UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE ED INFORMATICHE
Corso di Laurea in Informatica

Il Livello Network

Parte I : IPv4

RETI DI CALCOLATORI - a.a. 2023/2024

Roberto Alfieri

Il livello Network: sommario

PARTE I

- Scopi del livello Network
- Commutazione di circuito e di pacchetto
- La famiglia dei protocolli TCP/IP
- Il protocollo IPv4: trama indirizzi, instradamento
- Protocolli di servizio per IPv4: ARP, ICMP, DHCP

PARTE II

- IPv6

PARTE III

- Algoritmi e protocolli di routing
- Distance Vector e Link State.

RIFERIMENTI

Reti di Calcolatori, A. Tanenbaum, ed. Pearson
Reti di calcolatori e Internet, Forouzan , Ed. McGraw-Hill

Scopi e servizi del livello Network

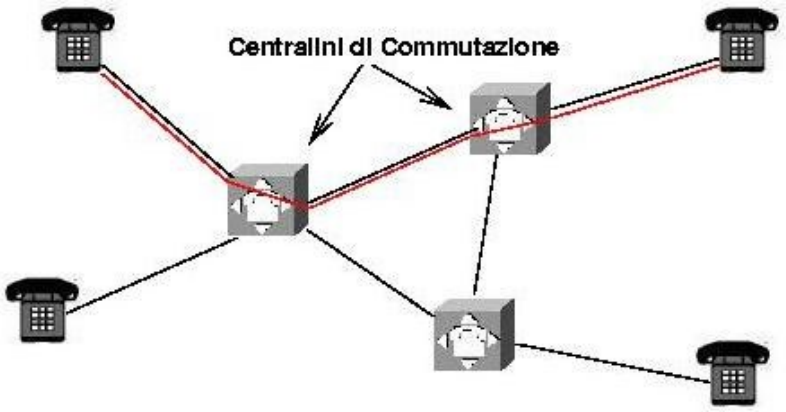
Estendere i servizi che il livello Data-Link offre a macchine connesse anche a macchine che non hanno una connessione diretta.
Compito fondamentale dello strato di rete è trasportare i pacchetti lungo tutto il percorso dal mittente al destinatario, attraversando tutti i nodi di transito dove sono possibili scelte alternative per le linee di uscita.
La funzione di collegamento di una linea di ingresso con una di uscita opportunamente scelta, che viene svolta nei nodi è detta **Commutazione** (Switching)

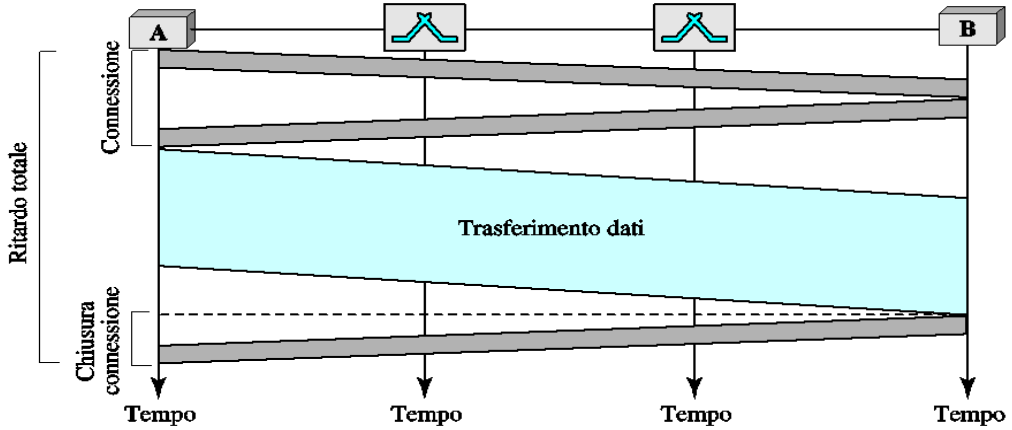
Le due tecniche di commutazione usate tradizionalmente nelle reti sono:

- **Commutazione di circuito** (utilizzata storicamente dai Provider di telefonia)
- **Commutazione di pacchetto** (utilizzata nelle reti di calcolatori)

Commutazione di Circuito

- I nodi di transito sono i Centralini di Commutazione (Manuali, Meccanici o Elettronici)
- L'algoritmo per la commutazione interviene all'apertura del canale fisico
- Nella fase di connessione vengono allocate le risorse necessarie
- Ritardo: è minimo nel trasferimento dati, ma è elevato in fase di apertura e chiusura della connessione
- Efficienza: le risorse allocate sono riservate anche se la connessione è inutilizzata. Questo non avviene per le telefonate, ma può avvenire per il trasferimento dati.

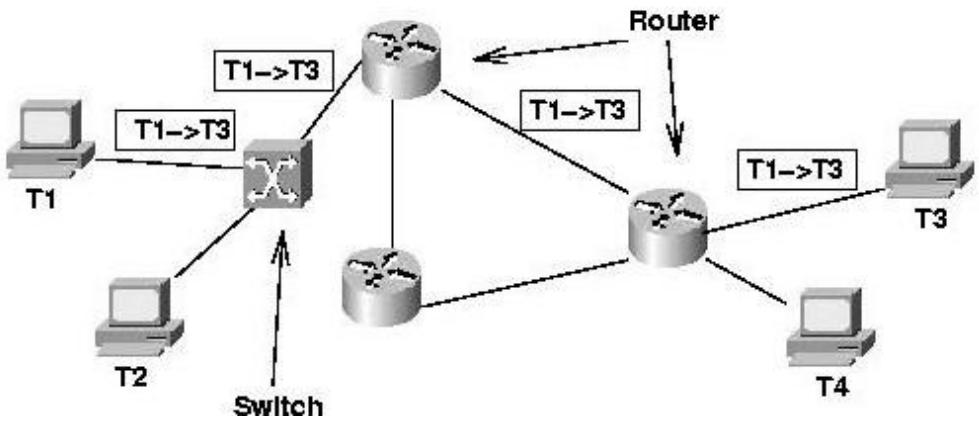




Commutazione di Pacchetto

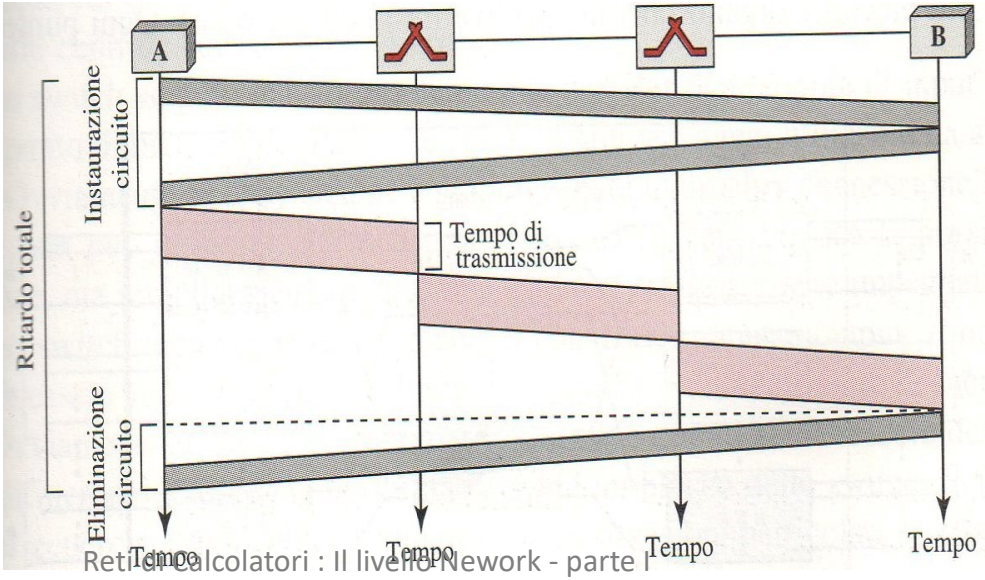
Commutazione di Pacchetto

- Comunicazione frazionata in “pacchetti”
- Algoritmo per la commutazione interviene sui pacchetti
- Esistono diversi tipi di nodi di transito a seconda della loro funzione:
  - Hub, Bridge, Switch, Router o Gateway.
- Esistono 2 tipologie di commutazione a pacchetto:
  - A circuito virtuale
  - A datagramma



