Segurança de Endereço IP e Verificação de Origem de Cabo

Contents

Introduction

A Cisco implementou melhorias nos produtos Cisco Cable Modem Termination System (CMTS) que inibem certos tipos de ataques de negação de serviço com base na falsificação de endereços IP e roubo de endereços IP em sistemas de cabos DOCSIS (Data-over-Cable Service Interface Specifications). A Referência de Comandos de Cabo do Cisco CMTS descreve o conjunto de comandos **cable source-verify que fazem parte desses aprimoramentos de segurança de endereços IP.**

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

O ambiente desprotegido DOCSIS

Um domínio DOCSIS MAC (Controle de acesso de mídia) é semelhante em natureza a um segmento de Ethernet. Se ficarem desprotegidos, os usuários neste segmento estarão vulneráveis a vários tipos de ataques de Recusa de serviço baseados em endereçamento de camada 2 e camada 3. Além disso, é possível que os usuários sofram um nível de serviço degradado devido à configuração incorreta de endereçamento em equipamentos de outros usuários. Os exemplos incluem:

- Configurando endereços IP duplicados em nós diferentes.
- Configurando endereços MAC duplicados em nós diferentes.
- O uso não autorizado de endereços IP estáticos em vez de endereços IP atribuídos ao Protocolo de Configuração de Host Dinâmico (DHCP).
- O uso não autorizado dos diferentes números de rede de um segmento.
- Configuração incorreta dos nós finais para responder às solicitações de ARP em nome de parte da sub-rede IP de segmento.

Embora esses tipos de problemas sejam fáceis de controlar e mitigar em um ambiente de Ethernet LAN rastreando fisicamente e desconectando o equipamento ofensivo, como problemas nas redes DOCSIS podem ser mais difíceis de isolar, solucionar e impedir devido ao grande tamanho da rede. Além disso, os usuários finais que controlam e configuram o Customer Premise Equipment (CPE) podem não ter o benefício de uma equipe de suporte IS local para garantir que suas estações de trabalho e PCs não sejam, intencionalmente ou não, configurados incorretamente.

O banco de dados CMTS CPE

O conjunto Cisco de produtos CMTS mantém um banco de dados dos endereços CPE IP e MAC conectados preenchidos dinamicamente. O banco de dados de CPE também contém detalhes sobre os Modems a Cabo correspondentes aos quais esses dispositivos de CPE pertencem.

Uma visualização parcial do Banco de Dados CPE correspondente a determinado modem a cabo pode ser obtida pela execução do comando oculto do CMTS show interface cable X/Y modem Z. Aqui, X é o número da placa de linha, Y é o número da porta de downstream e Z é o SID (Identificador de serviço) do modem a cabo. Z pode ser definido como 0 para exibir detalhes sobre todos os modems a cabo e CPE em uma interface downstream específica. Consulte o exemplo abaixo de uma saída típica gerada por esse comando.

```
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
```

Observação: como esse comando está oculto, ele está sujeito a alterações e não está garantido que esteja disponível em todas as versões do software Cisco IOS®.

No exemplo acima, a coluna de método do host com endereço IP 192.168.1.90 é listada como dhcp. Isso significa que o CMTS aprendeu sobre esse host observando as transações de DHCP

entre o host e o servidor de DHCP do provedor de serviço.

O host com endereço IP 192.168.1.77 está listado com método estático. Isso significa que o CMTS não aprendeu primeiro sobre esse host através de uma transação DHCP entre esse dispositivo e um servidor DHCP. Em vez disso, o CMTS viu primeiro outros tipos de tráfego de IP do seu host. Esse tráfego pode ter sido pesquisa na Web, e-mail ou pacotes de "ping".

