

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 downloading 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.

Windows Monitoring System Summary WLAN Report

Device IP	Serial Number	Location	Model	Vendor	System	Interface	Speed	Usage	Signal	Power
10.100.1.1	107000011	Chicago	Linksys WRT54GL	Linksys	Windows XP	eth0	100Mbps	100%	100%	100%

Syslog Server-

Enhance the security of your network and improve troubleshooting 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 and 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

Manage Device Traffic System: Add a Device to the Device Traffic System.

There are currently 2 devices being monitored for traffic.

Please use the following form to add another device to the system.

Device IP address	<input type="text"/>
Device description	<input type="text"/>
Interface number	<input type="text"/>
SNMP community string	<input type="text"/>
Device group (show groups)	<input type="text"/>

If you are unsure of the interface number click here [?](#) to generate an interface report.

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-

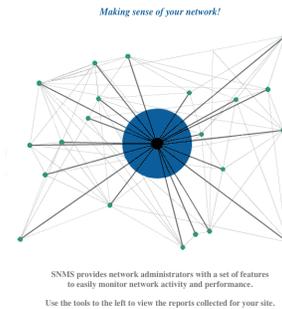
This tool produces a traditional trace route report listing the router hops discovered in the path between the SNMS server and a remote device.

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

Simple Network Monitoring System (3.5)

