

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

Document ID: 81871

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 hybrid mode (CatOS on the Supervisor Engine and Cisco IOS® Software on the 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 CatOS Software Release 8.5(6) on the Supervisor Engine and Cisco IOS Software Release 12.2(18)SXF on the MSFC

Note: You need CatOS Release 6.2 or later to support 802.1x port-based authentication.

Note: Before software release 7.2(2), once the 802.1x host is authenticated, it joins an NVRAM-configured VLAN. With software release 7.2(2) and later releases, after authentication, an

802.1x host can receive its VLAN assignment from the RADIUS server.

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

Note: A RADIUS server must be specified before enabling 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 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 making 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 (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Configure

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

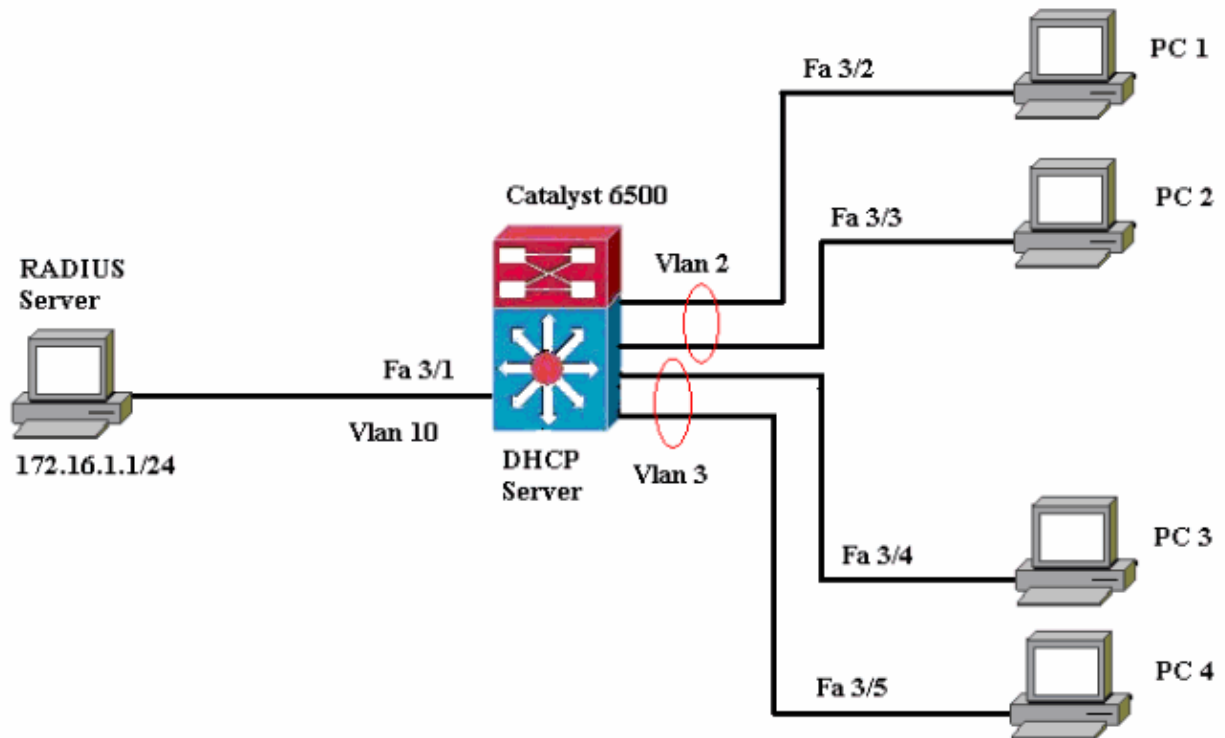
Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

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, requesting identity information from the client, verifying that information with the RADIUS server, and relaying 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 request access to the LAN and switch services and respond to requests from the switch. Here, PCs 1 to 4 are the clients that request an authenticated network access. PCs 1 and 2 will use the same logon credential to be in VLAN 2. Similarly, PCs 3 and 4 will use a logon credential for VLAN 3. PC clients are configured to attain the IP address from a DHCP server.

Note: In this configuration, any client that fails the authentication or any non-802.1x capable client connecting to the switch is denied network access by moving them to an unused VLAN (VLAN 4 or 5) using the authentication failure and guest VLAN features.

