Port Authentication

(802.1X & Radius)

Ethernet Switch

<u>ZyNOS 4.0</u>

Support Notes

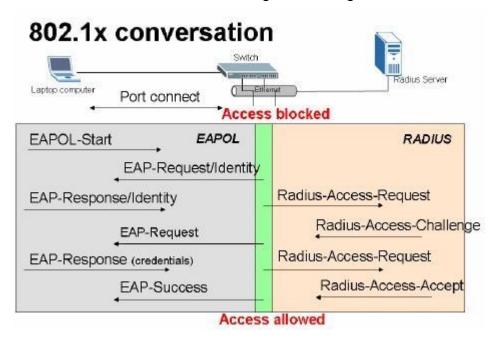
<u>Version 4.00</u> <u>Nov 2011</u>



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.

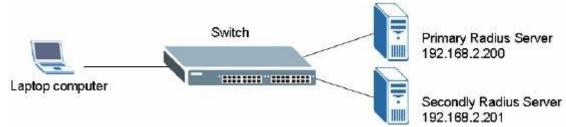
On the switch, IEEE 802.1X Port Authentication is activated Switch port 1~8. VLAN assignments and Bandwidth assignment will be supplied to the user computers after a successful login via 802.1X RADIUS.

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:

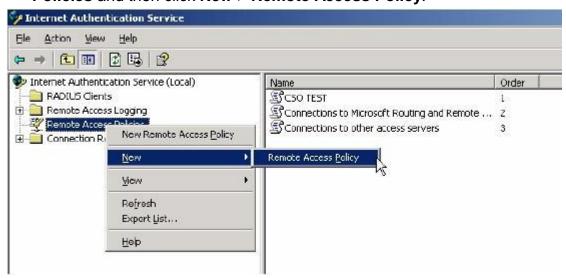
- You need to set the VLAN settings on the Switch first before you configure 802.1X authentication with VLAN assignment. In this example, you will need to create a VLAN with VID 500 and set the user ports to "Normal" and the uplink port(s) to "Fixed". Refer to the 802.1Q (tag based) support note for more information of VLAN setup.
- 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.

New Remote Acce	ss Policy Wizard		×
Policy Configu The wizard o		y, or you can create a custom policy	ŷ
	vant to set up this policy e wizard to set up a typic	? al policy for a common scenario	
● <u>S</u> et up	a custom policy		
Type a name t	that describes this policy.		
Policy name:	test	_	
	Example: Authenticate	e all VPN connections.	
			/
		< <u>B</u> ack <u>N</u> ext>	Cancel
		< <u>B</u> ack <u>N</u> ext>	Cancel

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

v Remote Access Policy	Wizard	
Policy Conditions To be authenticated, c	onnection requests must match the cor	nditions you specify.
Specify the conditions access.	nat connection requests must match to	be granted or denied
Policy conditions:		
Add.	dit <u>R</u> emove	
•	< <u>B</u> ack	Next > Cancel

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

Name	Description	
Authentication-Type	Specifies the authentication scheme that is u	100
Called-Station-Id	Specifies the phone number dialed by the us	
Calling-Station-Id	Specifies the phone number from which the c	
Client-Friendly-Name	Specifies the friendly name for the RADIUS c	
Client-IP-Address	Specifies the IP address of the RADIUS clier	
Client-Vendor	Specifies the manufacturer of the RADIUS pi	
Day-And-Time-Restric	Specifies the time periods and days of week	
Framed-Protocol	Specifies the protocol that is used.	
MS-RAS-Vendor	Description not yet defined	
NAS-Identifier	Specifies the string that identifies the NAS the	
NAS-IP-Address	Specifies the IP address of the NAS where th	
NAS-Port-Type	Specifies the type of physical port that is use	
Service-Type	Specifies the type of service that the user ha	
Tunnel-Type 🔨	Specifies the tunneling protocols used.	
Windows-Groups	Specifies the Windows arouns that the user b	-
	•	

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



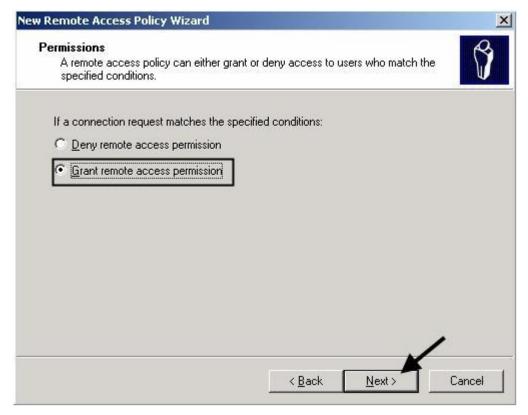
	<u>S</u> elected	types:
ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Async (Modem) Cable Ethernet FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.110 ISDN Async V.120		

