电缆来源验证与 IP 地址安全

目录

简介

思科在思科电缆调制解调器终端系统(CMTS)产品中实施了增强功能，这些增强功能可根据有线数据服务接口规范(DOCSIS)电缆系统中的IP地址欺骗和IP地址盗窃来抑制某些类型的拒绝服务攻击。Cisco CMTS电缆命令参考介绍了作为这些IP地址安全增强功能一部分的cable source-verify命令套件。

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介质访问控制(MAC)域的性质类似于以太网网段。如果网段中的用户未受保护，则很容易

受到许多基于第2层和第3层寻址的拒绝服务攻击。此外，用户可能由于其他用户设备上的寻址配置错误而遭受服务级别降级。例如：

- 在不同节点上配置重复的IP地址。
- 在不同节点上配置重复的MAC地址。
- 未经授权使用静态IP地址，而不是动态主机配置协议(DHCP)分配的IP地址。
- 网段内不同网络号的未经授权使用。
- 错误地配置终端节点来代表网段IP子网的一部分应答ARP请求。

在以太网LAN环境中，通过物理跟踪违规设备并断开其连接，这些类型的问题易于控制和缓解，但DOCSIS网络中的此类问题可能更难隔离、解决和预防，因为网络的规模可能很大。此外，控制和配置客户端设备(CPE)的最终用户可能没有本地IS支持团队的优势来确保他们的工作站和PC没有有意或无意地配置错误。

CMTS CPE 数据库

思科CMTS产品套件维护一个动态填充的内部数据库，其中包含连接的CPE IP和MAC地址。CPE数据库还包含这些CPE设备所属的相应电缆调制解调器的详细信息。

通过执行隐藏的CMTS命令**show interface cable X/Y modem Z**，可以查看与特定电缆调制解调器对应的CPE数据库的部分视图。此处，X是线卡号，Y是下行端口号，Z是电缆调制解调器的服务标识符(SID)。Z可设置为0，以查看特定下游接口上所有电缆调制解调器和CPE的详细信息。请参阅以下示例，了解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：由于此命令是隐藏的，因此它可能会更改，并且不保证在所有Cisco IOS®软件版本中都可用。

在上例中，IP地址为192.168.1.90的主机的method列列为dhcp。这意味着CMTS通过监视主机与服务提供商的DHCP服务器之间的DHCP事务来获知此主机。

IP地址为192.168.1.77的主机使用方法static列出。这意味着CMTS首先未通过此设备与DHCP服务器之间的DHCP事务获知此主机。相反，CMTS首先看到来自此主机的其他类型的IP流量。此流量可能是Web浏览、电子邮件或“ping”数据包。

