电缆来源验证与 IP 地址安全

目录

简介

思科实现在Cisco电缆调制解调器终端禁止根据IP地址伪装和在有线电缆数据服务接口规范(DOCSIS)电缆系统的IP地址盗窃的拒绝服务攻击特定类型的系统(CMTS)产品内的增强。本文描述是这些IP地址安全性增强的一部分的cable source-verify命令组。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文档不限于特定的软件和硬件版本。

不受保护的 DOCSIS 环境

DOCSIS媒体访问控制(MAC)域类似于本质上以太网段。如果左侧无保护，分段的用户是易受攻击对Layer2和第3层寻址基于拒绝服务攻击的许多类型。另外，遭受一个降低的级别服务由于编址的错误配置在其他用户设备的用户是可能的。此的示例能包括：

- 配置在另外节点的复制IP地址。
- 配置在另外节点的相同的MAC地址。
- 静态IP地址未经许可使用而不是分配的动态主机配置协议(DHCP) IP地址。
- 不同的网络号未经许可使用在分段内的。
- 不正确配置端节点代表分段IP子网的部分答复ARP请求。

当这些问题类型是容易控制和缓和在以太网LAN环境时通过物理的搜寻和断开触犯的设备，在DOCSIS网络的这样问题可能是更难隔离，解决和防止由于网络的可能增大的大小。另外，控制并且配置用户预定设备(CPE)的最终用户可能没有本地的好处是确保的支持团队，他们的工作站和PCs不是有意或无意配置了不适。

CMTS CPE 数据库

CMTS产品Cisco套件维护已连接CPE IP和MAC地址一个动态地填充的内部数据库。CPE数据库也包含在对应的有线调制解调器的详细信息这些CPE设备属于。

CPE数据库的一张部分视图与特定有线调制解调器相应的可以通过执行隐藏的cmts命令**show interface cable X/Y modem Z查看。**这里， X是信用卡号， Y是下行端口端口号，并且Z是服务标识符(SID)有线调制解调器。Z可能设置到0查看关于所有电缆调制解调器的在一个特定的下行接口的详细信息和CPE。参见下面示例此命令生成的典型输出。

```
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
```

注意： 因为此命令隐藏，是随时变化和没有保证是可用的在Cisco IOS软件所有版本。

在以上示例中，主机的方法列有IP地址192.168.1.90的列出作为dhcp。这意味着CMTS了解关于此主机通过观看在主机和服务提供商的DHCP服务器之间的DHCP处理。

有IP地址192.168.1.77的主机用方法静态列出。这意味着CMTS首先没有得知此主机通过在此设备和DHCP服务器之间的DHCP处理。反而CMTS首先看到了其他从此主机的IP数据流。此流量可能是Web浏览、电子邮件或者“ping”数据包。

