Périphérique IP dépistant l'aperçu (IPDT)

Contenu

Introduction

Le document décrit le périphérique IP dépistant (IPDT) et comment le désactiver et vérifier son exécution.

Aperçu IPDT

Définition et utilisation

La tâche principale IPDT est de maintenir les hôtes connectés (association de MAC et d'adresse IP). Afin de faire ceci, il envoie des sondes de Protocole ARP (Address Resolution Protocol) d'unicast avec un intervalle par défaut de 30 secondes ; ces sondes sont envoyées à l'adresse MAC de l'hôte connecté de l'autre côté du lien, et d'une couche 2 (L2) d'utilisation comme source par défaut l'adresse MAC de l'interface physique hors de laquelle l'ARP va et une adresse IP d'expéditeur de 0.0.0.0, basée sur la définition de sonde d'ARP répertoriée dans RFC 5227 extrait ici :

Dans ce document, la « sonde d'ARP » du terme est utilisée pour se rapporter à un paquet de demandes d'ARP, a annoncé sur le lien local, avec des toutes-zéro « adresses IP d'expéditeur. « L'adresse de matériel d'expéditeur » DOIT contenir l'adresse de matériel de l'interface envoyant le paquet. « Le champ des adresses IP d'expéditeur DOIT être placé à tous les zéros, pour éviter de polluer des caches d'ARP dans d'autres hôtes sur le même lien dans le cas où l'adresse s'avère être déjà en service par un autre hôte. « Le champ des adresses IP de cible DOIT être placé à l'adresse étant sondée. Une sonde d'ARP donne une question est-ce que (« n'importe qui utilise cette adresse ? ") et une déclaration implicite (« c'est l'espoir de l'adresse I à use.").

Le but d'IPDT est pour que le commutateur obtienne et pour met à jour une liste de périphériques qui sont connectés au commutateur par l'intermédiaire d'une adresse IP. La sonde ne remplit pas entrée de cheminement ; il est simplement utilisé afin de mettre à jour l'entrée dans la table après qu'on l'apprenne par une demande/réponse d'ARP de l'hôte.

L'inspection ARP IP est activée automatiquement quand IPDT est activé ; il détecte la présence de nouveaux hôtes quand il surveille des paquets d'ARP. Si l'inspection dynamique d'ARP est activée, seulement les paquets d'ARP qu'elle valide sont utilisés afin de détecter de nouveaux hôtes pour le périphérique dépistant la table.

L'ip dhcp snooping, si activé, détecte la présence ou la suppression de nouveaux hôtes quand le DHCP assigne ou retire leurs adresses IP.

IPDT est une caractéristique qui a toujours été disponible. Cependant, sur un Cisco IOS® plus récent libère, ses interdépendances sont activés par défaut (voir l'ID de bogue Cisco CSCuj04986). Il peut être extrêmement utile quand sa base de données des associations d'hôtes IP/MAC est utilisée afin de remplir source ip de Listes de contrôle d'accès (ACL) dynamique, ou mettre à jour une attache d'une adresse IP à une balise de groupe de sécurité.

La sonde d'ARP est envoyée au-dessous de deux circonstances :

- Le lien associé avec une entrée en cours dans la base de données IPDT se déplace d'un BAS à un état HAUT, et l'entrée d'ARP a été remplie.

- Un lien déjà dans le déclarer HAUT qui est associé avec une entrée dans la base de données IPDT a un intervalle expiré de sonde.

Problème connu

La sonde de « keepalive » envoyée par le commutateur est un contrôle L2. En tant que tels du point de vue du commutateur, les adresses IP utilisées comme source in les ARPs ne sont pas importantes : cette caractéristique peut être utilisée sur des périphériques sans l'adresse IP configurée du tout, ainsi la source IP de 0.0.0.0 n'est pas appropriée.

Quand l'hôte reçoit ce des messages, il répond de retour et remplit champ IP de destination avec la seule adresse IP disponible dans le paquet reçu, qui est sa propre adresse IP. Ceci peut entraîner des alertes fausses d'adresse IP en double, parce que l'hôte qui répond voit sa propre adresse IP comme source et destination du paquet ; référez-vous à l'adresse IP en double 0.0.0.0. Le message d'erreur dépannent l'article pour plus d'informations sur le scénario d'adresse IP en double.

État par défaut et exécution

Il est important de noter que, même si IPDT est activé globalement, cela n'implique pas nécessairement qu'IPDT surveille activement un port donné. Sur des releases où IPDT est toujours en fonction et où IPDT peut être off/on globalement basculé, quand IPDT est activé globalement, d'autres caractéristiques déterminent réellement s'il est en activité sur une interface spécifique (voyez la section de régions de fonctionnalité).

Régions de fonctionnalité

IPDT et ses sondes d'ARP envoyés hors d'une interface donnée sont utilisés pour ces caractéristiques :

- Services de mobilité Protocol (NMSP) de réseau, versions 3.2.0E, 15.2(1)E, 3.5.0E et plus tard
- Capteur de périphérique, versions 15.2(1)E, 3.5.0E et plus tard
- 1X, dérivation d'authentification MAC (MAB), gestionnaire de session
- Authentification basée sur le WEB
- Proxy d'authentification
- Passerelle de Services IP (IPSG) pour les hôtes statiques
- Technologie Flexible NetFlow
- Cisco TrustSec (CTS)
- Suivi de medias
- Le HTTP réoriente

Débronchement IPDT

Sur des releases où IPDT n'est pas activé par défaut, IPDT peut être arrêté globalement avec cette commande :

```
# no ip device tracking
```

Sur des releases où IPDT est toujours en fonction, la commande précédente n'est pas disponible ou elle ne te permet pas de désactiver IPDT (ID de bogue Cisco CSCuj04986). Dans ce cas, il y a plusieurs manières de s'assurer qu'IPDT ne fait pas surveille un port spécifique ou il ne génère pas des alertes d'IP en double.

Sélectionnez la commande de cheminement du retard 10 de sonde de périphérique d'IP

Cette commande ne permet pas à un commutateur pour envoyer une sonde pendant 10 secondes où elle détecte un lien UP/flap, qui réduit la possibilité pour avoir la sonde envoyée tandis que l'hôte de l'autre côté du lien vérifie les adresses IP en double. Le RFC spécifie une fenêtre de 10 secondes pour la détection d'adresse en double, ainsi si vous retardez la sonde de périphérique-cheminement, le problème peut être résolu dans la plupart des cas.

Si le commutateur envoie une sonde d'ARP pour le client tandis que l'hôte (par exemple, un PC de Microsoft Windows) a lieu dans sa phase de détection d'adresse en double, l'hôte détecte la sonde comme adresse IP en double et présente l'utilisateur avec un message qu'une adresse IP en double a été trouvée sur le réseau. Le PC ne pourrait pas obtenir une adresse, et l'utilisateur doit manuellement libérer/renouvelle l'adresse, la déconnecte et rebranche au réseau, ou

redémarre le PC afin de gagner l'accès au réseau.

En plus du sonde-retard, le retard se remet à l'état initial également quand le commutateur détecte une sonde du PC/host. Par exemple, si le temporisateur de sonde a compté vers le bas à cinq secondes et détecte une sonde d'ARP du PC/host, les remises de temporisateur de nouveau à 10 secondes.

Cette configuration a été faite à l'ID de bogue Cisco traversant disponible CSCtn27420.

Écrivez l'utilisation-svi de cheminement de sonde de périphérique d'IP. Commande

Avec cette commande, vous pouvez configurer le commutateur afin d'envoyer à un non-RFC la sonde conforme d'ARP ; la source IP ne sera pas 0.0.0.0, mais ce sera Switch Virtual Interface (SVI) dans le VLAN où l'hôte réside. Les ordinateurs de Microsoft Windows ne voient plus la sonde comme sonde comme définie par RFC 5227 et ne signalent pas un IP en double potentiel.

Écrivez l'automatique-source de cheminement de sonde de périphérique d'IP [<mask> de <host-ip> de retour] [dépassement] commande

Pour les clients qui n'ont pas périphériques prévisibles/contrôlables d'extrémité ou pour ceux qui ont beaucoup de Commutateurs dans un rôle L2-only, la configuration d'un SVI, qui introduit une variable de la couche 3 dans la conception, n'est pas une solution appropriée. Une amélioration a introduit, dans la version 15.2(2)E et ultérieures, la possibilité pour permettre l'attribution arbitraire d'un IP address qui n'a pas besoin d'appartenir au commutateur pour l'usage car l'adresse de source dans des sondes d'ARP générées par IPDT. Cette amélioration introduit l'occasion de modifier le comportement automatique du système de ces manières (cette liste affiche comment le système se comporte automatiquement après que chaque commande soit utilisée) :

Sélectionnez la commande de cheminement d'automatique-source de sonde de périphérique d'IP

1. Placez la source à VLAN SVI si présent.
2. Recherchez une paire source/MAC dans la table d'hôte IP pour le même sous-réseau.
3. Envoyez la source IP zéro comme dans le cas par défaut.

Sélectionnez la commande de cheminement de 0.0.0.1 255.255.255.0 de retour d'automatique-source de sonde de périphérique d'IP

1. Placez la source à VLAN SVI si présent.
2. Recherchez une paire source/MAC dans la table d'hôte IP pour le même sous-réseau.
3. Calculez le source ip de l'IP de destination avec le bit d'hôte et le masquez fourni.

Sélectionnez la commande de cheminement de priorité de 0.0.0.1 255.255.255.0 de retour d'automatique-source de sonde de périphérique d'IP

1. Placez la source à VLAN SVI si présent.

2. Calculez le source ip de l'IP de destination avec le bit d'hôte et le masquez fourni.

Remarque: Un dépassement vous incite à ignorer le rechercher une entrée dans la table. Comme un exemple des calculs précédents, assumez-vous hôte 192.168.1.200 de sonde. Les bits de masque et d'hôte étant fourni, vous générez une adresse source de 192.168.1.1.

