Kabelbron-verificatie en IP-adresbeveiliging

Inhoud

Inleiding

Cisco heeft verbeteringen geïmplementeerd binnen Cisco-kabelmodemterminalisatieproducten (CMTS) die bepaalde typen Denial of Service-aanvallen beperken op basis van IP-adressenscheiding en IP-adresdiefstal in DOCSIS-kabelsystemen (Data-over-Cable Service Interface Specifications). De Cisco CMTS Cable Opdracht Referentie beschrijft de **kabelbron-verify reeks opdrachten die deel uitmaken van deze IP-adresbeveiligingsverbeteringen.**

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De onbeschermde DOCSIS-omgeving

Een DOCSIS Media Access Control (MAC)-domein is qua aard gelijk aan een Ethernet-segment. Als onbeschermd blijven, zijn de gebruikers in het segment kwetsbaar aan vele types van Layer 2 en Layer 3 het richten van op gebaseerde Denial of Service aanvallen. Bovendien is het mogelijk voor gebruikers om te lijden onder een verminderde serviceniveaus door de defecte configuratie van het richten op de apparatuur van andere gebruikers. Voorbeelden hiervan zijn:

- Het configureren van dubbele IP adressen op verschillende knooppunten.
- Het configureren van dubbele MAC adressen op verschillende knooppunten.
- Het onbevoegde gebruik van statische IP-adressen in plaats van Dynamic Host Configuration Protocol (DHCP) heeft IP-adressen toegewezen.
- Het onbevoegde gebruik van verschillende netwerknummers binnen een segment.
- Onjuist configureren van eindknooppunten om ARP-verzoeken te beantwoorden namens een deel van het segment IP-net.

Terwijl deze typen problemen in een Ethernet LAN-omgeving gemakkelijk te beheersen en te verzachten zijn door de apparatuur die wordt aangedaan fysiek te traceren en los te koppelen, kunnen dergelijke problemen in DOCSIS-netwerken moeilijker te isoleren, op te lossen en te voorkomen zijn door de potentieel grote omvang van het netwerk. Bovendien kunnen eindgebruikers die Customer Premise Equipment (CPE) configureren niet het voordeel hebben van een lokaal IS-ondersteuningsteam om er zeker van te zijn dat hun werkstations en pc's niet opzettelijk of onbedoeld niet zijn geconfigureerd.

De CMTS CPE-database

De Cisco reeks CMTS producten onderhoudt een dynamisch bevolkte interne gegevensbank van aangesloten CPE IP en MAC adressen. De CPE-database bevat ook details over de corresponderende kabelmodems waarop deze CPE-apparaten behoren.

Een gedeeltelijke weergave van de CPE Database die aan een bepaalde kabelmodem overeenkomt kan worden bekeken door de verborgen CMTS opdracht **tonen interfacekabel X/Y modem Z** uit te voeren. Hier is X het lijnkaartnummer, Y is het downstream poortnummer en Z is de Service Identifier (SID) van de kabelmodem. Z kan op 0 worden ingesteld om details over alle kabelmodems en CPE op een bepaalde downstreaminterface te bekijken. Zie voorbeeld hieronder van een typische uitvoer die door deze opdracht gegenereerd is.

```
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
```

Opmerking: Aangezien deze opdracht verborgen is, is de opdracht onderhevig aan verandering en is de garantie niet aanwezig in alle releases van Cisco IOS®-software.

In het voorbeeld hierboven, is de methodiek van de gastheer met IP adres 192.168.1.90 vermeld als dhcp. Dit betekent dat CMTS over deze host heeft geleerd door naar de DHCP-transacties tussen de host en de DHCP-server van de serviceprovider te kijken.

De host met IP-adres 192.168.1.77 wordt weergegeven met een statische methode. Dit betekent dat CMTS niet eerst van deze gastheer via een transactie van DHCP tussen dit apparaat en een server van DHCP leerde. In plaats daarvan zag CMTS eerst andere soorten IP verkeer van deze gastheer. Dit verkeer had web browsing-, e-mail- of "ping"-pakketten kunnen zijn.

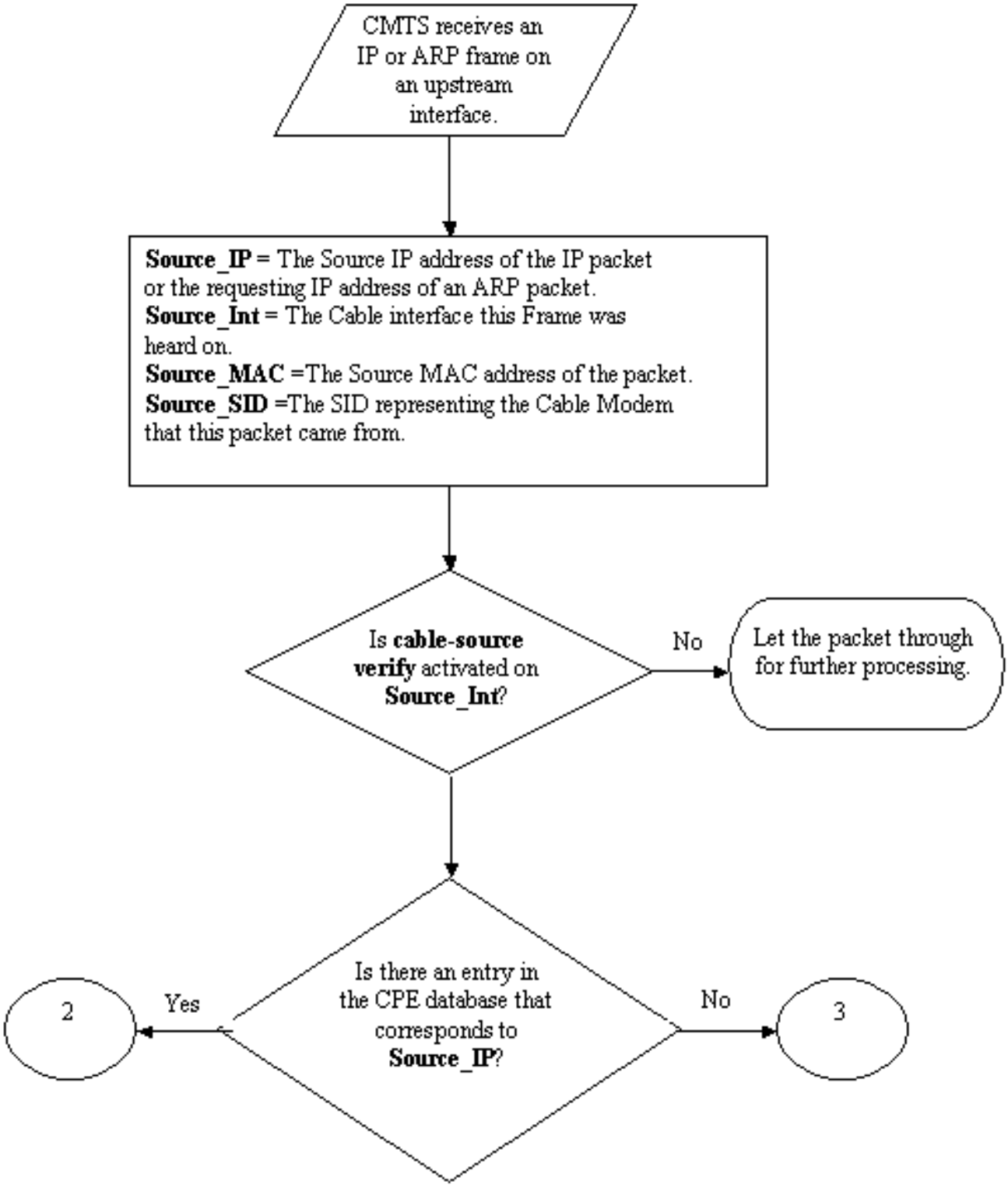
Hoewel het lijkt dat 192.168.1.77 is geconfigureerd met een statisch IP-adres, kan het zijn dat deze host in feite een DHCP-lease heeft verworven, maar de CMTS kan sinds de gebeurtenis zijn herstart en herinnert zij zich de transactie dan ook niet.

De CPE-database wordt normaal bevolkt door de CMTS-informatie die informatie bevat van de DHCP-transacties tussen CPE-apparaten en de DHCP-server van de serviceproviders. Bovendien kan CMTS naar ander IP verkeer luisteren dat van CPE apparaten komt om te bepalen welke CPE IP en MAC adressen behoren tot welke Kabelmodems.

De opdracht Bron controleren van de kabel

Cisco heeft de kabelbron-verify [dhcp] van de kabelinterface geïmplementeerd. Deze opdracht zorgt ervoor dat CMTS gebruik maakt van de CPE-database om de geldigheid van IP-pakketten die CMTS op zijn kabelinterfaces ontvangt te verifiëren en stelt de CMTS in staat om intelligente besluiten te nemen over het al dan niet doorsturen ervan.

In het onderstaande stroomschema wordt aangegeven welke extra verwerkings- en IP-pakketten op een kabelinterface moeten worden ontvangen voordat u door de CMTS kunt gaan.



Stroomdiagram 1

Het stroomschema begint met een pakje dat door een upstream poort op CMTS wordt ontvangen en eindigt met een pakje dat verder kan worden verwerkt of dat in het pakje wordt gevallen.

Voorbeeld 1 - Scenario met dubbele IP-adressen

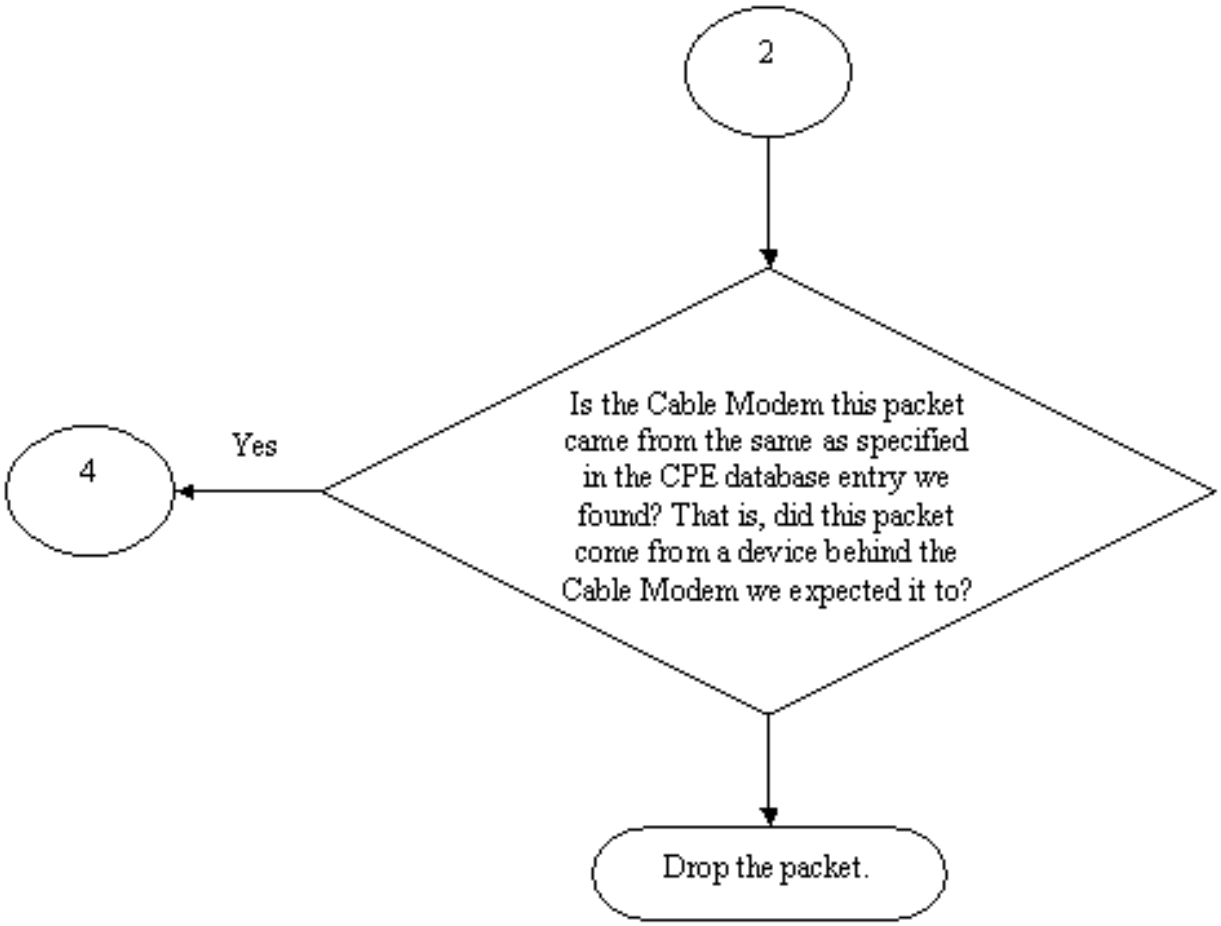
Het eerste Denial of Service-scenario dat we zullen aanpakken is de situatie met dubbele IP-adressen. Stel dat klant A op zijn serviceprovider is aangesloten en een geldige DHCP-lease voor deze pc heeft verkregen. Het IP-adres Customer A is verkregen en staat bekend als X.

Enige tijd nadat A zijn DHCP-lease heeft verworven, beslist klant B om zijn pc met een statisch IP-adres te configureren dat toevallig hetzelfde is als het adres dat momenteel wordt gebruikt door de apparatuur van Customer A. De informatie van de CPE Database in wat betreft IP adres X zou veranderen afhankelijk van welke CPE apparaat laatst een ARP verzoek namens X verstuurde.

In een onbeveiligd DOCSIS-netwerk kan Customer B de volgende hoprouter (in de meeste gevallen de CMTS) ervan overtuigen dat hij het recht heeft om IP adres X te gebruiken door een ARP-verzoek namens X naar de CMTS of de volgende-hop router te verzenden. Dit zou voorkomen dat het verkeer van de dienstverlener naar de klant A wordt doorgestuurd.

Door kabelbron-verify in te schakelen zouden CMTS kunnen zien dat IP- en ARP-pakketten voor IP-adres X afkomstig waren van de verkeerde kabelmodem en daarom zouden deze pakketten worden gedropt, zie Stroomdiagram 2. Dit omvat alle IP-pakketten met bronadres X en ARP-verzoeken namens X. De CMTS-bestanden zouden een bericht langs de lijnen van:

%UBR7200-3-BADIPSOURCE: Interface Cable3/0, IP-pakket uit ongeldige bron. IP=192.168.1.10, MAC=0001.422c.54d0, verwacht SID=10, Feitelijke SID=11



Stroomdiagram 2

Met deze informatie worden beide clients geïdentificeerd en kan de kabelmodem met het aangesloten dubbele IP-adres worden uitgeschakeld.

Voorbeeld 2 - Scenario met dubbele IP-adressen - Hiermee wordt een IP-adres gebruikt dat nog niet gebruikt is

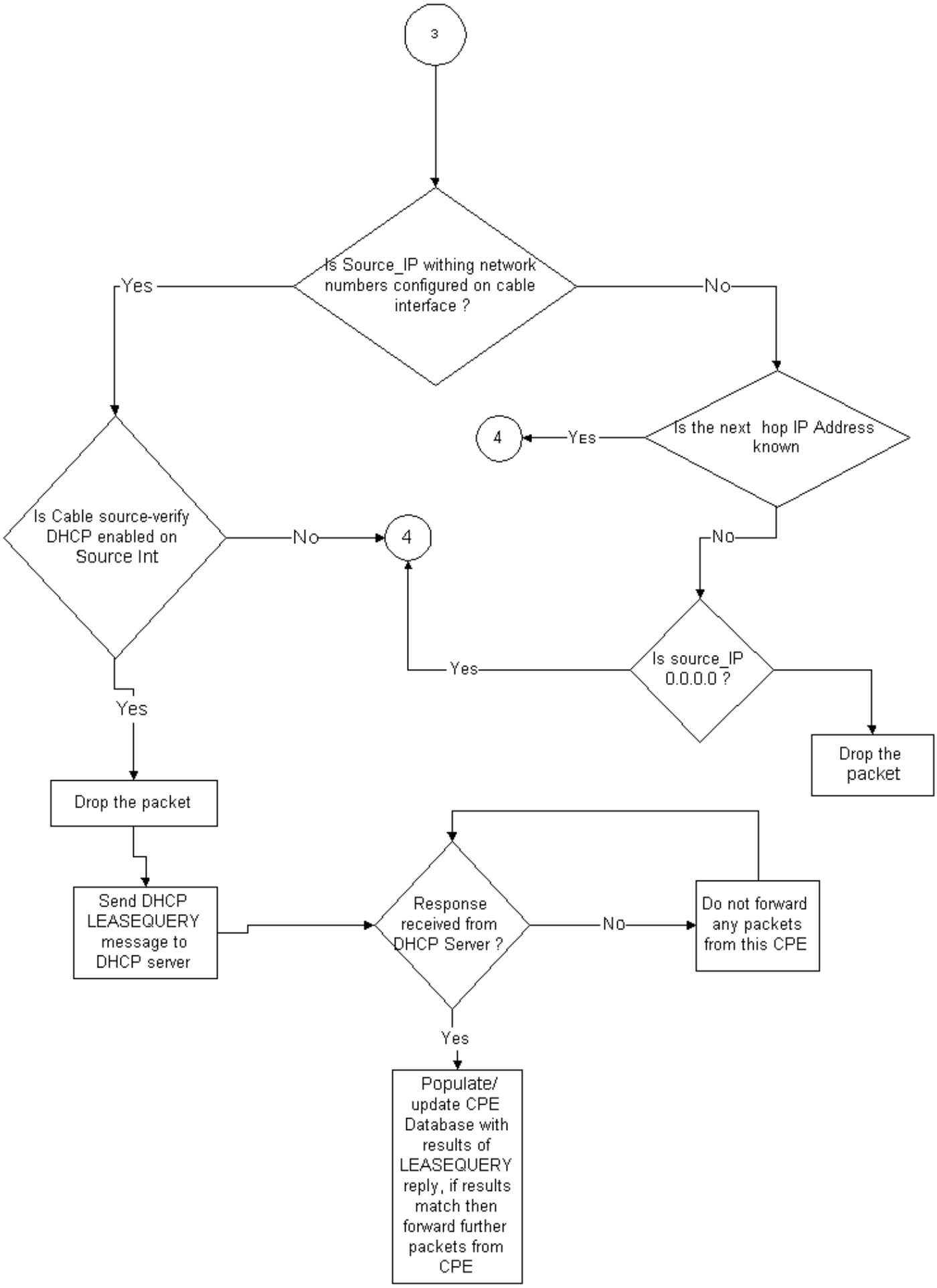
Een ander scenario is voor een gebruiker om statistisch een ongebruikt tot nu toe IP adres aan hun PC toe te wijzen die binnen het legitieme bereik van CPE adressen valt. Dit scenario veroorzaakt geen verstoring van de diensten voor iedereen in het netwerk. Laat ons zeggen dat klant B adres Y voor hun PC heeft toegewezen.

Het volgende probleem dat zich kan voordoen, is dat de klant C zijn werkstation op het netwerk van de serviceprovider kan aansluiten en een DHCP-leaseovereenkomst voor IP-adres Y kan verwerven. De CPE-database zou tijdelijk IP-adres Y aanduiden als een onderdeel van de kabelmodem van de klant. Het kan echter niet lang duren voor Customer B, de niet-legitieme gebruiker de juiste reeks ARP-verkeer verstuurt om de volgende hop ervan te overtuigen dat hij de legitieme eigenaar was van IP-adres Y, waardoor de service van Customer C wordt onderbroken.

Op dezelfde manier kan het tweede probleem worden opgelost door de **kabelbron-verify** in te **zetten**. Wanneer de **bron-verify-**kabel is ingeschakeld kan een CPE Database-ingang die is

gegenereerd door het scannen van details van een DHCP-transactie, niet worden verplaatst door andere soorten IP-verkeer. Alleen een andere DHCP-transactie voor dat IP-adres of de ARP-ingang op de CMTS-timing voor dat IP-adres kan de ingang vervangen. Dit waarborgt dat als een eindgebruiker met succes een DHCP-lease voor een bepaald IP-adres verkrijgt, dat die klant zich geen zorgen hoeft te maken over het feit dat CMTS verward wordt en dat zijn IP-adres aan een andere gebruiker toebehoort.

Het eerste probleem van het stoppen van gebruikers om nog ongebruikte IP adressen te gebruiken kan met **kabelbron-verify dhcp** worden opgelost. Door de dhcp parameter aan het eind van deze opdracht toe te voegen, kan CMTS de geldigheid van elk nieuw bron IP adres controleren waarover het hoort door een speciaal type DHCP-bericht uit te geven dat een LEASEQUERY (een LEASEQUERY-verbinding) wordt genoemd naar de DHCP-server. Zie Stroomdiagram 3.



Stroomdiagram 3

Voor een bepaald CPE IP adres, vraagt het LEASEQUERY-bericht wat het corresponderende adres van MAC en de kabelmodem zijn.

In deze situatie, als Customer B zijn werkstation met het kabelnetwerk verbindt met het statische adres Y, zal CMTS een LEASEQUERY naar de DHCP-server sturen om te controleren of adres Y is geleasd naar de PC van Customer B. De DHCP-server kan CMTS ervan op de hoogte stellen dat geen lease is verleend voor IP-adres Y en dat daarom de klant B geen toegang krijgt.

Voorbeeld 3 - Gebruik van een netwerknummer dat niet door de dienstverlener is bevoorraad

Gebruikers kunnen werkstations achter hun kabelmodems hebben geconfigureerd met statische IP-adressen die mogelijk niet in strijd zijn met de huidige netwerknummers van de serviceproviders, maar die in de toekomst problemen kunnen veroorzaken. Daarom kan een CMTS, met kabelbron-verify, pakketten uit IP-adressen van bron die niet van het bereik zijn gevormd op de kabelinterface van CMTS filteren.

Opmerking: om dit goed te laten werken, moet u ook de **ip verify-**omgekeerde **pad** opdracht configureren om spoofed IP-bronadressen te voorkomen. Raadpleeg Kabelopdrachten: kabel voor meer informatie .

Sommige klanten kunnen een router als een apparaat van CPE hebben en voor de dienstverrichter regelen om verkeer naar deze router te leiden. Als CMTS IP-verkeer van de CPE-router met een bron-IP-adres van Z ontvangt, zal de kabelbron-verify dit pakket doorlaten als CMTS een route naar het netwerk Z heeft behoort tot via dat CPE-apparaat. Raadpleeg grafiek 3.

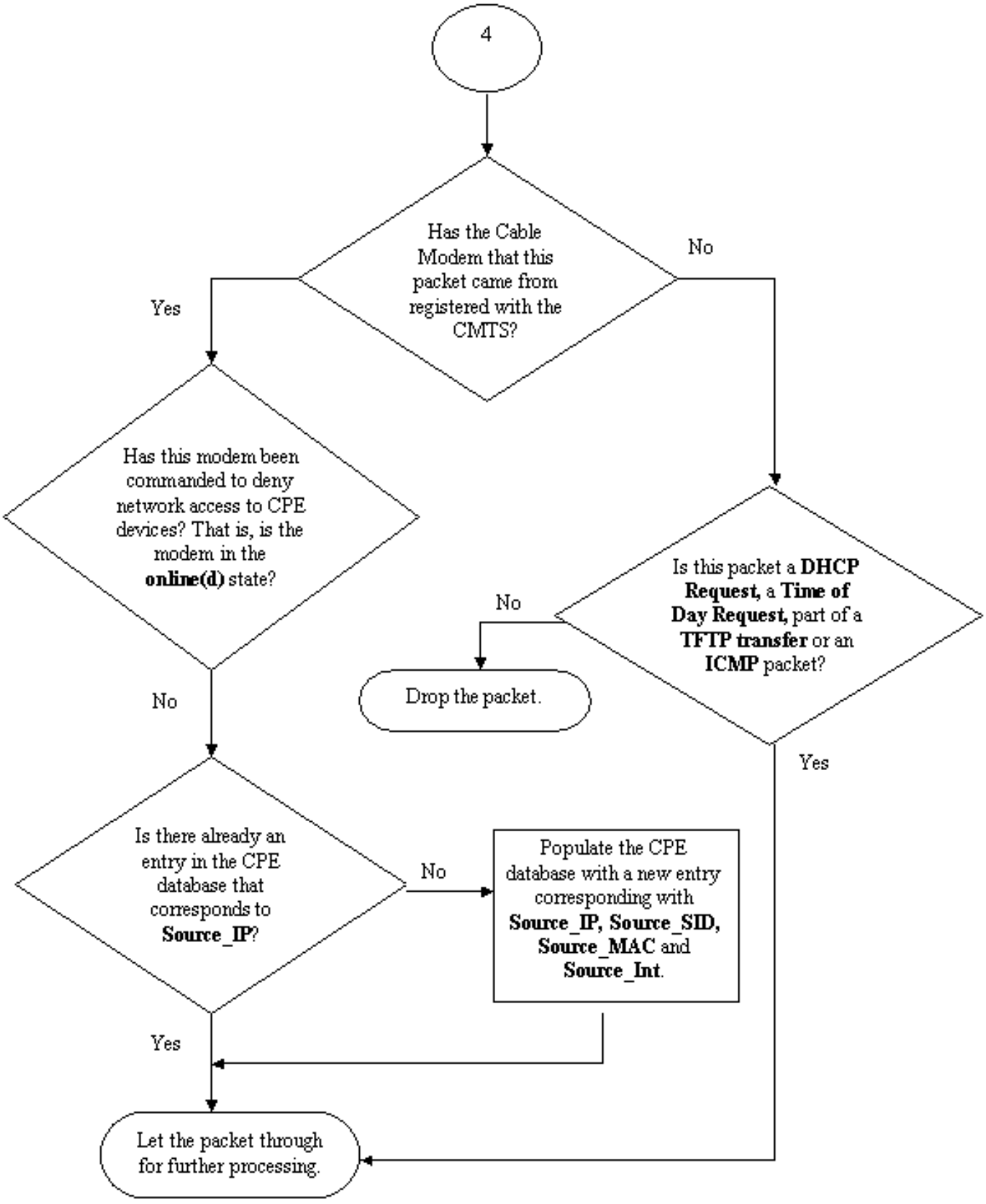
Bekijk nu het volgende voorbeeld:

Op CMTS hebben we de volgende configuratie:

```
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
```

aangenomen dat een pakket met bronIP-adres 172.16.1.10 bij CMTS van kabelmodem 24.2.2.10 is gearriveerd, zou CMTS zien dat 24.2.2.10 niet in de CPE-database verblijft, **toon in kabel x/y modem 0**, **ip verify-reverse-pad** mogelijk Unicast omgekeerd pad doorsturen (Unicast RPF), dat elk pakket controleert dat op een interface wordt ontvangen om te controleren dat het bron IP-adres van het pakket verschijnt in de routingtabellen die aan die interface behoren. De **kabelbron-verify** controleert wat de volgende hop voor 24.2.2.10 is. In de bovenstaande configuratie hebben we **ip-route 24.2.2.0 255.255.255.0 24.1.1.2**, wat betekent dat de volgende hop 24.1.1.2 is. Nu aangenomen dat 24.1.1.2 een geldige vermelding is in de CPE-database, concludeert de CMTS dat het pakket dus en zal het pakket verwerken volgens Flowchart 4.



Stroomdiagram 4

Controleer kabelbron

Het configureren van **kabelbron-verifieert** simpelweg het toevoegen van de **kabelbron-geverifieerde** opdracht aan de kabelinterface die u de functie wilt activeren. Als u kabelinterfacebundeling gebruikt, dan moet u **kabelbron-verify** toevoegen aan de configuratie van

de primaire interface.

Hoe moet u `de kabelbron` configureren, `zoals bijv.`

Opmerking: kabelbron-verify is eerst geïntroduceerd in Cisco IOS-softwarerelease 12.0(7)T en wordt ondersteund in Cisco IOS-softwarereleases 12.0SC, 12.1EC en 12.1T.

Het configureren **van** een **bron-geverifieerde dhcp** vereist een paar stappen.

Zorg ervoor dat uw DHCP-server het speciale DHCP LEASEQUERY-bericht ondersteunt.

Om gebruik te maken van de **kabelbron-verify dhcp-**functionaliteit moet uw DHCP-server reageren op de berichten zoals gespecificeerd door design-ietf-dhcp-leasingapparatuur-XX.txt. Cisco Network Registrar versies 3.5 en hoger kunnen dit bericht beantwoorden.

Zorg ervoor dat uw DHCP-server de verwerking van Relay Agent-informatie ondersteunt. Zie het gedeelte Relay Agent**.**

Een andere functie die moet worden ondersteund door uw DHCP-server is de verwerking van DHCP Relay Information Option. Dit wordt anders optie 82-verwerking genoemd. Deze optie wordt beschreven in DHCP Relay Information Option (RFC 3046). Cisco Network Registrar versies 3.5 en hoger ondersteunen de verwerking van Relay Agent-informatie, maar deze moet worden geactiveerd via het Cisco Network Registrar-hulpprogramma en de volgende volgorde van opdrachten:

nrcmd -U admin -P omschakeling -C 127.0.0.1 dhcp laat save-relais-agent-data toe

nrcmd -U admin -P omschakeling -C 127.0.0.1 behalve

nrcmd -U admin -P omschakeling -C 127.0.0.1 dhcp herlading

Het kan nodig zijn om de juiste gebruikersnaam, het wachtwoord en het IP-adres van de server te vervangen. Het bovenstaande toont de standaardwaarden. Als u in de nrcmd-melding bent, typt u ook het volgende:

dhcp maakt save-relais-agent-data mogelijk

opslaan

herladen van dhcp

Schakel de optie DHCP-relais in door op CMTS te verwerken.

Relay-agent

CMTS moet DHCP-verzoeken van Kabelmodems en CPE met de optie Relay Agent-informatie taggen **zodat** dhcp **van kabelbron** effectief is. De volgende opdrachten moeten in de mondiale configuratiemodus zijn ingevoerd via een CMTS-systeem met Cisco IOS-softwarereleases 12.1EC, 12.1T of hoger versies van Cisco IOS.

optie informatie over ip-dhcp

Als uw CMTS Cisco IOS-softwarereleases 12.0SC uitvoert, trad Cisco IOS op dan gebruikt u de opdracht **kabelrelais-agent-optie** kabelinterface in plaats daarvan.

Wees voorzichtig met het gebruik van de juiste opdrachten, afhankelijk van de versie van Cisco IOS die u uitvoert. Zorg ervoor om uw configuratie bij te werken als u treinen van Cisco IOS wijzigt.

De opdrachten **van de** informatie-**uitwisseling** van **relais** voegen een speciale optie, Optie 82 genoemd, of de optie van de relais informatie, toe aan het doorgevoerde DHCP-pakket wanneer de CMTS DHCP-pakketten afbreekt.

Optie 82 is bevolkt met een suboptie, de Agent Circuit-ID, die de fysieke interface op CMTS verwijst waarop het DHCP-verzoek werd gehoord. Daarnaast is er een andere suboptie, de Agent Remote ID, bevolkt met het 6 bytes MAC-adres van de kabelmodem dat het DHCP-verzoek is ontvangen of doorgestuurd.

Dus als een PC met MAC-adres 99:88:77:66:55:44 achter kabelmodems a.b:cc:dd:ee:ff een DHCP-verzoek verstuurt, zal CMTS het DHCP-verzoek doorsturen om de Agent Remote ID-suboptie van optie 82 in te stellen op het MAC-adres van de Cable Modem, a:bb:cc dd:zie:ff.

Door de optie Relay Information opgenomen in het DHCP-verzoek van een CPE-apparaat te hebben, kan de DHCP-server informatie opslaan over welke CPE behoort achter welke kabelmodems. Dit wordt in het bijzonder nuttig wanneer **kabelbron-verify-**dhcp op CMTS is ingesteld, omdat de DHCP-server de CMTS betrouwbaar kan informeren over wat het MAC-adres van een bepaalde client moet hebben, maar op welke kabelmodemclient een bepaalde client moet worden aangesloten.

Schakel het dhcp-opdracht van de kabelbron in onder de juiste kabelinterface.

De laatste stap is het **dhcp-**opdracht van de **kabelbron** in te voeren onder de kabelinterface waarop u de functie wilt activeren. Als CMTS kabelinterfacebundeling gebruikt, moet u de opdracht onder de primaire interface van de bundel invoeren.

Conclusie

Met de opdrachten **voor** de **kabelbron** en de eigenschappen van de opdrachten kan een serviceprovider het kabelnetwerk beveiligen tegen gebruikers met onbevoegde IP-adressen om het netwerk te gebruiken.

De kabel bron-verifieer opdracht op zichzelf is een effectieve en gemakkelijke manier om IP adresveiligheid uit te voeren. Hoewel het niet alle scenario's bestrijkt, zorgt het bij lease ervoor dat klanten met het recht om toegewezen IP-adressen te gebruiken, geen verstoringen zullen ondervinden door hun IP-adres door iemand anders te laten gebruiken.

In zijn eenvoudigste vorm zoals in dit document beschreven, kan een CPE-apparaat dat niet via DHCP is geconfigureerd geen toegang tot het netwerk verkrijgen. Dit is de beste manier om IP-adresruimte te beveiligen en de stabiliteit en betrouwbaarheid van een Data over Cable-service te vergroten. Meervoudige dienstenexploitanten (MSO's) die commerciële diensten hebben verleend die van hen verlangden statische adressen te gebruiken, wilden echter een strikte beveiliging van de **door de opdrachtbron geverifieerde dhcp** implementeren.

Versie 5.5 van de Cisco Network Registrar heeft een nieuwe mogelijkheid om te reageren op de

lease-vraag voor "gereserveerde" adressen, ook al is het IP-adres niet via DHCP verkregen. De DHCP-server bevat leasereserveringsgegevens in de DHCP-respons. In de voorgaande releases van netwerkregisters waren de reacties van DHCPLEASEQUERY alleen mogelijk voor gehuurde of eerder geleasede klanten waarvoor het MAC-adres was opgeslagen. Cisco uBR relais agenten, bijvoorbeeld, kunt DHCPLEASEQUERY-datagrammen weggooien zonder een MAC-adres en -leasetijd (dhcp-lease-time optie).

Met een NH-respons geeft de netwerkregistrator een standaardleasetijd van één jaar (31536000 seconden) terug voor gereserveerde leaseovereenkomsten. Als het adres daadwerkelijk geleased is, retourneert de netwerkregistrator de resterende leasetijd.

Gerelateerde informatie

- DHCP Relay Information Option (RFC 3046)
- Technische ondersteuning en documentatie – Cisco Systems