Überprüfen der Kabelquelle und Sicherheit der IP-Adresse

Inhalt

Einführung

Cisco hat Verbesserungen in Cisco Cable Modem Termination System (CMTS)-Produkten implementiert, die bestimmte Arten von Denial-of-Service-Angriffen aufgrund von IP-Adressen-Spoofing und Diebstahl von IP-Adressen in DOCSIS-Kabelsystemen (Data-over-Cable Service Interface Specifications) verhindern. Die Cisco CMTS Cable Command Reference beschreibt die **Befehlspalette zur Überprüfung der Kabelquelle**, die Teil dieser Sicherheitserweiterungen für IP-Adressen ist.

Vorbereitungen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Voraussetzungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die ungeschützte DOCSIS-Umgebung

Eine DOCSIS Media Access Control (MAC)-Domäne ähnelt einem Ethernet-Segment. Wenn die Benutzer im Segment ungeschützt bleiben, sind sie anfällig für viele Arten von Layer-2- und Layer-3-Adressierungsangriffen, die auf Denial-of-Service-Angriffen basieren. Darüber hinaus kann der Service für Benutzer aufgrund von Fehlkonfigurationen der Adressierung auf Geräten anderer Benutzer beeinträchtigt werden. Beispiele hierfür:

- Konfigurieren doppelter IP-Adressen auf verschiedenen Knoten
- Konfigurieren doppelter MAC-Adressen auf verschiedenen Knoten
- Die nicht autorisierte Verwendung statischer IP-Adressen anstelle von zugewiesenen DHCP-IP-Adressen.
- Die unbefugte Nutzung verschiedener Netzwerknummern innerhalb eines Segments.
- Endknoten werden falsch konfiguriert, um ARP-Anfragen für einen Teil des IP-Subnetzes des Segments zu beantworten.

Diese Probleme lassen sich in einer Ethernet-LAN-Umgebung zwar leicht kontrollieren und beheben, indem die Geräte, die die Sicherheitsverletzung begangen haben, physisch nachverfolgt und getrennt werden. Aufgrund der potenziell großen Netzwerkgröße können solche Probleme in DOCSIS-Netzwerken jedoch schwieriger zu isolieren, zu beheben und zu verhindern sein. Endbenutzer, die Geräte am Kundenstandort steuern und konfigurieren (Customer Premise Equipment, CPE), haben möglicherweise nicht den Vorteil, dass ein lokales IS-Supportteam sicherstellt, dass ihre Workstations und PCs nicht absichtlich oder unabsichtlich falsch konfiguriert sind.

Die CMTS CPE-Datenbank

Die Cisco CMTS-Produktsuite verwaltet eine dynamisch bestückte interne Datenbank mit angeschlossenen CPE-IP- und MAC-Adressen. Die CPE-Datenbank enthält auch Details zu den entsprechenden Kabelmodems, zu denen diese CPE-Geräte gehören.

Eine teilweise Ansicht der CPE-Datenbank, die einem bestimmten Kabelmodem entspricht, kann angezeigt werden, indem Sie den Befehl **show interface cable X/Y modem Z** ausführen. Hier ist X die Linecard-Nummer, Y die Downstream-Portnummer und Z der Service Identifier (SID) des Kabelmodems. Z kann auf 0 gesetzt werden, um Details zu allen Kabelmodems und CPE an einer bestimmten Downstream-Schnittstelle anzuzeigen. Im folgenden Beispiel finden Sie eine typische Ausgabe, die durch diesen Befehl generiert wird.

```
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
```

Hinweis: Da dieser Befehl ausgeblendet ist, unterliegt er Änderungen und ist nicht garantiert in allen Versionen der Cisco IOS® Software verfügbar.

Im obigen Beispiel wird die Methodenspalte des Hosts mit der IP-Adresse 192.168.1.90 als dhcp aufgeführt. Das bedeutet, dass das CMTS von diesem Host erfahren hat, indem es die DHCP-

Transaktionen zwischen dem Host und dem DHCP-Server des Service Providers überwacht hat.

Der Host mit der IP-Adresse 192.168.1.77 wird mit der statischen Methode aufgelistet. Das bedeutet, dass das CMTS nicht zuerst über eine DHCP-Transaktion zwischen diesem Gerät und einem DHCP-Server von diesem Host erfahren hat. Stattdessen sah der CMTS zunächst andere Arten von IP-Datenverkehr von diesem Host. Dieser Datenverkehr hätte Webbrowsing-, E-Mail- oder Ping-Pakete sein können.