虽然192.168.1.77似乎配置了静态IP地址，但可能是此主机实际上获取了DHCP租用，但CMTS可能自事件后就重新启动了，因此它不记得事务。

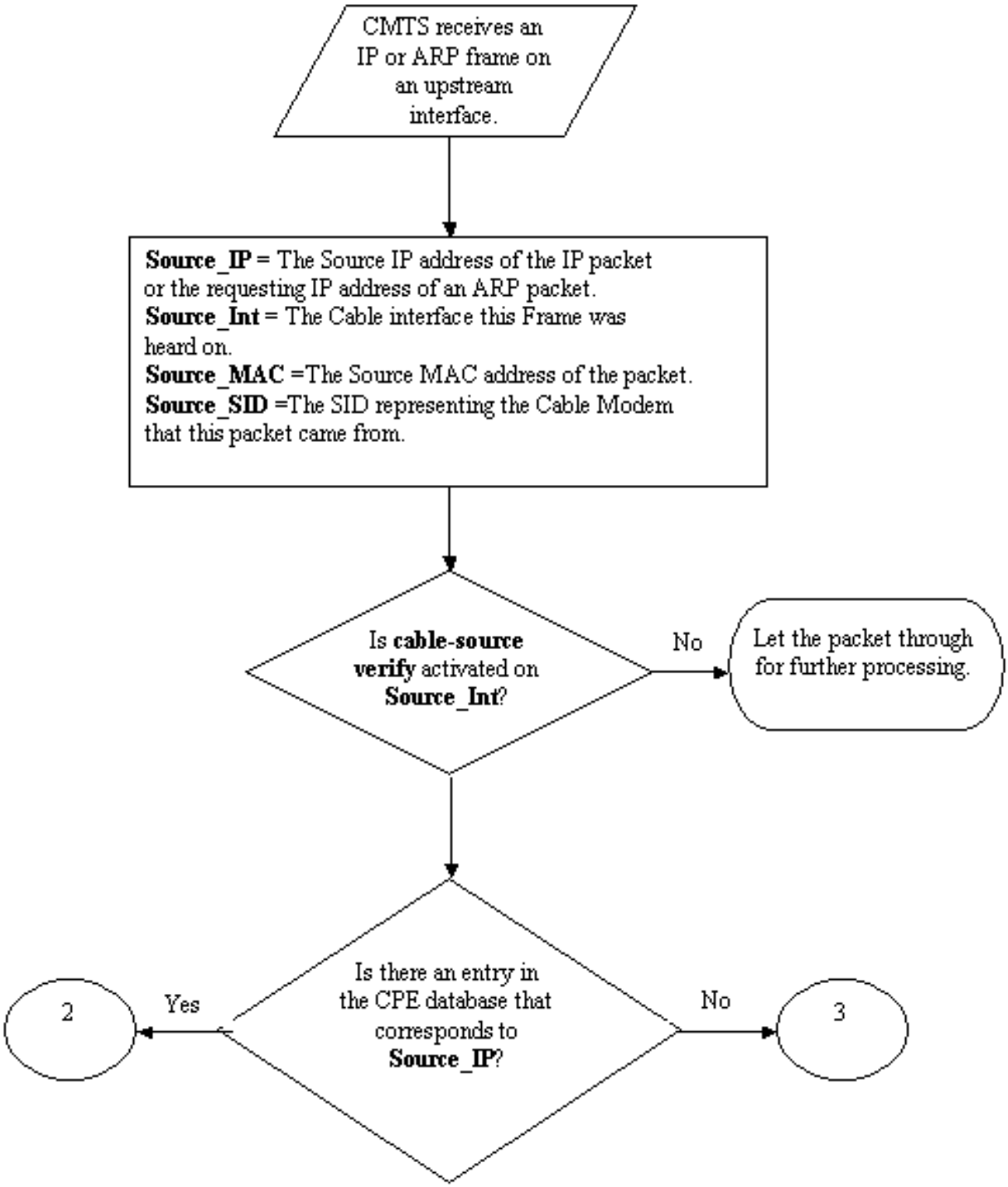
CPE数据库通常由CPE设备与服务提供商的DHCP服务器之间的DHCP事务中的CMTS收集信息来填充。此外，CMTS可以侦听来自CPE设备的其他IP流量，以确定哪些CPE IP和MAC地址属于哪些电缆调制解调器。

Cable Source-Verify 命令

思科已实施cable interface命令cable source-verify [dhcp]。此命令使CMTS利用CPE数据库验证CMTS在其电缆接口上接收的IP数据包的有效性，并允许CMTS做出是否转发这些数据包的智能决