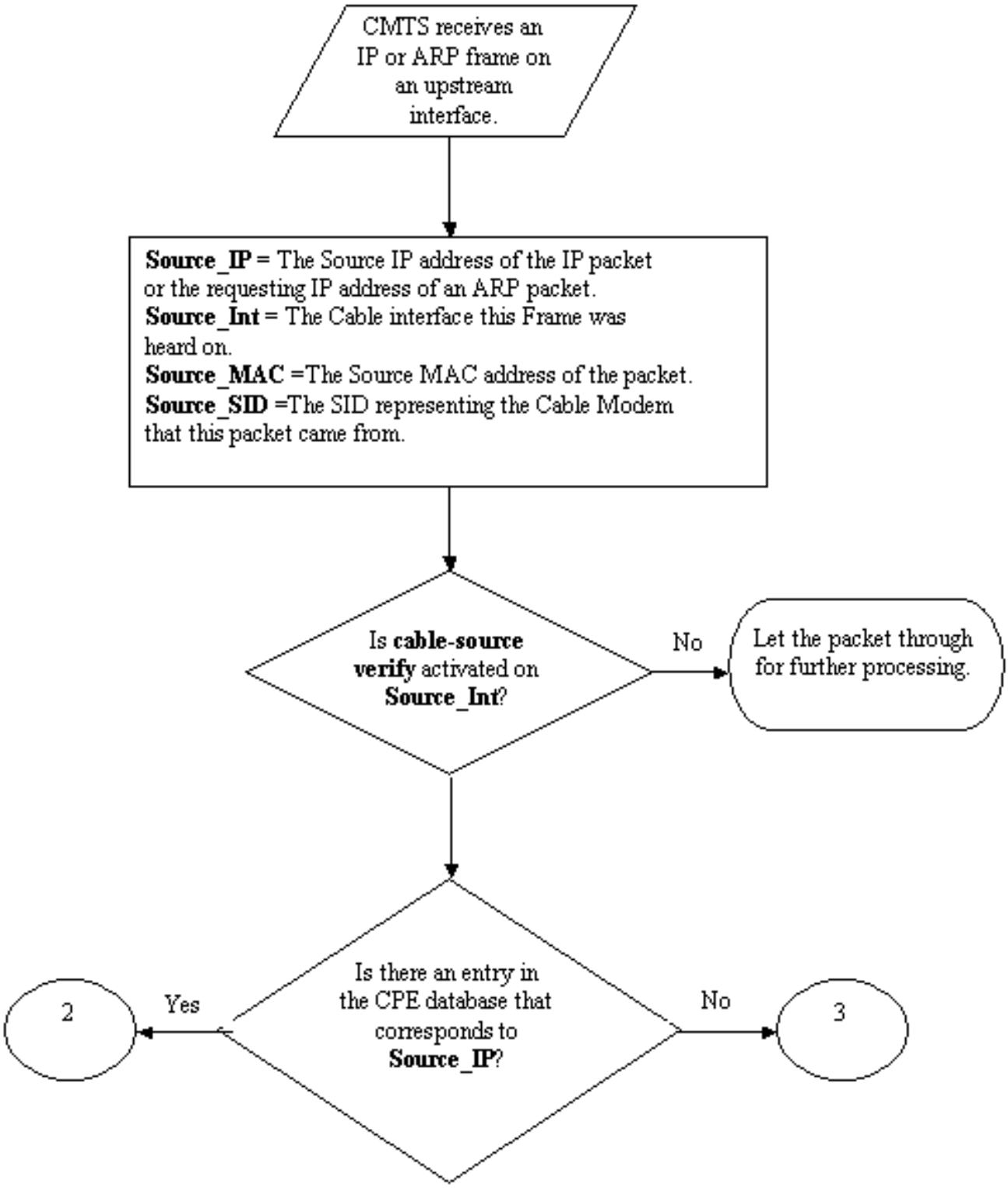
当可能看起来时192.168.1.77配置与静态IP地址，也许是此主机实际上获取了一DHCP租用，但是CMTS可能重新启动，因为事件并且它不记住处理。

CPE数据库由搜集从DHCP处理的CMTS通常填充信息在CPE设备和服务提供商的DHCP服务器之间。另外， CMTS能听来自CPE设备的其他IP数据流确定哪些CPE IP和MAC地址属于哪电缆调制解调器。

Cable Source-Verify 命令

Cisco实现cable interface命令cable source-verify [dhcp]。此命令造成CMTS利用CPE数据库验证IP信息包正确性在其电缆接口的CMTS接收并且允许CMTS做出关于是否的智能决策转发他们。

