Cisco IOS 소프트웨어 구성 실행 Catalyst 6500/6000을 통한 IEEE 802.1x 인증 예

목차

소개

이 문서에서는 기본 모드(수퍼바이저 엔진 및 MSFC용 단일 Cisco IOS® 소프트웨어 이미지)에서 실행되는 Catalyst 6500/6000에서 IEEE 802.1x를 구성하고 인증 및 VLAN 할당을 위해 RADIUS(Remote Authentication Dial-In User Service) 서버를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서의 독자는 다음 주제에 대해 알고 있어야 합니다.

- Windows 4.1용 Cisco Secure ACS 설치 설명서
- Cisco Secure Access Control Server 4.1 사용 설명서
- RADIUS 작동 방식
- Catalyst 스위칭 및 ACS 구축 설명서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Supervisor Engine에서 Cisco IOS Software 릴리스 12.2(18)SXF를 실행하는 Catalyst 6500**참고:** 802.1x 포트 기반 인증을 지원하려면 Cisco IOS Software 릴리스 12.1(13)E 이상이 필요합니다.
- 이 예에서는 Cisco ACS(Secure Access Control Server) 4.1을 RADIUS 서버로 사용합니다.**참고:** 스위치에서 802.1x를 활성화하려면 먼저 RADIUS 서버를 지정해야 합니다.
- 802.1x 인증을 지원하는 PC 클라이언트**참고:** 이 예에서는 Microsoft Windows XP 클라이언트를 사용합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

IEEE 802.1x 표준은 공개적으로 액세스 가능한 포트를 통해 무단 디바이스가 LAN에 연결되는 것을 제한하는 클라이언트 서버 기반 액세스 제어 및 인증 프로토콜을 정의합니다. 802.1x는 각 포트에서 두 개의 고유한 가상 액세스 포인트를 생성하여 네트워크 액세스를 제어합니다. 하나의 액세스 포인트는 제어되지 않는 포트입니다. 다른 포트는 제어 포트입니다. 단일 포트를 통과하는 모든 트래픽은 두 액세스 포인트 모두에서 사용할 수 있습니다. 802.1x는 스위치 포트에 연결된 각 사용자 디바이스를 인증하고, 스위치 또는 LAN에서 제공하는 서비스를 제공하기 전에 VLAN에 포트를 할당합니다. 디바이스가 인증될 때까지 802.1x 액세스 제어는 디바이스가 연결된 포트를 통과하는 EAPOL(Extensible Authentication Protocol over LAN) 트래픽만 허용합니다. 인증이 성공하면 일반 트래픽이 포트를 통과할 수 있습니다.

참고: 스위치가 802.1x 인증을 위해 구성되지 않은 포트에서 EAPOL 패킷을 수신하거나 스위치가 802.1x 인증을 지원하지 않는 경우 EAPOL 패킷이 삭제되고 업스트림 디바이스로 전달되지 않습니다.

구성

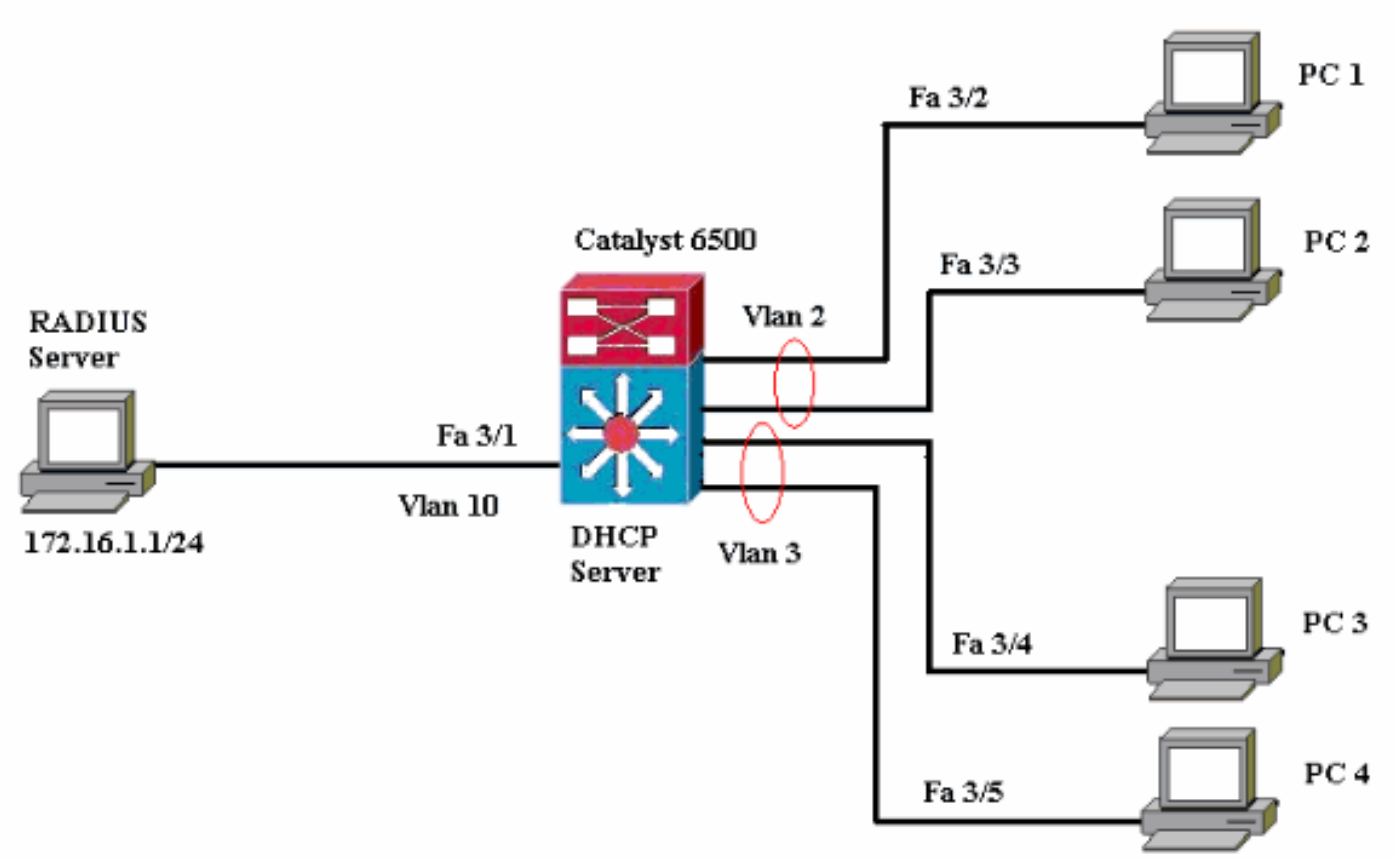
이 섹션에서는 이 문서에 설명된 802.1x 기능을 구성하는 데 필요한 정보를 제공합니다.

이 구성에는 다음 단계가 필요합니다.

