Protocolli ARP e RARP

Introduzione ai protocolli

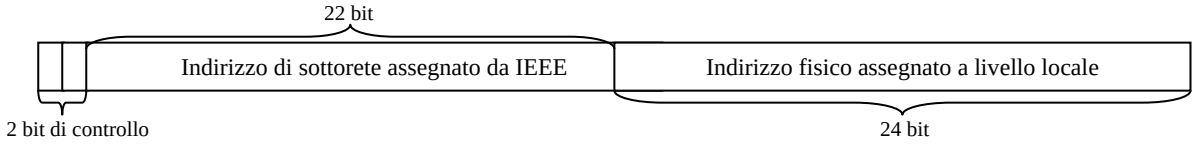
I protocolli che vedremo in questa sezione sono di fondamentale importanza per la comunicazione tra host.
E' importante sapere che non basta il semplice indirizzo IP per comunicare tra host. Quando da livello network scendiamo a livello datalink abbiamo bisogno di conoscere l'indirizzo hardware dell'host destinazione. Dobbiamo infatti ricordare che i pacchetti IP(livello rete) vengano "imbustati" all'interno di frame(livello datalink) per poi essere spediti su mezzo fisico. Naturalmente anche a livello datalink deve esistere una qualche forma di indirizzamento.
Gli indirizzi che vengono usati a livello 2 sono i cosiddetti MAC Address, ossia gli indirizzi fisici della nostra NIC (Network Interface Card, la scheda di rete).
Per capire tutto questo, poniamoci una semplice domanda: "Come fa un host A a comunicare con l'host B conoscendo unicamente l'indirizzo IP di B?".
Se il collegamento è point-to-point allora non ci sono problemi.
Se ci troviamo su una LAN sorge il problema di cui accennavo sopra:

- il pacchetto è destinato ad un host sulla rete: allora in questo caso qual è l'indirizzo datalink del nodo destinatario?
- il pacchetto è destinato al di fuori della rete: qual è allora l'indirizzo del router a livello datalink?

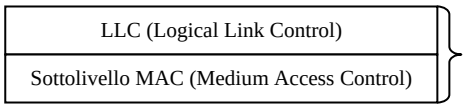
La risposta è: ATTRAVERSO IL PROTOCOLLO ARP (definito nell'RFC 826)!
Nonostante infatti dal punto di vista di programmatori/utenti siamo soliti vedere la comunicazione con un'atra macchina solamente mediante uno scambio di pacchetti che sfrutta gli indirizzi IP, la realtà è po' diversa.
Gli hardware di rete infatti per comunicare fra loro utilizzano degli indirizzi fisici che vengono codificati all'interno dell'hardware stesso.

Indirizzi fisici

Come dicevamo l'hardware di rete ha codificato sulla scheda d'interfaccia di rete un indirizzo fisico (hardware address). Questo indirizzo tipicamente è fisso, ma in casi particolari può essere modificato dall'utente mediante degli appositi software. Comunque la linea guida che la maggior parte dei produttori di schede seguono, è quella di impedire che l'indirizzo fisico possa essere modificato: solitamente infatti gli indirizzi sono memorizzati all'interno della PROM (Programmable Read-Only Memory) della scheda. Si tende ad adottare questa soluzione onde evitare che all'interno di una rete possa verificarsi che due scheda possano avere lo stesso MAC address.
La lunghezza dell'indirizzo hardware varia a seconda della tipologia di rete: ad esempio Ethernet (sarà il caso che considereremo noi) utilizza indirizzi di 48 bit.
Vediamo ora la struttura di un indirizzo hardware ethernet:



NOTA: Spesso quando ci si riferisce agli indirizzi fisici, si fa riferimento ad essi anche come MAC address: presto spiegato il perché. In sostanza il livello datalink si può dividere in due parti:



