Segurança de Endereço IP e Verificação de Origem de Cabo

Índice

Introdução

Cisco executou realces dentro do Produtos do sistema de terminação do cable modem Cisco (CMTS) que inibe os determinados tipos de ataque de recusa de serviço baseados na falsificação do endereço IP de Um ou Mais Servidores Cisco ICM NT e no roubo do endereço IP de Um ou Mais Servidores Cisco ICM NT em sistemas de cabo do Data-over-Cable Service Interface Specifications (DOCSIS). **Este documento descreve o conjunto dos cabos de verificação de fonte dos comandos que fazem parte dessas melhorias na segurança dos endereços IP.**

Antes de Começar

Convenções

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

Pré-requisitos

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, é possível para usuários sofrer um nível degradado do serviço devido ao malconfiguration do endereçamento no equipamento do outro usuário. 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 ajustado a 0 para ver detalhes sobre todo o Modems a cabo e CPE em uma relação do downstream particular. 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
```

Nota: Desde que este comando é hidden, é sujeito mudar e não é garantido para estar disponível em todas as liberações do software de Cisco IOS®.

No exemplo acima, a coluna de método do host com endereço IP 192.168.1.90 é alistada como o

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. Isto significa que o CMTS não aprendeu primeiramente deste host através de uma transação de DHCP entre este 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".

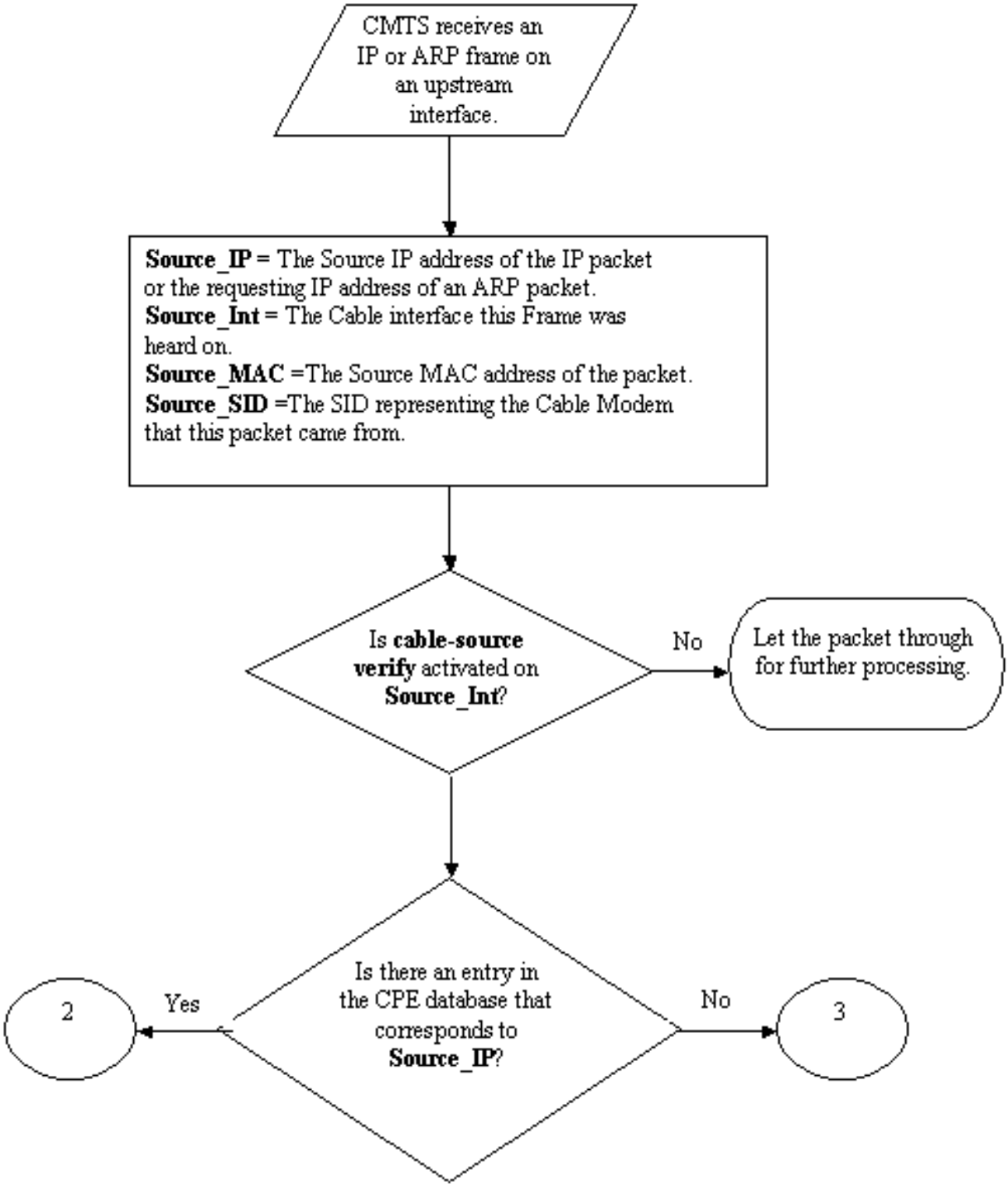
Embora pareça que o 192.168.1.77 foi configurado com um endereço IP estático, é possível que este host na verdade tenha adquirido uma concessão de DHCP, mas o CMTS pode ter sido reinicializado desde o evento e portanto não se lembra da transação.

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

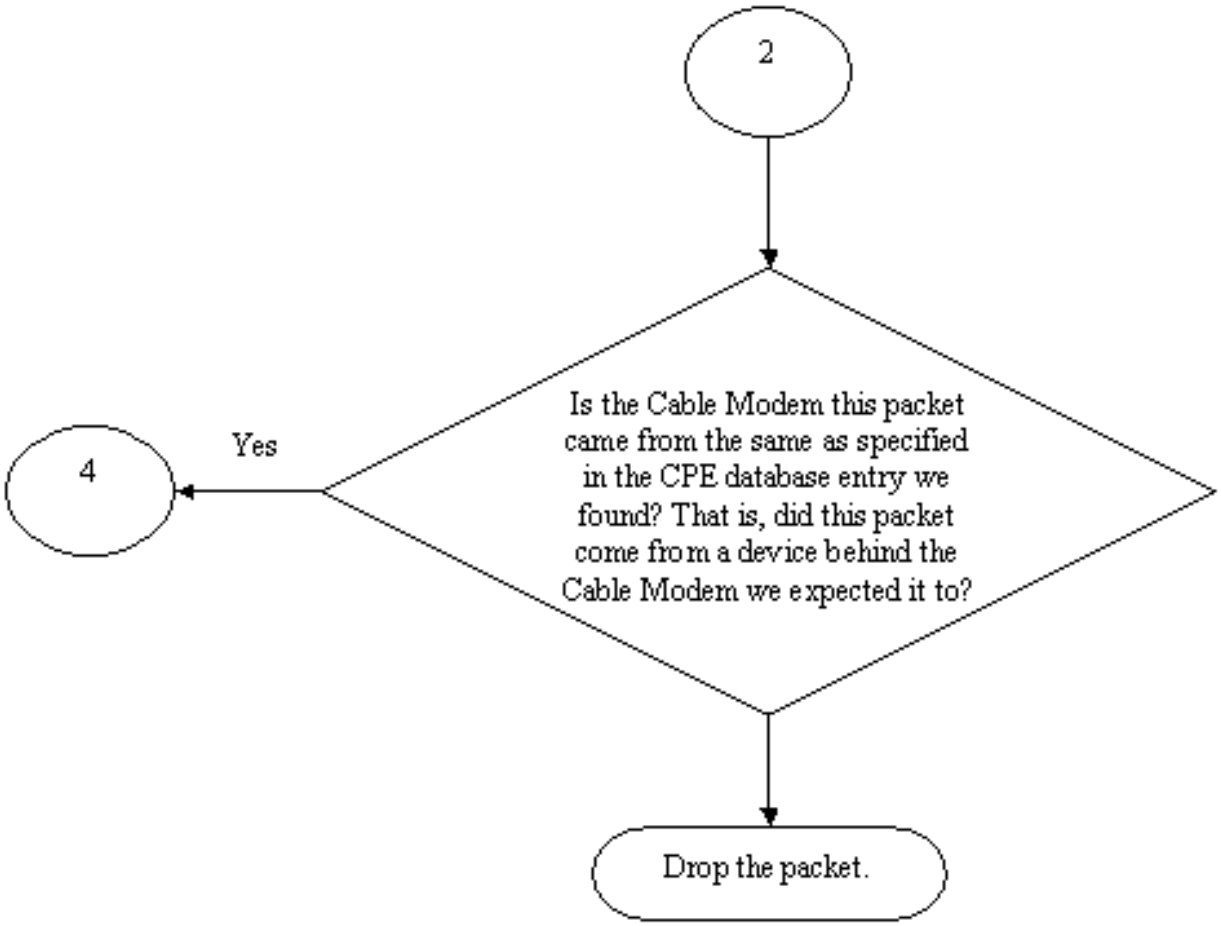
O primeiro cenário de Rejeição de Serviço que vamos abordar é a situação que envolve endereços IP duplicados. Suponhamos que o cliente A esteja conectado ao seu provedor de serviços e tenha obtido um aluguel de DHCP válido para seu PC. O cliente que do endereço IP de Um ou Mais Servidores Cisco ICM NT A obteve será sabido como o 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. A informação de base de dados de CPE com respeito ao endereço IP de Um ou Mais Servidores Cisco ICM NT X mudaria segundo que dispositivo CPE enviou por último uma requisição ARP em nome do 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.

Permitindo o cabo fonte-verifique, o CMTS poderia ver que o IP e os pacotes ARP para o endereço IP de Um ou Mais Servidores Cisco ICM NT X estavam sendo originado do Cable Modem errado e daqui, estes pacotes seria deixado cair, vê o fluxograma 2. Isto inclui todos os pacotes IP com endereço de origem X e requisições ARP em nome do X. Os logs CMTS mostrariam uma mensagem ao longo das linhas de:

%UBR7200-3-BADIPSOURCE: Relação Cable3/0, pacote IP do 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.

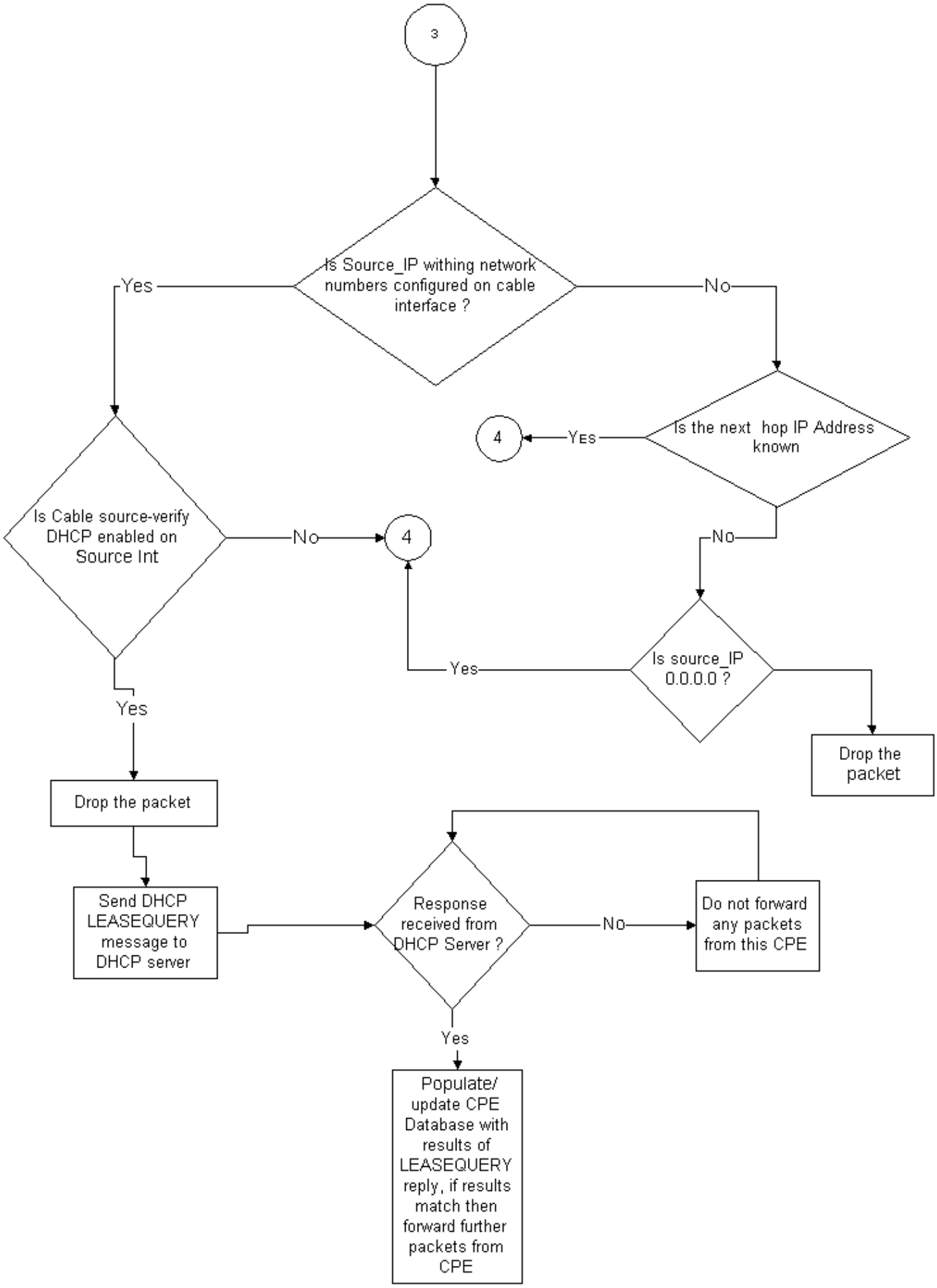
Exemplo 2 - Cenário com endereços IP duplicados - Uso de um endereço IP que ainda não foi usado

Uma outra encenação é para que um usuário atribua estaticamente até agora um endereço IP de Um ou Mais Servidores Cisco ICM NT não utilizado a seu PC que cai dentro da escala legítima 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 problema seguinte que pode elevarar é esse cliente que o C pôde conectar sua estação de trabalho à rede de provedor de serviços e adquire um aluguel de DHCP para o endereço IP de Um ou Mais Servidores Cisco ICM NT Y. O base de dados de CPE marcaria temporariamente o endereço IP de Um ou Mais Servidores Cisco ICM NT Y como pertencendo atrás do modem a cabo do cliente c. Contudo, não pôde ser muito antes do cliente B, o usuário NON-legítimo envia a sequência apropriada do tráfego ARP para convencer o salto seguinte que era o proprietário legítimo do endereço IP de Um ou Mais Servidores Cisco ICM NT Y, daqui causando uma interrupção ao serviço do cliente c.

