Port Authentication

(802.1X & Radius)

Ethernet Switch

ZyNOS 3.7

Support Notes

Version 3.70

August 2006

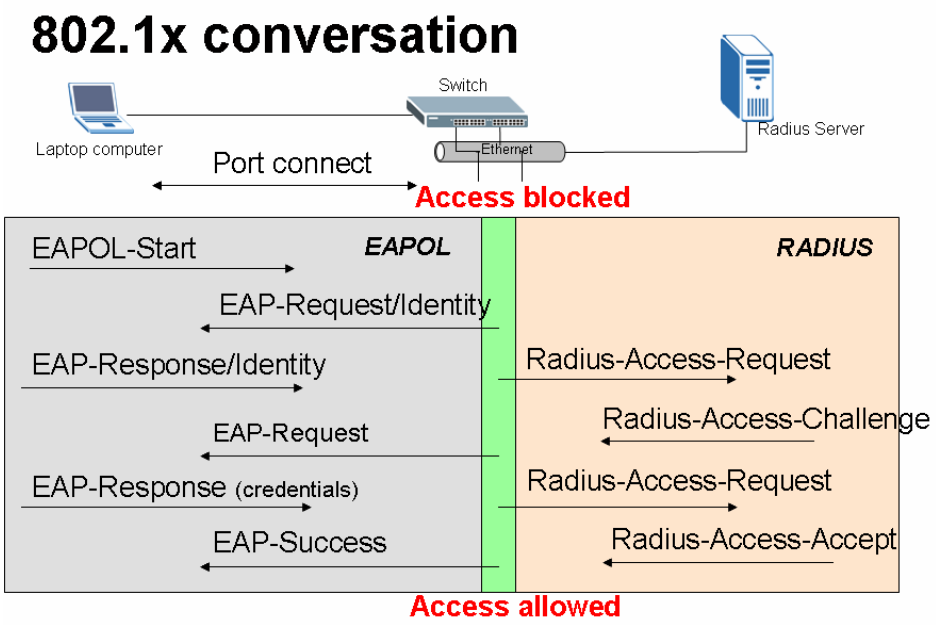
ZyXEL

Unleash Networking Power

Overview of 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control and it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, allows the establishment of a point-to-point connection or prevents access from that port if authentication fails. IEEE 802.1X is available on certain network switches, and can be configured to authenticate hosts which are equipped with supplicant software, thus denying unauthorized access to the network at the data link layer.

Upon detection of a new client (supplicant), the port on the switch (authenticator) will be enabled and set to the "unauthorized" state. In this state, only 802.1X traffic will be allowed; other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator will send out the EAP-Request identity to the supplicant which will then send out the EAP-response packet that the authenticator will forward to the authenticating server. The authenticating server can accept or reject the EAP-Request; if it accepts the request, the authenticator will set the port to the "authorized" mode and normal traffic will be allowed. When logging off, the supplicant will send an EAP-logoff message to the authenticator. The authenticator will then set the port to the "unauthorized" state - once again blocking all non-EAP traffic.



IEEE 802.1X RADIUS Network Example

In the following section, we will provide an example to illustrate how to configure IEEE 802.1X RADIUS. In this network example, two RADIUS servers (192.168.2.200 and 192.168.2.201) are installed for loading balancing. The pre-share key for both RADIUS servers is 1234 .

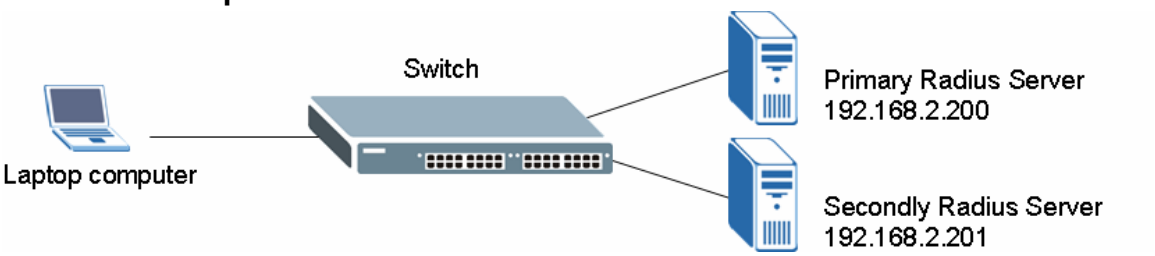
On the switch, IEEE 802.1X Port Authentication is activated Switch port 1~8. VLAN assignments and Bandwidth assignment will be supplied to the user computers after a successful login via 802.1X RADIUS.

For this example, we set up an user account of "abc" on both RADIUS Servers. This user will be assigned a VLAN ID of 500 and the ingress bandwidth of 100Kbps.

Configuration Overview:

1. Prepare your RADIUS Servers
2. Enable 802.1X RADIUS authentication and configure the RADIUS server settings on the Switch (Load balance Mode).
3. Enable Port Authentication on ports 1 to 8

Network Example



Important Notes:

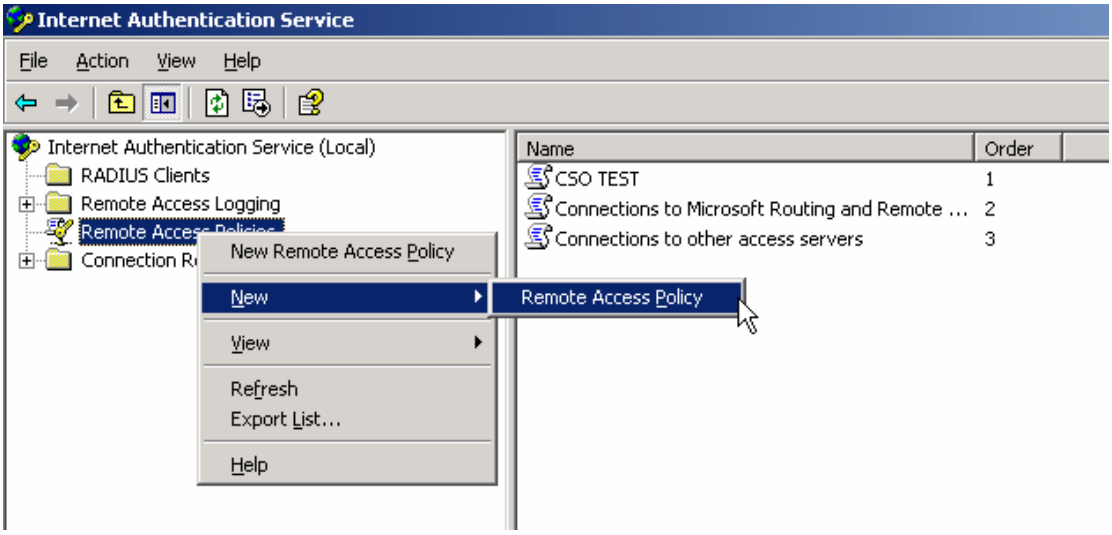
1. You need to set the VLAN settings on the Switch first before you configure 802.1X authentication with VLAN assignment. In this example, you will need to create a VLAN with VID 500 and set the user ports to "Normal" and the uplink port(s) to "Fixed". Refer to the 802.1Q (tag based) support note for more information of VLAN setup.
2. After a user is authenticated by the RADIUS server, you can check the result of the VLAN assignment by viewing the VLAN Status screen. However, you cannot check the bandwidth assignment status in the web

configurator or the CLI on the Switch.

