

Table of Contents

<u>Cable Source–Verify and IP Address Security</u>	1
<u>Document ID: 20691</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Prerequisites</u>	1
<u>Components Used</u>	1
<u>The Unprotected DOCSIS Environment</u>	1
<u>The CMTS CPE Database</u>	2
<u>The Cable Source–Verify Command</u>	3
<u>Example 1 – Scenario with Duplicate IP Addresses</u>	4
<u>Example 2 – Scenario with Duplicate IP Addresses – Using an IP address that's not yet used</u>	5
<u>Example 3 – Use of a network number not provisioned by the service provider</u>	7
<u>How to Configure Cable Source–Verify</u>	8
<u>Relay Agent</u>	9
<u>Conclusion</u>	10
<u>Related Information</u>	11

Cable Source–Verify and IP Address Security

Document ID: 20691

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

The Unprotected DOCSIS Environment

The CMTS CPE Database

The Cable Source–Verify Command

Example 1 – Scenario with Duplicate IP Addresses

Example 2 – Scenario with Duplicate IP Addresses – Using an IP address that's not yet used

Example 3 – Use of a network number not provisioned by the service provider

How to Configure Cable Source–Verify

Relay Agent

Conclusion

Related Information

Introduction

Cisco has implemented enhancements within Cisco cable modem termination system (CMTS) products that inhibit certain types of Denial of Service attacks based on IP address spoofing and IP address theft in Data-over-Cable Service Interface Specifications (DOCSIS) cable systems. This document describes the **cable source–verify** suite of commands that are part of these IP address security enhancements.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The Unprotected DOCSIS Environment

A DOCSIS Media Access Control (MAC) domain is similar in nature to an Ethernet segment. If left unprotected, users in the segment are vulnerable to many types of Layer 2 and Layer 3 addressing based Denial of service attacks. In addition, it is possible for users to suffer a degraded level of service due to the malconfiguration of addressing on other user's equipment. Examples of this could include:

- Configuring duplicate IP addresses on different nodes.
- Configuring duplicate MAC addresses on different nodes.
- The unauthorized use of static IP addresses rather than Dynamic Host Configuration Protocol (DHCP) assigned IP addresses.
- The unauthorized use of different network numbers within a segment.
- Incorrectly configuring end nodes to answer ARP requests on behalf of a portion of the segment IP subnet.

While these types of problems are easy to control and mitigate in an Ethernet LAN environment by physically tracking down and disconnecting the offending equipment, such problems in DOCSIS networks may be harder to isolate, resolve, and prevent due to the potentially large size of the network. In addition, end users who control and configure Customer Premise Equipment (CPE) may not have the benefit of a local IS support team to make sure that their workstations and PCs are not intentionally or unintentionally misconfigured.

The CMTS CPE Database

The Cisco suite of CMTS products maintains a dynamically populated internal database of connected CPE IP and MAC addresses. The CPE database also contains details on the corresponding Cable Modems that these CPE devices belong to.

A partial view of the CPE Database corresponding to a particular cable modem can be viewed by executing the hidden CMTS command **show interface cable X/Y modem Z**. Here, X is the line card number, Y is the downstream port number and Z is the Service Identifier (SID) of the Cable modem. Z may be set to 0 to view details about all Cable Modems and CPE on a particular downstream interface. See example below of a typical output generated by this command.

```
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
```

Note: Since this command is hidden, it is subject to change and is not guaranteed to be available in all releases of Cisco IOS® software.

In the example above, the method column of the host with IP address 192.168.1.90 is listed as dhcp. This means that the CMTS learned about this host by watching the DHCP transactions between the host and the service provider's DHCP server.

The host with IP address 192.168.1.77 is listed with method static. This means that the CMTS did not first learn of this host via a DHCP transaction between this device and a DHCP server. Instead the CMTS first saw other kinds of IP traffic from this host. This traffic could have been web browsing, email or "ping" packets.

