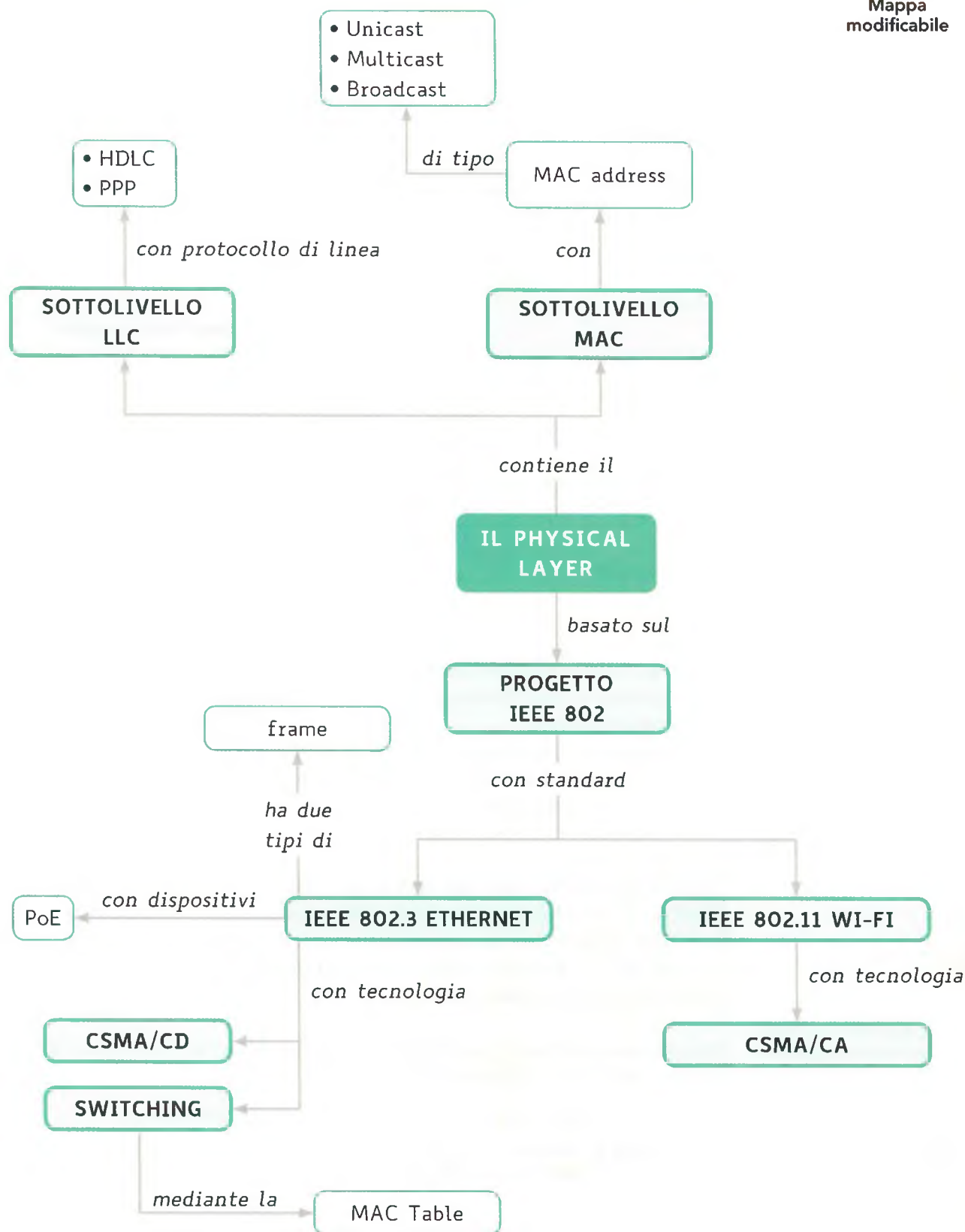




Mapa
modificabile



1 IL PROGETTO IEEE 802

IEEE, ISO e ANSI hanno sviluppato uno standard, noto come **Progetto IEEE 802**, così chiamato in virtù dell'anno (1980) e del mese (febbraio) in cui ebbe ufficialmente inizio, per stabilire come debbano essere realizzate le reti LAN ai livelli Physical e Data Link del modello ISO/OSI in termini di servizi disponibili e di protocolli per l'espletamento di questi servizi.

Gli standard introdotti dal Progetto 802 stabilirono 20 categorie con cui identificare **i diversi modi di accedere al canale di trasmissione** già commercializzate e quelle ancora in fase progettuale:

802	– Overview and Architecture	802.12	– Demand Priority Access Method [100VG AnyLAN]
802.1	– Bridging and Management	802.13	– Cable-TV Based Broadband Networks
802.2	– Logical Link Control	802.14	– Cable Modem LAN
802.3	– CSMA/CD Access Method [Ethernet]	802.15	– Wireless PAN [Bluetooth]
802.4	– Token-Passing Bus Access Method	802.16	– Broadband Wireless MAN
802.5	– Token Ring Access Method	802.17	– Resilient Packet Ring
802.6	– DQDB Access Method	802.18	– Radio Regulatory (Technical Advisory Group)
802.7	– Broadband (Technical Advisory Group)	802.19	– Coexistence (Technical Advisory Group)
802.8	– Fiber-Optic (Technical Advisory Group)	802.20	– Mobile Broadband Wireless Access
802.9	– Isochronous LAN		
802.10	– Interoperable LAN/MAN Security		
802.11	– Wireless LAN [Wi-Fi]		

#techwords

Con **frame** si intende una particolare sequenza di byte suddivisa in campi secondo regole prestabilite.

Il progetto 802 è in continuo aggiornamento e ha prodotto la standardizzazione delle principali tecnologie di rete oggi in uso e la definizione delle regole per passare da una tecnologia all'altra.

Sono per esempio in continuo sviluppo gli standard 802.3 (Ethernet) e 802.11 (Wi-Fi) i cui **#frame** approfondiremo in questa unità. Una parte della standardizzazione del livello Physical è delegata ai diversi enti che regolano le caratteristiche di cavi e connettori (EIA, TIA, ecc.) come abbiamo visto nel volume del terzo anno.

Il livello Physical deve preoccuparsi dell'accesso alla rete di comunicazione tenendo presente che le trasmissioni broadcast condividono un unico canale e che quindi è necessario verificare che il canale sia effettivamente libero prima di effettuare una trasmissione, risolvendo eventuali conflitti tra più stazioni che vogliano accedere contemporaneamente alla risorsa.

Occorre allora stabilire un algoritmo di accesso, cioè una tecnica che regoli il diritto a trasmettere sul canale condiviso.

Due sono le possibilità: la tecnica a contesa e la tecnica deterministica.

- La **tecnica a contesa** prevede l'accesso casuale al canale e se due o più stazioni cercano di trasmettere simultaneamente, il conflitto viene risolto secondo alcune regole di mediazione. Le prestazioni possono essere calcolate solo statisticamente, in relazione alla probabilità che all'inizio di una trasmissione non vi sia una con-

LEZIONE ONLINE

IEEE 802.5: TOKEN RING

È uno standard con topologia ad anello (ring) unidirezionale creato dall'IBM nel 1976. L'accesso al mezzo fisico è deterministico mediante una tecnica di token passing: il gettone (token) gira nell'anello, chi se ne impossessa trasmette e poi rilascia il token.

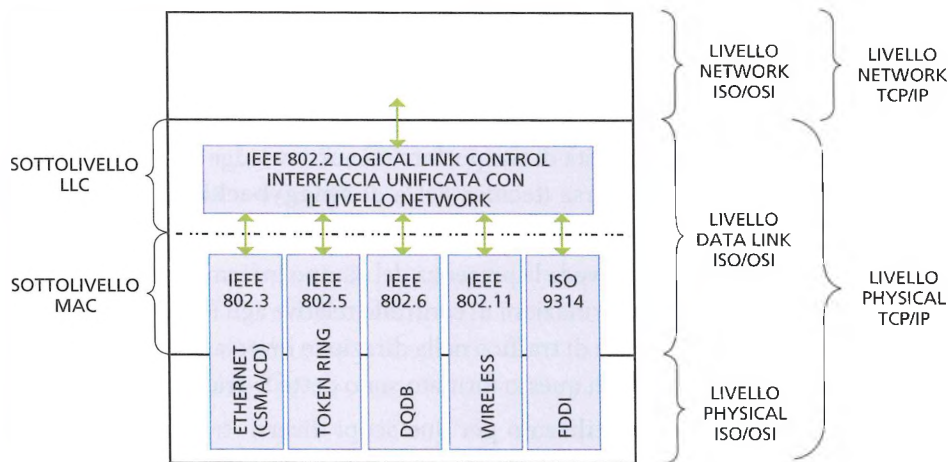
tesa tra stazioni per l'accesso al mezzo trasmissivo. Non è quindi possibile stabilire a priori l'intervallo di tempo necessario per portare a termine una trasmissione. La più nota tecnica a contesa è la **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) basata sulla gestione delle collisioni. Le reti Ethernet (IEEE 802.3) con hub e velocità di 10 Mbps utilizzano questa tecnica che verrà approfondita nella Lezione 5.

