Gli ingranaggi dell'Internet sono costituiti da una vasta rete di dispositivi di calcolo connessi tra loro, gestiti da un insieme di protocolli e standard che regolano l'invio e la ricezione dei messaggi. Questa rete comprende:

Host (Sistemi Periferici): I dispositivi periferici, come PC desktop, server, dispositivi mobili e altri oggetti fisici connessi (IoT), che eseguono le applicazioni di rete ai bordi dell'Internet.

Commutatori di Pacchetto: Dispositivi come router e switch che inoltrano i pacchetti di dati attraverso la rete.

Reti di Collegamenti: Utilizzano una varietà di tecnologie, tra cui fibre ottiche, cavi in rame, collegamenti radio e satellitari, per trasmettere dati ad un certo tasso di trasmissione (bandwidth).

ISP Interconnessi: Una rete di Internet Service Providers che formano la "rete di reti" dell'Internet.

Protocolli e Standard: Come HTTP, TCP/IP, WiFi, 4/5G, Ethernet, gestiscono la comunicazione e regolano il funzionamento di Internet.

Organizzazioni di Standardizzazione: Come IETF e IEEE, che definiscono e mantengono gli standard per le tecnologie di rete.

Servizi e Applicazioni (Infrastruttura): Internet fornisce una vasta gamma di servizi alle applicazioni, tra cui Web, streaming multimediale, e-commerce, social media, e altro ancora.

Interfaccia di Programmazione (API): Permette alle applicazioni di accedere e utilizzare i servizi di trasporto di Internet in modo simile al servizio postale, offrendo molte opzioni di servizio.

In sintesi, l'Internet è una complessa infrastruttura che collega miliardi di dispositivi e fornisce una vasta gamma di servizi e possibilità di connessione per le applicazioni distribuite in tutto il mondo.

I protocolli di rete sono fondamentali per governare l'intera comunicazione su Internet, definendo il formato e l'ordine dei messaggi scambiati tra dispositivi, come client e server, e regolando le azioni durante la trasmissione e la ricezione dei messaggi.

host: client (richiedono servizi) e server (erogano servizi) (server spesso nei data center).

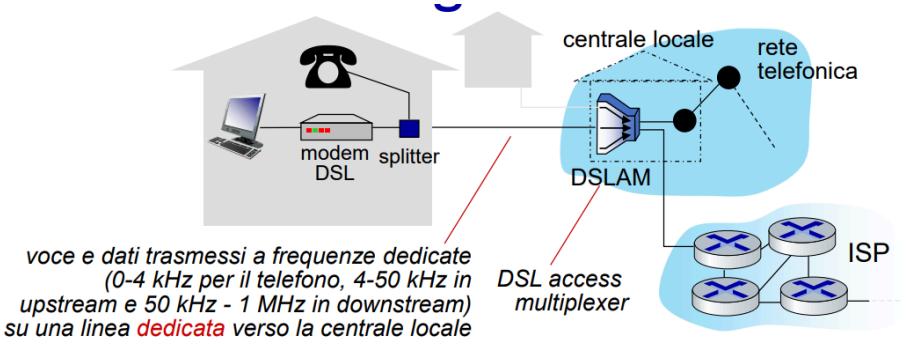
Il cloud computing permette l'accesso on-demand a risorse IT tramite Internet, eliminando la necessità di possedere e mantenere infrastrutture fisiche come data center e server.

Le reti di accesso, sia cablate che wireless, connettono i sistemi periferici e gli edge router, facilitando l'accesso agli utenti residenziali, aziendali e mobili attraverso reti come WiFi e 4G/5G.

Nei collegamenti via cavo, come HFC (Hybrid Fiber Coax), si utilizza il multiplexing a divisione di frequenza per trasmettere canali diversi su bande di frequenza diverse, consentendo velocità di trasmissione asimmetriche per downstream(download concorrenti avvengono ciascuno a velocità inferiori alla velocità totale del canale di downstream) e upstream (necessità di un protocollo di accesso multiplo distribuito per coordinare le trasmissioni).

Le reti DSL (Digital Subscriber Line) sfruttano le linee telefoniche esistenti, offrendo velocità asimmetriche di trasmissione dedicate per download e upload, limitate da fattori come la distanza e

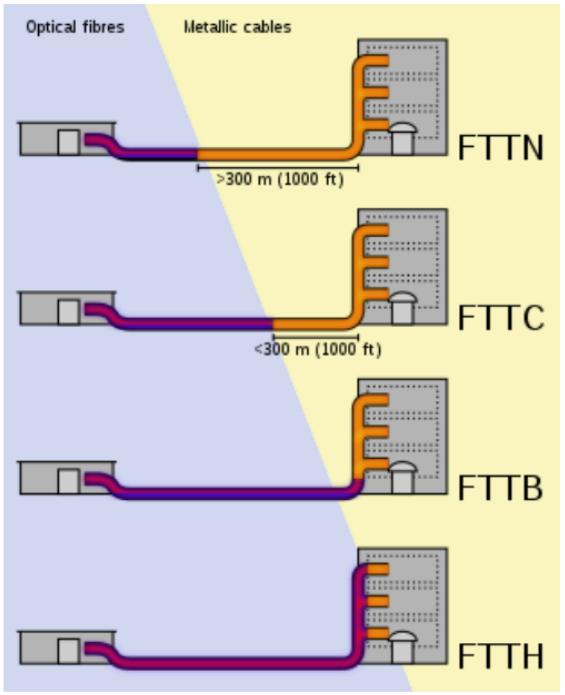
la qualità del materiale, N.B. Asimmetrico (velocità effettive inferiori per limitazioni del provider, distanza, qualità materiale e interferenze).



FFTTx:

Le reti di accesso offrono una varietà di tecnologie per connettere gli utenti alle infrastrutture di rete. Queste includono:

FTTH (Fiber-to-the-home)
FTTB (Fiber-to-the-building/basement)
FTTC (Fiber-to-the-cabinet) ,**FTTS** (Fiber-to-the-street)
FTTN (Fiber-to-the-node)
FTTW (Fiber-to-the-wireless) , **FTTR** (Fiber-to-the-radio).