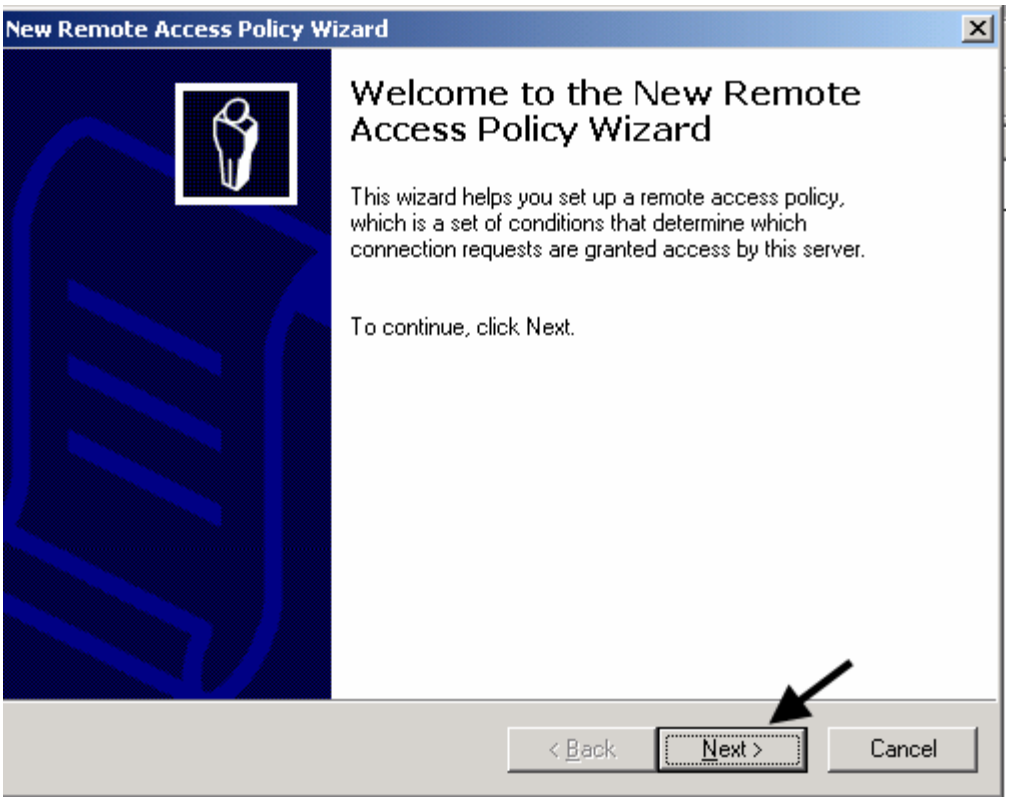
RADIUS Server Setup Example

You need to use a RADIUS server that supports VLAN and Bandwidth assignment through IEEE 802.1x. In this example, we will use Microsoft IAS Server (Internet Authentication Service). The latest version of Microsoft IAS Server is bundled with the Microsoft Windows 2003 Server.
Follow the steps below to configure remote access policies on IAS server.

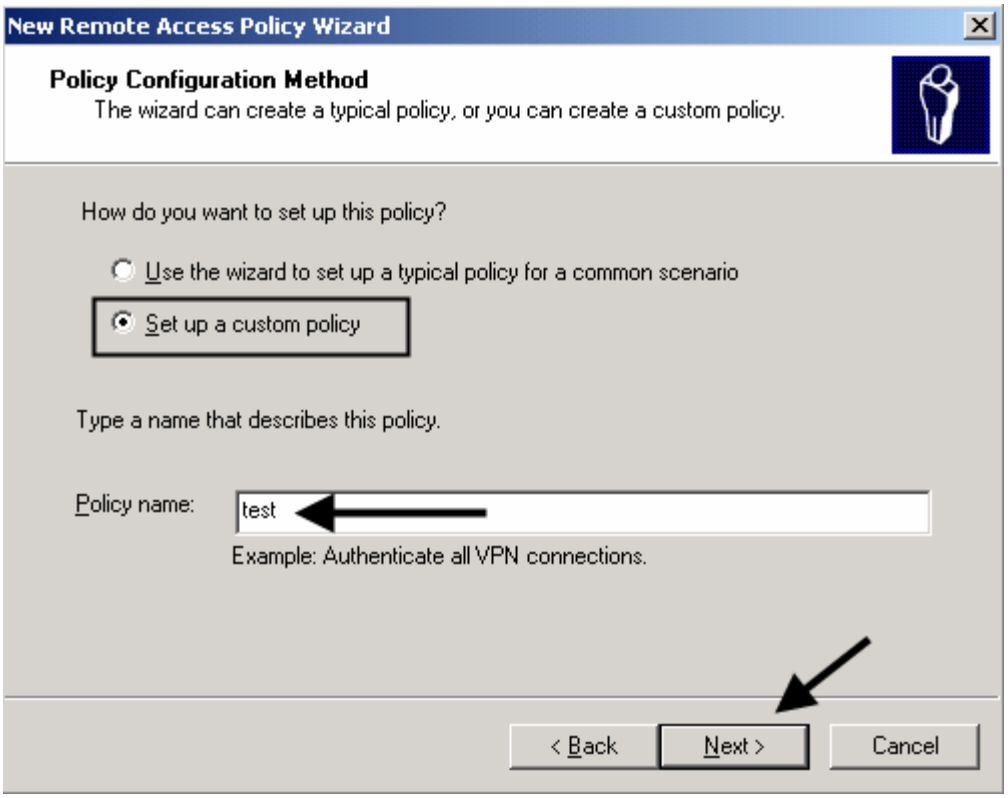
1. Open the Microsoft IAS Console and right-click on **Remote Access Policies** and then click **New** > **Remote Access Policy**.



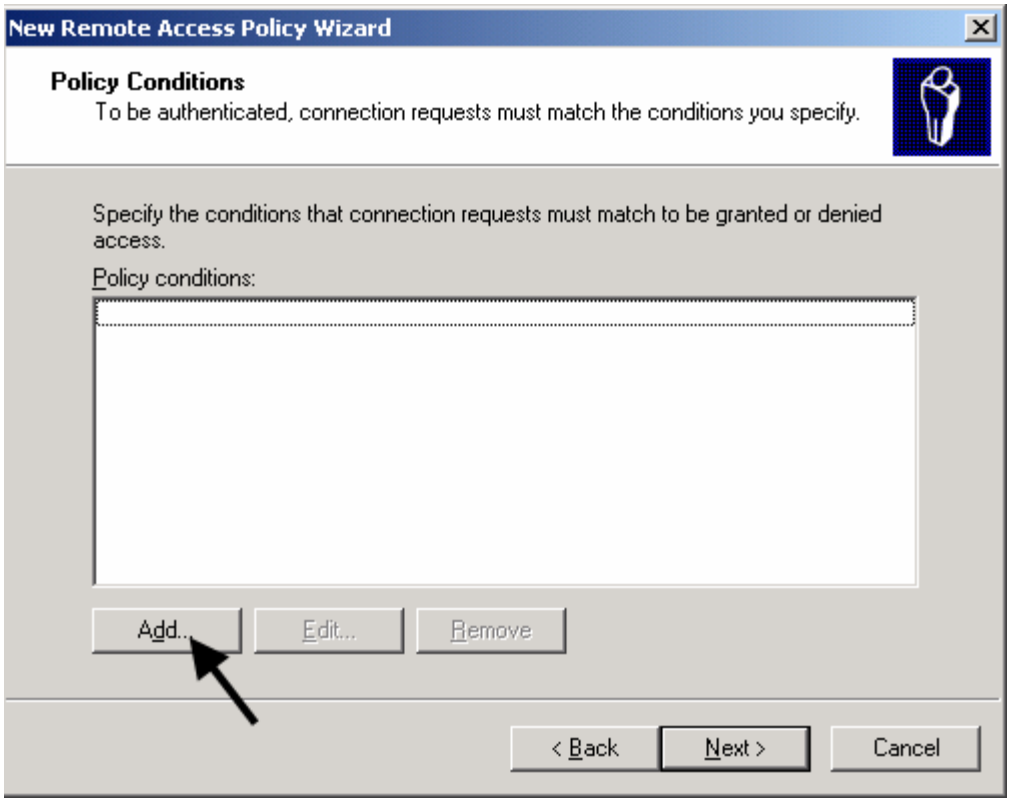
2. A welcome screen displays. Click **Next**.



