AAA and TACACS+

Ethernet Switch

ZyNOS 4.0

Support Notes

Version 4.0

July 2011

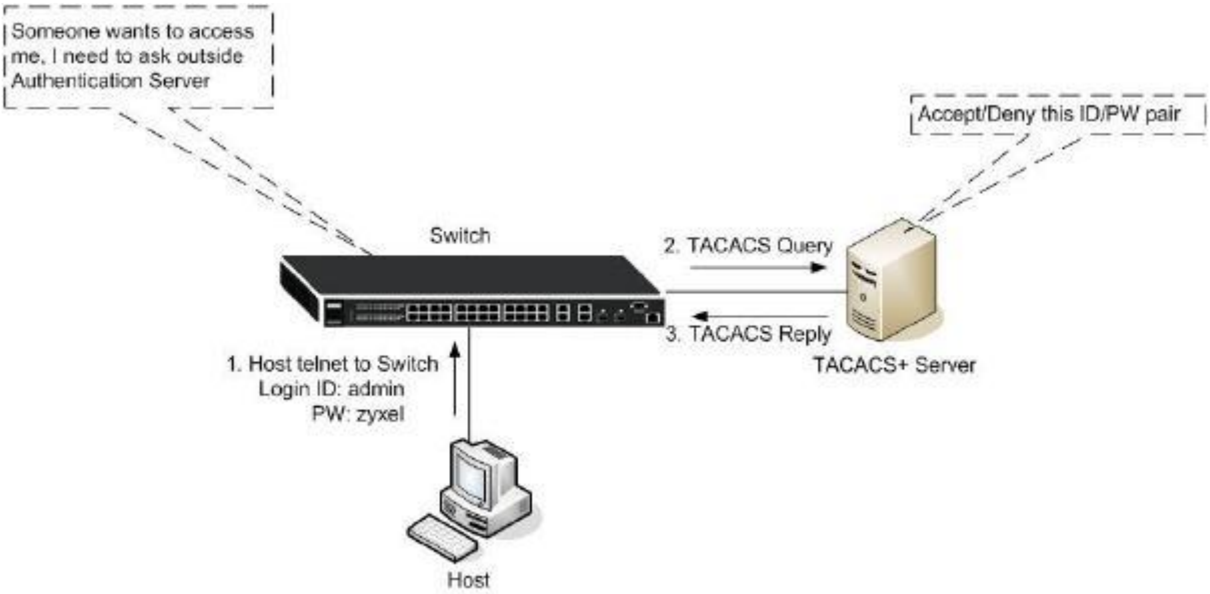
ZyXEL
Unleash Networking Power

Overview

AAA stands for "Authentication, Authorization, and Accounting" which provides access control and to keep track of the activity of users over a network.

Authentication: Identify who is allowed to access the device by.
Authorization: Identify what commands is allowed by what user.
Accounting: Count and trace the used commands and system events.

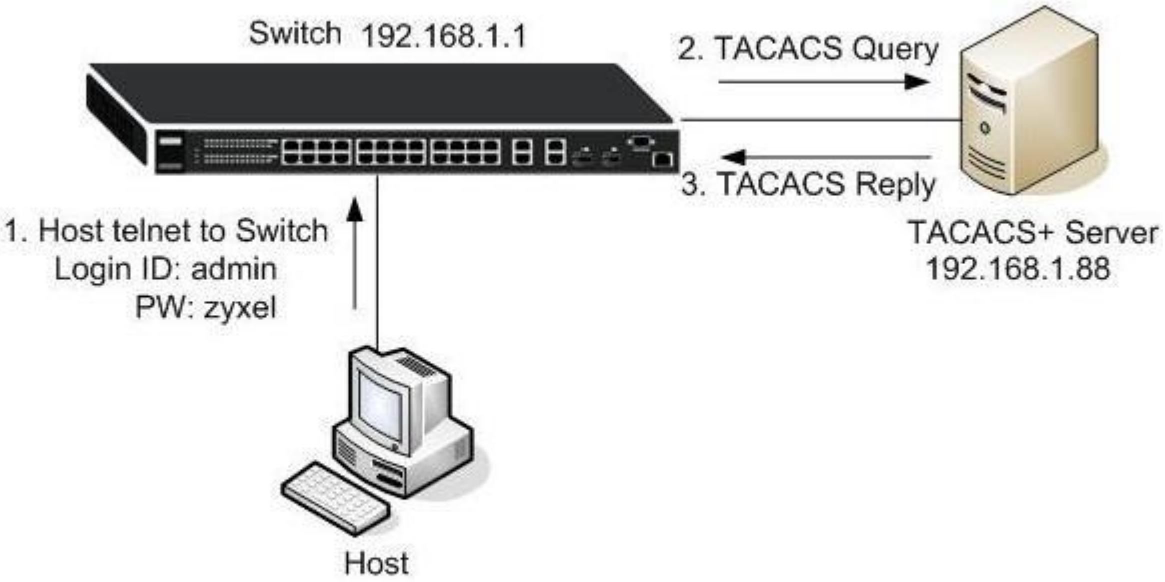
The AAA procedure can be done on local device (if it supported) or on a different outside server. See figure below



