Cisco Catalyst Layer 3 Fixed Configuration Switch의 레이어 2 보안 기능 컨피그레이션 예

목차

소개

이 문서에서는 Cisco Catalyst Layer 3 고정 컨피그레이션 스위치에서 구현할 수 있는 포트 보안, DHCP 스누핑, ARP(Dynamic Address Resolution Protocol) 검사 및 IP 소스 가드 같은 일부 레이어 2 보안 기능에 대한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 버전 12.2(25)SEC2가 포함된 Cisco Catalyst 3750 Series 스위치를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 다음 하드웨어 제품에서도 사용할 수 있습니다.

- Cisco Catalyst 3550 Series 스위치
- Cisco Catalyst 3560 Series 스위치
- Cisco Catalyst 3560-E Series 스위치
- Cisco Catalyst 3750-E Series 스위치

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

라우터와 유사하게, 레이어 2 및 레이어 3 스위치에는 각각 고유한 네트워크 보안 요구 사항이 있습니다.스위치는 라우터와 동일한 레이어 3 공격에 취약합니다.그러나 일반적으로 OSI 참조 모델의 스위치와 레이어 2는 서로 다른 방식으로 네트워크 공격을 받습니다.여기에는 다음이 포함됩니다.

- **CAM(Content Addressable Memory) 테이블 오버플로**CAM(Content Addressable Memory) 테이블의 크기는 제한되어 있습니다.다른 엔트리가 만료되기 전에 CAM 테이블에 충분한 엔트리를 입력하면 CAM 테이블이 채워져 새 엔트리를 수락할 수 없습니다.일반적으로 네트워크 침입자가 CAM 테이블이 가득 찰 때까지 유효하지 않은 소스 MAC(Media Access Control) 주소가 많은 스위치를 플러딩합니다.이 경우 CAM 테이블에서 특정 MAC 주소에 대한 포트 번호를 찾을 수 없기 때문에 스위치가 수신 트래픽이 있는 모든 포트를 플러딩합니다.스위치는 본질적으로 허브 역할을 합니다.침입자가 유효하지 않은 소스 MAC 주소의 플러드를 유지하지 않으면 스위치는 CAM 테이블에서 오래된 MAC 주소 항목을 시간 초과하고 다시 스위치 역할을 시작합니다.CAM 테이블 오버플로는 로컬 VLAN 내의 트래픽만 플러딩하므로 침입자는 자신이 연결된 로컬 VLAN 내의 트래픽만 볼 수 있습니다.스위치에 포트 보안을 구성하여 CAM 테이블 오버플로 공격을 완화할 수 있습니다.이 옵션은 특정 스위치 포트의 MAC 주소 사양 또는 스위치 포트에서 학습할 수 있는 MAC 주소 수의 사양을 제공합니다.포트에서 잘못된 MAC 주소가 탐지되면 스위치에서 문제의 MAC 주소를 차단하거나 포트를 종료할 수 있습니다.스위치 포트의 MAC 주소 사양은 운영 환경에 대한 솔루션을 관리할 수 없습니다.스위치 포트에서 MAC 주소 수의 제한을 관리할 수 있습니다.관리적으로 확장 가능한 솔루션은 스위치에서 동적 포트 보안을 구현하는 것입니다.동적 포트 보안을 구현하려면 학습할 최대 MAC 주소 수를 지정합니다.
- **MAC(Media Access Control) 주소 스푸핑**MAC(Media Access Control) 스푸핑 공격은 다른 호스트의 알려진 MAC 주소를 사용하여 대상 스위치가 원격 호스트로 향하는 프레임을 네트워크 공격자에게 전달하도록 시도하는 것을 포함합니다.단일 프레임이 다른 호스트의 소스 이더넷 주소로 전송되면, 네트워크 공격자는 CAM 테이블 항목을 덮어쓰므로, 해당 호스트가 목적지인 패킷을 네트워크 공격자에게 전달합니다.호스트가 트래픽을 전송할 때까지 트래픽을 수신하지 않습니다.호스트가 트래픽을 전송하면 CAM 테이블 엔트리가 다시 원래 포트로 이동하도록 다시 작성됩니다.포트 보안 기능을 사용하여 MAC 스푸핑 공격을 완화하십시오.포트 보안은 특정 포트에 연결된 시스템의 MAC 주소를 지정하는 기능을 제공합니다.또한 포트 보안 위반이 발생할 경우 수행할 작업을 지정할 수 있습니다.

