



Argomento



Definizione



Importante

Slide reti Rossante,

O- INTRO

Le reti di calcolatori:

- Una RDC è un insieme di modi di elaborazione → in grado di scambiare messaggi fra loro
- Le comunicazioni avvengono attraverso i canali:
 - Messaggi
 - Mittente
 - Destinatario
 - Mezzo di trasmissione
 - Protocollo
- Esistono diversi modelli di applicazioni
 - | client-server (accesso remoto e risorse fisiche)
 - | peer to peer (servizi collaborativi, VoIP)
 - | multi-tier e architetture middleware (app distribuita a più host che collaborano in rete)
- Metriche per la valutazione del c.d.c (canale di comunicazione)

- Ampiezza di banda (capacità teorica bit/sec)	- throughput (capacità reale bit/sec)	- Ritardo (latenza)	- Jitter (var. ritardo)
- Affidabilità	- Sicurezza		

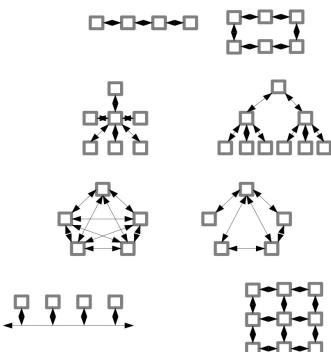
• Strutture fisica delle reti: insieme di nodi interconnessi

due nodi comunicano tramite connessione fisica se è presente un canale fisico (link) ↓
 ↓ termini | connessione logica se è una catena di canali fisici
 possono essere ↗ entrambi | di transito ↗ compone un canale virtuale

Topologie delle reti:

Principali topologie:

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



Definizioni:

- Links → canale
- Path → catena di link
- Hops → numero di link da attraversare
- Path per link → arco
- Diametro → hops fra 2 nodi estremi
- Scalabilità → sostenere > link

• Classificazione delle comunicazioni sui canali:

- | | |
|-----------|---|
| Direzione | Simplex (monodirezionali) |
| | half-duplex (bidir. non contemporaneamente) |
| | full-duplex (bidir contemporaneamente) |

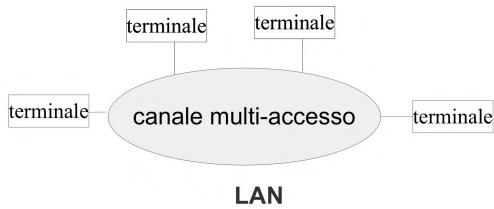
MODelli

- | | |
|--------------|-------------------------------|
| Destinazione | unicast |
| | broadcast |
| | multicast (sottoinsieme rete) |

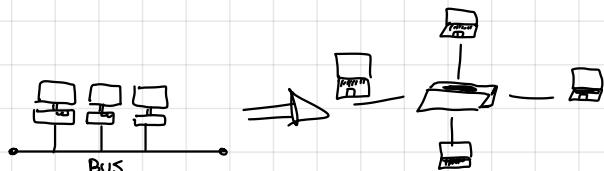
- I mezzi trasmissivi possono essere
 - punto-punto → 2 nodi
 - multi accesso → n nodi (bus)

• Local Area Network (LAN)

Rete particolare che include tutti i nodi che condividono lo stesso canale multi accesso



Le LAN supportano tutti i modelli di destinazione



LAN : le topologie diverse a stelle grazie a HUB e switch / anche ad albero

- Reti locali: Ethernet → infrastruttura multiaccesso utilizzando mezzi trasmissivi punto-punto

- Reti geografiche: WAN → reti che si estendono su grandi distanze geografiche, usano dei semplici link punto-punto.

(es. case ADSL centrali, 2 sedi remote di un'azienda)

- Intercanversione di reti: INTERNET → A livello di infrastruttura è una unione fra LAN e WAN interconnesse fra loro.

- Connessione di circuito e pacchetto: Connessione → percorso su cui far transitare i messaggi su cui canale virtuale. Ne esistono due tipi:

- Connessione di circuito (es reti telefoniche)

- percorso fra due terminali, circuito fisico temporaneo
- ritardo iniziale
- scambio dati come collegamento diretto
- canale chiuso al termine

- Connessione di pacchetto (es reti dati)

- dati frattornati in pacchetti, max dim K.
- nodi di transito introducono i pacchetti
- destinatario riassumba i pacchetti

- Strati ISO/OSI → sono 7, ogni strato serve il superiore, nascondendone l'implementazione.

- Strati TCP/IP → sono rimasti standard anche se si poteva sì avere l'OSI.

• Strati ISO/OSI

- Strato 1: Fisico - trasmissione di bit "grazzi". Gestire la connessione strato 2.
- Strato 2: Link - Attivare e disattivare la connessione fisica su linea per Strato 3. Collegamento affidabile.
- Strato 3: Network - Far giungere i pacchetti al destinatario determinando il percorso.
- Strato 4: Trasporto - fornire canale sicuro end-to-end.
- Strato 5: Sessione - Suddivide il dialogo fra le applicazioni in unità logiche.
- Strato 6: Presentazione - Adatta il formato dei dati preservandone il significato.
- Strato 7: Applicazione - L'utente.

• TCP/IP

Strati 1 e 2: fisico e collegamento. Sono strati strettamente legati all'hardware di rete.
Ci sono 2 protocolli: WAN HDLC PPP
LAN ethernet

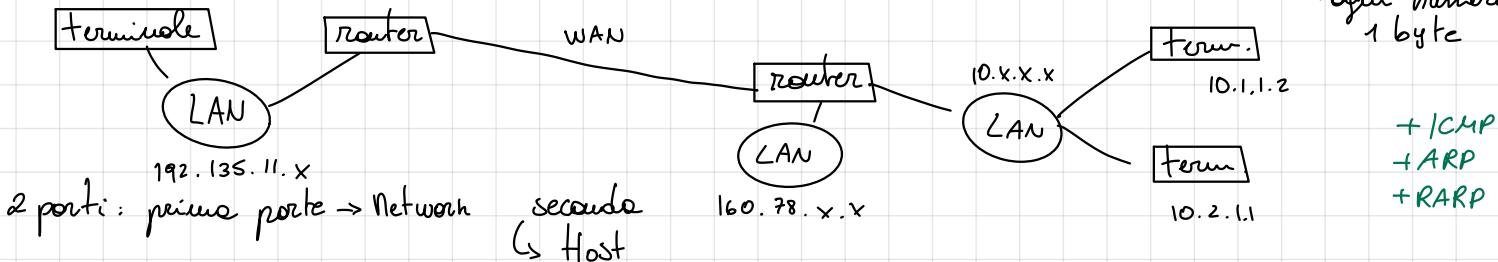
I protocolli dello strato fisico assegnano ad ogni interfaccia un indirizzo fisico

PACCHETTO
HEADER | PAYLOAD | FRAME

tra 0 e 255

Strato 3: Rete - implementa il protocollo IP + indirizzi logici IPv4. 32 bit (4 byte)

192.168.1.2



Strato 4 - Trasporto

Connessione fra due nodi:

- pacchettizzazione

- Multiplexing / demultiplexing (per le porte)

UDP - connection-less

↳ le coppie IPaddr + port → Socket

univoco

TCP - connection oriented

- API: Attraverso la Berkeley Socket Lib. lo strato di trasporto TCP/IP fornisce le API per implementare un modello di comunicazione Client/Server → connection oriented

↳ connection less

Strato 5 - Applicativo

Usa le porte TCP/UDP di cui ci sono le storiche: 23/TCP telnet 25/TCP SMTP 80/TCP HTTP

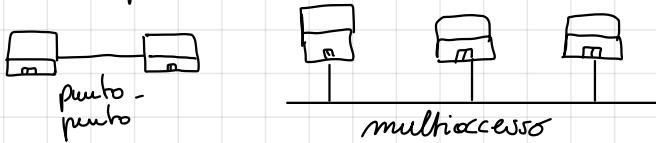
Ogni applicativo assegna ai propri oggetti un indirizzo specifico mnemonico tipo: www.unipi.it o offici@unipi.it

Le porte TCP/UDP vengono assegnate dalla IANA e sono well-known-ports

1A - Livello Fisico:

• Scopo del livello fisico:

Si occupa del trasferimento dei bit fra i nodi sullo stesso canale fisico



trasferimento → su un mezzo trasmissivo, su cui i bit vengono codificati, vengono trasformati in energia (luce, onde etc)

modi → hanno un adattatore per codifica e decodifica

• Mezzi trasmissivi

1. **Elettrico** → doppini telefonici (P-P)
2. **Ottici** → fibre ottiche (P-P)
3. **Wireless** → onde radio, satelliti

La scelta del mezzo dipende da caratteristiche del canale:

- latenza
- costo
- disturbo

• Banda passante:

Codifica → intervallo frequenze in Hz, contenute in una banda di larghezza H.
Attenuazione → dipende dalle frequenze

Banda di frequenze → da identificare → **banda passante**: determinata da caratteristiche fisiche del mezzo. Può essere limitata.

• Attenuazione: diminuzione del segnale sulla lunghezza del mezzo determina la **distanza max. raggiungibile**

davanti a: **perdite di energia**

Si misura in (db) → $10 \log_{10} P_2/P_1$ con P_1 trasmittente e P_2 ricevente

es: dimezzo: $10 \log_{10} 0.5 = -3 \text{ db}$ } come P_1/P_2 normale
raddoppio: $10 \log_{10} 2 = 3 \text{ db}$

• Se la banda di f non ha valori costanti → possono verificarsi **distorzioni**



• Rumore e disturbo:

Al segnale S si sovrappone rumore termico N (sempre presente)
Il rapporto segnale rumore $\rightarrow 10 \log_{10} S/N$

Disturbo: proveniente da rumori esterni / crosstalk - canali adiacenti

• Velocità massima di un canale:

La banda passante incide sulla v. max. / ampiezza banda digitale B in bit/sec.

de rel. fre b.p. analogico H e la b.p. digitale B su canale ideale è definita da Nyquist $B = 2H \log_2 V$ b/s \rightarrow numero dei simboli del segnale

In presenza di rumore: Shannon $B = H \log_2 (1 + S/N)$

Moo: Shannon determina B

Nyquist determina $V = 2^H$ (bitrate / 2H)

• Tempi delle comunicazione:

- tempo di consegna: tempo dato da mittente a destinatario

- Round trip time (RTT): tempo fra invio dato e ricezione di mess. di riscontro (ACK)

↳ incidono su questi: - tempo di trasmissione \rightarrow tempo che impiega una sequenza di bit a uscire dall'interfaccia di rete. $L > T_{Tr} = n \cdot \text{bit} / v_r \cdot \text{trasmissione}$

- tempo di propagazione \rightarrow tempo che impiega un bit a percorrere il mezzo.

$t_{pr} = l / v$ lunghezza mezzo / vel. propagaz. mezzo

$V = C/N$ C vel. luce $3 \cdot 10^8$ m/s v_r^2 indice rifrazione mezzo

fibre / rame $v_r = 2 \cdot 10^8$ m/s

aria $v_r = 3 \cdot 10^8$ m/s

• tempo preparazione mittente \rightarrow codifica e compressione

\rightarrow tempo riempimento del pacchetto \rightarrow flusso continuo dati (real time) riempimento pacchetto

• tempo attraversamento nodi di transito

\rightarrow tempo elaborazione \rightarrow processamento software/hardware

\rightarrow tempo attesa \rightarrow se ci sono code di trasmissione

• tempo elaborazione destinatario \rightarrow decodifica decompressione

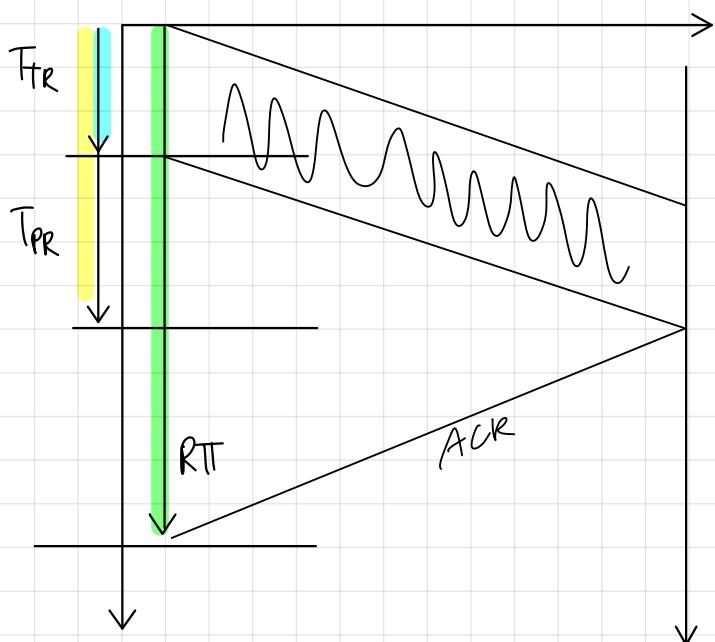
Diagramma spazio tempo: rappresentazione grafica dei tempi coinvolti nella spedizione dei pacchetti:

tempo trasmissione $T_{TR} = 800b / 1Gb/s = 0.8\mu s$

tempo propagazione $T_{PR} = 100 / 2 \cdot 10^8 s = 50 \cdot 10^{-8} s = 0.5\mu s$

tempo causale $T_c = T_{TR} + T_{PR} = 0.8 + 0.5\mu s = 1.3\mu s$

Round trip time $RTT = T_c \times 2 = 1.8\mu s$



- **Cavo coassiale**: 2 canali come concentrica; multi-accesso bidirezionale / reti locali / TV via cavo nel quale attenuazione $\rightarrow f.$ (Hz) e ℓ (m)
- **Doppino di rame**: coppia di fili di rame non schermati.
16 MHz telefonica digitale
- **Fibra ottica**: fibra di vetro che trasporta impulsi di luce.
componenti:
 - \nearrow sorgente luminosa
 - \swarrow mezzo trasmissione
 - \searrow rilevatore
- > Sicurezza
 > ottimo rapporto segnale / rumore
 > immune ai disturbi

modulazione \rightarrow OOK or /off keying
 \rightarrow SCM sub carrier mod (AF, AM)