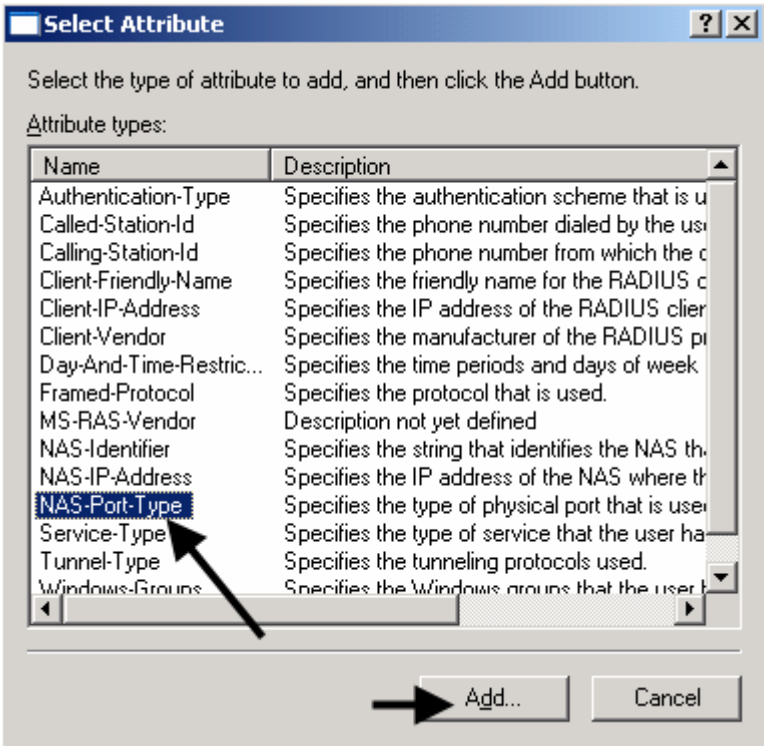
3. Select **Set up a custom policy** and enter a descriptive name in the **Policy name** field (for example, “test”). Click **Next** to continue.



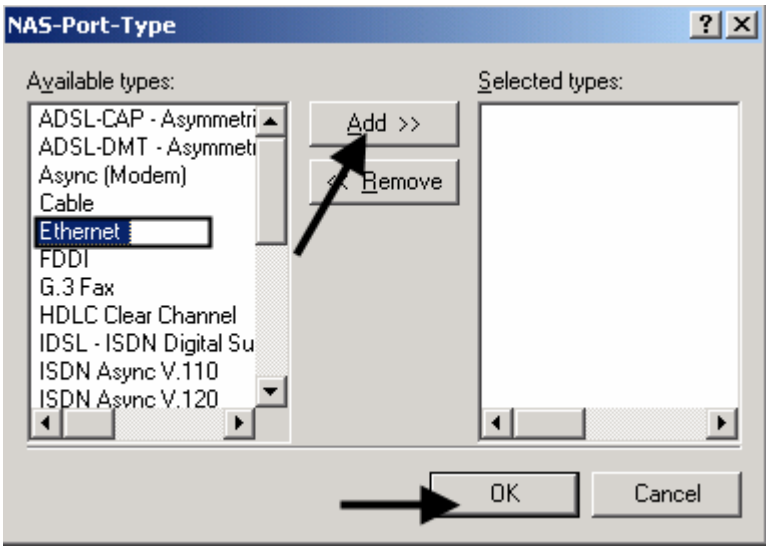
4. Click **Add** to create a new policy and click **Next**.



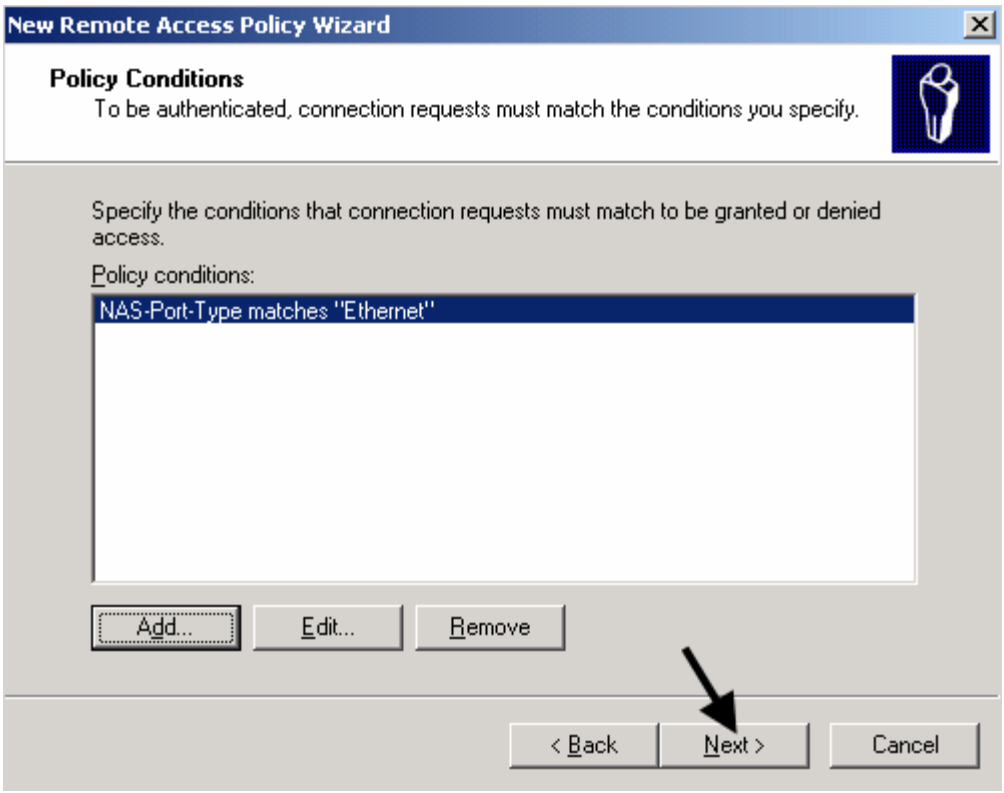
5. In the **Set Attribute** screen, select **NAS-Port-Type**.



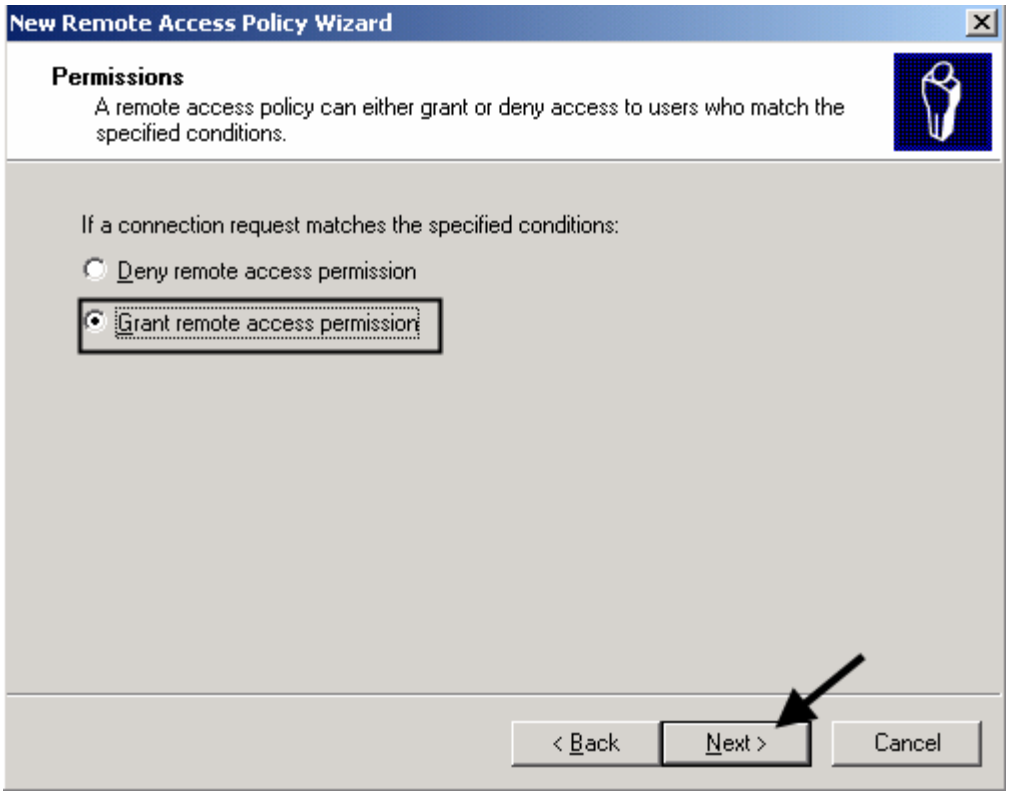
6. A screen displays as shown. Select **Ethernet** in the **Available types** list and click **Add**. Click **OK** to save the setting.