策。

下面的流程图显示了在电缆接口上收到的IP数据包必须经过的额外处理，才能通过CMTS。



流程图1

流程图从CMTS上的上游端口接收的数据包开始，以允许继续处理或丢弃数据包的数据包结束。

示例 1 - 具有重复 IP 地址的方案

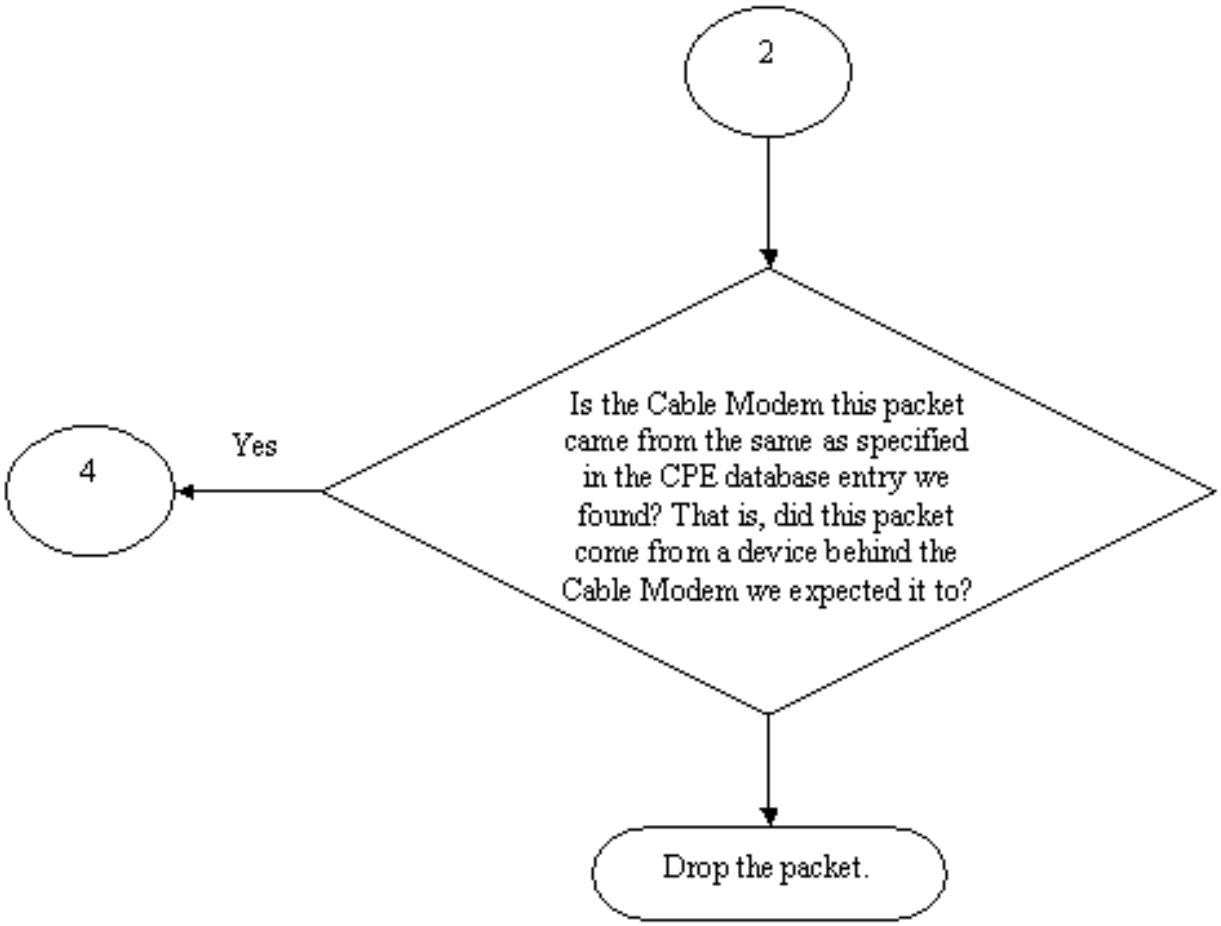
我们将解决的第一个拒绝服务场景是涉及重复IP地址的情况。假设客户A已连接到其服务提供商，并已获得其PC的有效DHCP租用。客户A获得的IP地址称为X。

在A获取其DHCP租用后的某个时间，客户B决定为其PC配置一个静态IP地址，该地址恰好与客户A的设备当前使用的地址相同。与IP地址X相关的CPE数据库信息会根据最后代表X发送ARP请求的CPE设备而改变。

在未受保护的DOCSIS网络中，客户B可能能够说服下一跳路由器（在大多数情况下是CMTS），他有权使用IP地址X，只需代表X向CMTS或下一跳路由器发送ARP请求。这将阻止来自服务提供商的流量转发到客户A。

通过启用电缆源验证，CMTS将能够看到IP地址X的IP和ARP数据包来自错误的电缆调制解调器，因此这些数据包将被丢弃，请参阅流程图2。这包括代表X的源地址为X的所有IP数据包和ARP请求。CMTS日志将显示一条消息，如下：

