Risoluzione dei problemi relativi al protocollo di configurazione host dinamico in reti switch Catalyst o aziendali

Sommario

Introduzione

In questo documento viene descritto come risolvere diversi problemi comuni relativi al protocollo DHCP (Dynamic Host Configuration Protocol) in una rete di switch Cisco Catalyst.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

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

> **Nota:** Solo i client Cisco registrati possono accedere ai report dei bug interni.

Premesse

DHCP fornisce un meccanismo tramite il quale i computer che utilizzano il protocollo TCP/IP (Transmission Control Protocol/Internet Protocol) possono ottenere automaticamente i parametri di configurazione del protocollo attraverso la rete. DHCP è uno standard aperto sviluppato dal Dynamic Host Configuration-Working Group (DHC-WG) dell'Internet Engineering Task Force (IETF).

DHCP si basa su un paradigma client-server, in cui il client DHCP, ad esempio un computer desktop, contatta un server DHCP per i parametri di configurazione. Il server DHCP si trova in genere in una posizione centrale e viene gestito dall'amministratore di rete. Poiché il server viene eseguito da un amministratore di rete, i client DHCP possono essere configurati in modo affidabile e dinamico con parametri appropriati all'architettura di rete corrente.

La maggior parte delle reti aziendali è costituita da più subnet suddivise in sottoreti denominate VLAN (Virtual LANS), in cui i router eseguono il routing tra le sottoreti. Poiché i router non superano i broadcast per impostazione predefinita, è necessario un server DHCP su ciascuna subnet, a meno che i router non siano configurati per inoltrare il broadcast DHCP con la funzionalità DHCP Relay Agent.

Concetti fondamentali

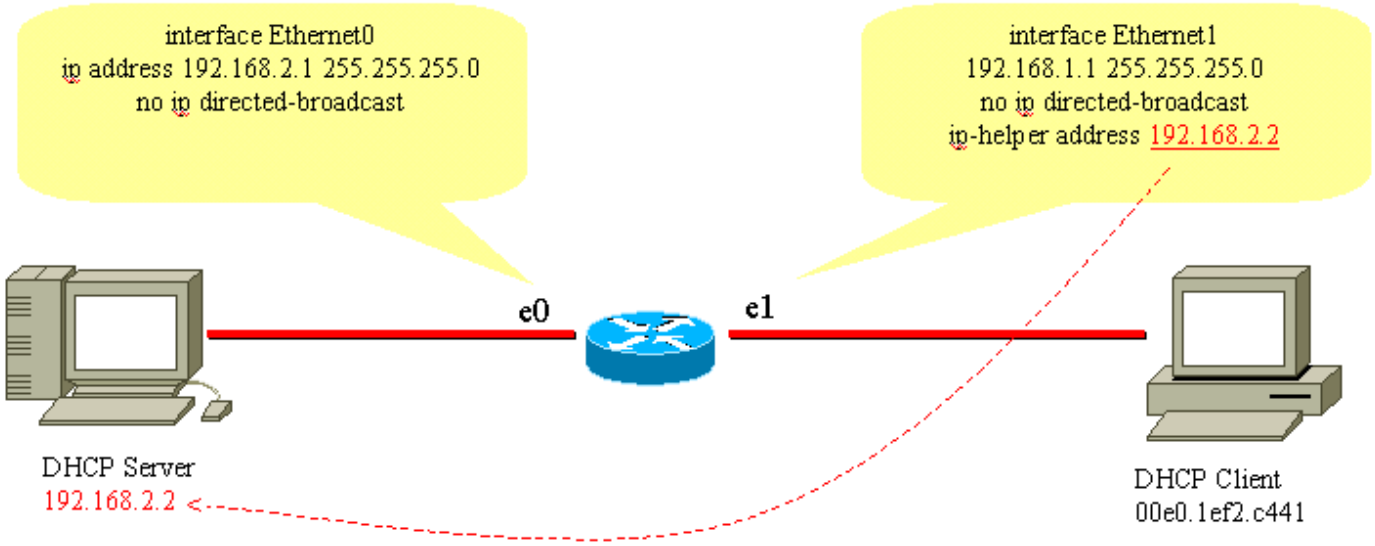
Di seguito vengono riportati alcuni concetti chiave di DHCP:

- I client DHCP inizialmente non dispongono di un indirizzo IP configurato e devono quindi inviare una richiesta di trasmissione per ottenere un indirizzo IP da un server DHCP.
- Per impostazione predefinita, i router non inoltrano le trasmissioni. Se il server DHCP si trova su un altro dominio di trasmissione (rete di livello 3 (L3)), è necessario soddisfare le richieste di trasmissione DHCP del client. Questa operazione viene eseguita tramite un agente di inoltro DHCP.
- L'implementazione del router DHCP dell'inoltro DHCP viene fornita tramite comandi di **helper IP a** livello di interfaccia

Scenari di esempio

Scenario 1: Routing del router Cisco tra le reti client e server DHCP

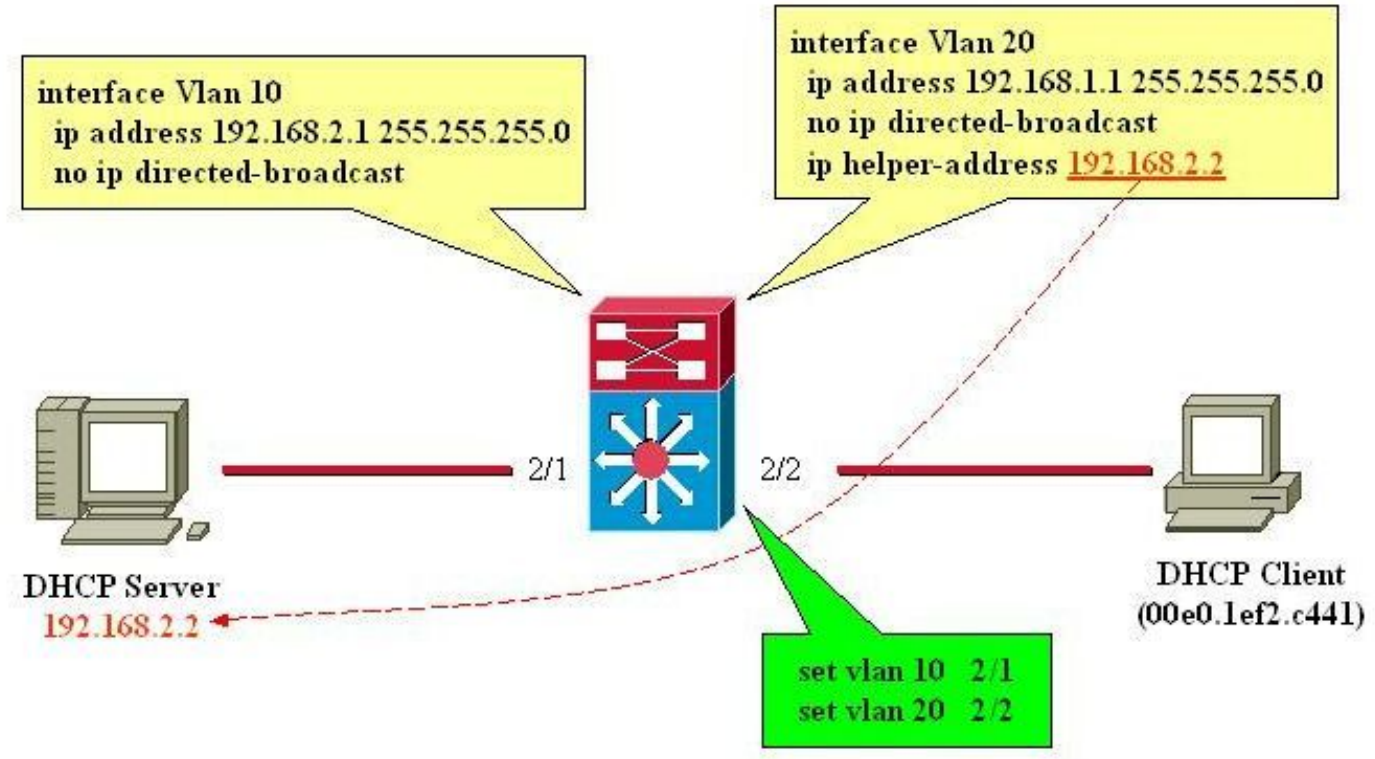
Come configurato in questo diagramma, l'interfaccia Ethernet1 inoltra il client broadcast DHCP DISCOVER a 192.168.2.2 tramite l'interfaccia Ethernet1. Il server DHCP soddisfa la richiesta tramite unicast. Nell'esempio, non è necessaria alcuna ulteriore configurazione del router.



