Verifica dell'origine dei cavi e sicurezza degli indirizzi IP

Sommario

Introduzione

Cisco ha implementato alcuni miglioramenti nei prodotti Cisco Cable Modem Termination System (CMTS) che impediscono determinati tipi di attacchi Denial of Service basati sullo spoofing di indirizzi IP e sul furto di indirizzi IP nei sistemi cablati DOCSIS (Data-Over-Cable Service Interface Specifications). La guida di riferimento ai comandi dei cavi Cisco CMTS descrive la suite di comandi per la **verifica dell'origine dei cavi** che fanno parte di questi miglioramenti alla sicurezza dell'indirizzo IP.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Ambiente DOCSIS non protetto

Un dominio MAC (Media Access Control) DOCSIS è simile per natura a un segmento Ethernet. Se non vengono protetti, gli utenti del segmento sono vulnerabili a molti tipi di attacchi di tipo Denial of Service basati su indirizzamento di layer 2 e layer 3. Inoltre, gli utenti possono soffrire di un livello di servizio degradato a causa della configurazione errata dell'indirizzamento sulle apparecchiature di altri utenti. Alcuni esempi:

- Configurazione di indirizzi IP duplicati in nodi diversi.
- Configurazione di indirizzi MAC duplicati su nodi diversi.
- Utilizzo non autorizzato di indirizzi IP statici anziché di indirizzi IP assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol).
- L'uso non autorizzato di diversi numeri di rete all'interno di un segmento.
- Configurazione non corretta dei nodi finali per rispondere alle richieste ARP per conto di una parte della subnet IP del segmento.

Anche se questi tipi di problemi sono facili da controllare e mitigare in un ambiente LAN Ethernet monitorando fisicamente e disconnettendo le apparecchiature in conflitto, tali problemi nelle reti DOCSIS possono essere più difficili da isolare, risolvere e prevenire a causa delle dimensioni potenzialmente elevate della rete. Inoltre, gli utenti finali che controllano e configurano CPE (Customer Premise Equipment) potrebbero non disporre dei vantaggi di un team di supporto IS locale per assicurarsi che le workstation e i PC non siano stati configurati in modo errato o intenzionale.

Database CPE CMTS

La suite di prodotti CMTS di Cisco gestisce un database interno popolato dinamicamente di indirizzi IP e MAC CPE connessi. Il database CPE contiene inoltre dettagli sui modem cablati corrispondenti a cui appartengono questi dispositivi CPE.

Èpossibile visualizzare una vista parziale del database CPE corrispondente a un particolare modem via cavo eseguendo il comando CMTS nascosto **show interface cable X/Y modem Z**. In questo caso, X è il numero della scheda di linea, Y è il numero della porta downstream e Z è l'identificativo di servizio (SID) del modem via cavo. Z può essere impostato su 0 per visualizzare i dettagli relativi a tutti i modem via cavo e CPE su una particolare interfaccia a valle. Vedere l'esempio seguente di un output tipico generato da questo 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: poiché questo comando è nascosto, è soggetto a modifiche e non può essere reso disponibile in tutte le versioni del software Cisco IOS®.

Nell'esempio di cui sopra, la colonna relativa al metodo dell'host con indirizzo IP 192.168.1.90 è elencata come dhcp. Ciò significa che il CMTS è venuto a conoscenza di questo host monitorando le transazioni DHCP tra l'host e il server DHCP del provider di servizi.

L'host con indirizzo IP 192.168.1.77 è elencato con il metodo static. Ciò significa che il CMTS non

è stato informato dell'host tramite una transazione DHCP tra il dispositivo e un server DHCP. Al contrario, il CMTS ha rilevato per la prima volta altri tipi di traffico IP da questo host. Questo traffico poteva essere il Web browsing, l'e-mail o i pacchetti "ping".

Anche se può sembrare che la versione 192.168.1.77 sia stata configurata con un indirizzo IP statico, è possibile che l'host abbia effettivamente acquisito un lease DHCP, ma il CMTS potrebbe essere stato riavviato a partire dall'evento e quindi non ricorda la transazione.

Il database CPE viene in genere popolato dai dati CMTS ricavati dalle transazioni DHCP tra i dispositivi CPE e il server DHCP del provider di servizi. Inoltre, il CMTS può ascoltare altro traffico IP proveniente dai dispositivi CPE per determinare gli indirizzi IP e MAC CPE appartenenti ai modem via cavo.

