

IEEE 802.1x Authentication with Catalyst 6500/6000 Running Cisco IOS Software Configuration Example

Document ID: 42665

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configure the Catalyst Switch for 802.1x Authentication
- Configure the RADIUS Server
- Configure the PC Clients to Use 802.1x Authentication

Verify

- PC Clients
- Catalyst 6500

Troubleshoot

Related Information

Introduction

This document explains how to configure IEEE 802.1x on a Catalyst 6500/6000 that runs in native mode (a single Cisco IOS® Software image for the Supervisor Engine and MSFC) and a Remote Authentication Dial-In User Service (RADIUS) server for authentication and VLAN assignment.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- Installation Guide for Cisco Secure ACS for Windows 4.1
- User Guide for Cisco Secure Access Control Server 4.1
- How Does RADIUS Work?
- Catalyst Switching and ACS Deployment Guide

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 6500 that runs Cisco IOS Software Release 12.2(18)SXF on Supervisor Engine

Note: You need Cisco IOS Software Release 12.1(13)E or later to support 802.1x port-based authentication.

- This example uses Cisco Secure Access Control Server (ACS) 4.1 as the RADIUS server.

Note: A RADIUS server must be specified before you enable 802.1x on the switch.

- PC clients that supports 802.1x authentication

Note: This example uses Microsoft Windows XP clients.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The IEEE 802.1x standard defines a client–server–based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before it makes available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Note: If the switch receives EAPOL packets from the port that is not configured for 802.1x authentication or if the switch does not support 802.1x authentication, then the EAPOL packets are dropped and are not forwarded to any upstream devices.

Configure

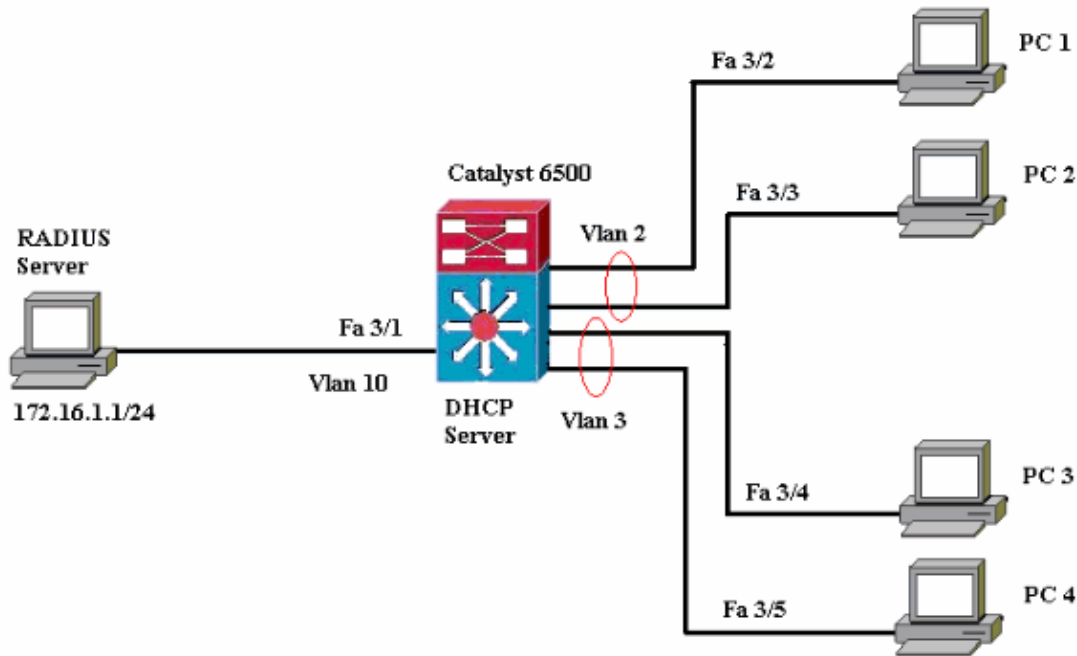
In this section, you are presented with the information to configure the 802.1x feature described in this document.

This configuration requires these steps:

- Configure the Catalyst switch for 802.1x authentication.
- Configure the RADIUS server.
- Configure the PC clients to use 802.1x authentication.

