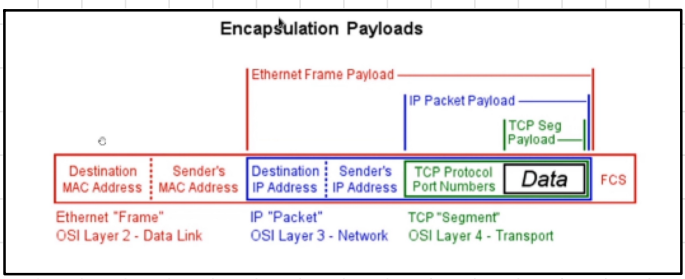
Incapsulamento

La comunicazione tra macchine diverse avviene tramite l'incapsulamento. Il processo di incapsulamento inizia dal livello applicativo, dove il **messaggio di livello applicativo** viene suddiviso in **segmenti di livello di trasporto**, ad esempio utilizzando il protocollo TCP o UDP. Il segmento di livello di trasporto contiene le informazioni necessarie per instradare il pacchetto attraverso la rete, come ad esempio i numeri di porta di origine e di destinazione. Successivamente, il segmento di livello di trasporto viene incapsulato in un **datagramma a livello di rete**, che contiene l'indirizzo IP di origine e di destinazione, necessario per instradare il pacchetto attraverso la rete. Il datagramma a livello di rete viene quindi incapsulato in un **frame a livello di collegamento dati**, ad esempio utilizzando il protocollo Ethernet. Il frame a livello di collegamento dati contiene gli indirizzi MAC di origine e di destinazione, necessari per instradare il pacchetto attraverso la rete locale. Infine, il frame a livello di collegamento dati viene tradotto in **bit a livello fisico**, che vengono trasmessi attraverso il mezzo di trasmissione fisico, come ad esempio un cavo Ethernet.

Il processo di decapsulamento avviene in modo inverso quando il pacchetto raggiunge la destinazione finale. Il livello fisico riceve i bit e li passa al livello di collegamento dati, che rimuove l'intestazione del frame a livello di collegamento dati. Successivamente, il livello di rete rimuove l'intestazione del datagramma a livello di rete e infine il livello applicativo riceve il segmento di livello di trasporto.



Ethernet

Ethernet è un protocollo di livello DLL (livello 2 con riferimento alla pila ISO/OSI) che si occupa di trasmissione di dati su reti locali LAN cablate attraverso i cavi Ethernet. Grazie a Ethernet, i dispositivi di rete possono comunicare tra loro in modo efficiente e affidabile, all'interno di una rete locale (LAN). Un frame Ethernet è il pacchetto di dati che viene trasmesso attraverso la rete Ethernet.

MAC address (media acces control)

Nella rete LAN assume una certa rilevanza l'indirizzo MAC dei singoli dispositivi, oltre a quello IP, in quanto il pacchetto deve comunque passare dal livello DLL per essere inviato ad un altra macchina.

Un MAC address è un indirizzo univoco ed è costituito da 6 byte di dati espressi in formato esadecimale.

00 : 1A : 2B : 3C : 4D : 5E

Il MAC viene assegnato a una scheda di rete dal produttore e viene utilizzato per identificare in modo univoco i dispositivi all'interno di una rete. MAC **è un indirizzo flat** poiché non ha una struttura gerarchica e non è possibile dedurre l'ubicazione geografica di un dispositivo di rete solo dal suo MAC address.
Poiché l'indirizzo MAC è un identificatore flat, viene utilizzato principalmente per identificare i dispositivi all'interno di una rete locale (LAN), dove viene utilizzato dal protocollo Ethernet per instradare i pacchetti attraverso la rete locale.

ARP (adress resolution protocol)

ARP è un protocollo utilizzato per mappare un indirizzo IP a un indirizzo MAC sulla stessa subnet, quindi funziona solo nella LAN locale. Questo processo è necessario perché i pacchetti vengono trasmessi utilizzando gli indirizzi IP, ma la comunicazione effettiva avviene attraverso gli indirizzi MAC.

Quando un dispositivo su una rete locale deve inviare un pacchetto IP a un altro dispositivo sulla stessa subnet, utilizza ARP per ottenere l'indirizzo MAC del dispositivo di destinazione. Il dispositivo mittente invia una **ARP request** broadcast che arriva a tutte le macchine in rete contenente l'indirizzo IP del dispositivo di destinazione (nota che invece, a livello IP, il messaggio è diretto ad una precisa macchina) . Tutti i dispositivi sulla stessa subnet ricevono la richiesta e il dispositivo di destinazione risponde con un pacchetto **ARP reply**, contenente il proprio indirizzo MAC.

La risposta ARP viene quindi memorizzata nella cache ARP del dispositivo mittente, che associa l'indirizzo IP del dispositivo di destinazione con il corrispondente indirizzo MAC. In questo modo, il dispositivo mittente può utilizzare l'indirizzo MAC per inviare il pacchetto IP al dispositivo di destinazione. La cache ARP viene utilizzata per memorizzare le corrispondenze tra gli indirizzi IP e MAC e viene aggiornata periodicamente o in risposta a nuove richieste ARP. Tuttavia, la cache ARP può essere soggetta ad attacchi di spoofing, in cui un attaccante invia pacchetti ARP falsificati per inserire informazioni false nella cache ARP di un dispositivo.

- **Vulnerabilità ARP**

Una delle principali vulnerabilità di ARP è che non richiede autenticazione, il che significa che un dispositivo a cui non è realmente destinato un frame ARP può riceverlo. Questo può portare a diverse forme di attacchi, come l'ARP spoofing, in cui un attaccante invia deliberatamente un frame ARP modificato per mappare l'indirizzo MAC del suo dispositivo all'indirizzo IP di un altro dispositivo, al fine di **dirottare il traffico IP** destinato a quel dispositivo.

Inoltre, ARP è stateless, ovvero non tiene traccia delle richieste e risposte degli utenti. Ciò significa che una ARP response può essere ricevuta senza l'invio di una precedente ARP request, il che può essere sfruttato per attacchi in cui un attaccante invia una ARP response fraudolenta per aggiornare la cache ARP di un host con un indirizzo MAC falso.

I controlli sulla correttezza dell'indirizzo MAC del destinatario vengono fatti ad un livello più alto secondo protocolli che richiedono autenticazione.

RARP (Reverse Address Resolution Protocol)

Questo è un protocollo utilizzato per mappare un indirizzo MAC a un indirizzo IP sulla stessa subnet. A differenza di ARP, che mappa un indirizzo IP a un indirizzo MAC, RARP utilizza il processo inverso.

RARP è stato sviluppato per risolvere il problema di avvio dei computer diskless (senza disco), che non hanno un indirizzo IP assegnato in modo permanente. In questo caso, il computer avvia il proprio sistema operativo tramite il network, ma non ha un indirizzo IP assegnato, quindi non può comunicare con altri computer sulla rete.

Per risolvere questo problema, il computer diskless invia un pacchetto RARP broadcast contenente il proprio indirizzo MAC e richiedendo l'assegnazione di un indirizzo IP valido. Il server RARP sulla rete riceve la richiesta e invia un pacchetto RARP response contenente l'indirizzo IP richiesto.

Tuttavia, RARP ha alcune vulnerabilità di sicurezza simili ad ARP, come l'assenza di autenticazione e la possibilità di attacchi di spoofing.

BOOTP (bootstrap protocol)

Il BOOTP è un protocollo di rete utilizzato per consentire a un computer di avviarsi e di ricevere un indirizzo IP, in particolare viene utilizzato durante la fase di boot del computer, quando il sistema deve acquisire un indirizzo IP valido per poter comunicare sulla rete.
Il client BOOTP invia un messaggio di richiesta di boot (BOOTREQUEST) contenente il proprio indirizzo MAC al server BOOTP, che risponde con un messaggio di offerta di boot (BOOTREPLY) contenente l'indirizzo IP da assegnare al client.

Requisiti di configurazione

Per essere configurata in una rete, una macchina ha bisogno di diverse informazioni e impostazioni, tra cui:

1. Indirizzo IP: è l'indirizzo numerico univoco assegnato alla macchina per identificarla sulla rete. L'indirizzo IP può essere assegnato manualmente o automaticamente da un server DHCP.

2. Subnet mask: è un valore numerico che permette di definire la suddivisione logica della rete in sottoreti. La subnet mask definisce quali bit dell'indirizzo IP identificano la parte di rete e quali bit identificano la parte di host.

3. Gateway predefinito: è l'indirizzo IP del router che consente alla macchina di comunicare con le reti esterne alla sua sottorete.

4. DNS: è l'indirizzo IP del server DNS (Domain Name System) che consente alla macchina di risolvere i nomi dei domini in indirizzi IP.

5. Nome della macchina: è il nome utilizzato per identificare la macchina sulla rete, che può essere utilizzato per la risoluzione dei nomi di dominio.

6. Indirizzo MAC: è l'indirizzo univoco assegnato dalla scheda di rete del dispositivo, utilizzato a livello di collegamento dati per identificare la macchina all'interno della rete locale.

7. Protocolli di rete: la macchina deve essere configurata in modo da supportare i protocolli di rete utilizzati nella rete, come ad esempio il protocollo Ethernet.

Comunicazione su reti differenti

Se le macchine si trovano nella stessa rete LAN possono comunicare. Nel caso in cui le macchine si trovano in reti differenti la situazione si complica : quando un pacchetto viene trasmesso attraverso una rete, ogni dispositivo di rete che inoltra il pacchetto sostituisce l'indirizzo MAC del mittente con il proprio indirizzo MAC come sorgente del pacchetto, e l'indirizzo MAC della destinazione con l'indirizzo MAC del prossimo dispositivo di rete che inoltrerà il pacchetto. In questo modo, il pacchetto può essere correttamente instradato attraverso la rete.

Tuttavia, è importante sottolineare che l'indirizzo MAC non cambia casualmente, ma viene sostituito da una macchina intermedia solo durante il passaggio del pacchetto attraverso quella macchina. L'indirizzo MAC originale del mittente e della destinazione viene preservato all'interno del pacchetto stesso.

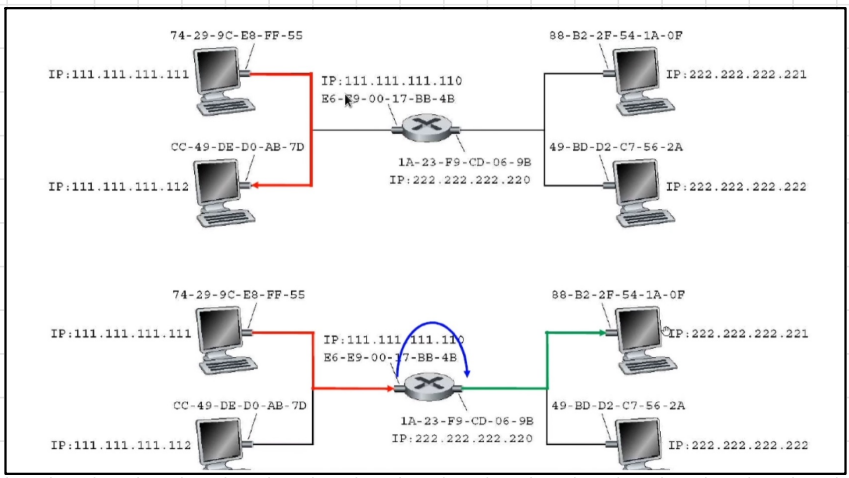
Se la destinazione del pacchetto si trova al di fuori della LAN, allora il pacchetto deve essere inviato al router di rete. Il router funge da gateway predefinito per la rete e viene utilizzato per instradare i pacchetti di dati tra le diverse reti. Il router analizza l'indirizzo IP di destinazione del pacchetto e lo inoltra alla rete corretta fino a quando non raggiunge la destinazione finale.

Discussione d'esame

Due LAN separate da un Router (Livello 3 quindi) di mezzo.Ha infatti sia indirizzi IP che MAC per ogni interfaccia. Supponiamo che una macchina abbia necessità di parlare con un'altra macchina, che potrebbe trovarsi sia nella sua stessa LAN che in una LAN differente, anche attraversando più router.

stessa LAN ←

LAN differenti ←



Le due operazioni sono nettamente differenti:

Stessa LAN :

Il mittente deve solo scoprire che il destinatario appartiene alla stessa LAN, quindi può preparare una frame Ethernet (ricordiamo che la comunicazione avviene a livello DLL, non IP, perché il datagramma IP è incapsulato nella frame Ethernet). Deve solo scoprire il MAC Address del destinatario, cosa che può fare con ARP mandando in broadcast la richiesta. Questa macchina potrà rispondere tranquillamente alla richiesta broadcast in quanto si trova sulla stessa LAN

LAN Differenti :

Se il destinatario è fuori dalla sua LAN non può usare ARP per scoprire il MAC address della destinazione, per due motivi:

a. Il router non fa passare nulla a livello DLL, perché per quanto riguarda il router ha due livelli DLL differenti, quello della LAN rossa e quello della LAN verde. Anche se il mittente riuscisse a scoprire il MAC address che gli interessa, la frame Ethernet verrebbe comunque spacchettata una volta arrivato al router, e ovviamente scartata.

b. Non esiste solo Ethernet: Ci sono reti DLL che non hanno il MAC Address(per esempio tante macchine collegate tutte punto a punto), quindi semplicemente dire che il mittente vuole conoscere il MAC Address della destinazione è inutile, perché potrebbe anche non esistere.

Quindi se la macchina è fuori dalla LAN devo indirizzare il pacchetto al router, il quale spacchetterà la frame Ethernet, leggerà il pacchetto IP e creerà un'ulteriore frame Ethernet da spedire dentro l'altra LAN (verde).

Tabella host

Ogni macchina all'interno di una rete fa da router ed è dotata di una tabella di routing che serve ad associare un indirizzo IP di destinazione a un'interfaccia di rete sulla stessa macchina o su un router di rete.

La tabella di routing contiene informazioni sui router, insieme alle relative interfacce di rete e ai percorsi di instradamento. Quando una macchina deve inviare un pacchetto di dati, consulta la tabella di routing per determinare il percorso migliore per la destinazione. Se la destinazione si trova sulla stessa subnet, la macchina invia il pacchetto direttamente alla destinazione. In caso contrario, cerca il router di rete predefinito(gateway predefinito) e invia il pacchetto a questo router per l'instradamento verso la destinazione.

DHCPv4 (Dynamic Host Configuration Protocol versione 4)

Con l'avvento dei portatili nasce l'esigenza di assegnare un indirizzo ad una macchina che non ne ha uno.
Il protocollo DHCPv4 è un protocollo di rete utilizzato per l'assegnazione dinamica degli indirizzi IP alle macchine sulla rete. DHCPv4 consente alle macchine di ottenere un indirizzo IP valido in modo automatico e semplificato, senza la necessità di assegnare manualmente un indirizzo IP a ciascuna macchina.

Il protocollo DHCPv4 supporta anche l'assegnazione di indirizzi IP temporanei, noti come indirizzi IP "leasing".
In questo caso, l'indirizzo IP viene assegnato alla macchina solo per un periodo di tempo limitato, dopo il quale la macchina deve rinnovare l'assegnazione dell'indirizzo IP. Questo consente di gestire in modo più efficiente gli indirizzi IP disponibili sulla rete. Il protocollo DHCPv4 prevede quattro fasi principali per l'assegnazione dell'indirizzo IP:

1. **Scoperta DHCP**: la fase di Scoperta DHCP inizia quando il client DHCP si connette alla rete e invia un messaggio di scoperta in broadcast sulla rete locale alla ricerca di un server DHCP disponibile. Il messaggio contiene informazioni come l'identificatore del client, il tipo di hardware utilizzato e le opzioni di configurazione richieste.

2. **Offerta DHCP**: il server DHCP riceve il messaggio di scoperta e invia un messaggio di offerta al client. In questo messaggio, il server offre un indirizzo IP disponibile al client DHCP, insieme ad altre informazioni di configurazione come la subnet mask e l'indirizzo del gateway.