Il Comando Cable Source-Verify

Cisco ha implementato il comando cable interface source-verify [dhcp]. Con questo comando il CMTS utilizza il database CPE per verificare la validità dei pacchetti IP che il CMTS riceve sulle proprie interfacce cablate e può prendere decisioni intelligenti per inoltrarli o meno.

Il diagramma seguente mostra l'ulteriore elaborazione attraverso cui deve passare un pacchetto IP ricevuto su un'interfaccia via cavo prima di poter procedere attraverso il CMTS.

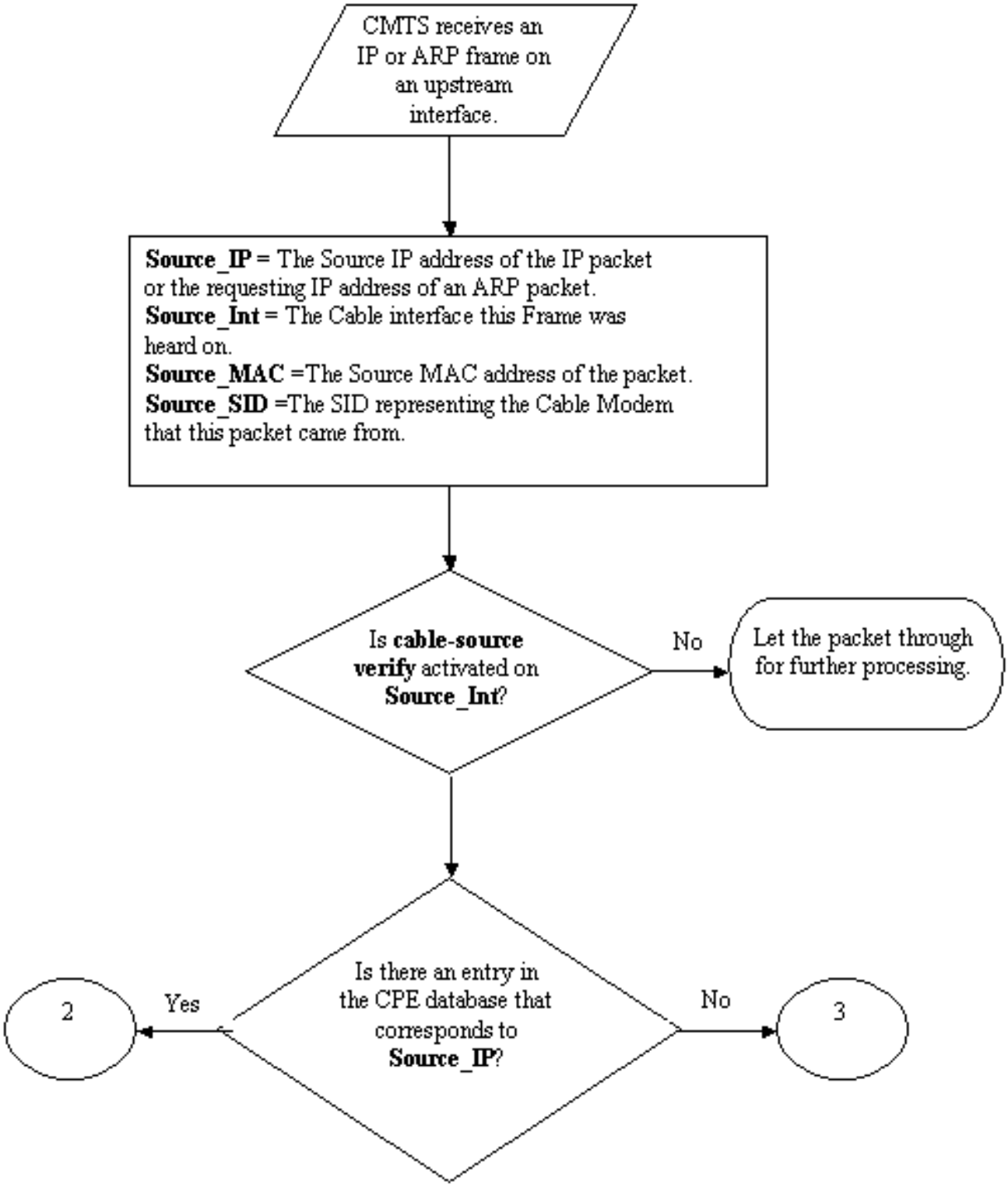

Diagramma di flusso 1

Il diagramma di flusso inizia con un pacchetto ricevuto da una porta a monte sul CMTS e termina con il pacchetto autorizzato a continuare l'elaborazione o nel pacchetto scartato.

Esempio 1 - Scenario con indirizzi IP duplicati

Il primo scenario di negazione del servizio che verrà affrontato è la situazione relativa agli indirizzi IP duplicati. Si supponga che il cliente A sia connesso al proprio provider di servizi e abbia ottenuto un lease DHCP valido per il PC. L'indirizzo IP ottenuto dal Cliente A sarà noto come X.

Qualche tempo dopo che A ha acquisito il lease DHCP, il cliente B decide di configurare il suo PC con un indirizzo IP statico che risulta essere lo stesso attualmente utilizzato dalle apparecchiature del cliente A. Le informazioni del database CPE relative all'indirizzo IP X cambiano a seconda del dispositivo CPE che ha inviato per ultimo una richiesta ARP per conto di X.

In una rete DOCSIS non protetta, il Cliente B potrebbe essere in grado di convincere il router dell'hop successivo (nella maggior parte dei casi, il CMTS) di avere il diritto di utilizzare l'indirizzo IP X inviando semplicemente una richiesta ARP per conto di X al CMTS o al router dell'hop successivo. In questo modo il traffico proveniente dal provider di servizi non verrà inoltrato al Cliente A.

Abilitando la verifica dell'origine dei cavi, il CMTS potrebbe verificare che i pacchetti IP e ARP per l'indirizzo IP X provengano dal modem via cavo errato e quindi, questi pacchetti verrebbero scartati, vedere il diagramma di flusso 2. Ciò include tutti i pacchetti IP con indirizzo di origine X e richieste ARP per conto di X. I registri CMTS visualizzerebbero un messaggio simile al seguente:

%UBR7200-3-BADIPSOURCE: Cavo interfaccia 3/0, pacchetto IP da origine non valida. IP=192.168.1.10, MAC=0001.422c.54d0, SID previsto=10, SID effettivo=11

