

INTERNET : rete di calcolatori che interconnette dispositivi di calcolo in tutto il mondo

Vengono connessi a internet sistemi non tradizionali (pc, tablet, smartphone, console ...) detti HOST o SISTEMI PERIFERICI (end system)

↓

connessi tra loro tramite **rete di collegamenti** e
PACKET SWITCH.

Collegamenti diversi possono trasmettere dati a velocità differenti.

⇒ **VELOCITA' DI TRASMISSIONE** (transmission rate) → bps

PACCHETTO = insieme di informazioni risultanti dall' invio di dati ad un altro host , suddivisi in sottoparti aventi ciascuna un'intestazione .

commutatori di pacchetto
inviati nel nucleo della rete

inviati nel nucleo della rete

LINK-LAYER SWITCH : usati nelle reti d'accesso

commutatori a livello di collegamento

inviati nel nucleo della rete

sequenza di collegamenti e commutatori attraversata dal singolo pacchetto = **PERCORSO / ROUTE / PATH**

Gli hosts accedono a Internet tramite gli ISP

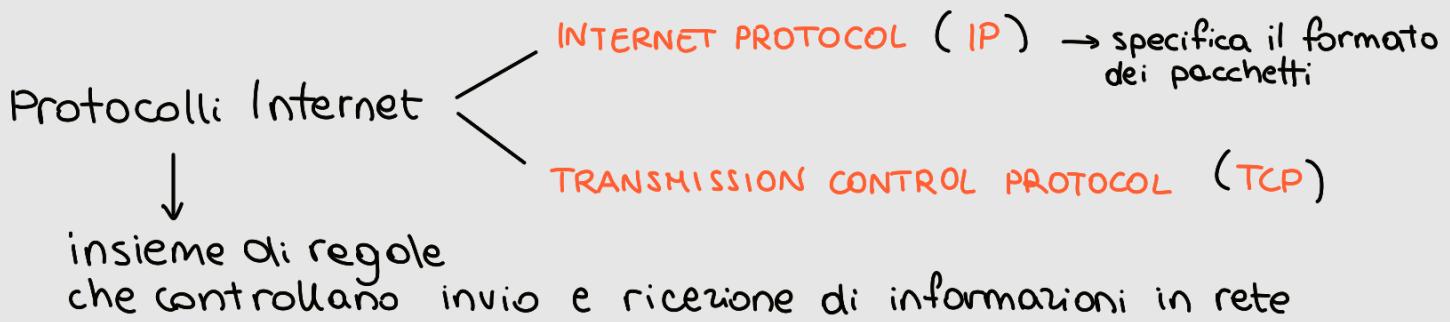
(INTERNET SERVICE PROVIDERS) che comprendono:

- ISP residenziali (= compagnie telefoniche)
- ISP aziendali
- ISP universitari
- ISP che forniscono WiFi in luoghi pubblici (hotel, bar, aeroporti etc)



per consentire la comunicazione: connessi a ISP nazionali e internazionali.

Ciascuna rete di un ISP è gestita in modo indipendente e fa uso del protocollo IP



INTERNET ^(anche) = infrastruttura che fornisce servizi alle applicazioni

Vengono eseguite sui Sistemi periferici e non sui router

APPLICAZIONI DISTRIBUITE:

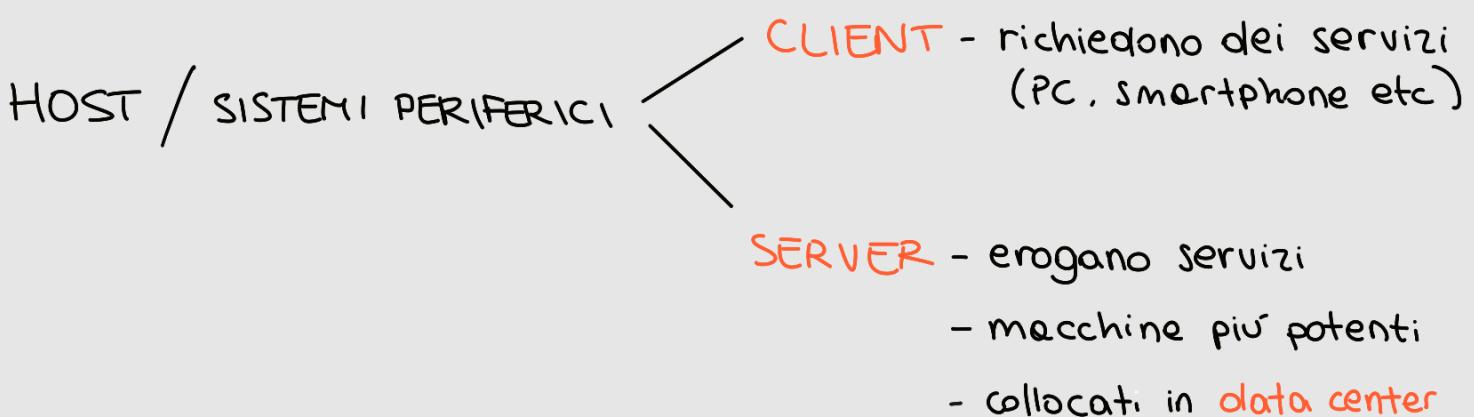
coinvolgono più host che si scambiano reciprocamente dati.

Gli host collegati a Internet forniscono delle API (application programming interface) che specificano come il pezzo di software eseguito su un host possa chiedere a internet di recapitare dati ad un altro specifico host.

⇒ API = insieme di regole che il modulo software mittente deve seguire in modo che i dati siano recapitati al programma di destinazione

Qualsiasi attività in Internet che coinvolge due o più entità remote in comunicazione viene governata da un **protocollo**.

N.B. **PROTOCOLLO** : definisce il formato e l'ordine dei messaggi scambiati tra due o più entità in comunicazione , così come le azioni intraprese in fase di trasmissione e/o ricezione di un messaggio



ACCESS NETWORK = rete che connette fisicamente un sistema (reti di accesso) al suo **edge router** (primo router sul path)

ACCESSO RESIDENZIALE

DSL (digital subscriber line):

- la compagnia telefonica assume il ruolo di ISP
- accesso asimmetrico : velocità di trasmissione in downstream ≠ upstream

cable based (via cavo)

- utilizza infrastrutture esistenti della televisione via cavo
- sistema HYBRID FIBER COAX (HFC) (fibra ottica + cavo coassiale)
- richiede modem speciali (cable modem) che dividono la rete HFC in due canali
- accesso asimmetrico

IMPORTANTE: HFC rappresenta un mezzo di trasmissione condiviso.

Ciascun pacchetto inviato dalla stazione di testa (^{cable head end}) viaggia sul canale di downstream in tutti i collegamenti e verso ogni abitazione;

ciascun pacchetto inviato da un'abitazione viaggia sul canale di upstream verso la stazione di testa.

E' richiesto un protocollo di accesso multiplo distribuito per coordinare la trasmissione ed evitare collisioni.

ETHERNET: utilizza doppino di rame intrecciato per collegare numerosi host tra loro e connetterli a uno switch ethernet che viene connesso a internet.

Per eseguire i propri compiti le applicazioni scambiano messaggi.

La sorgente suddivide i messaggi lunghi in parti più piccole → **PACCHETTI** → vengono trasmessi su ciascun collegamento a una velocità pari alla velocità totale di trasmissione del collegamento stesso.

$$\left. \begin{array}{l} \text{Pacchetto di } L \text{ bit} \\ \text{Canale con velocità } R \text{ bps} \end{array} \right\} \text{TEMPO DI TRASMISSIONE} \quad T = \frac{L}{R}$$

TRASMISSIONE STORE-AND-FORWARD: il commutatore deve ricevere l'intero pacchetto prima di poterne cominciare la trasmissione.

I router necessitano di ricevere, memorizzare ed elaborare l'intero pacchetto prima di inoltrarlo.

TRASMISSIONE DI UN PACCHETTO DALLA SORGENTE ALLA DESTINAZIONE SU UN PERCORSO DI N CONNESSIONI OGNUNO CON VELOCITÀ DI TRASMISSIONE R :

$$d_{\text{end-to-end}} = N \cdot \frac{L}{R}$$

Per ogni collegamento, il commutatore mantiene un **BUFFER (coda)** di **OUTPUT** per conservare i pacchetti che sta per inviare su quel collegamento.
=> i pacchetti subiscono anche **ritardi di accodamento**, che sono variabili e dipendono dal livello di traffico nella rete.

La dimensione dei buffer è finita => se un pacchetto in arrivo trova il buffer completamente riempito, si verifica una **PERDITA DI PACCHETTO (packet loss)**

COME FA IL ROUTER A DETERMINARE SU QUALE COLLEGAMENTO IL PACCHETTO DOVREBBE ESSERE INOLTRATO ?

Ogni host ha un IP.

Ogni pacchetto contiene nell'intestazione l'IP della sua destinazione che presenta una struttura gerarchica.

Quando un pacchetto giunge a un router nella rete, quest'ultimo esamina una parte dell'IP di destinazione e lo inoltra a un router adiacente.

Ogni router ha una **TABELLA DI INOLTRO** (forwarding table) che mette in relazione gli IP di destinazione con i collegamenti in uscita.

COME VENGONO IMPOSTATE LE TABELLE DI INOLTRO?

Internet ha protocolli di instradamento (ROUTING PROTOCOL) specifici che usa per impostare automaticamente le tabelle di inoltro.

Per spostare i dati nella rete esistono due approcci:

• COMMUTAZIONE DI CIRCUITO

- le risorse lungo un percorso sono riservate per l'intera durata della sessione di comunicazione
- es. reti telefoniche
- velocità di trasmissione costante per la durata della connessione
- implementato tramite multiplexing a divisione di frequenza (FDM) oppure multiplexing a divisione di tempo (TDM)
- **DI SPENDIOSA** → i circuiti dedicati sono inattivi durante i periodi di silenzio

N.B. - tempo di trasmissione INDIPENDENTE dal numero di collegamenti

AMPIEZZA DI BANDA = BANDWIDTH

PARLEREMO DI RETI A COMMUTAZIONE DI PACCHETTO

Ad ogni tappa, il pacchetto subisce vari tipi di ritardo:

- ritardo di ELABORAZIONE (processing delay)
- ritardo di ACCODAMENTO (queuing delay)

$\frac{L}{R}$ ← • ritardo di TRASMISSIONE (transmission delay)

RITARDO TOTALE DI NODO
(nodal delay)

DISTANZA
DAL ROUTER
VELOCITA'
PROPAGAZIONE

$\frac{d}{v_p}$ ← • ritardo di PROPAGAZIONE (propagation delay)

Il ritardo di elaborazione è spesso trascurabile MA può influenzare pesantemente il THROUGHPUT massimo del router (= velocità max di trasmissione del router)

Il ritardo di accodamento puo' variare da pacchetto a pacchetto e diventa rilevante se il traffico arriva a raffiche

=> progettare il sistema in modo che l'INTENSITA' DI TRAFFICO non superi 1

$$\frac{La}{R}$$

La → velocità media di arrivo dei bit in coda
R → velocità di trasmissione

Quando una coda e' piena e arriva un pacchetto (che verrà perduto) si verifica **buffer overflow**.

La frazione di pacchetti perduti aumenta in proporzione all'intensità di traffico.

Per ottenere una misura efficiente dei ritardi → TRACEROUTE

programma diagnostico eseguibile su qualsiasi host

PROTOCOLLI → organizzati per **livelli o strati** (layer).

MODELLO DI SERVIZIO (service model) di un livello :

- ogni livello fornisce il suo servizio effettuando determinate azioni all'interno dello stesso e utilizzando i servizi del livello immediatamente inferiore.
- Un livello puo' essere implementato via software, hardware o con una combinazione dei due.
- La modularità rende più facile aggiornare la componentistica.
- **PILA DI PROTOCOLLI** (protocol stack) → 5 livelli

APPLICATION	5
TRANSPORT	4
NETWORK	3
LINK	2
PHYSICAL	1

5 - **APPLICATION LAYER** : e' la sede delle applicazioni di rete e dei relativi protocolli (HTTP, SMTP, FTP, ...).

Un protocollo a livello di applicazione e' distribuito su piu' sistemi periferici, tramite i quali vengono scambiati pacchetti di informazioni , detti **messaggi**.

4 - **TRANSPORT LAYER** : trasferisce i messaggi da un processo ad un altro , usando i servizi del livello di rete.

Due protocolli di trasporto

TCP (fornisce un servizio legato alla connessione)

UDP (fornisce un servizio senza connessione)

Pacchetti nel transport layer = **SEGMENTI**

3 - **NETWORK LAYER** : trasferisce i pacchetti a livello di rete (= **DIAGRAMMI**) da un host a un altro.

Mette a disposizione il servizio di consegna del segmento al livello di trasporto nell'host di destinazione.

Comprende il protocollo IP e variati protocolli di instradamento.

2 - **LINK LAYER** : instrada un diagramma attraverso una serie di router tra sorgente e destinazione.

A ogni nodo , il livello di rete passa il diagramma al link layer , che lo porta al nodo successivo.

Pacchetti a livello di collegamento = **FRAME**

1 - **PHYSICAL LAYER** : trasferisce i singoli bit del frame da un nodo a quello successivo.

I protocolli sono dipendenti dal collegamento e dal mezzo trasmittivo (doppino, fibra ottica,...)

INCAPSULAMENTO : i router e i commutatori al link layer sono tutti commutatori di pacchetto e organizzano il loro hardware e software di rete a livelli. Non implementano tutti i livelli della pila, ma solo quelli inferiori

⇒ i commutatori a link layer implementano 1 e 2.

i router implementano da 1 a 3.

⇒ A ciascun livello, il pacchetto ha due tipi di campi:

INTESTAZIONE e **PAYLOAD**.

NETWORK SECURITY

MALWARE = contenuti "cattivi" che possono infettare i dispositivi.

↳ molti sono auto replicanti

VIRUS = malware che richiedono una qualche interazione con l'utente per infettare il dispositivo.

WORM = malware che possono accedere al dispositivo senza alcuna interazione esplicita con l'utente.

DoS = DENIAL OF SERVICE = negazione del servizio

↳ rende inutilizzabile dagli utenti una rete, un host o un'altra parte di infrastruttura.

↳ TRE CATEGORIE

- ─ Attacchi alla vulnerabilità dei sistemi
- ─ Bandwidth flooding
- ─ Connection flooding

PACKET SNIFFING : un ricevitore passivo memorizza una copia di ciascun pacchetto che transita (che puo' contenere dati personali, password, etc)

IP SPOOFING : capacita' di immettere pacchetti in Internet con un indirizzo sorgente falso.

LINEE DI DIFESA :

- **AUTENTICATION** - ad es. via SIM card
- **CONFIDENTIALITY** - attraverso crittografia
- **INTEGRITY CHECKS** - firme digitali rivelano le manomissioni
- **ACCESS RESTRICTIONS** - VPN
- **FIREWALLS** - monitora il traffico in entrata e uscita