스위치에서 IPv4 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.

IPv4 기반 ACL은 트래픽에 대한 액세스를 허용하거나 거부하기 위해 레이어 3 정보를 사용하는 소스 IPv4 주소의 목록입니다.IPv4 ACL은 구성된 IP 필터를 기반으로 IP 관련 트래픽을 제한합니다.필터에는 IP 패킷과 매칭하는 규칙이 포함되어 있으며, 패킷이 매칭할 경우, 규칙에서도 패킷을 허용할지 거부할지 여부를 지정합니다.

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 스위치에서 IPv4 기반 ACL 및 ACE를 구성하는 방법에 대한 지침을 제공합니다.

적용 가능한 디바이스

- SX350 시리즈
- SG350X 시리즈
- SX500 시리즈
- SX550X 시리즈

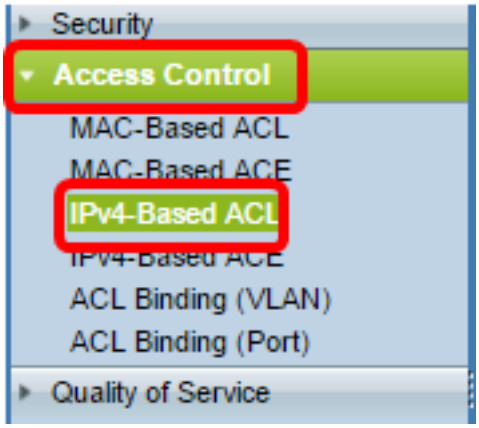
소프트웨어 버전

- 1.4.5.02 - SX500 시리즈
- 2.2.5.68 - SX350 Series, SG350X Series, SX550X Series

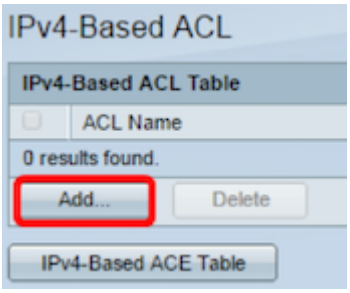
IPv4 기반 ACL 및 ACE 구성

IPv4 기반 ACL 구성

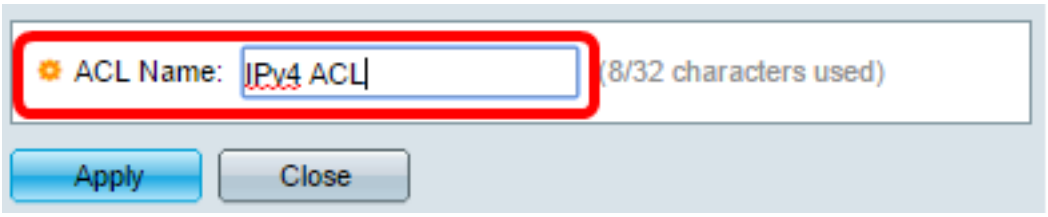
1단계. 웹 기반 유틸리티에 로그인한 다음 **Access Control(액세스 제어) > IPv4 기반 ACL로 이동합니다**.



2단계. **Add** 버튼을 클릭합니다.

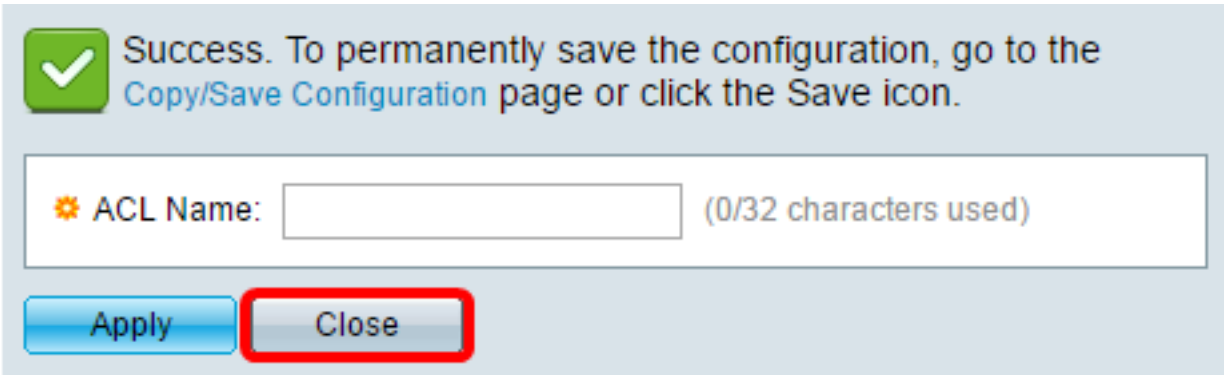


3단계. *ACL 이름* 필드에 새 ACL의 이름을 입력합니다.



참고:이 예에서는 IPv4 ACL이 사용됩니다.

4단계. **적용**을 클릭한 다음 **닫기**를 클릭합니다.



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

이제 스위치에서 IPv4 기반 ACL을 구성해야 합니다.

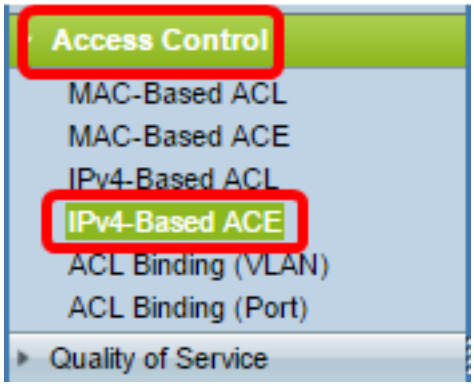
IPv4 기반 ACE 구성

포트에서 패킷이 수신되면 스위치는 첫 번째 ACL을 통해 패킷을 처리합니다.패킷이 첫 번째 ACL의 ACE 필터와 일치하면 ACE 작업이 수행됩니다.패킷이 ACE 필터와 일치하지 않으면 다음 ACL이 처리됩니다.모든 관련 ACL의 ACE에 일치하는 항목이 없으면 패킷이 기본적으로 삭제됩니다.

