

## INTRODUZIONE

Un *Rete* è un insieme di dispositivi collegati per condividere **risorse** e **servizi**.

Si collegano insieme dispositivi anche molto diversi tra loro (pc fissi, portatili, cellulari, stampanti di rete, HDD di rete, etc) per aumentare le potenzialità di ogni singolo **host** (ciascuno dei dispositivi).

Le risorse che possono essere condivise possono essere **hardware** (ad esempio uno **stampante**) o software (**servizi**). Alcuni dei servizi che possono essere condivisi in una rete di computer:

*World Wide Web:* Il **server web** condivide un *sito internet* ovvero pagine scritte in html (ipertesti), php e javascript, inviate ai client: una applicazione detta **browser** (Internet Explorer, Mozilla Firefox, Google Chrome, Safari)

I computer connessi alla rete condividono quindi un servizio di navigazione tra pagine web.

Protocolli di riferimento: http, https (sicuro)

*Posta Elettronica:* il **server di posta** fornisce il servizio di gestione ricezione e invio di email. I client accedono a questo servizio in due modi:

- con un'applicazione client (**client di posta**): Outlook, Mozilla Thunderbird, Mail (Mac OS X)  
 protocolli di riferimento: pop3 (ricezione), smtp (invio)
- **webmail**: attraverso il servizio www collegandosi tramite un browser al sito internet del servizio di posta (gmail, yahoo, libero, hotmail etc).

*FTP – File Transfert Protocol:* Servizio di trasferimento file. Diversi client possono caricare/scaricare file da un server. Applicazioni di riferimento: *FileZilla*.

Protocollo di riferimento: FTP

*Cloud Storage* Servizio di salvataggio dati “nel cloud”. Un server remoto mette a disposizione una spazio su disco per il salvataggio dei dati di un utente registrato.

Vantaggio: si può accedere ai dati da qualsiasi computer connesso alla rete (tramite l'autenticazione sul server). E' possibile fornire l'accesso ai propri dati anche ad altri account

Esempi: Dropbox, Google Drive, iCloud (Apple), OneDrive (Windows)

*File Sharing* Servizio di condivisione file. E' un servizio *peer-to-peer*, senza server. Ogni client mette a disposizione della rete alcuni file. Ogni host può dunque cercare e scaricare file dai client che lo hanno messo a disposizione.

Es. Emule, Torrent

*Video chiamata* Servizio di trasferimento della voce in tempo reale su canale dati (rete di computer). Tipicamente viene trasferita anche il flusso video. Il protocollo usato è il *VoIP* (Voice over Internet Protocol), acronimo usato anche per identificare il tipo di servizio.

Applicazioni di riferimento: Skype, Whatsapp (telefonate)

*Connessione Remota* E' un servizio che permette di connettersi ad un host (tipicamente un computer), da un dispositivi remoto. La connessione può utilizzare protocolli diversi: es. SSH, TELNET (non sicuro).

Applicazioni di riferimento: citiamo putty.exe come applicazione per SSH in ambiente windows.

Anche Desktop Remoto e Team Viewer rientrano in questo tipo di servizio.

Questi servizi possono aderire a due **modelli** differenti: *Client/Server* o *PeerToPeer*.

Nel modello Client/Server (C/S) il servizio è fornito da un host particolare detto **Server**, sul quale viene eseguita un'applicazione detta *demone* (daemon). Questa applicazione (sempre attiva in background) è quella che risponde alle richieste dei **Client** che vogliono accedere al servizio. Questo

è il caso del servizio WWW, fornito dal webserver che gestisce le pagine del sito o del servizio di posta elettronica.

Nel modello **PeerToPeer** non ci sono host che funzionano da server: ogni dispositivo agisce fornendo/ricevendo il servizio direttamente agli/dagli altri host. E' questo l'esempio del servizio di File Sharing (Torrent, Emule) nel quale ogni computer mette in condivisione i propri file, senza che questi siano caricati dapprima su un server.

SERVIZI	APPLICAZIONI CLIENT	SERVER	PROTOCOLLI
WWW (navigazione tra pagine web)	Browser: Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera:	Il Sito Internet che si vuole visitare (serverweb)	HTTP HTTPS (sicuro)
MOTORE DI RICERCA	Browser	Google, Bing	HTTP
POSTA ELETTRONICA	Applicazione di posta: Mozilla Thunderbird, Microsoft Outlook, Mail di Apple, applicazione GMAIL per cellulare  Webmail: il servizio è fornito attraverso un browser	Provider che fornisce il servizio: Gmail, Yahoo, Hotmail etc.	Ricezione: POP3, IMAP Trasmissione SMTP  HTTP
TRASFERIMENTO FILE	Es. Filezilla	Server FTP	FTP
CLOUD STORAGE	Applicazioni dedicate (su smartphone o PC Desktop)	Dropbox, iDrive, Goolge Drive, OneDrive.	
FILE SHARING	Es. Emule, uTorrent	<i>E' un servizio PeerToPeer, non ci sono server</i>	
VIDEOCHIAMATA	Skype, Whatsapp	Server di chi fornisce il servizio	VOIP
CONNESSIONE REMOTA SSH	Putty.exe	Server SSH	SSH