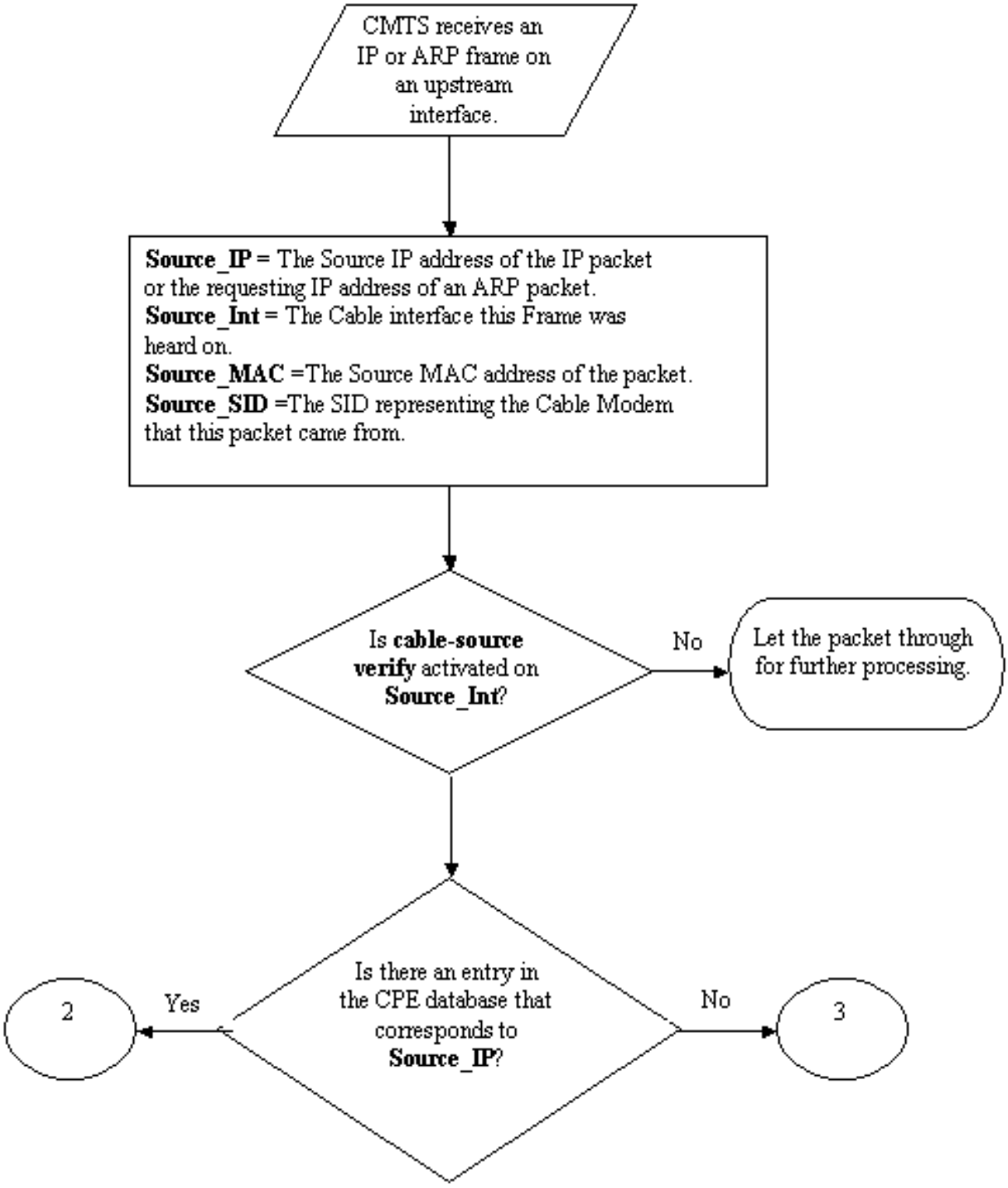
Obwohl es den Anschein hat, als ob 192.168.1.77 mit einer statischen IP-Adresse konfiguriert wurde, kann es sein, dass dieser Host tatsächlich einen DHCP-Lease erworben hat, aber das CMTS seit dem Ereignis möglicherweise neu gestartet wurde und sich daher nicht an die Transaktion erinnert.

Die CPE-Datenbank wird in der Regel von den CMTS-Informationen übernommen, die aus den DHCP-Transaktionen zwischen CPE-Geräten und dem DHCP-Server des Service Providers stammen. Darüber hinaus kann das CMTS anderen IP-Datenverkehr von CPE-Geräten überwachen, um festzustellen, welche CPE-IP- und MAC-Adressen zu welchen Kabelmodems gehören.

Der Befehl zur Überprüfung der Kabelquelle

Cisco hat den Cable Interface Command Cable Source-Verification [dhcp] implementiert. Dieser Befehl veranlasst das CMTS, die CPE-Datenbank zur Überprüfung der Gültigkeit von IP-Paketen zu verwenden, die das CMTS an seinen Kabelschnittstellen empfängt, und ermöglicht es dem CMTS, intelligente Entscheidungen darüber zu treffen, ob diese weitergeleitet werden sollen oder nicht.

