS only) |
| %DEVICE-YEARLY-RAM% | Prints base64 encoding of the yearly RAM utilization graph (Cisco IOS only) |
| %DEVICE-YEARLY-LATENCY% | Prints base64 encoding of the yearly latency graph (VoIP only) |
| %DEVICE-YEARLY-JITTER% | Prints base64 encoding of the yearly jitter graph (VoIP only) |
| %DEVICE-YEARLY-LOSS% | Prints base64 encoding of the yearly loss graph (VoIP only) |
| %DEVICE-YEARLY-MOS% | Prints base64 encoding of the yearly MOS graph (VoIP only) |
| %URL-INT% | Prints the full URL to the specified interface page |
| %INT-NUMBER% | Prints the interface number |
| %INT-DESCRIPTION% | Prints the interface description |
| %INT-ALIAS% | Prints the interface alias |
| %INT-NAME% | Prints the interface name |
| %INT-DAILYERRORRATE% | Prints the daily peak error rate |
| %INT-DAILYERRORRATECOLOR% | Prints the daily peak error rate color |
| %INT-DAILYTXRATE% | Prints the peak daily transmit rate |
| %INT-DAILYTXRATECOLOR% | Prints the peak daily transmit rate color |
| %INT-DAILYRXRATE% | Prints the peak daily receive rate |
| %INT-DAILYRXRATECOLOR% | Prints the peak daily receive rate color |
| %INT-SPEED% | Prints the interface speed of the interface |
| %INT-DUPLEX% | Prints the interface duplex of the interface |
| %INT-ADMINSTATUS% | Prints the current admin status of the interface |
| %INT-OPERSTATUS% | Prints the current oper status of the interface |
| %INT-TXBROADCAST% | Prints the transmit broadcast rate of the interface |
| %INT-RXBROADCAST% | Prints the receive broadcast rate of the interface |
| %INT-ADMINSTATUSLAST% | Prints the last admin status of the interface |
| %INT-OPERSTATUSLAST% | Prints the last oper status of the interface |
| %INT-CURRTXUTIL% | Prints the current (last poll) transmit rate of the interface |
| %INT-CURRRXUTIL% | Prints the current (last poll) receive rate of the interface |
| %INT-CURRERRPCT% | Prints the current (last poll) error rate of the interface |
| %INT-DAILY-BPS% | Prints base64 encoding of the daily bits per second graph |
| %INT-DAILY-PCT% | Prints base64 encoding of the daily percentage graph |
| %INT-DAILY-PPCT% | Prints base64 encoding of the daily peak percentage graph |
| %INT-DAILY-PKTS% | Prints base64 encoding of the daily packets graph |
| %INT-DAILY-BCSTS% | Prints base64 encoding of the daily broadcasts graph |
| %INT-DAILY-ERRORS% | Prints base64 encoding of the daily errors graph |
| %INT-WEEKLY-BPS% | Prints base64 encoding of the weekly bits per second graph |
| %INT-WEEKLY-PCT% | Prints base64 encoding of the weekly percentage graph |
| %INT-WEEKLY-PPCT% | Prints base64 encoding of the weekly peak percentage graph |
| %INT-WEEKLY-PKTS% | Prints base64 encoding of the weekly packets graph |
| %INT-WEEKLY-BCSTS% | Prints base64 encoding of the weekly broadcasts graph |
| %INT-WEEKLY-ERRORS% | Prints base64 encoding of the weekly errors graph |
| %INT-MONTHLY-BPS% | Prints base64 encoding of the monthly bits per second graph |
| %INT-MONTHLY-PCT% | Prints base64 encoding of the monthly percentage graph |
| %INT-MONTHLY-PPCT% | Prints base64 encoding of the monthly peak percentage graph |
| %INT-MONTHLY-PKTS% | Prints base64 encoding of the monthly packets graph |
| %INT-MONTHLY-BCSTS% | Prints base64 encoding of the monthly broadcasts graph |
| %INT-MONTHLY-ERRORS% | Prints base64 encoding of the monthly errors graph |
| %INT-YEARLY-BPS% | Prints base64 encoding of the yearly bits per second graph |
| %INT-YEARLY-PCT% | Prints base64 encoding of the yearly percentage graph |
| %INT-YEARLY-PPCT% | Prints base64 encoding of the yearly peak percentage graph |
| %INT-YEARLY-PKTS% | Prints base64 encoding of the yearly packets graph |
| %INT-YEARLY-BCSTS% | Prints base64 encoding of the yearly broadcasts graph |
| %INT-YEARLY-ERRORS% | Prints base64 encoding of the yearly errors graph |

# Establishing Device Parent-Child Relationships

Parent-child relationships can be established so alerts for subordinate devices are not received when the parent device is unresponsive.

