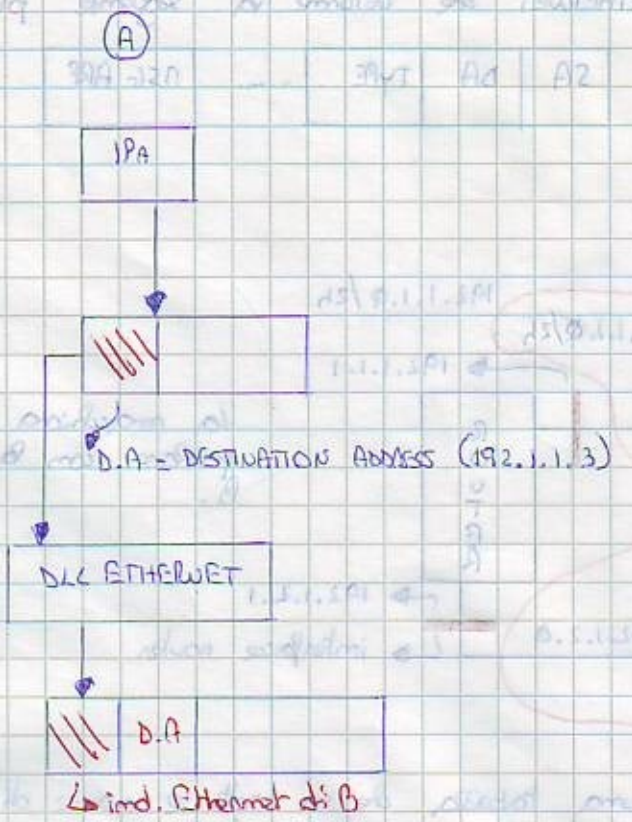
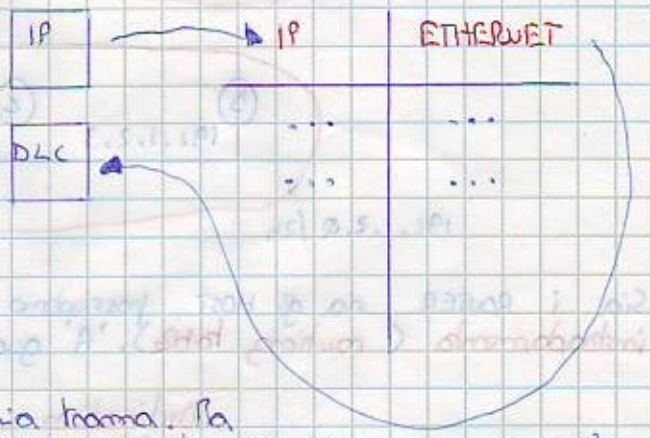
pacchetto speciale di broadcast che chiede all'host con indirizzo IP_B di rispondere con il proprio indirizzo fisico. Per essere più precisi partiamo dall'inizio. Supponiamo di conoscere l'indirizzo ETHERNET di B.



La trama viene spedita in broadcast sulla rete fisica.

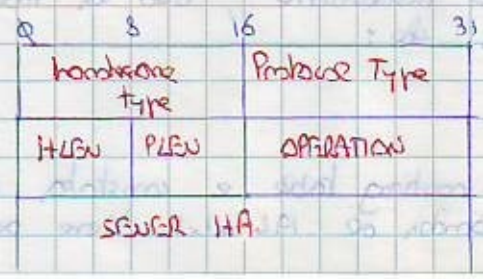
Ogni PC analizza il campo D.A. Quando B "vede" che il campo D.A è il suo, analizza il pacchetto. Si noti attenzione al fatto che per mappare gli indirizzi IP sugli indirizzi ETHERNET, si usa una tabella denominata:

ARP CACHE TABLE



Così facendo posso tranquillamente generare la mia trama. Ma quando avvio la macchina, la mia ARP CACHE TABLE è vuota. E allora come faccio? Qui si usa ARP.

La macchina A sollecita ARP, o meglio A chiama ARP che a sua volta crea un messaggio che si chiama ARP REQUEST che contiene codificata la richiesta di risoluzione dell'indirizzo IP. Questo messaggio viene "imbustato" in una trama ETHERNET con indirizzo BROADCAST. Tutti i PC presenti nella rete elaborano tale messaggio. Ogni DLC della macchina riceve tale messaggio e lo invia ad ARP. Chiaramente risponderanno solo i PC che hanno la stessa "mapping". A questo punto B confeziona un messaggio di ARP REPLY contenente l'indirizzo richiesto, e lo spedisce ad A. A riceve tale messaggio e aggiorna la ARP TABLE. Si noti che se la macchina C non conosceva il mapping, aggiornano automaticamente la loro ARP-TABLE. Vediamo ora la STRUTTURA DI UN MESSAGGIO ARP:



NB: sender = la macchina che ci invia la risposta.