Das folgende Flussdiagramm zeigt die zusätzliche Verarbeitung, die ein auf einer Kabelschnittstelle empfangenes IP-Paket durchlaufen muss, bevor es den CMTS durchlaufen darf.



Flussdiagramm 1

Das Flussdiagramm beginnt mit einem Paket, das von einem Upstream-Port des CMTS empfangen wird, und endet, wenn das Paket entweder zur weiteren Verarbeitung weiterverarbeitet

oder verworfen werden darf.

Beispiel 1: Szenario mit doppelten IP-Adressen

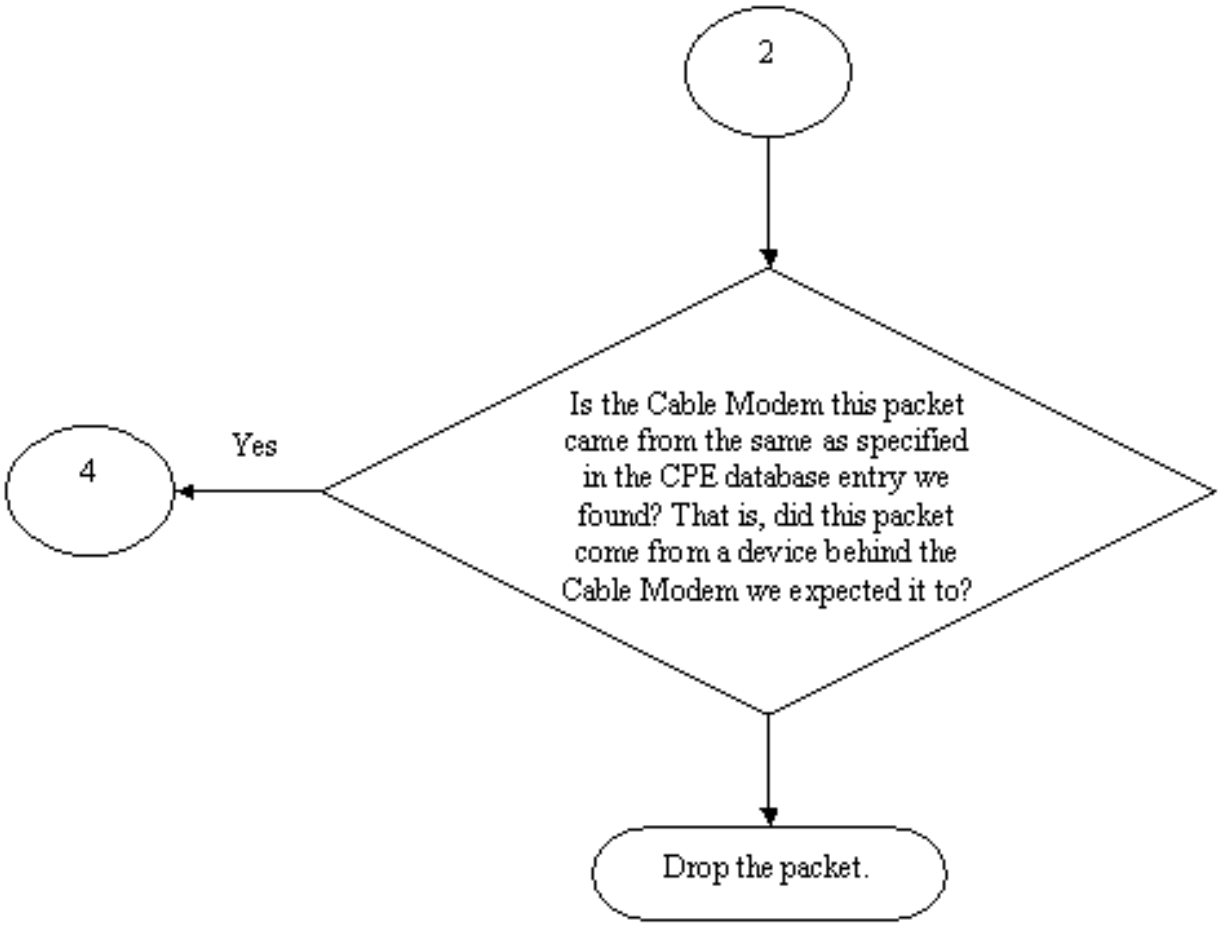
Das erste Denial of Service-Szenario, das wir behandeln werden, betrifft die doppelte Anzahl von IP-Adressen. Beispiel: Kunde A ist mit seinem Service Provider verbunden und hat ein gültiges DHCP-Lease für seinen PC erhalten. Die IP-Adresse, die Kunde A erhalten hat, wird als X bezeichnet.

Kurz nach Erwerb des DHCP-Leasings beschließt Kunde B, seinen PC mit einer statischen IP-Adresse zu konfigurieren, die zufällig mit der IP-Adresse übereinstimmt, die derzeit von Geräten des Kunden A verwendet wird. Die CPE-Datenbankinformationen bezüglich der IP-Adresse X ändern sich, je nachdem, welches CPE-Gerät zuletzt eine ARP-Anfrage im Auftrag von X gesendet hat.

In einem ungeschützten DOCSIS-Netzwerk kann Kunde B möglicherweise den nächsten Hop-Router (in den meisten Fällen das CMTS) davon überzeugen, dass er das Recht hat, die IP-Adresse X zu verwenden, indem er einfach eine ARP-Anfrage im Namen von X an den CMTS oder Next-Hop-Router sendet. Dadurch wird die Weiterleitung des Datenverkehrs vom Service Provider an Kunde A verhindert.

Durch die Aktivierung der Überprüfung der Kabelquelle konnte der CMTS sehen, dass IP- und ARP-Pakete für die IP-Adresse X vom falschen Kabelmodem bezogen wurden. Daher würden diese Pakete verworfen, siehe Flussdiagramm 2. Dies umfasst alle IP-Pakete mit der Quelladresse X und ARP-Anfragen im Auftrag von X. Die CMTS-Protokolle zeigen eine Meldung entsprechend der folgenden Zeilen an:

%UBR7200-3-BADIPSOURCE: Schnittstellenkabel3/0, IP-Paket von ungültiger Quelle. IP=192.168.1.10, MAC=0001.422c.54d0, Erwartete SID=10, Tatsächliche SID=11



Flussdiagramm 2

Anhand dieser Informationen werden beide Clients identifiziert, und das Kabelmodem mit der angeschlossenen doppelten IP-Adresse kann deaktiviert werden.

Beispiel 2: Szenario mit doppelten IP-Adressen - Verwendung einer noch nicht verwendeten IP-Adresse

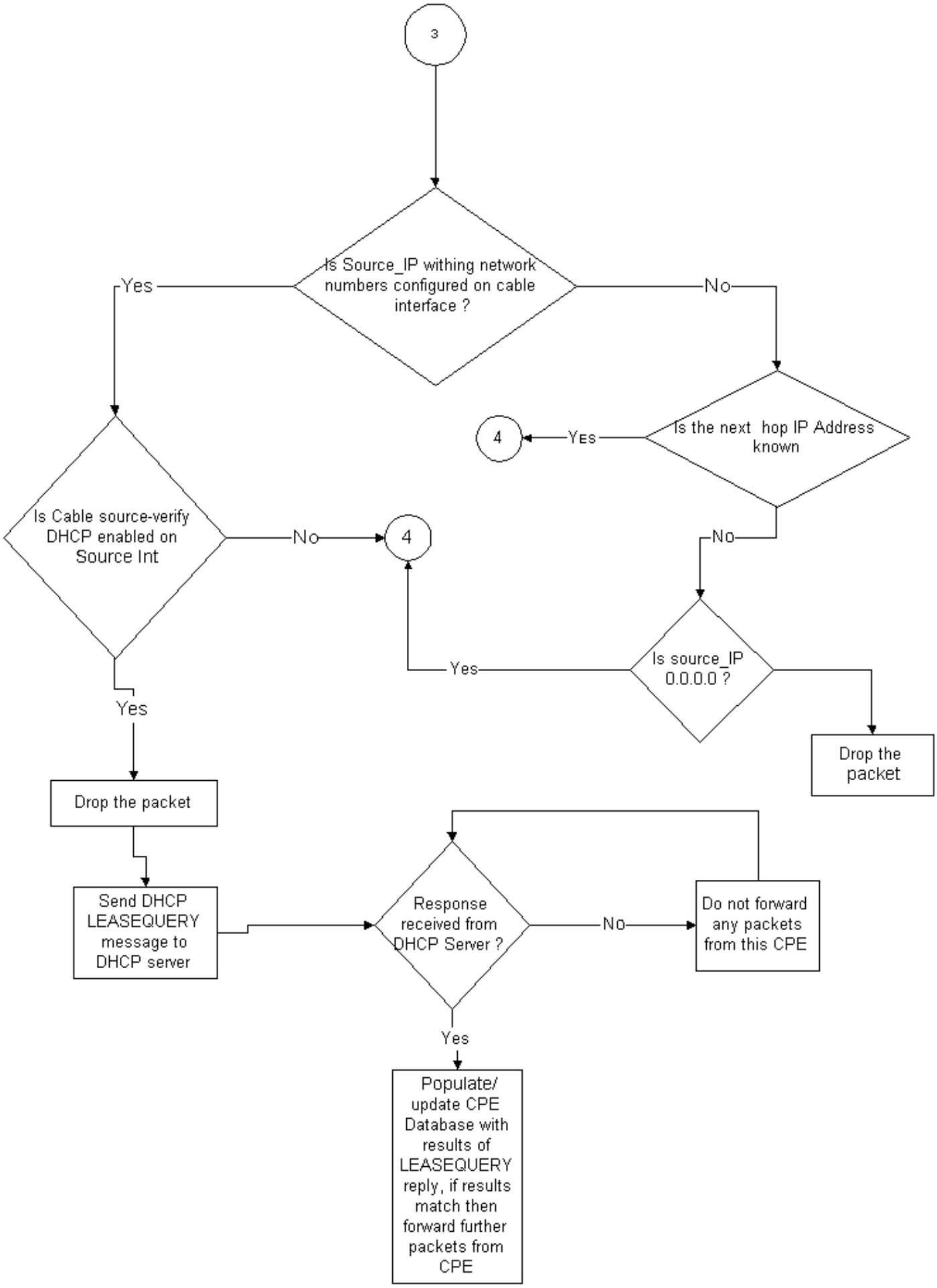
Ein weiteres Szenario ist, dass Benutzer ihrem PC statisch eine noch nicht verwendete IP-Adresse zuweisen, die dem legitimen Bereich von CPE-Adressen entspricht. Dieses Szenario verursacht keine Serviceunterbrechung für alle im Netzwerk. Nehmen wir an, Kunde B hat Adresse Y für seinen PC zugewiesen.

Das nächste mögliche Problem besteht darin, dass Kunde C seine Workstation mit dem Netzwerk des Service Providers verbinden und einen DHCP-Lease für die IP-Adresse Y erwerben könnte. In der CPE-Datenbank wird die IP-Adresse Y vorübergehend als hinter dem Kabelmodem des Kunden C gehörend markiert. Es kann jedoch nicht lange dauern, bis Kunde B ist. Der nicht berechtigte Benutzer sendet die entsprechende Sequenz von ARP-Datenverkehr, um den Next-Hop davon zu überzeugen, dass er der legitime Eigentümer der IP-Adresse Y war, was zu einer Unterbrechung des Service von Kunde C führte.

Ebenso kann das zweite Problem durch Einschalten der **Kabelquellenprüfung** gelöst werden.

Wenn die Kabelquellenüberprüfung aktiviert ist, kann ein CPE-Datenbankeintrag, der durch die Erfassung von Details aus einer DHCP-Transaktion generiert wurde, nicht durch andere Arten von IP-Datenverkehr ersetzt werden. Nur eine andere DHCP-Transaktion für diese IP-Adresse oder der ARP-Eintrag im CMTS-Timing für diese IP-Adresse kann den Eintrag ersetzen. Dadurch wird sichergestellt, dass ein Endbenutzer, der erfolgreich ein DHCP-Lease für eine bestimmte IP-Adresse erhält, sich keine Sorgen darüber machen muss, dass das CMTS verwirrt wird und dass seine IP-Adresse einem anderen Benutzer gehört.

Das erste Problem, Benutzer daran zu hindern, noch nicht verwendete IP-Adressen zu verwenden, kann mithilfe von DHCP gelöst werden, das die Kabelquelle verifiziert. Durch Hinzufügen des DHCP-Parameters zum Ende dieses Befehls kann der CMTS die Gültigkeit jeder neuen Quell-IP-Adresse überprüfen, indem er dem DHCP-Server einen speziellen DHCP-Nachrichtentyp namens LEASEQUERY übermittelt. Siehe Flussdiagramm 3.



Flussdiagramm 3

Für eine bestimmte CPE-IP-Adresse werden in der LEASEQUERY-Nachricht die entsprechende MAC-Adresse und das entsprechende Kabelmodem gefragt.

Wenn in dieser Situation der Kunde B seine Workstation mit dem Kabelnetzwerk über die statische Adresse Y verbindet, sendet das CMTS eine LEASEQUERY an den DHCP-Server, um zu überprüfen, ob die Adresse Y an den PC von Kunde B geleast wurde. Der DHCP-Server kann dem CMTS mitteilen, dass für die IP-Adresse Y kein Leasing gewährt wurde und Kunde B daher keinen Zugriff mehr erhält.

Beispiel 3 - Verwendung einer Netzwerknummer, die nicht vom Dienstanbieter bereitgestellt wird

Benutzer können Workstations hinter ihren Kabelmodems mit statischen IP-Adressen konfigurieren, die nicht mit den aktuellen Netzwerknummern des Service Providers in Konflikt stehen, aber in Zukunft Probleme verursachen können. Aus diesem Grund kann ein CMTS mithilfe der Überprüfung der Kabelquelle Pakete herausfiltern, die von Quell-IP-Adressen stammen, die nicht aus dem Bereich stammen, der für die Kabelschnittstelle des CMTS konfiguriert wurde.

Hinweis: Damit dies ordnungsgemäß funktioniert, müssen Sie auch den Befehl **ip verify unicast reverse path** konfigurieren, um Spoofing-IP-Quelladressen zu verhindern. Siehe Kabelbefehle: Kabel für weitere Informationen.

Einige Kunden verfügen möglicherweise über einen Router als CPE-Gerät und veranlassen, dass der Service Provider den Datenverkehr an diesen Router weiterleitet. Wenn der CMTS IP-Datenverkehr vom CPE-Router mit der Quell-IP-Adresse Z empfängt, lässt die Überprüfung der Kabelquelle dieses Paket durchlaufen, wenn der CMTS über eine Route zum Netzwerk Z verfügt, die über dieses CPE-Gerät zu diesem CPE-Gerät gehört. Siehe Flussdiagramm 3.

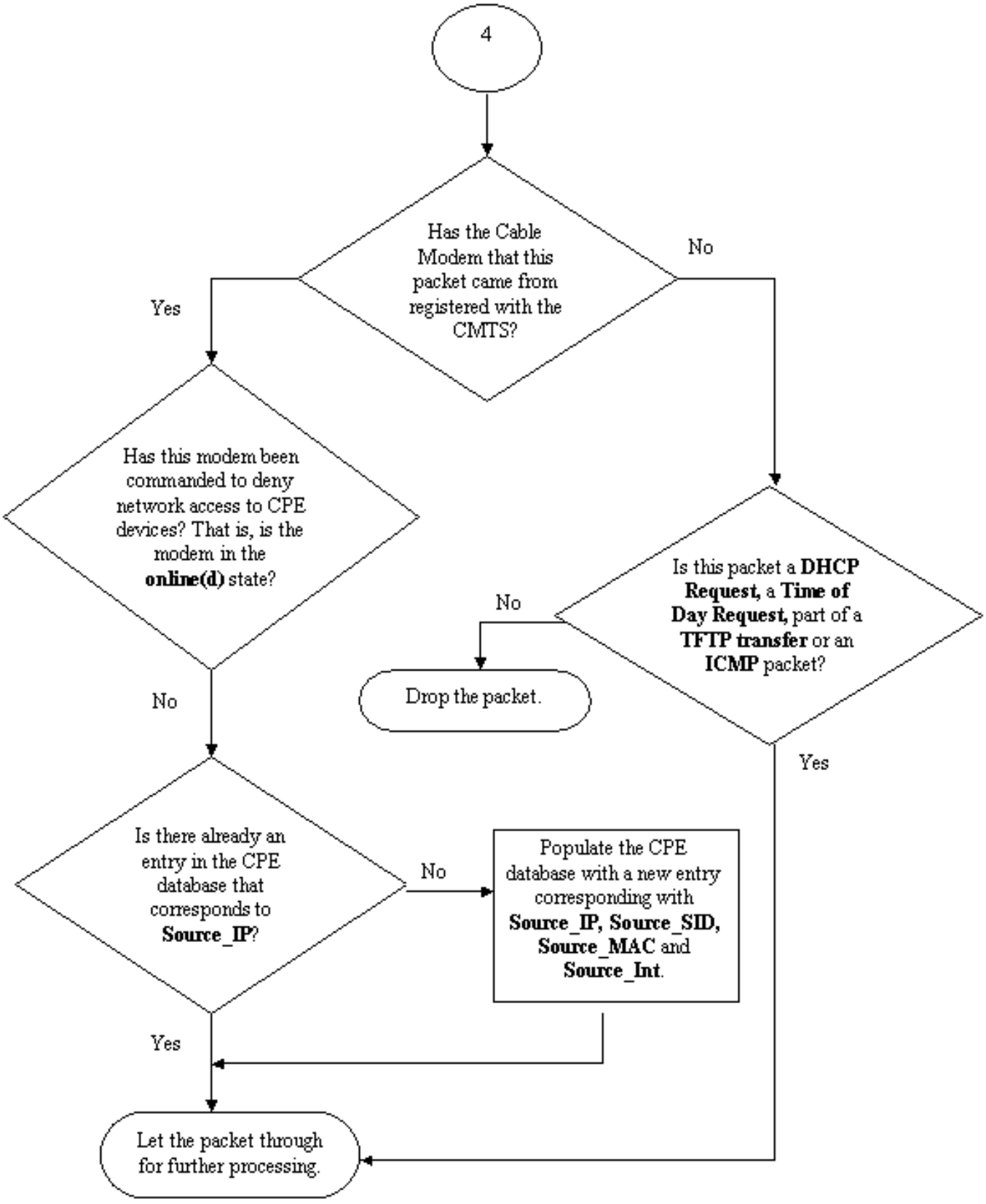
Betrachten Sie nun das folgende Beispiel:

Für das CMTS wird folgende Konfiguration verwendet:

```
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
```

Wenn ein Paket mit der Quell-IP-Adresse 172.16.1.10 vom Kabelmodem 24.2.2.10 beim CMTS eingeht, würde das CMTS sehen, dass 24.2.2.10 nicht in der CPE-Datenbank vorhanden ist. **Zeigen Sie int-Kabel x/y-Modem 0 an**, **ip jedoch unicast verse-path** aktiviert Unicast Reverse Path Forwarding (Unicast RPF), das jedes an einer Schnittstelle empfangene Paket überprüft, um sicherzustellen, dass die Quell-IP-Adresse des Pakets in den Routing-Tabellen angezeigt wird, die zu dieser Schnittstelle gehören. Die **Überprüfung der Kabelquelle** überprüft, was der nächste Hop für 24.2.2.10 ist. In der obigen Konfiguration befindet sich die **ip route 24.2.2.0 255.255.255.0 24.1.1.2**, was bedeutet, dass der nächste Hop 24.1.1.2 ist. Wenn jetzt angenommen wird, dass 24.1.1.2 ein gültiger Eintrag in der CPE-Datenbank ist, kommt der CMTS zu dem Schluss, dass das Paket in Ordnung ist und verarbeitet das Paket daher gemäß Flussdiagramm 4.



Flussdiagramm 4

So konfigurieren Sie die Kabelquellenüberprüfung

Bei der Konfiguration **der Kabelquellenverifizierung** muss der Kabelschnittstelle einfach der Befehl **zur Überprüfung der Kabelquelle** hinzugefügt werden, auf dem die Funktion aktiviert werden soll. Wenn Sie die Bündelung der Kabelschnittstelle verwenden, müssen Sie der Konfiguration der

primären Schnittstelle die **Überprüfung** der **Kabelquelle** hinzufügen.

Konfigurieren von `DHCP zur Überprüfung der Kabelquelle`

Hinweis: Die Überprüfung der Kabelquellen wurde erstmals in der Cisco IOS Software-Version 12.0(7)T eingeführt und wird von den Cisco IOS Software-Versionen 12.0SC, 12.1EC und 12.1T unterstützt.

Die Konfiguration von **DHCP zur Überprüfung der Kabelquelle** erfordert einige Schritte.

Stellen Sie sicher, dass Ihr DHCP-Server die spezielle DHCP LEASEQUERY-Nachricht unterstützt.

Um die **DHCP-**Funktion zur **Überprüfung der Kabelquelle** nutzen zu können, muss der DHCP-Server die Meldungen wie in Draft-ietf-dhcp-leasequery-XX.txt angegeben beantworten. Cisco Network Registrar Version 3.5 und höher können diese Nachricht beantworten.

Stellen Sie sicher, dass Ihr DHCP-Server die Verarbeitung von Relay Agent Information Option unterstützt. Siehe Relay Agent.

Eine weitere Funktion, die vom DHCP-Server unterstützt werden muss, ist die Verarbeitung von DHCP Relay Information Option (DHCP-Relay-Informationsoption). Dies wird auch als Verarbeitung der Option 82 bezeichnet. Diese Option wird in der DHCP Relay Information Option (RFC 3046) beschrieben. Cisco Network Registrar, Version 3.5 und höher, unterstützt die Verarbeitung von Relay Agent Information Option. Sie muss jedoch über das Befehlszeilendienstprogramm von Cisco Network Registrar mit der folgenden Befehlsfolge aktiviert werden:

nrcmd -U admin -P change -C 127.0.0.1 dhcp enable save-relais-agent-data

nrcmd -U admin -P change -C 127.0.0.1 save

nrcmd -U admin -P change -C 127.0.0.1 dhcp reload

Möglicherweise müssen Sie den entsprechenden Benutzernamen, das Kennwort und die Server-IP-Adresse ersetzen. Die oben angegebenen Standardwerte werden angezeigt. Wenn Sie sich an der Eingabeaufforderung nrcmd befinden, >nrcmd geben Sie einfach Folgendes ein:

dhcp enable save-relais-agent-data

speichern

DHCP-Neuladen

Aktivieren Sie die Verarbeitung der DHCP-Relay-Informationen auf dem CMTS.

Relay-Agent

Das CMTS muss DHCP-Anfragen von Kabelmodems und CPE mit der Option Relay Agent Information (Option für Relay-Agent-Informationen) kennzeichnen, damit die **DHCP-Funktion bei der Kabelquelle überprüft** werden kann. Die folgenden Befehle müssen auf einem CMTS, auf dem Cisco IOS Software Releases 12.1EC, 12.1T oder höher ausgeführt werden, im globalen

Konfigurationsmodus eingegeben werden.

ip dhcp relais information option

Wenn auf Ihrem CMTS die Cisco IOS Software Releases 12.0SC Train Cisco IOS ausgeführt wird, verwenden Sie stattdessen den Befehl Leiste-Relay-Agent-Option Kabel.