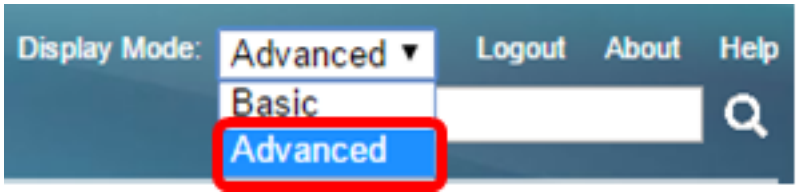
이 시나리오에서는 특정 사용자 정의 소스 IPv4 주소에서 모든 목적지 주소로 전송되는 트래픽을 거부하기 위해 ACE가 생성됩니다.

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

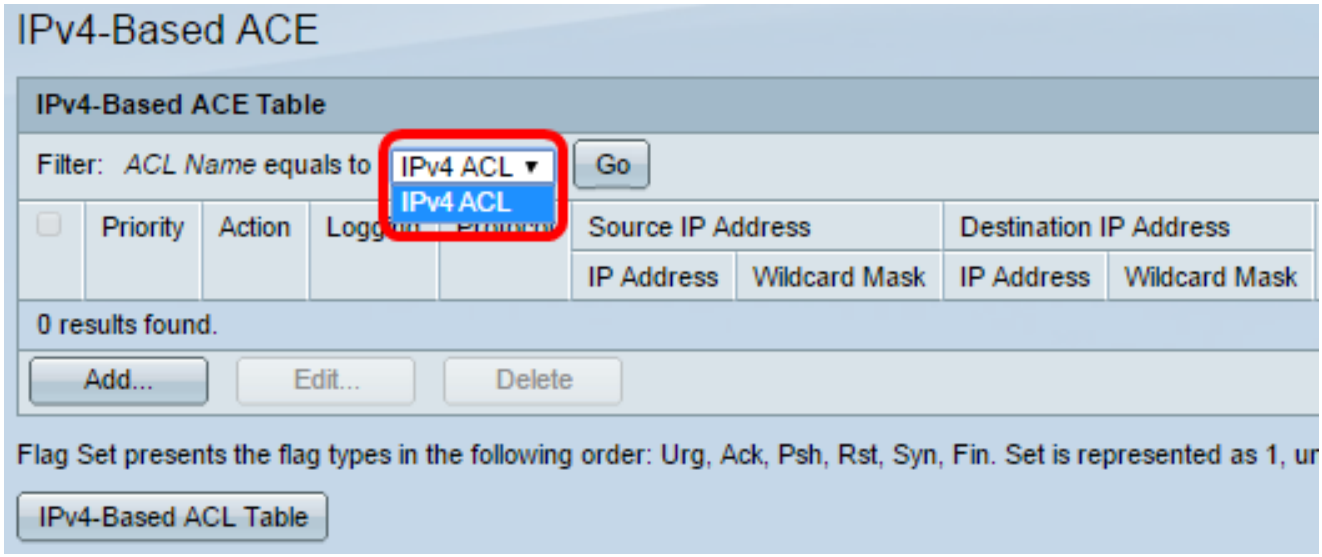
1단계. 웹 기반 유틸리티에서 Access Control(**액세스 제어) > IPv4-Based ACE로 이동합니다**.



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.

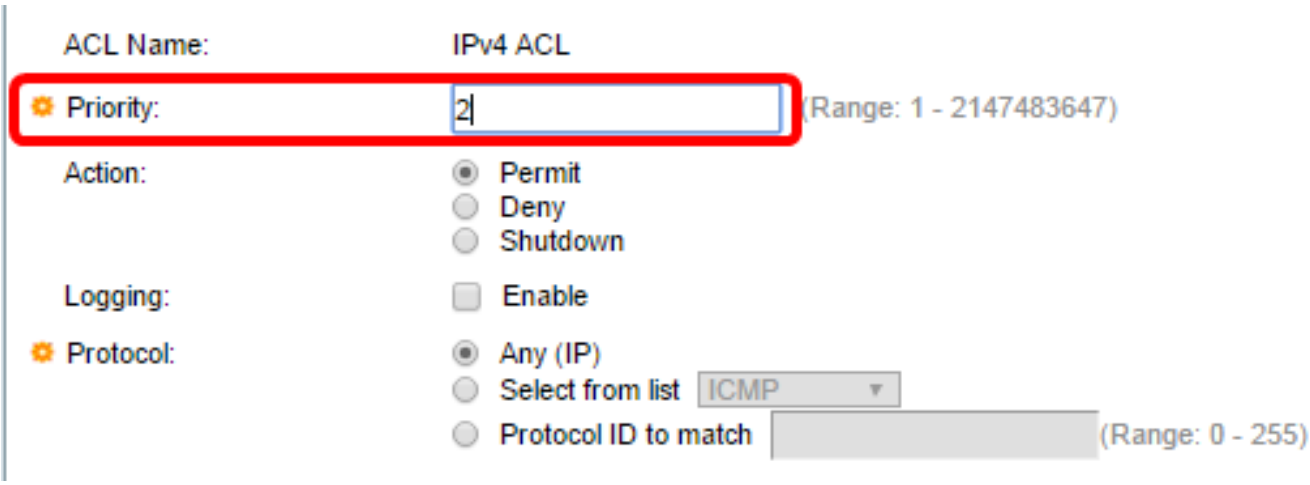


참고:ACL에 대해 이미 구성된 ACE가 테이블에 표시됩니다.

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.범위는 1~2147483647입니다.



참고:이 예에서는 2가 사용됩니다.

