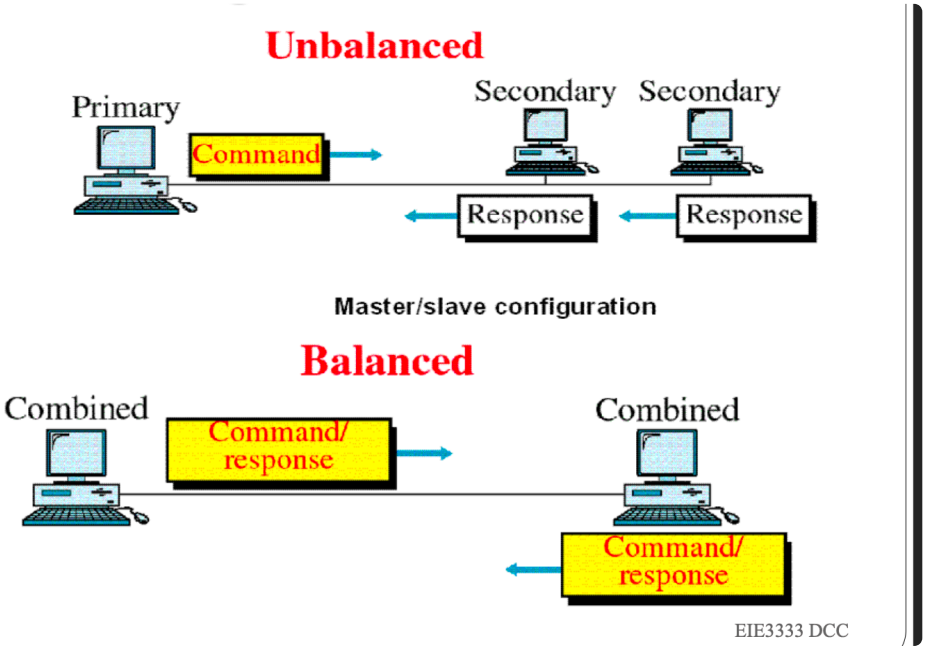
lecture 5 Data Link Layer - HDLC&PPP

High-level Data Link Control (HDLC)

- half-duplex and full-duplex communications over point to point and multipoint links
- bit-oriented protocol, data section of a frame is a sequence of bits
- ASCII
- 3 types of stations, 2 link configurations, and 3 data transfer modes
  - Station type
    - Primary Station - complete control of the link and sends commands to secondary stations
    - Secondary Station - receives commands and send response to primary station
    - Combined Station - sends command and response
  - Configurations
    - Unbalanced - One primary station and one or more secondary station
    - Balanced - Two combined stations

HDLC Configurations



HDLC Transfer Modes

- a mode in HDLC is the relationship between two devices involved in an exchange
- the mode or communication describes who controls the link
- support three modes of communication between stations:
  - Normal Response Mode (NRM)
  - Asynchronous Balanced Mode (ABM)
  - Asynchronous response mode (ARM)

Normal Response Mode

- Used with an unbalanced configuration
- Refers to the standard primary-secondary relationship
- The primary may initiate the data transfer to a secondary, but a **secondary may only transmit date in response to a command from the primary**
  - it must have permission from the primary device before transmitting

Asynchronous Balanced Mode (ABM)

- Used with a balanced configuration
- All stations are equal and therefore only combined stations connected in point-to-point are used
- **Either combined station may initiate transmission with the other combined station without permission**

	NRM	ABM
Station type	Primary & Secondary	Combined
Initiator	Primary	Any

EIE3333 DCC

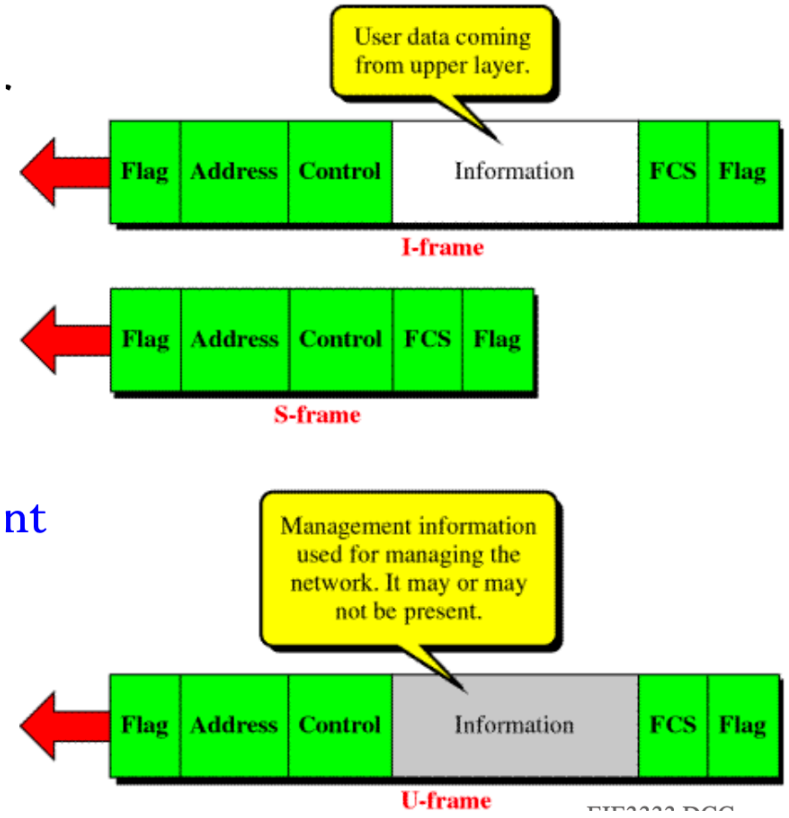
HDLC Frame types

Three types of frames, each with a different control field format

- **Information frames (I-frames)**
  - Used to transport user data and control information relating to user data
- **Supervisory frames (S-frames)**
  - Used only to transport control information, primarily data link layer ==flow control and error control ==
- **Unnumbered frames (U-frames)**
  - Reserved for system management, information carried by U-frames is intended for managing the link itself

HDLC Frame Structures

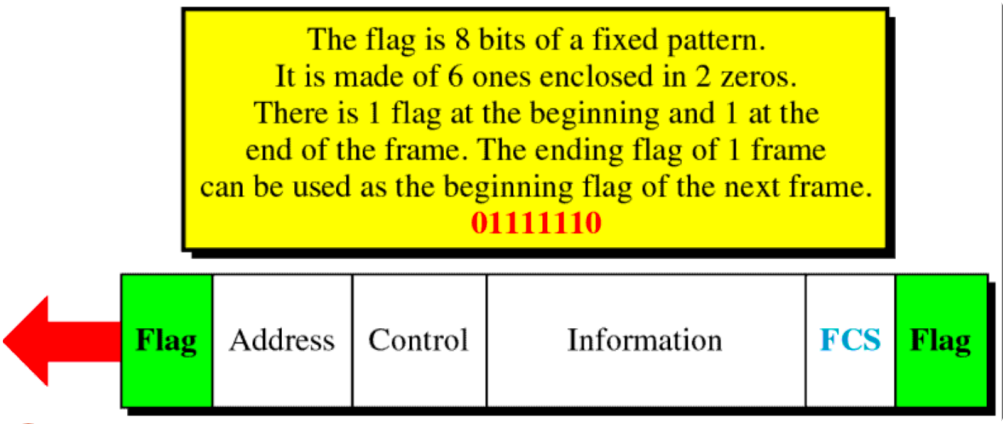
- six fields
  - Beginning flag
  - Address
  - Control
  - Information (absent in S-frames)
  - Frame Check Sequence (FCS)
  - Ending flag