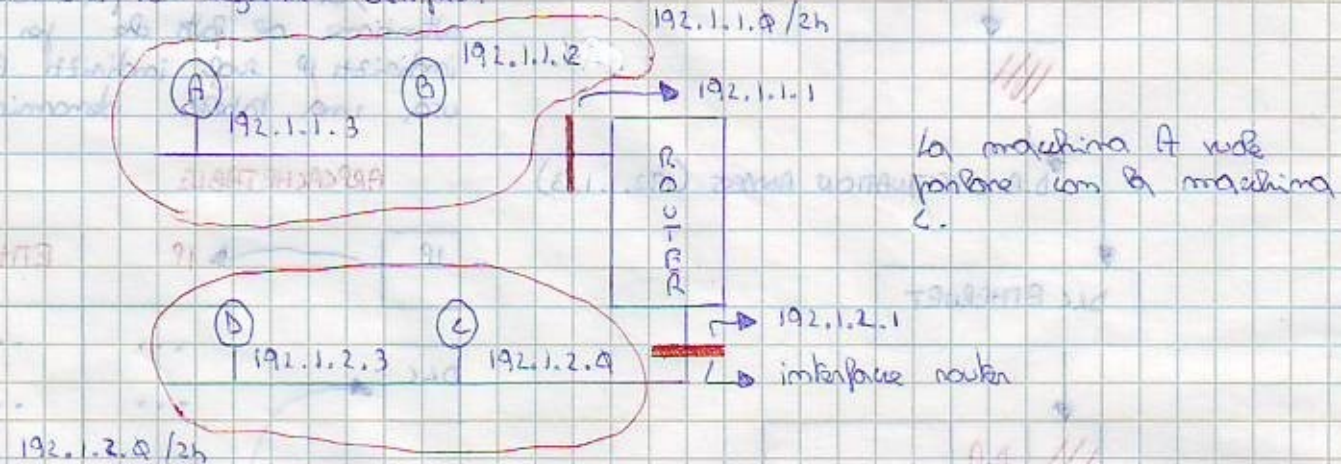
16

sender HA	sender IP
sender IP	Target HA
TARGET HA	
TARGET IP	

Questo messaggio viene incapsulato nella trama ETHERNET che assume la seguente forma:

SA	DA	TYPE	...	MSG ARP

Analizziamo ora il seguente esempio:



La macchina A vuole parlare con la macchina C.

Sia i ROUTER sia gli HOST possiedono una tabella che va sotto il nome di tabella di instradamento (routing table). A guarda la propria routing table:

Destination Network	Next Hop
192.1.1.0 /24	INSTRADAMENTO DIRETTO.
DEFAULT GATEWAY	192.1.1.1

In breve se il pacchetto instradato va verso una rete non listata in tabella, allora si va verso l'interfaccia del router. In questo modo A sa raggiungere tutto il mondo. Quindi A "guarda" la ROUTING TABLE e trova la seguente entry:

192.1.1.2

In questo caso si usa l'instradamento diretto. Dopo di che guarda la ARP CACHE TABLE, se non si ha una risoluzione, si chiama il protocollo ARP e poi crea la trama ETHERNET da trasmettere, altrimenti se ha risoluzione crea la trama e la trasmette senza scomodare l'ARP. Supponiamo ora che:

D.A = 192.1.2.3 (D)

Il meccanismo cambia. A consulta la routing table e constata che non c'è una entry esplicita. Dopo di che al next hop si ha 192.1.1.1 viene analizzata la ARP

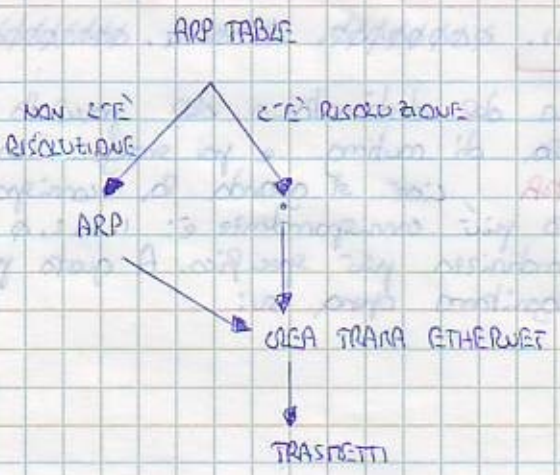
CACHE TABLE. Anche qui se c'è risoluzione non si scomoda ARP, altrimenti lo si scomoda. Viene creata la trama Ethernet e viene trasmessa. Quindi il router riceve il pacchetto con:

D.A = 192.1.2.3

Quindi il router controlla la sua routing table così fatta:

DESTINATION NETWORK	NEXT HOP
192.1.1.0 /24	INSTRADAMENTO DIRETTO SU 192.1.1.1
192.1.2.0 /24	INSTRADAMENTO DIRETTO SU 192.1.2.1
DEFAULT GATEWAY	? IP NEXT ROUTER.

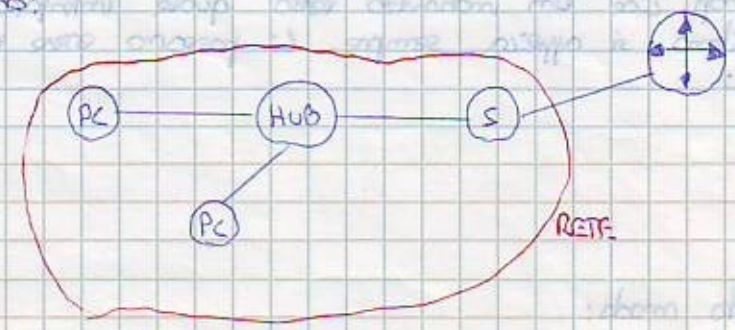
Quindi:



NB: Esistono due tipi di instradamento:

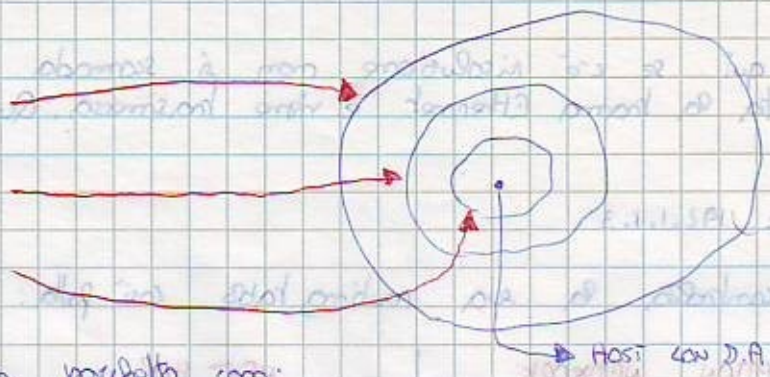
1) diretto
2) indiretto → sequenza di instradamenti diretti.

Perciò se abbiamo:



le macchine presenti nella rete usano tutte un instradamento di tipo diretto, altrimenti si usa un instradamento indiretto. Per fare quest'ultimo tipo di routing si usano le tabelle di routing degli host, dei router, e in caso ARP per risolvere gli indirizzi IP sugli indirizzi hardware. Per quanto riguarda l'indirizzamento IP abbiamo già visto il subnetting, cioè la suddivisione della rete in sottoreti. Per esempio:

(18)



Supponiamo di avere un pacchetto con:

D.A: 11.1.2.5 → ci chiediamo ora a quale rete appartiene.

L'host appartiene alla rete ①, ②, ③. Spesso nei router quando arriva un pacchetto da instradare, nasce un'ambiguità. Abbiamo:

11.1.2.5 —(in binario)→ 00001011.00000001.00000010.00000101

11.1.2.0/24 → 00001011.00000001.00000010.00000000

11.1.0.0/16 → 00001011.00000001.00000000.00000000

11.0.0.0/8 → 00001011.00000000.00000000.00000000

Il router fa l'AND bit a bit tra l'indirizzo di destinazione del pacchetto e la Network mask della singola entry della tabella di routing e poi svolge il confronto. In merito si usa la tecnica del longest match cioè si guarda la corrispondenza più lunga. Nel nostro caso la riga che ha ottenuto più corrispondenze è: 11.1.2.0/24. Quindi il longest match altro non è che un indirizzo più specifico. A questo punto il router attiva un algoritmo di routing e l'algoritmo opera su:

1) pacchetto da instradare
2) Tabella di routing

e in uscita fornisce un next hop, cioè un indirizzo verso quale interfaccia di rete bisogna mandare il pacchetto. Tale algoritmo si applica sempre. Ci possono essere vari tipi di algoritmi di routing, tra cui:

1) OSPF
2) RIP

L'algoritmo funziona in questo modo:

1) estrae il D.A del pacchetto.
2) Si scandisce la tabella di routing e per ogni riga si controlla la corrispondenza. In particolare per ogni destination network si prende la network mask relativa e si fa del matching con i primi m bit di D.A. Qui m è il suffisso cioè il numero di bit significativi.
   2.1) se esiste una corrispondenza, acquisisci il next hop e trasmetti il pacchetto.