Routing tra reti client e server DHCP

Scenario 2: Cisco Catalyst Switch con routing del modulo L3 tra reti client e server DHCP

Come configurato nel diagramma, l'interfaccia VLAN20 inoltra il client DHCPDISCOVER a 192.168.2.2 tramite l'interfaccia VLAN10. Il server DHCP soddisfa la richiesta tramite unicast. Nell'esempio, non è necessaria alcuna ulteriore configurazione del router. Le porte dello switch devono essere configurate come porte host con portfast abilitata dal protocollo Spanning-Tree Protocol (STP) e trunking e channeling disabilitati.



Route del modulo L3 tra reti client e server DHCP

Informazioni su DHCP

Il protocollo DHCP è stato definito inizialmente nelle RFC (Request for Comments) 1531 e da allora è diventato obsoleto nella RFC 2131. Il protocollo DHCP si basa sul protocollo Bootstrap

(BootP), definito nella RFC 951.

Il protocollo DHCP viene utilizzato dalle workstation (host) per ottenere le informazioni di configurazione iniziali, ad esempio l'indirizzo IP, la subnet mask e il gateway predefinito all'avvio. Con DHCP, non è necessario configurare manualmente ciascun host con un indirizzo IP. Inoltre, se un host viene spostato su una subnet IP diversa, deve utilizzare un indirizzo IP diverso da quello utilizzato in precedenza. DHCP si occupa di questa operazione automaticamente. Consente all'host di scegliere un indirizzo IP nella subnet IP corretta.

Riferimenti RFC DHCP correnti

- RFC 2131 - DHCP
- RFC 2132 - Opzioni DHCP ed estensioni del fornitore BootP
- RFC 1534 - Interoperabilità tra DHCP e BootP
- RFC 1542 - Chiarimenti ed estensioni per BootP
- RFC 2241 - Opzioni DHCP per Novell Directory Services
- RFC 2242 - Nome e informazioni del dominio Netware/IP
- RFC 2489 - Procedura per la definizione delle nuove opzioni DHCP

DHCP utilizza un modello client-server in cui uno o più server (server DHCP) allocano indirizzi IP e altri parametri di configurazione facoltativi ai client (host) all'avvio del client. Questi parametri di configurazione vengono concessi in lease dal server al client per un periodo di tempo specificato. All'avvio di un host, lo stack TCP/IP trasmette un messaggio broadcast (DHCPDISCOVER) per ottenere un indirizzo IP e una subnet mask, tra gli altri parametri di configurazione. In questo modo viene avviato uno scambio tra il server DHCP e l'host. Durante questo scambio, il client passa attraverso questi stati ben definiti:

1. Inizializzazione
2. Selezione
3. Richiesta
4. Associato
5. Rinnovo
6. Rebinding

Per spostarsi tra questi stati, il client e il server possono scambiarsi i tipi di messaggi elencati nella tabella dei messaggi DHCP.

Tabella messaggi DHCP

Riferimento	Messaggio	Descrizione
0x01	DHCPDISCOVER	Il client cerca i server DHCP disponibili.
0x02	DHCPOFFER	Risposta del server al comando DHCPDISCOVER del client.
0x03	DHCPREQUEST	Il client trasmette al server, richiede parametri offerti da un server in particolare, definito nel pacchetto.
0x04	DHCPDECLINE	La comunicazione client-server indica che l'indirizzo di rete è già in uso.
0x05	DHCPACK	Comunicazione tra server e client con parametri di configurazione e indirizzo di r confermato.

0x06	DHCPNAK	La comunicazione server-client rifiuta la richiesta del parametro di configurazione
0x07	DHCPRELEASE	La comunicazione client-server, restituisce l'indirizzo di rete e annulla il lease rimanente.
0x08	DHCPINFORM	La comunicazione client-server richiede solo i parametri di configurazione locali c client ha già configurato esternamente come indirizzo.

DHCPDISCOVER

Quando un client viene avviato per la prima volta, si dice che si trovi nello stato Inizializzazione in corso e trasmette un messaggio DHCPDISCOVER sulla subnet fisica locale tramite la porta UDP (User Datagram Protocol) 67 (server BootP). Poiché il client non ha modo di conoscere la subnet a cui appartiene, DHCPDISCOVER è un broadcast di tutte le subnet (indirizzo IP di destinazione di 255.255.255.255), con un indirizzo IP di origine di 0.0.0.0. L'indirizzo IP di origine è 0.0.0.0 poiché il client non ha un indirizzo IP configurato. Se nella subnet locale è presente un server DHCP configurato e correttamente funzionante, il server DHCP ascolta la trasmissione e risponde con un messaggio DHCP. Se nella subnet locale non esiste un server DHCP, è necessario che nella subnet locale sia presente un agente di inoltro DHCP/BootP per inoltrare il messaggio DHCPDISCOVER a una subnet che contiene un server DHCP.

Questo agente di inoltro può essere un host dedicato (ad esempio, Microsoft Windows Server) o un router (ad esempio, un router Cisco configurato con istruzioni helper IP a livello di interfaccia).

DHCPOFFER

Un server DHCP che riceve un messaggio DHCPDISCOVER può rispondere con un messaggio DHCP sulla porta UDP 68 (client BootP). Il client riceve il DHCPOFFER e passa allo stato di selezione. Questo messaggio DHCP contiene le informazioni di configurazione iniziale per il client. Ad esempio, il server DHCP inserisce l'indirizzo IP richiesto nel campo yiaddr del messaggio DHCP POFFER. La subnet mask e il gateway predefinito sono specificati rispettivamente nel campo options (Opzioni), subnet mask (Subnet mask) e router (Opzioni router). Altre opzioni comuni nel messaggio DHCPOFFER includono la durata del lease dell'indirizzo IP, il tempo di rinnovo, il server del nome di dominio e il server dei nomi NetBIOS (WINS). Il server DHCP invia il DHCPOFFER all'indirizzo di broadcast ma include l'indirizzo hardware del client nel campo chaddr dell'offerta, in modo che il client sappia che si tratta della destinazione prevista. Nel caso in cui il server DHCP non si trovi nella subnet locale, il server DHCP invia DHCP POFFER, come pacchetto unicast, sulla porta UDP 67, all'agente di inoltro DHCP/BootP da cui proviene DHCPDISCOVER. L'agente di inoltro DHCP/BootP trasmette o trasmette in unicast il DHCPOFFER nella subnet locale sulla porta UDP 68, che dipende dal flag Broadcast impostato dal client Bootp.

DHCPREQUEST

Dopo aver ricevuto un DHCPOFFER, il client risponde con un messaggio DHCPREQUEST e indica la propria intenzione di accettare i parametri in DHCPOFFER e passa allo stato richiedente. Il client può ricevere più messaggi DHCP, uno da ogni server DHCP che ha ricevuto il messaggio DHCPDISCOVER originale. Il client sceglie un DHCP e risponde solo a quel server DHCP e, implicitamente, rifiuta tutti gli altri messaggi DHCP. Il client identifica il server selezionato dopo aver popolato il campo dell'opzione Identificatore server con l'indirizzo IP del server DHCP. Anche DHCPREQUEST è un broadcast, pertanto tutti i server DHCP che hanno inviato un DHCPOFFER visualizzano DHCPREQUEST e ognuno sa se il DHCPOFFER è stato accettato o rifiutato. Le

eventuali opzioni di configurazione aggiuntive richieste dal client sono incluse nel campo options del messaggio DHCPREQUEST. Anche se al client è stato offerto un indirizzo IP, invia il messaggio DHCPREQUEST con un indirizzo IP di origine di 0.0.0.0. In questo momento, il client non ha ancora ricevuto la verifica che sia chiaro utilizzare l'indirizzo IP.

DHCPACK

Dopo aver ricevuto la richiesta DHCPREQUEST, il server DHCP la riconosce con un messaggio DHCP e quindi completa il processo di inizializzazione. Il messaggio DHCP ha un indirizzo IP di origine del server DHCP e l'indirizzo di destinazione è di nuovo una trasmissione e contiene tutti i parametri richiesti dal client nel messaggio DHCPREQUEST. Quando il client riceve il pacchetto DHCP, passa allo stato Bound e può utilizzare l'indirizzo IP per comunicare sulla rete. Nel frattempo, il server DHCP memorizza il lease nel proprio database e lo identifica in modo univoco con l'identificatore del client o chaddr e l'indirizzo IP associato. Sia il client che il server utilizzano questa combinazione di identificatori per fare riferimento al lease. L'identificatore del client è l'indirizzo MAC del dispositivo più il tipo di supporto.

