Cisco Business 220 스위치의 포트 보안

목표

이 문서에서는 Cisco Business 220 시리즈 스위치의 포트 보안 옵션에 대해 설명합니다.

적용 가능한 디바이스 | 펌웨어 버전

- CBS220 시리즈(DataSheet) | 2.0.0.17

소개

특정 MAC 주소를 가진 사용자에게 포트 액세스를 제한하여 네트워크 보안을 강화할 수 있습니다.MAC 주소는 동적으로 학습하거나 정적으로 구성할 수 있습니다.포트 보안은 수신 및 학습된 패킷을 모니터링합니다.잠긴 포트에 대한 액세스는 특정 MAC 주소를 가진 사용자로 제한됩니다.

802.1X가 활성화된 포트 또는 SPAN 대상으로 정의된 포트에서 포트 보안을 활성화할 수 없습니다.

포트 보안에는 두 가지 모드가 있습니다.

- **Classic Lock** - 포트에서 학습된 모든 MAC 주소가 잠기며 포트에서 새 MAC 주소를 인식하지 못합니다.학습된 주소는 에이징 또는 재학습의 대상이 아닙니다.
- **Limited Dynamic Lock(제한된 동적 잠금)** - 디바이스에서 허용되는 주소의 구성된 제한까지 MAC 주소를 학습합니다.제한에 도달하면 디바이스에서 추가 주소를 학습하지 않습니다.이 모드에서는 주소가 에이징 및 재학습이 적용됩니다.

새 MAC 주소의 프레임이 인증되지 않은 포트에서 탐지되면(포트가 완전히 잠겨 있고 새 MAC 주소가 있거나 포트가 동적으로 잠기며 허용되는 최대 주소 수를 초과함) 보호 메커니즘이 호출되며 다음 작업 중 하나가 발생할 수 있습니다.

- 프레임이 삭제됩니다.
- 프레임이 전달됩니다.
- 프레임이 삭제되고 SYSLOG 메시지가 생성됩니다.
- 포트가 종료되었습니다.

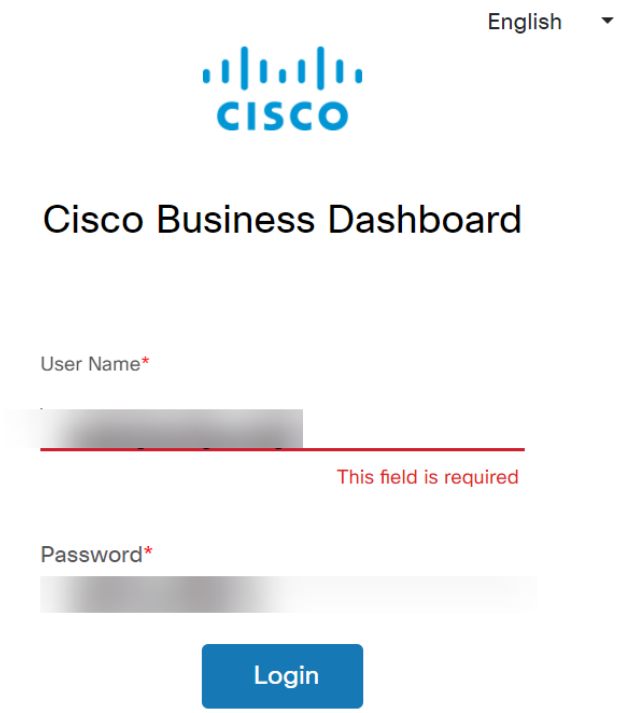
다른 포트에서 보안 MAC 주소가 확인되면 프레임이 전달되지만 MAC 주소는 해당 포트에서 학습되지 않습니다.

이러한 작업 중 하나 외에도 트랩을 생성하고 디바이스 오버로드를 방지하기 위해 빈도 및 수를 제한할 수 있습니다.