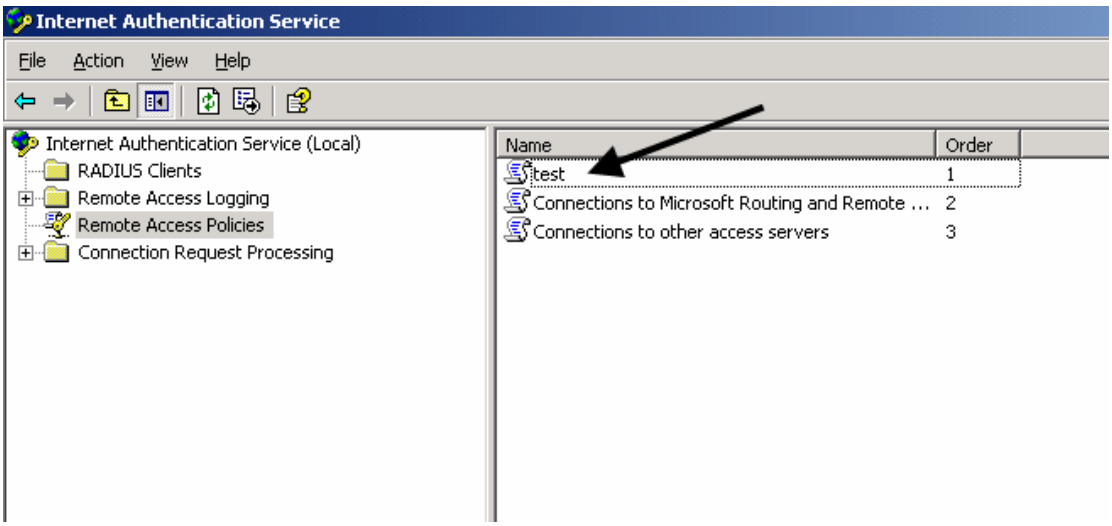
7. Click **Next**.



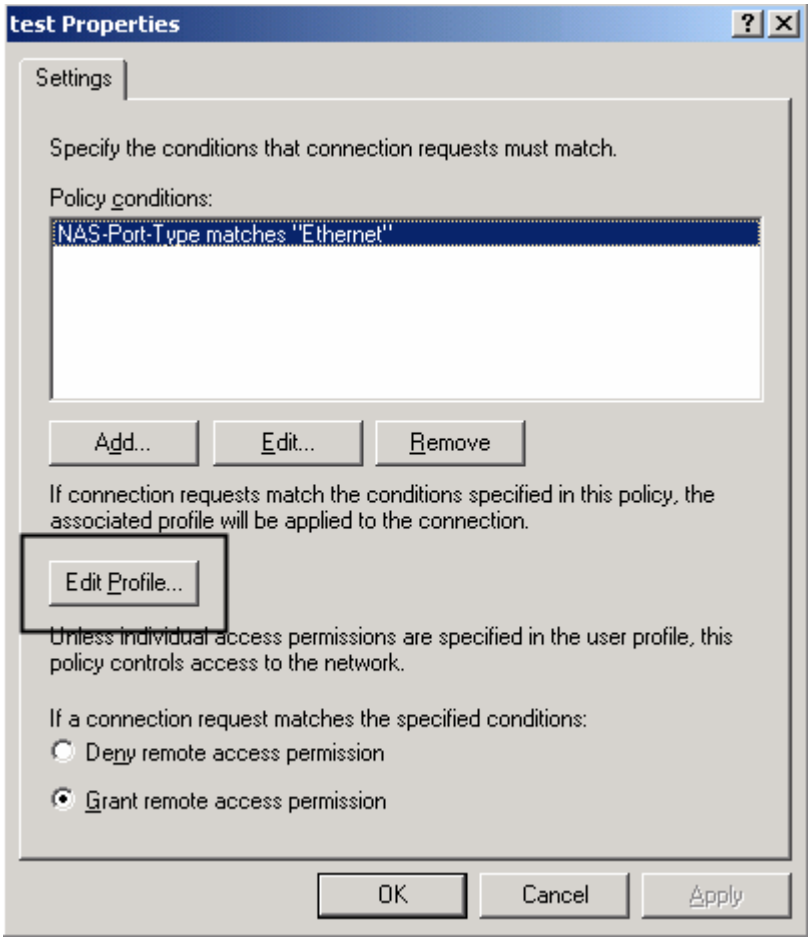
8. Select **Grant remote access permission** and click **Next** in each screen. In the last screen, click **Finish**.



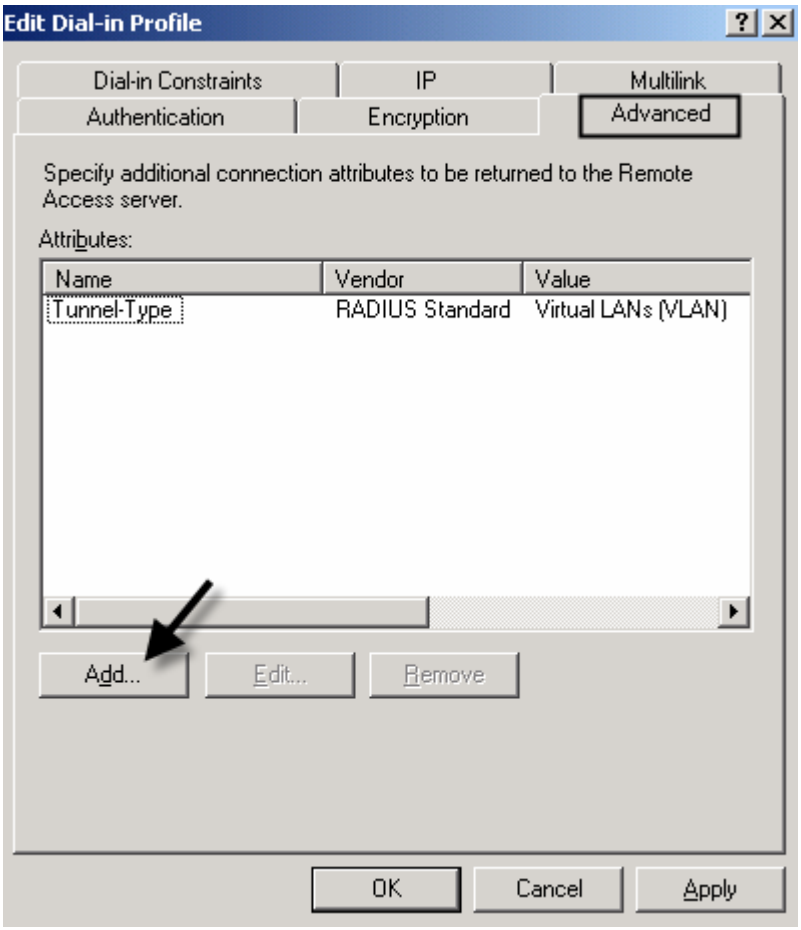
9. Return to the console screen and double-click on the policy that you have just created.



