SNMP

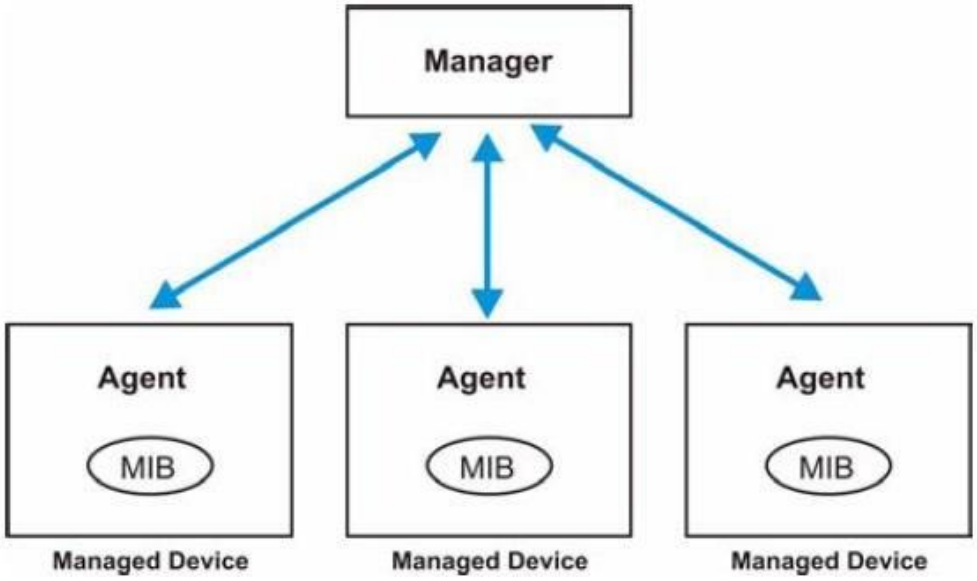
GS1900 Series

Support Note

Version 2.00 Nov. 2022

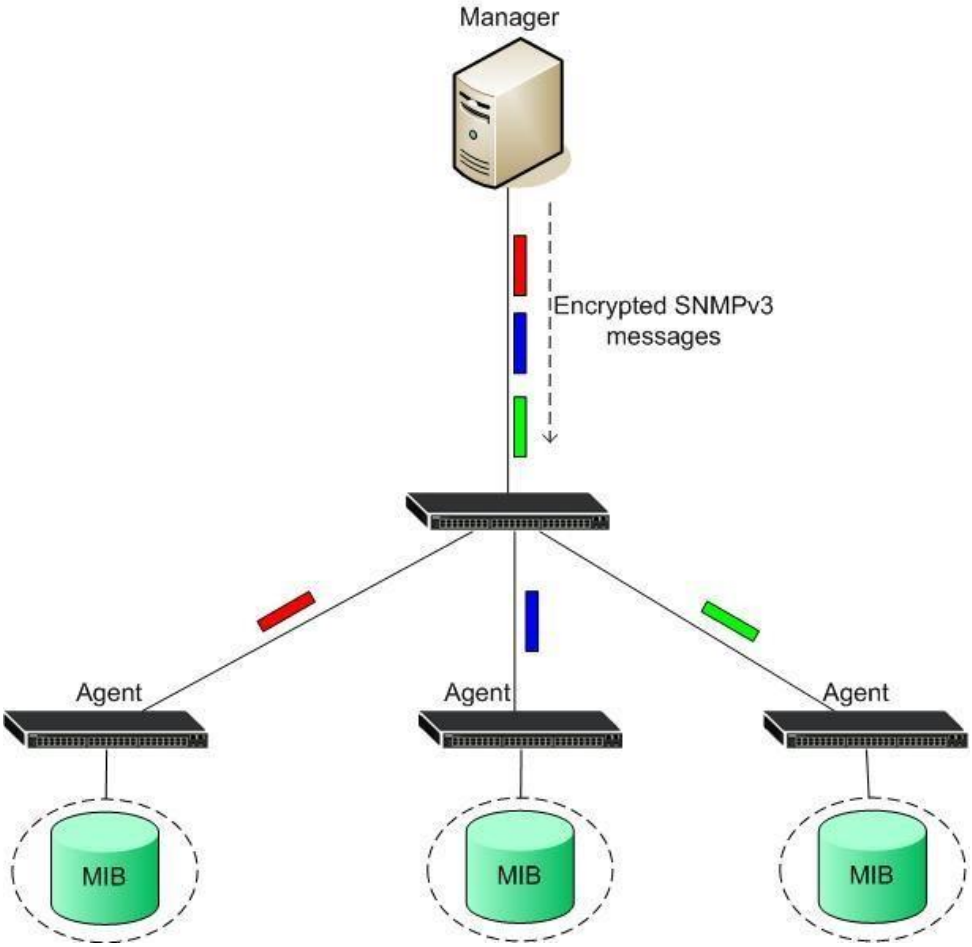
Introduction to SNMP

SNMP is a set of operations that allow the administrator to change the state of the SNMP based devices, such as UNIX systems, Windows systems, Switches, and Routers, etc. The SNMP system consists of three parts: SNMP manager, SNMP agent, and MIB. SNMP agents are the controlled devices where the SNMP manager is playing the role of the managing device. The MIB (Management Information Base) is a database of the managed devices that will be tracked.



Difference between SNMPv3 and others (SNMPv1 and SNMPv2c)