This can reduce and/or eliminate the large number of device outage alerts that are received when one device goes down, permitting you to focus your energies on responding to the one device that did fail.

Relationships are established via the ParentList.cfg file. Edit this file with a text editor like Notepad and enter your devices. Each “Child Device” should have one or more “Parent Device” defined.

```
;CHILD DEVICE     PARENT DEVICE
;--------------   ----------------------
192.168.1.56      192.168.1.12
192.168.1.12      192.168.1.1
192.168.1.12      192.168.1.2
```

In the above example, if 192.168.1.12 goes down, the child device 192.168.1.56 will not generate an alert if it is unreachable.

In the above example, if 192.168.1.1 goes down, the child device 192.168.1.12 will still generate an alert because another parent is defined as a means of reaching it. If both 192.168.1.1 and 192.168.1.2 are down, then no alert will be generated for 192.168.1.12.

After saving this file, the service should be stopped and re-started to have it take effect.

# Troubleshooting

*There are no devices listed on the web page*

The quick config will attempt to locate any devices that are configured to respond to SNMP.  You should check to make sure that SNMP is enabled on your network devices, and the device will respond to SNMP queries from the PathSolutions' Network Monitor computer.

*Nothing happens when the service starts, or the service fails to start*

Check the Windows Event Application log to see what is the problem.  Detailed error descriptions have been created to help you determine what the program needs to be able to operate correctly.

*PathSolutions' Network Monitor does not check all of my interfaces*

If you have more interfaces on your network than you possess license keys, then PathSolutions' Network Monitor adds a notice at the bottom of all web pages informing you that there are not enough licenses to monitor all of your interfaces.

# Frequently Asked Questions

*I want to customize the Network Weather Report emails that are sent. How do I do this?*

If you want to modify the Network Weather Report emails that are sent, modify the "WeatherMail.txt" file in the directory where you installed the program.

*How do you clear out the utilization statistics?*

PathSolutions' Network Monitor saves statistics in files in the "Data" directory where you installed the program. Each filename corresponds to a device on your network. You should stop the PathSolutions' Network Monitor service before deleting files.

*How many interfaces can I monitor with PathSolutions' Network Monitor?*

The collection engine at the core of PathSolutions' Network Monitor has been tested to be able to monitor networks with more than 30,000 interfaces within a 5-minute polling period. Make sure you have adequate RAM for the service if you plan on monitoring a lot of interfaces.

*Is PathSolutions' Network Monitor safe to use on the Internet?*

PathSolutions' Network Monitor has been tested for buffer overflow errors from browsers to make sure that it is safe to use on Intranets, Extranets, and the Internet. If you intend to use the product over the Internet, care should be taken to limit access to only IP addresses that should be able to access the PathSolutions' Network Monitor machine, and not permit general access. You should enable authentication and require passwords to be used to access the system.

**Note:** The PathSolutions' Network Monitor passwords are sent in Base64 encoding. This provides simple encryption of passwords and accounts, and should only be used to deter casual hackers. In general, a VPN should be employed to provide security between a computer on the Internet and the PathSolutions' Network Monitor server. The PathSolutions' Network Monitor accounts should be used as a method of preventing internal users from accessing network information.

*Why are the transmitted and received information reversed?*

When you view statistics, they should be viewed from the switch interface's perspective. If your backup server is receiving lots of information at 2:00am, the switch interface that connects to the backup server would be transmitting a lot of information to the backup server.

*How do I assign descriptive names to interfaces?*

If your switch does not allow you to assign names to each interface, PathSolutions' Network Monitor can allow you to assign names to each interface. Edit the IntDescription.cfg file in the directory where you installed the program.

# Appendix A: Error Descriptions

## *Alignment Errors*

*Rare event*

*Official definition*: A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions are obtained, according to the conventions of IEEE 802.3 Layer Management, are counted exclusively according to the error status presented to the LLC.