Un'altra tecnica è la **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance) basata sulla prevenzione delle collisioni. Le reti Wi-Fi (IEEE 802.11) utilizzano questa tecnica che verrà approfondita nella Lezione 7.

- La **tecnica deterministica** dà luogo a reti deterministiche, in cui ogni trasmissione avviene in un istante definito e sicuramente va a buon fine, dato che in quell'istante la stazione trasmittente è l'unica a possedere l'accesso al canale. Le prestazioni delle reti non a contesa possono essere determinate con precisione, rendendo le reti particolarmente adatte alle trasmissioni in real time. Le più note tecniche deterministiche sono quelle basate su un **token** (gettone) che autorizza a trasmettere chi se ne impossessa. Lo standard Token Ring (IEEE 802.5) utilizza questa tecnica che viene approfondita nella lezione online.

Le architetture di rete hanno dovuto tenere conto delle diverse tecnologie e dei metodi di accesso alternativi standardizzati dal Progetto 802.

In particolare il livello Data Link di ISO/OSI è stato suddiviso in due sottolivelli: **LLC** (Logical Link Control) e **MAC** (Media Access Control) che rappresentano il cuore del Progetto 802 (FIGURA 1).



LEZIONE ONLINE

IEEE 802.6: DQDB (Distributed Queue Dual Bus)

Si tratta di uno standard progettato agli inizi degli anni '90 per fungere da dorsale (backbone) di interconnessione di LAN diverse (Ethernet, Token Ring, ...) creando così reti metropolitane (MAN) o geografiche (WAN) generalmente in fibra ottica.

LEZIONE ONLINE

ISO 9314: FDDI (Fiber Distributed Data Interface)

È uno standard che rappresenta un'evoluzione della Token Ring sempre basato sul token passing ma con un doppio anello (dual ring) in fibra ottica. I due anelli sono unidirezionali e in opposizione, cioè le trasmissioni fluiscono in direzioni opposte.

FIGURA 1
Sottolivelli
LLC e MAC

FISSA LE CONOSCENZE

- In che cosa consiste il Progetto IEEE 802?
- Il livello Physical di TCP/IP quali livelli di ISO/OSI comprende?
- Che cosa si intende per tecnica a contesa?
- Che cosa si intende per tecnica deterministica?

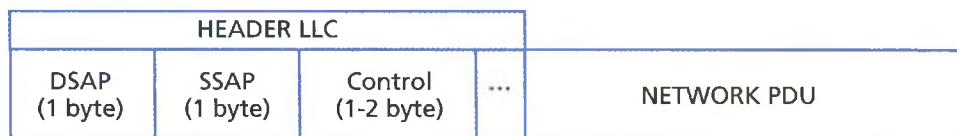
2 I SOTTOLIVELLI LLC E MAC

2.1 Il sottolivello LLC

Il sottolivello superiore è l'**LLC** che ha il fondamentale compito di fornire un'interfaccia unificata verso il livello Network, pur a fronte di tecnologie trasmissive e mezzi fisici differenziati. Può inoltre occuparsi del controllo del flusso di trasferimento dei dati.

Poiché a livello di Network possono operare vari protocolli (il principale è IP), il sottolivello LLC deve individuare qual è il protocollo usato per la comunicazione. Proprio per questo scopo il frame di LLC (**FIGURA 2**) contiene due indirizzi, da un byte ciascuno, detti **DSAP** (Destination Service Access Point) e **SSAP** (Source Service Access Point), che rappresentano rispettivamente l'identificatore del protocollo di livello superiore, cui deve essere consegnato il frame (**PDU**) ricevuto, e l'identificatore del protocollo di livello superiore, da cui il packet è arrivato nel dialogo tra due peer entity.