Queste sigle indicano diverse modalità di distribuzione della fibra ottica, con velocità che variano da 1 Gbps in downlink per FTTH a velocità più basse per le altre varianti, a seconda della distanza dalla destinazione finale.

Architetture:

- Active Optical Network (AON) : Ethernet commutate in grado di ricevere/trasmettere segnali ottici.
- Passive Optical Network (PON) : Splitter ottici non alimentati che trasmettono in broadcast.

Fixed Wireless Access: Utilizza una combinazione di fibra e tecnologie radio, inclusi il 5G, per raggiungere i clienti, offrendo velocità fino a 100 Mbps.

Reti Domestiche: Spesso integrate in un unico dispositivo, includono access point wireless WiFi, modem via cavo o DSL, router, firewall e Ethernet cablata.

Reti di Accesso Wireless: Comprendono reti locali wireless (WLANs), che operano tipicamente entro o intorno agli edifici, con velocità che variano da 11 Mbps a 450 Mbps. Per l'accesso su scala geografica, sono utilizzate reti cellulari come il 4G Plus, che può raggiungere velocità fino a 300 Mbps.

Reti di Accesso Aziendale: Utilizzate da aziende e università, queste reti combinano tecnologie cablate e wireless, offrendo accesso a velocità variabili tra 100 Mbps e 10 Gbps sia tramite Ethernet che WiFi.

Reti dei Data Center: Caratterizzate da collegamenti ad alta larghezza di banda, collegano centinaia o migliaia di server tra loro e a Internet, con velocità che possono variare da decine a centinaia di Gbps.

Gli host inviano pacchetti di dati seguendo un processo che include la suddivisione del messaggio dell'applicazione in frammenti più piccoli, noti come pacchetti (di lunghezza L bit) , e la trasmissione di questi pacchetti nella rete di accesso a un determinato tasso di trasmissione R (bits/sec), definito come il **tasso di trasmissione del collegamento** o la capacità del link.
Il ritardo di trasmissione del pacchetto = tempo necessario per trasmettere pacchetti di L bit nel collegamento = $L\ (bits)/\ R\ (bits/sec)$

I mezzi trasmissivi possono essere **guidati**, come il doppino di rame intrecciato, il cavo coassiale e la fibra ottica, o **non guidati**, come i canali radio. Il doppino di rame intrecciato offre varie categorie (cat5 e cat6) con velocità di trasmissione fino a 10Gbps per brevi distanze. Il cavo coassiale è bidirezionale e offre larghezza di banda multipla, mentre la fibra ottica consente trasmissioni ad alta velocità (decine e centinaia di Gbps) con bassa attenuazione del segnale e tassi di errore ridotti.

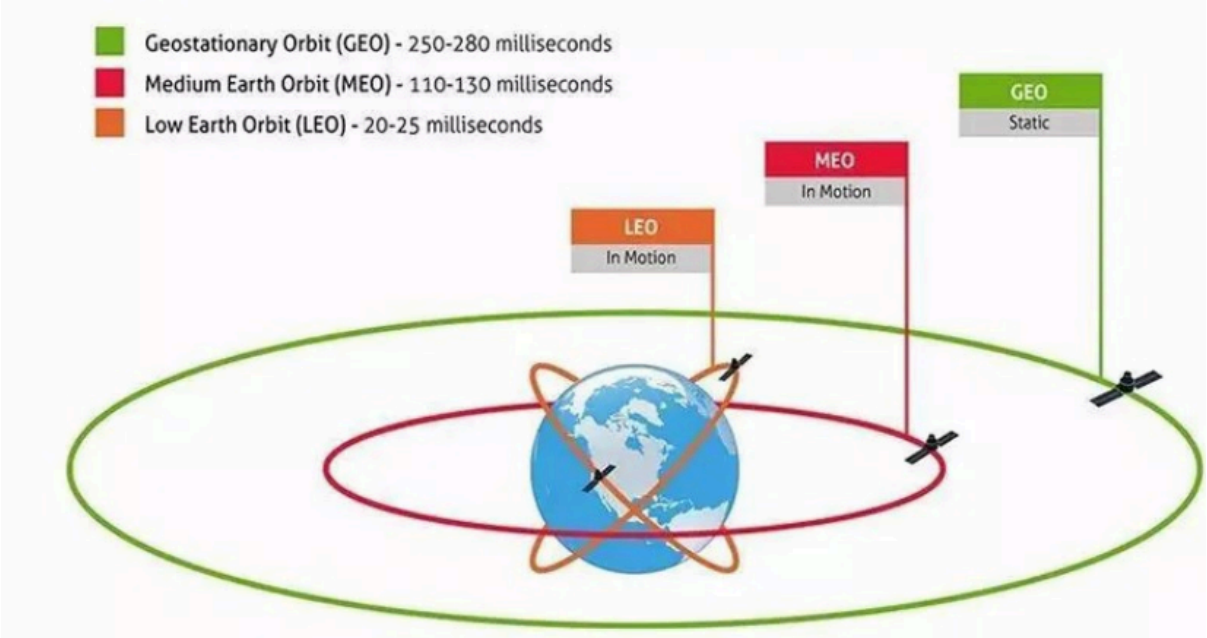
I canali radio trasportano segnali nell'ambiente elettromagnetico, offrendo opzioni come WLAN (WiFi) con velocità di decine/centinaia di Mbps, wide-area networks come il 4G con velocità fino a 300 Mbps su distanze di ~10 km, Bluetooth per distanze brevi e microonde terrestri e satellitari per trasmissioni punto-punto con velocità fino a 45 Mbps e oltre 100 Mbps rispettivamente.

I satelliti per le telecomunicazioni possono essere suddivisi in due categorie principali: quelli in orbita geostazionaria (GEO) e quelli in orbita terrestre bassa (LEO).

