Simple Network Monitoring System

OVERVIEW

As networks become increasingly complex, managers can no longer afford merely to react to problems, but must position themselves to continuously monitor critical systems and to be among the first to know when systems fail.

Traditional network management systems (NMS) provide a mechanism to scrutinize network operation in great detail. However, these systems are difficult to implement and costly to maintain. The high overhead associated with commercial NMS systems has discouraged many managers from utilizing these solutions – leaving them with few unified tools to anticipate and trouble-shoot network issues.

Switch Technologies, Inc. addresses this dilemma with its Simple Network Monitoring System (SNMS). The design philosophy of SNMS is to provide a service that is easy to purchase, easy to implement and easy to maintain.

SNMS is an authenticated-access, on-site monitoring server administrated via intuitive web pages. Integration into a network can literally take minutes and continued management is equally convenient.

The following pages describe the features of the SNMS solution.

Contact your STI technical representative to find out if this solution works for you.

(631) 228-4405
sales@switchtechnologies.com

Web-Based Interface-

The technician interacts with all features of this system via a normal web browser. Password authentication is required for access to the system. The web page uses the https protocol for additional security.

User Alert System-

The server attempts to contact devices specified in the User Alert System once a minute. If a specified device fails to respond for 5 consecutive contacts a text and/or e-mail is sent to a custom list of recipients.

SNMS logs a Failure History for all device failures for devices in the User Alert System. This history is useful in the identification of devices with periodic, but short, down times.

Traffic Monitoring System-

SNMS contacts specified devices every five minutes to measure traffic across important interfaces. This feature is useful in the identification of traffic bottlenecks. Data is summarized in four charts: Daily, Weekly, Monthly and Annually. These charts enable both short and long term projections for network performance.

Server Monitoring System-

A summary report containing useful information about critical servers is created in real-time when requested. Various drill down reports are available for servers, depending on their ability to provide the information. The system can report on a variety of Mac OSX, Windows, Linux and Unix servers.

Current Device Probe System-

When selected, this page automatically refreshes every two minutes. The system contacts a customized list of devices to determine if they are running. If a device cannot be contacted its display cell turns red.

Port Scan Security System-

This service requires that the port signature of a device be determined and stored in a device database. For example, a web-based mail server might have the following open ports: SSH (22), SMTP (25), HTTP (80) and POP3 (110.) Once in the database, the system performs port scans on a regular interval and compares the results with the database entry for the device. If a port (or service) is *down* an alert can be sent via the text page/e-mail facility. In the evening the system scans the device to determine if a *new* port is has been opened. If an unauthorized port is found and alert is sent. Since hackers typically open back-door ports on a hacked system this facility provides an early warning of any intrusions.

Document Storage-

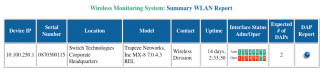
SNMS provides a web interface for simple uploading and down-loading of files to a shared area.

Secure Repository Manager-

The Secure Repository Manager is a highly secure database that can be used to store sensitive information for an unlimited number of objects. Critical information (passwords, system configuration files etc.) are stored on the system in an encrypted format and remain unreadable without a decryption key.

Authenticated users can create, modify, read and delete this information via a web-based interface using the proper encryption key. Encryption keys can be different for each object or similar for user defined object classifications. The key is always sent in an encrypted form to prevent capture by network sniffers. The keys are *not* stored on the SNMS system.

Audit logs are kept that track when a user reads or modifies any object. Authorized user may retire items from the list of available objects. However, retired objects are never deleted. The system administrator can review a list of retired objects and restore any object.


Wireless Monitoring System: Summary WLAN Report

Device IP	Serial Number	Location	Model	Contact	Uptime	Interface Status Adm/Oper	Expected # of SSIDs	DAP Report
10.100.250.1	0839500115	Switch Technologies Corporate Headquarters	Trapeze Networks, Inc MX-8 7.0.4.3 REL	Wireless Division	14 days, 2:33:50		2	

Syslog Server-

Enhance the security of your network and improve trouble-shooting by managing the log files of critical devices to the SNMS server. An easy to use web-based interface allows you to inspect logs easily, storing information by device address and device sub-system.

The system is self-pruning and will generate alerts when the storage area is 60% full. At 80% it will cleave, in half, any file

over 2mbs – discarding the oldest material.

The logs can be rolled to archive servers for long-term storage.

UPS Monitoring System-

SNMS provides a summary report for all UPS devices that are equipped with a networked SNMP service. The report includes information about battery age and condition, current output load ad current input voltage. Also provided is a strip-chart that records input voltage and output load over time for each device.

Wireless Monitoring System-

SNMS provides a summary report for enterprise level wireless controllers. Reports are available for each radio connected to a wireless controller.

Administrative Tools

SNMS is easy to administer. A limited access web page is provided that contains a set of management and configuration tools for each of the previously described systems.

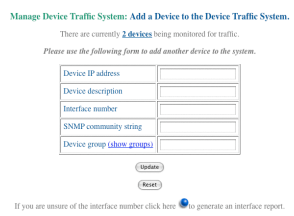
In addition to the system management screens, several general diagnostic tools are available.

Ping Tool-

This tool enables you to contact devices in a variety of ways: using normal ping protocol or using TCP or UDP to specified ports.

Interface Report-

The Interface Report is provided for analysis and inspection of the performance of all interfaces on a device. For a server, this would be each Ethernet NIC, for a switch this would be each switch port. This report includes in and out bytes on each interface, in and



out errors on each interface and a description of the interface setting: full or half duplex, the interface speed and its status.

Port Scanner-

This tool allows the technician to port scan a device and reports the up/down status of a service port in a variety of user selectable formats.

Address Scanner-

This tool allows the technician to enter an IP address range and produce a list of those devices within the range that responded to a contact attempt. The list of responding devices can be easily copied for import to other user programs. In addition, by clicking on a reported address, the manager can produce a device profile wherein SNMS attempts to discern the OS running on the remote system. SNMS also produces a port scan of the system and lists currently running network services on the device.

Trace Route-

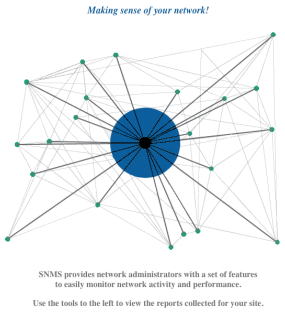
This tool produces a traditional trace route report listing the router hops discovered in the path between the SNMS server and a remote device.

SNMP Tool-

This tool enables the manager to send an SNMP query from the SNMS server to a remote device. The user can specify SNMP versions 1, 2c or 3. Queries can be made to return one data value (a get) or an entire sub-tree (a walk).