7. Click Next.

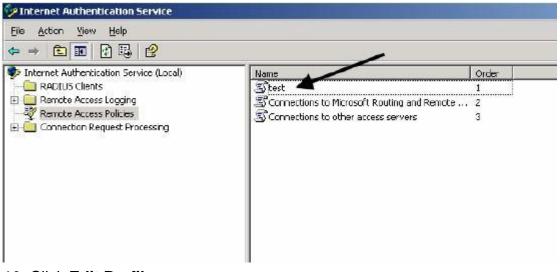
Conditions be authenticated, connection requests must match the conditions you specify. Decify the conditions that connection requests must match to be granted or denied access. Solicy conditions: AS-Port-Type matches "Ethernet"	Ø
cess. Dicy conditions:	
AS-Port-Type matches "Ethernet"	
Add	
`	
< <u>B</u> ack Next> Cance	-1

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.

est Properties				? ×
Settings				
Specify the conditions	that connec	tion request	s must match.	
Policy <u>c</u> onditions:				
NAS-Port-Type match	nes "Etherne	(¹¹		
15				
Add	Edit	Remove	. 1	
	l			
 If connection requests associated profile will I 				licy, the
Edit <u>P</u> rofile				
Unless individual acce			ified in the user p	rofile, this
policy controls access	to the netwo	ork.		
If a connection reques	at matches th	ne specified	conditions:	
C Deny remote acce	ss permissio	n		
• Grant remote acce	ess permissio	n		
		ок	Cancel	Apply
				CHHA

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

11



Dial-in Profile		?
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connec Access server. Attri <u>b</u> utes:		
Name Tunnel-Type	Vendor RADIUS Standard	Value Virtual LANs (VLAN)
		<u>,</u>
Add	t <u>R</u> emove	[
	OK	Cancel Apply

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

	ed, select the Vendor-Specific altr	Louise.
lbigot e :		
Name	Vendor	Description
Login-TCP-Part	RADIUS Standard	Specifies the TCP port to which the user should connect.
NAS-Port-Id	RADIUS Standard	Specifies the port of the NAS that authenticates the user to
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the auth
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Tunnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned.
Tunnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Lunnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunh
TunnelPassword	RADIUS Standard	Specifies the password used for authenticating to a remote
TunnelPreference	RADIUS Standard	Specifies the relative preference appiqued to each turnel u
Tunnel-Pyt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Lunnel-Servel-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during the
Funnel-Server-Endpt	RADIUS Standard	Specilies the IP address of the server end of the tunnel
I unnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
/endor-Specilic	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco AV-Par	Cisco	Specilies the Cisco AV Par VSA.
Allowed-Certificate-OID	Microsoft ,	Specifies the certificate purpose or usage object identifiers,
•		•

All contents copyright (c) 2011 ZyXEL Communications Corporation.

Information	?
Value	Mave <u>U</u> p
Viitual LANs (VLAN)	Move <u>D</u> awn
	<u>PP</u>
	<u>R</u> emove
	Edt
	F

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.



Atiribute name:		
Tunnel-Medium-Type		
Atiribute number.		
65		
Attribute formal:		
Enumerator		
A <u>t</u> iribute values:		
Vendor	Value	Mave <u>U</u> p
RADIUS Standard	802 (includes al 802 media plus E	Move <u>D</u> own
		Add
	1	
		Remove
		<u>E</u> dit
•	•	
	Second Seco	

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



Multivalued Attribute	Information		? ×
Attribute name:			
Tunnel-Pvt-Group-ID			
Attribute number:			
81			
Attribute format			
OctetString			
Aţtribule values:			
Vendor	Value		Move <u>U</u> p
RADIUS Standard	500		Move <u>D</u> own
			<u>A</u> dd
			<u>H</u> emove
			Edt
•		<u>}</u>	1
		OK	Cancel

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

thibute:		
Name	Vendor	Description
Login-TCP-Part	RADIUS Standard	Specifies the TCP port to which the user should connect
NAS-Port-Id	RADIUS Standard	Specifies the port of the NAS that authenticates the user t
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the auth
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Tunnel-Assignment-ID	RADIUS Standard	Specifies the turnel to which a session is assigned.
Lunnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Tunnel-Client-Endot	RADIUS Standard	Specifies the IP address of the initiator and of the tunnel.
Turnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a turn
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Turnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each funnel u
Tunnel-Pyt-Group-ID	BADIUS Standard	Specifies the Group IO for a tunneled session
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the turnel
Turnel-Type	RADIUS Standard	Specifies the tunneling protocols used
Vendor Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Ü\$co	Specifies the Cisco AV Pair VSA
Allowed-Certificate-OID	Microsoft	Specifies the certificate purpose or usage object identifiers
•) () () () () () () () () () (

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



endor-Specific Attribut	e Informatio	n	<u>? ×</u>
Attribute name:			
Vendor-Specific			
Specify network access se	rver vendor.		
C Select from list:	RADIUS	Standard	Y
Enter Vendor Code:	890	For ZyXEL	
 Yes. It conforms. No. It does not conform 			
Configure <u>A</u> ttribute			

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)

	? ×
1 for Ingress	
2 for Egress	
	•
OK Ca	ancel
	2 for Egress

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.

🚣 gn680t Properties	? ×
General Authentication Advanced	
Select this option to provide authenticated network acce Ethernet networks.	ss for
Enable IEEE 802.1x authentication for this network	
EAP type: MD5-Challenge	•
Authenticate as <u>c</u> omputer when computer information available Authenticate as guest when user or computer information unavailable	
ОК	Cancel

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).
- Open an Internet browser such as IE and enter <u>http://192.168.1.1</u> 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.

ZyXEL							∎s	ave 1815	Status (1 Logou	t 🖬 Hel
Basic Setting	Can	ort Sta	atus								
	Port	Name	Link	State	LACP:	TxPlds	ExPlita	Errers	Tx KB/s	Rx HB/s	Up Time
Advanced Application	1		Down	STOP	Disabled	3996	5649	0	0.0	0.0	0.00.00
P Application	2		Down	BTOP	Disabled	0	0	0	0.0	0.0	0.00.00
Management	2		Down	STOP	Disabled	0	0	0	0.0	0.0	0.00.00
	1		Down	STOP	Disabled	Ď	0	Ū.	0.0	0.0	0.00.00
	5		Down	STOP	Disabled	0	0	0	0.0	0.0	0.00.00
	ē		Down	STOP	Disabled	D	D		0.0	0.0	0.00.00
	7		Down	BTOP	Disabled			0 0 0	0.0	0.0	0.00.00
	2 8 9		Down	STOP	Disabled	D D	0	0	0.0	0.0	0100:00
	9		Down	BTOP	Disabled	D	D	0	0.0	0.0	0.00.00
	10		Down	STOP	Disabled	D	p	0	0.0	0.0	0.00.00
	11		100MF	FORMARDING		15	16	0	0.78	0.78	0.00.09
			Down	STOP	Disabled		0	0	0.0	0.0	0.00.00
	12		1.122.026.9	STOP	Disabled	D			0.0	0.0	0.00.00
	13		Down	STOP	TV 101 106351 C	0 0	D	0	1.2.2		
	14		Down	0.47.03203	Disabled	D	0	0	0.0	0.0	0.00.00
	15		Down	STOP	Disabled	0	0	u	0.0	0.0	D:00:00
	<u>18</u>		Down	STOP	Disabled	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	0	0	0.0	0.0	0.00.00
	17 18		100MF	FORMARDING		30790	3315	0	6.0	0.0	14:37:44
			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**.

Basic Setting			
Advanced Application 🛁 🗕			
P Application	RADIUS	Click here	
Management	802.1x	Click here	
VLAN			
Static MAC Forwarding			
Filtering			
Spanning Tree Protocol			
Bandwidth Control			
Broadcast Storm Control			
Mirroring			
Link Aggregation			
Port Authentication			
Part Becurity			
Classifier			
Policy Rule			
Gueuing Method			
VLAN Stacking			
Multicast			
DHCP Relay			

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.

IP Address	192.168.2.200	
UDP Port	1812	
Shared Secret	1234	

9. Enable Port Authentication on ports 1 to 8.

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

ZyXEL			🕅 Statu
MENU			
Basic Setting	Port Authentication		
Advanced Application 🗲			
IP Application	RADIUS	Click here	
Management	802.1x	Click here	
VLAN			
Static MAC Forwarding			
Filtering			
Spanning Tree Protocol			
Bandwidth Control			
Breadcast Storm Control			
Mirroring			
Link Aggregation		and the same share the second state of the same share the second state s	
Port Authentication	-		
Port Security			
Queuing Method			
Classifier			
Policy Rule			
Multicast			

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.

rt Authentica	Port			802.1x
		-► 1	ctive	A
ntication Time	Reauthent	Reauthentication	Active	Port
seconds		On 💌		*
seconds	3600	On 💌		1
seconds	3600	On 💌		2
seconds	3600	On 💌		3
seconds	3600	On 💌		4
seconds	3600	On 💌		5
seconds	3600	On 💌		6
seconds	3600	On 💌		7
seconds	3600	On 💌		8
seconds	3600	On 💌		9
seconds	3600	On 💌		10



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

 Connect your computer to the console port on the switch.
 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