- **ARP(Address Resolution Protocol) 스푸핑**ARP는 동일한 서브넷의 호스트가 상주하는 LAN 세그먼트의 MAC 주소에 IP 주소 지정을 매핑하는 데 사용됩니다.일반적으로 호스트는 특정 IP 주소가 있는 다른 호스트의 MAC 주소를 찾기 위해 브로드캐스트 ARP 요청을 전송하고, ARP 응답은 해당 주소가 요청과 일치하는 호스트에서 수신됩니다.그런 다음 요청 호스트가 이 ARP 응답을 캐시합니다.ARP 프로토콜 내에서, 호스트에서 원하지 않는 ARP 응답을 수행하도록 또 다른 프로비저닝이 수행됩니다.요청되지 않은 ARP 회신을 GARP(무상 ARP)라고 합니다 .GAP는 공격자가 LAN 세그먼트에서 IP 주소의 ID를 스푸핑하기 위해 악의적인 공격을 받을 수 있습니다.일반적으로 이 ID는 "중간자(man-in-the-middle)" 공격의 기본 게이트웨이에서 두 호스트 간 또는 모든 트래픽 간에 ID를 스푸핑하는 데 사용됩니다.ARP 응답이 작성되면 네트워크 공격자는 자신의 시스템이 발신자가 찾는 대상 호스트로 표시되도록 할 수 있습니다.ARP 회신을 통해 발신자는 네트워크 공격자 시스템의 MAC 주소를 ARP 캐시에 저장합니다.이 MAC 주소는 스위치가 해당 CAM 테이블에 저장됩니다.이러한 방식으로 네트워크 공격자는 시스템의 MAC 주소를 발신자의 스위치 CAM 테이블과 ARP 캐시 모두에 삽입했습니다.이렇게 하면 네트워크 공격자가 스푸핑하는 호스트로 향하는 프레임을 가로채게 됩니다.인터페이스 컨피그레이션 메뉴의 보류 타이머를 사용하면 엔트리가 ARP 캐시에 유지되는 시간을 설정하여 ARP 스푸핑 공격을 줄일 수 있습니다.그러나 대기 타이머 자체만으로는 부족합니다.모든 최종 시스템에서 ARP 캐시 만료 시간을 수정하는 것은 물론 고정 ARP 항목을 수정해야 합니다.다양한 ARP 기반 네트워크 익스플로잇을 완화하는 데 사용할 수 있는 또 다른 솔루션은 동적 ARP 검사와 함께 DHCP 스누핑을 사용하는 것입니다.이러한 Catalyst 기능은 네트워크의 ARP 패킷을 검증하고 잘못된 MAC 주소가 있는 ARP 패킷의 IP 주소 바인딩에 대한 차단, 로깅 및 삭제를 허용합니다.DHCP 스누핑은 보안을 제공하기 위해 신뢰할 수 있는 DHCP 메시지를 필터링합니다.그런 다음 이러한 메시지를 사용하여 DHCP 스누핑 바인딩 테이블을 만들고 유지 관리합니다.DHCP 스누핑은 DHCP 서버 포트가 아닌 사용자 연결 포트에서 시작된 DHCP 메시지를 신뢰할 수 없는 것으로 간주합니다.DHCP 스누핑 관점에서, 이러한 신뢰할 수 없는 사용자 연결 포트는 DHCP 서버 유형 응답(예: DHCPOFFER, DHCPACK 또는 DHCPNAK)을 전송해서는 안 됩니다.DHCP 스누핑 바인딩 테이블에는 스위치의 로컬 신뢰할 수 없는 인터페이스에 해당하는 MAC 주소, IP 주소, 리스 시간, 바인딩 유형, VLAN 번호 및 인터페이스 정보가 포함됩니다.DHCP 스누핑 바인딩 테이블에는 신뢰할 수 있는 인터페이스와 상호 연결된 호스트에 대한 정보가 포함되지 않습니다.신뢰할 수 없는 인터페이스는 네트워크 또는 방화벽 외부에서 메시지를 수신하도록 구성된 인터페이스입니다.신뢰할 수 있는 인터페이스는 네트워크 내에서 보낸 메시지만 수신하도록 구성된 인터페이스입니다.DHCP 스누핑 바인딩 테이블에는 IP 주소 바인딩에 대한 동적 및 고정 MAC 주소가 모두 포함될 수 있습니다.동적 ARP 검사는 DHCP 스누핑 데이터베이스에 저장된 IP 주소 바인딩에 대한 유효한 MAC 주소를 기반으로 ARP 패킷의 유효성을 결정합니다.또한 동적 ARP 검사는 사용자 구성 가능한 ACL(Access Control List)을 기반으로 ARP 패킷을 검증할 수 있습니다. 이렇게 하면 정적으로 구성된 IP 주소를 사용하는 호스트에 대해 ARP 패킷을 검사할 수 있습니다.동적 ARP 검사를 사용하면 포트별 및 PACL(VLAN Access Control List)을 사용하여 특정 IP 주소에 대한 ARP 패킷을 특정 MAC 주소로 제한할 수 있습니다.
- **DHCP(Dynamic Host Configuration Protocol) 기아**DHCP 기아 공격은 스푸핑된 MAC 주소가 있는 DHCP 요청을 브로드캐스트하여 작동합니다.충분한 요청이 전송되면 네트워크 공격자는 일정 기간 동안 DHCP 서버에 사용 가능한 주소 공간을 낭비할 수 있습니다.그런 다음 네트워크 공격자는 시스템에 비인가 DHCP 서버를 설정하고 네트워크의 클라이언트에서 새 DHCP 요청에 응답할 수 있습니다.네트워크에 비인가 DHCP 서버를 배치하면 네트워크 공격자는 클라이언트에 주소 및 기타 네트워크 정보를 제공할 수 있습니다.DHCP 응답에는 일반적으로 기본 게이트웨이 및 DNS 서버 정보가 포함되므로 네트워크 공격자는 자신의 시스템을 기본 게이트웨이 및 DNS 서버로 제공할 수 있습니다.이 경우 중간자(man-in-the-middle) 공격이 발생합니다.그러나 모든 DHCP 주소의 배출은 비인가 DHCP 서버를 도입하는 데 필요하지 않습니다 .DHCP 스누핑과 같은 Catalyst 스위치 제품군의 추가 기능을 사용하여 DHCP 기아 공격을 방

지할 수 있습니다.DHCP 스누핑은 신뢰할 수 없는 DHCP 메시지를 필터링하고 DHCP 스누핑 바인딩 테이블을 구축하고 유지하는 보안 기능입니다.바인딩 테이블에는 MAC 주소, IP 주소, 리스 시간, 바인딩 유형, VLAN 번호 및 스위치의 로컬 신뢰할 수 없는 인터페이스에 해당하는 인터페이스 정보와 같은 정보가 포함됩니다.신뢰할 수 없는 메시지는 네트워크 또는 방화벽 외부에서 받은 메시지입니다.신뢰할 수 없는 스위치 인터페이스는 네트워크 또는 방화벽 외부에서 이러한 메시지를 수신하도록 구성된 인터페이스입니다.IP 소스 가드와 같은 다른 Catalyst 스위치 기능은 DHCP 기아 및 IP 스푸핑과 같은 공격에 대한 추가적인 방어 기능을 제공할 수 있습니다.DHCP 스누핑과 마찬가지로, 신뢰할 수 없는 레이어 2 포트에서 IP 소스 가드가 활성화됩니다.DHCP 스누핑 프로세스에 의해 캡처된 DHCP 패킷을 제외하고 모든 IP 트래픽이 초기에 차단됩니다.클라이언트가 DHCP 서버에서 유효한 IP 주소를 수신하면 PACL이 포트에 적용됩니다.이렇게 하면 클라이언트 IP 트래픽이 바인딩에 구성된 소스 IP 주소로 제한됩니다.바인딩의 주소 이외의 소스 주소를 가진 다른 IP 트래픽은 필터링됩니다.