Satelliti GEO: Si trovano in orbita geostazionaria, sincronizzati con la rotazione terrestre, quindi appaiono immobili nel cielo. Offrono un'ampia copertura e sono ideali per servizi di comunicazione su larga scala. Tuttavia, presentano un'elevata latenza a causa della grande distanza tra il satellite e la Terra.

Satelliti LEO: Sono in orbita terrestre bassa e non sono limitati a un'orbita equatoriale. Si spostano rapidamente nel cielo, quindi per fornire copertura continua di un'area è necessario un sistema di costellazione. Anche se la loro copertura può essere più limitata rispetto ai satelliti GEO, offrono tempi

di latenza inferiori e possono essere più adatti per applicazioni che richiedono una connessione più reattiva.

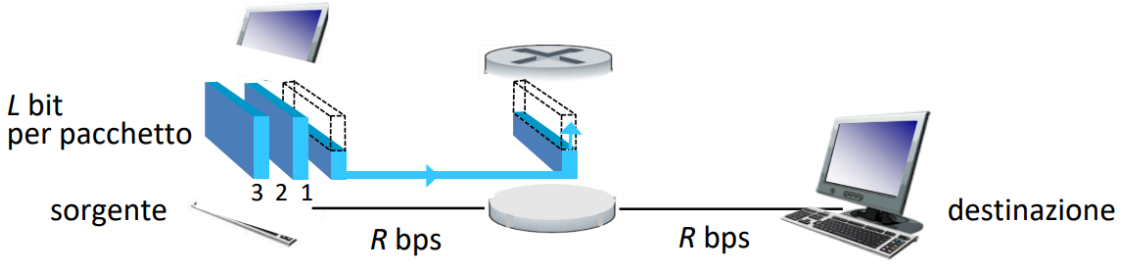


In generale, i satelliti per le telecomunicazioni fungono da ripetitori tra le stazioni a terra e possono essere utilizzati per fornire servizi di comunicazione su vasta scala.

Il nucleo della rete è costituito da una maglia di commutatori di pacchetti e collegamenti che interconnettono i sistemi periferici di Internet. Questo nucleo opera attraverso la commutazione di pacchetto (packet-switching) , dove i messaggi vengono suddivisi in pacchetti (packets) e inoltrati da un router al successivo (forwards) lungo un percorso dalla sorgente alla destinazione(path o route).

Le due funzioni chiave del nucleo della rete sono l'**inoltro** (forwarding) e l'**istradamento** (routing). L'inoltro è un'azione locale che sposta i pacchetti dal collegamento di ingresso al collegamento di uscita appropriato, mentre l'istradamento è un'azione globale che determina i percorsi dei pacchetti dalla sorgente alla destinazione attraverso algoritmi di instradamento.

La commutazione di pacchetto avviene tramite il metodo store-and-forward, che introduce un ritardo di trasmissione (delay) dovuto al tempo necessario per trasmettere i pacchetti attraverso i collegamenti (L/R secondi per trasmettere packets di L bits attraverso un collegamento a R bps) .



Commutazione di pacchetto: store-and-forward (1)

Ritardo da un capo all'altro (end-to-end) per la trasmissione di 1 pacchetto su un percorso di N collegamenti di pari velocità R:

$d_{end-to-end} = N * (L/R)$

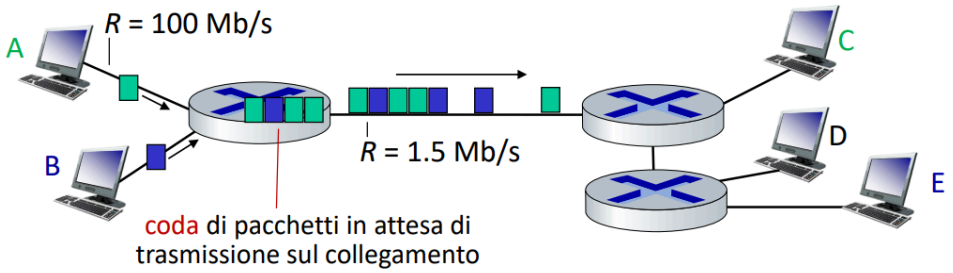
Trascurando il ritardo di propagazione e altre forme di ritardo.

Commutazione di pacchetto: store-and-forward (2)

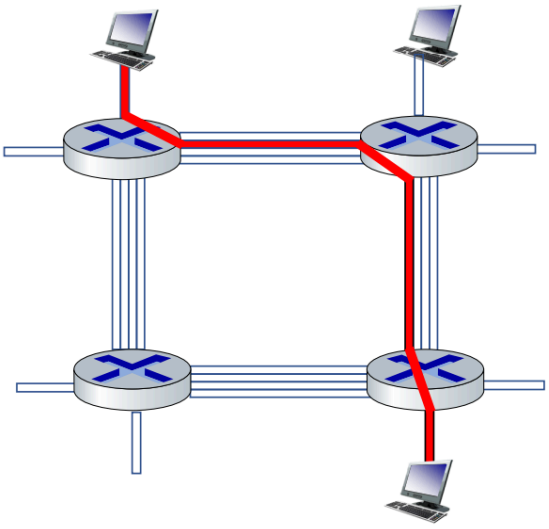
Ritardo da un capo all'altro (end-to-end) per la trasmissione di P pacchetto su un percorso di N collegamenti di pari velocità R:
$d_{end-to-end} = (N + P - 1) *(L/R)$

Trascurando il ritardo di propagazione e altre forme di ritardo.

L'accodamento si verifica quando i pacchetti arrivano più velocemente di quanto possano essere serviti, portando a un accumulo di pacchetti in attesa di essere trasmessi e potenzialmente causando la perdita di pacchetti se la memoria di buffer si riempie.