*Basic definition:* All frames on the segment should contain a number of bits that are divisible by eight (to create bytes). If a frame arrives on an interface that includes some spare bits left over, the interface does not know what to do with the spare bits. Example: If a received frame has 1605 bits, the receiving interface will count 200 bytes and will have 5 bits left over. The Ethernet interface does not know what to do with the remaining bits. It will discard the bits and increment the Alignment Error count. Because of these remaining bits, it is more likely that the CRC check will fail (causing FCS Errors to increment) as well.

**What you should do to fix this problem:**

*Cause 1:* If you have a switch port configured for full-duplex, and the workstation is configured for half-duplex, (or vice-versa) the network connection will still pass traffic, but the full-duplex side of the network will report Alignment Errors (it cannot report any collisions because it cannot detect collisions on a full-duplex link). The half-duplex side of the network will report collisions correctly, and will not detect any abnormalities. Check to see if there is a duplex mismatch on this interface.

*Cause 2:* Occasionally, a collision can create an alignment error. If you have a segment with lots of collisions, and you see occasional alignment errors, you should solve the collision problem and then note if the alignment error problem also goes away. Implement full-duplex to solve the collision and the alignment problem.

*Cause 3:* Sometimes alignment errors will increment when there is induced noise on the physical cable. Perform a cable test. Check the environment for electrical changes (industrial electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from electro-magnetic interference.

*Cause 4:* If you have alignment errors that occur without collisions, it usually means that you have a bad or corrupted software driver on a machine on that segment. Check to see what new machines have been added to that segment, or new network cards and/or drivers.

## *Carrier Sense Errors*

*Rare event*

*Official definition:* The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

*Basic definition:* Carrier Sense Errors occur when an interface attempts to transmit a frame, but no carrier is detected, and the frame cannot be transmitted.

**What you should do to fix this problem:**

*Cause 1:* Carrier Sense Errors can occur when there is an intermittent network cabling problem. Check for cable breaks that may cause occasional outages. Use a cable tester to insure that the physical cabling is good.

*Cause 2:* Carrier Sense Errors can occur when the device connected to the interface has a failing network interface card (NIC). The network card connected to this interface should be replaced.

## Deferred Transmissions

*Common event*

*Official definition:* A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.

*Basic definition:* If an interface needs to transmit a frame, but the network is busy, it increments Deferred Transmissions. Transmissions that are deferred are buffered up and sent at a later time when the network is available again.

**What you should do to fix this problem:**

*Cause 1:* Deferred Transmissions can be deferred because of non-collision media access problems. For example: If the network is constantly busy (and a network card cannot get a word in edgewise), there is a media access problem (the NIC cannot get control of the network). This kind of deferred transmission is usually associated with Single or Multiple Collision Frames. Implementing a full-duplex connection can solve this problem.

*Cause 2:* Deferred Transmissions can be created on a switch or bridge that is forwarding packets to a destination machine that is currently using its network segment to transmit. This can usually be solved by implementing a full-duplex connection (if possible) on the segment.

## Excessive Collisions

*Rare event*

*Official definition*: A count of frames for which transmission on a particular interface fails due to excessive collisions.

*Basic definition:* If there are too many collisions (beyond Multiple Collision Frames), the transmission will fail.

**What you should do to fix this problem:**

*Cause 1:* A faulty NIC can cause Excessive Collisions. Check the network cards on the segment to insure that they are functioning correctly.

*Cause 2*: A failed transceiver can cause Excessive Collisions. Check the transceivers on the segment to insure that they are functioning correctly.

*Cause 3:* Improper network wiring (wrong pairs, split pairs, crossed pairs) can cause Excessive Collisions. Use a cable tester to insure that wiring is good.

*Cause 4:* A network segment with extremely high utilization and high collision rates can cause Excessive Collisions. If utilization is high, attempt to implement full-duplex to solve this problem.

## FCS Errors

*Rare event*

*Official definition*: A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS (Frame Check Sequence) check. The count represented by an instance of this object is incremented when the FrameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions are obtained, according to the conventions of IEEE 802.3 Layer Management, are counted exclusively according to the error status presented to the LLC.

*Basic definition:* An FCS error is a legal sized frame with a bad frame check sequence (CRC error). An FCS error can be caused by a duplex mismatch, faulty NIC or driver, cabling, hub, or induced noise.

**What you should do to fix this problem:**

*Cause 1:* FCS errors can be caused by a duplex mismatch on a link. Check to make sure that both interfaces on this link have the same duplex setting.

