

## Lo Strato di Rete

### Funzioni

#### • INSTRADAMENTO (ROUTING)

E' una funzione decisionale, essa è implementata da protocolli ed algoritmi specifici. Il routing determina il percorso che seguiranno i pacchetti dall'origine alla destinazione. Decide anche su quale interfaccia di uscita (di un router) deve essere mappato.

#### • INOUTRO (FORWARDING)

E' una funzione attuativa. Trasferisce il pacchetto, fisicamente, dalla linea di ingresso a quelle di uscita. Principalmente è una funzione che avviene nel nodo.

Queste funzioni sono implementate diversamente a seconda delle modalità della rete.

#### 1. COMMUTAZIONE A CIRCUITO (Circuit Switching):

- Instaura una comunicazione con connessione, il cammino (PATH) è stabilito all'inizio.
- I nodi hanno una funzione STATEFUL, cioè mantengono delle informazioni sullo stato.
- Alla fine della conversazione bisogna liberare le risorse e cancellare le info sugli stati.
  - ↳ avviene tramite messaggi (Fase set-up)
- Comunicazione telefonica
- PRO = comunicazione e risorse esclusive

CONTRO = + Spreco di risorse se non trasmetto per tutto la sessione

• Perdite di tempo con la fase di set-up

#### 2. PACKET SWITCHING:

- Le reti sono dette a "datagramma"
- La comunicazione si instaura senza connessione quindi i pacchetti sono inviati senza un preventivo accordo con destinatario e con la rete
- L'instradamento è deciso pacchetto per pacchetto quindi possono seguire path diversi
- I router hanno un funzionamento STATELESS, non memorizzano nulla
- PRO = Semplicità degli algoritmi

CONTRO = - Non vi è ordine nella consegna dei pacchetti

• La qualità della comunicazione è bassa

- Non sempre circuiti fisici disponibili

× Ip → anche se per alcuni servizi via comunicazioni con connettori.

### 3. VIRTUAL CIRCUIT

~ Molto usato, è una novità.

~ E' una comunicazione senza connessioni ma al�ori si stabilisce un cammino. Le risorse vengono conquistate rotta per rotta, così da evitare sprechi.

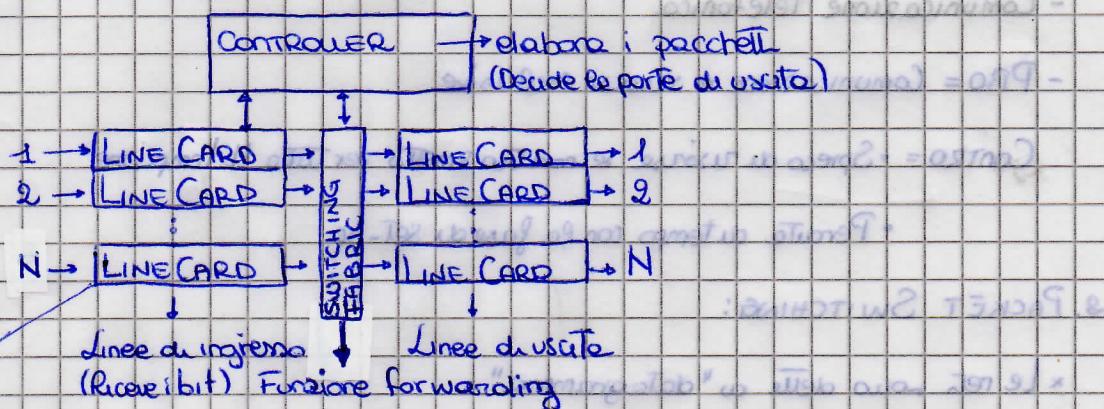
Nella comunicazione a pacchetto (Packet Switching) ogni pacchetto è indipendente, quindi deve possedere un'intestazione che contiene il destinatario.

Inoltre, cioè i router, hanno una tabella di routing che contiene tutti gli indirizzi possibili, naturalmente sono raggruppati a seconda di dove si trovano.

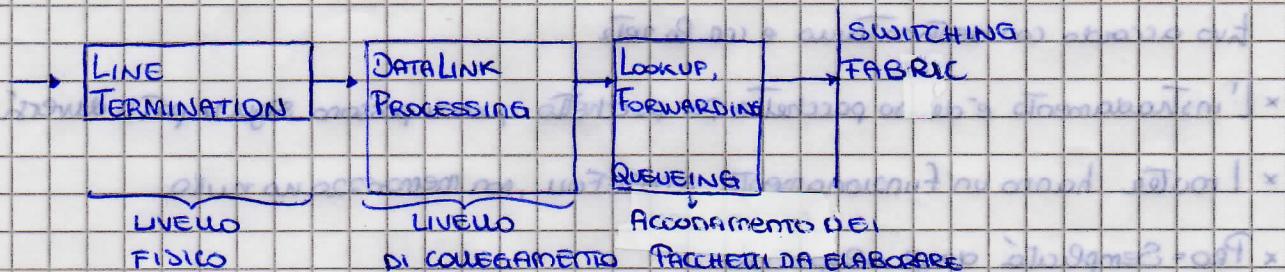
Le tabelle di routing sono simili a quelle degli switch ma sono più estese. Gli indirizzi inseriti nei router sono strutturati in modo da individuare prima la "zona" in cui si trova e solo quando sono nella stessa, l'host specifico.

### ARCHITETTURA DI UN ROUTER

L'rete in cui ci troviamo è a pacchetto o datagramma.



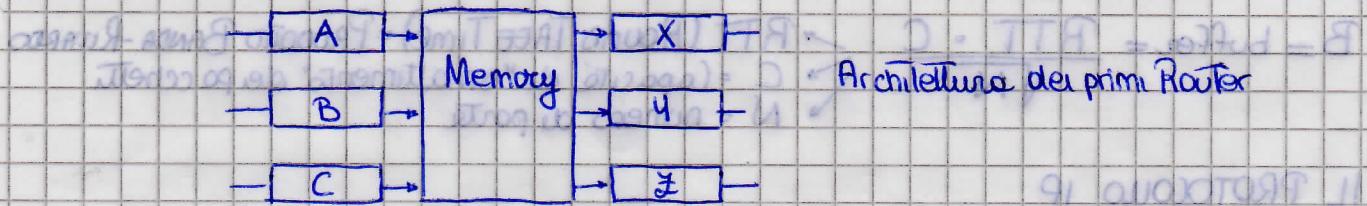
**INPUT LINE CARD (Porte d'ingresso)**



**3 TECNICHE DI COMMUTAZIONE** (collegamento tra ingresso ed uscita)

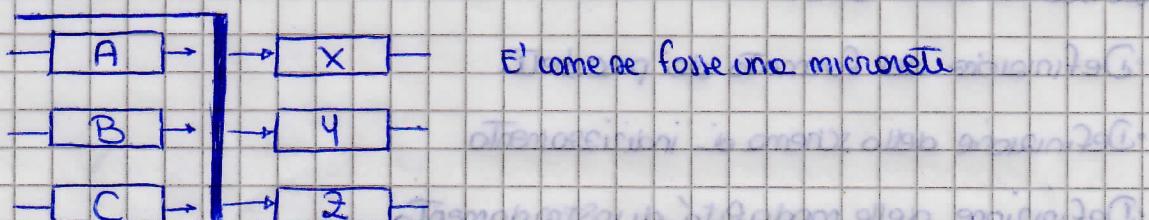
1. SHARED MEMORY

- il pacchetto viene copiato in memoria (RAM) assieme ad analoghi e strutturati
- la commutazione avviene sotto diretto controllo del controller (BENE)



## 2. Bus Interconnection

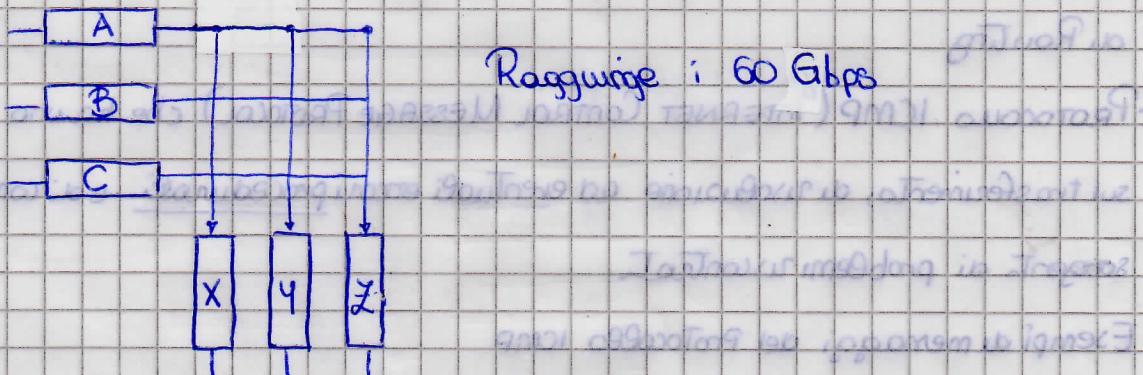
- le porte d'ingresso trasferiscono il pacchetto direttamente alle porte di uscita su un bus condensato



## 3. CROSSBAR

### Griglia di connessioni (cavi)

- Passa un pacchetto alla volta, vengono abilitate solo le connessioni che gli permettono di raggiungere le porte di uscita giuste.



La matrice più famosa di router è Cisco.

L'operatività di switching deve essere molto veloce per evitare il "collo di bottiglia".

### Porte d'uscita



Simili alle porte di ingresso, i pacchetti vengono memorizzati (un'uscita potrebbe ricevere più pacchetti) per trasmessi allo strato 2 ed infine allo strato 1.

Importante è calcolare la memoria (buffer) che deve avere una line card.

La RFC 3439 suggerisce questa formula

$$B = \text{buffer} = \frac{\text{RTT} \cdot C}{N}$$

RTT (Round TRIP Time) = Prodotto BANDA - Ritardo  
C = Capacità di "smaltimento" dei pacchetti  
N = numero di porte

## IL PROTOCOLO IP

Il cuore dello strato di rete è proprio il protocollo IP. Esso è definito dalle RFC 791, 919, 922, 950 e 1349. Opera senza connessione e non ha alcuna garanzia.

Le sue funzioni sono:

- Definizione del formato dei pacchetti
- Definizione dello schema di indirizzamento
- Definizione delle modalità di instradamento
- Operazione di frammentazione e riassembaggio delle unità di dati

Insieme ad IP lavorano altri protocolli che permettono il funzionamento di IP stesso.

- Essi sono:
- Protocolli di instradamento (RIP, OSPF, BGP) che hanno il compito di compilare le tabelle di Routing
  - Protocollo ICMP (INTERNET Control Message Protocol) che ha una funzione di controllo sul trasferimento, di risoluzione ad eventuali errori procedurali e di comunicazione alle sorgenti di problemi riscontrati.

Esempi di messaggi del Protocollo ICMP

- Source Quench: il destinatario chiede l'interruzione dell'emissione dei pacchetti al mittente
- Redirect: il destinatario segnala al mittente di reinstradare il pacchetto verso un altro host
- Destination Unreachable: notifica il mittente la non-raggiungibilità di un host
- Echo: controlla se il destinatario è attivo

## FORMATO DEL PACCHETTO (o datagrammi)

Il pacchetto è strutturato in ughe da 32 bit

VERS: Version del protocollo	HEADER LENGTH: lunghezza del header min 80 byte max 60 byte.	SERVICE TYPE: Specifico dell'utente dui parametri du quelli del protocollo	TOTAL LENGTH: lunghezza complessiva del pacchetto, specificata in byte. Comprende PCI + SDU. Il valore max è 65536 byte	P byte	C byte	MAX 65536 byte	MAX 40 byte	S byte
IDENTIFICATION:	Numeri identificativi del pacchetto da frammentare	FLAG + FRAGMENT OFFSET:	Specificano se il pacchetto è unico o è frammentato da uno più grande					
Time To Live:	Indica il tempo massimo che il pacchetto può restare nello strato di rete prima di essere eliminato.	Protocollo:	Indica il protocollo (TCP, UDP, ICMP, ecc.) che viene utilizzato per trasportare i dati.	Header Checksum:	Bit di controllo sul header. In IP non vi è controllo di errore sui dati. (Dunque Berengere in 2110bit poi servirà al parziale facendo mod 16)			
Source IP Address:	Indirizzo dell'host sorgente	TCP = 6, UDP = 17, ICMP = 1						
Destination IP Address:	Indirizzo dell'host destinazione							
Options:	Campi opzionali							
DATA:	Dati trasportati							

## TERMINI DELLA RETE IP

I terminali di una rete IP sono chiamati HOST, invece i nodi sono ROUTER. Un host e un router possono essere collegati tramite dei link ma più precisamente i secondi sono stati inseriti per interconnettere delle SOTTORETI di cui i primi fanno parte.

Internet è infatti, l'unione di migliaia di reti.

## OPERAZIONE DI FRAMMENTAZIONE

L'operazione di frammentazione è ben definita nei vari RFC di IP, cioè le sue modalità sono state standardizzate.

Il pacchetto IP viene suddiviso quando l'unità massima di trasmissione (MTU), cioè la massima quantità di dati trasportabili a livello di collegamento, ha una lunghezza minore. La ricostruzione del pacchetto avverrà solo nell'HOST FINALE. Ogni frammento ha vita propria, quindi potrebbero prendere strade diverse e potrebbero essere divisi da altri router.

In questa operazione entrambi in gioco:

- IDENTIFICATION (16 bit) = uguale per il padre e per i vari figli

- FLAGS (3 bit) = 1° bit non usato e posto a zero, 2° bit DF (Don't Fragment) pari a 0 se la frammentazione è permessa, pari a 1 se la frammentazione è vietata (quindi la trasmissione impedita), 3° bit MF (More Fragment) pari a 0 se è l'ultimo frammento del datagramma, altrimenti è pari a 1.

- FRAGMENT OFFSET (13 bit) = posizione del frammento all'interno del pacchetto, è espresso in 8 byte. Indica quanto è sfasato dall'inizio del pacchetto

L'offset viene calcolato come (lunghezza del frammento precedente - header)

PACCHETTO = 4000 byte

MTU = 1500 byte



L'offset permette di riordinare i frammenti in fase di riassemblaggio ma ciò può avvenire solo se vengono ricevuti tutti.

## Protocollo ICMP

• Serve per inviare messaggi di errore all'host sorgente. Le anomalie che seguono sono:

• errori di indirizzamento; si ottiene con l'ITT i pacchetti non più destinati.

• TTL Time To Live (TTL) scaduto → ogni router decremente di 1 il TTL, quando è 0 invia un ICMP.

• congestione eccessiva.

Esso ha l'unico scopo di notificare scorrettezze, non specificando le azioni da prendere.

E' l'host sorgente che decide come comportarsi.

Non si generano altri messaggi ICMP a seguito di malfunzionamenti legati ai pacchetti contenenti messaggi ICMP.

Formato messaggio ICMP

Type	Code	Checksum	DATA
identifica il tipo di errore	contiene il codice di errore	calcolo del checksum	contiene parte del datagramma IP

ICMP DATA: consente di individuare il pacchetto, causa di errore → Infatti il messaggio ICMP si riferisce ad uno specifico pacchetto.

Nel caso di frammentazione, il messaggio ICMP sarà emesso solo per il frammento 0.

Alcuni esempi di messaggio ICMP:

- Redirect Message:

Se emesso da un router significa che i successivi pacchetti dovranno essere inviati verso un altro router (indicato nel messaggio) a causa di una modifica alla tabella di indirizzamento.

- Time Exceeded

Indica che il TTL è esaurito.

- Echo e Echo REPLAY

Servono per stabilire l'attività di un host.

- DESTINATION UNREACHABLE

Indica che l'indirizzamento di un pacchetto non è stato completato.

Due protocolli che sfruttano i messaggi ICMP sono:

1. PING = individua l'attività di un host e il tempo di transito tra sorgente e destinazione. Utilizza i messaggi ECHO e ECHO Replay.

Per utilizzarlo andare sul PROMPT dei comandi ed inserire

>> ping indirizzo mnemonicico ("www.google.it") o l'indirizzo IP

2. TRACEROUTE: Traccia il percorso di un pacchetto. Mostre tutti i router che attraversa. Per far ciò forza il TTL del pacchetto IP; infatti invia un primo datagramma con TTL=1, raggiungerà il primo router che decrementerà TTL ed invierà un messaggio di errore riportando il proprio nome e il proprio indirizzo IP. Alcuni router non hanno il permesso di mandare i propri identificativi così in quel punto verranno indicati asterischi (\* \* \*). Poi ne invierà un secondo con TTL=2, così identificherà il secondo router, quindi un terzo, ... fino al raggiungimento della destinazione.

Il traceroute per tracciare il percorso ci prova 3 volte.

Per vedere il path per raggiungere un sito dobbiamo sempre andare sul prompt dei comandi e scrivere:

>> traceroute indirizzomnemonico o indirizzo ip.

Il protocollo a mostrerà la lista dei router attraversati con il loro nome e IP e il tempo impiegato per raggiungereli. Quest'ultimo, naturalmente dipende dal traffico che è sulla rete in quell'istante.