Prima che il client DHCP inizi a utilizzare il nuovo indirizzo, deve calcolare i parametri temporali associati a un indirizzo in lease, ovvero Lease Time (LT), Renewal Time (T1) e Rebind Time (T2). La durata predefinita tipica è 72 ore. Se necessario, è possibile ridurre i tempi di lease per conservare gli indirizzi.

DHCPNAK

Se il server selezionato non è in grado di soddisfare il messaggio DHCPREQUEST, il server DHCP risponde con un messaggio DHCPNAK. Quando il client riceve un messaggio DHCPNAK o non riceve una risposta a un messaggio DHCPREQUEST, riavvia il processo di configurazione quando passa allo stato Requesting. Il client ritrasmette DHCPREQUEST almeno quattro volte entro 60 secondi prima di riavviare lo stato di inizializzazione.

DHCPDECLINE

Il client riceve il DHCPACK e, facoltativamente, esegue un controllo finale sui parametri. Il client esegue questa procedura quando invia le richieste ARP (Address Resolution Protocol) per l'indirizzo IP fornito nel DHCPACK. Se il client rileva che l'indirizzo è già in uso quando riceve una risposta alla richiesta ARP, invia un messaggio DHCPDECLINE al server e riavvia il processo di configurazione nello stato Richiedente.

DHCPINFORM

Se un client ha ottenuto un indirizzo di rete in altro modo o ha un indirizzo IP configurato manualmente, una workstation client può utilizzare un messaggio di richiesta DHCPINFORM per ottenere altri parametri di configurazione locale, ad esempio il nome di dominio e i server dei nomi di dominio (DNS). Quando i server DHCP ricevono un messaggio DHCPINFORM, crea un messaggio DHCPACK con i parametri di configurazione locali appropriati per il client senza un nuovo indirizzo IP. DHCPACK inviato come unicast al client.

DHCPRELEASE

Un client DHCP può scegliere di rinunciare al lease su un indirizzo di rete quando invia un

messaggio DHCPRELEASE al server DHCP. Il client identifica il lease da rilasciare mediante l'utilizzo del campo dell'identificatore `client` e dell'indirizzo di rete nel messaggio DHCPRELEASE. Per estendere l'intervallo corrente del pool DHCP, rimuovere il pool di indirizzi corrente e specificare il nuovo intervallo di indirizzi IP nel pool DHCP. Per rimuovere indirizzi IP specifici o un intervallo di indirizzi da includere nel pool DHCP, utilizzare il comando **ip dhcp exclude-address**.

> **Nota:** Se i dispositivi usano BOOTP, i lease di lunghezza infinita vengono mostrati nei binding DHCP dei router.

Rinnova il leasing

Poiché l'indirizzo IP viene assegnato in lease solo dal server, il lease deve essere rinnovato di tanto in tanto. Quando metà del tempo di lease è scaduto (T1=0,5 x LT), il client tenta di rinnovare il lease. Il client entra nello stato di rinnovo e invia un messaggio DHCPREQUEST al server, che contiene il lease corrente. Il server risponde alla richiesta di rinnovo con un messaggio DHCPACK se accetta di rinnovare il lease. Il messaggio DHCPACK contiene il nuovo lease ed eventuali nuovi parametri di configurazione, nel caso in cui vengano apportate modifiche al server durante il lease precedente. Se il client non è in grado di raggiungere il server quando detiene il lease per qualche motivo, tenta di rinnovare l'indirizzo da qualsiasi server DHCP dopo che il server DHCP originale non ha risposto alle richieste di rinnovo entro un tempo T2. Il valore predefinito di T2 è (7/8 x LT). Ciò significa T1 < T2< LT.

Se in precedenza al client era assegnato un indirizzo IP DHCP e il client viene riavviato, il client richiede esplicitamente l'indirizzo IP precedentemente assegnato in lease in un pacchetto DHCPREQUEST. DHCPREQUEST dispone ancora l'indirizzo IP di origine come 0.0.0.0 e la destinazione come indirizzo di broadcast IP 255.255.255.255.

Quando un client invia una richiesta DHCPREQUEST durante un riavvio, non deve compilare il campo dell'identificatore del server e deve invece compilare il campo dell'opzione dell'indirizzo IP richiesto. Solo i client conformi alla RFC compilano il campo ciaddr con l'indirizzo richiesto anziché con il campo dell'opzione DHCP. Il server DHCP accetta entrambi i metodi. Il comportamento del server DHCP dipende da una serie di fattori, ad esempio nel caso dei server DHCP Windows NT, la versione del sistema utilizzato e altri fattori, ad esempio l'ambito esteso. Se il server DHCP stabilisce che il client può ancora utilizzare l'indirizzo IP richiesto, rimane invisibile all'utente o invia un DHCPACK per DHCPREQUEST. Se il server stabilisce che il client non può utilizzare l'indirizzo IP richiesto, invia un DHCPNACK al client. Il client passa quindi allo stato Initializing e invia un messaggio DHCPDISCOVER.

> **Nota:** Il server DHCP assegna l'indirizzo IP inferiore di un pool di indirizzi IP ai client DHCP. Alla scadenza del lease dell'ultimo indirizzo, questo viene assegnato a un altro client, se richiesto. Non è possibile modificare l'ordine di assegnazione degli indirizzi DHCP.

Tabella pacchetti DHCP

Il messaggio DHCP ha una lunghezza variabile ed è costituito dai campi elencati nella tabella dei pacchetti DHCP.

> **Nota:** Questo pacchetto è una versione modificata del pacchetto BootP originale.

Campo	Byte	Nome	Descrizione
op	1	Codice operativo	Identifica il pacchetto come richiesta o risposta: 1=BOOTREQUEST, 2=BOOTREPLY
tipo	1	Tipo di hardware	Specifica il tipo di indirizzo hardware di rete.
hlen	1	Lunghezza hardware	Specifica la lunghezza dell'indirizzo hardware.
hop	1	Hop	Il client imposta il valore su zero e il valore viene incrementato se la richies viene inoltrata attraverso un router.
xid	4	ID transazione	Numero casuale scelto dal client. Tutti i messaggi DHCP scambiati per una determinata transazione DHCP utilizzano l'ID (xid).
sec	2	Secondi	Specifica il numero di secondi dall'avvio del processo DHCP.
flag	2	Flag	Indica se il messaggio è trasmesso o unicast.
ciaddr	4	Indirizzo IP client	Utilizzato solo quando il client conosce il proprio indirizzo IP come negli sta Bound, Renew o Rebinding.
yiaddr	4	Indirizzo IP	Se l'indirizzo IP del client è 0.0.0.0, il server DHCP inserisce in questo cam l'indirizzo IP del client offerto.
siaddr	4	Indirizzo IP server	Se il client conosce l'indirizzo IP del server DHCP, questo campo viene compilato con l'indirizzo del server DHCP. In caso contrario, viene utilizzat DHCP POFFER e DHCP dal server DHCP.
giaddr	4	Indirizzo IP router (GI ADDR)	Indirizzo IP del gateway, specificato dall'agente di inoltro DHCP/BootP.
chaddr	16	Indirizzo MAC client	Indirizzo MAC del client DHCP.
sname	64	Nome server	Il nome host del server facoltativo.
file	128	Nome file di avvio	Nome del file di avvio.
opzioni	variabile	Parametri opzione	Parametri facoltativi che possono essere forniti dal server DHCP. La RFC offre tutte le opzioni possibili.

