User Guide

ManageEngine® OpUtils 5

http://www.oputils.com

Table Of Contents

Introduction

Welcome to ManageEngine OpUtils

Why ManageEngine OpUtils ?

Businesses increasingly rely on their networks and resources for basic operations. ManageEngine OpUtils with its suite of 40+ tools, addresses the need of Network Engineers for troubleshooting connectivity issues, and on-demand monitoring of the network.

What does ManageEngine OpUtils consist of ?

ManageEngine OpUtils comes with a set of 34 tools and intuitive GUI to address the day-to-day needs of Network administrators and System administrators.

The toolkit can be used for

- Troubleshooting connectivity issues in a LAN environment.
- Monitoring the performance, bandwidth and traffic statistics of routers, switches and other networking resources.
- Providing information on IP Addresses, MAC Addresses and DNS names.
- Tracking Desktop information such as system configuration, resource usage and software listing.
- Monitoring Cisco devices and maintaining the devices in good condition
- Browsing MIB's and viewing configured Traps.

The tools available in the ManageEngine OpUtils toolkit are

Featured Tools

1. **Switch Port Mapper** - Tool to check and display the devices connected to the ports of a Switch.
2. **Rogue Detection** - Provides a list of rogue devices detected in the network.
3. **MAC IP List** - To get the list of MAC and IP Addresses in the network.
4. **IP Address Manager** - Tool to identify whether an IP Address is currently available or not.

Diagnostic Tools

1. **Ping Tool** - Tool to ping a node to check its connectivity status in the network.
2. Ping Scan - Tool to scan a range of IP addresses to check if they are alive and reachable in the network.
3. SNMP Ping - Tool to ping a node, for checking if the node is SNMP enabled.
4. **SNMP Scan** - Tool to scan a range of SNMP-enabled IP addresses to check if they are alive and reachable.
5. **Proxy Ping** - Tool to do a ping test from a remote router to another remote device.

6. **Trace Route** - Tool to record the route (the specific gateway computers at each hop) through the network from Host to the target Destination.

Address Monitoring Tools

1. **DNS Resolver** - A data query tool to translate host name into IP Address and vice versa.
2. **DNS Scan** - Tool to audit the given range of IPs for Reverse Lookup.
3. **MAC Address Resolver** - Tool to resolve IP Address or Host Name to MAC Address and vice versa.
4. **MAC Address Scan** - Tool to discover the physical address of a given range of devices and map them with the corresponding IP addresses.
5. **DHCP Scope Monitor** - Tool to find the used and available IP addresses in the scopes of the DHCP Server.

Network Monitoring Tools

1. **Bandwidth Monitor** - Tool to monitor the average BPS and percentage utilization of all the Interfaces in the specified device.
2. **Network Monitor** - Utility to continuously monitor the response time of multiple devices and generate e-mail action based on severity.
3. **Wake-On-LAN** - Tool to remotely power on a PC.
4. **Port Scanner** - Tool to scan the ports of a system.
5. **System Details Update** - Tool to view and update the details, such as Name, Location, and Contact details.
6. **System Explorer** - Tool to get the complete details of a server like system snapshot, disk space details, CPU usage, running processes, and installed software.
7. **TCP Reset** - Tool to find and reset the list of TCP connections established with the switches, routers, etc., in the network.

CISCO Tools

1. **Config file Manager** - Config File Manager downloads/uploads the StartUp and/or the Running config files from the given CISCO Router and displays them. It also shows the colored difference between the two files.
2. **TFTP Server** - Tool to view the Config Files available in the TFTP Root. You can also change the TFTP Root and edit/upload config files from here.
3. **Device Scan** - Utility to scan a subnet or a range of IP Addresses to collect the details of the Cisco Devices in the scanned range.
4. **Device Explorer** - Utility to scan a Cisco device to get the details like device snapshot, chassis details, IOS details, flash memory details, interfaces, IP routes, CPU and memory utilization, and access lists.

SNMP Tools

1. **MIB Viewer** - Utility to view the details of a MIB node. It accepts the node name or the OID as input and provides the complete information on the MIB node including MIB name, parent node name, OID, OID type, status, syntax, access, definition, and the next node. It also provides some general information about the

MIB and also provides the defined attributes, total number of nodes, defined TCs, and the defined traps.

2. **SNMP Graph** - Tool to gather data in real time and to draw graph for any SNMP device using the available data.
3. **Trap Receiver** - Tool to view the configured traps.
4. **SNMP Walker** - Tool to retrieve information for a set of OIDs in a MIB.
5. **SNMP Table** - Tool to retrieve the data for the specified Table OID from the device.
6. **MIB Browser** - Tool to load, browse, search, and walk through SNMP MIBs, and perform certain basic SNMP functions.
7. **Community Checker** - Tool to detect the read and write community strings of the devices in the network.

Custom SNMP Tools

1. **Custom Tabular Tool** - Helps to create a tabular representation of the custom MIB nodes of your choice.
2. **Custom Graph Tool** - Helps to create a Graphical representation of the custom MIB nodes of your choice.

Document Organization

The AdventNet ManageEngine OpUtils User Guide is divided into the following sections:

Technology Overview

This section provides an overview of SNMP, ICMP and CLI basics.

Getting Started

This section outlines the basic requirements to work with ManageEngine OpUtils. Information related to the system requirements, installing the software, other prerequisites, and working with the OpUtils are discussed in detail.

Configuring ManageEngine OpUtils

This section discusses how to configure common protocols, and outlines the general features of the tools.

Featured Tools

Switch Port Mapper : Utility to check and display the device connected to the ports of a remotely located Switch in real time network. The tool is useful for system and network engineers to gain visibility into the IP, MAC, status and availability of ports. Since this is a real-time discovery you can also view the operational status and port speed of each port. This tool maps switch ports to the devices connected to them.

IP Address Manager : Utility to check for used, available and transient IP's in a given subnet or network. The tool helps manage the IP addresses in a static DNS environment, using pre-defined user policy. The tool scans a subnet and provides the availability status of IP addresses in that subnet. One can check whether a particular IP is reserved or available.

Rogue Detection : Provides a list of rogue devices detected in the network.

MAC IP List : Provides a list of MAC and IP Addresses discovered from the routers and scanned IP ranges/subnets.

Tool Categories

Diagnostic Tools	This section, provides detailed explanation of the tools that are categorized under the Diagnostic Tools category. The tools include **Ping, Ping Scan, SNMP Ping, SNMP Scan, Proxy Ping,** and **Trace Route**.
Address Monitoring Tools	This section, provides a detailed description of the tools that are categorized under the Address Monitoring Utilities category. The tools include **DNS Resolver, DNS Scan, MAC Address Resolver, MAC Address Scan,** and **DHCP Scope Monitor.**

Network Monitoring Tools	This section, provides detailed explanation about the tools that are categorized under the Network Monitoring Utilities. The tools include, **Bandwidth Monitor, Network Monitor, Wake-On-LAN, System Explorer, System Details Update, TCP Reset,** and **Port Scanner.**
CISCO Tools	This section, provides detailed explanation about the tools that are categorized under the CISCO Utilities. The tools include **Config File Manager, TFTP Server, Device Scan,** and **Device Explorer.**
SNMP Tools	This section, provides detailed explanation about the tools that are categorized under SNMP Tools. The tools include **Trap Receiver, SNMP Walker, SNMP Table, SNMP Graph, MIB Browser, MIB Viewer,** and **Community Checker**.

Appendix

This section includes, Interpreting Error Messages, FAQ, Troubleshooting Tips, and Known Issues and Limitations of OpUtils.

Product Edition Matrix

OpUtils is available in three editions - **Free, Standard,** and **Professional** Edition. The OpUtils product matrix is given below.

Tools	Free Edition	Standard Edition	Professional Edition
Switch Port Mapper*	✗	✗	✓
IP Address Manager	✗	✗	✓
Rogue Detection	✗	✗	✓
MAC IP List	✗	✗	✓
Diagnostic			
Ping	✓	✓	✓
Ping Scan	✓	✓	✓
SNMP Ping	✓	✓	✓
SNMP Scan	✓	✓	✓
Proxy Ping	✓	✓	✓
Trace Route	✓	✓	✓
Address Monitoring			
DNS Resolver	✓	✓	✓
DNS Scan	✓	✓	✓
MAC Address Resolver	✓	✓	✓
MAC Address Scan	✓	✓	✓
Subnet List	✓	✓	✓
DHCP Scope Monitor	✗	✓	✓
Network Monitoring			
Bandwidth Monitor*	✗	✓	✓
Network Monitor*	✗	✓	✓
Wake-On-LAN	✗	✓	✓
Port Scanner	✗	✓	✓
System Details Update	✗	✓	✓
System Explorer	✗	✓	✓
TCP Reset	✓	✓	✓
Cisco Tools			
Config File Manager*	✗	✗	✓
TFTP Server	✗	✗	✓
Device Scan*	✗	✗	✓
Device Explorer	✗	✗	✓
SNMP Tools			
MIB Viewer	✓	✓	✓
SNMP Graph	✓	✓	✓
Trap Receiver*	✗	✓	✓
SNMP Walker	✗	✓	✓

Tools	Free Edition	Standard Edition	Professional Edition
SNMP Table	✗	✓	
MIB Browser	✗	✓	✓
Community Checker	✓	✓	✓
Custom Tools	✗	✗	✓

* - restricted access to these tools will be available in the Free Edition

Release Notes

Release Notes for 5.0

1. Wake on LAN tool enhanced to include multiple groups of devices that can be scheduled differently.
2. Important tools are moved to tabs for easy navigation
3. The left tree will be removed for better tool visibility
4. All the Server Monitoring tools and Cisco Tools are merged into one for ease of use.
5. Switch Port Mapper enhanced to include the ability to group switches.
6. Switch Port Mapper will list all the switch ports even if no matching port is found in the Bridge MIB.
7. Network Monitor tool enhanced to include email templates.
8. Ability to enable/disable a switch port included in Switch Port Mapper tool.
9. Ability to export switch inputs from the Add/Edit switch view has been added.
10. Support for mapping Alcatel switches using the Switch Port Mapper tool has been added.

Release Notes for 4.4

1. Rogue Detection tool enhanced to include views for Trusted and Rogue Devices.
2. Global Environment enhanced with the ability to add switches, gateway servers etc., in addition to the routers.
3. TFTP Server tool included.
4. Cisco Device Scanner tool added.
5. SNMP Table Tool included.
6. Alerts can now be notified by playing a sound.
7. Global Alerts provides an unified view of alerts generated by OpUtils.
8. Email Alert added for Rogue devices.
9. DHCP Scope Monitor tool enhanced to store details in the database with email alert options.
10. Auto-publishing of Switch Port Mapper results to a CSV format.

Release Notes for 4.0

1. Support for storing the configuration and monitored information in the database.
2. Five new tools added - DHCP Scope Monitor, Rogue Detection, TCP Reset, System Details Update, SNMP Community Checker, and Custom Tool.
3. Reports about your network infrastructure - Network Report, Inventory Report, IP Availability Report, Port Availability Report, MAC Address Report, Rogue Devices, and SNMP Devices.
4. Enhanced Wake on LAN tool to broadcast the WOL packet in the subnet.
5. Config File Manager enhanced to include scheduled backup, compare config files between versions, and the ability to upload it to the device.
6. Trap Receiver tool enhanced to include the trap received time and the intelligence to refresh the page automatically when a trap is received.

Release Notes for 3.2.2

1. Issue in generating an alert when a device goes down, in Network Monitor tool is fixed.
2. Issue in adding a system in the Wake on LAN tool is fixed.
3. Issue in exporting the results of SNMP Walker tool is fixed.
4. Issue in receiving multi-varbind traps in Trap Receiver tool is fixed.

Release Notes for 3.2.1

1. Network Scan tool enhanced to scan up to ten subnets.
2. You can now select and scan individual switches from the Switch Port Mapper results.
3. Trap Receiver tool enhanced to provide the description of the Trap OIDs. The text equivalent of the enumerated integers and textual conventions will be shown along with the trap OID value.
4. Cisco Interfaces tool enhanced to include Interface Name.
5. Enhanced log messages for easy debugging.
6. Option to retrieve VLAN ID is added to fix the issue related to Switch Port Mapper when configured community string contains character '@'.
7. Issue related to performance of Switch Port Mapper tool when DNS Name is not able to resolve is fixed.
8. Issue in using NATIVE PING in non-English OS is fixed.

Release Notes for 3.2.0

1. Switch Port Mapper, IP Address Manager, and Wake on LAN tools enhanced to accept multiple inputs.
2. A new tool, Port Scanner, to scan the ports of a given range of IP Addresses has been added.
3. MAC Address Database provides the details if the IP Addresses, MAC Addresses, and DNS names of the devices in the network.
4. Bandwidth Monitor and Performance Monitor tools can now be configured to send e-mail notifications.
5. Multiple SNMP community strings can be specified as comma separated values.
6. Ability to zip and send the log files from the client.

Release Notes for 3.1.4

1. You can now send us your queries and feature requirements from the product by selecting the **OpUtils Support** tab.
2. Tools that uses SNMP to get the information was throwing an exception, which is now fixed.
3. Issue related to OpUtils icon in the Windows system tray has been fixed.

Release Notes for 3.1.3

1. Issue in applying timeout values from the ICMP settings is fixed.
2. When the response length exceeds the specified limit, the Switch Port Mapper shows "The Specified OID not implemented" error. This is now handled internally
3. In Switch Port Mapper tool, appropriate error messages will be displayed, when data could not be retrieved from the Bridge MIB.

Release Notes for 3.1.2

1. Issue in starting OpUtils when the previous instance was abruptly killed is fixed.
2. Algorithm for identifying a switch using the Switch Port Mapper tool is changed.
3. Issue in MIB Browser requests getting timed out in multiple client sessions is fixed.
4. Enhanced Network Scan tool to include more machine types, such as Intel 510T Switch, HP Switch, and so on.
5. Identifying MAC addresses from ARP cache for non-SNMP nodes is optimized.

Release Notes for 3.1.1

1. OpUtils can now be installed and run as a windows service.
2. Operations, such as starting OpUtils, stopping OpUtils, and so on, can be performed from the windows system tray icon
3. Starting the OpUtils server will automatically launch the client in the default browser.

Release Notes for 3.1.0

1. In IP Address Manager Tool, support for Class B network, which is now a subnet of Class C has been added.
2. Support for localization added. With this, OpUtils will now run on non-English operating systems, such as Japanese, Chinese, and so on.
3. Ability to add user-defined MIBs in MIB Module Viewer and MIB Browser Tools.
4. Optimized the performance by addressing the high CPU usage and memory related issues.

Contacting AdventNet

AdventNet Headquarters

Web site	www.adventnet.com
AdventNet Headquarters	AdventNet, Inc. 5200 Franklin Dr, Suite 115 Pleasanton, CA 94588 USA Phone: +1-925-924-950 E-mail: info@adventnet.com
AdventNet Development Center	AdventNet Development Centre (I) Private Limited 11 Sarathy Nagar, Vijayanagar, Velachery, Chennai 600 042 INDIA Phone: +91-44-22431115 (10 lines) Fax: +91-44-22435327 E-mail: info@adventnet.com

Sales

For purchasing ManageEngine OpUtils from any part of the world, you can fill out the Sales Request Form. A sales person will contact you shortly. You can also send us e-mail at sales@adventnet.com.

You can also call the AdventNet headquarters at the following numbers:
Phone: +1-925-924-9500
Fax: +1-925-924-9600 and request for Sales

Technical Support

One of the value propositions of AdventNet to its customers is excellent support. During the evaluation phase the support program is extended to users free of charge. Check the FAQ section - there is a possibility that your query might have been answered there. If not, please mail to support@oputils.com

When you encounter an issue or a problem, you can send us the details of the problem along with the support file. To create a support file, follow the steps given below:

1. Select **Settings --> General** from the client window.
2. Change the log level to **INFO** and save.
3. Perform the same steps as you did earlier.
4. Select the **OpUtils Support** tab from the client window.
5. Click the **Create Support File** link.

6. After the support file is created, save the file and attach it along with your mail and send it to support@oputils.com

Alternatively, select the **OpUtils Support** tab from the client window. It has the following options to reach us:

- Request Technical Support - Submit your technical queries online.
- Need Features? - Request for new features in OpUtils.
- Discussion Forum - Participate in a discussion with other OpUtils users.
- Contact Us - Speak to our technical team using the toll free number (1-888-720-9500)

Technology Overview

To get started with ManageEngine OpUtils it is essential to be familiar with basics of SNMP, ICMP and CLI. Read the following sections for more details. If you are familiar with the basics, you can skip this section.

- **SNMP Overview**
- **ICMP Overview**
- **CLI Overview**

SNMP Overview

A network provides ease of communication between computers. To use networks effectively, a set of rules are required by which all the networks should abide. The set of rules is called protocols. Simple Network Management Protocol (SNMP) is one such protocol and is used to transfer network management information between two or more network entities or nodes.

Features

The three major components of the SNMP that form an integral part of its foundation are the network device, the agent and the manager.

Network device: A network device or the Managed Object is a part of the network that requires some form of monitoring and management.

Agent: An agent is a mediator between the manager and the device. The agent resides inside the network device. It collects the management information from the device and makes it available to the manager. Note that an agent is a program that resides in the device and is not a separate entity.

A typical agent

- Implements full SNMP protocol.
- Stores and retrieves management information as defined in the MIB.
- Collects and maintains information about its local environment.
- Signals an event to the manager.
- Acts as a proxy for some non-SNMP manageable network node.

Manager: A manager or management system is a separate entity that manages the agents from a remote place. This is typically a computer that is used to run one or more network management systems. Consider an organization having its branches in different geographical locations. Administration of all the computers present in different localities would be difficult. When the System Administrator’s computer is installed with the manager and all other systems and devices across all the offices are installed with the agent, management becomes easier. The administrator has to just query the agent through its manger to know the functioning of the device.

A typical manager

- Implements the network management system.
- Implements full SNMP protocol.
- Queries agents, gets responses from agents, sets variables in agents, and acknowledges asynchronous events from agents.

Communication Between the Manager and Agent: The communication between the manager and the agent in the network is enabled through Protocol Data Units (PDUs). These PDUs allow the manager to interact with the agent in the device. The extent of management possible depends on the data available to the manager from the agent.

Before data can be transported across the network, it must be passed to the network mass and encapsulated. PDUs are encapsulated in the User Datagram Protocol (UDP). UDP is a connectionless transport protocol included in the TCP/IP suite and described in RFC 768.

The SNMP network management is composed of the following three parts to which both the management applications and agents conform. They are:

- The **protocol**, which defines the functioning of the basic operations of SNMP and the format of the messages exchanged by management systems and agents.
- **Structure of Management Information** (SMI), which is a set of rules used to specify the format for defining managed objects or the devices that are accessed using SNMP.
- **Management Information Base** (MIB) is a collection of definitions, which define the properties of the managed object or the device.

The MIB modules and the SMI are expressed using a text-based data description notation called Abstract Syntax Notation One (ASN.1), which is an unambiguous description of data in an ASCII text format. The MIB data is conveyed across a network using SNMP messages, which are encoded using Basic Encoding Rules (BER).They are similar to SMI, but the messages are encoded in a binary format. Both the ASN.1 and BER are essential for the implementation of SNMP.

Basic Operations

SNMP is a request-and-response protocol. The basic SNMP operations performed are categorized as follows

- Retrieving data
- Altering variables
- Receiving unsolicited messages

Retrieving data: The manager sends a request to an agent to retrieve data by performing the following operations

- GET: The GET operation is a request sent by the manager to the managed object. It is performed to retrieve one or more values from the managed objects.
- GETNEXT: This operation is similar to the GET operation. The significant difference is that the GETNEXT operation retrieves the value of the next OID in the tree.
- GETBULK: The GETBULK operation is used to retrieve voluminous data from large table.

Altering variables: At times, the manager might want to change the value of a variable.

- SET: This operation is used by the managers to modify the value of the network device.

Receiving unsolicited messages: The agent, when faced with problems in the transmission of message, responds to the manager by sending unsolicited messages by using the TRAP operation.

Versions of SNMP

Internet Engineering Task Force (IETF) publishes documents that are called Requests For Comments (RFCs). These documents specify standards, operational practices, opinions, humor, etc. for the Internet protocol suite.

The different versions of SNMP are the **SNMPv1**, **SNMPv2c**, and **SNMPv3**. The following is a brief of each version.

SNMPv1: This is the first version of the protocol, which is defined in RFCs 1155 and 1157.

SNMPv2c: This is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, and MIB structure elements but using the existing SNMPv1 administration structure ("community based" and hence SNMPv2c). It is defined in RFC 1901, RFC 1905, and RFC 1906.

SNMPv3: SNMPv3 defines the secure version of the SNMP. SNMPv3 also facilitates remote configuration of the SNMP entities. It is defined by RFC 1905, RFC 1906, RFC 2571, RFC 2572, RFC 2574, and RFC 2575.

MIB

SNMP agents for different types of devices provide access to objects that are specific to the type of device. In order to enable the SNMP manager or management application to operate intelligently on the data available on the device, the manager needs to know the names and types of objects on the managed device.

This is made possible by Management Information Base (MIB) modules, which are specified in MIB files usually provided with managed devices. For example, RFC1213-MIB (also known as MIB-II) is a MIB module which is typically supported by all SNMP agents on TCP/IP enabled devices or systems.

This MIB file contains a description of the object hierarchy on the managed device, as well as the name (Object ID), syntax and access privileges for each variable in the MIB.

ICMP Overview

The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. ICMP is documented in RFC 792.

What does an ICMP do?

Announces network errors such as a host or entire portion of the network being unreachable, due to some failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.

Announces network congestion when a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it generates ICMP Source Quench messages. Directed at the sender, these messages cause the rate of packet transmission to be slow. Of course, generating too many Source Quench messages would cause even more network congestion, so they are used sparingly.

Assists in troubleshooting and network discovery. ICMP supports an Echo function, which just sends a packet on a round-trip between two hosts. Ping, is based on this feature. Ping transmits a series of packets, measuring average round-trip times and computes loss percentages.

Announces Timeouts If an IP packet's TTL field drops to zero, the router discarding the packet often generates an ICMP packet. TraceRoute is a tool which maps network routes by sending packets with small TTL values and watches the ICMP timeout announcements.

CLI Overview

Command Line Interface is a user-friendly interface. It is mostly used in network device management. Using Command Line Interface, user can easily communicate to any component in a computer, hardware device, network device, operating system, and other applications.

Despite advances in network management technologies and the advent of other popular management protocols, such as SNMP, there are still numerous devices in the network, which offer CLI as the only way or preferred way of managing them. Also CLI-based configuration tasks have been simplified using scripts. Thus it has become by far the most prevalent management connectivity in the world. After the popularity of the Internet and IP networks, the CLI protocol was offered not only on serial links but also over TCP and other transport protocols. This offered a lot of flexibility to CLI users who could still use the same CLI command from a remote terminal to manage the device instead of being tied down to a terminal connected to the device over a serial link. These management terminals (remote and local) gradually came to be known as 'Management Console' or 'Management Stations'.

Advantages of CLI

Following are the advantages of the Command Line Interface:

- You can make and modify configuration settings.
- You can create, update, and delete a component, device in a network, or any database information
- You can start, stop and suspend any service in network operation.
- You can control a service running on a network device.
- You can enable and disable a switching component in a network or in any conditional storage variable.
- You can view the properties of a network device or any specified component.
- Command line Interface is either text string based or character key based. This makes the Command Line Interface very user friendly. Any terminal interface, such as Telnet interface, Serial interface, etc. acts as a CLI.

Getting Started

This section explains

- System Requirements
- Installing and Starting OpUtils
- Prerequisites
- Installing SNMP
- Licensing the Product

System Requirements

Hardware Requirements

Hardware	Recommended
Processor	P4 - 1.0 GHz
RAM	512 MB
Disk Space	200 MB

Software Requirements

Supported JDK

- JDK 1.5 and above.

Supported Platforms

ManageEngine OpUtils is platform independent and supports the following operating systems

- Windows 2000
- Windows NT
- RedHat Linux 7.x

Supported Browsers

ManageEngine OpUtils requires one of the following browsers to be installed in the system

- Internet Explorer 5.5 and above
- Netscape 7.0 and above
- Mozilla Firefox 1.0 and above

Preferred screen resolution 1024 x 768 pixels or higher

Installing and Starting OpUtils

OpUtils is distributed in the following formats

For Windows

- Self-extracting EXE format

For Linux

- Binary file

For more read the sections

- Installing and Starting OpUtils in Windows
- Installing and Starting OpUtils in Linux

Note: OpUtils package comes with a collection of MIB's that are stored in the FireBird database.