5단계. 프레임이 ACE의 필수 기준을 충족할 때 필요한 작업에 해당하는 라디오 버튼을 클릭합니다.

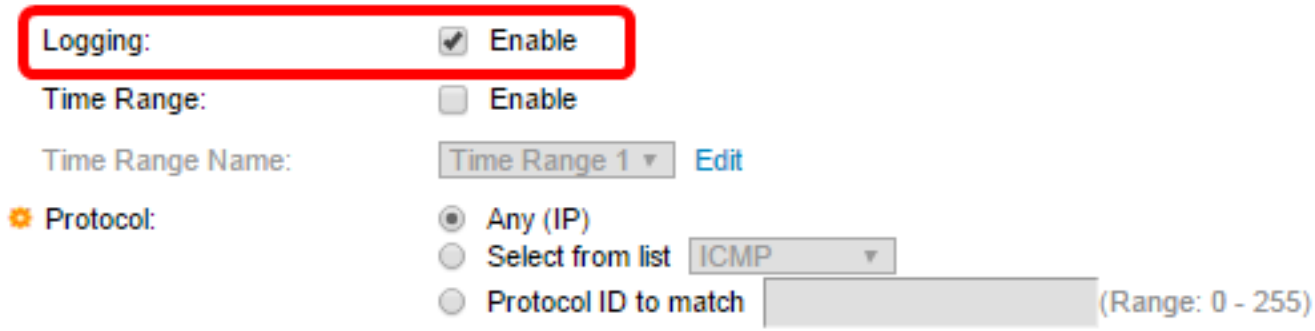
참고:이 예에서는 Permit(허용)이 선택됩니다.

- 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.

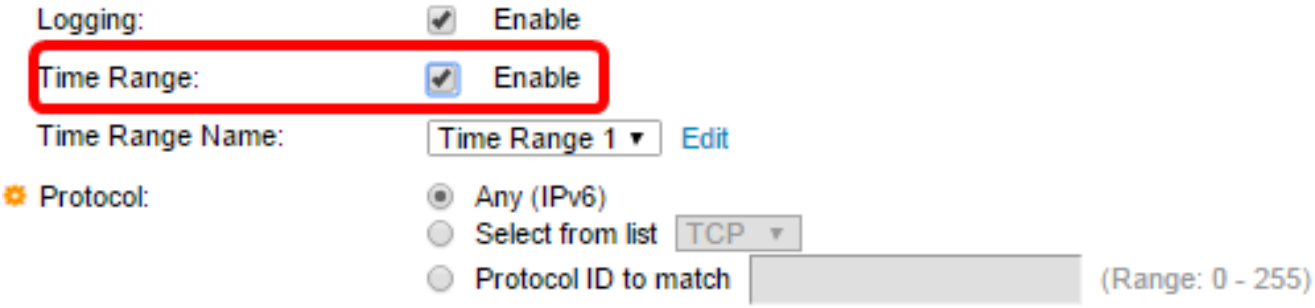
참고:비활성화된 포트는 Port Settings 페이지에서 다시 활성화할 수 있습니다.

6단계. (선택 사항) Enable Logging(로깅 **활성화**) 확인란을 선택하여 ACL 규칙과 일치하는

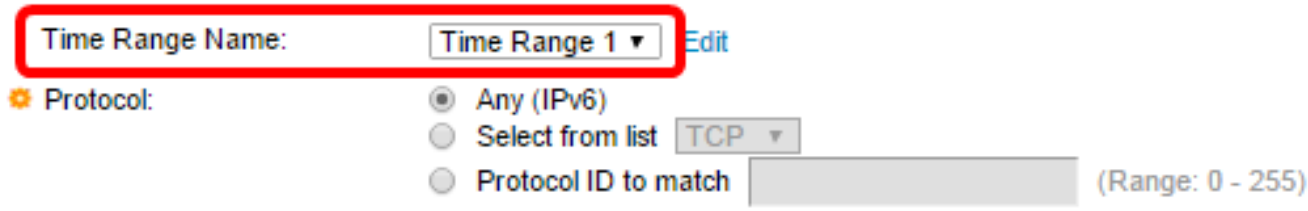
ACL 흐름의 로깅을 활성화합니다.



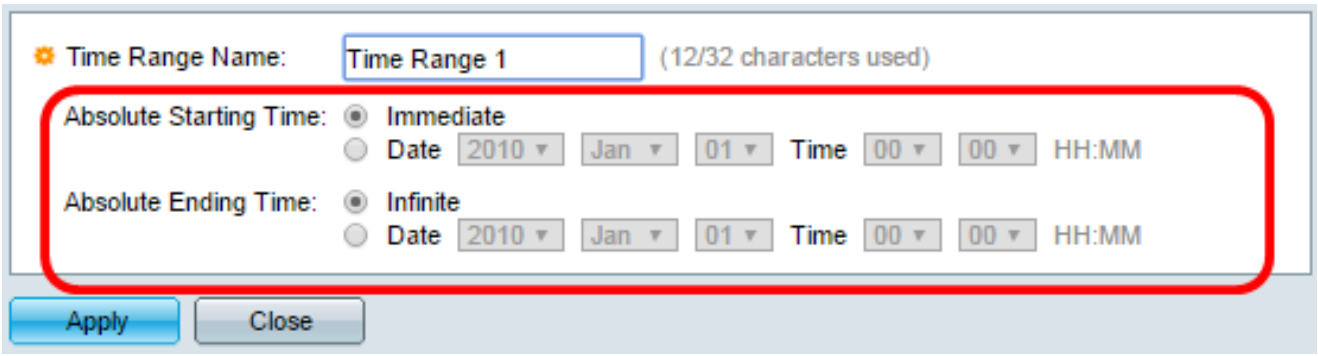
7단계. (선택 사항) Enable Time Range(시간 범위 활성화) 확인란을 선택하여 시간 범위를 ACE로 구성합니다.시간 범위는 ACE가 적용되는 시간을 제한하는 데 사용됩니다.