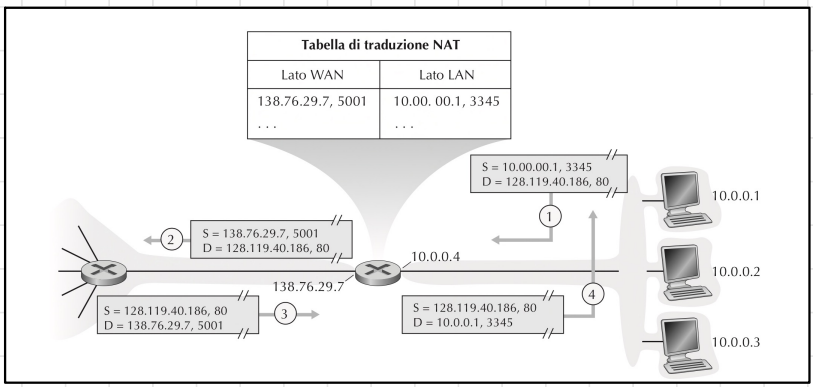
3. **Richiesta DHCP**: il client DHCP riceve il messaggio di offerta dal server e invia un messaggio di richiesta per confermare l'assegnazione dell'indirizzo IP offerto dal server. In questo messaggio, il client DHCP richiede l'assegnazione dell'indirizzo IP offerto dal server.

4. **ACK DHCP**: il server DHCP riceve il messaggio di richiesta e invia un messaggio di ACK al client DHCP per confermare l'assegnazione dell'indirizzo IP richiesto. Il messaggio ACK contiene l'indirizzo IP assegnato al client DHCP, insieme alle altre informazioni di configurazione richieste.

Il protocollo DHCP prevede queste quattro fasi principali per l'assegnazione dell'indirizzo IP, e solo dopo aver completato queste fasi il client può utilizzare l'indirizzo fornito dal server DHCP. Il server DHCP mantiene un registro dello stato delle assegnazioni degli indirizzi IP ai client, però non prevede l'autenticazione.

NAT (network acces translation)

Nella figura vi è una rete privata, ossia una rete i cui indirizzi hanno significato solo per i dispositivi interni ed un router abilitato al NAT. Le quattro interfacce della rete domestica hanno lo stesso indirizzo di sottorete, 10.0.0.0/24. Esistono centinaia di migliaia di reti private, molte delle quali usano un identico spazio di indirizzamento, 10.0.0.0/24, per scambiare pacchetti fra i loro dispositivi. Ovviamente, quelli inviati sull'Internet globale non possono utilizzare questi indirizzi come sorgente o destinazione. Ma se gli indirizzi privati hanno significato solo all'interno di una data rete, come viene gestito l'indirizzamento dei pacchetti relativi all'Internet globale, in cui gli indirizzi sono necessariamente **univoci**? La risposta è il NAT.



I router abilitati al NAT non appaiono come router al mondo esterno, ma si comportano come un unico dispositivo con un unico indirizzo IP. Supponiamo che un utente che si trovi nella rete domestica dietro l'host 10.0.0.1 richieda una pagina web da un server (porta 80) con indirizzo IP 128.119.40.186. L'host 10.0.0.1 assegna il numero di porta di origine (arbitrario) 3345 e invia il datagramma nella rete locale. Il router NAT riceve il datagramma, genera per esso un nuovo numero di porta di origine 5001, sostituisce l'indirizzo IP sorgente con il proprio indirizzo IP sul lato WAN 138.76.29.7 e sostituisce il numero di porta di origine iniziale 3345 con il nuovo numero 5001. Il NAT del router aggiunge inoltre una riga alla propria tabella di traduzione NAT.

Il web server, ignaro della manipolazione subita dal datagramma in arrivo con la richiesta HTTP, risponde con un datagramma con l'indirizzo IP del router NAT come destinazione e il cui numero di porta di destinazione è 5001. Quando questo datagramma arriva al router NAT, quest'ultimo consulta la tabella di traduzione NAT usando l'indirizzo IP di destinazione e il numero di porta di destinazione per ottenere l'appropriato l'indirizzo IP (10.0.0.1) e il corretto numero di porta di destinazione (3345) del browser nella rete domestica. Il router quindi riscrive l'indirizzo di destinazione del datagramma e il suo numero di porta di destinazione e inoltra il datagramma nella rete domestica.

NB
- Il server NAT non necessariamente è un router ma potrebbe essere una macchina sulla rete.
- Nella rete NAT il primo pacchetto scambiato deve partire necessariamente dalla rete locale.