SNMPv3 (Simple Network Management Protocol version 3) can be thought of as SNMPv2 with additional security and administration capabilities. In SNMPv1 and SNMPv2, the authentication method amounts to nothing more than a password (the community string), which was sent in plain text. In SNMPv3, Security can be enhanced by encrypting the SNMP messages, only the authenticated receivers can decrypt the message.



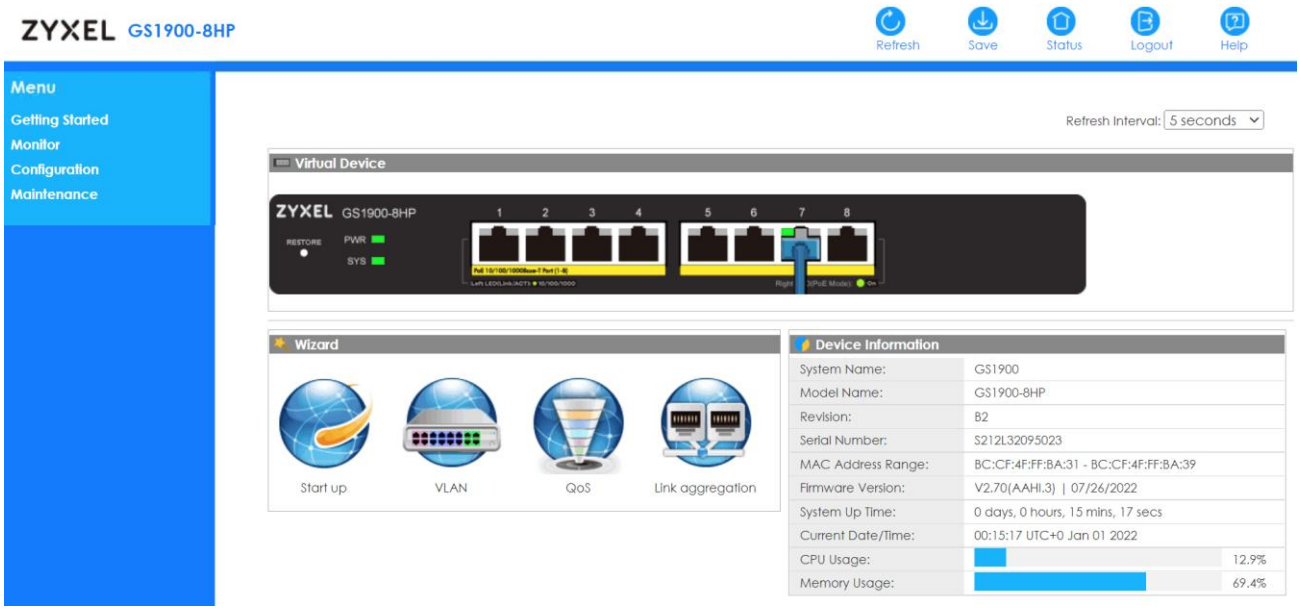
The ZYXEL switches offer three levels of security:

1. **noauth:** To use the username as the password string to send to the SNMP manager.
2. **auth:** To implement an authentication algorithm for SNMP messages sent by this user.
3. **priv:** To implement authentication and encryption for SNMP messages sent by this user.

There are two authentication methods implemented on ZYXEL switches: MD5 and SHA.