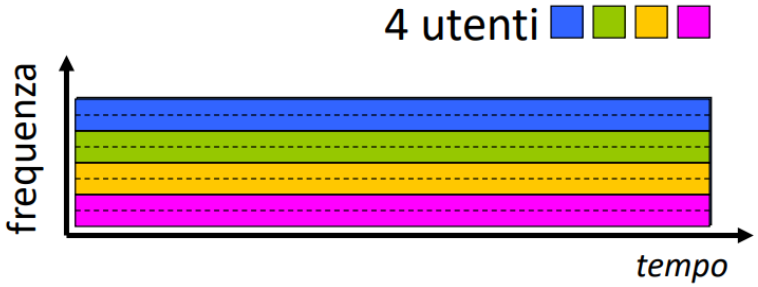


Nella commutazione di circuito, le risorse lungo un percorso sono riservate per l'intera durata della sessione di comunicazione, garantendo una velocità costante e dedicata per la trasmissione dei dati. Questo metodo viene comunemente utilizzato nella rete telefonica tradizionale e comporta l'assenza di condivisione delle risorse.

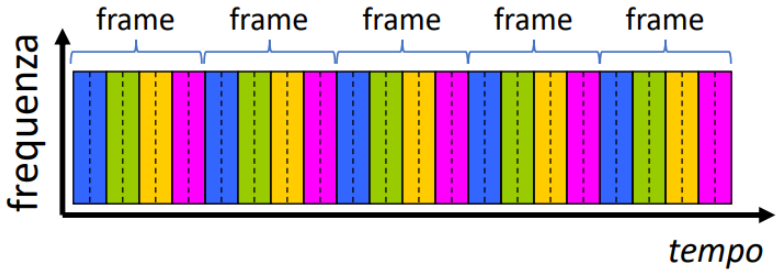


Due tecniche utilizzate nella commutazione di circuito sono il **Multiplexing a Divisione di Frequenza** (***FDM***) e il **Multiplexing a Divisione di Tempo** (***TDM***).

FDM: Consiste nella suddivisione dello spettro di frequenza di un collegamento in bande separate, con ciascun circuito che ha la sua banda dedicata e può trasmettere alla massima velocità all'interno di quella banda. L'idea di base si basa sulla combinazione di segnali a frequenze diverse in un unico segnale, che può poi essere suddiviso nuovamente nelle sue componenti originali.



TDM: Prevede la suddivisione del tempo in frame di durata fissa, ciascuno suddiviso in un numero fisso di slot temporali. Ogni circuito riceve slot periodici e può trasmettere alla massima velocità durante i propri slot temporali.



In sintesi, la commutazione di circuito garantisce risorse dedicate e una velocità costante per la trasmissione dei dati lungo il percorso, utilizzando tecniche come FDM e TDM per ottimizzare l'utilizzo delle risorse disponibili.

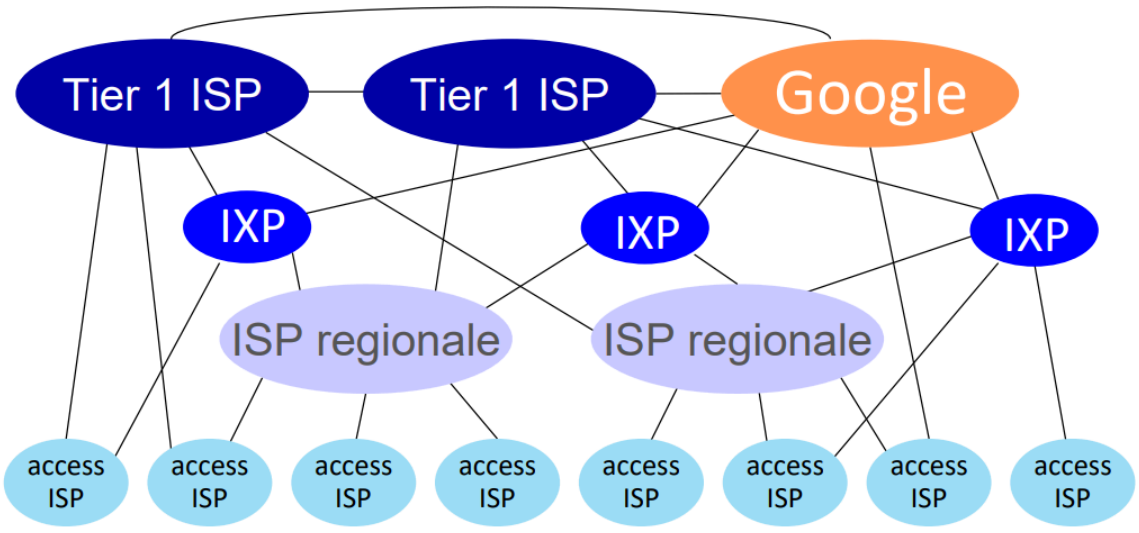
La commutazione di pacchetto e la commutazione di circuito presentano vantaggi e svantaggi distinti. La commutazione di pacchetto è adatta per dati a "raffica" con necessità variabili di trasmissione, consentendo una condivisione efficiente delle risorse e l'allocazione su richiesta. Tuttavia, può causare congestione e ritardi imprevedibili, richiedendo protocolli aggiuntivi per il trasferimento affidabile dei dati. Al contrario, la commutazione di circuito offre una velocità costante e dedicata, ma richiede risorse dedicate per l'intera durata della comunicazione, risultando meno efficiente per dati a raffica. Inoltre, entrambi i metodi possono affrontare sfide nella gestione dei servizi in tempo reale come la telefonia e la videoconferenza, dove la latenza e la perdita di pacchetti possono compromettere la qualità del servizio.

$$= 1 - \sum_{i=0}^{10} P(utenti\ attivi = i) = 1 - \sum_{i=0}^{10} \binom{35}{i} 0.1^i (1-0.1)^{35-i} =$$

$$= 1 - \sum_{i=0}^{10} \frac{35!}{i!\,(35-i)!} 0.1^i (1-0.1)^{35-i} \leq 0.0004$$

Internet è strutturata come una "rete di reti", dove i sistemi periferici accedono tramite Internet Service Provider (ISP) di accesso che, a loro volta, devono essere interconnessi. Questa complessa rete è guidata dall'economia e dalle politiche nazionali. Collegare direttamente ogni ISP di accesso non è scalabile, quindi si ricorre a Internet Exchange Points (IXP) dove gli ISP possono fare peering tra di loro, stabilendo connessioni dirette a costo zero. Le reti regionali emergono per collegare le reti di accesso agli ISP.