下面的流程图显示在电缆接口接收的IP数据包必须在继续前的允许经历通过CMTS的额外处理。



流程图1

流程图从CMTS的一个上行端口和末端接收的数据包开始用允许的数据包继续为进一步处理或在丢弃的数据包。

示例 1 - 具有重复 IP 地址的方案

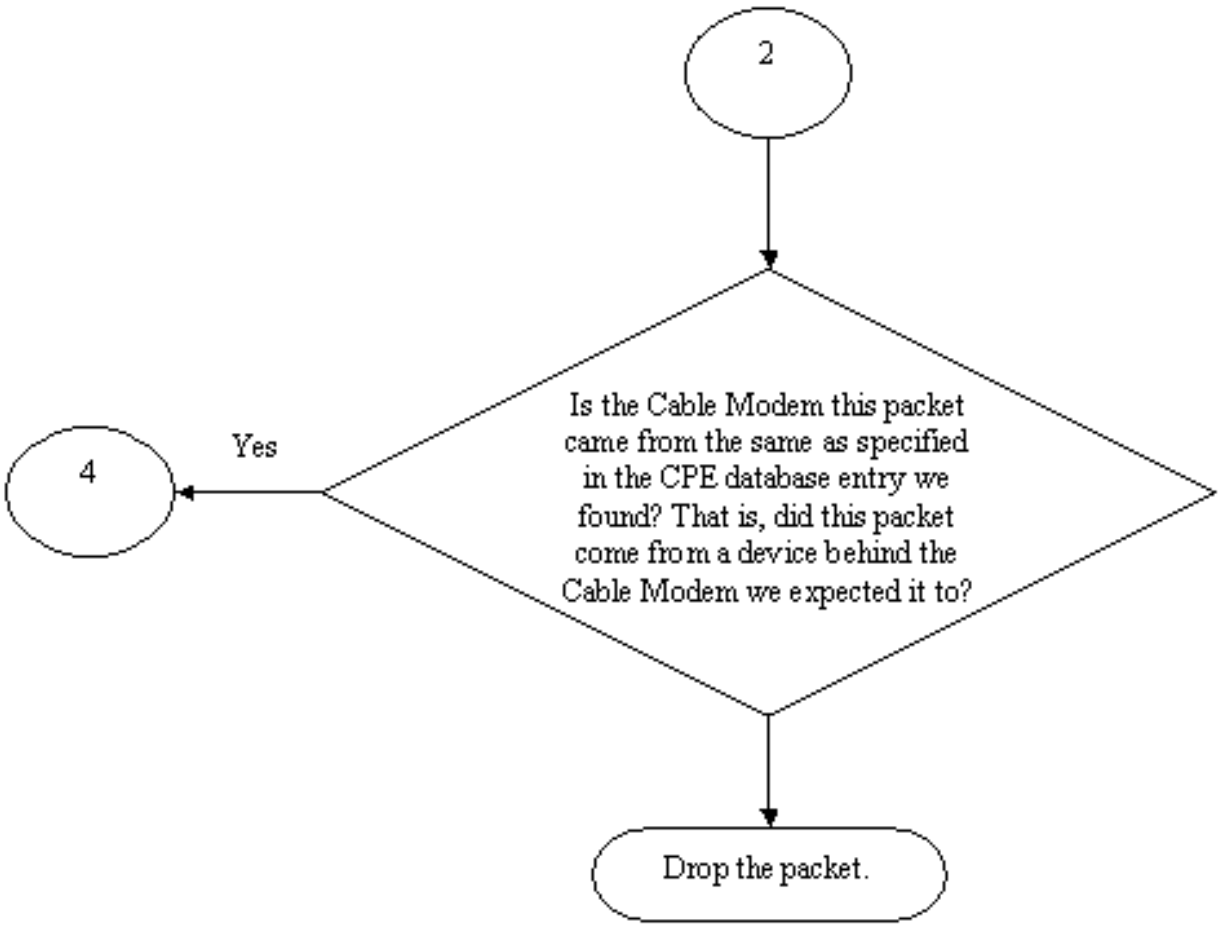
我们将寻址的第一个拒绝服务的场合是介入复制IP地址的情况。假设客户A连接对他的服务提供商和获取他的PC的一有效DHCP租用。A得到了的IP地址客户叫作X。

某时，在A获取他的DHCP租用后，客户B决定配置偶然是相同的象当前被使用由客户A的设备的他的有静态IP地址的PC。关于IP地址x的CPE数据库信息根据哪CPE设备为时将更改代表X.发送ARP请求。

在无保护的DOCSIS网络中， B也许能说服下一跳路由器的客户(在大多数情况下， CMTS)该他有权利通过发送ARP请求使用IP地址x代表X对CMTS或下一跳路由器。这从从转发的服务提供商将终止流量给客户A。

通过启用cable source-verify， CMTS能发现IP和ARP数据包IP地址的x从错误的有线调制解调器被发出并且，这些数据包将丢弃，参见流程图2。这代表X.包括有源地址x和ARP请求的所有IP信息包。CMTS日志将表示一个消息沿着线路：

%UBR7200-3-BADIPSOURCE ：接口Cable3/0，从无效源的IP数据包。IP=192.168.1.10，MAC=0001.422c.54d0，预计SID=10，实际SID=11



