IL PHYSICAL LAYER DEL TCP/IP

ALGORITMI DI ACCESSO AL MEZZO FISICO

TECNICA A CONTESA

Accesso casuale al canale, se 2 o più stazioni cercano di trasmettere simultaneamente il conflitto viene risolto seguendo alcune regole di mediazione (generalmente si ritenta dopo che è trascorso un tempo t random).

Le prestazioni possono essere calcolate solo statisticamente in base alla probabilità che non si verifichino conflitti sul canale.

- **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection)
  usata dalle reti Ethernet con hub e velocità di 10 Mb/s
- **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance)
  usata dalle reti WI-FI, si basa sulla prevenzione delle collisioni

TECNICA DETERMINISTICA

Ogni trasmissione avviene in un istante definito perciò sicuramente andrà a buon fine dato che la stazione che trasmette è l'unica (in quell'istante) ad avere il **token.**

Le prestazioni possono essere calcolate con certezza → queste reti sono particolarmente adatte per la trasmissione in real time

SOTTOLIVELLO LLC (sottolivello superiore)

Ha il compito di fornire un'interfaccia unificata verso il livello Network a fronte di tecnologie e mezzi trasmissivi diversi. Si può occupare del controllo del flusso di dati

Contiene 2 indirizzi:

- **DSAP** (Destination Service Access Point)

  Identificatore del protocollo di livello superiore (a cui sarà consegnata la PDU)

- **SSAP** (Source Service Access Point)

  Identificatore del protocollo di livello inferiore (da cui è arrivata la PDU)

HEADER LLC				
DSAP 1 Byte	SSAP 1 Byte	CONTROL 1-2 Byte	…	NETWORK PDU

Il campo **Control** può avere 3 formati:

- **Information**
  - usato per trame che trasportano dati in modalità connessa
  - possibilità di trasportare un ACK (messaggio di ritorno)
  - trame dette **I-frame**
- **Supervisor**
  - usato per trasportare informazioni di controllo relative agli I-frame
  - fornisce ACK in assenza di traffico oppure opera il controllo di flusso
  - non prevede la presenza del campo information

    - trame dette **S-frame**
- **Unnumbered**
    - usato per trasportare dati do utente in modalità non connessa
    - usato per trasportare messaggi di controllo del collegamento (diagnostica)
    - trame dette **U-frame**

Il campo **NETWORK PDU** può avere 0 o più byte (non è stabilito un limite ma le PDU troppo grandi sono suddivise dal sottolivello MAC) e contiene la PDU che il livello superiore (Network Layer) si attende di ricevere dal sottolivello MAC in trasmissione.

Il sottolivello LLC prevede 3 modi di funzionamento:

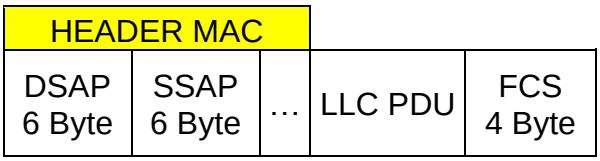
- **Unacknowledged Connectionless Service**
    - costituito solo da primitive di trasferimento dati
    - servizio non affidabile e non orientato alla connessione
    - non richiede conferma della ricezione (ACK)
    - non sono richieste comunicazioni preliminari allo scambio di dati
- **Connection Oriented Service**
    - costituito da primitive (trasferimento e apertura/chiusura) della connessione
    - funzioni per il controllo di errore, di flusso e di sequenza
    - richiede conferma della ricezione (ACK)
    - servizio affidabile e orientato alla connessione
- **Semireliable Connectionless Service**
    - costituito da primitive (trasferimento dati)
    - non è orientato alla connessione ma garantisce la consegna ordinata
    - richiede conferma della ricezione (ACK)
    - non sono richieste comunicazioni preliminari allo scambio di dati

SOTTOLIVELLO MAC (sottolivello inferiore)