## COLLEGAMENTO AD UNA RETE INTERNET

Per collegarsi ad una rete internet un host ha bisogno di una configurazione adeguata ed in particolare di:

**INDIRIZZO IP:** è l'indirizzo che identifica l'host nella rete (vedi capitoli successivi)

**SUBNET MASK:** è una maschera che identifica la sottorete a cui appartiene l'indirizzo IP (cap. successivi)

**INDIRIZZO DI GATEWAY** è l'indirizzo IP del dispositivo (di solito un **router**) che permette l'accesso (l'invio di pacchetti) a reti esterne rispetto alla propria

**INDIRIZZO DNS:** è l'indirizzo del server DNS (tipicamente esterno alla rete) che traduce gli indirizzi url (ad esempio [www.calvino.ge.it](http://www.calvino.ge.it)) nell'indirizzo IP da contattare

Questi indirizzi possono essere configurati a mano o assegnati in automatico da un apposito servizio chiamato **DHCP** (Dynamic Host Configuration Protocol).

Per configurare gli indirizzi a mano su Windows 10 eseguire i seguenti passaggi:

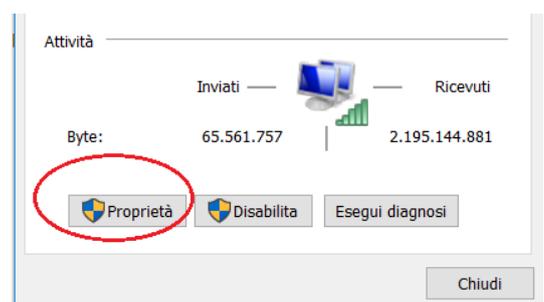
- 1) cliccare con il tasto destro sull'icono del collegamento alla rete che appare a destra nella barra delle applicazioni e scegliere "Apri centro connessioni di rete e condivisioni"



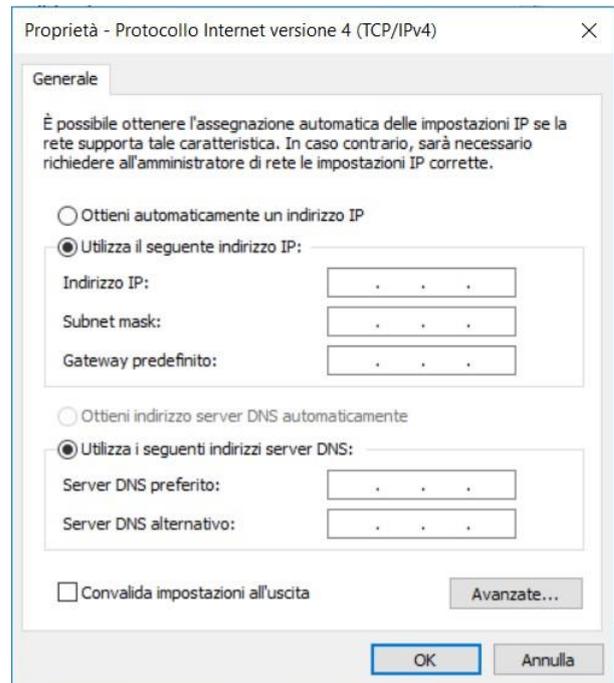
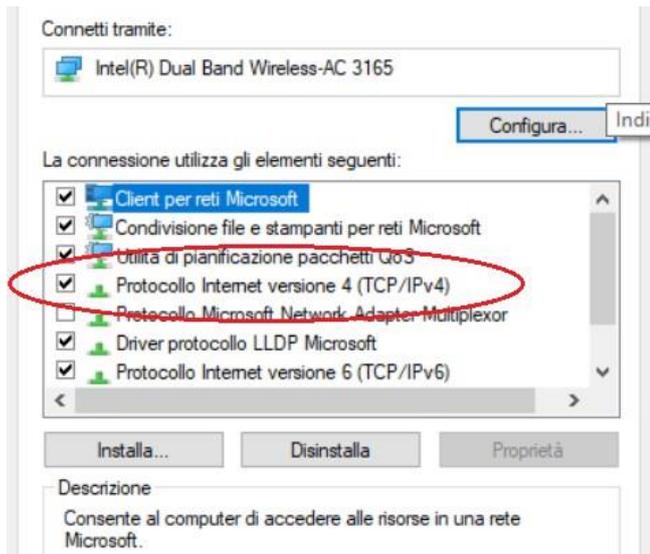
- 2) Cliccare con il tasto sinistro sul simbolo della connessione che si vuol configurare



- 3) Nella nuova schermata scegliere proprietà



- 4) Ora fare doppio clic su "Protocollo internet versione 4 (TCP/IP)" 5) In questa schermata potete configurare gli indirizzi o lasciarli configurare al server DHCP



Uno schema sufficientemente completo di accesso alla rete internet da casa propria (ad esempio per fare una richiesta al serverweb per vedere una pagina internet) è il seguente:

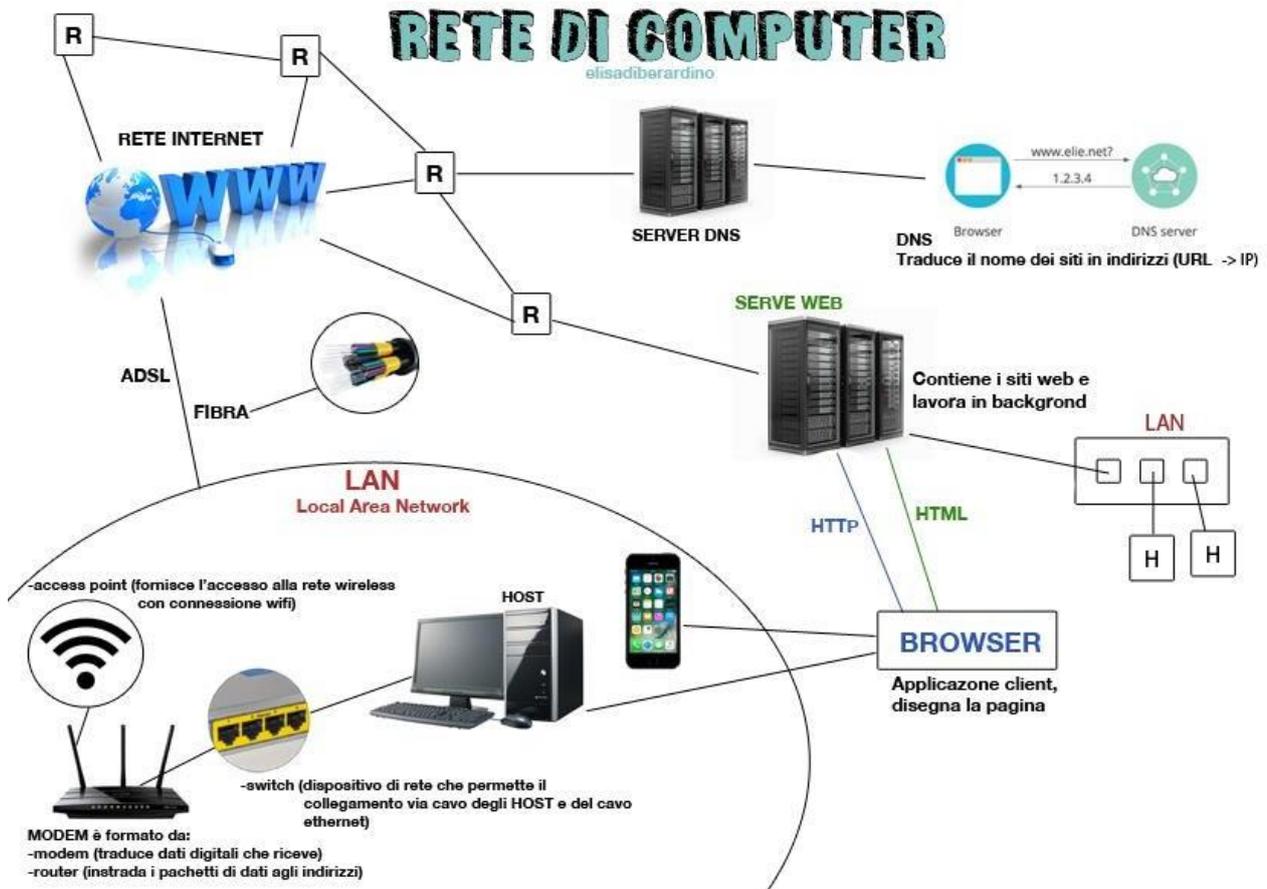


Figura 1© Elisa Di Berardino

## CLASSIFICAZIONE DELLE RETI

Esistono enti preposti alla **standardizzazione** (o alla regolamentazione) delle tantissime specifiche relative alle reti di computer. E' importante infatti riflettere alla dimensione davvero incredibile che ha raggiunto la rete Internet, al suo ruolo fondamentale nella vita di tutti e alla moltitudine di persone, e organizzazioni coinvolte in essa. E' fondamentale avere qualche tipo di regolamentazione degli standard per permettere a tutti di agire in modo coordinato.

Alcune organizzazioni particolarmente importanti sono:

**ISO** *International Standard Organization*. E' il più grande ente di standardizzazione mondiale, non governativo. Ne fanno parte gli enti nazionali (per l'Italia l'UNI)

**IEEE** *Institute of Electrical and Electronic Engineers*. E' un organismo privato (a scopo di lucro) per lo sviluppo e la standardizzazione soprattutto in ambito ingegneristico. Le sue pubblicazioni sono alla base di molti standard ISO

**W3C** *World Wide Web Consortium*. E' un consorzio che non fa standardizzazione ma fornisce raccomandazioni in ambito web che costituiscono uno standard *de facto*

### Classificazione delle reti per dimensioni

**PAN** *Personal Area Network*. Dimensioni: <100m Velocità: <10Mbit/s

Dispositivi solitamente ad uso personale (portatile, palmare, cellulare) tipicamente collegati wireless (WiFi o Bluetooth). Gli elementi sono collegati direttamente tra di loro, senza un elemento centrale.

**LAN** *Local Area Network* Dimensioni: <1Km Velocità: >10 Mbit/s

Rete di computer che si estende tipicamente su un edificio, *senza attraversamento di suolo pubblico*. I dispositivi appartengono di solito alla stessa azienda/organizzazione e sono collegati con cavi o wireless. Gli host sono collegati tra di loro tramite una **Switch** (se collegati con cavo) e tramite un **Access Point** (se collegati wireless).

