

# Cisco Catalyst Layer 3 Fixed Configuration Switches **컨피그레이션의 IEEE 802.1x 다중 도메인 인증 예**

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[관련 제품](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[802.1x 다중 도메인 인증을 위한 Catalyst 스위치 구성](#)

[RADIUS 서버 구성](#)

[802.1x 인증을 사용하도록 PC 클라이언트 구성](#)

[802.1x 인증을 사용하도록 IP 전화 구성](#)

[다음을 확인합니다.](#)

[PC 클라이언트](#)

[IP 전화](#)

[레이어 3 스위치](#)

[문제 해결](#)

[IP Phone 인증 실패](#)

[관련 정보](#)

## [소개](#)

다중 도메인 인증을 사용하면 IP Phone과 PC가 동일한 스위치 포트에서 인증하는 동시에 해당 음성 및 데이터 VLAN에 배치할 수 있습니다. 이 문서에서는 Cisco Catalyst Layer 3 고정 구성 스위치에서 IEEE 802.1x MDA(Multi-Domain Authentication)를 구성하는 방법에 대해 설명합니다.

## [사전 요구 사항](#)

### [요구 사항](#)

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- [RADIUS 작동 방식](#)

- [Catalyst 스위칭 및 ACS 구축 설명서](#)
- [Cisco Secure Access Control Server 4.1 사용 설명서](#)
- [Cisco Unified IP Phone 개요](#)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS<sup>®</sup> Software 릴리스 12.2(37)SE1을 실행하는 Cisco Catalyst 3560 Series 스위치**참고:** 다중 도메인 인증 지원은 Cisco IOS Software Release 12.2(35)SE 이상에서만 사용할 수 있습니다.
- 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.
- Cisco Unified IP Phone 7970G with SCCP 펌웨어 버전 8.2(1)
- Cisco Unified IP Phone 7961G with SCCP 펌웨어 버전 8.2(2)
- Cisco Unified Communications Manager(Cisco CallManager) 4.1(3)sr2가 포함된 MCS(Media Coverage Server)

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.

## 관련 제품

이 컨피그레이션은 다음 하드웨어 제품에서도 사용할 수 있습니다.

- Cisco Catalyst 3560-E Series 스위치
- Cisco Catalyst 3750 Series 스위치
- Cisco Catalyst 3750-E Series 스위치

**참고:** Cisco Catalyst 3550 Series 스위치는 802.1x 멀티 도메인 인증을 지원하지 않습니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

## 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 서로 다른 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.

802.1x는 세 가지 기본 구성 요소로 구성됩니다. 각각 PAE(Port Access Entity)라고 합니다.

- 서플리컨트 - 네트워크 액세스를 요청하는 클라이언트 장치 (예: IP 전화 및 연결된 PC)
- Authenticator - Cisco Catalyst 3560과 같이 신청자 권한 부여 요청을 지원하는 네트워크 디바이스
- Authentication Server(인증 서버) - 인증 서비스를 제공하는 RADIUS(Remote Authentication Dial-in User Server)(예: Cisco Secure Access Control Server)

Cisco Unified IP Phone에는 802.1X 신청자도 포함되어 있습니다. 이 신청자를 사용하면 네트워크 관리자가 LAN 스위치 포트에 대한 IP Phone 연결을 제어할 수 있습니다. IP Phone 802.1X 신청자의 초기 릴리스는 802.1X 인증을 위한 EAP-MD5 옵션을 구현합니다. 다중 도메인 컨피그레이션에서는 IP Phone과 연결된 PC가 사용자 이름 및 비밀번호 사양에 따라 네트워크에 대한 액세스를 독립적으로 요청해야 합니다. 인증자 디바이스에는 RADIUS의 특성 정보가 필요할 수 있습니다. 특성은 특정 VLAN에 대한 액세스가 신청자에 대해 허용되는지 여부와 같은 추가 권한 부여 정보를 지정합니다. 이러한 특성은 공급업체별로 지정할 수 있습니다. Cisco는 인증자(Cisco Catalyst 3560)에게 (IP Phone)가 음성 VLAN에서 허용됨을 알리기 위해 RADIUS 특성 `cisco-av` 을 사용합니다.

## 구성

이 섹션에서는 이 문서에 설명된 802.1x 다중 도메인 인증 기능을 구성하는 정보를 제공합니다.

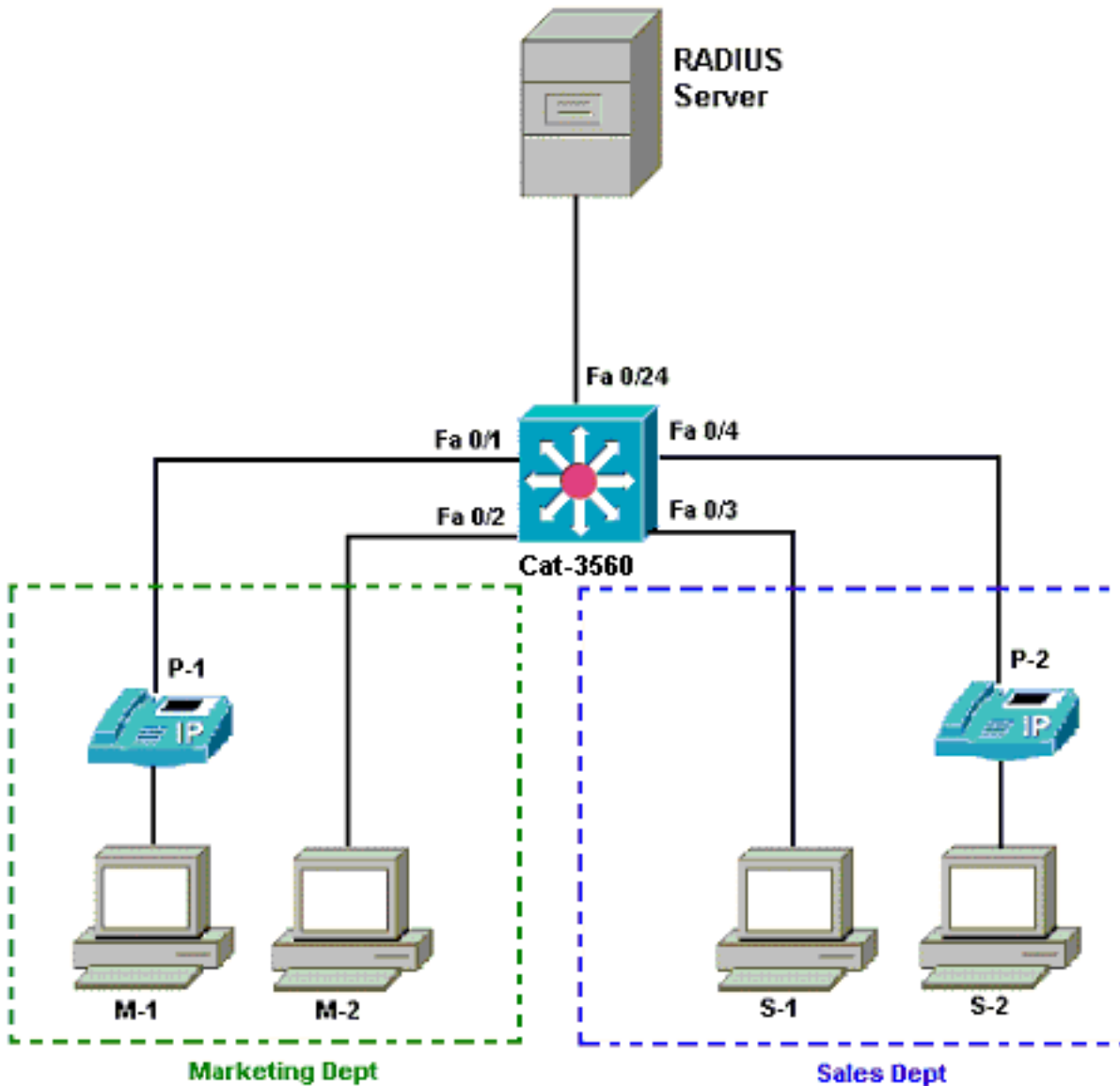
이 구성에는 다음 단계가 필요합니다.

- [802.1x 멀티 도메인 인증을 위한 Catalyst 스위치를 구성합니다.](#)
- [RADIUS 서버를 구성합니다.](#)
- [802.1x 인증을 사용하도록 PC 클라이언트를 구성합니다.](#)
- [802.1x 인증을 사용하도록 IP Phone을 구성합니다.](#)

**참고:** 이 문서에 사용된 명령에 대한 자세한 내용을 보려면 [명령 조회 도구](#)([등록된 고객만 해당](#))를 사용하십시오.

## 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. 여기에서 Cisco ACS는 인증 및 VLAN 할당을 위해 MCS(Media Coverage Server)에 설치 및 구성됩니다. MCS는 TFTP 서버 및 IP Phone용 Cisco Unified Communications Manager(Cisco CallManager)이기도 합니다.
- 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 3560 스위치도 DHCP 서버로 구성됩니다. DHCP(Dynamic Host Configuration Protocol)에 대한 802.1x 인증 지원을 사용하면 DHCP 서버가 IP 주소를 다른 최종 사용자 클래스에 할당할 수 있습니다. 이를 위해 인증된 사용자 ID를 DHCP 검색 프로세스에 추가합니다. 포트 FastEthernet 0/1 및 0/4는 802.1x 다중 도메인 인증을 위해 구성된 유일한 포트입니다. 포트 FastEthernet 0/2 및 0/3은 기본 802.1x 단일 호스트 모드입니다. 포트 FastEthernet 0/24는 RADIUS 서버에 연결됩니다. **참고:** 외부 DHCP 서버를 사용하는 경우 클라이언트가 있는 SVI(vlan) 인터페이스에서 DHCP 서버를 가리키는 **ip helper-address** 명령을 추가해야 합니다.
- 클라이언트 - LAN 및 스위치 서비스에 대한 액세스를 요청하고 스위치의 요청에 응답하는 장치(예: IP 전화 또는 워크스테이션)입니다. 여기서 클라이언트는 DHCP 서버에서 IP 주소를 얻기 위해 구성됩니다. 디바이스 M-1, M-2, S-1 및 S-2는 네트워크에 대한 액세스를 요청하는 워크스

테이션 클라이언트입니다.P-1 및 P-2는 네트워크에 대한 액세스를 요청하는 IP Phone 클라이언트입니다.M-1, M-2 및 P-1은 마케팅 부서의 클라이언트 디바이스입니다.S-1, S-2 및 P-2는 영업 부서의 클라이언트 디바이스입니다.IP Phone P-1 및 P-2는 동일한 음성 VLAN(VLAN 3)에 있도록 구성됩니다. 워크스테이션 M-1과 M-2는 성공적인 인증 후 동일한 데이터 VLAN(VLAN 4)에 있도록 구성됩니다.Workstation S-1 및 S-2는 성공적인 인증 후 동일한 데이터 VLAN(VLAN 5)에 있도록 구성됩니다.참고: 데이터 디바이스에 대해서만 RADIUS 서버에서 동적 VLAN 할당을 사용할 수 있습니다.

## 802.1x 다중 도메인 인증을 위한 Catalyst 스위치 구성

이 샘플 스위치 컨피그레이션에는 다음이 포함됩니다.

- 스위치 포트에서 802.1x 다중 도메인 인증을 활성화하는 방법
- RADIUS 서버 관련 컨피그레이션
- IP 주소 할당을 위한 DHCP 서버 구성
- 인증 후 클라이언트 간 연결을 위한 VLAN 간 라우팅

MDA 구성 방법에 대한 지침은 Using Multidomain Authentication을 참조하십시오.

참고: RADIUS 서버가 항상 인증된 포트 뒤에 연결되어야 합니다.

참고: 여기에 관련 컨피그레이션만 표시됩니다.

### Cat-3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
!--- Sets the hostname for the switch. Cat-
3560(config)#vlan 2
Cat-3560(config-vlan)#name SERVER
Cat-3560(config-vlan)#vlan 3
Cat-3560(config-vlan)#name VOICE
Cat-3560(config-vlan)#vlan 4
Cat-3560(config-vlan)#name MARKETING
Cat-3560(config-vlan)#vlan 5
Cat-3560(config-vlan)#name SALES
Cat-3560(config-vlan)#vlan 6
Cat-3560(config-vlan)#name GUEST_and_AUTHFAIL
!--- VLAN should already exist in the switch for a
successful authentication. Cat-3560(config-vlan)#exit
Cat-3560(config)#interface vlan 2
Cat-3560(config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for the RADIUS Server.
Cat-3560(config-if)#interface vlan 3
Cat-3560(config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for IP Phone clients in
VLAN 3. Cat-3560(config-if)#interface vlan 4
Cat-3560(config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
4. Cat-3560(config-if)#interface vlan 5
Cat-3560(config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
5. Cat-3560(config-if)#exit
```

```

Cat-3560(config)#ip routing
!--- Enables IP routing for interVLAN routing. Cat-
3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#shut
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
!--- This is a dedicated VLAN for the RADIUS server.
Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 ,
fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
!--- You must configure the voice VLAN for the IP phone
when the !--- host mode is set to multidomain. !---
Note: If you use a dynamic VLAN in order to assign a
voice VLAN !--- on an MDA-enabled switch port, the voice
device fails authorization.

Cat-3560(config-if-range)#dot1x port-control auto
!--- Enables IEEE 802.1x authentication on the port.
Cat-3560(config-if-range)#dot1x host-mode multi-domain
!--- Allow both a host and a voice device to be !---
authenticated on an IEEE 802.1x-authorized port. Cat-
3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
!--- The guest VLAN and restricted VLAN features only
apply to the data devices !--- on an MDA enabled port.
Cat-3560(config-if-range)#dot1x reauthentication
!--- Enables periodic re-authentication of the client.
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
!--- Set the number of seconds between re-authentication
attempts. Cat-3560(config-if-range)#dot1x auth-fail max-
attempts 2
!--- Specifies the number of authentication attempts to
allow !--- before a port moves to the restricted VLAN.
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
!--- By default a 802.1x authorized port allows only a
single client. Cat-3560(config-if-range)#dot1x guest-
vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- This pool assigns ip address for IP Phones. !---
Option 150 is for the TFTP server. Cat-3560(dhcp-
config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- This pool assigns ip address for PC clients in
Marketing Dept. Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
!--- This pool assigns ip address for PC clients in

```

```

Sales Dept. Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1
Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group
radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat-3560(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat-3560(config)#radius-server host
172.16.2.201 key Cisco123
!--- The key must match the key used on the RADIUS
server. Cat-3560(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat-3560(config)#interface
range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

```


VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Gi0/1, Gi0/2
2 SERVER	active	Fa0/24
3 VOICE	active	Fa0/1, Fa0/4
4 MARKETING	active	
5 SALES	active	
6 GUEST_and_AUTHFAIL	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

**참고:** 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 [명령 조회 도구](#)(등록된 고객만 해당)를 사용하십시오.

## RADIUS 서버 구성

RADIUS 서버는 고정 IP 주소 172.16.2.201/24으로 구성됩니다. AAA 클라이언트에 대해 RADIUS 서버를 구성하려면 다음 단계를 완료하십시오.

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



# Network Configuration

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture

### AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		
<input type="button" value="Add Entry"/> <input type="button" value="Search"/>		

### AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">CCM-4</a>	172.16.2.201	CiscoSecure ACS

3. 다음과 같이 AAA 클라이언트 호스트 이름, IP 주소, 공유 비밀 키 및 인증 유형을 구성합니다.  
 .AAA 클라이언트 호스트 이름 = 스위치 호스트 이름(Cat-3560).AAA 클라이언트 IP 주소 = 스위치의 관리 인터페이스 IP 주소(172.16.2.1).공유 암호 = 스위치에 구성된 RADIUS 키 (CisCo123).참고: 올바른 작동을 위해 공유 비밀 키는 AAA 클라이언트 및 ACS에서 동일해야 합니다.키는 대/소문자를 구분합니다.다음을 사용하여 인증 = RADIUS(Cisco IOS/PIX 6.0).참고: 이 옵션에서는 Cisco AV(Attribute-Value) 쌍 특성을 사용할 수 있습니다.
4. 다음 예와 같이 변경 사항을 적용하려면 Submit + Apply를 클릭합니다



### Add AAA Client

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration**
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

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

**그룹 설정**

인증을 위해 RADIUS 서버를 구성하려면 이 표를 참조하십시오.

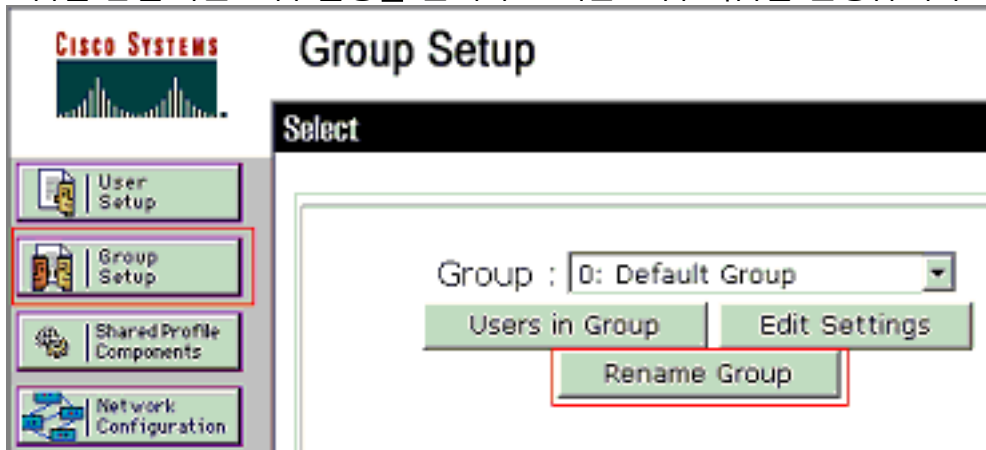
장치	부서	그룹	사용자	비밀번호	VLAN	DH CP 풀
M-1	마케팅	마케팅	mkt 관리자	Cisco	마케팅	마케팅
M-2	마케팅	마케팅	mkt 직원	MScisco	마케팅	마케팅
S-2	영업	영업	영업 관리자	SMcisco	영업	영업
S-1	영업	영업	영업 직원	시스코	영업	영업

P-1	마케팅	IP 전화	CP-7970G-SEP001759E7492C	P1cisco	음성	IP 전화
P-2	영업	IP 전화	CP-7961G-SEP001A2F80381F	P2cisco	음성	IP 전화

VLAN 3(VOICE), 4(MARKETING) 및 5(SALES)에 연결하는 클라이언트의 그룹을 생성합니다. 여기서는 IP Phone, 마케팅 및 영업을 이러한 목적으로 그룹화합니다.

**참고:** 이는 마케팅 및 IP 전화 그룹의 구성입니다. 영업 그룹 컨피그레이션의 경우 마케팅 그룹에 대한 단계를 완료합니다.

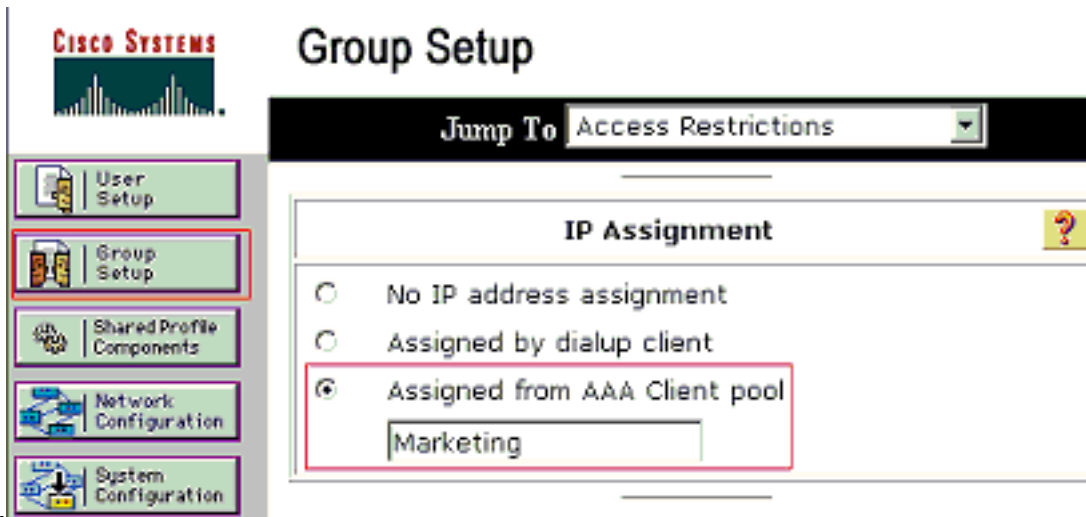
1. 그룹을 만들려면 그룹 설정을 선택하고 기본 그룹 이름을 변경합니다



2. 그룹을 구성하려면 목록에서 그룹을 선택하고 Edit Settings(설정 편집)를 클릭합니다



3. 클라이언트 IP 주소 할당을 AAA 클라이언트 풀에 의해 할당됨으로 정의합니다. 이 그룹 클라이언트에 대해 스위치에 구성된 IP 주소 풀의 이름을 입력합니다



**참고:** 이 사용자

가 AAA 클라이언트에 구성된 IP 주소 풀에 의해 할당된 IP 주소를 가질 경우에만 이 옵션을 선택하고 상자에 AAA 클라이언트 IP 풀 이름을 입력합니다. **참고:** IP Phone 그룹 컨피그레이션만 사용하려면 다음 단계, 4단계를 건너뛰고 5단계로 이동하십시오.

4. IETF(Internet Engineering Task Force) 특성 **64**, **65** 및 **81**을 정의한 다음 **Submit + Restart**를 클릭합니다. 이 예제와 같이 값의 태그가 1로 설정되어 있는지 확인합니다. Catalyst는 1이 아닌 다른 태그를 무시합니다. 사용자를 특정 VLAN에 할당하려면 해당 VLAN 이름 또는 VLAN 번호로 특성 **81**도 정의해야 합니다. **참고:** VLAN 이름을 사용하는 경우 스위치에 구성된 이름과 정확히 동일해야 합니다

Jump To Access Restrictions

---

### IETF RADIUS Attributes

[064] Tunnel-Type  
 Tag 1 Value VLAN

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

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

[Back to Help](#)

참고: [RFC](#)

[2868](#)을 참조하십시오. 이러한 IETF 특성에 대한 자세한 내용은 [터널 프로토콜 지원 RADIUS 특성을 참조하십시오](#). 참고: ACS 서버의 초기 컨피그레이션에서 IETF RADIUS 특성이 사용자 설정에 표시되지 않을 수 있습니다. 사용자 컨피그레이션 화면에서 IETF 특성을 활성화하려면 Interface configuration(인터페이스 컨피그레이션) > RADIUS (IETF)를 선택합니다. 그런 다음 사용자 및 그룹 열에서 특성 64, 65 및 81을 선택합니다. 참고: IETF 특성 81을 정의하지 않고 포트가 액세스 모드의 스위치 포트이면 클라이언트는 포트의 액세스 VLAN에 할당됩니다. 동적 VLAN 할당에 대한 특성 81을 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. 참고: 다음 단계는 IP Phone 그룹에만 적용됩니다.

- 음성 장치에 권한을 부여할 Cisco AV(Attribute-Value) 쌍 특성을 전송하도록 RADIUS 서버를 구성합니다. 이 기능이 없으면 스위치는 음성 디바이스를 데이터 디바이스로 취급합니다. Cisco AV(Attribute-Value) 쌍 특성을 `device-traffic-class=voice` 값으로 정의하고 Submit +Restart를 클릭합니다



## Group Setup

Jump To Access Restrictions

- User Setup
- Group Setup**
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

### IP Assignment

- No IP address assignment
- Assigned by dialup client
- Assigned from AAA Client pool

IP-Phones

### Cisco IOS/PIX 6.x RADIUS Attributes

[009\001] cisco-av-pair

device-traffic-class=voice

[009\101] cisco-h323-credit-amount

[009\102] cisco-h323-credit-time

[009\103] cisco-h323-return-code

Submit

**Submit + Restart**

Cancel

## 사용자 설정

사용자를 추가 및 구성하려면 다음 단계를 완료합니다.

1. 사용자를 추가하고 구성하려면 User Setup(사용자 설정)을 선택합니다. 사용자 이름을 입력하고 Add/Edit(추가/수정)를 클릭합니다



# User Setup

Select

















- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

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](#)

2. 사용자의 사용자 이름, 비밀번호 및 그룹을 정의합니다

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

## User: mkt-manager (New User)

Account Disabled

### User Setup

Password Authentication:

ACS Internal Database 

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

Password   
 Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password   
 Confirm 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:

Marketing 

Callback

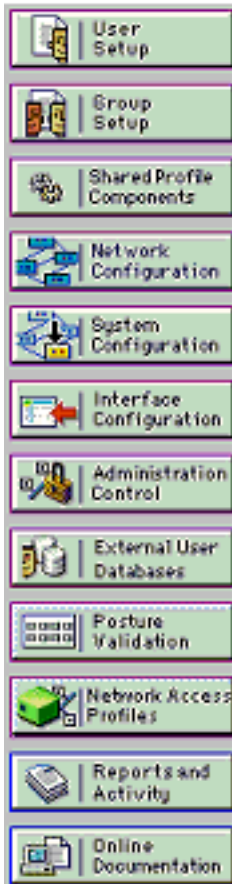
Use group setting

Submit

Delete

Cancel

3. IP Phone은 디바이스 ID를 사용자 이름으로 사용하고 공유 암호를 인증 비밀번호로 사용합니다. 이러한 값은 RADIUS 서버에서 일치해야 합니다. IP Phones P-1 및 P-2의 경우 구성된 공유 암호와 동일한 디바이스 ID 및 비밀번호와 동일한 사용자 이름을 생성합니다. IP Phone의 [Device ID](#) 및 Shared Secret에 대한 자세한 내용은 [Configure the IP Phones to Use 802.1x Authentication\(802.1x 인증을 사용하도록 IP 전화기 구성\)](#) 섹션을 참조하십시오



**User: CP-7961G-SEP001A2F80381F**

Account Disabled

## User Setup

Password Authentication:

ACS Internal Database

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

Password \*\*\*\*\*

Confirm Password \*\*\*\*\*

Separate (CHAP/MS-CHAP/ARAP)

Password \*\*\*\*\*

Confirm 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:

IP Phones

Submit

Delete

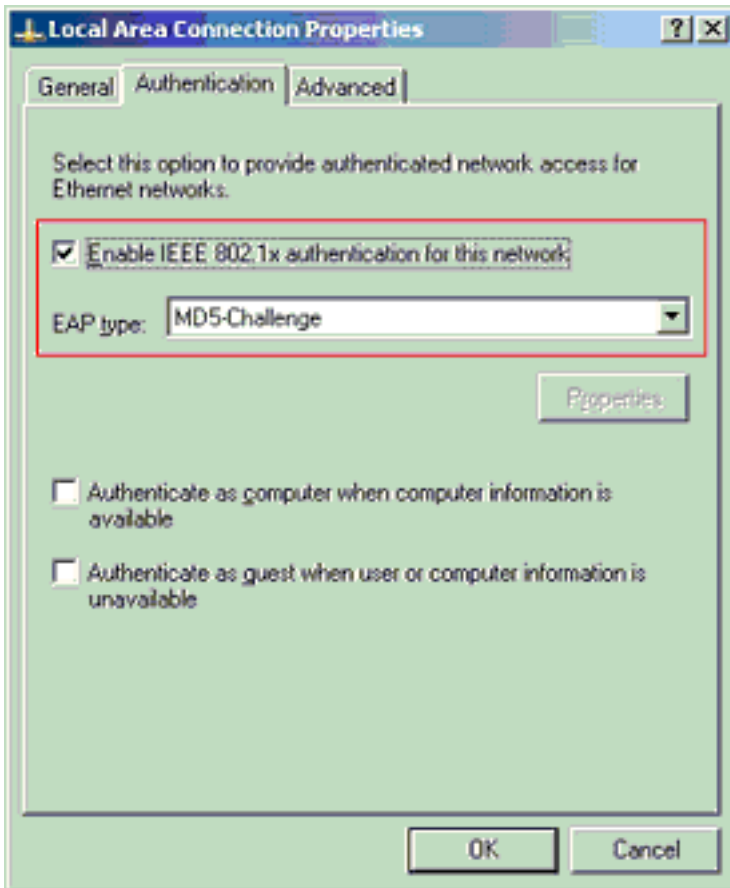
Cancel

## 802.1x 인증을 사용하도록 PC 클라이언트 구성

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

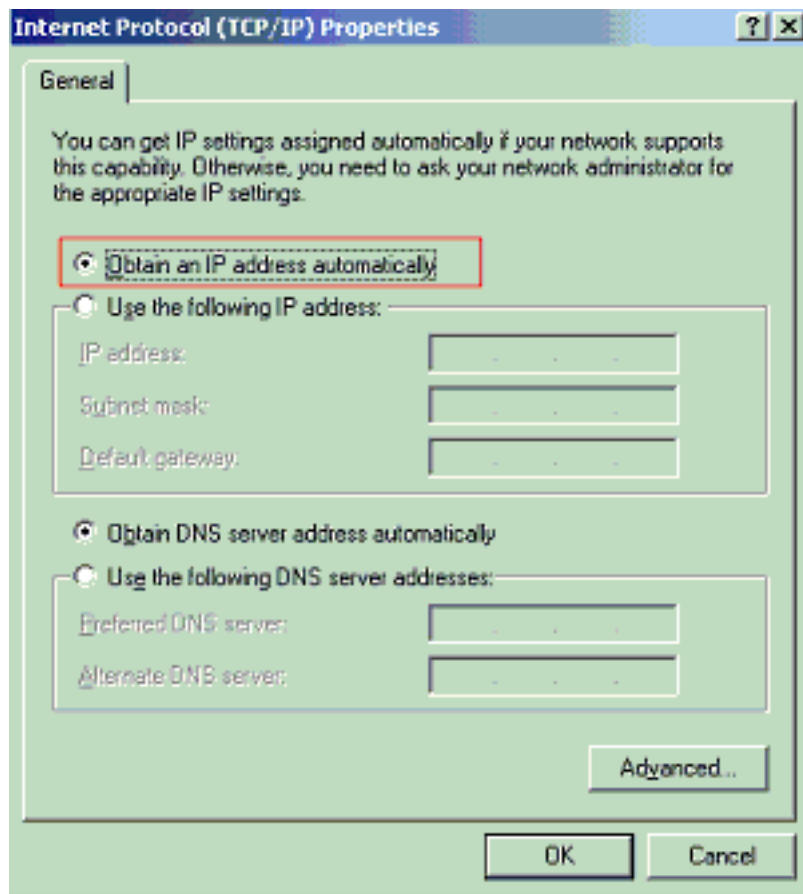
1. Start(시작) > Control Panel(제어판) > Network Connections(네트워크 연결)를 선택한 다음 Local Area Connection(로컬 영역 연결)을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 선택합니다.
2. General(일반) 탭 아래에 연결된 경우 알림 영역에 아이콘 표시를 선택합니다.
3. Authentication(인증) 탭에서 이 네트워크에 대해 IEEE 802.1x 인증 활성화를 선택합니다.
4. EAP 유형을 MD5-Challenge로 설정합니다. 이 예에서는 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



## 802.1x 인증을 사용하도록 IP 전화 구성

802.1x 인증을 위해 IP Phone을 구성하려면 다음 단계를 완료하십시오.

1. **802.1X 인증** 설정에 액세스하려면 **Settings(설정)** 버튼을 누르고 Security Configuration(보안 컨피그레이션) > **802.1X Authentication(802.1X 인증)** > **Device Authentication(디바이스 인증)**을 선택합니다.
2. Device **Authentication(디바이스 인증)** 옵션을 Enabled(활성화됨)로 설정합니다.
3. 저장 소프트웨어 키를 누릅니다.
4. 전화에서 비밀번호를 설정하려면 **802.1X Authentication > EAP-MD5 > Shared Secret**을 선택합니다.
5. 공유 암호를 입력하고 Save를 누릅니다.참고: 비밀번호는 숫자 또는 문자의 조합으로 구성된 6~32자 사이여야 합니다. 메시지가 표시되며 이 조건이 충족되지 않으면 비밀번호가 저장되지 않습니다.참고: 802.1X 인증을 비활성화하거나 전화기에서 공장 재설정을 수행하면 이전에 구성된 MD5 공유 암호가 삭제됩니다.참고: 다른 옵션인 Device ID 및 Realm은 구성할 수 없습니다.디바이스 ID는 802.1x 인증을 위한 사용자 이름으로 사용됩니다.이 형식은 전화 모델 번호 및 고유한 MAC 주소의 파생입니다.CP-<model>-SEP-<MAC>.예: **CP-7970G-SEP001759E7492C**.자세한 내용은 [802.1X 인증 설정](#)을 참조하십시오.

DHCP 서버에서 IP 주소를 얻기 위해 IP Phone을 구성하려면 다음 단계를 완료합니다.

1. **Network Configuration** 설정에 액세스하려면 **Settings(설정)** 버튼을 누르고 Network Configuration(네트워크 컨피그레이션)을 선택합니다.
2. 네트워크 구성 옵션 잠금 해제잠금을 해제하려면 **\*\*#**을 누르십시오.참고: 옵션을 잠금 해제하려면 **\*\*#**을 누르지 말고 바로 **\*\*#**을 다시 눌러 옵션을 잠그십시오.전화기에서 이 시퀀스를 **\*\*#\*\***로 해석하여 전화기를 재설정합니다.잠금을 해제한 후 옵션을 잠그려면 **\*\*#**을 다시 누르기 전에 10초 이상 기다립니다.

3. DHCP Enabled(DHCP 활성화) 옵션으로 스크롤하고 **Yes(예)** 소프트키를 눌러 DHCP를 활성화합니다.
4. **저장** 소프트키를 누릅니다.

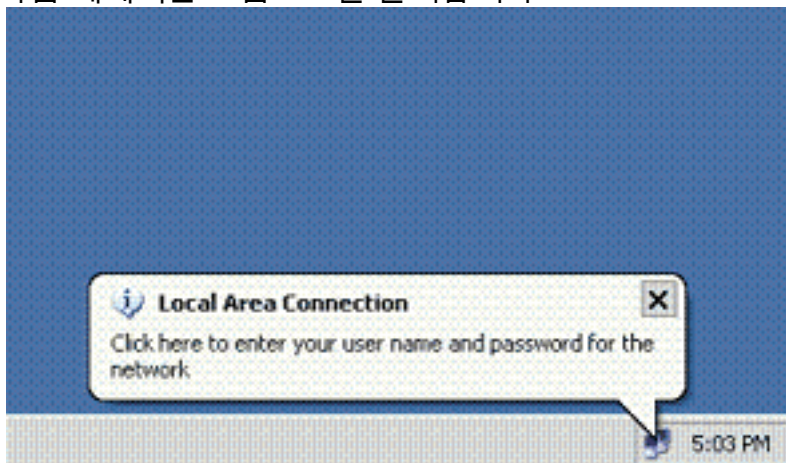
## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

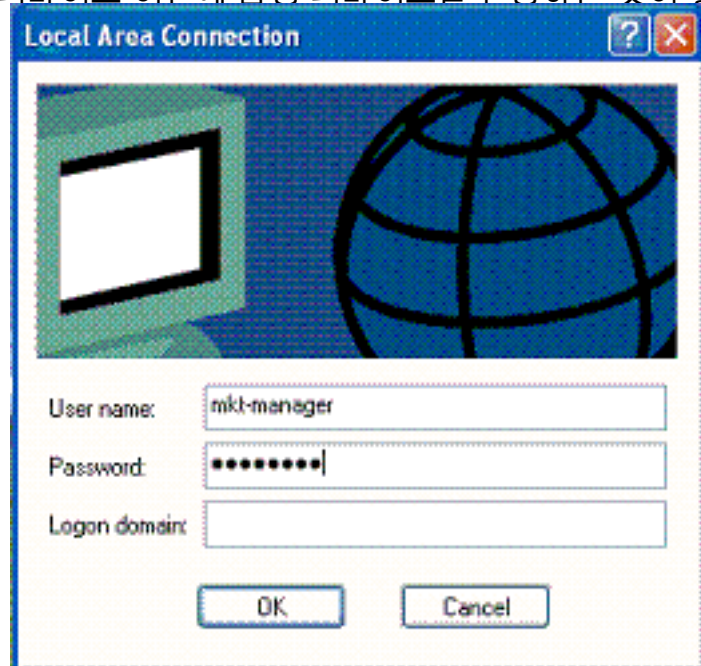
### PC 클라이언트

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

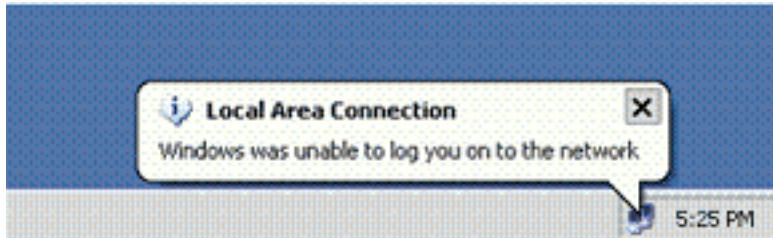
1. 다음 예에서는 프롬프트를 클릭합니다



사용자 이름 및 비밀번호 입력 창이 표시됩니다.참고: MDA는 디바이스 인증 순서를 적용하지 않습니다.그러나 최상의 결과를 얻으려면 MDA 지원 포트의 데이터 디바이스 이전에 음성 디바이스를 인증하는 것이 좋습니다.



2. 사용자 이름과 암호를 입력합니다.
3. 오류 메시지가 나타나지 않으면 네트워크 리소스 액세스 및 ping과 같은 일반적인 방법과의 연결을 **확인합니다**.참고: 이 오류가 나타나면 사용자 이름과 암호가 올바른지 확인합니다



## IP 전화

IP Phones의 802.1X Authentication Status(802.1X 인증 상태) 메뉴에서 인증 상태를 모니터링할 수 있습니다.

1. 802.1X Authentication Real-Time Stats(802.1X 인증 실시간 통계)에 액세스하려면 **Settings(설정)** 버튼을 누르고 **Security Configuration(보안 컨피그레이션) > 802.1X Authentication Status(802.1X 인증 상태)**를 선택합니다.
2. 트랜잭션 상태는 인증되어야 합니다. 자세한 내용은 [802.1X 인증 실시간 상태](#)를 참조하십시오.  
.참고: 인증 상태는 Settings(설정) > Status(상태) > Status Messages(상태 메시지)에서도 확인할 수 있습니다.

## 레이어 3 스위치

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

1. AUTHORIZED를 나타내는 포트 상태를 .

```
Cat-3560#show dot1x all summary
```

Interface	PAE	Client	Status
Fa0/1	AUTH	0016.3633.339c	AUTHORIZED
		0017.59e7.492c	AUTHORIZED
Fa0/2	AUTH	0014.5e94.5f99	AUTHORIZED
Fa0/3	AUTH	0011.858D.9AF9	AUTHORIZED
Fa0/4	AUTH	0016.6F3C.A342	AUTHORIZED
		001a.2f80.381f	AUTHORIZED

```
Cat-3560#show dot1x interface fastEthernet 0/1 details
```

```
Dot1x Info for FastEthernet0/1
```

```
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_DOMAIN
ReAuthentication = Enabled
QuietPeriod = 10
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 60 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Auth-Fail-Vlan = 6
Auth-Fail-Max-attempts = 2
Guest-Vlan = 6
```

Dot1x Authenticator Client List

```
-----  
Domain = DATA  
Supplicant = 0016.3633.339c  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE  
Port Status = AUTHORIZED  
ReAuthPeriod = 60  
ReAuthAction = Reauthenticate  
TimeToNextReauth = 29  
Authentication Method = Dot1x  
Authorized By = Authentication Server  
Vlan Policy = 4
```

```
Domain = VOICE  
Supplicant = 0017.59e7.492c  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE  
Port Status = AUTHORIZED  
ReAuthPeriod = 60  
ReAuthAction = Reauthenticate  
TimeToNextReauth = 15  
Authentication Method = Dot1x  
Authorized By = Authentication Server
```

인증 성공 후 VLAN 상태를 확인합니다.

Cat-3560#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Gi0/1 Gi0/2
2 SERVER	active	Fa0/24
3 VOICE	active	Fa0/1, Fa0/4
4 MARKETING	active	Fa0/1, Fa0/2
5 SALES	active	Fa0/3, Fa0/4
6 GUEST_and_AUTHFAIL	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

!--- Output suppressed.

## 2. 성공적인 인증 후 DHCP 바인딩 상태를 확인합니다.

Router#show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
172.16.3.2	0100.1759.e749.2c	Aug 24 2007 06:35 AM	Automatic
172.16.3.3	0100.1a2f.8038.1f	Aug 24 2007 06:43 AM	Automatic
172.16.4.2	0100.1636.3333.9c	Aug 24 2007 06:50 AM	Automatic
172.16.4.3	0100.145e.945f.99	Aug 24 2007 08:17 AM	Automatic
172.16.5.2	0100.166F.3CA3.42	Aug 24 2007 08:23 AM	Automatic
172.16.5.3	0100.1185.8D9A.F9	Aug 24 2007 08:51 AM	Automatic

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 show 명령을 지원합니다.show 명령 출력의 분석을 보려면 OIT를 사용합니다.

## 문제 해결

### [IP Phone 인증 실패](#)

IP Phone Status(IP IP 또는 802.1x 인증 실패 시 등록)가 표시됩니다.이 문제를 해결하려면 다음 단계를 완료하십시오.

- IP 전화기에서 802.1x가 활성화되어 있는지 확인합니다.
- 인증(RADIUS) 서버에 사용자 이름으로 디바이스 ID를 입력했는지 확인합니다.
- 공유 암호가 IP 전화기에 구성되어 있는지 확인합니다.
- 공유 암호가 구성된 경우 인증 서버에 입력한 공유 암호가 동일한지 확인합니다.
- 스위치 및 인증 서버와 같은 다른 필수 디바이스를 올바르게 구성했는지 확인합니다.

## 관련 정보

- [IEEE 802.1x 포트 기반 인증 구성](#)
- [802.1x 인증을 사용하도록 IP Phone 구성](#)
- [Cisco Catalyst 스위치 환경에서 Windows NT/2000 서버용 Cisco Secure ACS 구축 지침](#)
- [RFC 2868:터널 프로토콜 지원을 위한 RADIUS 특성](#)
- [Cisco IOS 소프트웨어 구성 실행 Catalyst 6500/6000을 통한 IEEE 802.1x 인증 예](#)
- [Catalyst 6500/6000을 통한 IEEE 802.1x 인증 CatOS 소프트웨어 구성 예](#)
- [LAN 제품 지원 페이지](#)
- [LAN 스위칭 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)