Come funziona il protocollo ARP ?

Corso e Certificazione: Cisco CCNA

Ogni Host, per inviare un Pacchetto ad un nodo della stessa LAN con un certo indirizzo IP, deve incapsularlo in una Trama, ove scrivere il giusto MAC destinatario. Le coppie IP-MAC vengono mantenute (mapped) da ogni Host in **una tabella in RAM, detta "ARP table**" o "ARP cache" (dato che si svuota a tempo).

Come mostrato nel corso Cisco CCNA (cap 1-9.7 =, la **Tabella ARP** è solitamente **aggiornata** in **tre modi**:

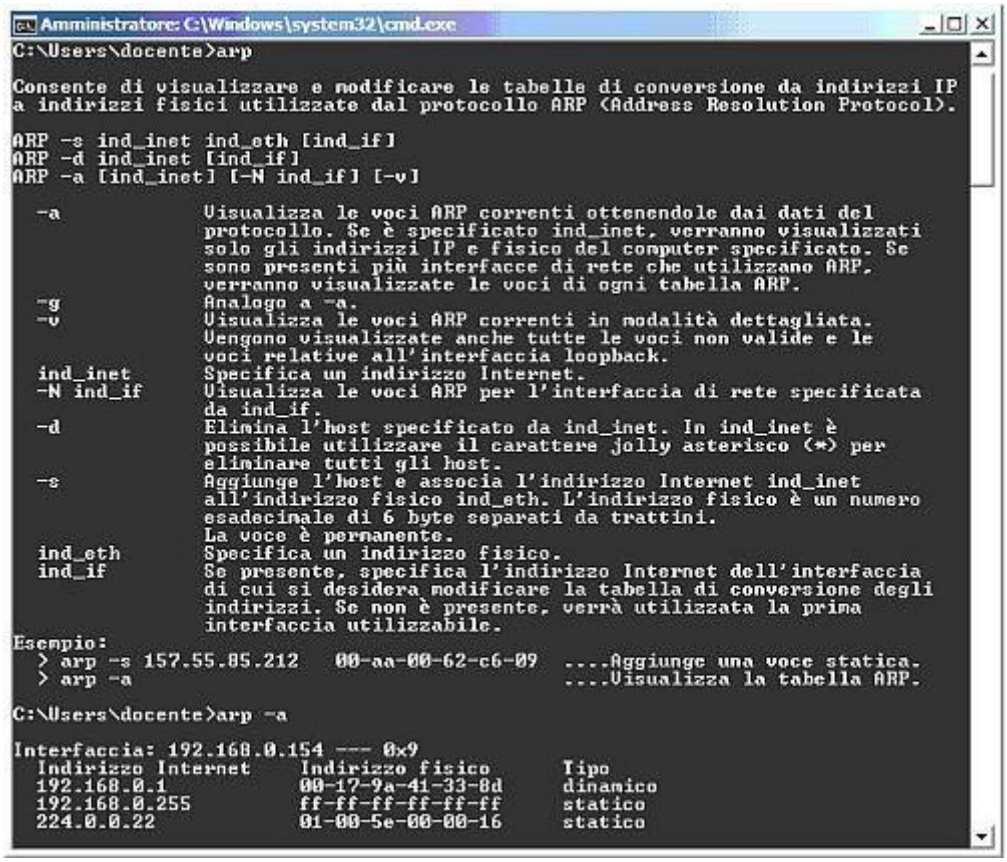
- monitorando il traffico di rete e prendendo nota degli IP e dei MAC delle Trame in transito
- emettendo in broadcast una "ARP request" che chiede a tutti gli Host della LAN chi abbia quel certo IP, e ricevendo in unicast, dall'Host interessato, la "ARP reply" con il suo MAC. Queste "entry" scadono, come quelle della "MAC table" degli Switch, di solito dopo 120"
- memorizzando una coppia IP-MAC configurata manualmente, che non scade mai: è raro.

Il modo normale per "**risolvere un IP in un MAC**", se non già presente in "ARP table" è il secondo; se l'IP interrogato non risponde, la Trama non può essere creata e il Pacchetto è scartato, avvisando dell'errore i livelli superiori dello "stack". Se il Pacchetto è scartato da un Router, questi può anche inviare un messaggio ICMP di notifica dell'errore al mittente remoto del Pacchetto stesso.

Se l'Host mittente deve inviare un **Pacchetto** ad un IP di una **rete diversa dalla propria** (cosa che si verifica confrontando il campo "network+subnet" del proprio IP con quelli dell'IP di destinazione) esso deve essere incapsulato per il "Default Gateway" della rete, configurato in modo statico o dinamico (da DHCP) tra i propri parametri di rete. Se il MAC del "Default Gateway" non è già in "ARP table", viene richiesto con una normale "ARP request" all'IP del Gateway stesso.

