



## Tipi di servizio offerti al livello di trasporto

### ■ Con connessione

- L'entità di trasporto del trasmittente deve instaurare una connessione con l'entità del ricevente
- I processi si accordano sulla qualità e sul costo del servizio
- La comunicazione avviene nelle due direzioni
- Il controllo di flusso evita che il trasmittente possa sovraccaricare il ricevente

### ■ Senza connessione

- Non c'è alcuna connessione
- Non c'è alcuna garanzia sulla qualità del servizio offerto.

## Organizzazione del livello Rete

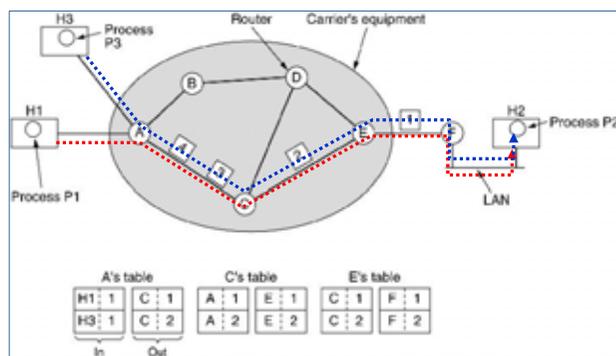
### ■ Circuiti virtuali (servizio con connessione)

- La creazione della connessione prevede la definizione del percorso di consegna dalla sorgente alla destinazione.
- Non si deve scegliere il percorso per ogni pacchetto.
- I pacchetti contengono indicazione dei circuiti virtuali a cui appartengono.
- I router devono mantenere memoria dei circuiti virtuali che passano attraverso di essi.
- Maggiore qualità

### ■ Datagrammi (servizio senza connessione)

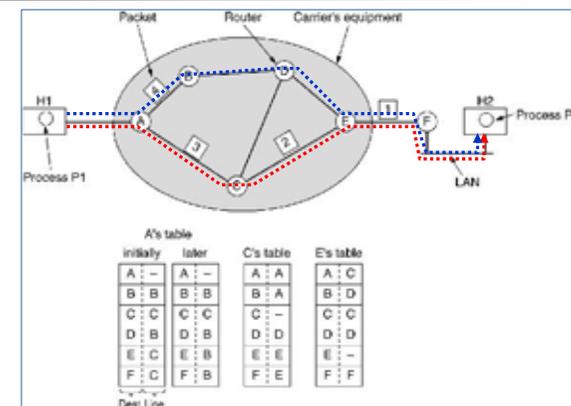
- I pacchetti fra due host possono seguire anche percorsi diversi.
- I router hanno tabelle che indicano quale linea di uscita utilizzare per ogni possibile router destinazione
- Maggiore robustezza

## Implementazione di un servizio con Circuito Virt.



Tablelle dei circuiti virtuali

## Implementazione di un servizio a datagrammi



Tablelle di instradamento



## Routing

- Definizione
  - Un algoritmo di routing decide quale connessione usare per instradare i pacchetti dalla macchina sorgente alla macchina destinazione.
- Requisiti:
  - Correttezza nel routing dei datagrammi
  - Semplicità e efficienza delle implementazioni del routing
  - Robustezza: la rete deve funzionare anche in presenza di guasti
  - Stabilità: le informazioni nelle tabelle di routing devono raggiungere un punto di equilibrio
  - Imparzialità ed Ottimalità nel routing dei datagrammi
- Alcuni criteri di ottimalità:
  - Percorso minimo, ottimizzazione traffico, ...



## Generazione delle Tabelle di routing

- Manuale
  - Tabella creata ad hoc
  - Utile in piccole reti
  - Utile se l'instradamento non cambia.
- Automatica
  - Il software crea/aggiorna le tabelle
  - Necessario in grandi reti
  - L'instradamento cambia in caso di guasti
- Due tipi di algoritmi
  - **non adattivi (Routing Statico):**
    - calcolano i percorsi quando la rete non è ancora attiva.
  - **adattivi (Routing Dinamico):**
    - modificano i percorsi in base alle situazioni di traffico ed ad altre informazioni locali come congestione, guasti, ecc.