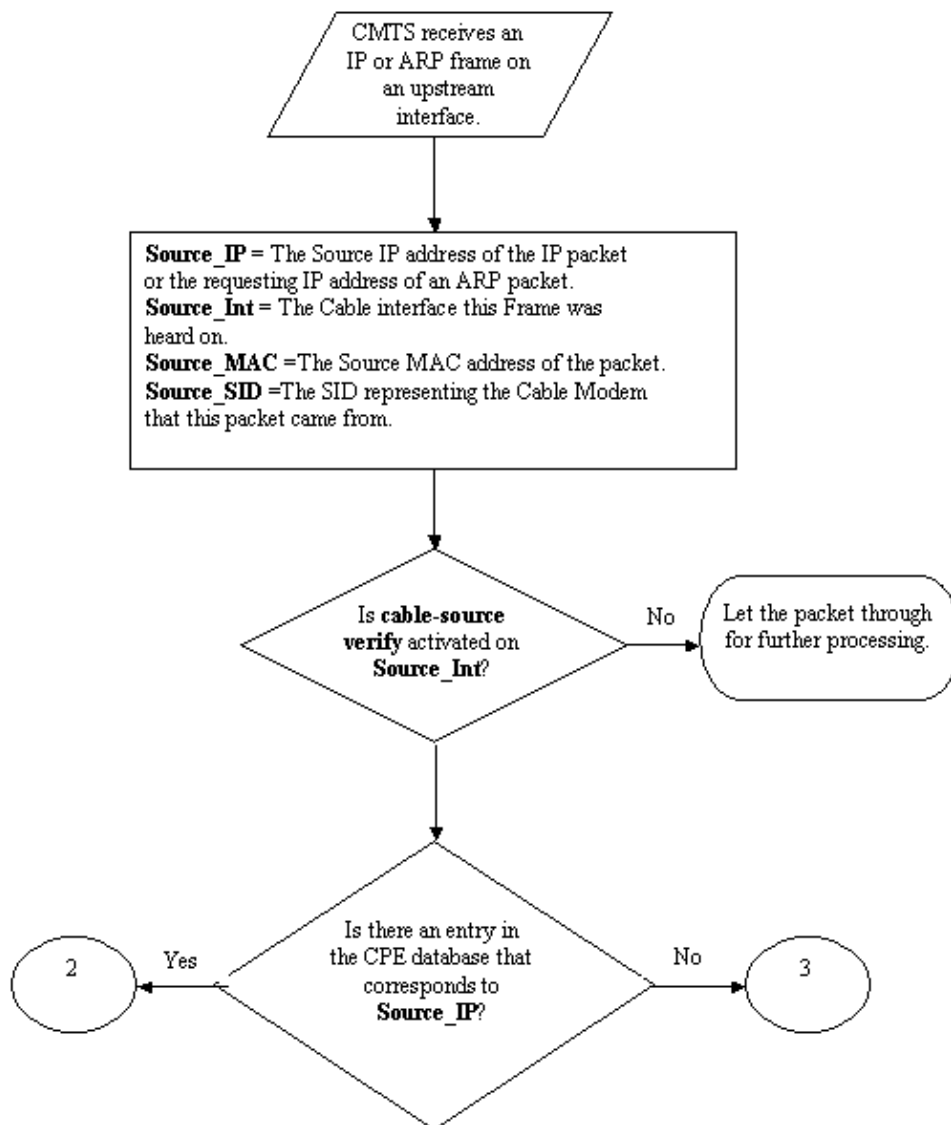
While it may seem that 192.168.1.77 has been configured with a static IP address, it may be that this host did in fact acquire a DHCP lease, but the CMTS may have been rebooted since the event and therefore it does not remember the transaction.

The CPE database is normally populated by the CMTS glean information from the DHCP transactions between CPE devices and the Service Provider's DHCP server. In addition, the CMTS can listen to other IP traffic coming from CPE devices to determine which CPE IP and MAC addresses belong to which Cable Modems.

