# SNMPv3

**Ethernet Switch**

**ZyNOS 4.0**

# Support Notes

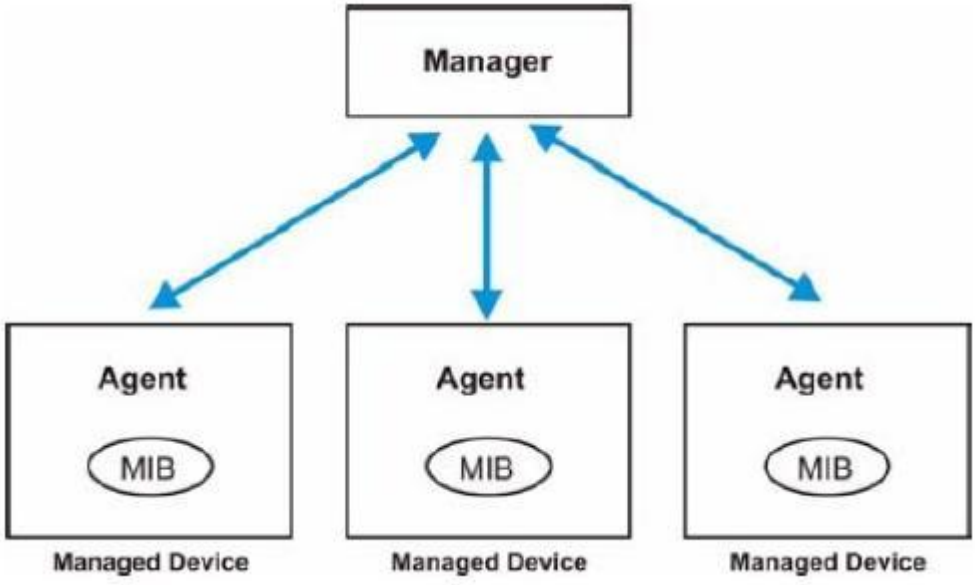
Version 4.0

July 2011

ZyXEL
Unleash Networking Power

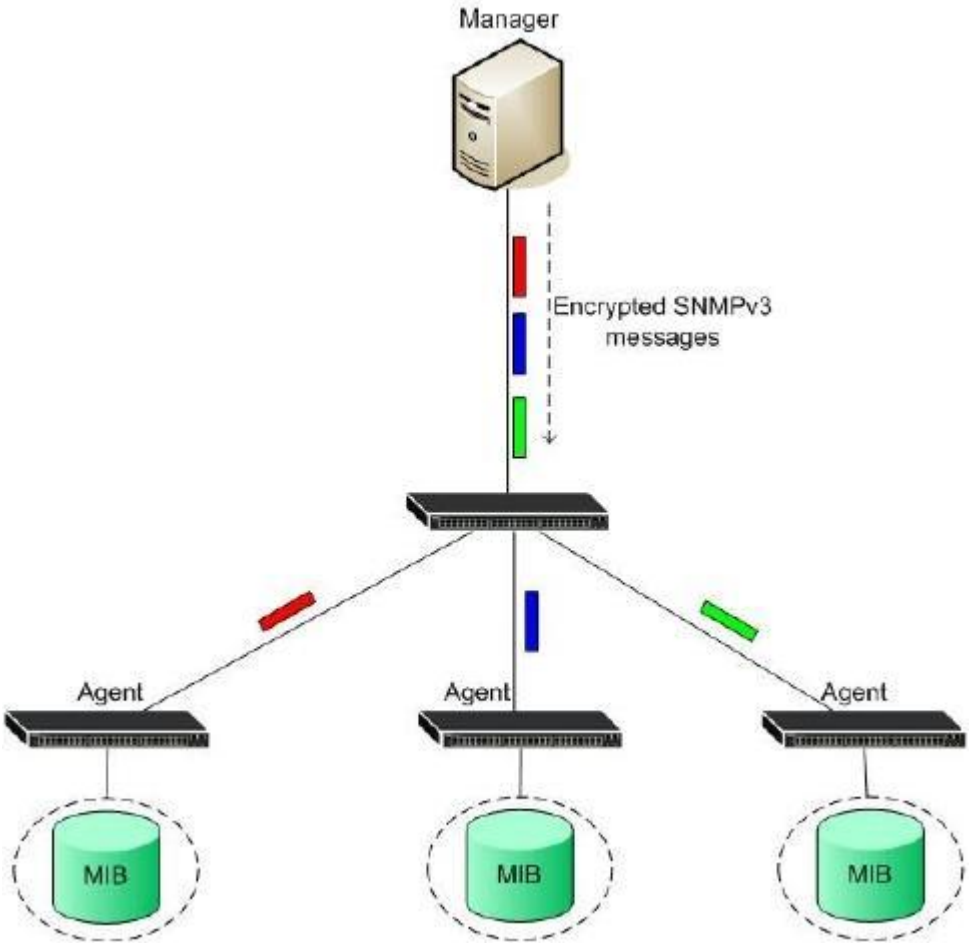
# Introduction to SNMP

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, Routers…etc. The SNMP system consists of three parts: SNMP manager, SNMP agent, and MIB. SNMP agents are the controlled devices where 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.



