

# Assignment One

## ITN534 – Network Management

**Title:** Report on an Integrated Network Management Product (*Solar winds 2001 – Engineer's Edition*)

Unit Co-coordinator,  
*Mr. Neville Richter*

By,  
*Vijayakrishnan Pasupathinathan (N2810743)*  
*v.krishnanp@student.qut.edu.au*

### Abstract

In today's networking environment the task of system administrators are enormous. The task of maintaining the availability of devices like routers, hubs, servers, etc., to the end-users are critical in a modern day environment. To maintain such system, managers would like to monitor network devices for bandwidth utilization, bottlenecks, cabling and routing information. As networks continue to grow in size and complexity, the need for management tools increases. This report is an investigation of some of the tools that are available in Solar Winds 2001 – Enterprise Edition.

## 1. Introduction

Network management tools are very essential in today's networking environments, which are huge and complex. They provide network administrators with valuable information on current condition of the network, the network devices like routers, hubs, etc.

The important point that has to be considered while looking for a good management tool is how accurate the tool depicts the behavior of the network. It is also crucial for the tool to portray the result in a graphical form making it easier for network managers to understand the conditions of the network quickly and accurately.

Solar Winds 2001 is a network management tool for Windows class of Operating systems. The engineer's edition contains a set of 36 Network management tools. The investigation of this product was carried out in an evaluation version of the engineer's edition which is freely downloadable from the company's website. (<http://www.solarwinds.net>)

## 2. Product Description

The tools in Solar Winds 2001 are classified into 9 categories:

- I. Network performance monitoring
- II. Network discovery
- III. Network monitoring
- IV. Tools for CISCO networks
- V. IP address management
- VI. Security
- VII. Ping and Diagnostic
- VIII. MIB browser
- IX. Miscellaneous

Each of the above categories consists a set of tools that perform network management tasks.

Network performance monitoring include tools like *Bandwidth Monitor*, *Router CPU load*, *Advance Bandwidth Monitor* and *Network performance Monitor*. Bandwidth monitor tool, monitor's the amount of data being received and transmitted for any remote network device. It uses SNMP to communicate with a remote device and gather bandwidth statistics. Router CPU Load tool, monitors the load on multiple Cisco routers concurrently. Advance Bandwidth Monitor is an extension of bandwidth monitor and can

be used for monitoring the bandwidth utilization of a usage based service provider. It also provides a better graphical display of the results.

Network Discovery tools include tools like *Subnet list*, *Ping sweep*, *DNS Audit*, *IP Network browser*, *IP Address Management*, *MAC Address discovery*, *SNMP sweep*, *Network Sonar*. The Subnet List tool is used in discovery of all subnets on a network. Ping Sweep displays IP addresses are in use and also supports reverse DNS lookup for each address. DNS Audit scans a range of IP Addresses and performs Forward and Reverse Look-up. IP Network browser scans and performs a detailed discovery on one device or an entire range. IP Address Management automatically determines IP addresses are not in use and how long it has been since they have been used. MAC address discovery scans the subnet and constructs a table of relating IP Address to MAC Address. SNMP sweep queries the IP Address range defined and then locates both used & unused IP Addresses. Network sonar is an SNMP discovery engine, which creates a detailed discovery database of the network. It can exports results into MS Access for easy analysis.

Network Monitoring tools include tools like *Watch It*, *Network Monitor*, *Network Performance Monitor*, *Syslog server*. Watch it monitors the availability of devices and will notify the user the moment a router, circuit, or server becomes unavailable. Network monitor is an interactive performance and fault monitor, Network Monitor will alert the user with visual and audible alarms and is also capable of sending email and paging. SysLog Server listens for incoming Syslog messages on UDP port 514 and then decodes the messages for logging purposes.

Tools for Cisco Works include tools like *IP Network Browser*, *Router CPU load*, *Config Downloader*, *Config Uploader*, *Config editor/viewer*, *Proxy ping*, *Compare running v/s startup configs*, *Router password decryption*.

Tools for IP Address Management include tools like, Advanced Subnet Calculator, which runs a real-time DNS and PING test, and generate subnets. DNS/Who is resolver tool does forward and reverse DNS looks-ups. It also allows determining who owns or controls a Domain Name, Network or IP Address. DHCP Scopes monitors and shows which scopes are low on addresses. The number of dynamically assigned (and unassigned) IP Addresses for each scope is displayed.

Security tools include tools like, *Router password Decryption*, *Dictionary editor*, *TCP reset*, *SNMP- brute force attack*, and *SNMP- dictionary attack*. Router Password can be used to change any Cisco configuration parameter via SNMP. Dictionary Editor is used with SNMP Dictionary Attack tool. The editor allows making additions to the dictionaries or import new dictionaries directly. TCP reset can be used to set the name, contact, and location for network printers, hubs, and terminal servers. The SNMP Brute Force Attack will remotely determine an SNMP read-only or read-write community string by trying every possible combination of letters and numbers. The SNMP Brute Force Attack determines an SNMP read-only or read-write community string by trying every possible combination of letters and numbers.

Ping and Diagnostic tools include tools like, *Ping*, *Enhanced ping*, *Trace route*, *Proxy ping*, *Ping sweep*. Ping tool does a simple ping. Enhanced ping can be used to view multiple devices concurrently. The results are displayed both graphically as well as in a table at the bottom of the screen. Trace route traces a route from computer to any other device; it also displays the response time for each node by resolving the DNS real

time. Proxy Ping tools remotely initiates a PING test from any remote Cisco router to any other SNMP enabled device.

MIB Browser tools include tools like, *MIB walk, MIB browser and Update system MIB's*. MIB Walk will walk the SNMP tree for a target device and dump the value of each OID and produce a complete listing of all supported MIB's and OID's and report the current setting for each OID. The MIB Browser uses extensive MIB database of over 100,000 unique OID's compiled from over a thousand standard and proprietary MIB's. The MIB Browser can walk MIB trees, view MIB tables, search MIB's, remotely modify SNMP values, and many other SNMP functions. Update system MIB's tool is used to download the System information from any Cisco MIB, edit the information and upload the edits.

Miscellaneous tools include tools like, *TFTP Server and WAN killer*. TFTP server is a multi-threaded server and can transmit and receive multiple files concurrently. WAN Killer is a Wide Area Network traffic generator; it can be used to set the circuit bandwidth and the percent of load needed and WAN Killer will generate random traffic.

### 3. Considerations for Measurement of the product

The following aspects were considered during the evaluation of the tools: -

- a) *Efficiency and speed* of the software:
- b) *Price* evaluation of the software.
- c) Level of *support* provided by the *Vendor*
- d) *Tools functionality* to perform various management tasks.
- e) *User Interface* of the software.
- f) *Support* of the tools to *various hardware*.
- g) The *requirements* of the software *on the system*.

The following TEN tools were evaluated during this assignment:

- Bandwidth Monitor
- Network Performance Monitor
- IP Network Browser
- MAC Address Discovery
- Network Monitor
- Watch it
- IP Address Management
- Advance subnet calculator
- Ping and Enhanced Ping
- Trace route.

The software was evaluated in 2 stages.

Stage One consisted of examining the software in its entirety. The system requirements and support of the software, Pricing of the software and Vendor support provided with the software.

Stage Two consisted of examining the ten tools that were chosen for evaluation in this assignment. The tools were evaluated on basis of their functionality, Efficiency, user interface and support both in term of hardware and software.

**The analysis of the evaluation based on the above criteria's are as follows:**

**System Requirements:** The system requirements of the software for the solar winds engineer's edition as suggested by the company are:

<u>Operating system:</u>	Windows 95/ 98/NT/2000/ Millennium.
<u>CPU:</u>	Pentium II 500Mhz and higher.
<u>Memory:</u>	128MB or higher recommended.
<u>Disk Space:</u>	200MB plus
<u>Network Connection:</u>	Network Card or Modem
<u>Software:</u>	Internet Explorer.
<u>Others:</u>	Sound card recommended.

**Pricing:** The Solar winds 2001 – Engineer's Edition is priced at **\$995** for a single user license and **\$4475** for a five user license. The company also provides bi annual CD shipments, which includes bug fixes and product enhancements for a nominal fee of \$395 per license for a 12-month subscription.

**Vendor support:** The software is accompanied with help files, which explain the working of various tools that are included in each edition of solar winds. The

**Support:** The software is accompanied with help files, which explain the working of various tools that are included in each edition of solar winds.

**Efficiency:** The software works at a good speed but requires a good amount of memory and processing speed to perform it tasks.

## **Tools**

### *1. Bandwidth Monitor*

**Functionality:** Bandwidth Monitor polls the remote interface about every five (5) seconds and calculates an average bits-per-second since the last poll for outbound (transmitting) and incoming (receiving) data on each interface. Bandwidth Monitor can display real-time traffic utilization for any device that supports

User Interface: The program calculates separate statistics for outbound (transmitting) and incoming (receiving) data on each interface. Gauges can be save to a file and reloaded when necessary. The interface is compact and displays the output in a analogous form.

## *2. Network Performance Monitor*

Functionality: Network performance monitor can track network latency, packet loss, traffic, and bandwidth usage. It can monitor and collect traffic statistics from any device that supports SNMP.

User Interface: The program is accompanied with menus that are include exporting the charts and graphs as pictures or as raw data files. The program displays the network and has additional links to program like telnet, ping , traceroute which can be executed directly from this program.

## *3. IP Network Browser*

Functionality: IP Network Browser scans subnets and show the details about the devices on that subnet. Each IP addresses is PINGed. For each responding address, IP Network Browser attempts to gather more information using SNMP.

User Interface: The program has interfaces to scan an individual device or an entire subnet. If a subnet is scanned the devices in that subnet are displayed in a hirearchical tree structure .

## *4. MAC Address Discovery*

Functionality: This program can discover Physical Addresses for a locally attached subnet.It uses ARP to dicoverly the addresses.

User Interface: The local subnets are displayed in a drop down menu and upon selection of a particular subnet the MAC address of all the terminals in that subnet are shown.

## *5. Network Monitor*

Functionality: The program monitors connections and keeps track of response time and packet losses.

User Interface: The program provides a good interface to display all the nodes. This program is also equiped with event notification such as notification if a network node is down or up. The notification can be either a sound or a dialog box or an e-mail.

## *6. Watch it*

Functionality: Watch is a network monitor.

User Interface: This program places a toolbar on the desktop with light indicating whether a network is up or down. On clicking a light a menu appears and it opens up a list of nodes. This program also has link to other programs like ping, traceroute etc.,

### *7. IP Address Management*

Functionality: This program monitors which IP addresses are in use on your network and it can allocate IP addresses before they are used.

User Interface: The program shows a list containing the information about an IP Address like IP Address Status, DNS name, Machine Type, System Name, Location Response Time. The program can be customised to display only used, available, reserved or all IP addresses.

### *8. Advance subnet calculator*

Functionality: This program helps to calculate subnet masks for IP address.

User Interface: The program displays the subnet mask and the IP address of a particular node. This program can also be used to create a subnet and examine how the IP address can be managed efficiently

### *9. Ping and Enhanced Ping*

Functionality: The ping program does a normal ping on an address and displays the result in a text format. The enhanced ping can be used to monitor several addresses at the same time.

User Interface: The ping program interface is simple and provides just a display in text format. The enhanced ping provides a graphical output.

### *10. Trace route.*

Functionality: This program traces the route taken by the packet to a destination address. It can also display selected SNMP information about the devices it discovers.

User Interface: The program displays the route taken as a list and also provides various other information about the machines that are encountered in the packets path.

## **Conclusion**

The computer is an essential tool for most businesses, and internetworking has allowed for the exchange of information such that the worker of today can work smarter and more efficiently than ever before. In today's Networking Environment the requirement of a good network management tools is of utmost importance.

Solar winds 2001 – Engineers edition is a very valuable tool for network managers providing them with a wide range of tools to monitor, control and help them in overall management of the their network.

A graphical representation of the result even if it is not very accurate would be sufficient to analyse and understand the problem and solar winds 2001 provides a good graphical representation of the network and other statistics.