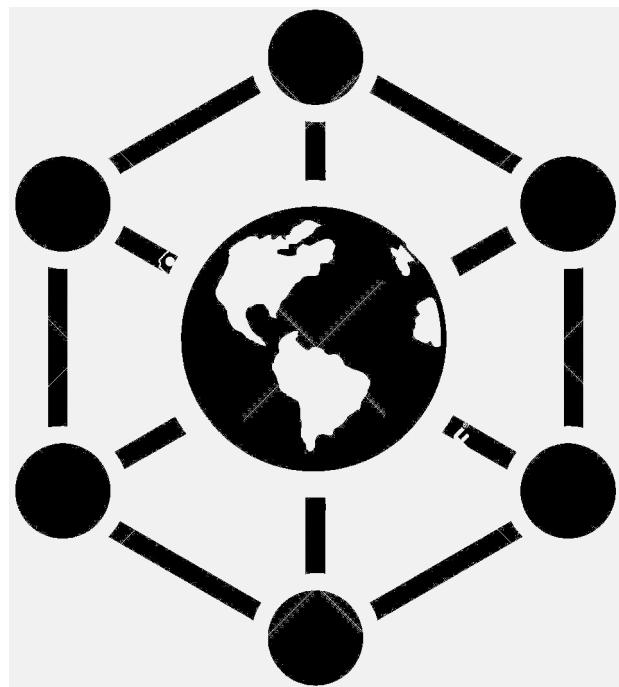


Carmine D'angelo
Emanuele Vitale
Gaetano Vietri
Francesco Tranzillo



Reti di Calcolatori

Asfnazza

INTRODUZIONE

Oggi giorno parlare di reti di calcolatori è errato, perchè oramai non più soltanto i calcolatori sono connessi ad una rete ma anche altri dispositivi (tablet, smartphone, tv, ecc...). Si prevede che entro 5 anni i dispositivi in rete saranno oltre 50 miliardi, si può quindi affermare che le reti oggi giorno influenzano la nostra vita. Una rete è fatta di connessioni, cioè entità interconnesse tra loro. Una di queste reti è Internet, fu creata nel 1969 dalla DARPA con il nome di ARPANET e il suo scopo iniziale era quello di collegare 5 nodi fra di loro, con il tempo questi 5 nodi sono diventati miliardi di miliardi fino ad arrivare alla nascita della rete Internet(*"Un ponte lanciato a colmare il divario tra spazio e tempo"*). Il 95% dell'infrastruttura di internet si trova sotto il livello dell'acqua ed è composta da vetro e silicio(fibra ottica), il resto 5% si trova sopra il livello dell'acqua ed è composta da vari elementi (rame, doppini, reti wireless, ecc...). Il fatto che si trovi sott'acqua porta anche ad altri problemi, il maggior problema sono gli squali attirati dalle onde elettromagnetiche che possono mordere i cavi, e per sostituirli ci vogliono 2 navi quindi è un'operazione costosa. Una rete è fatta di routers che trasmettono per di più segnali analogici, sono utilizzati perchè ad alto livello si lavora con quest'ultimi; infatti convertire un segnale da digitale ad analogico o viceversa comporta un delay nel tempo di trasmissione. Per trasmettere un segnale analogico vengono utilizzati dei prismi che non hanno problemi di delay o latenza.

A questo punto sorge una domanda ma come è organizzata la rete di Internet? Ci sono varie tipologie di strutture che verranno studiate in seguito, ma nessuna di quella è utilizzata da internet, questo perchè ognuna di loro ha un problema. Internet alla fini utilizza una via di mezzo, si dice che si sia trovato il giusto equilibrio tra caos e quiete. Un segnale infatti nella rete di Internet sfrutta il "principio dei 6 gradi associazioni"ma un pò modificato, infatti se proviamo a connetterci ad un sito e vedere quanti router passiamo prima di arrivarci vedremo che non supereremo mai i 32 salti fra router, questo perchè ogni volta riesce a capire qual è il nodo più vicino al punto di arrivo. Questa cosa riesce anche perchè abbiamo tantissimi nodi con poche connessioni ma pochi nodi con molte connessioni (i nodi sono i provider della connettività). Tramite il *lg del numero di nodi* si può ottenere la distanza media che viene percorsa tra due nodi.

COMPONENTI DI UNA RETE

Hardware:

- Apparati di interconnessione
- Apparati per il controllo della trasmissione

Software:

- Protocolli e Drivers:
 1. codifica e formattazione dei dati.
 2. rilevamento di errori e correzione.
 3. controllo della congestione.
 4. Qualità del servizio.

FUNZIONALITÀ DI UNA RETE

Una rete serve per garantire un'accesso a distanza a delle risorse su larga scala. Una rete deve essere affidabile perchè non deve perdere i dati efficiente perchè deve farlo nel modo più veloce. Scalabile perchè l'infrastruttura che realizziamo si deve adeguare al flusso dei dati che inviamo. Deve essere anche eterogeneo, cioè deve essere capace di interconnettersi tra diversi dispositivi.

Una rete deve essere in grado di trovare dati sbagliati, corrotti, eventuali duplicazioni e essere anche in grado di riordinare i pacchetti che eventualmente sono arrivati in ordine diverso.

L'informazione si partiziona in tante unità che vengono trasmesse in sequenze, la rete in questa fase deve individuare il percorso più veloce, meno costoso, ecc., la rete quindi deve essere in grado di fare l'ingegneria del traffico, in modo da trovare il percorso ottimale per raggiungere uno scopo.

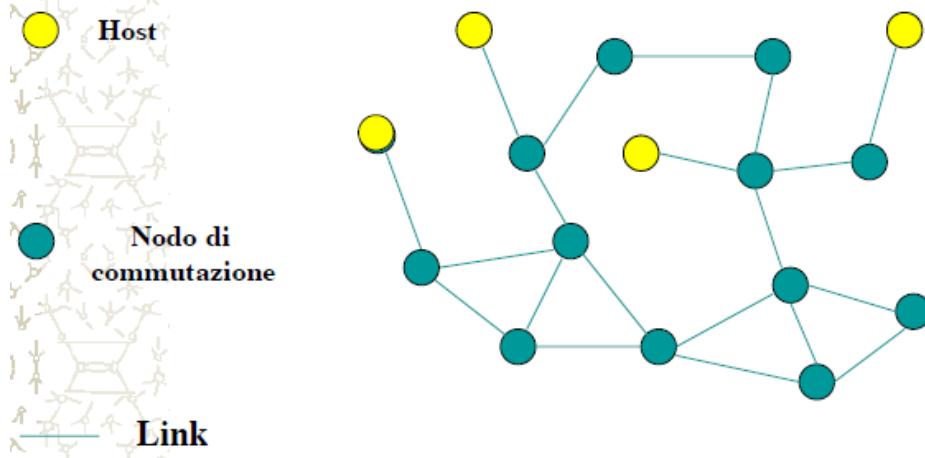
Ultimamente l'utilizzo delle tecnologie informatiche e delle telecomunicazioni ha permesso la nascita delle reti telematiche, cioè un insieme di dispositivi informatici mutuamente collegati tra di

loro. Una rete di Telecomunicazione può essere definita, in modo funzionale, come un sistema distribuito che permette la trasmissione di informazioni da un capo all'altro, consentendo un indirizzamento universale. Quindi deve implementare:

- La funzionalità per il **trasporto dell'informazione**: un'informazione deve essere trasmessa da un inizio ad una fine.
- Funzionalità per l'**indirizzamento** e per la **commutazione**: capire a che sono inviate le informazioni.

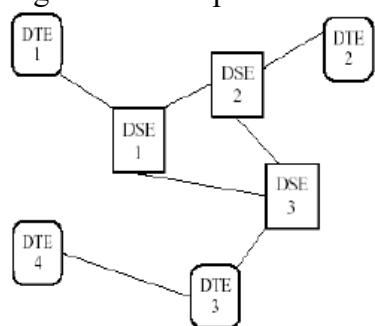
Un possibile modello fisico che implementa la definizione data di rete di telecomunicazione deve prevedere la presenza:

- **hosts**: dispositivi autonomi connessi a una rete.
- **links**: collegamenti tipicamente **point-to-point**, interconnessi fra loro tramite nodi commutazione.
- **nodi di commutazione**: il cui compito è quello di riconoscere le richieste per l'apertura di una connessione e fare in modo che i dati, relativi a tale connessione, arrivino al nodo di destinazione.



TERMINOLOGIA

Gli apparecchi che si devono collegare alla rete si chiamano DTE (*Data Terminal Equipment*), il DTE può essere dunque un supercalcolatore, un semplice PC o anche semplicemente un qualsiasi oggetto connesso in rete come utente finale. Si può perciò affermare che lo scopo della rete è l'interconnessione dei vari DTE per la condivisione delle risorse, lo scambio di dati e la cooperazione tra i processi applicativi. Un DTE si collega alla rete tramite un apposito dispositivo che si chiama DCE(*Data CircuitTerminating Equipment*), che svolge le funzioni di sorgente e destinazione di una comunicazione dati. Il DTE in trasmissione converte i dati dell'utente in segnali e in ricezione riconverte i segnali ricevuti. In ambito di Ethernet può essere uno switch o un router. Un DSE(*Data Switching Equipment*) o nodo di **commutazione** è un nodo intermedio della rete, senza alcuna funzione di supporto diretto agli utenti, la cui principale funzione è quella di commutare(switch) il traffico tra due o più DTE non direttamente collegati tra loro. La commutazione avviene attraverso la cross-connessione fra due interfacce, temporanea o semipermanente. Di seguito un esempio di DSE:

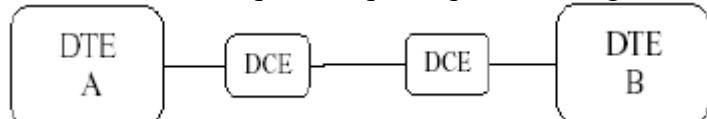


Sulla base di opportuni criteri e di adeguati informazioni di servizio, un DSE seglie dunque la strada (percorso di rete) che i messaggi devono seguire per arrivare alla loro destinazione. A parte i malfunzionamenti, il DSE può operare una scelta di percorso anche in ragione del carico delle linee, questo problema rientra nel vasto campo del cosiddetto **controllo della cogestione**.

MODALITÀ DI TRASMISSIONE DI UNA CONNESSIONE

Di seguito sono elencate varie modalità di trasmissione:

Point-to-point: Un circuito fisico è detto point-to-point quando collega due DTE.



Questo collegamento è spesso utilizzato nella connessione tra due computer oppure in quella tra un computer ed un terminale. I principali vantaggi sono:

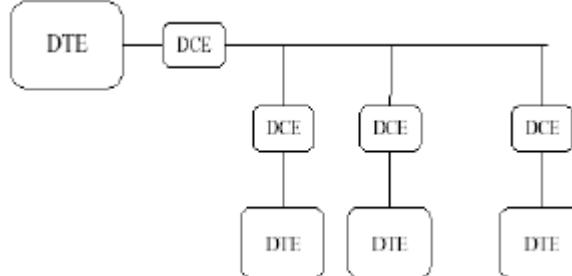
- semplicità di gestione: quello che viene trasmesso da un DTE è sempre diretto all'altro;
- tempi di attesa nulli: il DTE che deve trasmettere trova sempre il circuito disponibile, per cui può trasmettere ogni volta che ne ha bisogno.

Ci sono però anche alcuni svantaggi:

- in primo luogo, il costo della linea, specie se essa corre su una distanza notevole, può diventare elevato;
- inoltre, un'organizzazione che volesse collegare, al proprio mainframe, 10.000 terminali con questa tecnica, dovrebbe provvedere a installare 10.000 linee di collegamento.

La trasmissione point-to-point con un trasmettitore e un ricevitore a volte è chiamata **unicasting**.

Multi-point: un circuito fisico multi-point consiste nel mettere più di due DTE sulla stessa linea.



Possono nascere problemi di contesa.

Broadcast: hanno un solo canale di comunicazione che è condiviso fra tutte le macchine della rete. Brevi messaggi, chiamati in alcuni contesti **pacchetti**, sono inviati a ciascuna macchina e ricevuti da tutte le altre. Un campo indirizzo nel pacchetto individua il destinatario. Alla ricezione del pacchetto, una macchina controlla il campo indirizzo, se il pacchetto è indirizzato ad essa il pacchetto viene catturato, altrimenti è ignorato. I sistemi broadcast danno di solito anche la possibilità di indirizzare un pacchetto a tutti o destinatari usando uno speciale codice speciale nel campo di destinazione, questo metodo è chiamato **broadcasting**. Un'altra possibilità è inviare il pacchetto ad un sottoinsieme degli elaboratori, si parla in questo caso di **multicasting** e succede che solo gli elaboratori del suddetto sottoinsieme prendono in considerazione il pacchetto, che invece viene ignorato dagli altri. In ogni pacchetto è presente un bit che indica che si tratta di una trasmissione multicasting, mentre i restanti bit contengono l'indirizzo del gruppo destinatario ed ovviamente i dati. In particolare, il bit che indica o meno il multicasting appartiene allo stesso campo contenente l'indirizzo: se N sono i bit di tale campo, quindi, solo N-1 sono riservati all'indirizzo vero e proprio. Una rete Broadcast si può suddividere in statica e dinamica. Le statiche consistono nel suddividere il tempo in intervalli discreti e usare un algoritmo round-robin, permettendo ad ogni macchina di eseguire il broadcast solo quando è il proprio turno, questo tipo di allocazione spreca la capacità del canale quando la macchina non ha nulla da trasmettere,

per questo molte volte si cerca di allocare il canale dinamicamente. Le allocation dinamica per un canale condiviso possono essere centralizzati o non centralizzati. In quella centralizzato esiste una singola entità, per esempio un'unità di arbitraggio del bus che stabilisce a chi spetta di volta in volta l'uso del mezzo.

- **Centralizzata:** non esiste un'entità centrale, ogni macchina deve decidere in autonomia se trasmettere, stabilisce quindi chi deve trasmettere.
- **Distribuita:** il canale è distribuito ad ogni stazione in un determinato intervallo di tempo, e ogni stazione può utilizzarlo per quell'intervallo ma mai contemporaneamente.

FLUSSI E CIRCUITI

Il flusso trasmittivo lungo una linea di comunicazione può avvenire in 3 modi diversi.

Il caso più semplice è quello della trasmissione **simplex**, in cui i dati viaggiano lungo una sola direzione. Quando due entità sono collegate, l'una ha sempre il ruolo di trasmittente, l'altra sempre il ruolo di ricevente, senza mai alternarsi, come avviene ad esempio nella televisione. Un esempio solo le trasmissioni radio-televisive e le reti di comunicazione delle agenzie stampa.

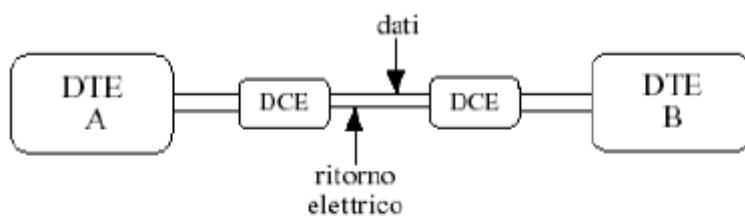
Generalmente non è utilizzato per la comunicazione dei dati anche quando il flusso è unidirezionale, perché nella comunicazione dei dati è necessario il controllo della correttezza della ricezione, questa operazione può essere fatta solo dall'utente una volta ricevuto il messaggio, in caso di errore richiede la ritrasmissione.

Un'altra trasmissione è l'**half-duplex**, qui i dati possono viaggiare in entrambe le direzioni ma non contemporaneamente. È il modo classico di operare dei terminali conversazionali, che prevede l'invio di una richiesta, la ricezione della risposta e così via.

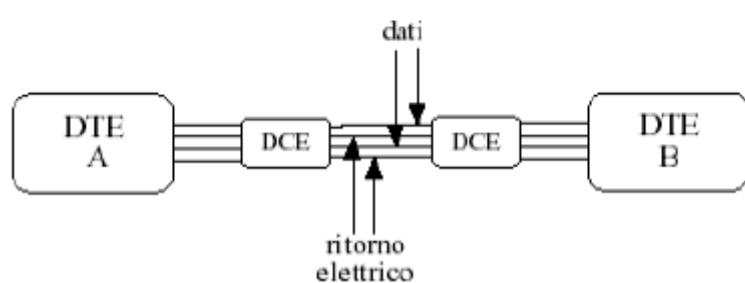
L'ultimo tipo e quello più completo è la **full-duplex**, in questo caso i dati possono viaggiare contemporaneamente in entrambe le direzioni. È molto indicato per le reti a configurazione multipunto, infatti è possibile che il DTE master riceva una richiesta da un DTE slave e contemporaneamente invii una risposta ad un altro DTE slave.

Molte volte si confondono le caratteristiche fisiche dell'half e full duplex; l'half-duplex si realizza su un circuito a due fili, con un filo per i dati e l'altro per il ritorno elettrico; mentre per il full-duplex richiede il doppio **doppino telefonico**, ossia 4 fili, di cui due per i dati e gli altri due per i rispettivi ritorni elettrici.

circuito a 2 fili



circuito a 4 fili



Tutte le affermazioni precedenti sono vere, ma è anche vero che la trasmissione full-duplex è possibile anche sul circuito a due fili, ossia sul singolo doppino telefonico, quest'ultima risulterà più lenta di quella con due doppini telefonici. Il tipo di linea dipende dalle esigenze, se si deve fare un normale circuito telefonico commutato allora si fa l'uso dei due fili, se invece la linea è ericamente allora il collegamento può essere effettuato sia con 2 che con 4.

LA COMMUTAZIONE

La **commutazione** è quell'operazione che predispone il percorso che le informazioni emesse dal mittente devono seguire per raggiungere il destinatario, esistono due tipi di commutazione:

- **commutazione di pacchetto(datagram).**

- **Commutazione di circuito.**

Commutazione di pacchetto: la commutazione di pacchetto si basa sulla suddivisione del messaggio in più unità autonome, ciascuna corredata dalle opportune informazioni di controllo:

- identificativi del mittente e del destinatario;
- numero d'ordine del pacchetto all'interno dell'intero messaggio.

Un'altra caratteristica è la capacità di instradamento autonoma nei singoli organi di commutazione della rete:

- Ogni pacchetto è instradato indipendentemente (e su percorsi differenti).
- La rete non ne garantisce l'inoltro e la ricezione nel giusto ordine.

Le risorse devono essere utilizzate in modo ottimale in ragione del principio di **multiplazione statistica**: il flusso di informazioni è segmentato in pacchetti divisi statisticamente sul fabbisogno di quello che deve essere spedito. La moltiplicazione statica è semipermanente.

Commutazione di circuito: tramite una serie di dispositivi di commutazione intermedia si determina una connessione fisica diretta, anche se effettivamente priva di continuità elettrica/ottica, che simula un unico cavo/canale tra le due stazioni che necessitano di comunicare. Tale connessione è assegnata permanentemente ed unicamente alla coppia di stazione ed è mantenuta fino al termine della comunicazione.

Le sue caratteristiche sono la presenza di un tempo di attivazione della connessione e la bassa efficienza nell'uso del mezzo in quanto la connessione rimane "instaurata" anche quando i due tenti momentaneamente non la utilizzano per comunicare (es: la chiamata). La moltiplicazione statica è temporanea.

PRO E CONTRO

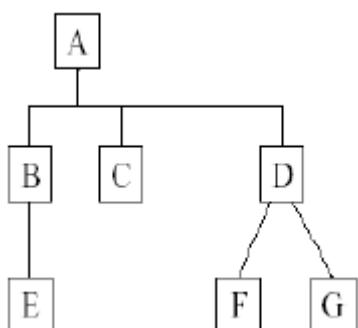
La commutazione di pacchetto è in media più scalabile e ottimizza la gestione delle risorse. È estremamente efficiente per il trasporto di pacchetti di piccole dimensioni (e-mail, rlogin, transazioni www) che comportano trasferimenti di alcune centinaia di KB. Però è evidente l'inadeguatezza della commutazione di pacchetto per il trasporto di grandi quantità di informazioni (diversi Tera o Peta-bytes) sulla rete. Gestire decisioni di instradamento ogni 1500 Bytes per trasferire ad es. 1.5TB di dati richiede di reiterare le stesse decisioni circa un bilione di volte su tutti i routers coinvolti. È inoltre praticamente impossibile riservare risorse in anticipo o fare ingegneria del traffico scegliendo i percorsi. La logica del multiplexing statistico non scala su grandi volumi.

TOPOLOGIE DI RETE

Prende il nome di topologia di rete la configurazione geometrica dei collegamenti tra i vari componenti della rete. Esistono vari tipi di topologie, la scelta dei quali è legata al conseguimento di alcuni obiettivi fondamentali:

- Massima affidabilità: tasso di guasto e ridondanza.
- Scalabilità: margini di crescita.
- Altro rendimento complessivo: banda e latenza.
- Minimi costi di startup ed esercizio.

La più comune è la tipologia di rete gerarchica o ad albero:

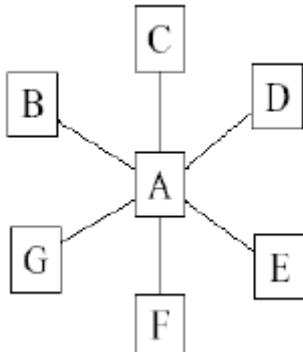


Il traffico di dati va dai nodi dei livelli più bassi verso i nodi intermedi o verso il nodo del livello più alto. Quest'ultimo è in genere il nodo più potente dell'intera struttura, visto che deve provvedere alle richieste di tutta la rete. Spesso è responsabile della gestione completa della rete, è anche possibile che ci sia una cooperazione, per la gestione ed il controllo della rete, tra il nodo principale e alcuni o tutti i nodi del livello immediatamente inferiore. Gli inconvenienti sono: il sovraccarico del nodo principale che può portare ad un rallentamento

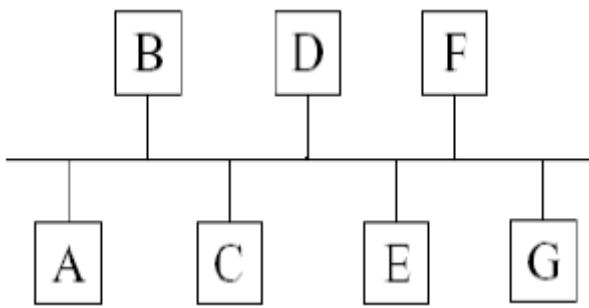
dei servizi per tutti gli utenti; e la caduta del nodo principale che rende inutilizzabile l'intera rete. A quest'ultimo inconveniente si può ovviare adottando una **politca di back-up**, bisogna cioè mettere in grado uno o più nodi della rete di svolgere le stesse attività di quello principale in caso che quest'ultimo venisse a mancare.

La **rete a stella** è simile ad un albero, con la fondamentale differenza che non c'è alcuna distribuzione funzionale, ossia non ci sono livelli diversi ma solo uno collegato al nodo centrale.

- Bastano $n-1$ collegamenti per connettere n nodi.
- Controllo centralizzato del traffico.
- Problemi di robustezza: single point of failure.
- Problemi di capacità del nodo centrale.
- Non scala col numero di nodi.



Rete a dorsale o bus condiviso, è diventata popolare in quanto è adottata dalle reti locali tipo **Ethernet**, è definita anche **BMA(Broadcast Multiple access)**. La caratteristica è che c'è un unico cavo che collega tutte le stazioni, come nello schema seguente:

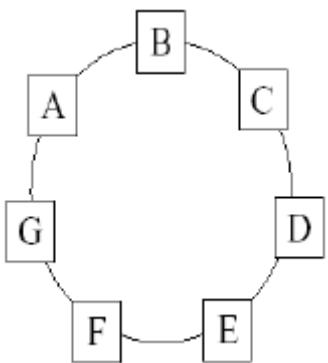


La trasmissione di una stazione viene ricevuta da tutte le altre. È l'analogo del bus che viene usato nelle architetture dei moderni calcolatori: il bus è l'insieme di cavi elettrici che mettono in comunicazione tutti i dispositivi da cui il calcolatore è costituito. In questo caso mette in comunicazione i vari nodi di rete. In ogni istante solo un elaboratore può trasmettere, mentre gli altri devono astenersi, in maniera del tutto analoga

a quanto avviene in un singolo calcolatore, dove il bus è a disposizione di un dispositivo per volta; è quindi necessario un meccanismo di **arbitraggio** per risolvere i conflitti quando due o più elaboratori vogliono trasmettere contemporaneamente; l'arbitraggio può essere centralizzato o distribuito. Il vantaggio è nella tecnologia di accesso, il quale, nel caso di rete locale, è davvero molto semplice. I principali inconvenienti sono invece i seguenti:

- i potenziali problemi di prestazioni dovuti al fatto che un unico portante trasmissivo serve tutte le stazioni;
- una eventuale interruzione del portante mette fuori uso l'intera rete;
- la mancanza di punti di concentrazione rende difficoltosa l'individuazione di eventuali punti di malfunzionamento.

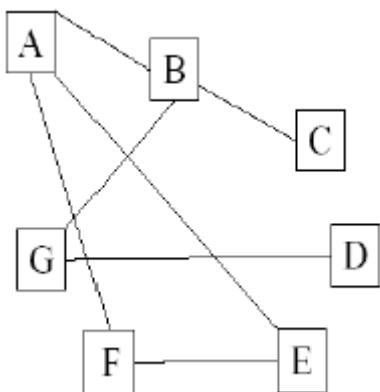
Rete da anell (ring), è stata resa popolare dalle prime LAN di tipo *Token-Ring* o FDDI. La trasmissione è in questo caso unidirezionale, ma essendo l'anello un circuito chiuso su se stesso, è possibile inviare un messaggio da qualsiasi stazione verso un'altra. In un ring ogni bit circumnaviga l'anello, anche qui è necessario un meccanismo di arbitraggio (token). Un importante pregio di questa topologia è che apre ottime prospettive per l'utilizzo della **fibra ottica**.



- Bastano n collegamenti per connettere n nodi.
- Doppio percorso fra coppie di nodi.
- Non scala col numero di nodi: percorsi infinitamente lunghi.
- Problemi di congestione sui percorsi.
- Problemi di capacità dei nodi.

Rete a maglia o mesh, consiste nel collegare le varie stazioni con diversi circuiti. Una topologia di questo tipo assicura buone prestazioni in quanto il traffico viene ripartito sui vari percorsi, inoltre, essa conferisce una elevata affidabilità all'intera struttura, proprio grazie alla presenza di percorsi multipli.

Allo stesso tempo, però, i costi dei collegamenti possono anche essere elevati ed inoltre la gestione della struttura è chiaramente più complessa rispetto agli altri casi esaminati.



- Servono $n(n-1)/2$ collegamenti per connettere n nodi -troppi!
- Massima affidabilità e percorsi dedicati.
- Non scala col numero di nodi: costo inaccettabile.

PROTOCOLLI

Un protocollo è una serie di norme, convenzioni e tecniche per lo scambio di dati, comandi e informazioni di controllo tra due elementi. Esistono vari livelli di protocolli, si va dal livello più basso, che regola il modo di trasmettere i segnali sulla linea (**protocollo di conessione**), al livello più alto, che indica come interpretare dati e comandi a livello applicativo, passando per una serie variabile di ulteriori livelli. Un tipo di protocollo potrebbe essere il seguente:

Una volta individuata la stazione (DTE) destinazione, bisogna stabilire quale strada usare per connetterla alla stazione(DTE) sorgente. Questa scelta compete al cosiddetto **protocollo di instradamento (routing protocol)** che quindi si aggiunge al **protocollo di linea** necessario al passaggio di dati su ciascuna linea. In altre parole, solo dopo la scelta del percorso interviene il protocollo di linea per la gestione dei singoli collegamenti. Tale protocollo viene usato tante volte quante sono le linee che costituiscono il percorso fissato.

ES:

Consideriamo la figura seguente, in cui è presente un terminale, situato fisicamente a Torino, che intende connettersi ad una applicazione situata fisicamente a Verona, passando per Milano. Il terminale di Torino invia un messaggio per il terminale di Verona usando un protocollo di linea che prevede una risposta da parte della stazione ricevente sull'esito positivo o negativo della trasmissione. Il protocollo di linea effettua la trasmissione solo fino al nodo intermedio di Milano, per cui è quest'ultimo che effettua il controllo di correttezza della trasmissione. Si parla in questo caso di **Protocollo di Trasporto**. Un **protocollo di linea**, che agisce sulle singole tratte, è di tipo **box-to-box**, mentre un **protocollo di trasporto** è di tipo **end-to-end**.

NOTA:

End-to-end: se si hanno due applicazioni che comunicano tramite una rete, tutte le funzioni e le operazioni specifiche richieste da tali applicazioni, come il controllo degli errori, devono essere realizzate ed eseguite in modo completo nei nodi terminali (o end point) e non nei nodi intermedi della rete. Ha diversi limiti, non può essere applicato nel caso in cui le applicazioni siano eseguite su nodi diversi, non chiarisce abbastanza quali siano le funzioni che devono essere implementate

nel nodo terminale, in quanto si limita a dire "tutte le funzioni e le operazioni specifiche richieste da tali applicazioni", infine non chiarisce abbastanza bene cosa fare nel caso in cui le funzioni richieste non possano essere realizzate ed eseguite in modo completo nei nodi terminali.

STANDARDIZZAZIONE DELLE RETI

Esistono molti costruttori e fornitori di reti, ognuno con le proprie idee sul modo di fare le cose. In assenza di un coordinamento ci sarebbe il caos totale su cosa applicare, per questo sono stati creati degli standard di rete. Gli standard non permettono solo la comunicazione tra computer diversi, ma aumentano il mercato per i prodotti che vi aderiscono. Più è ampio quest'ultimo più benefici aumenano, come il calare dei prezzi dei prodotti. Gli standard ricadono in due categorie: de facto e de jure. Gli standard **de facto** (in latino della realtà), sibi quelli che si sono stabiliti senza piani formali. Il PC IBM e i suoi successori sono un esempio per lo standard de facto dei personal computer, UNIX come sistema operativo per le facoltà universitarie di informatica.

Gli standard **de jure** (in latino per legge) sono al contrario formali, adottati da qualche organismo di standardizzazione autorizzato. Queste autorità sono divise in due classi: quelle stabilite dalle nazioni, e quelle che comprendono organizzazioni volontarie.

Le principali autorità di standardizzazione sono le seguenti:

- **PTT (Post, Telephone and Telegraph)**: amministrazione statale che gestisce i servizi trasmissivi (in Italia è il *Ministero delle Poste e delle Telecomunicazioni*);
- **CCITT (Consultative Committee for International Telegraph and Telephone)**: organismo internazionale che emette le specifiche tecniche che devono essere adottate dalle PTT. E' entrato da poco a far parte dell'**ITU (International Telecommunication Union)**;
- **ISO (International Standard Organization)**: il principale ente di standardizzazione internazionale, che si occupa fra l'altro anche di reti;
- **ANSI (American National Standards Institution)**: rappresentante USA nell' ISO;
- **UNINFO**: rappresentante italiano, per le reti, nell'ISO;
- **IEEE (Institute of Electrical and Electronic Engineers)**: organizzazione professionale mondiale degli ingegneri elettrici ed elettronici; ha gruppi di standardizzazione sulle reti;
- **IRTF (Internet Research Task Force)**: comitato rivolto agli aspetti di ricerca a lungo termine in merito alla rete Internet;
- **IETF (Internet Engineering Task Force)**: comitato rivolto agli aspetti di ingegnerizzazione a breve termine della rete Internet;
- **IAF (Internet Architecture Board)**: comitato che prende le decisioni finali su nuovi standard da **adottare per Internet, di solito proposti da IETF o IRTF**.

TIPI DI RETI

LAN(*Loical Area Network*), sono reti private installate all'interno di un singolo edificio o campus, con dimensione fino a qualche Km. Sono molto utilizzate per collegare personal computer e workstation negli uffici delle aziende e nelle fabbriche, allo scopo di condividere risorse (ad esempio stampanti) e scambiare informazioni. Si distinguono dalle altre reti per : dimensione, la tecnologia di trasmissione e la topologia.

Le LAN hanno dimensioni contenute, il che significa che il tempo di trasmissione più sfavorevole ha un limite, che è noto. Conoscere questo limite permette l'uso di alcune tecniche che altrimenti non sarebbero applicabili. Le LAN possono usare un cavo a cui sono connesse tutte le macchine.

Lavorano tradizionalmente ad una velocità che varia tra 10Mbps e 100Mbps, hanno bassi ritardi e pochissimi errori. Le più recenti operano fino a 10Gbps.

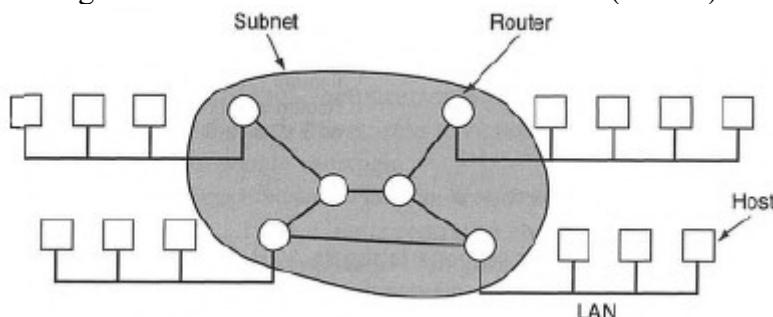
Per le LAN broadcast sono possibili differenti tipologie. In una rete bus, a ogni istante è master soltanto una macchina, tutte le altre devono aspettarsi dal trasmettere, questo è possibile tramite un sistema di arbitraggio. Un esempio di rete è la IEEE 802.3, chiamata abitualmente **Ethernet**, ed è una rete a broadcast a bus con controllo non centralizzato, infatti tutti i computer possono trasmettere quando vogliono, se due o più pacchetti collidono attendono per un tempo casuale e

riprovano.

Un secondo tipo di sistema broadcast è l'anello, in cui ogni bit si propaga in modo autonomo senza aspettare il resto del pacchetto a cui appartiene. L'accesso all'anello è gestito assegnando dei turni alle macchine IEEE 802.5 (token ring IBM).

MAN (Metropolitan Area Network), copre un'intera città, l'esempio più nodo di MAN è la rete di televisione via cavo disponibile in molte città degli Stati Uniti. Questo sistema sviluppato partendo dagli originari sistemi di antenna comunitari, col tempo molte aziende iniziarono ad interessarsi a questi sistemi, ottenendo contratti per cablare intere città. Quando Internet iniziò ad attirare un pubblico di massa, le aziende capirono il potenziale di questo servizio, e il sistema via cavo inizia a trasformarsi piano piano in una MAN. Le prestazioni classiche raggiunte sono comprese tra i 2 Mb/s e i 10 Gb/s. Inizialmente era basata sulle tecnologie delle reti geografiche ma su scala urbana, ultimamente invece si è affermata la tecnologia Ethernet ed effettivamente si arriva ad usare fino a 10 Gb/s.

WAN (Wide Area Network) copre un'area geograficamente estesa. Racchiude una raccolta di macchine destinate a eseguire programmi utente, queste macchine sono chiamate **host**. Gli host sono collegati da una **communication subnet**. Gli host sono di proprietà dei clienti, mentre la subnet è generalmente gestita da una compagnia telefonica o un Internet provider. Il compito di una subnet è quello di trasportare i messaggi da un host all'altro. Nella maggior parte delle WAN la subnet è formata da due elementi: linee di trasmissione e elementi di commutazione. Le **linee di trasmissione** sostengono i bit tra le macchine, possono essere realizzate con cavo di rame, fibra ottica o collegamenti radio. Gli **elementi di commutazione** sono computer specializzati che collegano tre o più linee di trasmissione. Quando i dati arrivano ad una linea ricevente, l'elemento di commutazione deve scegliere una linea di uscita su cui inoltrarlo (**router**).



Nella maggior parte delle WAN la rete contiene molte linee di trasmissione, ciascuna delle quali collega una coppia di router, se due router non condividono la stessa linea di trasmissione ma vogliono comunicare devono farlo indirettamente tramite altri router. Quando un pacchetto viene inviato da un router verso un altro, attraverso router intermedi, il pacchetto viene ricevuto integralmente da ciascun router intermedio, memorizzato finché non si libera la linea di uscita necessaria, e poi inoltrato. Una subnet organizzata secondo questo principio si chiama **store-and-forward** o **packet-switched**. Tutte le WAN hanno questo tipo di subnet. Se i pacchetti inviati sono piccoli e hanno la stessa dimensione, sono spesso chiamati celle. Non tutte le WAN sono a commutazione di pacchetto. Una seconda possibilità per una WAN è il sistema satellitare. Ogni router ha un'antenna attraverso la quale può trasmettere e ricevere. Tutti i router possono ascoltare l'uscita *dal* satellite, e in alcuni casi anche le trasmissioni dei router paritetici *verso* il satellite. A volte i router sono collegati a una subnet cablata punto-punto, e solo alcuni hanno un'antenna per il satellite. Le reti satellitari sono intrinsecamente di tipo broadcast e sono particolarmente utili quando la proprietà broadcast è importante. Le WAN hanno spesso una **struttura a maglia** ed una configurazione dei collegamenti a volte complessa; la struttura a maglia serve a garantire strade alternative nel caso di indisponibilità di qualche componente o per ripartire il traffico su più percorsi. A scopo di interoperabilità sono basate su tecnologie di comunicazione standardizzate dal CCITT.

Reti wireless

La comunicazione digitale senza fili (wireless) non è un'idea nuova. Già nel 1901 il fisico Guglielmo Marconi dimostrò la telegrafia senza fili da una nave usando il codice Morse (punti e linee sono binari, dopotutto). I sistemi digitali wireless moderni hanno prestazioni migliori, ma l'idea di base è la stessa.

In prima approssimazione le reti wireless si possono classificare in tre categorie principali:

1. connessioni all'interno di un sistema;
2. LAN wireless;
3. WAN wireless.

La connessione all'interno di un sistema coinvolge il collegamento delle periferiche di un computer tramite segnali radio a portata ridotta.

per abolire i cavi di collegamento die computer si pensò alla nascita di una piccola rete wireless, il Bluetooth.

Il **Bluettooh** permette inoltre di collegare al computer macchine fotografiche digitali, cuffie senza fili, scanner e altri dispositivi semplicemente portandoli nella zona di copertura. Niente cavi e niente installazione di driver: solo avvicinare, accendere e usare. Per molti questa semplicità d'uso è un grande vantaggio.Nella loro forma più semplice, le reti di collegamento interne al sistema usano il paradigma master-slave.

Il passo successivo nelle reti wireless sono le LAN. Si tratta di sistemi dove ogni computer ha un modem radio e un'antenna con cui può comunicare con altri sistemi. Spesso c'è un'antenna nel soffitto con cui i computer dialogano. Tuttavia, quando i computer sono abbastanza vicini, possono comunicare direttamente tra di loro in una configurazione peer-to-peer. Le LAN wireless stanno diventando sempre più comuni nei piccoli uffici e nelle abitazioni (dove l'impegno per installare Ethernet è considerato eccessivo), negli edifici per uffici più vecchi, nelle sale riunioni e in altri posti. Lo standard per LAN wireless, chiamato IEEE 802.11, che è implementato dalla maggioranza dei sistemi e che sta diventando estremamente diffuso. Il terzo tipo di reti wireless è usato nei sistemi su area estesa. La rete radio usata dai telefoni cellulari è un esempio di sistema wireless a banda ridotta. Il sistema è già arrivato alla terza generazione. La prima generazione era analogica e solo per la voce. La seconda generazione è digitale e solo per la voce. La terza generazione è digitale e trasporta voce e dati. In un certo senso, le reti wireless cellulari assomigliano a LAN wireless, eccetto che le distanze sono molto superiori e i bit rate molto più bassi. Le LAN wireless possono funzionare a cadenze che si spingono a 50 Mbps su distanze di decine di metri. I sistemi cellulari lavorano sotto a 1 Mbps, ma la distanza tra la stazione base e il computer o telefono si misura in chilometri invece che metri.

Sono in sviluppo anche reti wireless a larga banda e copertura estesa. Il focus iniziale è l'accesso a Internet ad alta velocità da abitazioni e uffici, scavalcando il sistema telefonico. Questo servizio è spesso chiamato *local multipoint distribution service*, per esso è stato sviluppato uno standard, chiamato IEEE 802.16. Quasi tutte le reti wireless prima o poi si collegano alla rete fissa per consentire l'accesso a file, database e Internet.

Le **reti locali domestiche** sono all'orizzonte. L'idea di base è che in futuro la maggior parte delle abitazioni sarà predisposta per la rete locale; ogni dispositivo domestico sarà capace di comunicare con ogni altro, e tutti quanti saranno accessibili tramite Internet. Questo è uno di quei concetti visionari che nessuno ha previsto (come il telecomando della TV o i telefoni cellulari), ma una volta arrivati nessuno riesce a immaginarsi come poteva vivere senza.

Esinuo molte altri tipi di reti come la **PAN** (*Personal Area Network*) o la **BAN** (*Body Area Network*) che sta nascendo nell'ultimo periodo.

Una caratteristica comune fra queste reti è il modo in cui può avvenire la comunicazione fra due DTE della rete. Ci sono infatti due modi:

- **Connection oriented mode (orientato alla connessione):** i due DTE prima di effettuare lo scambio di dati, si assicurano della presenza reciproca di linea, fatta questa verifica, viene instaurata la connessione (o colloquio o sessione), la quale dura per tutto il tempo necessario allo scambio dati, non appena tale scambio è terminato, anche la connessione

viene abbandonata. La connessione è continuamente gestita dal software dei due DTE, il quale svolge diverse funzioni:

1. gestione del ritmo di intercambio (velocità di trasmissione);
2. Controllo delle regole dello scambio;
3. Capacità di interrompere la controparte (per inviare un messaggio urgente);
4. Controllo degli errori ed eventuale loro correzione.

Tutti questi controlli assumono importanza critica nella WAN, data la bassa affidabilità delle linee.

- **Connectionless mode (non orientato alla connessione):** un DTE può inviare un messaggio all'altro DTE anche se questo non è presente in linea; è come affidare le lettere alla posta, sprando che vengano consegnate. Il vantaggio è che non sono necessari servizi di controllo o di supporto, il che può essere vantaggioso per le LAN, mentre non è molto opportuno per le WAN, per i citati problemi di scarsa affidabilità. Il problema principale del *connectionless mode* riguarda il controllo degli errori che, sia pure raramente, possono verificarsi: infatti, non essendoci controlli immediati durante la trasmissione, il DTE sorgente non può sapere come è andata la trasmissione. D'altra parte, *l'onere dei controlli ripetitivi spesso diventa inutile sulle reti ad alta affidabilità, dove gli errori sono decisamente pochi*. La soluzione cui si può pensare è allora quella di affidare il controllo degli errori direttamente alle applicazioni, il che alleggerisce i protocolli di linea, che possono occuparsi solo del trasporto dei dati, nonché anche i nodi intermedi, che devono occuparsi sono di instradare i dati sui percorsi desiderati. **Quest'ultimo concetto è di importanza cruciale.**

NOTA:

La prima modalità è tipica della commutazione di circuito, la seconda di quella di pacchetto. commutazione del pacchetto: se un dato viene perso la rete fisica non ci assicura che il dato sarà ricevuto e reinviato.

circuiti orientati alla connessione : si crea una rete virtuale che garantisce all'utente la corretta ricezione del pacchetto, riinviadolo in caso di perdita.

CONTROLLO DI CONGESTIONE DEL FLUSSO

Due DTE della rete comunicano tramite due nodi intermedi, ad es. DSE1 e DSE2. Se affidiamo il controllo degli errori ai protocolli di linea, ciascun DSE, ricevendo un *pacchetto* di dati, ne controlla sempre la correttezza: se non ci sono errori, il pacchetto viene instradato, altrimenti viene inviato al mittente un messaggio che richiede la ritrasmissione. Se il collegamento è ad alta velocità, il DSE non può concedersi il lusso di effettuare questi controlli; l'unica sua funzione deve essere quella di prendere i dati in arrivo ed instradarli senza operazioni intermedie di eccessiva complessità. Da qui l'opportunità di demandare alle applicazioni il controllo degli errori, lasciando ai DSE solo compiti marginali, eseguibili mediante *circuiti dedicati* molto veloci. Questi problemi rientrano nel vasto campo di problemi di **controllo di congestione del flusso** di una rete di telecomunicazioni.

Controllare la velocità del trasmittente rispetto al destinatario

RETI DI SISTEMI (INTERNETWORK)

Nel mondo esistono molte reti, con hardware e software diversi. La gente che si collega a una rete spesso vuole comunicare con persone collegate a una rete differente. La soddisfazione di questo desiderio obbliga all'interconnessione di reti diverse (e spesso incompatibili tra loro), a volte tramite macchine chiamate **gateway** che stabiliscono la connessione e offrono i servizi di conversione necessari, in termini di hardware e di software. Un insieme di reti interconnesse si chiama **internetwork** o **internet**.

Una forma comune di internet è rappresentata da un gruppo di LAN collegate da una WAN. Spesso si fa confusione tra subnet, reti e internetwork. Subnet è un termine particolarmente appropriato al contesto delle Wide Area Network, dove si riferisce all'insieme di router e linee di comunicazione possedute dall'operatore di rete. Per analogia, il sistema telefonico è composto da

centrali di commutazione connesse una all'altra da linee ad alta velocità, e collegate alle abitazioni e uffici da linee a bassa velocità. Linee e apparati, posseduti e gestiti dalla società telefonica, formano le subnet della rete telefonica. I telefoni (che in questa analogia sono gli host) non fanno parte delle subnet. La combinazione delle subnet e dei rispettivi host è una rete. Nel caso di una LAN, il cavo e gli host formano la rete; non c'è una vera e propria subnet.

Un internetwork viene creato quando si collegano tra loro reti distinte. Nella nostra ottica, collegando una LAN con una WAN o due LAN tra di loro si ottiene un internetwork, ma nell'industria del settore c'è poca concordanza sulla terminologia. Una regola di massima è che se organizzazioni differenti hanno pagato la costruzione di parti diverse della rete, e ciascuna gestisce la propria parte, ci troviamo di fronte a un internetwork e non a una singola rete. Inoltre, se la tecnologia sottostante cambia nelle diverse parti (per esempio in alcune è broadcast e in altre punto-punto), probabilmente abbiamo due reti.

Ricapitolando bisogna evitare la confusione sui seguenti termini:

- **sottorete (subnet)**: nel contesto di una WAN è l'insieme dei DSE e delle linee di trasmissione;
- **rete (network)**: è l'insieme costituito da una subnet e da tutti gli host collegati;
- **internetwork**: è una collezione di più network, anche non omogenee, collegate per mezzo di gateway.
- **internet** (con la *i* minuscola) è sinonimo di internetwork, cioè la interconnessione di più reti generiche;
- **Internet** (con la *I* maiuscola) per riferirci alla specifica internetwork, basata su protocollo TCP/IP, che ormai tutti conoscono.

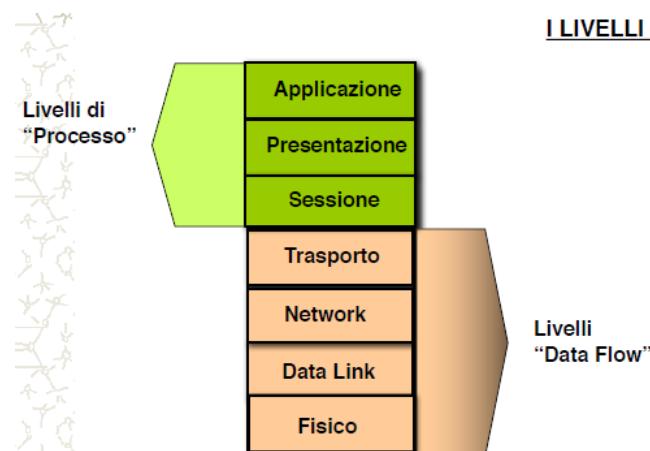
IL MODELLO ISO-OSI

Il modello OSI si fonda su una proposta sviluppata dall'*International Standards Organization* (ISO) come primo passo verso la standardizzazione internazionale dei protocolli impiegati nei diversi strati. Si chiama modello di riferimento ISO OSI (*Open System Interconnection*) perché riguarda la connessione di sistemi aperti, cioè sistemi che sono “aperti” verso la comunicazione con altri. Il modello OSI ha sette strati. I principi che sono stati applicati per arrivare ai sette strati si possono brevemente riassumere come segue:

1. si deve creare uno strato quando è richiesta un'astrazione diversa;
2. ogni strato deve svolgere una funzione ben definita;
3. la funzione di ogni strato va scelta con uno sguardo rivolto alla definizione di protocolli internazionali;
4. i confini degli strati vanno scelti per minimizzare il flusso d'informazioni attraverso le interfacce
5. il numero di strati deve bastare per evitare la necessità di radunare funzioni distinte nello stesso strato, ma essere abbastanza piccolo da rendere l'architettura attuabile.

Osservare che il modello OSI in sé non è un'architettura di rete, perché non specifica quali sono esattamente i servizi e i protocolli da usare in ciascuno strato; si limita infatti a definire ciò che ogni strato deve compiere. Tuttavia, ISO ha prodotto anche standard per ciascuno strato, benché non facciano parte del modello di riferimento: ognuno è stato pubblicato come standard internazionale distinto. Per ogni livello troviamo diversi standard. Il flusso di informazioni fra due livelli deve essere il più limitato possibile. Tutti i livelli sono astrazioni alla fine, l'unico vero mezzo alla fine è

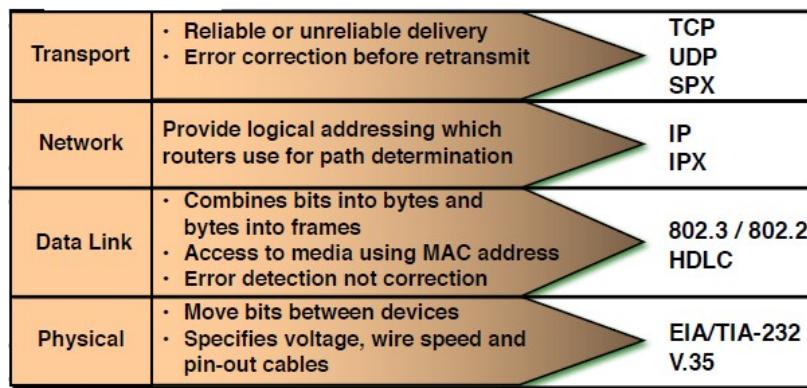
I LIVELLI OSI il livello fisico.



Di seguito sono elencati una minima parte dei livelli:

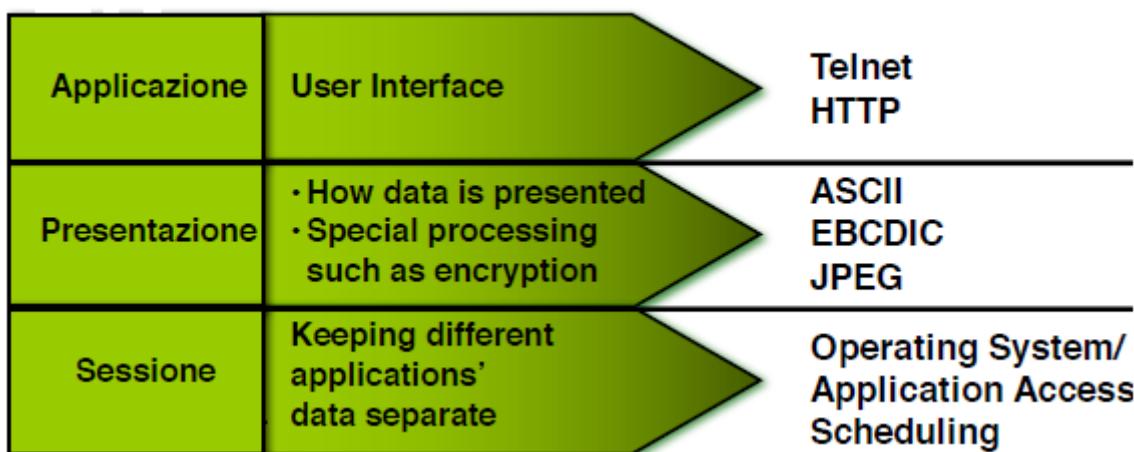
- **Strato fisico:** si occupa della trasmissione di bit grezzi sul canale di comunicazione. I requisiti di progetto devono assicurare che ogni bit trasmesso con valore 1 sia ricevuto ancora con valore 1, e non con valore 0. Problemi tipici riguardano quanti Volt bisogna usare per rappresentare un 1 e quanti per uno 0, quanti nanosecondi deve durare un bit, se la trasmissione può avvenire simultaneamente in entrambe le direzioni, come si stabilisce la connessione iniziale e come viene abbattuta quando entrambe le parti hanno terminato, quanti contatti deve avere il connettore di rete e che funzione va assegnata a ciascuno. Le specifiche riguardano per lo più interfacce meccaniche o elettriche e temporizzazioni, oltre che il mezzo di trasmissione che si trova sotto allo strato fisico.
- **Strato data link:** il compito principale consiste nel cercare di rilevare, per quanto possibile, gli errori di trasmissione così da evitare di trasmettere questi errori riconosciuti al livello superiore. L'obiettivo è raggiunto forzando il trasmettitore a suddividere i dati d'ingresso in data frame che vengono trasmessi sequenzialmente. Se il servizio è affidabile, il ricevitore conferma la corretta ricezione di ciascun frame rimandando indietro un **acknowledgment frame**. Un altro problema che nasce nello strato data link (e nella maggior parte degli strati superiori) riguarda il modo per evitare che un trasmettitore veloce saturi le possibilità di un ricevitore lento. Le reti broadcast hanno un problema in più nello strato data link: come controllare l'accesso al canale condiviso. Di questo problema si occupa uno speciale sottoinsieme dello strato data link, chiamato *medium access control (MAC)*.
- **Strato network:** controlla il funzionamento della subnet. Un problema chiave riguarda la modalità con cui i pacchetti sono inoltrati dalla sorgente alla destinazione. L'inoltro si può basare su tabelle statiche che sono "cablate" dentro la rete e raramente modificate. Potrebbe essere altamente dinamico, determinato per ogni pacchetto in modo da riflettere lo stato corrente del carico della rete. Quando nella subnet sono presenti contemporaneamente troppi pacchetti, vanno a interferire l'un l'altro formando colli di bottiglia. Anche il controllo di queste congestioni spetta allo strato network. Quando un pacchetto deve viaggiare da una rete all'altra per arrivare a destinazione possono nascere molti problemi. L'indirizzamento usato dalla seconda rete potrebbe essere diverso da quello della prima, la seconda rete potrebbe rifiutare il pacchetto perché troppo grosso, i protocolli potrebbero essere diversi, e così via. E compito dello strato network risolvere questi problemi per consentire la comunicazione tra reti eterogenee.
- **Strato trasporto:** la sua funzione essenziale è quella di accettare dati dallo strato superiore, dividerli in unità più piccole quando necessario, passarle allo strato network e assicurarsi che tutti i pezzi arrivino correttamente all'altra estremità. Lo strato trasporto stabilisce inoltre che tipo di servizio offrire allo strato sessione e, in definitiva, agli utenti della rete. Il tipo di connessione trasporto più comune è un canale punto-punto privo di errori che consegna messaggi o byte nello stesso ordine usato per la trasmissione. Lo strato trasporto copre tutto il percorso da sorgente a destinazione; in altri termini, un programma sul computer sorgente instaura una conversazione con un programma corrispondente sul computer destinatario, utilizzando intestazioni dei messaggi e messaggi di controllo. Negli strati inferiori i protocolli riguardano la comunicazione tra ciascun computer e i vicini immediati, e non tra i computer sorgente e destinatario, che possono essere separati da molti router.

I LIVELLI DI DATA FLOW



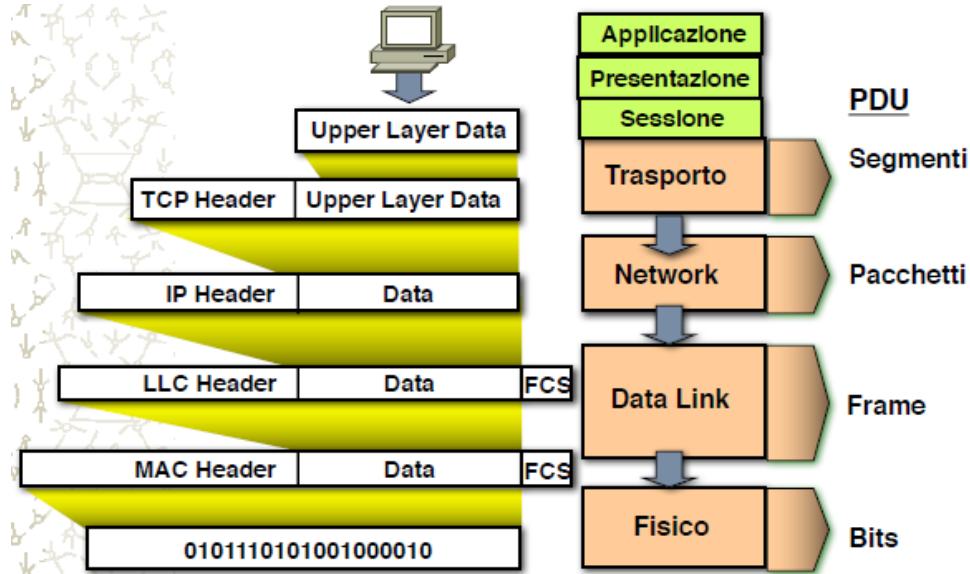
- **Strato sessione:** permette agli utenti su computer diversi di stabilire tra loro una **sessione**. Le sessioni offrono diversi servizi, tra cui: **controllo del dialogo** (tenere traccia di quando è il turno di trasmettere e quando di ricevere), **gestione dei token** (evitare che le **41 due parti tentino la stessa operazione critica al medesimo istante**) e **sincronizzazione** (supervisionare una lunga trasmissione per consentire la sua ripresa dal punto in cui si è interrotta a causa di un crash).
- **Strato presentazione:** si occupa della sintassi e della semantica dell'informazione trasmessa. Per consentire la comunicazione tra computer con differenti rappresentazioni dei dati, le strutture dati da scambiare si possono definire in modo astratto, assieme a una codifica standard usata “sul filo”. Lo strato presentazione gestisce queste strutture dati astratte e consente lo scambio e la definizione di strutture dati di livello superiore (per esempio transazioni bancarie).
- **Strato applicazione:** comprende una varietà di protocolli comunemente richiesti dagli utenti. Un protocollo applicativo largamente usato è HTTP (*HyperText Transfer Protocol*), che è la base del World Wide Web. Quando un browser richiede una pagina Web, invia al server il nome della pagina desiderata usando HTTP, quindi il server risponde inviandola. Altri protocolli applicativi si usano per trasferimento file, posta elettronica e news.

I LIVELLI DI PROCESSO

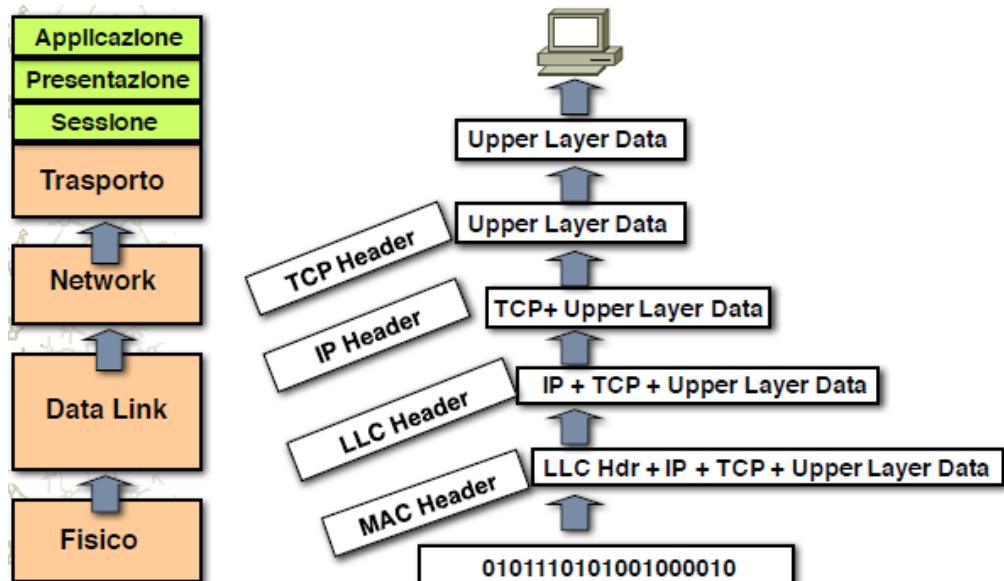


Ogni protocollo incapsula i dati ricevuti dal livello superiore e li unisce in pacchetti da inviare a quello successivo, e così via fino ad arrivare al livello fisico che invia tutti questi dati ad un altro terminale che si occuperà di deincapsulamento. Di seguito uno schema.

Incapsulamento



Deincapsulamento

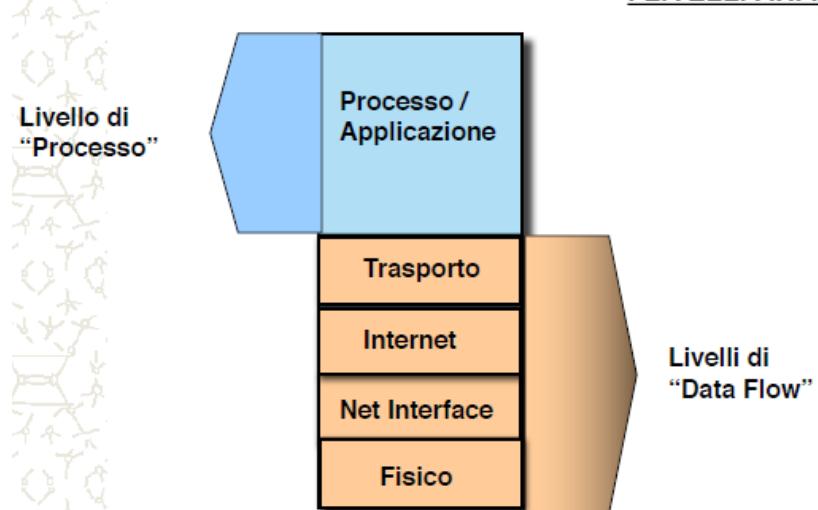


L'architettura ISO-OSI non è quella attualmente utilizzata per internet, si utilizza infatti l'architettura ARPANET, basata sul protocollo **TCP/IP** dal nome dei due suoi principali protocolli, questa architettura si basa sul unire i 3 strati processi in un unico livello creando lo strato *Processo/Applicazione*, quindi alla fine abbiamo 5 livelli:

- **Strato fisico:** stesse funzioni del modello ISO-OSI.
- **Strato Net Interface:** si trova sotto lo strato internet c'è un grande vuoto. Il modello di riferimento TCP/IP non dice molto su quanto accade in questo territorio, limitandosi a segnalare che l'host deve collegarsi alla rete usando qualche protocollo che gli permetta di spedire pacchetti IP. Questo protocollo non è definito e varia da host a host e da rete a rete.

- **Strato internet:** è l'architrave su cui poggia l'intera architettura. Il suo scopo è quello di consentire agli host di mandare pacchetti in qualsiasi rete, e farli viaggiare in modo indipendente l'uno dall'altro fino alla destinazione (che magari è su una rete diversa). Potrebbero persino arrivare con un ordine diverso da quello con cui sono stati spediti, e in questo caso (se è richiesta una consegna in sequenza) è compito degli strati superiori riordinarli. Il termine “internet” viene usato in senso generico in questo contesto, anche se questo strato è presente nella Internet. Lo strato internet definisce un formato ufficiale per i pacchetti e un protocollo chiamato **IP** (*Internet Protocol*). Lo scopo dello strato internet è quello di consegnare i pacchetti IP alla destinazione corretta. L'instradamento dei pacchetti è chiaramente il problema più importante, assieme alla necessità di garantire l'assenza di congestioni. Per questi motivi è ragionevole dire che lo strato TCP/IP internet ha funzionalità simili allo strato network OSI.
- **Strato trasporto:** È progettato per consentire la comunicazione tra entità pari degli host sorgente e destinazione, come nello strato trasporto OSI. In questo strato sono stati definiti due protocolli di trasporto end-to-end: il primo, TCP (*Transmission Control Protocol*), è un protocollo affidabile orientato alla connessione che permette a un flusso di byte emessi da un computer di raggiungere senza errori qualsiasi altro computer sulla Internet. Suddivide il flusso di byte entrante in messaggi discreti e passa ciascun frammento allo strato internet. Nella destinazione, il processo TCP ricevente ricompone il messaggio ricevuto per formare il flusso di uscita. TCP gestisce anche il controllo di flusso, per garantire che una sorgente veloce non possa sommergere un ricevitore lento con una quantità di messaggi superiore a quelli che sa gestire. Il secondo protocollo di questo strato, UDP (*User Datagram Protocol*), è un protocollo inaffidabile senza connessione per le applicazioni che non vogliono la garanzia di ordinamento e il controllo di flusso di TCP, ma preferiscono gestire queste funzioni in modo autonomo. È inoltre largamente impiegato per le query client-server singole di tipo domanda-risposta, e dalle applicazioni dove la consegna rapida è più importante dell'accuratezza, come la trasmissione di voce e filmati.
- **Strato Processi/Applicazione:** Il protocollo di emulazione terminale consente all'utente di un computer di eseguire un login su un computer remoto per lavorare su di esso. Il protocollo di trasferimento dei file è un mezzo efficiente per spostare dati da un computer a un altro: in origine la posta elettronica era solo una specie di trasferimento file, prima che venisse sviluppato un protocollo specializzato (SMTP). Nel corso degli anni a questi si sono aggiunti molti altri protocolli: *Domain Name System* (DNS) che fa corrispondere i nomi degli host ai loro indirizzi di rete; NNTP, il protocollo per spostare sulla rete i messaggi dei gruppi di discussione USENET; HTTP, il protocollo per prelevare pagine sul World Wide Web, e altri ancora. Se si vuole sicurezza si può usare il protocollo HTTPS che sfrutta la crittografia secondo due standard SSL e DLS.

I LIVELLI ARPANET



Differenza fra OSI e TCP/IP

I modelli di riferimento OSI e TCP/IP hanno molto in comune. Sono entrambi basati sul concetto di pila (*stack*) di protocolli indipendenti, e la funzione degli strati è grosso modo simile.

Nel modello OSI sono presenti tre concetti essenziali:

- **servizi:** Ogni strato offre un servizio a quello che lo sovrasta; la definizione del *servizio* descrive ciò che fa lo strato, e non le modalità d'accesso da parte delle entità sovrastanti o quelle di funzionamento. Definisce la semantica dello strato.
- **Interfacce:** spiega le modalità di accesso ai processi sovrastanti. Specifica quali sono i parametri e i risultati, ma non dice nulla delle modalità di funzionamento interno.
- **Protocolli:** sono l'essenza fondamentale di uno strato, lo strato può usare i protocolli che preferisce, se portano ai risultati desiderati (cioè svolgono i servizi offerti), e li può cambiare senza disturbare il software degli strati superiori

Il motivo che ha portato all'affermazione del modello TCP/IP è che il suo stack è enormemente più semplice di quello dell'OSI, in più quante nacque OSI il TCP/IP era già presente nel mondo accademico.

In entrambi i modelli sono presenti delle imperfezioni, quelle del modello OSI sono le seguenti:

- **Poca tempestività:** il modello e i suoi standard furono creati ormai quando la sua controparte TCP/IP era ormai largamente utilizzata.
- **Tecnologia scandente:** La scelta di sette strati fu più politica che tecnica: due strati (sessione e presentazione) sono quasi vuoti, mentre altri due (data link e network) sono sovraccarichi. Il modello OSI con le corrispondenti definizioni di servizi e protocolli ha una complessità straordinaria: se vengono messe una sull'altra, le copie stampate degli standard formano una pila di carta alta quasi un metro; per giunta sono difficili da implementare e inefficienti. OSI non ha solo il problema di essere incomprensibile: alcune funzioni come l'indirizzamento, il controllo di flusso e quello di errore riappaiono più e più volte in ogni strato, quando per essere efficiente basta farlo una sola volta e nello strato più alto.
- **Implementazioni carenti:** vista l'enorme complessità del modello e dei protocolli, non fu una sorpresa che le implementazioni iniziali fossero enormi, scomode e lente. Tutti quelli che ci tentarono rimasero scottati. Non ci volle molto per creare l'associazione mentale tra "OSI" e "scarsa qualità". I prodotti migliorarono col tempo, ma la fama rimase.
- **Incapacità politica:** OSI, d'altro canto, era largamente ritenuto la creatura dei ministeri delle telecomunicazioni europei, della Comunità Europea, e più tardi del governo USA. L'impressione era in parte vera, ma evocò l'immagine di un gruppo di burocrati che cercavano di cacciare in gola ai poveri ricercatori e programmatore uno standard mediocre, ostacolando gli sforzi per ottenere qualcosa che funziona davvero.

Le imperfezioni del modello TCP/IP sono le seguenti:

- Innanzitutto, il modello non distingue in modo chiaro i concetti di servizio, interfaccia e protocollo. Un buon approccio all'ingegneria del software impone di tenere distinte le specifiche dall'implementazione, cosa che OSI segue alla lettera al contrario di TCP/IP. La conseguenza è che il modello TCP/IP serve a poco se bisogna progettare reti basate su tecnologie nuove.
- In secondo luogo, il modello TCP/IP è poco generale e inadatto per descrivere pile di protocolli diverse dal TCP/IP: per esempio, è assolutamente impossibile usare il modello TCP/IP per descrivere Bluetooth.
- Terzo, lo strato host-to-network non è un vero e proprio strato, inteso con il significato che ha nel contesto dei protocolli stratificati. È piuttosto un'interfaccia tra gli strati network e data link. La distinzione tra interfaccia e strato è cruciale, e non si dovrebbe trascurare.

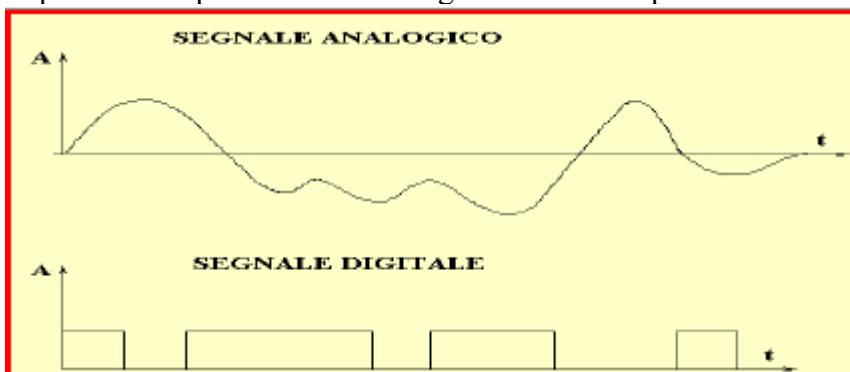
- Il modello TCP/IP in generale non possiede lo strato fisico, ma il modello che studiamo noi è un imbrido che lo implementa.
- Infine, anche se i protocolli IP e TCP furono pensati con cura e implementati bene, molti altri protocolli risolvono problemi ad-hoc, e di solito erano prodotti da dottorandi che facevano tentativi finché non si stancavano. A questo punto le implementazioni del protocollo erano distribuite gratuitamente, diventando largamente utilizzate e molto radicate, quindi difficili da sostituire. Per concludere, nonostante i suoi problemi il *modello OSI* (eccetto gli strati sessione e presentazione) si è dimostrato eccezionalmente utile per discutere le reti di computer; al contrario i *protocolli OSI* non sono diventati popolari. Per TCP/IP è vero l'opposto: il *modello* praticamente non esiste, ma i *protocolli* sono molto usati.

IL LIVELLO FISICO

Il livello fisico si occupa di gestire la trasmissione sul livello fisico, cioè far viaggiare i segnali. I segnali sono variazioni di grandezze fisiche che trasportano informazioni, e che variano nel tempo(modulare), *possono essere di vario tipo: acustico, elettrico, luminoso, elettromagnetico, ecc.*

I segnali elettrici trasmessi sono essenzialmente di due tipi:

- ***ANALOGICI***: Sono analogici quei segnali che, al variare del tempo, possono assumere tutti i valori compresi fra i valori massimo e minimo consentiti dal canale di comunicazione.
- ***DIGITALI***: Con il termine digitale, o numerico, si intende invece un segnale che può assumere solo due valori, o comunque soltanto un numero discreto di valori, come, ad esempio avviene per i dati che sono generati dai computer.



Per ottenere questi valori, lo si divide in slot temporali e infine vediamo il loro valore (campionare il segnale), cioè leggere il segnale in specifici intervalli di tempo. Più frequentemente campioniamo un segnale più possiamo trasmettere velocemente, questo però ha un contro ed è che il segnale viene ricevuto ed interpretato da un altro dispositivo che usa la sua stessa frequenza, in più un segnale è soggetto a fenomeni di attenuazione(col tempo si riduce) e può essere perturbato dal tipo di mezzo trasmittivo. Un mezzo trasmittivo infatti trasforma un segnale da analogico a digitale.

Serie di Fourier

All'inizio del XIX secolo Jean-Baptiste Fourier ha dimostrato che: una funzione periodica $y(t)$ è sviluppabile in una serie costituita da un termine costante A_0 e da una somma di infinite sinusoidi:

$$y(t) = A_0 + \sum_{n=1}^{\infty} A_n \cos(n\omega_0 t) + \sum_{n=1}^{\infty} B_n \sin(n\omega_0 t)$$

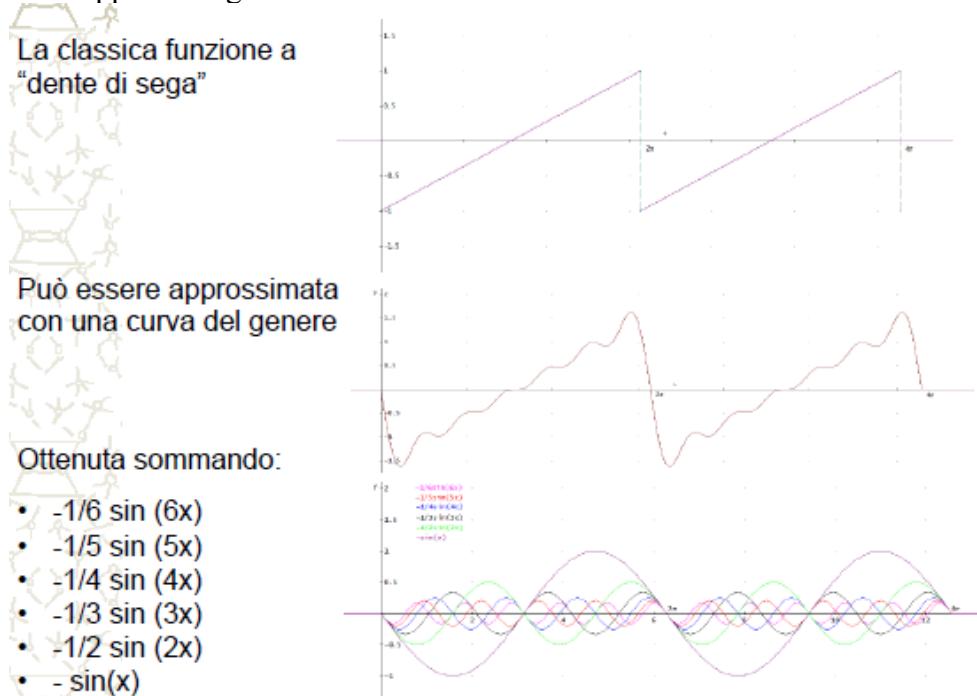
le cui frequenze f_n sono multiple intere della frequenza fondamentale f_0 della funzione data:

$$f_0 = \frac{1}{T} \quad f_n = n f_0$$

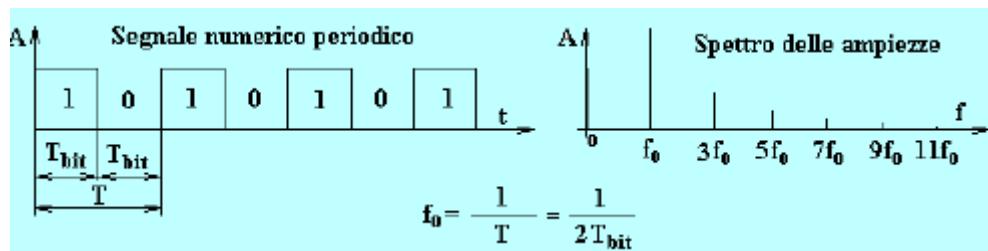
e di ampiezze A_n e B_n (di sin e cos della n-esima armonica) calcolabili secondo le formule:

$$A_0 = \frac{1}{T} \int_0^T y(t) dt \quad A_n = \frac{2}{T} \int_0^T y(t) \cos(n\omega_0 t) dt \quad B_n = \frac{2}{T} \int_0^T y(t) \sin(n\omega_0 t) dt$$

Il suo sviluppo è il seguente:

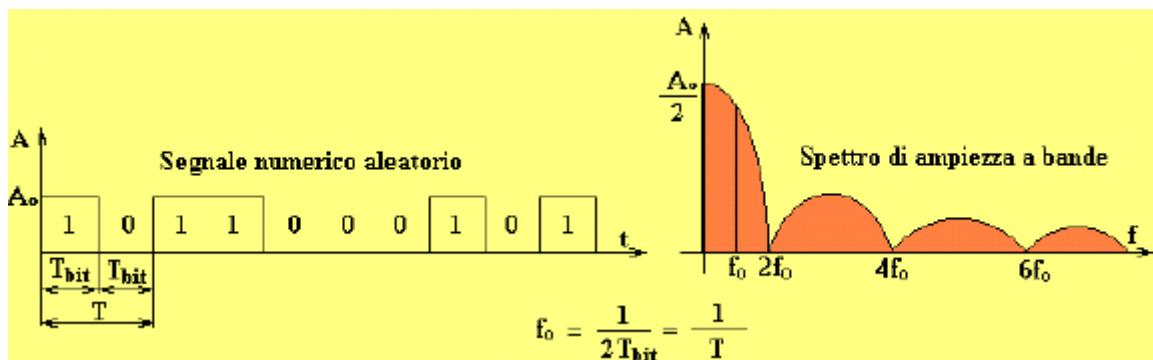


Un segnale numerico di periodo T può essere sviluppato in serie di Fourier in una somma di infinite sinusoidi di ampiezza variabile.

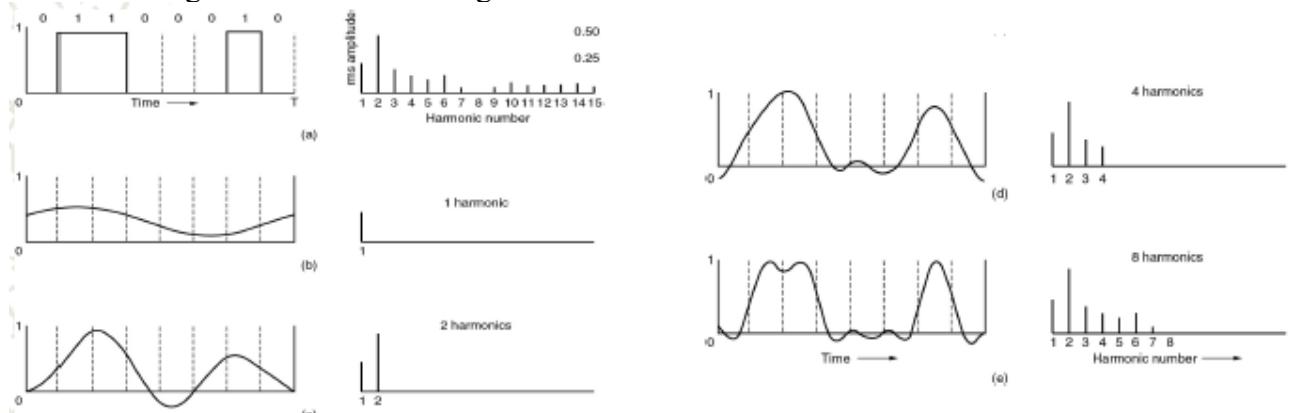


In questo caso la frequenza f_0 è uguale a: $f_0 = \frac{1}{2 \cdot T_{bit}}$

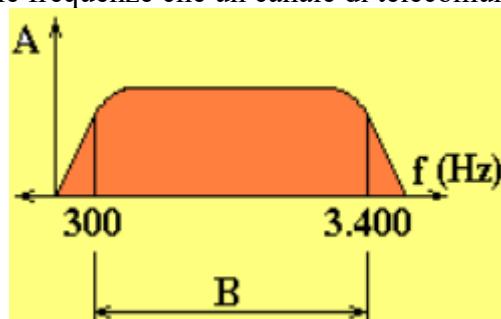
Con questi calcoli otteniamo una nuova visione del segnale, vedendolo nel dominio della frequenza, non facendo vedere più quindi come cambia nel tempo ma come varia nella frequenza (spettro), le ampiezze ora saranno rapportate alla frequenza. Se il mezzo trasmittivo mi garantisce il passaggio di tutte le frequenze, possiamo essere certo che il segnale venga ricostruito. I quadrati delle ampiezze sono proporzionali all'energia trasmessa alla frequenza corrispondente. Nel mezzo trasmittivo parte dell'energia si perde. Se tutte le componenti fossero attenuate in modo uniforme il segnale risulterebbe ridotto in ampiezza ma avrebbe la stessa forma. Ciò non avviene e il segnale viene distorto. Lo studio dello sviluppo in serie e dell'integrale di **FOURIER**, però, ci dice che lo spettro di un segnale **ALEATORIO**, costituito da impulsi discreti rettangolari, comprende la componente continua e larghezza di banda teoricamente infinita.



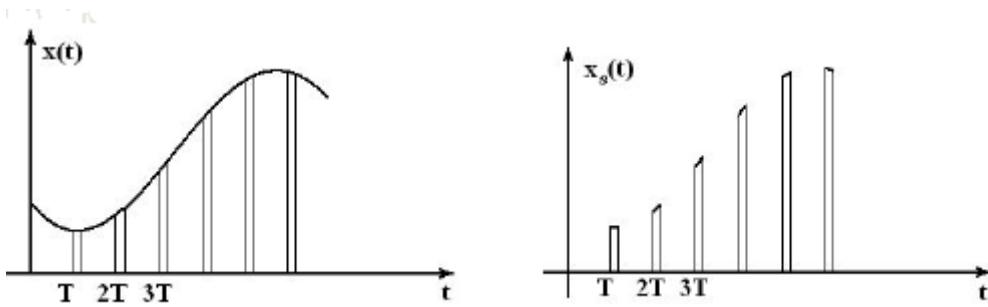
Quindi un segnale numerico aleatorio si sviluppa secondo uno **spettro** a bande. Le componenti di Fourier del segnale o armoniche vengono attenuate in maniera differente dal mezzo trasmittivo:



I canali di telecomunicazioni usati per trasmettere dati sono basati su mezzi trasmittivi quali: **il rame, la fibra ottica, l'etere**. Ogni canale trasmittivo consente di norma il passaggio solo di alcune componenti in frequenza del segnale ed escludendone altre, questo perchè si comporta da filtro, e imposta un range di frequenza in cui il segnale riesce a passare. E' definita pertanto larghezza di banda **B** l'insieme delle frequenze che un canale di telecomunicazioni fa passare.



Il problema da affrontare quindi è: con **quale frequenza** si deve campionare il segnale per poterlo **ricostruire** a partire dal segnale campionato?



Nel 1924 H. Nyquist dimostrò che un segnale a larghezza di banda B può essere ricostruito perfettamente campionando lo stesso al doppio della larghezza di banda, quindi a partire da $2B$ campioni del segnale stesso. IL teorema del campionamento (o teorema di Nyquist) afferma che: ***dato un segnale $x(t)$ a banda limitata B , si puo' ricostruire completamente il segnale a partire da un campionamento del segnale se la frequenza di campionamento e' $F \geq 2B$.***

In generale la frequenza di campionamento dovrà essere almeno leggermente superiore a $2B$, per disporre di un intervallo utile (banda di guardia) al fine di prevenire che effetti di non idealità dei filtri taglino parti utili del segnale.

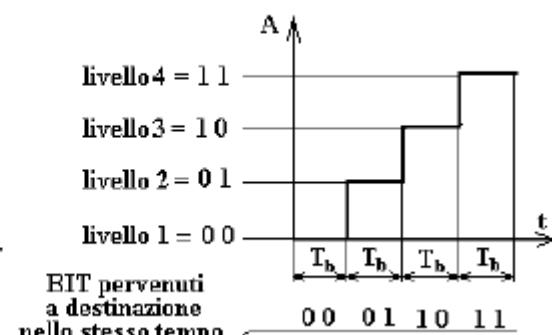
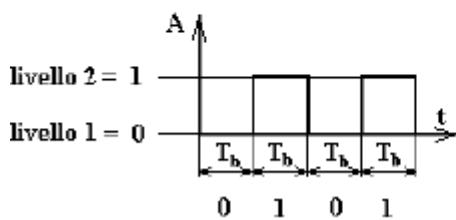
Con l'ausilio di questa relazione riuscì a stabilire che considerando di usare un numero V di livelli trasmissivi equiprobabili, dato che la quantità di informazione associata è esprimibile come $Q = \log_2 V$, allora la massima quantità di informazione trasmessa in un canale non rumoroso, dato un segnale costituito da V livelli, è di $2BQ$ cioè:

$$I[\text{bit/s}] = 2B \log_2 V$$

Il teorema del campionamento è sostanzialmente la stessa cosa della legge sulla massima capacità di un canale privo di rumore: se il livello del segnale trasmesso rappresenta una sequenza di simboli, la massima capacità di trasferimento la otteniamo quando ogni campione identifica un simbolo ne segue che al massimo siamo in grado di identificare $2B$ simboli. Quindi usando un codice in cui si trasmettono quattro livelli diversi di tensione invece di due, per ogni livello in arrivo l'informazione sarà di due bit e non di uno solo e poiché il tempo di arrivo di un livello di tensione è sempre lo stesso, perché determinato dallo stesso criterio di **NYQUIST**, otterremo che, mentre la velocità di modulazione rimane la stessa, la velocità di trasmissione invece raddoppia.

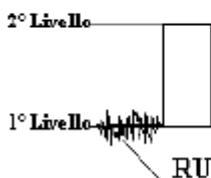
CODICE A QUATTRO LIVELLI

CODICE A DUE LIVELLI

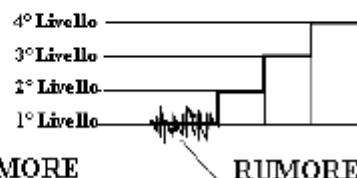


Aumentando il numero dei livelli di tensione, è possibile aumentare la quantità di informazione che va a destinazione nello stesso tempo. Ma aumentare il numero dei livelli, a parità di tensione massima, comporta che il singolo livello diventa sempre più piccolo, finché in ricezione non sia più distinguibile dal rumore, sempre presente, come indicato nel disegno seguente in cui si fa un esempio di codifica a 2, 4 e 8 livelli.

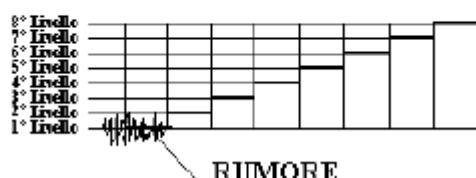
CODIFICA A DUE LIVELLI



CODIFICA A QUATTRO LIVELLI



CODIFICA A OTTO LIVELLI



Esiste comunque un limite massimo all'aumento dei livelli definito, analiticamente da una formula determinata da **C. SHANNON**. Quindi possiamo dire che conoscendo tutti questi dati possiamo trasmettere ad una frequenza in cui non possiamo perdere informazione, anzi possiamo quindi usare il mezzo trasmittivo al meglio che possiamo. Infatti più aumenta il livello di trasmissione più sale la quantità di informazione, ma il conto è che l'hardware diventa sempre più sofisticato, facendo aumentare anche il rumore.

IL RUMORE

Il rumore va a disturbare il segnale i modo casuale, infatti è una forma di energia indesiderata che si somma al segnale utile degradandone il contenuto informativo, ed impedendo così di rilevare, in ricezione, tutto l'insieme delle informazioni trasmesse. Il rumore e l'attenuazione sono proprietà del mezzo trasmittivo.

Esistono vari tipi di rumore che interessano il campo dell'Elettronica e delle Telecomunicazioni e che si schematizzano come segue:

- **Rumore bianco** - Forma di rumore il cui spettro comprende energia a tutte le frequenze dello spettro elettromagnetico ed equamente distribuita.
- **Rumore di intermodulazione** - Rumore prodotto dalla non linearità dei dispositivi elettronici e che consiste nella presenza, nel segnale in uscita dal dispositivo, di armoniche indesiderate non presenti nel segnale in ingresso. Il segnale viene quindi alterato in maniera imprevedibile.
- **Rumore di modo comune** o di modo normale - Rumore presente in ingresso ad uno strumento di misura insieme al segnale da misurare e non separabile da questo.
- **Rumore di quantizzazione** - Perdita di informazione che ha luogo durante la trasformazione di un segnale analogico in digitale, ad esempio nel **P.C.M.**
- **Rumore termico** - Rumore dovuto all'agitazione termica degli elettroni presenti in una resistenza. È funzione della temperatura ma è anche un rumore bianco.

Alla luce di questo nel C. Shannon estese il lavoro di Nyquist a canali soggetti a rumore casuale (termico). Se indichiamo con S la potenza del segnale e con N la potenza del rumore, la massima informazione trasmessa è:

$$I[\text{bit/s}] = B \log_2 \left(1 + \frac{S}{N} \right) \quad \frac{S}{N} = \text{rapporto fra potenza del segnale e del rumore.}$$

Quindi meno è potente il rumore e più è potente il segnale migliore procedono le cose, viceversa peggiorano sempre di più. In questa formula, C è detta **CAPACITÀ DI CANALE**, si misura in **BIT AL SECONDO**, ed indica la massima velocità teorica di trasmissione dei bit oltre la quale in ricezione essi vengono confusi con il rumore; quindi, in un canale telefonico banda di circa 3 KHz, il rapporto S/N è di circa 30 dB (cioè $10 \log_{10} 1000 = 30$ dB), allora la quantità massima di bit trasmessi è di circa 33.000 bps.

Secondo la relazione vista, sembrerebbe possibile aumentare il **tasso** di trasferimento dati aumentando il **livello** del segnale. Questo è vero, ma come già osservato l'aumento del livello del segnale comporta l'aumento di effetti come la non linearità che vanno ad **accrescere** il tasso di errore in ricezione, quindi effettivamente la limitazione di banda costituisce un **limite** alla velocità di trasferimento dei bit che converrebbe non superare mai.

TRASMISSIONE DEI SEGNALI

La trasmissione dei segnali è detta **analogica** se il segnale viene trasmesso senza curarsi del suo significato, cioè facciamo variare nel mezzo trasmittivo una grandezza analogica in base all'informazione che vogliamo inviare, e con questo rappresentiamo in un dato momento un dato digitale (modulo un segnale analogico).

La trasmissione **digitale** tiene conto del contenuto dei dati se si deve intervenire per amplificare il segnale, non viene semplicemente amplificato, ma viene interpretato, si estraе il contenuto informativo e si rigenera il segnale tramite apparati detti ripetitori. Trasmettere in digitale significa prendere un segnale numerico e trasmetterlo in analogico, il segnale sarà quindi trasformato e conserverà soltanto qualche tratto. Un esempio di dispositivo che operava con questa tecnologia è il *modem 52k*.

I vantaggi della trasmissione digitale:

- immunità maggiore alla alterazione dei dati verso lunghe distanze
- omogeneizzazione della trasmissione per diverse tipologie di dato
- sicurezza e riservatezza

Gli svantaggi della trasmissione digitale

- costi superiori
- maggiore complessità dell'elettronica
- richiede rinnovo di infrastrutture già esistenti

Una volta generato il segnale da trasmettere, questo può essere immesso direttamente sul canale; in questo caso si parla di trasmissione in **banda base**: il segnale che trasporta le informazioni ed il segnale sulla linea sono identici. Vi sono diverse circostanze che rendono opportuno trasmettere il segnale in modo che occupi una banda differente di frequenze; questo tipo di trasmissione si realizza tramite un processo di modulazione.

CODIFICA DEI DATI NUMERICI

La rappresentazione di dati numerici con segnali numerici è normalmente fatta tramite sequenze di impulsi discreti di tensione di una certa durata temporale. Il dato binario è **codificato** in modo da far corrispondere al valore di un bit un determinato livello del segnale. La codifica serve a capire come un impulso digitale viene modificato in un certo livello corrispondente ad un bit. Il trasmettitore e il ricevitore si devono sincronizzare sulla codifica del segnale. Infatti il ricevitore deve sapere quando inizia e finisce il bit, leggere il valore del segnale al momento giusto, determinare il valore del bit in base alla codifica utilizzata. La migliore valutazione si ottiene campionando il segnale al tempo corrispondente a metà bit.

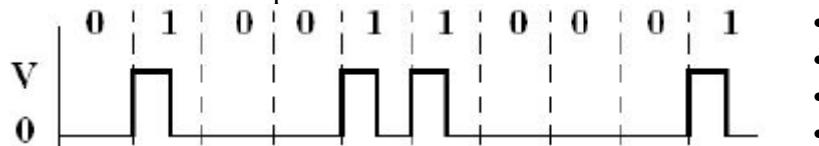
Sono possibili diverse scelte di codifica, con caratteristiche differenti che possono migliorare le prestazioni della trasmissione, le caratteristiche determinanti sono:

- **Spettro del segnale:**
 - componenti ad alta frequenza richiedono una banda maggiore
 - l'assenza di componente continua è preferibile, perché la sua assenza migliora il sincronismo, perché le variazioni del segnale aiutano a capire quale si sta trasmettendo. Su un mezzo trasmittivo può essere mandato solo un segnale, per non vere problemi conviene mettersi a metà della capacità della frequenza.
 - spettro concentrato nel centro della banda
- **Sincronizzazione temporale:** il ricevitore deve essere sincronizzato con il trasmettitore per identificare i bit; alcune codifiche facilitano questa funzione.
- **Rilevazione di errore:** funzione caratteristica dei livelli superiori, ma può essere utile anche a livello fisico:
 - Solidità del segnale rispetto ad interferenza o rumore.
 - Costo e complessità di realizzazione.

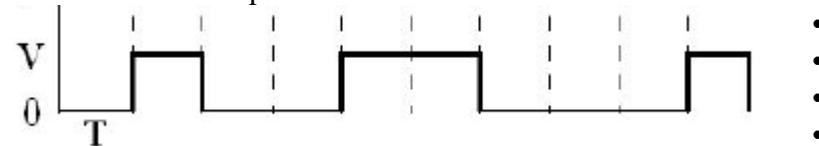
NOTA: l'interferenza è rumore, cioè energia causata da un effetto esterno, per esempio da fili che possono essere vicini tra loro si creano interferenze.

Esistono molti tipi di codifiche di seguito ne saranno elencate alcune:

- La **codifica unipolare RZ (Return to Zero)** prevede la trasmissione di un segnale di lunghezza T per ogni bit. Il segnale è nullo in corrispondenza del bit 0, mentre è un impulso di tensione di durata $T/2$ per il bit 1.



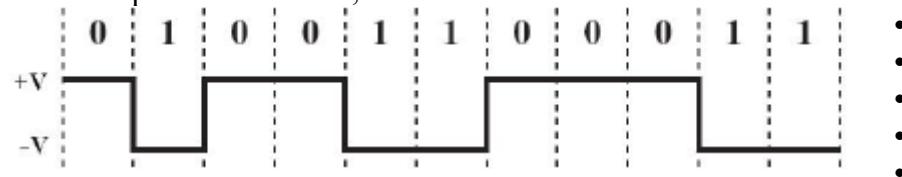
- La **codifica unipolare NRZ** (Non Return to Zero) differisce dalla RZ perché il livello di tensione per il bit 1 rimane alto per tutta la **durata del bit**.



- La codifica NRZ ha dei pregi e dei difetti. I pregi sono che è facile da progettare e realizzare, il suo utilizzo efficiente della larghezza di banda (la potenza è concentrata tra 0 ed $R/2$, dove R è la capacità trasmissiva in bit/s (transmission rate)). I difetti sono che esiste una componente continua, infatti lunghe sequenze di bit di uguale valore producono un segnale continuo senza transizioni: il ricevitore può perdere la sincronia.

La differenza tra RZ e NRZ è che nella RZ quando si passa da 1 a 0 si passa ad una frequenza maggiore, mentre nella NRZ si passa ad una minore.

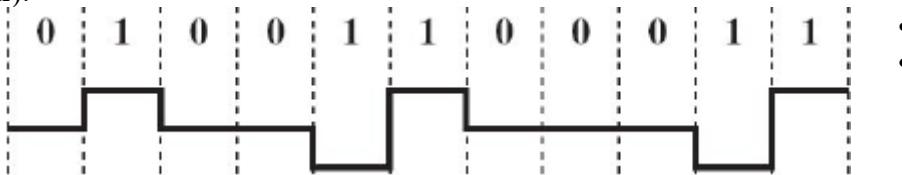
- La codifica **NRZL(Non Return to Zero Level)** è utilizzata per migliorare le precedenti caratteristiche e prevede un segnale a $+V$ per il bit 1, ed a $-V$ per il bit 0 questo riduce l'impatto della componente continua, ma non la annulla.



- La codifica **NRZI(Non Return to Zero Invert on ones)** il segnale cambia in occasione di un bit 1.



- Le codifiche a **multilivello binario** utilizzano tre livelli: lo zero indica il bit 0, mentre il bit 1 è identificato con segnali a $+V$ e a $-V$ alternati (**AMI bipolar: Alternate Mark Inversion**).



La codifica AMI ha i seguenti vantaggi rispetto alla NRZ: risolve il problema della sequenza di bit 1, che presentano sempre una transizione utilizzabile in ricezione per sincronizzare (ma resta il problema per sequenze di 0). La componente continua è di fatto azzerata, utilizza a parità di transmission rate una larghezza di banda inferiore, errori isolati possono essere evidenziati come violazione del codice infatti se abbiamo 2+V consecutivi c'è un errore.

Vi sono anche svantaggi: utilizza 3 livelli, quindi ogni simbolo potrebbe trasportare più informazione ($\log_2(3) = 1.58$) e a parità di bit rate richiede circa 3 dB in più rispetto alla NRZ. È utilizzata in diversi casi su linee punto-punto (ISDN).

- La codifica **pseudoternaria** è la stessa, con 1 e 0 invertiti.



- La codifica **Manchester** utilizza due livelli di tensione; il bit 1 e' rappresentato da un segnale -V per mezzo periodo, +V per il seguente mezzo periodo; il bit 0 e' rappresentato in modo opposto (+V per il primo mezzo periodo, -V per il restante mezzo periodo).



I vantaggi di questa codifica sono:

sincronizzazione: ogni bit ha una transizione in mezzo, che puo' essere utilizzata per la sincronizzazione dal ricevitore, una totale assenza di componente continua e rivelazione di errore (in assenza della transizione prevista).

Ma ha anche degli svantaggi:

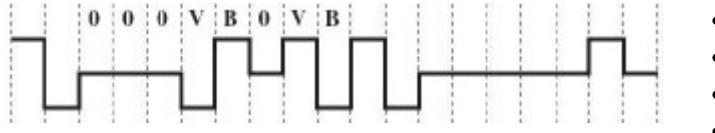
richiede un segnale a frequenza doppia rispetto al bit rate: 1 bit richiede 2 baud, quindi richiede una banda doppia.

L'utilizzo piu' diffuso della codifica Manchester e' negli standard 802.3 (ethernet) e 802.5 (token ring) sia su coassiale che su doppino.

- La codifica **Manchester differenziale** utilizza lo stesso tipo di rappresentazione, ma rappresenta il bit 1 come variazione rispetto alla codifica del bit precedente.



- Codifica **B8ZS(Bipolar with 8 Zeros Substitution)**: ogni sequenza di 8 zeri viene codificata come 000+-0-+ se l'ultimo impulso e' stato positivo o 000-+0+- se l'ultimo impulso e' stato negativo, in questo modo scompaiono lunghe sequenze di zeri, e la sequenza e' identificata da due violazioni del codice AMI. È utilizzata nel Nord America.



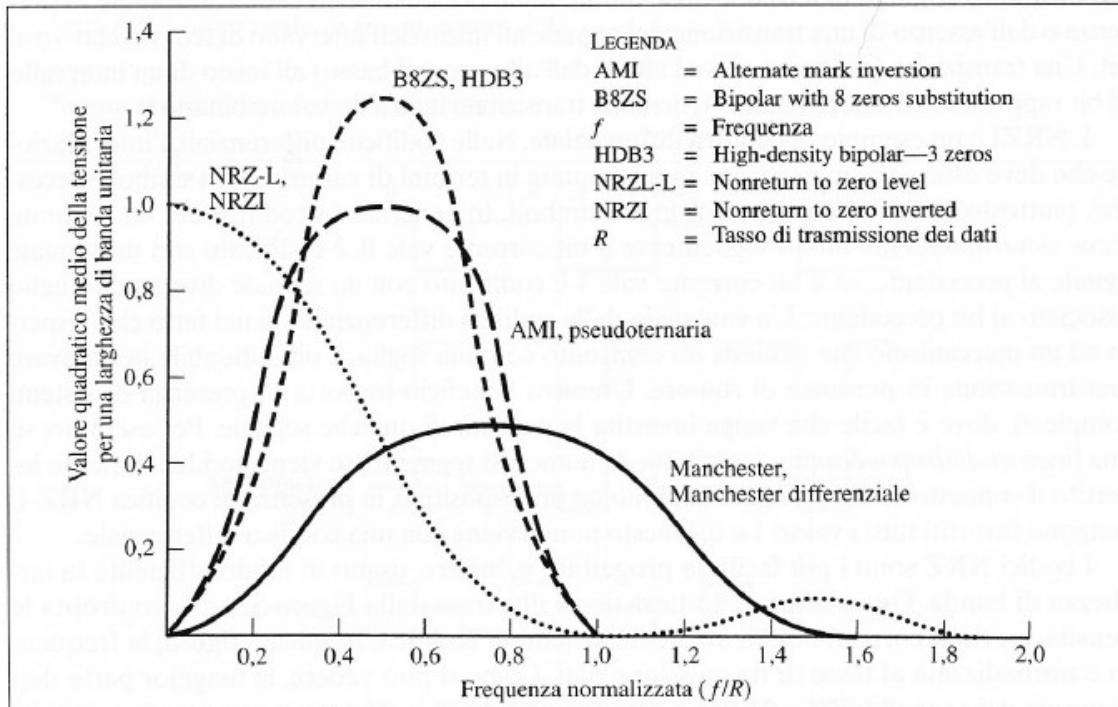
- Codifica **HDB3(High Density Bipolar 3 zeros)**: ogni sequenza di 4 zeri viene codificata come se la polarita' dell'ultimo impulso e' stata negativa: 000- se c'e' stato numero dispari di 1 dall'ultima sostituzione o +00+ se c'e' stato un numero pari di 1 dall'ultima sostituzione. Se la polarita' dell'ultimo impulso e' stata positiva: 000+ per un numero dispari di 1 dall'ultima sostituzione o -00- per un numero pari di 1 dall'ultima sostituzione, anche in questo caso scompaiono lunghe sequenze di zeri, e la sequenza e' identificata da violazioni opportune del codice AMI. È utilizzata in Europa e Giappone.



Le due codifiche hanno sempre componente continua nulla (le violazioni sono alternate). Hanno un efficiente utilizzo della banda, con la potenza concentrata a metà' della banda come con AMI, e' possibile riconoscere gli errori singoli. Generalmente utilizzate nella trasmissione dati ad elevata distanza.



Spettro delle codifiche numeriche in banda base



MODULAZIONE

La modulazione è un processo con il quale il segnale da trasmettere (segnale modulante) viene utilizzato per modificare nel tempo le caratteristiche di un segnale ausiliario sinusoidale (portante). Questa operazione ha la caratteristica di generare un segnale che ha una occupazione di banda dell'ordine di grandezza di quella del segnale modulante, centrata però intorno alla frequenza del segnale portante. Utilizzando una portante ad alta frequenza si può quindi spostare la banda necessaria alla trasmissione delle informazioni in un intervallo più opportuno per la trasmissione stessa. Quindi più aumenta il segnale modulante più aumenta la frequenza e quindi la banda.

NOTA:

Modulante: comanda l'occupazione di frequenza, è il segnale che dobbiamo trasmettere.

Modulato: comanda il posizionamento del segnale nel mezzo, lo fa variare in ragione di quello che devo trasmettere.

Spesso per la trasmissione sono preferibili determinati intervalli di frequenza:

ad esempio, la trasmissione via ponte radio (a vista) richiede una antenna; la dimensione della antenna deve essere dello stesso ordine di grandezza della lunghezza d'onda; per trasmissioni a 1 KHz $l = 300$ Km, per trasmissioni a 1GHz $l = 30$ cm, quindi per trasmettere i segnali radio si può sfruttare la riflessione multipla dalla ionosfera, che riflette bene frequenze di 5-30 Mhz.

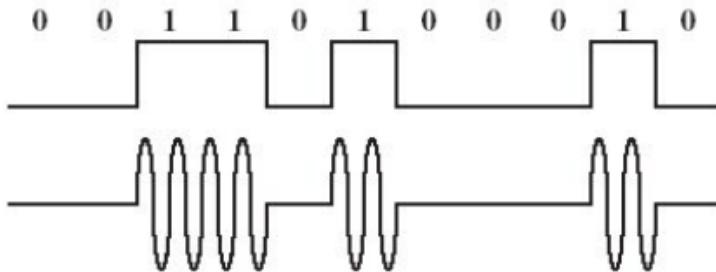
Un altro vantaggio è legato alla possibilità di trasmettere più comunicazioni differenti e contemporanee sullo stesso mezzo, trasferendo le bande relative alle diverse comunicazioni in zone differenti della banda utile per la trasmissione (**multiplexing a divisione di frequenza**).