*Cause 2:* Sometimes FCS errors will increment when there is induced noise on the physical cable. Perform a cable test. Check the environment for electrical changes (industrial electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from electro-magnetic interference.

*Cause 3:* If you notice that FCS Errors increases, and Alignment Errors increase, attempt to solve the alignment error problem first. Alignment errors can cause FCS errors.

*Cause 4:* If you see FCS errors increase, check the network cards and transceivers on that segment. A failing network card or transceiver may transmit a proper frame, but garble the data inside, causing a FCS error to be detected by listening machines.

*Cause 5:* Check network driver software on that segment. If a network driver is bad or corrupt, it may calculate the CRC incorrectly, and cause listening machines to detect an FCS Error.

*Cause 6*: If you have an Ethernet cable that is too short (less than 0.5meters), FCS errors can be generated.

*Cause 7*: If you have an Ethernet cable that is too long (more than 100meters), FCS errors can be generated.

*Cause 8*: If you are using 10Base-2, and have poor termination, or poor grounding, FCS errors can be generated.

## Frame Too Longs

*Rare event*

*Official definition:* If a frame is detected on an interface that is too long (as defined by ifMTU), this counter will increment.

*Basic definition:* Frame Too Longs occur when an interface has received a frame that is longer (in bytes) than the maximum transmission unit (MTU) of the interface.

**What you should do to fix this problem:**

*Cause 1:* Switches that use VLAN (Virtual LAN) tagging of frames can cause FrameTooLongs. To solve this specific problem, upgrade the device reporting the FrameTooLong error to support VLANs, or turn off VLAN tagging on neighboring switches.

*Cause 2:* Faulty NIC cards can cause FrameTooLongs. Check NIC cards on the segment to insure that they are running correctly.

*Cause 3:* Cabling or grounding problems can cause FrameTooLongs. Use a network cable tester to insure that the cabling is not too long, or out of specification for the technology you are using.

*Cause 4:* Software drivers that do not respect the correct MTU (Maximum Transmission Unit) of the medium can cause FrameTooLongs. Check network drivers to make sure they are functioning properly.

## *Inbound Discards*

*Rare event*

*Official definition:* The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

*Basic definition:* If too many packets are received, and the protocol stack does not have enough resources to properly handle the packet, it may be discarded.

**What you should do to fix this problem:**

*Cause 1:* Insufficient memory allocated for inbound packet buffers. Research how to increase the inbound packet buffers on the interface.  This may be modified in the device's configuration.

*Cause 2:* The CPU on the device may not be fast enough to process all of the inbound packets. Employing a faster CPU may remedy this problem.

## *Inbound Errors*

*Rare event*

*Official definition:* The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

*Basic definition:* These packets contained one or more various data-link layer errors, and were thus discarded before being passed to the network layer. The root cause of these errors are undefined. In order to more accurately research these types of errors, you should deploy a packet analyzer in front of this interface to track the specific errors that occur, as the device is not capable of tracking any additional information relating to these errors.  If this interface provides Ethernet specific errors, these errors may be detailed in that section.

**What you should do to fix this problem:**

*Cause 1:* There are various sources of this type of error.  The interface does not possess enough information as to the exact cause of this error.  Deploy a packet analyzer in front of this interface to inspect the exact type of error that is occurring.

## *Inbound Unknown Protocols*

*Common event*

*Official definition:* The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

*Basic definition:* If the physical and data-link layer do their job successfully and deliver a frame to the correct MAC address, it is assumed that the requested protocol will be available on the machine. If the protocol is not available, the frame is discarded. If your machine receives an AppleTalk packet, but your machine is not running AppleTalk, it will discard the packet and increment this counter.

**What you should do to fix this problem:**

*Cause 1:* Broadcasts can cause inbound unknown protocol errors. If you have a Novell server on the segment, it will send out periodic IPX broadcasts that some devices will not understand (because they do not have the IPX protocol loaded in their network stack). This is a normal event. To attempt to reduce this, work on reducing the number of different protocols that exist on your network, or install additional protocols on your machines to be able to communicate with additional clients.

*Cause 2:* Inbound unknown protocols can be caused by mis-configurations of other machines. Check the configurations of other machines on the network to try to determine why this machine is receiving an unknown protocol. If inbound unknown protocols error is incrementing rapidly, attach a network analyzer and look at the protocols that are being sent to this machine, and their source.

