Commande cable source-verify et sécurité d'adresse IP

Contenu

Introduction

Cisco a mis en oeuvre des améliorations au sein des produits CMTS (Cable Modem Termination System) de Cisco qui empêchent certains types d'attaques par déni de service basées sur l'usurpation d'adresse IP et le vol d'adresse IP dans les systèmes câblés DOCSIS (Data-over-Cable Service Interface Specifications). Le Guide de référence des commandes du câble Cisco CMTS décrit la suite de commandes **cable source-verify** qui font partie de ces améliorations de sécurité des adresses IP.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Environnement DOCSIS non protégé

Un domaine MAC (Media Access Control) DOCSIS est de nature similaire à un segment Ethernet. S'ils ne sont pas protégés, les utilisateurs du segment sont vulnérables à de nombreux types d'attaques par déni de service basées sur l'adressage de couche 2 et de couche 3. En outre, il est possible que les utilisateurs souffrent d'un niveau de service dégradé en raison d'une mauvaise configuration de l'adressage sur l'équipement d'un autre utilisateur. Voici quelques exemples :

- Configuration des adresses IP en double sur différents noeuds.
- Configuration des adresses MAC dupliquées sur différents noeuds.
- L'utilisation non autorisée d'adresses IP statiques plutôt que d'adresses IP attribuées au protocole DHCP (Dynamic Host Configuration Protocol).
- Utilisation non autorisée de différents numéros de réseau dans un segment.
- Configuration incorrecte des noeuds finaux pour répondre aux requêtes ARP au nom d'une partie du sous-réseau IP du segment.

Bien que ces types de problèmes soient faciles à contrôler et à atténuer dans un environnement de réseau local Ethernet en suivant et déconnectant physiquement les équipements incriminés, de tels problèmes dans les réseaux DOCSIS peuvent être plus difficiles à isoler, résoudre et prévenir en raison de la taille potentiellement importante du réseau. En outre, les utilisateurs finaux qui contrôlent et configurent l'équipement client (CPE) peuvent ne pas avoir l'avantage d'une équipe d'assistance informatique locale pour s'assurer que leurs stations de travail et leurs PC ne sont pas configurés de manière intentionnelle ou non.

Base de données CMTS CPE

La suite de produits CMTS Cisco gère une base de données interne dynamique des adresses IP et MAC CPE connectées. La base de données CPE contient également des détails sur les modems câble correspondants auxquels ces périphériques CPE appartiennent.

Une vue partielle de la base de données CPE correspondant à un modem câble particulier peut être affichée en exécutant la commande masquée CMTS **show interface cable X/Y modem Z**. Ici, X est le numéro de carte de ligne, Y est le numéro de port en aval et Z est l'identificateur de service (SID) du modem câble. Z peut être défini sur 0 pour afficher les détails de tous les modems câble et CPE sur une interface en aval particulière. Voir l'exemple ci-dessous d'un résultat type généré par cette commande.

```
CMTS# show interface cable 3/0 modem 0
SID   Priv bits  Type      State     IP address    method    MAC address
1     00         host      unknown   192.168.1.77  static    000C.422c.54d0
1     00         modem     up        10.1.1.30     dhcp      0001.9659.4447
2     00         host      unknown   192.168.1.90  dhcp      00a1.52c9.75ad
2     00         modem     up        10.1.1.44     dhcp      0090.9607.3831
```

Remarque : Comme cette commande est masquée, elle peut être modifiée et n'est pas garantie d'être disponible dans toutes les versions du logiciel Cisco IOS®.

Dans l'exemple ci-dessus, la colonne de méthode de l'hôte avec l'adresse IP 192.168.1.90 est répertoriée sous le nom dhcp. Cela signifie que le CMTS a appris sur cet hôte en observant les transactions DHCP entre l'hôte et le serveur DHCP du fournisseur de services.

L'hôte dont l'adresse IP est 192.168.1.77 est répertorié avec la méthode static. Cela signifie que le CMTS n'a pas appris d'abord de cet hôte via une transaction DHCP entre ce périphérique et un serveur DHCP. Au lieu de cela, le CMTS a d'abord vu d'autres types de trafic IP en provenance de cet hôte. Ce trafic pouvait être des paquets de navigation Web, de messagerie électronique ou de « ping ».

