WAP551 및 WAP561 액세스 포인트에서 MAC 기반 ACL(Access Control List) 구성

목표

ACL(Access Control List)은 보안을 제공하고, 권한이 없는 사용자를 차단하고, 권한이 있는 사용자가 특정 리소스에 액세스할 수 있도록 하는 규칙(규칙)이라는 허용 및 거부 조건의 모음입니다.ACL은 네트워크 리소스에 도달하려는 비보증적 시도를 차단할 수 있습니다. MAC ACL은 레이어 2 ACL입니다.네트워크 디바이스는 프레임을 검사하고 프레임의 내용에 대해 ACL 규칙을 확인합니다.어떤 규칙이 내용과 일치하면 프레임에 허용 또는 거부 작업이 수행됩니다.

이 문서의 목적은 WAP551 및 WAP561 액세스 포인트에서 MAC ACL을 만들고 구성하는 방법을 사용자에게 보여 주는 것입니다.

적용 가능한 디바이스

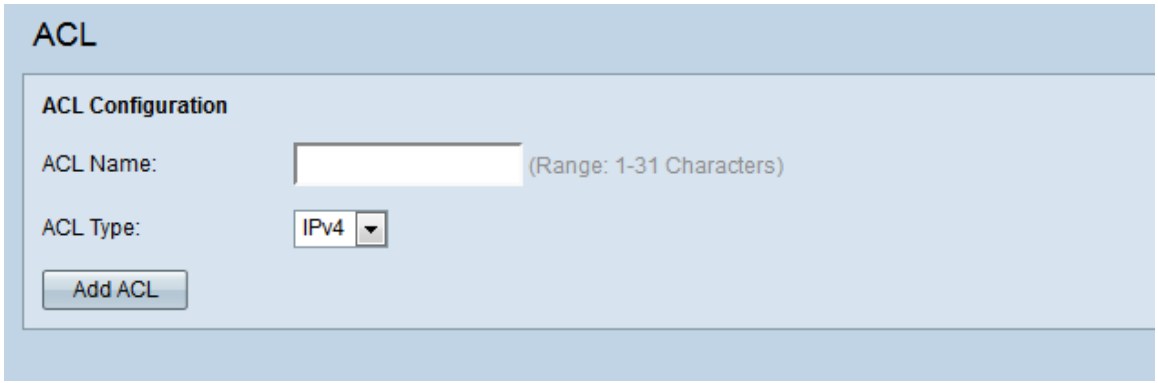
·WAP551
· WAP561

소프트웨어 버전

·v1.0.4.2

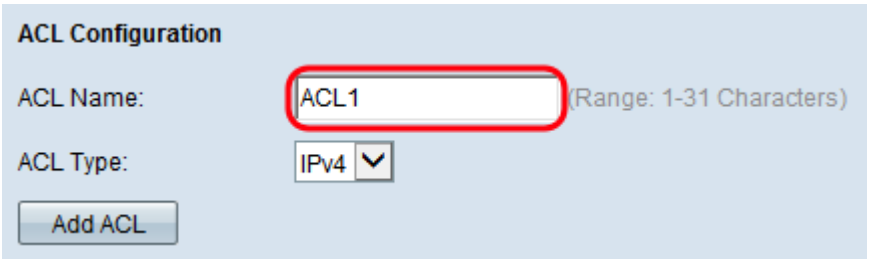
MAC ACL 구성

1단계. 웹 구성 유틸리티에 로그인하고 Client QoS(클라이언트 QoS) **> ACL을** 선택합니다. *ACL* 페이지가 열립니다.

