케이블 소스 확인 및 IP 주소 보안

목차

소개

Cisco는 DOCSIS(Data-over-Cable Service Interface Specifications) 케이블 시스템의 IP 주소 스푸핑 및 IP 주소 도용을 기반으로 특정 유형의 서비스 거부 공격을 금지하는 Cisco CMTS(Cable Modem Termination System) 제품 내에서 향상된 기능을 구현했습니다.Cisco CMTS Cable Command Reference에서는 이러한 IP 주소 보안 개선 사항**의** 일부인 케이블 소스 **검증** 명령 제품군에 대해 설명합니다.

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

보호되지 않은 DOCSIS 환경

DOCSIS MAC(Media Access Control) 도메인은 기본적으로 이더넷 세그먼트와 유사합니다.보호되지 않은 상태로 두면 세그먼트의 사용자가 서비스 거부 공격을 기반으로 하는 여러 유형의 레이어 2 및 레이어 3 공격에 취약해집니다.또한 다른 사용자의 장비에 대한 주소 지정이 잘못 구성되어 사용자가 서비스 수준이 저하될 수 있습니다.예를 들면 다음과 같습니다.

- 다른 노드에서 중복 IP 주소를 구성하는 중입니다.
- 여러 노드에서 중복 MAC 주소를 구성하는 중입니다.
- DHCP(Dynamic Host Configuration Protocol)가 할당한 IP 주소가 아닌 고정 IP 주소를 무단으로 사용하는 경우
- 세그먼트 내에서 서로 다른 네트워크 번호의 무단 사용.
- 세그먼트 IP 서브넷의 일부를 대신하여 ARP 요청에 응답하도록 엔드 노드를 잘못 구성합니다.

이러한 유형의 문제는 물리적으로 문제의 장비를 추적하여 이더넷 LAN 환경에서 제어하고 완화하기 쉽지만, DOCSIS 네트워크의 이러한 문제는 네트워크의 규모가 클 수 있으므로 격리, 해결 및 방지가 어려울 수 있습니다.또한 CPE(Customer Premise Equipment)를 제어하고 구성하는 최종 사용자는 로컬 IS 지원 팀의 혜택을 받지 못할 수 있으며, 해당 워크스테이션 및 PC가 의도적이거나 의도적이지 않게 잘못 구성되어 있지 않은지 확인할 수 있습니다.

CMTS CPE 데이터베이스

Cisco CMTS 제품군은 연결된 CPE IP 및 MAC 주소로 구성된 동적으로 채워진 내부 데이터베이스를 유지합니다.CPE 데이터베이스에는 이러한 CPE 디바이스가 속한 해당 케이블 모뎀에 대한 세부 정보도 포함되어 있습니다.

숨겨진 CMTS 명령 **show interface cable X/Y modem Z**를 실행하여 특정 케이블 모뎀에 해당하는 CPE 데이터베이스의 부분 보기를 볼 수 있습니다. 여기서 X는 라인 카드 번호이고, Y는 다운스트림 포트 번호이고 Z는 케이블 모뎀의 SID(서비스 식별자)입니다.특정 다운스트림 인터페이스의 모든 케이블 모뎀 및 CPE에 대한 세부 정보를 보려면 Z를 0으로 설정할 수 있습니다.이 명령으로 생성된 일반적인 출력의 예는 아래 예를 참조하십시오.

```
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
```

참고: 이 명령은 숨겨져 있으므로 변경될 수 있으며 Cisco IOS® 소프트웨어의 모든 릴리스에서 사용할 수 있다고 보장되지 않습니다.

위의 예에서 IP 주소가 192.168.1.90인 호스트의 method 열은 dhcp로 나열됩니다.즉, CMTS가 호스트와 서비스 제공자의 DHCP 서버 간의 DHCP 트랜잭션을 관찰하여 이 호스트에 대해 알게 되었습니다.

IP 주소가 192.168.1.77인 호스트는 메서드 정적으로 나열됩니다.이는 CMTS가 이 디바이스와 DHCP 서버 간의 DHCP 트랜잭션을 통해 이 호스트에 대해 처음 학습하지 않았음을 의미합니다.대신 CMTS는 이 호스트에서 다른 종류의 IP 트래픽을 처음으로 확인했습니다.이 트래픽은 웹 브라우징, 이메일 또는 "ping" 패킷일 수 있습니다.

192.168.1.77이 고정 IP 주소로 구성된 것처럼 보일 수 있지만, 이 호스트가 실제로 DHCP 임대를 획득했을 수 있지만 이벤트 이후 CMTS가 리부팅되어 트랜잭션이 기억나지 않을 수 있습니다.

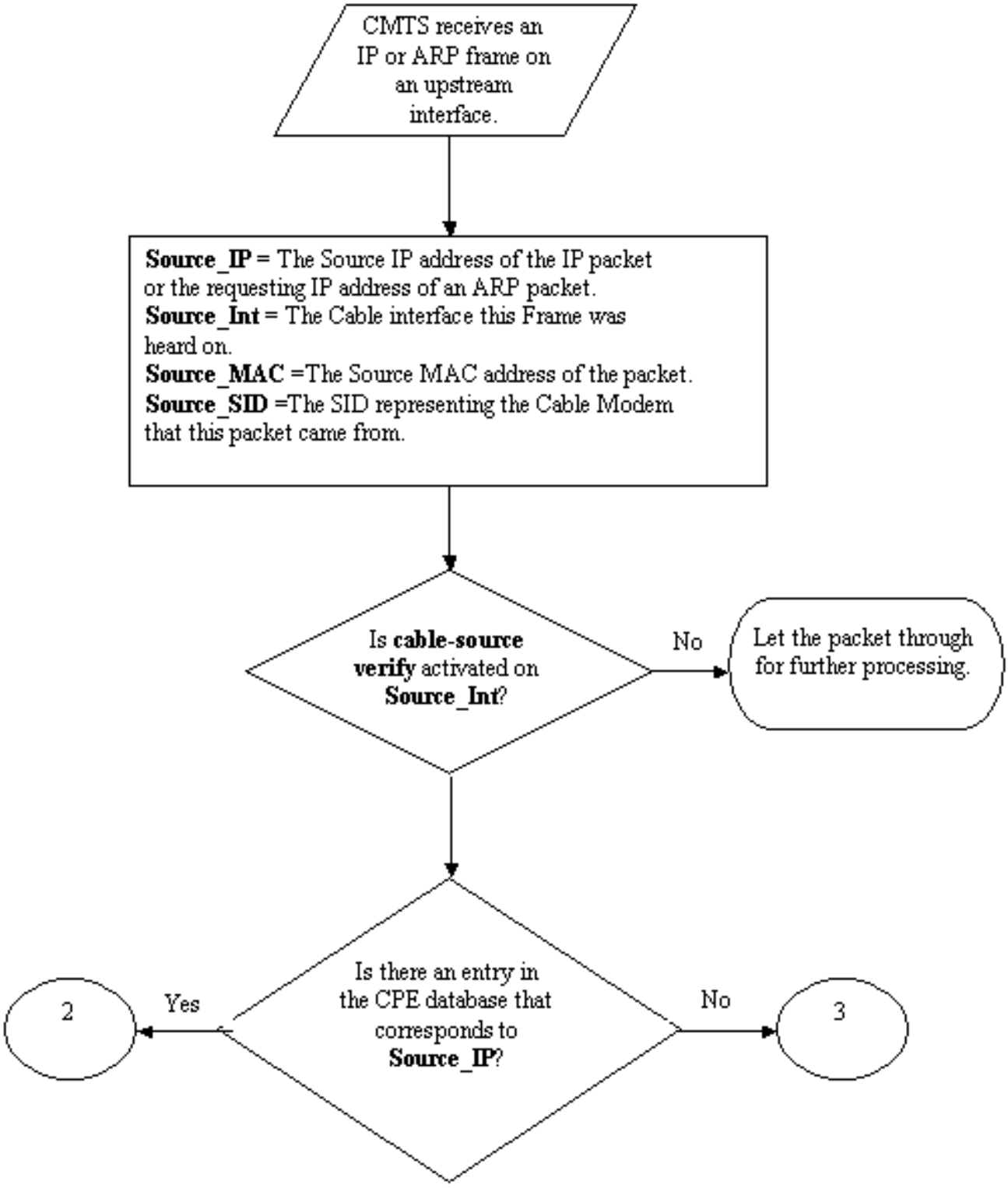
CPE 데이터베이스는 일반적으로 CPE 디바이스와 서비스 공급자의 DHCP 서버 간의 DHCP 트랜

잭션에서 CMTS gigning 정보로 채워집니다.또한 CMTS는 어떤 CPE IP 및 MAC 주소가 어떤 케이블 모뎀에 속하는지 확인하기 위해 CPE 디바이스에서 오는 다른 IP 트래픽을 수신할 수 있습니다.

케이블 소스 검증 명령

Cisco는 케이블 인터페이스 명령 케이블 source-verify [dhcp]를 구현했습니다.이 명령을 사용하면 CMTS는 CPE 데이터베이스를 사용하여 CMTS가 케이블 인터페이스에서 수신하는 IP 패킷의 유효성을 확인하고 CMTS가 이를 전달할지 여부에 대한 지능적인 결정을 내릴 수 있습니다.

아래 순서도는 CMTS를 계속 진행하려면 케이블 인터페이스에서 수신한 IP 패킷이 거쳐야 하는 추가 처리를 보여줍니다.



순서도 1

흐름도는 CMTS의 업스트림 포트에서 수신되는 패킷으로 시작하고 추가 처리를 위해 또는 삭제되는 패킷에서 패킷이 계속 진행될 수 있도록 허용합니다.

예 1 - 중복 IP 주소가 있는 시나리오

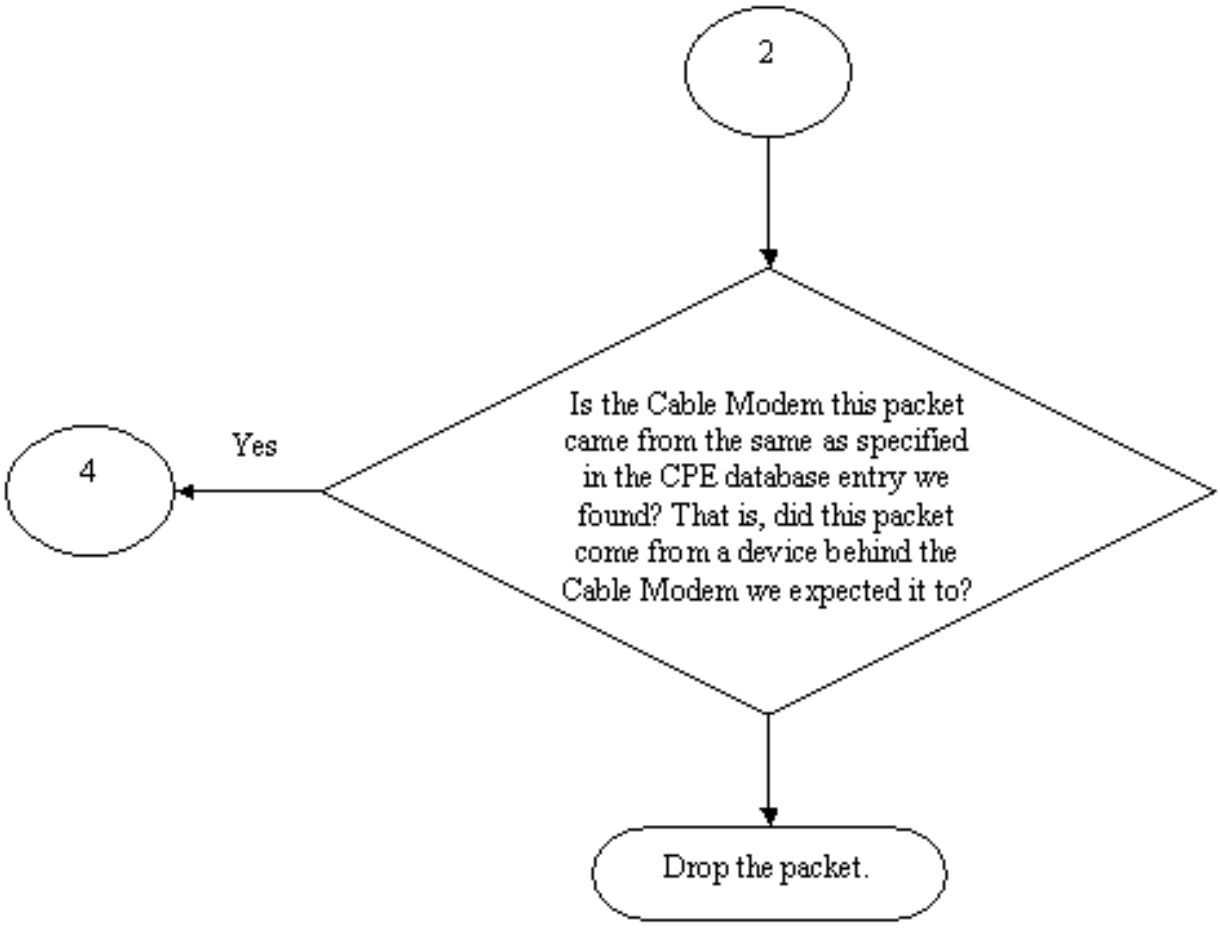
첫 번째 Denial of Service 시나리오는 중복 IP 주소와 관련된 상황입니다.고객 A가 서비스 공급자에 연결되어 있으며 PC에 대해 유효한 DHCP 임대를 받았다고 가정해 보겠습니다.Customer A가 얻은 IP 주소를 X라고 합니다.

A가 DHCP 임대를 취득한 후 고객 B는 현재 고객 A의 장비에서 사용되고 있는 것과 동일한 고정 IP 주소로 PC를 구성하기로 합니다.IP 주소 X와 관련된 CPE 데이터베이스 정보는 X 대신 마지막으로 ARP 요청을 보낸 CPE 디바이스에 따라 달라집니다.

보호되지 않는 DOCSIS 네트워크에서 Customer B는 X 대신 ARP 요청을 CMTS 또는 next-hop 라우터로 전송하여 IP 주소 X를 사용할 수 있는 권한이 있는 다음 hop 라우터(대부분의 경우 CMTS)를 설득할 수 있습니다.이렇게 하면 통신 사업자의 트래픽이 고객 A로 전달되지 않습니다.

케이블 소스 확인을 활성화하면 CMTS에서 IP 주소 X에 대한 IP 및 ARP 패킷이 잘못된 케이블 모뎀에서 소싱되고 있음을 확인할 수 있으므로 이러한 패킷은 삭제될 수 있습니다(순서도 2 참조). 여기에는 소스 주소 X와 ARP 요청이 있는 모든 IP 패킷이 X를 대신하여 포함됩니다. CMTS 로그에는 다음 라인에 대한 메시지가 표시됩니다.

%UBR7200-3-BADIPSOURCE:인터페이스 케이블 3/0, 잘못된 소스의 IP 패킷.IP=192.168.1.10, MAC=0001.422c.54d0, 예상 SID=10, 실제 SID=11



순서도 2

이 정보를 사용하여 두 클라이언트를 모두 식별하고 연결된 중복 IP 주소가 있는 케이블 모뎀을 비활성화할 수 있습니다.

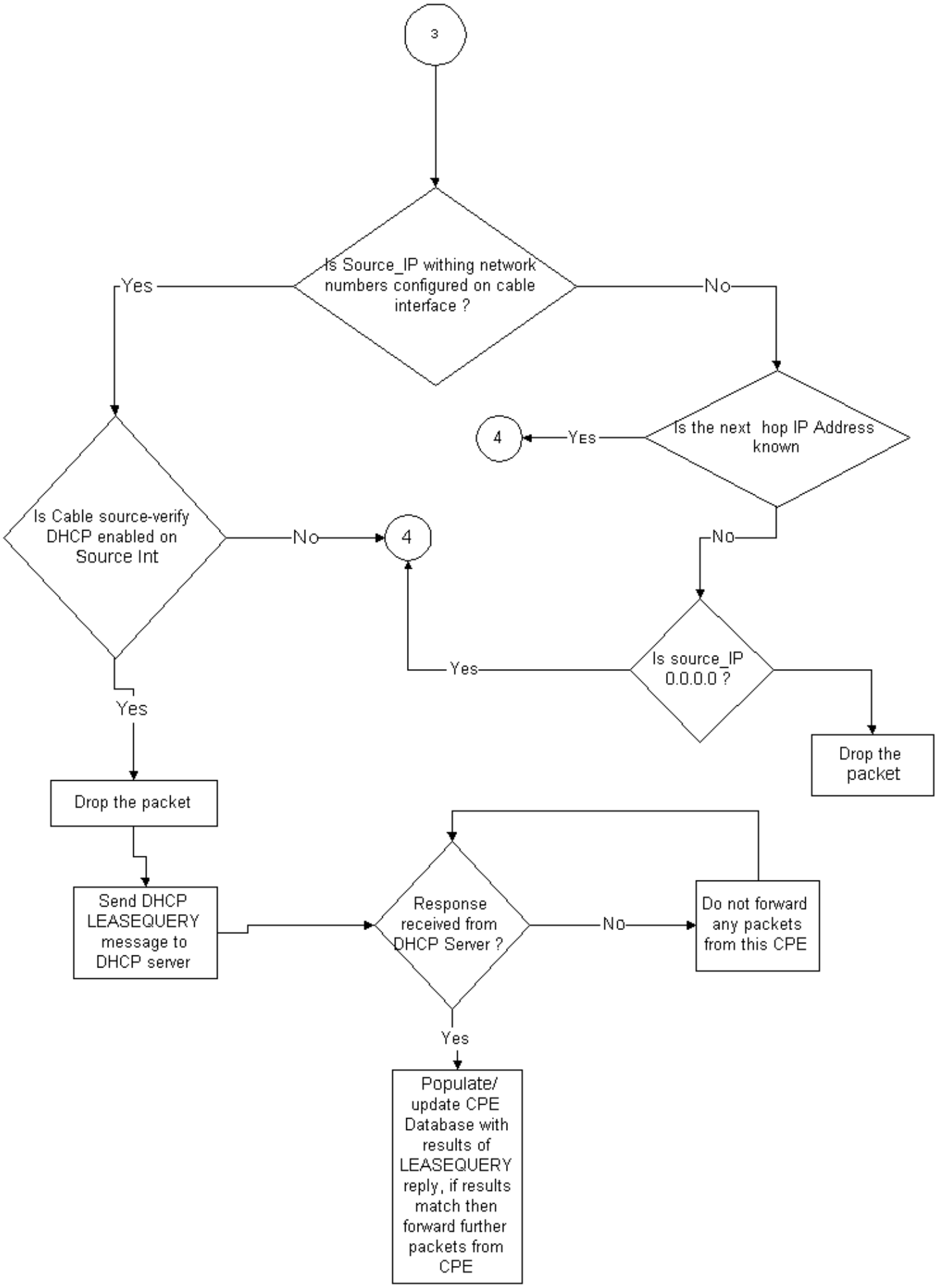
예 2 - 중복 IP 주소가 있는 시나리오 - 아직 사용되지 않은 IP 주소 사용

또 다른 시나리오는 사용자가 PC에 아직 사용되지 않은 IP 주소를 정적으로 할당하여 CPE 주소의 합법적인 범위에 속한다는 것입니다.이 시나리오에서는 네트워크의 모든 사용자에게 서비스가 중단되지 않습니다.고객 B가 PC에 주소 Y를 할당했다고 가정해 보겠습니다.

다음 문제는 고객 C가 자신의 워크스테이션을 서비스 공급자의 네트워크에 연결하고 IP 주소 Y에 대한 DHCP 임대를 획득할 수 있다는 것입니다. CPE 데이터베이스는 일시적으로 IP 주소 Y를 고객 C의 케이블 모뎀 뒤에 속하는 것으로 표시합니다.그러나 Customer B가 Y라는 IP 주소 Y의 합법적인 소유자라는 사실을 확신시키기 위해 비합법적인 사용자가 적절한 ARP 트래픽 시퀀스를 전송하여 Customer C의 서비스가 중단되는 날이 얼마 남지 않았습니다.

마찬가지로, 두 번째 문제는 **케이블 소스 확인**을 켜서 해결할 수 있습니다.**케이블 소스 검증**이 켜지면 DHCP 트랜잭션의 세부 정보를 취합하여 생성된 CPE 데이터베이스 항목은 다른 종류의 IP 트래픽으로 대체될 수 없습니다.해당 IP 주소에 대한 다른 DHCP 트랜잭션 또는 해당 IP 주소에 대한 CMTS 타이밍 아웃의 ARP 항목만 항목을 대체할 수 있습니다.이렇게 하면 최종 사용자가 지정된 IP 주소에 대한 DHCP 임대를 성공적으로 획득할 경우, CMTS가 혼란스러워지고 자신의 IP 주소가 다른 사용자의 것으로 간주되는 것에 대해 고객은 걱정할 필요가 없습니다.

사용자가 아직 사용하지 않은 IP 주소를 사용하지 못하도록 막는 첫 번째 문제는 **케이블 소스 확인 dhcp**를 사용하여 해결할 수 있습니다.CMTS는 이 명령의 끝에 dhcp 매개변수를 추가하여 DHCP 서버에 LEASEQUERY라는 특수 유형의 DHCP 메시지를 발행함으로써 새로운 소스 IP 주소의 유효성을 확인할 수 있습니다.순서도 3을 참조하십시오.


3
Is Source_IP withing network numbers configured on cable interface ?
Yes
No
Is Cable source-verify DHCP enabled on Source Int
No
4
Yes
Drop the packet
Send DHCP LEASEQUERY message to DHCP server
Response received from DHCP Server ?
No
Do not forward any packets from this CPE
Yes
Populate/ update CPE Database with results of LEASEQUERY reply, if results match then forward further packets from CPE
Is the next hop IP Address known
4
Yes
No
Is source_IP 0.0.0.0 ?
Yes
Drop the packet

순서도 3

지정된 CPE IP 주소의 경우 LEASEQUERY 메시지가 해당 MAC 주소와 케이블 모뎀이 무엇인지 묻습니다.

이 경우 고객 B가 정적 주소 Y를 사용하여 워크스테이션을 케이블 네트워크에 연결할 경우 CMTS는 DHCP 서버에 LEASEQUERY를 보내 주소 Y가 고객 B의 PC에 임대한 것인지 확인합니다 .DHCP 서버는 CMTS에 IP 주소 Y에 대한 리스가 부여되지 않았으므로 고객 B에 액세스가 거부됨을 알릴 수 있습니다.

예 3 - 서비스 공급자가 프로비저닝하지 않은 네트워크 번호 사용

사용자가 케이블 모뎀 뒤에 고정 IP 주소를 사용하여 워크스테이션을 구성했을 수 있습니다. 이 주소는 통신 사업자의 현재 네트워크 번호와 충돌하지 않지만 향후 문제가 발생할 수 있습니다.따라서 CMTS는 케이블 소스 검증을 사용하여 CMTS의 케이블 인터페이스에 구성된 범위에서 벗어난 소스 IP 주소에서 오는 패킷을 필터링할 수 있습니다.

참고: 이 작업이 제대로 작동하려면 스푸핑된 IP 소스 주소를 방지하기 위해 **ip verify unicast reverse-path** 명령도 구성해야 합니다.자세한 내용은 케이블 명령:케이블을 통해 자세한 정보를 확인할 수 있습니다.

일부 고객은 라우터를 CPE 디바이스로 사용하고 통신 사업자가 이 라우터로 트래픽을 라우팅하도록 할 수 있습니다.CMTS가 소스 IP 주소가 Z인 CPE 라우터에서 IP 트래픽을 수신하면 CMTS가 해당 CPE 디바이스를 통해 네트워크 Z에 속한 경로가 있는 경우 케이블 소스 검증에서 이 패킷을 통과시킵니다.순서도 3을 참조하십시오.

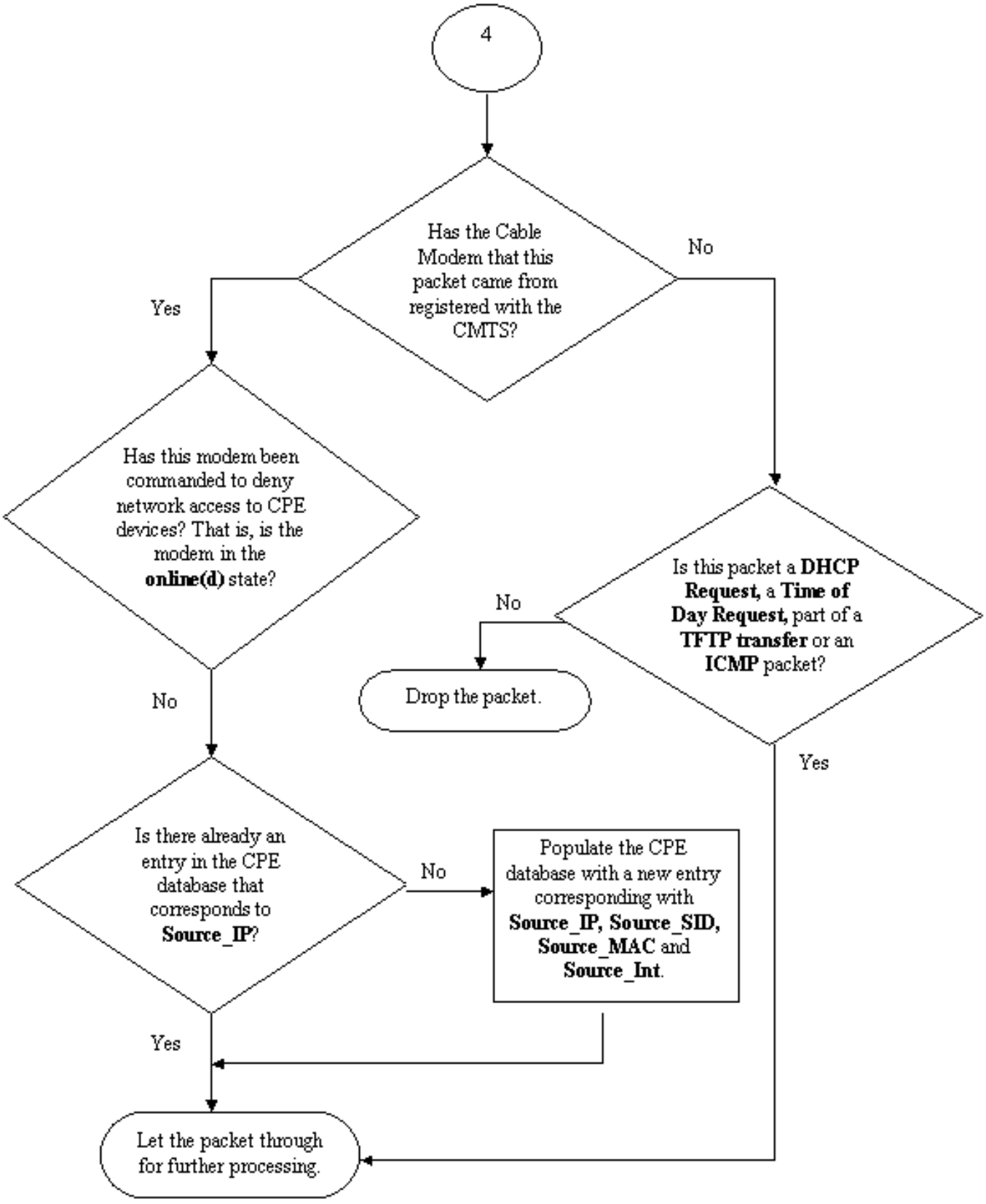
이제 다음 예를 고려하십시오.

CMTS에서는 다음 컨피그레이션을 제공합니다.

```
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
```

소스 IP 주소가 172.16.1.10인 패킷이 케이블 모뎀 24.2.2.10에서 CMTS에 도착했다고 가정할 때 CMTS는 24.2.2.10이 CPE 데이터베이스에 없는 것을 확인하고 **show int cable x/y modem 0**을 표시하지만 **ip verify unicast reverse-path**는 인터페이스에서 수신한 각 패킷을 확인하는 Unicast Reverse Path Forwarding(Unicast RPF)를 활성화합니다. 이. 그러면 해당 패킷의 소스 IP 주소가 해당 라우팅 테이블에 속하는지 확인합니다.**케이블** source-**verify**는 24.2.2.10에 대한 다음 홉이 무엇인지 확인합니다.위의 컨피그레이션에는 **ip 경로 24.2.2.0 24.1.1.2가 있습니다**. 즉 다음 홉이 24.1.1.2입니다. 이제 24.1.1.2이 CPE 데이터베이스의 유효한 항목이라고 가정하면 CMTS는 패킷이 OK라고 간주하고 Flowchart 4에 따라 패킷을 처리합니다.



순서도 4

케이블 소스 확인 구성 방법

케이블 소스 검증 구성은 기능을 활성화하려는 **케이블** 인터페이스에 **케이블** source-verify 명령을 추가하는 것뿐입니다.케이블 인터페이스 번들링을 사용하는 경우 기본 인터페이스의 컨피그레이션에 **케이블 소스 검증**을 추가해야 합니다.

dhcp를 구성하는 방법

참고: 케이블 source-verify는 Cisco IOS Software 릴리스 12.0(7)T에서 처음 도입되었으며 Cisco IOS Software 릴리스 12.0SC, 12.1EC 및 12.1T에서 지원됩니다.

케이블 소스 확인 dhcp를 구성하려면 몇 단계가 필요합니다.

DHCP 서버가 특수 DHCP LEASEQUERY 메시지를 지원하는지 확인합니다.

케이블 소스 확인 dhcp 기능을 사용하려면 DHCP 서버가 draft-ietf-dhcp-leasequery-XX.txt에 지정된 대로 메시지에 응답해야 합니다.Cisco Network Registrar 버전 3.5 이상은 이 메시지에 응답할 수 있습니다.

DHCP 서버가 릴레이 에이전트 정보 옵션 처리를 지원하는지 확인합니다.릴레이 에이전트 섹션을 참조하십시오.

DHCP 서버에서 지원해야 하는 또 다른 기능은 DHCP 릴레이 정보 옵션 처리입니다.이를 Option 82 프로세싱이라고 합니다.이 옵션은 DHCP 릴레이 정보 옵션(RFC 3046)에 설명되어 있습니다. Cisco Network Registrar 버전 3.5 이상은 Relay Agent Information Option 처리를 지원하지만 다음 명령 시퀀스와 함께 Cisco Network Registrar 명령줄 유틸리티 nrcmd를 통해 활성화해야 합니다.

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 저장

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

적절한 사용자 이름, 비밀번호 및 서버 IP 주소로 대체해야 할 수 있습니다. 위의 에는 기본값이 표시됩니다.또는 nrcmd 프롬프트에 있는 경우 >nrcmd를 입력하면 됩니다.

dhcp enable save relay-agent-data

저장

dhcp reload

CMTS에서 DHCP 릴레이 정보 옵션 처리를 설정합니다.

릴레이 에이전트

케이블 소스에서 dhcp를 유효하게 확인하려면 CMTS가 케이블 모뎀 및 CPE의 DHCP 요청에 릴레이 에이전트 정보 옵션을 태그해야 합니다.다음 명령은 Cisco IOS Software Releases 12.1EC, 12.1T 이상 버전의 Cisco IOS를 실행하는 CMTS에서 글로벌 컨피그레이션 모드에서 입력해야 합니다.

ip dhcp 릴레이 정보 옵션

CMTS에서 Cisco IOS Software Releases 12.0SC를 실행하는 경우 Cisco IOS를 교육하려면 **케이블 릴레이 에이전트 옵션** 케이블 인터페이스 명령을 대신 사용합니다.

실행 중인 Cisco IOS의 버전에 따라 적절한 명령을 사용해야 합니다.Cisco IOS의 기차를 변경할 경우 컨피그레이션을 업데이트해야 합니다.

relay **information option 명령**은 CMTS가 DHCP 패킷을 릴레이할 때 릴레이된 DHCP 패킷에 Option 82라는 특수 옵션 또는 릴레이 정보 옵션을 추가합니다.

옵션 82는 DHCP 요청이 수신되는 CMTS의 물리적 인터페이스를 참조하는 하위 옵션인 Agent Circuit-ID로 채워집니다.또한 다른 하위 옵션인 Agent Remote ID는 DHCP 요청이 수신되거나 전달된 케이블 모뎀의 6바이트 MAC 주소로 채워집니다.

예를 들어, 케이블 모뎀 뒤에 있는 MAC 주소가 99:88:77:66:55:44인 PC가 DHCP 요청을 전송하는 경우, CMTS는 옵션 82의 에이전트 원격 ID 하위 옵션 설정 DHCP 요청을 케이블 모뎀의 MAC 주소, aa:bb:cc:dd:ee:ff:ff로 전달합니다.

CPE 디바이스의 DHCP 요청에 Relay Information Option이 포함되어 있으면 DHCP 서버는 어떤 CPE가 어떤 케이블 모뎀 뒤에 속하는지에 대한 정보를 저장할 수 있습니다.이 기능은 DHCP 서버가 CMTS에 **케이블 소스 확인 dhcp**를 구성할 때 특히 유용합니다. DHCP 서버는 특정 클라이언트가 가져야 할 MAC 주소뿐만 아니라 연결할 케이블 모뎀 특정 클라이언트에 대해서도 CMTS에 안정적으로 알릴 수 있기 때문입니다.

적절한 케이블 인터페이스에서 케이블 source-verify dhcp 명령을 활성화합니다.

마지막 단계에서는 **케이블** 인터페이스 아래에 **케이블 source-verify dhcp** 명령을 입력하여 피쳐를 활성화합니다.CMTS에서 케이블 인터페이스 번들링을 사용하는 경우 번들의 기본 인터페이스 아래에 명령을 입력해야 합니다.

결론

케이블 source-verify 명령 모음을 사용하면 서비스 공급자가 무단 IP 주소가 있는 사용자로부터 네트워크를 사용하여 케이블 네트워크를 보호할 수 있습니다.

케이블 source-verify 명령 자체는 IP 주소 보안을 구현하는 효과적이고 쉬운 방법입니다.모든 시나리오는 다루지 않지만 할당된 IP 주소를 사용할 수 있는 권한이 있는 고객은 다른 사용자가 자신의 IP 주소를 사용하면서 어떠한 장애도 발생하지 않도록 해야 합니다.

이 문서에서 설명한 것처럼 가장 간단한 형식으로 DHCP를 통해 구성되지 않은 CPE 디바이스는 네트워크 액세스를 얻을 수 없습니다.이는 IP 주소 공간을 보호하고 Data over Cable 서비스의 안정성과 안정성을 높이는 가장 좋은 방법입니다. 그러나 MSO(Service Operators)가 여러 개이며, 이 서비스 때문에 고정 주소를 사용해야 했습니다. 이 서비스 운영자는 명령 **케이블 source-verify dhcp**의 엄격한 보안을 구현하고자 했습니다.

Cisco Network Registrar 버전 5.5는 DHCP를 통해 IP 주소를 얻지 못한 경우에도 "예약된" 주소에 대한 리스 쿼리에 응답하는 새로운 기능을 제공합니다. DHCP 서버에는 DHCPLENEQUERY 응답에 임대 예약 데이터가 포함됩니다.Network Registrar의 이전 릴리스에서는 DHCPLENEQUERY 응답이 MAC 주소가 저장된 임대 또는 이전에 임대한 클라이언트에만 가능합니다.예를 들어 Cisco uBR 릴레이 에이전트는 MAC 주소 및 리스 시간이 없는 DHCPLEERY 데이터그램을 삭제합니다(dhcp-lease-time 옵션).

Network Registrar는 DHCPLEERY 응답에서 예약된 임대에 대해 1년(31536000초)의 기본 임대 시간을 반환합니다.주소가 실제로 임대한 경우 Network Registrar는 나머지 임대 시간을 반환합니다.

관련 정보

- DHCP 릴레이 정보 옵션(RFC 3046)

- 기술 지원 및 문서 – Cisco Systems