Verifica delle operazioni dei dispositivi IPDT

Sommario

Introduzione

In questo documento viene descritto come verificare le operazioni IPDT (IP Device Tracking) e come disattivare queste azioni.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Gli output di questo documento si basano sulle seguenti versioni software e hardware:

- Cisco WS-C2960X
- Cisco IOS® 15.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica di IPDT

Definizione e utilizzo

L'attività principale di IPDT consiste nel tenere traccia degli host connessi (associazione di MAC address e indirizzi IP). A tale scopo, vengono inviate richieste ARP (Address Resolution Protocol) unicast con un intervallo predefinito di 30 secondi. Queste richieste vengono inviate all'indirizzo MAC dell'host connesso sull'altro lato del collegamento e utilizzano il layer 2 (L2) come origine predefinita per l'indirizzo MAC dell'interfaccia fisica da cui proviene l'ARP e un indirizzo IP mittente di 0.0.0.0, in base alla definizione della sonda ARP riportata nella RFC 5227

Estratto

In questo documento, il termine ARP Probe viene usato per riferirsi a un pacchetto di richiesta ARP, trasmesso sul collegamento locale, con un indirizzo IP di un mittente tutto zero. L'indirizzo hardware del mittente DEVE contenere l'indirizzo hardware dell'interfaccia che invia il pacchetto. Il campo dell'indirizzo IP del mittente DEVE essere impostato su tutti gli zeri per evitare il danneggiamento delle cache ARP in altri host sullo stesso collegamento, nel caso in cui l'indirizzo risulti già utilizzato da un altro host. Il campo dell'indirizzo IP di destinazione DEVE essere impostato sull'indirizzo sondato. Una sonda ARP trasmette sia una domanda (Qualcuno utilizza questo indirizzo?) che una dichiarazione implicita (Questo è l'indirizzo che spero di utilizzare).

Lo scopo di IPDT è che lo switch ottenga e conservi un elenco di dispositivi connessi allo switch tramite un indirizzo IP. La sonda non popola la voce di rilevamento, ma viene semplicemente utilizzata per mantenere la voce nella tabella dopo essere stata appresa tramite una richiesta/risposta ARP dall'host.

L'ispezione ARP di IP viene abilitata automaticamente quando IPDT è attivato. rileva la presenza di nuovi host quando quest'ultimo monitora i pacchetti ARP. Se l'ispezione ARP dinamica è abilitata, vengono utilizzati solo i pacchetti ARP che questa convalida con l'obiettivo di rilevare i nuovi host per la tabella sul monitoraggio dei dispositivi.

Lo snooping DHCP di IP, se abilitato, rileva la presenza o la rimozione di nuovi host quando DHCP assegna o revoca i relativi indirizzi IP. Quando il traffico DHCP viene rilevato su un determinato host, il timer dell'intervallo di probe ARP IPDT viene reimpostato.

IPDT è una funzione che è sempre stata disponibile. Tuttavia, nelle versioni più recenti di Cisco IOS®, le interdipendenze sono abilitate per impostazione predefinita (fare riferimento all'ID bug Cisco CSCuj04986). Questa funzione può essere estremamente utile quando viene utilizzato il

suo database di associazioni di host IP/MAC per compilare l'IP di origine degli Access Control list (ACL) dinamici o per mantenere un'associazione tra un indirizzo IP e un tag del gruppo di sicurezza.

Il probe ARP viene inviato in due circostanze:

- Il collegamento associato a una voce corrente nel database IPDT passa da uno stato DOWN a uno UP e la voce ARP è stata popolata.
- Un collegamento già nello stato UP associato a una voce nel database IPDT ha un intervallo di richiesta scaduto.

Problema

La sonda keepalive inviata dallo switch è un controllo L2. Per questo motivo, dal punto di vista dello switch, gli indirizzi IP utilizzati come origine negli ARP non sono importanti: questa funzione può essere utilizzata su dispositivi senza alcun indirizzo IP configurato, quindi l'origine IP di 0.0.0.0 non è rilevante.

Quando l'host riceve questi messaggi, risponde e popola il campo relativo all'IP di destinazione con l'unico indirizzo IP disponibile nel pacchetto ricevuto, ossia il proprio indirizzo IP. Ciò può causare falsi avvisi relativi a indirizzi IP duplicati, in quanto l'host che risponde considera il proprio indirizzo IP sia come origine che come destinazione del pacchetto. Vedere l'indirizzo IP duplicato 0.0.0.0. Articolo sulla risoluzione dei problemi relativi ai messaggi di errore per ulteriori informazioni sullo scenario di indirizzi IP duplicati.

Stato e funzionamento predefiniti

La configurazione di accensione/spegnimento globale per IPDT è un comportamento legacy che ha causato problemi sul campo in quanto i clienti non erano sempre consapevoli di dover attivare IPDT per il funzionamento di alcune funzionalità. Nelle versioni correnti, IPDT è controllato esclusivamente a livello di interfaccia quando attiva una funzionalità che richiede IPDT.

In queste versioni, IPDT è attivo per impostazione predefinita a livello globale, ovvero non è disponibile alcun comando di configurazione globale:

- Catalyst 2000/3000: 15,2(1)E
- Catalyst 3850: 3.2.0SE
- Catalyst 4k: 15,2(1)E / 3,5.0E

È importante notare che, anche se IPDT è abilitato a livello globale, ciò non implica per forza che monitori attivamente una determinata porta.

Nelle versioni in cui IPDT è sempre attivo e in cui IPDT può essere attivato e disattivato a livello globale quando IPDT è attivato a livello globale, altre funzionalità determinano se IPDT è attivo su un'interfaccia specifica (vedere la sezione Aree funzionalità).

Aree di funzionalità

IPDT e le relative richieste ARP inviate da una determinata interfaccia vengono utilizzati per le seguenti funzioni:

- NMSP (Network Mobility Services Protocol), versioni 3.2.0E, 15.2(1)E, 3.5.0E e successive
- Device Sensor, versioni 15.2(1)E, 3.5.0E e successive
- 1X, MAB (MAC Authentication Bypass), gestore sessioni
- Autenticazione basata sul Web
- Auth-proxy
- IP Source Guard (IPSG) per host statici
- Flexible NetFlow
- CTS (Cisco TrustSec)
- Mediatrace
- Reindirizzamenti HTTP

Matrice

Piattaforma	Funzionalità	Predefinito su (Inizia da)	Disable, metodo	Disabilita CLI
Cat 2960/3750 (Cisco IOS)	IPDT	15.2(1)E *	CLI globale (versioni precedenti) * per interfaccia	nessun rilevamento dei dispositivi ip * massimo rilevamento dispositivo ip 0 ***
Cat 2960/3750 (Cisco IOS)	NMSP	no	CLI globale o CLI per interfaccia	nessuna abilitazione nmsp soppressione allegato nmsp ****
Cat 2960/3750 (Cisco IOS)	Sensore dispositivo	15.0(1)SE	CLI globale	no macro auto monitor
Cat 2960/3750 (Cisco IOS)	Snooping ARP	15.2(1)E **	n/d	n/d
Cat 3850	IPDT	tutte le release *	per interfaccia *	massimo rilevamento dispositivo ip 0 ***
Cat 3850	NMSP	tutte le release	per interfaccia	soppressione allegato

				nmsp
Cat 3850	Sensore dispositivo	no	n/d	n/d
Cat 3850	Snooping ARP	tutte le release **	n/d	n/d
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	CLI globale (versioni precedenti) * per interfaccia	nessun rilevamento dei dispositivi ip * massimo rilevamento dispositivo ip 0 ***
Cat 4500	NMSP	no	CLI globale o CLI per interfaccia	nessuna abilitazione nmsp soppressione allegato nmsp ****
Cat 4500	Sensore dispositivo	15.1(1)SG / 3.3.0SG	CLI globale	no macro auto monitor
Cat 4500	Snooping ARP	15.2(1)E / 3.5.0E **	n/d	n/d

Caratteristiche

- Nelle versioni più recenti, IPDT non può essere disabilitato globalmente, ma è attivo solo sulle porte se sono attive alcune funzionalità che lo richiedono.
- Lo snooping ARP è attivo solo se è possibile utilizzare combinazioni di caratteristiche specifiche.
- Se si disabilita IPDT per singole interfacce, lo snooping ARP non viene interrotto e non viene impedito il rilevamento IPDT. È disponibile da i3.3.0SE, 15.2(1)E, 3.5.0E e versioni successive.
- L'eliminazione NMSP per interfaccia è disponibile solo se NMSP è abilitato globalmente.

Disattivazione di IPDT

Nelle versioni in cui IPDT non è abilitato per impostazione predefinita, può essere disattivato a

livello globale con questo comando:

<#root>

```
Switch(config)#
```

no ip device tracking

Nelle versioni in cui IPDT è sempre attivo, il comando precedente non è disponibile o non consente di disabilitare IPDT (ID bug Cisco CSCuj04986). In questo caso, esistono diversi modi per garantire che IPDT non monitori una porta specifica o non generi avvisi di IP duplicati.

Immissione del comando ip device tracking probe delay 10

Questo comando impedisce a uno switch di inviare una richiesta per dieci secondi quando rileva un collegamento UP/flap, il che riduce al minimo la possibilità di inviare la richiesta mentre l'host dall'altro lato del collegamento controlla gli indirizzi IP duplicati. L'RFC specifica una finestra di 10 secondi per il rilevamento degli indirizzi duplicati, quindi se si ritarda la sonda di rilevamento del dispositivo, il problema può essere risolto nella maggior parte dei casi.

Se lo switch invia una richiesta ARP per il client mentre l'host (ad esempio, un computer Microsoft Windows) è in fase di rilevamento degli indirizzi duplicati, l'host rileva la richiesta come un indirizzo IP duplicato e mostra all'utente un messaggio che indica che è stato trovato un indirizzo IP duplicato sulla rete. Se il PC non ottiene un indirizzo e l'utente deve rilasciare/rinnovare manualmente l'indirizzo, disconnettersi e riconnettersi alla rete o riavviare il PC per ottenere l'accesso alla rete.

Oltre al ritardo della richiesta, il ritardo si reimposta automaticamente quando lo switch rileva una richiesta dal computer/host. Ad esempio, se il timer della richiesta è arrivato a cinque secondi e rileva una richiesta ARP dal computer/host, il timer viene reimpostato a dieci secondi.

Questa configurazione è stata resa disponibile tramite l'ID bug Cisco CSCtn27420.

Immettere il comando IP Device Tracking Probe Use SVI

Con questo comando, è possibile configurare lo switch per inviare una sonda ARP non conforme alla RFC; l'origine IP non è 0.0.0.0, ma è l'interfaccia virtuale dello switch (SVI) nella VLAN in cui risiede l'host. I computer Microsoft Windows non vedono più la richiesta come definita da RFC 5227 e non segnalano un potenziale IP duplicato.

Immissione del comando ip device tracking probe auto-source [fallback <host-ip> <mask>] [override]

Per i clienti che non dispongono di dispositivi terminali prevedibili/controllabili o per coloro che hanno molti switch con un ruolo solo L2, la configurazione di una SVI, che introduce una variabile di layer 3 nel progetto, non è una soluzione adatta. Un miglioramento introdotto nella versione

15.2(2)E e successive, la possibilità di consentire l'assegnazione arbitraria di un indirizzo IP che non deve necessariamente appartenere allo switch per essere utilizzato come indirizzo di origine nelle sonde ARP generate da IPDT. Questo miglioramento consente di modificare il comportamento automatico del sistema in questi modi (questo elenco mostra come il comportamento automatico del sistema dopo l'uso di ogni comando):

Immissione del comando ip device tracking probe auto-source

1. Impostare la sorgente sulla VLAN SVI, se presente.
2. Cercare una coppia di origine/MAC nella tabella di host IP per la stessa subnet.
3. Inviare l'origine IP zero come nello scenario predefinito.

Immissione del comando ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0

1. Impostare la sorgente sulla VLAN SVI, se presente.
2. Cercare una coppia di origine/MAC nella tabella di host IP per la stessa subnet.
3. Calcolare l'IP di origine dall'IP di destinazione con la mask e il bit dell'host forniti.

Immissione del comando ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override

1. Impostare la sorgente sulla VLAN SVI, se presente.
2. Calcolare l'IP di origine dall'IP di destinazione con la mask e il bit dell'host forniti.

> Nota: una sostituzione consente di ignorare la ricerca di una voce nella tabella.

Come esempio dei calcoli precedenti, si supponga di eseguire la sonda dell'host 192.168.1.200. Con la maschera e i bit dell'host forniti, si genera l'indirizzo di origine 192.168.1.1. Se si esegue la sonda della voce 10.5.5.20, è possibile generare una sonda ARP con indirizzo di origine 10.5.5.1 e così via.

Immissione del comando ip device tracking maximum 0

Questo comando non disabilita realmente IPDT, ma limita il numero di host monitorati a zero. Questa non è una soluzione consigliata e deve essere utilizzata con cautela perché influisce su tutte le altre funzionalità che si basano su IPDT, compresa la configurazione dei canali delle porte descritta nell'ID bug Cisco CSCun81556.

Disattivazione delle funzioni attive che abilitano IPDT

Alcune funzionalità che possono attivare IPDT sono NMSP, il sensore dei dispositivi, dot1x/MAB, WebAuth e IPSG. Si consiglia di non abilitare queste funzionalità sulle porte trunk. Questa soluzione è consigliata per le situazioni più difficili o complesse, in cui tutte le soluzioni disponibili in passato non funzionavano come previsto o creavano ulteriori problemi. Questa è, tuttavia, l'unica soluzione che consente la massima granularità quando si disabilita IPDT, perché è possibile disattivare solo le funzioni correlate a IPDT che causano problemi e lasciare tutto il resto inalterato.

Nella versione più recente di Cisco IOS, 15.2(2)E e versioni successive, viene visualizzato un output simile al seguente:

<#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
```

Le due righe scritte tutte in maiuscolo nella parte inferiore dell'output sono quelle che utilizzano IPDT per funzionare. La maggior parte dei problemi creati quando si disabilita il monitoraggio del dispositivo può essere evitata se si disattivano i singoli servizi in esecuzione nell'interfaccia.

Nelle versioni precedenti di Cisco IOS, questo metodo semplice per sapere quali moduli sono abilitati tramite un'interfaccia non è ancora disponibile, quindi è necessario eseguire un processo più complesso per ottenere gli stessi risultati. È necessario attivare debug ip device track interface, un file di registro a bassa frequenza che nella maggior parte delle configurazioni deve essere sicuro. Fare attenzione a non attivare debug ip device tracking all perché questo, al contrario, satura la console in situazioni di scalabilità.

Una volta attivato il debug, ripristinare l'interfaccia predefinita, poi aggiungere e rimuovere un servizio IPDT dalla configurazione dell'interfaccia. I risultati dei debug indicano quale servizio è stato abilitato/disabilitato con il comando utilizzato.

Esempio

<#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)#
```

L'output rivela che avete abilitato la feature 00000008 e che la nuova maschera è 0000004C.

A questo punto, rimuovere la configurazione appena aggiunta:

<#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)#
```

Una volta rimossa la funzione 00000008, è possibile vedere la mask 00000044, che deve essere stata quella originale e predefinita. Questo valore di 00000044 è previsto poiché AIM è 0x00000004 e SM è 0x00000040, che insieme generano 0x00000044.

Esistono diversi servizi IPDT che possono essere eseguiti in un'interfaccia:

Servizio IPT	Interfaccia
HOST_TRACK_CLIENT_IP_ADMISSIONS	= 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

Nell'esempio, i moduli HOST_TRACK_CLIENT_SM (SESSION-MANAGER) e HOST_TRACK_CLIENT_ATTACHMENT (noto anche come AIM/NMSP) sono configurati per IPDT. Per disattivare IPDT su questa interfaccia, è necessario disabilitarli entrambi, poiché IPDT risulta disattivato SOLO quando lo sono anche tutte le funzioni che lo utilizzano.

Dopo aver disabilitato queste funzioni, si ottiene un output simile al seguente:

<#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
-------------------------------------------
```

In questo modo, IPDT viene disabilitato con maggiore granularità.

Ecco alcuni esempi di comandi utilizzati per disabilitare alcune delle funzioni descritte in precedenza:

- nmsp attach suppress
- no macro auto monitor

Nota: la funzionalità più recente deve essere disponibile solo sulle piattaforme che supportano le Smart Port, utilizzate per abilitare le funzionalità in base alla posizione di uno switch nella rete e per le distribuzioni di configurazione di massa nella rete.

Verifica del funzionamento di IPDT

Utilizzare questi comandi per verificare lo stato di IPDT sul dispositivo:

- show ip device tracking
  Questo comando visualizza le interfacce dove IPDT è abilitato e dove sono attualmente tracciate le associazioni MAC/IP/interfaccia.
- clear ip device tracking
- Questo comando cancella le voci relative a IPDT.

Nota: lo switch invia sonde ARP agli host rimossi. Se è presente un host, risponde alla richiesta ARP e lo switch aggiunge una voce IPDT per l'host. È necessario disattivare le sonde ARP prima del comando clear IPDT; in questo modo, tutte le voci ARP non saranno più presenti. Se le richieste ARP sono abilitate dopo il comando clear ip device tracking, tutte le voci vengono nuovamente ripristinate.

- debug ip device tracking
  Questo comando consente di raccogliere i debug per visualizzare l'attività IPDT in tempo reale.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).