Al centro di Internet vi sono poche grandi reti ben connesse, come gli ISP commerciali "tier-1" con copertura nazionale e internazionale. Inoltre, reti di fornitori di contenuti come Google e Facebook gestiscono le proprie reti private per avvicinare i servizi agli utenti, aggirando talvolta gli ISP tier-1 e regionali.



I **ritardi** e le **perdite** nei pacchetti si verificano principalmente a causa dell'**accodamento** dei pacchetti nei buffer dei router quando il tasso di arrivo dei pacchetti supera temporaneamente la capacità del collegamento. Se i buffer si riempiono, si verifica la perdita dei pacchetti.

Il ritardo per i pacchetti è causato principalmente da quattro fattori:

Ritardo di elaborazione del nodo (**delab**): Coinvolge il controllo degli errori sui bit, la determinazione del canale di uscita e altri processi nel router. Tipicamente, questo ritardo è molto breve, nell'ordine dei microsecondi.

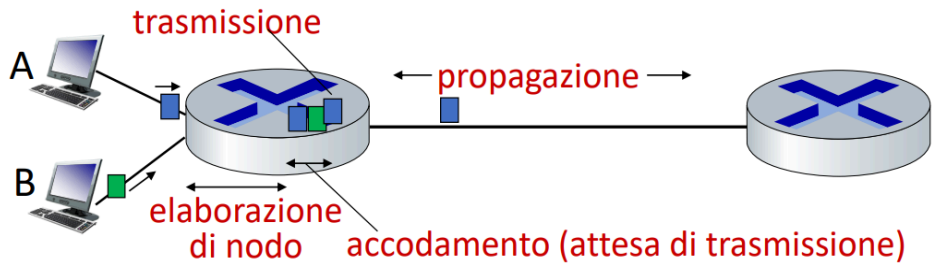
Ritardo di accodamento (**dacc**): È dovuto all'attesa dei pacchetti in coda per la trasmissione e dipende dal livello di congestione del router.

Ritardo di trasmissione (**dtrasm**): Dipende dalla lunghezza del pacchetto (L in bit) e dal tasso di trasmissione del collegamento (R in bps). È calcolato come rapporto tra la lunghezza del pacchetto e il tasso di trasmissione del collegamento. « L/R»

Ritardo di propagazione (**dprop**): Dipende dalla lunghezza fisica del collegamento (d) e dalla velocità di propagazione del segnale (v). È calcolato come rapporto tra la lunghezza del collegamento fisico e la velocità di propagazione. «d/v»

dnodo = delab + dacc + dtrasm + dprop

Questi ritardi possono essere molto diversi tra loro, ma tutti contribuiscono al ritardo totale di un pacchetto.



Il **ritardo end-to-end** (o punto-punto) di un pacchetto in un sistema di commutazione di pacchetto è determinato dalla somma dei ritardi accumulati durante il percorso dalla sorgente alla destinazione. Questo include il ritardo di elaborazione del nodo, il ritardo di accodamento, il ritardo di trasmissione e il ritardo di propagazione.
$d_{end-to-end}$ = ? ($delabi$ + $dacci$ + $dtrasmi$ + $dpropi$)

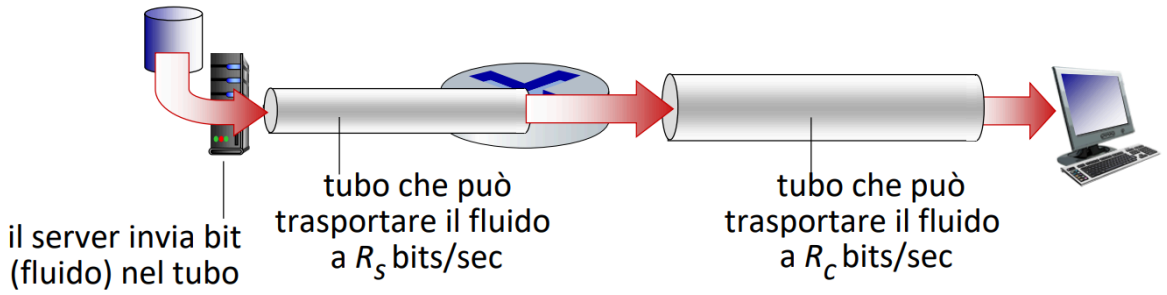
Il ritardo di accodamento dei pacchetti dipende dalla velocità media di arrivo dei pacchetti (a), dalla lunghezza del pacchetto (L) e dalla velocità di trasmissione (R). È calcolato come (L * a) / R, dove (L * a) rappresenta la velocità di arrivo dei bit e R la velocità di servizio dei bit. Un ritardo di accodamento elevato si verifica quando il tasso di arrivo dei pacchetti supera la capacità del collegamento.
La/R ~ 0: ritardo medio di accodamento piccolo
La/R -> 1: ritardo medio di accodamento grande
La/R > 1: più "lavoro" in arrivo di quanto possa essere servito - ritardo tende all'infinito

Traceroute è un programma diagnostico che fornisce una misura del ritardo dalla sorgente al router lungo i percorsi Internet punto-punto verso la destinazione. Utilizza pacchetti con il campo time-to-live per ottenere informazioni sui router lungo il percorso.

La perdita di pacchetti si verifica quando la coda (o buffer) precedente a un collegamento ha capacità finita e un pacchetto trova la coda piena, venendo quindi scartato. I pacchetti persi possono essere

ritrasmessi dal nodo precedente o dal sistema terminale che li ha generati, oppure non essere ritrasmessi affatto.

Il **throughput** rappresenta la frequenza alla quale i bit sono trasferiti tra mittente e ricevente, espresso in bit per unità di tempo. Può essere istantaneo, misurato in un determinato istante, o medio, calcolato su un periodo più lungo.



Nel caso in cui la velocità di trasmissione del mittente (Rs) sia minore o uguale alla velocità di ricezione del ricevente (Rc), il throughput medio end-to-end è limitato dalla velocità di trasmissione o ricezione più bassa.