## *Outbound Discards*

*Rare event*

*Official definition:* The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

*Basic definition:* If too many packets are queued to be transmitted, and the network interface is not fast enough to transmit all of the packets, it may be discarded.

**What you should do to fix this problem:**

*Cause 1*: Insufficient memory allocated for outbound packet buffers. This may be modified in the device's configuration.

*Cause 2:* The network interface may not be fast enough to process all of the outbound packets. Employing a faster speed interface may remedy this problem.

## Outbound Errors

*Rare event*

*Official definition:* The number of outbound packets that could not be transmitted because of errors.

*Basic definition:* These packets could not be transmitted due to one or more various data-link layer errors. The root cause of these errors are undefined. In order to more accurately research these types of errors, you should deploy a packet analyzer in front of this interface to track the specific errors that occur, as the device is not capable of tracking any additional information relating to these errors. If this interface provides Ethernet specific errors, these errors may be detailed in that section.

**What you should do to fix this problem:**

*Cause 1:* There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Deploy a packet analyzer in front of this interface to inspect the exact type of error that is occurring.

## Outbound Queue Length

*Common event*

The length of the output packet queue (in packets). This number should return to zero in a short amount of time. If it ends up being any non-zero value for any length of time, you should consider upgrading the interface to a faster technology, or full duplex (if not already enabled).

## Internal Mac Transmit Errors

*Rare event*

*Official definition*: A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

*Basic definition:* If a transmission error occurs, but is not a late collision, excessive collision, or carrier sense error, it is counted as an error here. NIC vendors may identify these kinds of errors specifically. Check with the device's manufacturer to determine their interpretation of InternalMacTransmitErrors.

**What you should do to fix this problem:**

*Cause 1:* A faulty network transmitter can cause InternalMACTransmitErrors. Check the device to insure that it is functioning correctly.

*Cause 2:* Check with the device's manufacturer to determine what their interpretation is of InternalMACTransmitErrors.

## Late Collisions

*Rare event*

*Official definition*: The number of times that a collision is detected on a particular interface later than 512 bit-times (64 bytes) into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10-megabit per second system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.

*Basic definition:* Collisions should be detected within the first 64 bytes of a transmission. If an interface transmits a frame and detects a collision before sending out the first 64 bytes, it declares it to be a "normal collision" and increments Single Collision Frames (or Multiple Collision Frames if more collisions follow). If an interface transmits a frame and detects a collision after sending out the first 64 bytes, it declares it to be a Late Collision. If a machine detects a Late Collision, it will treat the collision like any other collision (send a jam signal, and wait a random amount of time before attempting to retransmit). The other sending machine may or may NOT have detected the collision because it was so late in the transmission. The other sending machine may detect the collision AFTER it is done sending its frame, and will believe that its frame was sent out successfully.

**What you should do to fix this problem:**

*Cause 1:* A duplex mismatch can cause Late Collisions. Check to make sure that the duplex setting on both interfaces are set to use the same duplex.

*Cause 2*: A faulty NIC card on the segment can cause Late Collisions.

*Cause 3:* Late Collisions can be caused by a network that is physically too long. A network is physically too long if the end-to-end signal propagation time is greater than the time it takes to transmit a legal sized frame (about 57.6 microseconds). Check to make sure you do not have more than five hubs connected end-to-end on a segment, counting transceivers and media-converters as a two-port hub. Also check individual NIC cards for transmission problems.

*Cause 4*: If you have a switch on the network that is configured for "low-latency" forwarding (anything except "store and forward"), it may be causing the Late Collisions. Low latency forwarding ends up having the switch act like a very slow hub. It reduces traffic like a switch, but does not insure that frames reach the destination successfully. The frame "worms" its way through multiple switches, slowing down at each switch. If there is a collision on the end segment, the frame gets dropped by the switch, and the transmitting workstation does not detect that the frame was dropped. To fix this, do not use "low-latency" forwarding features on switches that are hooked up to other switches with "low-latency" forwarding features. Configure the switches to use "store and forward" forwarding methodology.

## *MAC Receive Errors*

*Rare event*

*Official definition*: A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

*Basic definition:* This is the number of frames that could not be transmitted due to an unknown problem. This unknown problem is not related to collisions or carrier sense errors. The device manufacturer's documentation may provide additional information on locating the source of these errors.

**What you should do to fix this problem:**

*Cause 1:* There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Contact the device manufacturer to determine how they define the MacReceiveError and how to fix this problem.

## Multiple Collision Frames

*Rare event*

*Official definition:* A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts or ifOutNUcastPkts object and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.

*Basic definition:* If a network interface attempts to transmit a frame, and detects a collision, it will attempt to re-transmit the frame after the collision. If the retransmission also causes a collision, then Multiple Collision Frames is incremented.

**What you should do to fix this problem:**

*Cause 1*: A faulty NIC or transceiver can cause Multiple Collision Frames. Check the network cards and transceivers on the segment for failures.

*Cause 2:* An extremely overloaded network can cause Multiple Collision Frames (average utilization should be less than 40%).

*Cause 3:* If you are using 10Base-2, and have poor termination, or poor grounding, Multiple Collision Frames can be generated.

*Cause 4*: If you have a bad hardware configuration (like creating an Ethernet ring), Multiple Collision Frames can be generated.

## Single Collision Frames

*Common event*

*Official definition*: A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts or ifOutNUcastPkts object and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object.

*Basic definition:* If a network interface attempts to transmit a frame, and detects a collision, it will attempt to re-transmit the frame after the collision. If the retransmission was successful, then the event is logged as a single collision frame.

**What you should do to fix this problem:**

*Cause 1:* Single Collision Frames can be caused by multiple machines wanting to transmit at the same time. This is a normal occurrence on Ethernet.

*Cause 2:* If Single Collision Frames increases dramatically, this could indicate that the segment is becoming overloaded (too many machines on the segment, or too many heavy talkers on the segment). As the segment continues to become overloaded, Single Collision Frame count may decrease, as Multiple Collision Frames increases. Converting the segment to a switched environment may solve this problem. Another possible solution is to reduce the number of machines on this segment, or install a bridge to segregate the segment into two halves.

*Cause 3:* Single Collision Frames can be caused by poor wiring or induced noise. Use a cable tester to insure that the physical cable is good.

*Cause 4:* Single Collision Frames can be caused by a bad network interface card, or failing transceiver. Check to make sure the network cards and transceivers on the segment are functioning correctly.

## *SQE Test Errors*

*Rare event*

*Official definition*: A count of times that the SQE TEST ERROR message is generated by the PLS sub layer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.

*Basic definition:* SQE stands for "Signal Quality Error", and may also be referred to as the Ethernet "heartbeat". With early Ethernet cards that required transceivers, the transceiver would send a "Signal Quality Error" back to the Ethernet card after each frame was transmitted to insure that the collision detection circuitry was working. With modern network cards, this SQE test can cause network cards to believe that an actual collision occurred, and a collision is sent out on the network when a SQE test is detected. This can seriously degrade network performance, as each frame successfully transmitted on the network is followed by a collision caused by the SQE test.

**What you should do to fix this problem:**

*Cause 1:* SQE Test Errors can be caused by a transceiver that have the "SQE test" dip switch turned on (it should be turned off). Check the switch settings on all transceivers on the segment.

*Cause 2:* SQE Test errors can be caused by broken transceivers. Check for failed transceivers on the segment.

# Appendix B: SMTP E-mail Forwarding

Most companies use SMTP gateways to allow email from the Internet to reach internal users.

This gateway is typically set up to receive emails that are destined for mailboxes on the company's system.

If you configure PathSolutions’ Network Monitor to use your company's SMTP mail gateway, the gateway should accept SMTP messages destined for internal users, but should not accept SMTP messages destined for outside addresses.

For example:

If you configured PathSolutions’ Network Monitor to use "mail.company.com " as the SMTP mail gateway, and set the "Globally send to" field to jdoe@company.com, the mail gateway would accept emails sent to this address because it exists on the same domain.  If the "Globally send to" field was set to jdoe@outside.com, then the gateway would refuse this request because most mail systems do not allow relaying of messages from one to another.

This is done by mail administrators to prevent abuse by spammers.  Email spammers will search the Internet for anonymous SMTP mail forwarders that they can use to send their emails out.

This allows them to send untraceable emails.

To allow PathSolutions’ Network Monitor to send emails to different domains, there are a number of solutions:

- Ask your ISP if they have an SMTP relay server that can be used by your machines.  They may have a server set up that will relay only your messages.  In this case, you would configure PathSolutions’ Network Monitor to use their SMTP relay server.
- Ask your email administrator to configure the SMTP gateway to allow relaying from the server that PathSolutions’ Network Monitor is installed on.