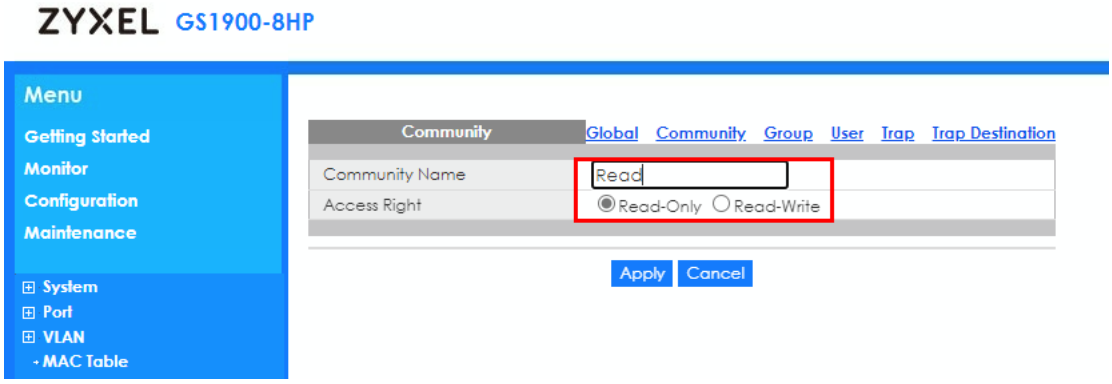
Configure the ZYXEL Switch using the Web GUI

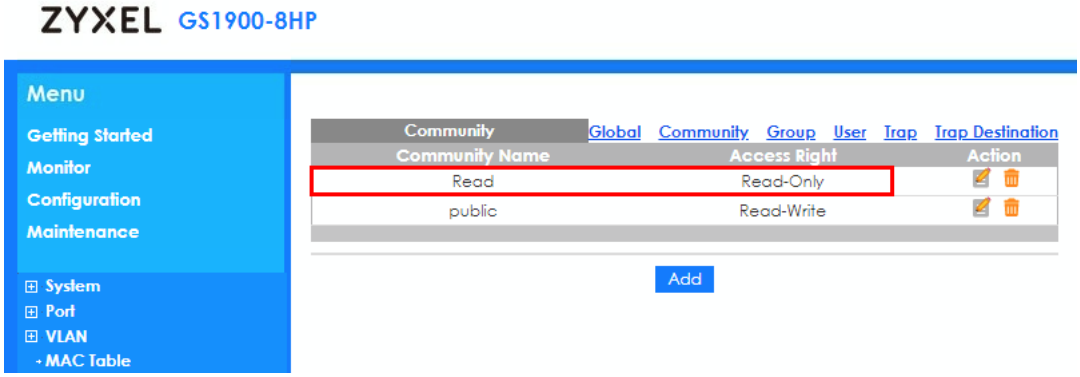
1. Connect the MGMT port to a PC or notebook computer with an RJ-45 cable.
2. By default, the MGMT IP address is 192.168.1.1/24.
3. Set the IP address of the NIC to 192.168.1.100/24.
4. Open an Internet browser (e.g. IE) and enter http://192.168.1.1 into the URL field.
5. By default, the username for the administrator is "admin" and the password is "1234".
6. After successfully logging in you will see a screen similar to the one below.



7. To enter the "SNMP" page, click "**Configuration**" → "**Management**" → "**SNMP**".

8. In the "SNMP" page, we can setup Community, Group, User, Trap/Trap destination.
9. In the "Community" page, we can create a "**Community Name**" and add "**Access Right**" for SNMP.





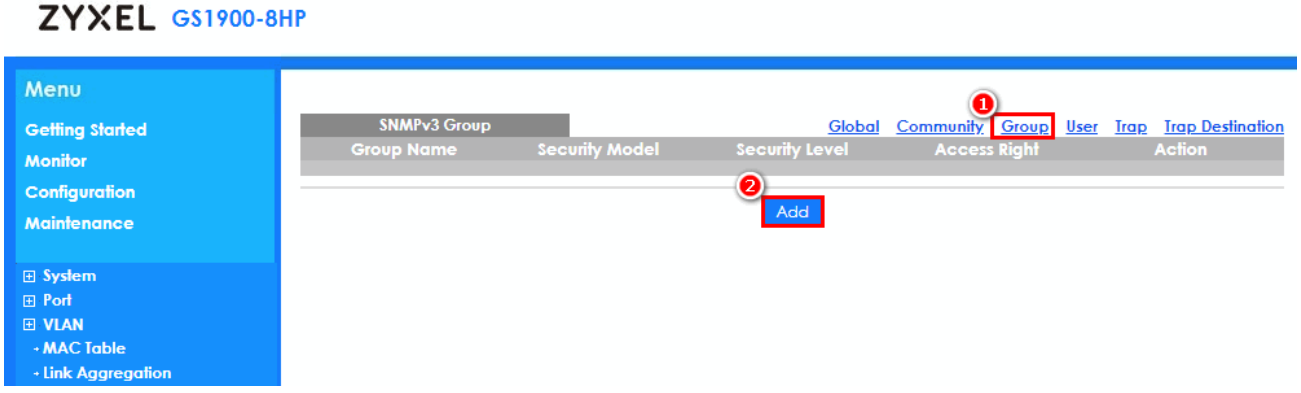
10. In "Group" page, we can add Groups and choose the security level & Access mode ("ro" is Read-only; "rw" is Read-write).