Invece, se la velocità di trasmissione del mittente è maggiore della velocità di ricezione del ricevente, il throughput medio end-to-end è limitato dalla velocità di ricezione del ricevente.

Il ***collo di bottiglia*** si verifica quando un collegamento su un percorso punto-punto vincola il throughput end-to-end.

Nello scenario di Internet, il throughput end-to-end dipende dalla velocità di trasmissione dei collegamenti attraversati dal flusso di dati. In condizioni di basso traffico, il throughput può essere approssimato alla velocità di trasmissione del collegamento più lento nel percorso. Tuttavia, in presenza di altri flussi di dati, la velocità di trasmissione di un collegamento deve essere suddivisa tra i vari flussi che lo attraversano.

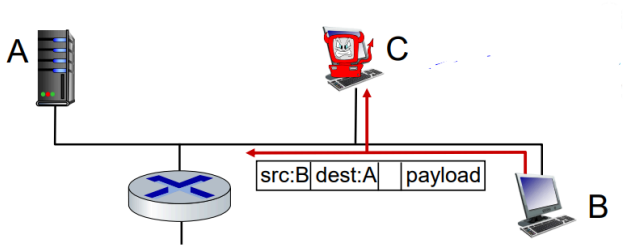
Il throughput effettivo può essere inferiore a causa di fattori aggiuntivi, come i protocolli utilizzati.

Schema sugli attacchi alla rete

Intercettazione dei pacchetti

Analisi dei pacchetti (packet sniffing):

- Media di trasmissione: Ethernet condivisa, wireless
- Un'interfaccia di rete promiscua legge e registra tutti i pacchetti (ad esempio, anche le password!) che la attraversano.

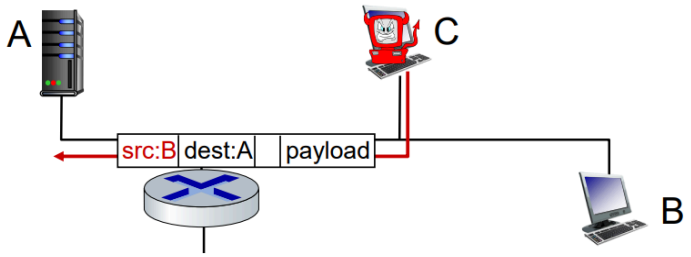


Malintenzionati:

- **Identità falsa (IP spoofing):** Iniezione di pacchetti con indirizzo sorgente falso.

Usi:

- Ostacolare l'identificazione/blocco di una sorgente di attacco (vedi DoS dopo, sebbene meno rilevante nel caso di DDoS)
- Sfruttare la relazione di fiducia tra host (es. accesso senza autenticazione da host nella medesima rete locale)
- Indirizzare messaggi di risposta verso B, montando un attacco di negazione di servizio contro B (vedi dopo), basato sull'amplificazione del traffico generato da C (vedi DNS Amplification Attack, in cui una richiesta a un DNS produce una riposta più grande indirizzata verso la vittima)



Negazione del servizio (DoS)

Definizione:

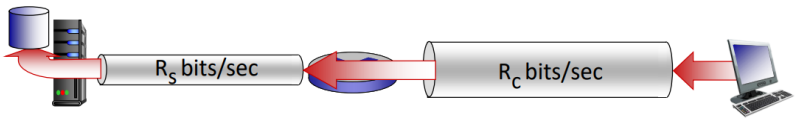
- Gli aggressori rendono una rete, un host o altro elemento infrastrutturale non disponibile per gli utenti legittimi.

Categorie di attacchi DoS:

1. **Attacchi alla vulnerabilità dei sistemi:** Invio di (pochi) pacchetti costruiti ad arte per causare il blocco di un servizio o lo spegnimento di un host, sfruttando vulnerabilità delle applicazioni o dei sistemi operativi.
2. **Bandwidth flooding (inondazione di banda):** Invio massivo di pacchetti all'host obiettivo impedendo al traffico legittimo di raggiungerlo.
3. **Connection flooding (inondazione di connessioni):** Stabilire un gran numero di connessioni TCP con l'host obiettivo, impedendogli di accettare le connessioni legittime.

Esempio di bandwidth flooding:

- Rs (velocità di accesso del server)
- Rc (velocità di accesso dell'attaccante)



Considerazioni:

- Una singola sorgente di attacco potrebbe avere una velocità di accesso insufficiente (tipicamente Rc ≪ Rs) e sarebbe comunque facile da identificare e bloccare.

Schema di attacco DoS distribuito (DDoS):

1. Selezionare l'obiettivo
2. Irrompere negli host attraverso la rete (vedi botnet)
3. Inviare pacchetti verso l'obiettivo da host compromessi

Note:

- Un botnet è una rete di computer compromessi controllati da un malware.
- Un attacco DDoS sfrutta la potenza di elaborazione di un gran numero di host compromessi per sopraffare l'obiettivo con un volume elevato di traffico.

Linee di difesa

Autenticazione

- Dimostrare di essere chi si dice di essere.
- Reti cellulari: identità hardware tramite SIM.
- Internet tradizionale: mancante di supporto hardware per l'autenticazione.

Riservatezza

- Protezione dei dati tramite cifratura.

Integrità

- Firma digitale per prevenire o rilevare manomissioni.

Restrizioni di accesso

- VPN protette da password per reti private.
- Firewall: "middlebox" per reti di accesso e di base.

Firewall

- Off-by-default: filtrare i pacchetti in entrata per limitare:
  - Mittenti
  - Destinatari
  - Applicazioni
- Rilevare e reagire agli attacchi DoS:

    - Protezione da IP spoofing (impedire l'ingresso di pacchetti da reti esterne con indirizzi falsi)
    - Impedire connessioni a determinate applicazioni
    - Altre misure

Schema: Livelli di protocollo e modelli di riferimento

Introduzione

Le reti sono complesse e composte da molteplici elementi:

- Host
- Router
- Mezzi trasmissivi
- Applicazioni
- Protocolli
- Hardware e software

Livelli o strati (Layer)

Per semplificare la gestione di sistemi complessi, le reti vengono suddivise in livelli o strati. Ogni livello:

- Implementa un servizio specifico.
- Esegue determinate azioni all'interno del livello.
- Utilizza i servizi del livello sottostante.

