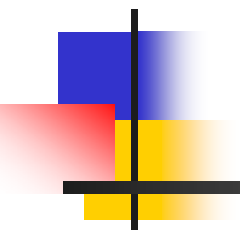
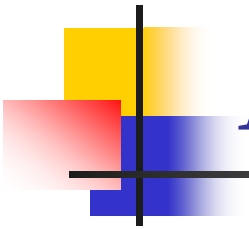


# Introduction to PPP: Point-to-Point Protocol

Hao-Ran Liu

2002/9/13

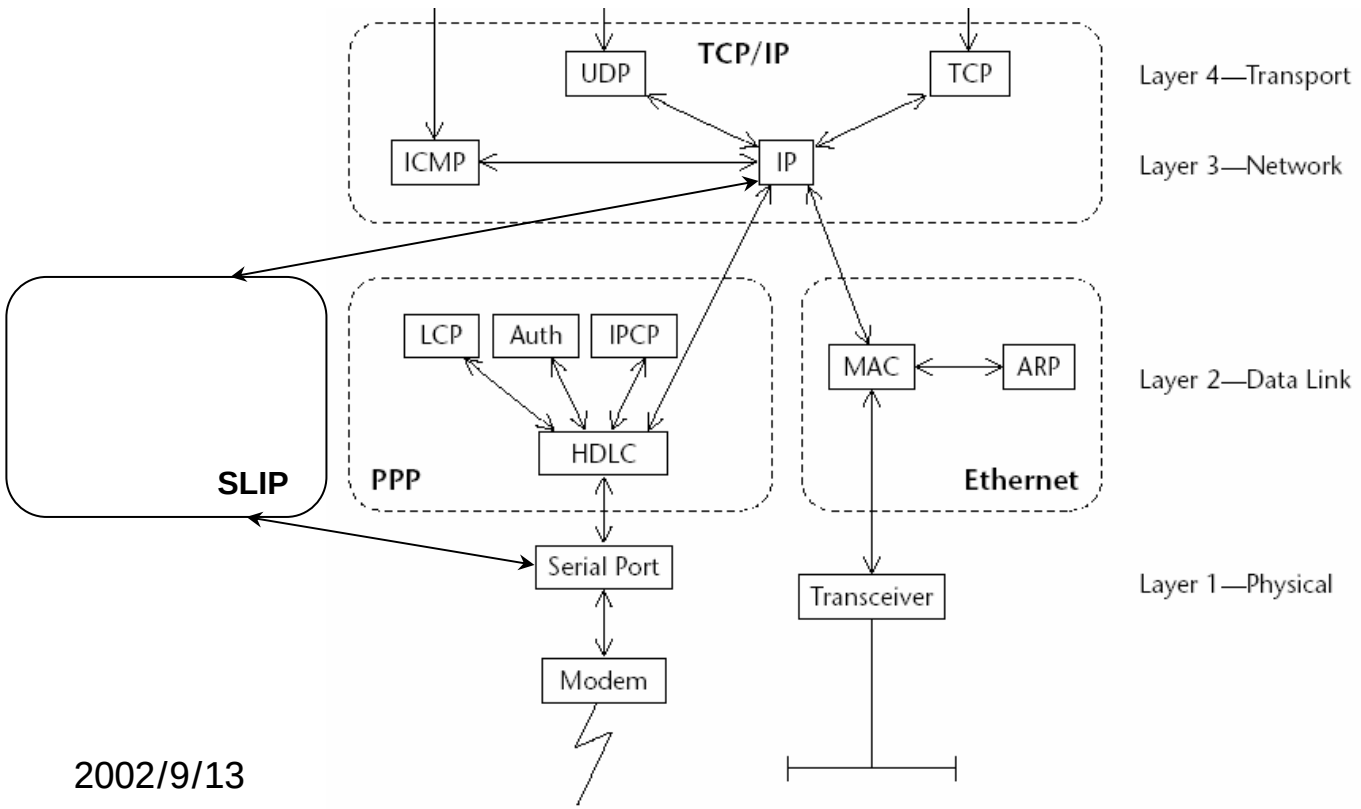