N.B. Il tempo necessario per raggiungere una destinazione da una sorgente è chiamato ROUND TRIP TIME (RTT)

## INDIRIZZAMENTO IP

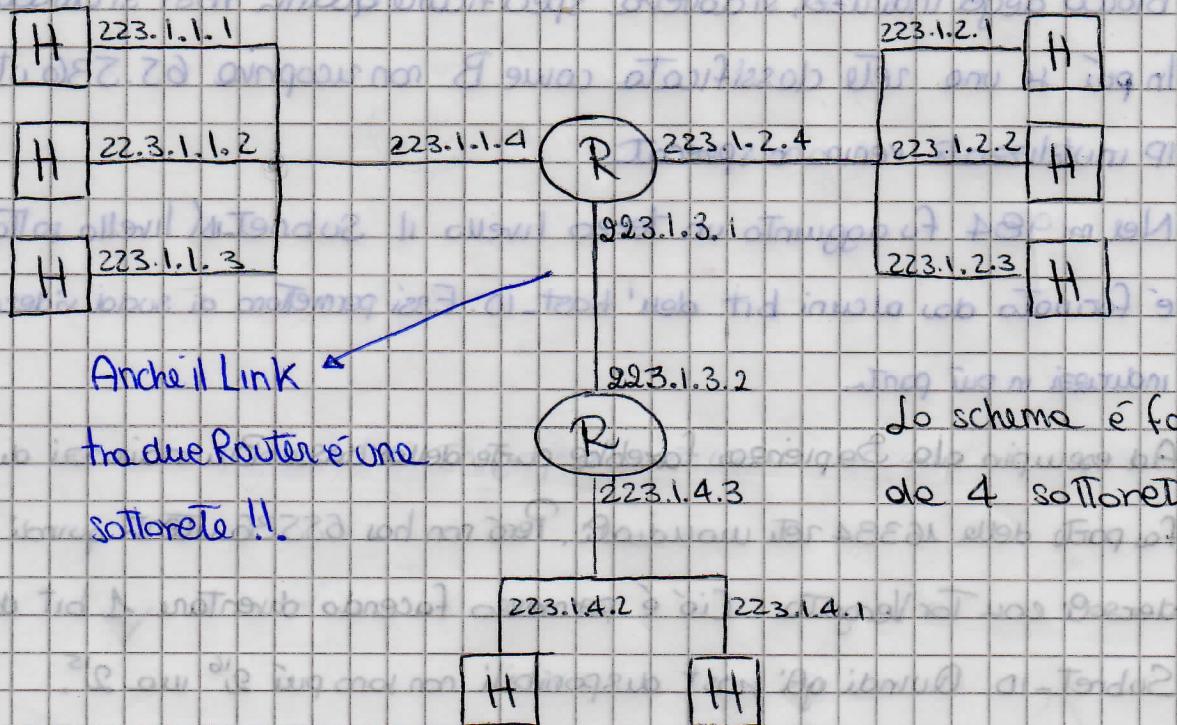
L'IP address è una sequenza di 32 bit che identifica una singola interfaccia di rete. Esso è unico in tutte le reti (IP pubblico) o sottoreti (IP privato).

Come sappiamo INTERNET è un'interconnessione di migliaia di sottoreti. Esse sono rete isolate i cui punti terminali sono collegati all'interfaccia di un host o di un router, sono anche chiamate reti IP.

L'ip identifica ogni interfaccia quando i router hanno tanti indirizzi quanti sono le sottoreti a cui sono collegati.

L'indirizzo è una stringa binaria di 32 bit, può essere riscritto tramite la notazione "dotted", cioè ogni gruppo di 8 bit è tradotto in decimale e separato da un punto "•".

Esempio di collegamenti tra sottoreti con i relativi IP address



Un indirizzo IP è formato da due parti: Net-ID (identificativo delle sottorete) e Host-ID (identificativo del singolo host della sottorete).

La divisione fra Net-ID e Host-ID è variabile.

Gli host di una stessa sottorete hanno lo stesso Net-ID.

Per assegnare gli indirizzi IP, all'inizio, era stato adottato lo schema "CLASSFULL".

CLASSE	BIT INIZIALE	Net-ID	Host-ID	Rete Disponibile	Host Disponibili
A	0	7 bit	94 bit	128	16.777.216
B	10	14 bit	16 bit	16.384	65.536
C	110	21 bit	8 bit	2.097.152	256

INDIRIZZI:

Da queste devono essere esclusi due

host-id "speciali": 1. Formato da  
tutti 0 (identifica la sottorete)

2. Formato da tutti 1 (indirizzo Broadcast)

A	0	Net-ID	Host-ID	
---	---	--------	---------	--

→ I bit iniziali identificano la classe

Il Net-ID occupa i bit più significativi

Esistono altre due classi: D (Indirizzi MULTICAST) e E (Ip futuri).

Questo schema fu abbandonato velocemente in quanto, all'assegnazione dei blocchi degli indirizzi, si doveva specificare quanti host si avrebbero avuti. In più se una rete classificata come B non uscivano 65.536 utenti, gli IP inutilizzati venivano sprecati.

Nel 1984 fu aggiunto un terzo livello il Subnet-ID (livello sottorete). Esso è formato da alcuni bit dell'Host-ID. Essi permettono di suddividere i blocchi di indirizzi in più parti.

Ad esempio alla Sapienza sono assegnati il blocco di indirizzi di classe B, quindi fa parte delle 16384 reti mondiali. Però non ha 65536 utenti quindi decide di dividerceli con Tor Vergata. Ciò è permesso facendo diventare 1 bit dell'Host-ID, Subnet-ID. Quindi gli host disponibili non sono più  $2^{16}$  ma  $2^{15}$ .

Gli indirizzi possono essere suddivisi ulteriormente, ad esempio se decidono di dividerli tra 4 sottoreti, riserverò 2 bit per il Subnet-ID, se tra 8, i bit da riservare saranno 3...

ORIGINAL ADDRESS	10	NET-ID	HOST-ID
"	10	NET-ID	HOST-ID
SUBNETTED ADDRESS	10	NET-ID	SUBNET-ID HOST-ID
"	10	NET-ID	SUBNET-ID HOST-ID

Questa nuova struttura degli indirizzi si chiama SUBNETTING.

Accanto all'IP address viene innata la SUBNET MASK; essa è una parola di 32 bit in cui sono presenti tanti 1 quanto sono lunghi il NET-ID e il Subnet-ID e tanti 0 quanto è lungo l'Host-ID.

IP ADDRESS	10	NET-ID	SUBNET-ID	HOST-ID
SUBNET MASK	11	....	11100...00	01-101101

Il Subnetting può essere di due diversi tipi:

- **STATICO:** Le sottoreti che vengono ricavate dalla stessa rete, hanno subnet mask uguali;

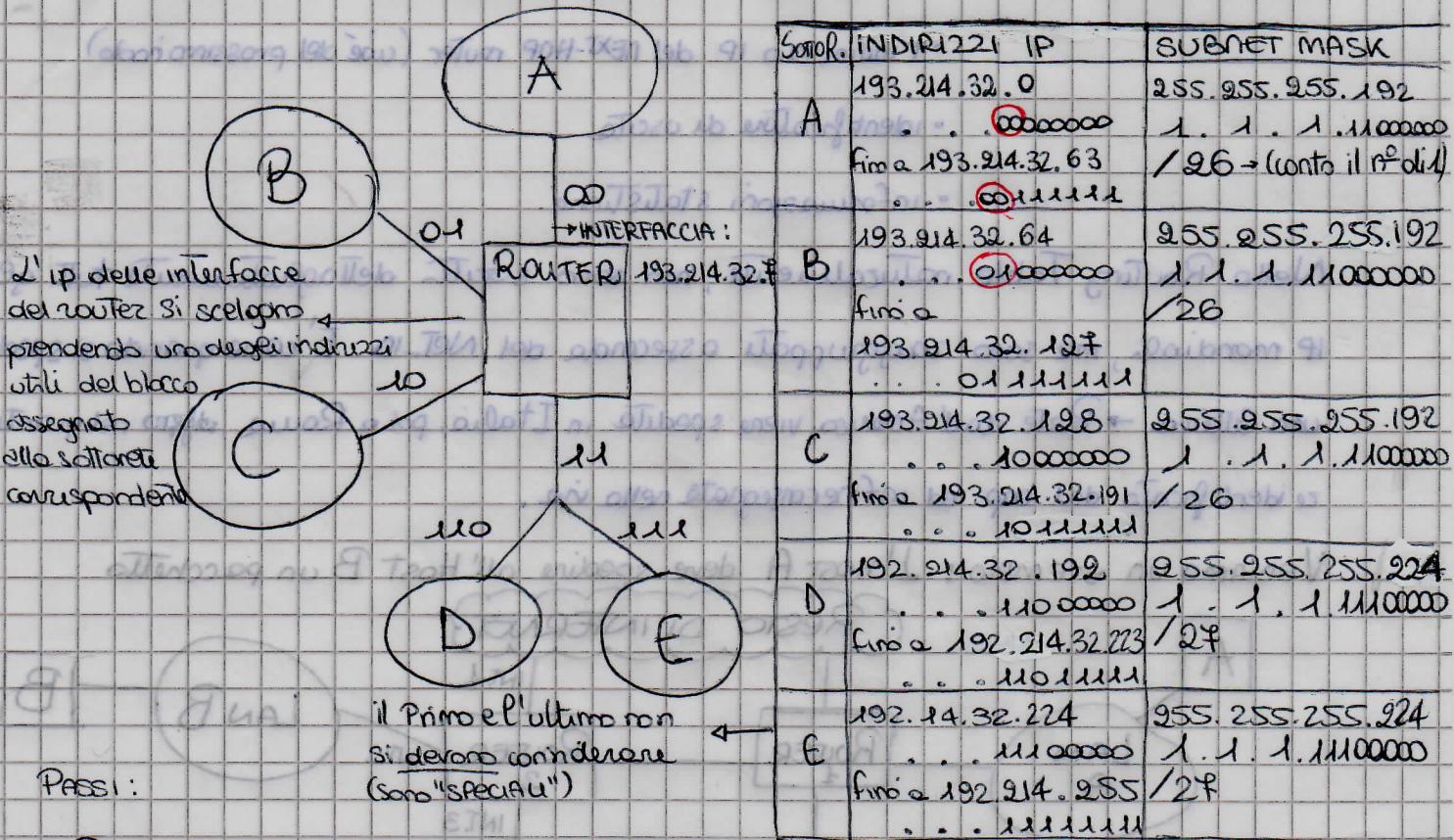
Questo modo è semplice da implementare ma comporta un alto spreco di indirizzi.

In sottoreti di piccole dimensioni.

- **VARIABILE:** Ogni sottorete ha una propria maschera, a seconda degli indirizzi di cui necessita.

# ESEMPIO DI ASSEGNAZIONE DI INDIRIZZO con SUBNETTING A LUNGHEZZA VARIABILE

- Dato l'indirizzo di classe C : 193.214.32.0 assegnare ad ognuna delle 5 sottoreti un gruppo di indirizzi IP, sapendo che A, B, C possiedono 50 host (tra gli host è contata anche l'interfaccia del Router) D, E // 30 host



1. Parto dalla sottorette con più host, in questo caso sono A, B, C.

Per avere 50 host su ogni sottorette, ho bisogno di 6 bit per l'Host-ID e quindi  $8 - 6 = 2$  di Subnet-ID

2. Con 2 bit di Subnet-ID posso suddividere i miei indirizzi tra 2 sottoreti (quindi include la sottorette D+E)

3. Assegno i subnet-ID: A → 00, B → 01, C → 10, D+E → 11

4. D+E devo risuddividerlo (in più ho bisogno solo di 5 bit dell'Host-ID) e quindi uscirò un ulteriore bit per il subnet-ID. Quindi D → 110, E → 111

5. Ho finito di assegnare le subnet-ID quindi posso compilare la tabella

(sotto ogni IP ho scritto l'ultimo byte in binario e cerchiato in rosso il subnet-ID)

6. Per assegnare gli indirizzi: I primi 3 byte sono fissi, l'ultimo (lo scrivo prima in binario)

Io calcolo prima scavendo il subnet-ID (es. 00) poi t. tt. zeri, dopo lo trasformo in decimale. Per avere l'indirizzo finale pongo (in binario) lo subnet-ID e poi tutti 1 dopo traduco.

## INDIRIZZAMENTO IP

L'indirizzamento IP oppure Routing sfrutta la suddivisione degli indirizzi IP.

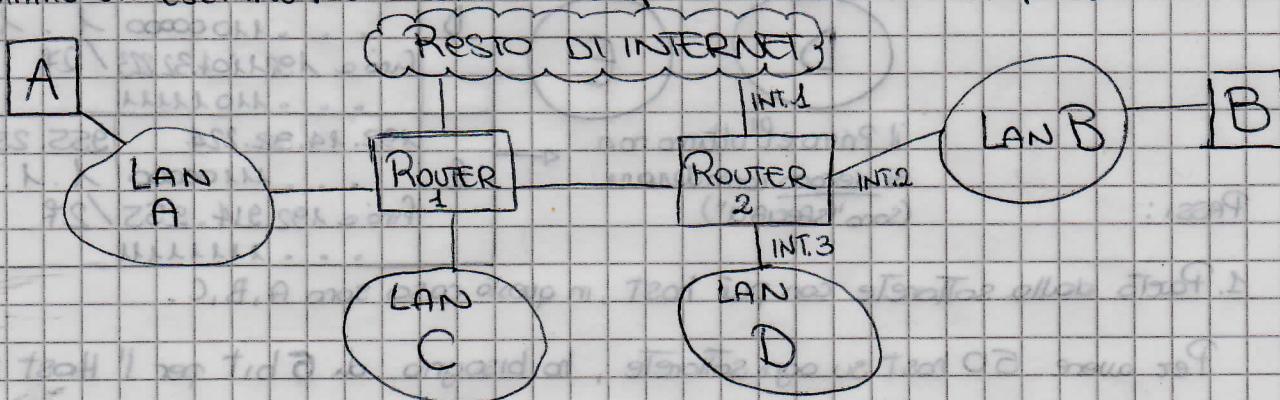
Per scegliere dove inviare un pacchetto per farlo arrivare a eff. Host finale, sia Router che anche l'host sorgente sfruttano la propria tabella di Routing (Routing Table).

Essa è composta da:

- l'indirizzo IP di destinazione
- l'indirizzo IP del NEXT-HOP router (cioè del prossimo nodo)
- identificatore di uscita
- informazioni statistiche

Nella Routing Table, naturalmente, non sono scritti dettagliatamente tutti gli IP mondiali, ma sono raggruppati secondo del Net-ID. E' come quando si spedisse una lettera → Parte dall'America, viene spedita in Italia, poi a Roma, dopo nel quartier re identificato dal cap ed infine consegnata nella via.

VEDIAMO UN ESEMPIO: L'Host A deve spedire all'Host B un pacchetto



- L'HOST A inserisce nel pacchetto il proprio IP, nel campo SOURCE ADDRESS, e l'IP di B nel DESTINATION ADDRESS. (L'IP di B può essere trovato grazie al protocollo DNS che converte indirizzi mnemonic in IP corrispondenti → Possiamo vedere la conversione grazie all'applicazione DNS Look Up online)
- A controlla nella propria routing table se B appartiene alla sua sottorete (così usa direttamente l'interfaccia di rete), la risposta è NO e quindi il pacchetto deve essere inviato al DEFAULT GATEWAY (Default Router)

Però, per inviarlo A deve trovare il MAC Address del Router (naturalmente se B fosse appartenuto alla stessa rete il mac da trovare sarebbe stato direttamente il suo)

Quindi A spedisce un messaggio ARP chiedendo il mac relativo all'IP del gateway predefinito

## VEDI: "APPROFONDIMENTO ARP"

Router 1 risponde con il proprio MAC che viene inserito nell'header del frame nel campo di destinazione.  $\Rightarrow$  Il pacchetto viene spedito.

• Router 1 spedisce l'unità informativa e mette l'IP di destinazione.

Confronta l'indirizzo con la propria tabella

### CRITERI DI RICERCA

1. Destination Address completo

2. Destination Net-ID (Prefisso)

3. Default Router

4. Emette un messaggio ICMP  $\rightarrow$  Dichiara l'host destinazione irraggiungibile

Legge che quell'IP deve essere inviato al Router 2. Così invia un messaggio ARP in modo da scoprire il suo MAC da inserire nel frame. Infine spedisce il pacchetto.

• Arriva a Router 2, legge l'IP e scopre che B fa parte della sottorete che si trova sull'interfaccia 2. Manda un messaggio ARP e scopre il MAC address di B.

Invia finalmente il pacchetto che arriverà a destinazione.

OSS. L'IP di destinazione e di origine non variano mai, vengono solo modificati i MAC address, che servono per spedire il frame fisicamente da una sottorete all'altra.

In questo esempio sono stati usati 2 diversi indirizzamenti:

INDIRIZZAMENTO DIRETTO = usa l'interfaccia collegata direttamente alla sottorete

(ROUTER 2  $\rightarrow$  LAN B)

// INDIRETTO = sfrutta il next-hop (ROUTER 1  $\rightarrow$  ROUTER 2)

Ogni oggetto collegato ad Internet ha un proprio IP, quindi anche lavatrici, televisori, frigoriferi... Ciò sta facendo esaurire la disponibilità di indirizzi, quindi l'occupazione che assegna i blocchi (IANA) sta cercando di trovare una soluzione.