The ZYXEL switches offer three levels of security:

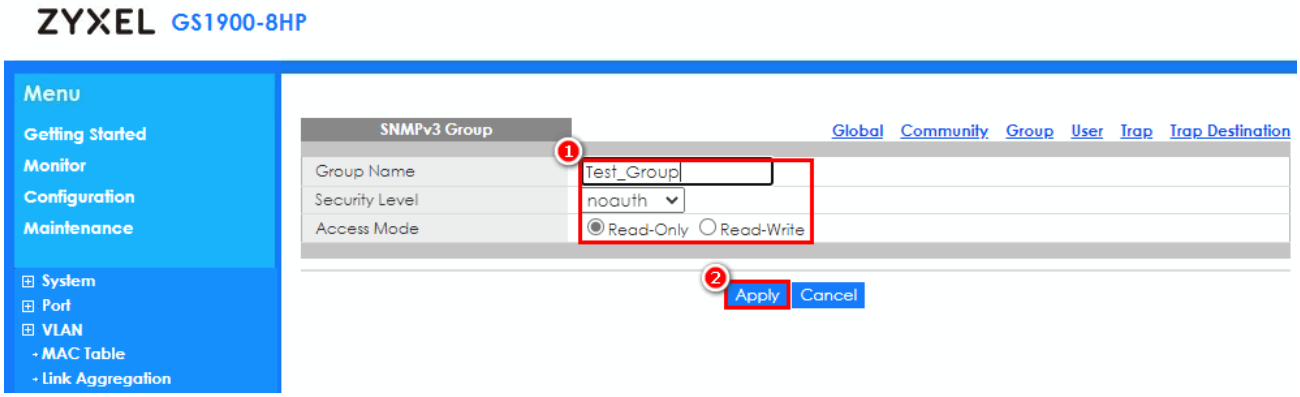
a. **noauth**: To use the username as the password string to send to the SNMP manager.

b. **auth**: To implement an authentication algorithm for SNMP messages sent by this user.

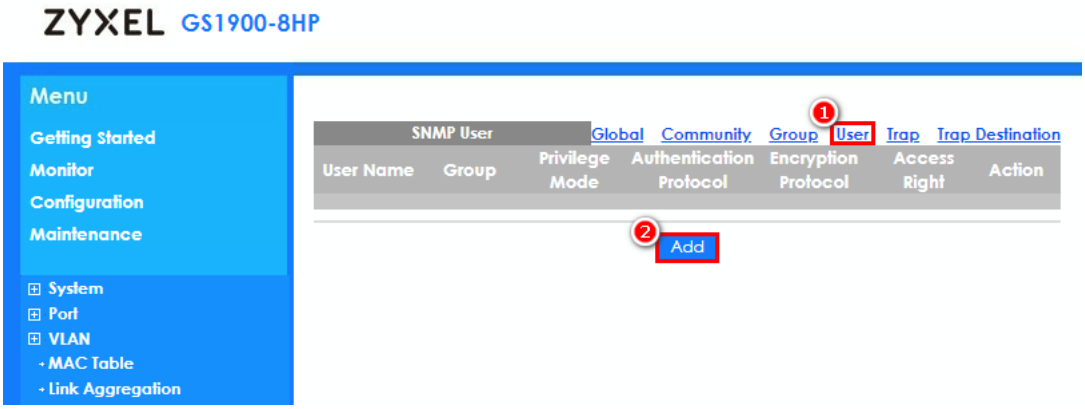
c. **priv**: To implement authentication and encryption for SNMP messages sent by this user.

