Switch Management and Network Information

Chapter 5

In this Chapter...

Switch Management and Network Information

Chapters 3 and 4 detail features that affect the traffic across the switch. **Stride** managed switches also have many features that assist in maintaining the network itself. This chapter describes these network management features.

LLDP

Link Layer Discovery Protocol provides a standard network discovery method. Network information is shared among connected devices and saved to respond to queries from network management system devices.

Information can only be displayed when both this switch and neighbor devices have LLDP enabled.

ARP

The switch management interface maintains an ARP table listing hosts that have accessed the switch management interface.

In general, the switch will learn ARP entries automatically without need of static entry configuration.

Max 512 total ARP entries are supported, with no more than 256 static entries. When the number of ARP entries exceeds 512, any new entry will replace the oldest dynamic entry.

IP addresses configured as static entries must be on the same subnet as the switch's IP address.

SNTP

Simple Network Time Protocol calibrates time by requests and responses between servers and clients. The switch will be a client to calibrate time according to the messages from the server. Up to four time servers may be configured on the switch but only a single time server is in an active state, any other configured servers will be inactive. The switch sends a request to all configured servers and the first to respond is assigned as the active server.

SSH Server

SSH (Secure Shell) encrypts switch management messages to prevent information disclosure. SSH encrypts only Command Line interface communications, not browser based switch management communication.

A Local Key Value may be generated by the switch and copied to the devices that will be allowed to access switch management functions. Or, the key may be generated by the connecting device and copied into the switch, typically using a key generation application such as PuTTYgen.

If the key will be generated by the switch and copied to the devices allowed to access switch management:

1. Disable SSH
2. Click the Set SSH Server button
3. Enable SSH
4. Configure:

- Authentication Retry – the number of unsuccessful login attempts that will be allowed before disabling access to the switch management interface.
- Time Out – the number of minutes of inactivity before terminal sessions automatically logout to prevent unauthorized access. The default is 5 minutes.

5. Copy the Local Key Value to the devices that are allowed to access switch management.
6. Add SSH Users on the SSH User Manager page (see below)

If the key will be generated by the connected device:

1. Enter a Name for the new key on the Key Configuration page.
2. Copy the key from the connected device to the Key Value field on the Key Configuration page
3. The key now appears in the Public Key List on the User Manager page.
4. Add SSH Users assigned to that key on the User Manager page.

Adding SSH Users on the User Manager page:

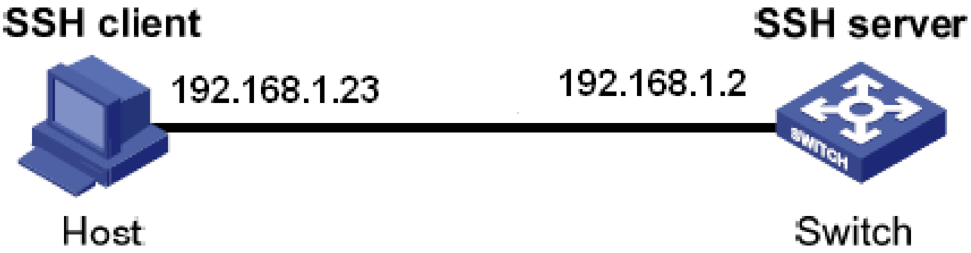
1. Enter a User name (login name)
2. Select either

- Password – Enter the Password that this User will type to login from a connected device
- Public Key – Select a key from the Public Key List of keys configured on the Key Configuration page.

3. Click Add to add this new user.

Typical configuration examples

The Host works as the SSH client to request a local connection with Switch, as shown below.



SSH USER with Authentication Type "Password"

1.On the SSH Server configuration page:

a) Disable SSH.

b) Click the Set SSH Server button to create a new Key Value.

c) Enable SSH.

