관리되는 스위치에서 MAC 기반 ACL(Access Control List) 및 ACE(Access Control Entry) 구성

목표

ACL(Access Control List)은 보안을 개선하는 데 사용되는 네트워크 트래픽 필터 및 상호 관련된 작업의 목록입니다.사용자가 특정 리소스에 액세스하는 것을 차단하거나 허용합니다.ACL에는 네트워크 디바이스에 대한 액세스가 허용되거나 거부된 호스트가 포함됩니다.MAC(Media Access Control) 기반 ACL(Access Control List)은 레이어 2 정보를 사용하여 트래픽에 대한 액세스를 허용하거나 거부하는 소스 MAC 주소 목록입니다.패킷이 무선 액세스 포인트에서 LAN(Local Area Network) 포트로 또는 그 반대로 오는 경우, 이 장치는 패킷의 소스 MAC 주소가 이 목록의 모든 항목과 일치하는지 확인하고 프레임의 내용에 대해 ACL 규칙을 확인합니다.그런 다음 일치하는 결과를 사용하여 이 패킷을 허용하거나 거부합니다.그러나 LAN에서 LAN 포트로의 패킷은 검사되지 않습니다.ACE(Access Control Entry)에는 실제 액세스 규칙 기준이 포함되어 있습니다.ACE가 생성되면 ACL에 적용됩니다.액세스 목록을 사용하여 네트워크에 액세스하기 위한 기본적인 수준의 보안을 제공해야 합니다.네트워크 디바이스에서 액세스 목록을 구성하지 않으면 스위치나 라우터를 통과하는 모든 패킷이 네트워크의 모든 부분으로 허용될 수 있습니다.

이 문서에서는 관리 스위치에 MAC 기반 ACL 및 ACE를 구성하는 방법에 대한 지침을 제공합니다.

적용 가능한 디바이스 | 소프트웨어 버전

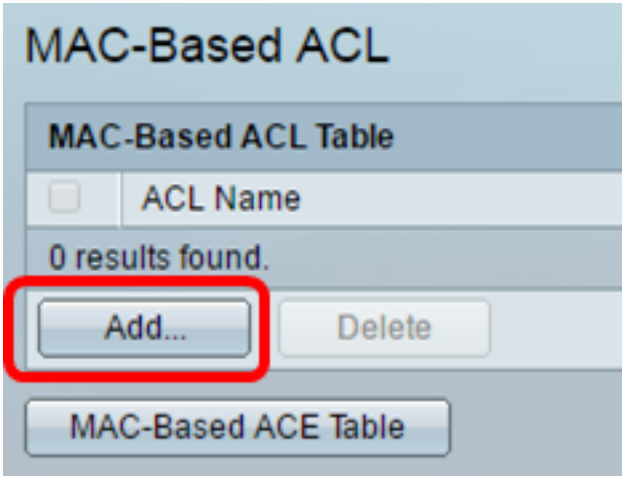
- SX350 시리즈 | 2.2.0.66(최신 다운로드)
- SG350X 시리즈 | 2.2.0.66(최신 다운로드)
- SX500 시리즈 | 1.4.5.02(최신 다운로드)
- SX550X 시리즈 | 2.2.0.66(최신 다운로드)

MAC 기반 ACL 및 ACE 구성

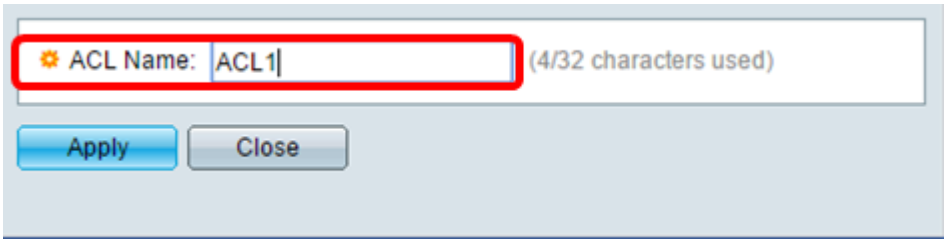
MAC 기반 ACL 구성

1단계. 웹 기반 유틸리티에 로그인한 다음 **Access Control(액세스 제어) > MAC-Based ACL로 이동합니다**.