Server Monitoring System: Summary Server Report: 4 Servers

System Address, Name, Type, Location	Model	Uptime	Interfaces	RAM	Hard Drives	Load																																																												
<p>mailsanctdemo.switchtechnologies.com 192.x.x.x</p> <p>Mac OS X Server 10.4 "STI World Headquarters"</p> <ul style="list-style-type: none"> ● SNMP Statistics 	<p>Darwin mailsanctdemo.switchtechnologies.com 8.11.1 Darwin Kernel Version 8.11.1: Wed Oct 10 18:23:28 PDT 2007; root:xnu-792.25.20~1/RELEASE_ARM_T186 i386</p>	<p>23 days, 16:02:06</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Interface</th> <th>Admin</th> <th>Oper</th> </tr> </thead> <tbody> <tr><td>lo0 127.0.0.1</td><td style="background-color: #008000;"></td><td style="background-color: #008000;"></td></tr> <tr><td>gif0</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>stf0</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>en0 10.100.25.25</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>en1</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>wl0</td><td style="background-color: #008000;"></td><td style="background-color: #008000;"></td></tr> <tr><td>fw1</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> </tbody> </table> <p>● More info...</p>	Interface	Admin	Oper	lo0 127.0.0.1			gif0			stf0			en0 10.100.25.25			en1			wl0			fw1			<p>Data not available for Mac OS X Server 10.4</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Disk</th> <th>Total GB</th> <th>Used GB</th> <th>% Used</th> </tr> </thead> <tbody> <tr><td>/</td><td>74.21</td><td>23.64</td><td>31.86%</td></tr> <tr><td>/dev</td><td>9.53</td><td>9.53</td><td>100%</td></tr> <tr><td>/dev</td><td>9.53</td><td>9.53</td><td>100%</td></tr> <tr><td>/vol</td><td>0.00</td><td>0.00</td><td>100%</td></tr> <tr><td>/Network</td><td>0</td><td>0</td><td>0%</td></tr> <tr><td>/automount</td><td>0</td><td>0</td><td>0%</td></tr> <tr><td>/Servers</td><td>0</td><td>0</td><td>0%</td></tr> <tr><td>/automount/static</td><td>0</td><td>0</td><td>0%</td></tr> </tbody> </table>	Disk	Total GB	Used GB	% Used	/	74.21	23.64	31.86%	/dev	9.53	9.53	100%	/dev	9.53	9.53	100%	/vol	0.00	0.00	100%	/Network	0	0	0%	/automount	0	0	0%	/Servers	0	0	0%	/automount/static	0	0	0%	<p>Current users 0</p> <ul style="list-style-type: none"> ● Current Sessions - <p>Load-1 0.32</p> <p>Load-5 0.11</p> <p>Load-15 0.04</p>
Interface	Admin	Oper																																																																
lo0 127.0.0.1																																																																		
gif0																																																																		
stf0																																																																		
en0 10.100.25.25																																																																		
en1																																																																		
wl0																																																																		
fw1																																																																		
Disk	Total GB	Used GB	% Used																																																															
/	74.21	23.64	31.86%																																																															
/dev	9.53	9.53	100%																																																															
/dev	9.53	9.53	100%																																																															
/vol	0.00	0.00	100%																																																															
/Network	0	0	0%																																																															
/automount	0	0	0%																																																															
/Servers	0	0	0%																																																															
/automount/static	0	0	0%																																																															
<p>msgw 10.x.x.x</p> <p>Debian Etch STI World Headquarters</p> <ul style="list-style-type: none"> ● Arp Cache ● SNMP Statistics 	<p>Linux msgw 2.6.18-6-amd64 #1 SMP Sun Feb 10 17:50:19 UTC 2008 x86_64</p>	<p>33 days, 5:28:52</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Interface</th> <th>Admin</th> <th>Oper</th> </tr> </thead> <tbody> <tr><td>lo 127.0.0.1</td><td style="background-color: #008000;"></td><td style="background-color: #008000;"></td></tr> <tr><td>eth0 10.100.50.49</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>si0</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> </tbody> </table> <p>● More info...</p>	Interface	Admin	Oper	lo 127.0.0.1			eth0 10.100.50.49			si0			<p>Total: 0.97 GB Used: 0.23 GB Used %: 23.86%</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Disk</th> <th>Total GB</th> <th>Used GB</th> <th>% Used</th> </tr> </thead> <tbody> <tr><td>/</td><td>70.55</td><td>0.70</td><td>1%</td></tr> <tr><td>/sys</td><td>0</td><td>0</td><td>0%</td></tr> <tr><td>/proc/bus/usb</td><td>0</td><td>0</td><td>0%</td></tr> </tbody> </table>	Disk	Total GB	Used GB	% Used	/	70.55	0.70	1%	/sys	0	0	0%	/proc/bus/usb	0	0	0%	<p>Current users 0</p> <ul style="list-style-type: none"> ● Current Processes 52 ● Current Sessions - ● Estab-TCP Connects 0 <p>Load-1 0.00</p> <p>Load-5 0.00</p> <p>Load-15 0.00</p>																																
Interface	Admin	Oper																																																																
lo 127.0.0.1																																																																		
eth0 10.100.50.49																																																																		
si0																																																																		
Disk	Total GB	Used GB	% Used																																																															
/	70.55	0.70	1%																																																															
/sys	0	0	0%																																																															
/proc/bus/usb	0	0	0%																																																															
<p>XCHANGE 167.206.x.x</p> <p>Windows 2003 STI World Headquarters</p> <ul style="list-style-type: none"> ● Installed Software ● SNMP Statistics 	<p>Hardware: x86 Family 15 Model 6 Shipping 5 AT AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)</p>	<p>7 days, 6:45:10</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Interface</th> <th>Admin</th> <th>Oper</th> </tr> </thead> <tbody> <tr><td>MS TCP Loopback interface 127.0.0.1</td><td style="background-color: #008000;"></td><td style="background-color: #008000;"></td></tr> <tr><td>Intel(R) PRO/100 VE Network Connection 10.100.111.111</td><td style="background-color: #008000;"></td><td style="background-color: #008000;"></td></tr> </tbody> </table> <p>● More info...</p>	Interface	Admin	Oper	MS TCP Loopback interface 127.0.0.1			Intel(R) PRO/100 VE Network Connection 10.100.111.111			<p>Total: 0.99 GB Used: 0.51 GB Used %: 51.06%</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Disk</th> <th>Total GB</th> <th>Used GB</th> <th>% Used</th> </tr> </thead> <tbody> <tr><td>CA</td><td>74.52</td><td>21.06</td><td>28.26%</td></tr> <tr><td>FA</td><td>148.85</td><td>85.60</td><td>57.50%</td></tr> <tr><td>GA</td><td>252.88</td><td>65.72</td><td>28.22%</td></tr> </tbody> </table>	Disk	Total GB	Used GB	% Used	CA	74.52	21.06	28.26%	FA	148.85	85.60	57.50%	GA	252.88	65.72	28.22%	<p>Current users 2</p> <ul style="list-style-type: none"> ● Current Processes 50 ● Current Sessions - ● Estab-TCP Connects 86 <p>Load data not available for Windows 2003</p>																																			
Interface	Admin	Oper																																																																
MS TCP Loopback interface 127.0.0.1																																																																		
Intel(R) PRO/100 VE Network Connection 10.100.111.111																																																																		
Disk	Total GB	Used GB	% Used																																																															
CA	74.52	21.06	28.26%																																																															
FA	148.85	85.60	57.50%																																																															
GA	252.88	65.72	28.22%																																																															
<p>msl 172.16.x.x</p> <p>Debian Etch STI World Headquarters</p> <ul style="list-style-type: none"> ● Arp Cache ● SNMP Statistics 	<p>Linux msl 2.6.18-5-amd64 #1 SMP Wed Oct 3 09:37:45 PDT 2007 x86_64</p>	<p>5 days, 17:52:29</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Interface</th> <th>Admin</th> <th>Oper</th> </tr> </thead> <tbody> <tr><td>lo 127.0.0.1</td><td style="background-color: #008000;"></td><td style="background-color: #008000;"></td></tr> <tr><td>eth0 10.100.200.1</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>eth1</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> <tr><td>si0</td><td style="background-color: #ff0000;"></td><td style="background-color: #ff0000;"></td></tr> </tbody> </table> <p>● More info...</p>	Interface	Admin	Oper	lo 127.0.0.1			eth0 10.100.200.1			eth1			si0			<p>Total: 7.87 GB Used: 6.38 GB Used %: 81.10%</p>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Disk</th> <th>Total GB</th> <th>Used GB</th> <th>% Used</th> </tr> </thead> <tbody> <tr><td>/</td><td>140.66</td><td>1.40</td><td>1.00%</td></tr> <tr><td>/sys</td><td>0</td><td>0</td><td>0%</td></tr> <tr><td>/proc/bus/usb</td><td>0</td><td>0</td><td>0%</td></tr> <tr><td>/data</td><td>1833.39</td><td>730.09</td><td>39.82%</td></tr> </tbody> </table>	Disk	Total GB	Used GB	% Used	/	140.66	1.40	1.00%	/sys	0	0	0%	/proc/bus/usb	0	0	0%	/data	1833.39	730.09	39.82%	<p>Current users 1</p> <ul style="list-style-type: none"> ● Current Processes 101 ● Current Sessions - ● Estab-TCP Connects 0 <p>Load-1 0.00</p> <p>Load-5 0.01</p> <p>Load-15 0.01</p>																									
Interface	Admin	Oper																																																																
lo 127.0.0.1																																																																		
eth0 10.100.200.1																																																																		
eth1																																																																		
si0																																																																		
Disk	Total GB	Used GB	% Used																																																															
/	140.66	1.40	1.00%																																																															
/sys	0	0	0%																																																															
/proc/bus/usb	0	0	0%																																																															
/data	1833.39	730.09	39.82%																																																															