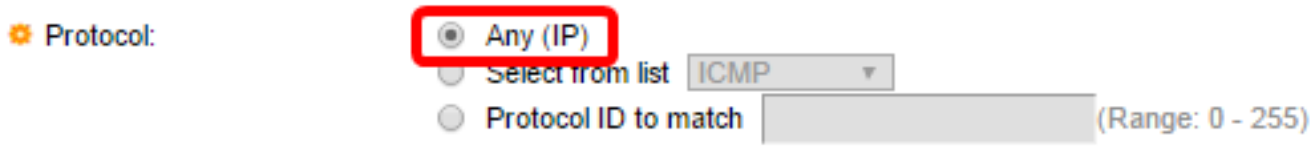
8단계. (선택 사항) Time Range Name 드롭다운 목록에서 ACE에 적용할 시간 범위를 선택합니다.



참고: Edit(**수정**)**를** 클릭하여 Time Range(시간 범위) 페이지에서 시간 범위를 탐색하고 생성할 수 있습니다.



9단계. Protocol(프로토콜) 영역에서 프로토콜 유형을 선택합니다.ACE는 특정 프로토콜 또는 프로토콜 ID를 기반으로 생성됩니다.

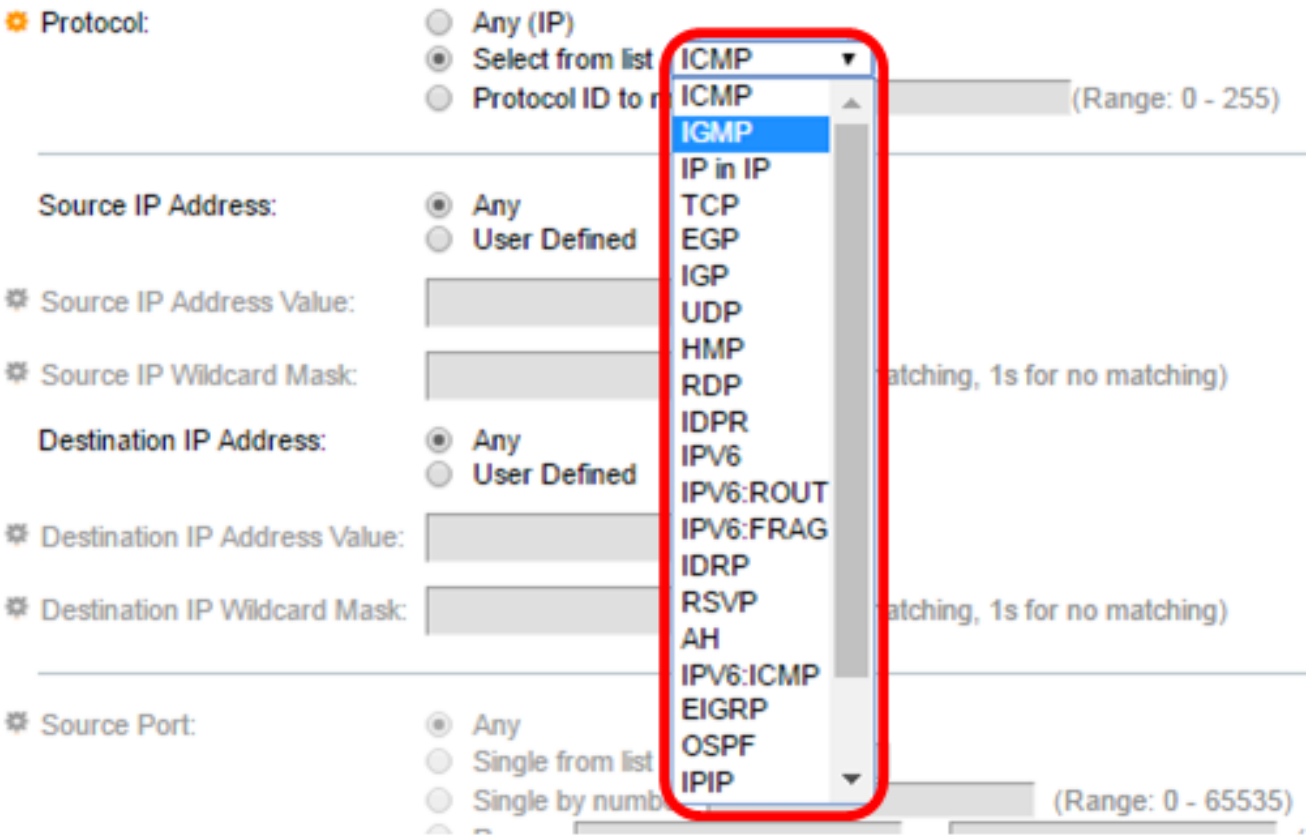


옵션은 다음과 같습니다.

- Any(IP) — 이 옵션은 모든 IP 프로토콜을 허용하도록 ACE를 구성합니다.
- 목록에서 선택 — 이 옵션을 사용하면 드롭다운 목록에서 프로토콜을 선택할 수 있습니다 .이 옵션을 원하는 경우 10단계로 건너뜁니다.
- 일치시킬 프로토콜 ID — 이 옵션을 사용하면 프로토콜 ID를 입력할 수 있습니다.이 옵션을 원하는 경우 11단계로 건너뜁니다.

참고:이 예에서는 Any(IP)가 선택됩니다.

10단계(선택 사항) 9단계의 목록에서 선택을 선택한 경우 드롭다운 목록에서 프로토콜을 선택합니다.

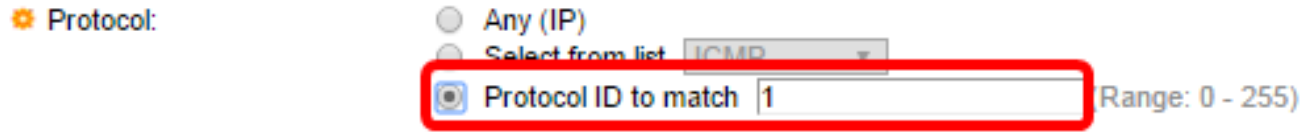


옵션은 다음과 같습니다.

- ICMP — 인터넷 제어 메시지 프로토콜
- IP in IP — IP 캡슐화의 IP
- TCP — 전송 제어 프로토콜
- EGP — 외부 게이트웨이 프로토콜
- IGP — 내부 게이트웨이 프로토콜
- UDP — 사용자 데이터그램 프로토콜
- HMP — 호스트 매핑 프로토콜
- RDP — 신뢰할 수 있는 데이터그램 프로토콜
- IDPR — 도메인 간 정책 라우팅
- IPV6 — IPv4 터널링을 통한 IPv6
- IPv6:RNSG — 게이트웨이를 통해 IPv4 경로를 통해 IPv6에 속하는 패킷을 확인합니다.
- IPV6:FRAG — IPv4 프래그먼트 헤더를 통해 IPv6에 속하는 패킷을 확인합니다.
- IDRP — IS-IS 도메인 간 라우팅 프로토콜
- RSVP — ReSerVation 프로토콜

- AH — 인증 헤더
- IPV6:ICMP — IPv6용 ICMP
- EIGRP — 향상된 내부 게이트웨이 라우팅 프로토콜
- OSPF — Open Shortest Path First
- IPIP — IP의 IP
- PIM — 프로토콜 독립 멀티캐스트
- L2TP — 레이어 2 터널링 프로토콜

11단계(선택 사항) 9단계에서 Protocol ID(프로토콜 ID)를 선택하여 일치시킨 경우 *Protocol ID* to match 필드에 프로토콜 ID를 입력합니다.



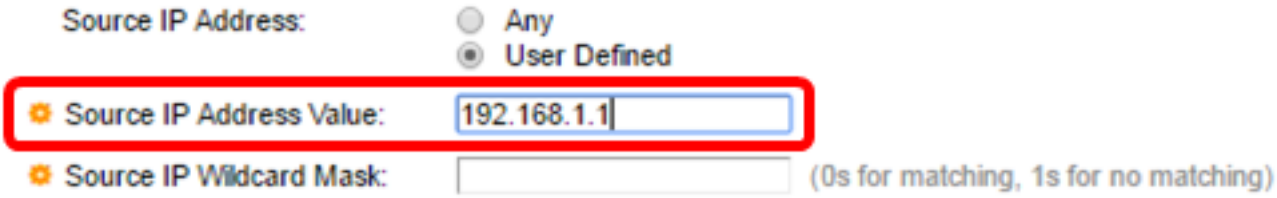
12단계. Source IP Address(소스 IP 주소) 영역에서 ACE의 원하는 기준에 해당하는 라디오 버튼을 클릭합니다.

옵션은 다음과 같습니다.

- Any — 모든 소스 IPv4 주소가 ACE에 적용됩니다.
- User Defined(사용자 정의) — Source IP Address Value(소스 *IP 주소 값*) 및 Source IP Wildcard Mask(소스 *IP 와일드카드 마스크*) 필드에서 ACE에 적용할 IP 주소 및 IP 와일드카드 마스크를 입력합니다.와일드카드 마스크는 IP 주소 범위를 정의하는 데 사용됩니다.

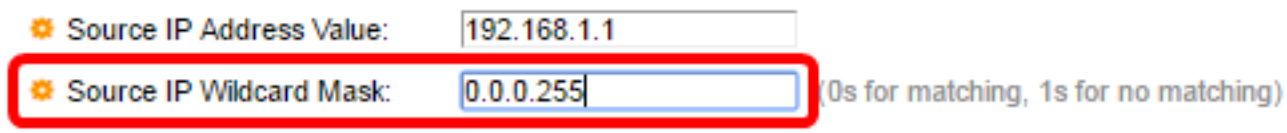
참고:이 예에서는 User Defined(사용자 정의)가 선택됩니다.Any(모두)를 선택한 경우 15단계로 건너뜁니다.

13단계. 소스 IP 주소 값 필드에 소스 IP 주소를 입력합니다.



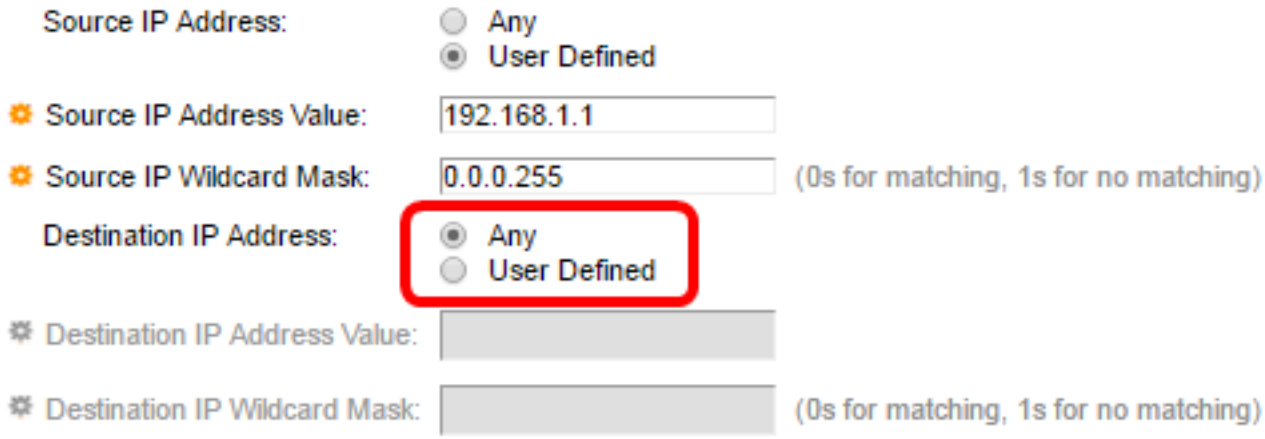
참고:이 예에서는 192.168.1.1이 사용됩니다.

14단계. Source *IP Wildcard Mask* 필드에 소스 와일드카드 마스크를 입력합니다.



참고:이 예에서는 0.0.0.255이 사용됩니다.

15단계. Destination IP Address 영역에서 ACE의 원하는 기준에 해당하는 라디오 버튼을 클릭합니다.

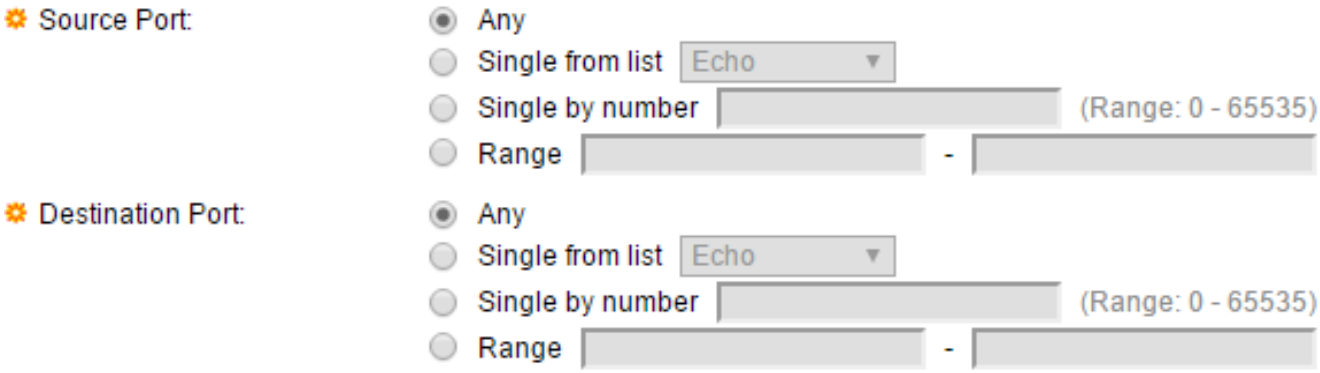


옵션은 다음과 같습니다.

- Any — 모든 대상 IPv4 주소가 ACE에 적용됩니다.
- User Defined(사용자 정의) — Destination IP Address Value(*대상 IP 주소 값*) 및 Destination IP Wildcard Mask(대상 IP *와일드카드 마스크*) 필드에서 ACE에 적용할 IP 주소 및 IP 와일드카드 마스크를 입력합니다.와일드카드 마스크는 IP 주소 범위를 정의하는 데 사용됩니다.

참고:이 예에서는 Any가 선택됩니다.이 옵션을 선택하면 생성할 ACE가 지정된 IPv4 주소에서 모든 목적지로 들어오는 ACE 트래픽을 허용합니다.

16단계(선택 사항) Source Port(소스 포트) 영역에서 라디오 버튼을 클릭합니다.기본값은 Any입니다.



- Any — 모든 소스 포트에 일치시킵니다.
- 단일 시작 목록 — 패킷이 매칭되는 단일 TCP/UDP 소스 포트를 선택할 수 있습니다.이 필드는 목록에서 선택 드롭다운 메뉴에서 800/6-TCP 또는 800/17-UDP를 선택한 경우에만 활성화됩니다.
- Single by number — 패킷이 매칭되는 단일 TCP/UDP 소스 포트를 선택할 수 있습니다.이 필드는 목록에서 선택 드롭다운 메뉴에서 800/6-TCP 또는 800/17-UDP를 선택한 경우에만 활성화됩니다.
- 범위 — 패킷이 일치하는 TCP/UDP 소스 포트의 범위를 선택할 수 있습니다.구성할 수 있는 포트 범위는 8가지가 있습니다(소스 포트와 대상 포트 간에 공유).TCP 및 UDP 프로토콜은 각각 8개의 포트 범위를 가집니다.

17단계(선택 사항) Destination Port(대상 포트) 영역에서 라디오 버튼을 클릭합니다.기본값은 Any입니다.

- Any — 모든 소스 포트에 일치

- 단일 시작 목록 — 패킷이 매칭되는 단일 TCP/UDP 소스 포트를 선택할 수 있습니다.이 필드는 목록에서 선택 드롭다운 메뉴에서 800/6-TCP 또는 800/17-UDP를 선택한 경우에만 활성화됩니다.
- Single by number — 패킷이 매칭되는 단일 TCP/UDP 소스 포트를 선택할 수 있습니다.이 필드는 목록에서 선택 드롭다운 메뉴에서 800/6-TCP 또는 800/17-UDP를 선택한 경우에만 활성화됩니다.
- 범위 — 패킷이 일치하는 TCP/UDP 소스 포트의 범위를 선택할 수 있습니다.구성할 수 있는 포트 범위는 8가지가 있습니다(소스 포트와 대상 포트 간에 공유).TCP 및 UDP 프로토콜은 각각 8개의 포트 범위를 가집니다.

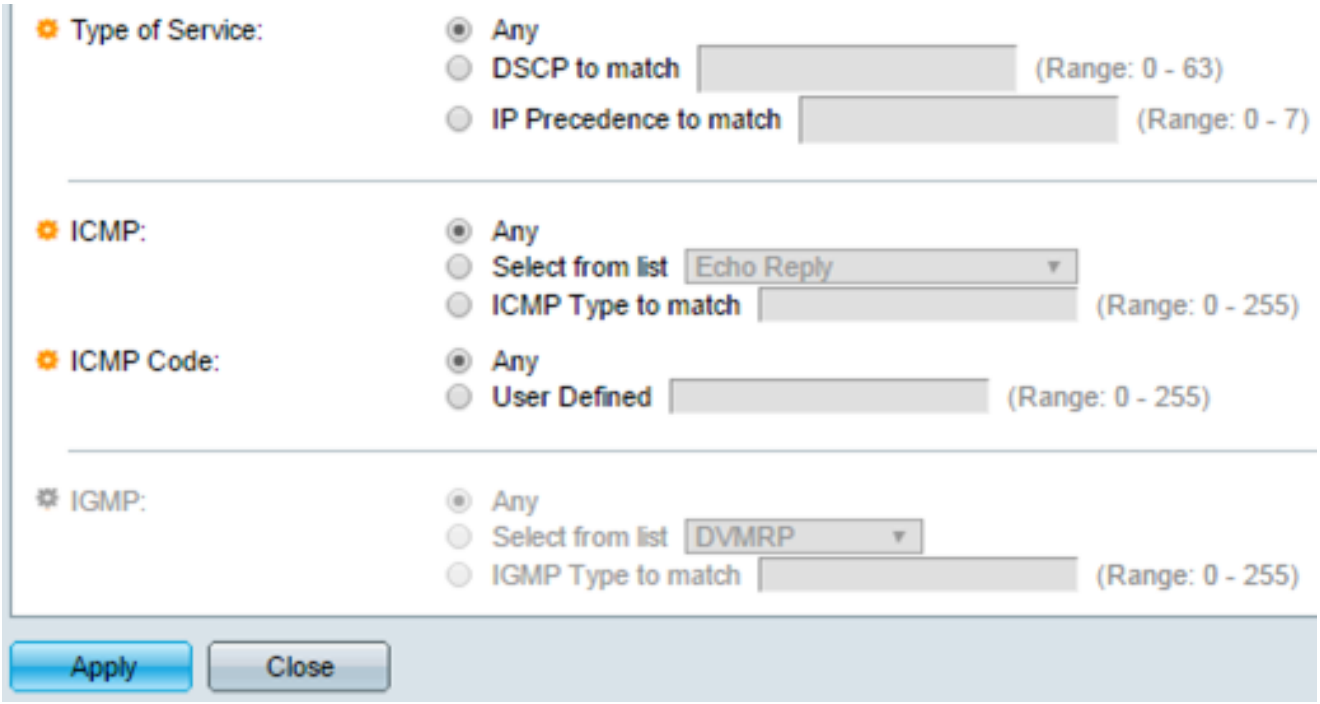
18단계. (선택 사항) TCP Flags(TCP 플래그) 영역에서 패킷을 필터링할 하나 이상의 TCP 플래그를 선택합니다.필터링된 패킷은 전달 또는 삭제됩니다.TCP 플래그로 패킷을 필터링하면 패킷 제어가 증가하여 네트워크 보안이 향상됩니다.

- 설정 — 플래그가 설정된 경우 일치시킵니다.
- Unset — 플래그가 설정되지 않은 경우 일치시킵니다.
- Don't care — TCP 플래그를 무시합니다.

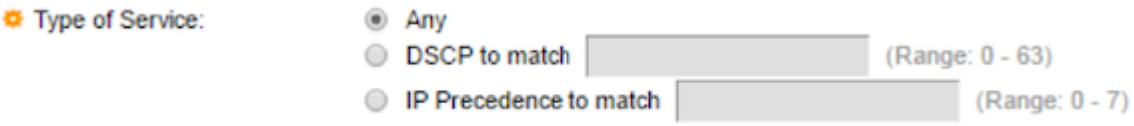
TCP 플래그는 다음과 같습니다.

- Urg — 이 플래그는 수신 데이터를 Urgent로 식별하는 데 사용됩니다.
- ACK — 이 플래그는 패킷의 성공적인 수신을 확인하는 데 사용됩니다.
- Psh — 이 플래그는 데이터가 우선 순위(해당 사항)를 받고 전송 또는 수신 끝에서 처리되도록 하는 데 사용됩니다.
- Rst — 이 플래그는 현재 연결에 사용되지 않는 세그먼트가 도착하면 사용됩니다.
- Syn — 이 플래그는 TCP 통신에 사용됩니다.
- Fin — 이 플래그는 통신 또는 데이터 전송이 완료될 때 사용됩니다.

19단계(선택 사항) Type of Service(서비스 유형) 영역에서 IP 패킷의 서비스 유형을 클릭합니다.



옵션은 다음과 같습니다.



- Any — 트래픽 정체를 위한 모든 유형의 서비스가 될 수 있습니다.
- DSCP to Match — DSCP는 네트워크 트래픽을 분류하고 관리하는 메커니즘입니다.6비트(0-63)는 각 노드에서 패킷 경험의 홉별 동작을 선택하는 데 사용됩니다.
- 일치할 IP 우선 순위 — IP 우선 순위는 네트워크에서 적절한 QoS(Quality of Service) 약속을 제공하기 위해 사용하는 TOS(Type of Service) 모델입니다.이 모델은 RFC 791 및 RFC 1349에 설명된 대로 IP 헤더에서 서비스 유형 바이트의 가장 중요한 세 비트를 사용합니다.IP Preference 값이 있는 키워드는 다음과 같습니다.

  - 0 - 루틴용
  - 1 - 우선 순위
  - 2 - 즉시
  - 3 - 플래시의 경우
  - 4 - 플래시 재정의용
  - 5 - 중요
  - 6 - 인터넷용
  - 7 - 네트워크용

20단계. (선택 사항) ACL의 IP 프로토콜이 ICMP인 경우 필터링에 사용되는 ICMP 메시지 유형을 클릭합니다.이름으로 메시지 유형을 선택하거나 메시지 유형 번호를 입력합니다.

- Any — 모든 메시지 유형이 수락됩니다.

- 목록에서 선택 — 이름별로 메시지 유형을 선택할 수 있습니다.
- 일치시킬 ICMP 유형 — 필터링 목적으로 사용할 메시지 유형 수입니다.범위는 0~255입니다.

21단계. (선택 사항) ICMP 메시지에는 메시지 처리 방법을 나타내는 코드 필드가 있을 수 있습니다.다음 옵션 중 하나를 클릭하여 이 코드를 필터링할지 여부를 구성합니다.

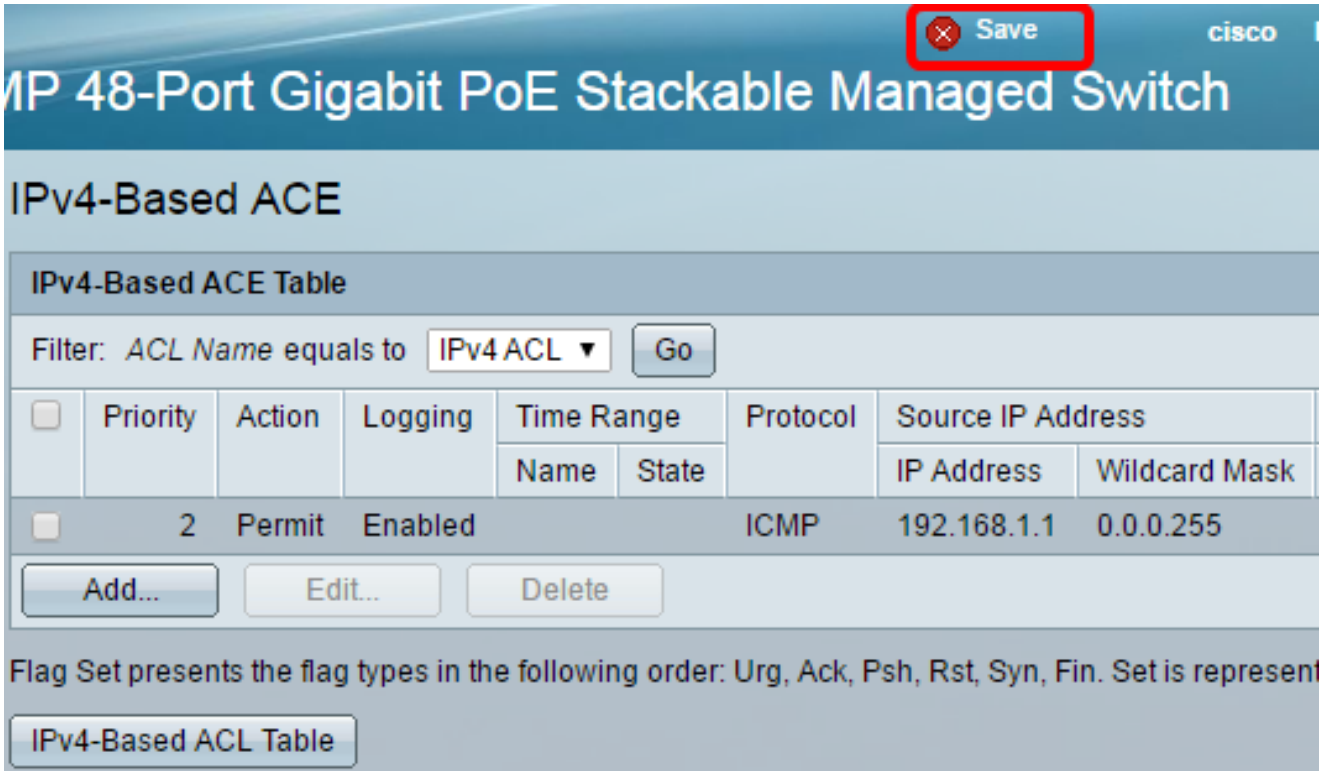
- 모두 — 모든 코드를 적용합니다.
- User Defined(사용자 정의) — 필터링 목적으로 ICMP 코드를 입력할 수 있습니다.범위는 0~255입니다.

22단계. (선택 사항) ACL이 IGMP를 기반으로 하는 경우 필터링에 사용할 IGMP 메시지 유형을 클릭합니다.이름으로 메시지 유형을 선택하거나 메시지 유형 번호를 입력합니다.

- Any — 모든 메시지 유형이 수락됩니다.
- 목록에서 선택 — 드롭다운 목록에서 옵션을 선택할 수 있습니다.
- DVMRP — 리버스 경로 플러딩 기술을 사용하여 패킷이 도착한 것을 제외한 각 인터페이스를 통해 수신된 패킷의 사본을 전송합니다.
- Host-Query — 정보를 위해 연결된 각 네트워크에서 일반 호스트 쿼리 메시지를 주기적으로 전송합니다.
- Host-Reply — 쿼리에 응답합니다.
- PIM — PIM(Protocol Independent Multicast)은 멀티캐스트 서버에서 여러 멀티캐스트 클라이언트로 멀티캐스트 트래픽을 전달하기 위해 로컬 및 원격 멀티캐스트 라우터 간에 사용됩니다.
- 추적 — IGMP 멀티캐스트 그룹 가입 및 탈퇴에 대한 정보를 제공합니다.
- IGMP Type to match — 필터링에 사용할 메시지 유형 수입니다.범위는 0~255입니다.

23단계. Apply(적용)를 **클릭한** 다음 **Close(닫기)**를 클릭합니다.ACE가 생성되어 ACL 이름에 연결됩니다.

24단계. 설정을 시작 구성 파일에 저장하려면 저장을 누릅니다.



이제 스위치에 IPv4 기반 ACE를 구성해야 합니다.