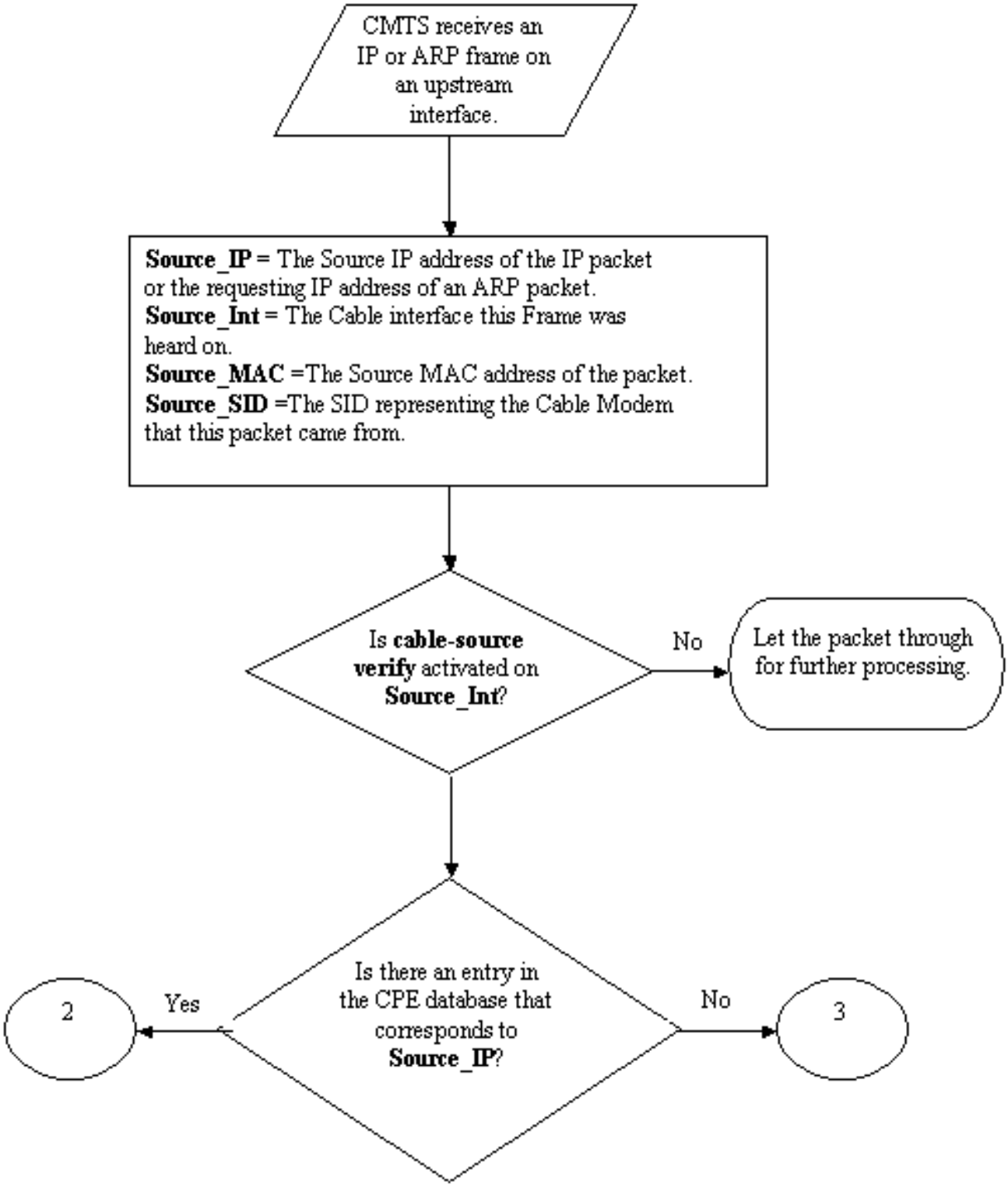
Bien qu'il puisse sembler que 192.168.1.77 a été configuré avec une adresse IP statique, il se peut que cet hôte ait en fait acquis un bail DHCP, mais le CMTS a peut-être été redémarré depuis l'événement et par conséquent il ne se souvient pas de la transaction.

La base de données CPE est normalement renseignée par les informations de collecte CMTS des transactions DHCP entre les périphériques CPE et le serveur DHCP du fournisseur de services. En outre, le CMTS peut écouter d’autres trafics IP provenant de périphériques CPE pour déterminer quelles adresses IP et MAC CPE appartiennent à quels modems câble.

La commande Cable Source-Verify

Cisco a mis en oeuvre la commande cable interface source-verify [dhcp]. Cette commande entraîne le CMTS à utiliser la base de données CPE pour vérifier la validité des paquets IP que le CMTS reçoit sur ses interfaces câblées et permet au CMTS de prendre des décisions intelligentes quant à leur transmission ou non.

Le diagramme ci-dessous montre le traitement supplémentaire qu'un paquet IP reçu sur une interface de câble doit subir avant d'être autorisé à passer par le CMTS.



Organigramme 1

L'organigramme commence par la réception d'un paquet par un port en amont sur le CMTS et se termine par l'autorisation de poursuivre le traitement du paquet ou par l'abandon du paquet.

Exemple 1 : scénario avec des adresses IP en double

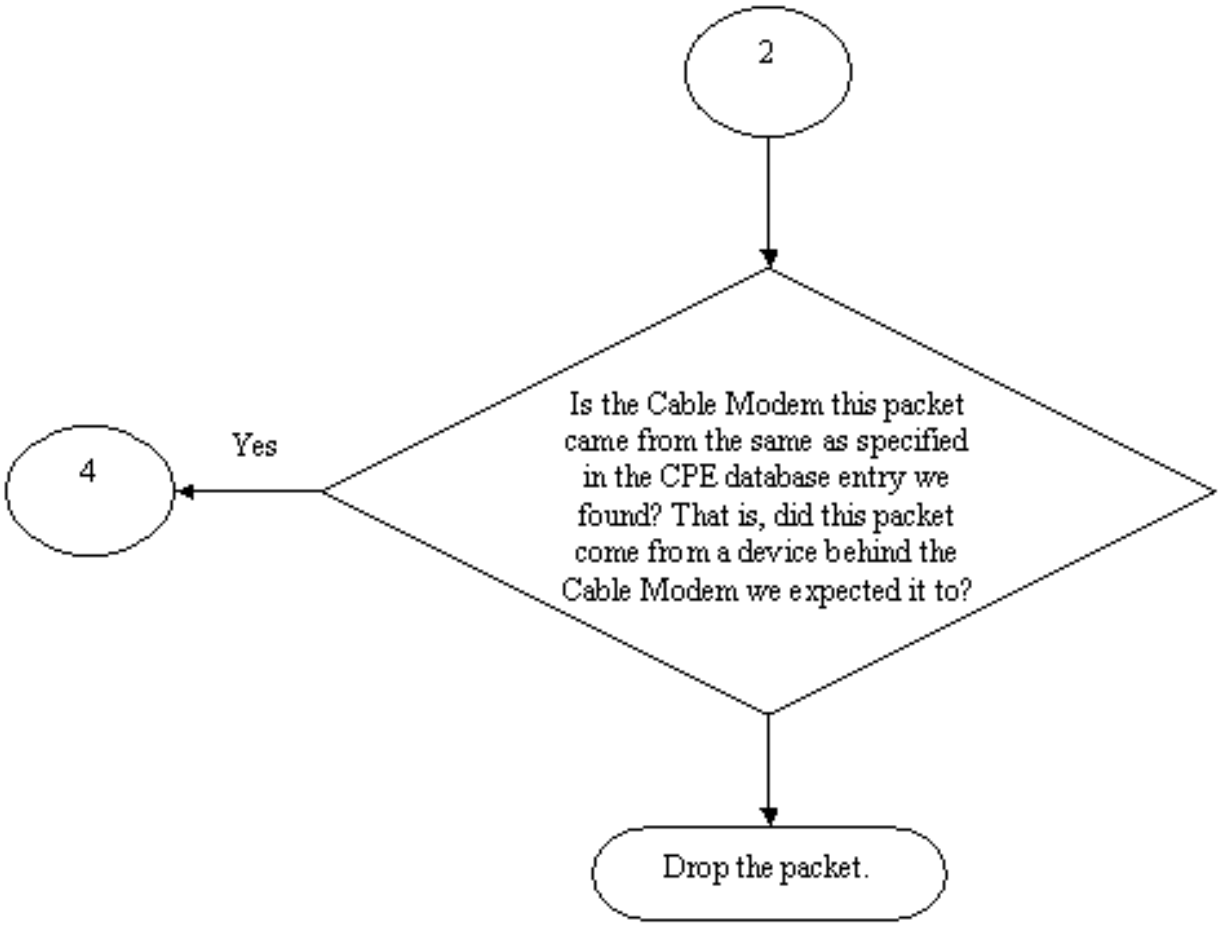
Le premier scénario de déni de service que nous allons aborder est la situation impliquant des adresses IP en double. Disons que le client A est connecté à son fournisseur de services et a obtenu un bail DHCP valide pour son PC. L'adresse IP que le client A a obtenue sera appelée X.

Quelque temps après l'acquisition de son bail DHCP par A, le client B décide de configurer son PC avec une adresse IP statique qui se trouve être identique à celle actuellement utilisée par l'équipement du client A. Les informations de la base de données CPE relatives à l'adresse IP X changeraient en fonction du périphérique CPE qui a envoyé une requête ARP pour le compte de X pour la dernière fois.

Dans un réseau DOCSIS non protégé, le client B peut être en mesure de convaincre le routeur de tronçon suivant (dans la plupart des cas, le CMTS) qu'il a le droit d'utiliser l'adresse IP X en envoyant simplement une requête ARP au nom de X au CMTS ou au routeur de tronçon suivant. Cela empêcherait le trafic du fournisseur de services d'être transféré au client A.

En activant la vérification de la source du câble, le CMTS pourrait voir que les paquets IP et ARP pour l'adresse IP X provenaient du mauvais modem câble et, par conséquent, ces paquets seraient abandonnés, voir Organigramme 2. Cela inclut tous les paquets IP avec l'adresse source X et les requêtes ARP pour le compte de X. Les journaux CMTS afficheraient un message suivant :

%UBR7200-3-BADIPSOURCE : Câble d'interface 3/0, paquet IP provenant d'une source non valide. IP=192.168.1.10, MAC=001.422c.54d0, SID prévu=10, SID réel=11



Organigramme 2

Àl'aide de ces informations, les deux clients seraient identifiés et le modem câble avec l'adresse IP dupliquée connectée peut être désactivé.

Exemple 2 - Scénario avec des adresses IP en double - Utilisation d'une adresse IP qui n'est pas encore utilisée

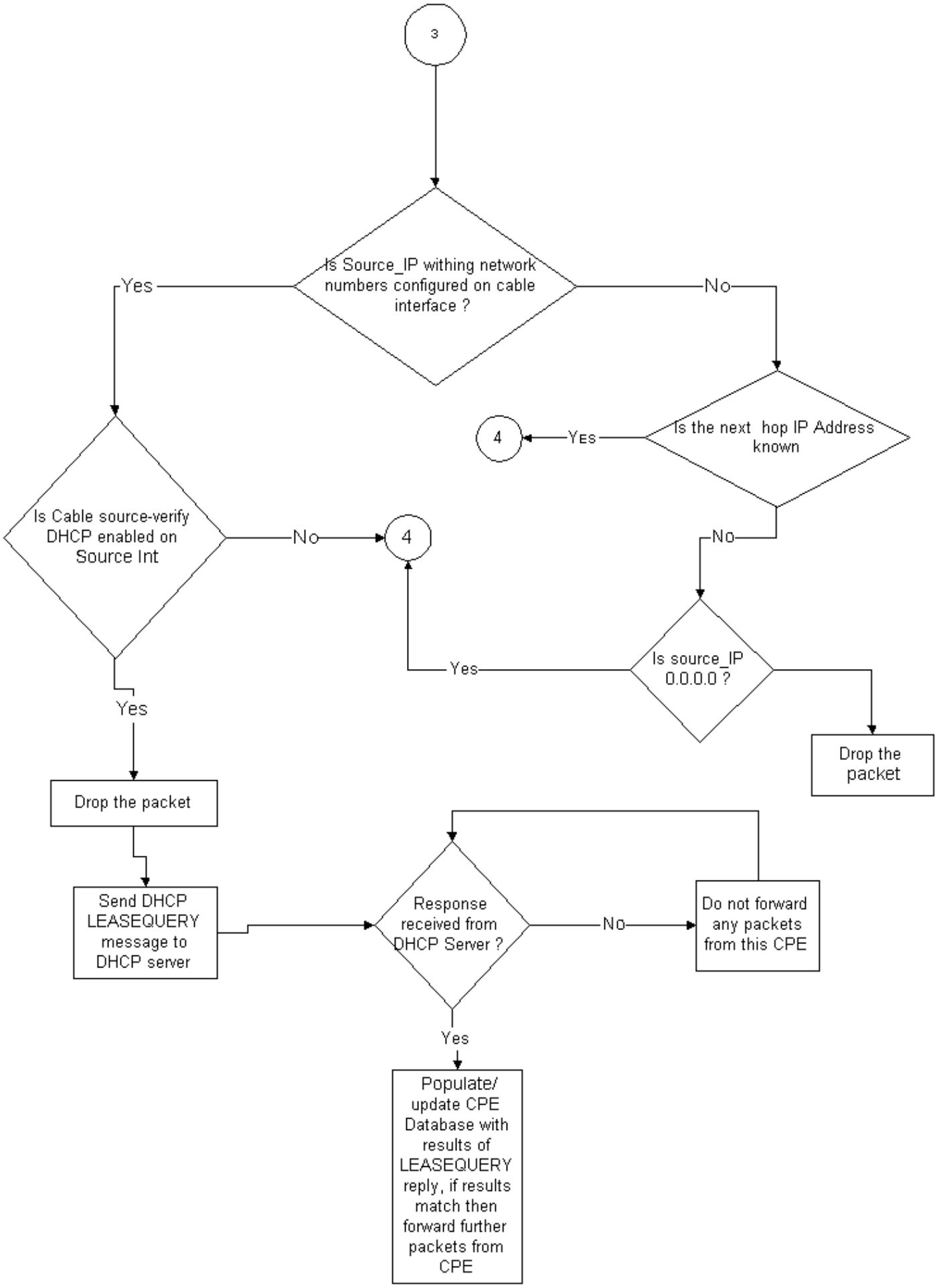
Un autre scénario consiste pour un utilisateur à attribuer de manière statique une adresse IP inutilisée jusqu'à présent à son PC qui se trouve dans la plage légitime d'adresses CPE. Ce scénario n'entraîne aucune interruption des services pour quiconque sur le réseau. Supposons que le client B a attribué l'adresse Y à son PC.

Le problème suivant peut survenir : le client C peut connecter sa station de travail au réseau du fournisseur de services et acquérir un bail DHCP pour l'adresse IP Y. La base de données CPE marquerait temporairement l'adresse IP Y comme appartenant au modem câble du client C. Cependant, il se peut qu'il ne soit pas long avant que le client B, l'utilisateur non légitime envoie la séquence appropriée du trafic ARP pour convaincre le saut suivant qu'il était le propriétaire légitime de l'adresse IP Y, causant ainsi une interruption du service du client C.

De même, le deuxième problème peut être résolu en activant la commande **cable source-verify**. Lorsque **cable source-verify** est activé, une entrée de base de données CPE générée par la

collecte de détails à partir d'une transaction DHCP ne peut pas être déplacée par d'autres types de trafic IP. Seule une autre transaction DHCP pour cette adresse IP ou l'entrée ARP sur la temporisation CMTS pour cette adresse IP peut remplacer l'entrée. Cela garantit que si un utilisateur final acquiert avec succès un bail DHCP pour une adresse IP donnée, ce client n'aura pas à s'inquiéter de la confusion du CMTS et à penser que son adresse IP appartient à un autre utilisateur.

Le premier problème consistant à empêcher les utilisateurs d'utiliser des adresses IP inutilisées jusqu'à présent peut être résolu avec **le protocole dhcp de vérification de la source par câble**. En ajoutant le paramètre dhcp à la fin de cette commande, le CMTS peut vérifier la validité de chaque nouvelle adresse IP source qu'il entend en émettant un type spécial de message DHCP appelé LEASEQUERY au serveur DHCP. Voir Organigramme 3.



Organigramme 3

Pour une adresse IP CPE donnée, le message LEASEQUERY demande quelle est l'adresse MAC et le modem câble correspondants.

Dans ce cas, si le client B connecte sa station de travail au réseau câblé avec l'adresse statique Y, le CMTS envoie une LEASEQUERY au serveur DHCP pour vérifier si l'adresse Y a été louée au PC du client B. Le serveur DHCP peut informer le CMTS qu'aucun bail n'a été accordé pour l'adresse IP Y et que, par conséquent, le client B se verra refuser l'accès.

Exemple 3 : utilisation d'un numéro de réseau non provisionné par le fournisseur de services

Les postes de travail peuvent être configurés derrière leurs modems câblés avec des adresses IP statiques qui peuvent ne pas entrer en conflit avec les numéros de réseau actuels du fournisseur de services, mais qui peuvent causer des problèmes à l'avenir. Par conséquent, à l'aide de la vérification de la source du câble, un CMTS peut filtrer les paquets provenant d'adresses IP source qui ne proviennent pas de la plage configurée sur l'interface de câble du CMTS.

Remarque : Pour que cela fonctionne correctement, vous devez également configurer la commande **ip verify unicast inverpath-path** afin d'empêcher les adresses source IP usurpées. Reportez-vous aux commandes de câble : le câble est pour plus d'informations.

Certains clients peuvent disposer d'un routeur en tant que périphérique CPE et s'arranger pour que le fournisseur de services achemine le trafic vers ce routeur. Si le CMTS reçoit le trafic IP du routeur CPE avec une adresse IP source Z, la vérification de la source du câble laissera passer ce paquet si le CMTS a une route vers le réseau Z appartient à via ce périphérique CPE. Référez-vous à Organigramme 3.

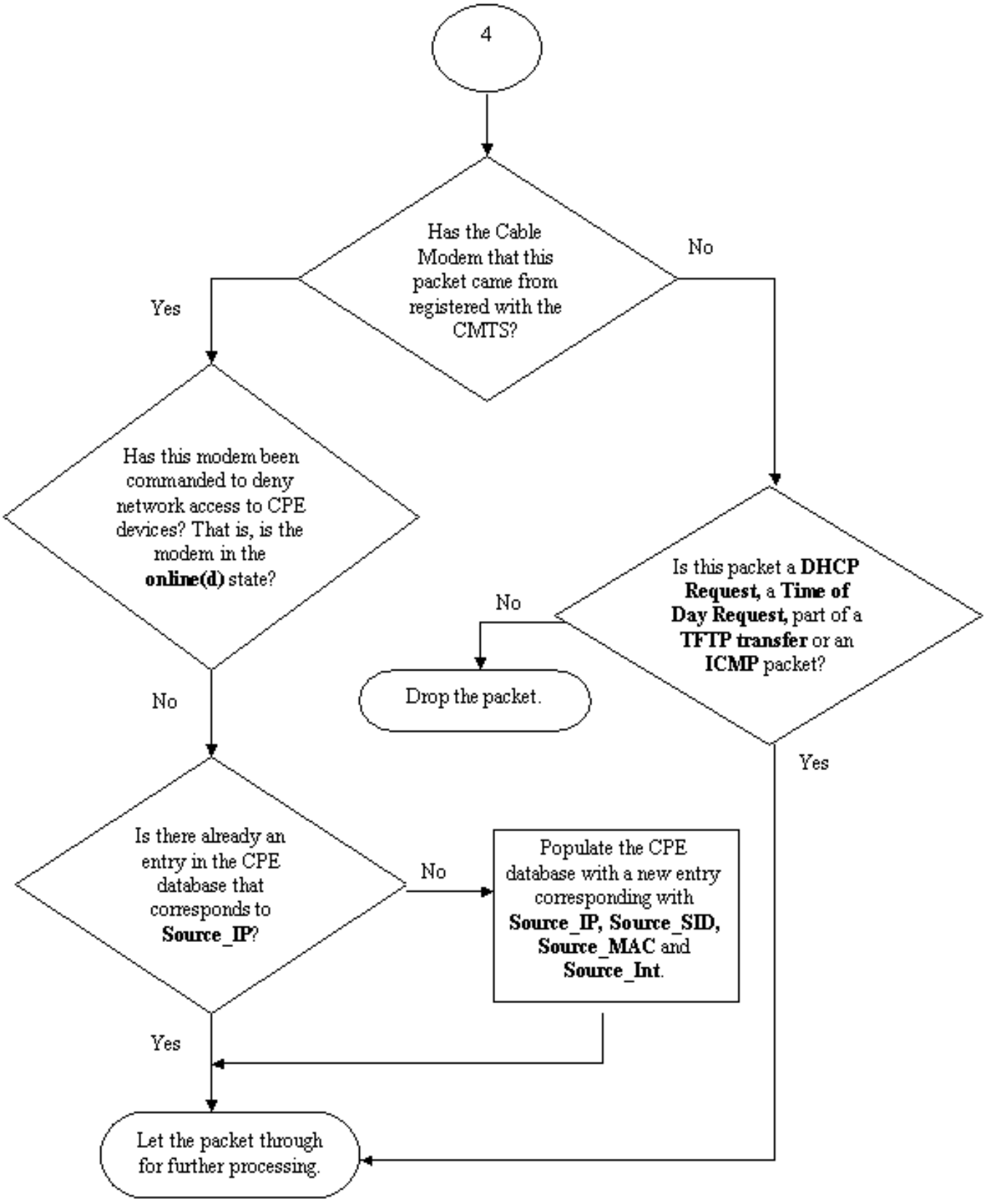
Prenons maintenant l'exemple suivant :