Una rete LAN basata su collegamenti wireless si dice **WLAN** (Wireless LAN)

**MAN** *Metropolitan Area Network* Dimensioni: <10Km Velocità: >100Mbit/s (alta velocità)

Reti di computer privati che si estende attraversando suolo pubblico (utilizza infrastruttura pubbliche). Collega, ad esempio, cluster di computer della stessa organizzazione ma dislocati in edifici diversi.

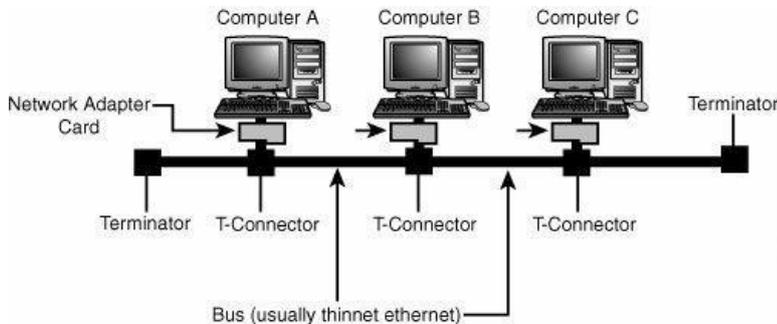
**WAN** *Wide Area Network* Dimensioni: >100KM Velocità: < 10Mbit/s (basse)

Sono reti estese su aree geografiche, utilizzando infrastrutture pubbliche per le telecomunicazioni (rete telefonica, satellitare etc). Poco veloci ma molto estese. La rete Internet è una WAN estesa su tutto il pianeta.

## Classificazione topologica

Le reti possono essere classificate in base al loro collegamento

### RETI A BUS



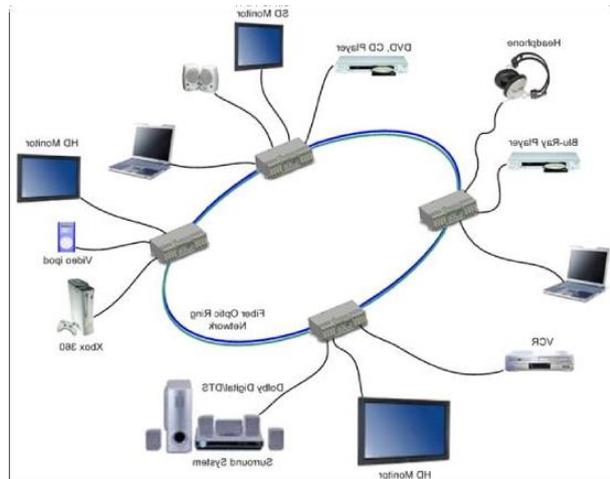
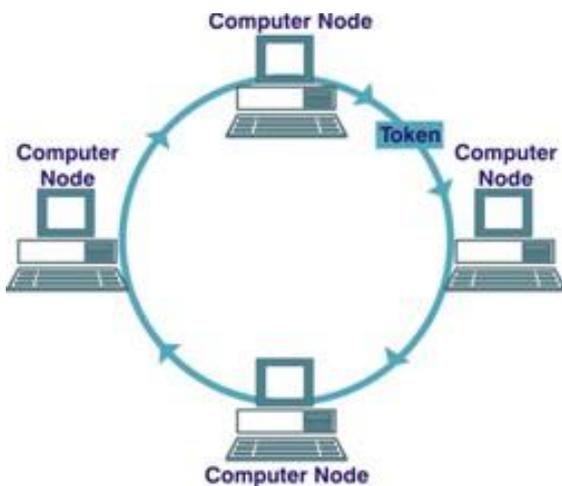
Tutti gli host sono collegati ad una *dorsale* o (**backbone**) tramite dei **tap** (schede o connettori per il bus).

Tutte le comunicazioni passano per la dorsale ma solo gli host interessati (destinatario) riconosce come proprio il messaggio. La dorsale dovrà essere terminata con dei particolari dispositivi (**terminatore**) necessari per regolarizzare i segnali elettrici circolanti sul bus

PRO	CONTRO
<ul style="list-style-type: none"> <li>• semplice da cablare: una volta posizionata la dorsale collego gli host con poco cavo</li> <li>• Utilizzo una comunicazione broadcast e non devo fare routing dei pacchetti</li> </ul>	<ul style="list-style-type: none"> <li>• Molto delicata: un eventuale danno alla dorsale o ai terminatori compromette il funzionamento di tutta la rete+</li> <li>• Deve prevedere algoritmi anti collisione dei pacchetti, in quanti tutti utilizzano lo stesso canale trasmissivo (la dorsale)</li> </ul>

Le prime reti LAN, realizzate con **cavo coassiale**, avevano una topologia a bus.

**RETI AD ANELLO**



Gli host sono collegati in un loop. L’invio di un messaggio (pacchetto) da mittente (MIT) a destinatario (DES) avviene utilizzando un particolare protocollo detto **token ring**

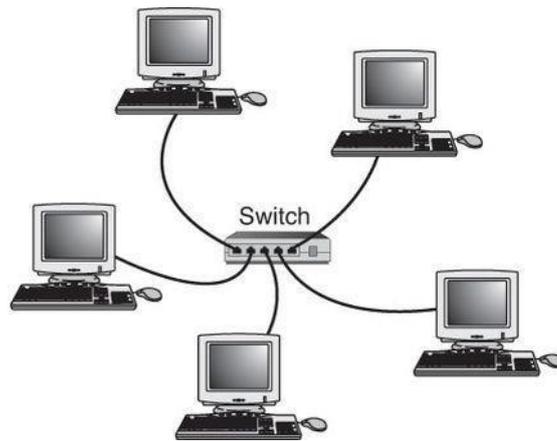
- 1) Un pacchetto speciale detto gettone (token) percorre l’anello passando da un host all’altro
- 2) Chi vuole trasmettere un messaggio (MIT) interrompe il gettone e invia sull’anello un pacchetto così composto

MIT	DES	MESSAGGIO
-----	-----	-----------

- 3) Il pacchetto percorre l’anello passando da host all’altro. Viene ignorato dagli host che non sono il destinatario
- 4) Il destinatario (DES) riceve e processa il messaggio e invia un particolare pacchetto di **acknowledge (ACK)** al mittente, utilizzando lo stesso formalismo del precedente pacchetto.
- 5) Il pacchetto ACK raggiunge il mittente passando di host in host
- 6) Ricevuto il pacchetto ACK il mittente rimette in circolo il gettone

<p>Questo protocollo ha poi alcuni casi particolari nel caso di problemi di comunicazione: passato un determinato tempo il pacchetto viene considerato perso e il token rimesso in circolo.</p> <p><b>PRO</b></p> <ul style="list-style-type: none"> <li>• E’ una rete chiusa e quindi robusta dal punto di vista della sicurezza</li> <li>• Non c’è bisogno di instradamento né di algoritmi anti collisione dei pacchetti</li> </ul>	<p style="text-align: center;"><b>CONTRO</b></p> <ul style="list-style-type: none"> <li>• La rete non è facilmente scalabile (è piuttosto complicato aggiungere host)</li> <li>• La comunicazione è piuttosto lenta soprattutto in reti composte da tanti host</li> <li>• Rete poco robusta: un malfunzionamento ai cavi o ad un host compromette il funzionamento della rete</li> </ul>
--	--

**RETE A STELLA**



E' la tipologia utilizzata nelle rete LAN.

Gli host sono collegati ad uno **switch** centrale e diversi switch possono essere collegati tra loro. La comunicazione avviene in **broadcast**: tutti i messaggi vengono mandati dagli switch a tutti gli host ma solo i destinatari processano il messaggio.

Dopo i primi messaggio gli host possono memorizzare l'indirizzo degli host e associarlo alla porta a cui sono collegati. In questo modo lo switch è capace di fare un semplice instradamento dei pacchetti.

<b>PRO</b>	<b>CONTRO</b>
<ul style="list-style-type: none"> <li>• Rete facilmente scalabile: è semplice aggiungere host, collegandoli direttamente agli switch</li> <li>• Rete robusta: un malfunzionamento agli host o ai cavi non compromette il funzionamento della rete</li> </ul>	<ul style="list-style-type: none"> <li>• Il cablaggio è piuttosto complesso e utilizza molti cavi (da uno switch parte un cavo per ogni host)</li> <li>• Richiede algoritmi anticollisione per i pacchetti</li> </ul>

## Indirizzi

Ogni host collegato ad una rete deve avere un indirizzo univoco che lo identifichi. Assoceremo in seguito questi indirizzi ai diversi livelli che compongono i protocolli con cui vengono composti i pacchetti con cui gli host condividono informazioni e servizi sulla rete

### Indirizzi IPv4

E' l'indirizzo *logico* dell'host e non è legato ad un componente fisico, solitamente viene utilizzato al livello 3 dell'architettura ISO/OSI (Network)

E' composto da 4 byte solitamente rappresentati in notazione decimale separata da un punto (**dotted decimal**). Ovviamente ogni byte può rappresentare un numero da 0 a 255

Questi indirizzi possono essere suddivisi in 5 classi diverse

A	0xxx xxxx. H . H . H	0 – 126. H . H . H	Il primo byte identifica la rete gli altri 3 l'host
B	10xx xxxx. N . H . H	128 – 191. N . H . H	I primi due byte identificano la rete gli altri 2 l'host
C	110x xxxx. N . N . H	192 – 223. N . N . H	Solo l'ultimo byte identifica l'host
D	1110 xxxx. X . X . X	224 – 239 . X . X . X	Indirizzi usati per il multicast (gruppi)
E	1111 xxxx. X . X . X	240 – 255. X . X . X	Usi futuri

**Indirizzo di Loopback:** L'indirizzo 127.0.0.1 è utilizzato per indicare "se stessi". Per questo gli indirizzi che iniziano con 127 (0111.1111) non appartengono a nessuna classe e non possono essere assegnati ad un host

Come illustrato per ciascun gruppo solo alcuni byte identificano l'host. Gli altri identificano la sottorete a cui l'host è collegato. Per capire, in un indirizzo, quale parte identifica la sottorete viene solitamente utilizzata una

**Subnet mask.** E' una maschera di zeri e uno che *messa in and* con l'indirizzo ne maschera l'host (a zero) e ne *evidenzia la sottorete*

Indirizzi di classe A, ad esempio hanno una subnet mask 255.0.0.0

Indirizzi di classe C hanno subnet mask 255.255.255.0

La subnet mask viene anche scritta in decimale al termine dell'indirizzo indicando quanti bit sono a uno. Esempi:

Classe A:	37.5.5.13/8	subnet mask: 255.0.0.0	→ 3 byte per gli host
Classe B:	172.16.13.110/16	subnet mask: 255.255.0.0	→ 2 byte per gli host
Classe C:	192.168.1.220/25	subnet mask: 255.255.255.0	→ 1 byte per gli host

## INDIRIZZI IPv6

Avendo a disposizione 32bit con indirizzi di tipo IPv4 possono essere scritto circa 4 miliardi di indirizzi. Vista l'espansione della rete Internet questi indirizzi iniziano ad essere insufficiente (nel 2003 si è raggiunta la saturazione degli indirizzi)

E' stato per questo introdotto un nuovo indirizzamento composto da **128 bit**: gli indirizzi IPv6.

Questi indirizzi vengono espressi con *8 gruppi di quattro caratteri esadecimali separati da "due punti"* (ogni quartetto è scritto con 16 bit, 4 bit per ogni carattere esadecimale). Esempio

A073:0000:0000:738°:1248:ffff:ca3b:6f6e

Sequenza di bit a zero possono essere sostituite da "::". Nel caso precedente, ad esempio:

A073::738°:1248:ffff:ca3b:6f6e

Gli ultimi due "quartetti" rappresentano solitamente l'indirizzi IPv4.

Per trasformare un indirizzo IPv4 in IPv6 è sufficiente infatti convertire i byte del IPv4 in esadecimale e aggiungere zeri nei primi byte dell'indirizzo IPv6

192.168.89.9 → 1100 0000 . 1010 1000 . 0101 1001 . 0000 1001 → C0.A8.59.09

L'indirizzo IPv6 corrispondente può essere scritto come **::C0A8:5909**

**Indirizzi a disposizione:** con IPv6 si possono scrivere  $2^{128}$  indirizzi. Questo vorrebbe dire che per ogni metro quadrato di superficie terrestre ci sono a disposizione  $2^{27}$  indirizzi da utilizzare.

## MAC ADDRESS

Il Mac Address è l'indirizzo associato ad ogni scheda di rete prodotta. Questo è un indirizzo utilizzato a livello 1 e 2 della pila ISO/OSI (Datalink).

Questo indirizzo è composto da 6 byte ovvero 48 bit. L'indirizzo è solitamente scritto *come coppie di valori esadecimali separati da "due punti"*. Esempio

5C:26:0A:29:BE:34

I primi tre byte sono assegnati alla casa produttrice. Ogni casa assegna i successivi 3 byte ai propri prodotti.

Ad esempio i prodotti Intel hanno Mac Address 00:AA:00:xx:xx:xx mentre i prodotti IBM 08:00:5A:xx:xx:xx

## PACCHETTI E PROTOCOLLI

Un pacchetto (**PDU – Protocol Data Unit**) è un’unità base di **informazione** che viene scambiata tra due sistemi attraverso un protocollo.

Nel campo informatico la comunicazione avviene tipicamente tra due calcolatori o comunque tra due sistemi elettronici. Le regole alla base della comunicazione sono di tipo molto diverso (linguaggio da utilizzare, sintassi, regole di invio, impacchettamento dei dati etc.) e i protocolli vengono divisi in **livelli** in base alle loro caratteristiche

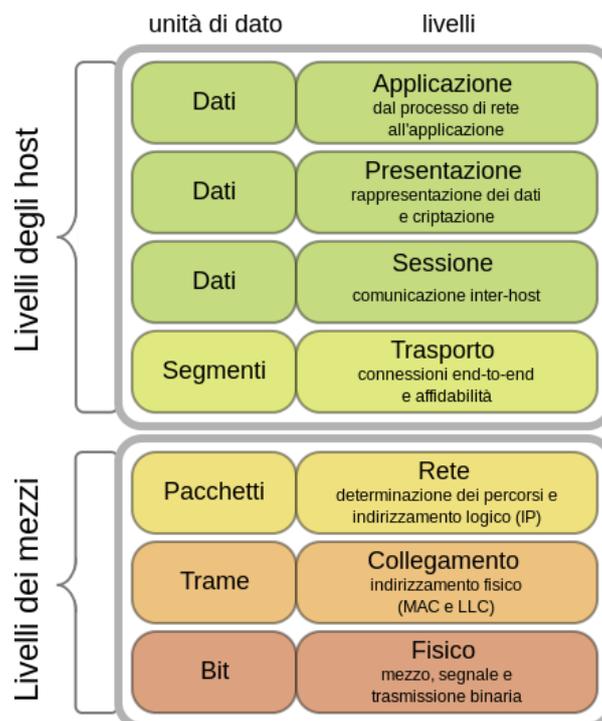
### Modello ISO/OSI

**ISO** è la più grande organizzazione mondiale senza scopo di lucro per la determinazione di standard utilizzabili in diversi ambiti (International Organization for Standardization); **OSI** è una standard utilizzato per la connessione e la comunicazione tra dispositivi informatici (Open System Interconnection)

Far comunicare due computer tipicamente significa far scambiare dati a due applicazioni che girano su due macchine diverse (facenti parte di una rete). Per far questo ho bisogno di regole che stabiliscano come comunicare. Lo standard ISO/OSI divide queste regole (protocolli) in **7 diversi livelli**

Ogni livello fornisce dei **servizi** ai livelli superiori in modo da rendere più semplice e uniforme la realizzazione delle tecnologie di rete operanti a qualsiasi livello. Ogni servizio è implementato da uno (o più) **protocolli** attraverso opportune **interfacce**.

Di seguito vengono descritti i servizi che devono essere forniti dai protocolli che lavorano ai diversi livelli della pila ISO/OSI. E’ importante notare che il modello in questione **non** stabilisce quali debbano essere i protocolli utilizzati per implementare questi servizi. Nell’elenco seguente tra parentesi sono introdotti i nomi dei protocolli comunemente utilizzati.



**APPLICATION** (HTML, SMTP, FTP, SSH, TELNET)

I protocolli a questo livello sono delle **interfacce per le applicazioni**, ovvero forniscono strumenti alle applicazioni per poter utilizzare la rete (scambiare dati con altre applicazioni che usino lo stesso protocollo). Questo livello fornisce un servizio direttamente all'utente, attraverso l'applicazione.

**PRESENTATION** (SSL, TLS)

Gestisce la sintassi del messaggio da scambiare, ovvero la formattazione, la compressione (se necessaria) e la crittografia per la sicurezza.

**SESSION** (RPC)

Gestisce la sincronizzazione della comunicazione tra le applicazioni: autenticazione, stabilire una connessione, gestire la comunicazione mono/bi-direzionale.

(A questo livello, ad esempio, avviene l'interruzione della comunicazione tramite Skype quando manca la connessione)

**TRANSPORT** (TCP, UDP)

E' il primo livello (partendo dal basso quindi dal livello Fisico) **end to end** ovvero dove stabilisco una connessione tra le due macchine che devono comunicare (non tra le applicazioni). Questo livello gestisce:

- La creazione della connessione tra le macchine
- La gestione del flusso dei pacchetti (controllo della corretta ricezione di ogni pacchetto)
- Evita la congestione della rete (invio di troppi pacchetti insieme)
- Gestisce la divisione dei dati (frammentazione) in **segmenti**

**NETWORK** (IPv4, IPv6)

Gestisce gli indirizzi di rete e l'instradamento (**routing**) dei **pacchetti** verso la destinazione finale. I livelli superiori devono essere liberi di **non sapere** i dettagli tecnologici di come avviene l'invio dei pacchetti, di cui si occupa questo livello.

**DATA LINK** (Ethernet-802.3 , WiFi 802.11)

Gestisce e maschera ai livelli superiori tutti i possibili errori del livello fisico. Esegue l'incapsulamento dei byte dei pacchetti in entità più piccolo (**frame**) ne controlla header e tail e gestisce gli errori di invio e di ricezione dei pacchetti (a livello basso). Inoltre gestisce l'accesso al canale di comunicazione.

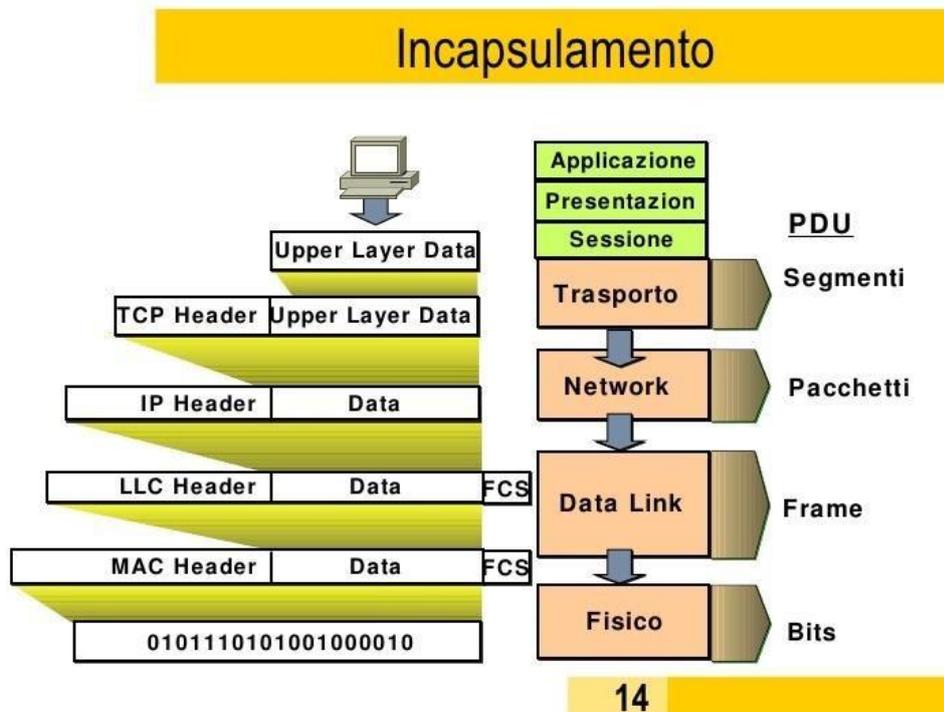
**FISICO** (ADSL, Fibra ottica, doppino telefonico, Satellitare, 4G)

Si occupa di controllare l'hardware (scheda di rete) e il canale trasmissivo, stabilendo tutte le regole circa le tensioni, le correnti e l'utilizzo dei mezzi di comunicazione fisico.

## Imbustamento e frammentazione

La **frammentazione**, può avvenire a diversi livelli della pila di protocolli e consiste nel dividere in dato in più pacchetti (o segmenti, o frame a seconda del livello) per ridurre la dimensione del PDU. In questo modo, tipicamente, si mantiene fissa la dimensione del PDU.

L'imbustamento (**incapsulamento**) è l'inserimento di un header (intestazione) al pacchetto per ogni livello dell'architettura di rete utilizzata. Nel caso della pila ISO/OSI:

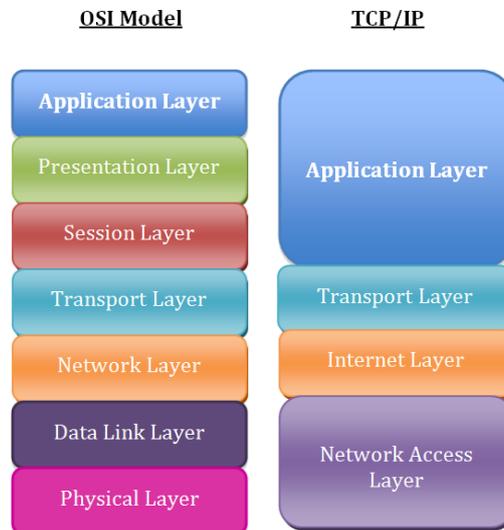


Queste intestazioni saranno diverse a seconda dei protocolli utilizzati ad ogni livello. L'intestazione consiste in una serie di byte contenente delle informazioni utili ad implementare i servizi di cui il protocollo si fa carico. Tra le informazioni presenti nell'header ci sono sicuramente:

- Indirizzi Mac nelle intestazioni di livello 2-Datalink
- Indirizzi IP nelle intestazioni di livello 3-Network
- Le porte di comunicazione come indirizzi di livello 4-Trasporto

## IPS – Internet Protocol Suite

L'Internet Protocol Suite è l'insieme dei protocolli di fatto usati nella comunicazione su internet. L'insieme di protocolli non rispetta completamente il modello ISO/OSI in quanto alcuni livelli non vengono esplicitati direttamente. Esiste però una mappatura tra questi protocolli e i livelli visti in precedenza.



### APPLICATION LAYER

I protocolli a questo livello uniscono le caratteristiche dei tre livelli più alti della pila ISO/OSI. A questo livello troviamo ad esempio il protocollo HTTP per lo scambio dei dati tra applicazioni client e server durante la navigazione tra pagine web (servizio World Wide Web)

### TRANSPORT LAYER

Vengono utilizzate (sulla rete Internet) due protocolli diversi: TCP e UDP.

Il protocollo **TCP (Transmission Control Protocol)** è in **connection mode** ovvero stabilisce una connessione sicura con l'host di destinazione. Il protocollo esegue un controllo di ricezione dei pacchetti tramite **acknowledge (ACK)** ovvero messaggi che confermino la ricezione del pacchetto. I pacchetti per cui non viene ricevuto ACK vengono ritrasmessi. La comunicazione è dunque **affidabile**.

Il protocollo **UDP (User Datagram Protocol)** è in **connectionless mode**: non viene stabilita una connessione sicura a questo livello (ma può essere stabilita una connessione tra le applicazioni al livello superiore). Non viene fatto un controllo di ricezione dei pacchetti inviati (non vengono quindi ritrasmessi quelli persi). Il protocollo è usato, ad esempio, per comunicazioni di **streaming audio o video live**. La comunicazione non è affidabile come con il protocollo TCP.

### INTERNET LAYER

A questo livello opera il protocollo **IP (internet protocol)** si occupa dell'instradamento dei pacchetti attraverso l'indirizzo di destinazione (indirizzo IP). Lavora in **connectionless mode** (non stabilisce a priori una connessione ma utilizza l'indirizzo del destinatario)

### NETWORK ACCESS LAYER

Questo è il livello dei protocolli di accesso alla rete, che non vengono esplicitati nel modello IPS.

## Indirizzi del TRANSPORT LAYER

A livello di TRASPORTO (protocollo TCP) non vengono stabiliti degli indirizzi dell'host di destinazione. L'indirizzo a questo livello riguarda **l'applicazione che viene utilizzata** e viene definito **porta**.

La porta viene identificata con un **numero intero a 16 bit** quindi con 65536 porte.

Ogni applicazione utilizza delle porte per l'invio e la ricezione dei dati.

Possiamo dividere le porte in diverse classi

<b>0 - 1023</b>	<b>Porte note (applicativi server)</b>	20 FTP (anche 21) 22 SSH 23 TELNET 25 SMTP 110 POP3 80 HTTP
<b>1024 - 49151</b>	<b>Porte Registrate (applicativi utente)</b>	3389 DESKTOP REMOTO 4462 EMULE (anche 4472) 8080 HTTP (alternativa o secondo server)
<b>49152 - 65535</b>	<b>Porte Dinamiche</b>	