Cable Source-Verify和IP Address Security

目錄

簡介

思科已在思科纜線資料機終端系統(CMTS)產品中實施增強功能，可防止在有線電纜資料服務介面規範(DOCSIS)纜線系統中進行基於IP位址詐騙和IP位址盜竊的特定型別的拒絕服務攻擊。Cisco CMTS Cable Command Reference描述了**cable source-verify**命令套件，這些命令是這些IP地址安全增強功能的一部分。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

未受保護的DOCSIS環境

DOCSIS媒體訪問控制(MAC)域的性質與乙太網段類似。如果不加保護，該網段中的使用者會受到

許多型別的第2層和第3層定址型拒絕服務攻擊。此外，使用者也可能由於其他使用者裝置上地址配置錯誤而降低服務水準。例如：

- 在不同節點上配置重複的IP地址。
- 在不同節點上配置重複的MAC地址。
- 未經授權使用靜態IP地址而不是動態主機配置協定(DHCP)分配的IP地址。
- 未經授權使用網段內的不同網路號。
- 將終端節點配置為代表網段IP子網的一部分應答ARP請求不正確。

儘管在乙太網LAN環境中，通過物理方式跟蹤違規裝置並斷開其連線，可以輕鬆控制和緩解此類問題，但由於網路可能規模較大，DOCSIS網路中的此類問題可能更難隔離、解決和預防。此外，控制和配置客戶端裝置(CPE)的終端使用者可能不具備本地IS支援團隊的優勢，因此無法確保其工作站和PC不會有意或無意地發生配置錯誤。

CMTS CPE資料庫

思科CMTS產品套件維護動態填充的內部資料庫，包括連線的CPE IP和MAC地址。CPE資料庫還包含這些CPE裝置所屬相應電纜數據機的詳細資訊。

通過執行隱藏CMTS命令**show interface cable X/Y modem Z**，可以檢視與特定電纜數據機對應的CPE資料庫的部分檢視。其中，X是線卡號，Y是下游埠號，Z是電纜數據機的服務識別符號(SID)。Z可設定為0以檢視特定下游介面上所有電纜數據機和CPE的詳細資訊。請參見下面此命令生成的典型輸出的示例。