Network Diagram

This document uses this network setup:



- RADIUS server Performs the actual authentication of the client. The RADIUS server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Here, the RADIUS server is configured for authentication and VLAN assignment.
- Switch Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the RADIUS server. It requests identity information from the client, verifies that information with the RADIUS server, and relays a response to the client. Here, the Catalyst 6500 switch is also configured as a DHCP server. The 802.1x authentication support for the Dynamic Host Configuration Protocol (DHCP) allows the DHCP server to assign the IP addresses to the different classes of end users by adding the authenticated user identity into the DHCP discovery process.
- Clients The devices (workstations) that requests access to the LAN and switch services and responds to requests from the switch. Here, PCs 1 to 4 are the clients that request an authenticated network access. PCs 1 and 2 use the same logon credential that is in VLAN 2. Similarly, PCs 3 and 4 use a logon credential for VLAN 3. PC clients are configured to attain the IP address from a DHCP server.

Configure the Catalyst Switch for 802.1x Authentication

This sample switch configuration includes:

- How to enable 802.1x authentication on FastEthernet ports.
- How to connect a RADIUS server to VLAN 10 behind FastEthernet port 3/1.
- A DHCP server configuration for two IP pools, one for clients in VLAN 2 and the other for clients in VLAN 3.
- Inter-VLAN routing to have connectivity between clients after authentication.

Refer to 802.1x Port-Based Authentication Guidelines and Restrictions for the guidelines on how to configure 802.1x authentication.

Note: Make sure that the RADIUS server always connects behind an authorized port.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Cat6K

!--- Sets the hostname for the switch.

Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3

!--- VLAN should be existing in the switch for a successful authentication.

Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER

!--- This is a dedicated VLAN for the RADIUS server.

Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut

!--- Assigns the port connected to the RADIUS server to VLAN 10.
!--- Note:- All the active access ports are in VLAN 1 by default.

Cat6K(config-if)#exit
Cat6K(config)#dot1x system-auth-control

!--- Globally enables 802.1x.

Cat6K(config)#interface range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut

!--- Enables 802.1x on all the FastEthernet interfaces.

Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model

!--- Enables AAA.

Cat6K(config)#aaa authentication dot1x default group radius

!--- Method list should be default. Otherwise dot1x does not work.

Cat6K(config)#aaa authorization network default group radius

!--- You need authorization for dynamic VLAN assignment to work with RADIUS.

Cat6K(config)#radius-server host 172.16.1.1

!--- Sets the IP address of the RADIUS server.

Cat6K(config)#radius-server key cisco

!--- The key must match the key used on the RADIUS server.

Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
```

```

!--- This is used as the gateway address in RADIUS server
!--- and also as the client identifier in the RADIUS server.

Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut

!--- This is the gateway address for clients in VLAN 2.

Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut

!--- This is the gateway address for clients in VLAN 3.

Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.2.1

!--- This pool assigns ip address for clients in VLAN 2.

Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1

!--- This pool assigns ip address for clients in VLAN 3.

Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

VLAN Name                Status      Ports
-----
1    default                active     Fa3/2, Fa3/3, Fa3/4, Fa3/5
                                           Fa3/6, Fa3/7, Fa3/8, Fa3/9
                                           Fa3/10, Fa3/11, Fa3/12, Fa3/13
                                           Fa3/14, Fa3/15, Fa3/16, Fa3/17
                                           Fa3/18, Fa3/19, Fa3/20, Fa3/21
                                           Fa3/22, Fa3/23, Fa3/24, Fa3/25
                                           Fa3/26, Fa3/27, Fa3/28, Fa3/29
                                           Fa3/30, Fa3/31, Fa3/32, Fa3/33
                                           Fa3/34, Fa3/35, Fa3/36, Fa3/37
                                           Fa3/38, Fa3/39, Fa3/40, Fa3/41
                                           Fa3/42, Fa3/43, Fa3/44, Fa3/45
                                           Fa3/46, Fa3/47, Fa3/48
2    VLAN2                  active
3    VLAN3                  active
10   RADIUS_SERVER          active     Fa3/1
1002 fddi-default          act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup

!--- Output suppressed.
!--- All active ports are in VLAN 1 (except 3/1) before authentication.