Risolve il problema dell'acceso al mezzo trasmissivo condiviso, il suo compito è arbitrare l'accesso. Lo standard MAC (condiviso tra sottolivello MAC e Physical Layer) è diverso per ogni tipo di rete e mezzo fisico di trasmissione (a differenza dell'LLC che è unico)

Anche il sottolivello MAC contiene 2 indirizzi:

- **DSAP** (Destination Service Access Point) → indirizzo MAC sorgente
- **SSAP** (Source Service Access Point) → indrizzo MAC destinatario



- Il campo **LLC PDU** contiene il frame LLC
- Il campo **FCS** (Frame Check Sequence) tecnica di rilevazione degli errori CRC (Cyclic Redundancy Check)

Gli indirizzi MAC possono essere di 3 tipi:

- **Unicast** (stazione singola)
- **Multicast** (gruppo di stazioni)
- **Broadcast** (tutti gli host in rete)

HDLC (High Level Data Link Control)

LLC oltre a essere un sottolivello del Physical Layer è un **protocollo di linea.**

Il **protocollo HDLC** è generalmente utilizzato su reti di grandi dimensioni, può essere usato per gestire connessioni multipunto ma attualmente è usato esclusivamente per connessioni punto-punto.

Il **frame HDLC** è composto da 3 parti racchiuse tra 2 sequenze di flag:

- Header (address + control)
- Data (campo di lunghezza variabile)
- FCS (trailer per il controllo degli errori)

flag	address	control	data	FCS	flag
01111110	8 bit	8 o 16 bit	lunghezza variabile, da 0 o più bit a multipli di 8	16 o 32 bit	01111110

Flag: Sono 2 sequenze di 8 bit (01111110) che racchiudono ogni frame, il loro compito è quello di stabilire la connessione. Inoltre i flag vengono trasmessi in modo continuativo quando non ci sono altre informazioni da trasmettere (linea in idle).

***Bit stuffing*:** in fase di trasmissione viene inserito un bit a “0” dopo che si trovano sequenze di 5 bit a "1", così facendo nessuna sequenza del massaggio potrà essere interpretata come flag. In fase di ricezione, al contrario, viene tolto questo “0” ripristinando il messaggio allo stato originale prima della trasmissione.

Address: Viene utilizzato per le line multipunto per identificare i diversi terminali, utilizzando di norma su connessioni punto-punto non è necessario.

Control: Identico al campo control del frame LLC con i 3 formati.

Data: dati da trasmettere, non esistono limiti di lunghezza dato che la fine della trasmissione viene identificata dal flag.

FCS: codice di ridondanza ciclica (CRC) che viene utilizzato dal ricevitore per controllare la correttezza dei dati ricevuti.

PPP (Point to Point Protocol)

Il protocollo HDLC ha una grave carenza → non possiede una modalità standard per trasmettere sullo stesso canale pacchetti generati da protocolli diversi, di livello superiore.

Il **frame PPP** è composto da 3 parti racchiuse tra 2 sequenze di flag:

- Header (address + contro + protocoll)
- Data (campo di lunghezza variabile)
- FCS (trailer per il controllo degli errori)

flag	address	control	protocol	information	data	FCS	flag
01111110	1 byte	1 byte		0/1550 byte	lunghezza variabile, da 0 o più bit a multipli di 8	2 byte	01111110

La differenza principale rispetto all'HDLC è la presenza di un **campo protocol** che contiene la codifica del protocollo di livello superiore (la cui PDU è contenuta nel **campo information**.

Address: seve SEMPRE contenere la sequenza binaria 11111111 (corrisponde alla codifica broadcast) PPP non assegna indirizzi alle stazioni essendo un protocollo punto-punto.

Control: deve sempre contenere la sequenza 00000011 (indica che si tratta di U-frame) ovvero frame senza numero di sequenza.

Infomration: ha una lunghezza compresa tra 0 e 1500 byte, anche se la lunghezza massima può essere cambiata su negoziazione tra i 2 host.

FCS: la sua lunghezza può essere portata a 4 byte su negoziazione tra i 2 host, viene utilizzato dal ricevitore per controllare la correttezza di quanto ricevuto.

