CHAPTER 9

Configuring IEEE 802.1x Port-Based Authentication

IEEE 802.1x port-based authentication prevents unauthorized devices (clients) from gaining access to the network.

The Catalyst 2960 switch command reference and the “RADIUS Commands” section in the Cisco IOS Security Command Reference, Release 12.2, have command syntax and usage information.

Understanding IEEE 802.1x Port-Based Authentication

clients from connecting to a LAN through publicly accessible ports unless they are authenticated. The authentication server authenticates each client connected to a switch port before making available any switch or LAN services.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic passes through the port.

-
- 02.1x Authentication with Guest VLAN, page 9-18
- 802.1x Authentication with Restricted VLAN, page 9-19
- 802.1x Authentication with Inaccessible Authentication Bypass, page 9-20

Note

-
-
- 02.1x Authentication with Wake-on-LAN, page 9-23

Note To use IEEE 802.1x authentication with wake-on-LAN, the switch must be running the LAN base image.

- 802.1x Authentication with MAC Authentication Bypass, page 9-23
- Network Admission Control Layer 2 802.1x Validation, page 9-25

Note To use Network Admission Control, the switch must be running the LAN base image.

- Flexible Authentication Ordering, page 9-25

  Open1x Authentication, page 9-25

  Using Voice Aware 802.1x Security, page 9-26

  802.1x Switch Supplicant with Network Edge Access Topology (NEAT), page 9-26

  802.1x Authentication with Downloadable ACLs and Redirect URLs, page 9-17

  Web Authentication, page 9-27

To use Web Authentication, the switch must be running the LAN base image.

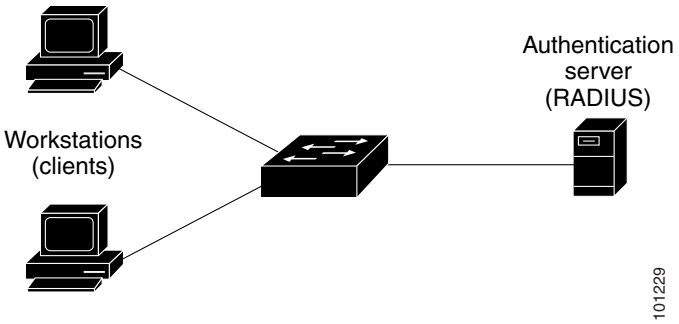
Using IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute, page 9-30

To use IEEE 802.1x authentication with ACLs and the Filter-Id attribute, the switch must be running the LAN base image.

Device Roles

:

Figure 9-1 802.1x Device Roles



Client—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant*

Microsoft Knowledge Base article at this URL:
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

