WAP121 및 WAP321 액세스 포인트에서 MAC 기반 ACL(Access Control List) 생성 및 구성

목표

ACL(Access Control List)은 보안을 제공하고 권한이 없는 사용자를 차단하고 권한 있는 사용자가 특정 리소스에 액세스할 수 있도록 허용하는 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 소스 및 대상 MAC 주소와 같은 프레임의 내용에 대해 ACL 규칙을 확인합니다.어떤 규칙이 내용과 일치하면 프레임에 허용 또는 거부 작업이 수행됩니다.

이 문서에서는 WAP121 및 WAP321 액세스 포인트(WAP)에서 MAC ACL을 생성하고 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

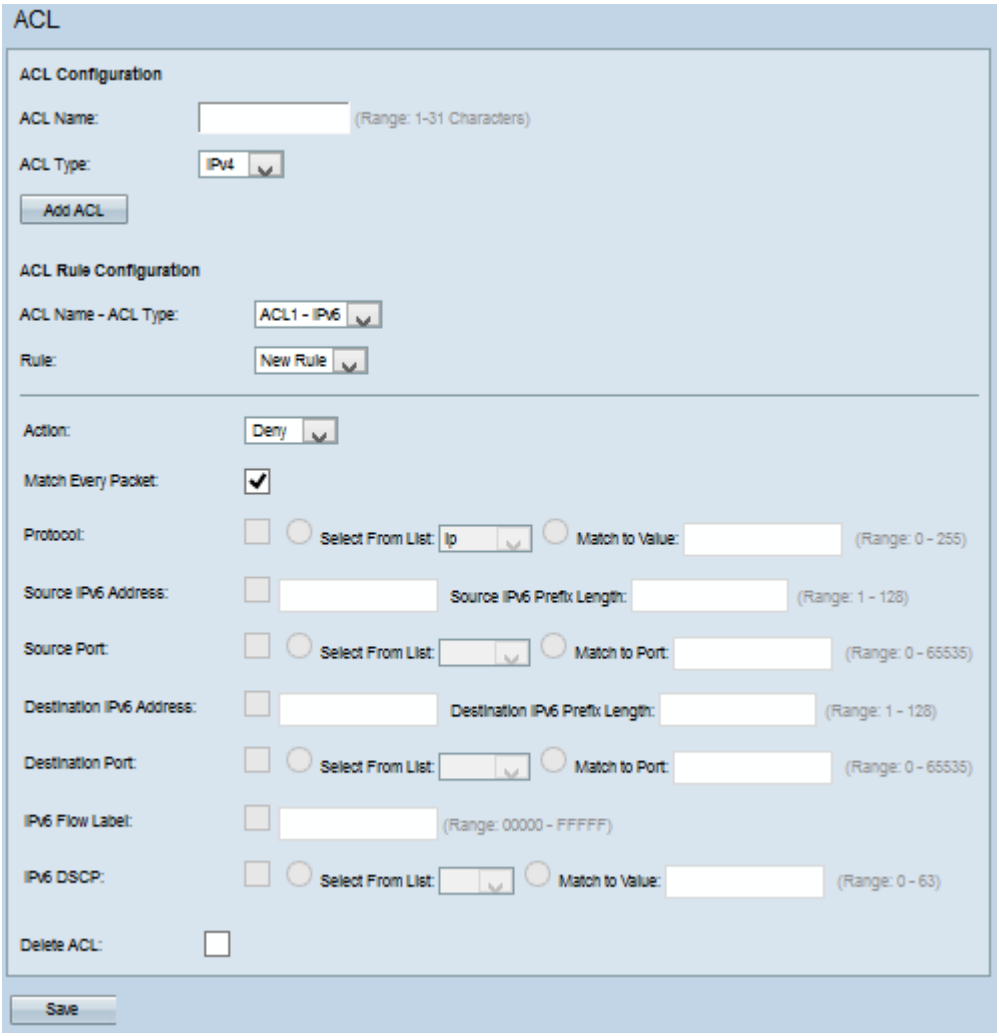
·WAP121
· WAP321

소프트웨어 버전

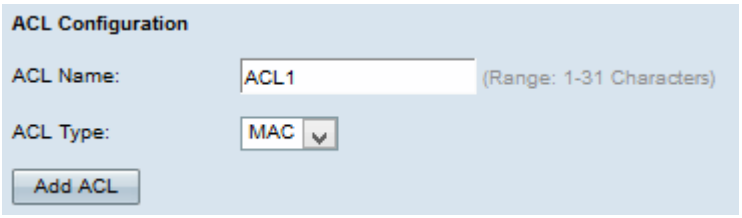
·v1.0.3.4

MAC 기반 ACL 생성

1단계. Access Point Configuration Utility에 로그인하고 Client QoS **> ACL을** 선택합니다.*ACL* 페이지가 열립니다.



