# Livello host to network

Lo scopo di questo livello è quello di collegare due nodi che abbiano un **canale** in comune. Nel modello ISO/OSI il livello h2n sono il livello 1 e 2. Nella realtà questi livelli sono profondamente interconnessi e, di fatto, indistinguibili.

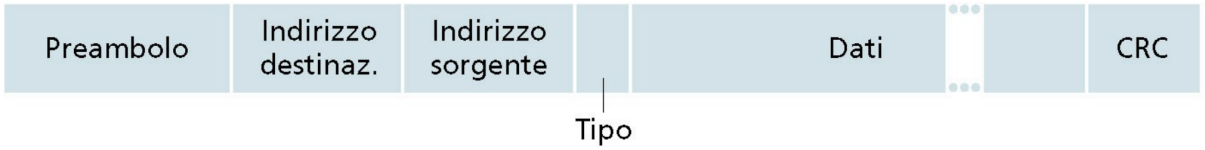
Lo standard **de facto** h2n è *Ethernet,* per connessioni via cavo. Tipicamente Ethernet è indicato come lo standard 802.3.
Ovviamente per connessioni via etere lo standard è LAN Wireless.
L'unità di dato **trasmesso** dal livello h2n è il **frame**.

# 1. Ethernet

Lo standard Ethernet è una soluzione al problema di collegamento h2n molto efficiente, poiché estremamente scalabile e poco costosa.
Ethernet si basa esclusivamente sulla **comunicazione broadcast**: al momento di trasmissione di un pacchetto, tutti gli host ricevono tale pacchetto.
Serve un modo, quindi, per **indirizzare** i pacchetti che sto inviando: entra in gioco il MAC address.

Ogni NIC (l'interfaccia di rete) ha un MAC address da 48 bit, univoco e permanente. Ogni scheda di rete ha un indirizzo **univoco** (per produttore).
FF:FF:FF:FF:FF:FF è l'indirizzo MAC broadcast.

Un frame ethernet è sempre composto da:




- il preambolo è sempre di 8B, i primi 7 hanno tutti valore 10101010, l'ultimo byte 10101011, che servono per sincronizzare le due NIC.
- indirizzo di dest e di src sono due MAC
- il tipo è 2B e serve all'adattatore (NIC) per sapere a quale dei protocolli dello strato di rete debba essere passato il campo dati di ciascun frame ricevuto
- la parte "dati" contiene la dimensione dei dati e i dati stessi (1500B massimi generalmente, 9000B per i jumbo frame). Il payload dev'essere almeno di 46B.
- CRC è un campo utilizzato per la verifica degli errori all'interno del frame.

## 1.2 ARP

Il protocollo ARP (Address Resolution Protocol) si occupa di mappare i MAC address agli indirizzi IP (da IP a MAC).
Prevede due tipi di messaggio:

- richiesta: contiene l'IP del destinatario
- risposta: contiene il MAC corrispondente

Poiché ARP lavora in broadcast, l'utilizzo della rete da parte di questo protocollo è abbastanza intensivo. Per questo motivo, l'associazione di un MAC ad un indirizzo IP viene cacheata all'interno della tabella ARP di ciascun host.
La cache ARP è memorizzata nella **RAM** dell'host di riferimento e l'implementazione della struttura dati è fatta nel **kernel**.

Oltre a ARP esiste RARP, che fa l'esatto opposto, traduce un MAC address in IP, con meccanismi analoghi.

### *Pacchetti ARP/RARP*

- **Payload di 28 bytes**
- **Hardware type (ht) tipo di protocollo livello fisico**
  - Ethernet=1
- **Network protocol type (pt) tipo di protocollo livello rete**
  - IP=0x800
- **Hardware address size (hs)**
- **Network protocol address size (ps)**
- **Operation (op)**
  - 1 ARP richiesta
  - 2 ARP risposta
  - 3 RARP richiesta
  - 4 RARP risposta

**Caso comune: IP su Ethernet**

- **Sender HW address**
- **Sender net address**
- **Receiver HW address**
- **Receiver net address**

| ht 2 | pt 2 | hs 1 | ps 1 | op 2 | snd hw add 6 bytes | snd net 4 | rcv hw add 6 bytes | rcv net 4 |
|---|---|---|---|---|---|---|---|---|

## 1.3 Interconnessione di LAN

Ci sono svariati apparati di rete che permettono di interconnettere reti locali fra di loro:

- hub: non lavora in store and forward, pertanto forza tutti la rete a lavorare alla stessa velocità (ovvero la velocità del dispositivo più lento). Un altro problema dell'hub non **isola il dominio delle collisioni**: il traffico di un host viene propagato su tutte le porte dell'hub.
- bridge: dispositivo che lavora in store and forward che inoltra selettivamente (in base al mac address destinatario) i messaggi alle varie porte. A differenza dell'hub il bridge può ricevere un frame intero e decidere a chi mandarlo. In caso di collisione, che diventa **molto meno probabile** rispetto all'hub, dato che può bufferizzare

l'interezza del frame, l'implementazione di CSMA/CD viene naturale. La tabella di filtraggio di un bridge ha una dimensione massima che, se viene raggiunta, fa regredire il comportamento del bridge a quello di un hub.
- switch: bridge "on drugs". Ha molte porte e permette la comunicazione parallela su più porte. Operano in modalità **store and forward** e **cut through** (si aspetta la parte contenente l'indirizzo MAC e si instrada il pacchetto, senza aspettarlo per intero).
- switch di livello 3

### Spanning tree

Uno spanning tree è una particolare topologia di rete che garantisce ridondanza senza cicli. Si realizza disabilitando determinate interfacce degli apparati di rete.

## 1.4 VLAN (802.1Q)

Le VLAN (Virtual LAN) permettono di creare virtualmente più reti locali e *taggare* il traffico in modo tale che un dominio broadcast corrisponda ad una data VLAN.
In questo modo è possibile utilizzare una stessa infrastruttura **fisica** e suddividerla in contesti differenti, riducendo i domini di broadcast delle varie reti virtuali che vado ad implementare, aumentando la flessibilità e riducendo i costi.
Gli switch che supportano le VLAN sono chiamati *managed*.

Le VLAN possono essere realizzate mediante due meccanismi principali:
- port based: ogni porta è battezzata come appartenente ad una data VLAN;
- tagged: è possibile taggare una determinata porta come appartenente ad una data VLAN via software (tramite lo standard 802.1Q). Ogni frame avrà al suo interno a quale VLAN farà riferimento.

Per lo standard 802.1Q lo switch deve poter essere in grado di smistare il traffico in base a tre principali funzioni:
- **ingress**: il bridge deve essere in grado di capire a quale VLAN appartenga un frame in ingresso da una porta;
- **egress**: il bridge deve essere in grado di poter trasmettere il frame in uscita in modo che la sua appartenenza alla VLAN venga correttamente interpretata da altri bridge a valle;
- **forwarding**: il bridge deve conoscere verso quale porta deve essere inoltrato il frame verso destinazione, in funzione della VLAN di appartenenza.

In base ai frame **ingress**, associo un determinato frame ad una VLAN e riesco a farle uscire sulla stessa VLAN tramite la funzione di **egress**. Tramite la funzione di **forwarding** lo switch è in grado di scegliere su che porta mandare tale frame.

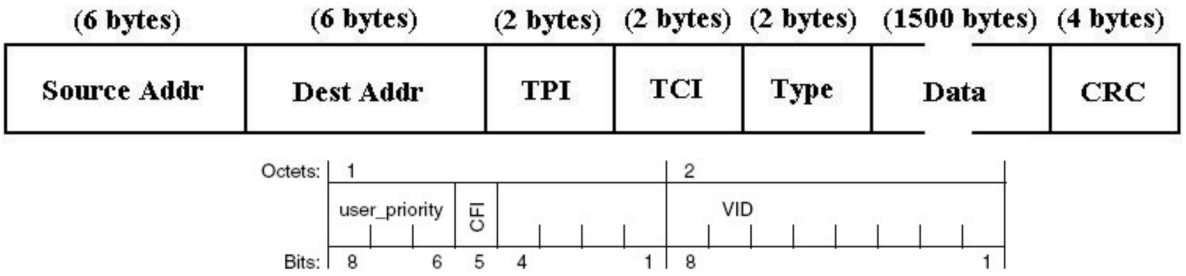
### 1.4.1 Port based VLAN

Tutte le porte lavorano con traffico **untagged** e le porte vengono assegnate staticamente ad una data VLAN.
Le funzioni di egress/ingress sono praticamente l'associazione del traffico ad una porta e niente di più, mentre la funzione di forwarding praticamente è assente, dato che lo switch viene partizionato fisicamente.

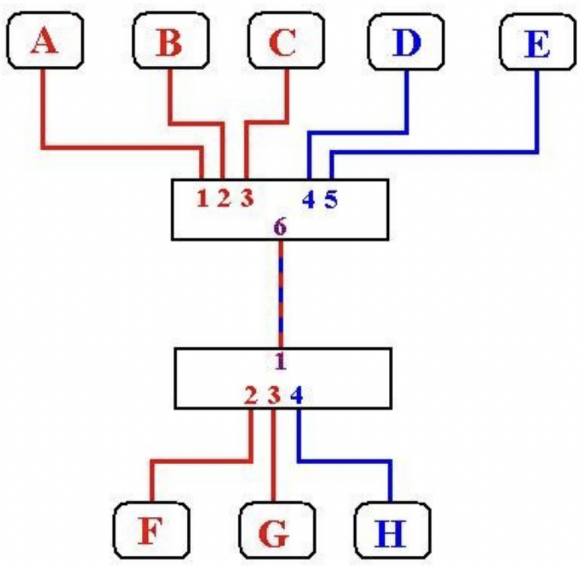
### 1.4.2 Tagged VLAN

Al frame ethernet viene assegnato un identificatore di VLAN e quindi il problema della separazione fisica non esiste. Non serve quindi collegare fisicamente apparati di una determinata VLAN a specifiche porte.
Viene modificato il campo **type** del frame ethernet nel seguente modo:

- TPI (Tag Protocol Identifier): due bytes di valore 81 00 che identificano il frame come frame 802.1Q
- TCI (Tag Control Information): due bytes che trasportano le informazioni sulla tag
  - i primi tre bit (user priority) indicano l'eventuale livello di priorita' del frame
  - il quarto bit (CFI) vale 1 se il frame proviene da una LAN token ring
  - i restanti 12 bit (VID) trasportano la VLAN tag (da 0 a 4095)
    - i valori 0 e 4095 sono riservati e non vanno utilizzati come VLAN ID




Associare un frame alla VLAN è compito della funzione **ingress**: se un frame ha un tag, la VLAN si legge dai campi specifici. Se non è presente un tag, gli switch managed assegnano la VLAN 0 a tutti i frame non taggati.
N.B: la VLAN 0 è la VLAN di partenza con la quale vengono taggate tutte le porte quando lo switch managed non è configurato.
La funzione **egress** si occuperà di togliere o meno il tag dal frame (in base a come lo switch è configurato - port based o managed).




Il link fra i due switch, quando devono comunicare usando più VLAN in modalità tagged, utilizzano un cavo di tipo **trunk**, che trasporta VLAN prefissate (che vengono configurate).

Supponendo che A faccia una query ARP su G. La funzione ingress dello switch in alto capisce che è arrivato un frame sulla porta 1, pertanto la funzione di forwarding dice di mandare il frame su tutte le porte della VLAN rossa. La funzione egress prende il frame e lo inoltra su tutte le porte corrispondenti che lavorano in modalità port based (2,3).

Cosa succede sulla porta 6? Il frame è associato alla VLAN rossa, pertanto la funzione egress, dato che la porta 6 funziona in modalità **trunk**, tagga il frame con la VLAN rossa. A questo punto, sulla porta 1, la funzione ingress rileva il tag “VLAN rossa” sul frame e lo associa a tale VLAN. La funzione forwarding associa questo frame alle porte 2,3 e la funzione egress butta tutto su tali porte **togliendo il tag** (poiché le porte 2,3 sono *access link*, ovvero funzionanti in modalità **port based**).

### 1.4.2 Porte ibride

Ad una porta possono essere associate sia una VLAN in modalità untagged e altre VLAN in modalità tagged.