## Tipi di algoritmi di routing

- **Isolati**
  - routing calcolato con sole informazioni locali, indipendentemente dal resto (stato degli altri nodi e stato della rete). (Es. SNA/IBM)
  - Es: flooding
- **Centralizzati**
  - Un centro di controllo conosce lo stato globale. calcola il cammino ottimo per ogni coppia (mittente,destinatario) e dirama le tabelle. (Es. TYMNET)
- **Distribuiti**
  - I nodi cooperano e comunicano frequentemente il proprio stato e quello della rete. (Es. Internet)
  - Es: stato dei collegamenti



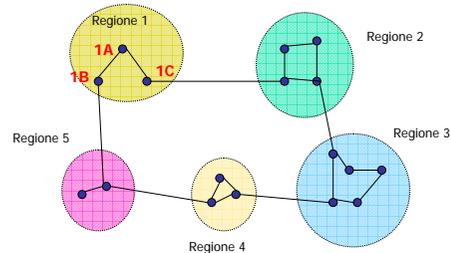
## Routing gerarchico

- Il numero di host di Internet diventa sempre più grande.
  - Le tabelle di routing crescono di conseguenza.
- Quindi conviene dividere i router in regioni.
  - Ogni router conosce i dettagli della propria regione e come comunicare con le altre, ma non conosce la struttura interna delle altre regioni.

## Routing gerarchico

Due (o più) livelli di routing:

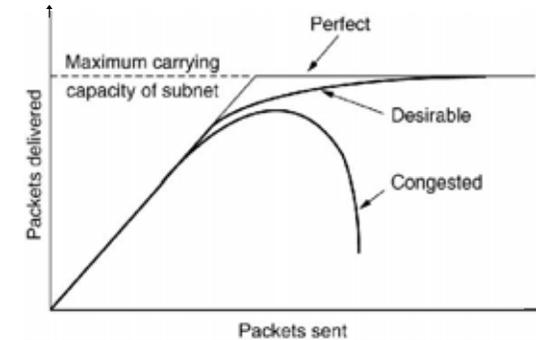
- un primo livello di **routing interno** ad ogni regione
  - sanno come arrivare a tutti gli altri router della regione;
- un secondo livello di routing fra **router di confine**.
  - particolari router a cui i router interni inviano i dati che devono pervenire ai router di un'altra regione.



- 1B e 1C sono i router di confine per la regione 1
- La tabella di routing di 1A contiene 6 entrate (invece di 16)

## Controllo della congestione

- Quando nella rete (o in una sottorete) sono presenti troppi pacchetti le prestazioni degradano (si ha **congestione**).



## Scelte che influiscono sul controllo della congestione

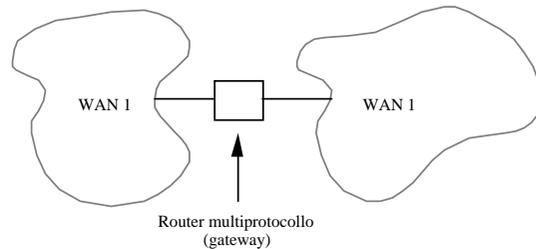
- Nei livelli Data link e Trasporto
  - Criterio di ritrasmissione
  - Criterio di gestione dei pacchetti fuori sequenza
  - Criterio per l'acknowledgement
  - Controllo del flusso
- Nel livello Rete
  - Algoritmo di routing
  - Criterio di gestione dei buffer di pacchetti
  - Criterio di scelta dei pacchetti da scartare
  - Vita utile dei pacchetti

## Controllo della congestione

- Il controllo della congestione è cosa diversa dal controllo di flusso che viene effettuato nei livelli 2 e 4 (singola connessione sorgente-destinazione)
- La congestione può essere dovuta a diverse cause:
  - traffico troppo intenso!
  - i buffer dei router sono limitati: se sono pieni, i pacchetti in arrivo vengono scartati
  - processori dei router troppo lenti
  - linee di trasmissione troppo lente
- La congestione alimenta se stessa, perché i timeout sul trasmettitore scadono, ed i pacchetti vengono ritrasmessi aumentando il traffico

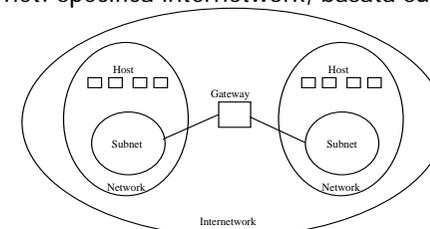
## Interconnessione di reti (Internetwork)

- Reti diverse (LAN, MAN o WAN) sono collegate fra loro.
- Connettesione di reti (progettualmente) diverse tramite router multiprotocollo (o gateway)



## Internetworking

- sottorete (subnet): l'insieme dei router e delle linee di trasmissione
- rete (network): una subnet più tutti gli host collegati
- internet(-work): interconnessione di più network, anche non omogenee
- Internet: specifica internetwork, basata su TCP/IP.