Installing and Starting OpUtils in Windows

For Windows OS, OpUtils is distributed in the EXE format

To Install

Self-extracting EXE format

1. Run the **self-extracting EXE format** with an Install Shield program for installation and follow the instructions provided.

To Install OpUtils Service

To install OpUtils as a Windows Service, select **Start -->Programs -->ManageEngine OpUtils 5 --> Administrative Options --> Install Service**

> **Note:** This is not required, if you have selected the option to Install OpUtils as Service during installation or if you do not wish to run OpUtils as a Windows Service.

To Start OpUtils Server

To start OpUtils, select **Start --> Programs --> ManageEngine OpUtils 5--> Start OpUtils**.

On starting the server, the client is automatically launched in the default browser to show the details about the installation and the tools available in the free, standard, and professional editions. Click **Continue** to proceed.

Note: The FireBird database runs by default when OpUtils server is started.

To Stop OpUtils

Exe users

Select **Start --> Programs --> ManageEngine OpUtils 5 --> Stop OpUtils**

To Manage OpUtils from System Tray

OpUtils can also be managed from the system tray icon. To view the icon in the system tray, select **Start --> Programs --> ManageEngine OpUtils 5 --> Show Tray Icon**. Right-click the icon to perform the following functions:

- **Start OpUtils**: To start OpUtils server.
- **Stop OpUtils**: To stop OpUtils server.
- **Exit**: To exit the system tray icon.
- **Options**: To change the default port of OpUtils and to set the log level.
- **About**: To view the product version and support information.
- **Send Support File**: To create and send support file to our support team.

Note:

1. Exiting the system tray icon will only remove the icon from the system tray and does not stop the OpUtils server.
2. The log level INFO is meant for debugging purpose only and hence it is not recommended to run OpUtils continuously with this log level as it consumes a lot of disk space.

To Uninstall OpUtils Service

To uninstall OpUtils from Windows Service, select **Start --> Programs --> ManageEngine OpUtils 5 --> Administrative Options --> Uninstall Service**

To Uninstall OpUtils

1. Stop Firebird by right clicking on the yellow-black icon of a bird representing Firebird in the system tray and select the Shutdown menu.
2. Click **Start->Programs->ManageEngine OpUtils 5 ->Uninstall**

Installing and Starting OpUtils in Linux

For Linux OS OpUtils is distributed as a bin file.

To Install OpUtils

1. Download the bin file.
2. Check the executable permission of the binary file
3. Change the permission using chmod -R 755 <bin file name>
4. Execute the bin file as given below and follow the instructions
   ./<bin file name>

To Install OpUtils in Console Mode

If you do not have X-Windows, you can install OpUtils in the console mode as below:

1. Download the bin file.
2. Check the executable permission of the binary file
3. Change the permission using chmod -R 755 <bin file name>
4. Execute the bin file as given below and follow the instructions
   ./<bin file name> -console

Note: OpUtils uses FireBird database to store the configurations and monitored information. To install and start Firebird:

1. Login in as superuser to install FireBird. Execute the script **installFirebird.sh** located in the *<OpUtils Home>/bin/ directory* to install firebird. <OpUtils Home> refers to the directory where Oputils is installed. For example if OpUtils is installed in /home/<user name>/ directory run the script from /home/<user name>AdventNet/ME/OpUtils/bin directory.
2. By default FireBird will get started once installation is completed.

Warning : FireBird will not work in Redhat 7.x because by default Red Hat Linux 7.2, has only libstdc++-2.96-98 installed. To install firebird in linux, libstdc++-3.2.7 should be installed as a separate package (please do not upgrade the default version) in Linux.
libstdc++-3.2-7.i386.rpm requires GLIBC_2.3.x which in turn includes the following packages that need to be installed
glibc-devel-2.3.2-4.80.8
glibc-common-2.3.2-4.80.8
glibc-debug-static-2.3.2-4.80.8
glibc-debug-2.3.2-4.80.8
glibc-2.3.2-4.80.8
glibc-utils-2.3.2-4.80.8

To Start OpUtils

1. To start the OpUtils Server run the script **sh startOputils.sh** located in *<OpUtils Home>/bin* directory.
2. On starting the server, the client is automatically launched in the default browser to show the details about the installation and the tools available in the free, standard, and professional editions. Click **Continue** to proceed.

To Stop OpUtils

Run the script **shutdownOpUtils.sh** located in *<OpUtils Home>/bin* directory.

Un-installing OpUtils

1. Stop Firebird database.
2. Remove the directory in which OpUtils is installed.

Service Pack

A service pack is a collection of bug fixes and minor feature enhancements, which can be applied at a single instance over the product. It is an efficient and easy process for maintaining and updating the product. When a service pack is developed all the product users and customers are informed of the service pack and the fixes available in it.

Installing a Service Pack

The installation of service pack is explained under the section Installing Service Pack. The service pack will be available in web site.

Un-installing a Service Pack

It is possible to revert to any previous version of service pack or the base version of the product. The un-installation of service pack is explained under the section Uninstalling Service Pack.

Installing Service Pack

AdventNet periodically provides Service Packs which provide new features (requested by the customers), fixes for certain bugs and document updates in the form of HTML files. Service Packs can be downloaded from the web site, and updated into ManageEngine OpUtils using the Update Manager tool.

Installing the Service Pack Using Update Manager Through UI

Note: Ensure that no application is running when applying the Service Pack. This prevents any files used by the application from being over-written. For example if the OpUtils server is running, stop the server and then install the service pack.

The steps to apply a Service Pack are as follows.

Step 1:Start Update manager by executing the script **UpdateManager.bat/sh** file in the <OpUtils Home>/bin directory.

Step 2 : Click "**Browse**" button and select the Service Pack file (.ppm) to be installed. Click **Install** button to install the Service Pack.

Step 3: You can go through the Readme file of the Service Pack by clicking the "Readme" button.

Note: On clicking the "Install" button, the tool checks whether there is enough space for the installation of the service pack. If there is not enough space, the tool informs the user about the lack of space. You must clear the space and then proceed with the installation.

Un-Installing Service Pack

You have the option of reverting the changes incorporated by the installation of a Service Pack. You can revert to the previous version of the Service Pack or to the base version of the application. Before you start the un-installation process, make sure no application is running.

Un-installing the Service Pack

The steps to revert to a previous version are as follows.

1. Start Update Manager: Run **UpdateManager.bat/sh** from *<OpUtils Home>/bin* directory.
2. Select the service pack, which needs to be uninstalled, from the Installed Service Pack list. Click the **Uninstall** button to proceed with the un-installation.
3. The list of dependent service packs if any will be shown for your confirmation before proceeding with the process. Click **Finish** button to proceed.
4. Thus the specified Service Pack is un-installed in the application. You can now continue with the screen (like un-installing another Service Pack) or quit the tool by clicking the **Exit** button.

Prerequisites

The prerequisites for working with each tool set of ManageEngine OpUtils are listed below

Diagnostic Tools

Tool	Is SNMP needed?	Required MIBs
Ping	No	None
Ping Scan	No	None
SNMP Ping	YES	RFC1213-MIB
SNMP Scan	YES	RFC1213-MIB
Proxy Ping	YES	**CICSO-PING-MIB
Trace Route	No	None

Address Monitoring Tools

Tool	Is SNMP needed?	Required MIBs
DNS Resolver	No	None
DNS Scan	No	None
MAC IP List	No	None
MAC Address Resolver	YES	RFC1213-MIB
MAC Address Scan	YES	RFC1213-MIB
Subnet List	YES	RFC1213-MIB
IP Address Manager	YES	RFC1213-MIB
DHCP Scope Monitor	YES	RFC1213-MIB, DHCP-MIB, MSFT-MIB
Rogue Detection	No	None

Server Monitoring Tools

Tool	Is SNMP needed?	Required MIBs
System Snapshot	YES	RFC1213-MIB HOST-RESOURCE-MIB
Disk Space Monitor	YES	RFC1213-MIB HOST-RESOURCE-MIB
CPU Monitor	YES	RFC1213-MIB HOST-RESOURCE-MIB
Process Scan	YES	RFC1213-MIB HOST-RESOURCE-MIB
Software Scan	YES	RFC1213-MIB HOST-RESOURCE-MIB
IP Node Browser	YES	RFC1213-MIB HOST-RESOURCE-MIB
TCP Reset	YES	

Network Monitoring Tools

Tool	Is SNMP needed?	Required MIBs
Bandwidth Monitor	YES	RFC1213-MIB
Switch Port Mapper	YES	RFC1213-MIB BRIDGE-MIB**
Performance Monitor	YES	RFC1213-MIB
Network Scan	No	None
Network Monitor	No	None
IP Network Browser	YES	RFC1213-MIB HOST-RESOURCE-MIB
Wake-On-LAN	No	None
Port Scanner	No	None
System Details Update	YES	RFC1213-MIB
System Explorer	YES	RFC1213-MIB HOST-RESOURCE-MIB
TCP Reset	YES	RFC1213-MIB

CISCO Tools

Tool	Is SNMP needed?	Platform Series	Required MIBs
Config File Manager	YES	CISCO2500 series and above	RFC1213-MIB OLD-CISCO-SYS-MIB CISCO-CONFIG-COPY-MIB
TFTP Server	NO	NA	NA
Device Scan	YES	CISCO2500 series and above	RFC1213-MIB
Device Explorer	YES	CISCO2500 series and above	RFC1213-MIB OLD-CISCO-INTERFACES-MIB

SNMP Tools

Tool	Is SNMP needed?
MIB Viewer	No
SNMP Walker	YES
SNMP Graph	YES
Trap Receiver	NA
MIB Browser	YES
Community Checker	YES
SNMP Table	YES

Note:

- For details on installing SNMP on different OS read the Installing SNMP section.
- For enabling SNMP in a CISCO Router read the Configuring Simple Network Management Protocol (CISCO Documentation) section.

Installing SNMP

Before starting OpUtils, it is advisable to check if your system or the systems to be monitored are SNMP enabled.

For checking SNMP in Windows OS

1. Go to Start-> Settings-> Control Panel->Administrative Tools-> Services
2. Check for SNMP Service.
3. If SNMP Service does not exist, install SNMP. To do so, read the Installing SNMP on Windows section
4. If **SNMP Service** is displayed but the status of the Service is not displayed, double click on SNMP Service and click on **Start** to start the Service. You can also choose to start the service manually or automatically.

For checking SNMP in Linux

1. Execute any one of the command in the console
   $ /etc/rc.d/init.d/snmpd status or $ **service snmpd status**
2. If SNMP is installed, but is not started, execute any one of the command in the console to start SNMP (as root)
   $ /etc/rc.d/init.d/snmpd start or $ service snmpd start
3. If SNMP is not installed, install SNMP. To do so, read the Installing SNMP on Linux section.

Windows

(Adapted from Microsoft Windows help)

- Installing and configuring SNMP Agent and Traps on Windows XP/2000
- Installing and configuring SNMP Agent and Traps on Windows NT

Prerequisites

You need to know the following information before you install the Simple Network Management Protocol (SNMP) service on your computer:

- Community names in your network.
- Trap destinations for each community.
- IP addresses and computer names for SNMP management hosts.

To install SNMP on Windows XP or 2000 follow the steps given below:

1. You must be logged on as an **administrator** or a member of the **Administrators group** to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.
2. Click **Start**, point to **Setting**s, click **Control Panel**, double-click **Add** or **Remove Programs**, and then click **Add/Remove Windows Components**.
3. In **Components**, click **Management and Monitoring Tools** (but do not select or clear its check box), and then click **Details**.
4. Select the **Simple Network Management Protocol** check box, and click **OK.**
5. Click **Next**.
6. Insert the respective CD or specify the complete path of the location at which the files stored.
7. SNMP starts automatically after installation.

Configuring SNMP Agent

To configure SNMP agent in Windows XP and 2000 systems, follow the steps given below:

Step 1 - Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools** and then double-click **Computer Management**.

Step 2 - In the console tree, click **Services and Applications** and then click **Services**.

Step 3 - In the details pane, scroll down and click **SNMP Service**.

Step 4 - On the **Action** menu, click **Properties**.

Step 5 - On the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.

Step 6 - Under **Accepted community** names, click **Add**.

Step 7 - Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.

Step 8 - In **Community Name**, type a case-sensitive community name, and then click **Add**.

Step 9 - Specify whether or not to accept SNMP packets from a host:

- To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
- To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate **host name, IP or IPX address**, and then click **Add** again.

Step 10 - Click **Apply** to apply the changes.

Configuring Traps

Step 1 - Click Start, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Computer Management**.

Step 2 - In the console tree, click **Services and Applications** and then click **Services**.

Step 3 - In the details pane, click **SNMP Service**.

Step 4 - On the **Action** menu, click **Properties**.

Step 5 - On the **Traps** tab, under **Community name**, type the case-sensitive community name to which this computer will send trap messages, and then click **Add to list**.

Step 6 - In Trap destinations, click **Add**.

Step 7 - In **Host name, IP or IPX address**, type information for the host, and click **Add**.

Step 8 - Repeat steps 5 through 7 until you have added all the communities and trap destinations you want.

Step 9 - Click **OK** to apply the changes.

To install SNMP in Windows NT, follow the steps given below:

1. Right-click the Network Neighborhood icon on the Desktop.
2. Click Properties.
3. Click Services.
4. Click Add. The Select Network Service dialog box appears.
5. In the Network Service list, click SNMP Service, and then click OK.

6. Insert the respective CD or specify the complete path of the location at which the files stored and click **Continue**.
7. After the necessary files are copied to your computer, the Microsoft **SNMP Properties** dialog box appears.

To configure SNMP Agent in Windows NT Systems follow the steps given below:

Step 1 - Right-click on the **Network Neighborhood** icon on the Desktop.

Step 2 - Click **Properties**.

Step 3 - Click **Services**.

Step 4 - Click **SNMP Service**, and then click **Properties**.

Step 5 - Click the **Security** tab.

Step 6 - If you want to send a trap for failed authentications, select the Send Authentication Trap check box.

Step 7 - Under **Accepted Community Names**, click **Add**.

Step 8 - In the **Community Names** box, type a community name from which you will accept requests.

Step 9 - To move the name to the **Accepted Community Names** list, click **Add**.

Step 10 - Repeat step 9 for any additional community name.

Step 11 - To specify whether to accept SNMP packets from any host or from only specified hosts, click one of two options:

- **Accept SNMP Packets From Any Host**, if no SNMP packets are to be rejected on the basis of source computer ID.
- **Only Accept SNMP Packets From These Hosts**, if SNMP packets are to be accepted only from the computers listed. To designate specific hosts, click **Add**, type the names or addresses of the hosts from which you will accept requests in the IP Host or IPX Address box, and then click **Add** to move the name to the **Only Accept SNMP Packets From These Hosts list**.

Repeat step 11 for any additional hosts.

On the **Agent** tab, specify the appropriate information (such as comments about the user, location, and services). Click **OK** to apply the changes.

To configure SNMP Traps follow the steps given below:

1. Right-click on the **Network Neighborhoo**d icon on the Desktop.
2. Click **Properties**.
3. Click **Services**.
4. Click **SNMP Service** and then click **Properties**.
5. Click the **Traps** tab.

6. To identify each community you want this computer to send traps, type the name in the **Community Name** box. Community names are case sensitive.
7. After typing each name, click **Add** to add the name to the list.
8. To specify hosts for each community you send traps to, after you have added the community and while it is still highlighted, click **Add** under **Trap Destination**.
9. To move the name or address to the **Trap Destination** list for the selected community, type the host name in the **IP Host/Address** or **IPX Address** box and then click **Add**.
10. Repeat step 10 for any additional hosts.
11. Click **OK** to apply the changes.

Linux

The installation of new version of SNMP is required only for Redhat Linux versions.

Download the latest version of SNMP using the following URL:

http://heanet.dl.sourceforge.net/sourceforge/net-snmp/

Extract the file using following command:

tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Log in as root user.
2. Execute the command to set the path of the C compiler:
3. Export PATH=<gcc path>:$PATH
4. Execute the following four commands from the directory where you have extracted the ucd-snmp:
   - ./configure --prefix=<directory_name> --with-mib-modules="host" . directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP therefore do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

In case of rpm (redhat package manager) package installation use the following command.

$ rpm -i <package name>

Configuring the Agent in Linux versions prior to 8

1. Stop the agent if it is already running using the command:

   /etc/rc.d/init.d/snmpd stop

2 . Make the following changes in the /etc/rc.d/init.d/snmpd file

- o Replace the line
  daemon /usr/sbin/snmpd $OPTIONS
  with
  daemon /root/ucd_agent/sbin/snmpd $OPTIONS
- o Replace the line
  killproc /usr/sbin/snmpd
  with
  killproc /root/ucd_agent/sbin/snmpd

This is to choose the current installed version while starting and stopping the SNMP agent.

3.Start the agent using the command /etc/rc.d/init.d/snmpd start.

Configuring the Agent in Linux versions 8 and Above

On Linux versions 8 and above, the latest version of SNMP will already be available. You need to just make the following changes in snmpd.conf file:

1. Insert the line

```
view allview      included   .1.3.6
```

next to the line

```
# name incl/excl subtree mask(optional)
```

3.Change the line

```
access  notConfigGroup "" any noauth exact systemview none none
```

next to the line

```
# group context sec.modelsec.level prefix read   write  notif
```

as

```
access  notConfigGroup ""   any  noauth   exact  allview none none
```

4.Then restart the SNMP agent using the following command:

```
/etc/rc.d/init.d/snmpd restart
```

Licensing the Product

OpUtils is available in three editions - **Free**, **Standard**, and **Professional** Edition.

Download the product from our Website

The **Free Edition**, **Standard Edition**, and **Professional Edition**, both come packaged as a single download. During the evaluation phase, the **Professional Edition** is installed, and can be evaluated for 15 days. After 15 days, it is automatically reverted to the **Free Edition**, unless the **Standard**/**Professional Edition** license is purchased

Details on the tools available in the Free Edition, Standard Edition, and Professional Edition are discussed in the Product Edition Matrix section.

For purchase of license or any queries please contact sales@adventnet.com. The license file will be sent through e-mail.

To Upgrade from Trial/Free Edition to Standard/Professional Edition

1. Click **Upgrade** available in the right corner of the OpUtils client page**.**
2. In the **Upgrade ManageEngine OpUtils** 5 dialog choose the license file sent by sales@adventnet.com using the **Browse** button.
3. Click the **Upgrade** button to upgrade from Trial or Free Edition to Standard or Professional Edition.

Configuring ManageEngine OpUtils

ManageEngine OpUtils not only provides users the flexibility to configure the Protocols that are essential for the functioning of the tool, but also provides user privileges to personalize the tool based on requirements. The option to export and print reports of all the results generated by the tool is another important feature available in the tool.

To know more read:

- Adding Routers
- Settings
- Managing Scheduled Tasks
- Global Alerts
- Personalize
- User Management
- Exporting, Printing, and E-mailing Results

Adding Routers

The Add Routers screen lets you specify the routers, switches, and gateway servers in your network and schedule scanning. OpUtils, based on the scheduler details, scans the devices to collect the MAC IP data of the network devices. The data collected is used in arriving the reports and in the tools that uses the MAC IP data.

To add your Routers

1. Click the tab **Admin -> Add Router** from the left panel. You can also add routers from the Rogue Detection and Switch Port Mapper tools.
2. Click the **Add Router** link.
3. The **Add Manually** option is selected by default.
4. Specify the **Device Name** and **its SNMP Community**.
5. Optionally, you can also specify the CLI Settings to get the details through CLI:
    1. Select the Router/ Switch vendor. The input fields vary with the vendor.
    2. Specify the username, password, password prompt, enable password, and enable password prompt as required.
6. Click **Add Device**.
7. Repeat step 3 for adding all the devices in your network.
8. The SNMP details of the devices can also be imported from a csv file by selecting the **Import form CSV** option.
9. To schedule scanning of routers, click **Disabled** link available beside the **Next Scan** and specify the scan interval.
10. To resolve the DNS names of the devices during every scan, click the **Disabled** link available beside the Resolve DNS Name and enable it.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E1004: Not a Router, E2001 No Response to SNMP Queries

Settings

ManageEngine OpUtils relies heavily on ICMP and SNMP and CLI protocols for data retrieval, and SMTP for e -mailing reports generated by the tools. The MAC-IP data of the devices in Windows network are retrieved through WMI. As most of the tools use SNMP, ICMP and SMTP, the settings for all the tools are captured in one place for a hassle free protocol configuring experience. In addition to the above function, the polling interval and the number of plots in graphs can also be configured.

To set ICMP, SNMP, CLI, SMTP, WMI, Linux, and Graph values for all the tools

1. Click the tab **Admin -> Settings** from the left panel
2. Click the ICMP, SNMP, SMTP, WMI, Linux, Graphs, and General tabs to enter values.

For details read the sections

- Configuring ICMP
- Configuring SNMP
- Configuring SMTP
- Configuring WMI
- Configuring Linux
- Configuring Graphs
- Configuring Encoding and Log Level

Configuring ICMP Properties

Field	Purpose	Maximum Value
Packet Count	To send the specified number of packets from the host to the target destination for checking the aliveness of a network element.	100
Packet Size	To send the packet with the specified size from the host to the target destination for checking the aliveness of a network element.	200 bytes
Time to Live	For specifying the number of hops a packet can travel before being discarded or returned.	255 seconds/hops.
Timeout	For specifying the maximum amount of time in seconds that the ping should wait for a response from the target network element. If the target NE does not respond within the number of milliseconds set here, PING will assume it is down and a Request timed out response is sent.	5000 seconds.

Click **Save** to save the values. To maintain the default values click **Restore Defaults.**

Configuring SNMP Properties

Field	Purpose	Default Value
SNMP Version	For setting the values for the two supported versions of the SNMP protocol- SNMPv1 and SNMPv2c	SNMPv1 or SNMPv2c
Port	For specifying the port in which the SNMP agent is running. Port value must be between 1 and 65535.	Port 161
Community	For specifying the community of the SNMP enabled device	
Timeout	For specifying the time interval in seconds that the device will wait for a response to an SNMP query. The value specified should be within the range 1and10.	4 seconds
Retries	For specifying the number of times an SNMP request is resent if the preceding request times out. Retries values should be between 0 and 5.	0
MAX repetitions (For Get Bulk)	For specifying the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list. The MAX repetitions values should be between 1 and 1000000000. Supported only for SNMPv2.	50
Non Repeaters (For Get Bulk)	For specifying the number of variables in the variable-bindings list for which a single lexicographic successor is to be returned. The Non Repeaters values should be between 1 and 1000000000. Supported only for SNMPv2.	0

Click **Save** to save the values. To maintain the default values click **Restore Defaults**.

Configuring SMTP Properties

Field	Purpose
SMTP Server	For specifying the name of the SMTP Server
Port	For specifying the port where the SMTP Server runs.
From Address	The sender's email address. By default the email specified will be displayed as the sender email id for all messages sent from OpUtils.

If the SMTP server specified requires authentication, select the **Authentication Required** checkbox and specify the **User Name** and **Password.**

Click **Save** to save the values or use the **Restore defaults** button to restore to the state prior to the modification.

Configuring WMI Properties

when the WMI parameters are configured, OpUtils fetches the MAC-IP data of the devices in the network through WMI.

Field	Purpose
Administrator Login Name	For specifying the name of the administrator account of the Windows domain
Password	The password to this administrator account.
Domain	The Domain to which this account belongs.

Click **Save** to save the values. To maintain the default values click **Restore Defaults**

Configuring Linux Properties

Configure any common Linux user account that are available in all / most of the linux machines in the network. OpUtils, using this account, will fetch the mac-ip details of the linux machines. For example, you can specify a guest account.

Field	Purpose
Login Name	For specifying the name of the linux user account
Password	The password to this user account.

Click **Save** to save the values. To maintain the default values click **Restore Defaults**

Configuring Graphs Properties

Field	Purpose
Polling Interval	Polling the device at the interval specified. The interval specified must be between 1 and 65535 seconds
Number of Plots	The number of plots (plot values in Server memory) to be plotted for the graphs. The number of plots must be between 1 and 100.

Click **Save** to save the values or use the **Restore defaults** button to restore to the state prior to the modification

Configuring Encoding and Log Level

Configuring Encoding

Why should character coding/encoding values be set ?

The character coding/encoding values should be set to enable the OpUtils user to view valid values from the SNMP Agent in the OpUtils Client. Hence the user should set the character coding/encoding value based on the language version of the SNMP Agent queried by the User. For example if OpUtils is running in a Chinese machine,the character coding/encoding should be set to GB18030 or GB2312. Hence, values fetched from the SNMP Agent will be displayed in Chinese for all the tools.

How to set encoding values

Step 1 : Click the **General** tab.

Step 2 : Choose encoding values from the **Character Coding/Encoding** list box based on the language where the OpUtils Server runs. The list box holds all the supported coding/encoding values supported in the OpUtils JVM.

