

DEFINIZIONI

MEZZO TRASMISSIVO E CANALE

BANDA (Bit Rate)

CAPACITÀ

TRAFFICO

TOPOLOGIA DI UNA RETE DI TELECOMUNICAZIONE

TIPI DI CANALE

CANALE PUNTO-PUNTO

CANALE MULTI-PUNTO

CANALE BROADCAST

TOPOLOGIE A MAGLIA COMPLETA

TOPOLOGIA AD ALBERO

TOPOLOGIA A STELLA ATTIVA

TOPOLOGIA A STELLA PASSIVA

TOPOLOGIA A MAGLIA

TOPOLOGIA AD ANELLO

TOPOLOGIA A BUS

BUS ATTIVO

BUS PASSIVO

TOPOLOGIA FISICA E LOGICA

TOPOLOGIA FISICA

TOPOLOGIA LOGICA

TOPOLOGIE E PRESTAZIONI

TRASMISSIONE

PROCESSO DI NUMERIZZAZIONE

MODI DI TRASFERIMENTO

MULTIPLAZIONE

MULTIPLAZIONE STATISTICA

ACCESSO MULTIPLO

CONDIVISIONE DI UN NODO

COMMUTAZIONE DI CIRCUITO

COMMUTAZIONE DI PACCHETTO

RITARDI SUBITI DA UN PACCHETTO

PACCHETTO

COMMUTAZIONE DI PACCHETTO A CIRCUITO VIRTUALE

CIRCUITI PERMANENTI E COMMUTATI

TECNICHE DI SEGNALAZIONE

QUALITA' DI SERVIZIO

SORGENTI DI INFORMAZIONE

SORGENTI NUMERICHE

SORGENTI CBR

SORGENTI VBR

INDICI DI QUALITA'

ARCHITETTURE E PROTOCOLLI

PROTOCOLLI

ARCHITETTURE: MODELLO A STRATI

ARCHITETTURE: MODELLO DI RIFERIMENTO OSI

ARCHITETTURE DI RETE

STRATI (O LIVELLI)

STRATO 1: FISICO (physical layer)

STRATO 2: COLLEGAMENTO (data link layer)

STRATO 3: RETE (network layer)

STRATO 4: TRASPORTO (transport layer)

STRATO 5: SESSIONE (session layer)

STRATO 6: PRESENTAZIONE (presentation layer)

STRATO 7: APPLICAZIONE (application layer)

SERVIZI

 SERVICE ACCESS POINT

PROTOCOLLI

 CREAZIONE PDU

 SISTEMI

PROTOCOLLI A FINESTRA

 PROTEZIONE DAGLI ERRORI DI TRASMISSIONE

 BIT DI PARITA'

 CODICE A RIPETIZIONE

 PARITA' DI RIGA E COLONNA

 INTESTAZIONE PACCHETTI

 CORREZIONE O RECUPERO?

 ARQ

 STOP AND WAIT

 CANALE NON SEQUENZIALE

 GO BACK N

 SELECTIVE REPEAT

 SEMANTICA DEGLI ACK

 SIGNIFICATO CUMULATIVO

 SIGNIFICATO SELETTIVO (O INDIVIDUALE)

 SIGNIFICATO NEGATIVO (NAK)

 PIGGYBACKING

 POSIZIONI RELATIVE CORrette TRA WT e WR

 NUMERAZIONE PDU (GO-BACK-N)

 NUMERAZIONE PDU (SELECTIVE-REPEAT)

 EFFICIENZA E THROUGHPUT

STRATO FISICO (1)

MEZZI TRAMISSIVI

 MEZZI TRAMISSIVI ELETTRICI

 IL DOPPINO

 CAVO COASSIALE

 MEZZI TRAMISSIVI OTTICI

 FIBRA OTTICA

 MEZZI TRAMISSIVI RADIO

 CANALE RADIO (MOBILE)

CODIFICHE

 CODIFICHE UNIPOLARI

 CODIFICHE POLARI

 CODIFICHE BIPOLARI

 CODIFICHE nBmB

 MODULAZIONI DIGITALI

RETI DI ACCESSO

 DSL E ADSL

 ACCESSO DSL: IL MODEM

 ADSL: APPARATI UTENTE

 ADSL: APPARATI DI CENTRALE

 VDSL

 DISTANZA E VELOCITA'

 PASSIVE OPTICAL NETWORKS (PON)

 RETI MOBILI A BANDA LARGA

 ARCHITETTURA DI UNA RETE CELLULARE (LTE)

RETI DI TRASPORTO

 TRASMISSIONE SU RETI DI TRASPORTO

 SINCRONIZZAZIONE

 PDH

 SONET/SDH

STRATO COLLEGAMENTO (2)

PROTOCOLLI

STRATO 2 NELLE RETI PUBBLICHE

CARATTERISTICHE COMUNI

TRASPARENZA NEL TRASFERIMENTO DATI

BYTE STUFFING

PROTOCOLLO PPP - RFC 1661

INCAPSULAMENTO

LCP - LINK CONTROL PROTOCOL

NCP - NETWORK CONTROL PROTOCOL

PROTOCOLLO ATM

FORMATO CELLA ATM

AAL: ATM ADAPTATION LAYER

STRATO 2 NELLE RETI PRIVATE/LOCALI

IEEE 802.2 LLC

FORMATO PDU LLC

SNAP PDU

INTESTAZIONE SNAP PDU

CARATTERISTICHE RETI LOCALI

CONDIVISIONE DI UN CANALE (PROTOCOLLI PER LAN)

MAC - PROTOCOLLI AD ACCESSO CASUALE

ALOHA

SLOTTED ALOHA

CSMA (CARRIER SENSE MULTIPLE ACCESS)

CSMA/CD (Collision Detection)

CSMA/CA (Collision Avoidance)

STANDARD IEEE 802

FUNZIONI STRATO 2 IN RETI LOCALI

INDIRIZZI

INDIRIZZI MAC

PROTOCOLLO ETHERNET

PARAMETRI DI PROGETTO

ETHERNET - LIVELLO FISICO

LE RETI ETHERNET OGGI

HUB

SWITCH

INSTRADAMENTO MEDIANTE SWITCH

TRANSPARENT SWITCHING

ADDRESS LEARNING

FRAME FORWARDING

SPANNING TREE

VANTAGGI INTERCONNESSIONE LAN

VLAN: LAN VIRTUALI

GIGABIT ETHERNET

LE RETI WIFI

ARCHITETTURA 802.11

STRATO FISICO

STRATO MAC

DCF

VELOCITA' DI TRASMISSIONE

PROBLEMA: TERMINALE NASCOSTO

PROBLEMA: ANOMALIA DELLE VELOCITA' TRASMISSIVE

STRATO RETE (3)

INSTRADAMENTO

ALGORITMI DI INSTRADAMENTO

COSTO

ALGORITMI DI INSTRADAMENTO SEMPLICI

ALGORITMI DI INSTRADAMENTO COMPLESSI

ALGORITMI DISTRIBUITI - INFORMAZIONE

- ALGORITMI LINK STATE
- ALGORITMI DISTANCE VECTOR
- PROBLEMA DEL COUNT TO INFINITY
- CONFRONTO TRA ALGORITMI LS E DV
- PROTOCOLLO IP
 - IP FRAGMENTATION
 - IP ADDRESSING
 - SPECIAL ADDRESSING
 - IP ADDRESSING: CLASSFUL
 - IP ADDRESSING: SUBNETTING
 - IP ADDRESSING: CLASSLESS (CIDR)
 - IP ADDRESSING: DEVICE CONFIG
 - FUNZIONAMENTO IP ROUTING
 - LONGEST PREFIX MATCHING
 - TIPI ROUTING TABLE
 - LOGICAL IP SUBNETS (LIS)
 - PHYSICAL NETWORK
 - SUBNETS E PHYSICAL NETWORKS
 - ARP - ADDRESS RESOLUTION PROTOCOL
 - ICMP (Internet Control Message Protocol)

STRATO TRASPORTO (4)

- MULTIPLEXING
- DEMULITPLEXING
 - DEMULITPLEXING CONNECTIONLESS
 - DEMULITPLEXING CONNECTION-ORIENTED
- WELL-KNOWN PORTS
- TCP
 - TCP SEQUENCE NUMBERS
 - TCP ACKs
 - TCP OPEN/CLOSE CONNECTION
 - TCP FLOW CONTROL
 - TCP CONGESTION CONTROL
 - AIMD (Additive Increase Multiplicative Decrease) o Congestion Avoidance
 - TCP SLOW START
 - TCP: REAZIONE ALLE PERDITE

TRASFERIMENTO AFFIDABILE

STRATO APPLICAZIONE (7)

- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)
 - TIPI DI RECORD DNS
- APP DI RETE
 - ARCHITETTURE DELLE APPLICAZIONI
 - COMUNICAZIONE TRA PROCESSI
 - TIPI DI SERVIZI CHE PUÒ RICHIEDERE UN'APP
- HTTP (Hyper Text Transfer Protocol)
 - HTTP REQUEST MESSAGE
 - HTTP RESPONSE MESSAGE
 - COOKIE
 - WEB CACHES (PROXY SERVER)
- POSTA ELETTRONICA
 - FORMATO MAIL
 - PROTOCOLLO POP3

DEFINIZIONI

MEZZO TRASMISSIVO E CANALE

- *mezzo trasmittivo* → mezzo fisico in grado di trasportare segnali tra due o più punti.
- *canale* → singolo mezzo trasmittivo o concatenazione di mezzi trasmittivi.

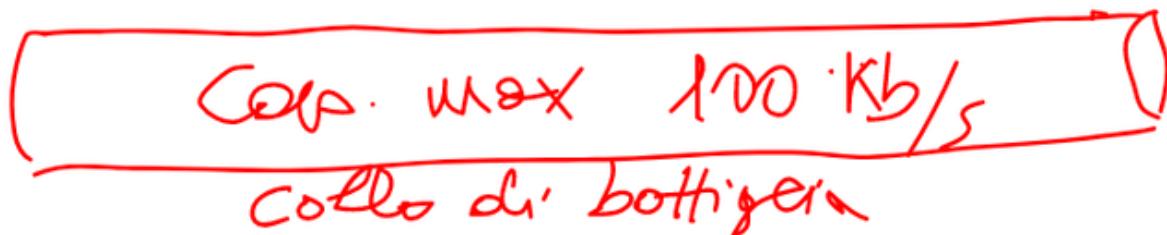
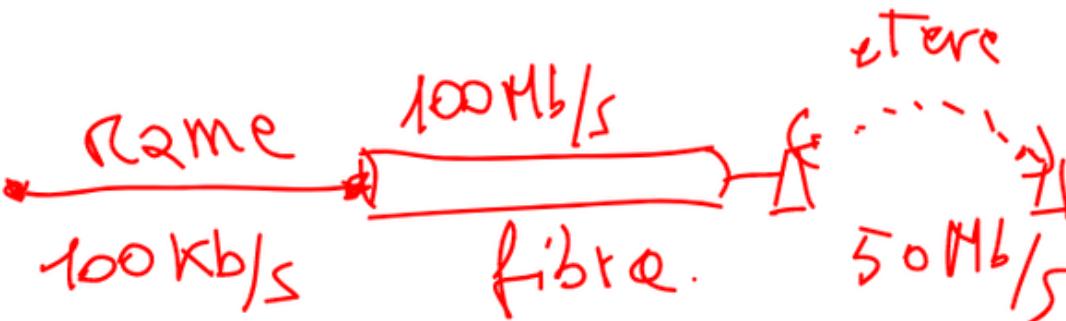
BANDA (Bit Rate)

Secondo le:

- *teoria dei segnali* → ampiezza spettrale di un segnale o di un canale
- *reti telematiche* → quantità di dati (bit) per unità di tempo (secondi)

CAPACITÀ

- La **capacità di un mezzo trasmittivo** è la massima velocità trasmittiva → dipende dalla tecnologia con cui sono realizzati trasmittitore e ricevitore.
- La **capacità di un canale** è la capacità del mezzo trasmittivo a bit rate inferiore tra quelli che lo compongono (collo di bottiglia).



TRAFFICO

- *traffico offerto* → quantità di dati per unità di tempo che una sorgente cerca di inviare in rete
- *traffico smaltito (throughput)* → porzione di traffico offerto che riesce ad essere consegnata correttamente alla destinazione

In generale:

- *throughput ≤ capacità del canale*
- *throughput ≤ traffico offerto*

TOPOLOGIA DI UNA RETE DI TELECOMUNICAZIONE

Definizione di topologia:

un insieme di nodi e segmenti che fornisce un collegamento tra due o più punti per permettere la telecomunicazione tra essi.

- *Si chiama **nodo** un punto in cui avviene la commutazione.*
- *Si chiama **segmento** un mezzo di trasmissione o un canale.*

TIPI DI CANALE

CANALE PUNTO-PUNTO

Due soli nodi collegati agli estremi del canale che viene utilizzato in modo paritetico

CANALE MULTI-PUNTO

Più nodi collegati ad un unico canale:

- *un nodo master*
- *numerosi slave*

CANALE BROADCAST

Un unico canale di comunicazione, condiviso da tutti i nodi. L'informazione inviata da un nodo è ricevuta da tutti gli altri. Se i dati trasmessi contengono l'indirizzo del nodo destinazione, realizzo di fatto un punto-punto.

La disposizione di nodi e canali definisce la topologia della rete di telecomunicazione.

Una topologia di rete è definita da un grafo $G=(V,A)$ dove:

- $V \rightarrow$ insieme dei vertici
- $A \rightarrow$ insieme di archi

Gli archi possono essere:

- *diretti* → orientati, unidirezionali
- *indiretti* → non orientati, bidirezionali

Definiamo:

- $N = |V| \rightarrow$ cardinalità dell'insieme dei vertici (nodi)
- $C = |A| \rightarrow$ cardinalità dell'insieme canali (bidirezionali) (archi)

TOPOLOGIE A MAGLIA COMPLETA

$$C = N(N-1)/2$$

Vantaggio:

- *tolleranza ai guasti (molti percorsi tra i nodi)*

Svantaggio:

- *elevato numero di canali*

Viene usata solo quando i nodi sono pochi.

TOPOLOGIA AD ALBERO

$$C = N-1$$

Vantaggio:

- *basso numero di canali*

Svantaggio:

- *vulnerabilità ai guasti (solo un percorso tra due nodi)*

E' usata per ridurre i costi e semplificare la stesura dei canali.

TOPOLOGIA A STELLA ATTIVA

$$C = N \text{ (centro stella non è un nodo)}$$

Vantaggio:

- *basso numero di canali*

Svantaggio:

- *vulnerabilità ai guasti del centro stella*

E' usata per ridurre i costi e semplificare la stesura dei canali.

Il centro stella (intelligente) seleziona chi deve ricevere i dati.

TOPOLOGIA A STELLA PASSIVA

$$C = 1 \text{ (anche se ci sono } N \text{ fili)}$$

Vantaggio:

- *basso numero di canali*

Svantaggio:

- *potenzialmente vulnerabile ai guasti del centro stella*

E' usata per ridurre i costi e semplificare la stesura dei canali.

TOPOLOGIA A MAGLIA

$$N-1 < C < N(N-1)/2$$

Vantaggio:

- *tolleranza ai guasti e numero di canali selezionabili a piacere*

Svantaggio:

- *topologia non regolare*
- *esiste un elevato numero di percorsi alternativi*

E' la più usata (internet, telefonia).

TOPOLOGIA AD ANELLO

Può essere **unidirezionale** o **bidirezionale**.

Unidirezionale:

$$C = N/2$$

Bidirezionale:

$$C = N$$

E' molto usata in reti locali e metropolitane.

In caso di guasto, l'anello bidirezionale assicura la sopravvivenza della rete (a capacità dimezzata).

TOPOLOGIA A BUS

BUS ATTIVO

E' un caso particolare di topologia ad albero.

$$C = N-1$$

BUS PASSIVO

Equivale ad una topologia a stella passiva senza centro stella.

$$C = 1$$

Esiste una sola scelta possibile di percorso tra ogni coppia di nodi. Veniva usata in reti locali e metropolitane. E' ormai in disuso (obsoleta).

TOPOLOGIA FISICA E LOGICA

TOPOLOGIA FISICA

Tiene conto del percorso dei mezzi trasmissivi.

(Come è effettivamente costruita)

TOPOLOGIA LOGICA

Definisce l'interconnessione tra nodi mediante canali.

(Come avviene effettivamente la comunicazione)

TOPOLOGIE E PRESTAZIONI

La scelta della topologia ha ricadute sulle prestazioni di una rete. A pari capacità disponibile sui canali, la quantità di traffico smaltibile da una rete dipende:

- *dalla media della distanza tra ogni coppia di nodi della rete, pesata dalla quantità di traffico scambiata tra i due nodi*

In particolare, per traffico uniforme e topologie regolari, il traffico smaltibile è inversamente proporzionale alla distanza media.

TRASMISSIONE

Può essere di più tipi, comunemente:

- *analogica* → l'informazione viene trasferita per mezzo di un segnale elettrico **continuo, limitato e di infiniti possibili valori**
- *numerica* → l'informazione viene trasferita per mezzo di un segnale elettrico **discontinuo, limitato e con un numero finito di possibili valori**

Altri tipi di trasmissione:

- *parallela* → l'informazione è trasferita in parallelo (es. 1 byte alla volta) su bus di comunicazione con segnali di dati e segnali di temporizzazione (clock)
- *seriale* → l'informazione viene prima serializzata e quindi trasmessa un bit alla volta
- *asincrona* → ogni byte di informazioni è trasmesso separatamente dagli altri
- *sincrona* → le informazioni da trasmettere sono strutturate in trame

PROCESSO DI NUMERIZZAZIONE

Nelle reti telematiche, l'informazione è trasferita in forma digitale usando segnali:

- *analogici*
- *digitali*

Se l'informazione originale si presenta in forma analogica (audio, video, ecc.), prima del trasferimento viene convertita in forma digitale usando un **processo di numerizzazione**.

Il processo ha il seguente funzionamento: *analogico* → *campionamento* → *quantizzazione* → *numerico*

MODI DI TRASFERIMENTO

- *condivisione di canale* → *multiplazione e accesso multiplo*
- *condivisione di nodo* → *commutazione*

MULTIPLAZIONE

Tutti i flussi sono disponibili in un unico punto.



Può essere di 4 tipi:

- *multiplazione di frequenza* → la separazione è ottenuta usando bande di frequenza diverse
- *multiplazione di tempo* → la separazione tra i flussi avviene utilizzando intervalli di tempo diversi
- *multiplazione di codice* → la separazione tra i flussi avviene mediante diverse codifiche
- *multiplazione di spazio*

MULTIPLAZIONE STATISTICA

Le multiplazioni sopra citate possono essere:

- *predeterminate* (sulla scala temporale della dinamica delle connessioni)
- *statistica* (funzione delle variazioni "istantanee" di traffico)

ACCESSO MULTIPLO

Se i flussi accedono al canale da punti differenti.



CONDIVISIONE DI UN NODO

E' il processo di allocazione delle risorse di rete necessarie per il trasferimento dell'informazione.

- *commutazione di circuito* → se i flussi sono continui (es. telefonia)
- *commutazione di pacchetto e cella* → se i flussi sono intermittenti (es. trasmissione dati)

COMMUTAZIONE DI CIRCUITO

Un circuito costituisce un collegamento fisico tra i due terminali di utente.

In particolare:

- *il circuito è di uso esclusivo dei due utenti per tutta la durata della comunicazione*
- *le risorse sono rilasciate solo al termine della comunicazione, su indicazione degli utenti*

Vantaggi:

- *banda costante garantita*
- *ritardi di trasferimento costanti*
- *trasparenza del circuito (formati, velocità, protocolli)*
- *bassi ritardi nell'attraversamento dei nodi*

Svantaggi:

- *risorse dedicate a una comunicazione*
- *efficienza buona solo per sorgenti non intermittenti*
- *tempo di apertura del circuito*
- *nessuna conversione di formati, velocità, protocolli*
- *tariffazione in base al tempo di esistenza del circuito*

COMMUTAZIONE DI PACCHETTO

Non si allocano risorse per l'uso esclusivo di due o più utenti. E' studiata espressamente per sorgenti intermittenti (es. chat).

L'informazione da trasferire è organizzata in unità dati (PDU) che comprendono informazione di utente e di controllo.

Terminologia:

- *PDU* → *protocol data unit (unità dati - pacchetto)*
- *PCI* → *protocol control information (controllo - header)*
- *SDU* → *service data unit (informazione di utente - dati)*

$$\text{PCI} + \text{SDU} = \text{PD}$$

In questo tipo di commutazione:

- *i pacchetti sono consegnati alla rete*
- *ogni nodo → ** :*
 - *memorizza il pacchetto (non per forza tutto, anche solo l'header per avere le informazioni di inoltro)*
 - *elabora il pacchetto e determina il canale su cui inoltrarlo*
 - *mette il pacchetto in coda per la trasmissione sul canale*

Questa procedura (quella dei nodi → **) viene definita **store and forward**.

L'informazione dell'utente può dover essere frazionata in molti pacchetti (di dimensione fissa o variabile).

Vantaggi:

- *utilizzo efficiente delle risorse anche in presenza di traffico intermittente*
- *possibilità di controllo di correttezza lungo il percorso*
- *possibilità di conversioni di velocità, formati, protocolli*
- *tariffazione in funzione del traffico trasmesso*

Svantaggi:

- *difficile ottenere garanzie di banda*
- *elaborazione di ogni pacchetto in ogni nodo*
- *ritardo di trasferimento variabile*

RITARDI SUBITI DA UN PACCHETTO

Durante il suo percorso tra sorgente e destinazione, un pacchetto può subire diversi ritardi:

- *su ogni canale su cui è trasmesso:*
 - *ritardo di trasmissione (e di ricezione)*
 - *ritardo di propagazione*
- *su ogni nodo di commutazione:*
 - *ritardo di elaborazione*
 - *ritardo di accodamento*

Esiste un altro ritardo, definito come **ritardo di accesso**, cioè il ritardo causato dal tempo che intercorre tra il momento in cui il pacchetto è pronto ad essere trasmesso e il momento in cui effettivamente inizia la trasmissione sulla rete.

PACCHETTO

Dimensione P di un pacchetto:

- misurata in bit o byte (PCI+SDU)

Tempo di trasmissione T_{TX} di un pacchetto:

- varia da canale a canale

$$T_{TX} = P/V_{TX}$$

dove V_{TX} = velocità di trasmissione sul canale

Dimensione M (in metri) di un pacchetto su un canale:

- $M = (\text{velocità della luce}) \times (\text{tempo di trasmissione } T_{TX})$

COMMUTAZIONE DI PACCHETTO A CIRCUITO VIRTUALE

La comunicazione è suddivisa in tre fasi:

- apertura connessione (segnalazione)
- trasferimento dati
- chiusura connessione (segnalazione)

Esiste un accordo preliminare tra i due interlocutori e il fornitore del servizio.