Configure the Catalyst Switch for 802.1x Authentication

This sample switch configuration includes:

- Enable 802.1x authentication and associated features on FastEthernet ports.
- Connect RADIUS server to VLAN 10 behind FastEthernet port 3/1.
- DHCP server configuration for two IP pools, one for clients in VLAN 2 and other for clients in VLAN 3.
- Inter-VLAN routing to have connectivity between clients after authentication.

Refer to Authentication Configuration Guidelines for the guidelines on how to configure 802.1x authentication.

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

Catalyst 6500

```
Console (enable) set system name Cat6K
System name set.

!--- Sets the hostname for the switch.

Cat6K> (enable) set localuser user admin password cisco
Added local user admin.
Cat6K> (enable) set localuser authentication enable
LocalUser authentication enabled

!--- Uses local user authentication to access the switch.

Cat6K> (enable) set vtp domain cisco
VTP domain cisco modified

!--- Domain name must be configured for VLAN configuration.

Cat6K> (enable) set vlan 2 name VLAN2
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 2 configuration successful

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

Cat6K> (enable) set vlan 3 name VLAN3
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful

!--- VLAN names will be used in RADIUS server for VLAN assignment.

Cat6K> (enable) set vlan 4 name AUTHFAIL_VLAN
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 4 configuration successful

!--- A VLAN for non-802.1x capable hosts.

Cat6K> (enable) set vlan 5 name GUEST_VLAN
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 4 configuration successful

!--- A VLAN for failed authentication hosts.

Cat6K> (enable) set vlan 10 name RADIUS_SERVER
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 10 configuration successful

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

Cat6K> (enable) set interface sc0 10 172.16.1.2 255.255.255.0
Interface sc0 vlan set, IP address and netmask set.

!--- Note: 802.1x authentication always uses the
!--- sc0 interface as the identifier for the authenticator
```

!--- when communicating with the RADIUS server.

```
Cat6K> (enable) set vlan 10 3/1  
VLAN 10 modified.  
VLAN 1 modified.  
VLAN Mod/Ports  
-----  
10    3/1
```

!--- Assigns port connecting to RADIUS server to VLAN 10.

```
Cat6K> (enable) set radius server 172.16.1.1 primary  
172.16.1.1 with auth-port 1812 acct-port 1813  
added to radius server table as primary server.
```

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

```
Cat6K> (enable) set radius key cisco  
Radius key set to cisco
```

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

```
Cat6K> (enable) set dot1x system-auth-control enable  
dot1x system-auth-control enabled.  
Configured RADIUS servers will be used for dot1x authentication.
```

!--- Globally enables 802.1x.

*!--- You must specify at least one RADIUS server before
!--- you can enable 802.1x authentication on the switch.*

```
Cat6K> (enable) set port dot1x 3/2-48 port-control auto  
Port 3/2-48 dot1x port-control is set to auto.  
Trunking disabled for port 3/2-48 due to Dot1x feature.  
Spantree port fast start option enabled for port 3/2-48.
```

!--- Enables 802.1x on all FastEthernet ports.

!--- This disables trunking and enables portfast automatically.

```
Cat6K> (enable) set port dot1x 3/2-48 auth-fail-vlan 4  
Port 3/2-48 Auth Fail Vlan is set to 4
```

*!--- Ports will be put in VLAN 4 after three
!--- failed authentication attempts.*

```
Cat6K> (enable) set port dot1x 3/2-48 guest-vlan 5  
Ports 3/2-48 Guest Vlan is set to 5
```

*!--- Any non-802.1x capable host connecting or 802.1x
!--- capable host failing to respond to the username and password
!--- authentication requests from the Authenticator is placed in the
!--- guest VLAN after 60 seconds.
!--- **Note:** An authentication failure VLAN is independent
!--- of the guest VLAN. However, the guest VLAN can be the same
!--- VLAN as the authentication failure VLAN. If you do not want to
!--- differentiate between the non-802.1x capable hosts and the
!--- authentication failed hosts, you can configure both hosts to
!--- the same VLAN (either a guest VLAN or an authentication failure VLAN).
!--- For more information, refer to
!--- Understanding How 802.1x Authentication for the Guest VLAN Works.*

```
Cat6K> (enable) switch console  
Trying Router-16...  
Connected to Router-16.  
Type ^C^C^C to switch back...
```

!--- Transfers control to the routing module (MSFC).