Vantaggi della stratificazione

- **Progettazione e discussione di sistemi complessi:**
    - La struttura a strati facilita l'identificazione dei componenti e delle loro interrelazioni.
- **Modularità:**
    - Semplifica la manutenzione e l'aggiornamento del sistema.
- **Trasparenza:**
    - Le modifiche a un livello non influenzano il resto del sistema.

Svantaggi della stratificazione

- **Duplicazione di funzionalità:**
    - Lo stesso servizio può essere implementato in più livelli (es. correzione degli errori).

- **Violazione della separazione tra livelli:**
    - Un livello potrebbe aver bisogno di informazioni disponibili solo a un livello inferiore.

Pila di protocolli di Internet

La pila di protocolli di Internet è composta da diversi livelli:

1. Applicazione (Application Layer):

- Supporta le applicazioni di rete (HTTP, IMAP, SMTP, DNS).

2. Trasporto (Transport Layer):

- Trasferisce dati tra processi (TCP, UDP).

3. Rete (Network Layer):

- Trasferisce pacchetti di rete (datagrammi) da un host all'altro (IP, protocolli di instradamento).

4. Collegamento (Link Layer):

- Trasferisce dati tra elementi di rete vicini (Ethernet, 802.11 (WiFi), PPP).

5.Fisico (Physical Layer):

- Trasmette bit "sul filo".

Servizi, Stratificazione e Incapsulamento

Ogni livello fornisce un servizio al livello superiore e utilizza i servizi del livello inferiore. L'incapsulamento avviene ad ogni livello:

- Il livello di applicazione invia un messaggio al livello di trasporto.
- Il livello di trasporto incapsula il messaggio con un header per creare un segmento.
- Il livello di rete incapsula il segmento con un header per creare un datagramma.
- Il livello di collegamento incapsula il datagramma con un header per creare un frame.
- Il livello fisico trasmette i bit del frame sul mezzo trasmissivo.

Modello di servizio e incapsulamento

Introduzione

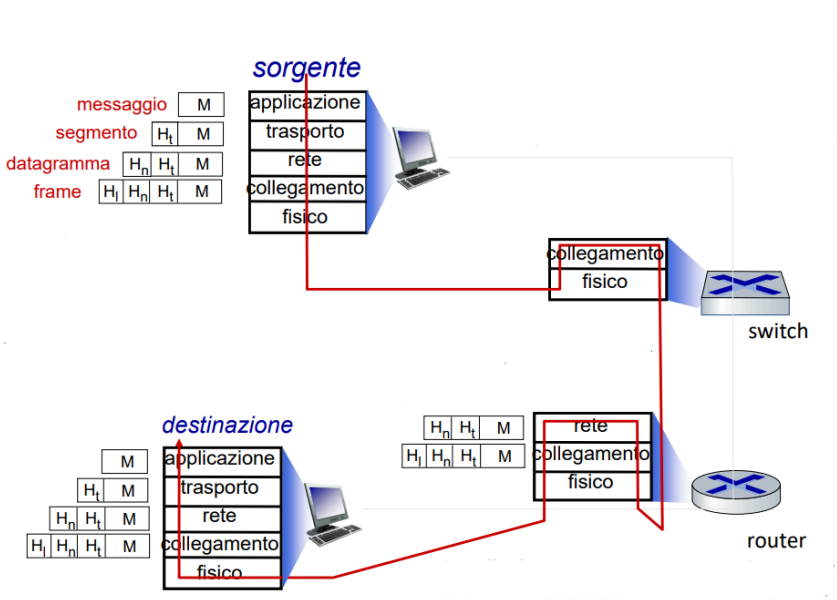
Un modello di servizio definisce l'insieme dei servizi offerti da un livello al livello superiore.

Servizi offerti dai livelli

- **Diversi protocolli possono implementare lo stesso servizio.**
- **Il livello di collegamento può offrire servizi diversi a seconda del protocollo utilizzato sul link (es. Ethernet, Wi-Fi, PPP).**
- **Un protocollo di livello di collegamento può supportare diversi protocolli di livello fisico a seconda della tecnologia di trasmissione e del mezzo trasmissivo del link.**
    - Esempio: Ethernet ha diversi protocolli di livello fisico per doppino intrecciato, fibra ottica e cavo coassiale.

Incapsulamento

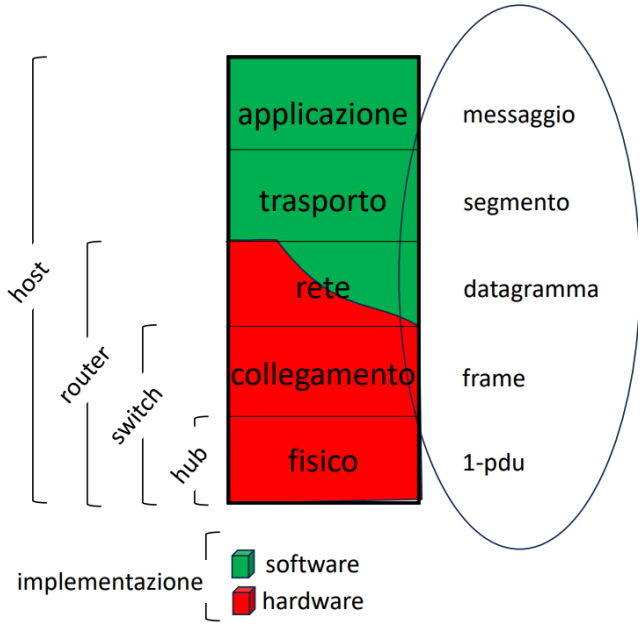
- L'incapsulamento è il processo di aggiungere un header a un'unità di dati per trasportarla su un livello inferiore.
- Un protocollo di livello n può essere distribuito tra sistemi periferici, commutatori di pacchetto e altri elementi di rete.
- **Host, router e switch implementano solo i livelli necessari alle loro funzionalità.**
- **L'intestazione di un livello (Hn) può cambiare durante l'inoltro (es. decremento del Time to Live).**
- **Il livello di rete può ricevere un servizio diverso a seconda del protocollo di livello di collegamento, man mano che un datagramma attraversa collegamenti di tipo diverso.**



PDU (Protocol Data Unit)

- Una n-PDU è la singola unità di informazione scambiata tra pari attraverso un protocollo di livello n.
- La n-PDU contiene:
    - **Informazioni di controllo specifiche per il protocollo.**

- **Un carico utile (payload): in genere una (n+1)-PDU.**



Schema: Modello di riferimento ISO/OSI

Introduzione

Il modello di riferimento ISO/OSI è un modello concettuale che descrive la struttura logica di una rete di comunicazione. È suddiviso in sette livelli, ognuno dei quali fornisce un servizio specifico (POSSIEDE 2 LIVELLI IN Più):

1. Applicazione (Application Layer): Supporta le applicazioni di rete (HTTP, FTP, SMTP, DNS).

2. Presentazione (Presentation Layer): Interpreta il significato dei dati (crittografia, compressione, rappresentazione).

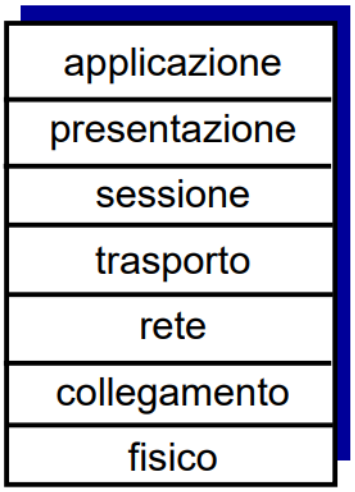
3. Sessione (Session Layer): Gestisce lo scambio di dati tra applicazioni (sincronizzazione, checkpointing).

4. Trasporto (Transport Layer): Fornisce un trasferimento di dati affidabile (TCP, UDP).

5. Rete (Network Layer): Inoltra pacchetti di dati da un host all'altro (IP, routing).

6. Collegamento (Link Layer): Trasmette dati su un singolo collegamento (Ethernet, Wi-Fi).

7. Fisico (Physical Layer): Trasmette bit sulla rete fisica (cablaggio, onde radio).



Schema: Storia di Internet

Nascita e Sviluppo (1960-1980)

1960:

- Kleinrock dimostra l'efficacia della commutazione di pacchetto.
- Baran studia la commutazione di pacchetto per reti militari.

1967:

- Nasce il progetto ARPANet.

1969:

- Primo nodo operativo ARPANet.

1972:

- Dimostrazione pubblica di ARPANet.
- NCP (primo protocollo host-to-host).
- Primo programma di posta elettronica.
- ARPANet ha 15 nodi.

1972-1980:

- Sviluppo di Internetworking e reti proprietarie.
- Rete satellitare ALOHAnet (1970).
- Architettura per l'interconnessione delle reti (Cerf e Kahn, 1974).
- Ethernet (Xerox PARC, 1976).
- Architetture proprietarie (DECnet, SNA, XNA, fine anni '70).
- ARPANet ha 200 nodi (1979).

Principi di Internetworking (***Cerf e Kahn***):

- Minimalismo e autonomia.
- Modello di servizio "best effort".
- Router stateless.
- Controllo decentralizzato.

Nuovi protocolli e proliferazione (1980-1990)

1983:

- Rilascio di TCP/IP.

1982:

- Definizione del protocollo SMTP per la posta elettronica.

1983:

- Definizione del DNS per la traduzione degli indirizzi IP.

1985:

- Definizione del protocollo FTP.

1988:

- Controllo della congestione TCP.

Nuove reti nazionali:

- CSnet
- BITnet
- NSFnet
- Minitel

100.000 host collegati alla confederazione delle reti.

Commercializzazione, Web e nuove applicazioni (1990-2000)

Primi anni '90:

- Dismissione di ARPANet.
- Decadenza delle restrizioni sull'uso commerciale di NSFnet (1991).

Primi anni '90:

- Nasce il Web:
    - Ipertestualità (Bush 1945, Nelson 1960s).
    - HTML, HTTP (Berners-Lee).
    - Mosaic (1994), poi Netscape.

Fine anni '90:

- Commercializzazione del web.

Fine anni '90 - inizi 2000:

- "Killer application": messaggistica istantanea, condivisione di file P2P.
- Sicurezza di rete in primo piano.
- 50 milioni di host, 100 milioni+ di utenti.
- Velocità nelle dorsali dell'ordine di Gbps.

Scala, SDN, mobilità e cloud (2005-presente)

2005-presente:

- Diffusione aggressiva dell'accesso domestico a banda larga (10-100 Mbps).
- Software-defined networking (SDN, 2008).
- Crescente ubiquità dell'accesso wireless ad alta velocità (4G/5G, WiFi).
- Fornitori di servizi (Google, FB, Microsoft) creano le proprie reti:
    - Scavalcano l'Internet commerciale per connettersi "vicino" all'utente finale.
    - Forniscono accesso "istantaneo" a social media, ricerca, contenuti video.
- Le imprese gestiscono i loro servizi in "cloud" (es., Amazon Web Services, Microsoft Azure).
- Ascesa degli smartphone: più dispositivi mobili che fissi su Internet (2017).
- ~15 miliardi di dispositivi connessi a Internet (2023, statista.com).

Eventi chiave

- **1960:** Teoria delle code e commutazione di pacchetto.
- **1967:** Progetto ARPANet.
- **1972:** Dimostrazione pubblica di ARPANet e NCP.
- **1974:** Architettura per l'interconnessione delle reti (Cerf e Kahn).
- **1983:** Rilascio di TCP/IP e DNS.
- **Primi anni '90:** Nascita del