WLC를 사용하는 게스트 WLAN 및 내부 WLAN 컨피그레이션 예

목차

소개

이 문서에서는 게스트 WLAN(무선 LAN) 및 WLAN 컨트롤러(WLC) 및 LAP(lightweight 액세스 포인트)를 사용하는 보안 내부 WLAN에 대한 컨피그레이션 예를 제공합니다. 이 문서의 컨피그레이션에서 게스트 WLAN은 웹 인증을 사용하여 사용자를 인증하고 보안 내부 WLAN은 EAP(Extensible Authentication Protocol) 인증을 사용합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 기본 매개변수로 WLC를 구성하는 방법에 대한 지식
- DHCP 및 DNS(Domain Name System) 서버를 설정하는 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 4.0을 실행하는 Cisco 2006 WLC
- Cisco 1000 Series LAP
- 펌웨어 릴리스 2.6을 실행하는 Cisco 802.11a/b/g Wireless Client Adapter
- Cisco IOS® 버전 12.4(2)XA를 실행하는 Cisco 2811 라우터
- Cisco IOS 버전 12.0(5)WC3b를 실행하는 Cisco 3500 XL Series Switch
- Microsoft Windows 2000 서버에서 실행되는 DNS 서버

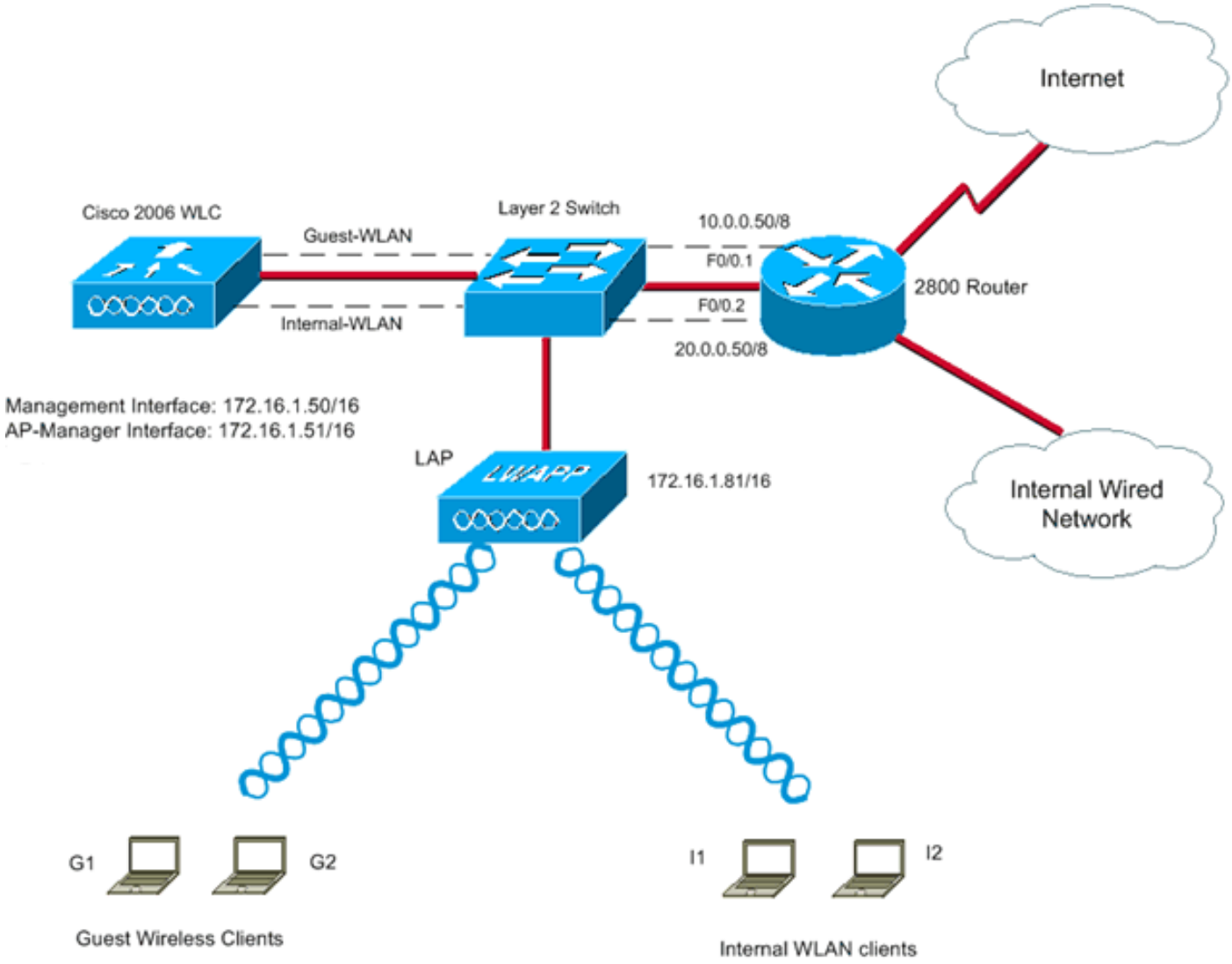
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

네트워크 설정

이 문서의 구성 예제에서는 이 다이어그램에 표시된 설정을 사용합니다.LAP는 WLC에 등록됩니다.WLC는 레이어 2 스위치에 연결됩니다.사용자를 WAN에 연결하는 라우터는 레이어 2 스위치에도 연결됩니다.두 개의 WLAN을 생성해야 합니다. 하나는 게스트 사용자용이고 다른 하나는 내부 LAN 사용자용입니다.게스트 및 내부 무선 클라이언트에 IP 주소를 제공하려면 DHCP 서버가 필요합니다.게스트 사용자는 네트워크에 액세스하기 위해 웹 인증을 사용합니다.내부 사용자는 EAP 인증을 사용합니다.2811 라우터는 무선 클라이언트의 DHCP 서버 역할도 합니다.



참고: 이 문서에서는 WLC가 기본 매개변수로 구성되고 LAP가 WLC에 등록되었다고 가정합니다 .WLC에서 기본 매개변수를 구성하는 방법 및 LAP를 WLC에 등록하는 방법에 대한 자세한 내용은 WLC(Lightweight AP)에 대한 LAP(Registration to a Wireless LAN Controller)를 참조하십시오.

DHCP 서버로 구성된 경우 일부 방화벽은 릴레이 에이전트의 DHCP 요청을 지원하지 않습니다 .WLC는 클라이언트의 릴레이 에이전트입니다.DHCP 서버로 구성된 방화벽은 이러한 요청을 무시합니다.클라이언트는 방화벽에 직접 연결되어야 하며 다른 릴레이 에이전트 또는 라우터를 통해 요청을 보낼 수 없습니다.방화벽은 직접 연결된 내부 호스트에 대해 간단한 DHCP 서버로 작동할 수 있습니다.이렇게 하면 방화벽이 직접 연결되어 있고 볼 수 있는 MAC 주소를 기반으로 테이블을 유지할 수 있습니다.따라서 DHCP 릴레이에서 주소를 할당하려고 할 수 없으며 패킷이 폐기됩니다 .PIX 방화벽에는 이러한 제한이 있습니다.

구성

이 네트워크 설정에 대한 디바이스를 구성하려면 다음 단계를 완료합니다.

1. 게스트 및 내부 사용자에 대해 WLC에서 동적 인터페이스 구성
2. 게스트 및 내부 사용자에 대한 WLAN 생성
3. WLC에 트렁크 포트로 연결하는 레이어 2 스위치 포트 구성
4. 두 VLAN에 대한 라우터 구성

게스트 및 내부 사용자에 대해 WLC에서 동적 인터페이스 구성

첫 번째 단계는 WLC에 두 개의 동적 인터페이스를 생성하는 것입니다. 하나는 게스트 사용자이고 다른 하나는 내부 사용자입니다.