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



流程图2

使用此信息，将识别两个客户端，并禁用具有连接的重复IP地址的电缆调制解调器。

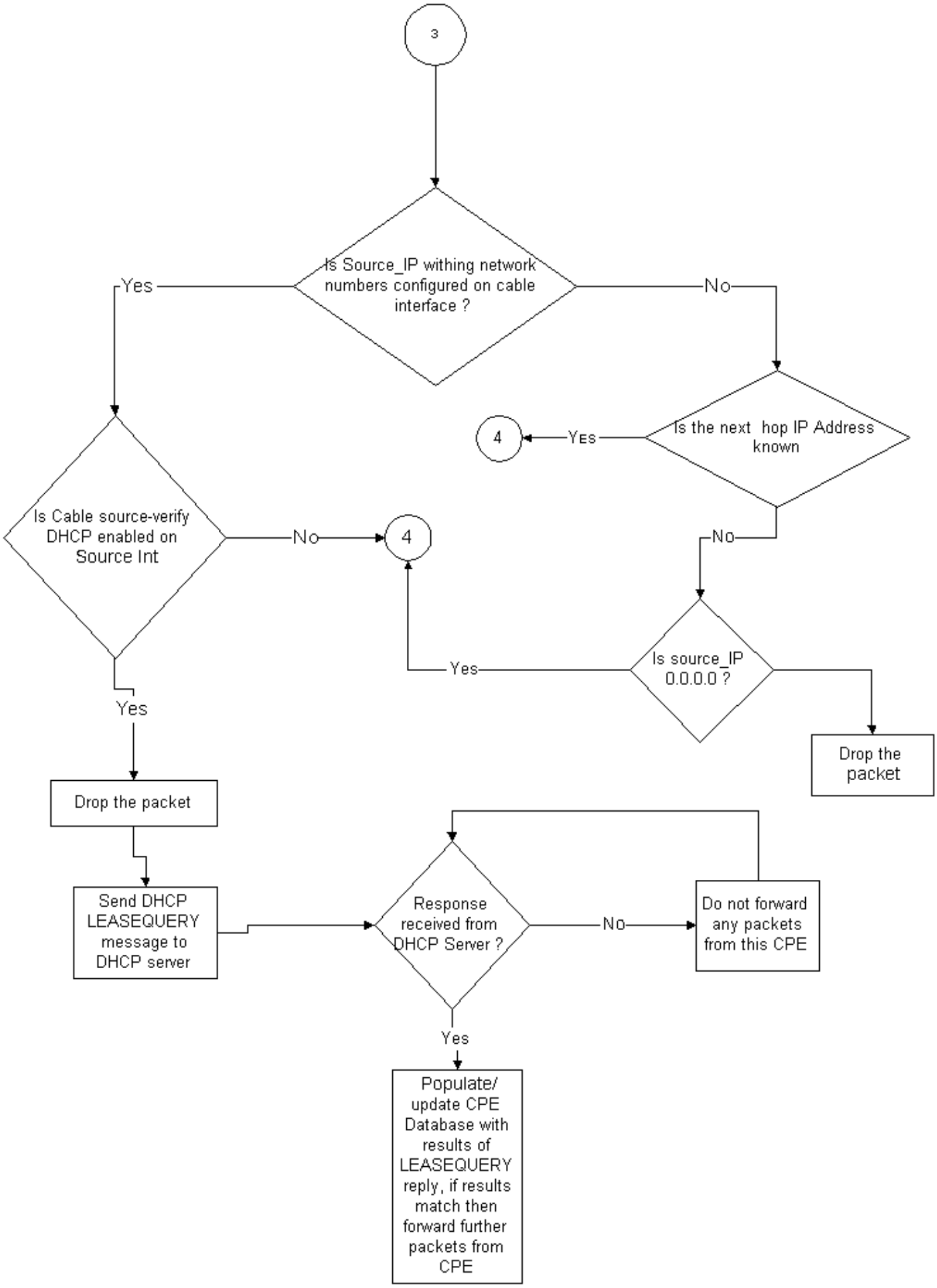
示例 2 - 具有重复 IP 地址的方案 - 使用尚未使用的 IP 地址

另一种情况是，用户将尚未使用的IP地址静态分配给属于合法CPE地址范围的PC。此场景不会对网络中的任何人造成任何服务中断。假设客户B为其PC分配了地址Y。

可能出现的下一个问题是，客户C可能将其工作站连接到服务提供商的网络，并获取IP地址Y的DHCP租用。CPE数据库会临时将IP地址Y标记为属于客户C的电缆调制解调器。但是，不久之后，非合法用户可能会发送适当的ARP流量序列，以使下一跳相信他是IP地址Y的合法所有者，从而导致客户C的服务中断。