- 802.1x 인증을 위한 Catalyst 스위치를 구성합니다.
- RADIUS 서버를 구성합니다.
- 802.1x 인증을 사용하도록 PC 클라이언트를 구성합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



- RADIUS 서버 - 클라이언트의 실제 인증을 수행합니다. RADIUS 서버는 클라이언트의 ID를 검증하고 클라이언트가 LAN 및 스위치 서비스에 액세스할 수 있는 권한이 있는지 여부를 스위치에 알립니다. 여기서 RADIUS 서버는 인증 및 VLAN 할당을 위해 구성됩니다.
- Switch(스위치) - 클라이언트의 인증 상태에 따라 네트워크에 대한 물리적 액세스를 제어합니다. 스위치는 클라이언트와 RADIUS 서버 간의 중간(프록시) 역할을 합니다. 클라이언트에서 ID 정보를 요청하고, RADIUS 서버를 사용하여 해당 정보를 확인하고, 클라이언트에 응답을 릴레이합니다. 여기서는 Catalyst 6500 스위치도 DHCP 서버로 구성됩니다. DHCP(Dynamic Host Configuration Protocol)에 대한 802.1x 인증 지원을 사용하면 DHCP 서버가 DHCP 검색 프로세스에 인증된 사용자 ID를 추가하여 최종 사용자의 다른 클래스에 IP 주소를 할당할 수 있습니다.
- 클라이언트 - LAN 및 스위치 서비스에 대한 액세스를 요청하고 스위치의 요청에 응답하는 장치(워크스테이션)입니다. 여기서 PC 1~4는 인증된 네트워크 액세스를 요청하는 클라이언트입니다. PC 1과 2는 VLAN 2에 있는 동일한 로그온 자격 증명을 사용합니다. 마찬가지로 PC 3과 4는 VLAN 3에 대한 로그온 자격 증명을 사용합니다. PC 클라이언트는 DHCP 서버에서 IP 주소를 얻도록 구성됩니다.

802.1x 인증을 위한 Catalyst 스위치 구성

이 샘플 스위치 컨피그레이션에는 다음이 포함됩니다.

- FastEthernet 포트에서 802.1x 인증을 활성화하는 방법.
- FastEthernet 포트 3/1을 통해 RADIUS 서버를 VLAN 10에 연결하는 방법.
- 두 IP 풀에 대한 DHCP 서버 컨피그레이션(VLAN 2의 클라이언트용, VLAN 3의 클라이언트용).
- VLAN 간 라우팅으로 인증 후 클라이언트 간 연결 가능

802.1x 인증 구성 방법에 대한 지침은 802.1x 포트 기반 인증 지침 및 제한 사항을 참조하십시오.

참고: RADIUS 서버가 항상 인증된 포트 뒤에 연결되어야 합니다.

Catalyst 6500

```
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.
```

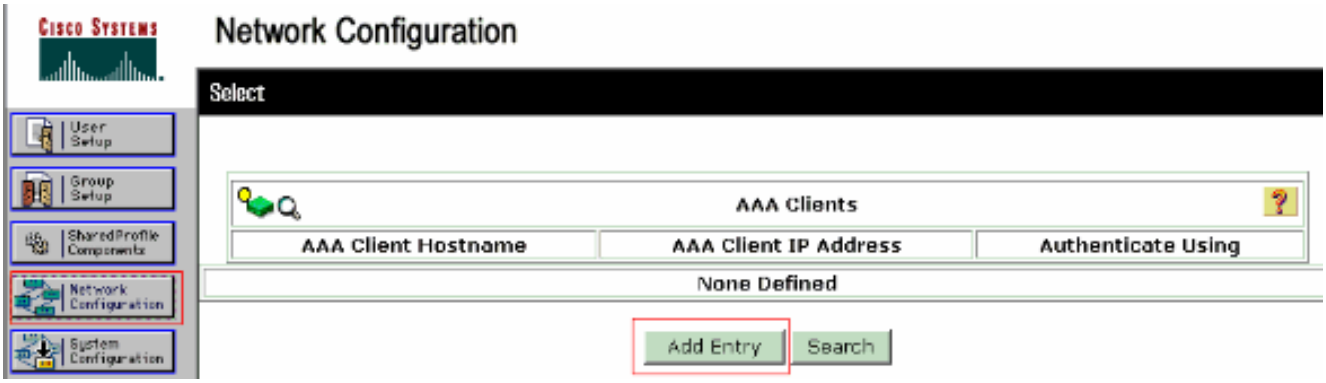
참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

RADIUS 서버 구성

RADIUS 서버는 고정 IP 주소 172.16.1.1/24으로 구성됩니다. AAA 클라이언트에 대해 RADIUS 서버를 구성하려면 다음 단계를 완료하십시오.

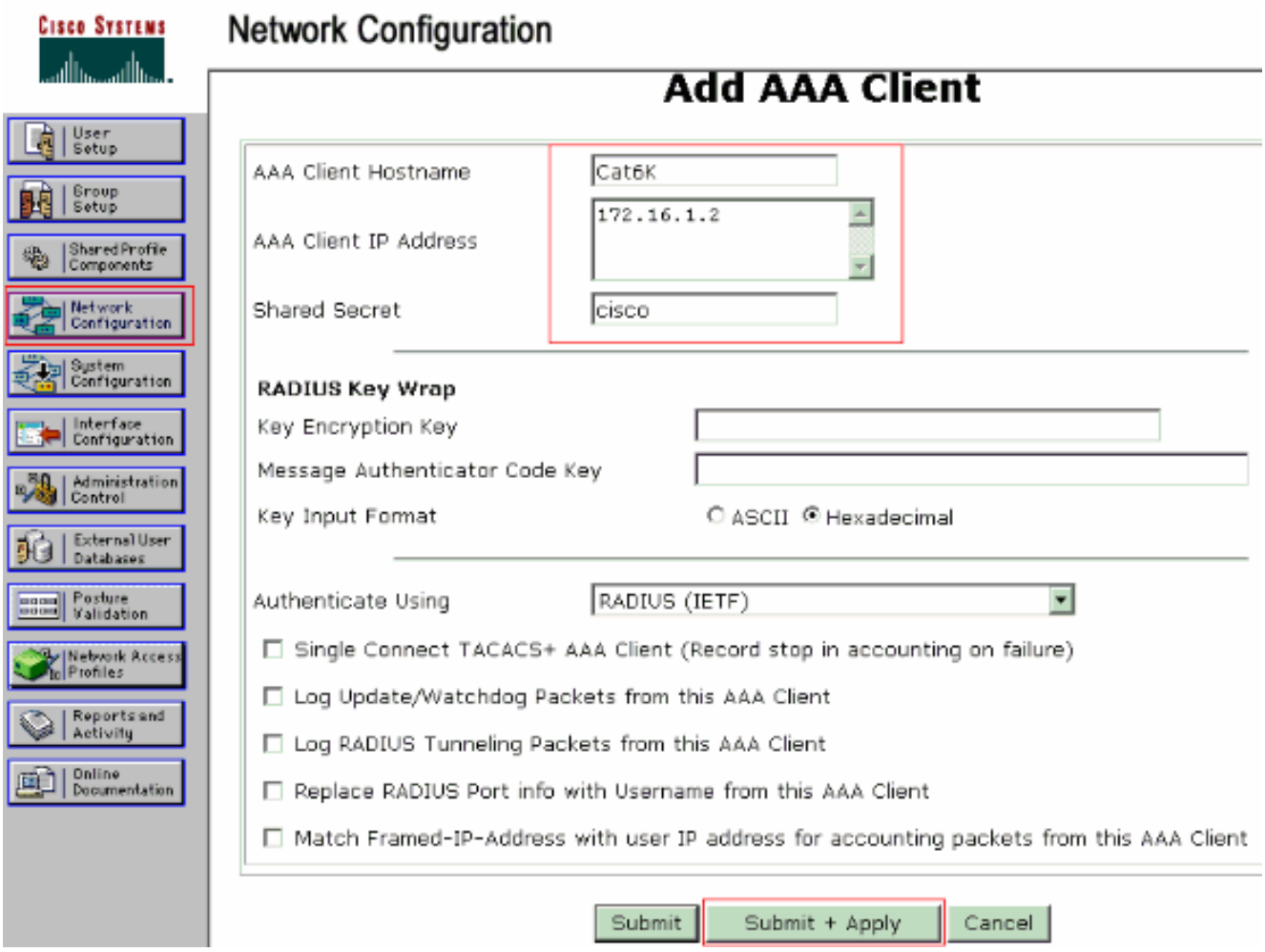
1. ACS **클라이언트**를 구성하려면 ACS 관리 창에서 네트워크 구성을 클릭합니다.
2. AAA **Clients** 섹션 아래에서 Add Entry를 클릭합니다