Pacchetti diversi con uguale sorgente e destinazione seguono tutti lo stesso percorso.

Vantaggi rispetto al datagram:

- *mantenimento della sequenza*
- *minor variabilità dei ritardi*
- *instradamento solo in fase di apertura di connessione*

CIRCUITI PERMANENTI E COMMUTATI

- PVC:
 - *creati tramite il sistema di gestione della rete, non in tempo reale*
 - *definiscono una rete semi-statica*
- SVC:
 - *creati su richiesta dell'utente tramite segnalazione della rete, in tempo reale*

QUIZ 1:

Il processo di store and forward:

- non è MAI eseguito da nodi di una rete a commutazione di pacchetto datagram
- è eseguito SOLO da nodi di una rete a commutazione di pacchetto
- non è MAI eseguito da nodi di una rete a commutazione di pacchetto a circuito virtuale
- è eseguito SOLO da nodi di una rete a commutazione di pacchetto a circuito virtuale

Risposta corretta: B.

QUIZ 2:

Il ritardo di trasmissione e il ritardo di propagazione:

- dipendono da fattori diversi caratteristici di una rete di calcolatori
- sono aspetti diversi del ritardo di accesso alla rete
- sono uguali se la velocità di propagazione del mezzo è uguale alla velocità di trasmissione
- sono uguali se le dimensioni delle PDU sono sempre le stesse

Risposta corretta: A.

QUIZ 3:

Per ridurre il ritardo di pacchettizzazione è consigliabile:

- A. ridurre la dimensione del campo dati delle PDU
- B. aumentare la dimensione dell'intestazione
- C. scegliere una destinazione vicina
- D. diminuire il ritardo di accesso

Risposta corretta: A.

TECNICHE DI SEGNALAZIONE

Si distinguono:

- *segnalazione di utente* → scambio di info tra utente e nodo
- *segnalazione internodale* → scambio di info tra i nodi

Una segnalazione può essere:

- *associata al canale* (es. telefonia mobile):
 - esiste una corrispondenza biunivoca tra canale controllante (*informazioni di segnalazione*) e canale controllato (*informazioni di utente*)
 - *in banda* → canale controllante e controllato coincidono - sono usati *in tempi diversi*
 - *fuori banda* → canale controllante e controllato distinti
- *a canale comune*:
 - un canale di segnalazione controlla più canali di informazioni di utente
 - il canale di segnalazione funziona a pacchetto (per specificare a chi si riferisce la segnalazione)

QUALITA' DI SERVIZIO

Per il progetto di una rete si devono definire le caratteristiche secondo le quali le informazioni sono emesse dalle sorgenti nell'ambito di un servizio di telecomunicazione. L'**analisi** e il **progetto** di una rete di TLC si basano su modelli **quantitativi** che permettono di stimare la qualità del servizio fornito a partire da ipotesi relative alle risorse e alle attività.

- *Problema di progetto:*
 - *dati:*
 - richieste di servizio
 - qualità di servizio
 - *determinare:*
 - risorse necessarie
- *Problema di analisi:*
 - *dati:*
 - richieste di servizio
 - risorse disponibili
 - *determinare:*
 - qualità del servizio

Servono quindi modelli matematici per:

- caratterizzare le richieste di servizio
- descrivere l'interazione tra attività e risorse
- calcolare la qualità del servizio

SORGENTI DI INFORMAZIONE

- analogiche: voce, video
 - caratterizzate dalle loro caratteristiche spettrali (occupazione in banda, correlazione, ecc)
- numeriche (o numerizzate): dati, voce (numerizzata), video (numerizzato)
 - caratterizzate dalla velocità di cifra e dalla loro impulsività (burstiness)

SORGENTI NUMERICHE

Possono essere:

- a velocità costante (Constant Bit Rate - CBR)
- a velocità variabile (Variable Bit Rate - VBR)

SORGENTI CBR

Caratterizzate da:

- velocità (b/s) (e dimensione del dato)
- durata (s)
- processo di generazione delle chiamate

SORGENTI VBR

Caratterizzate da:

- velocità di picco (b/s)
- velocità media (b/s)
 - oppure grado di intermittenza = (velocità di picco) / (velocità media)
- durata (s)
- processi di generazione delle chiamate

INDICI DI QUALITÀ'

Tipi di informazione diversi richiedono alla rete prestazioni diverse.

Indici di qualità possono essere:

- ritardo (valor medio, percentile, tempo reale)
- velocità
- probabilità di errore (sul bit)
- probabilità di perdita (se l'errore non può essere recuperato dalla codifica)
- probabilità di blocco

Esempi:

- **Telefonia (CBR)** - ciò che mi importa principalmente:
 - ritardo massimo pari a qualche decimo di secondo - tempo reale
 - velocità fino a 64 kb/s

- probabilità di errore non superiore a qualche unità percentuale (voce distorta, ecc)
- probabilità di blocco bassa
- **Posta elettronica (VBR)** - ciò che mi importa principalmente:
 - ritardo massimo fino a diversi minuti
 - velocità bassa
 - probabilità di errore trascurabile
 - probabilità di blocco trascurabile
- **Video streaming**:
 - ritardo massimo fino a qualche secondo - tempo reale
 - velocità da 100 kb/s a qualche Mbit/s
 - probabilità di errore non superiore a qualche unità percentuale
 - probabilità di blocco molto bassa

ARCHITETTURE E PROTOCOLLI

Definizione CCITT di "**comunicazione**": "trasferimento di informazioni secondo convenzioni prestabilite"

In una rete, le regole che definiscono l'interazione tra elementi di una rete si chiamano **protocolli di comunicazione**. La gerarchia tra i protocolli definisce una **architettura di rete**.

PROTOCOLLI

Definizione CCITT: "descrizione formale delle procedure adottate per assicurare la comunicazione tra due o più oggetti dello stesso livello gerarchico"

Un protocollo prevede lo scambio di messaggi, definendone:

- **tipologia**
 - richieste e risposte
- **sintassi**
 - struttura dei messaggi
- **semantica**
 - significato di campi di bit dentro ai messaggi
- **temporizzazione**
 - sequenze temporali di comandi e risposte

ARCHITETTURE: MODELLO A STRATI

Un'architettura di rete definisce:

- il processo di comunicazione
- le relazioni tra le entità coinvolte nella comunicazione
- le funzioni necessarie per la comunicazione
- le modalità organizzative delle funzioni

Si usano **architetture stratificate** (ogni "strato" svolge un ruolo ben preciso) per diversi motivi, tra cui:

- semplicità di progetto
- facilità di gestione
- semplicità di standardizzazione

- *separazione di funzioni*

ARCHITETTURE: MODELLO DI RIFERIMENTO OSI

Storicamente è il **primo modello a strati** (1983). I principi fondamentali definiti dal modello di riferimento OSI (Open System Interconnection) sono oggi universalmente accettati.

Questo modello si suddivide in (importante l'ordine):

- *Application → Applicazione*
- *Presentation → Presentazione*
- *Session → Sessione*
- *Transport → Trasporto*
- *Network → Rete*
- *Data Link → Collegamento*
- *Physical → Fisico*

ARCHITETTURE DI RETE

In astratto, una rete è composta di **sistemi** (terminali, nodi, ecc) collegati tra loro da **mezzi trasmissivi**.

All'interno di ogni sistema, ci sono "processi" applicativi (*ad esempio: task che trova la strada per consegnare il pacchetto*).

STRATI (O LIVELLI)

Ogni sistema è composto da sottosistemi. Ogni sottosistema realizza le funzioni proprie di uno strato tramite delle **entità** (processi applicativi).

Notazioni del tipo

(3)-strato oppure (4)-entità

indicano

"strato 3" oppure "entità di strato 4"

Nel caso OSI, lo strato più alto è lo **strato 7**, mentre quello più basso è lo **strato 1**.

Ogni strato (o livello):

- *fornisce servizi allo strato superiore*
- *usa:*
 - *i servizi dello strato inferiore*
 - *le proprie funzioni*
- *migliora/integra il servizio offerto dallo strato inferiore*

Possiamo identificare quindi:

- *fornitori di servizio*
- *utenti del servizio*
- *punti di accesso al servizio: SAP (Service Access Point)*

STRATO 1: FISICO (physical layer)

Fornisce i mezzi meccanici, fisici, funzionali e procedurali per attivare, mantenere e disattivare le connessioni fisiche.

Ha il compito di effettuare il trasferimento delle cifre binarie scambiate dalle entità di strato di collegamento.

STRATO 2: COLLEGAMENTO (data link layer)

Fornisce i mezzi funzionali e procedurali per il trasferimento delle unità dati tra entità di strato rete e per fronteggiare malfunzionamenti dello strato fisico.

Ha principalmente i seguenti compiti:

- *delimitazione delle unità dati*
- *rivelazione e recupero degli errori di trasmissione*
- *controllo di flusso*

STRATO 3: RETE (network layer)

Fornisce i mezzi per instaurare, mantenere e abbattere le connessioni di rete tra entità di strato trasporto.

Ha principalmente i seguenti compiti:

- *instradamento*
- *controllo di flusso e congestione*
- *tariffazione*

STRATO 4: TRASPORTO (transport layer)

Colma le carenze di qualità di servizio delle connessioni di strato rete.

Ha principalmente i seguenti compiti:

- controllo di errore
- controllo di sequenza
- controllo di flusso

E' lo strato che esegue l'eventuale segmentazione dei dati in pacchetti e la loro ricomposizione a destinazione.

STRATO 5: SESSIONE (session layer)

Assicura alle entità di presentazione una connessione di sessione; organizza quindi il colloquio tra le entità di presentazione.

Ha il compito di strutturare e sincronizzare lo scambio di dati in modo da poterlo sospendere, riprendere e terminare ordinatamente.

STRATO 6: PRESENTAZIONE (presentation layer)

Risolve i problemi di compatibilità per quanto riguarda la rappresentazione dei dati da trasferire.

Ha il compito di risolvere i problemi relativi alla trasformazione della sintassi dei dati. Può fornire anche servizi di cifratura delle informazioni.

STRATO 7: APPLICAZIONE (application layer)

Fornisce ai processi applicativi i mezzi per accedere all'ambiente OSI.

SERVIZI

Gli utenti dello **strato N** (le **(N+1)-entità**), cooperano e comunicano usando lo **(N)-servizio** fornito dallo **(N)-fornitore di servizio**.

Un servizio può essere:

- **connection-oriented (CO)** → *si stabilisce un accordo preliminare (connessione) tra rete e interlocutori, poi si trasferiscono i dati e infine si rilascia la connessione*
- **connectionless (CL)** → *i dati vengono immessi in rete senza un accordo preliminare e sono trattati in modo indipendente*

Uno strato N+1 percepisce gli strati inferiori come fornitori di un (N)-servizio.

Tutti gli strati da N in giù sono una "black box" per le (N+1)-entità.

black-box → *entità di cui non conosciamo il funzionamento ma che possiamo definire solo attraverso il servizio che ci offre*

SERVICE ACCESS POINT

Un (N)-servizio è offerto ad una (N+1)-entità con una connessione che passa per un **punto di accesso al servizio** (Service Access Point - SAP).

PROTOCOLLI

Lo scambio di informazioni tra (N)-entità **omologhe** di sistemi diversi avviene con un (N)-protocollo.

CREAZIONE PDU

- *in un sistema a strati, i dati utente presenti allo strato N sono detti N-SDU (Service Data Unit)*
- *lo strato N aggiunge proprie informazioni di controllo dette N-PCI (Protocol Control Information), comunemente chiamata "intestazione"*
- *N-PCI + N-SDU = N-PDU*
- *ogni strato inferiore tratta la PDU dello strato superiore come se fosse una "busta chiusa" a cui aggiungere solo un'intestazione*

Prima della trasmissione, ai dati sono aggiunte tante intestazioni quanti sono gli strati attraversati nel sistema (l'unico strato a non aggiungere un'intestazione è quello fisico).

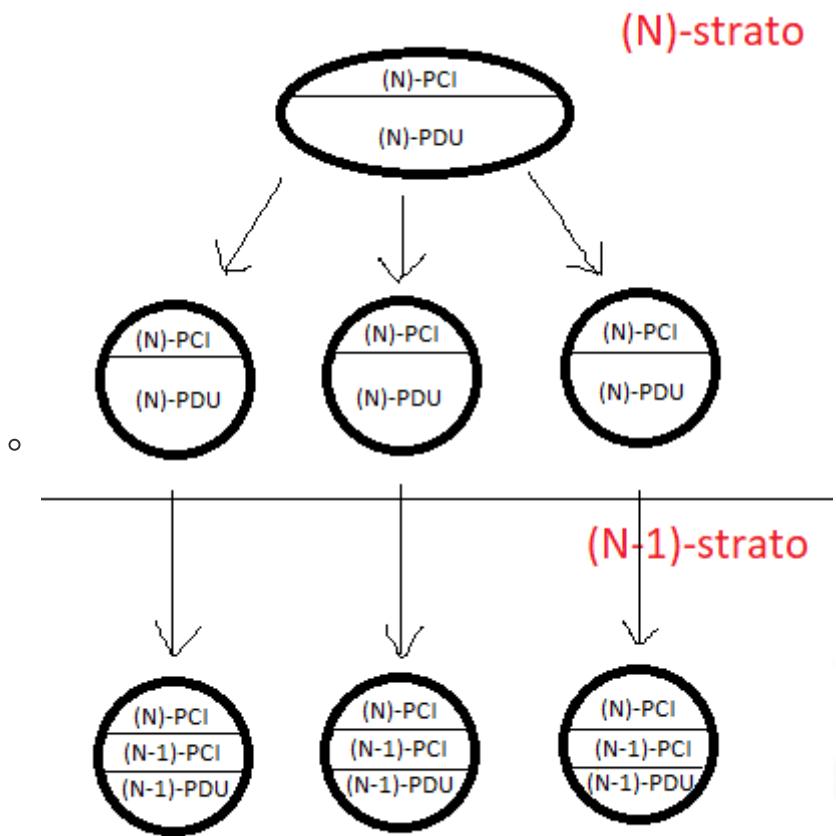
In ricezione avviene il processo inverso (le intestazioni possono essere presenti in testa e in coda).

Sulle unità è possibile che avvengano:

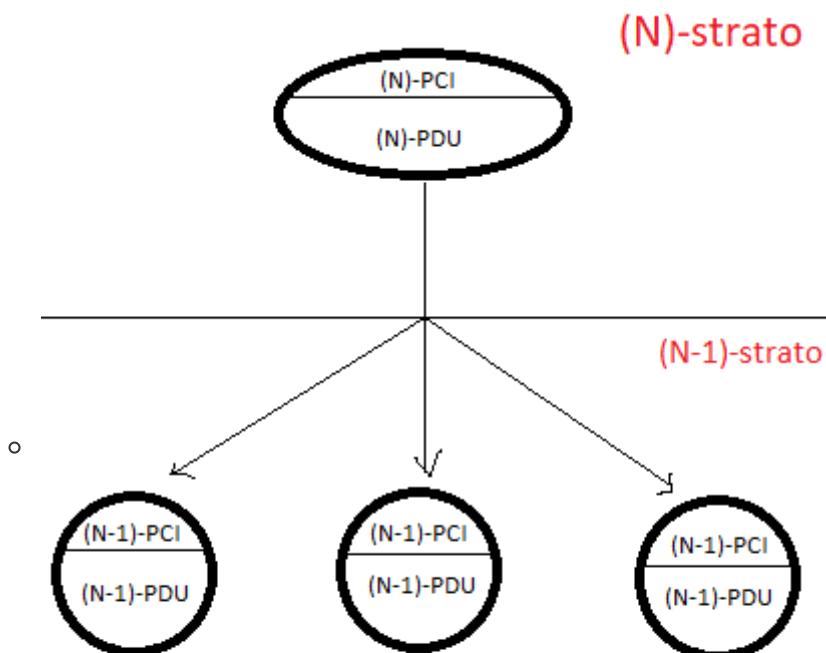
- *segmentazione*
- *concatenazione*

Possono entrambe avvenire:

- *costruendo più (N)-PDU da una (N)-SDU*



- generando più $(N-1)$ -SDU da una (N) -PDU



Segmentare NON conviene in quanto:

- ci sarà maggiore quantità di intestazioni
- necessita di ri-assemblare in ricezione

- se perdo "un pezzo" perdo tutto il dato

SISTEMI

Si dividono in:

- *sistemi terminali* (es. utenti)
- *sistemi di relay* (es. nodi)

I due tipi di sistemi comunicano per mezzo dei **mezzi trasmissivi**.

QUIZ:

Un (N)-protocollo regola le interazioni:

- tra una (N)-entità ed un (N-1)-SAP
- tra (N)-entità dello stesso sistema o di sistemi diversi
- tra (N)-entità e tutte le entità al di sotto di esse nella pila protocollare
- tra una (N)-entità e la (N-1)-entità

Risposta corretta: B.

PROTOCOLLI A FINESTRA

Compaiono in quasi tutte le reti telematiche moderne e passate. Il loro scopo è:

- *il recupero di errori di trasmissione*
- *il controllo del flusso di trasmissione*
- *il controllo della sequenza*

PROTEZIONE DAGLI ERRORI DI TRASMISSIONE

A seconda del tipo di canale, la probabilità di errore sul bit varia da 10^{-12} (fibra ottica) a 10^{-3} (canale radio rumoroso).

Occorrono quindi delle tecniche per rilevare ed eventualmente recuperare (correggere) gli errori.

Le tecniche utilizzate sono: **codifiche di canale**.

BIT DI PARITA'

| | |
|----------------------|----------|
| 0 1 1 0 1 0 1 0 | 0 |
| 0 1 1 1 0 1 0 | 1 |

- *riconosce errori in numero dispari*
- *non correggo*
- *se si verificano (ad esempio) 2 errori, il bit di parità non rileva l'errore (statisticamente è difficile che si verifichino 2 errori)*

CODICE A RIPETIZIONE

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

[Nell'immagine si prende la combinazione 01101010 (riga 1 e 3) per maggioranza.]

- *decisione a maggioranza*
- *permette di correggere errori*
- *maggior ridondanza*

PARITA' DI RIGA E COLONNA

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |

- *consente la correzione di errori singoli*
- *maggior ridondanza della parità di riga (o colonna)*
- *minore ridondanza del codice a ripetizione*

INTESTAZIONE PACCHETTI

Si introducono bit di parità tra le informazioni di controllo all'interno delle PDU:

- *CRC (Cyclic Redundancy Check)*
- *Internet Checksum*

CORREZIONE O RECUPERO?

A seconda della quantità di bit di parità, si possono impiegare tecniche diverse:

- **FEC (Forward Error Correction)** → i bit di parità (tanti) sono usati per cercare di correggere gli errori in ricezione, senza ritrasmettere il pacchetto
- **ARQ (Automatic Retransmission reQuest)** → i bit di parità (pochi) sono usati per cercare di rivelare gli errori e permettere al ricevitore di chiedere la ritrasmissione della PDU

ARQ

Si introducono bit di numerazione tra le informazioni di controllo (PCI) all'interno delle PDU.

Alcune tecniche ARQ sono:

- *Stop and wait (Alternating bit)*
- *Go back N*

- *Selective repeat*

Nella PCI del pacchetto dati, troveremo:

- *bit di parità*
- *N(T), numero di sequenza*
- *indirizzi*

Nella PCI del pacchetto di riscontro (**ACK**) (un'intestazione che viene ritornata dal ricevitore al trasmettitore), troveremo:

- *bit di parità (per autoprotezione)*
- *N(R), numero di sequenza atteso*
- *indirizzi*

STOP AND WAIT

Il trasmettitore:

- *fa una copia della PDU per possibile ritrasmissione*
- *invia la PDU*
- *attiva un orologio, timer (tempo di timeout)*
- *si pone in attesa della conferma di ricezione (acknowledgment - ACK)*
- *se scade il timeout prima dell'arrivo della conferma, ripete la trasmissione riattivando il timeout*

Il trasmettitore, quando riceve un ACK:

- *controlla la correttezza dell'ACK (i suoi bit di parità)*
- *controlla il numero di sequenza*
- *se l'ACK è relativo all'ultima PDU trasmessa, si abilita la trasmissione della prossima PDU, altrimenti l'ACK viene ignorato (scartato)*

Il ricevitore, quando riceve una PDU:

- controlla la correttezza della PDU:
 - se è corretta invia la conferma di ricezione
- controlla il numero di sequenza:
 - se è quella attesa, viene consegnata ai livelli superiori

Struttura del processo:

- *Inizializzazione:*
 - *la connessione è configurata alla sua apertura*
 - *TX e RX concordano i parametri del protocollo*
 - *V(T) = 0 al trasmettitore (contatore)*
 - *R(T) = 0 al ricevitore (contatore)*
- *(TRASMETTORE) Trasmissione di una PDU con N(T) = V(T):*
 - *avvio dell'orologio*
- *(RICEVITORE) Ricezione di una PDU:*
 - *controllo di correttezza*
 - *controllo di sequenza: N(T) = V(R) ?*
 - *se corretta e in sequenza, invio a livelli superiori*
- *(RICEVITORE) Incremento di V(R)*
- *(RICEVITORE) Trasmissione di un ACK con N(R) = V(R)*

- (*TRASMETTITORE*) Ricezione di un ACK
 - controllo di correttezza
 - controllo di sequenza: $N(R) = V(T)+1$?
 - arresto dell'orologio
- *FINE DEL CICLO*

N.B. : Per mantenere il conteggio (contatori), servono dei bit di numerazione; se si usa un solo bit di numerazione si parla di **Alternating bit protocol**.

CANALE NON SEQUENZIALE

Si tratta di un canale sul quale i pacchetti inviati in un determinato ordine, possono essere ricevuti in ordine diverso.

In questo caso, si possono verificare malfunzionamenti come:

- *perdita di PDU*
- *duplicazione di PDU*
- *il protocollo si blocca in loop*

Si riducono le possibilità di malfunzionamento usando:

- *un maggior numero di bit per la numerazione*
- *un tempo di vita massimo per le PDU e gli ACK*

GO BACK N

Permette la trasmissione di più di una PDU prima di fermarsi in attesa delle conferme.

La **finestra di trasmissione W_T** rappresenta:

la quantità massima di PDU in sequenza che il trasmettitore è autorizzato ad inviare in rete senza averne ricevuto riscontro (ACK).