PPP fornisce un metodo standard per trasmettere pacchetti provenienti da più protocolli diverso sullo stesso collegamento seriale, viene principalmente usato per le connessioni punto-punto tra 2 router o nella comunicazione tra utente e provider (es. Internet Service Provider – utente che accede tramite connessione telefonica).

Per fare ciò utilizza:

LCP (Link Control Protocol): protocollo di controllo per creare, configurare e testare la linea, LCP stabilisce e termina la connessione PPP, inoltre negozia le operazioni di configurazione (lunghezza dei campi protocol, information, FCS)

NCP (Network Control Protocol): famiglia di protocolli per configurare i diversi protocolli di rete (es. nel protocollo IP viene utilizzato per negoziare l'attribuzione dell'IP dinamico dell'host)

I protocolli HDLC e PPP sono **protocolli sincroni.**

Nelle **trasmissioni sincrone** i dati da inviare sono raggruppati in frame di molti byte, ogni frame è preceduto da alcuni byte che servono per la sincronizzazione.

La **trasmissione asincrona** permette invece di trasmettere e ricevere un solo byte per volta, delimitato da un bit di start e da un bit di stop, inoltre non è definito il tempo che intercorre tra l'arrivo di un byte e il successivo.

I FRAME ETHERNET

Lunghezza variabile tra 64 e 1518 byte (ottetti)

Esistono 2 formati:

- Ethernet v2.0
- IEEE 802.3

Ethernet v2.0

preamble	SFD	Destin. Add.	Source Add.	Type	data	FCS
7 byte	1 byte	6 byte	6 byte	2 byte	da 46 a 1500 byte	4 byte

Preamble: preambolo con tutti i 7 byte uguali (10101010), ha lo scopo di permettere al destinatario di sincronizzarsi.

SFD (Start Frame Delimiter): è un byte uguale a 11010101 che indica l'inizio del frame.

Destination Address: indirizzo fisico del destinatario (MAC).

Source Adddress: indirizzo fisico del sorgente (MAC)

Type: codice associato al protocollo di livello superiore che ha generato la PDU (Protocol Data Unit) contenuta nel campo data.

Data: dati da trasmettere (può essere vuoto → frame di controllo).

FCS: bit di check del CRC per la rilevazione degli errori in trasmissione.

IEEE 802.3

preamble	SFD	Destin. Add.	Source Add.	Lenght	data	PAD	FCS
7 byte	1 byte	6 byte	6 byte	2 byte	da 46 a 1500 byte	da 0 a 46 byte	4 byte

Lenght: al posto del camp Type, contiene la lunghezza in byte del campo data.

PAD: sequenza ripetitiva che garantisce che la lunghezza minima del frame sia di 64 byte (campo dati vuoto) al fine di rendere possibile distinguere un frame da un frammento di frame a seguito di una collisione.

Inter-frame spacing: ha lo scopo di definire lo spazio temporale minimo tra due frame consecutivi (valore minimo standardizzato nelle reti ethernet è di **96 bit time**).

Wire speed: un dispositivo che trasmette a wire speed sta trasmettendo alla sua massima efficienza trasmissiva. L'efficienza trasmissiva viene espressa in **pps** (packets per second) e viene valutata con i pacchetti di lunghezza minima 64 ottetti (byte).

CSMA/CD

Slot Time = 64 [B] / 10 [MB/s] = 51,2 µs
Tempo di attesa effettivo = r *Slot Time
$0 < r < 2^k-1$
K = min(n, 10) → k = limite di backoff, n = numero di collisioni consecutive

SWITCHING

Negli switch il dominio di collisione non coincide con il domino di broadcast → traffico ridotto ma non si eliminano le collisioni half-duplex.

Viene introdotto il full-duplex, la tecnica CSMA/CD viene superata non avendo più rischio di collisioni.

MAC TABLE (o switch table): tabella dove vengono memorizzati gli indirizzi MAC dei dispositivi connessi alle varie porte dello switch.