## Internetworking

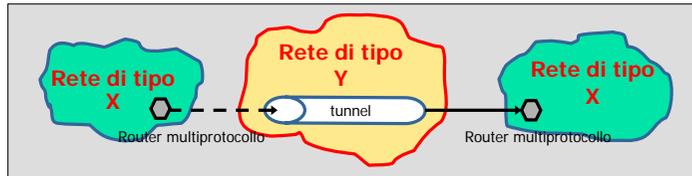
- Reti eterogenee possono differire per:
  - tipi di servizio (con connessione o senza connessione)
  - formati e dimensione dei pacchetti
  - indirizzamento
  - multicast (supportato o non supportato)
  - meccanismi di controllo dell'errore
  - meccanismi di controllo della congestione
  - politiche di sicurezza
  - politiche di accounting
  - ...

## Soluzioni per l'Internetworking

- Livello 1: i **ripetitori** copiano bit tra i cavi di interconnessione
- Livello 2: i **bridge** memorizzano e inviano frame di data link tra reti differenti (possono anche selezionare la rete: **switch**)
- Livello 3: i **router multiprotocollo** inviano pacchetti tra reti differenti
- Livello 4: i **gateway di trasporto** connettono flussi di dati
- Livelli > 4: i **gateway di applicazione** convertono i dati a livello delle applicazioni.

## Tunneling

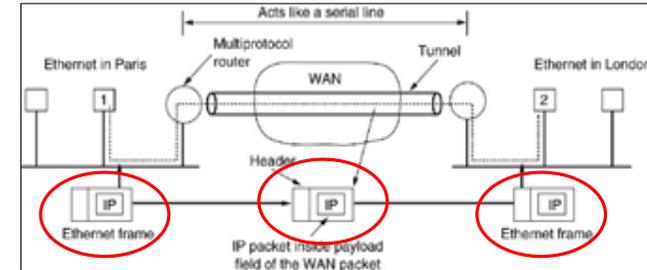
- Quando l'host sorgente e l'host destinazione appartengono allo stesso tipo di rete ma bisogna attraversare reti differenti si può usare la tecnica del **tunneling** (incapsulamento).



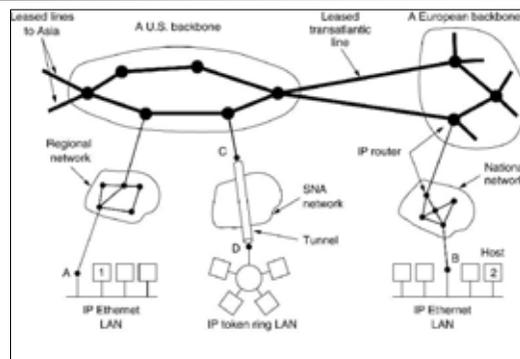
- la rete Y non ha router multiprotocollo.
- un router nelle due reti X è multiprotocollo, e incapsula i pacchetti delle reti di tipo X dentro pacchetti di tipo Y, consegnandoli alla rete di tipo Y.

## Esempio di Tunneling

- L'invio di un pacchetto IP da una rete Ethernet ad un'altra rete Ethernet tramite una WAN (che non usa IP)



## Internet



Internet è una collezione di reti basata su IP

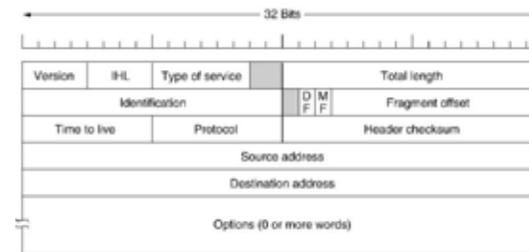
## Internet Protocol (IP)

- Lo standard **IPv4** è il più diffuso protocollo di livello 3
  - specificato da IETF (Internet Engineer Task Force) come RFC 791
- E' la base dell'attuale Internet.
- IP è un protocollo **senza connessione**:
  - I pacchetti contengono l'indirizzo completo della destinazione.
  - Ogni pacchetto viene spedito/gestito indipendentemente.

## Datagramma IP

- Lunghezza massima di un datagramma IP= 65.536 byte.
  - Di solito ha lunghezza pari a circa 1024 byte.
- Formato del datagramma IP: blocchi di 32 bit (4 byte).
- Un datagramma IP consiste di:
  - un **preambolo** (header) di 20 byte fissi più massimo di 40 byte opzionali e
  - una **parte dati**.