포트 보안 구성

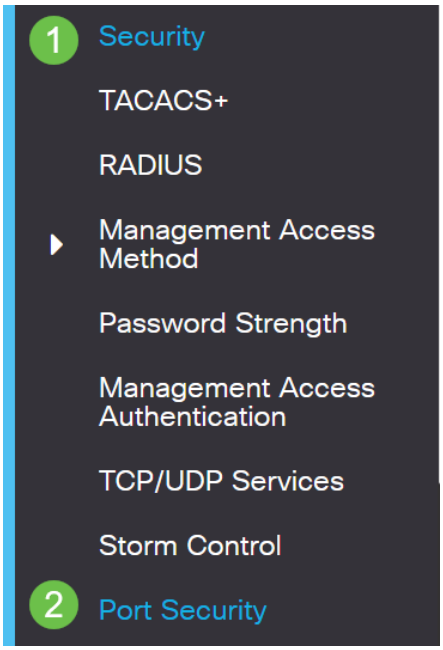
1단계

웹 사용자 인터페이스(UI)에 로그인합니다.



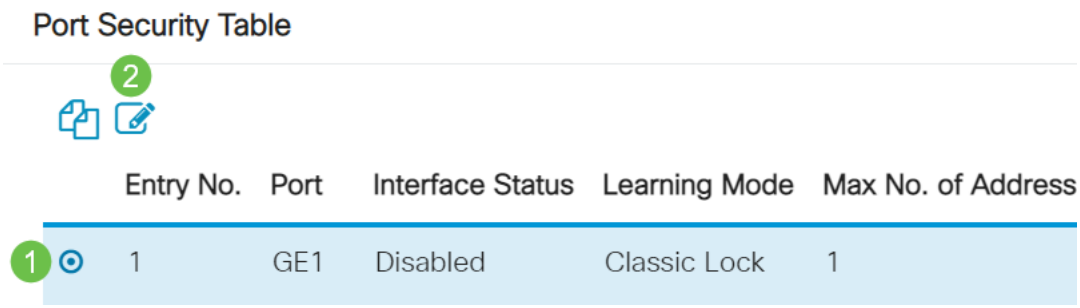
2단계

왼쪽의 메뉴에서 Security(보안) **> Port Security(포트 보안)를** 선택합니다.



3단계

수정할 인터페이스를 선택한 다음 **수정 아이콘**을 클릭합니다.

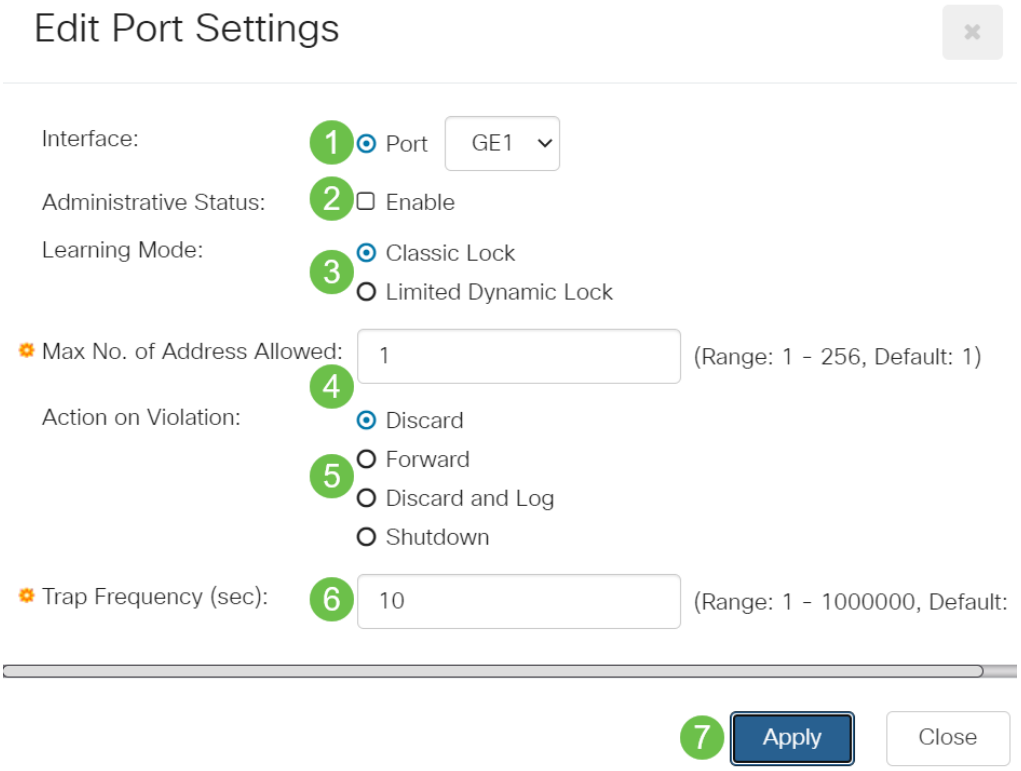


4단계

매개변수를 입력합니다.

- **Interface**(인터페이스) - 인터페이스 이름을 선택합니다.
- **Administrative Status**(관리 상태) - 포트를 잠그려면 선택합니다.
- **Learning Mode(학습 모드)** - 포트 잠금 유형을 선택합니다.이 필드를 구성하려면 인터페이스 상태를 잠금 해제해야 합니다.Learning Mode 필드는 Interface Status 필드가 잠긴 경우에만 활성화됩니다.학습 모드를 변경하려면 잠금 인터페이스를 지워야 합니다.모드가 변경되면 인터페이스 잠금(Lock Interface)을 복원할 수 있습니다.옵션은 다음과 같습니다.
  - **Classic Lock**(기존 잠금) - 이미 학습한 주소 수에 관계없이 포트를 즉시 잠급니다.
  - **Limited Dynamic Lock(제한된 동적 잠금)** - 포트와 연결된 현재 동적 MAC 주소를 삭제하여 포트를 잠급니다.포트는 포트에서 허용되는 최대 주소를 학습합니다.MAC 주소의 재학습과 에이징이 모두 활성화됩니다.
- **Max No. of Addresses Allowed(허용되는 최대 주소 수)** - Limited Dynamic Lock 학습 모드를 선택한 경우 포트에서 학습할 수 있는 최대 MAC 주소 수를 입력합니다.숫자 0은 인터페이스에서 고정 주소만 지원됨을 나타냅니다.
- **Action on Violation(위반**에 대한 작업) - 잠긴 포트에 도착하는 패킷에 적용할 작업을 선택합니다.옵션은 다음과 같습니다.
  - **Discard**(폐기) - 확인되지 않은 소스에서 패킷을 삭제합니다. ·
  - **Forward**(전달) - MAC 주소를 배우지 않고 알 수 없는 소스에서 패킷을 전달합니다.
  - **Discard and Log(삭제 및 로그)** - 학습되지 않은 소스의 패킷을 삭제하고, 인터페이스를 종료하고, 이벤트를 로깅하며, 트랩을 지정된 트랩 수신자에 Shutdown(종료) - 알려지지 않은 소스의 패킷을 삭제하고 포트를 종료합니다.포트가 다시 활성화될 때까지 또는 디바이스가 재부팅될 때까지 종료되지 않습니다.
  - **Trap Frequency(트랩 빈도)** - 트랩 간에 경과하는 최소 시간(초)을 입력합니다.

Apply를 **클릭합니다**.



CBS220에서 포트 보안에 대한 기본 동작의 예를 보려면 포트 보안 동작을 확인하십시오.

결론

그것은 그렇게 간단합니다.안전한 네트워크를 즐겨보세요!

자세한 컨피그레이션은 Cisco Business 220 Series 스위치 관리 가이드를 참조하십시오 .

다른 문서를 보려면 Cisco Business 220 Series 스위치 지원 페이지를 확인하십시오.