同样，通过打开电缆源验证，可以解**决第二个问题**。打开**电缆源验证**后，通过从DHCP事务收集详细信息而生成的CPE数据库条目无法被其他类型的IP流量取代。只有该IP地址的另一个DHCP事务或CMTS上ARP条目超时该IP地址才能取代该条目。这可确保如果最终用户成功获取给定IP地址的DHCP租用，则客户不必担心CMTS变得混乱，并认为其IP地址属于另一用户。

使用cable source-verify dhcp可解决阻止用户使用尚未使用的IP地址**的第一个问题**。通过在此命令的末尾添加dhcp参数，CMTS可以通过向DHCP服务器发出称为LEASEQUERY的特殊类型的DHCP消息来检查它听到的每个新源IP地址的有效性。参见流程图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

对于给定CPE IP地址，LEASEQUERY消息会询问相应的MAC地址和电缆调制解调器是什么。

在这种情况下，如果客户B使用静态地址Y将其工作站连接到有线网络，CMTS将向DHCP服务器发送LEASEQUERY，以验证地址Y是否已租给客户B的PC。DHCP服务器能够通知CMTS，尚未授予IP地址Y的租用，因此客户B将被拒绝访问。

示例 3 - 使用不是由服务提供商提供的网络编号

用户可能在其电缆调制解调器后配置了静态IP地址的工作站，这些地址可能与服务提供商的任何当前网络号不冲突，但将来可能会导致问题。因此，使用电缆源验证，CMTS能够过滤来自源IP地址的数据包，这些数据包不来自CMTS电缆接口上配置的范围。

注：为了使此命令正常工作，您还需要配置**ip verify unicast reverse-path**命令，以防止伪造的IP源地址。请参阅电缆命令：以了解详细信息。

有些客户可能将路由器用作CPE设备，并安排服务提供商将流量路由到此路由器。如果CMTS从源IP地址为Z的CPE路由器接收IP流量，则电缆源验证将允许此数据包通过（如果CMTS具有通过该CPE设备到达网络Z的路由）。请参阅流程图3。

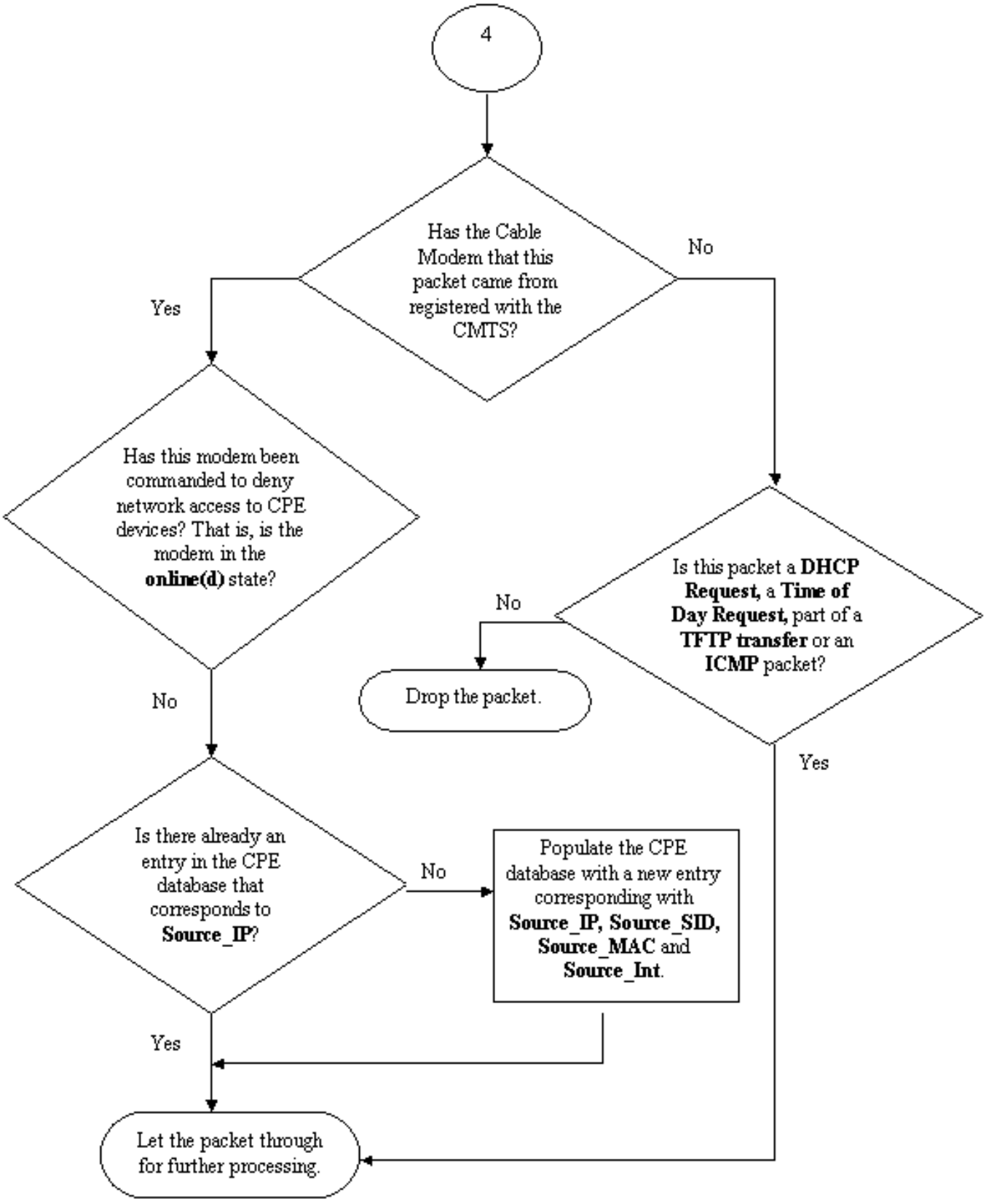
现在考虑以下示例：

在CMTS上，我们有以下配置：

```
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
```

假设源IP地址为172.16.1.10的数据包从电缆调制解调器24.2.2.10到达CMTS，CMTS将看到24.2.2.10不驻留在CPE数据库中， **show int cable x/y modem 0** ，但**ip verify unicast reverse-path启用单播反向路径转发（单播RPF），它检查接口上收到的每个数据包，以验证数据包的源IP地址是否出现在属于该接口的路由表中。**电**缆源验证**检查24.2.2.10的下一跳是什么。在上述配置中，我们有**ip route 24.2.2.0 255.255.255.0 24.1.1.2**，这意味着下一跳是24.1.1.2。现在假设24.1.1.2是CPE数据库中的有效条目，则CMTS会得出以下结论数据包正常，因此将按照流程图4处理该数据包。



流程图4

如何配置cable source-verify

配置cable source-verify只需将cable source-verify**命令**添加到要激活其功能的电缆接口。如果使用电缆接口捆绑，则需要将电**缆源验证**添加到主接口的配置。

如何配置电dhcp

注意： 电缆源验证最初在Cisco IOS软件版本12.0(7)T中引入，在Cisco IOS软件版本12.0SC、12.1EC和12.1T中受支持。

配置**电缆源验证dhcp**需要几个步骤。

确保DHCP服务器支持特殊的DHCP LEASEQUERY消息。

为了使用电缆源**验证dhcp功能**,DHCP服务器必须对draft-ietf-dhcp-leasequery-XX.txt指定的消息进行应答。Cisco Network Registrar 3.5及更高版本能够回答此消息。

确保DHCP服务器支持中继代理信息选项处理。请参阅"中继代理"部分。

DHCP服务器必须支持的另一个功能是DHCP中继信息选项处理。这也称为选项82处理。此选项在DHCP中继信息选项(RFC 3046)中描述。 Cisco Network Registrar 3.5及更高版本支持中继代理信息选项处理，但必须通过Cisco Network Registrar命令行实用程序nrcmd使用以下命令序列激活它：

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

您可能需要替换适当的用户名、密码和服务器IP地址，上面显示默认值。或者，如果您位于nrcmd提示符下，则>nrcmd只需键入以下内容：

dhcp enable save-relay-agent-data

保存

dhcp reload

在CMTS上启用DHCP中继信息选项处理。

中继代理

CMTS必须使用中继代理信息选项标记来自电缆调制解调器和CPE的DHCP请求，以便**电缆源验证dhcp**生效。在运行Cisco IOS软件版本12.1EC、12.1T或更高版本的Cisco IOS的CMTS上，必须在全局配置模式下输入以下命令。

IP DHCP中继信息选项

如果您的CMTS运行的是Cisco IOS软件版本12.0SC系列Cisco IOS，则请改**用cable relay-agent-option** cable interface命令。

根据您所运行的Cisco IOS版本，请小心使用适当的命令。如果更改Cisco IOS系列，请确保更新配置。

当CMTS中继DHCP数据包时，**relay information option**命令会向中继DHCP数据包添加一个名为Option 82的特殊选项或中继信息选项。

选项82填充了一个子选项，即代理电路ID，该子选项引用了DHCP请求所在的CMTS上的物理接口。此外，另一个子选项“代理远程ID”(Agent Remote ID)填充有电缆调制解调器的6字节MAC地址，该DHCP请求是从该调制解调器接收或通过的。

例如，如果MAC地址为99:88:77:66:55:44的PC位于电缆调制解调器a:bb:cc:dd:ee:ff后，CMTS发送DHCP请求，DHCP请求将选项82的Agent Remote ID子选项设置转发到电缆调制解调器的MAC地址a:bb:cc:dd:ee:ff。

通过将中继信息选项包含在来自CPE设备的DHCP请求中，DHCP服务器能够将关于哪个CPE属于哪个电缆调制解调器的信息存储在后面。当在CMTS上配置**cable source-verify dhcp**时，这变得特别有用，因为DHCP服务器不仅能够可靠地通知CMTS特定客户端应具有的MAC地址，而且能够可靠地通知特定客户端应连接到哪个电缆调制解调器特定客户端。

在适当的电缆接口下启用cable source-verify dhcp命令。

最后一步是在要激活**功能的电缆接**口下输入cable source-verify dhcp命令。如果CMTS使用电缆接口捆绑，则必须在捆绑的主接口下输入命令。

结论

cable source-**verify命令**套件允许服务提供商保护有线网络，防止具有未授权IP地址的用户使用该网络。

cable source-verify命令本身是实施IP地址安全的一种有效且简单的方法。虽然它不涵盖所有场景，但它在租用时确保有权使用已分配IP地址的客户不会因为其IP地址被他人使用而受到任何中断。

在本文档中所述的最简单形式中，未通过DHCP配置的CPE设备无法获得网络访问。这是保护IP地址空间并提高有线数据服务的稳定性和可靠性的最佳方法。 但是，拥有商业服务的多个服务运营商(MSO)需要使用静态地址，这些运营商希望对cable source-verify dhcp命令实**施严格的安全性**。

Cisco Network Registrar 5.5版具有响应“保留”地址的租用查询的新功能，即使IP地址未通过DHCP获取。 DHCP服务器在DHCPLEASEQUERY响应中包括租用预留数据。在Network Registrar的以前版本中，DHCPLEASEQUERY响应仅可用于存储MAC地址的租用或之前租用的客户端。例如，Cisco uBR中继代理丢弃没有MAC地址和租用时间（dhcp-lease-time选项）的DHCPLEASEQUERY数据报。

Network Registrar在DHCPLEASERY响应中为保留的租用返回一年的默认租用时间(31536000秒)。如果地址实际是租用的，Network Registrar会返回其剩余租用时间。

相关信息

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