Considering this topology, AAA process in the Switch chose TACACS+ as its login method. When a Host want to access this switch via telnet , serial , or web GUI , he needs to send an ID/PW pair to the Switch, then this Switch starts an Authentication procedure (here, via TACACS for example). When the outside Server checks and confirms the ID/PW pair with its database, it will decide to accept or deny this ID/PW pair.

TACACS+ (Terminal Access Controller Access-Control System plus) is an authentication protocol that allows a remote access server to forward a user's logon name and password to an authentication server to determine whether access can be
allowed to a given system.

Scenario



Consider the scenario depicted, according to this topology, the host wants to logon to the switch via serial port. To implement AAA function with TACACS+ on this switch so that the switch can query an outside TACACS+ server for authentication. We need

to build a TACACS+ server and make some configuration on this switch.

Configuration using the Web GUI

1. Connect the MGMT port to a PC or Notebook with the RJ45 Cable.

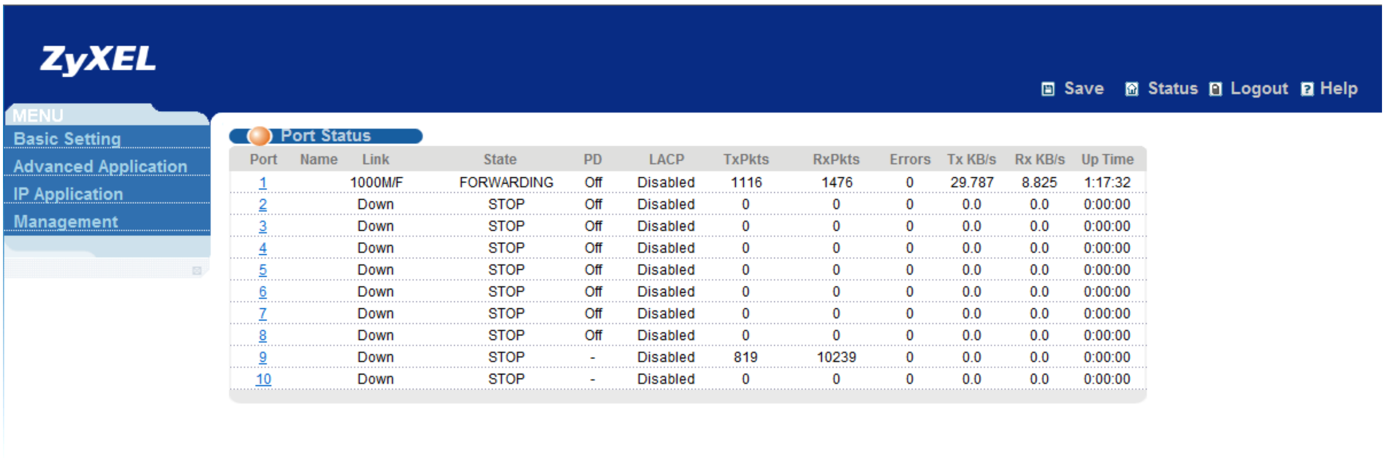
2. By default, the MGMT IP address of the out-band port is 192.168.0.1/24

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".