Sur le CMTS, nous avons la configuration suivante :

```
interface cable 3/0
 ip verify unicast reverse-path
 ip address 10.1.1.1 255.255.255.0
 ip address 24.1.1.1 255.255.255.0 secondary
 cable source-verify
!
ip route 24.2.2.0 255.255.255.0 24.1.1.2

Note: This configuration shows only what is
relevant for this example
```

En supposant qu'un paquet avec l'adresse IP source 172.16.1.10 est arrivé au CMTS à partir du modem câble 24.2.2.10, le CMTS verrait que 24.2.2.10 ne réside pas dans la base de données CPE, **show int cable x/y modem 0**, cependant **ip verify unicast inverpath** active Unicast Reverse Path Forwarding (Unicast RPF), qui vérifie chaque paquet reçu sur une interface afin de vérifier que l'adresse IP source du paquet apparaît dans les tables de routage qui appartiennent à cette interface. La **vérification de la source du câble** vérifie le saut suivant pour 24.2.2.10. Dans la configuration ci-dessus, nous avons **ip route 24.2.2.0 255.255.255.0 24.1.1.2** ce qui signifie que le prochain saut est 24.1.1.2. Maintenant, en supposant que 24.1.1.2 est une entrée valide dans la base de données CPE, le CMTS conclut que le paquet est OK et traitera donc le paquet conformément au diagramme de flux 4.



Organigramme 4

Configuration de la source du câble - Vérification

La configuration de **cable source-verify** implique simplement l'ajout de la commande **cable source-verify** à l'interface de câble sur laquelle vous souhaitez activer la fonction. Si vous utilisez l'agrégation d'interface de câble, vous devez ajouter **cable source-verify** à la configuration de

l'interface principale.

Comment configurer `le protocole dhcp de vérification de la source du câble`

Remarque : cable source-verify a été introduit pour la première fois dans le logiciel Cisco IOS Version 12.0(7)T et est pris en charge dans le logiciel Cisco IOS Versions 12.0SC, 12.1EC et 12.1T.

La configuration de **la commande cable source-verify dhcp** nécessite quelques étapes.

Assurez-vous que votre serveur DHCP prend en charge le message spécial DHCP LEASEQUERY.

Afin d'utiliser la fonctionnalité **cable source-verify dhcp**, votre serveur DHCP doit répondre aux messages comme spécifié par draft-ietf-dhcp-leasequery-XX.txt. Cisco Network Registrar versions 3.5 et ultérieures peuvent répondre à ce message.

Assurez-vous que votre serveur DHCP prend en charge le traitement de l'option Relay Agent Information. Consultez la section Relay Agent.

Le traitement de l'option DHCP Relay Information Option doit également être pris en charge par votre serveur DHCP. Il s'agit également du traitement de l'option 82. Cette option est décrite dans DHCP Relay Information Option (RFC 3046). Les versions 3.5 et ultérieures de Cisco Network Registrar prennent en charge le traitement des options d'informations de l'agent de relais, mais elles doivent être activées via l'utilitaire de ligne de commande nrcmd de Cisco Network Registrar avec la séquence de commandes suivante :

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp enable save-relay-agent-data

nrcmd -U admin -P changeme -C 127.0.0.1 save

nrcmd -U admin -P changeme -C 127.0.0.1 rechargement dhcp

Vous devrez peut-être remplacer le nom d'utilisateur, le mot de passe et l'adresse IP du serveur appropriés. Les valeurs par défaut ci-dessus s'affichent. Sinon, si vous êtes à l'invite nrcmd, >nrcmd vous pouvez simplement taper ce qui suit :

dhcp enable save-relay-agent-data

enregistrer

dhcp reload

Activez le traitement des options d'informations de relais DHCP sur le CMTS.

Agent de relais

Le CMTS doit marquer les requêtes DHCP des modems câble et du CPE avec l'option Relay Agent Information afin que le protocole **dhcp de vérification de la source du câble** soit efficace. Les commandes suivantes doivent être entrées en mode de configuration globale sur un CMTS exécutant le logiciel Cisco IOS Versions 12.1EC, 12.1T ou des versions ultérieures de Cisco IOS.

ip dhcp relay information option

Si votre système CMTS exécute le logiciel Cisco IOS Versions 12.0SC formez Cisco IOS, utilisez la commande **cable relay-agent-option** cable interface à la place.

Veillez à utiliser les commandes appropriées, en fonction de la version de Cisco IOS que vous utilisez. Veillez à mettre à jour votre configuration si vous modifiez les catégories de Cisco IOS.

Les commandes **d'information de relais** ajoutent une option spéciale appelée Option 82, ou option d'information de relais, au paquet DHCP relayé lorsque le CMTS relaie des paquets DHCP.

L'option 82 est remplie avec une sous-option, l'ID de circuit de l'agent, qui fait référence à l'interface physique du CMTS sur laquelle la requête DHCP a été entendue. En outre, une autre sous-option, l'ID distant de l'agent, est renseignée avec l'adresse MAC de 6 octets du modem câble dont la demande DHCP a été reçue ou transmise.

Ainsi, par exemple, si un PC dont l'adresse MAC est 99:88:77:66:55:44 et qui se trouve derrière le modem câble aa:bb:cc:dd:ee:ff envoie une requête DHCP, le CMTS transmettra la demande DHCP définissant la sous-option Agent Remote ID de l'option 82 à l'adresse MAC du modem câble aa:bb:cc:dd:ee ff.

En faisant inclure l'option Relay Information dans la requête DHCP d'un périphérique CPE, le serveur DHCP peut stocker des informations sur le CPE qui appartient derrière les modems câble. Cela devient particulièrement utile lorsque **le dhcp de vérification de la source du câble** est configuré sur le CMTS, car le serveur DHCP est en mesure d'informer le CMTS de manière fiable non seulement sur l'adresse MAC qu'un client particulier doit avoir, mais sur le modem câble auquel un client particulier doit être connecté.

Activez la commande cable source-verify dhcp sous l'interface de câble appropriée.

La dernière étape consiste à entrer la commande **cable source-verify dhcp** sous l'interface de câble sur laquelle vous souhaitez activer la fonction. Si le CMTS utilise l'agrégation d'interface de câble, vous devez entrer la commande sous l'interface principale du bundle.

Conclusion

Les suites de commandes **cable source-verify** permettent à un fournisseur de services de protéger le réseau câblé des utilisateurs disposant d'adresses IP non autorisées pour utiliser le réseau.

La commande cable source-verify en elle-même est un moyen efficace et facile d'implémenter la sécurité des adresses IP. Bien qu'il ne couvre pas tous les scénarios, il s'assure en tout cas que les clients ayant le droit d'utiliser les adresses IP attribuées ne rencontreront aucune interruption en faisant utiliser leur adresse IP par quelqu'un d'autre.

Dans sa forme la plus simple comme décrit dans ce document, un périphérique CPE non configuré via DHCP ne peut pas obtenir d'accès au réseau. Il s'agit du meilleur moyen de sécuriser l'espace d'adressage IP et d'accroître la stabilité et la fiabilité d'un service Data over Cable. Cependant, plusieurs opérateurs de services (MSO) qui ont des services commerciaux qui leur ont demandé d'utiliser des adresses statiques voulaient mettre en oeuvre une sécurité stricte de la commande **cable source-verify dhcp**.

La version 5.5 de Cisco Network Registrar offre une nouvelle capacité de réponse à la requête de

bail pour les adresses « réservées », même si l'adresse IP n'a pas été obtenue via DHCP. Le serveur DHCP inclut les données de réservation de bail dans les réponses DHCPLEASEQUERY. Dans les versions précédentes de Network Registrar, les réponses DHCPLEASEQUERY n'étaient possibles que pour les clients loués ou précédemment loués pour lesquels l'adresse MAC était stockée. Les agents de relais Cisco uBR, par exemple, ignorent les datagrammes DHCPLEASEQUERY qui n'ont pas d'adresse MAC et de durée de bail (option dhcp-lease-time).

Network Registrar renvoie une durée de bail par défaut d'un an (31536000 secondes) pour les baux réservés dans une réponse DHCPLEASEQUERY. Si l'adresse est effectivement louée, Network Registrar renvoie le temps de bail restant.

Informations connexes

- Option d'informations de relais DHCP (RFC 3046)
- Support et documentation techniques - Cisco Systems