L'LLC è specificato dallo standard IEEE 802.2, mentre esempi di protocolli per il MAC sono l'IEEE 802.3 ossia quella che noi erroneamente chiamiamo Ethernet (in realtà si tratta del protocollo CSMA/CD); l'IEEE 802.4 o Token Bus (destinato alle LAN ad automazione industriale); l'IEEE 802.5 o Token Ring (rete ad anello originariamente progettata da IBM).
Concludiamo questa digressione accennando brevemente ai ruoli di MAC e LLC.
Il sottolivello MAC è utilizzato nelle reti di tipo broadcast (dove c'è un canale di comunicazione condiviso) per stabilire quale sia la prossima stazione abilitata a trasmettere. Il layer LLC serve per fornire una sorta di interfaccia al livello network nascondendo le varie differenze fra i sottolivelli MAC. I vari standard IEEE che abbiamo nominato sopra sono differenti fra loro sia dal punto di vista del livello fisico, sia dal punto di vista del sottolivello MAC, ma esiste compatibilità a livello datalink, fornita appunto dal layer LLC.
Va da sé che si è soliti chiamare l'indirizzo hardware come MAC address, proprio per la stretta interazione che c'è fra sottolivello MAC e livello fisico.

Dopo aver visto la struttura dell'indirizzo fisico (o MAC address) vediamo il significato dei vari campi di bit.

Il bit più a sx indica se (nel caso specifico) si tratta di "indirizzo individuale" (bit posto 0) o di "indirizzo di gruppo" (bit posto 1). Nota: nel caso questo bit sia posto a 1 tutte le stazioni di rete vengono considerate come destinatarie.
Il secondo bit U/L (Universal/Local) viene chiamato anche "bit locale" (bit a 1) o "bit universale" (bit a 0).
Un identificativo di rete assegnato a livello locale viene utilizzato unicamente all'interno di strutture LAN e WAN chiuse, perché si potrebbero avere grossi problemi di conflitti se l'indirizzo venisse passato ad altre reti (possibile indirizzo MAC duplicato).
I successivi 22 bits sono assegnati dall'IEEE, mentre gli 24 restanti sono assegnati e gestiti localmente dall'amministratore di rete.

I frame Ethernet
Diversi tipi di reti, significano anche diversi frame, ognuno dei quali con la propria struttura e la propria lunghezza.
Siccome il protocollo Ethernet è forse il più diffuso in ambito LAN, vedremo la struttura dei frame che circolano in una tipica rete Ethernet appunto.

Preambolo	Receiver Address	Sender Address	Tipo	Dati	CRC
64 bit	48 bit	48 bit	16 bit	Variabile	32 bit

Il preambolo viene utilizzato fondamentalmente per la sincronizzazione della comunicazione: al termine di esso (la parte finale) viene posta una particolare sequenza di bit detta SFD (Start Frame Delimiter) che indica l'inizio vero e prorpio del frame.
Receiver e Sender Address hanno dimensione di 48 bit per quanto abbiamo visto sopra, quando abbiamo parlato di indirizzi fisici. Il campo tipo serve per specificare quale protocollo viene utilizzato.
Il campo dati ha lunghezza variabile che va da 64 byte a 1500 byte. Se i dati sono meno di 64 byte, il campo viene riempito con bit 0 di padding.
Al termine del frame viene posizionato il checksum CRC (Cyclic Redundancy Check) per individuare eventuali errori di trasmissione nel frame stesso, e quindi se necessario scartarlo.
NOTA: frame Ethernet e frame del protocollo IEEE 802.3 non sono uguali, perchè alcuni campi cambiano di significato.

Protocollo ARP (Address Resolution Protocol)
Abbiamo già accennato nell'introduzione che quando ci troviamo in ambito LAN è necessario per poter inviare pacchetti-dati conoscere anche l'indirizzo fisico di una macchina. Non basta conoscere l'indirizzo IP utilizzato normalmente dalle applicazioni per rifersi ad un host. C'è necessità quindi di un meccanismo di traduzione IP Address→MAC Address.