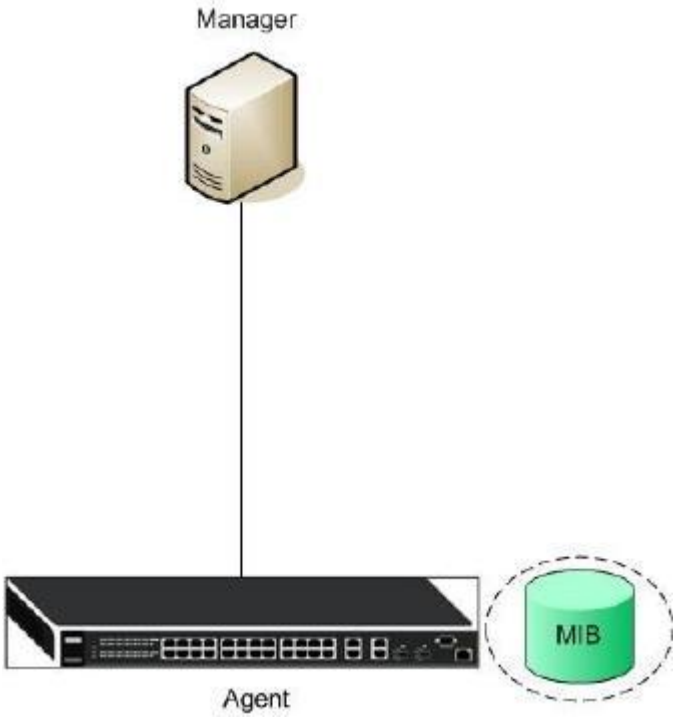

In ZyXEL switches, there are three security levels:

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, (i)MD5 (ii)SHA and two encryption methods (i)DES (ii)AES

# Scenario

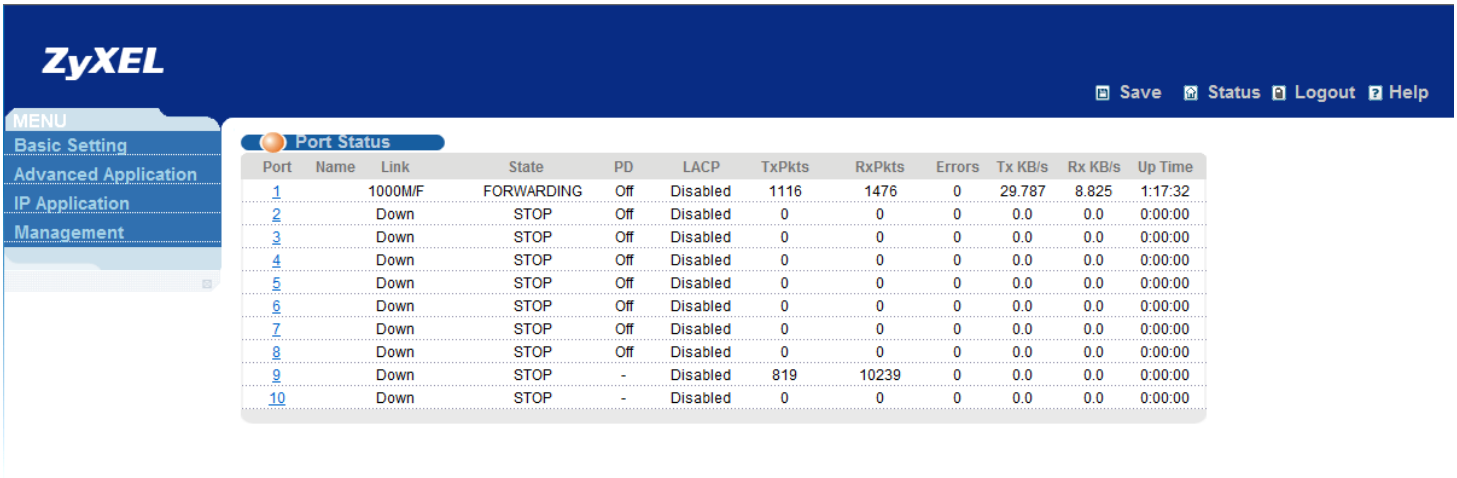
Below is a simple topology which could give us a common view about SNMP.




There are three SNMP components in this topology: Manager, Agent, and MIB. In this sample, we use SNMPc as the manager server. SNMPc could be installed on a Windows system.