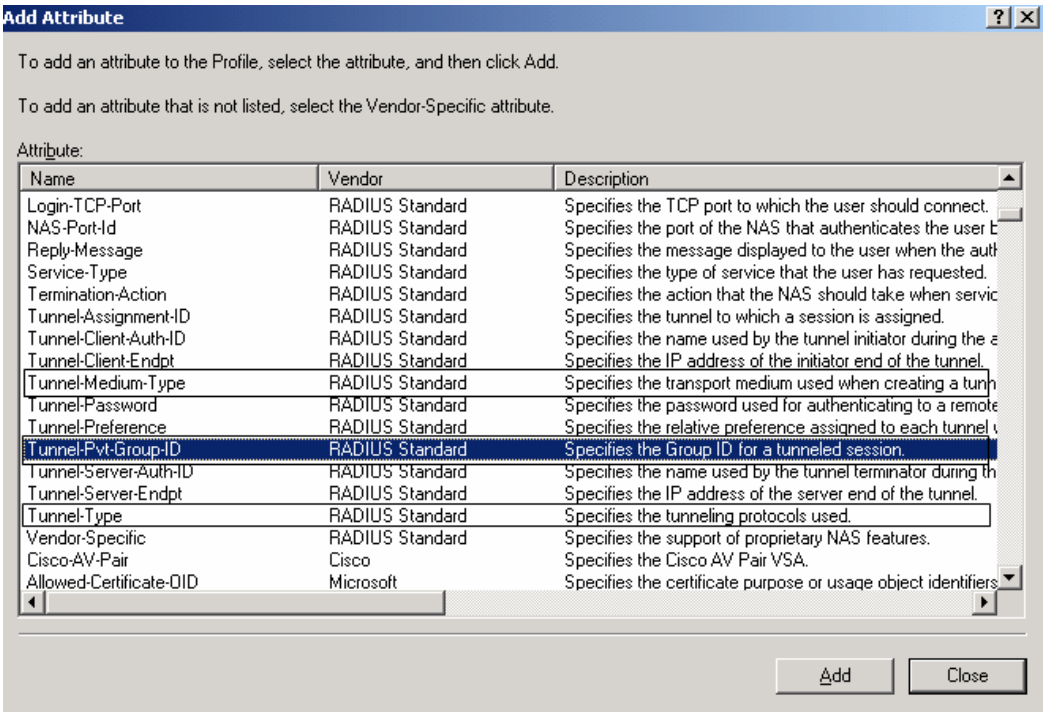
10. Click **Edit Profile**.



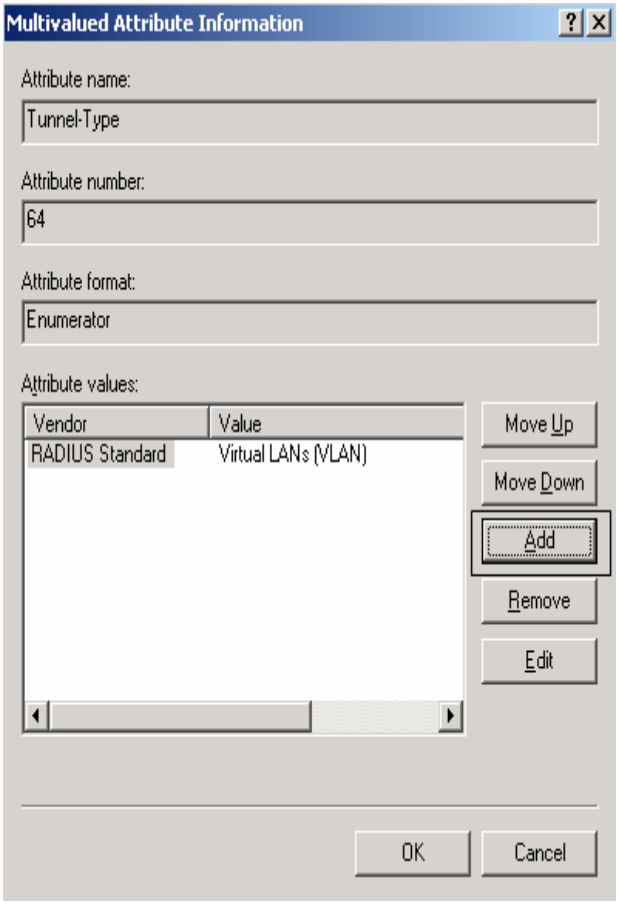
11. Click the **Advanced** tab and **Add**.



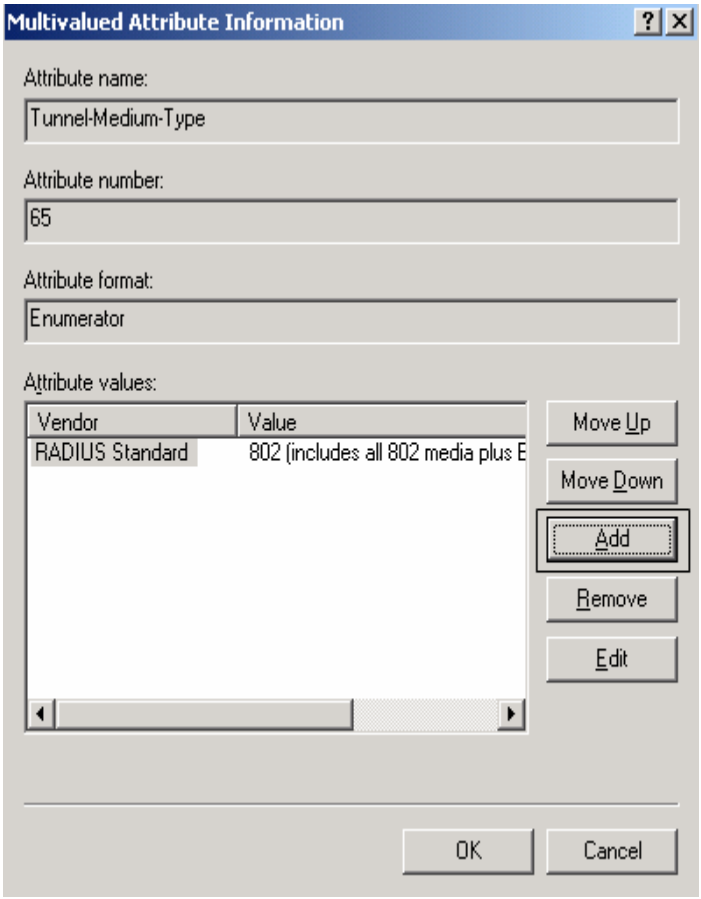
12. In the **Add Attribute** screen, add the **Tunnel-Medum-Type**, **Tunnel-Pvt-Group-ID**, and **Tunnel-Type** attributes.



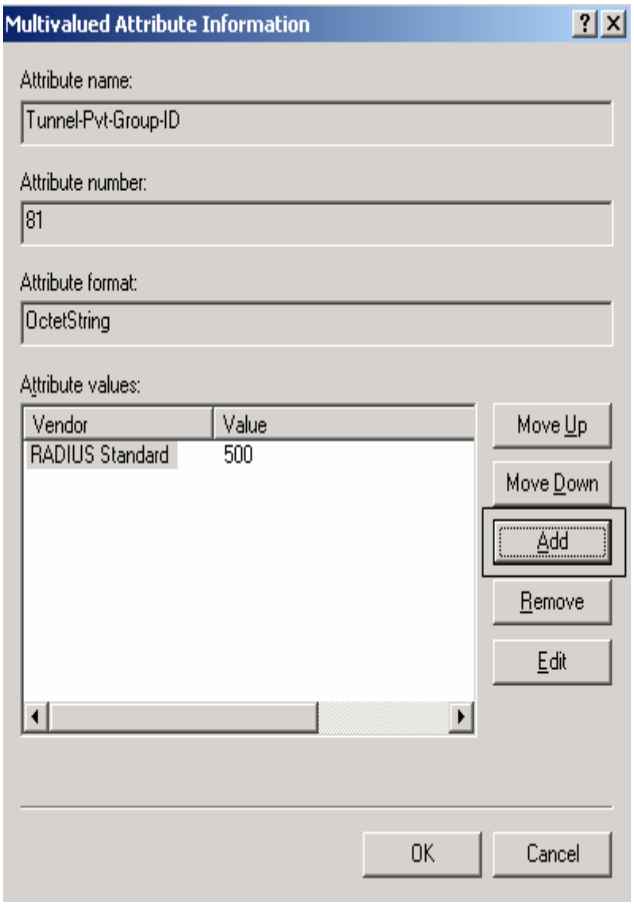
13. For the **Tunnel-Type** attribute, add a **Virtual LANs** value.



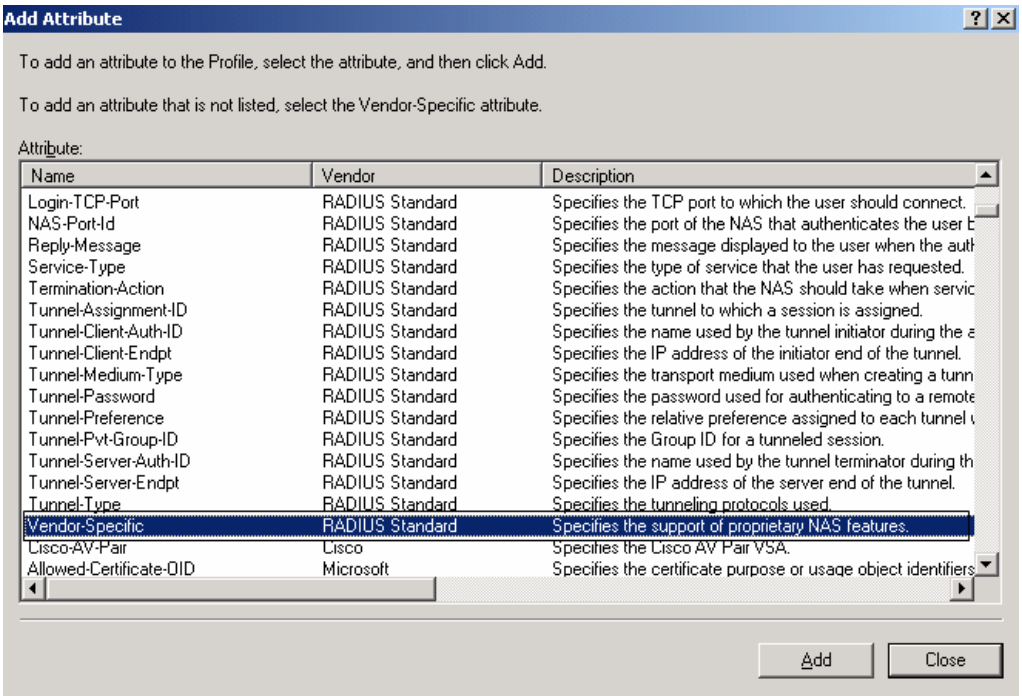
14. For the **Tunnel-Medium-Type** attribute, add a **802 (includes all 802 media…)** value.



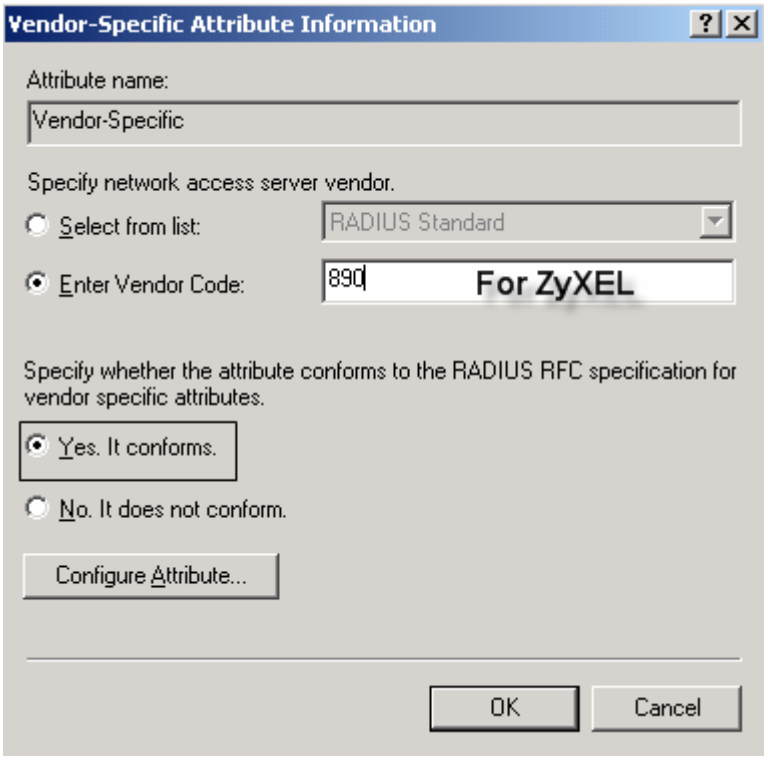
15. For the **Tunnel-Pvt-Group-ID** attribute, add the VLAND ID as the value. In this example, add a VLAN ID of 500.



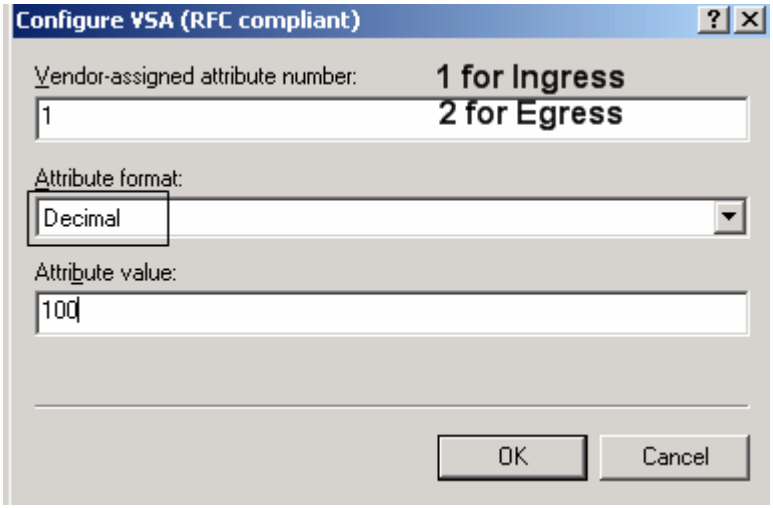
16. For bandwidth assignment, add a **Vendor Specific** attribute.



17. Select **Enter Vendor Code** and enter “890” (for ZyXEL). The select **Yes. It conforms**. Click **Configure Attribute**.



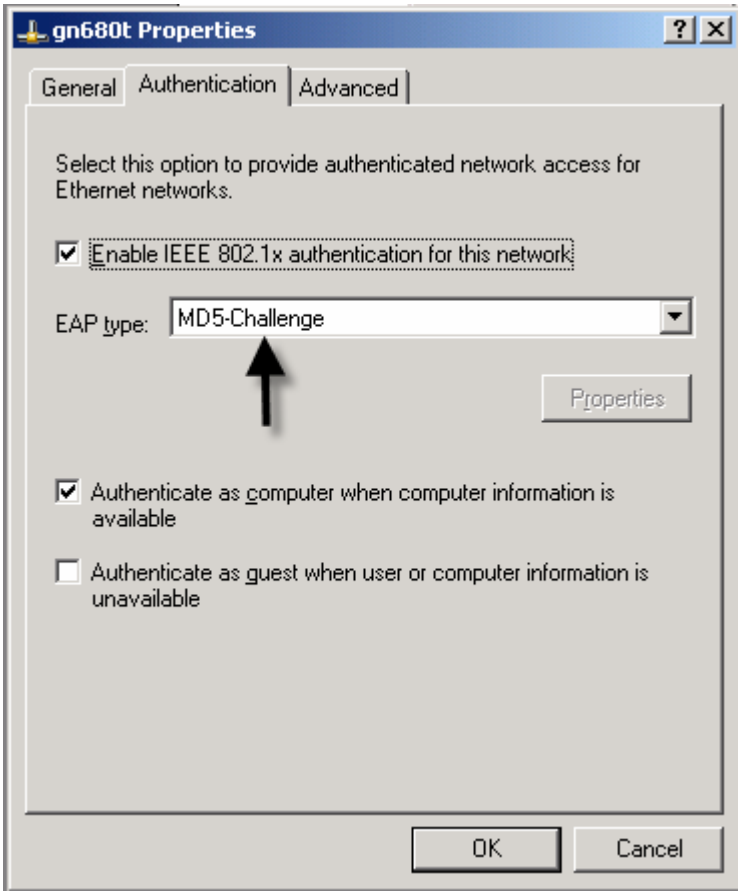
18. In the **Vendor-assigned attribute number** field, enter “1” for Ingress bandwidth control, or enter “2” for Egress bandwidth control. Then select **Decimal** in the **Attribute format** field and enter the PIR bandwidth allowed in the **Attribute value** field. as the value. *(Ingress CIR is not supported)



19. Click **OK** to save the settings. Now you have completed the VLAN and bandwidth assignment configuration for the policy on the IAS Server.

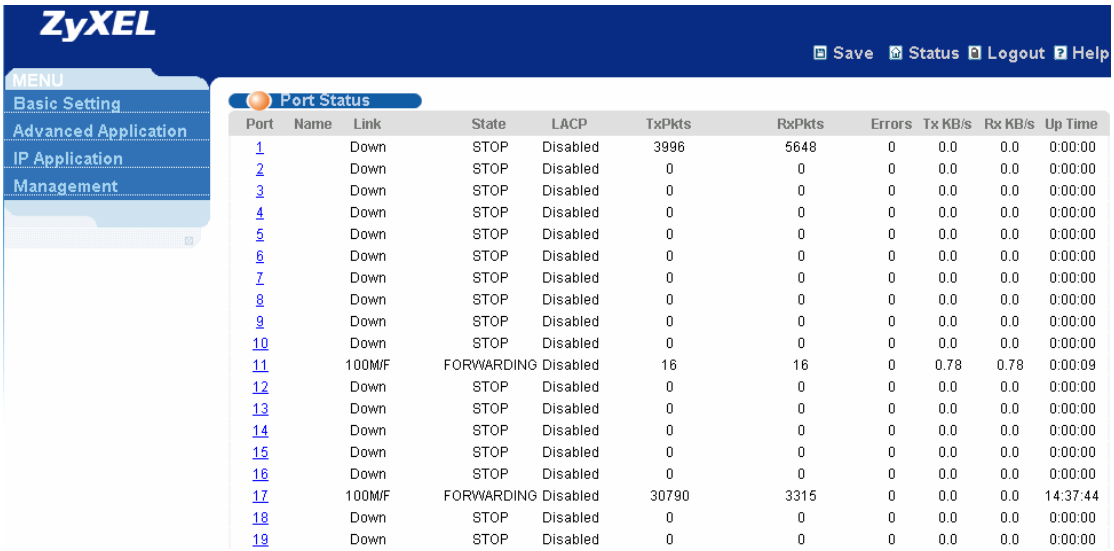
IMPORTANT: The previous steps only shows you how to configure policies on the IAS server. You will still need to configure the user

accounts on the IAS server and specify which policy is to be applied on the accounts and the method the server is to use to authenticate the clients through IEEE 802.1x. For example, you may enable MD5 authentication on the client's network adaptor.



ZyXEL Switch Setup using the Web Configurator

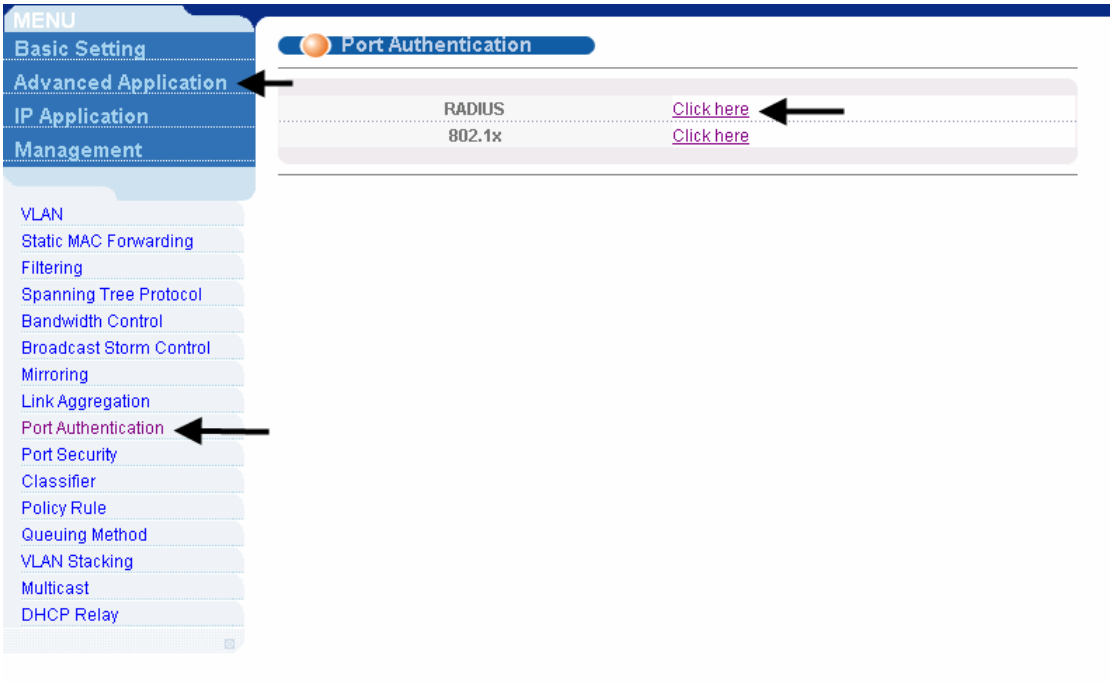
1. Use an Ethernet cable to connect your computer to port 1 on the ZyXEL switch.
2. By default, the management IP of the ZyXEL switch is 192.168.1.1/24 through any port.
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.1.2/24).
4. Open an Internet browser such as IE and enter http://192.168.1.1 as the URL.
5. Enter the user name (“admin” is the default) and the password (“1234” is the default).
6. After you have logged in successfully, the main screen displays similar to the one shown below.



Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Disabled	3996	5648	0	0.0	0.0	0:00:00
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11		100M/F	FORWARDING	Disabled	16	16	0	0.78	0.78	0:00:09
12		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17		100M/F	FORWARDING	Disabled	30790	3315	0	0.0	0.0	14:37:44
18		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
19		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

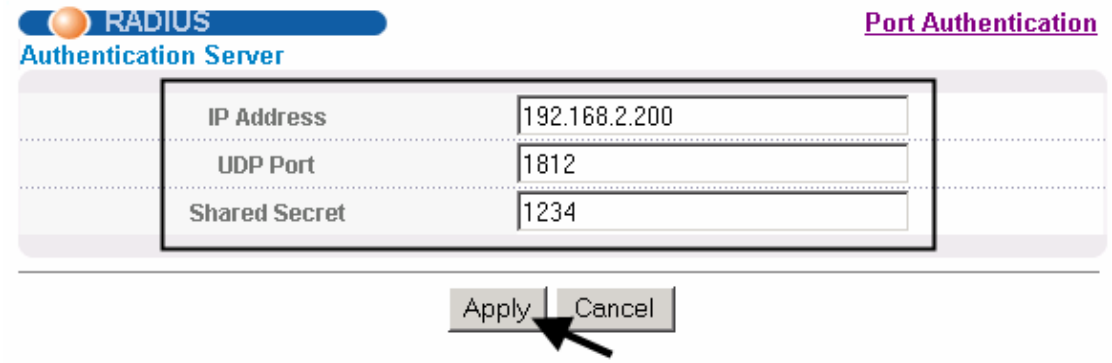
7. **Configure the RADIUS server settings on the ZyXEL switch. There are two RADIUS servers on the network for load balancing, Set the primary RADIUS server settings in the web configurator.**

   In the navigation panel, click **Advanced Application > Port Authentication** and click the **Click here** link for **RADIUS**.



