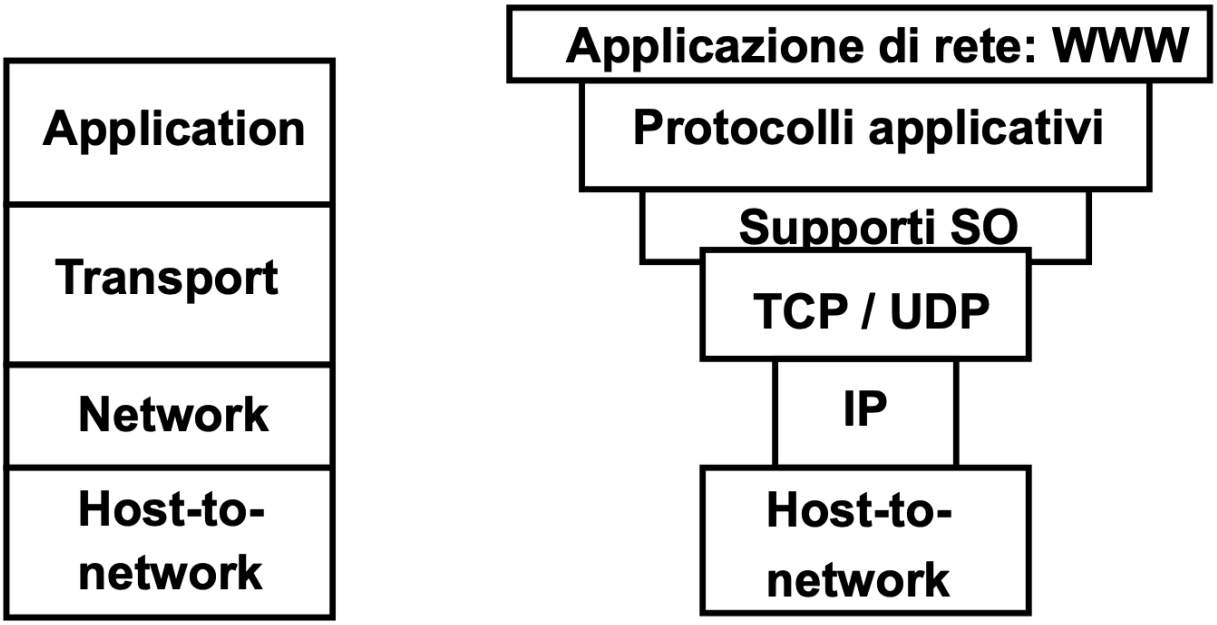


Il livello Host to Network affronta le problematiche di:

- interconnessione tra due o più host
- trasmissione dati tra host direttamente connessi
- connessione di un host a interne

> I servizi offerti da differenti protocolli h2n possono essere diversi

> L'unità minima trasmessa è chiamata FRAME

Modalità di trasmissione

Esistono diversi paradigmi di trasmissione:

- Unicast --> Comunicazione fra 1 e 1
- Multicast --> un mittente e più riceventi
- Anycast
- Broadcast

Tipi di collegamento

- Half-Duplex: un solo partecipante può usare il canale di trasmissione o/e quasi sempre è unidirezionale
- Full-Duplex: destinatario e mittente possono comunicare indipendentemente, è un canale bidirezionale

Il mezzo di trasmissione può essere analogico o digitale, spesso vengono modulate le informazioni digitali in analogiche.

Lan Ethernet

Rete LAN: rete in cui i nodi possono comunicare fra di loro tramite lo stesso protocollo H2N.

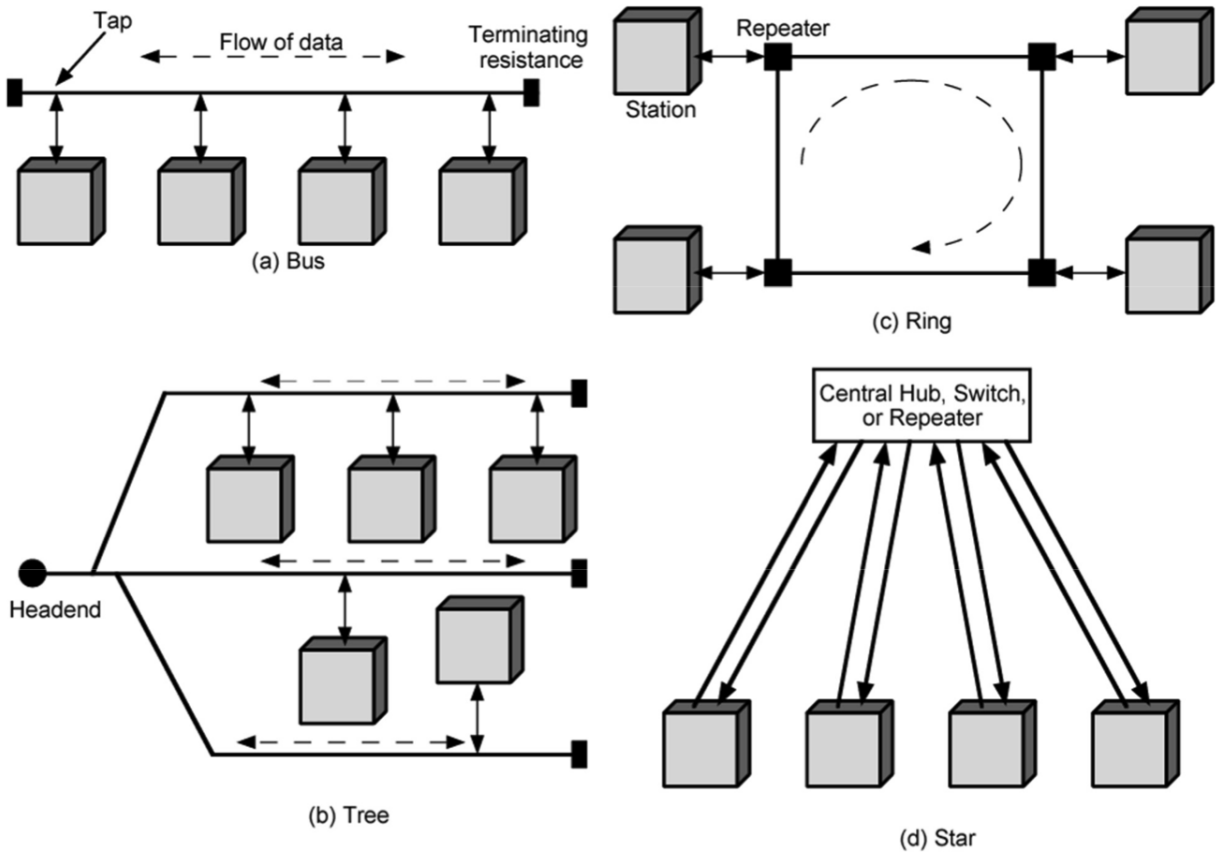
Il protocollo H2N è implementato all'interno di una scheda fisica **adattrice** conosciuta con il nome di *Network Interface Card* o **NIC**. Tutti i dispositivi per collegarsi hanno bisogno di una scheda di rete.

Le LAN costituiscono gli elementi fondamentali di accesso a Internet e sono dette **back end LAN** e possono essere collegate mediante **backbone LAN**:

- le back end LAN realizzano sistemi di medie dimensioni, interconnettendo server dispositivi di storage ecc...
- le backbone LAN servono per interconnettere diverse back-end LAN e devono garantire affidabilità ed elevata capacità di traffico

Topologia per LAN

A seconda dei contesti e dei protocolli impiegati possiamo individuare diverso topologie di LAN:

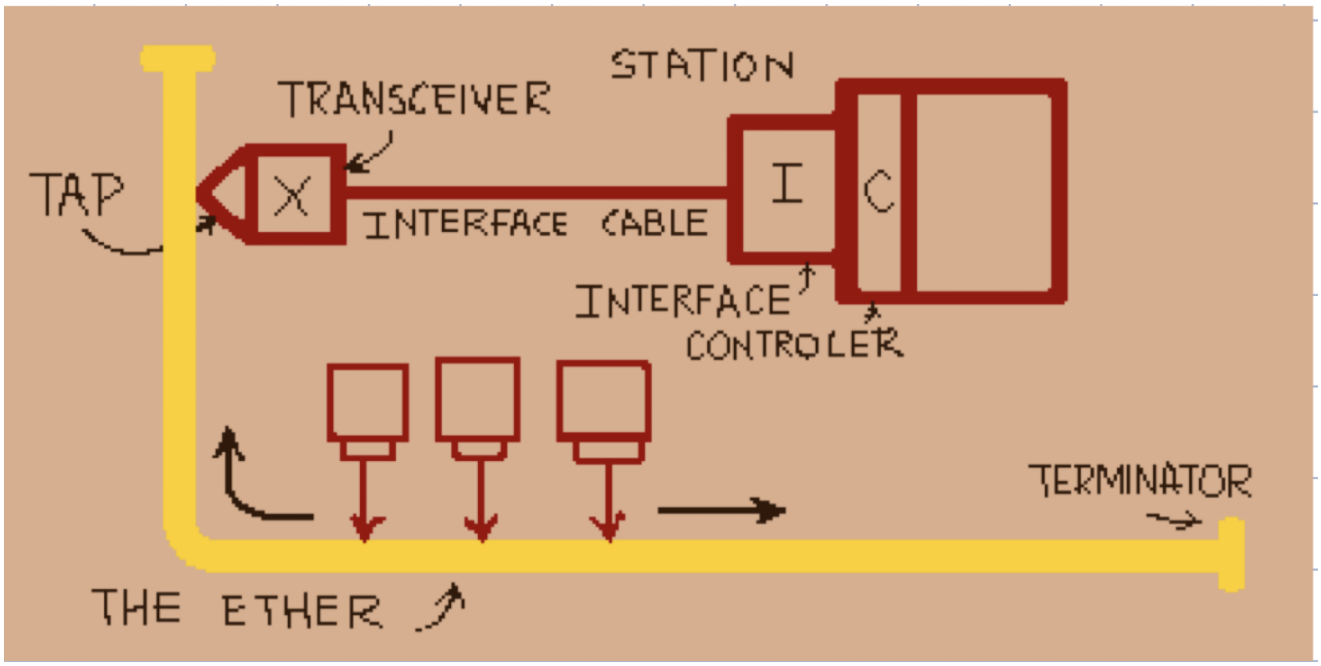


- **BUS**: Collegamento cablato condiviso, consiste in un cavo (dorsale) che collega tutti gli HOST. Ha un terminatore, per evitare il rimbalzo

- **Anello**:ogni host agisce come un ripetitore
- **Stella**: c'è un dispositivo intermedio centrale apposta per gestire il traffico di rete: ogni comunicazione passa attraverso questo dispositivo

Ethernet

Ethernet è stato pensato inizialmente per una tipologia a BUS, con velocità di trasmissione fino a 10Mbps.



Relativamente poco costosa, funziona bene e si integra perfettamente con i protocolli IP e TCP, è molto flessibile e si presta a diverse:

- **topologie** (metodi di connettere host alla rete)
- **tecnologie** (tecnologia del mezzo trasmissivo usato per le connessioni)

Il tipo di collegamento è di tipo **Broadcast**, ma la modalità di trasmissione (a livello logico quindi) è *unicast* (alcune comunicazioni speciali possono essere broadcast)

Indirizzo MAC

A livello Ethernet gli host utilizzano un indirizzo **hardware** o **Indirizzo MAC** (Media Access Control). In realtà il MAC si riferisce alla NIC, infatti ogni NIC ha un indirizzo univoco di `48 bit` tipicamente rappresentato da 6 coppie di numeri esadecimali. L'indirizzo MAC di un NIC è **univoco** e **permanente**.

> Esiste un solo indirizzo non assegnabile: `FF:FF:FF:FF:FF` che è quello di broadcast.

È un sistema di indirizzamento di tipo `piatto`: i bit non hanno importanza in base alla loro disposizione. Solitamente i primi 3 byte sono tipicamente associati al produttore e non è una buona idea fidarsi dell'indirizzo MAC per l'autenticazione.

Quando un host vuole trasmettere, inserisce nel **frame** l'indirizzo MAC del destinatario. Se il MAC destinazione di un pacchetto corrisponde al MAC di un dispositivo allora la NIC fa passare il pacchetto e lo manda al sistema operativo, altrimenti lo scarta.

Frame Ethernet

I pacchetti scambiati a livello H2N vengono detti **frame**. Indipendentemente dalla tipologia dei mezzi e dalla velocità di trasmissione, tutte le tecnologie Ethernet fanno uso dello stesso formato per il FRAME che trasmettono.

- Preambolo e CRC sono legati al livello fisico
- Gli altri sono legati al livello data-link

Preambolo

Sono `8 byte` sempre uguali:

- i primi 7 sono `10101010`
- l'ultimo è `10101011`

Questo serve per attivare gli adattatori dei ricevitori e sincronizzare i clock, serve per preparare alla comunicazione. I due `11` finali servono per indicare la fine della sincronizzazione

Indirizzi

Subito dopo il preambolo ci sono `6 byte` che identificano il destinatario, e dopo altri `6 byte` che identificano il mittente:

- quando una NIC riceve un frame ethernet con indirizzo di destinazione diverso dal proprio, o dall'indirizzo broadcast della LAN, lo scarta

Tipo

Campo di `2 byte`, serve a gestire logica di multiplazione del livello rete. In base tipo di protocollo Ethernet gestisce in modo diverso il pacchetto:

- il campo tipo serve all'adattatore per sapere quale dei protocolli dello strato di rete debba essere passato il campo dati di ciascun frame

Dati

Contiene i dati reali (solitamente il datagramma IP). L'unità massima di trasferimento si dice **MTU** (Maximum Transfer Unit) per Ethenet è di `1500 byte`. La dimensione

minima del campo dati è di `46 byte` (in caso contrario il campo viene riempito di dati che poi verranno rimossi *stuffing*)

> Esiste una policy che stabilisce che l'MTU minimo è di 600 byte per poter essere trasparente, se no bisogna frammentare a livello locale

> L'MTU deve essere univoco a livello di rete locale

CRC

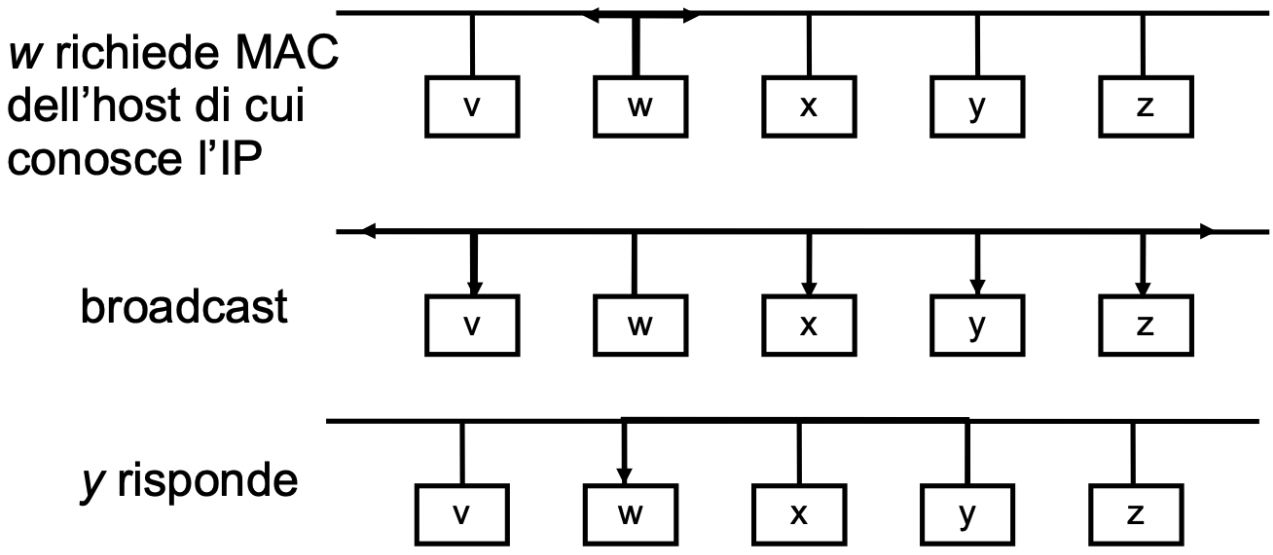
Controllo di Ridondanza Ciclica (`4 byte`): serve per sapere se il pacchetto arrivato è corretto oppure è corrotto. Il destinatario calcola il CRC sul pacchetto ricevuto e lo confronta con quello inviato: se sono uguali allora il pacchetto è sano, altrimenti è presente un errore

Protocollo ARP

Risolve dinamicamente la corrispondenza tra IP address e Indirizzo MAC (**Address Resolution Network**). Utilizza due tipi di messaggi ARP:

- **richiesta**: contenente l'indirizzo IP del destinatario
- **risposta**: contenente il corrispondente indirizzo MAC

> ARP utilizza il broadcast nella richiesta



1. Inizialmente ARP invia un messaggio broadcast (sapendo già l'ip di destinazione)
2. richiede tramite questo messaggio il MAC associato
3. se sei l'host interessato rispondi inviando il tuo MAC address

Cache ARP: Per ridurre il traffico sulla rete causato dal protocollo ARP, ciascun host effettua un caching temporaneo delle risoluzioni IP/MAC nella sua tabella di instradamento. Se l'input è l'indirizzo IP:

1. controlla se l'IP è nell'ARP table
2. se assente o con TTL scaduto: esegue il protocollo ARP

3. Uso il MAC address ottenuto nel payload della risposta come MAC address di destinazione. La mancata risposta è interpretata come mancata presenza dell'host

> le richieste ARP di rinnovo sono UNICAST

> Esiste anche il protocollo RARP che fa esattamente il contrario, ma è deprecato

Dentro al payload dei pacchetti ARP c'è l'indirizzo IP

Accesso al mezzo trasmissivo CSMA/CD

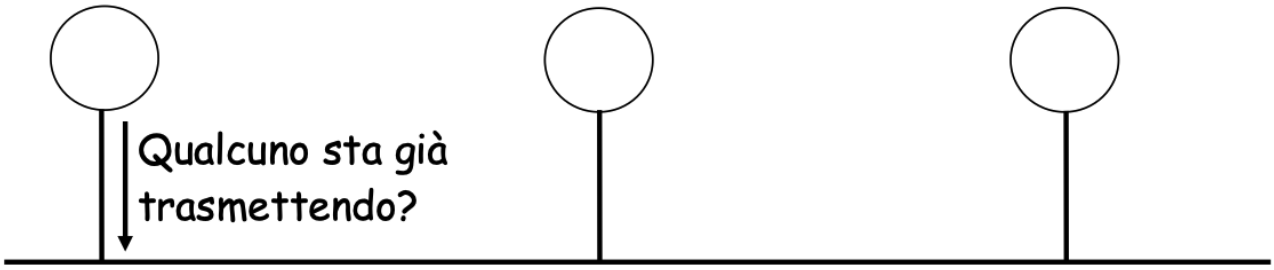
I frame Ethernet vengono trasmessi dagli host collegati allo stesso segmento di LAN su un canale condiviso broadcast. È quindi necessario un protocollo di accesso al mezzo per coordinare le trasmissioni sul canale condiviso in modo da evitare, se possibile, collisioni (ovvero gestirle nel caso avvengano).

Per questo nasce il protocllo **Carrier Sense Multiple Access with Collision Detection**:

- È un protocollo ad accesso casuale
- completamente decentralizzato

Carrier Sense

CS = Carrier Sense (rilevazione della portante). Ogni host che deve trasmettere ascolta il bus e decide di trasmettere solo se lo trova libero (**listen before talking**).

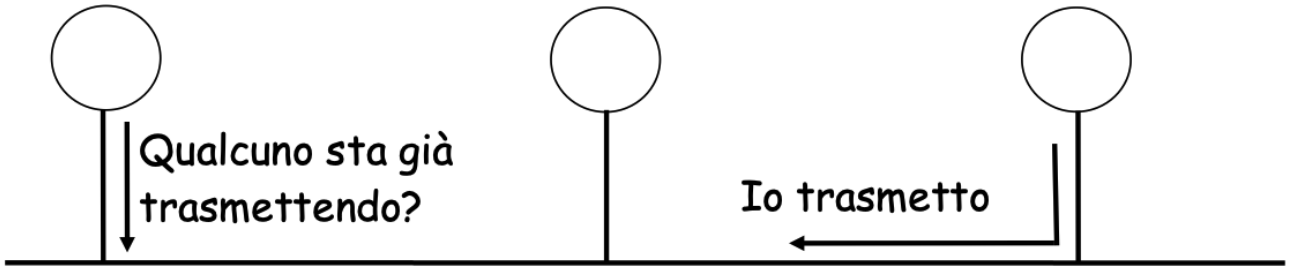


Due frame consecutivi vengono sempre distanziati per un tempo che corrisponde alla lunghezza del pacchetto dati più piccolo. Questo intervallo è detto **Inter Frame Gap (IFG)**: serve a garantire agli host in ascolto sulla rete di poter distinguere la fine della trasmissione di un frame dall'inizio della trasmissione successiva.

> prima di poter trasmettere il primo frame un host deve riscontrare che il canale sia libero per la durata di un IFG

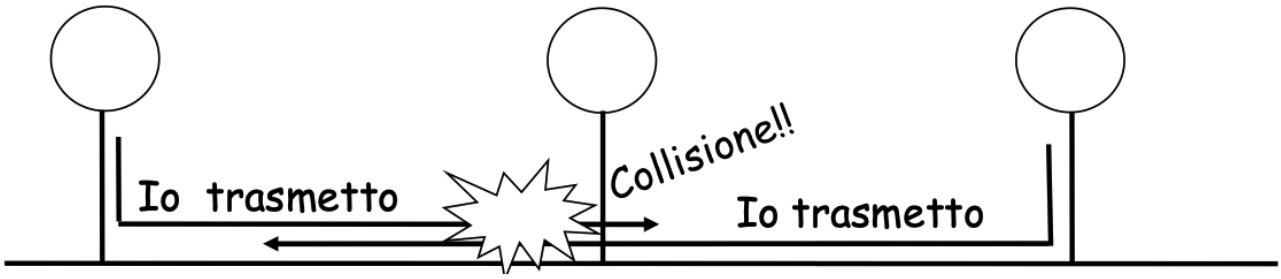
Multiple Access

MA = Multiple Access (accessi multipli). Nonostante la funzione di *Carrier Sense*, essendo un protocollo decentralizzato, due host potrebbero decidere di trasmettere in contemporanea. Essendo il tempo di propagazione del segnale sulla rete non nullo, un host può decidere di trasmettere anche se un altro ha già iniziato a trasmettere



Collision Detection

CD = Collision Detection (rilevamento della collisione). Se si verifica una sovrapposizione di trasmissioni si ha una collisione. Per rilevare una collisione ogni host mentre trasmette, ascolta i segnali sul mezzo, confrontandoli con quelli da esso generati. Se viene rilevata una collisione, l'host **interrompe la trasmissione**



A seguito di una collisione:

- Ogni host sospende la trasmissione e trasmette un segnale di **JAMMING** per avvisare della collisione gli host
- Questo assicura che ogni host rilevi la collisione anche nel caso in cui la collisione sia stata breve
- Gli host riprendono il tentativo di trasmissione dopo un ritardo (pseudo casuale) determinato mediante un algoritmo di **exponential back-off** fino a un massimo di 16 ritrasmissioni

Dispositivi di rete

I principali dispositivi di rete di livello 1-2 sono:

- Hub --> Livello 1
- Switch --> Livello 2
- Bridge --> Livello 2

> Il termine Bridge identifica una funzionalità logica che può svolgere un dispositivo intermedio

Hub

Dispositivo di livello fisico dotato di 2 o più interfacce. Inoltra un segnale elettrico ricevuto su una porta su tutte le altre porte. Gli unici benefici che comporta un Hub sono:

- Aumento della distanza coperta da una LAN (fa da ripetitore)
- Resistenza ai guasti

Rimangono infatti le criticità di un BUS, ma ha performance migliorate

> **Dominio di Collisione**: Definisce quali host non possono parlare contemporaneamente

Switch

Sono dispositivi fisici che implementano un *Inoltro Selettivo* dei frame nelle proprie porte: questo riduce il dominio di collisione, quasi annullandolo, migliorando le performance.

Applica una logica di funzionamento di tipo **Store and Forward**, memorizzando, analizzando e poi inoltrando i frame.

> Lo switch ha anche quindi una memoria, che si può riempire, in questo caso si comporta da Hub con chi non conosce

Esistono switch che applicano una logica di tipo **cut-trought** che inoltrano il pacchetto senza aspettare che tutto il frame sia arrivato al commutatore, è sufficiente che la parte contenente il MAC address di destinazione sia stato letto.

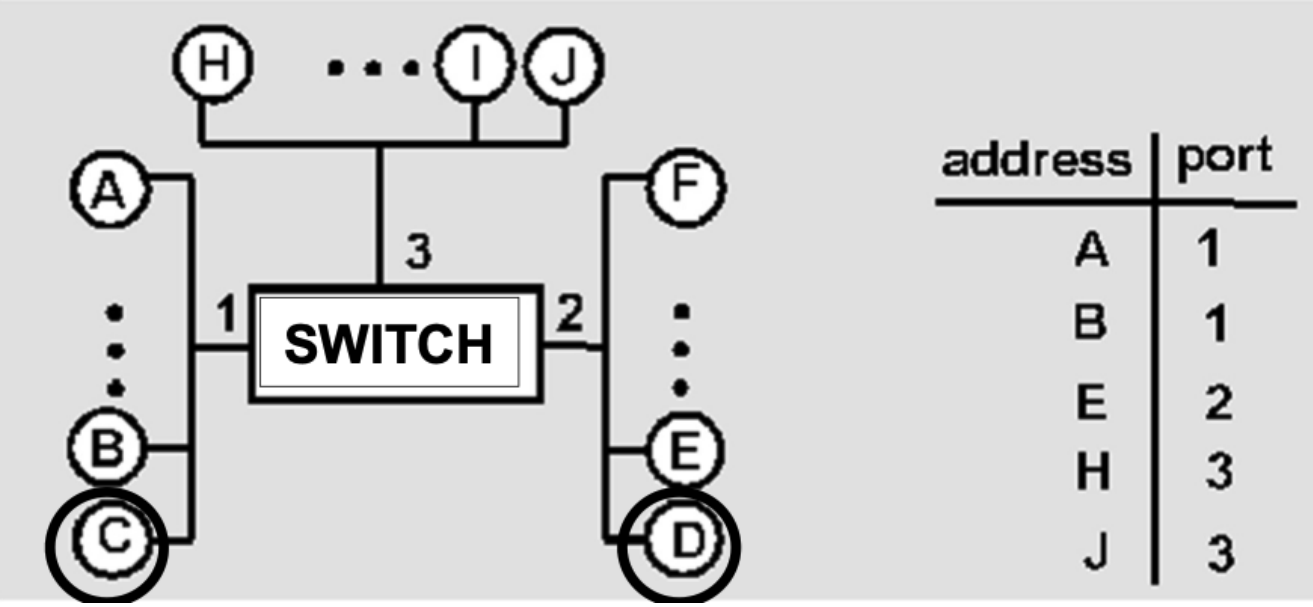
Filtraggio e inoltro

- **Filtraggio** --> non invia i frame a parti della rete che non sono interessate
- **Inoltro** --> ha una logica di come raggiungere un destinatario. Per l'inoltro lo switch fa uso del MAC address.

1. Quando riceve un pacchetto legge il MAC di destinazione: se non lo ha mai visto lo inoltra su tutte le porte (tranne al mittente)
2. Auto apprende --> legge il MAC del mittente e lo assegna a una porta in una **tabella di instradamento**

> lo switch è un dispositivo passivo, non genera traffico di rete

Le tabelle di instradamento hanno un TTL per prevenire la saturazione di esse. Ovviamente in caso di risposta o se si conosce già la destinazione il pacchetto non viene inviato nuovamente a tutti, ma solo al legittimo destinatario.



Bridge

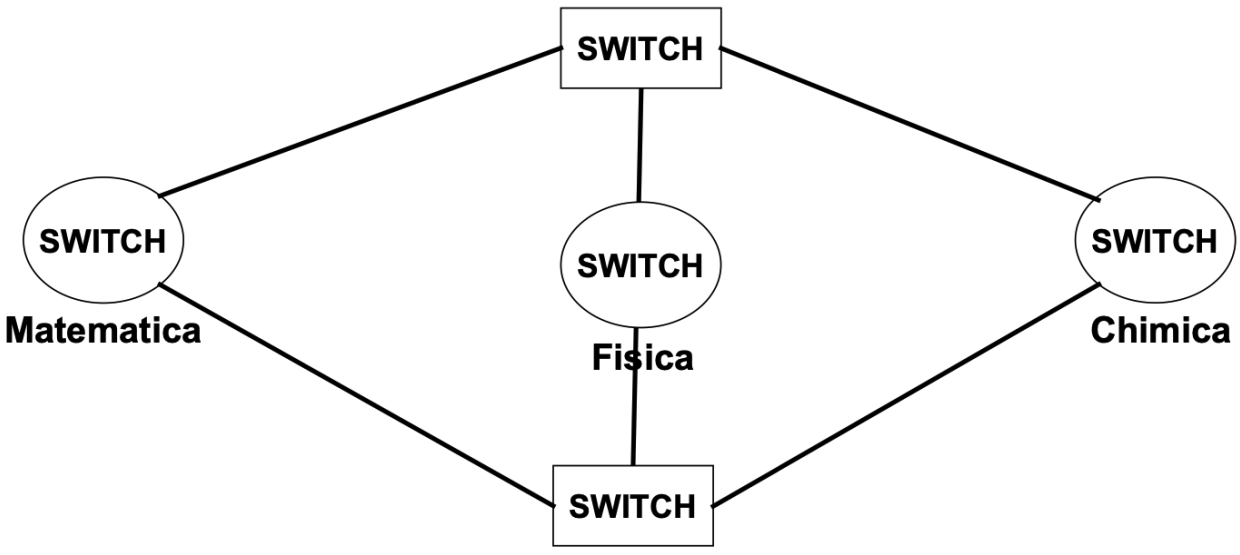
È un dispositivo di livello 2, esamina l'heade dei frami e li inoltrano selettivamente sulla base del MAC address di destinazione, è analogo allo switch ma può supportare più mezzi fisici.

Esistono due tipi di bridging:

- **Trasparente** --> collega due tecnologie fisiche che impiegano lo stesso sistema di indirizzamento di livello 2
- **Non trasparente** --> lo switch implementa logiche per "convertire2" i protocolli di LV2, compresi indirizzi HW

Affidabilità delle LAN

Per aumentare l'affidabilità di una rete è necessario avere **ridondanza**, ovvero avere **cammini alternativi** della sorgente alla destinazione



Tuttavia avendo cammini multipli possono crearsi cicli e conseguentemente gli switch potrebbero moltiplicare i frame. La soluzione è l'utilizzo di un protocollo chiamato **Spanning Tree Protocol**:

- permette di individuare link ridondanti in modo automatico e dinamico
- per funzionare deve essere supportato ed attivato su tutti gli switch della rete locale interessata

Spanning Tree Protocol

Si basa sulla generazione di traffico aggiuntivo da parte degli switch: *Bridge Protocol Data Units*. Si basa sull'identificazione di un **Root Bridge** (o switch):

- ad ogni switch è assegnato un numero identificativo chiamato bridge priority
- Lo switch con il valore minore è il Root Switch
- L'obbiettivo del protocollo è mantenere attive solo le porte che permettono a ciascuno switch di comunicare con il root switch con il costo minore

---

> Non si utilizza una unica grande LAN perchè ci sarebbe un dominio di broadcast enorme e unico, oltretutto tutti i dispositivi dovrebbero condividere la stessa larghezza di banda

Organizzazione interna di Internet

- Gli host terminali sono connessi a **Internet Service Provider locali** (ISP)
- Gli ISP locali sono collegati a **ISP regionali** (tipicamente nazionali)
- Gli ISP regionali sono collegati a **ISP internazionali** detti **NATIONAL BACKBONE PROVIDER**

Infrastruttura di Internet

Ciascun ISP locale ha dei **Point-Of-Presence** (POP) tramite cui si collegano gli utenti privati o aziendali. A loro volta gli ISP locali si connettono agli ISP regionali mediante linee tramite i NAP (Network Access Point).