# Configuration ZyXEL switch using the Web GUI

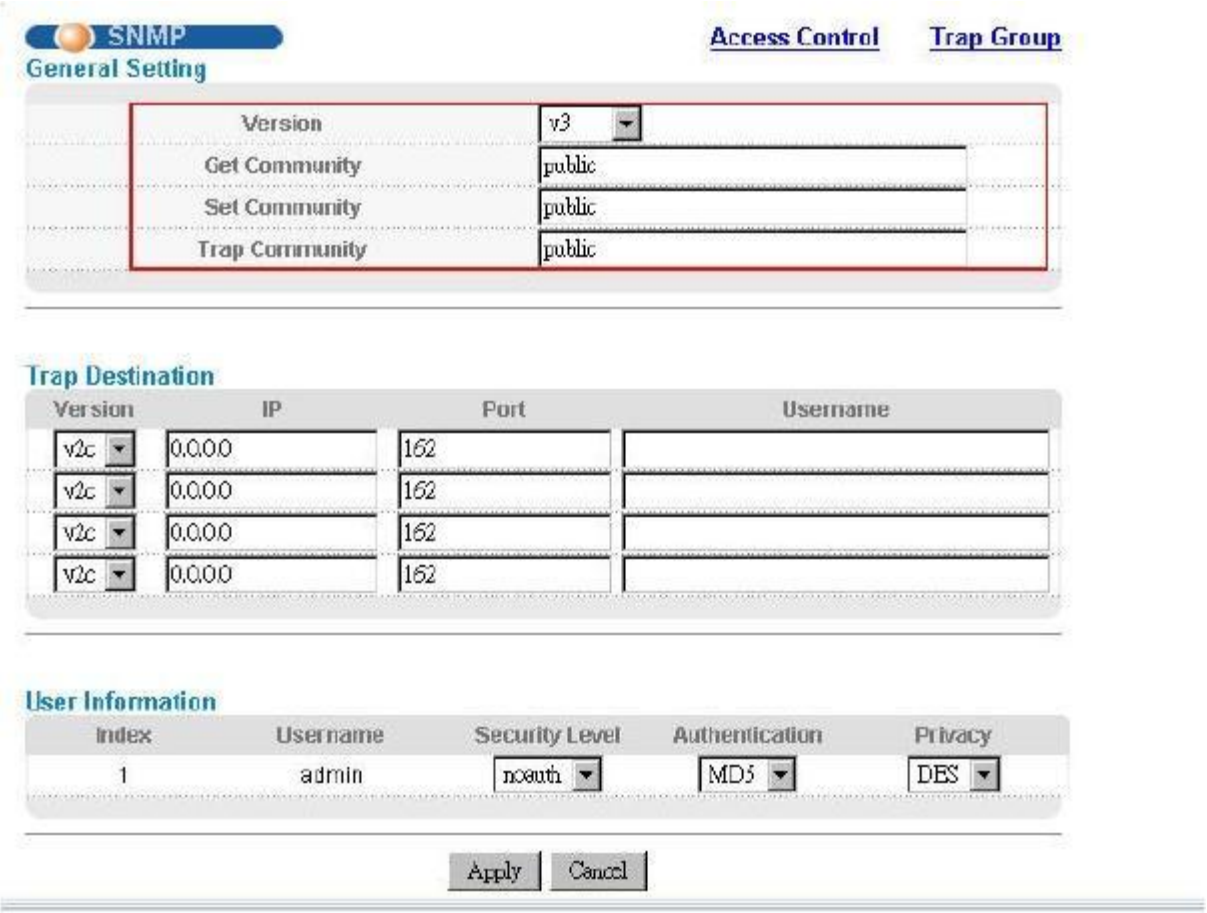
1. Connect the MGMT port to a PC or Notebook with the RJ45 Cable.
2. By default, the MGMT IP address of the out-band port is 192.168.0.1/24
3. Set your NIC to 192.168.0.100/24
4. Open an Internet browser (e.g. IE) and enter http://192.168.0.1 into the URL field.
5. By default, the username for the administrator is "admin" and the password is "1234".
6. After successfully logging in you will see a screen similar to the one below.



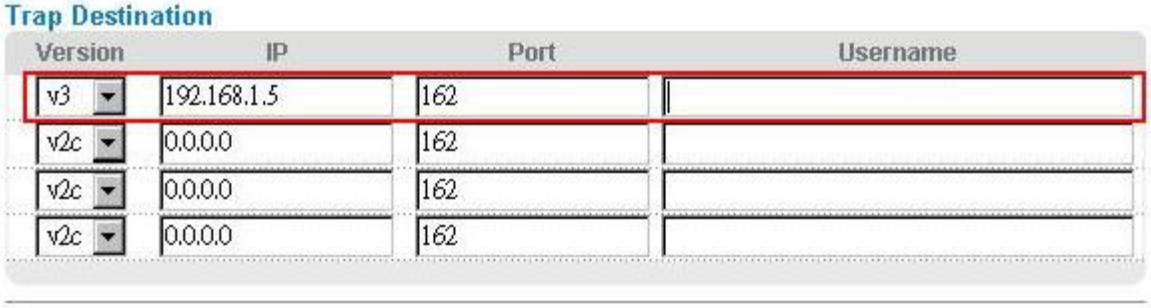

| Port | Name | Link | State | PD | LACP | TxPkts | RxPkts | Errors | Tx KB/s | Rx KB/s | Up Time |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | 1000M/F | FORWARDING | Off | Disabled | 1116 | 1476 | 0 | 29.787 | 8.825 | 1:17:32 |
| 2 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 3 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 4 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 5 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 6 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 7 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 8 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 9 | | Down | STOP | - | Disabled | 819 | 10239 | 0 | 0.0 | 0.0 | 0:00:00 |
| 10 | | Down | STOP | - | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |

7. To enter the "**SNMP**" page, click "**Management**" "**Access Control**" "**SNMP**"


8. In the "SNMP" page, we can choose what SNMP version, SNMPv2c, SNMPv3 or both. Here we choose to use SNMPv3. Then configure the "**Get Community**", "**Set Community**", and "**Trap Community**" values. The term "**Community**" is nothing more than "**password**". "**Get Community**" which means: The password to get the SNMP messages and so on. Here we use the default communities to let users easier to understand. By default, the communities are "**public**".




9. We can configure which kind of events should trigger the SNMP trap message. 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.



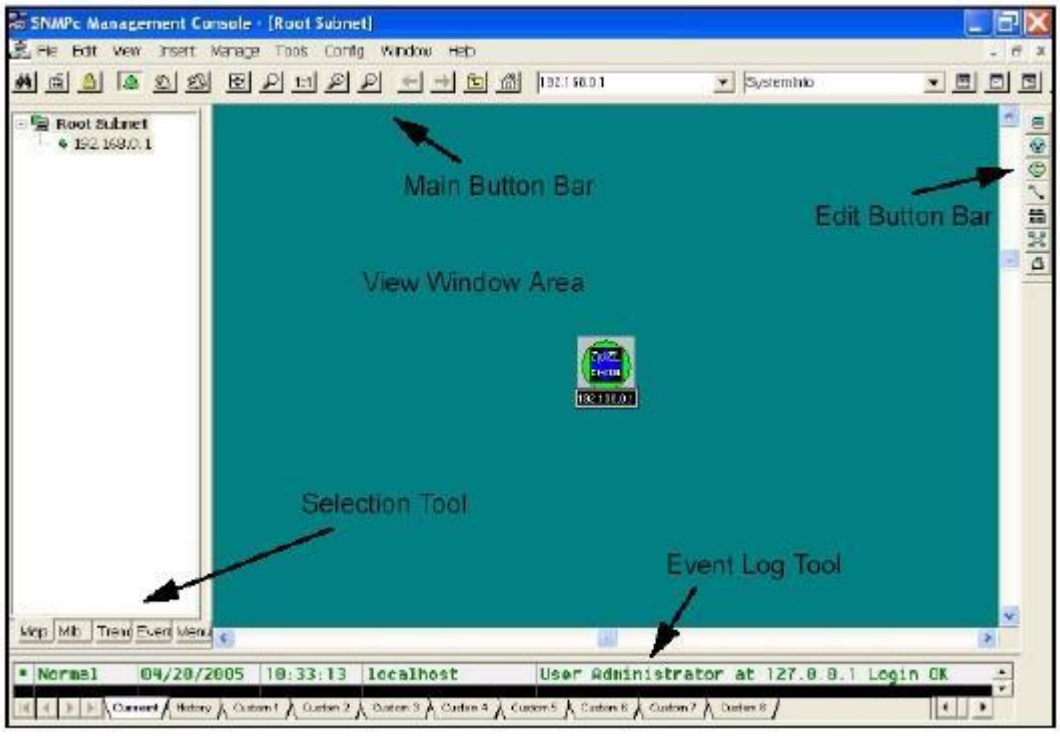

10. Configure the "**User information**". There we can choose Security Level, Authentication methods, and encryption methods. Here we use "**noauth**" for no authentication.Click "**Apply**"

# Overview of SNMPc

The following diagram shows the main elements of SNMPc. SNMPc includes the following functions:

- **Main Button Bar**: Button and controls to execute commands quickly
- **Edit Button Bar**: Button to quickly insert map element
- **Event Log Tool**: Button to display filtered event log entries
- **View Window Area**: Map View, Mib Tables and Mib Graph windows are displayed here.
- **View Window Area**: Map View, Mib Tables and Mib Graph windows.

**Figure 2 Main elements of SNMPc**

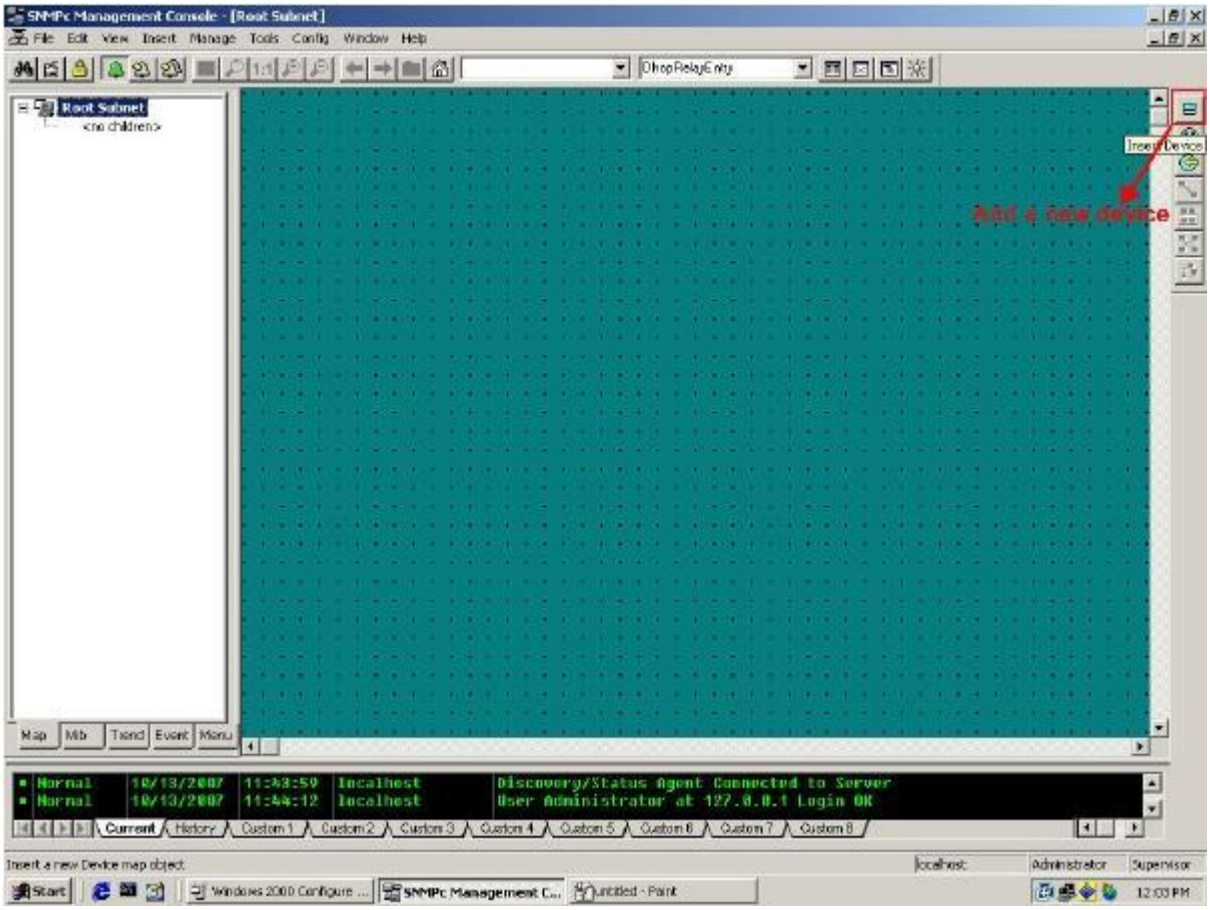


## Adding a new device via SNMPc

In the following example, we will illustrate how to get started with adding a new device with SNMPc and NetAtlas. Follow the procedures from Step 1 to Step 11.

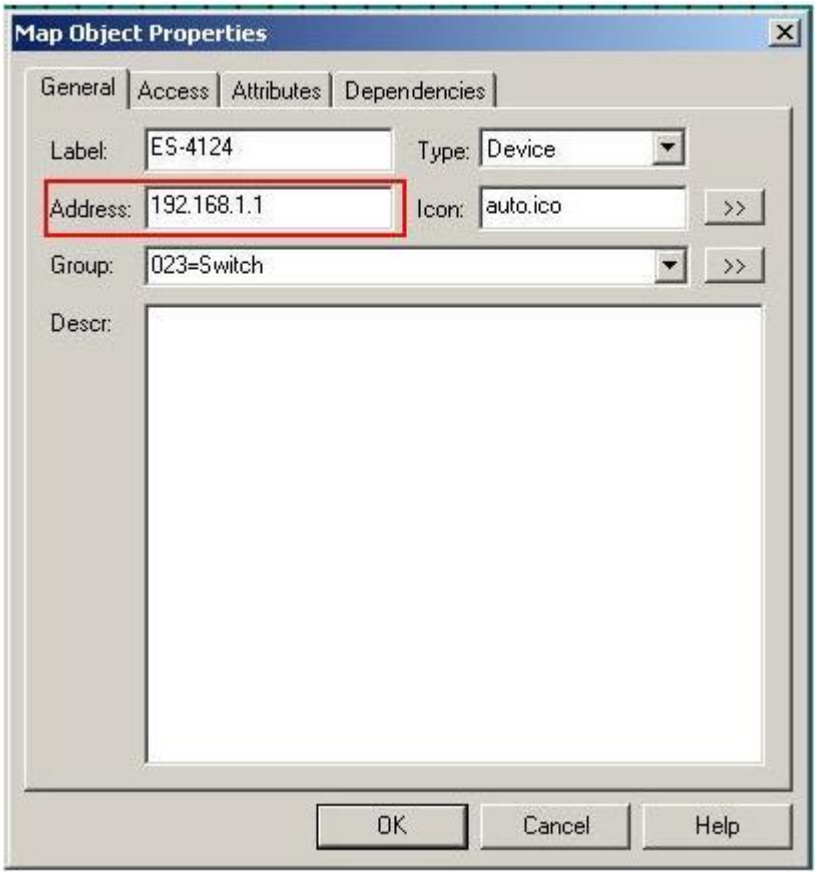
**Step 1**: In the edit button bar shown in the Figure 4, click the icon to insert a new element.

**Figure 4 Adding a new Device**



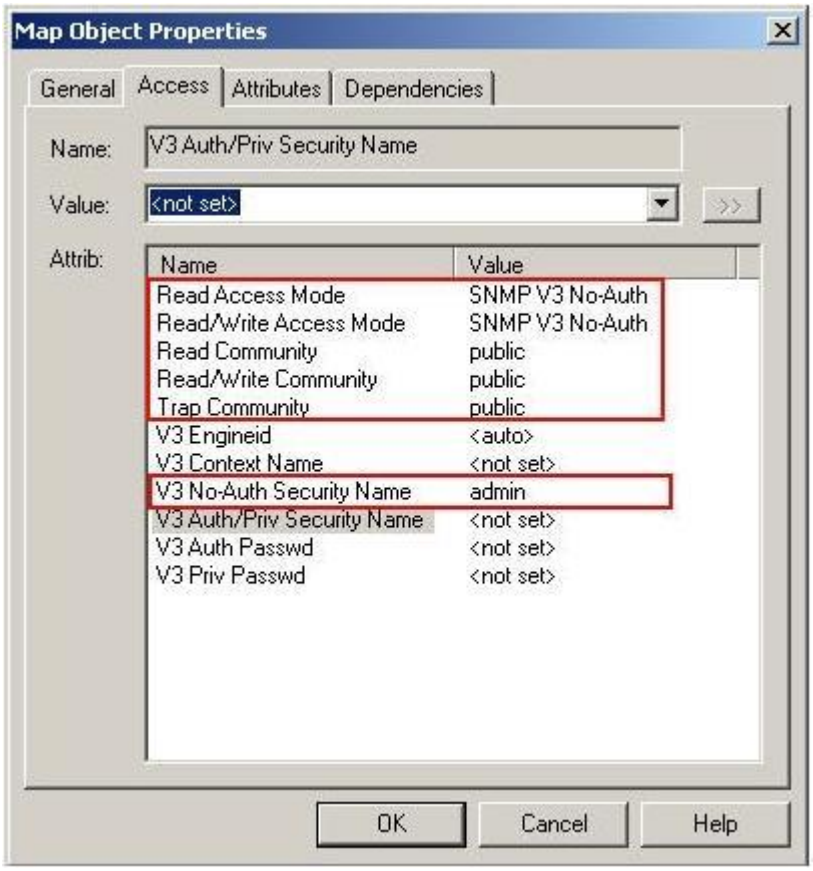

**Step 2:** In the map object properties, insert the label name and the IP address of the selected device. In this example, we set 192.168.1.1 as the IP address of your Switch as shown on Figure 5

