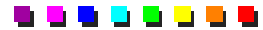




HDLC e PPP

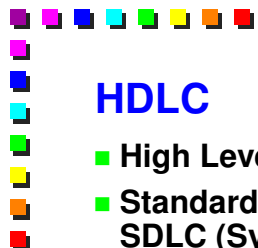
Silvano GAI
Pietro Nicoletti



Nota di Copyright

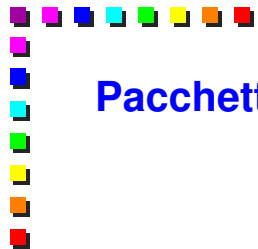
- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.



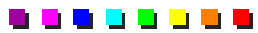
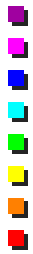
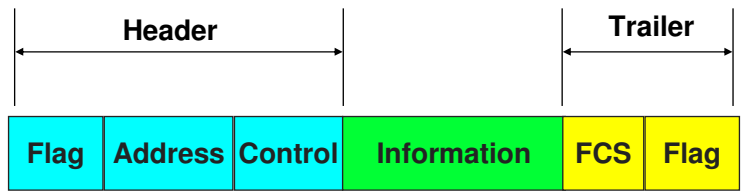


HDLC

- High Level Data Link Control
- Standard ISO derivato dal protocollo IBM/SNA SDLC (Synchronous Data Link Control)
- Altri protocolli della stessa famiglia:
 - LAPB (Link Access Procedure Balanced)
 - LAPD (Link Access Procedure D-channel)
 - LAPF (Link Access Procedure to Frame mode Bearer Services)
 - LLC (Logical Link Control) - 802.2



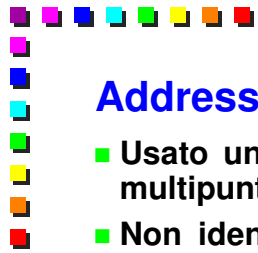
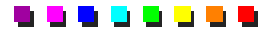
Pacchetto HDLC





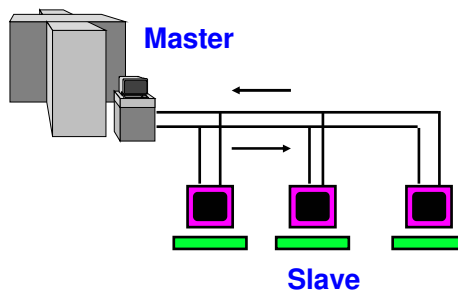
Flag

- Il carattere Flag è un marcatore di Inizio/Fine trama (01111110)
- La tecnica del “bit stuffing” impedisce che il carattere Flag compaia erroneamente nel campo dati
 - in fase di trasmissione, inserisce un bit a zero addizionale dopo 5 bit a uno consecutivi, indipendentemente dal valore del bit successivo
 - in fase di ricezione, ignora un bit a zero dopo 5 bit a uno consecutivi



Address

- Usato unicamente per la gestione delle linee multipunto
- Non identifica il protocollo di livello 3 come nel caso di LLC



Control

- Utilizzato per disporre di tre diversi tipi di pacchetto:
 - Information
 - Supervisor
 - Unnumbered (00000011)
- che consentano di utilizzare HDLC:
 - come protocollo connesso
 - come protocollo non-connesso
- Su rete geografica si adotta la modalità connessa che usa tutti e tre i tipi di pacchetti



Tipi di trame e numerazione

- Information
 - Dati in modalità connessa
 - Acknowledge
- Supervisor
 - Acknowledge
- Unnumbered
 - Dati in modalità non connessa
 - Iniziare e terminare connessioni
- Numeri di sequenza
 - Usati in fase di trasmissione e di acknowledge
 - Due schemi di numerazione possibili:
 - modulo 8
 - modulo 128



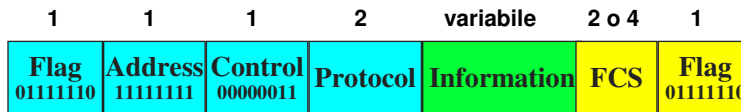
HDLC e CDN

- HDLC è idoneo a collegare tramite un CDN:
 - due bridge remoti
 - due router monoprotocollo
- HDLC non fornisce un supporto multiprotocollo nativo e non è quindi adatto a collegare:
 - router multiprotocollo di costruttori diversi
 - brouter

Point to Point Protocol (PPP)

- Metodo per l'imbastamento di pacchetti su link seriali di tipo punto-punto
 - estensione di HDLC con *supporto multiprotocollo*
 - supporta comunicazioni full-duplex
 - può trasportare protocolli di livello 2 e 3
 - adatto per connettere host, bridge e router
- RFC1661 - Status Standard (rende obsoleti gli RFC 1548 - 1331)

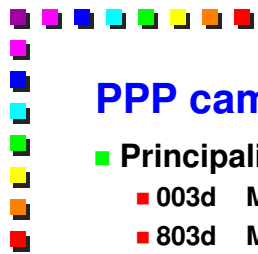
Point to Point Protocol (PPP)



- Il campo Protocol contiene l'identificativo del tipo di protocollo trasportato
- Information field contiene i dati
 - MRU (Maximum Receive Unit) 1500 byte di default

PPP campo di Protocol

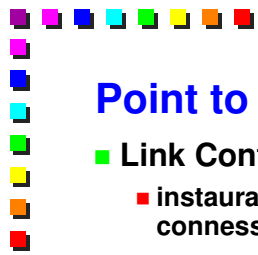
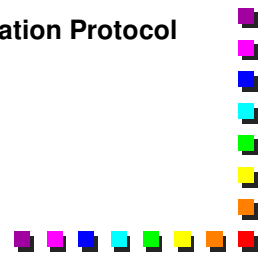
- Principali codici protocollo
 - 0021 Internet Protocol
 - 0023 OSI Network Layer
 - 0027 DECnet Phase IV
 - 0029 Appletalk
 - 002b Novell IPX
 - 0031 Bridging PDU
 - 8021 Internet Protocol Control Protocol
 - 8023 OSI Network Layer Control Protocol
 - 8027 DECnet Phase IV Control Protocol
 - 8029 Appletalk Control Protocol
 - 802b Novell IPX Control Protocol
 - 8031 Bridging NCP



PPP campo di Protocol

■ Principali codici protocollo

- 003d Multi-Link
- 803d Multi-Link Control Protocol
- 80fd Compression Control Protocol
- 0201 802.1d Hello Packets
- c021 Link Control Protocol
- c023 Password Authentication Protocol
- c025 Link Quality Report
- c223 Challenge Handshake Authentication Protocol



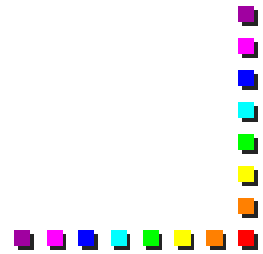
Point to Point Protocol (PPP)

■ Link Control Protocol (LCP)

- instaurazione, configurazione e controllo delle connessioni

■ Network Control Protocol (NCP)

- famiglia di protocolli per configurare vari protocolli di rete



Comunicazione su link seriali

- Invio di pacchetti LCP per configurare e collaudare il collegamento di livello data-link
- Negoziazione dei parametri opzionali di livello data-link
- Invio di pacchetti NCP per scegliere e configurare uno o più protocolli di livello rete
- Invio dei pacchetti di livello rete
- Il link rimane operativo fino a che non viene chiuso esplicitamente mediante un pacchetto LCP o NCP

IP Control Protocol

- NCP per IP
- Negoziazione del protocollo di compressione
- Negoziazione dell'indirizzo IP locale
 - notifica dell'indirizzo proposto
 - richiesta dell'indirizzo da usare
- Negoziazione dell'indirizzo IP remoto
 - proposta di un indirizzo
 - richiesta dell'indirizzo remoto

Autenticazione

■ Password Authentication Protocol (PAP) RFC 1334

- il router che richiede il collegamento invia nome e password in chiaro
- il router locale conferma la connessione

■ Challenge Handshake Authentication Protocol (CHAP) RFC 1994

- il router locale manda un pacchetto CHAP ad un altro durante la fase di apertura della connessione
- il router remoto è sfidato (challenged) a rispondere
 - una password crittografata
 - un valore casuale
 - il proprio nome

Controllo della qualità

■ Pacchetti Link Quality Report (LQR) sono inviati periodicamente

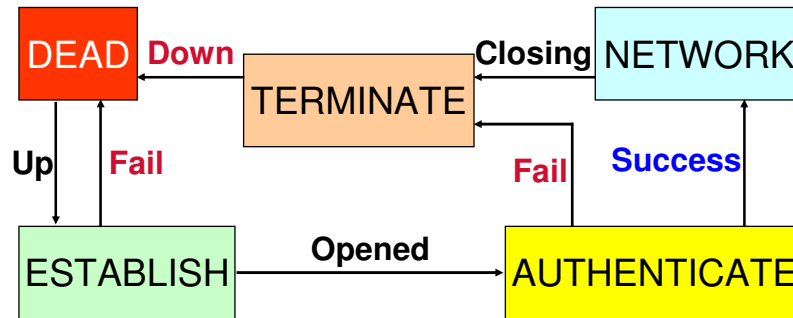
- ad un LQR viene risposto con l'invio di un LQR

■ La qualità del collegamento è controllata

- qualità in uscita: rapporto tra il traffico ricevuto all'altro estremo e quello generato localmente
- qualità in ingresso: rapporto tra il traffico ricevuto e quello generato all'altro estremo

■ Se la qualità scende sotto una soglia predefinita, la connessione è abbattuta

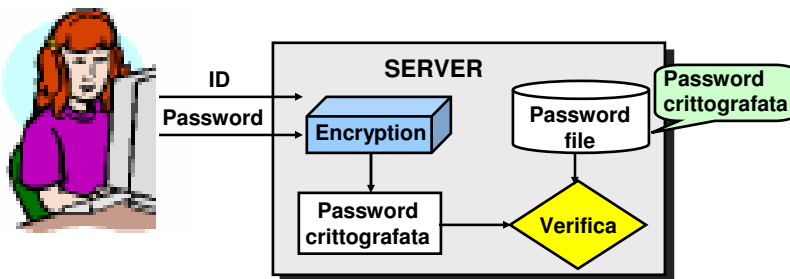
Diagramma a stati del PPP



Meccanismo di autenticazione PAP

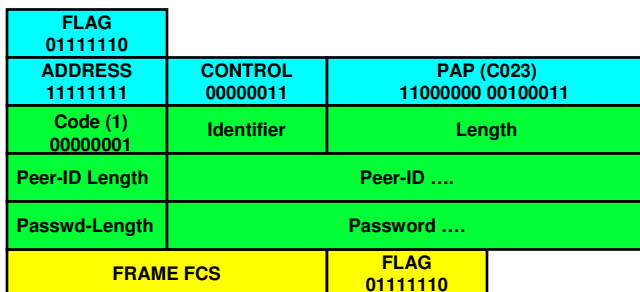
■ Server di autenticazione

- il Server mantiene la password crittografata nel *password-file*
- la password inviata dall'utente non viene crittografata
- il Server crittografa la password ricevuta dall'utente e la verifica con la password mantenuta nel *password-file*



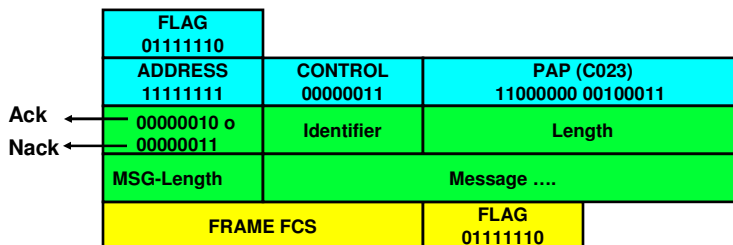
PAP: Password Authentication Protocol

- Autenticazione in 2 fasi:
 - richiesta di autenticazione (Authenticate-Request)
 - conferma di autenticazione
- Pacchetto PAP Authenticate-Request



PAP: Password Authentication Protocol

- Pacchetto PAP Authenticate Ack e Nack
- Ack (codice 2) conferma di autenticazione
- Nack (codice 3) autenticazione fallita



CHAP: Challenge-Handshake Authentication Protocol

- Il protocollo CHAP fornisce una protezione contro gli attacchi di tipo playback attraverso l'uso di:
 - un identificativo che cambia in modo incrementale
 - un valore di sfida variabile
- Per limitare l'esposizione temporale di ogni singolo attacco la sfida viene ripetuta periodicamente



CHAP: Challenge-Handshake Authentication Protocol

- Il protocollo CHAP verifica periodicamente l'identità dell'estremità opposta connessa che avviene in 3 fasi:
 - fase 1 (sfida): dopo aver stabilito la connessione l'autenticatore lancia un messaggio di sfida (challenge) all'estremità opposta
 - *identifier* che identifica la sfida
 - fase 2: l'estremità opposta risponde alla sfida con un *valore calcolato* e lo stesso *identifier* ricevuto precedentemente
 - fase 3: l'autenticatore verifica la risposta con il proprio valore calcolato
 - ad intervalli casuali l'autenticatore ripete la sfida cambiando *identifier* e *valore*



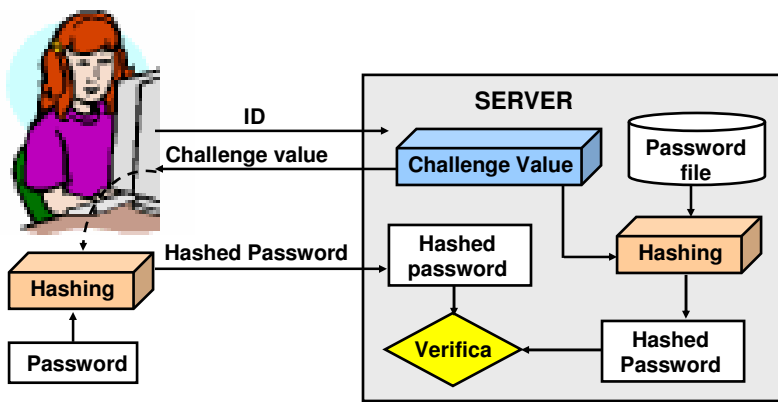
Meccanismo di autenticazione CHAP

■ Autenticazione in dettaglio

- Il server mantiene la password nel *password-file*
- Il server crea un valore di sfida e lo invia all'utente
- alla password utente viene applicata una funzione di hashing in combinazione con il valore di sfida inviato dal server che produce un valore o parola chiave che viene inviata al server
- il server applica una funzione di hashing combinata con il valore di sfida precedentemente inviato e confronta il risultato con la parola chiave ricevuta, a cui era stata applicata la stessa funzione di hashing



Meccanismo di autenticazione CHAP



Multilink PPP

- RFC 1990 Status Standard (rende obsoleto lo RFC 1717)
- Studiato aggregare canali multipli sugli accessi ISDN di tipo Base e Primario
- Crea un link virtuale costituito da due o più canali
- Può frammentare i pacchetti suddividendo i frammenti sui vari canali ad un'estremità e riassemblare i pacchetti all'estremità opposta



Frammentazione Multilink PPP

FLAG 01111110			
ADDRESS 11111111		CONTROL 00000011	PROTOCOL (003d) 00000000 00111101
B	E	0	0
0	0	0	0
0	0	0	0
Sequence numb.		Sequence number (L)	
Fragment data ...			
FRAME FCS		FLAG 01111110	

- Bit B (beginning) quando è impostato a 1 indica che il frammento è quello iniziale del pacchetto
- Bit E (ending) quando è impostato a 1 indica che il frammento è quello terminale del pacchetto



PPP Bridging Control Protocol

- RFC 1638 (Status Standard)
- Il PPP identifica e trasporta MAC-PDU differenti:
 - Ethernet/802.3 - MAC Type 1
 - Token Bus/802.4 - MAC Type 2
 - Token Ring/802.5
 - MAC Type 3 non canonical addresses
 - MAC Type 11 canonical addresses
 - FDDI
 - MAC Type 4 non canonical addresses
 - MAC Type 12 canonical addresses
- Supporta spanning tree multipli e VLAN (definiti su standard 802.1G - Remote Bridge)



Imbustamento frame 802.3/Ethernet

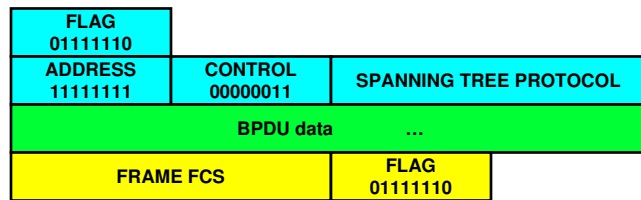
FLAG 01111110		
ADDRESS 11111111	CONTROL 00000011	PROTOCOL (0031) 00000000 00110001
F Z 0 Pads	MAC TYPE	LAN ID high word (optional)
LAN ID low word (optional)		DESTINATION MAC ADDRESS
DESTINATION MAC ADDRESS		
SOURCE MAC ADDRESS		
SOURCE MAC ADDRESS		LENGTH/TYPE
LLC DATA ...		
potential line protocol pad		
FRAME FCS		FLAG 01111110



Imbustamento BPDU

Il campo Spanning Tree protocol:

- valore 0201 = IEEE 802.1D o 802.1G
- valore 0203 = IBM Source Route Bridge
- valore 0205 = DEC LANbridge 100



PPP LAN Extension

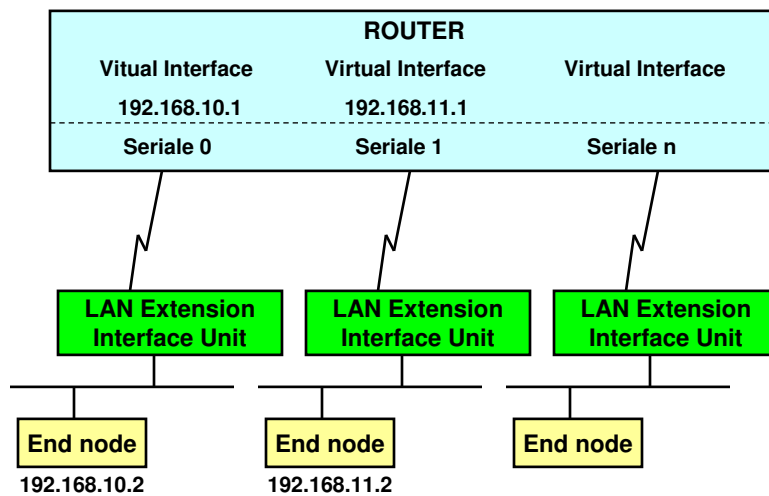
- RFC 1841- Status Informational
- Permette di collegare una piccola LAN via linea seriale a un router remoto
- E' necessario avere un apparato denominato **LAN extension interface unit** che collega la LAN al router remoto centrale via linea seriale
- Il router crea una **virtual interface** che rispecchia le caratteristiche della LAN extension unit (funzione di mirror)
 - la virtual interface assume gli stati (up o down) della LAN extension interface unit e identifica la LAN extension Interface Unit tramite il suo indirizzo MAC

PPP LAN Extension

- Il router è come se avesse il piccolo gruppo di macchine collegato localmente, ma con la banda di una linea seriale
 - il protocollo LAN extension interface trasferisce le frame MAC al router centrale attraverso la linea seriale
 - all'estremità opposta il router inoltra le frame di livello 3
 - è ammessa una sola subnet per LEX
 - l'indirizzo IP della virtual interface nel router deve essere nella stessa subnet delle macchine della LAN connessa alla LAN extension unit
 - la LAN extension unit non ha indirizzo IP



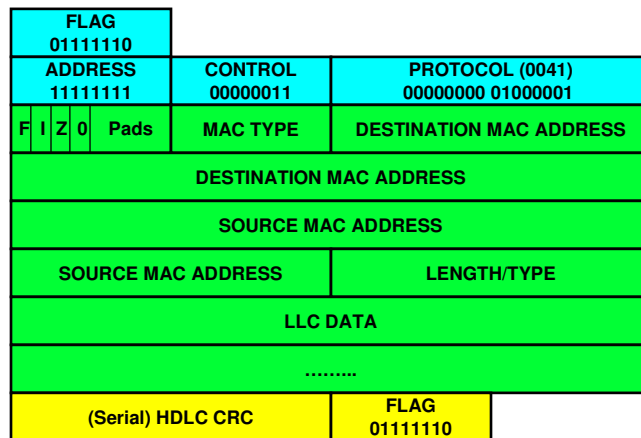
Topologia PPP LAN Extension



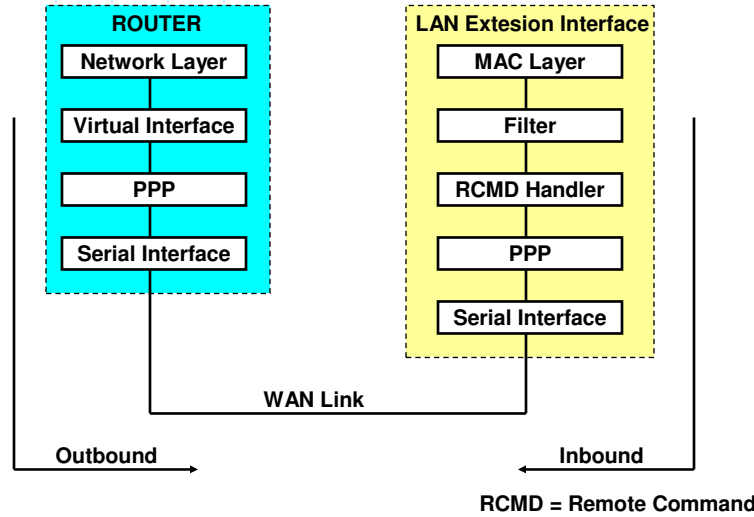
PPP LAN Extension o Bridge?

- PPP LEX assomiglia alla connessione bridge, ma si differenzia per:
 - l'apparato LAN Extension Interface Unit dipende sempre dal router e non può operare in modalità standalone o essere connessa back-to-back con un'altra LEX Unit
 - LEX Unit non adotta lo spanning tree
 - la LEX Unit trasferisce i pacchetti MAC in modo simile al bridge, ma il router a cui viene connessa può operare sia in modalità routing, sia bridging

Formato pacchetto dati PPP-LEX



Architettura LAN extension interface



LEX Inbound

■ La funzione di inbound:

- la LAN Extension Unit riceve e filtra eventualmente (permit o deny per MAC addr. o protocollo) le frame dalla LAN
- incapsula le frame MAC nel PPP e le trasmette sulla WAN
- il router toglie la busta PPP e passa le frame alla Virtual Interface che gestisce le gestisce come se le avesse ricevute dalla sua interfaccia locale e le inoltra con tecnica di routing o bridging

LEX outbound

■ La funzione di outbound:

- la Virtual Interface decide se inoltrare le frame in base ai filtri definiti sulla LAN Extension Unit
- la Virtual Interface del router costruisce la frame completa di header ed indirizzi MAC
 - nella fase di startup la LAN Extension Unit invia il suo indirizzo MAC per autenticarsi e lo fissa alla corrispondente Virtual Interface sul router
- il router aggiunge la busta PPP e la trasmette sulla WAN
- la LAN Extension Interface Unit rimuove la busta PPP ed inoltra la frame sulla LAN