La **finestra di ricezione W_R** rappresenta:

la sequenza di PDU che il ricevitore è disposto ad accettare e memorizzare.

Nel caso del protocollo **GO BACK N**:

- $W_T > 1$
- $W_R = 1$

E' importantissimo l'utilizzo del timeout, che viene azzerato e fatto ripartire solo in due casi:

- *nel momento in cui il trasmettitore riceve un ACK dal ricevitore*
- *quando il trasmettitore trasmette una nuova PDU (la aggiunge alla finestra W_T)*

Se il timeout scade senza aver ricevuto alcun ACK, viene ripetuta la trasmissione di tutte le PDU non ancora confermate presenti nella finestra di trasmissione.

Il trasmettitore:

- *invia fino ad $N = W_T$ PDU, facendo di ognuna una copia*
- *attiva un solo orologio per le N PDU (alla fine della trasmissione dell'ultima PDU)*
- *si pone in attesa degli ACK*
- *per ogni ACK in sequenza ricevuto, fa scorrere in avanti la finestra di tanti pacchetti quanti sono i pacchetti confermati*

- se scade il timeout prima della conferma di ricezione relativa alla PDU che ha settato il timeout, ripete la trasmissione di tutte le PDU non ancora confermate

Il ricevitore, quando riceve una PDU:

- controlla la correttezza della PDU
- controlla il numero di sequenza:
 - se la PDU è corretta invia la conferma di ricezione (ACK)
 - se la PDU contiene il primo numero di sequenza non ancora ricevuto, viene consegnata ai livelli superiori

SELECTIVE REPEAT

Rispetto al go-back-N questo protocollo può accettare PDU corrette ma fuori sequenza. Con questo protocollo **soltamente la finestra di trasmissione W_T e la finestra di ricezione W_R sono di pari dimensioni e maggiori di 1.**

Il trasmettitore:

come go-back-N

Il ricevitore:

- riceve una PDU
- controlla il numero di sequenza **E** la correttezza della PDU:
 - se la PDU è corretta e in sequenza → viene consegnata al livello superiore (eventualmente insieme ad altre PDU ricevute in sequenza)
 - se la PDU è corretta ma non in sequenza:
 - se è dentro la finestra di ricezione la memorizza
 - se è fuori dalla finestra di ricezione la scarta
- invia comunque un ACK relativo all'ultima PDU ricevuta in sequenza

SEMANTICA DEGLI ACK

Trasmettitore e Ricevitore si devono accordare **preventivamente** sulla semantica degli ACK.

SIGNIFICATO CUMULATIVO

Si notifica la corretta ricezione di tutti i pacchetti con numero di sequenza inferiore a quello specificato nell'ACK.

ACK(n) → "ho ricevuto tutto in sequenza fino ad n escluso"

SIGNIFICATO SELETTIVO (O INDIVIDUALE)

Si notifica la corretta ricezione di un pacchetto particolare.

ACK(n) → "ho ricevuto il pacchetto n , ma non ti do indicazioni sui pacchetti precedenti o successivi"

SIGNIFICATO NEGATIVO (NAK)

Si notifica la richiesta di ritrasmissione di un singolo pacchetto.

NAK(n) → "ritrasmetti il pacchetto n , ma non ti do indicazioni su quali pacchetti sono stati ricevuti"

PIGGYBACKING

Nel caso di flussi di informazione bidirezionali, è sovente possibile scrivere l'informazione di riscontro (ACK) nell'intestazione di PDU di informazione che viaggiano nella direzione opposta.

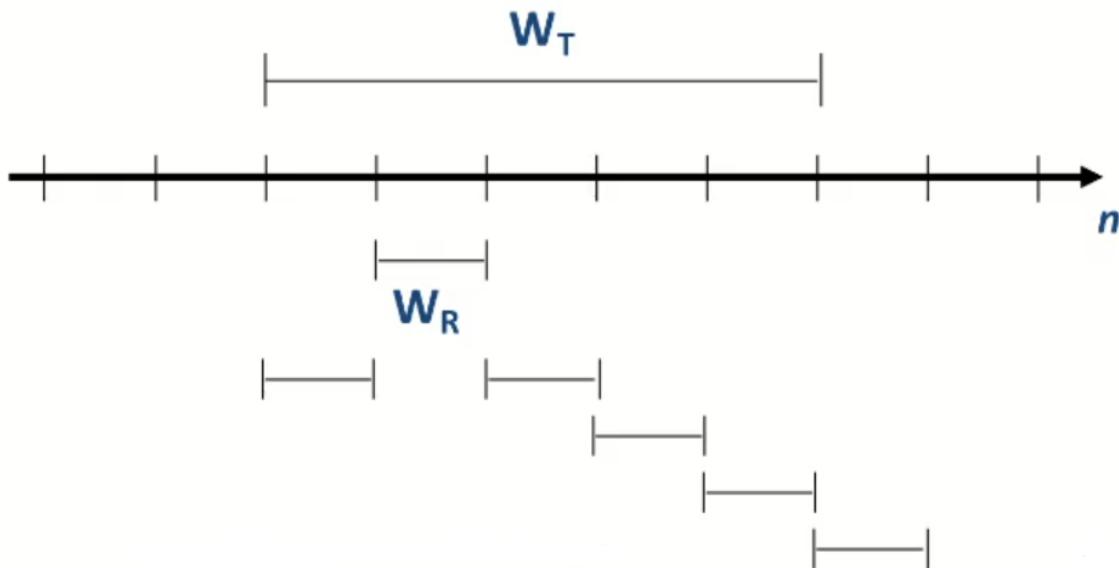
Permette risparmio di ACK.

POSIZIONI RELATIVE CORRETTE TRA W_T e W_R

W_T e W_R possono solo trovarsi nelle seguenti posizioni reciproche:

- W_R all' "interno" di W_T o massimo alla "casella" successiva a quella finale della finestra di trasmissione

Altre posizioni danno luogo a malfunzionamenti.



NUMERAZIONE PDU (GO-BACK-N)

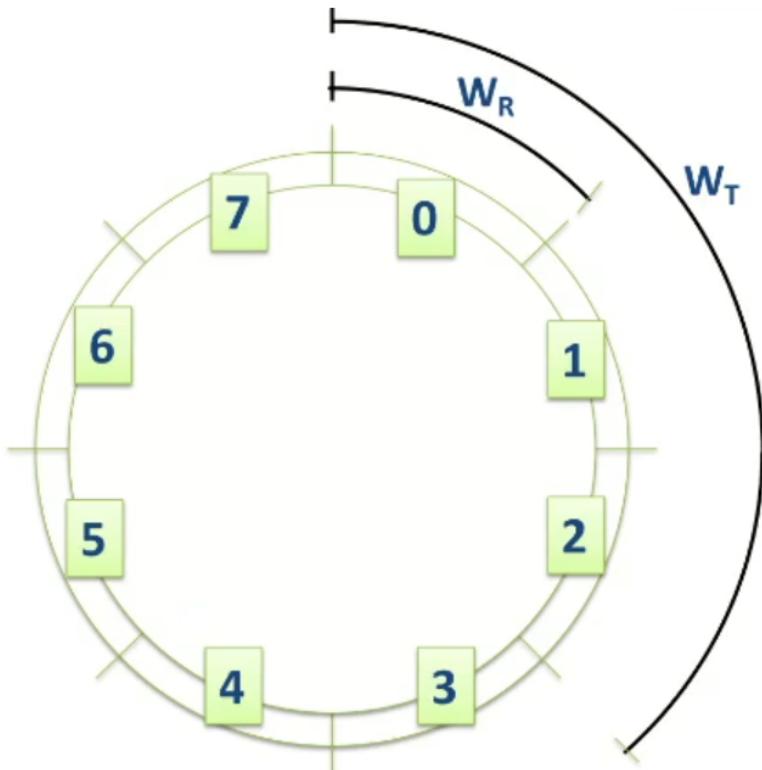
La numerazione delle PDU è ciclica:

- k bit di numerazione
- numerazione modulo 2^k

3 bit di numerazione

$$W_R = 1$$

$$W_T = 3$$



Ma quale può essere la relazione tra la numerazione delle PDU e la W_T ?

Tre possibili casi:

- $2^k < W_T \rightarrow \text{non funziona}$
- $2^k = W_T \rightarrow \text{non funziona}$
- $2^k > W_T \rightarrow \text{funziona}$

QUIZ 1:

Un nodo che usa un protocollo a finestra Go-Back-N con semantica cumulativa degli ACK per ricevere dati da un altro nodo si vede recapitare una PDU duplicata. Quale delle seguenti azioni intraprende?

- A. invia sempre un ACK relativo al numero di sequenza atteso
- B. invia sempre un ACK relativo al numero di sequenza della PDU duplicata
- C. se la PDU rientra nella finestra di ricezione, invia sempre un ACK relativo al numero di sequenza della PDU duplicata
- D. invia un ACK relativo al numero di sequenza atteso solo se non è ancora scaduto il timeout del trasmettitore

Risposta corretta: A.

QUIZ 2:

Un protocollo a finestra di tipo go-back-N con finestra W_T prevede che:

- A. nel momento in cui una PDU è ricevuta con un errore siano ritrasmesse le ultime W_T unità dati
- B. il trasmettitore riceva i riscontri per le ultime W_T PDU trasmesse prima di poter iniziare la trasmissione di altre PDU

C. il trasmettitore non possa inviare più W_T PDU prima di aver ricevuto almeno almeno un ACK di quelle inviate

D. ogni volta che scade un time-out siano ritrasmesse le W_T PDU precedenti all'ultima PDU confermata

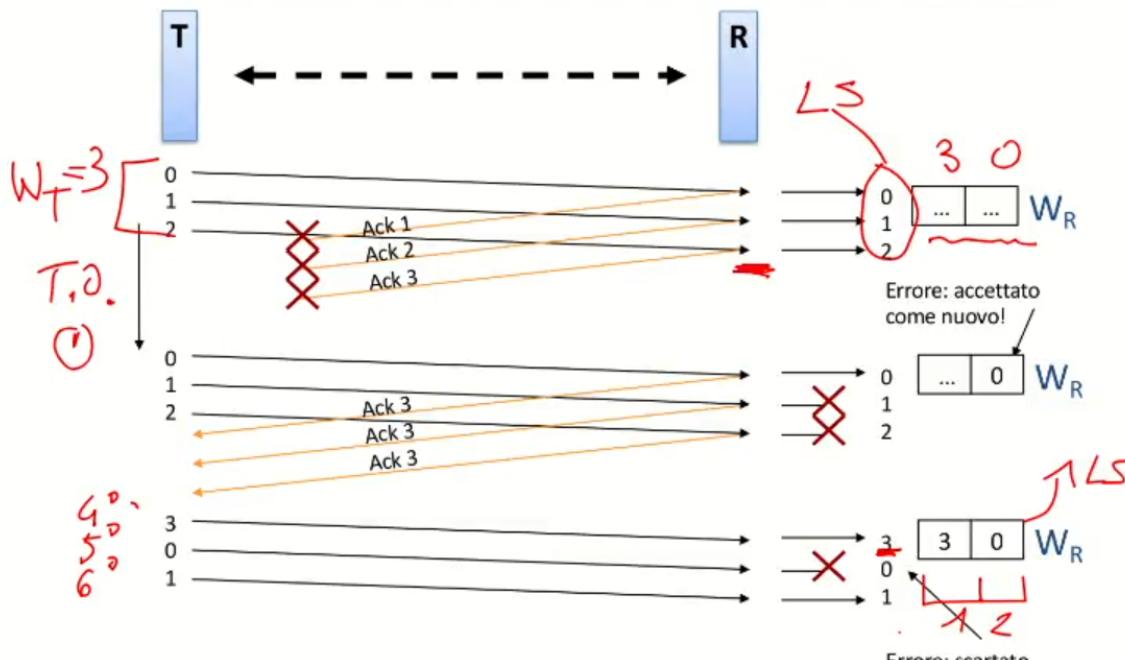
Risposta corretta: C.

NUMERAZIONE PDU (SELECTIVE-REPEAT)

Nel protocollo selective repeat vale la relazione:

$$W_T + W_R \leq 2^k$$

Nel caso in cui ad esempio $W_T(3) + W_R(2) > 2^k(4)$:



Copyright Gruppo Reti – Politecnico di Torino

76

EFFICIENZA E THROUGHPUT

Throughput in un canale a capacità C:

$$\theta = \eta C$$

Posso regolare il throughput agendo su:

- dimensione della finestra
- Round Trip Time (RTT)

QUIZ:

Un nodo che usa un protocollo a finestra Selective Repeat con semantica cumulativa degli ACK per ricevere dati da un altro nodo si vede recapitare una PDU duplicata. Assumendo che nessun dato sia stato perso, quale dei seguenti motivi è più probabilmente la causa di questo comportamento?

- A. il timeout del trasmettitore è troppo breve
- B. il timeout del trasmettitore è troppo lungo

C. la finestra del trasmettitore è troppo piccola

D. la finestra del ricevitore è troppo piccola

Risposta corretta: A.

QUIZ:

Se un nodo che usa un protocollo a finestra dà riceve una PDU fuori sequenza e con i bit di parità errati:

A. scarta la PDU e non invia alcun ACK

B. scarta la PDU e invia un ACK del numero di sequenza atteso

C. invia un ACK relativo al numero di sequenza contenuto nella PDU ma scarta la PDU

D. inserisce la PDU in memoria se questa rientra nella finestra di ricezione, senza inviare alcun ACK.

Risposta corretta: A. (*sembra B ma fidatevi, non lo è*)

QUIZ:

In un intervallo di tempo T, un nodo trasmettitore che usa un protocollo a finestra Go-Back-N con finestra pari a 10 PDU trasmette le PDU numerate 13, 14 e 15 e riceve ACK (cumulativi) 5 e 6. Assumendo che ACK sia quello con numero di sequenza più alto ricevuto fino a questo punto, quale delle seguenti azioni è consentita dalle regole del protocollo in questa situazione?

A. nessuna azione fino alla ricezione di altri ACK

B. inviare la PDU 16

C. inviare le PDU 16 e 25

D. ritrasmettere le PDU da 7 in avanti

Risposta corretta: A.

STRATO FISICO (1)

MEZZI TRASMISSIVI

Possono essere:

- *elettrici*
- *ottici*
- *radio*

MEZZI TRASMISSIVI ELETTRICI

Presentano:

- *resistenza, capacità parassite e impedenza basse*
- *buona resistenza alla trazione*

- *flessibilità*
- *facilità di collegamento dei ricetrasmettitori*

Le caratteristiche dipendono da:

- *geometria*
- *numero di conduttori a distanza reciproca*
- *tipo di isolante*
- *tipo di schermatura*

Parametri di merito:

- *impedenza (in funzione della frequenza)*
- *velocità di propagazione (0.5c-0.7c per cavi e 0.6 per fibre ottiche)*
- *attenuazione (cresce linearmente, in dB, con la distanza e la radice quadrata della frequenza)*
- *Diafonia o Cross-Talk (misura del disturbo indotto da un cavo vicino - cresce con la distanza fino a stabilizzarsi)*

IL DOPPINO

Detto anche coppia (pair). è il mezzo trasmittivo classico della telefonia. Si tratta di due fili di rame ritorti (binati, twisted) per ridurre le interferenze elettromagnetiche usando tecniche trasmissive differenziali. Hanno costi ridotti e un'installazione semplice.

CAVO COASSIALE

Composto da un connettore centrale e una o più calze di schermo. Soffre di minori interferenze, in quanto ha una maggiore schermatura dai disturbi esterni (gabbia di Faraday). Ha costi elevati e una maggiore difficoltà di installazione.

MEZZI TRAMISSIVI OTTICI

FIBRA OTTICA

Minuscolo e flessibile filo di vetro costituito da due parti (**core** (interno) e **cladding** (subito esterno al core)) con indici di rifrazione diversi. Per la *legge di Snell*, il raggio luminoso introdotto nella fibra entro un "angolo di accettazione" rimane confinato nel core.

Vantaggi:

- *totale immunità da disturbi elettromagnetici*
- *alta capacità trasmittiva (fino a decine di Terabit/s)*
- *bassa attenuazione, dipendente dalla lunghezza d'onda*
- *dimensioni ridotte e costi contenuti*

Svantaggi:

- *adatte solo a collegamenti punto-punto*
- *difficili da collegare tra loro e con connettori*
- *ridotto raggio di curvatura*
- *soffre vibrazioni*

MEZZI TRAMISSIVI RADIO

CANALE RADIO (MOBILE)

Noto anche come "etero". Supporta la propagazione di segnali inviati da un trasmettitore ad uno o più ricevitori mediante l'uso di antenne. Se almeno uno tra TX e RX è in movimento, si parla di canale *radiomobile*.

(Idealmente) La qualità dipende dal rapporto tra:

- *potenza ricevuta*
- *potenza trasmessa*

La potenza ricevuta dipende dal quadrato di frequenza e distanza:

$$\frac{P_R}{P_T} = G_T G_R \frac{\lambda^2}{(4\pi D)^2}$$

con λ = lunghezza d'onda, D = distanza TX/RX.
 G_T e G_R sono i guadagni di TX e di RX.

(Realmente) La potenza ricevuta è anche soggetta ad attenuazione dovuta a:

- *fenomeni atmosferici*
- *interferenza da sorgenti sulla stessa frequenza*
- *ostacoli fissi e in movimento* → la loro presenza determina **riflessioni** e **rifrazioni**, che producono copie del segnale trasmesso, disturbando la ricezione:
 - *fading* (variazione veloce del segnale dovuta all'azione delle copie ricevute da percorsi diversi dall'originale)
 - *shadowing* (variazioni lente dell'ampiezza del segnale)

QUIZ:

In un cavo UTP (Unshielded Twisted Pair) la trasmissione del segnale avviene sfruttando:

- A. la differenza tra le tensioni di coppie diverse di conduttori
- B. la differenza tra la tensione di un singolo conduttore e la "terra"
- C. la differenza tra le tensioni sui componenti di una coppia di conduttori
- D. la differenza tra la tensione di un singolo conduttore e la calza metallica

Risposta corretta: C.

CODIFICHE

CODIFICHE UNIPOLARI

Molto semplici e "primitive". Usano il livello di tensione 0 per "0" e uno per "1".

Problemi:

- *in mezzi elettrici, un segnale con componente continua non nulla può venire filtrato da alcuni sistemi*
- *perdita di sincronismo se trasmetto lunghe sequenze dello stesso simbolo*
- *in mezzi ottici, lunghe sequenze di "1" (luce) possono portare al sovraccarico del LED di trasmissione*

CODIFICHE POLARI

Usano due livelli di tensione con polarità diverse (si riduce la componente continua).

Esistono 3 varianti:

- *NRZ (Non-Return-to-Zero) → non c'è transizione su tensione nulla nel passaggio tra due bit consecutivi*
- *RZ (Return-to-Zero) → transizione su tensione nulla tra due bit consecutivi*
- *Bifase (es. Manchester) → ogni bit rappresentato da due livelli di tensione di polarità inversa*

Le bifase sono migliori per il sincronismo, ma RZ e bifase richiedono bit rate elevati.

CODIFICHE BIPOLARI

Chiamate anche AMI (Alternate Mark Inversion).

Si usa tensione nulla per rappresentare "0" e due polarità opposte per "1", usate in alternativa. Permettono l'uso di simboli ternari (-1, 0, +1), come nella codifica 8B6T (8 bit codificati con 6 simboli ternari).

Si basano sull'utilizzo di **codebook**.

CODIFICHE nBmB

Si tratta di codifiche in cui simboli di **n** bit sono rappresentati da simboli di **m** bit, con **n < m**.

Molto popolari perché:

- *richiedono meno banda di codifiche polari*
- *permettono il controllo sulla scelta delle parole di codice, limitando quelle con troppi 0 e 1 consecutivi*
- *limita la componente continua*
- *fornisce caratteri speciali per delimitazione pacchetti, trasmissione in idle o padding*

Si basano sull'utilizzo di **codebook**.

MODULAZIONI DIGITALI

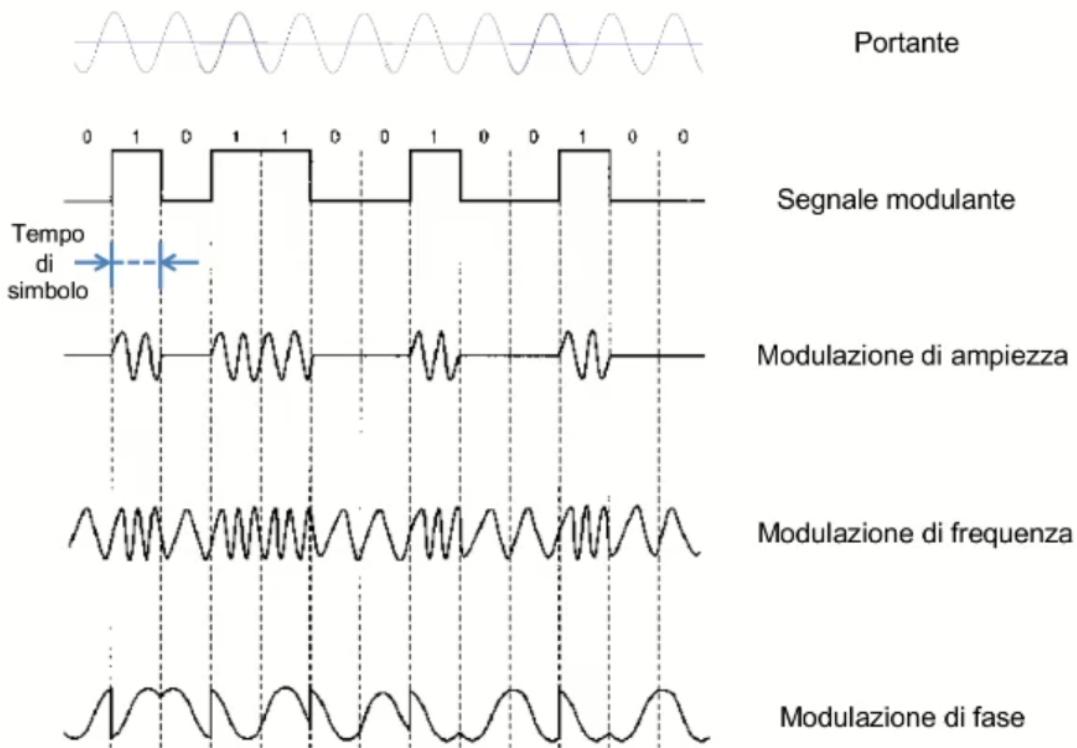
Si tratta di tecniche per la rappresentazione di informazioni numeriche mediante segnali analogici su mezzi radio, ottici ed elettrici. L'informazione è impressa su di un segnale sinusoidale portante (*carrier*) variandone l'ampiezza, la frequenza, la fase o loro combinazioni.

