Vérifier le fonctionnement des périphériques IPDT

Table des matières

Introduction

Ce document décrit comment vérifier les opérations IPDT (IP Device Tracking) et comment désactiver ces actions.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les résultats de ce document sont basés sur les versions logicielles et matérielles suivantes :

- Cisco WS-C2960X
- Cisco IOS® 15.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation de IPDT

Définition et utilisation

La tâche principale de l'IPDT consiste à effectuer le suivi des hôtes connectés (association d'adresses MAC et IP). Pour ce faire, il envoie des sondes ARP (Address Resolution Protocol) monodiffusion avec un intervalle par défaut de 30 secondes. Ces sondes sont envoyées à l'adresse MAC de l'hôte connecté de l'autre côté de la liaison et utilisent la couche 2 (L2) comme source par défaut vers laquelle l'adresse MAC de l'interface physique à partir de laquelle le protocole ARP sort et une adresse IP d'expéditeur de 0.0.0.0, sur la base de la définition de la sonde ARP indiquée dans la RFC 5227

Extrait

Dans ce document, le terme Sonde ARP est utilisé pour désigner un paquet de requête ARP, diffusé sur la liaison locale, avec une adresse IP d'expéditeur ne contenant que des zéros. L'adresse matérielle de l'expéditeur DOIT contenir l'adresse matérielle de l'interface qui envoie le paquet. Le champ de l'adresse IP de l'expéditeur DOIT être défini sur tous les zéros pour éviter la corruption des caches ARP dans d'autres hôtes, sur la même liaison, dans le cas où l'adresse s'avère être déjà utilisée par un autre hôte. Le champ d'adresse IP cible DOIT être défini sur l'adresse analysée. Une sonde ARP transmet à la fois une question (Est-ce que quelqu'un utilise cette adresse ?) et une instruction implicite (Il s'agit de l'adresse que j'espère utiliser.)

L'objectif de l'IPDT est que le commutateur obtienne et tienne une liste des périphériques connectés au commutateur via une adresse IP. La sonde ne remplit pas l'entrée de suivi ; elle est simplement utilisée afin de maintenir l'entrée dans la table après qu'elle a été apprise par le biais d'une requête/réponse ARP de l'hôte.

L'inspection IP ARP est activée automatiquement lorsque l'IPDT est activé. Il détecte la présence de nouveaux hôtes lorsqu'il surveille les paquets ARP. Si l'inspection ARP dynamique est activée, seuls les paquets ARP qu'elle valide sont utilisés afin de détecter de nouveaux hôtes pour la table de suivi des périphériques.

La surveillance DHCP IP, si elle est activée, détecte la présence ou la suppression de nouveaux hôtes lorsque DHCP attribue ou révoque leurs adresses IP. Lorsque le trafic DHCP est détecté pour un hôte donné, le compteur d'intervalle d'analyse ARP IPDT est réinitialisé.

L'IPDT est une fonctionnalité qui a toujours été disponible. Cependant, dans les versions plus récentes de Cisco IOS®, ses interdépendances sont activées par défaut (voir ID de bogue Cisco CSCuj04986). Il peut être extrêmement utile lorsque sa base de données d'associations d'hôtes IP/MAC est utilisée pour remplir l'adresse IP source des listes de contrôle d'accès (ACL) dynamiques ou pour maintenir une liaison d'une adresse IP à une balise de groupe de sécurité.

La sonde ARP est envoyée dans deux cas :

- Le lien associé à une entrée en cours dans la base de données IPDT passe d'un état DOWN à un état UP, et l'entrée ARP a été remplie.
- Une liaison déjà à l'état UP associée à une entrée dans la base de données IPDT a un intervalle d'exploration expiré.

Problème

La sonde keepalive envoyée par le commutateur est un contrôle de couche 2. Par conséquent, du point de vue du commutateur, les adresses IP utilisées comme source dans les ARP ne sont pas importantes : cette fonctionnalité peut être utilisée sur des périphériques sans aucune adresse IP configurée, de sorte que la source IP 0.0.0.0 n'est pas pertinente.

Lorsque l'hôte reçoit ces messages, il répond et renseigne le champ IP de destination avec la seule adresse IP disponible dans le paquet reçu, qui est sa propre adresse IP. Cela peut entraîner de fausses alertes d'adresse IP dupliquée, car l'hôte qui répond voit sa propre adresse IP à la fois comme source et comme destination du paquet ; reportez-vous à la section Adresse IP dupliquée 0.0.0.0. Message d'erreur Article Dépannage pour plus d'informations sur le scénario d'adresse IP dupliquée.

État et fonctionnement par défaut

La configuration globale on/off pour IPDT est un comportement hérité qui a causé des problèmes sur le terrain car les clients n'étaient pas toujours conscients qu'ils devaient activer IPDT pour que certaines fonctionnalités fonctionnent. Dans les versions actuelles, l'IPDT est uniquement contrôlé au niveau de l'interface lorsqu'il active une fonctionnalité qui nécessite l'IPDT.

IPDT est activé globalement par défaut dans ces versions ; c'est-à-dire, aucune commande de configuration globale :

- Catalyst 2000/3000 : 15.2(1)E
- Catalyst 3850 : 3.2.0SE
- Catalyst 4k : 15.2(1)E / 3.5.0E

Il est important de noter que, même si l'IPDT est activé globalement, cela n'implique pas nécessairement que l'IPDT surveille activement un port donné.

Dans les versions où IPDT est toujours activé et où IPDT peut être activé/désactivé globalement lorsque IPDT est activé globalement, d'autres fonctionnalités déterminent en fait s'il est actif sur une interface spécifique (voir la section Zones de fonctionnalité).

Domaines de fonctionnalité

IPDT et ses sondes ARP envoyées à partir d'une interface donnée sont utilisées pour les fonctions suivantes :

- Network Mobility Services Protocol (NMSP), versions 3.2.0E, 15.2(1)E, 3.5.0E et ultérieures
- Capteur de périphérique, versions 15.2(1)E, 3.5.0E et ultérieures
- 1X, MAC Authentication Bypass (MAB), gestionnaire de session
- Authentification basée sur le Web
- Auth-proxy
- IP Source Guard (IPSG) pour les hôtes statiques
- Flexibilité du flux réseau
- Cisco TrustSec (CTS)
- suivi de support
- Redirections HTTP

Matrice de fonctions

Plateforme	Fonctionnalité	Par défaut le (début entrant)	Disable, méthode	Désactiver CLI
Cat 2960/3750 (Cisco IOS)	IPDT	15.2(1)E *	interface de ligne de commande globale (anciennes versions) * par interface	no ip device tracking * ip device tracking maximum 0 ***
Cat 2960/3750 (Cisco IOS)	NMSP	non	CLI globale ou CLI par interface	no nmsp enable nmsp attachment suppress ****
Cat 2960/3750 (Cisco IOS)	Capteur de périphérique	15.0(1)SE	ILC globale	no macro auto monitor
Cat 2960/3750 (Cisco IOS)	Surveillance ARP	15,2(1)E **	S/O	S/O
Cat 3850	IPDT	toutes les versions *	par interface *	ip device tracking maximum 0 ***

Cat 3850	NMSP	toutes les versions	par interface	nmsp attachment suppress
Cat 3850	Capteur de périphérique	non	S/O	S/O
Cat 3850	Surveillance ARP	toutes les versions **	S/O	S/O
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	interface de ligne de commande globale (anciennes versions) * par interface	no ip device tracking * ip device tracking maximum 0 ***
Cat 4500	NMSP	non	CLI globale ou CLI par interface	no nmsp enable nmsp attachment suppress ****
Cat 4500	Capteur de périphérique	15.1(1)SG / 3.3.0SG	ILC globale	no macro auto monitor
Cat 4500	Surveillance ARP	15.2(1)E / 3.5.0E **	S/O	S/O

Caractéristiques

- IPDT ne peut pas être désactivé globalement dans les versions plus récentes, mais IPDT n'est actif que sur les ports, si les fonctionnalités qui le nécessitent sont actives.
- La surveillance ARP est active uniquement si des combinaisons de fonctions spécifiques l'activent.
- Si vous désactivez IPDT sur une base par interface, il n'arrête pas la surveillance ARP, il empêche le suivi IPDT. Disponible à partir des versions i3.3.0SE, 15.2(1)E, 3.5.0E et ultérieures.
- La suppression NMSP par interface n'est disponible que si NMSP est activé globalement.

Désactiver IPDT

Dans les versions où IPDT n'est pas activé par défaut, IPDT peut être désactivé globalement avec cette commande :

<#root>

```
Switch(config)#
```

no ip device tracking

Dans les versions où IPDT est toujours activé, la commande précédente n'est pas disponible, ou elle ne vous permet pas de désactiver IPDT (ID de bogue Cisco CSCuj04986). Dans ce cas, il existe plusieurs façons de s'assurer que l'IPDT ne surveille pas un port spécifique ou qu'il ne génère pas d'alertes IP en double.

Entrez la commande IP Device Tracking Probe Delay 10.

Cette commande ne permet pas à un commutateur d'envoyer une sonde pendant 10 secondes lorsqu'il détecte une liaison UP/flap, ce qui minimise la possibilité d'envoyer la sonde pendant que l'hôte de l'autre côté de la liaison recherche des adresses IP en double. La RFC spécifie une fenêtre de 10 secondes pour la détection des adresses en double, donc si vous retardez la sonde de suivi de périphérique, le problème peut être résolu dans la plupart des cas.

Si le commutateur envoie une sonde ARP pour le client alors que l'hôte (par exemple, un PC Microsoft Windows) est dans sa phase de détection d'adresse dupliquée, l'hôte détecte la sonde comme adresse IP dupliquée et présente à l'utilisateur un message indiquant qu'une adresse IP dupliquée a été trouvée sur le réseau. Si le PC n'obtient pas d'adresse, et que l'utilisateur doit libérer/renouveler manuellement l'adresse, se déconnecter et se reconnecter au réseau, ou redémarrer le PC afin d'obtenir l'accès au réseau.

En plus de la fonction probe-delay, le délai se réinitialise également lorsque le commutateur détecte une sonde du PC/hôte. Par exemple, si le compteur d'analyse a décompté jusqu'à cinq secondes et détecte une sonde ARP à partir du PC/hôte, le compteur revient à 10 secondes.

Cette configuration a été mise à disposition via l'ID de bogue Cisco CSCtn27420.

Entrez la commande IP Device Tracking Probe Use SVI

Avec cette commande, vous pouvez configurer le commutateur afin d'envoyer une sonde ARP non conforme à la RFC ; la source IP n'est pas 0.0.0.0, mais c'est l'interface virtuelle de commutateur (SVI) dans le VLAN où réside l'hôte. Les ordinateurs Microsoft Windows ne voient plus la sonde comme une sonde telle que définie par la RFC 5227 et ne signalent pas une adresse IP potentiellement dupliquée.

Entrez la commande IP Device Tracking Probe Auto-Source [fallback <host-ip> <mask>] [override]

Pour les clients qui n'ont pas de périphériques finaux prévisibles/contrôlables, ou pour ceux qui ont de nombreux commutateurs dans un rôle de couche 2 uniquement, la configuration d'une interface SVI, qui introduit une variable de couche 3 dans la conception, n'est pas une solution appropriée. Une amélioration introduite dans la version 15.2(2)E et ultérieure, la possibilité d'autoriser l'attribution arbitraire d'une adresse IP qui n'a pas besoin d'appartenir au commutateur pour être utilisée comme adresse source dans les sondes ARP générées par IPDT. Cette amélioration introduit la possibilité de modifier le comportement automatique du système de la manière suivante (cette liste montre comment le système se comporte automatiquement après l'utilisation de chaque commande) :

Entrez la commande IP Device Tracking Probe Auto-Source

1. Définissez la source sur VLAN SVI, le cas échéant.
2. Recherchez une paire source/MAC dans la table d’hôtes IP pour le même sous-réseau.
3. Envoyez la source IP zéro comme dans le cas par défaut.

Entrez la commande IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0

1. Définissez la source sur VLAN SVI, le cas échéant.
2. Recherchez une paire source/MAC dans la table d’hôtes IP pour le même sous-réseau.
3. Calculez l’adresse IP source à partir de l’adresse IP de destination avec le bit et le masque d’hôte fournis.

Entrez la commande IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Override

1. Définissez la source sur VLAN SVI, le cas échéant.
2. Calculez l’adresse IP source à partir de l’adresse IP de destination avec le bit et le masque d’hôte fournis.

> Remarque : si vous remplacez une entrée, vous ignorez la recherche d'une entrée dans la table.

Comme exemple des calculs précédents, supposons que vous sondez l’hôte 192.168.1.200. Avec les bits de masque et d’hôte fournis, vous générez l’adresse source 192.168.1.1. Si vous sondez l'entrée 10.5.5.20, vous pouvez générer une sonde ARP avec l'adresse source 10.5.5.1, etc.

Entrez la commande IP Device Tracking Maximum 0

Cette commande ne désactive pas vraiment IPDT, mais elle limite le nombre d'hôtes suivis à zéro. Cette solution n'est pas recommandée et doit être utilisée avec prudence car elle affecte toutes les autres fonctionnalités qui reposent sur IPDT, qui inclut la configuration port-channels comme décrit dans l'ID de bogue Cisco CSCun81556.