Esistono diverse tecniche di modulazione, e in queste si sfrutta il segnale modulante per modulare le caratteristiche della portante:

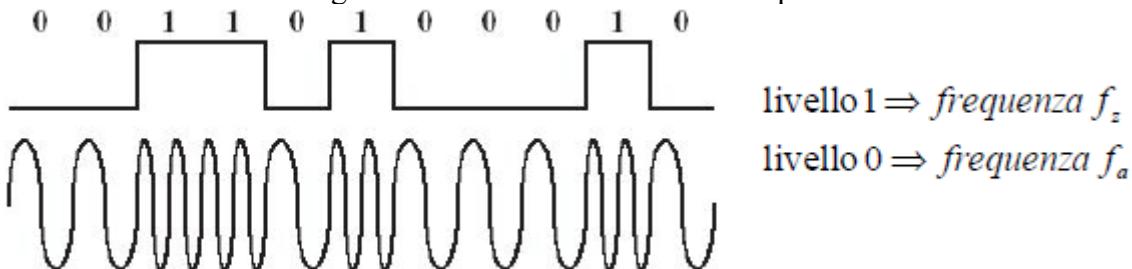
- **ampiezza:** il segnale viene utilizzato per modificare il valore della ampiezza della portante (modulazione di ampiezza).
- **frequenza:** il segnale modulante modifica istante per istante la frequenza della portante (modulazione di frequenza).
- **fase:** il segnale modulante cambia la fase della portante (modulazione di fase).

Di seguito saranno elencate alcune tecniche di modulazione:

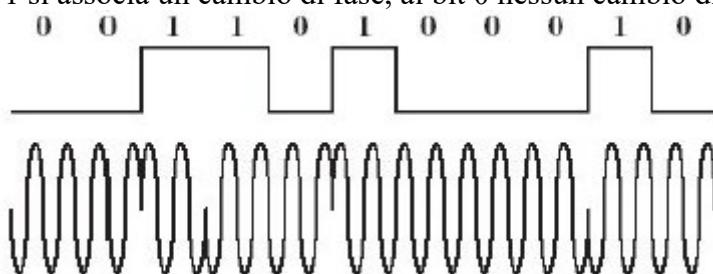
- **Tecnica ASK(Amplitude Shift Keying)** Partendo da un segnale numerico (ad esempio un segnale NRZ) si puo' modulare in ampiezza una portante sinusoidale moltiplicando la sua ampiezza per **il segnale numerico**.



- **Tecnica FSK(Frequency Shift Keying)** Il segnale numerico puo' essere utilizzato per modulare in frequenza una portante sinusoidale, modificando la sua frequenza in funzione del segnale modulante , cioe' facendo corrispondere due frequenze ai due valori del bit, se la frequenza aumenta corrisponde ad uno se diminuisce a 0. Un requisito importante nella FSK è la continuità di fase negli istanti di transizione da una frequenza all'altra.



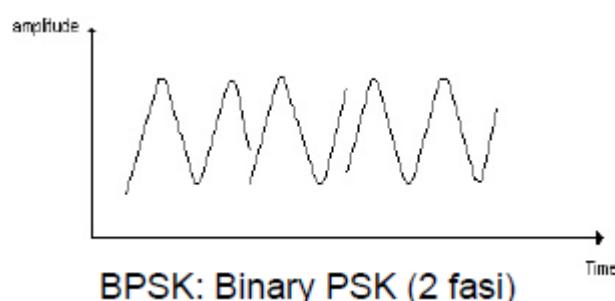
- **Tecnica PSK(Phase Shift Keying):** Il segnale numerico puo' modulare in fase una portante sinusoidale associano un certo valore di fase ad un certo valore di bit . Nell'esempio in figura al bit 1 si associa un cambio di fase, al bit 0 nessun cambio di fase:



- **Tecnica BPSK(Binary Phase Shift Keying):** si ha una sola portante e quindi i due valori numerici uno e zero sono fatti corrispondere a due fasi diverse della stessa frequenza: 0° e 180° . Precisamente:

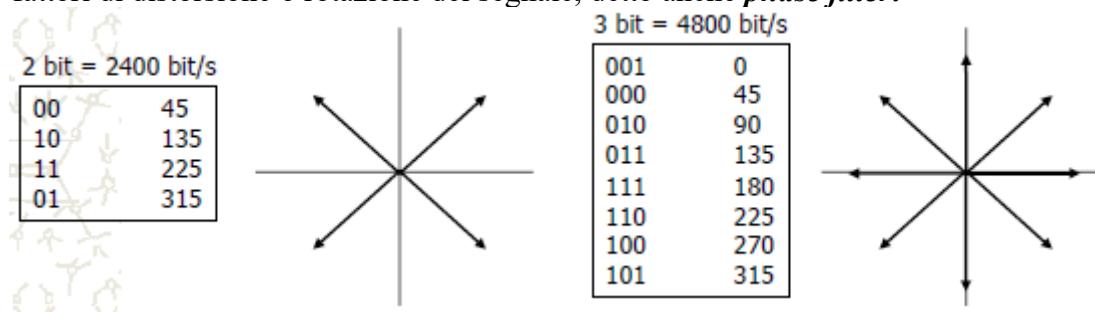
livello 1 \Rightarrow fase φ_z

livello 0 \Rightarrow fase φ_a

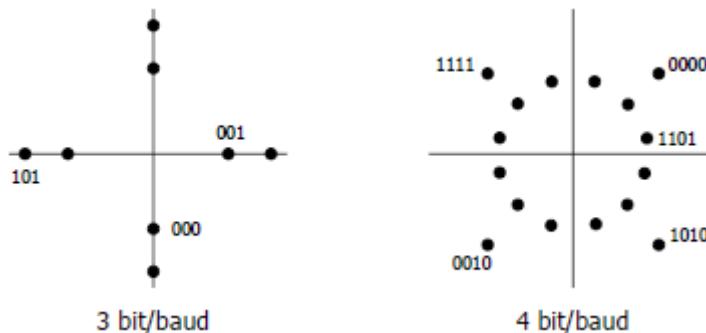


Si ottiene una migliore efficienza del canale modulando in modo che ogni simbolo trasporti piu' bit. La modulazione polifase si realizza effettuando una codifica preliminare dei bit provenienti dal terminale, raggruppandoli in parole di n bit e facendo corrispondere a ciascuna delle 2^n parole possibili una determinata fase della frequenza portante.

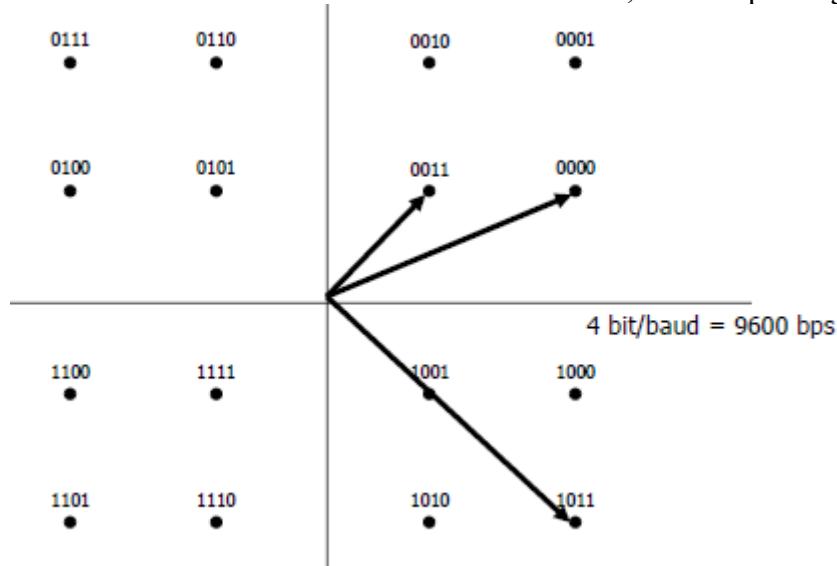
- **Tecnica QPSK (Quadrature Phase Shift Keying):** ha 4 fasi, Nella modulazione QPSK si utilizzano quattro angoli di fase per trasmettere due bit per simbolo; ad esempio: Non si può aumentare indefinitamente il numero di bit per campione perché entrano in gioco fattori di distorsione o rotazione del segnale, detto anche *phase jitter*.



- **Tecnica QAM(Quadrature Amplitude Modulation):** per aumentare la velocità di trasmissione, mantenendo costante la velocità di modulazione, invece di trasmettere solo due valori angolari, 0° e 180° , si trasmette un maggior numero di angoli diversi fra loro, e per consentire una più facile demodulazione in ricezione, si fa variare anche l'ampiezza del segnale modulato dando luogo così alla modulazione QAM. Le più moderne modulazioni numeriche, quelle quindi che determinano grandi velocità di trasmissione, sono quindi modulazioni di fase e di ampiezza. Quindi la codifica dei bit non viene solo affidata alla variazione di fase, ma anche a quella di ampiezza.



Questi schemi risultatni sono chiamati costellazioni, un esempio migliore è il seguente:

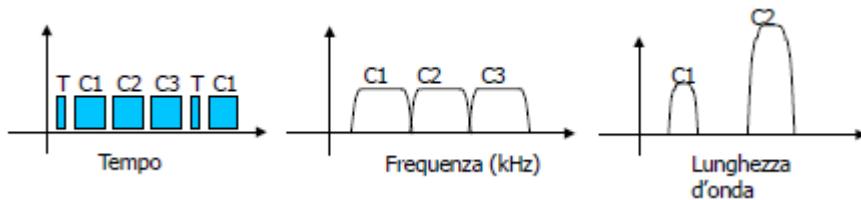


MULTIPLAZIONE E TECNICHE DI MULTIPLAZIONE

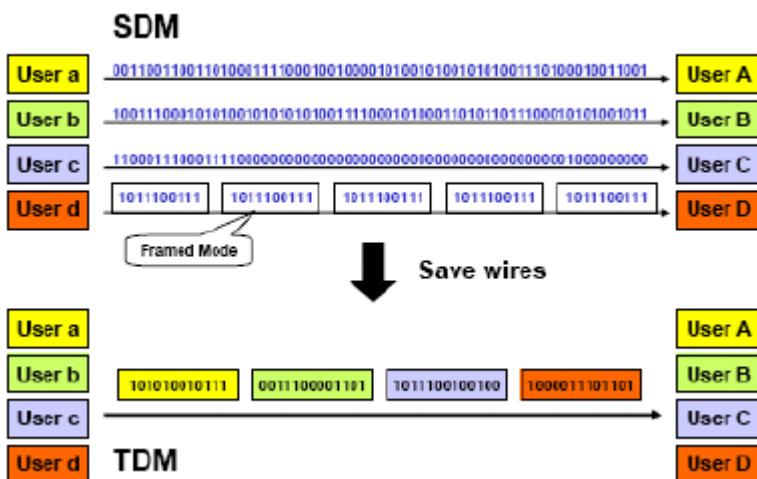
Nelle telecomunicazioni, elettronica e reti di computer, la **multiplazione(multiplexing)**, è il meccanismo o tecnica di trasmissione per cui più canali trasmissivi in ingresso condividono la stessa capacità trasmissiva disponibile in uscita ovvero combinando più segnali analogici o flussi di dati digitali (detti segnali tributari) in un solo segnale (detto multiplato) trasmesso in uscita su uno stesso collegamento fisico. In una comunicazione dati la multiplazione permette di risparmiare sul cablaggio (riducendo il numero di linee di segnale) e sul numero di componenti. Il dispositivo elettronico preposto alla multiplazione è detto multiplexer(è un circuito integrato che seleziona uno o più segnali in ingresso [o](#) analogici o digitali e li inoltra di volta in volta attraverso una singola linea di uscita).

Di seguito sono elencate alcune tecniche di Multiplazione:

- **A divisione di tempo (TDM):**
 - modalità deterministica o dinamica (banda dedicata e ritardo fisso, a quale utente tocca trasmettere "arbitraggio")
 - modalità statistica o statica (banda e delay variabili e migliore sfruttamento del mezzo) tanti utenti utilizzano il mezzo trasmittivo in base al tempo.
 - **A divisione di spazio (SDM):** Dati inviati su media fisicamente separati (fibra).
 - **A divisione di frequenza (FDM e WDM):** usa differenti frequenze o lunghezze d'onda per differenziare i dati trasmessi.
 - Per **codifica (CDM):** La differenziazione dei dati trasportati è ottenuta utilizzando diversi tipi di codifica, li trasmette quindi simultaneamente nel canale trasmittivo codificandoli in modo diverso.



- SDM: una connessione fisica per trasmissione.
 - TDM: La stessa connessione utilizzata per 4 trasmissioni distinte
 - Richiede tramatura dei flussi e uso di Multiplexer e demultiplexer.
 - Meno efficiente ma ottimizza l'uso dei mezzi trasmissivi.

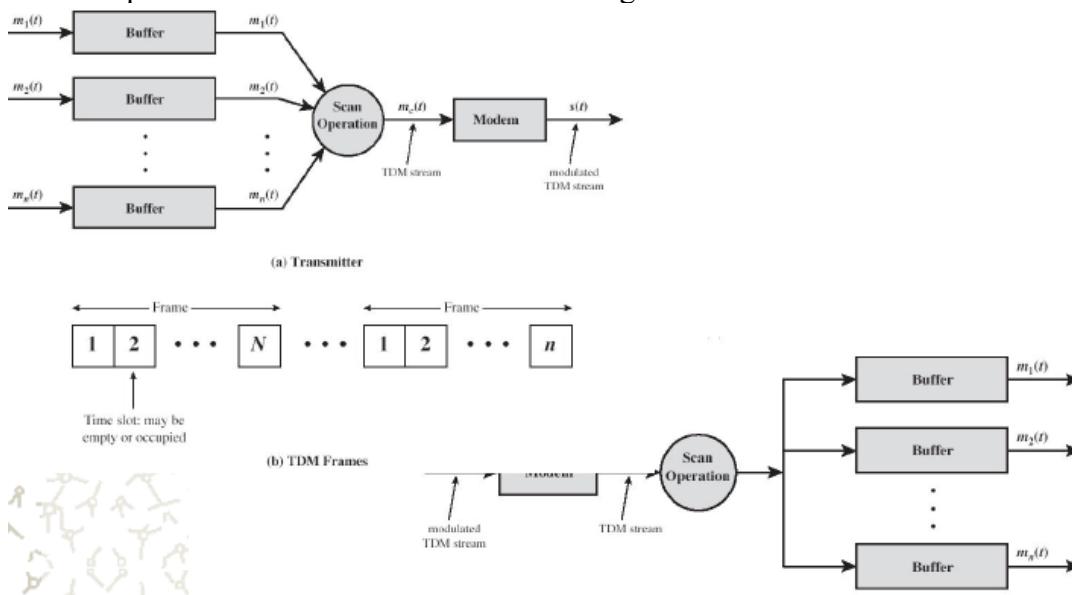


TDM (TIME DIVISION MULTIPLEXING)

Il multiplexing a divisione di tempo è utilizzato quando si dispone di un canale digitale capace di un elevato tasso di trasmissione dati in cui poter trasmettere contemporaneamente un insieme di comunicazioni a tasso inferiore. Si mischiano i dati delle diverse comunicazioni, inframezzando i bit delle diverse trasmissioni. Di fatto si divide la disponibilità del canale in periodi temporali, e si dedicano a turno i diversi periodi a diversi flussi trasmissivi.

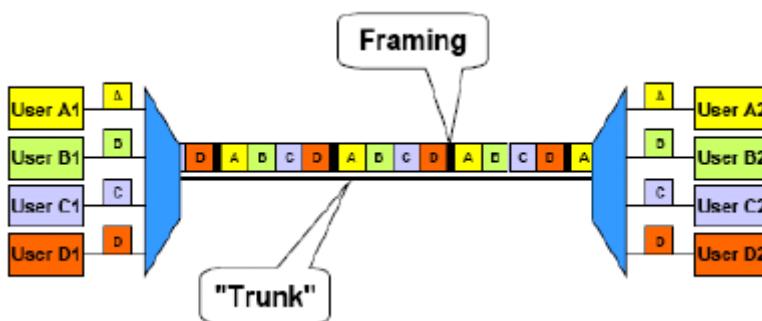
Ogni intervallo temporale si chiama slot e può contenere uno o più bit relativi ad un flusso indipendente. Il flusso dei dati è organizzato in trame (frame). Una trama è l'insieme di slot temporali che contiene almeno un bit per ciascuna trasmissione. Uno slot potrebbe far passare un'intera trama o una parte di essa.

Anche in questo caso il flusso relativo ad una singola trasmissione è detto canale.



Esistono essenzialmente due metodi di multiplazione nel TDM:

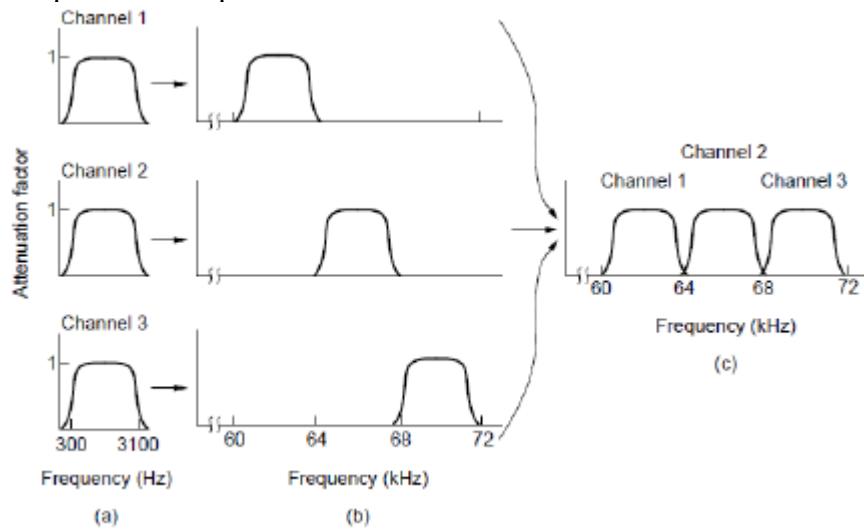
- **Deterministico:** ogni canale di comunicazione è identificato dalla sua posizione in termini di slot temporali all'interno della trama. Questa correlazione fissa fra il canale di comunicazione e il relativo timeslot è il principale svantaggio del TDM deterministico: se il canale non è usato comunque occupa il timeslot inviando un pattern idle. Il pattern idle è costituito da un trunk che aggredisce i canali, infatti ogni slot è associato ad un canale di lunghezza fissa, ed ogni slot trasporta una trama, ogni trama ha dimensione uguale. Il frame all'interno di un pattern è ripetuto ciclicamente ogni tot intervalli di tempo.



- **Statistico:** non esiste correlazione fra canale di comunicazione e relativo timeslot. La capacità del mezzo è distribuita statisticamente fra gli utenti che ne concorrono all'uso. È necessario uno schema separato di tramatura e indirizzamento per garantire le associazioni dinamiche: se un canale non è usato gli altri canali possono disporre della sua capacità trasmissiva. Qui i frame hanno taglia differente, per far in modo che non si liberi mai si una un sistema di bufferizzazione per tenerlo occupato. Per evitare starvation ha bisogno di un sistema di scheduling, è molto utilizzato perché è sempre occupato.

FDM (FREQUENCY DIVISION MULTIPLEXING)

Se il segnale che mando lo invio ad una velocità tale che occupa uno spazio limitato, possiamo modulare più segnali in modo che nessuno di loro si tocchi. Usa la trasmissione in banda passante, dividendo lo spettro in bande di frequenza separate, una per canale. Nessuna coppia di canali può condividere la stessa porzione di spettro.

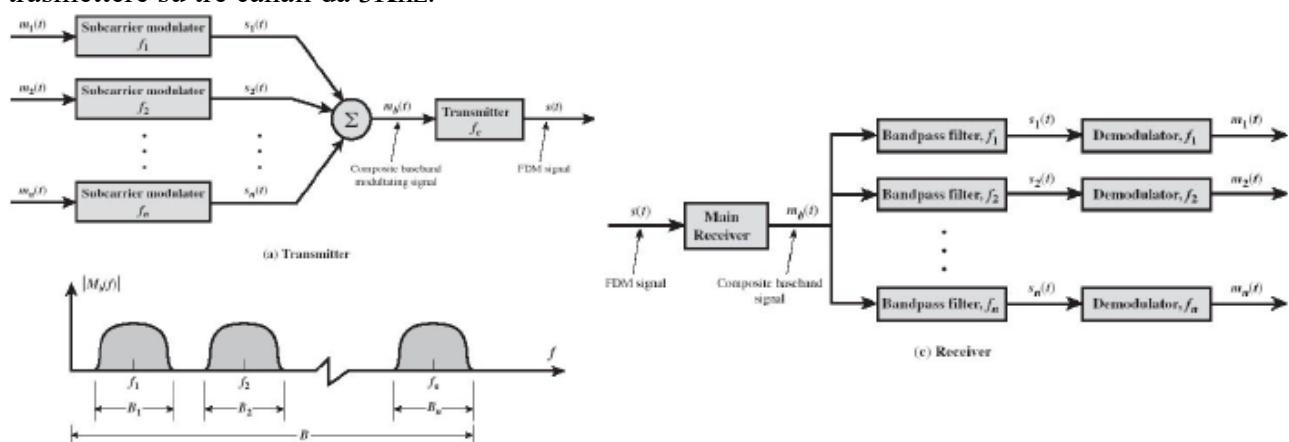


NOTA:

Il portante è il mezzo trasmissivo.

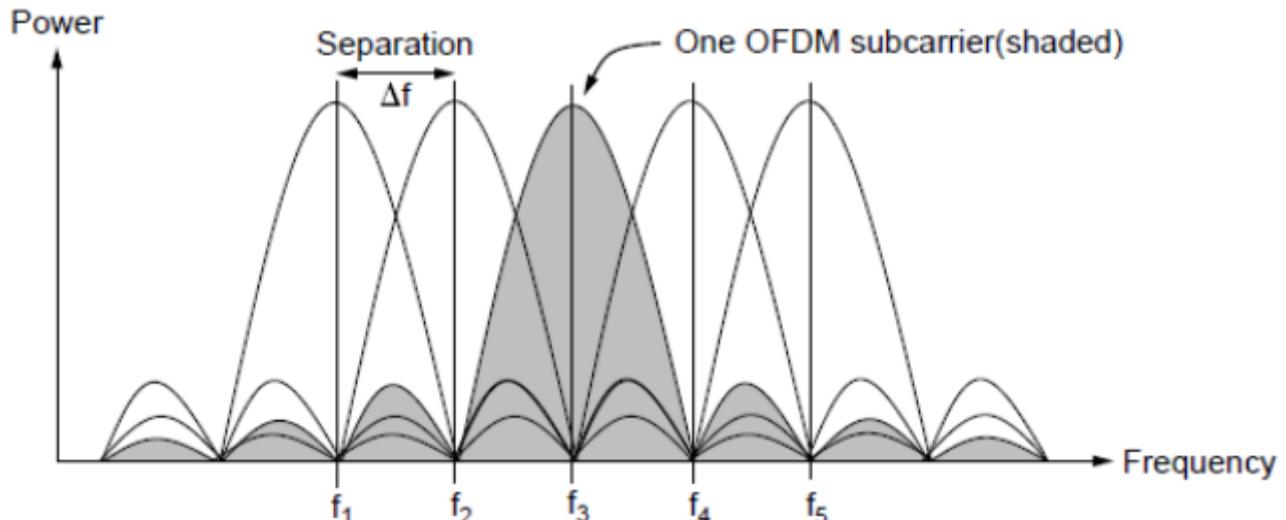
La portante è il segnale modulato per trasportare i dati.

L'effetto della modulazione su un segnale sinusoidale a frequenza f si traduce nella generazione di un segnale il cui spettro ha la stessa forma dello spettro del segnale modulante ma traslato attorno alla frquenza f della portante. In presenza di una serie di segnali ciascuno con Banda B, e di un mezzo che ha una capacità di banda limitata dai valori f_1 e f_2 ($f_2-f_1 \gg B$), possiamo utilizzare ciascun segnale per modulare segnali sinusoidali alle frequenze f_1+B , f_1+2B , f_1+3B , ecc. I segnali modulanti ooccuperanno porzioni distinte entro la banda trasmissiva del mezzo, e potranno essere trasmessi contemporaneamente senza interferire. In ricezione, opportune operazioni di demodulazione e filtraggio permetteranno di separare i detersi traffici, facendo transitare solotanto il segnale che desideriamo. Sfruttando questo meccanismo con un segnale di 10Khz possiamo trasmettere su tre canali da 3Khz.



OFDM(ORTOGONAL FREQUENCY DIVISION MULTIPLEXING)

Si individuano delle portanti precise, si calcola la loro probabilità di rimbalzo e eventualmente vengono usate. Si scelgono molto più fitte in modo che occupino sezioni dello spettro molto piccole, in modo che tra loro siano ortogonali. Per distinguere questi segnali si usa la trasformata di Fourier. Nel leggere i segnali si ha che il segnale che si cerca è posizionato ad 1 mentre tutti gli altri a 0. Così facendo vengono multiplati più canali che grazie a questa proprietà non creano interferenza tra loro(esempio: wi-fi).



CDM(CODE DIVISION MULTIPLEXING)

La multiplazione è realizzata moltiplicando in trasmissione l'informazione binaria generata da una sorgente per un'opportuna parola di codice detta chip. La sequenza $s(t)$ in uscita dal moltiplicatore sarà successivamente modulata e infine trasmessa sul canale. In ricezione il segnale ricevuto $r(t)$ dal ricevitore sarà costituito dalla somma vettoriale (comprensiva di modulo e fase) di tutti i segnali trasmessi dalle singole sorgenti di informazione, con in più un eventuale termine dovuto al rumore termico. Se i chip delle sorgenti sono ortogonali tra loro, l'estrazione dell'informazione associata a ciascuna sorgente potrà essere fatta in maniera complementare alla trasmissione moltiplicando il segnale ricevuto con il particolare codice associato alla sorgente che si vuole estrarre e integrando successivamente il segnale ottenuto in un intervallo di tempo pari alla durata del bit di informazione. Ciò permette di ottenere un segnale che è dato dalla somma di un segnale di ampiezza dominante, (o utile, associato alla sorgente da estrarre), e di un segnale di ampiezza minore, costituito da una combinazione fra rumore termico e quelli associati alle altre sorgenti. La codifica del segnale non condiziona l'intelligibilità. Il codificatore CDM è costituito principalmente da due parti, la prima che divide la sequenza di bit generata da un codificatore (opzionale) in M repliche (ad esempio, se la sequenza era $+1 +1 -1$, ora sarà M volte $+1$, M volte $+1$ ecc..), e la seconda parte che moltiplica ogni replica generata per un termine $d[m]$, chiamato CODICE DI CANALIZZAZIONE di lunghezza M . Ogni bit del codice di canalizzazione (ad es $+0-1$) viene moltiplicato con le repliche della sequenza iniziale in modo da generare un codice in base alla sequenza di partenza. In ricezione, quindi, il segnale potrà essere decodificato soltanto da chi avrà il codice di canalizzazione esatto.

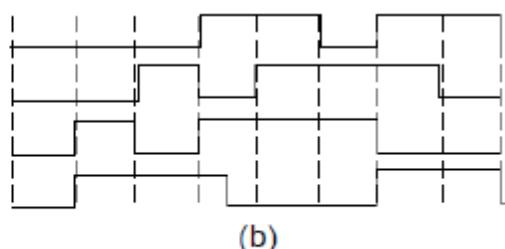
$$A = (-1 -1 -1 +1 +1 -1 +1 +1)$$

$$B = (-1 -1 +1 -1 +1 +1 +1 -1)$$

$$C = (-1 +1 -1 +1 +1 +1 -1 -1)$$

$$D = (-1 +1 -1 -1 -1 -1 +1 -1)$$

(a)



Chip sequences for four stations

Signals the sequences represent

$$\begin{array}{ll}
 S_1 = C & = (-1 + 1 - 1 + 1 + 1 + 1 - 1 - 1) \\
 S_2 = B + \bar{C} & = (-2 \ 0 \ 0 \ 0 + 2 + 2 \ 0 - 2) \\
 S_3 = A + B & = (\ 0 \ 0 - 2 + 2 \ 0 - 2 \ 0 + 2) \\
 S_4 = A + \bar{B} + C & = (-1 + 1 - 3 + 3 + 1 - 1 - 1 + 1) \\
 S_5 = A + B + \bar{C} + D & = (-4 \ 0 - 2 \ 0 + 2 \ 0 + 2 - 2) \\
 S_6 = A + B + C + D & = (-2 - 2 \ 0 - 2 \ 0 - 2 + 4 \ 0)
 \end{array}
 \quad
 \begin{array}{l}
 S_1 \cdot C = [1+1-1+1+1-1-1]/8 = 1 \\
 S_2 \cdot C = [2+0+0+0+2+2+0+2]/8 = 1 \\
 S_3 \cdot C = [0+0+2+2+0-2+0-2]/8 = 0 \\
 S_4 \cdot C = [1+1+3+3+1-1+1-1]/8 = 1 \\
 S_5 \cdot C = [4+0+2+0+2+0-2+2]/8 = 1 \\
 S_6 \cdot C = [2-2+0-2+0-2-4+0]/8 = -1
 \end{array}$$

(c)

(d)

MEZZI TRASMISSIVI

I mezzi trasmissivi si dividono in due tipologie:

- **Linee:** Rame, fibre ottiche;
- **Wireless:** Suoni, luce, raggi infrarossi, radiofrequenza, microonde.

Possiamo classificare questi mezzi fisici di trasmissione in ulteriori due categorie:

- **Mezzi guidati:** elettronici, ottici;
- **Mezzi non guidati:** onde radio, laser via etere.

Ogni mezzo è tipicamente caratterizzato da:

- Larghezza di banda.
- Delay: tempo che ci mette il segnale dalla partenza alla destinazione.
- Costo: un mezzo troppo costoso non è molto conveniente, è per questo motivo che si preferisce il rame all'oro.
- Facilità di installazione e manutenzione: quanto è pratica l'installazione e la manutenzione del mezzo trasmissivo.
- Rapporto segnale rumore: è una caratteristica in modo indipendente dal tipo di trasmissione, e si tratta di quanto rumore genera il mezzo trasmissivo.

I mezzi trasmissivi elettrici rappresentano ancora oggi il mezzo più diffuso, e nell'ambito delle reti locali assumono fondamentale importanza soprattutto per la realizzazione di infrastrutture per la trasmissione di segnali all'interno degli edifici. Dovendo trasportare il segnale in forma di energia elettrica, è necessario che le caratteristiche elettriche del mezzo siano tali da rendere massima la trasmissione dell'energia da un estremo all'altro e minima la dissipazione in altre forme (ad esempio calore, irradiazione elettromagnetica). Con l'attuale tecnologia è possibile realizzare mezzi trasmissivi elettrici di caratteristiche sufficientemente elevate da permettere la trasmissione dei dati a velocità superiori a 1000 Mb/s. Il mezzo più largamente diffuso è il rame, ed è molto meno soggetto a fenomeni d'interferenza rispetto al wireless.

Un mezzo trasmissivo elettrico **ideale**, che trasporti tutta l'energia del segnale trasmesso senza attenuazione né distorsione, **non esiste**. Un mezzo trasmissivo elettrico **ottimale** è caratterizzato da bassa resistenza, bassa capacità e bassa induttanza, cioè è un mezzo poco dispersivo e poco dissipativo. In tale mezzo **quasi tutta la potenza** inviata sul canale dal trasmettitore **arriva al ricevitore** ed il segnale non viene distorto. Conviene infatti seguire il mezzo in base alla distanza cui dobbiamo trasmettere.

SCHERMATURA

È in continua crescita l'attenzione al problema dei disturbi elettromagnetici (EMI), dei quali le reti locali sono al contempo vittime e sorgenti. Con la presenza di schermi e con una corretta messa a terra si possono ridurre drasticamente la sensibilità e l'emissione di disturbi elettromagnetici, e possono migliorare anche notevolmente le caratteristiche elettriche di un cavo.

Ne esistono numerosi tipi, i più utilizzati nelle LAN sono:

- **"foglio"** (*foil*): si tratta normalmente di un foglio di alluminio molto sottile (da 0.05 mm a 0.2 mm) che avvolge il cavo immediatamente sotto alla guaina di protezione esterna. Poiché l'alluminio presenta elevata resistenza elettrica rispetto al rame, e, a spessori così ridotti, una notevole fragilità, lungo il foglio scorre un filo di rame nudo, detto *drain*, che garantisce continuità elettrica anche in caso di eventuali crepe; tale filo è utilizzato per il collegamento di terra;
- **"calza"** (*braid*): si tratta di una treccia di fili di rame che avvolgono il cavo in due

direzioni opposte. Presenta una conducibilità molto migliore del foglio di alluminio, ma la copertura non è completa, in quanto in corrispondenza degli intrecci rimangono inevitabilmente dei fori nello schermo.

I migliori risultati si ottengono dalla combinazione di più schermi diversi

TIPI DI MEZZI TRASMISSIVI:

NASTRO MAGNETICO

Uno dei sistemi più comuni adottati per trasferire i dati da un computer a un altro funziona così: si scrivono le informazioni su un nastro magnetico o su un supporto rimovibile (per esempio un DVD), si trasporta fisicamente il nastro o il disco, e infine si utilizza l'apposita unità installata nel computer di destinazione per leggere i dati. Anche se non è sofisticato come la comunicazione satellitare geosincrona, questo metodo è spesso più economico, soprattutto nel caso di applicazioni in cui un'elevata ampiezza di banda o il costo per bit trasmesso rappresentano i fattori chiave. Una scatola di nastri come questa può essere spedita ovunque negli Stati Uniti in 24 ore con Federal Express o un altro corriere espresso. L'ampiezza di banda effettiva di questa trasmissione è pari a 1.600 terabit/86.400 sec, ossia 19 Gbps. Se la destinazione si trova a un'ora di strada, l'ampiezza di banda supera i 400 Gbps. Nessuna rete di computer è in grado di raggiungere questa velocità. Per una banca che ha la necessità di trasferire ogni giorno il backup di molti GB di dati su una seconda macchina, probabilmente nessun'altra tecnologia di trasmissione è in grado di raggiungere le stesse prestazioni dei nastri magnetici. Certo, le reti stanno diventando sempre più veloci, ma anche la densità dei nastri sta aumentando.

IL DOPPINO

L'ampiezza di banda del nastro magnetico è eccellente, ma il suo ritardo è eccessivo; la durata della trasmissione è espressa in minuti e in ore, non in millisecondi. Molte applicazioni richiedono una connessione on-line: uno dei mezzi di trasmissione più vecchi, ma ancora molto in voga, è il doppino.

Il doppino è composto da due conduttori di rame isolati. L'intreccio è utilizzato perché due cavi paralleli formano un'eccellente antenna; quando invece i cavi sono intrecciati, i campi elettromagnetici generati dai due conduttori si annullano a vicenda, perciò il cavo irradia meno.

L'applicazione più comune del doppino è il sistema telefonico. Quasi tutti i telefoni sono collegati alla centrale telefonica attraverso un doppino. I doppini possono estendersi per diversi chilometri senza richiedere un'amplificazione del segnale, ma per distanze più lunghe è necessario installare dei ripetitori. Quando molti doppini procedono in parallelo per lunghe distanze, come accade per i cavi che collegano uno stabile alla centrale telefonica, è necessario fasciare insieme i cavi rivestendoli con una guaina protettiva; se non ci fosse l'intreccio, i doppini in questi fasci interferirebbero l'uno con l'altro. Nelle zone in cui le linee telefoniche sono aeree, capita di vedere sui pali telefonici fasci di cavi con diametro di alcuni centimetri.

I doppini si possono usare per trasmettere segnali analogici e digitali. L'ampiezza di banda dipende dal diametro del cavo e dalla distanza percorsa, ma il più delle volte per tratti lunghi pochi chilometri è possibile raggiungere velocità di alcuni Mb al secondo. Per il loro basso costo e il discreto livello di prestazioni, i doppini sono largamente utilizzati e probabilmente lo saranno anche per gli anni a venire. I doppini riescono ad eliminare anche il problema della diafonia; La diafonia è un fenomeno di accoppiamento elettrico tra mezzi trasmissivi vicini non isolati adeguatamente. Il segnale trasmesso su un cavo genera per induzione un segnale corrispondente nel cavo vicino, che si sovrappone al segnale trasmesso in quest'ultimo. Si può verificare anche nella trasmissione con mezzi non guidati, quando un segnale emesso da una antenna si disperde durante la propagazione nell'aria; la parte dispersa può guingere in prossimità di un'altra antenna. Il doppino riesce ad eliminarla grazie alla binatura, utilizzando anche cavi con più coppie (4, 25, 50 e oltre).

I doppini sono nati come mezzo trasmissivo a banda molto ridotta, ma negli ultimi anni hanno raggiunto prestazioni una volta raggiungibili soltanto con i cavi coassiali. I miglioramenti sono stati ottenuti realizzando nuovi materiali isolanti, curando la geometria delle coppie (anche tramite

l'adozione di particolari guaine esterne), mettendo a punto sofisticati algoritmi di differenziazione dei passi di binatura e aumentando la sezione dei conduttori. Il doppino è stato creato per rispattare una perfetta binatura fino a 100m prima di avere la diafonia, con un errata binatura dopo 5 o 6 metri si ha il fenomeno di diafonia. Le caratteristiche che hanno tuttavia inciso maggiormente sulla diffusione del doppino sono la compatibilità con la telefonia e la facilità di posa in opera. Esistono varie versioni di doppino:

- STP (*Shielded Twisted Pair*), versione con uno schermo per ogni coppia più uno schermo globale (calza in rame);
- Screened, FTP (*Foiled Twisted Pair*) o S-UTP (figura 3.22), versione con un unico schermo (normalmente in foglio di alluminio) per tutto il cavo;
- UTP (*Unshielded Twisted Pair*) (figura 3.23) versione non schermata.

I parametri elettrici di qualsiasi cavo variano con la frequenza. Occorre chiedersi, per una data applicazione, a quale frequenza sia opportuno operare per decidere se un cavo sia adeguato all'applicazione stessa. È stata creata una classificazione che prevede sette *categorie*, in base alle applicazioni per le quali i cavi sono idonei. La categoria 1 è quella dei cavi peggiori, la 7 quella dei migliori. Ogni categoria è idonea a fornire tutti i servizi offerti da quelle inferiori:

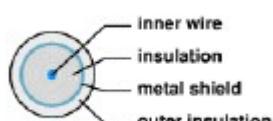
- La **categoria 1** (*Telecommunication*) comprende i cavi adatti unicamente a telefonia analogica.
- La **categoria 2** (*Low Speed Data*) comprende i cavi per telefonia analogica e digitale (ISDN) e trasmissione dati a bassa velocità (per esempio linee seriali).
- La **categoria 3** (*High Speed Data*) è la prima categoria di cavi adatti a realizzare reti locali fino a 10 Mb/s, in particolare per soddisfare gli standard 10BaseT di 802.3 e Token-Ring a 4Mb/s.
- La **categoria 4** (*Low Loss, High Performance Data*) comprende i cavi per LAN Token-Ring fino a 16 Mb/s.
- La **categoria 5** (*Low Loss, Extended Frequency, High Performance Data*) comprende cavi per applicazioni fino a 100 Mb/s, su distanze di 100 metri.
- La **categoria 6** (*Low Loss, High Frequency, High Performance Data*) comprende i migliori cavi disponibili, per applicazioni fino a 1000 Mb/s, su distanze di 100 metri.
- La **categoria 7** (ISO/IEC 11801 Class F), nome informale. Lo standard specifica 4 STP all'interno di un unico cavo, per velocità fino a 10Gb/s.

Tutte queste caratteristiche devono durare per 25 anni. I cavi di categoria 6 rappresentano oggi lo stato dell'arte nel campo del cablaggio delle LAN. Tutti gli standard di rete a velocità di 100 Mb/s maggiori con trasmissione su due coppie prevedono l'uso di cavi di categoria 5 o superiore. Oggi sono diffusi cablaggi secondo la categoria 6, ed è stata standardizzata anche la categoria 7 per applicazioni ad altissime velocità.

IL CAVO COASSIALE

Un altro mezzo di trasmissione molto comune è il cavo coassiale. Essendo più schermato del doppino, il cavo coassiale può estendersi per distanze più lunghe e consente velocità più elevate. Esistono due tipi di cavi coassiali: il primo, a 50 Ohm, è utilizzato per le trasmissioni digitali; il secondo, a 75 Ohm, è utilizzato per le trasmissioni analogiche, per la televisione e le connessioni Internet via cavo. Non è più usato nelle LAN, perché è stato eliminato dallo standard ISO/IEC 11801 per i cablaggi strutturati e sostituito dalle fibre ottiche nella fascia ad alte prestazioni e dai doppini in quella a medie prestazioni, mentre continua ad essere utilizzato nelle reti **geografiche (micro-coassiale)**.

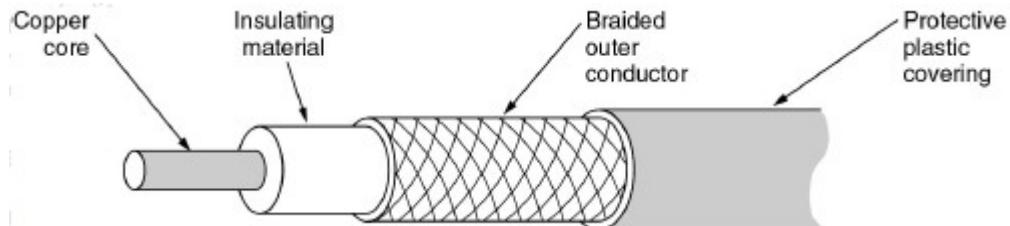
Cavo coassiale a banda base: Consiste in un filo di rame rigido circondato da una garza metallica che funge da schermo:



era in genere di 50ohm.

La larghezza di banda dipende dalla lunghezza del cavo: per lunghezze di 1 km sono possibili velocità che variano da 1 a 2 Gbps. Si possono avere anche cavi più lunghi, ma occorre ridurre la velocità di trasmissione e frammezzare ai tratti di cavo degli amplificatori di segnale.

Cavo coassiale a larga banda: Consiste in un cavo identico a quello in banda base, ma con un sistema di trasmissione diverso. Su coassiale in banda larga, la trasmissione avviene in analogico, cioè in maniera del tutto simile alla trasmissione televisiva.

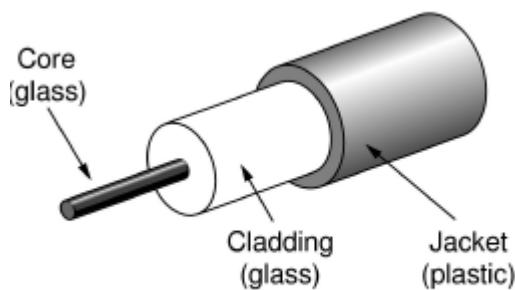


La larghezza di banda in questo caso è di 300 Mhz, con lunghezze anche di 100 km. I sistemi a banda larga suddividono il canale totale in canali da 6 Mhz, che possono essere utilizzati per la trasmissione di emittenti TV, audio ad alta qualità (1,4 Mbps) o un flusso digitale a 3 Mbps.

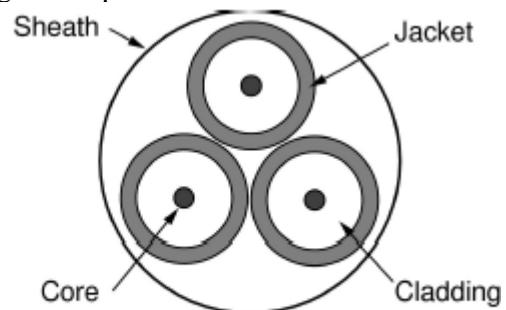
La trasmissione power line (o a onde convogliate) è una tecnologia per la trasmissione dati che utilizza la rete di alimentazione elettrica come mezzo trasmissivo. Si realizza sovrapponendo al trasporto di corrente elettrica, continua o alternata a bassa frequenza (50 Hz in Europa e gran parte dell'Asia e dell'Africa, 60 Hz in altre regioni del mondo), un segnale a frequenza più elevata che è modulato dall'informazione da trasmettere. La separazione dei due tipi di correnti si effettua grazie al filtraggio e separazione degli intervalli di frequenze utilizzate.

FIBRE OTTICHE

Consistono in un cavo composto da un anima trasparente di silicio avvolto in un rivestimento di vetro con indice di rifrazione diverso. Tutta la parte in vetro è ricoperta da una guaina di plastica nera. Le fibre sono normalmente raggruppate insieme intorno ad un filo di metallo che facilita la posa del cavo. Non è soggetta a interferenze elettromagnetiche, lla parte per trasmettere è il core; il cladding è un materiale che ha un indice di rifrazione maggiore rispetto al core.



(a)



(b)

Caratteristiche principali:

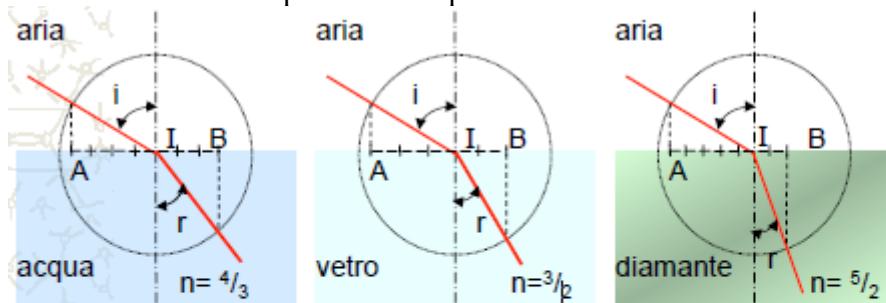
- +banda (alcune decine di THz)
- +immunità ai disturbi
- + leggerezza e flessibilità
- + meno pericolosa dei mezzi metallici
- + meno costosa dei mezzi metallici
- + sicurezza e protezione da intrusioni
- - difficoltà di connettorizzazione e interfacciamento
- - dispersioni
- - effetti non lineari.

Dalla soluzione delle equazioni di Maxwell si ricava che l'energia si propaga nella fibra in un numero discreto di configurazioni. Queste configurazioni sono chiamate modi e ogni singolo modo ha sue caratteristiche di propagazione. La larghezza di banda in questo caso è di oltre 30.000 Ghz.

L'attuale limite di trasmissione è dovuto semplicemente al fatto che un sistema a fibra ottica necessita di due conversioni: la prima da elettrico a luce, e la seconda luce ad elettrico.

$$\left\{ \begin{array}{l} \nabla^2 \phi - \frac{1}{c^2} \frac{\partial^2 \phi}{\partial t^2} = -\frac{\rho}{c} \\ \nabla^2 A_x - \frac{1}{c^2} \frac{\partial^2 A_x}{\partial t^2} = -\mu \rho v_x \\ \nabla^2 A_y - \frac{1}{c^2} \frac{\partial^2 A_y}{\partial t^2} = -\mu \rho v_y \\ \nabla^2 A_z - \frac{1}{c^2} \frac{\partial^2 A_z}{\partial t^2} = -\mu \rho v_z \end{array} \right.$$

Si definisce rifrazione “il fenomeno per cui un raggio luminoso (non perpendicolare alla superficie di contatto) passando da un mezzo trasparente ad un altro, anch’esso trasparente, cambia direzione nel punto in cui attraversa la superficie di separazione dei due mezzi”.



$$n = \frac{IA}{IB} = \frac{\sin i}{\sin r}$$

Indice di rifrazione del secondo mezzo (attraversato dal raggio luminoso) rispetto al primo; il rapporto è costante al variare dell'angolo "i" del raggio incidente.

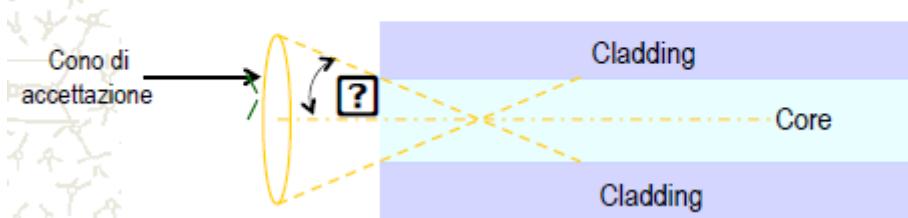
NOTA:

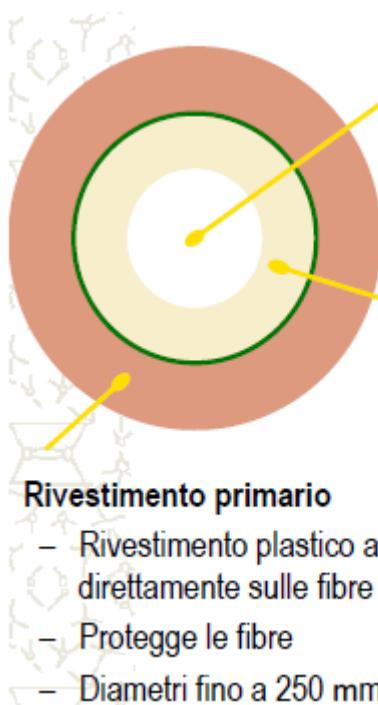
Con la rifrazione si attiva uno spostamento di un certo angolo del segnale.

Con la riflessione il segnale va avanti e torna indietro disturbando quindi il segnale.

L'apertura numerica indica la “quantità di luce che è possibile lanciare all'interno della fibra senza che questa venga riflessa”. È quindi caratterizzata da un angolo limite che varia in funzione degli indici di rifrazione del core e del cladding.

$$NA = \sqrt{n_1^2 - n_2^2} = \text{sen } ?$$





Core

- La luce viaggia attraverso il core
- Le dimensioni del core vanno da 8 a 100 mm

Cladding

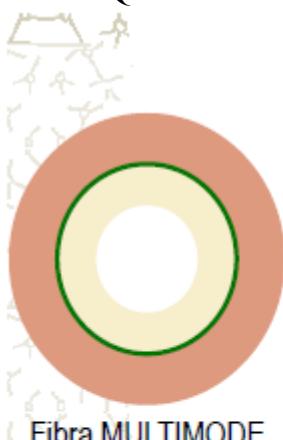
- Elemento in vetro come il core
- Fornisce un diverso indice di rifrazione rispetto al core
- Diametri da 125 - 140 mm

Rivestimento primario

- Rivestimento plastico applicato direttamente sulle fibre
- Protegge le fibre
- Diametri fino a 250 mm

La trasmissione all'interno dell'anima di vetro può avvenire con modalità diverse:

- **Fibra multimodale:** È una fibra il cui nucleo è abbastanza ampio da permettere diversi angoli di rimbalzo della luce trasmessa.
- **Fibra monomodale:** È una fibra il cui nucleo permette il passaggio di poche lunghezze d'onda. Questo fa comportare la fibra come una semplice guida d'onda.



Fibra MULTIMODE

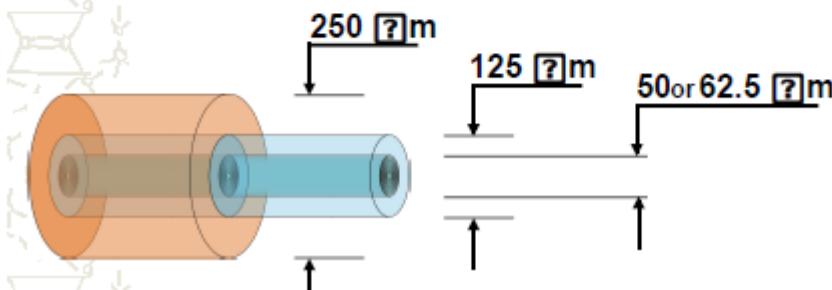
Disponibile in diverse dimensioni

- 50/125mm
- 62.5/125mm

Distanze fino a 2000 m

- Uso relativamente poco costoso con trasmittitori LED & VCSEL
- Finestre di operazione (1^a e 2^a)

- 850 nm
- 1300 nm



Dimensioni del core 8.1 - 10 mm

La fibra si comporta come una guida d'onda ammettendo una sola modalità di propagazione

La banda passante è elevatissima (centinaia di GHz*Km)

Dimensione del cladding 125mm

Distanze fisiche fino a 60 km, ma limitata in applicazioni locali a 3 Km

Uso di trasmettitori laser

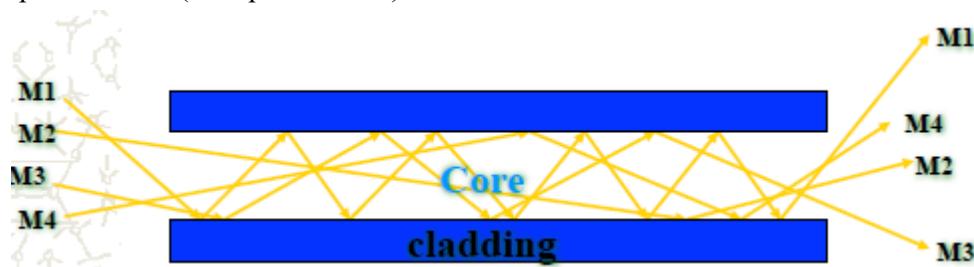
Finestre di operazione (2^a e 3^a finestra)

- 1310 nm

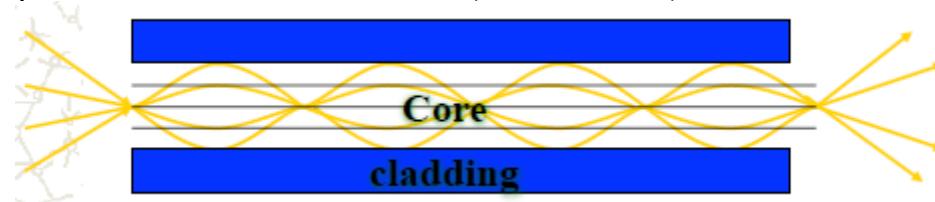
- 1550 nm

All'interno di una fibra ottica la luce ha più modi di propagazione, ciò genera dispersione modale che ne limita la banda; esistono diversi modi di "propagare" la luce all'interno della fibra:

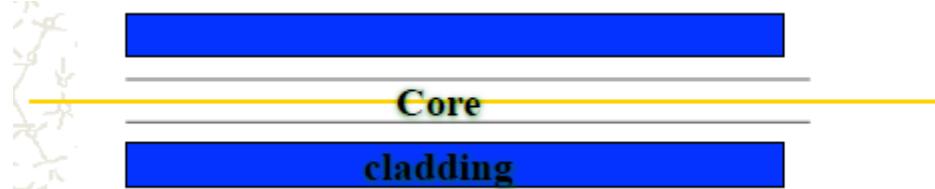
- **Fibre ottiche multimodali:** propagazione con diversi modi e percorsi.
- **Fibre ottiche multimodali step-index:** La variazione dell'indice di rifrazione tra core e cladding è brusca e causa molta dispersione modale, per questo motivo non vengono ormai più utilizzate (esempio: internet).

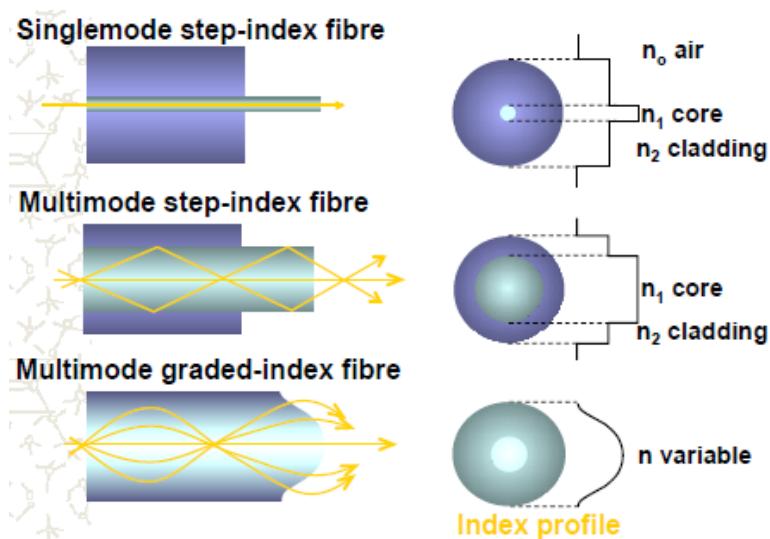


- **Fibre ottiche multimodali graded-index:** La variazione continua degli indici di rifrazione rallenta i raggi più centrali, per questo hanno una banda passante molto superiore alle step-index possono lavorare in 1^a e 2^a finestra (850 e 1300 nm).

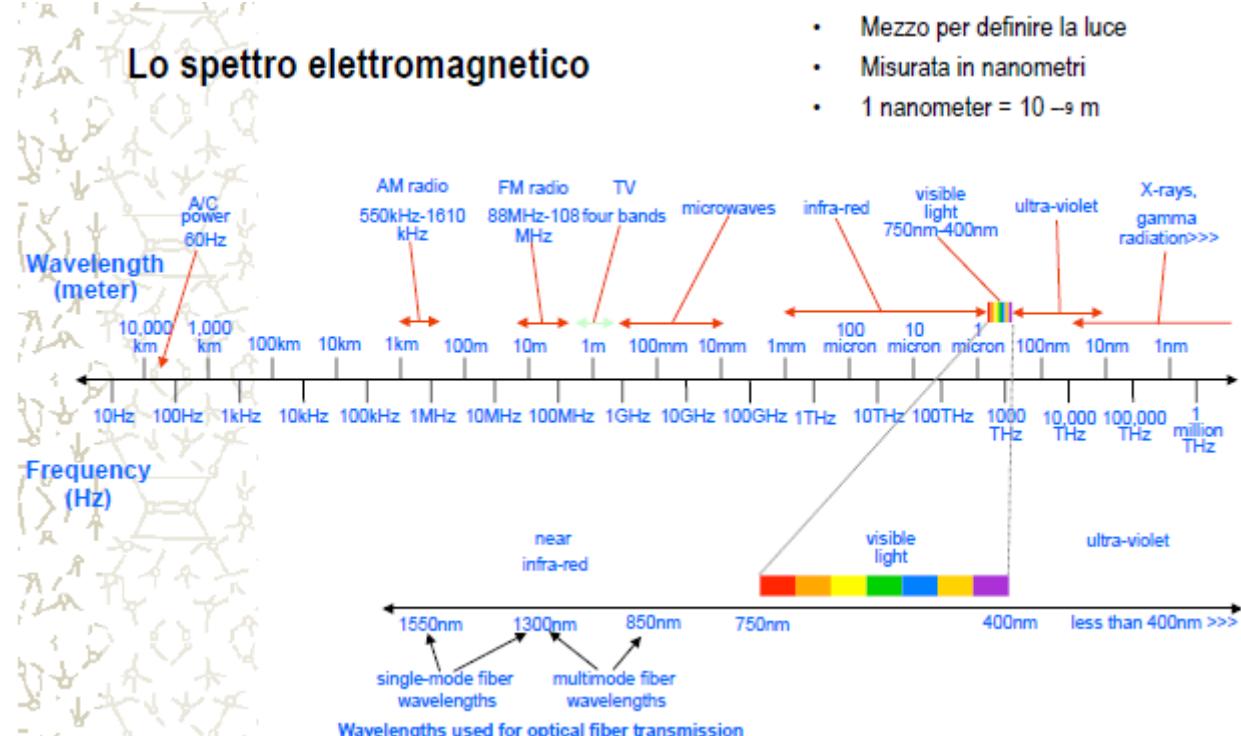


- **Fibre ottiche monomodali:** propagazione in un unico modo, la fibra si comporta come una guida d'onda quindi con una sola modalità di propagazione. Non si ha dispersione modale, anche se nella pratica un pò c'è. La banda passante è elevatissima. Possono lavorare in 2^a e 3^a finestra.





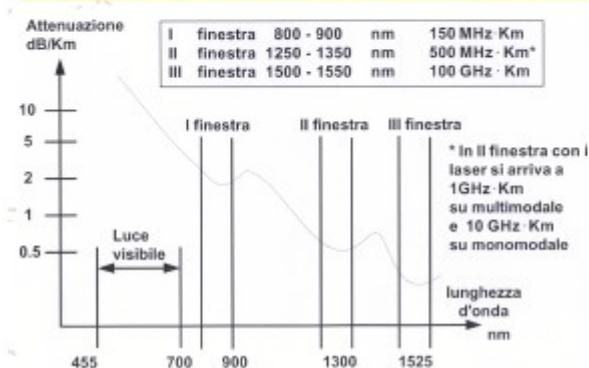
- Mezzo per definire la luce
- Misurata in nanometri
- 1 nanometer = 10^{-9} m



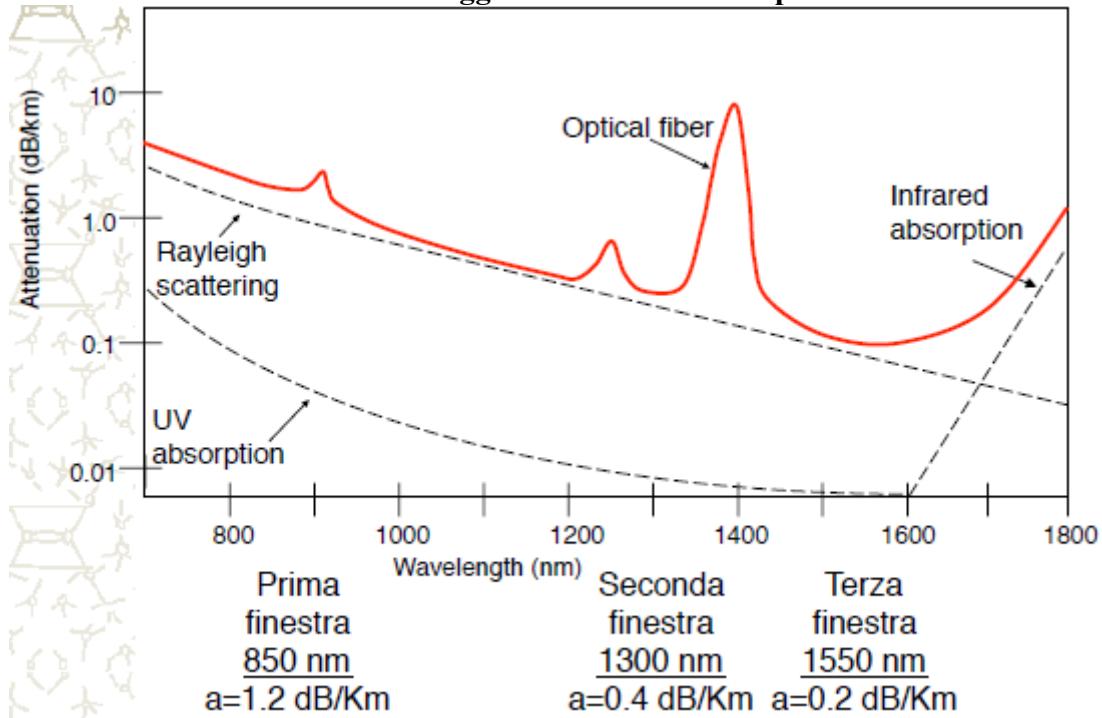
Lo spettro rappresenta un'insieme di frequenze che descrivono le caratteristiche del mezzo trasmittivo.

Window	Operation
800 - 900 nm	850 nm
1250 - 1350 nm	1300 / 1310 nm
1500 - 1600 nm	1550 nm

Una finestra è il range di lunghezza d'onda in cui la fibra funziona meglio. Sono centrate intorno alla lunghezza d'onda, studiandole possiamo notare che conviene scegliere quella con l'attenuazione minore.



ATTENUAZIONE: Parte dell'energia luminosa che si propaga lungo la fibra viene assorbita dal materiale o si diffonde in esso, costituendo quindi una perdita ai fini del segnale trasmesso. Il rapporto tra la potenza ottica trasmessa e quella ricevuta, dopo aver percorso una lunghezza di fibra di riferimento, definisce l'attenuazione della fibra stessa, in funzione della lunghezza d'onda e del tipo di fibra. **Minore è l'attenuazione maggiore la distanza utile per la trasmissione.**

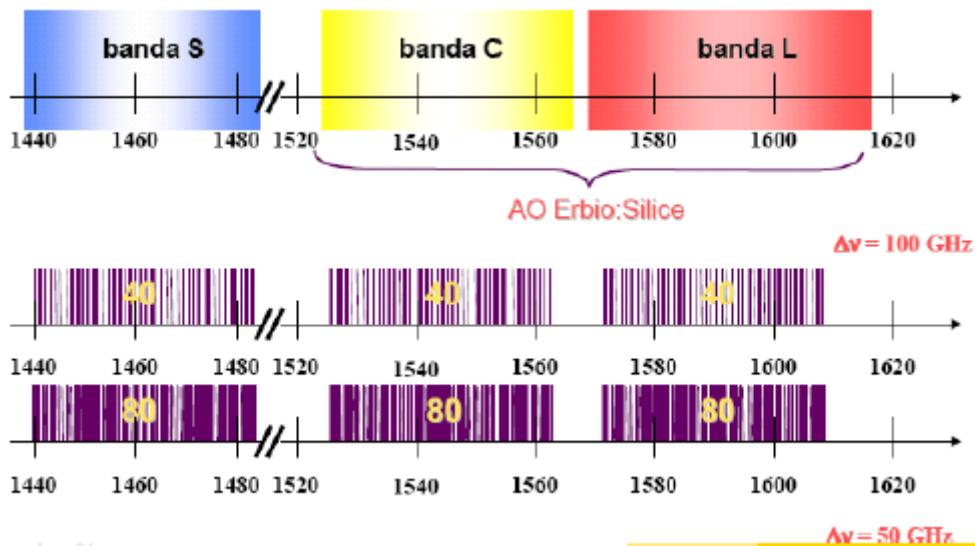


Dal grafico precedente possiamo notare che se trasmettiamo nella terza finestra l'attenuazione sarà minore e il segnale percorrerà più strada.

Le fibre ottiche sono utilizzate per scopi di telecomunicazioni per distanze superiori a qualche chilometro e velocità di trasmissione superiori ai 100 Mbit/s nelle bande attorno a:

- 1300 nm (II finestra)
- 1550 nm (III finestra, minimo assoluto dell'attenuazione)

La banda trmissiva nelle due finestre è circa 25000 Ghz.



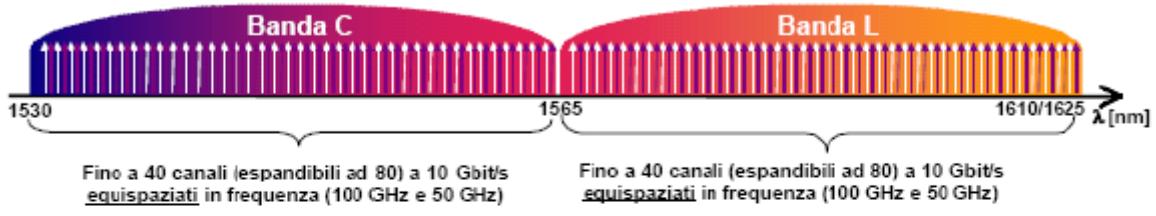
Le fibre più utilizzate sono:

- Fibra standard ITU-T G.652 (ottimizzata per l'uso in II finestra)
- Fibra standard ITU-T G.653 (Dispersion Shifted, ottimizzata per l'uso in III finestra)
- Fibra a dispersione non nulla ITU-T G.655 (ottimizzata per DWDM in III finestra)

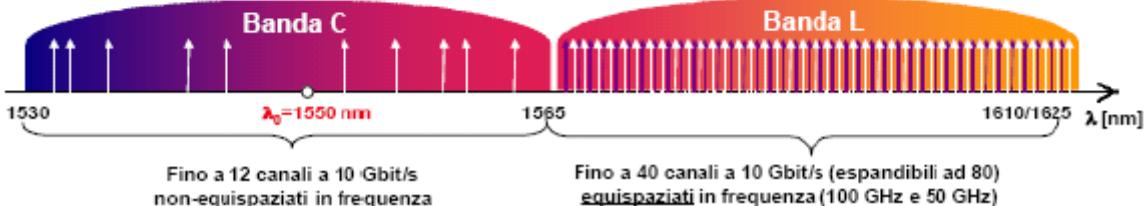
Nel caso di fibra G.652, i sistemi WDM Nx2.5-Gbit/s sono limitati dall'dispersione cromatica e di

polarizzazione mentre nel caso di fibra G.653, i sistemi WDM Nx2.5-Gbit/s sono limitati dal FWM.

Fibra G.652 / G.655

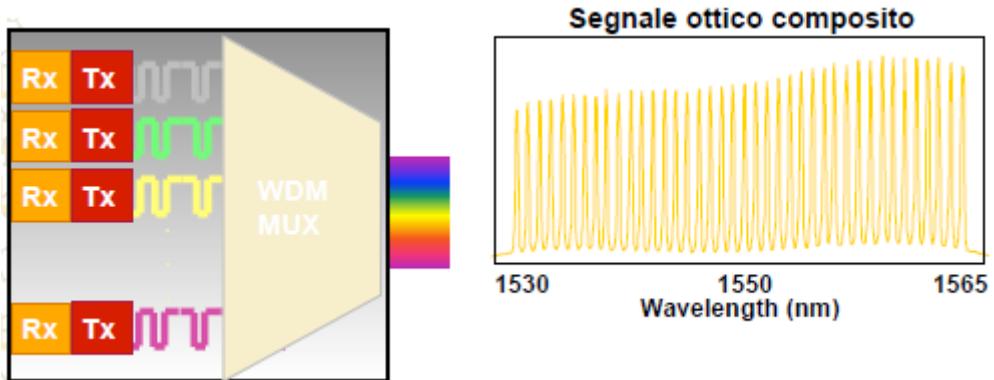


Fibra G.653

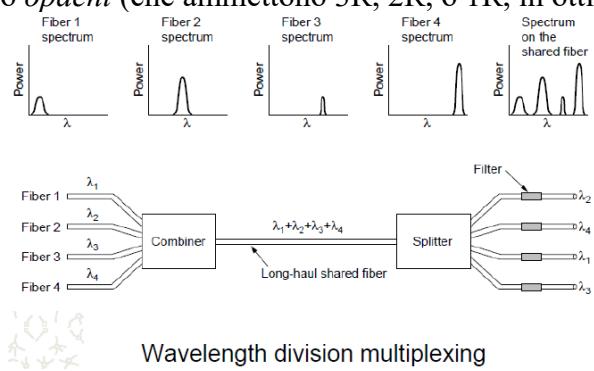


Come nella trasmissione via doppino, anche qui ci sono diversi mezzi per multiplcare il segnale:

- **Wavelength Division Multiplexing (WDM):** Consente di veicolare più lunghezze d'onda λ (oggi fino a 320) all'interno del medesimo portante fisico, ciascuna con capacità trasmittiva fino a 40 Gbps (OC768), dipendentemente dalla qualità della fibra e degli apparati *di trasmissione*. I segnali sono multiplexati nel dominio delle lunghezze d'onda. Ognuno di questo segnale viaggia su un colore, e non interferirà mai con gli altri. Su un singolo cavo riusciamo a trasmettere 320 canali.

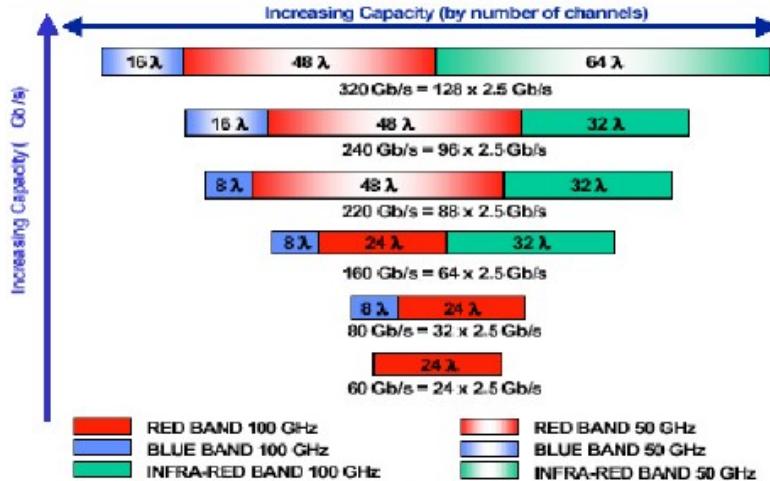


Le tecniche WDM sono più naturali nel dominio fotonico. La divisione della banda disponibile in canali è comunque necessaria in quanto il canale ottico, anche se attraversa solo punti di commutazione operanti nel dominio fotonico, è attestato nel dominio elettronico. Nel caso di puro WDM, è possibile offrire agli utenti canali trasparenti end-to-end, chiamati *lightpath*. Se le distanze coperte sono grandi, può essere necessario Rigenerare i segnali, operazione cui è sovente associata una Risincronizzazione e una Risagomatura (si parla di 3R) nel caso di segnali numerici. Possiamo avere lightpath *trasparenti* (tutto ottici) o *opachi* (che ammettono 3R, 2R, o 1R, in ottica o in elettronica).



La separazione fra bande ci permette di capire su che apparato siamo, i canali sono i seguenti:

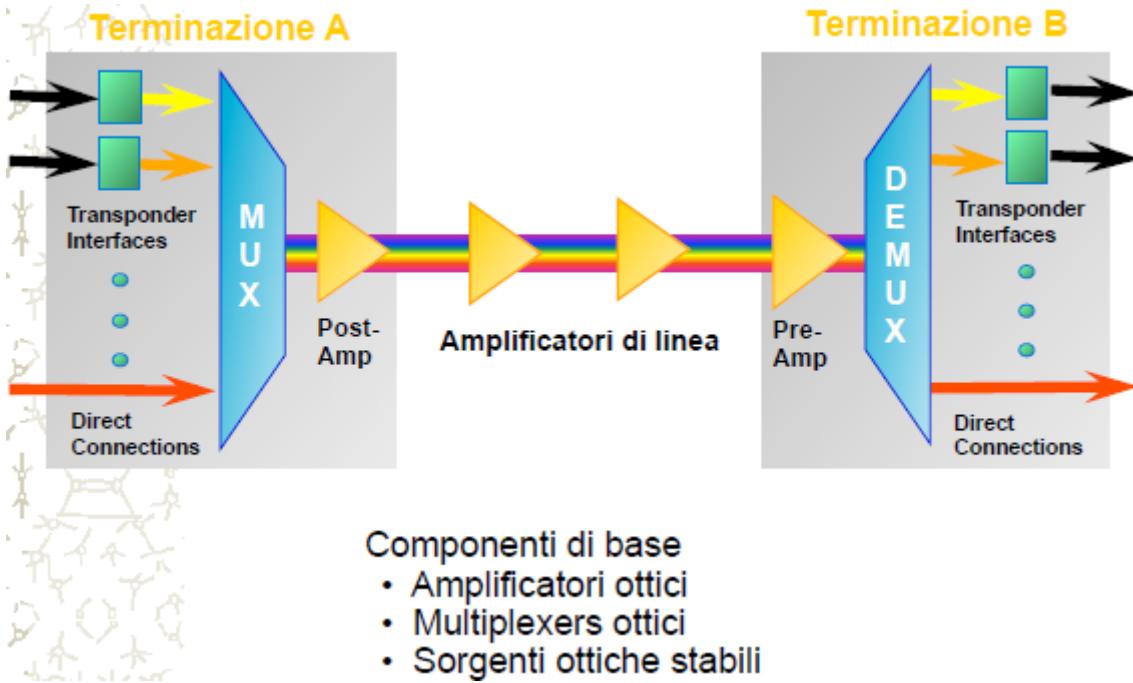
1. BLUE BAND: regione 1529-1536nm
 - (8 canali 100Ghz spaced/16 canali 50Ghz spaced multiplexabili)
2. RED BAND: regione 1542-1561nm
 - (24 canali 100Ghz spaced/48 canali 50Ghz spaced multiplexabili)
3. INFRARED BAND: regione 1575-1602nm
 - (32 canali 100Ghz spaced/64 canali 50Ghz spaced multiplexabili)



NOTA:

La lunghezza d'onda è una fibra virtuale ricavata su quella fisica, non è sottoposta a interferenza con le altre lunghezze d'onda. Ogni lunghezza è un canale e può trasportare fino a 100GHz, però nel momento dell'uso se non vengono usati tutti si ha uno spreco. Quindi applicando una OFDM possiamo ottenere una sottolunghezza d'onda, così che dedichiamo una minima parte soltanto ad un canale, e di fatto possiamo avere più canali su una sola lunghezza d'onda.

COMPONENTI DELL'ARCHITETTURA WDM

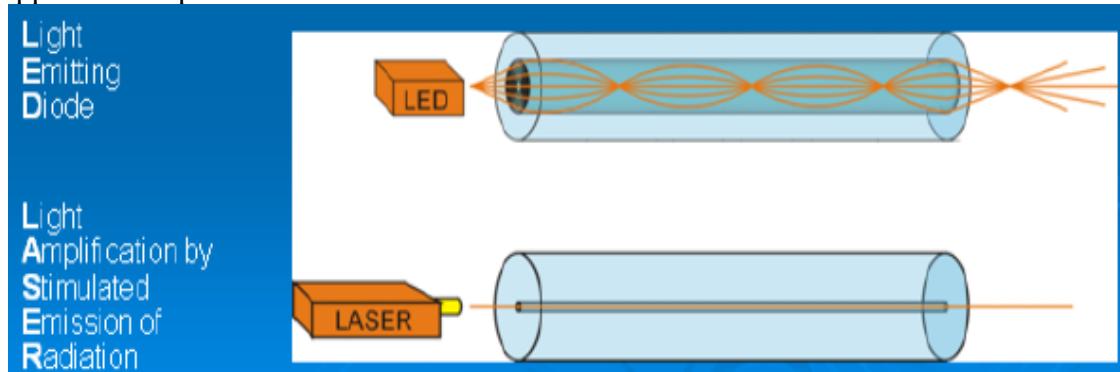


- Trasponder: prende un segnale e lo trasla su una lunghezza d'onda
- multiplexer: multiplica le lunghezze d'onda su un mezzo trasmittivo
- amplificatori: aumentano la potenza del segnale inserendo del rumore
- demultiplexer: decodifica le lunghezze d'onda e li manda ad un altro trasponder che lo ritrasforma in segnale.

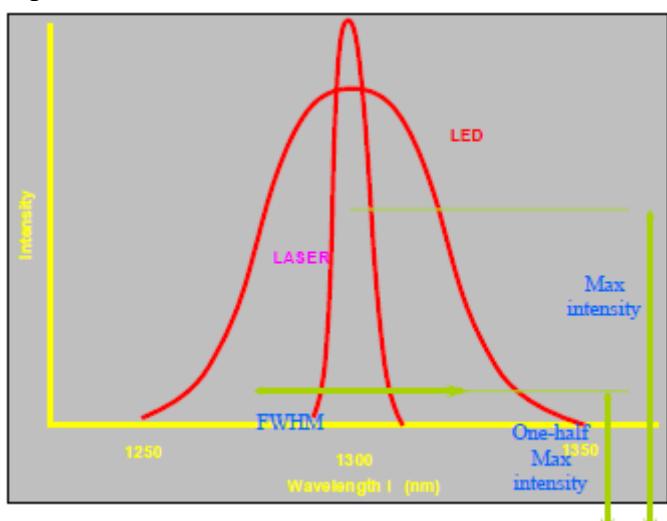
La trasmissione attraverso la fibra ottica può essere effettuata con due diverse modalità

- Con LED Light Emission Diode sulle fibre Multimodali, è poco preciso nel trasmettere.
- Con Laser (classe 2) sulle fibre Monomodali, è molto preciso a trasmettere.
- Con i VCSEL, (vertical cavity - surface emitting lasers) laser a semiconduttore che , hanno un sistema ottico non particolarmente complesso che permette l'emissione del fascio laser perpendicolarmente alle superfici di crescita dei semiconduttori, con ridotta difficoltà costruttiva, dimensioni inferiori necessità di potenze di alimentazione inferiori .

Le due diverse modalità di trasmissione hanno costi molto diversi e possono essere utilizzate per applicazioni specifiche anche a seconda della finestra di utilizzo.



La potenza totale emessa da un trasmittitore è distribuita su un range di lunghezze d'onda diffuse intorno al centro d'onda. Questo range e la larghezza di spettro, misurato in nanometri. La larghezza di spettro varia da stretta (alcuni nanometri) a larga (da decine a centinaia di nanometri) dipendente dal tipo di sorgente utilizzata (Laser o LED). Larghe ampiezze di spettro portano a incrementare la dispersione .



Una differenza importante nell'impiego di LED, VCSEL e LASER risiede anche nella maniera in cui queste sorgenti lanciano impulsi di luce nelle fibre. Un LED realizza una condizione di lancio detta “**Overfilled Launch**” (illumina completamente il nucleo di una fibra multimodale, con molti modi copre l'intero diametro di una MMF). I VCSEL sono più focalizzati dei LED nell'immettere potenza ottica nella fibra. Il diametro del fascio luminoso del LASER impiegato per gli apparati 1000BaseLX è ancor più ridotto.

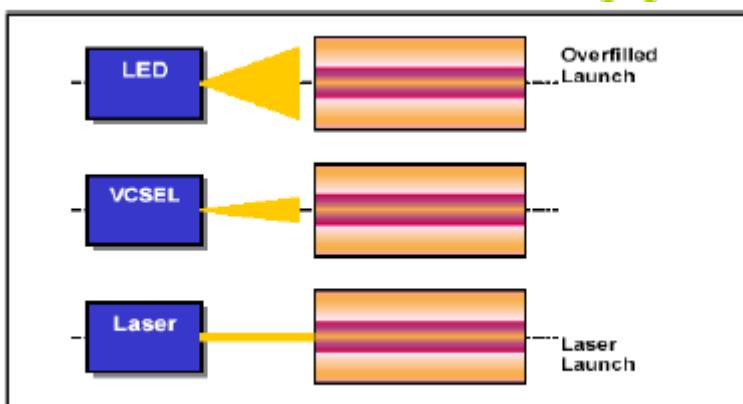


Figura 1: Differenti tipologie di lancio

NOTA: PARADOSSO DI TANEMBAUM

Il paradosso dice che non si deve sottovalutare la proprietà di trasmissione di una station wagon piena di dischi magnetici lanciata a grande velocità su di un'autostrada. Questa cosa era vera finché non sono nate le fibre ottiche.

Infatti consideriamo una singola fibra ottica:

- Allo stato dell'arte è possibile trasportare 320λ in una singola banda dello spettro (e.g. C-Band)
- Ogni λ può trasportare una capacità di 100 Gbit/s. La capacità totale è: $320 * 100 * 10^9 / 8 = 4000 \text{ GByte/sec}$

Invece consideriamo ora un camioncino tipico da 10 tonnellate di carico:

- Un singolo nastro che può immagazzinare 80 Gbyte, pesa circa 100 g (0.1 Kg)
- Il camioncino può trasportare $(10000 / 0.1) * 80 \text{ Gbyte} = 8 \text{ Pbyte}$
- **camion / fibra = 8 PByte / 4000 GByte/sec = 2000 s} \approx 0.55 h**

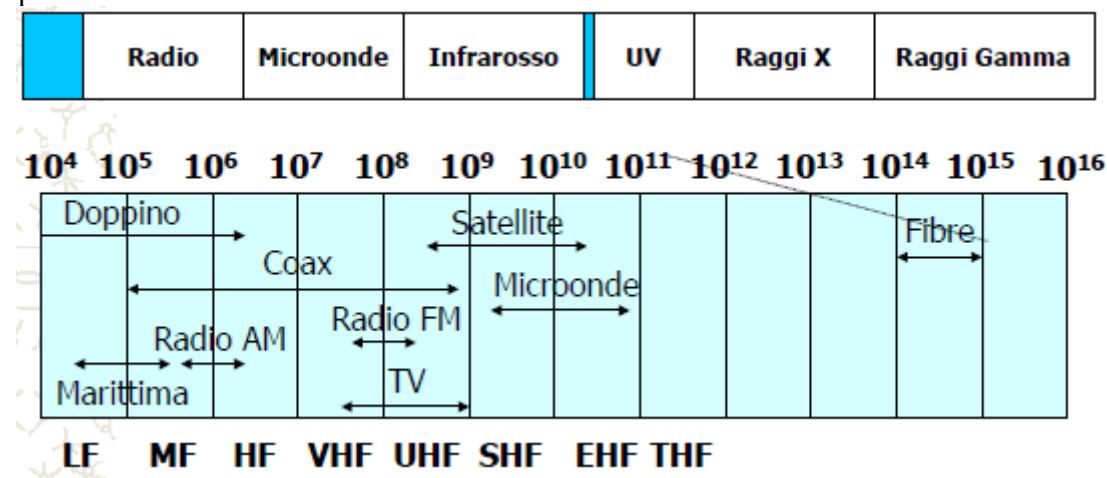
LA fibra **vince** per distanze più lunghe di quelle reggibili in 0.55 ore, cioè circa 50 km (senza considerare il tempo necessario per gestire 100000 tapes).

TRASMISSIONE WIRELESS

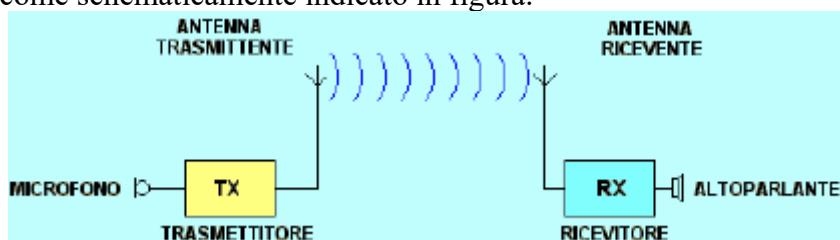
Si passa ora da un mezzo guidato ad uno non guidato, il segnale qui è fortemente vulnerabile. È interessato infatti da molti fenomeni come: interferenza, riflessione e interferenza dello stesso segnale nel momento in cui ritorna indietro. Questa tecnologie sono differenziate dalla sezione dello spettro elettromagnetico:

- Trasmissione Radio.
- Trasmissione Microwave.
- Trasmissione Infrarossi e Onde millimetriche.
- Trasmissione Lightwave.

L'aria è un buon mezzo di trasmissione, in particolare le onde radio sono facili da generare, possono viaggiare per lunghe distanze e penetrano facilmente negli edifici. Inoltre sono omnidirezionali, quindi il trasmettitore e il ricevitore non devono essere allineati.

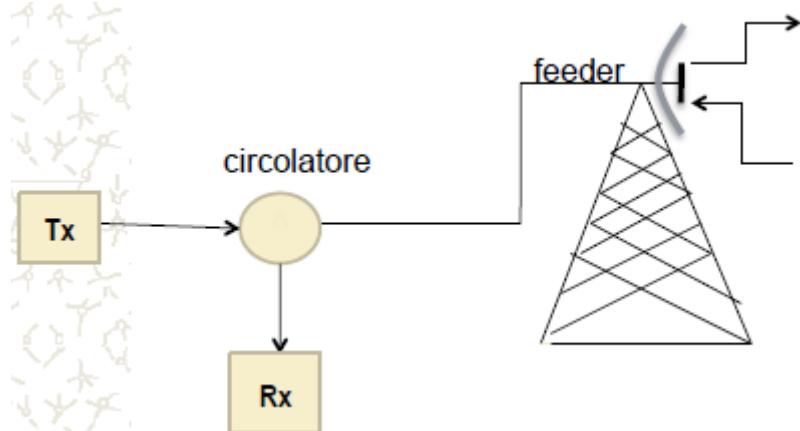


Ogni trasmissione radio via etere, utilizza due stazioni (trasmittente e ricevente) separate dall'etere come schematicamente indicato in figura.



I ruoli possono essere alternati. Il segnale viene irradiato tramite un'antenna, e ricevuto tramite un'altra antenna.

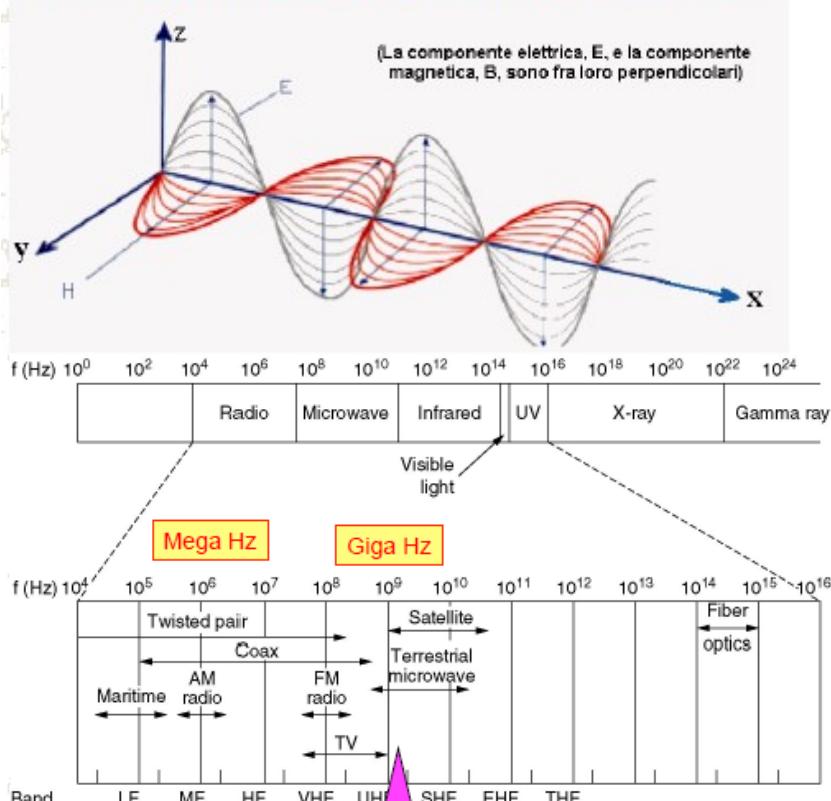
ANTENNA:



- L'elemento più importante è **l'elemento irradiante o ricevente**: è l'antenna vera e propria che realizza la trasduzione (trasmissione di energia da un punto a un altro di un sistema).
- **Feeder di antenna**: è il mezzo trasmissivo più utilizzato per collegare il trasmettitore o il ricevitore con l'antenna.
- **Dispositivi di diramazione o circolatore**: è utilizzato quando si vuole impiegare l'antenna sia per trasmettere che per ricevere; consente di separare la trasmissione dalla ricezione.

Per trasmettere con l'antenna si utilizzano anche le onde elettromagnetiche. Le onde elettromagnetiche, ipotizzate teoricamente da James Clerk Maxwell nel 1864, sperimentate in laboratorio da Hertz e utilizzate nella Radio da Marconi nel 1895, sono costituite da oscillazioni, del campo elettrico e del campo magnetico, che si propagano nel vuoto alla velocità di circa: $c = 300.000 \text{ Km/sec}$.

Rappresentazione schematica di un campo elettromagnetico che si propaga lungo la direzione "x"



Se proviamo a trasmettere nella zona visibile, possiamo trasmettere in Lightwave con un laser che arriva ad un fotorilevatore, e avere una trasmissione simile alla fibra.

A frequenze f basse si possono veicolare pochi bit/Hz, ma a frequenze più alte si può arrivare fino a 40 bit/Hz, infatti riducendo la frequenza diminuisce la velocità di trasmissione. Abbiamo quindi:

$$f = \frac{c}{\lambda} , \text{ visto che la frequenza e la lunghezza d'onda sono uguali abbiamo anche che } \lambda = \frac{c}{f}$$

dove $c = \text{velocità della luce}$, $\lambda = \text{lunghezza d'onda}$ e $f = \text{frequenza}$.

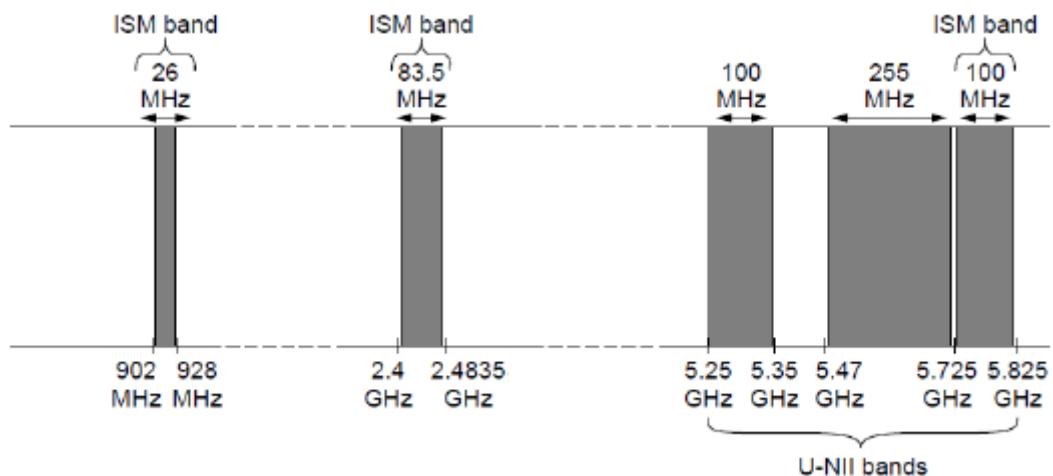
Differenziando rispetto alla lunghezza d'onda lambda, si ha:

$$\frac{(df)}{(d\lambda)} = \frac{c}{\lambda^2} \text{ quindi } \Delta f = \frac{(c \Delta \lambda)}{\lambda^2} , \text{ per la fibra in seconda finestra abbiamo quindi che:}$$

$$\lambda = 1,3 \cdot 10^{-6} \quad \Delta \lambda = 1,7 \cdot 10^{-7} \quad f \approx 30 \text{ THz} .$$

ASSEGNAZIONE DELLE FREQUENZE

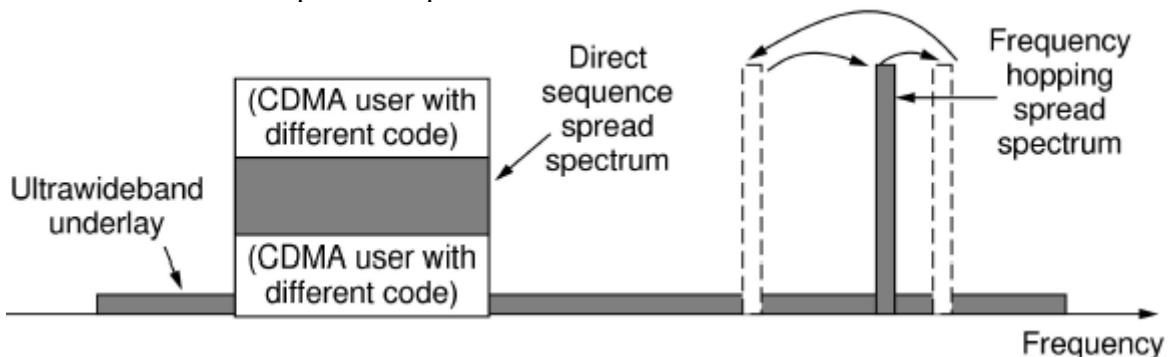
Le frequenze sono una risorsa. Enti nazionali / internazionali provvedono ad assegnare le frequenze (ITU, FCC); in Italia è competenza del ministero PP TT. La polizia postale è preposta al controllo del rispetto delle bande assegnate. Per il wi-fi non vale, oppure per sezioni non regolamentate dello spettro, ma questo implica che se vogliamo trasmettere in queste frequenze la qualità della trasmissione non sarà sempre ottima. Esistono altre bande non licenziate come le ISM che sono assegnate ad utilizzo industriale-scientifico-medico, ed appunto non richiedono licenza, ma come prima trasmettere qui comporta molti rischi, come il fatto che sulla stessa frequenza possono trasmettere più persone creando interferenza.



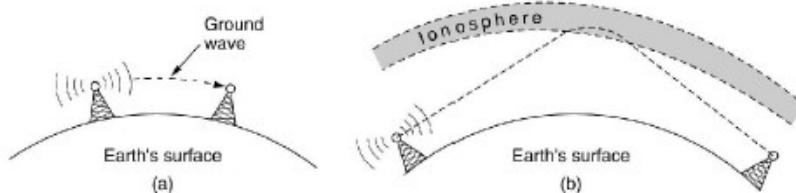
TIPOLOGIE DI TRASMISSIONE RADIO

Per trasmettere le frequenze via onde radio esistono molti modi, di seguito saranno elencati alcuni:

- **Direct Sequence Spread Spectrum (DSSS):** tecnologia di trasmissione a "frequenza diretta" a banda larga, nella quale ogni bit viene trasmesso come una sequenza ridondante di valori (chip). Indicato per la trasmissione e la ricezione di segnali deboli. Consente l'interoperabilità delle reti wireless attuali. Per codificare il segnale si usa la multiplazione CDMA.
- **Spettro diffuso (Spread Spectrum):** il trasmettitore opera continui "salti" di frequenza (*frequency hopping*). Origine militare, difficile da individuare e disturbare. Per interpretare l'informazione devo sapere la sequenza esatta di salti fra canali.



- **La radiodiffusione:** viene utilizzata generalmente per la trasmissione analogica di segnali radio-televisivi in modalità broadcast. Utilizza due tecniche trasmissive differenti in funzione della regione di frequenze:
 1. nella regione fino al MHz (VLF, LF ed MF) il segnale si propaga seguendo la curvatura terrestre ed attraversa bene gli ostacoli: una stazione trasmittente può essere ricevuta fino a 1000 Km di distanza; oltre l'attenuazione (proporzionale all'inverso del quadrato della distanza) diviene eccessiva.
 2. nella regione dal MHz al GHz (HF, VHF e UHF) il segnale viene assorbito dalla superficie della terra, ma viene riflesso molto bene dalla ionosfera; i segnali vengono quindi inviati verso il cielo raggiungono la stazione ricevente dopo la riflessione.



- **Trasmissione via ponte radio:** La banda di frequenza delle microonde (1-40 GHz) ha le caratteristiche di poter utilizzare antenne paraboliche di dimensioni maneggevoli (fino a qualche metro di diametro) per poter collimare e dare direzione all'emissione. Si può quindi realizzare una comunicazione punto-punto tra sorgente e destinazione con allineamento ottico delle antenne: la trasmissione è rettilinea, ed è indispensabile la visibilità tra le antenne delle stazioni comunicanti. Questa tecnica di trasmissione va in competizione con le linee in coassiale e via fibra ottica:
 1. per le lunghe distanze, quando l'alternativa con mezzo guidato risulta troppo costosa o impossibile per motivi morfologici.
 2. per le brevi distanze (ad esempio per connettere due palazzi vicini di una stessa compagnia) come alternativa alla stesura di una fibra qualora si dovesse attraversare suolo pubblico o di altra proprietà, per evitare le complicazioni connesse alle autorizzazioni.

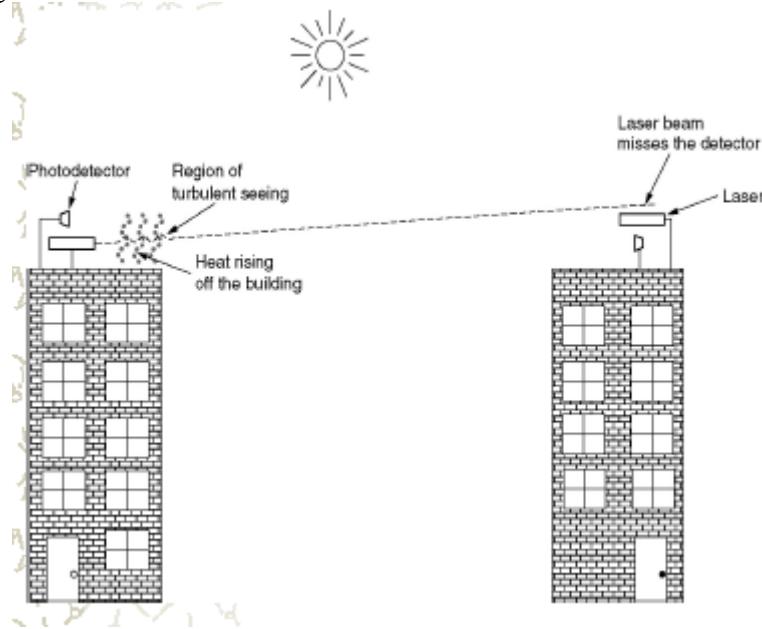
Utilizzando diverse stazioni ripetitrici si riescono a coprire distanze elevate (svariate centinaia di Km); una singola tratta può coprire in condizioni favorevoli fino a qualche centinaia di Km. Data la dipendenza dell'attenuazione dalla distanza, per le tratte lunghe si utilizzano generalmente due bande di frequenza: 2-6 GHz e 10-14 GHz.

Le connessioni a breve distanza possono utilizzare le frequenze più alte (fino a 40 GHz) per le quali si hanno i vantaggi:

1. antenne più piccole
2. fascio più collimato (quindi minore necessità di potenza)
3. minori problemi di interferenza per lo scarso utilizzo di trasmissioni in quella regione di frequenza.

- **Utilizzo dei ponti radio:** Generalmente utilizzati per trasmissioni analogiche (fonia, televisione) o digitali (per reti private o utilizzate dalle compagnie telefoniche fornitori di servizi). Le diverse bande di frequenza sono suddivise in canali di diversa larghezza (non uniformi nei diversi paesi), con canali tra i 7 MHz (a 2 GHz) ed i 220 MHz (a 18 GHz), e tassi trasmissivi che vanno dai 12 ai 274 Mbps (in funzione della banda disponibile e del livello di modulazione utilizzato, solitamente QAM-x).
- **Trasmissione Radio – microonde:** Sopra i 100 Mhz ($\lambda < 3 \text{ m}$) le onde tendono a propagarsi in linea retta. Usando antenne direzionali ad alto guadagno (paraboliche) si migliora il rapporto S/N. È però necessario l'allineamento. Curvatura della terra È Necessità di ripetitori per tratte lunghe. Multipath da rifrazione in atmosfera (dipendente da tempo e frequenza). Oltre 8 GHz si ha assorbimento da parte dell'acqua. Richiede infrastrutture più "leggere" della fibra ottica.

- **Trasmissione Radio – infrarossi:** Utili per comunicazioni a piccola distanza (telecomandi). Non attraversano oggetti (confinamento O non interferenza). Più sicure delle onde radio, non richiedono licenza. Proposte per LAN interne con infrastruttura fissa (beacon). Non utilizzabili in esterno per la presenza di emissioni solari. IRDA (115 Kbps) IRDA 2 (4 Mbps). Un problema delle trasmissioni infrarossi è appunto il fatto che la luce solare li annulla completamente.
- **Lightwave transmission:** Grande larghezza di banda, non richiede licenza. Necessita di grande precisione nel puntamento, pur utilizzando lenti per avere una leggera sfuocatura del raggio. Attenuazione da precipitazioni atmosferiche. Disturbi da turbolenze nell'aria dovuti a convezione. Questo tipo di trasmissione non è soggetta a interferenze radio, ma è molto soggetta a interferenze ambientali.



TRASMISSIONI SATELLITARI

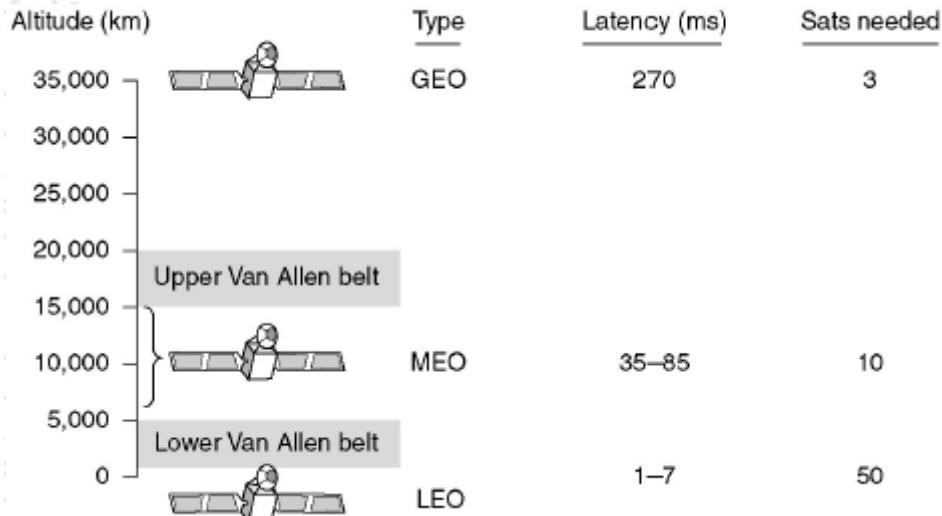
Il satellite si comporta come una stazione ripetitrice del segnale di un ponte radio. Il segnale viene inviato dalla stazione terrestre al satellite (uplink), che lo rimanda a terra verso la stazione o le stazioni riceventi (downlink), generalmente utilizzando frequenze differenti. Un satellite opera su più bandi di frequenza, con la tecnologia FDM; i singoli canali si chiamano **transponder** (canali tra 15 e 500 MHz di banda) e sono dei ricetrasmettitori satellitari. Ognuno ascolta una parte dello spettro, amplifica il segnale in ingresso e lo ritrasmette su un'altra frequenza per evitare interferenze con il segnale in arrivo. I raggi puntati verso il basso possono essere larghi e coprire una considerevole frazione della superficie terrestre, oppure stretti e coprire un'area dal diametro di poche centinaia di chilometri. Questa modalità operativa è chiamata **bent pipe**. Sui canali il satellite può fare TDM per gestire diverse comunicazioni. Le bande utilizzate sono quelle tra 1 e 10 Ghz:

- sopra l'attenuazione atmosferica è troppo grande
- sotto ci sono interferenze ed assorbimento dalla ionosfera

Il sovrappiombo delle frequenze spinge attualmente verso l'utilizzo di bande a frequenza superiore, nonostante che i problemi di attenuazione atmosferica divengano sempre più importanti. Abbiamo tre tipi di satelliti:

- **GEO(Geostationary Earth Orbit):** satelliti a 36000 Km di quota in orbita equatoriale, che appaiono in posizione fissa nel cielo, questi satelliti sono adatti alla trasmissione dati in quanto il puntamento delle antenne è fisso, per motivi di interferenza i satelliti vengono distanziati di due gradi, quindi si possono avere al massimo 180 satelliti. La trasmissione dati deve tenere conto del ritardo di propagazione del segnale, che è pari a 0.25 secondi (inefficienti i protocolli con controllo degli errori **ertrasmissione dei pacchetti**).

- **MEO (Medium Earth Orbit):** satelliti a 18000 Km di quota, con 6 ore di periodo dell'orbita, sono inadatti per la trasmissione dati. Esempio: i satelliti del GPS (Global Positioning System).
- **LEO (Low Earth Orbit):** tra 750 e 1500 Km di quota sono molto veloci nel transito, ma vicini, quindi si ha poco ritardo e si richiede poca potenza in trasmissione. Esempi: Iridium (per fonia, fax, dati, navigazione), Globalstar.



Le caratteristiche operative includono l'altitudine a partire a terra, il round-trip delay time e il numero di satelliti necessari a una copertura globale.