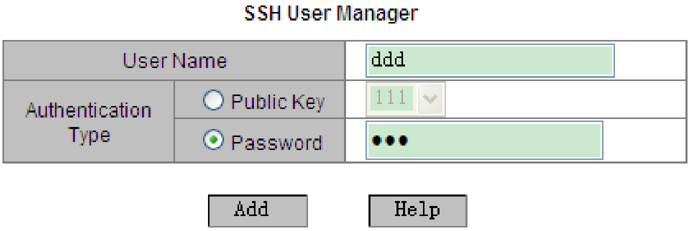
d) Click Apply

2. On the SSH User Manager page:

a) Enter user name ddd.

b) Choose the authentication type of "Password".

c) Enter password 444.



SSH User Manager

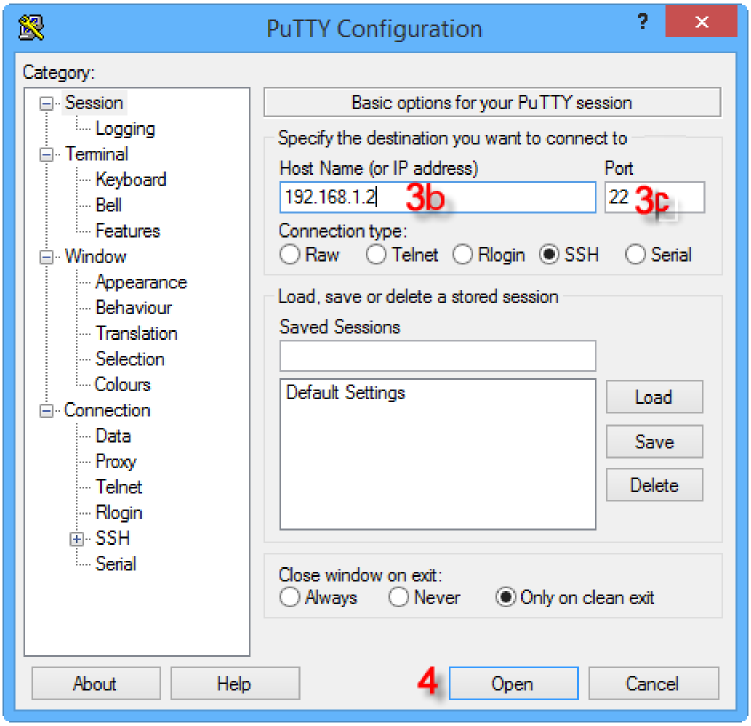
User Name		ddd
Authentication Type	○ Public Key	111
	● Password	•••

3. Establish the connection with the SSH server.

a) Open the terminal application, PuTTY.exe in our example.

b) Enter the switch management IP address in the Host Name field, 192.168.1.2 is the default, we are using 192.168.1.2 in this example.

c) Enter port 22 and select SSH connection type.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.2 3b

Port: 22 3c

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

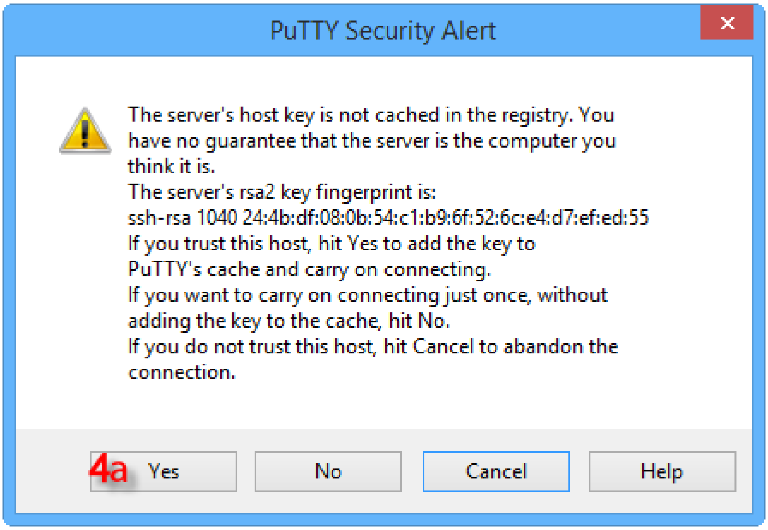
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