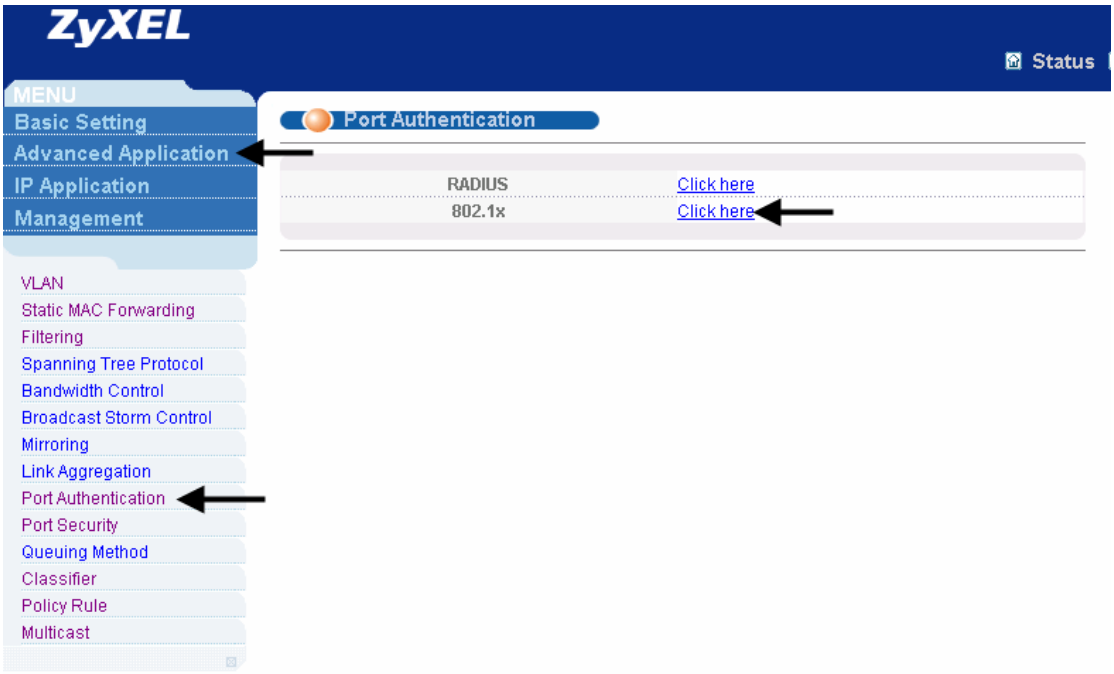
8. Enter the IP address, UDP Port, and shared secret of your primary RADIUS Server in the fields below.

   IMPORTANT: You can only set the You must use the CLI to configure the secondary RADIUS server and the server mode.

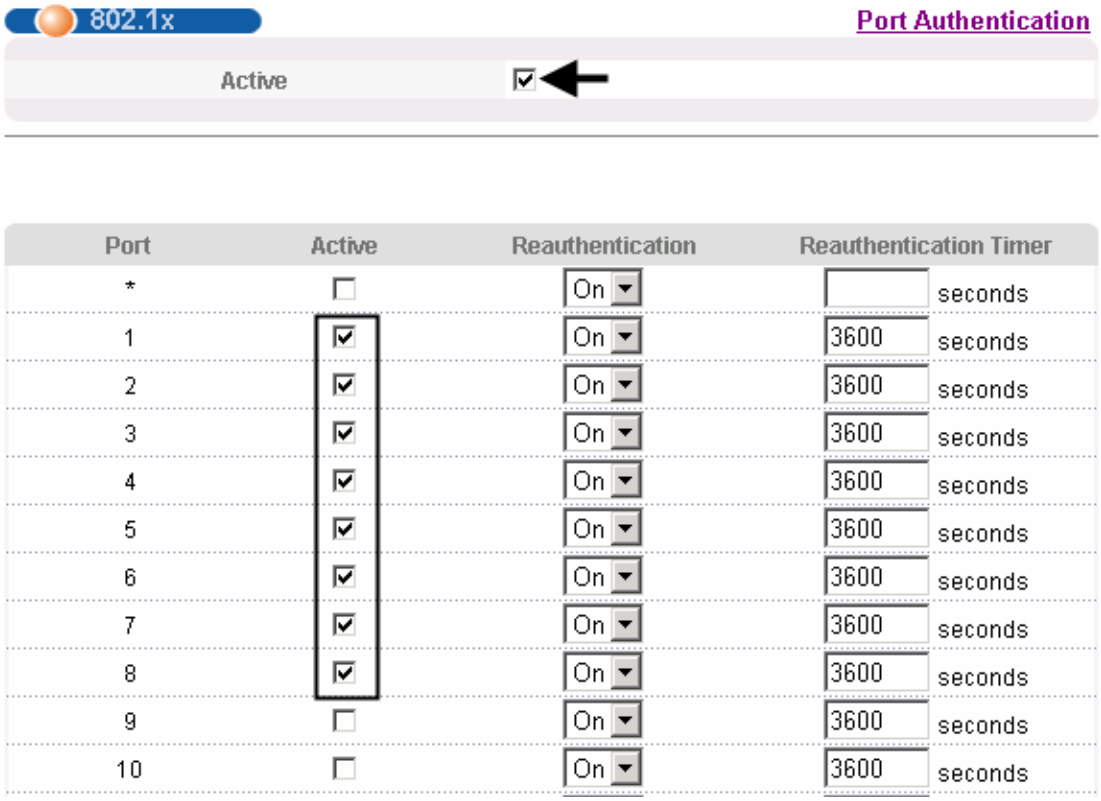


9. **Enable Port Authentication on ports 1 to 8.**

   Click **Advanced Application > Port Authentication** click the **Click here** link for **802.1X**.



10. Select the top Active check box to enable 802.1X on the ZyXEL switch. Then select the Active check boxes for the specific ports (for example, ports 1 to 8) to enable 802.1X on the ports.



Please note that you need to create VLAN groups on the Switch before you enable 802.1X authentication with VLAN assignment. In this network example, you will need to create a VLAN group with a VLAN ID of 500 and set the user ports to “Normal” and the uplink port(s) to “Fixed”. Refer to the 802.1Q (tag based) support note for more information on VLAN setup.

802.1X and RASIU Setup Using the CLI

1. Connect your computer to the console port on the switch.
2. Open your Terminal program.(Ex, Hyper Terminal in Windows System) and set the console port settings to the following

bps:9600
Data bits:8
Parity: None
Stop bits:1
Flow control: None:

Note: You can also access the CLI via telnet / SSH using the default in-band IP of 192.168.1.1 on the Switch.

3. After you have connected successfully, enter the administrator login user name and password.
4. You should enter the privileged mode in the CLI.

5. Enter *configure* to enter the configuration mode.

Enter the following commands to configure the RADIUS servers and set the load balancing mode for the RADIUS servers in this example.

Set the two Radius Servers in the load balancing mode:

Switch(config)# radius-server host 1 192.168.2.200 key 1234
Switch(config)# radius-server host 2 192.168.2.201 key 1234
Switch(config)# radius-server mode round-robin

Enter the following commands to enable Port Authentication on ports 1 to 8.

To enable Port Authentication on port 1 to 8:

Switch(config)# port-access-authenticator
Switch(config)# port-access-authenticator 1-8

Notes:

You can always enter the follow command to check the current RADIUS server configuration on the Switch.

Switch# show radius-server