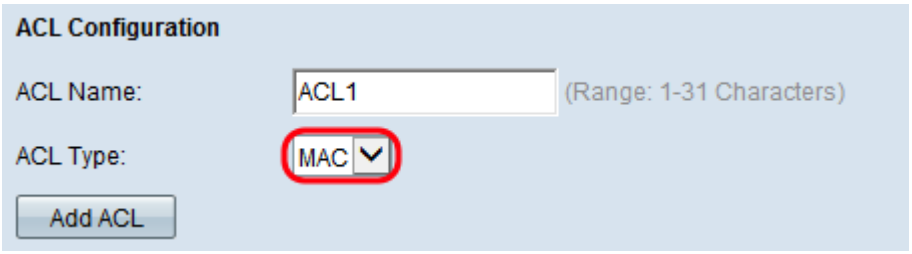


MAC ACL 생성

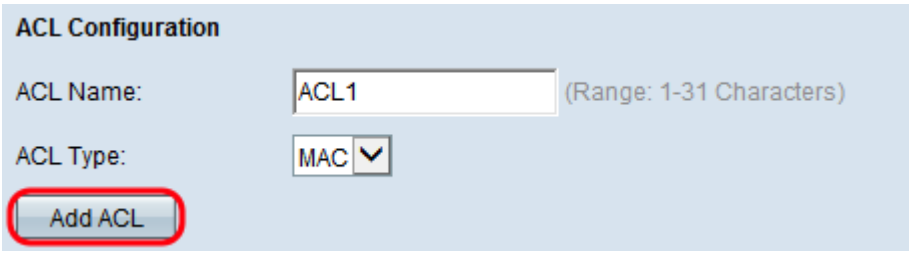
1단계. *ACL 이름* 필드에 ACL의 이름을 입력합니다.



2단계. *ACL Type* 드롭다운 목록에서 ACL 유형에 대한 **MAC**을 선택합니다.

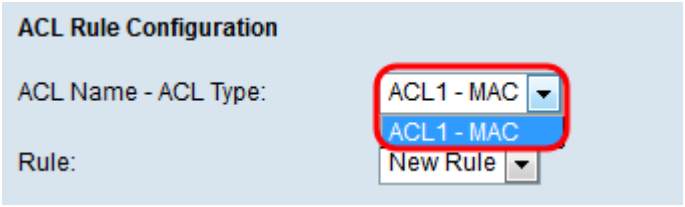


3단계. **Add ACL(ACL 추가)**을 클릭하여 새 MAC ACL을 생성합니다.

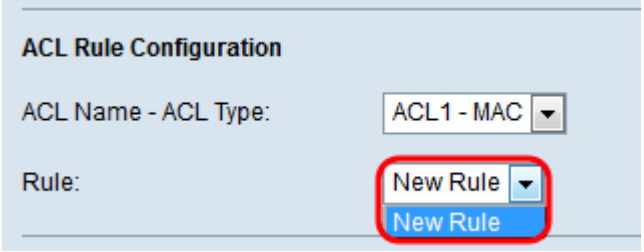


MAC ACL에 대한 규칙 컨피그레이션

1단계. ACL *Name-ACL Type(ACL 이름-ACL 유형)* 드롭다운 목록에서 규칙을 추가할 ACL을 선택합니다.

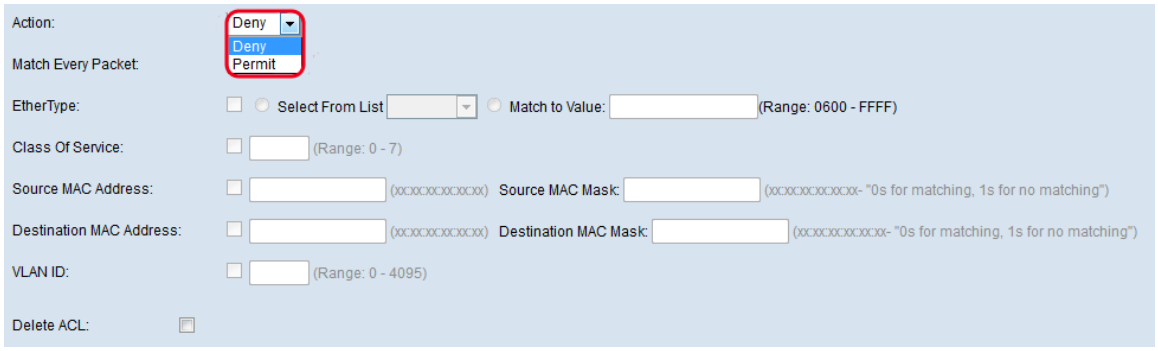


2단계. 선택한 ACL에 대해 새 규칙을 구성해야 하는 경우 *Rule* 드롭다운 목록에서 **New Rule(새 규칙)**을 선택합니다.그렇지 않으면 Rule 드롭다운 목록에서 현재 규칙 중 하나*를* 선택합니다.



