ケーブルソース - 確認およびIP アドレスセキュリティ

内容

概要

シスコでは、Cisco Cable Modem Termination System（CMTS; ケーブル モデム終端システム）製品に、IP アドレスのスプーフィングに基づくある種のサービス拒絶攻撃と、Data-over-Cable Service Interface Specifications（DOCSIS）ケーブル システムでの IP アドレスの盗用を阻止する改良を実装しています。『Cisco CMTSケーブルコマンドリファレンス』では、これらのIPアドレスのセキュリティ強化の一部であるcable source-verifyコマンド群について説明しています。

はじめに

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

前提条件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

無防備なDOCSIS 環境

DOCSIS Media Access Control（MAC; メディア アクセス制御）ドメインは、本質的にイーサネット セグメントに似ています。保護せずに放置しておくと、セグメント内のユーザはレイヤ 2 およびレイヤ 3 アドレッシング ベースの各種サービス拒絶攻撃に対して無防備になります。また、他のユーザの機器でのアドレス設定の不良が原因で、サービス レベルが低下するおそれもあります。具体的には、次のような設定不良が考えられます。

- 異なるノードでの重複した IP アドレスの設定
- 異なるノードでの重複した MAC アドレスの設定
- Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）によって割り当てられた IP アドレスではなく、スタティックな IP アドレスの不正使用
- 同一セグメント内での異なるネットワーク番号の不正使用
- エンド ノードが適切に設定されていないため、そのエンド ノードがセグメントの IP サブネット部分の ARP 要求に応答する

この種の問題は、イーサネット LAN 環境では問題の機器を物理的に突き止めて取りはずすことにより、容易に解決できますが、DOCSIS ネットワークではネットワークのサイズが潜在的に大きいため、問題を切り離したり、解決、防止したりすることが難しい場合があります。また、Customer Premise Equipment（CPE; 顧客宅内機器）を操作および設定しているエンド ユーザがローカルの IS サポート チームのサポートを受けられず、自分のワークステーションおよび PC が、故意にせよ過失にせよ、正しく設定されていないことを確認できない場合もあります。

CMTS CPE データベース

シスコの CMTS 製品群は、接続された CPE の IP アドレスと MAC アドレスが動的に入力された内部データベースを保持しています。CPE データベースにも、これらの CPE デバイスが属するケーブル モデムの詳細情報が格納されています。

隠しコマンド**show interface cable X/Y modem Z**を実行すると、特定のケーブルモデムに対応するCPEデータベースの一部が表示されます。ここで、Xはラインカード番号、Yはダウンストリームポート番号、Zはケーブルモデムのサービス識別子(SID)です。Z を 0 に設定すると、特定のダウンストリーム インターフェイス上にあるすべてのケーブル モデムと CPE についての詳細情報が表示されます。このコマンドによって生成される典型的な出力例を次に示します。

```
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
```

注：このコマンドは隠しコマンドであるため、変更される可能性があります。また、Cisco IOS(R) ソフトウェアのすべてのリリースで使用できることが保証されているわけではありません。

上記の例では、IP アドレス 192.168.1.90 のホストの method カラムが dhcp となっています。これは、CMTS がホストとサービス プロバイダーの DHCP サーバとの間の DHCP トランザクションを監視することで、このホストについて学習したことを意味します。

IP アドレス 192.168.1.77 のホストの method カラムは static となっています。これは、CMTS が

最初にこのデバイスと DHCP サーバとの間の DHCP トランザクションによってこのホストを学習しなかったことを意味します。その代わりに CMTS は、このホストから他の種類の IP トラフィックを観測しました。このトラフィックには、Web ブラウジング、電子メール、「ping」パケットなどが該当します。

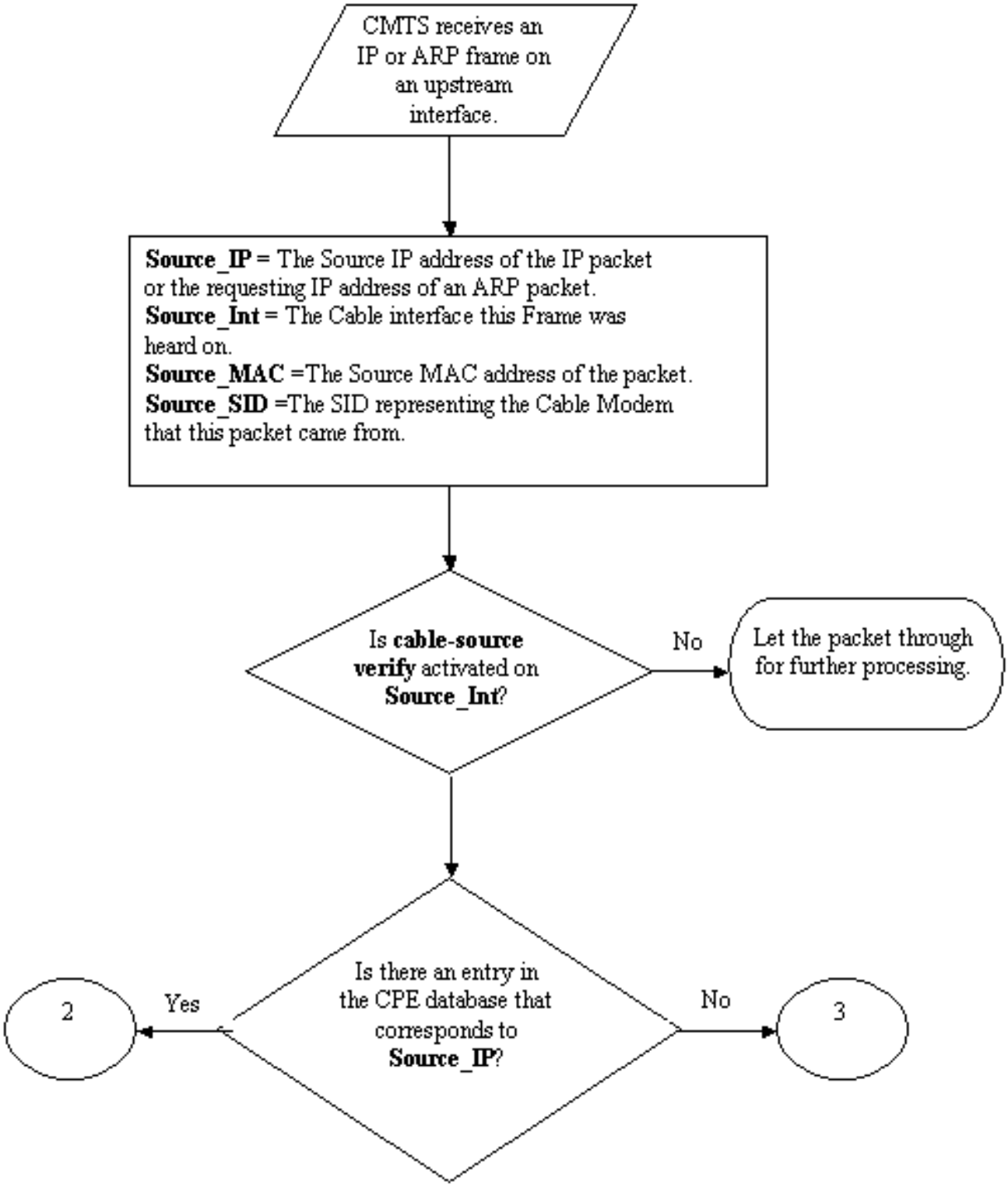
192.168.1.77 にはスタティック IP アドレスが設定されているように見えますが、このホストは実際には DHCP リースを取得している可能性があります。CMTS がそのイベントの後でリブートされた場合は、そのトランザクションを記憶していません。

CPE データベースは通常、CPE デバイスとサービス プロバイダーの DHCP サーバとの間の DHCP トランザクションから情報を取得している CMTS によって入力されます。また、CMTS は CPE デバイスから到達したその他の IP トラフィックを受信し、どの CPE の IP アドレスと MAC アドレスがどのケーブル モデムに属しているかを判断することができます。

cable source-verify コマンド

シスコはケーブル インターフェイス コマンド cable source-verify [dhcp] を実装しました。このコマンドを使用すると、CMTS が CPE データベースを利用して、CMTS のケーブル インターフェイスで受信された IP パケットの有効性を確認できるようになるため、そのパケットを転送するかどうかについてインテリジェントな決定を下すことができます。

次のフローチャートは、ケーブル インターフェイスで受信された IP パケットが CMTS で処理される前に必ず通過する追加のプロセスを示しています。



フローチャート 1

フローチャートは CMTS のアップストリーム ポートでパケットが受信されたところから始まり、そのパケットが後続の処理を許可されるか、または廃棄されるかで終ります。

例1 - 重複したIPアドレスのシナリオ

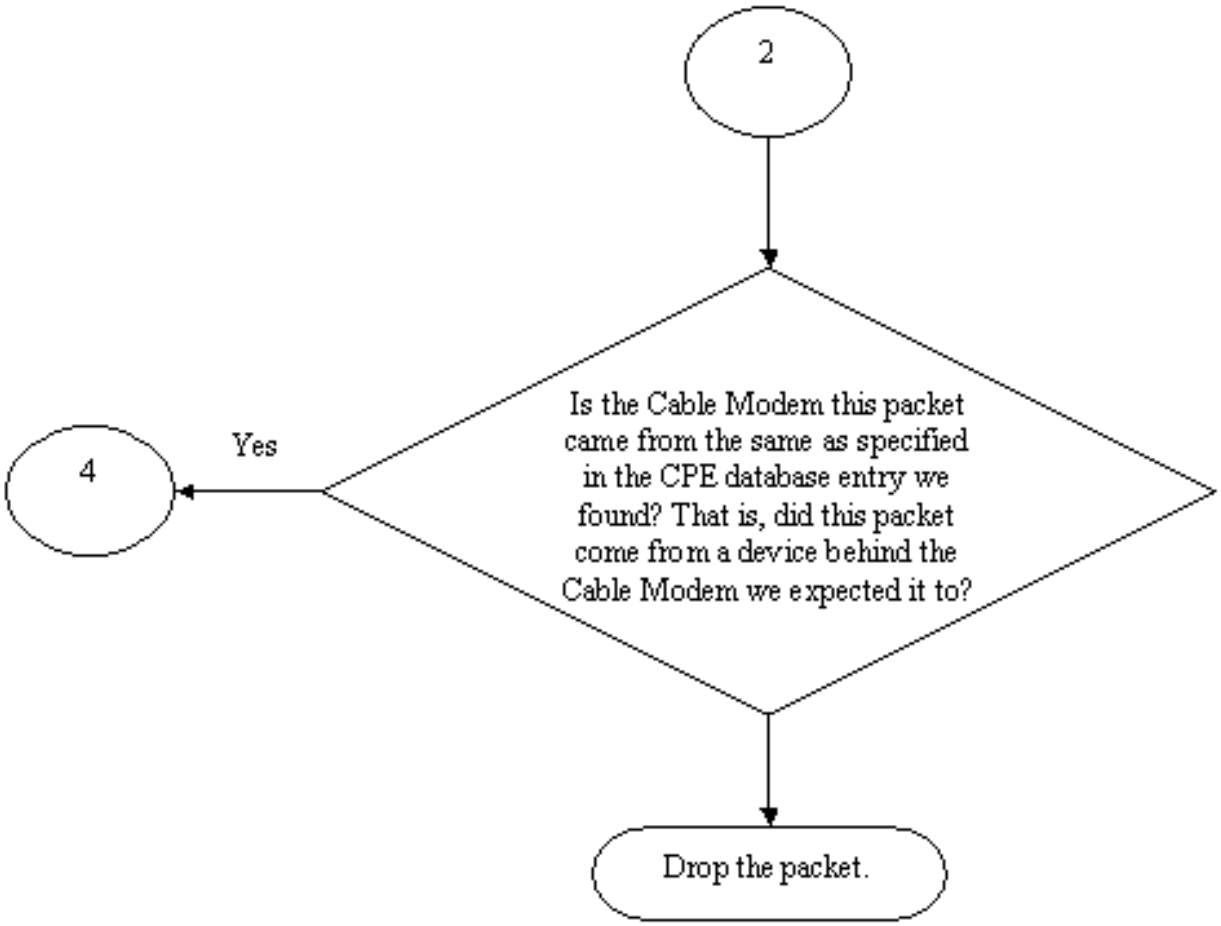
最初に取り上げるサービス拒絶のシナリオは、重複した IP アドレスが関係している場合です。お客様 A がサービス プロバイダーに接続し、PC にとって有効な DHCP リースを取得しました。お客様 A が取得した IP アドレスを X とします。

A が DHCP リースを取得した後、お客様 B が偶然、お客様 A の機器が現在使用している IP アドレスと同じアドレスをスタティック IP アドレスとして自分の PC に設定しました。IP アドレス X に関する CPE データベースの情報は、最後にどの CPE デバイスが X の ARP 要求を送信したかによって変わります。

保護されていない DOCSIS ネットワークでは、お客様 B がネクストホップ ルータ（ほとんどの場合 CMTS）に X の ARP 要求を送信するだけで、CMTS またはネクストホップ ルータはお客様 B が IP アドレス X を使用する権利を持つと見なす可能性があります。こうなると、サービス プロバイダーからのトラフィックはお客様 A には転送されません。

cable source-verify を有効にすると、IP アドレス X の IP パケットと ARP パケットが誤ったケーブル モデムから発信されていることを CMTS が確認できるため、これらのパケットは廃棄されます。フローチャート 2 を参照してください。これには、X を送信元アドレスとするすべての IP パケットと X の ARP 要求が含まれます。CMTS のログには次のようなメッセージが表示されます。

%UBR7200-3-BADIPSOURCE:Interface Cable3/0, IP packet from invalid source.IP=192.168.1.10, MAC=0001.422c.54d0, Expected SID=10, Actual SID=11



フローチャート 2

この情報を使用して両方のクライアントを識別し、重複した IP アドレスが接続されたケーブル モデムを無効にできます。

例2 - 重複したIPアドレスのシナリオ- 未使用のIP アドレスの使用

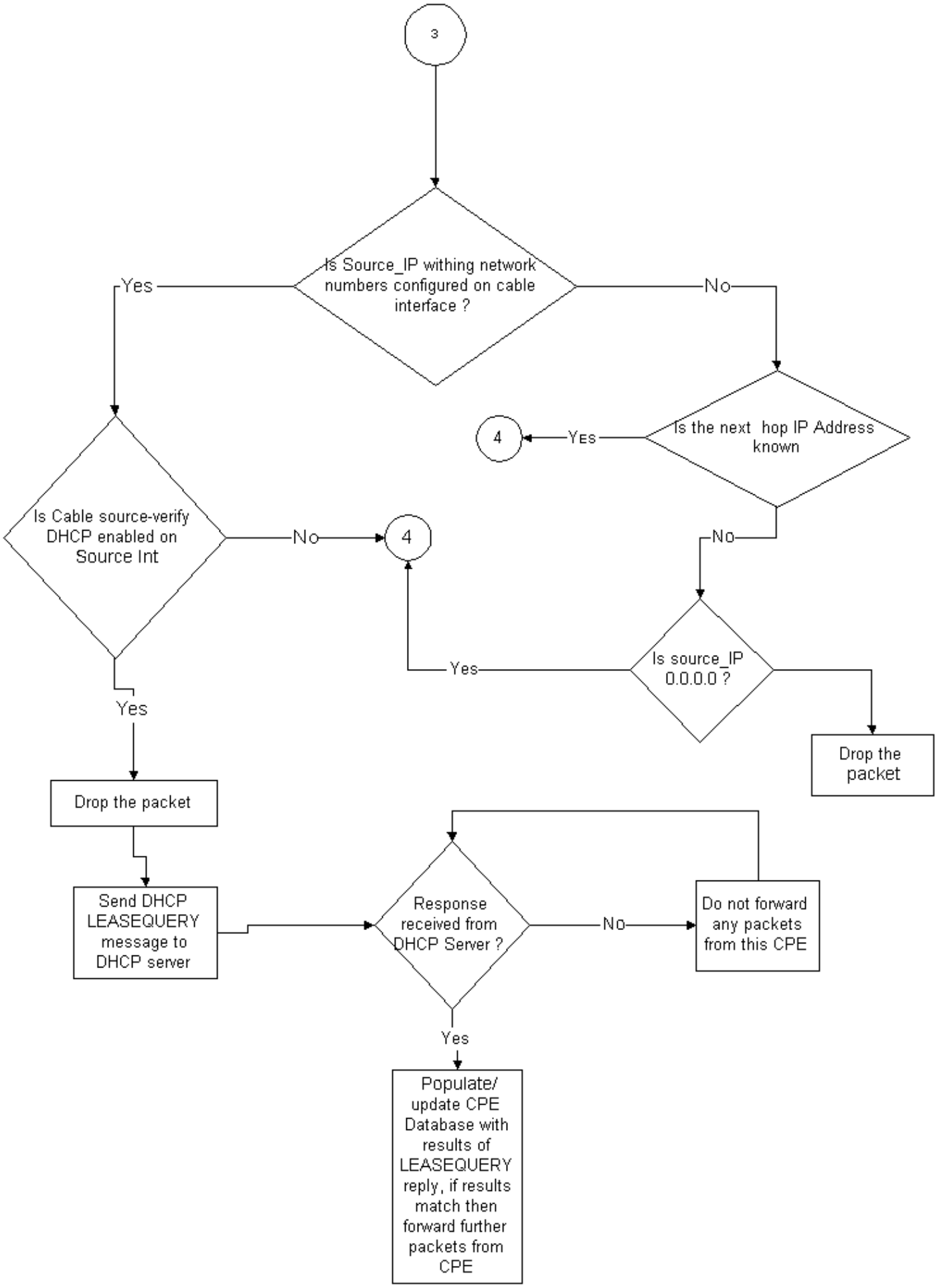
もう 1 つのシナリオとして、ユーザが CPE アドレスの正規の範囲内にある未使用の IP アドレスを、自分の PC にスタティックに割り当てた場合が考えられます。このシナリオでは、ネットワーク内のどのユーザにもサービスの中断は起こりません。お客様 B が自分の PC にアドレス Y を割り当てたとします。

次に起こりうる問題は、お客様 C がワークステーションをサービス プロバイダーのネットワークに接続し、IP アドレス Y の DHCP リースを取得することです。CPE データベースは一時的に、IP アドレス Y をお客様 C のケーブル モデムの背後にあるものとしてマークします。しかし、お客様 B (非正規ユーザ) が一連の適切な ARP トラフィックを送信し、ネクストホップによってお客様 B が IP アドレス Y の正規の所有者であると見なされるまで、それほど時間はかかりません。こうなると、お客様 C のサービスが中断します。

この 2 番目の問題も、cable source-verify をオンにすることで解決できます。cable source-verify をオンにすると、DHCP トランザクションから詳細情報を取得して生成された CPE データベースのエントリは、他の種類の IP トラフィックによって置き換えられなくなります。エントリが置き換えられるのは、その IP アドレスについて別の DHCP トランザクションが起こった場合と、

CMTS 上のその IP アドレスの ARP エントリがタイムアウトした場合のみです。そのためエンドユーザは、特定の IP アドレスの DHCP リースを正常に取得していれば、CMTS が混乱してその IP アドレスが別のユーザのものであると見なすような事態を心配する必要はありません。

ユーザが未使用の IP アドレスを使用できないようにするという最初の問題を解決するには、cable source-verify dhcp を使用します。このコマンドの最後に dhcp パラメータを追加すると、CMTS は LEASEQUERY という特別な DHCP メッセージを DHCP サーバに発行することにより、新たに受信した送信元 IP アドレスの有効性をチェックできます。フローチャート 3 を参照してください。


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

フローチャート 3

LEASEQUERY メッセージは、特定の CPE IP アドレスについて、対応する MAC アドレスとケーブル モデムを問い合せます。

この例では、お客様 B がスタティック アドレス Y を使用してワークステーションをケーブル ネットワークに接続しようとしたときに、CMTS は DHCP サーバに LEASEQUERY を送信して、アドレス Y がお客様 B の PC にリースされているかどうかを確認します。DHCP サーバは IP アドレス Y のリースが付与されていないことを CMTS に通知するため、お客様 B のアクセスは拒否されます。

例3 - サービスプロバイダーによって提供されないネットワーク番号の使用

ユーザがサービス プロバイダーの現在のネットワーク番号と競合しないスタティック IP アドレスを、ケーブル モデムの背後にあるワークステーションに設定している場合がありますが、これは将来的に問題を引き起こす可能性があります。そのため、CMTS で cable source-verify を使用して、CMTS のケーブル インターフェイスに設定した範囲に含まれない送信元 IP アドレスから到達したパケットを除去できます。

注：これを正しく動作させるには、スプーフィングされたIP送信元アドレスを防ぐために、**ip verify unicast reverse-pathコマンドを設定する必要**があります。詳細は、『ケーブルコマンド：ケーブルs」を参照してください。

お客様がルータを CPE デバイスとして使用していて、トラフィックをこのルータにルーティングするよう依頼している場合があります。CMTS が CPE ルータから Z を送信元 IP アドレスとする IP トラフィックを受信した場合、cable source-verify は、その CPE デバイス経由で所属しているネットワーク Z へのルートが CMTS 上に存在すれば、そのパケットを通過させます。フローチャート 3 を参照してください。

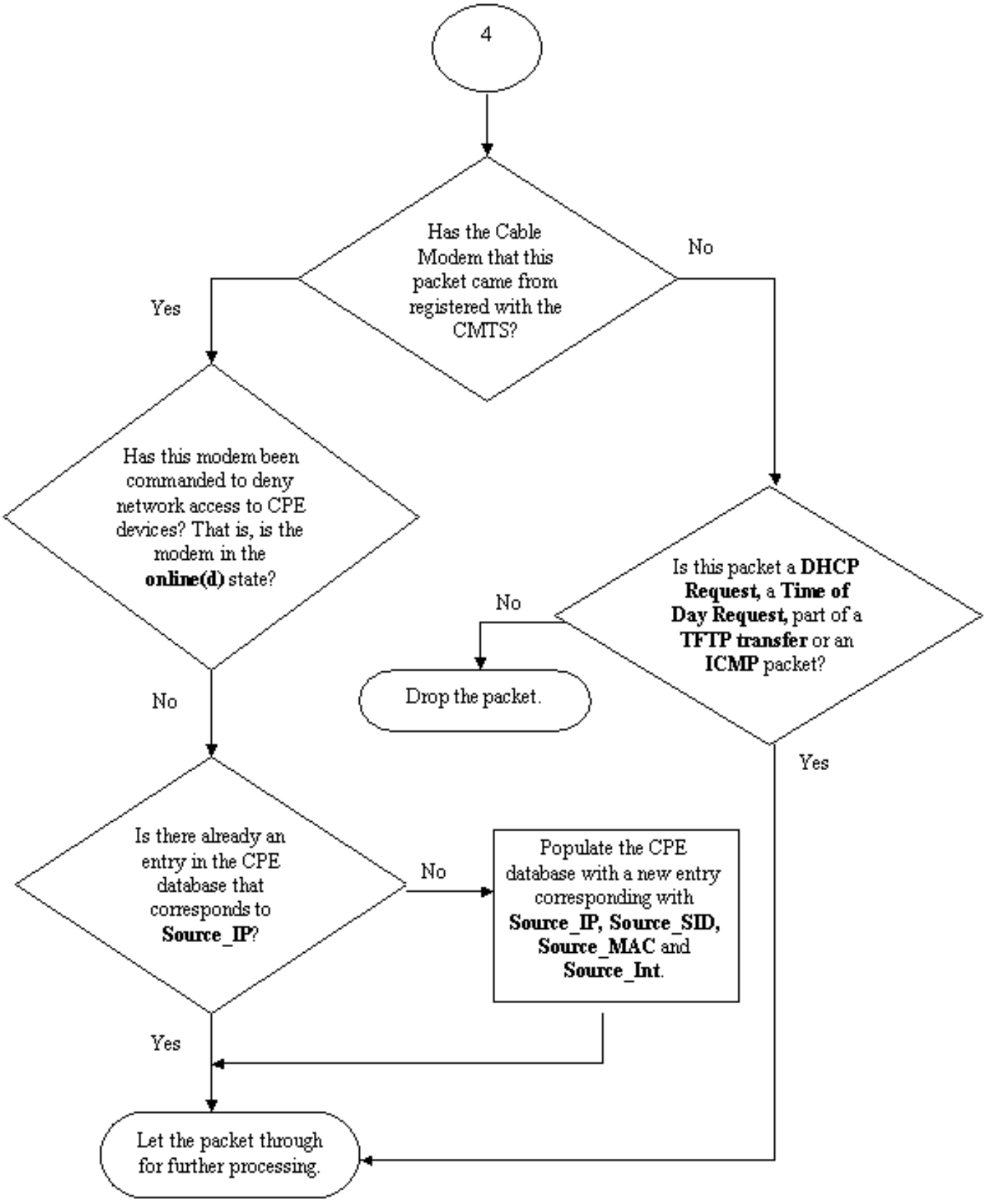
ここで、次の例について考えます。

CMTS は次のように設定されています。

```
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
```

送信元IPアドレスが172.16.1.10のパケットがケーブルモデム24.2.2.10からCMTSに到着したと仮定すると、CMTSはCPEデータベースに24.2.2.10が存在しないことを確認します。**ip verify unicast reverse-path**は、送信元で受信された各パケットを確認しますパケットのIPアドレスは、そのインターフェイスに属するルーティングテーブルに表示されます。**cable source-verify**は、24.2.2.10のネクストホップが何であるかを確認します。上記の設定では、**ip route 24.2.2.0 255.255.255.0 24.1.1.2**があり、ネクストホップが24.1.1.2であることを意味します。ここで、24.1.1.2がCPEデータベースの有効なエントリであると仮定すると、CMTSはパケットが正常であると判断し、フローチャート4に従ってパケットを処理します。



フローチャート 4

ケーブルソース確認を設定する方法

cable source-verify を設定するには、この機能を有効にしたいケーブル インターフェイスに cable source-verify コマンドを追加します。ケーブルインターフェイスのバンドリングを使用している場合は、プライマリインター**フェイスの設定に**cable source-verifyを追加する必要がありま

す。

cable source-verify dhcp の設定方法

注： cable source-verifyは、Cisco IOSソフトウェアリリース12.0(7)Tで初めて導入され、Cisco IOSソフトウェアリリース12.0SC、12.1EC、および12.1Tでサポートされています。

cable source-verify dhcp の設定にはいくつかの手順が必要です。

DHCP サーバが特別な DHCP LEASEQUERY メッセージをサポートしていることを確認します。

cable source-verify dhcp機能を使用するには、draft-ietf-dhcp-leasequery-XX.txtで指定されたメッセージにDHCPサーバが応答する必要があります。Cisco Network Registrarバージョン3.5以降では、このメッセージに応答できます。

DHCP サーバがリレー エージェント情報オプション処理をサポートしていることを確認します。

リレーエージェントのセクションを参照してください。

DHCP サーバがサポートしていなければならないもう 1 つの機能は DHCP リレー情報オプション処理です。これは「Option 82 処理」とも呼ばれます。このオプションについては、DHCP Relay Information Option（RFC 3046）に説明があります。 Cisco Network Registrar バージョン 3.5 以降はリレー エージェント情報オプション処理をサポートしていますが、Cisco Network Registrar のコマンドライン ユーティリティ nrcmd で次の一連のコマンドを入力してアクティブにする必要があります。

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 dhcp reload

上記のコマンドはデフォルト値を示しています。ユーザ名、パスワード、およびサーバの IP アドレスは適切なものに置き換えてください。または、nrcmdプロンプトで>nrcmdを入力し、次のように入力します。

dhcp enable save-relay-agent-data

save

dhcp reload

CMTS で DHCP リレー情報オプション処理をオンにします。

リレーエージェント

cable source-verify dhcp を有効にするためには、CMTS がケーブル モデムおよび CPE からの DHCP 要求にリレー エージェント情報オプションをタグ付けする必要があります。Cisco IOS ソフトウェア リリース 12.1EC、12.1T、またはそれ以降のバージョンの Cisco IOS を実行している CMTS では、グローバル設定モードで次のコマンドを入力します。

ip dhcp relay information option

Cisco IOS ソフトウェア リリース 12.0SC 群を実行している CMTS では、上記のコマンドの代わりに cable relay-agent-option ケーブル インターフェイス コマンドを使用します。

使用している Cisco IOS のバージョンに応じて適切なコマンドを使用してください。Cisco IOS のリリース群を変更する場合は、必ず設定を更新してください。

relay information option コマンドは、CMTS が DHCP パケットを中継するときに、Option 82 と呼ばれる特別なオプション（リレー情報オプション）を、中継する DHCP パケットに追加します。

Option 82 には Agent Circuit-ID というサブオプションが含まれています。これは、DHCP 要求を受信した CMTS の物理インターフェイスを参照します。この他に、Agent Remote ID という別のサブオプションも含まれます。これは、DHCP 要求の発信元のケーブル モデム、または DHCP 要求を通過させたケーブル モデムの 6 バイトの MAC アドレスを示します。

たとえば、MAC アドレス aa:bb:cc:dd:ee:ff のケーブル モデムの背後にある、MAC アドレス 99:88:77:66:55:44 の PC が DHCP 要求を送信した場合、CMTS は Option 82 の Agent Remote ID サブオプションをケーブル モデムの MAC アドレス aa:bb:cc:dd:ee:ff に設定してから DHCP 要求を転送します。

CPE デバイスからの DHCP 要求にリレー情報オプションを含めることで、DHCP サーバは、どの CPE がどのケーブル モデムの背後にあるかについての情報を保存できます。これは、CMTS で cable source-verify dhcp が設定されている場合に特に役立ちます。というのは、特定のクライアントがどの MAC アドレスを持っているかだけでなく、どのケーブル モデムに接続するかについても、DHCP サーバから CMTS に確実に通知できるためです。

適切なケーブル インターフェイスのもとで cable source-verify dhcp コマンドを有効にします。

最後に、この機能を有効にしたいケーブル インターフェイスのもとで cable source-verify dhcp コマンドを入力します。CMTSがケーブルインターフェイスバンドリングを使用している場合は、バンドルのプライマリインターフェイスでコマンドを入力する必要があります。

結論

サービス プロバイダーは cable source-verify コマンド群を使用することで、不正な IP アドレスを使用するユーザからケーブル ネットワークを保護できます。

cable source-verify コマンドはそれだけで、IP アドレス セキュリティを実装するための効果的かつ容易な手段となります。すべてのシナリオに対応できるわけではありませんが、少なくとも、割り当てられた IP アドレスを使用する権利を持つお客様を確認し、それらの IP アドレスの使用を他のユーザに許可することで中断を招くような事態を防ぐことができます。

この文書で説明した最も単純な形態では、DHCP を通じて設定されていない CPE デバイスはネットワークにアクセスできません。これは、IPアドレス空間を確保し、Data over Cable(DOCSIS)サービスの安定性と信頼性を高める最良の方法です。 しかし、スタティックアドレスを使用する必要がある商業サービスを持つ複数のサービス事業者(MSO)は、コマンド**cable source-verify dhcpの厳密なセキュリティを実装したいと考えていました。**

Cisco Network Registrarバージョン5.5には、IPアドレスがDHCP経由で取得されていなくても、「予約済み」アドレスのリースクエリーに応答する新しい機能があります。 DHCPサーバは、DHCPLEASEQUERY応答にリース予約データを含めます。Network Registrar の前のバージョンでは、DHCPLEASEQUERY の応答は、MAC アドレスが保存されているリース済みクライアント

、または以前にリースしたクライアントについてのみ可能でした。Cisco uBR リレー エージェントは、たとえば、MAC アドレスとリース時間を持たない DHCPLEASEQUERY データグラムを廃棄します（dhcp-lease-time オプション）。

Network Registrar は、予約されたリースについて、DHCPLEASEQUERY 応答で 1 年（31536000 秒）のデフォルト リース時間を返します。アドレスが実際にリースされている場合、Network Registrarは残りのリース時間を返します。

関連情報

- DHCPリレー情報オプション(RFC 3046)
- テクニカル サポートとドキュメント – Cisco Systems