



UNIVERSITÀ
DI PARMA

DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE ED INFORMATICHE
Corso di Laurea in Informatica

Introduzione

RETI DI CALCOLATORI - a.a. 2023/2024
Roberto Alfieri

Contenuti

- ▶ Definizioni, topologie, canali di comunicazione e mezzi trasmissivi, gli standard
- ▶ Reti locali, reti geografiche, Internet
- ▶ La storia, Il modello ISO/OSI
- ▶ I livelli TCP/IP: livello rete, trasporto e applicazione
- ▶ Sicurezza
- ▶ Contenuti del corso

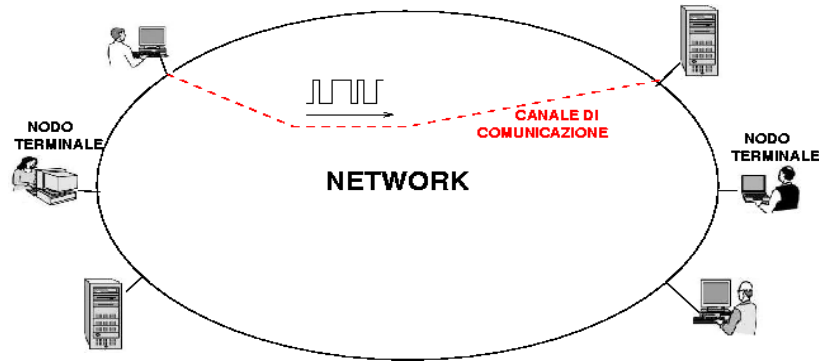
RIFERIMENTI

- ▶ *Reti di Calcolatori*, A. Tanenbaum, ed. Pearson
- ▶ *Reti di calcolatori e Internet*, Forouzan , Ed. McGraw-Hill

Cosa sono le Reti di Calcolatori

Una rete di calcolatori è un insieme di nodi di elaborazione

- autonomi tra loro
- connessi mediante un opportuno sistema di comunicazione
- in grado di interagire mediante scambio di messaggi al fine di consentire alle applicazioni in esecuzione sui nodi di comunicare tra loro



La comunicazione avviene attraverso canali individuati sulla rete e ha 5 componenti:

- **Messaggio:** informazione da trasferire
- **Mittente:** dispositivo che spedisce il messaggio
- **Destinatario:** dispositivo che riceve il messaggio
- **Mezzo di trasmissione:** cammino fisico percorso dal messaggio
- **Protocollo:** insieme di regole che governano la comunicazione

Applicazioni : una tassonomia

modello client-server (User to resource)

Servizi che consentono all'utente di accedere a risorse remote

- ▶ Accesso a risorse remote: sistemi, applicazioni, storage, stampanti, ..

modello peer to peer (user to user)

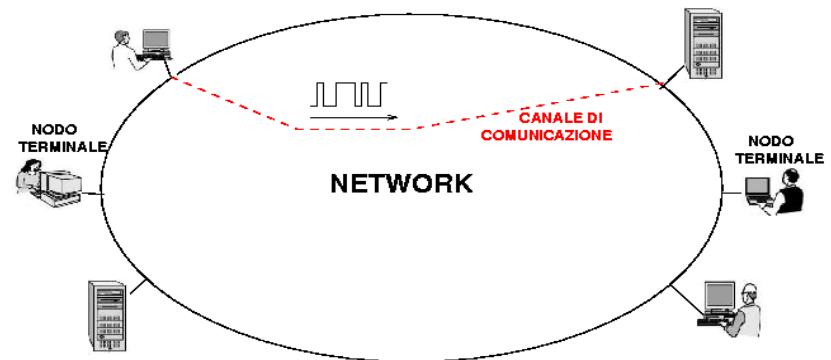
Servizi collaborativi per 2 o più utenti remoti

- ▶ File sharing, audio/video conferenza, VoIP

modello multi tier e architetture middleware (resource to resource)

Una applicazione viene distribuita su diversi host/device che cooperano via rete.

- ▶ Sistemi distribuiti (Modularità e affidabilità)
- ▶ Accelerazione delle prestazioni (HPC)
- ▶ Internet of Things



Metriche per la valutazione del canale di comunicazione

La qualità dei canali di comunicazione è stabilita dai seguenti parametri primari:

- **Ampiezza di Banda Digitale:** Quantità di dati (bit) che possono essere trasmessi nell'unità di tempo. Si misura in bit/sec
- **Ritardo (latenza) :** Tempo di trasferimento di un bit da un terminale all'altro (secondi)
- **Jitter :** Variazione del ritardo
- **Affidabilità:** Intolleranza agli errori di trasmissione (Percentuale di bit persi)
- **Sicurezza:** capacità di opporsi ad accesso non autorizzato, danno o violazioni della rete

Le applicazioni hanno sensibilità diverse rispetto ai parametri primari.

Ad esempio:

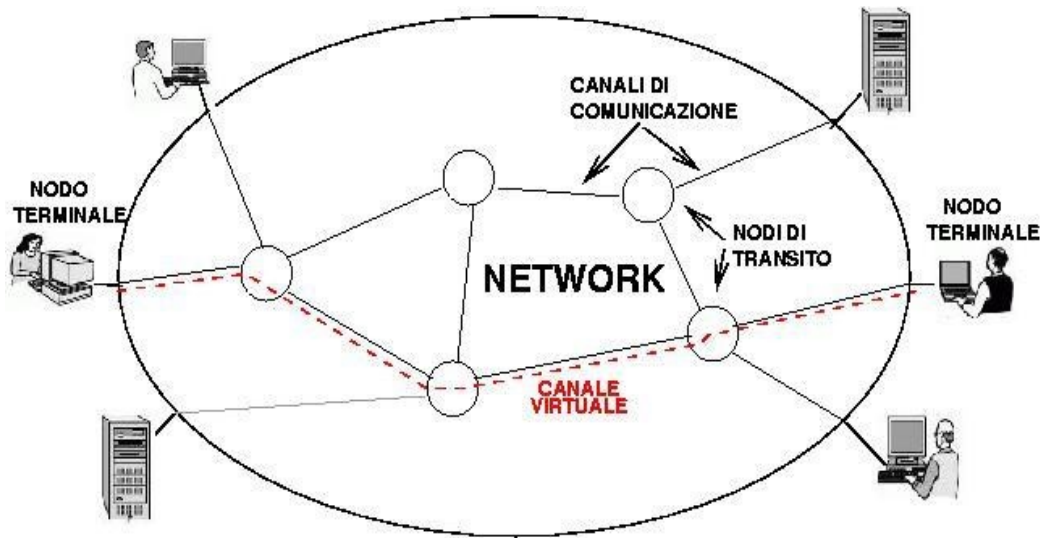
Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Struttura fisica della Rete

La rete è un insieme di nodi interconnessi tra loro.

Due nodi comunicano mediante una **connessione fisica** se è presente un **canale fisico (link)** che li collega direttamente. Una catene di canali fisici forma una **connessione logica** su di un percorso (**path**) statico o dinamico detto **canale virtuale**.

In una connessione i nodi possono essere **terminali** (punto di arrivo di una connessione logica), di **transito** (nodi con funzionalità di **commutazione** dei dati tra un canale fisico e il successivo) o con **entrambe** le funzioni.

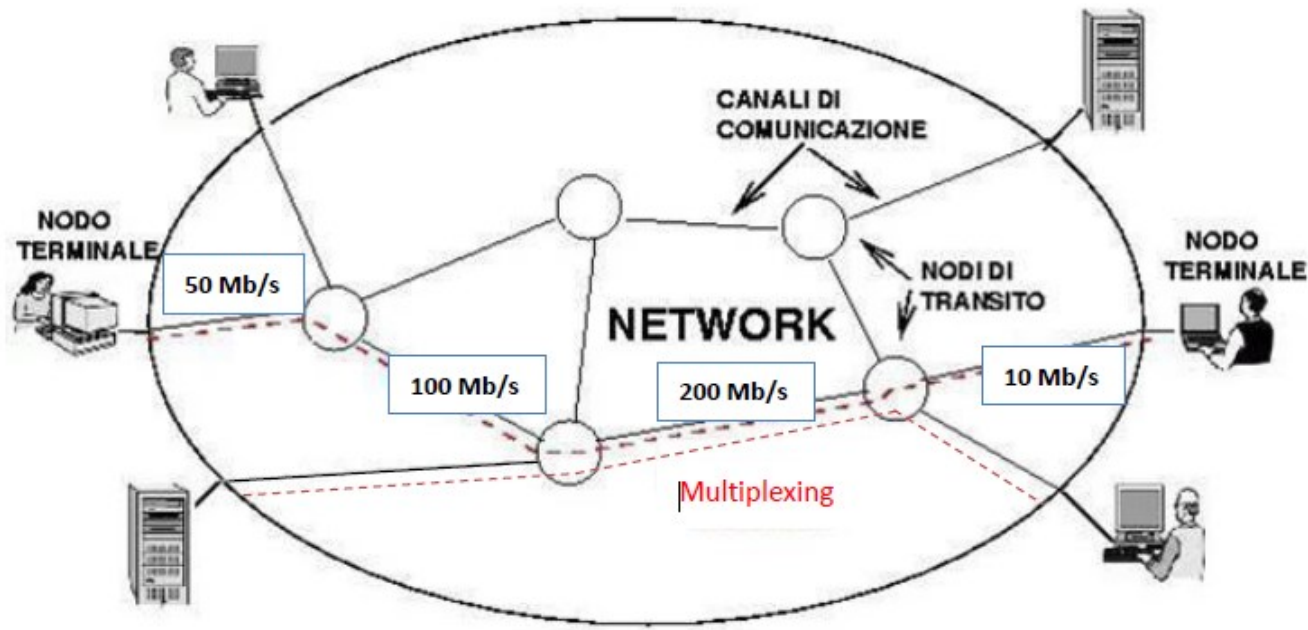


Ampiezza di banda e throughput

Ogni link ha la propria ampiezza di banda (dipende dal mezzo trasmissivo e dalla tecnica di codifica) e latenza (dipende principalmente dalla distanza).

L'effettiva velocità di trasmissione sul canale virtuale (throughput) non potrà superare l'ampiezza di banda del link più lento.

E' possibile attivare più canali virtuali contemporaneamente sullo stesso link utilizzando una tecnica di condivisione del canale (multiplexing). L'ampiezza di banda del link viene quindi condivisa tra i diversi canali virtuali.

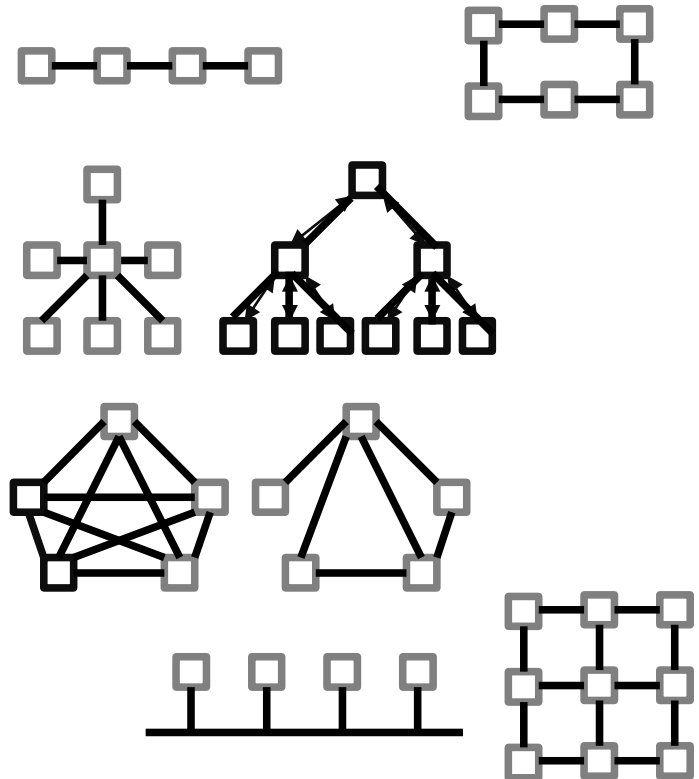


Topologia della rete

La topologia di rete è il modello geometrico finalizzato a rappresentare le relazioni di connettività, fisica o logica, tra i nodi della rete.

Principali topologie:

- Lineare aperta o ad anello
- A stella
- Ad albero
- Completamente o parzialmente magliata
- A bus
- A griglia



Topologia della rete : alcune definizioni

Link: è il canale di comunicazione che interconnette fisicamente due nodi.

Path: è la catena di link che compone un canale virtuale tra due nodi.

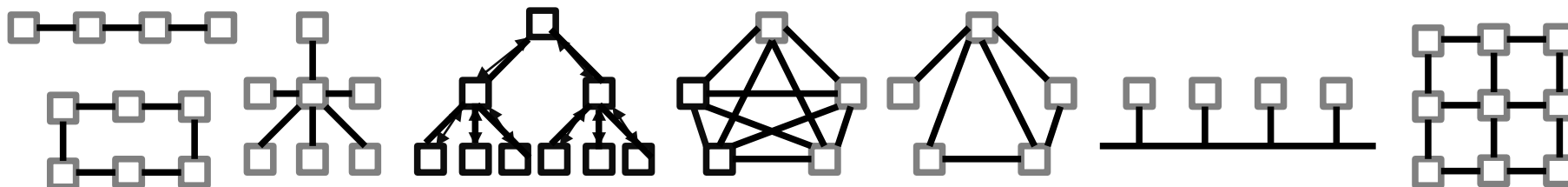
Nota: Per ogni coppia di nodi esistono uno o più path possibili. Attraverso opportune metriche possiamo attribuire un costo ad ogni path e determinare il path a costo minimo tra due nodi.

Hops: è il numero di link da attraversare.

Diametro: è la distanza (hops) tra i due nodi più lontani

Grado: numero massimo di link connessi ad un nodo

Scalabilità: Capacità della topologia di sostenere un numero crescente di nodi.



Modelli di utilizzo del canale

Le comunicazioni sui canali possono essere classificate in base a

Direzione:

- **Simplex** (monodirezionali, esempio TV)
- **Half-Duplex** (Entrambe le direzioni, non contemporaneamente, esempio walkie-talkie)
- **Full-Duplex** (Entrambe le direzioni contemporaneamente, esempio telefono)

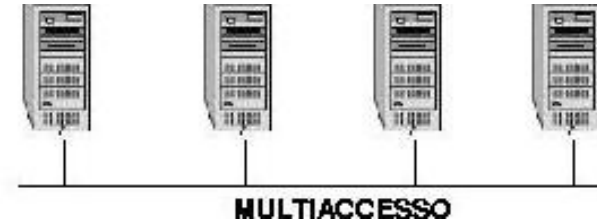
Destinazione:

- **Unicast** (Un singolo destinatario)
- **Broadcast** (Tutti i nodi appartenenti ad una rete o sottorete)
- **Multicast** (Un sottoinsieme dei nodi della rete)

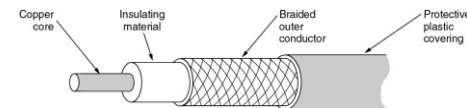
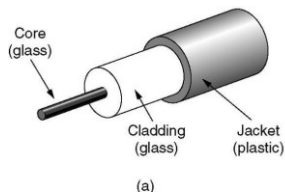
Canali di Comunicazione (link) e mezzi trasmissivi

I mezzi trasmissivi possono essere:

- **Punto-Punto: comunicazione tra 2 nodi**
- **Multi-Accesso : comunicazione tra N nodi (Bus)**



Ad esempio la fibra ottica e il doppino telefonico sono punto-punto, mentre il cavo coassiale e il wireless possono essere multi-accesso.

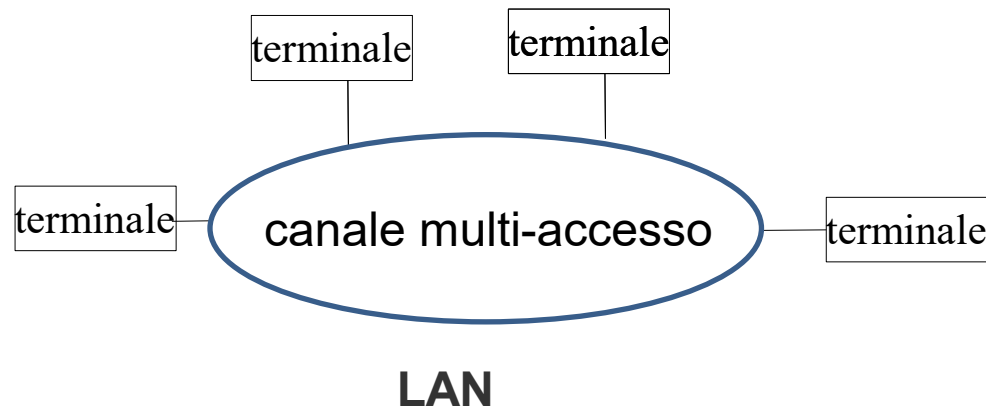


Local Area Network (LAN)

I mezzi trasmissivi multi-accesso possono essere utilizzati per realizzare un particolare tipo di rete detta LAN (Local Area Network) che include tutti i nodi che condividono lo stesso canale multi-accesso.

Le reti LAN supportano tutti i modelli di destinazione:

- Unicast, Broadcast e Multicast

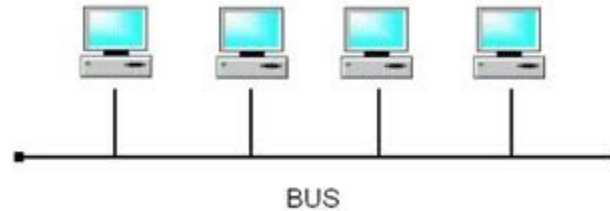


Le reti LAN dispongono di un opportuno **protocollo** per disciplinare l'accesso al canale e per gestire dell'indirizzamento (comunicazioni unicast, broadcast o multicast)

Reti locali: Ethernet

Ethernet è la tecnologia dominante per le reti LAN.

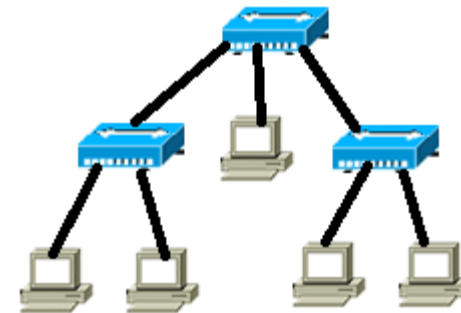
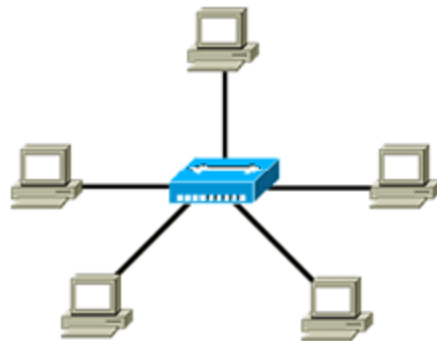
Nella versione Ethernet 2.0 (1980) l'ampiezza di banda era di 10Mb/s su cavo coassiale (topologia a BUS).



Nel 1995 esce lo standard denominato "Fast Ethernet" a 100Mb/s e nel 1999 arriva il Gigabit Ethernet a 1 Gb/s.

La topologia diventa a stella con l'introduzione di opportuni apparati di rete (HUB e switch), che consentono di realizzare una infrastruttura multi-accesso utilizzando mezzi trasmissivi punto-punto:

i dati ricevuti in una porta dell'apparato di rete vengono replicati su tutte e altre porte. La topologia può anche essere ad albero connettendo più hub/switch in cascata.



Reti Geografiche (WAN)

Per realizzare reti che si estendono su grandi distanze geografiche (WAN - Wide Area Network) si possono utilizzare semplici link punto-punto

- ad esempio la connessione ADSL tra casa e la centrale telefonica



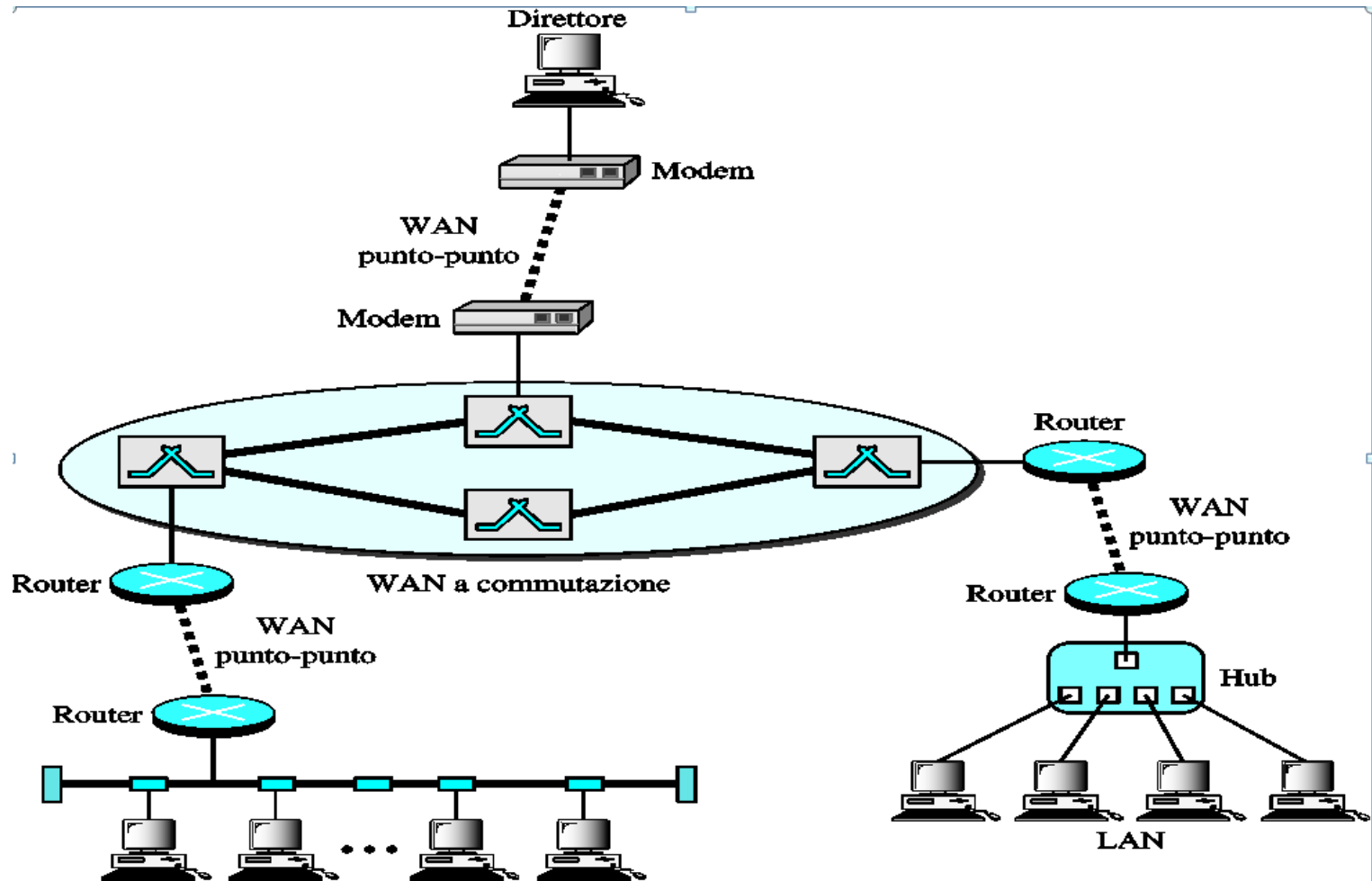
oppure infrastrutture di commutazione fornite da terze parti, come la rete ATM dei providers di telefonia.

- ad esempio la connessione tra 2 sedi remote di una azienda



Interconnessione di reti: internet

Dal punto di vista dell'infrastruttura fisica della rete internet (con la i minuscola) è l'unione di reti LAN e WAN interconnesse tra loro, con topologia magliata.



Commutazione di Circuito e di Pacchetto

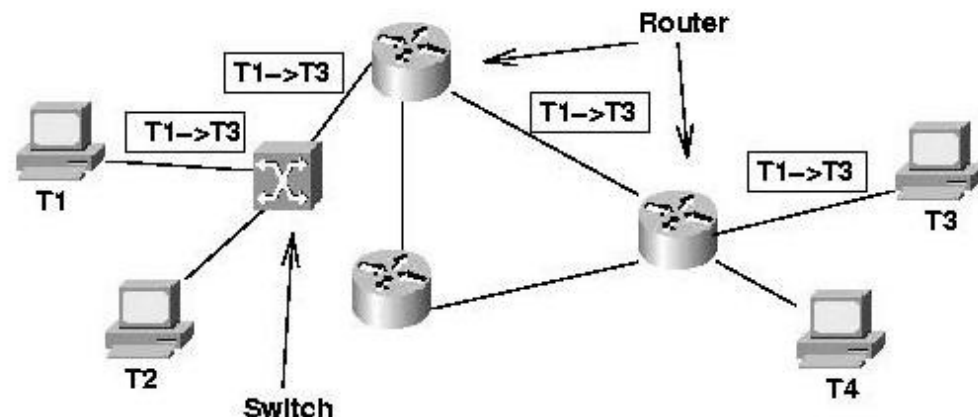
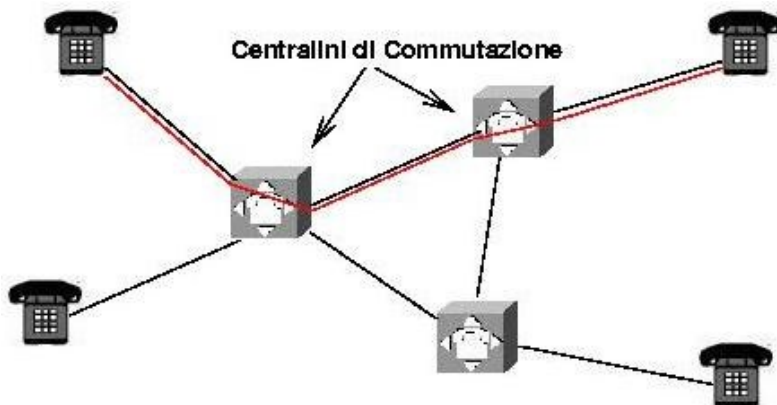
Il processo per individuare ed utilizzare il percorso su cui far transitare i messaggi su un canale virtuale è detto commutazione. Esistono due modelli di commutazione:

Commutazione di circuito (tipico delle reti telefoniche)

- Viene individuato il percorso tra i due terminali e creato un circuito fisico temporaneo.
- Esiste un ritardo iniziale dovuto al tempo necessario per instaurare il circuito.
- I terminali scambiano i dati (come se fosse un collegamento diretto).
- Il canale viene chiuso al termine della comunicazione.

Commutazione di Pacchetto (tipico delle reti dati)

- I dati della comunicazione sono frazionati in “pacchetti” con una lunghezza massima stabilita.
- I nodi di transito (router, switch, ..) hanno il compito di instradare ogni pacchetto.
- Il destinatario riassume i pacchetti e ricostruisce il messaggio.



Gli inizi: Le reti proprietarie

Negli anni 70 **IBM** dominava il mercato dei calcolatori con i propri “Mainframe” (prevalentemente della serie 370, con sistema operativo VM).

Nel 1974 rilascia per la prima volta un sistema operativo con un protocollo di rete denominato SNA (system Network Architecture).

DIGITAL Equipment Corporation (DEC) rilasciò nel 1978 un “mini” elaboratore che ebbe un grande successo: il VAX 11/780 (sistema operativo VAX/VMS).

Nel 1982 VAX/VMS incluse il protocollo di rete proprietario DECnet.

Negli anni 80 si diffusero a livello mondiale 2 reti indipendenti con tecnologie proprietarie: la rete BITnet basata su SNA degli elaboratori IBM e la rete HEPnet basata su DECnet. Le due reti non erano in grado di comunicare tra loro.

Standardizzazione delle reti

Esistono molti costruttori e fornitori di reti, ognuno con le proprie impostazioni.

La necessità dell'interoperabilità richiede la presenza di standard condivisi per ogni aspetto della rete.

Gli standard vengono proposti da diversi organismi internazionali. I principali sono:

ITU (International Telecommunication Union) ha il compito di standardizzare le telecomunicazioni, principalmente telefoniche. ITU-T è un settore di ITU che si occupa di telefonia e scambio dati.

ISO (International Standard Organization) definisce standard per una vasta gamma di argomenti. Sono stati emanati più di 17000 standard, incluso lo standard OSI (Open System Interconnect).

IEEE (Institute of Electrical and Electronics Engineers) è il principale ente professionale del mondo. Pubblica periodici, organizza conferenze e emana standard nel campo dell'ingegneria elettrica e dei computers. Il comitato IEEE 802 ha standardizzato molti tipi di LAN.

ISoc (Internet Society) è nata nel 1992 su iniziativa di Vint Cerf and Bob Kahn per governare la crescita di internet. Gli standard sono emanati da **IETF (Internet Engineer Task Force)** attraverso gli **RFC (Request For Comment)**.

W3C (World Wide Web Consortium) è un consorzio industriale guidato da Tim BernesLee (creatore del Web) che sviluppa protocolli e linee guida per la crescita a lungo termine del Web (HTTP, HTML, privacy, ecc.)

Il modello ISO/OSI

A partire dal 1976 la ISO (International Organization for Standardization) ha dato il via a lavori per giungere ad una serie di standard unificati per la realizzazione di reti di calcolatori aperte.

ISO ha proposto un modello di riferimento detto **Open System Interconnection Reference Model (OSI-RM)** che nel 1983 è diventato standard internazionale ISO 7498, detta comunemente ISO-OSI.

ISO-OSI è basato sul concetto centrale di una **architettura a strati**.

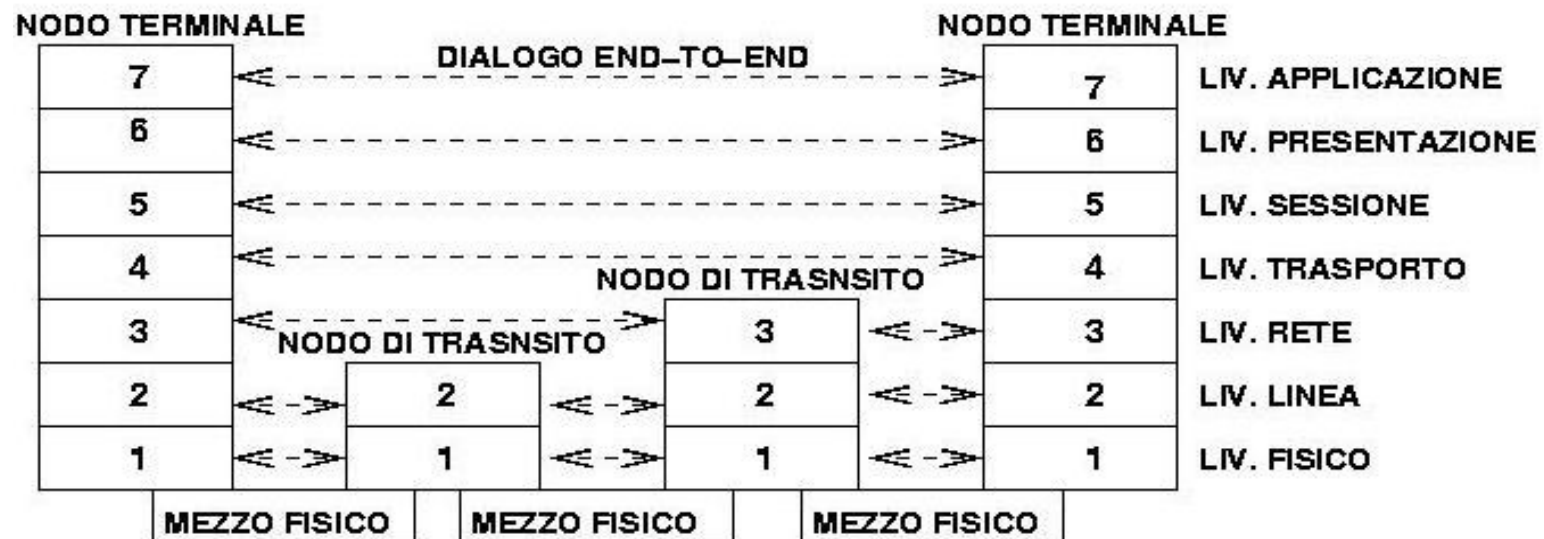
L'architettura a strati ha alcuni grandi vantaggi:

- scompone il problema in sotto-problemi posti a diversi **livelli**, più semplici da trattare
- rende i vari livelli indipendenti, comunicanti mediante una interfaccia standard
- starti diversi possono essere sviluppati da enti diversi.

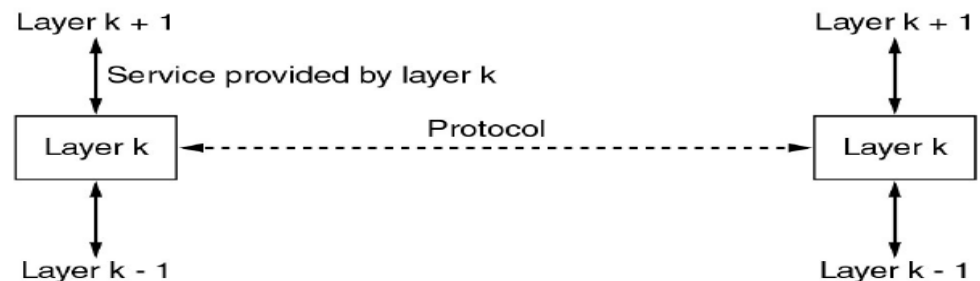
Strati ISO/OSI

OSI scompone la comunicazione in **7 strati (o livelli)**. Lo scopo di ciascun strato è quello di fornire servizi agli strati superiori, mascherando come questi servizi sono implementati.

I nodi terminali devono avere tutti i livelli implementati, mentre i nodi di transito utilizzano solo i livelli più bassi, in base alla loro funzione.

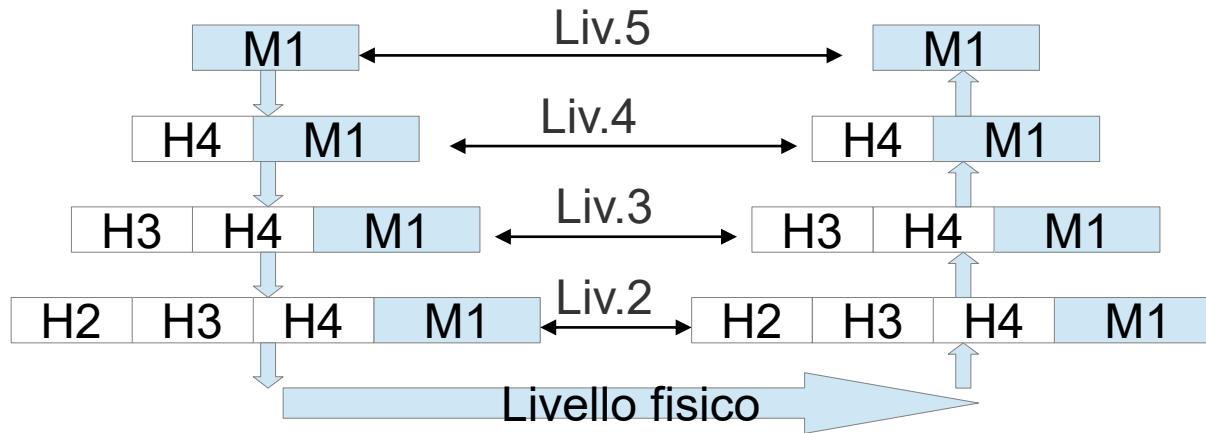


Ogni strato comunica logicamente con il pari stato del nodo remoto (peer), mentre fisicamente comunica con lo strato superiore ed inferiore dello stesso nodo.



Flusso dei dati

Il messaggio M viene frazionato in segmenti (M1, M2, ..) che vengono spediti in rete. Ogni strato aggiunge una intestazione in cui inserisce propri dati di servizio:



Strato 1 di OSI: Fisico

Scopo dello strato fisico è la trasmissione di bit “grezzi” sul canale di comunicazione. Deve attivare, mantenere e disattivare la connessione fisica per conto dello strato 2.

Per fare questo deve specificare le caratteristiche:

- meccaniche (forma di prese e spine, numero di contatti)
- elettriche (voltaggio e caratteristiche elettriche dei segnali associati all'interfaccia)
- funzionali (significato dei vari segnali, schemi di codifica dei bit in grandezze fisiche)



Strato 2 di OSI: Linea

Lo strato di linea deve

- attivare, mantenere e disattivare la connessione fisica su una linea (link) per conto dello strato 3
- rendere affidabile il collegamento diretto di un canale fisico

Le funzioni tipicamente svolte dallo strato 2 sono le seguenti:

- strutturazione del flusso di dati in unità di dialogo, denominati trame o frames
- controllo e gestione degli errori di trasmissione
- controllo di flusso (congestione)
- controllo di sequenza (ordine)

Per svolgere queste funzioni viene aggiunta una intestazione (Header) intesa ad ogni frame contenente informazioni di servizio.



Strato 3 di OSI: Rete

Scopo dello strato di rete è di far giungere le unità di informazione, dette pacchetti (**packets**), al destinatario determinando il percorso (**path**) attraverso la rete

Si occupa dunque del problema della commutazione. Nelle reti di calcolatori si usa la **commutazione di pacchetto** e la funzione svolta dallo strato 3 viene detta **routing**

Occorre un modo per individuare i destinatari: è necessario uno **schema di indirizzi**.
Se si vuole un'unica rete lo schema di indirizzi deve essere universale.

Strato 4 di OSI : Trasporto

Scopo dello strato di trasporto è **fornire un canale sicuro end-to-end (tra un processo mittente e un processo destinatario)**, svincolando gli strati superiori (applicativo) da tutti i problemi di rete

Tipiche funzioni

- **frammentare** i dati forniti dagli strati superiori (fragmenting/reassembling)
- Fornire una libreria di API per la programmazione

Può avere molte altre funzioni fra cui

- controllo dell'errore
- controllo di flusso
- gestione di dati prioritari
- ecc..

Non tutti le applicazioni hanno bisogno delle stesse funzioni, per cui si possono definire diverse **Classi di Trasporto**

Strato 5 di OSI: Sessione

Suddivide il dialogo fra le applicazioni in unità logiche (dette appunto **sessioni**)

Una sessione deve essere individuata, eventualmente interrotta e ripresa per fare fronte a vari eventi catastrofici: **perdita di dati, caduta della linea, momentaneo crash** di uno dei due interlocutori

Permette la chiusura ordinata (soft) del dialogo, con la garanzia che tutti i dati trasmessi sono arrivati a destinazione

Anche gli strati di sessione hanno molte funzionalità e possono essere più o meno completi a seconda delle richieste

Strato 6 di OSI: Presentazione

Adatta il **formato dei dati** usato dai due interlocutori preservandone il significato

La descrizione del tipo di dati usati per una applicazione e del loro formato si dice una sintassi

Ogni interlocutore ha una sua Sintassi locale per la rappresentazione dei dati e durante il dialogo bisogna concordare una Sintassi di trasferimento

E' stato definito un linguaggio detto Abstract Syntax Notation 1 (ASN 1) per descrivere e negoziare le sintassi

Strato 7 di OSI: Applicazione

Lo strato di Applicazione è l'utente della rete di calcolatori e pertanto non deve offrire servizi a nessuno

Rappresenta il programma applicativo (Applicazione) che per svolgere i suoi compiti ha bisogno di comunicare con altre applicazioni remote

Critica del modello OSI

Alla fine degli anni 80 sembrava che i protocolli OSI avrebbero dominato la scena mondiale. Questo non e' successo per 4 motivi:

Poca tempestività

- ▶ Prima c'e' la fase di ricerca, poi gli investimenti delle industrie.
- ▶ Le implementazioni OSI arrivano quando oramai TCP/IP era ampiamente diffuso.

Tecnologia scadente

- ▶ La scelta di 7 layer era più politica che tecnica.
- ▶ Due livelli quasi vuoti (presentation e session) e due troppo pieni (data link e network)

Implementazioni carenti

- ▶ Prime implementazioni lente, complicate ed enormi
- ▶ Al contrario TCP/IP era semplice veloce e Open (parte di Unix)

Incapacità politica

- ▶ Sviluppi dominati dalle Telecom, Ministeri, Comunità Europea e USA.
- ▶ Percepito con un insieme di standard imposti da burocrati.

ARPAnet e TCP/IP

1957: il Dipartimento della Difesa degli US crea l'Advanced Research Projects Agency (ARPA)

1970: nasce ARPAnet che collega alcune Università americane, utilizzando il protocollo host-to-host NCP (Network Control Protocol)

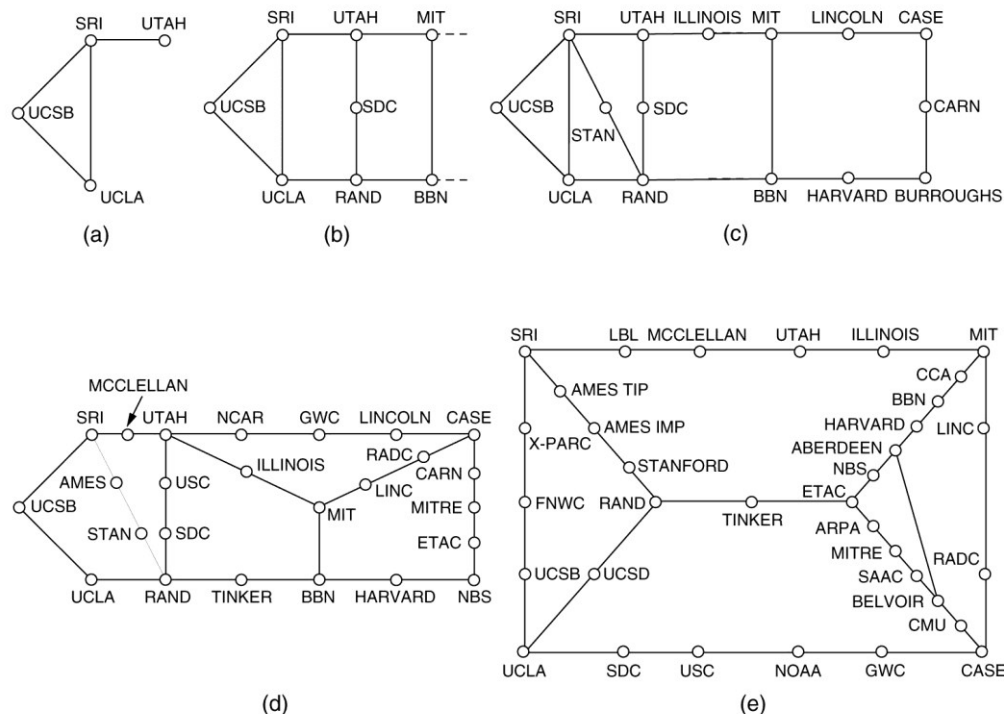
1974: Sulla base di un progetto finanziato da ARPA gli scienziati Vint Cerf e Bob Kahn pubblicano "A Protocol for Packet Network Intercommunication" in cui viene definita l'architettura del TCP/IP

1983: Il TCP/IP è adottato da ARPAnet

1986: La National Science Foundation (NSF) statunitense inizia lo sviluppo di NSFNET che oggi fornisce la maggior parte della spina dorsale dei servizi per Internet.

Inizia la crescita esponenziale di Internet.

Crescita di Arpanet dal 1969 (a) al 1972 (e)



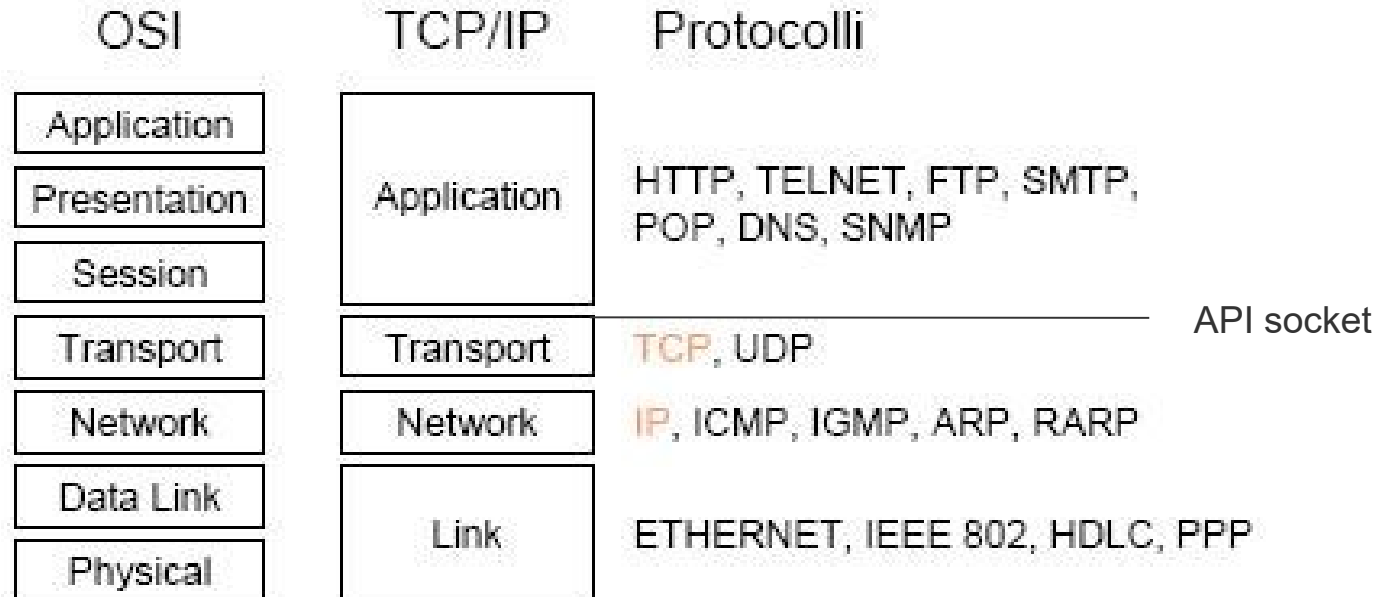
ISO/OSI e TCP/IP

Per alcuni anni si è ritenuto che TCP/IP fosse una soluzione transitoria e che prima o poi si sarebbe adottato OSI.

Il governo USA nominò una commissione per valutare la transizione e nel 1991 DECnet rilasciò una nuova versione (DECnet phase V) compatibile OSI, nella speranza di contrastare la crescita di TCP/IP.

Ma oramai le installazioni di TCP/IP erano così numerose da rendere troppo costosa la migrazione.

ISO/OSI rimane solo una architettura di riferimento.



Strati 1 e 2 di TCP/IP: fisico e collegamento

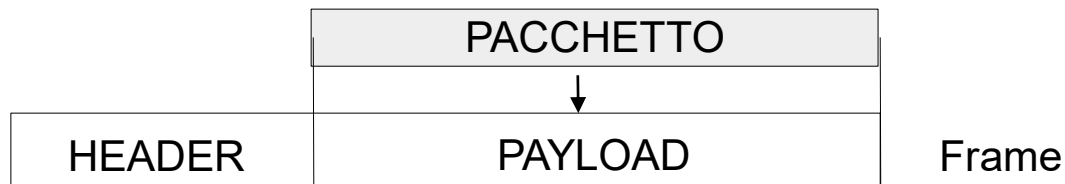
Per questi strati il modello TCP/IP non definisce nessun protocollo. Sono strati strettamente legati all'hardware di rete e vengono generalmente implementati nel device-driver della scheda e comunicano con i livelli superiori mediante una interfaccia standard.

Abbiamo 2 famiglie di protocolli:

- I protocolli WAN Esempi: HDLC e PPP.
- I protocolli LAN Esempio: Ethernet.

I protocolli dello stato fisico assegnano ad ogni interfaccia un indirizzo specifico, denominato **indirizzo fisico**. Ad esempio Ethernet utilizza indirizzi di 6 byte del tipo : 08 00 20 00 70 DF .

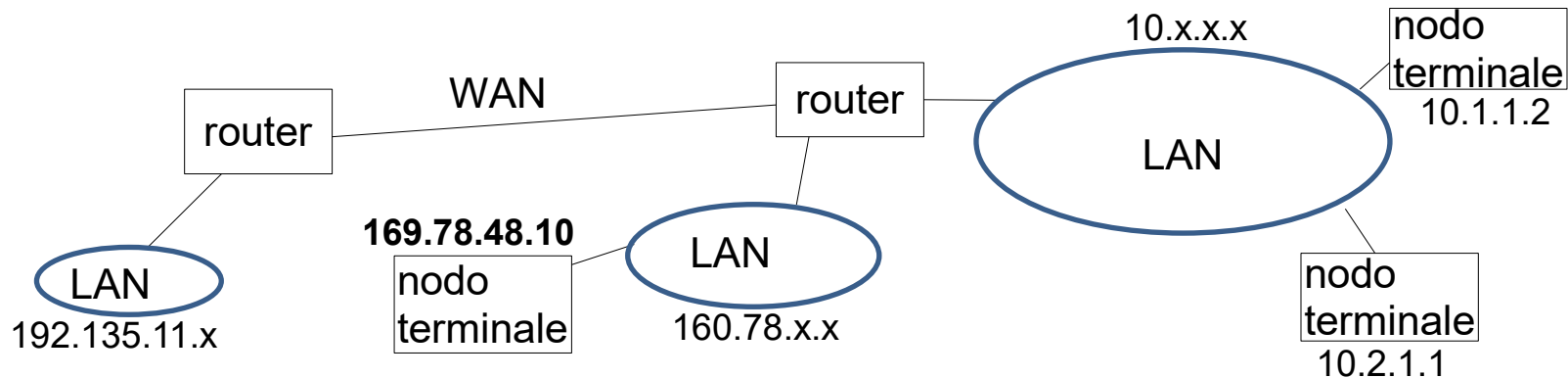
Tutti questi protocolli ricevono il **Payload** (carico utile) dal livello rete (pacchetto) che imbustano in una **Frame** in cui viene aggiunta una intestazione (**Header**) con campi necessari per il rilevamento degli errori, lo smistamento al livello superiore, l'indirizzamento.



Strato 3 di TCP/IP: rete

Lo strato rete ha il compito di mettere in comunicazione nodi appartenenti a reti LAN o WAN diverse. Richiede l'esistenza di particolari nodi di transito, detti **Router**, al confine tra 2 reti, con il compito di “ruotare” da una rete all'altra solamente i pacchetti che ne hanno necessità.

La suite di protocolli TCP/IP implementa questa funzionalità nel **protocollo IP**, che assegna ad ogni nodo un indirizzo logico univoco, come ad esempio 160.78.48.10. I bit della sequenza sono suddivisi in 2 parti: la prima parte denominata Network è comune a tutti i nodi della stessa rete LAN (esempio 160.78), mentre la seconda parte, denominata Host (esempio 48.10), distingue i nodi all'interno della LAN.



I router si coordinano tra loro tramite specifici protocolli (**link state o distance vector**) per individuare in modo dinamico il percorso migliore della comunicazione.

Lo strato 4 di TCP/IP: trasporto

Questo strato fornisce una connettività diretta tra 2 nodi indipendentemente dal percorso fisico di collegamento, svincolando gli strati superiori da tutti i problemi di rete.

Servizi Offerti:

Pacchettizzazione (fragmenting/reassembling): il flusso di dati da spedire viene frazionato in Segmenti che diventano il Payload dei pacchetti di livello rete.

Multiplexing/demultiplexing: Ad ogni applicazione verrà associato un numero di porta univoco sul nodo, in modo da distinguere i pacchetti provenienti dallo stato inferiore e dirottarli sull'applicazione corretta.

Diversi tipi di servizio, in base alle necessità:

Connection-Less, fornito dal **protocollo UDP**. Senza garanzia di ricevimento, senza riscontro, utilizzato da applicazioni che devono scambiarsi rapidamente brevi messaggi.

Connection-Oriented, fornita dal **protocollo TCP** in cui viene attivato un canale virtuale tra le due parti. Il TCP fornisce la garanzia di consegna senza errori e il controllo del flusso.

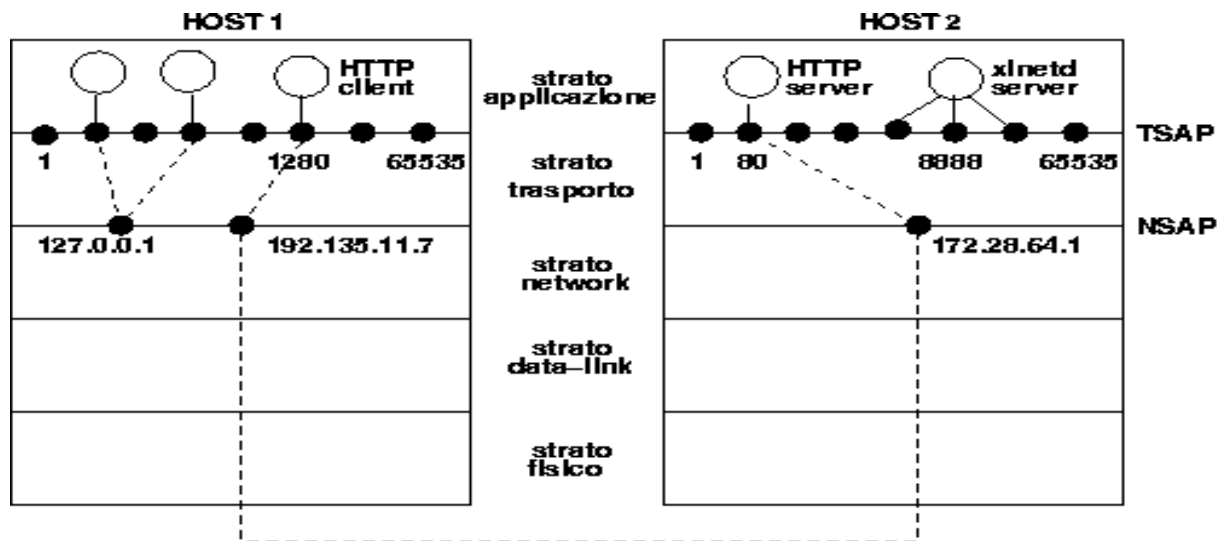
API: Le applicazioni del nodo potranno essere implementate per mezzo di una opportuna libreria di API, scegliendo il tipo di servizio più adatto alle proprie esigenze

Strato 4 di TCP/IP: demultiplexing

Visto che e' possibile avere piu' applicazioni di rete sullo stesso nodo, il livello di trasporto fornisce un meccanismo di multiplexing e demultiplexing basato sul concetto di porta.

Ad ogni applicazione verra' associato un numero di porta univoco sul nodo, in modo da distinguere i pacchetti provenienti dallo stato inferiore e dirottarli sull'applicazione corretta.

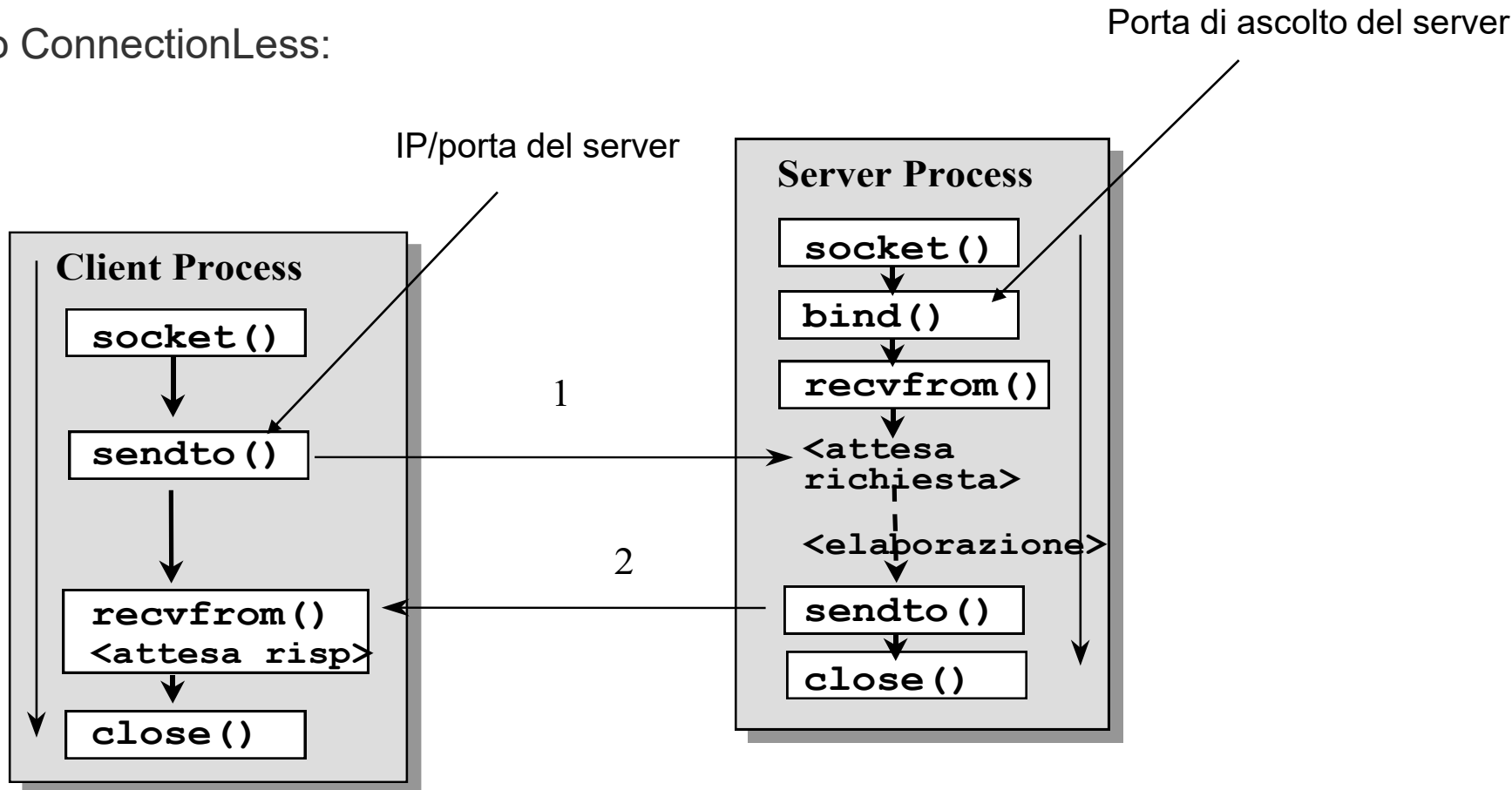
La porta e' un identificativo numerico (**indirizzo di porta**) che rappresenta il punto di arrivo di una connessione su di un host. La coppia (IPaddr, Port) identifica quindi univocamente un estremo di una connessione ed è detta **Socket**.



Strato 4 di TCP/IP : API

Attraverso le Berkeley Socket Library lo strato di trasporto di TCP/IP fornisce le API per implementare un modello di comunicazione **Client/Server** di tipo ConnectionLess o ConnectionOriented.

Esempio ConnectionLess:



Strato 5 di TCP/IP: Applicativo

Il modello client-server richiede che sia ben identificabile e indirizzabile il server. Le porte TCP o UDP assegnate ad applicativi con ampia diffusione vengono assegnate da un organismo internazionale (IANA) e prendono il nome di [Well Known Ports](#). Contrariamente le porte dei client vengono determinate dinamicamente dal sistema operativo al momento dell'accesso al server.

Esistono alcuni applicativi “storici” di TCP/IP quali:

- telnet (23/TCP) per il servizio di terminale remoto a linea di comando
- smtp (25/TCP) per il servizio di posta elettronica
- ftp (20/TCP e 21/TCP) per il trasferimento di file

Altri importanti applicativi si sono aggiunti successivamente, tra cui:

- dns (53/UDP) per la traduzione dei nomi
- http (80/TCP) per il trasferimento di ipermedia (WWW).

Ogni applicativo assegna ai propri oggetti un **indirizzo specifico** mnemonico.

Esempio di questi indirizzi sono www.unipr.it per il servizio Web e alfieri@unipr.it per il servizio di posta elettronica.

Sicurezza delle reti

L'utilizzo pervasivo delle reti anche in ambiti critici come l'economia, la finanza e la salute ha portato ad una attenzione crescente sulla sicurezza nell'utilizzo delle reti e ad una conseguente revisione delle architetture di rete a tutti i livelli.

A livello architetturale viene definito un perimetro delle risorse da difendere (Rete locale o singolo PC) che viene protetto con strumenti di controllo e limitazioni (riduzione della superficie d'attacco) rispetto a possibili attacchi informatici provenienti dall'esterno, introducendo strumenti come Firewall, Intrusion Detection/Prevention Systems e, più recentemente, strumenti di Intelligence con la CyberSecurity.

A livello dei protocolli un ruolo fondamentale è dato dall'introduzione di **strumenti crittografici** per rafforzare servizi di sicurezza come l'autenticazione, la riservatezza e il non ripudio. L'utilizzo della crittografia sta portando ad una graduale sostituzione dei protocolli di rete sia a livello applicativo (HTTPS, IMAPS, LDAPS, ecc) che ai livelli sottostanti (SSL, IPsec, ecc).

Contenuti del corso

Lezioni:

- Il **livello fisico** e la telefonia.
- Il **livello link** e Ethernet
- Il **livello rete**, IPv4, protocolli di servizio, IPv6, protocolli di routing.
- Il **livello trasporto**, UDP, TCP, programmazione di rete, gestione della congestione
- Il **livello applicativo**, DNS, Posta elettronica e WWW.
- **Sicurezza delle reti**, crittografia applicata, la sicurezza nei protocolli.

Laboratorio:

- Net-tools e Net-sniffing
- Net-programming
- WWW server e client
- Networking con Docker
- Crittografia applicata con OpenSSL
- Virtualhost SSL, programmazione SSL, password cracking