The Cable Source–Verify Command

Cisco has implemented the cable interface command `cable source–verify [dhcp]`. This command causes the CMTS to make use of the CPE database to verify the validity of IP packets the CMTS receives on its Cable interfaces and allows the CMTS to make intelligent decisions about whether to forward them or not.

The flowchart below shows the extra processing an IP packet received on a Cable interface must go through before being allowed to proceed through the CMTS.



Flowchart 1

The flowchart starts with a packet being received by an upstream port on the CMTS and ends with the packet either being allowed to continue on for further processing or in the packet being dropped.

Example 1 – Scenario with Duplicate IP Addresses

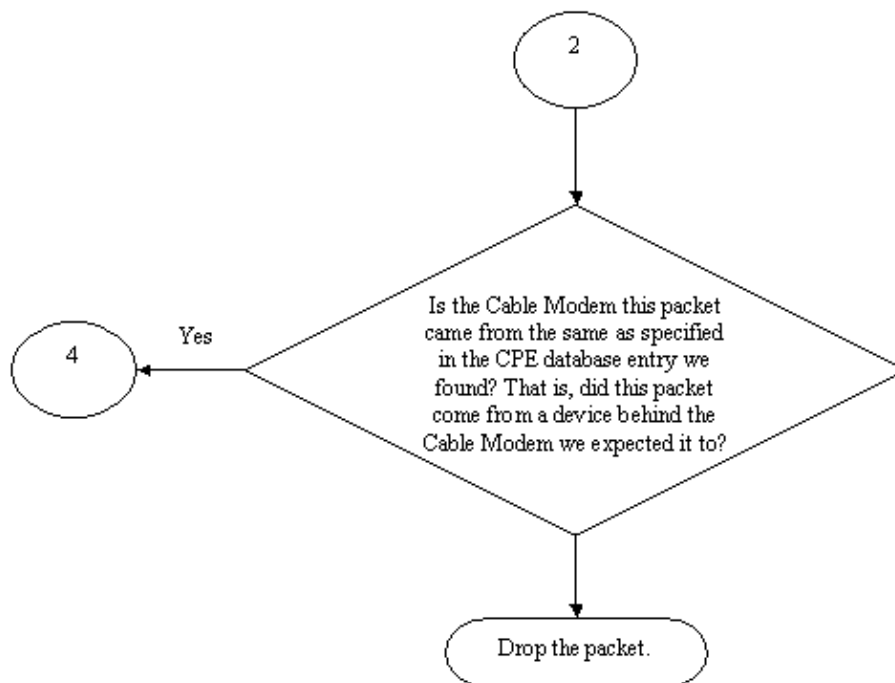
The first Denial of Service scenario we will address is the situation involving duplicate IP addresses. Let's say that customer A is connected to his service provider and has obtained a valid DHCP lease for his PC. The IP address Customer A has obtained will be known as X.

Sometime after A acquires his DHCP lease, customer B decides to configure his PC with a static IP address that happens to be the same as that currently being used by Customer A's equipment. The CPE Database information in regards to IP address X would change depending on which CPE device last sent an ARP request on behalf of X.

In an unprotected DOCSIS network, Customer B might be able to convince the next hop router (in most cases, the CMTS) that he has the right to use IP address X by simply sending an ARP request on behalf of X to the CMTS or next-hop router. This would stop traffic from the service provider from being forwarded to Customer A.

By enabling cable source-verify, the CMTS would be able to see that IP and ARP packets for IP address X were being sourced from the wrong cable modem and hence, these packets would be dropped, see Flowchart 2. This includes all IP packets with source address X and ARP requests on behalf of X. The CMTS logs would show a message along the lines of:

```
%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
```



Flowchart 2

Using this information, both clients would be identified and the Cable Modem with the connected duplicate IP address can be disabled.