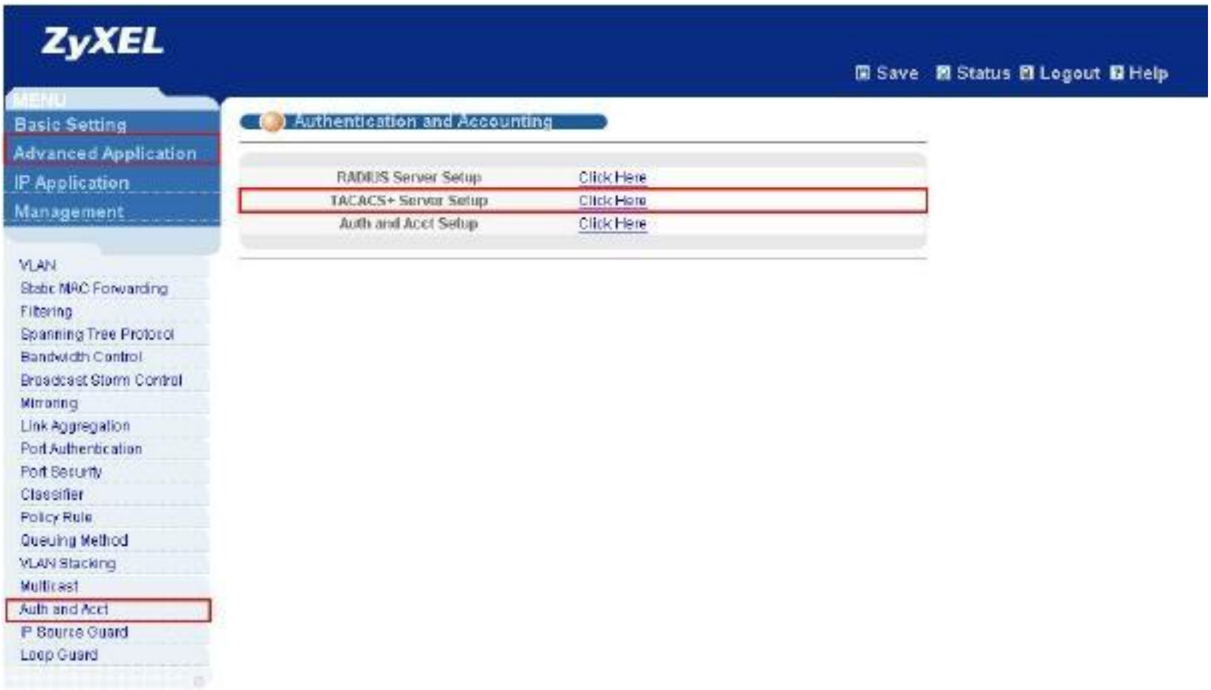
6. After successfully logging in you will see a screen similar to the one below.



Port Status

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

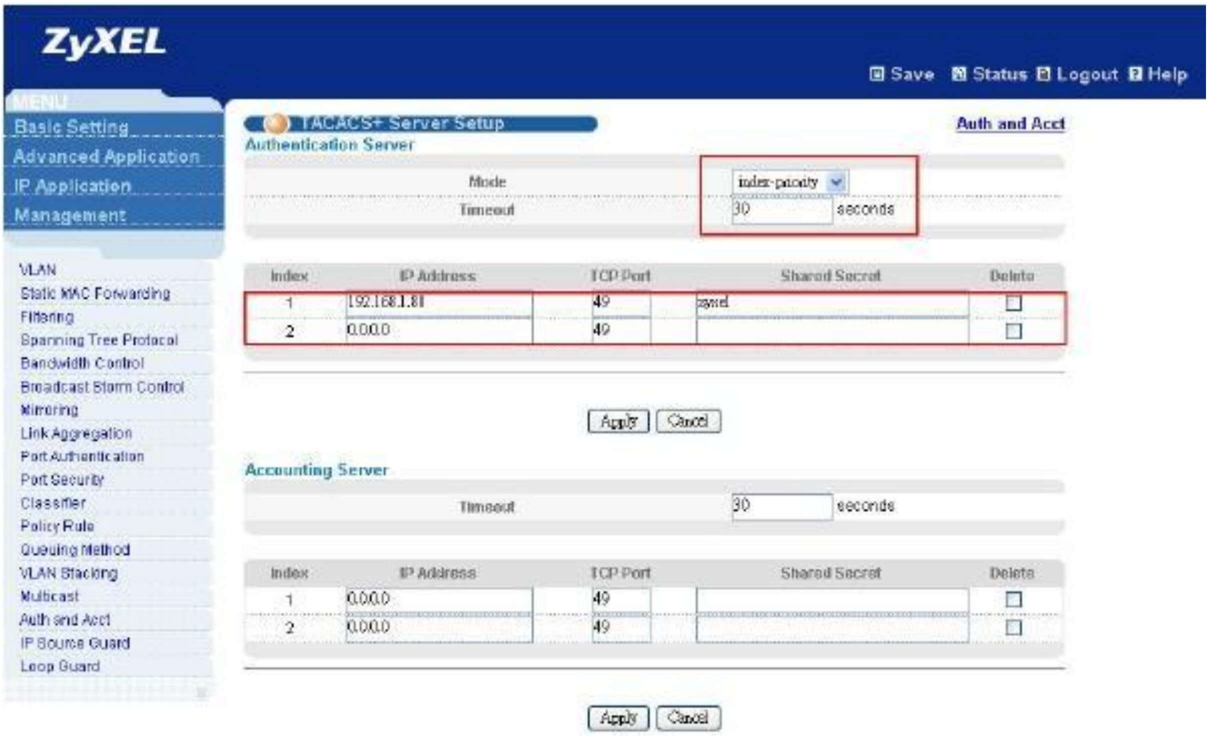
7. Go to the "**TACACS+ Server Setup**" page by clicking "**Advanced Application**" "**Auth and Acct**" "**TACACS+ Server Setup**"