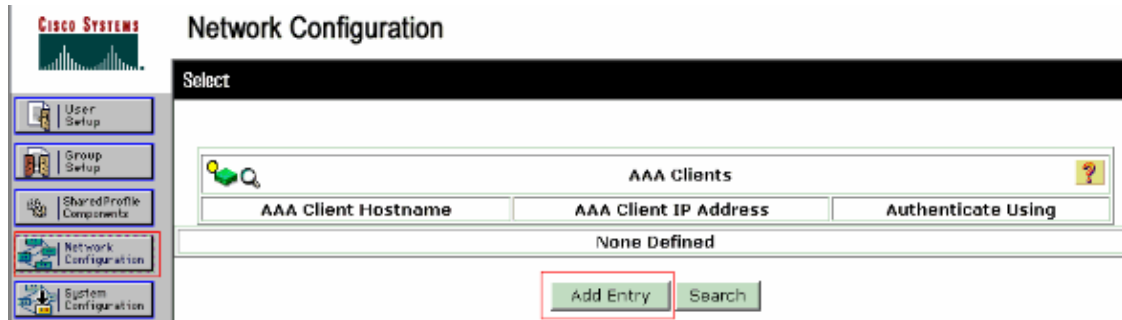
```

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Configure the RADIUS Server

The RADIUS server is configured with a static IP address of 172.16.1.1/24. Complete these steps in order to configure the RADIUS server for an AAA client:

1. Click **Network Configuration** on the ACS administration window in order to configure an AAA client.
2. Click **Add Entry** under the AAA clients section.

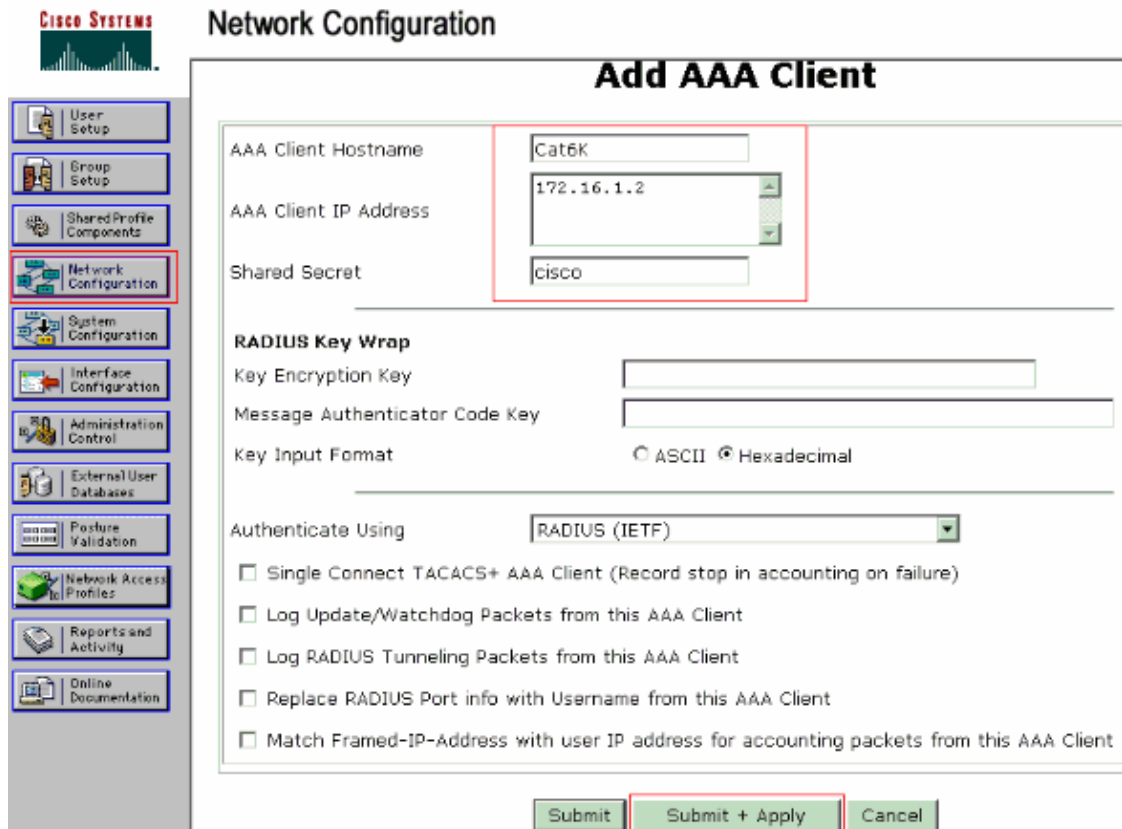


3. Configure the AAA client hostname, IP address, shared secret key and authentication type as:

- ◆ AAA client hostname = Switch Hostname (**Cat6K**).
- ◆ AAA client IP address = Management interface IP address of the switch (**172.16.1.2**).
- ◆ Shared Secret = RADIUS Key configured on the switch (**cisco**).
- ◆ Authenticate Using = **RADIUS IETF**.

Note: For correct operation, the shared secret key must be identical on the AAA client and ACS. Keys are case sensitive.

4. Click **Submit + Apply** to make these changes effective, as this example shows:

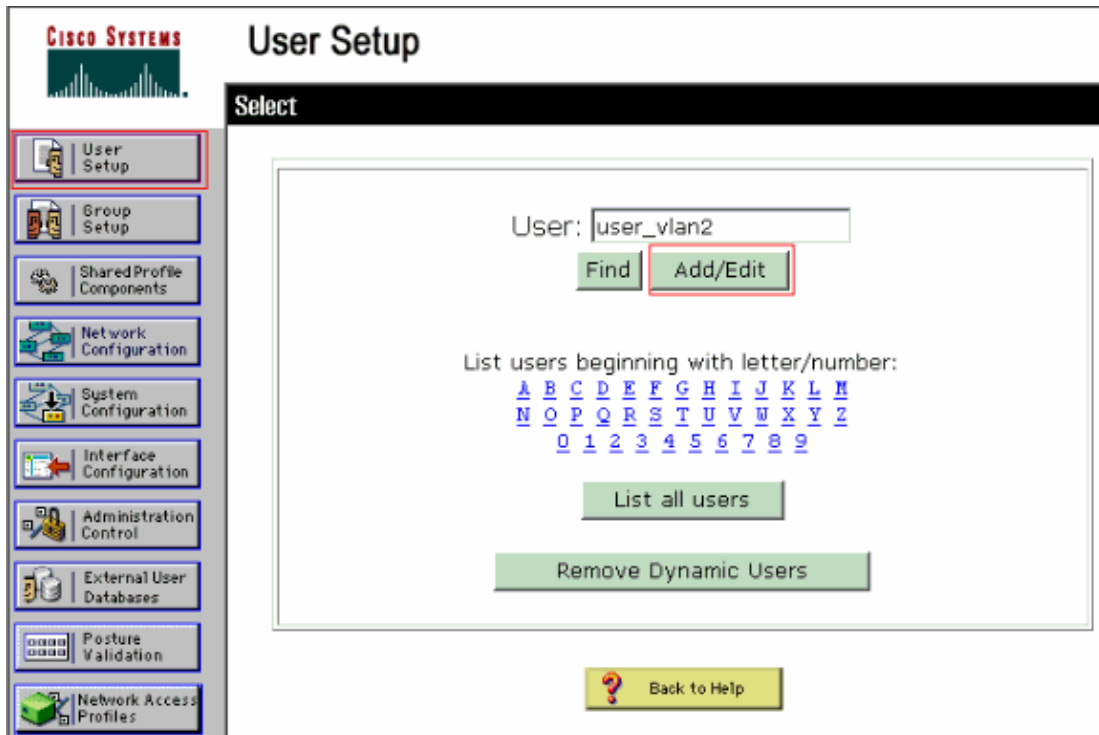


Complete these steps in order to configure the RADIUS server for authentication, VLAN and IP address assignment.

Two user names have to be created separately for clients that connect to VLAN 2 as well as for VLAN 3. Here, a user **user_vlan2** for clients that connect to VLAN 2 and another user **user_vlan3** for clients that connect to VLAN 3 are created for this purpose.

Note: Here, the user configuration is shown for clients that connect to VLAN 2 only. For users that connect to VLAN 3, follow the same procedure.

1. In order to add and configure users, click **User Setup** and define the user name and password.



CISCO SYSTEMS **User Setup**

Edit

User: user_vlan2 (New User)

Account Disabled

Supplementary User Info ?


Real Name: user_vlan2
Description: client in VLAN 2

User Setup ?

Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: [Redacted]
Confirm Password: [Redacted]

2. Define the client IP address assignment as **Assigned by AAA client pool**. Enter the name of the IP address pool configured on the switch for VLAN 2 clients.