FIGURA 2 Il frame LLC



#techwords

Il **piggybacking** è la tecnica per cui il destinatario può rimandare l'invio dell'ACK includendolo nel successivo messaggio inviato al mittente. In questo caso si può dire che il messaggio inviato "piggybacks" (porta con sé) l'ACK relativo all'ultima ricezione avvenuta.

Il campo **Control** può essere lungo 1 o 2 byte e avere 3 formati:

- il formato **information** è usato per le trame che trasportano i dati in modalità connessa e ha anche la possibilità di trasportare un acknowledge (ACK) per la trasmissione nella direzione inversa (tecnica detta di **#piggybacking**). Le trame di questo formato sono dette **I-frame**;
- il formato **supervisor** non prevede la presenza del campo information nella trama ed è usato per trasportare informazioni di controllo relative agli I-frame; per esempio, fornire un ACK in assenza di traffico nella direzione inversa oppure operare il controllo di flusso. Le trame di questo formato sono dette **S-frame**;
- il formato **unnumbered** è utilizzato per due scopi diversi: trasportare dati di utente in modalità non connessa e trasportare messaggi di controllo del collegamento (inizializzazione, diagnostica, ecc.). Le trame di questo formato sono dette **U-frame**.

Il campo **NETWORK PDU** può avere 0 o più byte (non è stabilito un limite massimo, ma PDU troppo grandi potrebbero essere frammentate dal sottolivello MAC) che contengono la PDU che il livello superiore (Network Layer) si attende di ricevere dal sottolivello MAC in ricezione o invia al sottolivello MAC in trasmissione.

Il sottolivello LLC prevede 3 modi di funzionamento:

- **Unacknowledged Connectionless Service:** costituito solo da primitive di trasferimento dati, è un servizio non affidabile e non orientato alla connessione.

È costituito da singoli datagrammi che vengono trasmessi in modo indipendente l'uno dall'altro, senza richiedere conferma sulla ricezione (ACK) e senza alcuna forma di correzione degli errori né di controllo di flusso. Qualora tali funzioni siano necessarie, devono essere fornite dai protocolli di livello superiore. Non sono richieste comunicazioni preliminari allo scambio dei dati;

- **Connection Oriented Service:** costituito da primitive di trasferimento e di apertura e chiusura di una connessione con le funzioni per il controllo di errore, di flusso e di conservazione della sequenza. È un servizio affidabile e orientato alla connessione quindi richiede la conferma della ricezione (ACK);
- **Semireliable Connectionless Service:** costituito anch'esso solo da primitive di trasferimento dati ma, pur essendo non orientato alla connessione, prevede una conferma di ricezione (ACK) per i datagrammi inviati e garantisce la consegna ordinata dei dati trasmessi. Anche in questo caso non sono richieste comunicazioni preliminari allo scambio dei dati.

2.2 Il sottolivello MAC

Il sottolivello inferiore è il **MAC** che risolve il problema dell'accesso al mezzo trasmissivo condiviso. Cioè il suo compito è arbitrare l'accesso all'unico mezzo trasmissivo comune tra tutti i sistemi che hanno necessità di trasmettere in una determinata rete.

Quindi mentre l'LLC è unico, si avrà invece uno standard MAC (condiviso tra sottolivello MAC e livello Physical) diverso per ogni tipo di rete e mezzo fisico di trasmissione.

Anche il frame del MAC (FIGURA 3) contiene due indirizzi di tipo **DSAP** e **SSAP**, detti proprio **indirizzi MAC** del sorgente e del destinatario, che hanno evidentemente lo scopo di identificare l'indirizzo fisico delle due peer entity che si stanno scambiando la PDU destinata al, o in arrivo dal, sottolivello LLC.

HEADER MAC			LLC PDU	FCS (4 byte)
DSAP (6 byte)	SSAP (6 byte)	...		

FIGURA 3 Il frame MAC

Il campo **LLC PDU** contiene il frame LLC (mostrato in Figura 2).

L'**FCS** (Frame Check Sequence) è la tecnica di correzione degli errori in trasmissione **CRC** (Cyclic Redundancy Check) affrontata nel terzo anno.

Ricordiamo anche che l'indirizzo MAC è costituito da 6 byte rappresentati da 12 cifre esadecimali raggruppate in sei coppie separate da un trattino.