**Figure 5 Map Object Properties**



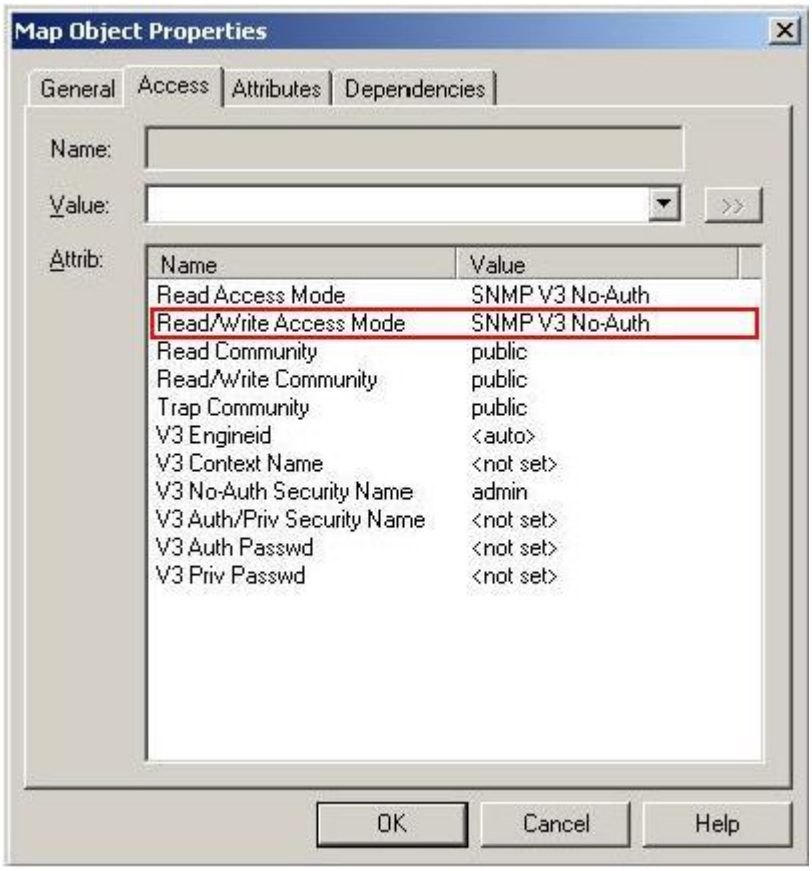

**Step 4:** In the map object properties, select "**Access"** tab to set the parameters of Read Access Mode to "**SNMP V3 No-Auth**" shown on Figure 6. Change the value of Read Access Mode to "**SNMP V3 No-Auth**". Set all the communities to "**public**", set the "**V3 No-Auth Security Name**" to "**admin**"

**Figure 6 Read Access mode**



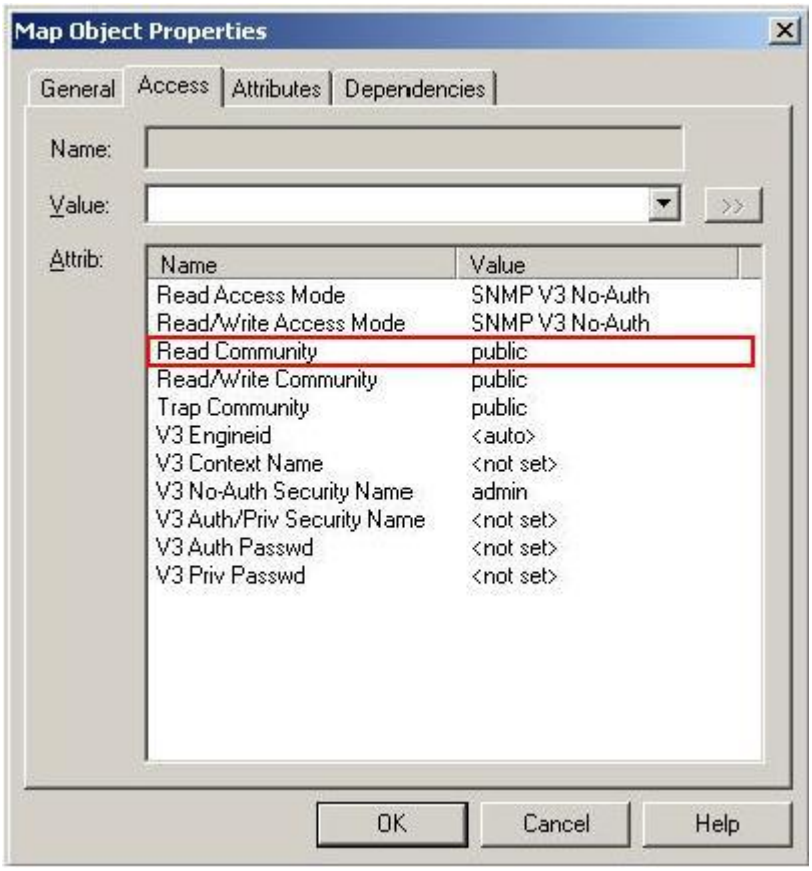

**Step 5:** In the map object properties, select **Access** tab to set the parameters of Read /Write Access Mode to SNMP V2c shown on Figure 7. Change the value of Read/write Access Mode to "**SNMP V3 No-Auth**".