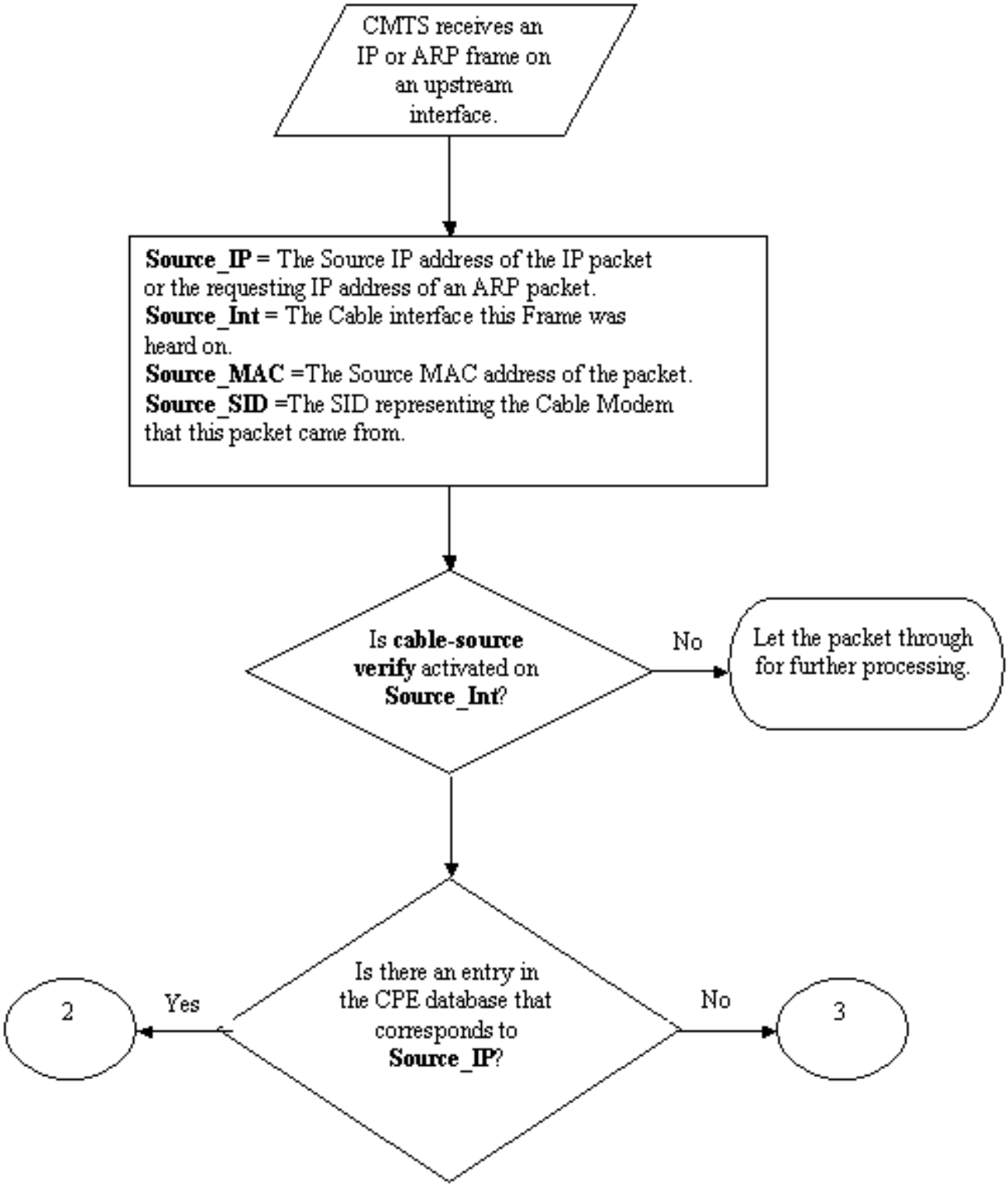
Embora pareça que o 192.168.1.77 foi configurado com um endereço IP estático, é possível que este host na verdade tenha adquirido uma concessão de DHCP, mas o CMTS pode ter sido reinicializado desde o evento e portanto não se lembra da transação.

Normalmente, o banco de dados de CPE é preenchido pelo CMTS coletando informações das transações DHCP entre dispositivos CPE e o servidor DHCP do provedor de serviços. Além disso, o CMTS pode ouvir outro tráfego IP de entrada dos dispositivos CPE para determinar quais endereços IP CPE e MAC pertencem a quais Modems a Cabo.

O comando cable source-verify

O Cisco implementou o comando cable source-verify [dhcp] da interface de cabo. Esse comando faz com que o CMTS utilize o banco de dados CPE para verificar a validade dos pacotes IP que o CMTS recebe em suas interfaces de cabo, e permite que o CMTS tome decisões inteligentes quanto a encaminhá-los ou não.