4

4. Click <Open> button and the following warning message appears.

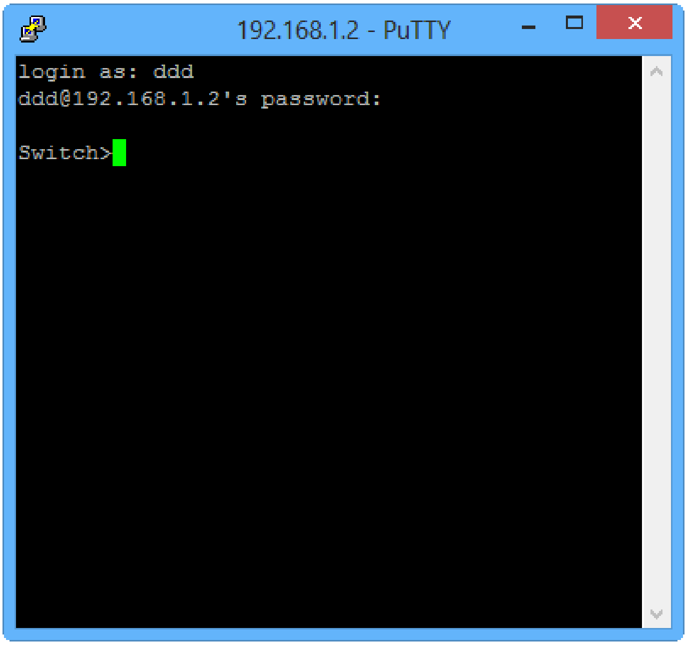
   a.)Click “Yes”.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1040 24:4b:df:08:0b:54:c1:b9:6f:52:6c:e4:d7:ef:ed:55
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