User Alerts

Traffic Monitor

Server Monitor

View the Summary Server Report

Device Probe

Port Security

Document Store

Repository

Device Syslogs

UPS Monitor

Wireless Tools

Helpful Links

[Outlook Web Access](#)

[Barracuda Spam Firewall](#)

[MailSanctuary](#)

[Sophos Firewall Administration](#)

[VPN Client Download](#)

Copyright 2009 Switch Technologies

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



Switch Technologies, Inc.
Simple Network Monitoring System (3.5)

Server Monitoring System: Server List Edit Screen

Server Address	Community String	Server Type
10.x.x.x	public	OSX104
192.168.x.x	public	DebianEtch
172.16.x.x	public	Windows2003
10.3.x.x	public	DebianEtch
167.206.x.x	public	Solaris10i8sx

Use this form to modify, add or delete entries.

Delete

Server Address:

Community String:

Server Type:

[Open User Screen](#)



Copyright 2009 Switch Technologies

A few Screen Shots

- ▶ User Alerts
- ▶ Traffic Monitor
- ▶ Server Monitor
- ▶ Device Probe
- ▶ Port Security
- ▶ Document Store
- ▶ UPS Monitor
- ▶ Wireless Tools
- ▶ User Manager
- ▶ Miscellany

[Open User Screen](#)



Copyright 2009 Switch Technologies

[Back](#)

Miscellaneous Tools: Device Profile ?

Scanning 10.50.200.100.

Please be patient.

Drilling for more details takes considerably longer.

Device Profile Report	
Device Type	general purpose
OS Guess	Microsoft Windows NT/2K/XP/2003/.NET
Additional OS Details	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2
MAC Address	00:21:5A:A8:19:7E (Unknown)
Number of Closed Ports	1654
Service Info	Host: Server.com; OS: Windows
Open Ports	25 tcp open smtp Microsoft ESMTP 6.0.3790.3959 42 tcp open wins Microsoft Windows Wins 53 tcp open domain Microsoft DNS 80 tcp open http Microsoft IIS webserver 6.0 88 tcp open tcvrwrapped 110 tcp open pop3 MS Exchange 2003 pop3d 6.5.7226.0 135 tcp open msrpc Microsoft Windows RPC 139 tcp open netbios-ssn 389 tcp open ldap Microsoft LDAP server 443 tcp open ssl/http Microsoft IIS webserver 6.0 445 tcp open microsoft-ds Microsoft Windows 2003 microsoft-ds 464 tcp open tcvrwrapped 593 tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 636 tcp open tcvrwrapped 691 tcp open resvc Microsoft Exchange routing server 6.5.7226.026.0 995 tcp open tcvrwrapped 1026 tcp open msrpc Microsoft Windows RPC 1027 tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 1083 tcp open msrpc Microsoft Windows RPC 1103 tcp open msrpc Microsoft Windows RPC 3268 tcp open ldap Microsoft LDAP server 3269 tcp open tcvrwrapped 3389 tcp open microsoft-rdp Microsoft Terminal Service 6001 tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 6002 tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 6004 tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

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 SMART2200RML2U	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 SMART2200RML2U	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



- ▶ 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