Authentication server

Switch

authenticator

server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

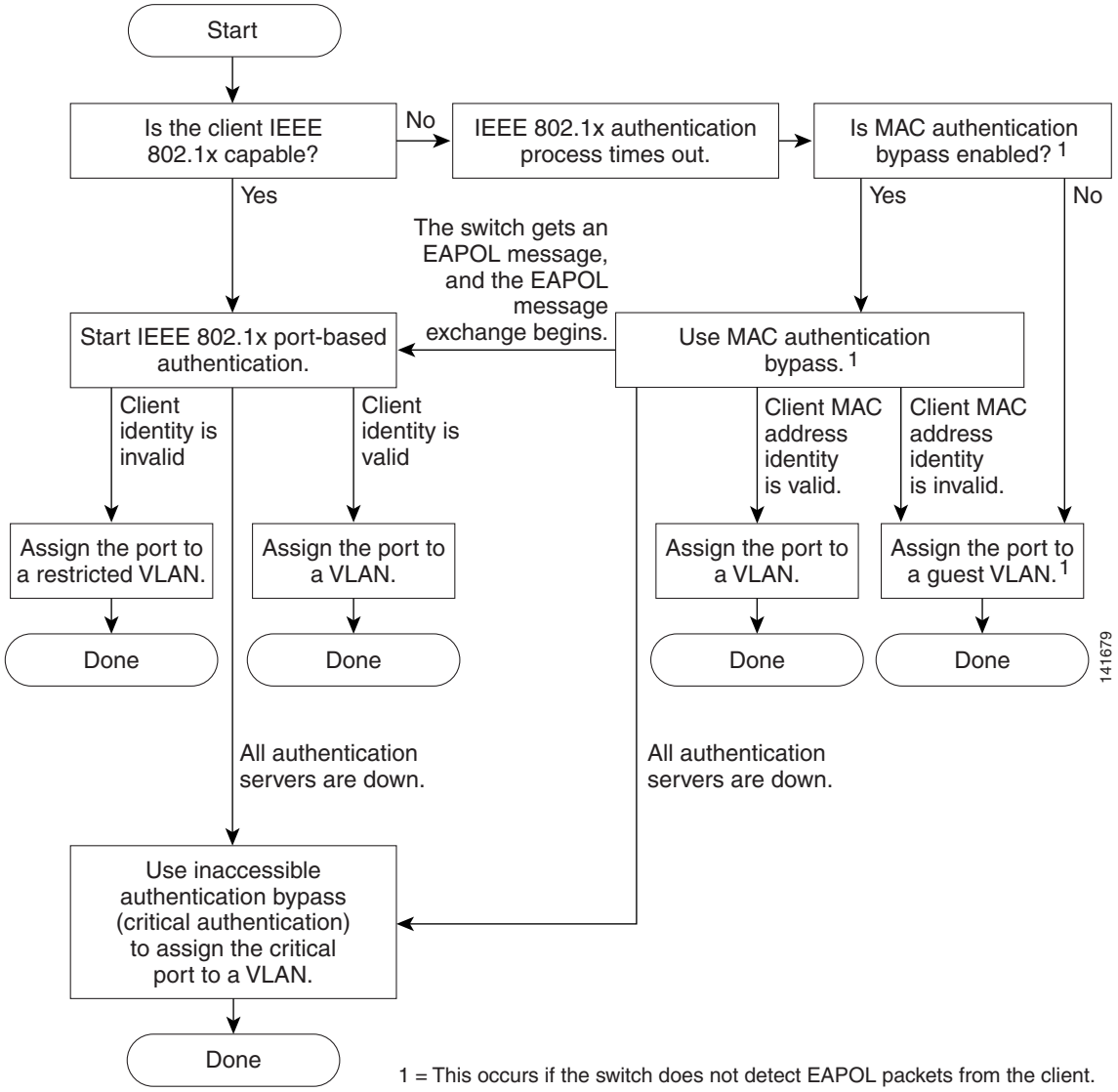
The devices that can act as intermediaries include the Catalyst 3750-E, Catalyst 3560-E, Catalyst 3750, Catalyst 3560, Catalyst 3550, Catalyst 2975, Catalyst 2970, Catalyst 2960, Catalyst 2955, Catalyst 2950, Catalyst 2940 switches, or a wireless access point. These devices must be running software that supports the RADIUS client and 802.1x authentication.

Authentication Process

-
-
-
-

Note

Authentication Flowchart



You can configure the re-authentication timer to use a switch-specific value or to be based on values from the RADIUS server.

After 802.1x authentication using a RADIUS server is configured, the switch uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which re-authentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during re-authentication. The actions are *Initialize* *ReAuthenticate* *Initialize* *DEFAULT* *ReAuthenticate*