Si vous sondez l'entrée 10.5.5.20, vous génèreriez une sonde d'ARP avec l'adresse source 10.5.5.1, et ainsi de suite.

Entrez dans l'ip device tracking maximum 0 commandes

Cette commande ne désactive pas vraiment IPDT, mais elle limite le nombre d'hôtes dépistés à zéro. Ce n'est pas une solution recommandée et il devrait être utilisé avec prudence, parce qu'il affecte toutes les autres caractéristiques qui se fondent sur IPDT, qui inclut la configuration de Ports canalisés comme décrit dans l'ID de bogue Cisco CSCun81556.

Arrêtez les caractéristiques actives qui déclenchent IPDT

Quelques caractéristiques qui pourraient déclencher IPDT incluent NMSP, capteur de périphérique, dot1x/MAB, WebAuth, et IPSG. Cette solution est réservée pour le plus difficile ou les situations complexes, où l'un ou l'autre de toutes les solutions précédemment disponibles n'ont pas fonctionné comme prévu, ou elles ont créé des problèmes supplémentaires. C'est, cependant, la seule solution qui permet la finesse extrême quand vous désactivez IPDT, parce que vous pouvez arrêter seulement les caractéristiques liées IPDT qui posent des problèmes et laissent tout d'autre inchangé.

Dans le Cisco IOS le plus récent, Versions15.2(2)E et plus tard, vous voyez un résultat semblable à ceci :

```
Switch#show ip device tracking interface gig 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 dans des tous les CAPS au bas de la sortie sont ceux qui emploient IPDT afin de fonctionner. La plupart des problèmes créés quand vous désactivez le cheminement de périphérique peuvent être évitées si vous désactivez les services simples ce passage dans l'interface.

Dans les versions antérieures du Cisco IOS, de cette façon « facile » de connaître quels modules sont activés sous une interface n'est pas disponible encore, ainsi vous doit passer par un processus plus impliqué afin d'obtenir les mêmes résultats. Vous devez s'activer **mettez au point le track interface de périphérique d'IP**, qui est un log basse fréquence qui devrait être sûr dans la plupart des installations. Faites attention à ne pas s'activer **mettent au point le périphérique d'IP**

dépistant tous parce que ceci, au contraire, inonde la console dans des situations d'échelle.

Une fois le débogage est allumé, apporte une interface de nouveau au par défaut, et puis ajoute et enlève un service IPDT de la configuration d'interface. Les résultats du met au point te disent quel service a été activer/avec la commande que vous avez utilisée.

Voici un exemple :

```
Switch(config)#int gig 1/0/9
Switch(config-if)#ip device track max 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)#
```

Ce que la sortie indique est que vous avez activé la caractéristique **00000008**, et que de la nouvelle le masque caractéristique est **0000004C**.

Maintenant, retirez la configuration que vous avez juste ajoutée :

```
Switch(config-if)#no ip device track max 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 que vous retirez la caractéristique **00000008**, vous pouvez voir le masque **00000044**, qui doit avoir été l'original, masque par défaut. Cette valeur de **00000044** est prévue puisqu'AIM est **0x00000004** et SM est **0x00000040**, qui ont ensemble comme conséquence **0x00000044**.

Il y a plusieurs services IPDT qui peuvent fonctionner sous une interface :

Service IPDT	Interface
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

Dans l'exemple, des modules HOST_TRACK_CLIENT_SM (SESSION-MANAGER) et HOST_TRACK_CLIENT_ATTACHMENT (également connu sous le nom d'AIM/NMSP) sont configurés pour IPDT. Afin d'arrêter IPDT sur cette interface, vous devez désactiver chacun des deux, parce qu'IPDT est désactivé SEULEMENT quand toutes les fonctions qui l'utilisent sont aussi bien désactivées.

Après que vous désactiviez ces configurations, vous avez un résultat semblable à ceci :

```
Switch(config-if)#do show ip dev trac int gig 1/0/9
-------------------------------------------
```

```
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled IPDT is disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IP Device Tracking Enabled Features:
? No active features
-----------------------------------------
```

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

Voici un certain exemple des commandes utilisées afin de désactiver certaines des fonctions discutées précédemment :

- **l'attache de nmsp suppriment**
- **aucun macro moniteur automatique**

  Remarque: La dernière caractéristique devrait être disponible seulement sur les Plateformes qui prennent en charge les ports intelligents (présentation instantanée de SmartPort), qui sont utilisés afin d'activer des caractéristiques et des configurations basées sur l'emplacement d'un commutateur dans le réseau et pour des déploiements de masse de configuration à travers le réseau.

Vérifiez l'exécution IPDT

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

- **show ip device tracking…**

  Cette commande affiche des interfaces où IPDT est activé et où des associations MAC/IP/interface sont actuellement dépistées.

- **clear ip device tracking…**

  Cette commande efface les entrées liées IPDT.

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

- **mettez au point le cheminement de périphérique d'IP…**

  Cette commande te permet pour collecter met au point afin d'afficher l'activité IPDT en temps réel.