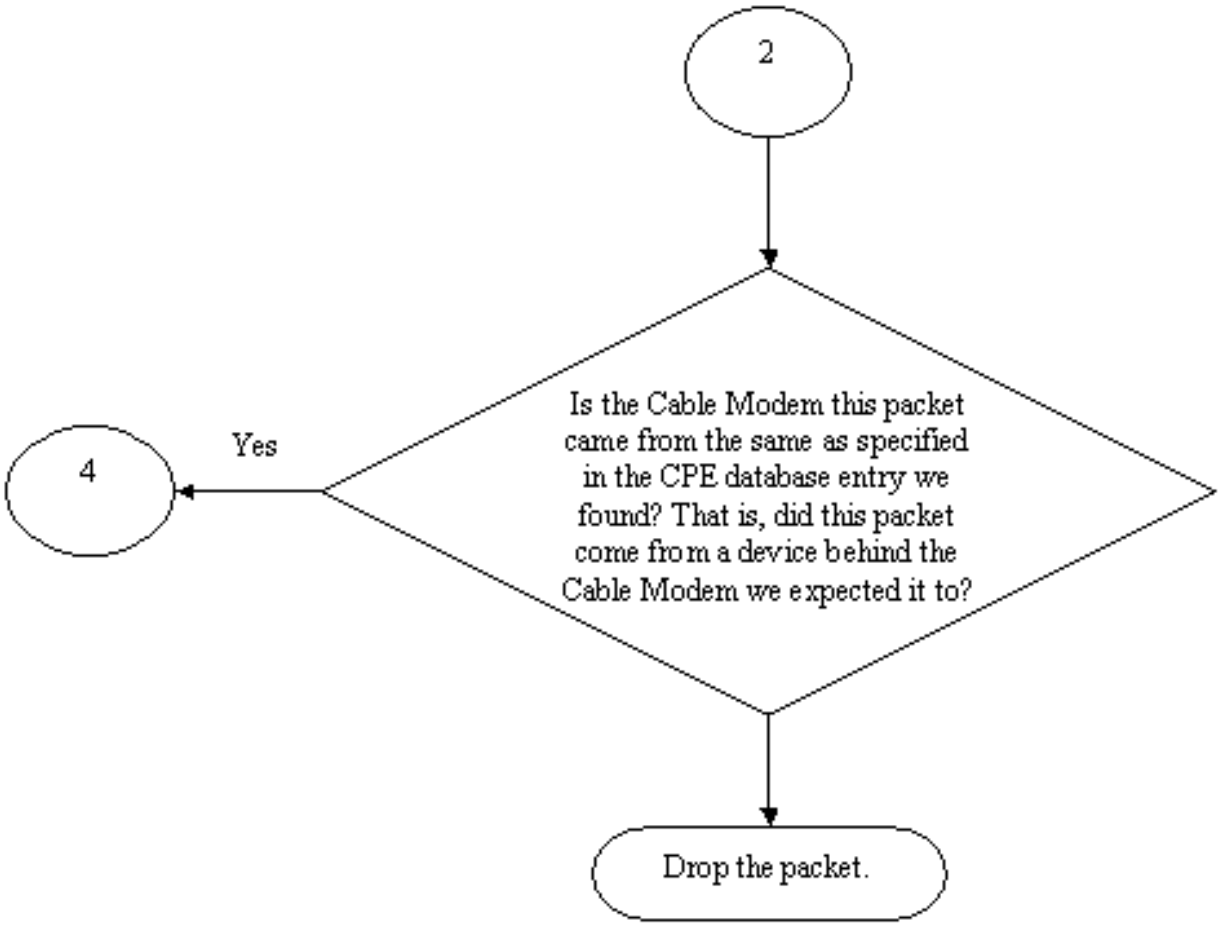

Diagramma di flusso 2

Utilizzando queste informazioni, vengono identificati entrambi i client e il modem via cavo con l'indirizzo IP duplicato collegato può essere disabilitato.

Esempio 2 - Scenario con indirizzi IP duplicati - Utilizzo di un indirizzo IP non ancora utilizzato

Un altro scenario prevede l'assegnazione statica di un indirizzo IP non ancora utilizzato al PC che rientra nell'intervallo legittimo di indirizzi CPE. Questo scenario non causa interruzioni dei servizi per nessuno nella rete. Supponiamo che il cliente B abbia assegnato l'indirizzo Y al proprio PC.

Il problema successivo che potrebbe verificarsi è che il cliente C potrebbe connettere la propria workstation alla rete del provider di servizi e acquisire un lease DHCP per l'indirizzo IP Y. Il database CPE contrassegnerebbe temporaneamente l'indirizzo IP Y come appartenente dietro il modem via cavo del cliente C. Tuttavia, potrebbe non trascorrere molto tempo prima che il Cliente B invii la sequenza appropriata di traffico ARP per convincere l'hop successivo di essere il legittimo proprietario dell'indirizzo IP Y, causando così un'interruzione al servizio del Cliente C.

Analogamente, il secondo problema può essere risolto attivando la **verifica della sorgente del cavo**. Quando la verifica dell'origine dei cavi è attivata, una voce del database CPE generata acquisendo i dettagli da una transazione DHCP non può essere sostituita da altri tipi di traffico IP.

Solo un'altra transazione DHCP per tale indirizzo IP o la voce ARP nel CMTS relativo al timeout per tale indirizzo IP può spostare la voce. In questo modo, se un utente finale acquisisce un lease DHCP per un determinato indirizzo IP, non dovrà più temere che il CMTS possa diventare confuso e pensare che il proprio indirizzo IP appartenga a un altro utente.

Per risolvere il primo problema, ovvero impedire agli utenti di utilizzare indirizzi IP non ancora utilizzati, è possibile usare il **cavo dhcp di verifica dell'origine**. Aggiungendo il parametro dhcp alla fine di questo comando, il CMTS può verificare la validità di ogni nuovo indirizzo IP di origine di cui viene a conoscenza inviando un tipo speciale di messaggio DHCP chiamato LEASEQUERY al server DHCP. Vedere il diagramma di flusso 3.

