IPDT 장치 작업 확인

목차

소개

이 문서에서는 IPDT(IP 장치 추적) 작업을 확인하는 방법과 이러한 작업을 비활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 출력은 다음과 같은 소프트웨어 및 하드웨어 버전을 기준으로 합니다.

- Cisco WS-C2960X
- Cisco IOS® 15.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

IPDT 개요

정의 및 사용

기본 IPDT 작업은 연결된 호스트(MAC 및 IP 주소 연결)를 추적하는 것입니다. 이를 위해 유니캐스트 ARP(Address Resolution Protocol) 프로브를 기본 간격 30초로 전송합니다. 이러한 프로브는 링크의 다른 쪽에 연결된 호스트의 MAC 주소로 전송되며, RFC 5227에 나열된 ARP 프로브 정의에 따라 레이어 2(L2)를 ARP가 전송되는 물리적 인터페이스의 MAC 주소와 발신자 IP 주소 0.0.0.0의 기본 소스로 사용합니다

발췌

이 문서에서는 ARP 프로브라는 용어를 사용하여 모든 발신자 IP 주소가 0인 로컬 링크에서 브로드캐스트되는 ARP 요청 패킷을 참조합니다. 발신자 하드웨어 주소에는 패킷을 전송하는 인터페이스의 하드웨어 주소가 포함되어야 합니다. 다른 호스트에서 주소를 이미 사용 중인 것으로 확인된 경우 동일한 링크에서 다른 호스트의 ARP 캐시가 손상되지 않도록 하려면 sender IP address 필드를 모두 0으로 설정해야 합니다. 대상 IP 주소 필드는 프로브되는 주소로 설정되어야 합니다. ARP 프로브는 질문(이 주소를 사용하는 사람이 있습니까?)과 암시된 설명(이 주소는 사용하려는 주소입니다.)을 모두 전달합니다.

IPDT의 목적은 스위치가 IP 주소를 통해 스위치에 연결된 장치 목록을 가져오고 유지 관리하는 것입니다. 프로브는 추적 항목을 채우지 않습니다. 호스트에서 ARP 요청/응답을 통해 항목을 학습한 후 테이블의 항목을 유지 관리하기 위해 사용합니다.

IP ARP 검사는 IPDT가 활성화된 경우 자동으로 활성화됩니다. ARP 패킷을 모니터링할 때 새 호스트의 존재를 탐지합니다. 동적 ARP 검사가 활성화된 경우, 디바이스 추적 테이블에 대한 새 호스트를 탐지하기 위해 검증하는 ARP 패킷만 사용됩니다.

IP DHCP 스누핑이 활성화된 경우 DHCP가 IP 주소를 할당하거나 취소할 때 새 호스트의 존재 또는 제거를 탐지합니다. 지정된 호스트에 대해 DHCP 트래픽이 표시되면 IPDT ARP 프로브 간격 타이머가 재설정됩니다.

IPDT는 항상 사용 가능한 기능입니다. 그러나 최신 Cisco IOS® 릴리스에서는 기본적으로 상호 종속성이 활성화되어 있습니다(Cisco 버그 ID CSCuj04986 참조). 동적 ACL(Access Control List)의 소스 IP를 채우거나 보안 그룹 태그에 대한 IP 주소의 바인딩을 유지하기 위해 IP/MAC 호스트 연결의 데이터베이스를 사용하는 경우 매우 유용할 수 있습니다.

ARP 프로브는 두 가지 상황에서 전송됩니다.

- IPDT 데이터베이스의 현재 항목과 연결된 링크가 DOWN에서 UP 상태로 이동하고 ARP 항목이 채워집니다.
- IPDT 데이터베이스의 항목과 연결된 UP 상태의 링크에 프로브 간격이 만료되었습니다.

문제

스위치가 보낸 keepalive 프로브는 L2 검사입니다. 따라서 스위치의 관점에서 ARP에서 소스로 사용되는 IP 주소는 중요하지 않습니다. 이 기능은 IP 주소가 전혀 구성되지 않은 디바이스에서 사용할 수 있으므로 IP 소스 0.0.0.0은 관련이 없습니다.

호스트는 이 메시지를 받으면 다시 회신하고 수신 패킷에서 사용 가능한 유일한 IP 주소(자체 IP 주소)로 대상 IP 필드를 채웁니다. 이렇게 하면 응답하지 않는 중복 IP 주소 알림이 발생할 수 있습니다. 응답하는 호스트가 자체 IP 주소를 패킷의 소스와 대상으로 인식하기 때문입니다. 중복 IP 주소 0.0.0.0을 참조하십시오. 중복 IP 주소 시나리오에 대한 자세한 내용은 오류 메시지 문제 해결 문서를 참조하십시오.

기본 상태 및 작업

IPDT에 대한 글로벌 on/off 컨피그레이션은 특정 기능이 작동하기 위해 IPDT를 켜야 한다는 사실을 고객이 항상 인지하지 못했기 때문에 현장에서 문제를 일으킨 레거시 동작입니다. 현재 릴리스에서 IPDT는 IPDT가 필요한 기능을 활성화할 때 인터페이스 레벨에서만 제어됩니다.

IPDT는 이러한 릴리스 내에서 기본적으로 전역적으로 사용됩니다. 즉, 전역 컨피그레이션 명령이 없습니다.

- Catalyst 2k/3k: 15.2(1)E
- Catalyst 3850: 3.2.0SE
- Catalyst 4k: 15.2(1)E / 3.5.0E

IPDT가 전역적으로 활성화된 경우에도 이는 IPDT가 지정된 포트를 적극적으로 모니터링한다는 의미는 아닙니다.

IPDT가 항상 켜져 있고 IPDT가 전역적으로 활성화된 경우 IPDT를 전역적으로 전환/해제할 수 있는 릴리스에서는 다른 기능이 실제로 특정 인터페이스에서 IPDT가 활성화되어 있는지 여부를 결정합니다(기능 영역 섹션 참조).

기능 영역

지정된 인터페이스에서 전송된 IPDT 및 해당 ARP 프로브는 다음 기능에 사용됩니다.

- NMSP(Network Mobility Services Protocol), 버전 3.2.0E, 15.2(1)E, 3.5.0E 이상
- 장치 센서, 버전 15.2(1)E, 3.5.0E 이상
- 1X, MAB(MAC Authentication Bypass), 세션 관리자
- 웹 기반 인증
- 인증 프록시
- 고정 호스트용 IPSG(IP Source Guard)
- Flexible Netflow
- Cisco TrustSec(CTS)

- 미디어 추적
- HTTP 리디렉션

기능 매트릭스

플랫폼	기능	기본값 설정(시작 위치)	Disable 메서드	CLI 비활성화
Cat 2960/3750(Cisco IOS)	IPDT	15.2(1)E *	글로벌 CLI(이전 릴리스) * 인터페이스당	ip 디바이스 추적 없음* ip 장치 추적 최대 0***
Cat 2960/3750(Cisco IOS)	NMSP	아니요	글로벌 CLI 또는 인터페이스당 CLI	nmsp 활성화 없음 nmsp 첨부 파일 ****
Cat 2960/3750(Cisco IOS)	장치 센서	15.0(1)SE	글로벌 CLI	매크로 자동 모니터 없음
Cat 2960/3750(Cisco IOS)	ARP 스누핑	15.2(1)E **	해당 없음	해당 없음
Cat 3850	IPDT	모든 릴리스 *	인터페이스당 *	ip 장치 추적 최대 0***
Cat 3850	NMSP	모든 릴리스	인터페이스당	nmsp 첨부 파일 표시 안 함
Cat 3850	장치 센서	아니요	해당 없음	해당 없음
Cat 3850	ARP 스누핑	모든 릴리스 **	해당 없음	해당 없음
고양이 4500	IPDT	15.2(1)E / 3.5.0E *	글로벌 CLI(이전 릴리스) *	ip 디바이스 추적 없음* ip 장치 추적 최대 0***

			인터페이스당	
고양이 4500	NMSP	아니요	글로벌 CLI 또는 인터페이스당 CLI	nmsp 활성화 없음 nmsp 첨부 파일 ****
고양이 4500	장치 센서	15.1(1)SG / 3.3.0SG	글로벌 CLI	매크로 자동 모니터 없음
고양이 4500	ARP 스누핑	15.2(1)E / 3.5.0E **	해당 없음	해당 없음

기능

- IPDT는 최신 릴리스에서 전역적으로 비활성화할 수 없지만, IPDT가 필요한 기능이 활성화되어 있는 경우 포트에서만 활성화됩니다.
- ARP 스누핑은 특정 기능 조합이 활성화하는 경우에만 활성화됩니다.
- 인터페이스별로 IPDT를 비활성화하면 ARP 스누핑이 중지되지 않고 IPDT 추적이 방지됩니다. i3.3.0SE, 15.2(1)E, 3.5.0E 이상에서 사용할 수 있습니다.
- 인터페이스당 NMSP 억제는 NMSP가 전역적으로 활성화된 경우에만 사용할 수 있습니다.

IPDT 비활성화

IPDT가 기본적으로 활성화되지 않은 릴리스에서는 다음 명령을 사용하여 IPDT를 전역적으로 끌 수 있습니다.

```
<#root>

Switch(config)#

no ip device tracking
```

IPDT가 항상 켜져 있는 릴리스에서는 이전 명령을 사용할 수 없거나 IPDT를 비활성화할 수 없습니다(Cisco 버그 ID CSCuj04986). 이 경우 IPDT가 특정 포트를 모니터링하지 않거나 중복 IP 알림을 생성하지 않도록 하는 몇 가지 방법이 있습니다.

IP Device Tracking Probe Delay 10 명령을 입력합니다

이 명령을 사용하면 링크 UP/플랩을 탐지할 때 10초 동안 스위치에서 프로브를 전송할 수 없습니다. 그러면 링크의 다른 쪽에 있는 호스트가 중복 IP 주소를 확인하는 동안 프로브를 전송할 가능성이 최소화됩니다. RFC는 중복 주소 감지를 위해 10초 기간을 지정하므로 디바이스 추적 프로브를 지연하면 대부분의 경우 문제를 해결할 수 있습니다.

호스트(예: Microsoft Windows PC)가 중복 주소 탐지 단계에 있는 동안 스위치에서 클라이언트에 대한 ARP 프로브를 보내는 경우, 호스트에서 프로브를 중복 IP 주소로 탐지하고 네트워크에서 중복 IP 주소가 발견되었다는 메시지를 사용자에게 표시합니다. PC에서 주소를 가져오지 못한 경우, 사용자가 수동으로 주소를 해제/갱신하고 연결을 끊은 다음 네트워크에 다시 연결하거나 PC를 재부팅해야 네트워크에 액세스할 수 있습니다.

프로브 지연 이외에도 스위치가 PC/호스트에서 프로브를 탐지할 때 지연이 자체적으로 재설정됩니다. 예를 들어, 프로브 타이머가 5초로 카운트다운되고 PC/호스트에서 ARP 프로브를 탐지하면 타이머가 다시 10초로 재설정됩니다.

이 컨피그레이션은 Cisco 버그 ID CSCtn27420을 통해 사용할 수 있습니다.

IP Device Tracking Probe(IP 디바이스 추적 프로브) Use SVI(SVI 사용) 명령을 입력합니다

이 명령을 사용하면 비 RFC 규격 ARP 프로브를 보내도록 스위치를 구성할 수 있습니다. IP 소스는 0.0.0.0이 아니라 호스트가 상주하는 VLAN의 SVI(Switch Virtual Interface)입니다. Microsoft Windows 시스템은 더 이상 프로브를 RFC 5227에 정의된 프로브로 보지 않으며 잠재적인 중복 IP에 플래그를 지정하지 않습니다.

IP Device Tracking Probe Auto-Source [fallback <host-ip> <mask>] [override] 명령을 입력합니다

예측 가능/제어 가능한 엔드 디바이스가 없거나 L2 전용 역할의 스위치가 많은 고객의 경우, 설계에 레이어 3 변수를 도입하는 SVI의 컨피그레이션은 적합한 솔루션이 아닙니다. 버전 15.2(2)E 이상에서 도입된 개선 사항으로, IPDT에서 생성한 ARP 프로브에서 소스 주소로 사용하기 위해 스위치에 속할 필요가 없는 IP 주소를 임의로 할당할 수 있습니다. 이러한 개선 사항에서는 다음과 같은 방법으로 시스템의 자동 동작을 수정할 수 있습니다(이 목록에서는 각 명령이 사용된 후 시스템이 자동으로 동작하는 방식을 보여줍니다).

IP Device Tracking Probe Auto-Source 명령을 입력합니다

1. 소스가 있는 경우 VLAN SVI로 설정합니다.

2. 동일한 서브넷에 대한 IP 호스트 테이블에서 소스/MAC 쌍을 검색합니다.

3. 기본 경우와 같이 제로 IP 소스를 전송합니다.

IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 명령을 입력합니다

1. 소스가 있는 경우 VLAN SVI로 설정합니다.

2. 동일한 서브넷에 대한 IP 호스트 테이블에서 소스/MAC 쌍을 검색합니다.

3. 제공된 호스트 비트 및 마스크로 대상 IP에서 소스 IP를 계산합니다.

IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Override 명령을 입력합니다

1. 소스가 있는 경우 VLAN SVI로 설정합니다.

2. 제공된 호스트 비트 및 마스크로 대상 IP에서 소스 IP를 계산합니다.

> 참고: 재정의를 사용하면 테이블의 항목 검색을 건너뛸 수 있습니다.

이전 계산의 예로 호스트 192.168.1.200을 프로브한다고 가정합니다. 제공된 마스크 및 호스트 비트를 사용하여 192.168.1.1의 소스 주소를 생성합니다. 항목 10.5.5.20을 프로브하는 경우 소스 주소 10.5.5.1 등의 ARP 프로브를 생성할 수 있습니다.

IP Device Tracking Maximum 0 명령을 입력합니다

이 명령은 IPDT를 실제로 비활성화하지는 않지만 추적되는 호스트 수를 0으로 제한합니다. 이는 권장되는 솔루션이 아니며, Cisco 버그 ID CSCun81556에 설명된 대로 포트 채널 컨피그레이션을 포함하는 IPDT를 사용하는 다른 모든 기능에 영향을 주므로 주의해서 사용해야 합니다.

IPDT를 트리거하는 활성 기능 끄기

IPDT를 트리거할 수 있는 일부 기능에는 NMSP, 장치 센서, dot1x/MAB, WebAuth 및 IPSG가 있습니다. 이러한 기능은 트렁크 포트에서 활성화하지 않는 것이 좋습니다. 이 솔루션은 이전에 사용 가능했던 모든 솔루션이 예상대로 작동하지 않거나 추가 문제가 발생한 가장 어렵거나 복잡한 상황을 위해 예약되어 있습니다. 그러나 IPDT를 비활성화할 경우 문제를 일으키는 IPDT 관련 기능만 끄고 다른 모든 기능은 영향을 받지 않도록 할 수 있기 때문에 이 솔루션만이 매우 세분화된 기능을 제공합니다.

최신 Cisco IOS 버전 15.2(2)E 이상에서는 다음과 유사한 출력이 표시됩니다.

<#root>

```
Switch#

show ip device tracking interface GigabitEthernet 1/0/9


------------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IPv6 Device Tracking Client Registered Handle: 75
IP Device Tracking Enabled Features:
       HOST_TRACK_CLIENT_ATTACHMENT
       HOST_TRACK_CLIENT_SM
```

출력 하단에 있는 모든 대문자의 두 줄은 IPDT를 사용하여 작동합니다. 인터페이스에서 실행되는 단일 서비스를 비활성화하면 디바이스 추적을 비활성화할 때 발생하는 대부분의 문제를 방지할 수 있습니다.

이전 버전의 Cisco IOS에서는 인터페이스에서 어떤 모듈이 활성화되었는지 알 수 있는 이 쉬운 방법을 아직 사용할 수 없으므로 동일한 결과를 얻으려면 좀 더 관여된 프로세스를 거쳐야 합니다. 대부분의 설정에서 안전해야 하는 저빈도 로그인 debug ip device track interface를 설정해야 합니다. 디버그 IP 장치 추적을 모두 켜지 않도록 주의하십시오. 이는 반대로 확장 상황에서 콘솔을 플러딩하기 때문입니다.

디버그가 켜지면 인터페이스를 기본값으로 되돌린 다음 인터페이스 컨피그레이션에서 IPDT 서비스를 추가 및 제거합니다. 디버깅의 결과는 사용한 명령으로 어떤 서비스가 활성화/비활성화되었는지 알려줍니다.

예

```
<#root>

Switch(config)#

interface GigabitEthernet 1/0/9


Switch(config-if)#

ip device tracking maximum 10


Switch(config-if)#
*Mar 27 09:58:49.470: sw_host_track-interface:Feature 00000008 enabled on port
Gi1/0/9, mask now 0000004C, 65 ports enabled
*Mar 27 09:58:49.471: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max set to 10
Switch(config-if)#
```

출력에서 알 수 있는 것은 기능 마스크를 00000008 새 기능 마스크가 0000004C라는 것입니다.

이제 방금 추가한 컨피그레이션을 제거합니다.

```
<#root>

Switch(config-if)#

no ip device tracking maximum 10


Switch(config-if)#
*Mar 27 10:02:31.154: sw_host_track-interface:Feature 00000008 disabled on port
Gi1/0/9, mask now 00000044, 65 ports enabled
*Mar 27 10:02:31.154: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max cleared
*Mar 27 10:02:31.154: sw_host_track-interface:Max limit has been removed from
the interface GigabitEthernet1/0/9.
```

```
Switch(config-if)#
```

피쳐 마스크를 00000008 원래 기본 마스크여야 하는 00000044 마스크를 볼 수 있습니다. AIM이 0x00000004이고 SM이 0x00000040이므로 이 00000044 값이 예상되므로 0x00000044이 됩니다.

인터페이스에서 실행할 수 있는 여러 IPDT 서비스가 있습니다.

IPT 서비스	인터페이스
HOST_TRACK_CLIENT_IP_ADMISSION	= 0x00000001
HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_ATTACHMENT	= 0x00000004
HOST_TRACK_CLIENT_TRACK_HOST_UPTO_MAX	= 0x00000008
HOST_TRACK_CLIENT_RSVP	= 0x00000010
HOST_TRACK_CLIENT_CTS	= 0x00000020
HOST_TRACK_CLIENT_SM	= 0x00000040
HOST_TRACK_CLIENT_WIRELESS	= 0x00000080

이 예에서는 HOST_TRACK_CLIENT_SM(SESSION-MANAGER) 및 HOST_TRACK_CLIENT_ATTACHMENT(AIM/NMSP라고도 함) 모듈이 IPDT에 대해 구성됩니다. 이 인터페이스에서 IPDT를 끄려면 둘 다 비활성화해야 합니다. IPDT를 사용하는 모든 기능이 비활성화된 경우에만 IPDT가 비활성화되기 때문입니다.

이러한 기능을 비활성화하면 다음과 유사한 출력이 표시됩니다.

<#root>

```
Switch(config-if)#
```

do show ip device tracking interface GigabitEthernet 1/0/9

```
-------------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled     ß IPDT is disabled
```

```
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IP Device Tracking Enabled Features:
ß No active features
-----------------------------------------
```

이러한 방식으로, IPDT는 더 세분화하여 비활성화된다.

다음은 앞에서 설명한 기능 중 일부를 비활성화하는 데 사용되는 명령의 몇 가지 예입니다.

- nmsp 연결 억제
- 매크로 자동 모니터 없음

참고: 최신 기능은 네트워크의 스위치 위치에 따라 기능을 활성화하고 네트워크 전반에 걸친 대규모 컨피그레이션 구축에 사용되는 Smart Ports를 지원하는 플랫폼에서만 사용할 수 있어야 합니다.

IPDT 작업 확인

디바이스에서 IPDT 상태를 확인하려면 다음 명령을 사용합니다.

- ip 장치 추적 표시
  이 명령은 IPDT가 활성화된 인터페이스와 MAC/IP/인터페이스 연결이 현재 추적되는 인터페이스를 표시합니다.
- ip 장치 추적 지우기
- 이 명령은 IPDT 관련 항목을 지웁니다.

참고: 스위치는 제거된 호스트에 ARP 프로브를 전송합니다. 호스트가 있으면 ARP 프로브에 응답하고 스위치는 호스트에 대한 IPDT 항목을 추가합니다. clear IPDT 명령을 실행하기 전에 ARP 프로브를 비활성화해야 합니다. 이렇게 하면 모든 ARP 항목이 사라집니다. clear ip device tracking 명령 이후에 ARP 프로브가 활성화되면 모든 항목이 다시 반환됩니다.

- debug ip 장치 추적
  이 명령을 사용하면 IPDT 활동을 실시간으로 표시하기 위해 디버그를 수집할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.