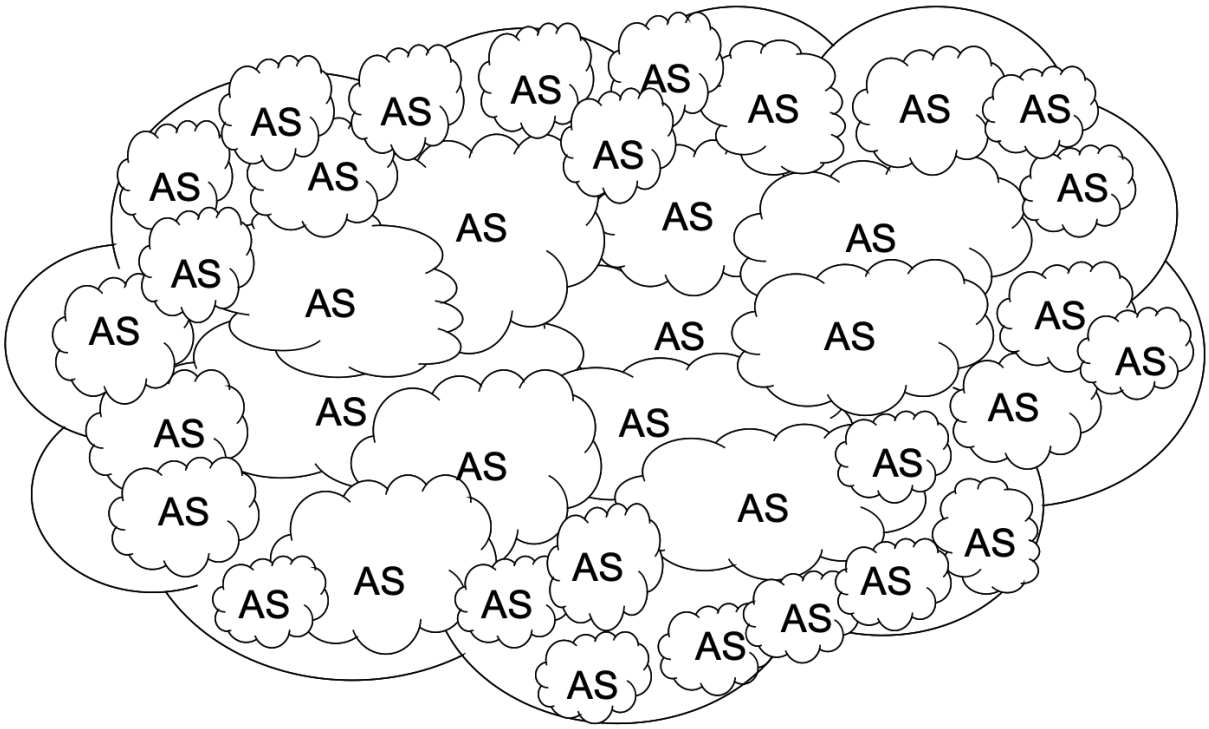
Gli ISP regionali noleggiano accesso ai NBP ovvero provider intercontinentali

Autonomus System

Internet non è che un insieme di router "sparsi" nel mondo che sono interconnessi tra loro in modo casuale.

> I router sono aggregati in regioni chiamate **Autonomus System (AS)**: un insieme di reti, di indirizzi IP e di router sotto il controllo di una organizzazione (o consorzio)

Dal punto di vista gestionale Internet è un insieme di AS



Collegamenti utenze

Si utilizza il protocollo PPP (point-to-point) per collegamenti dedicati

Protocollo PPP

Tipico collegamento **punto-punto**: un mittente, un destinatario. Molto più semplice da gestire di un link broadcast:

- non c'è Media Access Control e non ci sono problemi di conflitto
- non c'è necessita di un indirizzamento MAC esplicito

Il protocollo PPP (**point-to-point protocol**) è lo standard attuale per gestire questo tipo di collegamenti:

- supporto multiprotocollo
- supporto all'autenticazione
- rilevamento degli errori
- supporto a indirizzamento IP dinamico

Componenti principali:

- Metodo di incapsulazione per pacchetti di diversi protocolli
- **Link Control Protocol** per stabilire, configurare e monitorare la connessione PPP
- **Network Control Protocol** per configurare i diversi protocolli a livello network che vengono trasportati

Orientato alla conenssione

- Fase 1: definizione della connessione

- Fase 2: Autenticazione
- Fase 3: configurazione del protocollo di rete che si utilizzerà
- Fase 4: terminazione della connesione