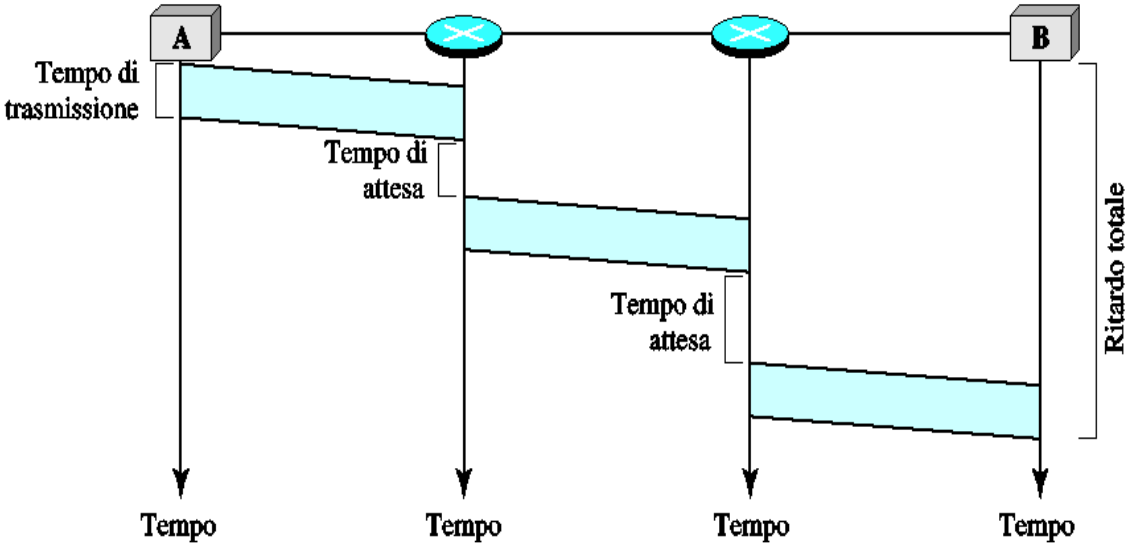
Commutazione di pacchetto a circuito virtuale

- Algoritmo per la commutazione interviene solo all'inizio per l'apertura del Canale Virtuale (VC).
- Ad ogni nuovo VC viene assegnata una etichetta; ogni router viene marcato con l'etichetta del VC e la relativa porta di uscita.
- I pacchetti seguono il percorso individuato
- Implementazioni principali:
  - ATM. E' la rete che utilizza la commutazione di pacchetto a circuito virtuale per la telefonia.
  - In internet è possibile creare isole a circuito virtuale con il protocollo MPLS
  - La versione 6 di IP supporta (anche) reti a circuito virtuale.



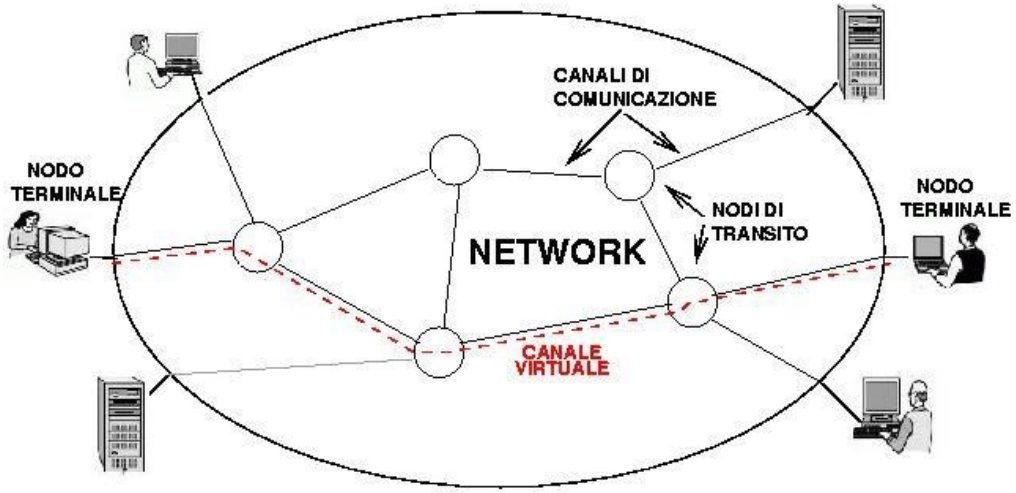
Commutazione di pacchetto a datagramma

- I pacchetti sono instradati in modo indipendente in base all'indirizzo di destinazione
- L'instradamento è determinato dai router attraversati in base "**tabelle di instradamento**" che ogni router costruisce dinamicamente mediante gli "**algoritmi di routing**".
- Pacchetti della stessa connessione possono seguire strade diverse.
- Implementazioni principali: IPv4 e IPv6.



Routing

Il routing è quella parte del software dello strato Network che si preoccupa di dell'instradamento dei pacchetti in transito.



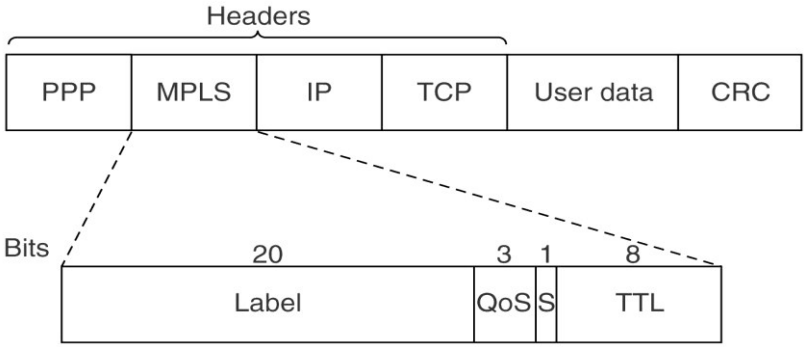
- Se la **Rete è a Datagramma** il routing viene determinato per ogni pacchetto, poiché il percorso migliore può cambiare nel tempo.
- Se la **Rete è a Circuito Virtuale** il routing viene determinato al momento dell'attivazione del circuito. Da quel momento in poi tutti i pacchetti seguono il percorso stabilito.

Confronto tra i metodi di commutazione a pacchetto

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Reti a Circuito Virtuale: MPLS

MPLS (MultiProtocol Label Switching) consente di creare in Internet aree a commutazione di Label.
E' uno strato che si pone sotto il livello rete aggiungendo un proprio Header di 4 byte tra l'header di livello rete (IP) e quello di livello dati (ppp o Ethernet). Per questo può essere considerato un protocollo di livello 2.5.
I campi principali sono la Label (20bit), QoS, e TTL.