Le idee che per ora circolano sono:

1. Ricidare IP non più usati
2. Creare una nuova versione (ora uscirà da 4 da 32 bit), sarebbe da 6 da 128 bit.

Ciò però comporterebbe una modifica di tutte le routing table  $\rightarrow$  Long-Term Solution

Gió nel 1990, cioè solo dopo 10 anni dalla struttura Classful e 6 dal Subnetting, si evidenziavano due grossi problemi:

1. ESAUIMENTO DEGLI INDIRIZZI IP: usati molti indirizzi di classe B (con alti sprechi) e pochi di classe C considerati troppo piccoli.
2. CRESCITA DEGLI ENTRIES DELLE ROUTING TABLE: tra il 1991 e il 1995 raddoppiavano le proprie dimensioni ogni 10 mesi. Quindi aumentava il tempo di processamento e le dimensioni della memoria.

Per avere una soluzione a breve termine furono introdotti 3 nuovi punti:

- Classless Inter Domain Routing (CIDR) [RFC 1518]
- Una nuova politica di allocazione [RFC 2050]
- CLASSLESS INTER DOMAIN ROUTING (CIDR)

Come abbiamo detto, molti indirizzi C non venivano usati in quanto consentivano di avere solo 254 ( $2^8 - 2$ ) host. Allora si pensò al CIDR, cioè unire un certo numero di blocchi contigui di indirizzi. Questa modalità è chiamata SUPERNETTING, funziona come il SUBNETTING ma invece di sfornare nella parte HOST-ID, subisce alcuni bit dalla parte NET-ID.

Oltre ad un utilizzo con meno sprechi degli indirizzi IP, CIDR migliorava le Tabelle di Routing mettendo un unico prefisso (bit più significativi) che coinvolgeva o una singola sottorete o più sottoreti raggruppate (Supersottoreti).

Grazie a questo nuovo modo gli indirizzi di classe A e B venivano assegnati solo se strettamente necessari → NUOVA POLITICA DI ALLOCAZIONE

Possiamo essere assegnati blocchi consecutivi di classe C (fino a 64) con stesso prefisso.

Vennero ripianificati geograficamente tutti gli indirizzi di classe C.

ESEMPIO: all'Europa fu dato da 194.0.0 a 195.255.255

Tutti gli host europei hanno come prefisso .194 (11000010) o .195 (11000011)

Tutto questo consente la crescita delle dimensioni della Routing Table.

Ogni sottorete è formata da un entry, i router capiscono dove mandare il pacchetto

grazie alla maschera (f.d. 255.255.255.0) (maschera di broadcast).

Concluso: Ogni router si sente la richiesta con codice risposta "OK".

Esempio:

## 1. ASSEGNAZIONE INDIRIZZI IN NORD AMERICA $\rightarrow$ 198.0.0.0/8

Un INTERNET SERVICE PROVIDER (ISP) chiede 2048 blocchi di indirizzi di classe C

- trasformo 198.0.0.0 in binario

11000110.0000000.0000000.0

↳ byte host

Per avere 2048 blocchi ho bisogno di 11 bit

$$(2048 = 2^{11})$$

Quindi ad esempio i blocchi inizieranno da

198.24.0.0 (11000110.0001000.0000000.0) w } CDR MASK

198.31.255.0 (11000110.0001111.1111111.0)  $\rightarrow$  198.24.00/13

Un altro ISP chiede 16 blocchi

Punto sempre da 11000110.0000000.0000000.0

Questa volta ho bisogno di 4 bit ( $2^4 = 16$ )

Quindi per esempio potrebbero partire da

198.24.16.0 (11000110.0011000.0001000.0) w } CDR MASK

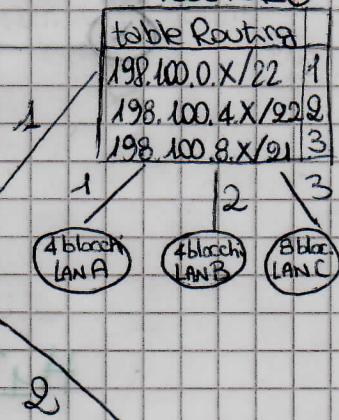
198.24.31.0 (11000110.0011000.0011111.0)  $\rightarrow$  198.24.16.0/20

Ora vediamo un esempio che tratta dell'utilizzo dei prefissi e delle maschere

ROUTER 3

ROUTER 1		
table Routing		
IP	MASK	INTERFACCIA
198.100.6.22		
198.100.32.X	/18	1
198.100.0.X	/19	2
198.100.128.X	/17	3

ROUTER 2		
table Routing		
IP	MASK	INTERFACCIA
196.100.0.X	/20	1
196.100.16.X	/20	2



Il router 1 legge l'ip 198.100.6.22 e gli applica OGNI MASCHERA delle proprie entry. 198.100.6.22 in decimale sarebbe 11000110.01100100.00000110.00001010

Applico la maschera 18 (cioè zero a 0 gli ultimi 32-18 bit) perciò rimane

11000110.01100100.00000000.00000000 in decimale 198.100.0.0 = non combacia

Applico la maschera 19 ed ottengo in decimale 198.100.0.0  $\Rightarrow$  coincide con entry 2

Applico la maschera 1<sup>st</sup> ed ottengo di nuovo 198.100.0.0  $\Rightarrow$  non coincide con entry 3

Perciò il mio pacchetto viene trasferito al router 2 sull'interfaccia 2

- Il Router 2 legge l'IP destinazione 198.100.6.22 ed anche lui applica per ogni entry la maschera corrispondente.

Applico la maschera 20 ed ottengo 198.100.0.0  $\Rightarrow$  coincide solo con l'entry 1 quindi il pacchetto arriva al router 3 tramite interfaccia 1

- Il Router 3 legge l'IP 198.100.6.22 e gli applica la propria maschera

Applico maschera 22 ed ottengo 198.100.4.0  $\Rightarrow$  combacia con l'entry 2

Applico la maschera 21 ed ottengo 198.100.0.0  $\Rightarrow$  non combacia con entry 3

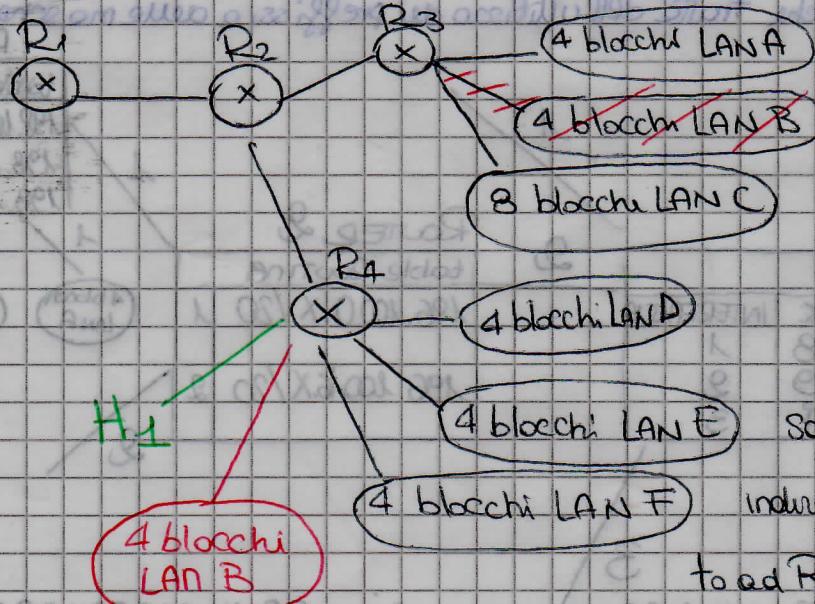
Quindi il pacchetto viene spedito sulla seconda interfaccia continuando il suo viaggio fino all'host finale.

Nell'esempio il mio IP, a cui applicavo la maschera, coincide solo con un entry. Potrebbe capitare che invece, l'IP "mascherato" sia uguale a più entry.

Per decidere su quale interfaccia inviarlo, il Router applica le regole: LONGEST

PREFIX MATCHING, cioè scelgo l'entry con prefisso maggiore (=maschera più lunga)

Come posso spostare un intero sottoretro su esempio da 4 blocchi?



Voglio spostare LAN B  
e collegarlo al router 4

Per spostare un'intera sotto rete basta che modifichi le tabelle di Routing, precisamente quelle di R2 (il pacchetto

indirizzato alla lan B dovrà essere inviato ad R3), quelle di R4 (dovrà aggiungere una riga contenente il prefisso e la maschera relativa a LAN B) e cancellare l'interfaccia di LanB da R3.

Se invece volessi spostare solo un host (ad esempio di LAN A e collegarla a R4):  
devo scrivere l'IP di H1 (quindi con maschera /32) sia in R2 (con next hop R4)  
sia in R4.

Io posso spostare anche solo un blocco ad esempio dei 4 della Lan B.

Per far questo ho due modi:

1. Sposto i 254 utenti uno per uno, quindi interendo ogni loro indirizzo IP in R2 e R4 e mettendoli con maschera 32

2. I 4 blocchi iniziamo ad esempio da 193.64.4.0 fino a 193.64.4.255.

Facciamo finta che voglio spostare il blocco due, quindi quello che va da

193.64.5.0 fino a 193.64.5.255, ed attaccarlo al Router R4.