구성

이 섹션에서는 포트 보안, DHCP 스누핑, 동적 ARP 검사 및 IP 소스 가드 보안 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

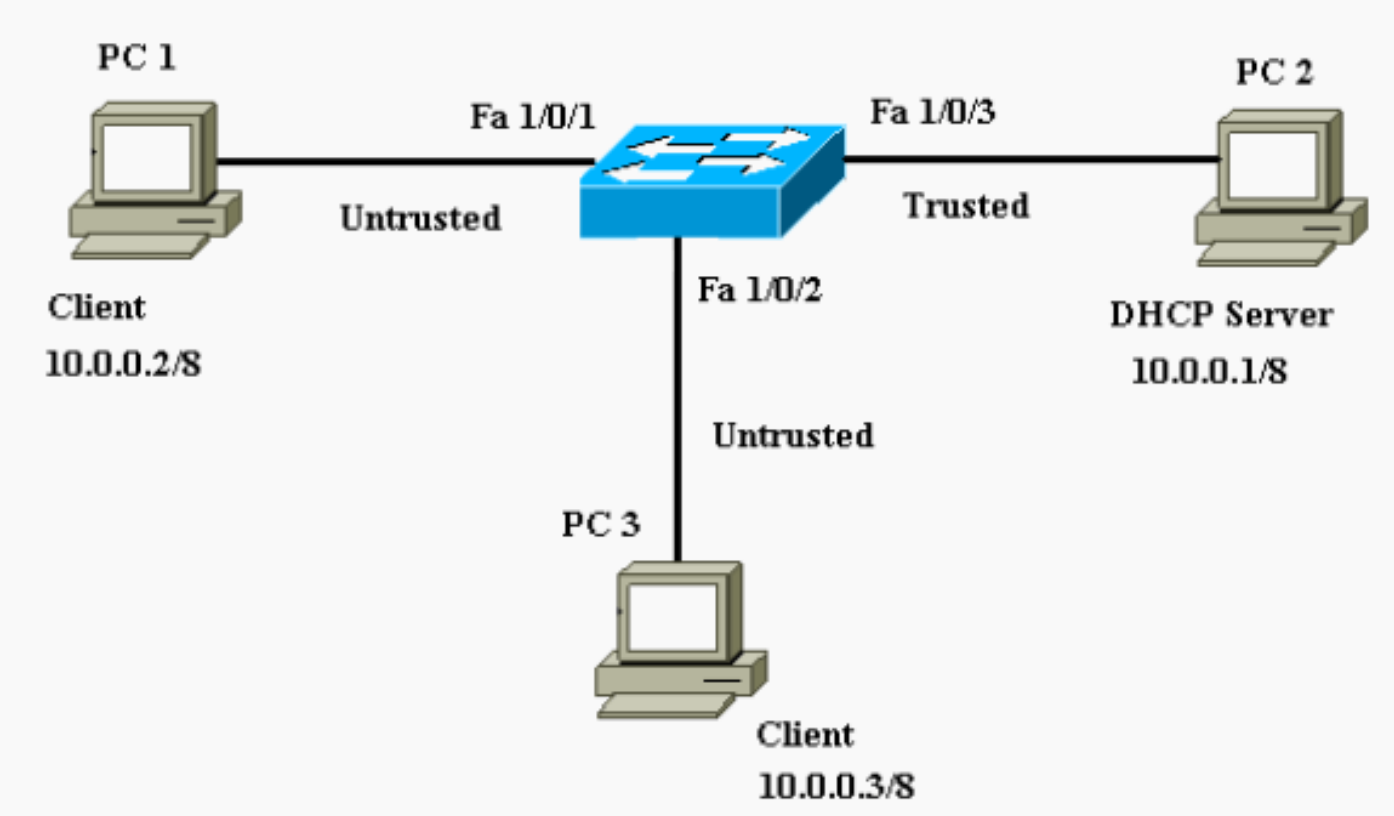
Catalyst 3750 스위치의 구성은 다음과 같습니다.

- 포트 보안
- DHCP 스누핑
- 동적 ARP 검사
- IP Source Guard

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

- PC 1과 PC 3은 스위치에 연결된 클라이언트입니다.
- PC 2는 스위치에 연결된 DHCP 서버입니다.
- 스위치의 모든 포트는 동일한 VLAN(VLAN 1)에 있습니다.
- DHCP 서버는 MAC 주소를 기반으로 클라이언트에 IP 주소를 할당하도록 구성됩니다.