dot1x re-authenticate interface *interface-id*

Authentication Initiation and Message Exchange

authentication port-control auto **dot1x port-control auto**

Figure 9-3 Message Exchange

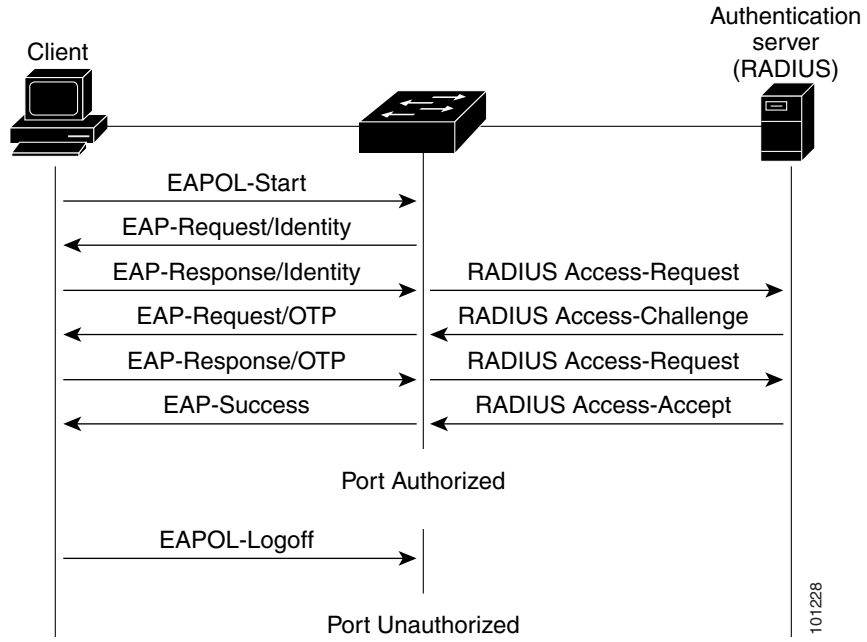
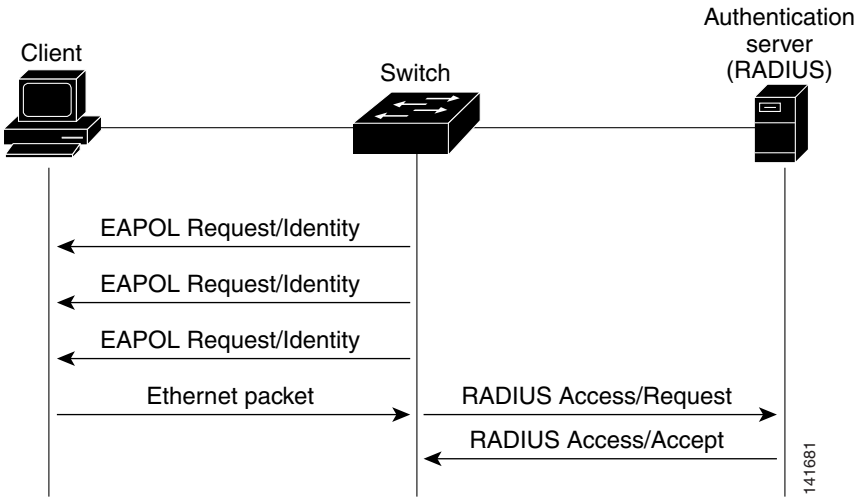


Figure 9-4 Message Exchange During MAC Authentication Bypass



Authentication Manager

-
-
-

Port-Based Authentication Methods

Table 9-1 802.1x Features

Authentication method	Mode			
	Single host	Multiple host	MDA[1]	22
	[3] Redirect URL [2]	VLAN assignment	VLAN assignment Per-user ACL[2] Filter-Id attribute[2] Downloadable ACL[2] Redirect URL[2]	Per-user ACL[2] Filter-Id attribute[2] Downloadable ACL[2] Redirect URL[2]
MAC authentication bypass	VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL[2] Redirect URL[2]	VLAN assignment	VLAN assignment Per-user ACL[2] Filter-Id attribute[2] Downloadable ACL[2] Redirect URL[2]	Per-user ACL[2] Filter-Id attribute[2] Downloadable ACL[2] Redirect URL[2]
Standalone web authentication[4]	Proxy ACL, Filter-Id attribute, downloadable ACL[2]			
NAC Layer 2 IP validation	Filter-Id attribute[2] Downloadable ACL Redirect URL	Filter-Id attribute[2] Downloadable ACL Redirect URL	Filter-Id attribute[2] Downloadable ACL Redirect URL	Filter-Id attribute[2] Downloadable ACL[2] Redirect URL[2]
Web authentication as fallback method[4]	Proxy ACL Filter-Id attribute[2] Downloadable ACL[2]	Proxy ACL Filter-Id attribute[2] Downloadable ACL[2]	Proxy ACL Filter-Id attribute[2] Downloadable ACL[2]	Proxy ACL[2] Filter-Id attribute[2] Downloadable ACL[2]