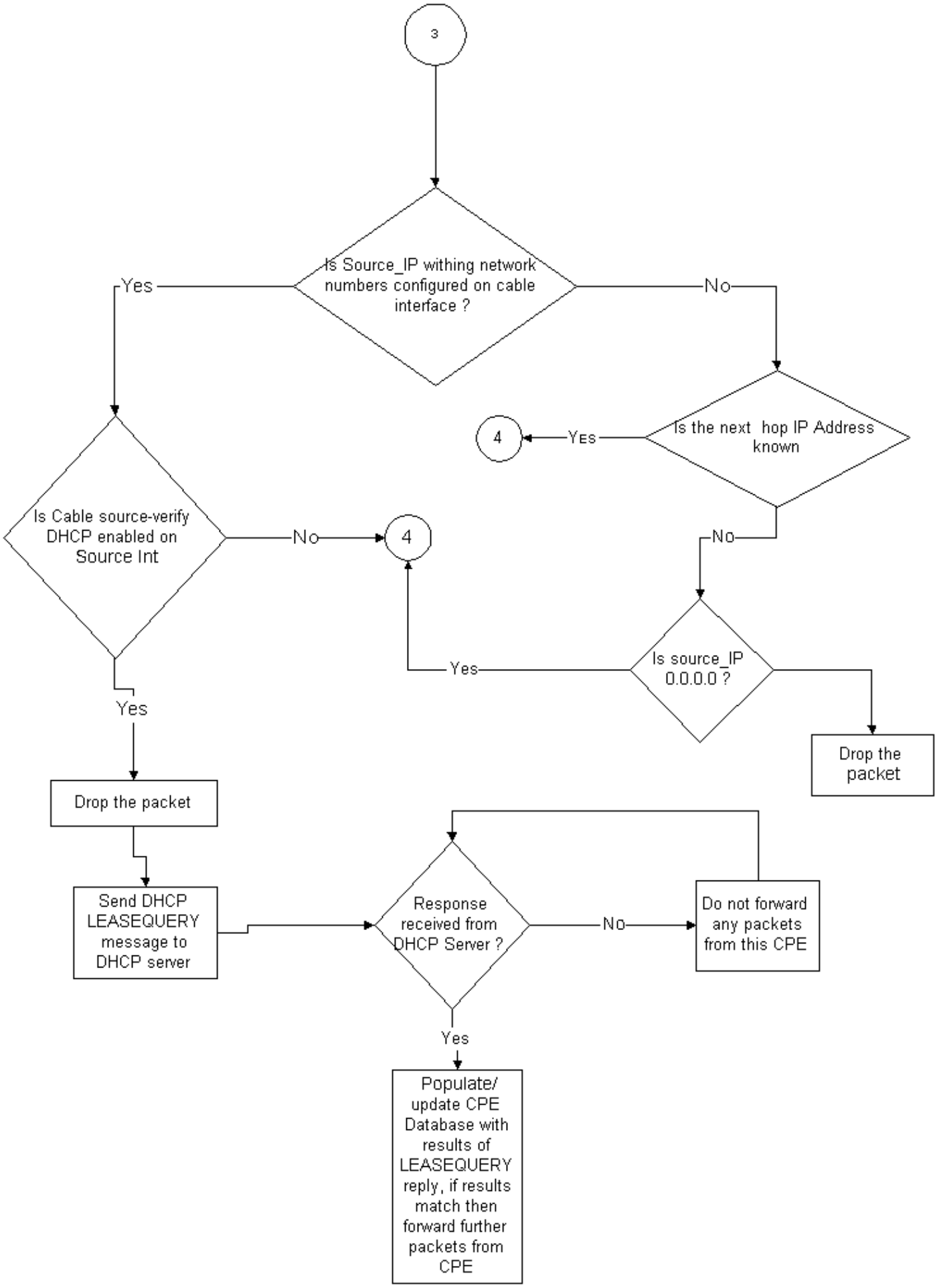

Diagramma di flusso 3

Per un determinato indirizzo IP CPE, il messaggio LEASEQUERY chiede quali sono l'indirizzo MAC e il modem via cavo corrispondenti.

In questo caso, se il Cliente B connette la propria workstation alla rete via cavo con l'indirizzo statico Y, il CMTS invierà una LEASEQUERY al server DHCP per verificare se l'indirizzo Y è stato assegnato in leasing al PC del Cliente B. Il server DHCP è in grado di informare il CMTS che non è stato concesso alcun lease per l'indirizzo IP Y e di conseguenza al cliente B verrà negato l'accesso.

Esempio 3 - Uso di un numero di rete non fornito dal provider di servizi

Gli utenti possono avere delle workstation configurate dietro i loro modem via cavo con indirizzi IP statici che non possono essere in conflitto con nessuno dei numeri di rete correnti del provider di servizi, ma che potrebbero causare problemi in futuro. Pertanto, utilizzando la funzione di verifica dell'origine dei cavi, un CMTS è in grado di filtrare i pacchetti provenienti da indirizzi IP di origine non compresi nell'intervallo configurato sull'interfaccia dei cavi del CMTS.