Come detto, le "entries" della "ARP table" vengono eliminate dopo un certo tempo di non utilizzo; tale tempo dipende dal Sistema Operativo, e va di solito dai 2' ai 10'.

Esiste in DOS il comando: arp con varie opzioni, per esaminare la "ARP table" e per eliminare una o tutte le "entries". Si noti che tale comando non lancia il protocollo, ma permette solo di accedere alla "ARP table": il protocollo è integrato nello "stack" TCP/IP, ed è del tutto trasparente.



Come spiegato nel corso Cisco CCNA, ci sono **un paio di problemi** potenzialmente associati al **protocollo ARP**:

- i broadcast sono ricevuti da tutti gli Host della rete; se un gruppo di nodi si avvia ed emette contemporaneamente molte "ARP request", la rete può soffrire dei rallentamenti temporanei
- inoltre, il protocollo ARP può essere oggetto di un attacco informatico, basato sul cosiddetto "ARP spoofing" (falsificazione dell'ARP) o "ARP poisoning" (avvelenamento dell'ARP). L'attaccante emette false "ARP *replies" (non "requests"!)* ed ottiene di dirottare (hijack) verso di sè Trame contenenti Pacchetti destinati ad altri IP.
  Per combattere questo attacco, un metodo è quello di configurare a mano la "ARP table", almeno per alcuni "devices" (Server) particolarmente importanti o riservati.

Esaminiamo il formato dei Pacchetti ARP e RARP:

Formato Pacchetto ARP

Il Pacchetto ARP, emesso da un PC che chiede in broadcast il MAC di un'altra macchina in rete, di cui conosce l'indirizzo IP, secondo la RFC 826 è così costituito (ogni riga è di 32 bit; si noti che questo è il "payload" della Trama, preceduto dall'Header di livello 2 e seguito dall'FCS):

Richiesta ARP

Tipo di interfaccia = 1		Prot. liv. 3 (IP) = 0x800
HLen.=48	PLen.=32	Op. (ARP request) = **1**
Prima parte MAC Sender SHA		
Seconda parte SHA		Prima p. IP Sender SPA
Seconda parte SPA		undefined
undefined		
IP Target TPA		

Risposta ARP

Tipo di interfaccia = 1		Prot. liv. 3 (IP) = 0x800
HLen.=48	PLen.=32	Op. (ARP reply) = **2**
Prima parte MAC Sender SHA		
Seconda parte SHA		Prima p. IP Sender SPA
Seconda parte SPA		**Pr. p. MAC Target THA**
Seconda parte MAC Target THA		
IP Target TPA		

N.B.: il MAC viene chiamato HA-Hardware Address, mentre l'IP è detto PA-Protocol Address; il prefisso S indica il mittente (Source), mentre T indica il destinatario (Target).
Nella Richiesta, il MAC cercato è ancora indefinito (in grigio); nella Risposta, tutti i Campi sono significativi, e il THA è il MAC richiesto, quello della macchina con IP = TPA.

Formato Pacchetto RARP

Un metodo dinamico per ottenere un IP, usato ad es. dalle "diskless workstation" (che non possono quindi memorizzarlo) è il RARP-Reverse Address Resolution Protocol. Esso è lanciato da un programma in ROM (BIOS), e richiede in broadcast al RARP Server, che deve essere presente in rete, di fornire l'IP associato al MAC del mittente. Il formato dei Pacchetti RARP di richiesta e risposta è molto simile a quello dell'ARP, e secondo la RFC 903 è il seguente:

Richiesta RARP

Tipo di interfaccia = 1		Prot. liv. 3 (IP) = 0x800
HLen.=48	PLen.=32	Op. (RARP request) = **3**
Prima parte MAC Sender SHA		
Seconda parte SHA		undefined
undefined		Pr. p. MAC Target THA
Seconda parte MAC Target THA (broadcast L2)		
undefined		

Risposta RARP

Tipo di interfaccia = 1		Prot. liv. 3 (IP) = 0x800
HLen.=48	PLen.=32	Op. (RARP reply) = **4**
Prima parte MAC Sender SHA		
Seconda parte SHA		**Prima p. IP Sender SPA**
Seconda parte SPA		Pr. p. MAC Target THA
Seconda parte MAC Target THA		
IP Target TPA		

N.B.: nella Richiesta, THA=FF FF FF FF FF FF (broadcast L2) e tutti gli IP sono indefiniti.
Nella Risposta, tutti i Campi sono significativi, e l'SPA è l'IP richiesto dalla workstation; nel campo "IP Target TPA" il Server RARP fornisce anche il proprio indirizzo IP, per eventuali usi futuri.