流程图2

使用此信息，两个客户端会识别，并且有已连接重复IP地址的有线调制解调器可以禁用。

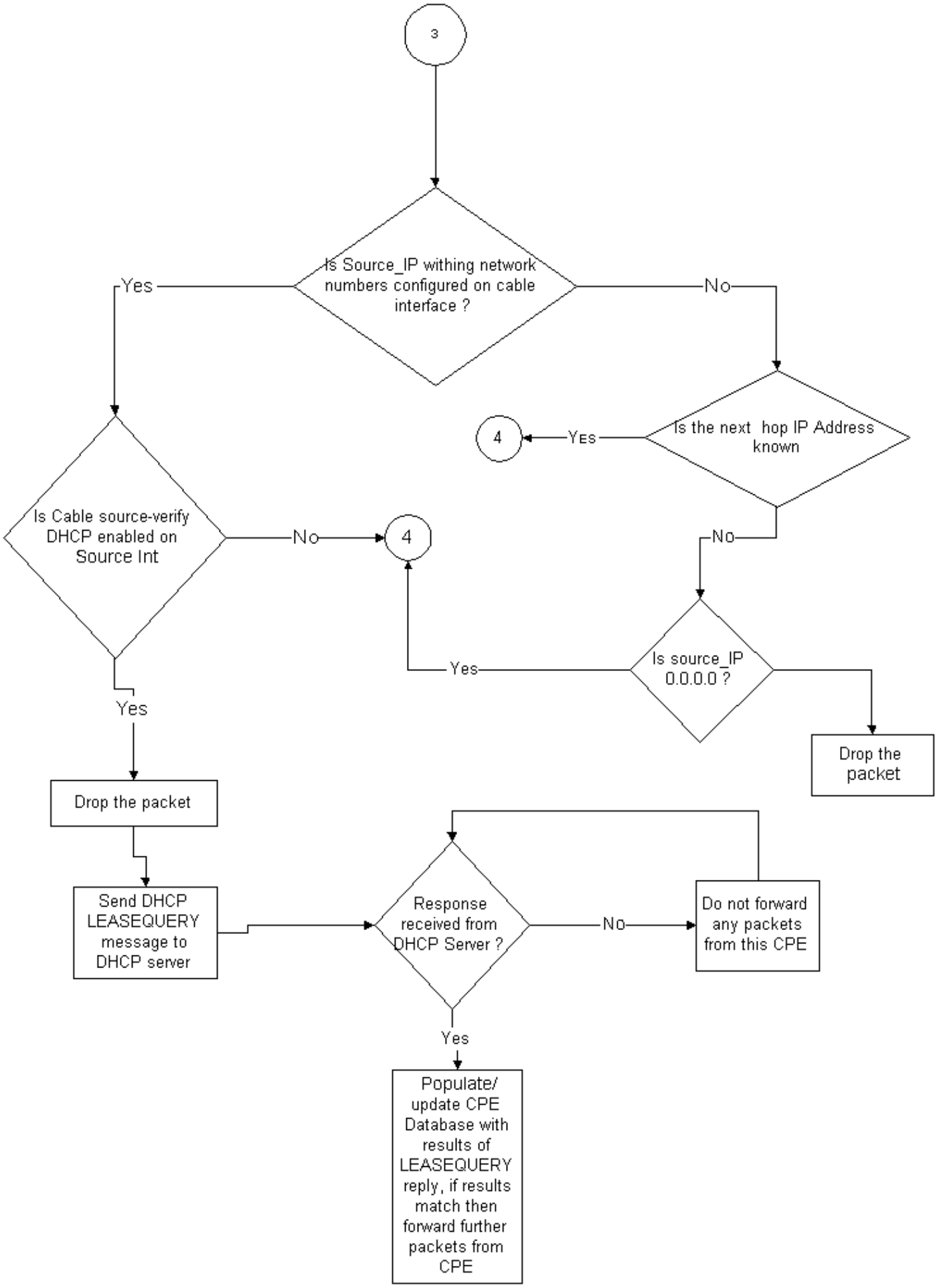
示例 2 - 具有重复 IP 地址的方案 - 使用尚未使用的 IP 地址

另一个方案是为了用户能静态分配一个未使用IP地址到属于合法范围CPE地址的他们的PC。此方案不导致服务的任何中断任何人的网络。假设客户B为他们的PC分配地址Y。

可能出现的下问题是C也许连接他的工作站到服务提供商的网络并且获取IP地址的Y.一DHCP租用的该客户。CPE数据库临时地将指示IP地址Y如属于在客户C的有线调制解调器后。然而，它也许不是在客户B之前，非合法用户发送ARP流量适当的顺序说服他是IP地址Y的合法所有者，因此导致中断的下一跳客户C的服务。