포트 보안

포트 보안 기능을 사용하여 포트에 액세스할 수 있는 스테이션의 MAC 주소를 제한하고 식별할 수 있습니다.이렇게 하면 인터페이스에 대한 입력이 제한됩니다.보안 MAC 주소를 보안 포트에 할당할 때 포트는 소스 주소가 정의된 주소 그룹 외부에 있는 패킷을 전달하지 않습니다.보안 MAC 주소의 수를 1로 제한하고 단일 보안 MAC 주소를 할당하는 경우 해당 포트에 연결된 워크스테이션은 포트의 전체 대역폭을 보장합니다.포트가 보안 포트로 구성되어 있고 보안 MAC 주소의 최대 수에 도달하는 경우, 포트에 액세스하려고 시도하는 스테이션의 MAC 주소가 식별된 보안 MAC 주소와 다를 경우 보안 위반이 발생합니다.또한 보안 MAC 주소가 한 보안 포트에서 구성되거나 학습된 스테이션에서 다른 보안 포트에 액세스하려고 하면 위반이 플래그로 표시됩니다.기본적으로 보안 MAC 주소의 최대 수를 초과할 경우 포트가 종료됩니다.

참고: Catalyst 3750 스위치가 스택에 조인하면 새 스위치에서 구성된 보안 주소를 수신합니다.모든 동적 보안 주소는 다른 스택 멤버에서 새 스택 멤버에 의해 다운로드됩니다.

포트 보안 구성 방법에 대한 지침은 구성 지침을 참조하십시오.

여기서는 FastEthernet 1/0/2 인터페이스에 포트 보안 기능이 구성되어 있습니다.기본적으로 인터페이스에 대한 보안 MAC 주소의 최대 수는 1입니다.인터페이스의 포트 보안 상태를 확인하기 위해 **show port-security interface** 명령을 실행할 수 있습니다.

포트 보안

```
Cat3750#show port-security interface fastEthernet 1/0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
```

```
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
!--- Default port security configuration on the switch.
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#interface fastEthernet 1/0/2
Cat3750(config-if)#switchport port-security
Command rejected: FastEthernet1/0/2 is a dynamic port.
!--- Port security can only be configured on static
access ports or trunk ports. Cat3750(config-
if)#switchport mode access
!--- Sets the interface switchport mode as access.
Cat3750(config-if)#switchport port-security
!--- Enables port security on the interface.
Cat3750(config-if)#switchport port-security mac-address
0011.858D.9AF9
!--- Sets the secure MAC address for the interface.
Cat3750(config-if)#switchport port-security violation
shutdown
!--- Sets the violation mode to shutdown. This is the
default mode. Cat3750# !--- Connected a different PC (PC
4) to the FastEthernet 1/0/2 port !--- to verify the
port security feature. 00:22:51: %PM-4-ERR_DISABLE:
psecure-violation error detected on Fa1/0/2, putting
Fa1/0/2 in err-disable state 00:22:51: %PORT_SECURITY-2-
PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0011.8565.4B75 on port FastEthernet1/0/2.
00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet1/0/2, changed state to down
00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2,
changed state to down !--- Interface shuts down when a
security violation is detected. Cat3750#show interfaces
fastEthernet 1/0/2
FastEthernet1/0/2 is down, line protocol is down (err-
disabled)
!--- Output Suppressed. !--- The port is shown error-
disabled. This verifies the configuration. !--- Note:
When a secure port is in the error-disabled state, !---
you can bring it out of this state by entering !--- the
errdisable recovery cause psecure-violation global
configuration command, !--- or you can manually re-
enable it by entering the !--- shutdown and no shutdown
interface configuration commands.


Cat3750#show port-security interface fastEthernet 1/0/2
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0011.8565.4B75:1
Security Violation Count   : 1
```

참고: 동일한 MAC 주소를 스위치의 서로 다른 포트에서 보안 및 고정 MAC 주소로 구성해서는 안 됩니다.

IP 전화기가 음성 VLAN에 대해 구성된 스위치 포트를 통해 스위치에 연결되면 전화기는 태그가 지정되지 않은 CDP 패킷 및 태그가 지정된 음성 CDP 패킷을 전송합니다.따라서 IP 전화의 MAC 주소는 PVID와 VVID 모두에서 학습됩니다.적절한 수의 보안 주소가 구성되지 않은 경우 다음 메시지와 유사한 오류 메시지가 나타날 수 있습니다.

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:
```

이 문제를 해결하려면 포트에서 허용되는 최대 보안 주소를 2개(IP 전화의 경우)와 액세스 VLAN에서 허용되는 최대 보안 주소 수를 설정해야 합니다.

자세한 내용은 포트 보안 구성을 참조하십시오.

DHCP 스누핑

DHCP 스누핑은 신뢰할 수 없는 호스트와 DHCP 서버 간의 방화벽 역할을 합니다.DHCP 스누핑을 사용하여 최종 사용자에게 연결된 신뢰할 수 없는 인터페이스와 DHCP 서버 또는 다른 스위치에 연결된 신뢰할 수 있는 인터페이스를 구별합니다.스위치가 신뢰할 수 없는 인터페이스에서 패킷을 수신하고 DHCP 스누핑이 활성화된 VLAN에 속하는 경우, 스위치는 소스 MAC 주소와 DHCP 클라이언트 하드웨어 주소를 비교합니다.주소가 일치하면(기본값) 스위치가 패킷을 전달합니다.주소가 일치하지 않으면 스위치가 패킷을 삭제합니다.다음 상황 중 하나가 발생하면 스위치가 DHCP 패킷을 삭제합니다.

- DHCP 서버의 패킷(예: DHCPOFFER, DHCPACK, DHCPNAK 또는 DHCPLEERY 패킷)은 네트워크 또는 방화벽 외부에서 수신됩니다.
- 신뢰할 수 없는 인터페이스에서 패킷이 수신되고 소스 MAC 주소와 DHCP 클라이언트 하드웨어 주소가 일치하지 않습니다.
- 이 스위치는 DHCP 스누핑 바인딩 데이터베이스에 MAC 주소가 있는 DHCPRELEASE 또는 DHCPDECRION 브로드캐스트 메시지를 수신하지만 바인딩 데이터베이스의 인터페이스 정보는 메시지가 수신된 인터페이스와 일치하지 않습니다.
- DHCP 릴레이 에이전트는 DHCP 패킷을 전달합니다. 여기에는 0.0.0.0이 아닌 릴레이 에이전트 IP 주소가 포함되거나, 릴레이 에이전트는 옵션-82 정보가 포함된 패킷을 신뢰할 수 없는 포트로 전달합니다.

DHCP 스누핑을 구성하는 방법에 대한 지침은 DHCP 스누핑 구성 지침을 참조하십시오.

참고: DHCP 스누핑이 제대로 작동하려면 모든 DHCP 서버가 신뢰할 수 있는 인터페이스를 통해 스위치에 연결되어야 합니다.

참고: Catalyst 3750 스위치를 사용하는 스위치 스택에서 DHCP 스누핑은 스택 마스터에서 관리됩니다.새 스위치가 스택에 조인할 때 스위치는 스택 마스터에서 DHCP 스누핑 컨피그레이션을 받습니다.멤버가 스택을 떠나면 스위치와 연결된 모든 DHCP 스누핑 바인딩이 타임아웃됩니다.

참고: 데이터베이스의 임대 시간이 정확한지 확인하려면 NTP를 활성화하고 구성하는 것이 좋습니다.NTP가 구성된 경우 스위치 시스템 클럭이 NTP와 동기화되는 경우에만 스위치에서 바인딩 변경 사항을 바인딩 파일에 기록합니다.

비인가 DHCP 서버는 DHCP 스누핑 기능으로 완화할 수 있습니다.스위치에서 **DHCP를** 전역적으로 활성화하기 위해 ip dhcp snooping 명령이 실행됩니다.DHCP 스누핑으로 구성된 경우 VLAN의 모

든 포트는 DHCP 회신을 위해 신뢰할 수 없습니다.여기서는 DHCP 서버에 연결된 FastEthernet 인터페이스 1/0/3만 신뢰할 수 있는 인터페이스로 구성됩니다.

DHCP 스누핑

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1
!--- DHCP snooping is not active until DHCP snooping is
enabled on a VLAN. Cat3750(config)#no ip dhcp snooping
information option
!--- Disable the insertion and removal of the option-82
field, if the !--- DHCP clients and the DHCP server
reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit
(pps)
------------------------     -------     ---------------
-
FastEthernet1/0/3            yes         unlimited
!--- Displays the DHCP snooping configuration for the
switch. Cat3750#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type
VLAN  Interface
------------------  ---------------  ----------  -------
------  ----  --------------------
00:11:85:A5:7B:F5     10.0.0.2        86391       dhcp-
snooping  1    FastEtheret1/0/1
00:11:85:8D:9A:F9     10.0.0.3        86313       dhcp-
snooping  1    FastEtheret1/0/2
Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.
```

자세한 내용은 DHCP 기능 구성을 참조하십시오.

동적 ARP 검사

동적 ARP 검사는 네트워크의 ARP 패킷을 검증하는 보안 기능입니다.유효하지 않은 IP-MAC 주소 바인딩으로 ARP 패킷을 인터셉트, 로그 및 폐기합니다.이 기능은 특정 중간자 공격으로부터 네트워크를 보호합니다.

동적 ARP 검사는 유효한 ARP 요청 및 응답만 릴레이되도록 합니다.스위치는 다음과 같은 활동을 수행합니다.

- 신뢰할 수 없는 포트에서 모든 ARP 요청 및 응답 차단
- 이러한 인터셉트된 각 패킷은 로컬 ARP 캐시를 업데이트하기 전에 또는 패킷을 적절한 대상에 전달하기 전에 유효한 IP-MAC 주소 바인딩을 가지고 있는지 확인합니다.
- 잘못된 ARP 패킷을 삭제합니다.

동적 ARP 검사는 신뢰할 수 있는 데이터베이스인 DHCP 스누핑 바인딩 데이터베이스에 저장된 유효한 IP-MAC 주소 바인딩을 기반으로 ARP 패킷의 유효성을 결정합니다.이 데이터베이스는 VLAN 및 스위치에서 DHCP 스누핑이 활성화된 경우 DHCP 스누핑에 의해 구축됩니다.ARP 패킷이 신뢰할 수 있는 인터페이스에서 수신되면 스위치는 확인 없이 패킷을 전달합니다.신뢰할 수 없는 인터페이스에서 스위치는 유효한 경우에만 패킷을 전달합니다.

비 DHCP 환경에서 동적 ARP 검사는 정적으로 구성된 IP 주소가 있는 호스트의 사용자 구성 ARP ACL에 대해 ARP 패킷을 검증할 수 있습니다.ARP ACL을 정의하기 위해 arp **access-list** 전역 컨피그레이션 명령을 실행할 수 있습니다.ARP ACL은 DHCP 스누핑 바인딩 데이터베이스의 항목보다 우선합니다.스위치는 ACL을 구성하기 위해 **ip arp 검사 필터 vlan** 전역 컨피그레이션 명령을 실행하는 경우에만 ACL을 사용합니다.스위치는 먼저 ARP 패킷을 사용자 구성 ARP ACL과 비교합니다.ARP ACL이 ARP 패킷을 거부하면 스위치는 DHCP 스누핑으로 채워진 데이터베이스에 유효한 바인딩이 존재하더라도 패킷을 거부합니다.

동적 ARP 검사 구성 방법에 대한 지침은 동적 ARP 검사 컨피그레이션 지침을 참조하십시오.

VLAN별로 **동적 ARP** 검사를 활성화하려면 ip arp inspection vlan 전역 컨피그레이션 명령이 실행됩니다.여기서는 DHCP 서버에 연결된 FastEthernet 인터페이스 1/0/3만 **ip arp inspection trust** 명령을 사용하여 신뢰된 **것으로** 구성됩니다.동적으로 IP 주소를 할당한 ARP 패킷을 허용하려면 DHCP 스누핑을 활성화해야 합니다.DHCP 스누핑 구성 정보는 이 문서의 DHCP 스누핑 섹션을 참조하십시오.

동적 ARP 검사

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip arp inspection vlan 1
!--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match
Static ACL
 ----     -------------    ---------   ---------
----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
!--- Verifies the dynamic ARP inspection configuration.
Cat3750#
```

자세한 내용은 동적 ARP 검사 구성을 참조하십시오.

IP Source Guard

IP 소스 가드는 라우팅되지 않은 레이어 2 인터페이스에서 IP 트래픽을 제한하기 위해 DHCP 스누핑 바인딩 데이터베이스 및 수동으로 구성된 IP 소스 바인딩을 기반으로 트래픽을 필터링하는 보안 기능입니다.호스트가 인접 디바이스의 IP 주소를 사용하려고 할 때 발생하는 트래픽 공격을 방지하려면 IP 소스 가드를 사용할 수 있습니다.IP 소스 가드는 IP/MAC 스푸핑을 방지합니다.

신뢰할 수 없는 인터페이스에서 DHCP 스누핑이 활성화된 경우 IP 소스 가드를 활성화할 수 있습니다.인터페이스에서 IP 소스 가드가 활성화되면 스위치에서는 인터페이스에서 수신된 모든 IP 트래픽을 차단합니다. 단, DHCP 스누핑에서 허용하는 DHCP 패킷은 제외합니다.포트 ACL이 인터페이스에 적용됩니다.포트 ACL은 IP 소스 바인딩 테이블에 소스 IP 주소가 있는 IP 트래픽만 허용하고 다른 모든 트래픽을 거부합니다.

IP 소스 바인딩 테이블에는 DHCP 스누핑으로 학습되거나 수동으로 구성된 바인딩(고정 IP 소스 바인딩)이 있습니다. 이 테이블의 항목에는 IP 주소, 관련 MAC 주소 및 관련 VLAN 번호가 있습니다.스위치는 IP 소스 가드가 활성화된 경우에만 IP 소스 바인딩 테이블을 사용합니다.

소스 IP 주소 필터링 또는 소스 IP 및 MAC 주소 필터링을 사용하여 IP 소스 가드를 구성할 수 있습니다.이 옵션을 사용하여 IP 소스 가드를 활성화하면 소스 IP 주소를 기반으로 IP 트래픽이 필터링됩니다.소스 IP 주소가 DHCP 스누핑 바인딩 데이터베이스의 항목 또는 IP 소스 바인딩 테이블의 바인딩과 일치할 경우 스위치는 IP 트래픽을 전달합니다.이 옵션을 사용하여 IP 소스 가드를 활성화하면 소스 IP 및 MAC 주소를 기반으로 IP 트래픽이 필터링됩니다.스위치는 소스 IP 및 MAC 주소가 IP 소스 바인딩 테이블의 항목과 일치하는 경우에만 트래픽을 전달합니다.

참고: IP 소스 가드는 액세스 및 트렁크 포트를 포함하는 레이어 2 포트에서만 지원됩니다.

IP 소스 가드 구성 방법에 대한 지침은 IP Source Guard 구성 지침을 참조하십시오.

여기서 소스 IP 필터링이 포함된 IP 소스 가드는 FastEthernet 1/0/1 인터페이스에서 **ip verify source** 명령을 사용하여 구성됩니다.VLAN에서 소스 IP 필터링이 있는 IP 소스 가드가 활성화된 경우 인터페이스가 속한 액세스 VLAN에서 DHCP 스누핑을 활성화해야 합니다.스위치에서 IP 소스 **가드** 컨피그레이션을 확인하려면 show ip verify source 명령을 실행합니다.

IP Source Guard

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1
!--- See the DHCP Snooping section of this document for
!--- DHCP snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source
!--- Enables IP source guard with source IP filtering.
Cat3750#show ip verify source
Interface  Filter-type  Filter-mode  IP-address
Mac-address        Vlan
---------  -----------  -----------  ---------------  --
---------------  -----
Fa1/0/1    ip           active       10.0.0.2
1
!--- For VLAN 1, IP source guard with IP address
filtering is configured !--- on the interface and a
binding exists on the interface. Cat3750#
```

자세한 내용은 IP Source Guard 이해를 참조하십시오.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 프라이빗 VLAN 및 VLAN 액세스 제어 목록으로 네트워크 보안 설정
- LAN 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems