



## **Lab 7.2.8 Configure 802.1x Port-Based Authentication**

### **Objective**

In this lab, the students will complete the following tasks:

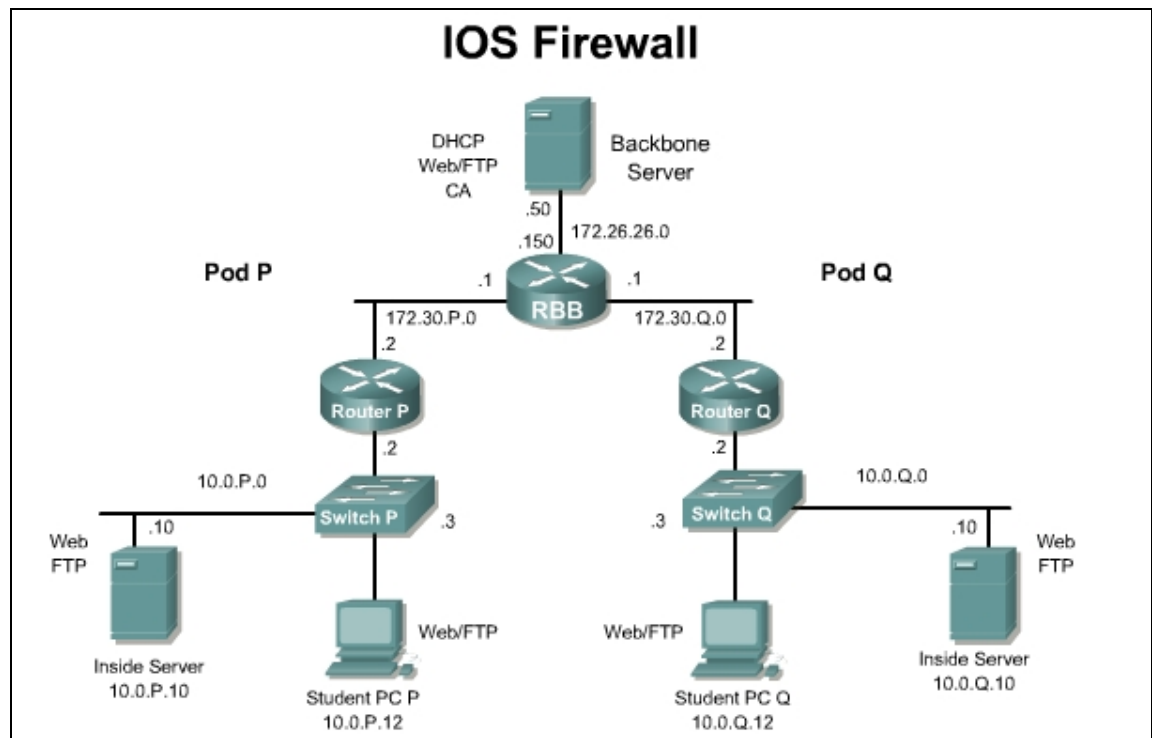
- Enable 802.1x authentication.
- Configure the switch-to-RADIUS server communication.
- Enable periodic re-authentication.
- Manually re-authenticate a client connected to a port.
- Change the quiet period.
- Change the switch-to-client retransmission time.
- Set the switch-to-client frame-retransmission number.
- Enable multiple hosts.
- Reset the 802.1x configuration to the default values.
- Display 802.1x statistics and status.

### **Scenario**

Now that the Cisco Secure ACS has been configured with the parameters that enable it to perform as an 802.1x authentication server, the XYZ company network is ready for 802.1x switch configuration. The PCs that are permitted to be on the network will also need to be configured to act as 802.1x clients. In this activity, students will configure 802.1x port-based authentication on a Catalyst 2950 switch.

## Topology

This figure illustrates the lab network environment.



## Preparation

Begin with the standard lab topology and verify the starting configuration on the pod switch. Access the pod switch console port using the terminal emulator on the Windows 2000 server. If desired, save the switch configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

## Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- A second PC to be used as an 802.1x client

## Additional materials

Further information about the objectives covered in this lab can be found at,

[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_configuration\\_guide\\_chapter09186a00800d84b9.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00800d84b9.html)