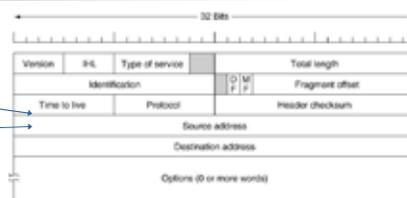
## Formato del preambolo IP



- **Version**: numero di versione del protocollo (4 bit)
- **IHL**: lunghezza preambolo (header) in parole di 32 bit, da 5 a 15 word.
- **Total length**: lunghezza del pacchetto (in byte), massimo 65.535 byte.
- **Type of service**: affidabilità e velocità richieste - ignorato dai router

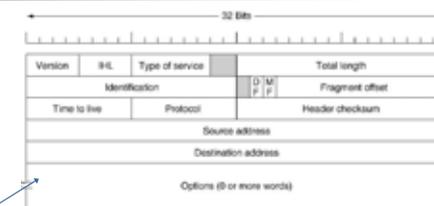
## Formato del preambolo IP

- **Source address**
- **Destination address**



- **Gestione dei frammenti**
  - **Identification**: identifica i frammenti di uno stesso pacchetto
  - **DF don't fragment** =1, non frammentare
  - **MF more fragments** =1, il pacchetto non è ancora finito
  - **Fragment offset**: indice del frammento nel pacchetto (multiplo di 8 byte)
- **Time to live**: contatore (inizialmente impostato a un numero  $\leq 255$ ); è decrementato ad ogni hop (o sec); se=0 il pacchetto viene scartato
- **Protocol**: tipo di servizio di livello trasporto cui consegnare i dati
- **Header checksum**: verifica la correttezza dell'header: si calcola ad ogni hop, perché il *time to live* cambia

## Formato del preambolo IP



- **Options**: solo cinque tipi oggi definiti (il primo byte identifica il tipo)
  - **security**: livello di segretezza del pacchetto (spesso ignorato);
  - **strict source routing**: cammino esatto da seguire;
  - **loose source routing**: lista di router da non mancare;
  - **record route**: ogni router deve inserire il suo indirizzo: 40 bytes non sono sufficienti!
  - **timestamp**: oltre all'indirizzo inserire il timestamp

## Datagrammi IP

IP fornisce un servizio **best effort**

I datagrammi possono essere:

- ritardati
- duplicati
- distribuiti fuori ordine
- persi
- possono seguire percorsi diversi

Questi problemi devono essere affrontati e risolti dal protocollo di trasporto (es. TCP); il protocollo di trasporto UDP **non** li risolve.

## Indirizzi IP

- Un indirizzo IP **non identifica** un computer, ma una connessione computer-rete.
  - Un computer con connessioni multiple di rete (es. un router) ha assegnato un indirizzo IP per ogni connessione.
- Gli indirizzi sono assegnati alle interfacce di rete
  - un host con N interfacce di rete (es. router connesso ad una LAN e ad N-1 linee punto-punto) ha N indirizzi
  - un host con una interfaccia di rete ha un unico indirizzo IP

## Indirizzi IP: dettagli

- Sono divisi in due parti
  - **network (o prefisso)**: identifica la sottorete
  - **host (o suffisso)**: identifica host e interfaccia
- Assegnamento **indirizzi univoci**:
  - autorità nazionali (NIC, Network Information Center) coordinate a livello mondiale
  - L'amministratore locale assegna un unico suffisso ad ogni coppia host-interfaccia

## Classi di Indirizzi IP

Class	Network	Host	Range of host addresses
A	0		1.0.0.0 to 127.255.255.255
B	10		128.0.0.0 to 191.255.255.255
C	110		192.0.0.0 to 223.255.255.255
D	1110	Multicast address	224.0.0.0 to 239.255.255.255
E	1111	Reserved for future use	240.0.0.0 to 255.255.255.255

**4 CLASSI DI FORMATO**  
I 4 bit iniziali determinano la classe, che a sua volta determina il confine tra Network e Host.

Modo semplice per esprimere indirizzi IP: **rappresentare ogni byte in decimale usando punti come separatori tra i byte**

Esempio: **196.145.63.1**

	32-bit Binary Number	Equivalent Dotted Decimal
	10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
	11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
	00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
	10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
	10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

## Dimensioni delle Reti

La massima dimensione di una rete dipende dalla classe

- Classe A: fino a più di 16 milioni di host
- Classe B: fino a 65536 host
- Classe C: al più 256 host.