Nota: per il corretto funzionamento di questo comando, è necessario configurare anche il comando **ip verify unicast reverse-path** in modo da impedire lo spoofing degli indirizzi di origine IP. Per ulteriori informazioni, fare riferimento al documento Comandi per i cavi: per ulteriori informazioni.

Alcuni clienti possono avere un router come dispositivo CPE e fare in modo che il provider di servizi instradi il traffico a questo router. Se il CMTS riceve il traffico IP dal router CPE con l'indirizzo IP di origine Z, la verifica dell'origine dei cavi consentirà il passaggio del pacchetto se il CMTS dispone di un percorso alla rete a cui Z appartiene tramite il dispositivo CPE. Fare riferimento al diagramma di flusso 3.

Si consideri ora il seguente esempio:

Sul CMTS è disponibile la seguente configurazione:

```
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
```

Supponendo che un pacchetto con indirizzo IP di origine 172.16.1.10 sia arrivato al CMTS dal modem via cavo 24.2.2.10, il CMTS rileva che 24.2.2.10 non risiede nel database CPE, **show int cable x/y modem 0**, tuttavia **ip verify unicast reverse path** abilita Unicast Reverse Path Forwarding (Unicast RPF), che controlla ogni pacchetto ricevuto su un'interfaccia per verificare che l'indirizzo IP di origine del pacchetto appaia nelle tabelle di routing a esso appartenenti . La funzione **cable source-verify** controlla l'hop successivo per la versione 24.2.2.10. Nella configurazione sopra riportata, il **router ip è 24.2.2.0 255.255.255.0 24.1.1.2,** quindi l'hop successivo è 24.1.1.2. Supponendo ora che il valore 24.1.1.2 sia una voce valida nel database CPE, il CMTS conclude che il pacchetto è corretto e quindi lo elaborerà come mostrato nel diagramma di flusso 4.

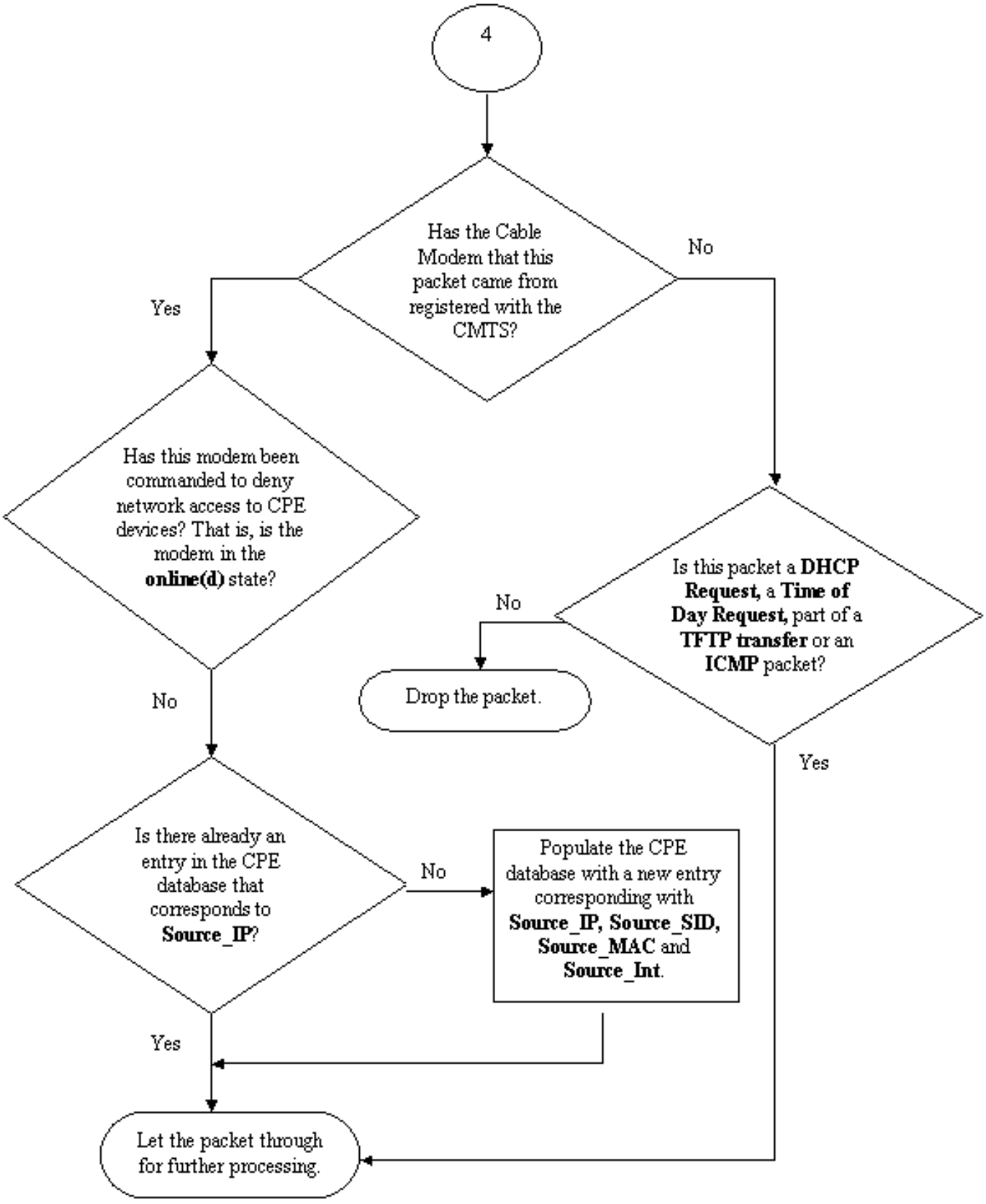

Diagramma di flusso 4

Configurazione della verifica dell'origine del cavo

La configurazione di **cable source-verify** implica semplicemente l'aggiunta del comando **cable source-verify** all'interfaccia del cavo su cui si desidera attivare la funzione. Se si utilizza il bundling dell'interfaccia del cavo, è necessario aggiungere la **verifica dell'origine del cavo** alla

configurazione dell'interfaccia primaria.

Come configurare il `dhcp per la verifica dell'origine del cavo`

Nota: la verifica dell'origine dei cavi è stata introdotta per la prima volta nel software Cisco IOS versione 12.0(7)T ed è supportata nel software Cisco IOS versione 12.0SC, 12.1EC e 12.1T.

La configurazione del protocollo **dhcp per la verifica dell'origine del cavo** richiede alcuni passaggi.

Verificare che il server DHCP supporti il messaggio speciale DHCP LEASEQUERY.

Per utilizzare la funzionalità **dhcp di verifica dell'origine** del cavo, il server DHCP deve rispondere ai messaggi come specificato in draft-ietf-dhcp-leasequery-XX.txt. Cisco Network Registrar versione 3.5 e successive è in grado di rispondere a questo messaggio.

Verificare che il server DHCP supporti l'elaborazione dell'opzione Informazioni agente di inoltro. Vedere la sezione Agente di inoltro.

Un'altra funzionalità che deve essere supportata dal server DHCP è l'elaborazione delle opzioni di inoltro delle informazioni DHCP. Questa operazione è nota anche come elaborazione dell'opzione 82. Questa opzione è descritta in DHCP Relay Information Option (RFC 3046). Cisco Network Registrar versione 3.5 e successive supportano l'elaborazione dell'opzione Informazioni agente di inoltro, ma deve essere attivata tramite l'utilità della riga di comando di Cisco Network Registrar nrcmd con la seguente sequenza di comandi:

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp abilita salvataggio-relay-agent-data

nrcmd -U admin -P changeme -C 127.0.0.1 save

nrcmd -U admin -P changeme -C 127.0.0.1 ricaricamento dhcp

In alcuni casi può essere necessario sostituire il nome utente, la password e l'indirizzo IP del server appropriati. I valori riportati sopra sono predefiniti. In alternativa, se è visualizzato il prompt nrcmd, >nrcmd è sufficiente digitare quanto segue:

dhcp: abilitazione salvataggio-relay-agent-data

salvare

reload dhcp

Attiva l'elaborazione delle informazioni di inoltro DHCP nel CMTS.

Agente di inoltro

Affinché il protocollo **dhcp per la verifica dell'origine** dei **cavi** sia efficace, il CMTS deve contrassegnare le richieste DHCP provenienti da modem via cavo e CPE con l'opzione **Relay Agent** Information. I comandi seguenti devono essere immessi in modalità di configurazione globale su un CMTS con software Cisco IOS versione 12.1EC, 12.1T o successive.

opzione ip dhcp relay information

Se il CMTS utilizza il software Cisco IOS versione 12.0SC, addestrare Cisco IOS, quindi usare il comando **cable relay-agent-option** cable interface.