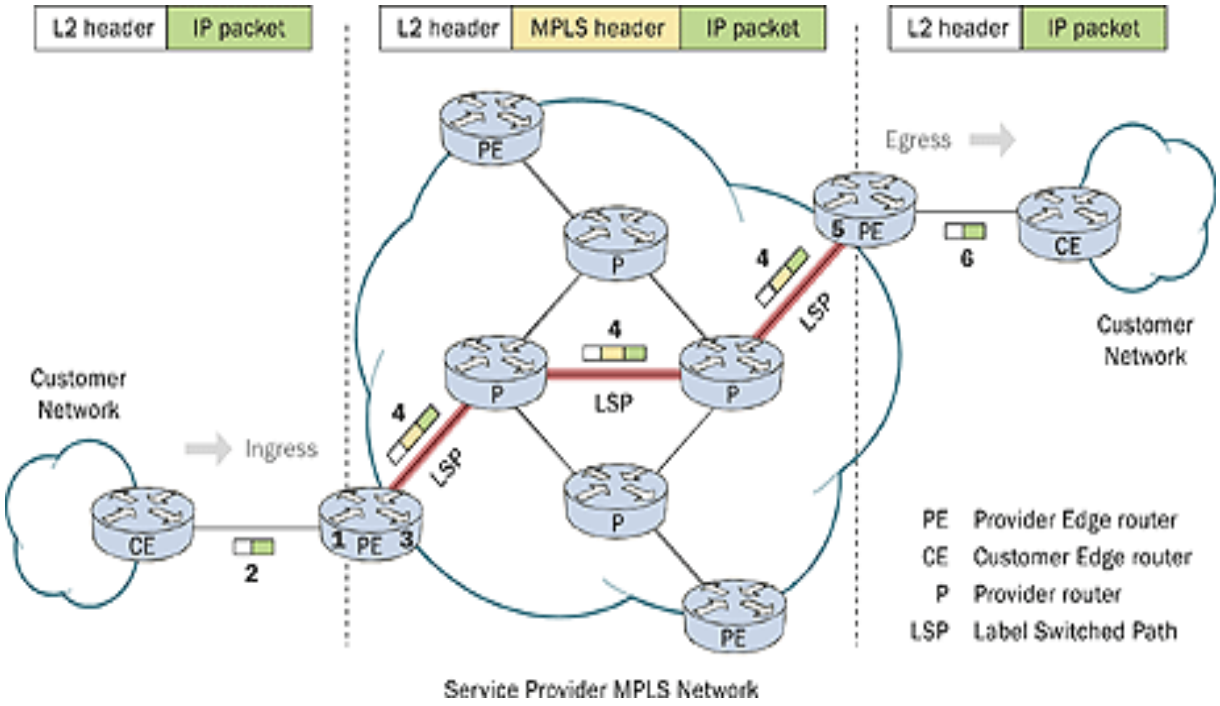


Vantaggi: QoS, Traffic Shaping (e-mail,web, ..), VPN.

Il routing MPLS

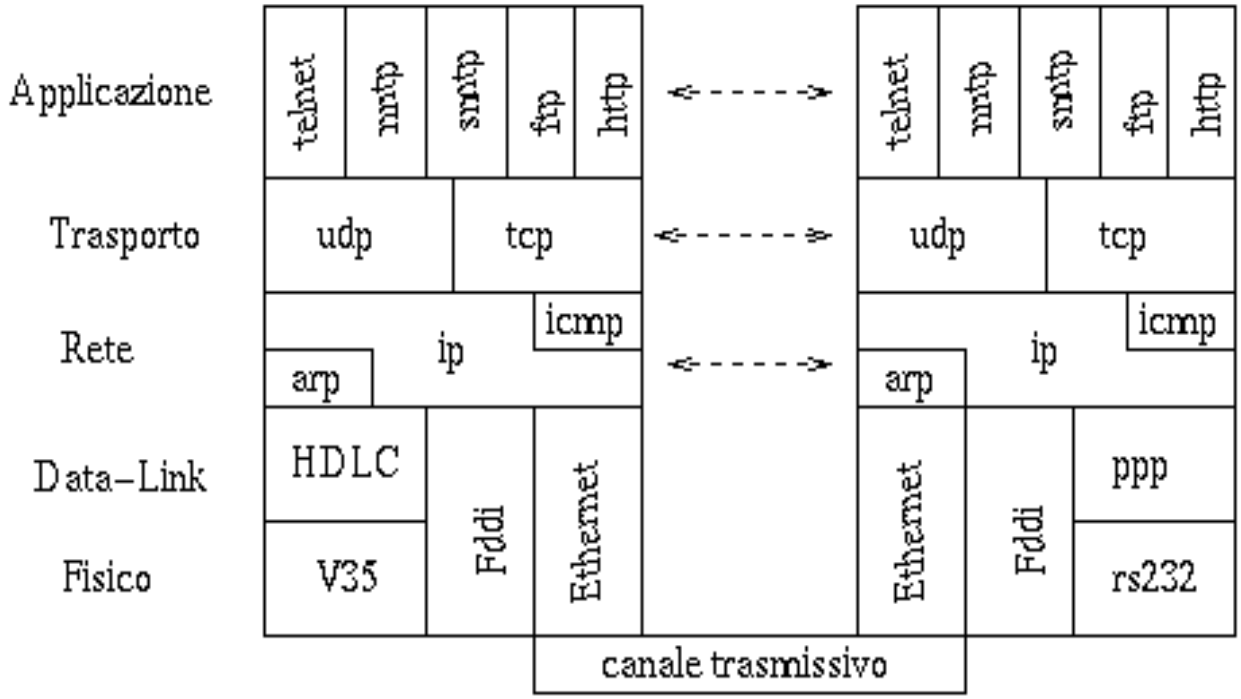
Richiede al proprio interno Router specifici che supportano il protocollo.
Il router di frontiera (Edge) determina il percorso e aggiunge l'header MPLS al pacchetto.

Attraverso le etichette il primo pacchetto definisce un “tunnel” nella rete MPLS.
I pacchetti successivi della stessa connessione seguono il percorso del primo.

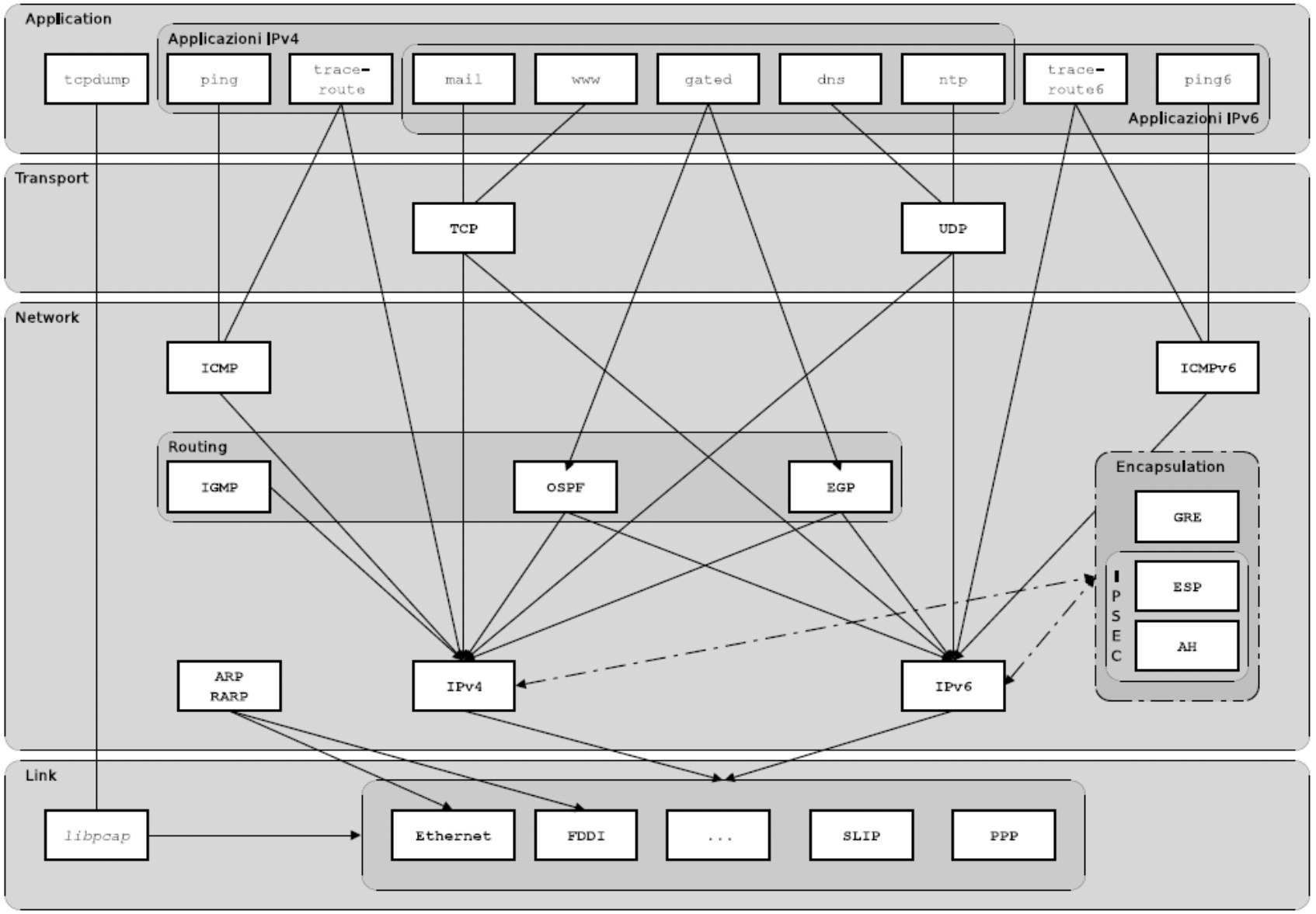


La famiglia dei protocolli TCP/IP

- Nessuna specifica per gli strati sotto IP, in quanto relativi alla singola sottorete.
- IP svolge funzioni di rete e instradamento dei pacchetti
- TCP (o UDP) svolge le funzioni di trasporto e di controllo della connessione end-to-end
- Lo strato di applicazione contiene applicativi utilizzati per fornire servizi all'utente



Quadro generale dei protocolli TCP/IP (da Gapil)



Gli Standard di Internet : Internet Society, RFC

Non esistono veri e propri enti che svolgono la funzione di gestione, ma solo enti di coordinamento delle attività di ricerca e di sviluppo che ora convergono nella **Internet Society**.
Dalla **IS** dipende l'**Internet Advisory Board** (IAB) e si compone di due sottogruppi:

- **Internet Research Task Force (IRTF):** coordina le attività di ricerca
- **Internet Engineering Task Force (IETF):** coordina le attività di ingegnerizzazione ed implementazione
  - IETF pubblica nei **Request For Comment (RFC) -** http://www.ietf.org/rfc.html
  - Tipi di RFC
    - Informational (FYI)
    - Best Current Practice (BCP)
    - Standard (STD) 3 stati : **Proposed Standard, Draft Standard, Standard**

Gli Standard di Internet : ICANN , IANA

ICANN (Internet Corp. for Assigned Names and Numbers - http://www.icann.org/) è l'ente no-profit che assegna gli indirizzi IP e l'identificatore di protocollo e gestisce il DNS di primo livello (Top-Level Domain).
Funzione svolta operativamente da IANA (www.iana.org) che è una sua emanazione.

Data la complessità della gestione, sono state individuate 5 organizzazioni denominate RIR (Regional Internet Registries) che in cooperazione con IANA hanno il compito di gestire le allocazioni a livello continentale.
Le RIR sono: ARIN, APNIC, RIPE, LACNIC e AFRINIC.

Principi architetturali di Internet

Descritti nell'RFC 1958 http://www.ietf.org/rfc/rfc1958.txt, in ordine di importanza:

1) Assicurarsi che funzioni
2) Mantenerlo semplice (nel dubbio, la soluzione più semplice)
3) Fare scelte chiare (se si può fare in diversi modi sceglierne uno)
4) Sfruttare la modularità
5) Aspettarsi l'eterogeneità
6) Evitare opzioni e parametri statici
7) Mirare ad un buon progetto (non necessariamente perfetto)
8) Essere rigorosi nell'invio e tolleranti nella ricezione
9) Pensare alla scalabilità (IPv4 e IPv6..)
10) Considerare le prestazioni e i costi

IP: Lo stato Network in Internet

Interconnette più reti di livello Data-Link (LAN o connessioni punto-punto).
Fornisce uno servizio per il trasporto di datagrammi (pacchetti) tra mittente e destinatario indipendentemente dalle loro reti di appartenenza - http://www.ietf.org/rfc/rfc791.txt
La versione del protocollo IP attualmente in uso, descritta in queste slides, è IPv4.

Operazioni:

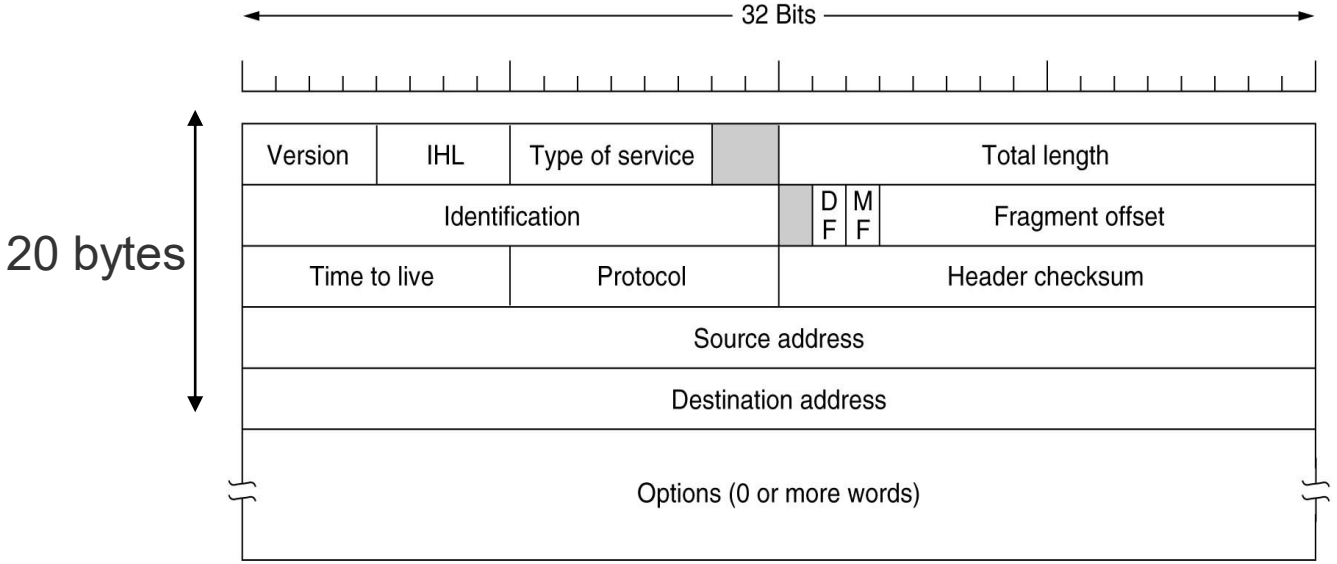
- Lo stato di trasporto prende il flusso di dati e li **divide in datagrammi** che passa allo stato IP. La dimensione massima è di 64KB, ma generalmente vengono scelti datagrammi non superiori a 1500 Byte (per compatibilità con Ethernet).
- Il datagramma di trasporto (detto Segmento) **viene incorporato nella Trama IP** e trasferito da un router all'altro fino a destinazione.
- Il datagramma può subire una **frammentazione** nel caso di passaggio attraverso un livello data-link con dimensione massima (MTU) inferiore. I frammenti vengono riassemblati a destinazione.
  Alcuni MTU (byte): 802.3=1500, 802.11=2312, PPP=576(tipico), FibreChannel=2112
- Il datagramma (eventualmente riassemblato) viene **estratto dalla trama IP** e passato al livello di trasporto, che **ricostruisce il flusso.**
- **QoS**: La consegna è di tipo **"Best Effort"**.

La trama IP (1/3)

Il datagramma IP è costituito dall'intestazione (header) IP seguita dal segmento del livello di trasporto.

		Segmento liv. Trasporto
HeaderLiv2	Header IP	Payload (max 64KB)

L'header ha una parte fissa e una parte opzionale variabile e viene trasmessa in ordine big endian.



La trama IP (2/3)

- **Version (4 bit):** i primi 4 bit di ogni pacchetto IP contengono il numero di versione.
- **HLEN (4 bit) :** dimensione dell'header espressa in parole di 4 byte (da 5 a 15)
- **Type of Service (6 bit):**
  - Inizialmente per controllo della rete (priorità e segnalazioni).
  - Con l'RFC 2474 diventa Servizi Differenziati per la codifica delle Classi di Servizio.
  - In realtà Internet è "best effort": questo campo è quasi sempre inutilizzato.
- **Total Lenght (16 bit):** Numero di byte totali header+dati (fino a 64K)
- **Identification (16 bit):** Tutti i frammenti di datagramma hanno lo stesso valore
- **DF (1 bit):** Don't Fragment → ordina ai router di non frammentare
- **MF (1 bit):** More Fragments → 1 per tutti i frammenti tranne l'ultimo
- **Fragment Offset (13 bit):** Indica la posizione del frammento nel datagramma corrente, espressa in blocchi di 8 byte (max. 8192 frammenti).
- **TTL (8 bit):** Numero max di salti; si decrementa ad ogni passaggio. Quando arriva a 0 il pacchetto viene eliminato.

La trama IP (3/3)

- **Protocol (8 bit):** Protocollo di livello superiore (ICMP=1,TCP=6, UDP=17, ..)
- **Header Checksum (16 bit):** Checksum dell'**header**
  - ricalcolato da ogni router , perché il TTL cambia ad ogni salto.
  - Aiuta a rilevare errori generati da locazioni di memoria difettose nei router.
  - Somma tutte le sequenze di 16 bit (con l'aritmetica del complemento a 1) e poi prende il complemento a 1 del risultato.
- **Source e Destination Address (32+32 bit):** Indirizzi di sorgente e destinazione
- **Options**: Pensato per poter aggiungere estensioni non previste.

  Lista completa: http://www.iana.org/assignments/ip-parameters

  Formato: Opt. code (1 byte) - Opt. Length (1byte) - Opt. Data (n Byte)
  - 0 - End of Option List
  - 130 - Security: lista di reti vietate, non usato.
  - 7 - Route record: ogni router aggiunge il proprio indirizzo
  - 68 - Time Stamp: ogni router aggiunge il proprio indirizzo e data/ora.
  - 137 - Source routing: lista dei router da percorrere
- **Padding:** bit aggiunti per rendere il campo Options multiplo di 32 bit.

Indirizzi IP

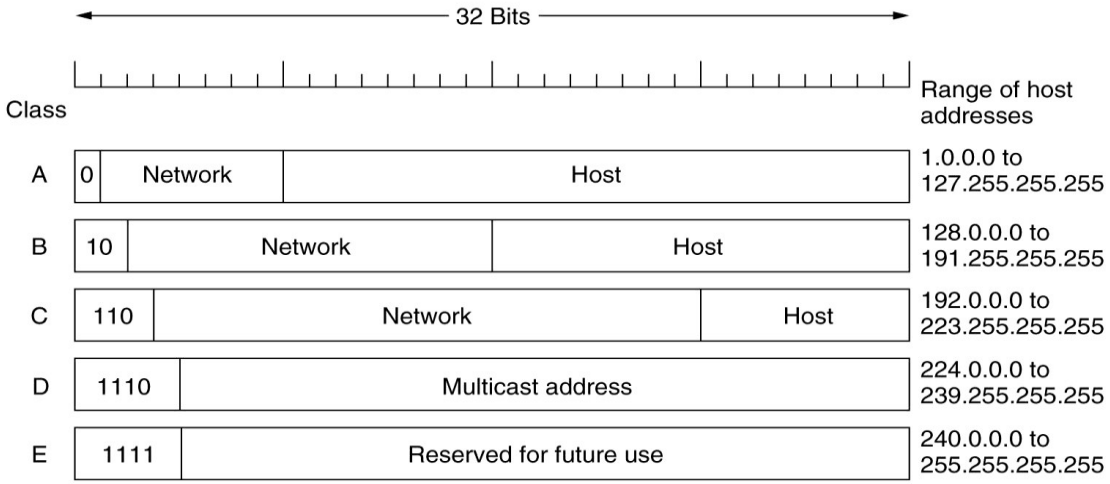
Indirizzi a 32 bit con notazione "**dotted decimal**": 4 decimali (0-255) separati da punto
*Esempio: 0x89CCD401 = 10001001.11001100.11010100.00000001 -> **137.204.212.1***

Numero max. di indirizzi 2^{32} = 4.294.967.296
Per motivi di routing la sequenza è suddivisa in due parti:

– **NETid**: Identifica una Rete liv.2 Utilizzata dai router per l'instradamento dei pacchetti

– **HOSTid**: Distingue gli Host della stessa Rete.

Classfull Addressing:



Classi IP

Classe	bit-iniziali	inizio	fine	indirizzi	default-mask	CIDR-equiv	reti	host
A	0	0.x.x.x	127.x.x.x	2G	255.0.0.0	/8	126	16M
B	10	128.x.x.x	191.x.x.x	1G	255.255.0.0	/16	16K	64K
C	110	192.x.x.x	223.x.x.x	0.5G	255.255.255.0	/24	2M	254
D	1110	224.x.x.x	239.x.x.x	0.25G	Multicast			
E	1111	249.x.x.x	255.x.x.x	0.25G	Reserved			

La numerazione è gestita da IANA che delega gerarchicamente alle RIR:

Vedi ad esempio il comando: whois 160.78.0.0

Indirizzi IP di rete e di Broadcast

< network >	00000000000000000000
< network >	11111111111111111111

Address of the network
Broadcast of a specific network

Se la parte Host è di N bit, il numero di indirizzi effettivamente assegnabili agli host è **2^N-2**, poiché il primo indirizzo (tutti zeri nella parte host) identifica la rete, mentre l'ultimo indirizzo (tutti uni nella parte host) è l'indirizzo di broadcast.

Indirizzi IP per uso privato

Le seguenti reti sono riservate da ICANN per uso privato (Intranet) e gli indirizzi non possono essere annunciati dai Router (http://www.ietf.org/rfc/rfc1918.txt):

Classi	inizio	Fine	indirizzi
1 classe A	10.x.x.x		16M
16 classi B	172.16.x.x	172.31.x.x	1M
255 classi C	192.168.0.x	192.168.255.x	64K

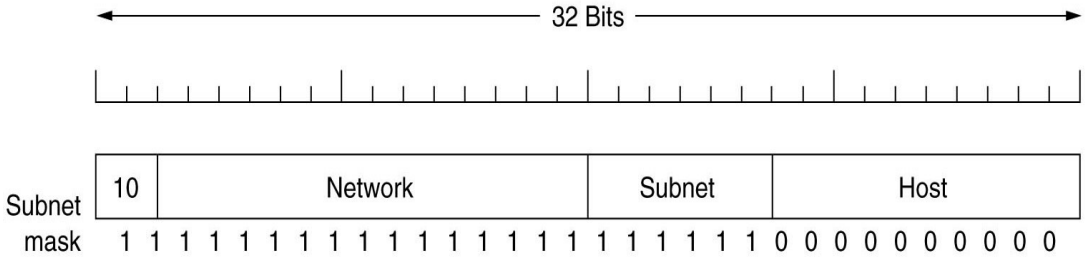
LOOPBACK
La rete 127.0.0.0/16 è riservato per il loopback (RFC 3330).
Per convenzione su ogni host viene definita una interfaccia virtuale di loopback con indirizzo IP predefinito 127.0.0.1, con nome **localhost**, che consente la comunicazione TCP/IP tra due processi locali senza il coinvolgimento di interfacce fisiche.

ZEROCONF
La rete 169.254.0.0/16 (IPv4 link-local) è utilizzata dal servizio Zeroconf (http://www.ietf.org/rfc/rfc3927.txt) per assegnare un indirizzo IP agli host di una LAN senza dipendere da una infrastruttura, ovvero quando non è possibile ottenere un indirizzo dinamico da un server DHCP.

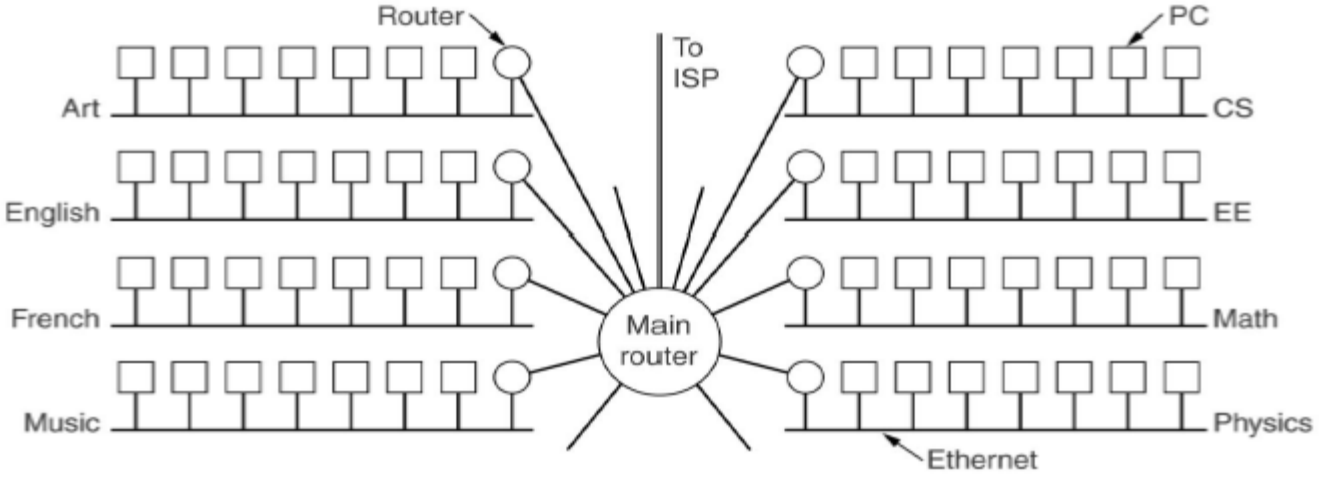
IP subnetting

Consente un ulteriore livello di gerarchia per gli indirizzi IP: NET-SUBNET-HOST
Il **NETMASK** è un parametro di 32 bit che stabilisce la suddivisione:

- Bit a 1 in corrispondenza del campo NET o SUBNET
- Bit a 0 in corrispondenza del campo HOST



Esempio: rete di classe B 160.78.0.0 partizionata in 256 Subnet da 256 indirizzi:
NETMASK 255.255.255.0 -> 11111111 11111111 11111111 00000000



CIDR – Classless Inter-Domain Routing

- Il numero di indirizzi IP (4G) è insufficiente
- Molte reti di classe B usano meno 50 indirizzi

CIDR http://www.ietf.org/rfc/rfc1519.txt
- soluzione temporanea in attesa di IPv6
- Assegna gli indirizzi IPv4 rimanenti in blocchi di dimensione variabile nella forma
  netaddress/NetMaskBit
- routing più complicato (tabelle lunghe)

Il **Supernetting** (route aggregation) consente di accorpare più reti contigue come fossero un'unica rete, per ottimizzare i tempi di routing

- In caso di sovrapposizioni tra 2 reti vince la netmask più lunga

no. of addrs	bits	pref	mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255
512	9	/23	255.255.254
1 K	10	/22	255.255.252
2 K	11	/21	255.255.248
4 K	12	/20	255.255.240
8 K	13	/19	255.255.224
16 K	14	/18	255.255.192
32 K	15	/17	255.255.128
64 K	16	/16	255.255
128 K	17	/15	255.254
256 K	18	/14	255.252
512 K	19	/13	255.248
1 M	20	/12	255.240
2 M	21	/11	255.224
4 M	22	/10	255.192
8 M	23	/9	255.128
16 M	24	/8	255
32 M	25	/7	254
64 M	26	/6	252
128 M	27	/5	248
256 M	28	/4	240
512 M	29	/3	224
1024 M	30	/2	192

Instradamento dei Datagrammi

La rete di appartenenza di un Host è fondamentale per determinare la modalità di consegna, che può essere **diretta** o **indiretta**.

Direct delivery : host sorgente e destinatario condividono la stessa rete.

- trova l'indirizzo fisico del **destinatario** (con ARP) che associa all'IP del destinatario
- inoltra il pacchetto al livello Link indirizzando il destinatario:

```
1) ARPrequest   to:Broadcast from: MACmitt          Who has IPdest?
2) ARPreply     to:MACmitt   from: MACdest
3) Send IP      to:MACdest   from: MACmitt          toIP:dest, fromIP:mitt
```

Indirect delivery : sorgente e destinatario appartengono a reti IP diverse

- individua il router da contattare consultando la propria **Tabella di Routing**
- trova l'indirizzo fisico del **router** (con ARP) che associa all'IP del destinatario
- inoltra il pacchetto al livello Link indirizzando il router.

```
1) ARPrequest     to:Broadcast from: MACmitt        Who has IProuter?
2) ARPreply       to:MACmitt   from: MACrouter
3) Send IP        to:MACrouter from: MACmitt        toIP:dest, fromIP:mitt
```

La scelta del tipo di consegna avviene consultando la tabella di routing locale.

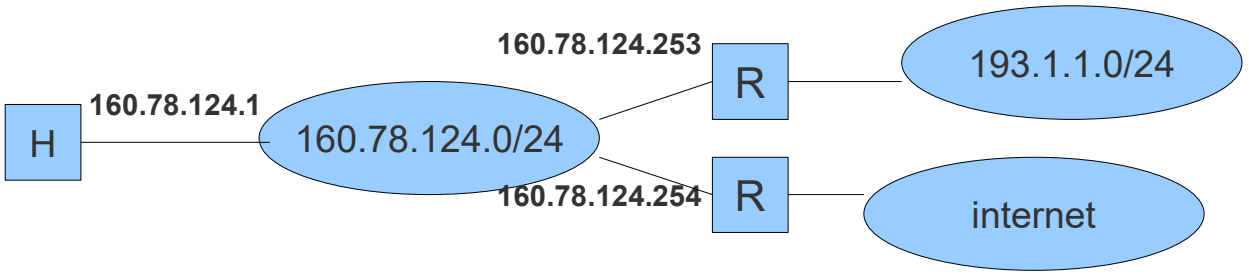
Tabella di routing

E' una tabella che contiene le destinazioni e i percorsi per raggiungerle.

Esempio di tabella di routing (comando “route” di linux) per l'host 160.78.124.1:

Destination	Router	Mask	Interface
160.78.124.0	*	255.255.255.0	eth0 (consegna diretta)
193.1.1.0	160.78.124.253	255.255.255.0	eth0 (consegna indiretta)
default	160.78.124.254	0.0.0.0	eth0 (consegna indiretta)

La prima riga (Router *) indica che gli host della rete 160.78.124.0/24 vengono raggiunti in consegna diretta.
La seconda riga (Router 160.78.124.253) indica che gli host della rete 193.1.1.0/24 sono raggiunti in modalità indiretta tramite il router 160.78.124.253
Generalmente le reti locali hanno al proprio interno un router di riferimento (indicato come “**Default Router**”) a cui vengono consegnate tutte le destinazioni non note.
Nell'esempio tutte le destinazioni diverse da 160.78.124.0/24 e 192.1.1.0/24 vengono consegnate al router 160.78.124.254.



Ricerca nella tabella

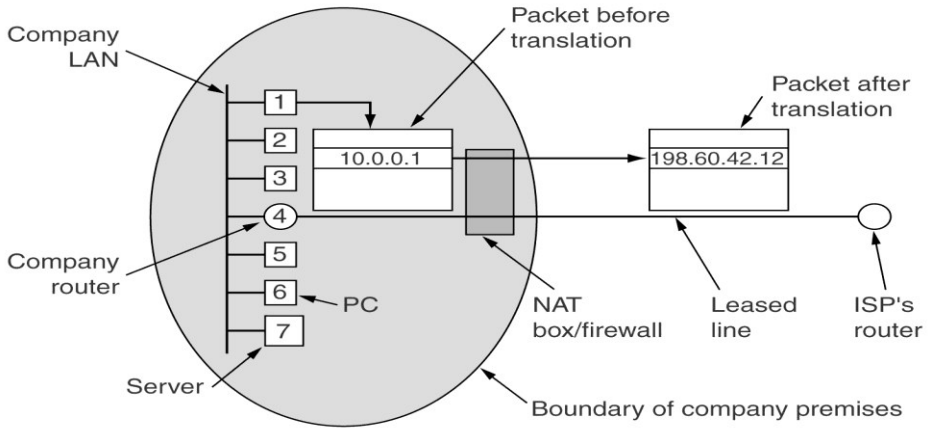
La ricerca avviene utilizzando
- l'IP di destinazione (IPdest)
- La rete di destinazione e Netmask (Mask) di ciascuna riga della tabella