Create a mail alias on your email system (for example: jdoe@company.com) that forwards to an outside address (jdoe@outside.com).

A free SMTP mail relay agent (SMTP forwarder) is included with Windows 2000 server's IIS implementation.

# Appendix C: Configuring SNMP on Devices

A variety of device configuration instructions are available on the PathSolutions website:

http://www.PathSolutions.com/SwitchConfig.html

Other device manufacturer instructions should be available through the device manufacturer's website.

# Appendix D: Changing Interface Names and Speed

Many device manufacturers do not allow interface names to be changed to a descriptive name to help document the network. In this case, PathSolutions' Network Monitor can be configured to ignore the interface description in the device and use information from a config file.

Use a text editor such as Notepad to open the IntDescription.cfg file in the directory where PathSolutions' Network Monitor is installed.

You should see a document with a description of how to enter the switch interfaces and descriptions.

The file is composed of a number of columns or fields; each separated by one or more <TAB> characters.

**Note:** The fields in the configuration file need to be separated by at least one <TAB> character, not spaces.

Here is an example of a configuration file:

```
;This line is commented out
;
;IPAddress              Interface   Speed       Description
;-----------            ---------   ------      ---------------
192.168.1.10            1           /           Internet connection
calvin.company.com      156         1544000     FE0/6
192.168.2.2             3           /           Connection to New York
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

## *IP Addresses*

The IP address of the switch must be entered to identify the device. If the config file has a DNS name, then that identical name should be used here to identify the same device.

## *Interface #*

The interface number (as listed in the web reports) should be entered here. If you are unsure of the exact number to use, reference your device manufacturer's documentation to map the SNMP interface numbers to the physical addresses on the device. Then use your network documentation to determine what device is physically connected to the interface on the device.

## *Speed*

If you desire to override the reported interface speed, you can enter the speed in bits per second here. For example: You may want to change the reported interface speed of a router interface connected to the internet from 100 Mbps to the actual capacity of the link it is connected to (1.544 Mbps for a T1 connection). This will help to determine when the link utilization is exceeded. If you do not want to override this information, enter a slash "/" to skip this field.

## *Description*

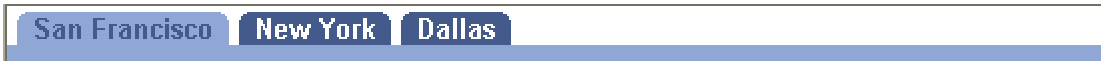
Enter the description here. The description field should not contain a semicolon character.

**Note:** The service must be stopped and re-started after this file is modified in order to have the descriptions take effect.

# Appendix E: Configuring Multiple Locations

If you have multiple PathSolutions’ Network Monitor implementations, PathSolutions’ Network Monitor can be configured to make it easy to navigate between the sites.

Each web page will display tabs across the top of the web page indicating the site that you are viewing:



To configure multiple sites, use a text editor like Notepad to open the MultiSite.cfg file in the directory where you installed the program.

You should see a document with a description of how to enter the site names and URLs.

The file is composed of a number of columns or fields; each separated by one or more <TAB> characters.

**Note:** The fields in the configuration file need to be separated by at least one <TAB> character, not spaces.

Here is an example of a configuration file:

```
;Example for the San Francisco server:
;
;Current   Site Name        URL
;-------   --------------   -------------------------------------------
YES        San Francisco    http://sfserver.company.com:8084
NO         New York         http://nyserver.company.com:8084
NO         Chicago          http://chicago.company.com:8084

;Example for the New York server:
;
;Current   Site Name        URL
;-------   --------------   -------------------------------------------
NO         San Francisco    http://sfserver.company.com:8084
YES        New York         http://nyserver.company.com:8084
NO         Chicago          http://chicago.company.com:8084
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

### *Current*

This field identifies which site should be highlighted.  Only one site should be highlighted per config file. The config file on the New York server should have "Yes" for the New York entry.

### *Site Name*

This is the name that is displayed in the tab.

### *URL*

Enter the server's full URL and port here. This will allow linking from the other PathSolutions’ Network Monitor servers.

**Note:** The service must be stopped and re-started after this file is modified in order to have the links work.

The order of the listed sites should be similar for each deployed site so the tabs will display correctly for each site.