同样地，第二问题可以通过打开**cable source-verify**解决。当**cable source-verify**打开时，通过搜集从DHCP处理的详细信息生成的CPE数据库条目不可能由其他IP数据流偏移。该IP地址的另一DHCP处理或在为该IP地址时间的CMTS的仅ARP条目能偏移条目。这保证，如果最终用户成功地获取一个给的IP地址的一DHCP租用，该客户不会必须担心变为混淆和认为的CMTS他的IP地址属于另一个用户。

终止用户第一问题从使用未使用IP地址可以解决与**cable source-verify dhcp**。通过添加dhcp参数到此命令结尾， CMTS能检查通过发出特殊类型听到DHCP信息呼叫LEASEQUERY对DHCP服务器每新的源IP地址的正确性。请参阅流程图3。


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
4
Yes
Is the next hop IP Address known
No
Is source_IP 0.0.0.0 ?
Yes
Drop the packet

流程图3

对于一个给的CPE IP地址， LEASEQUERY消息问什么对应的MAC地址和有线调制解调器是。欲了解更详细的信息请参阅DHCPLEASEQUERY消息。

在这种情况下，如果客户B连接他的工作站对与静态地址Y的有线网络， CMTS将发送LEASEQUERY对DHCP服务器验证，如果对客户B的PC的地址Y租用。DHCP服务器能通知CMTS租期未为IP地址Y授权并且客户B将是拒绝访问。

示例 3 - 使用不是由服务提供商提供的网络编号

用户也许有在他们的电缆调制解调器后配置的工作站用不也许与任何服务提供商的当前网络号相冲突，但是可以在将来引起问题的静态IP地址。所以，使用cable source-verify， CMTS能过滤来自不是从在CMTS的电缆接口配置的范围的IP原地址的数据包。

注意： 为使这能正常工作，您也需要配置**ip verify unicast reverse-path命令**以便防止伪装的IP源地址。参考的电缆命令：电缆s欲知更多信息。

一些客户可能有路由器作为CPE设备和为服务提供商安排到路由流量到此路由器。如果CMTS收到从CPE路由器的IP数据流有Z源IP地址的，则cable source-verify通过将让此数据包，如果CMTS有一个路由对网络Z属于通过该CPE设备。参考的流程图3。