Alcune di queste tecniche sono:

- *modulazione di ampiezza (ASK - Amplitude Shift Keying)*
- *modulazione di frequenza (FSK - Frequency Shift Keying)*
- *modulazione di fase (PSK - Phase Shift Keying)*
- *QAM - Quadrature Amplitude Modulation (una combinazione di variazioni)*

Solitamente la sigla è preceduta da un numero che indica il numero di simboli del segnale modulante.

Esempio: 8-PSK.



QUIZ:

Quale delle seguenti opzioni è più realistica per una codifica di tipo 8B10B?

- la codifica **10101010** può rappresentare i dati utente **1111111110**
- la codifica **11111110** può rappresentare i dati utente **1010101010**
- la codifica **1111111110** può rappresentare i dati utente **10101010**
- la codifica **1010101010** può rappresentare i dati utente **11111110**

Risposta corretta: D.

RETI DI ACCESSO

Per arrivare all'utenza residenziale, l'ultima tratta di rete è detta **rete d'accesso (local loop)**.

Principali tecnologie nelle reti di accesso:

- *Digital Subscriber Loop (DSL)*
- *Reti di accesso ottiche (PON)*
- *Reti ibride ottico-coassiali (HFC)*
- *Accesso Broadband Mobile (reti cellulari)*

Tecnologie secondarie e obsolete:

- *reti via radio Wi-MAX*
- *reti ISDN*
- *reti satellitari*

DSL E ADSL

DSL è una famiglia di tecnologie (chiamate anche xDSL) → fornisce servizio dati ad alta velocità sulla rete di accesso

La più diffusa è ADSL (Asymmetric DSL):

- velocità maggiore in *downstream* che in *upstream*
- pensata per applicazioni client-server

Hanno un bit rate dedicato fino al nodo di accesso.

ACCESSO DSL: IL MODEM

Deriva da: **M**odulatore e **D**emodulatore.

Si utilizza per effettuare trasmissioni digitali su cavi della rete telefonica pubblica:

- trasformano il segnale da digitale ad analogico e viceversa
- rendono il segnale idoneo alla trasmissione su rete pubblica in tecnologia analogica su bande adiacenti a quella fonica

ADSL: APPARATI UTENTE

Filtro Splitter → ha il compito di separare il segnale vocale dai dati

Modem → (de)modula il segnale alle frequenze opportune (es. per ADSL dai 25KHz in upstream ai 240 KHz in downstream)

ADSL: APPARATI DI CENTRALE

Filtro/modem POTS → funzione duale del filtro splitter dell'utente, separa flussi voce e dati

DSLAM (DSL Access Multiplexer) → riceve flussi dati diversi e li convoglia su un unico canale

VDSL

In ambiente urbano e su distanze contenute, VDSL (very-High-Rate DSL) permette di aumentare ulteriormente i bit rate:

- migliori standard di trasmissione e modulazione
- bande di frequenza superiori ad ADSL2+

DISTANZA E VELOCITA'

La velocità in downstream diminuisce al crescere della distanza, a causa di attenuazione e rumore. Occorre ridurre la lunghezza della tratta VDSL (in rame).

PASSIVE OPTICAL NETWORKS (PON)

Architettura per la connettività di ultimo miglio in fibra ottica senza componenti attivi (ossia non alimentati elettricamente):

- da una centrale
- al punto più vicino agli utenti residenziali

Un PON è composto da:

- OLT (Optical Line Terminator) in centrale
- ONU (Optical Network Units) nelle cabine di strada
- ONT (Optical Network Terminals) a casa dell'utente
- ODN (Optical Distribution Network)

La PON sostituisce (FTTH - Fiber-to-the-home) o integra (FTTC - Fiber-to-the-cabinet) la connettività VDSL

- alte velocità (tratta in rame più breve quindi meno attenuazione)
- costi elevati (posa delle fibre al posto del rame)

RETI MOBILI A BANDA LARGA

Offrono servizi voce/dati ad utenti residenziali o in mobilità. Sostituiscono o affiancano la connettività ADSL.

Soluzioni tecnologiche:

- reti cellulari (tutto il territorio)
- reti Wi-MAX, Hiperlan (aree rurali)
- reti satellitari

Principio → copertura capillare del territorio mediante antenne di portata limitata:

- a coperture piccole corrispondono bit rate elevati
- le risorse sono condivise da un numero minore di utenti, ma comportano un costo maggiore per l'operatore

Danno supporto alla mobilità degli utenti:

- roaming → rintracciabilità dell'utente sul territorio
- handover → continuità della connessione nel passaggio da una cella all'altra

Esistono diverse tecnologie, tra cui UMTS (3G), LTE (4G), NR (5G). Oggi usiamo le diverse generazioni in base al luogo in cui ci troviamo:

- in una valle poco frequentata in montagna:
 - Voce: GSM
 - Dati: GPRS (2G), forse EDGE, probabilmente nulla
- in campagna:
 - Voce: GSM e 3G
 - Dati: GPRS, EDGE e 3G
- su un'autostrada:
 - Voce: GSM e 3G
 - Dati: GPRS, EDGE, 3G e LTE
- in città:
 - Voce: GSM, 3G e 4G VoLTE
 - Dati: GPRS, EDGE, 3G e LTE (presto 5G)

Gli operatori continuano ad usare GSM per la telefonia perché:

- la rete è già dimensionata per le telefonate
- l'infrastruttura c'è già
- non si consuma preziosa banda dati delle reti 3G e LTE

ARCHITETTURA DI UNA RETE CELLULARE (LTE)

Divisa in rete di accesso (Access Network) e rete di core (Core Network).

RETI DI TRASPORTO

Creano l'interconnessione tra reti di accesso. Come nodi, hanno commutatori telefonici e dati (*router*) in una topologia magliata e gerarchica. Questi nodi sono connessi da linee ad alta velocità (solitamente in fibra ottica).

Questo tipo di reti vengono gestite da più operatori telefonici o dati (ISP) in competizione:

- *alcuni operatori sono proprietari delle infrastrutture*
- *altri affittano l'infrastruttura ed offrono solo il servizio di trasporto (operatori virtuali)*

TRASMISSIONE SU RETI DI TRASPORTO

La trasmissione:

- *è interamente digitale*
- *si è evoluta dalla rete telefonica tradizionale*
- *è strutturata secondo principi di multiplazione gerarchica a divisione di tempo*

SINCRONIZZAZIONE

PDH

I sistemi di multiplazione gerarchica si sono evoluti a partire dalla Plesiochronous Digital Hierarchy (PDH):

- pensata per canali vocali numerici a 64Kb/s
- non usa Store-and-Forward → occorre una stretta sincronizzazione end-to-end tra TX e RX
- sistemi quasi-sincrono (plesio-synchronous) con orologi solo nominalmente entro margini di tolleranza
- inserzione/rimozione dinamica di bit lungo il percorso (bit stuffing) per mantenere il sincronismo
- velocità di trasmissione limitate
- standard diversi in USA/Europa/Giappone

SONET/SDH

L'attuale infrastruttura della rete di trasporto è in larga misura basata sulle gerarchie sincrone:

- *SONET → Synchronous Optical NETwork*
- *SDH → Synchronous Digital Hierarchy (equivalente europea ed internazionale di SONET)*
- *STS → Synchronous Transport Signal (standard corrispondente per i segnali elettrici)*

La topologia è spesso ad anelli bidirezionali per motivi di affidabilità (recupero automatico dai guasti).

QUIZ:

Nella connettività di ultimo miglio (dalla cabina all'utenza), al decrescere della lunghezza del cavo in rame:

- A. cresce l'attenuazione, aumentando la capacità del canale
- B. diminuisce la componente di rumore, diminuendo la capacità del canale
- C. diminuisce l'attenuazione, aumentando il bit rate
- D. cresce la componente di rumore, diminuendo il bit rate

Risposta corretta: C.

STRATO COLLEGAMENTO (2)

Ha diverse funzioni:

- *delimitazione trama*
 - *delimitatori esplicativi*
 - *indicatori lunghezza*
 - *lunghezza fisica*
 - *silenzio tra pacchetti*
- *multiplazione* → tecnica attraverso la quale lo strato tiene memoria dei protocolli utilizzati per l'elaborazione di una PDU (cosicché il ricevitore (nello stesso strato) sa quale protocollo utilizzare). (**Non confondere con la multiplazione vista precedentemente (di canale)**)
- *indirizzamento locale*
- *rivelazione errore*
- *controllo di flusso (con protocolli a finestra)*
- *controllo di sequenza (protocollo a finestra)*
- *correzione errore (con protocolli a finestra)*
- *protocolli accesso multiplo (solo per canali condivisi)*
- *controllo di flusso sull'interfaccia (verso livelli superiori)*

PROTOCOLLI

Derivano dal protocollo SDLC (Synchronous Data Link Control) utilizzato nell'architettura IBM SNA.

L'ANSI ha standardizzato SDLC come ADCCP (Advanced Data Communication Control Procedure) e l'ISO come HDLC (High-level Data Link Control).

Alla stessa famiglia di protocolli che derivano da HDLC appartengono:

- *LLC 802.2 (Logical Link Control - LAN)*
- *PPP (Point-to-Point Protocol - ADSL)*
- *LAPDm (LAP for the mobile D channel - GSM)*

I protocolli di strato 2 sono usati:

- *in reti pubbliche di accesso* → collegamenti punto-punto dalla casa/sede dell'utenza alla rete di un gestore (rete di accesso)
- *in reti private (locali)* → reti per interconnettere apparati in ambienti circoscritti (lab, uffici, data center, ecc.) con prevalenza di collegamenti broadcast

STRATO 2 NELLE RETI PUBBLICHE

- *DTE* → *Data Terminal Equipment (apparati utente)*
- *DCE* → *Data Circuit-terminating Equipment (apparati del gestore)*

I protocolli di strato 2 vengono utilizzati principalmente nei canali tra cabina e modem. Le loro principale funzioni sono:

- *delimitare i pacchetti (PDU)*
- *rilevazione del funzionamento corretto del collegamento*

CARATTERISTICHE COMUNI

- Formato *generico* delle PDU nelle reti pubbliche e private:



- i protocolli sono orientati al bit (*in disuso*) o al byte (come LLC 802.2 e PPP)
- il flag di delimitazione 01111110 non può comparire nella PDU per garantire la trasparenza dei dati
- l'indirizzo server per le configurazioni multipunto (master/slave)
- il campo protocollo differenzia le PDU

Nella figura sopra, il CRC è il Cyclic Redundancy Check: è una sequenza di bit che si occupa di effettuare il controllo di parità.

TRASPARENZA NEL TRASFERIMENTO DATI

Occorre evitare che il flag possa essere scambiato per una sequenza 01111110 nella SDU dallo strato superiore (e negli altri campi della PCI).

Esistono 2 tecniche principali con questo scopo:

- *bit stuffing* → usata su mezzi fisici sincroni e per protocolli orientati al bit (*in disuso*)
- *byte stuffing* → usata su mezzi asincroni con protocolli orientati al byte

BYTE STUFFING

Fasi:

- il trasmettitore inserisce un byte di escape 01111101 prima di ogni byte 01111110 o 01111101 di dati
- il ricevitore scarta il primo 01111101 della coppia

PROTOCOLLO PPP - RFC 1661

E' utilizzato nei collegamenti su linea telefonica o ADSL tra host di utenza residenziale e provider Internet, oltre che su connessioni SONET/SDH.

Il collegamento punto-punto cablato è più facile da gestire rispetto a collegamenti radio o a canali broadcast in generale.

PPP è diviso in tre sotto-protocolli:

- *Incapsulamento (delimitazione delle PDU)*
- *LCP (Link Control Protocol)*
- *NCP (Network Control Protocol)*

Obiettivi di PPP:

- *delimitazione delle PDU*
- *trasparenza del contenuto (byte stuffing)*
- *riconoscimento (non correzione) degli errori*
- *multiplazione di più protocolli di strato rete*
- *controllo dell'attività sul collegamento*
- *negoziazione dell'indirizzo di livello rete (tipicamente IP) → i nodi ai due estremi del collegamento apprendono o configurano i propri indirizzi di rete*
- *semplicità*

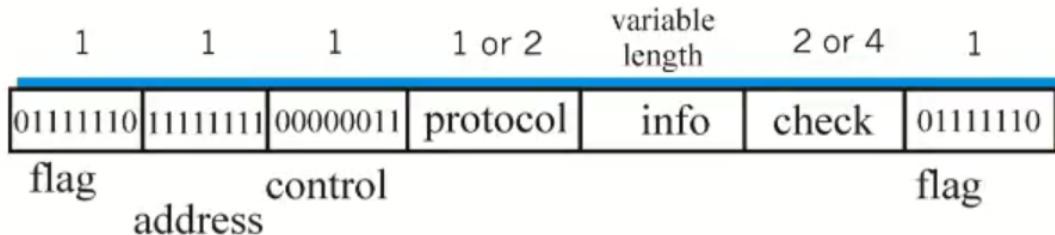
Non obiettivi di PPP:

- *correzione o recupero degli errori*
- *controllo di flusso*
- *mantenimento della sequenza*
- *gestione di collegamenti multipunto*

INCAPSULAMENTO

Struttura di una trama PPP:

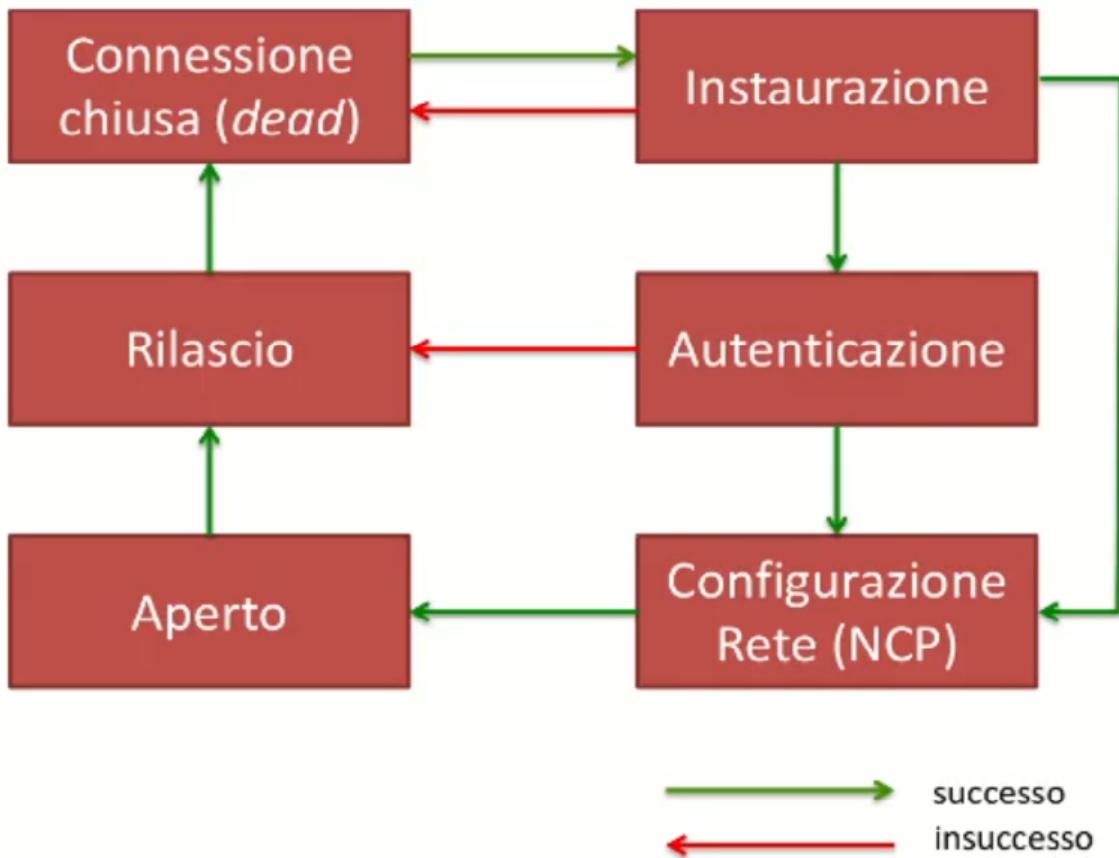
- *flag → delimitatore per il "framing"*
- *address → non ha significato (mantiene compatibilità con HDLC)*
- *control → come per address*
- *protocol → protocollo di livello superiore cui destinare i dati*



LCP - LINK CONTROL PROTOCOL

Serve a creare e abbattere il collegamento PPP, negoziando le opzioni:

- *inizia nello stato di DEAD*
- *opzioni:*
 - *max frame length*
 - *authentication protocol*
 - *skip address and control fields*
- *una volta stabilito il collegamento PPP e fatta l'autenticazione, è configurata la tipologia di connessione*



NCP - NETWORK CONTROL PROTOCOL

Interviene dopo l'eventuale autenticazione con successo:

- *definisce le modalità di trasferimento delle unità dati*
- *negozia l'assegnazione di un indirizzo*

Per ogni protocollo di livello superiore, esiste un diverso protocollo NCP.

PROTOCOLLO ATM

Offre una rete a pacchetto con servizio a circuito virtuale.

Obiettivi e caratteristiche generali:

- *velocità elevate*
- *bassa latenza per il trasporto di voce e video*
- *uso di PDU dette **celle** di dimensione fissa pari a 53 byte (48 di dati + 5 di intestazione)*

Oggi viene utilizzata tra DSLAM e Centrale dell'operatore.

Si basa su un approccio *core and edge*:

- *i nodi "vicini" all'utente (edge) contengono i livelli:*
 - $L1 \rightarrow$ fisico
 - $L2 \rightarrow$ ATM
 - $L2 \rightarrow$ AAL (*si occupa di segmentazione e riassemblaggio dei pacchetti (53 byte)*)
- *i nodi di commutazione ATM (core) contengono:*
 - $L1 \rightarrow$ fisico
 - $L2 \rightarrow$ ATM

ATM e AAL sono due sottolivelli del livello 2.

FORMATO CELLA ATM

Si usano celle di dimensione fissa per ridurre la complessità dei commutatori. Questo tipo di celle (di piccole dimensioni) permettono:

- *bassa latenza*
- *basso ritardo di pacchettizzazione della voce*

L'intestazione della cella ATM (5 byte = 40 bit) è formata da:

- *VPI (12 bit) → Virtual Path Identifier (percorso definito tra più commutatori ATM)*
- *VCI (16 bit) → Virtual Circuit Identifier (identifica il singolo circuito virtuale all'interno di un VP)*
- *PT (3 bit) → Payload Type (classifica il tipo di informazione presente nel payload)*
- *CLP (1 bit) → Cell Loss Priority*
- *HEC (8 bit) → Header Error Code*

AAL: ATM ADAPTATION LAYER

Integra il trasporto ATM per offrire differenti servizi ai livelli superiori.

All'inizio aveva 5 funzioni specifiche, ora ne rimane una sola, la AAL-5:

- *gestisce la segmentazione e il riassemblaggio delle unità dati (SDU) generando più (N-1)-SDU da una (N)-SDU*

Come avviene questa segmentazione?

- *Alla PDU di livello 3 è aggiunta una "coda" (trailer) con padding, lunghezza e CRC*
- *3-PDU e coda sono divisi in segmenti di 48 byte e inseriti in ordine in celle ATM*
- *L'ultima cella ha il terzo bit del campo PT nell'intestazione ATM a 1 (permette di ricostruire il pacchetto dai segmenti)*

STRATO 2 NELLE RETI PRIVATE/LOCALI

Il livello 2 è diviso in due sottolivelli:

- *LLC → Logical Link Control (derivato da HDLC)*
- *MAC → Medium Access Control*

IEEE 802.2 LLC

Principali caratteristiche:

- *protocollo orientato al byte*
- *non si utilizzano delimitatore (delimitazione delegata al MAC)*
- *non si controllano gli errori (non c'è il campo CRC)*
- *PDU contengono indirizzo sorgente e indirizzo destinazione*
- *PDU di dimensione variabile*

FORMATO PDU LLC

Il campo di controllo è di 8 bit nelle PDU non numerate, di 16 nelle PUD numerate.

| **La dimensione massima dipende dai vincoli dello strato MAC.**

SNAP PDU

Si tratta di una porzione di PDU, formata da:

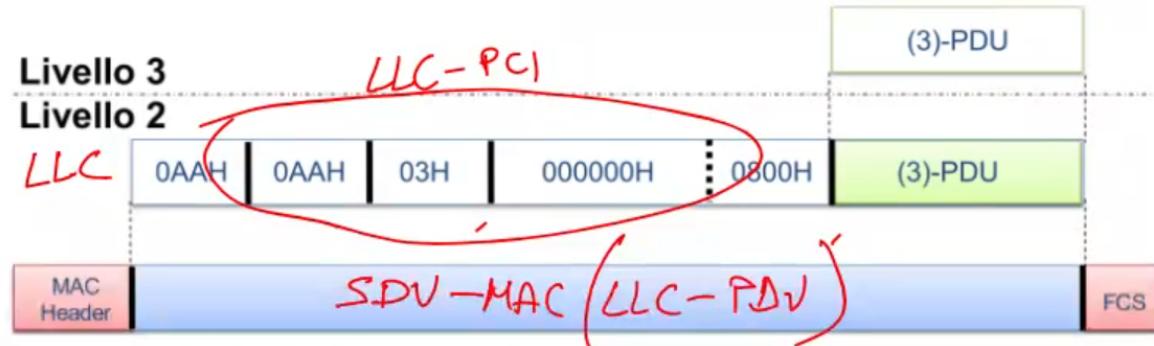
- *OUI → identificativo di chi assegna il PT*

- *PT (Protocol Type) → indica il protocollo utilizzato (es. IP)*

INTESTAZIONE SNAP PDU

Rispetto allo standard LLC, l'intestazione è formata da:

- *DSAP → Destination Service Access Point*
- *SSAP → Source Service Access Point*
- *controllo → utilizzato per funzioni aggiuntive (es. controllo di flusso)*



CARATTERISTICHE RETI LOCALI

LAN = Local Area Network.