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface vlan 10
Router(config-if)#ip address 172.16.1.3 255.255.255.0

!--- This is used as the gateway address in RADIUS server.

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

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

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

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

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

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

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

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

Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 172.16.2.1
Router(config)#ip dhcp excluded-address 172.16.3.1

!--- In order to go back to the Switching module,
!--- enter Ctrl-C three times.

Router#
Router#^C
Cat6K> (enable)
Cat6K> (enable) show vlan
VLAN Name                Status    IfIndex Mod/Ports, Vlans
-----
1    default                active    6        2/1-2
                                     3/2-48
2    VLAN2                   active    83
3    VLAN3                   active    84
4    AUTHFAIL_VLAN          active    85
5    GUEST_VLAN             active    86
10   RADIUS_SERVER          active    87        3/1
1002 fddi-default           active    78
1003 token-ring-default    active    81
1004 fddinet-default       active    79
1005 trnet-default        active    80

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

Cat6K> (enable) show dot1x

```

```

PAE Capability           Authenticator Only
Protocol Version        1
system-auth-control    enabled
max-req                 2
quiet-period            60 seconds
re-authperiod           3600 seconds
server-timeout          30 seconds
shutdown-timeout        300 seconds
supp-timeout            30 seconds
tx-period               30 seconds

!--- Verifies dot1x status before authentication.