Una corrispondenza tra indirizzi IP e indirizzi fisici potrebbe essere mantenuta, costruendo "manualmente" una tabella.
Tuttavia questa soluzione è troppo scomoda e non è praticamente mai adottata.
Il funzionamento di ARP prevede invece che venga mantenuta una cosiddetta *tabella ARP* in maniera dinamica, anche se è possibile inserire manualmente le voci. Oltre alla tabella ARP viene mantenuta una *cache ARP* in memoria in modo che gli indirizzi vengano dapprima ricercati in cache e poi eventualmente in tabella. Le voci dinamiche (presenti in cache) vengono cancellate dopo un timeout prestabilito, mentre eventuali entry statiche possono continuare a persistere in tabella.
Esempio di entry nella arp table.

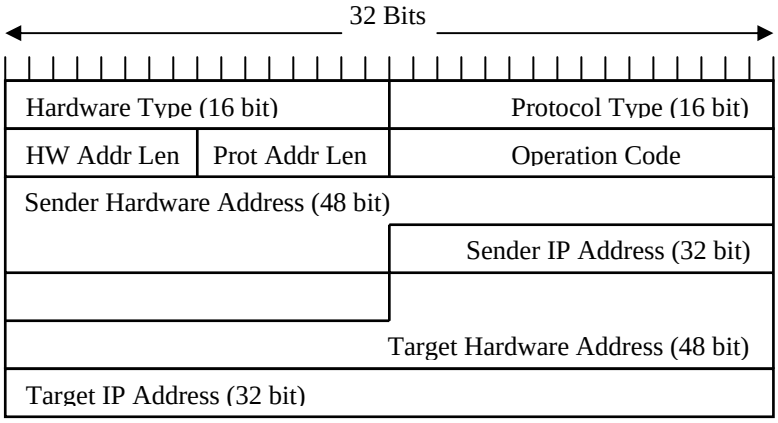
```
C:\Documents and Settings\Massimo>arp -a

Interfaccia: 0.0.0.0 --- 0x2
  Indirizzo Internet    Indirizzo fisico      Tipo
  127.0.0.1             00-e0-18-86-6c-09     statico
```

Ad ogni riga presente nella cache corrisponde un dispositivo per il quale sono mantenute le seguenti informazioni:
1. Indice Interfaccia (IF index): la porta fisica
2. Indirizzo fisico
3. Indirizzo IP
4. Tipo di entry

Per il tipo sono possibili quattro valori: 2 indica una entry non valida, 3 indica una mappatura dinamica e quindi un valore variabile, 4 indica una entry statica, 1 indica nessuno dei casi precedenti.

DOMANDA: Cosa succede quando ARP non trova in cache o nella tabella l'indirizzo IP dell'host di cui vuole sapere il MAC address?
RISPOSTA: Viene inviata in broadcast la cosiddetta *richiesta ARP* che una forma del tipo "Qual è il MAC address dell'host che ha indirizzo ip 192.168.0.12?".
Nel caso l'host interessato riconosca il proprio ip come argomento della richiesta, allora risponderà inviando al mittente il proprio indirizzo fisico. Una volta ricevute, queste informazioni vengono inserite nella cache e nella tabella arp.

Struttura di un ARP packet
Vediamo ora qual è la struttura di un pacchetto ARP (richieste e risposte).



Vediamo ora il significato dei vari campi.

- HARDWARE TYPE: indica il tipo di interfaccia hardware. Tra i vari valori possibili ricordiamoil valore 1 che indica Ethernet.
- PROTOCOL TYPE: indica il tipo di protocollo impiegato dall'interfaccia mittente. Esempi: 2054 per ARP, 32821 per RARP, 2048 per IP.
- HARDWARE ADDRESS LENGTH: indica la lunghezza dell'indirizzo fisico.
- PROTOCOL ADDRESS LENGTH: lunghezza dell'indirizzo utilizzato a livello superiore (es. indirizzo IP).
- OPERATION CODE: indica se si tratta di una risposta (valore 2) o una richiesta (valore 1).
- SENDER HARDWARE ADDRESS: indirizzo fisico dell'interfaccia mittente.
- SENDER IP ADDRESS: indirizzo IP dell'interfaccia mittente.
- TARGET HARDWARE ADDRESS: indirizzo fisico dell'interfaccia ricevente.
- TARGET IP ADDRESS: indirizzo IP dell'interfaccia ricevente.

Alcune considerazioni su ARP
Osservando la struttura di un arp packet può sorgere la seguente domanda: "Che senso può avere inviare in una richiesta anche il MAC address del mittente?". Presto detto: il ricevente dovrà rispondere a questa interrogazione, però per farlo ha bisogno anche lui di sapere l'indirizzo fisico del mittente. In questa maniera si evita che anche il ricevente invii una richiesta arp in broadcast.
Un'altra possibile ottimizzazione richiede che una volta inizializzato, un host invii in broadcast la propria coppia <Indirizzo IP, Indirizzo Ethernet> sotto forma di arp-request con argomento il proprio indirizzo IP.
Lo scopo di tutto ciò è verificare eventuali problemi di indirizzi IP duplicati. Se si ottiene una risposta questo significa appunto che a due macchine differenti è stato assegnato lo stesso IP. L'host che invia questa "strana" richiesta dovrebbe eventualmente preoccuparsi di segnalare l'anomalia all'amministratore di sistema e bloccare il proprio funzionamento.
Anche se nella maggior parte dei casi non si ottiene risposta a questa particolare arp-request, l'utilità di questa operazione sta nel fatto che una volta inviata questa request iniziale, tutti gli host sulla rete avranno una nuova entry nella propria cache ARP.

DOMANDA: "Cosa succede quando l'IP di destinazione non appartiene alla rete su cui si trova l'host mittente?".
RISPOSTA: L'uso del protocollo ARP non funziona poiché la richiesta broadcast viene bloccata dal router (non viene inoltrato il traffico broadcast a livello Ethernet) e non può quindi raggiungere la rete su cui è presente l'host con l'IP destinatario. Esistono però due modi di agire.

1. Meccanismo ***PROXY ARP***: si tratta di utilizzare una sorta di protocollo arp-modificato. Il gateway interposto fra le due reti (es: il router) mantiene una tabella "mista" in cui compaiono sia entry di una rete sia entry dell'altra. Il gateway è quindi configurato per essere in grado di risolvere le richieste ARP su più reti locali. In

questa maniera nella tabella dell'host mittente si creerà una registrazione del tipo: <IP_Destinazione, MAC_Address_Gateway>.

2. L'host mittente è in grado di riconoscere immediatamente che l'host non sta sulla propria rete, e sa già che deve inviare tutto il traffico verso il default gateway (es: il router di cui parlavamo sopra). I frame vengono quindi indirizzati usando indirizzo fisico del gateway predefinito.

In ambo i casi cmq si capisce come il pacchetto IP venga inserito in un frame che è indirizzato al gateway. Il router/gateway provvede poi a rimuovere il pacchetto dal frame e cerca l'IP destinatario fra le proprie tabella di routing, individuando in ogni caso il prossimo router lungo il percorso. Questa operazione se necessario viene ripetuta più volte. Quando arriva sul router collegato alla rete a cui appartiene l'IP di destinazione, viene ricercato l'indirizzo fisico dell'host di destinazione o eventualmente viene fatta un'arp-request. Fatto questo il pacchetto IP viene finalmente imbustato in un frame che ha come indirizzo fisico quello dell'host destinatario.

Protocollo RARP (Reverse Address Resolution Protocol)

Le specifiche del protocollo possono essere trovate nell'RFC 903.
Come dice il nome stesso questo protocollo ha funzioni esattamente opposte a quelle di ARP. Dato un indirizzo fisico si preoccupa di individuare l'indirizzo IP corrispondente.
Situazioni tipiche in cui si rende necessaria questo tipo di risoluzione riguardano per lo più i sistemi diskless.
Il problema si presenta al momento dell'accensione di questi tipi di host: l'immagine binaria del sistema operativo infatti viene ricevuta da un file server remoto e caricata in memoria. Queste workstation non dispongono di archivi locali e le volte in cui dispongono di disco, non lo usano per mantenere parametri relativi alle configurazioni TCP/IP ma solamente per velocizzare le operazioni del sistema operativo o per mantenere un'area locale di swap.
L'unica informazione di cui sono certe è il proprio indirizzo fisico. Ecco perché mandano in broadcast una richiesta rarp in cui indica il proprio mac address richiedendo il proprio indirizzo IP. Non tutti gli host sulla rete possono rispondere ad una richiesta del genere, ma solamente quegli host che fungono da server RARP (primari o secondari). Un server RARP infatti mantiene dei file di configurazione in cui sono presenti delle entry che mettono in relazioni indirizzo fisico e indirizzo ip. L'host richiedente terrà in considerazione unicamente la prima risposta proveniente da un server rarp e scarterà tutte le successive.
Un domanda può sorgere spontanea: "Perché non inserire l'indirizzo ip della macchina in questione all'interno del file immagine del sistema operativo?". Il motivo è semplice: in questa maniera lo stesso file immagine può essere riutilizzato per tutte le macchine, in caso contrario si dovrebbe mantenere un file immagine per ogni differente macchina.
Il fatto che RARP utilizzi il meccanismo di broadcast (indirizzo di destinazione di tutti 1) significa che l'utilizzo è limitato all'interno di un segmento di rete (una sottorete). In sostanza questi messaggi non possono inoltrati dai router e di conseguenza c'è bisogno di avere almeno un server rarp per rete.
Una soluzione a questo inconveniente è stato raggiunta con l'invenzione del protocollo BOOTP, un protocollo di bootstrap alternativo. A differenza di RARP infatti BOOTP utilizza pacchetti UDP che vengono inoltrati dai router.
L'uso di questo protocollo inoltre permette di fornire ai sistemi diskless informazioni aggiuntive, quali IP del file server che mantiene l'immagine del sistema operativo, l'IP del default gateway e la subnet-mask da utilizzare.
Per ulteriori informazioni su BOOTP vedere l'RFC 951 (e anche le RFC 1048 e 1084).
Il protocollo RARP utilizza lo stesso formato dei pacchetti ARP con alcune variazioni nei valori che sono contenuti nei campi. Ad esempio il campo PROTOCOL_TYPE contiene il valore 32821 (che indica appunto il protocollo RARP).

Il fenomeno dell RARP storm

Può succedere che il server rarp non sia disponibile per varie ragioni: guasto hardware, failure del sistema operativo, interruzione del link etc.
Quando il server RARP è spento, per i client RARP (i sistemi diskless di cui parlavamo sopra) è impossibile avviarsi.
Oltre a questo inconveniente c'è anche il problema dell'incremento del traffico di rete: i client continuano nel tentativo di conoscere il proprio indirizzo IP creando così un massiccio traffico broadcast che appesantisce la rete.
Questo fenomeno è comunemente conosciuto come rarp storm.
Per questo motivo al fine di rendere più affidabile la disponibilità dei servizi RARP, si ricorre a più server RARP.
Costituendo un ambiente multiserver è possibile rendere decisamente affidabile il servizio. Onde evitare che più server rispondano alla stessa risposta, creando traffico di rete in surplus, l'architettura tipica prevede un server principale e altri server secondari (detti anche di backup). In questa maniera il server a rispondere sarà (in linea di massima) quello primario. Nel caso non lo faccia entro un determinato timeout il server di backup (o secondario) risponde alla richiesta, considerando quindi il server primario come spento (e inutilizzabile).
Un ulteriore miglioramento allo schema consiste nel fare in modo che i vari server secondari prima di rispondere attendano un tempo casuale: questo per evitare ancora una volta che tutti tentino di rispondere (sostiuendosi al server primario "spento").

NOTE AL DOCUMENTO

Fonti bibliografiche:

- Andrew S. Tanenbaum "RETI DI COMPUTER"
- Appunti del corso di Protocolli di Rete. Anno Accademico 2002/2003
- TCP/IP Tutto & Oltre

Autore del documento: sego

Informazioni di carattere generale: qualsiasi suggerimento o critica costruttiva è ben accetto. Se avete idee per migliorare il documento inviatemi pure una mail. La segnalazione di errori o disattenzioni è altresì ben accetta.

sego (owner/webmaster of the-skulls.com)
indirizzo di posta elettronica: sego@the-skulls.com
sito web di riferimento: http://www.the-skulls.com