# Agenda

- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

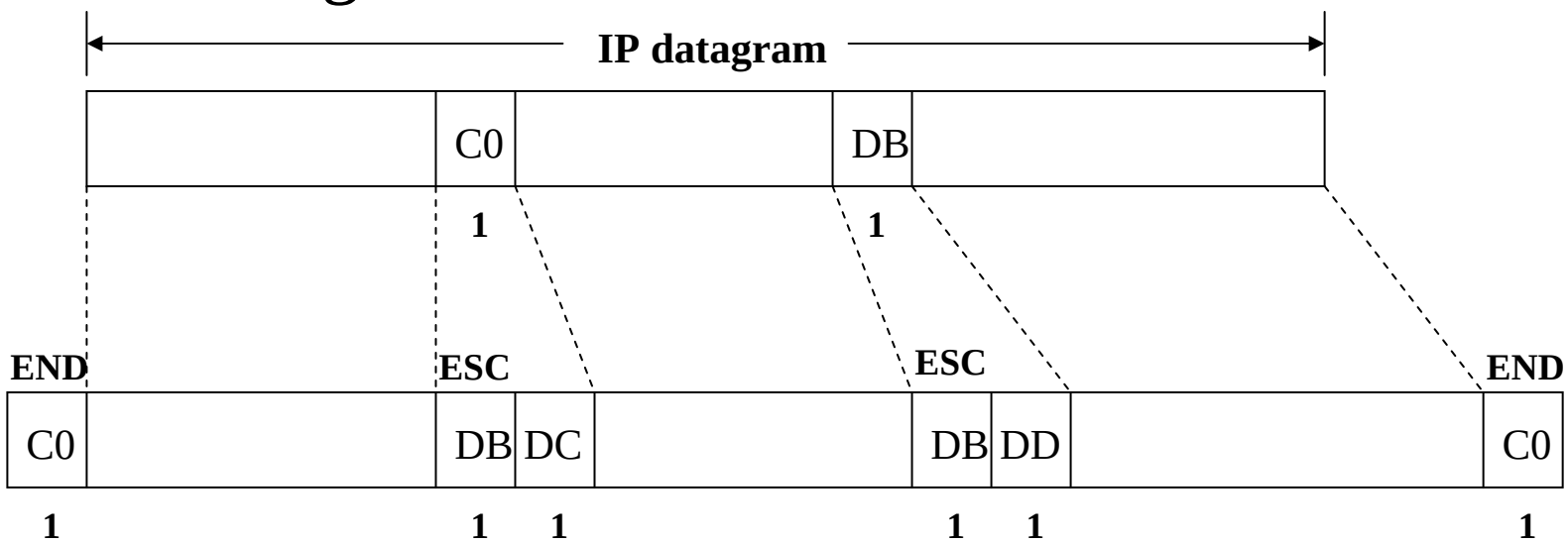
# PPP Overview

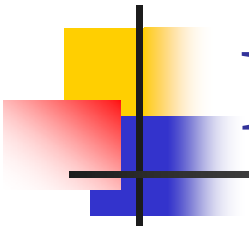
- PPP and SLIP are two commonly used protocols for point-to-point serial link.