Le principali bande satellitari sono:

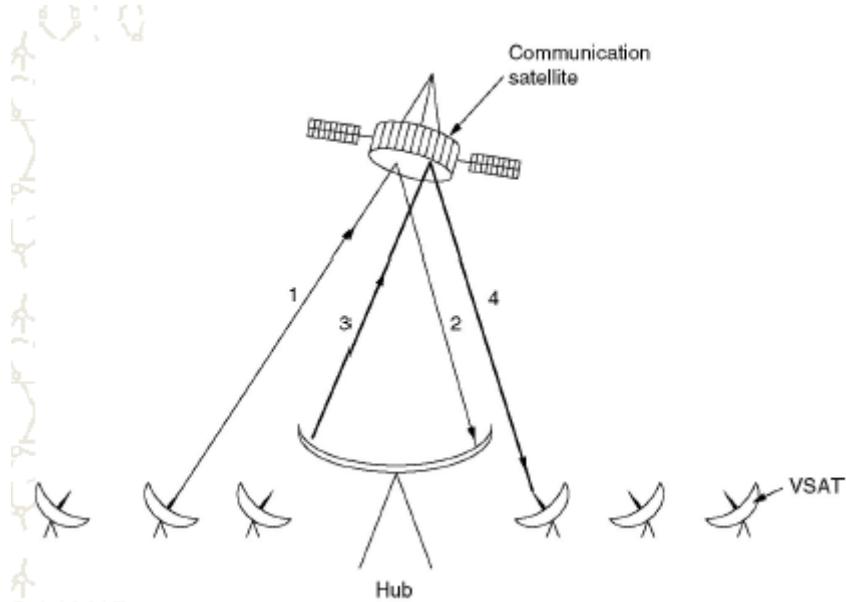
Band	Downlink	Uplink	Bandwidth	Problems
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial interference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain, equipment cost

Le bande L ed S sono state aggiunte nel 2000 in base ad accordi internazionali, ma sono strette e affollate. La prossima banda a disposizione delle società di telecomunicazioni commerciali è la banda Ku (*K under*). Questa banda non è ancora congestionata e a queste frequenze i satelliti possono essere collocati a solo un grado angolare di distanza l'uno dall'altro; purtroppo esiste un altro problema: la pioggia. L'acqua assorbe in modo eccellente queste microonde corte. Le ampiezze di banda sono state assegnate al traffico commerciale anche nella banda Ka (*K above*), ma l'attrezzatura necessaria è ancora costosa. Oltre a queste bande commerciali, esistono molte bande governative e militari.

VSAT

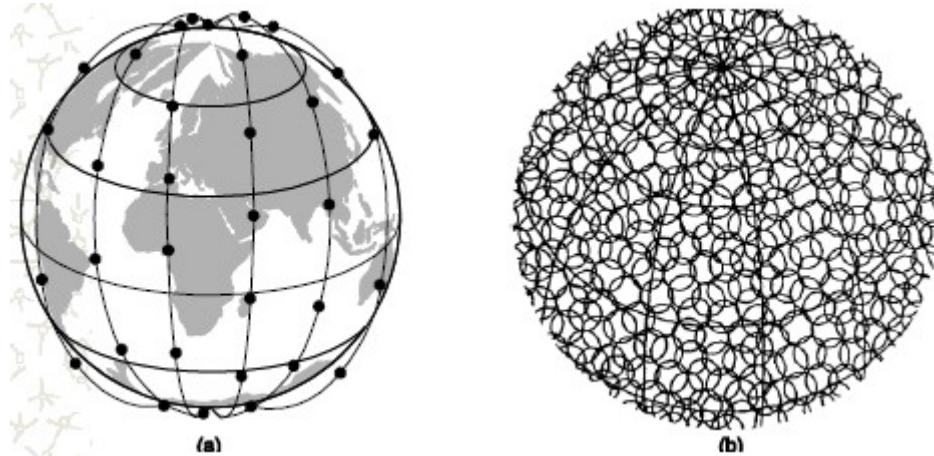
Un nuovo sviluppo nel settore delle comunicazione satellitari è rappresentato dalle microstazioni a basso costo chiamate anche VSAT (*Very Small Aperture Terminal*) (Abramson, 2000). Questi terminali leggeri hanno antenne grandi un metro o anche meno (le antenne GEO sono grandi dieci metri) e possono generare circa 1 watt di potenza. La trasmissione uplink (verso il satellite) di solito arriva a 19,2 kbps, ma la velocità in downlink (verso terra) può anche superare i 512 kbps. Le televisioni satellitari utilizzano questa tecnologia per le loro trasmissioni unidirezionali. In molti sistemi VSAT le microstazioni non hanno abbastanza energia per comunicare direttamente le une con le altre (via satellite, logicamente), per questo motivo è necessario installare speciali stazioni

terrestri, chiamate hub, dotate di grosse antenne ad alto guadagno che trasmettono il traffico attraverso le stazioni VSAT.



SATELLITI LOW-EARTH ORBIT (IRIDIUM)

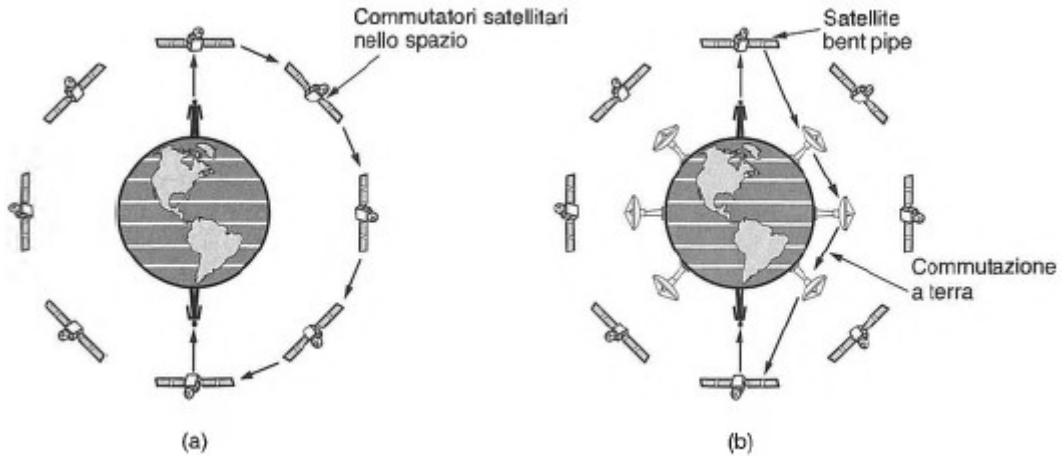
Nel 1990 Motorola aprì un nuovo orizzonte presentando una domanda all’FCC che chiedeva il permesso di lanciare su orbite basse i 77 satelliti del progetto Iridium. L’idea era che non appena un satellite spariva dalla vista, un altro sarebbe apparso all’orizzonte. Questa proposta fece esplodere una frenesia crescente tra le altre società di telecomunicazioni; in meno che non si dica tutti volevano lanciare la loro catena di satelliti su orbite basse. I satelliti Iridium vennero lanciati nel 1997. In un primo momento il progetto Iridium fallì, ma nel marzo del 2001 venne riavviato. Il progetto Iridium fornisce un servizio di telecomunicazione a livello mondiale basato su dispositivi tascabili in grado di comunicare direttamente con i satelliti Iridium. Questo servizio permette di trasmettere voce, dati, fax e informazioni di navigazione ovunque: sulla superficie del pianeta, in mare e in aria. I satelliti Iridium si trovano a un’altitudine di 750 Km, in orbite polari circolari; sono sistemati in catene che vanno da nord a sud, con un satellite ogni 32 gradi di latitudine. Con sei catene di satelliti è possibile coprire l’intero pianeta. Questa disposizione ricorda un po’ quella di un atomo di disporio: la Terra funge da nucleo e i satelliti le orbitano intorno come gli elettroni. Una proprietà interessante di Iridium è che la comunicazione tra clienti distanti avviene nello spazio, dove ogni satellite trasmette i dati al successivo.



SATELLITI LOW-EARTH (GLOBALSTAR)

Globalstar, un progetto alternativo a Iridium, si basa su 48 satelliti LEO e utilizza un diverso schema di commutazione. Globalstar invece utilizza un modello tradizionale bent pipe. La chiamata che ha origine al Polo Nord viene ritrasmessa sulla terra, è raccolta da una grande stazione

terrestre e dirottata attraverso una rete terrestre alla stazione più vicina al destinatario. Questo schema ha il grande vantaggio di tenere la complessità sulla terra, dove è più facile da gestire. Inoltre le grandi antenne delle basi terrestri, capaci di trasmettere segnali potenti e di ricevere segnali deboli, consentono di adoperare telefoni di bassa potenza. Dopo tutto, il telefono trasmette solo pochi milliwatt di energia, perciò il segnale che arriva alla stazione terrestre è abbastanza debole anche se è stato amplificato dal satellite. Il problema di questa connessione è appunto il fatto che il segnale andando prima sulla terra deve percorrere molta strada. Se si utilizzasse il ***relayng in space***, in cui ogni segnale è trasmesso da un satellite ad un altro finché non arriva a destinazione, senza compiere discese inutili sul suolo terrestre.



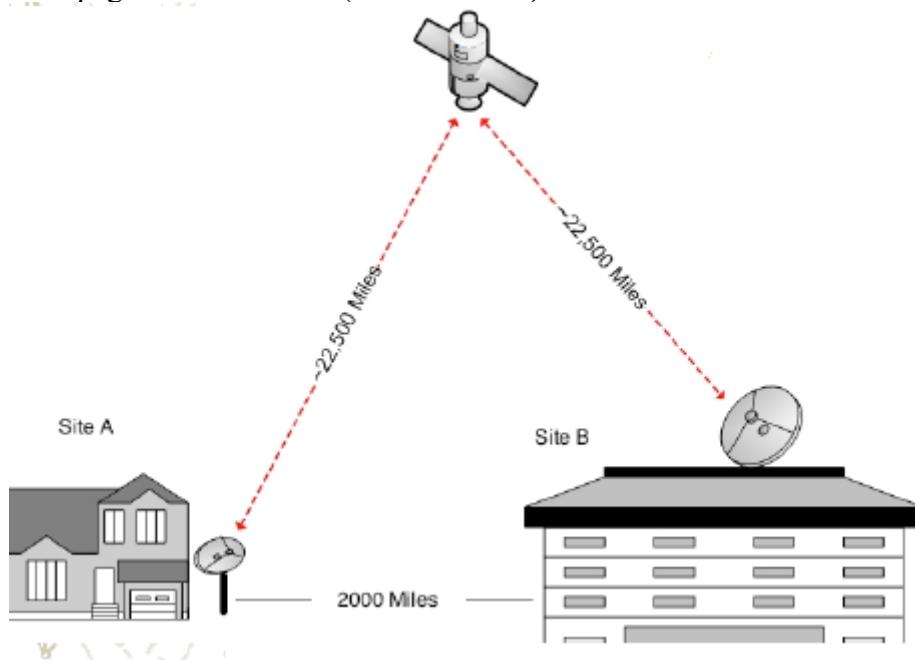
SATELLITI CONTRO FIBRA

La fibra alla fine dei conti è sempre migliore di una conessione satellitare perché quest'ultima per inviare un informazione deve compiere due volte la distanza che deve percorrere. Infatti abbiamo :

- Fibra - distanza: ≈ 3200 Km \rightarrow Latenza: 10ms.
- Satellite - distanza: ≈ 71000 Km \rightarrow Latenza: 236ms.

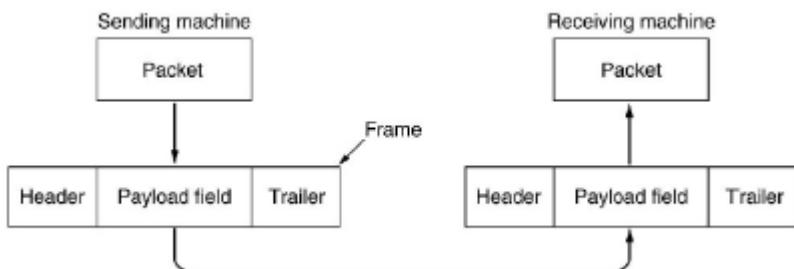
Quindi :

- Velocità fibra: $\approx 97\% c$
- Propagazione onde: $\approx c (3.00 \times 10^8 \text{ m/s})$



IL LIVELLO DATA LINK

È il primo livello che prende un servizio dal livello fisico e da un servizio al livello di rete. Il Data Link Layer (anche livello di collegamento dati, o più semplicemente: livello 2) ha la funzione principale di fornire allo strato di rete servizi per il recapito di dati al nodo direttamente adiacente sulla rete. Il compito del data link layer è quindi quello di organizzare il trasferimento dei dati tra due apparati adiacenti, e di fornire una interfaccia definita per consentire allo strato di rete di accedere ai servizi offerti. Apparati adiacenti significa logicamente connessi da un “canale” che trasmette i bit da una parte e li riceve dall’altra, nell’ordine di trasmissione. Il data link layer utilizzerà i servizi dello strato fisico per il recapito dei dati al suo processo paritario sul calcolatore ricevente, ma logicamente la comunicazione avverrà direttamente con il processo di data link layer remoto come sia fatto il “canale” non è argomento che riguardi il data link layer, ma lo strato fisico: non importa se ci sia un cavo, una fibra, una sequenza di mezzi differenti con interposti ripetitori, convertitori elettrico/ottici, modem, multiplexer, antenne o altro. Per realizzare le sue funzioni il data link layer riceve i dati dallo strato di rete (pacchetti), li organizza in trame (frame), unità trasmessa dal data link; eventualmente spezzando in più frame il blocco di dati ricevuto dal livello 3, aggiunge ad ogni frame una intestazione ed una coda (header e trailer), e passa il tutto allo strato fisico per la trasmissione. In ricezione il data link layer riceve i dati dallo strato fisico, effettua i controlli necessari, elimina header e trailer, ricombina i frame e passa i dati ricevuti allo strato di rete. Il segnale analogico a questo punto non esiste più.



SERVIZI DEL DATA LINK

Normalmente la progettazione dello strato 2 fornisce allo strato di rete i servizi:

- **trasmissione dati senza riscontro e senza connessione** (unacknowledged senza connessione): La classe di servizio non affidabile senza connessione è adatta su linee di elevata qualità. Il controllo sugli errori e la ritrasmissione di frame errati comporta un’inefficienza in termini di numero di bit trasmessi rispetto ai dati, con riduzione del tasso utile ed aumento della probabilità di errore. Il controllo può essere demandato ai livelli superiori a vantaggio della efficienza del livello di data link. Generalmente questi servizi sono utilizzati su rete locale, traffico voce e video.
- **trasmissione dati affidabile senza connessione** (acknowledged senza connessione): Questo genere di servizio continua a non usare nessun tipo di connessione logica, però ciascun frame è inviato individualmente e ne viene fatto l’acknowledge (conferma della ricezione). In questo modo il mittente riesce a sapere se un frame è arrivato a destinazione in modo corretto oppure no. Se non è arrivato entro uno specifico intervallo di tempo, il frame può essere rispedito. Si tratta di un servizio utile per i canali di trasmissione non affidabili, come per esempio le reti wireless.
- **trasmissione affidabile con connessione** (acknowledged orientato alla connessione): è adatta su linee più frequentemente soggette ad errori:
 1. demanda il controllo e la ritrasmissione ai livelli superiori (che generalmente trasmettono pacchetti costituiti da più frame) in caso di elevata probabilità di errore potrebbe causare la ritrasmissione di molti pacchetti, mentre al livello due può essere sufficiente la ritrasmissione del singolo frame).
 2. Implementa meccanismi di riscontro per verificare la necessità di ritrasmissioni
 3. tipicamente utilizzata su linee a grande distanza (connessioni WAN), anche se la fibra ottica riduce notevolmente questo problema

Il data link layer deve quindi poter offrire le diverse classi di servizio, per soddisfare le diverse esigenze conseguenti alle diverse circostanze.

NOTA:

ACK, in ambito telecomunicazionario e informatico, è il simbolo che identifica un segnale di Acknowledge emesso in risposta alla ricezione di un'informazione completa.

Un tipico esempio è il pacchetto di controllo previsto dal protocollo TCP trasmesso dal ricevente al mittente per segnalare la corretta ricezione di un pacchetto dati. L'ACK può anche essere di tipo cumulativo (quello usato dal TCP), indicando cioè l'avvenuta corretta ricezione di più pacchetti di dati.

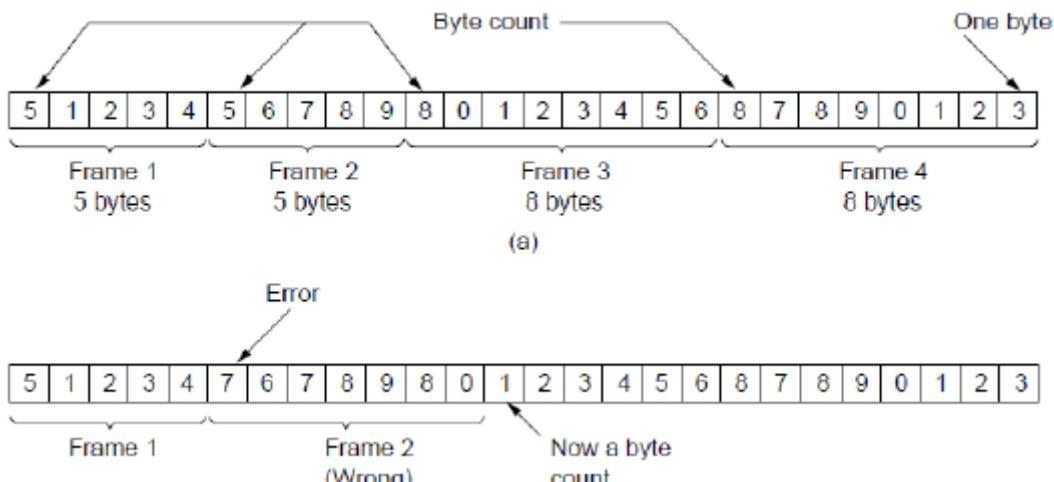
Per poter svolgere le sue funzioni il data link layer dovrà curare i seguenti aspetti:

- l'organizzazione del flusso di bit in frame, con controllo per la sincronizzazione, inserimento e rimozione di header e trailer, riordinamento dei frame in ricezione.
- Organizzare il trasferimento dei dati in modo da gestire eventuali errori di trasmissione, utilizzando codici di correzione degli errori o codici di identificazione degli errori e gestendo la ritrasmissione dei frame errati.
- Realizzare il controllo di flusso, per utilizzare in modo efficiente il canale trasmissivo impedendo al contempo ad un trasmettitore veloce di sovraccaricare un ricevitore lento.

Per trasportare i bit il Data Link Layer utilizza i servizi dello strato fisico, detto **framing**. Lo strato fisico non può garantire il trasferimento privo di errori, che dovranno essere gestiti dal DLL. Per fare ciò il DLL organizza i bit in frame, ed effettua i controlli per ogni frame. La gestione del frame deve prevedere in primo luogo la possibilità del ricevente di identificare il frame, quindi si devono adottare regole per delimitarlo e poterne identificare i limiti in ricezione.

Esistono diverse tecniche:

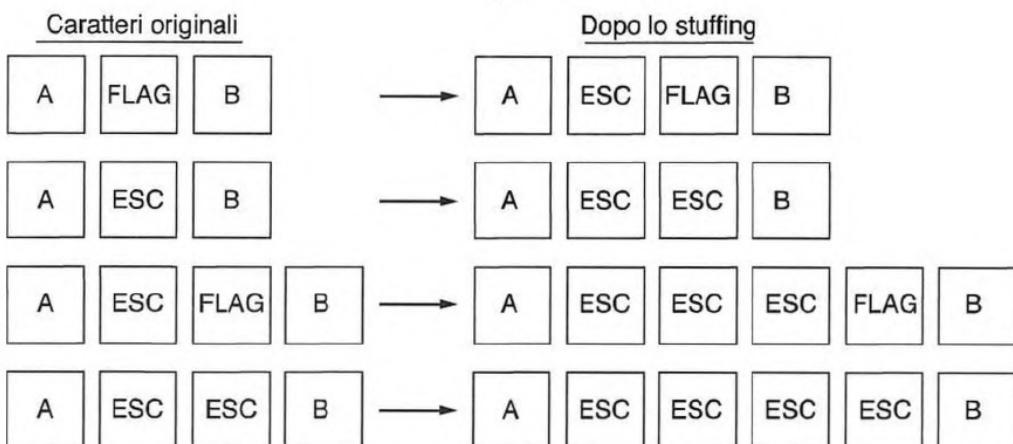
- **conteggio dei caratteri:** Un campo dell'intestazione indica il numero di caratteri nel pacchetto. Se si perde il sincronismo non si riesce a trovare l'inizio di un pacchetto successivo.



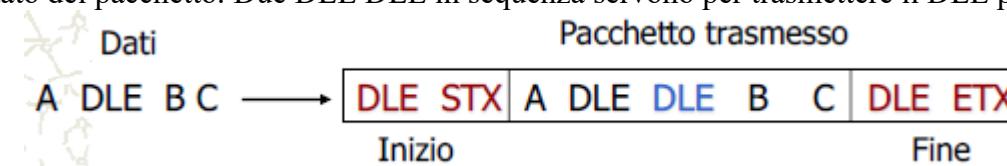
- **byte di flag, e byte stuffing:** aggira il problema della nuova sincronizzazione, necessaria a seguito di un errore, introducendo un byte speciale all'inizio e al termine di ogni frame. Nel passato i byte di inizio e fine erano differenti, mentre oggi la maggior parte dei protocolli usa lo stesso byte, chiamato flag byte, per delimitare sia l'inizio sia la fine dei frame, con FLAG. In questo modo, quando il destinatario perde la sincronizzazione, può semplicemente cercare il flag byte per trovare la fine del frame corrente. Due flag byte consecutivi indicano la fine di un frame e l'inizio del successivo. Questo metodo presenta un problema molto serio quanto vengono trasferiti dati binari, per esempio eseguibili o numeri in virgola mobile. In questo caso può facilmente accadere che il valore corrispondente al flag byte compaia naturalmente dentro ai dati, interferendo così con le operazioni di framing.

FLAG	Intestazione	Carico utile	Coda	FLAG
------	--------------	--------------	------	------

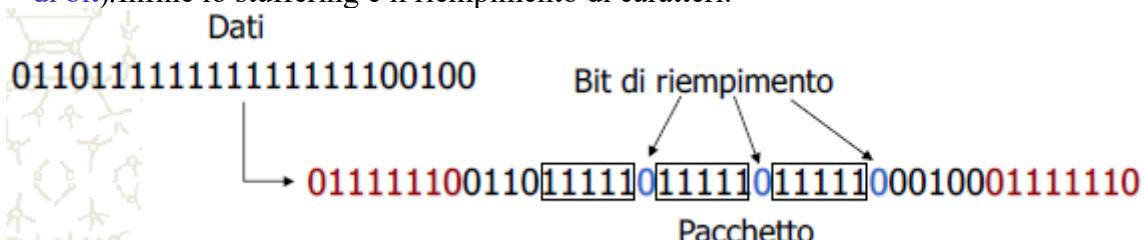
(a)



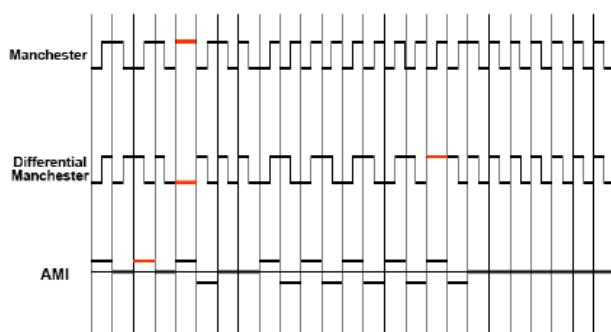
- **bit(s) di flag di inizio, e fine e bit stuffing:** I pacchetti sono iniziati dai caratteri ASCII **DLE** (Data Link Escape – 0x10) e **STX** (Start of TeXt - 0x02) e terminati da **DLE ETX** (End of TeXt – 0x03). Ci si può sincronizzare nuovamente cercando la sequenza DLE STX. I dati nel pacchetto non possono contenere queste due sequenze. In trasmissione si duplica ogni DLE nei dati che poi si elimina in ricezione. Un STX o ETX preceduto da due DLE è un dato del pacchetto. Due DLE DLE in sequenza servono per trasmettere il DLE proprio.



I pacchetti sono iniziati e terminati con una sequenza speciale di bit: *Flag byte = 01111110*. Per evitare che il flag byte possa trovarsi all'interno dei dati del pacchetto, viene inserito un bit 0 dopo ogni gruppo di 5 bit a 1. Il bit inserito viene eliminato in ricezione (**riempimento di bit**). Infine lo stuffing è il riempimento di caratteri.



- **Violazioni di codifica:** È possibile segnalare l'inizio o la fine di una trama con una deliberata violazione delle regole di codifica del segnale. Ad esempio, usando la codifica Manchester differenziale è possibile ottenere una violazione omettendo la transizione da 1 a 0 o da 0 a 1 nel mezzo di un impulso per indicare rispettivamente la fine o l'inizio di una trama.



IL CONTROLLO DI FLUSSO

Può capitare che una sorgente sia in grado di trasmettere ad un tasso più alto della capacità di ricevere a destinazione. Senza controllo, questo implica che la destinazione inizierebbe a scartare frame trasmessi correttamente per mancanza di risorse (tempo di processamento, buffer). Il protocollo deve poter gestire questa situazione e prevedere meccanismi per rallentare la trasmissione. Tipicamente il protocollo prevederà dei frame di controllo con cui il ricevente può inibire e riabilitare la trasmissione di frame, cioè il protocollo stabilisce quando il trasmittente può inviare frame. Più avanti vedremo diverse tecniche, che si differenziano per complessità ed efficienza di utilizzo della linea.

L'implementazione del data link layer prevederà la realizzazione dell' interfaccia con i livelli adiacenti, ad esempio due procedure *from-network-layer()* e *to-network-layer()* per scambiare dati con il livello superiore, e due procedure analoghe per scambiare dati con lo strato fisico.

In aggiunta sarà prevista una procedura *wait-for-event()* che metterà il data link layer in attesa di un evento. Questo evento sarà in generale la segnalazione, da parte di uno dei due livelli adiacenti, che sono disponibili dei dati. Infine, saranno definite procedure per il trattamento dei dati (inserimento/rimozione di header, calcolo di checksum, ...). In ricezione, il data link layer verrà svegliato per prelevare dati dallo strato fisico, processarli, e passarli allo strato di rete. Di fatto il DDL in ricezione non sarà in grado di rispondere ad eventi per il tempo che intercorre tra la chiamata alla procedura *from-physical-layer()* e la fine della procedura *to-network-layer()*. In questo intervallo di tempo, dati in arrivo saranno messi in un buffer, in attesa di essere processati, poiché il tempo di elaborazione non è nullo, si deve gestire l'eventualità che i dati arrivino troppo velocemente.

Un semplice meccanismo può essere quello di valutare i tempi di risposta del ricevente, ed inserire dei ritardi nel processo di trasmissione per adattarlo alla capacità di ricezione. Il problema è che il tempo di processamento in ricezione non è una costante e può dipendere dal numero di linee che il nodo ricevitore deve gestire. Basarsi sul caso peggiore comporta un grosso limite di efficienza, infatti vedremo esempi di protocolli che implementano un controllo di flusso di complessità crescente al fine di utilizzare al meglio la banda.

Il **frame** del data link prevede un'intestazione (**header**) e una coda (**trailer**) aggiunti al pacchetto passato dal livello di rete. Le informazioni di framing e di checksum sono gestite in hardware. La presenza di campi di controllo dipende dal **protocollo** di comunicazione utilizzato nel livello data link:

- **Tipo del pacchetto (type)** (es. **data, ack, nack**)
- **Numero di sequenza del pacchetto (seq)**: in caso di connectionless mi permette di ristabilire l'ordine dei pacchetti.
- **Numero di riscontro (ack)**: l'ack è riscontro della trama fino alla sequenza q.

Start flag	type	seq	ack	Pacchetto (livello rete)	Check sum	End flag
------------	------	-----	-----	--------------------------	-----------	----------

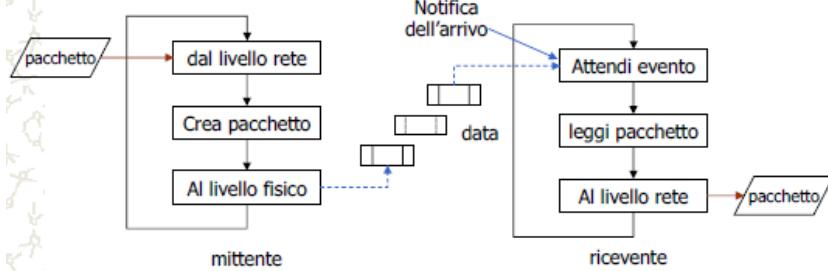
NOTA:

Riscontro: dal quel momento in poi tutto quello che ho mandato è archiviato, quindi non serve rimandarlo.

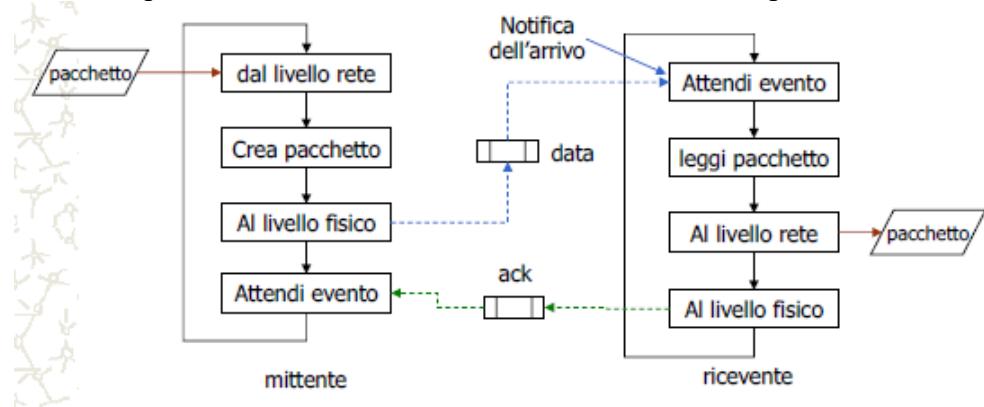
Protocolli del data link

Definiscono le modalità di scambio dei pacchetti fra mittente e ricevente (ack, stop-and-wait, ritrasmissione,...), di seguito ne saranno specificati alcuni:

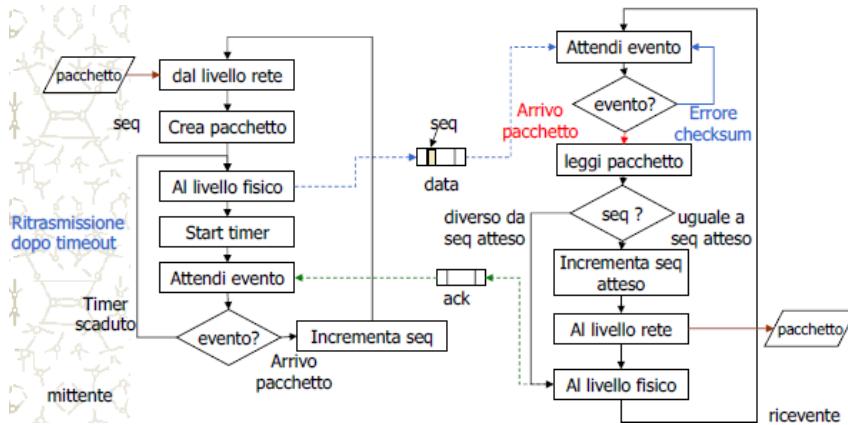
- **Protocollo non limitato:** Protocollo senza conferma e senza connessione. I pacchetti possono andare persi o essere accettati anche se corrotti.



- **Protocollo stop – and wait:** Sincronizzazione della trasmissione con ack. Evita il flooding del ricevente. Funziona solo se c'è garanzia dell'arrivo dei pacchetti di ack. Ipotizziamo che il canale sia privo di errori e che il traffico dati scorra in una direzione sola, dal trasmittente (A) al ricevente (B), cioè protocollo simplex, abbiamo quindi che :
 1. Il protocollo stop-and-wait prevede che A, dopo aver inviato il frame, si fermi per attendere un riscontro.
 2. B, una volta ricevuto il frame, invierà ad A un frame di controllo, cioè un frame privo di dati, allo scopo di avvisare A che può trasmettere un nuovo frame.
 3. Il frame di riscontro di indica generalmente con il termine ACK (ACKnowledge) o RR (Receiver Ready).
 4. Va osservato che il traffico dati è simplex, ma i frame devono viaggiare nelle due direzioni, quindi il canale fisico deve essere almeno half-duplex.



- **Protocollo con timeout:** Il numero di sequenza (seq) impedisce che il ricevente accetti un pacchetto duplicato (invia in caso di perdita dell'ack). Nel caso di ricezione con errore si aspetta lo scadere del timeout. Protocollo PAR (Positive Acnowledgement with Retransmission) o anche ARQ (Automatic Repeat reQuest). Il tempo di timeout non deve essere troppo corto per evitare continue ritrasmissioni. Il protocollo può fallire se un ack ritarda ad arrivare e nel frattempo scade il timeout e si ritrasmette (si perde il sincronismo dell'ack). Dipende dal fatto che l'ack è anonimo (senza seq). Gestisce il caso di canali disturbati (perdita pacchetti).



- **Trasmissioni full duplex:** Quando il canale di comunicazione permette l'invio di dati in entrambe le direzioni contemporaneamente e' possibile definire protocolli di comunicazione detti full duplex. In caso di linea full duplex il canale trasmette frame di dati in un verso e frame di ACK relativi alla comunicazione nel verso opposto, mischiati tra loro. I frame saranno distinti da una informazione contenuta nell'header del frame, che etichetta i frame come "dati" o come "frame di controllo".
- **Acknowledge in piggybacking:** Per motivi di efficienza spesso si utilizza una tecnica (detta "piggybacking") per evitare di dover costruire e trasmettere un frame di ACK; gli si dedica un campo dell'header di un frame di dati per trasportare l'ACK della trasmissione in senso inverso. Quando si deve trasmettere un ACK, si aspetta di dover trasmettere un frame di dati che possa trasportare l'informazione di ACK. Se non ci sono dati da inviare, si dovrà comunque inviare un frame di ACK prima che scada il timeout del trasmittente questo implica il dover utilizzare un altro timer per decidere dopo quanto tempo inviare comunque l'ACK in caso di mancanza di dati da inviare in senso inverso.
- **Protocolli a finestra scorrevole:** I protocolli a finestra scorrevole (sliding window) permettono di inviare piu' di un frame prima di fermarsi per attendere il riscontro, fino ad un valore massimo W fissato a priori. Poiche' in ricezione possono arrivare piu' frame consecutivi, i frame devono essere numerati per garantire in ricezione che non si siano persi frame: saranno dedicati n bit di controllo per la numerazione, ed i frame potranno avere numero da 0 a $2^n - 1$. In ricezione non e' necessario riscontrare tutti i frame: il ricevente puo' attendere di ricevere un certo numero di frame (fino a W) prima di inviare un solo riscontro cumulativo. La numerazione dei frame e' in modulo 2^n , cioe' il frame successivo a quello numerato $2^n - 1$ avra' come identificativo il numero 0. Per non avere sovrapposizione dei numeri identificativi tra i frame in attesa di riscontro, questi non dovranno essere in numero maggiore di 2^n , quindi si avra' sempre $W \leq 2^n$; in funzione del protocollo usato si potranno avere restrizioni maggiori. Questo tipo di protocolli necessita' di maggiori risorse di buffer: in trasmissione devono essere memorizzati i frame inviati in attesa di riscontro, per poterli ritrasmettere in caso di necessita' ad ogni riscontro ricevuto, vengono liberati i buffer relativi ai frame riscontrati, per occuparli con i nuovi frame trasmessi a seconda del protocollo anche in ricezione di deve disporre di buffer, ad esempio per memorizzare frame fuori sequenza; ad ogni riscontro inviato, i frame riscontrati vengono passati allo strato di rete ed i relativi buffer vengono liberati per poter accogliere nuovi frame in arrivo. Hanno bisogno di anche una maggiore complessita' di calcolo.
- La dimensione della finestra (W) puo' essere fissata a priori dal protocollo, ma esistono protocolli che permettono di modificarne il valore dinamicamente tramite informazioni di controllo del protocollo. La finestra più è piccola e più spreca banda, mentre più è grande e più la utilizza in modo ottimale.
- Ci sono dieci tipi di finestre, e differiscono nel fatto che possono essere asincrone, cioè di dimensione diversa, ma tipicamente non conviene farlo. Le due finestre sono:
 1. **Finestra in trasmissione:** In trasmissione si deve tenere conto dei frame inviati e

non riscontrati, e del numero massimo di frame che possono essere ancora inviati prima di dover fermare la trasmissione. Si utilizza una sequenza di numeri, indicanti gli identificativi dei frame. In questa sequenza di numeri si tiene conto di una finestra che contiene l'insieme dei frame che il trasmittente è autorizzato ad inviare. Con il procedere della trasmissione la finestra scorre in avanti:

- I. inizialmente la finestra ha limiti 0 e W-1.
- II. ad ogni frame inviato, il limite inferiore della finestra cresce di una unità; quando la finestra si chiude (cioè quando sono stati inviati W frame in attesa di riscontro) la trasmissione deve fermarsi.
- III. per ogni frame riscontrato, il limite superiore della finestra si sposta in avanti di una unità (o più se si è ricevuto un riscontro cumulativo), permettendo al trasmittente di inviare nuovi frame.

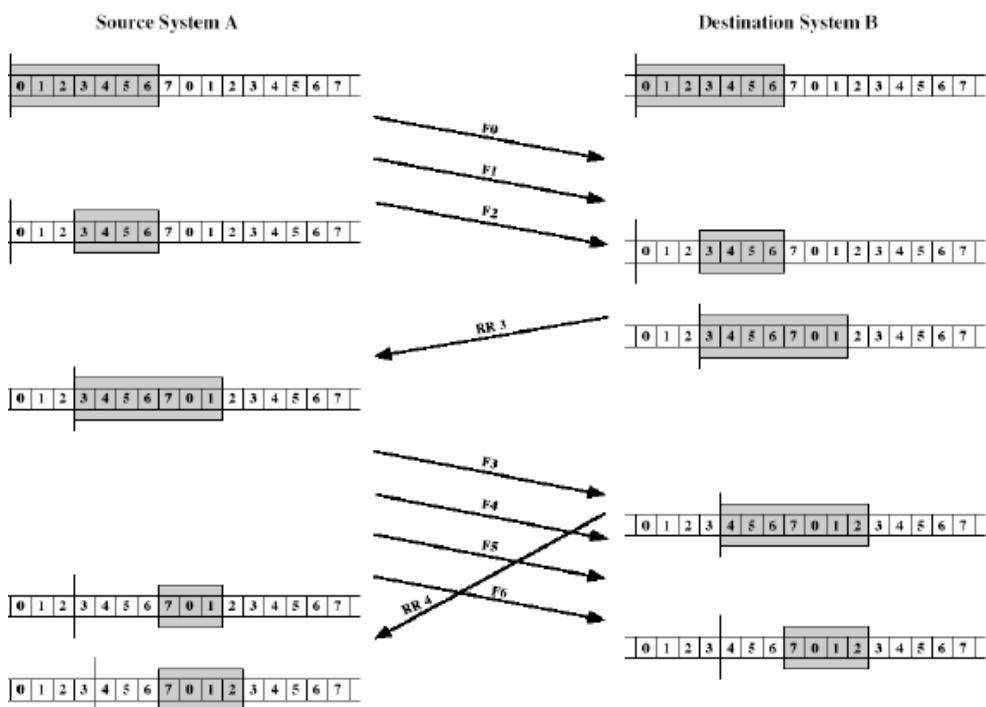
La dimensione della finestra di trasmissione varia, ma non può mai superare il valore di W.

2. **Finestra in ricezione:** In ricezione si deve tenere conto dei frame ricevuti di cui non è stato ancora inviato l'ACK, e del numero di frame ancora accettabili. Si utilizza una finestra analoga a quella in ricezione: la finestra contiene i numeri dei frame accettabili, il limite inferiore è il numero del frame successivo all'ultimo ricevuto, mentre il limite superiore è dato dal primo non ancora riscontrato più W.

Ad ogni nuovo frame ricevuto il limite inferiore della finestra cresce di una unità, mentre ad ogni acknowledgement inviato il limite superiore avanza di una unità.

La dimensione della finestra non può eccedere il valore di W (tutti i frame ricevuti sono stati riscontrati). Quando la finestra si azzerà significa che si devono per forza inviare i riscontri, perché la ricezione è bloccata. Qualsiasi frame ricevuto con numero fuori dalla finestra di ricezione sarà buttato via. La finestra in ricezione non deve necessariamente avere la stessa dimensione della finestra in trasmissione: ad esempio una finestra in ricezione più piccola costringerà il ricevente ad inviare ACK prima che in trasmissione sia stata azzerata la finestra.

- **Protocolli a finestra scorrevole:** Ogni frame spedito contiene un numero progressivo a n bit. La **finestra di trasmissione** del mittente corrisponde ai frame che può ritrasmettere (frame ancora senza ack). La **finestra di ricezione** del ricevente che indica i frame che può accettare (pacchetti attesi che non sono stati ancora ricevuti).



Spiegazione dell'esempio: inizialmente sono inviate 3 trame, tutte e 3 vengono ricevute correttamente e viene inviato un RR3, poi A ne reinvia 4; ma risponde con RR4 che sta ad indicare che solo F3 è arrivata correttamente.

Il mittente mantiene in un buffer di dimensione w tutti i frame nella finestra nel caso debbano essere ritrasmessi. Quando il buffer è pieno (non si sono ricevuti ack) il livello data link del mittente non accetta più pacchetti dal livello di rete.

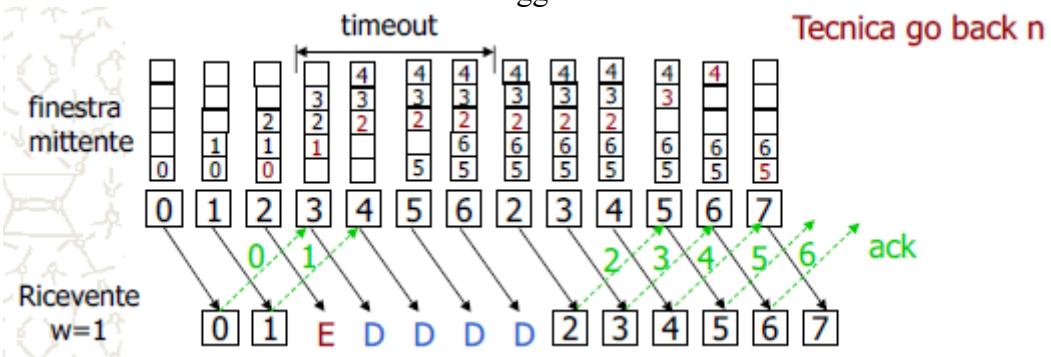
Se $w=1$ si ha un protocollo stop-and-wait (si aspetta l'ack prima di spedire un nuovo frame). Il protocollo stop-and-wait spreca banda per le attese in caso di mezzo fisico con ritardo non trascurabile.



L'utilizzo di un protocollo sliding window permette di utilizzare meglio la linea, ma complica il problema di gestire gli errori; il trasmittente, prima di accorgersi che un frame è stato ricevuto con errore, ha già inviato altri frame, in ricezione possono quindi arrivare frame corretti con numero di sequenza successivo ad un frame rigettato (non ricevuto). Questi protocolli prevedono l'invio sia di frame **ACK** (per riscontrare un frame), indicati anche come **RR** (*Receiver Ready*), che **NAK** (*Not AcKnowledged*), indicato anche come **REJ** (*REject*), utilizzato per informare il trasmittente che è stato ricevuto un frame fuori sequenza. Sia gli ACK (RR) che i REJ riportano l'indicazione del numero di sequenza del frame che è atteso in ricezione (quello successivo all'ultimo riscontrato). Questi protocolli implementano anche frame di controllo **RNR** (*Receiver Not Ready*) che impongono al trasmittente di fermarsi fino alla ricezione di un nuovo RR; questi possono essere utilizzati come ulteriore controllo di flusso, per gestire situazioni non di errore ma di congestione o temporanea sospensione della attività in ricezione.

Esistono due protocolli che gestiscono in modo differente questa situazione:

- **protocollo go-back-N:** Questo protocollo segue la logica che in ricezione vengano rifiutati tutti i frame successivi ad un frame danneggiato o mancante.

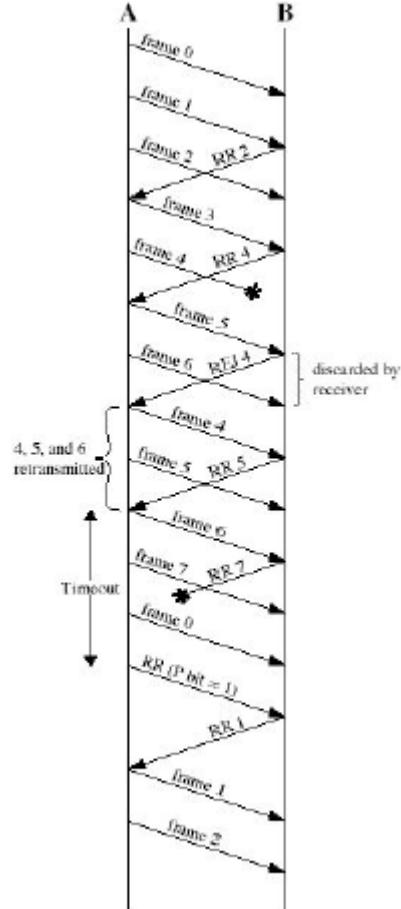


Esistono due possibilità:

1. **frame errato:** in questo caso B scarta il frame: se A non invia frame successivi, non accade nulla fino allo scadere del timer di A, quindi A ricomincia ad inviare frame a partire dal primo non riscontrato. Invece se A invia frame successivi, B risponde con un REJ dei frame ricevuti, in modo da notificare ad A che il frame indicato nel REJ è andato perso; al primo REJ ricevuto, A ricomincia dal primo frame non riscontrato.
2. **ACK errato:** in questo caso B ha accettato il frame: se A non invia frame successivi, allo scadere del timer: A invia nuovamente il frame; B lo rifiuta (duplicato) ma invia nuovamente l'ACK; alternativamente, al timeout A può inviare un frame di controllo per chiedere conferma dell'ultimo frame ricevuto correttamente, a cui B risponde con l'ACK relativo. Invece se A invia frame successivi, B risponde con

l'ACK del frame successivo; poiche' gli ACK sono cumulativi, l'ACK del frame successivo riscontra anche quello di cui A non ha ricevuto l'ACK, quindi il trasferimento dati continua senza interruzioni.

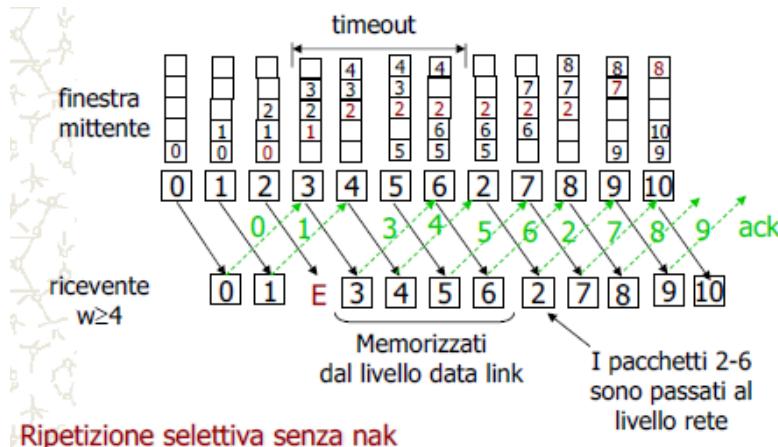
ES:



In questa immagine gli ACK sono indicati come RR (Receiver Ready). Alla ricezione del frame 5 B identifica la perdita del 4, ed invia un REJ che indica il 4 come frame atteso; questo permette a B di ripartire dal 4 prima del timeout, la perdita di RR7 comporta un timeout in quanto B non ha riscontrato i frame 7 e 0 in tempo; in questa situazione A sollecita un frame di RR, riceve il riscontro fino al frame 0 e ricomincia da 1.

Poiche' i riscontri sono cumulativi, la dimensione della finestra deve essere $W \leq 2^n - 1$; infatti supponiamo di avere $n=3$ (quindi numeri da 0 a 7) e scegliamo per W il valore 8; A invia il frame 7, e riceve ACK0 (riscontro del frame 7) poi A invia i frame da 0 a 7, e riceve ACK 0, A non puo' sapere se tutti i frame sono stati ricevuti (ACK 0 e' il riscontro dell'ultimo frame inviato) o sono stati tutti perduti (ACK 0 e' il riscontro ripetuto del primo frame inviato precedentemente. Se nell'esempio la finestra e' $W = 7$, A puo' inviare frame da 0 a 6; a questo punto se sono arrivati tutti, A ricevera' ACK 7; se sono andati tutti persi, A ricevera' ACK 0 quindi con $W \leq 2^n - 1$ non c'e' ambiguita'.

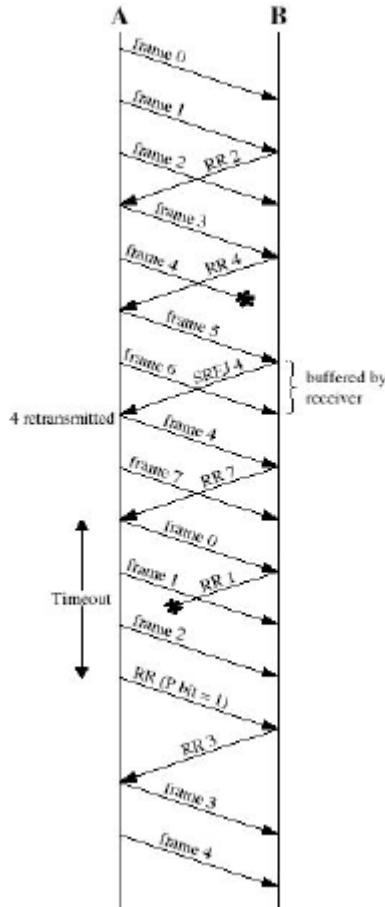
- **protocollo selective reject:** Il protocollo selective reject prevede che in ricezione possano essere accettati frame fuori sequenza, utilizzando un meccanismo di ritrasmissione selettiva dei frame errati.



- in questo modo si riduce ulteriormente il numero di frame ritrasmessi, mantenendo la caratteristica di recapitare allo strato di rete i dati nell'ordine corretto. In ricezione i frame fuori ordine (ma dentro la finestra) vengono mantenuti nei buffer fino a che non siano stati ricevuti tutti i frame intermedi.

Quando si ha un frame perduto, B riceverà il frame successivo fuori sequenza, al quale risponderà con un ACK relativo al frame perduto. A non ritrasmette tutti i frame successivi a quello, ma solo quello perduto, quindi proseguirà con la normale sequenza. B ha memorizzato i frame successivi, ed alla ricezione del frame ritrasmesso libererà tutti i buffer inviando un ACK relativo all'ultimo frame ricevuto correttamente. In caso di perdita dell'ACK, sarà il timeout di A a generare un frame di sollecito di ACK per B, che risponderà di conseguenza.

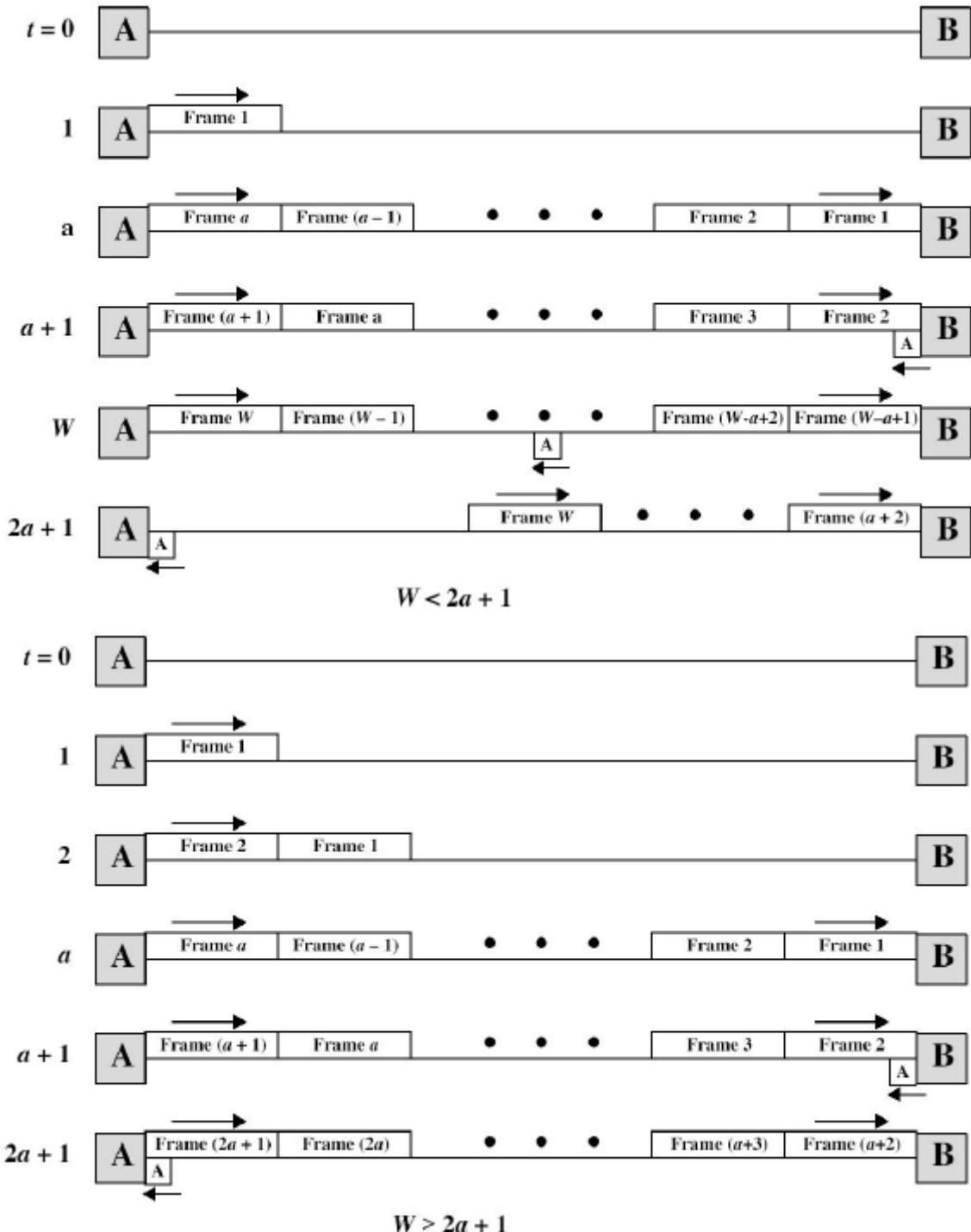
ES:



Alla ricezione del frame 5 B identifica la perdita del 4, ed invia un REJ che indica il 4 come frame atteso; questo permette a B di trasmettere il 4 dopo aver trasmesso il 6. Nel frattempo A ha memorizzato il 5 ed il 6, ed alla ricezione del 4 invia l'RR per il 6 la perdita di RR1 comporta un timeout in quanto B non ha riscontrato i frame 1 e 2 in tempo; in questa situazione A sollecita un frame di RR, riceve il riscontro fino al frame 2 e ricomincia da 3

La ricezione non sequenziale limita ulteriormente la massima dimensione della finestra in funzione del numero di bit per la numerazione del frame. Come prima, supponiamo di avere 3 bit, ed una finestra a dimensione 7 (idonea per il protocollo go-back-N). A trasmette da 0 a 6, B risponde con ACK 7 e sposta la sua finestra in (7,0,1,2,3,4,5), l'ACK 7 si perde; dopo il timeout A ritrasmette il frame 0, B accetta 0 come un nuovo frame (ipotizza che il 7 sia andato perduto) e trasmette NACK 7, A riceve NACK 7, lo identifica come un errore di protocollo e chiede la ripetizione del riscontro, a cui B risponde con un ACK 7, A ritiene a questo punto che i frame da 0 a 6 siano arrivati tutti e riparte con i nuovi: 7,0,1,..., A riceve 7 (OK) ma lo 0 nuovo lo interpreta come duplicato di quello ricevuto precedentemente e lo butta; quindi si prosegue; in questo esempio lo strato di rete riceve il frame 0 vecchio al posto del frame 0 nuovo. Per eliminare l'ambiguità è necessario che le finestre in trasmissione e ricezione non si sovrappongano; questo si ottiene imponendo che la finestra abbia dimensione $W \leq 2^{(n-1)}$, cioè la metà dello spazio di indirizzamento dei frame.

Efficienza del protocollo go-back-N



RILEVAZIONE DELL'ERRORE

Il livello fisico offre un canale di trasmissivo non privo di errori:

- errori su singolo bit
- replicazione di bit
- perdita di bit

Per la rilevazione di tali errori, nell'header di ogni trama il livello 2 inserisce un campo denominato **checksum** (il checksum è il risultato di un calcolo fatto utilizzando i bit trama), la destinazione ripete il calcolo e confronta il risultato con il checksum: se coincide la trama è corretta. La rivelazione degli errori serve a realizzare un servizio affidabile.



Oltre alla checksum esistono altre tecniche per il controllo degli errori:

- **I campi di Galois:** Un campo finito con q elementi su cui sono definite due operazioni aritmetiche (addizione e moltiplicazione) che godono della proprietà commutativa ed associativa viene chiamato **Campo di Galois** ed indicato con $GF(q)$. $GF(q)$ è chiuso rispetto all'addizione e moltiplicazione. In generale q deve essere sempre primo o potenza di numeri primi. Le operazioni di somma e moltiplicazione vengono calcolate utilizzando i concetti aritmetici tradizionali con l'applicazione di un ulteriore operazione di **mod q** . Come la checksum non è molto corretta se ci sono più di un errore.

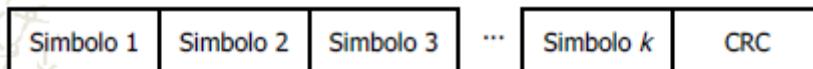
$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

\times	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+$	0	1
0	0	1
1	1	0

\times	0	1
0	0	0
1	0	1

- **Cyclic Redundance Check-sum:** Basato sul concetto di codice ciclico, in cui permutando ciclicamente gli elementi di una qualsiasi combinazione, si ottengono sempre combinazioni dello stesso codice.



$$\text{CRC} = \sum_i m_i \text{ su } GF(q)$$

$$\text{Data } m = 1023110223242234 \quad \text{CRC} = 2$$

- **Rappresentazione tramite polinomi:** Una sequenza di N bit puo' essere rappresentata tramite un polinomio a coefficienti binari, di grado pari a $N-1$, tale che i suoi coefficienti siano uguali ai valori dei bit della sequenza. Il bit piu' a sinistra rappresenta il coefficiente del termine di grado $N-1$, mentre il bit piu' a destra rappresenta il termine noto (di grado 0). Ad esempio, la sequenza 1001011011 puo' essere rappresentata dal polinomio:

$$x^9 + x^6 + x^4 + x^3 + x + 1$$

Il grado del polinomi è determinato dal primo bit a sinistra, che ha valore 1.

- **Codifica polinominale (CRC) :** La tecnica consiste nel considerare i dati (m bit) da inviare come un polinomio di grado m-1. Trasmettitore e ricevitore si accordano sull'utilizzo di un polinomio generatore G(x) di grado r. Il trasmettitore aggiunge in coda al messaggio una sequenza di bit di controllo (CRC) in modo che il polinomio associato ai bit del frame trasmesso, costituito dall'insieme di dati e CRC, sia divisibile per G(x). In ricezione si divide il polinomio associato ai dati ricevuti per G(X), se la divisione ha resto nullo, si assume che la trasmissione sia avvenuta senza errori, invece se la divisione ha resto non nullo, sono certamente avvenuti errori.

Di seguito una spiegazione dei codici ciclici:

Assegniamo un polinomio P di grado p-1 al messaggio che vogliamo trasmettere.

$$m = 10100011 \Rightarrow P(x) = 1 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0 \\ \text{cioè } P(x) = x^7 + x^5 + x + 1$$

Scelto G(x) di grado r <= p - 1, detto **polinomio generatore** (conosciuto sia dalla sorgente che dall'utente), si aggiungono r zeri ai p bit del blocco da trasmettere, per esempio:

$$G(x) = x^3 + 1 \quad \text{diviene} \quad x^3 P(x) = x^{10} + x^8 + x^4 + x^3 \quad \text{cioè } P = 10100011000$$

$$\text{Effettuando la divisione: } \frac{x^r P(x)}{G(x)} \rightarrow Q(x)G(x) + R(x) = x^r P(x)$$

$$\text{cioè } x^r P(x) - R(x) = Q(x)G(x) \quad \text{Poiché operiamo nel caso dei codici binari, il campo di Galois utilizzato è GF(2). Quindi } -R(x) = +R(x)$$

$$\text{La formula precedente diventa: } x^r P(x) + R(x) = Q(x)G(x)$$

$$\text{Nel nostro esempio diviene: } Q(x) = 10110101 \rightarrow x^7 + x^5 + x^4 + x^2 + 1 \\ R(x) = 101 \rightarrow x^2 + 1$$

$$\text{Quindi quello che trasmettiamo è esattamente la parola di codice corrispondente al polinomio: } x^r P(x) + R(x)$$

$$\text{Che nel nostro caso è: } T = 10100011101 \quad T(x) = x^{10} + x^8 + x^4 + x^3 + x^2 + 1$$

Come conseguenza delle definizioni precedenti T(x) definisce una parola di un codice cirlico che è sempre multiplo del polinomio generatore G(x).

Quindi per verificare la corretta trasmissione basta dividere T(x) per G(x). Se il resto della divisione è zero, allora non si è verificato nessun errore.

Ci sono dei polinomi di fatto usati come standard:

$G(x) = x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$	CRC-12	
$G(x) = x^{16} + x^{15} + x^2 + 1$	CRC-16	CRC-32
$G(x) = x^{16} + x^{12} + x^5 + 1$	CRC-CCITT	$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Tutti contengono x+1 come fattore. CRC-16 e CRC-CCITT riconoscono errori singoli e doppi, errori con un numero dispari di bit, i burst di errori di lunghezza massima 16, il 99.997% dei burst di lunghezza 17 bit. Il circuito per il calcolo del checksum può essere realizzato semplicemente in hardware.

NOTA:

In un servizio unreliable(non affidabile) non viene fatto nessuno di questi controlli. Infatti sono tutti fatti al livello di trasporto.

Su reti piccole non conviene implemenarli, conviene implementarli successivamente nel livello di trasporto.
Su reti di dimensione più vasta conviene invece utilizzarli.

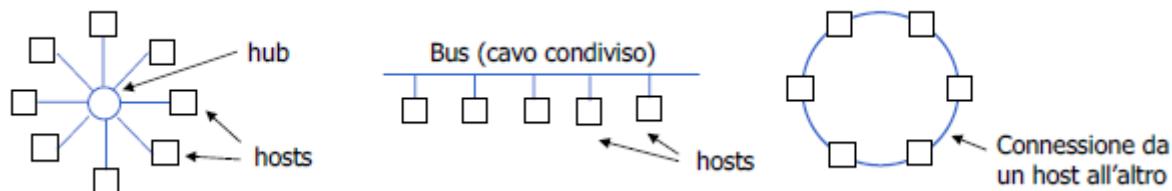
RETI BROADCAST MULTI-ACCESS

Sono usate spesso nelle LAN. Il canale è condiviso fra N stazioni indipendenti. Si devono risolvere i conflitti di accesso. Si divide in due tipi:

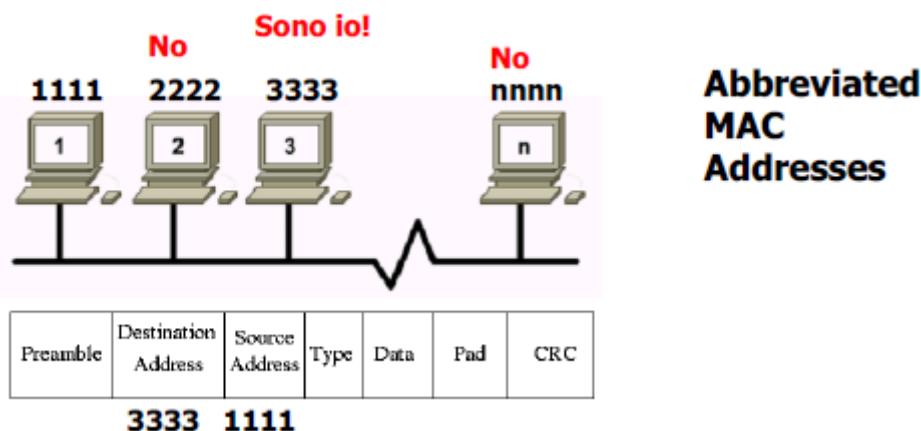
- **Allocazione statica (FDM o TDM)**: non è efficiente in ambienti altamente dinamici, il numero di stazioni è variabile, il carico è variabile (stazioni inattive).
- **Allocazione dinamica (risoluzione dei conflitti di accesso)**: *Collisione*: due segnali trasmessi simultaneamente si sovrappongono e il segnale risultante sarà confuso. Le stazioni possono rilevare le collisioni. Una collisione corrisponde ad un errore di trasmissione. È molto usata nelle LAN tramite la multiplazione statistica.

MEZZO CONDIVISO

Un mezzo condiviso tra tutte le stazioni per trasmettere e ricevere. Solo una stazione alla volta può trasmettere. Le stazioni operano a turni. Stelle e cavo condiviso fanno parte sempre di una topologia a Bus.

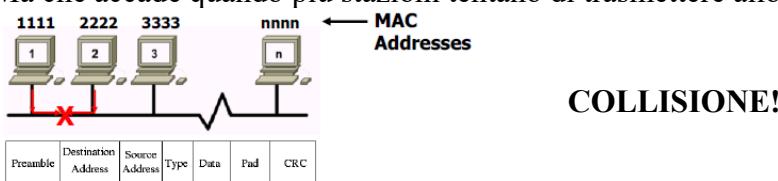


- **Collision-Detection** esempio: IEEE 802.3 (Ethernet).
- **Collision-free** (non si possono mai verificare delle collisioni) esempio: IEEE 802.5 (Token Ring) o IEEE 802.17 RPR.



Quando una trama viene inviata sul mezzo condiviso tutti i dispositivi collegati la ricevono. Ogni NIC confronta il suo MAC address con quello il destination address sulla trama. Se corrispondono, copia il resto della trama. Altrimenti, la ignora, a meno che la NIC non operi in **modalità promiscua**.

Ma che accade quando più stazioni tentano di trasmettere allo stesso tempo?



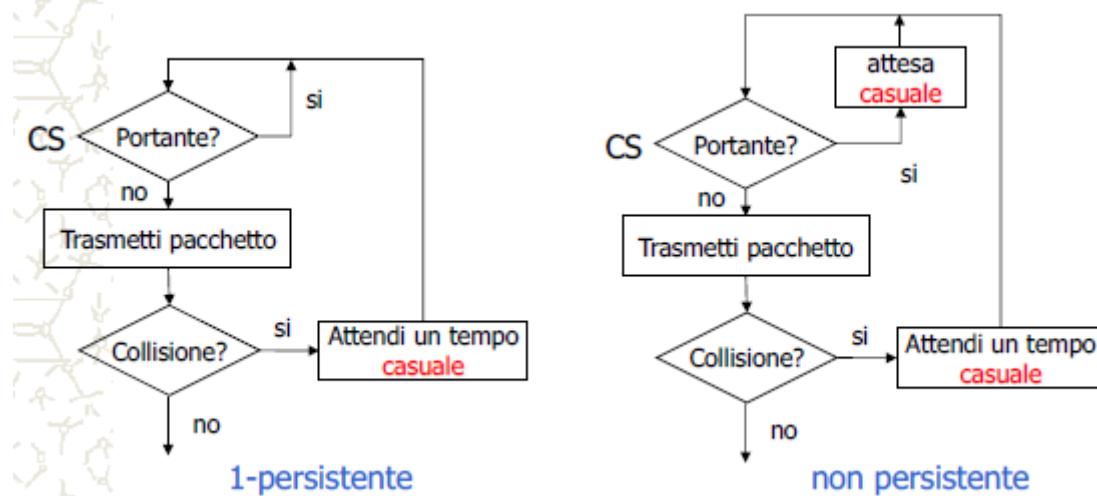
COLLISIONE

È un concetto nato per le reti broadcast:



La collisione viene rilevata ascoltando il canale e verificando che il segnale ricevuto corrisponda a quello trasmesso senza interferenze basta una minima sovrapposizione dei due pacchetti per farli andare persi.

Prima di iniziare dobbiamo capire se qualcuno sta trasmettendo sul mezzo. Ascoltando se c'è una portante, se c'è si possono avere diversi protocolli. Protocolli con rilevamento della portante (**Carrier Sense – CS**). Migliorano l'utilizzo del canale perché evitano le collisioni quando il canale è già impegnato.

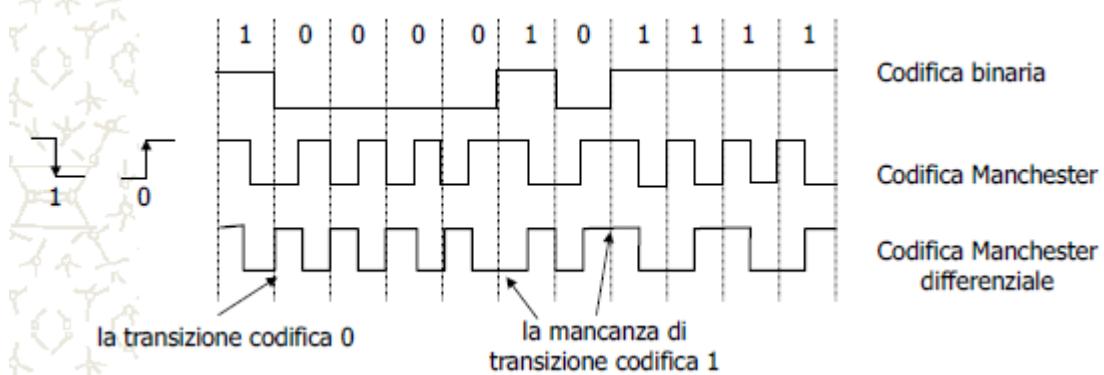


- **CSMA 1 – PERSISTENTE:** Il più semplice di questi protocolli ha il seguente funzionamento:
 - quando un calcolatore ha dati da trasmettere, ascolta il segnale presente sul mezzo trasmisivo, se trova il canale libero trasmette il frame, invece se trova il canale occupato, continua ad ascoltare fino a che il canale non si libera, e poi trasmette il frame.
 - in caso di collisione, la stazione aspetta un tempo casuale e ripete l'algoritmo.
 Il protocollo si chiama 1-persistente perché quando trova il canale occupato, resta in ascolto continuamente, ed appena il canale si libera trasmette **con probabilità 1 (sempre)**. Con questo protocollo acquista grande importanza il ritardo di propagazione del segnale tra due stazioni; infatti, quando una stazione inizia a trasmettere, una seconda stazione potrebbe voler trasmettere, ed ascolta il canale, mentre se il segnale trasmesso dalla prima stazione non ha ancora avuto il tempo di propagarsi fino alla seconda stazione, questa troverà il canale libero e trasmetterà, generando una collisione. Maggiore è il ritardo di propagazione, più numerose saranno le collisioni dovute alla eventualità sopra descritta.
- Nota: questa situazione si presenterà sempre ed indipendentemente dal ritardo di propagazione qualora due stazioni volessero trasmettere mentre una terza sta' trasmettendo: alla fine della trasmissione della terza stazione, le due stazioni in attesa si metteranno sempre a trasmettere contemporaneamente.*

Come slotted aloha, questo protocollo non interferisce con le trasmissioni già in atto. A differenza di slotted aloha, questo protocollo non prevede di dover attendere la time slot successiva, evitando ad esempio di lasciare inutilizzata una slot temporale per il tempo di durata della slot stessa. Inoltre CSMA 1-persistente non richiede la sincronizzazione delle stazioni connesse alla rete.

- **CSMA NON PERSISTENTE (0 – PERSISTENTE):** Si differenzia dal precedente per il fatto che una stazione, quando vuole trasmettere ma trova il canale occupato, non resta ad ascoltare in continuazione, ma attende un tempo casuale e riprova. Questo meccanismo riduce sensibilmente le collisioni dovute al fatto che due stazioni vogliono trasmettere durante la trasmissione di una terza:
 - ora le stazioni attenderanno generalmente tempi diversi prima di ritentare
 - la prima che ritenta troverà il canale libero e trasmetterà
 - la seconda troverà nuovamente il canale occupato, quindi non interferirà ed aspetterà ancora.
 Questo protocollo alza notevolmente l'efficienza di utilizzo del canale con l'aumento del carico, cioè delle stazioni connesse alla rete. Il problema principale di questo protocollo è che in condizioni di elevato carico il tempo che intercorre tra l'istante in cui la stazione vuole trasmettere e **l'istante in cui riesce a trasmettere può crescere enormemente**.
- **CSMA P-PERSISTENTE:** In questa ultima versione del protocollo a rilevamento della portante, il tempo è suddiviso in slot temporali come nello slotted aloha. In questo caso, chi desidera trasmettere ascolta il canale continuamente e quando lo trova libero trasmette con probabilità p , oppure attende la slot successiva con probabilità $(1-p)$, alla slot successiva, se libera, trasmette nuovamente con probabilità p o aspetta la successiva con probabilità $1-p$, e così via, in caso di collisione, o se durante i tentativi di trasmissione qualche altra stazione inizia a trasmettere, la stazione attende un tempo casuale e ripete l'algoritmo.
Questo protocollo è una via di mezzo tra il protocollo 1-persistent (a cui tende per p che tende ad 1) e quello non persistente. Come nel caso di CSMA non persistente, ad elevato carico e per bassi valori di p cresce l'efficienza di utilizzo della linea ma cresce il ritardo di trasmissione rispetto all'arrivo dei dati dallo strato di rete. Per alti valori di p l'efficienza di utilizzo della linea desce rapidamente con l'aumentare del carico.

Nota: Rilevazione di una portante significa accorgersi che qualcuno sta trasmettendo. Per farlo si usa la codifica Manchester per i segnali i bit sono codificati da transizioni (usa il doppio della banda). I livelli in presenza di segnale sono standardizzati IEEE 802.3: -0.85, +0.85. L'assenza di portante è codificata dal segnale nullo (linea idle).



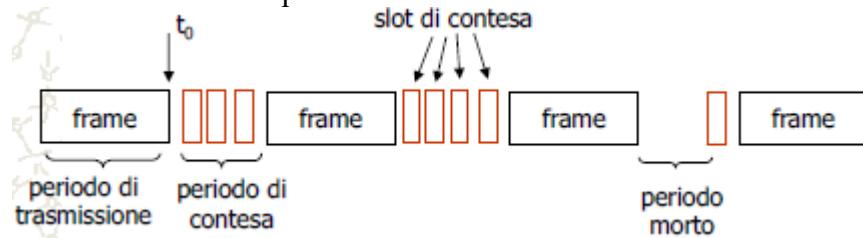
CSMA

Il protocollo opera in tre diverse fasi:

- **carrier sense:** (rilevazione della trasmissione): ogni stazione che deve trasmettere ascolta il bus e decide di trasmettere solo se questo è libero (listen before talking);
- **multiple access:** nonostante il carrier sense è possibile che due stazioni, trovando il mezzo trasmittivo libero, decidano contemporaneamente di trasmettere; la probabilità di questo evento è aumentata dal fatto che il tempo di propagazione dei segnali sul cavo non è nullo, e quindi una stazione può credere che il mezzo sia ancora libero anche quando un'altra ha già iniziato la trasmissione;
- **collision detection:** se si verifica la sovrapposizione di due trasmissioni si ha una "collisione"; per rilevarla, ogni stazione, mentre trasmette un pacchetto, ascolta i segnali sul mezzo trasmittivo, confrontandoli con quelli da lei generati (listen while talking).

CSMA/CD (collision detection)

Le stazioni bloccano la trasmissione quando rilevano una collisione.



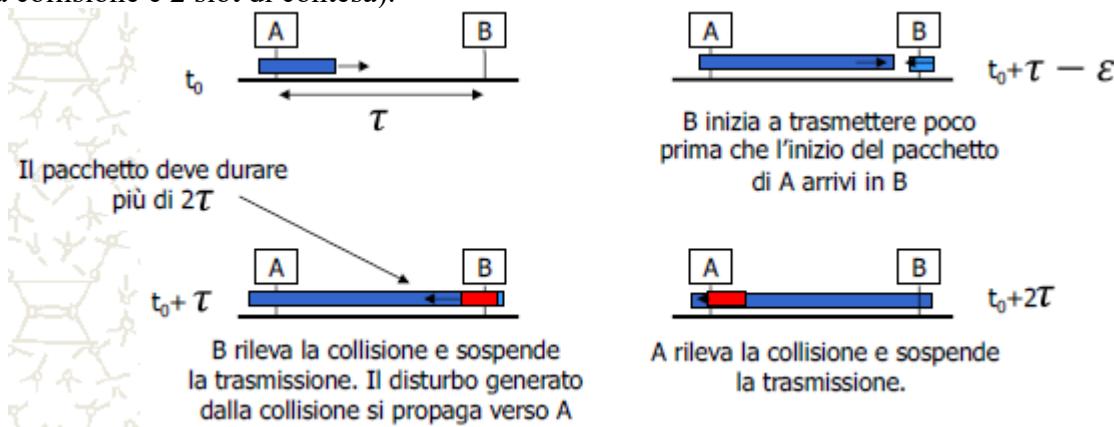
Alla fine di una trasmissione si può avere un periodo di contesa se 2 o più stazioni iniziano a trasmettere. L'ampiezza di ciascun slot di contesa dipende dal ritardo di propagazione (dalla distanza delle stazioni che trasmettono in contemporanea). I periodi morti si hanno quando nessuna stazione ha frame da trasmettere. Al termine del periodo di contesa chi ha vinto la contesa può trasmettere.

A seguito di un'avvenuta collisione si intraprendono le seguenti azioni:

- la stazione trasmittente sospende la trasmissione e trasmette una sequenza di *jamming* (interferenza trasmisiva) composta da 32 bit per 802.3 ed un numero di bit compreso tra 32 e 48 per Ethernet v.2.0; questa sequenza permette a tutte le stazioni di rilevare l'avvenuta collisione;
- le stazioni in ascolto, riconoscendo il frammento di collisione costituito dalla parte di pacchetto trasmessa più la sequenza di jamming, scartano i bit ricevuti;
- la stazione trasmittente ripete il tentativo di trasmissione dopo un tempo pseudo-casuale per un numero di volte non superiore a 16.

Dopo 16 volte si dice che la rete è jammed (intasata). Il dominio della collisione cresce troppo, cioè insieme di macchine che concorrono in logica CSMA/CD.

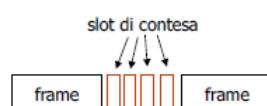
Sia $t(\tau)$ il tempo di propagazione fra le stazioni più lontane. Il tempo massimo per la rilevazione di una collisione è 2 slot di contesa).



Per risolvere le collisioni si usa l'algoritmo *Exponential Back-Off*:

Calcolo del tempo di attesa dopo una collisione

Lo slot di contesa è pari a 2τ (512 bit - 51.2 μ s per 10Mbps)



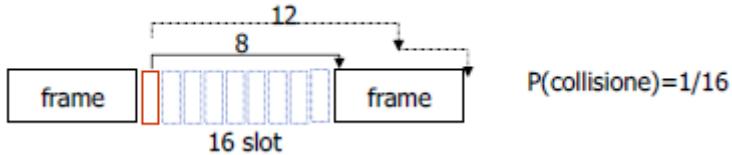
Prima collisione: aspetta 0 o 1 slot

Seconda collisione: aspetta 0,1,2 o 3 slot

Collisione n: aspetta r slot con r scelto in modo casuale nell'intervallo $0 \leq r \leq 2^{k-1}$
dove $k=\min(n,10)$

Collisione 16: si notifica l'errore di trasmissione

L'algoritmo adatta l'attesa al numero di stazioni che vogliono trasmettere. Un intervallo di slot di attesa alto diminuisce la probabilità che due stazioni collidano di nuovo ma introduce un ritardo medio elevato.

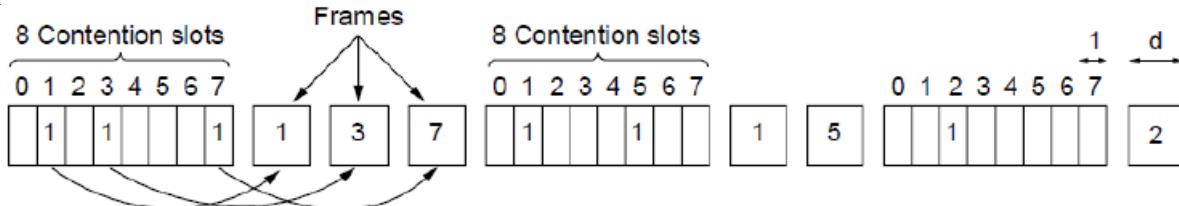


Un intervallo di slot di attesa basso rende improbabile la risoluzione della collisione quando molte stazioni collidono.

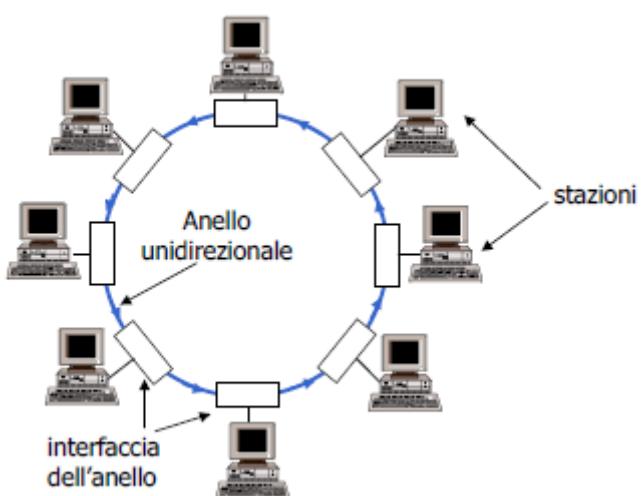
$$\frac{2 \text{ slot}}{100 \text{ stazioni}} \quad 99 \text{ su slot 0 e 1 su slot 1} \longrightarrow P(\text{non collisione}) = (0.5)^{99}$$

PROTOCOLLI COLLISION FREE: PRENOTAZIONE

Un esempio di protocollo a prenotazione è il protocollo a mappa di bit elementare: sulla rete ci sono N stazioni, numerate da 0 a N-1, alla fine della trasmissione di un frame inizia un periodo di contesa, in cui ogni stazione, andando per ordine di indirizzo, trasmette un bit che vale 1 se la stazione deve trasmettere, 0 altrimenti. Al termine del periodo di contesa (privo di collisioni in quanto ogni stazione aspetta il suo turno) tutti hanno appreso quali stazioni devono trasmettere, e le trasmissioni procedono un frame alla volta sempre andando per ordine, se una stazione riceve dati da trasmettere quando la fase di prenotazione è terminata, deve attendere il successivo periodo di contesa per prenotare la propria trasmissione. L'efficienza di questo protocollo è bassa per grandi valori di N e basso carico trasmissivo; in queste condizioni una stazione deve attendere tutti gli N bit delle altre stazioni (delle quali la maggior parte o la totalità non desidera trasmettere) prima di poter trasmettere.



Un esempio di questo tipo è la Token Ring. Non utilizza un mezzo broadcast ma un insieme di collegamenti punto-punto associati in successione per analizzare una topologia ad anello.

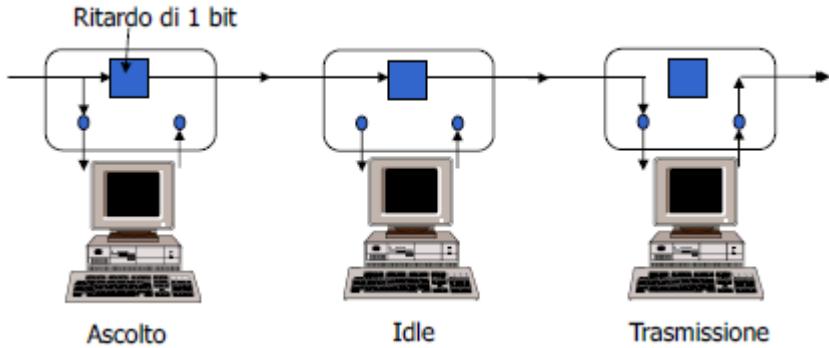


Token ring (standard IEEE 802.5), questo protocollo prevede l'utilizzo di una topologia ad anello, sull'anello circola un piccolo frame, detto token (gettone) che le stazioni ricevono da una parte e ritrasmettono dall'altra in continuazione. Una stazione è autorizzata a trasmettere dati solo quando è in possesso del token; la stazione riceve il token, lo trattiene ed inizia a trasmettere dati, terminata la trasmissione, ritrasmette il token in coda ai frame di dati, esistono specifiche a 4 e 16 Mbps. Esiste una versione modificata del token ring standardizzata per trasmissione su doppio anello in fibra ottica, detto **FDDI (Fiber Distributed Data Interface)** a 100 Mbps. L'IEEE ha

sviluppato uno standard molto simile, dedicato alle topologie a bus (token bus: IEEE 802.4), in questo protocollo il problema aggiuntivo è determinato dalla necessità di configurare un ordine sequenziale delle stazioni, che viene fatto in una fase di inizializzazione del protocollo.

Ogni bit che raggiunge l'interfaccia è copiato in un buffer di 1 bit. Il bit viene ritrasmesso

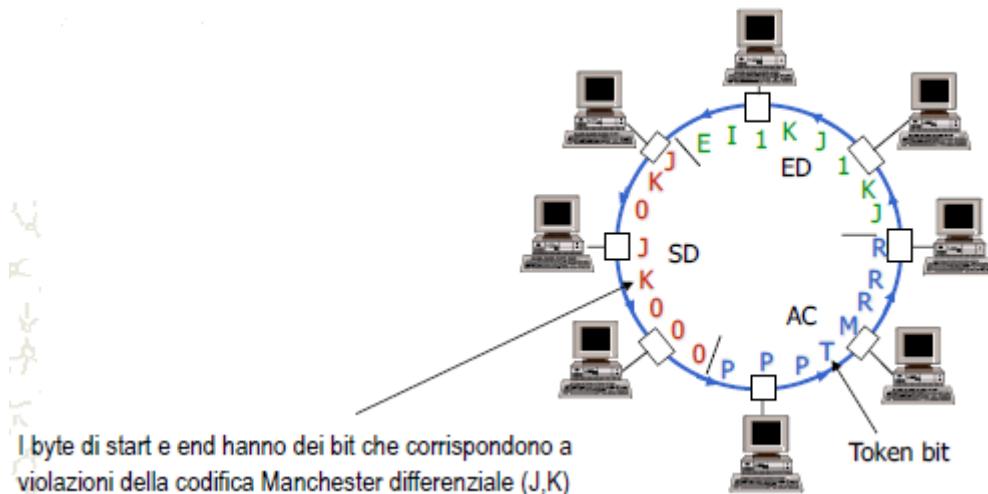
sull'anello dopo un'eventuale controllo (ascolto) o modifica (trasmissione). Si ha un ritardo di 1 bit per ogni interfaccia.



Il **token** è una sequenza particolare di bit che circola sull'anello quando tutte le stazioni sono inattive. Quando una stazione vuole trasmettere, si impossessa del token e lo rimuove dall'anello. Una sola stazione può trasmettere (quella che possiede il token).



L'anello deve avere un ritardo sufficiente per contenere un token completo circolante quando tutte le stazioni sono inattive. La velocità di propagazione tipica è di $200\text{m}/\mu\text{s}$. Se la velocità di trasmissione è di R Mbps, ogni bit occupa $200/R$ m.

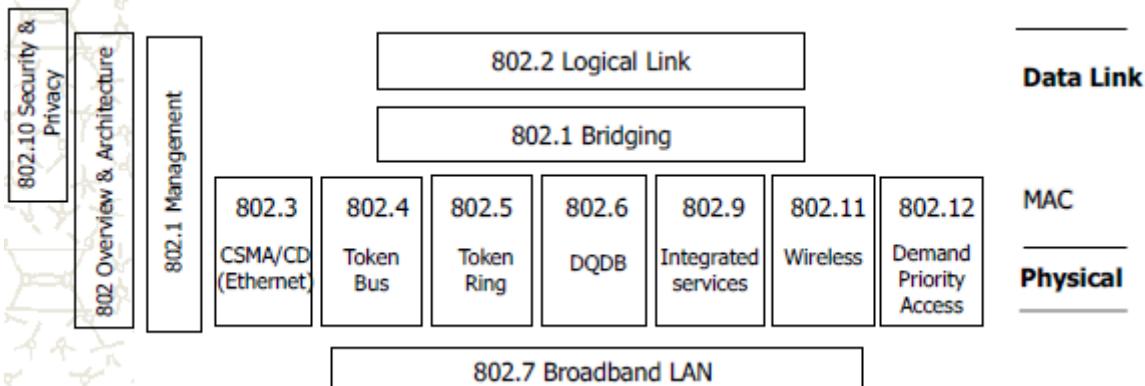


Efficienza:

Il protocollo token ring (come tutti quelli a turno) è poco efficiente in condizioni di basso carico, la stazione che deve trasmettere deve attendere di ricevere il token (o in generale deve attendere il suo turno) prima di poterlo fare, anche se il canale non è occupato. In condizioni di carico elevato, quando tutti vogliono trasmettere, l'efficienza del protocollo sfiora l'unica, il solo overhead è dovuto alla necessità che ha una stazione di identificare il token prima di poter trasmettere, in questi protocolli il token è scelto in modo opportuno per minimizzare l'overhead. Una importante caratteristica di questo genere di protocolli è la possibilità di valutare un tempo massimo di ritardo per le trasmissioni; una stazione che desidera trasmettere dovrà attendere al più N tempi di trasmissione (uno per stazione, nel caso tutti debbano trasmettere) prima che tocchi nuovamente ad essa, questo permette l'utilizzo del protocollo in situazioni in cui i tempi di risposta possono essere determinanti (ad esempio una catena di montaggio).

STANDARD IEEE 802

Standard LAN che includono CSMA/CD, token bus, token ring. Differenze al livello fisico e MAC ma compatibilità al livello data link : <http://standards.ieee.org/getieee802/>.



Quando le prime LAN cominciarono a diffondersi (ARC, Ethernet, Token Ring, ecc.), l'IEEE decise di costituire sei comitati per studiare il problema della standardizzazione delle LAN e delle MAN, complessivamente raccolti nel progetto IEEE 802.

Tali comitati sono:

- 802.1 Overview, Architecture, Bridging and Management;
- 802.2 Logical Link Control;
- 802.3 CSMA/CD (*Carrier Sense, Multiple Access with Collision Detection*);
- 802.4 Token Bus;
- 802.5 Token Ring;
- 802.6 Metropolitan Area Networks - DQDB (Distributed Queue, Dual Bus).

A tali comitati in seguito se ne sono aggiunti altri tra cui:

- 802.3u 100BaseT;
- 802.3z 1000baseX
- 802.3ae 10GbaseX
- 802.7 Broadband technical advisory group;
- 802.8 Fiber-optic technical advisory group;
- 802.9 Integrated data and voice networks;
- 802.10 Network security;
- 802.11 Wireless LAN networking;
- 802.16 WiMAX (Worldwide Interoperability for Microwave Access);

Il lavoro di tali comitati procede in armonia con il modello di riferimento OSI, e la relazione esistente tra il progetto OSI, il progetto IEEE 802 e lo standard EIA/TIA.

STANDARD IEEE 802.1

È lo standard contenente le specifiche generali del progetto 802; esso è composto da molte parti, tra cui:

- *802.1 Part A* (Overview and Architecture);
- *802.1 Part B* (Addressing Internetworking and Network Management);
- *802.1 Part D* (MAC Bridges).ù

IEEE 802 introduce l'idea che le LAN e le MAN devono fornire un'interfaccia unificata verso il livello Network (livello rete), pur utilizzando tecnologie trasmissive differenziate. Per ottenere tale risultato, il progetto IEEE 802 suddivide il livello Data Link in due sottolivelli:

- **LLC (Logical Link Control)**: mette a disposizione al livello successivo i servizi del data link.
- **MAC (Media Access Control)**: ogni MAC dipende dalle caratteristiche fisiche del mezzo su cui trasmette.

Il sottolivello LLC è comune a tutte le LAN, mentre il MAC è peculiare di ciascuna LAN, così come il livello fisico al quale è strettamente associato. Il sottolivello LLC è l'interfaccia unificata

verso il livello Network ed è descritto nell'apposito standard IEEE 802.2, mentre i vari MAC sono descritti negli standard specifici di ogni rete locale (ad esempio il MAC CSMA/CD è descritto nello standard IEEE 802.3). Nel seguito, per facilità di lettura, si parlerà solo di reti locali (LAN), ma quanto detto vale ovviamente anche per le reti metropolitane (MAN), **comprese anch'esse nel progetto IEEE 802**.

Che cos'è il MAC?

Il sottolivello MAC è specifico di ogni LAN e risolve il problema della condivisione del mezzo trasmittivo. Esistono vari tipi di MAC, basati su principi diversi, e sono:

- la contesa;
- il token;
- la prenotazione;
- round-robin.

Il MAC è indispensabile in quanto a livello 2 (Data Link) le LAN implementano sempre una sottorete trasmittiva di tipo broadcast in cui ogni sistema riceve tutti i frame inviati dagli altri. Trasmettere in broadcast, cioè far condividere un unico canale trasmittivo a tutti i sistemi, implica la soluzione di due problemi:

- in trasmissione, verificare che il canale sia libero prima di trasmettere e risolvere eventuali conflitti di più sistemi che vogliono utilizzare contemporaneamente il canale;
- in ricezione, determinare a quali sistemi è effettivamente destinato il messaggio e quale sistema lo ha generato.

La soluzione del primo problema è data dai vari algoritmi di MAC che, per poter soddisfare il requisito "apparecchiature indipendenti", devono essere algoritmi distribuiti su vari sistemi e non necessitare di un sistema master.

La soluzione del secondo problema implica la presenza di indirizzi a livello MAC (quindi nella MAC-PDU) che trasformino trasmissioni broadcast in:

- trasmissioni punto-a-punto, se l'indirizzo di destinazione indica un singolo sistema;
- trasmissioni punto-gruppo, se l'indirizzo di destinazione indica un gruppo di sistemi;
- trasmissioni effettivamente broadcast, se l'indirizzo di destinazione indica tutti i sistemi.

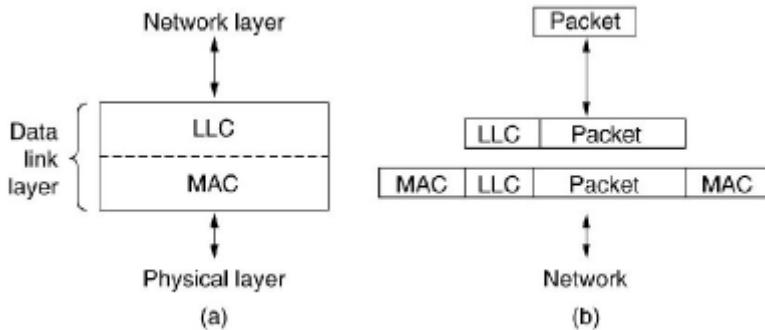
Il MAC deve anche tener conto della topologia della LAN, che implica leggere variazioni sulle possibili modalità di realizzazione del broadcast: con topologie a bus, è un broadcast a livello fisico (elettrico), mentre con topologie utilizzanti canali punto-a-punto, quali l'anello, è un broadcast di tipo logico. Le reti locali hanno canali sufficientemente affidabili, quindi non è in genere necessario effettuare correzione degli errori. Se ciò fosse richiesto, sarebbe il sottolivello LLC ad occuparsene essendo il MAC sempre connectionless.

Nelle reti locali, al livello 2 OSI, sono presenti due tipi di PDU (*Protocol Data Unit è l'unità d'informazione o pacchetto scambiata tra due peer entities in un protocollo di comunicazione di un'architettura di rete a strati.*) corrispondenti ai due sottolivelli LLC e MAC. Il formato della LLC-PDU è comune a tutte le reti locali, mentre quello della MAC-PDU è peculiare di ogni singolo MAC. Tuttavia alcuni campi principali, rappresentati in figura, sono presenti in tutte le MAC-PDU. In particolare una MAC-PDU contiene due indirizzi(SAP), uno di mittente (**MAC-SSAP**) e uno di destinatario (**MAC-DSAP**), un campo INFO contenente la LLC-PDU (cioè il pacchetto di livello LLC) e una FCS (*Frame Control Sequence*) su 32 bit, cioè un codice a ridondanza ciclica (CRC) per l'identificazione di errori di trasmissione.

MAC-DSAP	MAC-SSAP	INFO	
Indirizzo di destinazione	Indirizzo di mittente	LLC PDU	FCS

Che cos'è l' LLC?

I protocolli MAC visti fin qui non esauriscono le funzioni del data link layer. Le specifiche dei protocolli MAC devono essere filtrate per poter offrire allo strato di rete una interfaccia analoga ai protocolli delle linee punto-punto. IEEE ha definito le specifiche di un sottostrato del data link layer che fornisce verso l'alto questa interfaccia, appoggiandosi sopra il sottostrato MAC: il Logical Link Control.



La funzione principale del LLC definito da IEEE e' di mascherare allo strato di rete le specifiche dei protocolli 802 utilizzati a livello di MAC, in modo da offrire allo strato superiore una interfaccia uniforme. Un esempio del suo utilizzo e' quello di implementare un servizio orientato alla connessione, o non connesso ma affidabile per la comunicazione a livello 2. Lo strato di rete passa i suoi dati al LLC, che aggiunge un suo header con le informazioni di numerazione del frame, riscontro etc. Quindi il LLC passa al sottostrato MAC il campo dati che il MAC gestisce con le sue specifiche. In ricezione il MAC recapita il frame all' LLC che rimuove l'header e passa i dati allo strato di rete. Il formato dell'header ed i meccanismi di funzionamento del LLC ricalcano quelli dell'HDLC(**High-Level Data Link Control**, controllo collegamento dati ad alto livello, è un protocollo di rete del livello data link).

IEEE 802.2 è lo standard del sottolivello LLC. Esso definisce sia i servizi forniti dal livello LLC, sia il protocollo che li implementa. LLC ha lo scopo di fornire un'interfaccia unificata con il livello network, il più simile possibile a quella delle reti geografiche. Per queste ultime l'OSI ha accettato come standard i protocolli della famiglia HDLC e quindi LLC è stato progettato come una variante di HDLC per le reti locali.

LLC ha una sua PDU (*LLC-PDU*), illustrato in figura.

DESTINATION ADDRESS	SOURCE ADDRESS	CONTROL	INFORMATION
1 OTTETTO	1 OTTETTO	1 o 2 OTTETTI	m OTTETTI

Si osservi che nel contesto dei protocolli per reti locali si suole usare il termine ottetto al posto di byte.

In funzione dei valori assunti dal campo control, si distinguono tre tipi di PDU di cui il primo è il più importante:

- *Unnumbered PDU* (U-PDU). Si utilizzano per trasportare i dati di utente (nella modalità non connessa) per scopi di inizializzazione e per ragioni diagnostiche;
- *Information PDU* (I-PDU). Sono usate nella modalità connessa per trasportare i dati di utente;
- *Supervisory PDU* (S-PDU). Sono usate nella modalità connessa per trasportare le informazioni di controllo del protocollo.

LLC offre al livello Network tre tipi di servizi:

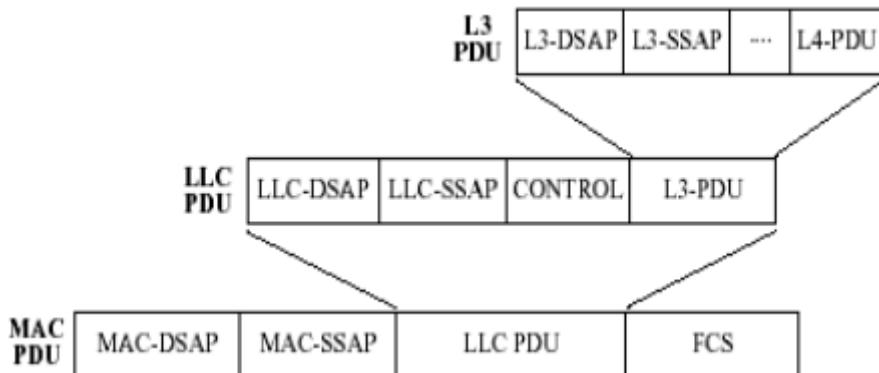
- *Unacknowledged connectionless service* (LLC Type 1). In questa modalità il trasferimento dati è non connesso senza conferma. È la modalità preferita da molte architetture di rete proprietarie tra cui DECnet e TCP/IP;
- *Connection oriented service* (LLC Type 2). Questa modalità crea dei circuiti virtuali tra

mittenti e destinatari prima di effettuare la trasmissione. È una modalità connessa, molto spesso adottata nelle architetture di rete IBM;

- *Semireliable service* (LLC Type 3). In questa modalità il trasferimento dati è non connesso, ma con conferma. È una modalità pensata per i protocolli da utilizzarsi in ambito di fabbrica.

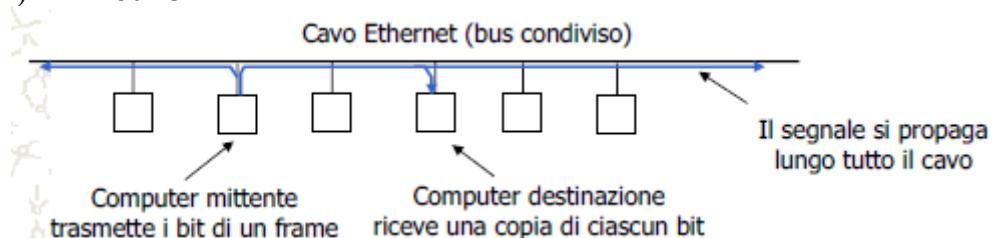
Relazione tra LLC e MAC

Ogni interfaccia di rete locale è gestita da un suo livello MAC. Su tale livello MAC si appoggia un livello LLC. Il livello MAC è implementato nell'hardware della scheda di rete locale, mentre il livello LLC è di solito realizzato in software. Ogni livello LLC può gestire un solo livello MAC: questo significa che un livello LLC non può avere funzionalità di "relaying" (non può inoltrare pacchetti) tra più MAC. Tale funzionalità di instradamento dei pacchetti è delegata al livello 3.

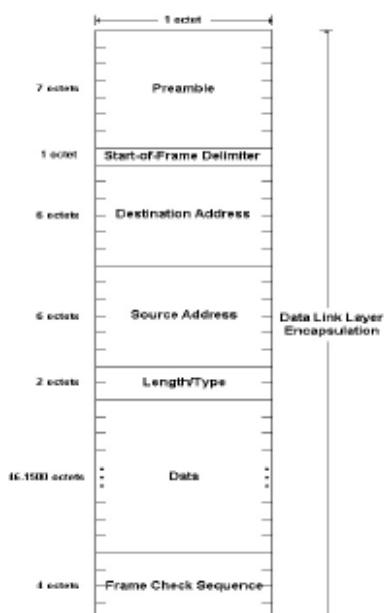


STANDARD IEEE 802.3 E ETHERNET

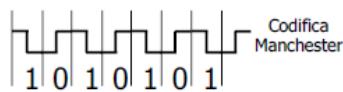
Standard per una LAN CSMA/CD 1-persistente (fino a 100Mbps), se si cambia velocità di trasmissione le uniche modifiche sono effettuate sul MAC. Ethernet è un prodotto che implementa (più o meno) IEEE 802.3.



Di seguito sarà descritto il formato del grame IEEE 802.3:



Preambolo (7 byte): vengono trasmessi 7 byte 10101010. Produce un'onda quadra a 10MHz per 5.6µs (56 bit x 0,1 µs/bit) Permette la sincronizzazione del clock del mittente e del ricevente.

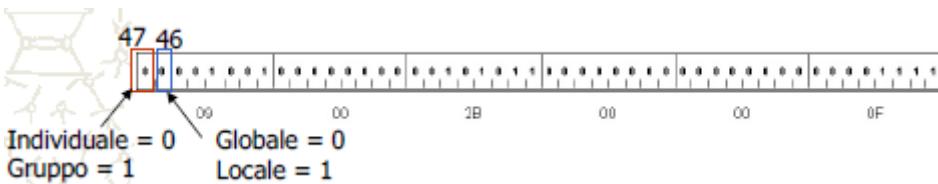


Start of frame (1 byte): Vale 10101011, indica l'inizio del pacchetto.

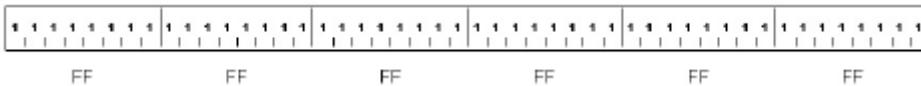
Indirizzi: Seguono due campi di indirizzo relativi alla destinazione ed alla sorgente del grame costituiti da 2 blocchi da 6 byte.

Come funziona l'indirizzamento su Ethernet?

Gli indirizzi sono rappresentati su 6 byte (48 bit). Il frame contiene l'indirizzo del mittente e del destinatario.



Il bit IG definisce se il frame è indirizzato ad una singola stazione (unicast) o a un gruppo di stazioni (multicast). Un indirizzo composto da tutti 1 è riservato per il broadcast (il frame è ricevuto da tutte le stazioni).



Tutte le stazioni vedono il frame e lo accettano se l'indirizzo destinazione è compatibile con quello a loro assegnato. Se la trasmissione è unicast solo la stazione con l'indirizzo specificato nel campo destinazione del frame accetta il pacchetto. Le altre stazioni lo scartano, il riconoscimento dell'indirizzo è a livello hardware. Se l'interfaccia è configurata in modo promiscuo, accetta tutti i pacchetti (snoop di rete). Quindi possiamo dire che il MAC address è un indirizzo di 48 bit in binario, ma per convenzione viene letto o in esadecimale dividendo con ":" ogni coppia di numero, oppure sempre in esadecimale ma in gruppi di quattro separati da un punto; Es:

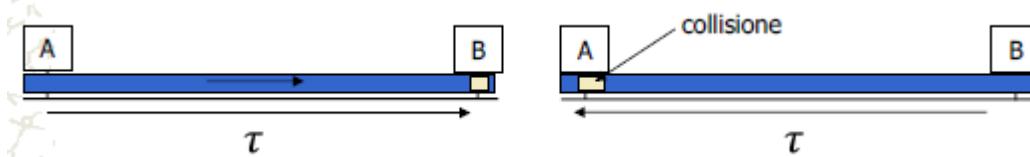
1. **00:15:4C:1E:01:00**
2. **0015.4C1E.0100**

Il bit 46 distingue gli indirizzi locali da quelli globali. Gli indirizzi globali sono assegnati dalla IEEE per assicurare l'unicità degli indirizzi. Con il MAC address possiamo infatti distinguere da una stazione ad un'altra quindi, non dobbiamo quindi mai avere due MAC uguali, perché altrimenti la situazione diventa ingestibile, e non può essere risolta a livello di protocollo ma soltanto a livello di legge impedendo ai costruttori di associare due MAC uguali in dispositivi diversi.