- The flag, address, and the control fields that precede the information field are known as a header
- the frame check sequence and flag fields following the data field referred to as a trailer

Flag Field of HDLC frame

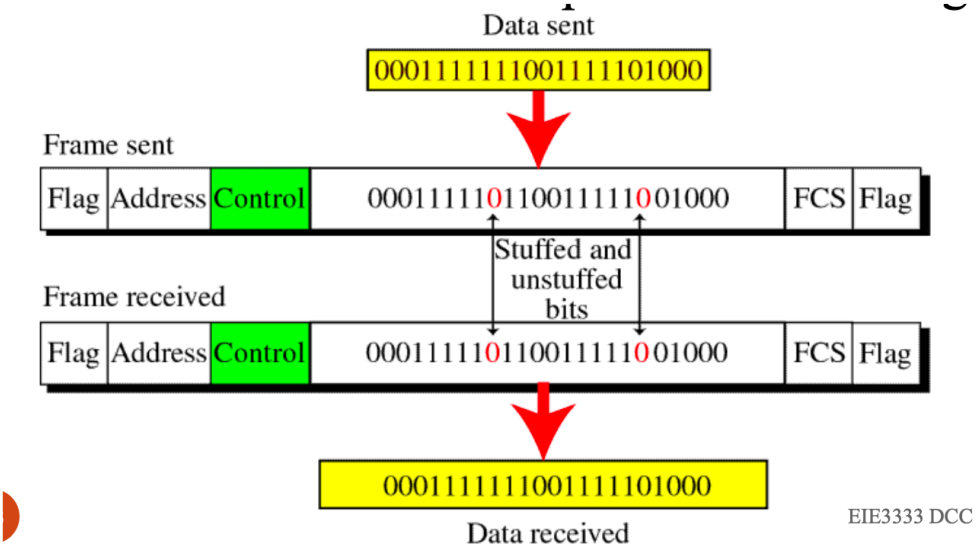
- Flag field is an 8-bit pattern of `01111110`, which delimits the frame at both ends
- It is a synchronization pattern for the receiver
  - 接收端识别 `01111110` 作为 **同步信号**，帮助定位帧的起点。



- Problem: data field of HDLC may contain the same sequence pattern
- Solution: Bit stuffing
  - Guarantee the flag field sequence does not appear anywhere else in the frame

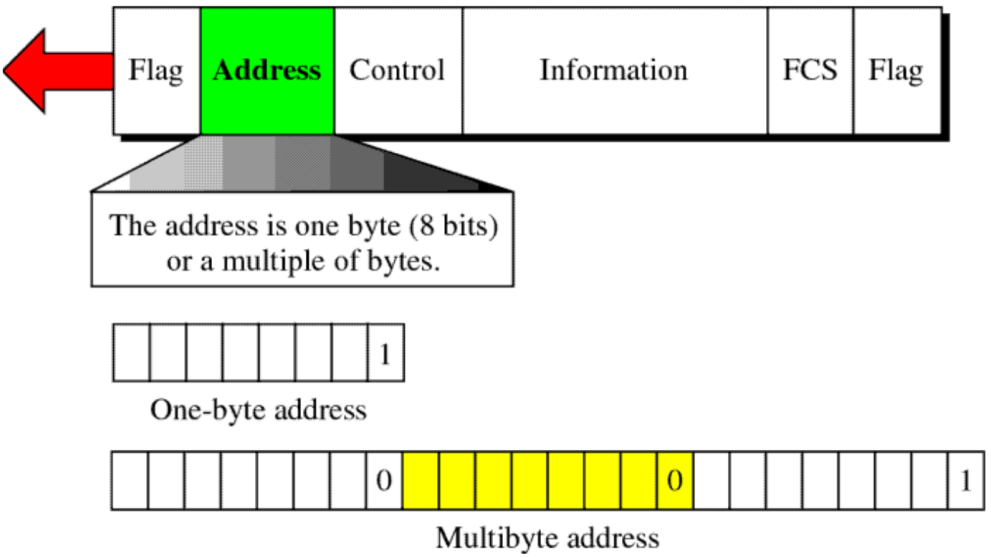
Bit stuffing in HDLC

- Process of adding one extra 0 whenever there are five consecutive 1s in the data
- Receiver does not mis interpret the data as flag



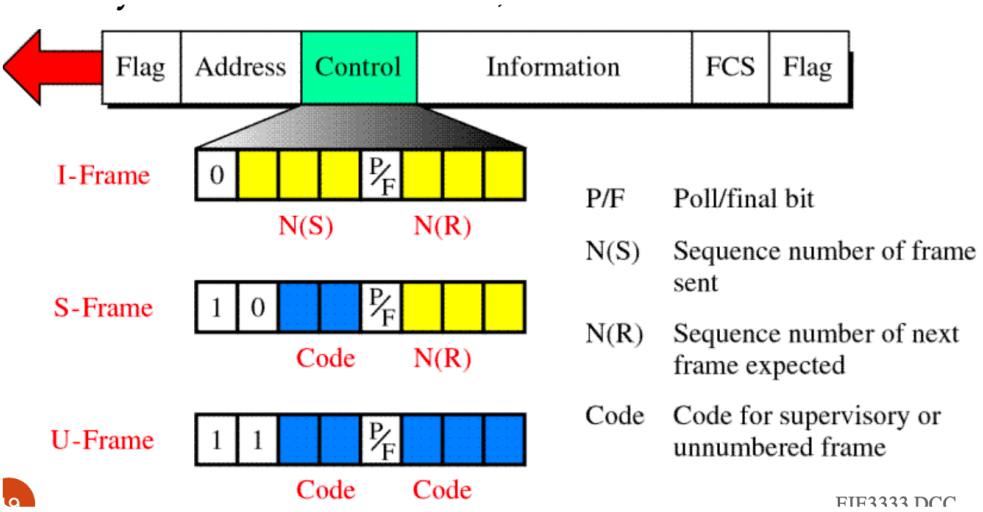
Address Field of HDLC Frame

- Address field contains the address of the secondary station that is either the originator or destination of the frame
- usually one byte, i.e. 8 bits long, but a large network may require multiple-byte address fields:
  - The actual address length is a multiple of 7 bits
  - The rightmost bit of each octet is 1 if it is the last octet of the address field, and 0 otherwise; the remaining 7 bits of each octet form part of the address.



Control Field of HDLC Frame

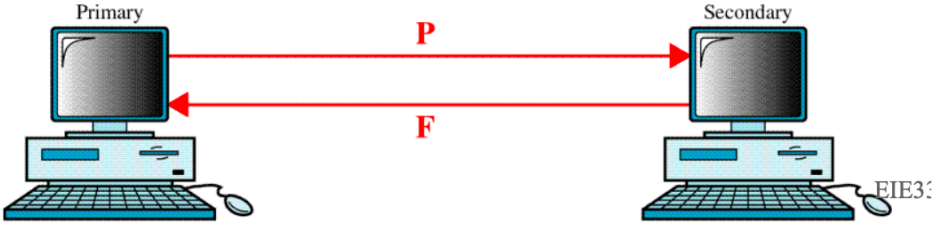
- The control field determines the type of frame and defines its functionality. It a one-byte segment (could be two bytes in some situations)



P/F field of Control field

The single-bit P/F field has a dual purpose and has meaning only when it is set (bit = 1) and can mean poll or final.

- It means poll (or select) when the frame is sent by a primary station to a secondary (the address field contains the receiver address), asking whether the secondary has anything to send.
- It means final when the frame is sent by a secondary to a primary 从站发送 F=1 帧，表示它对主站的请求作出最终响应 (the address field contains the sender address): Secondary replies that there is nothing to send; otherwise it would reply with an I-frame



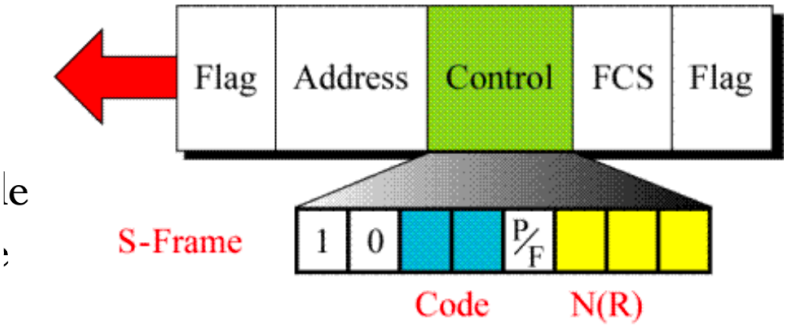
N(S) and N(R) in Control Field for flow control

- I-frame contains both N(S) and N(R) fields
- S-frame contains an N(R) only
  - S-frame are used to return N(R) for flow control when the receiver does not have data to send
- U-frame has neither N(S) nor N(R) field

- U-frames are used for system management information, not for user data exchange or acknowledgment

Control Codes in S-Frame

- S-frame is used for acknowledgment, flow control, and error control
- the control is used to define the type of S-Frame: four types



Code	Command	
00	RR	Receive ready
01	REJ	Reject
10	RNR	Receive not ready
11	SREJ	Selective-reject

RR (Receive Ready): 00

- acknowledges the receipt of a safe and sound frame or group of frame
- the value of N(R) defines the acknowledgment number

> **Note**
>
> - N(R) 是一个序列号，它表示 接收方已经成功接收了所有编号小于 N(R) 的帧，并且期待收到编号为 N(R) 的帧。
>
>   ...
> - N(R) 也是确认编号（ACK Number），在 HDLC 的 监督帧（Supervisory Frame, S-Frame） 或 无编号帧（Unnumbered Frame, U-Frame）中，N(R) 用来告知发送方 哪些帧已经被正确接收。

RNR (Receive Not Ready): 10

- acknowledges the receipt of a frame or group of frames and it announces that receiver is busy and cannot receive more frames
- congestion-control mechanism 拥塞控制机制 by asking sender to slow down
- The value of N(R) is the acknowledgment number.

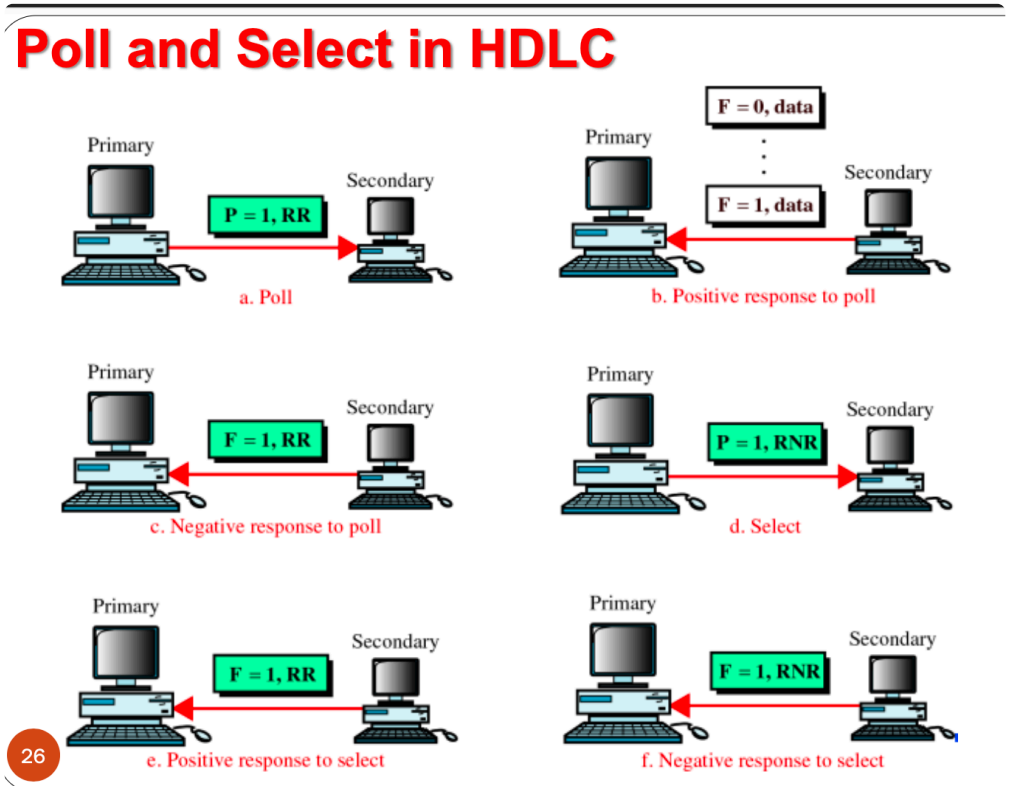
REJ (Reject): 01

- a NAK frame, but not like the one used for selective repeat ARQ
- used in Go-Back-N ARQ
- Before the sender timer expires, that the last frame is lost or damaged
- The value of N(R) is the negative acknowledgment number.

SREJ (Selective-reject): 11

- a NAK frame used in Selective Repeat ARQ
- term selective reject instead of selective repeat
- The value of N(R) is the negative acknowledgment number

Poll and Select in HDLC

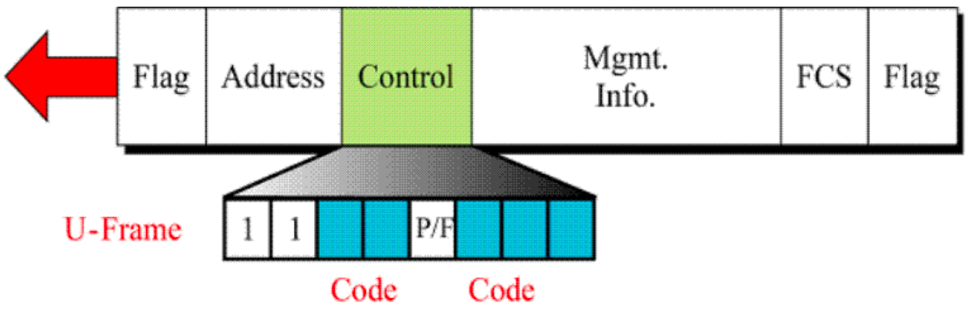


	对比项	Poll（轮询）	Select（选择）
1	作用	询问从站是否有数据要发送	通知从站主站有数据要发送
2	触发者	主站主动轮询 从站	主站主动通知 从站
3	适用场景	从站发送数据	主站发送数据
4	主要信号	P=1（轮询请求）	P=1（RNR）+ F=1（RR）
5	响应方式	从站如果有数据，则发送数据，否则发送 RR	从站如果繁忙，先发送 RNR；恢复后发送 RR
6	是否需要从站先发送数据	是	否

- Poll（轮询）： 主站请求从站发送数据，适用于 主站被动等待从站的数据。
- Select（选择）：主站通知从站它要发送数据，适用于 主站主动发送数据。

Control Codes of U-Frame

- used to exchange session management and control information between connected devices

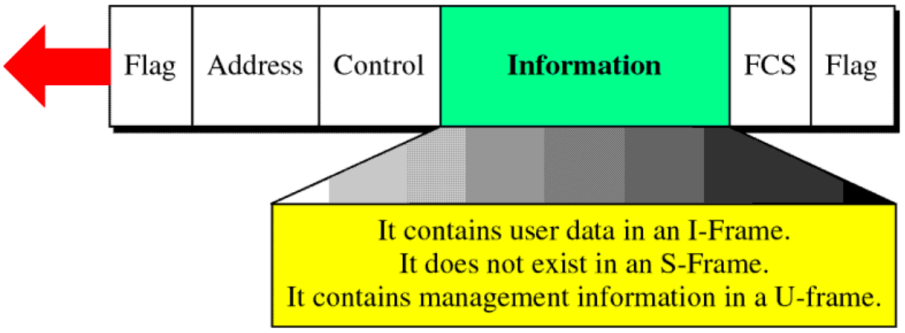


- 2+3 control bits in U-frames, 32 possible combinations
- 5 types:
  - Mode setting - set NRM, ARM or ABM modes
  - Disconnection - negative acknowledgement of mode setting commands
  - Unnumbered exchange - exchange of specific data such as data and time
  - Initialization mode - initialize data link functions
  - Miscellaneous - exchange of address, resetting of sequence numbers, etc

Code	*Command*	*Response*	*Meaning*
00 001	SNRM		Set normal response mode
11 011	SNRME		Set normal response mode, extended
11 100	SABM	**DM**	Set asynchronous balanced mode or **disconnect mode**
11 110	SABME		Set asynchronous balanced mode, extended
00 000	UI	**UI**	Unnumbered information
00 110		**UA**	**Unnumbered acknowledgment**
00 010	DISC	**RD**	Disconnect or **request disconnect**
10 000	SIM	**RIM**	Set initialization mode or **request information mode**
00 100	UP		Unnumbered poll
11 001	RSET		Reset
11 101	XID	**XID**	Exchange ID
10 001	FRMR	**FRMR**	Frame reject

Information Field and Piggybacking

- Contain user data (variable length) in I-frame
- Contains network management data (if any) in U-frames
- The main purpose of I-frames is to carry user data in the Information field, but they also use N(S) and N(R) fields to acknowledge receipt of frames
- The combination of data and acknowledgement in one single frame is called Piggybacking
- Frame check sequence is for error detection
  - 2 or 4 byte CRC

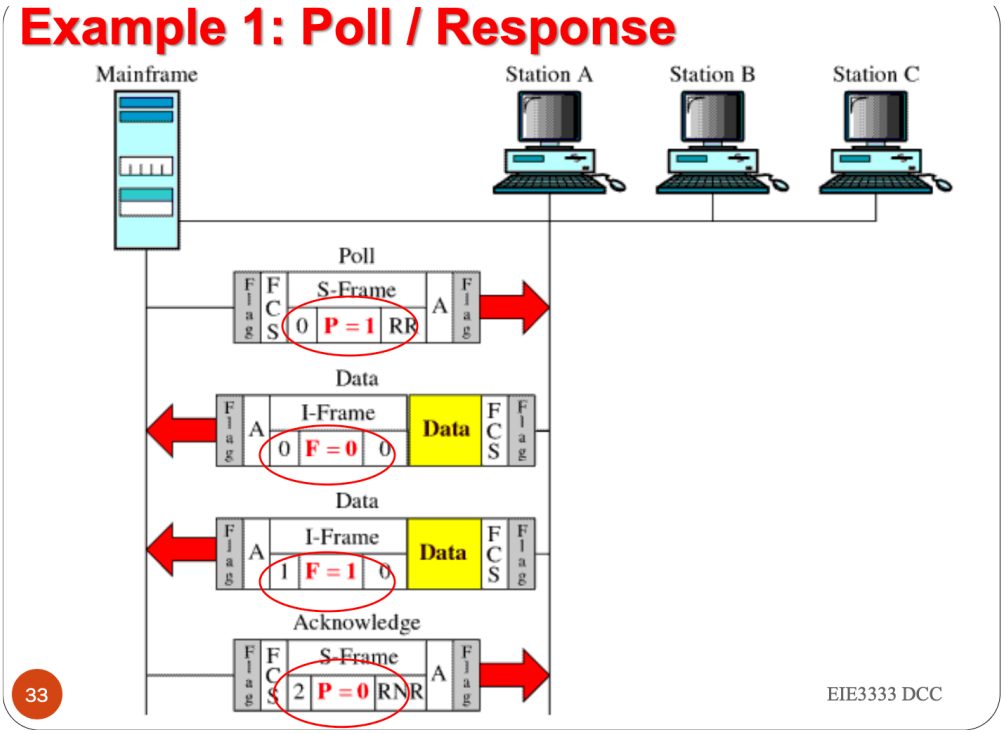


HDLC Operation

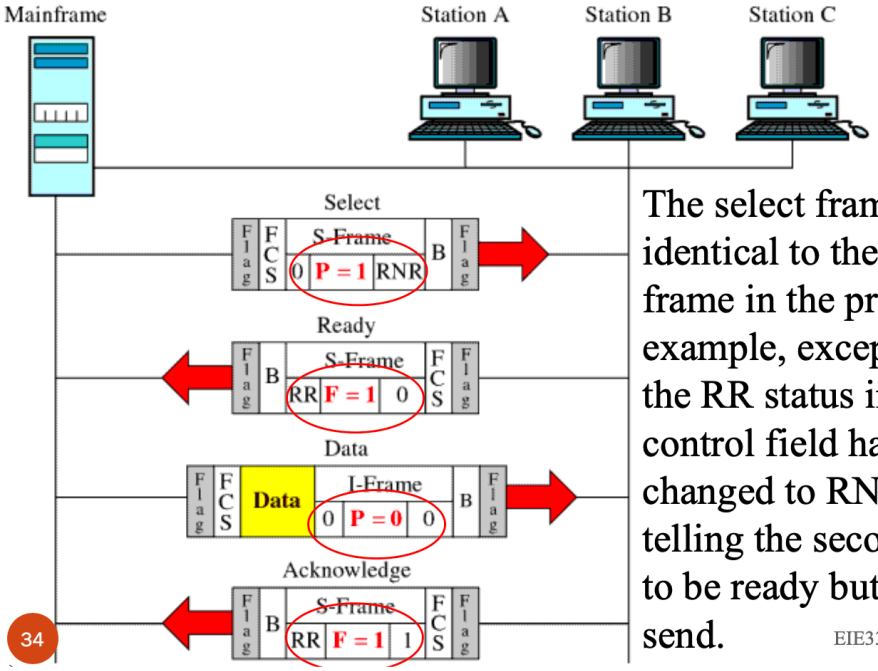
- consists of exchange of information, supervisory and unnumbered frames
- three phases

- Initialization
  - by either side, set mode & sequence number
- Data transfer
  - with flow and error control
  - using both I & S-frame (RR, RNR ...)
- Disconnect
  - when ready or fault noted; a disconnect (DISC) frame will be sent

HDLC Operation Example



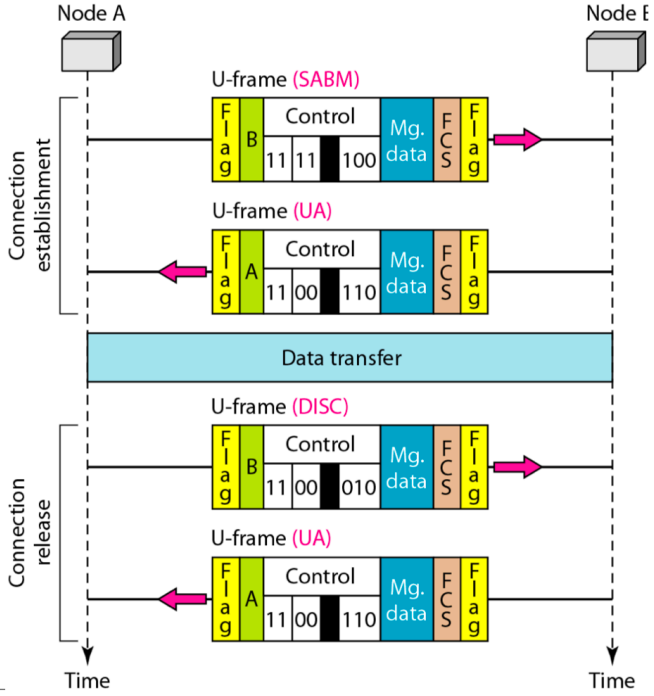
Example 2: Select / Response



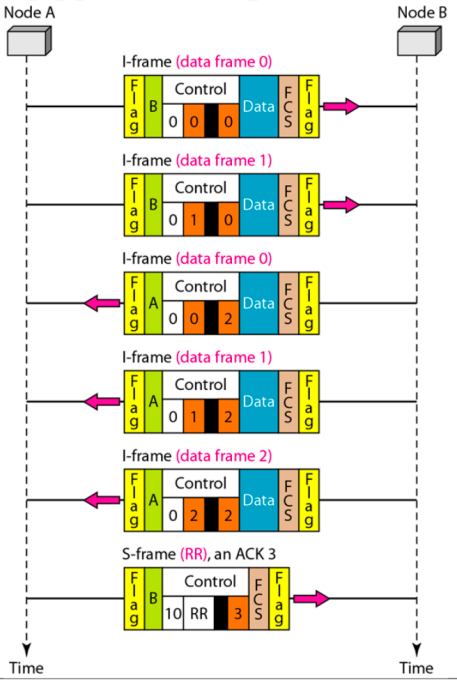
The select frame is identical to the poll frame in the previous example, except that the RR status in the control field has been changed to RNR, telling the secondary to be ready but not to send.

Example 3: Connection & Disconnection

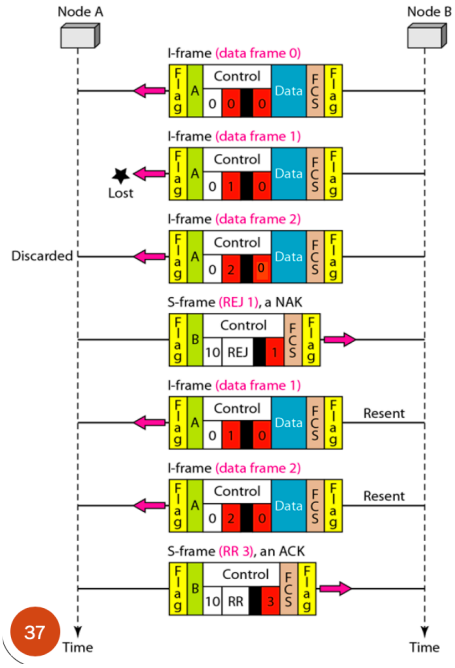
Node A asks for a connection with a set asynchronous balanced mode (SABM) frame; node B gives a positive response with an unnumbered acknowledgment (UA) frame. After these two exchanges, data can be transferred between the two nodes. After data transfer, node A sends a DISC (disconnect) frame to release the connection; it is confirmed by node B responding with a VA (unnumbered acknowledgment).



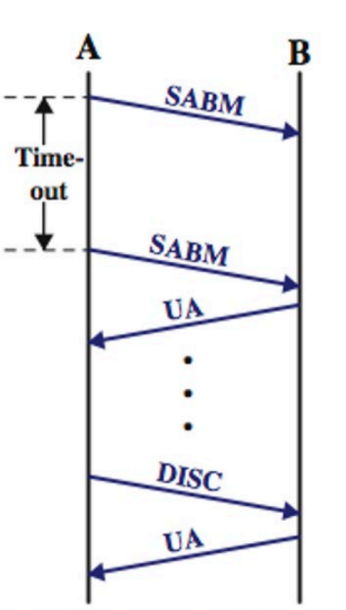
Example 4: Piggybacking



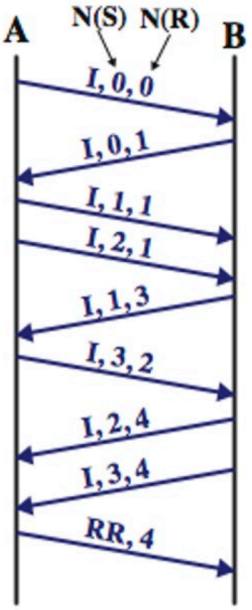
Example 5: Piggybacking with Error



- Node B sends three data frames (0, 1, and 2), but frame 1 is lost.
- When node A receives frame 2, it discards it and sends a REJ frame for frame 1.
- Note that the protocol being used is Go-Back-N with the special use of an REJ frame as a NAK frame.
- The NAK frame does two things here: It confirms the receipt of frame 0 and declares that frame 1 and any following frames must be resent.
- Node B, after receiving the REJ frame, resends frames 1 and 2.
- Node A acknowledges the receipt by sending an RR frame (ACK) with acknowledgment number 3.

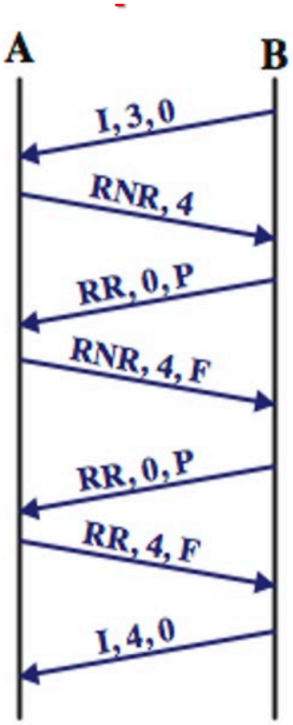


(a) Link setup and disconnect

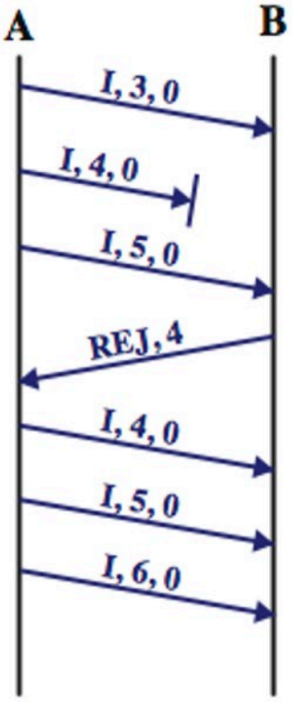


(b) Two-way data exchange

38



(c) Busy condition



(d) Reject recovery

39

Point-to-Point Protocol (PPP)

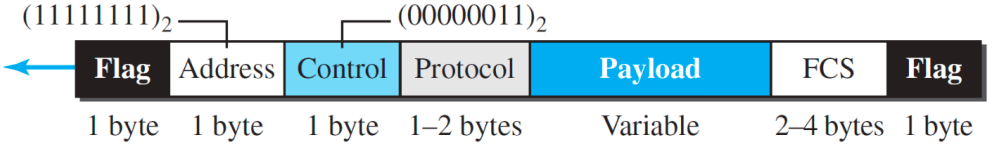
- router-to-router and host-to-network connections over synchronous and Asynchronous circuits, which can be either dialup or leased lines
- home computers to the server of an ISP internet service provider use PPP
- byte-oriented protocol
- HDLC is implemented by Point to point configuration and also multi-point configurations, while PPP is implement by Point to point configuration

PPP Services

- Services provided
  - Establishment of the link and the exchange of data
  - Authentication
  - Provide connections over multiple links (multilink PPP)
- Not provided
  - no flow control
  - no error control (only detection)
  - no sequence numbering

PPP Framing

- PPP uses a character-oriented (or byte-oriented) frame.



Flag: it starts and ends with a specific 1-byte pattern of 01111110

Address: A constant value and set to 11111111 (broadcast address)

Control: Set to a constant value 00000011 (imitating unnumbered frames in HDLC)

Protocol: Define what is being carried in the data field: either user data or other information.

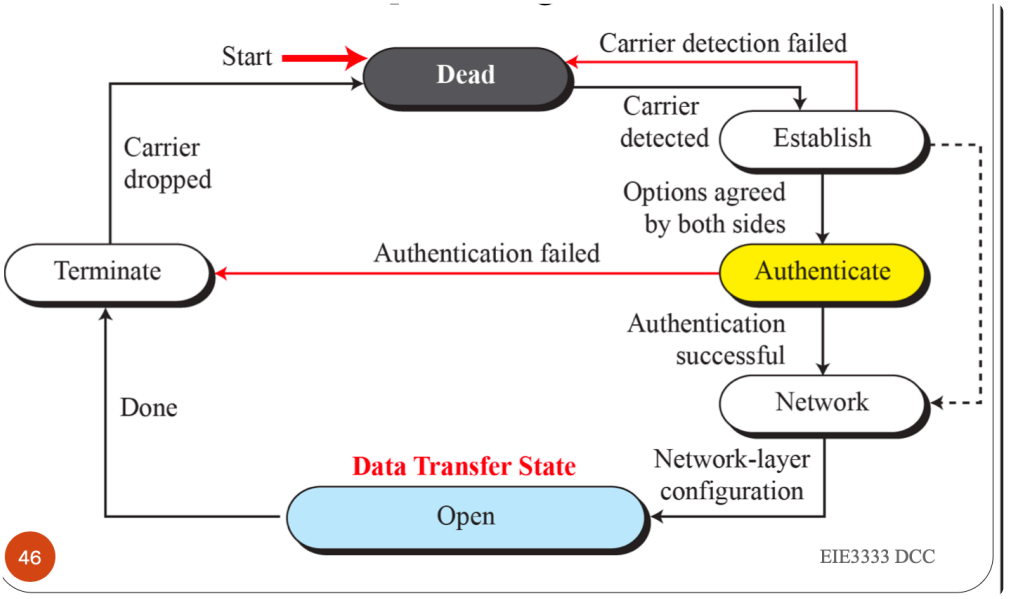
FCS: The frame check sequence is simply a 2-byte or 4-byte CRC.

- **Payload:** The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation.
- Byte Stuffing:

  Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame.

- The escape byte is 01111101. Every time when the flag-like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag. The escape byte that appears in the data should also be stuffed with another escape byte.
- Padding: Since there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or a maximum negotiated value.

PPP Transition Phases



1. Dead（死状态）：
   - 物理层没有信号，链路处于空闲状态。
   - 这里没有活动的载波，意味着通信未建立。
2. Establish（建立状态）：
   - 其中一端发起连接，开始链路建立过程。
   - LCP（Link Control Protocol，链路控制协议用于协商链路参数（如最大帧长度、错误检测、压缩选项等）。
   - The Link Control Protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here.
   - 如果双方同意进行认证，进入 Authenticate（认证状态）；否则进入 Network（网络层协议状态）。
3. Authenticate（认证状态，可选）：

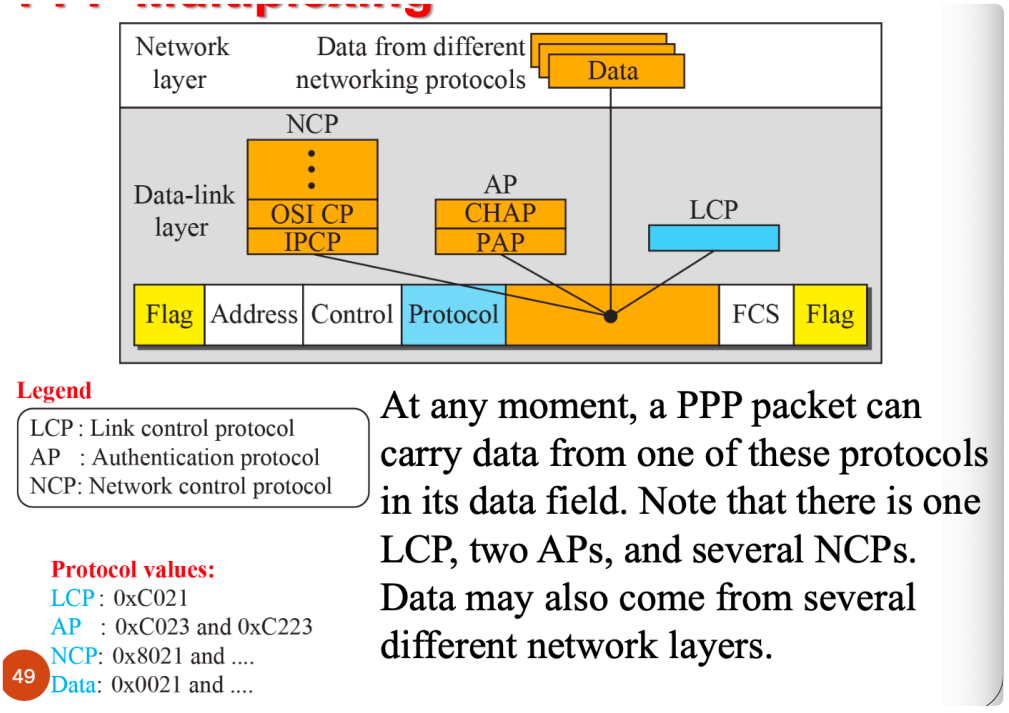
- 如果启用了认证（如 PAP 或 CHAP），则在此阶段进行身份验证。
- 认证通过后，进入 Network（网络层协议状态）

4. Network（网络层协议状态）：
   - 交换 NCP（Network Control Protocol，网络控制协议），用于配置 IP、IPv6 其他网络协议。
   - 这一步完成后，PPP 进入 Open（开放状态），开始数据传输。
5. Open（开放状态）：
   - 数据传输开始，PPP 链路进入正常工作状态。
   - 在该状态下，用户数据被封装到 PPP 帧中并传输。
6. Terminate（终止状态）：
   - 任何一方决定断开连接时，发送 **LCP-Terminate** 请求。
   - 收到 **LCP-Terminate** 确认后，物理层载波信号断开，链路回到 Dead（死状态）。

PPP Multiplexing

PPP 关键协议

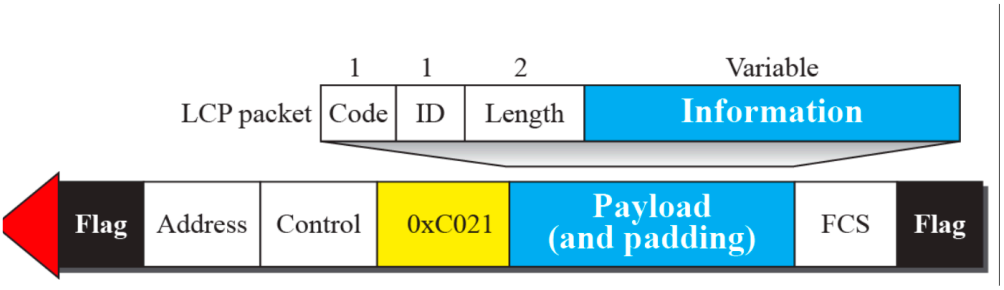
- **LCP（链路控制协议）** → 负责链路建立、配置和维护。
- **NCP（网络控制协议）** → 负责网络层协议的协商，如 IP、IPv6、IPX 等。
- **Two Authentication Protocols (APs)**
  - PAP（Password Authentication Protocol）/ CHAP（Challenge Handshake Authentication Protocol)→ 认证协议，确保安全性。



> **Note**
>
> ✅ **LCP 是 PPP 的一个控制协议**，它的控制信息被封装在 **PPP 帧的"信息字段"** 里，而该字段的数据单元称为 **LCP 数据包（LCP Packet）**。
>
> ✅ **PPP 仍然是帧交换协议**，但其 **帧的载荷部分可以携带 LCP "包"**，因此 LCP 的数据单位被称为 “包” 而不是 “帧”。

Link Control Protocol

- Responsible for ==establishing, maintaining, configuring, and terminating ==links
- It also provides negotiation mechanisms to set options between the two end points



LCP Packets

The code field defines 11 types of LCP packets (three categories: 1-4 for link configuration, 5-6 for link termination, and 7-11 for link monitoring and debugging):

Code	Packet Type	Description
0x01	Configure-request	Contains the list of proposed options and their values
0x02	Configure-ack	Accepts all options proposed
0x03	Configure-nak	Announces that some options are not acceptable
0x04	Configure-reject	Announces that some options are not recognized
0x05	Terminate-request	Request to shut down the line
0x06	Terminate-ack	Accept the shutdown request
0x07	Code-reject	Announces an unknown code
0x08	Protocol-reject	Announces an unknown protocol
0x09	Echo-request	A type of hello message to check if the other end is alive
0x0A	Echo-reply	The response to the echo-request message
0x0B	Discard-request	A request to discard the packet

- the ID field holds a value that matches a request with a reply
  - One endpoint inserts a value in this field, which will be copied into the reply packet.
- The length field defines the length of the entire packet
- the information field contains information, such as options, needed for some LCP packets

	字段	作用
1	**Code**	指定 LCP 包的类型（如请求、应答、终止等）
2	**ID**	**用于匹配请求和应答**，发送方填充一个值，接收方在回复时复制该值
3	**Length**	**整个 LCP 包的长度**（包括所有字段）
4	**Information（可选）**	**具体的配置信息**，某些 LCP 包需要填充

假设 A 发送 LCP 配置请求给 B，希望设置 最大接收单元(MRU)为 1500 字节，LCP 包可能如下：

```
| Code: Configure-Request (0x01) |
| ID: 0x05                       |
| Length: 8                      |
| Information: MRU=1500 (0x01 0x04 0x05DC) |
```

B 收到后，如果同意该配置，就会返回：

```
| Code: Configure-Ack (0x02) |
| ID: 0x05                   |  <-- **ID 保持一致**
| Length: 8                  |
| Information: MRU=1500      |
```

这样 A 才知道 B 认可了 MRU=1500 的配置，连接才能继续。

Options

- There are many options that can be negotiated between two end points

- inserted in the information field of the configuration packets. In this case, the information field is divided into three fields : option type, option length, and option data
- most common options

Option	*Default*
Maximum receive unit (payload field size)	1500
Authentication protocol	None
Protocol field compression	Off
Address and control field compression	Off

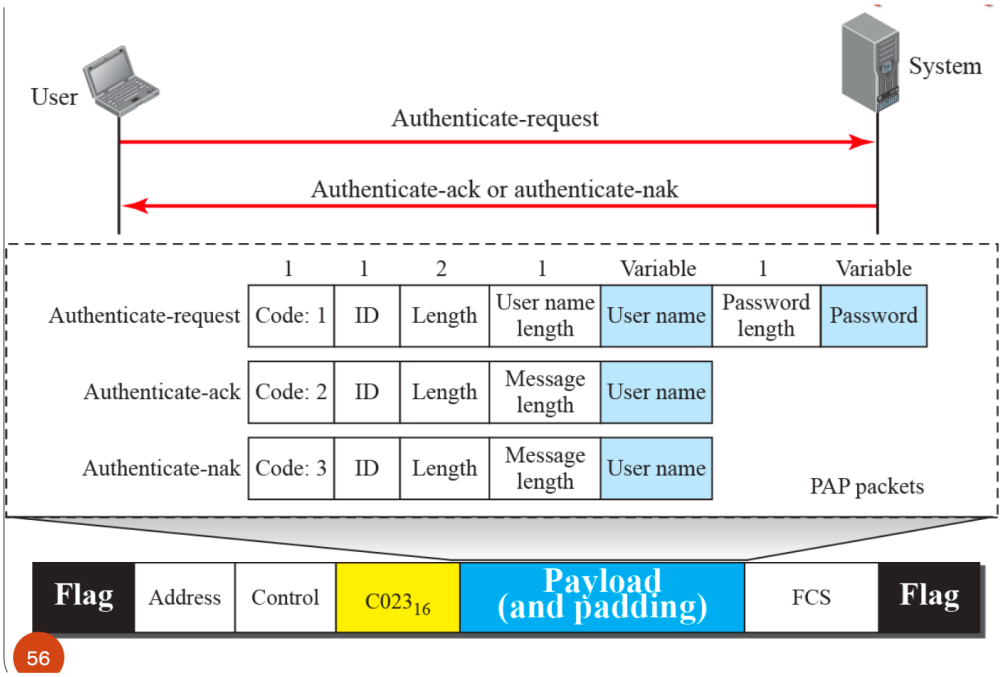
1. **0x01（Type = 1）**
   - 在 LCP 协议中，`0x01` 代表 **MRU（Maximum Receive Unit）**，即 **最大接收单元**，用于协商数据帧的最大长度。
2. **0x04（Length = 4）**
   - 说明这个选项字段的总长度是 `4` 字节，包括：
     - **Type（1字节）**
     - **Length（1字节）**
     - **Value（2字节）**
3. **0x05DC（Value = 1500）**
   - **MRU 的实际值，0x05DC 是十六进制，转换成十进制就是 `1500`**，表示最大接收单元为 1500 字节。

Authentication Protocols

- for use over dial-up links where verification of user identity is necessary
- Authentication means validating the identity of a user who needs to access a set of resources
- two protocols
  - Password Authentication Protocol
  - Challenge Handshake Authentication Protocol

PAP

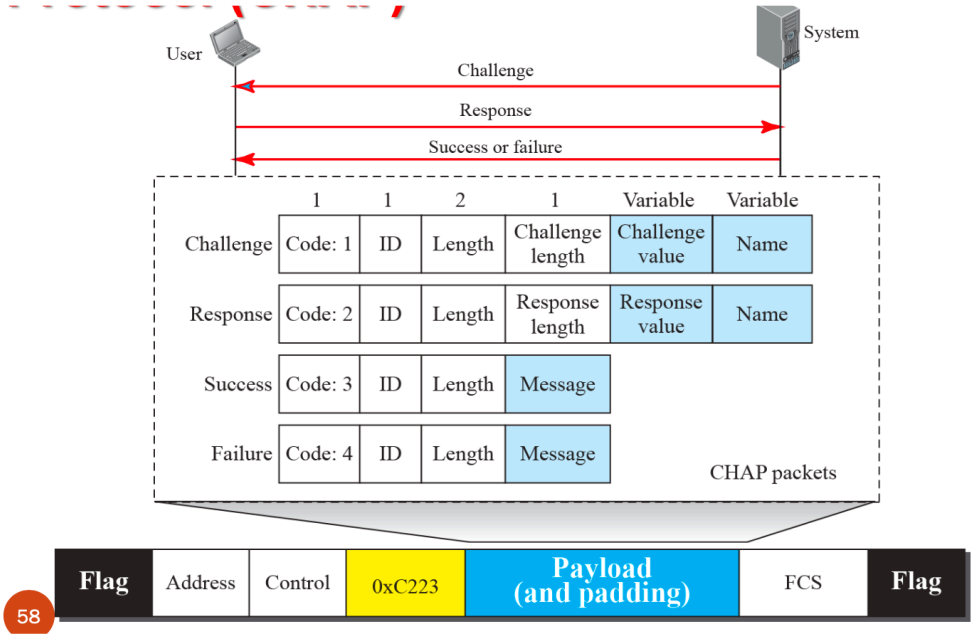
- user who wants to access a system sends an authentication identification (usually the user name) and a password
- the system check the validity of the identification and password the either accepts or denies connections



Challenge Handshake Authentication Protocol

- a three-way handshaking authentication protocol that provides greater than PAP.
- in CHAP, the password is kept secret; it is never sent online

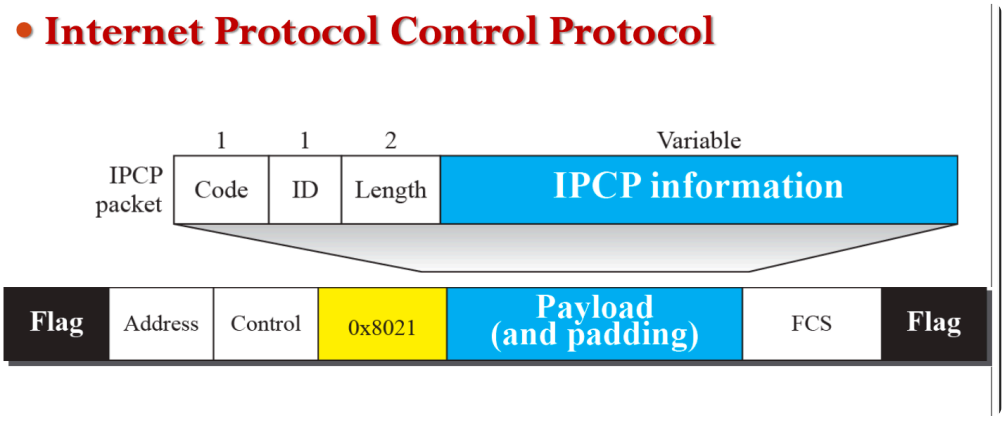
1. 挑战 (Challenge)
   - 服务器向客户端发送一个随机的挑战值（challenge value），通常是几个字节的随机数。
2. 响应（Response）
   - 客户端收到挑战值后，使用一个 哈希函数 (通常是 MD5) ==a predefined function ==计算：`response = Hash(challenge value + 用户密码)`
   - 然后客户端将计算结果（哈希值）发送给服务器。
3. 验证（Verification）
   - 服务器收到客户端的 **response** 后，使用同样的哈希函数计算：`expected_response = Hash(challenge value + 服务器存储的密码)`
   - 如果 `response == expected_response`，认证成功；否则，认证失败，拒绝访问



Network Control Protocols

- PPP has defined a specific Network Control Protocol for each network protocol.
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Control Protocol
  - Xerox NS IDP Control Protocol
- None of the NCP packets carry network layer data; they just configure the link at the network layer for the incoming data.
- NCP 主要用于协商和配置网络层参数，比如 IP 地址、路由信息等。
- 真正的网络层数据包（IP 数据等）不会通过 NCP 传输，而是通过 PPP 进行承载。

IPCP Packets

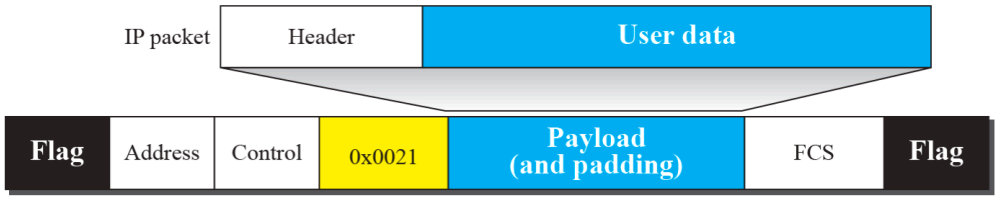


IPCP defines seven packets, distinguished by their code values:

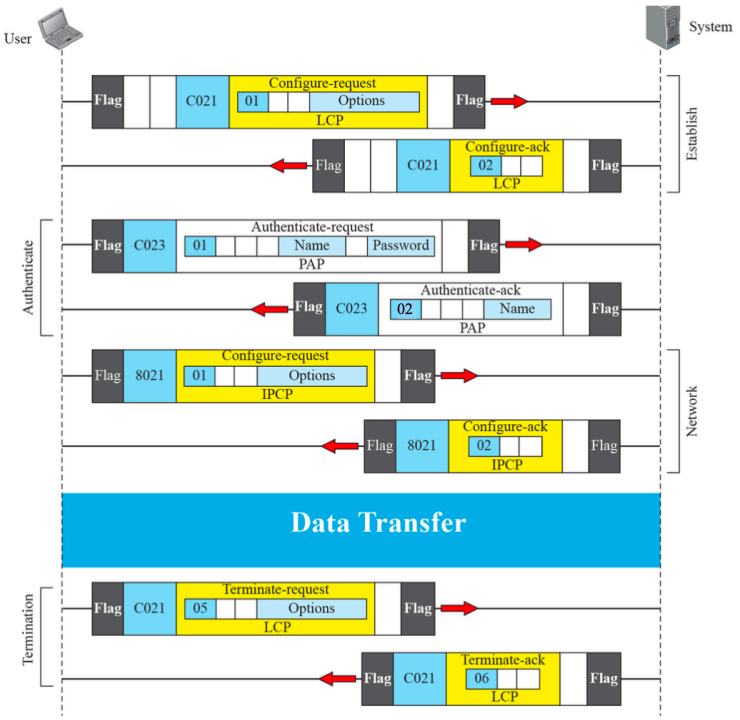
Code	*IPCP Packet*
0x01	Configure-request
0x02	Configure-ack
0x03	Configure-nak
0x04	Configure-reject
0x05	Terminate-request
0x06	Terminate-ack
0x07	Code-reject

Data from Network layer

- After the network-layer configuration is completed by one of the NCP protocols, the user can exchange data packets from the network layer.
- IP datagram encapsulated in a PPP frame:



An Example


User
System
Flag
C021
Configure-request
01
Options
LCP
Flag
Flag
C021
Configure-ack
02
LCP
Flag
Establish
Authenticate
Flag
C023
Authenticate-request
01
Name
Password
PAP
Flag
Flag
C023
Authenticate-ack
02
Name
PAP
Flag
Flag
8021
Configure-request
01
Options
IPCP
Flag
Flag
8021
Configure-ack
02
IPCP
Flag
Network
Data Transfer
Termination
Flag
C021
Terminate-request
05
Options
LCP
Flag
Flag
C021
Terminate-ack
06
LCP
Flag