User Setup

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:

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

Note: Select this option and type the AAA client IP pool name in the box, only if this user is to have the IP address assigned by an IP address pool configured on the AAA client.

3. Define the Internet Engineering Task Force (IETF) attributes **64** and **65**.

Make sure that the Tags of the Values are set to **1**, as this example shows. Catalyst ignores any tag other than 1. In order to assign a user to a specific VLAN, you must also define attribute **81** with a VLAN *name* or VLAN *number* that corresponds.

Note: If you use the VLAN *name*, it should be exactly same as the one configured in the switch.

Note: For more information on these IETF attributes, refer to RFC 2868: RADIUS Attributes for Tunnel Protocol Support .

Note: In the initial configuration of the ACS server, IETF RADIUS attributes can fail to display in **User Setup**. In order to enable IETF attributes in user configuration screens, choose **Interface configuration > RADIUS (IETF)**. Then, check attributes **64**, **65**, and **81** in the User and Group columns.

Note: If you do not define IETF attribute **81** and the port is a switch port in access mode, the client has assignment to the access VLAN of the port. If you have defined the attribute **81** for dynamic VLAN assignment and the port is a switch port in access mode, you need to issue the command **aaa authorization network default group radius** on the switch. This command assigns the port to the VLAN that the RADIUS server provides. Otherwise, 802.1x moves the port to the AUTHORIZED state after authentication of the user; but the port is still in the default VLAN of the port, and connectivity can fail. If you have defined the attribute **81**, but you have configured the port as a routed port, access denial occurs. This error message displays:

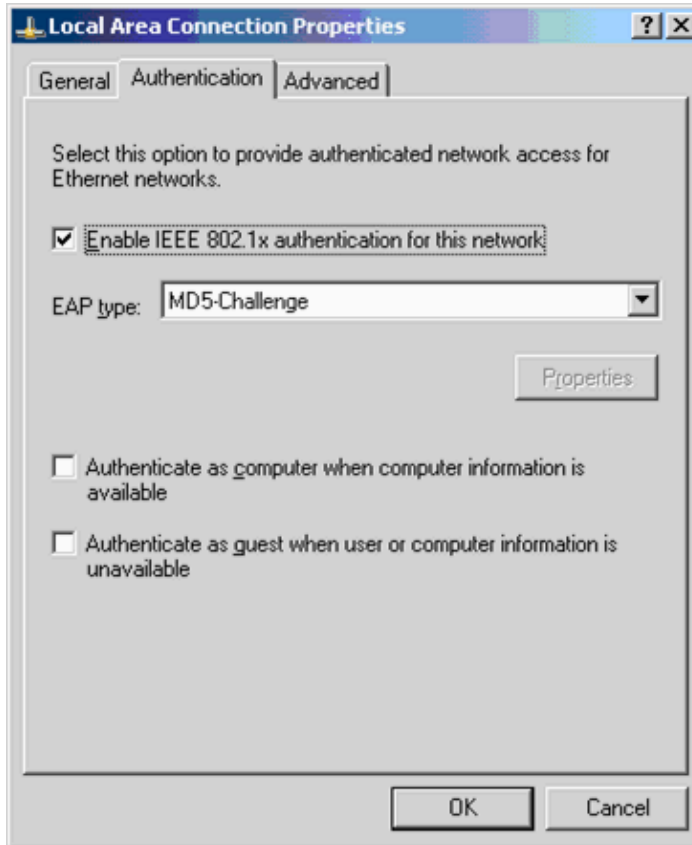
```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