Authentication and Accounting

RADIUS Server Setup	Click Here
TACACS+ Server Setup	Click Here
Auth and Acct Setup	Click Here

8. Identify the TACACS+ Authentication Server's IP address, shared secret, server mode, and timeout timer. Click "**Apply**"



TACACS+ Server Setup

Authentication Server

Mode: index-priority

Timeout: 30 seconds

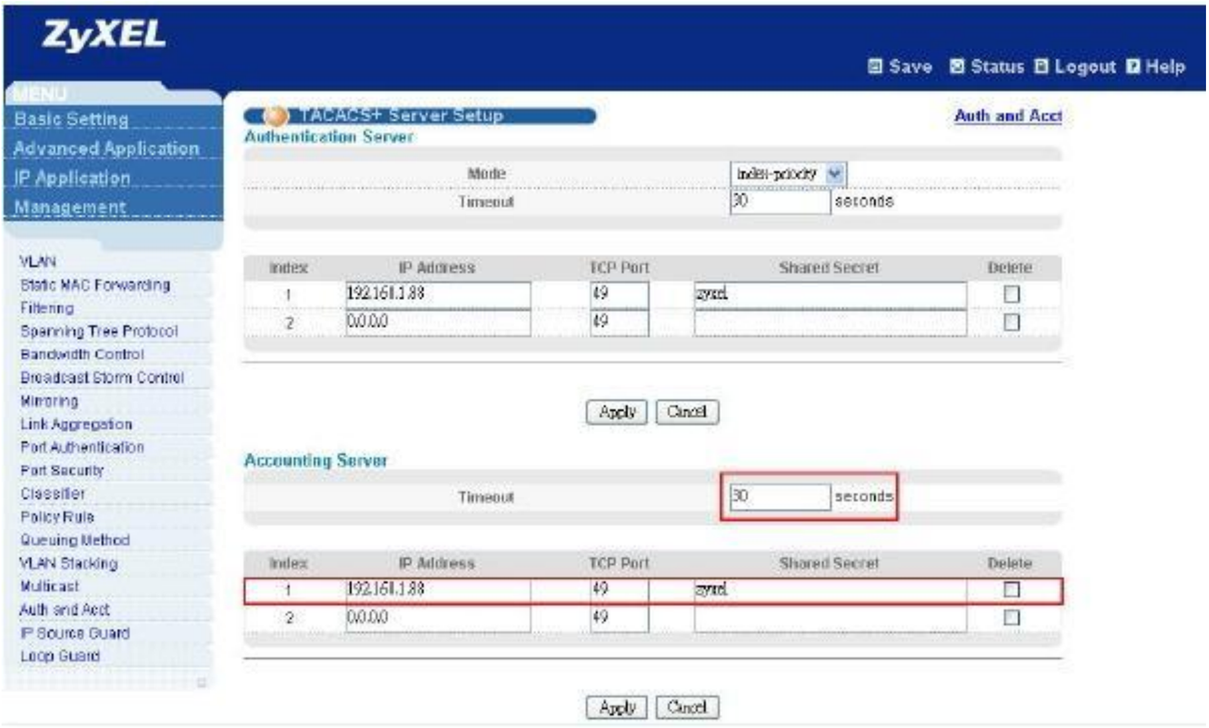
Index	IP Address	TCP Port	Shared Secret	Delete
1	192.168.1.81	49	zyxel	□
2	0.0.0.0	49		□