Similarmente, o segundo problema pode ser resolvido girando sobre o **cabo fonte-verifica**. 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 uma outra transação de DHCP para esse endereço IP de Um ou Mais Servidores Cisco ICM NT ou a entrada de ARP no CMTS que cronometra para fora para esse endereço IP de Um ou Mais Servidores Cisco ICM NT pode deslocar a entrada. Isto assegura-se de que se um utilizador final adquire com sucesso um aluguel de DHCP para um endereço IP de Um ou Mais Servidores Cisco ICM NT dado, esse cliente não tenha que se preocupar sobre o CMTS que se torna confundido e que pensa que seu endereço IP de Um ou Mais Servidores Cisco ICM NT pertence a um outro usuário.

O primeiro problema de interrupção de usuários de usar até agora endereços IP de Um ou Mais Servidores Cisco ICM NT não utilizados pode ser resolvido com **cabo fonte-verifica o DHCP**. Adicionando o parâmetro DHCP ao fim deste comando, o CMTS pode verificar a validez de cada endereço IP de origem que novo se ouve aproximadamente emitindo um tipo especial de mensagem DHCP chamado um LEASEQUERY ao 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. Consulte a mensagem DHCPLEASEQUERY para obter mais detalhes.

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.

Nota: Para que isto trabalhe corretamente, você igualmente precisa de configurar o **comando ip verify unicast reverse-path** para impedir endereços IP de origem falsificado. Refira comandos do cabo: cabografe s para mais informação.

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.

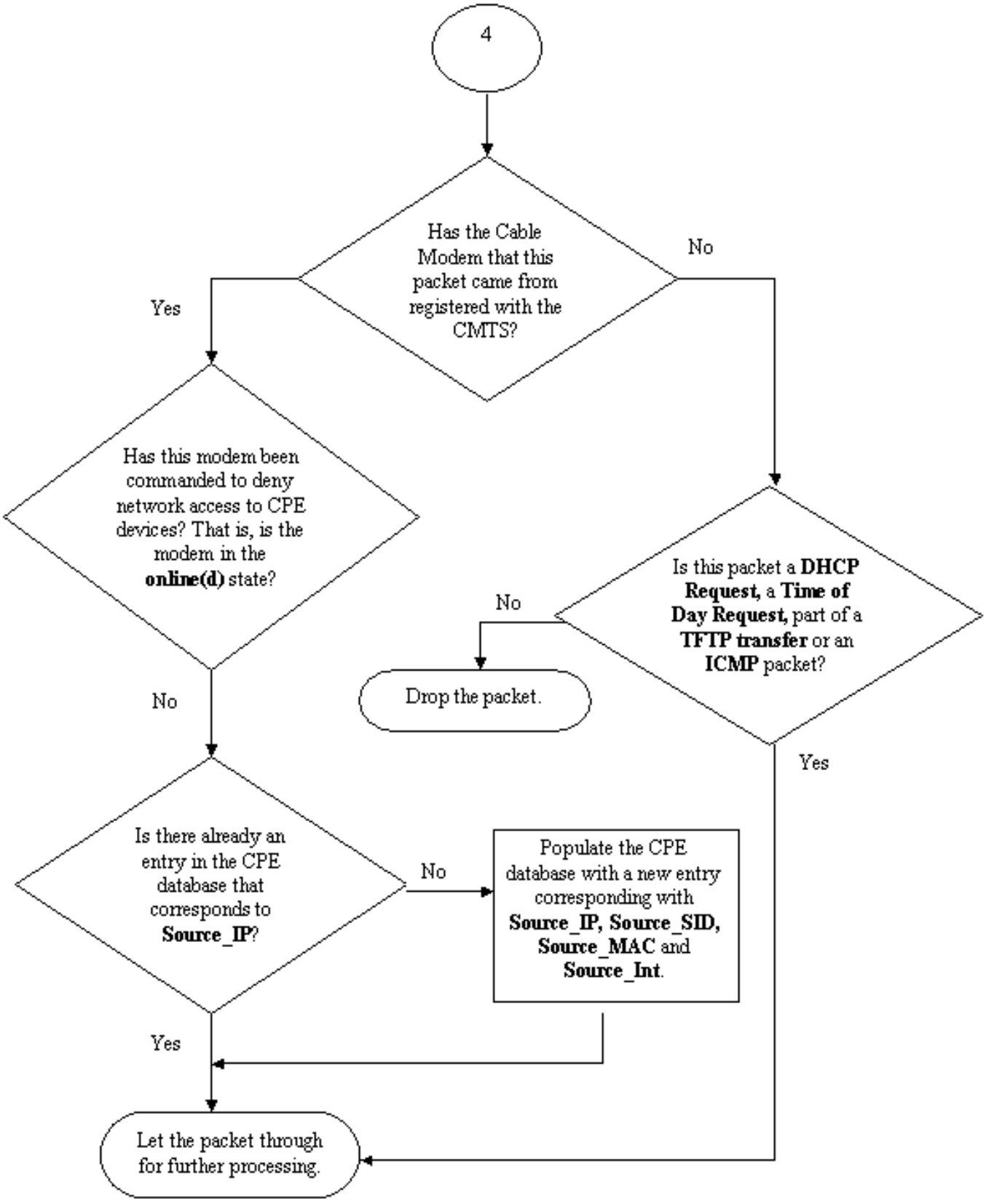
Agora, considere o seguinte exemplo:

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 endereço IP de origem 172.16.1.10 chegou no CMTS do modem a cabo 24.2.2.10, o CMTS veria que 24.2.2.10 não reside no base de dados de CPE, o **modem 0 do x/y do cabo int da mostra**, porém o **IP verifica que o caminho reverso do unicast** permite o Unicast Reverse Path Forwarding (unicast RPF), que verifica cada pacote recebido em uma relação a fim verificar que o endereço IP de origem do pacote aparece nas tabelas de roteamento que pertence a essa relação. **O cabo fonte-verifica** verificações para ver o que o salto seguinte para 24.2.2.10 é. 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

Configurando o **cabo fonte-verifique** envolve simplesmente adicionar o **comando cable source-verify à** interface de cabo que você gostaria de ativar sobre a função. Se você está usando o Agrupamento de cabos de interface, a seguir você precisa de adicionar o **cabo fonte-verifica à**

configuração da relação mestra.

Como configurar o `cabo fonte-verifique o DHCP`

Nota: o cabo fonte-verifica foi introduzido no Cisco IOS Software Release 12.0(7)T e é apoiado primeiramente nos Cisco IOS Software Release 12.0SC, 12.1EC e 12.1T.

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.

A fim utilizar o **cabo fonte-para verificar a** funcionalidade **DHCP**, seu servidor DHCP deve responder às mensagens como especificadas por draft-ietf-dhcp-leasequery-XX.txt. As versões de registro de rede Cisco 3.5 e podem acima responder a esta mensagem.

Certifique-se de que seu servidor DHCP apoia o processamento da opção de informação de agente de relay. Veja por favor estas instruções.

Um outro recurso que deve ser suportado pelo servidor DHCP é o processamento da opção de informações de transmissão de DHCP. Isto é sabido de outra maneira como a opção 82 que processa. 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 - Changeme P - Salvaguarda de 127.0.0.1 do C

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. Alternativamente, se você está na alerta do nrcmd, >nrcmd você apenas datilografa o seguinte:

o DHCP permite o salvaguarda-relé-agente-DATA

save

reload DHCP

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

Agente de transmissão

O CMTS deve etiquetar requisições DHCP do Modems a cabo e o CPE com a opção de informação de agente de relay para que o **cabo fonte-verifica o DHCP** para ser eficaz. Os comandos seguintes devem ser inscritos no modo de configuração global em Cisco IOS Software Release 12.1EC running CMTS, em 12.1T ou em umas versões mais atrasadas 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.

Seja cuidadoso usar os comandos apropriados, segundo a versão do Cisco IOS que você está executando. Certifique-se atualizar sua configuração se você muda 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.

Assim, por exemplo, se um PC com MAC address 99:88:77:66:55:44 que é atrás do modem a cabo aa: bb: centímetro cúbico: dd: EE: o ff envia uma requisição DHCP, o CMTS enviará a requisição DHCP que ajusta a subopção da identificação remota de Agente da opção 82 ao MAC address do modem a cabo, aa: bb: centímetro cúbico: dd: EE: 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 está usando o Agrupamento de cabos de interface então você deve incorporar o comando sob o pacote mestre conecta.

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 seu formulário mais simples como descrito neste documento, um dispositivo CPE não configurado através do DHCP não pode obter o acesso de rede. Esta é a melhor maneira de fixar o espaço de endereços IP e aumentar a estabilidade e a confiança de uns dados sobre o serviço de cabo. Contudo os operadores de serviço múltiplo (MSO) que têm os serviços comerciais que os exigiram usar endereços estáticos quiseram executar a Segurança restrita do commandcable fonte-**verificam o DHCP**.

A versão de registro de rede Cisco 5.5 tem uma capacidade nova de resposta à pergunta do aluguer para endereços “reservados”, mesmo que o endereço IP de Um ou Mais Servidores Cisco

ICM NT não seja obtido através do DHCP. O servidor DHCP inclui dados da reserva do aluguer 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 transmissão do uBR de Cisco, por exemplo, rejeitam as datagramas DHCPLEASEQUERY que não têm um MAC address e o Lease Time (opção do 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 alugado realmente, o registro de rede retorna seu Lease Time restante. Mais características podem ser encontradas na seção de pergunta dos alugueres de configurar escopos de DHCP e alugueres.

Informações Relacionadas

- Opção de informação da transmissão de DHCP (RFC 3046)
- Suporte Técnico e Documentação - Cisco Systems