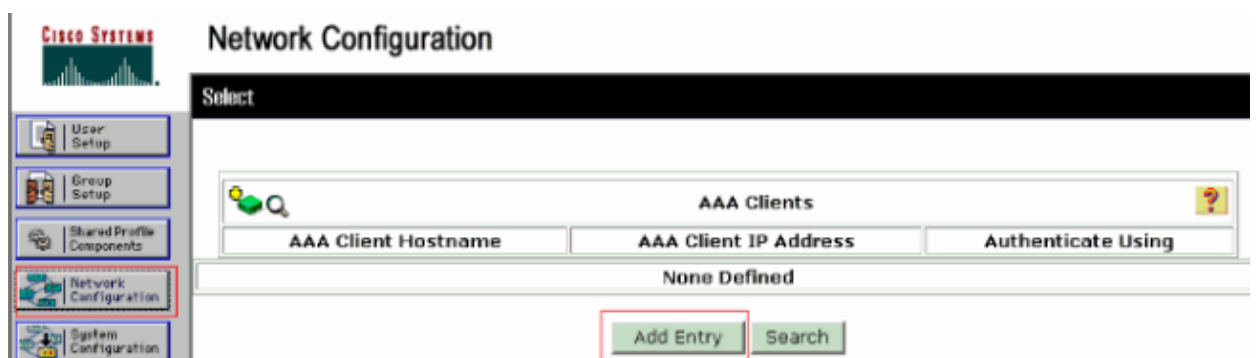
Cat6K> (enable)

```

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

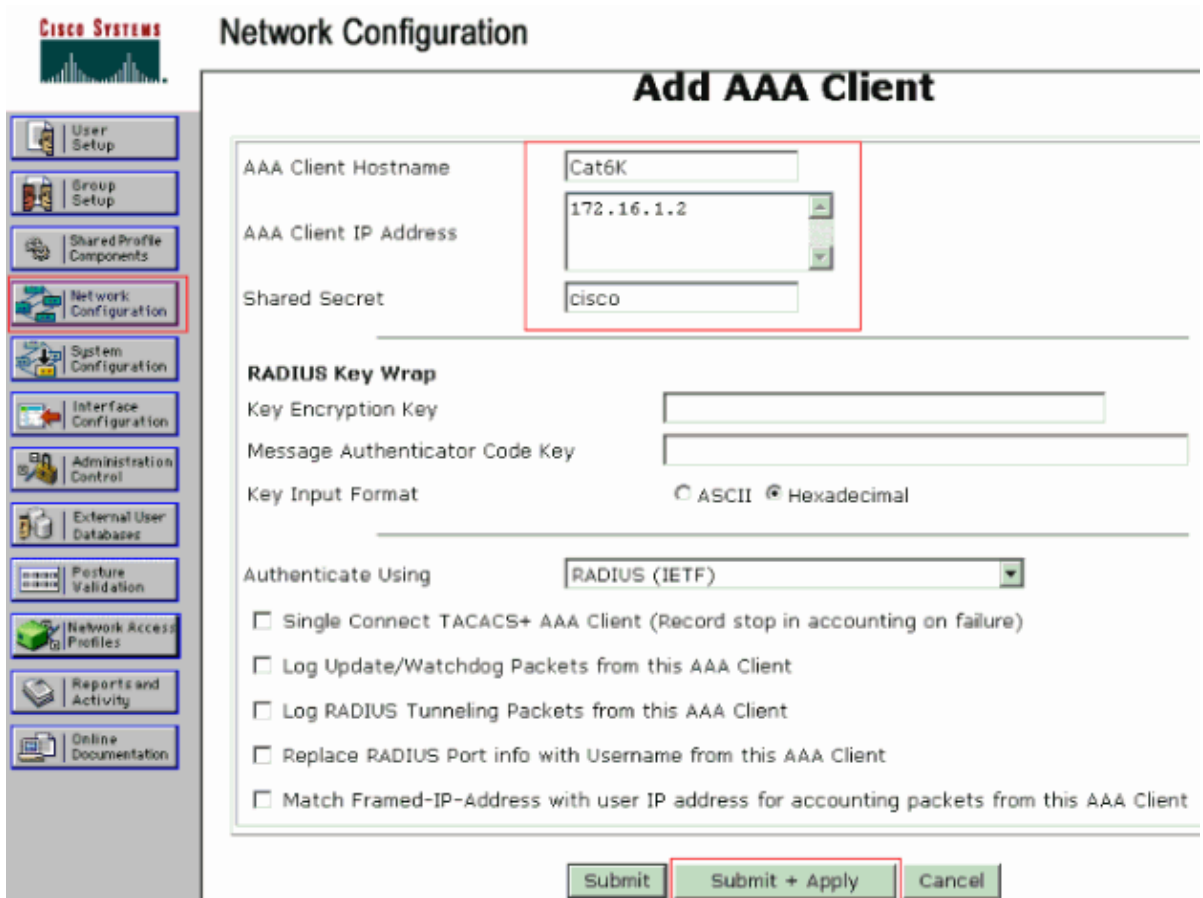


3. Configure the AAA client hostname, IP address, shared secret key and authentication type as:

- ◆ AAA client hostname = Switch Hostname (**Cat6K**).
- ◆ AAA client IP address = Management interface (sc0)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:



CISCO SYSTEMS Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using:

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

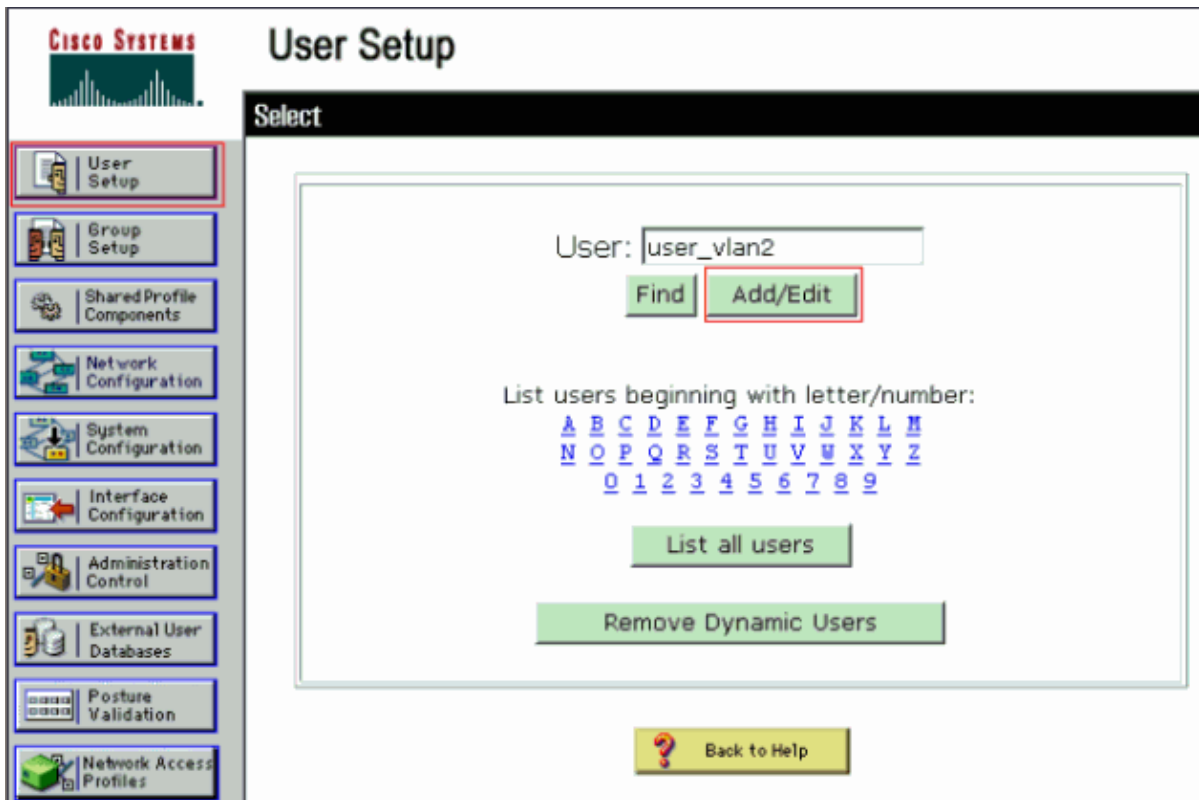
Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

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 connecting to VLAN 2 and another user **user_vlan3** for clients connecting to VLAN 3 are created for this purpose.

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

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



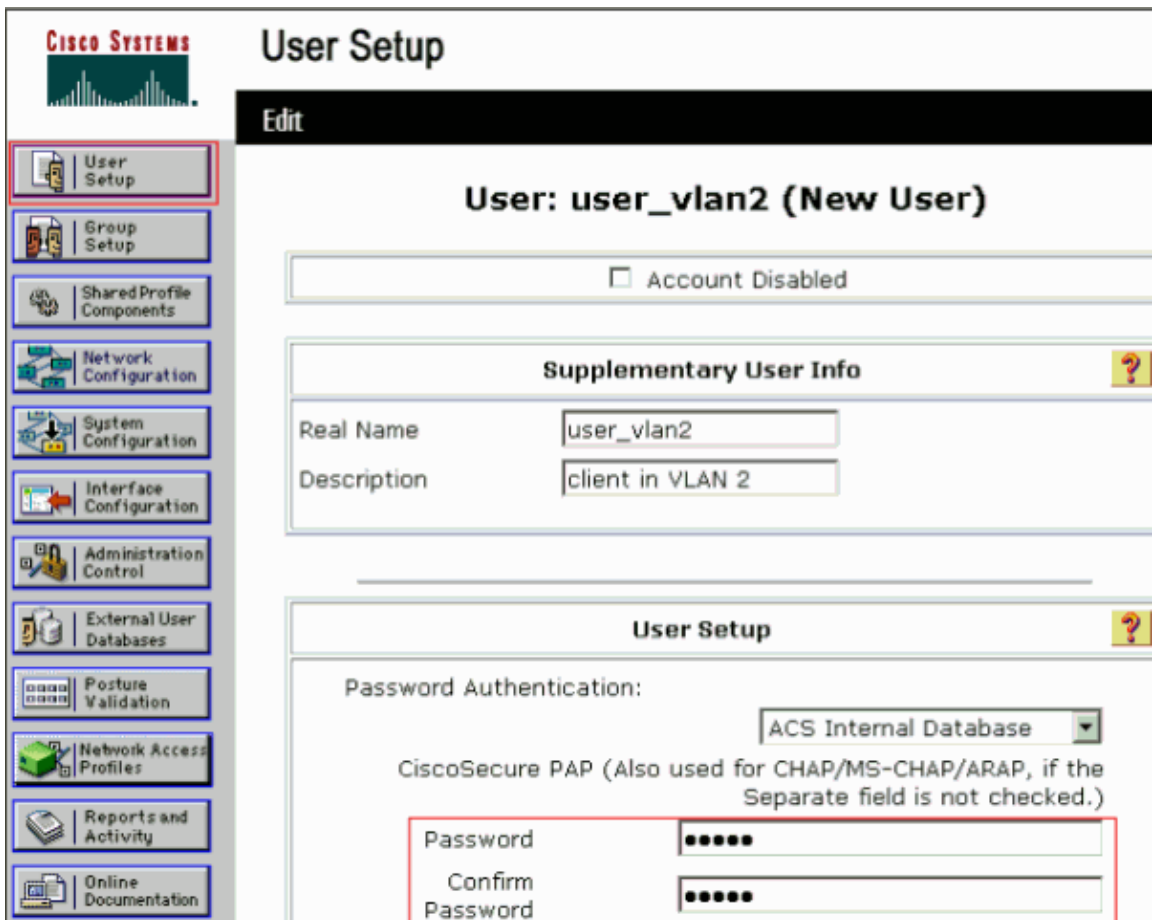
CISCO SYSTEMS User Setup

Select

User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)



CISCO SYSTEMS User Setup

Edit

User: user_vlan2 (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup


Password Authentication:

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

Password

Confirm Password

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* that corresponds.

Note: The VLAN *name* should be exactly same as the one configured in the switch.

Note: VLAN assignment based on VLAN *number* is not supported with CatOS.

CISCO SYSTEMS

User Setup

Checking this option will **PERMIT** all UNKNOWN Services

Default (Undefined) Services

IETF RADIUS Attributes

[006] Service-Type

[064] Tunnel-Type
Tag 1 Value VLAN

[065] Tunnel-Medium-Type
Tag 1 Value 802

[081] Tunnel-Private-Group-ID
Tag 1 Value VLAN2

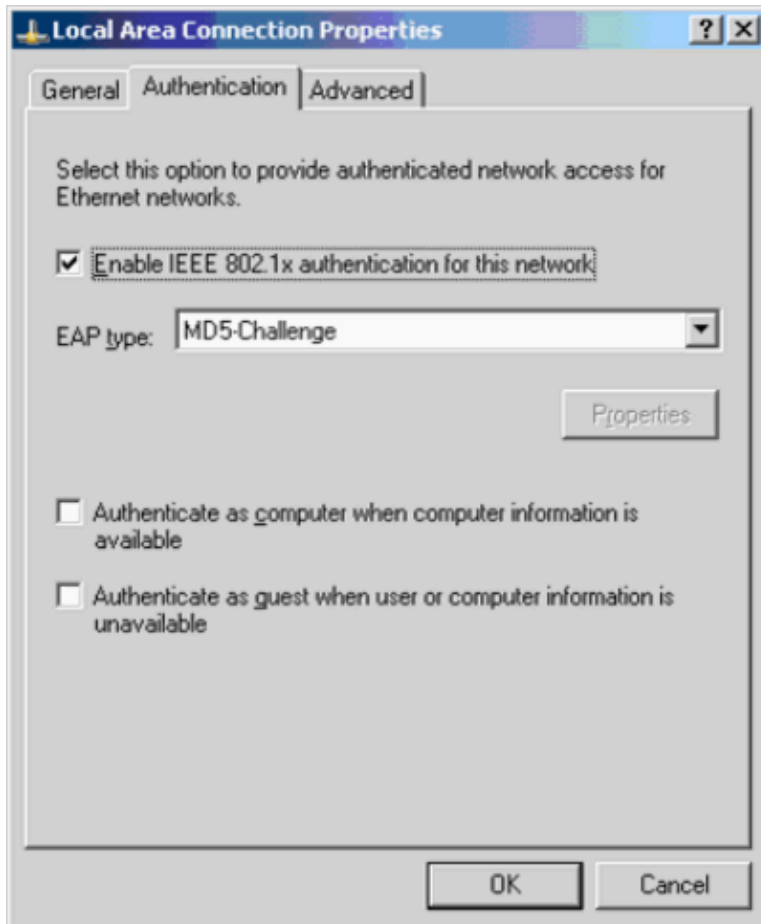
Refer to RFC 2868: RADIUS Attributes for Tunnel Protocol Support for more information on these IETF attributes.

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

Configure the PC Clients to Use 802.1x Authentication

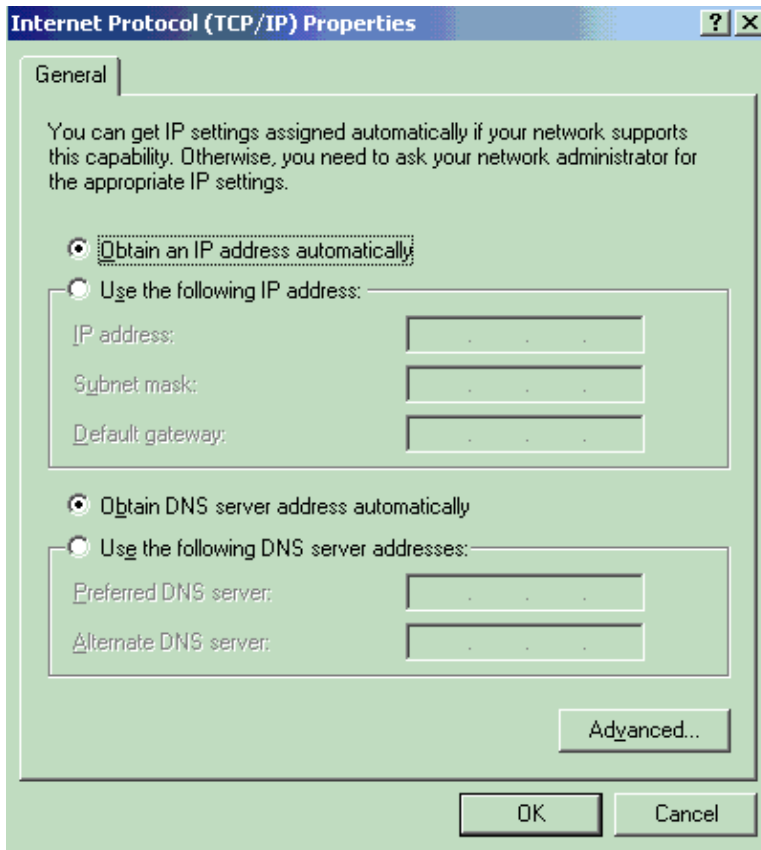
This example is specific to the Microsoft Windows XP Extensible Authentication Protocol (EAP) over LAN (EAPOL) client. Complete these steps:

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 in order to configure the clients to obtain an 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

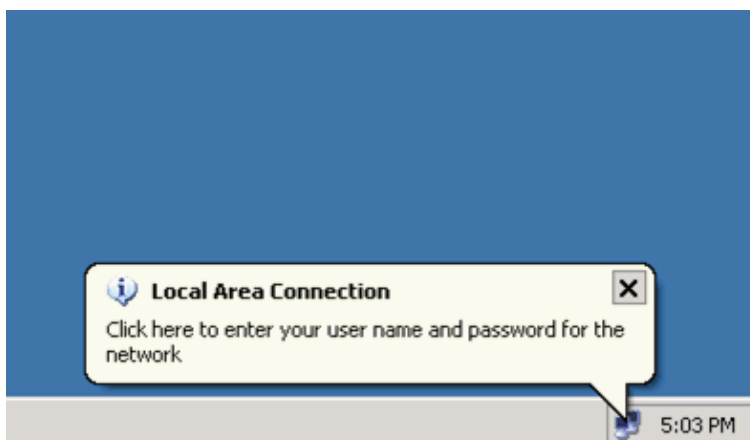
Use this section to confirm that your configuration works properly.

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

PC Clients

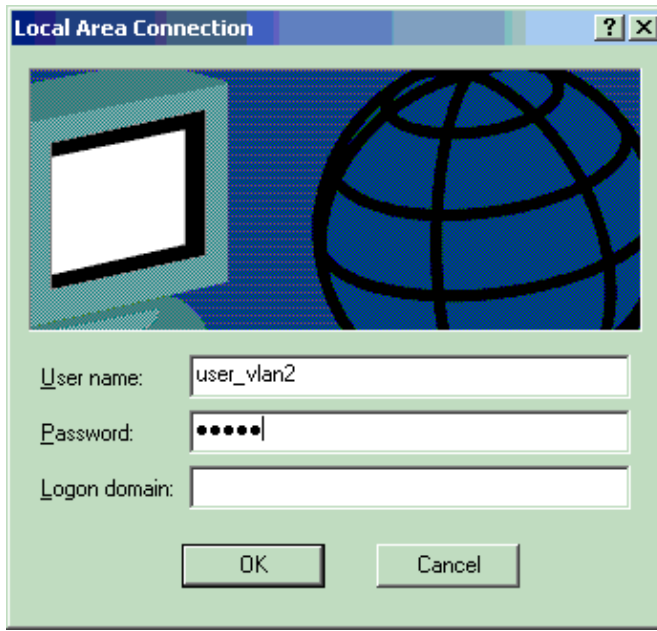
If you have correctly completed the configuration, the PC clients displays a popup prompt to enter a username and password.

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



A username and password entry window displays.

2. Enter the username and password.



- Note:** In PC 1 and 2, enter VLAN 2 user credentials. 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 the **ping** command. This is an output from PC 1, which 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

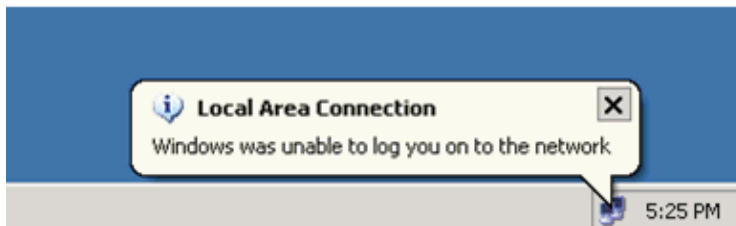
Pinging 172.16.3.2 with 32 bytes of data:

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 username and password are correct:



Catalyst 6500

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

1. Look for a port status that indicates authorized.

```
Cat6K> (enable) show port dot1x 3/1-5
```

Port	Auth-State	BEnd-State	Port-Control	Port-Status
3/1	force-authorized	idle	force-authorized	authorized

!--- This is the port to which RADIUS server is connected.

3/2	authenticated	idle	auto	authorized
3/3	authenticated	idle	auto	authorized
3/4	authenticated	idle	auto	authorized
3/5	authenticated	idle	auto	authorized

Port	Port-Mode	Re-authentication	Shutdown-timeout
3/1	SingleAuth	disabled	disabled
3/2	SingleAuth	disabled	disabled
3/3	SingleAuth	disabled	disabled
3/4	SingleAuth	disabled	disabled
3/5	SingleAuth	disabled	disabled

Verify the VLAN status after successful authentication.

```
Cat6K> (enable) show vlan
```

VLAN	Name	Status	IfIndex	Mod/Ports, Vlans
1	default	active	6	2/1-2 3/6-48
2	VLAN2	active	83	3/2-3
3	VLAN3	active	84	3/4-5
4	AUTHFAIL_VLAN	active	85	
5	GUEST_VLAN	active	86	
10	RADIUS_SERVER	active	87	3/1
1002	fddi-default	active	78	
1003	token-ring-default	active	81	
1004	fdnet-default	active	79	
1005	trnet-default	active	80	

!--- Output suppressed.

2. Verify the DHCP binding status from the routing module (MSFC) after successful authentication.

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

IP address	Hardware address	Lease expiration	Type
172.16.2.2	0100.1636.3333.9c	Feb 14 2007 03:00 AM	Automatic
172.16.2.3	0100.166F.3CA3.42	Feb 14 2007 03:03 AM	Automatic
172.16.3.2	0100.145e.945f.99	Feb 14 2007 03:05 AM	Automatic
172.16.3.3	0100.1185.8D9A.F9	Feb 14 2007 03:07 AM	Automatic

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [IEEE 802.1x Authentication with Catalyst 6500/6000 Running Cisco IOS Software Configuration Example](#)
- [Catalyst Switching and ACS Deployment Guide](#)

- **RFC 2868: RADIUS Attributes for Tunnel Protocol Support**
 - **Configuring 802.1x Authentication**
 - **LAN Product Support Pages**
 - **LAN Switching Support Page**
 - **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 19, 2007

Document ID: 81871