<http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>

## Command List

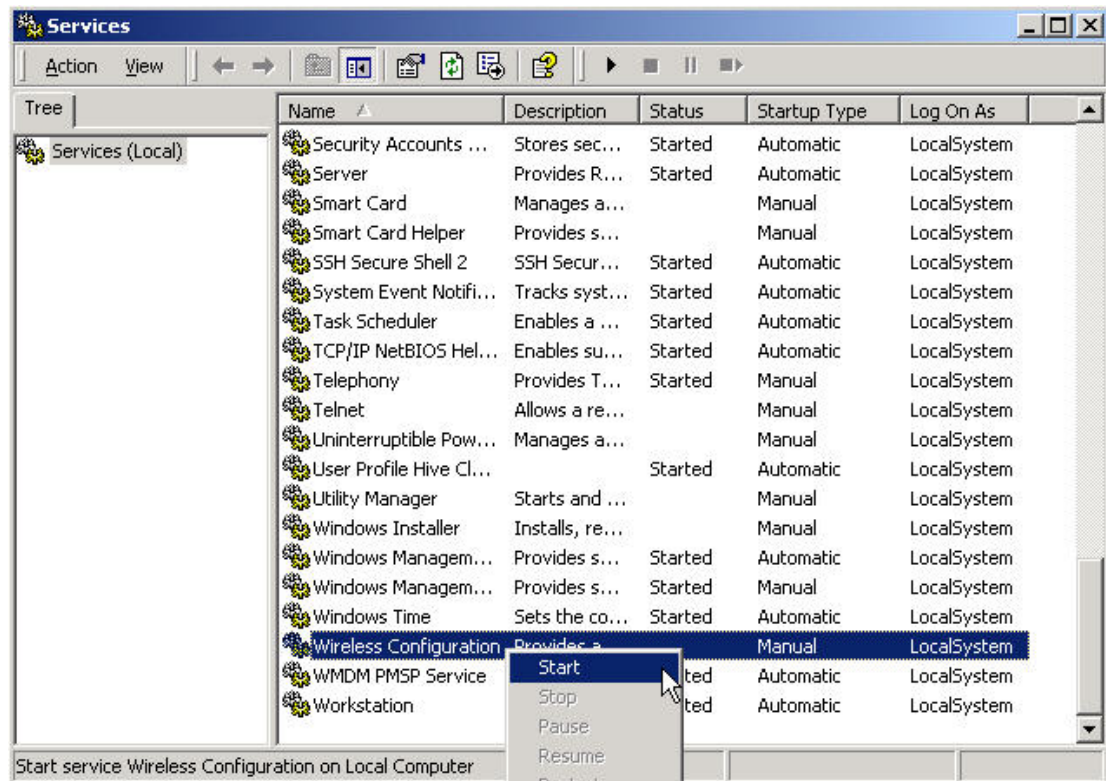
In this lab exercise, the following switch commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