Accounting Server

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		□
2	0.0.0.0	49		□

9. Identify the TACACS+ Accounting Server's IP address, shared secret and the timeout timer. Click "**Apply**"



TACACS+ Server Setup

Authentication Server

Mode	index-priority
Timeout	30 seconds

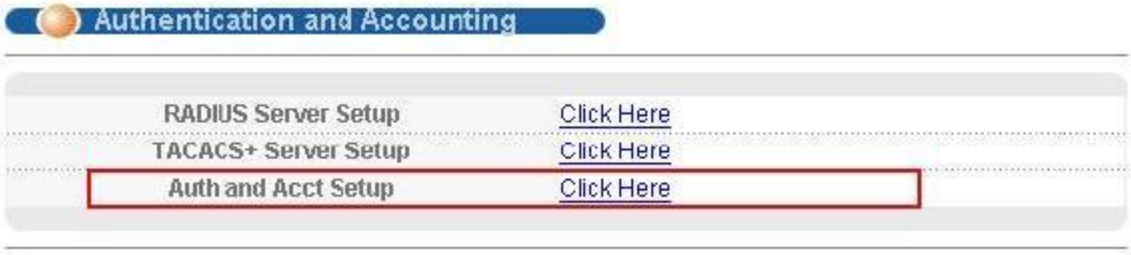
Index	IP Address	TCP Port	Shared Secret	Delete
1	192.161.1.88	49	zyxel	□
2	0.0.0.0	49		□

Accounting Server

Timeout	30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	192.161.1.88	49	zyxel	□
2	0.0.0.0	49		□

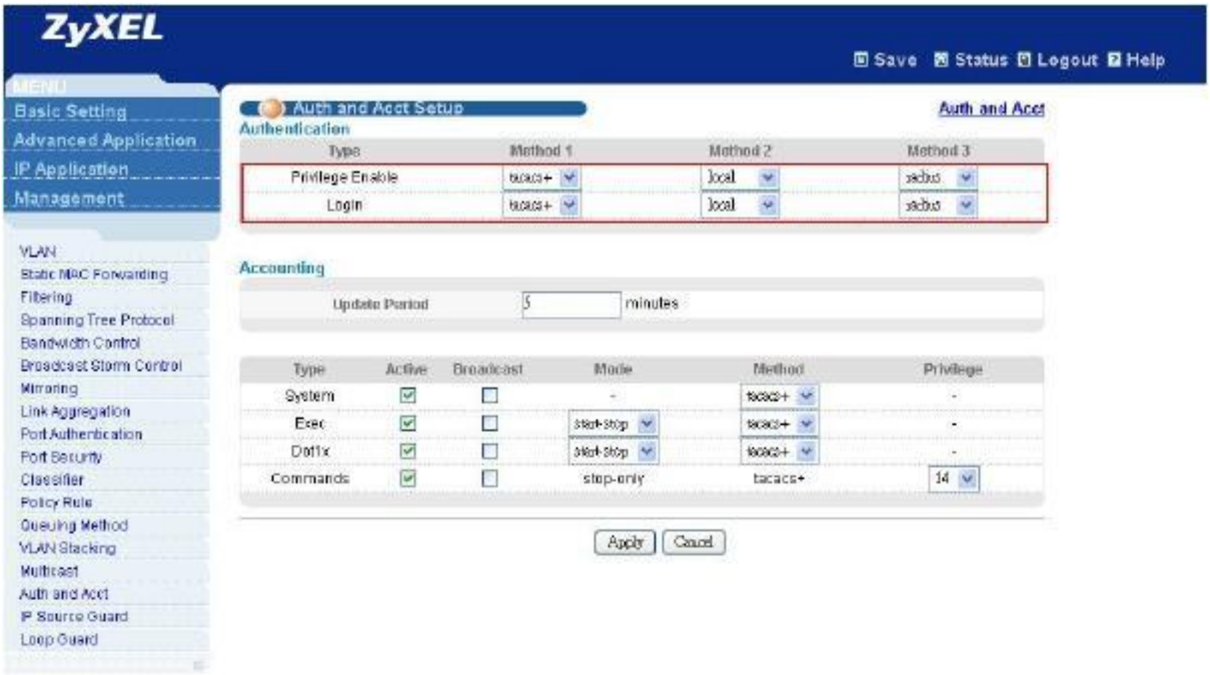
10. Go to “**Auth and Acct Setup**” page.



Authentication and Accounting

RADIUS Server Setup	Click Here
TACACS+ Server Setup	Click Here
Auth and Acct Setup	Click Here

11. Configure the Authentication method sequence. Here we choose tacacs+ as our first authentication method, local as the second, and radius as the third. If method 1 failed, the device will use method 2 and so on. You can also leave the method bar
blank.



Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	tacacs+	local	radius
Login	tacacs+	local	radius

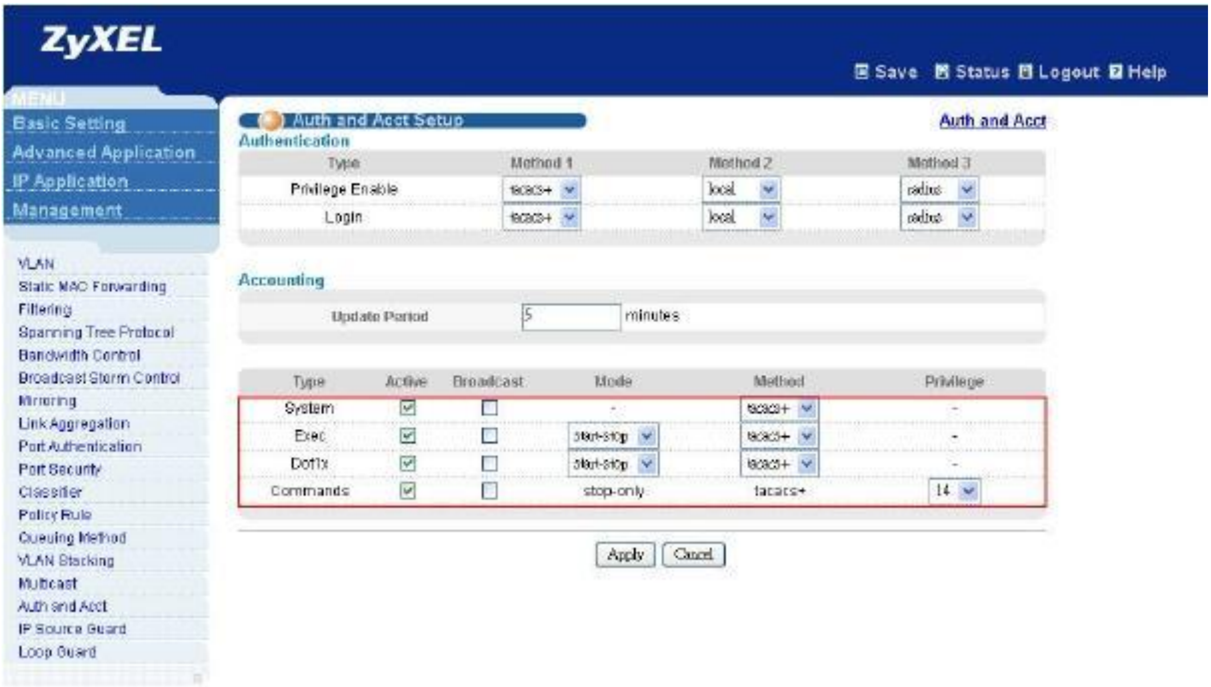
Accounting

Update Period 5 minutes

Type	Active	Broadcast	Mode	Method	Privilege
System	☑	□	-	tacacs+	-
Exec	☑	□	start-stop	tacacs+	-
Dot1x	☑	□	start-stop	tacacs+	-
Commands	☑	□	stop-only	tacacs+	14

12. Choose what kind of events will trigger the Accounting, when will it send accounting info to the Server (when start and stop the type of service or only when stop the service), and what kind of servers is using (here we use TACACS+ in stead).

Click “**Apply**”



Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	tacacs+	local	radius
Login	tacacs+	local	radius

Accounting

Update Period 5 minutes

Type	Active	Broadcast	Mode	Method	Privilege
System	☑	□	-	tacacs+	-
Exec	☑	□	start-stop	tacacs+	-
Dot1x	☑	□	start-stop	tacacs+	-
Commands	☑	□	stop-only	tacacs+	14

Configuration using the CLI

Configure the aaa authentication order:

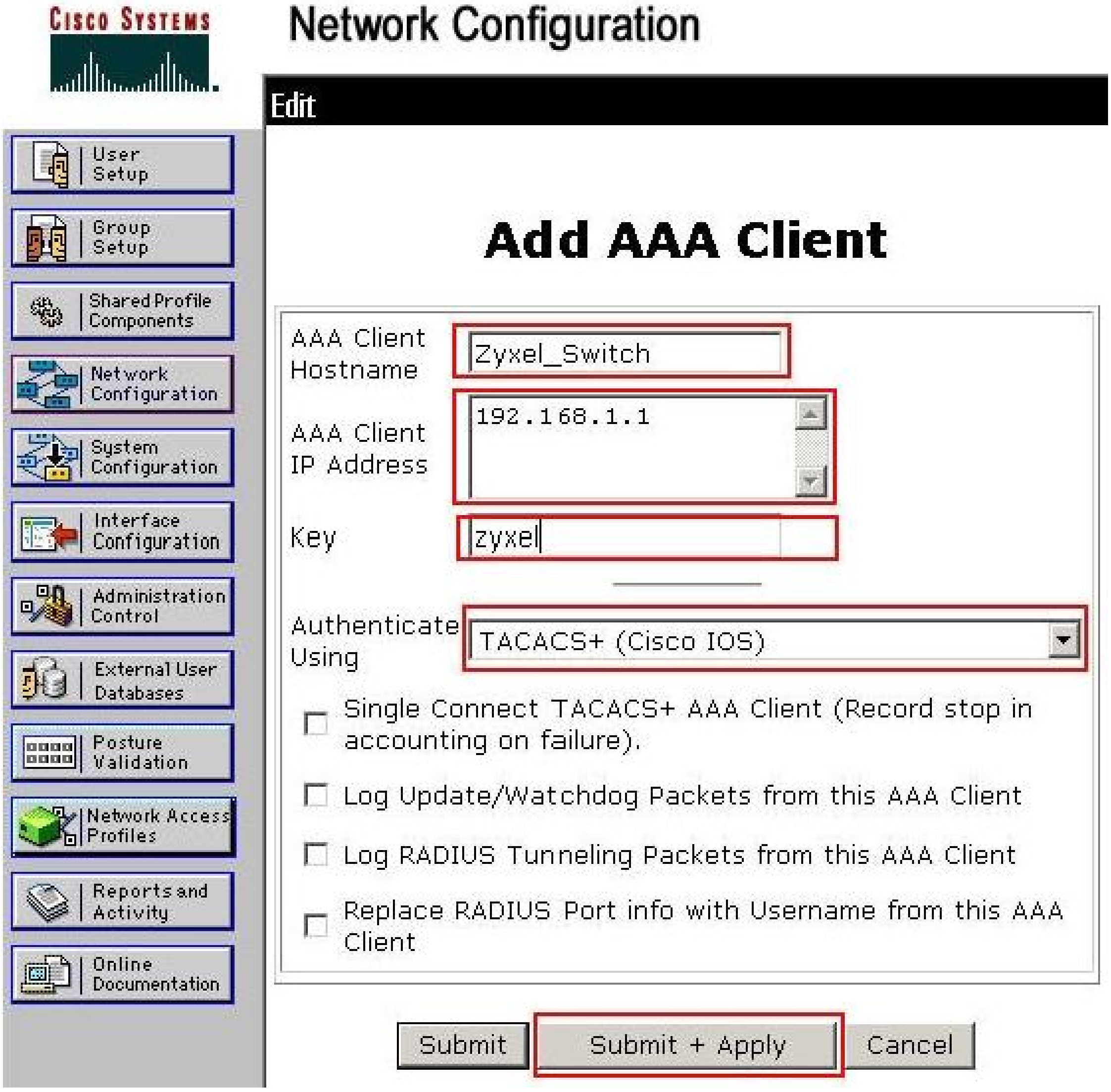
```
Switch#conf
Switch(config)#aaa authentication enable <method 1> <method 2> <method
3> Switch(config)#aaa authentication login <method 1> <method 2> <method
3>
```

The running-config:

```
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
ip address 192.168.0.1 255.255.255.0 tacacs-
server host 1 192.168.1.88 key zyxel tacacs-
accounting host 1 192.168.1.88 key zyxel aaa
accounting update periodic 5
aaa accounting system tacacs+
aaa accounting exec start-stop tacacs+
aaa accounting dot1x start-stop tacacs+
aaa accounting commands 14 stop-only tacacs+
```

TACACS+ Server configuration (Using Cisco ACS)

1. Create the AAA Client (the Zyxel switch for example) hostname, IP address, shared key, Authentication method. Click "**Submit + Apply**"



Add AAA Client

AAA Client Hostname: Zyxel_Switch

AAA Client IP Address: 192.168.1.1

Key: zyxel

Authenticate Using: TACACS+ (Cisco IOS)