Per esempio:

08-00-2B-C4-BE-F3

Gli indirizzi MAC possono essere di 3 tipi:

- **unicast:** individua una stazione singola;

#prendinota

La caratteristica fondamentale dell'indirizzo MAC è di essere univoco: non esistono due indirizzi MAC uguali, cioè non ci sono due schede di rete (quindi due host) con lo stesso MAC.

- **multicast:** individua un gruppo di stazioni. In questi casi si trasmette per primo il bit meno significativo (bit 0) del primo byte messo a 1. La rappresentazione formale è del tipo:

FF-FF-FF-[0:F]X-XX-XX

usata per indicare tutti gli host che hanno scheda di rete di qualsiasi produttore con la prima cifra del terzo byte compresa tra 0 e F;

- **broadcast:** **FF-FF-FF-FF-FF-FF** individua tutti gli host connessi alla rete.

Per sapere l'indirizzo MAC della scheda di rete del proprio computer in ambiente Windows è sufficiente aprire (per esempio con start-esegui-cmd) il prompt dei comandi e digitare **ipconfig/all**.

Tra le molte informazioni che compariranno ci sarà

Scheda Ethernet Connessione alla rete locale (LAN)

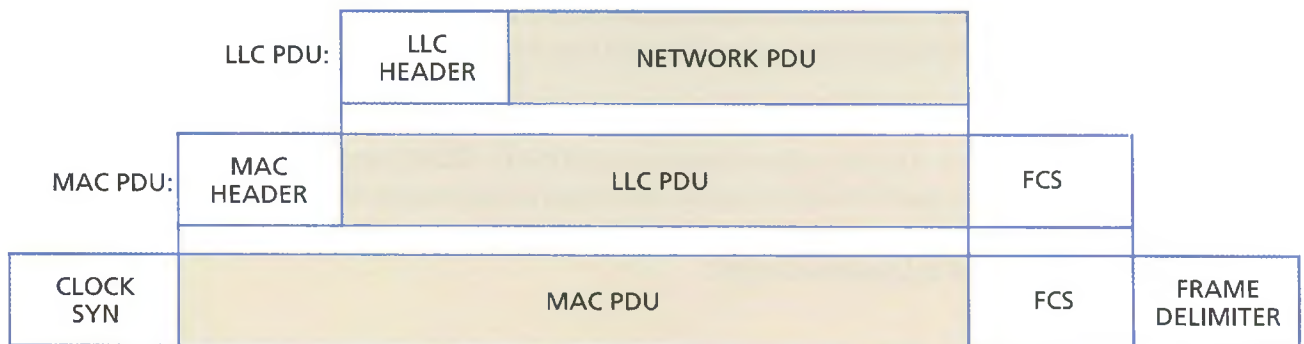
seguita dalla descrizione del produttore e del modello della scheda.

Subito sotto si potrà leggere l'indirizzo fisico, cioè il MAC address che stavamo cercando.

Anche le schede wireless hanno un indirizzo fisico e anch'esso è rilevabile col comando **ipconfig/all**.

Come in tutti i modelli a strati il passaggio di livello (e sottolivello in questo caso) produce l'operazione di **incapsulamento** del frame, come mostrato nella **FIGURA 4**.

FIGURA 4 L'operazione di incapsulamento



Ricordiamo che nelle architetture a livelli, gli header incapsulati a un certo livello (o sottolivello) verranno letti solo dal corrispondente livello (o sottolivello) dell'host con cui si sta comunicando.

Il meccanismo dell'incapsulamento serve proprio a questo: a far sì che ogni livello (o sottolivello) inoltri la PDU incapsulata ricevuta, analizzandone solo l'header e disinteressandosi del resto.

FISSA LE CONOSCENZE

- Spiega a che cosa serve il sottolivello superiore LLC.
- Che cosa rappresentano i due indirizzi contenuti nel frame LLC?
- Spiega a che cosa serve il sottolivello MAC.
- Che cosa rappresentano i due indirizzi contenuti nel frame MAC?
- Gli indirizzi MAC si dividono in 3 tipi. Quali sono?

3 L'EVOLUZIONE DI LLC: HDLC E PPP

3.1 HDLC (High Level Data Link Control)

LLC oltre a essere un sottolivello del Physical Layer è un **protocollo di linea** (data link protocol) standardizzato nel Progetto 802 con la sigla IEEE 802.2.

I protocolli di linea sono i protocolli (di livello 2 ISO/OSI: Data Link) che vengono utilizzati sulle linee pubbliche per la trasmissione di dati, progettati per canali geografici di tipo punto-punto o multipunto.

Tali protocolli formano una famiglia i cui componenti più importanti sono LLC, HDLC e PPP.

Il protocollo adottato per LLC, il cui frame abbiamo visto nella Figura 2 della Lezione precedente, è una versione semplificata di HDLC.

Il **protocollo HDLC** è generalmente utilizzato su reti di grandi dimensioni. Può essere usato per connessioni multipunto, ma attualmente è usato quasi esclusivamente per collegamenti punto-punto. Lo standard OSI prevede esplicitamente l'adozione di HDLC.

Numerose sono state le specifiche emesse dall'ISO relative a questo protocollo, l'ultimo standard, pubblicato nel 2002, che rende obsoleti tutti i precedenti è ISO 13239. In HDLC lo scambio delle informazioni avviene con frame di formato fisso.

Il frame HDLC è composto da 3 parti: un header (costituito dai campi address e control), un campo dati a lunghezza variabile e un trailer per il controllo degli errori (FCS). Il tutto racchiuso tra due sequenze di flag (**FIGURA 5**).

FIGURA 5 Il frame HDLC

flag	address	control	data	FCS	flag
01111110	8 bit	8 o 16 bit	lunghezza variabile, 0 o più bit a multipli di 8	16 o 32 bit	01111110
← header →			← trailer →		

Vediamo nel dettaglio i singoli campi:

- **flag**: due particolari sequenze di 8 bit 01111110, che racchiudono ogni frame. Hanno il compito di stabilire la sincronizzazione, inoltre vengono trasmessi in modo continuativo quando non ci sono altre informazioni da trasmettere (la linea è idle). Accorgimenti particolari devono essere perciò usati nella trasmissione di sequenze di bit in cui figurino più di 5 bit a 1 consecutivi. In particolare, in trasmissione viene inserito un bit a 0 dopo 5 bit a 1 consecutivi (**bit stuffing**); in ricezione questo bit viene tolto in modo da ricostituire la sequenza originale;
- **address**: si utilizza solo per linee multipunto per identificare i diversi terminali, infatti il protocollo HDLC si usa di norma su link punto-punto e quindi non necessita di un indirizzo di destinazione;
- **control**: resta identico al campo control del frame LLC con i 3 formati: information (I-frame), supervisor (S-frame) e unnumbered (U-frame);

#prendinota

La tecnica del **bit stuffing** garantisce che solo il carattere flag contenga 6 bit a 1 consecutivi. Infatti il bit stuffing analizza la trama (flag esclusi) prima di trasmetterla e inserisce un bit a 0 dopo 5 bit a 1 consecutivi (indipendentemente dal valore del bit successivo). Il ricevitore, se riceve una sequenza di 5 bit a 1 e uno 0, elimina lo 0 che era stato inserito dal bit stuffing, se riceve 6 bit a 1 e uno 0 identifica il carattere flag.

#prendinota

La tecnica a finestra prevede di non inviare il riscontro a ogni messaggio ricevuto, ma solo dopo una finestra di n messaggi. La tecnica di **sliding window** è un'evoluzione della tecnica a finestra in cui non è più necessario terminare una finestra prima di aprirne un'altra.

- **data**: contiene i dati da trasmettere. Non esistono limiti di lunghezza per questo campo visto che sarà la sequenza flag a determinare la fine della trama (l'operazione di bit stuffing fa sì che non siano trasmesse sequenze consecutive di bit a 1 superiori a 5, evitando qualsiasi confusione con la sequenza di flag);
- **FCS** (Frame Check Sequence): è il codice di ridondanza ciclica (CRC) che viene utilizzato dal ricevitore per controllare la correttezza di quanto ricevuto.

Il protocollo HDLC sfrutta il sistema di trasmissione a finestre scorrevoli (**sliding window**) che permette un incremento della velocità generale del sistema.

I tempi di trasmissione possono essere relativamente lunghi e conviene pertanto spedire più frame di seguito, considerato che è assai più probabile che un frame risulti ricevuto correttamente piuttosto che distrutto o alterato.