# Appendix F: Entering Custom OIDs to be Monitored

PathSolutions' Network Monitor can monitor custom OIDs such as CPU utilization, memory usage, and temperature if the device provides this information via SNMP.

The configuration file OIDEntry.cfg is used to configure custom OID monitoring.  This file is found in the directory where the program was installed.

Edit this file with a text editor like Notepad.

You will need to enter the following information to be able to set up monitoring of a custom OID:

- IP address of the device ("10.0.1.16")
- Interface to be associated with or "/" if you want to associate it with the device instead of an interface ("23")
- Unique filename for storing the data collected for this OID ("FRAMERELAY")
- Description of this graph ("Frame Relay FECN & BECN")
- Y Axis description ("Packets")
- OID #1 Description ("FECN")
- OID #1 ("GAUGE:1.3.6.1.2.1.2.2.1.17.1")
- OID #2 Description ("BECN")
- OID #2 ("GAUGE:1.3.6.1.2.2.1.18.1")

**Note:** When entering the OID value, put the prefix "GAUGE:", "COUNTER:", or "COUNTER:8" in front of the OID to identify how the OID should be tracked.

**Note:** After saving this file, you will have to stop and restart the PathSolutions' Network Monitor service for the changes to take effect.

# Appendix G: Configuring Additional OUIs for Phones Tab

A number of OUIs (Organizationally Unique Identifiers) for various VoIP equipment manufacturers have already been added to the OUIFilter.cfg file. This file can be edited with a text editor (like Notepad) to add additional OUIs.

An OUI is the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.

The OUIFilter.cfg file will require you to enter the OUI (each byte separated by a period "."), then a tab, then the name of the manufacturer.

**Note:** After saving this file, you will have to stop and restart the PathSolutions' Network Monitor service for the changes to take effect.

# Appendix H: Changing the Map File

The map file can be changed to any custom JPG file desired.

PathSolutions' Network Monitor uses the map file:

```
      C:\Program Files\PathSolutions\PathSolutions' Network
Monitor\Graphics\map.jpg
```

Note: It's advised to rename the existing map file instead of overwriting this file so it can be used in the future if desired. Otherwise you will need to uninstall and reinstall to recover the map file.

The map can be centered on the screen by modifying the following registry entries:

```
HKEY_LOCAL_MACHINE/Software/Netlatency/PathSolutions' Network
Monitor/DestWebMapStartX
HKEY_LOCAL_MACHINE/Software/Netlatency/PathSolutions' Network
Monitor/DestWebMapStartY
```

This will set the starting X and Y coordinates for the upper left corner of the map file. If you want the map to initially display in the upper left corner, set both of these coordinates to 0 (zero).

After the map file has been replaced and the starting coordinates modified, stop and restart the PathSolutions PathSolutions' Network Monitor service to have the changes take effect.

# Glossary

*IETF* - This acronym stands for the Internet Engineering Task Force, and is the governing body for all standards that relate to Internet and associated communications technologies. Website: www.ietf.org

*MAC* – Media Access Control: This is a unique address that is used by Ethernet adapters to transmit and receive frames on the network. They are only used for conveying layer 2 frames between nodes on a LAN.

*MIME* - Multi-Purpose Internet Mail Extensions: This is an email standard that defines how different content is handled inside email messages. This allows graphics, audio, HTML text, formatted text, and video to be displayed correctly inside email messages. MIME is defined by the IETF's RFC1521 document, and is available on the IETF's website: http://www.ietf.org/rfc/rfc1521.txt?number=1521

*Network Weather Report* - System Monitor can email network reports to you on a daily basis. The network Weather Report helps to keep you informed of the overall health of your network.

*OSI* - Open Systems Interconnect: This is a standard description or "reference model" for how services are provided on a network.

*OUI* – Organizationally Unique Identifer: This is the identification of the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.

*SNMP read-only community string* - This is an SNMP password with the rights to be able to read statistical information from a device.

*SNMP* - Simple Network Management Protocol. This protocol allows network management software (like System Monitor) to communicate with network devices to read statistical information.

*SMTP email address* -- This is a standard Internet email address. For example: jdoe@company.com.

*SMTP* -- Simple Mail Transport Protocol. This protocol allows email clients and servers to communicate over the Internet.

*WAP* -- Wireless Application Protocol: This protocol uses HTTP to transfer WML pages that are suitable for display on wireless devices like cell phones or PDAs.