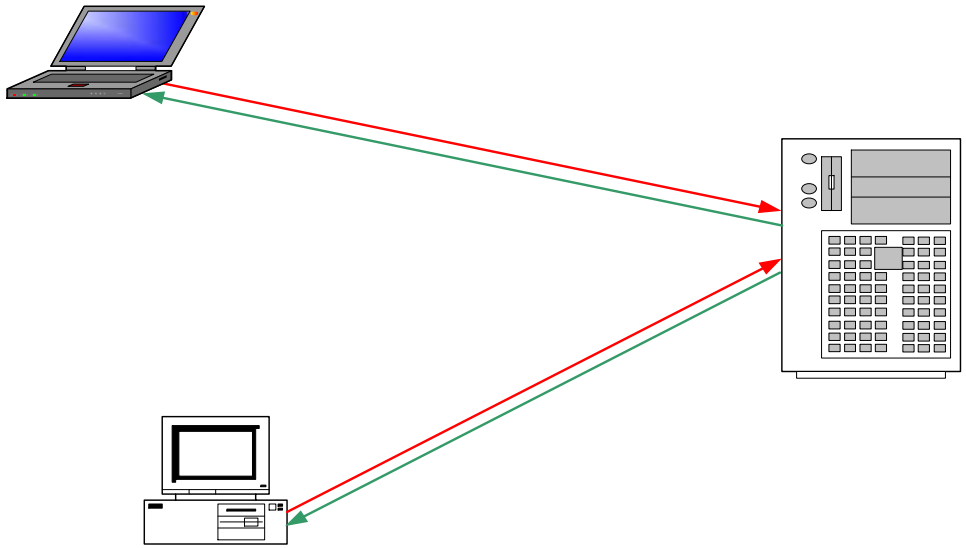
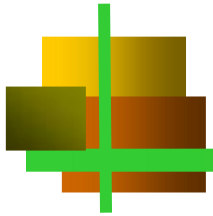
Dynamic Host Configuration Protocol

L'assegnazione automatica dei parametri di configurazione (e.g. network address) al momento dell'avvio dei client di una rete, semplifica l'amministrazione della stessa



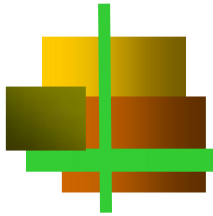


Esigenze da soddisfare

- I diversi protocolli (TCP/IP, IPX/SPX, etc) hanno bisogno di informazioni specifiche (parametri) per funzionare

- Il software di protocollo utilizza i parametri per funzionare su una data rete e/o su un dato hardware

- Il processo di fornitura dei parametri viene chiamato *configurazione*

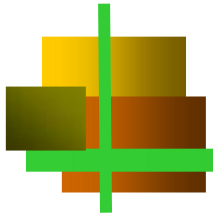


Problema del bootstrap

- All'avvio bisogna lanciare il software di protocollo
- Servono: Software, Parametri
- Da dove caricare il software
- Come ottenere i parametri di configurazione

Origine software e parametri

- Il software di protocollo può essere:
  - Ricavato da una rom interna
  - Caricato da un disco al boot
  - Precaricato col sistema operativo
- I parametri del protocollo possono essere:
  - Inseriti manualmente
  - Ricavati da un file locale su disco
  - Ottenuti automaticamente dalla rete



DHCP e DNS

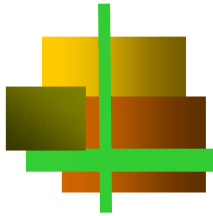
Inizialmente si è provveduto alla impostazione manuale dei diversi parametri negli host di una rete e a introdurre la coppia *domain name - network address* nei file di configurazione dei nameserver della zona

Questa soluzione va bene nel caso di poche ed infrequenti variazioni poiché per ogni variazione si deve agire manualmente sui file di configurazione

Nel caso di variazioni frequenti (e.g. spostamenti da una subnet ad un'altra) e/o di reti di grandi dimensioni dà luogo ad un lavoro complesso ed intenso per il network administrator

Inoltre provoca uno sfruttamento non ottimale degli IP address che risultano impegnati anche quando non servono.

Opportuna quindi una soluzione automatica → DHCP

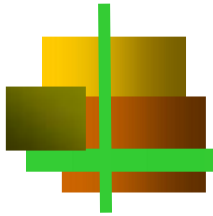


Cosa è e fa DHCP

- DHCP soluzione della suite TCP/IP
- DHCP consente una messa in rete *plug-and-play*
- Gli host (client) inviano al server una richiesta
- Il server trova un IP address inutilizzato
- Il server aggiunge l'IP address al suo elenco
- Il server trasmette all'host l'IP address ed i parametri

Parametri del protocollo IP

- IP address (dipendente dalla rete in cui l'host si trova)
- Subnet mask (necessaria per ricavare la subnet e definire il subnet addressing)
- Gateway address (address a cui spedire i pacchetti diretti all'esterno della subnet)
- Domain name (definisce il nome della rete in cui l'host opera)
- Etc . . .



Problematiche del TCP/IP

- TCP/IP - Suite aperta, robusta e adattabile ad ambienti diversi con molti vantaggi rispetto ad altre soluzioni
- TCP/IP - Amministrativamente pesante
- Conseguenza → Grande sforzo per l'amministrazione delle reti grandi e/o complesse

Problematiche del TCP/IP (2)

Con TCP/IP ogni dispositivo sulla rete deve avere un IP address valido

Nell'assegnazione degli IP address si devono seguire delle regole:

- Un IP address (con IPv4) è formato da 4 byte e deve essere unico.
- Tutti i dispositivi posti su un segmento devono avere lo stesso network address e lo stesso subnet address.
- I subnet address su una data subnet devono essere unici.
- Per comunicare con un nodo posto su una network differente bisogna attraversare un gateway.
- Per usare i domain names e non gli IP address bisogna conoscere l'IP address del nameserver.

Problematiche del TCP/IP (3)

Assegnazione IP address → Compito oneroso

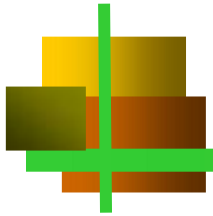
- Necessità di tenere conto degli IP address già assegnati.
- Necessità di seguire lo spostamento degli host da una subnet all'altra.
- Se un host si sposta su una subnet differente il suo host address potrebbe essere in conflitto con quello di un altro host.

Configurazione automatica

Problema generale

Metodologie possibili:

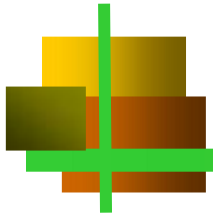
- Decentralizzata con determinazione indipendente
- Server based



Acquisizione decentralizzata

Problema: Come usare la rete per ricavare il network address ?

- Uso di un protocollo di livello più basso
- Uso di un indirizzo broadcast
  - AppleTalk (procedura collaborativa)
  - IPX [Novell] (assegnazione automatica)



Procedura AppleTalk

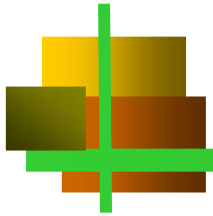
Ogni nodo AppleTalk ha un suo node ID

All'avvio un nodo AppleTalk prende un ID a caso

Il nodo trasmette ripetutamente in broadcast dei pacchetti di inquiry per determinare se un altro nodo sta già usando lo stesso node ID

Se nessun altro nodo risponde prima di un tempo limite, il nodo in fase di avvio assume come suo il node ID di tentativo

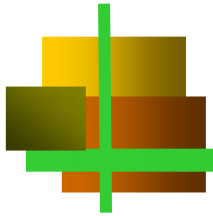
In caso di riposta il nodo incrementa il valore di ID e riprende il processo di inquiry



Procedura Novell IPX

Procedura semplice ed automatica

Indirizzo di rete Novell IPX generato dall'unione del network address (Netware Network ID number) e dal MAC address



Predecessori del DHCP

Necessità di meccanismi server-based

Primo RFC del DHCP: 1531 (Oct 1993)

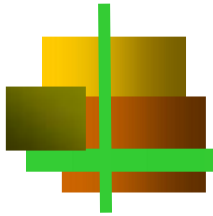
In precedenza:

- RARP
- ICMP
- BOOTP
- DRARP
- TFTP
- NIP
- .....