Campo di tipo: Segue un campo di 2 byte che serve ad indicare al ricevente cosa deve fare del frame ricevuto, generalmente il livello 2 viene utilizzato da più protocolli dello strato di rete simultaneamente, il campo type indica al ricevente a quale processo deve essere recapitato il frame.

Data(payload): Il campo dati trasporta le informazioni del protocollo di livello 3 ed ha dimensione variabile, con un limite superiore. Hanno una dimensione minima di 46 byte per poter avere il giusto tempo di ricevere il segnale di τ_{au} . Hanno una dimensione massima di 1500 byte, e fa sì che la lunghezza massima del frame Ethernet sia 1518 byte (preamble elencato), il valore massimo è determinato dal fatto che il transceiver deve ospitare l'intero frame in RAM, ed al momento della definizione dello standard la RAM era più costosa di oggi. Lo standard prevede che un frame Ethernet non possa essere inferiore a 64 byte. In caso di necessità il campo dati è seguito da un campo di riempimento costituito da tutti 0 per fare in modo che la somma dati+riempimento sia di almeno 46 byte, è compito dei livelli superiori forzare il campo dati ad essere almeno di 46 byte, od introdurre un indicatore di lunghezza per discriminare i dati dal riempimento.

Lunghezza del frame: un frame valido deve essere lungo almeno 64 byte. Se si tolgono i 6+6 riservati agli indirizzi, i 2 per il campo length e i 4 del checksum, il campo dati deve avere almeno 46 byte (eventuale padding). La lunghezza minima di un pacchetto deve garantire che la trasmissione non termini prima che il primo bit abbia raggiunto l'estremità più lontana e sia tornata indietro una eventuale collisione (per rilevare la collisione).



Per una LAN a 10Mbps di 2.5 Km con 4 ripetitori un pacchetto deve durare almeno 51.2 μ s (64 byte).

Prestazioni di Ethernet

Come gli altri protocolli CSMA anche Ethernet presenta le seguenti caratteristiche:

- in condizioni di basso carico i tempi di ritardo sono contenuti e l'efficienza assomiglia al CSMA 1-persistente con la miglioria legata al fatto che c'e' rilevazione della collisione;
- in condizioni di carico elevato crescono le collisioni, ma l'algoritmo di backoff esponenziale fa sì che le stazioni mutino il loro comportamento rendendo il protocollo simile ad un CSMA p-persistente con p sempre piu' piccolo;
- quindi al crescere del carico l'andamento dell'efficienza tende ad appiattirsi su una percentuale di valore non nullo;
- c'e' una forte dipendenza dalla dimensione media dei frame trasmessi; piu' piccolo e' il frame, piu' pesa l'overhead del periodo di contesa rispetto al periodo di trasmissione riuscita.

Che cos'è una prestazione?

- Analisi approssimata a carico costante
- Probabilità costante p di ritrasmissione per ogni slot
- k stazioni sempre pronte a trasmettere
- A è la probabilità che una stazione acquisisca il canale

$$A = k p (1-p)^{k-1}$$

Probabilità che:
 • una stazione trasmetta
 • le altre k-1 no
 • per ogni stazione disponibile (k)

- A è massima per $p=1/k$ [$A = (1-1/k)^{k-1}$]
- La probabilità che si abbiano j slot di contesa è

$$A (1-A)^{j-1}$$

Probabilità che:
 • trasmissione nello slot j
 • fallimento nei j-1 slot precedenti

Il numero medio di slot di contesa è $1/A$. Ogni slot ha durata $2t$ quindi l'intervallo medio di contesa

$$\text{è } 2t/A. \text{ Se un frame medio impiega } P \text{ per la trasmissione, l'efficienza del canale è : } E = \frac{P}{P + (2 \frac{t}{A})}$$

Diminuisce con la lunghezza della linea(t). Aumenta con la dimensione F del frame($P = F/B$). Decresce con il numero di stazioni pronte a trasmettere (carico). Più stazioni si aggiungono e più il traffico aumenta fino a saturare la LAN.

Tecnologie Ethernet

L'insieme di protocolli Ethernet domina tuttora saldamente il mercato delle LAN. La velocità di trasmissione originariamente era 10 Mbit/s su cavo coassiale. Ethernet è evoluta su diversi mezzi trasmissivi (coassiale, doppino, fibra) fino a 10 Gbit/s (Gigabit Ethernet), passando da trasmissioni nel dominio elettrico a trasmissioni su fibra. Ethernet, alle diverse velocità e per i diversi mezzi trasmissivi, è sempre stata standardizzata per permettere schede di interfaccia a basso costo, pensate per essere utilizzate in un PC.

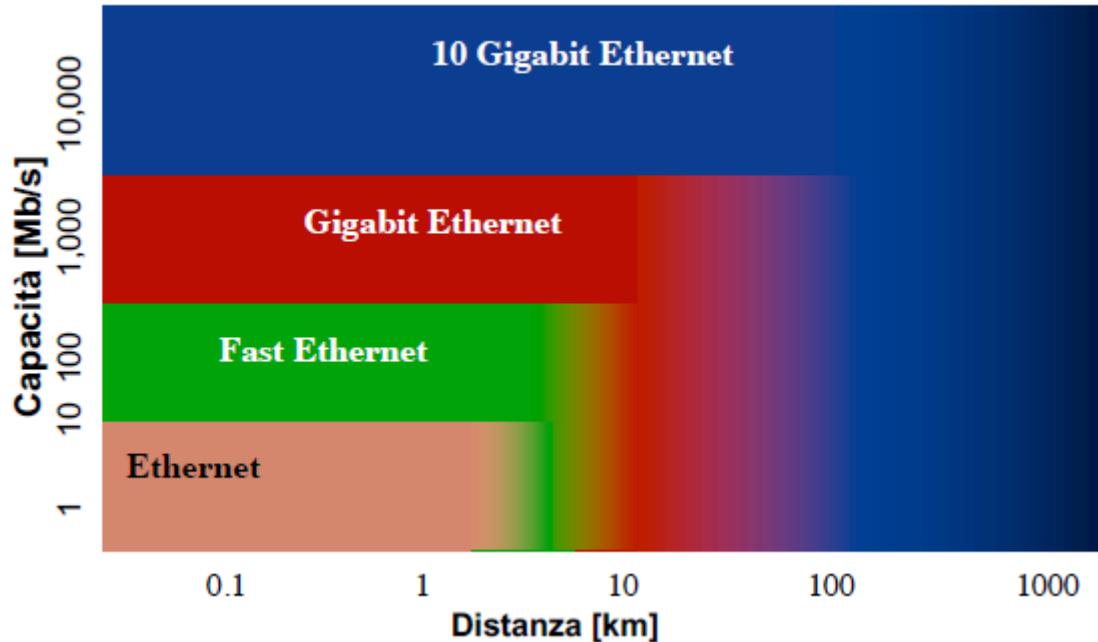
Abbiamo diversi tipi di Ethernet (10, 100, 1000, ... Mb/s), le sue caratteristiche sono:

- Banda confrontabile con la velocità interna dei terminali;
- Cavo coassiale condiviso;
- Distanza limitata (~ 1 km) da attenuazione e ritardi di propagazione;
- Bassi costi dovuti a semplicità ed economia di scala;
- Hub o switch: banda e cavi condivisi o dedicati ai terminali.

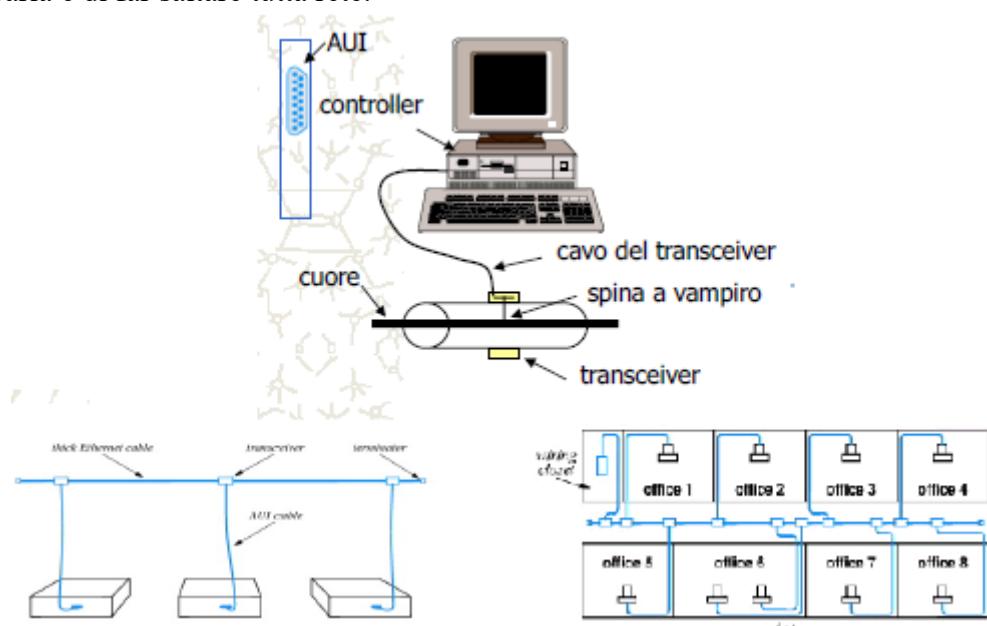
Nota domanda di esame: un ripetitore è un dispositivo di che tipo? È un dispositivo di livello fisico.

Sul mezzo condiviso la condizione di “**assenza di trasmissione**” e’ necessariamente identificata da assenza di segnale. Non sono quindi possibili codifiche che utilizzino il segnale a 0 volt per identificare un bit. La necessita’ di trasferire l’informazione di clock assieme al segnale ha portato alla invenzione della codifica Manchester già vista. Lo standard Ethernet utilizza la codifica Manchester con segnali a +0.85 V e -0.85 V (altri protocolli, come token ring, fanno uso della codifica Manchester differenziale).

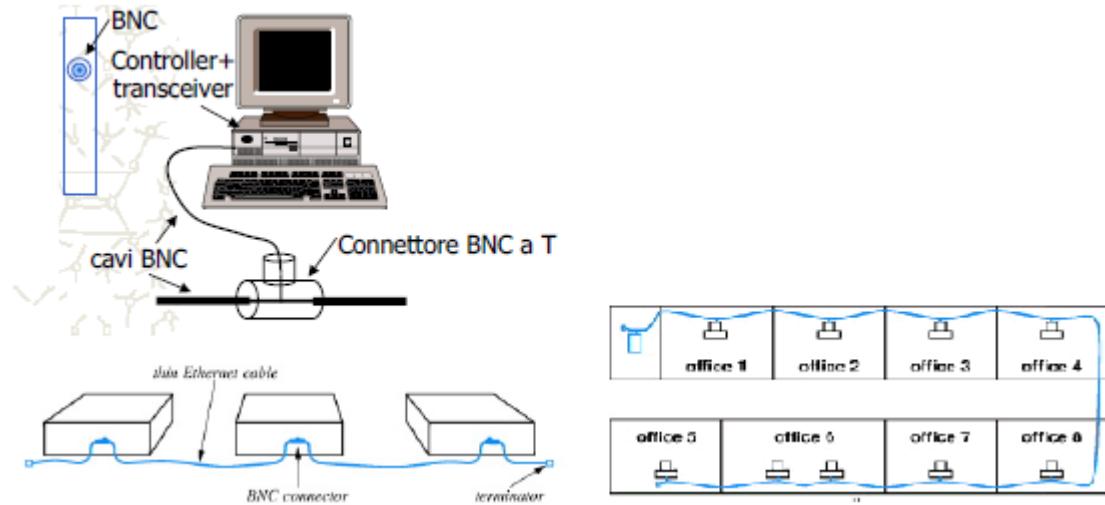
Evoluzione di Ethernet



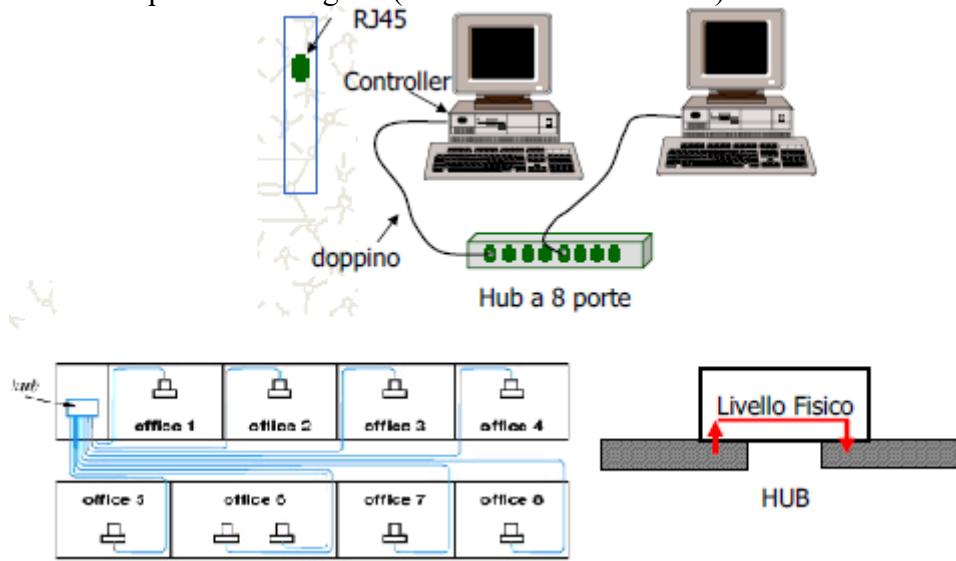
- **10Base5:** Thick Ethernet. Cavo giallo con tacche ogni 2.5 m a indicare i punti di aggancio delle spine. Il transceiver è un circuito elettronico che rileva la portante e le collisioni. Il cavo del transceiver ha 5 doppini schermati (dati in ingresso, dati in uscita, controllo in e out, alimentazione). Era detto sistema a vampiro perché per avere la connessione bisognava bucare il cavo fino ad arrivare all'anima e toccarla, se non si stava attento si rischiava di bucarla e di far saltare tutta rete.



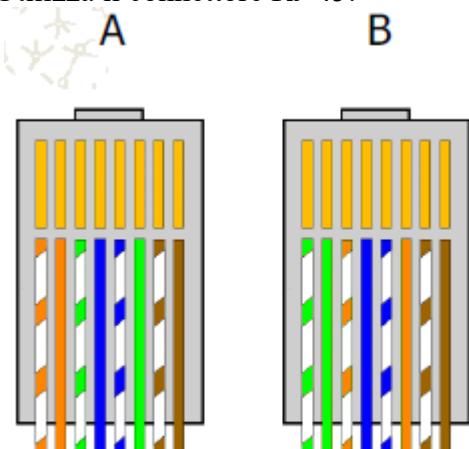
- **10Base2:** Thin Ethernet, il cavo è flessibile, il transceiver è in generale sul controller.



- **10BaseT:** Topologia a stella, la manutenzione è molto semplice. Distanza massima dall'hub = 100m. Tutte le stazioni collegate ad un hub sono nello stesso dominio di collisione. Gli hub sono solo ripetitori del segnale (lavorano al livello fisico).



Utilizza il connettore RJ-45:



Pin	Signal	Description
1	RxD (+)	Receive Data (+)
2	RxD (-)	Receive Data (-)
3	TxD (+)	Transmit Data (+)
4	NC	
5	NC	
6	TxD (-)	Transmit Data (-)
7	NC	
8	NC	

Fast Ethernet

Riduce il tempo di bit a 100ns a 10ns. Tutti i sistemi Fast Ethernet usano Hub. Richiede una banda di 100 Mbd (100 Mbps codifica Manchester). Può essere di 3 tipi:

- **100Base-T4:** Utilizza una velocità di 25 MHz su 4 doppini cat 3. Un doppino trasmette verso l'hub, un doppino riceve dall'hub, due doppini sono orientabili a seconda del verso della trasmissione. Non utilizza codifica Manchester. Si utilizzano 3 livelli 0,1,2. Si trasmette un “trit” su 3 doppini (27 simboli = 4 bit + ridondanza). Si ha un canale nell'altro verso a 33.3 Mbps.
- **100Base-TX:** Utilizza una velocità di 125 MHz su 2 doppini cat 5 (full-duplex), un doppino trasmette verso l'hub e un doppino riceve dall'hub. Utilizza una codifica 4B5B (4 bit in 5 periodi di clock). 100 Mbps bidirezionali.
- **100Base-FX:** Utilizza due cavi di fibra multimodale (full-duplex). Un cavo trasmette verso l'hub e un cavo riceve dall'hub. 100 Mbps bidirezionali.

Gigabit Ethernet

Inizia ad eliminare il protocollo CSMA-CD, confinandolo solo ad alcuni apparati. Elimina anche i ripetitori iniziando ad usare apparati denominati switch. Usa il formato di trama contenuto nell' 802.3. Può operare in half duplex e full duplex. Backward compatibility con mezzi fisici già installati (fibre mono e multimodali, doppino). Aumenta di un fattore 10 la dimensione minima di pacchetto con padding di simboli speciali.

Su fibra si utilizza una codifica nota come 8B/10B: una sequenza di 8 bit è codificata utilizzando 10 bit: 1024 codeword per 8 bit: c'è margine per scegliere opportunamente le codeword in modo che non ci siano mai più di 4 bit uguali consecutivi e non ci siano mai più di sei 0 o sei 1, spesso una sequenza ha più codeword associate, e viene scelta la migliore in funzione delle precedenti inviate per mantenere alternanza tra 0 ed 1 ed annullare la componente continua che passa nell'elettronica di conversione ottico/elettrico. Su rame si utilizzano tutte le quattro coppie del cavo UTP in modalità duplex con un simbolo a 5 livelli ogni ciclo di clock trasmette 5 simboli per coppia: 2 bit più un bit usato per segnali di controllo si ciascuna coppia, in cui 8 bit per ciclo a 125 MHz danno il throughput di 1 Gbps. La modalità di trasmissione duplex si realizza con una elettronica complessa finalizzata al trattamento del segnale per separare l'ingresso dall'uscita.

IEEE 802.3z specifica tre tipi di interfacce fisiche:

- **1000Base LX:** fibra multimodale (10 km) o monomodale (500 m)
- **1000Base SX:** fibra multimodale (da 200 m ai 500 m)
- **1000Base CX:** cavo di rame schermato (non si usa per niente)
- **1000Base T:** cavo STP o UTP (doppino in rame con 4 coppie schermato o non), è molto usata.

La gigabit prevede le seguenti opzioni:

SX: short-wavelength (850 nm)

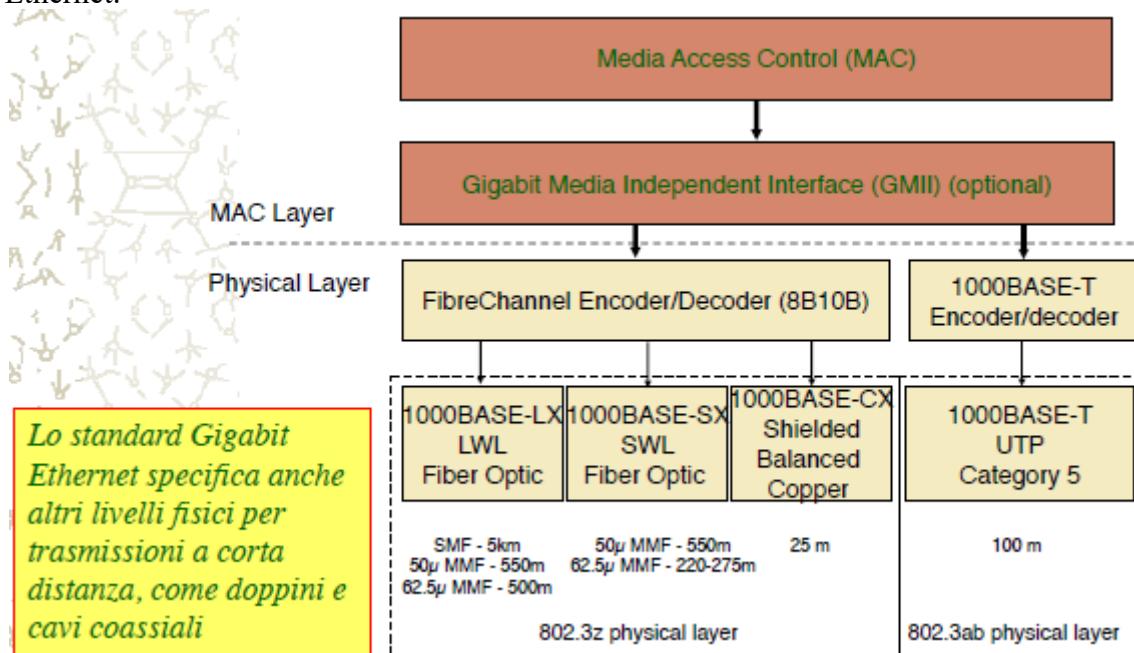
LX: long-wavelength (1300 nm)

standard	tipo di fibra	diametro (μm)	BW modale (MHz/km)	distanza minima (m)
1000BASESX (850 nm)	MM	62.5	160	2 to 220
	MM	62.5	200	2 to 275
	MM	50	400	2 to 500
	MM	50	500	2 to 550
1000BASELX (1300 nm)	MM	62.5	500	2 to 550
	MM	50	400	2 to 550
	MM	50	500	2 to 550
	SM	9	NA	2 to 10000

Quello che le differenza è il tipo di emettitore e ricevitore che si possono inserire nell'interfaccia, per poter personalizzare l'accesso (plag and play).

Poiché lo standard ammette la connessione di una stazione GE con una FE o Ethernet, è stato introdotto un meccanismo per il controllo di flusso a livello MAC. Lo switch comunica

all'interfaccia GE della stazione di sospendere le trasmissioni di frame utilizzando un frame Ethernet normale, con tipo 0x8808 (seguito da parametri nel campo dati, indicanti tra l'altro per quanto tempo sospendere la trasmissione). Un meccanismo analogo esiste nelle specifiche di Fast Ethernet.



La gigabit porta delle modifiche al protocollo; In modalità half duplex, slot minimo portato da 64 a 512 bytes (se ho pacchetti piccoli le prestazioni sono basse). Collision domain di 200 m. Solo topologie a stella. Consente la tecnica "frame bursting" per mantenere il controllo del canale fino ad un massimo di 8192 bytes (l'estensione della lunghezza minima del pacchetto è necessaria solo per il primo pacchetto). Fa uso anche del *buffered distributor*, Dispositivo che "remotizza" (rispetto al PC) il sottolivello MAC. Opera sempre in full duplex. Implementa un controllo di flusso tra il PC e il concentratore e memorizza localmente le trame fino a quando non riesce a trasmetterle. Rende la massima distanza delle stazioni indipendente dal protocollo.

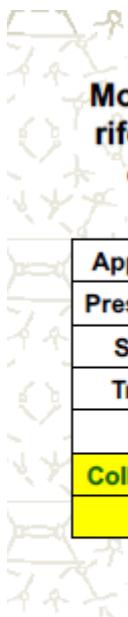
10 Gigabit Ethernet

Un comitato IEEE 802.3 è attivo nella standardizzazione di 10 Gbit/s Ethernet. Solo la modalità full duplex, senza CSMA-CD.

Soluzioni proposte:

- Seriale, con framing Ethernet, su distanze da LAN fino a 40 Km:
 - 650 m su fibra multimodo (MMF)
 - 300 m su MMF installata
 - 2 km su fibra monomodo (SMF)
 - 10 km su SMF
 - 40 km su SMF
- Seriale, su SONET, per distanze maggiori di 40 Km.

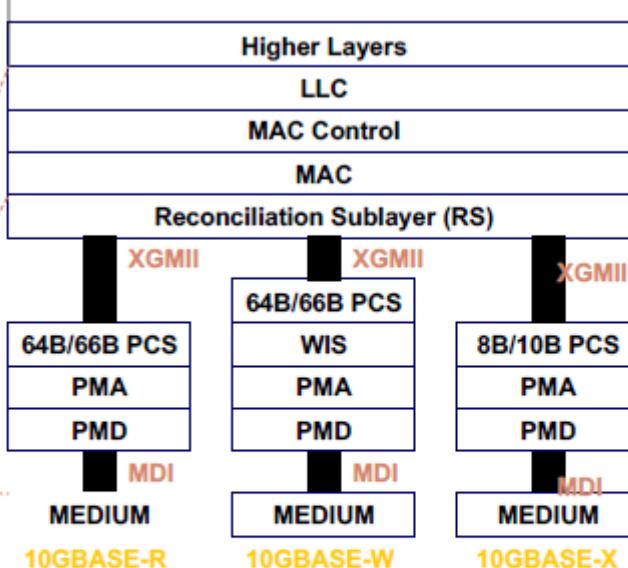
Fa uso dell' IEEE P802.3 ae. Mantiene il formato di trama di 802.3 Ethernet. Mantiene le dimensioni min/max del frame 802.3. Funziona solo in full duplex e supporta solo cavi in fibra ottica. L'interfaccia MAC-PHY arriva fino a 10.0 Gbps. In un ambiente LAN PHY la capacità dell'ambiente è di 10 Gbps, mentre in WAN PHY di ~ 9.29 Gbps (compatibile con SONET).



Modello di riferimento o OSI

Applicazione
Presentazione
Sessione
Trasporto
Rete
Collegamento
Fisico

Livelli P802.3ae



MDI = Medium Dependent Interface

XGMII = 10 Gigabit Media Independent Interface

PCS = Physical Coding Sublayer

PMA = Physical Medium Attachment

PMD = Physical Medium Dependent

WIS = WAN Interface Sublayer

10GBASE-R: collegamenti su fibra punto punto

10GBASE-W: compatibile con standard SONET

10GBASE-X: usa WDM, 4 λ a 2.5G in parallelo

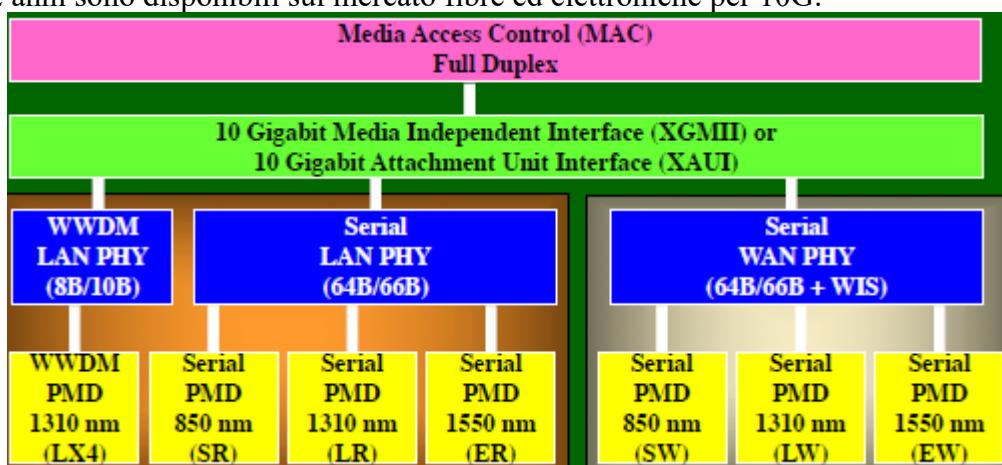
Esiste anche la 10G su fibra : IEEE 802.3 ae 10GbaseF:

Pubblicata nel Febbraio 2002 - 4 tipologie su fibra:

- **10GBASE-SR** (fino a 300m con fibre multimodali XG)
- **10GBASE-LX4** (fino a 300m fibre multimodali 50- e 62.5-micron)
- **10GBASE-LR** (fino a 10km con fibre monomodali)
- **10GBASE-ER** (fino a 40km con fibre monomodali)

L'ISO ha pubblicato ISO11801, 2nd Edizione nel Settembre 2002: Fibre OM-1, OM-2, OM-3 e OS-1

Da oltre 2 anni sono disponibili sul mercato fibre ed elettroniche per 10G:



Ecco una tassonomia dei principali standards con le loro limitazioni in distanza

Nome	Cavo	Max segmento	Nodi/segmento
10Base5	coassiale grosso	500m	100
10Base2	coassiale sottile	200m	30
10Base-T	doppino	100m	1024
10Base-FL	fibra ottica	2000m	1024

Nome	Cavo	Max segmento
100Base-T4	4 doppini cat 3	100m
100Base-TX	doppino cat 5	100m
100Base-FX	fibra ottica	2000m

100 Mbps (fast Ethernet)

10 Mbps

Nome	Cavo	Max segmento
10GBASE-SR	fibra ottica multimode	300m
10GBASE-LX4	fibra ottica multimode	300m
10GBASE-LR	fibra ottica singemode	10Km
10GBASE-ER	fibra ottica singemode	40Km

Nome	Cavo	Max segmento
1000Base-T	4 doppini cat 5e	100m
1000Base-SX	fibra ottica multimode	220m
1000Base-LX	fibra ottica multimode	500m
1000Base-LX	fibra ottica singemode	10Km

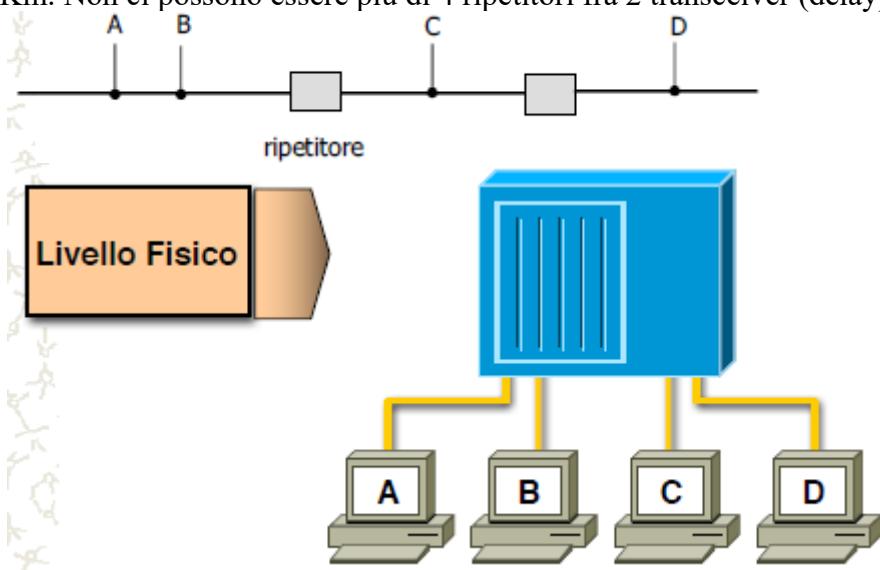
1000 Mbps (Giga Ethernet)

10000 Mbps (10 Giga Ethernet)

All fine della giostra la rete ethernet ha vinto perché i suoi costi di implementazione sono molto bassi.

Repeater e Hub:

Per costruire reti più ampie diversi cavi possono essere connessi con ripetitori. Un ripetitore opera al livello fisico amplificando e ritrasmettendo il segnale in modo bidirezionale. 2 transceiver (dispositivo che è in grado sia di trasmettere che di ricevere) non possono essere distanti più di 2.5 Km. Non ci possono essere più di 4 ripetitori fra 2 transceiver (delay).



- Tutti I dispositivi nello stesso dominio di collisione
- Tutti I dispositivi nello stesso dominio di broadcast
- Tutti I dispositivi condividono la banda

Dominio di broadcast: un indirizzo con tutti 1, che viene recepito da tutte le macchine aggregate sullo stesso segmento di rete. Il dominio di collisione e broadcast non condividono. Si deve infatti diminuire le collisioni su una rete. Man mano che aumentano le stazioni aumentano le collisioni.

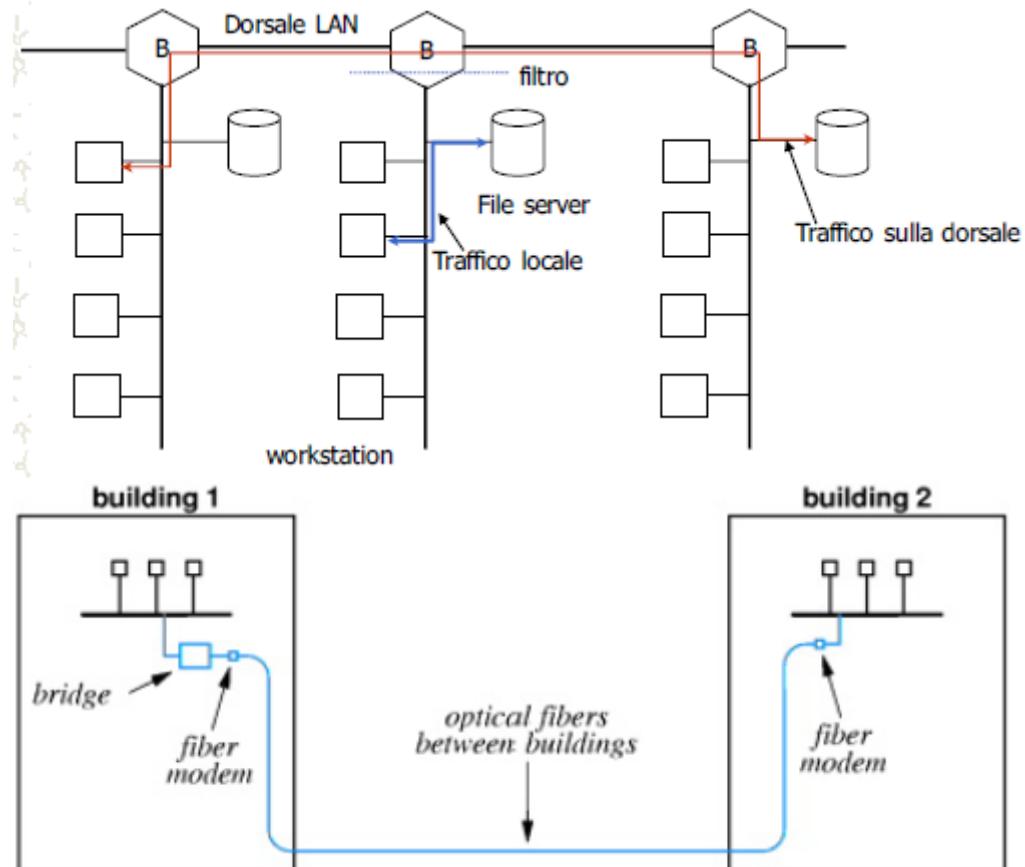
Usi di CSMA/CD, e limita le dimensioni della rete.

Bridge

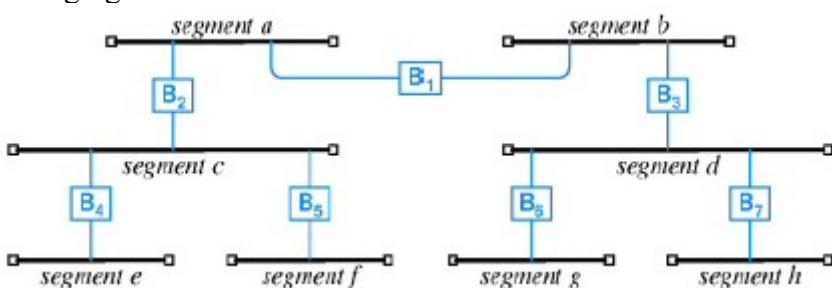
Bridge e *Switch* permettono di connettere più LAN mantenendo la suddivisione a livello data link. Si possono collegare LAN operanti con protocolli diversi. Si creano domini di collisione separati diminuendo il carico di ciascuna sottorete (il traffico locale rimane confinato nella sottorete). Si può aumentare la dimensione della LAN (es. lunghezza delle linee) frazionando la rete in segmenti. Si confinano i malfunzionamenti dovuti a stazioni difettose. Aumentano la sicurezza dei dati - uso "malizioso" del modo promiscuo (il traffico interno ad una sottorete non è visibile dalle altre collegate con bridge/switch).

Separazione di più laboratori con traffico interno intenso. Rende possibile più trasmissioni contemporanee che non interessano gli stessi segmenti.

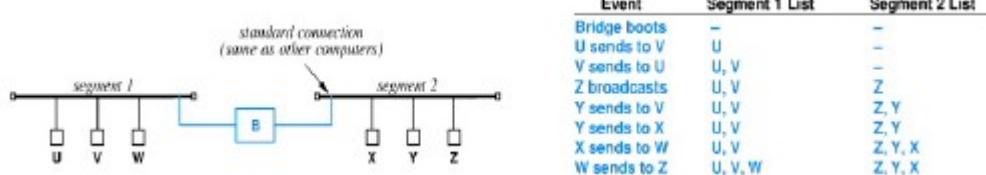
ES:



Brindging di rete ad albero:



Il bridging tipicamente è trasparante. Riduce il traffico sulla rete e impara da solo come è fatta. Il bridge osserva in modo promiscuo il traffico delle LAN a cui è connesso. Osservando il traffico costruisce una tabella hash interna (**MAC addressable**) che associa ogni indirizzo MAC alla porta corrispondente del bridge (**backward learning**). Con la tabella il bridge decide se scartare il frame (la destinazione è la stessa porta di arrivo) o ritrasmetterlo su un'altra linea.



Switches

Ha la stessa modalità di funzionamento del bridge. Ha un numero di porte superiore a 2 (es. 8, 12, 24). Ogni porta può essere collegata a un segmento della rete o a una stazione singola. Uno switch è funzionalmente equivalente a un bridge multi-porta.

NOTA: Il bridge opera principalmente sulla parte software, mentre lo switch sulla parte hardware. Lo switch opera col protocollo 802.3.

Separa la rete in n-domini di collisione, ma non separa i domini di broadcast. Ogni segmento individua un dominio di collisione. Tutti i segmenti sono sullo stesso dominio di broadcast. Il dominio di collisione è confinato alla singola porta (fra switch e dispositivo). In caso di trasmissione **full-duplex** non ci saranno collisioni dato che il dispositivo collegato e lo switch possono inviare e ricevere allo stesso tempo.

Come funziona? Apprendimento della topologia

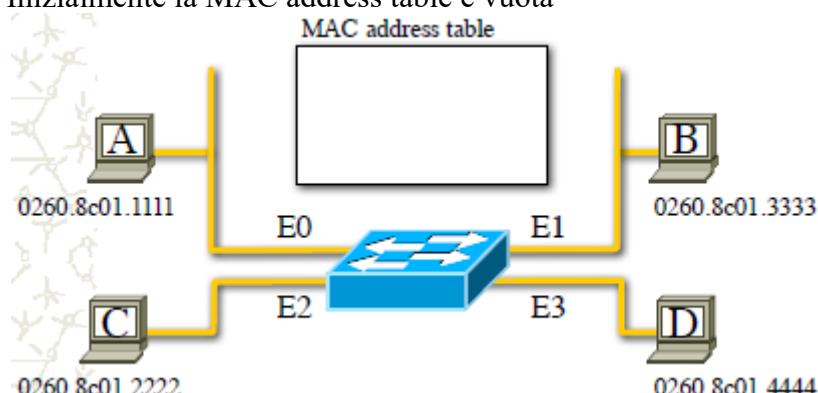
Per sapere su quale porta debba essere trasmesso il frame, lo switch deve creare e mantenere aggiornata una tabella relativa alla associazione tra indirizzo di destinazione e porta. La costruzione manuale di questa tabella sarebbe troppo costosa in termini di gestione della rete, ed è stato opportunamente inventato un meccanismo di auto apprendimento. Inizialmente questa tabella è vuota, e lo switch deve inoltrare ciascun frame ricevuto su tutte le porte connesse. Poiché i frame contengono l'indirizzo del mittente, ad ogni frame che arriva lo switch impara che la stazione che ha inviato il frame è raggiungibile attraverso la porta da cui è arrivato il frame stesso. Con il passare del tempo lo switch riempie la tabella e può svolgere la sua funzione in modo sempre più efficiente. Tutti i frame broadcast e multicast continueranno a dover essere trasmessi su tutte le porte connesse (tranne quella di provenienza), così come i frame destinati ad indirizzi non presenti nella tabella. L'aggiunta di stazioni connesse viene gestita dallo switch automaticamente attraverso il meccanismo di auto apprendimento.

Che cos'è il backward learning?

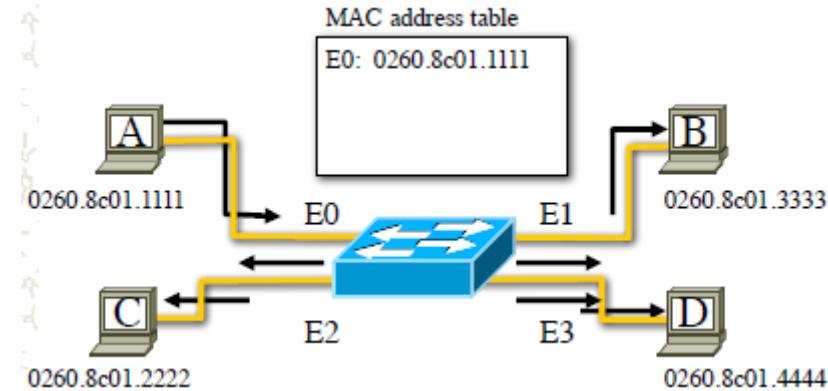
Al boot le tabelle sono vuote. Se un pacchetto ha una destinazione sconosciuta viene emesso su tutte le porte eccetto quella di provenienza. In ogni caso viene usato l'indirizzo di provenienza per definire la posizione del mittente nella tabella. Per gestire topologie dinamiche viene memorizzato anche il momento di arrivo dell'ultimo frame da un dato indirizzo. Periodicamente vengono eliminate le linee più vecchie. Dopo pochi messaggi le tabelle sono a regime e la struttura raggiunge la piena efficienza.

ES:

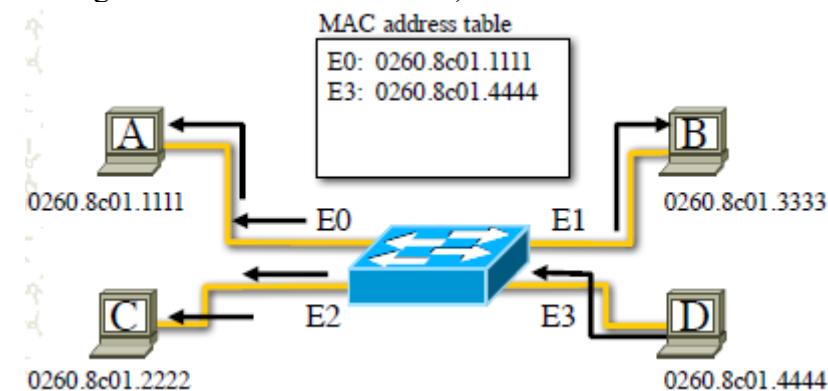
- Inizialmente la MAC address table è vuota



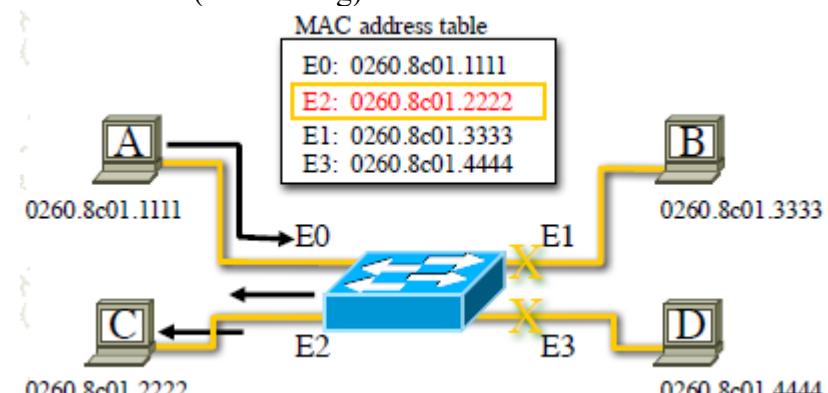
- La Stazione A invia una trama alla Stazione C. Lo Switch memorizza l'associazione fra il MAC address della stazione A e la porta E0 osservando l'indirizzo sorgente delle trame. La trama dalla stazione A alla stazione C è inviata su tutte le porte tranne la porta E0 (flooding verso gli indirizzi unicast non noti).



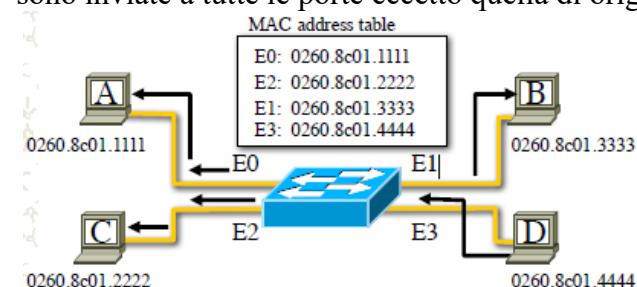
- La stazione D invia una trama alla stazione C. Lo Switch memorizza l'associazione fra il MAC address della stazione D e la porta E3 osservando l'indirizzo sorgente delle trame. La trama dalla stazione D alla stazione C è inviata su tutte le porte tranne la porta E3 (flooding verso gli indirizzi unicast non noti).



- La stazione D invia una trama alla stazione C. La destinazione è nota, la trama non viene inviata a tutti (no flooding).



- La stazione D invia una trama broadcast o multicast. Le trame broadcast e multicast frames sono inviate a tutte le porte eccetto quella di origine.



Differenze tra Bridging e Switching

Il Bridging:

- È essenzialmente software-based
- Una istanza di spanning-tree per bridge
- Tipicamente fino a 16 porte per bridge

LAN Switching

- Hardware based (ASIC : **application specific integrated circuit**)
- Multiple istanze di spanning-tree per bridge
- Un numero elevato di porte (dipende dalla fabric)

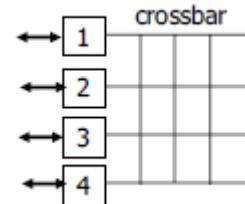
Tipi di switch

Abbiamo diversi tipi di switch con diverse tecnologie. Di seguito saranno elencati i tipi di switch:

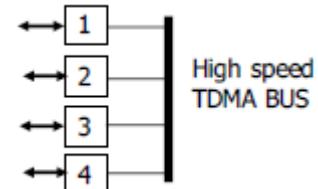
- **Cut-through switching**: Il frame è subito reindirizzato sulla porta corretta
- **Store-and-forward**: Il frame è letto completamente dallo switch. Viene controllato il CRC prima di inviarlo. In caso di errore il frame è scartato. Permette di filtrare il traffico.
- **Port-based switching**: Ad ogni porta corrisponde un solo indirizzo Ethernet.
- **Segment-based switching**: Ad ogni porta corrispondono più indirizzi (ad esempio è collegata ad un hub).

Le tecnologie che utilizzano invece sono le seguenti:

- **Shared Memory**: Memorizza i pacchetti in una memoria comune a tutte le porte. Invia i pacchetti in memoria alla porta destinazione.



- **Switching Matrix o Fabric**: Utilizza una matrice di commutazione. In base all'indirizzo e al contenuto della tabella viene attivata la connessione necessaria.

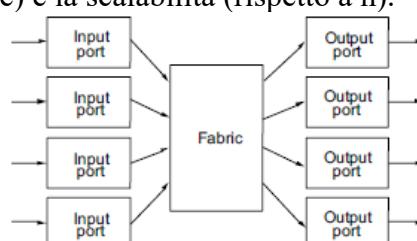


CARATTERISTICHE DEGLI SWITCH

Porte e Fabrics

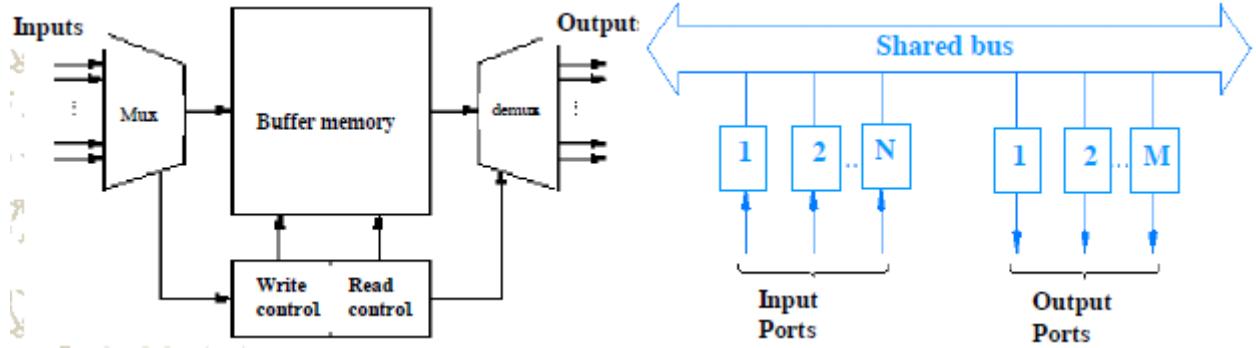
- **Porte**: Contengono le componenti elettriche o ottiche (circuiteria di controllo, hardware di interfaccia etc.) di trasmissione e ricezione. Prevedono meccanismi di bufferizzazione (cells) per le trame in attesa di trasmissione o ricezione.
- **Fabric**: Recapita le trame in input su una porta verso una di output. (più efficientemente possibile). Può effettuare bufferizzazione delle trame (*internal buffering fabric*).

Entrambe usano switch n x m, cioè n inputs e m outputs. L'obiettivo è quello di massimizzare il throughput (canale di comunicazione) e la scalabilità (rispetto a n).



Le caratteristiche dello *shared memory* e del *bus switch* sono quasi simili, infatti entrambi hanno:

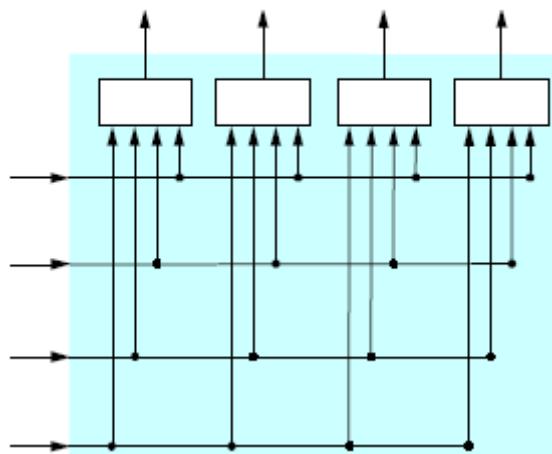
- Limitata scalabilità (le risorse condivise si saturano col carico)
- Grande disponibilità di spazio di bufferizzazione
- Realizzati tramite componenti COTS (es. PC)
- In grado di scrivere una trama alla volta in memoria o sul bus condiviso
- In presenza di n porte il trasferimento Mux-memoria deve essere n volte più veloce della capacità del link.



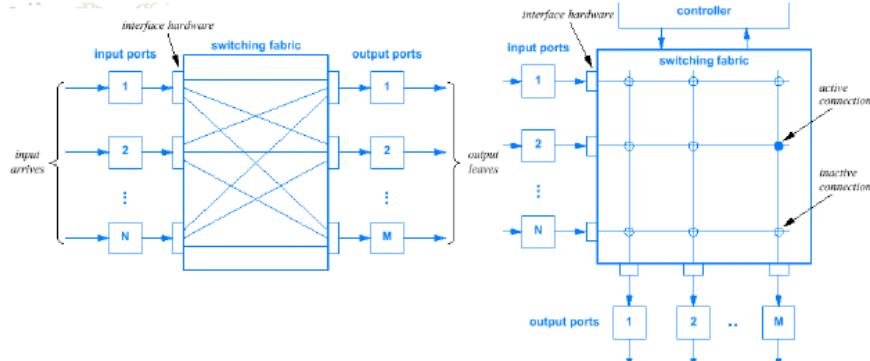
Invece le caratteristiche del *crossbar Switch* sono le seguenti:

- Concettualmente semplice (ogni input connesso a ogni possibile output).
- Possibili problemi di contesa (dipendenti dall'implementazione).
- La complessità delle porte di uscita aumenta più velocemente di quella delle porte in ingresso.
- Un crossbar switch “perfetto” può teoricamente commutare trame concorrentemente da tutte le n porte di input a tutte le m porte di output.

4X4 crossbar:

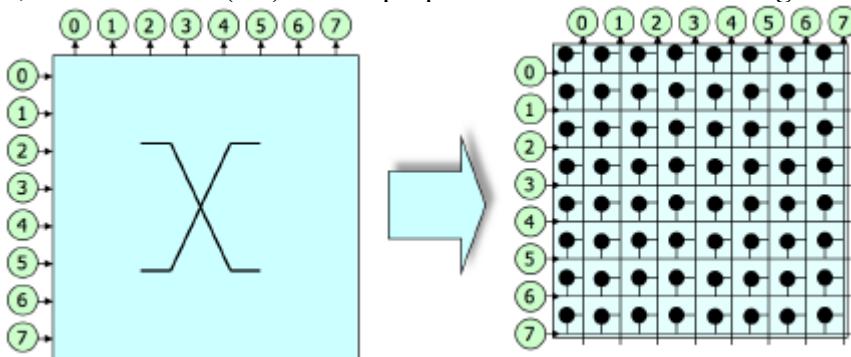


Possiamo dedurre quindi che il full fabric a differenza del crossbar è più vantaggioso perché tutti possono comunicare simultaneamente, ma c'è uno svantaggio cioè il costo dell'apparato.



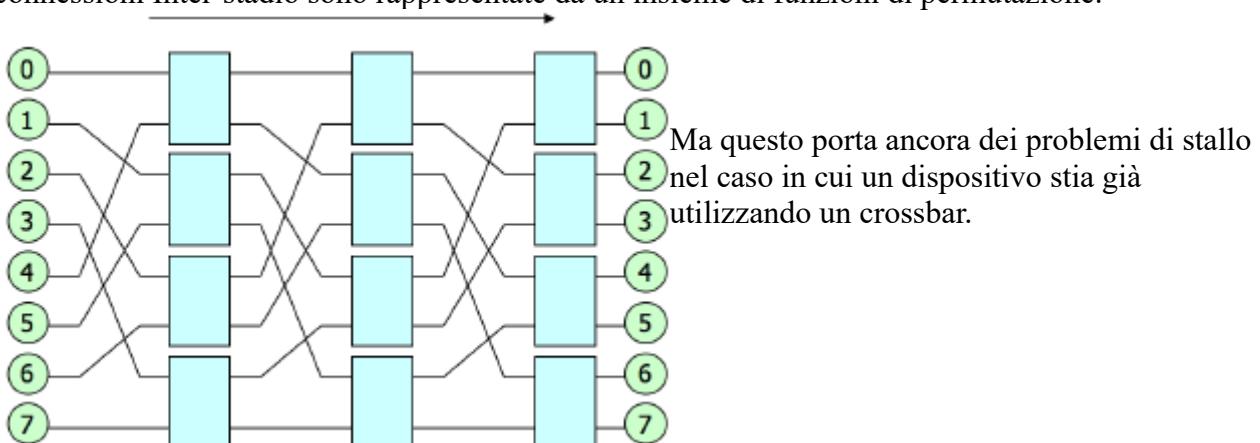
Crossbar Fabric a logica centralizzata

Logica di switching completamente centralizzata. Costo elevato dovuto al numero di switching points. La complessità della matrice cresce quadraticamente con il numero di porte di input/output ports, N , i.e., cresce come $O(N^2)$. Ha la proprietà di essere *non-blocking*.

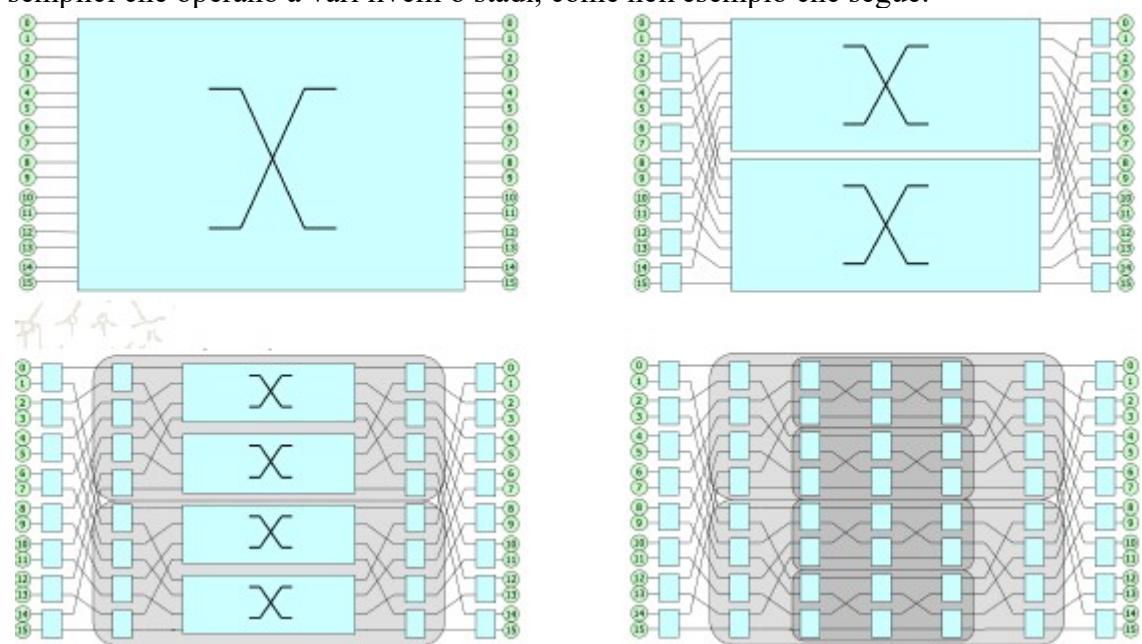


Un'alternativa è la **logica distribuita multistadio**:

Multistage interconnection network (MIN). Crossbar spezzata in diversi stadi che consistono di crossbars più piccole. La complessità cresce come $O(N \log N)$, dove N è il numero di porte. Le connessioni Inter-stadio sono rappresentate da un insieme di funzioni di permutazione.



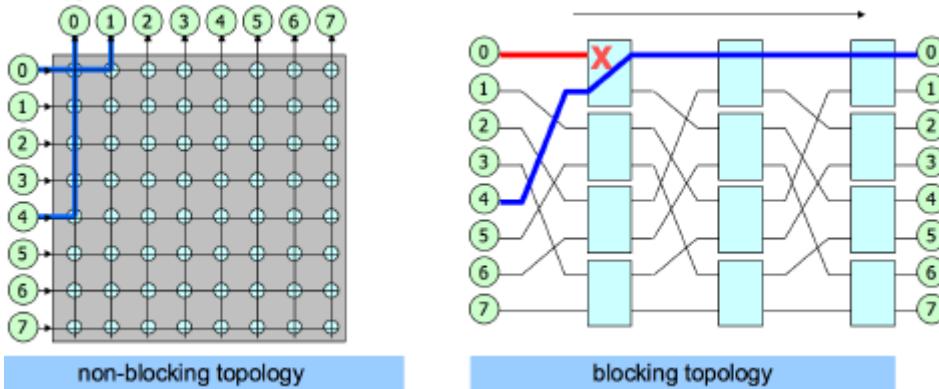
Quindi è possibile ridurre la complessità distribuendo la commutazione su multipli elementi più semplici che operano a vari livelli o stadi, come nell'esempio che segue:



Blocco e contesa

Riduzione del numero di switching points a discapito delle prestazioni:

- La topologia diventa potenzialmente *blocking*.
- Possono verificarsi fenomeni di *Contesa* in presenza di cammini dove differenti origini e destinazioni condividono uno o più linee.



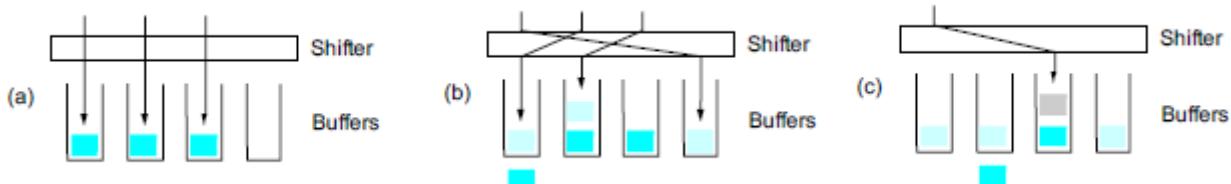
Si può ridurre con un meccanismo di **bufferizzazione**. Può ridurre il throughput (fino al 59% quando gli arrivi sono uniformemente distribuiti). È fondamentale per gestire la **QoS** (non si può sempre usare FIFO o RR). È indispensabile in presenza di possibili contese:

- Porte di input (contesa sulla fabric)
- fabric buffers interni (contesa sulle output ports)
- Porte di output (contesa sui links)

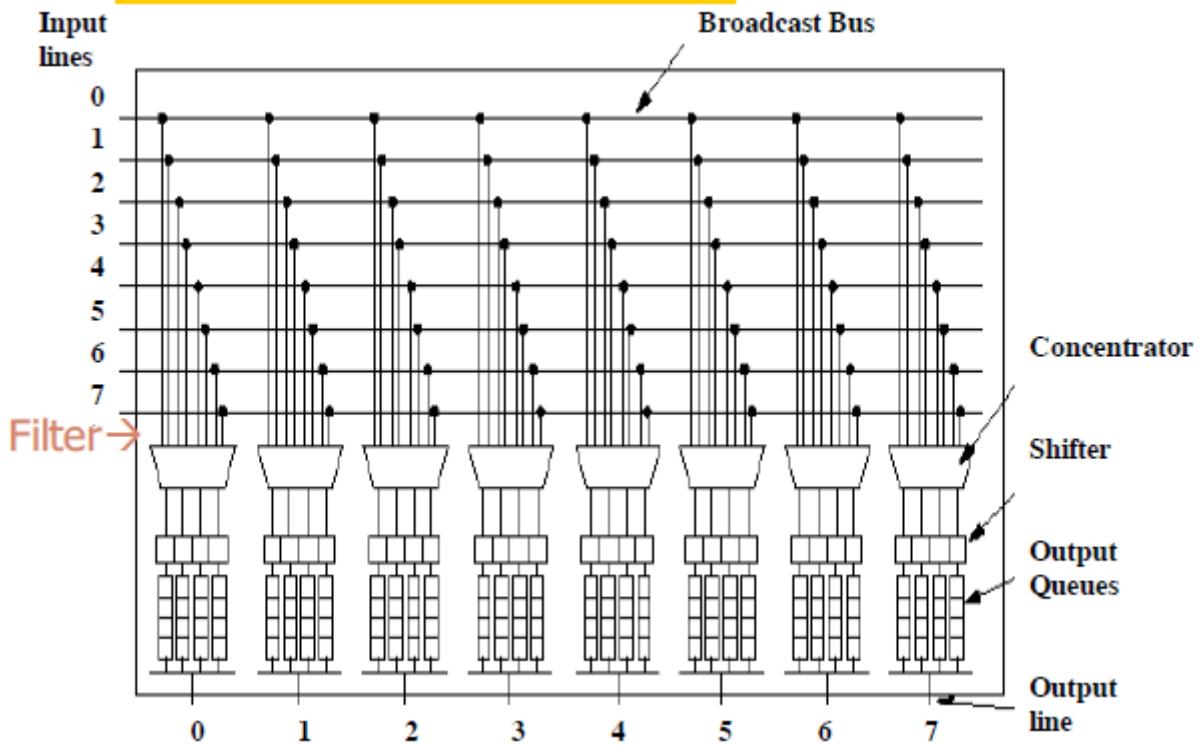


Ogni porta di output ha un buffer dedicato. I Buffers avengono riempiti in logica round-robin (da uno **shifter**). L'ordine di arrivo è preservato:

- (a) 3 packets arrive
- (b) 3 packets arrive, 1 leaves
- (c) 1 packet arrives, 1 leaves.

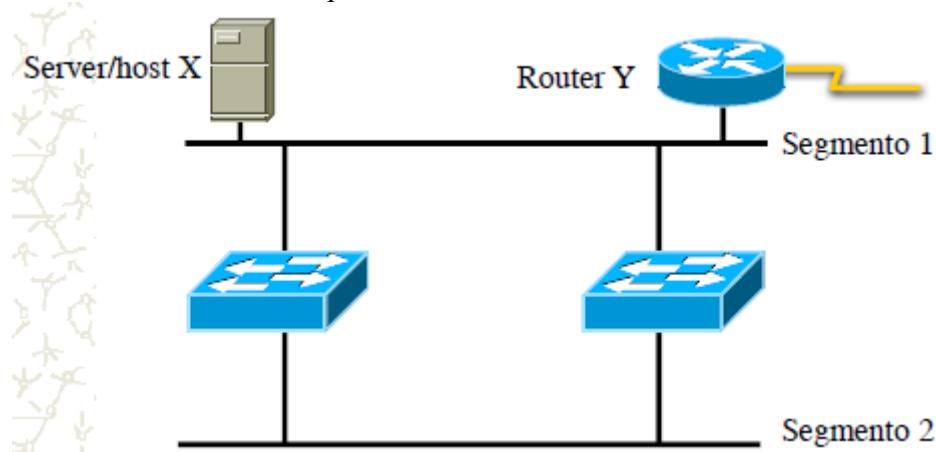


Crossbar Switch (Completo)



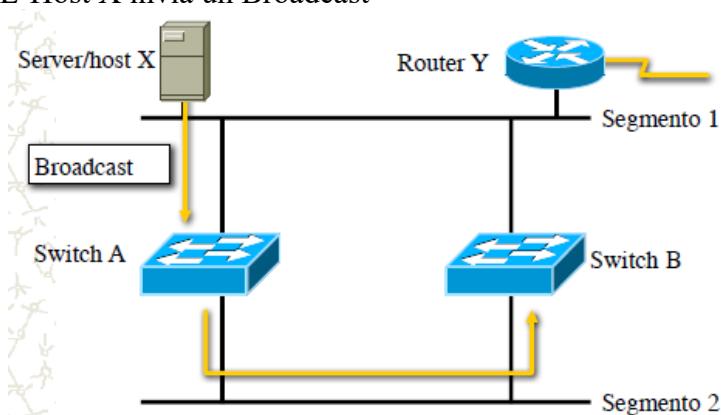
TOPOLOGIE CON RIDONDANZA

Topologie Ridondanti eliminano i single points of failure. In compenso possono essere causa di *broadcast storms*, *trame ripetute* e *instabilità del MAC address database*.

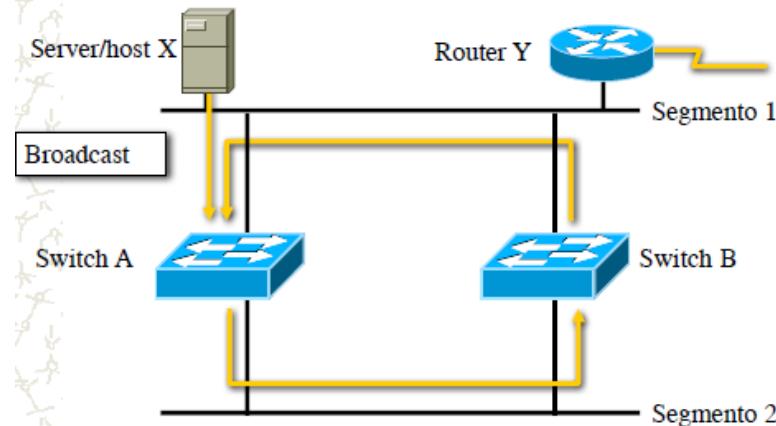


Broadcast Storm:

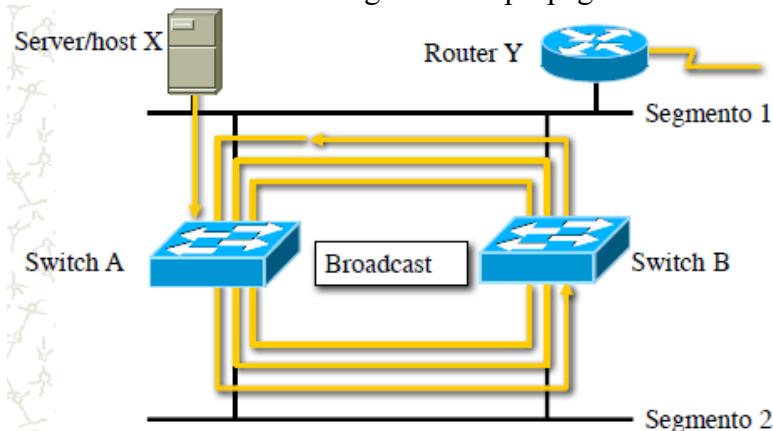
L'Host X invia un Broadcast



Lo switch A replica il Broadcast su tutte le sue porte (anche quella verso lo switch B). Lo switch B replica il Broadcast su tutte le sue porte (anche quella verso lo switch A). Il Broadcast ritorna ad A.

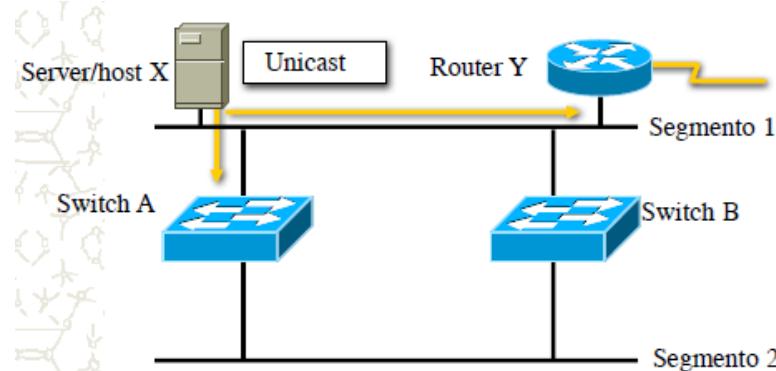


Gli switches continuano a rigenerare e propagare I broadcast all'infinito (Broadcast Storm)

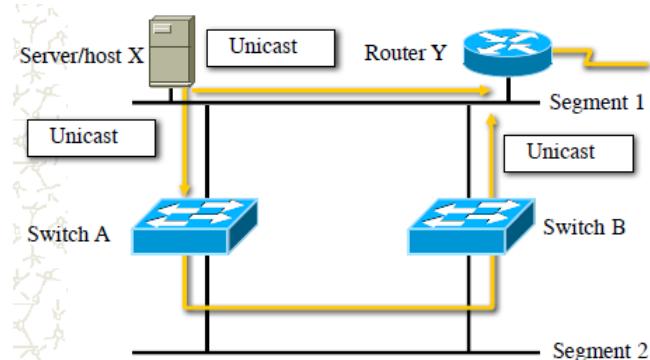


Replicazione di trama:

L'host X invia una trama unicast al router Y. L'indirizzo MAC del Router Y non è stato “imparato” da nessuno dei 2 switches.

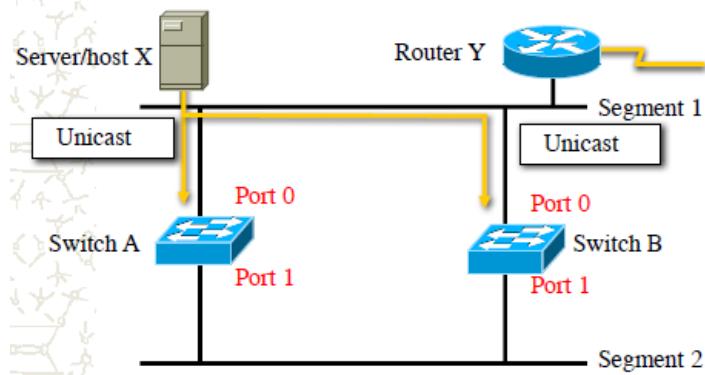


Entrambi gli switch inviano il messaggio su tutte le porte. Il Router Y riceve 2 copie della medesima trama.

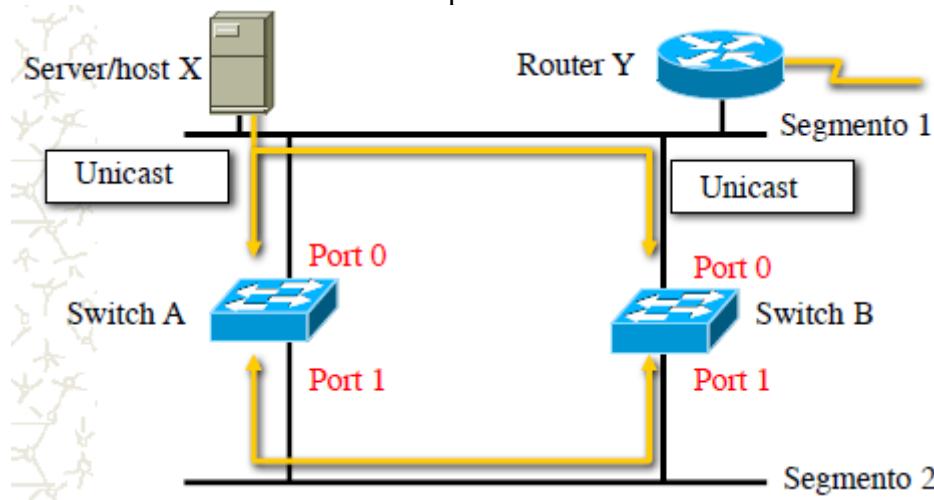


Instabilità del MAC address database:

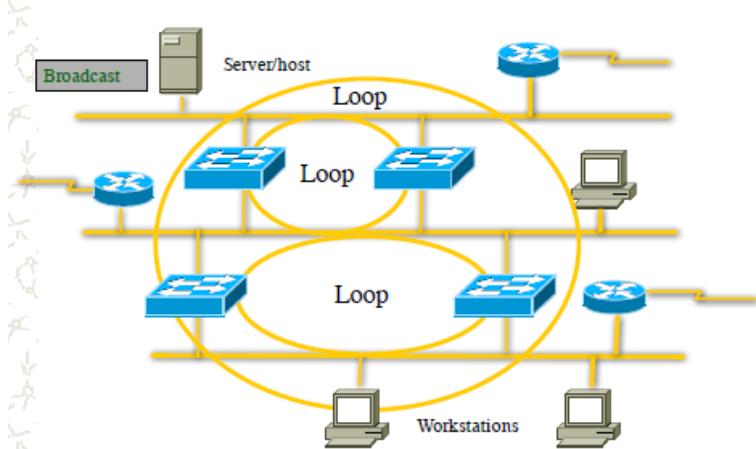
L'host X invia una trama unicast al router Y. L'indirizzo MAC del Router Y non è stato "imparato" da nessuno dei 2 switches. Gli Switch A and B vedono il MAC address di X sulla porta 0.



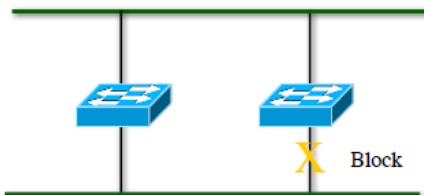
La trama diretta al router Y è inviata a tutte le porte. Gli switch A and B vedono in maniera non corretta il MAC address di X sulla porta 1.



Questo porta che con tipologie più complesse abbiamo loop multipli. Non esistono meccanismi per bloccare questi loop.



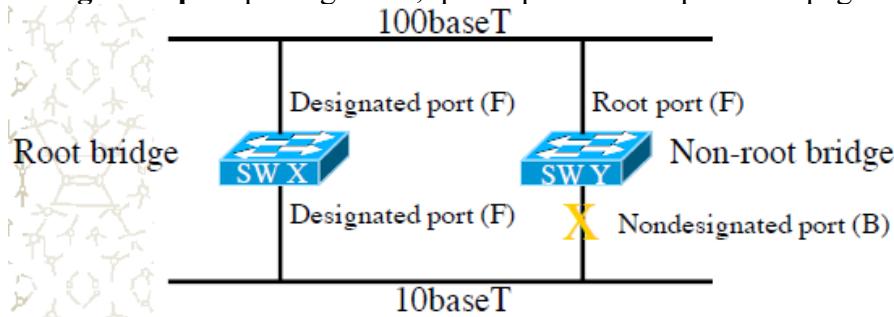
La soluzione è usare lo **Spanning-Tree Protocol**, che rende una topologia ridondante "loop free" mettendo in stato di blocco alcune porte.



Dal grafo ricaviamo un albero di copertura, che è in grado di raggiungere ogni nodo della rete (spanning-tree). Lo spanning tree fa parte dello standard IEEE 802.3P.

SPANNING TREE FUNZIONAMENTO

- Un **root bridge** per network (radice dell'albero)
- Una **root port** per non-root bridge (uplink verso radice), sono connesse alla root dell'albero. Sarà scelta tra quelle che si interfacciano con una capacità di trasmissione maggiore.
- Una **designated port** per segmento, queste porte non si possono spegnere.

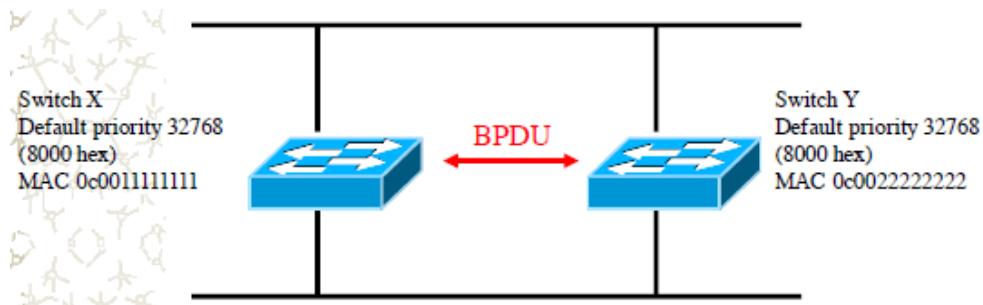


SELEZIONE DEL ROOT BRIDGE

Nella selezione del root Bridge abbiamo diversi fattori che partecipano:

- **BPDU** = Bridge protocol data unit (default = inviata ogni 2 seconds)
- **Root bridge** = Bridge col più basso bridge ID
- **Bridge ID** = Bridge priority + bridge MAC address

All'inizio infatti tutti vogliono fare da root bridge, verrà scelto poi quello che ha il Bridge ID più minore.



Il Bridge Protocol Data Unit (BPDU) trasporta le informazioni necessarie per:

- Eleggere il root bridge
- Localizzare i loops
- Bloccare le porte per evitare i loops
- Notificare I cambi di topologia
- Monitorare lo stato dello spanning tree

Nota:

ROOT ID: contiene l'identità del root bridge

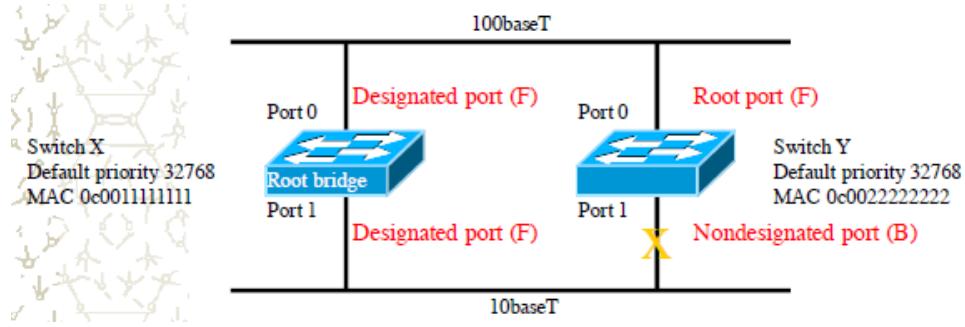
BRIDGE ID: contiene il proprio valore di bridge

Alla partenza: Bridge ID = Root ID

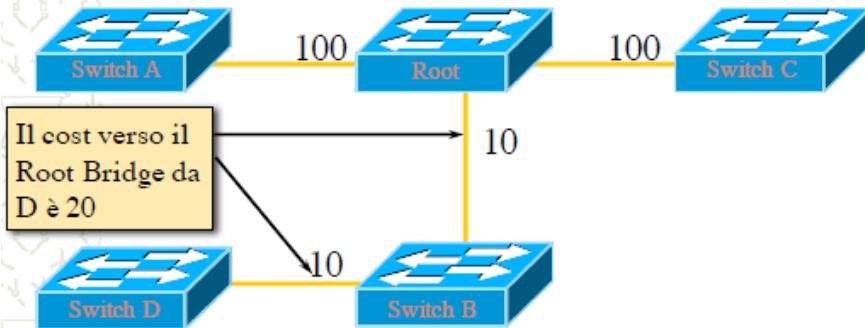
Bytes	Field
2	Protocol ID
1	Version
1	Message Type
1	Flags
8	Root ID
4	Cost of Path
8	Bridge ID
2	Port ID
2	Message Age
2	Maximum Time
2	Hello Time
2	Forward Delay

Questi calcoli sono infine distribuiti tra tutti gli switch, così da sapere quale è designato come root bridge, questo processo accade nel momento in cui la rete va in convergenza (cioè tutti comunicano con tutti). Da qui nasce l'albero di copertura, cioè un albero che ha il cammino più breve raggiungere ogni nodo della rete.

FUNZIONAMENTO DELLE PORT



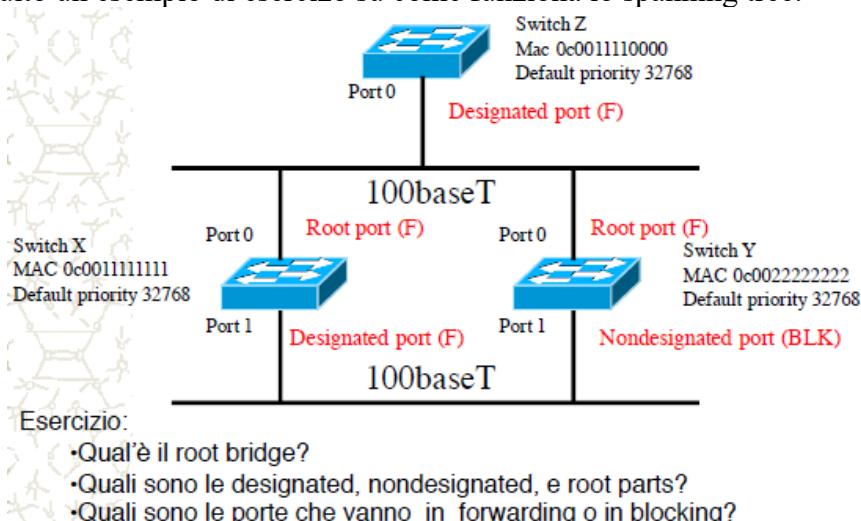
Il costo del calcolo avviene nel seguente modo: il costo è in funzione della banda su ogni link e è determinato su ciascun path come la somma dei link attraversati da origine a destinazione. Può essere opportunamente cambiato su ciascuna porta.



Di seguito una tabella con i costi della rete sui link:

Link Speed	Cost (reratify IEEE spec)	Cost (previous IEEE spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

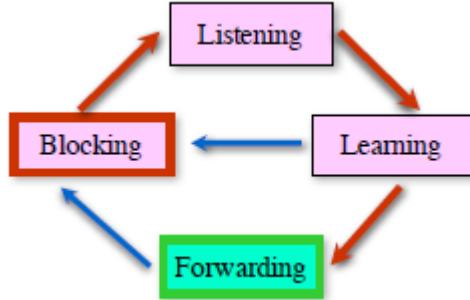
Di seguito un esempio di esercizio su come funziona lo spanning tree:



Nello Spanning-tree ogni porta transita attraverso 4 differenti stati:

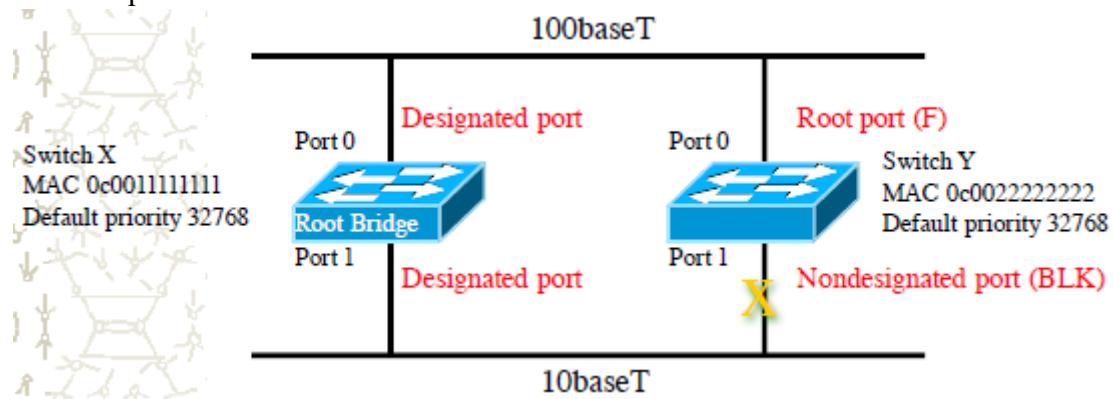
- Blocking (blocco)
- Listening (ascolto)
- Learning (apprendimento)
- Forwarding (trasmissione)

Passaggio da blocking a Forwarding: prima di passare dal blocking al forwarding si passa prima attraverso lo stato di **listening e learning**; il primo mette il bridge in ascolto di BPDU contenenti soluzioni migliori, l'altro impara la nuova posizione dei MAC address per scrivere la nuova MAC address table. La porta può uscire dallo stato blocking quando la topologia della rete cambia aggiungendo nuovi switch.

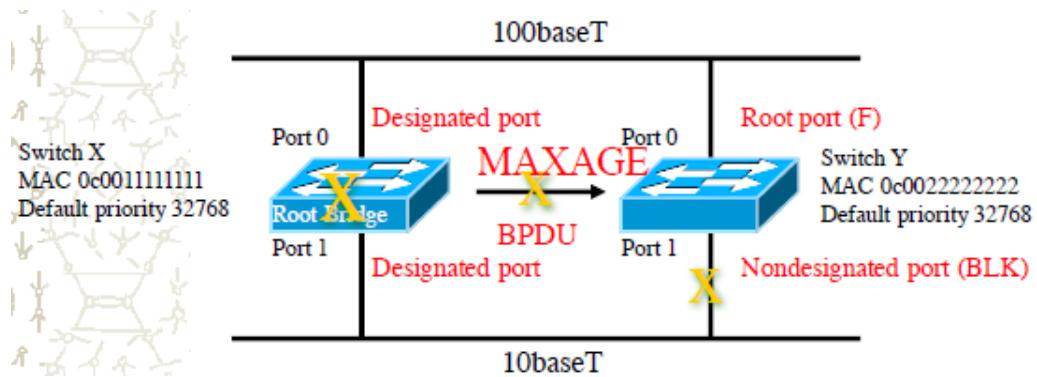


Esempio:

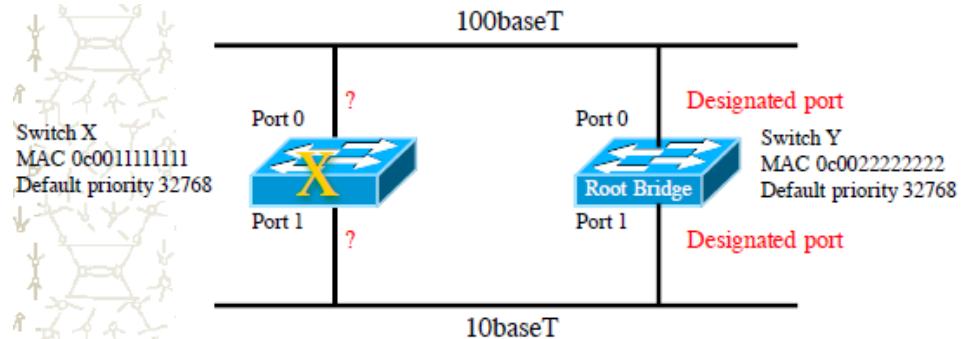
Partendo da questa situazione:



Ipotizziamo il caso in cui il root bridge va fuori servizio, il non-root bridge non riceverà quindi BPDU per più di MAXAGE secondi:



Quindi B diventa root bridge e la port 1 va in forwarding (si blocca) e diventa designated port:



VLAN (Virtual LAN)

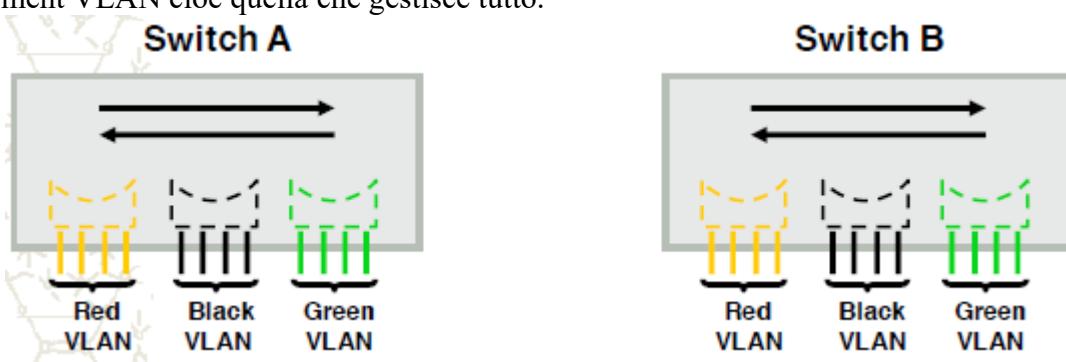
Per molte ragioni gli amministratori di rete amano raggruppare gli utenti delle LAN per riflettere la struttura dell'azienda, invece dello schema fisico dell'edificio.

- La prima è la sicurezza: ogni scheda di rete può essere attivata in modalità promiscua, e copiare tutto il traffico che scorre attraverso il cavo.
- Un secondo problema è il carico. Alcune LAN sono utilizzate più intensamente di altre, e talvolta può essere utile separarle.
- Un terzo problema è la trasmissione broadcast. La maggior parte delle LAN supporta questo tipo di comunicazione, e molti protocolli di strato superiore usano in modo esteso questa funzionalità.
- Un quarto problema era la flessibilità: infatti inizialmente in un'azienda si voleva spostare un utente da una LAN ad un'altra, l'amministratore di rete doveva raggiungere la centralina e scollegare l'utente da un hub e collegarlo a quello nuovo.

Per rispondere agli utenti che chiedevano maggiore flessibilità, i produttori di dispositivi di rete hanno studiato un metodo per ricablarne gli edifici interamente via software. Il concetto risultante è stato chiamato VLAN (*Virtual LAN*), standardizzato dal comitato IEEE802.2Q.

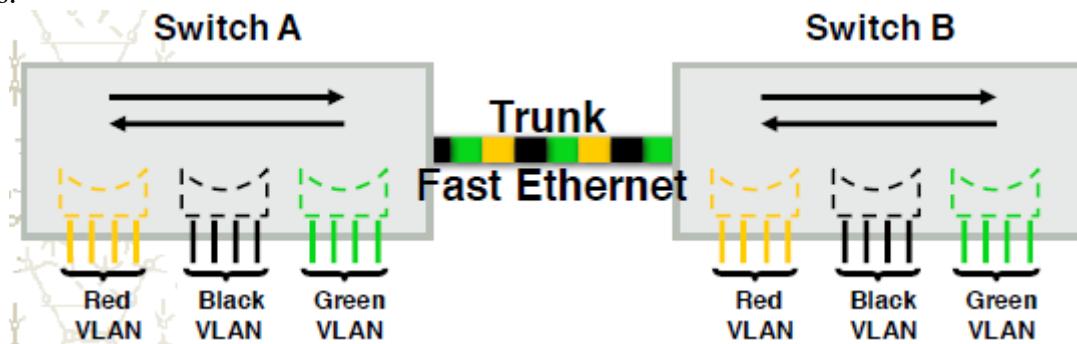
Una VLAN infatti partiziona una LAN in un certo numero di LAN virtuali.

Per impostare una rete basata su VLAN, l'amministratore di rete decide quante VLAN creare, quali computer collegare e quale nome assegnare a ogni VLAN. Spesso le VLAN vengono battezzate con nomi di colori, poiché in questo modo è possibile stampare diagrammi a colori che mostrano lo schema fisico delle macchine, con i membri della LAN rossa rappresentati in rosso, quelli della LAN verde rappresentati in verde e così via. In tal modo, con un solo schema è possibile rappresentare sia la disposizione fisica sia la disposizione logica della rete. Per far funzionare correttamente le VLAN, nei bridge o negli switch devono essere impostate delle tabelle di configurazione. Queste tabelle indicano quali VLAN sono accessibili attraverso le varie porte (linee). Ma più correttamente le VLAN sono indicate con dei numeri che variano fino ad un certo range (migliaia), solo un numero non è assegnabile cioè l'1; che di default è assegnata alla management VLAN cioè quella che gestisce tutto.



FUNZIONALITÀ DELLA VLAN

Ogni VLAN logica è equivalente a un bridge fisico. Le VLANs possono attraversare multipli switches. Non si vedono fra loro se non a livello 3. Ogni VLAN logica è equivalente a un bridge fisico. Le VLANs possono attraversare multipli switches. I trunks trasportano il traffico fra multiple VLANs.



Ci sono due modalità di associazione delle VLAN:

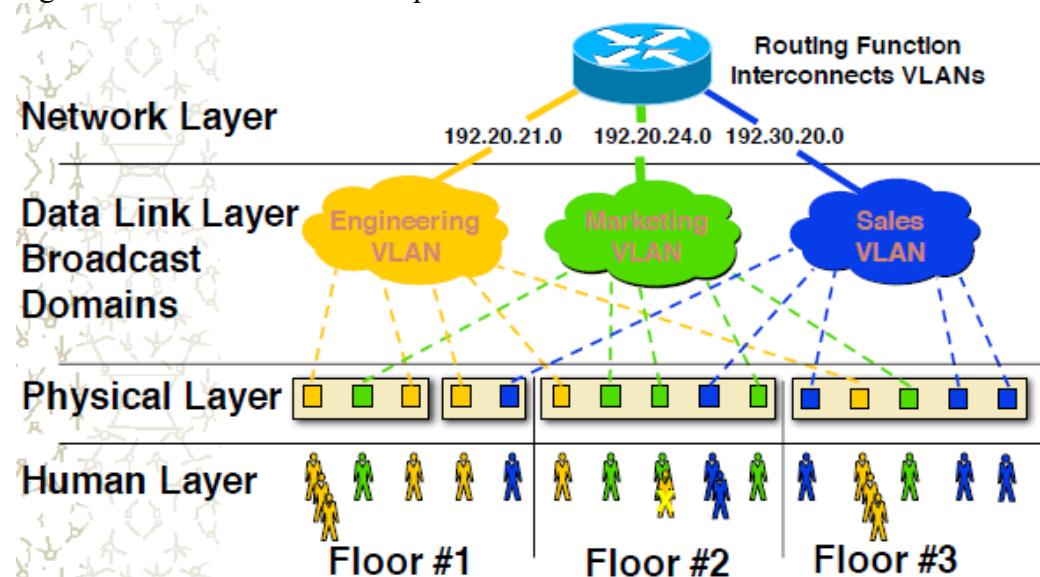
- **VLAN statiche:** vengono assegnate gruppi di porte sullo switch a delle VLAN. L'utente partecipa alla VLAN mappata sulla propria porta dello switch.
- **VLAN dinamiche:** l'utente partecipa alla VLAN in base al proprio MAC address. In questo modo si grantisca la mobilità dell'utente nell'edificio.

Si usa quasi sempre l'assegnamento statico. Un trunk può stare simultaneamente su più VLAN, mentre uno switch soltanto su una.

Per identificare a quale VLAN appartenga un frame in arrivo esistono due soluzioni:

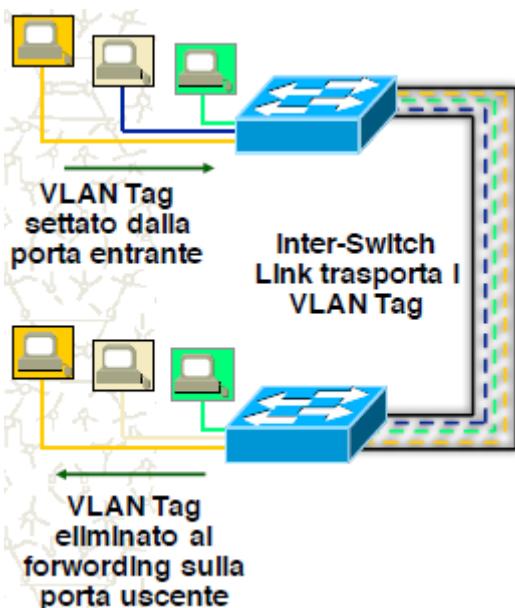
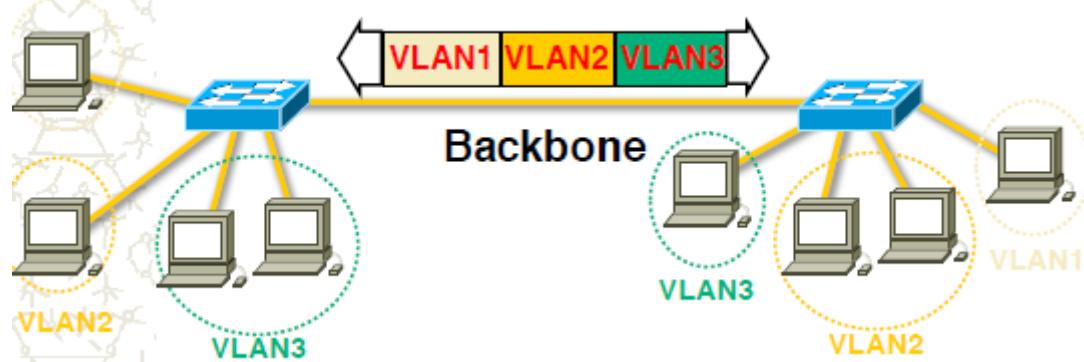
- identificare la VLAN in base alla linea di arrivo: in questo caso ogni linea appartiene ad una sola VLAN, lo switch e' realmente equivalente ad uno switch multiplo, se due switch interconnessi debbono trasferire traffico di due VLAN dovranno essere connessi da due linee, ciascuna appartenente ad una VLAN. Uno stesso ramo non puo' appartenere a due VLAN differenti in quanto non si saprebbe a quale VLAN assegnare i frame provenienti da quel ramo.
- identificare la VLAN in base al MAC address di provenienza: non si puo' basarsi sul MAC address di destinazione perche' non si potrebbe sapere a quale VLAN assegnare i frame broadcast, in questo caso è possibile avere linee appartenenti a due VLAN contemporaneamente, perche' non e' la porta di arrivo o di destinazione a determinare la VLAN.

Tutti gli utenti attaccati alla stessa porta sono nella stessa VLAN:



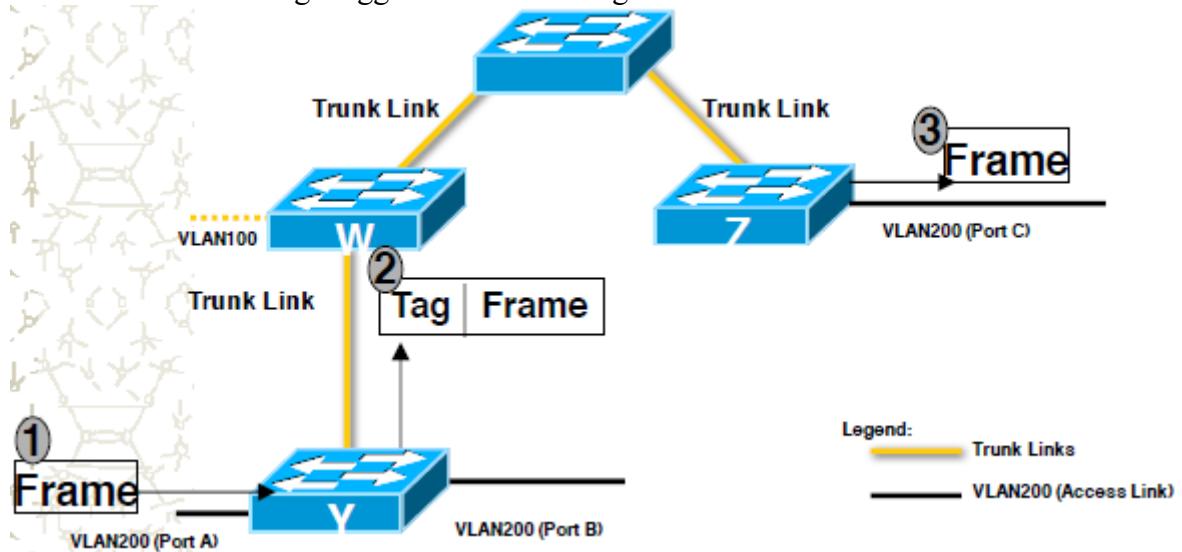
Ogni collegamento è associato ad una sola VLAN. Un trunk o tagged port è un collegamento in grado di trasportare VLAN multiple.

I frame sono associate alle VLAN tramite la logica inter-switch sviluppata per ambienti multi-VLAN, il frame viaggia contemporaneamente con il suo trunk. Nell'header di ciascuna trama è trasportato un VLAN ID.



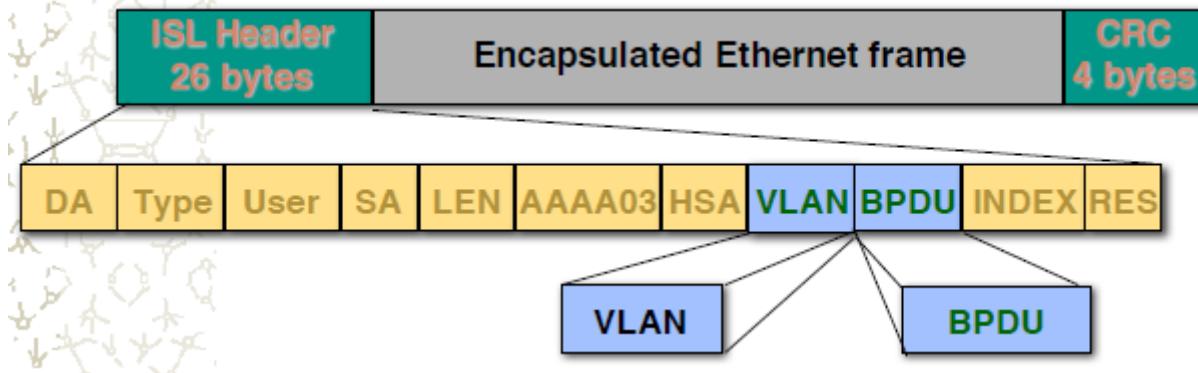
I trunks trasportano le VLANs sul backbone. È gestito in ASIC, non è intrusivo per le stazioni client ed è implementabile fra switches, router e switches, switches e server con interfacce in grado di supportare il tagging.

Le informazioni dei Tag viaggiano solo su collegamenti Trunk:

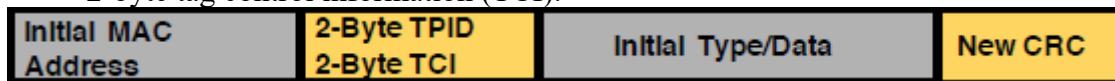


Esistono due protocolli possibili per l'interscambio di VLAN ID:

- **ISL (Proprietario):** Uno standard adottato dalla CISCO. Incapsula nel frame il VLAN ID e il BPDU tramite l'ISL header e un CRC dedicato. Ha un supporto per molte VLANs (1024). Non è molto conveniente perché si deve ricalcolare ogni volta il CRC.

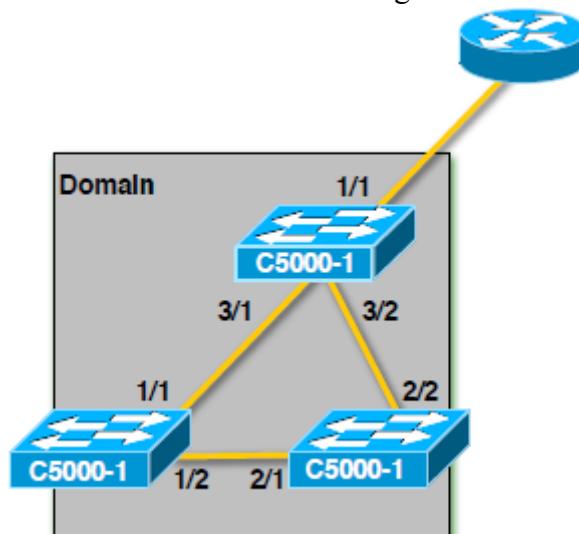


- **IEEE 802.1Q:** Il comitato 802 ha standardizzato un protocollo per l'utilizzo delle VLAN (802.1Q). La standardizzazione ha provocato la modifica del frame Ethernet con l'aggiunta di una etichetta che definisce l'appartenenza del frame ad una determinata VLAN. Il frame 802.1Q ha, dopo il campo destination address, due byte con valore 0x8100, seguito da due byte di Tag contenente il numero di 12 bit identificativo della VLAN, quindi dalla lunghezza del campo dati e dal resto del frame. In dettaglio:
 - 2-byte tag protocol identifier (TPID) fissato a 0x8100. Questo valore indica che la trama trasporta informazioni (tag) 802.1Q/802.1p.
 - 2-byte tag control information (TCI).



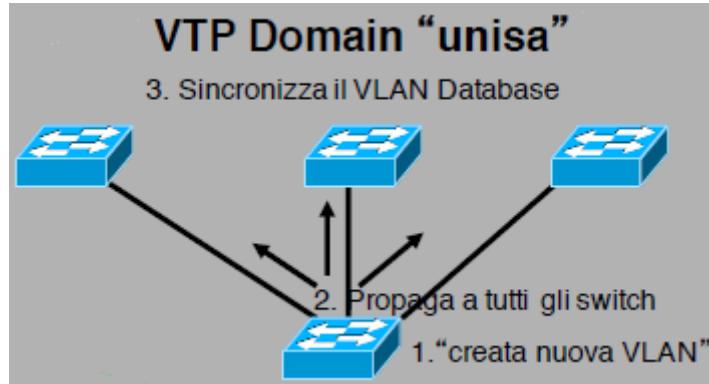
TRUNK NEGOTIATION

Il protocollo DTP (Dynamic Trunk Protocol) gestisce la negoziazione dinamica del trunking sui link. È utilizzato per la negoziazione dinamica di collegamenti in trunk (che trasportano più VLAN), generalmente tra due switch. Può essere configurato in 5 diverse modalità: Desirable, Auto, On, Off, Nonegotiate. La modalità Desirable forma un trunk qualunque sia la modalità configurata all'altro capo della connessione. La modalità Auto forma un trunk se all'altro capo sono configurate le modalità Desirable oppure On. La modalità On è in genere utilizzata se all'altro capo si ha un apparato di un altro produttore e forza la creazione di un trunk. La modalità Off forza il collegamento a non diventare un trunk. La modalità Nonegotiate disabilita l'invio di frame DTP.



Questo sistema è gestito dal VTP (VLAN Traming Protocol). Il VTP è un sistema/protocollo che diffondono le informazioni di configurazione delle VLAN information. Garantisce la consistenza dell'configurazioni delle VLAN all'interno di un singolo dominio amministrativo. Il VTP manda gli annunci solo sulle trunk ports. Il suo funzionamento è il seguente:

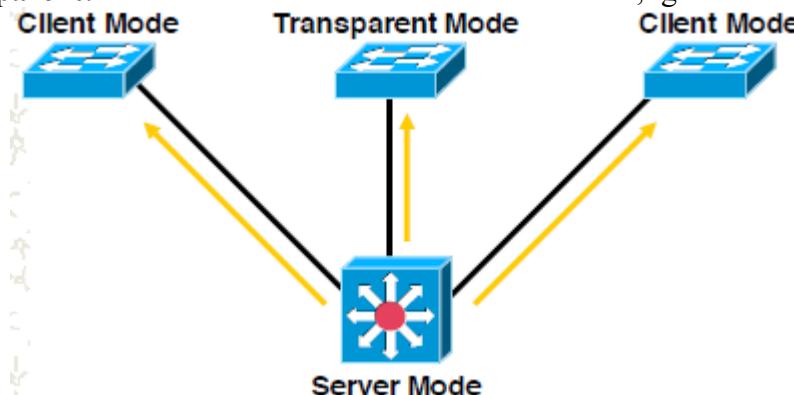
- Si individua una macchina master dove si inseriscono tutte le informazioni sulle VLAN presenti.
- Le informazioni sono così poi distribuiti a tutti gli switch senza doverli inserire manualmente uno ad uno su tutti.



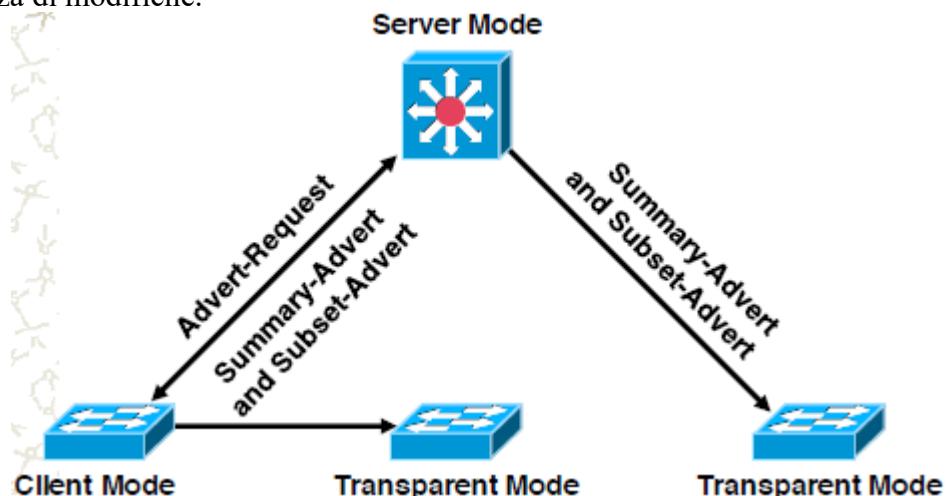
I routers bloccano la propagazione degli annunci VTP. Questo dominio vale soltanto per il livello 2, infatti appena passiamo al livello 3 tutto il sistema muore.

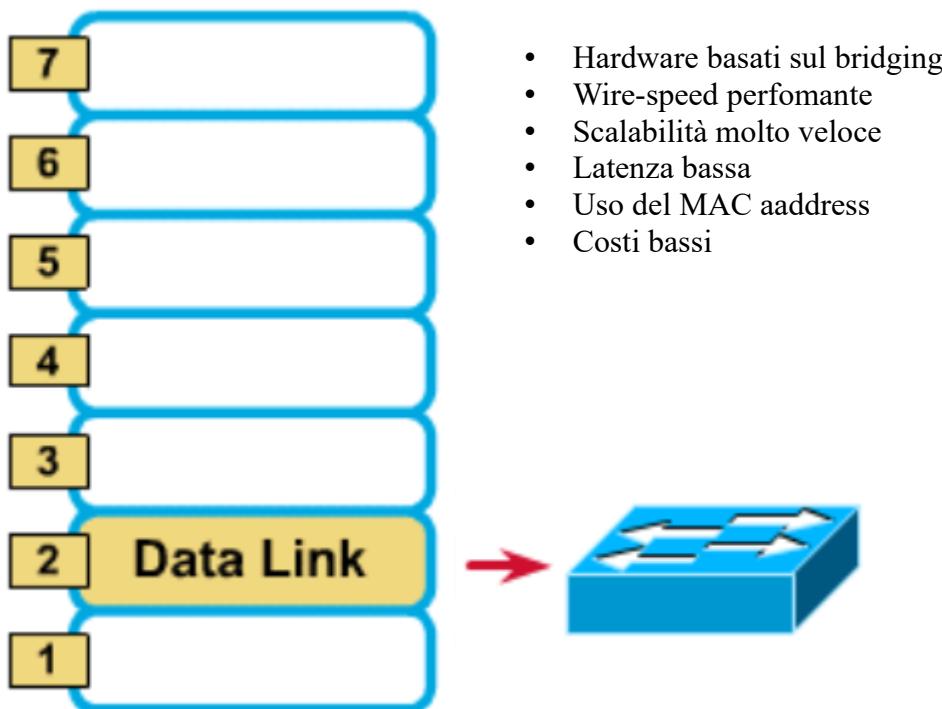
Il VTP opera in 3 diverse modalità operative:

- **Server mode:** Può creare e rimuovere VLANs
- **Client mode:** Non può modificare la configurazione VLANs
- **Transparent:** Può creare/rimuovere VLANs localmente, ignora e fa passare annunci VTP.



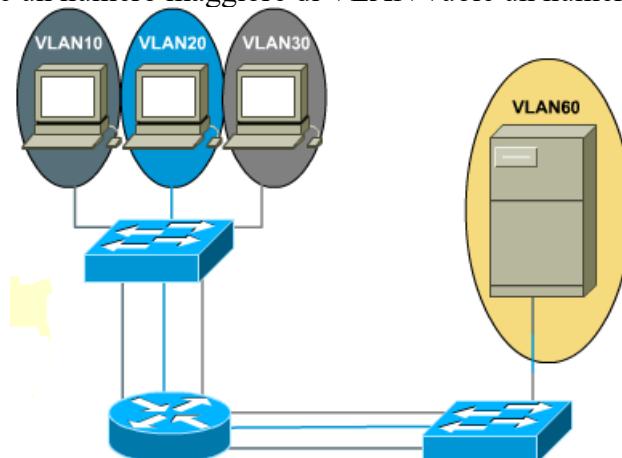
Gli annunci sono inviati come trame multicast periodicamente (di solito 5 minuti), su base richiesta o in presenza di modifiche.



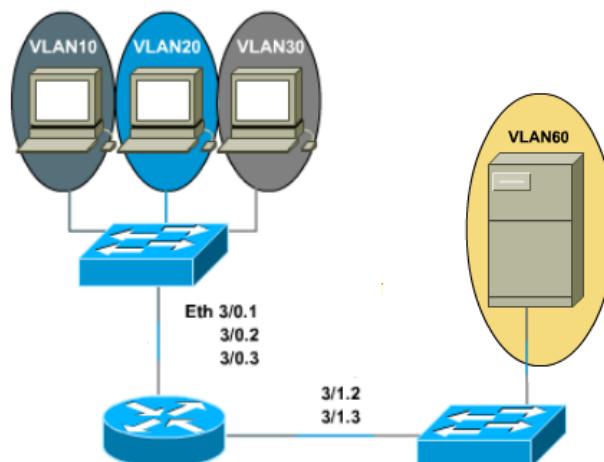


PROBLEMI DI SCALABILITÀ

La inter-VLAN ha problemi di scalabilità, infatti se abbiamo 3 VLAN sono necessari 3 porte in un router, questo comporta che un numero maggiore di VLAN vuole un numero maggiore di porte.

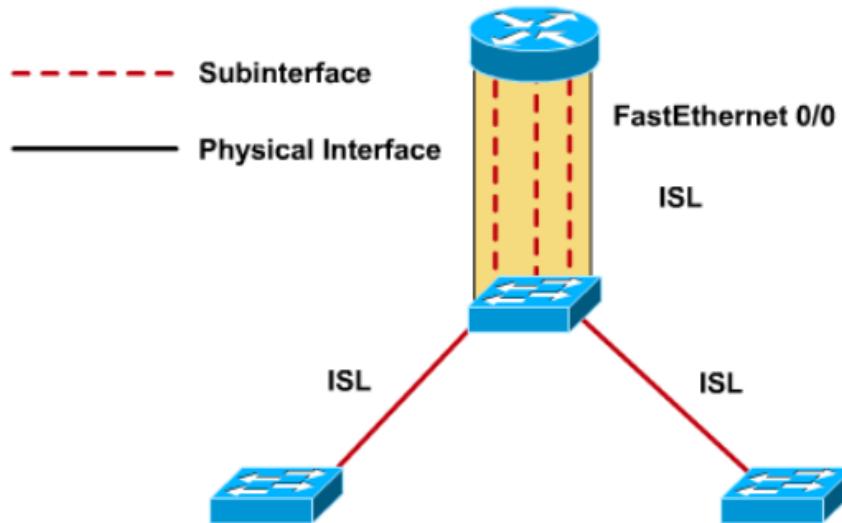


Il trunking risolve in parte questo problema. Infatti se si usa ISL o 802.1Q serve solo una porta. Le subinterfaces vanno configurate sul router.

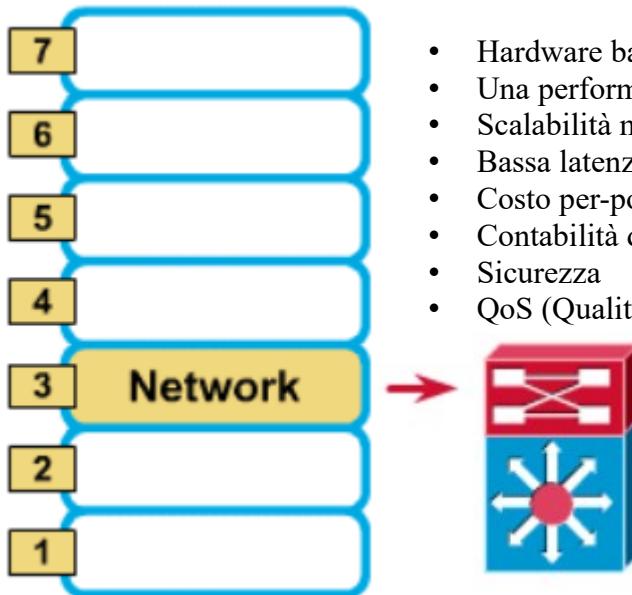


ROUTER ON A STICK

Frà il router e lo switch passano tutte le VLAN, perchè sul router viene creata un'interfaccia logica per ognuna delle VLAN. Un primo problema è che non è molto scalabile, un secondo invece è che il traffico è partizionato su tutte le VLAN.



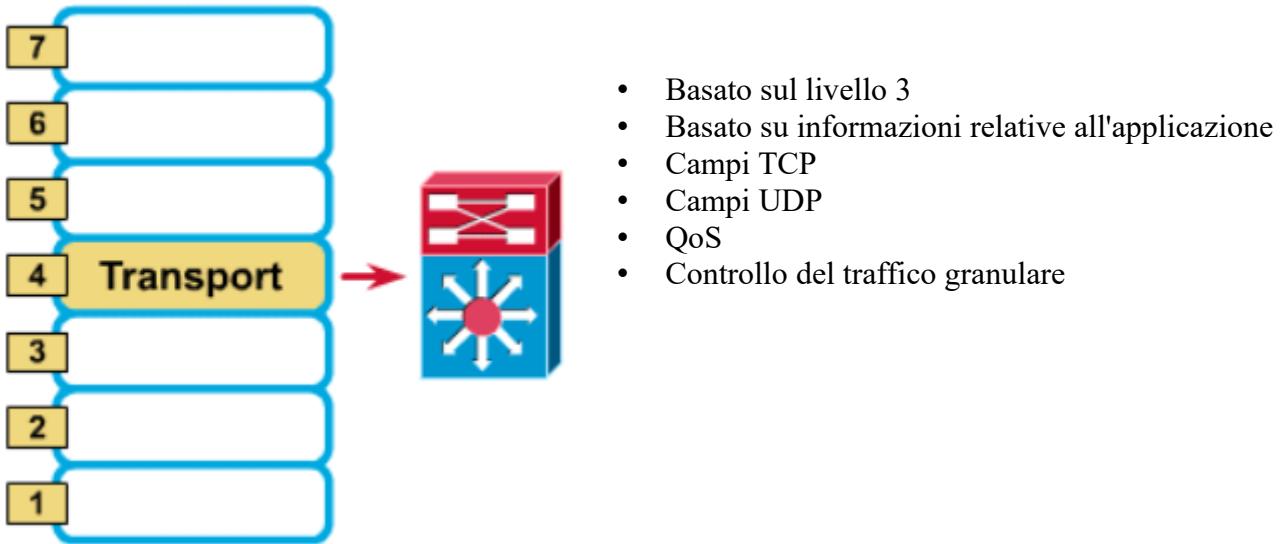
Per risolvere un pò questo problema si è pensato al **Layer 3 Switching**. Un hardware basato sul routing che integra funzioni di livello 3 nello switch.



- Hardware basato sull'inoltro di pacchetti
- Una performance alta sulla commutazione a pacchetto
- Scalabilità molto alta
- Bassa latenza
- Costo per-port basso
- Contabilità del flusso
- Sicurezza
- QoS (Quality of Service)

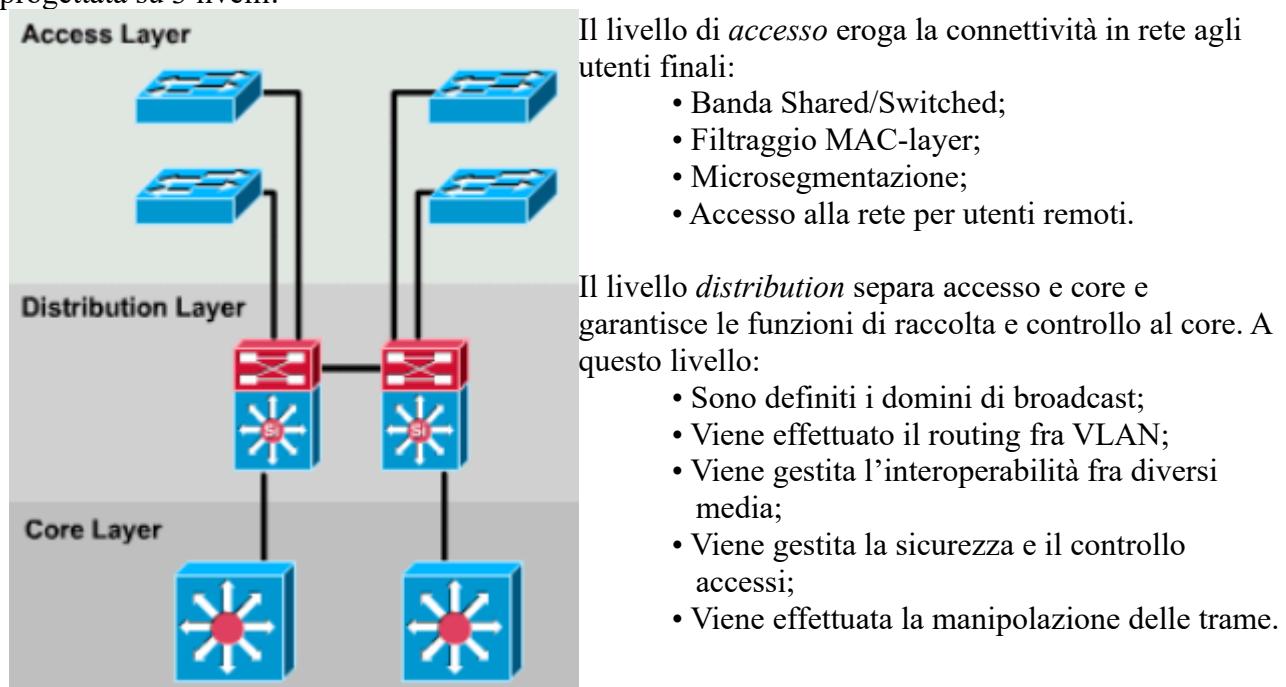
NOTA: La differenza fra uno switch layer 3 ed un router è che uno switch con le potentialità di un router è vincolato ad una singola tecnologia protocollare, mentre un router ha più interfacce protocollari.

Un miglioramento al layer 3 switching è il **Layer 4 switching**, cioè un hardware basato sul routing evoluto, integra il controllo di elementi trasporto ed applicazione nello switch.



GERARCHIE DELLA RETE

Tipicamente si tende a costruire una rete in maniera deistribuita. Una rete però dovrebbe essere progettata su 3 livelli:



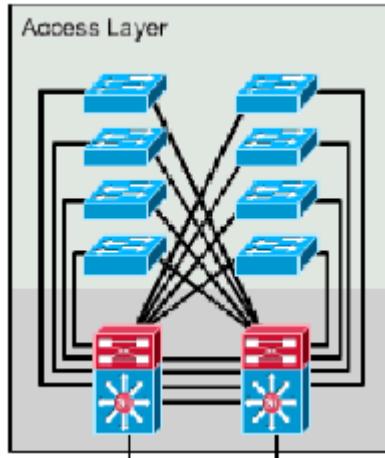
Il livello *core* commuta le trame alla massima velocità e non effettua nessuna elaborazione sulle stesse:

- Non supporta ACLs;
- Non prevede routing né VLAN trunking;
- Le VLANs sono terminate a livello di distribuzione.

Per queste gerarchie esistono dei modelli già preimpostanti di seguito ne saranno elencati alcuni.

SWITCH BLOCK

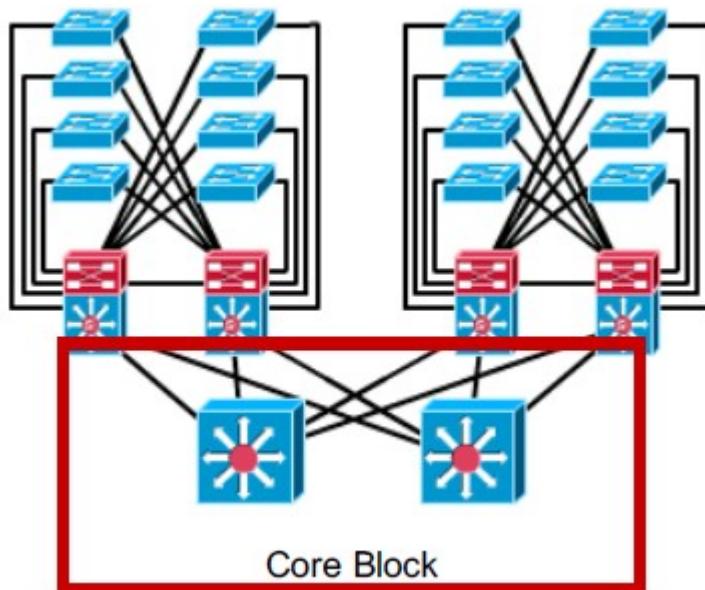
Switch Block 1



- **Access layer:** connette gli utenti finali alla rete garantendo banda dedicata su ogni porta.
- **Distribution layer:** eroga servizi di broadcast control, sicurezza e connessione ad altre reti.

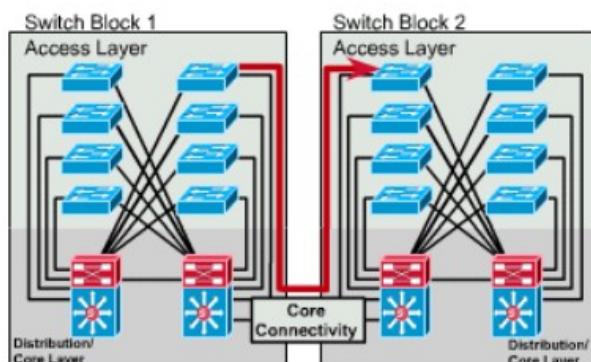
CORE BLOCK

Il traffico tra switch blocks deve transitare attraverso il core block. Dato che le VLANs sono terminate a livello di distribuzione I links non possono essere trunk links. Un minimo di 2 dispositivi deve essere presente nel core block a scopo di ridondanza. Lo spanning tree risolve i problemi di loops. Assenza di *singol point of failure*. Il core block è usato su LAN molto grandi per via del suo costo.



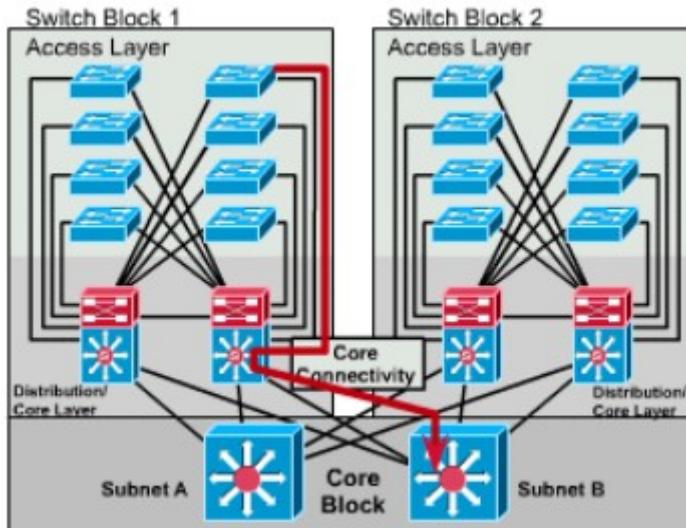
Se la LAN è molto piccola si ricorre al collapsed core.

COLLAPSED CORE



Consolidamento dei livelli di distribuzione e core in un solo livello (prevalente nei campus di piccole o medie dimensioni). Ogni switch di accesso ha un uplink ridondato alla distribuzione. Tutte le subnets terminano su porte di questo livello.

DUAL CORE



Necessario in presenza di 2 o più switch blocks e sono richieste connessioni ridondanti. Mette a disposizione il doppio dei paths e della banda. Ogni switch block è collegato in maniera ridondante a tutti gli switches di core consentendo coppie di path distinte al medesimo costo.

PROTOCOLLI DATALINK LAYER PER RETI WAN

ADSL

ADSL (Asymmetric Digital Subscriber Line) è lo standard per fornire all'abbonato un accesso digitale a banda più elevata di quanto non sia possibile con il modem. La linea telefonica terminale è costituita da un doppino su cui viene normalmente trasmessa la voce. Questa trasmissione si realizza applicando un filtro passa basso a 4 KHz. Tuttavia il doppino ha una capacità di banda che raggiunge il MHz (dipende dalla lunghezza del tratto terminale, che può variare in base alla situazione tra poche centinaia di metri a diversi Km). Lo spettro disponibile viene suddiviso in 256 canali da 4 KHz (fino a 60 Kbps ciascuno):

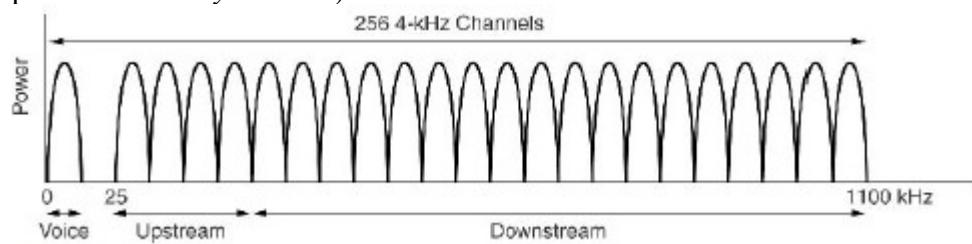
- Il canale 0 viene riservato per la telefonia
- I successivi 4 canali non vengono utilizzati per evitare problemi di interferenza tra la trasmissione dati e quella telefonica.

I restanti canali vengono destinati al traffico dati. Alcuni per il traffico uscente (upstream), altri per il traffico entrante (downstream). Il modem ADSL riceve i dati da trasmettere e li splitta in flussi paralleli da trasmettere sui diversi canali, genera un segnale analogico in banda base per ciascun flusso (con una modulazione QAM fino a 15 bit/baud a 4000 baud/s) e li trasmette sui diversi canali utilizzando la modulazione di frequenza.

La standardizzazione dell'ADSL è stata sviluppata inizialmente in ambito americano (ANSI T1.413), con una grande spinta di ADSL Forum e UAWG (per ADSL Lite). ITU-T ha prodotto raccomandazione su ADSL (G.992.1) e ADSL Lite (G.992.2, 6/99).

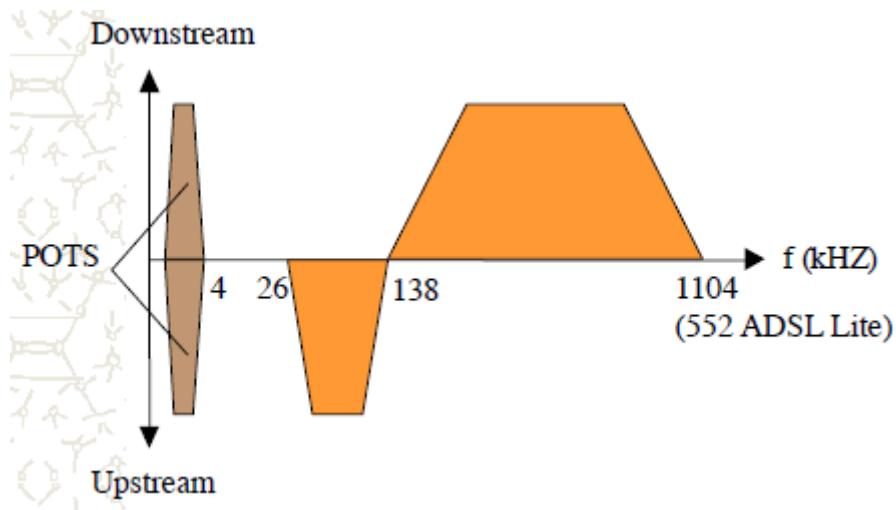
In teoria l'ampiezza di banda disponibile consente un traffico pari a 13.44 Mbps, ma non tutti i canali sono capaci di trasmettere a piena banda. L'operatore decide quale servizio offrire.

Generalmente vengono dedicati alcuni canali per il traffico entrante, ed altri (meno) per il traffico uscente (da qui il termine *Asymmetric*).



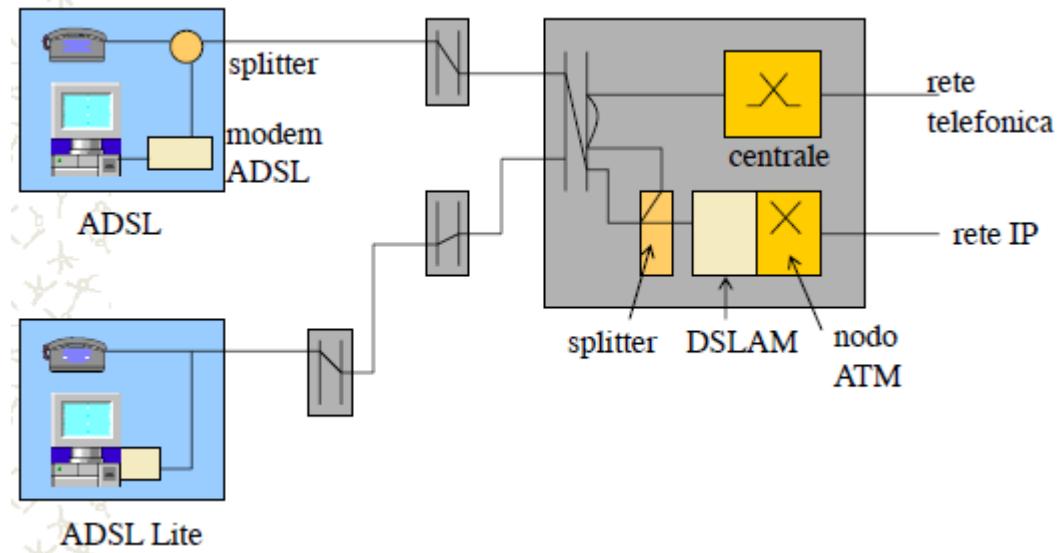
SPETTRO ADSL E ADSL LITE

Le singole portanti, modulate in QAM sono spaziate a 4.3 KHz. La banda fra 26 e 138 KHz è riservata al traffico in upstream mentre quella da 138 a 1104 (552) KHz è riservata al downstream.



ARCHITETTURA DI ACCESSO ADSL/ ADSL LITE

La prima architettura usata è la seguente:



Oggi le architetture si stanno evolvendo utilizzando la tecnologia VOIP (voce su ip), porta all'eliminazione del canale analogico.

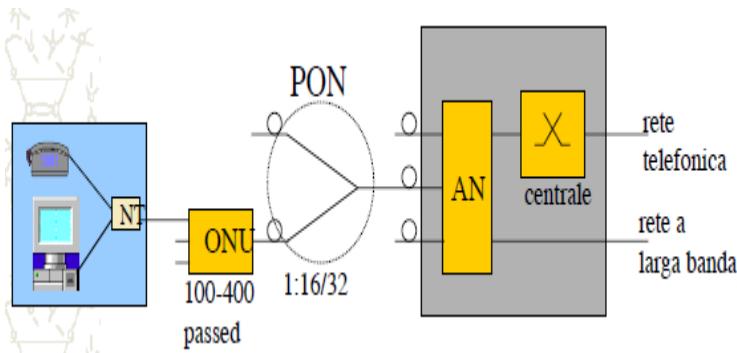
Esistono molte soluzioni, in cui la fibra arriva fino ad un certo livello di "profondità" (vicinanza all'utente); da quel punto il collegamento prosegue in rame. Differenti soluzioni comportano diversi livelli di investimento e capacità offerta all'utente. L'architettura dipende anche dalla situazione urbanistica. **FTTx** (Fiber To The x) indica delle architetture, non degli standard.

Le principali soluzioni FTTx sono:

- FTTO: Office
- FTTC: Curb
- FTTCab: Cabinet
- FTTB: Building
- FTTO: Office
- FTTH: Home
- FTTD: Desktop

Esempio: architettura FTTCab:

La fibra arriva direttamente nella centralina del fornitore. Con la PON parte uno split, che moltiplica la connessione sull'unica fibra del gestore. Il costo di quest'operazione è basso.



- AN: Access Node
- PON: Passive Optical Network
- ONU: Optical Network Unit
- NT: Network Termination

PROTOCOLLI DATALINK LAYER PER RETI WLAN

RETI WIRELESS

La diffusione di computer portatili, per offrire mobilità senza perdita di connessione, un altro fattore è l'estensibilità della rete senza necessità di cablaggio.

Bande trasmissive ISM

Lo strato fisico è realizzato con la trasmissione omnidirezionale in modulazione digitale di una portante, esistono bande di frequenza dedicate all'utilizzo senza necessità di registrazione ed allocazione. Queste bande si chiamano ISM (Industrial, Scientific, Medical). La legislazione specifica determinate caratteristiche obbligatorie per utilizzare queste bande, come ad esempio la potenza massima di trasmissione e l'utilizzo di tecniche trasmissive spread spectrum. Le bande utilizzate nelle trasmissioni wireless sono a 2.4 GHz ed a 5 Ghz, in questa regione le trasmissioni competono con apparati radiocomandati, telefoni cordless, fornì a microonde, ecc...

I vantaggi del Wireless sono i:

- Costi ridotti;
- Meno problemi legati alle distanze (impiego di più AP o *wireless relaying*);
- Mobilità delle postazioni della rete.

Uno svantaggio è che si spreca spettro, quindi possiamo dedurre che il wireless ha molti problemi di interferenza.

STANDARD 802.11x

L'IEEE ha definito diversi standard nel corso del tempo per le trasmissioni wireless.

Questi standard sono:

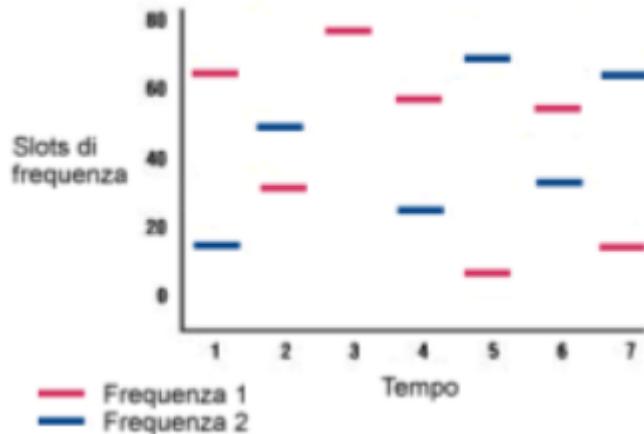
- IEEE 802.11 con tre differenti tecniche trasmissive (IR, FHSS, DSSS) e velocità ad 1 o 2 Mbps nella banda a 2.4 GHz
- IEEE 802.11b a velocità 1, 2, 5.5 e 11 Mbps a 2.4 GHz via HR-DSSS
- IEEE 802.11a con velocità fino a 54 Mbps nella banda a 5 GHz tramite OFDM
- IEEE 802.11g fino a 54 Mbps nella banda a 2.4 GHz
- IEEE 802.11n fino a 300 Mbps sia a 2.4 GHz che a 5 GHz, utilizza la tecnologia MIMO (multiple-input multiple-output) per utilizzare più antenne per trasmettere e più antenne per ricevere incrementando la banda disponibile utilizzando una multiplazione a divisione di spazio
- IEEE 802.11ac fino a 1Gbps a 5 Ghz estendendo i concetti di 802.11n

TECNICHE A DIVISIONE DI SPETTRO

Tecniche a divisione di spettro (SST):

1. FH – salto in frequenza (Frequency Hopping): **802.11 FHSS** (Frequency Hopping Spread Spectrum), utilizza 79 canali ad 1 MHz a partire da 2.4 GHz con la tecnologia Frequency Hopping: la trasmissione salta ad intervalli temporali definiti (minori di 400 ms) da una frequenza ad un'altra secondo una sequenza pseudocasuale nota a tutti. la banda disponibile è 1 Mhz, questa tecnica fornisce sicurezza (impossibile seguire la

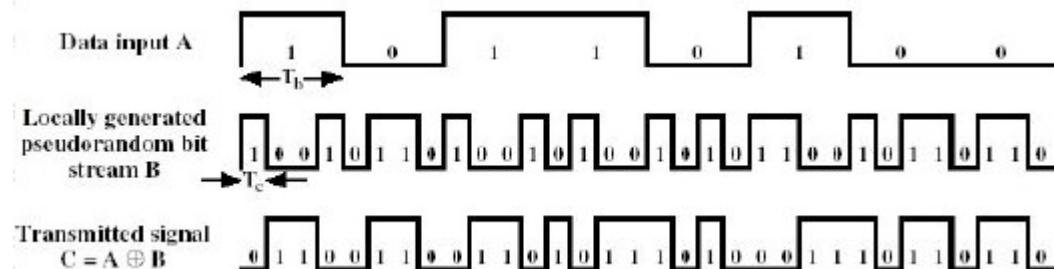
comunicazione senza conoscere la sequenza pseudocasuale) e solidita' contro il multipath fading (quando arriva il segnale riflesso la ricezione e' gia' spostata su un altro canale), supporta standard ad 1 e 2 Mbps, con codifiche a 2 o 4 simboli con (G)FSK.



2. DS – sequenza diretta (Direct Sequence): **802.11 DSSS** (Direct Sequence Spread Spectrum). Per far fronte al rumore si usa la tecnica “chipping”:

- Ogni bit è convertito in una serie di bit ridondanti (chip)
 - il tempo di un bit viene suddiviso in m intervalli temporali
 - il valore trasmesso e' la combinazione in OR esclusivo dei bit dei dati (di durata T_b) combinati con una sequenza pseudocasuale o predefinita di bit, ciascuno di durata $T_c = T_b/m$, detti chip.

Lo standard opera nella banda a 2.4 GHz ed utilizza una sequenza fissa di 11 chip (sequenza di Barker) per codificare un bit di dati.

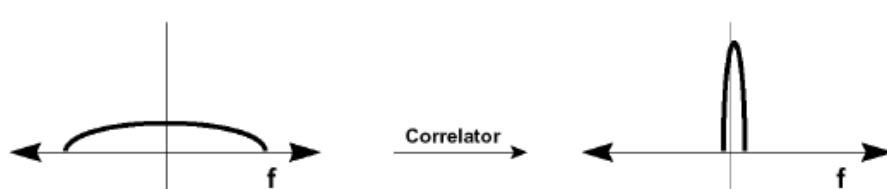


Occupano più banda del necessario ma. Aumentano l'immunità al rumore (DS). Aumentano la sicurezza della comunicazione.

SPREADING SPECTRUM



Figure 5a Effect of PN Sequence on Transmit Spectrum



Nel 802.11 DSSS (Direct Sequence Spread Spectrum) la banda disponibile è divisa in 14 canali di 5 MHz, a partire da 2.412 Ghz, le stazioni debbono essere configurate per determinare il canale utilizzato non tutti i canali sono disponibili in tutti i paesi, in USA il canale 14 è proibito, in Spagna sono ammessi solo il 10 e l'11, in Italia sono tutti ammessi. Le antenne trasmettono a 11 MHz; con modulazioni PSK a 2 o 4 livelli e 11 chip per bit lo standard permette trasmissioni a 1 o 2 Mbps, poiché l'ampiezza di banda del segnale inviato è intorno ai 22 MHz, nonostante i filtri dell'elettronica per non interferire due trasmissioni indipendenti nella stessa area debbono utilizzare canali separati da almeno 5 canali.

CANALI DSSS

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

Quindi infine possiamo dire:

- DSSS:
 - Codifica ridondante è più immune ai rumori.
 - Maggiore spreco di banda (30 MHz per canale).
 - Possibilità di arrivare a 11 Mbps.
- FHSS:
 - Più sicura.
 - Molto limitata in banda (1 Mhz).
 - Impossibile usarla nel WI-FI ad alti bit-rate.

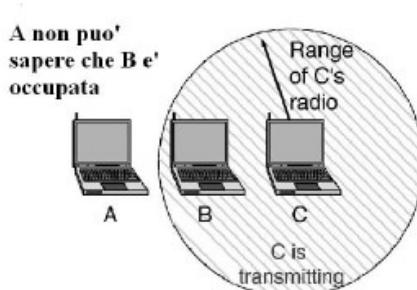
Dynamic Rate Shifting (for back)

Data Rates adattati automaticamente alla natura del canale: 300 → 55 → 11 → 5.5 → 2 → 1 Mbps e viceversa.

Si adatta bene quando c'è interferenza, o ci si allontana dall'apparato di trasmissione.

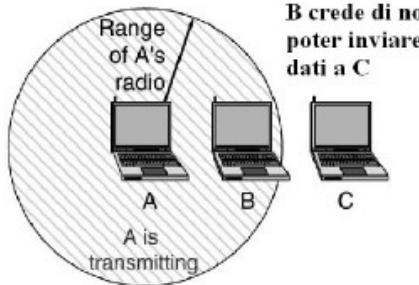
In outdoor un access point fa 350 metri, in indoor fa intorno ai 20/15 metri.

CSMA: stazione nascosta



Come esempio consideriamo tre stazioni A, B e C tali che B sia a portata di A e di C, ma A e C non possano rilevare le rispettive trasmissioni. Se C sta trasmettendo dati a B, A non potrà rilevare l'occupazione del canale in quanto è fuori portata. A inizierà a trasmettere ed il suo segnale arriverà a B interferendo con i dati che C sta trasmettendo. Questo è detto problema della stazione nascosta. Tutti sentono finché sono nel range di copertura.

CSMA: stazione esposta



Se nelle stesse ipotesi supponiamo che A stia trasmettendo verso un'altra destinazione, e che B desideri inviare dati a C, B ascolta il canale e lo trova occupato, quindi non trasmette. In realtà il canale sarebbe disponibile (nella ipotesi che la destinazione della trasmissione di A sia fuori dalla portata di B) perché in C i segnali non interferirebbero. Questo è il problema della stazione esposta.

MACA

Si risolve con il MACA. L'inefficacia del protocollo CSMA deriva dal fatto che per le trasmissioni wireless quello che conta è l'interferenza in prossimità del ricevente, mentre l'analisi della portante che può fare una stazione è solo in prossimità di se stessa, cioè del trasmittente. Il protocollo MACA (Multiple Access with Collision Avoidance) tenta di risolvere il problema nel seguente modo:

- il trasmittitore A invia un piccolo frame (RTS: Request To Send) al ricevitore B.
- il frame RTS contiene la richiesta di trasmettere un frame a B, specificandone la lunghezza.
- il ricevitore B trasmette un piccolo frame di conferma (CTS: Clear To Send) ad A, con le stesse informazioni del RTS quando A riceve il CTS trasmette il frame di dati a B.

Tutte le stazioni che ricevono il frame RTS sanno che:

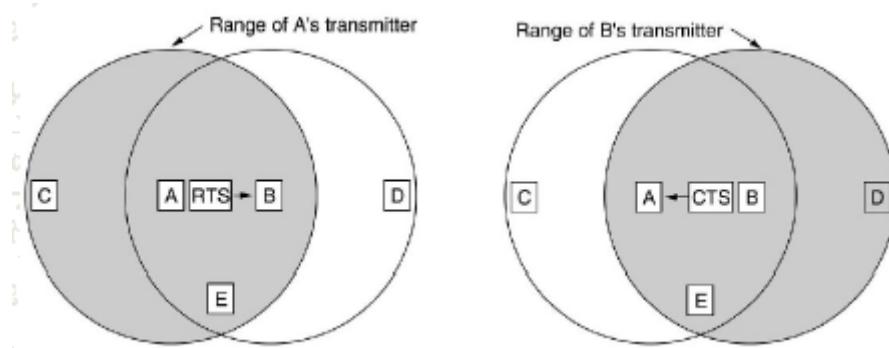
- B risponderà con un CTS
- in seguito A trasmetterà un frame di dati di lunghezza specificata in RTS

Queste stazioni attenderanno senza trasmettere un tempo sufficiente alla trasmissione dei dati. Le stazioni nascoste non vedono il frame RTS, ma vedono il frame CTS, quindi sanno che trasmesso il CTS B dovrà ricevere il frame di dati, di lunghezza specificato nel CTS.

Queste stazioni attenderanno senza trasmettere per il tempo necessario alla trasmissione del frame di A (che loro non vedranno in quanto nascoste, ma sanno che ci sarà).

Collisioni saranno possibili se un frame RTS venisse trasmesso contemporaneamente verso una destinazione collocata nel campo di ricezione dei due trasmittenti: i due frame andranno perduti.

In questo caso la stazione che non riceve il CTS dopo un timeout applica l'algoritmo di backoff esponenziale binario e ritenta.



Per risolvere i contenziosi del canale possiamo usare l'Exponential Backoff.

- Ogni stazione sceglie un numero random (n) compreso tra 0 e m .
- Attende $(n \times slot\ time)$ prima di riprovare.
- Ad ogni collisione m aumenta in maniera esponenziale.

Slot Time: definito in modo che ogni stazione possa determinare se un'altra ha acceduto al canale nello slot precedente questo riduce P(collisione) della metà.

Eseguito nei seguenti casi:

- Tx trova il mezzo occupato.
- Dopo ogni ritrasmissione.

- Dopo una trasmissione andata a buon fine.

Non viene eseguito:

- se una stazione vuole tx un nuovo pacchetto ed il mezzo è libero.

MACAW

Il protocollo MACAW (MACA per Wireless) introduce migliorie specifiche per le applicazioni wireless nella maggior parte dei casi la mancanza di ACK a livello 2 provoca la ritrasmissione solo a livello 4, con grossi ritardi, per questo motivo e' stato introdotto l'utilizzo di frame di ACK con meccanismo stop-and-wait; si e' anche notato che CSMA puo' essere utilizzato per impedire ad una stazione di trasmettere un RTS durante la trasmissione di un altro RTS verso la stessa destinazione; infine si e' modificato l'algoritmo di backoff in modo da applicarlo separatamente ai diversi flussi trasmisivi.

LAYER 3 RETE

Funzioni dello strato di rete

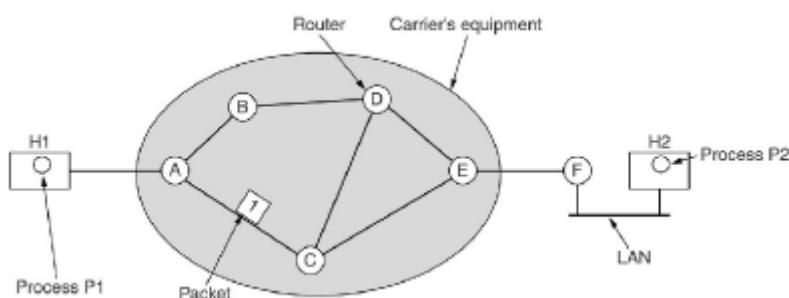
Allo strato di trasporto la comunicazione tra i processi peer di livello 4 deve apparire come una comunicazione punto-punto. Lo strato di rete ha quindi come funzione quella di fornire allo strato di trasporto un servizio per la consegna dei dati in modo da mascherare l'infrastruttura della rete (la sottorete).

Nomenclatura:

- host o end-node: stazione su cui opera lo strato di trasporto che deve trasmettere o ricevere i dati utilizzando il servizio dello strato di rete.
- pacchetto: insieme di dati+header+trailer che lo strato di rete costruisce e deve trasmettere fino a destinazione (Una **Protocol Data Unit** (PDU) è l'unità d'informazione o pacchetto scambiata tra due *peer entities* in un protocollo di comunicazione di un'architettura di rete a strati).
- router: stazione intermedia che opera a livello 3, che riceve i pacchetti e li inoltra attraverso la (sotto)rete.

Questo livello fornisce l'indirizzamento universale, cioè ogni oggetto sul mondo vede un'altro oggetto nel mondo attraverso un'indirizzamento univoco.

In generale due host sono separati da un certo numero di nodi, interconnessi da svariate linee. Spesso sono possibili piu' tragitti tra i due nodi (ad esempio nelle reti magliate). Potenzialmente i nodi sono separati da reti funzionanti con tecnologie differenti.



Lo strato di rete dovrà quindi occuparsi dei seguenti argomenti:

- determinare quale tragitto tra quelli disponibili dovranno seguire i dati (instradamento, routing), questo puo' richiedere che lo strato di rete conosca la topologia della rete;
- reagire a modifiche di topologie della rete: se esiste un meccanismo dinamico per l'apprendimento della topologia, questo permetterà di apprenderne anche le modifiche nel tempo.
- evitare di sovraccaricare linee quando sono disponibili percorsi alternativi (congestione).
- Risolvere i problemi connessi al transito attraverso reti differenti (internetworking).

Connection Oriented o Connectionless?

Inizialmente OSI prevedeva che lo strato di rete fornisse solo un servizio connection oriented:

- in modo analogo al funzionamento del servizio telefonico
- questo servizio, caldeggiaio dalle compagnie telefoniche, permette di operare fatturazione a tempo e di offrire servizi di qualita' riservando le risorse a priori.

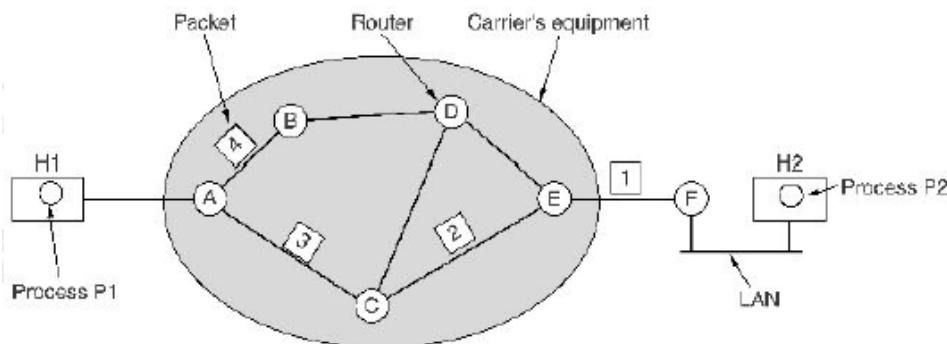
In seguito c'e' stata forte richiesta di introdurre nello standard anche un servizio connection less, e cosi' e' stato fatto:

- l'inaffidabilita' intrinseca della sottorete richiede un meccanismo piu' flessibile per il recapito dei dati.
- Comunque lo strato di trasporto dovrà occuparsi della integrita' dei dati, inutile farlo anche a livello di rete.

Instradamento connectionless

Il servizio senza connessione richiede che i pacchetti siano instradati indipendentemente uno dall'altro.

- Generalmente un router dispone di una tabella che definisce su quale linea di uscita debba essere trasmesso un pacchetto in base alla destinazione finale, il router riceve il pacchetto, lo memorizza per analizzarlo, quindi lo trasmette in base alla tabella (store and forward).
- Ogni pacchetto deve quindi contenere l'indirizzo di destinazione.
- Poiche' le tabelle possono modificarsi nel tempo, non e' detto che tutti i pacchetti seguano la stessa strada.



Instradamento connection oriented

L'idea di base e' di associare ad una connessione un circuito virtuale nella sottorete:

- Si definisce a priori – durante la fase di inizializzazione della connessione – la sequenza di router che i pacchetti dovranno attraversare.
- Tutti i pacchetti appartenenti alla stessa connessione seguiranno la stessa strada.
- L'instradamento del pacchetto sara' quindi fatto in base alla sua appartenenza ad una connessione e non alla sua destinazione finale.
- L'intestazione del pacchetto sara' piu' semplice, dovendo contenere solo l'identificativo della connessione.
- La connessione potra' essere stabilita in modo da garantire le risorse necessarie alla trasmissione, rendendola piu' affidabile.
- Una connessione successiva tra gli stessi nodi potrebbe definire un circuito virtuale differente dal precedente.

Utilizzare Connectionless vs. Connection Oriented

Caratteristica	Connectionless	Connection Oriented
Creazione circuito	Non richiesto	Richiesto
Indirizzamento	Ogni pacchetto contiene gli indirizzi sorgente e destinazione completi	Ogni pacchetto contiene un piccolo numero VC (Virtual Circuit)
Informazioni di stato	La sottorete non conserva informazioni di stato	Ogni circuito virtuale richiede spazio di tabella nella sottorete
Instradamento	Ogni pacchetto è instradato indipendentemente	Percorso scelto alla creazione del circuito virtuale: tutti i pacchetti seguono questo percorso
Effetti dei guasti nei router	Nessuno, a parte i pacchetti persi durante il guasto	Tutti i circuiti virtuali che passano attraverso il router guasto vengono terminati
Controllo di congestione	Complesso	Semplice se può essere allocato spazio sufficiente in anticipo per ogni circuito virtuale

Instradamento ed inoltro

La funzione principale dello strato di rete è l'instradamento (routing). Questo è il processo che permette al router di scegliere – tramite un algoritmo – la linea di uscita verso cui instradare i dati, questa operazione sarà ripetuta per ogni pacchetto nel caso connectionless, o una sola volta all'inizio per l'istradamento connection oriented.

Concettualmente si possono distinguere due operazioni:

- **Inoltro (forwarding):** il processo che, in base all'indirizzo di destinazione o al circuito virtuale, sceglie la linea di uscita in funzione di dati noti (tabelle, stato delle linee, ...). È la singola decisione di inoltro del pacchetto, ed è una decisione locale.
- **Instradamento:** il processo di creazione ed aggiornamento della tabella (detta tabella di routing) che associa alla destinazione la linea di uscita da utilizzare; questa operazione viene eseguita in base ad algoritmi detti algoritmi di routing. Viene fatto su un grafo di rete, ed è una decisione globale.

Per molti algoritmi queste sono operazioni distinte eseguite in momenti diversi da processi distinti all'interno dello strato di rete.

Routing information base: una tavola che ha l'indirizzo di rete con cui fare matching per la destinazione.

Caratteristiche di un algoritmo di routing

È desiderabile che un algoritmo di routing abbia le seguenti caratteristiche:

- **correttezza:** ovvio.
- **semplicità:** meno soggetto ad errori in implementazione o in esecuzione.
- **robustezza:** la rete non è stabile, e l'algoritmo deve poter fare fronte alle modifiche di topologia.
- **stabilità:** convergenza verso l'equilibrio.
- **imparzialità:** servire qualunque tragitto possibile senza penalizzare nessuno.
- **ottimizzazione:** soluzione che mi permette di impegnare nel miglior modo il mezzo che sfruttiamo.

INTERNET PROTOCOL (IP)

È uno standard di fatto, è il protocollo di rete della suite TCP/IP. Definito negli RFC 791 e 1122. Dall'RFC (Request for comment) 791:

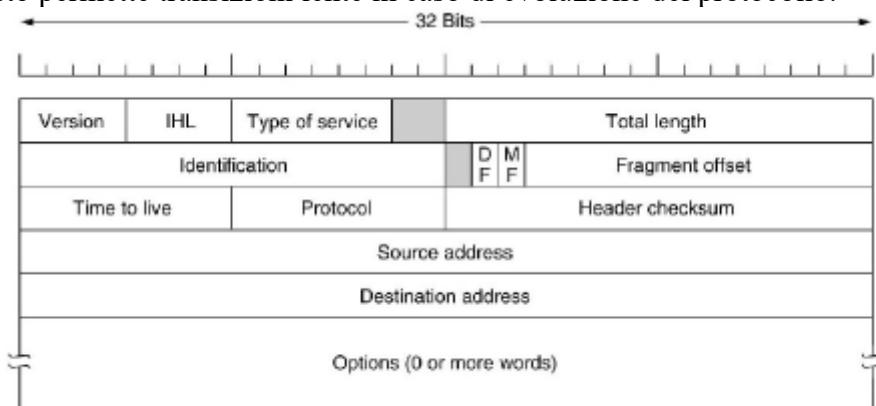
L'IP ha la funzione di recapitare un insieme di bit (internet datagram) dalla sorgente alla destinazione attraverso un sistema di reti interconnesse. Non sono previsti meccanismi di affidabilità, controllo di flusso, sequenzialità, rilevazione o correzione di errore. Il recapito viene operato direttamente se la destinazione appartiene alla stessa rete della sorgente, attraverso un sistema intermedio (router) altrimenti. Se possibile il datagramma viaggia intero, altrimenti viene spezzato in più parti, ciascuna trasportata poi individualmente; in questo caso il datagramma viene riassemblato a destinazione. L'Ip si preoccupa di trasmettere il datagramma da un host all'altro, fino alla destinazione, una rete alla volta.

Questa definizione corrisponde ad un protocollo che fornisce un servizio connection less cioè inaffidabile.

L'indirizzo ip non identifica la macchina, ma il punto di attacco alla rete, cioè un'interfaccia associata alla rete. Per poter identificare il destinatario, ogni host e router devono avere un indirizzo (IP) univoco, che distingue la rete di appartenenza dalle altre, e l'host dagli altri host appartenenti alla stessa rete. L'indirizzamento IP è gerarchico, a due livelli: indirizzo di rete ed indirizzo di host, a differenza di quello Ethernet che è piatto, in realtà ogni interfaccia di rete (cioè ogni connessione ad una rete) deve avere un indirizzo IP, generalmente i PC hanno una sola interfaccia di rete, ma i router (sempre) o i server di grosse dimensioni (talvolta) hanno più interfacce di rete: ciascuna di queste deve avere un indirizzo IP tutti i nodi IP hanno un ulteriore indirizzo, detto loopback, che rappresenta un indirizzo fittizio indicante "se stesso", ed utilizzato per motivi di diagnostica o per simulare connessioni di rete di un host con se stesso.

Struttura dell'indirizzo IP

L'indirizzo IP è costituito da 32 bit, o 4 byte, generalmente rappresentati da 4 numeri decimali di valore compreso tra 0 e 255, separati da un punto, ad esempio: 10.103.0.21. Questo indirizzo contiene una parte che specifica la rete, ed una parte che identifica l'host all'interno di quella rete. Il pacchetto IP è costituito da un header di lunghezza fissa 20 byte, più una parte opzionale (fino a 40 byte). Il campo version contiene il numero identificativo della versione di IP (per IPv4 è 4, per IPv6 è 6), questo permette transizioni lente in caso di evoluzione del protocollo.



- Il campo **IHL** (4 bit) contiene la lunghezza dell'header in parole di 32 bit (quindi un massimo di 60 byte complessivi).
- Il campo **type-of-service** serve ad indicare diverse classi di servizio (precedenza del pacchetto, basso ritardo, etc.), di solito ignorato dai router.
- **total-length** indica la lunghezza totale del pacchetto in byte, che ha un valore massimo di 65535.
- Il campo **version** indica la versione di IP che si sta utilizzando (Ipv4 e Ipv6).
- I campi identification, DF, MF e fragment-offset sono dedicati alla frammentazione: ogni datagramma IP inviato da una sorgente ha un numero identificativo differente dagli altri.

altri, riportato nel campo identification, se un datagramma viene frammentato, ogni frammento contiene nel campo identification lo stesso valore, mentre nel campo fragment-offset viene indicata la posizione del primo byte del frammento rispetto all'inizio del datagramma, espressa in multipli di 8 byte. In base all'identification la destinazione puo' raggruppare i diversi frammenti, in base a total-length ed agli offset, la destinazione puo' valutare se si fossero persi frammenti del datagramma:

il bit **MF** (More Fragments) viene impostato a 0 nell'ultimo frammento (o nel datagramma se non viene frammentato), ad 1 altrimenti.

il bit **DF** (Don't Fragment) viene impostato ad 1 se il datagramma non deve essere frammentato.

- Il campo **time-to-live** è un contatore che viene decrementato via via che il pacchetto viaggia in rete (hop tra gli host). Il pacchetto viene buttato via quando il time-to-live arriva a zero. Normalmente dovrebbe essere decrementato ad ogni secondo o ad ogni hop, ma talvolta i router non tengono conto del tempo
- Il campo **protocol** indica il protocollo di livello superiore a cui sono destinati i dati del pacchetto, vi sono diversi protocolli che possono fare uso di IP, come TCP (6) ed UDP (17), ma anche ICMP (1) ed altri.
- Il campo **checksum** contiene un codice CRC a 16 bit relativo al solo header viene controllato solo l'header per motivi di performance, secondo la logica di TCP/IP che delega il controllo della affidabilita' ai livelli superiori, il campo checksum viene ricalcolato ad ogni hop, in quanto alcuni dei campi precedenti (come quelli relativi alla frammentazione o time-to-live) cambiano durante il trasferimento del pacchetto.
- **Source e destination address** contengono gli indirizzi a 32 bit del sorgente e del destinatario del pacchetto.
- Le **opzioni aggiuntive** dell'header vengono utilizzate, se necessario, per svariati motivi, tra cui:

security options: classifica il pacchetto da "non classificato" a "top secret"; router che onorano questi campi possono essere indotti a instradamenti differenti in base a questa opzione.

record route: istruisce i router a registrare il loro indirizzo nei successivi campi opzionali via via che il pacchetto transita in rete (usato per motivi di debug del routing).

loose o strict source routing: istruisce i router a seguire un instradamento specifico definito dalla sorgente (che riempie i campi opzionali con gli indirizzi dei router che il pacchetto deve attraversare).

Sono disponibili 40 byte per queste opzioni, ogni campo inizia con un ottetto che definisce il tipo di estensione, seguito eventualmente da uno o piu' ottetti contenenti le informazioni relative (indirizzi IP, timestamp, ...).

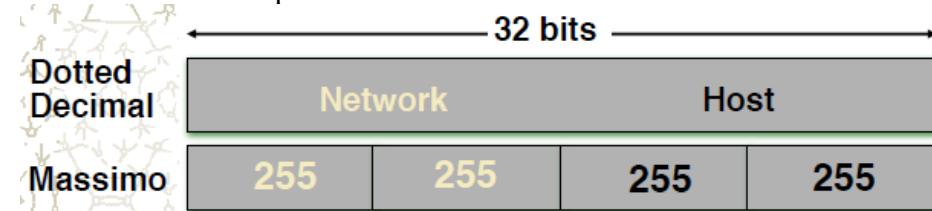
Divisione indirizzi IP

Sono divisi in due parti

- **prefisso:** identifica la rete
- **suffisso:** identifica host/interface

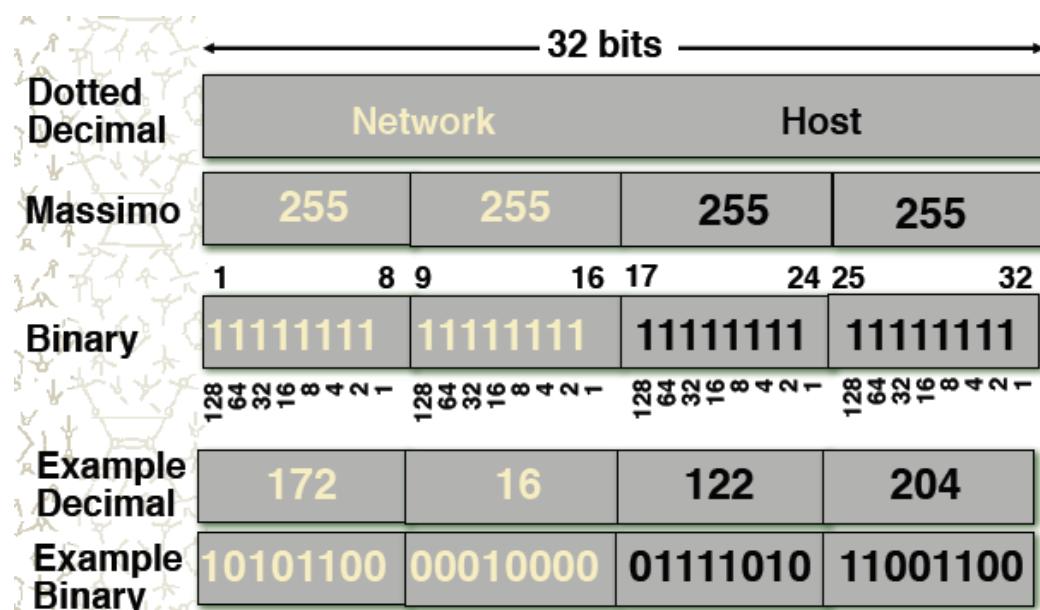
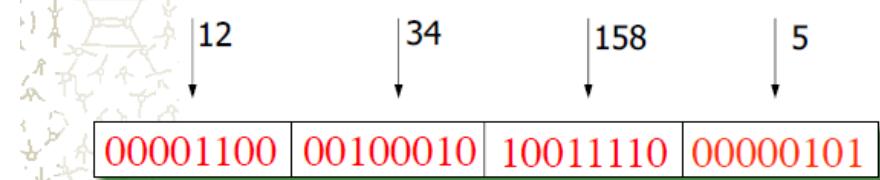
Un indirizzo IP **non identifica** un computer, ma una connessione computer-rete. Un computer con connessioni multiple di rete (e.g., un router) ha assegnato un indirizzo IP per ogni connessione.

Esiste una totale indipendenza dell'indirizzo IP dall'indirizzamento hardware (MAC).



Modo sintetico per esprimere indirizzi IP: rappresentare ogni otetto in decimale usando punti come separatori.

Esempio: 12.34.158.5

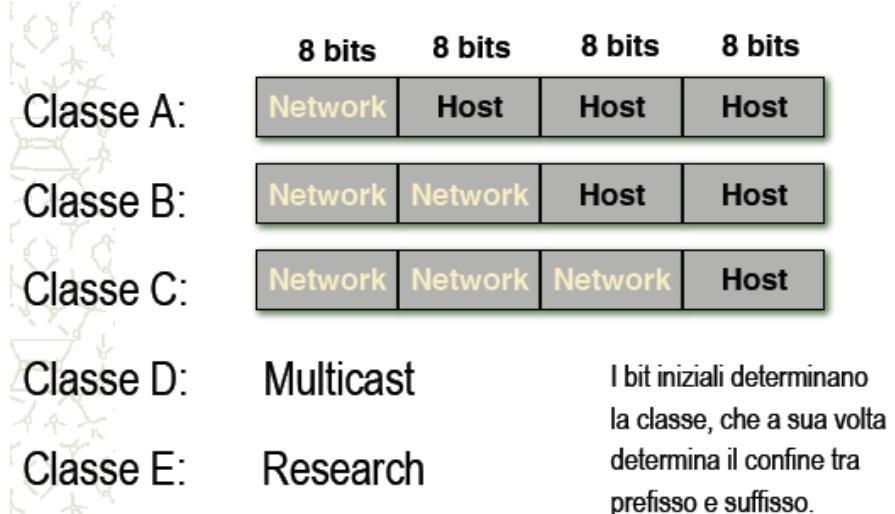


Gli indirizzi IP sono raggruppati in diverse categorie, dette classi:

- **indirizzi di classe A:** tutti quelli che iniziano con un bit 0, cioe' con il primo byte di valore compreso tra 0 e 127. Gli indirizzi di classe A hanno il primo byte dedicato all'indirizzo di rete, i restanti all'indirizzo di host; ad esempio, l'indirizzo 20.9.0.200 individua l'host appartenente alla rete "20", il cui indirizzo di host e' 9.0.200. Esistono quindi 125 network di classe A (le reti 0, 10 e 127 non vengono utilizzate), ciascuna rete di classe A puo' indirizzare 2^{24} host differenti (quasi 17 milioni). Abbiamo due indirizzi speciali uno di rete ed un'altro di broadcast, dobbiamo togliere anche quelli dalla classe A perchè riservati.
- **indirizzi di classe B:** tutti quelli che iniziano con la sequenza di bit 10, cioe' con il primo byte di valore compreso tra 128 e 191, gli indirizzi di classe B hanno i primi due byte dedicati all'indirizzo di rete, i restanti due dedicati all'indirizzo di host. 131.154.10.21 indica l'host di indirizzo "10.21" appartenente alla rete "131.154", esistono quindi 16383

reti di classe B, ciascuna contenente 65533 host.

- **indirizzi di classe C:** tutti quelli che iniziano con la sequenza di bit 110, cioè con il primo byte di valore compreso tra 192 e 223, questi indirizzi hanno i primi tre byte dedicati alla rete, il quarto all'indirizzo di host (193.206.144.1 indica l'host "1" della rete "193.206.144"). In classe C esistono circa 2 milioni di reti, ciascuna contenente al piu' 254 host.
- **indirizzi di classe D:** tutti quelli che iniziano con la sequenza di bit 1110, cioè con il primo byte compreso tra 224 e 239, gli indirizzi di classe D sono dedicati all'indirizzamento dei gruppi multicast.
- **indirizzi di classe E:** tutti quelli che iniziano con la sequenza di bit 1111, cioè con il primo byte compreso tra 240 e 255, gli indirizzi di classe E sono dedicati ad utilizzi sperimentali, e non devono mai essere utilizzati come effettivo indirizzo di macchine sulla rete.



Bits:	1	8 9	16 17	24 25	32
Classe A:	ONNNNNNN		Host	Host	Host
	Range (1-126)				
Bits:	1	8 9	16 17	24 25	32
Classe B:	10NNNNNN		Network	Host	Host
	Range (128-191)				
Bits:	1	8 9	16 17	24 25	32
Classe C:	110NNNNN		Network	Network	Host
	Range (192-223)				
Bits:	1	8 9	16 17	24 25	32
Classe D:	1110MMMM	Multicast Group	Multicast Group	Multicast Group	
	Range (224-239)				

Indirizzi speciali

L'indirizzo contenente tutti "0" nel campo di host viene utilizzato per indicare la rete:

- l'indirizzo 10.0.0.0 indica la rete "10" (di classe A)
- l'indirizzo 193.206.144.0 indica la rete "193.206.144" (di classe C)

L'indirizzo 0.0.0.0 ha il significato di "questo host di questa rete", e viene utilizzato dai calcolatori che, in fase di boot, non conoscono ancora il proprio indirizzo IP. L'indirizzo IP con tutti "0" nella parte di rete ha il significato di "questa rete"; ad esempio, se l'host 193.206.144.10 vuole inviare sulla rete locale un pacchetto all'host 193.206.144.20, puo' indirizzarlo a **0.0.0.20**. Queste convenzioni spiegano perche' la rete di classe A: 0.0.0.0 non venga utilizzata come rete indirizzabile

in IP: ad esempio, se così non fosse, il pacchetto indirizzato all'host 1 di una qualunque rete tramite la notazione "questa rete". 1 non potrebbe essere distinto dal pacchetto indirizzato all'host 1 della rete **0.0.0.0**.

Le *Reti Interne* sono definite come le reti elettriche senza obbligo di connessione di terzi questi indirizzi possono essere usati solo su reti locali, per andare sulla rete globale internet si deve fare il NAT. Il **network address translation** o **NAT**, ovvero *traduzione degli indirizzi di rete*, conosciuto anche come **network masquerading**, **native address translation**, è una tecnica che consiste nel modificare gli indirizzi IP contenuti negli header dei pacchetti in transito su un sistema che agisce da router all'interno di una comunicazione tra due o più host. Sono molto note anche alcune tipologie specifiche di NAT, come l'IP masquerading e il portforwarding.

L'indirizzo 255.255.255.255 (tutti bit 1) rappresenta l'indirizzo broadcast della rete locale direttamente connessa è l'indirizzo utilizzato per inviare un pacchetto IP broadcast sulla propria rete. Il 255.255.255.255 rappresenta il layer 3 broadcast.

L'indirizzo con tutti 1 nel campo host rappresenta l'indirizzo broadcast della rete specificata nel campo rete; ad esempio: l'indirizzo 130.90.255.255 indica l'indirizzo broadcast della rete 130.90.0.0, questo meccanismo permette di indirizzare un pacchetto a tutti gli host di una rete remota. Se mando da una rete locale 192.168.0.0 ad una rete 192.168.255.255 è come se stessi trasmettendo su 255.255.255.255 .

Indirizzi dedicati a scopi speciali

La rete di classe A 127.0.0.0 e' dedicata all'interfaccia di loopback; l'interfaccia prende sempre l'indirizzo 127.0.0.1 . Tre range di indirizzamento stabiliti dalla RFC 1918 sono dedicati ad indirizzi privati:

- 10.0.0.0 (una rete di classe A)
- da 172.16.0.0 a 172.31.0.0 (16 reti di classe B)
- da 192.168.0.0 a 192.168.255.0 (256 reti di classe C)

Il range 100.64.0.0/10 (questo indica quanto è lungo il prefisso definito dalla **maschera di rete**) è riservato secondo la RFC 6598 alle comunicazioni fra provider e subscriber (in presenza di carrier grade NAT). Il range 198.18.0.0/15 è riservato secondo la RFC 2544 per i test di comunicazioni fra diverse internetworks. Gli indirizzi privati possono essere utilizzati all'interno di una rete privata, ma non devono mai venire annunciati nelle tabelle di routing (così come la rete dell'interfaccia di loopback).

Il routing verso le macchine ad indirizzo privato deve essere fatto dal router di interconnessione con la rete pubblica ad insaputa del resto della rete; lo scopo degli indirizzi privati è quello di poter utilizzare la tecnologia TCP/IP in una realtà locale senza dover necessariamente chiedere ed utilizzare indirizzi pubblici, una tecnica diffusa che fa uso di questi indirizzi per dare connettività senza sprecare indirizzi pubblici è il NAT (Network Address Translation) che vedremo in seguito. Affinchè tutto funzioni correttamente in una internet gli indirizzi devono essere assegnati da una autorità centrale che garantisca innanzi tutto l'unicità delle assegnazioni. Per Internet gli indirizzi sono assegnati dalla ICANN (Internet Corporation for Assigned Names and Numbers). La ICANN ha poi delegato organizzazioni regionali (Europa, Asia, America, ...) assegnando loro gruppi di indirizzi da riassegnare al loro interno; per l'Europa: RIPE (*Réseaux IP Européens*) NCC. A loro volta le organizzazioni regionali possono delegare verso il basso, partizionando gli indirizzi a loro destinati dalla ICANN; in Italia: diverse istituzioni (ISP); per gli enti di ricerca si deve chiedere a GARR.

Carenza di indirizzi

Lo spazio di indirizzamento disponibile conta due miliardi di indirizzi, raggruppabili in 16500 reti di enormi dimensioni e 2 milioni di reti di piccole dimensioni.

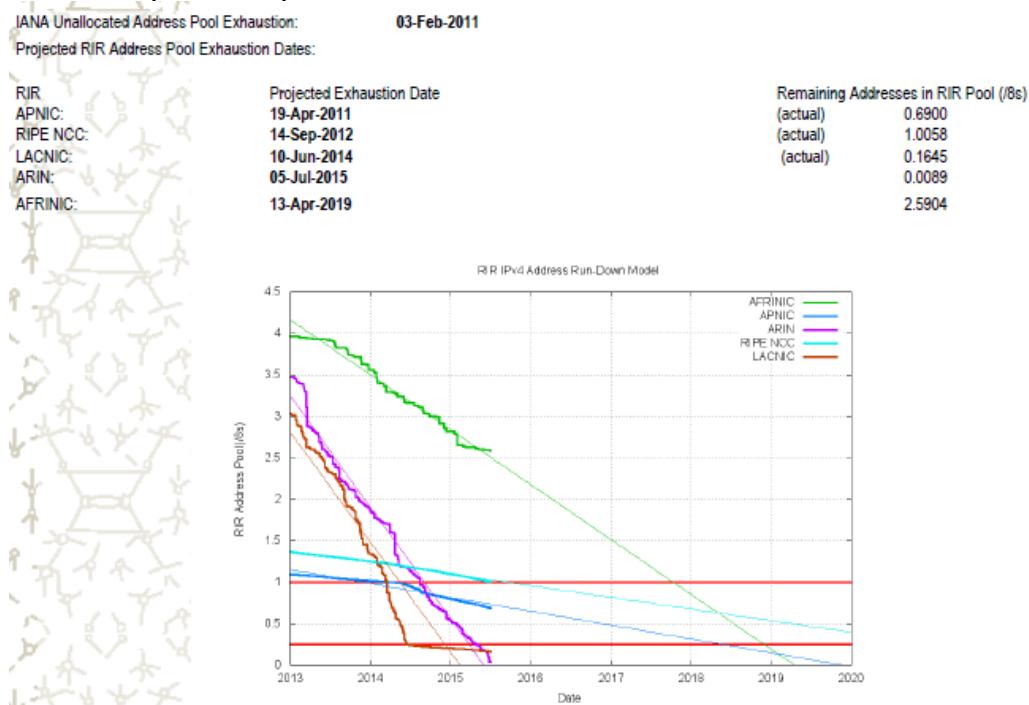
Sembrava impossibile esaurire lo spazio di indirizzamento ma la 100000-sima rete si è connessa in Internet nel 1996!

Tre i fattori che hanno determinato l'insorgere di problemi:

- lo spazio di indirizzamento delle classi A, e spesso anche quello delle classi B, è troppo vasto: nessuna rete può contenere 16 milioni di nodi distinti, o anche solo 65000. Un enorme numero di indirizzi infatti rimangono inutilizzati, una azienda o campus a cui è stata assegnata una classe A che deve estendere la sua rete per interconnettere diversi dipartimenti su reti locali distinte hanno bisogno di altre reti, benché il numero di indirizzi disponibile ecceda di gran lunga la necessità di indirizzi di host.
- la connessione punto-punto tra due router richiede l'utilizzo di una rete IP, per la quale sono utilizzati solo due indirizzi.
- lo spazio di indirizzamento delle reti di classe C risulta troppo piccolo con il crescere delle reti locali.

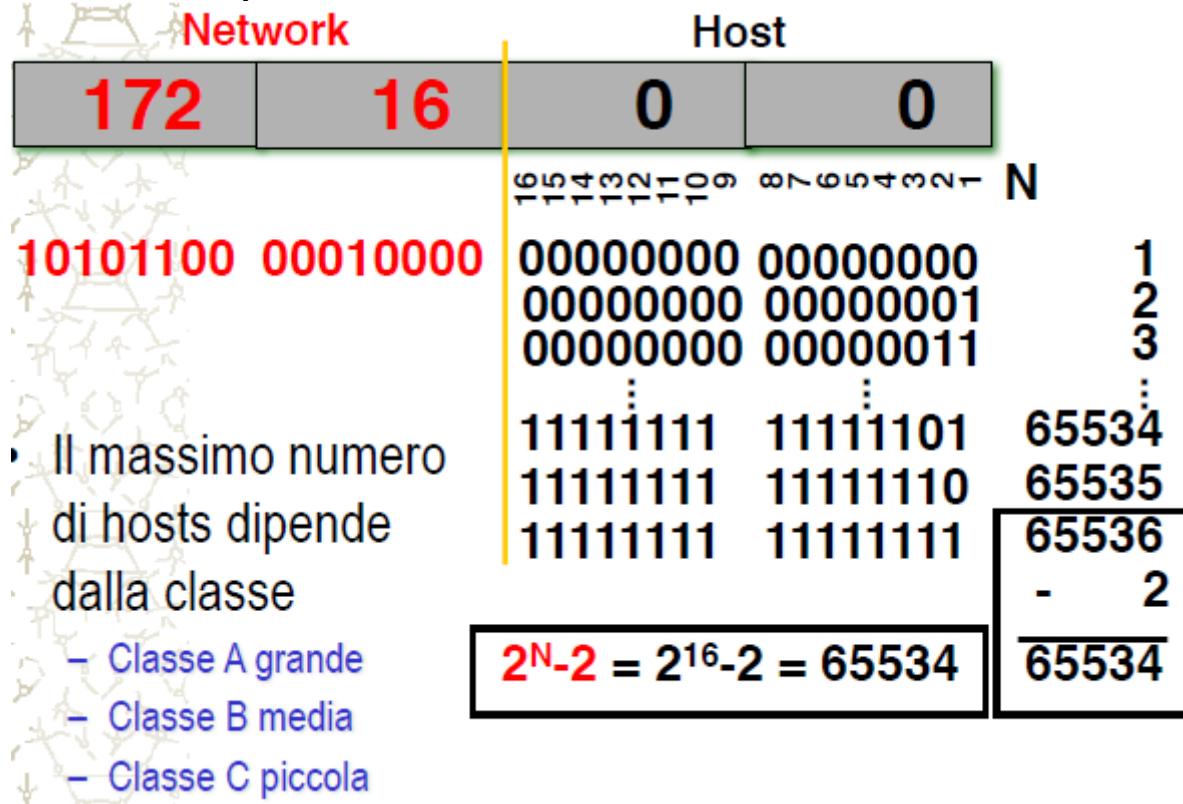
Ci sono tre soluzioni a questo problema:

- Nuova versione del protocollo IP(IPv6) passando da 32 a 128 bit.
- Logica NAT.
- Razionare l'uso dello spazio di indirizzamento perché le classi usate fino ad adesso sprecano molto spazio che portano ad una formattazione interna.



Per evitare che terminassero sono stati utilizzati alcuni indirizzi che non lo erano per motivi sperimentali.

Calcolo indirizzi disponibili in una rete



Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16
256.241.20.10	Nonexistent		

Subnetting (sottorete)

Per risolvere i problemi di carenza di indirizzi di rete è stata sviluppata una tecnica detta subnetting: un campus a cui e' stata assegnata una rete di classe A può suddividere il suo campo di indirizzi in gruppi piu' piccoli, trattando ogni gruppo come se fosse una "rete" a se stante; ad esempio, se la rete assegnata e' la 100.0.0.0, il campus puo' dedicare gli indirizzi 100.1.0.0 ad un dipartimento, gli indirizzi 100.2.0.0 ad un secondo dipartimento e cosi' via, trattando le due reti come se fossero reti di classe B, affinche' tutto funzioni a dovere, il router del campus dovrà annunciare verso l'esterno la sola rete di classe A, mentre internamente potra' trattare i vari pezzi come se fossero reti piu' piccole; per implementare le sottoreti e' necessario introdurre una informazione aggiuntiva agli indirizzi di rete, che specifichi quali bit dell'indirizzo definiscano l'indirizzo della (sotto)rete e quali definiscano l'indirizzo degli host.

Network mask

Per identificare quali bit definiscono la rete e quali bit l'host, si utilizza una “maschera”, anch’essa costituita da 32 bit, col significato seguente:

- se un bit della maschera vale 1, il corrispondente bit dell’indirizzo fa parte dell’indirizzo della rete
- se un bit della maschera vale 0, il corrispondente bit dell’indirizzo fa parte dell’indirizzo di host

Con questa convenzione, gli indirizzi di classe A hanno maschera 255.0.0.0, quelli di classe B hanno maschera 255.255.0.0, quelli di classe C hanno maschera 255.255.255.0. Utilizzando opportunamente le maschere è possibile spezzare una rete in sottoreti:

100.1.0.0 con maschera 255.255.0.0 indica una rete che puo’ indirizzare gli host da 100.1.0.1 a 100.1.255.254

Tutte le reti possono essere “subnigate”, anche le classi C:

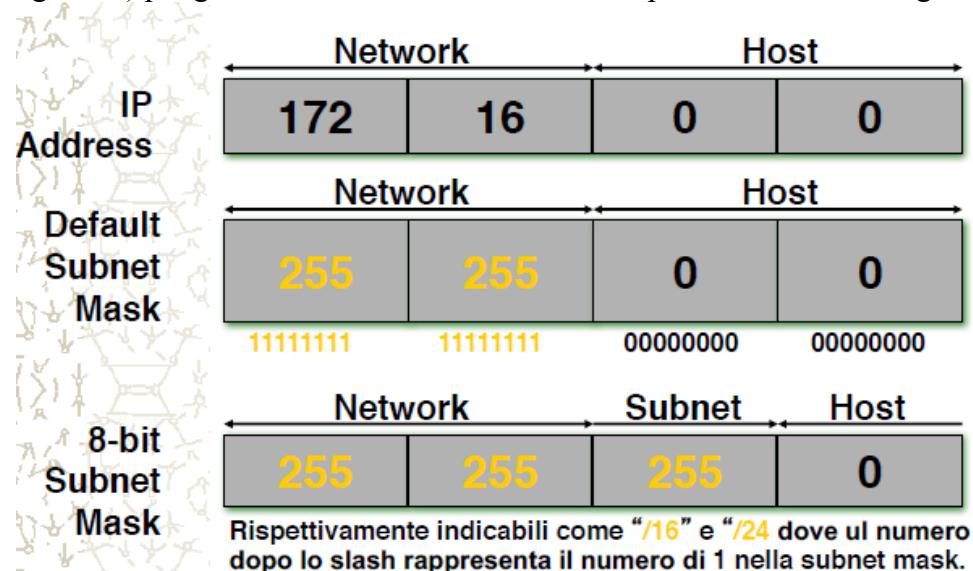
la rete 193.206.144.0 (classe C) puo’ essere ad esempio suddivisa in quattro sottoreti:

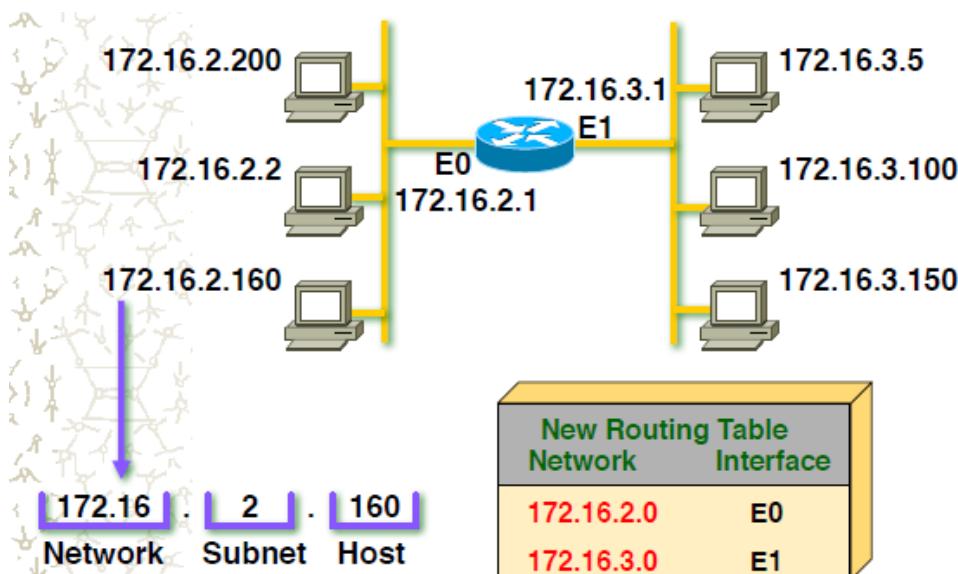
- 193.206.144.0 255.255.255.192 (indirizzi da 0 a 63)
- 193.206.144.64 255.255.255.192 (indirizzi da 64 a 127)
- 193.206.144.128 255.255.255.192 (indirizzi da 128 a 191)
- 193.206.144.192 255.255.255.192 (indirizzi da 192 a 255)

Una notazione molto diffusa per indicare la maschera è quella di indicare in coda all’indirizzo il numero di bit, a partire dal piu’ significativo, che costituiscono l’indirizzo di rete:

- la rete 131.154.20.0 255.255.255.0 si indica anche con la notazione 131.154.20.0/24: i primi 24 bit costituiscono l’indirizzo di rete
- la subnet 193.206.144.64 255.255.255.192 si indica con 193.206.144.64/26 (26 bit per l’indirizzo di rete)

Vale la pena di osservare che la sottorete di dimensioni minime deve avere un campo di 4 indirizzi: uno per indicare la sottorete, uno per indicare il broadcast, ed almeno uno per indirizzare un host; poiche’ al campo host vanno assegnati un certo numero di bit, un bit non è sufficiente, quindi ne servono almeno due, che forniscono due indirizzi per host, questa tecnica è utilizzata per assegnare indirizzi di rete alle connessioni punto-punto tra i router, risparmiando il maggior numero di indirizzi possibili. La definizione delle sottoreti non coinvolge la authority internazionale (o quella regionale) per gli indirizzi, le sottoreti fanno tutte parte dell’insieme degli indirizzi già assegnati.





	Network	Subnet	Host
172.16.2.160	10101100	00010000	00000010 10100000
255.255.255.0	11111111	11111111	11111111 00000000
	10101100	00010000	00000010 00000000

128 192 224 240 248 252 254 255

Network Number	172	16	2	0
----------------	-----	----	---	---

L'indirizzo di rete viene esteso di 8 bit a discapito degli hosts.

	Network	Subnet	Host
172.16.2.160	10101100	00010000	00000010 10100000
255.255.255.192	11111111	11111111	11111111 11000000
	10101100	00010000	00000010 10000000

128 192 224 240 248 252 254 255

Network Number	172	16	2	128
----------------	-----	----	---	-----

L'indirizzo di rete viene esteso di 10 bit a discapito degli hosts.

Esempio:

Assumiamo di voler partizionare il netblock 172.16.32.0/20 per ottenere 5 classi da 64 hosts (/26)

Netblock da partizionare: 172.16.32.0/20

In binario 10101100.00010000.00100000.00000000

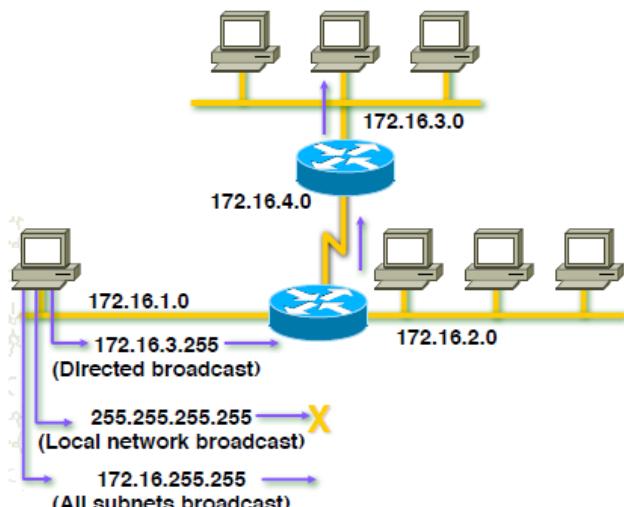
Prima subnet /26: 172.16.32.0/26

In binario 10101100.00010000.00100000.00000000

	Network	Subnet	VLSM Subnet	Host
1st subnet:	10101100 . 00010000	.0010	0000.00	000000=172.16.32.0/26
2nd subnet:	172 . 16	.0010	0000.01	000000=172.16.32.64/26
3rd subnet:	172 . 16	.0010	0000.10	000000=172.16.32.128/26
4th subnet:	172 . 16	.0010	0000.11	000000=172.16.32.192/26
5th subnet:	172 . 16	.0010	0001.00	000000=172.16.33.0/26

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0	B	172.16.2.0
10.6.24.20	255.255.240.0	A	10.6.16.0
10.30.36.12	255.255.255.0	A	10.30.36.0

Indirizzi Broadcast per Subnets



IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

Network	Network	Subnet	Host
172.16.2.121: 10101100	00010000	00000010	01111001
255.255.255.0: 11111111	11111111	11111111	00000000
Subnet: 10101100	00010000	00000010	00000000
Broadcast: 10101100	00010000	00000010	11111111

- Subnet Address = 172.16.2.0
- Host Addresses = 172.16.2.1–172.16.2.254
- Broadcast Address = 172.16.2.255
- 8 bit per ogni subnet

Quando si fa subnetting aumenta il numero di reti che vado a dimezzare questo porta ad un aumento delle dimensioni della routing table.

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248	C	201.222.10.56	201.222.10.63
15.16.193.6	255.255.248.0	A	15.16.192.0	15.16.199.255
128.16.32.13	255.255.255.252	B	128.16.32.12	128.16.32.15
153.50.6.27	255.255.255.128	B	153.50.6.0	153.50.6.127

Aggregazione di reti

L'indirizzamento a classi ha anche portato al problema opposto:

- una classe C prevede un massimo di 254 indirizzi (lo 0 ed il 255 non sono utilizzabili), spesso aziende o universita' hanno aumentato il numero di host connessi in rete fino ad eccedere questo limite.

Utilizzando la tecnica della maschera e' possibile accorpare classi C con indirizzi contigui opportuni:

ad esempio, la sezione INFN di Genova ha avuto assegnate 4 classi C, dalla 193.206.144.0 alla 193.206.147.0

il valore binario di queste reti e'

11000001 11001110 10010000 00000000
 11000001 11001110 10010001 00000000
 11000001 11001110 10010010 00000000
 11000001 11001110 10010011 00000000

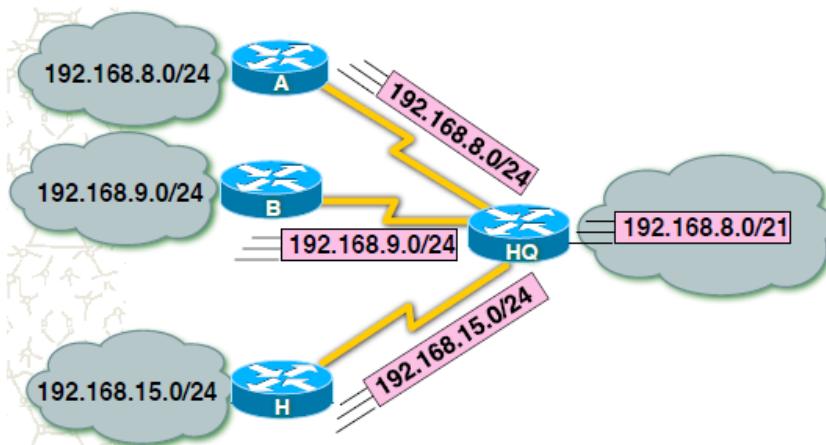
utilizzando una maschera a 22 bit e' possibile accorpare queste quattro reti in una unica rete IP indicata come 193.206.144.0/22 (o con maschera 255.255.252.0).

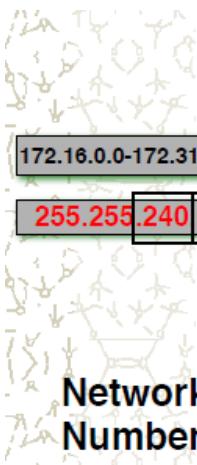
Classless InterDomain Routing

Per gestire questo nuovo schema di indirizzamento il modo in cui il router gestisce le tabelle di routing deve cambiare. È stato introdotto un nuovo standard che specifica queste modifiche (RFC 1519), col nome di CIDR. Secondo questo standard ogni record della tabella di routing specifica l'indirizzo della destinazione con la sua maschera, in modo da superare la definizione delle classi. Non esiste più una vera distinzione tra una rete 100.1.2.0/24 ed una rete 200.201.20.0/24

Questa soluzione comporta però un problema potenziale grave:

l'aumento considerevole delle reti indirizzabili può far esplodere la dimensione delle tabelle di routing, che virtualmente potrebbero dover contenere milioni di record. Per ovviare a ciò gli indirizzi vengono assegnati per quanto possibile a blocchi alle varie organizzazioni regionali e locali che devono annunciare verso l'esterno della loro area solo una rete, che costituisce l'aggregato delle sottoreti al suo interno.





	Network	Subnet	Host
172.16.0.0-172.31.0.0	10101100	00010000	00000000 00000000
255.255.240.0	11111111	11110000	00000000 00000000
	10101100	00010000	00000000 00000000
	128 192 224 240 252 254 255	240	128 192 224 240 248 254 255 128 192 224 240 248 252 254 128 192 224 240 248 254 255
Network Number	172	16	0 0 /12

Aggregate 16 sottoreti riducendo il network address di 4 bits.

Instradamento e CIDR (longest prefix match)

I pacchetti IP non sanno nulla delle maschere: come instradare?

Supponiamo di dover instradare un pacchetto indirizzato a 130.251.61.129, e di avere nelle tabelle di routing:

- 130.0.0.0/8 verso l'interfaccia 1
- 130.251.0.0/16 verso l'interfaccia 2
- 130.251.61.0/24 verso l'interfaccia 3
- 130.251.61.64/26 verso l'interfaccia 4

La scelta viene sempre fatta verso la rete (adatta) che ha la maschera piu' lunga, nell'esempio si ha:

- 1000010 1111011 0011101 10000001 (indirizzo di destinazione)
- 1000010 (130.0.0.0/8)
- 1000010 1111011 (130.251.0.0/16)
- 1000010 1111011 0011101 (130.251.61.0/24)
- 1000010 1111011 0011101 01 (130.251.61.64/26)

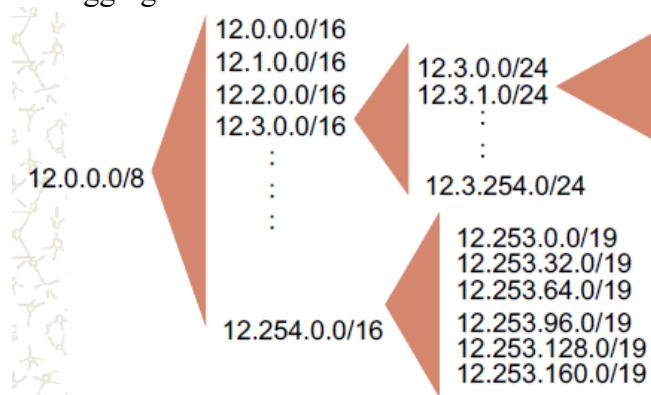
In questo caso l'indirizzo non fa parte della rete relativa alla quarta riga, ma puo' far parte delle reti relative alle altre righe; tra queste si sceglierà l'interfaccia 3 perché è quella verso la rete adatta (matching prefix) con la maschera piu' lunga.

In caso che le due subnet abbiano la stessa lunghezza si fa bilanciamento di carico, cioè una volta si usa una e un'altra volta un'altra.

CIDR: Hierarchical Address Allocation

Il CIDR è il meccanismo di base per la scalabilità di Internet:

- Indirizzi vengono allocati e distribuiti in blocchi contigui (prefix blocks)
- I protocolli e i meccanismi di routing lavorano su questi prefissi
- Aggregando si riesce a contenere la dimensione delle routing tables



IPv6

All'inizio degli anni '90 l'IETF inizio' la ricerca di un successore di Ipv4.

Motivazione primaria: la necessita' di ampliare lo spazio di indirizzi che potesse soddisfare tutte le nuove esigenze di interconnessione di nuovi elaboratori. Basandosi sul trend dell'epoca si affacciavano previsioni di esaurimento degli indirizzi tra il 2008 e il 2018. Nel 1996 l'American Registry for Internet Numbers dichiarava esaurita la classe A, risultava assegnato il 62% dello spazio indirizzi di classe B e il 37% di quelli della classe C. Sebbene questo consentisse comunque ancora del tempo prima dell'esaurimento totale, lo sforzo necessario e il tempo previsto per trovare un'alternativa stimolo' l'avvio dello studio e progettazione di un nuovo protocollo. Fu sviluppato un protocollo che i progettisti modellarono sull'IPv4 esistente, ampliando e migliorando alcune sue caratteristiche, chiamato IPv6 (o IPng: next generation).

Obiettivi:

- Indirizzamento illimitato
- Semplicita' del protocollo per ridurre i tempi di elaborazione nei router
- Sicurezza
- Supporto per pacchetti di grosse dimensioni
- Gestione del tipo di servizio
- Prevedere evoluzioni future del protocollo
- Supportare i protocolli di livello superiore che si appoggiano ad Ipv4

indirizzi

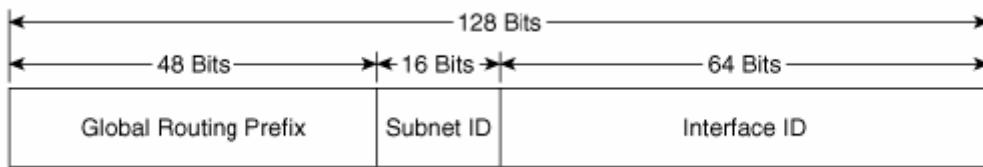
IPv6 prevede l'utilizzo di indirizzi a 16 byte (128 bit). La notazione utilizzata e' una sequenza di otto gruppi di quattro cifre esadecimali, separate da ":".

8000:0000:0000:0123:4567:89AB:CDEF

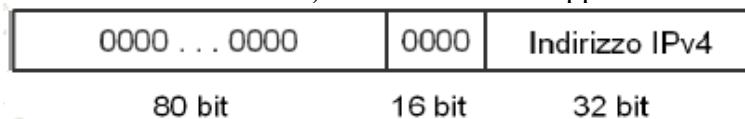
Per rappresentare piu' comodamente gli indirizzi si possono utilizzare ottimizzazioni:

- si possono omettere gli zeri ad inizio di un gruppo (:0123: diventa :123:)
- si possono omettere gruppi di zeri consecutivi, rappresentati da una sequenza "::"

8000::123:4567:89AB:CDEF



Un indirizzo compatibile IPv4 consente a un host che supporta IPv6 di parlare IPv6 anche se il router o i router locali non parlano Ipv6. Gli indirizzi compatibili IPv4 avvisano il software del mittente di creare un tunnel, incapsulando il pacchetto IPv6 in un pacchetto Ipv4. Gli indirizzi IPv4 sono rappresentati con 6 gruppi di zeri, e due gruppi che rappresentano l'indirizzo IPv4 (rappresentabili anche in notazione decimale): ::89AB:CDEF oppure ::137.171.205.239



Gli indirizzi mappati IPv4 consentono a un host che supporta sia IPv4 sia IPv6 di comunicare con un host che supporta solo Ipv4. L'indirizzo IPv6 si basa completamente sull'indirizzo IPv4 e consiste di 80 bit posti a 0 seguiti da 16 bit a uno, seguiti da un indirizzo IPv4 a 32 bit.

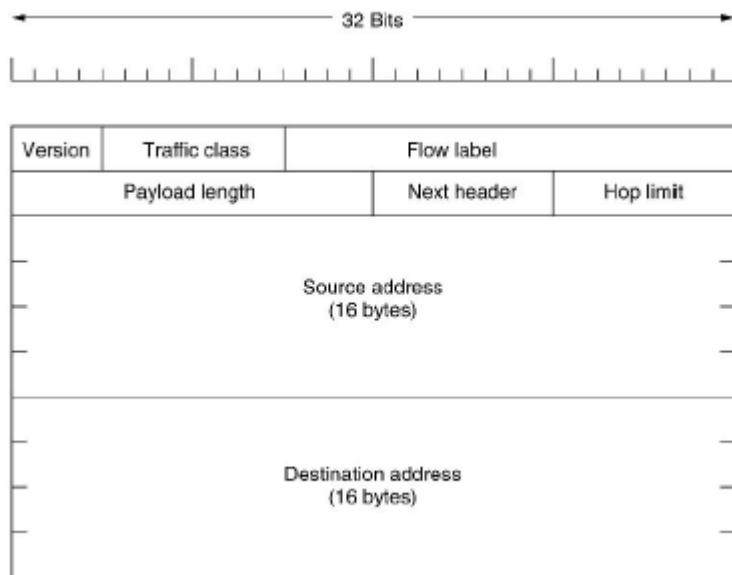


Come per IPv4 l'indirizzo contiene una informazione di rete ed una informazione di host. La notazione per definire quale parte dell'indirizzo e' dedicato alla rete e' quella di specificare la lunghezza in bit dell'indirizzo di rete dopo un "/" in coda all'indirizzo (come in Ipv4). Anche in

IPv6 la “rete” è identificata dall’indirizzo con tutti “0” nel campo di indirizzo dell’host.

Pacchetto IPv6

Il pacchetto IPv6 è costituito da un header di lunghezza fissa (40 byte) ed un campo dati; il campo dati può opzionalmente contenere altri header prima dei dati veri e propri.



Header di IPv6

- Il campo **version** non cambia significato, ed assume il valore 6.
- Il campo **traffic class** serve ad identificare i pacchetti che necessitano di un instradamento particolare, essenzialmente introdotto per supportare il traffico prioritario, o il traffico di tipo voce o video stream che richiede ritardi costanti; un campo simile esiste nell’header di IPv4, inutilizzato.
- Il campo **flow label** è stato introdotto per identificare in qualche modo i pacchetti appartenenti allo stesso flusso trasmissivo:
 1. sempre al fine di supportare meglio il traffico voce/video
 2. è un tentativo di identificare il flusso di dati di una “connessione” in un protocollo connection less
 3. attualmente in fase sperimentale
- Il campo **payload length** indica la lunghezza del pacchetto in byte, esclusi i 40 byte fissi dell’header: la lunghezza massima del pacchetto è di 65536 bytes (+ 40)
- Il campo **next header** indica: il protocollo del livello di trasporto a cui sono destinati i dati (TCP o UDP) se non c’è intestazione estesa
- il **tipo di intestazione estesa** successiva utilizzata (se c’è): in questo caso sarà il corrispondente campo dell’header dell’ultima intestazione estesa a specificare il protocollo di trasporto di destinazione.
- Il campo **hop limit** è equivalente al campo time to live dell’header IPv4, ma ora ha l’esclusivo significato di conto degli hop, viene decrementato ad ogni hop; raggiunto lo zero il pacchetto viene scartato; ha la stessa funzione del corrispondente campo IPv4: evitare che un pacchetto rimanga troppo a lungo in rete in caso di problemi di routing
- Gli ultimi campi sono gli **indirizzi sorgente e destinatario** del pacchetto

caratteristiche di IPv6

Il formato dell’intestazione dei datagrammi è stato notevolmente semplificato. Molti campi sono stati eliminati o modificati. IPv6 prevede più di un intestazione. Con questa variazione è possibile creare intestazioni per ogni tipo di servizio ipotizzabile.

cosa non c'è più

- Il campo **IHL** (Internet Header Length) che rappresenta la lunghezza dell'header non è più necessario, perché la lunghezza dell'header è fissata a 40.
- Il campo **protocol** è sostituito dal campo next header
- I campi riguardanti la **frammentazione**: IPv6 non prevede che i router eseguano frammentazione, perché fa perdere tempo. I nodi IPv6 tentano di identificare la dimensione corretta dei pacchetti da scambiarsi in modo dinamico non basta: se il router non può inoltrare un pacchetto, invia un messaggio (ICMP) indietro per notificare il fatto e butta il pacchetto, di fatto risulta più efficiente fare in modo che l'host di partenza invii i pacchetti di dimensione corretta che non frammentare nei router.
- Il campo **checksum**: IPv6 non utilizza checksum sui suoi pacchetti, per motivi di efficienza, pur nel caso ridotto di un checksum dedicato all'header, il controllo della correttezza risulta un processo molto costoso per i router essendoci meccanismi analoghi a livello di data link ed a livello di trasporto, IPv6 ne fa a meno.

estension header

I progettisti di IPv6 hanno previsto la possibilità di utilizzare header aggiuntivi (extension header), il campo **next header** dell'header fisso identifica con un codice opportuno il tipo di extension header che segue.

Ciascun extension header inizia con 2 byte:

- next header: il tipo di extension header che segue il corrente (o il protocollo di destinazione se il corrente è l'ultimo header)
- extension header length: la lunghezza in byte dell'extension header corrente (i diversi tipi hanno lunghezze differenti, ed alcuni tipi hanno lunghezza variabile) seguita dai dati specifici dell'extension header.

Sono stati definiti 6 tipi di extension header

- **opzioni hop-by-hop**: sono opzioni che tutti i router devono esaminare; al momento è definito un solo tipo di opzione (jumbo datagram) che serve per poter inviare pacchetti di dimensione superiore a 64 KB.
- **opzioni di destinazione**: introdotte per essere interpretate dall'host di destinazione, attualmente non ancora definite (fornisce flessibilità al protocollo per utilizzi futuri).
- **opzioni di routing**: per implementare source-routing, cioè instradamento definito dalla sorgente (simile al loose source routing di Ipv4).
- **opzioni di frammentazione**: da utilizzare se "la sorgente" deve frammentare (i router non frammentano); gestita come in Ipv4.
- **autenticazione**: finalizzata a fornire un meccanismo per accettare l'identità del mittente del pacchetto.
- **crittazione**: finalizzato a proteggere i dati tramite codifiche di cifratura.

trasizione da IPv4 a IPv6

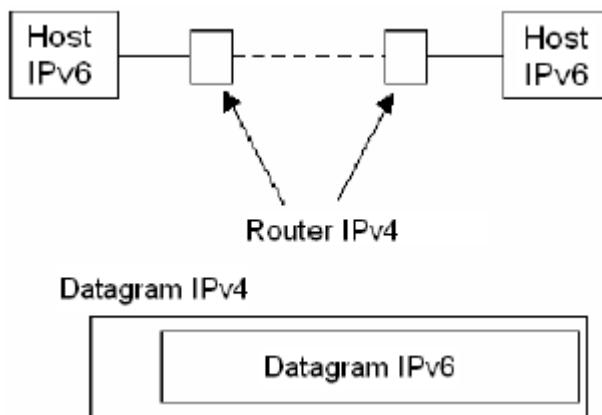
Problema che deve essere affrontato perché mentre l'IPv6 può essere costruito compatibile con IPv4 nel senso che può spedire, instradare e ricevere datagram IPv4, IPv4 non è in grado di gestire datagram Ipv6.

Possibile opzione: definire giorno e ora in cui tutte le macchine si aggiornano da IPv4 a Ipv6. Questa soluzione è stata già provata in passato per altre transizioni quando la rete era ancora agli esordi e provocò non pochi problemi. Diventa ancor più impensabile oggi che i nodi e i router coinvolti sono decine (centinaia?) di milioni.

Opzione nodi dual stack: Questa opzione prevede l'introduzione di nodi Ipv6 compatibili, in cui i nodi IPv6 dispongono pure di una completa implementazione Ipv4. I nodi IPv6/IPv4 (RFC 1933) hanno entrambi gli indirizzi e devono essere in grado di determinare se il nodo con cui devono parlare è un nodo Ipv6 compatibile o solo IPv4. Questo può comunque portare come risultato che

2 nodi IPv6 compatibili si scambino comunque tra loro datagram IPv4.

Tunnelling(incapsulamento) IPv4 e IPv6: Eseguito automaticamente dal kernel quando vengono usati indirizzi IPv6 compatibili IPv4.



Funzionamento con DNS: Un'applicazione IPv6 chiede al DNS (Domain Name System) l'indirizzo di un host, ma l'host ha solo un indirizzo IPv4. Il DNS crea automaticamente l'indirizzo IPv6 mappato IPv4. Il kernel capisce che si tratta di un indirizzo speciale e usa la comunicazione IPv4.

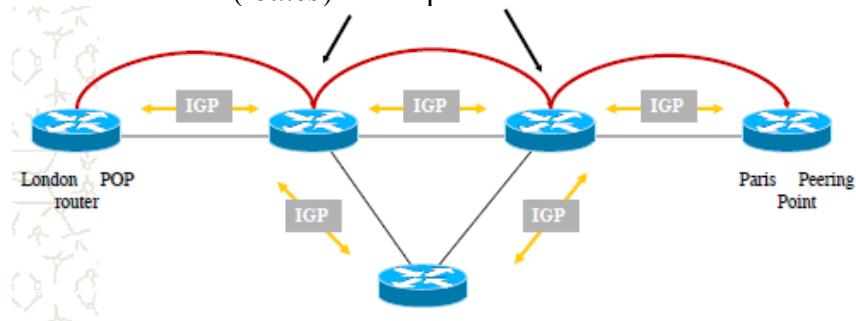
Principi del routing IP: Il routing IP è composto di due momenti:

- **routing control:** scambio di informazioni di routing tra i nodi della rete (routing protocol) per la definizione delle tabelle di routing (processo continuo)
- **packet forwarding** (decisione di instradamento per ogni pacchetto, basata sul solo indirizzo di destinazione)

Il routing IP segue una politica di best-effort dove i pacchetti possono essere:

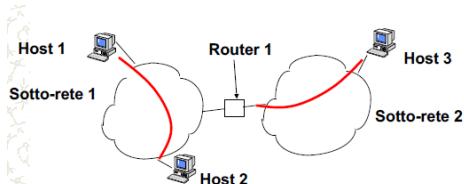
- Ritardati
- Duplicati
- Distribuiti fuori ordine
- Persi
- Possono cambiare percorso da pacchetto a pacchetto dello stesso messaggio

Decisione di routing ad ogni hop: ogni router ha le proprie tabelle di routing, e scambia con i suoi vicini le informazioni sulle strade (*routes*) in suo possesso.



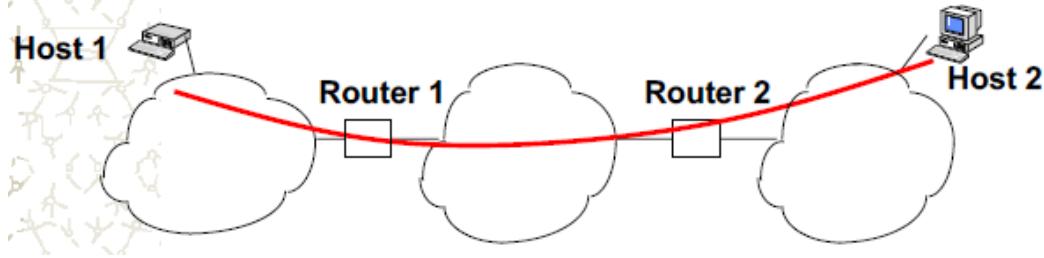
Instrandamento diretto

La trasmissione di un datagramma IP tra due macchine connesse su una stessa sotto-rete (stesso Net_id). Non coinvolge router intermedi. Il trasmettitore IP risolve l'indirizzo fisico dell'host destinatario (tramite il protocollo ARP), incapsula il datagramma nell'unità dati della rete fisica e lo invia verso destinazione. Utilizza i meccanismi propri della rete fisica in questione per inviare il datagramma



Instradamento indiretto

L'host di destinazione non è sulla stessa sotto-rete del mittente. Il mittente deve identificare un router a cui inviare il datagramma; il router deve inviare il datagramma verso la sotto-rete di destinazione. Il router esamina il datagramma IP ricevuto e, se l'host di destinazione non si trova in una sottorete a cui il router è direttamente connesso, decide il router successivo verso cui instradarlo, l'instradamento attraverso la sotto-rete che connette i due router avviene secondo i meccanismi della sotto-rete. Il processo si ripete di router in router sino alla sotto-rete di destinazione.



Forwarding di datagrammi IP

E' il processo che consente a un pacchetto di essere trasferito da un ingresso a una uscita del nodo e di nodo in nodo di essere trasportato dalla sorgente alla destinazione.

Ipotesi:

- Ogni datagramma contiene l'indirizzo IP della destinazione
- La parte di rete identifica in modo univoco la rete nell'ambito di Internet
- Host e router con lo stesso indirizzo di rete si scambiano i pacchetti su quella rete
- Ogni rete che e' parte di Internet ha almeno un router collegato ad un'altra rete

Funzionamento

L'host o il router stabilisce per confronto con il proprio indirizzo di rete se la destinazione appartiene o meno alla rete o alle reti a cui e' connesso. Se la risposta e' positiva si innesca la procedura ARP per l'individuazione dell'indirizzo fisico. Se il nodo e' connesso a una rete diversa occorre che il datagramma venga inviato a un router (next hop router). Il nhr si determina leggendo la tabella di forwarding che e' una lista di associazioni (numero di rete, next hop). C'e' comunque un default router a cui viene inviato il pacchetto nel caso l'indirizzo non venga trovato nella tabella precedente.

IP Routing/Forwarding

Dato un datagramma:

- Estrai il campo destinazione *DA* (Destination address)
- Cerca *DA* nella routing table
- Trova il prossimo "hop address": *HA*
- Spedisci il datagramma a *HA*

L'indirizzo di destinazione nell'header del datagramma si riferisce sempre all'ultima destinazione. Quando un router invia il datagramma ad un altro router, l'indirizzo del "next hop" non appare nell'header del datagramma.

Le conseguenze sono che:

- ad ogni "hop" viene "ricalcolata" la strada da seguire per tutti i pacchetti in transito
- i router devono poter sapere instradare tutti gli indirizzi => accrescimento tabelle di routing
- non c'e' distinzione tra i tipi di servizio e le loro esigenze in termini di qualità di servizio
- *connectionless*: non si possono definire percorsi end-to-end o indirizzare il traffico in determinati percorsi

Di fronte alla crescita "esponenziale" della Rete e della sua complessità, la soluzione è spesso stata di sovra-dimensionare l'infrastruttura:

- trunk ad alta capacità

- nodi ad elevato *throughput*
- router con capacità d'instradamento potenziata al massimo

Determinazione degli indirizzi fisici

Quando dobbiamo fare routing interno (instradamento diretto) occorre determinare l'indirizzo di linea corrispondente all'indirizzo IP per poter trasferire fisicamente il datagramma: ad esempio indirizzo Ethernet a 48 bit.

Ogni host costruisce una tabella di corrispondenze utilizzando il protocollo ARP (Address Resolution Protocol). La tabella si chiama ARP cache o ARP table e scade periodicamente.

ARP

Per instradare un pacchetto IP verso una destinazione appartenente alla stessa rete del mittente viene incapsulato il pacchetto IP in un pacchetto dello strato di data link sottostante (ad esempio: Ethernet); un host conosce il proprio indirizzo IP e la propria rete di appartenenza: analizzando l'indirizzo di destinazione di un pacchetto l'host puo' capire se il destinatario appartiene alla sua stessa rete, e quindi operare il delivery locale.

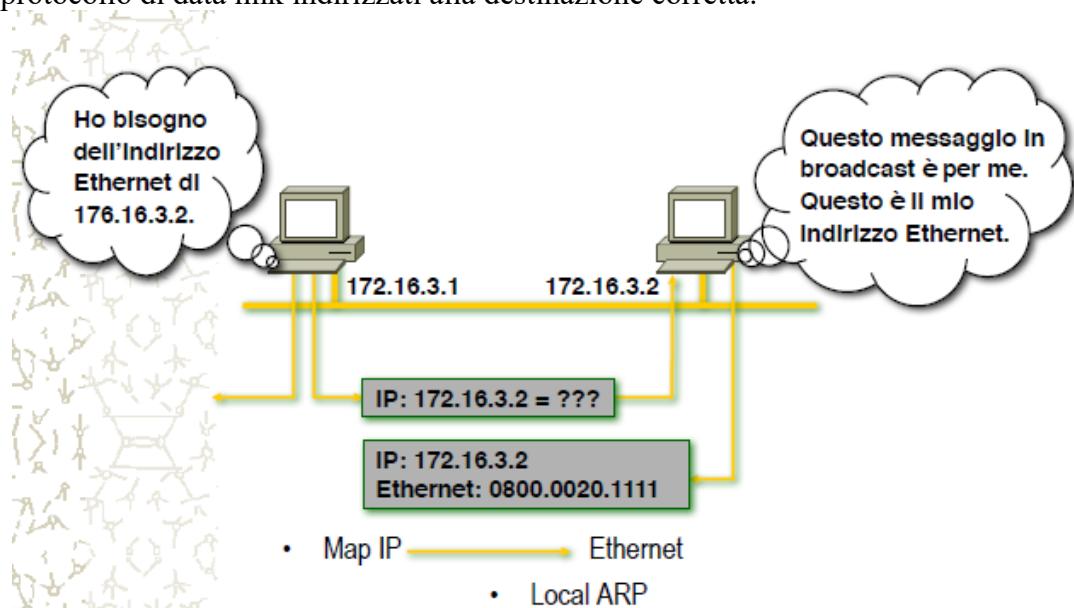
Il problema da risolvere è come fare a sapere a quale indirizzo di data link (Ethernet) inviare il pacchetto:

- l'host conosce solo l'indirizzo IP del destinatario
- serve quindi una mappa che associa un indirizzo IP della stessa rete al suo indirizzo di data link

Per risolvere questo problema IP si appoggia ad un protocollo chiamato ARP (Adderss Resolution Protocol).

Quando un host con indirizzo IP1 ed indirizzo hardware HW1 deve inviare un pacchetto IP ad un host con indirizzo IP2 sulla stessa rete, ARP si procura l'informazione necessaria in questo modo:

- viene costruito un pacchetto di data link (ARP request) contenente IP1, HW1, ed IP2, con un campo dedicato ad HW2 riempito con tutti 0
- questo pacchetto viene inviato broadcast sulla rete locale
- tutti ricevono il pacchetto ARP, ma solo l'host che ha l'indirizzo IP2 lo processa (gli altri lo scartano)
- l'host costruisce un pacchetto di data link (ARP response) contenente l'informazione mancante, e lo invia direttamente ad HW1 (non broadcast)
- ARP sul primo host acquisisce quindi l'informazione dell'indirizzo Ethernet dell'host remoto, e lo comunica ad IP, che puo' cosi' incapsulare i propri pacchetti IP in frame del protocollo di data link indirizzati alla destinazione corretta.



ARP cache

Per migliorare le prestazioni, ARP puo' gestire sull'host locale una cache in memoria. Ogni volta che viene appresa una nuova associazione IPaddress-Hwaddress, viene memorizzata nella cache. Quando ARP deve individuare un indirizzo HW, prima controlla nella cache: se l'informazione e' presente viene utilizzata senza inviare pacchetti sulla rete. Le entry nella cache di ARP hanno un tempo di scadenza, per evitare che eventi quali sostituzione di schede di rete o reindirizzamento degli host possano rendere impossibile la comunicazione, alla scadenza del tempo di validita' l'entry viene rimossa dalla cache, ed una successiva richiesta per quell'indirizzo provochera' una nuova emissione di ARP request sulla LAN. Alcuni sistemi permettono di definire nella cache di ARP delle entry manuali prive di scadenza. Talvolta necessarie, qualora l'host di destinazione non supporti correttamente il protocollo ARP; questa tecnica puo' essere utilizzata anche per motivi di efficienza e in ogni caso difficile da mantenere aggiornata la cache delle macchine: meglio evitare. Nell'ARP la richiesta è di tipo broadcast, mentre la response è unicast.

Problema dell'ARP cache:

ARP spoofing

Nell'ambito della sicurezza informatica, l'**ARP poisoning** (letteralmente *avvelenamento dell'ARP*) (detto anche **ARP spoofing**, letteralmente *falsificazione dell'ARP*) è una tecnica di *hacking* che consente ad un attacker, in una *switched lan*, di concretizzare un attacco di tipo *man in the middle* verso tutte le macchine che si trovano nello stesso segmento di rete quando queste operano a livello 3 cioè di *internetworking* con altre sottoreti scambiandosi traffico IP grazie al ricorso ad opportune manipolazioni tramite i protocolli di livello 2. L'ARP poisoning è oggi la principale tecnica di attacco alle lan commutate. Consiste nell'inviare intenzionalmente e in modo forzato risposte ARP contenenti dati inesatti o, meglio, non corrispondenti a quelli reali. In questo modo la tabella ARP (*ARP entry cache*) di un host conterrà dati alterati (da qui i termini *poisoning*, letteralmente avvelenamento e *spoofing*, raggiro).

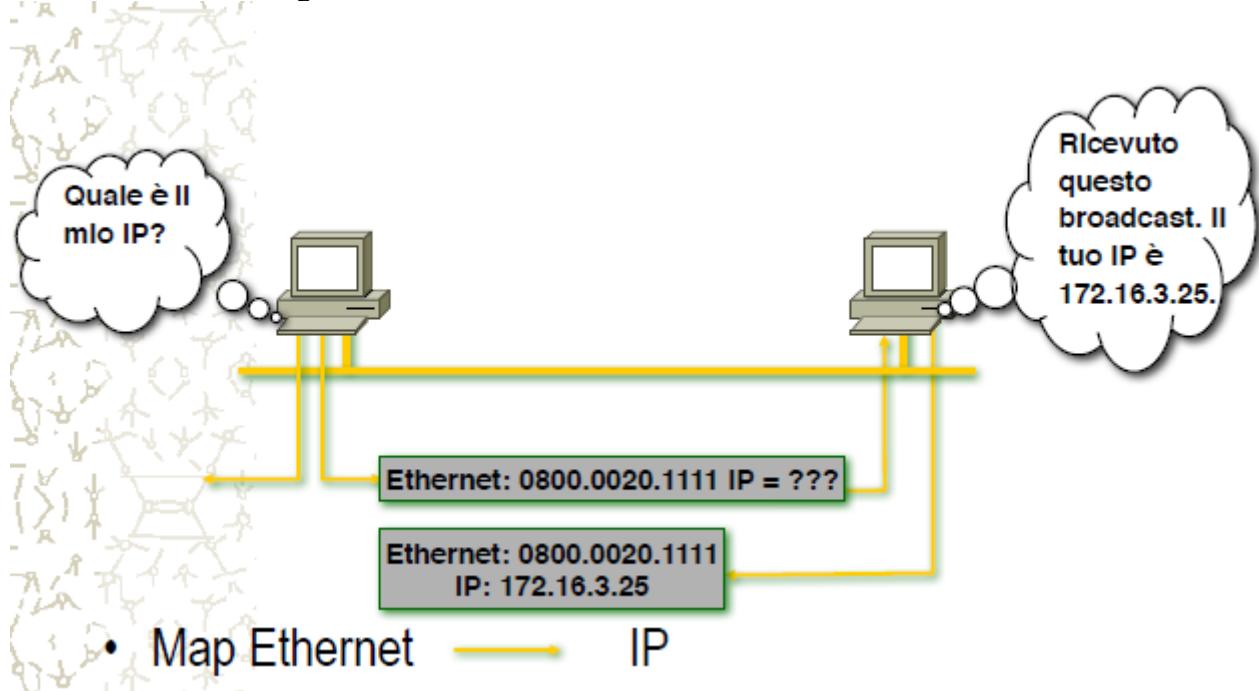
Funzionamento:

Il normale funzionamento del è il seguente: protocollo ARP si occupa di gestire l'associazione tra indirizzi IP e indirizzi MAC. Quest'associazione, in Ethernet, viene fatta prima di ogni tipo di comunicazione. Sono previsti due tipi di messaggi dal protocollo ARP: ARP request (effettuata in broadcast) e ARP reply (effettuata in unicast). Un ipotetico host 192.168.1.1 che vuole comunicare con l'host 192.168.1.2 manderà una ARP request in broadcast con il proprio MAC il proprio indirizzo IP e l'indirizzo IP di destinazione; quando 192.168.1.2 riceverà l'ARP request risponderà con un'ARP reply destinato al MAC sorgente e contenente il proprio MAC. Per ottimizzare le prestazioni e limitare il traffico queste informazioni (associazione indirizzo IP/indirizzo MAC) vengono memorizzate nella tabella ARP (ARP cache) di ciascun host così che non sia necessario effettuare continue richieste per successivi eventuali indirizzamenti verso terminali host già noti. Per migliorare ancora di più le prestazioni quando si ricevono delle ARP reply (alcuni anche con le ARP request), anche se non sollecitate, gli host aggiornano le informazioni della propria ARP cache.

Con lo spoofing vengono inviate continue richieste da un'altro indirizzo di rete in modo da far comparire nella ARP cache quest'ultimo indirizzo invece di quello originario, questo porta quindi ad un problema di intercettazione di dati.

Reverse ARP

Consente di determinare l'indirizzo IP a partire dall'indirizzo fisico. Serve quando si accende una workstation diskless. Ogni rete ha un suo RARP server.



il **Dynamic Host Configuration Protocol (DHCP)** (*protocollo di configurazione IP dinamica*) è un protocollo di rete di livello applicativo che permette ai dispositivi o terminali di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso a una rete IP (quale una LAN) la configurazione IP necessaria per stabilire una connessione e operare su una rete più ampia basata su Internet Protocol, cioè interoperare con tutte le altre sottoreti scambiandosi dati, purché anch'esse integrate allo stesso modo con il protocollo IP. Il protocollo è implementato come servizio di rete ovvero come tipologia di server .

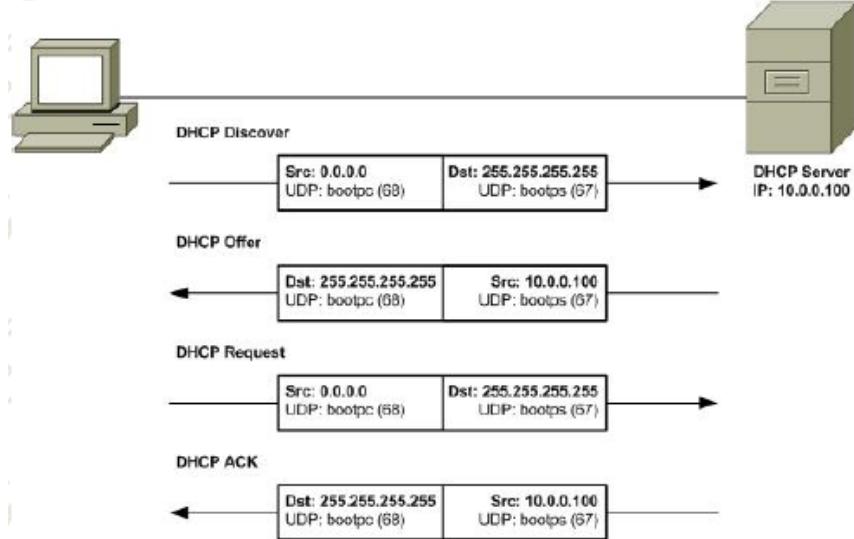
Le sue caratteristiche sono quindi :

- Standard in RFC 1531
- Permette agli host dopo lo startup di ottenere un indirizzo IP da un server
- Elimina costose configurazioni manuali
- Valida indirizzi IP sulla base di un predefinito periodo di lease

Ci sono tre tipi di allocazioni:

- **Allocazione dinamica:** Un amministratore di rete riserva un intervallo di indirizzi IP per DHCP e ogni client DHCP sulla LAN è configurato per richiedere un indirizzo IP dal server DHCP durante l'inizializzazione della rete. Il processo request-and-grant utilizza il concetto di lease con un periodo di tempo controllabile, consentendo al server DHCP di recuperare e quindi riallocare gli indirizzi IP non rinnovati.
- **Allocazione automatica:** il server DHCP assegna automaticamente un indirizzo IP a un client richiedente nell'intervallo definito dall'amministratore. Questo è come nell'allocazione dinamica, ma il server DHCP mantiene una tabella delle assegnazioni degli indirizzi IP passati, in modo che possa assegnare preferenzialmente a un client lo stesso indirizzo IP precedente.
- **Allocazione manuale(comunemente chiamata assegnazione statica):** il server DHCP emette un indirizzo IP privato dipendente dal MAC address di ciascun client, basato su una mappatura predefinita da parte dell'amministratore. Questa funzione è denominata in vari modi come assegnazione DHCP statica tramite DD-WRT, indirizzo fisso dalla documentazione dhcpcd, prenotazione indirizzo da Natgear, prenotazione DHCP o DHCP statico da parte di Cisco e Linksys e prenotazione indirizzo IP o binding indirizzo MAC/IP da altri router produttori. Se non viene rilevata alcuna corrispondenza per MAC address del client, il server può facoltativamente ricorrere all'assegnazione dinamica o

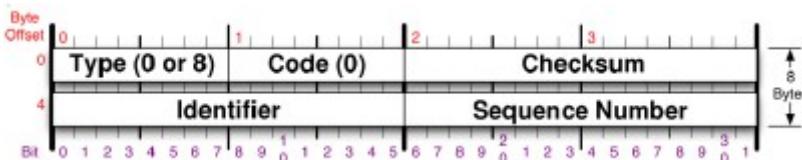
automatica. DHCP viene utilizzato per Internet Protocol versione 4 (IPv4), nonché per l'IPv6. Sebbene entrambe le versioni abbiano lo stesso scopo, i dettagli del protocollo per IPv4 e IPv6 differiscono sufficientemente da poter essere considerati protocolli separati.[1] Per l'operazione IPv6, i dispositivi possono utilizzare in alternativa l'autoconfigurazione dell'indirizzo stateless. Gli host IPv6 possono anche utilizzare l'indirizzamento locale del collegamento per ottenere operazioni limitate al collegamento di rete locale.



ICMP

Internet Control Message Protocol e' il protocollo utilizzato per monitorare il funzionamento del livello di rete. Esistono una dozzina di messaggi ICMP destinati ad avvisare i router o gli host di qualche evento specifico della rete. ICMP non ha lo scopo di rendere IP affidabile, ma di notificare allo strato di rete problemi non transienti nella comunicazione a livello 3 in modo da attivare quelle reazioni dinamiche al malfunzionamento della rete necessarie, ad esempio, a ridisegnare dinamicamente la topologia utilizzata per l'instradamento. ICMP utilizza IP come protocollo di trasporto per instradare i propri messaggi in questo senso c'e' una sorta di miscuglio degli strati in IP:

- ICMP e' una parte del protocollo di rete, in quanto ha funzioni di (auto)controllo dello strato di rete e non fornisce servizi agli strati superiori
- tuttavia ICMP utilizza IP come sottoprotocollo per trasmettere le sue informazioni tra gli host/router interessati

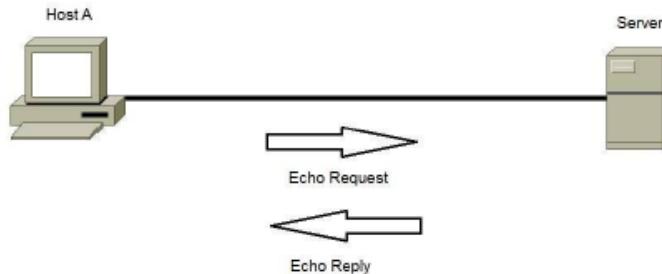


I principali messaggi ICMP disponibili sono:

- **destinazione irraggiungibile**: questo messaggio e' inviato dai router agli host sorgenti di un pacchetto IP per notificare che la destinazione non e' raggiungibile
- **time exceeded**: viene notificato alla sorgente di un pacchetto che il pacchetto ha raggiunto la scadenza del time-to-live
- **problema di parametri**: un router annuncia al router che gli ha inviato un pacchetto che i parametri dell'header sono inconsistenti
- **source quench**: utilizzato (in passato) per rallentare la sorgente che trasmette troppo velocemente in caso di congestione; l'evoluzione del TCP/IP ha spostato pero' il controllo della congestione sul livello di trasporto
- **redirect (reindirizzamento)**: il router avvisa l'host sorgente che ha inviato il pacchetto iniziale secondo un instradamento errato (ad esempio: se ci sono due router sulla LAN, ed

un pacchetto viene inviato da un host verso il router sbagliato).

- **echo ed echo reply:** utilizzati per verificare la raggiungibilità di un host:
 1. quando un host riceve un ICMP ECHO da una sorgente, deve immediatamente rispondere con un ICMP ECHO REPLY.
 2. molte utility fanno uso di questo messaggio ICMP (ad esempio ping)
- **timestamp e timestamp response:** analoghi ai messaggi ECHO/ECHO REPLY, inseriscono nei pacchetti informazioni di tempo per valutare il ritardo della connessione.

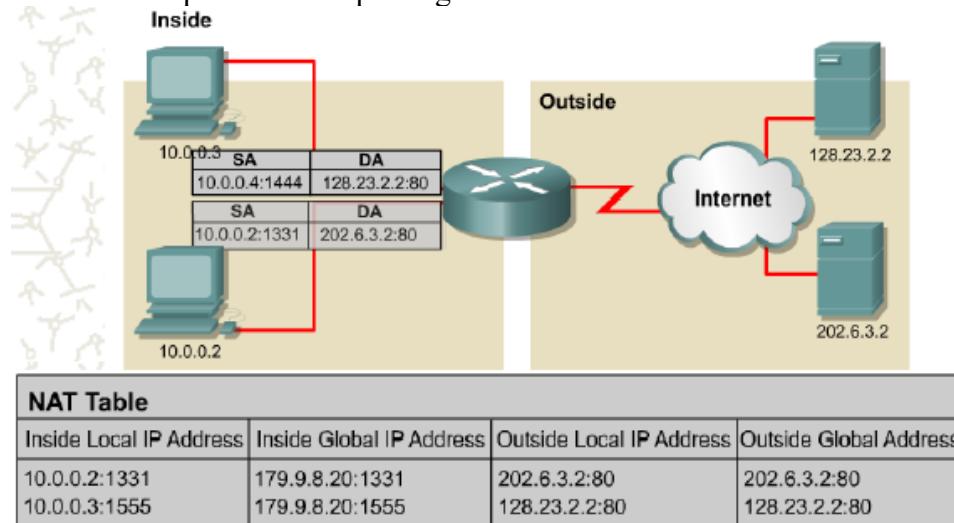


NAT

Il router traduce indirizzi interni in esterni, mappando indirizzi e porte nella NAT Table.

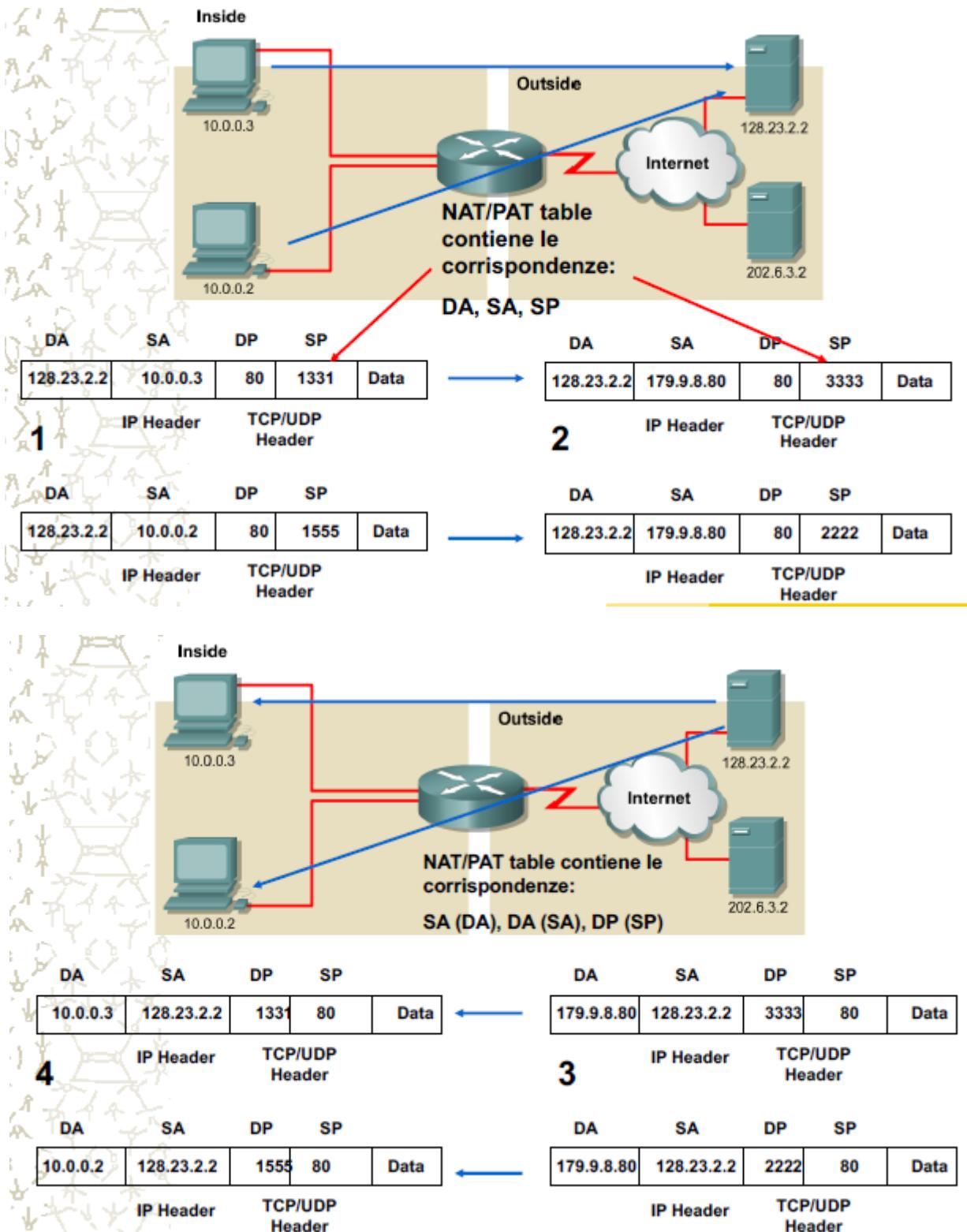
- **Inside local** – L'indirizzo IP assegnato all'host sulla rete interna.
- **Inside global** – Un indirizzo IP pubblico assegnato dal service provider che rappresenterà uno o più IP locali verso il mondo esterno.
- **Outside local** – L'indirizzo IP assegnato a un host sulla rete esterna come visto dagli hosts sulla rete interna
- **Outside global** – L'indirizzo IP assegnato a un host sulla rete esterna.

NOTA: Inside: indirizzi assegnati entrambi all'interno della rete, Outside: indirizzo sostituito che vedo in corrispondenza di quello globale.



Il NAT permette l'autoassegnamento di indirizzi di rete in modo autonomo, una volta che le macchine saranno collegate quest'ultimo maschererà questi indirizzi in uno nuovo (INSIDE), ma questo porta ad un problema nella rete globale cioè non possiamo vedere più l'indirizzo a cui facevamo riferimento internamente, per superare a questa mancanza c'è la logica OUTSIDE che fa la stessa cosa del NAT INSIDE ma in direzione opposta.

Esempio: Mi assegno indirizzi di rete 9, e inserisco un NAT, da quel momento in poi non sarò più in grado di vedere e comunicare con reti di indirizzo 8 su scala globale. Questo problema è risolto con L'outside NAT, che farà un remapping, cioè mi farà vedere l'indirizzo 8 della rete globale con un nuovo indirizzo cosicché possa riuscire a comunicare con quest'ultimo.

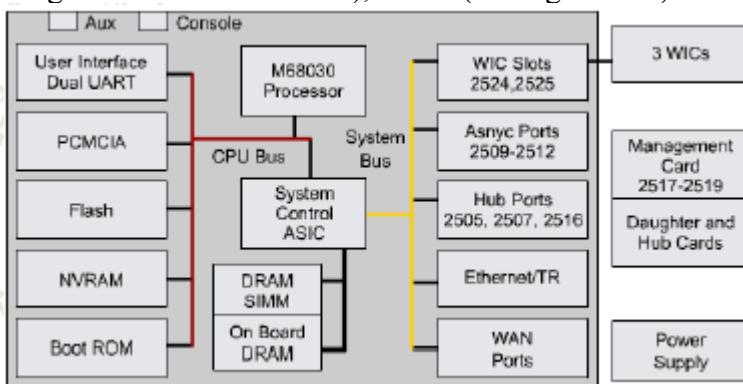


NETWORKING – INSTRADAMENTO

Router IP: Un router può interconnettere reti che usano diverse tecnologie, inclusi mezzi fisici diversi, tecniche di accesso, schemi di indirizzamento fisico e formato dei frames.

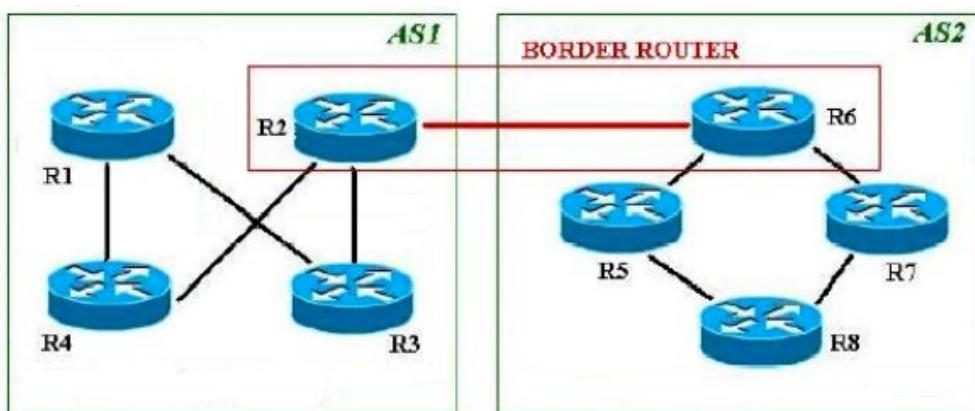
Il router, tipicamente realizzato in architettura special purpose, è configurato o attraverso una porta di console o via telnet e va inizializzato caricando un sistema operativo (**IOS**) nella sua memoria.

- Porte di Ingresso / Uscita (interfacce Ethernet, SONET, etc..)
- Blocco di commutazione, che collega le porte di ingresso con quelle di uscita
- Processore di instradamento: esegue protocolli di routing, aggiorna tabelle di routing
- Memorie: **ROM** (codice per Bootstrap [avvio] e POST [*Power-On Self Test* = diagnostica e manutenzione hardware]), **RAM** (tabelle di routing), **NVRAM** (configurazioni di avvio e il registro modalità di avvio), **Flash** (immagine IOS).



Collegamenti fra routers

Il collegamento di più reti sotto un unico dominio amministrativo prende il nome di **Autonomous System** (AS). I router che instradano messaggi all'interno dello stesso AS e non hanno diretta connessione con altre reti (network) esterne, sono chiamati **Interior Router** e scambiano informazioni di instradamento tramite un **IGP** (Interior Gateway Protocol). I router, che instradano i messaggi tra AS diversi sono detti **Exterior Router**, scambiano informazioni di instradamento utilizzano un protocollo **EGP** (Exterior Gateway Protocol). I router che fungono da “ponte di collegamento” tra AS diversi cioè sono il punto di ingresso e di uscita verso altri AS vengono detti **Border Router** o router di frontiera.



NOTA: Autonomous System: Un'autorità amministrativa si contraddistingue sia in base a elementi informatici (specifiche policy di routing), sia per motivi amministrativi. Esempio di sistema autonomo può essere quello che contraddistingue gli utenti di un unico provider oppure, più in piccolo, quello che costituisce la rete interna di un'azienda. All'interno di un sistema autonomo i singoli router comunicano tra loro, per scambiarsi informazioni relative alla creazione delle tabelle di routing o tabelle di instradamento, attraverso un protocollo IGP (*interior gateway protocol*). L'interscambio di informazioni tra router appartenenti a sistemi autonomi differenti avviene attraverso un protocollo BGP (*Border Gateway Protocol*) e punti di interscambio fisici tra i diversi sistemi (NAP). Ogni AS che utilizza la rete pubblica deve essere registrato presso il rispettivo RIR:

AfriNIC, APNIC, ARIN, LACNIC o RIPE. Ciascun AS è inoltre identificato da un numero univoco a 16 bit o 32 bit. In pratica, ad ogni AS viene assegnato un numero di indirizzi IP pubblici, che possono essere distribuiti.

Tabelle di routing

Per potere instradare in modo corretto i vari pacchetti che girano nella rete un router ha bisogno di avere alcune informazioni fondamentali:

- Indirizzo IP dell'HOST di destinazione
- L'indirizzo dei router ad esso adiacenti, da cui poter ricavare le informazioni delle varie reti e sottoreti remote raggiungibili
- I possibili percorsi (alternativi) per raggiungere queste reti remote
- Il miglior percorso verso ciascuna delle reti remote non direttamente connesse ad esso

Una tabella di instradamento (**Routing Table**) raccoglie le informazioni necessarie per individuare il percorso ottimale verso tutte le possibili reti.

TABELLA DI ROUTING

INDIRIZZO IP DI DESTINAZIONE	E' il campo più importante contenuto nella Routing Table, quando un router riceve un pacchetto dati attraverso la sua porta di IN, controlla nella propria tabella di routing se esiste una entry per tale destinazione, ed in caso affermativo inoltra il flusso dati nella corrispondente porta di OUT.
METRICA	Definisce l'algoritmo di instradamento (Hop Count, Load, Delay, Bandwidth, ecc.)
INDIRIZZO DEL ROUTER DI NEXT HOP	E' l'indirizzo del router successivo per raggiungere la rete di destinazione
INTERFACE	Interfaccia del router attraverso cui deve essere instradato il pacchetto verso il next hop
TIMER	Scandisce temporalmente ogni quanto tempo inviare gli updates ad i router vicini

Per la rete illustrata le tabelle per R2 ed R4 sono:

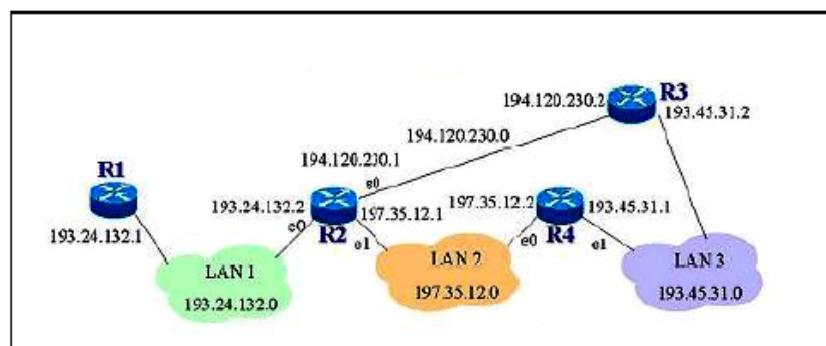


TABELLA DI ROUTING DEL ROUTER R2

NETWORK	INTERFACE	NEXT HOP	METRIC
192.24.132.0	Ethernet 0		0
197.35.12.0	Ethernet 1		0
195.45.31.0	Ethernet 1	197.35.12.2	1
195.45.31.0	Serial 0	194.120.230.2	1

TABELLA DI ROUTING DEL ROUTER R4

NETWORK	INTERFACE	NEXT HOP	METRIC
197.35.12.0	Ethernet 0		0
195.45.31.0	Ethernet 1		0
193.24.132.0	Ethernet 0	197.35.12.1	1

Metrica a 0 vuol dire che raggiungere la destinazione mi costa niente perché sono direttamente collegato ad essa.

Router di default (default gateway)

Router verso cui è inviato il traffico diretto ad una destinazione non presente nella tabella di routing
Non obbligatorio ma molto utilizzato:

- negli host, che possono anche non avere una tabella di routing propria e che inviano al router di default tutti i datagrammi non diretti alla rete cui sono collegati
- nei router, che pur avendo tabella di discrete dimensioni non coprono tutte le possibili destinazioni

Il default gateway è presente all'ultima riga della tabella di instradamento ed è rappresentato con tutti zero sia nel campo Prefisso di Destinazione che nel campo Subnet Mask.

Prefisso di Destinazione	Subnet Mask	Next hop	Interfaccia
20.0.0.0	255.0.0.0	d.c. (20.0.0.6)	eth0
130.11.0.0	255.255.0.0	d.c. (130.11.0.6)	eth1
0.0.0.0	0.0.0.0	20.0.0.5	eth0

Longest Prefix Matching

Per valutare se un host con indirizzo X appartiene ad una sottorete con indirizzo Y/M si effettua l'operazione di matching, cioè si verifica che: **X and M = Y and M**

Quando all'interno di un router si effettua l'operazione di instradamento il matching va effettuato per tutte le righe della tabella di routing: se il matching dà esito positivo per più righe si attua la regola del **Longest Prefix Matching**, si utilizza la riga che ha il maggior numero di bit in comune con X and M.

Instrandamento

- indirizzo 198.15.7.3
- indirizzo 198.15.4.4

➤ 198.15.7.3 -> porta 7

➤ 198.15.4.4 -> porta 1

Tabella di instradamento

Prefix	Porta d'uscita
198.15.0.0/16	1
198.15.7.0/24	7

Operazioni di instradamento:

Instrandamento effettuato dal router X:

estrae l'indirizzo IP di destinazione dal datagramma (Y)

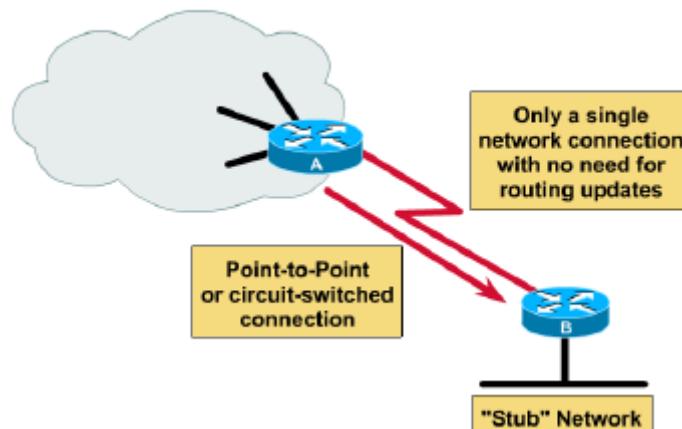
1. se l'indirizzo di destinazione Y coincide con X (la destinazione è il router X), estraie il contenuto informativo e lo consegna al protocollo indicato
2. decrementa il Time To Live del datagramma; se il Time To Live è arrivato a zero scarta il datagramma e ne da comunicazione all'host mittente
3. confronta la componente X and M con Y and M (M maschera di rete del router X), se sono uguali inoltra il datagramma direttamente (@ARP)
4. Per tutte le righe della tabella di instradamento [N,M,NH,I] confronta se Y and M = N and M (N indirizzo della sotto-rete, M maschera di sotto-rete, NH ind. prossimo router ed I interfaccia d'uscita). Inoltra il datagramma verso il router NH relativo alla corrispondenza con la maschera più lunga (Longest Prefix Match)
5. altrimenti (non c'è nessuna corrispondenza) inoltra verso il default router se ne è stato specificato uno oppure scarta il datagramma e dichiara errore di instradamento

Strategie di instradamento

Nel configurare le politiche di instradamento su una rete abbiamo essenzialmente due opzioni:

- **Routing Statico:** Prevede il calcolo dei percorsi offline quando la rete non è ancora attiva e la loro configurazione manuale, a carico dell'operatore.

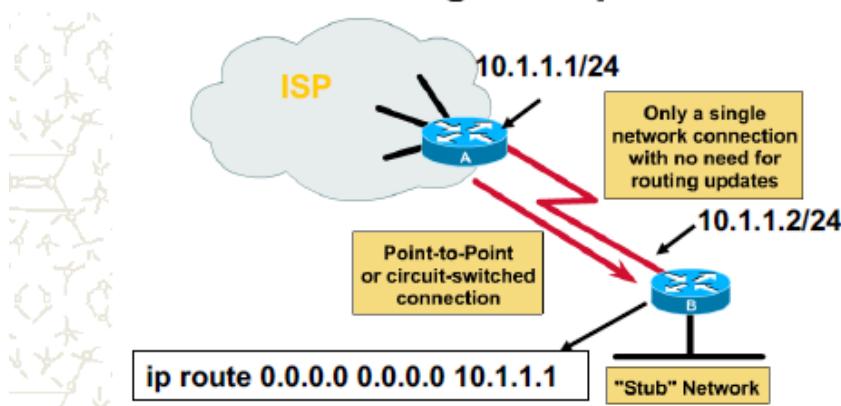
Static Routing Example



Il routing statico e' virtualmente ingestibile in condizioni di reti anche banalmente complesse, ma viene utilizzato in circostanze particolari:

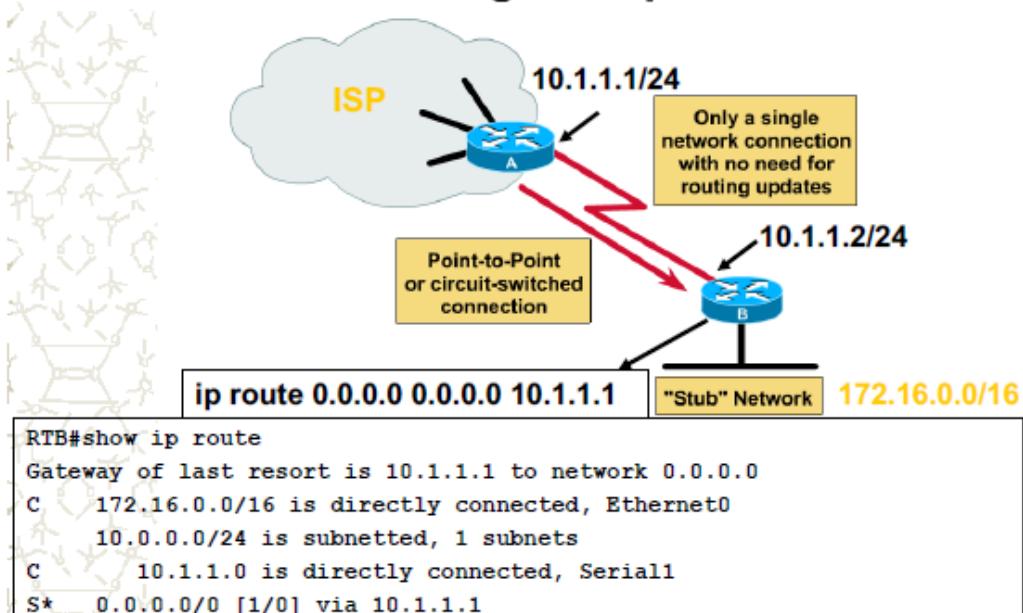
- un router ha una unica connessione
- un router ha piu' di una connessione, ma per tutte le connessioni tranne una c'e' una destinazione ben precisa che non puo' cambiare per motivi di topologia, e l'ultima connessione deve essere utilizzata per tutte le altre destinazioni.

Default Static Routing Example



La route di default specifica l'instradamento di tutti i pacchetti per i quali la tabella di instradamento non fornisce una route esplicita. Si specificano rete e mask con "0.0.0.0 0.0.0.0" oppure "0.0.0.0/0". La rete 0.0.0.0/0 risulta sempre ultima nel matching (longest prefix match) ma corrisponde sempre.

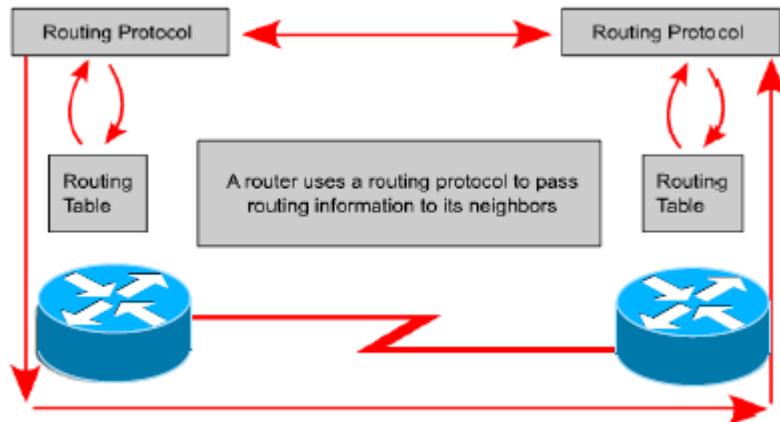
Default Static Routing Example



- **Routing Dinamico:** I percorsi cambiano dinamicamente in base alle situazioni di traffico ed ad altre informazioni locali come congestione, guasti, ecc.

Routing dinamico - Protocolli di routing

Sono protocolli utilizzati dai routers per costruire le tabelle che contengono le informazioni di instradamento dei pacchetti. Per costruire la tabella, ciascun router dovrà scambiare pacchetti informativi con i routers ad esso collegati. Per far questo si scambiano una serie di annunci relativi alle informazioni su come costruire la routing table.



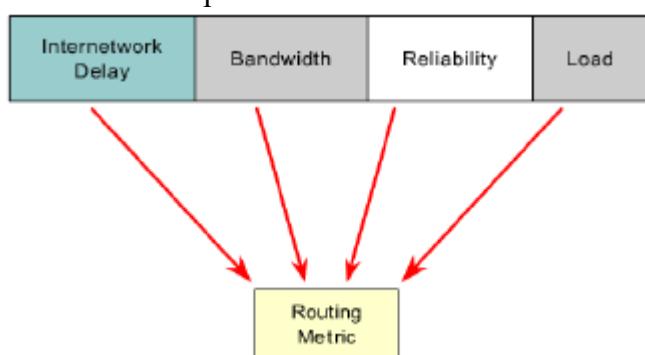
La scelta del percorso migliore avviene attraverso l'uso delle **metriche**. Interviene nella caratterizzazione di un percorso per l'instradamento di pacchetti tra due nodi. La Metrica serve per selezionare il percorso "migliore"

- Percorso più corto
- Percorso meno congestionato
- Percorso più ampio
- Percorso meno costoso
- ...

Metriche dinamiche: Come aggiornare le decisioni in presenza di variazioni

- Guasti
- Modifiche ai parametri
- Variazioni nel carico dei link

Esistono diversi protocolli con metriche diverse:



- **RIP(Routing Information Protocol) – Hop Count**
- **IGRP('Interior Gateway Routing Protocol) and EIGRP(Enhanced Interior Gateway Routing Protocol)** – **Bandwidth, Delay, Reliability, Load:** sono protocolli proprietari di CISCO, la loro metrica è molto complessa.
- **OSPF – Bandwidth:** è molto usato e si basa sulla banda
- **IS-IS – Cost**
- **BGP – Number of AS or policy**

Insieme alla metrica c'è anche un'altro elemento molto importante, la **distanza amministrativa** che quantifica l'attendibilità dell'informazione d' instradamento:

- Più il valore è basso, più l'informazione è "sicura"
- Se il router riceve da fonti diverse route alternative verso la stessa rete, userà la distanza amministrativa per decidere quale rendere attiva.
- Ci indica anche quanto è affidabile il protocollo usato dalla metrica.

Route Source	Administrative Distance	Default Metric(s)
Connected	0	0
Static	1	0
EIGRP Summary Route	5	0
External BGP	20	Bandwidth, Delay
Internal EIGRP	90	Link cost (bandwidth)
IGRP	100	Link cost (bandwidth)
OSPF	110	Hop count
IS-IS	115	Value assigned by admin
RIP	120	
External EIGRP	170	
Internal BGP	200	

CLASSIFICAZIONE ALGORITMI DI ROUTING

Gli algoritmi di routing si classificano secondo due gruppi:

Non adattivi: Utilizzano criteri fissi di instradamento, sono statici e deterministici. Appartengono al gruppo il Fixed Directory Routing ed il Flooding.

Adattivi: Calcolano ed aggiornano le tabelle di instradamento in funzione della topologia della rete e dello stato dei link, sono dinamici e non deterministici. Il Routing Centralizzato, il Routing Isolato ed il Routing Distribuito appartengono a questo gruppo.

Algoritmi di routing non adattivi

- **Fixed Directory Routing:** L'algoritmo prevede che ogni nodo abbia una tabella di instradamento che metta in corrispondenza il nodo da raggiungere con la linea da usare. Queste entry sono puramente statiche, poiché è il gestore che si occupa di determinarle e di configurare il router. Il gestore ha così il completo controllo sul traffico ed è necessario un suo intervento in caso di guasto.
- **Basati su Flooding:** Ciascun pacchetto che arriva ad un router viene instradato su tutte le porte(interfaccie), eccetto quella da cui è arrivata. Questo metodo, concepito per reti militari, massimizza la probabilità che i dati arrivino a destinazione, ma produce un altro volume di traffico sulla rete. È molto utile sulle reti ad hoc, il suo uso però è di pagare un overhead molto alto per via del continuo replicare dell'informazione.

Algoritmi di routing adattivi

- **Routing Centralizzato:** Un RCC, Routing Control Center, conosce la topologia di tutta la rete, calcola e distribuisce le tabelle di instradamento di ogni router. La gestione permette tabelle calcolate con algoritmi sofisticati, ma necessita un gestore a livello mondiale. La sua dimensione del grafo è infatti troppo grande e a lungo andare ingestibile. Soffre anche del problema del singol point of failure, infatti se viene attaccato il routing control center l'intera rete cade.
- **Routing Isolato:** Ogni router calcola le proprie tabelle di instradamento in modo indipendente.
- **Routing Distribuito:** È fusione dei due metodi precedenti, realizza le funzionalità RCC in

ogni singolo nodo della rete. Le tabelle vengono aggiornate dai routers scambiandosi informazioni di servizio mediante apposito protocollo. Gli algoritmi sono il *Distance Vector* ed il *Link State*. Il vantaggio è che quando si arriva ad una convergenza tutti i router vedranno l'intero grafo di rete e prenderanno tutta la stessa decisione, che sarà anche la migliore.

ROUTING E GRAFO DI RETE

Il concetto è quello di costruire un grafo della rete, dove ogni nodo del grafo rappresenta un router ed ogni arco del grafo rappresenta una linea di comunicazione (chiamata anche canale). Per scegliere un percorso tra due router, l'algoritmo cerca nel grafo il cammino più breve tra di essi. Metriche possibili:

- distanza geografica
- costi
- capacità

Il grafo che si viene a creare è chiamato anche **database topologico**; per scegliere il percorso ottimale la soluzione è trovare il percorso più breve, in base ad una certa metrica

Possono essere scelte differenti metriche:

- distanza geografica
- numero di salti
- costo delle linee
- ritardo di accodamento
- distanza chilometrica
- larghezza di banda
- o una funzione di alcune di queste

Definita una metrica, le linee potranno essere etichettate con un numero (peso o metrica): più basso è il numero, "più breve" è la linea (quindi preferibile). La distanza di un percorso è dato dalla somma delle distanze dei singoli salti. Dijkstra ha ideato un algoritmo (Shorted Path First) che determina, in base alla topologia ed ai pesi, il cammino più breve tra due nodi del grafo.

NOTA:

Algoritmo: metodo o procedura che si utilizza per arrivare alla soluzione di un problema.

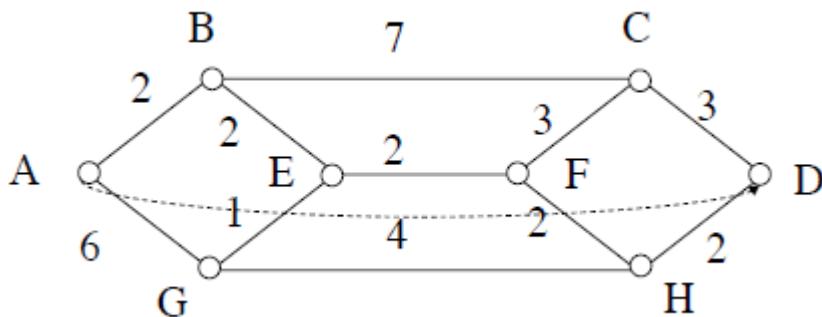
Protocollo: si basa su di un algoritmo, ma è di fatto uno standard che si usa per riuscire a comunicare in modo ottimale con tutte le macchine.

Algoritmo di Dijkstra

L'algoritmo di Dijkstra (1959) lavora su grafi orientati, che hanno pesi non negativi sui collegamenti. Questo algoritmo trova i percorsi più brevi tra un nodo di partenza e tutti gli altri.

- È utilizzato per calcolare il percorso a costo minimo
- Obiettivo: trovare il percorso più breve tra le coppie di nodi

Esempio:



Procedimento

I nodi vengono messi in due insiemi: esaminati e non esaminati. Ad ogni nodo i , devono essere associate due etichette, $\text{COSTO}[i]$ che indica il peso totale del cammino (la somma dei pesi sugli archi percorsi per arrivare al nodo i -esimo) e $\text{PRED}[i]$ che indica il nodo che precede i nel cammino minimo. Le etichette possono essere provvisorie o permanenti.

Il nodo sorgente è il primo nodo attivo

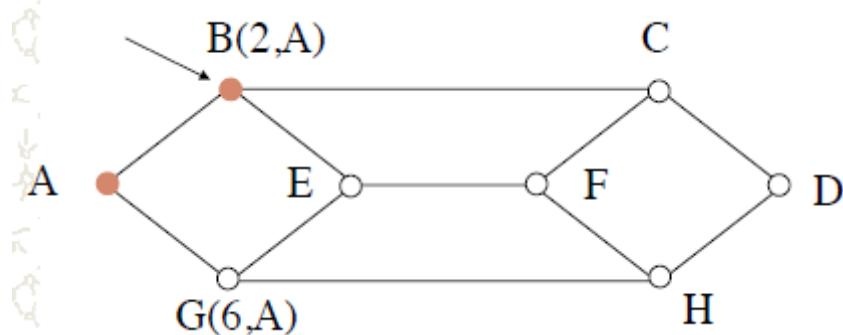
Si esaminano tutti i nodi i connessi al nodo attivo j e per ciascuno di essi si pone:

- $\text{PRED}[i] = j$
- $\text{COSTO}[i] = \text{COSTO}[j] + \text{LINK}[j,i]$

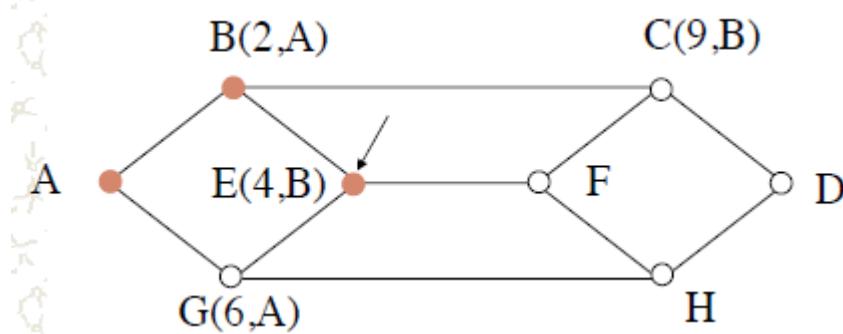
Il nuovo nodo attivo è quello con il costo più basso tra quelli esaminati e viene marcato come permanente. L'etichetta di un nodo permanente non viene più cambiata.

ES: Ricerca del percorso A-D

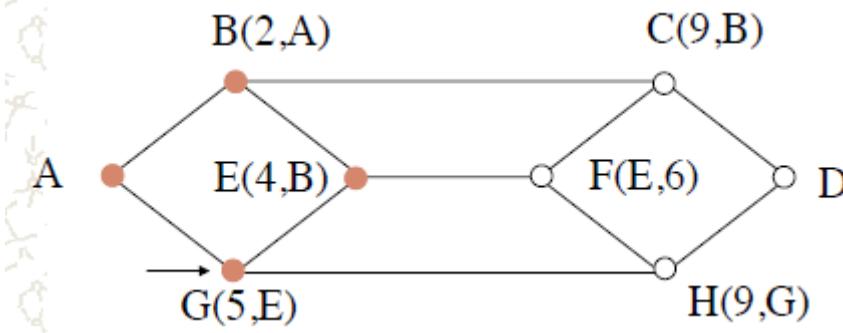
- Esamino ogni nodo adiacente ad A etichettandolo con la sua distanza da A
- Da A trovo il nodo adiacente più vicino e lo marco con costo e provenienza
- La provenienza permetterà di ricostruire il cammino finale



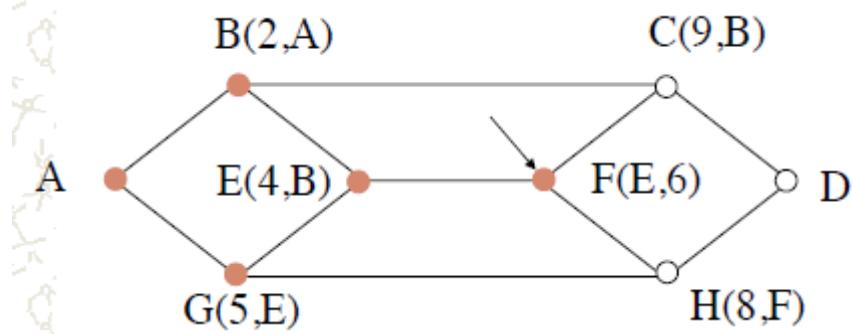
Da B si procede nello stesso modo esaminando i vicini E e C, se un nuovo nodo raggiungibile da B ha costo da A inferiore al costo del percorso che passa per B diventa il nuovo nodo attivo (appartiene al percorso minimo corrente).



Da E: si trova un percorso a costo inferiore che passa per G (rispetto a quello che passa per F) e quindi G diventa il nuovo nodo attivo. Partendo da G il prossimo nodo sarebbe solo H a distanza 9.

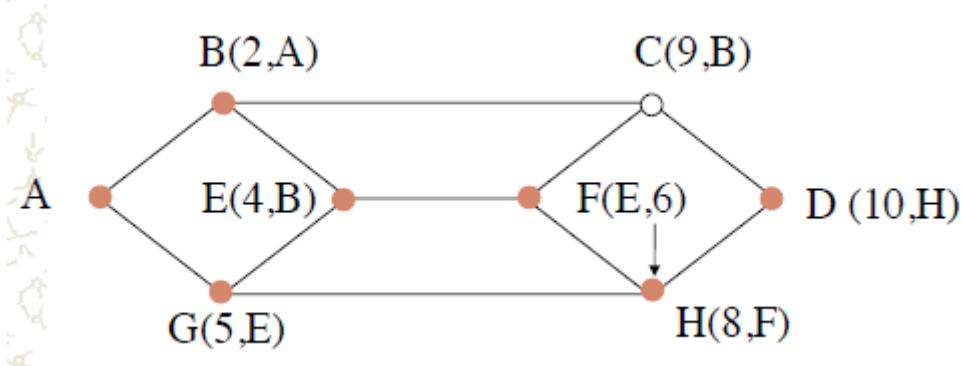


Viceversa, ripartendo da F, H risulta la scelta a costo inferiore (distanza 8).



Il percorso si costruisce individuando per ciascun nodo del percorso minimo il predecessore.

Risulta : A-B-E-F-H-D



Perche' funziona?

Supponiamo di aver trovato ABE come percorso minimo

Se esistesse un altro percorso AXE a costo più basso ci sarebbero 2 possibilità

Z è un nodo permanente, e è già stato esaminato e AXE è già stato individuato

Z è un nodo provvisorio

- O la sua label è > di quella di E e quindi non rappresenta il percorso minimo
- O la sua label è < di quella di E e quindi Z sarebbe il nodo attivo

Le precedenti considerazioni portano a concludere che la procedura individua il percorso a costo minimo. La complessità è $O(|V|^2)$.

L'unico problema è dovuto al fatto che per usarlo si deve conoscere l'intero grafo di rete.

Distance vector(Bellman-Ford)

Algoritmo adattivo sviluppato attorno al 1960, utilizzato per molto tempo. Arpanet lo ha utilizzato fino al 1979 nella implementazione chiamata RIP (ancora in uso adesso in realtà di piccole dimensioni). L'idea è quella di partire dal nodo sorgente e cominciare a guardare i nodi adiacenti assegnando loro il valore del costo per raggiungerli (determinato dal costo dell'arco + il valore del nodo da cui si è partiti). Si itera il ragionamento per ciascuno dei nodi raggiunti. Se il grafo ha $|V|$ nodi dopo $|V|-1$ iterazioni tutti i nodi avranno assegnato il costo minimo per essere raggiunti dal nodo sorgente. Nella sua struttura base è molto simile a quello di Dijkstra, ma invece di selezionare il nodo di peso minimo, tra quelli non ancora processati, con tecnica greedy, semplicemente processa tutti gli archi e lo fa $|V|-1$ volte. Ha una complessità temporale $O(|V| |E|)$, $|E|$ numero di archi del grafo.

Ad ogni linea e' assegnata una distanza, valutata in base ad una metrica, indicata anche col nome di costo. Le informazioni di routing vengono scambiate con tutti i router adiacenti. Ogni nodo acquisisce una visibilità della rete indiretta, mutuata dai vicini. In base alle informazioni ricevute dai vicini viene ricostruita la tabella di routing nuova. Il valore della distanza avrà un certo limite massimo, indicante che la destinazione non e' raggiungibile:

- nel caso di metrica ad hop, la distanza di infinito sarà pari al numero massimo di hop

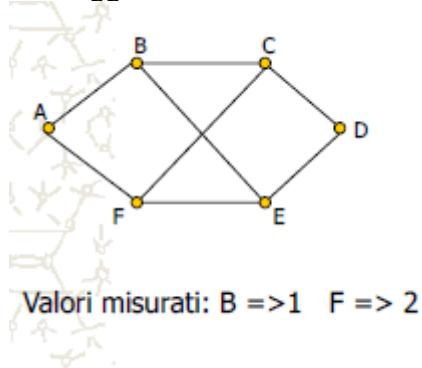
- possibili nella rete piu' uno
- in caso di metrica secondo i ritardi puo' essere piu' complesso determinare l'irraggiungibilita' della destinazione: si deve valutare a priori un valore ragionevolmente elevato ma non troppo

Valutazione delle distanze:

- il router deve conoscere i router adiacenti, ed il costo delle linee che li connettono direttamente, per fare questo un router scambia a tempi definiti con i propri vicini dei pacchetti per essere aggiornati sulla loro presenza, se la metrica scelta dipende dal ritardo della linea, questi pacchetti sono utilizzati per aggiornare la valutazione del costo della linea diretta verso il router adiacente
- Quando viene ricevuta la tabella di routing dai vicini, per ogni destinazione si valuta la distanza aggiungendo alla distanza riportata dal router adiacente quella relativa alla linea che li connette
- Tra tutte le distanze relative alla stessa destinazione riportate dai router adiacenti, e rivalutate in base alla distanza verso ciascun router adiacente, si sceglie quella con distanza inferiore

Algoritmi di routing distance vector

In dettaglio, questo tipo di algoritmi funziona mantenendo una tabella contenente la più piccola distanza conosciuta per ogni destinazione e quale canale utilizzare per raggiungerla. Queste tabelle sono aggiornate scambiando informazioni con i propri vicini.



B	A	2
	B	0
	C	4
	D	8
	E	3
	F	9

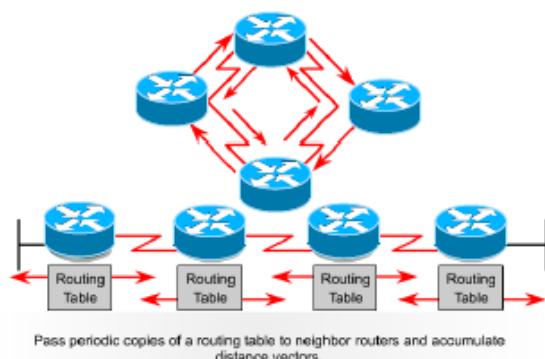
F	A	3
	B	9
	C	4
	D	6
	E	2
	F	0

A	A	0	-
	B	1	B
	C	5	B
	D	8	F
	E	4	B
	F	2	F

Ogni router mantiene in memoria, oltre alla propria tabella di instradamento, una struttura dati per ogni linea chiamata Distance Vector. Il Distance Vector associato a ciascuna linea, contiene informazioni ricavate dalla tabella di instradamento del router collegato all'altro estremo della linea. Il calcolo delle tabelle di instradamento dipende da tutti i distance vector associati alle linee attive del router. Quando un router calcola una nuova tabella, la invia ai routers adiacenti (cioè quelli collegati da un cammino fisico diretto) sotto forma di distance vector.

Ciascun router riceve la tabella di instradamento dai suoi vicini direttamente connessi. Ogni entry è composta da quattro parametri, indirizzo, hops, costo e linea, e la tabella contiene entry relative ad ogni nodo presente in rete. Il Distance Vector da inviare al router adiacente è composto dalle prime tre colonne.

Indirizzo	Hops	Costo	Linea
1	3	25	3
2	5	35	2
3	9	50	6
4	1	5	7
5	0	0	0



Il router che lo riceve verifica eventuali modifiche dal precedente e affermativamente aggiorna campi, hops e costo della propria tabella, fondendo (merge) tutti i Distance Vector pervenuti da ogni linea attiva. La fusione avviene selezionando tra le entry di uguale indirizzo quella a minor costo. A parità di costo è scelta quella con minor numero di hops. Il Distance Vector è un algoritmo di facile implementazione, ma è sconsigliato per reti di vaste dimensioni (mille nodi) perché lento a convergere (dipende dalla velocità del router più lento della rete). Reagisce bene ai miglioramenti del costo ma molto lentamente ai peggioramenti. Converge alla velocità degli elementi più lenti.

Flooding

Ogni pacchetto in arrivo viene inoltrato su ogni linea in uscita eccetto quella da cui è arrivato. Per prevenire la duplicazione eccessiva dei pacchetti:

- Questi vengono dotati di un contatore. Quando questo contatore raggiunge lo 0, il pacchetto viene eliminato.
- I router tengono traccia dei messaggi ricevuti e ritrasmessi, e non duplicano messaggi già replicati.
- Nel flooding selettivo invece, i pacchetti in arrivo vengono replicati ma solo sulle linee che approssimativamente vanno nella direzione richiesta dalla sorgente.

Gli algoritmi di flooding vengono utilizzati come benchmark, perché scelgono sempre il cammino più breve, in quanto lo ricercano in parallelo.

Algoritmo

Gli aspetti negativi di questo algoritmo sono essenzialmente legati alla inefficienza:

- ogni pacchetto va a finire su tutte le linee della rete, provocando un utilizzo inefficiente della rete stessa
- ogni pacchetto va a finire su tutti i router, aumentando il carico di lavoro dei router stessi (CPU, occupazione di buffer)

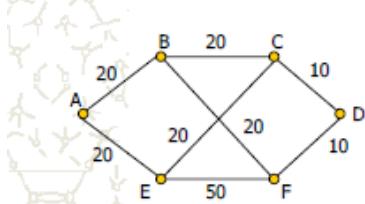
Aspetti positivi sono:

- qualsiasi pacchetto arriverà nel tempo più breve possibile (segue tutte le strade, anche la più veloce)
- estremamente resistente a modifiche della topologia: anche il malfunzionamento di grandi porzioni della rete permette il recapito del pacchetto se almeno un cammino rimane operativo, non richiede una conoscenza a priori della topologia della rete

Scarsamente utilizzato per via della inefficienza, le caratteristiche di estrema affidabilità di questo protocollo sono sfruttate in diverse circostanze particolari, ad esempio in campo militare.

Routing basato sul flusso

Considerano il **carico attuale** della rete oltre alla topologia



Devono essere noti:

- Topologia della rete
- La matrice di traffico
- La matrice delle capacità dei canali

Un'applicazione della Formula di Little ci dice il ritardo medio dei pacchetti:

$$\text{Ritardo} = \frac{1}{\text{Pacchetti/s} - \text{Traffico}}$$

	A	B	C	D	E	F
A	9 AB	4 ABC	1 ABFD	7 AE	4 AEF	
B	9 BA	8 BC	3 BFD	2 BFE	4 BF	
C	4 CBA	8 CB		3 CD	3 CE	2 CEF
D	1 DFBA	3 DFB	3 DC		3 DCE	4 DF
E	7 EA	2 EFB	3 EC	3 ECD		5 EF
F	4 FEA	4 FB	2 FEC	4 FD	5 FE	

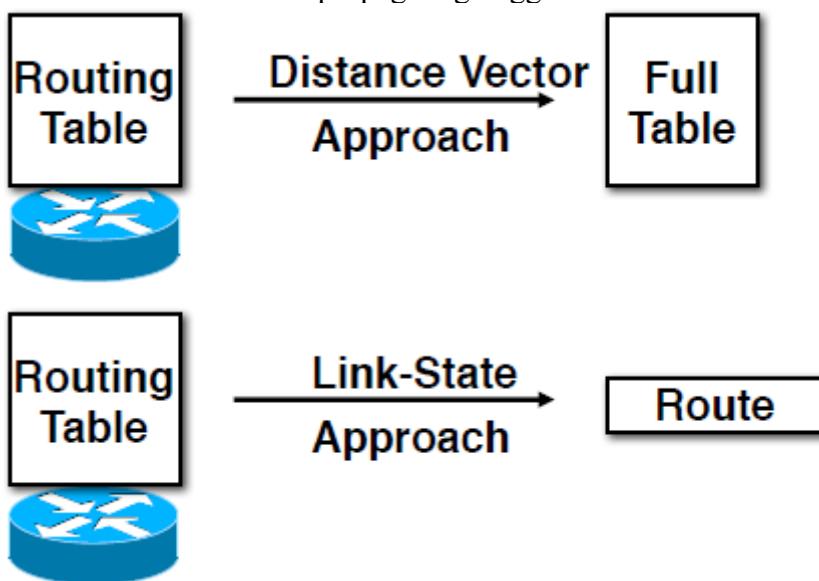
i	Linea	Traffico (p/s)	Capacità (kbps)	Pacchetti/s	Ritardo (ms)	Peso
1	AB	14	20	25	91	0.17
2	BC	12	20	25	77	0.14
3	CD	6	10	12.5	154	0.07
4	AE	11	20	25	71	0.13
5	EF	13	50	62.5	20	0.15
6	FD	8	10	12.5	222	0.09
7	BF	10	20	25	67	0.12
8	EC	8	20	25	59	0.09

Dimensione media del pacchetto 800 bit e Traffico totale 82 pacchetti/s

Aggiornamenti nei diversi protocolli

- **Distance Vector:** RIP, IGRP
- **Link State:** OSPF, IS-IS

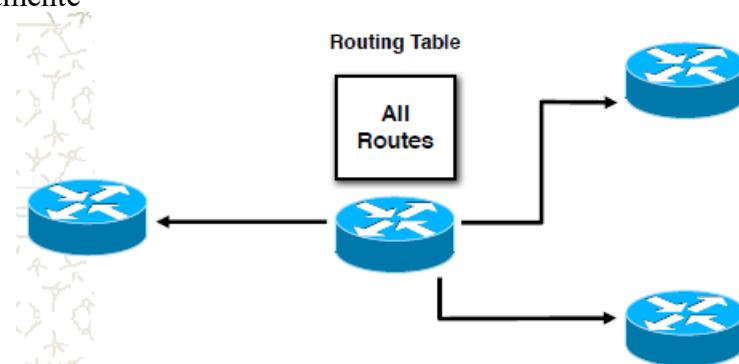
Hanno modi differenti di propagare gli aggiornamenti della routing table.



Aggiornamento in distance vector

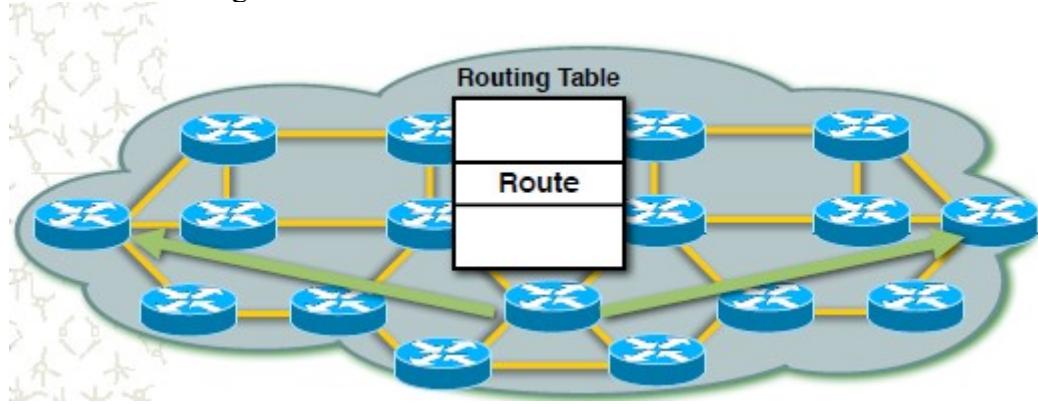
In una logica distance vector gli aggiornamenti presenti nell'intera routing table sono inviati solo ai vicini direttamente connessi. Gli aggiornamenti avvengono:

- Al cambiare della topologia
- Periodicamente



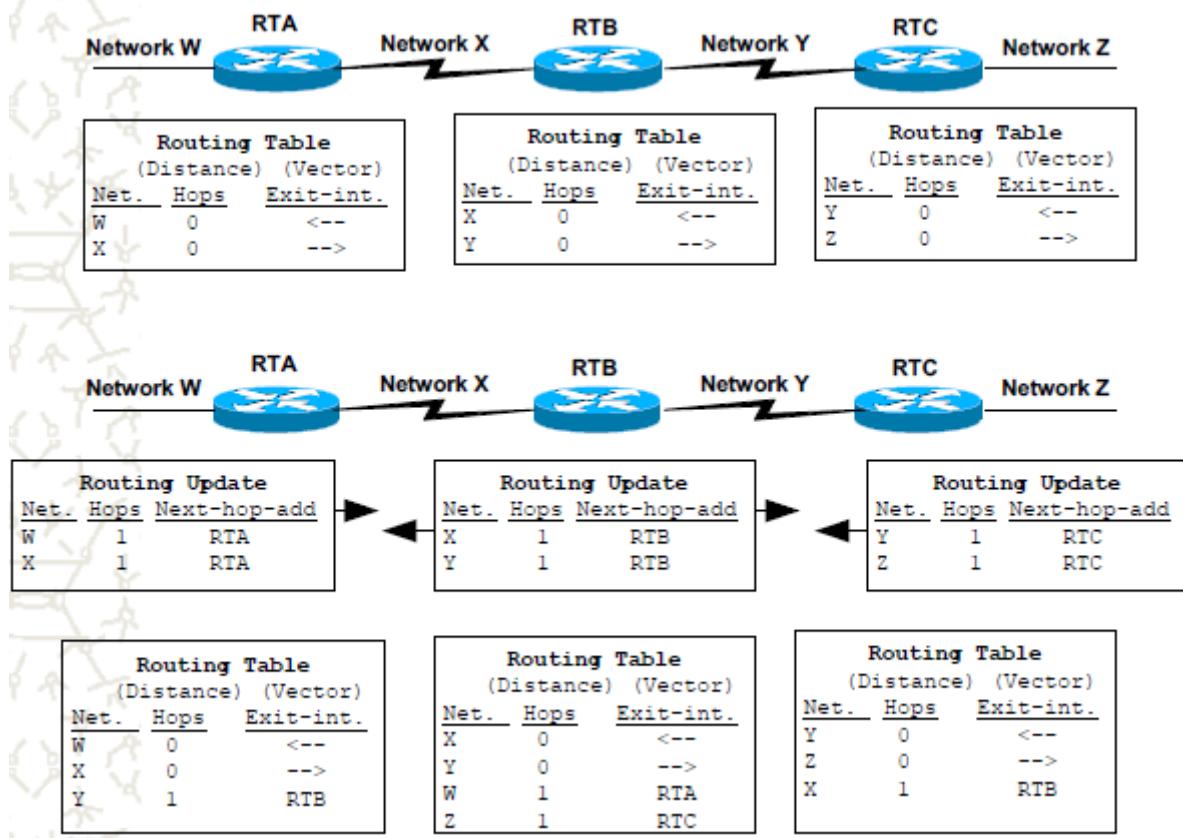
aggiornamento in link state

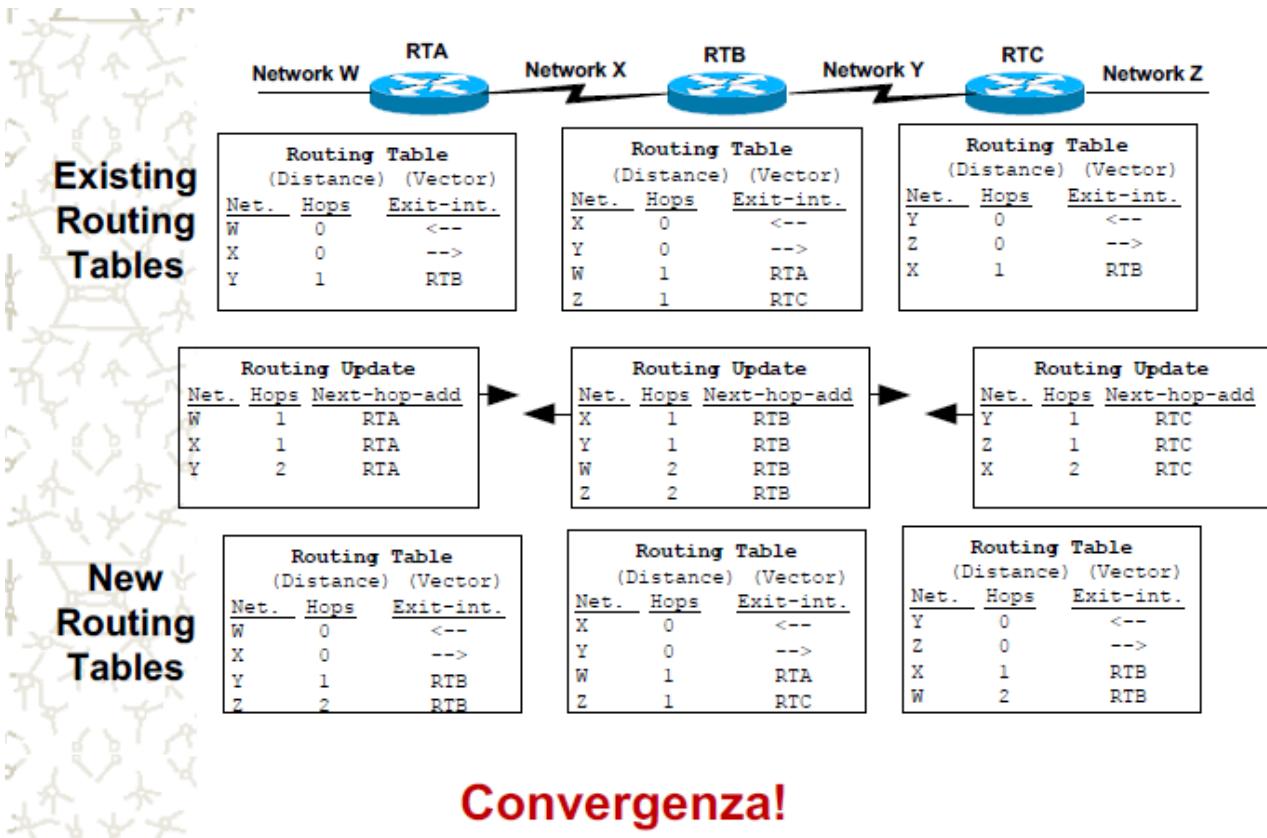
In una logica link state gli aggiornamenti sono propagati uno ad uno a tutti I nodi nel dominio di routing attraverso il flooding. Tecniche di design gerarchico possono limitare la dimensione del bacino di diffusione degli annunci.



NOTA: Nel distance vector l'aggiornamento della routing table avviene ogni t tempo tra i router vicini, e lo stesso avviene quando quei router devono farlo agli altri. Nel link state invece senza aspettare del tempo la routing table viene inviata instantaneamente.

Distance vector network discovery example



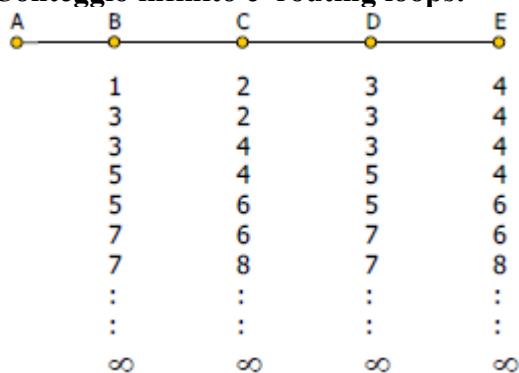


Problemi:

Inserimento di un nodo: Supponiamo che la metrica sia il numero di tratte. Ogni riga indica la distanza dopo l'i-esimo scambio di informazioni tra i nodi adiacenti a partire dalla attivazione del nodo A:

A	B	C	D	E	
1	inf	inf	inf		Dopo 4 scambi tutti i nodi sono già aggiornati.
1	2	inf	inf		
1	2	3	inf		
1	2	3	4		

Conteggio infinito e routing loops:



Non tiene conto delle capacità delle linee, converge dopo molto tempo.

Visto che la convergenza si può raggiungere dopo molto tempo, un esempio è quando il nodo si scollega dalla rete.

Supponiamo che A si disconetta dalla rete:

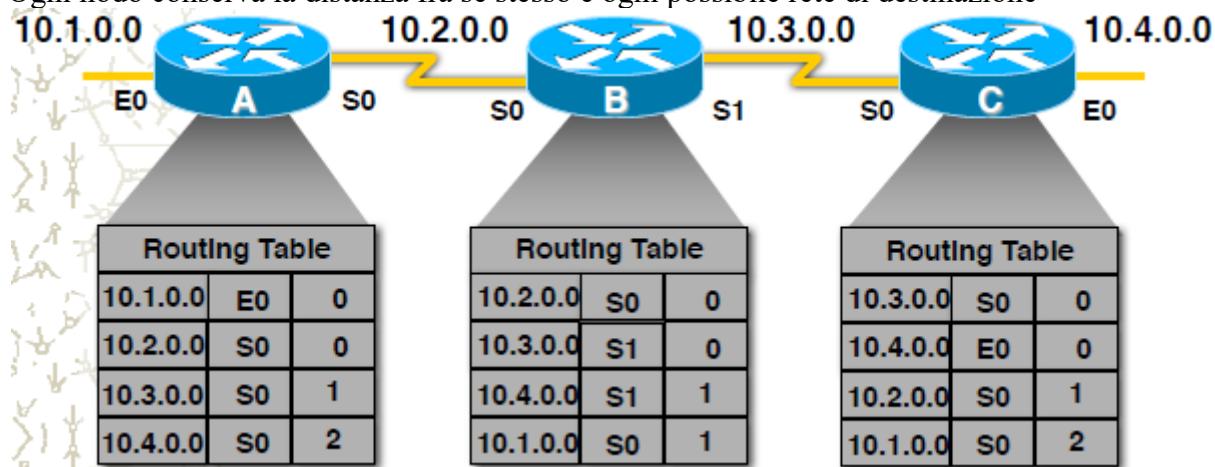
A	B	C	D	E
1	2	3	4	
3	2	3	4	
3	4	3	4	
5	4	5	4	
5	6	5	6	
7	6	7	6	
inf	inf	inf	inf	

B riconosce che A non risponde e che il suo vicino è a distanza 2 da A: pone erroneamente a 3 la sua distanza da A:

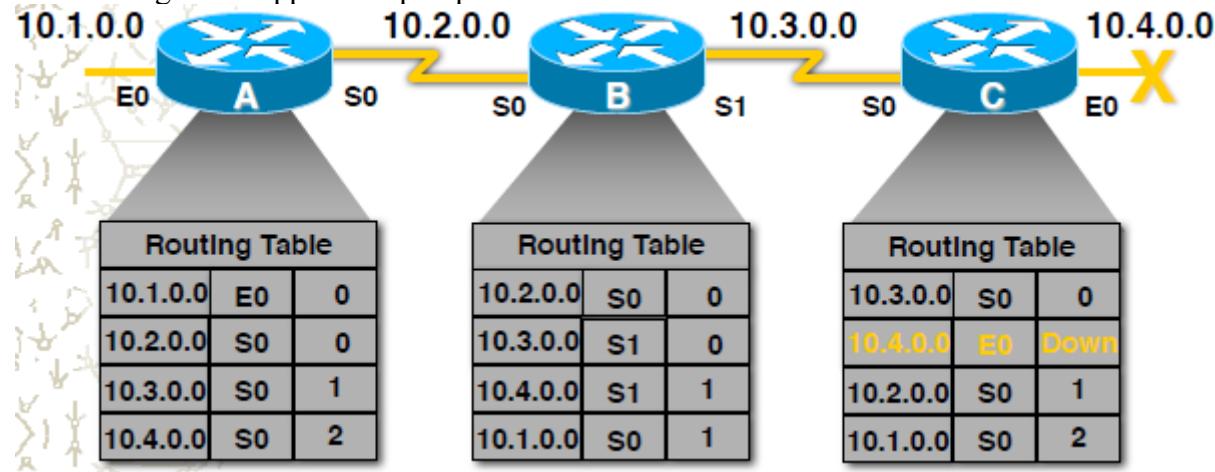
- L'informazione errata si propaga agli altri nodi
- I costi vanno all'infinito

Routing loops esempio:

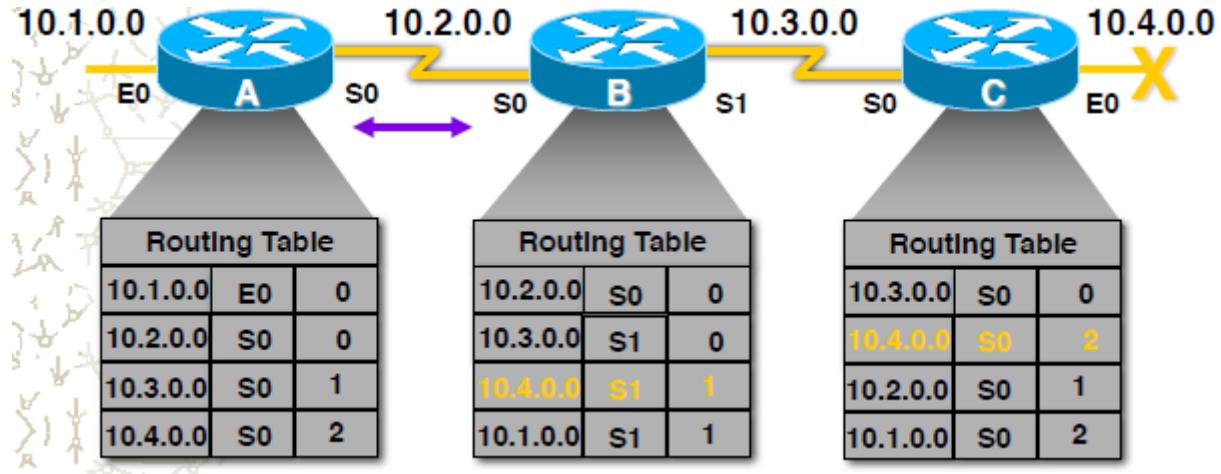
Ogni nodo conserva la distanza fra se stesso e ogni possibile rete di destinazione



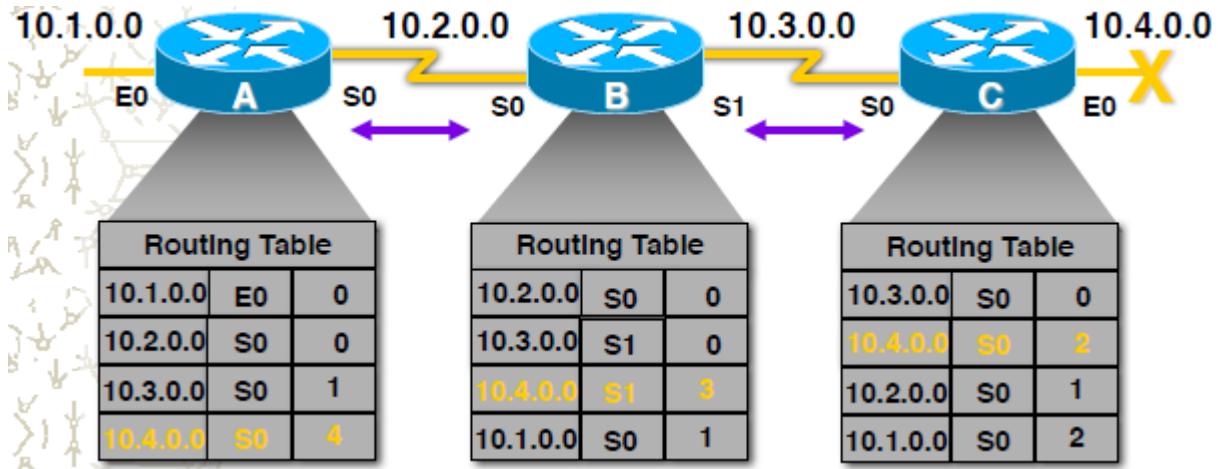
Una convergenza troppo lenta può portare a informazioni inconsistenti



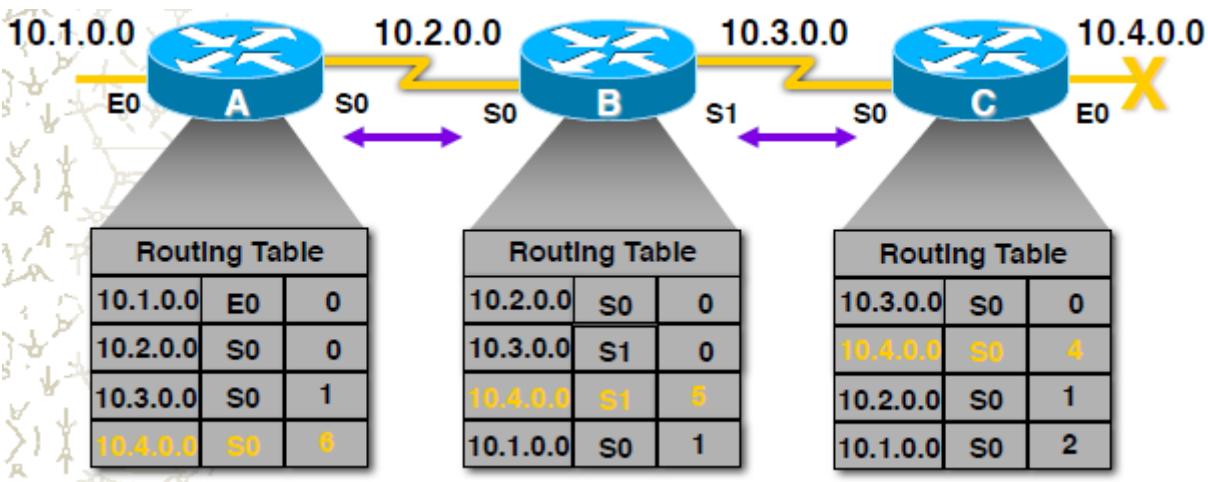
Il Router C conclude che il miglior percorso verso la network 10.4.0.0 è attraverso il Router B



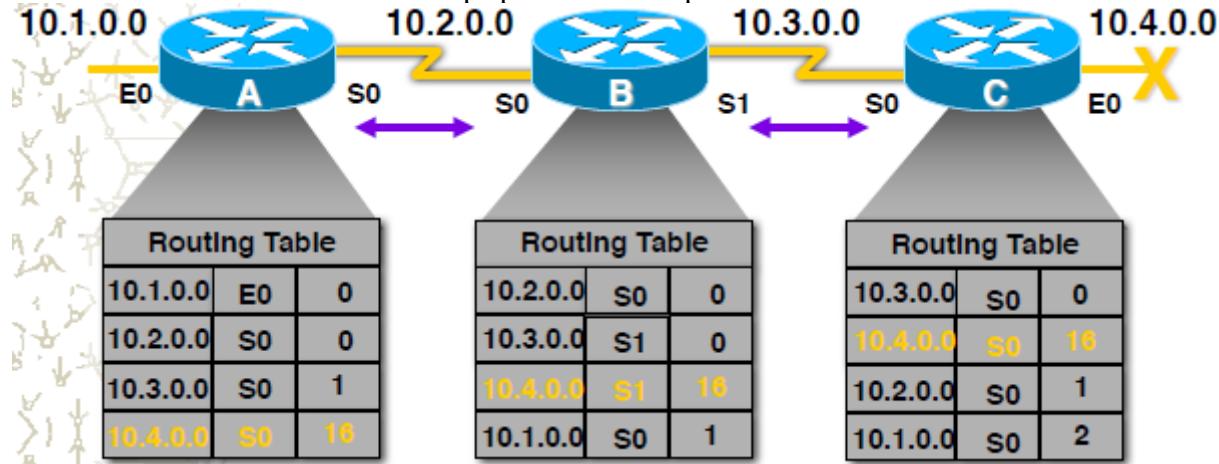
Il Router A aggiorna erroneamente la sua routing table riflettendo il nuovo hop count che è errato



I pacchetti per la network 10.4.0.0 rimbalzano fra i routers A, B, and C. L'hop count per la network 10.4.0.0 tende a infinito



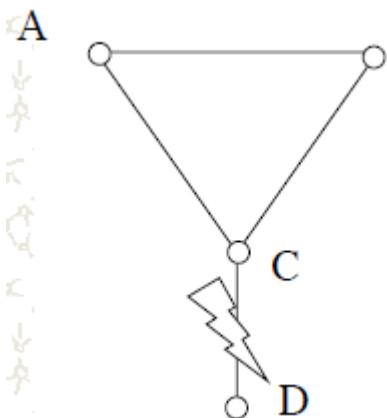
Va definito un limite sul numero di hops per evitare loops



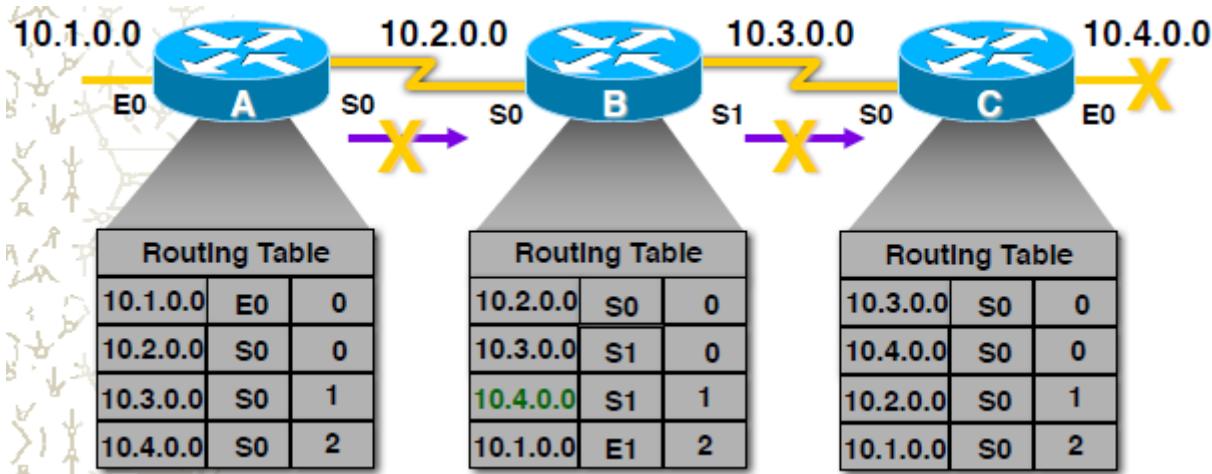
In questo esempio alla fine la rete è scomparsa, se ne accorgeranno soltanto quando la metrica arriverà a 255. Quindi il tempo che impiegherà sarà $t * 255$, quindi se un aggiornamento ci mette $t=60$ secondi, il tempo per accorgersi dell'errore è di 15 300 s. Per risolvere questo problema si mettono dei limiti alla metrica, di norma 16; in caso che si raggiunga il limite si riceverà subito la notifica della caduta di quella rete.

Una soluzione è lo **split horizon**, non si inviano le informazioni di costo verso la destinazione X sul link al quale vengono inviati i pacchetti per la destinazione X.

Nell'esempio precedente: C dice a D quanto dista da A ma dice a B che dista infinito da A. Ma in certi casi non serve:



B Se C-D va fuori servizio si innesca nuovamente il conto all'infinito; A infatti sa di avere un percorso alternativo verso B e la stessa cosa per B.

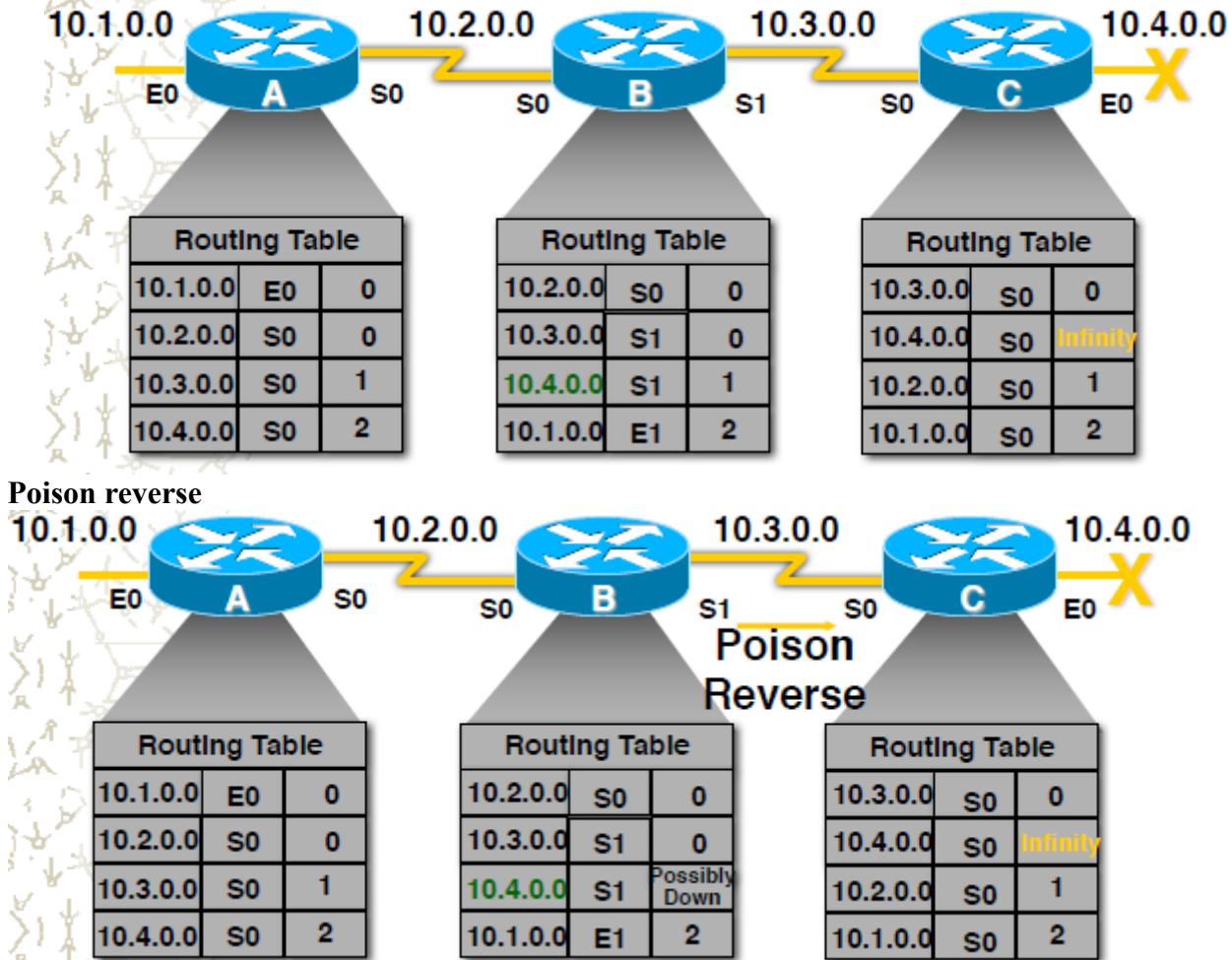


Non è mai utile inviare informazione circa lo stato di una route sulla stessa interfaccia da cui le stesse sono state acquisite.

Route poisoning

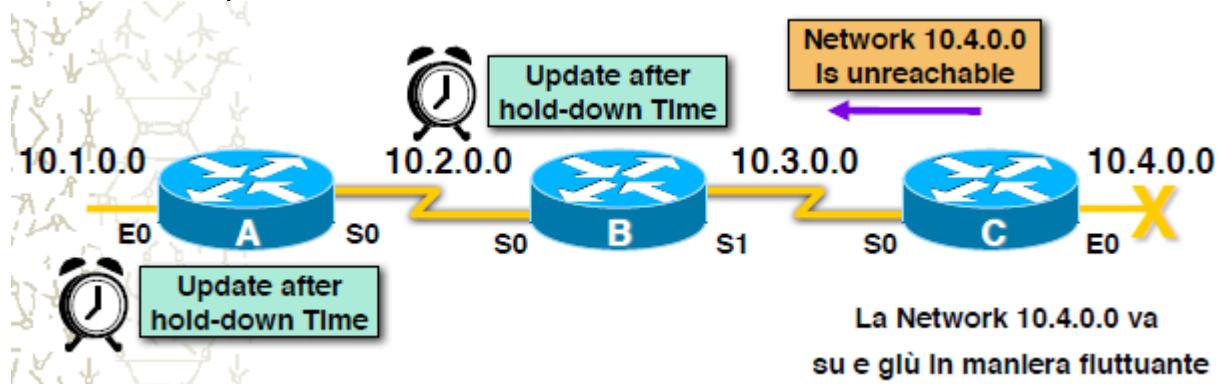
Nel momento che una rete cade, invece di dire che la rete è down, informa i vicini che la rete è andata fuori servizio mettendo la metrica ad infinito. I vicini non si limitano a riceverlo e basta, una volta che vedono che la metrica è infinita, mettono quella rete in possibility down (poison reverse).

Questa è l'unica regola che viola lo split horizon.



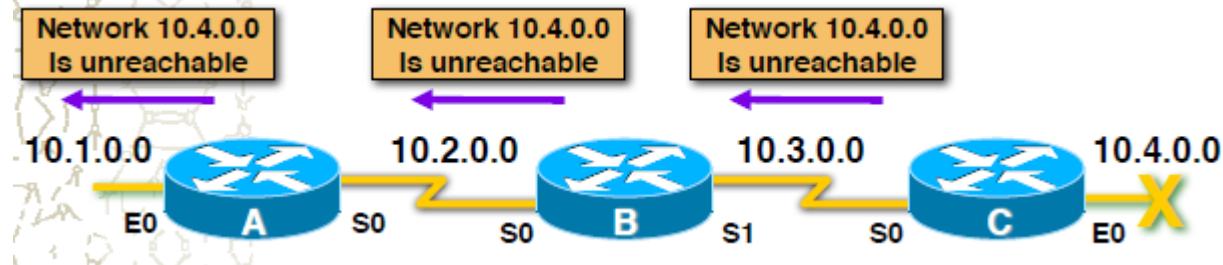
Hold-down timers

Mettendo un timer in cui aspettare che la rete torni in servizio (e quindi si ha avuto una fluttuazione), o se non torna su vuol dire che c'è stato un guasto vero e le routing table saranno aggiornate. Per evitare fluttuazioni alla ricezione di un annuncio il router setta un timer di hold-down e accetta la modifica solo alla spirazione dello stesso.



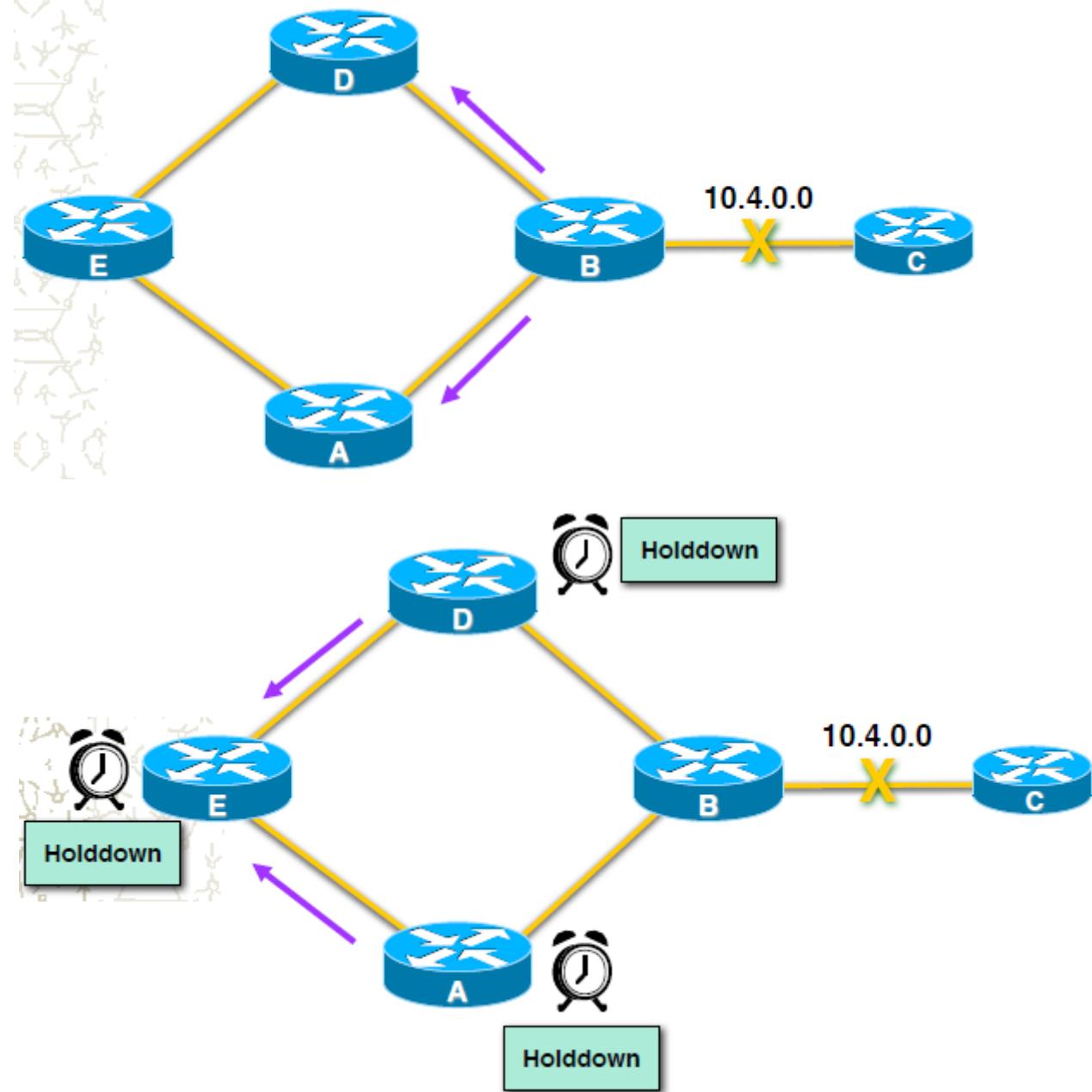
Triggered updates

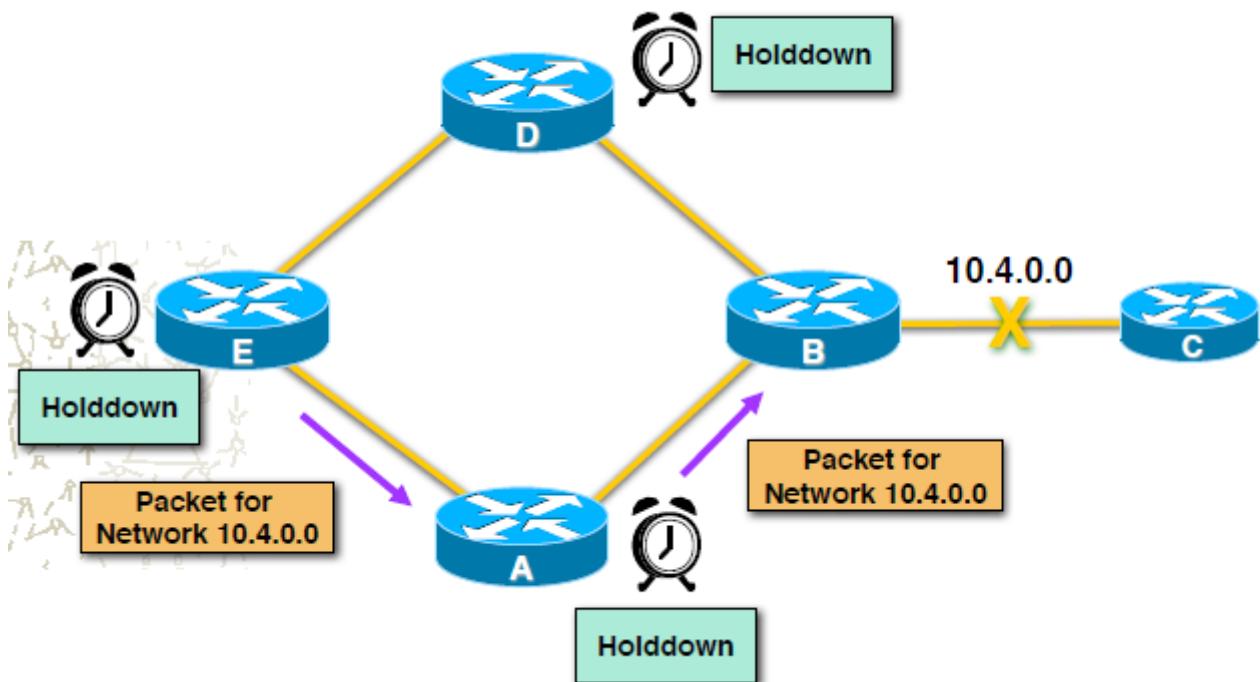
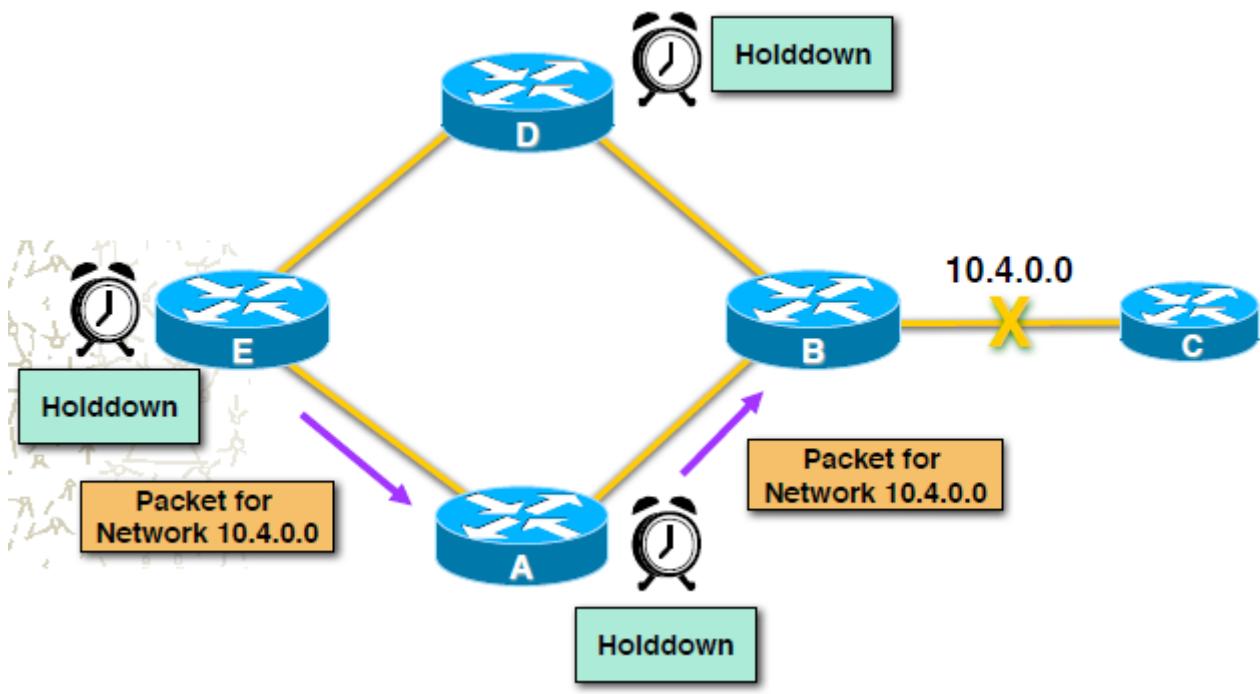
Fino ad esso tutti questi procedimenti avenivano ad un t tempo:



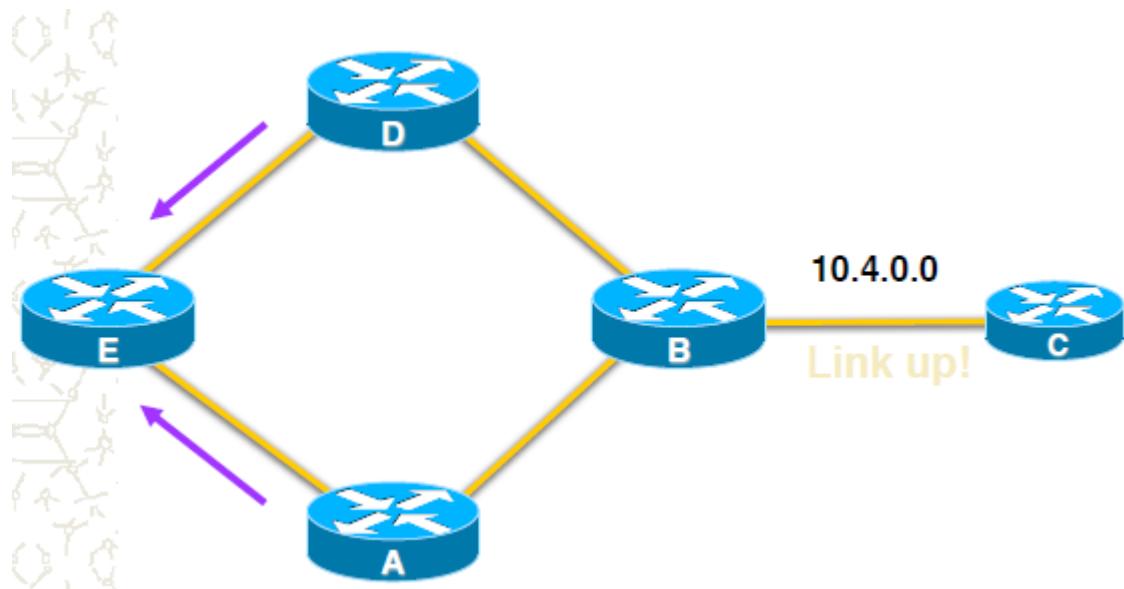
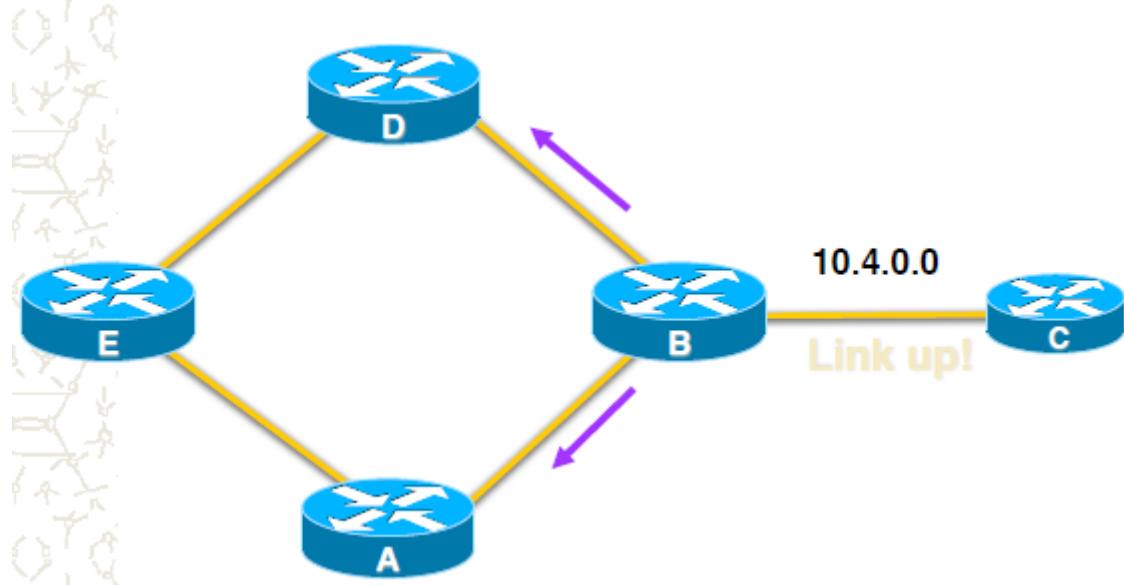
Il Router invia un aggiornamento immediato appena una modifia nella sua routing table ha luogo.
Tutte questo avviene in maniera asincrona.

Esempio:





Nel frattempo 10.4.0.0 torna attivo:



ALGORITMI DI ROUTING LINK STATE

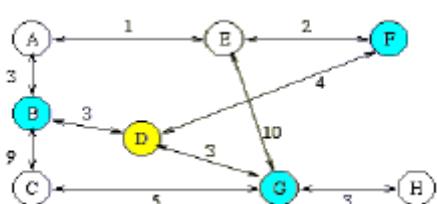
Sono stati introdotti dal 1979 al posto degli algoritmi distance vector. Si basa sull'invio di pacchetti contenenti le informazioni di costo e di ritardo relativi a ciascun link ai nodi adiacenti. Ogni nodo utilizza queste informazioni per calcolare il costo minimo verso tutti i nodi a lui noti.

Link state packet

Ogni router deve avere in memoria la mappa di tutta la rete e coopera per creare una di tutta la rete, mantenendola aggiornata; poi calcola indipendentemente la propria tabella. I routers apprendono i primi n nodi vicini, associando ad ognuno di essi il costo della linea. L'informazione è propagata ai router della rete con un messaggio definito Link State Packet (LSP). La propagazione avviene con l'algoritmo di tipo Flooding.

Meccanismi di invio: OLSA e LSP.

La mappa della rete si costruisce fondendo ogni LSP in un database come mostrato in tabella. L'



LSP database deve essere uguale per ogni router della rete, ne rappresenta la mappa e i costi associati, permette ai router di calcolare le tabelle di routing.

Link State Paket nodo D	
Adiacente	Costo
B	3
F	4
G	3

A	B/3	E/1	
B	A/3	C/9	D/3
C	B/9	G/5	
D	B/3	F/4	G/3
E	A/1	F/2	G/10
F	D/4	F/2	
G	C/5	D/3	E/10
H	G/3		

Passi fondamentali dell'LSP:

- Individuazione dei nodi vicini e dei relativi indirizzi (table discovery)
- Misura del ritardo e del costo verso ciascun vicino
- Costruzione dei pacchetti con le informazioni di routing
- Invio dei pacchetti a tutti gli altri router
- Calcolo del cammino più breve verso ciascun router

Alla fine di questi passi si lanciano più algoritmi di Dijkstra.

Individuazione dei nodi vicini

Quando un nodo si inserisce in rete invia un messaggio HELLO su ciascuna linea. I nodi che ricevono il messaggio rispondono con il loro identificativo. Si invia un messaggio ECHO a cui è richiesta una risposta immediata per misurare il round trip time la cui meta' è una stima del ritardo sulla linea. La valutazione del ritardo puo' comprendere o meno il ritardo di coda.

Pacchetti link state

Il pacchetto inizia con l'identificativo di chi lo manda seguito da un numero di sequenza (32 bit) e dall'età:

Si costruiscono:

- Periodicamente
- In conseguenza di variazioni significative
- Si usa la tecnica *flooding* per la distribuzione: viene controllata la coppia (sorgente, numero di sequenza) per evitare di considerare più volte lo stesso pacchetto
- Quando un nodo ha ricevuto le informazioni da tutti gli altri costruisce il grafo di rete: si utilizza Dijkstra per trovare i cammini minimi.

OSPF è un algoritmo link state.

Requisiti degli algoritmi link state

In una rete con n router e k nodi vicini per router la memoria richiesta in ciascun nodo è proporzionale a kn . Tempi di calcolo lunghi. Per reti estese si realizzano sottosistemi di routing indipendenti con organizzazione gerarchica.

Protocolli di routing gerarchico

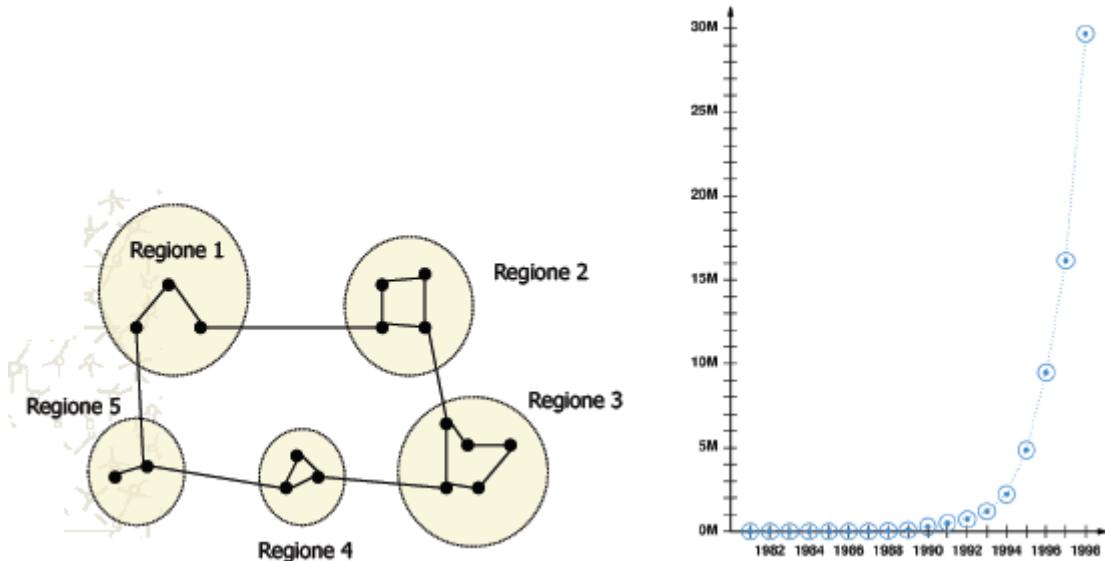
Non potendo gli algoritmi LSP gestire qualsiasi rete di qualsiasi dimensione, occorre organizzare il routing in modo gerarchico, cioè suddividere la rete in aree, dove il routing segue esattamente le regole descritte in precedenza. Per comunicare tra due nodi appartenenti ad aree diverse è necessario conoscere:

- l'instradamento tra il nodo mittente e la periferia dell'area cui il nodo mittente appartiene

- instradamento tra l'area mittente e l'area destinazione
- instradamento all'interno dell'area destinazione.

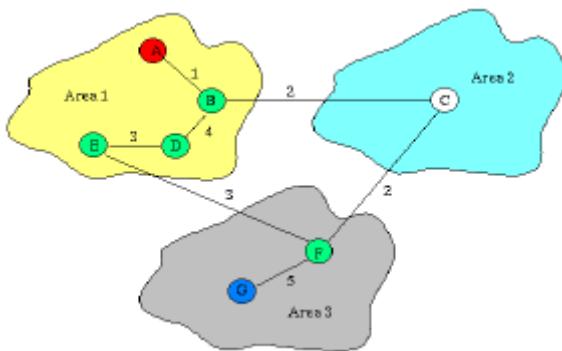
Gli SLP passano solo nei messaggi aggregati.

A causa della crescita esponenziale di Internet, le tabelle di routing diventano sempre più grandi. Quindi si divide il gruppo di router in regioni. Ogni router conosce i dettagli della propria regione e come comunicare con le altre, ma non conosce la loro struttura interna. Può occasionalmente generare cammini non ottimali, ma il vantaggio in termini di riduzione delle tabelle di routing vale la spesa.



Esempio:

Per instradare il messaggio dal nodo G ad A, si invia il messaggio ad F che lo instrada all'area 1 con due possibilità: il cammino diretto (costo 3) o quello indiretto (costo 4 tramite l'area 2). E' scelto il cammino (instradamento) diretto che passa E, D, B e A, nodo destinatario, ritenuto ottimale con costo 16: non è ottimo perché passando da C sarebbe stato 10. Non avendo una visione globale della rete, il routing gerarchico compie scelte che possono non essere l'ottimo globale.



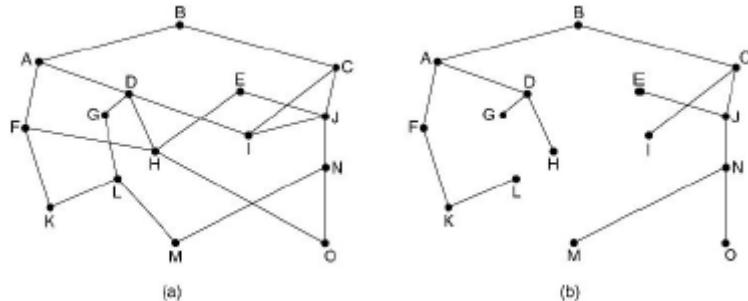
Routing broadcast

Alcune applicazioni desiderano inviare pacchetti a molti o tutti gli host della rete. Molti protocolli di livello di data link delle reti locali hanno questa funzionalità, che però non è disponibile nelle reti geografiche. Esistono diverse soluzioni:

- la sorgente invia un pacchetto distinto a tutte le destinazioni:
 - poco pratico, perché la sorgente deve sapere quali sono le destinazioni possibili
 - costoso in termini di efficienza
- l'instradamento flooding può essere utilizzato a questo scopo, ma ha il difetto di inondare la rete di pacchetti.

Una soluzione funzionale (anzi, la soluzione ottimale) è quella di applicare un algoritmo

funzionalmente simile allo spanning tree del data link layer, a partire dal router che ha generato la trasmissione. Questo meccanismo si basa sul principio di ottimalità: se il cammino ottimale da I a J attraversa K, allora il percorso ottimale da K a J segue la stessa strada. L'insieme dei cammini ottimali da un router verso tutte le destinazioni non può quindi contenere percorsi circolari, cioè ha una struttura ad albero, detta sink tree.



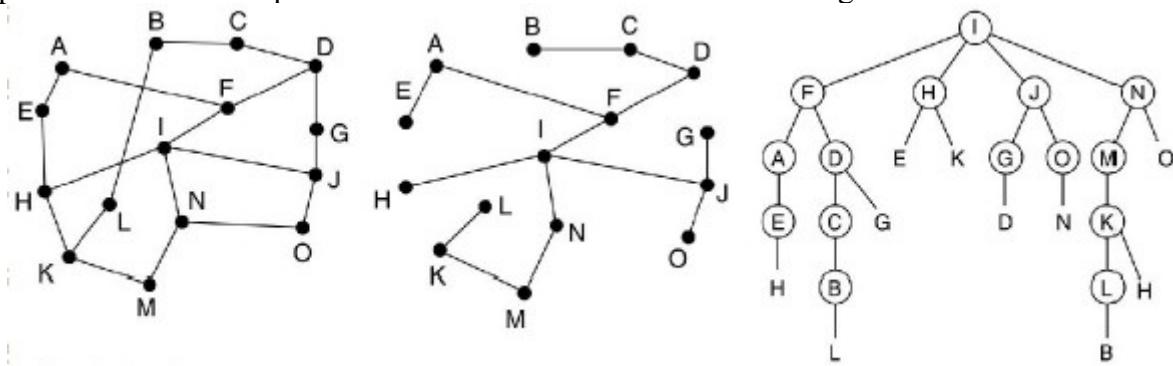
Utilizzando il sink tree, la trasmissione del pacchetto broadcast si può ottenere semplicemente: i router inviano il pacchetto solo sulle proprie linee uscenti appartenenti a quel sink tree.

Questo protocollo ha il difetto che ogni router deve essere capace di calcolare il sink tree relativo al router che ha generato il pacchetto, quindi deve conoscere la topologia della rete:

- ad esempio il distance vector non può farlo
- il link state può farlo

Una soluzione che non richiede la conoscenza della topologia è quella nota come reverse path forwarding: quando un router riceve un pacchetto broadcast da una sorgente, calcola se l'interfaccia da cui ha ricevuto il pacchetto è quella verso la quale instraderebbe un pacchetto destinato al router sorgente; se la strada è la stessa, allora il router che ha ricevuto il pacchetto appartiene al sink tree del router sorgente, ed inoltra il pacchetto su tutte le altre linee; se la strada non è la stessa, il pacchetto viene scartato. È meno efficiente del sink tree, ma di applicabilità più generale.

Il numero di pacchetti generati dal reverse path forwarding è superiore a quello del sink tree, ma ampiamente inferiore rispetto alla soluzione del meccanismo flooding.



Routing per host mobili

Si basa sul concetto di agenti:

Agenti Base: Ogni area o regione ha un agente che tiene traccia degli utenti la cui base è nell'area.

Agenti Ospite: Ogni area o regione ha uno o più agenti che tengono traccia degli utenti in visita.

1. Periodicamente, ogni agente ospite spedisce in broadcast un pacchetto che annuncia la sua esistenza e il suo indirizzo. Un host mobile appena arrivato aspetta uno di questi pacchetti, ma nel caso che non ne arrivi nessuno, può spedire in broadcast un pacchetto che chiede se ci sia un agente ospite disponibile.
2. L'host mobile si registra presso l'agente ospite, fornendo il proprio indirizzo base, il proprio indirizzo presente a livello data link e le informazioni per l'autenticazione dell'identità.
3. L'agente ospite contatta l'agente base dell'host mobile e lo avverte che uno dei suoi utenti è attualmente collegato. Il messaggio contiene anche tutte le informazioni di autenticazione

necessarie ad ottenere un autorizzazione dall'agente base stesso.

4. Se l'host mobile viene riconosciuto come proprio dall'agente base, allora viene trasmesso un messaggio di consenso all'agente ospite.

5. Solo a questo punto, l'agente ospite registra l'host mobile nelle tabelle di routing. Questo sistema permette anche il relay di informazioni dalla regione base alla regione attuale dell'host mobile.

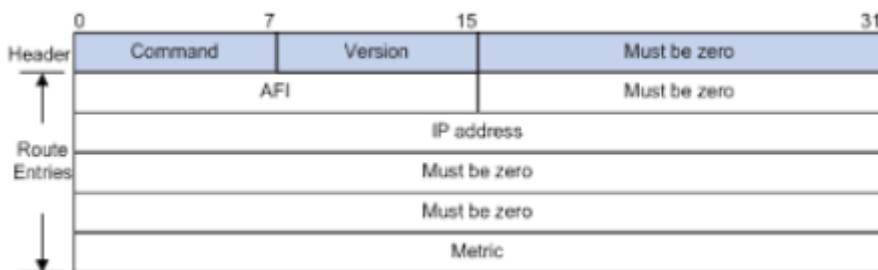
Protocolli IGP: RIP

Il primo protocollo di routing interno utilizzato in Internet e' il RIP (Routing Information Protocol), ereditato da Arpanet: RIP e' un protocollo basato sull'algoritmo distance vector. Deve la sua diffusione al fatto che una sua implementazione (routed) era compresa nella Berkeley Software Distribution di Unix che supportava il TCP/IP. Adatto a reti di dimensioni limitate, ha iniziato a mostrare i suoi limiti già alla fine degli anni '70. Attualmente ancora utilizzato come protocollo di routing in qualche piccola rete privata. Caratteristiche del modello distance vector utilizzate da RIP:

- Usa numero degli hop come metrica per il costo dei link: tutte le linee hanno costo 1
- Il costo massimo e' fissato a 15, quindi impone il suo uso su reti di estensione limitata (diametro inferiore a 15 hop)

Le tabelle di routing vengono scambiate tra router adiacenti ogni 30s via un messaggio di replica del RIP (*RIP response message*) o avviso di RIP (*RIP advertisement*).

Questo messaggio contiene voci della tabella del mittente per un massimo di 25 reti di destinazione dell'AS.



Protocolli IGP: OSPF

Nel 1979 Internet e' passata ad un protocollo di tipo link state:

- ciascun router utilizza il flooding per propagare lo stato delle sue connessioni agli altri router della rete
- ciascun router conosce la topologia completa della rete

Alla fine del 1988 e' stato sviluppato un successore chiamato OSPF (Open Short Path First), definito nell'RFC 2328. OSPF e' oggi il piu' diffuso protocollo IGP utilizzato in Internet.

OSPF e' stato progettato cercando di soddisfare diversi requisiti:

- nessun vincolo di brevetto (O = Open)
- supporto di diverse metriche per la distanza (distanza fisica, hop, ritardo, costo della linea, ...)
- algoritmo capace di reagire dinamicamente e rapidamente ad eventi che modificano la topologia (link state)
- instradamento basato sul tipo di servizio (sfruttando i campi esistenti nell'header di IP, ad esempio)
- questo e' stato incluso in OSPF, ma tutti (implementazioni ed applicativi) hanno continuato ad ignorare questa possibilita'
- capacita' di bilanciare il carico su diversi cammini
- supporto per sistemi gerarchici (quindi routing gerarchico anche all'interno dello stesso AS)
- implementazione di sicurezza
- supporto per il tunneling

OSPF gestisce tre tipi di connessione:

- linea punto-punto tra router
- rete locale multiaccesso: una rete locale dotata di più accessi, quindi di più router
- rete geografica multiaccesso: rete geografica connessa al resto dell'AS da più di un router

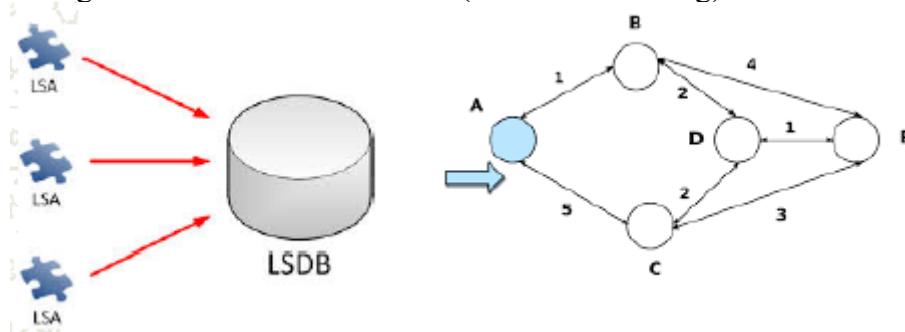
OSPF considera la rete come un grafo con i router come punti, e le linee come archi

- ogni linea fisica è costituita da due archi, uno per ogni verso
- una rete multiaccesso è considerata come un punto del grafo, connessa a ciascun router della rete da una coppia di archi

OSPF assegna un costo ad ogni arco, e determina il cammino più breve in base al costo complessivo del tragitto; i cammini nei due versi di una singola connessione possono avere costi differenti

I nodi di rete non hanno peso in OSPF, ed la loro connessione al router viene valutata a costo 0.

Funzionamento: Ciascun router invia a tutti gli altri router dell'area lo stato dei suoi collegamenti (LSA). Ogni router ha una visione completa della rete memorizzata in un suo LS DB (collezione di LSA) o database topologico. Attraverso l'algoritmo di Dijkstra ogni nodo calcola individualmente il percorso di minor costo da sé verso ogni altro nodo dell'area. Eventuali modifiche vanno segnalate a tutti i nodi nell'area (broadcast/flooding).



Messaggi OSPF:

LINK STATE UPDATE:

- Aggiornamenti sullo stato di link o nodi
- Ogni messaggio ha un numero di sequenza
- I messaggi vengono riscontrati (LS ACK)

LINK STATE REQUEST: È una richiesta esplicita di informazioni

DATA BASE DESCRIPTION:

- Fornisce i numeri di sequenza delle informazioni link state possedute da chi lo spedisce.
- È una copia del LS DB usata per sincronizzare un nuovo nodo.

0	8	16	24	31
LS age	Options	LS type		
Link State ID				
Advertising Router				
LS sequence number				
LS checksum	Length			

Arene OSPF:

Al crescere delle dimensioni anche alcuni AS sono diventati troppo complessi per essere gestiti in modo non gerarchico.

OSPF permette di dividere un AS in più aree:

- ogni area è una rete o un insieme di reti direttamente connesse
- le aree non hanno componenti sovrapposti
- in ciascun AS deve esistere un'area dorsale (l'area 0) a cui sono collegate tutte le altre aree dell'AS: è possibile passare da un'area qualunque ad un'altra area dell'AS attraverso la dorsale, che le connette tutte.

Tipi di router OSPF:

OSPF definisce quattro tipi di router

- router interni (internal router): router interni ad un'area
- router di confine (border router): router che collega due o più aree (una è sempre l'area

della dorsale)

- router di dorsale (backbone router): router interno della dorsale
- router di confine dell'AS (boundary router): router che collega l'AS ad uno o piu' AS differenti

Naturalmente le funzioni possono sovrapporsi

- un router di confine e' anche router interno
- un boundary router e' anche un backbone router
- un backbone router non connesso ad altre aree o ad altri AS e' un router interno (per l'area 0).

Instradamento fra aree nell'OSPF:

- Intra-area: Il router conosce gia' il cammino minimo
- Inter-area:
 - Dalla sorgente al router del backbone
 - Dal router del backbone all'area destinazione
 - Alla destinazione
- Inter-AS: Si utilizza un protocollo di routing esterno

Costruzione delle tabelle OSPF:

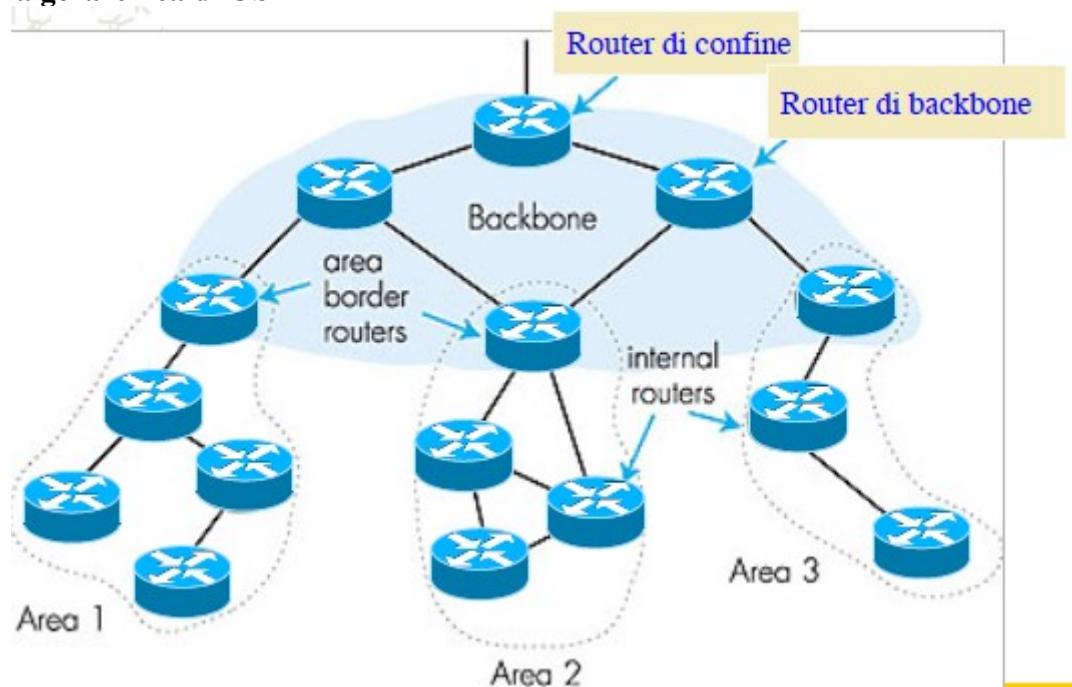
Secondo la logica link state, ogni router di ogni area conosce la topologia dell'area e puo' effettuare routing interno. All'interno di un'area i router hanno lo stesso insieme di dati link state.

Un router collegato a piu' aree mantiene i data base di ciascuna.

I router di backbone accettano le informazioni anche dai router di confine delle altre aree; in questo modo ogni router di backbone sa a quale router di confine di un'area inviare i pacchetti destinati a quella area.

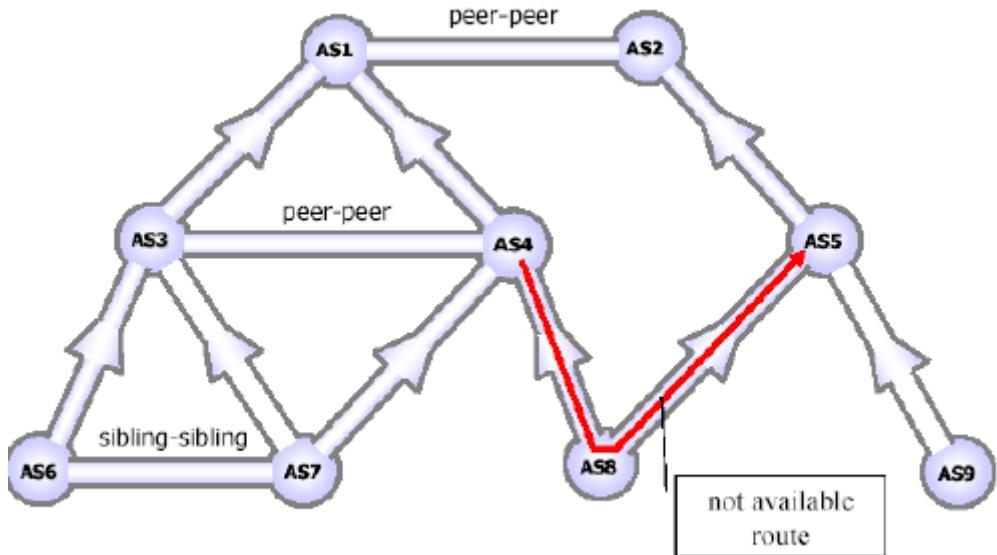
Le informazioni delle adiacenze dei router di confine verso l'area di backbone sono propagate dentro l'area; in questo modo ogni router interno sa a quale router di confine della propria area inviare un pacchetto destinato ad un'altra area.

Struttura gerarchica di OSPF



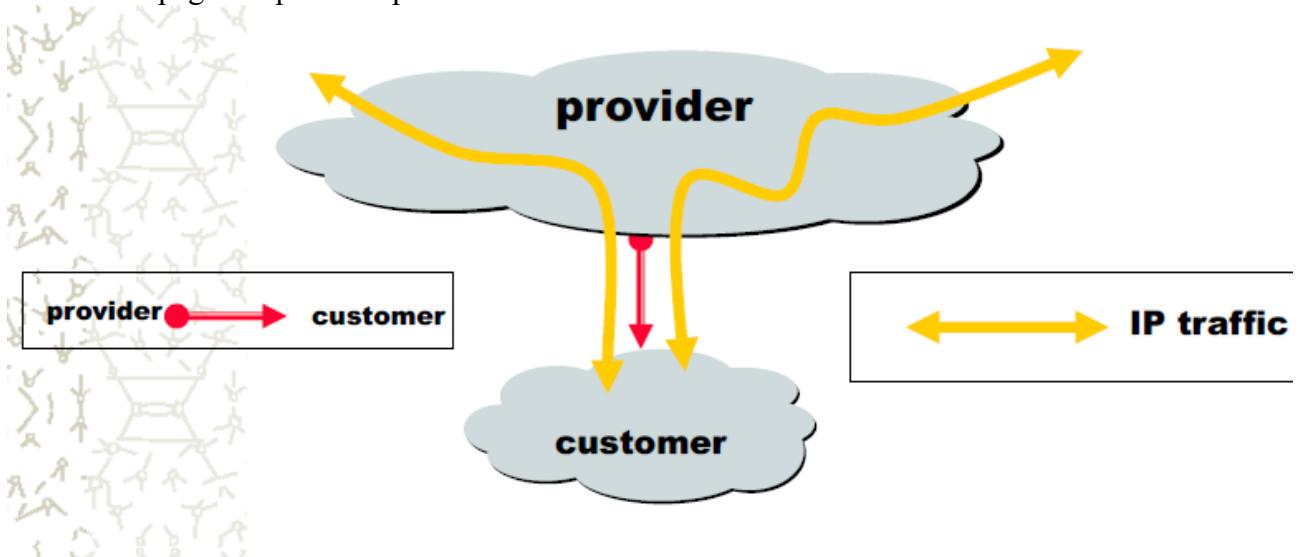
Sistemi autonomi

Ogni organizzazione è composta da un insieme di router e LAN sotto una singola amministrazione. Un algoritmo di routing è prescelto per aggiornare automaticamente le tabelle di instradamento. Un AS definisce in maniera coerente le politiche di instradamento all'interno della sua organizzazione. Quando più organizzazioni si uniscono per formare una Inter-rete, occorre stabilire tra loro punti di collegamento o di **peering** (rapporto di interscambio tra annunci).

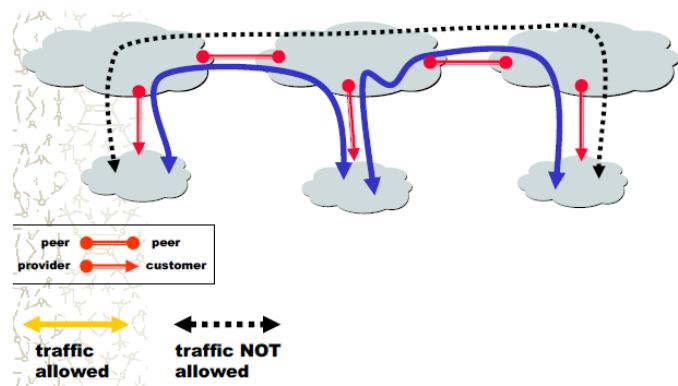


Ruoli nel peering: Customers e Providers

I Customer pagano i provider per accedere a Internet

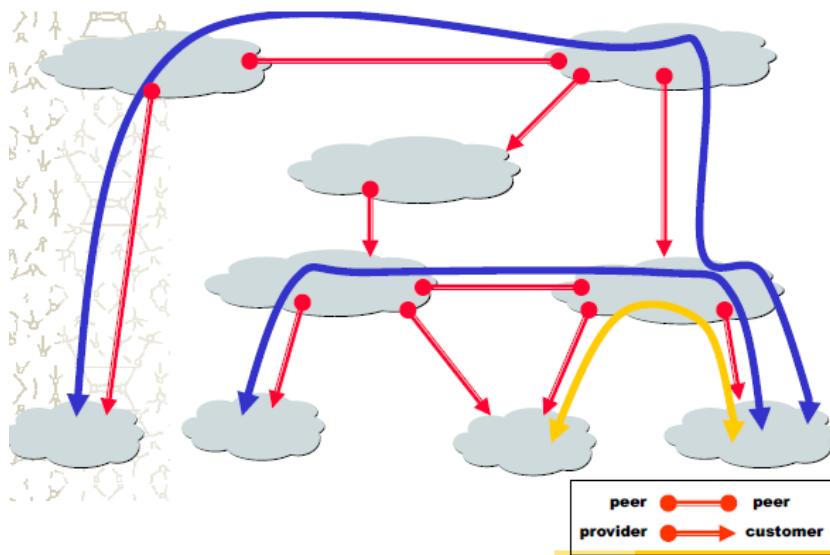


I provider di transito garantiscono il passaggio del traffico fra i rispettivi customers



Peering per la connettività Tier 1

La pratica del Peering consente la connettività tra i "Tier 1" providers.



Sistono anche altri tier:

Tier 3: i providers danno servizio ad utenti finali.

Tier 2: i providers danno servizio ad altri providers.

Instradamento tra AS

Ogni tabella deve avere un'entry per ogni possibile destinazione. Questo deve valere sia per le destinazioni locali che per quelle globali.

Le tabelle di instradamento si aggiornano in 3 modi:

1. Eseguire un unico algoritmo di instradamento tra organizzazioni adiacenti:

ha molti Svantaggi:

- Ritardo di propagazione, ex: distance vector
- Rallentamento: messaggi di instradamento inviati agli altri routers con l'elenco delle possibili destinazioni
- Tutte le organizzazioni sono forzate ad usare lo stesso algoritmo
- Un nuovo algoritmo di instradamento è di difficile adozione
- Non considera le relazioni politiche e commerciali tra sistemi autonomi

2. Aggiornare le tabelle di instradamento manualmente aggiungendo percorsi statici

predefiniti: Si nasconde la parte interna dell'AS. Per ogni obiettivo esterno si identifica un router alla frontiera del Sistema Autonomo di destinazione. Informazione sul cammino da seguire per raggiungere l'obiettivo. Svantaggi:

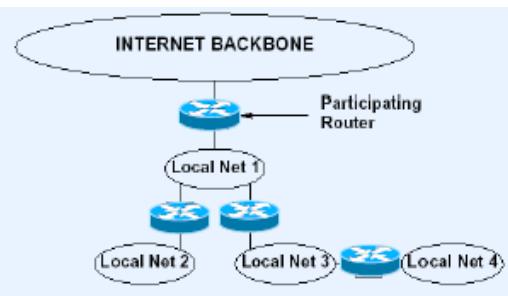
- difficile da aggiornare e da correggere
- I malfunzionamenti non sono gestiti, non si ha backup
- Nessuna garanzia che tutti i router del percorso sono in effetti disponibili per portare il traffico a destinazione

L'algoritmo di instradamento diffonderà all'interno dell'AS il traffico locale come il traffico che segue i percorsi statici.

3. Combinare un protocollo di instradamento intradomain con un protocollo di instradamento interdomain: Exterior gateway protocol

Le reti nascoste

Ogni AS ha una topologia complessa, formata da diverse Reti Locali. Non tutte le reti locali sono connesse ad un router di frontiera dell'AS. Occorre informare l'esterno delle Reti Locali raggiungibili. All'esterno dell'AS i suono protocolli comuni per poter comunicare in modo ottimale. Occorre avere un flusso informativo in due direzioni, sia dall'interno verso l'esterno che dall'esterno verso l'interno. L'AS si deve far carico di garantire la



consistenza degli instradamenti interni. Occorre annunciare all'esterno quali reti interne sono raggiungibili. Occorre assegnare le responsabilità per la diffusione delle informazioni riguardo l'instradamento.

Exterior gateway protocolli

Protocollo per lo scambio delle informazioni sull'instradamento tra Sistemi Autonomi.

BGP – Border Gateway Protocol: Due AS che si scambiano informazioni di instradamento designano due router che stabiliscono una sessione di peering. Router che partecipano a BGP sono detti Router di Confine o Gateway.

Approccio:

- Nascondi la parte interna degli AS
- Mantieni solo le zone di demarcazione e i router di frontiera degli AS

Ogni router di frontiera rappresenta le destinazioni interne come se fossero locali. Semplifica il grafo considerando le informazioni sulla raggiungibilità sia interna che esterna all'AS. Il grafo è gestito attraverso sessioni peering TCP. Risvolvi il problema dell'instradamento nel grafo così.

Definisci anche percorsi prestabiliti sulla base di considerazioni politiche. Abbiamo ora un grafo degli AS dove il nodo è l'AS ee l'arco è l'accordo.

BGPv4 : Border Gateway Protocolli

BGP mantiene aggiornate le tabelle di instradamento e propaga le informazioni sull'instradamento. BGP considera la disponibilità delle organizzazioni a cooperare nel processo di instradamento (accordi commerciali, questioni legali, preferenze locali).

Caratteristiche:

- Fornisce comunicazione tra AS
- Coordinamento tra speaker di uno stesso AS -- diffusione di informazioni coerenti
- Diffusione dell'informazioni di raggiungibilità all'interno dell'AS e attraverso l'AS, e apprende tali informazioni da altri AS
- Next hop routing – simile a distance vector routing
- Utilizza TCP per le sessioni di peering
- Invia messaggi Keep-alive per informare dello stato della connessione anche se nessun messaggio è inviato
- Informazioni sull'instradamento, router che saranno attraversati fino a destinazione
- Aggiornamenti incrementali per risparmiare banda
- Supporto CIDR – invio della maschera insieme all'indirizzo
- Aggregazione delle informazioni di instradamento per destinazione correlate
- Consente al destinatario di autenticare i messaggi

Numerazione degli AS

BGP richiede un numero identificativo per ogni AS (Autonomous System Number, asn) tra 1 e 65,535, è un numero univoco su tutta la rete internet. Numeri maggiori di 64,511 sono detti "privati". Un asn può essere ottenuto da:

- asn globale – all'autorità internet regionale: ripe, arin, apnic
- asn privato – all'isp

Funzionalità BGP

1. Apertura connessione tra peers
2. Annuncio informazioni sulla raggiungibilità
3. Verifica corretto funzionamento

Quattro tipi di messaggio BGP:

Type Code	Message Type	Description
1	OPEN	Initialize communication
2	UPDATE	Advertise or withdraw routes
3	NOTIFICATION	Response to an incorrect message
4	KEEPALIVE	Actively test peer connectivity

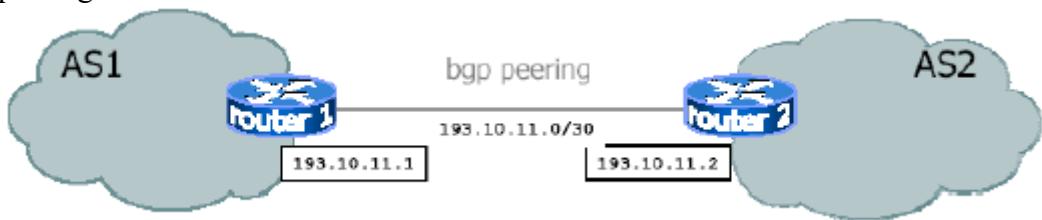
Intestazione messaggi:

Precede ogni messaggio BGP ed identifica il tipo di messaggio. Marker (16 byte): scelto in accordo tra le due parti per sincronizzare i messaggi. Questa funzione non è fornita da TCP. Length (2 byte): lunghezza del messaggio tra 19 e 4096 byte. Type: tipo di messaggio BGP.



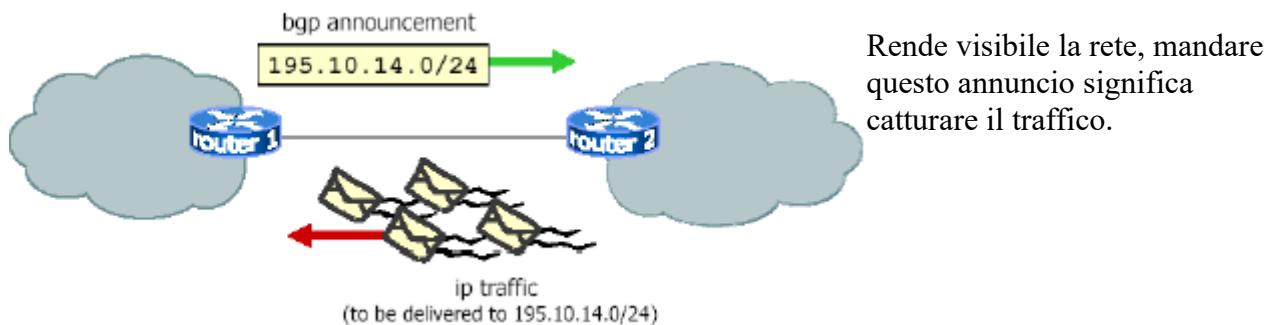
Peering tra due AS

Le informazioni possono essere scambiate tra due AS solo se una sessione peering è attiva. La sessione peering è una connessione TCP tra i due AS.



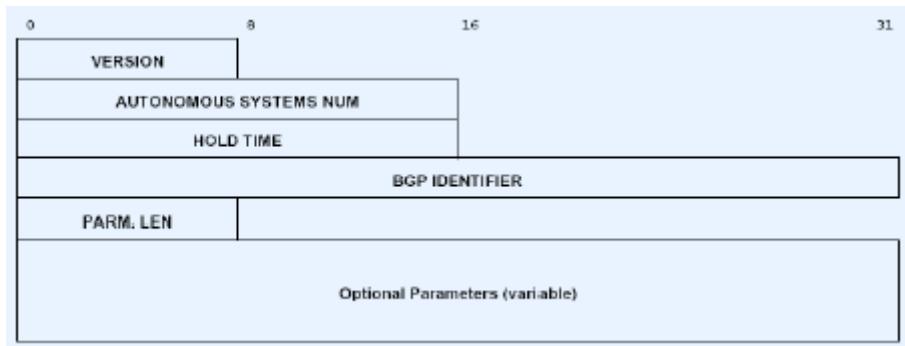
Annunci BGP

BGP permette ad un AS di offrire connettività ad un altro AS. Offrire connettività significa promettere il recapito ad una specifica destinazione.



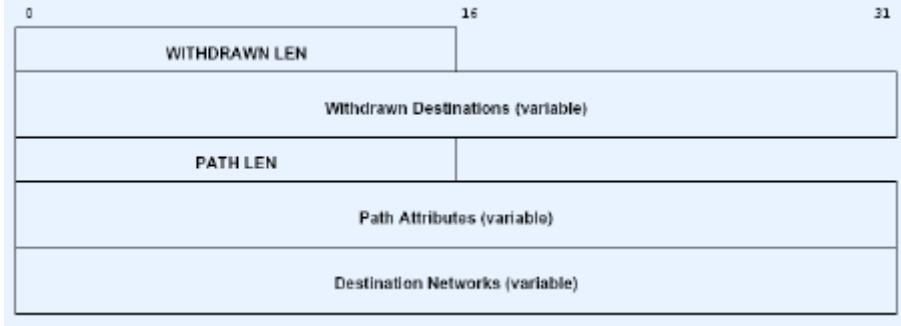
Comandi:

Open: Utilizzato per aprire una connessione peer. Il campo Hold specifica il massimo numero di secondi tra due messaggi successivi. Un router bgp è caratterizzato dall'asn e da un identificatore unico a 32 bit che deve usare per tutte le connessioni peering. Parametri opzionali: ad esempio per l'autenticazione.



Il router destinatario di un messaggio OPEN risponde con un KEEPALIVE. Connessione aperta quando entrambi i router inviano un messaggio OPEN ed un messaggio KEEPALIVE.

Update: Announcement = prefix + attributes values. Annuncia nuove reti raggiungibili ed eventualmente l'instradamento. Annuncia reti precedentemente annunciate non più.



Nota: *KEEPALIVE* = Verifica periodicamente la connessione TCP tra entità peer. Più efficiente rispetto ad inviare periodicamente messaggi di instradamento. Intervallo *KEEPALIVE* ogni 1/3 di HOLD time, mai inferiore a 1 sec.

NOTIFICATION = Controllo o segnalazione errori. BGP invia un messaggio di notifica e chiude la connessione TCP. Errori:

1. Errore nell'intestazione del messaggio
2. Errore nel messaggio OPEN
3. Errore nel messaggio UPDATE
4. Timer di attesa scaduto
5. Errore nella macchina a stati finiti
6. Fine (connessione terminata)

Prefissi di rete complessità

Specifica solo i bytes ,corrispondenti al prefisso: 1 – 4 byte: maschere fino a 8,16,24 bit
Ex: 220.123 o 220.16.128.



Filtraggio degli annunci:

Gli annunci sono inviati e/o accettati solo se alcune condizioni sono verificate. Gli annunci possono essere filtrati sulla base di:

- Una lista di prefissi validi
- Una lista di numeri di AS

Path attributes

BGP specifica più di un salto successivo verso la destinazione. Gli attributi possono indicare:

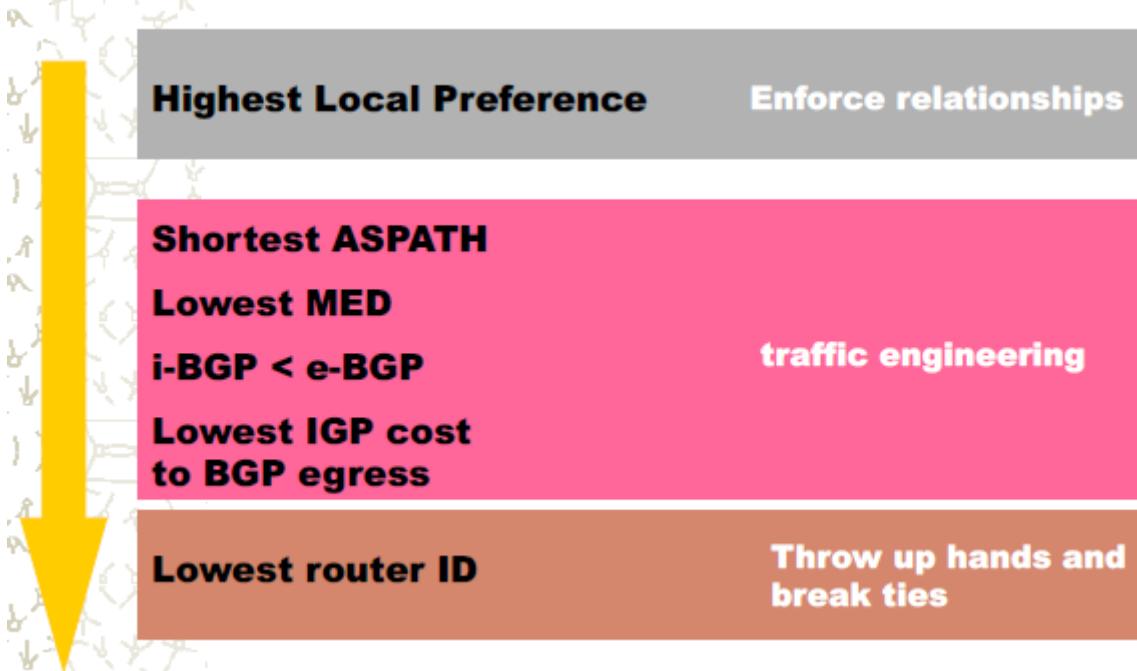
- Sistemi autonomi attraversati verso la destinazione
- Provenienza delle informazioni sull'instradamento: locali (igp) o apprese da altri sistemi autonomi (egp)

Attributi sono comuni a tutte le destinazioni annunciate. Destinazioni con attributi diversi devono essere annunciate con messaggi diversi. Permette di individuare cicli sugli instradamenti e provenienza dei messaggi. Sono delle decisioni che ci dicono come comportarci con quell'annuncio.

Codice tipo:

1. Origine informazione instradamento
2. Elenco sistemi autonomi sul percorso
3. Salto successivo (chi è l'ho successivo)
4. Discriminazione tra più punti di uscita all'AS (MED Multi Exit Discriminator)
5. Preferenza all'interno dell'AS (preferenza per il circuito che si desidera usare)
6. Indicazione di percorsi riuniti
7. ID dell'AS che ha riunito i percorsi

Route selection basata su Path attributes



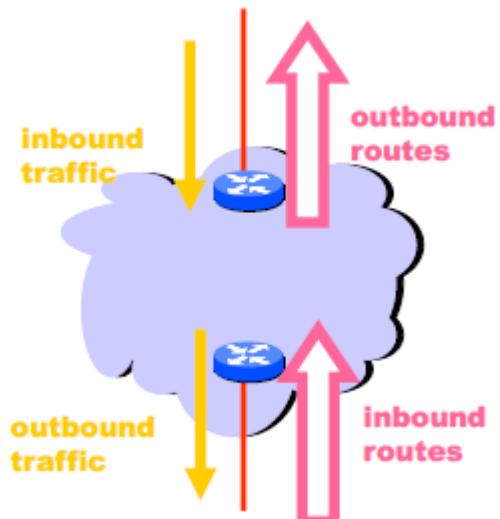
USO degli attributi BGP:

In ingresso:

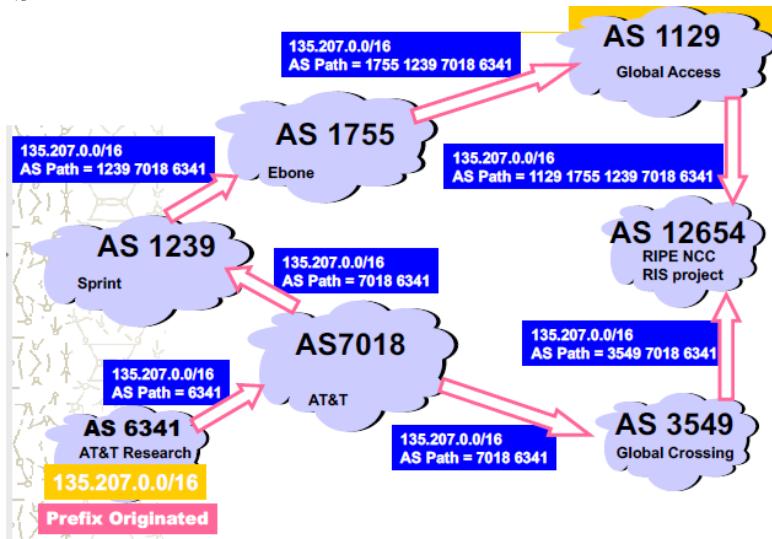
- Utilizzabili per il Filtraggio delle routes in ingresso.
- La manipolazione di attributi sulle routes uscenti consente **di tentare** di influenzare la selezione dei percorsi dagli altri AS verso l'interno.

In Uscita:

- Utilizzabili per il Filtraggio delle routes in uscita
- La manipolazione di attributi sulle routes entranti consente **di influenzare** la selezione dei percorsi verso l'esterno

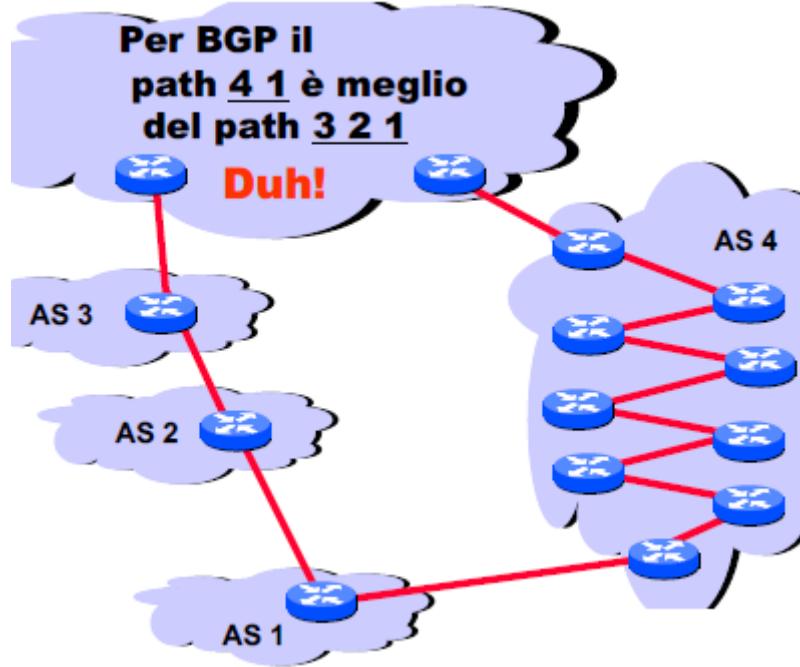


AS-PATH



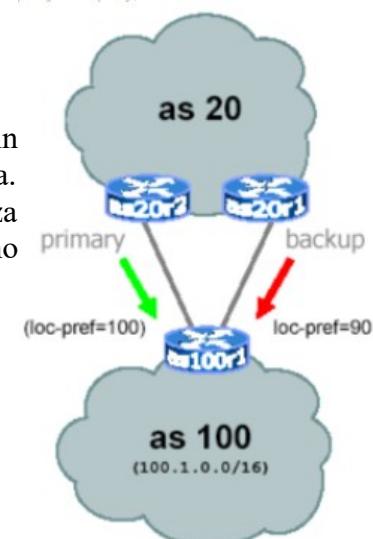
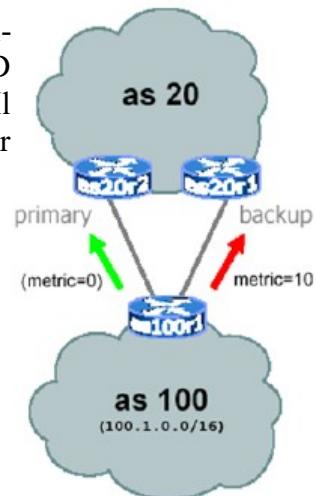
Equivoci sul percorso minimo

Il path più corto non corrisponde necessariamente al percorso di rete realmente più breve.



Metric o MED

L'attributo noto come «metrica» è anche chiamato «multi-exitdiscriminator» (MED). L'AS ricevente in presenza di 2 MED differenti dovrebbe adottare la route associata a quello più piccolo. Il valore di default del MED è 0. È usato sugli annunci in uscita per condizionare il comportamento del traffico in ingresso.

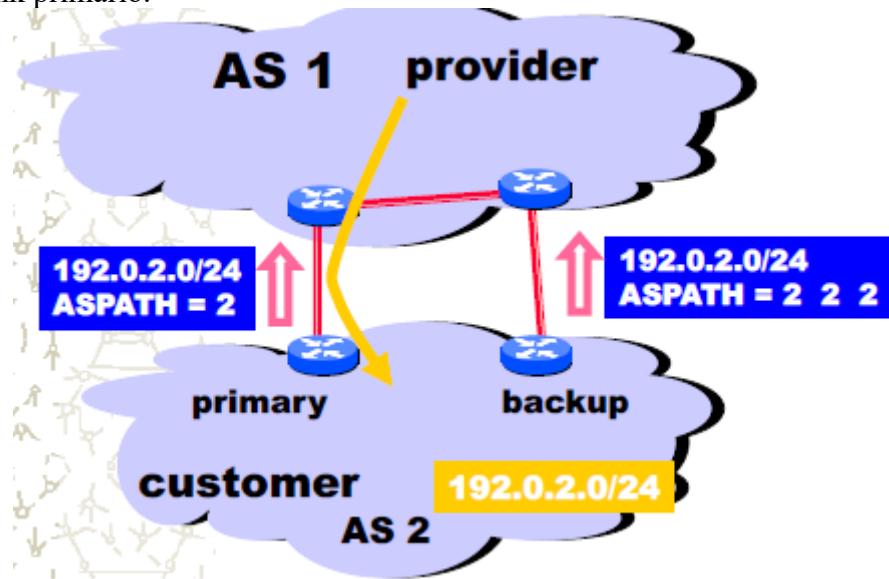


Local Preference

L'attributo noto come «local preference» è associabile agli annunci in ingresso ed è utile per gestire politiche di scelta sul traffico in uscita. Nell'algoritmo di decisione BGP è verificato prima della lunghezza dell'AS-PATH. Il valore di default è 100. Valori più elevati sono preferibili. Il traffico esce dove c'è preferenza maggiore.

AS path prepend

Il Padding del path con AS numbers ripetuti può essere utile per forzare il traffico da AS 1 attraverso il link primario.

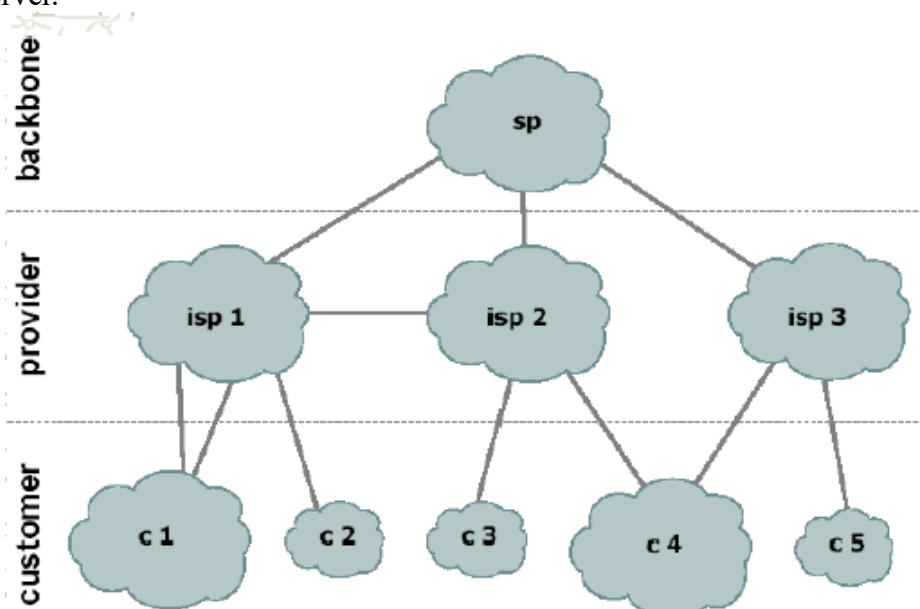


Limiti di BGP

BGP non può discriminare tra due percorsi sulla base della distanza o della congestione (discrimina solo in base alla lunghezza dell'AS path, MED o metrica). L'informazione di raggiungibilità fornita da due AS è indistinguibile (la scelta è fatta solo sul percorso più breve). Il BGP sceglie uno dei due percorsi possibili non sulla base di una metrica di costo. Il BGP permette di suddividere il carico attraverso la rete ma non in modo dinamico. Occorre configurare manualmente quale reti sono annunciate da quali routers esterni. Tutti i sistemi autonomi devono concordare su uno schema coerente per annunciare la raggiungibilità.

Intradamento con arbitraggio

Occorre un sistema per garantire la coerenza sulle informazioni di instradamento. Database autenticato e replicato che contiene le informazioni sulla raggiungibilità. Autenticazione permette di annunciare la raggiungibilità di una rete solo al SA che la possiede. NAP sono i router di interconnessione tra ISP. I NAP hanno un Router Server che mantiene il database BGP ma non sono necessariamente speaker BGP. Gli speaker BGP mantengono aperto un collegamento verso il Router Server.



Classificazione delle reti

Stub network: un collegamento ad un singolo isp.



Multi-homed stub network: due o più collegamenti allo stesso isp backup o divisione del carico.

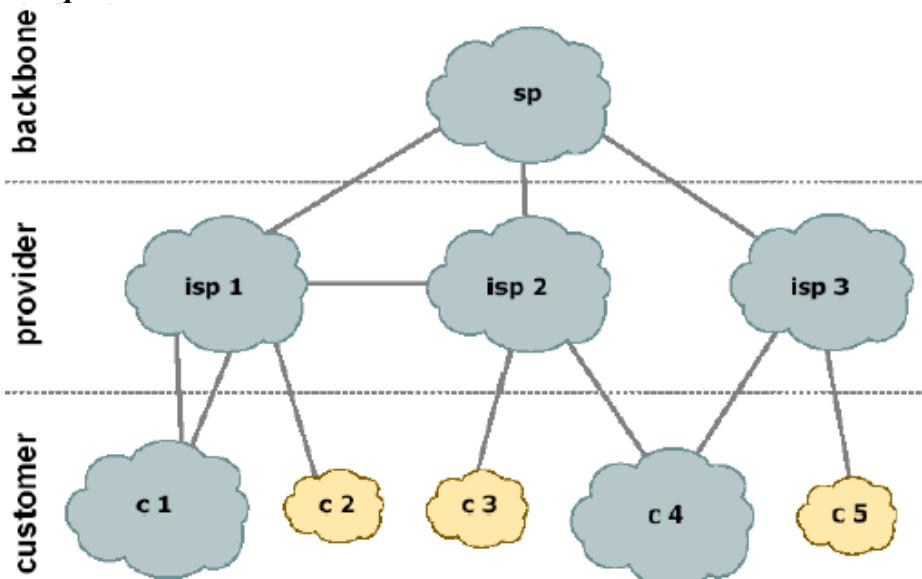


Multi-homed network: due o più collegamenti a isp differenti backup o divisione del carico.



NOTA: isp = provider.

Esempio di stub network



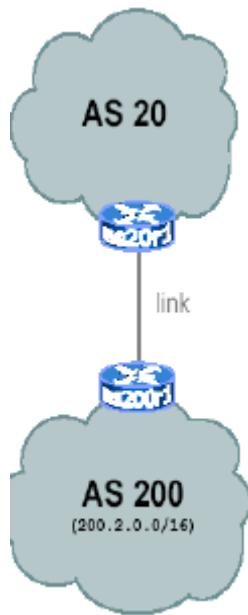
Stub network architettura

Un router della rete è scelto come gateway di default è connesso ad un singolo router dell'isp con una o più connessioni. Una singola sessione di peering in cui as 200 annuncia la sua raggiungibilità e accetta l'instradamento di default sul router.

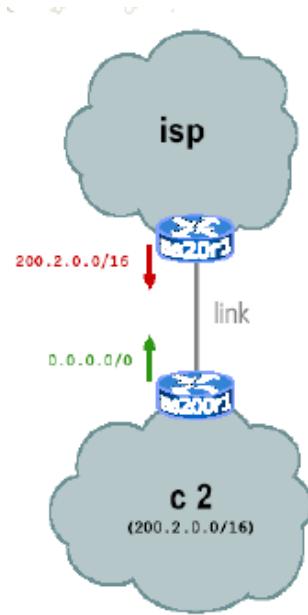
Instradamento statico:

Un instradamento statico di default è sufficiente per i pacchetti in uscita per essere inviati su internet attraverso la connessione all'isp. Un instradamento statico è anche sufficiente per i pacchetti in ingresso per raggiungere la rete attraverso la connessione all'isp. Non vi è alcun bisogno di BGP.

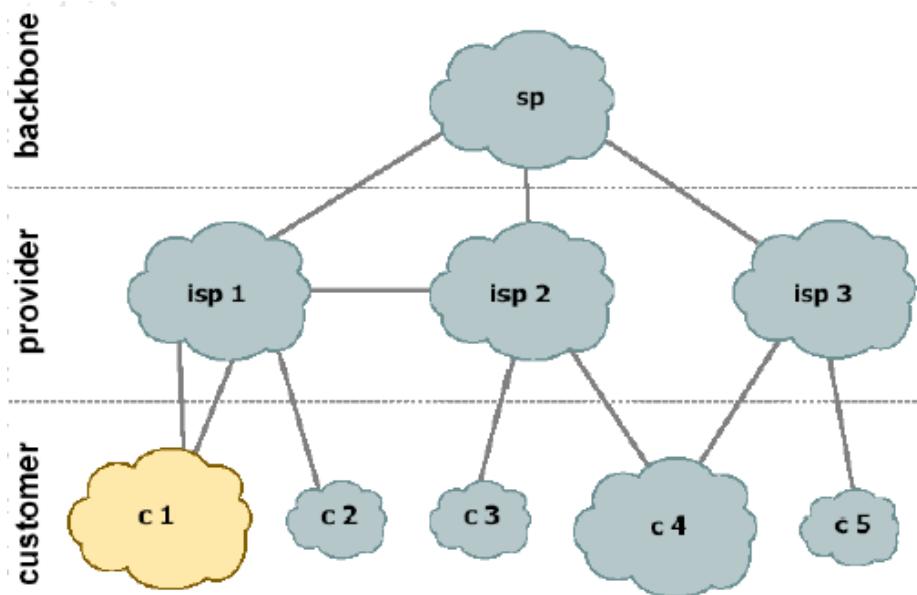
Archittettura stub network:



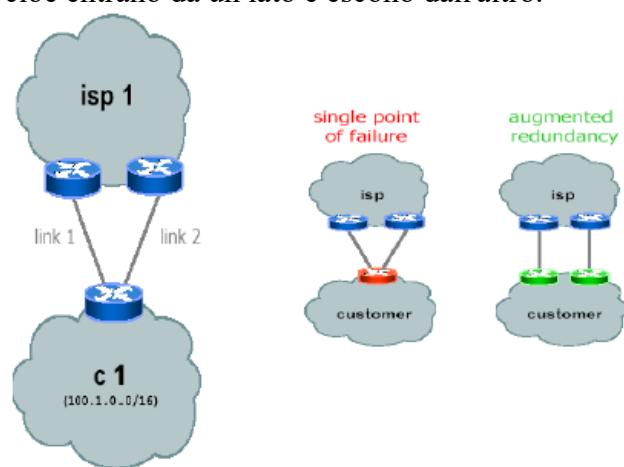
Instradamento statico:



Multi-homed stub networks



Due collegamenti allo stesso isp. Due routers della rete customer sono di solito coinvolti. Si può avere simmetria, cioè entrano da un lato e escono dall'altro.

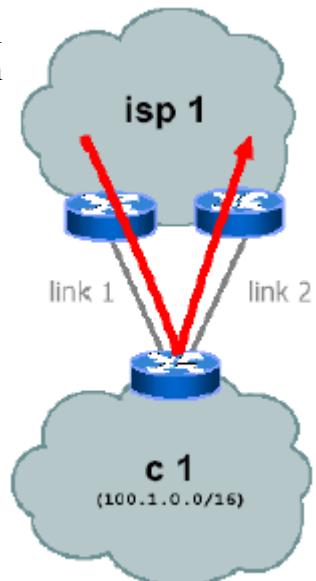


Instradamento nelle multi-homed

Un pacchetto diretto ad Internet può attraversare uno dei due link. Un pacchetto proveniente da Internet può attraversare uno dei due link. Un pacchetto in transito può attraversare entrambi i link.

Ci sono delle politiche che si applicano, e sono le seguenti:

- **Eliminare traffico in transito**
- **Traffico in ingresso:**
 - Utilizzare link 1
 - Utilizzare link 2 in caso di fault su link 1
- **Traffico in uscita:**
 - Utilizzare link 1
 - Utilizzare link 2 in caso di fault su link 1



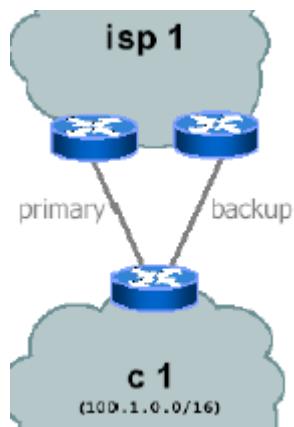
Esistono delle alternative all'uso di BGP.

- Usare un igp:
 1. Pacchetti usano link 1 o link 2 a seconda dello shortest path verso c1
 2. Non è possibile escludere pacchetti in transito quando link 1 e link 2 sono sul cammino minimo tra sorgente e destinazione
- Usare cammini statici:
 1. I routers dell'isp e la rete devono essere configurati manualmente in modo coerente.
 2. Non è possibile gestire un meccanismo di backup automatico.

BGP si basa su un'Annuncio/16 aggregato su ogni arco:

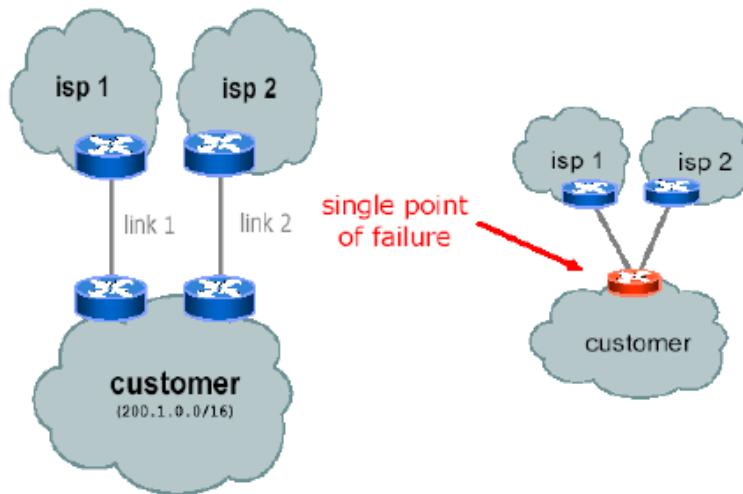
- Link primario invia un announcement standard
- Il link di backup aumenta il costo sugli annunci in uscita e riduce la preferenza sugli annunci in ingresso

Quando occorre un fault su un link, l'annuncio del /16 aggregato sull'altro link assicura la connettività.



Multi-homed network

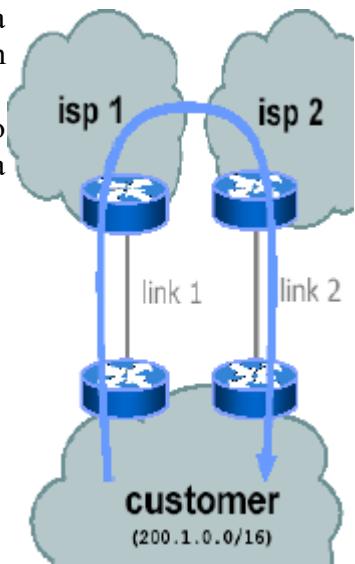
Due link a due providers differenti. In genere, due routers sono coinvolti in modo tale da evitare singoli punti di rottura.



Instradamento

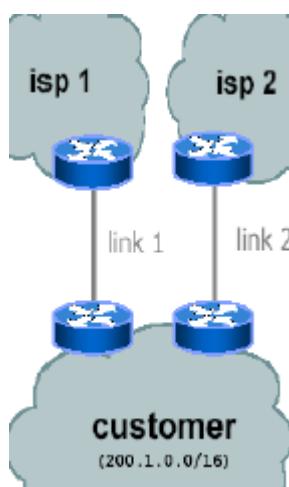
Un pacchetto in uscita può essere inviato attraverso uno dei due link per raggiungere Internet. Un pacchetto in ingresso può usare uno dei due link per raggiungere la rete. Un pacchetto internet può attraversare il link 1 ed il link 2. Un pacchetto interno può attraversare entrambi i link.

Posso usare entrambi i link con ridondanza, e così facendo rendo visibili soltanto le mie reti. Ma può capitare di ricevere annunci da ISP1 e ISP2, quindi la mia rete inizia a fare da tramite.



Il multi-homed usa la partizione di carico:

- **Elimina il traffico in transito**
- **Traffico in uscita:**
Metà degli host interni usano link 1,
l'altra metà usa link 2
- **Traffico in ingresso:**
usa link 1 per raggiungere metà degli host interni
Usa link 2 per l'altra metà

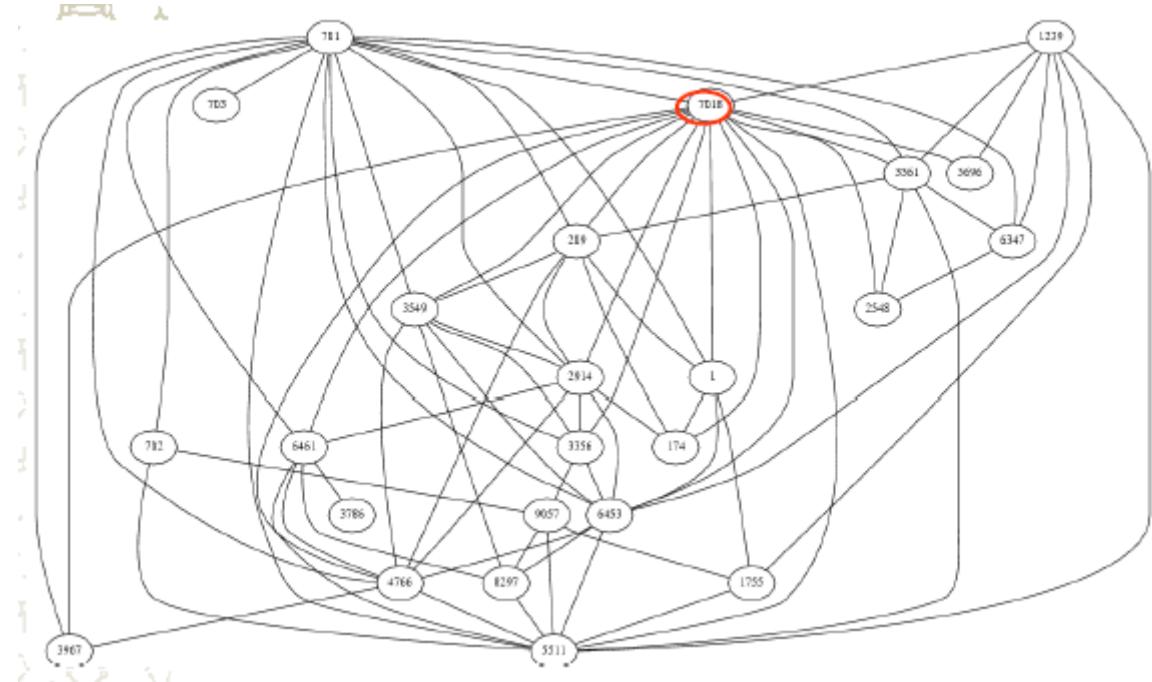


Uso di BGP per il partizionamento

Annuncia /19 aggregato su ogni link

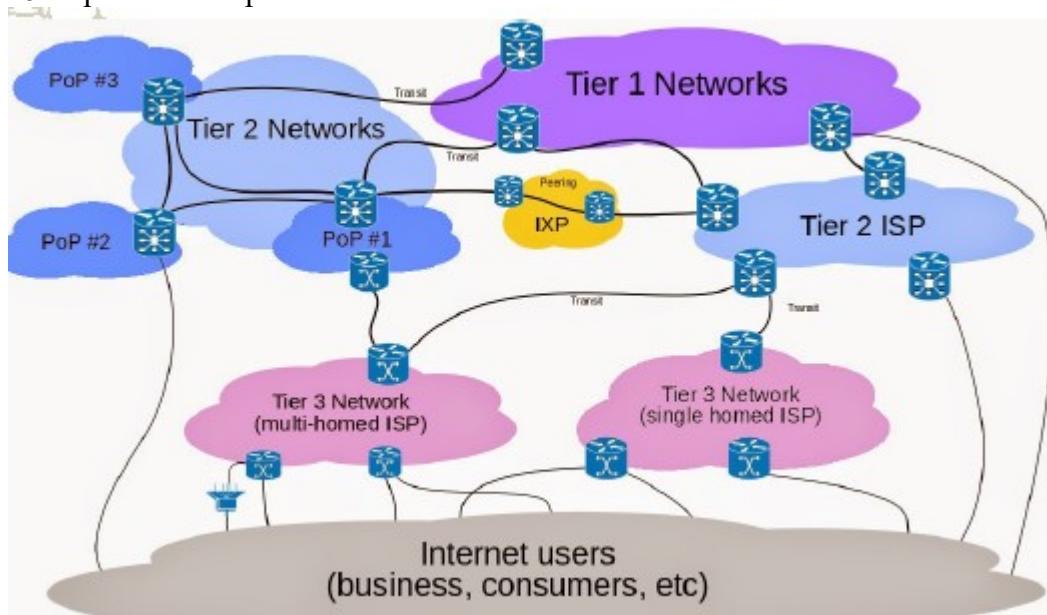
- split /19 e annuncia due /20, uno per ogni link:
 - Partizionamento del traffico approssimato sul traffico in ingresso
 - Assume uguale capacità ed anche distribuzione del traffico sul blocco di indirizzi
- Modifica lo split finchè un partizionamento perfetto è ottenuto
- Accetta l'instradamento di default upstream:
 - Partizionamento del traffico con instradamento verso l'uscita più vicina (igp)
 - Una buona approssimazione poiché molto del traffico è diretto verso la rete

Grafo dell'AS

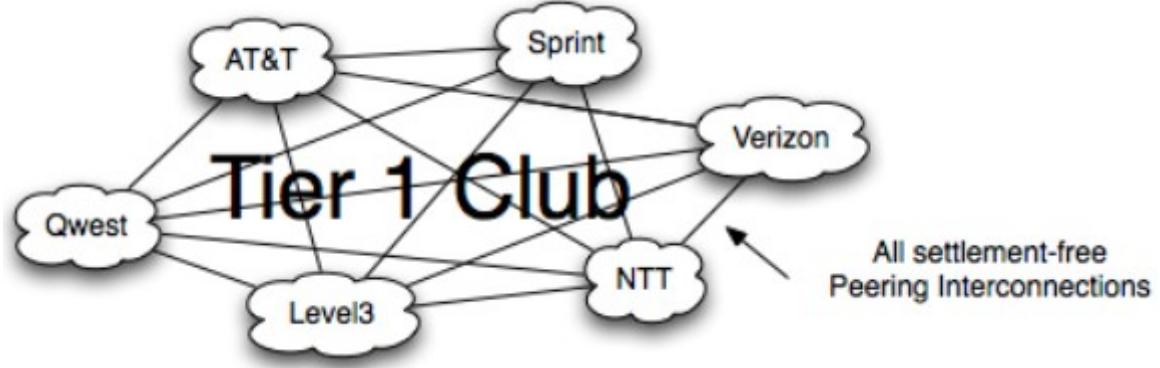


Struttura 3-tiers di internet

- Tier3: providers regionali e reti enterprise
- Tier2: providers a grande copertura
- Tier1: providers di providers



Il club dei Tier 1:



$n*(n-1)$ collegamenti.

Punti di interscambio IX e NAP

- Neutralità
- Scambio del transito fra ISP
- Possibilità di stabilire peering
- LAN che interconnette terminazioni di ogni ISP
- Realizzati a livello 2
- Switch ad altissime prestazioni

Un **Internet Exchange Point (IXP)**, o **punto di interscambio**, detto anche **NAP (Network Access Point)** è un'infrastruttura fisica che permette a diversi Internet Service Provider di scambiare traffico Internet fra loro, interconnettendo i propri Autonomous System attraverso accordi di peering generalmente gratuiti. Questo permette agli ISP di risparmiare una parte della banda che comprano dai loro upstream provider, e di guadagnare in efficienza e in affidabilità.

Funzionamento:

Lo scopo principale di un IXP è di permettere alle reti degli ISP di interconnettersi fra di loro direttamente, attraverso il punto di interscambio, piuttosto che far passare il traffico attraverso uno o più provider esterni. I vantaggi sono i seguenti:

- *Velocità*: la connessione diretta fra due Autonomous System, senza passaggi intermedi, minimizza il tempo di latenza dei pacchetti nell'attraversarli.
- *Efficienza*: la diversificazione delle connessioni che un operatore Internet ha verso il resto degli ISP gli permette di evitare un single point of failure, ovvero un oscuramento da Internet qualora l'unico collegamento (quello con l'upstream provider) venisse meno, aumentando così la ridondanza dell'infrastruttura di rete.
- *Costo*: il costo globale di afferenza ad un IXP (inclusi i costi di setup del collegamento) è generalmente molto minore (per megabit per secondo di banda scambiata) rispetto al costo del transito Internet. Gli accordi di peering tra i partecipanti ad un punto di interscambio sono nella maggior parte dei casi effettuati a titolo gratuito.

Struttura:

L'infrastruttura tipica di un Internet Exchange consiste di uno o più switch (*centri stella*) ai quali vengono collegati i router dei diversi afferenti. Attraverso il protocollo BGP, i router stabiliscono dei peering che permettono agli ISP di scambiarsi il traffico Internet.

La tecnologia di switching più usata nei punti di interscambio è passata da ATM (molto in voga negli anni 1990) ad ethernet.

LIVELLO TRASPORTO

Funzione del livello di trasporto

Il livello di trasporto ha lo scopo di fornire allo strato superiore un servizio di trasferimento dei dati *end to end*, mascherando completamente al livello superiore il fatto che tra i due host terminali esista una rete di qualsiasi tipo, topologia, tecnologia e complessità:

- per OSI lo strato superiore è il livello di sessione
- per TCP/IP lo strato superiore è il livello di applicazione

Per assolvere le sue funzioni lo strato di trasporto utilizza i servizi dello strato di rete.

Servizi

Può essere *con connessione* o *senza connessione*. È disponibile al programmatore delle applicazioni come un insieme di chiamate di procedura disponibili in una libreria. Il trasporto con connessione fornisce un *canale affidabile* su cui scrivere o da cui leggere dati (come un file).

Per il servizio connection oriented si possono elencare in

- **LISSEN**: lo strato superiore notifica al trasporto che è pronto a ricevere una connessione
- **CONNECT**: lo strato superiore chiede allo strato di trasporto di effettuare una connessione (si traduce nell'invio da parte del trasporto di un messaggio "Connection Request" al destinatario)
- **SEND**: lo strato superiore chiede al trasporto di inviare dati
- **RECEIVE**: lo strato superiore chiede allo strato di trasporto di trasmettergli i dati in arrivo
- **DISCONNECT**: lo strato superiore chiede di chiudere la connessione (si traduce nell'invio da parte dello strato di trasporto di un messaggio "Disconnection Request")

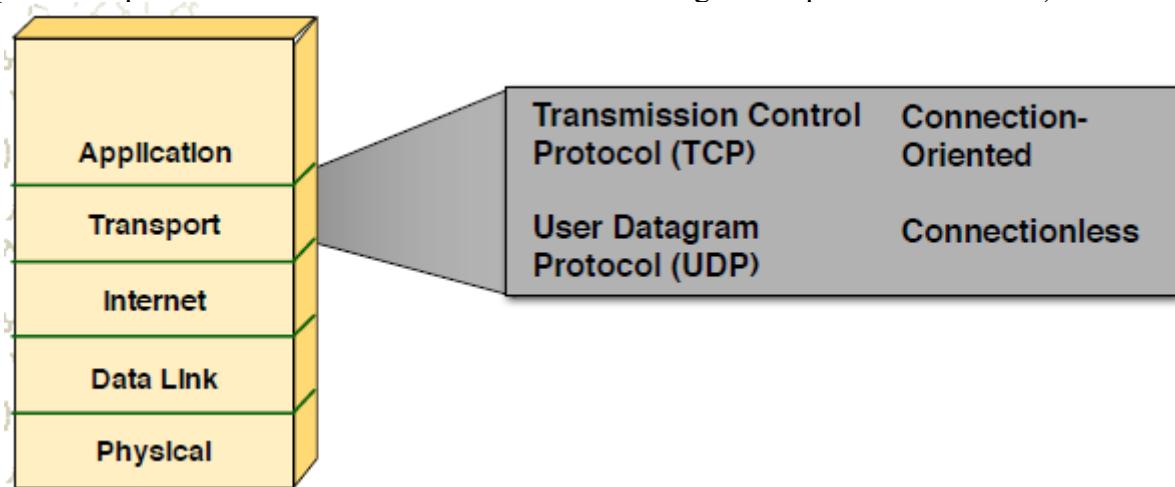
Per il servizio connectionless, le due primitive SEND e RECEIVE possono essere sufficienti.

Protocolli di trasporto

Gestiscono il *controllo degli errori*, i *numeri di sequenza* e il *controllo di flusso* per un collegamento attraverso una rete (situazione più complessa del caso del livello data link).

Occorre definire la modalità di *indirizzamento* a livello trasporto (su uno stesso host possono essere disponibili più connessioni). Viene introdotto il concetto di service port.

In generale il livello di trasporto su un host gestisce numerose connessioni. Il livello di trasporto provvede a multiplare e demultiplare i pacchetti provenienti dal livello di rete sulle diverse connessioni. Devono risolvere il problema della capacità di memorizzazione della rete (un pacchetto può essere memorizzato in un router e consegnato dopo un certo ritardo).



TCP e UDP

Protocolli di trasporto definiti su rete Internet (su IP):

Transmission Control Protocol (TCP) definisce un protocollo di trasporto orientato alla connessione; definito in RFC 793, RFC 1122 e RFC 1323; è progettato per fornire un flusso affidabile end-to-end su una internet inaffidabile

User Data Protocol (UDP) definisce un protocollo senza connessione; descritto in RFC 768 permette di inviare datagram IP senza stabilire una connessione.

Funzionalità del TCP

Trasmissione

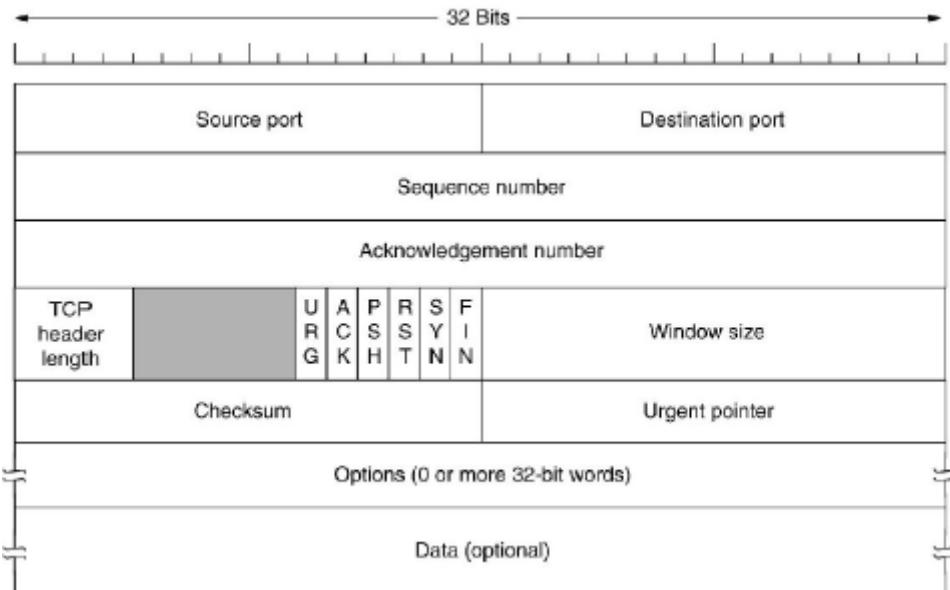
- Riceve un flusso di dati dall'applicazione
- Li organizza in unità lunghe al massimo 64Kb
- Spedisce le unità di dati come datagram IP

Ricezione

- Riceve i datagram IP
- Ricostruisce il flusso di byte originale nella sequenza corretta

Ritrasmissione dei datagram non ricevuti, riordinamento dei datagram arrivati in ordine sbagliato.

Header TCP



Header:

- **source e destination port**: le porte del sorgente e del destinatario, che permettono di identificare le applicazioni a cui sono destinati i dati (16 bit ciascuna)
- **sequence number (32 bit)**: il valore del primo byte trasmesso nel segmento; all'atto della connessione viene stabilito il valore iniziale, basato sul clock del trasmettente
- **acknowledge number (32 bit)**: il valore dell'ultimo byte riscontrato piu' uno (cioe' del successivo atteso)
- **TCP header length (4 bit)**: il numero di gruppi di 32 bit contenuti nella intestazione; necessario perche' sono previsti campi opzionali (non piu' di 60 byte)
- **flag URG (urgent)**: il campo dati contiene dati urgenti, che devono essere passati alla applicazione prima degli altri ancora in attesa nei buffer (ad esempio: il CTRL^C in applicazioni di terminale remoto)
- **flag ACK**: il segmento trasporta un riscontro; tutti i segmenti tranne il primo dovrebbero averlo settato. Ack utilizzato è quello del piggybacking
- **flag PSH (push)**: indica che l'applicativo ha richiesto l'invio dei dati senza ulteriore attesa (ed in ricezione deve essere fatto lo stesso)
- **flag RST (reset)**: utilizzato per comunicare che la connessione deve essere abortita, o quando viene rifiutata una nuova connessione
- **flag SYN (synchronize)**: utilizzato per stabilire una connessione; questi segmenti definiscono il sequence number iniziale per i due versi
- **flag FIN (finish)**: utilizzato per comunicare alla controparte che non si hanno piu' dati da inviare e che si desidera chiudere la connessione; il doppio FIN con relativo riscontro genera il rilascio della connessione
- **window size (16 bit)**: la dimensione in byte dello spazio disponibile dei buffer in ricezione:

il valore massimo e' di 64 KB, le reti moderne molto veloci rendono questo limite inefficiente: e' possibile utilizzare un header opzionale per accordarsi su una window size a 30 bit (buffer fino ad 1 GB)

- **checksum (16 bit):** obbligatoria per TCP (al contrario di UDP); anche in TCP la checksum viene calcolata su tutto il segmento piu' uno pseudo header che riporta gli indirizzi IP di sorgente e destinazione
- **urgent pointer (16 bit):** definisce l'offset dell'ultimo byte facente parte dei dati urgenti quando la flag URG e' settata

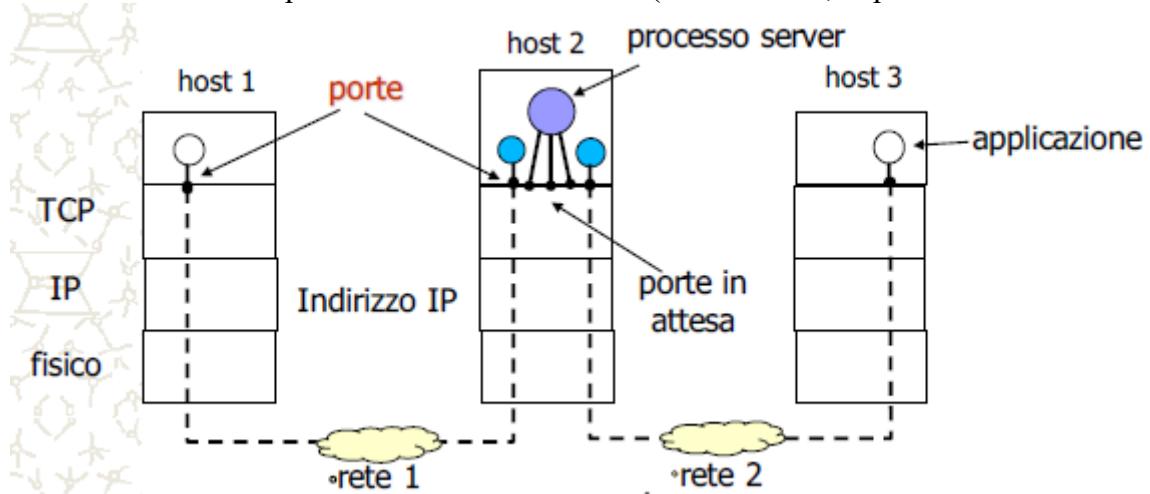
Header opzionali:

Le opzioni sono definite da una lunghezza, un tipo, ed i dati relativi; sono definite diverse opzioni, tra cui:

- **padding:** necessario in presenza di opzioni per rendere il campo header nel suo complesso un multiplo di 32 bit
- **MSS:** utilizzato con i segmenti SYN per determinare il MSS scambiandosi i valori di MTU ed MRU
- **window scale:** utilizzata per definire la dimensione della finestra fino a 30 bit
- **selective acknowledge:** TCP utilizza normalmente il go-back-N; questa opzione permette di utilizzare il selective reject
- **timestamp:** utilizzata per valutare (a livello di trasporto) il round trip time e poter definire valori opportuni per i timer interni

Indirizzamento:

Un indirizzo di trasporto identifica l'host e la specifica connessione sull'host. Le applicazioni che utilizzano il TCP/IP si registrano sullo strato di trasporto ad un indirizzo specifico, detto porta. La porta e' il meccanismo che ha a disposizione una applicazione per identificare l'applicazione remota a cui inviare i dati. La porta e' un numero di 16 bit (da 1 a 65535; la porta 0 non e' utilizzata).



Comunicazione fra TCP/IP stacks

Il **TCP** su un computer usa **IP** e i livelli inferiori per comunicare con il **TCP** di un altro computer.

Le porte:

Le porte attive definiscono i servizi TCP disponibili. Per connettersi ad un servizio specifico su un server si deve conoscere il numero di porta su cui il processo server accetta le connessioni. Esiste una autorita' centrale, lo IANA (Internet Assigned Numbers Authority), che pubblica la raccolta dei numeri di porta assegnati alle applicazioni negli RFC (<http://www.iana.org>).

Le porte inferiori alla 256 sono dette porte ben note (well-known ports) e corrispondono a servizi standard. In Unix la lista dei servizi e delle porte e' nel file /etc/services.

Ad esempio: la porta 21 di TCP corrisponde al servizio FTP (File Transfer Protocol)

la porta 80 di TCP corrisponde al servizio HTTP (Hypertext Transfer Protocol) ovvero al server Web. Un servizio "standard" puo' anche essere attivato su una porta diversa (es. HTTP su 8080).

