Überprüfung des Betriebs des IPDT-Geräts

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie IP Device Tracking (IPDT)-Vorgänge überprüft und diese Aktionen deaktiviert werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. Die Ergebnisse in diesem Dokument basieren jedoch auf den folgenden Software- und

Hardwareversionen:

- Cisco WS-C2960X
- Cisco IOS® 15.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

IPDT - Übersicht

Definition und Verwendung

Die wichtigste IPDT-Aufgabe besteht darin, den Überblick über verbundene Hosts zu behalten (Zuordnung von MAC- und IP-Adresse). Dazu sendet es Unicast Address Resolution Protocol (ARP)-Tests mit einem Standardintervall von 30 Sekunden. Diese Tests werden an die MAC-Adresse des Hosts gesendet, der auf der anderen Seite der Verbindung angeschlossen ist, und verwenden Layer 2 (L2) als Standardquelle für die MAC-Adresse der physischen Schnittstelle, von der der ARP ausgeht, und die Absender-IP-Adresse 0.0.0.0, basierend auf der ARP-Sondendefinition in RFC 5227.

Auszug

In diesem Dokument bezieht sich der Begriff "ARP-Anfrage" auf ein ARP-Anforderungspaket, das über den lokalen Link übertragen wird und eine "Absender-IP-Adresse" hat, die bei Null liegt. Die Hardwareadresse des Absenders MUSS die Hardwareadresse der Schnittstelle enthalten, die das Paket sendet. Das Feld 'Absender-IP-Adresse' MUSS auf alle Nullen gesetzt werden, um Beschädigungen von ARP-Caches auf anderen Hosts auf demselben Link zu vermeiden, falls sich herausstellt, dass die Adresse bereits von einem anderen Host verwendet wird. Das Feld 'Ziel-IP-Adresse' MUSS auf die Adresse gesetzt werden, die überprüft wird. Eine ARP-Anfrage vermittelt sowohl eine Frage (*Nutzt jemand diese Adresse?*) als auch eine implizite Aussage (*Dies ist die Adresse, die ich nutzen möchte.*).

Der Zweck von IPDT besteht darin, dass der Switch eine Liste der Geräte abruft und verwaltet, die über eine IP-Adresse mit dem Switch verbunden sind. Die Probe füllt den Verfolgungseintrag nicht aus; Sie wird einfach verwendet, um den Eintrag in der Tabelle beizubehalten, nachdem er über eine ARP-Anfrage/Antwort vom Host abgerufen wurde.

IP ARP Inspection wird automatisch aktiviert, wenn IPDT aktiviert ist. erkennt neue Hosts bei der Überwachung von ARP-Paketen. Wenn die dynamische ARP-Inspektion aktiviert ist, werden nur die validierten ARP-Pakete verwendet, um neue Hosts für die Tabelle "Device Tracking" (Geräteverfolgung) zu erkennen.

Wenn IP DHCP Snooping aktiviert ist, erkennt es das Vorhandensein oder Entfernen neuer Hosts, wenn DHCP ihre IP-Adressen zuweist oder widerruft. Wenn DHCP-Datenverkehr für einen bestimmten Host erkannt wird, wird der IPDT ARP-Intervall-Timer zurückgesetzt.

IPDT ist eine Funktion, die schon immer verfügbar war. Bei neueren Cisco IOS®-Versionen sind die Abhängigkeiten jedoch standardmäßig aktiviert (siehe "Cisco Bug ID CSCuj04986"). Es kann äußerst nützlich sein, wenn die eigene Datenbank mit IP/MAC-Hosts-Verknüpfungen verwendet wird, um die Quell-IP dynamischer Zugriffskontrolllisten (ACLs) auszufüllen oder die Bindung einer

IP-Adresse an ein Sicherheitsgruppen-Tag aufrechtzuerhalten.

Die ARP-Probe wird unter zwei Umständen gesendet:

- Der Link, der einem aktuellen Eintrag in der IPDT-Datenbank zugeordnet ist, wechselt vom Status "DOWN" in den Status "UP", und der ARP-Eintrag wurde ausgefüllt.
- Ein Link, der sich bereits im Status UP befindet und einem Eintrag in der IPDT-Datenbank zugeordnet ist, hat ein abgelaufenes Probe-Intervall.

Problem

Die vom Switch gesendete Keepalive-Anfrage ist eine L2-Prüfung. Aus Switch-Sicht sind daher die in den ARPs als Quelle verwendeten IP-Adressen nicht wichtig: Diese Funktion kann auf Geräten ohne konfigurierte IP-Adresse verwendet werden, sodass die IP-Quelle 0.0.0.0 nicht relevant ist.

Wenn der Host diese Nachrichten empfängt, antwortet er zurück und füllt das Ziel-IP-Feld mit der einzigen im empfangenen Paket verfügbaren IP-Adresse, nämlich der eigenen IP-Adresse, auf. Dies kann Warnungen über falsche doppelte IP-Adressen verursachen, da der antwortende Host seine eigene IP-Adresse sowohl als Quelle als auch als Ziel des Pakets sieht. Weitere Informationen zum Szenario mit doppelten IP-Adressen finden Sie im Artikel Duplicate IP Address 0.0.0.0. Error Message Troubleshoot.

Standardstatus und -betrieb

Die globale On/Off-Konfiguration für IPDT ist ein älteres Verhalten, das Probleme vor Ort verursachte, da Kunden nicht immer wussten, dass sie IPDT aktivieren mussten, damit bestimmte Funktionen funktionieren. In aktuellen Versionen wird IPDT nur auf Schnittstellenebene gesteuert, wenn eine Funktion aktiviert wird, für die IPDT erforderlich ist.

IPDT ist in diesen Versionen standardmäßig global aktiviert. d. h. kein globaler Konfigurationsbefehl aufgrund von 'Cisco Bug ID CSCua85383':

- Catalyst 2000/3000: 15.2(1)E
- Catalyst 3850: 3.2.0SE
- Catalyst 4000: 15.2(1)E/3.5.0E

Beachten Sie, dass selbst wenn IPDT global aktiviert ist, dies nicht unbedingt bedeutet, dass IPDT einen bestimmten Port aktiv überwacht.

Bei Versionen, bei denen IPDT immer aktiv ist und bei denen IPDT global ein- und ausgeschaltet werden kann, wenn IPDT global aktiviert ist, bestimmen andere Funktionen, ob es auf einer bestimmten Schnittstelle aktiv ist (siehe Abschnitt Funktionsbereiche).

Funktionsbereiche

IPDT und seine ARP-Tests, die von einer bestimmten Schnittstelle gesendet werden, werden für folgende Funktionen verwendet:

- Network Mobility Services Protocol (NMSP), Versionen 3.2.0E, 15.2(1)E, 3.5.0E und höher
- Gerätesensor, Versionen 15.2(1)E, 3.5.0E und höher

- 1X, MAC Authentication Bypass (MAB), Sitzungsmanager
- Webbasierte Authentifizierung
- Authentifizierungsproxy
- IP Source Guard (IPSG) für statische Hosts
- Flexible NetFlow
- Cisco TrustSec (CTS)
- Medienüberwachung
- HTTP-Umleitungen

Funktionsübersicht

Plattform	Funktion	Standard am (Start in)	Disable-Methode	CLI deaktivieren
Cat 2960/3750 (Cisco IOS)	IPDT	15.2(1)E *	globale Kommandozeile (ältere Versionen) * pro Schnittstelle	keine IP-Geräteverfolgu ip device tracking maxin ***
Cat. 2960/3750 (Cisco IOS)	NMSP	nein	globale CLI oder Kommandozeile pro Schnittstelle	Keine NMS-Aktivierung nmsp attachment unterdrücken ****
Cat 2960/3750 (Cisco IOS)	Gerätesenso r	15.0(1)SE	Globale CLI	Keine automatische Makroüberwachung
Cat 2960/3750 (Cisco IOS)	ARP-Snooping	15.2(1)E **	–	–
Cat 3850	IPDT	Alle Versionen *	pro Schnittstelle *	ip device tracking maxin ***
Cat 3850	NMSP	alle Versionen	pro Schnittstelle	NMSP-Anlage unterdrüc
Cat 3850	Gerätesenso r	nein	–	–
Cat 3850	ARP-Snooping	Alle Versionen **	–	–
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	globale Kommandozeile (ältere Versionen) * pro Schnittstelle	keine IP-Geräteverfolgu ip device tracking maxin ***
Cat 4500	NMSP	nein	globale CLI oder Kommandozeile pro Schnittstelle	Keine NMS-Aktivierung nmsp attachment unterdrücken ****
Cat 4500	Gerätesenso r	15.1(1)SG/3.3.0SG	Globale CLI	Keine automatische Makroüberwachung
Cat 4500	ARP-Snooping	15.2(1)E/3.5.0E **	–	–

Funktionen

- IPDT kann in neueren Versionen nicht global deaktiviert werden, aber IPDT ist nur an Ports aktiv, wenn Funktionen aktiv sind, die dies erfordern.
- ARP-Snooping ist nur aktiv, wenn bestimmte Funktionskombinationen es aktivieren.
- Wenn Sie IPDT auf Schnittstellenbasis deaktivieren, wird ARP-Snooping nicht gestoppt,

sondern die IPDT-Verfolgung wird verhindert. Verfügbar ab i3.3.0SE, 15.2(1)E, 3.5.0E.
- NMSP-Unterdrückung pro Schnittstelle ist nur verfügbar, wenn NMSP global aktiviert ist.

IPDT deaktivieren

In Versionen, in denen IPDT nicht standardmäßig aktiviert ist, kann IPDT mit dem folgenden Befehl global deaktiviert werden:

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

Bei Versionen, bei denen IPDT immer aktiviert ist, ist der vorherige Befehl nicht verfügbar, oder Sie können IPDT nicht deaktivieren ('Cisco bug ID CSCuj04986'). In diesem Fall gibt es mehrere Möglichkeiten sicherzustellen, dass IPDT einen bestimmten Port nicht überwacht oder keine doppelten IP-Warnmeldungen generiert.

Geben Sie ip device tracking probe delay 10 Command

Mit diesem Befehl kann ein Switch 10 Sekunden lang keinen Prüfpunkt senden, wenn er eine Verbindung UP/Flap erkennt. Dadurch wird die Möglichkeit minimiert, den Prüfpunkt senden zu lassen, während der Host auf der anderen Seite der Verbindung nach doppelten IP-Adressen sucht. Der RFC gibt ein 10-Sekunden-Fenster für die Erkennung doppelter Adressen an. Wenn Sie also die Geräteüberwachungsprüfung verzögern, kann das Problem in den meisten Fällen gelöst werden.

Wenn der Switch einen ARP-Prüfpunkt für den Client sendet, während sich der Host (z. B. ein Microsoft Windows-PC) in der Phase der Erkennung doppelter Adressen befindet, erkennt der Host den Prüfpunkt als doppelte IP-Adresse und sendet dem Benutzer die Meldung, dass eine doppelte IP-Adresse im Netzwerk gefunden wurde. Wenn der PC keine Adresse erhält und der Benutzer die Adresse manuell freigeben/erneuern muss, trennen Sie die Verbindung zum Netzwerk, und stellen Sie erneut eine Verbindung mit dem Netzwerk her, oder starten Sie den PC neu, um Netzwerkzugriff zu erhalten.

Zusätzlich zur "Probe-Delay"-Verzögerung setzt sich die Verzögerung auch zurück, wenn der Switch eine Probe vom PC/Host erkennt. Wenn der Zeitgeber beispielsweise bis zu fünf Sekunden gezählt hat und eine ARP-Anfrage vom PC/Host erfasst, wird er auf 10 Sekunden zurückgesetzt.

Diese Konfiguration wurde über 'Cisco Bug ID CSCtn27420' bereitgestellt.

Geben Sie ip device tracking probe use-svi Command

Mit diesem Befehl können Sie den Switch so konfigurieren, dass eine nicht RFC-konforme ARP-Anfrage gesendet wird. Die IP-Quelle ist nicht 0.0.0.0, sondern die Switch Virtual Interface (SVI) im VLAN, in dem sich der Host befindet. Microsoft Windows-Computer sehen den Prüfpunkt nicht mehr als einen Prüfpunkt, wie in RFC 5227 definiert, und markieren keine potenziell doppelte IP.

Geben Sie ip device tracking probe auto-source [fallback Command

Für Kunden, die über keine vorhersehbaren/steuerbaren Endgeräte verfügen, oder für Kunden mit vielen Switches in einer reinen L2-Rolle ist die Konfiguration einer SVI, die eine Layer-3-Variable in das Design einführt, keine geeignete Lösung. Eine Erweiterung führte in Version 15.2(2)E und

höher die Möglichkeit ein, eine beliebige Zuweisung einer IP-Adresse zu erlauben, die nicht zum Switch gehören muss, um als Quelladresse in von IPDT generierten ARP-Tests verwendet zu werden. Diese Erweiterung bietet die Möglichkeit, das automatische Verhalten des Systems auf diese Weise zu ändern (diese Liste zeigt, wie sich das System nach jedem Befehl automatisch verhält):

Geben Sie ip device tracking probe auto-source Command

1. Legen Sie die Quelle auf VLAN SVI fest, falls vorhanden.
2. Suchen Sie in der IP-Hosttabelle nach einem Quell-/MAC-Paar für dasselbe Subnetz.
3. Senden Sie die Null-IP-Quelle wie im Standardfall.

Geben Sie ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 Command

1. Legen Sie die Quelle auf VLAN SVI fest, falls vorhanden.
2. Suchen Sie in der IP-Hosttabelle nach einem Quell-/MAC-Paar für dasselbe Subnetz.
3. Berechnen Sie die Quell-IP aus der Ziel-IP mit dem bereitgestellten Host-Bit und der bereitgestellten Maske.

Geben Sie ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override Command

1. Legen Sie die Quelle auf VLAN SVI fest, falls vorhanden.
2. Berechnen Sie die Quell-IP aus der Ziel-IP mit dem bereitgestellten Host-Bit und der bereitgestellten Maske.

   Anmerkung: Bei einer Überschreibung überspringen Sie die Suche nach einem Eintrag in der Tabelle.

Nehmen Sie als Beispiel für die vorherigen Berechnungen an, Sie testen den Host 192.168.1.200. Mit den bereitgestellten Masken- und Host-Bits generieren Sie die Quelladresse 192.168.1.1. Wenn Sie den Eintrag 10.5.5.20 testen, können Sie einen ARP-Test mit der Quelladresse 10.5.5.1, usw.

Geben Sie ip device tracking maximum 0 Command

Mit diesem Befehl wird IPDT nicht wirklich deaktiviert, aber die Anzahl der verfolgten Hosts wird auf Null beschränkt. Dies ist keine empfohlene Lösung, und sie muss mit Vorsicht verwendet werden, da sie alle anderen Funktionen betrifft, die auf IPDT basieren. Dazu gehört auch die Port-Channel-Konfiguration, wie in "Cisco Bug ID CSCun81556" beschrieben.

Deaktivieren aktiver Funktionen, die IPDT auslösen

Zu den Funktionen, die IPDT auslösen können, gehören NMSP, Gerätesensor, dot1x/MAB, WebAuth und IPSG. Diese Funktionen sollten nicht auf Trunk-Ports aktiviert werden. Diese

Lösung ist für die schwierigsten oder komplexesten Situationen reserviert, in denen entweder alle zuvor verfügbaren Lösungen nicht wie erwartet funktionierten oder zusätzliche Probleme auftraten. Dies ist jedoch die einzige Lösung, die eine extreme Detailgenauigkeit ermöglicht, wenn Sie IPDT deaktivieren, da Sie nur die IPDT-bezogenen Funktionen deaktivieren können, die Probleme verursachen, und alles andere davon unberührt lassen.

In der neuesten Version von Cisco IOS, Version 15.2(2)E und höher, sehen Sie eine Ausgabe ähnlich dieser:

```
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
```

Die beiden Zeilen in allen Großbuchstaben am unteren Rand der Ausgabe sind diejenigen, die IPDT verwenden, um zu arbeiten. Die meisten Probleme, die beim Deaktivieren der Geräteverfolgung entstehen, können vermieden werden, wenn Sie die einzelnen Dienste deaktivieren, die auf der Schnittstelle ausgeführt werden.

In früheren Versionen von Cisco IOS ist diese einfache Möglichkeit, zu erfahren, welche Module unter einer Schnittstelle aktiviert sind, noch nicht verfügbar. Sie müssen daher einen aufwändigeren Prozess durchlaufen, um die gleichen Ergebnisse zu erzielen. Sie müssen die Nachverfolgungsschnittstelle für das Debugging-IP-Gerät aktivieren. Dies ist ein Protokoll mit niedriger Frequenz, das in den meisten Setups sicher sein muss. Achten Sie darauf, debug ip device tracking nicht zu aktivieren, da dies im Gegenteil die Konsole in Skalierungssituationen überflutet.

Sobald das Debugging aktiviert ist, setzen Sie eine Schnittstelle wieder auf die Standardeinstellung zurück, und fügen Sie dann einen IPDT-Dienst zur Schnittstellenkonfiguration hinzu bzw. entfernen Sie diesen. Die Ergebnisse der Fehlersuche zeigen Ihnen, welcher Dienst mit dem von Ihnen verwendeten Befehl aktiviert/deaktiviert wurde.

Beispiel

```
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)#
```

Die Ausgabe zeigt, dass Sie die Funktion 00000008 aktiviert haben und dass die neue Funktionsmaske 0000004C lautet.

Entfernen Sie nun die Konfiguration, die Sie gerade hinzugefügt haben:

```
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)#
```

Sobald Sie das Feature **00000008** entfernen, können Sie die **0000044** Maske sehen, die die ursprüngliche Standardmaske sein muss. Dieser Wert von **00000044** wird erwartet, da AIM **0 x 0000004** und SM 0 **x 00000040** ist, was zusammen 0 **x 0000004 ergibt.** 4.

Es gibt mehrere IPDT-Dienste, die unter einer Schnittstelle ausgeführt werden können:

IPT-Service	Schnittstelle
HOST_TRACK_CLIENT_IP_ADMISSIONS	= 0x00000001
HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_ATTACHING	= 0x00000004
HOST_TRACK_CLIENT_TRACK_HOST_UPTO_MAX	= 0x00000008
HOST_TRACK_CLIENT_RSVP	= 0x00000010
HOST_TRACK_CLIENT_CTS	= 0x00000020
HOST_SPUR_CLIENT_SM	= 0x00000040
HOST_TRACK_CLIENT_WIRELESS	= 0x00000080

Im Beispiel werden die Module HOST_TRACK_CLIENT_SM (SESSION-MANAGER) und HOST_TRACK_CLIENT_ATTACHMENT (auch als AIM/NMSP bezeichnet) für IPDT konfiguriert. Um IPDT auf dieser Schnittstelle zu deaktivieren, müssen Sie beide deaktivieren, da IPDT NUR dann deaktiviert ist, wenn alle Funktionen, die es verwenden, ebenfalls deaktiviert sind.

Nachdem Sie diese Funktionen deaktiviert haben, haben Sie eine Ausgabe wie diese:

```
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
------------------------------------------
```

Auf diese Weise wird IPDT detaillierter deaktiviert.

Nachfolgend finden Sie einige Beispiele für Befehle, mit denen einige der zuvor besprochenen Funktionen deaktiviert werden können:

- **Unterdrückung von NMSP-Anhängen**
- **Keine automatische Makroüberwachung**

Anmerkung: Die neueste Funktion darf nur auf Plattformen verfügbar sein, die SmartPorts unterstützen (SmartPort Flash-Präsentation). Diese werden verwendet, um Funktionen je nach Standort eines Switches im Netzwerk und für Massenkonfigurationen im gesamten Netzwerk zu aktivieren.

IPDT-Betrieb überprüfen

Verwenden Sie die folgenden Befehle, um den IPDT-Status auf Ihrem Gerät zu überprüfen:

- **IP-Geräteverfolgung anzeigen**
  Mit diesem Befehl werden Schnittstellen angezeigt, auf denen IPDT aktiviert ist und auf denen derzeit MAC/IP/Schnittstellenzuordnungen nachverfolgt werden.
- **Clear IP Device Tracking**
- Dieser Befehl löscht IPDT-bezogene Einträge.

Anmerkung: Der Switch sendet ARP-Tests an die entfernten Hosts. Wenn ein Host vorhanden ist, antwortet er auf den ARP-Test, und der Switch fügt einen IPDT-Eintrag für den Host hinzu. Sie müssen die ARP-Tests vor dem Befehl clear IPDT deaktivieren. auf diese Weise sind alle ARP-Einträge weg. Wenn ARP-Tests nach dem Befehl **clear ip device tracking** aktiviert werden, werden alle Einträge erneut angezeigt.

- **debug ip device tracking**
  Mit diesem Befehl können Sie Debugs sammeln, um IPDT-Aktivitäten in Echtzeit anzuzeigen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.