Configure the PC Clients to Use 802.1x Authentication

This example is specific to the Microsoft Windows XP Extensible Authentication Protocol (EAP) over LAN (EAPOL) client:

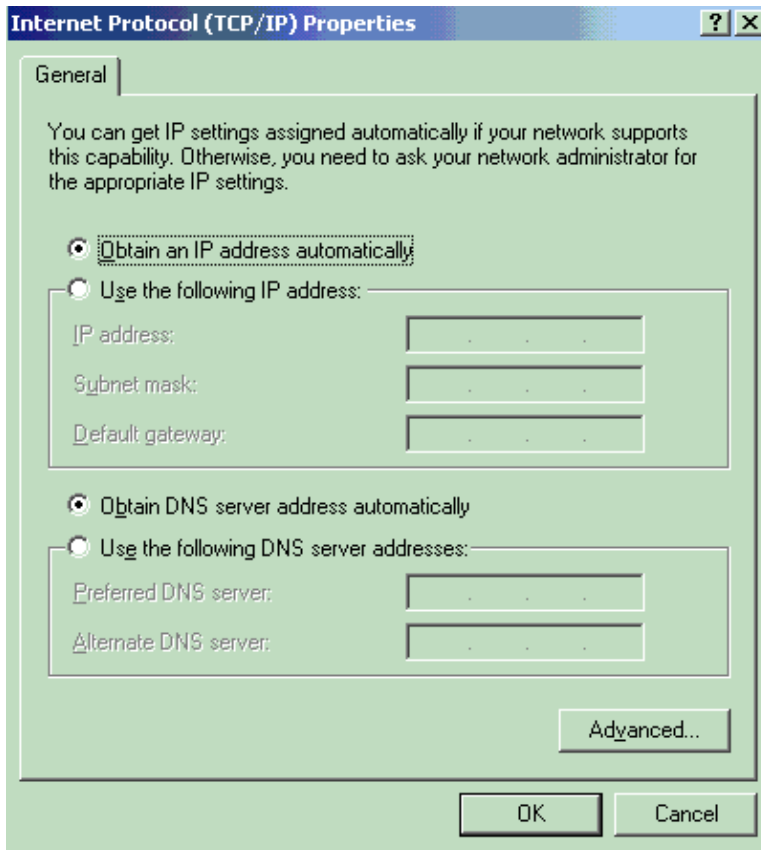
1. Choose **Start > Control Panel > Network Connections**, then right-click on your **Local Area Connection** and choose **Properties**.
2. Check **Show icon in notification area when connected** under the General tab.