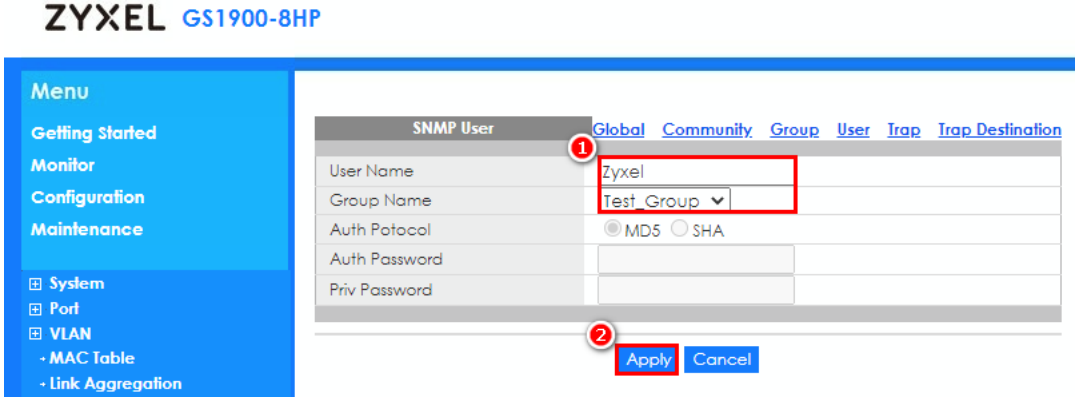


11. Configure the "**User information**". Here we can choose the Security Level, Authentication methods, and encryption methods. Here we use "**noauth**" for no authentication. Click on the "**Apply**" button to save the changes.

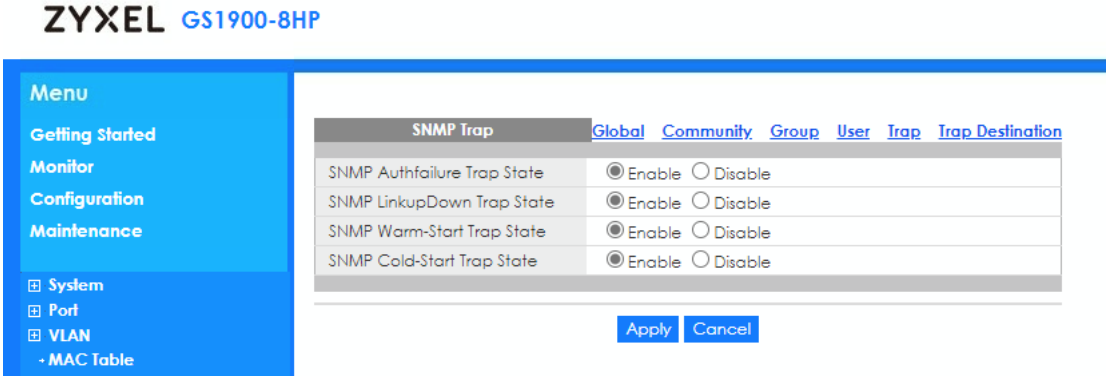


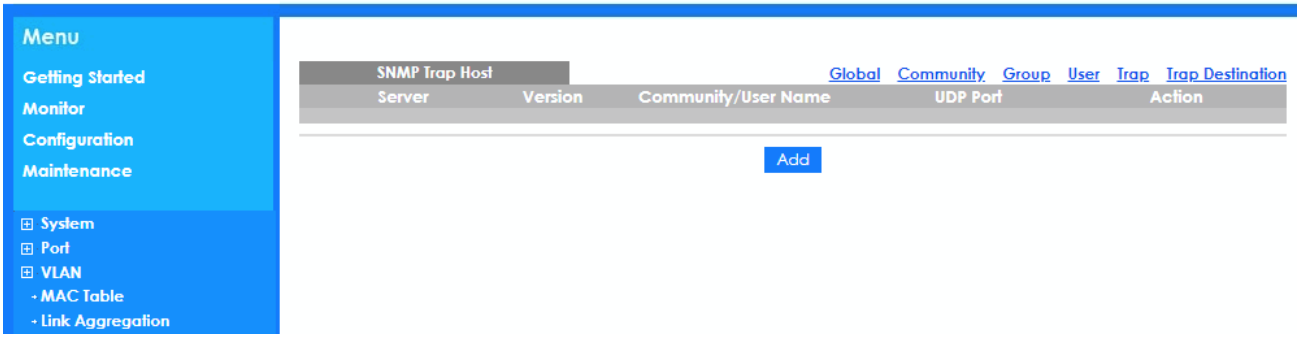
12. In this "User" part, we can define the Group, Auth Protocol, Encryption Protocol, Access Right, and Action for specific users. There are two authentication methods implemented on ZYXEL switches: MD5 and SHA.