Conversazione client-server per il client che ottiene l'indirizzo DHCP in cui il client e il server DHCP risiedono nella stessa subnet

Descrizione pacchetto	Indirizzo MAC di origine	Indirizzo MAC di destinazione	Source IP Addr	Indirizzo IP di destinazione
DHCPDISCOVER	Cliente	Trasmissione	0.0.0.0	255.255.255.255
DHCPOFFER	Server DHCP	Trasmissione	Server DHCP	255.255.255.255
DHCPREQUEST	Cliente	Trasmissione	0.0.0.0	255.255.255.255
DHCPACK	Server DHCP	Trasmissione	Server DHCP	255.255.255.255

Ruolo dell'agente di inoltro DHCP/BootP

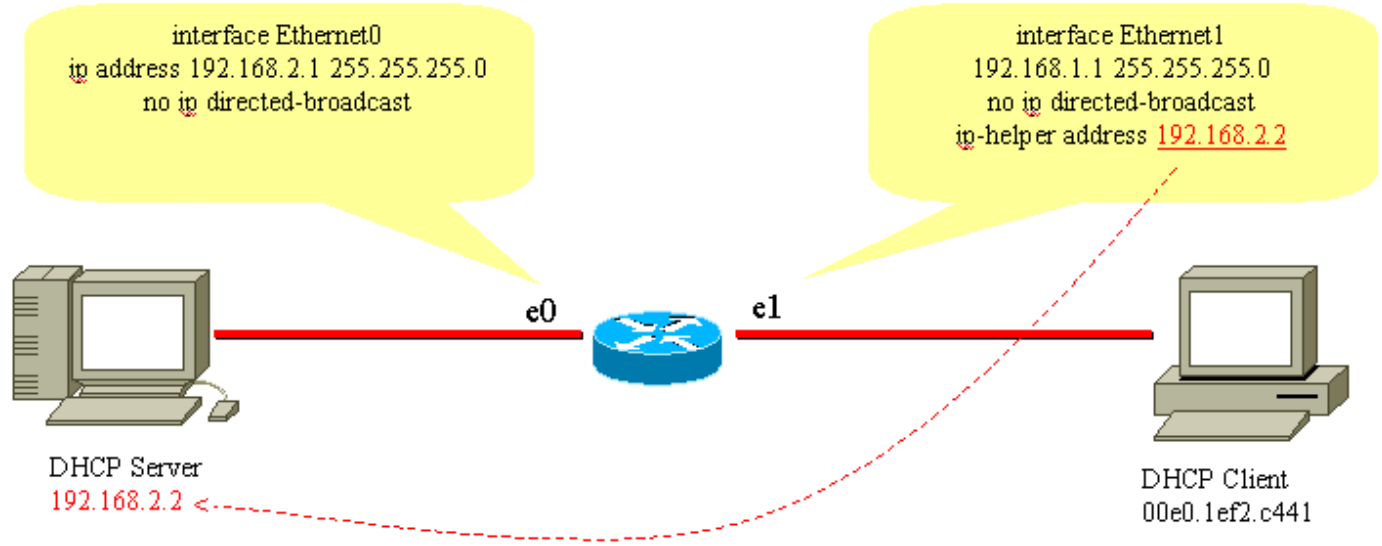
Per impostazione predefinita, i router non inoltrano i pacchetti di broadcast. Poiché i messaggi del client DHCP utilizzano l'indirizzo IP di destinazione 255.255.255.255 (tutte le reti broadcast), i client DHCP non possono inviare richieste a un server DHCP in una subnet diversa a meno che l'agente di inoltro DHCP/BootP non sia configurato sul router. L'agente di inoltro DHCP/BootP inoltra le richieste DHCP per conto di un client DHCP al server DHCP. L'agente di inoltro DHCP/BootP aggiunge il proprio indirizzo IP all'indirizzo IP di origine dei frame DHCP inviati al server DHCP. In questo modo il server DHCP può rispondere tramite unicast all'agente di inoltro DHCP/BootP. L'agente di inoltro DHCP/BootP popola inoltre il campo dell'indirizzo IP del gateway con l'indirizzo IP dell'interfaccia su cui il messaggio DHCP viene ricevuto dal client. Il server DHCP

utilizza il campo Indirizzo IP gateway per determinare la subnet da cui ha origine il messaggio DHCPDISCOVER, DHCPREQUEST o DHCPINFORM.

Configurazione della funzionalità DHCP/BootP Relay Agent sul router Cisco IOS®

Il processo di configurazione di un router Cisco per inoltrare le richieste BootP o DHCP è semplice. È sufficiente configurare un indirizzo dell'helper IP che punti al server DHCP/BootP o all'indirizzo di broadcast della subnet della rete su cui si trova il server.

Esempio di rete:



Agente di inoltro DHCP/BootP

Per inoltrare la richiesta BootP/DHCP dal client al server DHCP, viene usato il comando **ip helper-address interface**. L'indirizzo dell'helper IP può essere configurato per inoltrare qualsiasi trasmissione UDP in base al numero di porta UDP. Per impostazione predefinita, l'indirizzo dell'helper IP inoltra le seguenti trasmissioni UDP:

- Protocollo TFTP (Trivial File Transfer Protocol) (porta 69)
- DNS (porta 53), servizio Ora (porta 37)
- Server dei nomi NetBIOS (porta 137)
- Server datagramma NetBIOS (porta 138)
- Datagrammi client e server del protocollo di avvio (DHCP/BootP) (porte 67 e 68)
- Servizio Terminal Access Control Access Control System (TACACS) (porta 49)
- Servizio di denominazione IEN-116 (porta 42)

Gli indirizzi dell'helper IP possono indirizzare le trasmissioni UDP a un indirizzo IP unicast o broadcast. Tuttavia, non utilizzare l'indirizzo dell'helper IP per inoltrare le trasmissioni UDP da una subnet all'indirizzo di broadcast di un'altra subnet, a causa della grande quantità di broadcast che possono verificarsi. Sono supportate anche più voci di indirizzi dell'helper IP su una singola interfaccia:

```
version 12.0
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname router
!
!
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.2
ip helper-address 192.168.2.3

!--- IP helper-address pointing to DHCP server

no ip directed-broadcast
!
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

I router Cisco non supportano il bilanciamento del carico dei server DHCP configurati come agenti di inoltro DHCP. I router Cisco inoltrano il messaggio DHCPDISCOVER a tutti gli indirizzi dell'helper menzionati per quell'interfaccia. L'utilizzo di due o più server DHCP per la gestione di una subnet non fa che aumentare il traffico DHCP, in quanto i messaggi DHCPDISCOVER, DHCPOFFER e DHCPREQUEST / DHCPDECLINE vengono scambiati tra ogni coppia di client e server DHCP.

Imposta associazioni manuali

Èpossibile impostare le associazioni manuali in due modi: uno è per l'host Windows, l'altro è per gli host non Windows. Per la configurazione, sono disponibili due comandi: una è destinata ai client DHCP Microsoft e l'altra ai client DHCP non Microsoft: **DHCPclient-identifier** (binding manuale - client DHCP Microsoft) **e DHCPhardware-address** (binding manuale - client DHCP non Microsoft). La ragione di due diversi comandi è che un PC che esegue con Windows modifica i propri MAC, e un **01**viene aggiunto all'inizio dell'indirizzo. Di seguito sono riportati gli esempi di configurazione.

- Questa è una configurazione per i client DHCP Microsoft:

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
client-identifier 01xxxxxxxxxxxx

!--- xxxxxx represents 48 bit MAC address prepended with 01
```

- Questa è una configurazione per client DHCP non Microsoft:
  ```
  configure terminal
  ```

```
ip dhcp pool new_pool
host ip_address subnet_mask
hardware-address xxxxxxxxxxxx

!--- xxxxxx represents 48 bit MAC address
```

Come far funzionare DHCP sui segmenti IP secondari

Per impostazione predefinita, il protocollo DHCP prevede un limite in base al quale i pacchetti di risposta vengono inviati solo se la richiesta viene ricevuta dall'interfaccia configurata con l'indirizzo IP primario. Il traffico DHCP utilizza l'indirizzo di broadcast. Quando la richiesta DHCP viene ricevuta dall'interfaccia del router, viene inoltrata al server DHCP (quando è configurato l'indirizzo dell'helper IP) con l'indirizzo di origine dell'IP primario configurato sull'interfaccia per comunicare al server DHCP il pool IP da utilizzare (per il client) nel pacchetto di risposta DHCP.

Il router non è in grado di sapere se la richiesta di trasmissione DHCP proviene da un dispositivo che si trova sulla rete IP secondaria configurata sull'interfaccia. Per ovviare al problema, è possibile configurare una configurazione di sottointerfaccia (a condizione che il dispositivo collegato al router supporti il tagging dot1q) per separare le due subnet, in modo che entrambe ottengano correttamente gli indirizzi IP corrispondenti.

Se l'indirizzo secondario è quello preferito, è disponibile un'altra soluzione che consiste nell'abilitare il **relay smart dhcp** di configurazione globale. Questo è un limite in quanto utilizza solo l'IP secondario per inoltrare la richiesta DHCP se il server DHCP non risponde dopo tre richieste consecutive per il pool di indirizzi primario.

Conversazione client-server DHCP con funzione di inoltro DHCP

Nella tabella seguente viene illustrato il processo con cui un client DHCP ottiene un indirizzo IP da un server DHCP. Questa tabella è basata sul diagramma di rete precedente Configura funzionalità agente di inoltro DHCP/BootP. Ogni valore numerico del diagramma rappresenta un pacchetto descritto nella tabella seguente. Utilizzare questa tabella per comprendere il flusso di pacchetti della conversazione client-server DHCP. Consente inoltre di determinare dove si verificano i problemi.