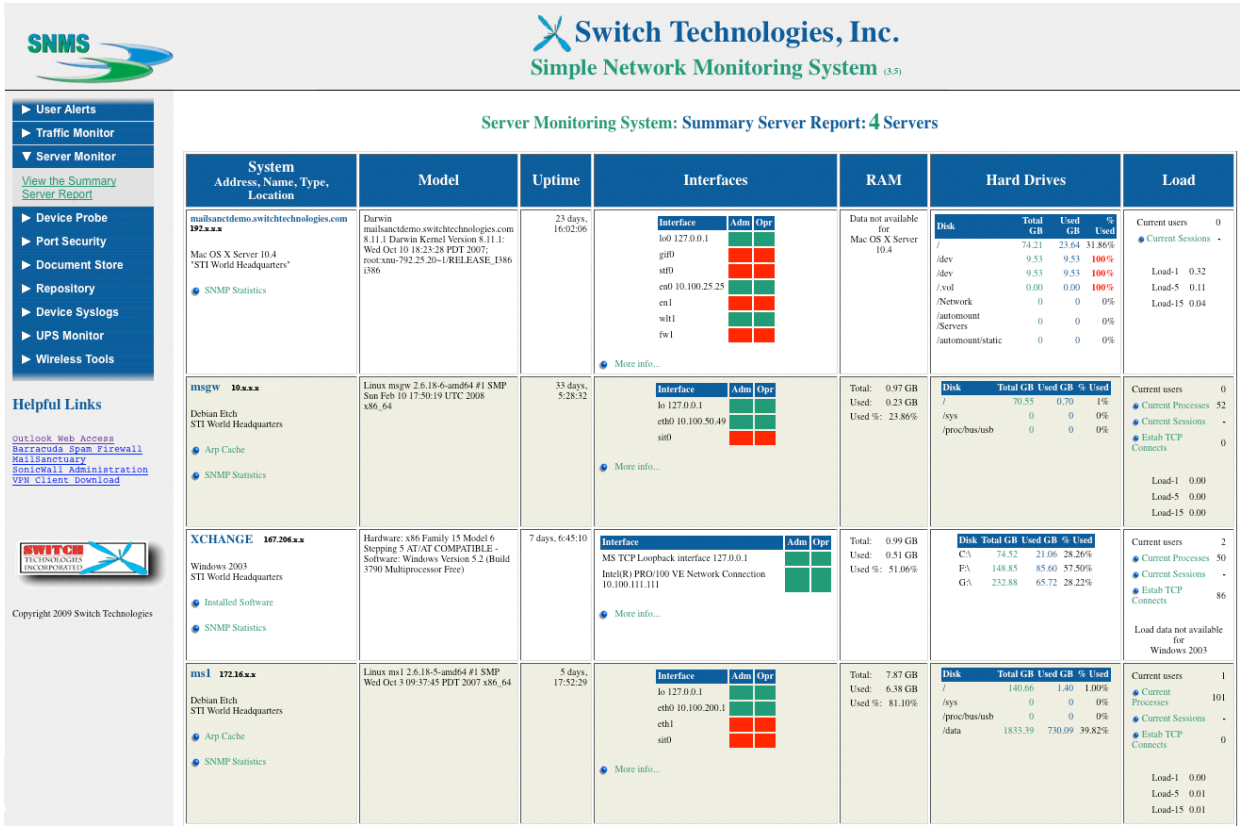
Hardware-

The appliance is fully hardened to protect against intrusion. The server is backed-up on a determined interval to a warm-backup hard drive. If a catastrophic failure occurs on the primary drive the system can be easily re-booted off the warm backup to its state as of the last backup. The system can be up and running again in minutes.