   .



3. 다음과 같이 AAA 클라이언트 호스트 이름, IP 주소, 공유 비밀 키 및 인증 유형을 구성합니다 .AAA 클라이언트 호스트 이름 = 스위치 호스트 이름(**Cat6K**).AAA 클라이언트 IP 주소 = 스위치의 관리 인터페이스 IP 주소(**172.16.1.2**).공유 암호 = 스위치에 구성된 RADIUS 키(**cisco**).Authenticate Using = RADIUS **IETF(를 사용하여 인증).참고:** 올바른 작동을 위해 공유 비밀 키는 AAA 클라이언트 및 ACS에서 동일해야 합니다. 키는 대/소문자를 구분합니다.
4. 다음 **예**와 같이 Submit **+ Apply**를 클릭하여 변경 사항을 적용합니다

.



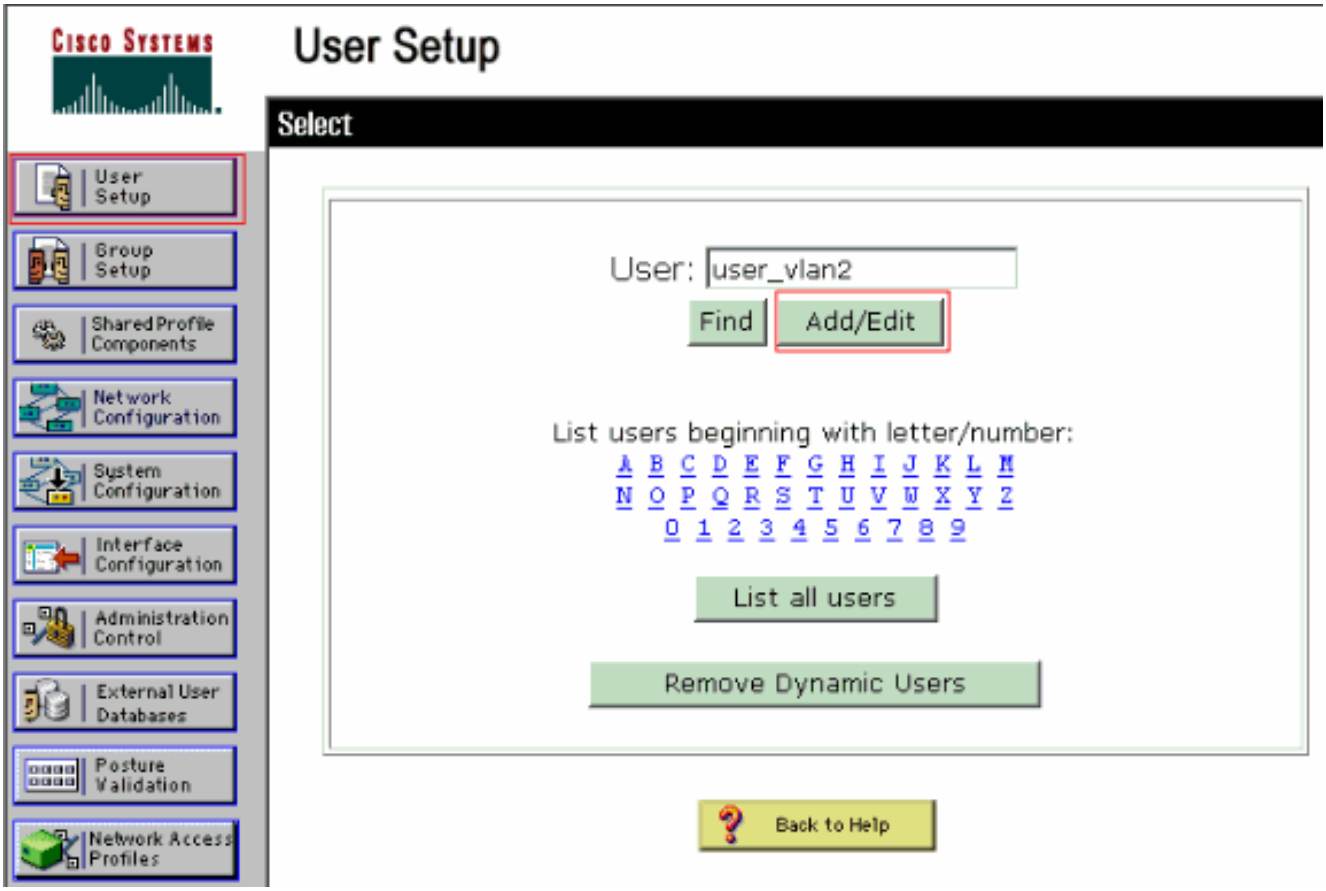
인증, VLAN 및 IP 주소 할당을 위해 RADIUS 서버를 구성하려면 다음 단계를 완료합니다.