참고:단일 ACL에 대해 최대 10개의 규칙을 생성할 수 있습니다.

3단계. Action(작업) 드롭다운 목록에서 ACL 규칙에 대한 *작업*을 선택합니다.



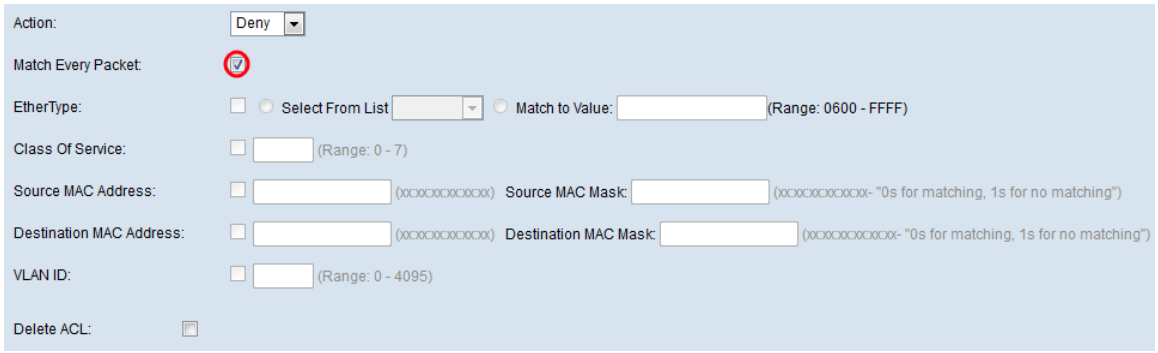
사용 가능한 옵션은 다음과 같이 정의됩니다.

·거부 — 규칙 기준을 충족하는 모든 트래픽을 차단하여 WAP 디바이스를 입력하거나 종료합니다.

·허용 — 규칙 기준을 충족하는 모든 트래픽이 WAP 디바이스를 입력하거나 종료할 수 있습니다.

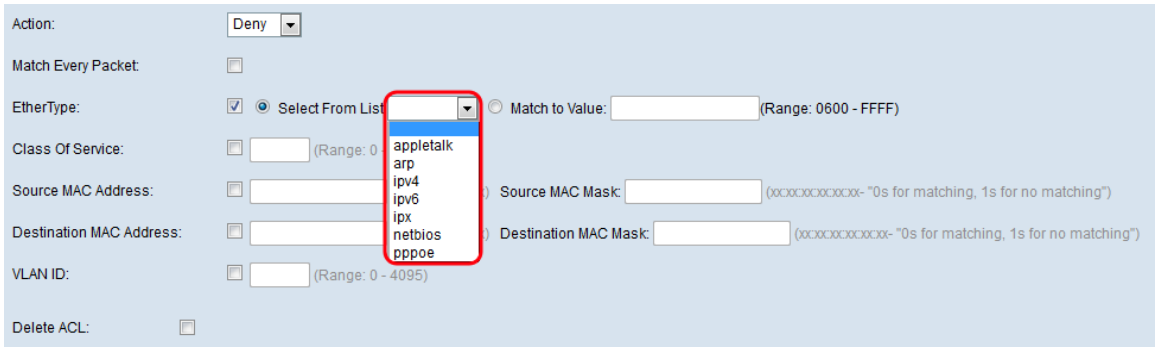
참고:4~9단계는 선택 사항입니다.ACL 규칙에 필터를 적용하지 않으려면 해당 상자의 선택을 취소합니다.

4단계. (선택 사항) **Match Every Packet(모든 패킷** 일치) 확인란을 선택하여 해당 내용에 관계없이 모든 프레임 또는 패킷에 대한 규칙을 일치시킵니다. **Match Every Packet(모든 패킷** 일치) 확인란의 선택을 취소하여 추가 일치 기준을 구성합니다.



Match Every Packet(모든 패킷 *일치)* 상자가 선택된 경우 11단계로 건너뜁니다.