Achten Sie darauf, die entsprechenden Befehle zu verwenden, abhängig von der Version von Cisco IOS, die Sie ausführen. Aktualisieren Sie Ihre Konfiguration, wenn Sie die Züge von Cisco IOS ändern.

Die **Weiterleitungsinformationsoptionen-**Befehle fügen dem weitergeleiteten DHCP-Paket eine spezielle Option mit der Bezeichnung Option 82 oder die Weiterleitungsinformationsoption hinzu, wenn das CMTS DHCP-Pakete weiterleitet.

Option 82 wird mit der Unteroption "Agent Circuit-ID" ausgefüllt, die auf die physische Schnittstelle des CMTS verweist, auf dem die DHCP-Anfrage gehört wurde. Darüber hinaus wird eine weitere Unteroption, die Agent Remote ID, mit der 6-Byte-MAC-Adresse des Kabelmodems gefüllt, von der die DHCP-Anfrage empfangen oder durchgegeben wurde.

Wenn beispielsweise ein PC mit der MAC-Adresse 99:88:77:66:55:44 hinter dem Kabelmodem aa:bb:cc:dd:ee:ff eine DHCP-Anfrage sendet, leitet der CMTS die DHCP-Anfrage zur Einstellung der Agent Remote ID-Unteroption 82 an die MAC-Adresse des Kabelmodems aa:bb:cc weiter.:dd:ee:ff.

Wenn die Option Relay Information (Relay-Informationen) in die DHCP-Anfrage eines CPE-Geräts integriert ist, kann der DHCP-Server Informationen darüber speichern, welches CPE zu welchen Kabelmodems gehört. Dies ist besonders dann nützlich, wenn **DHCP zur Überprüfung der Kabelquelle** auf dem CMTS konfiguriert ist, da der DHCP-Server das CMTS zuverlässig darüber informieren kann, welche MAC-Adresse ein bestimmter Client haben sollte, mit welchem Kabelmodem ein bestimmter Client verbunden werden soll.

Aktivieren Sie den DHCP-Befehl zur Überprüfung der Kabelquelle unter der entsprechenden Kabelschnittstelle.

Der letzte Schritt besteht darin, den Befehl **zur Überprüfung der Kabelquelle** unter der Kabelschnittstelle einzugeben, auf der die Funktion aktiviert werden soll. Wenn der CMTS die Bündelung der Kabelschnittstelle verwendet, müssen Sie den Befehl unter der primären Schnittstelle des Pakets eingeben.

Fazit

Die Befehle zur **Überprüfung der Kabelquelle** ermöglichen es einem Service Provider, das Kabelnetzwerk vor Benutzern mit nicht autorisierten IP-Adressen für die Verwendung des Netzwerks zu schützen.

Der Befehl zur Überprüfung der Kabelquelle allein ist eine effektive und einfache Methode zur Implementierung der IP-Adresssicherheit. Zwar werden nicht alle Szenarien abgedeckt, doch wird im Leasing-Zeitraum sichergestellt, dass Kunden, die zur Nutzung zugewiesener IP-Adressen berechtigt sind, keine Unterbrechungen durch die Verwendung ihrer IP-Adresse durch eine andere Person erleiden.

In der einfachsten Form, wie in diesem Dokument beschrieben, kann ein nicht über DHCP konfiguriertes CPE-Gerät keinen Netzwerkzugriff erhalten. Dies ist die beste Methode, um den IP-Adressraum zu sichern und die Stabilität und Zuverlässigkeit eines Data over Cable-Service zu erhöhen. Mehrere Service Operatoren (MSOs), die kommerzielle Dienste anbieten und statische Adressen verwenden mussten, wollten jedoch die strikte Sicherheit des **DHCP-Befehls** implementieren.

Cisco Network Registrar Version 5.5 bietet eine neue Möglichkeit, auf die Lease-Abfrage für "reservierte" Adressen zu reagieren, obwohl die IP-Adresse nicht über DHCP abgerufen wurde. Der DHCP-Server enthält Leasingreservierungsdaten in den DHCPLEASEQUERY-Antworten. In den vorherigen Versionen von Network Registrar waren die DHCPLEASEQUERY-Antworten nur für gemietete oder zuvor geleaste Kunden möglich, für die die MAC-Adresse gespeichert wurde. Cisco uBR Relay-Agenten verwerfen beispielsweise DHCPLEASEQUERY-Datagramme ohne MAC-Adresse und Leasingzeit (DHCP-Lease-Time-Option).

Network Registrar gibt für reservierte Leasing-Verträge in einer DHCPLEASEQUERY-Antwort eine standardmäßige Leasedauer von einem Jahr (31536000 Sekunden) zurück. Wenn die Adresse tatsächlich geleast wird, gibt der Network Registrar die verbleibende Leasingzeit zurück.

Zugehörige Informationen

- DHCP Relay Information Option (RFC 3046)
- Technischer Support und Dokumentation für Cisco Systeme