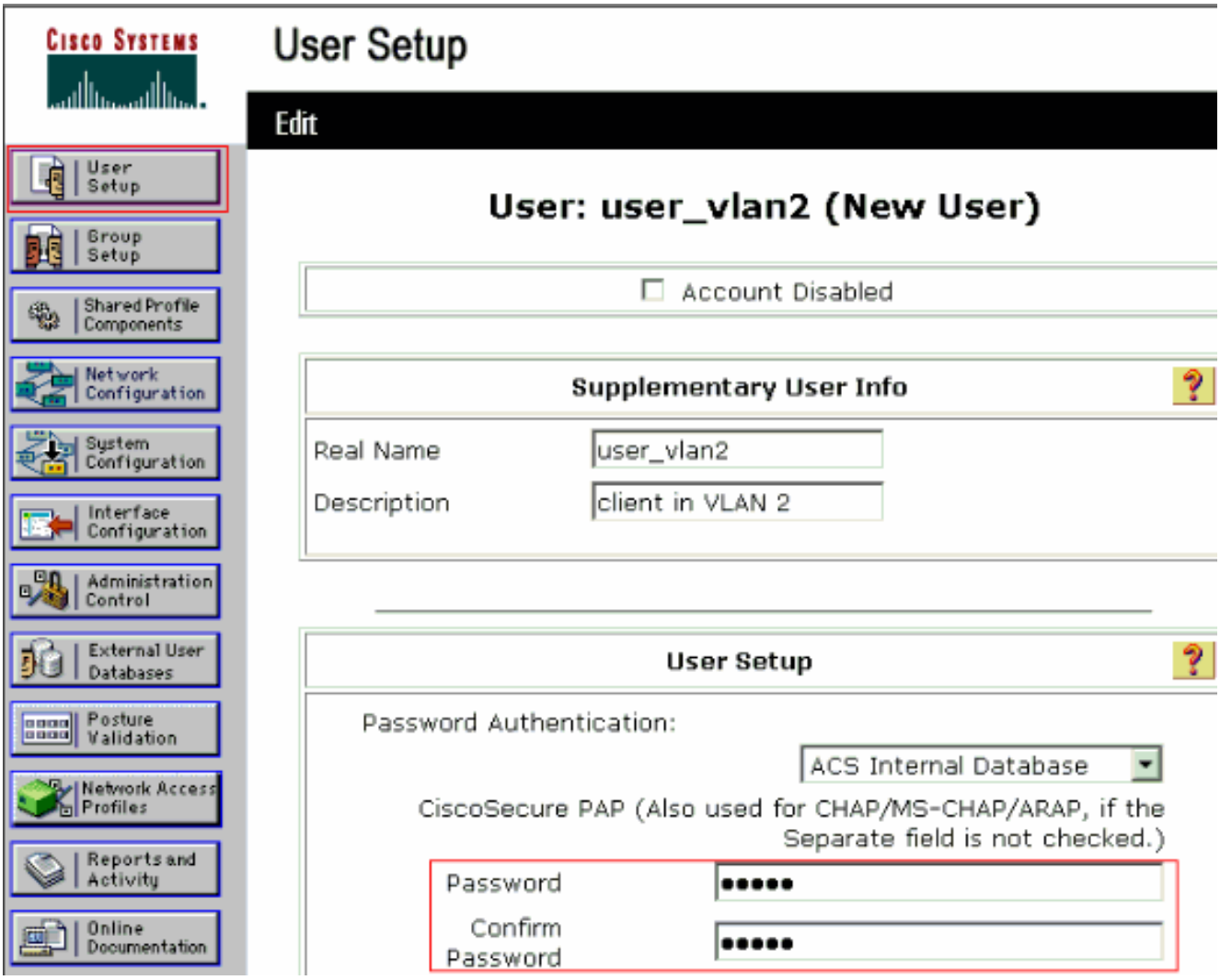
VLAN 2와 VLAN 3에 연결하는 클라이언트에 대해 두 개의 사용자 이름을 별도로 생성해야 합니다. 이 경우 VLAN 2에 연결하는 클라이언트의 user_**vlan2**와 VLAN 3에 연결하는 클라이언트의 또 다른 사용자 **user_vlan3**이 생성됩니다.

참고: 여기서는 VLAN 2에만 연결하는 클라이언트에 대한 사용자 컨피그레이션이 표시됩니다. VLAN 3에 연결하는 사용자의 경우 동일한 절차를 수행합니다.

1. 사용자를 추가 및 구성하려면 **User Setup(사용자 설정)**을 클릭하고 사용자 이름과 암호를 정의합니다

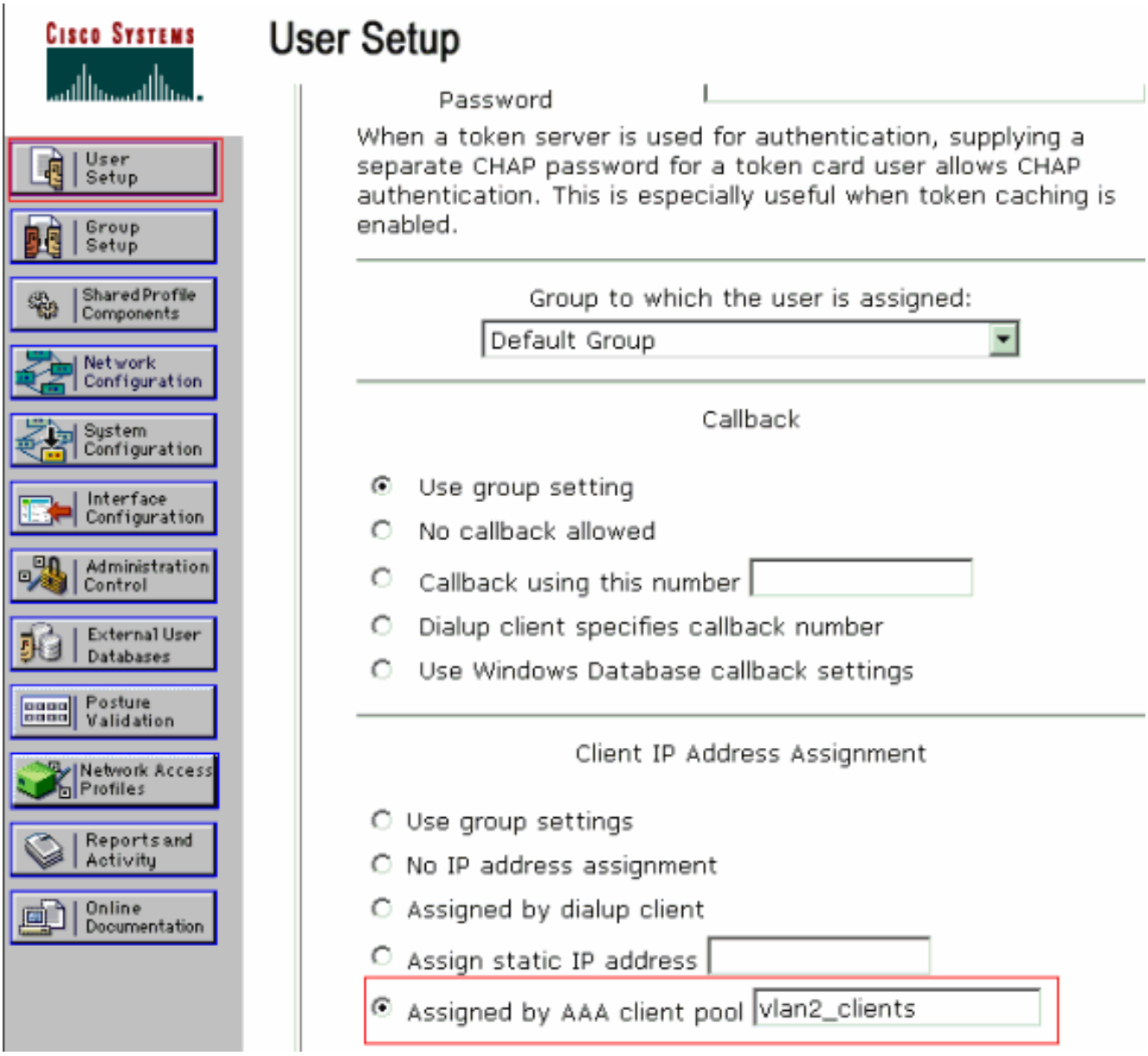
.