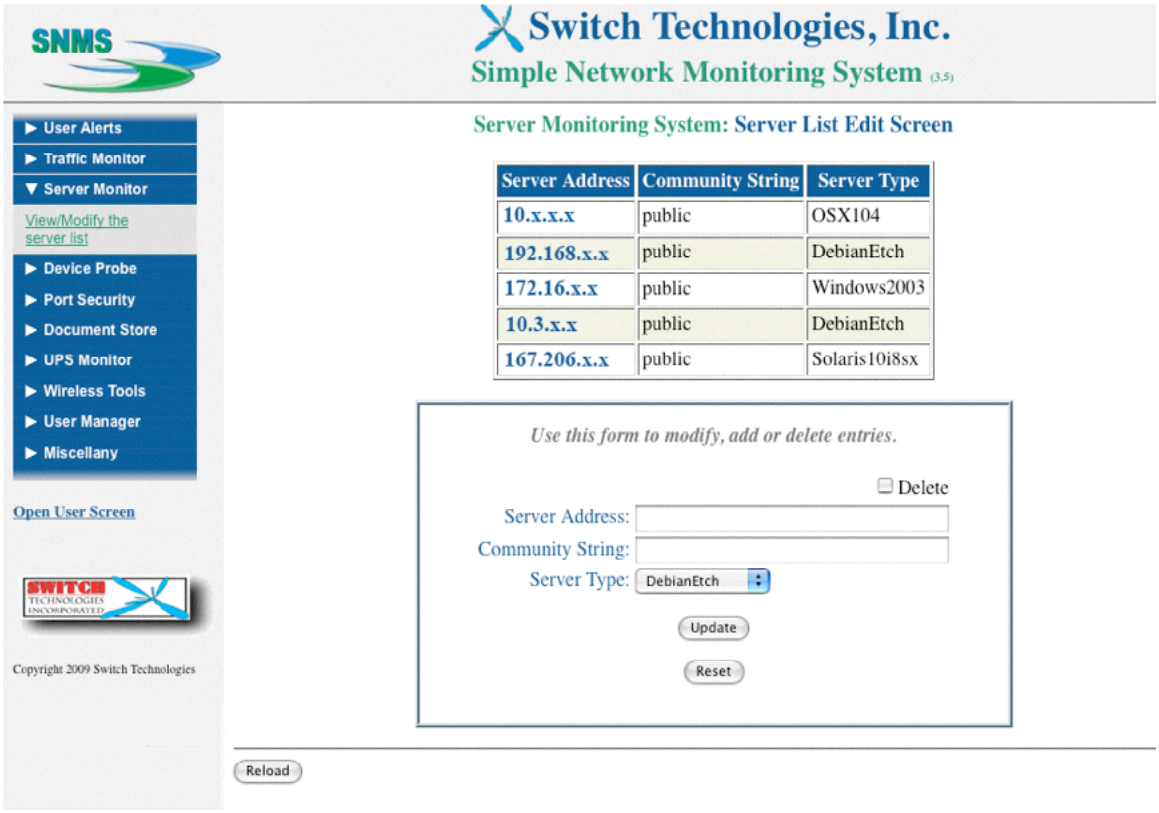


A system status report is performed and mailed to a specified list of users every evening. This report contains information about system performance. The report is always visible on the SNMS server via the System Report tool.

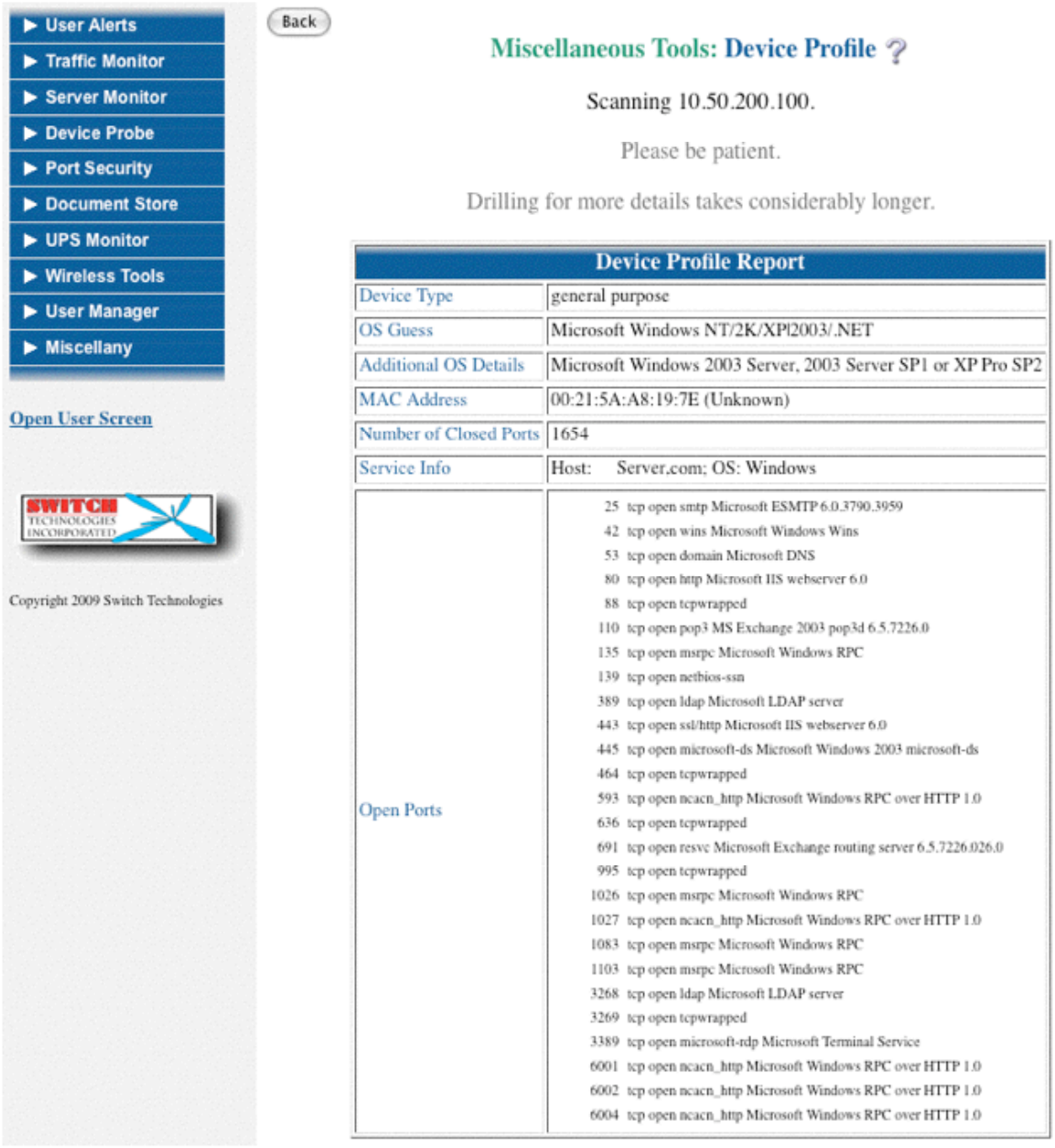
The SNMS User Screen: Displaying Server Summary Report