Step 3 : Click **Save** to save the **Character Coding/Encoding**. If the specified character coding/encoding is present in the server machine, it will be saved or else the default value is set. Also ensure your browser supports the specified character coding.

Note	Ensure the web-browser used for accessing OpUtils client supports the specified character coding/encoding.

Configuring Log Level

OpUtils supports the following log levels:

- **SEVERE**: Logs only the important events.
- **WARNING**: This is the default option. Logs both the important and warning events.
- **INFO**: Logs all the events. This is useful for debugging purposes. If this option is selected, you will get a warning message while logging into the client as it consumes more disk space.

To configure the log level, select the required log level from the **Log Level** combo box under the **General** tab.

Configuring Client Startup

Whenever OpUtils is started, the client is launched in the default browser. If you wish to disable launching the client, clear the "Open the client upon successful server startup" option available under the **General** tab.

Managing Scheduled Tasks

ManageEngine OpUtils supports scheduling of tools to run at a specified period. You can manage the scheduled tasks globally from here or from the respective tools. The following tools can be scheduled:

1. Wake on LAN
2. Switch Port Mapper
3. Network Monitor

Apart from the above tools, the Router and Subnet inputs provided in the Global Environment can also be scheduled to run at specified intervals.

To Manage Scheduled Tasks

1. Select **Admin --> Scheduler** to list the details of the scheduled tasks.
2. Click **Modify data** link to modify the interval or to enable/disable the task.

Global Alerts

ManageEngine OpUtils generates alerts in various tools to notify anomalies in the monitored device. The tools can be configured to notify the alerts through e-mail or by playing a sound. The table given below lists the tools that generates alerts and the conditions when an alert is generated:

Tool	Alert Condition
Bandwidth Monitor	When in traffic, out traffic, or both in and out traffic exceeds a specified limit
Network Monitor	When the response time exceeds a specified limit or when the device goes down.
IP Address Manager	When the state of an IP Address changes from "Used to Available" or from "Available to Used".
Switch Port Mapper	When the state of the port changes from "Up to Down" or from "Down to Up".
Trap Receiver	Whenever a trap is received
Rogue Detection	When a rogue device is detected.
DHCP Scope Monitor	When the available IP Addresses in a scope falls below the defined criteria.

To View the Alerts

To view all the alerts generated by OpUtils,

1. Click the **Alerts** link available in the top-right.
2. This opens the Alerts view to show the alerts generated by OpUtils.
3. The **View Alerts** tab is selected by default. This will list all the alerts generated by OpUtils with the details of the tool that generated the alert, Alert Time, Alert Severity, and Description.
4. To delete an alert, select and click **Delete**.

To Configure E-mail and Sound Alerts

1. Click the **Alerts** link available in the top-right.
2. This opens the Alerts view to show the alerts generated by OpUtils.
3. Click the **Configure Alerts** tab. This will list the tools and the status of email and sound alert configuration. To modify/edit, click the ✎ icon and make the necessary changes and save.

Personalize

ManageEngine OpUtils provides users with the functionality to configure user accounts based on personal priorities and requirements. The Personalize option enables users to reset the password as "admin", change an existing password and set the session time of the tool. This privilege is given to all users of the tool

To personalize, click **Admin** -> **Personalize**

To Reset Password

1. Click the tab **Change Password**.
2. Click the **Reset** button and click OK to confirm.

To Change Password

1.Click the tab **Change Password**.

2. Enter the following values :
   - Old Password : Enter the existing password
   - New Password : Enter the new password
   - Confirm Password : Enter the new password once gain for confirmation
3. Click **Save**.

Error Messages: **E: 6001 Old password is incorrect**

To Set / Modify the Session Time

1.Click the tab **Session Expiration.**
2.Select the session expiry time in hours from the combo box. Choose **Never** for an unlimited session.
3. Click **Save**.

User Management

Admin Privileges

The **admin** user is provided with the privileges to add/modify and delete Users.

To add a user

1. Click the **Admin** tab and choose **User Management** from the left panel**.**
2. In **Add User** section, enter the **Name** and **Password.** Click the **Add User** button. The User is added to the **User Account Data** table. View the details.

Note: As a User/Admin if you want to change/reset the Password and set the Session time for the tool read the Personalize section.

Error Messages : E6003 User already exists

To modify a user

1.Click the **Admin** tab and choose **User Management** from the left panel**.**
2. Click the icon.
3. Modify the user details.
4. Click the **Modify** button to save the changes.
5.Click **Cancel** to exit the operation

To delete a user

1. Click the icon located in the User name row. A confirmation dialog appears. Click **OK** to delete the user or click the **Cancel** button to exit from the operation.

Exporting, Printing, and E-mailing Results

After the results are generated by the tool, the results can be exported in any of the desired file formats. The same results can also be viewed, printed and e mailed for any further reference.

Exporting Results

After the results are generated

1. Click **Export** available in the top frame.
2. Choose any one of the file formats displayed.
3. Click **View** for a preview of the file to be saved.

Printing Results

After the results are generated by the tool, to print reports, click the **Print** option provided in the top frame. Check the preview provided, and press the **Print this Page** tab.

E-Mailing Results

After the results are generated,

1. Click **E Mail** available in the top frame.
2. Specify the **To** address. The **From** address is taken from the SMTP Settings.
3. Choose any one of the report formats displayed.
4. Click **Send**.

Note: Ensure the values for SMTP are set for email actions.

Error Messages : E 6002 Unable to send mail

Switch Port Mapper Tool

The Switch Port Mapper utility of OpUtils software discovers the devices plugged into each port of a specified switch. The tool is useful for system and network engineers to gain visibility into the IP, MAC, status and availability of ports. Since this is a real-time discovery you can also view the operational status and port speed of each port.

Switch Port Mapper Settings

Click the **Settings** link from the Switch Port Mapper tool to view/modify the values. Click **Save** after changing the values.

General Settings

Click the **General** tab under Switch Port Mapper settings to configure the following:

1. **Resolve DNS** - Select this option to resolve the DNS name of the connected devices during every scan.
2. **Show all the Switch Ports** - The Switch Port Mapper, by default, will only list the ports that have a matching port in the Bridge MIB. All the other ports will be excluded from the result view. To view all the switch ports even if no matching port is available in the Bridge MIB, select this option.
3. **Exclude Trunk Ports** - Select this option to exclude the trunk ports while exporting the switch port mapping results. When more than one MAC Address is learned in a port, OpUtils assumes it to be a trunk port.
4. **Number of Threads** - Specify the number of threads that OpUtils use for Switch Port Mapping. OpUtils allocates one thread to a

switch for scanning and when completed the next switch in queue is taken for scanning. This cycle continues till all the switches are scanned. When the switch count is high and if you wish the scanning to be completed faster, you can increase the number of threads to a maximum of 25. Increasing the number of threads will increase the CPU and Memory usage considerably. Hence, ensure that your system is capable of handling this high resource requirement before increasing the thread count.

Publish Mapping Results

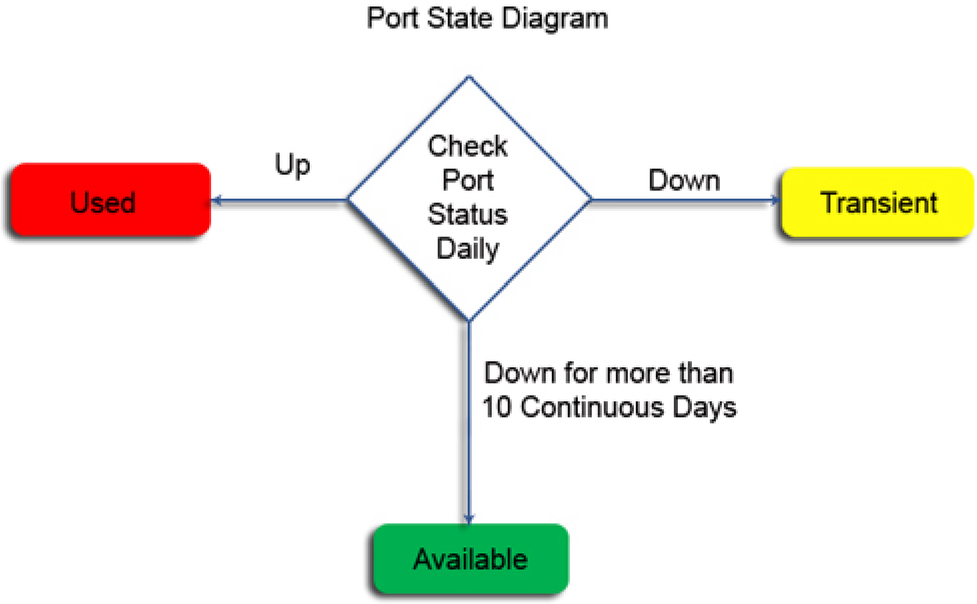
OpUtils provides an option to auto-publish the switch port mapping results to a csv file. This helps to view the history of port mapping details later. Click the **Publish** tab under Switch Port Mapper settings to publish the results of the scan to a csv file automatically.

1. **Enable Auto-Publish** - Select this option to enable publishing the results to a CSV file automatically. This option is selected by default.
2. **Publish Directory** - Specify a location to store the published results. The default location is *<OpUtils_Home>/webapps/SPMHistory*
3. **Create a consolidated CSV file for all the switches** - Select this option to create a consolidated CSV file containing the mapping results of all the switches scanned. It may be noted that you will be getting a consolidated reports only at the group-level, i.e., a single report for all the switches in a particular group. Also, the consolidated report will only be created whenever a scheduled scan happens for a particular group and not during manual scans.

Configure Email/Sound Alerts to Notify Port State Changes

Alerts are generated whenever the status of the port changes from "Available to Used" or from "Transient to Available". Click the **Alert** tab under Switch Port Mapper settings to configure alert settings:

1. **Policy to move a port from "Transient" to "Available" state** - Specify the continuous period of inactivity after which the ports will be declared as **Available**. If the ports are currently down and are down for less than the period specified here, the ports are shown as **Transient**.
2. **Enable Email Alert** - Select this option and specify the email addresses to notify the change in port states.
3. **Enable Sound Alert** - Select this option to play sound whenever there is a change in port state.
4. **Alert Cleanup Policy**: Specify the maximum number of Alerts to be stored in the database, the default being 2000. When you delete the older alerts, you have an option to save them as a csv file for future reference.



Grouping Switches

Switch Port Mapper allows you to group switches of your choice and schedule scanning of different groups at different times.

Adding Groups

1. Select the **Groups** tab. This will list all the groups that were created already.
2. Click the **Add Group** link. This opens the Group Configuration dialog
3. Specify a name for the group.
4. If you have already added the switches, you can select the switches for this group from the available switches. Else. you can create an empty group and can add switches later.
5. If you wish to schedule scanning of switches in this group, select **Enable** from the scheduler combo and specify the interval to perform the scan:
    1. **Hourly** - to update every 6, 8, or 12 hours from the specified time
    2. **Daily** - to update everyday. You need to specify the starting time.
    3. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
    4. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
    5. **Once Only** - to run the tool only once at the scheduled time.
6. Click **Save** to create the Group.

Note: You can also use the **Add Group** link from the Add Switch dialog to create a group and add switches.

Adding Switches to Groups

To add switches to Groups,

1. Select the **Groups** tab. This will list all the groups.
2. Click the **Modify** icon corresponding to the group to which you wish to add switches. This opens the Group Configuration dialog, showing the list of available switches.
3. Select the switches to add.
4. Click **Save**.

Note: A switch cannot be added in more than one group. When you move a switch to a group, it automatically gets removed from its previous group.

Schedule Scanning of Switches in Groups

1. Select the **Groups** tab. This will list all the groups.
2. Click the **Modify** link corresponding to the group that you wish to schedule. This opens the Group Configuration dialog, showing the list of available switches.
3. Select **Enable** from the scheduler combo and specify the interval to perform the scan:
   1. **Hourly** - to update every 6, 8, or 12 hours from the specified time
   2. **Daily** - to update everyday. You need to specify the starting time.
   3. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
   4. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
   5. **Once Only** - to run the tool only once at the scheduled time.
4. Click **Save** to save the changes.

Deleting Groups

1. Select the **Groups** tab. This will list all the groups.
2. Click the **Delete** icon corresponding to the group that you wish to delete.
3. Click **OK** to confirm.

Note: When you delete a group, all the switches in that group will be automatically moved to the Default Group. The Default Group cannot be deleted.

Adding Switches for Mapping

Adding Switches Manually

1. Click the **Tools Home** tab
2. Choose **Switch Port Mapper** available under the **Network Monitoring** category.

3. Click the **Add Switch** link available in the Switch Port Mapper tool. This will open a dialog to accept the switch input.
4. Select the **Add Manually** option.
5. Select the Group to which the switch has to be added.
6. Specify the **Switch Name** and its corresponding **SNMP Read Community** string.
7. Click the **Add Switch** button. The switch gets added under the **Switches** tab.
8. The added switch will be automatically mapped in the background and the status is shown in the status column. Repeat step four and five adding more switches.

Importing Switch Inputs from a CSV File

When you have a large number of switches in your network, adding switches one by one manually is a painful job. In such cases, importing the switch inputs from a csv file will be very handy. Create a csv file containing the Switch Name / IP Address, Switch Community, and the Group Name as comma separated values. Add each switch in a separate line. Import this file to the Switch Port Mapper tool.

Sample CSV entry:

```
catalyst2900,public,Default Group
foundry2402,private,Core
3com4400,public,
procurve2524,public,Building IV
```

1. Click the **Add Switch** link available in the Switch Port Mapper tool. This will open a dialog to accept the switch input.
2. Select the **Import From CSV** option.
3. Browse to select the CSV file. The CSV file should contain the Switch Name / IP Address, Switch Community, and the Group Name as comma separated values. Group Name is optional. If you are not specifying the group, just add a comma after the switch community. When the Group Name is not specified, the switch gets added to the Default Group. If you specify a non-existing group, it gets created. Multiple switch inputs should be in a separate line.
4. Click **Import CSV**.

The switches gets added and the import details are displayed in the top. The Switch Port Mapper will scan five switches at a time and the remaining switches are shown as **Yet to Scan**. If any errors are obtained during scan, the same is shown as **Scanning Failed**. Clicking the failed count will show the details of the errors from where you can modify and scan them again.

Note

1. Only Switches and Hubs that support the BRIDGE-MIB can be mapped because device details for Switches and Hubs that do not support a BRIDGE-MIB cannot be discovered.

2. Multiple devices may seem connected to the single port. This is because, if a Hub is connected to the Switch that is specified (Cascading) and multiple devices are connected directly to that hub, multiple devices appear as if they are connected to the same port of the switch.

Adding Routers

To resolve the IP Address of the device connected to a switch port, the Switch Port Mapper requires the router, switch, gateway server inputs to be provided in the Global Environment settings. You can use the Add Router link to add these devices and schedule scanning. This will collect the MAC-IP data of the devices in the network and stores them in the database.

Adding Routers Manually

1. Click the **Add Router** link available in the Switch Port Mapper tool. This will open a dialog to accept the router/device input.
2. Select the **Add Manually** option.
3. Specify the **Device Name** and its corresponding **SNMP Read Community** string.
4. Click the **Add Router** button.

Importing Router Inputs from a CSV File

Similar to importing switch inputs, you can also import router inputs through a csv file. Create a csv file containing the Device Name / IP Address and its SNMP Community as comma separated values. Add each device in a separate line. Import this file to the Switch Port Mapper tool.

Sample CSV entry:

```
testrouter,public
cisco3620,private
```

1. Click the **Add Router** link available in the Switch Port Mapper tool. This will open a dialog to accept the router/device input.
2. Select the **Import From CSV** option.
3. Browse to select the CSV file. The CSV file should contain the Device Name / IP Address and its SNMP Community as comma separated values. Multiple device inputs should be in a separate line.
4. Click **Import CSV**.

Viewing Switch Port Mapping Results

Once you have added all the switches, the mapping will be automatically performed and the status of the mapping is displayed. Click the Switch Name / IP Address link from the **Switches** View or from the **Summary Info** View to view its details. The following details are shown:

1. **IfIndex**: Refers to the port number in the switch.
2. **IfName**: The name of the port/interface.
3. **IfDescr**: The description of the port/interface.
4. **ifAlias:** The user-defined name of the port/interface.
5. **IfType**: The port type.
6. **IfSpeed**: The maximum speed of the port.
7. **Status**: The operation status of the port.
8. **Admin Status:** The administrative state of the port/interface.

9. **Availability**: Indicates whether the port is **Available** or **Used**. Ports that are continuously down for more than 10 days are shown as Available. If the ports are currently down and/or down for less than 10 continuous days, the ports are shown as **Transient**. You can configure the number of days of inactivity beyond which a port has to be declared as Available from Switch Port Mapper Settings.
10. **Location**: The physical location of the connected devices. Refer to Mapping Devices to Physical Location for details.
11. **MAC Address**: The physical address of the connected devices.
12. **IP Address**: The IP Address of the connected device.
13. **DNS Name**: The DNS name of the connected device.
14. **VLan**: The VLan number of the port.

You can select a different Switch using the combo box to view its details.
To Scan the Switches again, use the **Scan** or **Scan All** link from the **Add/Edit Switch** view.

To view the alerts generated by the Switch Port Mapper tool, click the **Alerts** tab. Alerts are generated whenever the status of the port changes from "Available to Used" or from "Transient to Available". The Alerts can also be notified through Email or by playing a sound. This can be configured from the Switch Port Mapper Settings.

Viewing Switch Port Mapping History

Whenever a switch is scanned using the Switch Port Mapper, the mapping results are published automatically as a csv file and is stored in the file system. You can change the location to publish or to disable this feature from Switch Port Mapper Settings.

When you have chosen to auto-publish the results, you can view the previous mapping results from the History tab as below:

1. Select the **History** tab from the Switch Port Mapper tool.
2. This will list the summary of all the switches scanned using Switch Port Mapper. You also have an option to filter the view based on a specific group by selecting it from the Select Group list.
3. Click the Name/IP Address of the switch to view all its previous mapping results. The date and time of previous mapping is shown for easy identification.
4. You can either choose to view or download it as a csv from here.

Exporting Switch Port Mapping Results

To export the Switch Port Mapping to a HTML or a PDF format, follow the steps below:

1. Click the **Tools Home** tab
2. Choose **Switch Port Mapper** available under the **Network Monitoring** category.
3. Click a switch whose results has to be exported to view its details.
4. Click the Export link available in the top-right.
5. Choose the format for export and click View.

You have an option to auto-publish the Switch Port Mapping results in to a CSV format. You can enable this option from Switch Port Mapper settings. When this option is enabled, OpUtils automatically publish the results in to a CSV file in the following scenarios:

1. When a scheduled scanning of Switches happen.
2. When you manually select switches and scan.

Searching a Specific Device using IP/DNS/MAC Address

When you have added all the switches and scanned once, the Switch Port Mapper can then be used to search for a specific device to locate the switch and port to which it is connected.

The Search field available in the Switch Port Mapper can be used for this purpose. The Search input can be either the Device MAC Address, IP Address, or the DNS Name. This will search all the switches that are scanned to locate the switch and port.

Mapping Devices to Physical Location

Switch Port Mapper provides an option to specify the physical location of the connected devices, which can be used for later reference.

The location of the connected devices can be manually added using the **Import Location as CSV** option when you move your mouse over the Actions label available in the **Switch Details** view. The CSV should contain the IfIndex port and its location as comma separated values and each port should be in a new line.

Note: To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.

Disabling/Enabling the Switch Interfaces

Switch Port Mapper provides an option to administratively disable or enable the switch ports.

1. From the switch details view, select the ports that you wish to disable or enable.
2. Move the mouse over the **Actions** label and select "**Administratively Disable Interfaces**" or "**Administratively Enable Interfaces**" to disable or enable a port respectively.
3. This will open the block/unblock dialog showing the selected ports.
4. Specify the **SNMP Write Community** of the switch and click **Block Port** / **Unblock Port**

Modifying ifAlias Name of the Switch Interfaces

1. From the switch details view, select the ports for which you wish to update the ifAlias Name.
2. Move the mouse over the **Actions** label and select **Modify ifAlias Name**. This will open the Modify ifAlias Name dialog showing the ifAlias Names of the selected ports.
3. Change the names as required.
4. Specify the **SNMP Write Community** of the Switch and click **Update**.

See Also

Error Messages
E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries
E1003: Not a Switch, E1004: Not a Router, E2005: Not able to retrieve complete data from the MIB, E2006: Not able to retrieve MAC Address of the Switch

Related Tools : Ping, SNMP Ping, MAC Address Resolver

IP Address Manager Tool

IP Address Manager utility of OpUtils software identifies whether an IP Address is currently available or not. The tool helps in management of the IP addresses in a static DNS environment, using pre-defined user policy. The tool scans a subnet and provides the availability status of IP addresses in that subnet. One can check whether a particular IP is used or available.

Adding Subnets for Scanning

1. Click the **IP Address Manager** tab.
2. Click the **Add/Edit Subnets** tab and click **Add Subnet** link. When you add a router from the Switch Port Mapper, Rogue Detection, or from Admin --> Add Routers, the subnets discovered in the routers will automatically be added to the IP Address Manager tool. You need to review these subnets and approve before it gets scanned.
3. Enter the Subnet or IP address of any network as input in the **Subnet/IP Address** field.
4. Select the **Subnet Mask** from the combo box.
5. Click **Add**. The subnet gets added to the table below and are automatically scanned.
6. Repeat steps 3 to 5 for adding more subnets.

IP Address Manager Settings

Schedule Subnet Scanning

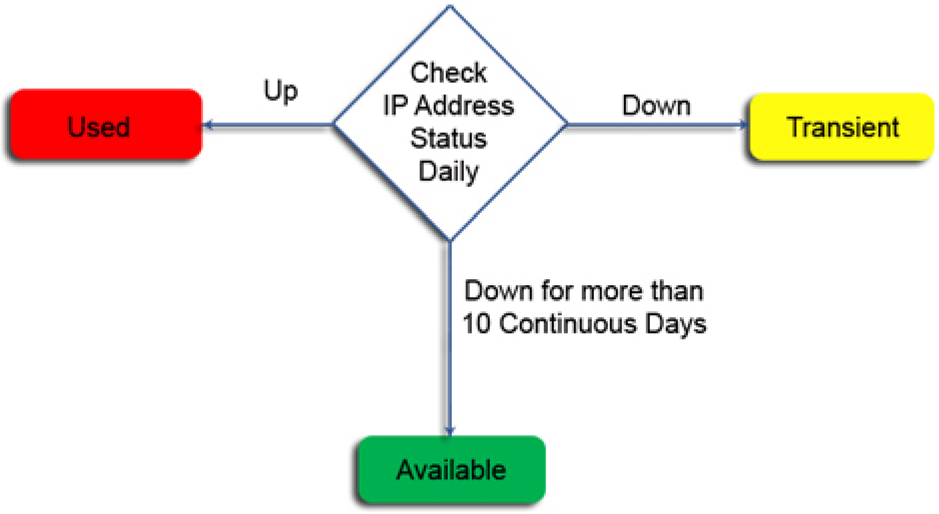
Click the **Click to Schedule** link to enable scanning of subnets periodically:

1. Change the Status to Enabled
2. Specify the interval to perform the scan:
   1. **Daily** - to update everyday. You need to specify the starting time.
   2. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
   3. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
   4. **Once Only** - to run the tool only once at the scheduled time.
3. Click **Schedule** to save the changes.

Configure Email/Sound Alerts to Notify Change in State

Alerts are generated whenever the status of the IP Address changes from "Available to Used" or from "Transient to Available". Click the Settings link to specify the period after which an IP Address has to be declared as Available and Save.

IP Address State Diagram


Used
Up
Check IP Address Status Daily
Down
Transient
Down for more than 10 Continuous Days
Available

The IP Address Manager tool can be configured to notify the change in state by email or by playing a sound:

1. Click the **Configure Alert** link. This opens the Configure Alert dialog.
2. Select the **Enable Email Alert** check box and specify the recipients email addresses as comma separated.
3. To enable sound alerts, select the **Enable Sound Alert** check box and select a sound file to be played. To play the selected sound, click the 🔊 icon. You can also import your own sound files to be played; browse to select the sound file and click OK. The imported sound file gets added to the list, which can now be selected.
4. **Alert Cleanup Policy**: Specify the maximum number of Alerts to be stored in the database, the default being 2000. When you delete the older alerts, you have an option to save them as a csv file for future reference.
5. Click **Save**.

Viewing IP Address Details

The Summary View provides the graphical representation of the Available and Used IP Addresses in a subnet. You can click the graph to view the corresponding IP Addresses. The summary is also presented in a table below the graph. The status of the IP Addresses are categorized as

- **Used IPs :** Displays the IP addresses which are currently in use. Such IP addresses should have responded to Ping in current discovery
  Tip : Such IP's should not be used when assigning addresses to new devices.
- **Available IPs :** Displays the IP addresses that are not responded. Such IP Addresses (1)should not have responded in last 10 days to ICMP request.

You can change this by clicking the **Settings** link available in the tool.
Tip : Such IP's can be assigned to new devices.
Note: When a user discovers a network for the first time, **Available IPs** will always be 0**.**

- **Transient IPs :** Displays the list of IP's that are not used in the network. Such addresses **should not have** responded to Ping in their first discovery and doesn't respond to Ping for the next 10 days.
  Tip : Such IP's cannot be assigned to new devices**.**

For each of the IP's, the other details displayed include the **Status**, the **DNS Name**, the **Last Alive Time**, and **Last Updated Time**. For SNMP-enabled devices additional details like **SysName**, **SysDescr**, **SysLocation**, and **SysOID** are retrieved and shown.

Adding Meaningful Names to IP Addresses

You can add meaningful names to the IP Addresses or can mark specific addresses to specific devices/persons manually. Follow the steps below to achieve this:

1. From the Summary View click on any subnet to view the details of the available and used IP Addresses in that subnet.
2. You will see an additional column as "**Alias Name**" with the default value as "**Not Defined**"
3. Click the Not Defined link to specify a name. This opens up a text field below to accept the name.
4. Specify the name and click **Update**. Note that the name or the description cannot exceed 100 character limit.
5. The specified name gets updated in the database.

Related Tools: **Ping**, **SNMP Ping**, **Trace Route**, **System Snapshot**

Rogue Detection Tool

Rogue Detection tool of OpUtils software helps in detecting unauthorized access of network resources. The tool scans your routers, subnets, switches, gateway servers, etc., periodically and detects the wireless / wired rogue systems, devices, Access Points, and more.

- Configuring Rogue Detection Tool
- Discovered Devices
- Trusted Devices
- Guest Devices
- Rogue Devices
- Block / Unblock Switch Ports
- Configure Alert Notifications

Configuring Rogue Detection Tool

1. Add all the routers, switches, and gateway servers, in your network from Admin -> Add Routers and schedule scanning.
2. To get the details of the Switch and Port a device is connected, map all your switches using the Switch Port Mapper tool

After successful scanning of your network, you can perform the following operations from here:

- Verify the list of discovered devices and mark all your network devices as trusted. The devices once marked as trusted, will not be listed in the Discovered tab again.
- Mark a unknown or unauthorized device as Rogue.
- Allow devices for a temporary period.
- Block the switch port to which a rogue device is connected.

Discovered Devices

OpUtils periodically scans the routers, switches, and gateway servers to discover the devices in the network. This includes all the devices in the network irrespective of whether the device is a rogue or not.

All the discovered devices are listed under the **Discovered** tab in the Rogue Detection tool. The administrator has to verify the device list and mark them accordingly. The following options are available:

- Mark the systems/devices as trusted
- Mark the systems/devices as guest to allow access for a specified period
- Mark the systems/devices as rogue and take appropriate action. The action could be to get the details of the switch and port through which the device is accessing the network and block the switch ports to stop unauthorized access.
- Configure email and sound alerts for instant notification

Trusted Devices

Trusted Devices represents the valid devices in your network. From the Discovered tab, you can select the devices and mark them as trusted so that they do not get listed in the Discovered tab again.

To Mark a Device as Trusted

1. Click the **Rogue Detection** tab.
2. Select the **Discovered** tab. This will list all the discovered devices in the network.
3. Select the valid devices and click **Mark as Trusted**. To mark all the discovered devices as valid, click **Mark All as Trusted**

The devices that are marked as trusted will be moved from the Discovered tab to the **Trusted** tab. You also have an option to mark the devices as Guest or Rogue from the **Trusted** tab.

Guest Devices

There might be situations where you need to allow certain devices to access your network resources for a temporary period. For example, a personnel from a different branch visits your office for a month or a student enrolled for a semester need to be given access till he/she completes the semester. In such cases, you can specify a period till which a particular device need to be considered as trusted.

To Allow Devices for a Temporary Period

1. Click the **Rogue Detection** tab.
2. Select the **Discovered** tab. This will list all the discovered devices in the network.
3. Select the devices that have to be given guest access and click **Mark as Guest**. This opens the Configure Guest Validity Period dialog with the details of the selected devices.
4. Specify a date until which the selected devices are valid.
5. Specify a comment or description and click **Save**.
6. The devices are moved to **Guest** tab with the specified details. You can perform the following actions from here:
    1. Mark a device as trusted
    2. Extend the validity period
    3. Block/Unblock the switch port
    4. Mark a device as rogue

Rogue Devices

To Mark a Device as Rogue

1. Click the **Rogue Detection** tab.

2. Select the **Discovered** tab. This will list all the discovered devices in the network.
3. Select the devices that have to be marked as rogue and click **Mark as Rogue**.

The devices that are marked as rogue will be moved to the **Rogue** tab. The administrator can take appropriate action and delete the device from the rogue list. If the same device is detected in subsequent scans, it will be listed here again.
You can perform the following actions from here:

1. Mark a device as trusted
2. Mark a device as guest
3. Block/Unblock Switch Ports

Important: If the device is not deleted from the rogue list, this will not get listed under the Discovered tab upon rediscovery.

Block / Unblock Switch Ports

To View the Switch Details

The details of the switch and port to which a device is connected is shown under the Switch Details column under the **Discovered** tab. The switch details could have three different values:

1. Switch IP, Switch Name, ifIndex, port, and ifName details - This refers to the actual details where a particular device is connected.
2. Learned in xyz, but not directly connected - This refers to the switches through which the device has communicated and are not connected directly to these switches.
3. Unknown - The switch details are not known. This can happen when you have not mapped all your switches using the Switch Port Mapper tool or the device is detected after scanning your switches. Mapping your switches again will show the details here.

To Block/Unblock a Switch Port

1. Select a rogue device for which you need to restrict the access by blocking the port and click **Block/Unblock Switch Port**. This opens the Block/Unblock Switch Port dialog with the details of the device and switch details.
2. Specify the SNMP Write Community of the switch and click **Block Port**.

When you block a switch port, the admin status of the port is set to "Down"

To unblock a blocked port, specify the Switch Name/IP Address, ifIndex, SNMP Write Community and click **Unblock Port**. This will set the "admin status" of the port to "Up"

Configure Alert Notifications

Alerts are generated whenever a rogue device is detected or when the temporary validity expires. The Rogue Detection tool can be configured to notify this through email or by playing a sound.

To Configure E-mail and Sound Alerts

1. Click the **Configure Alert** link. This opens the Alert Settings dialog.
2. Select the **Enable Email Alert** check box.
3. Select the **Notify when a Rogue Device is detected** option to notify whenever a rogue device is detected.
4. Select the **Notify when the Guest Validity Expires** option to notify when the guest validity period expires.
5. Specify the recipients email addresses as comma separated.
6. To enable sound alerts on detecting a Rogue device, select the **Enable Sound Alert** check box and select a sound file to be played. To play the selected sound, click the 🔊 icon. You can also import your own sound files to be played; browse to select the sound file and click OK. The imported sound file gets added to the list, which can now be selected.
7. Click **Save**.

Note: To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.

Related Tools:**Ping**, **MAC Address Resolver**, **MAC Address Scan**, **Process Scan**, **Switch Port Mapper**

MAC IP List

OpUtils periodically queries the routers and subnets defined in the Global Environment settings and collects the information, such as MAC Address, IP Address, and DNS Name of the devices and stores it in the database. The data is also updated whenever a scan is performed for a given IP range.

This data is presented in the form of a table showing the details of the collected information along with the time at which the data was updated.

To view the MAC IP List

1. Select the MAC IP List tab.
2. You can select to view the MAC-IP details of a specific subnet or search for a MAC or IP from the search box.

Related Tools: **MAC Address Resolver**, **MAC Address Scan**, **Ping**, **SNMP Ping**, **Trace Route**

Diagnostic Tools

Diagnostic Tools is a collection of generic utilities, for day-to-day management of the system and network. The tools can be used to troubleshoot, debug connectivity issues, packet loss and latency in a LAN environment.

The following are the tools available in this group

Ping : Utility to determine whether a specific IP is accessible in the network. It helps in discovery of the status of a network device; whether the device is alive or not. Before you ping a device you can configure the ping settings like number of packets, time to live, size, and timeout.

Ping Scan : Utility to scan a range of IP's to check if the given range of IP addresses are accessible. The tool displays the IP Address, the response time, and the DNS name of the discovered device. This tool uses the basic PING function as a base to perform the scan.

SNMP Ping : Utility to check if a specific IP is SNMP enabled. It helps the network engineers to know the availability of a device and also provides basic information like DNS name, system name, location, system type, and system description. Following the SNMP discovery, if required, more details of the node can be retrieved using SNMP Tools like SNMP walker, MIB Browser and SNMP Graph

SNMP Scan : Utility to scan a range of IP addresses to check if the IP Addresses are SNMP enabled or not. The tool displays the IP address, response time, DNS name, system name, and system type.

Proxy Ping : Utility to remotely initiate a PING test from a router to another IP which is remotely located. The router acts as the proxy for the target device and responds to the ping request.

Trace Route : Utility to record the route (route is calculated in terms of hops, i.e number of routers it crosses) through the network between the sender's IP and a specified destination IP. The user can configure the settings such as number of hops, and timeout value.

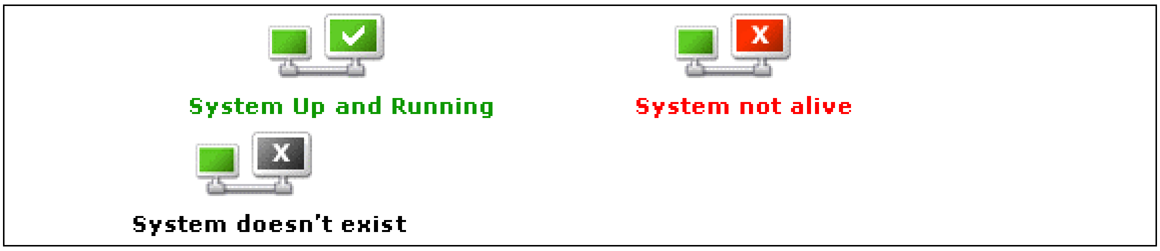
Ping Tool

Ping is the graphic implementation of the ICMP PING utility. It helps in the discovery of the status of a network device.

To check the connectivity status of an IP Address

1. Click the **Tools** tab.
2. Choose **Ping** available under the **Diagnostic Tools** category.
3. Enter the **IP Address/Host Name** to be pinged.
4. To configure ICMP properties click **Settings** located in the top right corner. For details read the Configuring ICMP section.
5. Click **Ping**.
6. Check the Ping results. The results are segregated into four sections - **Ping Status, Ping Action, Ping Statistics,** and **Graphical Representation**.

   - **Ping Status**: The status of the IP Address pinged is displayed. The status displayed are



     - **System up and Running** signifies the system is alive
     - **System not Alive** signifies the system exists in the network, but is not alive
     - **System does not exist** signifies the system does not exist in the network
   - **Ping Action**:The ping action results follow only after the Ping status is displayed. The ping action results display the number of packets sent, received, and lost, along with the maximum, minimum and average round trip time (in ms seconds).
   - **Ping Statistics**: The ping statistics table follows after the Ping Action results. The ping statistics displays the **Ping Status, Machine Name, IP Address, Packet Count, Packet Size, Time to Live, Timeout, Packets Received, Packets loss (%)** and **Round Trip Time**.
   - **Graphical Representation**: The graph represents the response time taken for the packets transmitted for the ping operation.

Related Tools : SNMP Ping, DNS Resolver, MAC Address Resolver, System Snapshot

Ping Scan Tool

Ping Scan utility of OpUtils software sweeps an entire range of IP Address to check their availability. The tool uses the basic PING function as a base to perform the sweep.

To check the connectivity status of a range of IP Addresses in a Network

1. Click the **Tools** tab.
2. Choose **Ping Scan** available under the **Diagnostic Tools** category.
3. The input to the Ping Scan tool can be any or combination of the following:
    1. **Add IP Range:** Enter the **Starting IP** and **Ending IP** in the text field provided and click **Add**. The specified range gets added to the table below.
    2. **Add IP List:** Enter the IP Addresses as comma separated values and click **Add**. You can also specify a range like 192.168.113.1-10,192.168.21-20. The specified IP Addresses gets added to the table below.
    3. **Import CSV:** Browse to select a file containing comma separated IP Addresses and click **Add**. The IP Addresses gets added to the table below.
4. To configure ICMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring ICMP section.
5. Click the **Scan** button.
6. To delete an IP Address from the table. select and click **Delete**.
7. Check the results. The results displayed include the **Total IPs**, **Responding IPs**, and **Non Responding IPs**. To view the details of each category click the respective hyperlink. The **IP Address**, **DNS Name, Response Time**, and the **Status** of the IP's are also displayed for all the above three categories. The icons and the status of the IP's are as follows:

✓	☒	☒
System up and running	**System does not exist**	**System not alive**

Related Tools : SNMP Ping, DNS Resolver, MAC Address Resolver, System Snapshot.

SNMP Ping Tool

SNMP Ping utility of OpUtils software checks whether a node is SNMP-enabled or not. The tool helps Network Engineers to know the availability of a device and also provides basic information like DNS name, System Name, Location, System Type, and System Description. Following the SNMP discovery, if required, more details of the node can be retrieved using SNMP Tools like SNMP Walker, MIB Browser and SNMP Graph.

To check for SNMP-enabled nodes

1. Click the **Tools** tab.
2. Choose **SNMP Ping** available under the **Diagnostic Tools** category.
3. Enter the **IP Address/Host Name.**
4. Enter the SNMP **Community** string in the text field provided.
5. To configure ICMP and SNMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring ICMP and Configuring SNMP section.
6. Click the **SNMP Ping** button.
7. Check the results. The results include the **Status** (SNMP-enabled or non-SNMP), **IP Address**, **DNS Name**, **Response Time**, **Location**, **Contacts**, **System Name**, **System Type** (the OS) and **System Description** of the IP Address.

Hints and Tips

To install SNMP for non-SNMP enabled nodes, read the Installing SNMP section.

Related Tools : System Snapshot, Disk Space Monitor, Process Scan, IP Node Browser

SNMP Scan Tool

SNMP Scan utility of OpUtils software sweeps an entire range of IP Addresses using SNMP ping and check for their availability.

To check a range of IP Addresses for SNMP-enabled nodes

1. Click the **Tools** tab.
2. Choose **SNMP Scan** available under the **Diagnostic Tools** category.
3. The input to the SNMP Scan tool can be any or combination of the following:
    1. **Add IP Range:** Enter the **Starting IP** and **Ending IP** in the text field provided and click **Add**. The specified range gets added to the table below.
    2. **Add IP List:** Enter the IP Addresses as comma separated values and click **Add**. You can also specify a range like 192.168.113.1-10,192.168.21-20. The specified IP Addresses gets added to the table below.
    3. **Import CSV:** Browse to select a file containing comma separated IP Addresses and click **Add**. The IP Addresses gets added to the table below.
4. To configure ICMP and SNMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring ICMP and Configuring SNMP section.
5. Click the **Scan** button.
6. To delete an IP Address from the table. select and click **Delete**.
7. Check the results. The results displayed includes, **All Nodes** total, along with the total number of **SNMP Nodes**, **Non-SNMP Nodes** and **Non Responding Nodes**. The **Non Responding Nodes** results include the IP addresses that does not exist in the network and those are not alive in the network. Click the respective hyperlinks to view the details in a table. The table displays the **IP Address, DNS Name, Response Time**, **System Type**, and the **Status** of the device. The following icons represent the status of the IP's scanned.

🟩	🟥	☒	☒
SNMP Node	**Non- SNMP Node**	**System does not exist**	**System not alive**

Hints and Tips

To install SNMP for non-SNMP enabled nodes read the Installing SNMP section.

Related Tools: DNS Scan, MAC Address Scan, System Snapshot, Disk Space Monitor

Proxy Ping Tool

Proxy Ping utility of OpUtils software is used to ping a target device using a Cisco router. The router acts as the proxy for the target device and responds to the ping request.

To check the connectivity status of a remote IP Address/Host from a Router

1. Click the **Tools** tab.
2. Choose **Proxy Ping** available under the **Diagnostic Tools** category.
3. Enter the **Proxy Router Name/IP Address** from where the Ping has to be initiated.
4. Enter the Router's **Write Community** String.
5. To configure SNMP properties for the router, click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring SNMP section.
6. Enter the **IP Address /Host Name** of the device to be contacted or select the IP Address/Host Name from the available list.
7. To change the Proxy Ping default settings click the **Settings** button, and specify values for the following:
   - **Number of Pings** - Enter the number of packets to be sent to the remote device from the CISCO router. The number of pings should be between 1 to 100.
   - **Packet Size** - Enter the size of the packets to be sent to the remote device. The packet size should be between 32 to 4096 bytes.
   - **Ping Delay** - The time in milliseconds between each successive Ping to the target IP address. The lesser the time specified the more the Pings to the target IP address.
   - **Timeout** (ms) - Enter the maximum time in milliseconds(ms) that a packet can wait/remain in the network before reaching its destination, after which the packet is discarded.
   - **Server Timeout** - Enter the maximum time in milliseconds that the Server should wait to get the Ping Result from the Cisco router
   - Click **Save** to save the values. To maintain the default values click **Restore Defaults**.

7. Click the **Ping** button.

8. Check the results. For devices that are not reachable, the target device is displayed in red. For targets that are reachable the Target device is shown in green.

9. The **Round Trip Time**, **Sent Packets,** and **Received Packets** along with the **Packet Loss Percentage** are also displayed in the table.

Note: The Ping test will work only from SNMP-enabled CISCO routers.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2003: Unable to perform SNMP Set, E2001 No Response to SNMP Queries, E4001: Not a CISCO Router, E3001 Operation timed out

Related Tools: DNS Resolver, MAC Address Resolver, System Snapshot, Router Snapshot

Trace Route Tool

Trace Route utility of OpUtils software records the route followed in the network between the sender's computer and a specific destination computer.

To track the Route and the number of hops taken to traverse from the Host to the Target

1. Click the **Tools** tab.
2. Choose **Trace Route** available under the **Diagnostic Tools** category.
3. Enter the **IP Address/Host Name** from which the route has to be traced.
4. Enter the **Maximum Hops** the packets should traverse before reaching the destination.
5. Enter the **Timeout** period in seconds, when the packet should be considered as expired and can be discarded.
6. To configure ICMP properties click **Settings** located in the top right corner or click **Admin -> Settings**. For details read the Configuring ICMP section.
7. Click the **Trace** button.
8. Check the results. The Trace Route results show the path that the TCP/IP packets take to reach a given destination, entered as an IP address or domain name. The results display the **Number of routers/hops** that the packets traverse before they reach the destination address/host, the **IP Address**, **DNS Name** and the **Response Time** taken for each hop. As three packets are sent for each hop, the response time taken for all the three hops are displayed in the result table.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host

Related Tools: **SNMP Ping**, **DNS Resolver**, **MAC Address Resolver**, **System Snapshot**.

Address Monitoring Tools

The Address Monitoring Utilities is a suite of tools for day-to-day monitoring and management of IP Addresses, DNS Names, and MAC Addresses.

The following are the tools available in this group

DNS Resolver : A general-purpose data query tool chiefly used for translating Host Name into IP Address and vice versa. It also shows details like the default netmask, network type, and the status for the forward and reverse lookups.

DNS Scan :Utility to scan a range of IP addresses for translating the IP Address into Domain Name. It also shows the response time. In cases where an IP is not used in the network, the tool prompts thatthe system does not exist in the network.

MAC Address Resolver :Utility to resolve MAC Address from Host Name or IP Address and vice versa. This tool also discovers the physical address of a device and maps it with the corresponding IP address. In addition to showing the MAC address, the tool also shows the SNMP availability, IP address, DNS name, port number, community, system type, and system description

MAC Address Scan :Utility to lookup MAC addresses for a range of IP's. The tool also displays the IP address, port number, community, MAC address, DNS name, system name, and system type

DHCP Scope Monitor : Utility to find the used and available IP addresses in the scopes of the DHCP Server

DNS Resolver Tool

DNS Resolver utility of OpUtils software fetches the host name of any node whose IP Address is known and vice versa.

To translate IP Address into Host Name and vice versa

1. Click the **Tools** tab.
2. Choose **DNS Resolver** available under the **Address Monitoring** category.
3. Enter the **IP Address** or the **Host Name** in the text field provided.
4. To configure ICMP properties click **Settings** located in the top right corner or click **Admin -> Settings**. For details read the Configuring ICMP section.
5. Click the **Resolve** button.
6. Check the results. The results include the **Host Name**, **IP Address**, **Status** (displays **Reverse** and **Forward Look up** of the address along with the information of ping status of the device), **Virtual Host of**, **Default Netmask, Network Type** and the **Response Time.**

What do the Results tell you?

Check the Reverse and Forward Lookup results. Issues in the results indicate problems with the DNS Server. In cases of web sites, if DNS fails, the web sites cannot be located and e-mail delivery stalls.

Related Tools:**Ping**, **SNMP Ping**, **Trace Route**

DNS Scan Tool

DNS Scan utility of OpUtils software scans a range of IP addresses to check the forward and reverse lookup actions.

To check Forward and Reverse Lookup for a specified range of IP addresses

1. Click the **Tools** tab
2. Choose **DNS Scan** available under the **Address Monitoring** category.
3. The input to the DNS Scan tool can be any or combination of the following:
    1. **Add IP Range:** Enter the **Starting IP** and **Ending IP** in the text field provided and click **Add**. The specified range gets added to the table below.
    2. **Add IP List:** Enter the IP Addresses as comma separated values and click **Add**. You can also specify a range like 192.168.113.1-10,192.168.21-20. The specified IP Addresses gets added to the table below.
    3. **Import CSV:** Browse to select a file containing comma separated IP Addresses and click **Add**. The IP Addresses gets added to the table below.
4. To configure ICMP properties click **Settings** located in the top right corner or click **Admin -> Settings**. For details read the Configuring ICMP section.
5. Click **Scan**.
6. To delete an IP Address from the table. select and click **Delete**.
7. Check the results. The **IP Address**, **IP -> DNS**, **DNS -> IP**, the **Forward Lookup** and **Reverse Lookup** status, the **Lookup Time** and the current ping **Status** of the IP are displayed. The icons displaying the current ping status of the IP's are as follows:

✓ **System exists in the network**	✗ **System does not exist in the network**

Related Tools: **Ping**, **Ping Scan**, **SNMP Scan**

MAC Address Resolver Tool

MAC Address Resolver utility of OpUtils software fetches the MAC Address for any SNMP-enabled node, based on the IP Address. The tool also discovers the physical address of a device and maps it with the corresponding IP address.

To resolve a MAC Address

1. Click the **Tools** tab.
2. Choose **MAC Address Resolver** available under the **Address Monitoring** category.
3. You have an option to resolve either a MAC from an IP or an IP from MAC. Select the required tab.
4. Based on the selected tab, enter the **IP Address/Host Name** of the device and the SNMP **Community** string or the **MAC Address**.
5. To configure ICMP and SNMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring ICMP and Configuring SNMP section.
6. Click the **Resolve** button.
7. Check the results. The results include the **MAC Address Status, SNMP Status, IP Address**, **DNS Name**, **MAC Address, Network Interface Card Type (NIC Type)**, the **Port** where the resource is connected, the **System Object ID**, **System Name, System Type,** and **System Description**.

Note:
Windows OS Users: Non SNMP- enabled nodes will not be resolved if the Server is running in Windows and the input provided is a Windows IP. To resolve the issue, ensure the IP is SNMP enabled. For details on installing SNMP in windows, read the Installing SNMP on Windows section.

Related Tools: **Ping**, **SNMP Ping**, **Trace Route**

MAC Address Scan Tool

MAC Address Scan utility of OpUtils software scans a given range of IP Addresses and display the MAC addresses for various devices available in the given range.

To resolve MAC Address for a range of IP Addresses

1. Click the **Tools** tab.
2. Choose **MAC Address Scan** available under the **Address Monitoring** category.
3. The input to the MAC Address Scan tool can be any or combination of the following:
    1. **Add IP Range:** Enter the **Starting IP** and **Ending IP** in the text field provided and click **Add**. The specified range gets added to the table below.
    2. **Add IP List:** Enter the IP Addresses as comma separated values and click **Add**. You can also specify a range like 192.168.113.1-10,192.168.21-20. The specified IP Addresses gets added to the table below.
    3. **Import CSV:** Browse to select a file containing comma separated IP Addresses and click **Add**. The IP Addresses gets added to the table below.
4. Check the **Use Cache** check box to retrieve details from the cache without scanning the whole range.
5. To configure ICMP and SNMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring ICMP and Configuring SNMP section.
6. Click the **Scan** button.
7. To delete an IP Address from the table. select and click **Delete**.
8. Check the Results**.** The results include the **IP Address, the DNS Name, the MAC Address**, the **Network Interface Card Type (NIC Type)**, and the **System Type** of each IP scanned**.**

Note: Windows OS Users: Non-SNMP-enabled nodes will not be resolved if the Server is running in Windows and an Windows IP is included in the range specified. To resolve the issue, ensure the non-SNMP IP is SNMP enabled. For details on installing SNMP in Windows read the Installing SNMP on Windows section.

Related Tools:**Ping**, **Ping Scan**, **SNMP Scan**

DHCP Scope Monitor

The DHCP Scope Monitor utility of the OpUtils software helps you to monitor the DHCP Scopes to find the available IP Address count in each of them. When the available IP Address count falls below a certain number, the results are shown in red color.

- Adding DHCP Servers to be Monitored
- DHCP Scope Monitor Settings
    - Schedule Monitoring of Scopes
    - Configure Email Alerts
- Viewing DHCP Scope Details

Adding DHCP Servers to be Monitored

1. Click the **Tools** tab.
2. Choose the **DHCP Scope Monitor** available under the Address Monitoring category.
3. Specify the **Name** or the **IP Address** of the DHCP Server.
4. Specify the **SNMP Read Community** of the DHCP Server.
5. Click Get DHCP Scope Details.
6. Repeat steps 3 to 5 for adding the scopes of all the DHCP Servers.

All the scopes of the added DHCP Servers along with their current available and used IP Address counts are retrieved and shown in the table below.

DHCP Scope Monitor Settings

Schedule Monitoring of Scopes

1. Click the **Settings** link to open the settings page.
2. Select the **Scheduler** tab.
3. Change the Status to **Enabled**
4. Specify the interval to perform the scan:
    1. **Daily** - to update everyday. You need to specify the starting time.
    2. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
    3. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
    4. **Once Only** - to run the tool only once at the scheduled time.
5. Click **Schedule** to save the changes.

Configuring Email Alerts

Alerts are generated when the available address count in scope falls below the specified value.

1. Click the **Settings** link to open the settings page.
2. Select the **Alert** tab
3. An email alert is generated when the available IP Addresses in a scope falls below 5. Specify a different value if required.
4. Select the Enable Email Alert check box and specify the email addresses as comma separated values.
5. To enable sound alerts, select the **Enable Sound Alert** check box and select a sound file to be played. To play the selected sound, click the 🔊 icon.
6. **Alert Cleanup Policy**: Specify the maximum number of Alerts to be stored in the database, the default being 2000. When you delete the older alerts, you have an option to save them as a csv file for future reference.
7. Click **Save** to save the changes.

Viewing DHCP Scope Details

The Summary view provides the details of the DHCP Scopes of all the DHCP Servers that are being monitored with the following details:

1. **Server IP**: The IP Address of the DHCP Server
2. **Scope Name**: The name of the DHCP Scope
3. **Used**: The number of used IP Addresses in that scope
4. **Available**: The number of available IP Addresses in that scope
5. **Size**: The total number of IP Addresses in that scope.
6. **Last Update Time**: The time at which the data was retrieved from the DHCP Server

To view the details of a specific DHCP Server, select the server from the combo box. To retrieve the current values, select the DHCP Server and click **Refresh**. Select **All** to view / refresh all the DHCP Servers.

To delete all the scopes of a DHCP Server, select the server and click **Delete**.

To export the scope details, select the DHCP Server and click **Export** and choose an appropriate format.

Top

Related Tools: **IP Address Manager**, **Switch Port Mapper**, **DNS Resolver**, **System Snapshot**

Network Monitoring Tools

Network Monitoring Utilities consists of tools to monitor the performance of Routers, Switches and other such devices. The tools provide graphical views of the monitored statistics.

Bandwidth Monitor : Utility to check the bandwidth utilization of a Switch. The Tool is ideal for identifying bottlenecks related to bandwidth within the network. This tool monitors the average BPS and percentage utilization of all the interfaces existing in the specified device. The tool shows the output in a graphical form.

Network Monitor : Utility to monitor the response time of multiple devices. The tool continuously monitors the response time of multiple devices and generates email alerts based on the severity. These alerts are set up at three different levels and displays the different status of the nodes

Wake-on-LAN : Utility to remotely power on a PC. For the tool to work, the PC should be configured to accept the Wake-On-LAN remote command.

Port Scanner : Utility to scan the TCP ports of a given range of IP Addresses to check whether the port is occupied or not.

System Details Update : Utility to view and update the details, such as Name, Location, and Contact details.

System Explorer : Utility to scan a SNMP-enabled device to get its complete details like system snapshot, CPU usage, Disk Space details , running processes, and installed software.

TCP Reset : Utility to find and reset the list of TCP connections established with the switches, routers, etc., in the network.

Bandwidth Monitor Tool

Bandwidth Monitor utility of OpUtils software provides a graphical view of real time traffic in a device. The Bandwidth Tool is ideal for identifying bottlenecks related to bandwidth within the network. You can monitor the network traffic utilization/ bandwidth usage both at the interface level and at the device level.

Adding Interfaces for Bandwidth Monitoring

1. Click the **Add Devices** link
2. Specify the Device IP Address/Name and its SNMP community in the respective fields and click **Get Interfaces**.
3. This will list all the available interfaces of the device along with its status and speed. The auto-detected SNMP version is also shown. You also have an option to choose an interval to monitor the interface, the default being 1 year. Select the interfaces to be monitored and click **Add Interface**.
4. The selected interface gets added for monitoring network traffic.
5. Repeat steps 2 & 3 for adding more interfaces.

Note: Bandwidth Monitoring of all the interfaces will happen at an pre-defined interval of 5 minutes. The In and Out bandwidth utilization values in the summary view will appear in the next polling cycle, i.e., after 5 minutes, which will be the cumulative bandwidth utilization value in the past 5 minutes.

Viewing Bandwidth Utilization Details

Summary View

The Summary View provides the details of the monitored interfaces along with their status, speed, and current in/out network bandwidth utilization details.

Clicking the interface link (ifName) will show the graphical representation of network bandwidth utilization for the last one hour, last one day, last one month, and last one year. A link to view the tabular data is also provided below each graphs.

To modify the Monitor Until period, click the Modify link corresponding to that interface and select a different period. Monitoring will continue till the selected period from the time of modification.

To delete an interface from being monitored, click Delete link corresponding to that interface.

Detailed View

To view the detailed network traffic for an interface:

1. Click a interface link from the Summary View.
2. Select the Detail Traffic tab to view its complete details

Select the Volume, Speed, Utilization, and Packets tab to view the corresponding information. The details provides both the graphical and tabular data of the selected parameter for the last one hour, last one day, last one month, and last one year. You can choose the period from the combo box.

Device-level Comparison

\Device-level network traffic comparison provides a graphical representation of the each of the interfaces of the selected device in a multi-line graph. This gives an immediate picture of the most bandwidth consuming interface of a device in the network. The comparison is provided for the following periods, each in separate tabs:

- **Current** - Comparison based on the current network traffic utilization values
- **Daily Traffic** - Based on the last one day network traffic utilization
- **Monthly** - Based on the last one month network traffic utilization
- **Yearly** - Based on the last one year network traffic utilization

Configuring Email and Sound Alerts

The Bandwidth Monitor tool measures and generates alerts whenever the network bandwidth utilization criteria is exceeded. The Bandwidth Monitor tool can be configured to notify these alerts through email or by playing a sound. Given below are the steps to configure:

1. Click the **Configure Alert** link available in the Bandwidth Monitor tool.
2. Select the device for which you wish to configure alerts. To configure alerts for all the devices, select **All** from the list.
3. Specify the Alert Criteria. Alerts will be generated by the Bandwidth Monitor tool based on the defined criteria.
4. To be notified by email, select the **Enable Email Alert** check box and specify the recipient email addresses as comma separated. You can have different email recipients for different devices.
5. Click **Save**.

Note: To enable email notifications, you should configure the SMTP properties. Refer to Configuring SNMP Properties topic for details.

To enable sound alerts, select the **Enable Sound Alerts** check box available under **Global Sound Alert Configuration**, select the sound to be played for different severity levels, and **Save**. It may be noted that the sound alert configuration applies commonly for all the devices added in the Bandwidth Monitor tool and not device-specific. To play the selected sound, click the 🔊 icon.

Alert Cleanup Policy: Specify the maximum number of Alerts to be stored in the database, the default being 2000. When you delete the older alerts, you have an option to save them as a csv file for future reference.

Exporting Bandwidth Utilization Reports

The Network Bandwidth Utilization Reports can be exported to PDF, XLS and CSV formats. To export the data, click the Export link from the top-right and select a format to export. This will export the data that is currently being viewed in the Bandwidth Monitor tool. The network traffic usage details from the Summary view, the details view, and the comparison view can be exported to the desired formats.

See Also

Error Messages
E1001: Unknown Host, **E1002: Unreachable Host**, **E2001: No Response to SNMP Queries**.

Related Tools:**Ping**, **SNMP Ping**, **SNMP Graph**

Network Monitor Tool

Network Monitor utility of OpUtils software continuously monitors the response time and packet loss of multiple devices, and generates email alerts, based on the severity.

- Adding Devices for Availability Monitoring
- Configuring Alerts
  - Configuring Email Alerts
  - Configuring Sound Alerts
  - Modifying Email Templates
  - Alert Cleanup Policy
- Viewing Alert History of a Device

Adding Devices for Availability Monitoring

1. Click the **Tools Home** tab.
2. Choose **Network Monitor** available under the **Network Monitoring** category.
3. Click the Add Host link.
4. Enter the IP Address or the Host Name to be monitored and click **Add**. To add multiple IP Addresses or Host Names follow the same procedure. The **Host Data** table gets updated simultaneously. The Host Data table displays details of the Host such as **IP Address**, **DNS Name**, **Status**, **Response Time**, **Added Time**, **Last Update Time**, **Alias Name, Sys Name, Sys Description, Sys Location,** and the **Community**. The three status displayed are 🟢 Normal, 🔴 Critical, and ⚠ Warning. You can select to choose the columns to view. The value for the columns Alias Name, Sys Name, Sys Description, Sys Location, and Community is based on the results obtained during the IP Address Manager scans.
5. Specify the monitoring interval by selecting the appropriate option from the Monitor every combo box.
6. To configure ICMP and SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring ICMP and Configuring SNMP section.

Configuring Alerts

Alerts are generated in the Network Monitor tool in the following cases:

- When the response time exceeds a defined limit (Warning Alert)
- When a device do not respond to a ping (Critical Alert).
- When the device becomes normal (Normal Alert).

Configuring Email Alerts

The Network Monitor tool can be configured to notify these alerts through email. Given below are the steps to configure:

1. Click the **Configure Alert** link available in the Network Monitor tool.
2. Select the **Alert Rule** tab.

3. Select the device for which you wish to configure alerts. To configure alerts for all the devices, select **All** from the list.
4. Specify the Alert Criteria. Alerts will be generated by the Network Monitor tool based on the defined criteria.
5. To be notified by email, select the **Enable Email Alert** check box and specify the recipient email addresses as comma separated. You can have different email recipients for different devices.
6. Click **Save**.

Note: To enable email notifications, you should configure the SMTP properties. Refer to Configuring SNMP Properties topic for details.

Configuring Sound Alerts

To configure Sound Alerts, follow the steps below:

1. Click the **Configure Alert** link available in the Network Monitor tool.
2. Select the **Sound Alert** tab.
3. Select the Enable Sound Alert check box and select the sound to be played for different severity levels. To play the selected sound, click the 🔊 icon.
4. Click **Save**.

Note: Sound alerts work only with Internet Explorer browser and applies commonly to all devices added in the Network Monitor tool.

Modifying Email Templates

The Network Monitor tool allows you to modify the email contents that are sent on occurrence of an alert. You can choose to modify both the mail subject and the message to suit your need. To modify the email templates, follow the steps below:

1. Click the **Configure Alert** link available in the Network Monitor tool.
2. Select the **Email Template** tab.
3. Select the Alert severity.
4. Modify the Alert Subject and Contents as required. You can choose the message and subject variables to be include in the subject/message, which will be replaced with the appropriate value while sending the email.
5. To modify the templates for other severity levels, follow the same procedure.
6. Click **Save** to save the changes.

Note: The Email templates applies commonly to all devices added in the Network Monitor tool and are not device-specific.

Alert Cleanup Policy

1. Click the **Configure Alert** link available in the Network Monitor tool.
2. Select the **Alert Cleanup** tab
3. Specify the maximum number of Alerts to be stored in the database, the default being 2000.
4. Specify whether to save the deleted alerts in a csv file.
5. Click **Save**.

Note: The alert cleanup policy apply globally to all the devices added in the Network Monitor tool.

Viewing Alert History of a Device

Alerts are generated whenever there is a change in severity for a particular device. While the top 20 Alerts are displayed at the bottom of the Host Data table, the complete alert history of the devices are stored in the database. To view the alert history of the Host click the **IP Address** link from the Host Data table.

Note: Alerts, from the Network Monitor tool, will be deleted when you choose to delete the alerts from the Global Alerts view.

Wake-On-LAN Tool

The Wake-On-LAN utility of OpUtils software remotely 'wakes-up' (boots up) a machine that is present in the network but not alive. For the tool to work, the PC should be configured to accept the Wake-On-LAN remote command.

- Configuring Wake on LAN
- Manually Waking Up a PC from Remote
- Schedule Waking Up PCs from Remote
  - Create a Wake on LAN Task
  - View the Status of each Tasks
  - Modify a Wake on LAN Task
  - Delete a Wake on LAN Task

Configuring Wake on LAN

BIOS Settings

The Wake-On-LAN functionality is generally disabled by default. The option to enable Wake-On-LAN is different with each computer manufacturer. The most common method adopted across different PC's are as follows:

1. During the computer's power-on self-test enter the BIOS setting screen by pressing the F1, INS, or DEL keys.
2. Select **Power** settings. Check for **Power Up Control**.
3. Enable settings related to Power Up on PCI card, LAN, or Network.
4. Click **Save** and exit the BIOS settings.

Operating System (OS) Settings

In some Windows OS, the drivers can enable the Wake ON LAN features of network adapters. For example in Windows 2000, click Power Management tab and under the **Adapters** properties, select the option **Allow this device to bring the computer out of standby**.

Alternatively, you can also check the **Advanced** setting table for parameters related to Wake on LAN and Waking on "Magic Packets" and enable them.

Wake-On-LAN (WOL) Cable

For Wake On LAN to work on computers with older PCI busses, a WOL cable must be installed between the Network Card and the Motherboard. Because this requires opening the computer case, we advice you to contact your PC manufacturer for specific instructions.

Enabling Directed Broadcasts on your Network

To send WOL packets from remote networks, the routers must be configured to allow directed broadcasts. To know if the IP broadcast packets have been disabled, check for the line "no ip directed-broadcast" in the interface configuration. If IP broadcasts are enabled, the line “no ip directed-broadcast” will not be present.

Manually Waking Up a PC from Remote

1. Click the **Tools** tab
2. Choose **Wake-On-LAN** available under the **Network Monitoring** category.
3. The Wake Up Now tab is selected by default.
4. You can either manually add the hosts that have to be powered on or choose from the available list. The list is updated based on the input given in the Global Environment settings. Click **Add Computers** and select the required option.
5. Based on the option selected above, enter the **IP Address** of the PC to be powered on, its corresponding **MAC Address**, and the **Subnet Mask** or select the hosts from the list. When you are selecting the hosts from the list, if the corresponding subnets of the machines are defined in the Global Environment, the Network Address and the Subnet Mask are automatically added. Else, you have to specify these values by clicking the **Apply Subnet Address** link before adding the machines from the list.
6. Click **Add**. For accurate results ensure
   - The IP Address is available in the network
   - The Wake-On-LAN command is enabled in the system. To enable Wake-On-LAN command read the section **Configuring Wake-On-LAN**.
7. Click the Settings link to specify the time to wait to check the status of the computers and whether to broadcast a WOL packet in the whole subnet. Broadcasting the WOL packet will produce better results.
8. To configure ICMP properties click **Settings** located in the top right corner or click **Admin -> Settings**. For details read the **Configuring ICMP** section.
9. After adding all the hosts, click the **Wake Up** button.

Schedule Waking Up PCs from Remote

You can create and schedule wake on lan tasks by selecting the Schedule Wake Up tab.

- Create a Wake on LAN Task
- View the Status of each Tasks
- Modify a Wake on LAN Task
- Delete a Wake on LAN Task

Create a Wake on LAN Task

1. Click **Add Task** to create a scheduled task and specify the following:
   1. A name for this task.
   2. Time to wait after executing a task to check the status of the computers.
   3. The use broad cast option when enabled will broadcast the WOL packets in the whole subnet. This will produce better results.
   4. Add Computers for this task either manually or from the list. The list is updated based on the input given in the Global

Environment settings. Click **Add Computers** and select the required option.

5. Based on the option selected above, enter the **IP Address** of the PC to be powered on, its corresponding **MAC Address**, and the **Subnet Mask** or select the hosts from the list. When you are selecting the hosts from the list, if the corresponding subnets of the machines are defined in the Global Environment, the Network Address and the Subnet Mask are automatically added. Else, you have to specify these values by clicking the **Apply Subnet Address** link before adding the machines from the list.
6. Select Enable to schedule this task and specify the scheduler details:
    1. **Daily** - to update everyday. You need to specify the starting time.
    2. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
    3. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
    4. **Once Only** - to run the tool only once at the scheduled time.
7. Click **Submit** to save the task. The task gets added to the table.

2. Repeat step 1 for creating more tasks.
3. The tasks will get executed at the specified time and the status gets updated.

View the Status of each Tasks

The wake on lan tasks gets executed at the schedule time and the status of the individual computers gets updated. To view the status of each task:

1. Select the **Schedule Wake Up** tab.
2. This will list all the tasks that are created with the details like **Last Wake On Time**, **Task Summary**, **Next Schedule At**, etc.
3. Clicking the task name will list the status of each computer in that task.
4. You can also modify or run the task from the task details view.

Modify a Wake on LAN Task

To modify a task, follow the steps below:

1. Select the **Schedule Wake Up** tab.
2. This will list all the tasks that are created with the details like **Last Wake On Time**, **Task Summary**, **Next Schedule At**, etc.
3. Click the modify icon from the actions column of a particular task.
4. Modify the task and click **Submit**.

Delete a Wake on LAN Task

To delete a task,

1. Select the **Schedule Wake Up** tab.
2. This will list all the tasks that are created with the details like **Last Wake On Time**, **Task Summary**, **Next Schedule At**, etc.
3. Click the delete icon from the he actions column of a particular task.
4. Click **OK** to confirm.
5. The task gets deleted from the table.

Error Message : E1001: Unknown Host, E1005 : MAC not available in cache

Related Tools: **Ping**, **SNMP Ping**, **MAC Address Resolver**

Port Scanner Tool

The Port Scanner utility of OpUtils software scans the TCP ports of the given IP Adddress and provides you the details of the ports that have been occupied. You have the option to associate the known applications/services with the ports, which enables you to identify the unwanted/unknown services running in the system easily.

To Scan the Ports of a range of IP Addresses in a Network

1. Click the **Tools** tab.
2. Choose **Port Scanner** available under the **Network Monitoring** category.
3. You can either scan a range of IP Addresses or a single IP Address. When scanning a range, you can only specify up to five ports. Select the required option.
4. Based on the option selected, specify a IP range or a single IP Address.
5. Specify the **Port Range**.
6. Some of the known services are associated with their default port numbers. Click **Configure** to either modify or to add new services to this list.
7. Click **Scan**.
8. Check the results. The IP Address and the status of the port as listening or not listening is shown. The icons and the status of the IP's are as follows:
    - ✓- Represents listening ports
    - ✗- Represents the nodes are responding but the port is not occupied.
    - ☒- Represents non-responding or nonexistent IP's.

Related Tools: **Ping**, **Ping Scan**, **Process Scan**, **Software Scan**

System Details Update

The System Details Update utility of OpUtils software enables you to view and update the system details, such as Name, Location, and Contact.

To view the System Details

1. Click the **Tools** tab
2. Choose **System Details Update** available under **Network Monitoring** category.
3. You have an option to view the details for a range of IP Addresses or for a single device. Select the required tab.
4. Based on the selected tab specify the start and end IP Addresses or the IP Address/ Host Name of the device.
5. Specify the SNMP Community string
6. Click **Get System Details**.
7. The system details are displayed.

To update the System Details

1. From the results of the system details, click the ✎ icon for the device you wish to update.
2. Change the details as required and click the 💾 icon. Please note that you should specify the SNMP Write Community to update the details.
3. Repeat the above steps for modifying the details of all the required devices.
4. After modifying the details, select the devices by selecting the check box and click **Update**. This will update the details in the device and shows the status.

Related Tools : Ping, SNMP Ping, System Snapshot, Process Scan, Software Scan

System Explorer

System Explorer utility of OpUtils software will scan any SNMP-enabled device to get its complete details, like system snapshot, CPU usage, Disk Space details , running processes, and installed software.

To get the System Details

1. Click the **Tools** tab
2. Choose the **System Explorer** available under the **Network Monitoring** category.
3. Enter the **IP Address** or the **Host Name** of the device in the IP Address/Host Name field.
4. Enter the SNMP **Community String**.
5. Click **Show**
6. The device snapshot is displayed. Select the required parameter from the tree to view the details.

The System Explorer provides the following details of a device:

1. System Snapshot
2. Disk Space Monitor
3. CPU Monitor
4. Process Scan
5. Software Scan

System Snapshot Tool

System Snapshot utility of OpUtils software provides the System Details, Address details and OS details of any SNMP-enabled node.

To get a Server Snapshot

1. Click the **Tools** tab
2. Choose the **System Explorer** available under **Network Monitoring** category.
3. Select the **System Snapshot** from the tree
4. Enter the **IP Address** or the **Host Name** of the device in the IP Address/Host Name field.
5. Enter the SNMP **Community String**.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. System data are displayed in four tables
    - **System Details**: Displays the **System Name**, **Location, Contact Address, Up Time** (i.e., the time from the last reboot) the **Number of Services** (running in the desktop), **Is Router** details and **System Object ID.**
    - **Address Details**: Displays the **IP Address**, **DNS Name**, and **MAC Address** of the device.
    - **OS Details**: Displays information about the **OS Name** and the **OS** description.

Note: The given server should be SNMP enabled and agent running in the device should support the HOST-RESOURCE-MIB.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001 No Response to SNMP Queries

Related Tools: **Ping**, **SNMP Ping**, **SNMP Graph**, **Disk Space Monitor**

Disk Space Monitor Tool

Disk Space Monitor utility of OpUtils software provides information on disk space utilization.

To check a Server's Hard disk space usage

1. Click the **Tools** tab
2. Choose the **System Explorer** available under **Network Monitoring** category.
3. Select the **Disk Space Monitor** from the tree
4. Enter either the **IP Address or the Host Name** of the device in the text field.
5. Enter the **SNMP Community** String.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin ->Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The System Space Summary displays details in a table and a graph for easy understanding. The table displays the Drive Name, the Total Space, Used Space and the Available disk space in GB. The adjacent pie-chart graphically displays the total used space and the available disk space.

Note: To retrieve data, the system should be SNMP enabled and the SNMP agent should have implemented HOST-RESOURCES-MIB.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries , E2002: OID not Implemented.

Related Tools: **Ping**, **SNMP Ping**, **DNS Resolver**, **SNMP Graph**, **CPU Monitor**

CPU Monitor Tool

CPU Monitor utility of OpUtils software is used to plot the real time CPU usage of any given node and display the CPU usage history graphically.

To monitor a Server's CPU usage

1. Click the **Tools** tab
2. Choose the **System Explorer** available under **Network Monitoring** category.
3. Select the **CPU Monitor** from the tree
4. Enter either the **IP Address** or the **Host Name** of the device in the text field.
5. Enter the SNMP **Community String**.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. To configure Graph settings such as the polling interval and number of plots, follow the same steps as given above. For more read the section Configuring Graphs
8. Click the **Show** button.
9. Set the **Refresh** period in seconds from the **Refresh Every** combo. By default the screen is refreshed every 5 seconds.
10. Check the results. The System Space summary of the desktop is categorized as
    - **CPU Usage** :Displays the current usage in percentage.
    - **CPU usage History** :Displays a graph of the **CPU usage** in percentage, over a period of time in seconds.
    - **OS Details :** Displays details of the operating system installed in the system. The results include the **OS type**, the number of **Services** installed in the system, and the **Hardware Information**.
    - **System Details :** Displays the details of the resource. The results include the Machine Name, the Up Time, and the location of the desktop. Click on the Machine Name link to view the SNMP ping results.

Note:

1. To retrieve data, the system should be SNMP enabled and the SNMP agent should have implemented HOST-RESOURCES-MIB.
2. Choose the Refresh time interval in seconds from the **Refresh every** list box. The page is refreshed based on the selected time interval.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries , E2002: OID not Implemented.

Related Tools:**Ping**, **SNMP Ping**, **SNMP Graph**, **Process Scan**

Process Scan Tool

Process Scan utility of OpUtils software provides the list of all processes running in a given IP node.

To scan the processes running in Servers

1. Click the **Tools** tab
2. Choose the **System Explorer** available under **Network Monitoring** category.
3. Select the **Process Scan** from the tree
4. Enter either the **IP Address** or the **Host Name** of the device in the text field.
5. Enter the SNMP **Community** String.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The results include the **Process Name;** (i.e., the processes/programs running in the desktop); the **Process ID** (i.e., the system allotted process ID for the process); the **Process Path** (i.e., the location from where the process has been initiated); the **Process Type** (i.e.,the type of process - application/system call etc); and the **Process Status**. The process status shown are

   running(1)
   runnable(2) - waiting for resource (CPU, memory, IO)
   notRunnable(3) - loaded but waiting for event
   invalid(4) - not loaded

Note: To retrieve data, the system should be SNMP enabled and the SNMP agent should have implemented HOST-RESOURCES-MIB.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries , E2002: OID not Implemented.

Related Tools: **Ping**, **SNMP Ping**, **SNMP Graph**

Software Scan Tool

Software Scan utility of OpUtils software is for Network Engineer in asset tracking and in getting a software list corresponding to the particular node. The tool displays the list of all software, the type of software, and the date of installation in any given device.

To check the software installed in a given system

1. Click the **Tools** tab
2. Choose the **System Explorer** available under **Network Monitoring** category.
3. Select the **Software Scan** from the tree
4. Enter either the **IP Address** or the **Host Name** of the device in the text field.
5. Enter the **SNMP Community** string.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The details displayed include **Software Installed** and the corresponding icon, the **Date of Installation,** and the **Type of software**.

Note: To retrieve data, the system should be SNMP enabled and the SNMP agent should have implemented HOST-RESOURCES-MIB.

See Also

Error Messages
E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries , E2002: Specified OID not Implemented.

Related Tools: **Ping**, **SNMP Ping**, **SNMP Graph**

TCP Reset

TCP Reset utility of OpUtils software is used to reset the unwanted TCP connections that are established with the switches and routers in the network.

To reset a TCP Connection

1. Click the **Tools Home** tab.
2. Choose the **TCP Reset** available under the **Server Monitoring** category.
3. Enter the **IP Address** or the **DNS Name** of the switch or the router in the text field.
4. Enter the **Read** and **Write Community** strings in the respective fields.
5. Click **Get Connection Details**. This will list all the TCP connections that are established with the device.
6. To reset a connection, click the ✖ icon from the **Action** column of that connection.

Related Tools: **Rogue Detection**, **SNMP Ping**, **System Snapshot**, **Switch Port Mapper**

CISCO Tools

ManageEngine OpUtils provides the following feature rich range of tools for specifically monitoring CISCO routers.

Config File Manager: Utility to download/upload the StartUp and/or the Running config files from or to the given CISCO Router. The tool also shows the difference between the two files.

TFTP Server: Tool to view the Config Files available in the TFTP Root. You can also change the TFTP Root and edit/upload config files from here.

Device Scan: Utility to scan a subnet or a range of IP Addresses to collect the details of the Cisco Devices in the scanned range.

Device Explorer : Utility to scan a Cisco device to get the details like device snapshot, chassis details, IOS details, flash memory details, interfaces, IP routes, CPU and memory utilization, and access lists.

Config File Manager

Config File Manager utility of OpUtils software downloads the StartUp and/or the Running config files from the given Cisco devices like Routers and Switches, helps to compare different versions, and upload them on to the device. The tool uses TFTP to download/upload the files. You can also schedule to take a backup of the config files from the device at the specified interval.

- Specifying IP Address for TFTP Server and TFTP Root Directory
- Downloading Startup and Running Config Files from Cisco Devices
- Viewing Startup and Running Config Files
- Scheduling Backup of Startup and Running Config Files
- Comparing Config Files
- Viewing Configuration Files History
- Uploading Startup and Running Config Files to Cisco Devices

Specifying IP Address for TFTP Server and TFTP Root Directory

If you are running Oputils in a m/c that has multiple IP Addresses, it is required to bind the TFTP Server to a specific IP Address to successfully back up the configuration files.

1. Click **Settings** link from the Config File Manager tool.
2. If the TFTP Server is already running, click **Stop**.
3. Specify the IP Address to which the TFTP Server has to be bind.
4. Optionally change the location of the TFTP Root Directory. The downloaded config files are stored in the TFTP Root Directory.
5. Click **Save**.
6. Click **Start** to start the TFTP Server and bind to the new IP Address specified.

Downloading Startup and Running Config Files from Cisco Devices

1. Click the **Tools** tab.
2. Choose **Config File Manager** available under the **CISCO Tools** category.
3. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
4. Enter the **Device Name** or its **IP Address**.
5. Enter the **SNMP Community** String of the Cisco device. The Community specified should have read/write permissions.
6. Click **Add**. The added Cisco device gets added to the table below. The Config File Manager tool will fetch both the startup and running config files of the specified cisco device in the background.
7. To manually download the startup and running config files, click the 🔄 icon corresponding to that device from the table.

Note:

1. The SNMP community string specified while adding a Cisco device (Switch / Router) is used for subsequent downloads of the startup and running config files. If the community string is changed in the device at a later date, subsequent

downloads will fail. Click the ✎ icon corresponding to that cisco device and change the community string.

2. The Cisco devices should have the CISCO-COPY-CONFIG MIB implemented in order to download the startup config files.

Viewing Startup and Running Config Files

The startup and running config files are automatically download when a cisco device is added to the Config File Manager tool. You can click the icons to view the config files pertaining to the latest download.

1. Click the S icon of a device to view its Startup Config file.
2. Click the Ricon of a device to view its Running Config File.
3. Click the ▤ icon to view the difference between the startup and running config files.

Scheduling Backup of Startup and Running Config Files

The Config File Manager helps you to take scheduled backup of the startup and running config files of all the Cisco devices, like Routers and Switches, that are added to the Config File Manager tool. All the configuration changes made to the Cisco devices can be verified and audited. To take scheduled backup, follow the steps below:

1. Click the Edit Scheduler link to open the Scheduler dialog
2. Change the Status to Enabled
3. Specify the interval to perform the backup:
    1. **Daily** - to update everyday. You need to specify the starting time.
    2. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
    3. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
    4. **Once Only** - to run the tool only once at the scheduled time.
4. Click **Schedule** to save the changes.

Note: When you schedule backup, the startup and running config files of all the cisco devices added to the tool will be backed up at the specified interval.

Comparing Config Files

The Config File Manager provides you an option to compare any two config files that are downloaded using OpUtils. This is very handy when you want to compare the configurations between two similar cisco devices. For example, you can compare two cisco router configs or two cisco switch config files.

1. Click the **Compare Config File** link.
2. Select the files you wish to compare by selecting the appropriate options.
3. Select the device from the combo box. This will list all the files that are downloaded previously.
4. Select the versions to be compared and click **Compare**.

Viewing Configuration Files History

The Config File Manager tool maintains a history of the startup and running config files that are downloaded using the tool. This includes both manual download and scheduled backup. To view the complete history of the config file downloads of a particular cisco device, click the IP Address of the device. This will list details of config file download of that particular device.

You can view the startup config, running config, difference between startup and running config of all the versions from here. The versions are named with the date and time of the download. You can also upload the startup or running config file of any version back to the device

Uploading Startup and Running Config Files to Cisco Devices

1. Click the **Upload Config File** link.
2. You have an option to upload the config files to a single device or to multiple devices. Select the appropriate tab.
3. Select whether to upload Startup or Running Config File.
4. Select the device(s) to which it has to be uploaded.
5. Browse and select the config file to be uploaded and click **Upload**.

   Note: The downloaded config files are located in *<Installed_Dir>/ AdventNet/ ME/ OpUtils/ webapps/ tftp/ <Device IP>* from where you can edit the files, if required and upload.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E2004: Community with read/write permission required, E4005: Not a CISCO Device, E5003 : Unable to bind to Port

Related Tools: **Ping**, **SNMP Ping**, **SNMP Walker**, **TFTP Server**

TFTP Server

TFTP Server is used by OpUtils to retrieve the config files from the cisco devices. It is started at port 69 automatically whenever you try to retrieve the config files using the Config File Manager. The config files are retrieved and are stored in the file system under the TFTP Root directory, the default location being *<OpUtils_Home>/webapps/tftp* directory.

TFTP Server tool can be used to view the contents of the TFTP Root directory. In addition to the files downloaded using the Config File Manager tool, you will also be able to view the files that have been downloaded manually using the TFTP Server of OpUtils. You can also edit the files and upload it back to the devices.

You can also change the TFTP Root directory from here using the Settings link.

Note: When the TFTP Root directory is changed, the config files that are download prior to this change are not copied to the new location.

Related Tools: **Config File Manager**, **Ping**, **SNMP Ping**, **SNMP Walker**

Cisco Device Scan

The Cisco Device Scan tool of OpUtils software scans the subnets or a range of IP Addresses and collects the information about the Cisco Devices in the scanned range. The details include, the Chassis ID, ROM version, IOS version, among other details.

To Scan for Cisco Devices

1. Click the **Tools** tab
2. Choose **Device Scan** available under **Cisco Tools** category.
3. You have an option to view the details for a range of IP Addresses or for a single subnet. Select the required tab.
4. Based on the selected tab specify the start and end IP Addresses or the subnet address to be scanned.
5. Specify the SNMP Community string. Add multiple community strings as comma separated.
6. Click **Get Cisco Details**.
7. The details of the cisco devices in the subnet are displayed.
8. Click the **Export** link to export the results in PDF, CSV, or XLS formats.

Restrictions in Trial Version

1. Will only display any 5 devices in the scanned range.
2. Delete and Search options are disabled.
3. Export option is disabled.

Related Tools : Ping, SNMP Scan, Bandwidth Monitor, Switch Port Mapper

Device Explorer

Device Explorer utility of OpUtils software provides you the complete details of a cisco device such as device snapshot, chassis details, flash memory details, interfaces, IOS details, IP routes, and access lists.

To get the details of a Cisco device

1. Click the Tools tab.
2. Choose Device Explorer available under the Cisco Tools.
3. Enter the **Device Name** or its **IP Address**.
   Note: Ensure the device specified is a CISCO device
4. Enter the SNMP **Community** String of the device.
5. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
6. Click the **Show** button.
7. The device snapshot is displayed. Select the required parameter from the tree to view the details.

The Device Explorer provides the following details of a Cisco device:

1. Device Snapshot
2. Chassis
3. Flash
4. IOS
5. IP Routes
6. Device Monitor
7. Interfaces
8. Access Lists

Device Snapshot Tool

Device Snapshot utility of OpUtils software provides a quick snap shot of the given Cisco device.

To check the system details of a Cisco Device

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **Device Snapshot** from the tree.
4. Enter the **Device Name** or its **IP Address**.
   Note: Ensure the device specified is a CISCO device
5. Enter the SNMP **Community** String of the device.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The results include the device **Name**; **Description**; **Model Type**; the **IOS Version**; the **Flash Memory** Size (used and available); **RAM** size; the **Location** (i.e., the physical location of the device as specified by the Administrator); the **Contact** person for the device (as specified by the Administrator); **Up since** time; and the router's **Interfaces** details. The status of the Interfaces is represented by the following icons:

✗	✓	✗	✓
Serial port down	**Serial port up**	**Ethernet port down**	**Ethernet port up**

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4005: Not a CISCO Device

Related Tools: **Ping**, **SNMP Ping**, **IP Node Browser**, **Chassis**, **IOS**, **Flash**, **Interfaces**

Chassis Tool

Chassis utility of OpUtils software provides the chassis details for a Cisco device.

To check the Routers' physical details

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **Chassis** from the tree.
4. Enter the **Device Name** or its **IP Address**.
   Note: Ensure the device specified is a CISCO device
5. Enter the SNMP **Community** String of the device.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The results include the device **Model** details; the **Processor** series; **Hardware Revision** number; **Processor Board ID**; **ROM Monitor Version**; **RAM** size; **Non Volatile RAM** details (that include total, free, and available NVRAM in the device); and the **Configuration Register** number.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4005: Not a CISCO Device

Related Tools: **Ping**, **SNMP Ping**, **IP Node Browser**

Flash Tool

Flash utility of OpUtils software provides the flash memory details of the Cisco device. It also provides the controller type, card type, and initialization time of the Cisco device.

To scan the Flash memory details

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **Flash** from the tree.
4. Enter the **Device Name** or its **IP Address**.

   Note: Ensure the device specified is a CISCO device.
5. Enter the SNMP **Community** String of the device.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The results include the **Controller Type** of the CISCO device's Flash memory, the **Card Type**, the **Initialization Time**, and the **Flash Memory** image details.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4005: Not a CISCO Device

Related Tools: **Ping**, **SNMP Ping**, **IP Node Browser**

IOS Tool

IOS utility of OpUtils software is used to know the details of Internetwork Operation System Software (IOS) installed in a Cisco device.

To check the IOS details

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **IOS** from the tree.
4. Enter the **Device Name** or its **IP Address**.
   Note: Ensure the device specified is a CISCO device.
5. Enter the SNMP **Community** String of the device.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin --> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The results include the **ROM IOS Version** details, the **Running IOS Version** details, the **Image File** name and the **Image File Size.**

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4005: Not a CISCO Device

Related Tools: **Ping**, **SNMP Ping**, **IP Node Browser**

IP Routes Tool

The IP Routes utility of OpUtils software is used to view the static and dynamic routes of a Cisco Router. If CDP is enabled the tool also provides details of the neighboring Cisco devices. The tool provides the IP routing details of the Cisco router. It shows the interface name, IP Address of the next hop, destination IP Address, type, protocol, and age.

To view the routes of a Router

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **IP Routes** from the tree.
4. Enter the **Router's Name** or its **IP Address**.
   Note: Ensure the Router specified is a CISCO Router.
5. Enter the SNMP **Community** String of the Router.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The results include the **Destination** IP Address; number of **Interfaces**; **Next Hop** details; the **Type** of connection (Remote/Direct) between the router and the destination; the **Protocol**; and the **Age** (i.e., the time in seconds taken between hops).

Note: All CDP-enabled neighbours of the specified router are automatically discovered along with the IP, the series number, and the CDP interfaces.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4001: Not a CISCO Router

Related Tools: **Ping**, **SNMP Ping**, **Network Scan**

Device Monitor Tool

Device Monitor utility of OpUtils software monitors the CPU utilization, memory utilization, buffer miss rate, and buffer failures of a Cisco device.

To monitor the load and utilization of a Cisco Device

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **Device Monitor** from the tree.
4. Enter the **Device Name** or its **IP Address**.
   Note: Ensure the device specified is a CISCO device.
5. Enter the SNMP **Community** String of the device.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. To configure Graph settings such as the polling interval and number of plots, follow the same steps as given above. For more read the section Configuring Graphs.
8. Click the **Show** button.
9. The following details about the device are displayed in graph.
   - **CPU Utilization** : Displays the CPU load of the device. To view the history of CPU Utilization check the table displayed below the graph.
     Note: High percentages indicate high CPU utilization.

   - **Memory Utilization** : Displays the memory utilization of the device. Every line in the graph represents the utilization of a memory pool.
     Note: If the Input queue drops, it is an indication of high percentage CPU Utilization.

   - **Buffer Miss Rate** : Displays the number of times a buffer request failed, because there were no buffers available in the free list, or there were fewer than "min" buffers in the free list.

   - **Buffer Failures** : Displays the number of failures to grant a buffer to a requester under interrupt time (remember that the router can create new buffers at process switching level, so "failure" does not occur unless there is "no memory"). The number of "failures" represents the number of packets that have been dropped due to buffer shortage.

Note: Choose the Refresh time interval in seconds from the **Refresh every** list box. The page is refreshed based on the selected time interval.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4005: Not a CISCO Device, E2002 : OID not Implemented

Related Tools: **Ping**, **SNMP Ping**, **Bandwidth Monitor**, **Performance Monitor**

Interfaces Tool

Interfaces utility of OpUtils software provides the list of interfaces, and its details for a Cisco device.

To retrieve the Interface details

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **Interfaces** from the tree.
4. Enter the **Device Name** or its **IP Address**.
   Note: Ensure the device specified is a CISCO device.
5. Enter the SNMP **Community** String.
6. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
7. Click the **Show** button.
8. Check the results. The following details about the Cisco device are displayed in a the table.
   - **Interface Description**: Displays the name of the Interface along with the description.
   - **Interface Type**: Displays the Type of interface.
   - **IP Address**: Displays the IP address of the Interface.
   - **Physical Address**: Displays the MAC Address at its protocol sub-layer.
   - **Bandwidth**: Displays the interface's current bandwidth in bits per second.
   - **Maximum Transfer Unit**: Displays the Maximum Transmission Unit i.e., size of the largest packet which can be sent or received on the interface, specified in octets.
   - **Admin Status**: Displays the desired state of the interface.
   - **Operational Status**: Displays the current operational state of the interface.

     Note: Check if the Admin status of an Interface is Up whereas the Operation state is down. This is a clear indication of trouble.

8. To view the Interface details click the Interface name in the table. For each of the Interfaces the Performance, and the Error details are displayed in a table.
   - **Performance Details**
     - The Progress bar displays the **input** and **output** percentage utilization.
   - **Error Details**
     - The **Received** and **Transmitted Errors**, the **In Discards** and **Out Discards**, along with the **Runts** and **Giants** are displayed in a table.

9. To monitor input and output utilization of the interface click the icon 📈 located at the right corner. Check the input and output utilization in graph. The refresh time can be set by choosing the time in seconds from the **Refresh Every** combo box. To traverse back to the Interface page click the **Back to Interfaces** link.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E4005: Not a CISCO Device

Related Tools: **Ping**, **SNMP Ping**, **Bandwidth Monitor**, **Performance Monitor**

Access Lists Tool

The Access Lists utility of OpUtils software provides the access control lists that are built into the cisco device.

To view all the Access Control lists configured on the given CISCO Device

1. Click the **Tools** tab.
2. Choose **Device Explorer** available under the **CISCO Tools** category.
3. Select the **Access Lists** from the tree.
4. Enter the **Device Name** or its **IP Address**.
5. Enter the **User Name** of the device. This is optional.
6. Enter the **password** of the device.
7. To set CLI values click **CLI Settings** link and specify the System Prompt, Login and the Password Prompts of the cisco device and Save.
8. Click the **Show** button.
9. All the Access List configured on the device are displayed in the result field.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E4005: Not a CISCO Device, E4002: Wrong CLI Authentication Parameters

Related Tools: **Ping**, **Enhanced Ping**, **Trace Route**

SNMP Tools

ManageEngine OpUtils provides the following utilities for performing basic SNMP operations.

MIB Viewer : Utility to view the details of a MIB node. It accepts the node name or the OID as input and provides the complete information on the MIB node including MIB name, parent node name, OID, OID type, status, syntax, access, definition, and the next node. It also provides some general information about the MIB and also provides the defined attributes, total number of nodes, defined TCs, and the defined traps.

SNMP Graph : Utility to periodically query the given SNMP device for the specified OID value and plot the results in a graph. It also provides the MIB node information like OID, syntax, description and MIB node properties.

Trap Receiver : Utility to receive and view SNMP traps on a specified port in a manager station.

SNMP Walker: Utility to view the data available through an SNMP agent in an IP node/device.

SNMP Table: Utility to retrieve the data from the specified Table OID from a IP node/device

MIB Browser : Utility to browse MIBs and perform various SNMP operations such as GET, GET-NEXT, GET-BULK, and SET on the specified agent.

Community Checker : Utility to detect the read and write community strings of the devices in the network.

MIB Viewer

MIB Viewer tool to OpUtils software provides the details of a particular MIB node and / or the complete details of the selected MIB. OpUtils comes with a set of standard and polpular MIBs for which you can view the details in just a couple of clicks. You have an option to add the proprietary MIBs in OpUtils before viewing their details.

To view the MIB details

1. Click the **Tools** tab.
2. Choose **MIB Viewer** available under the SNMP Tools category.
3. To view the details of a MIB node or a specific OID, select the MIB Node Viewer tab.
4. To view the details of all the MIB nodes of a specific MIB, choose the MIB Module Viewer tab.

MIB Node Viewer Tool

Many a times network engineers are aware of the MIB node (OID name) but not sure of the OID and its properties. In such situations MIB Node Viewer utility would be of great use. It accepts the node name or the OID as input and provides the complete information on the MIB node.

To view details of a MIB node

1. Click the **Tools** tab.
2. Choose **MIB Viewer** available under the SNMP Tools category.
3. Select the **MIB Node Viewer** tab.
4. Enter the **MIB Node** name or the **OID.**
5. Click the **Find** button.
6. Check the results. The results include:
    - **MIB Module Name**: Displays the MIB name where the Node/Object OID exists.
    - **Parent Name:** Displays the parent Variable/Node for the MIB node specified.
    - **OID**: Displays the unique OID of the MIB node.
    - **Numbered OID**: Displays the unique OID of the specified Variable/Node.
    - **Macro Type**: Displays the Macros defined in the SMIv1 and SMIv2.
    - **OID Type** : Displays the OID type. The OID types supported are Scalar, Table Column, Table, Index node, and Table Entry.
    - **Status**: Displays the status value of the node.
    - **Syntax** : Displays the syntax associated with the node.
    - **Access**: Displays the access permission for the node/variable defined as read-only, read-write, write-only, or none.
    - **Child Nodes**: Displays the number of Child nodes and names of the node (if any).
    - **Next Node**: Displays the variable/node that succeeds the node specified.
    - **Definition:** Displays the variable/node description as given in the MIB.
7. If you get an error message as "Unrecognised OID", try adding the MIB containing the OID using the **Load MIB** link and try again.

See Also

Error Message: E5001: Unrecognised OID

MIB Module Viewer Tool

The MIB Module Viewer provides a snapshot of a given MIB. It provides some general information on the MIB and also provides the defined attributes, total number of nodes, defined TCs, and the defined traps. It also provides the SMIv2 specific details.

To view the details of a MIB

1. Click the **Tools** tab.
2. Choose **MIB Viewer** available under the SNMP Tools category.
3. Select the **MIB Module Viewer** tab.
4. Check if the MIB to be viewed is available for selection in the **MIB Name** combo box. All the MIB's loaded by default are listed.
5. If you want to view the snapshot of a MIB that is not loaded by default, click the **Add MIB** button. In the **Add MIB** dialog that appears, use the **Browse** button to choose the MIB, and click the **Load** button. If a MIB has any dependent MIBs ensure that all the dependent MIBs are also loaded to avoid errors. Click **Close** to close the dialog. Check if the MIB that is loaded is displayed in the **MIB Name** combo box. Based on whether OpUtils is run in database or in non-database mode, the mibs will get added to the MIBs database or to *<OpUtils Home>/Application/mibs* directory respectively.
6. Choose the MIB from the combo box.
7. Click the **Show** button.
8. Check the results. The details are categorized as
   - **General Info :** Displays the basic information of the MIB. The details include, the MIB Module Name, the MIB Version details, the name of the MIB if the MIB file has been imported, and the Root Node name.
   - **SMI v2 MIB Details** - Displays the MIB version details. The details include, the **Organization** details (vendor details), the **Last Update** information, the **Revision** details (the revision timestamp in the UTC format) and the **Description**. The information is applicable only to certain MIB's.
   - **Total Number of Nodes Present** : Displays the total number of attributes in the MIB.
   - **Defined TCs** : Displays the Textual Conventions followed in the MIB.
   - **Defined Traps** : Displays the traps already defined in the MIB.
   - **MIB Node Details**: Displays the details of the nodes defined in the MIB. The details include the **MIB Node**, **Syntax,** and **MIB Type**.

SNMP Walker Tool

SNMP Walker is a utility where you can provide any OID value and query a device for the next consecutive OIDs.

To view Data from SNMP Agent

1. Click the **Tools** tab.
2. Choose **SNMP Walker** available under the **SNMP Tools** category.
3. Enter the **IP Address** or the **Host Name** of the device and the SNMP community.
4. Select the **SNMP** version: V1. V2c. Read the SNMP Overview section for more details
5. Enter the **OID** from which to start the walk.
6. Select the number of values to be retrieved.
7. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
8. Click the **Walk** button.
9. Check the results. For all the values retrieved, the following information is displayed in a table:
   - **MIB** - The name of the MIB that is queried to fetch the details of the IP Address/Host Name specified in the text field.
   - **Numbered OID** - The OIDs of the variables that are queried.
   - **Name -** The names of the variables queried.
   - **Type -** The result type of the query. The following types are valid data types: Bit Stream, Counter, Integer, IP address, Object Identifier, Opaque String, String, Time Ticks and Unsigned Integer.
   - **Value -** The value retrieved in the SNMP walk for the variable.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E5002 : Invalid OID.

Related Tools: **Ping**, SNMP Ping, DNS Resolver, MIB Module Viewer, MIB Node Viewer

SNMP Table Tool

SNMP Table is a utility to retrieve the table data of a MIB. This is useful where you have hundreds of rows and would like to view them and compare.

To get the Table details

1. Click the **Tools** tab.
2. Choose **SNMP Table** available under the **SNMP Tools** category.
3. Enter the **IP Address** or the **Host Name** of the device and the SNMP community.
4. Browse to select the Table OID. The **Select MIB** dialog lists a set of standard and popular MIBs. Selecting a MIB will list the available table OIDs of that MIB below. To Add a MIB to the Select MIB dialog, use the **Add MIB** link.
5. Click **SNMP Settings** link to specify the SNMP Settings, like version number, port, timeout, and retries.
6. Click **Get Table**.
7. Check the results. All the column/row data of the given table for the given device is shown.
8. You can customize the columns to view using the Add/Remove Columns link or search for a specific field/value using the Search option.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E2007 : Not a Table OID, E5002 : Invalid OID.

Related Tools: **Ping**, **SNMP Ping**, **DNS Resolver**, **MIB Module Viewer**, **MIB Node Viewer**

Trap Receiver Tool

Trap Receiver utility of OpUtils software listens for real-time network traps for processing.

To configure the agent to receive traps read the Configuring SNMP Agents section provided for Windows and Linux.

To view Traps

1. Click the **Tools** tab.
2. Click **Trap Receiver** available under the **SNMP Tools** category.
3. When the Trap Receiver tool is opened, it automatically starts listening for traps in port 162. If you are running OpUtils in Linux operating systems, you should have started OpUtils as a root user to use this tool.
4. When a trap is received, it automatically refreshes to show the received trap.
5. The **Name** column defines the type of the trap or the inform request.
6. The **OID** column refers to the Trap OID of the received trap.
7. The **Source** column represents the IP address of the source from where the traps were sent.
8. The **Time Stamp** column shows the duration when the trap was sent calculated from the agent start time.
9. The **Trap Received Time** shows the date and time when the trap was received in OpUtils.
10. The **Varbind Values** column has the VarBind list of the trap and its values, if any.
11. The **Varbind Desc** column shows the descriptions of the trap OIDs. If the description is not available, click the Add MIB link and add the MIB containing the trap OIDs.

To change the Trap Listening Port

1. Click the **SNMP Trap Settings** link. This opens a dialog to configure the port.
2. Click **Stop** to stop the SNMP Trap Service.
3. Change the port number and click **Start**.

To Configure E-mail and Sound Alerts

Alerts are generated whenever a trap is received. The Trap Receiver tool can be configured to notify this through email or by playing a sound.

1. Click the **Configure Alert** link. This opens the Configure Alert dialog.
2. Select the **Enable Email Alert** check box and specify the recipients email addresses as comma separated.
3. To enable sound alerts on receipt of a trap, select the **Enable Sound Alert** check box and select a sound file to be played. To play the selected sound, click the 🔊 icon. You can also import your own sound files to be played; browse to select the sound file and click OK. The imported sound file gets added to the list, which can now be selected.

4. **Alert Cleanup Policy**: Specify the maximum number of Alerts to be stored in the database, the default being 2000. When you delete the older alerts, you have an option to save them as a csv file for future reference.
5. Click **Save**.

Note: To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.

See Also

Error Messages: E5003 : Unable to bind to Port

Related Tools:**Ping**, **SNMP Ping**, **DNS Resolver**

SNMP Graph Tool

SNMP Graph utility of OpUtils software is used to gather real time data and draws a graph for any SNMP IP node. It also provides the MIB node information like OID, syntax, description and MIB node properties. The SNMP data to be polled should be of integer or unsigned integer data type (Counter, Gauge, or Timeticks).

To plot an SNMP graph

1. Click the **Tools** tab.
2. Choose **SNMP Graph** available under the **SNMP Tools** category.
3. Enter the **IP Address** or the **Host Name** of the device to be contacted and the SNMP community.
4. Select the **Object OID** or the **MIB Node** from the combo box (By default, eight OIDs are displayed in the OID combo box). OR enter the required **Object OID** or **MIB Node** to plot graph. Graph is plotted only for integer values.
   Note: You can also choose to give a node that does not have value in integer format, but the graph will not be plotted, only details about the MIB node will be provided.
5. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
6. To configure Graph settings such as the polling interval and number of plots, follow the same steps as given above. For more read the section Configuring Graphs
7. Click the **Plot** button.
8. View the SNMP graph. Check the **MIB Node Information** and **MIB Node Properties** details.
   - **MIB Node Information**
     - **MIB Name:** The MIB used to query the details for plotting the graph.
     - **Numbered OID:** The unique numbered OID of the system.
     - **OID :** The OID of the system**.**
   - **MIB Node Properties**
     - MIB Type : Displays the type of the MIB Node.
     - **Status** : Displays the status of the MIB node.
     - **Syntax** : Displays the node characteristic. The available syntax are Bit Stream, Counter, Integer, IP address, Object Identifier, Opaque String, String, Time Ticks and Unsigned Integer.

Note	1.Graphs show proper information only if the IP Address or Host Name is SNMP-enabled. 2. Choose the Refresh time interval in seconds from the **Refresh every** list box. The page is refreshed based on the selected time interval.

See Also

Error Messages : E1001: Unknown Host, E1002: Unreachable Host, E2001: No Response to SNMP Queries, E5002 : Invalid OID, E5001: Unrecognised OID

Related Tools: Ping, SNMP Ping, System Snapshot, MIB Module Viewer, MIB Node Viewer

MIB Browser

MIB Browser Tool

The MIB Browser utility of OpUtils software enables you to load and browse MIBs and perform SNMP operations. With this tool you can perform all SNMP-related operations like GET, GET-NEXT,SET etc. The above SNMP operations can be performed on the specified agent. For more details read the following sections.

- Loading MIBs
- Getting the value of SNMP variables
- Setting values to SNMP variables

Related Tools: **Ping**, **SNMP Ping**, **DNS Resolver**

Loading MIBs

MIB Browser allows you to load MIBs directly. Whenever the files are loaded, they are compiled and then loaded.

To load a MIB

1. Click the **Tools** tab.
2. Click the **MIB Browser** available under the **SNMP Tools** category.
3. Select a MIB from the Select MIB combo box. The Selected MIB gets loaded below.
4. If you want to load a MIB that is not available by default, click the **Add MIB** button. In the **Add MIB** dialog that appears, use the **Browse** button to choose the MIB, and click the **Add** button. If a MIB has any dependent MIBs ensure that all the dependent MIBs are also added to avoid errors. Click **Close** to close the dialog. Check if the MIB that is loaded is displayed in the list box.

Setting SNMP Parameters in MIB Browser

Most network devices have a default value maintained by the agent. To modify data use the SNMP SET operation. Values can be set only to variables having read-write access

To set values using SNMP SET operation

1. Load the MIB file. For more details, read the Loading MIBs section.
2. Enter the Host Name.
3. Select the SNMP variable from the tree.
4. Enter the value to be set in the **Set Value** box. Enter the Write Community string.
5. To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.
6. Click the **Set** button.

Getting the Values of SNMP Variables

Retrieving the value of an SNMP variable using GET operation

The operation is used by the SNMP manager applications to retrieve one or more values from the managed objects maintained by the SNMP agent. The applications typically perform an SNMP GET request by providing the host name of the agent and one or more OIDs along with the specific instance of the OID. The agent responds with a return value or with an error.

The SNMP GET operation is normally used to query the scalar variables in a MIB. Each scalar variable is identified by its OID and its instance. The instance is used to identify the specific instance of the scalar variable. It is specified by appending a ".0" to its OID. To proceed

1. Load the MIB file. For more read the Loading MIBs section.
2. Select the desired node in the MIB tree.
3. Click the **Get** button.

Result

- This operation gets all objects under the selected MIB object, or the specific object if the MIB instance is specified.

Retrieving values of multiple SNMP variables using GETNEXT operation

The operation retrieves the value of the next OID in the tree. The GETNEXT operation is particularly useful for retrieving the table data and also for variables that cannot be specifically named. It is used for traversing the MIB tree.To proceed

1. Follow the steps as given for retrieving the value of an SNMP Variable.
2. Click the **Get Next** button.

Result

- This operation gets the value of the next object, under the selected MIB variable.

Retrieving SNMP variables values using in GETBULK operation

The operation is normally used for retrieving large amount of data, particularly from large tables if your SNMP version in your network is v2c or v3. The GETBULK operation performs a continuous GETNEXT operation based on the Max-Repetitions value. The NonRepeaters value determines the number of variables in the variable list for which a simple GETNEXT operation has to be done. For the remaining variables, the continuous GETNEXT operation is done based on the Max-Repetitions value.

To proceed

1. Select the SNMP variable from the list and click **Get Bulk**.
2. The number of consecutive variables fetched, will depend on the value specified in the **Max-Repetitions** box. By default it is set to 50.

Result

- This operation gets the number of values retrieved depends on the value specified in the MAX-Repetition box.

Note	Note: To configure SNMP properties click **Settings** located at the top right corner or click **Admin -> Settings**. For details read the Configuring SNMP section.

Community Checker

The Community Checker utility of the OpUtils software scans the range of IP Addresses to get their SNMP read and write community strings based on the pre-defined set of default and standard community strings of the switches,routers, etc.

To get the SNMP Community String

1. Click the **Tools** tab.
2. Choose **Community Checker** available under the **SNMP Tools** category.
3. You have an option to scan a range of IP Addresses or a single device. Select the required tab.
4. Based on the selected tab specify the start and end IP Addresses or the IP Address/ Host Name of the device.
5. Click **Get Community**.
6. Check the result. The details of the read and write community strings of the devices are listed. **Not Responded** in the result could be of the following reasons:
    - The device did not respond to any of the available community string.
    - The device is not snmp-enabled (if both read and write communities could not be determined)

To Add/Edit Community Strings

The community Checker tool uses a pre-defined set of read and write community strings to determine the community of a device. You have an option to add or edit the list to include the community strings of the devices in your network as given below:

1. Select the Add/Edit Community tab.
2. Specify the read and write communities and click Add.
3. To modify a community, click the ✎ icon and edit. Click the 💾 icon to save the changes.
4. To delete a community string, click the ✖ icon.

Related Tools : Ping, SNMP Ping, System Snapshot, Process Scan, Software Scan

Custom SNMP Tools

Custom SNMP Tools of the OpUtils software enables you to add any OIDs of the MIB to be monitored. It also allows you to add your enterprise-specific MIBs. This tool allows you to create different tools for viewing the data in the tabular and in the graphical formats. While the custom graph tool only supports integer and counter data types, the tabular tool can be used to view all the data types. There is no limitations to the number of tools that can be created.

The following topics helps you to create your own tools:

- Custom Tabular Tool
- Custom Graph Tool

Custom Tabular Tool

The Custom Tabular tool of OpUtils enables you define a set of OIDs that have to be queried on demand and show its current value. The tool can be used to query any SNMP-enabled device to view its current value.

To create a Tabular Tool

1. Select **Add Custom Tool** link from the Custom Tool category from the Tools tab. This opens the Add Custom Tool page.
2. Provide a name for the tool.
3. Select the Type as "**Tabular**". This option is selected by default.
4. Select the MIB from the **MIB Name** combo box and click Show. You can use the **Add MIB** button to add the MIBs to the MIB Name combo box. This lists all the scalar and tabular nodes of the selected MIB.
5. Select the **Scalar Node** or **Tabular Column Node** tabs to view the MIB nodes of that type.
6. Click **Add>>** link to add the required nodes.
7. Repeat steps 5 and 6 to add nodes from other MIBs
8. After adding all the required nodes, click **Create Tool** button.

The tool gets created and added under the Custom Tools category in the Tools tab.

Using the created Tabular Tool

1. Click the name of the tool available under the Custom Tools category in the Tool tab.
2. Specify the device name and its SNMP community string in the respective fields.
3. Click **Scan**.
4. Check the results. The details of the MIB Nodes along with their current values are grouped and shown in a tabular format.

To delete a Custom Tool

To delete a custom tool, click the delete icon available next to the tool name in the Tools tab.

Custom Graph Tool

The Custom Graph Tool provides a dashboard view of the selected MIB nodes. It allows grouping of nodes that have to be plotted in a single multi-line graph. The tool has a capability to run continuously and plot the graph for the last one hour. The monitoring interval can also be configured.

To create a Graph Tool

1. Select **Add Custom Tool** link from the Custom Tool category from the Tools tab. This opens the Add Custom Tool page.
2. Provide a name for the tool.
3. Select the Type as "**Grapical**".
4. Select the MIB from the **MIB Name** combo box and click **Show**. This lists all the scalar and tabular nodes of the selected MIB. You can use the **Add MIB** button to add the MIBs to the MIB Name combo box.
5. Select the **Scalar Node** or **Tabular Column Node** tabs to view the MIB nodes of that type.
6. Click **Add>>** link to add the required nodes. If you wish to have multiple nodes in a same graph, select all the nodes and specify a group name and click **Create Group**.
7. Repeat steps 5 and 6 to add nodes from other MIBs
8. After adding all the required nodes, click **Create Tool** button.

The tool gets created and added under the Custom Tools category in the Tools tab.

Using the created Graph Tool

1. Click the name of the tool available under the Custom Tools category in the Tool tab.
2. Specify the device name and its SNMP community string in the respective fields.
3. Click **Add**.
4. You can also add multiple devices to be monitored simultaneously, which gets added as a different tab in the results pane.
5. Check the results. The graphical representation of all the groups are shown.
6. The default monitoring interval is 5 minutes, which is configurable by selecting the required interval from the combo box.
7. The last one hour data is shown.

To delete a Custom Tool

To delete a custom tool, click the delete icon available next to the tool name in the Tools tab.

Network Reports

OpUtils periodically scans the routers and subnets that are defined in the Global Environment. Apart from this, whenever you use the scan tools, Switch Port Mapper, IP Address Manager etc., the details are stored in the database. These data is presented in the form of reports that are useful to the administrators.

Report Features

- Drill down for more details.
- Customizable Columns
- Columnar sorting of reports
- Can be exported in PDF formats
- Options to print and e-mailing of reports.

The following types of reports are shown:

- Network Report
- Inventory Report
- IP Availability Report
- Port Availability Report
- MAC Address Report
- SNMP Devices Report
- Rogue Devices Report

Network Report

The Network Report provides the summary of the device types, IP availability and the Port availability.

- Managed Devices Summary: Provides the various types of devices in the network along with their count. Clicking a device type will list all the device of that type.
- IP Availability Summary: Provides the available, used, and transient IPs in the network. Clicking the link will show the IP Addresses of that state.
- Port Availability Summary: Provides the available, used, transient port of the switches in the network. You can view the switches and the ports by clicking a state.

Inventory Report

The Inventory Report provides a graphical representation of the device types of the subnets in the network. You can drill down the reports by clicking a device type from the graph.

IP Availability Report

The IP Availability Report provides the list of available/used/transient IP Addresses of the subnets in the network. You can drill down the reports by clicking a device type from the graph.

An IP Address, if it does not respond, is termed transient initially. It should meet the following criteria before it is moved to the available state:

- It should not respond for 10 continuous days.
- There should have been at least five polls in the above period.

Port Availability Report

The Port Availability Report provides the list of ports that are in available/used/transient states in the switches available in the network. You can drill down the reports either by clicking the graph or from the table.

Initially, all the non-responding ports are put in the transient state. If it does not respond continuously for more than 10 days, it is changed to available state.

MAC Address Report

The MAC Address Report provides the MAC and its corresponding IP Address and DNS Names of the devices in the network.

SNMP Devices Report

The SNMP Devices Report provides the list of devices in the network that responds to SNMP queries.

Rogue Devices Report

The Rogue Devices Report provides the list of new MAC addresses found in the network

Appendix

This section covers the following topics

- **Interpreting Error Messages**
- **FAQ**
- **Troubleshooting Tips**
- **Known Issues and Limitations**

Interpreting Error Message

E1001: Unknown Host

Message Summary

The IP Address or the Host Name does not exist in the network

Cause

1. Failure in ping action and DNS service (i.e. the DNS Server could not resolve the IP Address or the Host Name specified)

E1002: Unreachable Host

Message Summary

The IP Address or the Host Name is not alive in the network.

Cause

1. The IP Address or the Host Name specified is switched off.
2. The IP Address or the Host Name specified is behind a Firewall.

E1003 : Not a Switch

Message Summary

The referred IP Address or the Host Name is not a Switch.

E1004: Not a Router

Message Summary

The Router name specified is not that of a Router.

Cause

1. The input is not a switch.

Note: If the router has the OID .1.3.6.1.2.1.4.1 and "ip forwarding" set to "true(1)" the device is considered as a router.

E1005: MAC not available in cache

Message Summary

The MAC Address entered is not available in the OpUtils server cache.

E2001: No Response to SNMP Queries

Message Summary

The IP Address or the Host Name is not SNMP enabled.

Cause

1. The IP Address or the Host Name specified is not an SNMP device
2. The IP Address or the Host Name specified does not respond using the SNMP parameters available under SNMP Settings.

Action:

1. To install SNMP read the section Installing SNMP.
2. To change SNMP Settings click **My Home-> Settings-> SNMP**.

E2002: Specified OID is not Implemented

Message Summary

The required OID is not implemented by the SNMP agent running in the device specified.

E2003 : Unable to perform SNMP SET

Message Summary

The Server is not able to perform the SNMP SET operations on the specified host.

Cause

1. Unable to set the input parameters on the Target Host Name due to
   - invalid input parameters or
   - network traffic

Action:

1. To change SNMP Settings click **My Home-> Settings-> SNMP**.

E2004: Community with read/write permission required

Message Summary

The entered community string does not have the Write permission to perform the SET operation on the target host.

E2005: Not able to retrieve complete data from the MIB

Message Summary

The required information could not be retrieved from the MIB implemented in the input device.

E2006: Not able to retrieve MAC Address of the Switch

Message Summary

The MAC Address of the given switch cannot be retrieved from the MIB through SNMP. Mapping the switch ports will not be possible without the MAC Address of the switch.

E2007: Not a Table OID

Message Summary

When the specified OID is not a Table OID. Specify a valid table OID or browse to select a table OID of a MIB.

E3001: Operation Timed Out

Message Summary

Server wait time period (Server Timeout value) to get the response or result from the target host has expired.

E4001: Not a CISCO Router

Message Summary

The Router specified does not belong to the CISCO Router series.

E4002: Wrong CLI Authentication Parameters

Message Summary

Unable to login to the Router with the given CLI parameters

Cause

1. CLI system prompt or the password prompt or the password specified for CLI authentication is incorrect.

Action : To change CLI password prompt or the system prompt click **My Home-> Settings-> CLI**

E4005: Not a Cisco Device

Message Summary

The input device is not a Cisco device.

E4007: No Access Lists Available

Message Summary

No access lists available for the given Cisco device.

Cause

1. No data is available for the device being queried.

Action : Check whether the input device is a Cisco device.

E5001: Unrecognised OID

Message Summary

The OID does not exist in any of the loaded MIBs.

Cause

1. The OID does not exist either in the MIBs bundled with OpUtils or in the MIB's database.

E5002: Invalid OID

Message Summary

The OID specified is not valid.

Cause :

1. The Syntax is a displaystring OR
2. The OID Type is of type table or table entry OR
3. The OID Type is scalar and if the index value specified is not 0.

Note: The above error message occurs only for SNMP Graph Tool, as the OID specified cannot be plotted in a graph.

E5003: Unable to bind to Port

The message appears for the following tools

1. Trap Receiver
2. Config File Viewer
3. SNMP Trap Settings

Trap Receiver

The message appears

1. If OpUtils is not started as root AND the Port specified for receiving traps is less than 1024 (in Linux)

2. The port is already occupied

Action : To start Trap Service in port less than 1024, start OpUtils as root. Or else start Trap Service in port greater than 1024. To re-configure trap settings login as admin and click **My Home->SNMP Trap Settings** and change the Port number.

Config File Viewer

The message appears if OpUtils is not started as root or when port 69 is occupied. (TFTP Service is started by Oputils in Port 69)

Action : Start OpUtils as root or free the port

SNMP Trap Settings

The message appears if

1. If OpUtils is not started as root AND the Port specified for receiving traps is less than 1024 (in Linux)

E6001: Old Password is incorrect

Message Summary

The Password entered in the "Old Password" field is incorrect.

Action : Enter the password correctly.

E6002: Unable to send mail

Message Summary

Unable to send mail to the intended recipient.

Cause

1. The SMTP Server settings are incorrectly set.
2. The sender's email id is entered incorrectly.

Action

1. Click **Admin -> Settings** and choose SMTP. Recheck if the SMTP Service is running in the Port specified.
2. Check the sender's email id.

E6003: User already exists

Message Summary

The user specified already exists.

Action

1. Check the list of users displayed in the Admin -> User Management page.
2. Enter user name and password correctly.

E8001: TCP Reset tool supports only switches and routers

Message Summary

The input device in the TCP Reset tool can only be switches or routers.

Action: Specify a switch or a router as a input.

E8002: No TCP connection established in the device

Message Summary

The input device do not have any TCP connections currently established.

E8003: Could not reset the connection

Message Summary

The TCP connection could not be reset.

Cause: The given SNMP write community is incorrect.

Action: Specify the correct write community of the device.

E9001: Not a DHCP server

Message Summary

The input device is not a DHCP Server.

Action: Specify a DHCP Server to monitor its scopes.

E9002: DHCP Scope Monitor only supports windows NT and 2000 DHCP servers

Message Summary

The DHCP Scope Monitor tool can only be used to monitor the scopes of Windows NT and 2000 DHCP Servers.

E9003: The DHCP server already exist in the list

Message Summary

The specified device is already added.

E9004: The Community already exist in the list

Message Summary

The SNMP community string specified is already available in the lits of communities.

FAQ's

1. What operating systems does the OpUtils support?

OpUtils supports Windows and Linux operating systems.

2. What is MIB database?

OpUtils package comes with a collection of MIB's. By default Firebird database has been used to store the MIB's and is referred to as the MIB database. This database is useful to monitor any specific device on your network. The SNMP tools like SNMP walker and the MIB browser help in monitoring and collecting data about any device in the network using the MIB database.

3. What is Community?

Community refers to the SNMP Community string of the device being queried. This will be required in tools that used SNMP to get the required details. In most cases, a read-only community string is sufficient.

4. What system requirements are needed to run OpUtils?

To run OpUtils, you require a P III, 733 MHz processor with 256 MB RAM and 100 MB hard disk space

5. Can OpUtils be run in an non-English operating systems?

Yes, OpUtils can be run in non-English OS's as an English software.

6. Will I be able to access the OpUtils tools from remote?

OpUtils is Web-based and hence it can be accessed from anywhere in the network.

7. Can OpUtils monitor devices in my network such as Printers etc?

Yes, you can monitor any device using tools from ManageEngine OpUtils. To monitor any specific device (that is available on your network), you can use SNMP tools like MIB Browser, SNMP walker and collect data about your device.

8. Where can I get the complete list of tools present in OpUtils?

To get the complete list of tools click the **About** link in the top frame.

9. Can I send reports of the results as an e-mail?

Yes, you can send individual tool results by clicking the e-mail icon from the tool result page.

10. Can OpUtils be run as a service?

Yes, OpUtils can be run as a windows service. Installing OpUtils as a service can either be done during installation or later by selecting **Start --> Programs --> ManageEngine OpUtils 5 --> Administrative Options --> Install Service** option.

11. How can I get the list of used IP Addresses in my network?

Use the Ping Scan tool to scan a subnet and retrieve the list of IP Addresses used.

12. Is there any tool to help me identify if a specified Host Name is a virtual host?

Use the DNS Resolver tool to check virtual host details.

13. Can I know the NIC type of a machine using OpUtils?

Use the MAC Address Resolver tool to retrieve NIC type.

14. Can CISCO devices and Web Servers be monitored using Bandwidth monitor?

Yes. Bandwidth Monitor can monitor any device that supports SNMP.