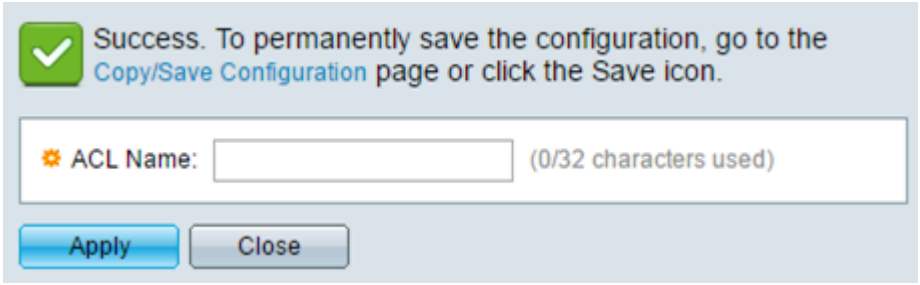
2단계. **Add** 버튼을 클릭합니다.



3단계. ACL 이름 필드에 새 ACL의 이름을 입력합니다.



4단계. **적용**을 클릭한 다음 **닫기**를 클릭합니다.



5단계. (선택 사항) **Save**를 클릭하여 시작 컨피그레이션 파일에 설정을 저장합니다.

이제 스위치에 MAC 기반 ACL을 구성해야 합니다.

MAC 기반 ACE 구성

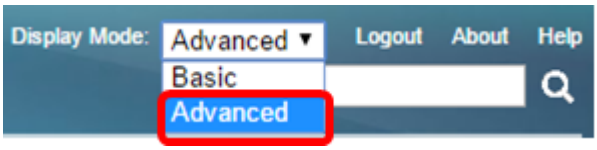
포트에서 프레임이 수신되면 스위치는 첫 번째 ACL을 통해 프레임을 처리합니다.프레임이 첫 번째 ACL의 ACE 필터와 일치하면 ACE 작업이 수행됩니다.프레임이 일치하는 ACE 필터가 없으면 다음 ACL이 처리됩니다.모든 관련 ACL의 ACE에 일치하는 항목이 없으면 기본적으로 프레임이 삭제됩니다.

이 시나리오에서는 특정 사용자 정의 소스 MAC 주소에서 모든 목적지 주소로 전송되는 트래픽을 거부하기 위해 ACE가 생성됩니다.

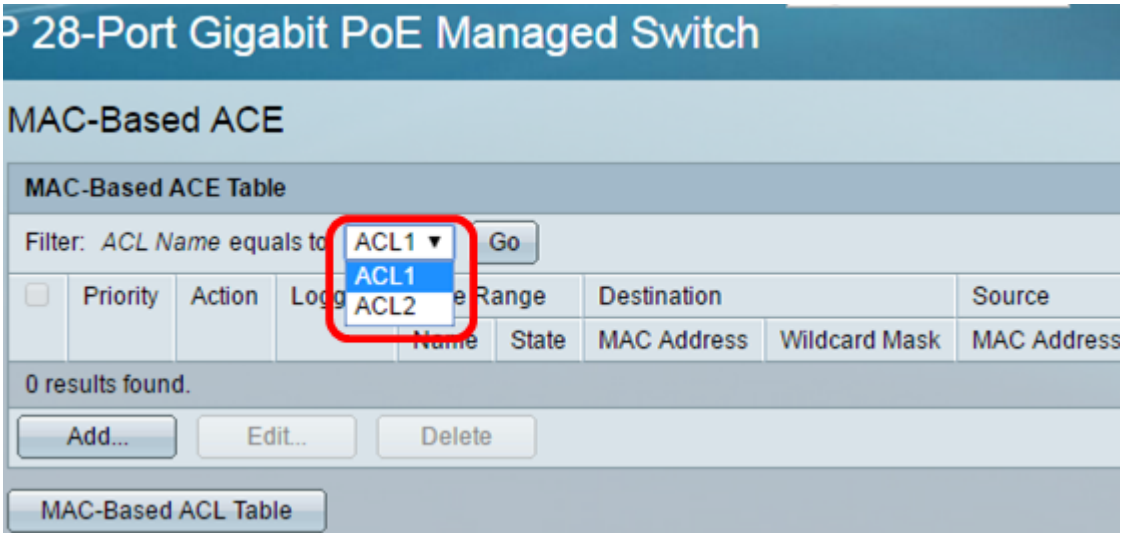
참고:이 기본 작업은 모든 트래픽을 허용하는 낮은 우선 순위 ACE를 생성하여 방지할 수 있습니다.