Procedura: IPdest AND Mask

- Se il risultato coincide con la rete presa in esame la riga è quella giusta
- Una volta trovato il risultato il lookup si ferma e il datagramma viene instradato
- Se nessuna riga corrisponde si usa il router di default

NAT (Network Address Translation)

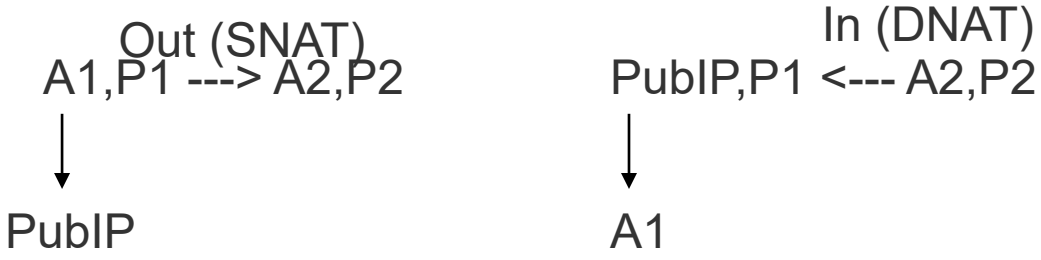
NAT (http://www.ietf.org/rfc/rfc3022.txt): dispositivo che consente agli host di una LAN (con indirizzi privati) di comunicare in Internet utilizzando un solo indirizzo pubblico.
La linea verso Internet possiede un indirizzo IP pubblico e viene visto dagli host della LAN come Default Router.
Le operazioni del NAT sono distinte in base alla direzione:
SNAT (Source-NAT) è la funzionalità che consente di manipolare l'indirizzo sorgente ed è tipicamente utilizzato per consentire ai pacchetti di una LAN privata di uscire in internet. Quando un Host della LAN si rivolge al NAT per uscire in Internet il NAT trasforma l'indirizzo del mittente IP nell'indirizzo IP pubblico del NAT, quindi contatta il destinatario.
DNAT (Destination-NAT) è utilizzata per manipolare l'indirizzo di destinazione.
E' usata tipicamente per dirottare verso una destinazione interna (con indirizzo privato) i pacchetti provenienti da Internet.



Le tabelle del NAT

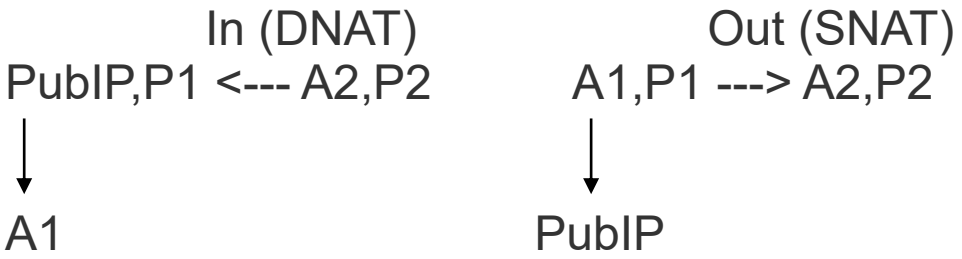
Le manipolazioni SNAT e DNAT sono rappresentate in tabelle che vengono consultate per ogni pacchetto che attraversa il NAT. Le entry delle tabelle possono essere statiche o dinamiche.

NAT Dinamico
Cl. interno: A1,P1
Serv esterno: A2,P2



Quando un client della LAN si rivolge al NAT per contattare un server esterno, il NAT genera una entry dinamica associando IP/porta del client con la IP/porta del server quindi applica **SNAT**.
L'entry viene utilizzata per il DNAT sulla risposta del server.

NAT Statico
Cl. esterno: A2,P2
Serv interno: A1,P1



Se vogliamo avere un server interno che deve essere contattato da un client esterno dobbiamo istruire il NAT mediante una entry statica che associa una porta del NAT con IP/porta del server interno.
Quando un client esterno contatta il NAT sulla porta viene consultata la entry statica e applicato **DNAT**. Viene inoltre creata una entry dinamica che verrà utilizzata per applicare SNAT sulla risposta.

Problemi dell'architettura NAT

- Violazione dell'univocità degli indirizzi: migliaia di Host usano gli stessi indirizzi privati.
- Sicurezza: è difficile tracciare l'identità dell'indirizzo IP pubblico.
- IP non è più connection-less
- IP non è più stratificato: Il Layer IP non dovrebbe entrare nei layer superiori
- Un guasto al NAT pregiudica tutte le connessioni che lo attraversano.

In realtà NAT ha avuto una grande diffusione e ha ridotto la spinta verso IPv6.

Protocollo ARP

Ogni interfaccia di rete di un nodo (Ethernet, LAN Wireless, Seriale, ecc) possiede un indirizzo fisico e, se utilizzata in internet, almeno un indirizzo IP.
Il protocollo **ARP (Address Resolution Protocol)** ha il compito di determinare l'indirizzo fisico di un nodo IP.
Quando un nodo mittente deve contattare un destinatario in **Direct Delivery** (Terminale o Router) di cui conosce solo l'indirizzo IP utilizzerà il protocollo ARP:

- Il nodo sorgente invia un pacchetto (**ARP Request**) con destinazione Broadcast sulla LAN, contenente l'indirizzo IP del destinatario.
- I terminali con indirizzo IP diverso ignoreranno il Pacchetto, mentre il nodo in oggetto risponderà (**ARP Replay**) con un Unicast inviando il proprio indirizzo fisico.
- Ogni host mantiene una tabella (**ARP Cache**) con le corrispondenze ottenute (comando arp –a). Ogni entry ha un tempo di vita tipicamente di 20 minuti.

Il Frame ARP contiene:

- Un campo codice 1=ARPrequest, 2=ARPreplay
- indirizzo IP e Indirizzo HW di partenza e destinazione

Protocollo RARP

In determinate situazioni alcuni nodi IP al momento dell'attivazione della rete non conoscono il loro indirizzo IP (ad esempio perché non hanno memoria permanente).
Esistono diverse soluzioni, tra cui **RARP** (Reverse ARP) - http://www.ietf.org/rfc/rfc903.txt
E' un protocollo ideato da SUN per risolvere il problema.
Il client invia in modalità Broadcast la richiesta:
"Questo è il mio indirizzo MAC: xx-xx-xx-xx-xx-xx, Qualcuno conosce il mio indirizzo IP?".
Un server RARP, con la tabella MAC-IP , risponderà con l'informazione richiesta.
Svantaggi:

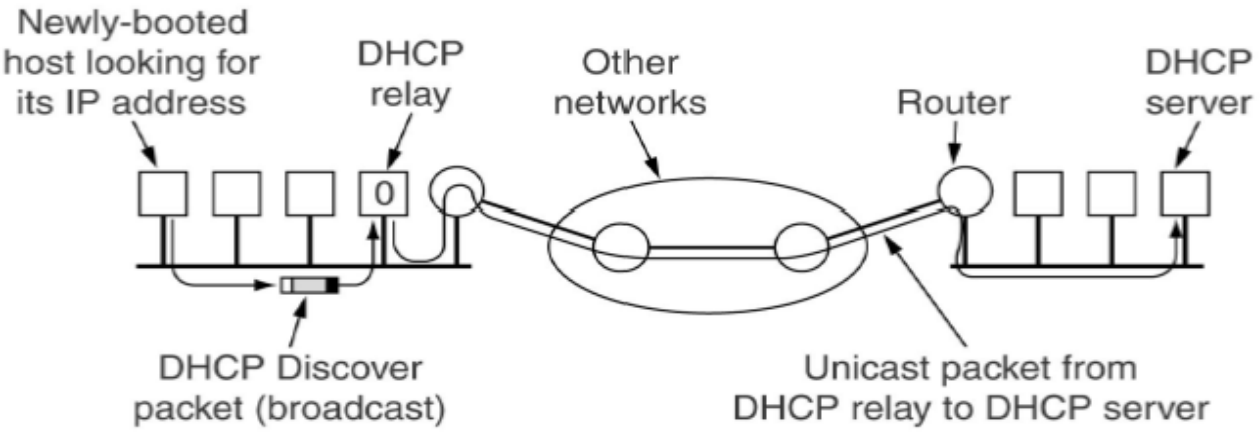
- la richiesta Broadcast non passa i router
- le associazioni MAC-IP sono statiche
- non sono previste altre informazioni

RARP è reso obsoleto dal suo successore DHCP.

Protocollo DHCP

DHCP (Dynamic Host Configuration Protocol, rfc2131.txt e rfc2132.txt) risolve lo stesso problema di RARP aggiungendo nuovi servizi.

- Il server DHCP può fornire più informazioni al client: indirizzo IP, NetMask, Default Router, DNS server, NTP server, ecc.
- L'indirizzo IP fornito può essere statico o dinamico (assegnato al momento della richiesta sulla base di un pool di indirizzi disponibili)
- Il server può risiedere in una LAN diversa dalla LAN del client (tramite relay)



E' un protocollo applicativo: utilizza la porta 67/UDP per il server e la 68/UDP per il client.

Funzionamento del DHCP

1) Il client DHCP invia in modalità broadcast un pacchetto **DHCP Discover**

`0.0.0.0:68 -> 255.255.255.255:67`

2) Il server risponde (tramite l'eventuale Agent) un pacchetto **DHCP Offer** che contiene l'indirizzo richiesto più eventuali altre informazioni.

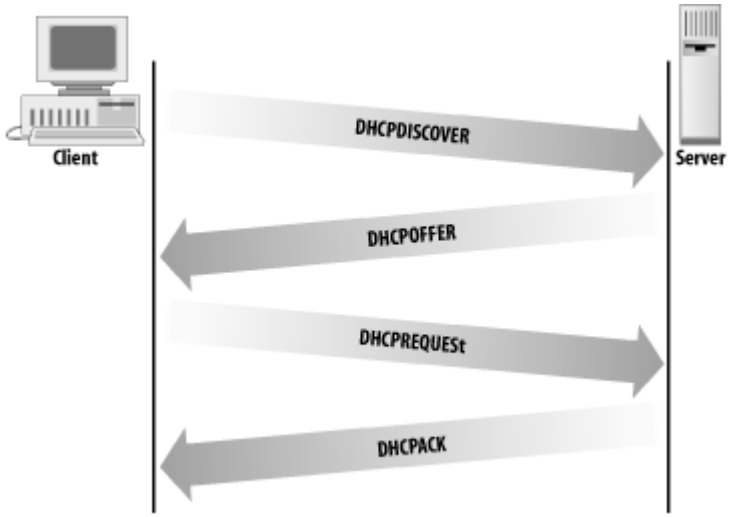
`Ipserver:67 -> Ipclient:68`

3) Il client accetta la prima risposta che ottiene e invia in Broadcast un **DHCP Request** in cui dice da quale server ha ricevuto l'indirizzo.

`0.0.0.0:68 -> 255.255.255.255`

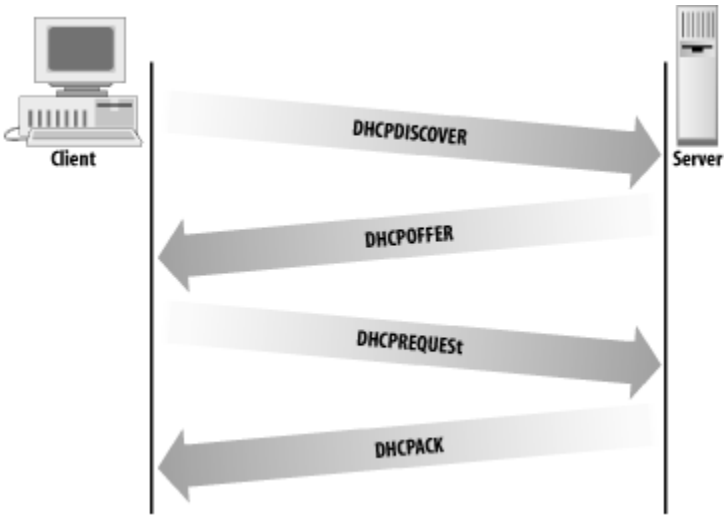
4) Infine il server manda un **DHCP ACK** al client per conferma.

`Ipserver:67 -> Ipclient:68`



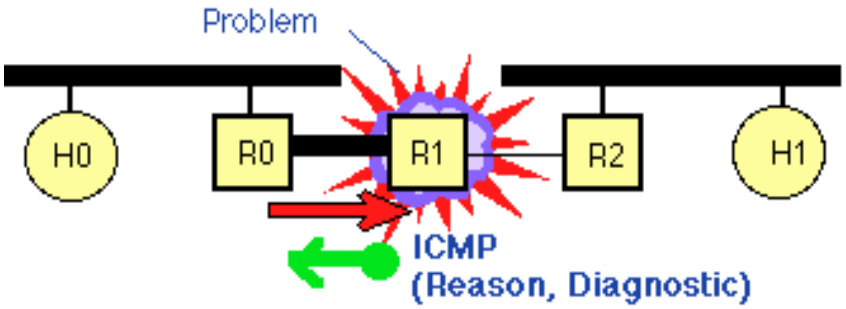
Funzionamento del DHCP: Rinnovo

Il server gestisce una tabella in cui gli indirizzi IP possono essere associati staticamente a indirizzi MAC oppure possono essere “**affittati”** dinamicamente al momento della richiesta. Il “leasing” ha un termine; il client deve chiederne un eventuale rinnovo, altrimenti l’indirizzo viene ritirato ed assegnato ad un altro client.
Le operazioni **DHCPREQUEST/DHCPACK** vengono ripetute per prolungare l'assegnazione dell’indirizzo. La richiesta avviene con 3 tentativi: 2 volte al 50% del tempo utilizzato e un’ultima volta all’ 87,5%



Protocollo ICMP

ICMP - Internet Control Message Protocol (http://www.ietf.org/rfc/rfc792.txt) è un protocollo di servizio di IP per lo scambio di messaggi di errore o di controllo che consentono agli Host e ai Router di accorgersi di eventuali malfunzionamenti della rete. Spedisce i messaggi di notifica dell'errore sempre al mittente del datagramma per il quale si è verificato l'errore.

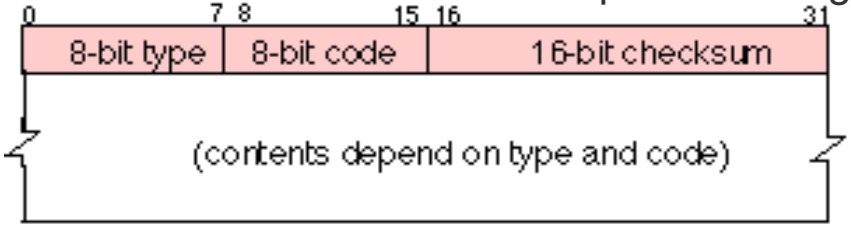


Formato del Frame ICMP

Il formato del frame è costituito da una intestazione e da un'area dati. La prima è composta da tre campi:

- **TIPO** è un numero di 8 bit che identifica il messaggio Tipi principali:
  - 0 = Risposta di ECHO
  - 3 = Destinazione irraggiungibile (esempio datagramma troppo grande, ma DF settato)
  - 4 = Rallentamento della sorgente (Il router informa che il pacchetto è stato eliminato e che la sorgente deve rallentare)
  - 8 = Richiesta di ECHO (comando ping)
  - 11 = TTL scaduto per un datagramma
  - 12 = Problema di parametri (argomento di un opzione scorretto)
  - 13 = Richiesta di contrassegno temporale (per sincronizzare gli orologi)
  - 14 = Risposta di contrassegno temporale
- **CODICE:** Info aggiuntive. Ad esempio se il Tipo è 3 il Codice dice qual'è il tipo di errore
- **CHECKSUM**, di 16 bit, è il CRC del frame ICMP (header+data)

L'area Dati varia in funzione del tipo di messaggio.



Il Frame ICMP è inserito direttamente nel payload di IP: