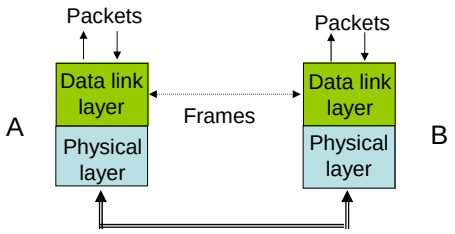
Data Link Protocols



Data Links Services

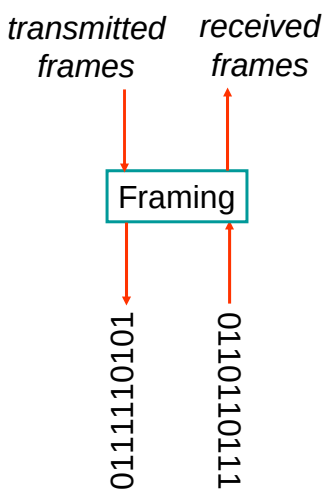
- Framing
- Error control
- Flow control
- Multiplexing
- Link Maintenance
- Security: Authentication & Encryption

- Directly connected, wire-like
- Losses & errors, but no out-of-sequence frames
- Applications: Direct Links; LANs; Connections across WANs

Examples

- PPP
- HDLC
- Ethernet LAN
- IEEE 802.11 (Wi Fi) LAN

5.4 Framing



- Mapping stream of physical layer bits into frames
- Mapping frames into bit stream
- Frame boundaries can be determined using:
  - Character Counts
  - Control Characters
  - Flags
  - CRC Checks

Character-Oriented Framing

Data to be sent

A	DLE	B	ETX	DLE	STX	E

After stuffing and framing

DLE	STX	A	DLE	DLE	B	ETX	DLE	DLE	STX	E	DLE	ETX

- Frames consist of integer number of bytes
  - Using ASCII to transmit printable characters
  - Octets with HEX value <20 are nonprintable
- Special 8-bit patterns used as control characters
  - STX (start of text) = 0x02; ETX (end of text) = 0x03;
- Byte used to carry non-printable characters in frame
  - DLE (data link escape) = 0x10
  - DLE STX (DLE ETX) used to indicate beginning (end) of frame
  - Insert extra DLE in front of occurrence of DLE STX (DLE ETX) in frame
  - All DLEs occur in pairs except at frame boundaries

Framing & Bit Stuffing

HDLC frame

Flag	Address	Control	Information	FCS	Flag

any number of bits

- Frame delineated by flag character
- HDLC uses *bit stuffing* to prevent occurrence of flag 01111110 inside the frame
- Transmitter inserts extra 0 after each consecutive five 1s *inside* the frame
- Receiver checks for five consecutive 1s
  - if next bit = 0, it is removed
  - if next two bits are 10, then flag is detected
  - If next two bits are 11, then frame has errors

Example: Bit stuffing & de-stuffing

(a) Data to be sent

0110111111111100

After stuffing and framing

*01111110*0110111110111110000*01111110*

(b) Data received

01111110000111011111011111011001111110

After destuffing and deframing

000111011111-11111-110

Byte-Stuffing in PPP

- PPP is character-oriented version of HDLC
- Flag is 0x7E (01111110)
- Control escape 0x7D (01111101)
- Any occurrence of flag or control escape inside of frame is replaced with 0x7D followed by

original octet XORed with 0x20 (00100000)

Data to be sent

41	7D	42	7E	50	70	46

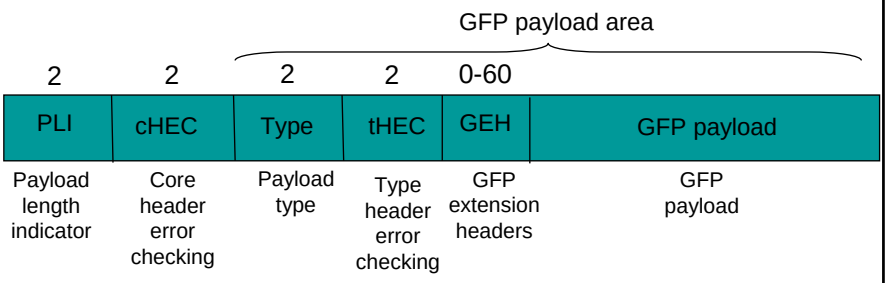
7E	41	7D	5D	42	7D	5E	50	70	46	7E

After stuffing and framing

Byte-Stuffing in PPP

- 7D → 7D 5D 7E → 7D 5E
- Problems with PPP byte stuffing
  - Size of frame varies unpredictably due to byte insertion
  - Malicious users can inflate bandwidth by inserting 7D & 7E

Generic Framing Procedure



- GFP combines frame length indication with CRC
  - PLI indicated length of frame, then simply count characters
  - cHEC (CRC-16) protects against errors in count field (single-bit error correction + error detection)
- GFP designed to operate over octet-synchronous physical layers (e.g. SONET)

5.5 PPP: Point-to-Point Protocol

- Data link protocol for point-to-point lines in Internet
  - Router-router; dial-up to router

1. Provides *Framing and Error Detection*
   - Character-oriented HDLC-like frame structure
2. *Link Control Protocol*
   - Bringing up, testing, bringing down lines; negotiating options
   - ***Authentication***: key capability in ISP access
3. A family of *Network Control Protocols* specific to different network layer protocols
   - IP, OSI network layer, IPX (Novell), Appletalk

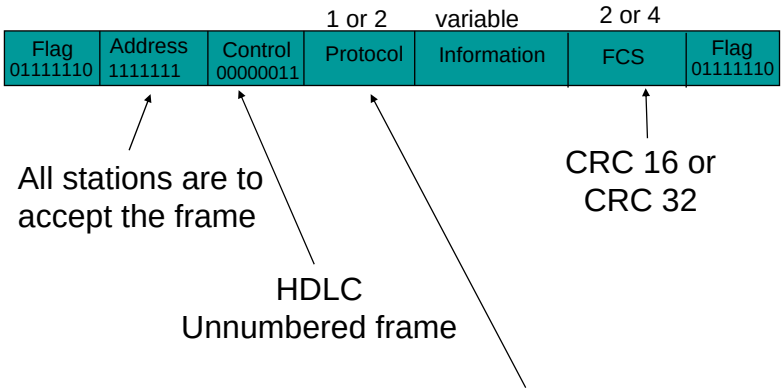
PPP Applications

PPP used in many point-to-point applications

- Telephone Modem Links 30 kbps
- Packet over SONET 600 Mbps to 10 Gbps
  - IP→PPP→SONET

- PPP is also used over shared links such as Ethernet to provide LCP, NCP, and authentication features
  - PPP over Ethernet (RFC 2516)
  - Used over DSL

PPP Frame Format



- PPP can support multiple network protocols simultaneously
- Specifies what kind of packet is contained in the payload
  - e.g. LCP, NCP, IP, OSI CLNP, IPX...

PPP Authentication

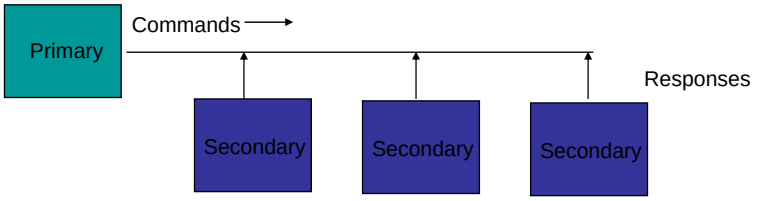
- Password Authentication Protocol
  - Initiator must send ID & password
  - Authenticator replies with authentication success/fail
  - After several attempts, LCP closes link
  - Transmitted <u>unencrypted,</u> susceptible to eavesdropping
- Challenge-Handshake Authentication Protocol (CHAP)
  - Initiator & authenticator share a secret key
  - Authenticator sends a challenge (random # & ID)
  - Initiator computes cryptographic checksum of random # & ID using the shared secret key
  - Authenticator also calculates cryptographic checksum & compares to response
  - Authenticator can reissue challenge during session

5.6 High-Level Data Link Control (HDLC)

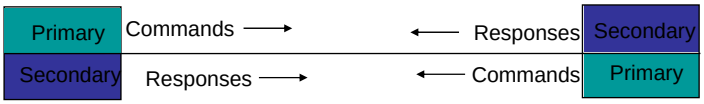
- Bit-oriented data link control
- Derived from IBM Synchronous Data Link Control (SDLC)
- Related to Link Access Procedure Balanced (LAPB)
  - LAPD in ISDN
  - LAPM in cellular telephone signaling

HDLC Data Transfer Modes

- Normal Response Mode
  - Used in polling multidrop lines



- Asynchronous Balanced Mode
  - Used in full-duplex point-to-point links



HDLC Frame Format

Flag	Address	Control	Information	FCS	Flag

- Control field gives HDLC its functionality
- Codes in fields have specific meanings and uses
  - Flag: delineate frame boundaries
  - Address: identify *secondary* station (1 or more octets)
  - Control: purpose & functions of frame (1 or 2 octets)
  - Information: contains user data; length not standardized, but implementations impose maximum
  - Frame Check Sequence: 16- or 32-bit CRC

Control Field Format

Information Frame

1	2-4	5	6-8
0	N(S)	P/F	N(R)

Supervisory Frame

1	0	S	S	P/F	N(R)

Unnumbered Frame

1	1	M	M	P/F	M	M	M

- S: Supervisory Function Bits
- N(R): Receive Sequence Number
- N(S): Send Sequence Number
- M: Unnumbered Function Bits
- P/F: Poll/final bit used in interaction between primary and secondary

Information frames

- Each I-frame contains sequence number N(S)
- Positive ACK piggybacked
  - N(R)=Sequence number of *next* frame expected acknowledges all frames up to and including N(R)-1
- 3 or 7 bit sequence numbering
  - Maximum window sizes 7 or 127
- Poll/Final Bit
  - NRM: Primary polls station by setting P=1; Secondary sets F=1 in *last* I-frame in response
  - Primaries and secondaries always interact via *paired* P/F bits

Supervisory frames

Used for error (ACK, NAK) and flow control (Don't Send):

- *Receive Ready* (RR), SS=00
  - ACKs frames up to N(R)-1 when piggyback not available
- *REJECT* (REJ), SS=01
  - Negative ACK indicating N(R) is first frame not received correctly. Transmitter must resend N(R) and later frames
- *Receive Not Ready* (RNR), SS=10
  - ACKs frame N(R)-1 & requests that no more I-frames be sent
- *Selective REJECT* (SREJ), SS=11
  - Negative ACK for N(R) requesting that N(R) be selectively retransmitted

Unnumbered Frames

- Setting of Modes:
  - SABM: Set Asynchronous Balanced Mode
  - UA: acknowledges acceptance of mode setting commands
  - DISC: terminates logical link connection
- Information Transfer between stations
  - UI: Unnumbered information
- Recovery used when normal error/flow control fails
  - FRMR: frame with correct FCS but impossible semantics
  - RSET: indicates sending station is resetting sequence numbers
- XID: exchange station id and characteristics