5단계. (선택 사항) **EtherType** 확인란을 선택하여 일치 기준을 이더넷 프레임 헤더의 값과 비교합니다.EtherType 확인란*을* 선택한 경우 *Select From List* 또*는 Match to Value* 라디오 버튼을 클릭합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

·목록에서 선택 — 드롭다운 목록에서 프로토콜을 선택할 수 있습니다.사용 가능한 옵션은 appletalk, arp, ipv4, ipv6, ipx, netbios 및 pppoe입니다.옵션을 선택하면 선택한 프로토콜의

패킷에 규칙이 적용됩니다.

- appletalk — Apple Inc.에서 Macintosh 컴퓨터를 위해 설계한 네트워크 프로토콜입니다.Appletalk는 플러그 앤 플레이 시스템입니다.사용자 입력 없이 자동으로 주소를 할당하고 다른 네트워크 구성을 처리합니다.

- arp — ARP(Address Resolution Protocol)는 IP 주소를 MAC 주소로 변환하는 데 사용되는 중요한 프로토콜입니다.

- ipv4 — IPv4(인터넷 프로토콜 버전 4)는 인터넷에서 대부분의 트래픽을 담당하는 중요한 프로토콜입니다.디바이스의 IP 주소를 처리합니다.

- ipv6 — IPv6는 IPv4 및 최신 버전의 인터넷 프로토콜의 후속 버전입니다.대부분의 기존 IPv4 IP 주소가 고갈된 것에 대응하여 개발되었습니다.

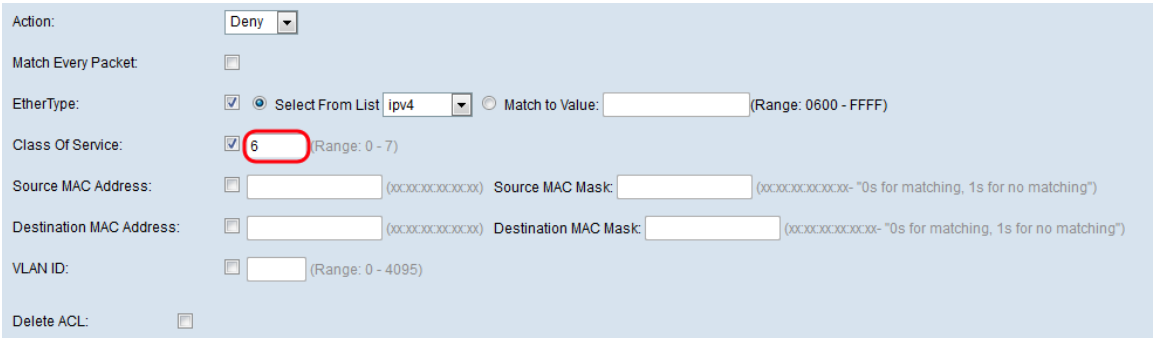
- ipx — IPX(Internetwork Packet Exchange)는 네트워크/전송 프로토콜입니다.프로토콜이 대규모 네트워크에서도 제대로 작동하지 않지만 IPX가 TCP/IP보다 훨씬 뛰어난 IPX는 사용하는 적은 양의 메모리입니다.

- netbios — NetBIOS(Network Basic Input/Output System)는 일반적으로 최신 네트워크에서 TCP/IP와 함께 실행되는 API(애플리케이션 프로그래밍 인터페이스)입니다.

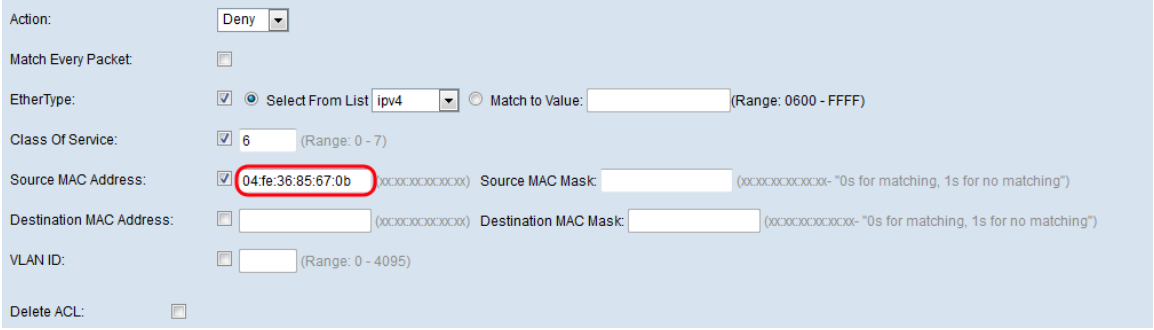
- pppoe - PPPoE(Point-to-Point Protocol over Ethernet)는 이더넷 패킷 내에 PPP 패킷을 캡슐화하는 데 사용되는 네트워크 프로토콜입니다.

·Match to Value(값에 일치) - Match to Value(값에 일치) 필드에 사용자 지정 프로토콜 식별자*를 입력할 수 있습니다*.이 옵션은 *Select From List* 드롭다운 목록에 포함되지 않은 프로토콜로 패킷을 필터링하려는 경우 유용합니다.유효한 사용자 지정 프로토콜 식별자의 범위는 0600부터 FFFF까지입니다.

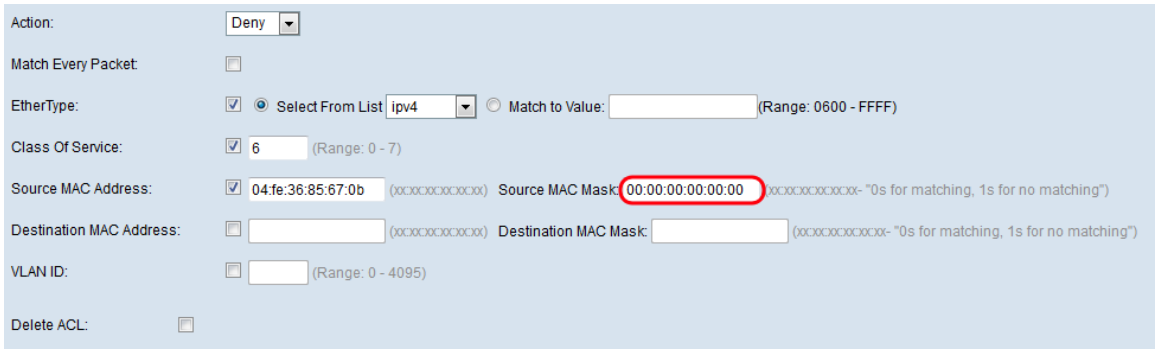
6단계. (선택 사항) **Class of Service** 확인란을 선택하여 이더넷 프레임과 비교할 802.1p 사용자 우선순위를 입력합니다.서비스 *클래스* 필드에 0~7의 우선순위*를* 입력합니다.



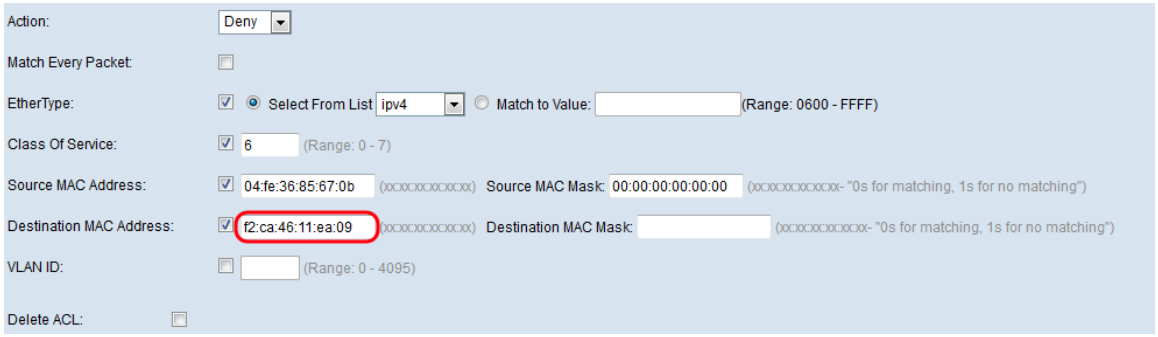
7단계. (선택 사항) 소스 MAC 주소를 이더넷 프레임과 비교하고 소스 MAC 주소를 Source *MAC Address* 필드에 입력하려면 Source MAC Address 확인란을 선택합니다.