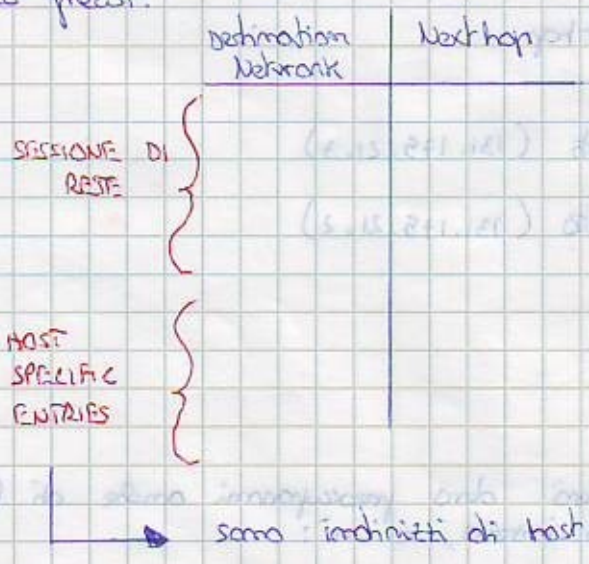
2.2) se non esiste una corrispondenza, allora controlla le host specific entries.

2.2.1) se esiste una corrispondenza allora legge il next hop e instrada il pacchetto.

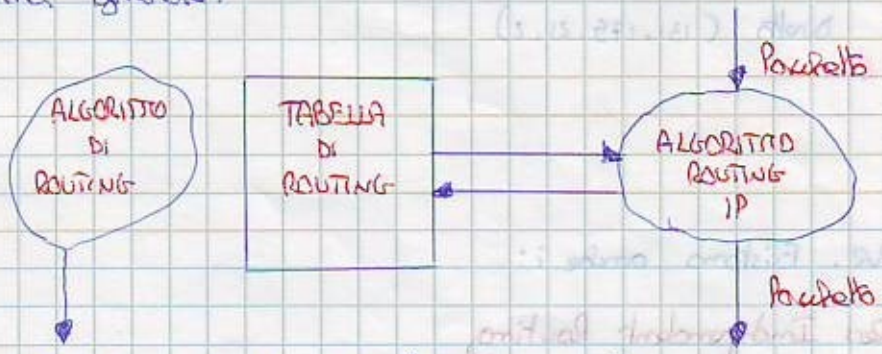
2.2.2) se non esiste una corrispondenza si guarda se esiste un default gateway.

2.2.3) se non c'è un default gateway, allora genera un'eccezione cioè il pacchetto non può essere instradato.

NB: Il default gateway permette di non avere tabelle complete.
NB: Per essere più precisi:

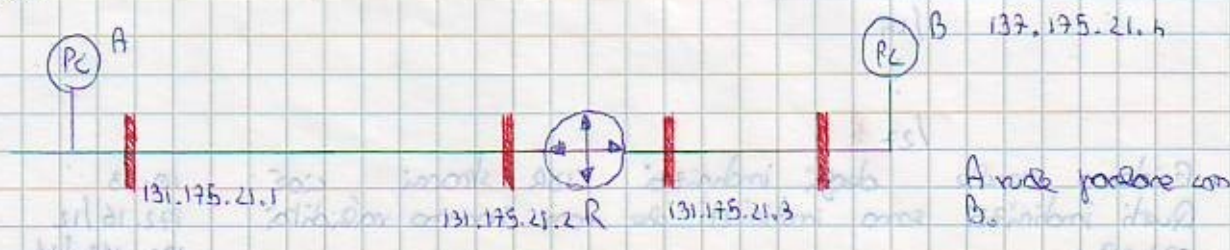


La tabella di routing può essere statica (scritta a mano) o dinamica e cioè scritta dagli algoritmi. Però sostanzialmente le cose non cambiano di molto. Vediamo ora lo schema generale:



è una cosa a se che si scrive la sua tabella routing. Non vedremo nessun pacchetto

Vediamo un esempio:



Quindi:

(29)

A:

Destination Network	Next hop
DEFAULT GATEWAY	131.175.21.2 (diretta) → Gli manda al router R.