1단계. 웹 기반 유틸리티에서 **Access Control(액세스 제어) > MAC-Based ACE로 이동합니다**.

중요:스위치의 사용 가능한 기능 및 기능을 완전히 활용하려면 페이지 오른쪽 상단 모서리의 Display Mode 드롭다운 목록에서 **Advanced**를 선택하여 Advanced 모드로 변경합니다.



2단계. ACL Name(ACL 이름) 드롭다운 목록에서 ACL을 선택한 다음 **Go(이동)**를 클릭합니다.

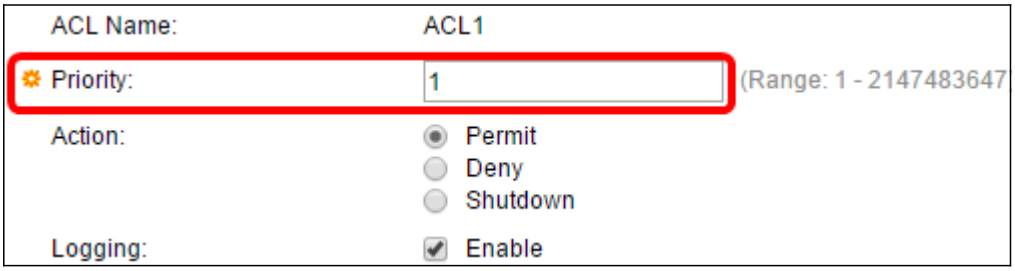


참고:ACL에 대해 이미 구성된 ACE가 테이블에 표시됩니다.

3단계. Add(**추가**) 버튼을 클릭하여 ACL에 새 규칙을 추가합니다.

참고:ACL *Name(ACL 이름)* 필드에는 ACL의 이름이 표시됩니다.

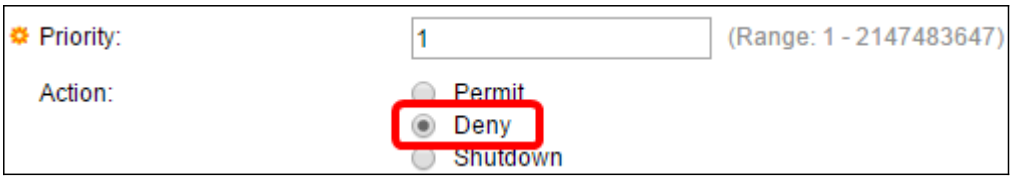
4단계. 우선순위 필드에 ACE의 우선순위 값을 *입력합니다*.우선 순위가 더 높은 ACE가 먼저 처리됩니다.값 1이 가장 높은 우선 순위입니다.



5단계. (선택 사항) Enable Logging 확인란을 선택하여 ACL 규칙과 일치하는 로깅 ACL 흐름을 활성화합니다.

6단계. 프레임이 ACE의 필수 기준을 충족할 때 필요한 작업에 해당하는 라디오 버튼을 클릭합니다.

참고:이 예에서는 Deny(거부)가 선택됩니다.



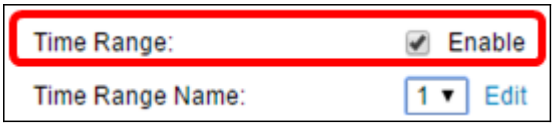
허용 — 스위치는 ACE의 필수 기준을 충족하는 패킷을 전달합니다.

거부 — 스위치가 ACE의 필수 기준을 충족하는 패킷을 삭제합니다.

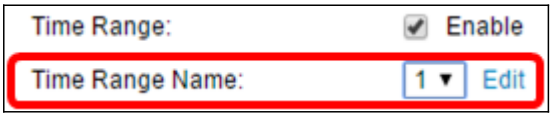
종료 — 스위치는 ACE의 필수 기준을 충족하지 않는 패킷을 삭제하고 패킷이 수신된 포트를 비활성화합니다.

참고:비활성화된 포트는 Port Settings 페이지에서 다시 활성화할 수 있습니다.