MAC 기반 ACL 생성

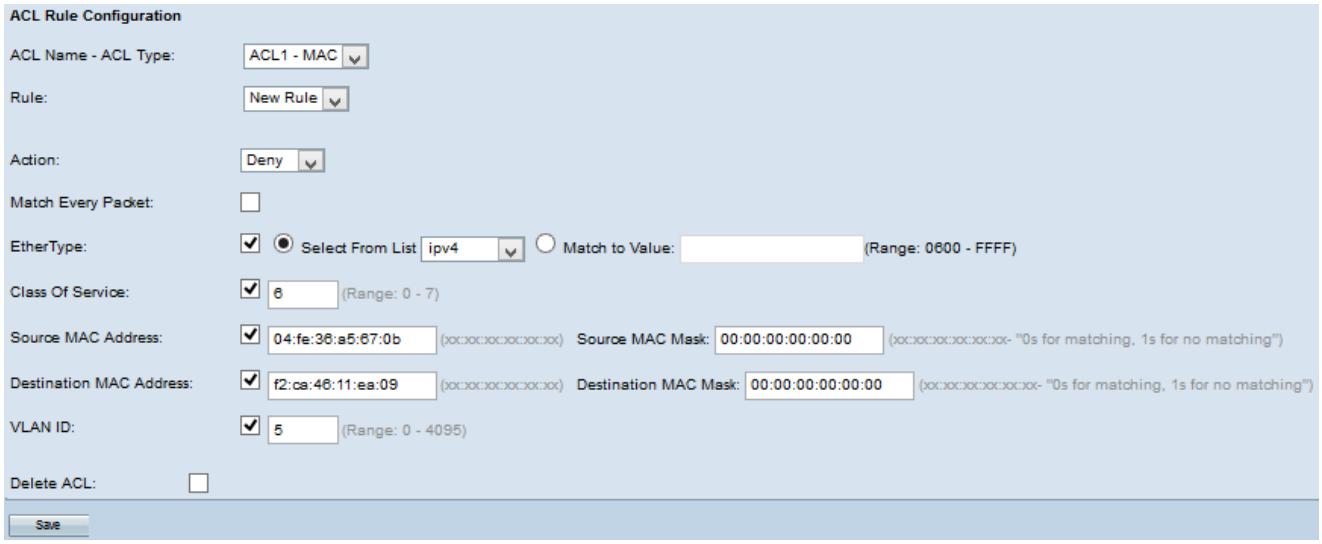


1단계. *ACL 이름* 필드에 ACL의 이름을 입력합니다.

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

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

MAC 기반 ACL에 대한 규칙 구성



1단계. *ACL 이름 - ACL 유형* 드롭다운 목록에서 원하는 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.

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

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

참고:4~11단계는 선택 사항입니다.선택한 필터가 활성화됩니다.이 특정 규칙에 적용하지 않으려면 필터의 확인란을 선택 취소합니다.

4단계. **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.

시간대버: Match Every **Packet(모든 패킷 일치)**을 선택한 경우 12단계로 건너뜁니다.

5단계. **EtherType** 확인란을 선택하여 일치 기준을 이더넷 프레임 헤더의 값과 비교합니다.이더 **유형** 확인란을 선택한 경우 이러한 라디오 버튼 중 하나를 클릭합니다.

·목록에서 선택 — 드롭다운 목록에서 프로토콜을 선택합니다.드롭다운 목록에는 appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe가 있습니다.

·값에 일치 — 사용자 지정 프로토콜 식별자의 경우0600에서 FFFF 사이의 식별자를 입력합니다.

6단계. **Class of Service** 확인란을 선택하여 802.1p 사용자 우선순위를 입력하여 이더넷 프레임과 비교합니다.*서비스 클래스* 필드에 0~7의 우선순위를 입력합니다.

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

8단계. 소스 MAC의 비트를 이더넷 프레임과 비교할 *소스 MAC*의 비트를 지정하는 소스 MAC

주소 마스크를 Source MAC Mask 필드에 입력합니다.MAC 마스크가 0비트를 사용하는 경우 주소가 수락되고 1비트를 사용하는 경우 주소가 무시됩니다.

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

10단계. 대상 MAC의 비트를 이더넷 프레임과 비교할 대상 MAC의 비트를 지정하는 *Destination MAC Mask* 필드에 대상 MAC 주소 마스크를 입력합니다.MAC 마스크가 0비트를 사용하는 경우 주소가 수락되고 1비트를 사용하는 경우 주소가 무시됩니다.

11단계. **VLAN ID** 확인란을 선택하여 VLAN ID를 이더넷 프레임과 비교합니다.VLAN *ID* 필드에 0~4095 범위의 VLAN ID를 입력합니다.

참고:새 VLAN을 생성하는 방법에 대한 자세한 내용은 WAP*121 및 WAP321의 관리 및 태그 없는 VLAN ID 구성 문서를 참조하십시오.*

12단계. **저장**을 클릭하여 설정을 저장합니다.

13단계. (선택 사항) 구성된 ACL을 삭제하려면 **Delete ACL** 확인란을 선택하고 **Save**를 클릭합니다.