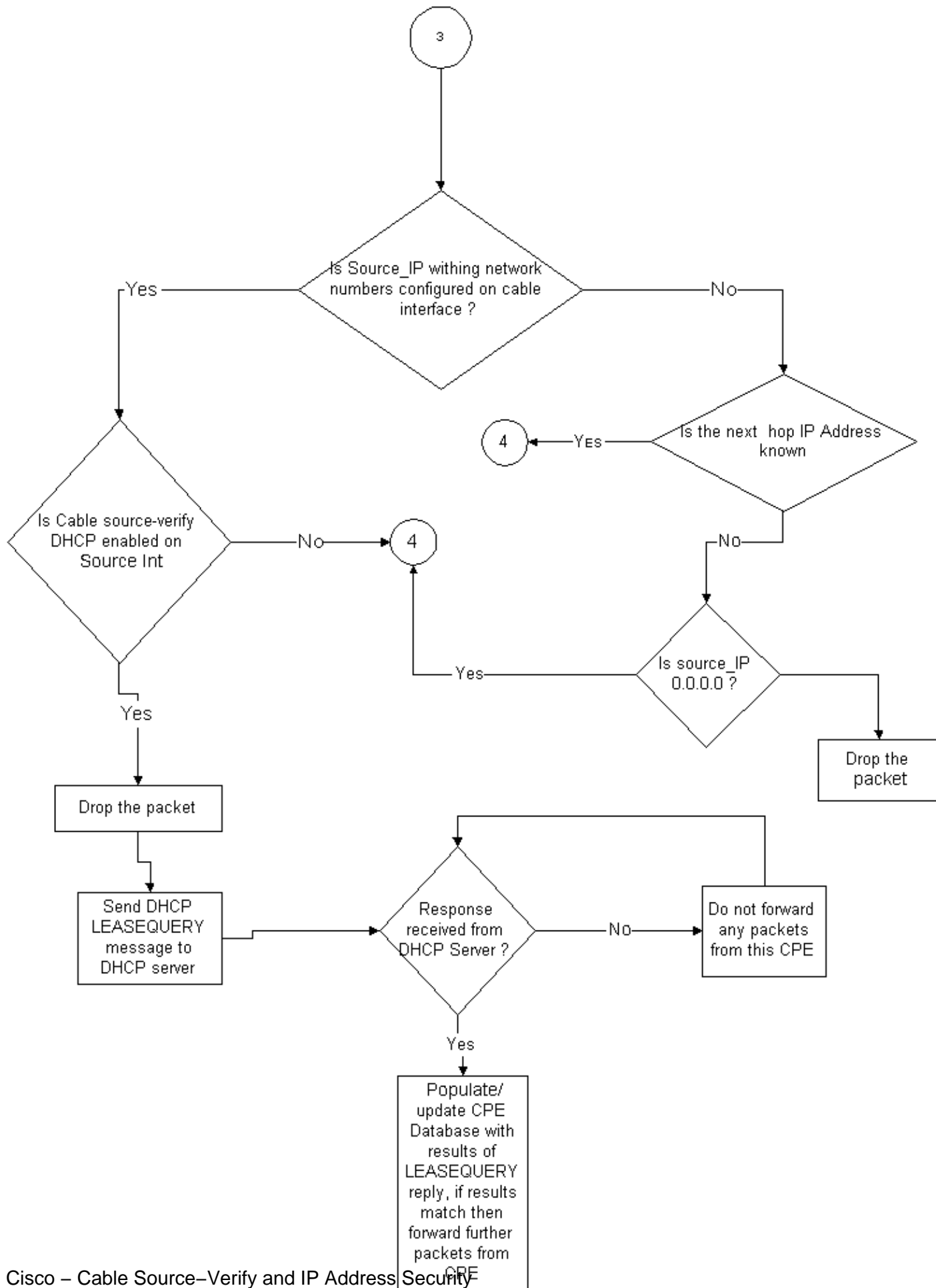
Example 2 – Scenario with Duplicate IP Addresses – Using an IP address that's not yet used

Another scenario is for a user to statically assign an unused as yet IP address to their PC that falls within the legitimate range of CPE addresses. This scenario does not cause any disruption of services to anyone in the network. Let's say that customer B has assigned address Y for their PC.