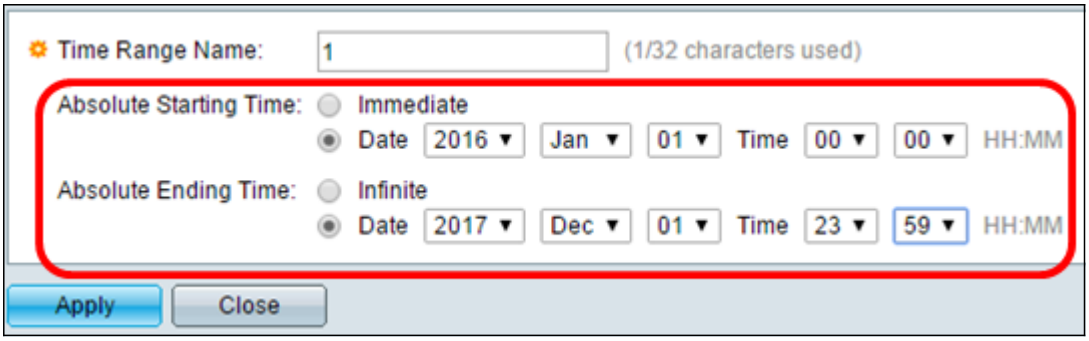
7단계. (선택 사항) Enable Time Range(시간 범위 활성화) 확인란을 선택하여 시간 범위를 ACE로 구성합니다.시간 범위는 ACE가 적용되는 시간을 제한하는 데 사용됩니다.



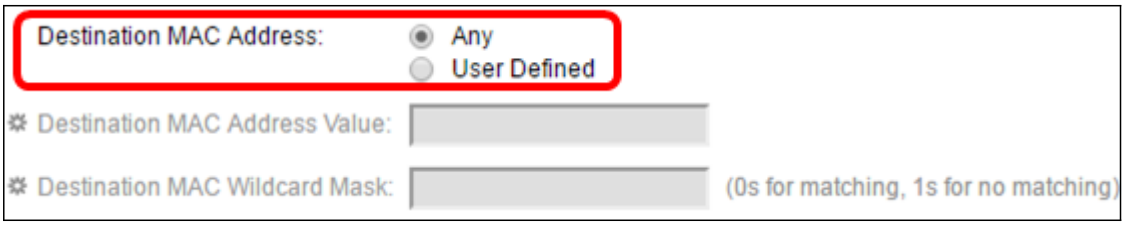
8단계. (선택 사항) Time Range Name 드롭다운 목록에서 ACE에 적용할 시간 범위를 선택합니다.



참고: Edit(**편집**)를 클릭하여 Time Range(시간 범위) 페이지로 이동하여 시간 범위를 생성할 수 있습니다.



9단계. Destination MAC Address 영역에서 ACE의 원하는 기준에 해당하는 라디오 버튼을 클릭합니다.