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

## Indirizzi Speciali

0 0	Questo host
0 0 ... 0 0 Host	Un host della rete locale
1 1	Broadcast sulla rete locale
Network 1 1 1 1 ... 1 1 1 1	Broadcast su una rete remota
127 (Anything)	Loopback

**Loopback:** messaggi che non lasciano mai il computer locale; sono usati per i test.

## IP - Protocolli di Controllo

- ICMP (Internet Control Message Protocol)
- DHCP (Dynamic Host Configuration Protocol)

## Uso di ICMP

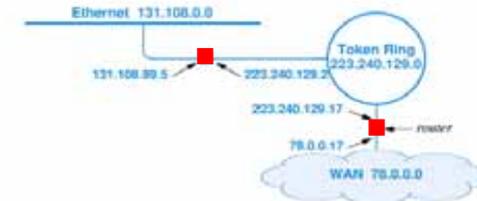
IP utilizza ICMP per migliorare le performance  
I messaggi ICMP sono incapsulati in datagrammi IP

- Programma **ping** (sintassi: `ping <host>`, terminare con CTRL-C)
  - Utilizza il messaggio ICMP **echo request** per verificare la raggiungibilità di un host e calcolare i tempi di risposta
- Programma **traceroute** (sintassi: `traceroute <host>`)
  - Restituisce il percorso completo verso un host
  - Il programma invia datagrammi con TTL=1, 2 ecc.
  - Quando un router riceve un datagramma con TTL=0, invia al mittente un messaggio **time exceeded**
  - Il programma intercetta i messaggi ICMP e ricostruisce il percorso, calcolando i tempi di risposta

## Dynamic Host Configuration Protocol (DHCP)

- Serve per assegnare in maniera dinamica gli indirizzi IP e gli altri parametri di configurazione
- Con DHCP è possibile evitare le configurazioni manuali.
- All'avvio gli host chiedono il proprio indirizzo IP ai server DHCP, inviando le richieste in broadcast
- I server DHCP assegnano due tipi di indirizzi: permanenti (es. per altri server) e volatili
- Gli indirizzi IP volatili sono validati sulla base di un predefinito periodo di assegnazione.

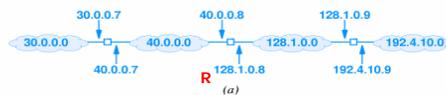
## Routers e Indirizzamento



- Nel router è necessario un indirizzo per connessione: in questo esempio ogni router ne ha due
- Il router dispone di una tabella che associa, ad ogni rete di destinazione, il prossimo router cui inviare i dati
- Il router possiede informazioni di instradamento per ogni rete conosciuta, non per ogni host.

## Tabella del router

- Una maschera di indirizzo consente di individuare la rete di appartenenza dell'host destinazione.
- Viene effettuata una operazione di AND tra l'indirizzo dell'host destinazione ed ognuna delle maschere.
  - Quando il risultato dell'AND è uguale alla rete destinazione, si invia il pacchetto al router indicato nella colonna a destra.
- Es: cosa succede se l'host destinazione è 128.1.10.12?



Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

Tabella di instradamento di R

## Sottoreti e subnet mask

- Ottenere un indirizzo per una nuova rete non è semplice e conveniente
  - Una organizzazione può suddividere la sua rete in sottoreti
  - Es., università -> dipartimenti
  - Un router per ogni sottorete e un router per la rete originaria
- Modifica dello schema di indirizzamento
  - una parte (iniziale) dei bit per l'indirizzo dell'host sono usati per specificare la sottorete di appartenenza
  - All'esterno l'indirizzo IP di un host della sottorete appare ancora un indirizzo della rete originaria
- Subnet-mask:
  - sequenza di 16 bit che demarcano le due parti
  - Una sequenza di 1 seguita da una sequenza di 0:
    - gli 0 corrispondono ai bit che specificano l'indirizzo dell'host (nella sottorete)
  - Il router centrale smista ai router delle sottoreti mettendo la maschera in AND con l'indirizzo IP richiesto



## Il futuro: una nuova versione di IP

**IPv6:** IP versione 6, successore di IP versione 4.

Principali differenze rispetto a IPv4

- indirizzi di 16 byte ->  $2^{128}$  ( $\approx 10^{38}$ ) indirizzi IP possibili!
- header semplificato: 7 campi contro 13 (risparmio nei tempi di computazione dei router)
- funzioni di autenticazione e privacy, basate su crittografia
- supporto delle classi di servizio e della priorità
- supporto più flessibile delle opzioni (header addizionali)

Non completamente compatibile con IPv4: coesistenza decennale.