Il router R avrà:

Destination Network	Next hop
131.175.21.3	Diretta (131.175.21.3)
131.175.21.1	Diretta (131.175.21.2)

Per quanto riguarda i router statici però devo preoccuparmi anche di fornire il percorso di risposta. Quindi devo mettere un path inverso, e cioè:

D.N	N.H
DEFAULT GATEWAY	131.175.21.3
131.175.21.1	Diretta (131.175.21.2)

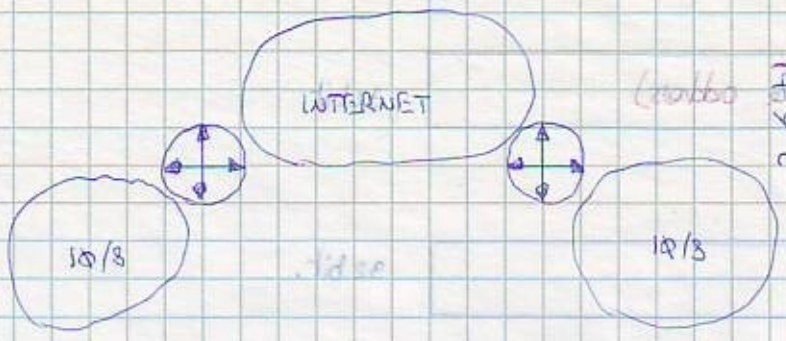
Abbiamo visto la tecnica classful. Esistono anche i:

CIDR = Classless Inderdependent Routing

in cui si possono associare indirizzi che non sono compresi nella classful. Per esempio:

/13
/14
.
.
/27

Esistono anche degli indirizzi CIDR strani cioè: 10.0/8
Questi indirizzi sono indirizzi che non hanno validità 172.16/12
globale. 192.168/16
169.254/16



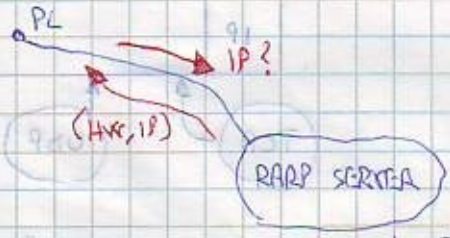
I router che compaiono in figura vengono chiamati NATBOX. Sostanzialmente trasformano gli indirizzi strani in indirizzi buoni.

Si fa ciò perché gli indirizzi buoni sono pochi. Vediamo ora brevemente anche il RARP. Esso è il contrario di ARP. Supponiamo che una macchina non conosca il proprio indirizzo IP. Il protocollo RARP sostanzialmente permette alla macchina di imparare il suo indirizzo IP. RARP funziona come ARP solo che qui la macchina conosce il suo indirizzo hardware e invia la richiesta di risoluzione inversa, cioè:

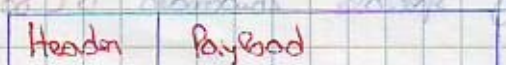
INDIRIZZO HARDWARE ⟶ INDIRIZZO IP

Anche qui ci sarà un RARP SERVER che possiede RARP TABLE fatta in questo modo:

IND. ETHERNET	IND. IP

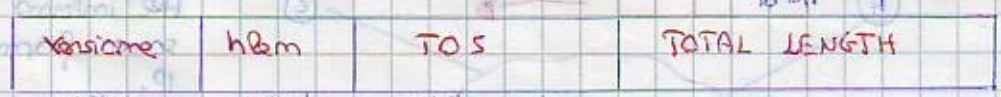


Oggi si tende in maniera automatica ad associare gli IP. Oggi in particolare si usa DHCP (Dynamic Host Configuration Protocol) che deriva da RARP. Vediamo ora come è fatto un pacchetto IP:



IPv4

Vediamo l'header; è composto da parole di 32 bit:



campo che specifica in byte la lunghezza di tutto il pacchetto (65535 byte).

Type of service che indica il modo in cui viene trattato il pacchetto dalle router.

mi codifica la versione (versione 4)

Header length (lunghezza base) con un'unità di misura: n° parole di 32 bit.

5 parole di 32 bit

Un pacchetto IP può essere frammentato perché ci possono essere link con capacità inferiori.