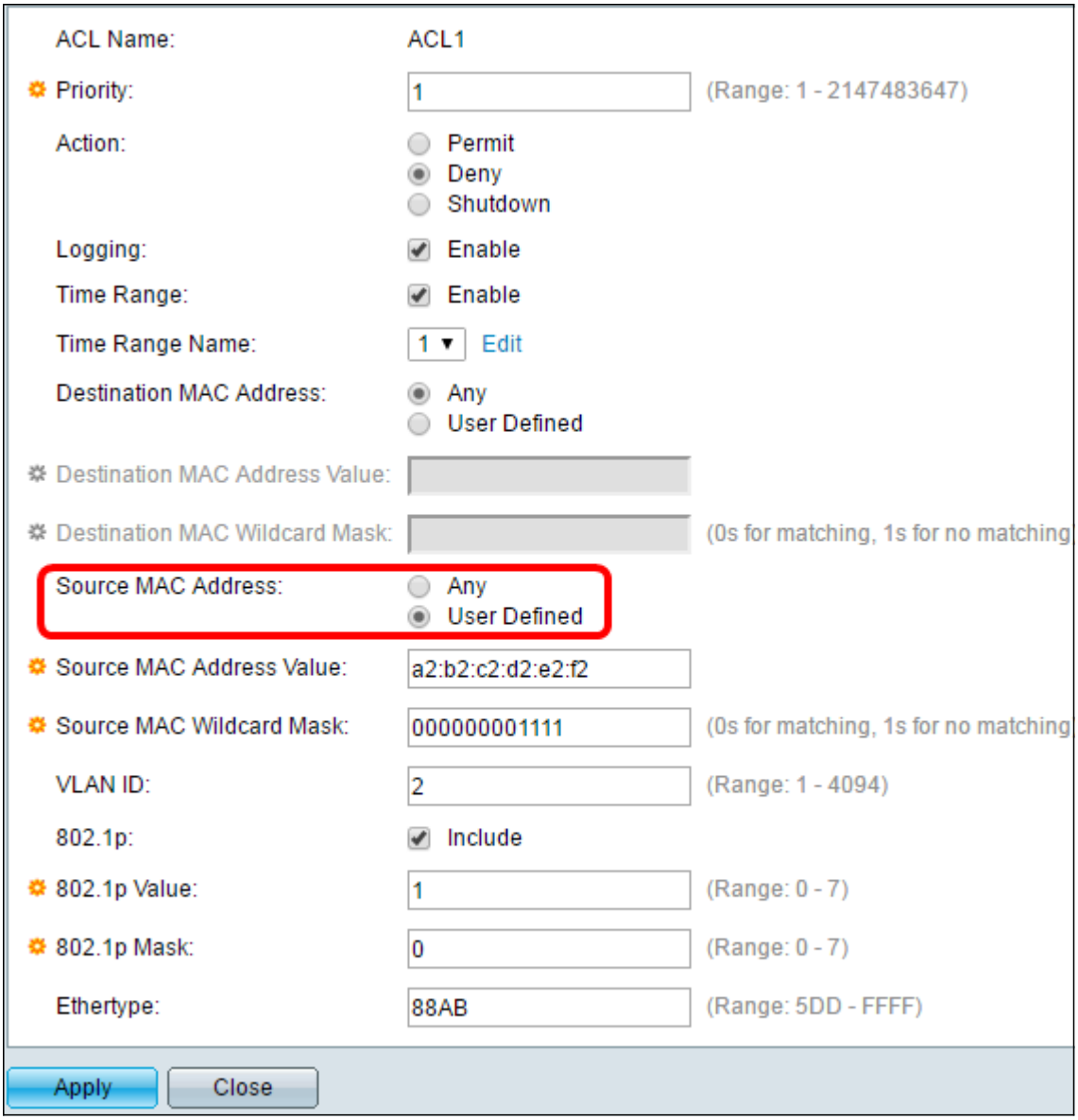
옵션은 다음과 같습니다.

Any — 모든 대상 MAC 주소가 ACE에 적용됩니다.

User Defined(사용자 정의) — Destination MAC Address Value(*대상 MAC 주소 값)* 및 Destination MAC Wildcard Mask(대상 MAC 와일드카드 마스크) 필드에서 ACE에 적용할 MAC 주소 및 MAC 와일드카드 마스크를 입력합니다.와일드카드 마스크는 MAC 주소 범위를 정의하는 데 사용됩니다.

참고:이 예에서는 Any가 선택됩니다.이 옵션을 선택하면 생성할 ACE가 ACE 트래픽을 거부합니다.

10단계. Source MAC Address(소스 MAC 주소) 영역에서 ACE의 원하는 기준에 해당하는 라디오 버튼을 클릭합니다.



옵션은 다음과 같습니다.

Any — 모든 소스 MAC 주소가 ACE에 적용됩니다.

User Defined(사용자 정의) — *Source MAC Address Value(*소스 MAC 주소 값) 및 *Source MAC Wildcard Mask(소스 MAC 와일드카드 마스크*) 필드에서 ACE에 적용할 MAC 주소 및 MAC 와일드카드 마스크를 입력합니다.와일드카드 마스크는 MAC 주소 범위를 정의하는 데 사용됩니다.

참고:이 예에서는 User Defined(사용자 정의)가 선택됩니다.

11단계(선택 사항) *VLAN ID* 필드에 프레임의 VLAN 태그와 일치시킬 VLAN ID를 입력합니다.

12단계. (선택 사항) ACE Criteria에 802.1p 값을 포함하려면 802.1p 확인란**에** 포함을 선택합니다.802.1p에는 CoS(Technology Class of Service)가 포함됩니다. CoS는 트래픽을 구별하는 데 사용되는 이더넷 프레임의 3비트 필드입니다.