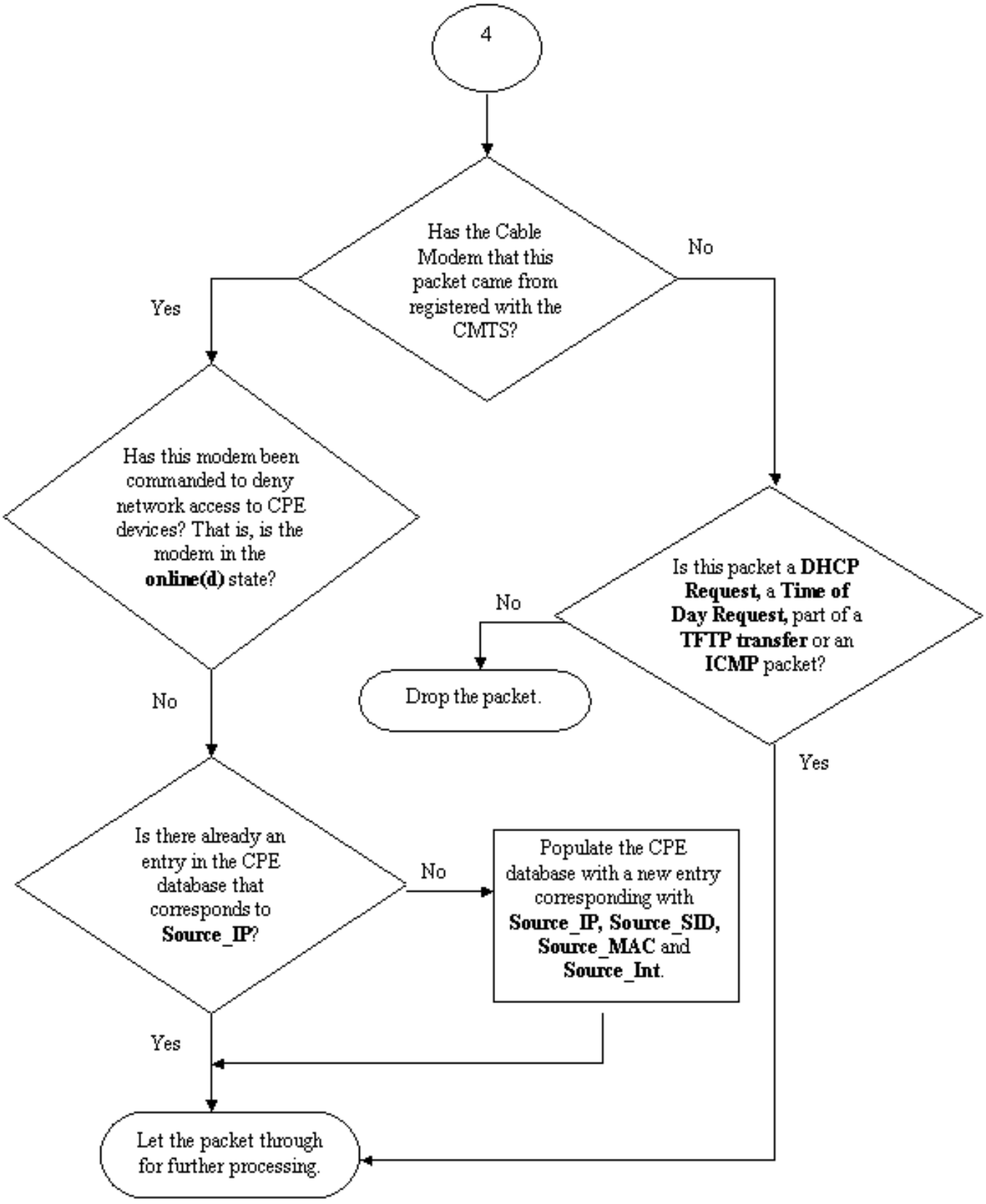
现在请参见以下示例：

在CMTS我们有以下设置：

```
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

假设，有源IP地址的172.16.1.10一数据包到达从有线调制解调器24.2.2.10的CMTS， CMTS将看到24.2.2.10不位于CPE数据库， **show int电缆x/y调制解调器0**，然而**ip验证单播reverse-path** enable (event)单播反向路径转发(单播RPF)，检查每数据包在接口接收为了验证属于该接口数据包的源IP地址在路由表里出现。**cable source-verify**检查发现什么24.2.2.10的下一跳是。在以上配置我们有**ip route 24.2.2.0 255.255.255.0**意味着的**24.1.1.2**下一跳是24.1.1.2。现在假设24.1.1.2是在CPE数据库的一有效条目CMTS然后认为，数据包是好的并且根据流程图4.处理数据包。



流程图4

如何配置cable source-verify

配置cable source-verify介入添加cable source-verify命令到电缆接口您希望激活功能。如果使用电缆接口链路，则您需要添加cable source-verify对重要的接口配置。

如何配置`cable source-verify dhcp`

注意： 在Cisco IOS软件版本12.0(7)T首先介绍和Cisco IOS软件版本12.0SC、12.1EC和12.1T支持**cable source-verify**。

配置**cable source-verify dhcp**要求一些个步骤。

确保您的DHCP服务器支持特殊DHCP LEASEQUERY消息。

为了利用**cable source-verify dhcp**功能，您的DHCP服务器必须回答到消息如指定由draft-ietf-dhcp-leasequery-XX.txt。Cisco网络注册版本3.5以上能回答到此消息。

确保您的DHCP服务器支持中继代理信息选项处理。请参阅这些说明。

必须由您的DHCP服务器支持的另一个功能是DHCP中继信息选项处理。这也叫作处理的选项82。此选项在DHCP中继信息选项(RFC 3046)描述。必须通过与命令以下顺序的Cisco Network Registrar line命令工具nrcmd激活在处理它的支持中继代理信息选项上的然而Cisco网络注册版本3.5和：

nrcmd - U Admin - P changeme - C 127.0.0.1 dhcp enable (event)保存中继代理程序数据

nrcmd - U Admin - P changeme - C 127.0.0.1保存

nrcmd - U Admin - P changeme - C 127.0.0.1 dhcp重新加载

您可能需要替代适当的用户名，密码，并且服务器IP地址，在上面显示默认值。或者，如果是在nrcmd提示符， >nrcmd您键入以下：

dhcp enable (event)保存中继代理程序数据

保存

dhcp重新加载

打开处理在CMTS的DHCP中继信息选项。

中继代理

CMTS必须用中继代理信息选项为了**cable source-verify dhcp**能标记从电缆调制解调器的DHCP请求和CPE有效。在运行Cisco IOS软件版本12.1EC、12.1T或以上版本的CMTS的全局配置模式必须输入以下命令Cisco IOS。