The next problem that may arise is that Customer C might connect his workstation to the service provider's network and acquire a DHCP lease for IP address Y. The CPE Database would temporarily mark IP address Y as belonging behind Customer C's Cable Modem. However, it might not be long before Customer B, the non-legitimate user sends the appropriate sequence of ARP traffic to convince the next-hop that he was the legitimate owner of IP address Y, hence causing an interruption to Customer C's service.

Similarly, the second problem can be solved by turning on **cable source-verify**. When **cable source-verify** is turned on, a CPE Database entry that has been generated by gleaning details from a DHCP transaction cannot be displaced by other kinds of IP traffic. Only another DHCP transaction for that IP address or the ARP entry on the CMTS timing out for that IP address can displace the entry. This ensures that if an end user successfully acquires a DHCP lease for a given IP address, that customer will not have to worry about the CMTS becoming confused and thinking that his IP address belongs to another user.

The first problem of stopping users from using as yet unused IP addresses can be solved with **cable source-verify dhcp**. By adding the `dhcp` parameter to the end of this command, the CMTS can check the validity of every new source IP address it hears about by issuing a special type of DHCP message called a LEASEQUERY to the DHCP server. See Flowchart 3.



Flowchart 3

For a given CPE IP address, the LEASEQUERY message asks what the corresponding MAC address and Cable Modem are. See DHCPLEASEQUERY Message for more details.

In this situation, if Customer B connects his workstation to the cable network with static address Y, the CMTS will send a LEASEQUERY to the DHCP server to verify if address Y has been leased to Customer B's PC. The DHCP server is able to inform the CMTS that no lease has been granted for IP address Y and hence customer B will be denied access.

Example 3 – Use of a network number not provisioned by the service provider

Users may have workstations configured behind their cable modems with static IP addresses which may not conflict with any of the service provider's current network numbers, but which may cause problems in the future. Therefore, using cable source-verify, a CMTS is able to filter out packets coming from source IP addresses that are not from the range configured on the CMTS's cable interface.

Some customers may have a router as a CPE device and arrange for the service provider to route traffic to this router. If the CMTS receives IP traffic from the CPE router with a source IP address of Z, then cable source-verify will let this packet through if the CMTS has a route to the network Z belongs to via that CPE device. Refer to Flowchart 3.

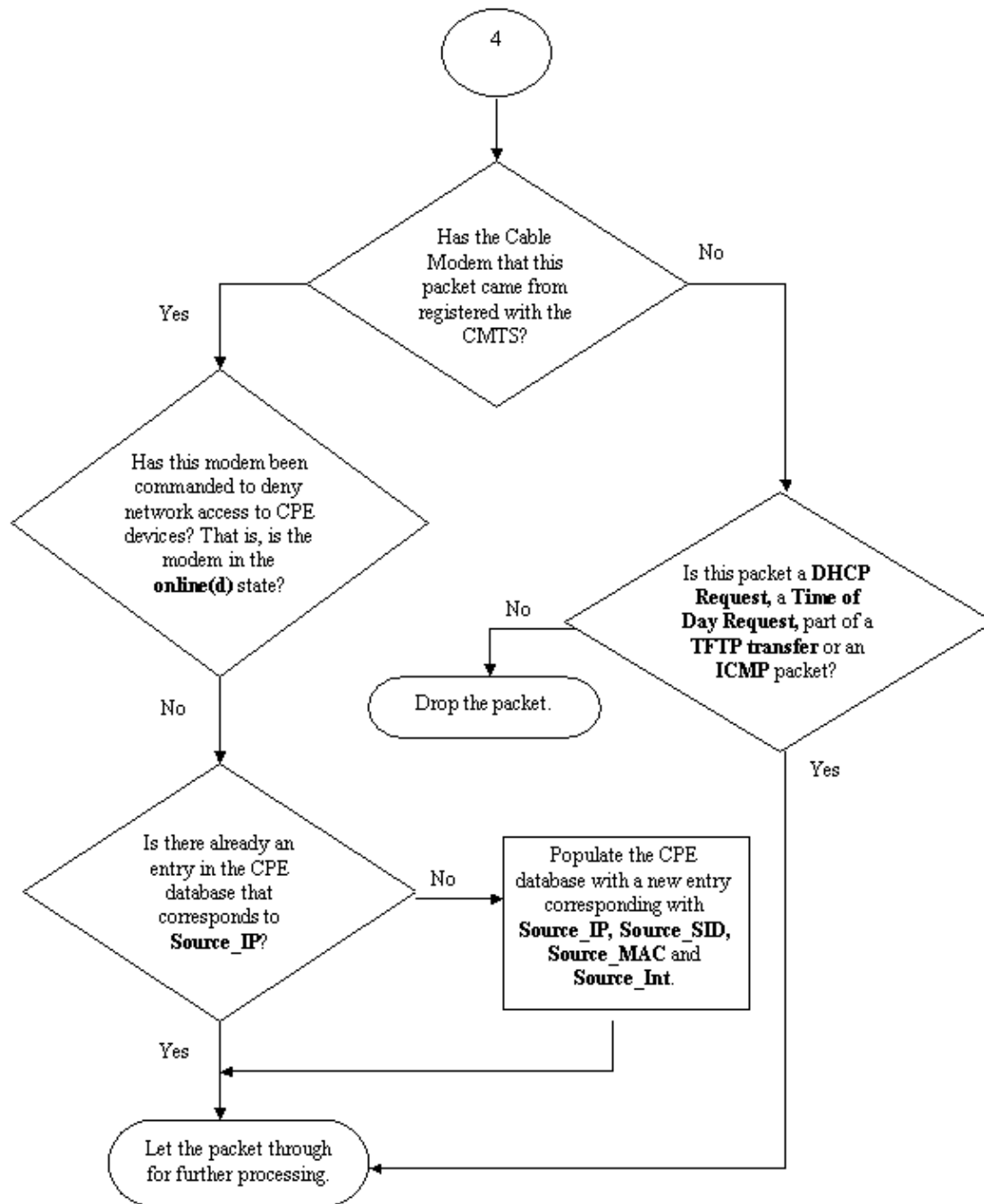
Now consider the following example:

On the CMTS we have the following config:

```
interface cable 3/0
 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

Assuming that a packet with source IP address 172.16.1.10 arrived at the CMTS from cable modem 24.2.2.10, the CMTS would see that 24.2.2.10 does not reside in the CPE database, **show int cable x/y modem 0**, however **cable source-verify** checks to see what the next hop for 24.2.2.10 is. In the configuration above we have **ip route 24.2.2.0 255.255.255.0 24.1.1.2** which means that the next hop is 24.1.1.2. Now assuming 24.1.1.2 is a valid entry in the CPE database then the CMTS concludes that the packet is OK and hence will process the packet as per Flowchart 4.



Flowchart 4

How to Configure Cable Source-Verify

Configuring **cable source-verify** simply involves adding the **cable source-verify** command to the cable interface that you'd like to activate the function on. If you're using cable interface bundling, then you need to add **cable source-verify** to the master interface's configuration.

How to configure cable source-verify dhcp

Note: **cable source-verify** was first introduced in Cisco IOS Software Release 12.0(7)T and is supported in Cisco IOS Software Releases 12.0SC, 12.1EC and 12.1T.

Configuring **cable source–verify dhcp** requires a few steps.

Make sure that your DHCP server supports the special DHCP LEASEQUERY message.

In order to make use of the **cable source–verify dhcp** functionality, your DHCP server must answer to the messages as specified by draft–ietf–dhcp–leasequery–XX.txt. Cisco Network Registrar versions 3.5 and above are able to answer to this message.

Make sure that your DHCP server supports Relay Agent Information Option processing. Please see instructions below.

Another feature that must be supported by your DHCP server is DHCP Relay Information Option processing. This is otherwise known as Option 82 processing. This Option is described in DHCP Relay Information Option (RFC 3046). Cisco Network Registrar versions 3.5 and above support Relay Agent Information Option processing however it must be activated via the Cisco Network Registrar command line utility nrcmd with the following sequence of commands:

```
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
```

You may need to substitute the appropriate username, password and server IP address, the above shows default values. Alternatively, if you're at the nrcmd prompt, >nrcmd you just type the following:

```
dhcp enable save–relay–agent–data
```

```
save
```

```
dhcp reload
```

Turn on DHCP relay information option processing on the CMTS.

Relay Agent

The CMTS must tag DHCP requests from Cable Modems and CPE with the Relay Agent Information Option in order for **cable source–verify dhcp** to be effective. The following commands must be entered in global configuration mode on a CMTS running Cisco IOS Software Releases 12.1EC, 12.1T or later versions of Cisco IOS.

```
ip dhcp relay information option
```

If your CMTS is running Cisco IOS Software Releases 12.0SC train Cisco IOS then use the **cable relay–agent–option** cable interface command instead.

Be careful to use the appropriate commands, depending on the version of Cisco IOS that you are running. Make sure to update your configuration if you change trains of Cisco IOS.

The **relay information option** commands add a special option called Option 82, or the relay information option, to the relayed DHCP packet when the CMTS relays DHCP packets.

Option 82 is populated with a sub-option, the Agent Circuit-ID, that references the physical interface on the CMTS that the DHCP request was heard on. In addition to this, another sub-option, the Agent Remote ID, is populated with the 6 byte MAC address of the cable modem that the DHCP request was received from or passed through.

So, for example, if a PC with MAC address 99:88:77:66:55:44 which is behind cable modem aa:bb:cc:dd:ee:ff sends a DHCP request, the CMTS will forward the DHCP request setting the Agent Remote ID sub-option of Option 82 to the MAC address of the Cable Modem, aa:bb:cc:dd:ee:ff.

By having the Relay Information Option included within the DHCP request from a CPE device, the DHCP server is able to store information about which CPE belongs behind what Cable Modems. This becomes especially useful when **cable source-verify dhcp** is configured on the CMTS, as the DHCP server is able to reliably inform the CMTS about not only what MAC address a particular client should have, but which cable modem particular client is meant to be connected to.

Enable the cable source-verify dhcp command under the appropriate cable interface.

The final step is to enter the **cable source-verify dhcp** command under the cable interface on which you'd like the feature activated. If the CMTS is using cable interface bundling then you must enter the command under the bundle's master interface.

Conclusion

The **cable source-verify** suites of commands allow a service provider to protect the cable network from users with unauthorized IP addresses to use the network.

The cable source-verify command by itself is an effective and easy way to implement IP address security. While it does not cover all scenarios, it at least makes sure that customers with the right to use assigned IP addresses, will not encounter any disruptions by having their IP address being used by someone else.

In its simplest form as described in this document, a CPE device not configured via DHCP cannot obtain network access. This is the best way to secure IP address space and increase the stability and reliability of a Data over Cable service. However multiple service operators (MSOs) that have commercial services which required them to use static addresses wanted to implement strict security of the command **cable source-verify dhcp**.

Cisco Network Registrar version 5.5 has a new capability of responding to the lease query for "reserved" addresses, even though the IP address was not obtained via DHCP. The DHCP server includes lease reservation data in the DHCPLEASEQUERY responses. In the previous releases of Network Registrar, the DHCPLEASEQUERY responses were possible only for leased or previously leased clients for which the MAC address was stored. Cisco uBR relay agents, for example, discard DHCPLEASEQUERY datagrams not having a MAC address and lease time (dhcp-lease-time option).

Network Registrar returns a default lease time of one year (31536000 seconds) for reserved leases in a DHCPLEASEQUERY response. If the address is actually leased, Network Registrar returns its remaining lease time. More features can be found at the Querying Leases section of Configuring DHCP Scopes and Leases.

Related Information

- **DHCP Relay Information Option (RFC 3046)**
 - **Technical Support – Cisco Systems**
-

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Nov 01, 2005

Document ID: 20691