## Switch Commands

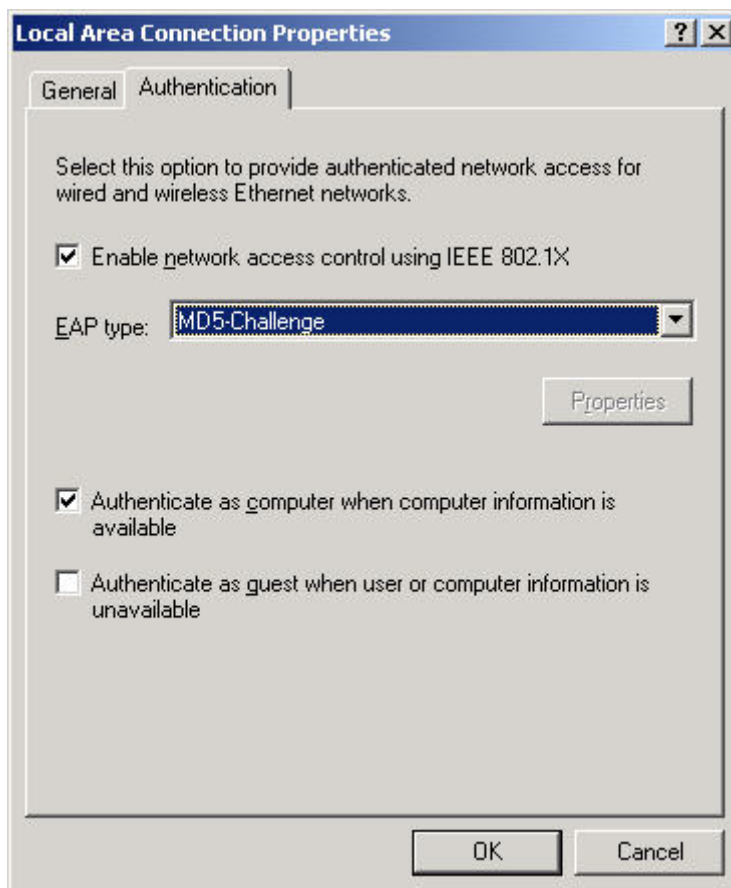
Command	Description
<b>aaa authentication dot1x</b> {default / listname} method1 [method2...]	To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x, use the <b>aaa authentication dot1x</b> command in global configuration mode. To disable authentication, use the <b>no</b> form of this command
<b>aaa new-model</b>	To enable the AAA access control model, issue the <b>aaa new-model</b> command in global configuration mode. To disable the AAA access control model, use the <b>no</b> form of this command.
<b>dot1x default</b>	To reset the global 802.1x parameters to their default values, use the <b>dot1x default</b> command in global configuration mode.
<b>dot1x max-req</b> number-of-retries	To set the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the <b>dot1x max-req</b> command in interface configuration or global configuration mode. To disable the number of times that were set, use the <b>no</b> form of this command.
<b>dot1x multiple-hosts</b>	To allow multiple hosts (clients) on an 802.1x-authorized port that has the <b>dot1x port-control</b> interface configuration command set to <b>auto</b> , use the <b>dot1x multiple-hosts</b> command in interface configuration mode. To return to the default setting, use the <b>no</b> form of this command.
<b>dot1x port-control</b> {auto   force-authorized   force-unauthorized}	To set an 802.1x port control value, use the <b>dot1x port-control</b> command in interface configuration mode. To disable the port-control value, use the <b>no</b> form of this command.
<b>dot1x re-authenticate</b> interface-type interface-number	To enable periodic reauthentication of the client PCs on the 802.1x interface, use the <b>dot1x reauthentication</b> command in interface configuration mode. To disable periodic reauthentication, use the <b>no</b> form of this command.
<b>dot1x timeout</b> {auth-period seconds   held-period seconds   quiet-period seconds   ratelimit-period seconds   reauth-period seconds   server-timeout seconds   start-period seconds   tx-period seconds}	To set retry timeouts, use the <b>dot1x timeout</b> command in interface configuration mode. To remove the retry timeouts, use the <b>no</b> form of this command.
<b>radius-server host</b> {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname   ip-address}]	To specify a RADIUS server host, use the <b>radius-server host</b> command in global configuration mode. To delete the specified RADIUS host, use the <b>no</b> form of this command.
<b>show dot1x</b> [interface interface-name [details]]	To show details for an identity profile, use the <b>show dot1x</b> command in privileged EXEC mode.
<b>show dot1x</b> [interface interface-name [details]]	To show details for an identity profile, use the <b>show dot1x</b> command in privileged EXEC mode.

## Step 1 Prepare a PC for 802.1x Authentication

- This lab requires an additional PC that must be capable of using 802.1x authentication. If the PC already has this capability, proceed to substep d.
- To enable the 802.1x client choose **Start > Settings > Control Panel > Administrative Tools > Services**. Right click on the **Wireless Configuration** icon and select **Start** from the menu.



- If necessary, an 802.1x client for Microsoft Windows can be downloaded from the following URL:  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>
- On the PC, under the **Authentication** tab of **Local Area Network Connection Properties** check the following:
  - Enable network access control using IEEE 802.1X box is checked.
  - EAP type = MD5-Challenge



## Step 2 Enable 802.1x Authentication on the Switch

- a. Enable AAA on the pod switch.

```
SwitchP(config)# aaa new-model
```

Create an 802.1x authentication method list. To create a default list that is used when a named list is not specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. The **group radius** keyword is used to indicate the list of all RADIUS servers that is configured on the switch will be used for authentication.

```
SwitchP(config)# aaa authentication dot1x default group radius local
```

- b. Configure AAA accounting.

```
SwitchP(config)# aaa accounting network default start-stop group radius
```

```
SwitchP(config)# aaa accounting connection default start-stop group radius
```

- c. Enable dot1x system-auth-control.

```
SwitchP(config)# dot1x system-auth-control
```

- d. Enter interface configuration mode, and specify the interface to be enabled for 802.1x authentication.

```
SwitchP(config)# interface fa0/12
```

- e. Enable 802.1x authentication on the interface.

```
SwitchP(config-if)# dot1x port-control auto
```

- f. Return to privileged EXEC mode.

```
Switch(config-if)# end
```

- g. Verify the entries. Check the Status column in the 802.1x Port Summary section of the display. An enabled status means the port-control value is set either to **auto** or to **force-unauthorized**.

```
SwitchP# show dot1x

Sysauthcontrol              = Enabled
Supplicant Allowed In Guest Vlan = Disabled
Dot1x Protocol Version      = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

1. What command enables system-authorization?
- 

### Step 3 Configure the Switch-to-RADIUS Server Communication

- a. Configure the RADIUS server parameters on the switch.