```
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：由於此命令是隱藏的，因此可能會發生更改，並且不能保證在所有版本的Cisco IOS®軟體中都能使用。

在上方示例中，IP地址為192.168.1.90的主機的方法列列為dhcp。這意味著CMTS通過觀察主機與服務提供商的DHCP伺服器之間的DHCP事務來獲知此主機。

列出了IP地址為192.168.1.77的主機的靜態方法。這意味著CMTS沒有首先通過此裝置與DHCP伺服器之間的DHCP事務獲知此主機。相反，CMTS首先看到來自此主機的其他型別的IP流量。此流量可能是Web瀏覽、電子郵件或「ping」資料包。

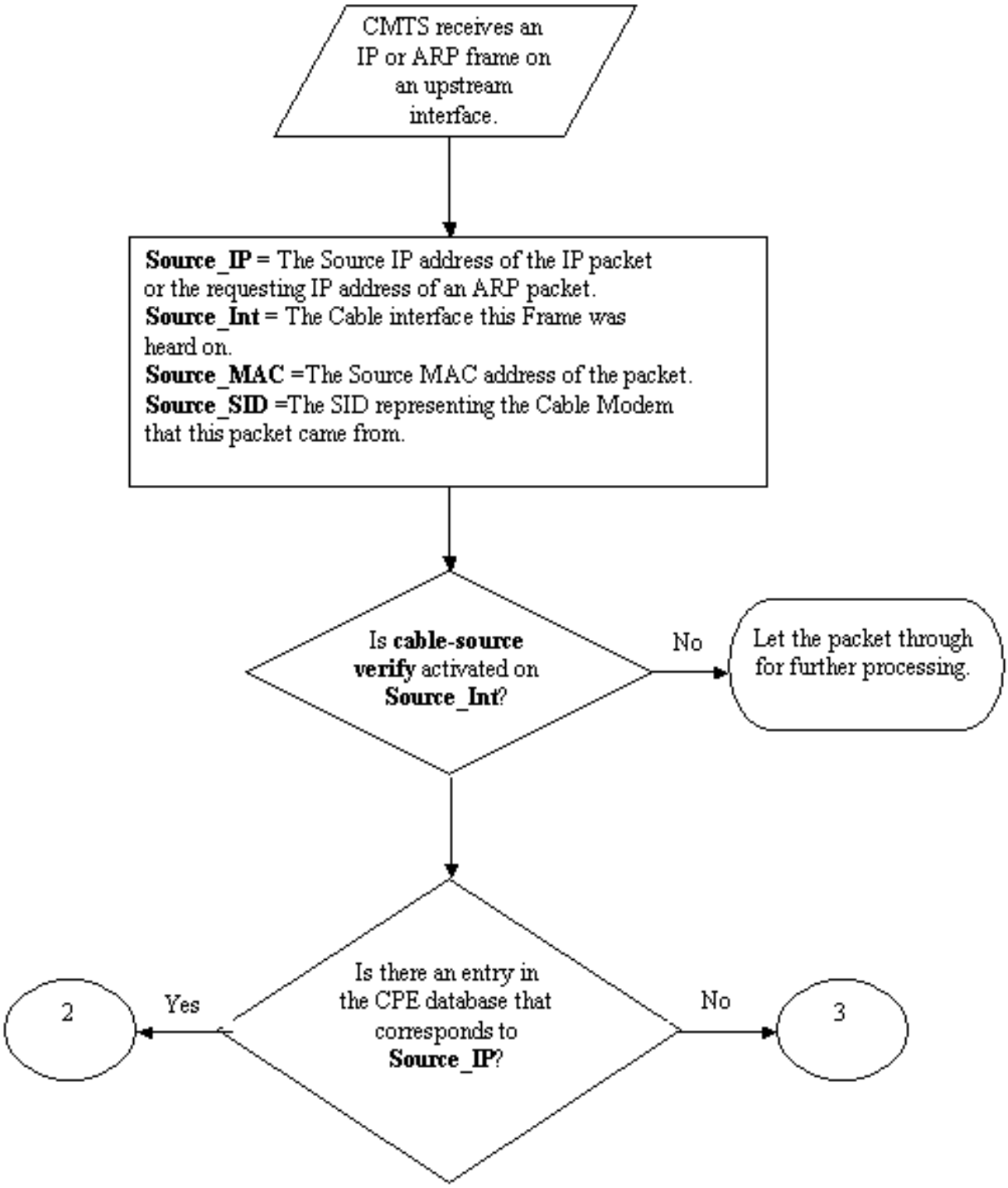
192.168.1.77似乎已配置了靜態IP地址，但可能是該主機實際上獲取了DHCP租用，但是CMTS可能自該事件以來已重新啟動，因此它不記得該事務。

CPE資料庫通常由CMTS從CPE裝置與服務提供商的DHCP伺服器之間的DHCP事務中收集的資訊填充。此外，CMTS可以偵聽來自CPE裝置的其他IP流量，以確定哪些CPE IP和MAC地址屬於哪個纜線資料機。

Cable Source-Verify命令

思科已實施電纜介面命令cable source-verify [dhcp]。此命令使CMTS使用CPE資料庫驗證CMTS在其電纜介面上接收的IP資料包的有效性，並允許CMTS做出是否轉發這些資料包的明智決策。

下面的流程圖顯示了有線介面上接收的IP資料包在允許通過CMTS之前必須經過的額外處理。



流程圖1

該流程圖以由CMTS上的上游埠接收的資料包開始，以允許該資料包繼續進一步處理或丟棄該資料包結束。

示例1 — 具有重複IP地址的方案

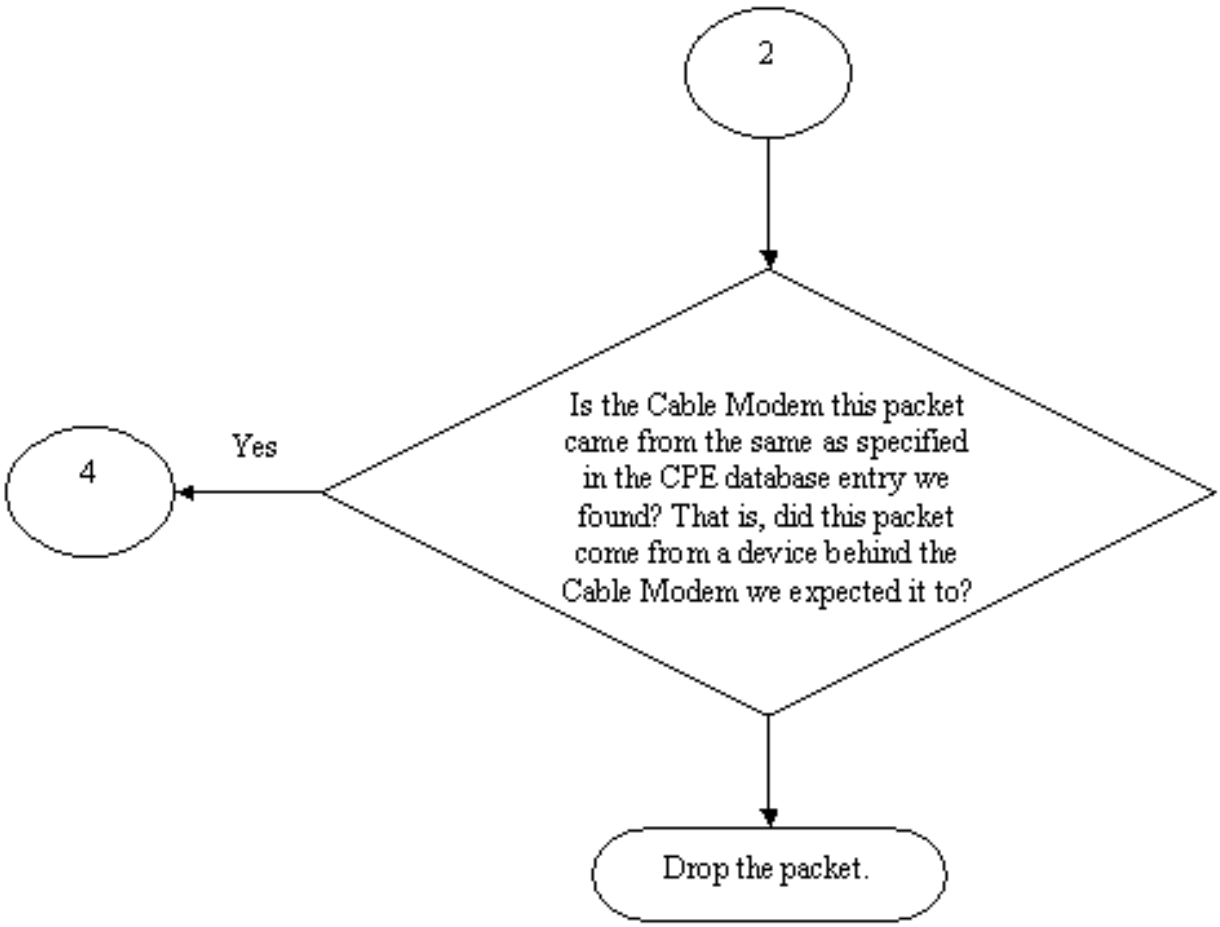
我們將解決的第一個拒絕服務情況是IP地址重複。假設客戶A已連線到其服務提供商，並且已為其PC獲得有效的DHCP租約。客戶A獲得的IP地址將稱為X。

在A獲得其DHCP租用之後，客戶B決定為其PC配置一個靜態IP地址，該地址恰好與客戶A的裝置當前使用的地址相同。有關IP地址X的CPE資料庫資訊會根據最後代表X傳送ARP請求的CPE裝置而變化。

在不受保護的DOCSIS網路中，客戶B可能能夠說服下一跳路由器（多數情況下是CMTS）他有權使用IP地址X，只需代表X向CMTS或下一跳路由器傳送ARP請求即可。這將阻止來自服務提供商的流量轉發到客戶A。

通過啟用纜線來源驗證，CMTS將能夠看到IP位址X的IP和ARP封包是來自錯誤的電纜資料機，因此，這些封包將被捨棄，請參閱流程圖2。這包括所有具有來源位址X的IP封包和代表X的ARP要求。CMTS記錄會顯示一則訊息，如下所示：

%UBR7200-3-BADIPSOURCE:Interface Cable3/0，來自無效源的IP資料包。
IP=192.168.1.10,MAC=0001.422c.54d0，預期SID=10，實際SID=11



流程圖2

使用此資訊可以識別兩個客戶端，並禁用帶有連線的重複IP地址的電纜數據機。

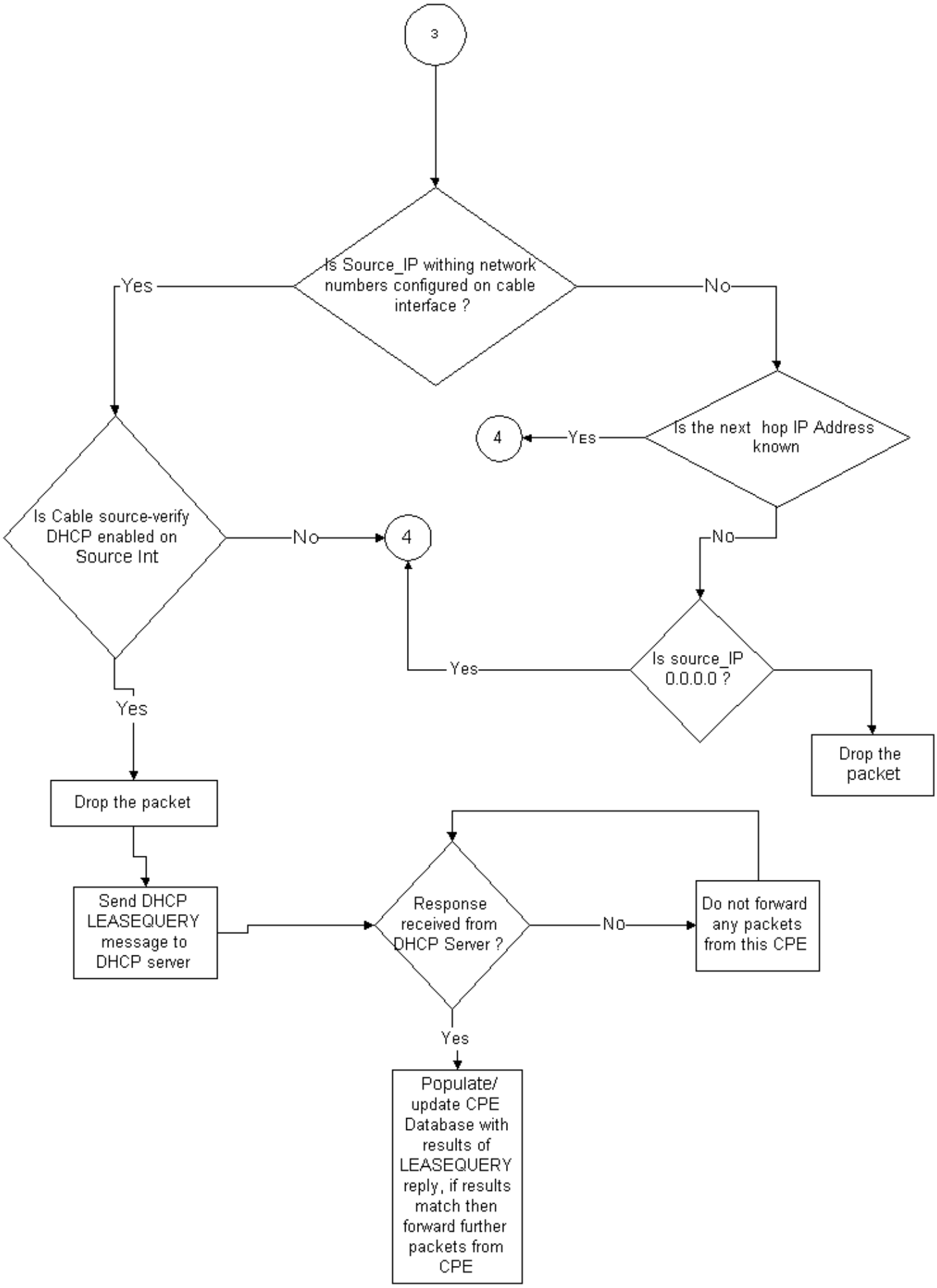
示例2 — 具有重複IP地址的情況 — 使用尚未使用的IP地址

另一種情況是，使用者將尚未使用的IP地址靜態分配給其PC，該PC屬於合法CPE地址範圍。此情況不會導致網路中任何人的服務中斷。假設客戶B為其電腦分配了地址Y。

接下來可能出現的問題是客戶C可能將其工作站連線到服務提供商的網路並獲得IP地址Y的DHCP租約。CPE資料庫會暫時將IP地址Y標籤為屬於客戶C的電纜數據機後面。但是，可能很快就會有客戶B，非合法使用者傳送適當的ARP流量序列，讓下一跳確信他是IP地址Y的合法所有者，從而導致客戶C的服務中斷。

同樣地，第二個問題也可以通過開啟**cable source-verify**來解決。當開啟**cable source-verify**時，通過從DHCP事務中收集詳細資訊生成的CPE資料庫條目不能被其他型別的IP流量所替代。只有該IP地址的另一DHCP事務或該IP地址的CMTS超時上的ARP條目才能取代該條目。這可確保如果終端使用者成功獲得指定IP地址的DHCP租約，該客戶將不必擔心CMTS變得混亂並且認為其IP地址屬於其他使用者。

使用**cable source-verify dhcp**可以解決第一個阻止使用者使用尚未使用的IP地址的問題。通過在此命令末尾新增dhcp引數，CMTS可以通過向DHCP伺服器發出一種稱為LEASEQUERY的特殊型別的DHCP消息，來檢查它所偵聽的每個新的源IP地址的有效性。請參見流程圖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

流程圖3

對於給定的CPE IP地址，LEASEQUERY消息會詢問相應的MAC地址和電纜數據機是什麼。

在這種情況下，如果客戶B將其工作站連線到使用靜態地址Y的電纜網路，則CMTS將向DHCP伺服器傳送LEASEQUERY，以驗證地址Y是否已租給客戶B的PC。DHCP伺服器可以通知CMTS尚未授予IP位址Y的租約，因此將拒絕客戶B存取。

示例3 — 使用服務提供商未調配的網路號

使用者可能在其電纜數據機後配置了靜態IP地址，此地址可能與服務提供商的任何當前網路號不衝突，但可能在將來導致問題。因此，使用纜線來源驗證，CMTS可以過濾出來自來源IP位址（而不是來自CMTS纜線介面上設定的範圍）的封包。

注意：為了使其正常工作，您還需要配置**ip verify unicast reverse-path**命令以防止偽裝IP源地址。請參閱電纜命令：電纜s瞭解詳細資訊。

某些客戶可能將路由器作為CPE裝置，並安排服務提供商將流量路由到此路由器。如果CMTS收到來自源IP地址為Z的CPE路由器的IP流量，則如果CMTS具有通過該CPE裝置屬於的網路Z的路由，cable source-verify將允許此資料包通過。請參閱流程圖3。

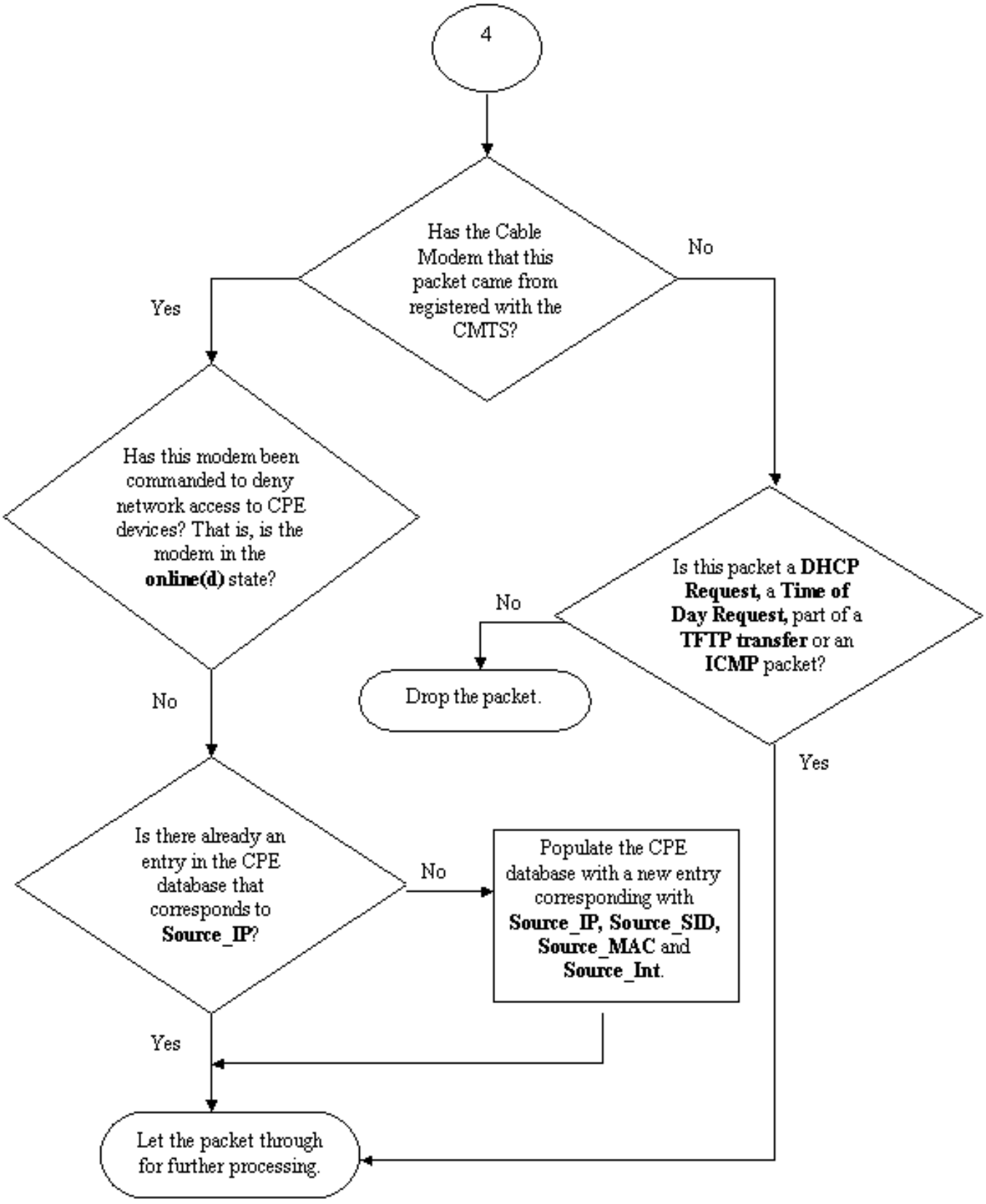
現在考慮以下示例：

在CMTS上，我們有以下配置：

```
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
```

假設源IP地址為172.16.1.10的資料包從電纜數據機24.2.2.10到達CMTS，CMTS會看到24.2.2.10並不位於CPE資料庫**show int cable x/y modem 0**中，但是**ip verify unicast reverse-path**會啟用單播反向路徑轉發（單播RPF），它會檢查介面上接收的每個資料包，以驗證資料包的源IP地址是否出現在該介面的路由表中。**cable source-verify**將檢查24.2.2.10的下一跳是什麼。在以上配置中，我們有**ip route 24.2.2.0 255.255.255.0 24.1.1.2**，這表示下一個躍點是24.1.1.2。現在假設24.1.1.2是CPE資料庫中的有效條目，則CMTS會認為封包沒有問題，因此會根據流程圖4處理封包。



流程圖4

如何配置電纜源驗證

設定cable source-verify時，只需將cable source-verify指令新增到您要在其上啟用功能的電纜介面即可。如果使用電纜介面捆綁，則需要將**電纜**source-verify新增到主介面的配置。

如何配置cable source-verify dhcp

附註： cable source-verify首先在Cisco IOS軟體版本12.0(7)T中匯入，並在Cisco IOS軟體版本12.0SC、12.1EC和12.1T中支援。

配置**cable source-verify dhcp**需要一些步驟。

確保DHCP伺服器支援特殊的DHCP LEASEQUERY消息。

為了使用**cable source-verify dhcp**功能，您的DHCP伺服器必須按照draft-ietf-dhcp-leasequery-XX.txt的要求回答消息。Cisco Network Registrar 3.5及更高版本能夠回答此消息。

確保DHCP伺服器支援中繼代理資訊選項處理。請參閱中繼代理部分。

DHCP伺服器必須支援的另一個功能是DHCP中繼資訊選項處理。這也稱為選項82處理。DHCP中繼資訊選項(RFC 3046)中介紹了此選項。 Cisco Network Registrar 3.5及更高版本支援中繼代理資訊選項處理，但是必須通過Cisco Network Registrar命令列實用程式nrcmd使用以下命令序列來啟用它：

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重新載入

您可能需要替換相應的使用者名稱、密碼和伺服器IP地址，上述內容顯示預設值。或者，如果您在nrcmd提示符下，>nrcmd只需鍵入以下內容：

dhcp enable save-relay-agent-data

儲存

dhcp重新載入

在CMTS上開啟DHCP中繼資訊選項處理。

中繼代理

CMTS必須使用中繼代理資訊選項標籤來自纜線資料機和CPE的DHCP請求，以便**cable source-verify dhcp**有效。以下命令必須在全域性配置模式下輸入運行Cisco IOS軟體版本12.1EC、12.1T或更高版本的Cisco IOS的CMTS。

ip dhcp relay information option

如果您的CMTS執行的是Cisco IOS軟體版本12.0SC系列Cisco IOS，則改用**cable relay-agent-option** cable interface指令。

請注意根據您運行的Cisco IOS版本使用適當的命令。如果您變更Cisco IOS系列產品，請確保更新您的配置。

當CMTS中繼DHCP資料包時，**relay information option**命令將名為Option 82的特殊選項或中繼資訊選項新增到中繼的DHCP資料包。

選項82中填充了一個子選項Agent Circuit-ID，該子選項引用了監聽DHCP請求的CMTS上的物理介面。除此之外，另一個子選項Agent Remote ID也使用接收或通過DHCP請求的電纜數據機的6位元組MAC地址填充。

例如，如果MAC地址為99:88:77:66:55:44的PC位於電纜數據機後面aa:bb:cc:dd:ee:ff傳送DHCP請求，CMTS會將設定選項82的Agent Remote ID子選項的DHCP請求轉發到電纜數據機的MAC地址aa:bb:cc:dd:ee:ff。

通過在CPE裝置的DHCP請求中包括中繼資訊選項，DHCP伺服器能夠儲存有關哪個CPE屬於哪一個纜線資料機的資訊。當CMTS上配置了**cable source-verify dhcp**時，這一點特別有用，因為DHCP伺服器不僅能夠可靠地通知CMTS特定客戶端應該具有哪個MAC地址，而且能夠告知要連線到哪個電纜數據機特定的客戶端。

在相應的電纜介面下啟用cable source-verify dhcp命令。

最後一步是在您要啟用功能的電纜介面下輸入**cable source-verify dhcp**命令。如果CMTS使用電纜介面捆綁，則必須在捆綁包的主介面下輸入命令。

結論

cable source-verify指令套件允許服務提供者保護纜線網路，防止具有未授權IP位址的使用者使用網路。

cable source-verify命令本身是實現IP地址安全性的有效且簡便的方法。雖然它並不涵蓋所有情形，但至少能確保擁有分配的IP地址使用權的客戶不會因為其IP地址被其他人使用而遇到任何中斷。

在本文檔所述的最簡單形式中，未通過DHCP配置的CPE裝置無法獲得網路訪問。這是保護IP地址空間和提高有線電纜資料服務穩定性和可靠性的最佳方法。 但是，多個具有要求其使用靜態地址的商業服務的服務運營商(MSO)希望實現命令**cable source-verify dhcp的嚴格安全性**。

Cisco Network Registrar 5.5版具有響應「保留」地址租用查詢的新功能，即使IP地址不是通過DHCP獲取的。 DHCP伺服器在DHCPLEASEQUERY響應中包括租用保留資料。在Network Registrar的先前版本中，DHCPLEASEQUERY響應僅可用於儲存MAC地址的租用或先前租用客戶端。例如，Cisco uBR中繼代理丟棄沒有MAC地址和租用時間（dhcp-lease-time選項）的DHCPLEASEQUERY資料包。

對於DHCPLEASEQUERY響應中的保留租約，Network Registrar將返回預設租賃時間：一年(31536000秒)。如果地址實際租用，Network Registrar將返回其剩餘租用時間。

相關資訊

- **DHCP中繼資訊選項(RFC 3046)**
- **技術支援與文件 - Cisco Systems**