Processo per ottenere un indirizzo IP da un client DHCP

Pacchetto	Indirizzo IP client	Indirizzo IP server	Indirizzo GI	Indirizzo MAC origine pacchetto	Indirizzo IP origine pacchetto	Indirizzo MAC di destinazione pacchetto	Indir desti pacc
1. DHCPDISCOVER viene inviato dal client.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.fff (broadcast)	255.
2. Il router riceve il comando DHCPDISCOVER sull'interfaccia E1. Il router riconosce che questo pacchetto è un broadcast UDP	0.0.0.0	0.0.0.0	192.168.1.1	Indirizzo MAC interfaccia E2	192.168.1.1	Indirizzo MAC del server DHCP	192.

DHCP. A questo punto, il router svolge la funzione di agente di inoltro DHCP/BootP e compila il campo Indirizzo IP gateway con l'indirizzo IP dell'interfaccia in ingresso, modifica l'indirizzo IP di origine in un indirizzo IP dell'interfaccia in ingresso e inoltra la richiesta direttamente al server DHCP.								
3. Il server DHCP ha ricevuto il comando DHCPDISCOVER e invia un comando DHCPOFFER all'agente di inoltro DHCP.	192.168.1.2	192.168.2.2	192.168.1.1	Indirizzo MAC del server DHCP	192.168.2.2	Indirizzo MAC interfaccia E2	192.
4. L'agente di inoltro DHCP riceve un DHCPOFFER e inoltra la trasmissione DHCP POFFER sulla LAN locale.	192.168.1.2	192.168.2.2	192.168.1.1	Indirizzo MAC interfaccia E1	192.168.1.1	ffff.ffff.ffff (broadcast)	255.
5. DHCPREQUEST inviato dal client.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.fff (broadcast)	255.
6. Il router riceve la richiesta DHCP sull'interfaccia E1. Il router riconosce che il pacchetto è un broadcast UDP DHCP. Il router ora funge da agente di inoltro DHCP e compilare il campo Indirizzo	0.0.0.0	0.0.0.0	192.168.1.1	Indirizzo MAC interfaccia E2	192.168.1.1	Indirizzo MAC del server DHCP	192.

IP gateway con l'indirizzo IP dell'interfaccia inviata, modificare l'indirizzo IP di origine in un indirizzo IP dell'interfaccia in ingresso e inoltrare la richiesta direttamente al server DHCP. 7. Il server DHCP ha ricevuto DHCPREQUEST e invia un DHCP all'agente di inoltro DHCP/BootP.	192.168.1.2	192.168.2.2	192.168.1.1	Indirizzo MAC del server DHCP	192.168.2.2	Indirizzo MAC interfaccia E2	192.
8. L'agente di inoltro DHCP/BootP riceve il DHCP e inoltra la trasmissione DHCP sulla LAN locale. Il client accetta l'ACK e utilizza l'indirizzo IP del client.	192.168.1.2	192.168.2.2	192.168.1.1	Indirizzo MAC interfaccia E1	192.168.1.1	ffff.ffff.ffff (broadcast)	255.

Considerazioni su Pre-Execution Environment (PXE) di avvio DHCP

Pre-Execution Environment (PXE) consente l'avvio di una workstation da un server in una rete prima dell'avvio del sistema nel disco rigido locale. L'amministratore di rete non deve visitare fisicamente la workstation specifica e avviarla manualmente. Il sistema operativo e altri software, ad esempio programmi di diagnostica, possono essere caricati sul dispositivo da un server in rete. L'ambiente PXE utilizza DHCP per configurare il proprio indirizzo IP.

La configurazione dell'agente di inoltro DHCP/BootP deve essere eseguita sul router se il server DHCP si trova su un altro segmento indirizzato della rete. **È** necessario configurare il comando **ip helper-address** sull'interfaccia del router locale. Per informazioni sulla configurazione, consultare la sezione Configurazione della funzione DHCP/BootP Relay Agent sui router Cisco IOS di questo documento.

Comprendere e risolvere i problemi relativi a DHCP con tracce di sniffer

Decodifica traccia sniffer di client e server DHCP sullo stesso segmento LAN

Topologia di rete in cui il client e il server DHCP risiedono sullo stesso segmento LAN

L'esempio di traccia dello sniffer è costituito da sei fotogrammi. Questi sei frame illustrano uno scenario in cui il client e il server DHCP risiedono sullo stesso segmento fisico o logico. Nell'esempio di codice seguente viene illustrato come risolvere i problemi relativi a DHCP. È importante far corrispondere la traccia dello sniffer alle tracce di questo esempio. Ci possono essere alcune differenze rispetto alle successive tracce illustrate, ma il flusso generale del pacchetto deve essere esattamente lo stesso. La traccia del pacchetto segue le discussioni precedenti sul funzionamento di DHCP.

```
- - - - - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 1arrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 9
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B988 (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
```

DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: **Message Type = 1 (DHCP Discover)**
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 5
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)

IP: Header checksum = F901 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = **67 (BootPs/DHCP)**
UDP: Destination port = **68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewal interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Frame 3 - DHCPREQUEST** - - - - - - - - - - - - - - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC9C640**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay

IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 10
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B987 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 6
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F900 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:

DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewal interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Frame 5 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- **Frame 6 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding

ARP:

Decodifica la traccia dello sniffer del client e del server DHCP separati da un router configurato come agente di inoltro DHCP

Traccia Sniffer-B

- **Frame 1 - DHCPDISCOVER** -

```
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1 [0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 124 arrived at 06:53:04.2043; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCF2C441
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 183
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8DA (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
```

```
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- - - - - - - - - - - - - - - - - - - - - - Frame 2 - DHCPOFFER - - - - - - - - - - - - - - - - - - - -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summaryr
125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772 0.012.764 05/31/2001 06:53:04 AM DHCP:
Reply,
 Message type: DHCP Offer
DLC: ----- DLC Header -----
DLC:
DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 003094248F71
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 45
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C9 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
```

```
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 68 (BootPc/DHCP)
UDP: Length = 313
UDP: Checksum = 8517 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Address Renewal interval = 49735 (seconds)
DHCP: Address Rebinding interval = 87037 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

- - - - - - - - - - - - - - - - - - - - - Frame 3 - DHCPREQUEST - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request,
 Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
```

IP: Total length = 604 bytes
IP: Identification = 184
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8D9 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: **Server IP address = [192.168.2.2]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary

4 [192.168.1.1] [255.255.255.255] 347 0:02:05.787 0.012.875 05/31/2001 06:53:04 AM DHCP: Reply,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 127 arrived at 06:53:04.2321; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 47
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C7 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 326F (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)

```
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

- - - - - - - - - - - - - - - - - - - - - Frame 5 - ARP - - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - - - - - - - - - - - - - - - - - Frame 6 - ARP - - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Sniffer-A Trace

- **Frame 1 - DHCPDISCOVER** -

```
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 52
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3509 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 0A19 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
```

DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 41
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3623 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 313
UDP: Checksum = A1F8 (correct)
UDP: [305 byte(s) of data]
UDP:

```
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Address Renewal interval = 86285 (seconds)
DHCP: Address Rebinding interval = 150999 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

- - - - - - - - - - - - - - - - - - - - Frame 3 - DHCPREQUEST - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 54
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
```

IP: Protocol = 17 (UDP)
IP: Header checksum = 3507 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [192.168.2.2]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: Checksum = 4699 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**

DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 42
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3622 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 313
UDP: Checksum = 7DF6 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**

```
DHCP: Domain name = "cisco.com"
DHCP:
```

Risoluzione dei problemi relativi a DHCP quando le workstation client non sono in grado di ottenere gli indirizzi DHCP

Case study 1: Server DHCP sullo stesso segmento LAN o VLAN del client DHCP

Quando il server DHCP e il client si trovano sullo stesso segmento LAN o sulla stessa VLAN e il client non è in grado di ottenere un indirizzo IP da un server DHCP. Tuttavia, è improbabile che il router locale causi un problema DHCP. Il problema è relativo ai dispositivi che connettono il server DHCP e il client DHCP. Tuttavia, il problema può riguardare il server DHCP o il client stesso. Questi moduli aiutano a risolvere i problemi e a determinare quale dispositivo causa un problema.

> **Nota:** Per configurare il server DHCP in base alle singole vlan, definire pool DHCP diversi per ciascuna VLAN che serva gli indirizzi DHCP ai client.

Case study 2: Il server DHCP e il client DHCP sono separati da un router configurato per la funzionalità dell'agente di inoltro DHCP/BootP

Quando il server e il client DHCP risiedono su segmenti LAN o VLAN diversi, il router svolge la funzione di agente di inoltro DHCP/BootP responsabile dell'inoltro di DHCPREQUEST al server DHCP. Per risolvere i problemi relativi all'agente di inoltro DHCP/BootP, nonché al server DHCP e al client, sono necessari ulteriori passaggi. Se si seguono questi moduli, è possibile determinare quale dispositivo causa i problemi.

Il server DHCP sul router non riesce ad assegnare gli indirizzi con un errore POOL EXHAUSTED

Èpossibile che alcuni indirizzi siano ancora detenuti dai client, anche se vengono rilasciati dal pool. È possibile verificare questa condizione **tramite il** conflitto **show ip dhcp** output. Un conflitto di indirizzi si verifica quando due host utilizzano lo stesso indirizzo IP. All'assegnazione dell'indirizzo, il DHCP verifica la presenza di conflitti con il ping e l'ARP gratuito.

Se viene rilevato un conflitto, l'indirizzo viene rimosso dal pool. L'indirizzo viene assegnato finché l'amministratore non risolve il conflitto. **Per** risolvere il problema, **configurare** l'opzione di registrazione dei **conflitti ip dhcp**.

Moduli di risoluzione dei problemi DHCP

Comprendere dove possono verificarsi problemi con DHCP

I problemi relativi al protocollo DHCP possono essere dovuti a diversi motivi. I motivi più comuni sono i problemi di configurazione. Tuttavia, molti problemi relativi al protocollo DHCP possono essere causati da problemi software nei sistemi, nei driver delle schede di interfaccia di rete (NIC, Network Interface Card) o negli agenti di inoltro DHCP/BootP eseguiti sui router. Dato il numero di aree potenzialmente problematiche, è necessario un approccio sistematico alla risoluzione dei problemi.

Elenco breve delle possibili cause dei problemi DHCP:

- Configurazione predefinita dello switch Catalyst
- Configurazione agente di inoltro DHCP/BootP
- Problema di compatibilità NIC o di funzionalità DHCP
- Installazione errata della scheda NIC o del driver della scheda NIC
- Interruzioni intermittenti della rete dovute a frequenti calcoli Spanning Tree
- Comportamento del sistema operativo o errore del software
- Configurazione dell'ambito del server DHCP o errore software
- Errore software dello switch Cisco Catalyst o dell'agente di inoltro DHCP/BootP Cisco IOS
- Controllo unicast Reverse Path Forwarding (uRPF) non riuscito. L'offerta DHCP viene ricevuta su un'interfaccia diversa da quella prevista. Quando su un'interfaccia è abilitata la funzione Reverse Path Forwarding (RPF), un router Cisco può eliminare i pacchetti DHCP (Dynamic Host Configuration Protocol) e BOOTstrap Protocol (BOOTP) con indirizzi di origine 0.0.0.0 e indirizzi di destinazione 255.255.255.255. Il router può anche eliminare tutti i pacchetti IP con destinazione IP multicast sull'interfaccia. Questo problema è documentato nell'ID bug Cisco CSCdw31925

Nota Solo i client Cisco registrati possono accedere alle segnalazioni dei bug.

- L'agente del database DHCP non viene utilizzato, ma la registrazione dei conflitti DHCP non è disabilitata

A. Verifica della connettività fisica

Questa procedura è applicabile a tutti i casi aziendali.

Verificare innanzitutto la connettività fisica di un client e di un server DHCP. Se collegato a uno switch Catalyst, verificare che il client e il server DHCP dispongano entrambi di connettività fisica. Per gli switch con Cisco IOS come Catalyst 2900XL/3500XL/2950/3550, usare il comando equivalente **per visualizzare lo stato della porta** e **visualizzare l'interfaccia <interface>**. Se lo stato dell'interfaccia è diverso da <`interface`> is up, il protocollo di linea è attivo, la porta non trasmette il traffico, nemmeno le richieste del client DHCP. L'output dei comandi:

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.acc1 (bia 0030.94dc.acc1)
```

Se la connessione fisica è stata verificata e non è presente alcun collegamento tra lo switch Catalyst e il client DHCP, utilizzare la sezione Risoluzione dei problemi di compatibilità NIC degli switch Cisco Catalyst per risolvere i problemi di connettività del livello fisico.

Un numero eccessivo di errori di collegamento dati causa lo stato err-disabled delle porte di alcuni switch Catalyst. Per ulteriori informazioni, fare riferimento a Ripristino di una porta disabilitata a causa di un errore sulle piattaforme Cisco IOS, che descrive lo stato err-disabled, spiega come ripristinare le porte disabilitate a causa di un errore e fornisce esempi di ripristino da questo stato.

B. Configurare la workstation client e l'IP statico per verificare la connettività di rete

Questa procedura è applicabile a tutti i casi aziendali.

Per risolvere i problemi relativi al protocollo DHCP, è importante configurare un indirizzo IP statico su una workstation client per verificare la connettività di rete. Se la workstation non è in grado di raggiungere le risorse di rete nonostante abbia un indirizzo IP configurato staticamente, la causa principale del problema non è DHCP. A questo punto, è necessario risolvere i problemi relativi alla connettività di rete.

C. Verifica del problema come problema di avvio

Questa procedura è applicabile a tutti i casi aziendali.

Se il client DHCP non riesce a ottenere un indirizzo IP dal server DHCP all'avvio, è possibile forzare manualmente il client a inviare una richiesta DHCP. Eseguire i passaggi successivi per ottenere manualmente un indirizzo IP da un server DHCP per il sistema operativo elencato.

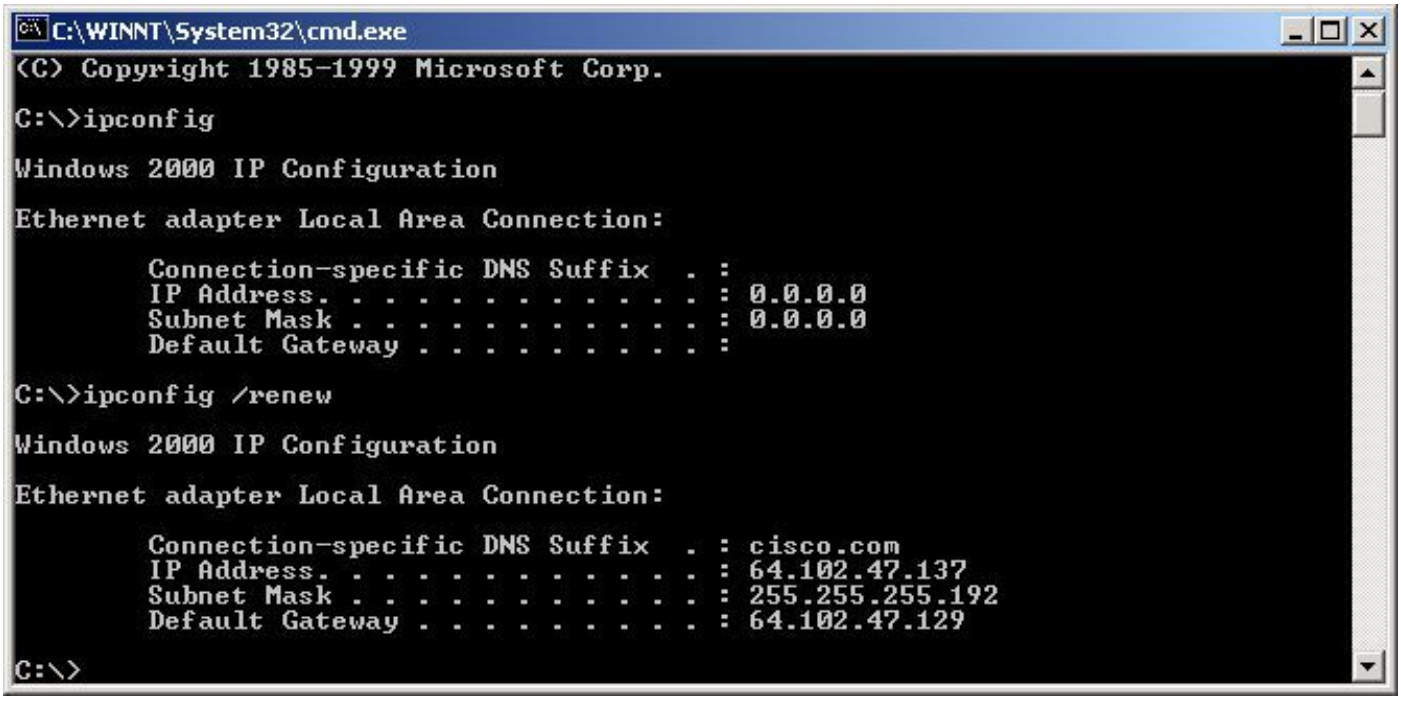
Microsoft Windows 95/98/ME:

1. Fare clic sul pulsante Start ed eseguire il programma WINIPCFG.exe.
2. Fare clic **sul** pulsante **Rilascia** tutto, seguito **dal** pulsante **Rinnova** tutto.
3. Il client DHCP è ora in grado di ottenere un indirizzo IP?

Finestra Configurazione IP

Microsoft Windows NT/2000:

1. Immettere **il** cmdlet **Start/**Runfield per aprire una finestra del prompt dei comandi.
2. Eseguire il comando **commandipconfig/**RENEP nella finestra del prompt dei comandi.
3. Il client DHCP è ora in grado di ottenere un indirizzo IP?



Prompt della riga di comando

Se il client DHCP è in grado di ottenere un indirizzo IP con un rinnovo manuale dell'indirizzo IP dopo che il PC ha completato il processo di avvio, è molto probabile che si tratti di un problema di avvio di DHCP. Se il client DHCP è collegato a uno switch Cisco Catalyst, il problema è probabilmente dovuto a un problema di configurazione che riguarda la portfast STP e/o il channeling e il trunking. Altre possibilità includono problemi con le schede NIC e problemi di avvio delle porte dello switch. Esaminare le fasi D ed E per escludere i problemi di configurazione della porta dello switch e della scheda NIC come causa principale del problema DHCP.

D. Verifica della configurazione delle porte dello switch (STP Portfast e altri comandi)

Se lo switch è un Catalyst 2900/4000/5000/6000, verificare che la porta abbia STP portfast abilitato e che il trunking/channeling disabilitato. La configurazione predefinita è STP portfast disabilitata e trunking/channeling auto, se applicabile. Per gli switch serie 2900XL/3500XL/2950/3550, l'unica configurazione richiesta è STP portfast. Queste modifiche alla configurazione risolvono i problemi più comuni dei client DHCP che si verificano con l'installazione iniziale di uno switch Catalyst.

Per ulteriori informazioni sui requisiti di configurazione delle porte dello switch affinché DHCP funzioni correttamente quando collegato agli switch Catalyst, consultare il documento sull'uso di Portfast e di altri comandi per risolvere i ritardi della connettività di avvio della workstation.

Dopo aver esaminato il documento, è possibile continuare a risolvere i problemi.

E. Verifica della presenza di problemi noti relativi alla scheda NIC o allo switch Catalyst

Se la configurazione dello switch Catalyst è corretta, è possibile che sullo switch Catalyst o sulla scheda NIC del client DHCP si sia verificato un problema di compatibilità software che potrebbe causare problemi con il server DHCP. Il passaggio successivo per la risoluzione dei problemi consiste nell'esaminare la risoluzione dei problemi di compatibilità NIC degli switch Cisco Catalyst e nell'escludere eventuali problemi software dello switch Catalyst o della scheda NIC che contribuiscono al problema.

Per eliminare correttamente eventuali problemi di compatibilità, è necessario conoscere il sistema operativo del client DHCP e le informazioni specifiche sulla scheda NIC, ad esempio il produttore, il modello e la versione del driver.

F. Distinguere se i client DHCP ottengono l'indirizzo IP nella stessa subnet o VLAN del server DHCP

Èimportante distinguere se DHCP funziona correttamente o meno quando il client si trova sulla stessa subnet o VLAN del server DHCP. Se il protocollo DHCP funziona correttamente sulla stessa subnet o VLAN del server DHCP, il problema DHCP è causato principalmente dall'agente di inoltro DHCP/BootP. Se il problema persiste anche quando si esegue il test del protocollo DHCP sulla stessa subnet o VLAN del server DHCP, il problema potrebbe essere causato dal server DHCP.

G. Verifica della configurazione del relay DHCP/BootP del router

Per verificare la configurazione:

1. Quando si configura il inoltro DHCP su un router, verificare che il comando **ip helper-**address si trovi sull'interfaccia corretta. **Il comando ip helper-**address deve essere presente sull'interfaccia in entrata delle workstation client DHCP e deve essere indirizzato al server DHCP corretto.
2. Verificare che il **comando di** configurazione globale **dhcp service** non sia presente. Questo parametro di configurazione disabilita tutte le funzionalità del server DHCP e dell'inoltro sul router. La configurazione predefinita, service dhcp, non viene visualizzato nella configurazione ed è il comando di configurazione predefinito. Se **il protocollo dhcp del servizio** non è abilitato, i client non ricevono gli indirizzi IP dal server DHCP.**Nota:** Nei router con versioni precedenti di Cisco IOS, il comando **ip bootp server** gestisce la funzione dell'agente di inoltro DHCP anziché il comando **service dhcp**. Per questo motivo, il comando **ip bootp server** deve essere abilitato in questi router se il comando **ip helper-address** è configurato per inoltrare i broadcast UDP DHCP e funzionare correttamente come agente di inoltro DHCP per conto del client DHCP.
3. Quando si utilizzano i comandi **ip helper-**address per inoltrare i broadcast UDP a un indirizzo di broadcast di subnet, verificare che no ip directed-broadcast non è configurato su nessuna interfaccia in uscita che i pacchetti di broadcast UDP devono attraversare. OSPF (Open Shortest Path First) no ip directed-broadcast blocca qualsiasi traduzione di una trasmissione diretta a trasmissioni fisiche. Questa configurazione di interfaccia è la configurazione predefinita nelle versioni software 12.0 e successive.
4. Quando le trasmissioni DHCP vengono inoltrate all'indirizzo di broadcast della subnet del server DHCP, può verificarsi un problema software. Per risolvere i problemi relativi a DHCP, provare a inoltrare i broadcast UDP DHCP all'indirizzo IP del server DHCP:

H. Opzione Identificazione Abbonato (82) Attivata

La funzionalità delle informazioni dell'agente di inoltro DHCP (opzione 82) consente agli agenti di inoltro DHCP (switch Catalyst) di includere informazioni su se stesso e sul client collegato quando inoltra le richieste DHCP da un client DHCP a un server DHCP.

Il server DHCP può utilizzare queste informazioni per assegnare indirizzi IP, eseguire il controllo

degli accessi e impostare criteri di qualità del servizio (QoS) e di sicurezza (o altri criteri di assegnazione dei parametri) per ogni sottoscrittore di una rete di provider di servizi. Quando lo snooping DHCP è abilitato su uno switch, abilita automaticamente l'opzione 82. Se il server DHCP non è configurato per gestire i pacchetti con l'opzione 82, cessa di allocare l'indirizzo alla richiesta. Per risolvere il problema, disabilitare l'opzione di identificazione del sottoscrittore (82) negli switch (agenti di inoltro) con il comando di configurazione globale,**no ip dhcp relay information option**.

I. Agente del database DHCP e registrazione dei conflitti DHCP

Un agente di database DHCP è un host, ad esempio un server FTP, TFTP o RCP, in cui viene archiviato il database dei binding DHCP. È possibile configurare più agenti di database DHCP e l'intervallo tra gli aggiornamenti e i trasferimenti di database per ogni agente. Utilizzare il comando **ip dhcp database** per configurare un agente di database e i relativi parametri.

Se si sceglie di non configurare un agente di database DHCP, disattivare la registrazione dei conflitti di indirizzi DHCP sul server DHCP. Eseguire il comando **noip dhcp conflict logging** per disabilitare la registrazione dei conflitti di indirizzi DHCP. Cancella i conflitti registrati in precedenza **con il conflitto clear ip dhcp**.

Se non è possibile disattivare la registrazione dei conflitti, viene visualizzato questo messaggio di errore:

```
%DHCPD-4-DECLINE_CONFLICT: DHCP address conflict: client
```

J. Controllare CDP per le connessioni telefoniche IP

Quando la porta dello switch collegata al telefono IP Cisco ha il protocollo CDP (Cisco Discovery Protocol) disabilitato, il server DHCP non può assegnare un indirizzo IP appropriato al telefono. Il server DHCP in genere assegna l'indirizzo IP che appartiene alla VLAN dati o alla subnet della porta dello switch. Se il CDP è abilitato, lo switch può rilevare che il Cisco IP Phone richiede il DHCP e può fornire le informazioni corrette sulla subnet. Il server DHCP è quindi in grado di allocare un indirizzo IP dal pool di voci VLAN/subnet. Non sono richiesti passaggi espliciti per associare il servizio dhcp alla voice vlan.

K. Remove Down SVI interrompe l'operazione di snooping DHCP

Sugli switch Cisco Catalyst serie 6500, viene creata automaticamente una SVI (in stato shutdown) dopo aver configurato il DHCP per lo snoop su una particolare VLAN. La presenza di questa SVI ha implicazioni dirette sul corretto funzionamento dello snooping DHCP.

Lo snooping DHCP sugli switch Cisco Catalyst serie 6500 con Cisco IOS nativo è implementato principalmente su Route Processor (RP o MSFC) e non su Switch Processor (SP o Supervisor). Cisco Catalyst serie 6500 intercetta i pacchetti nell'hardware con VACL che forniscono i pacchetti a una logica di destinazione locale (LTL) sottoscritta dall'RP. Una volta che i frame entrano nell'RP, devono prima essere associati a un IDB dell'interfaccia L3 (SVI) prima di poter essere trasmessi alla parte snooping. Senza una SVI, questo IDB non esiste, e i pacchetti vengono scartati nell'RP.

L. Indirizzo broadcast limitato

Quando un client DHCP imposta il bit di trasmissione in un pacchetto DHCP, il server DHCP e

l'agente di inoltro inviano messaggi DHCP ai client con l'indirizzo di trasmissione all-one (255.255.255.255). Se il comando **ip broadcast-address** è stato configurato per inviare una trasmissione in rete, la trasmissione all-one inviata da DHCP viene ignorata. Per risolvere questo problema, utilizzare il comando **ip dhcp limited-broadcast-address** per verificare che una trasmissione in rete configurata non sostituisca il comportamento DHCP predefinito.

Alcuni client DHCP possono accettare solo trasmissioni all-one e non sono in grado di acquisire un indirizzo DHCP a meno che questo comando non sia configurato sull'interfaccia del router connessa al client.

M. Debug DHCP con comandi di debug del router

Verifica che il router riceva la richiesta DHCP con i comandi di debug

Sui router che supportano il software di elaborazione dei pacchetti DHCP, è possibile verificare se un router riceve la richiesta DHCP dal client. Il processo DHCP ha esito negativo se il router non riceve richieste dal client. In questo passaggio viene configurato un elenco degli accessi per eseguire il debug dell'output. Questo elenco degli accessi viene usato solo per eseguire il debug di un comando e non è intrusivo per il router.

In modalità di configurazione globale, immettere il seguente elenco degli accessi:

access-list 100 allow ip host 0.0.0.0 host 255.255.255.255

In modalità di esecuzione, immettere il comando debug:

debug ip packet detail 100

Output di esempio

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

Da questo esempio di output è chiaro che il router riceve attivamente le richieste DHCP dal client. Questo output mostra solo un riepilogo del pacchetto e non il pacchetto stesso. Pertanto, non è possibile determinare se il pacchetto è corretto. Tuttavia, il router ha ricevuto un pacchetto di trasmissione con le porte IP e UDP di origine e di destinazione corrette per DHCP.

Verificare che il router riceva e inoltri la richiesta DHCP con il comando debug ip udp

Il comando **debug ip udp** può tracciare il percorso di una richiesta DHCP tramite un router. Tuttavia, questo debug è intrusivo in un ambiente di produzione, poiché tutti i pacchetti UDP commutati elaborati vengono visualizzati sulla console. Questo comando debug non deve essere utilizzato nella produzione.

Avviso: Il comando **debug ip udp** è intrusivo e può causare un elevato utilizzo della CPU.

In modalità di esecuzione, immettere il comando debug: **debug ip udp**

Output di esempio

```
Router#debug ip udp
UDP packet debugging is on
Router#

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPDISCOVER from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source
IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPOFFER from DHCP server directed to DHCP/BootP Relay Agent IP address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPOFFER from DHCP server to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPREQUEST from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source
IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to DHCP/BootP Relay Agent IP
address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.

00:18:50: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.
```

Verificare che il router riceva e inoltri la richiesta DHCP con il comando debug ip dhcp server packet

Se il router Cisco IOS è versione 12.0.x.T o 12.1 e supporta la funzionalità del server DHCP Cisco IOS, è possibile usare il comando **debug ip dhcp server packet**. Questo debug è stato progettato per essere usato con la funzionalità server DHCP IOS e per risolvere i problemi relativi all'agente di inoltro DHCP/BootP. Come per i passaggi precedenti, i debug del router non permettono di

determinare con esattezza il problema, in quanto il pacchetto effettivo non può essere visualizzato. Tuttavia, i debug consentono di fare deduzioni riguardo all'elaborazione DHCP. In modalità di esecuzione, immettere questo comando debug:

pacchetto server dhcp ip di debug

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.

!--- Router received DHCPDISCOVER/REQUEST/INRORM and setting Gateway IP address to 192.168.1.1
for forwarding.

00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..

!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.


!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.

00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.

!--- BOOTREPLY includes DHCPOFFER and DHCPNAK.


!--- Client's MAC address is 00e0.1ef2.c441.

00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.

!--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.

00:20:54: DHCPD: setting giaddr to 192.168.1.1.

!--- Router received DHCPDISCOVER/REQUEST/INFORM and set Gateway IP address to 192.168.1.1 for
forwarding.

00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..

!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.


!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.

00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.

!--- BOOTREPLY includes DHCPOFFER and DHCPNAK.


!--- Client's MAC address is 00e0.1ef2.c441.

00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.

!--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.
```

Esegui più debug contemporaneamente

Quando si eseguono più debug contemporaneamente, è possibile rilevare una quantità ragionevole di informazioni relative al funzionamento dell'agente di inoltro DHCP/BootP e del server. Se si usano le strutture precedenti per risolvere il problema, è possibile fare delle deduzioni su dove la funzionalità DHCP/BootP Relay Agent non funziona correttamente.

```
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328.
```

Ottenere la traccia dello sniffer e determinare la causa principale del problema DHCP

Controllare la traccia dello sniffer di decodifica del client e del server DHCP sullo stesso segmento LAN e decodificare la traccia dello sniffer del client e del server DHCP separati dal router configurato come sezioni dell'agente di inoltro DHCP

per decifrare le tracce dei pacchetti DHCP.

Per informazioni su come ottenere le tracce dello sniffer con la funzionalità Switched Port Analyzer (SPAN) sugli switch Catalyst, fare riferimento all'esempio di configurazione di Catalyst Switched Port Analyzer (SPAN).

Metodo alternativo di decodifica del pacchetto con debug sul router

Con il comando **debug ip packet detail dump <acl>**su un router Cisco, è possibile ottenere un intero pacchetto in formato esadecimale visualizzato nel log del sistema o nell'interfaccia della riga di comando (CLI). Verificare che il router riceva la richiesta DHCP con i comandi di debug e che il router riceva la richiesta DHCP e inoltri la richiesta al server DHCP con le sezioni dei comandi di debug precedenti, insieme alla parola chiave dump aggiunta all'elenco degli accessi, per ottenere le stesse informazioni di debug, ma con i dettagli del pacchetto in formato esadecimale. Per determinare il contenuto del pacchetto, il pacchetto deve essere tradotto. Un esempio è fornito nell'Appendice A.

Appendice A Configurazione di esempio per Cisco IOS DHCP

Il database del server DHCP è organizzato in una struttura ad albero. La radice dell'albero è il pool

di indirizzi per le reti naturali, i rami sono pool di indirizzi di sottorete e le foglie sono associazioni manuali ai client. Le sottoreti ereditano i parametri di rete e i client i parametri di sottorete. Pertanto, i parametri comuni, ad esempio il nome di dominio, devono essere configurati al livello più alto (rete o sottorete) della struttura.

Per ulteriori informazioni su come configurare DHCP e i comandi associati, consultare l'elenco delle attività di configurazione DHCP.

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password cisco
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.1.1 10.10.1.199

!--- Address range excluded from DHCP pools.

ip dhcp pool test_dhcp

!--- DHCP pool (scope) name is test_dhcp.

network 10.10.1.0 255.255.255.0

!--- DHCP pool (address will be assigned in this range) for associated Gateway IP address.

default-router 10.10.1.1

!--- DHCP option for default gateway.

dns-server 10.30.1.1

!--- DHCP option for DNS server(s).

netbios-name-server 10.40.1.1

!--- DHCP option for NetBIOS name server(s) (WINS).

lease 0 0 1

!--- Lease time.

interface Ethernet0
description DHCP Client Network
ip address 10.10.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
description Server Network
ip address 10.10.2.1 255.255.255.0
no ip directed-broadcast
!
line con 0
transport input none
line aux 0
transport input all
```

```
line vty 0 4
login
!
end
```

Informazioni correlate

- Strumenti e risorse
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).