Troubleshooting Tips

Installation and Startup

1. If I connect to the OpUtils from web browser (IE), it is asking user name and password, what to do ?

The default user name and password to login to OpUtils is admin and admin respectively. Provide the username and password to login.

2. I started OpUtils, but it says port 7080 is occupied. What should I do?

OpUtils by default run at port 7080. If this port is occupied, you will be prompted to specify your desired port number while starting OpUtils server.

3. Whenever I start OpUtils, the browser opens to launch the client? Is there a way I can disable this?

Yes, you can disable this by clearing the "Open the client upon successful server startup" option under settings --> Server.

4. After logging into the OpUtils client, clicking any links or tabs from the welcome screen takes me back to the login page. Why?

The possible reasons could be:

1. The DNS name is not configured the DNS Server - Try giving the IP Address to connect to the client.
2. Mis-configuration in Browser settings - Try connecting to the client from a different browser/ machine.
3. Security configuration, if any security software is installed - check after stopping the security software.

5. In the startup, some extra processes are running in the windows task manager, why?

The following processes are started along with OpUtils:

1. A javaw.exe process for the OpUtils server,
2. A javaw.exe process for the system tray operations, and
3. A fbserver.exe for the FireBird database server.

Diagnostic Tools

1. I installed the product in Linux machine, why is the default IP shown as 127.0.0.1?
2. Devices are not responding to ping.
3. Why does the Ping Tool hang when the Server runs in a Linux Machine?
4. When a machine is SNMP enabled why does SNMP Ping tool display it as non-SNMP node?
5. Why does the Trace Route tool display 3 different Response Time?
6. Can Proxy Ping be initiated from any Router?
7. Is there a way to increase the timeout value for Ping?
8. I see junk characters when I query a non-English machine. What should I do ?

1. I installed the product in Linux machine, why is the default IP shown as 127.0.0.1?

This problem occurs when the 'hosts' file under '/etc' directory has the corresponding hostname as an entry. Delete the entry. This will ensure the machine IP is displayed correctly.

2. Devices are not responding to ping.

This happens if

1. the device is not in the network
2. ICMP request times out
3. the packet size is too big

To resolve the ICMP Timeout, and the packet size issue, click the Settings link. In the ICMP table,

- Increase the Timeout value. The max value is 5000.
- Reduce the packet size. The min value is 0.

Note: When a Linux device is pinged, the default number of packets sent are 8 ICMP packets+ the number of packets specified by the user in the ICMP table. Hence, even if the packet size is reduced to 0 by the user, ping by default will sends 8 ICMP packets to the device.

3. Why does the Ping Tool hang when the Server runs in a Linux Machine?

The possible reason could be the given input machine is not in the network, but it's DNS name entry is present in the DNS Server. To resolve the issue update your DNS Server.

4. When a machine is SNMP enabled why does SNMP Ping tool display it as non-SNMP node?

To check SNMP settings go to **Admin -> Settings -> SNMP** page.

5. Why does the Trace Route tool display 3 different Response Time?

Each of the response columns indicates the response time of that router as each hop is tested thrice.

6. Can Proxy Ping be initiated from any Router?

No. Proxy Ping should be initiated from a CISCO router as Proxy PING uses the proprietary Cisco "Remote PING" MIB within CISCO IOS.

7. Is there a way to increase the timeout value for Ping?

Yes, you can increase the timeout value from **Admin --> Settings --> ICMP** page.

8. I see junk characters when I query a non-English machine. What should I do ?

To resolve the issue choose **Admin** and click on **Settings** available in the left panel. Choose the **General** tab. Enter appropriate character coding value and click Save. If the specified character coding is present in the server machine, it will be saved or else the default value is set. Also ensure your browser supports the specified character coding.

Address Monitoring Tools

1. Devices are identified by incorrect IP addresses and host names.
2. The Subnet List Tool does not display all the subnets in the network.
3. How to enable the MAC Address Scan tool to resolve more number of MAC Addresses?
4. When I run the IP Address Manager Tool for the first time, it does not show any IP Address as available though I have free IP Addresses available in my subnet.

1. Devices are identified by incorrect IP addresses and host names

The possible reasons could be:

the DNS Server is not reachable.
the DNS Server is down.
the DNS Server does not exist.

Try the Ping Tool.

2. The Subnet List Tool does not display all the subnets in the network

Subnet List creates the list of subnets by scanning the route tables, hence if the subnets have been summarized into a summary route on the router you are scanning, the Subnet List will not be able to discover the subnets in the network.

3. How to enable the MAC Address Scan tool to resolve more number of MAC Addresses?

To enhance the performance of the MAC Address Tool either ping scan your network,or specify the router and the subnet input in the Global Environment setting.

4. When I run the IP Address Manager Tool for the first time, it does not show any IP Address as available though I have free IP Addresses available in my subnet.

When you run the IP Address Manager for the first time, all the responding IP's are shown as used and non-responding IP's are put in transient state. This is because, not all the non-responding IP's are necessarily available; it may be down as well. If an IP **continuously** never respond in the next 10 days, then it will be shown as available.

Server Monitoring Tools

1. I am not able to get the desktop details for an non-SNMP device?
2. SNMP is enabled in all of my Linux servers. But I am not able see CPU utilization. What can be the possible reason?
3. CPU Monitor neither plots nor throws any error when I give Linux machine as input?

1. I am not able to get the desktop details for an non-SNMP device?

All the tools under the Server Monitoring tab retrieves data through SNMP. Enable SNMP in the device to get the details.

To check whether a device is SNMP-enabled or not, use the SNMP Ping tool.

2. SNMP is enabled in all of my Linux servers. But I am not able see CPU utilization. What can be the possible reason

Though the system is SNMP-enabled, OpUtils cannot fetch data as the agent does not support Host Resources MIB. Read the SNMP installation section to install recent version of SNMP agent in your system and configure the agent.

3. CPU Monitor neither plots nor throws any error when I give Linux machine as input?

This happens when the specified OID is implemented in the machine but the OID does not have any value.

Network Monitoring Tools

1. Performance Monitor tool does not show the list of correct Interfaces.
2. Switch Port Mapper displays only the MAC Address and not the IP Address.
3. How should I improve the performance of Switch Port Mapper as it is currently resolving very few MAC Addresses?

4. I did a 'Switch Port Mapping' using the Switch Port Mapper tools in OpUtils. In the results, I can see several devices connected to a single switch port? How is this possible?

1. Performance Monitor tool does not show the list of correct Interfaces.

This happens if the SNMP agent is not running in the device. Enable SNMP in the device.

To check whether a device is SNMP-enabled or not, use the SNMP Ping tool.

2. Switch Port Mapper displays only the MAC Address and not the IP Address.

The possible reasons could be:

1. The Router input is not specified. Enter the Router name to map MAC Addresses to IP Addresses. The Router should be in the same subnet as that of the devices connected to the switch.
2. If the router input is not specified, the information is obtained from the ARP cache of the switch. A cache file is also maintained locally to store this information. Perform a ping scan of the subnet to update the cache and then perform the Switch Port mapping. This will improve the MAC to IP resolution.

3. How should I improve the performance of Switch Port Mapper as it is currently resolving very few MAC Addresses?

Use the Ping Scan tool to scan the network where the input router is present to improve the performance of the Switch Port Mapper tool.

Alternatively, specify the router and the subnet input in the Global Environment setting.

4. I did a 'Switch Port Mapping' using the Switch Port Mapper tools in OpUtils. In the results, I can see several devices connected to a single switch port? How is this possible?

One possible reason could be that the device connected to that port is a Switch/Hub. In that case, the Switch Port Mapper will show the devices that are connected to that Switch/Hub.

Cisco Tools

1. Will I be able to get the Access Lists of a router in the AAA/ACS setup?
2. I do not have a username to access my router through CLI. What should I provide in the Username field?
3. In the ConfigFile Viewer tool, I am not getting the Startup Config file. It says "Cisco Config Copy MIB" is not supported?
4. Why do I get the error "E5003: Unable to bind to Port -69" in Config File Viewer?

1. Will I be able to get the Access Lists of a router in the AAA/ACS setup?

Yes. To get the Access Lists of a router un the AAA/ACS setup, provide the username and password in the respective fields.

2. I do not have a username to access my router through CLI. What should I provide in the Username field?

The username is required only for routers in AAA/ACS setup. Leave it blank, if it is not required.

3. In the ConfigFile Viewer tool, I am not getting the Startup Config file. It says "Cisco Config Copy MIB" is not supported?

Startup Config file of the router can be retrieved only if the Cisco Config Copy MIB is implemented in the router. If this MIB is not implemented, you can only view the Running Config file.

4. Why do I get the error "E5003: Unable to bind to Port -69" in Config File Viewer?

The Config File Viewer starts the TFTP Server at port 69 for downloading the config files from the Cisco devices. This error message is shown when it is unable to start the TFTP server at port 69, which can be due to the following:

1. When OpUtils is not started as a root in Linux operating systems.
2. When port 69 is already occupied by some other service.

SNMP Tools

1. The MIB Node Viewer shows an error as "Unrecognized OID"?
2. Why do I get the error "E5003: Unable to bind to Port -162" in Trap Receiver tool?
3. Is it possible to receive the traps with community string as other than public?

1. The MIB Node Viewer shows an error as "Unrecognized OID"?

The MIB Node Viewer retrieves the details of the specified OID from the MIB Database. If the specified OID is not present in any of the MIBs available in the MIB database, this error is shown.

However, you can add your own MIBs to the MIB Database and view the details using the MIB Node Viewer tool.

2. Why do I get the error "E5003: Unable to bind to Port -162" in Trap Receiver tool?

This error message is shown when it is unable to start the trap listening service at port 162, which can be due to the following:

1. When OpUtils is not started as a root in Linux operating systems.
2. When port 162 is already occupied by some other service.

3. Is it possible to receive the traps with community string as other than public?

Yes. Specify all the community strings as comma separated values in **Settings --> SNMP**.

Known Issues and Limitations

Known Issues

- ARP based MAC address resolving for Non- SNMP Nodes, will not work if the given IP is present in a different network in the VLAN environment
- When an HTML report is mailed, the images for the report will not be attached with the mail (i.e., the text content are only displayed).
- To stop the Email alerts configured for devices using the Bandwidth Monitor tool, you have to manually remove the configurations and save.
- Lower versions of Mozilla 1.5 , Netscape 7.0 and IE 5.5 are not supported.

Limitations

- Edit option is not available for Custom Tools.
- Firebird has to be manually installed in Linux.

Glossary

A B C D E F G H I J K L M N O P Q R
S T U V W X Y Z

A

ARP

Address Resolution Protocol. is an internet protocol used to map an IP address to a MAC address. ARP is a required TCP/IP standard defined in RFC 826. ARP resolves IP addresses used by TCP/IP-based software to Media Access Control addresses used by LAN hardware. ARP provides the following protocol services to hosts located on the same physical network.

- Media access control addresses are obtained by using a network broadcast request in the form of the question "What is the media access control address for a device that is configured with the enclosed IP address?"
- When an ARP request is answered, both the sender of the ARP reply and the original ARP requester record each other's IP address and media access control address as an entry in a local table called the ARP cache for future reference.

Access List

A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

B

Bandwidth

The speed at which a communications system can transfer data, usually measured in bits per second.

Broadcast Address

A special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones

BPS

Short for Bits Per Second. In data communications, bits per second (abbreviated bps) is a common measure of data speed for computer modem and transmission carriers. As the term implies, the speed in bps is equal to the number of bits transmitted or received each second.

Bottleneck

Bottlenecks refers to the delay in transmission of data through the circuits of a computer's microprocessor or over a TCP/IP network. The delay typically occurs when a system's bandwidth cannot support the amount of information being relayed at the speed it is being processed. There are, however, many factors that can create a bottleneck in a system.

Bottlenecks affect network performance by slowing down the flow of information transmitted across networks. TCP/IP connections were originally designed to transmit only text files, and the proliferation of bandwidth-intensive transmissions such as high-resolution graphics has caused bottlenecks in the process; therefore, the data moves more slowly across networks.

Broadcast Storm

An undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs. Broadcast storms can usually be prevented by carefully configuring a network to block illegal broadcast messages.

Buffer

A storage area used for handling data in transit. Buffers are used in internetworking to compensate for differences in processing speed between network devices. Bursts of data can be stored in buffers until they can be handled by slower processing devices. Sometimes referred to as a packet buffer.

Byte

A byte is a unit of data that is eight binary digits long. A byte is the unit most computers use to represent a character such as a letter, number, or typographic symbol (for example, "g", "5", or "?")

C

CDP

Short for Cisco Discovery Protocol. CDP is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. The devices do not need to have any network layer protocols configured in order to use CDP, although if these addresses are configured CDP will discover them.. Each device configured for CDP sends out periodic messages to a MAC layer multicast address. these advertisements include information about the capabilities and software version of the advertising platform. This gives you an easy way to see other Cisco devices on your network without having to figure out which devices are Cisco by the vendor code embedded in the Media Access Control address.

Configuration Register

All Cisco Router have a 16-bit configuration register, which is stored in a special memory location in NVRAM. This register controls a number of function, some of which are listed below:

- Force the system into the bootstrap program
- Select a bootsource and default boot file name
- Enable or disable the console Break function
- Set the console terminal baud rate

- Load operating software from ROM
- Enabling booting from a TFTP Server

The configuration register boot field is the portion of the configuration register that determines whether the router loads an IOS image, and if so where to get this image from. The least significant four bits, bits 0 through 3, of the configuration register make up the boot field.

If the boot field value is 0x0 (all four bits set to zeros), the router will enter ROM monitor mode.

If the boot field value is 0x1 (binary 0001), the router will boot from the image in the ROM.

If the boot field value is 0x2 through 0xF (binary 0010 through 1111) the router will follow the normal boot sequence and will look for boot system commands in the configuration file in NVRAM.

Community String

The Community String is a "password" that allows either Read Only (RO) or Read/Write (RW) control.

D

DHCP

Short for Dynamic Host Control Protocol. An effective way to dynamically assign and reuse a fixed number of IP addresses when there are more devices on the network than addresses available. A DHCP server dynamically assigns IP addresses to devices requesting them. These address assignments expire after a time specified by the network manager. The DHCP server then reassigns these addresses to other devices as needed. DHCP is an extension to BOOTP in which the address assignments are static.

DNS

Short for Domain Name System (or Service). The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

DNS Server

The DNS system consists of three components: DNS data (called resource records), servers (called name servers) and Internet protocols for fetching data from the servers. DNS Name server is a server that runs DNS server programs containing name-to-IP address mappings, IP address-to-name mappings, information about the domain tree structure, and other information. DNS servers also attempt to resolve client queries.

The billions of resource records in the DNS are split into millions of files called zones. Zones are kept on authoritative servers distributed all over the Internet, which answer queries based on the resource records stored in the zones they have copies of. Caching servers ask other servers for information and cache any replies. Most name servers are authoritative for some zones and perform a caching function for all other DNS information. Large name servers are often authoritative for tens of thousands of zones, but most name servers are authoritative for just a few zones.

Dword Address

A portion of memory, usually a variable, which has a length of four bytes. The term dword is given to anything which is four bytes in length. Literally, a dword is a "double word."

For example for the IP Address 206.191.158.55, enter the following keystrokes into the calculator exactly as shown:
206 * 256 + 191 = * 256 + 158 = * 256 + 55

The dword equivalent of the IP address will be the result. In this case, 3468664375.

E

Errors and Discards

In Performance monitoring Errors and Discards refers to the number of packets that could not be transmitted because of errors which results in discarded packets.

F

Forward Lookup

Forward DNS (domain name system) Lookup uses an Internet domain name to find an IP address. When you enter the address for a Web site at your browser, the address is transmitted to a nearby router which does a forward DNS lookup in a routing table to locate the IP address. Forward DNS lookup is the more common lookup since most users think in terms of domain names rather than IP addresses.

Flash Memory

A special type of EEPROM (electrically erasable programmable read-only memory) that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a Flash memory chip so that it can be updated easily if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.

G

Giants

Giants refers to the number of packets that are discarded by the router because they exceed the medium's maximum packet size.

H

HEX IP Address

A major numbering system used by computers is hexadecimal or Base 16. In this system, the numbers are counted from 0 to 9 then letters A to F before adding another digit. The letter A through F represent decimal numbers 10 through 15 respectively. The below chart indicates the values of the hexadecimal position compared to 16 raised to a power and decimal values It is much easier to work with large numbers using hexadecimal To convert a value from hexadecimal to binary, you merely translate each hexadecimal digit into its 4-bit binary equivalent. Hexadecimal numbers have either and 0x prefix or an h suffix. For example, the hexadecimal number:

0x3F7A

Translates into, Using the Binary chart and the below chart for Hex:
0011 1111 0111 1010. values than decimal.

DECIMAL	HEXADECIMAL	BINARY
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Hop

Gives the order in which the TCP/IP packets progress from machine to machine, called the 'distance' (in hops) from the originating machine.

Host Address

A fully qualified domain name (usually alphabetic) identifying the address of one specific host computer on the Internet. The host address is a subset of the IP address.

I

ICMP

Short for Internet Control Message Protocol. ICMP is an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

In Discards

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.

IOS

Short for Internetworking Operating System. The Cisco IOS software is the software that runs on the Cisco products, This platform is integral to the interoperations of network devices in a Cisco internetwork. Cisco IOS includes security, access control, authentication, firewall, encryption, and management services. The main purpose of IOS is to boot the Cisco hardware and begin the optimal transport of data across the internetwork.

IP Address

The 32-bit IP address is often depicted as a dot address that is, four groups (or quads) of decimal numbers separated by periods. Here's an example:

130.5.5.25

Each of the decimal numbers represents a string of eight binary digits. Thus, the above IP address really is this string of 0s and 1s:

10000010.00000101.00000101.00011001

Some portion of the IP address represents the network number or address and some portion represents the local machine address (also known as the host number or address). IP addresses can be one of several classes, each determining how many bits represent the network number and how many represent the host number. The most common class used by large organizations (Class B) allows 16 bits for the network number and 16 for the host number. Using the above example, here's how the IP address is divided:

```
<--Network address--><--Host address-->
       130.5     .       5.25
```

If you wanted to add subnetting to this address, then some portion (in this example, eight bits) of the host address could be used for a subnet address.

Thus:

```
<--Network address--><--Subnet address--><--Host address-->
       130.5         .         5        .     25
```

K

kbps

Short for kilobit per second**.** One kilobit per second (Kbps) equals 1000 bits per second (bps). Network performance is best measured in bps, but sometimes numbers are given in bytes per second (Bps). Then, one KBps equals one kilobyte per second, one MBps equals one megabyte per second, and GBps equals one gigabyte per second.

L

Latency

The time delay of data traffic through a network or a switch.

M

MAC Address

Short for Media Access Control address. MAC Address is a standardized data link layer address that uniquely identifies each device and is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6bytes long and area also known as a hardware address, MAC layer address, and physical address.

MIB

Short for Management Information Base. MIB is a database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Macros

The MIB file can contain one or more MIB modules.

Following are the macros defined in the SMIv1 and SMIv2.

OBJECT IDENTIFIER
OBJECT-TYPE

The following macro definition is defined only in SMIv1.

TRAP-TYPE

The following macro definitions are defined only in SMIv2.
MODULE-IDENTITY
NOTIFICATION-TYPE
OBJECT-IDENTITY

OBJECT-GROUP
AGENT-CAPABILITIES
NOTIFICATION-GROUP
MODULE-COMPLIANCE
TEXTUAL-CONVENTION

N

Netmask

A netmask is a 32-bit mask used to divide an IP address into subnets and specify the networks available hosts. In a netmask two bits are always automatically assigned. For example in 255.255.225.0, "0" is the assigned network address and in 255.255.255.255, "255" is the assigned broadcast address. The 0 and 255 are always assigned and cannot be used. (http://www.computerhope.com/jargon/n/netmask.htm)

Network Classes

Class A Network - binary address starts with 0, therefore the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octet) identify the network and the remaining 24 bits indicate the host within the network. An example of a Class A IP address is 102.168.212.226, where "102" identifies the network and "168.212.226" identifies the host on that network.

Class B Network - binary addresses starts with 10, therefore the decimal number can be anywhere from 128 to 191. (The number 127 is reserved for loopback and is used for internal testing on the local machine.) The first 16 bits (the first two octets) identify the network and the remaining 16 bits indicate the host within the network. An example of a Class B IP address is 168.212.226.204 where "168.212" identifies the network and "226.204" identifies the host on that network.

Class C Network - binary addresses starts with 110, therefore the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network and the remaining 8 bits indicate the host within the network. An example of a Class C IP address is 200.168.212.226 where "200.168.212" identifies the network and "226" identifies the host on that network.

Class D Network - binary addresses starts with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multicasting.

Class E Network -- binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented or utilized in a standard way.

NIC

Short for Network Interface Card. A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or Token Ring. Network interface cards provide a dedicated, full-time connection to a network.

NVRAM

Short for nonvolatile RAM. NVRAM is a special memory that does not lose its information when a router is powered off. It stores the system's startup configuration file and the virtual configuration register.

O

Octet Flow

In network monitoring the term Octet flow refers to the number of octets transmitted over the interface.

OID

Short for Object Identifier. The OID is a long numeric tag, used to distinguish each variable uniquely in the MIB and in SNMP messages.

Out Discards

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.

P

Packet Flow

A flow is a set of packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties derived from the data contained in the packet and from the packet treatment at the observation point.

Q

QoS

Quality of Service standards seek to maximize the use of available network bandwidth by prioritizing time-sensitive traffic.

Top

R

RAM

Short for random-access memory. RAM is a volatile memory that can be read and written by a computer.

Received Errors

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Reverse Lookup

Reverse DNS lookup uses an Internet IP address to find a domain name.

Round Trip Time

The Round Trip time refers to the timestamp placed by Ping in each packet, which is echoed back to calculate how long each packet exchange took.

Router

A router is an Intermediate System (IS) which operates at the network layer of the OSI reference model. Routers may be used to connect two or more IP networks, or an IP network to an internet connection.

A router consists of a computer with at least two network interface cards supporting the IP protocol. The router receives packets from each interface via a network interface and forwards the received packets to an appropriate output network interface.
A router introduces delay (latency) as it processes the packets it receives. The total delay observed is the sum of many components including:

- Time taken to process the frame by the data link protocol
- Time taken to select the correct output link (i.e. filtering and routing)
- Queuing delay at the output link (when the link is busy)
- Other activities which consume processor resources (computing routing tables, network management, generation of logging information)

The router queue of packets waiting to be sent also introduces a potential cause of packet loss. Since the router has a finite amount of buffer memory to hold the queue, a router which receives packets at too high a rate may experience a full queue. In this case, the router has no other option than to simply discard excess packets. If required, these may later be re-transmitted by a transport protocol.

ROM

Short for read-only memory. ROM is the non volatile memory that can be read , but not written , by the computer. The image in ROM is the image the router first uses when it is powered up. This image is usually an older and smaller version of IOS without the features of a full IOS version.

Runts

Runts refers to the number of packets that are discarded because they are smaller than the medium's minimum packet size.

S

SNMP Agent

A management entity consisting of hardware and embedded software which responds to SNMP requests over Ethernet from an SNMP manager

Subnet

A subnet (short for "subnetwork") is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Without subnets, an organization could get multiple connections to the Internet, one for each of its physically separate subnet, but this would require an unnecessary use of the limited number of network numbers the Internet has to assign. It would also require that Internet routing tables on gateways outside the organization would need to know about and have to manage routing that could and should be handled within an organization.

The Internet is a collection of networks whose users communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address (Internet Protocol address). This 32-bit IP address has two parts: one part identifies the network (with the network number) and the other part identifies the specific machine or host within the network (with the host number). An organization can use some of the bits in the machine or host part of the address to identify a specific subnet. Effectively, the IP address then contains three parts: the network number, the subnet number, and the machine number.

(adapted from searchNetworking.com)

Subnet Mask

A subnet mask is used to determine what subnet an IP address belongs to.

SMTP

Internet protocol providing e-mail services.

T

TCP / IP

TCP/IP - Stands for "Transmission Control Protocol / Internet Protocol" - TCP/IP is a suite of communications protocols that forms the basis for and defines the Internet.

Transmitted Errors

The number of outbound packets that could not be transmitted because of errors.

TTL

Short for Time to Live. TTL is a field in the Internet Protocol (IP) that specifies how many more hops a packet can travel before being discarded or returned.

Timeout

Timeout is the value to be set in milliseconds to wait for each packet reply before the connection is disconnected as no data is being sent.

U

UDP

A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams (a datagram is the term used to describe data that is packetised for network transport) typically over an IP network. It is used primarily for broadcasting messages over a network. UDP uses the Internet Protocol to get data from one computer or device to another but does not divide a message into sequenced packets nor reassemble it at the other end.