Fare attenzione a usare i comandi appropriati, a seconda della versione di Cisco IOS in esecuzione. Se si cambia treno in Cisco IOS, verificare di aggiornare la configurazione.

I comandi **relay information option** aggiungono un'opzione speciale chiamata Option 82, o relay information option, al pacchetto DHCP inoltrato quando il CMTS inoltra i pacchetti DHCP.

L'opzione 82 è compilata con un'opzione secondaria, Agent Circuit-ID, che fa riferimento all'interfaccia fisica sul CMTS su cui è stata ascoltata la richiesta DHCP. Inoltre, un'altra opzione secondaria, l'ID remoto agente, viene popolata con l'indirizzo MAC di 6 byte del modem via cavo da cui è stata ricevuta o passata la richiesta DHCP.

Ad esempio, se un PC con indirizzo MAC 99:88:77:66:55:44 e si trova dietro un modem via cavo a:bb:cc:dd:ee:ff invia una richiesta DHCP, il CMTS inoltrerà la richiesta DHCP impostando l'opzione secondaria ID remoto agente dell'opzione 82 all'indirizzo MAC del modem via cavo a:bb:cc:dd:ee:ff.

Includendo l'opzione Relay Information nella richiesta DHCP da un dispositivo CPE, il server DHCP è in grado di archiviare le informazioni sul CPE appartenente ai modem via cavo. Questa funzione è particolarmente utile quando sul CMTS è configurato il **dhcp per la verifica dell'origine dei cavi**, in quanto il server DHCP è in grado di informare in modo affidabile il CMTS non solo sull'indirizzo MAC di un determinato client, ma anche su quale modem via cavo deve essere connesso un determinato client.

Abilitare il comando cable source-verify dhcp nell'interfaccia del cavo appropriata.

Il passaggio finale consiste nell'immettere il comando **cable source-verify dhcp** nell'interfaccia del cavo su cui si desidera attivare la funzione. Se il CMTS utilizza il fascio di interfacce di cavi, è necessario immettere il comando nell'interfaccia principale del fascio.

Conclusioni

Le suite di comandi **cable source-verify** consentono a un provider di servizi di proteggere la rete via cavo dagli utenti con indirizzi IP non autorizzati a utilizzare la rete.

Il comando cable source-verify da solo è un modo efficace e facile per implementare la sicurezza dell'indirizzo IP. Pur non contemplando tutti gli scenari, garantisce almeno che i clienti con il diritto di utilizzare gli indirizzi IP assegnati non subiscano interruzioni se l'indirizzo IP viene utilizzato da un altro utente.

Nel modo più semplice, descritto in questo documento, un dispositivo CPE non configurato tramite DHCP non può ottenere l'accesso alla rete. Questo è il modo migliore per proteggere lo spazio degli indirizzi IP e aumentare la stabilità e l'affidabilità di un servizio Data over Cable. Tuttavia, più operatori di servizi (MSO) che dispongono di servizi commerciali che richiedono l'utilizzo di indirizzi statici desideravano implementare una rigida sicurezza del **cavo di connessione dhcp-verify**.

Cisco Network Registrar versione 5.5 offre una nuova funzionalità per rispondere alle richieste di lease per gli indirizzi "riservati", anche se l'indirizzo IP non è stato ottenuto tramite DHCP. Il server DHCP include i dati relativi alla prenotazione del lease nelle risposte DHCPLEASEQUERY.

Nelle versioni precedenti di Network Registrar, le risposte DHCPLEASEQUERY erano possibili solo per i client in lease o precedentemente in lease per i quali era stato memorizzato l'indirizzo MAC. Gli agenti di inoltro uBR Cisco, ad esempio, eliminano i datagrammi DHCPLEASEQUERY senza indirizzo MAC e durata del lease (opzione dhcp-lease-time).

Network Registrar restituisce un tempo di lease predefinito di un anno (31536000 secondi) per i lease riservati in una risposta DHCPLEASEQUERY. Se l'indirizzo viene effettivamente assegnato in lease, Network Registrar restituirà la durata residua del lease.

Informazioni correlate

- Opzione informazioni inoltro DHCP (RFC 3046)
- Documentazione e supporto tecnico – Cisco Systems