2. 클라이언트 IP 주소 할당을 **AAA 클라이언트 풀**에 **의해 할당됨으로 정의합니다**. VLAN 2 클라이언트에 대해 스위치에 구성된 IP 주소 풀의 이름을 입력합니다

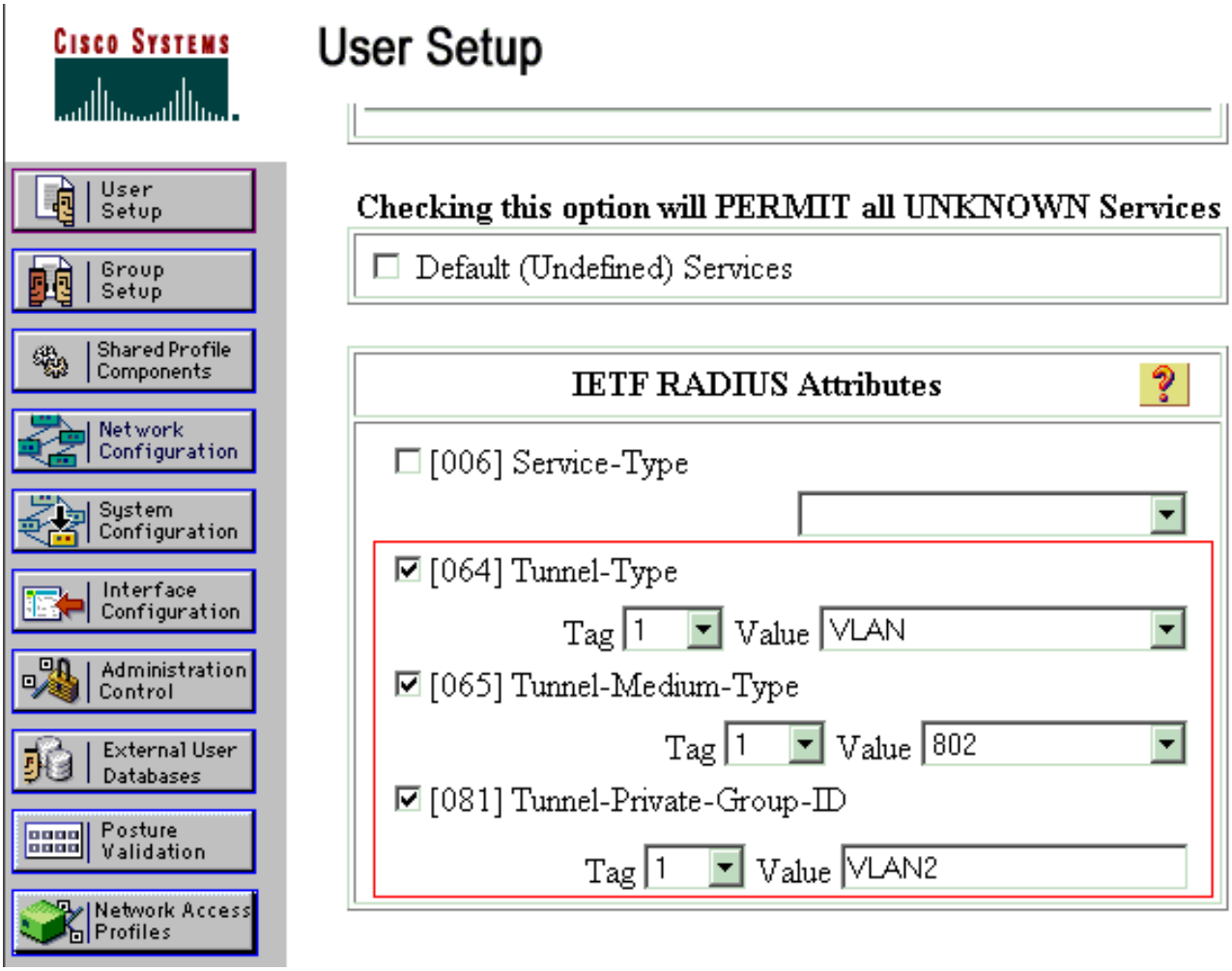
.



참고: 이 사용자가 AAA 클라이언트에 구성된 IP 주소 풀에 의해 할당된 IP 주소를 가질 경우에만 이 옵션을 선택하고 상자에 AAA 클라이언트 IP 풀 이름을 입력합니다.

3. IETF(Internet Engineering Task Force) 특성 **64** 및 **65를 정의합니다**.이 예제와 같이 값의 태그가 **1**로 설정되어 있는지 확인합니다. Catalyst는 1이 아닌 다른 태그를 무시합니다. 사용자를 특정 VLAN에 할당하려면 해당 VLAN *이름* 또는 VLAN *번호*로 특성 **81**도 정의해야 합니다.**참고:** VLAN *이름*을 사용하는 경우 스위치에 구성된 이름과 정확히 동일해야 합니다

.



