Il principale protocollo usato per la configurazione degli host è il DHCP (Dynamic Host Configuration Protocol). Per la gestione della rete si usa invece il protocollo SNMP (Simple Network Management Protocol).

Il DHCP

Quando nelle reti si diffusero la tecnologia wireless e l'uso di computer portatili, in ambito IETF fu definito il protocollo DHCP (Dynamic Host Configuration Protocol), la cui specifica si trova in RFC 2131.

Tramite DHCP, oltre all'indirizzo IP, un host può ricevere altri parametri di configurazione:

- subnet mask
- default gateway: per esempio l'indirizzo IP del router che connette la subnet alla rete Internet. A questo sono inviati i pacchetti IP aventi indirizzo di rete del destinatario diverso da quello del mittente
- DNS Server preferito
- DNS Server alternativo

Configurazione Modalità

L'amministratore di rete può configurare, per ogni subnet e per ogni host, la modalità con cui il DHCP Server risponderà alle richieste dei client scegliendo fra 3 diversi tipi di configurazione.

- Configurazione manuale: è possibile assegnare un indirizzo IP specifico a un host, inserendolo manualmente nel DHCP Server; di regola si utilizza per macchine come router e server che si trovano stabilmente in una rete o per host che necessitano di un indirizzo permanente
- Configurazione automatica: il DHCP Server assegna in modo automatico un indirizzo IP permanente a ogni host che si collega alla rete (si differenzia dalla configurazione dinamica per l'assenza del tempo di lease)
- Configurazione dinamica: il DHCP Server assegna un indirizzo IP a un host per un tempo limitato (tempo di lease) in base alla lease length policy stabilita. Allo scadere del tempo di lease il client può richiederne il rinnovo o richiedere l'assegnazione di un nuovo indirizzo

L'Architettura Client Server DHCP

Un solo DHCP Server è solitamente in grado di soddisfare le esigenze operative relative all'assegnazione degli indirizzi IP e al setting dei parametri di configurazione sui client della rete locale. In condizioni normali il carico che deriva da queste attività non è particolarmente pesante.

Un DHCP Server può anche essere configurato per servire più subnet, per due scopi:

- fault-tolerance: per cui in genere è opportuno inserire un secondo DHCP Server come backup, così da mantenere il servizio sempre attivo
- bilanciamento del carico di lavoro: così da diminuire i tempi di risposta del server. In tal caso, alla richiesta di un client per l'assegnazione di un indirizzo IP possono rispondere più di un DHCP Server

Quando un DHCP Server è responsabile dell'indirizzamento su una subnet diversa dalla propria è necessario introdurre un relay agent (agente di ritrasmissione), ossia una macchina che non è né un server né un client, ma svolge un ruolo di intermediario occupandosi di facilitare la comunicazione tra client e server attraverso più reti.

La Comunicazione tra DHCP Client e DHCP Server

I messaggi di trasporto tra DHCP Client e DHCP Server sono di due tipi: richieste (request) e risposte (reply). Il protocollo di trasporto utilizzato è UDP e utilizza le porte 67 per il server e 68 per il client.

Il Pacchetto DHCP

- op (operation code)
- htype (hardware type)
- hlen (Hardware address length)
- hops (Hops count)
- Transaction ID (xid)
- Seconds (secs)
- Flags (flags)
- Client IP address (ciaddr)
- 'Your' (client) IP address (yiaddr)
- Server IP address (siaddr)
- Gateway IP address (giaddr)

- Client hardware address (chaddr)
- Server host name (sname)
- Boot file name (file)
- Options

Assegnazione degli Indirizzi

La comunicazione tra il nuovo host e il server, al fine di ottenere i dati per la configurazione di rete, avviene in 4 fasi:

1. Ricerca del DHCP Server: quando un nuovo host si connette alla rete, per ottenere un IP, invia un messaggio di broadcast chiamato DHCP Discover. Questo messaggio viene inviato a tutti i dispositivi sulla rete locale, perché l'host non conosce ancora l'indirizzo del server DHCP che possa assegnargli una configurazione IP
2. Offerta al DHCP Client: quando il server DHCP riceve il messaggio di Discover, risponde con un messaggio chiamato DHCP Offer che contiene una proposta di configurazione per il client: un indirizzo IP disponibile, la subnet mask, il gateway, i DNS e altre informazioni utili
3. Richiesta al DHCP Server: dopo aver ricevuto le offerte, il client sceglie una delle proposte e invia un messaggio chiamato DHCP Request, con cui il client comunica al server DHCP che ha accettato l'offerta. Anche questo messaggio è un broadcast, così che anche gli altri server DHCP sappiano che la loro offerta è stata rifiutata
4. Conferma al DHCP Client: infine, il server DHCP riceve la richiesta e risponde con un messaggio chiamato DHCP ACK, con cui il server conferma l'assegnazione dell'indirizzo IP al client e ribadisce tutte le informazioni necessarie per la configurazione della rete

Problematiche di Sicurezza

Il DHCP utilizza i protocolli UDP e IP che sono intrinsecamente insicuri. Sono due i principali problemi di sicurezza:

- DHCP Server non autorizzati: un DHCP Server abusivo potrebbe inserirsi e inibire gli host o configurarli per azioni fraudolente
- DHCP Client non autorizzati: un host potrebbe danneggiare la rete, oppure esaurire gli indirizzi a disposizione e bloccare nuovi accessi

Per ovviare al problema si possono implementare meccanismi di sicurezza ai livelli più bassi, inoltre si potrebbe usare IPsec per rendere sicuro il livello Network.

Il DNS

Il DNS consente agli utenti della rete di usare dei nomi al posto dell'indirizzo IP. È un database distribuito usato dagli applicativi del TCP/IP per il mapping tra nomi e indirizzi IP. Il DNS è formato da 3 componenti principali:

- Domain Name Space, specifica la struttura ad albero dei nomi di dominio ed è suddiviso in 3 tipi di domini:
  - domini radice
  - domini intermedi
  - domini foglia
- Name Server, un processo applicativo con il ruolo di server che contiene informazioni su alcune parti del Name Space chiamate zone
- Resolver, un programma con il ruolo di client che ottiene informazioni dal Name Server

Come Funziona il DNS

L'albero gerarchico del DNS è realizzato mediante base di dati distribuita, cosa che garantisce il funzionamento della rete. Se tutte le informazioni fossero memorizzate su un unico server e questo si guastasse si fermerebbe infatti tutta la rete Internet.

Lo spazio dei nomi del DNS è stato suddiviso in zone disgiunte, ognuna con un Name Server principale (DNS primario) e dei Name Server secondari (DNS secondario) che attingono al principale.

I client che accedono ai Name Server sono i resolver. Se il Resource Record è authoritative per la zona richiesta, il DNS Server risponderà direttamente, in caso contrario farà una ricerca nello spazio dei nomi. Questo processo si chiama risoluzione dei nomi.

Problematiche di Sicurezza del DNS

Il DNS dal punto di vista della sicurezza è critico sotto vari punti di vista:

- non è autenticato: l'informazione richiesta potrebbe arrivare non dal DNS Server corretto ma da un'altra macchina
- è molto lento, quindi è possibile che qualcuno intercetti la richiesta destinata a un DNS Server e risponda al suo posto (spoofing)
- non offre meccanismi per proteggere l'integrità delle informazioni distribuite

Proprio per il ruolo critico che il DNS ricopre nell'internet, l'ICANN ha evidenziato la necessità di stabilire metriche e modalità per il controllo del DNS, individuando 5 indicatori importanti: coerenza, integrità, velocità, disponibilità e robustezza