PROTOCOLLI DI GESTIONE IP: ICMP, ARP, RARP, DHCP. IL PROTOCOLLO NAT

Questi protocolli non vengono utilizzati per il trasporto di dati. Al più possono essere definiti 'protocolli di servizio'.

PROTOCOLLO ARP (ADDRESS RESOLUTION PROTOCOL).

Quando si deve inviare un messaggio su una rete tra un dispositivo mittente ed un dispositivo destinatario, questi dispositivi sono identificati sulla rete dall'indirizzo IP che, come sappiamo, è un indirizzo logico (individua il nodo della rete ma non il dispositivo). Per individuare il dispositivo a cui è destinato il messaggio si deve conoscere l'indirizzo MAC: ricordiamo, infatti, che il livello 2 della pila ISO/OSI gestisce la comunicazione tra nodi a livello di MAC address. Il protocollo ARP serve allo scopo, ossia: noto l'indirizzo IP, individua sulla rete il Mac address del dispositivo a cui è stato assegnato l'indirizzo IP e lo comunica al dispositivo mittente che lo memorizza in una tabella interna, chiamata proprio Tabella ARP *(per visualizzare il contenuto di questa tabella dopo aver digitato il comando **cmd** – prompt dei comandi - nella sezione cerca, nel pannello che compare, digitare **arp -a**)*. Questa tabella memorizza, in modo temporaneo e dinamico, tutti i dispositivi con i quali si è scambiato messaggi nella rete locale.

Quando, quindi, si deve inviare un messaggio tra due dispositivi, il dispositivo mittente deve inviare preliminarmente, conoscendo il solo indirizzo IP, una richiesta a tutti i dispositivi collegati, dell'indirizzo Mac del dispositivo destinatario di cui conosce il solo l'indirizzo IP: questa richiesta viene effettuata tramite il protocollo ARP. Il dispositivo destinatario, ricevuta la richiesta, risponde inviando il proprio indirizzo Mac che viene memorizzato nella tabella Arp del dispositivo mittente.

Ora, dopo questa fase esplorativa, il messaggio vero e proprio, che deve essere inviato al dispositivo destinatario, viene completato dall'indirizzo Mac di quest'ultimo così che la trasmissione risulta più veloce, soprattutto negli invii successivi di messaggi tra lo stesso dispositivo mittente e lo stesso dispositivo destinatario.

PROTOCOLLO ICMP (INTERNET CONTROL MESSAGE PROTOCOL).

Questo protocollo serve ai nodi di una rete (router-host/host-host) per scambiarsi informazioni riguardanti lo stato e messaggi di errore. È, ad esempio, il

protocollo che viene usato quando si effettua il PING per verificare, in una rete locale o pubblica, se un dispositivo host è collegato e può essere raggiunto.

Vediamo come è formato l'header del pacchetto ICMP (che viene incapsulato nel pacchetto IP).

L'header del ICMP è formato:

Type (8 bit)	Code (8 bit)	Checkum (16 bit)	Dati (32 bit)

In cui: ***Type*** individua il tipo di messaggio: errore o interrogazione. ***Code*** ulteriori informazioni sul messaggio di Type *x*, ***Checksum*** controllo dell'integrita del pacchetto ICMP (se durante la trasmissione il pacchetto ha subito degli errori).

PROTOCOLLO RARP (REVERSE ADDRESS RESOLUTION PROTOCOL).

Questo protocollo è in grado di effettuare l'operazione inversa del protocollo ARP. Ossia: dato il Mac address di un Host, restituisce l' indirizzo IP associato a quel Mac address. Questo protocollo non è più utilizzato in quanto è sostituito dal DHCP.

PROTOCOLLO DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

Questo protocollo semplifica il lavoro degli amministratori di rete in quanto permette di assegnare in modo automatico e dinamico indirizzi IP agli Host.

Come funziona il protocollo DHCP? Quando un dispositivo si collega a una rete, richiede un indirizzo IP tramite una richiesta DHCPDISCOVERY che contiene il proprio indirizzo fisico. La richiesta viene inviata al/ai server DHCP presente/ti sulla rete. Il/i server invia/no il proprio identificativo ed un una configurazione IP tramite un DHCPOFFER; l'Host riceve l'offerta e, se l'accetta, invia una DHCPREQUEST contenente l'identificativo del server DHCP (eventualmente scelto, nel caso sulla rete sono presenti più DHCP server); il server DHCP (scelto) invia all'Host che ha effettuato il DHCPREQUEST un messaggio di conferma - DHCPACK. Il rilascio di un indirizzo IP da parte di un client avviene tramite l'invio da parte di quast'ultimo di un messaggio DHCPRELEASE. Tutti i messaggi tra client e server DHCP vengono effettuati in broadcast.

Il protocollo DHCP prevede tre metodi di allocazione dell'indirizzo IP:

- **Allocazione dinamica**. L'allocazione dinamica avviene quando un amministratore riserva un certo numero di indirizzi IP (minori del numero di

client che ne fa richiesta) per il DHCP. Quindi, ogni client DHCP sulla rete locale richiede un IP dal server DHCP durante la fase di inizializzazione della rete. L'intero processo si svolge durante un periodo di tempo (timeout) controllabile che consente a un server DHCP di recuperare e riallocare (a timeout scaduto) un indirizzo IP non utilizzato: in questo caso, lo stesso indirizzo IP può essere riassegnato a un altro client.

- **Assegnazione automatica**. Un server DHCP assegna un indirizzo IP a un client in base alle regole stabilite in precedenza da un amministratore. Si differenzia dall'allocazione dinamica perché il server DHCP gestisce, in base alle regole stabilite dall'amministratore, una tabella in cui sono presenti gli indirizzi fisici dei client a cui corrispondono gli indirizzi IP da assegnare.
- **Assegnazione statica**. In questo caso, la tabella è gestita da un amministratore che assegna manualmente a ciascun client a un indirizzo IP. In questo modo si assegna lo stesso IP al medesimo client ogni volta che il client accede alla rete.

La configurazione IP offerta dal server DHCP al client comprende, oltre l'indirizzo IP, ulteriori parametri di configurazione.

I parametri DHCP di solito definiscono:

- un gateway predefinito che instrada i dati avanti e indietro tra la rete locale e Internet.
- Una subnet mask.
- Un server DNS che traduce i nomi degli indirizzi IP in nomi che le persone possono ricordare (es. www.google.it).

PROTOCOLLO NAT (NETWORK ADDRESS TRANSLATION)

Ormai le reti locali hanno assunto dimensioni consistenti ed utilizzano tutti i dispositivi che vengono utilizzate nelle reti più grandi tanto che possono essere paragonate a delle 'internet in miniatura' e che, spesso, vengono identificate con il termine 'intranet'. Queste intranet utilizzano tutti i servizi che di solito sono utilizzati nelle reti più grandi come servizi di posta elettronica, server WWW… Anche queste reti intranet utilizzano indirizzi IP per individuare un nodo nella rete: questi indirizzi IP vengono definiti 'privati'(*) con i quali, però, non è possibile navigare sulle reti pubbliche (internet): in quest'ultime vengono utilizzati, per l'appunto, indirizzi IP pubblici (univoci). Una rete privata è, generalmente, collegata alla rete pubblica tramite router, proxy e quant'altro. Ovviamente i problemi che si hanno quando una rete privata è connessa ad una rete pubblica sono:

- Problemi di sicurezza (come evitare 'ingressi' indesiderati nella rete privata o gestire l'accesso dalla rete privata alla rete pubblica);
- problemi di gestione degli indirizzi (come 'tradurre' gli indirizzi privati in pubblici in modo da consentire la navigazione nella rete pubblica);
- come differenziare i servizi offerti nella rete privata da quelli offerti dalla rete pubblica.

il problema che vogliamo affrontare in questo paragrafo è il secondo, ossia come tradurre gli indirizzi privati in pubblici e viceversa. Questo viene risolto utilizzando due dispositivi: server proxy o router NAT/router classici.

I Proxy verranno trattati successivamente. Concentriamoci sull'utilizzo su l'utilizzo dei router. Se utilizzo un router classico per connetere la intranet con internet, la intranet deve necessariamente utilizzare al suo interno IP pubblici (al router, infatti, non è consentito instradare un pacchetto proveniente dall'interno della intranet verso la rete pubblica, se l'IP è privato) ma questo comporta seri problemi di sicurezza (dalla rete pubblica tutti possono accedere a tutti i servizi ed host della rete intranet). I router NAT (o meglio che usano la 'tecnologia' NAT: Nat più che un protocollo è una vera e propria tecnologia) oltre ad assolvere tutte le funzionalità di un router classico, effettuano il mapping di un insieme di indirizzi IP privati provenienti dalla intranet con un insieme di IP pubblici ad essi assegnati. Ossia il NAT utilizza una tabella nella quale associa gli indirizzi privati agli indirizzi pubblici. La gestione di tale tabella può essere statica, in questo caso parliamo di ***NAT statico***, ossia l'associazione tra indirizzo IP privato e pubblico è non modificabile, o dinamica, in questo caso parliamo di ***NAT dinamico***, quando ad un host locale che fa una richiesta ad un server remoto, viene assegnato il primo indirizzo IP pubblico, gestito dal NAT del router, disponibile.

Oltre il Nat statico e Nat dinamico esistono altre due tipologie NAT: ***Port Forwarding*** e ***PAT (Port Address Translation)***.

Il router che utilizza il ***port forwarding***, indirizza i pacchetti provenienti da internet alla porta logica (indicata nel pacchetto) e non all'indirizzo IP del dispositivo presente nella intranet (questa tecnica è utilizzata quando nella rete privata sono presenti server 'pubblici' come, ad esempio, un server di posta elettronica che utilizza, come sappiamo, la porta 25).

Il Router che utilizza il ***PAT*** gestisce i socket di comunicazione tra un dispositivo (client) interno alla rete locale che ha chiesto un servizio ad un Server su rete pubblica. Siccome il socket contiene la porta logica sia del mttente (client) che del destinataro, l'associazione nella tabella NAT non è tra indirizzo IP privato ed IP

pubblico, ma tra la porta logica del dispositivo client e l'IP pubblico. In questo caso il PAT assegna ad ogni dispositivo presente nella rete privata un numero di porta logica diverso.

(*) gli indirizzi IP privati sono non univoci nel senso che due diverse reti locali possono assegnare lo stesso indirizzo IP a due nodi che appartengono uno ad una rete e l'altro all'altra; inoltre le classi di indirizzi IP vengono suddivise tra indirizzi pubblici ed indirizzi privati, precisamente:

Classe IP	**Range di Indirizzi IP privati utilizzabili**		
A	10.0.0.0	-	10.255.255.255
B	172.16.0.0	-	172.31.255.255
C	192.168.0.0	-	192.168.255.255