The SNMS Administrator's Screen: Displaying Server List Edit Screen



A few Screen Shots



UPS Monitoring System: Summary UPS Report

10.50.200.98										
Name	**Location**	**Model**	**Output Load**	**Input Voltage**	**Battery Age**	**Battery Condition**	**Battery Temp.**	**Uptime** (dy:hr:mn:sec.cths)	**Full Report**	**Charts**
Core Network Devices		TRIPP LITE SMART2200RMXL2U	26 %	118.8 V	0.5 Years	OK	107.6 F	42:3:04:51.64		

10.50.200.99										
Name	**Location**	**Model**	**Output Load**	**Input Voltage**	**Battery Age**	**Battery Condition**	**Battery Temp.**	**Uptime** (dy:hr:mn:sec.cths)	**Full Report**	**Charts**
Core Network Devices	NOC Rack - Bottom UPS	TRIPP LITE SMART2200RMXL2U	22 %	120 V	0.5 Years	OK	105.8 F	42:3:01:52.21		

Legend

Battery Condition

1 = Unknown

2 = Normal

3 = Low

4 = Depleted

Switch Technologies, Inc.

Simple Network Monitoring System (3.5)

- ▶ User Alerts
- ▶ Traffic Monitor
- ▶ Server Monitor
- ▶ Device Probe
- ▶ Port Security
- ▶ Document Store
- ▼ Repository
  - Use the Secure Repository
- ▶ Device Syslogs
- ▶ UPS Monitor
- ▶ Wireless Tools

Helpful Links

Outlook Web Access
Barracuda Spam Firewall
MailSanctuary
SonicWall Administration
VPN Client Download

Secure Repository Manager: Manage Secure Repository

Retrieve Information	Owner	Modify Information	Remove from List
UserCreds	admin		
MOA_UserCreds	admin		
MSOffice-2003-key	admin		
RingMasterLicense	admin		
Tel _Licenses	admin		

- **Add** another object to the Secure Repository.
- **View** retired objects.
- **View** audit trail.

Product Specifications

Table 1. Simple Network Monitor System product specifications

Interfaces	
On-Board Dual Gigabit/100/1000T Ethernet	Two 100/1000 full or half-duplex (auto-negotiation) with RJ-45 UTP port
RS-232C Console	DB-9 serial connection, female DCE interface for out-of-band management
Dimensions	
Width	19”
Depth	14”
Height	1 U
Weight	10 lbs
Environmental specifications	
Operating temperature	10 to 35 degrees C
Operating humidity	8% to 80% (non-condensing)
Power specifications	
Power supply	100-240 VAC@ 60-50 Hz, 3.6-1.8 A
Power consumption	240 watts
MTBF	>50,000 hours
Certifications	
Emissions	US==FCC Class B

STI, Inc. is a leading network integration and support company.

Contact info:
www.switchtechnologies.com
sales@switchtechnologies.com
Phone: (631) 228-4405
Fax: (631) 821-2843