Reti di computer e protocolli

CLIENT-SERVER — PEER TO PEER

possono essere modelli di comunicazione basati su architetture

RETI DI COMPUTER

- CONSENTONO DI INSTRADARE DATI ATTRAVERSO LA COMMUTAZIONE
  - PUÒ ESSERE:
    - DI CIRCUITO
    - DI PACCHETTO
    - DI MESSAGGIO
- GARANTISCONO COMUNICAZIONI AFFIDABILI GENERALE ALL'USO DI PROTOCOLLI
  - INCLUDONO: TCP, IP
- POSSONO ESSERE CLASSIFICATE PER
  - ESTENSIONE GEOGRAFICA
    - BAN
    - PAN
    - LAN
    - MAN
    - WAN
    - GAN
    - CAN
  - TOPOLOGIA
    - A BUS
    - AD ANELLO
    - A STELLA
    - A MAGLIA
    - AD ALBERO

Una rete di computer è un insieme di dispositivi, collegati l'uno con l'altro da appositi canali di comunicazione (LINK), che per mezzo di opportuni protocolli di comunicazione hanno la possibilità di condividere risorse che possono essere materiali (DISP. FISICI es. STAMPANTE), o immateriali (COME DATI, INFORMAZIONI).

La rete fornisce un servizio di trasferimento dati, attraverso comuni funzionalità di trasmissione e ricezione, ad una popolazione di utenti distribuiti su un'area più o meno grande.

Esempi di rete informatica sono le reti BAN, PAN, LAN, MAN, WAN, GAN, CAN, la cui interconnessione globale da vita alla rete INTERNET. Le reti di computer generano traffico di tipo fortemente impulsivo ovvero pacchettizzato e asincrono, a differenza della rete telefonica sincrona, e per questo hanno dato origine e usano la tecnologia della commutazione di pacchetto, piuttosto che la commutazione di circuito come per le linee telefoniche tradizionali.

Di seguito sono riportati i principali componenti di una rete:

- HOST: dispositivo terminale di rete (COMPUTER, SMARTPHONE SERVER);
- NODO DI COMMUTAZIONE: dispositivi interni alla rete che gestiscono il traffico (ROUTER, SWITCH);
- CANALE (LINK) o COLLEGAMENTO TRA NODI O TRA HOST E NODI
- INTERFACCIA O SCHEDA DI RETE SUGLI HOST O SUI NODI CHE PERMETTONO LORO DI COMUNICARE.

Quando si parla di messaggi che vengono spediti nella rete si fa riferimento a:

- PACCHETTO vengono raggruppati in pacchetti con formati definiti dai vari

protocolli di comunicazione;

LVL 2 : FRAME

3 : PACCHETTO (packet)

4 : SEGMENTO (in TCP) o DATAGRAMMA (in UDP)

- INTESTAZIONE (header): Ogni pacchetto è diviso in 2 parti la prima è l'INTESTAZIONE o header, è la parte dove sono inserite le informazioni riguardanti il pacchetto come INDIRIZZI DI DESTINAZIONE E PROVENIENZA;

- PAYLOAD: è la parte del pacchetto che contiene i dati.

CLASSIFICAZIONE DELLE RETI IN BASE ALL'ESTENSIONE GEOGRAFICA

- BAN (body area network) o RETE CORPOREA, è la rete che permette la connessione intorno al corpo di dispositivi indossabili, nel raggio massimo di 1m;

- PAN (personal area network) o RETE PERSONALE, è la rete che connette più dispositivi nel raggio di qualche metro (hotspot, airdrop);

- LAN (local area network) o RETE LOCALE, è la rete che si estende per qualche decina massimo centinaia di metri;

- MAN (metropolitan area network) o RETE METROPOLITANA, è la rete che solitamente ricopre un' intera città;

- WAN (wide area network) o RETE GEOGRAFICA, è una rete molto estesa che può comprendere più MAN;

- GAN (global area network) o RETE GLOBALE, è una rete che tende a connettere elaboratori dislocati in tutto il mondo favorendo anche la comunicazione con l'uso di satelliti.

- CAN (campus area network) o RETE UNIVERSITARIA (un insieme di edifici adiacenti)

CLASSIFICAZIONE DELLE RETI IN BASE ALLA TECNOLOGIA TRASMISSIVA

Le reti si dividono in broadcast e punto a punto. Nelle reti broadcast tutti gli host condividono lo stesso canale, cioè quando uno trasmette il messaggio arriva a tutti e in base all' indirizzo solo il destinatario lo elabora; si dividono in:

- UNICAST (UNO A UNO)
- MULTICAST (UNO A MOLTI)
- BROADCAST (UNO A TUTTI)

Nelle reti punto a punto invece gli host sono collegati a coppie e i messaggi passano attraverso più nodi per raggiungere la destinazione
La scelta del percorso viene gestita dagli algoritmi di routing, indispensabili per garantire il corretto instradamento

CLASSIFICAZIONE DELLE RETI IN BASE AL CANALE TRASMISSIVO

Le reti possono essere classificate in base al tipo di canale trasmissivo in due grandi categorie: CABLATE e WIRELESS.

Le prime usano cavi fisici: i cavi di RAME (ethernet) che trasmettono segnali elettrici ma sono sensibili a interferenze e non superano i 100m, mentre la fibra ottica garantisce velocità molto più elevate e copre distanze anche fino a 1km, sfrutta impulsi luminosi.

Le reti wireless trasmettono onde radio con antenne e comprendono tecnologie come wi-fi, bluetooth, reti cellulare e satellitari. Le frequenze basse offrono una copertura ampia ma velocità minori, mentre quelle alte consentono trasmissioni più veloci ma sono ostacolate facilmente da edifici o alberi (come accade con il 5G)

CLASSIFICAZIONE IN BASE ALLA TOPOLOGIA DI RETE

La topologia di rete è il modello che rappresenta come i nodi (elementi di rete) sono collegati tra loro.

Ogni topologia ha svantaggi e vantaggi valutati in base a: il costo dell'infrastruttura, alla complessità di gestione, alla tolleranze dei guasti, alla scalabilità.
Le principali topologie di rete sono:

TOPOLOGIA AD ANELLO:

- I nodi sono collegati in un cerchio
- Ogni informazione percorre l'anello passando da tutti i nodi.
- Lo svantaggio è che un guasto rompe l'intera rete → BASSA EFFICIENZA
- I vantaggi sono che è economica e semplice
- Ad oggi poco usata

TOPOLOGIA A STELLA:

- Tutti i nodi sono collegati ad un nodo centrale
- Vantaggi: facile da gestire, scalabile, aggiungere nodi è semplice e riduce le collisioni.
- Svantaggi: il nodo centrale è un punto critico, se si guasta cade tutta la rete,
- Molto usata nelle reti LAN moderne.

TOPOLOGIA A BUS:

- Tutti i nodi condividono un unico canale di comunicazione.
- Vantaggi: economica ed efficiente in reti piccole

+

- Svantaggi: un guasto al bus ferma tutta la rete
- Questa rete è stata in gran parte sostituita dalla topologia a stella.

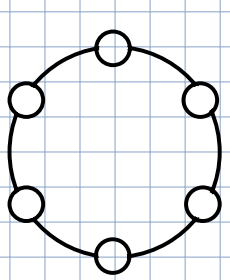
TOPOLOGIA A MAGLIA:

- Ogni nodo è collegato con tutti (MAGLIA COMPLETA) o con alcuni (MAGLIA PARZIALE)
- Vantaggi: alta tollerabilità a guasti, nessun problema di commutazione
- Svantaggi: costi troppo elevati e troppi collegamenti richiesti.
- Usata soprattutto a livello di dorsali internet.

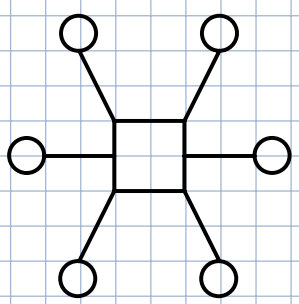
TOPOLOGIA AD ALBERO:

- Struttura gerarchica con un nodo RADICE e nodi PADRE - FIGLIO
- Vantaggi: molto affidabile (se un nodo padre cade, solo la sua sottorete è isolata), elevata scalabilità
- Svantaggi: punto debole nei nodi PADRE
- Molto utilizzata nelle reti di grande dimensione

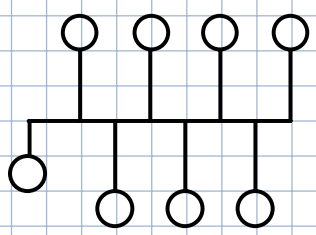
Ad anello



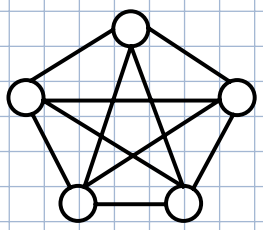
A stella



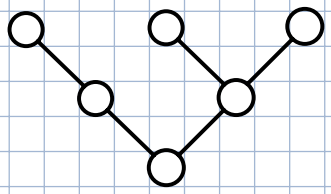
A bus



A maglia



Ad albero



MODALITÁ DI COMUNICAZIONE

Quando due host devono scambiarsi informazioni, la comunicazione può avvenire secondo diverse modalità, che si distinguono principalmente in base alla presenza o meno di una connessione preventiva tra emittente e destinatario:

- A CONNESSIONE (connection oriented): ha tre fasi APERTURA CONNESSIONE, TRASFERIMENTO DATI, CHIUSURA CONNESSIONE (es. telefonata). É sincrona perché mittente e destinatario agiscono nello stesso momento.

- SENZA CONNESSIONE (connectionless): i dati vengono inviati senza stabilire una connessione. Il mittente non sa se e quando il destinatario riceverà (es. mail). É asincrona perché non avviene in tempo reale.

MODALITÁ DI UTILIZZO DEL CANALE

Un aspetto importante della comunicazione riguarda il modo in cui viene utilizzato il canale trasmissivo, cioè esso consente la trasmissione dei dati in un solo verso, in entrambi ma alternati

oppure in contemporanea:

- SIMPLEX: trasmissione in un solo senso (es. RADIO);
- HALF-DUPLEX: trasmissione in entrambi i sensi ma non contemporaneamente (es. WALKIE-TALKIE)
- FULL-DUPLEX: trasmissione in entrambi i sensi contemporaneamente (es. TELEFONATA)

TECNICHE DI MULTIPLAZIONE DEL CANALE

Per ottimizzare l'uso delle risorse e permettere a più dispositivi di condividere lo stesso canale di comunicazione, si utilizzano tecniche di MULTIPLAZIONE, che possono essere statiche o dinamiche a seconda di come viene suddiviso il canale. La multiplazione serve per far usare lo stesso canale di comunicazione a più dispositivi.

- MULTIPLAZIONE STATICA: il canale è diviso in modo fisso e non cambia (es. TV, dove ogni canale ha la stessa frequenza)
- MULTIPLAZIONE DINAMICA: il canale è diviso solo quando serve e cambia in base all'uso, può funzionare in due modi:
  - PREASSEGNAZIONE: il canale viene dato a un dispositivo

per tutto il tempo dell'attività (es. TELEFONATA, quando chiami qualcuno ti viene dedicata una linea finché non chiudi la chiamata)

- ASSEGNAZIONE A DOMANDA: il canale viene dato solo quando serve, così tutti hanno la possibilità di usarlo e non si sprecano risorse (es. INTERNET (reti a pacchetto TCP, IP) i dati viaggiano in pacchetti che usano la rete solo quando devono trasmettere / wi-fi tutti i dispositivi condividono la stessa frequenza ma trasmettono solo quando hanno altri dati)

MODALITÁ DI ACCESSO AL CANALE

Servono a gestire l'uso di un canale di comunicazione in reti broadcast (più host dello stesso canale evitando collisioni e sprechi. Le modalità possono essere di 2 tipi principali:

- ACCESSO CENTRALIZZATO: in questo caso c'é un dispositivo specializzato chiamato MULTIPLEXER (MUX), che decide CHI può comunicare e QUANDO. É come un semaforo che regola il traffico: gli host NON scelgono da soli, ma seguono le indicazioni del MUX, l'assegnazione può essere fatta in modo STATICO (parti fisse sempre uguali) o DINAMICO (in base alle necessità del momento)

- ACCESSO DISTRIBUITO (o multiplo): qui invece NON c'è un controllore centrale, sono gli host stessi che decidono quando comunicare, ma devono seguire delle regole comuni per non ostacolarsi a vicenda. Le tecniche possono essere di 2 tipi:

1. DETERMINISTICHE (SENZA CONTESA):
   L'accesso al canale avviene in modo ORDINATO e PREVEDIBILE con:
   I → TDMA (TIME DIVISION MULTIPLE ACCESS):
   ad ogni host viene assegnato un intervallo di tempo in cui trasmettere
   II → FDMA o WDMA (FREQUENCY/WAVELENGHT DIVISION MULTIPLE ACCESS):
   ad ogni host viene assegnata una frequenza diversa
   III → LA TECNICA DEL PASSAGGIO DEL TESTIMONE:
   un host alla volta ha il diritto di trasmettere, quando ha finito passa il TOKEN a un altro host.

   Nei primi due casi le risorse sono pre-assegnate, nel tempo l'host può rinunciare se non c'è nessun messaggio da trasmettere (MULTIPLAZIONE A DOMANDA)
2. CASUALI (CON CONTESA):
   Qui non c'è una pianificazione preventiva, TUTTI possono provare a trasmettere, ma si rischia che 2 host lo facciano insieme causando collisioni. per questo esistono protocolli che gestiscono la contesa:
   I → ALOHA: è il metodo più semplice, si trasmette e se c'è una collisione si trasmette dopo un po'

II → CSMA/CD (CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION): usato in ETHERNET funziona ASCOLTANDO il primo canale, cioè se libero si trasmette, se è occupato si aspetta, se avviene una collisione la trasmissione viene interrotta e ripresa dopo un tempo casuale crescente.

III → CDMA (CODE DIVISION MULTIPLE ACCESS): usato nelle reti mobili, permette a tutti gli host di trasmettere contemporaneamente distinguendo la comunicazione tramite codici diversi

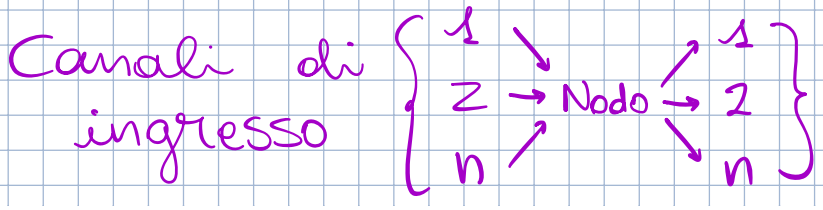
LE TECNICHE DI COMMUTAZIONE

In una rete la comunicazione tra host non direttamente collegati deve passare attraverso nodi intermedi, ogni nodo riceve informazioni e decide su quale canale mostrarle, questo processo si chiama COMMUTAZIONE (switch)

I tipi di commutazione sono:

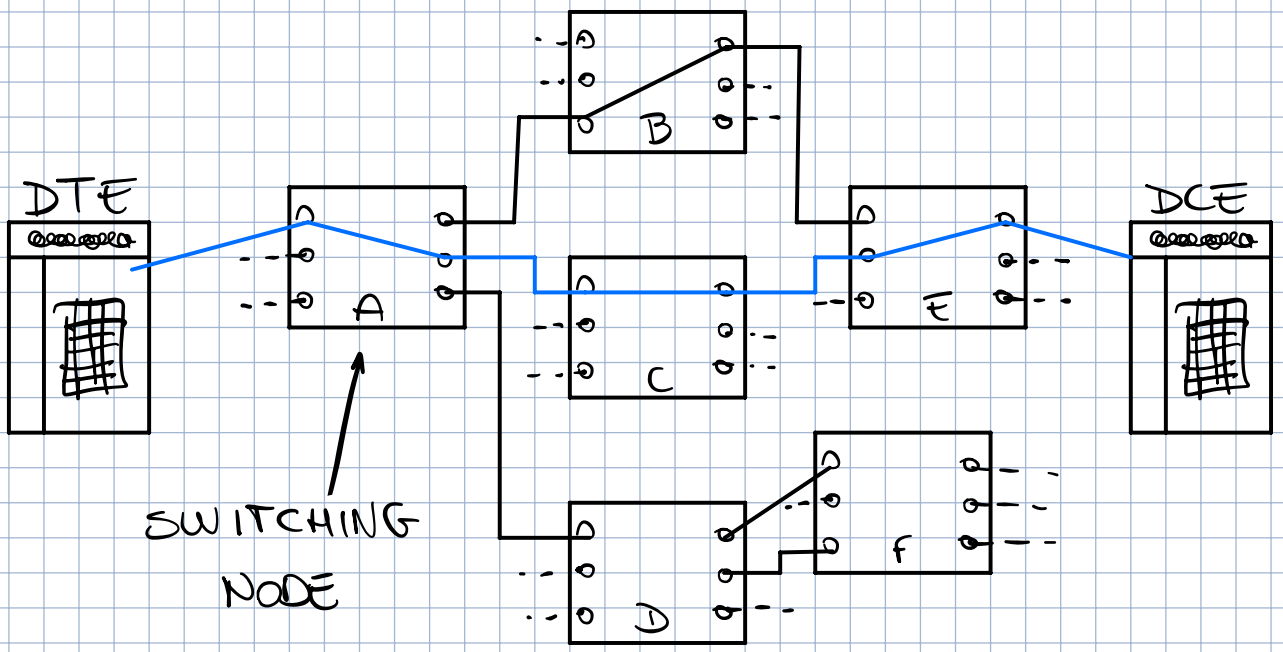
- DI CIRCUITO (circuit-switching)
- DI MESSAGGIO (message-switching)
- DI PACCHETTO (pack-switching)

es. quando mandiamo un messaggio su internet o facciamo una chiamata, la rete deve scegliere come far mandare i dati. A seconda del metodo di commutazione su un canale riservato (CIRCUITO) come blocchi interi (MESSAGGIO) o come pacchetti (INTERNET)



COMMUTAZIONE DI CIRCUITO

Caratteristica delle reti analogiche dove serve creare un canale fisico dedicato per tutta la durata della comunicazione
I nodi devono stabilire e mantenere il canale fino alla fine della trasmissione (vecchie reti telefoniche), solo al termine della comunicazione il canale può essere liberato. É una comunicazione connection-oriented cioè chiede una connessione stabile tra i due.
es. le vecchie reti telefoniche: quando si faceva una telefonata, il centralino creava un collegamento fisico tra i due telefoni, il canale restava occupato anche se nessuno parlava in quel momento.



DTE - Data terminal equipment
genera o utilizza dati

(COMPUTER, ROUTER LATO UTENTE)

DCE = Data circuit-terminating equipment
trasmette i dati attraverso la rete
(MODEM, ROUTER LATO RETE)

COMMUTAZIONE DI PACCHETTO

Usata nelle reti digitali.
Non richiede un canale dedicato.
I dati vengono suddivisi in pacchetti che possono viaggiare su percorsi diversi e vengono ricomposti dal destinatario.

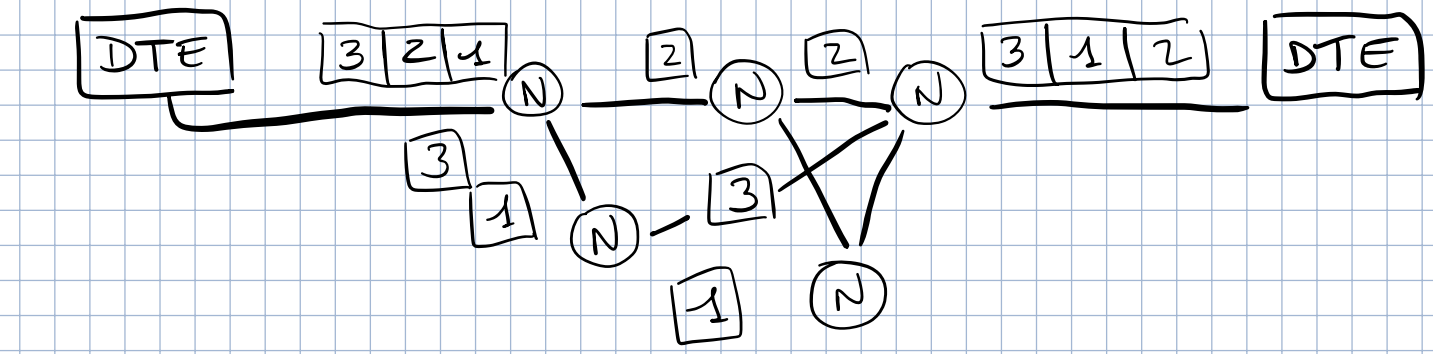
SVANTAGGI:

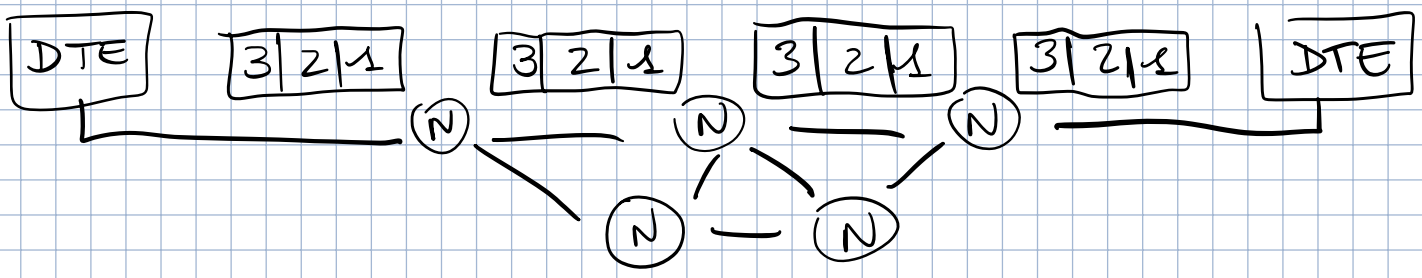
- Rispetto al circuito non garantisce una banda fissa, ma si possono aggiungere livelli di priorità per migliorare le prestazioni

Si distinguono due tipi:

- DATAGRAM: ogni pacchetto può eseguire percorsi diversi (INTERNET);
- CANALI VIRTUALI: tutti i pacchetti seguono lo stesso percorso formando un circuito virtuale esempio (ATM)

Quando invii una mail o un messaggio i dati vengono divisi in pacchetti che viaggiano su internet, alcuni vengono da Milano altri da Roma ma la destinazione è sempre la stessa e vengono ricomposti nell'ordine giusto.





ARCHITETTURA DELLA RETE INTERNET

Internet è una grande rete mondiale che unisce molte reti diverse: CABLATA, WIRELESS

La struttura non è unica ma si basa sulla topologia ad albero fortemente gerarchica.

Internet è gestita da diversi ISP (INTERNET SERVICE PROVIDER) che viene diviso in due punti:

- ISP di I LVL (Globali): gestiscono il nucleo principale della rete, sono internazionali e collegati tra loro.
- ISP II LVL (Nazionale): Collegano i provider globali con quelli locali
- ISP III LVL (Locale): Servono aree ristrette e collegano gli utenti finali.

Le topologie principali della rete internet sono:

- LIVELLO ALTO: magliate (collegamento tra ISP I LVL)
- LIVELLO INTERMEDIO: ad albero -> gerarchico.
- RETI LOCALI: vari tipi di topologia, ma strutturalmente collegate come foglie dell'albero principale.

INTERNET

Rete pubblica più estesa al mondo

Collega miliardi di dispositivi (HOST) permettendo di scambiare dati e informazioni digitali.

Principale forma di comunicazione di massa moderna

Tutti i dispositivi collegati possono comunicare tra loro indipendentemente dal sistema operativo.

CLIENT-SERVER

Modello più diffuso di funzionamento di internet

SI BASA SU 2 RUOLI

Client

L'utente chiede un servizio o risorsa

Server

Il computer fornisce quel servizio o risorsa.

Funzionamento:

1) Il client invia una richiesta (aprire pagina web)
2) Il server riceve la richiesta, la elabora e la invia.

Ogni server può elaborare diverse richieste contemporaneamente

ARCHITETTURA PEER - TO - PEER (P2P)

In una rete P2P tutti i computer sono sullo stesso livello, tutti possono essere CLIENT e SERVER
Si usa molto per condividere file, streaming, messaggi...
I vantaggi sono:

- MAGGIORE DISTRIBUZIONE DELLE RISORSE
- PIÙ AUTONOMIA DEI DISPOSITIVI
- NESSUN SERVER CENTRALE

Gli svantaggi sono:

- MAGGIORI PROBLEMI DI SICUREZZA
- DIFFICOLTÀ A GARANTIRE AFFIDABILITÀ E INTEGRITÀ DELLE INFO.

PROTOCOLLI DI COMUNICAZIONE

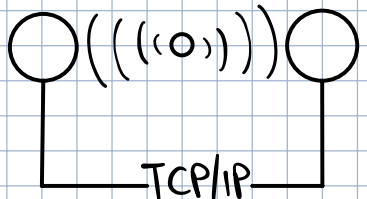
Un protocollo di comunicazione è un insieme di regole che stabiliscono come i dispositivi si scambiano i dati in modo sicuro e ordinato.

TCP
(Trasmission control protocol)
Garantisce che i dati arrivino completi nell'ordine giusto.

IP
(Internet protocol)
Si occupa di indirizzare i dati e di farli arrivare

Si occupa del controllo e della correzione degli errori.

al giusto destinatario



Formano la famiglia protocolli TCP/IP garantendo un'affidabile connessione a internet a tutti i dispositivi che ne fanno richiesta.

Indirizzi IP

Quando un dispositivo si connette a internet, alla sua scheda di rete viene assegnato un indirizzo IP, cioé un numero che lo identifica in modo univoco. Questo indirizzo non può essere utilizzato da altri dispositivi finchè è attivo

La configurazione automatica dell'indirizzo IP avviene attraverso il DHCP (dinamic host configuration protocol)

IPv4

La quarta versione dell'IP è composto da 32 bit (4 byte). Ogni byte può assumere valori da 0 a 255. Ed è scritto in 4 numeri divisi da punto: 103.60.7.24

L'IPv4 consente 4 miliardi di indirizzi ma oggi questo spazio è quasi esaurito, per questo è nato l'IPv6 che usa 128 permettendo numerosissime combinazioni.

IPv6

Gli IPv6 si scrivono con 8 gruppi di 4 cifre esadecimali separate da due punti.

Il DHCP è il protocollo che assegna automaticamente gli indirizzi IP collegati alla rete

In pratica:

- quando un dispositivo si connette alla rete invia una richiesta DHCP
- il server DHCP risponde assegnando un' indirizzo IP libero e altre informazioni necessarie.
- L'indirizzo viene concesso temporaneamente (lease) quando scade questa richiesta si libera l' indirizzo IP

IP STATICO

Gli IP statici restano sempre uguali, vengono assegnati a server o stampanti. → sempre raggiungibili

IP DINAMICO

Gli IP dinamici invece cambiano ogni volta che il dispositivo si connette (PC, SMARTPHONE)

GLI INDIRIZZI IP POSSONO ESSERE PUBBLICI O PRIVATI (ROUTER)

INDIRIZZO MAC E SCHEDE DI RETE

Ogni dispositivo ha una scheda di rete (NIC = network interface card) che lo collega fisicamente o via wi-fi alla rete. Questa scheda possiede un indirizzo MAC = media access control cioè una sorta di targa permanente formata da 12 caratteri in 6 coppie divisi da i due punti. 8A: 5F: 7B : 3C : 0A: 9E

É assegnato dal produttore e serve per riconoscere il dispositivo all'interno della rete locale.
A differenza dell'IP non può cambiare a meno che venga modificato manualmente. É utile per identificare dispositivi o configurare reti più sicuri (permettere di accedere alla rete solo ad alcuni MAC)

SUBNET MASK

Serve ad identificare l'indirizzo di rete di un host.

IPv4 address: 10.232.250.14 -> 00001010 . 11101000 . 11111010 . 00001110

Subnet mask: 255.255.255.0 -> 11111111 . 11111111 . 11111111 . 00000000

00001010 . 11101000 . 11111010 . 00001110

10	232	250	0
RETE	RETE	RETE	HOST

AND

A	B	A and B
0	0	0
0	1	0
1	0	0
1	1	1

Indirizzo IP e subnet mask vengono messi in AND e il confronto darà 1 soltanto se entrambi i bit valgono 1 (cioè sono veri).

La subnet divide l'indirizzo IP in due parti: la prima indica la rete, la seconda è dedicata all'host.

L'operatore booleano AND applicato tra IP e SUBNET restituisce l'indirizzo di rete e permette di capire se il dispositivo con cui si vuole comunicare appartiene o meno alla stessa rete

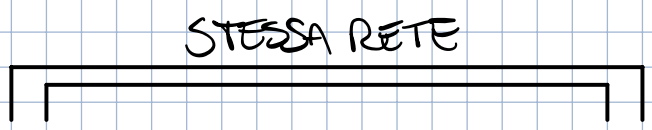
128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	= 10	1° OTTETTO
1	1	1	0	1	0	0	0	= 232	2° OTTETTO
1	1	1	1	1	0	1	0	= 250	3° OTTETTO
0	0	0	0	0	0	0	0	= 0	4° OTTETTO

l'indirizzo ip è stato progettato per far comunicare tra loro i dispositivi.
Un indirizzo ip è formato da 4 byte separati da un punto 10.232.250.14

00001010 11101000 11111010 00001110

1 byte : 8bit 4 byte : 32bit (0,1)

Per far comunicare due host della stessa rete bisogna avere un indirizzo ip univoco.



10.232.250.14 10.232.250.13

Per convertire rapidamente il formato decimale a quello binario basta affiancare a ciascuna sequenza di 8bit delle potenze di due sommando soltanto i valori dove il bit è settato a 1.

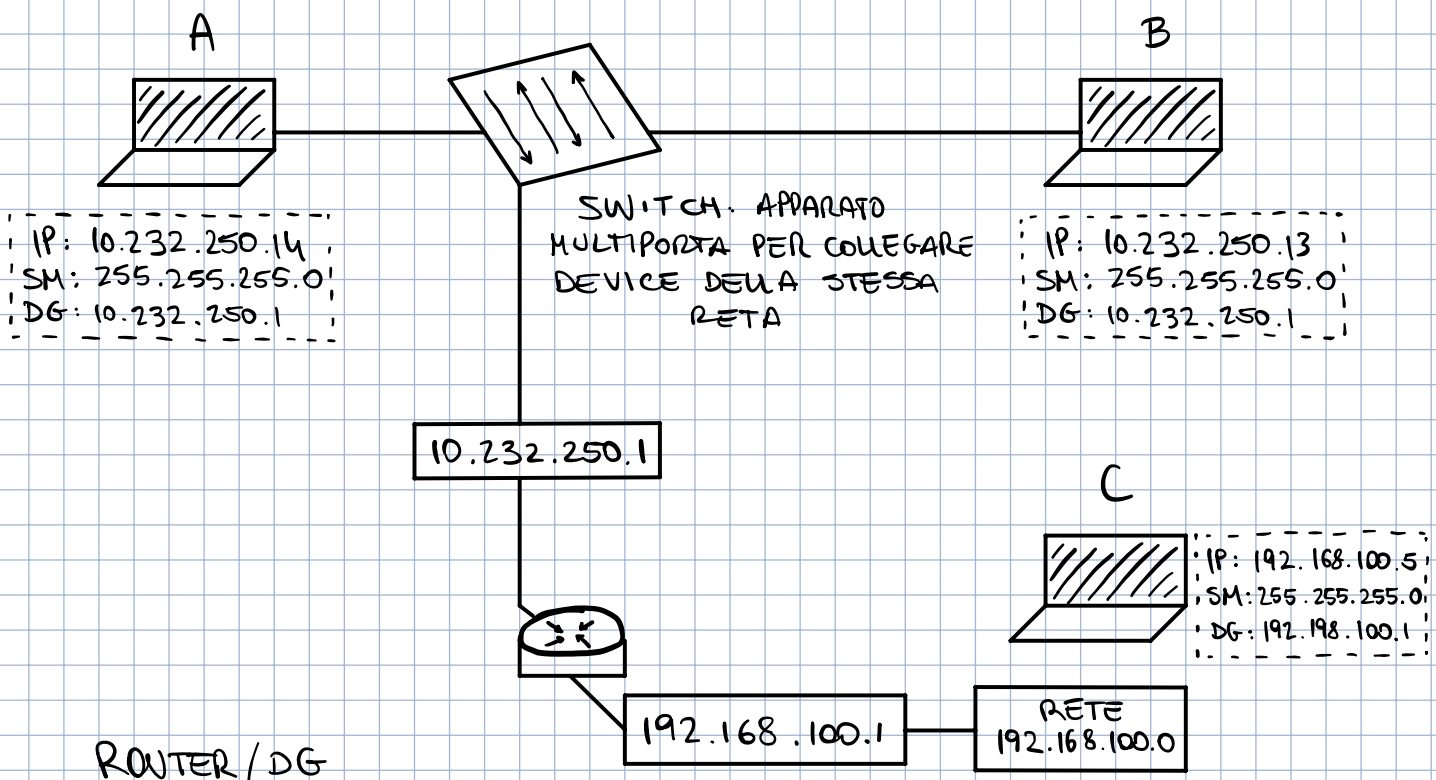
Altro elemento fondamentale della configurazione di rete di un host è il DEFAULT GATEWAY o ROUTER.

IPv4 Address: 10.232.250.14

Subnet mask (SM): 255.255.255.0

Default gateway (DG): 10.232.250.1

Il defaunt gateway è un device di rete multiporta, indispensabile per far comunicare dispositivi appartenenti a reti diversi.
Il router dispone di una tabella di routing in cui sono presenti gli indirizzi degli host di tutte le reti a cui è connesso.
Ogni porta del router ha un indirizzo IP della stessa rete degli host ad esso collegati, ogni host deve conoscere l'indirizzo del router.



ROUTER / DG

TABELLA DI ROUTING

HOST	INDIRIZZO IP	INDIRIZZO DI RETE
A	10.232.250.14	10.232.250.0
B	10.232.250.13	10.232.250.0
C	192.168.100.5	192.168.100.0

La configurazione di un dispositivo di rete si basa su 3 elementi base

PILA ISO-OSI

- APPLICAZIONE
- SESSIONE
- TRASPORTO

RETE COLLEGAMENTO

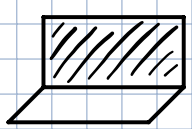
- FISICO

INDIRIZZO IP

MAC ADDRESS

AND

SUBNET MASK



INDIRIZZO IP

10.232.250.14

- indirizzo logico a 32 bit (RETE PILA ISO-OSI)
- identifica univocamente un pc in una rete

SUBNET MASK

255.255.255.0

- suddivide l'IP in 2 parti (RETE - HOST)

- con la messa in AND ci dà l'indirizzo di rete

MAC ADDRESS

F8-7A-A4-B3-F9-4C

- indirizzo fisico a 48 bit esadecimale
- identifica univocamente un pc nel mondo.

Ogni dispositivo in rete deve avere non soltanto l'indirizzo IP, ma anche la SUBNET-MASK per sapere il proprio indirizzo di rete.

Inizialmente gli indirizzi IPv4 vennero divisi in più classi sulla base della lunghezza della SUBNET-MASK, che era fissa per ciascuna rete.

8 bit per la rete | 24 bit per gli host

A 11111111 | 00000000 00000000 00000000 IP SM

16 bit rete | 16 bit host

B 11111111 11111111 | 00000000 00000000 IP SM

24 bit rete | 8 bit host

C 11111111 11111111 11111111 | 00000000 IP SM

D 224 - 239 IP

E 240 - 255 IP

Dalle classi si passa al CIDR (classes inter-domain routing) e SUBNET variabile

esempio: SUDDIVISIONE CLASSFUL

AZIENDA DI 500 DIPENDENTI $\xrightarrow[\text{BISOGNO DI}]{\text{HA}}$ 500 IP

LO IANA propone – UNA RETE CLASSE C (254 host; POCHI)
– UNA RETE CLASSE B (65'534 host; TROPPI)

Tranne che il CIDR viene concesso alla rete un indirizzo di rete con SUBNET MASK a 23 bit

130.170.100.0/23 NOTAZIONE CIDR
SUBNET MASK A 23 bit

IP	10000010	10101010	01100100	00000000
SM	11111111	11111111	11111110	00000000

9 bit per gli host; 510 indirizzi disponibili

Dopo il CIDR vengono introdotti gli indirizzi IPv4 privati e NAT (network address transmission) per garantire l'accesso (agli indirizzi privati) si utilizza il protocollo NAT.

CLASSI:

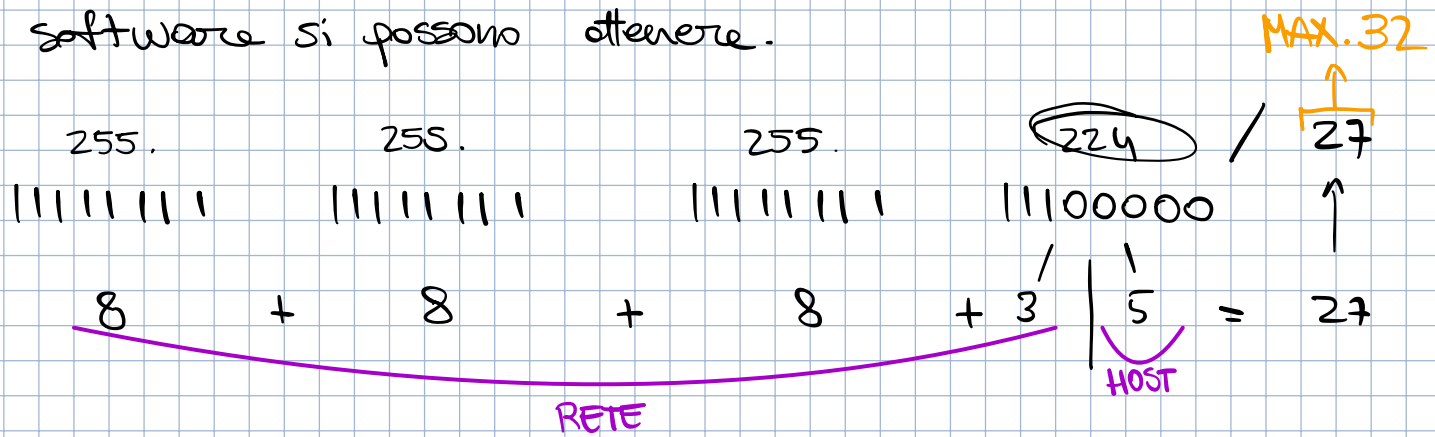
	DA	A	SM
1° FASCIA	10.0.0.0	10.255.255.255	8bit (/8 , 255.0.0.0)
2° FASCIA	172.16.0.0	172.16.0.0	12bit (/12, 255.240.0.0)
3° FASCIA	192.168.0.0	192.168.255.255	16bit (/16, 255.255.0.0)

DA	A
127.0.0.0	127.255.255.255
169.254.0.0	169.254.255.255
224.0.0.0	239.255.255.255

esempio:

Dato l'indirizzo IP: 200.110.112.0
con maschera di sottorete: 255.255.255.224

Specificare quante sottoreti e quanti host per software si possono ottenere.



/27 SM 3bit RETE = 2^3 8 SOTTORETE
5bit HOST = 2^5 32 SOTTORETE

HOST DISPONIBILI (5) $2^n - 2$ → $32 - 2 = 30$ HOST DISPONIBILI

INDIRIZZO DI RETE BROADCAST

Dato l'indirizzo IP: 200.110.12.0, partizionare la rete da esso individuata in 12 sottoreti specificando il numero di host che appartengono a ciascuna sottorete e individuare l'indirizzo IP del 3° host appartenente alla settima sottorete.

Classe: 3ª fascia

200. 110. 12. XXXXXXXX

255. 255. 255.

11111111 11111111 11111111

↓

$2^n - 2 =$

$2^4 - 2 = \boxed{14}$

Almeno 12 sottoreti utilizzabili.

200.110.12.0 1 $2^4 \cdot 0$

200.110.12.16 2 $2^4 \cdot 1$

200.110.12.32 3 $2^4 \cdot 2$

⋮ .48 4 $2^4 \cdot 3$

.64 5 $2^4 \cdot 4$

.80 6 $2^4 \cdot 5$

.96 7 $2^4 \cdot 6$

⋮

.240 16 $2^4 \cdot 15$

7° SOTTORETE: 200.110.12.96 (INDIRIZZO DI RETE) 11001000 01101110 00001100 01100000

.97 1°
.98 2°
.99 3° → TERZO HOST DELLA SETTIMA SOTTORETE
.100 4°
.101 5°
.102 6°
.103 7°
.104 8°
.105 9°
.106 10°
.107 11°
.108 12°
.109 13°
.110 14°
.111 (BROADCAST)

Dato l'indirizzo IP: 190.170.80.0 → 10 sottoreti con n° host
→ 4° host della 6° sottorete

190.170.80.0

255.255.255.XXXXXXXX

↓

$2^n - 2$ = almeno 10

$2^4 - 2 = 14$ ✓ n° host per ogni sottorete: 16

190.170.80.0 1
.16 2
.32 3
.48 4
.64 5
.80 6. → 190.170.80.80 (IND. DI RETE)
.96
.128

SM: 10111110.10101010.01010000.01010000 (7°)

.81 1
.82 2
.83 3
.84 4

.240

.85

.127

↘ BROADCAST

190.170.80.84

ALGORITMI e COMPLESSITÁ COMPUTAZIONALE

Un algoritmo è un insieme di passi finiti che serve a risolvere un problema.

Deve essere:

- CHIARO e NON AMBIGUO:
  Ogni passo deve essere comprensibile e definito con precisione
- FINITO:
  deve terminare con precisione dopo un numero finito di passaggi
- EFFICACIE:
  Ogni istruzione deve poter essere eseguita realmente e in tempo finito
- DETERMINISTICA:
  Ogni passo data una situazione deve avere una singola istruzione da compiere

Per confrontarli guardiamo alcuni parametri:

- TEMPO DI ESECUZIONE cioè quanti passi servono per arrivare alla soluzione
- SPAZIO DI MEMORIA cioè quanta memoria temporanea l'algoritmo ha bisogno di usare
- CORRETTEZZA deve dare sempre la soluzione giusta
- SEMPLICITÁ più l'algoritmo è semplice -> minore è la possibilità d'errore

Il parametro più import

Non possiamo misurarlo in secondi se un algoritmo ci impiega 2s in un computer e 0,2s su un computer più potente → vanno contati i passi base → le operazioni per risolverlo.
Le operazioni ha

IL CONSUMO DI RISORSE (tutto ciò che l'algoritmo usa mentre lavora)

IL TEMPO DI ESECUZIONE

Da questi due aspetti derivano complessità spaziale che va a misurare quante risorse fisiche utilizza e complessità temporale che misura quanto tempo impiega l'algoritmo per terminare.
Più dati l'algoritmo deve processare, più tempo ci impiega
Per questo si studia la complessità computazionale:
per trovare la relazione tra tempo di esecuzione e N (dati in ingresso)

COME SI CALCOLA LA COMPLESSITÀ COMPUTAZIONALE?

Si assegna un costo unitario a ogni operazione elementare dell'algoritmo (una somma una assegnazione di variabile un
Sommando tutti i costi di tutte le istruzioni che il nostro algoritmo deve compiere troveremo la complessità computazionale.
Ogni istruzione diversa avrà un costo differente, perché dal punto di vista dell'elaboratore sarà più semplice fare una somma che controllare una condizione, per semplicità per calcolare la C.C.

si da un costo fisso ad ogni istruzione.

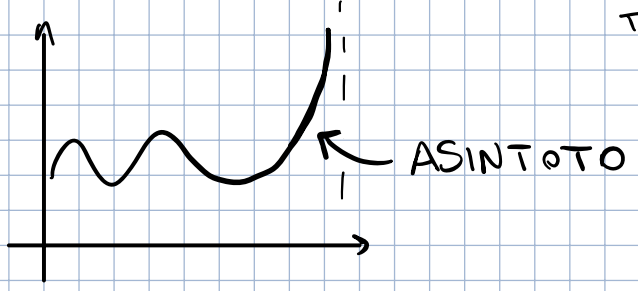
→ ogni istruzione eseguita dal nostro algoritmo ha costo 1, sommando tutti i costi avremo il costo complessivo.

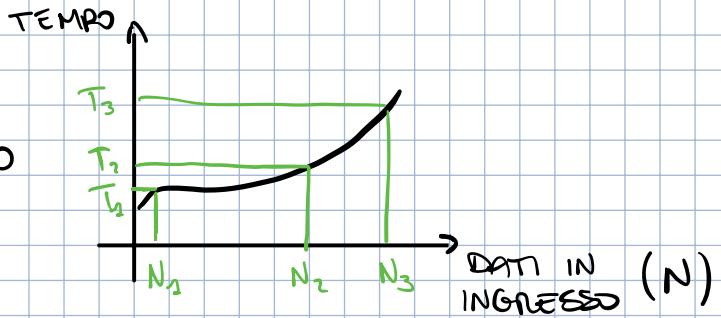
Ma dalla complessità del nostro algoritmo dipende la grandezza dei dati in ingresso quindi nella equazione finale ci saranno i costi di tutte le istruzione del nostro algoritmo quindi utilizziamo la variabile N, più questa variabile N sarà grande più i dati in ingresso saranno grandi e quindi il tempo di esecuzione aumenterà quindi bisogna creare una funzione dell' algoritmo in funzione di N

Ogni algoritmo è diverso e il nostro scopo è trovare quello più efficiente. lo scopo è capire quante operazioni servono per portare a termine l' algoritmo.

ANALISI ASINTOTICA

Un metodo per calcolare la C.C. è l'analisi asintotica. Un asintoto in matematica è quando una funzione tende all' infinito.
Consiste nel confrontare due funzioni e controllare il comportamento all' infinito cioè con N la grandezza dei dati ingresso nel nostro algoritmo tendente a infinito.





Per far ciò serve appunto una funzione quindi dobbiamo trasformare il costo del nostro algoritmo in un' equazione dei dati in ingresso.

$f(N)$ è una funzione che per ogni N quindi per ogni grandezza dei dati in ingresso ci restituisce un costo in termine di risorse usate dal nostro algoritmo.

MODELLO ISO / OSI

ISO = ente internazionale che ha standardizzato il modello ISO 7498.

OSI - descrive come i modelli comunicano tra loro.

Il modello ISO/OSI è uno schema a 7 livelli che descrive le funzioni necessarie per far comunicare 2 dispositivi in rete, dalla parte fisica alle applicazioni

SISTEMA DI RETE

↓

modello teorico che descrive le funzioni di un → rete di comunicazione end-to-end

MODELLO ISO/OSI

È COSTITUITO DA → sottorete di comunicazione

il flusso di dati subisce → IMBUSTAMENTO

prevede un'architettura → A LIVELLI

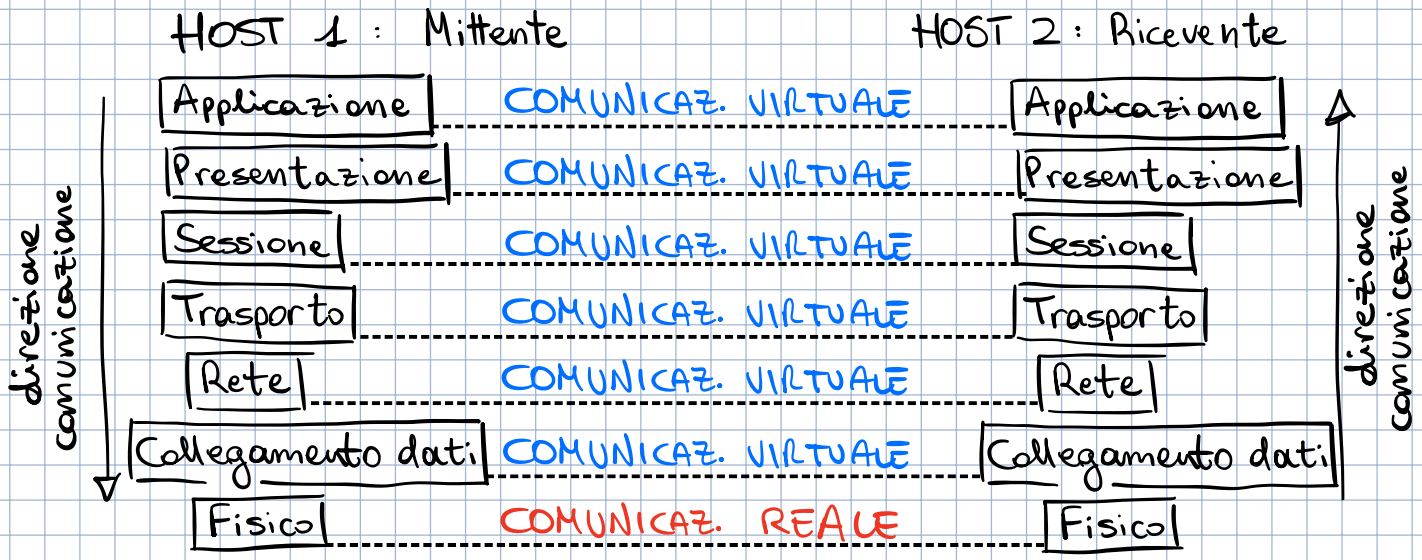
FORMATA DAI LIVELLI

3. rete
2. collegamenti dati
1. fisico

Obiettivi principali:

- STANDARDIZZAZIONE (tutti parlano la stessa lingua di rete)
- INTEROPERABILITÁ (dispositivi di marche diverse che possono comunicare)
- MODULARITÁ (ogni livello ha un compito separato, quindi facile da gestire)
- FLESSIBILITÁ (si possono aggiornare parti della rete senza rifare tutto)

La rappresentazione grafica del modello di comunicazione tra un host mittente e un host ricevente:



Nel modello ISO/OSI ogni livello di un computer (HOST MITTENTE) parla virtualmente con il livello corrispondente dell'altro computer (HOST RICEVENTE). Solo il livello fisico comunica davvero tramite cavi, onde ecc.

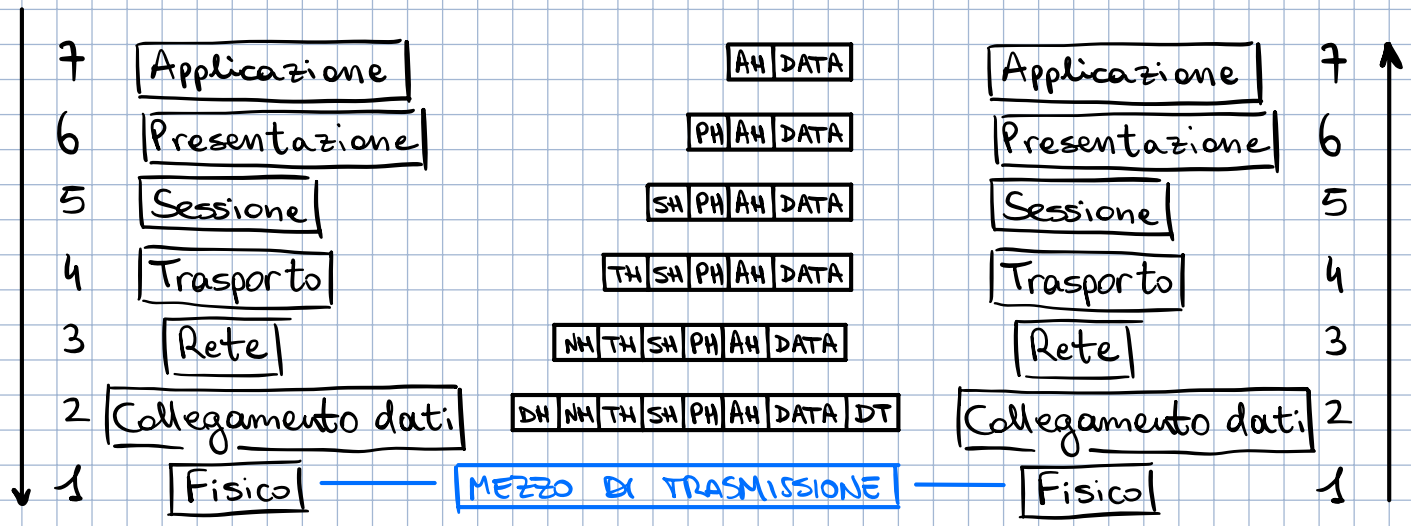
FUNZIONAMENTO:

1. Ogni livello non parla direttamente con il suo gemello nell'altro HOST
2. Parla solo con il livello nel proprio computer
3. Per far arrivare i dati al livello corrispondente dell'altro HOST, il messaggio scende tutti i livelli, viene trasmesso fisicamente e poi risale nell'altro HOST.

In un protocollo di comunicazione di un'architettura di rete a STRATI, l'unità di informazione scambiata tra due livelli corrispondenti

è chiamata PDU (protocol data unit).

Il PDU varia in funzione dello strato del modello che si analizza.



FUNZIONAMENTO DELL' INCAPSULAMENTO/IMBUSTAMENTO

Nel mittente:

1. Il messaggio parte dal livello 7 (APPLICAZIONE)
2. Scendendo verso il livello 1, ogni livello aggiunge la propria intestazione

AH: Application header
PH: Presentation header
SH: Session header
TH: Transport header
NH: Network header
DH: Data link header
DT: Data trailer (CONTROLLO INTEGRITÁ DI DATI TRASMESSI)

3. Il messaggio diventa sempre più imbustato
4. Al livello fisico 1 viene trasformato in bit e inviato sul mezzo fisico

Nel destinatario:

1. I bit arrivano al livello 1.
2. Risalendo i livelli, ogni strato rimuove la propria intestazione
3. Al livello 7 il destinatario riceve il messaggio originale

L'incapsulamento permette a ogni livello di lavorare indipendentemente.
Ogni livello aggiunge info utili alla comunicazione.

Livello 1:

livello fisico
è il livello che sta alla base di tutto, quello che si occupa di far viaggiare i bit, cioé 0 e 1 da un dispositivo all'altro.

Non interpreta i dati, non li controlla e non li capisce, il suo unico compito è trasportarli ~~sotto~~ forma di segnali.
Per farlo deve trasformare i bit in qualcosa che effettivamente può viaggiare ad esempio una tensione elettrica, un impulso luminoso o un'onda radio.
Per esempio in un cavo di rame un 1 può essere rappresentato da una tensione positiva mentre uno 0 da una tensione negativa; mentre in fibra ottica un 1 può essere rappresentato da un lampo di luce e uno 0 dall'assenza di luce.

Il livello fisico si occupa anche di stabilire come questi segnali devono essere inviati, quali valori di tensione usare, come modulare il segnale e come codificare i bit.

In ethernet ad esempio si usano tecniche come la codifica di Manchester che permettono di capire non solo se 0 o 1 ma anche quando inizia e quando finisce.

Altro compito fondamentale è la sincronizzazione, cioè trasmettitore e ricevitore devono essere d'accordo sul ritmo con cui i bit vengono inviati., altrimenti si rischia di leggere un bit nel momento sbagliato.

Il livello fisico definisce anche il mezzo di trasmissione che può essere un cavo di rame, una fibra ottica, un'onda radio, ogni mezzo però ha caratteristiche diverse e richiede regole diverse per comunicare.

Il livello fisico determina anche la topologia della rete.

Per far funzionare tutto questo esistono dei dispositivi che lavorano su questo livello. Il ripetitore ad esempio serve a rigenerare un segnale che si sta indebolendo

L'HUB prende un segnale e lo trasmette

a tutte le porte della porta.

Il modem converte i segnali digitali in analogici e viceversa.

I media converter permettono di collegare cavi diversi come la fibra e il rame.

La scheda di rete è ciò che permette al computer di collegarsi fisicamente alla rete.

Tutte queste tecnologie permettono di definire come dev'essere costruito il segnale, quali mezzi usare e quali regole fisiche seguire per far viaggiare i dati.

Livello 2: COLLEGAMENTO DATI

Il compito del secondo livello è garantire che i dati arrivino senza errori al destinatario, rendendo il livello fisico più sicuro per la trasmissione.

COSA FA:

1. Riceve i dati dal livello superiore (RETE) e li prepara per il livello fisico;
2. Suddivide i dati in frame cioè pacchetti strutturati sottoforma di header (CONTIENE INDIRIZZI MAC, TIPO DI PROTOCOLLO) e di un trailer (CONTIENE INFO PER IL CONTROLLO DEGLI ERRORI);
3. Controlla se ci sono errori nella trasmissione e se

necessario chiede la ritrasmissione

4. Gestisce il flusso di dati per evitare sovraccarichi.

Il PDU viene chiamato frame o meglio l'unità dati del livello collegamento, contiene i dati più informazioni di controllo.

FUNZIONI PRINCIPALI

Funzione	Spiegazione
• INDIRIZZAMENTO FISICO	• USA GLI INDIRIZZI MAC PER IDENTIFICARE I DISPOSITIVI
• ACCESSO AL MEZZO	• COORDINA L'USO DEL CANALE PER EVITARE COLLISIONE (es. CSMA/CD protocol)
• CONTROLLO DEGLI ERRORI	• RILEVA E SEGNALA ERRORI (es. PARITÀ / CRC)
• CONTROLLO DEL FLUSSO	• REGOLA LA VELOCITÀ DI TRASMISSIONE.

Il livello COLLEGAMENTO DATI è suddiviso in due sottolivelli:

- MAC (media access control)
- LLC (logical link control)

Questa suddivisione serve ad organizzare meglio i compiti. Cioè uno si occupa del controllo fisico del mezzo (MAC) mentre l'altro della gestione logica della comunicazione. questo per garantire che sia ordinata, affidabile e senza errori.

Il protocollo CSMA (carrier sense multiple access) CSMA/CD (carrier sense multiple access with collision detection) definisce una serie di tecniche per regolare

lo scambio di dati che condividono una rete, allo scopo di evitare che 2 o più host trasmettano contemporaneamente generando collisioni.

Il protocollo ascolta il canale prima di trasmettere, se il canale è occupato, aspetta e riprova secondo modalità di trasmissione predefinite.
Sono previste 3 varianti:

- CSMA persistente: trasmette appena il canale è libero.
- CSMA non-persistente: controlla se il canale è libero, se si trasmette, diversamente attende un intervallo casuale e ritrasmette.
- CSMA p-persistente: viene utilizzato in canali divisi per intervalli temporanei detti SLOTS.

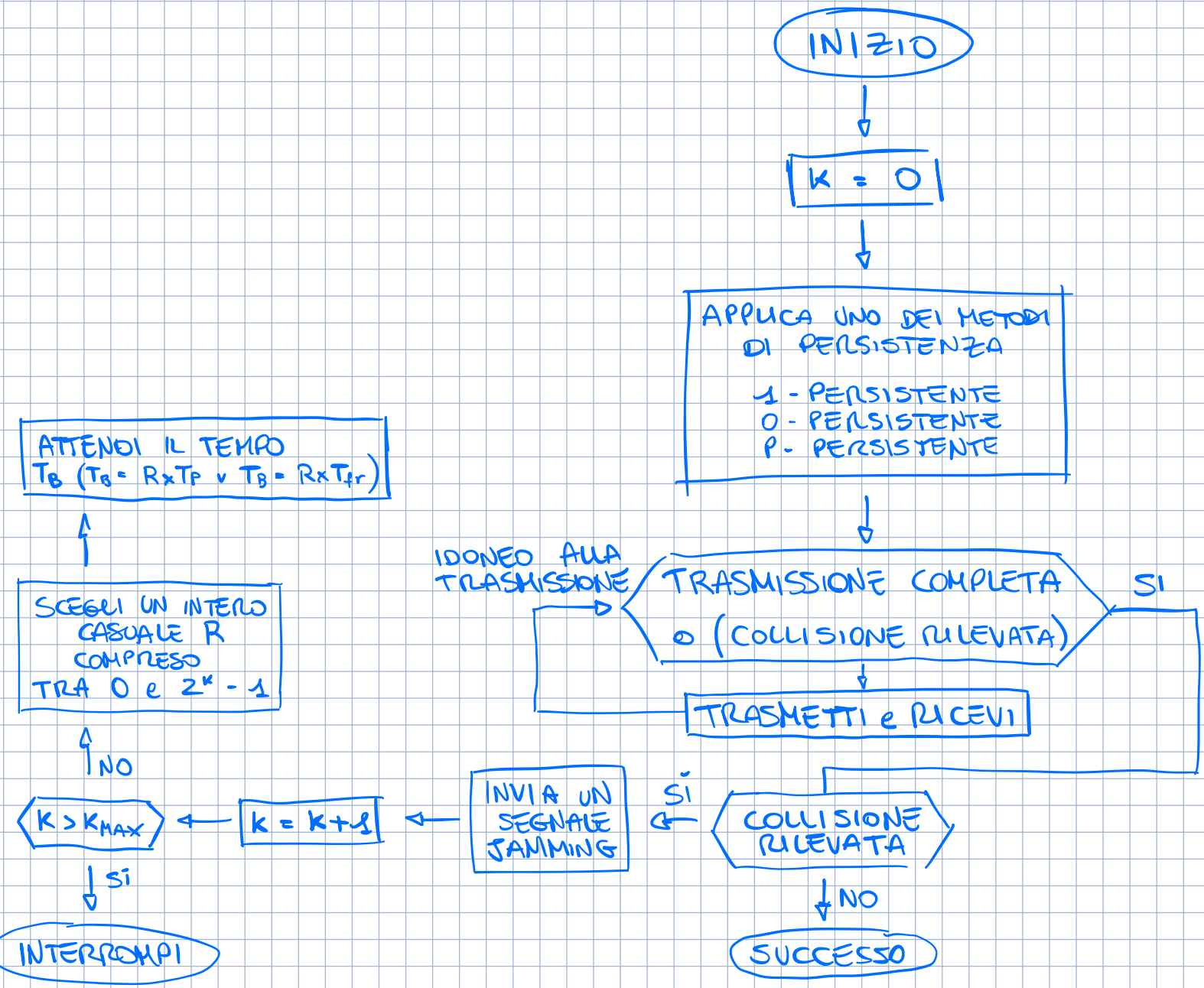
Il CSMA/CD aiuta ad evitare collisioni nei dati trasmessi su reti condivise, assicurando un utilizzo efficiente del canale di comunicazione e migliorando l'affidabilità delle trasmissioni.

K: NUMERO DI TENTATIVI

T_p: TEMPO MASSIMO DI PROPAGAZIONE

T_{fr}: TEMPO MASSIMO DI TRASMISSIONE PER UN FRAME

T_B: TEMPO DI ATTESA



Il controllo di parità è un codice di controllo che prevede l'invio di un bit supplementare nelle trasmissioni, con l'obiettivo di avere sempre un numero pari a 1 nelle sequenze inviate e verificare facilmente alcuni tipi di errore

Per esempio, se una sequenza di n bit contiene un numero pari a 1 come nel caso 1100110, per preservare tale parità in coda aggiungo uno 0 e la nuova sequenza sarà 1100110-0

Invece se una sequenza di n bit contiene un numero dispari di 1 1100010, per ottenere la parità dell' 1 in coda verrà aggiunto un 1 e la nuova sequenza sarà 1100010-1.

7 bit di dati:	Byte con bit di parità
1100110	1100110 - 0
1100010	1100010 - 1

Il CRC (Cyclic Redundancy Check) è un metodo di rilevamento di errori che si basa sul concetto di checksum, un particolare codice che viene calcolato a partire dai dati da inviare e da un polinomio generatore, condiviso tra mittente e destinatario

Funzionamento:

1. Il mittente prende i dati da inviare e calcola un codice chiamato checksum, usando un polinomio condiviso.

2. Aggiunge un checksum infondo ai dati e lo invia.
3. Il destinatario ricalcola il calcolo, se il checksum coincide i dati sono corretti, altrimenti c'è stato un errore.

Esempio di calcolo del checksum:

- Si sceglie il polinomio generatore
  CRC - 4 - ITU: → $x^4 + x + 1$ → in binario 10011
- Si aggiungono n-1 zeri in fondo ai dati.
- Si fa una divisione binaria modulo 2 (XOR divisione tra bit dove si usa al posto della sottrazione) tra i dati e il polinomio.
- il resto è il checksum

ESEMPIO:

Dati da inviare: 110100111011100
Polinomio: 10011
Checksum: 1011
Sequenza: 110100111011001011

Controllo del flusso del collegamento dati:

Il controllo del flusso assicura al mittente che esso non sovraccarichi il destinatario con più dati di quanto esso possa elaborare in un determinato intervallo di tempo.
Questo controllo è necessario per mantenere l'integrità e l'efficienza della connessione

evitando che i buffers del destinatario si sovraccarichino causando una perdita di frame.
Gli algoritmi del controllo del flusso più usati fanno uso dei seguenti tecni

- STOP - AND - WAIT : il mittente invia il pacchetto e aspetta la conferma (ACH) e se non arriva ritrasmette
- SLIDING WINDOW : il mitente può inviare più pacchetti contemporaneamente entro una finestra, quindi riceve una conferma man mano che li riceve. É più velsce ed efficiente.

Livello 3: LIVELLO RETE (NETWORK)

Permette ai dati di viaggiare da un dispositivo all'altro, anche se si trovano su reti diverse.
Ogni pacchetto contiene informazioni importante come l'indirizzo IP del mittente e del destinatario, un numero identificativo, tempo massimo che può rimanere in rete (TTL = tempo di vita -> indica quanti router può attraversare un pacchetto prima di essere eliminato).

Questi dati sono inseriti nell'intestazione di rete e consentono al router di capire dove inviare il pacchetto.
Quando un pacchetto è troppo grande per attraversare la rete (per esempio supera il limite

MTU = maximum trasmition unit. → indica la dimensione massima in byte che un pacchetto può contenere).

Ogni pacchetto viaggia su percorsi diversi e viene ricostruito una volta arrivato a destinazione, questo permette di evitare blocchi o rallentamenti.
Il livello rete gestisce anche gli indirizzi IP che possono essere assegnati in modo statico o dinamico (DHCP).

Per comunicare con dispositivi esterni e interni si usano tecniche come il NAT che permette di condividere a più dispositivi solo un indirizzo IP pubblico.

Inoltre il protocollo ARP (address resolution protocol) che va a tradurre gli indirizzi IP in indirizzi fisici (MAC), così da facilitare dalla comunicazione.

Per evitare che la comunicazione si intasi il livello di rete controlla il traffico, gestisce i dati in transito e le code, e ottimizza i processi per far si che i dati NON rimangano bloccati.

Dal punto di vista della sicurezza si possono utilizzare i protocolli IP - sec (security) che va a criptare i dati e garantirne la autenticità.

Mentre per i dati sensibili o delicati come le chiamate VOIP o lo streaming si può usare la qualità del servizio KUOS che da priorità a questi dati.

I principali dispositivi di rete di questo livello sono:

- IL ROUTER -> decide il percorso dei pacchetti.
- IL FIREWALL -> protegge la rete da accessi non autorizzati.
- IL GATEWAY -> collega reti diverse.
- IL PROXY -> fa da intermediario tra client e server.
- IL VPN-GATEWAY -> gestisce le connessioni sicure su reti remote.

MODELLO ISO-OSI → COSTITUITO DA

- RETE DI COMUNICAZIONE END-TO-END
  - 7. APPLICAZIONE
  - 6. PRESENTAZIONE
  - 5. SESSIONE
  - 4. TRASPORTO
- SOTTORETE DI COMUNICAZIONE

Livello 4: LIVELLO DI TRASPORTO

Il livello di trasporto si occupa di garantire che i dati arrivino correttamente in ordine e senza errori da un dispositivo all'altro.

È responsabile della comunicazione END-TO-END la comunicazione tra mittente e destinatario.

indipendentemente da come funziona la rete sottostante.

Quando un'applicazione invia dati, il livello di trasporto li divide in segmenti, dove ogni segmento riceve un'intestazione con informazioni fondamentali:

- Numeri di porta → quale applicazione ha inviato o deve ricevere i dati (PORTA 80 per il WEB)
- Numero di sequenza → ricostruire i dati in ordine giusto
- Acknowledgement → conferma che i dati sono stati ricevuti
- Controllo del flusso → evita che il destinatario sia sovraccaricato dai dati inviati.
- Controllo degli errori → verifica che i dati non siano stati danneggiati.

Per stabilire una connessione affidabile, il protocollo TCP usa un processo chiamato HANDSHAKE, una negoziazione in 3 fasi (POSSIAMO RICEVERE LA RISPOSTA, // , POSSIAMO CONTINUARE) che sincronizza i dispositivi prima di iniziare la trasmissione.

Il livello di trasporto gestisce la segmentazione e il riassemblaggio → se i dati sono troppo grandi

vengono divisi e riassemblati alla fine.

Grazie alla gestione delle porte più app. possono comunicare contemporaneamente sullo stesso dispositivo senza confondersi, perché ogni flusso ha la sua porta, come una corsia dedicata.

Il 4° livello implementa anche il MULTIPLEXING che permette di gestire più connessioni contemporaneamente sull' interfaccia di rete.

Dispositivi di rete al livello di trasporto:

- LOAD BALANCER → distribuisce il traffico a più server
- PROXY SERVER → intermedia tra CLIENT e SERVER, migliora la sicurezza
- VPN CONCENTRATOR → gestisce connessioni sicure su reti remote.

Livello 5: SESSIONE

Si occupa di gestire la comunicazione e le conversazioni tra applicazioni di rete.
Non trasmette dati direttamente, ma garantisce che la comunicazione sia controllata e recuperabile.
Stabilisce, mantiene e termina le sessioni usando protocolli come NETBIOS (network basic input output

system protocol) e RPC (remote procecute call)
é un programma che consente di eseguire funzioni su un dispositivo

Coordina chi può parlare e quando grazie ai token di controllo (UN SEGNALE CHE AUTORIZZA A UN' APP DI TRASMETTERE) e inserisce punti di salvataggio (CHECKPOINT -> SALVARE PER POI RIPRENDERE LA COMUNICAZIONE IN CASO DI ERRORE).
É fondamentale per applicazioni che richiedono continuità e affidabilità (VIDEOCONFERENZE o TRASFERIMENTO DATI)

Dispositi di rete al livello sessione:

- SERVER DI AUTENTICAZIONE → verifica le credenziali degli utenti e crea loro sessioni di accesso

Livello 6: PRESENTAZIONE

Questo livello i il traduttore e custode delle forme dei dati che si occupa di convertire, criptare e comprimere le informazioni affinché siano leggibie e sicre per le app.

Garantisce che 2 dispositivi possano capirsi e comunicare in modo sicuro anche se usano sistemi diversi.

Dispositi di rete al livello presentazione:

- GATEWAY di TRADUZIONE → converte i dati da un formato o protocollo a un altro.

- CIFRATORI / DECIFRATORI → criptano i dati per proteggerli e li rendono leggibili alla destinazione