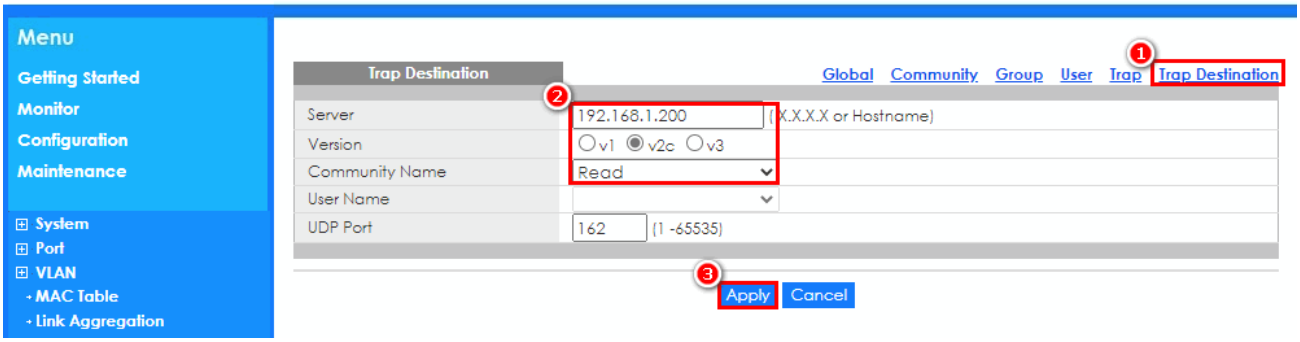


13. In the “Trap” section, we have 4 options to trigged SNMP trap. We can configure which kind of events should trigger the SNMP trap message.

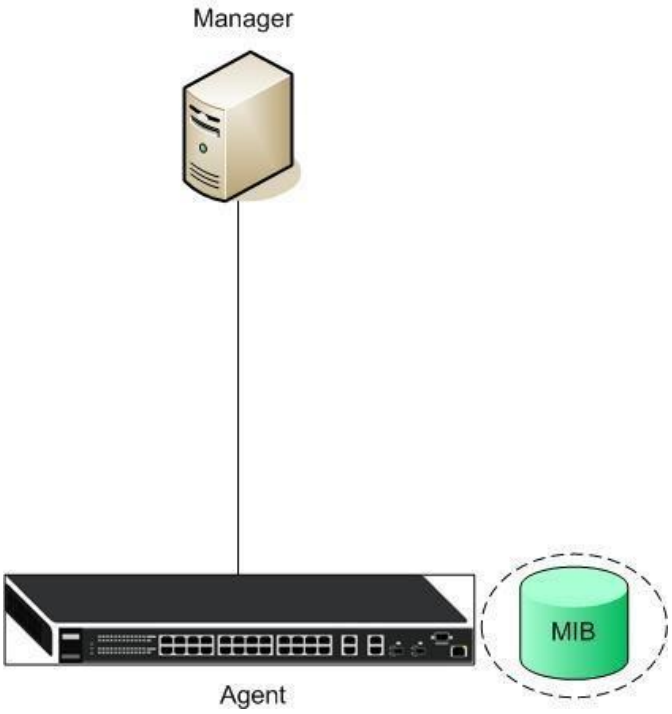




14. In the “Trap Destination” section, we can choose the SNMP version of the trap message, the destination we want to trigger to, destination port, and the username.