**Figure 7 Read/Write Access Mode**



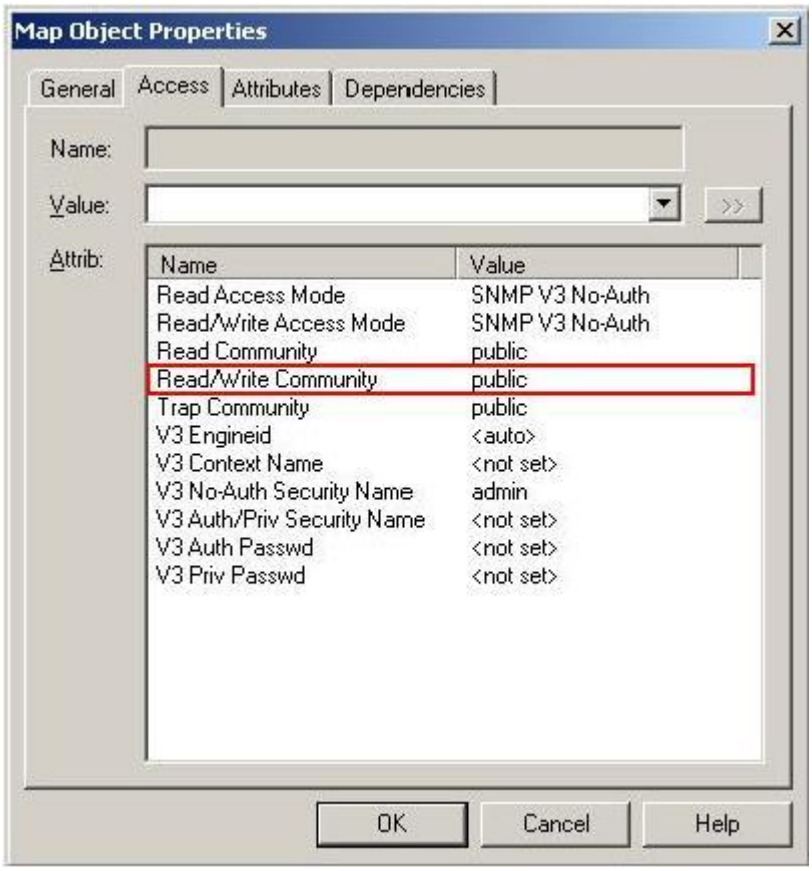

**Step 6:** In the map object properties, select **Access** tab to set the parameters of Read community to public as shown on Figure 8.

**Figure 8 Read Community**

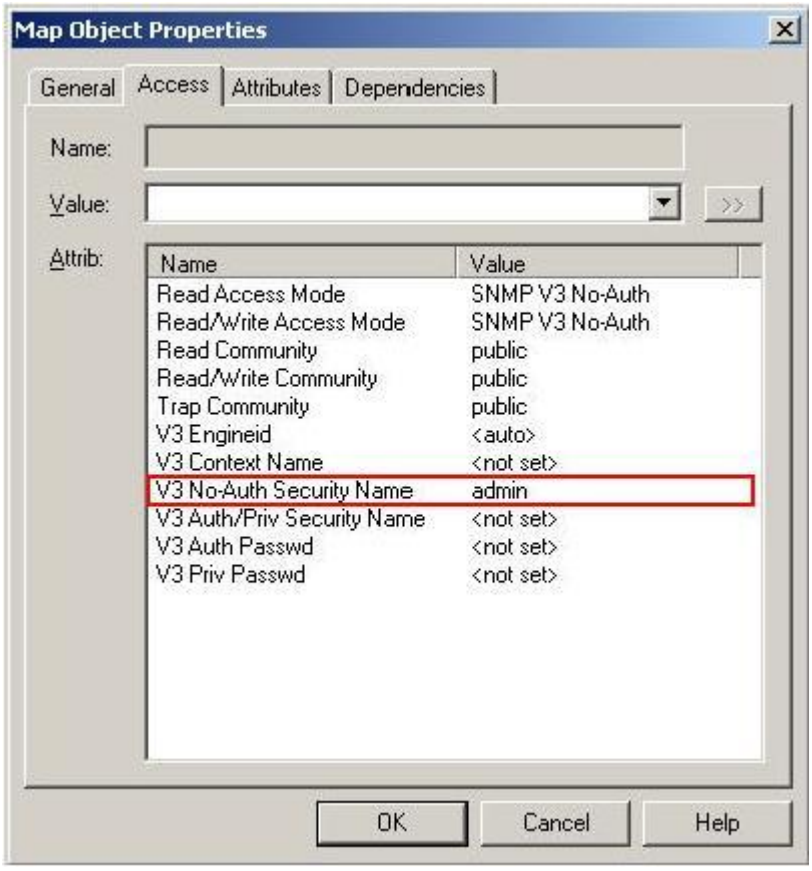



**Step 7:** In the map object properties, select **Access** tab to set the parameters of Read community to public as on Figure 9. Change the value of Read//write Community to Public.

**Figure 9 Read/write Community**




Step 8: In the map object properties, select Access tab Change the value of "**V3 No-Auth Security Name**" to "**Admin**" as on Figure 10. Click "**OK**"



Step 8: After successfully created a SNMP management entry, the link is up when the icon shows green. The SNMP session is distributed and the SNMP manager can control the device from the session from now on.

# Configuration ZyXEL switch using the CLI

```
vlan 1 name 1
    normal ""
    fixed 1-10
    forbidden ""
    untagged 1-10
    ip address 192.168.1.1 255.255.255.0
exit
interface route-domain 192.168.1.1/24
exit
snmp-server version v3
/*Using the default communities, thus, no more SNMPv3 related configuration
needed*/
```