○ Trasmissione ottica:

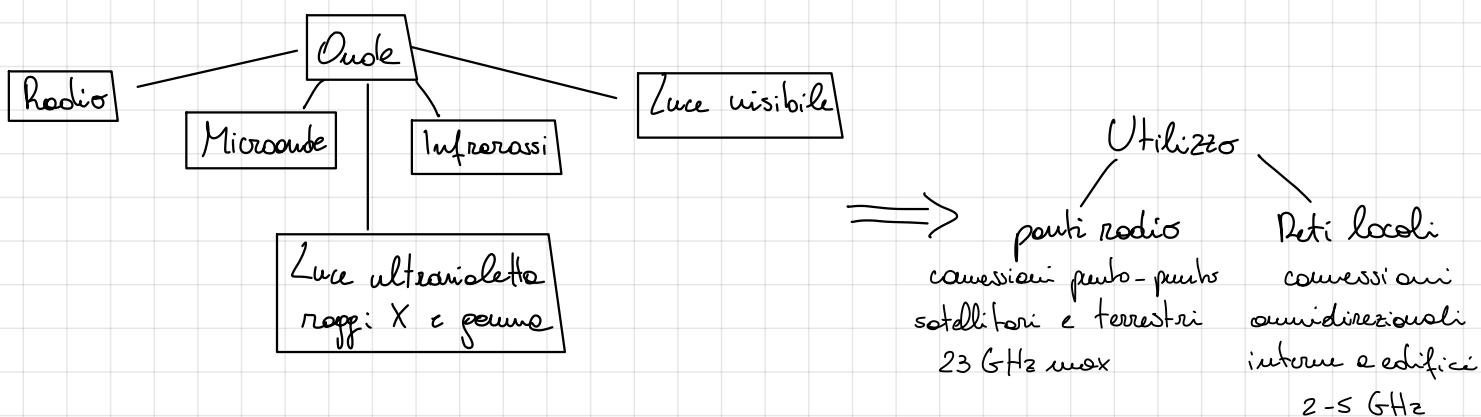
Su bande I II III tra 250 THz e 300 THz

Si hanno poi fibre \rightarrow monomoduli
 \rightarrow multimoduli

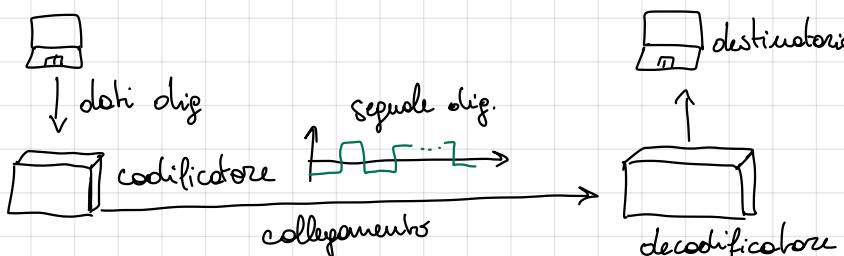
○ Onde elettromagnetiche:

Trasmettere informazioni senza l'utilizzo di un mezzo fisico guidato.

Si modulano le frequenze portanti tipo AM e FM



○ Modulazione digitale: conversione dati digitali in segnali digitali che possono essere voltaggi, intensità di luce o segnali e.m.



• Codifiche dei bit:

- trasmissione in

→ prevalentemente LAN

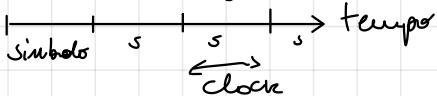
banda loose → segnale modulato, freq. inalterata

banda passante → modulazione freq. portante

• Trasmissione dei dati:

comunicazione generalmente seriale → 1 canale usato

I simboli vengono codificati ad intervalli di clock - sincronismo tra trasmettitore e ricevitore



Modalità

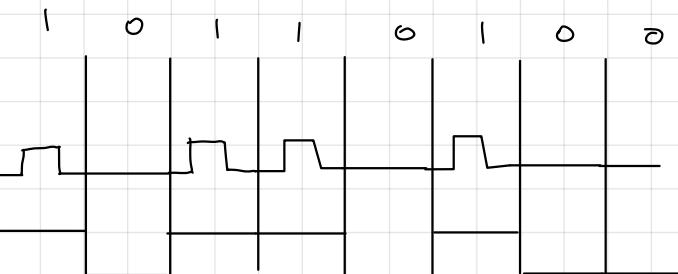
- **Sincrono**: no bit sincronismo: clock inviato parallelamente al canale dei dati
flusso mai interrotto
- **Asincrono**: possibile assenza segnale fra un gruppo di bit e l'altro
ogni gruppo è preceduto da una seq. di bit aggiuntivi
↳ ricostruisce il sincronismo.
+ comune in reti di calcolatori

• Codifica di linea

Seq. binaria

RZ → + soggetto a errori

NRZ → richiede circuiti complicati



• NRZ-I e Manchester

cambia simbolo codifica
al bit 1 o rimane invariato
M: codifica i bit con le
transizioni

• Codifica a blocchi

4B5B masta per
FastEthernet

• Codifica di linea multilivello

2B1Q: 4 liv. ten. - cod. 2 bit
8B6T: seq. 8 bit mod su 6 liv. ten
PAM5: 5 liv. tensione

• Modulazione di una frequenza portante:



modulazione d'ampiezza: fibre ott.

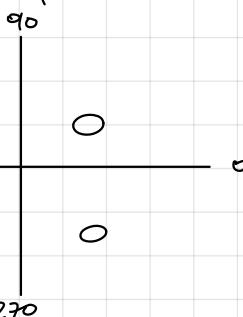
modulazione frequenza

modulazione fase

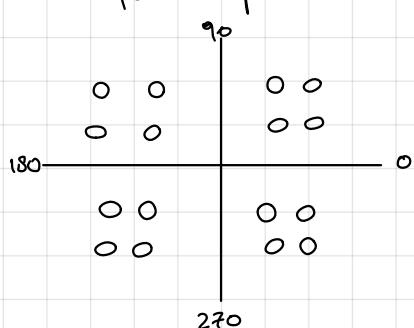
- Modulazione e costellazione: modulazione ampiezza + fase \rightarrow QAM (bestest)

Simboli \rightarrow determinato da una coppia fase-ampiezza \rightarrow rappresentato da un punto nel diagramma delle fasi. L'insieme è la "costellazione".

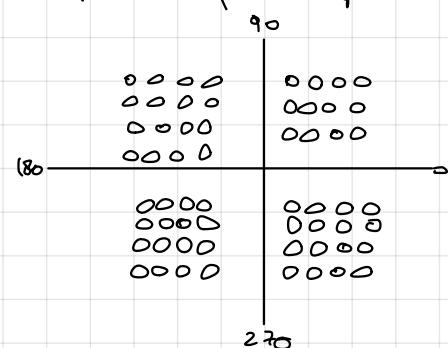
a) QPSK mod fase 4 sloti



b) QAM16 fase+amp 16 sloti

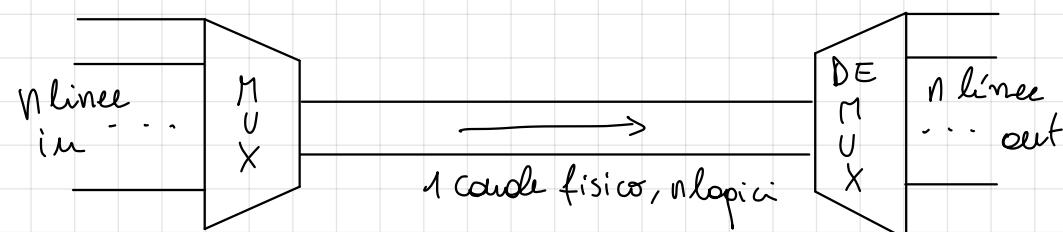


c) QAM64 fase+amp 64 sloti



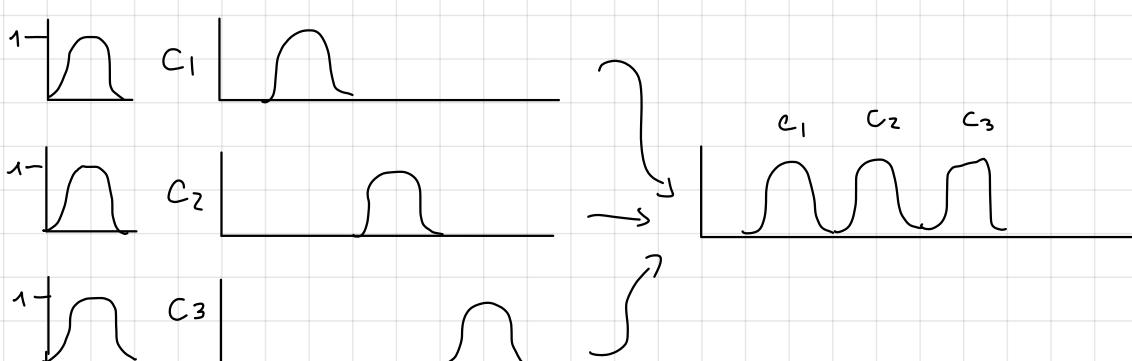
- Multiplexing: tecnica che permette trasmissione simultanea di + segnali in 1 canale.

2 tecniche \rightarrow FDM divisione di frequenze / analogico
TDM divisione di tempo / digitale



- Frequency Division Multiplexing: divide lo spettro in bande di sequenza.

Ogni canale viene codificato modulando le frequenze all'interno di una banda.



- Diffusione dello spettro: spettro frequenze suddiviso in più portanti per evitare interferenze e intercettazioni.

- FDSS (freq. hopping spread spectrum)

- CDMA (code division multiple access)

- OFDM - tecnica FDM con frequenze ortogonalmente fra loro

1B: Telefonia:

- Il sistema telefonico: **PSTN** - rete specializzata per la trasmissione di uno specifico tipo di dato: la voce analogica.

Orecchio umano: 20 Hz - 20 kHz

- Voce: 4 kHz → 300 - 3400 Hz
- Sistema telefonico → canali con ampiezza 4 kHz, **Collegamento casa - centralina**
- Telecom si divide "ultimo miglio", "local loop" ed è un doppino di cat. 3.
- **Codec** → lo trasforma in analogico → ricevente e destinazione
 ↑
 riceve il segnale
 in digitale
 ↓
 ricevente
- Si usano **multiplexing** di più canali con tecniche **FDM** o **TDM**.

- PCM: pulse code modulation - le comunicazioni sono sempre più digitali.
 conversione in digitale con campionamento PCM.

Canale analogico (4 kHz) campionamento su flusso 64 kbit/sec
 ↑ → 8 bit di dati →
 8000 camp/sec

- Il **pam** è il cuore del sistema telefonico moderno, può usare NRTZ o RTZ.

Portanti TDM per canali TDM:

Tecniche multiplexing su portanti di tipo T:

- | | | | |
|----------------|-------------------------|----------------------|---|
| T ₁ | 24 canali pam | 64 kbit/s → 1.5 Mb/s | } |
| T ₂ | 4 canali T ₁ | → 6.3 Mb/s | |
| T ₃ | 7 canali T ₂ | → 44 Mb/s | |
| T ₄ | 6 canali T ₃ | → 270 Mb/s | |

- Altre variazioni → tipo E
 gerarchia a 32
 E₁ 2.04 Mb/s
 E₂ 128 canali
 E₃ 512 canali
 E₄ 2048 canali
 E₅ 8192 canali

Modem, ISDN e XDSL:

- a 56 kbit/s si usavano i modem su canali da 4 kHz per le conversazioni telefoniche.
- una **rete TDM** gestisce canali digitali da 64 kbit/s che portano la voce tramite ISDN in casa
- per maggiore ampiezza canale → **XDSL** → segnale non a 4 kHz ma a 1.1 MHz
- banda 1.1 MHz tramite OFDM → 256 canali da 4.3 kHz
 ↳ modulazione QAM } r. max ~ 15 mb/s

• ADSL: Asymmetric DSL - XDSL pensato per l'home computing.

- Canali 0 (0-4.3 kHz) fonia
- Canali 1-5 (4.3-25 kHz)
- Canali 6-30 (24) per upload
- Canali 31-255 (244) per download

ADSL 2 > prestazioni tramite diverse codifiche ~ 2mb/s

+ ADSL 2+ bande doppie ~ 26 Mb/s

FttH → fiber to home 1Gb/s

Fttc → fiber to Cabinet 200 mb/s

• Sistema telefonico mobile:

1G: standard olandesi TACS (EU) e AMPS (USA)

2G: D-AMPS e GSM. Voce digitale

2.5G: GPRS e EGPRS (EDGE). trasmissione digitale e commutazione di pacchetto

3G: Standard UMTS, CDMA e HSDPA. Voce e dati digitali

4G: Standard LTE

5G: (2020)

1G: Celle → AMPS

area geografica 10-20 km di diametro. Celle → nuclei di 7 con freq. diverse.

2 celle con = freq. diverse 2 celle che le separano. 1 cella → 1/7 di 832 canali

2G: AMPS + D-AMPS + nuove frequenze, stessi canali

GSM → D-AMPS + FDM + TDM → resto del mondo

2.5: Sottastruttura del 2G → raggruppo pacchetti: IP + slot

EDGE → nuova modulazione

3G: Usa l'infrastruttura GSM ma tecnologia W-CDMA

4G: LTE nuova generazione - modulazione OFDM - min 1.25 MHz e max 20 MHz per user

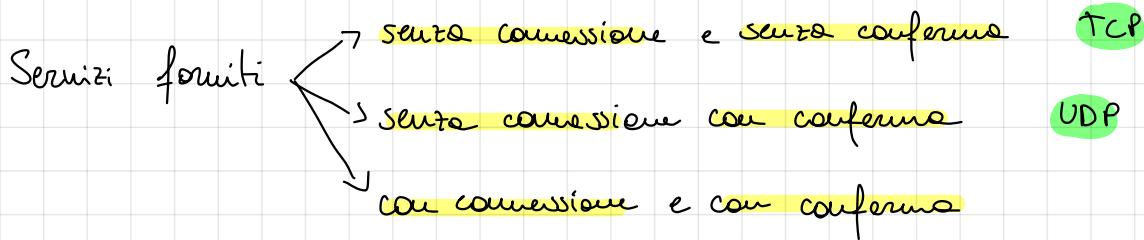
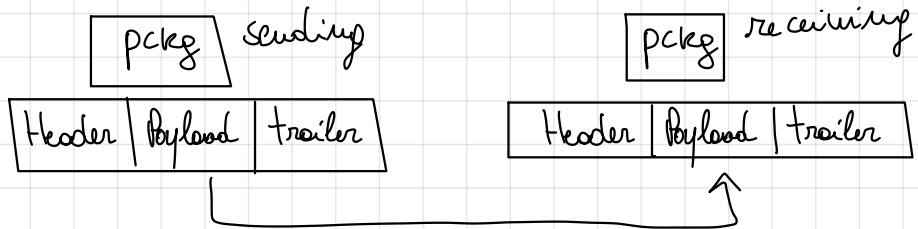
5G:	3 bande	· 700 MHz	3 servizi	· mMTC	elevato numero dispositivi in area geografica
		· 3.7 GHz		· URLLC	requisiti stringenti
		· 26 GHz		· eMBB	fornire accessi broadband su mobile.

2A - Link:

- Sopra livello data-link → trasferire in modo affidabile i dati tra nodi adiacenti.

Affidabilità → suddivisione del flusso di dati in **frame** con **lunghezza max fissata**.

→ meccanismo per rilevare errori e correggerli



- Impacchettamento: (framing) problems → delimitatore **inizio** e **fine** del frame può avere lunghezza variabile ↑

Intervallo temporale fra frames → non sufficiente
 ↳ precedere il frame con il numero di byte del frame
 ↳ delimitare il frame con caratteri speciali (**flop**)

↳ per byte oriented si mette un byte escluтивно del flop
 ↳ ricevente deve fare "destuffing"

(011110)

- Bit stuffing: se sono bit-oriented → open frame inizia con un **flop** → ogni 5 bit viene aggiunto un bit 0 (stuffing) per non confondere il destinatario.

Rilevazione e correzione errori:

Possono verificarsi **disturbi** o **rumore termico** ↳ a bit singolo
 ↓ ↳ a rotta (burst)
 per evitare si usa la **ridondanza** → breve codice (**FCS**) inserito assieme al frame.

Se il destinatario ottiene un FCS diverso c'è stato un errore.

2 strategie ↗ rilevazione errori: frame ritrasmesso
↗ rilevazione e correzione errori: usato in reti poco affidabili

o Codifica a blocchi: algoritmo per rilevare errori (semplice) Bit di parità
→ il numero totale di "1" nella sequenza deve essere pari (o dispari)
bit parità 2D → sottosequenza → inutile

o Cyclic redundancy check (CRC):

frame di n bit visto come lista di coeff. di un polinomio D con d termini.
trasmettitore e ricevitore d'accordo su pol. G di $r+1$ bit → generatore (n. primi)
trasmettitore aggiunge r bit (CRC) e il nuovo frame deve essere divisibile per G .
Ricevitore $\rightarrow M/G \rightarrow$ se resto diverso da 0 → errore

→ facilmente implementabile in hardware di basso costo
Ethernet → CRC 32
HDLC → CRC 16
ATM → CRC 8

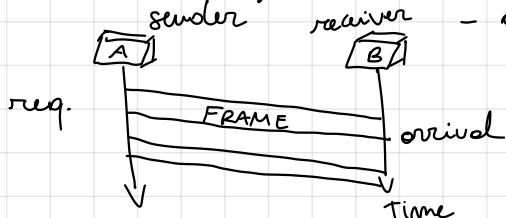
o Checksum / somme di controllo: Si sommano in complemento 1 su 16 tutti i dati del messaggio. Il checksum (16 bit) è il complemento del risultato.

Utile per implementazioni software → usato nei protocolli internet (IP, ICMP, TCP, UDP)

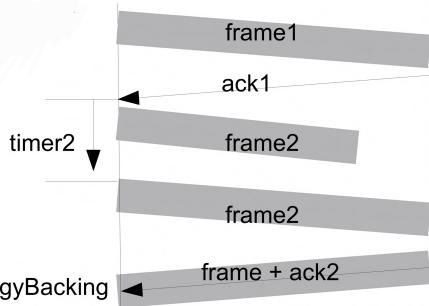
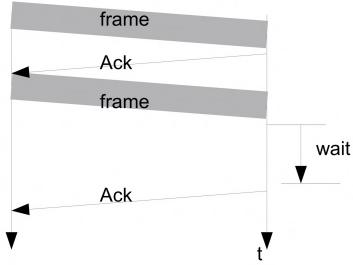
o Trasmissione affidabile: invece di protocolli per:
per canali senza rumore:
- semplice
- stop and wait

per canali con rumore:
- stop and wait ARQ
- protocolli a finestre scorrevole ↗ Go-back-n ARQ
↗ ripetizione selettiva ARQ

o Protocollo simplex:
- destinatario pronto a ricevere e gestire frame
- dati arrivano senza errore



- Stop-and-wait:
 - ricevendo bisogno di tempo per elaborare i dati ricevuti
 - come il simplex ma Ack prima del frame successivo



• Stop-and-wait ARQ

- frame danneggiati → scartati / NACK
- timer dopo frame → se ACK non ricevuto, rimanda il frame
- numerazione di frame e ACK
- Se connessione bidirezionale → ACK può viaggiare in un frame inviato in Piggybacking ← verso opposto

• Protocolli sliding windows:

Migliorano l'efficienza del canale → inviare SWS frame senza aspettare l'ACK. Le finestre avanzano man mano che arrivano gli ACK.

Ogni frame ha n. di sequenza: LFS lost frame sent
LAR lost ack received
regole = $LFS - LAR \leq SWS$

- Go-back-N ARQ: è un upgrade dello sliding windows → frame risulta errato quando diversi frame sono già stati inviati.
Se arrivano frame fuori ordine vengono scartati.
" " corretti vengono mantenuti nel buffer

Quando scade il timer del frame errato il mittente torna indietro e lo rispedisce

• Ripetizione selettiva:

I frame ricevuti correttamente, successivi a quello errato, vengono bufferati mentre quelli errati vengono rispediti previo sollecito tramite NACK

- Protocollo data-link: PPP → evoluzione HDLC in ADSL

PPP in ADSL:

Serve per comunicazioni punto-punto / multi-punto.
È un protocollo byte oriented e gestisce protocolli auxiliari.

↓
LAN WAN LAN
cable — ATM — provider
|
internet

Il frame PPP aggiunge 6 (08) byte di header al payload

o Reti e circuito virtuale: ATM

- Comutazione di pacchetto o circuito virtuale
- qualità del servizio
- pacchetti (celle) di lunghezza fissa 56 byte

- si usa solo in reti WAN
e in reti telefoniche

o Reti date-link: Local Area Network:

(broadcast)

Cavale multi-excesso → cavale condiviso per l'accesso diretto tra più terminali.
Si realizza un sotto-strato MAC per disciplinare l'accesso al cavale.

Un cavale broadcast può essere assegnato in modo statico o dinamico

- o Statico → FDM o TDM suddividendo in sotto-cavale
- o nelle LAN è dinamico

o Assegnazione dinamica del cavale: Accesso multiplo:

Singolo cavale condiviso fra N stazioni → utilizzato solo da chi deve spedire frame
tempo di trasmissione → continuo: può iniziare in qualsiasi istante
→ slotted: slinso in intervalli

Collisioni: accesso e cattura
↳ frame collide con un altro

Protocolli ed accesso multiplo (MA)

- ALOHA e Slotted ALOHA — MA puro
- CSMA
- CSMA/CD Eth su rame / fibra
- CSMA/CA Eth wireless

o ALOHA: 1^a implementazione di MA

Ogni terminale invia i frame senza accordo con gli altri (MA).
L'assenza di conferma viene letta come collisione con altri trasmittori, il frame viene quindi rispedito dopo un intervallo casuale → (tempo di backoff)

o Algoritmo backoff:

In caso di collisione fra terminali, l'algoritmo determina un tempo di attesa random prima di riprovare l'invio.
Vol max $10 \times \text{eth}$

In eth → esponenziale binario: dopo n collisioni consecutive ottende tra 0 e 2^{n-1} slot

2B - Ethernet:

o Standard IEEE 802:

Sono architetture per reti locali, personali e metropolitane standardizzate

IEEE 802 separa le funz. del liv. data-link in 2 sottolivelli: LLC e MAC

- MAC (medium access control) → gestisce l'accesso al mezzo mediante diversi protocolli sul accesso multiplo: Eth, LAN wireless, bluetooth ecc.

- LLC (logical link control) applica una intestazione contenente codifica del protocollo che ha generato il frame, n. seq. e ACK. Opera in 3 modalità:



o Medie Access Control: Ethernet:

- tecnologie predominante per le LAN.

Eth / IEEE 802.3 → max v 10Mb/s (802.0) → servizio di inizio frame serve {connessione riscontro}

→ servizio inaffidabile

- Il protocollo: CSMA/CD 1-persistent con algoritmo di backoff esponenziale binario.

Se canale libero → trasmette frame

 ↳ ascolta mentre trasmette

 ↓ se rileva disturbi in trasmissione ripete

Se canale occupato → riprova

o Codifiche manchester:

Opera in banda base del livello fisico oppure occupa una banda doppia rispetto alla codifica binaria.

o Formato del frame:

- Campo **preamble** 7/8 sequenze 10101010 (sono quadri soms) → sincronia ricevitore

- **SOF** (start of frame) indica inizio frame → contiene la 10101011 → gli ultimi 1 indicano che il prossimo bit sono l'inizio del frame.

- **type lenght** → contiene il codice del protocollo di livello superiore che ha generato il frame.

- **DATA** → contiene le PDU dei livelli superiori

- **FCS** → contiene il **CRC 32**

- marcatore fine frame → frame Gap IFG

o Indirizzi ethernet:

- Sono 6 byte (2^{48} possibili indirizzi) es: 08:00:20:70:0F
- viene scelto nel firmware del controller di rete \rightarrow primi 3 byte = vendor
- **Unicast** \rightarrow primo byte pari ($LSB=0$)
- **Multicast** \rightarrow primo byte dispari ($LSB=1$)
- **d'indirizzo broadcast** c'è FF:FF:FF:FF:FF:FF

Adattatore eth accette pacchetti nei casi:

- tutti i frame broadcast
- i frame unicast indirizzati all'interfaccia
- frame di un particolare multicast se interfaccie configurate opportunamente
- tutti frame se interfaccie configurate in modo promiscuous

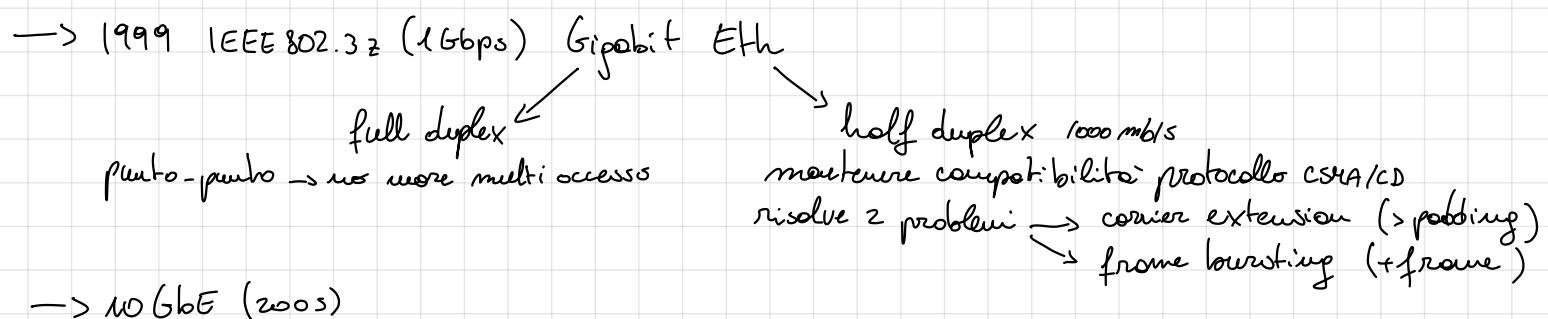
o Dimensione del frame e slot time:

Max dim. dati trasportabili da dato link \rightarrow MTU \rightarrow Eth 1500 byte

Min dim. di un frame \rightarrow 64 byte (46 payload + 18 header) = 512 bit

Durata minima frame $t = 51.2 \mu s \rightarrow$ Slot time

Evoluzione standard \rightarrow 1980 Ethernet \rightarrow 1983 IEEE 802.3 \rightarrow 1995 IEEE 802.3u (fast eth)



o Ethernet repeater:

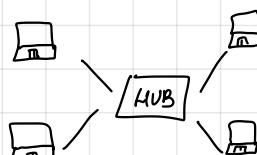
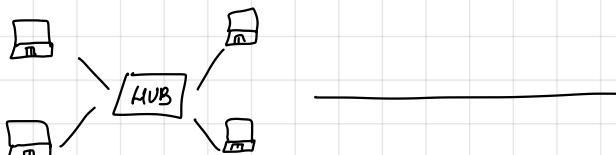
Il **repeater** è un modo di transito che **episce a livello fisico** connettendo 2 o più segmenti ethernet.



o Ethernet hub:

E' un **repeater** più di 2 interface Ethernet.

Consente di realizzare una rete broadcast usando canali punto-punto. Estende sia il dominio di collisione che il dominio broadcast.



o Commutazione nel livello date-link: Bridge

- **Filtering**: ritrasmette solamente i frame che devono transitare da una LAN a un'altra e i broadcast.
- **Individuamento (forwarding)**: avviene in base a una tabella bridge in cui sono indicati gli indirizzi MAC dietro a ogni interfaccia.
- o Bridge: **auto apprendimento**: costruita automaticamente in modo autonomo
 - accrescere con tabella vuota → arriva un frame e l'indirizzo sottile viene aggiunto
 - se non c'è l'indirizzo di destinazione il frame viene inviato a tutti (flooding).
 - il bridge cancella un indirizzo se non riceve frame per molto tempo.

o Bridge remoti:

- usati per collegare 2 o più lan distinte
- se LAN remote i bridge vengono collegati mediante linee punto-punto su cui possono utilizzare protocolli punto-punto e incapsulare al suo interno il frame MAC o linee punto-punto con protocollo MAC.
- bridge non cambia gli indirizzi fisici del frame
- ogni LAN ha un proprio formato del frame

o Ethernet commutate: gli switch

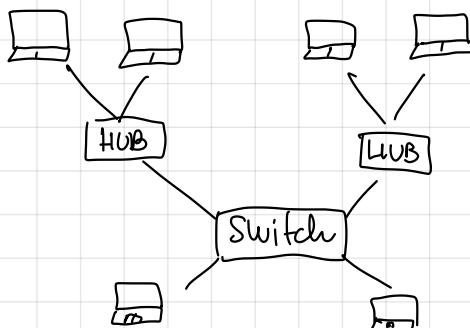
- Comutatore frame liv 2: frame destinati solo sull'interfaccia dove è attivato il destinatario corrispondente.
- Bridge offre prestazioni con interfacce multiple.

Vantaggi: Aumento del throughput sotto carico

Ogni connessione può essere full-duplex

Security

Segmenti → domini di collisione separati → primi di collisioni



o tecnologie switch: 2 tipi

o Store-and-forward

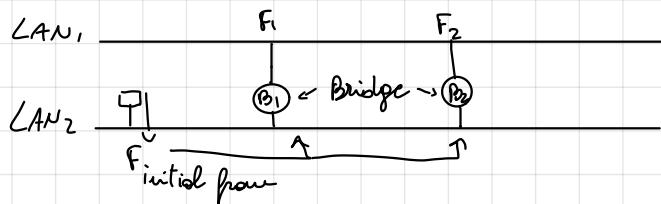
frame ricevuto poi ritrasmesso

o Cut-through

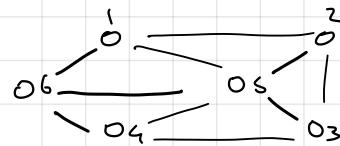
indirizzo destinazione analizzato mentre il frame entra nello switch

• Spanning tree:

In una LAN composta da Bridge/Switch → topologia multiplo per 2 nodi
 > rispetto di ridondanza, per avere percorsi alternativi in caso di guasti.
 > errore di configurazione



rendere ciclico un grafo →
 albero ricorrente (spanning tree)
 spezzi al grafo, e' STP



• Bridge con spanning tree protocol:

- > deve intervenire nel più breve tempo possibile
- > introdurre overhead limitato
- > essere flessibile

• LAN virtuali, VLAN

Sfruttano la capacità di insieme intelligente delle porte degli switch.

Vantaggi:

- > limitano il traffico di broadcast.
- > permettono la progettazione logica della rete.
- > aumentano il livello di sicurezza della rete

VLAN switch ⇒ switch che supportano le VLAN

L'appartenenza di un host ad una VLAN ha vari criteri:

- {- porta
- autenticazione
- protocollo

2C - Wireless:

o IEEE 802.11 Architettura e stack dei protocolli.

- È lo standard per le **rete WiFi**.

Le due modalità di utilizzo → con **infrastruttura**: client connesso a una stazione base (bridge).
→ reti **ad hoc**: rete di computer associati fra loro.

Standard 802.11 ha **2 sottostrati** → sottostrato **MAC 802.11** → problematiche della **condivisione**

→ sottostrato **fisico 802.11** → codifica dei dati

o 802.11 Varianti dello strato fisico:

Può usare **5 diverse tecniche di trasmissione**

tutte le implementazioni eccetto infrarossi
operano nella frequente ISM: 902-928 MHz

2400-2483 MHz

5727-5850 MHz

{ infrared
HDSS
DSSS
OFDM
HR-DSSS

Cause multi-access → throughput condiviso

o Sottostrato fisico di 802.11: (1997 protocollo originale)

- v. limitata 1 o 2 Mbps con 3 tecniche { infrared : non penetra muri
} FHSS : frequency hopping spread spectrum
} DSSS : direct sequence spread spectrum

o Sottostrato fisico di 802.11 b: (1999)

- opera a 2.4 GHz con modulazione HR-DSSS e schiera modulazione CCK
- t.r. 11 Mb/s ma MAC CSMA/CA ha overhead che lo dimezza.
- per evitare interferenze usa 2 gruppi di canali.

o Sottostrato fisico di 802.11 a: (2001)

Utilizza 8 canali da 20 MHz attorno ai 5.2 GHz

Tecnica di codifica OFDM → ogni canale da 20 MHz è suddiviso in 52 portanti da 300 kHz con mod. fase QPSK e dupl. QAM (= ADSL)

- non ha riscontro successivo / EU uso 5GHz riservato

Sottostretto fisico di 802.11g : (2003)

Uso le freq. olio 802.11b con cui è backward-compatible e modulazione OFDM su 52 portanti come 802.11a ma usa 14 canali 22MHz attorno ai 2.4GHz come 802.11b

I sottostretti fisici 802.11n e 802.11ac :

IEEE 802.11n opera a 2.4 e 5 GHz con canali da 20 o 40 MHz

Uso OFDM con mod. QPSK, 16-QAM o 64-QAM

MIMO - 4 antenne per flussi contemporanei di dati:

IEEE 802.11ac opera solo a 5GHz con canali più larghi (80-160MHz)

8 antenne MIMO

I sottostretti 802.11ax e 802.11ay

IEEE 802.11ax 2.4 e 5 GHz canali 20-40 MHz

uso OFDM e mod. fino 1024-QAM

utilizzate zone con ampie densità di utenza

IEEE 802.11ay - attualmente in fase di definizione

Sottostretto MAC 802.11:

Copre 3 funzioni:

- consegna affidabile frame
- controllo dell'accesso
- sicurezza

2 modalità di funzionamento



A contesa

DCF

Senza contesa

PCF

Protocolli MAC: inter frame space (IFS):

DCF e PCF possono condividere nella stessa cella.

- SIFS → separa frame singole trasmissioni
- PIFS → un eventuale AP può innanzitutto i suoi frame di controllo.
- DIFS → Se l'AP face le stazioni possono tentare di acquisire il canale

MAC a contesa (DCF): distributed coordination function

gestione distribuita (come eth) con CSMA/CA

stazione trasmette → RTS → ottendeCTS dal destinatario e invia frame per ogni frame → timer e ACK.

Le reti wireless sono soggette a rumore e quindi inaffidabili

o MAC senza contesa (PCF):

L'AP gestisce tutte le stazioni della sua cella.

Un broadcast (beacon frame) viene mandato 10/100 volte al secondo per sincronizzare le stazioni / associa di nuove stazioni.

Stazioni associate → possono comunicare in un periodo senza contesa tramite polling.

- fatte le stazioni supportano DCF.
- PCF → opzionale

o Frame di 802.11:

esistono 3 tipi di frame

- Data
- Controllo (RTS, CTS, ACK)
- Management

o Campi di un frame:

- **Frame control:** primo octetto suddiviso in 3:

- **Versione** dello standard IEEE 802.11
- **Tipo** (2 bit) specifica il tipo: 00 D or C 10 M
- **sottotipo** (4 bit)

8 flag che seguono, quando impostati a 1 significano

- **A1 DS**: frame diretto al sys di distribuzione
- **Dol DS**: frame proviene dal " " "
- **Altri frammenti**: frammenti appartenenti allo stesso frame
- **Retry**: ripetizione del frammento precedente
- **Risparmio energia**: la staz. base mette una staz. in sleep.
- **Altri frame**: trasmettitore ha altri frame per ricevitore
- **WEP**: campo dati crittato con WEP
- **ordinati**: frammento appartenente alla classe servizi strictly ordered

- **Duration**: quanto tempo il mezzo sarà occupato

- **Address**: frame IEEE 802. Frame contiene 4 indirizzi: MAC Station + AP entrata e uscita

- **Sequence**: consente di numerare i frammenti

- **Data**: è il payload lungo fino a 2312 byte

- **Crcsum**: solito CRC 32

Frame 802.11: indirizzi

trasmettore (TA) e ricevitore (RA) potrebbero non coincidere con la sorgente (SA) o destinazione (DA). In alcuni casi le comunicazioni passa per l'AP (BSSID)

[...] iMG

MTU e frammentazione:

payload max 2312 byte che è l'MTU di IEEE 802.11

la frammentazione migliora le prestazioni.

↳ riduce le probabilità di errore.

Servizi:

Ogni LAN WiFi conforme allo standard 802.11 fornisce 2 tipi di servizi:

- Servizi di **distribuzione**: forniti dall'AP

1. Associazione
2. Dissociazione
3. Riassociazione
4. Distribuzione
5. Integrazione

- Servizi di **stazione**:

1. Autenticazione → sist. aperto o a chiave condivisa
2. Deautenticazione
3. Riservatezza
4. Trasmissione

- **Beacon** → frame di management che viene mandato dall'AP ad intervalli regolari e contiene l'identificatore della cella SSID.

MAN Wireless:

Consente di distribuire dati in area Metropolitana, tramite una potente antenna.
Sono controllati da WiMAX Forum.

La sezione IEEE di WiMAX è la IEEE 802.16

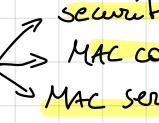
Strato fisico IEEE 802.16:

((01))

Onde in linea rette. Intensità perde a distanza



o Protocollo MAC IEEE 802.16:

data-link suddiviso in 3 sottostrati 
security
MAC common port
MAC service specific

- Formato frame 802.16

- EC payload cifrato
- Type tipo di frame
- Cl se esiste ccc finale
- EK chiavi di codifica usate
- Length lunghezza frame
- ConnID connessioni di appartenenza frame
- Header CRC
- Payload
- CRC finale opzionale

o Bluetooth e 802.15

{ 1999 Sony - IBM - Toshiba - Nokia \Rightarrow syst comunicazione senza fili tra disp. digitali.
{ bassa potenza, raggio 10 m, banda 1.54 o 2.4 GHz
{ banda suddivisa in canali di 1 MHz e usa FHSS

Un bluetooth master può gestire insieme max 7 slave entro 10 m \Rightarrow forma una PicoNet. Gli slave non possono comunicare.

802.15 \rightarrow emozione IEEE per WPAN basata su bt v. 1.1.

o RFID: radio frequency identification \rightarrow per l'identificazione wireless di vari tipi.

(\hookrightarrow passaporti, smartcard, libri, animali)

\hookrightarrow non è integrata nei protocolli di reti di calcolatori.
EPC ha le funzionalità di un codice a barre.

RFID-EPC ha tag e lett

o Low Power LAN: Reti wireless a lungo distanza e basso costo / consumo

o LoRa: long range: wireless a lungo raggio (50 km) e bassa potenza

- 2 livelli :
- physical layer
- MAC \rightarrow LoRAWAN

3A RETE:

Scopi e servizi liv. Network:
collegamento linea in → out opposto

- estendere i servizi dato - link
- trasportare più pacchetti
- commutazione (switching)

di circuito (telefonia)
di pacchetto (reti di calc)

○ Commutazione di circuito:

- modi di transito → centralini di commutazione.
- l'algoritmo di commutazione interviene all'apertura del circuito fisico.
- concessione → allocazione risorse necessarie.
- ritardo: minimo nel trasferimento.
- efficiente → risorse allocate anche se concessione utilizzata.

○ Commutazione di pacchetto:

- comunicazione frazionata in pacchetti.
- Algoritmo per commut. interviene sui pacchetti.

tipi di modi di transito
↓ ↓ ↓
Hub Switch Router Gateway

tipologie di commutazione e pacchetto

A circuito virtuale e datagramma.

○ Commutazione pacchetto e circuito virtuale: (VC)

- Algoritmo per commutazione solo all'inizio per l'apertura del canale virtuale VC.
- ogni router viene marcato con l'etichetta del VC
- pacchetti seguono il percorso individuato
- Implementazioni { ATM
 - internet con MPLS → isole o vc
 - IPVG supporta reti vc

○ Commutazione di pacchetto e datagramma:

- pacchetti inviati in modo indipendente in base all'indirizzo di destinazione.
- indirizzamento determinato dai router → tabelle di indirizzamento / algoritmo routing.
- pacchetti di connessione uguali possono seguire strade diverse.
- Implementazioni IPV4
IPVG

o Routing: parte del software dello strato network che si occupa dell'indirizzamento dei pacchetti

Se rete a datagramme → routing determinato per ogni pacchetto
 Se rete a circuito virtuale → routing determinato al momento dell'attivazione del circuito.

o Rete e CV: MPLS: multi protocol label switching

Consente di creare in internet aree e commutazione di label

Strato → sotto al livello di rete aggiungendo un proprio header 4 byte tra IP e eth PPP/

Vantaggi → QoS, VPN, traffic shaping

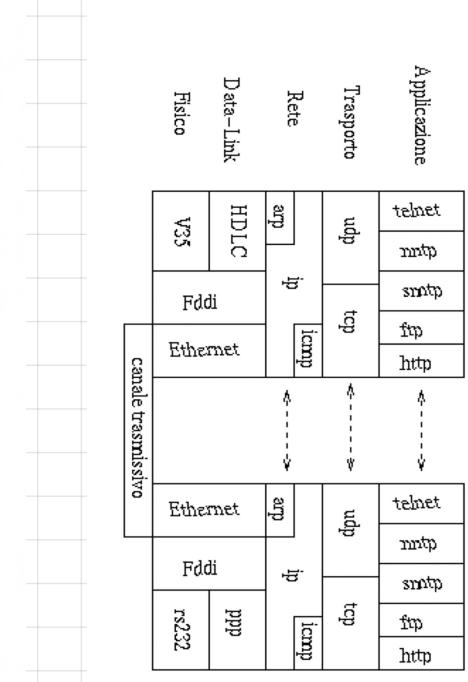
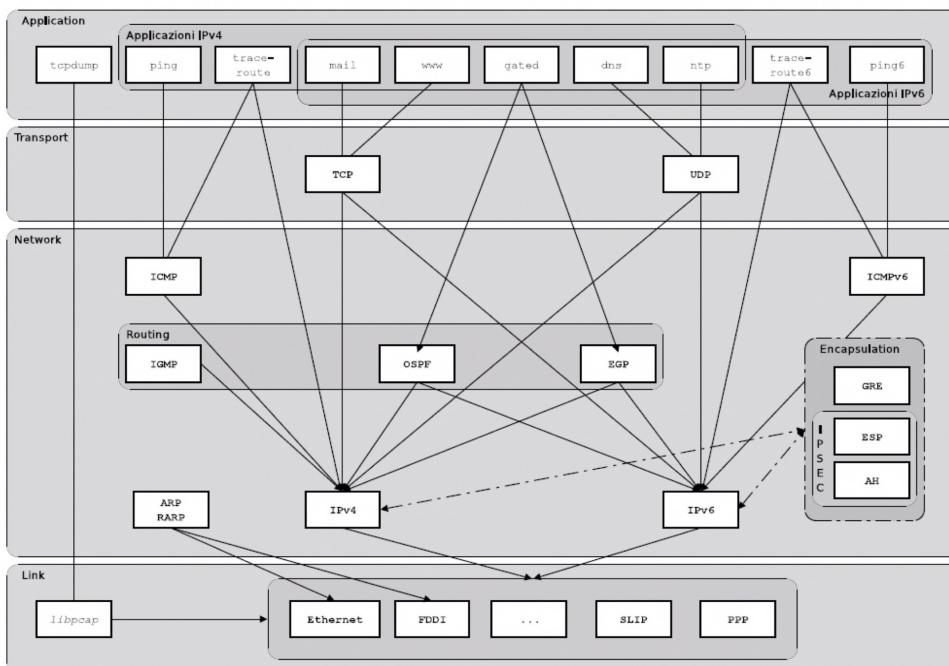
o Routing MPLS:

Il router deve supportare il protocollo

1° package → definisce tunnel nelle reti MPLS → i paesaggio seguono quel percorso

o Protocolli TCP/IP:

- Nessuno specifico per strati sotto IP.
- IP svolge indirizzamento e funzioni di rete
- TCP e UDP → funzioni di trasporto e controllo connessione end to end.
- Strati sop: fornisce servizi all'utente.



Standard internet: Internet society, RFC:

Esistono solo enti di coordinamento → internet society



ICANN, IANA

ICANN ente no profit che assegna gli indirizzi IP, iostut. protocollo e DNS relativi.

5 organizzazioni RIR

ARIN	: NA
APNIC	: AU / ASIA
RIPE	: EU / RU
LACNIC	: Sud America
AFRINIC	: Africa

IP: Lo stato Network di internet:

- interconnette più reti di livello data-link (LAN o punto-punto)
- servizio trasporto datagrammi
- IPv4

Operazioni:

flusso def; → diviso in datagrammi che posse uno stato IP → il datogramma viene incorporato nelle trame IP e trasferito da un router all'altro → intestazione

Il datogramma può subire frammentazione → viene estratto dalla trama IP (eventualmente riassemblato) e passato al livello di trasporto → ricostituisce il flusso.

QoS → la consegna è "Best effort"

Trama IP

Il datogramma IP → intestazione (header) IP → segmento del liv. di trasporto.

seg. liv. trasporto
Header L2 | Header IP | Payload max 64 kB

d' header ha una parte fisica e una parte opzionale variabile → trasmessa in ordine big endian

- | | |
|--|-------------------------------------|
| - Version (4bit) | - DF (1bit) don't frag |
| - HLEN (4 bit) dim header | - MF (1bit) more frag |
| - type of service (6 bit) controllo rete | - Fragment offset (13 bit) pos frag |
| - total length (16 bit) byte tot head + dati | - TTL (8bit) n. max salti |
| - Identification (16 bit) | |

- Protocol (8 bit) → prot. di liv. superiore
- header checksum (16 bit)
- SA e DA address (32+32 bit)
- options
- padding

o Indirizzi IP:

32 bit con notazione dotted decimal (0^4-2^{32}) separati da ":"

Muti indirizzi $2^{32} = 4\,294\,967\,296$

Seq. suddivise in 2 parti ↗ Host id = distingue host stesse reti
NET id = rete liv 2 usata dai router per indirizzamento.

o Classi IP:

classe	bit iniziali	inizio	fine	indirizzi
A	0	0.x.x.x	127	2 G
B	10	128.x.x.x	191	1 G
C	110	192.x.x.x	223	0.5 G
D	1110	224.x.x.x	239	0.25 G
E	1111	240.x.x.x	255	0.25 G

[slide p 23]

o IP per uso privato: riservate da ICANN uso privato (intranet)

Classi	inizio	fine
1 classe A	10.x.x.x	
16 classi B	127.x.x.x	127.31.x.x
256 classi C	192.x.x.x	192.168.255.x

o IP subnetting: lo concede l'IPv4

Ulteriore livello di gerarchie per IPs: Net → subnet → host
NET MASK → poram. 32 bit che suddivide → bit a 1 campo NET/SUBNET
bit a 0 campo host
→ riportisce una rete grande in tante piccole

o Indirizzamento datagrammi:

rete appartenente host → modalità consegne ↗ direct delivery
indirect delivery

direct: host SA e DA condividono la stessa rete

indirect: DA e SA appartengono a reti IP diverse

Tabelle di routing!

tabelle che contiene destinazioni e percorsi per raggiungerle

dest	router	mask	interface
160.78.124.0	*	255.255.255.0	eth0 diretta
193.1.1.0	160.78.124.253	255.255.255.0	eth0 indiretta
default	160.78.124.254	0.0.0.0	eth0 indiretta

prima riga → gli host di quella rete vengono raggiunti in diretta

seconda riga → gli host " " " " " tramite l'altro router

NAT (Network Address Translation) :

- dispositivo che consente agli host di una LAN (indirizzi privati) di comunicare in Internet utilizzando un solo IP pubblico.

Not : { - SNAT source → manipola l'indirizzo sorgente
- DNAT destination → manipola l'indirizzo destinazione

Tabelle NAT:

Le entry delle tabelle possono essere ↗ statiche
↘ dinamiche

Not statico:

server interno contatto da client esterno → entry statica che associa porta NAT con una porta/IP server interno.

Not dinamico:

client NAT si rivolge al NAT per contattare un server esterno, NAT genera entry dinamica associa IP/porta client con IP/porta server e applica SNAT.

Problemi NAT:

- violazione univocità: host usano stessi indirizzi
- IP non più connectionless
- IP non più stratificato
- questo NAT → problema

Protocollo ARP:

Ogni interfaccia di rete di un nodo possiede un indirizzo fisico e un IP

Il protocollo ARP determina quell'indirizzo fisico da un nodo IP.

Se un nodo mittente deve contattare un destinatario di cui sa solo l'IP usa ARP

- > il modo serpente \rightarrow ARP request \rightarrow diff. broadcast su LAN
- > il modo in oggetto \rightarrow ARP reply \rightarrow unicast
- > ogni host ha le sue ARP cache

o RARP Reverse ARP: (obsoleto \rightarrow DHCP)

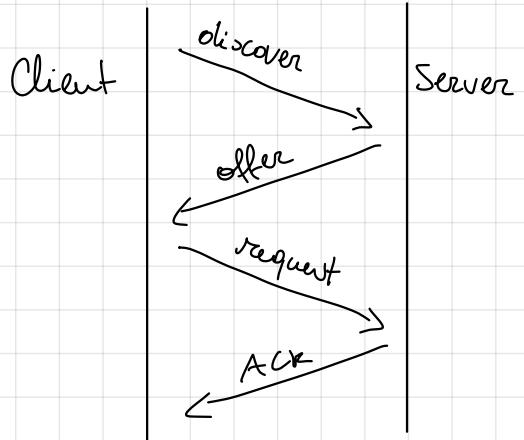
Alcuni nodi IP non conoscono il loro IP \rightarrow usano RARP mandano il MAC in broadcast chiedendo l'IP

o DHCP: Dynamic host configuration protocol.

- \rightarrow il server DHCP pu \circ fornire info al client
- \rightarrow l'IP pu \circ essere fornito statico o dinamico
- \rightarrow server pu \circ essere in LAN diverse da quella del client

funzionamento:

- 1) DHCP invia in broadcast pack DHCP discover
 - 2) Server risponde con pack DHCP offer
 - 3) Client accetta e rimanda un DHCP request (broadcast)
 - 4) Server manda DHCP ACK per conferme
- rimando dhcp continua in modo dinamico o statico



o ICMP: Internet control msg prot.

- protocollo di servizio IP per lo scambio di msg d'errore o controllo
 - \hookrightarrow consentono a host e client di accorgersi di eventuali malfunzionamenti

3B - IPV6:

Why → necessita nuovo layer IP per

SIPp → IPV6 → 16 byte = 128 bit

Notazione: 8 quaterne di numeri separate da ":"
gruppi di 4 zeri → ::

Gli IPV4 possono essere compresi tra gli IPV6 con un prefisso di 96 zeri.

- broadcast → non esistono in IPV6
- indirizzi speci → loopback etc.
- multicast → assegnati a più interfacce
- anycast → (nuovi) ↑

in URL fra [IPV6]: xxxx

IPV6: Indirizzi global unicast

IANA 2000::/3 prefisso 001 → frammentati in reti più piccole

RiPE 2001:600::/23 → " " " "

GARR 2001:700::/32 → "

UNiPR 2001:760:2E04::/48 Uni PR e infn PR

Interface ID:

Reti assegnate alle strutture per reti locali → 64 bit

Ultimi 64 bit di IPV6 possono essere assegnati in vari modi:

- via DHCPv6
- conf. manuale
- autogenerati
- autoconf. con interface ID

Seq di 64 bit univoci di ogni interfaccia
di rete, a partire dai 48 bit del MAC

O De MAC48 a Interface ID:

MAC48 gestiti da IEEE, che gestisce anche sua numerazione a 64 bit, EUI64

(l'interface ID usa una versione modificata di EUI64 (7° bit posto a 1 di EUI64))

IPV6: Indirizzi link-local

Sono destinati ai terminali dello stesso rete locale
prefisso 1111 1110 10

Gli indirizzi con questa notazione non attraversano mai un router

- ovvero miliardi di host
- semplificare routing
- > sicurezza
- > qualità
- mobilità e future evoluzioni

o IPv6: Indirizzi Site-local

Un **site** è un gruppo di link gestiti da un'unica autorità (es: Campus)
↳ sono per uso privato, analoghi a 192.168.0.0 /16 di IPv4

Prefisso 1111 1110 11. A differenza dei link local vanno configurati manualmente.

IPv6: Indirizzi multicast e anycast:

IPv6 multicast → identificare e raggiungere un gruppo di nodi simultaneamente
prefisso → 1111 1111 (FF) + 4 bit preziose + 4 ambito + 12 per identificare il gruppo.

IPv6 anycast → caratteristiche degli unicast, attribuiti a più interfacce di reti e componenti di rete differenti.

- Anycast deve essere supportato dal router. Il più comune serve a raggiungere tutti i router in link-local.

Loopback: 0:0:0:0:0:0:0:1 o ::1 identifica il nodo stesso come 127.0.0.1
IPv4 compatible: permettono di inserire IPv4 antepponendo 36-0

o Trama IPv6:

eliminato da IPv4 ↗ fragmentazione
↗ check-sum (preziosi)
↗ campo protocol (header)

header fields:

- version 4 bits
- traffic class 8 bits nuovo campo per QoS
- flow label 20 bits label switching
- payload length 16 bits
- next header 8 bits
- hop limit 8 bit - era il TTL
- source address 128 bit
- destination address 128 bit

o ICMPv6:

equivale a ICMP per IPv4 con nuove funzioni:

formato pacchetto:

type | code | checksum
message body

- path MTU discovery
- Neighbor discovery
- router discovery

o **path MTU discovery**: protocollo basato su ICMPv6 → consente di determinare l'MTU ideale per connessione TCP

o **Neighbor discovery**: sostituisce ARP per determinare l'indirizzo di rete LAN

- usa pacchetti ICMPv6 anziché ARP, multicast invece di broadcast.

o **Router discovery**: con IPv6 gli host possono individuare automaticamente i router in un link

- avviene con 2 messaggi: ICMPv6 {router solicitation | router advertisement}

o DHCPv6:

è il protocollo per IPv6 che consiste nello scambio di segmenti UDP quali:

- solicit
- advertise
- request
- reply

o Stateless address auto-configuration (SLAAC)

Combinando il protocollo di router discovery con l'autoconf. degli indirizzi link-local è possibile assegnare un indirizzo global unicast in modalità plug & play senza bisogno di un servizio DHCP.

3C - Routing: Scelta del percorso su cui inviare i dati quando mittente e destinatario appartengono a due reti diverse.

Il mittente affida le consegne ad una struttura interconnessa di router

- o Router: dotati di due funzioni:
 - intradomestico (1)
 - fuori (2)

(1): Gestione di una tavola di routing RT

- algoritmo di routing: scegliere lungo quale linea di uscita fare routing
- protocolli di routing: scambio informazioni necessarie per determinare topologia rete

(2): Applicazione dell'intradomestico sui singoli datagrammi:

- lettura intestazione IP
- look-up tavola routing
- switching

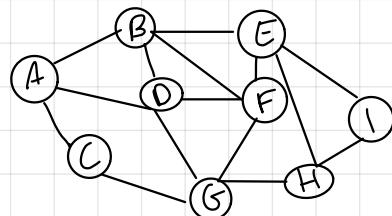
- o Algoritmo di flooding:

Algo di routing che rinvia ogni pacchetto entrante a tutte le linee eccetto il mittente.

Utilizzato in bridge e protocolli linee - shot

- o Alg. Shortest path first: (SPF)

- topologia della rete → grafo pesato non orientato
- cammino minimo di un nodo per un altro è "sink tree" o source tree.



- o Protocolli di routing: stabiliscono la modalità di comunicazione fra i router per la costruzione delle topologie di rete. Possono essere statici o dinamici.

- Routing statico: topologia e tavola routing definite in fase di setup. In caso di variazioni è richiesto intervento gestore.

- Routing dinamico: topologia rete automatica e dinamica in base ai cambiamenti.

- centralizzato: modo centrale raccoglie informazioni, calcola la RT per ogni nodo e le spedisce. tavole consistenti.
- distribuito: i nodi si scambiano informazioni sullo stato delle reti e ogni nodo calcola la sua tavola.

o Protocolli distance vector:

tpk/dlv/rv

Nel proto ogni coppia di nodi ha una distanza. Dipende dalla "metrica"

Nel protocollo DV invia ai primi vicini l'elenco delle distanze con gli altri nodi periodicamente. Le distanze vengono misurate (ECHO). La tabella contiene un entry per ogni nodo presente in rete.

entry —

indirizzo
hops
Costo
linee

 il dv contiene tutto ma non le linee

Il ricevente verifica se ci sono modifiche dal precedente e nel caso aggiorna
↳ aggiorna poi la propria tabella tramite merging.

A portata di costo si usa la strada con meno hops.

* Semplifica ma è lenta convergenza.

o RIP protocol: routing information protocol

È la prima implementazione di protocollo DV, ne esistono 3 versioni:

- RIPV1 (RFC 1058) routing classfull (reti senza NetMask)
- RIPng (RFC 2080) estensione per IPv6
- RIPV2 (RFC 2453) usa routing classless

o Protocolli Link-state:

È un RP con cui ogni nodo determina e mantiene aggiornata la topologia della rete da cui calcola le tabelle di routing applicando un RA

Fasi:

1. Scoperta dei vicini
2. Misurazione costo linea
3. Costruzione di un pacchetto
4. Distribuzione periodica del LSP a tutti i nodi della rete
5. Ogni nodo costruisce la topologia della rete e aplica RA per calcolo delle tabelle

o OSPF: (open shortest path first)

Protocollo IGP di tipo link state packet

- ciascun router emette periodicamente pacchetti "hello" multicast
- " " costruisce un pacchetto con l'elenco delle reti attive e i loro costi
- invia in flooding pacchetti link-state update
- se in base ai pacchetti ricevuti ci sono state modifiche, aggiorna la topologia della rete

o Protocolli gerarchici:

reti grandi → tabelle di routing non possibile per l'intera rete
↓ routing gerarchico

- intera rete riportata in aree
- i router all'interno fanno routing per le loro aree
- per destinazioni esterne si limitano a mandare pacchetti ai router "di bordo" che conoscono la topologia esterna
- i router di bordo si occupano solo di indirizzamento pacchetti fra aree

o Protocolli di routing in internet:

In TCP/UDP i router sono suddivisi in due classi:
→ exterior router (1)
→ interior router (2)

- (1) interconnettono due insiemi di reti distinti (Autonomous Sys)
- (2) utilizzano protocolli Exterior Gateway Prot. Sono i router all'interno di

Gli IGP più usati sono RIP(DV) e OSPF.

BGP → protocollo raccomandato in internet per interconnessione di Autonomous Sys
↓

Border Gate protocol

Path vector: invece di proporre i costi propone la sequenza di AS da attraversare per arrivare a destinazione

o Routing Anycast:

IP Anycast: consente a macchine e router di condividere l'IP

Gli algoritmi di routing basati su DV o LS gestiscono automaticamente percorsi multipli per raggiungere una destinazione

Il routing non è stabilito sugli IP ma sulle reti, quindi va stabilito uno anycast.

4A - TRASPORTO:

- Scopo del livello: fornire al liv. applicazione protocolli astratti per comunicazione fra due processi: flusso byte, scambio messaggi, chiamate funzione ecc.
- Offre al liv. applicativo una interfaccia indipendente (IPV4 IPV6)
- Use: servizi dello strato di rete.
- Presupposti: messaggi possono essere perduti, arrivare disordinati, più copie e ritardi

• Servizi livello trasporto:

Definiti dalla Socket Lib. di Berkeley

2 tipi di servizi di trasporto:

Affidabile (TCP)

orientato alla connessione,
garanzie di consegna.

Inaffidabile (UDP)

Scambio oleogrammi,
senza garanzie di consegna

Ricezione (demultiplexing): il liv trasporto gestisce una porta che associa il pacchetto IP in arrivo al processo applicativo a cui è destinato.

Spedizione (multiplexing): dato eventualmente ridotto in segmenti.

• Porte Berkely Socket Lib.

Porta: identificativo (16 bit, 64k porte) → punto di arrivo di una connessione su di un host.
la coppia IP+porta è un identificativo univoco: socket
ogni connessione è identificata come coppia di socket.

Porte 0-1024 → Well known ports (21 FTP 80 HTTP etc)
In Linux le WKP sono associate a socket solo da root.

- Come si trova le porte?

Servizio ↗ Standard: si usa una WKP o una porta non privilegiata
di rete dinamico: si usa un nome server con port mapper in ascolto su 1 WKP

- Segmentazione: Il mittente frantuma il flusso → segmenti consegnati al layer Network (IP) → si occupa delle consegne.

Se si incontra Link con MTU → frammentazione

Per evitare frammentazione → definito MSS in base al MTU dell'interfaccia locale.

o Client/Server: è il tipo di comunicazione usato nella *Berkeley Socket Lib.*

- **Server** → sempre in ascolto su porta stabilita. bind() assegna un indirizzo locale e un socket.
- **Client** → prende contatto col server specificando la porta.
→ necessario sapere IP e porta

o Prog. servizi a datagrammi:

Client → msg 1 sendto() e riceve da os il n° di porta dinamico.

Al succ. eventuale recvfrom() client ascolta sulle stesse porte.

Il server inizia con 1 e la sua porta di ascolto è definita da bind().

o Prog. servizi connection oriented: (TCP)

- listen() → predisponde code attesa per i client

- accept() → primitiva bloccante → server ascolta sulle porte. Server può creare nuovo processo (fork) / nuovo thread per gestire connessione sul nuovo socket.

- connect() → utilizzata dal client per aprire una connessione. send() con recv()

o Protocollo UDP:

modo per inviare datagrammi senza stabilire connessione.

Oltre a IP serve una porta di origine e destinazione per demultiplexing.

- Intestazione UDP → contiene la lunghezza del segmento

UDP usato per:

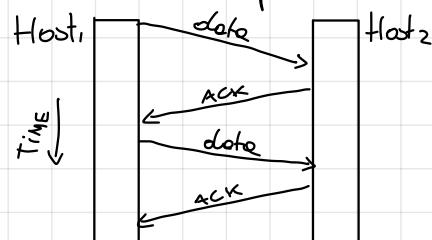
- implementazione protocolli applicativi per brevi scambi msg (DHCP, DNS, TFTP)
- costruzione di servizi di trasporto astratti "middleware" (RPC, RTP)
- comunicazioni broadcast, multicast.

o Protocollo TCP:

- flusso di byte end-to-end affidabile
- connessioni full duplex e unicast (no multi/broad)
- riceve flussi di byte da processi locali → spezza e spedisce datagrammi IP separati.
- send() consegna i dati in buffer di spedizione. Possono essere raggruppati o frammentati.
- segmenti max 64 kb
- flag PUSH → invio non ritardato
- TCP scrive i segmenti nel buffer di destinazione e ricostruisce.

o Corretto consegna e ordinamento segmenti:

Il riscontro o ACK abbinato al numero di sequenza → strumento per corretto consegna.



Mittente invia segmento dati

Destinatario invia pacchetto flag ACK

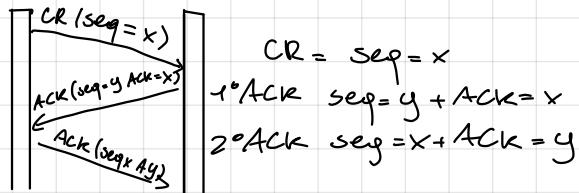
Mittente attiva Retransmission Time Out RTO x ogni seg.

o Attivazione connessione:

Dialogo client-server → inaffidabile. Possibili ritardi duplicati

Soluzione Tomlinson (1975) → handshake a 3 vie

1. Client manda CR
2. Server risponde ACK
3. Client manda terzo seg. con ACK



o Apertura connessione TCP:

Derivata da Tolimson:

- 1) Connect sul client invia segmento $\text{SYN}=1 \text{ ACK}=0 \text{ seq}=x$
- 2) Se server ascolta e accetta → risponde con seq. $\text{ACK}=1, \text{SYN}=1, \text{ACK}=\text{seq}+1$
- 3) Client termina apertura con riscontro seq. del server

o Chiusura TCP:

handshake a 2 vie per ogni direzione. Generalmente con 3 segmenti; secondo `FIN+ACK`

`close()` determina l'invio del `FIN`, quale messo chiuso.

Se risposta `FIN` non arriva in due RTT il mittente rilascia la connessione.

o Buffering:

Necessario per ogni connessione TCP $\xrightarrow{\text{ricezione}} \xleftarrow{\text{trasmissione}}$

ricezione:

- | | | |
|--------------------------------|-------------------------------------|---|
| - dati spediti non riscontrati | $\xrightarrow{\text{trasmissione}}$ | - dati ricevuti, riscontrati, non letti |
| - dati ancora da spedire | | - dati ricevuti non ancora riscontrati |
| - spazio libero | | - spazio libero |

o Socket NON blocking:

bloccati per default: `send()`



Si blocca se buffer trasmissione pieno. Libero quando c'è spazio

`recv()`



Blocca quando buffer ricezione è vuoto, ritorna quando ci sono dati.

Se pieno e settato non bloccante, nessun blocco ma ritorna -1 col errore `EWOULDBLOCK`

Se vuoto e settato non bloccante, nessun blocco ma ritorna -1 col errore `EWOULDBLOCK`

o Controllo di flusso: sliding window

Per controllo flusso e ottimizzazione throughput in TCP.

→ ricevente annuncia al trasmettitore la Receiver Window size (RWND)

→ trasmettitore può inviare anche più dati senza riscontro purché non ecceda le RWND in byte.

o Trama TCP:

Porta di provenienza + destinazione → estremi connessione

Numero sequenziale → contatore flusso byte spediti.

Numero riscontro → contatore n. byte ricevuti.

TLEN → 32 bit header campo opzioni variabile

4 bit per sviluppi futuri

8 bit di codice: quando a 1:

{ - CWR e ECE → quando ECN attivo

{ - ECE (ECN-Echo) :

- CWR :

- URG: puntatore urgente

- ACK: n. riscontro

- PSH: no buffering ricevente

- RST: reset connessione

- SYN: attivazione

- FIN: rilascio

- Finestra 16 bit → dico sliding window

- Checksum 16 bit → somma in complemento

a 1 delle sequeenze di 16 bit del seg. TCP
e la "pseudo-intestazione"

- puntatore urgente 16 bit → solo se URG=1 e
indica lo scostamento di byte dell'ultimo
byte urgente

OPZIONI:

- MSS: max dim segmento

- Scale finestra: n. shift e s

- SACK → selective acknowledgement

- Timestamp → orologio temporale

o Determinazione MSS ottimale

frammuntazione → overhead sull'attivita dei router

framm. troppo piccoli → overhead traffico di rete

MSS: max segment size

MSS ottimale → MTU minimo tra tutti gli MTU incontrati nel tracitto.

Alg descritto in RFC 1191: inizialmente determina MSS con la MTU dell'interfaccia locale
Inizia poi un segmento con bit DF a 1. Se si incontra un router per cui è troppo grande
restituisce errore e l'MSS si regola di conseguenza

o Opzione SACK:

TCP funziona con GoBack N oli solo: si rispediscono segmenti da quelli errato (per primo)

Per migliorare le prestazioni si propone Selective Ack - SACK → ricevitore determina quali
segmenti sono corretti così da forzare rinviare solo quelli errati.

2 opzioni header TCP:
- SACK permitted: incluso in SYN, consente di gestire SACK
- utilizzata dal ricevente per gestire le informazioni SACK.

Ozioni e ottimizzazioni TCP:

- **Delayed ACK**: dest. riceve un seg. in ordine può attendere fino a 200ms per il prossimo seg.
- **ACK cumulativo**: se durante l'attesa riceve un altro seg. in ordine risponde con il ACK cui. che riscontra l'ultimo byte della sequenza.
- **fast retransmission**: dest. riceve seg. fuori ordine \rightarrow invia ACK che riscontra l'ultimo seg. ricevuto in ordine \rightarrow ricevente ne riceve 3, riteasmette seg. perduto.

Prestazioni calano se

trasmettitore genera dati lentamente \rightarrow sol: Alg. Nagle (1)

ricevitore consuma dati lentamente \rightarrow sol: sol di Clark (2)

- 1) **Nagle**: se mittente ha pochi byte da spedire e ai suoi dati non riscontrati \rightarrow aspetta ACK se mittente ha molti byte da spedire/seg. piccoli riscontrati \rightarrow spedisca subito
- 2) **Clark**: se ricevente pubblica finestre troppo piccole l'alg. forza il ricevitore ad attendere che le finestre raggiungano un val minimo prima di comunicarlo al mittente.

Retrasmissione time out (RTO) di TCP:

Serve per decidere quando un pacchetto è perduto \rightarrow almeno pari a RTT, aggiornarsi dinamicamente e gestire congestioni.

Alg. Jacobson: se ACK arriva prima del RTO l'alg. calcola l'RTT e aggiorna le var:

$$\text{RTT medio} - \text{Dev Media} \Rightarrow \text{RTO} = \text{RTT}_M + 4 \times \text{Dev Media}$$

Alg. borchoff di Karn: RTO scade \rightarrow rete congestionata \rightarrow non aggiornare RTT_M e RTO x2 fino a quando i seg. non arrivano e dest al primo tentativo

$$\text{RTO}(i+1) = 2 * \text{RTO}(i)$$

Timer TCP Linux:

- Timer di persistenza: attivato a finestra chiusa ($RWND=0$)
- Timed wait: tempo attesa dopo un FIN.
- Timer keepalive: parte quando la linea è inattiva.

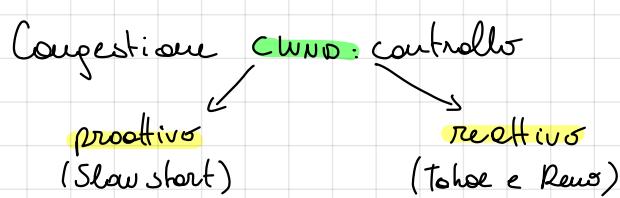
4B - Controllo della congestione QoS

o Controllo congestione:

troppi pacchetti in una porzione di rete → prestazioni degradate → necessario controllo congestione
si può fare prima che si verifichi o quando si è verificato
(proattivo) (reattivo)

o Controllo congestione in TCP:

introduzione finestra: CWND = congestion window
la finestra effettivamente utilizzata AWND è: receiver WND
$$AWND = \min(CWND, RWND) \geq Lost\ byte\ sent - Lost\ byte\ Acked$$



o Slow start e Tahoe:

- 1) Proattivo: mittente CWND=MSS e raddoppia fino:
- CWND → ha max di cui avoro = RWND
- CWND → raggiunge threshold
- 2) Reattivo: Se scade il timer → congestione e si torna a slow start con CWND=MSS

o Controllo reattivo con fast recovery (tcp Reno):

Migliore Reno → 2 meccanismi per perdite dati:
1 timeout timer → CWND=MSS
2 ricezione 3 ACK duplicati: fast rec.
CWND → new threshold

o Algoritmo RED (Random early detection):

- è sia proattivo che reattivo. Interviene sulla coda di pacchi nel buffer spedizione
- definisce 2 timer T_{min}, T_{max}.

- $X < T_{min}$ Paccodato
- $T_{min} < X < T_{max}$ Psorbatto/accodato
- $X > T_{max}$ P scartato

con X pacchetti P in coda

→ comporta l'invio di 3 ACK duplicati

o Segnalazione esplicita ECN: router avverte esplicitamente con pacchetto chocne

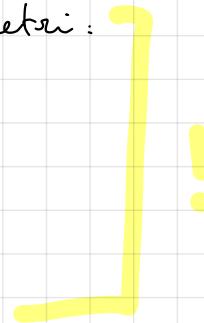
ECN in IP: segnalazione de router e mittente

} mittente risponde e liv. di trasporti
attivando fast recovery

ECN in TCP: segnalazione end-to-end

QoS: Quality of service: Si basa su 4 parametri:

- Affidabilità: garanzia consegna.
- Ritardo: tempo necessario x consegna.
- Jitter: Variabilità ritardo.
- Bande: Velocità trasmissione.



Gestione QoS:

- può essere concordata fra utente e fornitore tramite un Service Level Agreement
- per singolo flusso: all'apertura del canale si determinano tecniche tipo:
controllo accesso o prestazioni risorse
- per classi di servizio
- i servizi sono offerti da un insieme di router → dominio amministrativo

Rete ATM: ha definito 4 classi:

Classe A: Constant bit rate (CBR)

Classe B: Realtime variable bit rate (VBR-RT)

Classe C: non-real time traffic (VBR-RNT)

Classe D: Best effort. ABR (average bit rate)
UBR (unspecified bit rate)

Classi di servizio: Diff Serv (DS)

Introdotte a supporto di IPv4 e IPv6 - in IPv4 campo type of service
- in IPv6 campo traffic class

Classi diffserv più comuni:

- Default forwarding
- Expedited forwarding (EF)
- Voice adtnt (VA)
- Assured forwarding (AF)

Implementazione QoS: Class-based

- code e priorità: definite classi di priorità e create code per classe.
Le code ad alta priorità vengono servite prima

- code pesate: Ad ogni classe viene assegnato un peso: n. pacchetti multati proporzionali al peso vantaggio: code con meno peso servite comunque

○ Leaky Bucket: dati da spedire possono arrivare a qualsiasi velocità ma vengono accodati e rispediti ad un tasso costante limitato.

○ Token Bucket: + flessibile grazie ai token token → diritto a spedire un pacchetto i token vengono forniti a intervalli regolari ai mittenti

5A - DNS - EMAIL

• TFTP e FTP:

TFTP è la versione semplificata di FTP (trivial)

FTP → protocollo per trasferimento affidabile ed efficiente dati, basato su TCP

FTP fornisce inoltre autenticazione e gestione.

Porte TCP 21 comandi e TCP 20 dati.

Modalità attiva e passiva: Attiva → client apre canale comandi verso server
trasmissione dati → client svolge la funzione di server

Passiva: è prerogativa del client dare il via alla connessione x trasferimento dati.

TFTP non supporta l'autenticazione

- ↓ funzione tramite UDP con server listener su G9
- ↓ gestione del flusso a liv. applicativo all'interno di TFTP

• TFTP - Protocollo

- trasferimento iniziale con read (GET) o write (PUT)

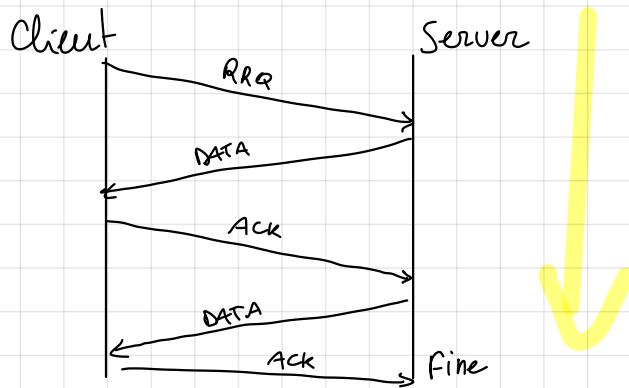
GET → server risponde con file frammentato in datagrammi numerati:

Ogni datagramma deve essere riscontrato

Fasi sessione TFTP

Client contatta il server (pack RRQ/WRQ) → server risponde con pack DATA

→ ACK per ogni scambio → pacchetti trasferiti fino a min. dimensione 512 Kb

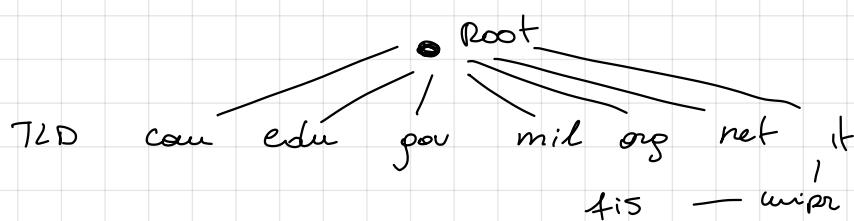


• DNS : Domain Name System :

Scopo: gestire uno spazio univoco dei nomi per i nodi delle reti

fornire traduzione numero-name e viceversa ad utenti IP
domini

netlab. fis. unipr. it → TLD → se già cosa sono
nome nodo locale



o Risoluzione inversa:

È la risoluzione del nome a partire dall'indirizzo IP

Il nome dei domini reverse è composto dai numeri della rete (ordine rovesciato) + stringa "in-addr.arpa" (TLD x risoluz. inversa)

o DNS client:

Ogni client deve essere configurato con almeno un server DNS locale e cui rivolgersi per le soluzioni.

Il server DNS locale recupera l'informazione e la comunica al client.

La config. DNS può essere impostata dinamicamente dal prot. DHCP assieme ad altro (IP, gateway...)

o Zone DNS:

I TLD possono organizzarsi in sottodomini di livello 2 e a loro volta livello 3.
Lo spazio dei nomi è gestito suddividendolo in zone.

Zone → gestita in modo autonomo con DNS primario e 1 o + secondari

↓
include una porzione
dell'albero

Configurazioni possibili (3) → Server autoritativo di zona

↓
coaching nome server (forwarder)

→ **primario** (master)
→ **secondario** (slave)

Se server → autoritativo → risponde direttamente

ma non autoritativo → attraverso l'albero passando da quello autoritativo

attraversamento → ricorsivo: se non c'è aut. passa la richiesta al succ. ricorsivamente

→ iterativo: il serv. restituisce al client l'indirizzo del server succ.
→ è il DNS che contatta direttamente i server coinvolti.

o Root Server: Internet ha 13 root server che contengono informazioni

↓ **TAB** | riguardanti i domini di primo livello.
solo non ricorsivi | Vengono contattati ogni volta che un client chiede informazioni relative ad altri TLD.

o Resource Record: le informazioni relative alla zone vengono memorizzate → RR

formato generico, compi:

- Nome
- TTL
- classe

- Tipo
- A
- AAAA

- CNAME
- MX
- NS

- PTR
- SOA

o DNS e la posta elettronica:

Ogni dominio in grado di ricevere posta, il suo DNS è in grado di fornire una lista SMTP e un inviare il messaggio.

Le queste info sono contenute nei record MX (mail exchanger)

- Formato del pacchetto DNS:

- Transaction ID
- flags significativi
- question
- answer
- authority
- additional

o DNS dinamico (ddns)

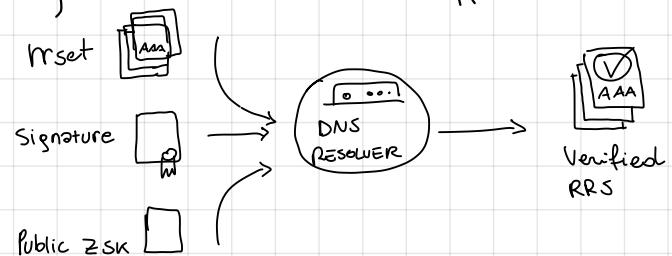
Permette ad un nome DNS in internet di essere sempre associato all'IP di uno stesso host, anche se l'indirizzo cambia nel tempo.

→ costituito da una popolazione di client dinamici, da 1 o + DNS dinamici e un protocollo di comunicazione fra le due parti.

o DNSSEC (security extensions):

Sono una serie di specifiche dell'IETF per garantire sicurezza e affidabilità delle informazioni fornite dai sistemi DNS.

Service → autenticazione
→ integrità dati ricevuti

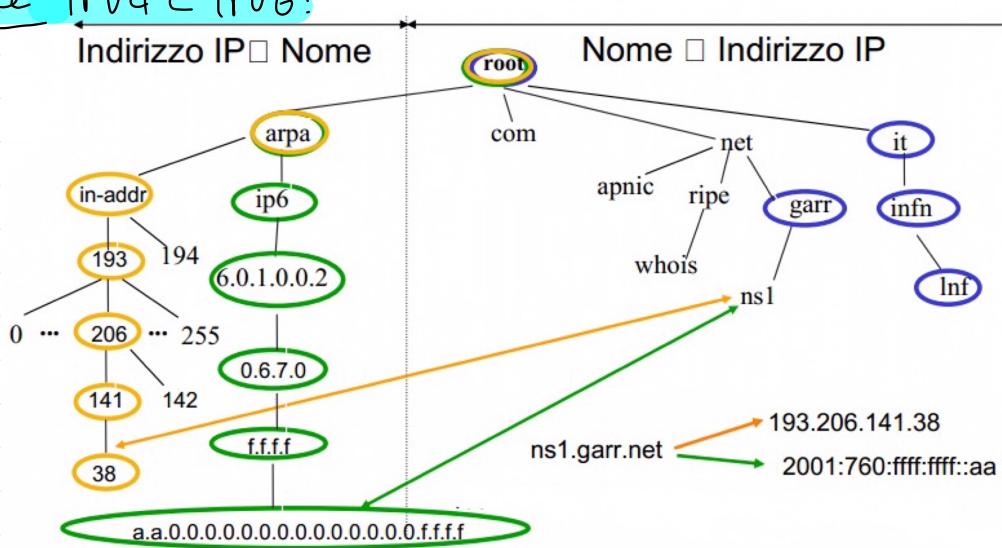


Per IPv6

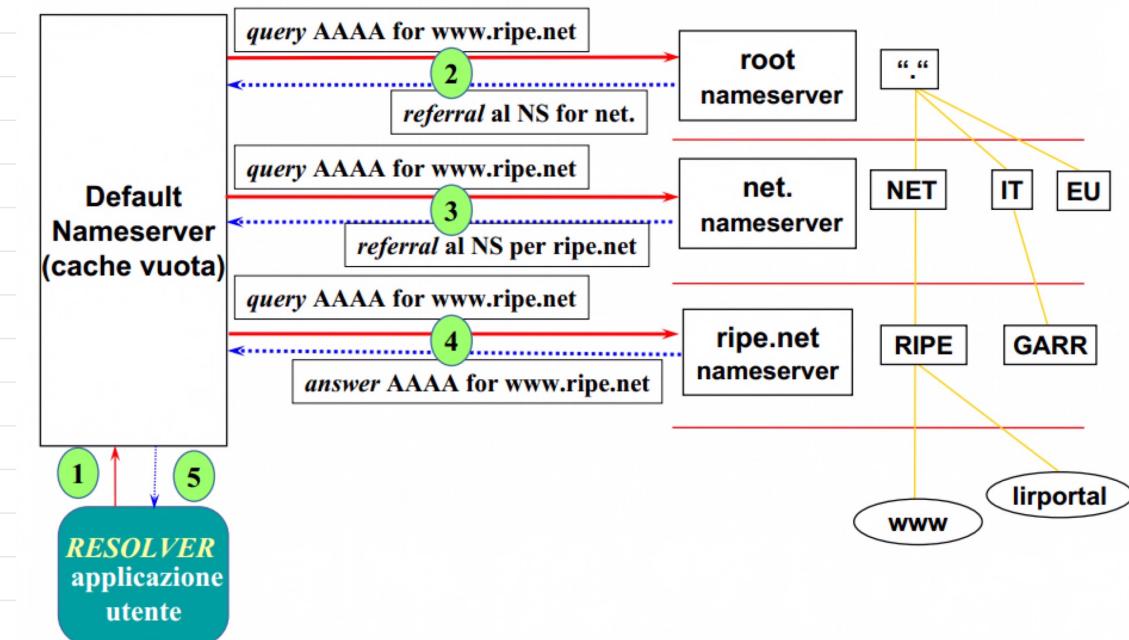
Nuovo RR AAAA

Nuovo dom. per ris. inversa

o Nomespace IPv4 e IPv6:



o Processo iterativo per risoluzione dei nomi:



12/12/2019

Reti di Calcolatori: dns e email

page 23

o Protocollo telnet:

Protocollo storico TCP/IP per accesso remoto alla console testuale di un host
Porta 23/TCP

Client: legge lo stream e lo gira al server. Lo stream del server è stocastico.
Server: legge le linee del client e le interpreta come comandi e invia al client l'output.

NB: è un protocollo testuale, basato su ASCII → sicurezza molto bassa

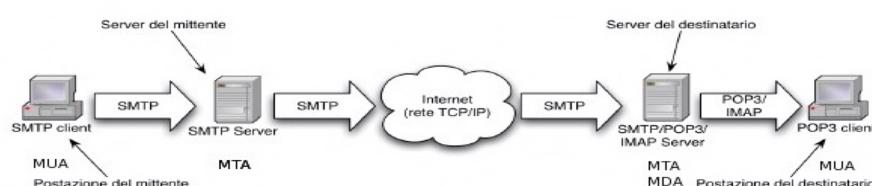
o Posta elettronica:

Indirizzo costituito da identificativo utente @ server → IP o ID DNS

MUA → Message user agent → ogni client ne ha bisogno → consente invio/ricezione posta.

MUA consegna → MTA → trasporta a destinazione.
↓
message transfer agent

Il 1° MUA è detto anche Submission Server. dovrebbe supportare SMTP AUTH.
Sull'ultimo MUA c'è presente l'MDA che consegna alla mailbox
(message delivery agent)



o Formato messaggi:

- Intestazione (header)
<cr><lf> (riga vuota)
- corpo (body)

Intestazioni: - To: - Cc: - Bcc:
- From: - received: - Date: - Subject:
- message ID: - useragent:

o Formato mailbox:

2 formati principali

Mbox, messaggi accodati in un singolo file x utente

Maildir: directory per ogni utente

o MIME: multi purpose internet mail extension

All'inizio la mail era pensata per trasportare solo testo (nessuno caratteri accentati)

introduce 5 nuove intestazioni:

- 1) MIME Version
- 2) Content-description
- 3) Content-id
- 4) Content-transfer-encoding
- 5) Content-type

o SMTP:

Protocollo applicativo (25/TCP) che si occupa del trasferimento di un messaggio da MUA a MTA
↳ codificato ASCII standard

o MTA a MTA.

Principali comandi del client SMTP:

- ▶ HELO: indirizzi dei destinatari
- ▶ MAIL FROM: mittente del messaggio
- ▶ RCPT TO: destinatario del messaggio
- ▶ DATA: corpo del messaggio
- ▶ QUIT: fine del messaggio
- ▶ RSET: reset
- ▶ HELP: nome del comando

Principali risposte del server SMTP:

- ▶ 220: Servizio pronto
- ▶ 250: Comando richiesto completato
- ▶ 251: Utente non locale, il messaggio sarà inoltrato
- ▶ 221: Chiusura canale di trasmissione
- ▶ 421: Servizio non disponibile
- ▶ 500: Errore di sintassi
- ▶ 501: Errore di sintassi nei parametri
- ▶ 554: Transazione fallita

o MUA: utile per inviare e ricevere posta

mail → MUA base linux, non gestisce MIME
elaine → MUA testuale gestisce schermi supporto MIME

o ESMTP (extended SMTP):

Esempio per gestire estensioni presenti e future.

Le estensioni più interessanti sono AUTH e STARTTLS che introducono autenticazione e cifrature

o SMTP-AUTH:

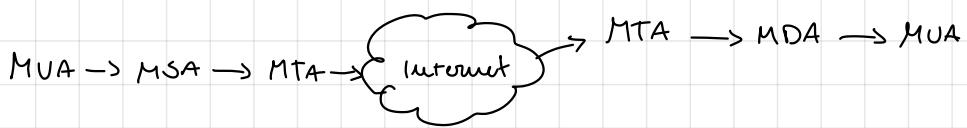
Visto che SMTP non prevede AUTH, chiunque può controllare un MTA per spacciare.

Per questo gli MTA vogliono mittente e destinatario (spesso) locali.

Per questo si usano server ESMTP con cui si possono eseguire login e crittografia.

ESMTP → SMTP AUTH → MTA dedicato (MSA)
message submission agent

Con l'avvento del PC il MUA si è separato dal MDA ed è nata la necessità di nuovi protocolli per MUA-MDA.
Nascono POP3 e IMAP.



- POP3: tipicamente usato da home users → modem o ADSL all'ISP

Protocollo ASCII con autenticazione per transfer messaggi da mailbox a MUA con TCP/110
Connessione → 3 fasi → autenticazione → transazione → aggiornamento
credenziali esecuzione QUIT, eliminazione

- IMAP: alternativo al POP3, consente a user agent la gestione dei msg ricevuti
usando TCP/143

A differenza di POP3 presume che i messaggi debbano rimanere sul server.

5B - World Wide Web

- WWW: Architettura client/server per consultazione di rete documenti multimediali e ipertestuali distribuiti in rete.
- Sviluppo gestito da w3c
- HTML: formato con cui vengono descritti gli ipertestuali
- HTTP: protocollo primario comunicazione client/server
- URL: indirizzo univoco internet

Documenti:
dinamici: generati al momento
statici: presenti sul drive

URL: Uniform Resource Locator, 4 parti: scheme://nameserver:port/nomeLocale

- Scheme: protocollo per raggiungere il documento
- Name Server: nome DNS del server
- port: porta di ascolto server
- Nome Locale: identificatore documento

altri scheme: ftp, file, obect

o tipi MIME: oltre ad HTML il www supporta altri formati (sempre in documenti)

Per alcuni formati il browser contiene l'interprete, per altri si oppone a un programma esterno o plug-in: estensione del browser o helper: programma separato.

o Web browser: prevalentemente grafici, ma anche testuali.

Dispongono di una cache su disco per documenti visualizzati recentemente.

Sequenza operazioni: input URL → verifica doc in cache → risoluzione DNS / IP → invio richiesta al server → ricezione doc dal server → parsing doc → eventuale richiesta doc collegati → → visualizzazione doc → rilascio connessione

o Web Server:

programma che fornisce su richiesta sue pagine WWW. Es: Apache e Tomcat

Seq. operazioni: accetta connessione TCP da client → determina percorso da URL → → accede al doc su disco → invia al client intestazione → rilascio connessione.

Funzioni avanzate:

Se sotto posti a grande carico, per migliorare le performance ci sono 2 modi:

- 1) Lettura da disco lento: sistema caching
- 2) server multithread: richieste gestite da front-end che invia la richiesta a un modulo di elaborazione libero (thread) e torna in ascolto.

• Web Caching:

Significa memorizzare temporaneamente le pagine in un punto più vicino al client per velocizzare la visualizzazione e ridurre il carico del server.

- i browser operano automaticamente caching sul disco
- una LAN può organizzare un servizio di caching × gli utenti della lan → proxy

• Content delivery Network (CDN):

Per contenuti che vanno distribuiti su scale globali, 2 approcci: → web caching
→ CDN

Con il CDN c'è il provider che distribuisce copie dei contenuti in un insieme di nodi in differenti posizioni e redirige i client di modo da usare in modo a lui vicino.

CDN:
- DNS redirection: nome server delle CDN gestite con stessa.
- routing anycast: mirror server hanno stessi indirizzi anycast e trovare il server più vicino è demandato al routing unicast.

- expiration: alcuni documenti HTML possono contenere questa opzione, indica il tempo di validità per cui rimane in cache.

Altri doc usano "no-cache" per impedire che venga solvuto direttamente.

• HTML:

linguaggio markup → contiene formattazione.

testo formattato e risorse esterne
definito entro tag grassetto
↓ elenchi

NB: XHTML importa alcune props del XML dentro ad HTML.

descrivono il contenuto indipendente dalla sua presentazione finale
→ altri tag definiscono come deve apparire al lettore

Separati in 2 aspetti → style sheet in CSS

• Protocollo HTTP:

Protocollo testuale (ASCII) su TCP/80 → deve trasportare un msg di richiesta dal client al server e un msg di risposta dal server al client con il doc. richiesto.

↓
header, CR+LF, body

richieste HTTP: GET: richiede tutte le info disp.

HEAD: richiede solo header senza risorsa

POST: invia al server molte info

- OPTIONS: richiede elenco metodi
- TRACE: traccia una richiesta
- DELETE: cancella un file del server
- PUT: carica un file sul server

• Marcatura di stato e cookie:

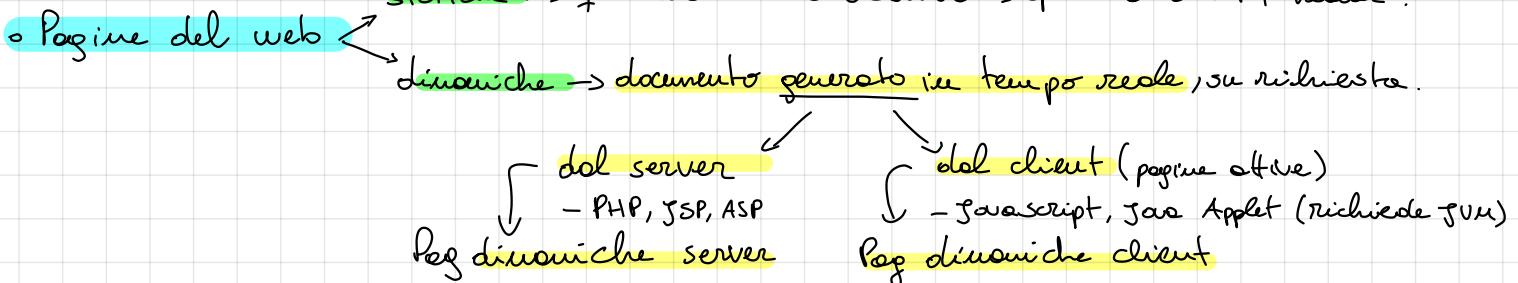
- Web privo di stato: ogni richiesta al server è indipendente, non ricorda i contatti precedenti.
 - in quei casi sarebbe utile avere memoria → vengono introdotti i cookie
- { generati dal server e scritti assieme al documento
browser li memorizza in opportuna directory}

- Contenuto cookie:
 - expire: (avvio)
 - dominio e percorso: ambito visibilità cookie
 - Secure: critto con HTTPS o no
 - contenuto: è variabile

Come funzionano?

- server invia i cookie al client inserendoli nell'header.
- client memorizza cookies ricevuti
- la prossima volta a visitare, browser cerca cookies appartenenti a quella pagina

statiche → files sul disco del server → spediti al client + header.



• Pagine dinamiche con CGI:

Il protocollo Common Gateway Interface consente di mettere in esecuzione un programma eseguibile sul server e redirigere lo std-out del programma al client → interpreta come normale risposta HTTP.

L'esecuzione di una pag. dinamica deve dare la possibilità di passare param. o dati all'eseguibile:
 GET → codifica parametri nell'URL → la query è preceduta da "?"
 POST → usa la parte body della richiesta → inserisce i dati nel body e escono in std-out

Vantaggio del Post: non parametri in URL e possibile trasformare anche dati oltre ai param.
 param e dati vengono codificati dalle FORM in una unica stringa.
 → è compito del programma fare parsing delle stringhe × decodificare

5C - Multimedie:

o Audio analogico e digitale:

Conversione analogico digitale \rightarrow freq. campionamento determinate da Nyquist:
 $f_{coup} = 2 \times f_{max} \text{ segnale}$

Quantizzazione: numero discreto di val possibili per le letture nel campionamento.

o Compressione audio:

transmissione internet \rightarrow compressione necessaria \rightarrow 2 modi:

- conversione per forma d'onda: segnale convertito nelle sue componenti nel dominio delle freq. \rightarrow Fourier
usa la minima quantità di bit possibile
- conversione percettiva: binhi acustici umani \rightarrow codifica il segnale in modo che sembri lo stesso ad un ascoltatore umano, pur differendo dall'originale.

o Video analogico:

monocromatico: telecamera spezzola l'immagine con un fascio di elettroni orizzontalmente. Finito, next frame.

Può essere $\begin{cases} \nearrow \\ \searrow \end{cases}$ a colori: come sopra ma 3 fasci all'insieme per visualizzare l'immagine

Metodi:

NTSC

PAL / SECAM

HDTV

o Video digitale: è semplicemente una sequenza di fotogrammi. Fluidità $\rightarrow \geq 25 \text{ FPS}$

Al posto delle linee di scorrimento ci sono i pixel

200 mbps per 640x480 con 24 bit per pixel

- la compressione è necessaria per upload su internet.
- servono anche 2 alg: codifica e decodifica. \rightarrow può non essere reversibile e costo di una piccola perdita, si ottiene compres. elevata

o JPEG:

Video = seq. foto + audio sincronizzati su canale comune a 90 kHz

compresso jpeg \rightarrow immagini statiche o forti continui

1) preparazione blocco $\rightarrow \rightarrow$ si applica DCT \rightarrow 3) quantizzazione

Quantizzazione differentiale: per ogni blocco (0,0) \rightarrow cambiato con le quantità di cui differisce dal blocco precedente.

Linearizzazione dei 64 elem. e codifica run-length

Codifica Huffman: codici più brevi a numeri più frequenti

MPEG-1, -2:

MPEG-1 ancora molto usato. Composto da

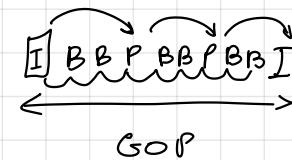
{
 } sync 90kHz
 } video
 } multiplexer

ridondanza → temporale: JPEG per ogni fotogramma
→ spaziale: vantaggio dei fotogrammi simili

Output MPEG-1:

- i-frame (intracodificati) → imm. statiche JPEG
- P-frame (predittivi) → imm. dipende dal frame prec.
- B-frame (bidirezionali) → dipende dal prec. e succ.

MPEG2 → per HDTV



Dati multimediali in rete:

Per streaming, real time, conference → fattori importanti

) throughput
 } jitter
 } Buffer
 } protocoli → linko
 } servizi

Streaming con RTSP e RTP (Musica)

file collegato al titolo è un metafile che rimanda
al file vero, dove poi il browser non fa più nulla.

Per gestire play/pause etc → RTSP real time streaming prot.

Per flusso dati: RTP o HTTP

real time transport prot.

RTP:

UDP multicast/unicast

○ VoIP

RTP/UDP con buffer piccoli → < latenza
necessaria

Sip protocol e H323

Guarda slide.

fuck this shit i'm out