1. MDA = Multidomain authentication.
2. Also referred to as *multiauth*
3. Supported in Cisco IOS Release 12.2(50)SE and later.
4. For clients that do not support 802.1x authentication.

Per-User ACLs and Filter-Ids

any

Authentication Manager CLI Commands

authentication host-mode authentication violation authentication timer

dot1x authentication port-control auto
dot1x system-authentication control g

authentication manager

Authentication Manager Commands and Earlier 802.1x Commands

The authentication manager commands in Cisco IOS Release 12.2(50)SE or later	The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier	Description
{both | }	**{ | }**	Enable 802.1x authentication with the wake-on-LAN (WoL) feature, and configure the port control as unidirectional or bidirectional.
	dot1x critical (interface configuration) **dot1x guest-vlan6**	
authentication fallback *fallback-profile*	*fallback-profile*	
	single-host | multi-host | multi-domain	

(continued)

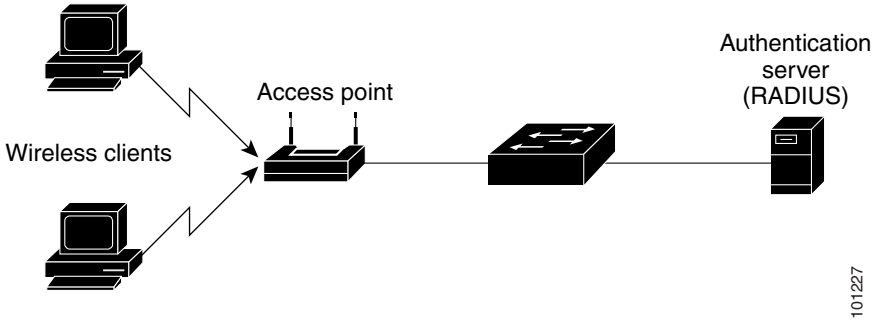
authentication order	**dot1x mac-auth-bypass**	
authentication periodic	**dot1x reauthentication**	
authentication port-control auto force-authorized orce-un authorized	**dot1x port-control {auto | force-authorized | force-unauthorized}**	
authentication timer	**dot1x timeout**	
authentication violation protect restrict shutdown	**dot1x violation-mode shutdown restrict protect**	
show authentication	**show dot1x**	

orts in Authorized and Unauthorized States

- **force-authorized**
- **force-unauthorized**

802.1x Host Mode

Figure 9-5 Multiple Host Mode Example



ultidomain Authentication

Note

-
-
-

Note

-

```
device-traffic-class=voice
```

802.1x Multiple Authentication Mode

Note

Note

802.1x Accounting

-
-
-
-

•

802.1x Accounting Attribute-Value Pairs

- START–sent when a new user session starts
- INTERIM–sent during an existing session for updates
- STOP–sent when a session terminates

Table 9-3 lists the AV pairs and when they are sent are sent by the switch:

Accounting AV Pairs

Attribute Number	AV Pair Name	START	INTERIM	STOP
			[1]	Sometimes[1]
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Always	Always
Attribute[43]	Acct-Output-Octets	Never	Always	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Always	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

1. The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

You can view the AV pairs that are being sent by the switch by entering the privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference, Release 12.2*

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800872ce.html

For more information about AV pairs, see RFC 3580, "802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines."

02.1x Readiness Check

Note

802.1x Authentication with VLAN Assignment

-
-
-
-
-
-
  -
  -

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Attribute [64] must contain the value *VLAN* *802*
VLAN name *VLAN ID*

dACL

Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL

-
-

Note

Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs

downloadable ACLs on the Cisco Secure ACS with the #ACL#-IP-name-number attribute.

- The is the ACL name.
- The is the version number (for example, 3f783768).

If a downloadable ACL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host-access-policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL that is configured on the switch port. However, if the switch receives an host access policy from the Cisco Secure ACS but the default ACL is not configured, the authorization failure is declared.

For configuration details, see the """Authentication Manager" section on page 9-8 and the "Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs" section on page 9-57.

802.1x Authentication with Guest VLAN

-
-

Note

02.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on 802.1x ports in single-host or multiple-hosts mode.

You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on trunk ports; it is supported only on access ports.

The switch supports *MAC authentication bypass*

authentication failed VLAN

EAP failure

link dow *EAP logoff*

link down *EAP logoff*

02.1x Authentication with Inaccessible Authentication Bypass

Note

-
-
-
-
-
-
-
-
-

802.1x Authentication with Voice VLAN Ports

-
-

Note

802.1x Authentication with Port Security

-

-

-
-
-
-

802.1x Authentication with Wake-on-LAN

Note

Note

802.1x Authentication with MAC Authentication Bypass

-
-
-
-
-
-

Network Admission Control Layer 2 802.1x Validation

Note

-
-
-
-
-

Network Admission Control Software Configuration Guide

Flexible Authentication Ordering

Open1x Authentication

-
-

-
-

Using Voice Aware 802.1x Security

Note

802.1x Switch Supplicant with Network Edge Access Topology (NEAT)