3.2 PPP (Point to Point Protocol)

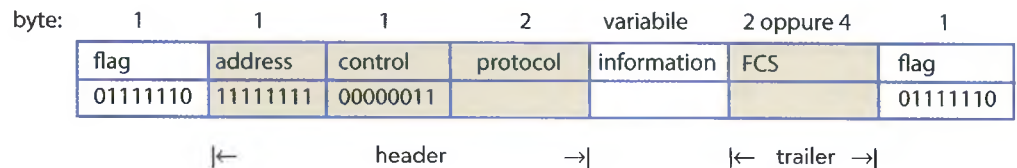
Il protocollo HDLC ha una grave carenza: non ha una modalità standard per trasmettere sullo stesso canale pacchetti generati da protocolli diversi, di livello superiore. Per questo motivo la comunità di Internet ha introdotto nel luglio 1990 una estensione di HDLC, basata sullo standard ISO 4335, detta **PPP**.

La differenza principale rispetto all'HDLC risiede nella presenza di un campo **protocol** lungo 2 byte. Tale campo contiene la codifica del protocollo di livello superiore la cui PDU è contenuta nel campo **information**, per esempio al protocollo IP corrisponde il codice esadecimale 0021h.

Il frame PPP è composto da 3 parti: un header (costituito dai campi address, control e protocol), un campo dati a lunghezza variabile e un trailer per il controllo degli errori (FCS).

Il tutto racchiuso tra due sequenze di flag (**FIGURA 6**).

FIGURA 6 Il frame PPP



Le specifiche di PPP definiscono anche il contenuto dei campi del frame, ponendo delle limitazioni:

- **address** deve sempre contenere la sequenza binaria 11111111 che corrisponde alla codifica broadcast. PPP non assegna indirizzi alle stazioni essendo un protocollo punto-punto;
- **control** deve sempre contenere la sequenza 00000011 a indicare che si tratta di un U-frame, cioè un frame senza numero di sequenza. La lunghezza del campo control è quindi sempre pari a 1 byte e la trasmissione è di tipo non connesso;
- **information** ha una lunghezza compresa tra 0 e 1500 byte (standard dei cosiddetti pacchetti Ethernet), anche se la lunghezza massima può essere cambiata su negoziazione tra i due host mittente e destinatario;

- **FCS** ha una lunghezza di 2 byte, ma può essere portato a 4 byte su negoziazione tra i due host, mittente e destinatario. È il codice di ridondanza ciclica (CRC) che viene utilizzato dal ricevitore per controllare la correttezza di quanto ricevuto.

PPP fornisce un metodo standard per trasmettere pacchetti provenienti da più protocolli diversi, sullo stesso collegamento seriale. Principalmente viene usato per la comunicazione punto-punto tra due router o nella comunicazione tra utente e provider (per esempio, tra Internet Service Provider e utente che accede tramite una connessione telefonica).

Per fare ciò utilizza:

- un protocollo di controllo **LCP** (Link Control Protocol) per creare, configurare e testare la linea; LCP stabilisce e termina la connessione PPP e negozia le opzioni di configurazione, per esempio la lunghezza dei campi protocol, information o FCS;
- una famiglia di protocolli **NCP** (Network Control Protocol) per configurare i diversi protocolli di rete; per esempio, nel caso del protocollo di rete IP, viene usato per negoziare l'attribuzione dell'indirizzo IP dinamico all'host (DHCP: Dynamic Host Configuration Protocol che vedremo nell'Unità 7).

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

Nelle **trasmissioni sincrone** i dati da inviare sono raggruppati in frame di molti byte e ogni frame viene preceduto da alcuni byte per la sincronizzazione che permettono al ricevitore di sincronizzarsi con il trasmettitore. Il ricevitore ricava dai byte di sincronismo un segnale di clock locale che pilota la lettura dei restanti bit di dati.

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

Per questi motivi le trasmissioni sincrone sono più veloci di quelle asincrone, ma hanno lo svantaggio che un solo bit errato danneggia l'intero frame.

#prendinota

La trasmissione **asincrona** è così chiamata perché l'intervallo di tempo tra il bit finale di una trasmissione e il bit iniziale della successiva è indefinito.

FISSA LE CONOSCENZE

- Descrivi il frame del protocollo HDLC.
- In che cosa il protocollo PPP migliora il protocollo HDLC?
- In quali contesti si usa il protocollo PPP?
- Che differenza c'è tra una trasmissione sincrone e una asincrona?