ip dhcp relay information option

如果您的CMTS运行然后Cisco IOS软件版本12.0SC系列Cisco IOS使用**cable relay-agent-option cable interface命令**。

小心根据Cisco IOS版本使用适当命令，您运作。如果换Cisco IOS，系列请确保更新您的配置。

当CMTS中继DHCP信息包时，**中继信息选项**add命令特殊选择呼叫Option 82或者中继信息选项，对中继的DHCP信息包。

选项82带有子选项，代理程序Circuit-id，参考在CMTS的物理接口DHCP请求听到了。除此之外，另一子选项，代理程序远程ID，带有有线调制解调器的6个字节MAC地址DHCP请求接收从或通过通过。

例如，因此，如果有是在有线调制解调器aa后的MAC地址的99:88:77:66:55:44 PC ：bb ：cc ：dd ：ee ：ff发送DHCP请求， CMTS将转发设置选项82的代理程序远程ID子选项的DHCP请求对有线调制解调器的MAC地址， aa ：bb ：cc ：dd ：ee ：ff.

由有在从CPE设备的DHCP请求内包括的中继信息选项， DHCP服务器能存储CPE在的信息什么电缆调制解调器后属于。这变得特别有用的，当**cable source-verify dhcp**在CMTS时配置，因为DHCP服务器能可靠通知CMTS关于不仅什么MAC地址特定的客户端应该有，但是哪个有线调制解调器特定的客户端被认为连接。

启用cable source-verify dhcp命令在适当电缆接口下。

最后一步将输入**cable source-verify dhcp命令**在您会类似被激活的功能的电缆接口下。如果CMTS使用电缆接口链路那么您必须输入命令在重要的套件的下建立接口。

结论

cable source-verify命令组允许服务提供商保护从用户的有线网络以未授权的IP地址使用网络。

cable source-verify命令单独是有效和简单的方法实现IP地址安全。当它不包括所有情形时，在租期确保客户以权利使用已分配IP地址，不会由有遇到任何中断别人使用的他们的IP地址。

以其正如本文所描述的简单形式，通过DHCP没配置的CPE设备不能获取网络访问。这是获取IP地址空间和增加Data over Cable Service的稳定性和可靠性的最佳方法。 然而有商业服务要求他们使用静态地址的多个服务运营商(MSO)要实现验证命令电缆源**dhcp的**严格安全。

Cisco网络注册版本5.5有响应的一个新的功能对“保留的”地址的租期查询，即使IP地址未通过DHCP获取。 DHCP服务器在DHCPLEASEQUERY答复包括租期预约数据。在网络寄存器中上一个版本， DHCPLEASEQUERY答复为MAC地址存储的租用的或以前租用的客户端是仅可能的。Cisco UBR中继代理，例如，丢弃有DHCPLEASEQUERY的数据包MAC地址和租用时间(dhcp-lease-time选项)。

网络寄存器返回默认租用时间一年(31536000秒)在DHCPLEASEQUERY答复的保留租期的。如果地址实际上租用，网络寄存器返回其剩余的租用时间。 更多功能可以在配置DHCP范围和租期的Querying Leases部分找到。

相关信息

- DHCP中继信息选项(RFC 3046)
- 技术支持和文档 - Cisco Systems