Principali caratteristiche:

- *piccola estensione geografica*
- *se uso mezzo trasmissivo condiviso → può trasmettere solo un nodo alla volta*
 - *motivazioni:*
 - *un canale dedicato sarebbe male utilizzato*
 - *quando trasmetto voglio alta velocità*
 - *trasmissione broadcast*
 - *comodo per traffico broadcast e multicast*
 - *si deve inserire l'indirizzo del destinatario per unicast*
- *topologie*
 - *bus, anello, stella, bus monodirezionale*

CONDIVISIONE DI UN CANALE (PROTOCOLLI PER LAN)

Tre famiglie principali:

- a contesa o accesso casuale (Ethernet, Wifi)
- ad accesso ordinato (Token Ring, Token Bus, FDDI)
- a slot con prenotazione (DQDB)

Gli unici ancora utilizzati sono i primi.

I parametri utilizzati per valutare protocolli LAN sono:

- *capacità e traffico smaltito (throughput)*
- *equità*
- *ritardo (accesso, propagazione, consegna)*
- *numero di nodi (stazioni), lunghezza della rete, topologia, facilità di realizzazione, robustezza*

MAC - PROTOCOLLI AD ACCESSO CASUALE

Quando un nodo deve trasmettere:

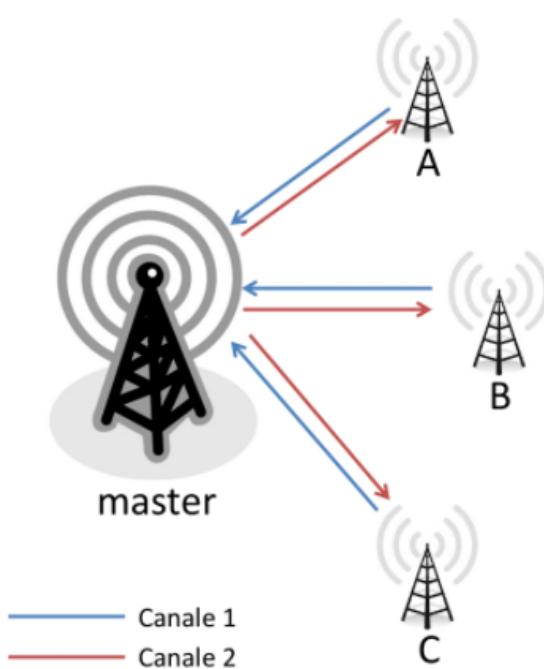
- trasmette la trama alla velocità R del canale
- senza coordinarsi con altri nodi

Si possono verificare problemi di **collisione**. I protocolli ad accesso casuale indicano:

- come rendere meno probabile la collisione
- come riconoscere la collisione
- come recuperare a fronte di collisione (ritrasmissione)

ALOHA

Idea → commutazione di pacchetto su onde radio



- Canali broadcast 1 e 2 multiplati in frequenza
 - Stazioni A, B, C trasmettono su canale 1 e ricevono su 2
 - Master trasmette su 2 e riceve su 1
- Se A ha una trama per C, la trasmette sul canale 1
- Se Master riceve la trama, la ritrasmette sul canale 2
 - C riceve la trama
 - A sente la trama ed ha conferma di ricezione
- Collisioni possibili solo su canale 1 (condiviso)

E' un procollo molto semplice:

- inizio trasmissione in qualunque istante
- conferma ricezione su canale separato senza collisioni
 - Stop&Wait → in caso di collisione ritrasmetto la trama dopo un timeout
- probabilità di collisione elevata

Per risolvere le collisioni, si esegue un **backoff**:

- le due (o più) stazioni che hanno colpito aspettano un tempo casuale prima di ritrasmettere la PDU:
 - il tempo casuale serve per rompere il determinismo (se aspettassero lo stesso tempo si avrebbe di nuovo collisione con probabilità 1)
- in caso di ulteriore collisione, si raddoppia il massimo tempo di attesa casuale (backoff esponenziale)

SLOTTED ALOHA

Idea → tempo diviso in slot di uguale dimensione

I nodi trasmettono all'inizio di uno **slot**.

Se c'è collisione → ritrasmetto in altro slot con probabilità p (equivalente a backoff) fino al successo

Sono entrambi protocolli semplici con:

- *throughput limitato a valori bassi (collisioni):*
 - sotto ipotesi di traffico uniforme e infiniti utenti si ottiene efficienza massima 0.18 (ALOHA) o 0.37 (SLOTTED ALOHA)
 - dipende dal tipo di traffico
- *ritardi di accesso non calcolabili a priori in modo deterministico (accesso casuale)*

CSMA (CARRIER SENSE MULTIPLE ACCESS)

Aloha ha una bassa efficienza perché i nodi trasmettono senza coordinarsi tra loro.

Per aumentare il throughput e diminuire le collisioni, posso ascoltare il canale (Carrier sense) prima di trasmettere:

- *se sento canale libero → trasmetto trama*
- *se sento canale occupato → ritardo trasmissione:*
 - **CSMA 1-persistente** → aspetto che si liberi il canale, poi trasmetto immediatamente
 - **CSMA non-persistente** → riprovo a sentire il canale dopo tempo casuale, se libero trasmetto
 - **CSMA p-persistente** → aspetto che si liberi il canale e trasmetto con probabilità p o rimando la trasmissione con probabilità $(1-p)$

L'ultimo tipo di CSMA è teorico, mai implementato.

Con questo protocollo, le collisioni sono **inevitabili** e determinano uno spreco di tempo di trasmissione. Fattori importanti che incidono sulla probabilità di collisione:

- *distanza (ritardo di propagazione)*
- *con trame di grandi dimensioni (nel tempo), a parità di traffico trasmesso, riduco il numero di contese (e quindi di collisioni)*

Varianti del CSMA:

- **CSMA/CD** (*Collision Detection, con rilevazione delle collisioni*) → adatto per mezzi cablati (usata in Ethernet)
- **CSMA-CS** (*Collision Avoidance, con prevenzione delle collisioni*) → adatto per canali radio (usata in WiFi)

CSMA/CD (Collision Detection)

La stazione che trasmette monitora il canale durante la trasmissione:

- *se sente solo la propria trasmissione, prosegue*
- *se sente altre trasmissioni contemporaneamente (collisione), interrompe la propria*

Non occorre conferma di ricezione se la trasmissione si è conclusa senza collisione, **purché la durata minima della trama sia superiore al doppio del tempo massimo di propagazione della rete.**

Dominio di collisione

Porzione della rete in cui, se due stazioni CSMA trasmettono simultaneamente o quasi, le due trame collidono. Se due stazioni sono troppo distanti, la trama raggiunge una delle due quando l'altra ha già terminato di trasmettere → la collisione **NON** viene rilevata!

Vantaggi:

- *se mi accorgo (in fretta) delle collisioni sospendo la trasmissione della trama*
- *riduco lo spreco dovuto ad una trasmissione inutile*

Collision Detection:

- *facile nelle LAN cablate → misuro potenza segnale, confronto segnale ricevuto e trasmesso*
- *non possibile in LAN wireless per modalità half duplex (quando trasmetto, il ricevitore è disattivato)*

Si hanno prestazioni migliori:

- *su reti piccole → riduco periodo di vulnerabilità*
- *su reti piccole rispetto alla dimensione della trama (parametro 'a' piccolo) → collisione rilevata prima, riduco lo spreco*
- *con velocità di trasmissione bassa → pochi bit trasmessi quando rilevo collisione*

Si preferisce la versione **1-persistent** perché migliore a basso carico:

- *ritardo di accesso inferiore*
- *costo collisione piccolo su reti piccole*
- *reti dimensionate per funzionare a basso carico*

NB: è difficile separare traffico a diversa priorità.

PROTOCOLLO UTILIZZATO DALLE RETI Ethernet.

CSMA/CA (Collision Avoidance)

Non potendo usare CSMA/CD su mezzi radio, l'obiettivo è di usare un approccio *conservativo* per prevenire le collisioni.

IN TRASMISSIONE:

Una stazione che deve trasmettere, ascolta il canale:

- *se il canale rimane libero per un periodo detto DIFS (Distributed Inter Frame Space), la stazione inizia la trasmissione*
- *se il canale è occupato (o lo diventa durante DIFS), la stazione sospende la procedura di trasmissione per un tempo casuale di backoff*

Una stazione decrementa il backoff solo mentre il canale rimane libero:

- *quando il backoff arriva a 0, ripete la procedura di TX*

IN RICEZIONE:

Il ricevitore verifica la correttezza della trama:

- *se corretta, risponde con una trama di ACK dopo un tempo SIFS (Short Inter Frame Space) < DIFS (la trama di ACK ha la priorità su ogni altra trama)*

Se il trasmettitore non riceve ACK, dopo un timeout:

- *estrae tempo di backoff e inizia a decrementarlo*
- *quando backoff è 0, riprova la procedura di trasmissione*

Il **tempo di turn around** è il tempo che impiega la scheda di rete a trasformare il suo stato da ricevitore a trasmettitore e viceversa.

Le collisioni si possono comunque verificare in caso di contemporaneo inizio di trasmissione (stesso tempo casuale estratto di backoff):

- *le stazioni coinvolte ripetono la trasmissione "raddoppiando" il massimo backoff*

"Raddoppiando" è tra virgolette in quanto non è un raddoppio preciso, bensì il range di estrazione del numero (casuale) di backoff è **[0,2ⁱ-1]**. La **i** viene incrementata ad ogni trasmissione "fallita", solitamente all'inizio vale 3 o 4 (avendo così range rispettivamente [0,7] o [0,15]).

Con questo tipo di protocollo si hanno migliori prestazioni:

- *su reti piccole → riduco il periodo di vulnerabilità (pari al ritardo di propagazione sul canale)*

PROTOCOLLO UTILIZZATO DALLE RETI WiFi 802.11.

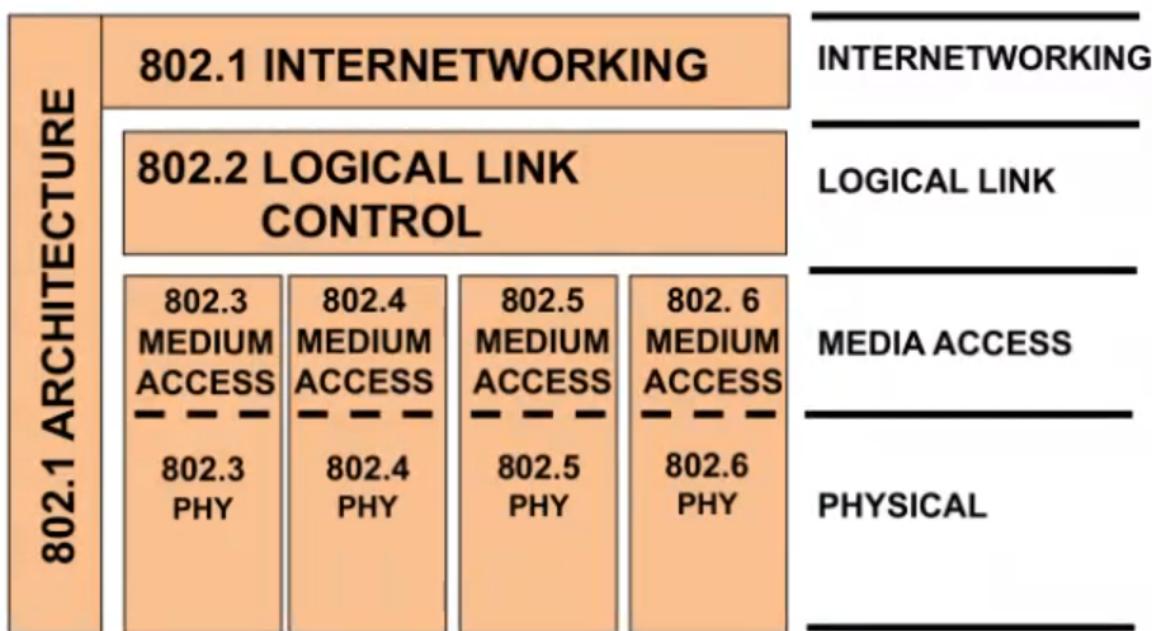
QUIZ:

Considerando la trasmissione di un solo pacchetto in una rete ad accesso multiplo:

- A. il protocollo ALOHA garantisce un ritardo di accesso minore di quello del protocollo SLOTTED ALOHA
- B. il protocollo SLOTTED ALOHA garantisce un ritardo di accesso minore di quello del protocollo ALOHA
- C. il protocollo ALOHA garantisce sempre lo stesso ritardo di accesso di quello del protocollo SLOTTED ALOHA
- D. è preferibile utilizzare un protocollo di accesso ordinato per ridurre il ritardo di accesso

Risposta corretta: A (**NB: un solo pacchetto**).

STANDARD IEEE 802



Un altro standard non menzionato nell'immagine è 802.11, per le reti WiFi.

FUNZIONI STRATO 2 IN RETI LOCALI

- *delimitazione trama*
 - *sottostrato MAC*
- *multiplazione*

- IEEE 802.2 LLC, MAC Ethernet
- rivelazione errore
 - sottostrato MAC
- indirizzamento
 - sottostrato MAC per identificare strada, sottostrato LLC per multiplazione

INDIRIZZI

LLC → permettono la multiplazione di più protocolli di strato superiore

MAC → permettono di identificare la scheda (mittente o destinatario) tra i nodi LAN.

INDIRIZZI MAC

Sono tipicamente di dimensione 6 byte.

All'inizio erano scritti in una ROM della scheda dal costruttore, attualmente sono configurabili via software.

Composti da 2 parti:

- 3 MSB → lotto di indirizzi assegnati al costruttore (OUI - Organization Unique Id)
- 3 LSB → numerazione progressiva interna decisa dal costruttore

Esempio: **EC-22-80-07-9A-4D** è una scheda DLink.

Gli indirizzi MAC possono essere:

- *single o unicast* → se riferiti ad una singola stazione
- *multicast* → se riferiti a gruppi di stazioni
- *broadcast (FF FF FF FF FF FF)* → se riferiti a tutte le stazioni

Una scheda MAC, quando riceve un pacchetto (corretto):

- se l'indirizzo MAC di destinazione coincide con quello di stazione, lo accetta
- se l'indirizzo MAC di destinazione è di tipo broadcast, lo accetta
- se l'indirizzo MAC di destinazione è di tipo multicast, lo accetta se il gruppo multicast è stato abilitato (di norma via sw)

Per motivi principalmente di diagnostica si possono configurare le schede in modo **promiscuo**. In questa modalità tutte le trame vengono inviate ai livelli superiori, indipendentemente dall'indirizzo MAC.

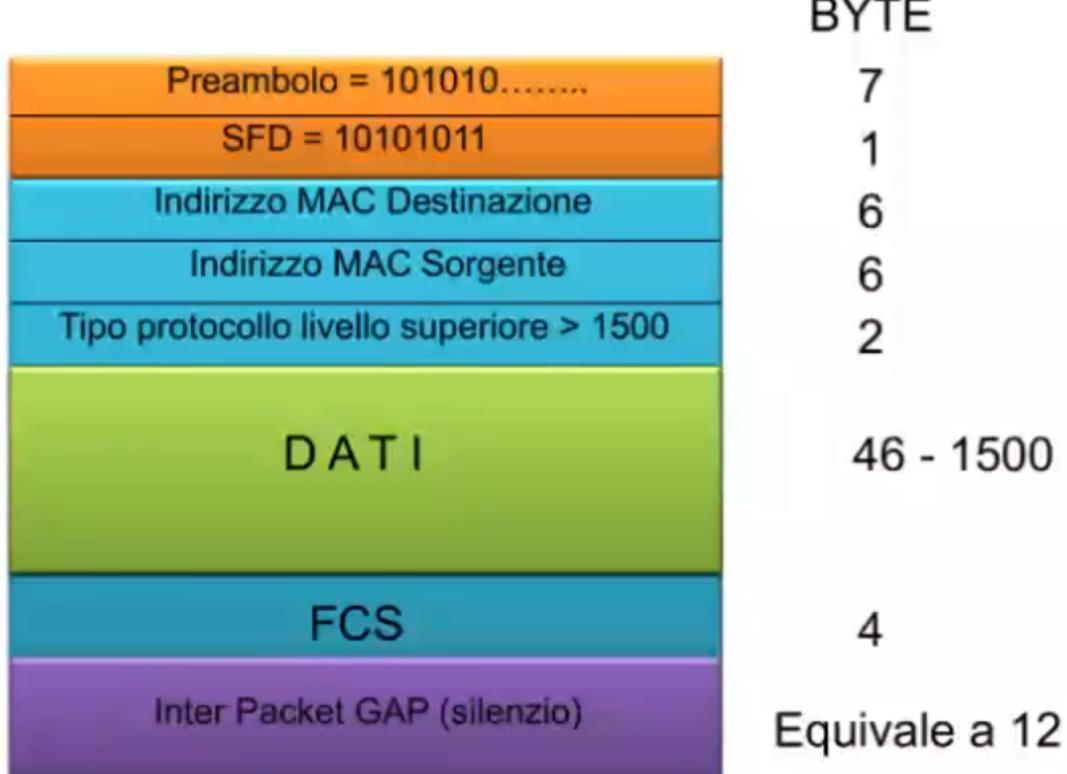
PROTOCOLLO ETHERNET

Funziona come il CSMA/CD 1-persistente.

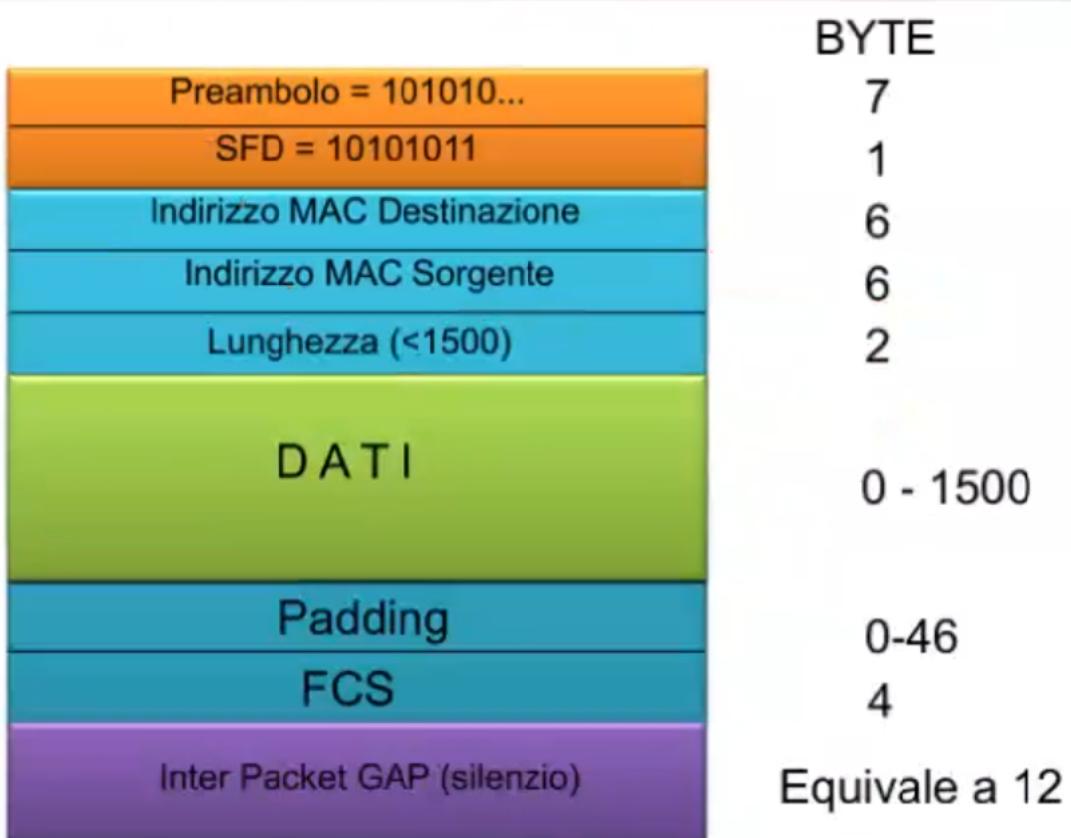
Possono verificarsi collisioni a causa della distanza fisica delle stazioni sulla rete e della persistenza del protocollo:

- se la collisione è rilevata durante la trasmissione, la stazione interrompe la TX e invia una **sequenza di jamming** (sequenza di interferenza)
- le stazioni che hanno colpito attendono un tempo casuale prima di riprovare
- all'avvenuta ricezione non segue una conferma (ACK) alla stazione che ha trasmesso

Ethernet: formato di trama



IEEE 802.3: formato di trama



PARAMETRI DI PROGETTO

- se stazioni sono nello stesso Dominio di Collisione, il tempo minimo di trasmissione di una trama non può essere inferiore al massimo RTT (Round Trip Time)
- la velocità del mezzo trasmissivo e le dimensioni della rete determinano quindi la lunghezza minima della trama
- la lunghezza di trama dipende anche dall'IPG (Inter-Packet Gap), che segnala la fine trama

ETHERNET - LIVELLO FISICO

- Velocità trasmissione → 10 Mb/s
- Codifica Manchester (20 Mbit/s di clock per facilitare recupero sincronismo in rete asincrona)
- Mezzi trasmissivi:
 - 10 BASE 5 → cavo coassiale spesso RG213
 - 10 BASE 2 → cavo coassiale spesso RG58
 - 10 BASE T → doppino UTP da 100 Ohm
 - 10 BASE FL, 10 BASE FB, 10 BASE FP → fibra ottica multimodale, prima finestra

All'inizio, dati i vincoli su RTT e durata di trama, Ethernet prevedeva reti di max 2800m con trame di almeno 64B.

Successivi standard:

- a 100 Mb/s hanno ridotto la distanza massima a 100m
- a 1 Gb/s hanno aumentato la dimensione minima del pacchetto

Oggi tutte le reti Ethernet usano cavi UTP o fibre ottiche.

Si usano solo topologie a stella in cui la contesa (collisioni) e i vincoli su RTT e durata di trama vengono eliminati se **stella attiva**.

LE RETI ETHERNET OGGI

Si tratta di reti più veloci, più affidabili, meno costose.

La topologia è a stella gerarchica, con un centro stella che può essere:

- hub (stella passiva) → banda condivisa
- switch (stella attiva) → banda dedicata

La gerarchia prevede la interconnessione di reti locali Ethernet.

Perché si vuole fare questa interconnessione?

Per aumentare:

- estensione geografica della rete
- numero di utenti collegabili ad una rete
- sicurezza (attraverso segregazione del traffico)

HUB

Apparato multiporta per l'interconnessione di LAN Ethernet che opera al livello 1:

- modello centro-stella passivo → rigenera su **tutte** le porte di uscita la codifica di linea ricevuta su una porta di entrata

Non riconosce le trame, si occupa solo di "smistamento".

Non fa variare la dimensione totale della rete.

E' sempre meno utilizzato.