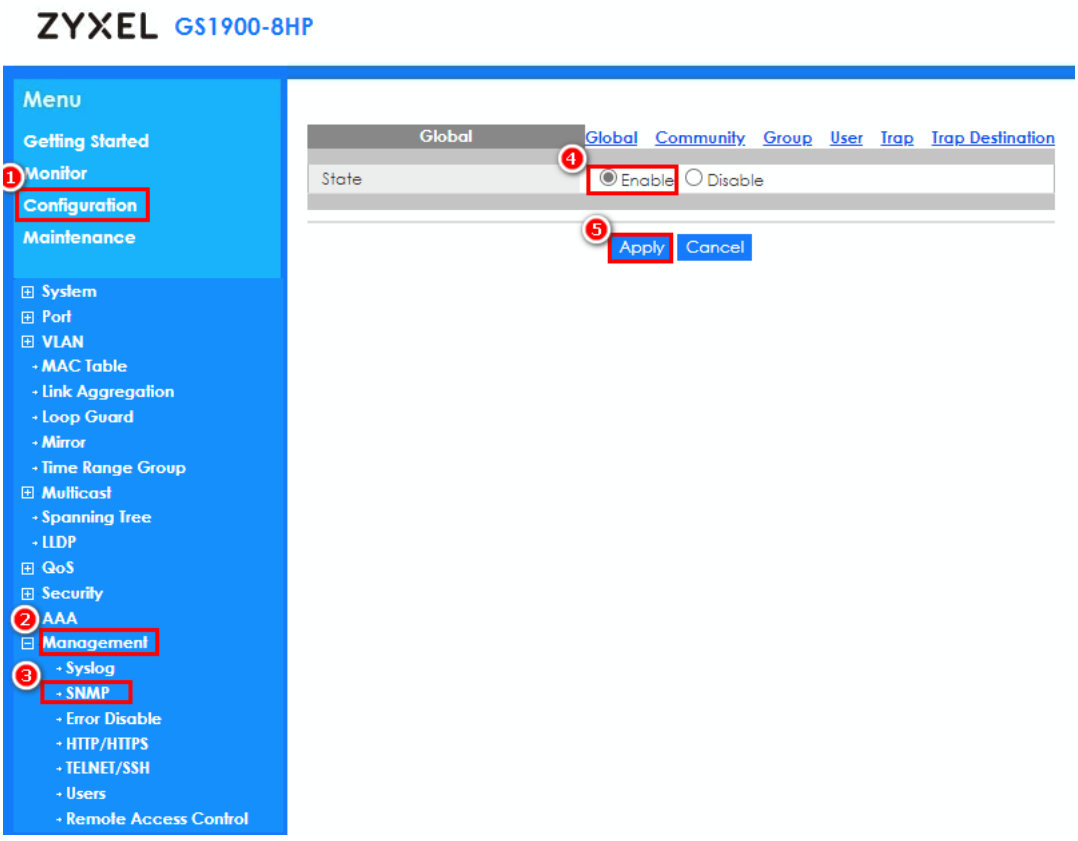
Scenario



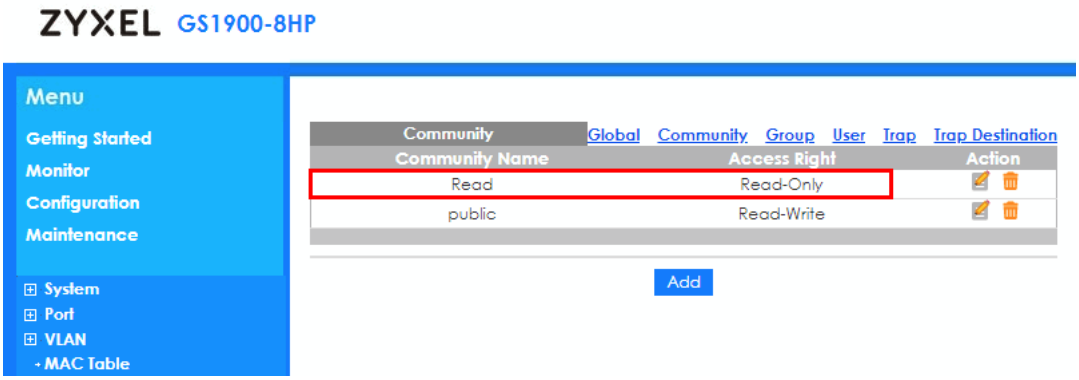
There are three SNMP components in this topology: Manager, Agent, and MIB. In this sample, we use iReasoning as the MIB browser, which can be installed on a Windows system.

Web GUI configuration

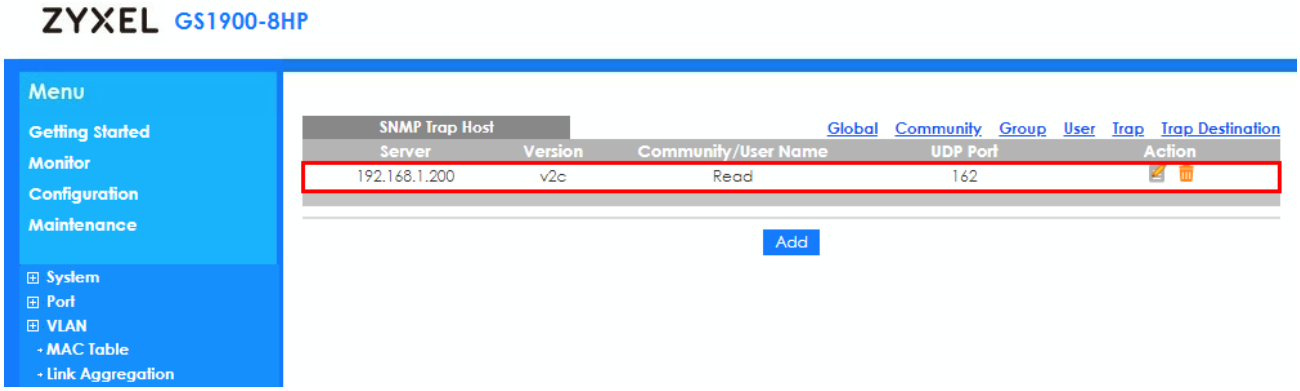
Step 1. Click on "Configuration" and go to "**Management**" → "**SNMP**", and then enable "SNMP".



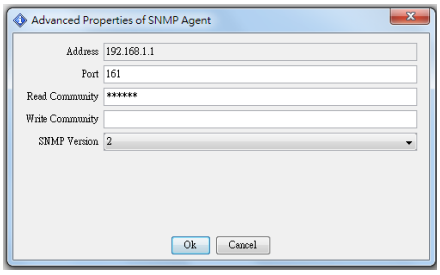
Step 2. Add a "Community" and choose "Access Right".

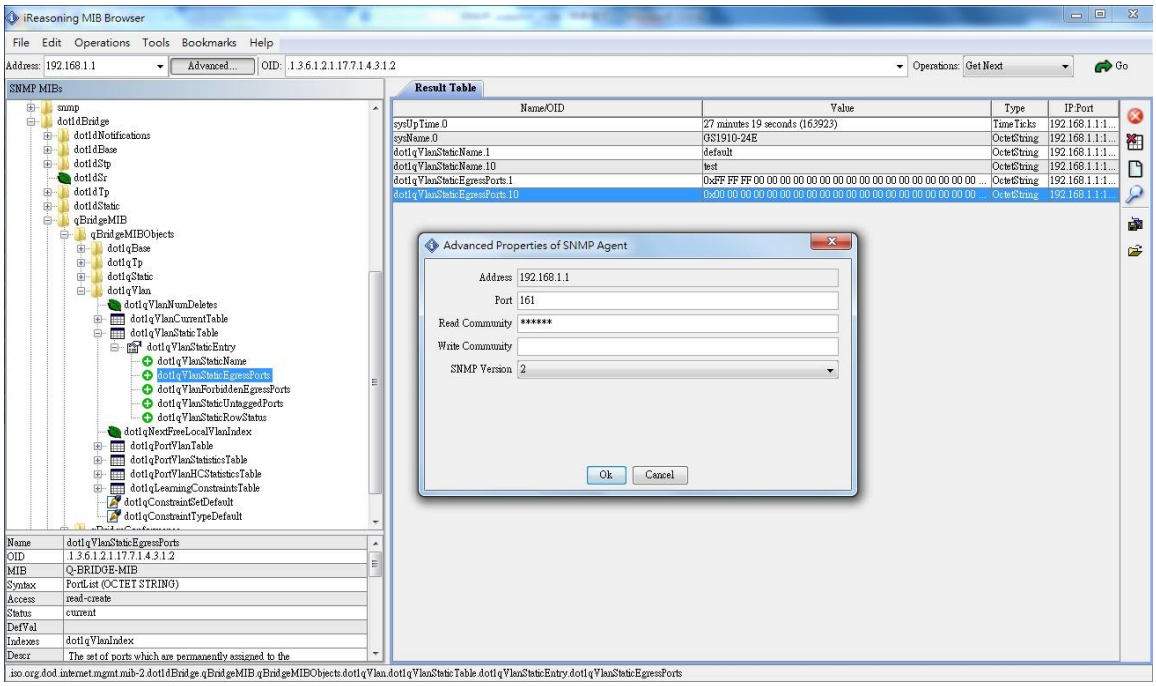


Step 3. Add SNMP trap destination when device reboots. The switch will then send an SNMP trap to the host.



Step 4. To read the VLAN status we need to install iReasoning MIB browser and enter the community and SNMP version as well as the port number, and then load "Q-Bridge" MIB to the polling VLAN status as shown below.





Step 5. After rebooting switch, then SNMP traps will be received as shown in the packet packets.