13단계. 802.1p 값이 포함된 경우 다음 필드를 입력합니다.

802.1p 값 — 일치시킬 802.1p 값을 입력합니다.802.1p는 레이어 2 스위치에서 트래픽의 우선

순위를 지정하고 동적 멀티캐스트 필터링을 수행할 수 있는 기능을 제공하는 사양입니다.값은 다음과 같습니다.

- 0 - 배경대량 전송, 게임 등과 같이 우선순위가 가장 낮은 데이터.

- 1 — 최선의 노력일반적인 LAN 우선 순위에 따라 최선의 노력을 기울여야 하는 데이터.네트워크는 전달에 대한 어떠한 보증도 제공하지 않지만, 데이터는 트래픽을 기반으로 지정되지 않은 비트 전송률과 전송 시간을 얻습니다.

- 2 — 탁월한 노력.중요한 사용자를 위해 최선의 노력을 기울여야 하는 데이터.

- 3 - LVS(Linux Virtual Server) SIP(Phone Session Initiation Protocol)와 같은 중요한 애플리케이션

- 4 — 비디오레이턴시 및 지터가 100ms 미만입니다.

- 5 — 음성 Cisco IP Phone 기본값레이턴시 및 지터가 10ms 미만입니다.

- 6 — 네트워크 간 제어 LVS 전화 실시간 전송 프로토콜(RTP)

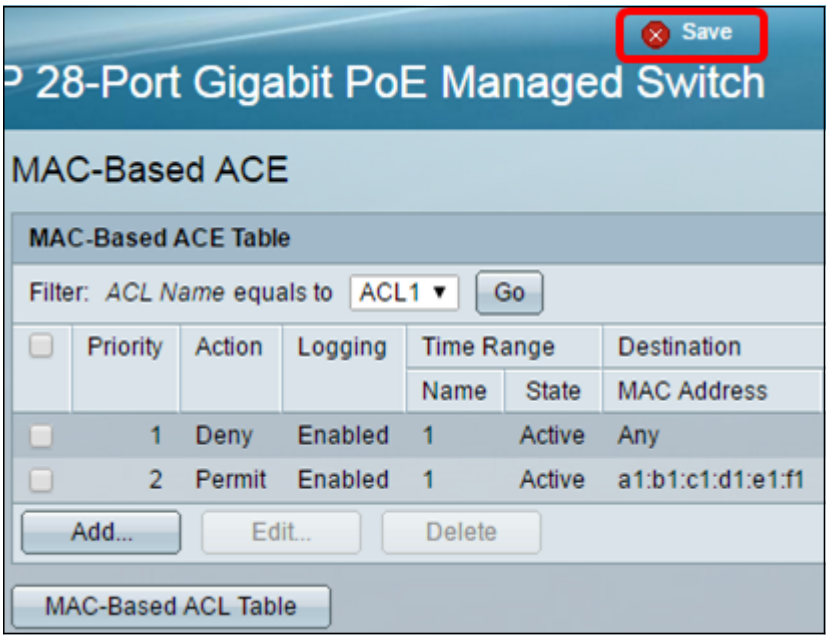
- 7 — 네트워크 제어.네트워크 인프라를 유지 관리하고 지원하기 위해 통과해야 하는 높은 요구 사항

802.1p Mask — 802.1p 값의 와일드카드 마스크를 입력합니다.이 와일드카드 마스크는 802.1p 값의 범위를 정의하는 데 사용됩니다.

14단계. (선택 사항) 매칭할 프레임의 Ethertype을 입력합니다.Ethertype은 프레임의 페이로드에 어떤 프로토콜을 사용하는지 나타내는 데 사용되는 이더넷 프레임의 28진수 필드입니다.

14단계. **적용**을 클릭한 다음 **닫기를 클릭합니다**.ACE가 생성되어 ACL 이름에 연결됩니다.

15단계. 설정을 시작 구성 파일에 저장하려면 저장을 누릅니다.



이제 스위치에 MAC 기반 ACE를 구성해야 합니다.

유용한 기타 링크:

- 350 Series 스위치 제품 페이지
- 350X Series 스위치 제품 페이지
- 550 Series 스위치 제품 페이지
- 550X Series 스위치 제품 페이지

이 문서와 관련된 비디오 보기...

여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.