RARP

- Reverse Address Resolution Protocol (RARP) fornisce solo IP address
- RARP realizzato nello stesso modo di ARP (stesso formato di pacchetto)
- Differenza essenziale: *sistema server based*
- Altre diversità: *opcode* e *protocol*
- L'host invia in broadcast una RARP request con il suo MAC address
- Il server cerca il MAC address nella sua tabella
- Il server risponde con l'IP address dell'host

Il client ed il server devono essere nella stessa subnet



RARP (2)

Limiti di RARP:

Serve soltanto gli host noti al server

Fornisce soltanto l'IP address

Funziona staticamente

Arricchimenti possibili:

Dopo l'ottenimento dell'IP address tramite RARP, utilizzare TFTP per acquisire dal server altre informazioni di configurazione

Soluzione SUN

Altra possibilità: Dynamic RARP (DRARP) RFC 1931

ICMP

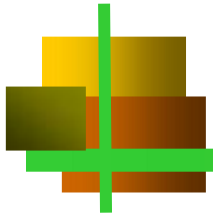
Più che un sistema diverso un arricchimento di RARP

Due funzioni:

- Reperimento della subnet mask
- Determinazione del gateway di default

Sequenza delle operazioni:

1. Invio in broadcast di una request RARP
2. Estrazione dell'IP address dalla risposta RARP
3. Invio in broadcast di una richiesta ICMP per la subnet mask
4. Estrazione della subnet mask da un replay ICMP
5. Invio in broadcast di una richiesta per il gateway
6. Estrazione dell'IP address del gateway da un replay ICMP



BOOTP

BOOTstrap Protocol - RFC 951 (Sept 1985)

Meccanismo di tipo client-server

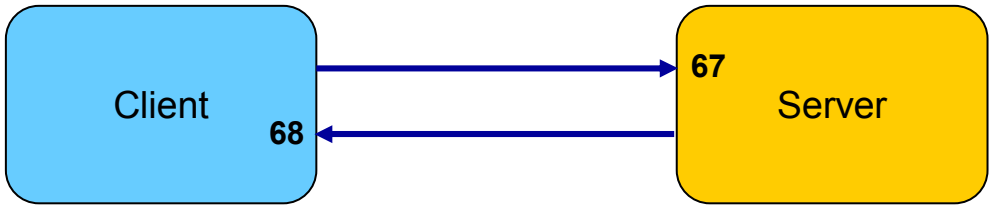
BOOTP basato su UDP

Client trasmette in broadcast BOOTREQUEST
con il MAC address

Server trasmette in broadcast BOOTREPLY
con IP address

BOOTP (2)

Uso di well-known port nei due sensi



Limited Broadcast Address 255.255.255.255

BOOTP fornisce al client diversi parametri: IP address, Subnet mask, gateway, servers, posizione del boot file, etc

BOOTP meccanismo statico
il client deve essere presente nel database del server prima di BOOTREQUEST

BOOTP (3)

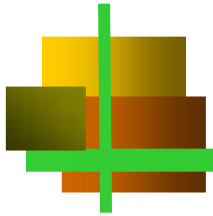
BOOTP forwarding

Avere un server BOOTP per ogni subnet oneroso

Relay agent BOOTP ascoltano BOOTREQUEST

Relay agent inoltrano le BOOTREQUEST ad unico server

Relay agent ritrasmettono le BOOTREPLY verso i client



Standard DHCP

DHCP oggi definito nella RFC 2131 (March 1997)

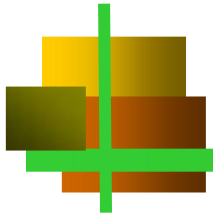
Dynamic Host Configuration Protocol

Nello stato di *Draft Standard*

Options di DHCP definite nella RFC 2132

DHCP Options and BOOTP Vendor Extensions

Nello stato di *Draft Standard*



DHCP e BOOTP

DHCP costruito a partire da BOOTP, con aggiunte:

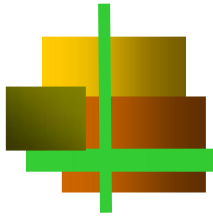
- Riallocazione automatica degli IP address riutilizzabili
- Opzioni aggiuntive e più ricche

DHCP fornisce tutti i parametri di configurazione di cui alla RFC 1122 *Requirements for Internet Hosts*
BOOTP solo una parte

Vendor extensions di BOOTP divengono *Options* di DHCP e passano da 64 a 312 bit

DHCP può accettare richieste da client BOOTP

DHCP usa il message format di BOOTP



DHCP components

DHCP costituito da due parti:

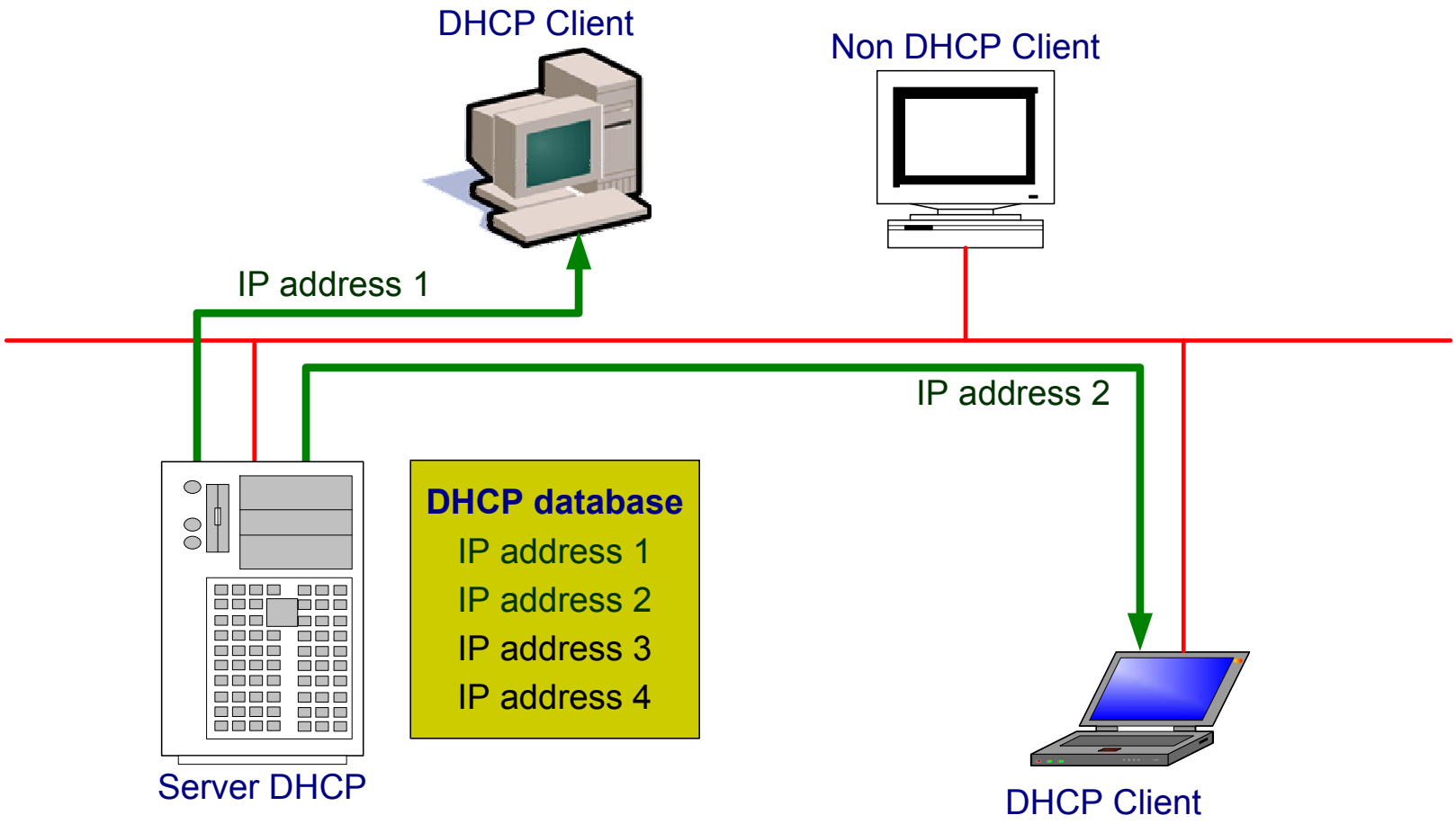
- Un protocollo per la richiesta e la consegna agli host dei parametri di configurazione

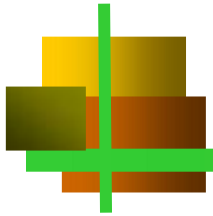
- Un meccanismo per la allocazione degli IP address agli host

  Protocollo standardizzato

  Meccanismo proprietario ed interno all'applicativo del server

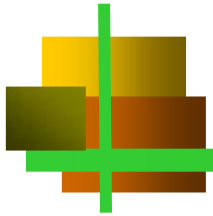
Architettura Client-Server





Servizi del DHCP

- Deposito dei parametri di configurazione dei diversi client
- Allocazione dinamica degli IP address
- Fornitura dei network parameters



Configuration parameters storage

Un host che invia una richiesta può mettere un suo *client ID*

Diversamente il client ID è fornito dal server
(IP-subnet-number, hardware addres)

Nel server database con entry il *client ID*
e valori dei parametri di rete

Il client può richiedere la ritrasmissione dei parametri avuti

IP address dynamic allocation

DHCP alloca address temporanei o permanenti

Un client all'avvio richiede un IP address

Opzionalmente può richiederlo per un periodo di tempo

Il server attribuisce al client un IP address per un
Tempo scelto in base alla sua policy ed alla richiesta

Periodo di tempo per DHCP = lease

IP address dynamic allocation (2)

Server assegna in IP address per un *lease-time*

Server garantisce di non dare ad altri client
un address già impegnato

Ogni volta che un client richiede un IP address il
server tenta di ridargli quello precedente

Client prima della scadenza del lease-time
può chiedere una estensione del lease

Client può richiedere un lease per un
tempo qualsiasi (anche infinito)

Server attribuisce il lease-time in base alla sua policy

IP address dynamic allocation (3)

3 policy per l'assegnazione del lease-time

- Dinamica (normale)
- Permanente (richiesta di ∞)
  [se consentita]
- Fixed (in base a preregistrazione)

Colloquio Client-Server

Tutti i messaggi scambiati tra client, server ed agent DHCP (e BOOTP) hanno lo stesso format

Nell'ipotesi più semplice

Al boot un host configurato come client DHCP invia in broadcast un messaggio DHCPDISCOVER

I server DHCP rispondono con un messaggio DHCPOFFER

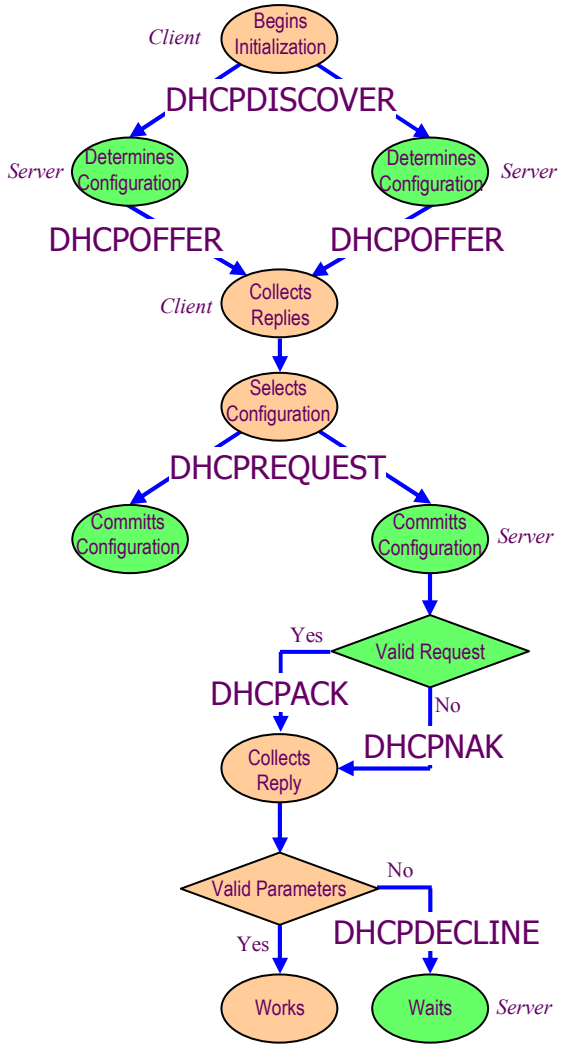
Il client trasmette un DHCPREQUEST con cui accetta l'offerta di un server

Il server risponde con un messaggio DHCPACK con cui fornisce i parametri

Colloquio Client-Server (2)

Realtà più complessa

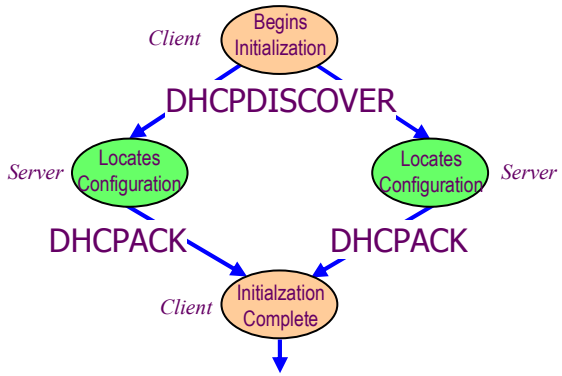
Messaggi scambiati nell'allocazione di un nuovo IP address



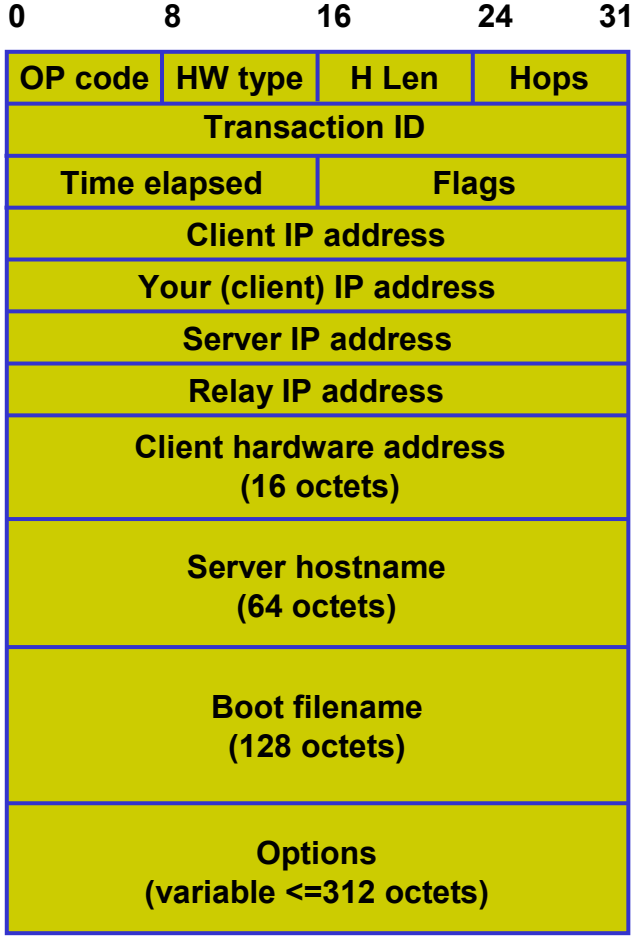
Server diversi operano su spazi di address differenti

Colloquio Client-Server (3)

Messaggi scambiati nell'allocazione di un IP address già usato



DHCP message format

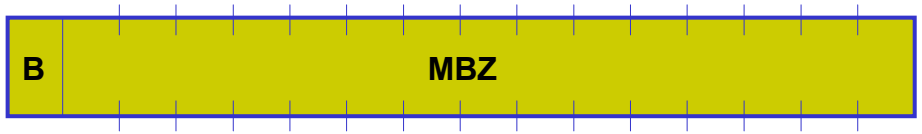


Tutti i messaggi con lo stesso format

OP code	1	BOOTREQUEST
	2	BOOTREPLY
HW type	6	IEEE 802
	11	LocalTalk
	..	.....
HLEN		Hardware address length
HOPS		Used only for relay agents
Transaction ID		Random number from client
Time elapsed		Time since init of process

DHCP message format (2)

Flags



Set only by client

B Broadcast flag

MBZ Must Be Zero

Client IP address

Set by client

If it unknows IP address is set to 0.0.0.0

DHCP message format (3)

Your (client) IP address	Client address set by the server if the received client IP address was 0.0.0.0
Server IP address	IP address set by the server
Relay IP address	IP address of relay agent if it is used
Client hardware address	Set by the client
Server host name	Optional server host name terminated by X'00'

DHCP message format (4)

Boot file name

generic o null in DHCPDISCOVER,
fqdn in DHCPOFFER

Options

Campo contenente un numero variabile di options

Primi quattro bytes contengono
il magic cookie 99.130.83.99

Option formate da: Code, Length e Data

Code	Length	Data

Code e Length 1 octet, Data variabile

Options

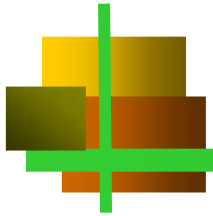
Length = Lunghezza in ottetti del campo Data

Due option "0" e "255" formate dal solo Code

Sempre presente l'option 53 "DHCP message type"

Option 53

Value	Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM
9	DHCPFORCERENEW



Interazione Client-Server

Ogni server DHCP ha un pool di IP address che può concedere.

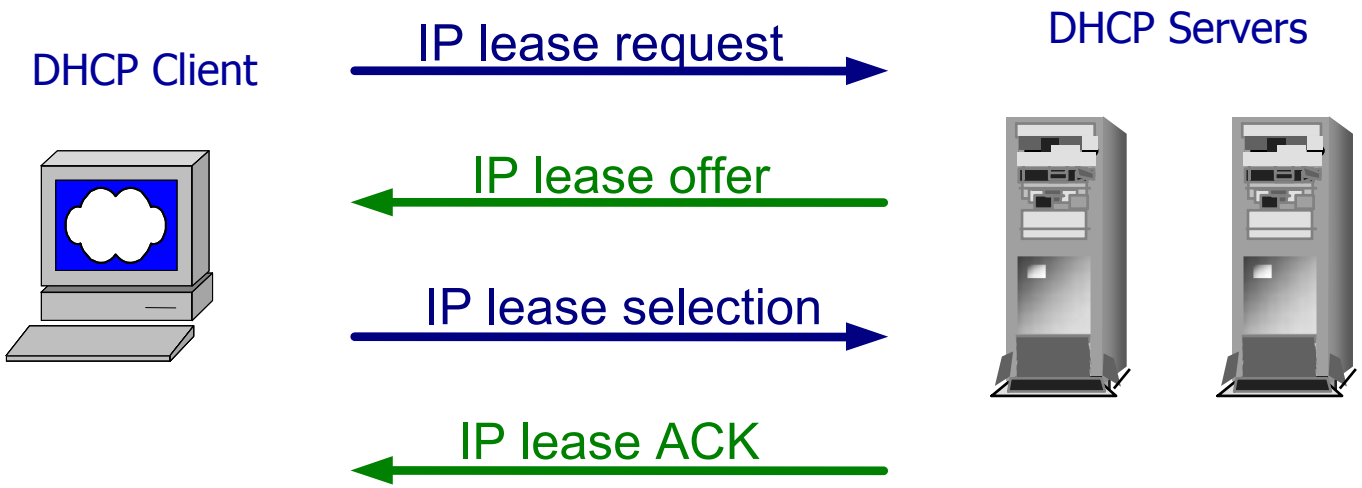
Ogni address viene concesso ad un client per un tempo (lease time) fissato dalla policy del server

Ogni server DHCP gestisce un database degli address concessi e dei lease time

Il client trasmette in broadcast un messaggio DHCPDISCOVER

Nel messaggio DHCPDISCOVER possono essere poste delle options come durata del lease, network address, etc

Interazione Client-Server (2)



Timers

Ricordiamo: Server DHCP trasmette in DHCPOFFER il lease time

DHCP client riceve il DHCPOFFER e il DHCPACK ed in base

al Lease time e alla sua implementazione, stabilisce:

Renewal time T1

Allo scadere di T1 il client trasmette al server DHCP in unicast un DHCPREQUEST con la richiesta di estendere il lease.
Se riceve un ACK i timer sono resettati e si calcola il nuovo lease expiration time.

Rebinding time T2

Se il client non riceve un DHCPACK, allora allo scadere di T2 trasmette in broadcast un DHCPREQUEST con la richiesta di estendere il lease.
Se riceve un ACK (anche da un server differente) i timer sono resettati e si calcola il nuovo lease expiration time.

Se il client non riceve un DHCPACK, allora al termine del lease ritorna allo stato iniziale.

Timers (2)

T1 e T2 configurabili dal server tramite options

In ogni modo:

T1 < T2 < Lease time

Tipicamente:

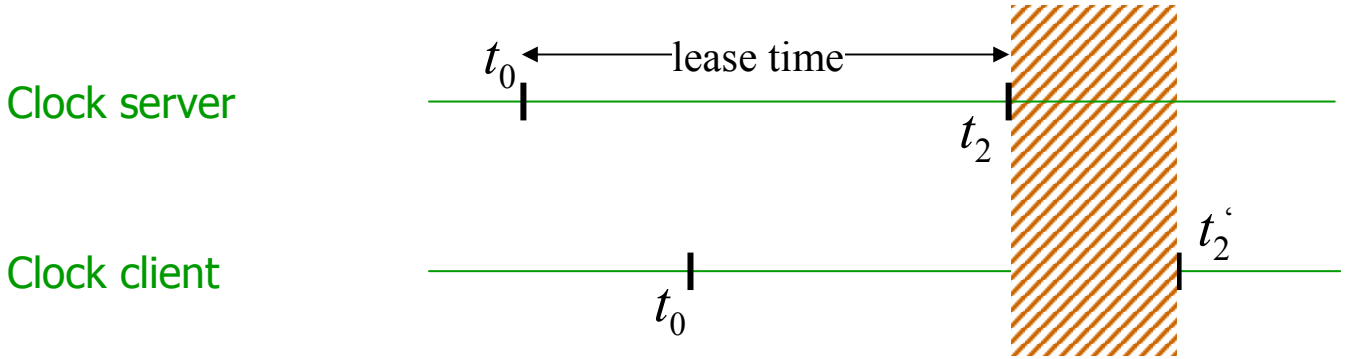
T1 = 0,5*Lease time

T2 = 0,875*Lease time

Sincronizzazione

Generalmente clock dei client e dei server non sincroni

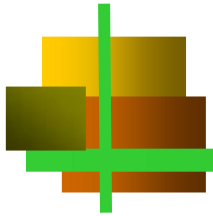
Possibilità di sfasamenti temporali



Soluzione: Tempi rappresentati come valori relativi

DHCP Messages

DHCPDISCOVER	c → s	b	To locate available servers
DHCPREQUEST	c → s	u	a) Requesting offered parameters form one server b) Confirming correctness of allocated address c) Extending the lease on a network address
DHCPDECLINE	c → s	u	Indication of IP addres already in use
DHCPRELEASE	c → s	u	Relinquishing IP address and cancelling lease
DHCPINFORM	c → s	u	Asking for local configuration parameters
DHCPOFFER	s → c	u	In response to DHCPDISCOVER with offer of configuration parameters
DHCPACK	s → c	u	Configuration parameters including IP address
DHCPNAK	s → c	u	Indication of incorrect request



Tipi di interazione

3 tipi di interazione client - server

Allocazione di un nuovo network address

Riuso di un network address precedentemente allocato

Ottenimento di parametri con network address configurato dall'esterno

Diagramma di stato client

Allocazione di un nuovo network address

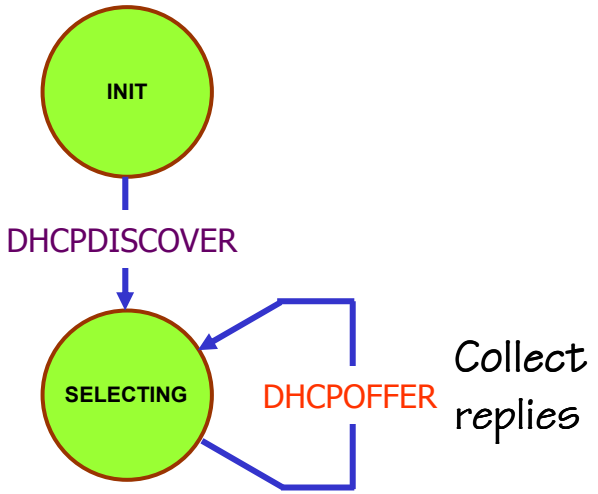


Diagramma di stato client

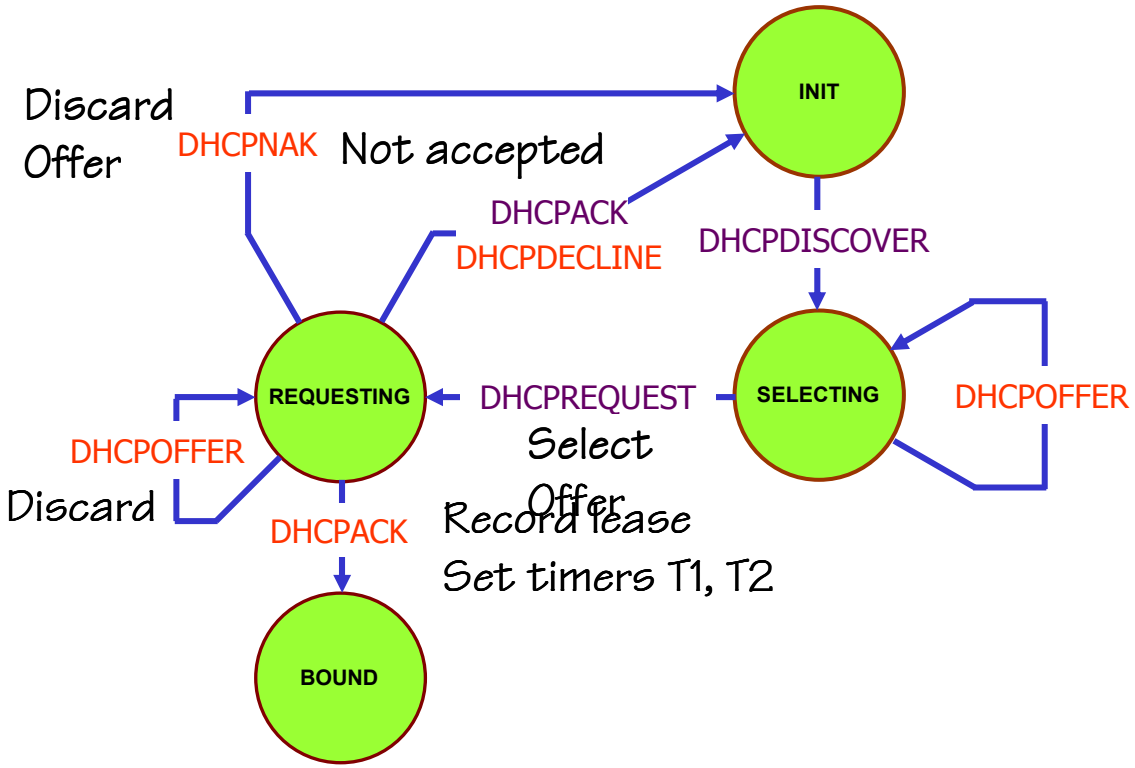


Diagramma di stato client

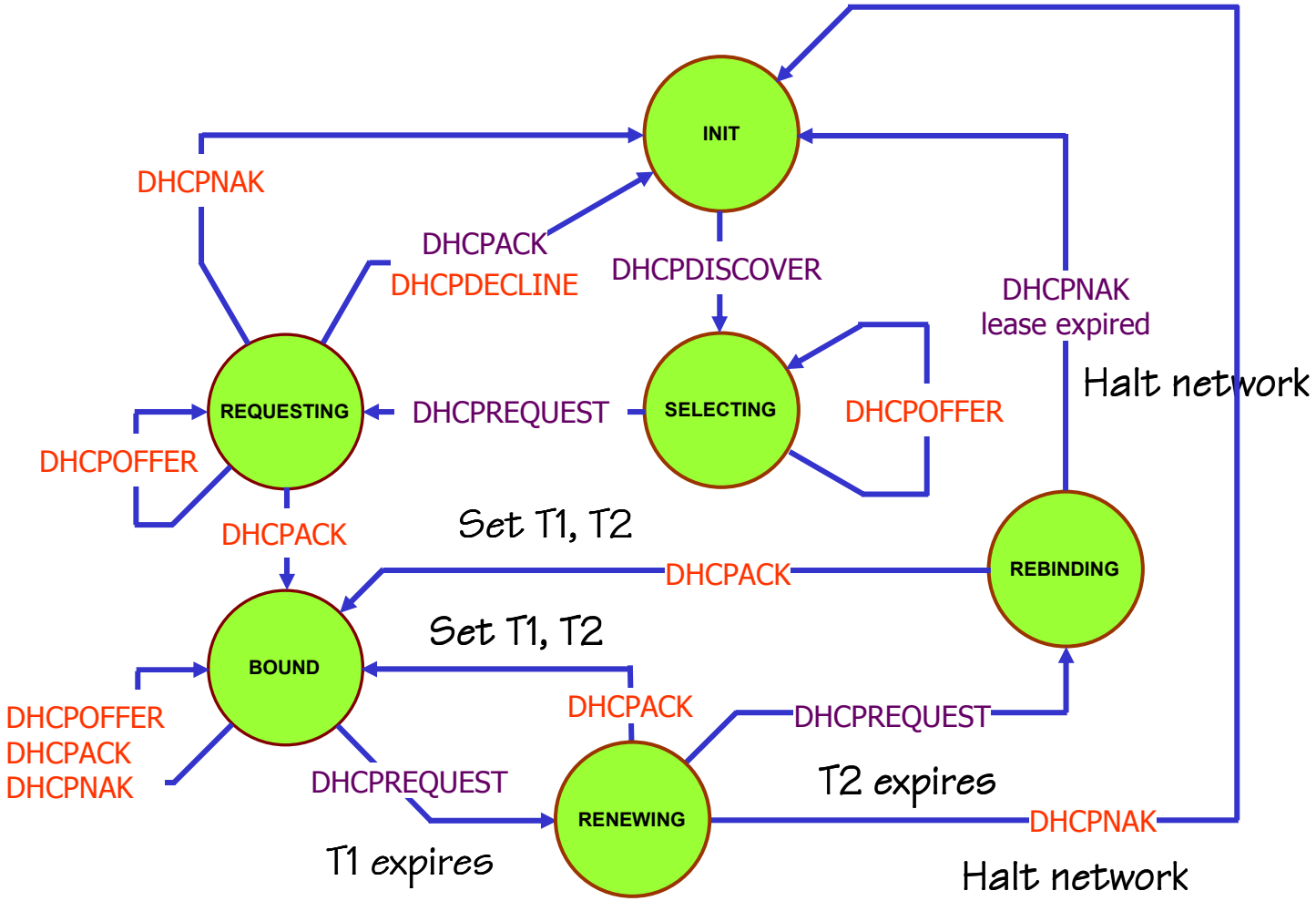


Diagramma di stato client

Inizializzazione con indirizzi di rete noti

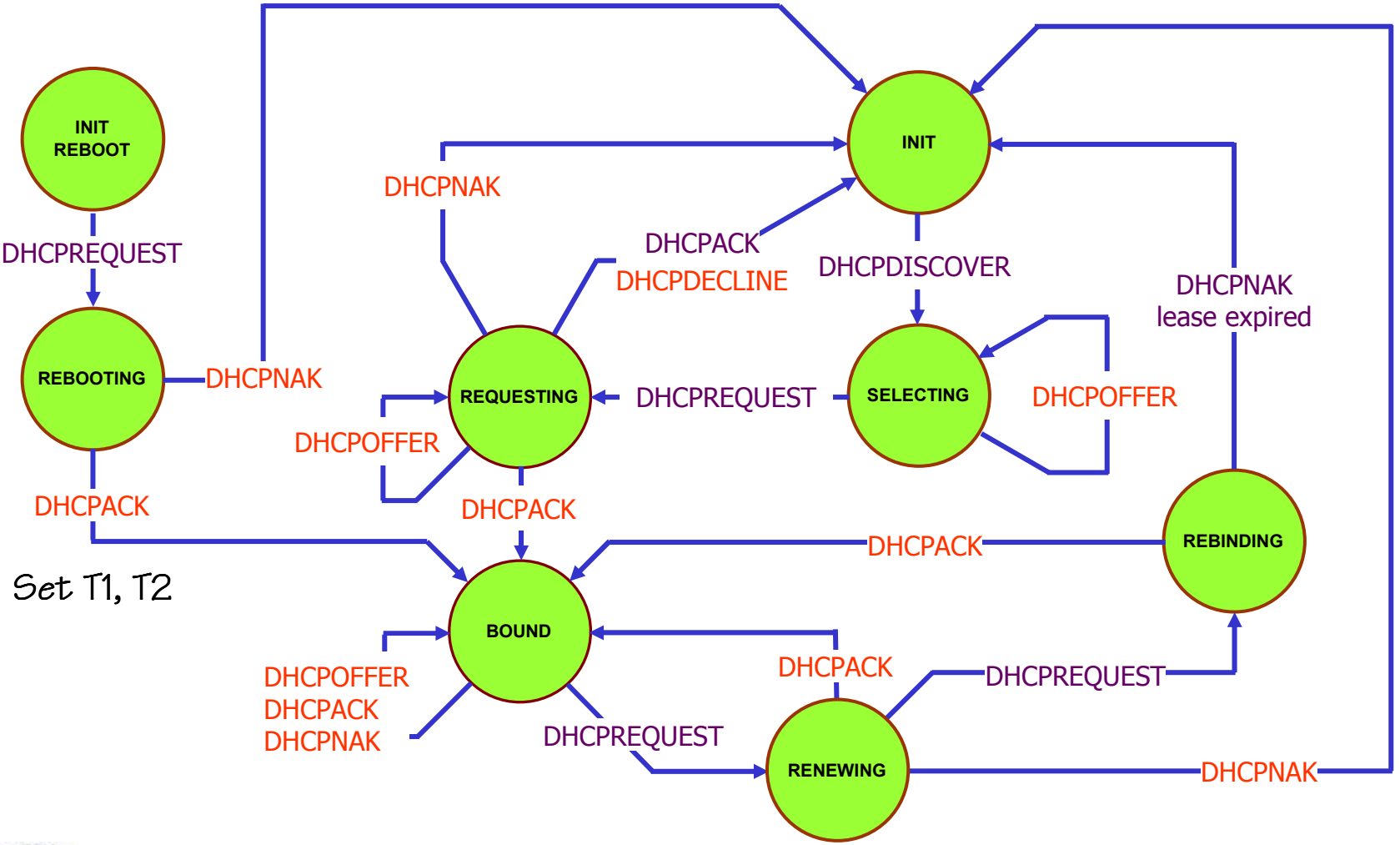


Diagramma di stato client

Ottenimento di parametri per host con IP address configurato manualmente

Tipico per server mission-critical e grandi sistemi

Client trasmette DHCPINFORM con suo IP address

Trasmissione broadcast o unicast

Option "parameter request list"

Server può rispondere con DHCPACK

Se nessun DHCPACK in tempo ragionevole (tip. 60 sec)
messaggio all'user e inizio con valori di default

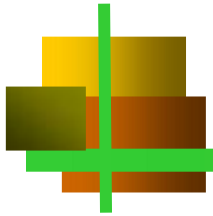
Altri messaggi

DHCPFORCENEW

Messaggio trasmesso dal server verso un client senza richiesta del client.
Client risponde con DHCPREQUEST con successiva fornitura di un nuovo address

DHCPLEASEQUERY

Messaggio trasmesso da un dispositivo o da un'applicazione verso il server
Server risponde con DHCPACK con dati del lease



Relay agent

Un client tenta di scoprire i server con il messaggio DHCPDISCOVER

Messaggio DHCPDISCOVER trasmesso in broadcast

Pacchetti broadcast non possono uscire dalla subnet

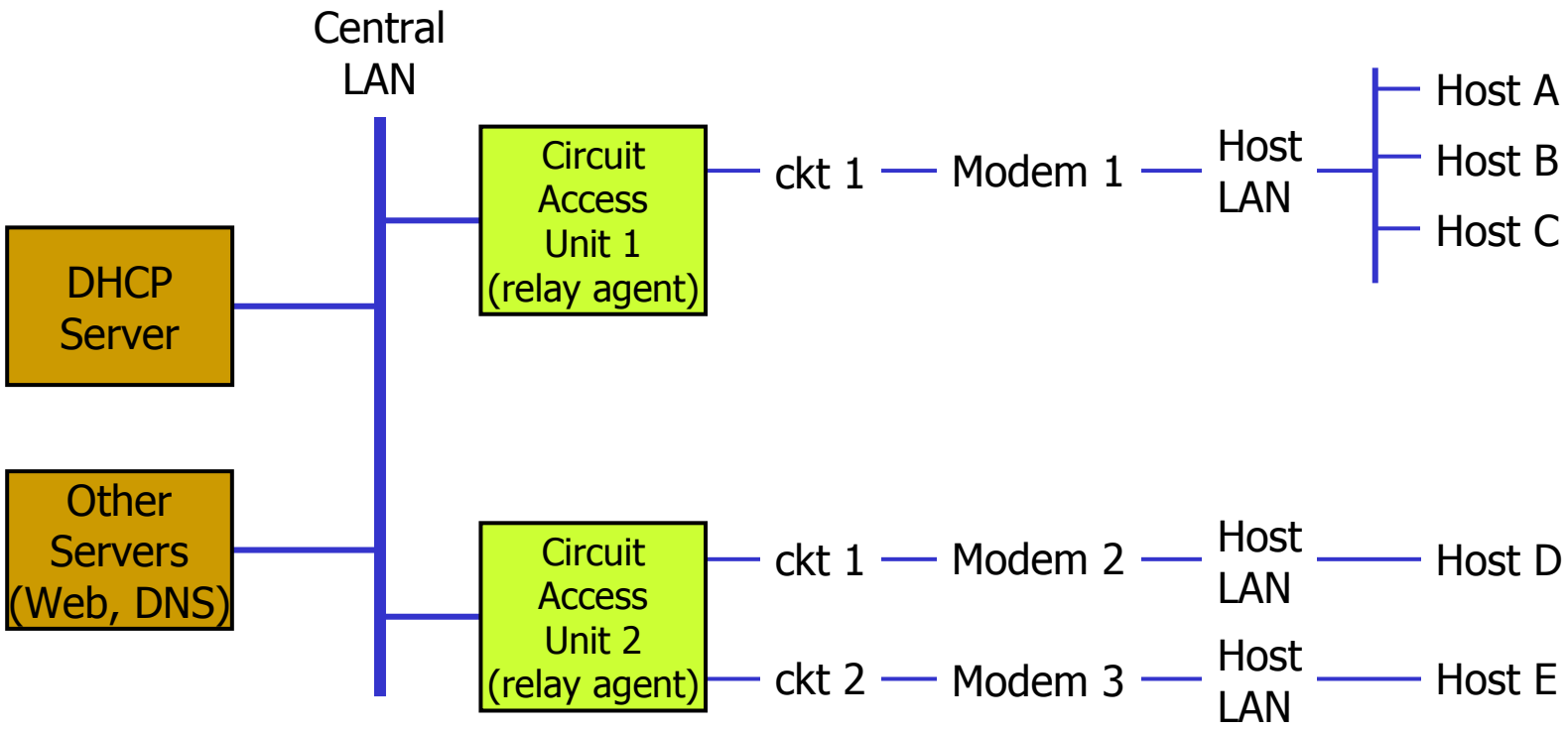
Risultato: Il server DHCP si dovrebbe trovare nella subnet da servire

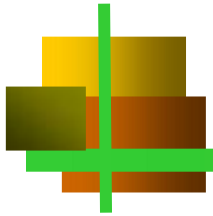
In tanti casi molte subnet con pochi host

Esempio tipico: LAN di utente connesse tramite linee ADSL ad una LAN centrale

Realy agent (2)

Soluzione: Un relay agent sulla subnet che fa il forwarding dei messaggi verso il server centrale





Relay agent (3)

Il relay agent deve conoscere l'IP address del server DHCP

Il relay agent riceve sulla porta 68 i messaggi broadcast trasmessi dal client

Il relay agent riempie il campo "Relay IP address" con il proprio address

Il relay agent converte i messaggi broadcast in arrivo in messaggi unicast diretti al server

Il server pone l'IP address per il client nel campo "Client IP address"

Il server ritorna il reply non al client ma al relay agent

Il relay agent inoltra il messaggio al client

Authenticated DHCP messages

Possibilità di minacce al server ed ai client DHCP

Minacce interne

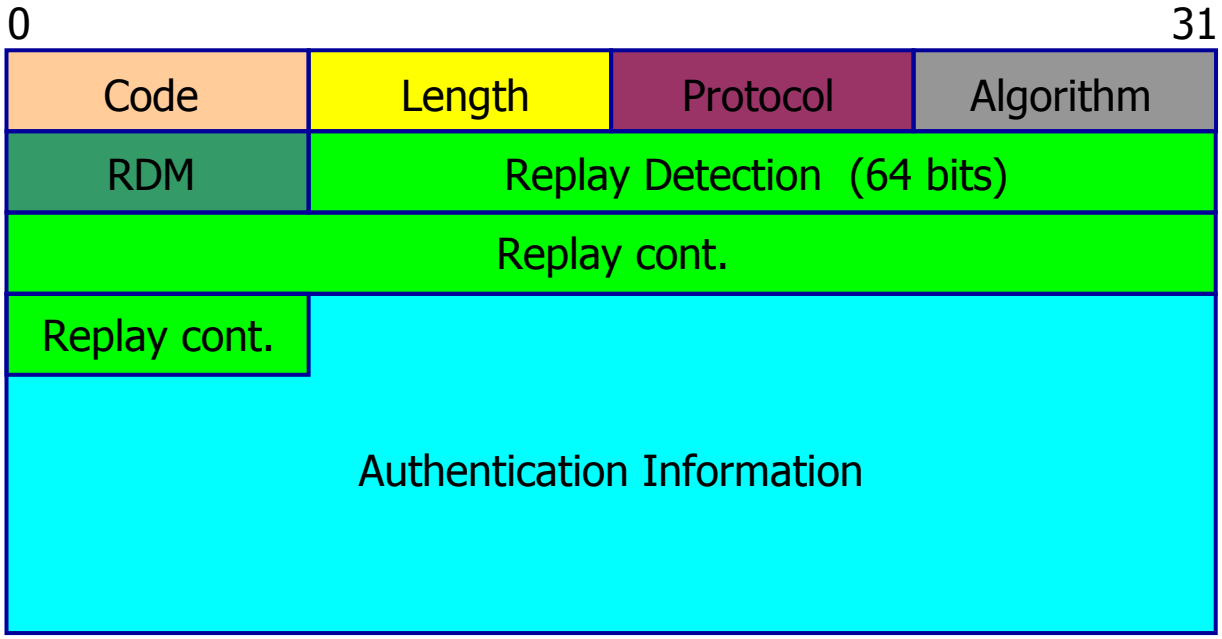
RFC 3118 – Authentication for DHCP Messages (June 2001)

Metodo di autenticazione e validazione nei due sensi

RFC 3118 definisce:

- Option di autenticazione
- Meccanismo di autenticazione

Authentication option



Code = 90

Length = Length in octets – 2 (code, length)

Authentication option (2)

Protocol = [Authentication token (0) – Delayed authentication (1)]

Algorithm = Definisce algoritmo all'interno del protocollo

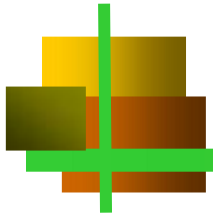
Oggi: 0 per authentication token
1 per delayed authentication

RDM = Replay Detection Method

Oggi: 0 per counter crescente

Replay Detection = Informazione usata per rivelare una risposta

Authentication Information - Variabile con protocollo ed algoritmo



Protocolli

Authentication Token

Estremamente semplice,
non realizza autenticazione di messaggio,
incapace di resistere ad un attacco

Praticamente non utilizzato

Delayed Authentication

Protocollo che effettua l'autenticazione
della sorgente e del messaggio.
Può usare diversi algoritmi, oggi solo HMAC-MD5

Oggi utilizzato

Delayed Authentication

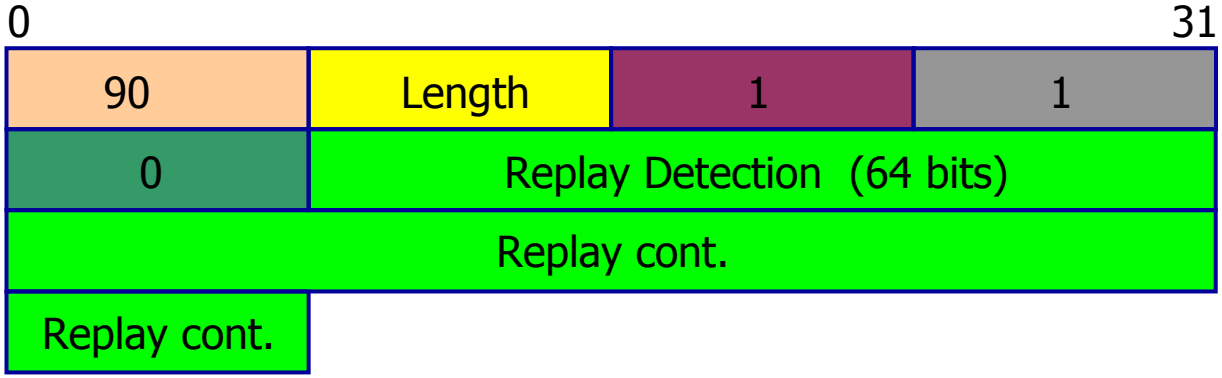
Ciascun client possiede una propria chiave K (secret)

Ogni secret ha un identificatore unico (secret ID) da 32 bit

Il server possiede le chiavi di tutti client autorizzati

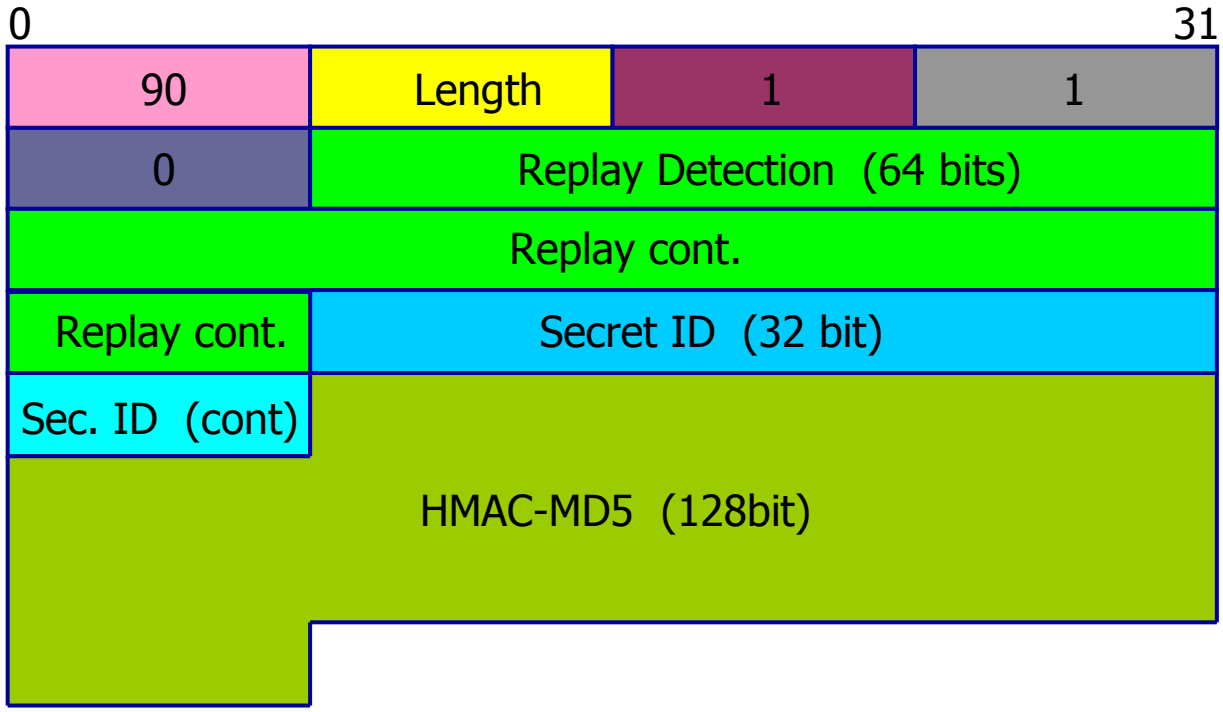
Le chiavi devono essere distribuite tramite un meccanismo esterno

L'host che inizia la procedura richiede l'autenticazione



Delayed Autentication (2)

I messaggi successivi a quello di inizio sono autenticati fornendo il secret ID ed una firma codificata con la chiave



Delayed Autentication (3)

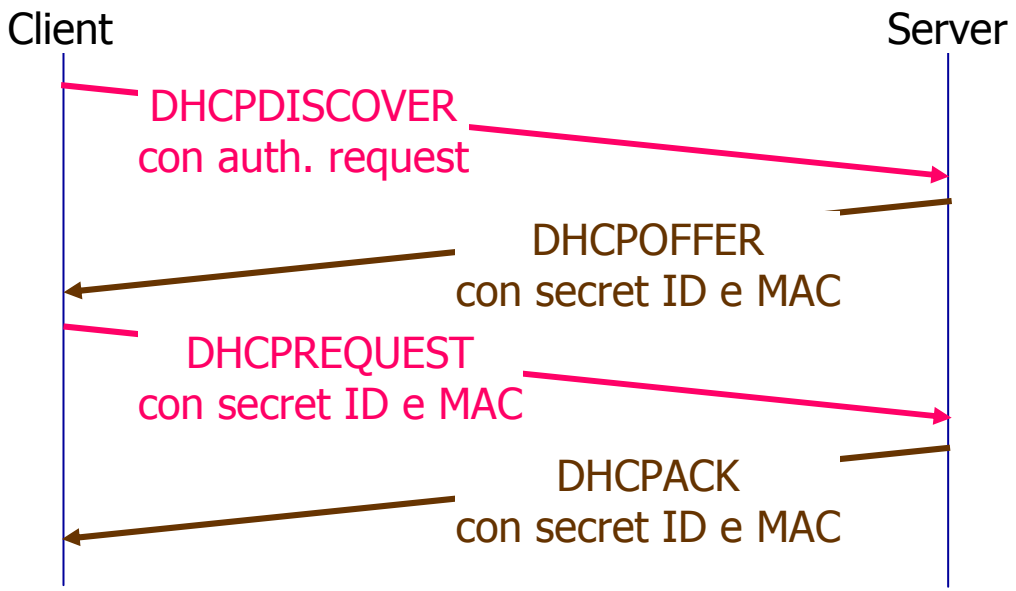
Il destinatario del messaggio, individua con il secret ID la chiave K e calcola con il messaggio e la chiave K il Message Authenticaction Code

Se il MAC è uguale a quello ricevuto il messaggio è accettato, diversamente viene scartato

Nei messaggi successivi viene usata lo stesso protocollo con identica chiave

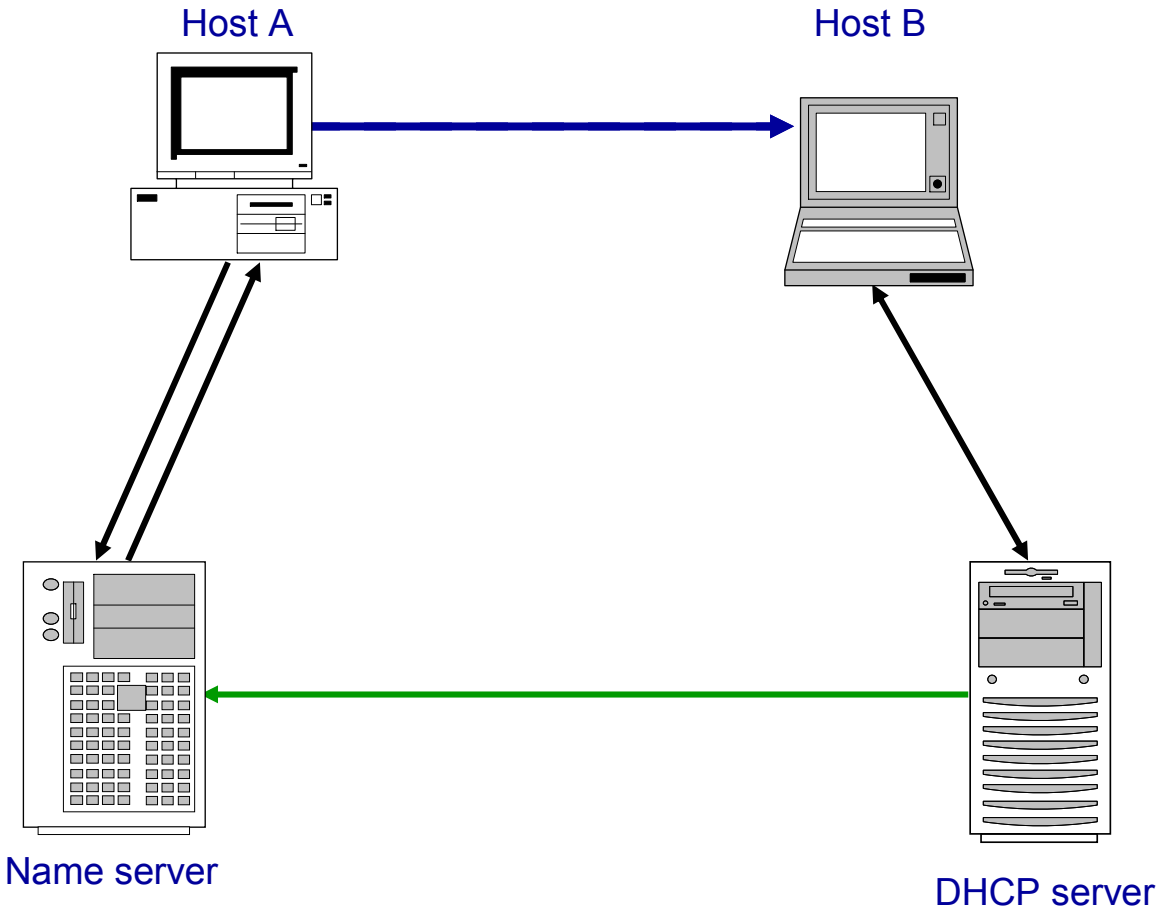
Controllo di identità e di originalità del messaggio

Delayed Autentication (4)

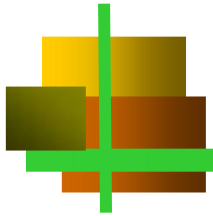


Svantaggio del protocollo: Non è scalabile.

Interazione DHCP - DNS



RFC 2136 – "Dynamic Updates in the Domain Name System", (April 1997)



Interazione DHCP – DNS (2)

Gravissimo pericolo nella possibilità di update del DNS

Operazione fattibile solo in presenza di autenticazione e validazione

Con autenticazione il server DHCP si autentica nei confronti del server DNS

Con validazione si controlla che i dati trasmessi non siano stati alterati

Oggi due procedure standardizzate: TSIG e DNSSEC

INTERAZIONE DHCP – DNS (3)

Dopo ogni variazione nei suoi leases il server DHCP compie dynamic update della zona del primary master server

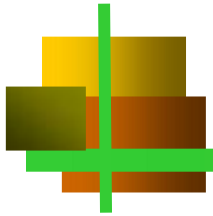
Risultato: Database del primary master server sempre updated

Primary master server con ogni update subisce cambiamento del serial number

Primary master server compie notify verso i suoi slave

Slave chiedono zone transfer al primary master server

Tutti i DNS sono updated



Multiserver e Failover

Un client trasmette in broadcast un messaggio DHCPDIDCOVER

Più server possono rispondere

In RFC 2131 nessuna interazione tra server

Ogni server deve gestire un pool di address differente

Se un server (o il link verso di esso) va in down nessun altro può gestire il lease

Più recentemente "DHCP Failover Protocol"

Multiserver e Failover (2)

Oggi: draft-ietf-dhc-failover-12.txt

Fini:

- Aumentare l'affidabilità nel caso di guasti
- Load balancing

Collaborazione tra una coppia di server (basata su una connessione TCP)

Sincronizzazione dei database mantenuti dai server

Quando un server va in down un client può essere servito dall'altro

Multiserver e Failover (3)

Pool di address suddiviso tra i due server

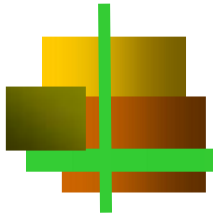
Una parte di address (free addresses) al primary server

Una parte di address (backup addresses) al secondary server

Tecnica *lazy updates* Tre principi:

- Il primary server gestisce i free address ed il secondary i backup
- Un server può estendere il lease soltanto per un periodo limitato oltre quello noto all'altro server
- Un address assegnato ad un client non può essere assegnato ad un'altro senza accordo tra i server

Nel caso di squilibrio del carico tra i server, si ripartiscono l'address pool



DHCP e IPv6

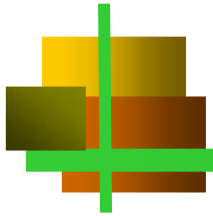
DHCP in effetti DHCPv4

DHCPv4 incompatibile con IPv6

IPv6 (address autoconfiguration) diminuisce la necessità del servizio DHCP

DHCP non fornisce soltanto IP address - quindi sempre utile

DHCPv6 può fornire più IP address per interface



Server DHCP

Oggi 3 server DHCP principali

Internet Software Consortium (ISC)

Free, Piene prestazioni, Text database

Microsoft (part of Windows 2000 Server)

Pagamento, Prestazioni limitate, Facilità d'uso

Nominum

Pagamento, Piene prestazioni, Relational database