Désactiver les fonctionnalités actives qui déclenchent IPDT

Parmi les fonctionnalités pouvant déclencher IPDT, citons NMSP, le capteur de périphérique, dot1x/MAB, WebAuth et IPSG. Il est déconseillé d'activer ces fonctionnalités sur les ports agrégés. Cette solution est réservée aux situations les plus difficiles ou les plus complexes, dans lesquelles soit toutes les solutions précédemment disponibles ne fonctionnaient pas comme prévu, soit elles créaient des problèmes supplémentaires. Il s'agit toutefois de la seule solution qui permet une granularité extrême lorsque vous désactivez l'IPDT, car vous ne pouvez désactiver que les fonctionnalités liées à l'IPDT qui causent des problèmes et ne touchent à rien d'autre.

Dans la version la plus récente de Cisco IOS, Versions15.2(2)E et ultérieures, vous voyez un résultat similaire à celui-ci :

<#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
```

Les deux lignes de toutes les majuscules en bas de la sortie sont celles qui utilisent IPDT pour fonctionner. La plupart des problèmes créés lorsque vous désactivez le suivi des périphériques peuvent être évités si vous désactivez les services uniques qui s'exécutent dans l'interface.

Dans les versions antérieures de Cisco IOS, cette façon simple de savoir quels modules sont activés sous une interface n'est pas encore disponible, de sorte que vous devez passer par un processus plus impliqué afin d'obtenir les mêmes résultats. Vous devez activer debug ip device track interface, qui est un journal basse fréquence qui doit être sûr dans la plupart des configurations. Veillez à ne pas activer la commande debug ip device tracking all car cela, au contraire, inonde la console dans des situations d'évolutivité.

Une fois le débogage activé, rétablissez la valeur par défaut d'une interface, puis ajoutez et supprimez un service IPDT de la configuration d'interface. Les résultats des débogages vous indiquent quel service a été activé/désactivé avec la commande que vous avez utilisée.

Exemple

<#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)#
```

Le résultat indique que vous avez activé la fonctionnalité 00000008 et que le nouveau masque de fonctionnalité est 0000004C.

Supprimez maintenant la configuration que vous venez d'ajouter :

<#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)#
```

Une fois la fonction 00000008 supprimée, vous pouvez voir le masque 00000044, qui doit avoir été le masque d'origine par défaut. Cette valeur de 00000044 est attendue, car AIM est 0x00000004 et SM est 0x00000040, ce qui donne 0x00000044.

Plusieurs services IPDT peuvent être exécutés sous une interface :

Service IPT	Interface

ADMISSIONS_IP_CLIENT_PISTE_HÔTE	= 0x00000001
HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_ATTACHMENT	= 0x00000004
HÔTE_SUIVI_CLIENT_SUIVI_HÔTE_JUSQU'À_MAX	= 0x00000008
HOST_TRACK_CLIENT_RSVP	= 0x00000010
HOST_TRACK_CLIENT_CTS	= 0x00000020
HÔTE_SUIVI_CLIENT_SM	= 0x00000040
HOST_TRACK_CLIENT_WIRELESS	= 0x00000080

Dans l'exemple, les modules HOST_TRACK_CLIENT_SM (SESSION-MANAGER) et HOST_TRACK_CLIENT_ATTACHMENT (également appelés AIM/NMSP) sont configurés pour IPDT. Pour désactiver IPDT sur cette interface, vous devez désactiver les deux, car IPDT est désactivé UNIQUEMENT lorsque toutes les fonctions qui l'utilisent sont également désactivées.

Après avoir désactivé ces fonctionnalités, vous obtenez un résultat similaire à celui-ci :

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

De cette façon, IPDT est désactivé avec plus de granularité.

Voici quelques exemples de commandes utilisées afin de désactiver certaines des fonctions discutées précédemment :

- nmsp attach suppress
- no macro auto monitor

Remarque : la dernière fonctionnalité doit être disponible uniquement sur les plates-formes prenant en charge les ports intelligents, qui sont utilisés pour activer des fonctionnalités en fonction de l'emplacement d'un commutateur sur le réseau et pour les déploiements de configuration en masse sur le réseau.

Vérifier le fonctionnement IPDT

Utilisez ces commandes afin de vérifier l'état IPDT sur votre périphérique :

- show ip device tracking
  Cette commande affiche les interfaces où IPDT est activé et où les associations MAC/IP/interface sont actuellement suivies.
- clear ip device tracking
- Cette commande efface les entrées associées à IPDT.

Remarque : le commutateur envoie des sondes ARP aux hôtes qui ont été supprimés. Si un hôte est présent, il répond à la sonde ARP et le commutateur ajoute une entrée IPDT pour l'hôte. Vous devez désactiver les sondes ARP avant la commande clear IPDT ; de cette façon, toutes les entrées ARP ont disparu. Si les sondes ARP sont activées après la commande clear ip device tracking, toutes les entrées reviennent.

- debug ip device tracking
  Cette commande vous permet de collecter des débogages afin d'afficher l'activité IPDT en temps réel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.