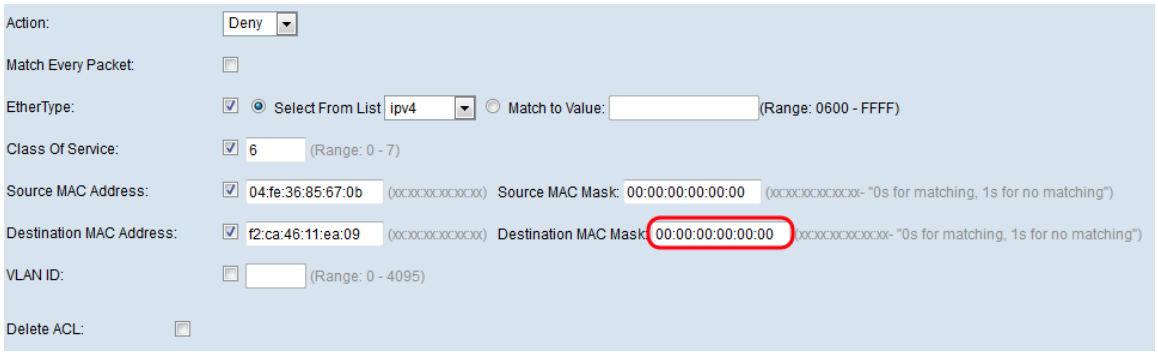
8단계. (선택 사항) 소스 MAC에서 이더넷 프레임과 비교할 비트를 지정하는 소스 MAC *마스크* 필드에 소스 MAC 주소 마스크를 입력합니다.



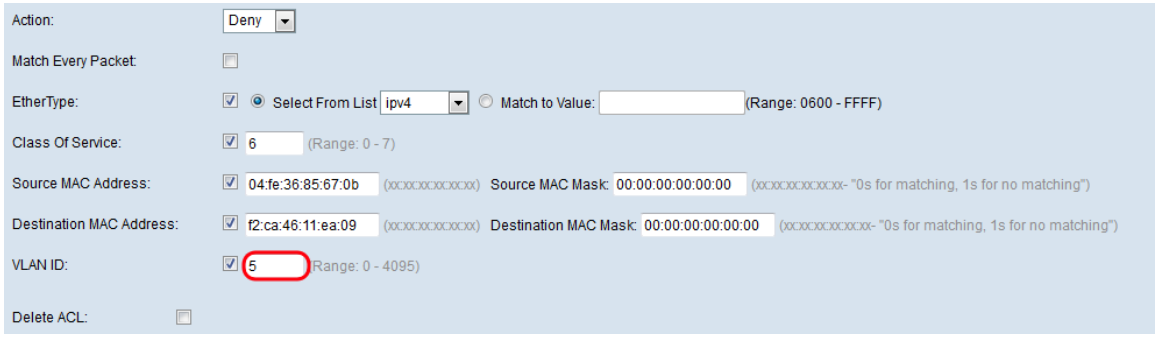
9단계. (선택 사항) 대상 MAC 주소를 이더넷 프레임과 비교하려면 **Destination MAC Address** 확인란을 선택하고 Destination MAC Address 필드에 대상 MAC 주소를 *입력합니다*.



10단계. (선택 사항) 대상 MAC의 비트를 이더넷 프레임과 비교할 대상 MAC의 비트를 지정하는 *Destination MAC Mask* 필드에 대상 MAC 주소 마스크를 입력합니다.



11단계. (선택 사항) VLAN ID를 이더넷 프레임과 비교하려면 **VLAN ID** 확인란을 선택합니다 .VLAN *ID* 필드에 0에서 4095 사이의 원하는 VLAN ID를 입력합니다.



12단계(선택 사항) 구성된 ACL을 삭제하려면 **Delete ACL** 확인란을 선택합니다.

13단계. 저장을 **클릭합니다**.