3. Under the Authentication tab, check **Enable IEEE 802.1x authentication for this network**.
4. Set the EAP type to **MD5-Challenge**, as this example shows:



Complete these steps to configure the clients to obtain the IP address from a DHCP server.

1. Choose **Start > Control Panel > Network Connections**, then right-click on your **Local Area Connection** and choose **Properties**.
2. Under the General tab, click **Internet Protocol (TCP/IP)** and then **Properties**.
3. Choose **Obtain an IP address automatically**.

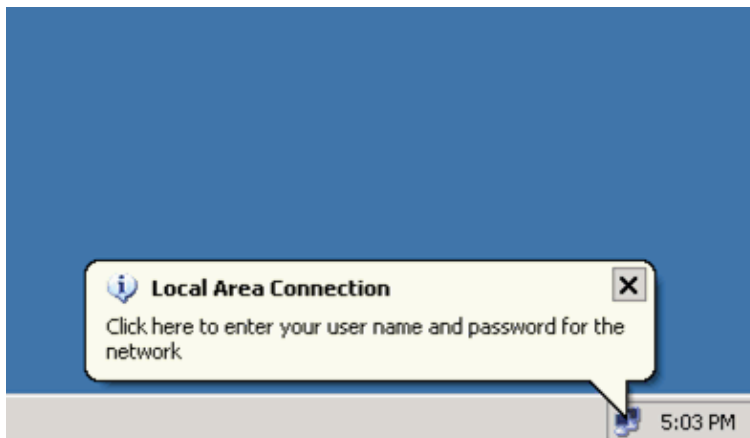


Verify

PC Clients

If you have correctly completed the configuration, the PC clients displays a popup prompt to enter a user name and password.

1. Click on the prompt, which this example shows:



- A user name and password entry window displays.
2. Enter the user name and password.



Note: In PC 1 and 2, enter VLAN 2 user credentials and in PC 3 and 4 enter VLAN 3 user credentials.

3. If no error messages appear, verify connectivity with the usual methods, such as through access of the network resources and with **ping**. This output is from PC 1, and shows a successful **ping** to PC 4:

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.1

C:\Documents and Settings\Administrator>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:

Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.3.2

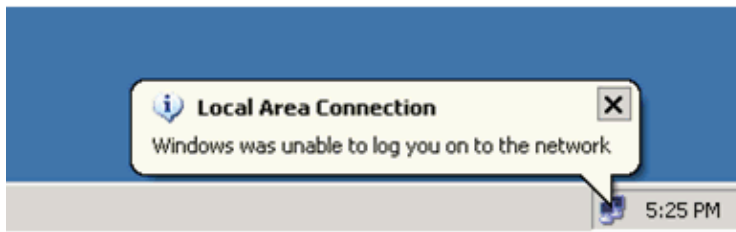
Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

If this error appears, verify that the user name and password are correct:



Catalyst 6500

If the password and user name appear to be correct, verify the 802.1x port state on the switch.

1. Look for a port status that indicates AUTHORIZED.

```
Cat6K#show dot1x
```

```
Sysauthcontrol           = Enabled
Dot1x Protocol Version   = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

```
Cat6K#show dot1x interface fastEthernet 3/2
```

```
AuthSM State             = AUTHENTICATED
BendSM State              = IDLE
PortStatus              = AUTHORIZED
MaxReq                    = 2
MultiHosts                = Enabled
Port Control              = Auto
QuietPeriod               = 60 Seconds
Re-authentication         = Disabled
ReAuthPeriod              = 3600 Seconds
ServerTimeout             = 30 Seconds
SuppTimeout               = 30 Seconds
TxPeriod                  = 30 Seconds
```

```
Cat6K#show dot1x interface fastEthernet 3/4
```

```
AuthSM State             = AUTHENTICATED
BendSM State              = IDLE
PortStatus              = AUTHORIZED
MaxReq                    = 2
MultiHosts                = Enabled
Port Control              = Auto
QuietPeriod               = 60 Seconds
Re-authentication         = Disabled
ReAuthPeriod              = 3600 Seconds
ServerTimeout             = 30 Seconds
SuppTimeout               = 30 Seconds
TxPeriod                  = 30 Seconds
```

```
Cat6K#show dot1x interface fastEthernet 3/1
```

```
Default Dot1x Configuration Exists for this interface FastEthernet3/1
AuthSM State             = FORCE AUTHORIZED
BendSM State              = IDLE
PortStatus              = AUTHORIZED
MaxReq                    = 2
MultiHosts                = Disabled
PortControl               = Force Authorized
QuietPeriod               = 60 Seconds
Re-authentication         = Disabled
ReAuthPeriod              = 3600 Seconds
```

```
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
TxPeriod           = 30 Seconds
```

Verify the VLAN status after successful authentication.

```
Cat6K#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa3/6, Fa3/7, Fa3/8, Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13, Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19, Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25, Fa3/26, Fa3/27, Fa3/28, Fa3/29, Fa3/30, Fa3/31, Fa3/32, Fa3/33, Fa3/34, Fa3/35, Fa3/36, Fa3/37, Fa3/38, Fa3/39, Fa3/40, Fa3/41, Fa3/42, Fa3/43, Fa3/44, Fa3/45, Fa3/46, Fa3/47, Fa3/48
2	VLAN2	active	Fa3/2, Fa3/3
3	VLAN3	active	Fa3/4, Fa3/5
10	RADIUS_SERVER	active	Fa3/1
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

!--- Output suppressed.

2. Verify the DHCP binding status from the after successful authentication.

```
Router#show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
172.16.2.2	0100.1636.3333.9c	Mar 04 2007 06:35 AM	Automatic
172.16.2.3	0100.166F.3CA3.42	Mar 04 2007 06:43 AM	Automatic
172.16.3.2	0100.145e.945f.99	Mar 04 2007 06:50 AM	Automatic
172.16.3.3	0100.1185.8D9A.F9	Mar 04 2007 06:57 AM	Automatic

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Collect the output of these **debug** commands in order to troubleshoot:

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug dot1x events** Enables debugging of print statements guarded by the dot1x events flag.

```
Cat6K#debug dot1x events
```

```
Dot1x events debugging is on
Cat6K#
```

!--- Debug output for PC 1 connected to Fa3/2.

```
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 14
00:13:36: dot1x-ev:Couldn't Find a process thats already handling
the request for this id 3
00:13:36: dot1x-ev:Inserted the request on to list of pending requests.
Total requests = 1
```

```
00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0
00:13:36: dot1x-ev:AAA Client-process processing Request
          Interface= Fa3/2,
          Request-Id = 14,
          Length = 15
00:13:36: dot1x-ev:The Interface on which we got this AAA Request
is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
          this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
          this id 13
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
          id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
          will pick up any pending requests from the queue
Cat6K#
Cat6K#

!--- Debug output for PC 3 connected to Fa3/4.

00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 8
00:19:58: dot1x-ev:Couldn't Find a process thats already handling
          the request for this id 1
00:19:58: dot1x-ev:Inserted the request on to list of pending requests.
          Total requests = 1
00:19:58: dot1x-ev:Found a free slot at slot: 0
00:19:58: dot1x-ev:AAA Client process spawned at slot: 0
00:19:58: dot1x-ev:AAA Client-process processing Request
          Interface= Fa3/4,
          Request-Id = 8,
          Length = 15
00:19:58: dot1x-ev:The Interface on which we got this AAA
Request is FastEthernet3/4
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
          for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
          for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
```

will pick up any pending requests from the queue
Cat6K#

- **debug radius** Displays information associated with RADIUS.

```
Cat6K#debug radius
Radius protocol debugging is on
Cat6K#
```

!--- Debug output for PC 1 connected to Fa3/2.

```
00:13:36: RADIUS: ustruct sharecount=1
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a
00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 1
00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812,
Access-Request, len 85
00:13:36: Attribute 4 6 AC100201
00:13:36: Attribute 61 6 00000000
00:13:36: Attribute 1 12 75736572
00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 79 17 0201000F
00:13:36: Attribute 80 18 CCEE4889
00:13:36: RADIUS: Received from id 17 172.16.1.1:1812,
Access-Challenge, len 79
00:13:36: Attribute 79 8 010D0006
00:13:36: Attribute 24 33 43495343
00:13:36: Attribute 80 18 C883376B
00:13:36: RADIUS: EAP-login: length of eap packet = 6
00:13:36: RADIUS: EAP-login: got challenge from radius
00:13:36: RADIUS: ustruct sharecount=1
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a
00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812,
Access-Request, len 109
00:13:36: Attribute 4 6 AC100201
00:13:36: Attribute 61 6 00000000
00:13:36: Attribute 1 12 75736572
00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343
00:13:36: Attribute 79 8 020D0006
00:13:36: Attribute 80 18 15582484
00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge,
len 104
00:13:36: Attribute 79 33 010E001F
00:13:36: Attribute 24 33 43495343
00:13:36: Attribute 80 18 0643D234
00:13:36: RADIUS: EAP-login: length of eap packet = 31
00:13:36: RADIUS: EAP-login: got challenge from radius
00:13:36: RADIUS: ustruct sharecount=1
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a
00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19 172.16.1.1:1812,
Access-Request, len 135
00:13:36: Attribute 4 6 AC100201
00:13:36: Attribute 61 6 00000000
00:13:36: Attribute 1 12 75736572
00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343
00:13:36: Attribute 79 34 020E0020
00:13:36: Attribute 80 18 E8A61751
00:13:36: RADIUS: Received from id 19 172.16.1.1:1812,
Access-Accept, len 124
00:13:36: Attribute 64 6 0100000D
00:13:36: Attribute 65 6 01000006
00:13:36: Attribute 81 8 01564C41
00:13:36: Attribute 88 15 766C616E
00:13:36: Attribute 8 6 FFFFFFFE
```