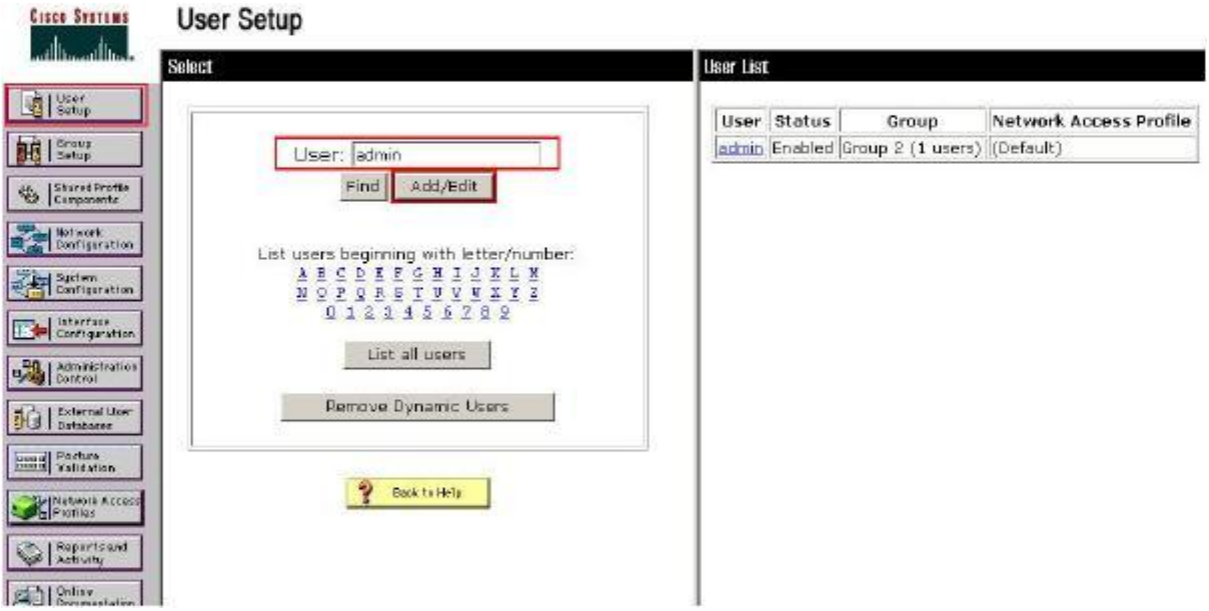
□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

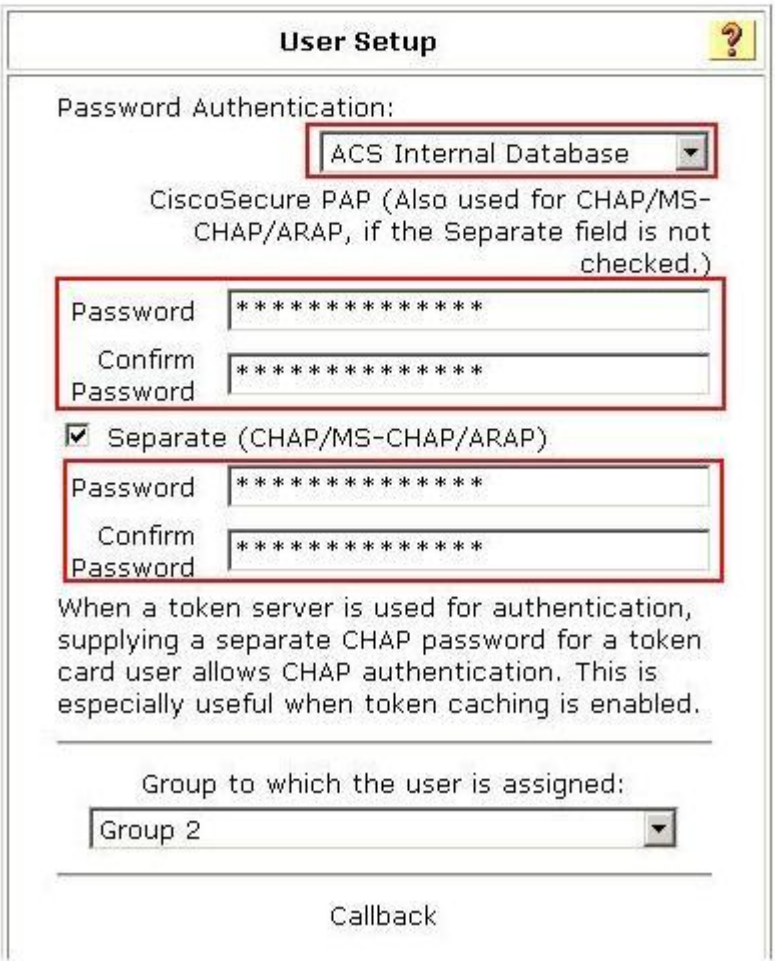
2. Create an account for logging in. Here we create an "admin" account for logging in.



User: admin

User	Status	Group	Network Access Profile
admin	Enabled	Group 2 (1 users)	(Default)

3. After creating the account, we have to set up what database ACS will search for and the user's password.



Password Authentication: ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: *************

Confirm Password: *************

☑ Separate (CHAP/MS-CHAP/ARAP)

Password: *************

Confirm Password: *************

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned: Group 2

4. After creating a new account, you can do login authentication via this outside TACACS+ Server.

5. When accounts are created, ACS will automatically do accounting when users logging in.