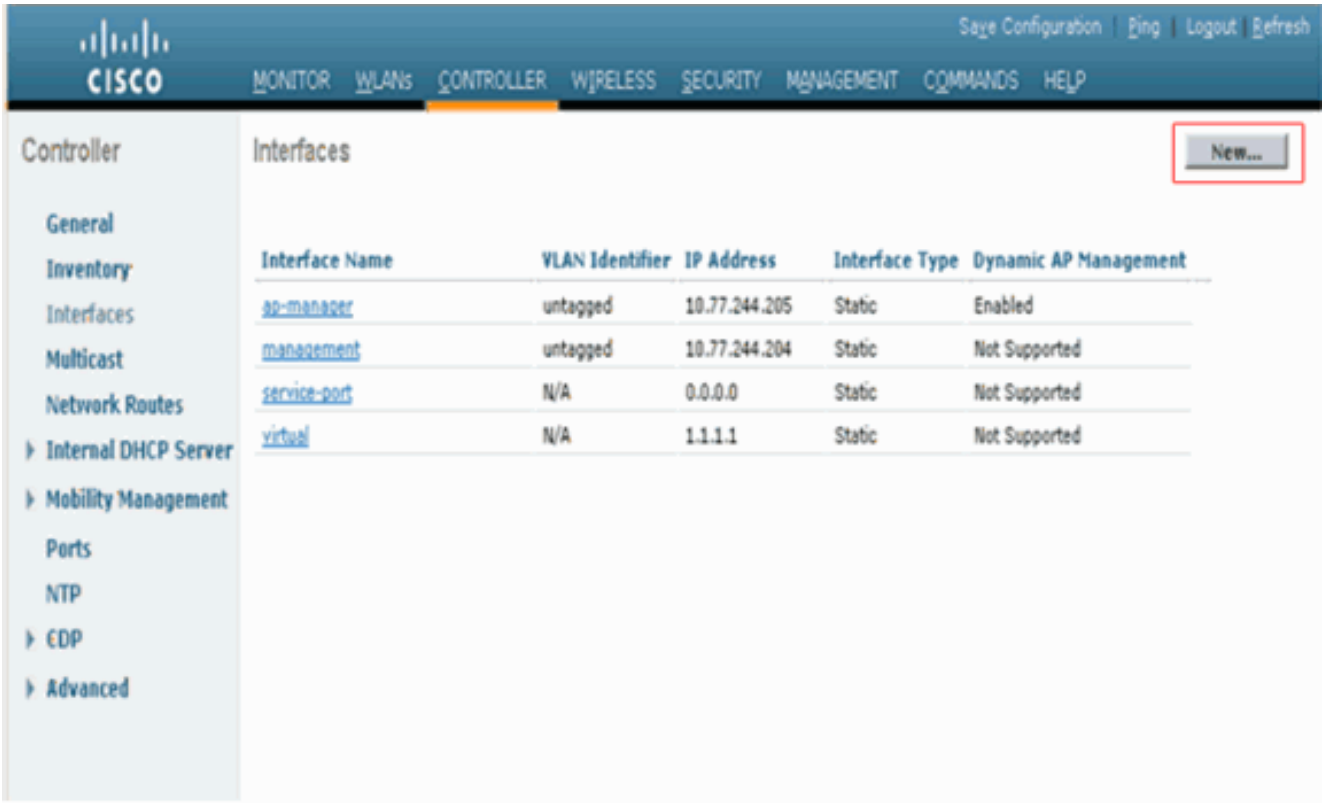
이 문서의 예에서는 동적 인터페이스에 대해 다음 매개변수 및 값을 사용합니다.

```
Guest-WLAN                                          Internal-WLAN
VLAN Id : 10                              VLAN Id : 20
IP address: 10.0.0.10                        IP address: 20.0.0.10
Netmask: 255.0.0.0 Netmask: 255.0.0.0
Gateway: 10.0.0.50                          Gateway: 20.0.0.50
Physical port on WLC: 1                       Physical port on WLC: 1
DHCP server: 172.16.1.60                        DHCP server: 172.16.1.60
```

다음 단계를 완료하십시오.

1. WLC GUI에서 Controllers(컨트롤러) **> Interfaces(인터페이스)를** 선택합니다.Interfaces 창이 나타납니다.이 창에는 컨트롤러에 구성된 인터페이스가 나열됩니다.여기에는 관리 인터페이스, ap-manager 인터페이스, 가상 인터페이스 및 서비스 포트 인터페이스, 사용자 정의 동적 인터페이스인 기본 인터페이스가 포함됩니다

   .

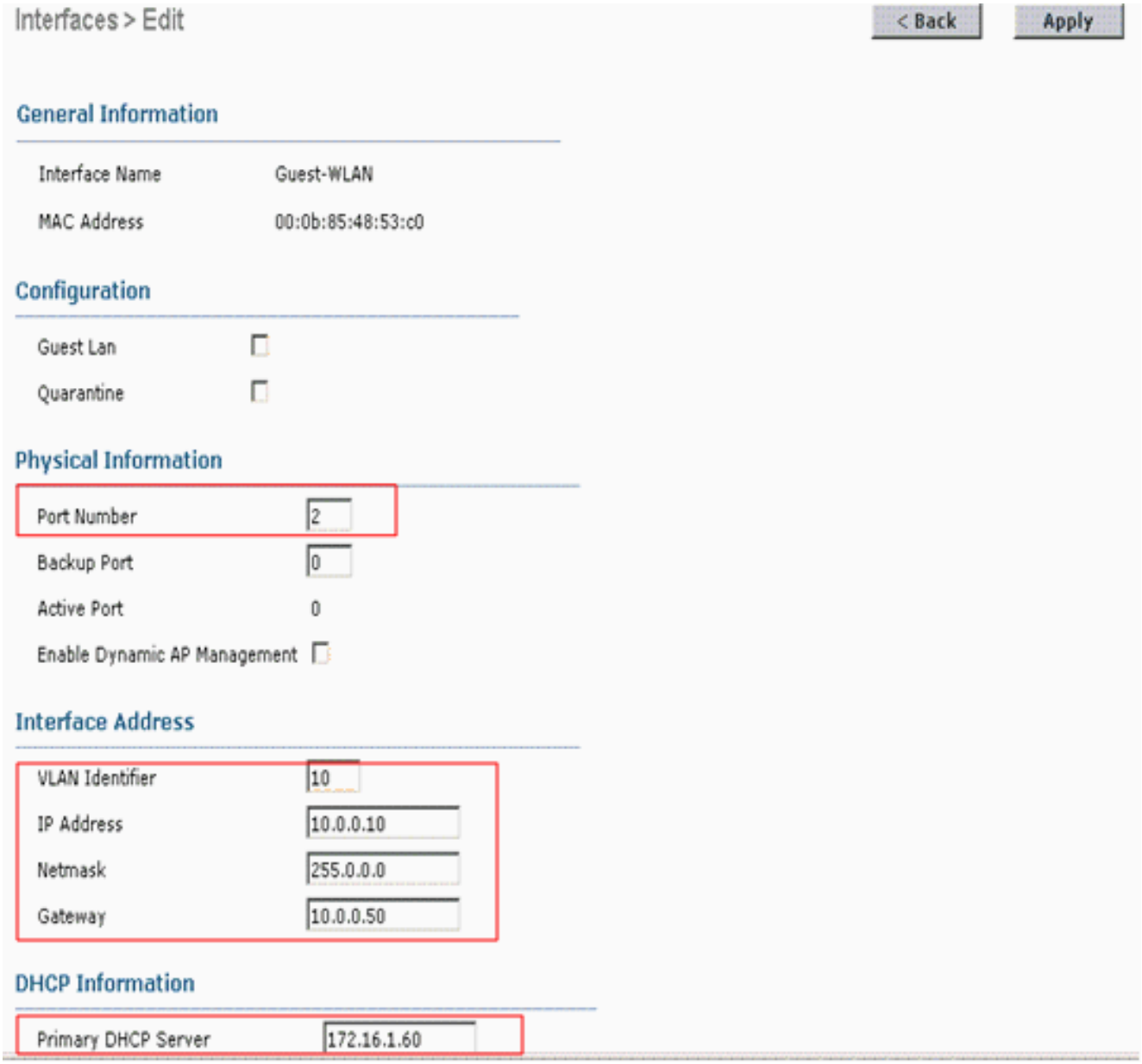


2. 새 동적 인터페이스**를** 생성하려면 New(새로 만들기)를 클릭합니다.
3. Interfaces(인터페이스) > New(새로 만들기) 창에서 Interface Name(인터페이스 이름) 및 VLAN Id(VLAN ID)를 입력한 다음 Apply(적용)를 **클릭합니다**.이 예에서 동적 인터페이스의 이름은 Guest-WLAN이고 VLAN Id는 10입니다

   .

4. Interfaces(인터페이스) > Edit(수정) 창에서 동적 인터페이스의 경우 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력합니다.WLC의 물리적 포트에 할당하고 DHCP 서버의 IP 주소를 입력합니다.그런 다음 **적용**을 클릭합니다.다음은 예입니다

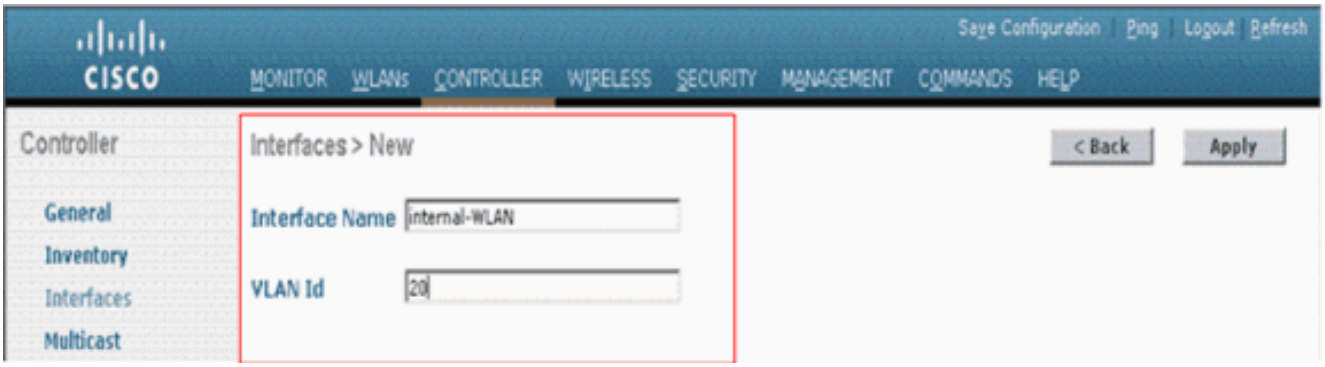
.



내부 WLAN에 대한 동적 인터페이스를 생성하려면 동일한 절차를 완료해야 합니다.

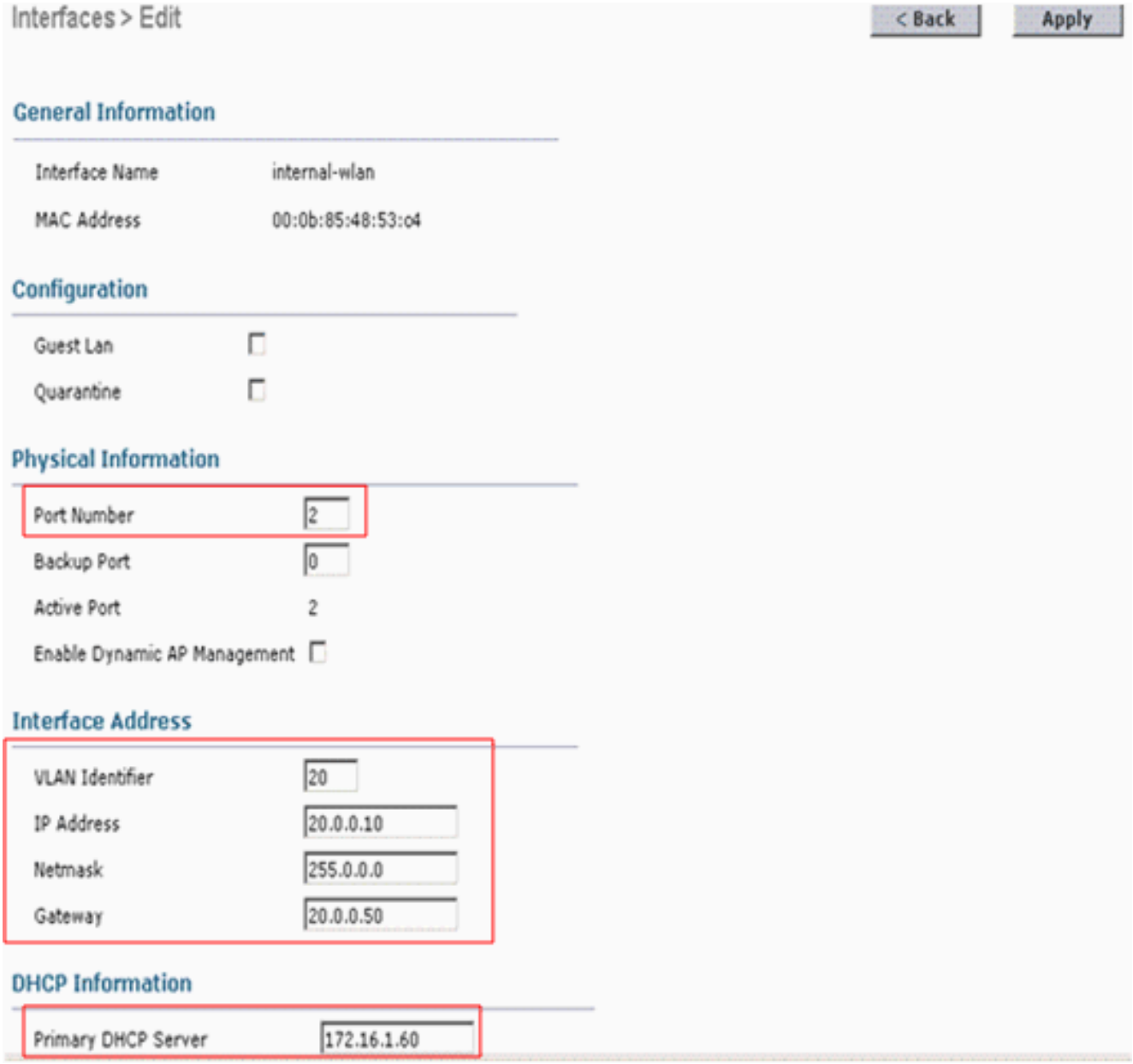
5. Interfaces(인터페이스) > New(새로 만들기) 창에서 내부 사용자의 동적 인터페이스에 대해 **Internal-WLAN**을 입력하고 VLAN ID에 **20**을 입력한 다음 Apply(적용)를 **클릭합니다**

.



6. Interfaces(인터페이스) > Edit(수정) 창에서 동적 인터페이스의 경우 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력합니다.WLC의 물리적 포트에 할당하고 DHCP 서버의 IP 주소를 입력합니다.그런 다음 **적용**을 클릭합니다

.



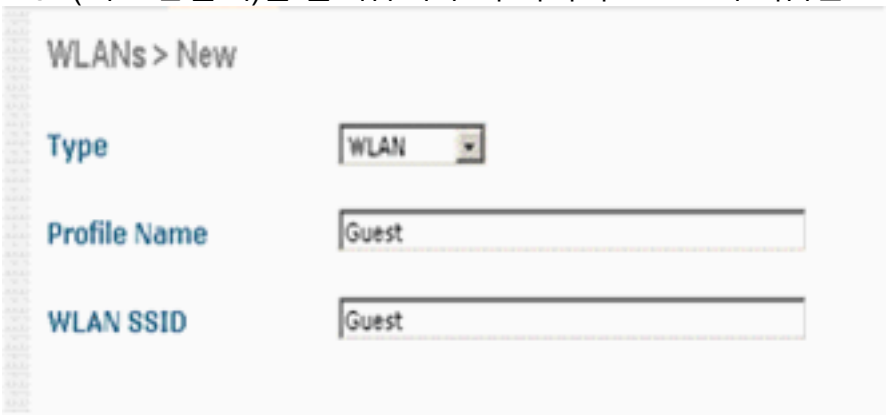
두 개의 동적 인터페이스가 생성되었으므로 Interfaces(인터페이스) 창에 컨트롤러에 구성된 인터페이스 목록이 요약됩니다

.

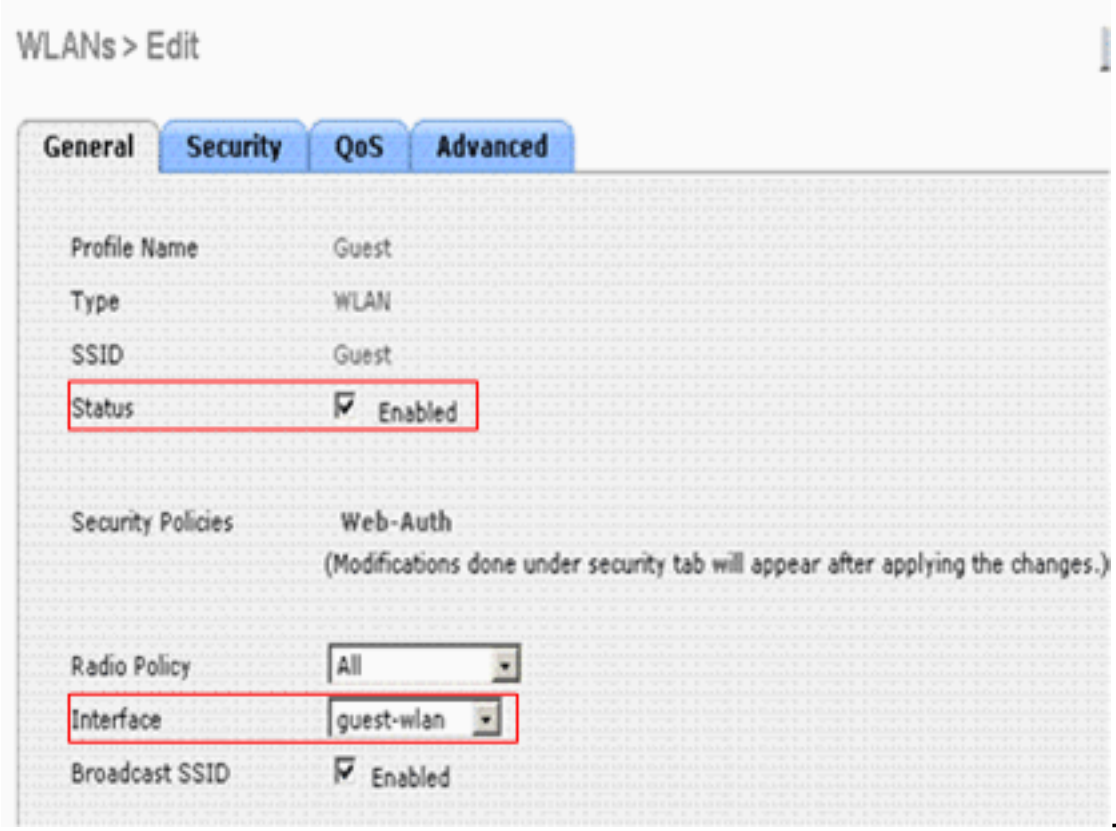
게스트 및 내부 사용자에 대한 WLAN 생성

다음 단계는 게스트 사용자 및 내부 사용자에 대한 WLAN을 생성하고 동적 인터페이스를 WLAN에 매핑하는 것입니다.또한 게스트 및 무선 사용자를 인증하는 데 사용되는 보안 방법을 정의해야 합니다.다음 단계를 완료하십시오.

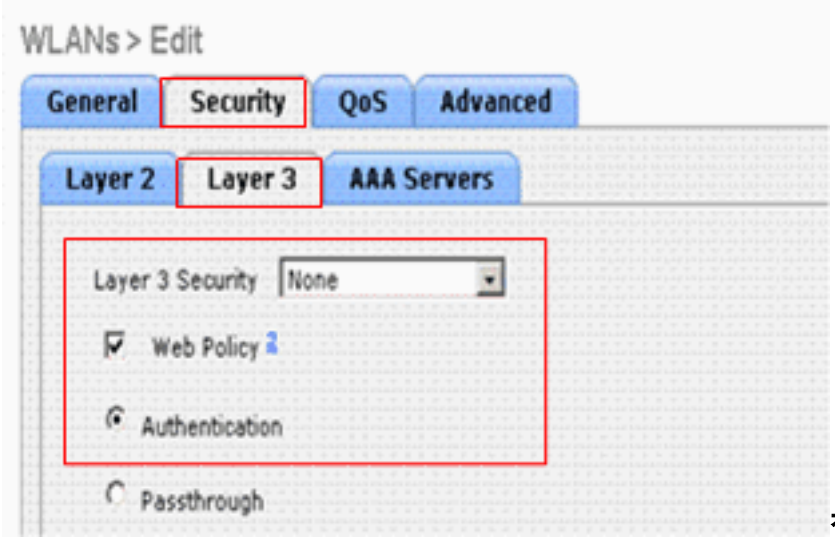
1. WLAN을 생성하려면 컨트롤러 GUI에서 WLANs를 클릭합니다.WLANs 창이 나타납니다.이 창에는 컨트롤러에 구성된 WLAN이 나열됩니다.
2. 새 WLAN을 구성하려면 **New**(새로 만들기)를 클릭합니다.이 예에서 WLAN의 이름은 *Guest*이고 WLAN ID는 2입니다.



3. 오른쪽 위에서 Apply를 클릭합니다.
4. 다양한 탭이 포함된 WLAN > Edit 화면이 나타납니다.게스트 WLAN의 **General**(일반) 탭 아래의 Interface Name(인터페이스 이름) 필드에서 **guest-wlan**을 선택합니다.이는 WLAN **게스트**에 이전에 생성된 동적 인터페이스 **게스트-wlan**을 **매핑합니다**.WLAN의 상태가 활성화되었는지 확인합니다

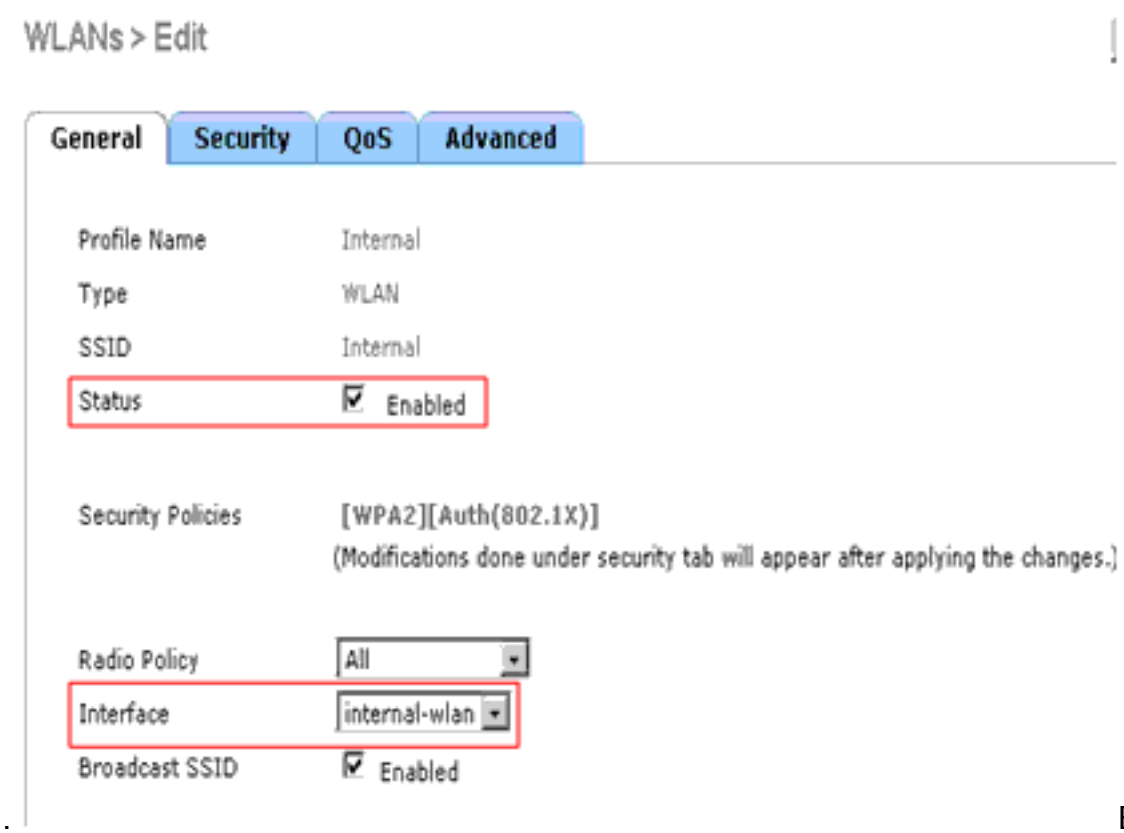


. **보안** 탭을 클릭합니다.이 WLAN의 경우 Web Authentication a Layer 3 보안 메커니즘이 클라이언트를 인증하는 데 사용됩니다.따라서 *Layer 2* Security 필드 아래에서 **None**을 선택합니다.Layer *3* Security 필드에서 **Web Policy(웹 정책)** 상자를 선택하고 Authentication(**인증**) 옵션을 선택합

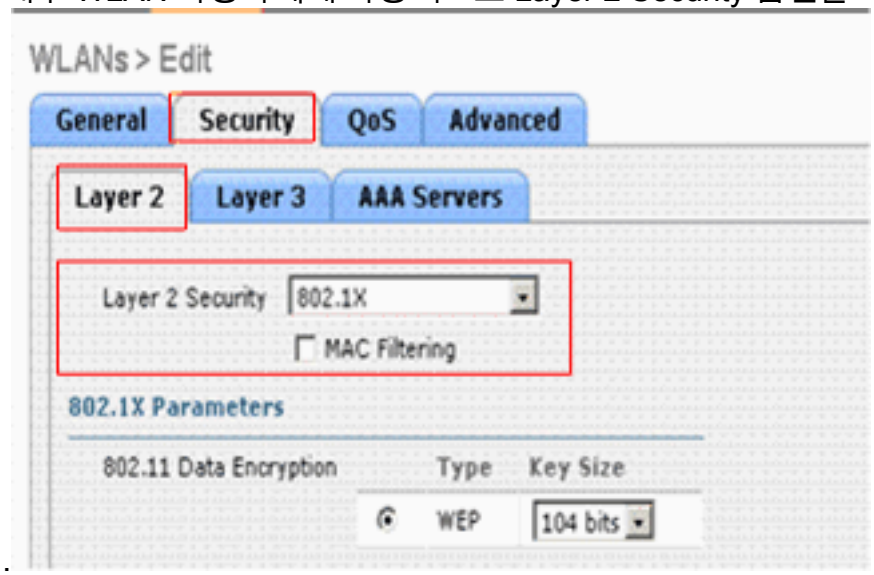


니다. **참고:** 웹 인증에 대한 자세한 내용은 Wireless LAN Controller 웹 인증 컨피그레이션 예를 참조하십시오.Apply를 **클릭합니다**.

5. 내부 사용자를 위한 WLAN을 생성합니다.WLANs(WLANs) > New(새) 창에서 **Internal(내부)**을 입력하고 **3(3)을** 선택하여 내부 사용자에 대한 WLAN을 생성합니다.그런 다음 **적용**을 클릭합니다.
6. WLANs > Edit(수정) 창이 나타납니다.General(*일반*) 탭의 Interface Name(인터페이스 이름) 필드**에서 internal-wlan**을 선택합니다.이렇게 하면 이전에 WLAN **내부**에 생성한 동적 인터페이스 **내부-wlan**이 **매핑됩니다**.WLAN이 활성화되었는지 확인합니다



. EAP 인증은 내부 WLAN 사용자에게 사용되므로 Layer 2 Security 옵션을 기본값 802.1x로 둡니다



.

7. Apply를 **클릭합니다**.WLAN 창이 나타나고 생성된 WLAN 목록이 표시됩니다

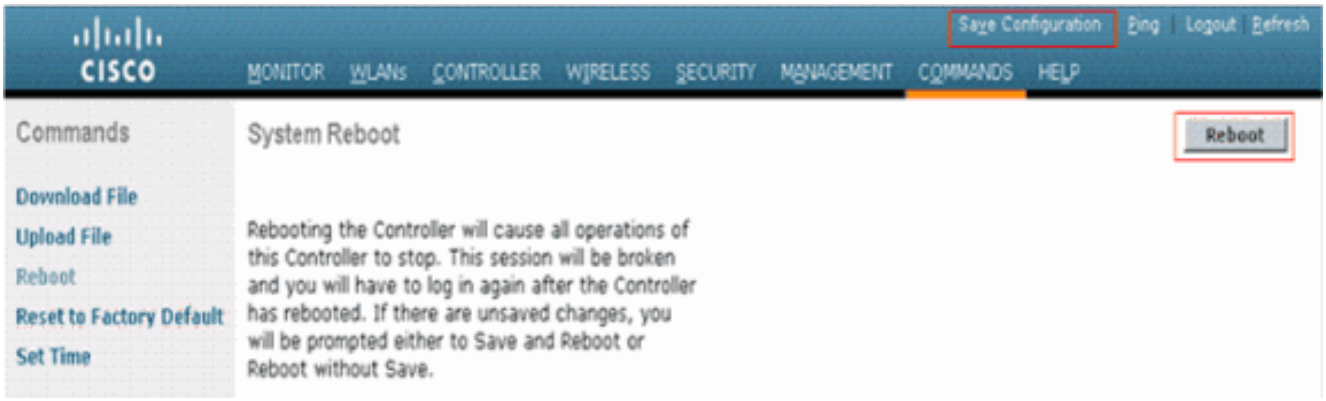
.

참고: WLC를 사용하여 EAP 기반 WLAN을 구성하는 방법에 대한 자세한 내용은 WLAN 컨트롤러(WLC)를 통한 EAP 인증 컨피그레이션 예를 참조하십시오.

8. WLC GUI에서 Save **Configuration**(컨피그레이션 저장)을 클릭한 다음 **Commands** from the

controller GUI를 클릭합니다.다음으로, **Reboot**(재부팅) 옵션을 선택하여 웹 인증이 적용되도록 WLC를 재부팅합니다

.



참고: Save **Configuration**(컨피그레이션 저장)을 클릭하여 재부팅 시 컨피그레이션을 저장합니다.

WLC에 트렁크 포트로 연결하는 레이어 2 스위치 포트 구성

WLC가 레이어 2 스위치에 연결되어 있으므로 WLC에 구성된 여러 VLAN을 지원하도록 스위치 포트를 구성해야 합니다.스위치 포트를 802.1Q 트렁크 포트로 구성해야 합니다.

각 컨트롤러 포트 연결은 802.1Q 트렁크이며 네이버 스위치에서 이 트렁크로 구성해야 합니다 .Cisco 스위치에서 802.1Q 트렁크의 네이티브 VLAN(예: **VLAN 1**)은 태그가 지정되지 않은 상태로 유지됩니다.따라서 네이버 Cisco 스위치에서 네이티브 VLAN을 사용하도록 컨트롤러의 인터페이스를 구성하는 경우 컨트롤러의 인터페이스를 태그되지 않은 것으로 구성해야 합니다.

VLAN 식별자(Controller > Interfaces 창에서)에 대한 0 값은 인터페이스가 태그가 지정되지 않았음을 의미합니다.이 문서의 예에서 AP-Manager 및 관리 인터페이스는 태그가 지정되지 않은 기본 VLAN으로 구성됩니다.

컨트롤러 인터페이스가 0이 아닌 값으로 설정된 경우 스위치의 네이티브 VLAN에 태깅하지 않아야 하며 스위치에서 VLAN을 허용해야 합니다.이 예에서 VLAN 60은 컨트롤러에 연결되는 스위치 포트에서 기본 VLAN으로 구성됩니다.

WLC에 연결되는 스위치 포트의 컨피그레이션입니다.

```
interface f0/12
Description Connected to the WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

다음은 라우터에 트렁크 포트로 연결하는 스위치 포트의 컨피그레이션입니다.

```
interface f0/10
Description Connected to the Router
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

LAP에 연결되는 스위치 포트의 컨피그레이션입니다.이 포트는 액세스 포트로 구성됩니다.

```
interface f0/9
Description Connected to the LAP
Switchport access vlan 60
switchport mode access
no ip address
```

두 WLAN에 대한 라우터 구성

이 문서의 예에서 2811 라우터는 게스트 사용자를 인터넷에 연결하고 내부 유선 사용자를 내부 무선 사용자에게 연결합니다.또한 DHCP 서비스를 제공하도록 라우터를 구성해야 합니다.

라우터에서 모든 VLAN에 대해 스위치의 트렁크 포트에 연결하는 FastEthernet 인터페이스 아래에 하위 인터페이스를 생성합니다.해당 VLAN에 하위 인터페이스를 할당하고 각 서브넷에서 IP 주소를 구성합니다.

참고: 라우터 컨피그레이션의 관련 부분만 지정되며 전체 컨피그레이션은 제공되지 않습니다.

이는 라우터에서 이 작업을 수행하는 데 필요한 컨피그레이션입니다.

다음은 라우터에서 DHCP 서비스를 구성하려면 실행해야 하는 명령입니다.

```
!
ip dhcp excluded-address 10.0.0.10
!--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC.
ip dhcp excluded-address 10.0.0.50 !--- IP excluded because this IP is assigned to the !--- sub-interface on the router. ip dhcp excluded-address 20.0.0.10 !--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC. ip dhcp excluded-address 20.0.0.50 !--- IP excluded because this IP is assigned to the sub-interface on the router. ! ip dhcp pool Guest !--- Creates a DHCP pool for the guest users. network 10.0.0.0 255.0.0.0 default-router 10.0.0.50 dns-server 172.16.1.1 !--- Defines the DNS server. ! ip dhcp pool Internal network 20.0.0.0 255.0.0.0 default-router 20.0.0.50 !--- Creates a DHCP pool for the internal users. !
```

다음 명령은 FastEthernet 인터페이스에서 실행되어야 설정 예시:

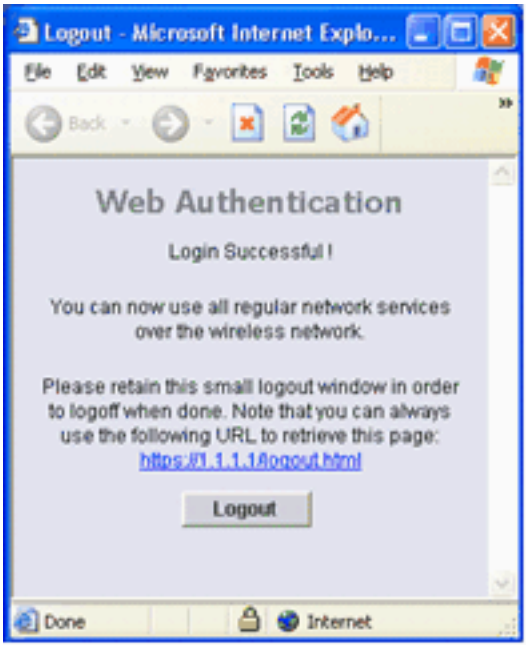
```
!
interface FastEthernet0/0
 description Connected to L2 Switch
 ip address 172.16.1.60 255.255.0.0
 duplex auto
 speed auto
!--- Interface connected to the Layer 2 switch. ! interface FastEthernet0/0.1 description Guest VLAN encapsulation dot1Q 10 ip address 10.0.0.50 255.0.0.0 !--- Creates a sub-interface under FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under FastEthernet0/0 for the internal VLAN. !
```

다음을 확인합니다.

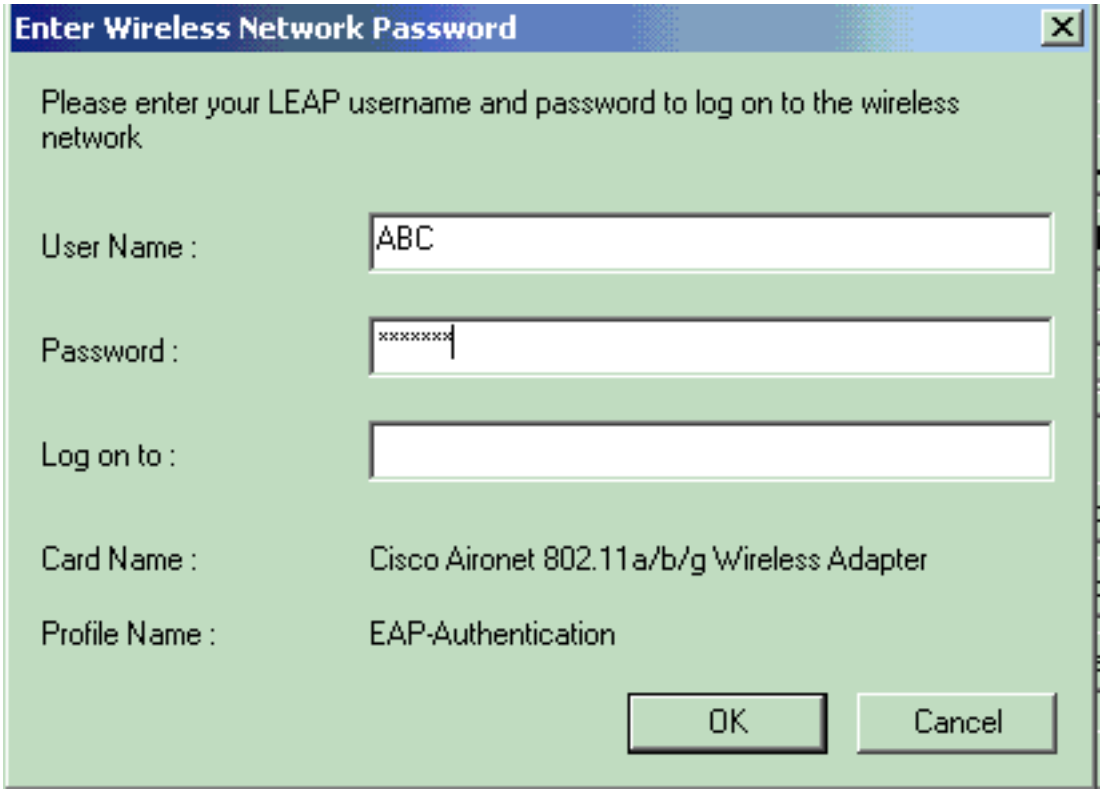
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

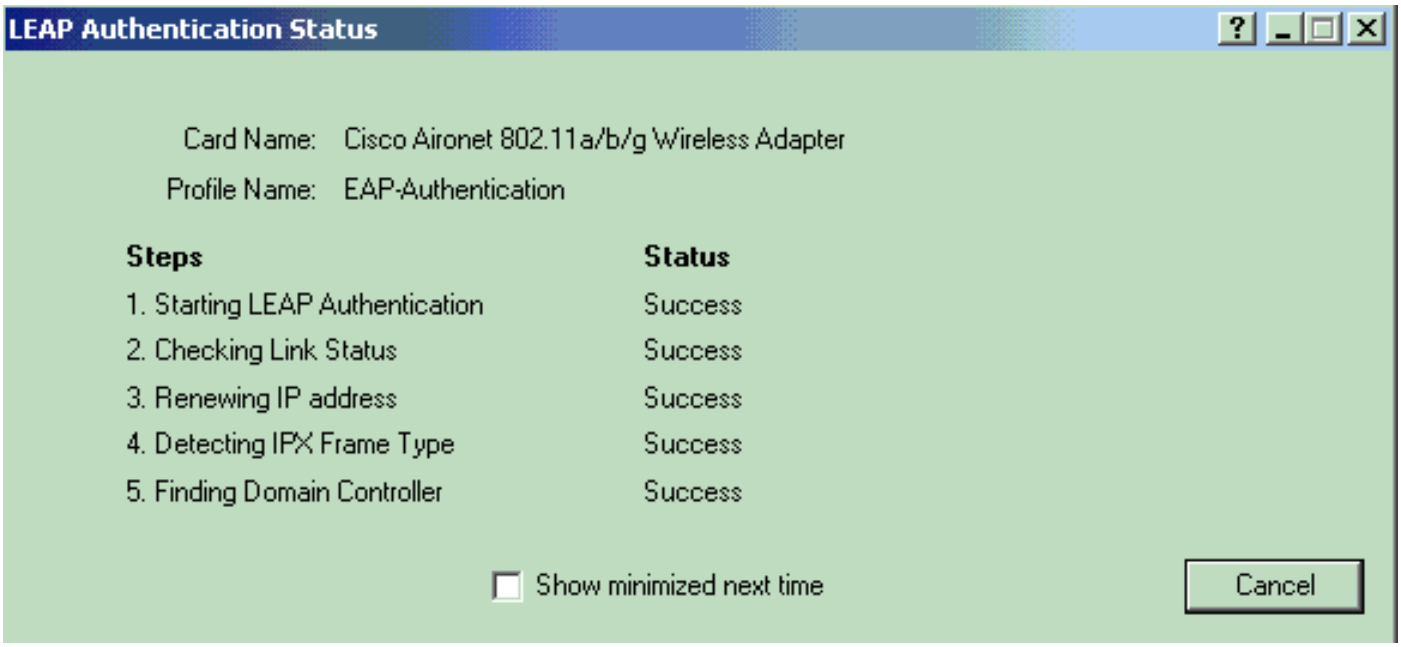
컨피그레이션이 예상대로 작동하는지 확인하기 위해 게스트 사용자(SSID(Service Set Identifier)**Guest**)와 내부 사용자(SSID **Internal** 포함) 1명의 두 무선 클라이언트를 연결합니다.

게스트 WLAN이 웹 인증을 위해 구성되었음을 기억하십시오.게스트 무선 클라이언트가 나타나면 웹 브라우저에 URL을 입력합니다.기본 웹 인증 페이지가 나타나고 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.게스트 사용자가 유효한 사용자 이름/비밀번호를 입력하면 WLC는 게스트 사용자를 인증하고 네트워크(인터넷 사용 가능)에 대한 액세스를 허용합니다. 다음 예에서는 사용자가 수신하는 웹 인증 창과 성공적인 인증에 대한 출력을 보여 줍니다.



이 예의 내부 WLAN은 802.1x 인증을 위해 구성됩니다.내부 WLAN 클라이언트가 나타나면 클라이언트는 EAP 인증을 사용합니다.EAP 인증을 위해 클라이언트를 구성하는 방법에 대한 자세한 내용은 Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter(CB21AG 및 PI21AG) Installation and Configuration Guide의 Using EAP Authentication(EAP 인증 사용) 섹션을 참조하십시오.인증에 성공하면 사용자는 내부 네트워크에 액세스할 수 있습니다.다음 예에서는 LEAP(Lightweight Extensible Authentication Protocol) 인증을 사용하는 내부 무선 클라이언트를 보여줍니다.





문제 해결

트러블슈팅 절차

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

컨피그레이션이 예상대로 작동하지 않으면 다음 단계를 완료하십시오.

1. WLC에 구성된 모든 VLAN이 WLC에 연결된 스위치 포트에서 허용되는지 확인합니다.
2. WLC와 라우터에 연결되는 스위치 포트가 트렁크 포트로 구성되어 있는지 확인합니다.
3. 사용된 VLAN ID가 WLC와 라우터에서 동일한지 확인합니다.
4. 클라이언트가 DHCP 서버에서 DHCP 주소를 수신하는지 확인합니다.그렇지 않은 경우

DHCP 서버가 올바르게 구성되었는지 확인합니다.클라이언트 문제 해결에 대한 자세한 내용은 Cisco Unified Wireless Network의 클라이언트 문제 해결을 참조하십시오.

웹 인증에서 자주 발생하는 문제 중 하나는 웹 인증 페이지로 리디렉션되는 것이 작동하지 않을 때입니다.브라우저를 열 때 사용자는 웹 인증 창을 볼 수 없습니다.대신 사용자가 https://1.1.1.1/login.html을 수동으로 입력해야 웹 인증 창에 액세스할 수 있습니다.이는 DNS 조회와 관련이 있으며, 웹 인증 페이지로 리디렉션되기 전에 작동해야 합니다.무선 클라이언트의 브라우저 홈페이지에서 도메인 이름을 가리키는 경우 클라이언트가 연결되면 성공적으로 nslookup 을 수행해야 리디렉션이 작동합니다.

또한 3.2.150.10 이전 버전을 실행하는 WLC의 경우 웹 인증이 작동하는 방식은 해당 SSID의 사용자가 인터넷에 액세스를 시도할 때 컨트롤러의 관리 인터페이스에서 URL이 유효한지 확인하기 위해 DNS 쿼리를 수행합니다.유효한 경우 URL은 가상 인터페이스 IP 주소가 있는 권한 부여 페이지를 표시합니다.사용자가 성공적으로 로그인하면 원래 요청이 클라이언트에 다시 전달될 수 있습니다.이는 Cisco 버그 ID CSCsc68105(등록된 고객만 해당) 때문입니다. 자세한 내용은 WLC(Wireless LAN Controller)에서 웹 인증 문제 해결을 참조하십시오.

문제 해결 명령

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

다음 debug 명령을 사용하여 컨피그레이션을 트러블슈팅할 수 있습니다.

- **debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx>** - 클라이언트에 대한 MAC 주소 디버깅을 구성합니다.
- **debug aaa all enable** - 모든 AAA 메시지의 디버그를 구성합니다.
- **debug pem state enable** - 정책 관리자 상태 시스템의 디버그를 구성합니다.
- **debug pem events enable** - 정책 관리자 이벤트의 디버그를 구성합니다.
- **debug dhcp message enable** - DHCP 클라이언트 활동에 대한 디버깅 정보를 표시하고 DHCP 패킷의 상태를 모니터링하려면 이 명령을 사용합니다.
- **debug dhcp packet enable** - DHCP 패킷 레벨 정보를 표시하려면 이 명령을 사용합니다.
- **debug pm ssh-appgw enable** - 애플리케이션 게이트웨이의 디버그를 구성합니다.
- **debug pm ssh-tcp enable** - 정책 관리자 tcp 처리의 디버그를 구성합니다.

다음은 다음 **debug** 명령의 샘플 출력입니다.

참고: 일부 출력 라인은 공간 이유로 인해 두 번째 행으로 래핑되었습니다.

```
(Cisco Controller) >debug dhcp message enable
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len,
including the magic cookie = 64
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: requested ip = 10.0.0.1
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option:
vendor class id = MSFT5.0 (len 8)
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions:
options end, len 64, actual 64
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 Forwarding DHCP packet
(332 octets)from 00:40:96:ac:e6:57
-- packet received on direct-connect port requires forwarding to external DHCP server.
```

```
Next-hop is 10.0.0.50
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len,
including the magic cookie = 64
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50
Fri Mar  2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions:
options end, len 64, actual 64
```

(Cisco Controller) >debug dhcp packet enable

```
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet:
Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1,
encap: 0xec03
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request,
client: 00:40:96:ac:e6:57: dhcp op: 1, port: 2, encap 0xec03, old mscb
port number: 2
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57
dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50,
dhcpRelay: 10.0.0.10  VLAN: 30
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57
Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50,
VLAN: 30, port: 2
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received:
DHCP REQUEST msg
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   op: BOOTREQUEST, htype:
Ethernet,hlen: 6, hops: 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   xid: 1674228912, secs: 0, flags: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   chaddr: 00:40:96:ac:e6:57
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   ciaddr: 10.0.0.1,  yiaddr: 0.0.0.0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   siaddr: 0.0.0.0,  giaddr: 10.0.0.10
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50,
len 350,switchport 2, vlan 30
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet:
Client 00:40:96:ac:e6:57  DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 2,
encap: 0xec00
Fri Mar  2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57, frame len412,
switchport 2
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP ACK msg
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   xid: 1674228912, secs: 0, flags: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   chaddr: 00:40:96:ac:e6:57
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   ciaddr: 10.0.0.1,  yiaddr: 10.0.0.1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   server id: 1.1.1.1
rcvd server id: 10.0.0.50
```

(Cisco Controller) >debug aaa all enable

```
Fri Mar  2 16:22:40 2007: User user1 authenticated
Fri Mar  2 16:22:40 2007: 00:40:96:ac:e6:57
Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57
Fri Mar  2 16:22:40 2007: AuthorizationResponse: 0xbadff97c
Fri Mar  2 16:22:40 2007: structureSize.............................70
Fri Mar  2 16:22:40 2007: resultCode................................0
```

```
Fri Mar  2 16:22:40 2007: protocolUsed.............................0x00000008
Fri Mar  2 16:22:40 2007: proxyState..............00:40:96:AC:E6:57-00:00
Fri Mar  2 16:22:40 2007:  Packet contains 2 AVPs:
Fri Mar  2 16:22:40 2007: AVP[01] Service-Type............0x00000001 (1) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[02] Airespace /
WLAN-Identifier......0x00000001 (1) (4 bytes)
Fri Mar  2 16:22:40 2007: 00:40:96:ac:e6:57 Applying new AAA override
for station 00:40:96:ac:e6:57
Fri Mar  2 16:22:40 2007: 00:40:96:ac:e6:57 Override values for station
00:40:96:ac:e6:57
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
         vlanIfName: '', aclName:
Fri Mar  2 16:22:40 2007: 00:40:96:ac:e6:57 Unable to apply override
policy for station 00:40:96:ac:e6:57
- VapAllowRadiusOverride is FALSE
Fri Mar  2 16:22:40 2007: AccountingMessage Accounting Start: 0xa62700c
Fri Mar  2 16:22:40 2007: Packet contains 13 AVPs:
Fri Mar  2 16:22:40 2007: AVP[01] User-Name...............user1 (5 bytes)
Fri Mar  2 16:22:40 2007: AVP[02] Nas-Port.............0x00000001 (1) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[03]
Nas-Ip-Address.......0x0a4df4d2 (172881106) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[04]
NAS-Identifier......0x574c4331 (1464615729) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[05]
Airespace / WLAN-Identifier..............0x00000001 (1) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[06]
Acct-Session-Id.........................45e84f50/00:40:96:ac:e6:57/9 (28 bytes)
Fri Mar  2 16:22:40 2007: AVP[07]
Acct-Authentic..........................0x00000002 (2) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[08]
Tunnel-Type.............................0x0000000d (13) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[09]
Tunnel-Medium-Type......................0x00000006 (6) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[10]
Tunnel-Group-Id.........................0x3330 (13104) (2 bytes)
Fri Mar  2 16:22:40 2007: AVP[11]
Acct-Status-Type........................0x00000001 (1) (4 bytes)
Fri Mar  2 16:22:40 2007: AVP[12]
Calling-Station-Id......................10.0.0.1 (8 bytes)
Fri Mar  2 16:22:40 2007: AVP[13]
Called-Station-Id.......................10.77.244.210 (13 bytes)
```

when web authentication is closed by user:

```
(Cisco Controller) >Fri Mar  2 16:25:47 2007: AccountingMessage
Accounting Stop: 0xa627c78
Fri Mar  2 16:25:47 2007: Packet contains 20 AVPs:
Fri Mar  2 16:25:47 2007:
AVP[01] User-Name...............................user1 (5 bytes)
Fri Mar  2 16:25:47 2007:
AVP[02] Nas-Port................................0x00000001 (1) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[03] Nas-Ip-Address..........................0x0a4df4d2 (172881106) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[04] NAS-Identifier..........................0x574c4331 (1464615729) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[05] Airespace / WLAN-Identifier..............0x00000001 (1) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[06] Acct-Session-Id.............45e84f50/00:40:96:ac:e6:57/9 (28 bytes)
Fri Mar  2 16:25:47 2007:
AVP[07] Acct-Authentic..........................0x00000002 (2) (4 bytes)
```

```
Fri Mar  2 16:25:47 2007:
AVP[08] Tunnel-Type.............................0x0000000d (13) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[09] Tunnel-Medium-Type......................0x00000006 (6) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[10] Tunnel-Group-Id.........................0x3330 (13104) (2 bytes)
Fri Mar  2 16:25:47 2007:
AVP[11] Acct-Status-Type........................0x00000002 (2) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[12] Acct-Input-Octets.......................0x0001820e (98830) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[13] Acct-Output-Octets......................0x00005206 (20998) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[14] Acct-Input-Packets......................0x000006ee (1774) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[15] Acct-Output-Packets.....................0x00000041 (65) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[16] Acct-Terminate-Cause....................0x00000001 (1) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[17] Acct-Session-Time.......................0x000000bb (187) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[18] Acct-Delay-Time.........................0x00000000 (0) (4 bytes)
Fri Mar  2 16:25:47 2007:
AVP[19] Calling-Station-Id......................10.0.0.1 (8 bytes)
Fri Mar  2 16:25:47 2007:
AVP[20] Called-Station-Id.......................10.77.244.210 (13 bytes)
```

(Cisco Controller) >debug pem state enable

```
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Change state to START (0)
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
AUTHCHECK (2) Change stateto L2AUTHCOMPLETE (4)
Fri Mar  2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8)
Fri Mar  2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14)
Fri Mar  2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_NOL3SEC (14) Change state to RUN (20)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1
DHCP_REQD (7) Change stateto RUN (20)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
```

```
START (0) Change state to AUTHCHECK (2)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2
DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)
```

(Cisco Controller) >debug pem events enable

```
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policy
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4)
Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Replacing Fast Path rule
  type = Temporary Entry
  on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Deleting mobile policy rule 27
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web RuleID 28 for
mobile 00:40:96:ac:e6:57
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
ReplacingFast Path rule
  type = Temporary Entry
  on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry.
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
```

관련 정보

- 무선 게스트 액세스 FAQ
- Cisco WLAN Controller를 사용한 유선 게스트 액세스 컨피그레이션 예
- 무선 LAN 컨트롤러 컨피그레이션에 대한 인증 예
- 무선 LAN 컨트롤러를 사용한 외부 웹 인증 컨피그레이션 예
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0
- 무선 제품 지원
- 기술 지원 및 문서 – Cisco Systems