TECNICHE DI SWITCHING:

Store-and-foreward: ogni frame che arriva allo switch viene salvato in un buffer e quindi inoltrato o scartato (in base a se l'indirizzo MAC è giusto o meno).

Cut-through: "prendere una scorciatoia" → inizia direttamente a trasmettere.

Fragment-free: applica lo store-and-foreward solo ai primi 64 byte (con lo scopo di verificare eventuali errori)

VULNERABILITÀ DEGLI SWITCH

Per proteggere la rete LAN è utile attivare la **protezione delle porte** negli switch, ogni switch può fornire protezione a 1024 indirizzi MAC + uno impostato come predefinito per ogni porta.

> Es. uno switch a 8 porte potrà fornire protezione a 1032 indirizzi MAC
> 1024 (suddivisi tra le 8 porte) + 8 predefiniti (uno per porta)

Di default tutti gli indirizzi specificati per ogni porta sono protetti permanentemente, si può però specificare un **intervallo di durata** per ogni porta allo scadere del quale gli indirizzi MAC perdono la loro protezione.

Quando un dispositivo si collega l'indirizzo MAC del dispositivo viene confrontato con quello nella tabella dello switch (memorizzata nella NVRAM), se i due indirizzi NON coincidono la porta passa in modalità **disattivazione** (in modo permanente o per un certo intervallo di tempo preconfigurato.

GLI STANDARD WIRELESS

802.11a Sfruttando una delle più versatili tecniche di modulazione poteva raggiungere i 54 Mb/s a 5,2 GHz.

802.11b Ha 2 nuove velocità → 5,5 Mb/s e 11 MB/s a 2,4 GHz. Questo standard è noto come marchio Wi-Fi (Wireless Fidelity) creato dalla **Wi-Fi Alliance.**

Lo standard b ha avuto più successo perché:

- il governo ha mantenuto quella banda di frequenza libera.
- Il 2,4 GHz può coprire una distanza 4 volte superiore al 5 GHz
- Il 5 GHz non oltrepassa gli ostacoli (es. i muri)

Molte apparecchiature sfruttano le bande ISM → possono interferire con il normale funzionamento delle reti domestiche e aziendali.

Ad esempio:

- telefoni cordless
- forni a microonde
- radiocomandi (per cancelli, sistemi di allarme e giocattoli)
- apparati radar
- bluetooth

Nel 2003 è stato creato lo standard 802.11g → 52 Mb/s nella banda a 2,4 GHz

LAN WIRELESS E WIRED

Wireless Terminal dispositivi mobili (notebook, tablet, smartphone) dotati di interfaccia 802.11 integrata o su schede PCMCIA o USB, oppure fissi (PC, stampanti) con schede PCI o adattatori USB.

Access Point hanno un doppio scopo:

- sono dei bridge che collegano la parte cablata (wired) con la parte wireless
- consentono ai Wireless Terminal di collegarsi alla rete wireless fingendo da gateway

Problema stazione esposta: 4 stazioni (A, B, C e D), ascoltando il canale C si sentirà la trasmissione di B e di conseguenza C non potrà trasmettere, mentre possono avvenire le trasmissioni fra A e D.

Soluzione: può essere risolto solo da un'accurata progettazione fisica della rete.

Problema stazione nascosta: 3 stazioni (A, B e C), A sta trasmettendo a B → se C ascolta il canale lo sente libero e sarà convinto di poter trasmettere a B → cominciando a trasmettere disturberà la trasmissione di A → sia A che C sono costretti a ritrasmettere.

Soluzione: può essere risolto con tecniche di **Carrier Sensing Virtuale** → il mittente invia un **frame RTS** (Request To Send) al destinatario, il destinatario risponde con un **frame CTS** (Clear To Send), alla ricezione di questo frame il mittente può iniziare la trasmissione.

AIFS (Arbitration Inter-Frame Space) intervallo durante il quale il trasmettitore attende al fine di accertarsi che non vi siano altri frame RTS e CTS sul canale. Se un'altra stazione tenta di trasmettere provocando una collisione → avviato un algoritmo di **backoff esponenziale binario** (attende un tempo random).