SWITCH

Apparato multiporta per l'interconnessione di LAN Ethernet che opera al livello 2:

- è un **nodo store-and-forward**:
 - riconosce ma non modifica le trame
 - possibile perdita di pacchetti per overflow delle memorie

Permette di estendere la dimensione della rete.

Grazie al centro-stella attivo:

- ritrasmette in modo selettivo su una o più porte di uscita le trame ricevute su una porta di entrata, secondo le regole del protocollo MAC
- instradamento semplice

Prestazioni potenzialmente superiori agli hub.

Per quel che riguarda le collisioni, si può dire che lo switch le elimini, eliminando anche la necessità quindi del CSMA/CD.

INSTRADAMENTO MEDIANTE SWITCH

Un insieme di segmenti di LAN interconnessi mediante switch è detto anche **LAN estesa**.

La tecnica di switching più diffusa prevede che le stazioni non modifichino il loro comportamento a causa della presenza degli switch (trasparenza).

Ogni switch ha un suo indirizzo unico nella LAN (switch_ID) e un identificativo per ogni porta (port_ID).

TRANSPARENT SWITCHING

- **address learning** → acquisizione di indirizzi e creazione tabella contenente coppie (indirizzo MAC destinazione, port_id dello switch)
- **frame forwarding** → ritrasmissione di trame ricevute con filtraggio degli indirizzi
- esecuzione algoritmo **spanning tree** per eliminare anelli logici da topologia fisica

ADDRESS LEARNING

Indirizzi non memorizzati in modo statico, ma inseriti in tabella in modo dinamico (tabelle (database) inizialmente vuote).

Per ogni trama ricevuta, lo switch:

- legge l'indirizzo MAC sorgente S e lo associa alla porta X da cui riceve la trama (eventualmente cancellando la vecchia entry)
- aggiorna il timer associato alla entry (S,X) → si tratta di un timer che viene settato solo per rendere obsolete le entry dopo un tot di tempo in cui sono rimaste inutilizzate

Algoritmo *backward learning*.

FRAME FORWARDING

Quando riceve una trama corretta con indirizzo MAX unicast con destinazione D da porta X:

- si cerca nel database (tabella) a quale porta è collegato D
- se associato a porta X, si scarta trama
- se associato a porta Y, inoltra trama su Y

- se non presente in tabella, inoltra la trama su tutte le porte attive tranne X

Se ricevo da porta X una trama di tipo multicast e/o broadcast:

- inoltra su tutte le porte (attive) tranne X

SPANNING TREE

Risolve il seguente problema:

- il backward learning funziona solo se in topologia non ci sono anelli

Idea algoritmo:

- crea albero logico tra switch per eliminare anelli, abilitando solo alcune porte

Requisiti:

- identificativo unico switch_ID per ogni switch (indirizzo)
- indirizzo multicast che raggiunga tutti gli switch
- identificativo unico per ogni porta di ogni switch e costo associato ad ogni porta

Alcuni switch non supportano questo algoritmo, perciò possono funzionare solo in topologie fisiche senza anelli.

VANTAGGI INTERCONNESSIONE LAN

Si partiziona la rete in **k** reti locali "indipendenti":

- aumento potenziale banda aggregata di rete

La probabilità di collisione con protocolli a contesa:

- si riduce al crescere del numero di hub
- si elimina con l'uso di switch

La rete locale diventa una rete classica a commutazione di pacchetto.

Nel caso di LAN interconnesse con switch:

- non serve un protocollo d'accesso (Ethernet diventa una tecnica di framing dei dati al livello 2)
- non ci sono limiti di distanza

Si introducono ritardi di store-and-forward.

VLAN: LAN VIRTUALI

Sono LAN costituite da host fisicamente collegati allo stesso segmento di rete (switch), ma logicamente partizionati in LAN separate.

Separo i domini di broadcast e raggruppo gli utenti che devono comunicare spesso.

Si tratta di un costrutto di livello 2, perciò deve essere supportato da switch:

- inserendo estensione (tag) della PCI MAC per identificare appartenenza alla specifica VLAN
- lo switch su LAN sorgente inserisce il tag, che viene rimosso poi dall'ultimo switch prima della consegna

GIGABIT ETHERNET

- usa formato di trama 802.3
- protocollo MAC CSMA/CD
- operazioni half duplex e full duplex, ma usato praticamente solo in full duplex

- controllo di flusso (definizione di master/slave)
- backward compatibility con mezzi fisici già installati
- **aumenta di un fattore 10 la dimensione minima di pacchetto con padding di caratteri speciali**
- **jumbo frame fino a 9216B (riduce overhead)**
- **codifica 8B10B (facilita il recupero di sincronismo senza incrementare eccessivamente il bit rate)**

Successive versioni sono:

- **10 Gigabit Ethernet** (standardizzato nel 2002), in modalità full duplex (trasmetto e ricevo contemporaneamente su canali separati), solo CSMA
- **100 Gigabit Ethernet** (standardizzato nel 2010), che aumenta le velocità (che sono nell'intervallo dai 40 Gb/s ai 100 Gb/s), utilizzando trasmissioni in parallelo (ad esempio 20 linee a 5 Gb/s)

LE RETI WIFI

Si tratta di una **certificazione di interoperabilità e aderenza allo standard IEEE 802.11**.

Questo standard copre le tecnologie delle reti locali wireless:

- strato fisico (comunicazione via radio)
- strato MAC (DCF, basato su CSMA/CA)
- interconnessione tra dispositivi
- sicurezza

Diverse varianti dello standard 802.11 sono:

La famiglia di standard IEEE 802.11

- IEEE 802.11 – 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a – 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b – support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c – Bridge operation procedures (2001)
- IEEE 802.11d – International roaming extensions (2001)
- IEEE 802.11e – Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11g – 54 Mbit/s @2.4 GHz (backwards compatible with b) (2003)
- IEEE 802.11h – Spectrum Managed 802.11a (5 GHz) for Europe (2004)
- IEEE 802.11i – Enhanced security (2004)
- IEEE 802.11j – Spectrum extensions for Japan (2004)
- IEEE 802.11n – High-speed WLAN (2009)
- IEEE 802.11p – WAVE Wireless Access for the Vehicular Environment (2010)
- IEEE 802.11r – Fast BSS transition (2008)
- IEEE 802.11s – ESS Mesh Networking (2012)
- IEEE 802.11ac – High-speed WLAN (January 2014)

IEEE 802.11ax (Wi-Fi 6)

ARCHITETTURA 802.11

(Topologia logica a stella attiva)

Con infrastruttura:

- i terminali comunicano solo tramite un Access Point (Ap), anche se sono vicini
- l'AP può fornire anche accesso verso Internet
- un AP è funzionalmente identico ad uno switch a livello MAC (ritrasmissione selettiva)

Senza infrastruttura:

- comunicazione diretta tra terminali
- tecnologia WiFi Direct

STRATO FISICO

802.11 lavora su bande di frequenza "non licenziate" (ISM bands) a 2.4 GHz e 5GHz:

- a 2.4 GHz, condivide la banda con Bluetooth, telefoni cordless, baby monitor, forni a microonde
- a 5 GHz, solo WiFi (versioni 11a, 11n, 11ac)

In 802.11 con infrastruttura, la banda ed il relativo canale sono imposti dall'AP:

- a 2.4 GHz → 14 canali possibili ma solo 3 non sovrapposti
- a 5 GHz → 23 canali disgiunti

Esiste anche una nuova versione del WiFi, il WiFi 6, che si appoggia a frequenze a 6 GHz, oltre che alle 2.4 GHz e 5 GHz.

STRATO MAC

Utilizza il protocollo Distributed Coordination Function (DCF) che non è altro che un CSMA/CA:

- per ogni pacchetto, la stazione deve vincere la contesa per il possesso del canale

Le stazioni sono half-duplex → o trasmettono o ricevono; il ricevitore DEVE confermare la ricezione con ACK per permettere di riconoscere collisioni

DCF

Trasmettitore:

- se canale libero per DIFS:
 - trasmette una trama
- se canale occupato:
 - aspetto per un tempo casuale e trasmette
 - se fallisce (no ACK) backoff esponenziale

Ricevitore:

- se dati ricevuti correttamente manda un ACK dopo SIFS

Altre stazioni:

- nessuna azione per un tempo pari alla durata dello scambio di trame (NAV - canale occupato)

Quando dura NAV? → la durata della trama viene indicata nell'intestazione della trama, perciò il tempo totale di rimanenza in stato NAV è uguale a quella durata.

VELOCITA' DI TRASMISSIONE

La velocità massima teorica dipende dalla versione in uso:

| Versione | Velocità max |
|-------------------|--------------|
| 802.11b | 11 Mb/s |
| 802.11g – 802.11a | 54 Mb/s |
| 802.11n (WiFi 4) | 600 Mb/s |
| 802.11ac (WiFi 5) | ~7 Gb/s |
| 802.11ax (WiFi 6) | ~11 Gb/s |

La velocità reale dipende dalla qualità del canale tra AP e stazione:

- minimo 1 Mb/s per 11b, 11g
- minimo 6 Mb/s per 11a, 11n, 11ac

PROBLEMA: TERMINALE NASCOSTO

Si verifica quando due o più stazioni:

- sono a portata radio dell'AP
- non sono a portata radio reciproca (non si sentono)

Quindi, se:

- A trasmette una trama all'AP
- B non sente A, pensa che il canale sia libero e trasmette a sua volta → collisione!

Possibile soluzione (DCF con hadshaking):

Il trasmettitore incia una microtrama RTS (Ready To Send) (di 20 byte) al ricevitore prima della trama dati:

- RTS contiene la durata complessiva dello scambio

Il ricevitore risponde dopo SIFS con una microtrama CTS (Clear To Send) (di 14 byte):

- CTS contiene la durata rimanente dello scambio

La microtrama CTS è sentita da tutti i terminali, anche quelli potenzialmente nascosti (i quali rimandano il potenziale accesso - NAV).

Nel caso di due RTS inviati contemporaneamente, siamo sfigati e abbiamo una collisione. La collisione avrà minore impatto in durata di occupazione del canale visto che le trame sono molto più corte.

PROBLEMA: ANOMALIA DELLE VELOCITA' TRASMISSIVE

Stazioni connesse allo stesso AP hanno velocità diverse:

- il throughput di tutti si uniforma alla stazione più lenta

QUIZ:

Due stazioni nello stesso collision domain in una rete Ethernet:

A. non possono mai creare una collisione grazie all'operazione di carrier sense tipica del protocollo CSMA/CD

B. possono creare una collisione solo nel caso di trasmissione esattamente contemporanea

- C. identificano la collisione grazie ad una trama NACK inviata dallo switch cui sono collegate
 - D. possono creare una collisione quando trasmettono un pacchetto
-

Risposta corretta: D.

QUIZ:

Il protocollo CSMA/CD, utilizzato nella rete Ethernet, per delimitare i pacchetti:

- A. utilizza silenzi (ovvero un tempo di attesa nella trasmissione sul canale) tra pacchetti consecutivi
 - B. prevede che il ricevitore invii una conferma di riconoscimento del pacchetto
 - C. utilizza un indirizzo di sorgente specifico e riservato per identificare la dimensione del pacchetto
 - D. utilizza pacchetti di lunghezza fissa, pari a 1024 byte
-

Risposta corretta: A (Inter Frame Gap).

QUIZ:

Nel protocollo WiFi con DCF ed handshaking:

- A. si evitano completamente le collisioni su qualunque tipo di dato trasmesso
 - B. l'invio dei pacchetti RTS e del CTS riduce la probabilità delle collisioni sui pacchetti dati
 - C. l'invio dei pacchetti RTS e del CTS permette a due terminali, di cui uno nascosto, di inviare contemporaneamente le loro trame
 - D. si evitano completamente le collisioni grazie al meccanismo di carrier sense
-

Risposta corretta: B.

STRATO RETE (3)

La funzione dello strato 3 è principalmente quella di instradamento (routing):

- *effettuato consultando tabelle di instradamento*
 - *per ogni PDU in rete datagram*
 - *per ogni connessione in rete a circuito virtuale*
- *tabelle di instradamento contengono informazioni del tipo*
 - *per ogni destinazione → next-hop (prossimo router)*
- *tre elementi*
 - *protocolli di instradamento (routing protocols) → definizione delle modalità di scambio di informazioni sullo stato della rete al fine di costruire le tabelle di instradamento*
 - *algoritmi di instradamento (routing algorithms) → operazioni necessarie per scegliere il percorso verso la destinazione, date le informazioni sullo stato della rete. Si occupano anche di creare le tabelle di instradamento*
 - *procedure di inoltro pacchetti (forwarding) → operazioni necessarie per instradare i singoli pacchetti verso la corretta porta di uscita. Usa le tabelle per inoltrare i pacchetti.*

Altre funzioni **relativamente** marginali:

- *indirizzamento*
 - *indirizzi univoci*
 - *risoluzione indirizzi (mapping)*
- *tariffazione*
 - *su rete pubblica*

INSTRADAMENTO

ALGORITMI DI INSTRADAMENTO

Obiettivo → **determinare un "buon" percorso (sequenza di link o nodi) nella rete da nodo sorgente a nodo destinazione.**

- Si trasforma la topologia in un grafo:
 - *vertici → nodi*
 - *archi → link fisici*
- Si assegnano costi agli archi.

A questo punto, un "buon" percorso è quello a costo minimo.

COSTO

Dipende da distanza, ritardom euro, livello di congestione, ecc.

Si può decidere di renderlo statico o dipendente dallo stato della rete.

ALGORITMI DI INSTRADAMENTO SEMPLICI

Semplici algoritmi senza necessità di coordinamento da parte dei nodi:

- **Random** → scelgo a caso una porta di uscita
- **Flooding** → instrado verso tutte le porte disponibili
- **Deflessione o hot potato** → su topologie regolari; instrado verso la porta corretta se libera, altrimenti instrado verso un'altra porta libera casuale

Questi algoritmi sono "buoni" solo per piccole reti.

ALGORITMI DI INSTRADAMENTO COMPLESSI

Calcolo percorso:

- *centralizzato:*
 - un nodo si occupa di raccogliere l'informazione da tutti gli altri nodi
 - calcola i percorsi
 - ridistribuisce il risultato del calcolo a tutti gli altri nodi
- *distribuito:*
 - tutti i nodi si scambiano informazioni tra loro (utilizzando protocolli di instradamento)
 - calcolano i percorsi (indipendentemente o in base a quanto fatto dai nodi adiacenti)

Vantaggi (centralizzato):

- è possibile usare percorsi, algoritmi e metriche complesse
- tutti i nodi usano un piano di instradamento coerente

Svantaggi (centralizzato):

- è sensibile al guasto del nodo centrale
- lo scambio dell'informazione da/verso il nodo centrale genera congestione

Vantaggi (distribuito):

- è robusto ai guasti
- lo scambio di informazione è uniforme su tutta la rete

Svantaggi (distribuito):

- richiede intelligenza nei nodi
- lo scambio di informazione parziale/errata porta a incongruenze nell'instradamento

ALGORITMI DISTRIBUITI - INFORMAZIONE

Lo scambio di informazione può essere:

- **globale:**
 - tutti i nodi conoscono la topologia completa, compresi i costi dei canali
 - scambio di informazioni tra tutti i nodi
 - algoritmi Link State
- **parziale:**
 - i nodi conoscono i nodi cui sono fisicamente collegati ed i costi dei canali cui sono collegati
 - scambio di informazione solo con i nodi adiacenti
 - algoritmi Distance Vector

ALGORITMI LINK STATE

- ogni nodo invia informazioni di costo (stato) dei soli suoi canali in multicast/broadcast a tutti gli altri nodi della rete
- tutti i nodi costruiscono una loro copia della topologia della rete e conoscono i costi di tutti gli archi
- data la topologia, ogni nodo calcola i percorsi a minimo costo verso tutti gli altri nodi
 - si ottengono tabelle di routing

Per determinare i cammini ottimi si utilizza l'**algoritmo di Dijkstra**:

- algoritmo iterativo → dopo **k** iterazioni si ottengono cammini a costo minimo per **k** destinazioni
- funziona solo con costi positivi

ALGORITMI DISTANCE VECTOR

Sono algoritmi iterativi:

- continuano fino a quando i nodi non scambiano più informazioni

Terminano in modo autonomo:

- nessun segnale esplicito di fine algoritmo

Distribuito:

- ogni nodo comunica solo con nodi adiacenti

Ogni nodo scambia periodicamente **solo** con i vicini diretti, un vettore contenente:

- le destinazioni che può raggiungere

- la distanza dalle destinazioni misurata in costo (es. numero di nodi da attraversare compreso se stesso)

Il nodo che riceve il vettore lo confronta con la propria RT (Routing Table, tabella di instradamento) ed effettua modifiche:

- aggiunge nuove destinazioni
- cambia instradamenti se ce ne sono di nuovi più brevi
- modifica i costi se ci sono variazioni di costo

Vantaggi:

- facile da implementare

Svantaggi:

- lento a convergere
- propaga errori di routing
- non molto scalabile (le dimensioni dei messaggi scambiati (vettori) dai nodi crescono al crescere della rete)

Implementazione:

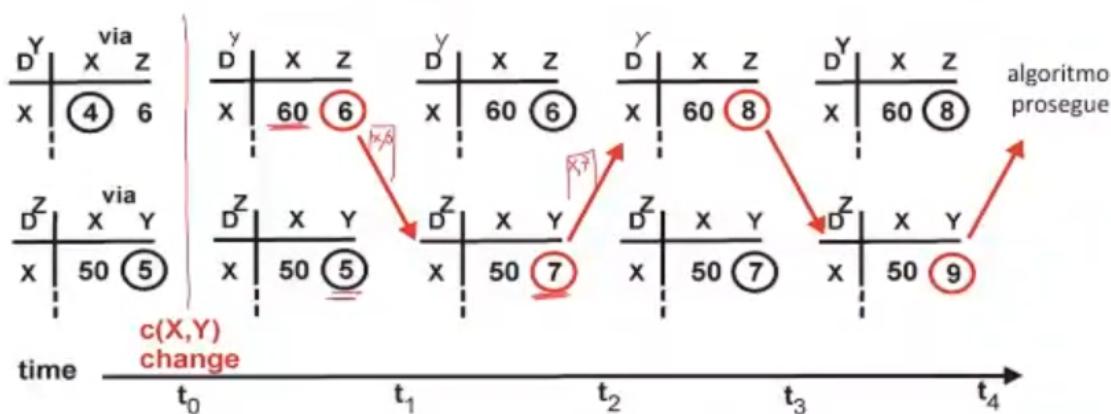
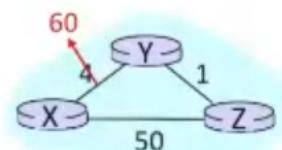
- struttura dati: tabella distanze
- ogni nodo possiede la propria tabella:
 - una riga per ogni possibile destinazione
 - una colonna per ogni nodo adiacente

PROBLEMA DEL COUNT TO INFINITY

Se il costo di un canale "peggiora", possono verificarsi problemi.

Modifica costo canale:

- good news travels fast
- bad news travels slow - problema del "count to infinity"!

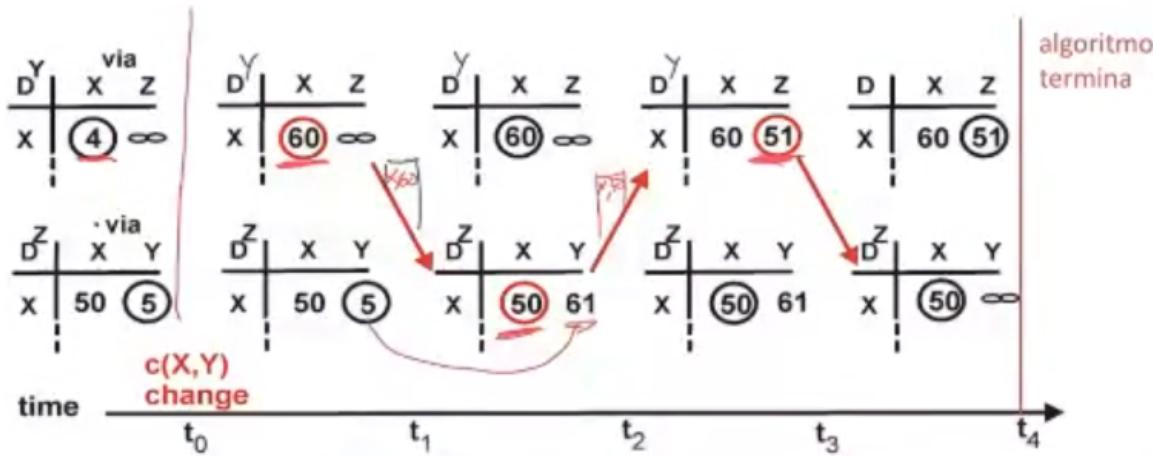
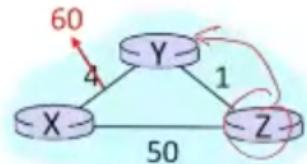


Per risolvere parzialmente questo problema:

Distance Vector: Poisoned Reverse

Se Z instrada via Y per raggiungere X:

- Z comunica ad Y sua distanza verso X è infinito
(Y non instraderà verso X passando da Z)
- non risolve il problema completamente



CONFRONTO TRA ALGORITMI LS E DV

Complessità messaggi: M nodi, E canali per nodo:

- LS → ogni nodo invia $O(M)$ messaggi, ciascuno lungo $O(E)$
- DV → ogni messaggio contiene tutte le destinazioni $O(M)$, ed è mandato a $O(E)$ vicini

Quindi: **$O(E M)$** .

Velocità di convergenza:

- LS → ogni volta che un link state è propagato, ho una nuova topologia → convergenza immediata
- DV → le scelte di un nodo dipendono dalle scelte dei nodi vicini; si richiedono più scambi di messaggi → tempo di convergenza variabile

Affidabilità (se un nodo non funziona correttamente):

- LS → i nodi possono annunciare costi dei canali scorretti:
 - ogni nodo calcola la propria tabella → tutti sbagliano
 - al prossimo annuncio tutto si corregge
- DV → i nodi possono annunciare costi dei cammini scorretti:
 - ogni annuncio è usato da tutti i nodi (indirettamente)
 - gli errori si propagano nella rete

Ma dove vengono utilizzati questi algoritmi?

Gli algoritmi Distance Vector si usano per gestire l'instradamento tra operatori attraverso gli Autonomous System.

All'interno di una rete di un operatore si usano invece algoritmi di tipo Link State

QUIZ:

Data una topologia (nodi, canali e costi associati), il percorso ottimo tra una sorgente ed una destinazione:

- A. non cambia mai anche nel caso in cui il costo dei canali cambia
- B. non cambia mai anche nel caso in cui un canale diventi indisponibile
- C. cambia a seconda del nodo che esegue l'algoritmo link state
- D. è lo stesso sia che si utilizzi un algoritmo link state sia che si utilizzi un algoritmo distance vector

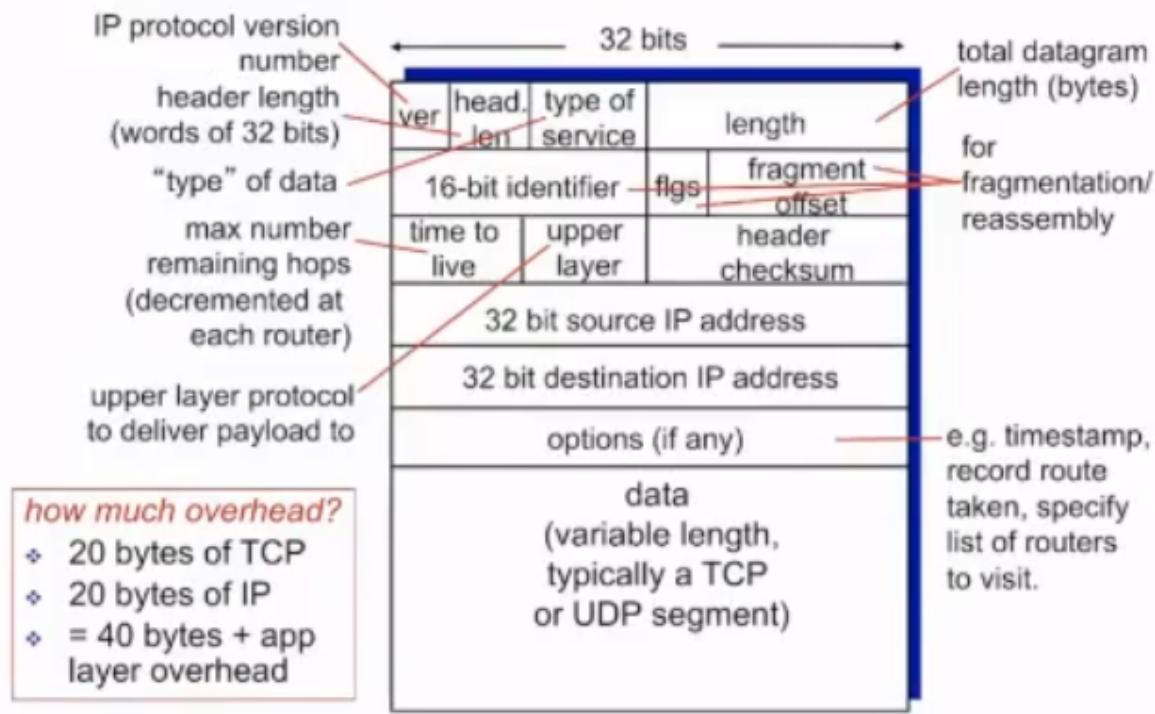
Risposta corretta: D.

PROTOCOLLO IP

routing → insieme delle procedure per scrivere la routing-table (si basa sui routing algorithms)

forwarding → insieme delle procedure per leggere la routing-table e scegliere l'appropriato output del router IP

IP datagram format



Campi:

- *version* → versione del protocollo IP
- *header length* → lunghezza dell'header
- *type of service* (oppure DS) → tipo del dato
- *length* → lunghezza totale del pacchetto
- *16-bit identifier / flags / fragment offset* → campi utilizzati per la frammentazione
- *time to live* → numero di massimo di hop dopo il quale il pacchetto verrà cancellato (il valore del campo verrà decrementato ad ogni hop)
- *upper layer* → indica il protocollo del dato
- *header checksum* → controllo di errore nell'header (se c'è errore il pacchetto viene scartato)
- *source / destination* → indirizzo IP sorgente / destinazione

- *options* → es. *timestamp, record route ecc* (campo poco utilizzato)
- *data* → contenuto dati del pacchetto (tipicamente TCP o UDP)

IP FRAGMENTATION

I canali hanno una MTU (Maximum Transmission Unit) fissata, cioè la dimensione massima trasportabile su di essi.

Se un pacchetto IP è più grande di questa dimensione, dovrà subire una frammentazione, cioè verrà "spezzato" in pacchetti più piccoli da poter essere trasferiti sul canale.

IP ADDRESSING

Gli indirizzi IP sono su 32 bit e identificano un'interfaccia host o un'interfaccia router.

Interfaccia → connessione host/router - link fisico

SPECIAL ADDRESSING

| | | |
|--------|--------------------|--------------------------------------|
| Subnet | All 0s | the (sub)network (network ID) |
| All 1s | | limited broadcast (local net) |
| Subnet | All 1s | directed broadcast for net |
| 127 | Anything (often I) | loopback |

IP ADDRESSING: CLASSFUL

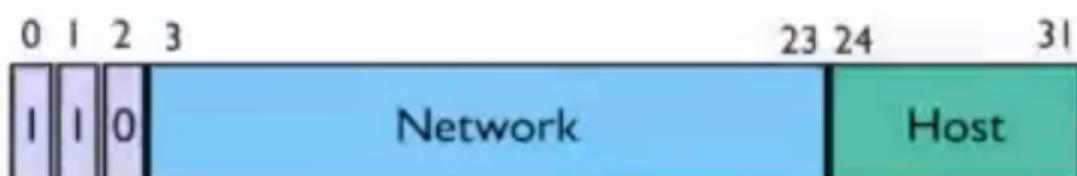
Si basa sulla divisione statica di network part e host part di un indirizzo IP.



Class A – 128 networks – 1st byte: 0-127



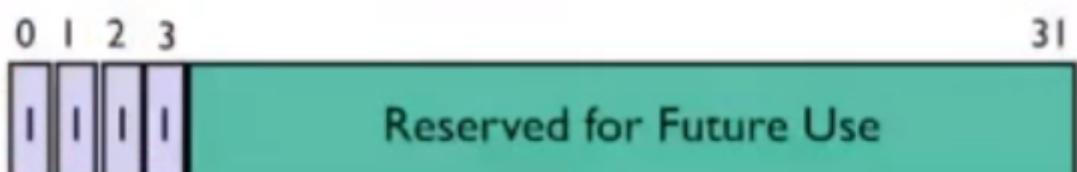
Class B – 16K networks – 1st byte: 128-191



Class C – 2M networks - 1st byte: 192-223



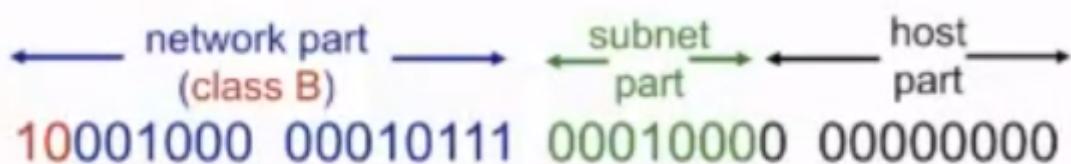
Class D – 1st byte: 224-239



Class E – 1st byte: 240-255

IP ADDRESSING: SUBNETTING

Si basa sul concetto di **VLSM** (Variable Length Subnet Masking).



In questo caso le reti andranno definite dalla coppia:

- *indirizzo IP*
- *subnet mask*

Esempio: 130.23.16.0 / 255.255.254.0

IP ADDRESSING: CLASSLESS (CIDR)

CIDR → Classless InterDomain Routing

Si basa sul concetto del non avere più classi e avere porzioni di indirizzi di lunghezza arbitraria.

In questo caso possiamo avere due notazioni:

1. *uguale a quella del subnetting*
2. *prefix length notation* → in cui viene indicata la lunghezza della network part

Esempio prefix length notation: 200.23.16.0/23

Numeri validi negli indirizzi delle subnet → sequenze di '1' seguite da sequenze di '0':

valid netmasks: possible values in the 4 bytes composing the address

| | | |
|-----|-----------|-------|
| 0 | 0000 0000 | (256) |
| 128 | 1000 0000 | (128) |
| 192 | 1100 0000 | (64) |
| 224 | 1110 0000 | (32) |
| 240 | 1111 0000 | (16) |
| 248 | 1111 1000 | (8) |
| 252 | 1111 1100 | (4) |
| 254 | 1111 1110 | (2)* |
| 255 | 1111 1111 | (1) |

*not valid in the 4° byte

IP ADDRESSING: DEVICE CONFIG

Ogni dispositivo IP per funzionare correttamente deve essere provvisto di:

- *un indirizzo IP*
- *una netmask*
 - *per riconoscere il proprio network ID*
 - *per riconoscere il network ID della destinazione*
- *un default gateway* (first-hop router)

FUNZIONAMENTO IP ROUTING

Q: Come fa un host a capire il proprio network ID?

- *Viene effettuato un AND bit-a-bit tra il suo indirizzo IP e la netmask*

interface IP address: 192.168.10.69

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

bit-wise AND result: 192.168.10.64

netmask: 255.255.255.192

Q: Come fa un host a capire se l'host con cui vuole comunicare è nella sua stessa rete (stesso network ID)?

- Viene effettuato un AND bit-a-bit tra l'**indirizzo IP dell'host destinazione** e la **netmask dell'host sorgente**

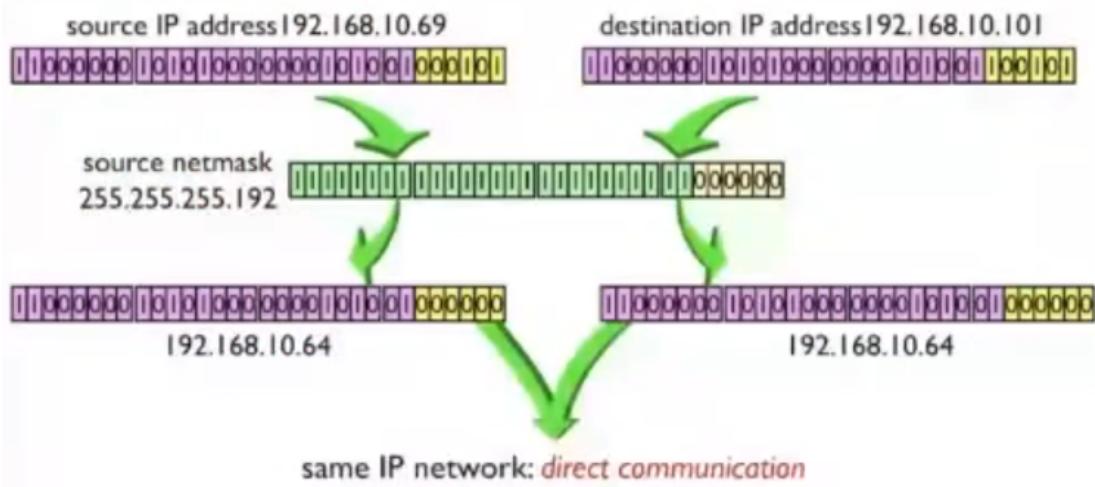
destination IP address: 192.168.10.101

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

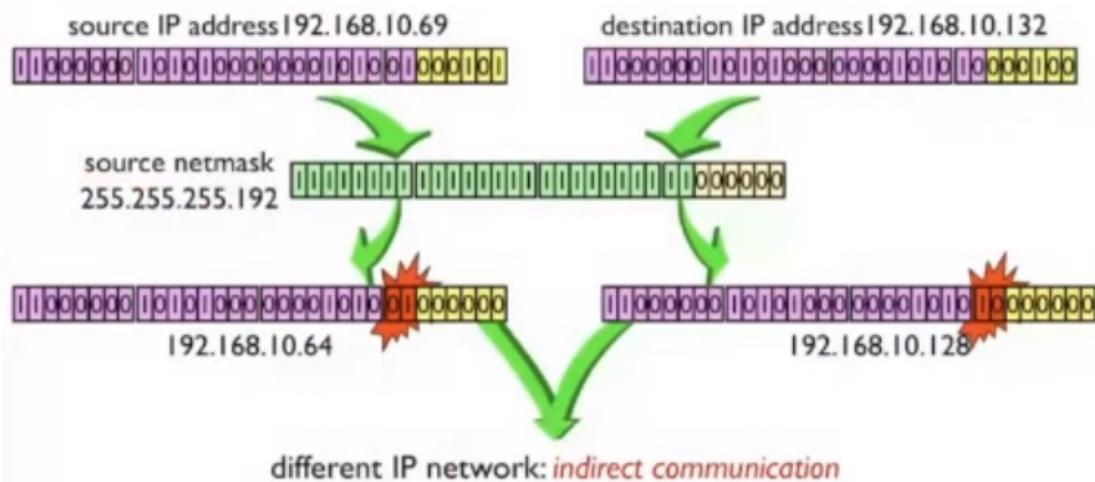
bit-wise AND result: 192.168.10.64

netmask: 255.255.255.192

Per capire meglio:



OPPURE



we need a router!

Q: Come fa un router a selezionare la porta di output corretta?

- Viene effettuato un AND bit-a-bit tra l'**indirizzo IP destinazione di un pacchetto** e la **netmask di ogni entry della routing table**, attendendo un match

Esempio:

Routing table

| destinazione | output port |
|-----------------------|-------------|
| <u>200.23.16.0/20</u> | 1 |
| 199.31.0.0/16 | 2 |

Indirizzo destinazione del pacchetto: 200.23.16.1

| | |
|---------------------------------|--------------------|
| destination IP address | 200.23.16.1 |
| netmask (output port 1 - 20bit) | 255.255.240.0 |
| bit-wise AND result | <u>200.23.16.0</u> |

Come si può notare, il risultato dell'AND bit-a-bit è uguale al network ID riportato nella routing table, quindi c'è un **match**. Pertanto la porta di uscita (**output port**) sarà la numero 1.

Per capire facciamo anche il test con la seconda entry:

| | |
|---------------------------------|-------------|
| | |
| destination IP address | 200.23.16.1 |
| netmask (output port 2 - 16bit) | 255.255.0.0 |
| bit-wise AND result | 200.23.0.0 |

Come si può notare, in questo caso il risultato dell'AND bit-a-bit non è uguale al network ID presente nella routing table, quindi non si verifica un **match**: la porta di uscita non è la 2.

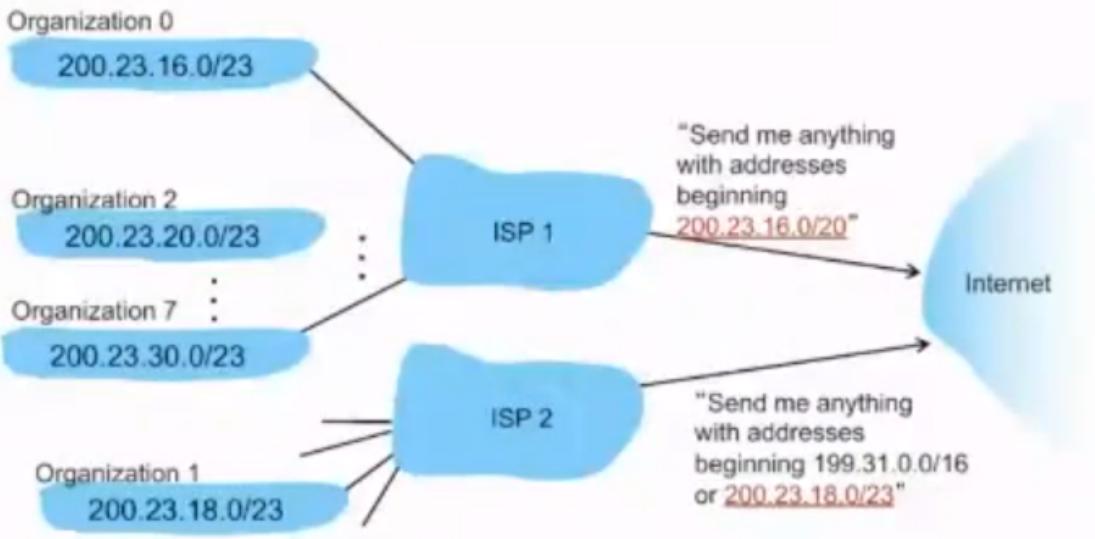
NB: effettuare i calcoli (bit-wise AND) in binario può essere più lungo ma più comprensibile

LONGEST PREFIX MATCHING

Concettualmente:

- quando ho più match, devo considerare quello fatto con il prefisso più lungo (cioè quello più specifico).

Esempio:



- Organizzazione 1 ha network ID 200.23.20.0/23 e fa parte di ISP 1 con network ID 200.23.16.0/20
- Organizzazione 1 decide di cambiare ISP **senza cambiare il proprio network ID** e passare con ISP 2 che però ha come network ID 199.31.0.0/16 (quindi ISP 2 dovrà gestire un network ID che è "fuori dal suo range")

| Destination Address Range | Link interface |
|-----------------------------------|----------------|
| 11001000 00010111 0001***** ***** | 0 |
| 11001000 00010111 0001001* ***** | 1 |
| 11000111 00011111 ***** | 1 |
| otherwise | 2 |

- Nella tabella qui sopra, avremo due match, sia con la entry 1 che con la 2 (prima e seconda riga):
 - verrà scelta la seconda (link interface 1), perché il prefisso è più lungo (23) e quindi più specifico

TIPI ROUTING TABLE

Ci sono 3 tipi di routes:

- *direct routes* → reti connesse direttamente al router
- *static routes* → routes configurate manualmente (per comunicare all'esterno)
- *dynamic routes* → routes configurate automaticamente (per comunicare all'esterno)

LOGICAL IP SUBNETS (LIS)

Si tratta di un insieme di dispositivi con la stessa subnet part dell'IP address.

Gli indirizzi IP vengono divisi in due parti:

- *subnet part* → *high order bits* (primi bit)
- *host part* → *low order bits* (ultimi bit)

| Le interfacce di una subnet dovrebbero essere in grado di raggiungersi fisicamente.

PHYSICAL NETWORK

Insieme di dispositivi che possono raggiungersi fisicamente gli uni con gli altri attraverso meccanismi di livello 2 (link layer mechanism).

SUBNETS E PHYSICAL NETWORKS

IP assume una corrispondenza biunivoca tra physical network e subnet.

Per questo:

- ogni volta che due host sono sulla stessa subnet, possono comunicare direttamente attraverso meccanismi di livello 2 (**comunicazione diretta**)
- ogni volta che due host si trovano su subnet diverse, utilizzeremo il routing IP (**comunicazione indiretta**)

| E' possibile avere:

- più subnet su una sola rete fisica (one-arm router)
- una subnet su più reti fisiche (proxy ARP) - poco utilizzata

ARP - ADDRESS RESOLUTION PROTOCOL

Come si può determinare l'indirizzo MAC di un'interfaccia, sapendo il suo indirizzo IP?

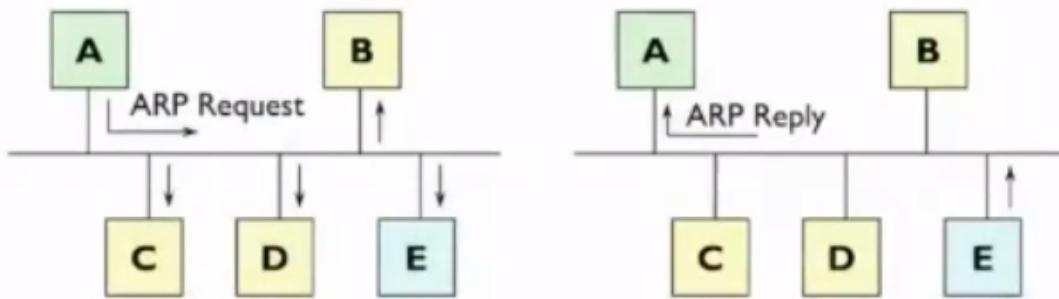
Ogni dispositivo ha una tabella chiamata **ARP table** con dentro associati gli indirizzi IP ai corrispondenti indirizzi MAC.

Procedura:

- **A** vuole inviare un pacchetto a **B** → l'indirizzo MAC di **B** non è nella ARP table di **A**
- **A** manda un pacchetto ARP broadcast contenente l'indirizzo IP di **B** (ARP request)
- **B** riceve il pacchetto ARP e risponde ad **A** con il suo indirizzo MAC (ARP reply)
- **A** salva la coppia IP-to-MAC nella sua ARP table (l'ARP table è una cache, quindi dopo un tot di tempo, verrà ripulita)

ARP è plug-and-play → i nodi creano le loro ARP table senza l'intervento dell'amministratore di rete

| most significant fields of the link layer header | | | | most significant fields of the ARP packet | | | |
|--|-------|-----------|-------|---|-------|-------|--|
| MAC broadcast | MAC A | ARP Req | MAC A | IP A* | ?? | IP E* | |
| ARP Request | | | | | | | |
| MAC A | MAC E | ARP Reply | MAC E | IP E* | MAC A | IP A* | |
| ARP Reply | | | | | | | |



*These fields are not IP source and destination fields of an IP header!

ICMP (Internet Control Message Protocol)

Si tratta di un protocollo di livello 3 incapsulato nell'IP datagram, utilizzato da host e router principalmente per comunicare:

- errori → unreachable host/network/port ecc.
- echo request/reply (usate da **ping**)

STRATO TRASPORTO (4)

Lo strato trasporto ha diverse funzioni:

- multiplexing/demultiplexing
- trasferimento "affidabile" dei dati
- controllo di flusso
- controllo di congestione

I due principali protocolli a cui si fa riferimento sono:

- TCP
- UDP

Questo strato riesce a funzionare utilizzando le **porte**, per indirizzare il traffico verso l'applicativo giusto.

NB: **trasferimento affidabile dei dati, controllo di flusso e controllo di congestione** sono presenti solo nel protocollo TCP, non nell'UDP.

MULTIPLEXING

Si tratta della raccolta dati dai processi di applicazione presenti sull'host sorgente, con successivo imbustamento dei dati con header (poi usati per il demultiplexing).

DEMUTLIPLEXING

L'host riceve il datagram IP contenente:

- *source IP address*
- *destination IP address*
- *un segmento di livello trasporto*

Quest'ultimo a sua volta contiene:

- *source port number*
- *destination port number*

L'host quindi utilizza gli **indirizzi IP** e i **numeri di porta** per inviare il traffico all'applicazione appropriata.

DEMUTLIPLEXING CONNECTIONLESS

In questo tipo di connessione, host sorgente e host destinazione non si sono messi d'accordo sul protocollo di comunicazione, di conseguenza non ho la certezza che un pacchetto multiplexato e inviato venga ricevuto (assenza di ack).

DEMUTLIPLEXING CONNECTION-ORIENTED

In questo tipo di connessione, host sorgente e host destinazione si sono messi d'accordo sul protocollo di comunicazione (handshaking), di conseguenza nel caso in cui il pacchetto venga correttamente ricevuto, mi tornerà indietro un ack.

WELL-KNOWN PORTS

Il range delle porte utilizzate dalle applicazioni è 0-1024 (UDP-TCP).

Ad esempio la porta TCP 80 è associata al protocollo (di livello 7) HTTP. Invece per un DNS Server si utilizza la porta UDP 53.

NB: questo range non è obbligatorio da rispettare, si tratta di una convenzione.

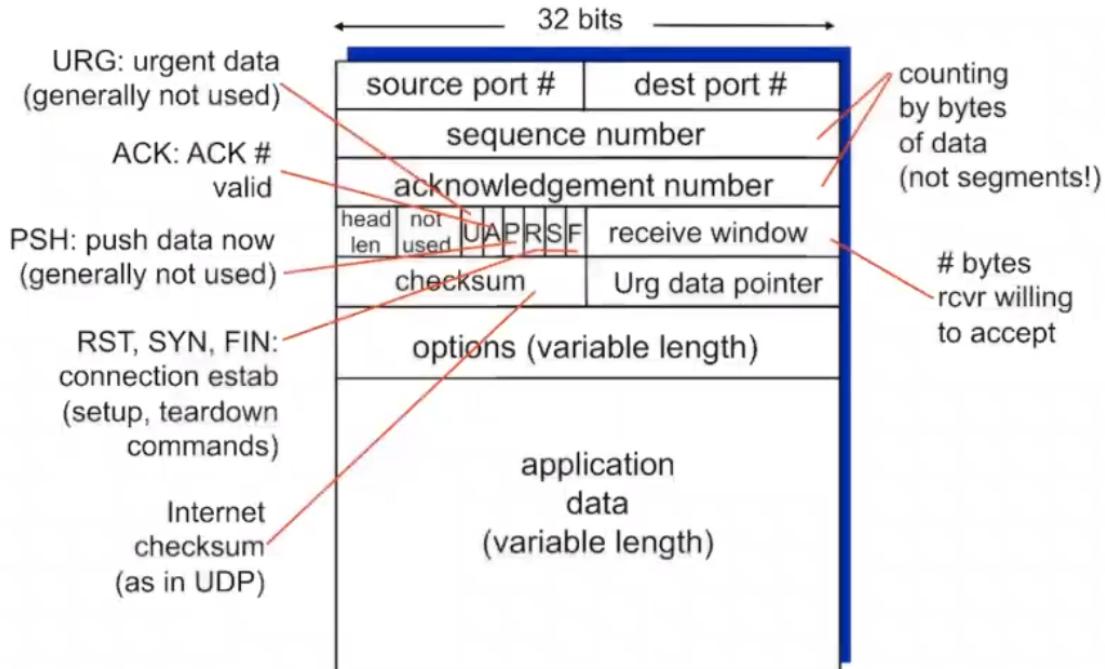
Per quel che riguarda invece le porte del client, esse vengono selezionate casualmente dal sistema operativo.

TCP

Si tratta di un protocollo point-to-point (un trasmettitore e un ricevitore). Le connessione TCP sono full-duplex (bidirezionali), quindi posso comunicare in entrambe le direzioni. Hanno controllo di flusso e di congestione, grazie ai quali viene settata la dimensione della finestra di invio/ricezione.

NB: rispetto al segmento UDP, quello TCP ha un header molto più complesso, con molti campi utili a gestire tutte le funzioni che il protocollo può garantire.

TCP segment structure



Per comunicare con lo strato applicazione, vengono utilizzati i socket, cioè degli intermediari.

TCP SEQUENCE NUMBERS

Indica il numero del primo byte (rispetto a tutto il byte stream) nella parte dati del segmento.

TCP ACKs

Indica il numero del prossimo byte atteso. Si tratta di ACK cumulativi.

TCP OPEN/CLOSE CONNECTION

APERTURA

La connessione viene iniziata dal trasmettitore inviando un segmento TCP contenente il flag SYN (S) settato a 1 (apertura solo in un verso). Quando il segmento viene ricevuto dal ricevitore, quest'ultimo invia un pacchetto di ACK contenente anch'esso il flag SYN settato a 1, in modo da aprire la connessione anche nel suo verso. A questo punto la connessione sarà utilizzabile normalmente.

CHIUSURA

Stessa procedura di apertura ma con il flag FIN (F) settato a 1.

TCP FLOW CONTROL

Il ricevitore comunica al trasmettitore la dimensione attualmente libera del suo buffer attraverso il campo **rwnd** (*receiver window*) presente nell'header TCP. Mano a mano che l'applicativo svuota il buffer, il valore in **rwnd** aumenta.

TCP CONGESTION CONTROL

AIMD (Additive Increase Multiplicative Decrease) o Congestion Avoidance

Il trasmettitore incrementa la dimensione della sua finestra di trasmissione, di poco alla volta, fino a che non subisco delle perdite.

- **additive increase** → *incremento la cwnd (congestion window) di un MSS (Maximum Segment Size) ogni RTT (quindi di 1/cwnd ogni ACK ricevuto) fino a quando non rilevo perdite*
- **multiplicative decrease** → *dimezzo la cwnd ogni volta che ho perdite*

TCP SLOW START

Quando viene stabilita la connessione tra trasmettitore e ricevitore, la **cwnd** viene settata a 1 MSS e aumenta esponenzialmente fino a quando non si verifica la prima perdita.

TCP: REAZIONE ALLE PERDITE

In base alla causa per cui si verifica la perdita si agisce diversamente:

- *per timeout* → *cwnd resettata a 1 MSS e si riprende a crescere esponenzialmente*
- *per 3 ACK duplicati* → *cwnd dimezzata e poi cresce linearmente (TCP version RENO)*
- *c'è un'altra versione, la TCP Tahoe che reagisce settando a 1 MSS la cwnd a prescindere dalla causa della perdita*

TRASFERIMENTO AFFIDABILE

L'obiettivo è quello di costruire un servizio affidabile su un canale che di per sé non lo è. Si risolve utilizzando i protocolli a finestra (pipelined protocols):

- *Go-Back-N*
- *Selective Repeat*

TCP, per creare un trasferimento affidabile, utilizza:

- *protocolli a finestra*
- *cumulative acks*
- *timer di ritrasmissione singolo*

Come funziona l'invio tramite TCP?

- *quando i dati (inviati dall'applicazione) vengono ricevuti dal trasmettitore, quest'ultimo crea un segmento con il numero del primo byte (rispetto al byte stream) dei dati che invierà tramite il segmento.*
- *viene fatto partire un timer se non è già attivo (il timer è riferito al più vecchio segmento di cui ancora non si è ricevuto l'ack)*
- *quando scatta un timeout, viene ritrasmesso solo il segmento che ha causato il timeout e viene fatto ripartire il timer*
- *quando viene ricevuto un ack (cumulativo), faccio ripartire il timer se ci sono ancora segmenti inviati che non sono riscontrati dall'ack ricevuto*

Come funziona la ricezione tramite TCP?

- quando ricevo un segmento con un seq# che stavo aspettando, posso utilizzare la tecnica del **delayed ACK**, cioè attendo 500ms prima di inviare l'ACK relativo a quel segmento, così se nel frattempo ricevo il segmento successivo, posso inviare solo l'ACK relativo all'ultimo ricevuto (tanto è cumulativo, risparmio ACK). Se dopo 500ms non ricevo nessun nuovo segmento, invio comunque l'ACK per evitare che scada un timeout inutile
- quando ricevo un segmento con un seq# che stavo aspettando ma il trasmettitore sta già attendendo un ACK relativo ad uno dei segmenti precedentemente inviati, allora mando immediatamente un ACK cumulativo per entrambi i segmenti ricevuti
- quando ricevo un segmento che ha un seq# maggiore di quello atteso (si crea un gap), invio immediatamente un **ACK duplicato**, indicando il segmento con seq# atteso
- quando ricevo un segmento che completa parzialmente o interamente un gap, invio immediatamente un ACK contenente il prossimo seq# atteso

Per capire meglio gli ultimi 2 punti (finestra di invio/ricezione di dimensione 4):

- vengono inviati 1,2,3,4
- 1 viene ricevuto → invio ACK 2
- 2 non viene ricevuto
- 3 viene ricevuto → invio ACK 2
- 4 viene ricevuto → invio ACK 2
- viene inviato 2
- 2 viene ricevuto → invio ACK 5

STRATO APPLICAZIONE (7)

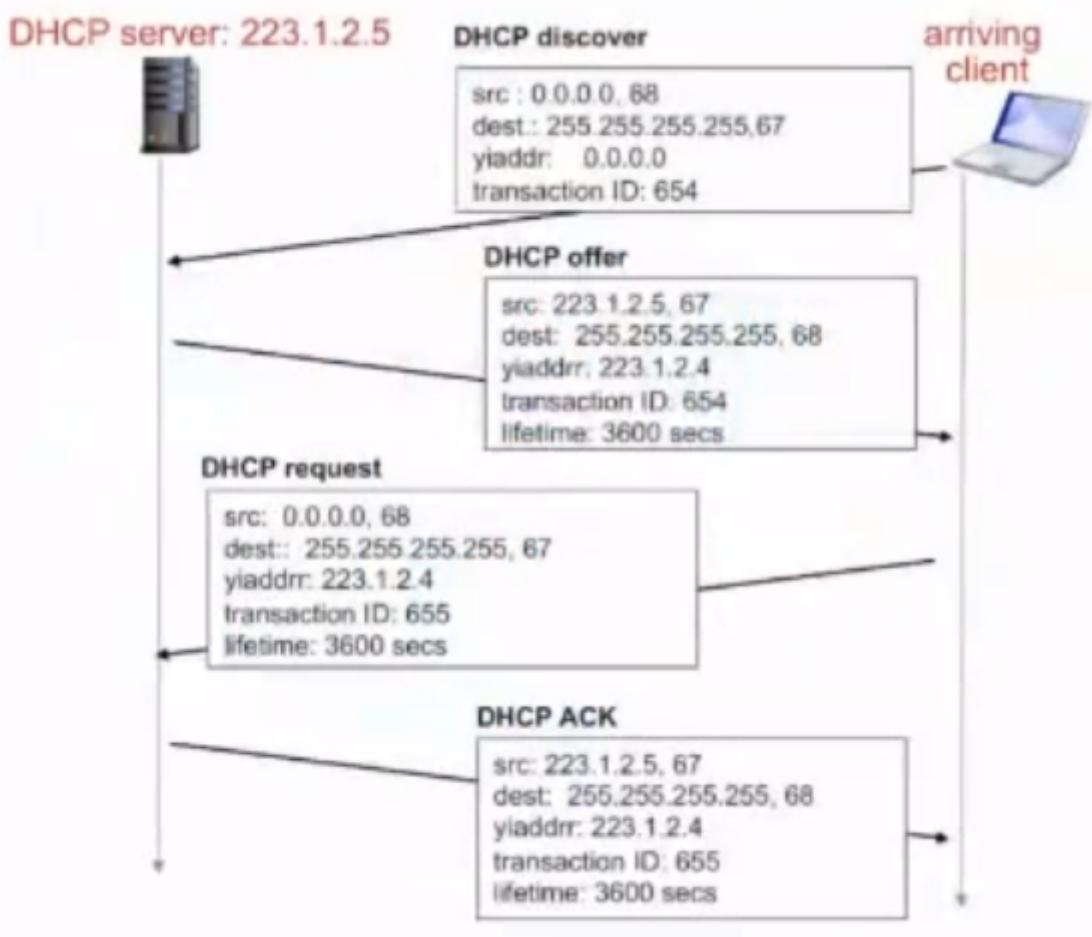
DHCP (Dynamic Host Configuration Protocol)

L'obiettivo di questo protocollo è quello di permettere agli host di ottenere dinamicamente un indirizzo IP dal server di rete.

Un'importante proprietà di questo protocollo è che permette di riutilizzare gli indirizzi IP precedentemente assegnati ad host che si sono successivamente scollegati.

L'assegnazione dell'indirizzo IP avviene in 4 fasi (messaggi):

- *DHCP discover* → messaggio broadcast inviato dall'host per far sapere ai server DHCP che c'è un nuovo dispositivo connesso in rete
- *DHCP offer* → messaggio inviato dal/dai DHCP server contenente l'indirizzo o gli indirizzi IP (se ci sono più DHCP server) disponibile/i
- *DHCP request* → messaggio inviato dall'host per scegliere un indirizzo IP tra quelli offerti
- *DHCP ack* → messaggio inviato dal server DHCP che ha offerto quell'indirizzo IP per confermarne l'assegnazione



I numeri posti dopo gli indirizzi IP *src* e *dst* sono chiamati **porte** e servono a rappresentare le applicazioni con cui parlare (Chrome, Skype, ecc.). In particolare il numero 67 nella foto rappresenta l'applicazione DHCP server (software), mentre il 68 rappresenta l'applicazione DHCP client.

NB: esistono delle convenzioni per l'assegnazione delle porte (well-known ports), per il DHCP server si utilizza la porta 67.

Il DHCP può ritornare più cose oltre all'indirizzo IP nelle subnet:

- *indirizzo del first-hop router*
- *nome e IP del DNS Server*
- *maschera di rete*

DNS (Domain Name System)

Si tratta di un sistema utilizzato per assegnare **nomi** agli host di una rete.

Questi nomi possono essere utilizzati al posto degli indirizzi IP (la cui traduzione avviene mediante il **processo di risoluzione**). La parte finale del nome (.it, .org, ecc.) viene chiamata **dominio di primo livello**. La parte precedente del nome, unita al dominio di primo livello (politico.it, wikipedia.org, ecc.) viene chiamata **dominio di secondo livello**. Esistono anche domini di altri livelli successivi al secondo, come ad esempio:

- *didattica.polito.it (terzo livello)*
- *cms.didattica.polito.it (quarto livello)*
- *ecc.*

Per velocizzare il processo di risoluzione, alcuni DNS Server salvano le precedenti risoluzioni in una memoria cache, accessibile molto più rapidamente quando vengono effettuate le richieste.

TIPI DI RECORD DNS

I record DNS possono essere di più tipi:

| Tipo | Campi |
|-------|---|
| A | name (www.polito.it), value (130.192.87.5) |
| NS | name (google.com), value (dns.google.com) |
| CNAME | name (alias for canonical name), value (canonical name) |
| MX | serve per la posta elettronica |

APP DI RETE

Lo scopo è quello di creare un programma che funzioni su diversi end-systems, capace di comunicare con la rete.

ARCHITETTURE DELLE APPLICAZIONI

Abbiamo 2 diversi paradigmi:

- **architettura client-server**
 - *client → sempre attivi, hanno un indirizzo IP permanente (nel caso di molte richieste, si possono utilizzare più server, creando un data center)*
 - *server → comunica con il server, possono essere connessi ad intermittenza con indirizzo IP dinamico*
- **architettura peer-to-peer (P2P)** → tutti i nodi hanno pari importanza e all'evenienza possono svolgere il ruolo di client o server

COMUNICAZIONE TRA PROCESSI

Il processo non è altro che l'esecuzione attiva del programma. Distinguiamo:

- **processi client** → coloro che iniziano la comunicazione
- **processi server** → coloro che attendono di essere contattati

NB: le applicazioni con architettura P2P hanno processi sia client che server.

Per funzionare correttamente, un'applicazione deve essere supportata da protocolli di livello applicazione, cioè entità che forniscono supporto all'applicazione stessa garantendone l'efficienza. Il protocollo di strato applicazione definisce:

- *il tipo di messaggi scambiati (request, response)*
- *la sintassi, cioè i campi presenti e come sono delineati/dimensionati*
- *la semantica, cioè il significato delle informazioni contenute nei campi*
- *le regole secondo le quali i processi rispondono ai messaggi*

I protocolli possono essere OPEN (definiti da un RFC - Request for Comments) o proprietari.

TIPI DI SERVIZI CHE PUÒ RICHIEDERE UN'APP

- **Data Integrity (servizio affidabile)** → app che richiedono un trasferimento senza perdite (file transfer)
- **Timing (molto bassi)** → giochi online o telefonia

- **Throughput** → alcune app che richiedono un mini throughput garantito (come app multimediali), altre no (app elastiche)
- **Sicurezza**

HTTP (Hyper Text Transfer Protocol)

È un protocollo basato su client-server. Il client è il browser che richiede e riceve **Web objects**. Il server è il Web Server che risponde a tali richieste.

Questo protocollo di livello 7 si basa a livello 4 su TCP:

- *il client inizia una connessione TCP*
- *il server la accetta*
- *vengono scambiati messaggi HTTP tra il browser e il Web Server*
- *si chiude la connessione TCP*

Si tratta di un **protocollo stateless**, cioè che non tiene traccia di informazioni su richieste di client passati.

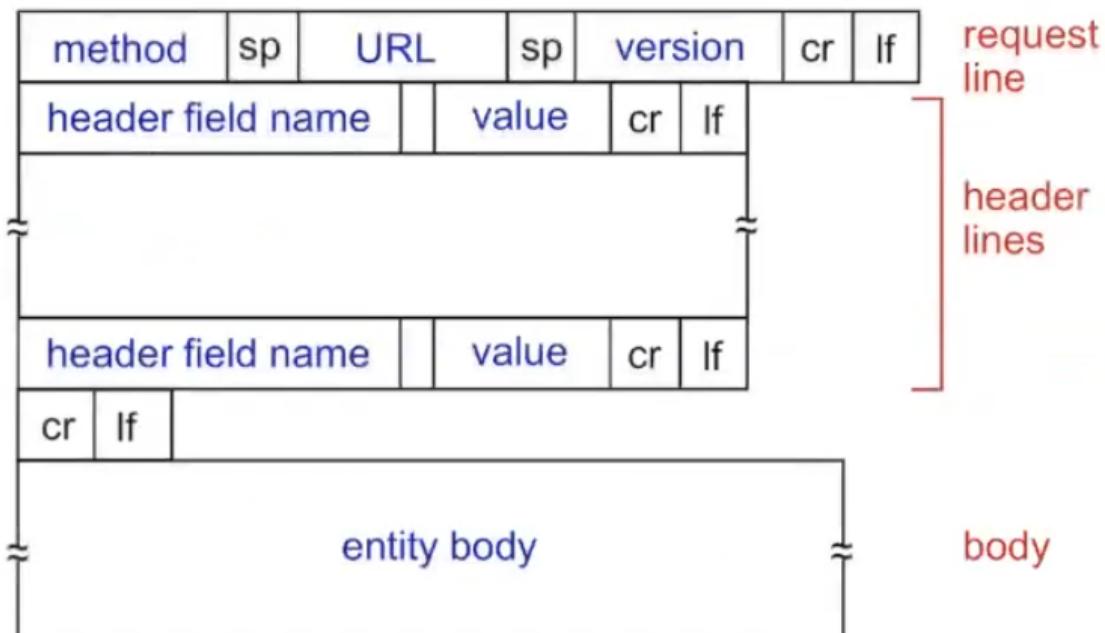
La connessione HTTP prevede due modalità:

- *non-persistent* → viene mandato un solo oggetto in TCP, poi viene chiusa la connessione
- *persistent* → più oggetti possono essere mandati su TCP

HTTP REQUEST MESSAGE

Questo messaggio è in formato ASCII.

HTTP request message: general format



In **HTTP 1.0** i metodi sono **GET, POST, HEAD** (quest'ultimo praticamente inutilizzato):

- **GET** → input direttamente nella request line (URL)
- **POST** → input caricato nel body

HTTP RESPONSE MESSAGE

Nella prima riga del messaggio di response, è presente uno status code:

- 200 → *OK (richiesta ricevuta)*
- 301 → *MOVED PERMANENTLY (oggetto spostato, indica la nuova location)*
- 400 → *BAD REQUEST (messaggio non interpretato dal server)*
- 404 → *NOT FOUND (documento non trovato sul server)*
- 505 → *HTTP VERSION NOT SUPPORTED*

COOKIE

Si tratta di particolari messaggi scambiati tra client e server che hanno tra i diversi scopi possibili, quello di tenere traccia delle autorizzazioni, dei login, delle impostazioni grafiche, ma anche di tenere traccia dei carrelli della spesa sui siti di e-commerce. Usi sgraditi ai clienti sono quelli invece in cui i cookie vengono utilizzati al fine di profilazione e mostrare pubblicità mirata.

WEB CACHES (PROXY SERVER)

L'obiettivo principale è quello di soddisfare le richieste del cliente senza contattare il server.

Il browser invia tutte le HTTP REQUEST alla cache, se la risposta alla richiesta è già presente in essa, viene ritornata direttamente, altrimenti la cache inoltra la richiesta al server originale. Può capitare che le cache non siano aggiornate, per ovviare a questa problematica si usano dei GET condizionali nelle HTTP REQUEST di tipo **IF-MODIFIED-SINCE:<DATE>** e il server risponde con **304 + body vuoto** se le cache sono aggiornate, altrimenti con **200 + risorsa richiesta**.

POSTA ELETTRONICA

Esistono 3 tipi di componenti principali:

- *lo user-agent* → si tratta del mail reader (*Outlook, Thunderbird, ecc.*) che permettono di inviare e ricevere posta dai mail server
- *i mail server* → formati da una mailbox che contiene tutti i messaggi in arrivo per l'utente e dalla coda dei messaggi in uscita (che stanno per essere inviati)
- *il protocollo SMTP (Simple Mail Transfer Protocol)* → usa la porta 25 per trasferire mail dal client al server. Il trasferimento avviene in 3 fasi:
 - *handshaking*
 - *trasferimento dei messaggi*
 - *chiusura*

I messaggi sono codificati in ASCII 7-bit

FORMATO MAIL

Regolarizzato dallo standard RFC 822.

Nell'header troviamo diversi campi tra cui:

- **to:**
- **from:**
- **subject:**

Per mandare altri dati al di fuori del testo, si utilizza MIME (Multipurpose Internet Mail Extensions), regolarizzato da RFC 2045 e 2046; vengono aggiunte delle informazioni nell'header riguardanti il tipo di file che viene inviato e il tipo di codifica utilizzato.

PROTOCOLLO POP3

Insieme ad IMAP, POP3 (Post Office Protocol) è il protocollo utilizzato per scaricare la posta sul proprio client. Il tutto avviene in 3 fasi:

1. *autorizzazione → si dichiarano username e password, se riconosciuti dal server, si apre la connessione*
2. *transazione → vengono scaricati i messaggi*
3. *aggiornamento → vengono cancellati gli eventuali messaggi per cui era stata richiesta la cancellazione e si chiude la connessione*