5. Input the user name “ddd” and the password “444” to enter the switch configuration interface, as shown below.



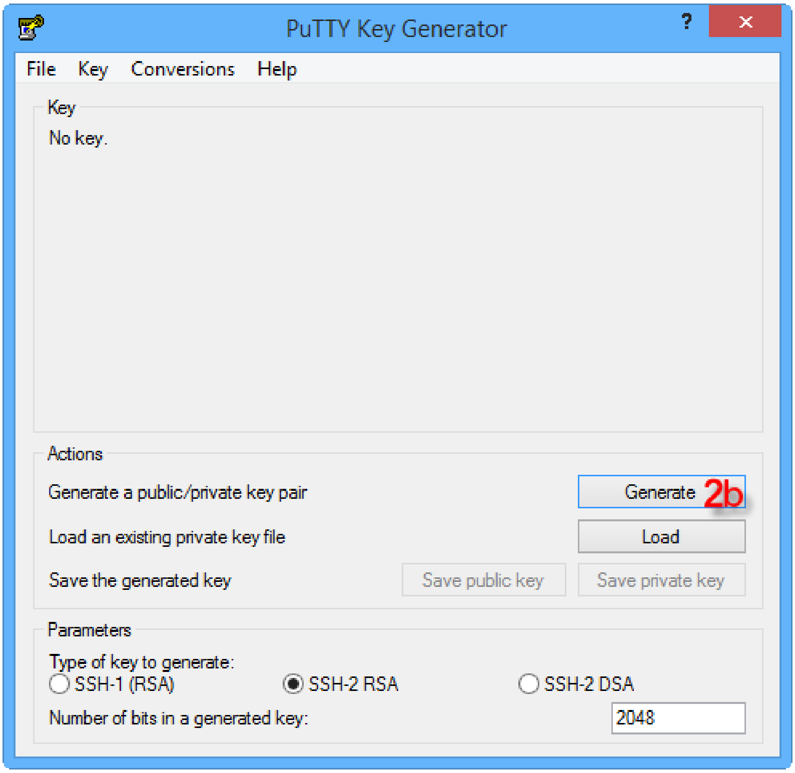
192.168.1.2 - PuTTY

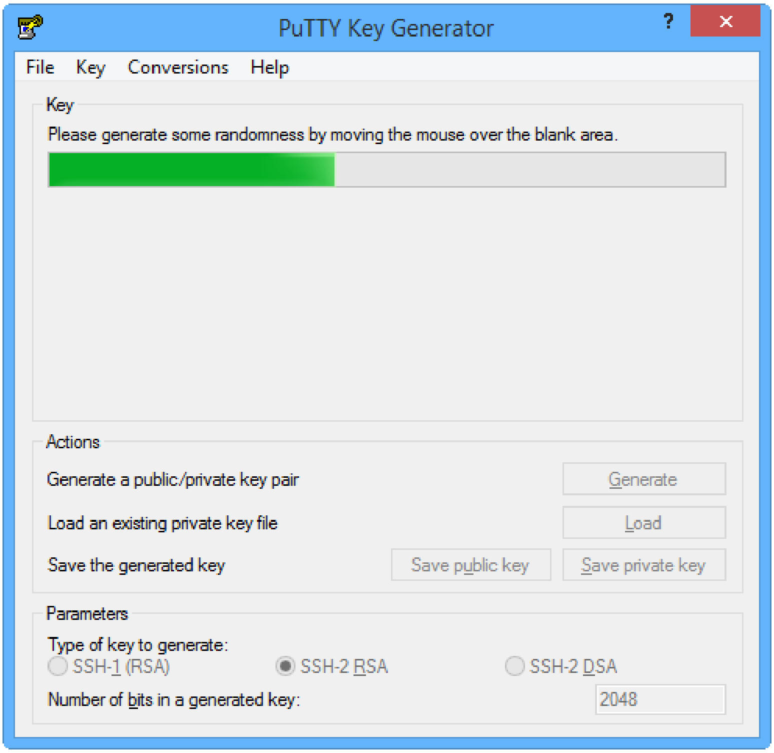
```
login as: ddd
ddd@192.168.1.2's password:

Switch>
```

SSH user with authentication type "Public Key"

1. On the SSH Server configuration page:
   - Disable SSH.
   - Click the Set SSH Server button to create a new Key Value.
   - Enable SSH.
   - Click Apply
2. On the device that will access switch management:
   a. Run PuTTYGen.exe
   b. Click <Generate> button to generate the client key pair:





Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key — Save private key

Parameters

Type of key to generate:

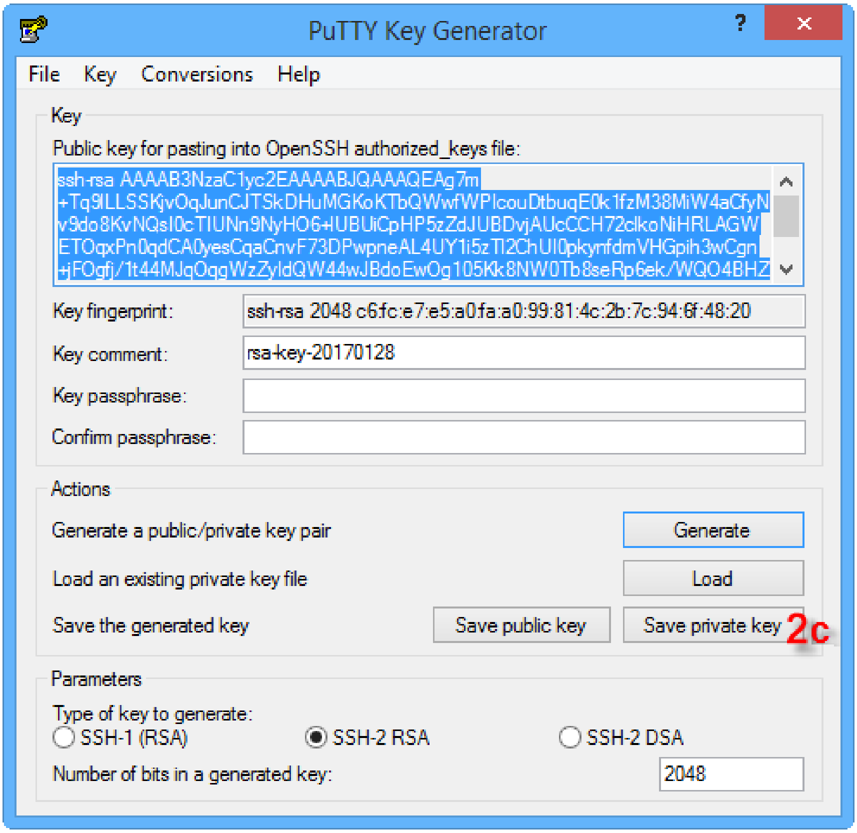
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

c. Click <Save private key> to save the private key,

d. Copy the public key to the switch SSH Key Configuration page in the Key Value box. Enter Key Name 111.

***NOTE:** Typically, PuTTYgen requires random mouse movement while the key is being generated*



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAg7m
+Tq9lLLSSKjvOqJunCJTSkDHuMGKoKTbQWwfWPIcouDtbuqE0k1fzM38MiW4aCfyN
v9do8KvNQsI0cTIUNn9NyHO6+UBUiCpHP5zZdJUBDvjAUcCCH72clkoNiHRLAGW
ETOqxPn0qdCA0yesCqaCnvF73DPwpneAL4UY1i5zTl2ChUI0pkynfdmVHGpih3wCgn
+jFOgfj/1t44MJqOqgWzZyldQW44wJBdoEwOg105Kk8NW0Tb8seRp6ek/WQO4BHZ
```

Key fingerprint: ssh-rsa 2048 c6:fc:e7:e5:a0:fa:a0:99:81:4c:2b:7c:94:6f:48:20

Key comment: rsa-key-20170128

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

3. On the switch SSH User Manager page:

a. Enter the SSH user name aaa.

b. Select authentication type “Public Key”.

c. Select key name 111.

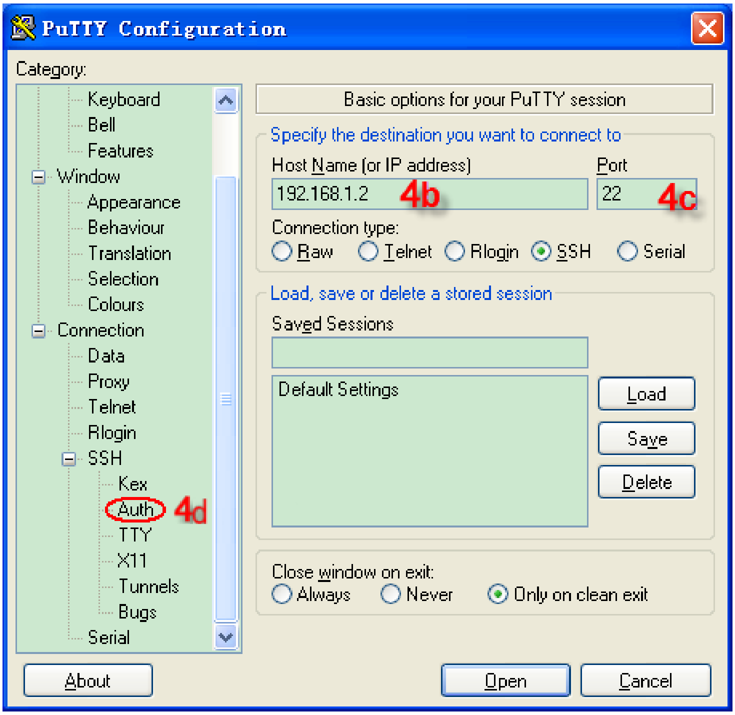
4. Establish the connection with the SSH server.

   a. Open the terminal application, PuTTY.exe in our example.

   b. Enter the switch management IP address in the Host Name field, 192.168.0.1 is the default, we're using 192.168.1.2 in our example.

   c. Enter port 22 and select SSH connection type.

   d. Click the Auth option in the navigation tree on the left of the PuTTY window.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.2

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

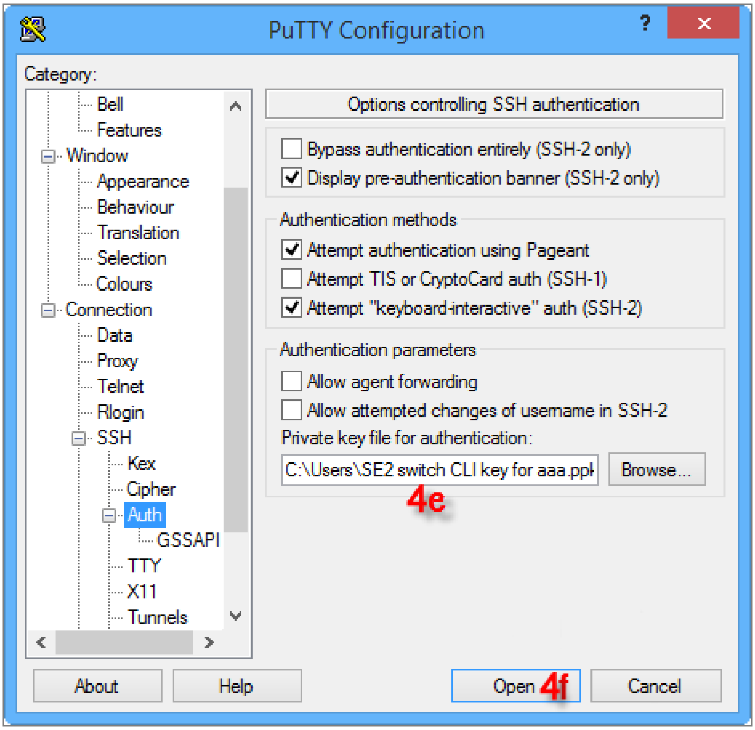
Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

e. Browse to the private file saved in the step 2c.

f. Click <Open> button;



PuTTY Configuration

Options controlling SSH authentication

☐ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

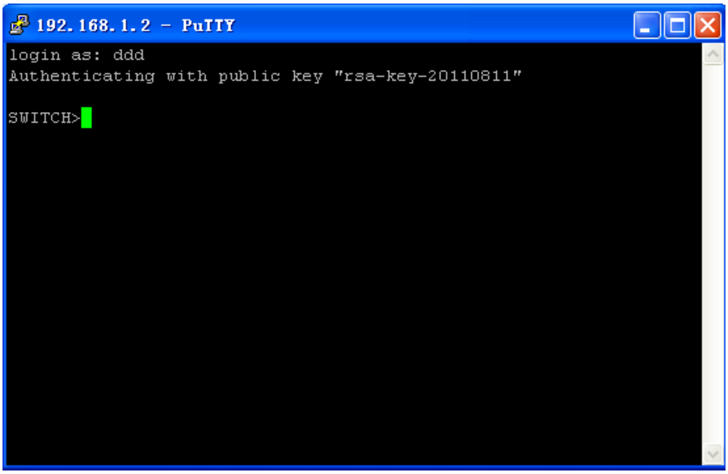
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Users\SE2 switch CLI key for aaa.ppk

g. Input the user name to enter the switch configuration interface



192.168.1.2 - PuTTY

```
login as: ddd
Authenticating with public key "rsa-key-20110811"

SWITCH>
```

RMON Statistics

RMON (Remote Network Monitoring) allows network management devices to actively monitor and manage network devices. Network management devices may use RMON to read statistical information from the switch, for example, traffic information per port. The switch may use RMON to send alarms to the network management device, for example, traffic exceeding a configured threshold. The switch can automatically record alarm events in an RMON log, or send a Trap message to the management device.

RMON Group

The **Stride** SE2 series switches support statistics group, history group, event group and alarm group of public MIB. Each group supports max 32 entries.

CAUTION: If a sampled value of an alarm variable exceeds the threshold multiple times in the same direction, only the first time can trigger an alarm event. That is, in order to capture multiple occasions of a rising condition, an alarm event must be configured for the falling condition to reset the alarm.

Syslog

The system log file, Syslog, records the switch system information and operation information for troubleshooting. It includes a System log and Running log. Syslog is enabled by default and Runlog is disabled by default.

System log contains:

- Task suspension log
- Reboot caused by task suspension
- Reboot caused by pressing <Reset> button on switch front panel
- Reboot caused by Reboot command
- Reboot caused by clicking <Reboot> button on Web interface
- System reboot

Running log contains:

- Port state change
- Power state change
- Reboot caused by Reboot command
- Reboot caused by clicking <Reboot> button on Web interface

Max 1024 logs are supported. When the number exceeds 1024, a new entry will overwrite the oldest entry.

Save in Flash – when enabled, the logs can be viewed on the switch management interface.

Send to Server – when enabled, switch logs can be uploaded to server in real time.

Remote-server IP – Configure the IP address of server to upload logs

SNMP

SNMP (Simple Network Management Protocol) allows the network administrator to check device information, modify device parameters, monitor device status and locate network faults.

Implementation

SNMP protocol adopts manager/agent mode, so SNMP network contains NMS and Agent.

- NMS (Network Management Station) is a workstation running the SNMP-supported client network management software, playing a core role in SNMP network management.
- Agent is a program in the managed device, the SE2 switch in our case. It is responsible for receiving, processing requests from NMS. When an alarm happens, Agent will automatically inform the NMS.

NMS manages the SNMP network, while Agent is managed by SNMP network. The management information exchange between NMS and Agent is through SNMP protocol. SNMP provides 5 basic operations:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

Explanation

SNMP Agent in **Stride** SE2 series switches, supports SNMPv2 and SNMPv3 versions. SNMPv2 is compatible with SNMPv1.

SNMPv1 adopts Community Name Authentication. The community name works as a password and is used to restrict SNMP NMS accessing SNMP Agent. If the community name of the SNMP message cannot pass device authentication, this message will be dropped.

SNMPv2 also adopts Community Name Authentication. It not only is compatible with SNMPv1, but also expands the functions of SNMPv1.

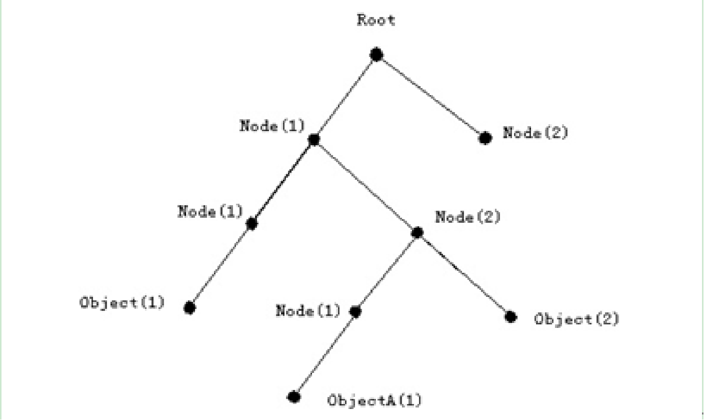
NMS and Agent must support the same SNMP version. Agent can be configured with multiple versions at the same time, and use different versions to communicate with different Network Management Station.

MIB Introduction

Any managed resource can be viewed as an object called a managed object.

An MIB (Management Information Base) is a collection of all managed objects. It defines the hierarchical relationships between managed objects and defines a series of attributes of objects, such as object name, access rights, data types, and so on. Each Agent has its own MIB. NMS can read or write objects in the MIB according to its rights.

MIB defines a tree structure and each tree node is a managed object. Each tree node contains an OID (Object Identifier) that can indicate the node position in the MIB tree structure. As this figure shows, the OID of the managed object A is 1.2.1.1.



SNMPv3

Introduction

SNMPv3 provides a USM (User-Based Security Model) authentication mechanism. User can configure authentication and encryption functions. Authentication is used to verify the legitimacy of the message sender to avoid access by unauthorized users. Messages between NMS and Agent are encrypted. The combination of authentication and encryption improves the communication security between SNMP NMS and SNMP Agent.

Implementation

SNMPv3 has four configuration tables each of which can configure 16 entries. These tables codetermine whether the specified users based on context group can access MIB information.

User table is used to create users. Each user can use different security policies to realize user authentication, encryption and other security functions.

Access table can access MIB node information by matching group name, context name, and by setting security model, security level.

Group table is a collection of multiple users. Access rights are subject to a user group, the access rights of a group are applicable for all users in the group.

Context tables are readable character strings to identify users. It has nothing to do with the specific security model.

Modbus TCP

Industrial applications may be able to more easily and more effectively use Modbus TCP or EtherNet/IP to manage the network, rather than SNMP or RMON. Modbus addresses defined in the SE2 series managed switches may be accessed to read the conditions of the switch, similar to RMON and SNMP. The switch may generate alerts written to the Modbus master. The master may also write to the switch to change some configuration settings.

The Modbus TCP server listening port is 502.

Client devices may read status of Modbus registers as follows:

Item	Description	Protocol Address	Modbus Address
1	Device information	0x0000–0x0fff	400001–404096
2	Port Information	0x1000–0x2fff	404097–412288
3	Alarm Information	0x3000–0x3fff	412289–416384
4	AD–RING Information	0x4000–0x4fff	416385–420480
5	AD–RP Information	0x5000–0x5fff	420481–424576
6	RSTP Information	0x6000–0x6fff	424577–428672

Refer to Appendix E for details on the Modbus TCP switch management features.

EtherNet/IP

Industrial applications may be able to more easily and more effectively use Modbus TCP or EtherNet/IP to manage the network, rather than SNMP or RMON. EtherNet/IP addresses defined in the SE2 series managed switches may be accessed to read the conditions of the switch, similar to RMON and SNMP. The switch may generate alerts written to the EtherNet/IP master.

The master may also write to the switch to change the status. These addresses are detailed in Appendix D.

The SE2 managed switches support EtherNet/IP in the following ways:

Class 1 Implicit I/O Messaging Server/Adapter

Class 3 Explicit Messaging Server/Adapter

Unconnected Explicit Messaging Server/Adapter

Refer to Appendix D for details on the EtherNet/IP switch management feature.

Firmware Update

Occasionally a new firmware version will become available to add features and/or fix bugs. The firmware .bin file may be accessed from a folder on the connected PC or from an FTP server on the network.

When the firmware is in a folder on the connected PC, you may simply Browse to that folder, highlight the new firmware .bin file and Click the Update button.

When the firmware is available from an FTP or TFTP server, carefully enter the full file name including the .bin extension.

Take care to avoid interrupting power to the switch and the source device during the firmware update process.

When the firmware update completes successfully, reboot the switch and check the switch Basic Information page to ensure the new version is reflected in the basic information table.

Configuration Upload and Download

NOTE: *All configuration changes except IP address and password must be committed to the switch by performing SAVE. If not committed by SAVE, changes will be lost on power cycle.*
Likewise, changes made by performing LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.

It is always helpful to backup the work of configuring a switch in the event you must replace the switch, or in case the configuration is unintentionally changed.

The configuration file may be saved to the connected PC or to an FTP/TFTP server.

A saved configuration file may be written into the switch from a connected PC or from a FTP/TFTP server on the network. After a configuration file is written into the switch, SAVE must be performed to commit the configuration to the switch.

Load Default

NOTE: *All configuration changes except IP address and password must be committed to the switch by performing SAVE. If not committed by SAVE, changes will be lost on power cycle Likewise, changes made by performing LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.*

Besides the software Load Default feature, the **Stride** SE2 series switches may Load Default by pressing the RESET button on the face of the switch for longer than 5 seconds until all LEDs start to flash. When the button performs the Load Default, the previous configuration will not be accessible afterward.

Reboot

NOTE*: All configuration changes except IP address and password must be committed to the switch by performing SAVE. If not committed by SAVE, changes will be lost on power cycle. Likewise, changes made by performing LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.*

If changes have been made to the configuration or a software Load Default was performed unintentionally, the switch can revert to the previous configuration by performing Reboot.

Besides the software Reboot feature, the SE2 series switches have a Reboot button on the face of the switch. Reboot can be performed by pressing the Default button on the face of the switch for 1 to 5 seconds. If held for more than 5 seconds, it will reset configuration back to default.