참고: 이러한 IETF 특성에 대한 자세한 내용은 RFC 2868: 터널 프로토콜 지원을 위한 RADIUS 특성 .**참고:** ACS 서버의 초기 컨피그레이션에서 IETF RADIUS 특성이 **사용자 설정**에 표시되지 않을 수 있습니다. 사용자 컨피그레이션 화면에서 IETF 특성을 활성화하려면 Interface configuration(인터페이스 컨피그레이션) **> RADIUS (IETF)를** 선택합니다. 그런 다음 사용자 및 그룹 열**에서 특성 64**, **65** 및 **81**을 선택합니다.**참고:** IETF 특성 **81**을 정의하지 않고 포트가 액세스 모드의 스위치 포트인 경우 클라이언트는 포트의 액세스 VLAN에 할당됩니다. 동적 VLAN 할당에 대한 특성 **81**을 정의했으며 포트가 액세스 모드의 스위치 포트인 경우 스위치에서 aaa **authorization network default group radius** 명령을 실행해야 합니다. 이 명령은 RADIUS 서버가 제공하는 VLAN에 포트를 할당합니다. 그렇지 않으면 802.1x는 사용자 인증 후 포트를 AUTHORIZED 상태로 이동합니다. 포트가 여전히 포트의 기본 VLAN에 있으며 연결이 실패할 수 있습니다. 특성 **81**을 정의했지만 포트를 라우티드 포트로 구성한 경우 액세스 거부가 발생합니다. 다음 오류 메시지가 표시됩니다.