-

Note

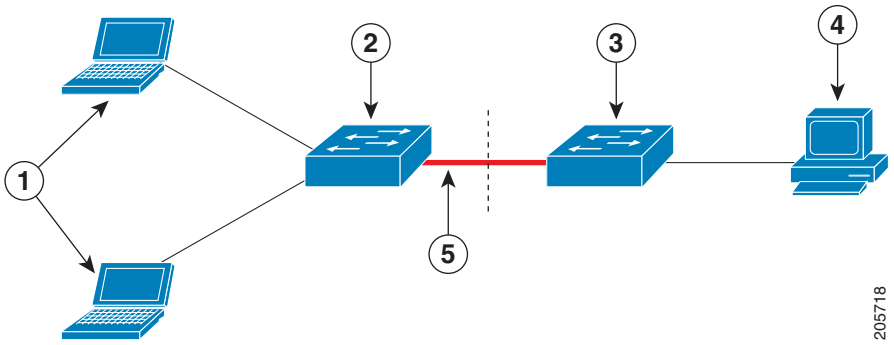
-

-

device-traffic-class=switch

group *user*

Figure 9-6 Authenticator and Supplicant Switch using CISP



3		**4**	
5			

priv-lvl=15 *15*

ip:inacl

proxyacl source any
any

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

proxyacl

Web Authentication with Automatic MAC Check

Note

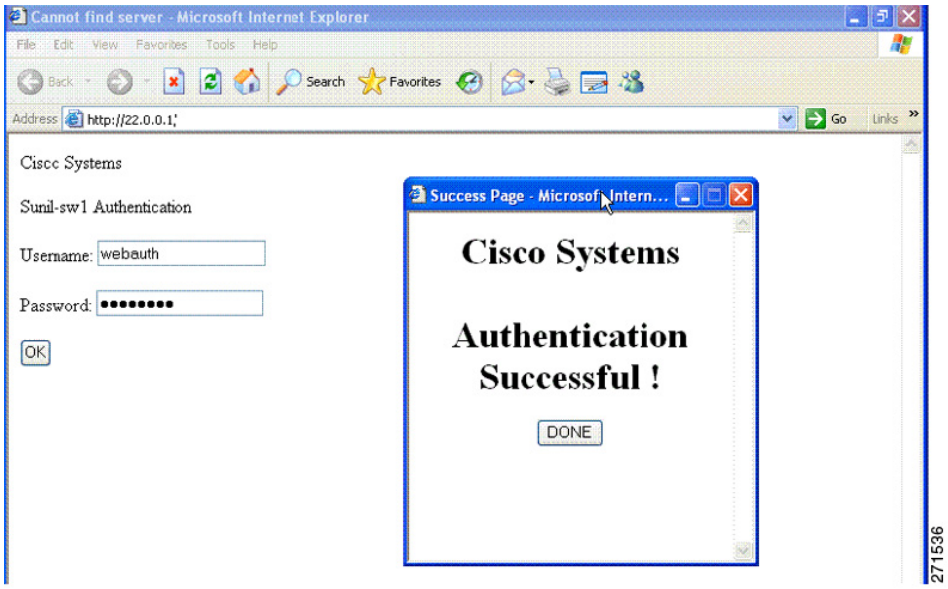
Local Web Authentication Banner

Note

-
-
-

admission auth-proxy-banner http

Figure 9-7 Authentication Successful" Banner



admission auth-proxy-banner http

admission auth-proxy-banner http

Figure 9-8 Customized Web Banner

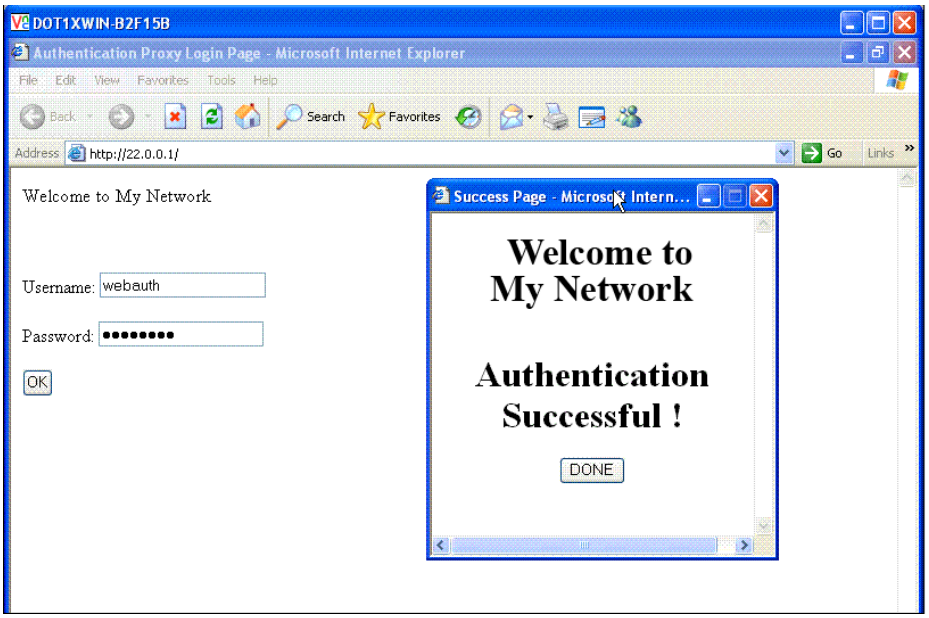
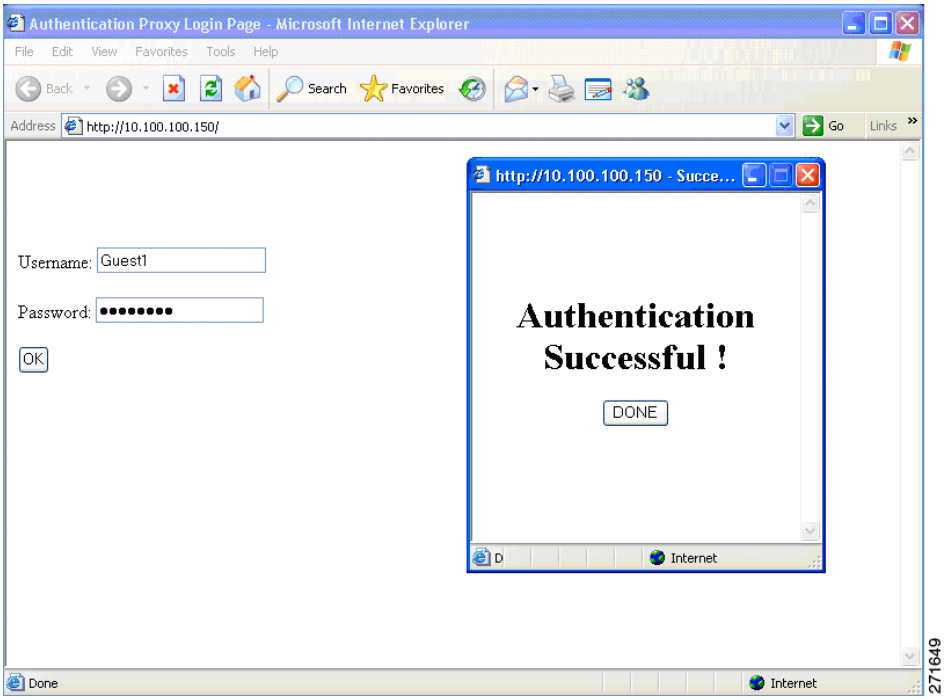


Figure 9-9 Login Screen With No Banner



Configuring 802.1x Authentication

Default 802.1x Authentication Configuration

Feature	Default Setting
• • •	• • •

Feature	Default Setting

802.1x Authentication Configuration Guidelines

-
-
-
-

802.1x Authentication

-
-
-
-

-

VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

-

-

-

-

dot1x timeout quiet-period)
authentication timer reauthentication dot1x timeout tx-period)

-

-

MAC Authentication Bypass

-
-
-
-
-

Maximum Number of Allowed Devices Per Port

-
-
-

Configuring 802.1x Readiness Check

-
-
-

Step 1		**Note**
Step 1		
Step 2		
Step 3		
Step 4		

```
switch# dot1x test eapol-capable interface gigabitethernet0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/13 is EAPOL
capable
```

-
- vlan

Step 5	
Step 6	
Step 7	
Step 8	

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

```
clear errdisable interface gigabitethernet0/2 vlan
```

•

	Command	Purpose
Step 1		
Step 2		
Step 3		Note
Step 4		
Step 5		
Step 6		• • •
Step 7		
Step 8		
Step 9		

Configuring 802.1x Authentication

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

Step 7

Step 8

	Command	Purpose
Step 1		
Step 2		
Step 3		**Note**
Step 4		
Step 5		
Step 6		
Step 7		
Step 8		
Step 9		
Step 10		
Step 11		
Step 12		
Step 13		

Configuring the Switch-to-RADIUS-Server Communication

rad123

```
radius-server host 172.120.39.46 auth-port 1612 key rad123
```


```
interface gigabitethernet0/1
   dot1x port-control auto
   dot1x host-mode multi-host
   end
```

```
interface gigabitethernet0/1
   dot1x port-control auto
   dot1x host-mode multi-domain
   switchport voice vlan 101
   end
```



```
dot1x reauthentication
dot1x timeout reauth-period 4000
```

```
dot1x re-authenticate interface gigabitethernet0/1
```

Changing the Quiet Period

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

```
dot1x timeout quiet-period 30
```

Changing the Switch-to-Client Retransmission Time

Note

	Command	Purpose
Step 1		
Step 2		

	Command	Purpose
Step 3		
Step 4		
Step 5		
Step 6		

```
dot1x timeout tx-period 60
```

Setting the Switch-to-Client Frame-Retransmission Number

Note

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

```
dot1x max-req 5
```

Setting the Re-Authentication Number

Note


```
dot1x max-reauth-req 4
```

Configuring 802.1x Accounting

```
Accounting message %s for session %s failed to receive Accounting Response.
```

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```


```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```


```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x guest-vlan 2
```

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```


```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x auth-fail vlan 2
```



```
Switch(config-if)# dot1x auth-fail max-attempts 2
```

[acct-port auth-port test username idle-time ignore-acct-port ignore-auth-port key	**acct-port** *udp-port*— *udp-port*— *name* *time*— — — *string*— **0** **7**
dot1x critical eapol recovery delay	**eapol** **recovery delay**

interface	
dot1x critical recovery action reinitialize vlan	**recovery action reinitialize** **vlan**
end	
show authentication interface **show dot1x interface**	
copy running-config startup-config	

no radius-server dead-criteria **no radius-server deadtime** **no radius-server host** **no dot1x critical eapol | recovery delay** **no dot1x critical**

```
dot1x critical recovery action reinitialize
dot1x critical vlan 20
end
```

configure terminal	
interface	

authentication control-direction {both | in} **dot1x control-direction both in**	**both** **in**
end	
show authentication interface **show dot1x interface**	
copy running-config startup-config	

no authentication control-direction **no dot1x control-direction**

```
authentication control-direction both
```

```
dot1x control-direction both
```

configure terminal	
interface	
authentication port-control auto **dot1x port-control auto**	

dot1x mac-auth-bypass eap timeout activity	**eap** **timeout activity**
end	
show authentication **show dot1x interface**	
copy running-config startup-config	

no dot1x mac-auth-bypass

```
dot1x mac-auth-bypass
```

configure terminal	
interface	
dot1x guest-vlan	
authentication periodic **dot1x reauthentication**	

dot1x timeout reauth-period server	**server**
end	
show authentication interface **show dot1x interface**	
copy running-config startup-config	

```
configure terminal
        interface gigabitethernet0/1
           dot1x reauthentication
           dot1x timeout reauth-period server
```

configure terminal	
cisp enable	

interface	
switchport mode access	**access**
authentication port-control auto	
dot1x pae authenticator	
spanning-tree portfast	
end	
show running-config interface	
copy running-config startup-config	

```
configure terminal
        cisp enable
        interface gigabitethernet2/0/1
           switchport mode access
           authentication port-control auto
           dot1x pae authenticator
           spanning-tree portfast trunk
```

configure terminal	
cisp enable	
dot1x credentials	
username	
password	
interface	
switchport trunk encapsulation dot1q	
switchport mode trunk	
dot1x pae supplicant	
dot1x credentials	
end	
show running-config interface	
copy running-config startup-config	

```
configure terminal
        cisp enable
        dot1x credentials test
        username suppswitch
        password myswitch
```


```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)# ip access-list extended default_acl
                         permit ip any any
                         exit
                radius-server vsa send authentication
                int fastEthernet 2/13
                   ip access-group default_acl in
                   exit
```


```
configure terminal
        interface gigabitethernet 1/0/1
        authentication order dot1x webauth
```


```
configure terminal
        interface gigabitethernet 1/0/1
        authentication control-direction both
        autentication fallback profile1
```

radius-server attribute 8 include-in-access-req	
radius-server vsa send authentication	
ip device tracking	**no ip device tracking**
end	

configure terminal	
ip admission name proxy http	
interface	
switchport mode access	
ip access-group in	
ip admission	
end	
show running-config interface	
copy running-config startup-config	

configure terminal	
ip admission name proxy http	
fallback profile -	


```
Switch(config-fallback-profile)#
Switch(config-fallback-profile)#
Switch(config-fallback-profile)#
Switch(config)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
```

banner-text | *file-path*	*C banner-text C,* *C*

```
Switch(config)
Switch(config)#
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
                end
```

interface-id	
interface-id *interface-id*	

```
interface gigabitethernet0/1
   no dot1x pae authenticator
```

Resetting the 802.1x Authentication Configuration to the Default Values

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

Displaying 802.1x Statistics and Status