```
00:13:36:      Attribute 79 6 030E0004
00:13:36:      Attribute 25 39 43495343
00:13:36:      Attribute 80 18 11A7DD44
00:13:36: RADIUS: EAP-login: length of eap packet = 4
Cat6K#
Cat6K#
```

!--- Debug output for PC 3 connected to Fa3/4.

```
00:19:58: RADIUS: ustruct sharecount=1
00:19:58: RADIUS: Unexpected interface type in nas_port_format_a
00:19:58: RADIUS: EAP-login: length of radius packet = 85 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11 172.16.1.1:1812,
Access-Request, len 85
00:19:58:      Attribute 4 6 AC100201
00:19:58:      Attribute 61 6 00000000
00:19:58:      Attribute 1 12 75736572
00:19:58:      Attribute 12 6 000003E8
00:19:58:      Attribute 79 17 0201000F
00:19:58:      Attribute 80 18 0001AC52
00:19:58: RADIUS: Received from id 11 172.16.1.1:1812, Access-Challenge,
len 79
00:19:58:      Attribute 79 8 010B0006
00:19:58:      Attribute 24 33 43495343
00:19:58:      Attribute 80 18 23B9C9E7
00:19:58: RADIUS: EAP-login: length of eap packet = 6
00:19:58: RADIUS: EAP-login: got challenge from radius
00:19:58: RADIUS: ustruct sharecount=1
00:19:58: RADIUS: Unexpected interface type in nas_port_format_a
00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812,
Access-Request, len 109
00:19:58:      Attribute 4 6 AC100201
00:19:58:      Attribute 61 6 00000000
00:19:58:      Attribute 1 12 75736572
00:19:58:      Attribute 12 6 000003E8
00:19:58:      Attribute 24 33 43495343
00:19:58:      Attribute 79 8 020B0006
00:19:58:      Attribute 80 18 F4C8832E
00:19:58: RADIUS: Received from id 12 172.16.1.1:1812,
Access-Challenge, len 104
00:19:58:      Attribute 79 33 010C001F
00:19:58:      Attribute 24 33 43495343
00:19:58:      Attribute 80 18 45472A93
00:19:58: RADIUS: EAP-login: length of eap packet = 31
00:19:58: RADIUS: EAP-login: got challenge from radius
00:19:58: RADIUS: ustruct sharecount=1
00:19:58: RADIUS: Unexpected interface type in nas_port_format_a
00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812,
Access-Request, len 135
00:19:58:      Attribute 4 6 AC100201
00:19:58:      Attribute 61 6 00000000
00:19:58:      Attribute 1 12 75736572
00:19:58:      Attribute 12 6 000003E8
00:19:58:      Attribute 24 33 43495343
00:19:58:      Attribute 79 34 020C0020
00:19:58:      Attribute 80 18 37011E8F
00:19:58: RADIUS: Received from id 13 172.16.1.1:1812, Access-Accept,
len 120
00:19:58:      Attribute 64 6 0100000D
00:19:58:      Attribute 65 6 01000006
00:19:58:      Attribute 81 4 0133580F
00:19:58:      Attribute 88 15 766C616E
00:19:58:      Attribute 8 6 FFFFFFFF
00:19:58:      Attribute 79 6 030C0004
```

00:19:58: Attribute 25 39 43495343
00:19:58: Attribute 80 18 F5520A95
00:19:58: RADIUS: EAP-login: length of eap packet = 4
Cat6K#

Related Information

- **IEEE 802.1x Authentication with Catalyst 6500/6000 Running CatOS Software Configuration Example**
 - **Guidelines for the Deployment of Cisco Secure ACS for Windows NT/2000 Servers in a Cisco Catalyst Switch Environment**
 - **RFC 2868: RADIUS Attributes for Tunnel Protocol Support**
 - **Configuring IEEE 802.1X Port-Based Authentication**
 - **LAN Product Support**
 - **LAN Switching Technology Support**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 27, 2007

Document ID: 42665