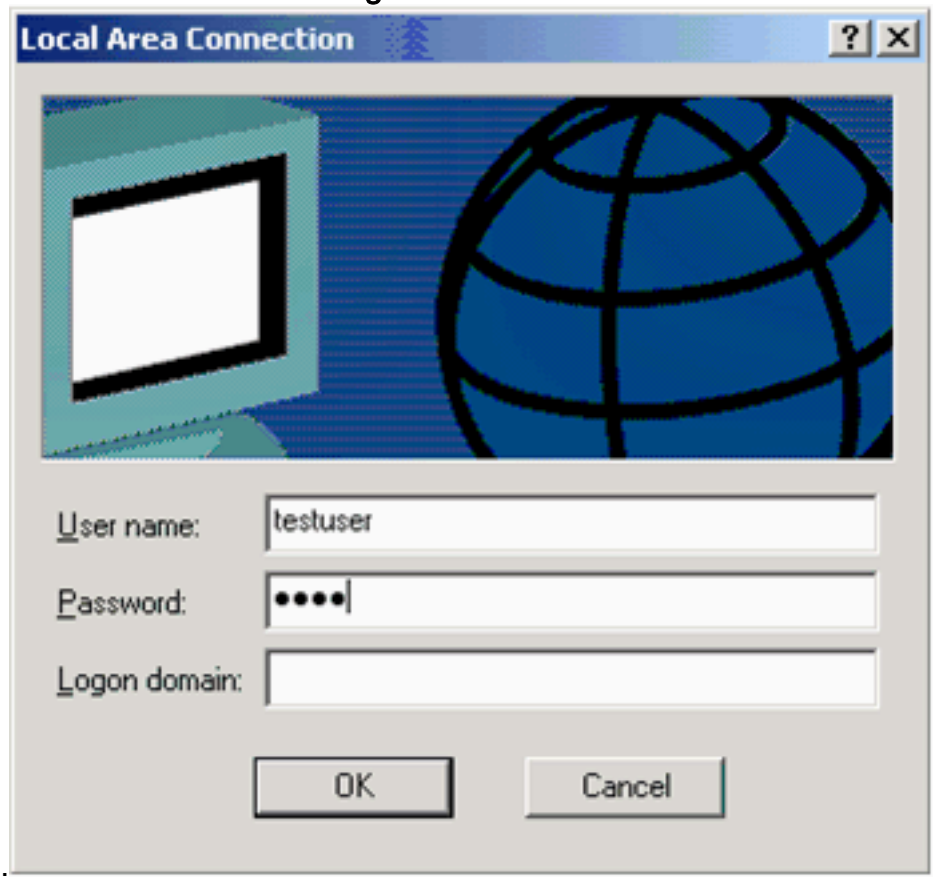
```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

802.1x 인증을 사용하도록 PC 클라이언트 구성

이 예는 Microsoft Windows XP EAP(Extensible Authentication Protocol) over LAN(EAPOL) 클라이언트에 한정되어 있습니다.

1. Start(**시작) > Control Panel(제어판) > Network Connections(네트워크 연결)를** 선택한 다음 **Local Area Connection(로컬 영역 연결)을** 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)를 선택합니다**.
2. General(**일반)** 탭 아래**에 연결된 경우 알림 영역**에 **아이콘 표시**를 선택합니다.

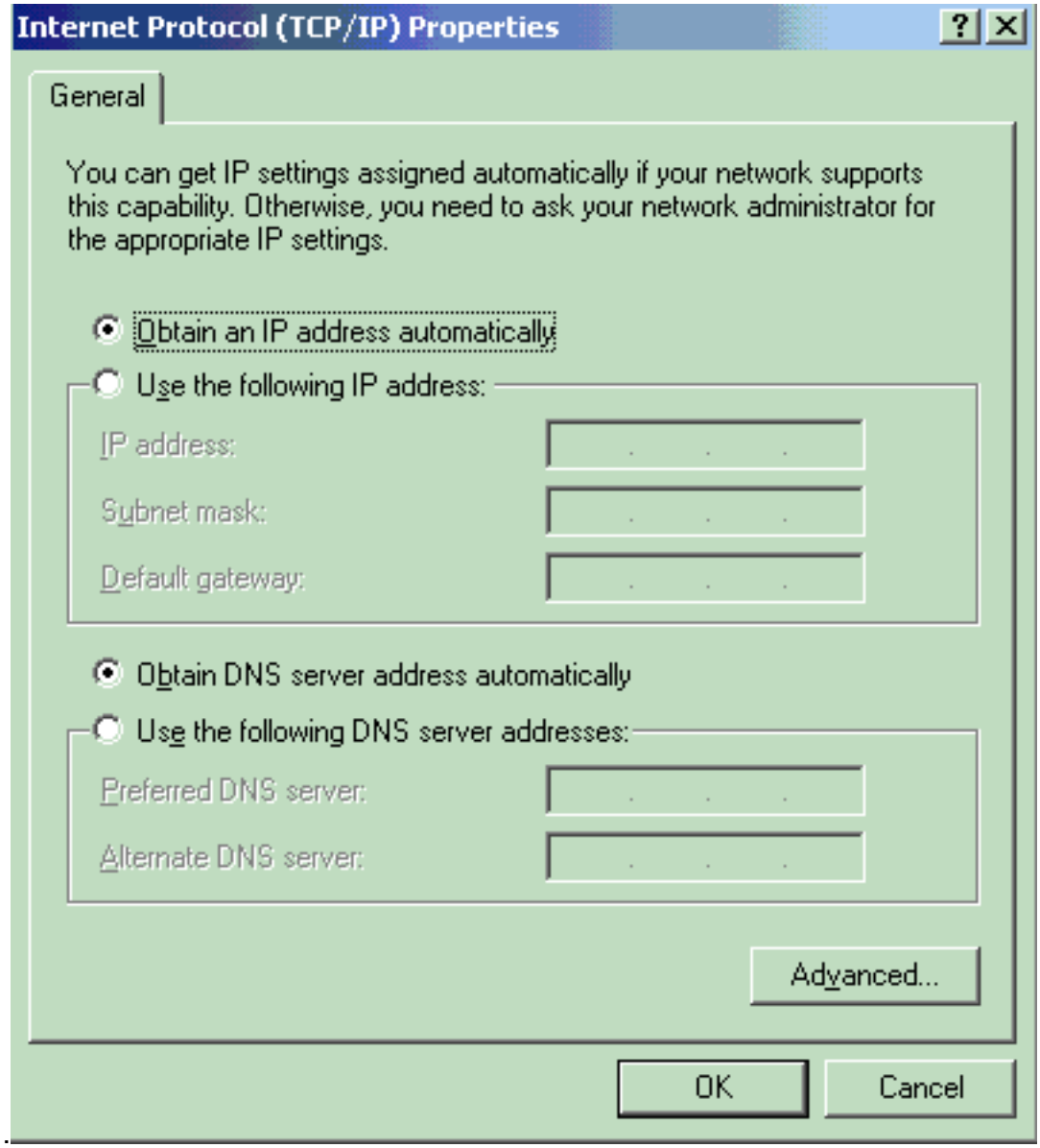
3. Authentication(인증) 탭에서 **이 네트워크에 대해 IEEE 802.1x 인증 활성화를 선택합니다**.
4. EAP 유형을 MD**5-Challenge**로 설정합니다. 이 예에서는 다음과 같습니다



.

DHCP 서버에서 IP 주소를 얻도록 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. Start(**시작) > Control Panel(제어판) > Network Connections(네트워크 연결)를** 선택한 다음 **Local Area Connection(로컬 영역 연결)을** 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)를 선택합니다**.
2. General(일반) 탭에서 **인터넷 프로토콜(TCP/IP)을** 클릭한 다음 **속성을 클릭합니다**.
3. Obtain **an IP address automatically를 선택합니다**

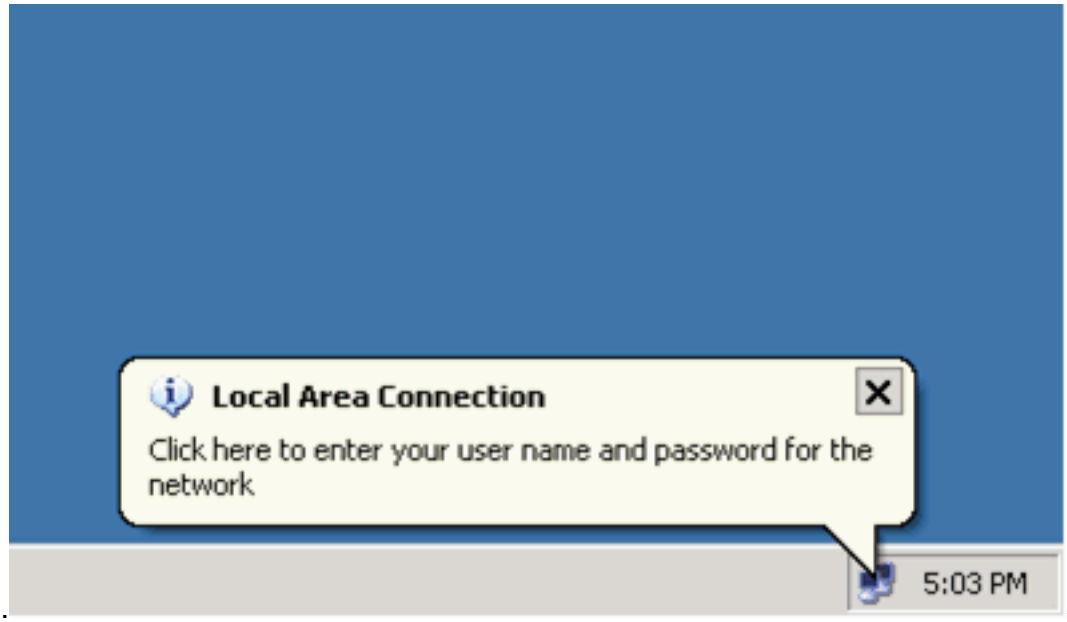


다음을 확인합니다.

PC 클라이언트

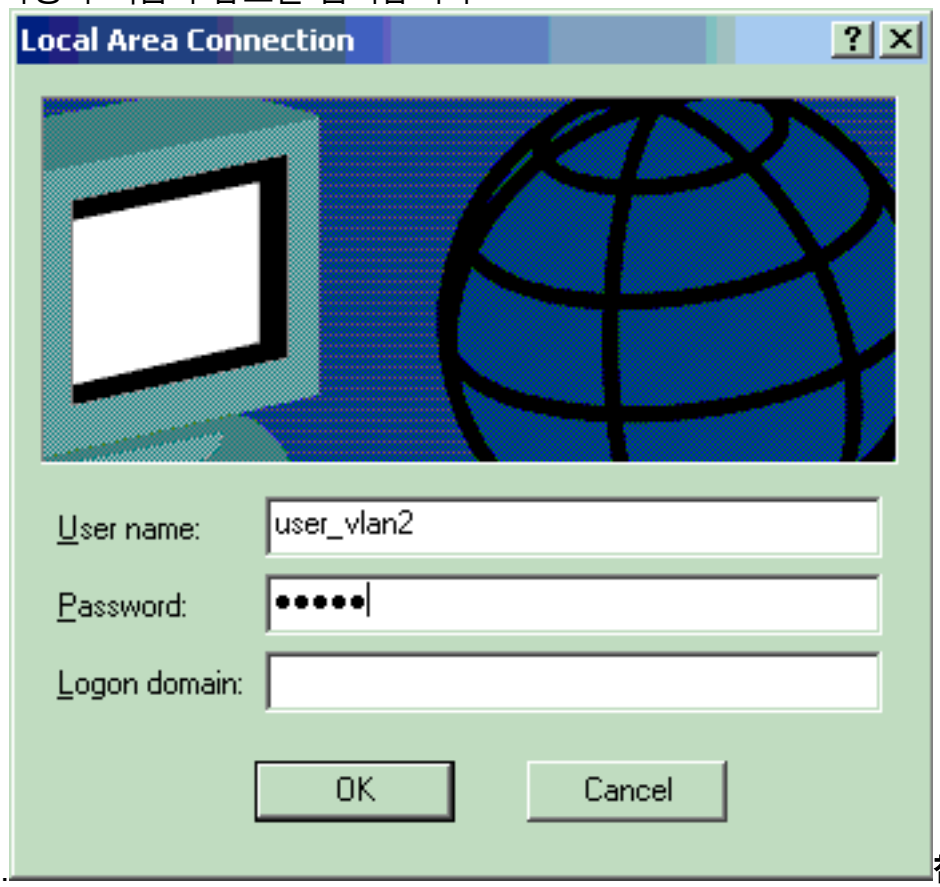
컨피그레이션을 올바르게 완료한 경우 PC 클라이언트에는 사용자 이름과 비밀번호를 입력하라는 팝업 프롬프트가 표시됩니다.

1. 다음 예에서는 프롬프트를 클릭합니다



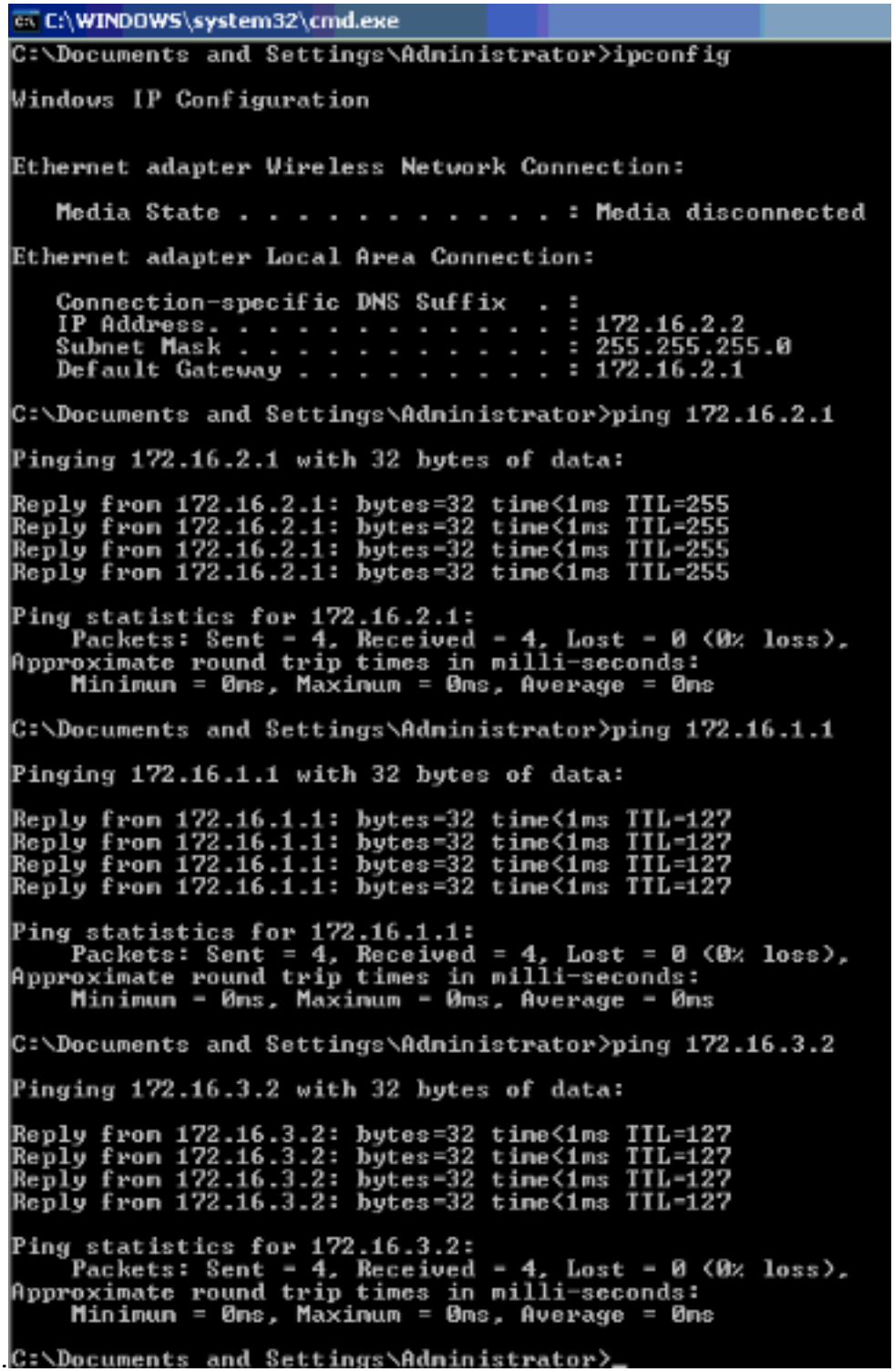
. 사용자 이름 및 비밀번호 입력 창이 표시됩니다.

2. 사용자 이름과 암호를 입력합니다

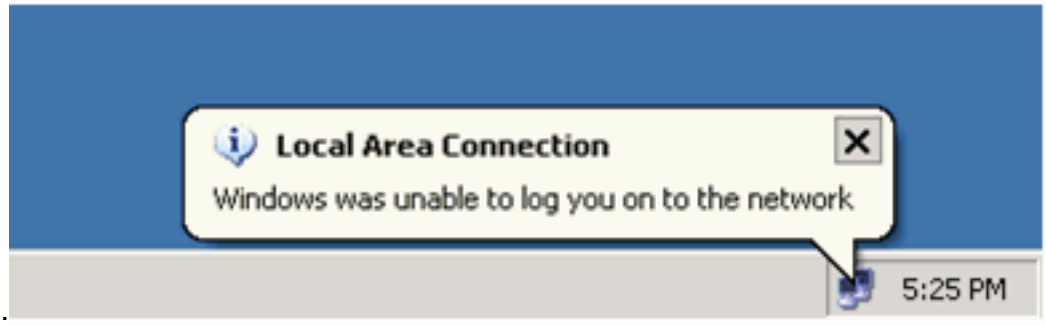


. **참고:** PC 1 및 2에서 VLAN 2 사용자 자격 증명을 입력하고 PC 3 및 4에 VLAN 3 사용자 자격 증명을 입력합니다.

3. 오류 메시지가 나타나지 않으면 네트워크 리소스 액세스 및 ping과 같은 일반적인 방법과의 연결을 **확인합니다**. 이 출력은 PC 1의 것이며 PC 4에 대한 성공적인 **ping**을 보여줍니다



이 오류가 나타나면 사용자 이름과 암호가 올바른지 확인합니다



Catalyst 6500

암호와 사용자 이름이 올바른 경우 스위치에서 802.1x 포트 상태를 확인합니다.

1. AUTHORIZED를 나타내는 포트 상태를 .

```
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
```

인증 성공 후 VLAN 상태를 확인합니다.

```
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. 인증 성공 후 에서 DHCP 바인딩 상태를 확인합니다.

```
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
```

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

문제 해결을 위해 다음 **debug** 명령의 출력을 수집합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug dot1x events** - dot1x 이벤트 플래그가 지정된 print 문의 디버깅을 활성화합니다.

```
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** - RADIUS와 관련된 정보를 표시합니다.

```
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 FFFFFFFE 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#
```

관련 정보

- Catalyst 6500/6000을 통한 IEEE 802.1x 인증 CatOS 소프트웨어 구성 예
- Cisco Catalyst 스위치 환경에서 Windows NT/2000 서버용 Cisco Secure ACS 구축 지침
- RFC 2868: 터널 프로토콜 지원을 위한 RADIUS 특성
- IEEE 802.1X 포트 기반 인증 구성
- LAN 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems