Catalyst 6500/6000을 통한 IEEE 802.1x 인증 CatOS 소프트웨어 구성 예

목차

<u>소</u>개 사전 요구 사항 요구 사항 <u>사용되는 구</u>성 요소 표기규칙 배경 정보 구성 네트워크 다이어그램 802.1x 인증을 위한 Catalyst 스위치 구성 RADIUS 서버 구성 802.1x 인증을 사용하도록 PC 클라이언트 구성 다음을 확인합니다. PC 클라이언트 Catalyst 6500 문제 해결 관련 정보

<u>소개</u>

이 문서에서는 하이브리드 모드(수퍼바이저 엔진의 CatOS 및 MSFC의 Cisco IOS® 소프트웨어)에 서 실행되는 Catalyst 6500/6000에서 IEEE 802.1x를 구성하고 인증 및 VLAN 할당을 위해 원격 인 증 전화 접속 사용자 서비스(RADIUS) 서버를 구성하는 방법에 대해 설명합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서의 독자는 다음 주제에 대해 알고 있어야 합니다.

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

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Supervisor Engine에서 CatOS Software 릴리스 8.5(6)를 실행하고 MSFC에서 Cisco IOS Software 릴리스 12.2(18)SXF를 실행하는 Catalyst 6500**참고:** 802.1x 포트 기반 인증을 지원하 려면 CatOS 릴리스 6.2 이상이 필요합니다.**참고:** 소프트웨어 릴리스 7.2(2) 전에 802.1x 호스트 가 인증되면 NVRAM으로 구성된 VLAN에 조인합니다. 소프트웨어 릴리스 7.2(2) 이상 릴리스 에서 인증 후 802.1x 호스트는 RADIUS 서버로부터 VLAN 할당을 받을 수 있습니다.
- 이 예에서는 Cisco ACS(Secure Access Control Server) 4.1을 RADIUS 서버로 사용합니다.참 고: 스위치에서 802.1x를 활성화하기 전에 RADIUS 서버를 지정해야 합니다.
- 802.1x 인증을 지원하는 PC 클라이언트.**참고:** 이 예에서는 Microsoft Windows XP 클라이언트 를 사용합니다.

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

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

<u>배경 정보</u>

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 포트에 서 두 개의 고유한 가상 액세스 포인트를 생성하여 네트워크 액세스를 제어합니다. 하나의 액세스 포인트는 제어되지 않는 포트입니다. 다른 포트는 제어 포트입니다. 단일 포트를 통과하는 모든 트 래픽은 두 액세스 포인트 모두에서 사용할 수 있습니다. 802.1x는 스위치 포트에 연결된 각 사용자 디바이스를 인증하고, 스위치 또는 LAN에서 제공하는 서비스를 사용하기 전에 VLAN에 포트를 할 당합니다. 디바이스가 인증될 때까지 802.1x 액세스 제어는 디바이스가 연결된 포트를 통과하는 EAP(Extensible Authentication Protocol) over LAN(EAPOL) 트래픽만 허용합니다. 인증이 성공하 면 일반 트래픽이 포트를 통과할 수 있습니다.

<u>구성</u>

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

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

이 구성에는 다음 단계가 필요합니다.

- <u>802.1x 인증을 위한 Catalyst 스위치 구성</u>
- <u>RADIUS 서버 구성</u>
- 802.1x 인증을 사용하도록 PC 클라이언트 구성

<u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



- RADIUS 서버 클라이언트의 실제 인증을 수행합니다. RADIUS 서버는 클라이언트의 ID를 검 증하고 클라이언트가 LAN 및 스위치 서비스에 액세스할 수 있는 권한이 있는지 여부를 스위치 에 알립니다. 여기서 RADIUS 서버는 인증 및 VLAN 할당을 위해 구성됩니다.
- Switch(스위치) 클라이언트의 인증 상태에 따라 네트워크에 대한 물리적 액세스를 제어합니 다. 이 스위치는 클라이언트와 RADIUS 서버 간의 중간(프록시) 역할을 하며 클라이언트로부터 ID 정보를 요청하고 RADIUS 서버와의 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 프로세 스에 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 클라이언트입니 다. 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 주 소를 얻도록 구성됩니다.**참고**: 이 컨피그레이션에서 인증에 실패한 클라이언트 또는 스위치에 연결하는 802.1x가 아닌 모든 지원 클라이언트가 인증 실패 및 게스트 VLAN 기능을 사용하여 사용하지 않는 VLAN(VLAN 4 또는 5)으로 이동하여 네트워크 액세스가 거부됩니다.

802.1x 인증을 위한 Catalyst 스위치 구성

이 샘플 스위치 컨피그레이션에는 다음이 포함됩니다.

- FastEthernet 포트에서 802.1x 인증 및 관련 기능을 활성화합니다.
- FastEthernet 포트 3/1 뒤에 RADIUS 서버를 VLAN 10에 연결합니다.
- 두 IP 풀에 대한 DHCP 서버 컨피그레이션(VLAN 2의 클라이언트용, VLAN 3의 클라이언트용)
- VLAN 간 라우팅으로 인증 후 클라이언트 간 연결 가능

802.1x 인증을 구성하는 방법에 대한 지침은 <u>인증 구성 지침</u>을 참조하십시오.

참고: RADIUS 서버가 항상 인증된 포트 뒤에 연결되어야 합니다.

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 successsful 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 |
| <pre>! Any non-802.1x capable host connecting or 802.1x !-</pre> |
| capable host failing to respond to the username and |
| password ! authentication requests from the |
| Authenticator is placed in the ! quest VLAN after 60 |
| seconds. ! Note: An authentication failure VLAN is |
| independent ! of the quest VLAN. However, the quest |
| 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 |
| <pre>server. Router(config-if)#no shut</pre> |
| 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 |
| <pre>! This pool assigns ip address for clients in VLAN 2.</pre> |
| 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 a | address for clients in VLAN 3. | | |
| Router(dhcp-config)# exit | | | |
| Router(config)#ip dhcp excl | uded-address 172.16.2.1 | | |
| Router(config)#ip dhcp excl | uded-address 172.16.3.1 | | |
| ! In order to go back to | o the Switching module, ! | | |
| enter Ctrl-C three times. H | Router# Router#^C Cat6K> | | |
| (enable) Cat6K> (enable) sh | now 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) | | | |

RADIUS 서버 구성

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

- 1. AAA 클라이언트를 구성하려면 ACS 관리 창**에서 Network Configuration**을 클릭합니다.
- 2. AAA Clients 섹션 아래에서 Add Entry를 클릭합니다

| CISCO SYSTEMS | Network Configuration | | |
|------------------------------|-----------------------|-----------------------|--------------------|
| | Select | | |
| User Setup | | | |
| Greup Setup | % Q | AAA Clients | ? |
| Shared Profile Components | AAA Client Hostname | AAA Client IP Address | Authenticate Using |
| Network | | None Defined | |
| System Configuration | | Add Entry Search | |

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 = 스위 치의 관리 인터페이스(sc0)IP 주소(172.16.1.2).공유 암호 = 스위치에 구성된 Radius 키 (cisco)입니다.Authenticate Using = RADIUS IETF(를 사용하여 인증).참고: 올바른 작동을 위 해 공유 비밀 키는 AAA 클라이언트 및 ACS에서 동일해야 합니다. 키는 대/소문자를 구분합니 다.

4. 다음 예와 같이 Submit + Apply를 클릭하여 변경 사항을 적용합니다

| Cisco Systems | Network Configuration | | | |
|------------------------------|--|--|--|--|
| | Add AAA Client | | | |
| User Setup | | | | |
| Setup | AAA Client Hostname | | | |
| Shared Profile Components | AAA Client IP Address | | | |
| Network Configuration | Shared Secret cisco | | | |
| System Configuration | RADIUS Key Wrap | | | |
| Configuration | Key Encryption Key | | | |
| Administration Control | Message Authenticator Code Key | | | |
| External User Databases | Key Input Format C ASCII Hexadecimal | | | |
| Posture Validation | Authenticate Using RADIUS (IETF) | | | |
| Network Access Profiles | Single Connect TACACS+ AAA Client (Record stop in accounting on failure) | | | |
| Reports and | Log Update/Watchdog Packets from this AAA Client | | | |
| Activity | Log RADIUS Tunneling Packets from this AAA Client | | | |
| Documentation | 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 | | | |
| | Submit Submit + Apply Cancel | | | |

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 및 VLAN 3에 연결하는 클라이언트의 또 다 른 사용자 user_vlan3이 생성됩니다.

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

.

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

| CISCO SYSTEMS | User Setup | |
|---|--|-------------|
| millium | Select | |
| User Setup | | |
| Group Setup | Licen: Juser vian2 | |
| and I Shared Profile | Find Add/Edit | |
| Components | | |
| Configuration | List users beginning with letter/number: | |
| System Configuration | <u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V U X Y Z</u> | |
| Interface Configuration | 0 1 2 3 4 5 6 7 8 9 | |
| Administration | List all users | |
| External User | Remove Dynamic Users | |
| Databases | | |
| Validation | Back to Help | |
| Profiles | | |
| CISCO SYSTEMS | User Setup | |
| tllutllu | Edit | |
| | | |
| User | Loit | |
| User Setup | User: user_vlan2 (New User) | |
| User Setup | User: user_vlan2 (New User) | |
| User Setup Setup Setup Shared Profile Components | User: user_vlan2 (New User) | |
| User Setup Setup Setup Shared Profile Components Network Configuration | User: user_vlan2 (New User) Account Disabled Supplementary User Info | ? |
| User Setup Setup Setup Shared Profile Components Network Configuration System Configuration | User: user_vlan2 (New User) Account Disabled Supplementary User Info Real Name user_vlan2 | P• |
| User Setup Setup Shared Profile Components Network Configuration System Configuration | User: user_vlan2 (New User) Account Disabled Supplementary User Info Real Name user_vlan2 Description Client in VLAN 2 | ? |
| User Setup Setup Shared Profile Components Network Configuration System Configuration | User: user_vlan2 (New User) Account Disabled Supplementary User Info Real Name user_vlan2 Description Client in VLAN 2 | ? |
| User Setup Setup Setup Shared Profile Components Network Configuration System Configuration System Configuration Interface Configuration | User: user_vlan2 (New User) Account Disabled Supplementary User Info Real Name User_vlan2 Description Client in VLAN 2 | - - |
| User Setup Setup Setup Shared Profile Components Network Configuration System Configuration System Configuration Interface Configuration Configuration Configuration External User Databases | User: user_vlan2 (New User) Account Disabled Supplementary User Info Real Name user_vlan2 Description Client in VLAN 2 User Setup | ? - |
| User Setup Setup Setup Setup Shared Profile Components Network Configuration System Configuration System Configuration Configuration Configuration External User Databases | User: user_vlan2 (New User) Account Disabled Supplementary User Info Real Name user_vlan2 Description Client in VLAN 2 User Setup Password Authentication: | ? ? |
| User Setup Setup Setup Shared Profile Components Network Configuration System Configuration System Configuration Configuration Configuration External User Databases Databases | 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 | - - - |
| User Setup Setup Setup Setup Shared Profile Components Network Configuration System Configuration System Configuration Configuration Configuration External User Databases Descent Databases Network Access Profiles | 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 th Separate field is not checked | ? - • |
| User Setup Setup Setup Setup Setup Shared Profile Components Network Configuration System Configuration System Configuration Configuration Configuration External User Databases External User Databases Network Access Profiles Network Access Profiles | 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 th Separate field is not checked Password Confirm | ? • |

2. 클라이언트 IP 주소 할당을 AAA 클라이언트 풀에 의해 할당됨으로 정의합니다. VLAN 2 클라 이언트에 대해 스위치에 구성된 IP 주소 풀의 이름을 입력합니다

| CISCO SYSTEMS | User Setup |
|----------------------------|--|
| | Password I |
| User Setup | 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. |
| Shared Profile | Group to which the user is assigned: |
| Network | Default Group |
| Configuration | Callback |
| Interface | Our Setting |
| Configuration | O No callback allowed |
| Administration Control | Callback using this number |
| External User | O Dialup client specifies callback number |
| 2 Databases | C Use Windows Database callback settings |
| Validation | Client ID Address Assistment |
| Network Access Profiles | Client IP Address Assignment |
| Reports and | C Use group settings |
| Activity | O No IP address assignment |
| Documentation | O Assigned by dialup client |
| | C Assign static IP address |
| | Assigned by AAA client pool vlan2_clients |

참고: 이 사용자가 AAA 클라이언트에 구성된 IP 주소 풀에 의해 할당된 IP 주소를 가질 경우에 만 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 태그 가 1로 설정되어 있는지 확인합니다. Catalyst는 1이 아닌 다른 태그를 무시합니다. 특정 VLAN에 사용자를 할당하려면 해당 VLAN *이름*으로 특성 81도 정의해야 합니다.**참고:** VLAN *이름*은 스위치에 구성된 이름과 정확히 같아야 합니다.**참고:** VLAN *번호* 기반 VLAN 할당은 CatOS에서 지원되지 않습니다



RFC 2868을 참조하십시오. 이러한 IETF 특성에 대한 자세한 내용은 터널 프로토콜 지원 RADIUS 특성을 참조하십시오.참고: ACS 서버의 초기 컨피그레이션에서 IETF RADIUS 특성 이 사용자 설정에 표시되지 않을 수 있습니다. Interface configuration(인터페이스 컨피그레이 션) > RADIUS(IETF)를 선택하여 사용자 컨피그레이션 화면에서 IETF 특성을 활성화합니다. 그런 다음 사용자 및 그룹 열에서 특성 64, 65 및 81을 선택합니다.

<u>802.1x 인증을 사용하도록 PC 클라이언트 구성</u>

이 예제는 Microsoft Windows XP EAP(Extensible Authentication Protocol) over LAN(EAPOL) 클라 이언트에만 적용됩니다. 다음 단계를 완료하십시오.

- 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 MD**5-Challenge**로 설정합니다. 이 예에서는 다음과 같습니다

| Local Area Connection Properties | | |
|---|--|--|
| General Authentication Advanced | | |
| Select this option to provide authenticated network access for Ethernet networks. | | |
| EAP type: MD5-Challenge | | |
| Properties | | |
| Authenticate as computer when computer information is available | | |
| Authenticate as guest when user or computer information is unavailable | | |
| | | |
| | | |
| | | |
| OK Cancel | | |

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 **속성**을 **클릭합니다**.
- 3. Obtain an IP address automatically를 선택합니다

| ternet Protocol (TCP/IP) Prop General | erties ? × | | |
|---|-------------------|--|--|
| You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. | | | |
| Obtain an IP address automatically | | | |
| $\square \square \bigcirc$ Use the following IP addres | s: / | | |
| [P address: | | | |
| S <u>u</u> bnet mask: | | | |
| Default gateway: | | | |
| Obtain DNS server address | automaticallu | | |
| O Use the following DNS server | ver addresses: | | |
| Preferred DNS server: | | | |
| Alternate DNS server: | · · · · | | |
| | Ad <u>v</u> anced | | |
| | OK Cancel | | |

<u>다음을 확인합니다.</u>

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

<u>PC 클라이언트</u>

컨피그레이션을 올바르게 완료한 경우 PC 클라이언트는 사용자 이름과 비밀번호를 입력하라는 팝 업 프롬프트를 표시합니다.

1. 다음 예에서는 프롬프트를 클릭합니다

| Local Area Connection Click here to enter your user name and password for the network | |
|---|---------------|
| 5:03 PM | 사용자 이를 및 비 |
| 밀번호 입력 창이 표시됩니다. 사용자 이름과 비밀번호를 입력합니다 Iocal Area Connection ? | |
| | |
| User name: user_vlan2 | |
| Password: | |
| Logon domain: | |
| OK Cancel 참고: PC | : 1과 2에서 VLAN |

2 사용자 자격 증명을 입력합니다. PC 3 및 4에서 VLAN 3 사용자 자격 증명을 입력합니다. 3. 오류 메시지가 나타나지 않을 경우 네트워크 리소스 액세스 및 ping 명령을 통해 연결하는 것 과 같은 일반적인 방법과의 연결을 **확인합니다**. 이것은 PC 1의 출력으로서 PC 4에 대한 성공 적인 ping을 보여줍니다

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 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 Ping statistics for 172.16.2.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms 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 Ping statistics for 172.16.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms 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 Ping statistics for 172.16.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms C:\Documents and Settings\Administrator>___

오류가 나타나면 사용자 이름과 암호가 올바른지 확인합니다

0



Catalyst 6500

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

1. 을 나타내는 포트 상태를 .

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 idle 3/5 authenticated auto authorized Port Port-Mode Re-authentication Shutdown-timeout _____ ____ _____ 3/1 SingleAuth disabled disabled disabled 3/2 SingleAuth disabled 3/3 SingleAuth disabled disabled 3/4 SingleAuth disabled disabled 3/5 SingleAuth disabled disabled 인증 성공 후 VLAN 상태를 확인합니다. Cat6K> (enable) **show vlan** Status IfIndex Mod/Ports, Vlans VLAN Name ____ _____ -----_____ 2/1-2 1 default active 6 3/6-48 2 VLAN2 active 83 3/2-3 3 VLAN3 active 84 3/4-5 active 85 AUTHFAIL_VLAN 4 86 GUEST_VLAN 5 active 10 RADIUS_SERVER 87 3/1 active active 78 1002 fddi-default 1003 token-ring-default active 81 1004 fddinet-default active 79 1005 trnet-default active 80 !--- Output suppressed. 2. 인증에 성공한 후 MSFC(라우팅 모듈)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 Feb 14 2007 03:00 AM Automatic Feb 14 2007 03:03 AM Automatic 172.16.2.3 0100.166F.3CA3.42

 Feb 14 2007 03:05 AM
 Automatic

 Feb 14 2007 03:07 AM
 Automatic



172.16.3.2

172.16.3.3

0100.145e.945f.99

0100.1185.8D9A.F9

<u>관련 정보</u>

- <u>Cisco IOS 소프트웨어 구성 실행 Catalyst 6500/6000을 통한 IEEE 802.1x 인증 예</u>
- <u>Catalyst 스위칭 및 ACS 구축 설명서</u>
- <u>RFC 2868: 터널 프로토콜 지원을 위한 RADIUS 특성</u>
- <u>802.1x 인증 구성</u>
- <u>LAN 제품 지원 페이지</u>
- <u>LAN 스위칭 지원 페이지</u>
- <u>기술 지원 및 문서 Cisco Systems</u>