I numeri delle porte vengono divisi in tre gruppi:

- **Well-Known-Ports (0 – 1023)**: Queste porte vengono assegnate univocamente dall'IANA
- **Registered Ports (1024 – 49151)**: L'uso di queste porte viene registrato a beneficio degli utenti della rete, ma non esistono vincoli restrittivi
- **Dynamic and/or Private Ports (49152 – 65535)**: Non viene applicato nessun controllo all'uso di queste porte

Le porte del client

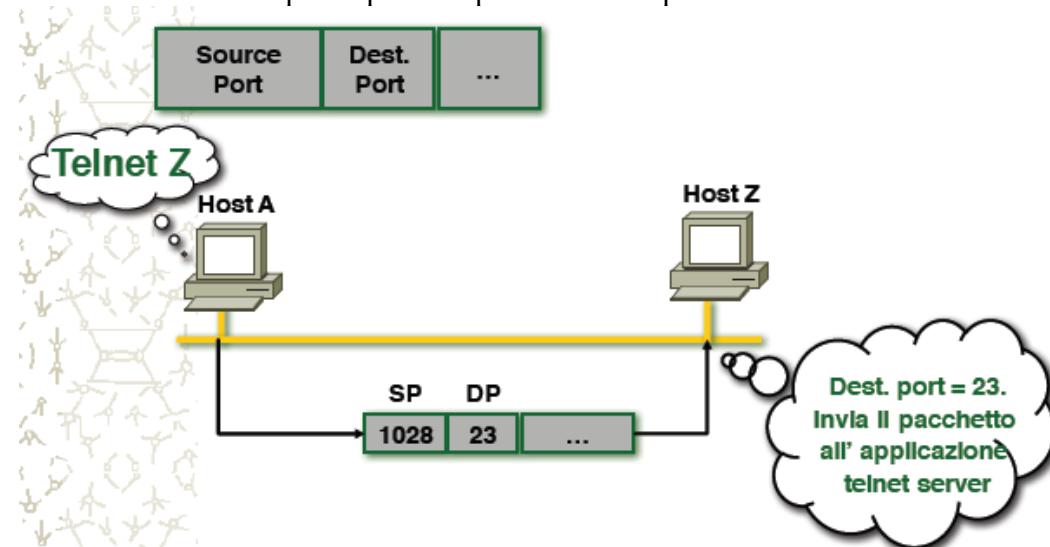
Il client definisce la porta di ogni sua connessione utilizzando numeri in genere elevati e scelti in modo da essere unici sull'host.

Ad esempio:

richiesta di connessione ad un server TELNET:

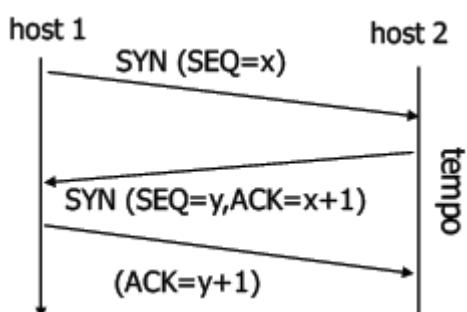
- client port 23443
- server port 23

Le connessioni sono quindi punto-a-punto e full duplex.



Apertura della connessione

Si utilizza un protocollo 3-way handshaking:



Bisogna stabilire una connessione end-to-end su entrambe le macchine. L'host 1 manda una prima sequenza di sincronizzazione mandando il proprio sequence number (seq = x). L'host 2 risponderà con un riscontro della richiesta di sincronizzazione, e manda il proprio sequence number (seq = y, ack = x + 1). La host 1 manda un riscontro dell sequence number dell'host 2 (ack = y + 1).

Se il TCP ricevente non verifica la presenza di nessun processo in attesa sulla porta destinazione manda un segmento di rifiuto della connessione (RST).

Un esempio di connessione

Connessione Telnet fra da 10.6.1.9 a 10.6.1.2 catturata con tcpdump *

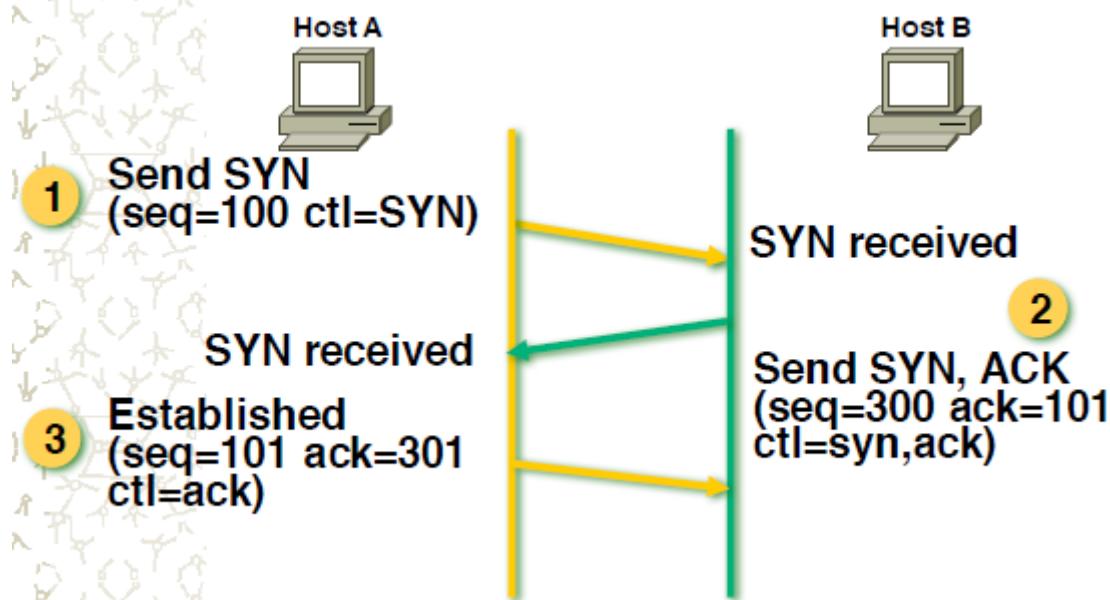
porta client 4548 - porta server 23 (telnet)

```
10.6.1.9.4548 > 10.6.1.2.23: S 2115515278:2115515278 (0) win 32120
<mss 1460,nop,nop,sackOK,nop,wscale 0> (DF)

10.6.1.2.23 > 10.6.1.9.4548: S 1220480853:1220480853 (0)
ack 2115515279 win 32120 <mss 1460,nop,nop,sackOK,nop,wscale 0>
(DF)

10.6.1.9.4548 > 10.6.1.2.23: . ack 1220480854 win 32120 (DF)

* tcpdump -S -n -t \(dst 10.6.1.2 and src 10.6.1.9\) or \(
dst 10.6.1.9 and src 10.6.1.2\)
```

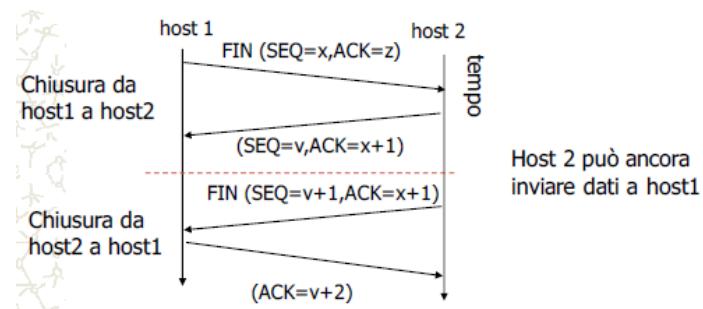


Chiusura della connessione

La connessione è full-duplex e le due direzioni devono essere chiuse indipendentemente.

L'host 1 manda un segnale con bit di FIN con un sequence number e un ack dell'ultimo frame ricevuto (FIN(SEQ = x, ACK = z)). L'host 2 manda un sequence number e un ack del frame appena ricevuto (Seq = v, Ack = x + 1), la connessione viene chiusa da host 1 a host 2. Ora l'host 2 invia un bit di fin in cui manda il suo sequence number e l'ack dell'ultimo frame ricevuto (FIN (SEQ = v+1, ACK = X+1)). L'host 1 manda un ack del frame ricevuto (ACK = v + 2), la connessione è chiusa anche da host 2 a host 1.

Se l'ack di un messaggio FIN si perde l'host mittente chiude comunque la connessione dopo un timeout.



Esempio di chiusura

Chiusura Telnet da 10.6.1.9

porta client 4548 - porta server 23 (telnet)

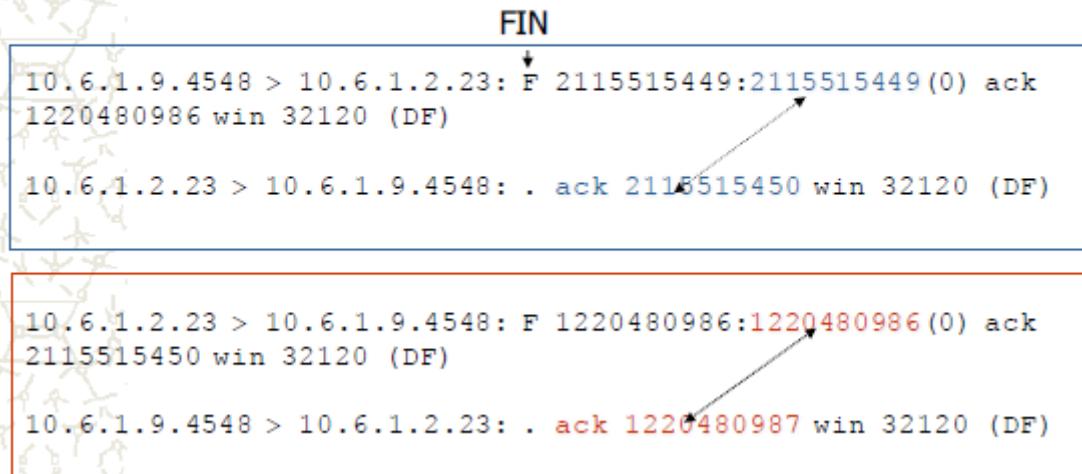
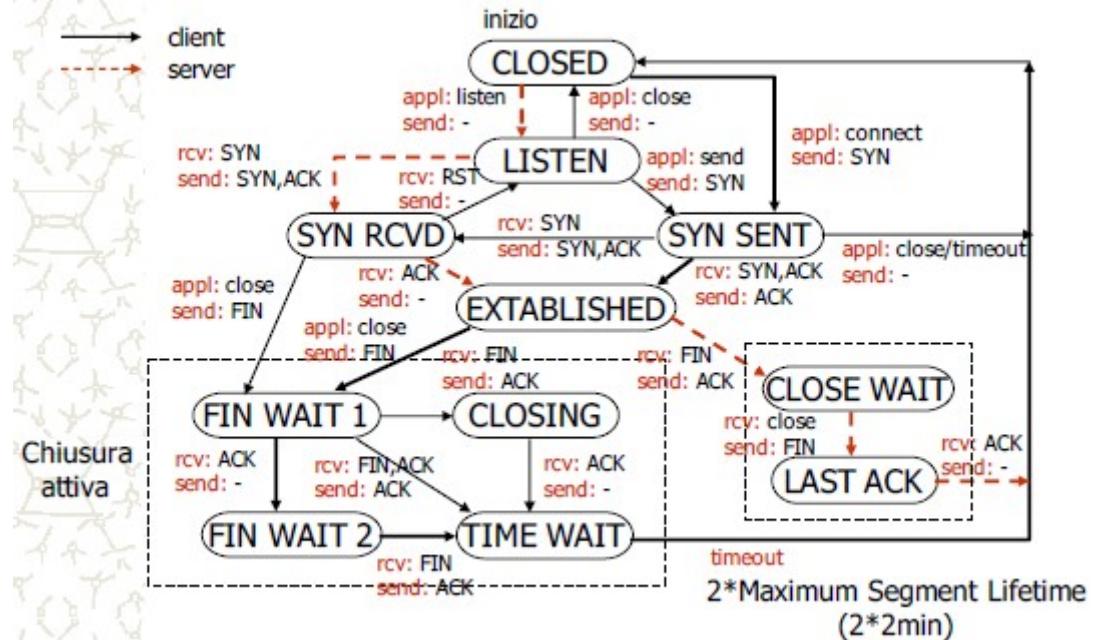


Diagramma degli stati TCP



Il timeout MSL

Il **Maximum Segment Lifetime** (MSL=2 min in RFC 793) indica il massimo tempo per il quale un segmento TCP può sopravvivere nella rete prima di essere scartato. Attendere 2MSL nello stato TIME WAIT garantisce che tutti i segmenti relativi alla connessione siano spariti dalla rete. Nello stato TIME WAIT si impedisce che nel client possa aprirsi una connessione con lo stesso indirizzo di quella appena chiusa (porta+IP). Il vincolo più rigido in molte implementazioni è che non venga riusato il numero di porta locale (non è comunque un problema). Per il server questo non avviene (la porta essendo pubblicata deve rimanere attiva).

Flusso di dati interattivi

Si considera il caso di una connessione interattiva (es. telnet):

- Non si possono accumulare i dati ma occorre inviare segmenti piccoli
- Il 90% dei segmenti telnet porta circa 10 byte

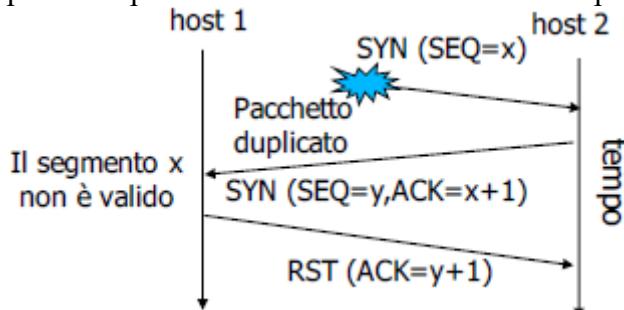
Nel caso limite si ha un segmento per ogni carattere battuto con il ricevente che genera un echo del medesimo carattere:

- Segmento dal client col carattere battuto ($26\text{IP} + 20\text{TCP} + 1\text{byte} = 47\text{byte}$)
- Segmento di ack dal server al client (46 byte)
- Segmento di echo dal server (47 byte)
- Segmento di ack dal client (46 byte)

In totale si userebbero 186 byte in 4 segmenti TCP per 1 carattere!!

Caso duplicazione dei pacchetti

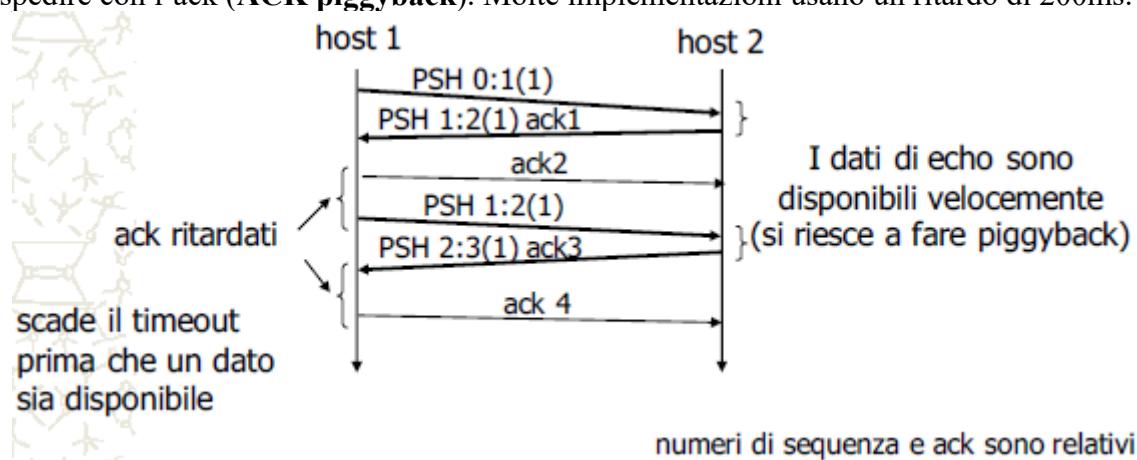
I pacchetti possono essere memorizzati e ricomparire nella rete



La numerazione iniziale è fatta con un orologio locale (tick=4 ms). L'intervallo dei numeri di sequenza (32 bit) garantisce che non venga riutilizzato lo stesso numero prima di qualche ora. A causa del **time to live** dei pacchetti IP segmenti con lo stesso numero non possono coesistere sulla rete.

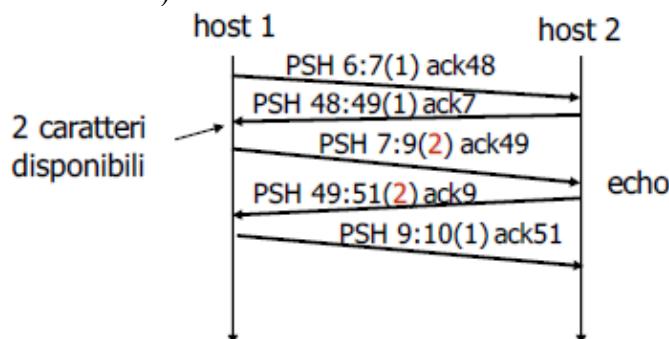
ACK ritardati

Normalmente il TCP non invia un ack istantaneamente ma ritarda l'invio sperando di avere dati da spedire con l'ack (**ACK piggyback**). Molte implementazioni usano un ritardo di 200ms.

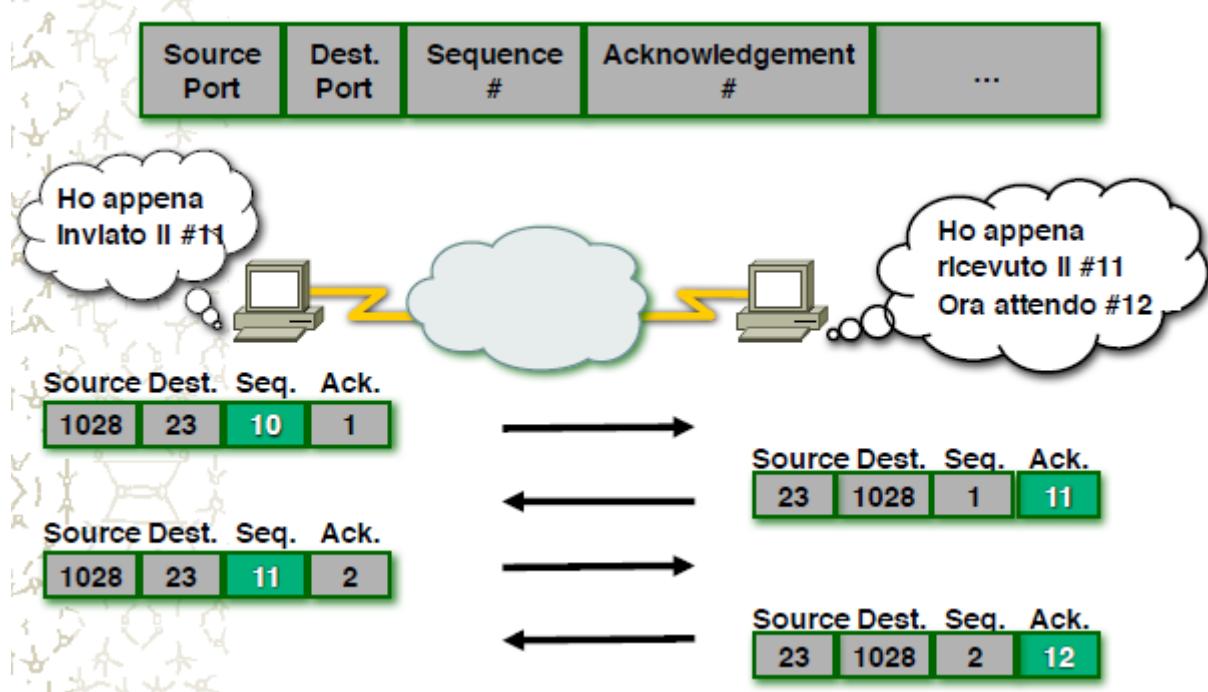


L'algoritmo di Nagle (1984)

Ha effetto per connessioni lente (es. WAN) - attesa ack. Si accumulano i dati fino a che non si riceve l'ack per il segmento inviato in precedenza. In alcuni casi deve essere disabilitato (es. mouse in Xwindows).

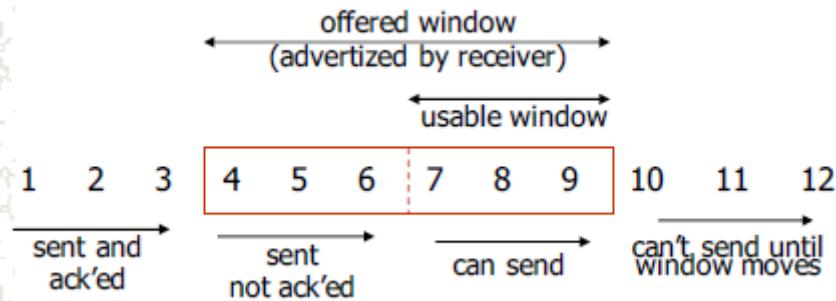


Sequence e Ack numbers

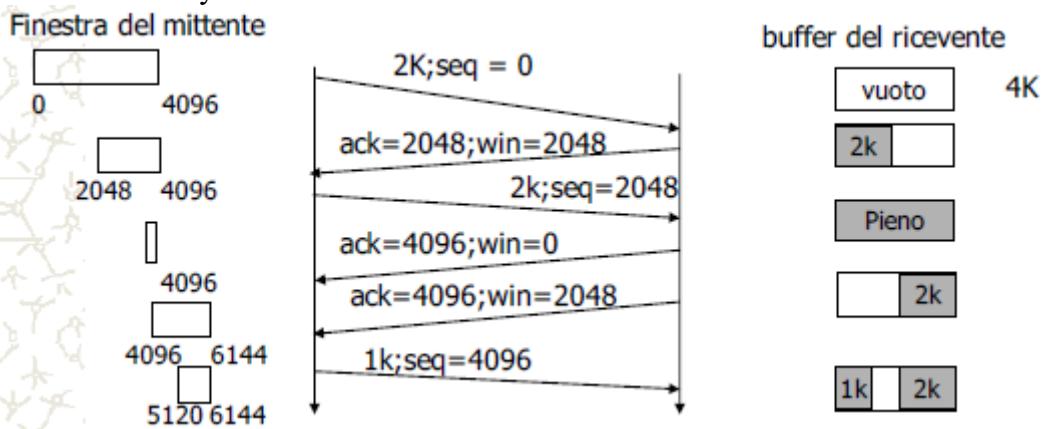


Trasmissione di flussi di dati

Viene utilizzato un protocollo a finestra scorrevole (sliding window). Il ricevente indica la dimensione della finestra che può gestire in un dato momento:

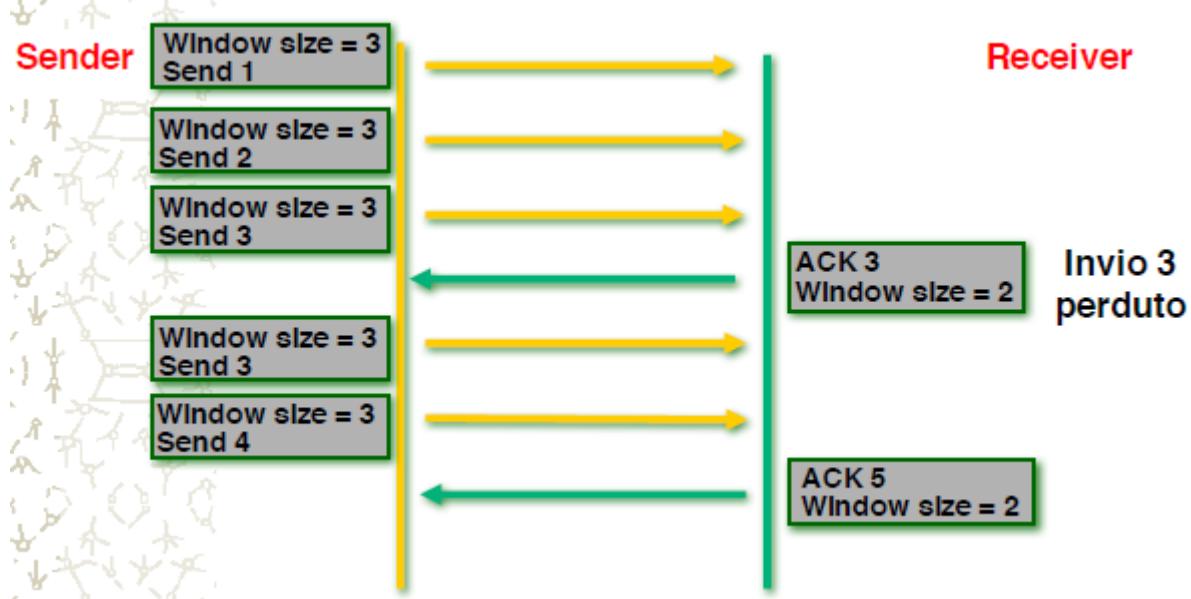


La finestra di dati trasmissibili ancora senza aspettare l'ack è ottenuta dall'ampiezza della finestra e dal numero dell'ultimo byte ricevuto.



Se il ricevente indica una finestra 0 il mittente non può trasmettere dati. Il mittente può inviare un segmento di un byte per forzare il destinatario a indicare il prossimo byte atteso e l'ampiezza della finestra (per non rimanere in attesa infinita se si perdono pacchetti) - **timer di persistenza**

Windowing



Il sendere invia con una finestra di dimensione 3, il receiver invia un Ack= 3 e dice che la sua finestra è di dimensione 2, il sendere quindi reinvia il bit 3 e invia anche un bit quattro, il receiver manda un ack a 5 per dire che tutto è andato bene.

TCP timeout e ritrasmissione

TCP utilizza un timeout di attesa dell'ack dopo di che provvede alla ritrasmissione dei dati. Il problema è determinare il valore del timeout migliore in quanto i ritardi possono essere molto variabili nel tempo sulla rete:

- Se il timeout è troppo piccolo si fanno ritrasmissioni inutili
- Se il timeout è troppo elevato si avranno ritardi di trasmissione

Si utilizza un algoritmo di stima del migliore timeout basato sulla misura del **Round-Trip Time** (RTT).

Stima del timeout

Per ogni connessione si tiene una stima di RTT, aggiornandola per ogni pacchetto con

$$RTT_i = \sqrt{RTT_{i-1}} + (1 - \sqrt{ }) T_{rtt}(pkt_i)$$

Si stima poi la deviazione media

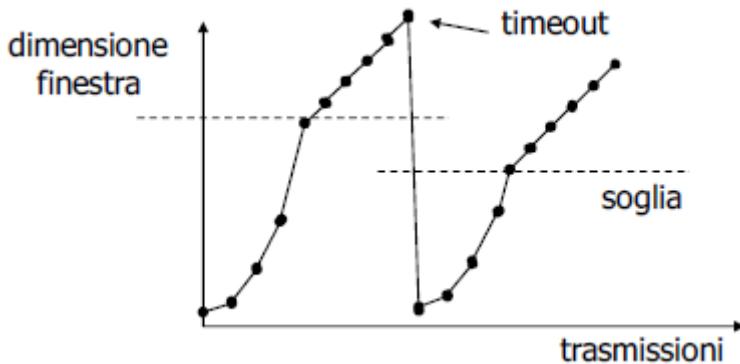
$$D_i = \sqrt{D_{i-1}} + (1 - \sqrt{ }) |RTT_i - T_{rtt}(pkt_i)|$$

E si sceglie

$$\text{timeout} = RTT + 4 * D$$

Controllo di congestione

Il TCP adatta la velocità di trasmissione alla capacità della rete utilizzando una finestra di congestione che ha la stessa funzionalità della finestra di trasmissione usata per il ricevente. La dimensione della finestra di congestione è ridotta se scade il timeout di ritrasmissione.



UDP (User Datagram Protocol)

UDP implementa un servizio di consegna inaffidabile dei dati a destinazione. UDP riceve i dati dalla applicazione e vi aggiunge un header di 8 byte, costruendo così il segmento da inviare.

L'applicazione specifica (l'indirizzo di rete e) la porta di destinazione, ed in ricezione UDP recapita il campo dati al destinatario. UDP non si preoccupa di sapere nulla sul destino del segmento inviato, ne' comunica alla applicazione qualsiasi informazione. Di fatto costituisce semplicemente una interfaccia ad IP (che fornisce lo stesso tipo di servizio), con l'aggiunta di fare multiplexing del traffico delle applicazioni su IP:

- tramite il meccanismo delle porte a cui sono associate le applicazioni, di fatto UDP realizza un multiplexing dei dati delle diverse applicazioni su IP.

Orientato al datagramma

A differenza di TCP, UDP si occupa di un datagramma per volta:

- quando una applicazione passa dati ad UDP, UDP li maneggia in un unico segmento, senza suddividerlo in pezzi
- il segmento di massime dimensioni che UDP puo' gestire deve stare interamente nel campo dati del pacchetto IP
- il segmento viene passato ad IP che eventualmente lo frammenta, ma a destinazione UDP ricevera' il datagramma intero
- l'applicazione di destinazione ricevera' quindi il blocco completo di dati inviato dalla applicazione che li ha trasmessi

Il segmento UDP

Il segmento UDP e' costituito da un header di lunghezza fissata (8 byte) piu' il campo dati, che deve avere dimensione massima tale da stare dentro il campo dati di IP:

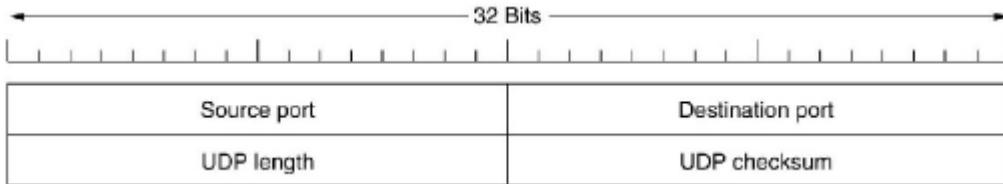
- poiche' il pacchetto IP puo' essere lungo 65535 byte, il campo dati UDP puo' essere lungo al massimo ($65535 - 8 - \text{lunghezza header IP}$) byte.

Header UDP

L'header e' costituito da quattro campi di due byte:

- **source e destination port:** le porte di associazione alle applicazioni mittente e destinataria dei dati
- **length:** lunghezza del segmento in byte (compreso l'header)
- **checksum:** questo campo contiene una checksum del segmento completo (anz: viene aggiunto uno pseudo-header con le informazioni degli indirizzi IP di sorgente e destinazione):

- l'utilizzo del campo checksum e' opzionale, e l'applicativo puo' decidere di non utilizzarlo (in questo caso il campo e' riempito con zeri)
- molti applicativi non lo utilizzano per motivi di efficienza
- se viene utilizzato, un errore provoca la rimozione del segmento senza che vengano prese altre iniziative.



Caratteristiche di UDP

Benché inaffidabile, UDP ha caratteristiche che per molte applicazioni sono appetibili:

- puo' utilizzare trasmissione multicast o broadcast. TCP e' un protocollo orientato alla connessione, quindi per definizione non puo' gestire una comunicazione tra piu' di due entita'.

È molto leggero, quindi efficiente.

- la dimensione ridotta dell'header impone un overhead minimo, ed una rapidita' di elaborazione elevata
- la mancanza di meccanismi di controllo rende ancora piu' rapida l'elaborazione del segmento ed il recapito dei dati

Applicativi che utilizzano UDP

- Applicativi che necessitano di trasmissioni broadcast
- Applicativi per i quali la perdita di una porzione di dati non e' essenziale, ma richiedono un protocollo rapido e leggero: stream voce/video
- Applicativi che si scambiano messaggi (e non flussi di byte) di piccole dimensioni, e che non risentono della perdita di un messaggio:
 - interrogazione di database
 - sincronizzazione oraria
 - in questi casi la perdita della richiesta e della risposta provoca un nuovo tentativo di interrogazione
- Applicativi che necessitano di risparmiare l'overhead temporale provocato dalla connessione, ed implementano a livello di applicazione il controllo della correttezza dei dati:
 - ad esempio applicativi che scambiano dati con molti host, rapidamente, per i quali dover stabilire ogni volta una connessione e' peggio che ritentare se qualcosa va storto.

Applicativi standard su UDP

Sono molti, ed in aumento. Gli applicativi che storicamente utilizzano UDP sono:

- DNS, sulla porta 53
- TFTP (Trivial File Transfer Protocol), sulla porta 69
- NetBIOS Name Service (anche WINS) sulla porta 137
- SNMP (Simple Network Management Protocol) sulla porta 161
- NTP (Network Time Protocol) sulla porta 123
- NFS (Network File System) via portmap

LIVELLO APPLICATIVO

Gli strati sotto lo strato applicazione forniscono il trasporto affidabile, ma non svolgono alcun lavoro per gli utenti. Tuttavia, anche nello strato applicazione c'è l'esigenza dei protocolli di supporto che permettono alle applicazioni di funzionare. Uno di questi protocolli è il DNS, che gestisce i nomi all'interno di Internet .

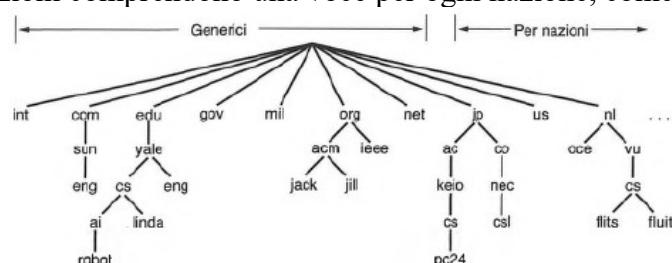
DNS: il sistema dei nomi di dominio

Anche se i programmi possono teoricamente fare riferimento a host, caselle di posta e altre risorse tramite i loro indirizzi di rete (per esempio IP), le persone ricordano con difficoltà questi indirizzi. Inoltre, inviare un messaggio di posta elettronica a *tana@128.111.24.41* significa che se l'ISP o l'organizzazione di Tana sposta il server di posta su una macchina con un indirizzo IP diverso, anche l'indirizzo di posta elettronica deve cambiare. Per questi motivi sono stati introdotti nomi ASCII per separare i nomi dei computer dai rispettivi indirizzi, e in questo modo l'indirizzo di Tana potrebbe essere simile a *tana@art.ucsbs.edu*. Ciò nonostante, la rete in sé sa interpretare solo indirizzi numerici, pertanto sono richiesti meccanismi per convertire le stringhe ASCII in indirizzi di rete. Ai tempi di ARPANET esisteva solamente un file, *host.txt*, che elencava tutti gli host e i loro indirizzi IP. Ogni notte, tutti gli host lo prelevavano dal sito in cui era mantenuto. Per una rete composta da poche centinaia di grandi computer che lavoravano in timesharing questo approccio funzionava abbastanza bene, con l'aumentare delle connessioni si capì che questo sistema non poteva più funzionare, perché da una parte la dimensione del file sarebbe cresciuta sempre di più, inoltre c'era il rischio di avere conflitti tra i vari nomi degli host. Per risolvere questi problemi fu inventato **DNS** (*Domain Name System*, sistema dei nomi di dominio). L'essenza di DNS è l'invenzione di uno schema di denominazione gerarchico basato su dominio, e di un sistema di database distribuito per l'implementazione di questo schema di denominazione. È principalmente utilizzato per associare nomi di host e destinazioni di posta elettronica agli indirizzi IP, ma può essere utilizzato anche per altri scopi. DNS è definito in RFC 1034 e 1035. In breve, DNS viene utilizzato come segue. Per associare un nome a un indirizzo IP, un programma applicativo chiama una procedura di libreria chiamata **risolutore**, passando il nome come parametro. Il risolutore invia un pacchetto UDP a un server DNS locale, che quindi cerca il nome e restituisce l'indirizzo IP al risolutore, che a sua volta lo restituisce al chiamante. Armato dell'indirizzo IP, il programma può quindi stabilire una connessione TCP con la destinazione oppure inviarle pacchetti UDP.

Lo spazio dei nomi DNS

Concettualmente, Internet è divisa in oltre 200 **domini** di primo livello, dove ogni dominio copre molti host. Ogni dominio è partizionato in sottodomini, che sono a loro volta divisi e così via. Tutti questi domini possono essere rappresentati con una struttura ad albero. Le foglie rappresentano i domini che non hanno sottodomini (ma naturalmente contengono computer). Un dominio foglia può contenere un singolo host, o può rappresentare una società e contenere migliaia di host. I domini di primo livello sono di due tipi: generici e per nazioni.

- domini generici originali erano *com* (commerciale), *edu* (istituzioni educative), *gov* (governo federale degli Stati Uniti), *int* (organizzazioni internazionali selezionate), *mil* (forze armate statunitensi), *net* (provider di rete) e *org* (organizzazioni senza scopo di lucro).
 - I domini per nazioni comprendono una voce per ogni nazione, come definito in ISO 3166.



Nel novembre del 2000, ICANN ha approvato quattro nuovi domini di primo livello generici, vale a dire *biz* (business), *info* (informazioni), *name* (nomi delle persone) e *pro* (professioni, come medici e avvocati). Inoltre, su richiesta di alcune industrie sono stati introdotti tre domini di primo livello più specializzati. Si tratta di *aero* (industria aero- spaziale), *coop* (cooperative) e *museum* (musei). In generale, ottenere un dominio di secondo livello come *nomesocietà.com* è più facile. E necessario solamente contattare un *registrar* (autorità di registrazione dei domini) per il dominio di primo livello corrispondente (*com* in questo caso), per controllare se il nome desiderato è disponibile e se altri non possiedono il marchio. Se non vi sono problemi, il richiedente paga una tariffa annuale e ottiene il nome. Per ora, quasi ogni parola inglese è stata utilizzata per il dominio *com*. Ogni dominio è denominato dal percorso compreso tra esso e la radice (non denominata). I componenti sono separati da punti (a volte pronunciati “dot”), di conseguenza il reparto ingegneristico di Sun Microsystems potrebbe utilizzare *eng.sun.com.*, piuttosto che un nome in stile UNIX come */com/sun/eng*. Occorre notare che questa denominazione gerarchica garantisce che *eng.sun.com.* non è in conflitto con un potenziale utilizzo di *eng* in *eng.yale.edu.*, che potrebbe essere utilizzato dal dipartimento di lingua inglese di Yale.

I nomi di dominio possono essere assoluti o relativi:

- Un nome di dominio assoluto termina sempre con un punto (per esempio *eng.sun.com.*), al contrario di un nome relativo.
- I nomi relativi devono essere interpretati in un contesto per determinarne univocamente il reale significato.

In entrambi i casi, il dominio fa riferimento a un nodo specifico nella struttura e a tutti i nodi sottostanti.

I nomi di dominio sono *case insensitive*, pertanto *edu*, *Edu* ed *EDU* indicano la stessa cosa. I componenti del nome possono essere lunghi fino a 63 caratteri, mentre il percorso completo non deve superare 255 caratteri.

In teoria i domini possono essere inseriti nella struttura in due modi diversi. Per esempio, *cs.yale.edu* poteva essere elencato sotto il dominio per nazioni *us* come *cs.yale.ct.us*. In pratica, però, la maggior parte delle organizzazioni negli Stati Uniti utilizza un nome generico, mentre la maggior parte di quelle esterne agli Stati Uniti sceglie il dominio della sua nazione. Non esistono regole per la registrazione in due domini di primo livello, ma ben poche società lo fanno (a eccezione delle multinazionali, per esempio *sony.com* e *sony.nl*).

I record delle risorse

A ogni dominio, che sia rappresentato da un singolo host o sia un dominio di primo livello, può essere associato un insieme di **resource records** (record delle risorse).

Per un singolo host, il record delle risorse più comune è solo l'indirizzo IP, ma possono esistere molti altri tipi di record delle risorse. Quando un risolutore fornisce un nome di dominio a DNS, ciò che ottiene sono i record delle risorse associati a tale nome. Di conseguenza, la funzione principale di DNS è associare i nomi di dominio ai record delle risorse.

Un record delle risorse è una quintupla. Anche se sono codificati in binario per efficienza, nella maggior parte delle esposizioni i record delle risorse sono presentati come testo ASCII, una riga per ciascun record delle risorse. Il formato che useremo è il seguente: Domain_name Time_toJive Class Type Value.

- *Domainjame* indica il dominio a cui si riferisce il record. Normalmente esistono molti record per ogni dominio, e ogni copia del database contiene informazioni su più domini. Questo campo è pertanto la prima chiave di ricerca utilizzata per soddisfare le interrogazioni. L'ordine dei record nel database non è significativo.
- Il campo *timejoive* offre un indicatore della stabilità del record. Alle informazioni altamente stabili viene assegnato un valore elevato, come 86.400 (il numero di secondi in un giorno). Alle informazioni di breve durata viene invece assegnato un valore piccolo, come 60 (1 minuto). Torneremo su questo punto in seguito quando parleremo del caching.
- Il terzo campo di ogni record delle risorse è *class*. Per le informazioni Internet è sempre *IN*.

per altre informazioni non Internet possono essere utilizzati altri codici, che in pratica però sono utilizzati raramente.

- Il campo *type* specifica il tipo di record. I tipi più importanti sono elencati di seguito:

Tipo	Nome	Significato	Valore
SOA	Start of Authority	Fonte dell'autorità	I parametri per questa zona
A	IP address of a host	Indirizzo IP di un host	Intero a 32 bit
MX	Mail exchange	Scambio di posta	La priorità e il nome con cui il dominio desidera accettare la posta elettronica
NS	Name Server	Server dei nomi	Il nome del server per questo dominio
CNAME	Canonical name	Nome canonico	Il nome di dominio
PTR	Pointer	Puntatore	L'alias per un indirizzo IP
HINFO	Host description	Descrizione dell'host	La CPU e l'OS in ASCII
TXT	Text	Testo	Testo ASCII non interpretato

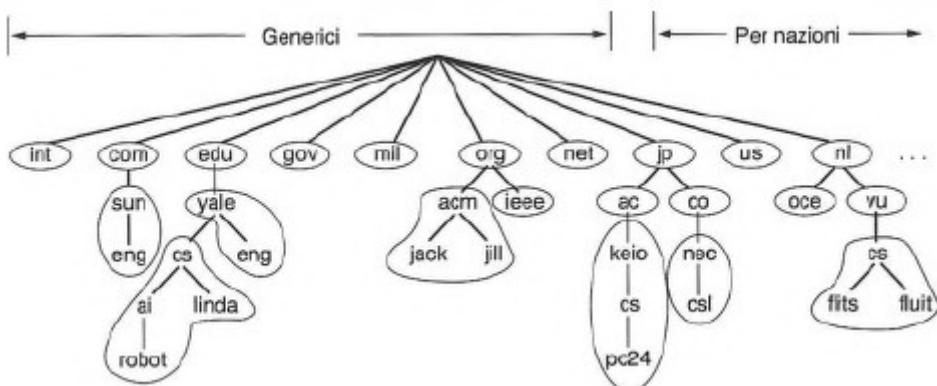
- Un record *SOA* fornisce il nome della fonte primaria di informazioni sulla zona del server dei nomi (descritta in seguito), l'indirizzo di posta elettronica del suo amministratore, un numero di serie univoco e diversi flag e timeout.
- Il tipo di record più importante è il record *A* (*Address*). Contiene l'indirizzo IP a 32 bit di un qualche host. Ogni host Internet deve avere almeno un indirizzo IP affinché le altre macchine possano comunicare con esso. Alcuni host presentano due o più connessioni di rete, e in questo caso possiedono un record delle risorse di tipo *A* per ciascuna connessione di rete.
- Un altro tipo di record importante è il record *MX*. Specifica il nome dell'host configurato per accettare la posta elettronica per il dominio specificato. È utilizzato perché non tutte le macchine sono capaci di accettare la posta elettronica. Se qualcuno desidera inviare messaggi a *bill@microsoft.com*, per esempio, l'host di invio deve trovare un server di posta in *microsoft.com* che desidera accettare la posta elettronica. Il record *MX* può fornire queste informazioni.
- Il record *NS* specifica i server dei nomi.
- I record *CNAME* consentono la creazione di alias.
- Il record *PTR* come *CNAME* punta verso un'altro nome, tuttavia, a differenza di *CNAME* che è soltanto una definizione macro, *PTR* è un tipo di dati DNS regolare la cui interpretazione dipende dal contesto in cui viene trovata. In pratica, è quasi sempre utilizzato per associare un nome a un indirizzo IP per consentire le ricerche che forniscono gli indirizzi IP e restituiscono i nomi delle macchine corrispondenti. Sono chiamate **reverse lookups** (ricerche inverse).
- I record *HINFO* consentono alle persone di scoprire a quale tipo di macchina e sistema operativo corrisponde un dominio.
- I record *TXT* consentono ai domini di identificare sé stessi in modo arbitrario.
- Per finire è disponibile il campo *value*, che può essere un numero, un nome di dominio o una stringa ASCII. La semantica dipende dal tipo di record. Una breve descrizione dei campi *value* per ognuno dei tipi principali di record è data dalla seguente figura:

```
; Dati autorevoli per cs.vu.nl
cs.vu.nl.      86400   IN    SOA     star boss (9527,7200,7200,241920,86400)
                86400   IN    TXT    "Divisie Wiskunde en Informatica."
                86400   IN    TXT    "Vrije Universiteit Amsterdam."
                86400   IN    MX     1 zephyr.cs.vu.nl.
                86400   IN    MX     2 top.cs.vu.nl.
```

flits.cs.vu.nl.	86400	IN	HINFO	Sun Unix
flits.cs.vu.nl.	86400	IN	A	130.37.16.112
flits.cs.vu.nl.	86400	IN	A	192.31.231.165
flits.cs.vu.nl.	86400	IN	MX	1 flits.cs.vu.nl.
flits.cs.vu.nl.	86400	IN	MX	2 zephyr.cs.vu.nl.
flits.cs.vu.nl.	86400	IN	MX	3 top.cs.vu.nl.
www.cs.vu.nl.	86400	IN	CNAME	star.cs.vu.nl
ftp.cs.vu.nl.	86400	IN	CNAME	zephyr.cs.vu.nl
rowboat		IN	A	130.37.56.201
		IN	MX	1 rowboat
		IN	MX	2 zephyr
		IN	HINFO	Sun Unix
little-sister		IN	A	130.37.62.23
		IN	HINFO	Mac MacOS
laserjet		IN	A	192.31.231.216
		IN	HINFO	"HP Laserjet IISI" Proprietary

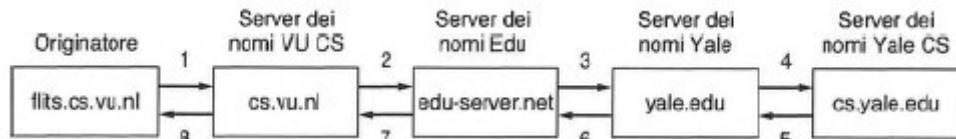
Il server dei nomi

In teoria, un singolo server dei nomi potrebbe contenere l'intero database DNS e rispondere a tutte le interrogazioni. In pratica, questo server sarebbe troppo sovraccaricato per essere utile. Inoltre, se dovesse incontrare un problema, l'intera Internet sarebbe bloccata. Per evitare i problemi associati alla disponibilità di una singola fonte di informazioni, lo spazio dei nomi DNS viene diviso in **zone** non sovrapposte. Un modo per dividere lo spazio dei nomi è mostrato nella figura seguente:



Ogni zona contiene alcune parti della struttura, e contiene anche i server dei nomi con le informazioni su tale zona. Di norma, una zona avrà un server dei nomi primario, che ottiene le sue informazioni da un file su disco, e uno o più server dei nomi secondari, che ottengono le loro informazioni dal server dei nomi primario. Per migliorare l'affidabilità, alcuni server per una zona possono essere situati all'esterno della zona. La posizione dei confini di zona all'interno di una zona è una scelta lasciata all'amministratore. La decisione viene presa in gran parte sulla base del numero di server dei nomi desiderati e della loro posizione.

Quando un risolutore ha un'interrogazione su un nome di dominio, passa l'interrogazione a uno dei server dei nomi locali. Se il dominio è all'interno della giurisdizione del server dei nomi (come *ai.cs.yale.edu* che ricade in *cs.yale.edu*), restituisce i record autorevoli delle risorse. Un **record autorevole** è un record fornito dall'autorità che gestisce il record, ed è pertanto sempre corretto. I record autorevoli si contrappongono ai record archiviati nella cache, che potrebbero non essere aggiornati. Se invece il dominio è remoto e non sono disponibili localmente informazioni su di esso, il server dei nomi invia un messaggio d'interrogazione al server dei nomi di primo livello per il dominio richiesto.



Per chiarire il processo spiegamo la figura sopra riportata:

Un risolutore su *flits.cs.vu.nl* desidera conoscere l'indirizzo IP dell'host *linda.cs.yale.edu*. Nel passaggio 1, invia un'interrogazione al server dei nomi locale, *cs.vu.nl*. Questa interrogazione contiene il nome di dominio, il tipo (A) e la classe (IN). Si supponga che il server dei nomi locale non abbia mai fatto un'interrogazione su questo dominio e di conseguenza non conosca nulla di esso. Potrebbe chiedere ad altri server dei nomi vicini, ma se nessuno di essi possiede informazioni deve inviare un pacchetto UDP al server per *edu* indicato nel suo database (Figura 7.5), *edu-server.net*. È improbabile che questo server conosca l'indirizzo di *linda.cs.yale.edu*, e probabilmente non conosce nemmeno *cs.yale.edu*, ma deve conoscere tutti i suoi figli, pertanto inoltra la richiesta al server dei nomi per *yale.edu* (passaggio 3). A sua volta, questo inoltra la richiesta a *cs.yale.edu* (passaggio 4), che deve disporre dei record autorevoli delle risorse. Visto che ogni richiesta proviene dal client per un server, il record delle risorse richiesto percorre la sua strada tornando indietro nei passaggi da 5 a 8. Quando i record vengono consegnati al server dei nomi *cs.vu.nl* sono inseriti in una cache locale, nel caso fossero necessari in seguito. Tuttavia, queste informazioni non sono autorevoli, perché le modifiche apportate a *cs.yale.edu* non saranno propagate in tutte le cache del mondo conosciute. Per questo motivo, le voci nella cache non dovrebbero durare troppo a lungo. Questo è il motivo per cui il campo *time to live* è stato incluso in ogni record delle risorse. Comunica ai server dei nomi remoti il tempo per cui archiviare i record nella cache. Se una macchina ha mantenuto lo stesso indirizzo IP per anni, potrebbe essere sicuro archiviare l'informazione per 1 giorno. Per informazioni di breve durata, è più sicuro eliminare i record dopo pochi secondi o dopo un minuto.

Il metodo di interrogazione descritto è conosciuto come **interrogazione ricorsiva**, perché ogni server che non possiede le informazioni richieste deve trovarle altrove e poi restituirle. E anche possibile utilizzare una forma alternativa. In questa forma, quando un'interrogazione non può essere soddisfatta localmente, l'interrogazione fallisce ma viene restituito il nome del successivo server da provare a usare (**interrogazione iterativa**). Alcuni server non implementano le interrogazioni ricorsive, e restituiscono sempre il nome del server successivo. Bisogna anche evidenziare che quando un Client DNS non riesce a ottenere una risposta prima della scadenza del suo timer, la volta successiva proverà di norma un altro server. Suppone infatti che il server non sia attivo, e non che il problema sia dovuto alla perdita della richiesta o della risposta. Anche se DNS è molto importante per il corretto funzionamento di Internet, il suo unico compito è associare nomi simbolici per le macchine ai loro indirizzi IP. Non aiuta a individuare persone, risorse, servizi e oggetti in generale. Per queste operazioni è stato definito un altro servizio directory, chiamato LDAP (*Lightweight Directory Access Protocol*). È una versione semplificata del servizio directory OSI X.500 ed è descritta in RFC 2251. Organizza le informazioni come una struttura ad albero e supporta la ricerca per diversi elementi. Può essere considerato come una sorta di rubrica telefonica o “pagine gialle”.

La posta elettronica

La posta elettronica, o **e-mail**, è disponibile da circa due decenni. Prima del 1990 era utilizzata principalmente nelle università. Negli anni '90 è divenuta nota al grande pubblico, ed è cresciuta in modo esponenziale: basti pensare che il numero di e-mail attualmente spedite ogni giorno è di molto superiore al numero di lettere tradizionali (chiamate anche **snail mail**). La posta elettronica, come molte altre forme di comunicazione, presenta propri stili e convenzioni. In particolare, è molto informale e ha una bassa soglia di utilizzo. Le persone che non si sono mai sognate di telefonare o scrivere una lettera a un VIP non esitano un secondo a spedire un messaggio di posta elettronica scritto in modo approssimativo. I messaggi di posta elettronica contengono numerose “parole in codice”, come CMQ (comunque) in italiano oppure ROTFL (Rolling On The Floor Laughing, mi sto rotolando sul pavimento dalle risate) in inglese. Molte persone utilizzano nei loro messaggi anche piccoli simboli ASCII chiamati **smiley** o **emoticon**. I primi sistemi di posta

elettronica erano semplicemente protocolli di trasferimento file, con la convenzione che la prima riga di ogni messaggio (o file) conteneva l'indirizzo del destinatario. Con il trascorrere del tempo le limitazioni di questo approccio sono divenute più evidenti.

Alcune tra le più gravi sono qui elencate:

1. L'invio di un messaggio a un gruppo di persone era scomodo. I manager spesso hanno bisogno di questa funzione per inviare promemoria a tutti i loro subordinati.
2. I messaggi non avevano una struttura interna, complicando l'elaborazione da parte del computer. Per esempio, se un messaggio inoltrato era incluso nel corpo di un altro messaggio, l'estrazione della parte inoltrata dal messaggio ricevuto era difficile.
3. Il mittente non poteva sapere se un messaggio era arrivato o no.
4. Se qualcuno pianificava di allontanarsi dall'azienda per diverse settimane e voleva che tutta la posta in arrivo fosse gestita dalla sua segretaria, non era facile organizzarsi.
5. L'interfaccia utente era integrata in modo scadente con il sistema di trasmissione, e richiedeva agli utenti di modificare il file, uscire dall'editor e aprire il programma di trasferimento file.
6. Non era possibile creare e inviare messaggi contenenti un insieme di testo, disegni, fax e voce.

Con l'esperienza sono stati proposti sistemi di posta elettronica più elaborati. Nel 1982, le proposte per la posta elettronica di ARPANET furono pubblicate in RFC 821 (protocollo di trasmissione) e 822 (formato dei messaggi). Alcune revisioni minori (RFC 2821 e RFC 2822) sono divenute standard Internet, ma tutti fanno ancora riferimento alla posta Internet con RFC 822. Nel 1984, CCITT ha abbozzato la sua raccomandazione X.400. Dopo due decenni di competizione, i sistemi di posta elettronica basati su RFC 822 sono ampiamente utilizzati, mentre quelli basati su X.400 sono scomparsi. Il motivo del successo di RFC 822 non sta tanto nella sua validità, ma nel fatto che X.400 era progettato in modo così scadente e complesso che nessuno poteva implementarlo correttamente. La scelta era tra un sistema di posta elettronica semplice (ma funzionante) basato su RFC 822 e un sistema di posta meraviglioso (ma non funzionante) basato su X.400, quindi molte organizzazioni scelsero il primo.

L'architettura e i servizi

In questa sezione forniremo una panoramica di ciò che possono fare i sistemi di posta elettronica, e del modo in cui sono organizzati. Normalmente sono composti da due sottosistemi: gli **agenti utente**, che consentono alle persone di leggere e inviare la posta elettronica, e gli **agenti di trasferimento dei messaggi**, che spostano i messaggi dall'origine alla destinazione. Gli agenti utente sono programmi locali che forniscono un metodo basato su comandi, menu o interfaccia grafica per interagire con il sistema di posta elettronica. Gli agenti di trasferimento dei messaggi sono generalmente **daemon** di sistema, vale a dire processi eseguiti in background. Il loro compito è spostare i messaggi di posta elettronica nel sistema.

Generalmente, i sistemi di posta elettronica supportano cinque funzioni di base. Vediamo quali sono:

- La **composizione** è il processo di creazione di messaggi e risposte. Anche se è possibile utilizzare un editor di testo qualsiasi per il corpo del messaggio, il sistema stesso può fornire assistenza per l'indirizzamento e i numerosi campi di intestazione associati a ogni messaggio.
- Il **trasferimento** indica lo spostamento dei messaggi dal mittente al destinatario. Per lo più consiste nello stabilire una connessione con la destinazione o a qualche computer intermedio, copiare il messaggio in output e rilasciare la connessione. Il sistema di posta elettronica dovrebbe svolgere automaticamente l'operazione, senza disturbare l'utente.
- Il **reporting** ha a che fare con la comunicazione al mittente di ciò che è avvenuto al messaggio. È stato consegnato? È stato rifiutato? È stato perso? Esistono numerose applicazioni in cui la conferma della consegna è importante e può avere un significato

legale.

- La **visualizzazione** dei messaggi in arrivo è necessaria affinché le persone possano leggere la loro posta elettronica. A volte è richiesta una conversione, oppure deve essere aperto un visualizzatore speciale, per esempio se il messaggio è un file PostScript o una voce digitalizzata. A volte vengono tentate semplici operazioni di conversione e formattazione. La **collocazione** è il passaggio finale e riguarda l'operazione svolta dal destinatario con il messaggio dopo la ricezione. Egli potrebbe cancellarlo prima di leggerlo, eliminarlo dopo averlo letto, salvarlo e così via. Dovrebbe inoltre essere possibile recuperare e rileggere i messaggi salvati, inoltrarli o elaborarli in altri modi.

Oltre a questi servizi di base, alcuni sistemi di posta elettronica (specialmente quelli interni alle aziende) forniscono numerose funzionalità avanzate; di seguito ne sono citate alcune. Quando le persone si spostano o si allontanano per qualche periodo, potrebbero desiderare che la loro posta venga inoltrata: il sistema dovrebbe quindi essere in grado di farlo automaticamente.

La maggior parte dei sistemi consente agli utenti di creare **mailbox** (caselle di posta) per archiviare la posta in arrivo. Sono necessari comandi per creare ed eliminare le caselle di posta, analizzarne il contenuto, inserire ed eliminare messaggi e così via. I manager delle aziende spesso inviano un messaggio a tutti i loro subordinati, clienti o fornitori. Da qui è nata l'idea delle **mailing list**, vale a dire elenchi di indirizzi di posta elettronica. Quando un messaggio viene inviato alla mailing list, copie identiche vengono consegnate a tutti i membri dell'elenco. Un'idea importante nei sistemi di posta elettronica è la distinzione tra **l'involucro** e il suo contenuto. L'involucro incapsula il messaggio e contiene tutte le informazioni necessarie per il trasporto del messaggio, come l'indirizzo di destinazione, la priorità e il livello di protezione, che sono distinte dal messaggio stesso. Gli agenti di trasporto dei messaggi utilizzano l'involucro per il routing, come gli uffici postali tradizionali utilizzano le buste. Il messaggio all'interno dell'involucro consiste di due parti: **l'intestazione** e **il corpo**. L'intestazione contiene le informazioni di controllo per gli agenti utente. Il corpo è dedicato interamente al destinatario umano.

L'agente utente

Un agente utente è di norma un programma che accetta una varietà di comandi per comporre, ricevere e rispondere ai messaggi, nonché per organizzare le caselle di posta. Alcuni agenti utente presentano un'interessante interfaccia grafica con menu e icone che richiede l'utilizzo di un mouse, mentre altri prevedono comandi a caratteri impariti da tastiera. A livello di funzioni, comunque, si equivalgono.

Invio di posta elettronica:

Per inviare un messaggio di posta elettronica, un utente deve fornire il messaggio, l'indirizzo di destinazione e magari qualche altro parametro. Il messaggio può essere prodotto con un editor di testo autonomo, un programma di elaborazione testi o possibilmente un editor di testo specializzato incorporato nell'agente utente. L'indirizzo di destinazione deve essere in un formato che l'agente utente può gestire. Molti agenti utente si aspettano gli indirizzi nella forma *utente@indirizzo-dns*. Visto che abbiamo già studiato DNS non ripeteremo qui il suo funzionamento.

Tuttavia, vale la pena notare che esistono altre forme di indirizzamento. In particolare, gli indirizzi X.400 appaiono radicalmente diversi dagli indirizzi DNS. Sono composti di coppie *attributo = valore* separate da barre, come in questo esempio:

/C=US/ST=MASSACHUSETTS/L=CAMBRIDGE/PA=360 MEMORIAL DR./CN=KEN SMITH/

Sono consentiti molti altri attributi, pertanto potete inviare la posta elettronica a qualcuno di cui non conoscete l'esatto indirizzo di posta elettronica, purché conosciate altri attributi (per esempio la società e il titolo professionale). Anche se i nomi X.400 sono considerevolmente meno pratici dei nomi DNS, la maggior parte dei sistemi di posta elettronica dispone di alias (o nickname) che permettono all'utente di inserire o selezionare il nome di una persona per ottenere il corretto indirizzo di posta elettronica. Di conseguenza, anche con gli indirizzi X.400, solitamente non è

necessario digitare queste stringhe. La maggior parte dei sistemi di posta elettronica supporta le mailing list, pertanto un utente può inviare lo stesso messaggio a un elenco di persone con un singolo comando. Se la mailing list viene gestita localmente, l'utente può inviare un messaggio separato a ogni destinatario previsto; se invece la lista è gestita in remoto, i messaggi saranno espansi in tale posizione.

Lettura della posta elettronica:

Generalmente, quando un agente utente viene avviato, cerca nella casella di posta dell'utente i messaggi in arrivo prima di visualizzare altro sullo schermo. Potrebbe quindi annunciare il numero di messaggi nella casella di posta o visualizzare un riepilogo di una riga per ognuno, attendendo un comando. In questo esempio, la casella di posta contiene otto messaggi:

#	Flag	Byte	Mittente	Oggetto
1	K	1030	asw	Modifiche a MINIX
2	KA	6348	trudy	Non tutte le Trudy sono cattive
3	K F	4519	Amy N. Wong	Richiesta di informazioni
4		1236	bal	Bioinformatica
5		104110	kaashoek	Materiale su peer-to-peer
6		1223	Frank	R: Una fantastica proposta
7		3110	guido	Il documento è stato accettato
8		1204	dmr	R: La visita dei miei studenti

Ogni riga della visualizzazione contiene diversi campi estratti dall'involucro o dall'intestazione del messaggio corrispondente. In un semplice sistema di posta elettronica la scelta dei campi visualizzati è fissa, mentre nei sistemi più sofisticati l'utente può specificare quali campi visualizzare fornendo un **profilo utente**, vale a dire un file che descrive il formato di visualizzazione. In questo esempio di base il primo campo è il numero del messaggio. Il secondo campo, *flag*, può contenere una *K*, che indica che il messaggio non è nuovo ma è stato letto in precedenza e conservato nella casella di posta, una *A*, che indica che al messaggio è stata inviata una risposta, e/o una *F*, che indica che il messaggio è stato inoltrato a qualcun altro. Sono consentiti anche altri flag. Il terzo campo comunica la lunghezza del messaggio, mentre il quarto specifica chi ha inviato il messaggio. Dal momento che questo campo è stato semplicemente estratto dal messaggio, potrebbe contenere nomi di campo, nomi completi, iniziali, nomi di login o qualsiasi cosa che il mittente ha scelto di inserire qui. Infine, il campo *oggetto* offre un breve riepilogo del contenuto del messaggio. Le persone che dimenticano di includere un campo *oggetto* scoprono spesso che le risposte ai loro messaggi tendono a non avere la priorità più alta. Dopo avere visualizzato le intestazioni, l'utente può scegliere quale azione eseguire, per esempio visualizzare un messaggio, eliminare un messaggio e così via. I vecchi sistemi erano basati su testo e generalmente usavano comandi di un carattere per eseguire queste attività, come T, A, D e F. Un argomento specificava il messaggio in questione. I sistemi più recenti utilizzano le interfacce grafiche: di solito l'utente seleziona un messaggio con il mouse e poi fa clic su un'icona per digitare, rispondere, eliminarlo o inoltrarlo.

La posta elettronica ha compiuto molti passi avanti dai giorni in cui rappresentava solo un trasferimento di file. Agenti utente sofisticati permettono la gestione di un elevato volume di messaggi. Per le persone che ricevono e inviano migliaia di messaggi all'anno, questi strumenti sono inestimabili.

I formati dei messaggi

Passiamo ora dall'interfaccia utente al formato dei messaggi di posta elettronica stessi. Per prima cosa osserveremo i messaggi di posta ASCII che utilizzano RFC 822, e poi studieremo le estensioni multimediali a RFC 822.

RFC 822

I messaggi sono costituiti da un primitivo involucro (descritto in RFC 821), alcuni campi di intestazione, una riga vuota e il corpo del messaggio. Ogni campo di intestazione consiste logicamente di una singola riga di testo ASCII contenente il nome del campo, un carattere di due punti e, per la maggior parte dei campi, un valore. RFC 822 è stata progettata decenni fa e non distingue chiaramente i campi dell'involucro dai campi dell'intestazione. Anche se è stata rivista in RFC 2822, riscriverla completamente non è stato possibile a causa del suo utilizzo diffuso.

I campi di intestazione principali correlati al trasporto del messaggio sono elencati nella seguente figura:

Intestazione	Significato
To:	Gli indirizzi di posta elettronica dei destinatari primari
Cc:	Gli indirizzi di posta elettronica dei destinatari secondari
Bcc:	Gli indirizzi di posta elettronica per le copie per conoscenza nascoste
From:	La persona che ha creato il messaggio
Sender:	L'indirizzo di posta elettronica del mittente vero e proprio
Received:	La riga aggiunta da ogni agente di trasferimento lungo il percorso
Return-path:	Può essere utilizzato per identificare un percorso di ritorno al mittente

- Il campo *to*: indica l'indirizzo DNS del destinatario principale; è consentito indicare più destinatari.
- Il campo *cc*: indica gli indirizzi dei destinatari secondari. In termini di consegna non vi è una distinzione tra destinatari principali secondari: si tratta solo di una differenza psicologica che può essere importante per le persone coinvolte, ma non per il sistema di posta elettronica. Il termine *cc*: significa copia per conoscenza; molte persone lo intendono come “copia carbone”, una definizione datata ma sempre valida.
- Il campo *bcc*: (copia per conoscenza nascosta) è simile al campo *cc*; tranne per il fatto che la riga viene eliminata da tutte le copie inviate ai destinatari principali e secondari. Questa funzionalità consente alle persone di inviare copie a terze parti senza che i destinatari principali e secondari lo sappiano.
- I due campi successivi, *from*: e *sender*:, indicano rispettivamente chi ha scritto e inviato il messaggio. Non devono necessariamente avere lo stesso contenuto.
- Una riga contenente *received*: viene aggiunta da ogni agente di trasferimento dei messaggi lungo il percorso. La riga contiene l'identità dell'agente, la data e l'ora di ricezione del messaggio e altre informazioni che possono essere utilizzate per trovare i bug nel sistema di routing.
- Il campo *return-path*: viene aggiunto dall'agente di trasferimento dei messaggi finale e ha 10 scopi di spiegare come ritornare al mittente. In teoria, questa informazione può essere raccolta da tutte le intestazioni *received*: (tranne per il nome della casella di posta del mittente), ma viene raramente compilata in questo modo e di norma contiene solo l'indirizzo del mittente.

Esistono anche altri campi d'intestazione utilizzati dagli agenti utenti o destinatari umani:

Intestazione	Significato
Date:	La data e l'ora di invio del messaggio
Reply-to:	L'indirizzo di posta elettronica a cui inviare le risposte
Message-id:	Un numero univoco per fare riferimento a questo messaggio in seguito
In-reply-to:	L'ID del messaggio a cui si riferisce questa risposta
References:	Altri ID di messaggio rilevanti
Keywords:	Parole chiave scelte dall'utente
Subject:	Un breve riepilogo del messaggio da visualizzare su una riga

- Il campo *reply-to*: viene a volte utilizzato quando né la persona che compone il messaggio né la persona che lo invia desiderano vedere la risposta.

Il documento RFC 822 afferma in modo esplicito che gli utenti possono inventare nuove intestazioni per utilizzo privato, purché tali intestazioni inizino con la stringa *X-*. È garantito che nessuna intestazione futura userà nomi che iniziano con *X-*, per evitare conflitti con intestazioni private e ufficiali.

L'intestazione è seguita dal corpo del messaggio. Gli utenti possono inserire tutto quello che desiderano.

MIME (*Multipurpose Internet Mail Extensions*)

Agli esordi di ARPANET, la posta elettronica consisteva esclusivamente di messaggi di testo scritti in inglese ed espressi in ASCII. Per questo ambiente, RFC 822 svolgeva alla perfezione il lavoro: specificava le intestazioni e lasciava il contenuto agli utenti. Oggi sulla Internet mondiale questo approccio non è più adeguato. I problemi che possono nascere comprendono l'invio e la ricezione di:

1. messaggi scritti in lingue con accenti (per esempio italiano e francese)
2. messaggi in alfabeti non latini (per esempio ebraico e russo)
3. messaggi scritti in lingue con alfabeti ideografici (per esempio cinese e giapponese)
4. messaggi che non contengono testo (per esempio audio o immagini).

Una soluzione è stata proposta in RFC 1341 e aggiornata nelle RFC da 2045 a 2049. Questa soluzione, chiamata MIME (*Multipurpose Internet Mail Extensions*), oggi è ampiamente utilizzata e quindi sarà descritta di seguito.

L'idea di base di MIME è continuare a utilizzare il formato RFC 822, aggiungendo una struttura al corpo del messaggio e definendo le regole di codifica per i messaggi non ASCII. Visto che non si discosta da RFC 822, i messaggi MIME possono essere inviati utilizzando i programmi e i protocolli di posta esistenti. Tutto ciò che deve essere cambiato sono i programmi di invio e ricezione, che è un compito lasciato agli utenti.

MIME definisce cinque nuove intestazioni dei messaggi:

Intestazione	Significato
MIME-version:	Identifica la versione di MIME
Content-description:	Una stringa leggibile che comunica che cosa contiene il messaggio
Content-id:	Un identificatore univoco
Content-transfer-encoding:	Indica come il corpo del messaggio è stato preparato per la trasmissione
Content-type:	Il tipo e il formato del contenuto

- La prima indica semplicemente all'agente utente di ricevere il messaggio in questione come un messaggio MIME e specifica la versione utilizzata. Qualsiasi messaggio che non contiene l'intestazione *MIME-version*: è un messaggio di testo normale in lingua inglese e viene elaborato come tale.
- L'intestazione *content-description*: è una stringa ASCII che comunica il contenuto del messaggio. Questa intestazione è necessaria per consentire al destinatario di decidere se vale

la pena di decodificare e leggere il messaggio. Se la stringa afferma “Foto del criceto di Barbara” e la persona che riceve il messaggio non è un grande estimatore di criceti, il messaggio sarà probabilmente scartato anziché decodificato in una fotografia a colori ad alta risoluzione.

- L'intestazione *content-id*: identifica il contenuto. Usa lo stesso formato dell'intestazione standard *message-id*.
- L'intestazione *content-transfer-encoding*: spiega da cosa è costituito l'involucro per la trasmissione su una rete che può accettare solo oggetti contenenti caratteri costituiti da lettere, numeri e segni di punteggiatura. Sono previsti cinque schemi (più un carattere per indicarne di nuovi), e il più semplice è il testo ASCII. I caratteri ASCII usano 7 bit e possono essere trasportati direttamente dal protocollo di posta elettronica se le righe non superano la lunghezza di 1.000 caratteri.
- L'ultima intestazione è quella più interessante, che specifica la natura del corpo del messaggio. RFC 2045 definisce sette tipi, per ognuno dei quali sono disponibili uno o più sottotipi. Il tipo e il sottotipo sono separati da una barra, come in Content-type: video/mpeg. Il sottotipo deve essere fornito esplicitamente nell'intestazione; non sono forniti valori predefiniti. L'elenco iniziale di tipi e sottotipi specificato in RFC 2045 è:

Tipo	Sottotipo	Descrizione
Text	Plain	Testo non formattato
	Enriched	Testo con semplici comandi di formattazione
Image	Gif	Immagine statica nel formato GIF
	Jpeg	Immagine statica nel formato JPEG
Audio	Basic	Suono udibile
Video	Mpeg	Filmato nel formato MPEG
Application	Octet-stream	Una sequenza di byte non interpretata
	Postscript	Un documento stampabile in PostScript
Message	Rfc822	Un messaggio MIME RFC 822
	Partial	Un messaggio diviso per la trasmissione
	External-body	Il messaggio vero e proprio deve essere prelevato dalla rete
Multipart	Mixed	Parti indipendenti nell'ordine specificato
	Alternative	Lo stesso messaggio in formati diversi
	Parallel	Le parti devono essere visualizzate contemporaneamente
	Digest	Ogni parte è un messaggio RFC 822 completo

- Il tipo *text* è per il testo ASCII normale.
 - La combinazione *text/plain* è per i messaggi ordinari che possono essere visualizzati come vengono ricevuti, senza codifica o ulteriori elaborazioni. Questa opzione consente ai messaggi ordinari di essere trasportati in MIME con poche intestazioni extra.
 - Il sottotipo *text/enriched* permette l'inclusione nel testo di un semplice linguaggio di markup. Questo linguaggio offre un modo indipendente dal sistema per esprimere grassetto, corsivi, dimensioni in punti più o meno elevate, rientri, giustificazioni, apici e pedici, nonché un semplice layout di pagina. Il linguaggio di markup è basato su SGML (Standard Generalized Markup Language), utilizzato anche come base per HTML.
- Il tipo MIME successivo è *image*, utilizzato per trasmettere immagini statiche. Oggi sono ampiamente utilizzati molti formati per archiviare e trasmettere le immagini, con o senza compressione. Due di questi, GIF e JPEG, sono incorporati in quasi tutti i browser, ma ne esistono altri che sono stati aggiunti all'elenco originale.
- I tipi *audio* e *video* sono dedicati rispettivamente al suono e alle immagini in movimento. Occorre notare che *video* include solo le informazioni visive, non la colonna sonora. Se diventa necessario trasmettere un filmato con audio, le porzioni audio e video devono essere trasmesse separatamente, a seconda del sistema di codifica utilizzato.
- Il tipo *application* è un “ripostiglio” per i formati che richiedono un'elaborazione esterna

non compresi nelle altre tipologie.

- Un *octet-stream* è semplicemente una sequenza di byte non interpretati. Dopo la ricezione di tale flusso, un agente utente deve probabilmente visualizzarlo suggerendo all'utente che deve essere copiato in un file e richiedendo un nome file. L'elaborazione successiva è lasciata all'utente.
- L'altro sottotipo definito è *postscript*, che fa riferimento al linguaggio PostScript definito da Adobe Systems e ampiamente utilizzato per la descrizione di pagine stampate.
- Il tipo *message* consente a un messaggio di essere incapsulato in un altro. Questo schema è utile per l'inoltro della posta elettronica. Quando un messaggio RFC 822 completo viene incapsulato in un messaggio più esterno, deve essere utilizzato il sottotipo *rfc822*.
 - Il sottotipo *partial* permette di suddividere in più parti un messaggio incapsulato e di inviarle separatamente.
 - il sottotipo *external-body* può essere utilizzato per messaggi molto lunghi (come i filmati). Anziché includere il file MPEG nel messaggio, viene fornito un indirizzo FTP cui l'agente utente del ricevitore può fare riferimento nel momento opportuno.
- L'ultimo tipo è *multipari*, che consente di inserire più parti in un messaggio delimitando chiaramente l'inizio e la fine di ciascuna.
 - Il sottotipo *mixed* consente a ogni parte di essere diversa, senza strutture aggiuntive imposte.
 - il sottotipo *alternative* consente allo stesso messaggio di essere incluso più volte ma espresso con due o più supporti diversi.
 - Il sottotipo *parallel* è utilizzato quando tutte le parti devono essere "viste" contemporaneamente.
 - il sottotipo *digest* viene utilizzato quando molti messaggi sono uniti in un messaggio composito.

Il trasferimento dei messaggi

Il sistema di trasferimento dei messaggi si occupa della trasmissione dei messaggi dal mittente al destinatario. Il modo più semplice per svolgere questa operazione è stabilire una connessione di trasporto dalla macchina di origine a quella di destinazione per poi trasferire semplicemente il messaggio.

SMTP (*Simple Mail Transfer Protocol*)

All'interno di Internet, la posta elettronica viene consegnata costituendo una connessione tra la macchina di origine e la porta 25 della macchina di destinazione. In ascolto su questa porta esiste un daemon di posta elettronica che utilizza SMTP (*Simple Mail Transfer Protocol*). Questo daemon accetta le connessioni in ingresso e copia nelle caselle di posta appropriate i messaggi ricevuti da queste connessioni. Se un messaggio non può essere consegnato, al mittente viene restituito un rapporto di errore contenente la prima parte del messaggio non consegnabile.

SMTP è un semplice protocollo ASCII. Dopo avere stabilito la connessione TCP alla porta 25, la macchina di invio (che opera come Client) attende la comunicazione da parte della macchina ricevente (che opera come server). Il server inizia inviando una riga di testo che comunica la sua identità e la possibilità di inviare la posta. Se questo non avviene, il client rilascia la connessione e riprova in seguito.

Se il server è pronto ad accettare la posta elettronica, il client annuncia da chi proviene il messaggio e a chi è destinato. Se tale destinatario esiste nella destinazione, il server comunica al client di inviare il messaggio. Dopo di che, il client invia il messaggio e il server fornisce

l'acknowledgement. Non sono necessari checksum, perché TCP offre un flusso di byte affidabile. Se vi sono più messaggi di posta elettronica, ora vengono inviati tutti. Una volta scambiata tutta la posta elettronica in entrambe le direzioni, la connessione viene rilasciata.

Di seguito commenteremo alcuni comandi presenti nel seguente esempio:

```

S: 220 xyz.com SMTP service ready
C: HELO abcd.com
    S: 250 xyz.com says hello to abcd.com
C: MAIL FROM: <elinor@abcd.com>
    S: 250 sender ok
C: RCPT TO: <carolyn@xyz.com>
    S: 250 recipient ok
C: DATA
    S: 354 Send mail; end with "." on a line by itself
C: from: elinor@abcd.com
C: to: carolyn@xyz.com
C: MIME-version: 1.0
C: message-id: <0704760941.AA00747@abcd.com>
C: content-type: multipart/alternative; boundary=qwertyuopasdfghjklzxcvbnm
C: subject: La terra orbita intorno al sole un numero intero di volte
C:
C: Questo è il preambolo. L'agente utente lo ignora. Buona giornata.
C:
C: --qwertyuopasdfghjklzxcvbnm
C: content-type: text/enriched
C:
C: Tanti auguri a te
C: Tanti auguri a te
C: Tanti auguri, cara <b>Carolyn</b>
C: Tanti auguri a te
C:
C: --qwertyuopasdfghjklzxcvbnm
C: content-type: message/external-body;
C: access-type="anon-ftp";
C: site="bicycle.abcd.com";
C: directory="pub";
C: name="birthday.snd"
C:
C: content-type: audio/basic
C: content-transfer-encoding: base64
C: --qwertyuopasdfghjklzxcvbnm
C: .
    S: 250 message accepted
C: QUIT
    S: 221 xyz.com closing connection

```

Il primo comando dal Client è *HELO*. Delle varie combinazioni di quattro caratteri che rappresentano abbreviazioni di *HELLO* (ciao), questa presenta numerosi vantaggi sulle rivali. Il messaggio è inviato a un solo destinatario, per cui viene utilizzato un solo comando *RCPT*. Questo comando permette l'invio di un singolo messaggio a più destinatari, dove per ognuno viene ricevuto un acknowledgement o un rifiuto. Anche se alcuni destinatari vengono rifiutati (perché non esistono nella destinazione), il messaggio può essere inviato agli altri.

Per finire, anche se la sintassi dei comandi di quattro caratteri dal client è specificata in modo rigido, la sintassi delle risposte lo è di meno: in realtà contano solo i codici numerici, e ogni implementazione può inserire la stringa che desidera dopo di essi.

Per comprendere meglio come funzionano SMTP e altri protocolli descritti in questo capitolo si può fare una prova. Per prima cosa occorre individuare una macchina connessa a Internet. Su un sistema UNIX, digitare nella shell: *telnet mail.isp.com 25*

sostituendo alla scritta *mail.isp.com* dell'esempio il nome DNS del server di posta dell'ISP (internet Service provider) utilizzato. Su un sistema Windows, selezionate Start, Esegui e digitate il comando nella finestra di dialogo. Questo comando stabilirà una connessione telnet (cioè TCP) alla porta 25 del computer indicato, cioè alla sua porta SMTP (vedere la Figura 6.27 per alcune porte comuni). Probabilmente otterrete una risposta come la seguente:

Connessione a *mail.isp.com...*

Connesso a *mail.isp.com*

Il carattere di escape è

220 mail.isp.com Smail #74 ready at Thu, 25 Sept 2002 13:26 +0200

Le prime tre righe provengono da telnet, che comunica che cosa sta facendo. L'ultima riga proviene dal server SMTP sulla macchina remota, che annuncia il suo desiderio di comunicare e di accettare la posta elettronica. Per scoprire i comandi accettati è possibile digitare: *HELP*.

Anche se il protocollo SMTP è completamente ben definito, possono comunque sorgere dei problemi. Uno è legato alla lunghezza del messaggio: alcune vecchie implementazioni non possono gestire i messaggi che superano 64 KB. Un altro problema riguarda i timeout. Se il client e il server sperimentano diversi timeout, uno dei due potrebbe abbandonare i tentativi mentre l'altro è ancora occupato, terminando inaspettatamente la connessione. Per finire, in casi rari, si potrebbero innescare tempeste di mail infinite. Per risolvere questi problemi, in RFC 2821 è stato definito ESMTP (*Extended SMTP*). I client che desiderano utilizzarlo devono inviare un messaggio iniziale *EHLO* al posto di *HELO*. Se viene rifiutato, il server è un normale server SMTP e il client deve procedere nel modo solito. Se *EHLO* viene accettato, sono consentiti i nuovi comandi e parametri.

Consegna finale

Con l'avvento delle persone che accedono a Internet chiamando l'ISP tramite un modem, il sistema è diventato inadeguato. Il problema è il seguente: che cosa accade quando Elinor desidera inviare un messaggio di posta elettronica a Carolyn, ma Carolyn al momento non è online? Elinor non può stabilire una connessione TCP a Carolyn, e quindi non può eseguire il protocollo SMTP.

Una soluzione consiste nell'avere un agente di trasferimento dei messaggi su una macchina dell'ISP, che accetta la posta elettronica per i suoi clienti e la archivia nelle caselle di posta sulla macchina dell'ISP. Dal momento che questo agente può essere sempre online, la posta elettronica può essere inviata in qualsiasi momento.

POP3

Sfortunatamente, questa soluzione crea un altro problema: come può l'utente ricevere la posta elettronica dall'agente di trasferimento dei messaggi dell'ISP? La soluzione a questo problema è creare un altro protocollo, che consente agli agenti di trasferimento dell'utente (sui PC client) di contattare l'agente di trasferimento dei messaggi (sulla macchina dell'ISP) per effettuare la copia della posta elettronica dall'ISP all'utente. Uno di questi protocolli è POP3 (*Post Office Protocol version 3*), descritto in RFC 1939.

La situazione in cui il mittente e il ricevitore dispongono di una connessione permanente a Internet è mostrata nella seguente figura, insieme alla situazione in cui il mittente è attualmente online al contrario del destinatario:

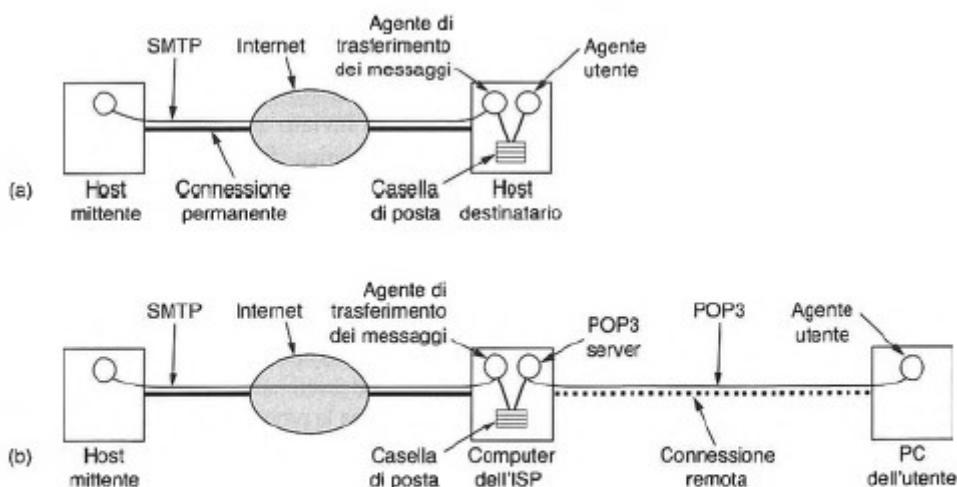


Figura 7.15. (a) Invio e lettura della posta quando il destinatario ha una connessione permanente a Internet e l'agente utente viene eseguito sulla stessa macchina dell'agente di trasferimento dei messaggi. (b) Lettura della posta elettronica quando il destinatario utilizza una connessione telefonica a un ISP.

POP3 viene avviato quando l'utente apre il lettore della posta. Il lettore della posta chiama l'ISP (a meno che sia già disponibile una connessione) e stabilisce una connessione TCP con l'agente di trasferimento dei messaggi alla porta 110. Una volta stabilita la connessione, il protocollo POP3 attraversa sequenzialmente tre stati:

1. autorizzazione
2. transazioni

3. aggiornamento

Lo stato di autorizzazione si occupa del login dell'utente; lo stato delle transazioni consente all'utente di raccogliere la posta e cancellarla dalla casella dell'TSP. Lo stato di aggiornamento provoca l'effettiva eliminazione dei messaggi. Questo comportamento può essere osservato digitando qualcosa di simile a: `telnet mail.isp.com 110`, dove `mail.isp.com` rappresenta il nome DNS del server di posta dell'ISP. Telnet stabilisce una connessione alla porta 110, su cui è in ascolto il server POP3. Dopo avere accettato la connessione TCP, il server invia un messaggio ASCII che annuncia la sua presenza. Solitamente, inizia con `+OK` seguito da un commento.

Le righe contrassegnate da *C*: provengono dal client (utente), mentre quelle indicate con *S*:

S: +OK POP3 server ready
C: USER carolyn
 S: +OK
C: PASS vegetables
 S: +OK login successful
C: LIST
 S: 1 2505
 S: 2 14302
 S: 3 8122
 S: .
C: RETR 1
 S: (invia il messaggio 1)
C: DELE 1
C: RETR 2
 S: (invia il messaggio 2)
C: DELE 2
C: RETR 3
 S: (invia il messaggio 3)
C: DELE 3
C: QUIT
 S: +OK POP3 server disconnecting

provengono dal server (agente di trasferimento dei messaggi sulla macchina dell'TSP).

Durante lo stato di autorizzazione, il client invia il suo nome utente e la sua password. Dopo il login, il client può inviare il comando *LIST*, che chiede al server di elencare il contenuto della casella di posta, un messaggio per riga, specificando la lunghezza di ogni messaggio. L'elenco è terminato da un punto.

Il client può quindi recuperare i messaggi utilizzando il comando *RETR* e contrassegnarli per l'eliminazione con *DELL*. Una volta recuperati tutti i messaggi (e possibilmente dopo averli contrassegnati per l'eliminazione), il client impartisce il comando *QUIT* per terminare lo stato delle transazioni ed entrare nello stato di aggiornamento. Quando il server ha eliminato tutti i messaggi, invia una risposta e interrompe la connessione TCP.

IMAP

Per un utente con un account di posta elettronica presso un ISP, che accede sempre dallo stesso PC, POP3 è perfetto ed è ampiamente utilizzato per la sua semplicità e solidità. Tuttavia, è una verità dell'industria informatica che, non appena qualcosa funziona bene, qualcuno inizia a richiedere altre funzionalità (ottenendo altri bug). Questo è accaduto anche per la posta elettronica. Per esempio, molte persone che disponevano di un singolo account di posta elettronica al lavoro o a scuola desideravano accedervi dal lavoro, dal PC della loro abitazione, dai loro portatili quando erano in viaggio di affari e dai cyber-café in vacanza. Anche se POP3 lo consente, di norma scarica tutti i messaggi archiviati ad ogni contatto: il risultato è che la posta dell'utente viene rapidamente dispersa su più macchine, più o meno casualmente (alcune non appartengono nemmeno all'utente!). Questo svantaggio ha portato alla nascita di un protocollo di consegna alternativo, IMAP (*Internet Message Access Protocol*), definito in RFC 2060. A differenza di POP3, che fondamentalmente presume che l'utente cancelli la casella di posta a ogni contatto, IMAP presume che tutti i messaggi devono rimanere sul server all'infinito, in più cartelle di posta. IMAP fornisce sofisticati meccanismi per leggere in tutto o in parte i messaggi, funzione utile durante l'utilizzo di un modem lento per leggere la parte di testo di un messaggio *multipar* con grandi allegati audio e video. Visto che si ipotizza che i messaggi non saranno trasferiti al computer dell'utente per un'archiviazione permanente, IMAP fornisce meccanismi per creare, distruggere e manipolare più cartelle di posta sul server. In questo modo, un utente può mantenere una cartella di posta per ogni corrispondente e spostare i messaggi dalla posta in arrivo dopo la lettura. IMAP ha molte funzionalità, come la capacità d'indicizzare la posta non per numeri di arrivo, ma utilizzando gli attributi. A differenza di POP3, IMAP può anche accettare la posta in uscita per rinvio alle destinazioni, oltre che consegnare la posta in arrivo. L'impostazione generale del protocollo IMAP è simile a quella di POP3,

ranne per il fatto che esistono decine di comandi. Il server IMAP è in ascolto sulla porta 143. Un confronto tra POP3 e IMAP è presentato di seguito:

Caratteristica	POP3	IMAP
Definizione del protocollo	RFC 1939	RFC 2060
Porta TCP utilizzata	110	143
Luogo di archiviazione della posta	PC dell'utente	Server
Lettura della posta	Offline	Online
Tempo di connessione richiesto	Ridotto	Elevato
Utilizzo delle risorse del server	Minimo	Estensivo
Più cartelle di posta	No	Sì
Chi esegue il backup delle caselle di posta	Utente	ISP
Valido per utenti in movimento	No	Sì
Controllo dell'utente sul download	Ridotto	Elevato
Download parziale dei messaggi	No	Sì
Le quote del disco sono un problema	No	Potrebbero esserlo nel tempo
Semplice da implementare	Sì	No
Supporto diffuso	Sì	In crescita

Si dovrebbe notare, comunque, che non tutti gli ISP e non tutti i programmi di posta elettronica supportano entrambi i protocolli. Di conseguenza, quando si sceglie un programma di posta elettronica, è importante scoprire quali protocolli supporta e assicurarsi che l'ISP ne supporti almeno uno.

Le funzionalità di consegna:

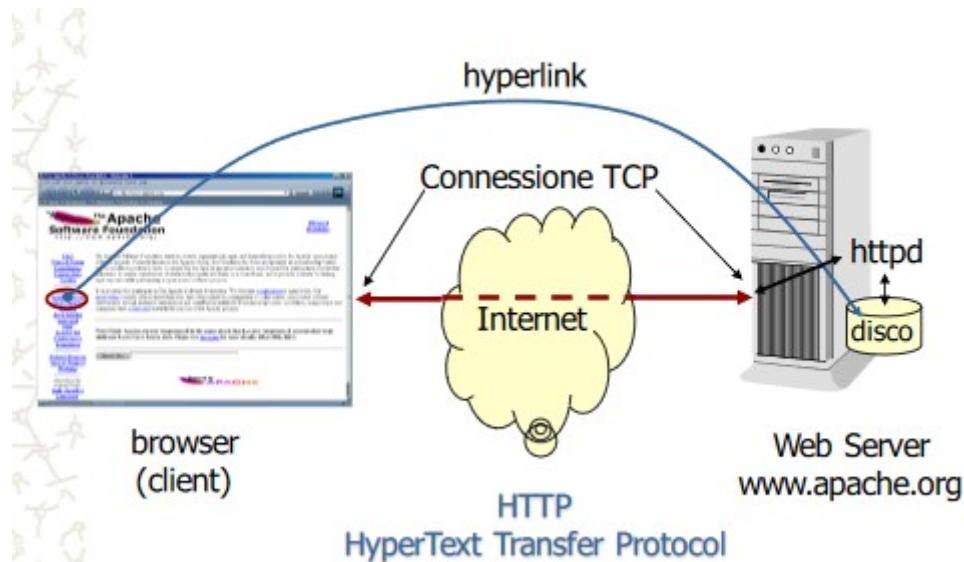
Indipendentemente dall'utilizzo di POP3 o IMAP, molti sistemi forniscono agganci per un'ulteriore elaborazione della posta elettronica. Una funzionalità particolarmente preziosa per molti utenti della posta elettronica è la possibilità di impostare **filtri**. Si tratta di regole controllate alla ricezione della posta elettronica o all'avvio dell'agente utente. Ogni regola specifica una condizione e un'azione. Alcuni ISP forniscono un filtro che divide automaticamente in categorie la posta in arrivo, separando i messaggi importanti dallo spam (posta indesiderata) e archiviando ogni messaggio nella cartella corrispondente. Tali filtri lavorano generalmente controllando prima se la fonte è uno spammer noto. Poi esaminano generalmente la riga dell'oggetto. Se centinaia di utenti hanno ricevuto un messaggio con la stessa riga dell'oggetto, probabilmente si tratta di spam. Per il rilevamento dello spam vengono utilizzate anche altre tecniche. Un'altra funzionalità di consegna fornita spesso è la capacità di inoltrare temporaneamente la posta in arrivo a un indirizzo diverso. Questo indirizzo può anche essere relativo a un computer gestito da un servizio commerciale, che inoltra le pagine via radio o via satellite visualizzando la riga *subject*: sul cercapersone dell'utente. Un'altra utile funzionalità di consegna finale è la possibilità di installare un **daemon per le assenze**. Si tratta di un programma che esamina ogni messaggio in arrivo e invia al mittente una risposta insipida come:

Ciao. Sono in vacanza! Tornerò il 24 di agosto. Buone ferie!

Tali risposte possono anche specificare come gestire questioni urgenti nel frattempo, altre persone da contattare per problemi specifici e così via. La maggior parte dei daemon per le assenze tiene traccia delle persone a cui ha già inviato la risposta ed evita di inviare alla stessa persona una replica identica. I più validi controllano anche se il messaggio in arrivo è stato inviato a una mailing list, e in questo caso non inviano la risposta automatica.

IL WEB

Nato nel 1989 al CERN di Ginevra come mezzo per scambiare informazioni. Il web è una collezione di documenti ipertestuali distribuita su server collegati alla rete Internet. La ragnatela (web) è un grafo i cui nodi sono i singoli documenti collegati fra loro da puntatori (hyperlink). La maggior parte dei documenti su web è in formato HTML(HyperText Markup Language) ma si trovano anche altri formati (Macromedia Flash, pdf, postscript, ecc..).



HTTP

Ogni sito Web ha un processo server in ascolto su una porta TCP. La porta standard è la numero 80. HTTP definisce il protocollo di comunicazione fra il client e il server. È utilizzato per trasferire ogni tipo di risorsa (file) su WWW. Una risorsa è un' entità individuata da un URL(Uniform Resource Locator): file di qualsiasi formato prodotto dall' esecuzione di una interrogazione o di uno script.

Utilizza un modello client-server:

- Il client HTTP apre la connessione e invia un messaggio di richiesta al server HTTP
- Il server invia una risposta che in genere contiene la risorsa richiesta e poi chiude la connessione

Il protocollo è senza stato (non c'è memoria delle transazioni).

Formato dei messaggi HTTP

I messaggi di richiesta e risposta hanno formato simile

```
Linea Iniziale (diversa per richiesta e risposta)
Header1: valore1
Header2: valore2
Header3: valore3
          Linea vuota!
Corpo del messaggio (contenuto del file, risultato di
una interrogazione; può essere lungo molte linee e
essere binario)
```

L'intestazione è separata dal corpo da una linea vuota (CR LF)

Richieste HTTP

La linea iniziale di una richiesta è formata da 3 parti

- Metodo
- Percorso locale della risorsa richiesta
- Versione di HTTP usata

Esempio di richiesta

```
GET /index.html HTTP/1.1          ← Linea Iniziale
Host: univac.di.unisa.it
User-Agent: Mozilla/5.0 (Windows; U; Win98; en-US; m18)
Gecko/20010131 Netscape6/6.01
Accept: */*
Accept-Language: en
Accept-Encoding: gzip,deflate,compress,identity
Keep-Alive: 300
Connection: keep-alive
```

header {

I metodi definiscono le operazioni possibili su una risorsa:

- **GET**: chiede il trasferimento di una risorsa. Se è seguita dall'intestazione If-Modified-Since
il server invia i dati solo se sono stati modificati dopo la data specificata (gestione cache del browser)
- **HEAD**: Richiede solo le intestazioni relative alla risorsa. Serve per verificare le caratteristiche della risorsa senza trasferirla
- **POST**: Utilizzato per inviare dati da elaborare al server. L'intestazione è seguita da un corpo della richiesta che contiene i dati. Il tipo e la dimensione dei dati è indicata dagli header MIME Content-Type e Content-Length.

Risposta HTTP

- La linea iniziale di una risposta costituisce una linea di stato

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2001 22:44:40 GMT
Server: Apache/1.3.20 (Win32)
Last-Modified: Wed, 06 Jun 2001 22:32:26 GMT
ETag: "0-64-3bleaf7a"
Accept-Ranges: bytes
Content-Length: 100
Connection: close
Content-Type: text/html
```

headers {

risorsa {

```
<HTML>
<HEAD>
<TITLE>Prova</TITLE>
</HEAD>
<BODY>
<H2>File HTML di Prova</H1>
</BODY>
```

Linea vuota ←

Codici di stato

La linea di stato riporta un codice di stato e la sua "spiegazione"

HTTP/1.1 200 OK

I codici più comuni sono

200 OK

Richiesta con successo. La risorsa è nel corpo della risposta

404 Not Found

La risorsa richiesta non esiste

301 Moved Permanently

302 Moved Temporarily

303 See Other (in HTTP 1.1)

La risorsa è stata spostata ad un altro URL specificato nel campo `Location:` dell'intestazione. Il client dovrebbe saltare a tale locazione (redirect).

500 Server Error

Intestazioni

Seguono il formato specificato in RFC 822 anche per l'email

HTTP 1.0 definisce 16 header (tutti opzionali)

HTTP 1.1 definisce 46 header (obbligatorio `Host:`)

`User-Agent:`

Identifica il programma client che effettua la richiesta. Individua webots, spiders, ecc..

`Server:`

Identifica il server

`Last-Modified:`

Indica la data di modifica della risorsa. E' usata per gestire le cache

`Content-Type:`

Tipo MIME del corpo del messaggio

`Content-Length:`

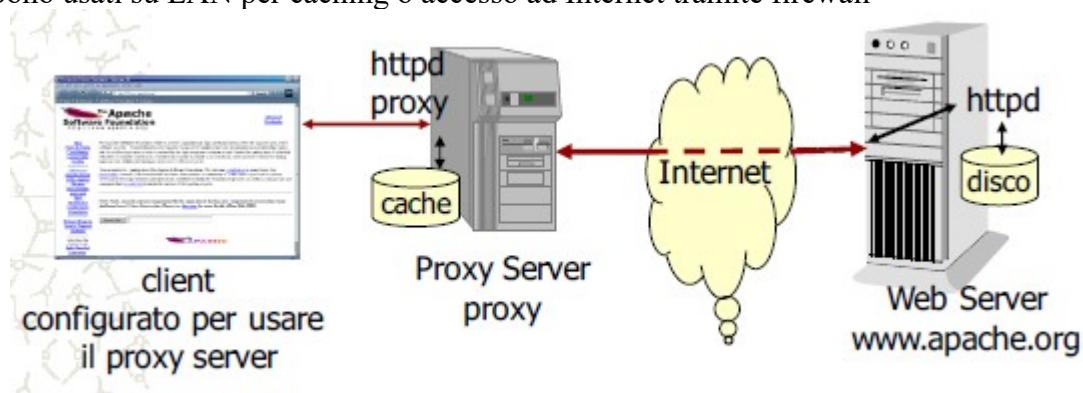
Lunghezza in byte del corpo del messaggio

Proxy HTTP

Un proxy HTTP agisce da intermediario fra il client e il server

- Riceve le richieste dal client
- Propaga la richiesta al server corretto

Sono usati su LAN per caching o accesso ad Internet tramite firewall



HTTP 1.1

Permette più transazioni su una stessa connessione persistente

- Attivo di default. Si inviano le richieste in pipelining e si recuperano le risposte nello stesso ordine

Ha introdotto il supporto per le cache (`If-Modified-Since:`). Risposta più veloce per pagine generate dinamicamente utilizzando la codifica chunked:

- Non si deve specificare la lunghezza del messaggio nell'intestazione
 - Il messaggio è scomposto in blocchi (chunks)

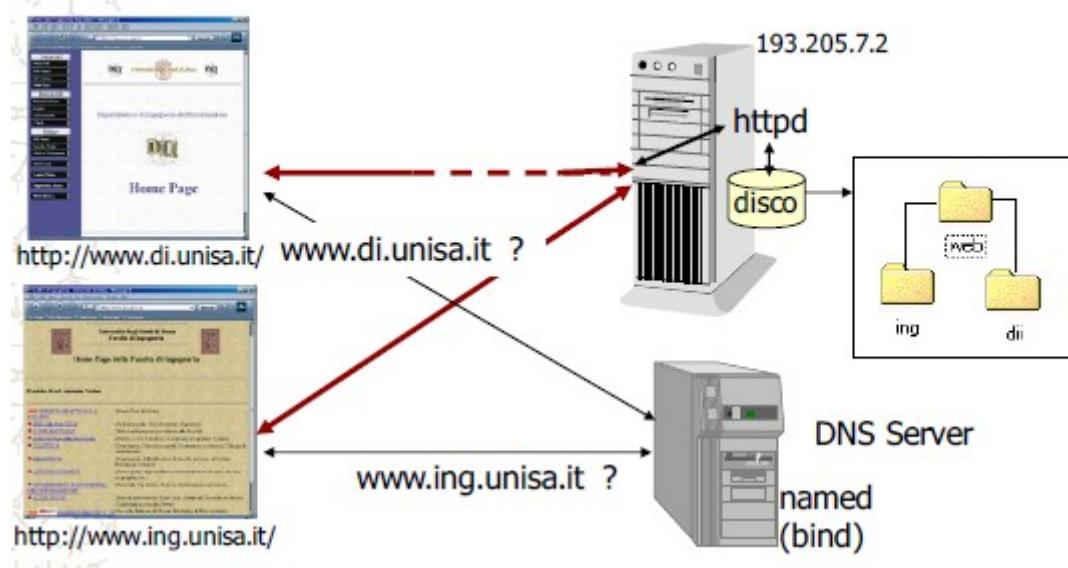
Uso migliore degli indirizzi IP permettendo di ospitare più siti virtuali su uno stesso server con un solo IP

- Uso dell'intestazione Host: -> specifica il nome del sito a cui è indirizzata la richiesta

Multi-homed IP

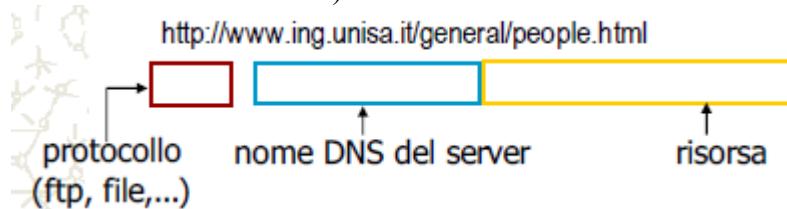
Un server allo stesso indirizzo IP può gestire più domini

Richiede alias nel DNS



URL

Un URL (Uniform Resource Locator) individua univocamente una risorsa su web:



Al nome DNS possono essere aggiunte

- la porta TCP (altrimenti si usa quella di default del protocollo)
 - una coppia username/password per accedere a risorse che richiedono autenticazione

<http://johnm-x34j23@www.ieee.org:8080/>



HTML (HyperText Markup Language)

E' un linguaggio che usa annotazioni (**markup**) per definire la formattazione del testo:

****scrittura in grassetto****

↑ ↑
tag di apertura **tag di chiusura**

Attualmente è alla

versione 4.0 che ha standardizzato il concetto di fogli di stile (Cascading Style Sheets - css)

Una pagina prevede un'intestazione e un corpo compresi fra il tag <HTML> e </HTML>

- <HEAD>...</HEAD> definiscono l'intestazione (titolo, stili, meta, ..)
- <BODY>...</BODY> definisce il corpo del documento.

Dedicato a: Francesco Palmieri



Francesco Palmieri nato il 26 giugno 1965 a Salerno. È attualmente professore associato presso il Dipartimento di Informatica dell'Università degli Studi di Salerno. Ha conseguito la laurea in Scienze dell'Informazione, quella in Informatica e il dottorato di ricerca in Informatica presso l'Università di Salerno. Ha inoltre conseguito l'abilitazione all'esercizio della professione di Ingegnere dell'Informazione presso l'Università di Napoli Federico II. I suoi interessi scientifici sono focalizzati sulle reti di telecomunicazioni fisse e mobili, sulle tecnologie di trasporto e instradamento del traffico, sui sistemi di elaborazione distribuiti in rete, nonché sulla sicurezza, privacy e integrità delle comunicazioni in rete. All'inizio della sua carriera ha lavorato in aziende multinazionali del comparto telecomunicazioni, occupandosi di progettazione, gestione ed esercizio di sistemi di telecomunicazione e trasmissione su larga scala, ed in particolare di problematiche di instradamento e controllo del traffico nazionale e internazionale. Successivamente è stato responsabile, in qualità di direttore tecnico presso il centro Servizi Informatici, della gestione delle infrastrutture di rete e della sicurezza per l'Università di Napoli Federico II. È stato inoltre ricercatore universitario presso il Dipartimento di Ingegneria Industriale e dell'Informazione della Seconda Università di Napoli. Ha avuto un ruolo significativo nello sviluppo della rete Internet nel meridione d'Italia e, più in generale, delle reti della ricerca sull'intero territorio nazionale, come membro del Comitato Tecnico Scientifico Nazionale della Rete Italiana della Ricerca GARR. Ha contribuito inoltre attivamente alla sicurezza delle reti in Italia, come membro fondatore del Computer Emergency Response Team della Rete GARR. È stato membro del Tavolo Tecnico ICT4UNIVERSITY-Università Digitali, occupandosi della diffusione delle tecnologie VoIP tra le università italiane. Infine, ha partecipato a vari livelli di responsabilità, a importanti progetti finanziati di Ricerca/Sviluppo nel settore delle reti, nazionali ed internazionali. È Editor in Chief di una rivista scientifica internazionale, nonché membro di vari editorial board e guest editor per diversi special issues. È stato chair di convegni e membro di numerosi comitati di programma.