```
SwitchP(config)# radius-server host 10.0.P.12 auth-port 1812 key  
secretkey
```

---

**Note** If CSACS is not installed on the student PC, use the host address of the PC where CSACS is installed.

---

---

**Note** Port 1812 is the default UDP destination port for RADIUS authentication requests.

---

- b. Return to privileged EXEC mode.

```
SwitchP(config)# end
```

- c. Verify the entries in the configuration.

```
SwitchP# show running-config
```

The following lines should appear in the configuration:

```
!  
radius-server host 10.0.2.12 auth-port 1812 acct-port 1813 key  
secretkey  
radius-server retransmit 3  
!
```

- d. View the current status of the port that has been configured for 802.1x authentication with the **show dot1x all** command.

```
Dot1x Info for interface FastEthernet0/12
```

```
-----  
Supplicant MAC <Not Applicable>  
AuthSM State      = CONNECTING  
BendSM State      = IDLE  
PortStatus        = UNAUTHORIZED  
MaxReq            = 3  
HostMode          = Multi  
Port Control      = Auto  
QuietPeriod       = 90 Seconds  
Re-authentication = Enabled  
ReAuthPeriod      = 4000 Seconds  
ServerTimeout     = 30 Seconds  
SuppTimeout       = 30 Seconds  
TxPeriod          = 45 Seconds  
Guest-Vlan        = 0
```

- e. Connect the second PC to port FastEthernet 12 on the pod switch.
- f. When prompted for authentication, enter the username **aaauser** and the password **aaapass**. Leave the Login Domain blank.



- g. The PC is now authenticated as an 802.1x client. Verify that the port has been authenticated with the **show dot1x interface** command.

```
SwitchP# show dot1x interface fa0/12
Supplicant MAC 0002.557a.4ab8
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

#### Step 4 Enable Periodic Re-authentication

- a. Change to interface configuration mode.

```
SwitchP(config)#int fa0/12
```

- b. Enable periodic re-authentication of the client, which is disabled by default.

```
SwitchP(config-if)# dot1x reauthentication
```

- c. Set the number of seconds between re-authentication attempts. The default is 3600 seconds.

```
SwitchP(config-if)# dot1x timeout reauth-period 4000
```

- d. Return to privileged EXEC mode.

```
SwitchP(config)# end
```

- e. Verify the entries in the configuration.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
-----
Supplicant MAC 0002.557a.4ab8
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Enabled
```



```
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

### Step 5 Manually Re-Authenticate a Client Connected to a Port

- a. Manually re-authenticate the client connected to a port.

```
SwitchP# dot1x re-authenticate interface fa0/12
```

- b. Use the **show dot1x all** command to verify that the client has been re-authenticated.

```
SwitchP# show dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```
-----
Supplicant MAC <Not Applicable>
  AuthSM State      = CONNECTING
  BendSM State      = IDLE
PortStatus          = UNAUTHORIZED
MaxReq              = 2
HostMode            = Single
Port Control        = Auto
QuietPeriod         = 60 Seconds
Re-authentication   = Enabled
ReAuthPeriod        = 4000 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
TxPeriod            = 30 Seconds
Guest-Vlan          = 0
```

### Step 6 Change the Quiet Period

- a. Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535 seconds; the default is 60.

```
SwitchP(config-if)# dot1x timeout quiet-period 90
```

- b. Issue a **show dot1x all** command to verify that the quiet period has been changed.

```
SwitchP# show dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```
Supplicant MAC 0002.557a.4ab8
  AuthSM State      = AUTHENTICATED
  BendSM State      = IDLE
PortStatus          = AUTHORIZED
MaxReq              = 2
```

```

HostMode           = Single
Port Control       = Auto
QuietPeriod        = 90 Seconds
Re-authentication  = Enabled
ReAuthPeriod       = 4000 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
TxPeriod           = 30 Seconds
Guest-Vlan         = 0

```

## Step 7 Change the Switch-to-Client Retransmission Time

- Set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535 seconds; the default is 30.

```
SwitchP(config-if)# dot1x timeout tx-period 45
```

- Issue a **show dot1x all** command to verify the change in the configuration.

```

SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
-----
Supplicant MAC 0002.557a.4ab8
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 45 Seconds
Guest-Vlan        = 0

```

## Step 8 Set the Switch-to-Client Frame-Retransmission Number

- Set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10 and the default is 2.

```
SwitchP(config-if)# dot1x max-req 3
```

- Issue a **show dot1x all** command to verify the change in the configuration.

```

SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12

```

```

-----
Supplicant MAC 0002.557a.4ab8
    AuthSM State      = AUTHENTICATED
    BendSM State      = IDLE
PortStatus           = AUTHORIZED
MaxReq               = 3
HostMode             = Single
Port Control         = Auto
QuietPeriod          = 90 Seconds
Re-authentication    = Enabled
ReAuthPeriod         = 4000 Seconds
ServerTimeout        = 30 Seconds
SuppTimeout          = 30 Seconds
TxPeriod             = 45 Seconds
Guest-Vlan           = 0

```

## Step 9 Enable Multiple Hosts

- a. Enter interface configuration mode, and specify the interface to which multiple hosts are indirectly attached.

```
SwitchP(config)# interface fa0/12
```

- b. Allow multiple hosts (clients) on an 802.1x-authorized port.

```
SwitchP(config-if)# dot1x host-mode multi-host
```

---

**Note**      The **dot1x port-control** interface configuration command must be set to **auto** for the specified interface.

---

- c. Issue a **show dot1x all** command to verify the change to the configuration.

```

SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
-----
Supplicant MAC 0002.557a.4ab8
    AuthSM State      = AUTHENTICATED
    BendSM State      = IDLE
PortStatus           = AUTHORIZED
MaxReq               = 3
HostMode             = Multi
Port Control         = Auto
QuietPeriod          = 90 Seconds
Re-authentication    = Enabled
ReAuthPeriod         = 4000 Seconds
ServerTimeout        = 30 Seconds

```

```
SuppTimeout      = 30 Seconds
TxPeriod         = 45 Seconds
Guest-Vlan       = 0
```

## Step 10 Display 802.1x Statistics and Status

- a. Use the **show dot1x statistics interface** command to display 802.1x statistics for a specific interface.

```
SwitchP# show dot1x statistics interface Fa0/12
PortStatistics Parameters for Dot1x
-----
TxReqId = 8      TxReq = 10      TxTotal = 15
RxStart = 0      RxLogoff = 0    RxRespId = 2    RxResp = 4
RxInvalid = 0    RxLenErr = 0    RxTotal= 6
RxVersion = 1    LastRxSrcMac 0002.557a.4ab8
```

## Sample configuration

A sample configuration is shown below:

```
Switch1#show run
Building configuration...

Current configuration : 2404 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch1
!
aaa new-model
aaa authentication dot1x default group radius local
aaa accounting connection default start-stop group radius
enable secret 5 $1$4vWf$S3sXATwAalDNolsolkYQA0
!
ip subnet-zero
!
no ip domain-lookup
ip ssh time-out 120
ip ssh authentication-retries 3
!
```

```
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
!
!
!
interface FastEthernet0/1
    switchport access vlan 301
!
interface FastEthernet0/2
    switchport access vlan 301
!
interface FastEthernet0/3
    switchport mode access
!
interface FastEthernet0/4
    switchport mode access
!
interface FastEthernet0/5
    switchport mode access
!
interface FastEthernet0/6
    switchport mode access
!
interface FastEthernet0/7
    switchport mode access
!
interface FastEthernet0/8
    switchport mode access
!
interface FastEthernet0/9
    switchport mode access
!
interface FastEthernet0/10
    switchport mode access
!
interface FastEthernet0/11
```

```
switchport mode access
!
interface FastEthernet0/12
switchport mode access
dot1x port-control auto
dot1x host-mode multi-host
dot1x timeout quiet-period 90
dot1x timeout tx-period 45
dot1x timeout reauth-period 4000
dot1x max-req 3
dot1x reauthentication
spanning-tree portfast
!
interface FastEthernet0/13
switchport mode access
!
interface FastEthernet0/14
switchport mode access
!
interface FastEthernet0/15
switchport mode access
!
interface FastEthernet0/16
switchport mode access
!
interface FastEthernet0/17
switchport mode access
!
interface FastEthernet0/18
switchport mode access
!
interface FastEthernet0/19
switchport mode access
!
interface FastEthernet0/20
switchport mode access
!
interface FastEthernet0/21
switchport mode access
```

```

!
interface FastEthernet0/22
    switchport mode access
!
interface FastEthernet0/23
    switchport mode access
!
interface FastEthernet0/24
    switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
    no ip address
    no ip route-cache
    shutdown
!
interface Vlan301
    ip address 10.0.1.3 255.255.255.0
    no ip route-cache
!
ip http server
radius-server host 10.0.1.12 auth-port 1812 acct-port 1813 key
secretkey
radius-server retransmit 3
!
line con 0
line vty 0 4
    password cisco
line vty 5 15
!
!
end

```