Controleer de werking van IPDT-apparaten

Inhoud

Inleiding

Dit document beschrijft hoe de IPDT-bewerkingen (IP Device Tracking) moeten worden geverifieerd en hoe deze acties moeten worden uitgeschakeld.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies. De resultaten in dit document zijn echter gebaseerd op deze software- en hardwareversies:

- Cisco WS-C2960X switch
- Cisco IOS® 15.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

IPDT - Overzicht

Definitie en gebruik

De belangrijkste taak van IPDT is het bijhouden van verbonden hosts (koppeling van MAC- en IP-adres). Hiertoe worden door het UNICAST Address Resolution Protocol (ARP)-probes met een standaardinterval van 30 seconden verstuurd. deze sondes worden verzonden naar het MAC-adres van de host die is aangesloten aan de andere kant van de link, en gebruiken Layer 2 (L2) als de standaardbron het MAC-adres van de fysieke interface waaruit de ARP gaat en een IP-adres van de afzender van 0.0.0.0, gebaseerd op de ARP-sonde-definitie die in RFC 5227 wordt vermeld.

fragment

In dit document wordt de term 'ARP Probe' gebruikt om te verwijzen naar een ARP-verzoekpakket, uitgezonden via de lokale link, met een all-zero 'afzender IP-adres'. Het 'sender hardware address' MOET het hardware adres bevatten van de interface die het pakket verstuurt. Het veld 'Afzender IP-adres' MOET worden ingesteld op alle nullen om corruptie te voorkomen bij ARP-caches in andere hosts op dezelfde link in het geval dat het adres al in gebruik blijkt te zijn door een andere host. Het veld 'IP-adres doel' MOET worden ingesteld op het adres dat wordt gepeild. Een ARP-sonde bevat zowel een vraag (*gebruikt iemand dit adres?*) als een impliciete verklaring (*Dit is het adres dat ik hoop te gebruiken*.)

Het doel van IPDT is voor de switch om een lijst van apparaten te verkrijgen en te handhaven die met de switch via een IP adres worden verbonden. De sonde vult het volgpunt niet in; het wordt eenvoudig gebruikt om de ingang in de lijst te handhaven nadat het door een ARP verzoek/antwoord van de gastheer wordt geleerd.

IP ARP-inspectie wordt automatisch ingeschakeld wanneer IPDT is ingeschakeld; het detecteert de aanwezigheid van nieuwe hosts wanneer het ARP-pakketten bewaakt. Als dynamische ARP-inspectie is ingeschakeld, worden alleen de ARP-pakketten die worden gevalideerd gebruikt om nieuwe hosts voor de tabel Apparaattracering te detecteren.

IP DHCP-spionage detecteert, indien ingeschakeld, de aanwezigheid of verwijdering van nieuwe hosts wanneer DHCP hun IP-adressen toewijst of intrekt. Wanneer DHCP-verkeer wordt gezien voor een bepaalde host, wordt de IPDT ARP-sonde interfacetimer opnieuw ingesteld.

IPDT is een functie die altijd beschikbaar is geweest. Bij recentere Cisco IOS®-releases is de onderlinge afhankelijkheid echter standaard ingeschakeld (zie 'Cisco bug-id CSCuj04986'). Het kan uiterst nuttig zijn wanneer zijn database van IP/MAC-hostassociaties wordt gebruikt om de IP-bron van dynamische toegangscontrolelijsten (ACL's) te vullen of om een binding van een IP-adres aan een beveiligingsgroeptag te handhaven.

De ARP-sonde wordt onder twee omstandigheden verzonden:

- De link die gekoppeld is aan een huidige ingang in de IPDT-database beweegt zich van een DOWN naar een UP-staat en de ARP-ingang is ingevuld.
- Een link die al in de UP staat die is gekoppeld aan een ingang in de IPDT-database heeft een verlopen sonderinterval.

Probleem

De "keepalive"-sonde die door de switch wordt verzonden is een L2-controle. Vanuit het oogpunt van de switch zijn de IP-adressen die als bron in de ARP's worden gebruikt, niet van belang: Deze optie kan worden gebruikt op apparaten zonder IP-adres dat helemaal niet is geconfigureerd, dus de IP-bron van 0.0.0.0 is niet relevant.

Wanneer de host deze berichten ontvangt, antwoordt hij terug en vult het IP-doelveld met het enige IP-adres dat beschikbaar is in het ontvangen pakket, dat zijn eigen IP-adres is. Dit kan valse dubbele IP adreswaarschuwingen veroorzaken, omdat de gastheer die antwoordt zijn eigen IP adres als zowel bron als bestemming van het pakket ziet; Raadpleeg het gedeelte IP-adres dupliceren 0.0.0.0. Error Message Troubleshoot voor meer informatie over het scenario met het dubbele IP-adres.

Stand en werking

De wereldwijde aan/uit-configuratie voor IPDT is een legacy-gedrag dat problemen in het veld veroorzaakte omdat klanten zich niet altijd bewust waren dat ze IPDT moesten inschakelen om bepaalde functies te laten werken. In huidige releases wordt IPDT alleen bestuurd op interfaceniveau wanneer het een functie inschakelt die IPDT vereist.

IPDT is wereldwijd standaard ingeschakeld met in deze releases; dat wil zeggen, geen globale configuratieopdracht vanwege 'Cisco bug ID CSCua85383':

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

Het is belangrijk om op te merken dat, zelfs als IPDT mondiaal wordt toegelaten, dat niet noodzakelijk impliceert dat IPDT actief een bepaalde haven controleert.

Op releases waar IPDT altijd is ingeschakeld en waar IPDT globaal kan worden uitgeschakeld, als IPDT wereldwijd is ingeschakeld, bepalen andere functies of het actief is op een specifieke interface (zie de sectie Functionaliteitsgebieden).

Functionaliteitsgebieden

IPDT en zijn ARP sondes die uit een bepaalde interface worden verzonden worden gebruikt voor deze eigenschappen:

- Network Mobility Services Protocol (NMSP), versies 3.2.0E, 15.2(1)E, 3.5.0E en hoger
- Apparaatsensor, versies 15.2(1)E, 3.5.0E en hoger
- 1X, MAC-verificatie-omleiding (MAB), sessiebeheer
- Webgebaseerde verificatie
- Automatische proxy
- IP-bronbewaking (IPSG) voor statische hosts

- Flexibele netflow
- Cisco TrustSec (CTS)
- Mediatraining
- HTTP-omleidingen

Functiematrix

Platform	Feature	Standaard ingeschakeld (Start in)	Methode uitschakelen	CLI uitschakelen
Kat 2960/3750 (Cisco IOS)	IPDT	15.2, lid 1, onder e) *	wereldwijde CLI (oudere releases) * per interface	geen ip-apparaat trackir IP-apparaat tracking maximaal 0 ***
Kat 2960/3750 (Cisco IOS)	NMSP	nee	wereldwijde CLI of per-interface CLI	geen nmsp inschakelen nmsp-bijlage onderdruk
Kat 2960/3750 (Cisco IOS)	Apparaatsensor	15.0(1)SE	wereldwijde CLI	geen macro auto monitc
Kat 2960/3750 (Cisco IOS)	ARP-controle	15.2(1)E **	N.v.t.	N.v.t.
Kat 3850	IPDT	alle releases *	per interface *	IP-apparaat tracking maximaal 0 ***
Kat 3850	NMSP	alle releases	per interface	nmsp-bijlage onderdruk
Kat 3850	Apparaatsensor	nee	N.v.t.	N.v.t.
Kat 3850	ARP-controle	alle releases **	N.v.t.	N.v.t.
Kat 4500	IPDT	15.2(1)E / 3.5.0E *	wereldwijde CLI (oudere releases) * per interface	geen ip-apparaat trackir IP-apparaat tracking maximaal 0 ***
Kat 4500	NMSP	nee	wereldwijde CLI of per-interface CLI	geen nmsp inschakelen nmsp-bijlage onderdruk
Kat 4500	Apparaatsensor	15.1(1)SG / 3.3.0SG	wereldwijde CLI	geen macro auto monitc
Kat 4500	ARP-controle	15.2(1)E / 3.5.0E **	N.v.t.	N.v.t.

Functies

- IPDT kan niet wereldwijd worden uitgeschakeld in nieuwere releases, maar IPDT is alleen actief op poorten als er functies zijn waarvoor het nodig is.
- ARP snooping is alleen actief als specifieke functie combinaties het mogelijk maken.
- Als u IPDT op een per-interfacebasis onbruikbaar maakt stopt niet ARP snooping het verhindert IPDT het volgen. Dit is verkrijgbaar bij i3.3.0SE, 15.2(1)E, 3.5.0E en hoger.
- NMSP-onderdrukking per interface is alleen beschikbaar als NMSP wereldwijd is ingeschakeld.

IPDT uitschakelen

Op releases waar IPDT standaard niet is ingeschakeld, kan IPDT globaal worden uitgeschakeld met deze opdracht:

```
Switch(config)#no ip device tracking
```

Op releases waarop IPDT altijd is ingeschakeld, is de vorige opdracht niet beschikbaar of u kunt IPDT niet uitschakelen ('Cisco bug ID CSCuj04986'). In dit geval zijn er verschillende manieren om ervoor te zorgen dat IPDT geen specifieke poort controleert of geen dubbele IP-waarschuwingen genereert.

Voer het ip device tracking probe delay 10 Opdracht

Met deze opdracht kan een switch 10 seconden lang geen sonde verzenden wanneer hij een link UP/flap detecteert, waardoor de mogelijkheid om de sonde te laten versturen wordt geminimaliseerd terwijl de host aan de andere kant van de link dubbele IP-adressen controleert. De RFC specificeert een venster van 10 seconden voor dubbele adresdetectie, dus als u de apparaat-tracking sonde uitstelt, kan het probleem in de meeste gevallen worden opgelost.

Als de switch een ARP-sonde voor de client verstuurt terwijl de host (bijvoorbeeld een Microsoft Windows PC) zich in de fase van Duplicate-Address Detection bevindt, detecteert de host de sonde als een dubbel IP-adres en geeft deze aan de gebruiker een bericht dat op het netwerk een dubbel IP-adres is gevonden. Als de PC geen adres verkrijgt en de gebruiker het adres handmatig moet vrijgeven/vernieuwen, de verbinding moet verbreken en opnieuw verbinding moet maken met het netwerk, of de PC moet opnieuw opstarten om netwerktoegang te krijgen.

Naast de sonde-vertraging, stelt de vertraging zich ook terug wanneer de switch een sonde van PC/host detecteert. Als de sonde bijvoorbeeld is afgeteld tot vijf seconden en een ARP-sonde van de PC/host wordt gedetecteerd, wordt de timer teruggezet op 10 seconden.

Deze configuratie is beschikbaar gesteld via 'Cisco bug ID CSCtn27420'.

Voer het ip device tracking probe use-svi Opdracht

Met deze opdracht kunt u de switch configureren om een niet-RFC-conforme ARP-sonde te verzenden. de IP-bron is niet 0.0.0.0, maar is de Switch Virtual Interface (SVI) in het VLAN waar de host zich bevindt. Microsoft Windows-machines zien de sonde niet meer als een sonde zoals gedefinieerd door RFC 5227 en markeren geen potentiële dubbele IP.

Voer het ip device tracking probe auto-source [fallback Opdracht

Voor klanten die niet beschikken over voorspelbare / controleerbare eindapparaten of voor klanten die veel switches hebben in een L2-functie, is de configuratie van een SVI, die een Layer 3-variabele in het ontwerp introduceert, geen geschikte oplossing. Een verbetering introduceerde, in Versie 15.2(2)E en later, de mogelijkheid om willekeurige toewijzing van een IP adres toe te staan dat niet aan de switch voor gebruik als bronadres in ARP sondes hoeft te behoren die door IPDT worden geproduceerd. Deze verbetering introduceert de kans om het automatische gedrag van het systeem op deze manieren te wijzigen (deze lijst toont hoe het systeem zich automatisch gedraagt nadat elke opdracht wordt gebruikt):

Voer het ip device tracking probe auto-source Opdracht

1. Stel de bron in op VLAN SVI indien aanwezig.
2. Zoek naar een bron/MAC-paar in de IP-hosttabel voor dezelfde subnetverbinding.
3. Verzend de nul IP bron zoals in het standaardgeval.

Voer het ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 Opdracht

1. Stel de bron in op VLAN SVI indien aanwezig.
2. Zoek naar een bron/MAC-paar in de IP-hosttabel voor dezelfde subnetverbinding.
3. Bereken de bron-IP vanaf de bestemming-IP met het geleverde hostbit en -masker.

Voer het ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override Opdracht

1. Stel de bron in op VLAN SVI indien aanwezig.
2. Bereken de bron-IP vanaf de bestemming-IP met het geleverde hostbit en -masker.

Opmerking: Met een overschrijving slaat u de zoekactie voor een item in de tabel over. Als voorbeeld van de vorige berekeningen, veronderstel je probe host 192.168.1.200. Met de masker en host bits die beschikbaar zijn, genereert u een bronadres van 192.168.1.1. Als u test ingang 10.5.5.20, kunt u een ARP-sonde genereren met bronadres 10.5.5.1, enzovoort.

Voer het ip device tracking maximum 0 Opdracht

Deze opdracht schakelt IPDT niet echt uit, maar beperkt wel het aantal getraceerde hosts tot nul. Dit is geen aanbevolen oplossing en deze moet met voorzichtigheid worden gebruikt, omdat deze invloed heeft op alle andere functies die afhankelijk zijn van IPDT, inclusief de poortkanaalconfiguratie zoals beschreven in 'Cisco bug ID CSCun81556'.

Schakel actieve functies uit die IPDT activeren

Sommige functies die IPDT kunnen activeren zijn NMSP, apparaatsensor, dot1x/MAB, WebAuth en IPSG. Deze functies worden niet aanbevolen om ingeschakeld te worden op trunkpoorten. Deze oplossing is gereserveerd voor de moeilijkste of meest complexe situaties, waar ofwel alle oplossingen die voorheen beschikbaar waren niet werkten zoals verwacht, of ze creëerden extra problemen. Dit is echter de enige oplossing die extreme granulariteit toestaat wanneer je IPDT uitschakelt, omdat je alleen de IPDT-gerelateerde functies die problemen veroorzaken kunt uitschakelen en alles onaangetast laat.

In de meest recente Cisco IOS-software, versie 15.2(2)E en hoger, ziet u een uitvoer die vergelijkbaar is met deze:

```
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
```

De twee regels in alle caps aan de onderkant van de output zijn de regels die IPDT gebruiken om te werken. De meeste problemen die ontstaan wanneer u de apparaattracering uitschakelt, kunnen worden vermeden als u de afzonderlijke services die in de interface worden uitgevoerd, uitschakelt.

In eerdere versies van Cisco IOS is deze eenvoudige manier om te weten welke modules zijn ingeschakeld onder een interface nog niet beschikbaar, zodat u door een meer betrokken proces moet gaan om dezelfde resultaten te verkrijgen. U moet **debug ip de interface van het apparatenspoor** aanzetten, die een laag-frequentielogboek is dat in de meeste opstellingen veilig moet zijn. Zorg ervoor dat **debug** van **ip-apparaat** niet wordt ingeschakeld omdat dit, integendeel, de console overspoelt in schaalsituaties.

Zodra debug is, breng een interface terug naar gebrek, en voeg en verwijder dan de dienst IPDT uit de interfaceconfiguratie toe. De resultaten van de debugs vertellen u welke service is ingeschakeld/uitgeschakeld met de opdracht die u gebruikte.

Voorbeeld

```
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)#
```

Wat de output onthult is dat u eigenschap **00000008** toeliet, en dat het nieuwe eigenschapmasker **0000004C** is.

Verwijder nu de configuratie die u zojuist hebt toegevoegd:

```
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)#
```

Zodra u eigenschap **00000008** verwijdert, kunt u het masker van **00000044** zien, dat het originele, standaardmasker moet zijn geweest. Deze waarde van **00000044** wordt verwacht aangezien AIM **0x00000004** is en SM **0x000000040** is, wat samen resulteert in **0x0000044**.

Er zijn verschillende IPDT-services die onder een interface kunnen worden uitgevoerd:

IPT-service	Interface
HOST_TRACK_CLIENT_IP_TOEGANGSRECHTEN	= 0x00000001
HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_BIJLAGE	= 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_DRAADLOOS	= 0x00000080

In het voorbeeld zijn HOST_TRACK_CLIENT_SM (SESSION-MANAGER) en HOST_TRACK_CLIENT_ATTACHMENT (ook bekend als AIM/NMSP) modules geconfigureerd voor IPDT. Om IPDT op deze interface uit te schakelen moet u beide uitschakelen, omdat IPDT ALLEEN uitgeschakeld is als alle functies die het gebruiken ook uitgeschakeld zijn.

Nadat u die functies hebt uitgeschakeld, hebt u een uitvoer die vergelijkbaar is met deze:

```
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:
ßNo active features
------------------------------------------
```

Op deze manier wordt IPDT uitgeschakeld met meer granulariteit.

Hier zijn een paar voorbeelden van opdrachten die worden gebruikt om een aantal van de eerder besproken functies uit te schakelen:

- nmsp-attach-onderdrukking
- geen macro auto monitor

Opmerking: De nieuwste functie moet alleen beschikbaar zijn op platformen die Smart Ports (SmartPort Flash-presentatie) ondersteunen, die worden gebruikt om functies mogelijk te maken op basis van de locatie van een switch in het netwerk en voor massaconfiguratie-implementaties in het netwerk.

Controleer de werking van IPDT

Gebruik deze opdrachten om de IPDT-status op uw apparaat te verifiëren:

- Toon ip apparaat het volgen
  Deze opdracht geeft interfaces weer waar IPDT is ingeschakeld en waar momenteel MAC/IP/interface-associaties worden bijgehouden.
- overzichtelijk IP-apparaat bijhouden
- Deze opdracht schakelt IPDT-gerelateerde vermeldingen uit.

Opmerking: De switch stuurt ARP-sondes naar de hosts die zijn verwijderd. Als een host aanwezig is, reageert deze op de ARP-sonde en voegt de switch een IPDT-vermelding toe

voor de host. U moet ARP sondes vóór het duidelijke bevel IPDT onbruikbaar maken; op die manier zijn alle ARP-vermeldingen verdwenen. Als ARP sondes na het **duidelijke IP apparaat het volgen** bevel worden toegelaten, komen alle ingangen opnieuw terug.

- **foutherstel van IP-apparaat**
  Met deze opdracht kunt u debugs verzamelen om IPDT-activiteit in real time weer te geven.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.