O fluxograma abaixo mostra que o processamento extra em um pacote IP recebido em uma interface de cabo deve ser bem-sucedido para que possa prosseguir pelo CMTS.



Fluxograma 1

O gráfico de fluxo começa com um pacote sendo recebido por uma porta upstream no CMTS e termina com o pacote tendo permissão de continuar para processamento adicional ou com o

descarte do pacote.

Exemplo 1 - Cenário com endereços IP duplicados

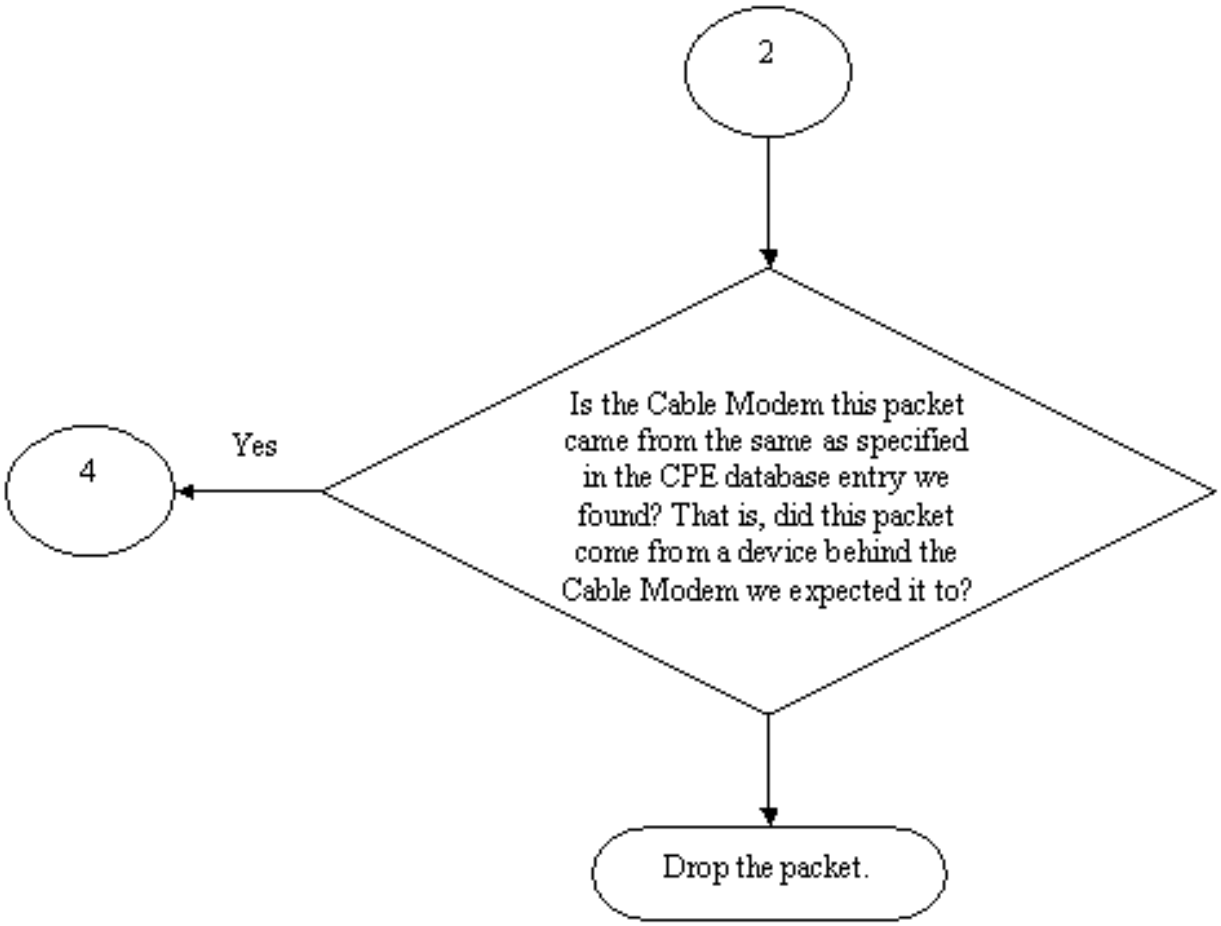
O primeiro cenário de Rejeição de Serviço que vamos abordar é a situação que envolve endereços IP duplicados. Suponhamos que o cliente A esteja conectado ao seu provedor de serviços e tenha obtido um aluguel de DHCP válido para seu PC. O endereço IP que o cliente A obteve será conhecido como X.

Às vezes, após A adquirir seu aluguel de DHCP, o cliente B decide configurar o PC com um endereço IP estático que, por acaso, é igual ao endereço IP atualmente em uso no equipamento do Cliente A. As informações do banco de dados CPE em relação ao endereço IP X seriam alteradas dependendo do dispositivo CPE que enviou pela última vez uma solicitação ARP em nome de X.

Em uma rede DOCSIS desprotegida, o cliente B pode conseguir convencer o roteador de próximo salto (na maioria dos casos, o CMTS) de que tem o direito de utilizar o endereço de IP X simplesmente enviando uma requisição ARP em nome de X ao CMTS ou roteador de próximo salto. Isso interromperia o tráfego do provedor de servidor do encaminhamento para o Cliente A.

Ao habilitar a verificação da fonte do cabo, o CMTS seria capaz de ver que os pacotes IP e ARP para o endereço IP X estavam sendo originados do modem a cabo errado e, portanto, esses pacotes seriam descartados, consulte o fluxograma 2. Isso inclui todos os pacotes IP com o endereço de origem X e solicitações ARP em nome de X. Os registros CMTS mostrariam uma mensagem na linha de:

%UBR7200-3-BADIPSOURCE: Interface Cable3/0, pacote IP de origem inválida. IP=192.168.1.10, MAC=0001.422c.54d0, SID esperado=10, SID real=11



Fluxograma 2

Utilizando essas informações, os dois clientes seriam identificados, e o modem a cabo com o endereço IP duplicado conectado poderia ser desabilitado.

Exemplo 2 - Cenário com endereços IP duplicados - Uso de um endereço IP que ainda não foi usado

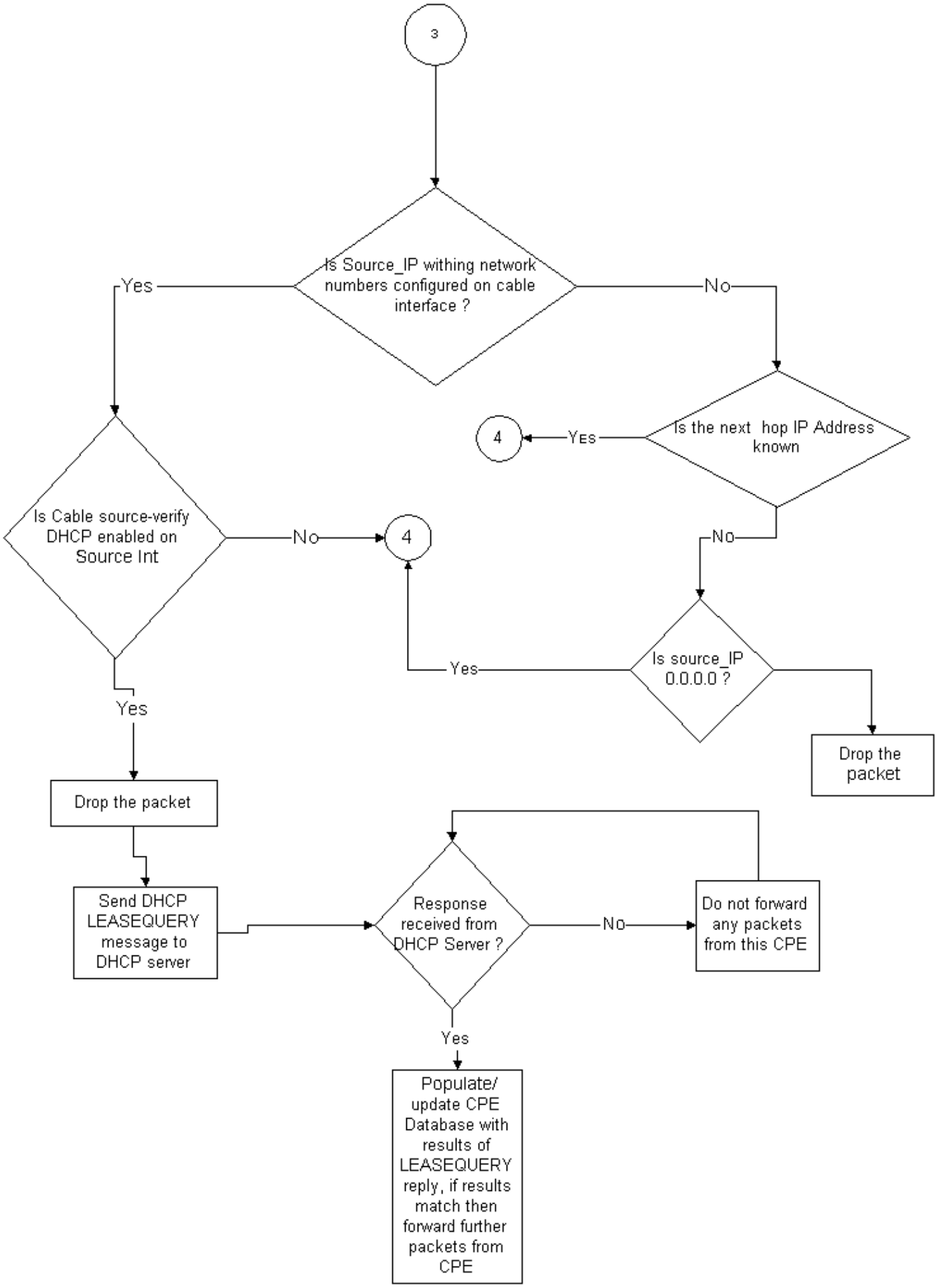
Outro cenário é que um usuário atribua estaticamente um endereço IP ainda não utilizado a seu PC que esteja dentro do intervalo legítimo de endereços CPE. Este cenário não causa qualquer tipo de interrupção dos serviços a ninguém na rede. Digamos que o cliente B atribuiu um endereço Y ao PC deles.

O próximo problema que pode surgir é que o Cliente C pode conectar sua estação de trabalho à rede do provedor de serviços e adquirir um aluguel de DHCP para o endereço IP Y. O banco de dados CPE marcaria temporariamente o endereço IP Y como pertencente ao modem a cabo do cliente C. No entanto, pode não demorar muito até que o Cliente B, o usuário não legítimo, envie a sequência adequada de tráfego ARP para convencer o próximo salto de que ele era o proprietário legítimo do endereço IP Y, causando, assim, uma interrupção no serviço do Cliente C.

Da mesma forma, o segundo problema pode ser resolvido ligando-se a **verificação da fonte do cabo**. Quando a verificação de origem do cabo está ativada, uma entrada do banco de dados

CPE que foi gerada por detalhes graduais de uma transação DHCP não pode ser substituída por outros tipos de tráfego IP. Somente outra transação DHCP para esse endereço IP ou a entrada ARP no intervalo de tempo do CMTS para esse endereço IP pode substituir a entrada. Isso garante que, se um usuário final adquirir com êxito um aluguel de DHCP para um determinado endereço IP, esse cliente não precisará se preocupar com o CMTS se tornando confuso e pensando que seu endereço IP pertence a outro usuário.

O primeiro problema de impedir que os usuários usem endereços IP ainda não utilizados pode ser resolvido com o **dhcp de verificação de fonte de cabo**. Ao adicionar o parâmetro dhcp ao final desse comando, o CMTS pode verificar a validade de cada novo endereço IP de origem que ouve ao emitir um tipo especial de mensagem DHCP chamada LEASEQUERY para o servidor DHCP. Consulte o Fluxograma 3.



Fluxograma 3

Para determinado endereço CPE IP, a mensagem LEASEQUERY pergunta o que são o endereço MAC correspondente e o Modem a Cabo.

Nessa situação, se o Cliente B conectar sua estação de trabalho à rede a cabo com o endereço estático Y, o CMTS enviará uma LEASEQUERY ao servidor DHCP para verificar se o endereço Y foi concedido ao PC do Cliente B. O servidor DHCP pode informar ao CMTS que nenhum aluguel foi concedido para o endereço IP Y e que, portanto, o cliente B terá o acesso negado.

Exemplo 3 - Uso de um número de rede não fornecido pelo provedor de serviços

Os usuários têm estações de trabalho configuradas atrás de modems a cabo com endereços IP estáticos que podem não conflitar com qualquer número de rede atual do provedor de serviços, mas podem causar problemas no futuro. Portanto, usando o comando cable source-verify, um CMTS pode filtrar pacotes originários de endereços IP que não estejam na faixa configurada na interface do cabo CMTS.

Observação: para que isso funcione corretamente, você também precisa configurar o comando **ip verify unicast reverse-path** para evitar endereços IP de origem falsificados. Consulte Comandos de Cabo: para obter mais informações.

Alguns clientes podem ter um roteador como dispositivo CPE e providenciar para que o provedor de serviço roteie o tráfego até esse roteador. Se o CMTS recebe tráfego IP do roteador CPE com um endereço IP de origem definido como Z, a verificação de origem de cabo permitirá que esse pacote passe se o CMT tiver um roteador para a rede a que pertence Z, por meio do dispositivo CPE. Consulte o fluxograma 3.

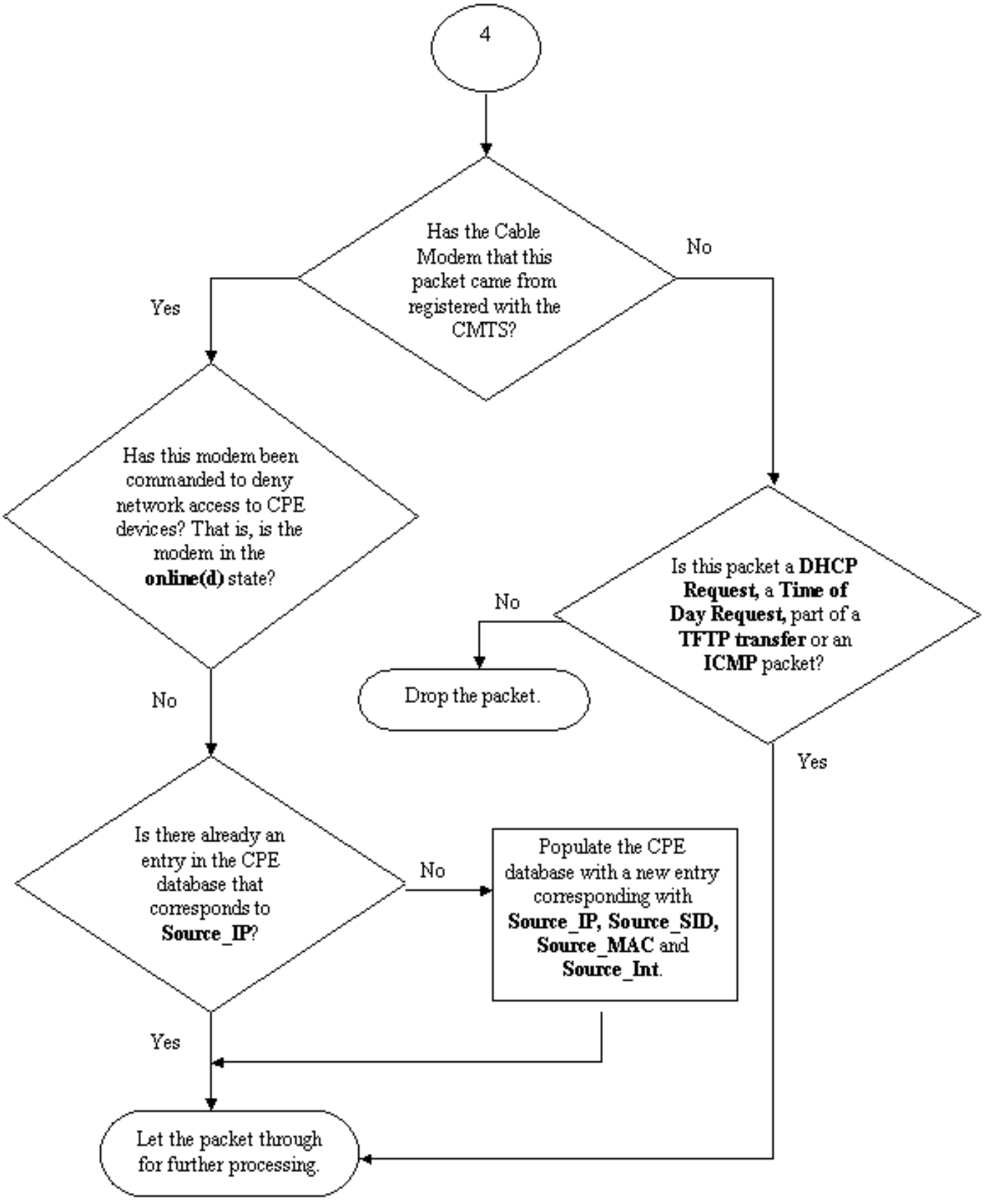
Agora, considere o seguinte exemplo:

No CMTS, temos a configuração a seguir:

```
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
```

Supondo que um pacote com o endereço IP de origem 172.16.1.10 tenha chegado ao CMTS do modem a cabo 24.2.2.10, o CMTS veria que 24.2.2.10 não reside no banco de dados do CPE, **show int cable x/y modem 0**, no entanto, **ip verify unicast reverse-path** ativa Fast Reverse Path Forwarding (Unicast RPF), que verifica cada pacote recebido em uma interface para verificar se o endereço IP origem do pacote aparece nas tabelas de roteamento que pertencem a essa interface. O **cabo source-verify** verifica qual é o próximo salto para 24.2.2.10. Na configuração acima, temos o IP Route 24.2.2.0 255.255.255.0 24.1.1.2 que significa que o Next Hop é 24.1.1.2. Presumindo que 24.1.1.2 é uma entrada válida no banco de dados CPE, o CMTS conclui que o pacote está OK e, por isso, processará o pacote por Fluxograma 4.



Fluxograma 4

Como configurar a verificação de origem de cabo

Configurar o **cable source-verify** envolve simplesmente adicionar o comando **cable source-verify** à interface de cabo na qual você gostaria de ativar a função. Se estiver usando o agrupamento de interface de cabo, você precisará adicionar **cable source-verify** à configuração da interface

primária.

Como configurar `dhcp de verificação de fonte de cabo`

Observação: a verificação da fonte do cabo foi introduzida pela primeira vez no Cisco IOS Software Release 12.0(7)T e é suportada nas versões 12.0SC, 12.1EC e 12.1T do Cisco IOS Software.

A configuração de cable source-verify dhcp requer a execução de alguns passos.

Verifique se o servidor DHCP oferece suporte à mensagem especial DHCP LEASEQUERY.

Para usar a funcionalidade **dhcp de verificação de origem de cabo**, o servidor DHCP deve responder às mensagens conforme especificado por draft-ietf-dhcp-leasequery-XX.txt. O Cisco Network Registrar versões 3.5 e superiores podem responder a esta mensagem.

Certifique-se de que o servidor DHCP suporta o processamento da opção de informações de agente de retransmissão. Consulte a seção Relay Agent.

Um outro recurso que deve ser suportado pelo servidor DHCP é o processamento da opção de informações de transmissão de DHCP. Isso é conhecido como processamento da Opção 82. Esta opção é descrita na DHCP Relay Information Option (Opção de informações de transmissão DHCP) (RFC 3046). As versões 3.5 e superiores do Cisco Network Registrar suportam processamento de Relay Agent Information Option, entretanto ele deve ser ativado por meio do utilitário da linha de comando nrcmd do Cisco Network Registrar com a seqüência de comandos a seguir:

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

Talvez seja necessário substituir o nome de usuário, a senha e o endereço IP do servidor apropriados; os valores acima são os valores padrão. Como alternativa, se você estiver no prompt nrcmd, >nrcmd, digite o seguinte:

dhcp enable save-relay-agent-data

save

dhcp reload

Ative o processamento da opção de informação de transmissão de DHCP no CMTS.

Agente de transmissão

O CMTS deve marcar as solicitações DHCP dos modems a cabo e do CPE com a opção de informações do agente de retransmissão para que o **dhcp de verificação de fonte de cabo** seja eficaz. Os comandos a seguir devem ser inseridos no modo de configuração global em um CMTS executando Cisco IOS Software Releases 12.1EC, 12.1T ou versões posteriores do Cisco IOS.

ip dhcp relay information option

Se o CMTS estiver executando as versões de treinamento 12.0SC do software Cisco IOS, o Cisco IOS usará o comando cable relay-agent-option cable interface.

Tenha cuidado para usar os comandos apropriados, dependendo da versão do Cisco IOS que você está executando. Certifique-se de atualizar sua configuração se você alterar trens do Cisco IOS.

Os comandos relay information option adicionam uma opção especial denominada Option 82 (Opção 82), ou opção de informações de retardo, ao pacote DHCP retardado quando o CMTS retarda pacotes DHCP.

A opção 82 é ocupada com uma subopção, a Agent Circuit-ID, que se relaciona com a interface física no CMTS em que a solicitação de DHCP foi percebida. Além disso, outra subopção, Agent Remote ID, é preenchida com o endereço MAC de 6 bytes do modem a cabo que enviou ou repassou a requisição DHCP.

Por exemplo, se um PC com endereço MAC 99:88:77:66:55:44, que está por trás do modem a cabo aa:bb:cc:dd:ee:ff envia uma solicitação DHCP, o CMTS encaminhará a configuração da solicitação DHCP da subopção ID Remota do Agente da Opção 82 para o endereço MAC do modem a cabo, aa:bb:cc:cc:e: ff.

Ao incluir a Opção Relay Information (Informações de Retardo) na solicitação DHCP de um dispositivo CPE, o servidor DHCP será capaz de armazenar as informações sobre qual CPE pertence a quais modems a cabo. Isso se torna muito útil quando o cabo de verificação de origem dhcp está configurado no CMTS, porque o servidor DHCP é capaz de informar com confiança ao CTMS não apenas sobre que endereço MAC um cliente específico deve ter, mas a que modem a cabo o cliente específico deve estar conectado.

Habilite o comando cable source-verify dhcp na interface de cabo adequada.

A etapa final é inserir o comando cable source-verify dhcp na interface de cabo na qual você gostaria de ativar o recurso. Se o CMTS estiver usando o agrupamento de interface de cabo, insira o comando na interface primária do pacote.

Conclusão

O conjunto de comandos cable source-verify permite que um provedor de serviços proteja a rede a cabo contra a utilização por usuários com endereços IP não autorizados.

O comando cable source-verify sozinho é uma forma fácil e eficaz de implementar a segurança do endereço IP. Embora não abranja todos os cenários, pelo menos, garante que os clientes com o direito de usar os endereços IP atribuídos não encontrarão interrupções tendo seu endereço IP usado por outra pessoa.

Em sua forma mais simples como descrito neste documento, um dispositivo CPE não configurado via DHCP não pode obter acesso à rede. Essa é a melhor maneira de proteger o espaço de endereços IP e aumentar a estabilidade e a confiabilidade de um serviço de Dados por Cabo. No entanto, vários operadores de serviço (MSOs) que possuem serviços comerciais que exigiam o uso de endereços estáticos queriam implementar uma segurança rigorosa do comando **cable source-verify dhcp**.

O Cisco Network Registrar versão 5.5 tem um novo recurso de responder à consulta de leasing para endereços "reservados", mesmo que o endereço IP não tenha sido obtido via DHCP. O servidor DHCP inclui dados de reserva de concessão nas respostas DHCPLEASEQUERY. Nas versões anteriores do Network Registrar, as respostas de DHCPLEASEQUERY eram possíveis apenas para clientes alugados ou anteriormente alugados para os quais o endereço MAC estava armazenado. Os agentes de retransmissão Cisco uBR, por exemplo, descartam os datagramas DHCPLEASEQUERY que não têm um endereço MAC e um tempo de concessão (opção dhcp-lease-time).

O Network Registrar retorna um tempo de uso padrão de um ano (31536000 segundos) para usos reservados em uma resposta DHCPLEASEQUERY. Se o endereço é realmente alugado, o Network Registrar retorna seu tempo de leasing restante.

Informações Relacionadas

- Opção de Informações de Retransmissão DHCP (RFC 3046)
- Suporte Técnico e Documentação - Cisco Systems