Affinché R2 capisca che un pacchetto indirizzato al blocco 2 non debba andare da R3, dovrà inserire una riga alla sua Routing Table.

Se la tabella di R2 fosse per esempio così:

193.64.0.0 /20 → R3 (•)

193.64.16.0 /20 → R4

Dovrà aggiungere una 3<sup>a</sup> riga con maschera maggiore a (•) [così da non creare ambiguity]. Quindi, per esempio:

193.64.5.0 /24 → R4

## Protocollo DHCP (Dynamic Host Configuration Protocol)

Come sappiamo un host per comunicare in internet deve conoscere questi campi:

\* il proprio IP address

\* il SUBNET mask

\* il GATEWAY predefinito

\* il SERVER DNS (ha il compito di tradurne l'indirizzo mnemonico in IP)

Questi campi non sempre sono statici, qui entra il gioco il DHCP che li autoconfigura.

I server DHCP hanno a disposizione un certo numero di IP che assegnano dinamicamente agli host che vogliono accedere alla rete.

Gli IP vengono assegnati ad un terminale per un certo tempo (GESTIONE STATISTICA).

DEGLI INDIRIZZI) Questo protocollo è stato introdotto per evitare "sprechi" sull'attribuzione di indirizzi IP. Infatti esso consente il riuso degli IP e anche il ritiro delle proprietà durante una stessa sessione. Supporta anche i dispositivi mobili.

Il DHCP supporta tre meccanismi per la gestione:

1. AUSCIAZIONE AUTOMATICA → assegnazione permanente dell'IP

2. " DINAMICA → " per un tempo limitato (rinnovabile)

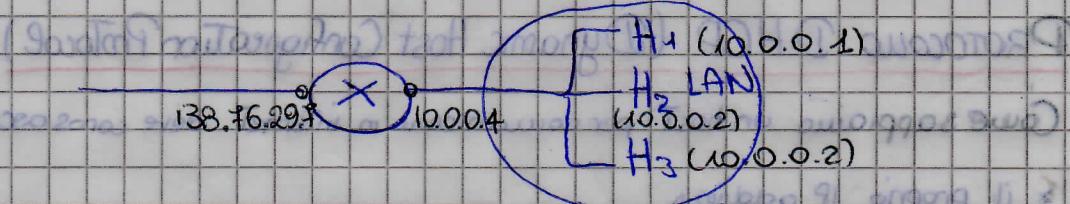
3. " MANUALE → " tramite amministratore di rete

Funzionamento:

- Il nuovo host invia un DHCP\_DISCOVER in maniera Broadcast per trovare il server DHCP.
- Il DHCP risponde con un DHCP\_Offer in cui assegna un indirizzo IP.
- L'HOST invia al server un DHCP\_REQUEST per richiedere gli ulteriori parametri di configurazione oppure chiede l'estensione temporale dell'utilizzo dell'IP.
- Il DHCP risponde con un DHCP\_ACK in cui ci sono le configurazioni richieste.

### NAT (NETWORK ADDRESS TRANSLATOR)

Il NAT è un'ulteriore tecnica per ridurre l'occupazione di indirizzi IP. Esso sfrutta le INTRANET. Ogni terminale di una sottorete ha un proprio indirizzo IP privato, cioè non può essere usato all'esterno di quella LAN. Essa è collegata ad un Router, il quale possiede la funzione NAT, che possiede l'unico IP pubblico. Ogni pacchetto destinato ad un host della sottorete deve riportare quell'IP unico.



Quindi un Router NAT nasconde i dettagli di una intranet al mondo esterno.

Questa tecnica è molto vantaggiosa, perché intere LAN sono rappresentate da un unico IP pubblico. Rendono anche più semplice la gestione, ad esempio cambiare indirizzi dei terminali senza che tutta la rete globale lo saprà.

Funzionamento:

Il NAT sfrutta un altro indirizzo, oltre all'IP, cioè quello specifico allo strato di Trasporto: LA PORTA.

- Il ROUTER NAT riceve un pacchetto da un host che vuole comunicare col mondo esterno.
- Modifica l'indirizzo di origine con l'IP pubblico e modifica anche la porta scegliendo una casuale che non sia una WELL-KNOWN PORT (numeri di porta conosciute ed usate).

Aggiorna la propria TABELLA DI TRADUZIONE

Ad esempio H2 (IP: 100.0.2) vuole comunicare con HB (IP: 100.30.7.3)

La porta uscente da H2 è 3348

Il Router-NAT segna nella Tabelle

LATO WAN			
IP PUBBLICO	PORTA	IP PRIVATO	PORTA
138.76.29.7	5001	10.0.0.1	3345

• Avere la risposta dalla destinazione che avrà come DESTINATION ADDRESS l'IP del Router e come Porta quella inventata.

• Il router legge il Datagramma e modifica la destinazione con l'IP privato che sulla Tabelle di Traduzione corrisponde a quella porta casuale.

• L'Host riceve l'Unità.

Quindi HB manderà un datagramma con

IP DESTINATION ADDRESS: 138.76.29.7 → CAMBIO 10.0.0.1

PORT DESTINATION : 5001 → NAT 3345

• all'esterno una rete è collegata ad un Router-NAT sembra un unico nodo.

Naturalmente il Router-NAT ogni volta che riceve un datagramma deve operare tutti i controlli checksum quindi avrà un piccolo tempo di processamento.

Se ricevo un'unità dall'esterno, il router dovrà tradurla ed inviarla al giusto host. Per far ciò ad esempio potrebbe associare sempre una determinata porta ad un determinato terminale oppure sfruttare i protocolli Universal Plug and Play e IGD<sup>(\*)</sup>.

Ci sono però alcuni punti che vengono contestati a questa tecnica:

• I Router-NAT operano anche a livello 4 e quindi è contro ai principi dell'architettura.

• Un host non è visibile dall'esterno (se commettessi operazioni illegali non sarebbe rintracciabile).

• Incompatibile con il protocollo ICMP.

• Interferisce con alcune applicazioni.

• Se ci fosse un cambio di indirizzi IP bisognerebbe recalcularne il checksum dei pacchetti UDP e TCP.

(\*) Internet Gateway Device Protocol. Ultimo modo è usare il Relay, cioè il NAT fa da ponte.

tra il client NAT e il client. (Usato ad esempio da SKYPE)

## INSTRADAMENTO

La prima funzione dello strato di Rete, è inoltre, si occupa di processare il pacchetto (leggere l'IP, mascherarlo per trovarlo sulle Tabelle di Routing...), insomma tutto quello che abbiamo visto fino ad ora.

La seconda è quella dell'INSTRADAMENTO che in parole povere è la compilazione delle Tabelle di Routing e quindi la determinazione delle strade.

Per far ciò i Router si scambiano dei pacchetti di controllo ed utilizzano appositi protocolli di routing per leggerli e compilare le Tabelle.

Grazie a questi protocolli, i nodi riusciranno ad avere un'idea della Topologia di Rete.

Essi servono anche ad implementare degli Algoritmi di Routing, che servono per calcolare i cammini migliori, cioè con minimo costo, minimo ritardo, minimo numero di hop da attraversare e massima affidabilità.

I path migliori non saranno sempre gli stessi, come la Topologia di rete, infatti possono guastarsi dei link o aumentare del traffico su un collegamento oppure aggiungersi una nuova connessione. Tutto questo comporta un aggiornamento periodico delle Tabelle, precisamente ogni 30 secondi, grazie all'invio dei pacchetti di controllo dei protocolli di Routing.

I requisiti che devono avere questi protocolli sono:

- Risposta Alla Variazione di STATO (cambiamenti Topologici, stato di congestione, questi)
- OTTIMIZZA (migliore utilizzo delle risorse di rete, minimizzazione dei cammini)
- ROBUSTEZZA (continuità del servizio anche in condizioni anomale (congestione alta, questi..))
- SEMPLICITÀ (bassa complessità di elaborazione)

L'istradamento può essere:

- STATICO: i cammini sono configurati manualmente e non variano mai. Usati in reti piccole in cui è prevedibile il traffico oppure per imporre percorsi particolari
- Utilizzato anche per dare un instradamento di default (Router predefinito)
- DINAMICO: sostiene le variazioni dello stato di rete. I cammini vengono calcolati automaticamente sulla base di informazioni recente per mezzo dei protocolli di routing

(9.2) Le Tabelle di Routing sono costituite da: (visibile col comando ROUT PRINT)  
« IP destinazione » « Subnet Mask » « IP next-hop » « Interfaccia » « METRICA »  
E sono formate da tante righe quante sono i nodi o sottoreti a cui mandare pacchetti.  
Per ridurre queste entry la rete IP è stata gerarchizzata, cioè suddivisa in zone (Domini, sistemi autonomi, ecc.). I router non hanno tutta stessa importanza.  
E' una soluzione efficiente in quanto non si cerca subito lo specifico host ma prima la rete, poi la città, le sottoreti ed infine il singolo terminale.

I router non conoscono l'intero cammino ma solo il Next-hop.

Quando ricevono un pacchetto operano questi passi:

- × ESTRAE L'IP ADDRESS DELLA DESTINAZIONE
- × RICERCA L'INDIRIZZO NELLA ROUTING TABLE APPUCANDO IL "LONGEST PREFIX MATCHING"
- × SE NON LO TROVA SI AVRAE DEL ROUTER DEFAULT (ROUTER PIÙ POTENTE CON UNA PIU' AMPIA TABELLA)
- × SE NEANCHE IL ROUTER DEFAULT LO TROVA, ALLORA PREPARE UN MESSAGGIO ICMP E LO INVIÀ ALL'HOST SORGENTE.

Per calcolare il next-hop il router si avvale dell'algoritmo di routing che si basa sull'utilizzo della metrica. Questo campo rappresenta il costo per arrivare a quella destinazione. Esso dipende da vari fattori (lunghezza del filo, host all'interno, utenti...) ed è sempre aggiornato (come la Tabella stessa).

Gli algoritmi sfruttano anche la Topologia della rete contenuta nel TOPOLOGICAL DATABASE dei router.

Come abbiamo detto prima, la rete IP è gerarchica e quindi divisibile in zone. Alcune di queste sono i SISTEMI AUTONOMI (Autonomous System - AS) e un insieme di host e router controllato da un'autorità amministrativa (es. INTERNET SERVICE PROVIDER).

Un particolare AS è chiamato "Core AS" e costituisce il back bone di internet.

I sistemi autonomi sono collegati tra di loro grazie a dei router chiamati di confine.

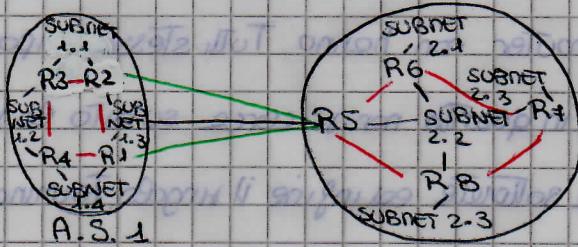
I protocolli di routing che girano all'interno di un sistema autonomo sono chiamati

Interior Gateway (come antico per chiamare il Router) Protocols (IGP).

Però un AS ha bisogno di confrontarsi anche con altri perhangere su internet.

I protocolli che girano su più sistemi si chiamano Exterior Gateway Protocols (EGP)

Essi girano anche sui router di confine. E' da sottolineare che molti percorri non prendono una determinata strada che attraversa un AS preferendone un altro non solo per problemi tecnici ma anche per questioni politiche ed amministrative



### Algoritmi di Instradamento

La rete puo' essere rappresentata come un GRAFO PESATO  $G = (N, E, c)$

dove  $N$  = insieme dei nodi,  $E$  = insieme degli archi,  $c$  = costi associati ai nodi.

Il costo di un cammino è definito dalla somma di tutti i costi degli archi lungo il cammino (se i link hanno costo unitario, l'algoritmo cerca la strada con meno hop da attraversare)

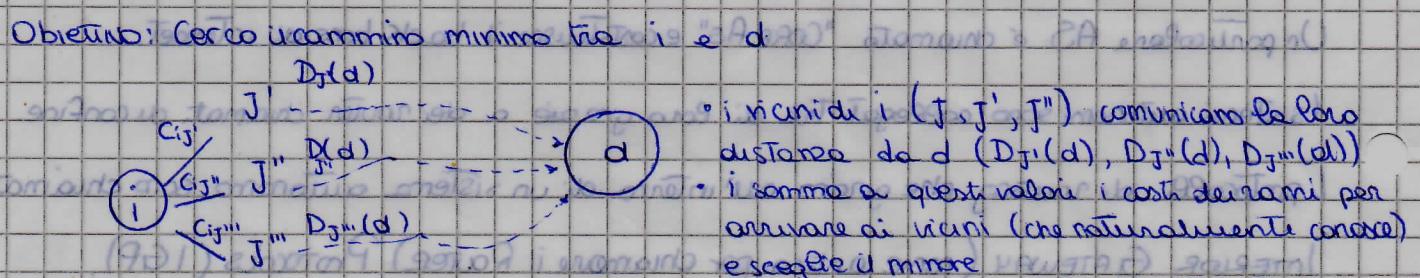
Esistono due diversi algoritmi: 1) Bellman-Ford, 2) Dijkstra

1. Algoritmo Bellman-Ford: Ha un approccio distribuito (non conosce la topologia della rete, il nodo comunica con solo i suoi vicini, questi a loro volta comunicano con i propri vicini e così). La famiglia dei protocolli che lo implementano si chiama DISTANCE VECTOR PROTOCOLS.

2. Algoritmo di Dijkstra: L'approccio è centralizzato (cioè i router conoscono l'intera topologia della rete). La famiglia che lo implementa si chiama LINK STATE PROTOCOLS.

Algoritmo Bellman-Ford: I router vicini si scambiano i Distance Vector = DV (Destinazione, distanza), grazie a

questo ogni nodo puo' definire il next-hop migliore. Obiettivo: Cerco il cammino minimo tra i nodi  $d$  e  $a$ .

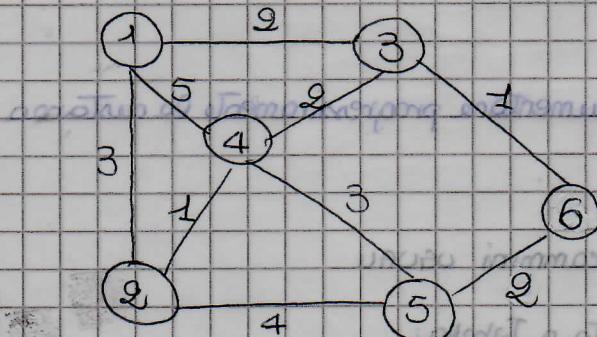


Naturalmente anche  $J^1, J^2, J^3$  hanno eseguito questi passi per conoscere la loro distanza da  $d$ .

## Funzionamento Algoritmo:

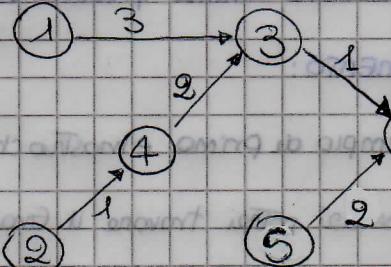
OBIETTIVO: scoprire le distanze e il next-hop per ogni nodo per arrivare alla destinazione.

Vediamo un esempio:



Voglio calcolare i DV di tutti i nodi per arrivare

GRADO  
MINIMO



ITERAZIONE	Nodo 1	Nodo 2	Nodo 3	Nodo 4	Nodo 5
INIZIO	(-1, $\infty$ )				
1	(-1, $\infty$ )	(-1, $\infty$ )	(6, 1)	(-1, $\infty$ )	(6, 2)
2	(3, 3)	(5, 6)	(6, 1)	(3, 3)	(6, 2)
3	(3, 3)	(4, 4)	(6, 1)	(3, 3)	(6, 2)

inizializzazione

6 parla con i vicini 3 e 5

5 e 3 parlano con i vicini

4 per raggiungere 6 parla per 3 e passa per 2 e 1 = 3

Ora i rimanenti vicini parlano con i propri

Questo algoritmo deve essere ripetuto per ogni destinazione (così da avere una tabella completa)

→ oltre al numero di iterazioni indica il massimo di hop da attraversare

Ogni cella dell'ultima riga rappresenta una riga della Routing Table del rispettivo nodo

A d'esempio la tabella del nodo 2 avrà una riga composta da:

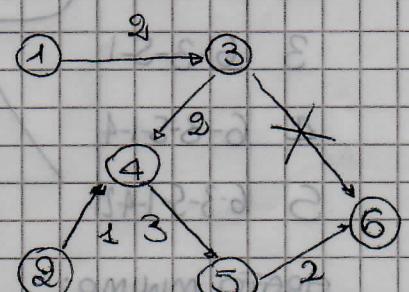
<< IP DESTINATION : IP di 6 >> << SUBNET-MASK >> << IP NEXT-HOP : IP di 4 >> << METRICA : 4 >>

N.B. la subnet-mask in un link è sempre 30 (infatti ho bisogno solo di 4 indirizzi (2

"speciali" + 2 per i router) quindi 2 bit per l'Host-ID).

Se il link tra 3 e 6 si guastasse, cosa succederebbe?

ITERAZIONE	Nodo 1	Nodo 2	Nodo 3	Nodo 4	Nodo 5
INIZIO	(3, 3)	(4, 4)	(6, 1)	(3, 3)	(6, 2)
1	(3, 3)	(4, 4)	(4, 5)	(3, 3)	(6, 2)
2	(3, 2)	(4, 4)	(4, 5)	(5, 5)	(6, 2)
3	(3, 2)	(4, 6)	(4, 7)	(5, 5)	(6, 2)



Se il nodo 3 non avvisava del guasto, 4 continuava ad inviare i propri pacchetti destinati a

6 a lui, ma essendo il link tra 3 e 6 guasto glieli rispediva. Si creava un effetto "Ping pong" che

creare un contagio infinito. Ci sono alcune Tecniche per evitare questi loop infiniti. Una di queste è lo SPLIT HORIZON con POISON REVERSE: il router invia a tutti il proprio DV settato ad  $\infty$  cioè per lui la destinazione è infinita.

## ALGORITMO DI DIJKSTRA

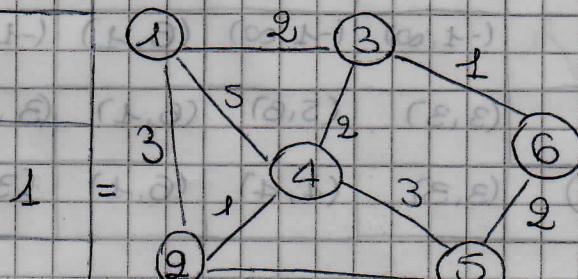
Trova il cammino minimo procedendo in modo da aumentare progressivamente la distanza.

### FUNZIONAMENTO:

Uno è l'esempio di prima e mostri che verranno due cammini uguali.

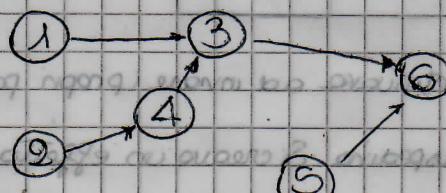
In alcuni esercizi potrai trovare il Grafo rappresentato a Tabella:

NODI	1	2	3	4	5	6
1	0	3	2	5		
2	3	0		1	4	
3	2		0	2		
4	5	1	0	3		
5			4	3	0	2
6				1	2	0



Passo	N	metrica	Next-hop
0	6	D(1), P(1)	
1	6-3	3, 3	1, 3
2	6-3-5	3, 3	6, 5
3	6-3-5-1	6, 5	LA CANCELLO PERCHE' E' IL MASSIMO CHE POSSO AVERE
4	6-3-5-1-4	4, 4	
5	6-3-5-1-4-2		

### GRAFO MINIMO:



I cerchi sono le righe della Tabella routing

corrispondenti al nodo. Per avere una tabella completa darei ripetere l'algoritmo partendo da ogni nodo

Protocolli di Routing

I protocolli di instanciamento, cioè quelli che implementano gli algoritmi, sono INTERIOR GATEWAY PROTOCOL (IGP), perciò grano all'interno di un unico sistema autonomo.

Sono due i protocolli più famosi:

1. RIP (Routing Information Protocol) di tipo DISTANCE VECTOR → (Bellman-Ford)

2. OSPF (Open Shortest Path First) di tipo LINK STATE → (Dijkstra)

1. RIP:

E' stato il primo ad essere pensato. Ogni router invia al proprio vicino le sue tabelle di routing; esse contengono tutte le sottorete a cui puo' inviare pacchetti. Quindi i messaggi che si inviano sono molto pesanti. Il RIP, e' usato per piccole-medie reti.

I router si scambiano due tipi di messaggi:

- REQUEST: chiede ai vicini le distance vector

- RESPONSE: annuncia le distance vector

Gli aggiornamenti vengono scambiati ogni 30 secondi.

I messaggi elencano un massimo di 25 sottorete ed hanno questa struttura:

HEADER
IP ADDRESS 1
SUBNET MASK
NEXT HOP
METRIC
:
IP ADDRESS 25
SUBNET MASK
NEXT HOP
METRIC

Riga 25^ del  
ROUTING  
TABLE

Funziona esattamente come l'algoritmo Bellman-Ford

Se un nodo non riceve notizie dal suo vicino per 180 sec allora il nodo adiacente viene considerato spento o guasto. Perciò RIP modifica la tabella e propaga la notizia ai vicini, se anche loro modificheranno la propria allora propagheranno l'errore.

2. OSPF: immagine mostra una rete con 6 nodi e 9 link

Usato per reti grandi (geografiche). I router si scambiano informazioni per avere l'immagine delle Topologie di rete. I messaggi che vengono scambiati sono i LINK STATE

Advertisements (LSA) e vengono trasmessi tramite la tecnica di flooding. Essi sono emessi quando un router contatta un nuovo link, quando un link si guasta, quando varia il costo di un link, ogni tot di tempo.

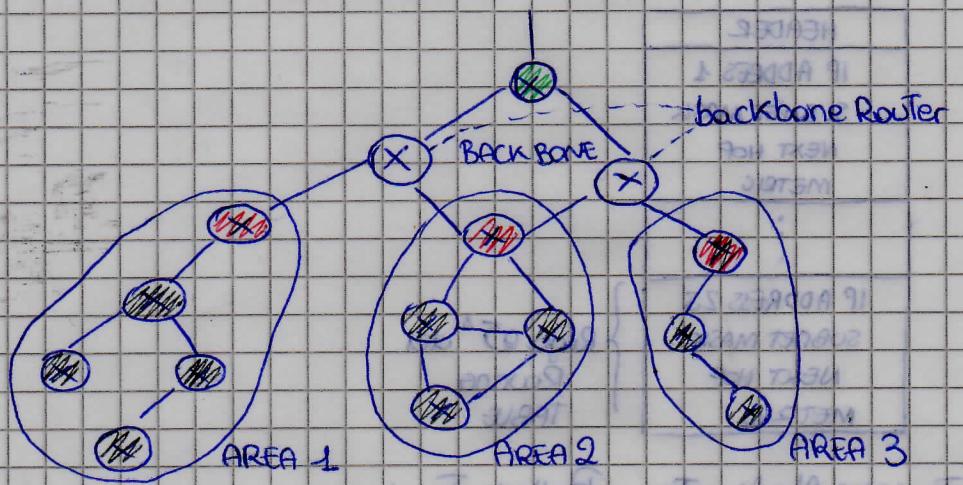
I LSA sono rilanciati da un router su tutte le sue interfacce tranne da quelle da cui è stato ricevuto. Essi hanno dei numeri di sequenza o riferimenti temporali per evitare di rifacciare pacchetti già inviati e consentire un miglior confronto.

Quindi i LSA "inondano" la rete e perciò esplorano tutti i possibili cammini. E' estremamente affidabile la tecnica del Flooding. Però questo invio costante crea un traffico che dipende dalle dimensioni della rete e può essere molto elevato. Per evitare questo problema OSPF adotta un istru-

damento di tipo gerarchico. Una rete IP viene suddivisa in aree interconnesse da un area di backbone. I router sono divisi in:

- \* Intra-Area Router (IAR): router interni all'area, inviano LSA agli altri router dell'area
- \* Area Border Router (ABR): router collegati a 2 o più aree (sono gerarchicamente i più alti)
- \* AS Boundary Router (ASBR): router al confine delle AS, scambiano LSA all'interno con informazioni sui percorsi esterni.

Questa modularità gerarchica permette di implementare meglio il protocollo.



L'OSPF è un protocollo pensato per le reti BACKBONE quindi molto rilevante, e molto evolu-

to e supporta anche metriche più evolute adattabili ai servizi che voglio avere.

### BORDER GATEWAY Protocol (BGP)

Il BGP è il protocollo che viene usato per far comunicare sistemi autonomi diversi. Quindi sono quelli che guardano tra router di bordo (o confine). È un protocollo sofisticato in quanto deve coordinare sistemi che potrebbero implementare diversi protocolli in più i

I router oltre a scambiarsi informazioni topologiche, stabiliscono le politiche. Queste implicano costi e limitatezze al traffico per attraversare alcune AS oppure di reti di passaggio a causa di questioni politiche o amministrative da parte di AS.

I messaggi BGP contengono:

- \* AS number: identificativo univoco di un AS a 16 bit

- \* AS path: lista di AS attraversati in un cammino (serve per far scegliere ai router strade che entrambano alcune AS o per scegliere più facilmente il percorso minimo)

Essi sono attraversati da delle connessioni TCP, aprono un vero e proprio scambio dati, come delle applicazioni.

I router interni devono sapere quali sono i router di bordo; quando ricevono un pacchetto che deve essere inviato all'esterno della propria AS, applicano la tecnica "Hot Potato": scelgono un router di confine a caso e gli passano l'unità senza preoccuparsi di nulla.

Ricapitolando:

I router hanno 2 diversi tipi di instradamenti:

- INTORNO AD UN AS → usano protocollo IGP

- VERSO ALTRI AS → uso del protocollo BGP