# SLIP Frame Format

- SLIP: Serial Line IP
- A simple form of encapsulation for IP datagrams

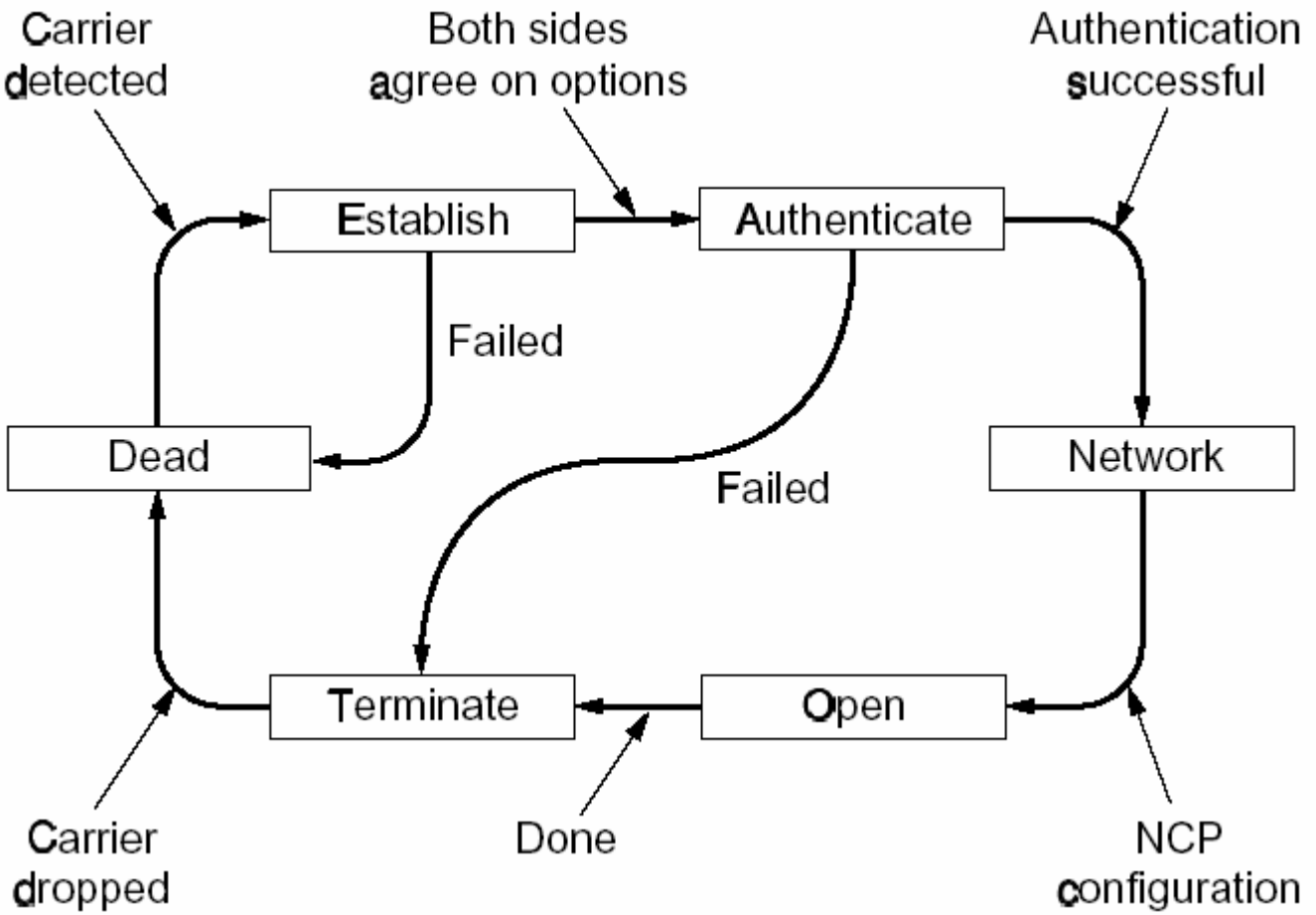




# PPP Definition

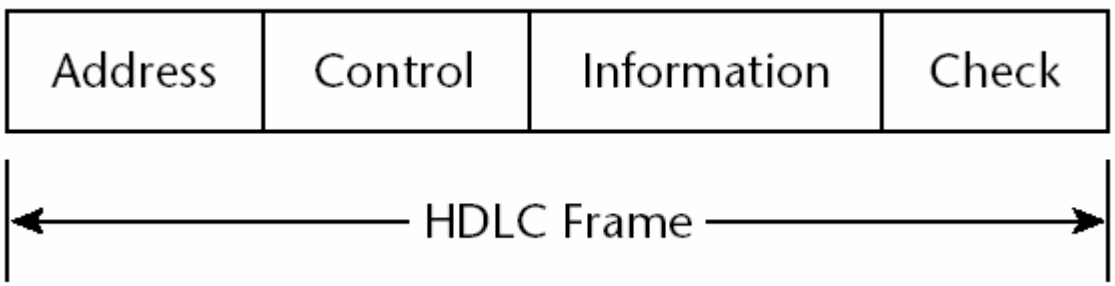
- RFC 1661
  - A method for transporting multi-protocol datagrams over point-to-point links
  - Three main components
    - A method for encapsulating multi-protocol datagrams.
    - A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
    - A family of Network Control Protocols (NCP) for establishing and configuring different network-layer protocols.

# PPP Link Phase Diagram



# PPP Framing

- PPP is built on top of HDLC protocol




- Address and control field are fixed
  - Address = FF (all stations)
  - Control = 03 (unnumbered information)

# PPP Frame Format

- PPP HDLC Framing

| flag 7E | addr FF | control 03 | protocol | information | CRC | flag 7E |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | up to 1500 bytes | 2 | 1 |

- Example

| Protocol 0021 | IP datagram |
|---|---|

| Protocol C021 | link control data |
|---|---|

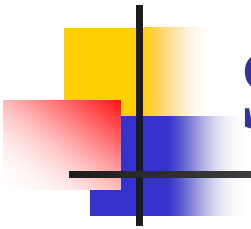
| Protocol 0021 | network control data |
|---|---|

# PPP Protocol Number Assignment

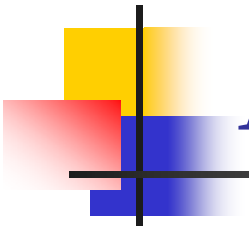
| | |
|---|---|
| 0*** -- 3*** | Network layer protocol |
| 8*** -- b*** | Network control protocol |
| c*** -- f*** | Link layer control protocol |

| | | |
|---|---|---|
| 0021 IPv4 | 8021 IPCP | C021 Link Control Protocol |
| 002B IPX | 802B IPXCP | C023 PAP |
| 002D VJ Compressed TCP/IP | | C025 Link Quality Report |
| 003D Multilink PPP (MP) | | C223 CHAP |
| 0053 Encryption | 8053 Encryption CP | |
| 00FD Compression | 80FD Compression CP | |

# The advantage of PPP over SLIP



- Support multiple network layer protocols.
- A CRC checksum on every frame.
- Includes authentication protocol
- Dynamic negotiation of IP address
- Data-link options can be negotiated via a link control protocol.

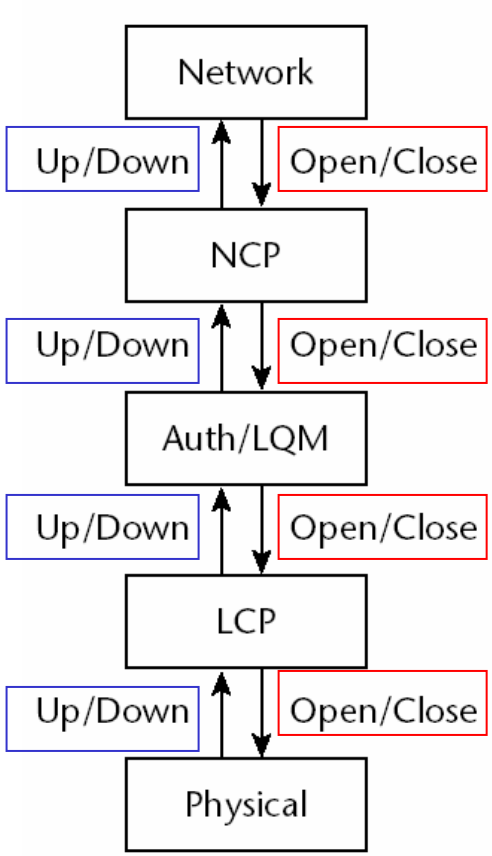


# Agenda

- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

# PPP phases as layers

- PPP link phases are run sequentially.

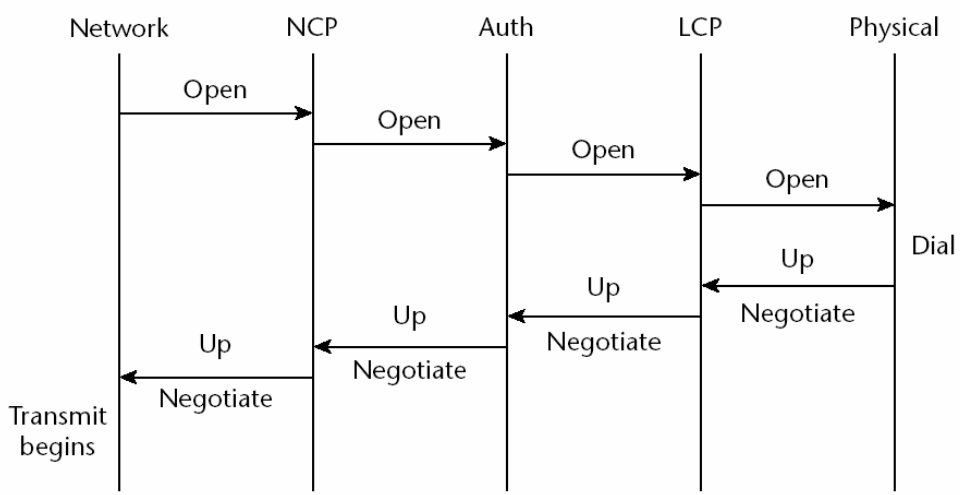



Command

Event

# Bring a layer "Up"

- Bring a layer up requires:
  - An Open request from a higher layer
  - An Up event from the next lower layer
  - The successful negotiation of parameters at that particular layer.



# Negotiation Message Types

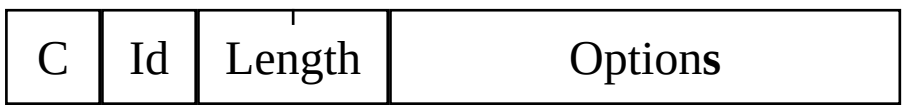
| Name | Direction | Description |
|---|---|---|
| Configure-Request | I >> R | List of proposed options and values |
| Configure-Ack | I << R | All options are accepted |
| Configure-Nak | I << R | Some options are not accepted |
| Configure-Reject | I << R | Some options are not negotiable |
| Terminate-Request | I >> R | Request to shut the line down |
| Terminate-Ack | I << R | OK, line shut down |
| Code-Reject | I << R | Unknown request received |
| Protocol-Reject | I << R | Unknown protocol requested |
| Echo-Request | I >> R | Please send this frame back |
| Echo-Reply | I << R | Here is the frame back |
| Discard-Request | I >> R | Just discard this frame (for testing) |

# Negotiation Message Format


PPP Frame

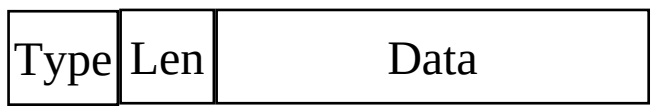
```
Flag     : 7E
Address  : FF   (All-stations address)
Control  : 03   (Unnumbered Information)
Protocol : C021 (LCP)
           C023 (PAP)
           8021 (IPCP)
```

## Negotiation Message




```
Code   = 1 (Configure-Request)  7 (Code-Reject)
         2 (Configure-Ack)      8 (Protocol-Reject)
         3 (Configure-Nak)      9 (Echo-Request)
         4 (Configure-Reject)  10 (Echo-Reply)
         5 (Terminate-Request) 11 (Discard-Request)
         6 (Terminate-Ack)
Id     = identify a pair of configure-req/ack
Length = length of the whole negotiation message
```

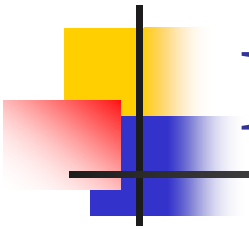
## Option Encoding




- Type and Len are a single octet
- Len field is the length of the whole option block
- Data field is information for the option being negotiated

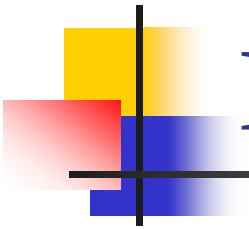
# Negotiation Message in Different Control Protocols

- The packet format described above is used on all PPP control protocols (LCP, NCP, PAP, CHAP, ECP, CCP, etc.)
- The only difference in the packet of these control protocols
  - Protocol field
  - Code field (range of code number used)
  - Options for specific control protocol.



# Example Negotiations

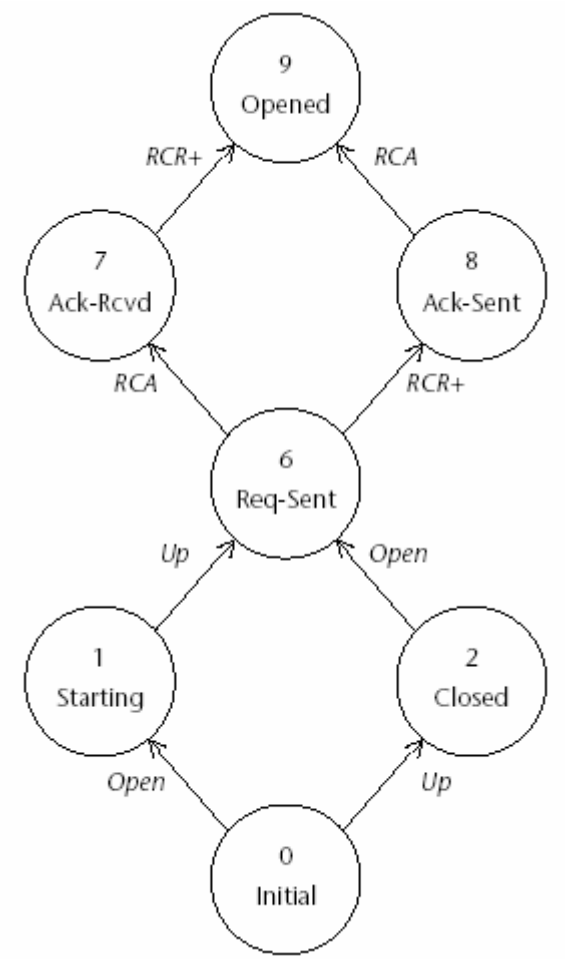
```
1. A: Configure-Request    ID:1 [ 1 4:01010101 5:80 9 ]
2. B: Configure-Reject     ID:1 [ 1 5:80 ]
3. A: Configure-Request    ID:2 [ 4:01010101 9 ]
4. B: Configure-Nak        ID:2 [ 4:01010102 ]
5. A: Configure-Request    ID:3 [ 4:01010102 9 ]
6. B: Configure-Ack        ID:3 [ 4:01010102 9 ]
7. B: Configure-Request    ID:1 [ 2 9 ]
8. A: Configure-Ack        ID:1 [ 2 9 ]
```



# Example Frame

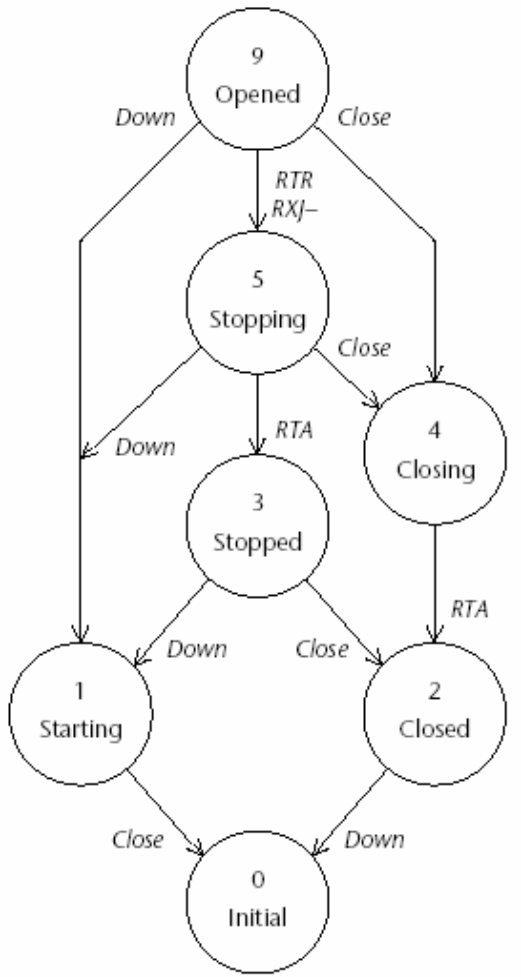
```
FF 03          - Standard PPP HDLC address and control fields
C0 21          - Protocol number C021 (LCP)
01             - Code field; 01 is Configure-Request
01             - ID field (number 1)
00 0E          - Length field (14 octets)
02             - Type field; option 02 for protocol C021
06             - Len field (6 octets)
00 00 00 00    - Data for this option
07             - Type field; option 07 for protocol C021
02             - Len field (2 octets)
08             - Type field; option 08 for protocol C021
02             - Len field (2 octets)
70 34          - CRC
```

# Negotiation State Machine – Simplified layer establishment

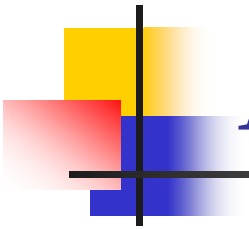



```
Up   = lower layer is Up
Open = administrative Open
RCR+ = Receive-Configure-Request (Good)
RCA  = Receive-Configure-Ack
```

# Negotiation State Machine – Simplified layer tear-down

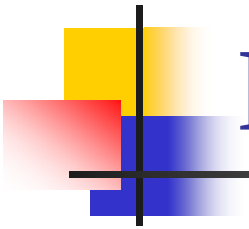



```
Down = lower layer is Down
Close= administrative Close
RTR  = Receive-Terminate-Request
RTA  = Receive-Terminate-Ack
RXJ- = Receive-Code-Reject (catastrophic)
```



# Agenda

- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

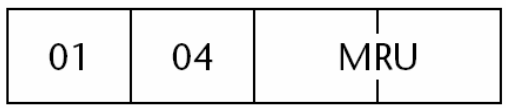


# Link Control Protocol

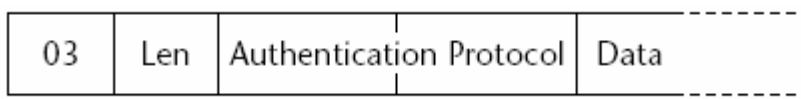
- Negotiation of modification to the default characteristics of a point-to-point link.
  - A default value is specified for each option.
  - No need to send the default value for a option in a Configure-Request.

# LCP Configuration Options

- Maximum Receive Unit (MRU)
  - RFC 1661
    - At least 1500 octets.
  - RFC 2516
    - must NOT larger than 1492 octets for PPPoE.

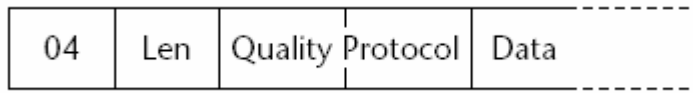



- Authentication Protocol
  - PAP: c023
  - CHAP: c22305
  - MS-CHAPv2: c22381

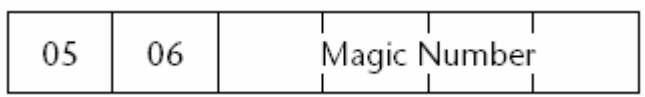


# LCP Configuration Options

- Quality Protocol




  - Link-Quality-Report
    - RFC 1989
    - Value assigned in PPP: c025
- Magic Number
  - A random number chosen to distinguish loopback or error conditions.



# LCP Configuration Options

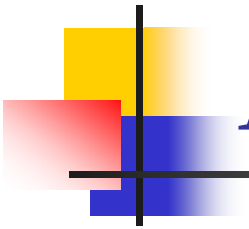
- Protocol Field Compression (PFC)

| 07 | 02 |
|---|---|

  - Reduce PPP protocol field from 2 octets to 1 octet by omit MSB when MSB is zero.
- Address & Control Field Compress (ACFC)

| 08 | 02 |
|---|---|

  - Sender of the option wants to receive PPP frame without HDLC address and control fields (normally set to FF 03)

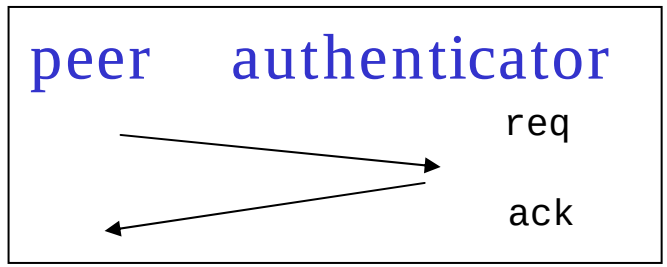


# Agenda

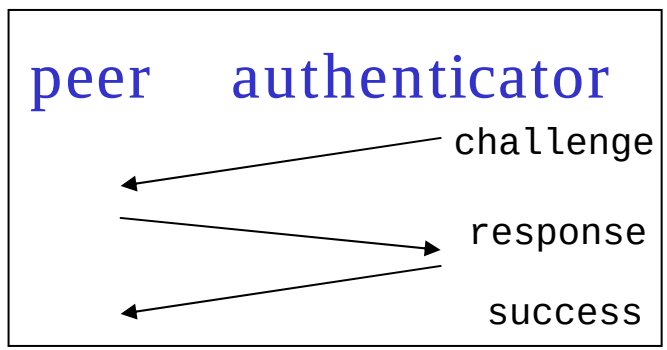
- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

# Authentication Protocol

- Authentication protocol is specified at Link Establish stage (LCP)
- PAP
  - RFC 1334
  - 2 way handshake.
  - Plaintext password over the wire.

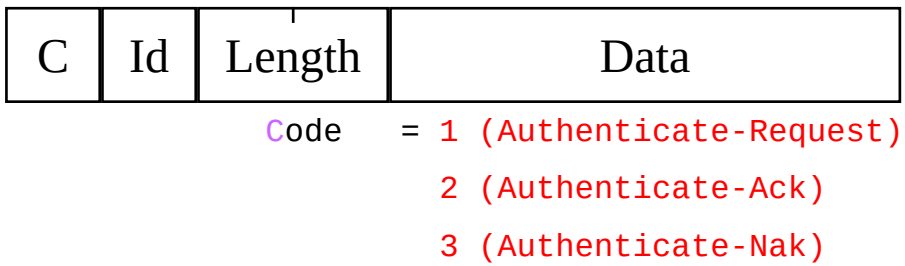



- CHAP
  - RFC 1994
  - 3 way handshake
  - Password is encrypted.



# PAP – PPP Authentication Protocol

PAP Negotiation Message

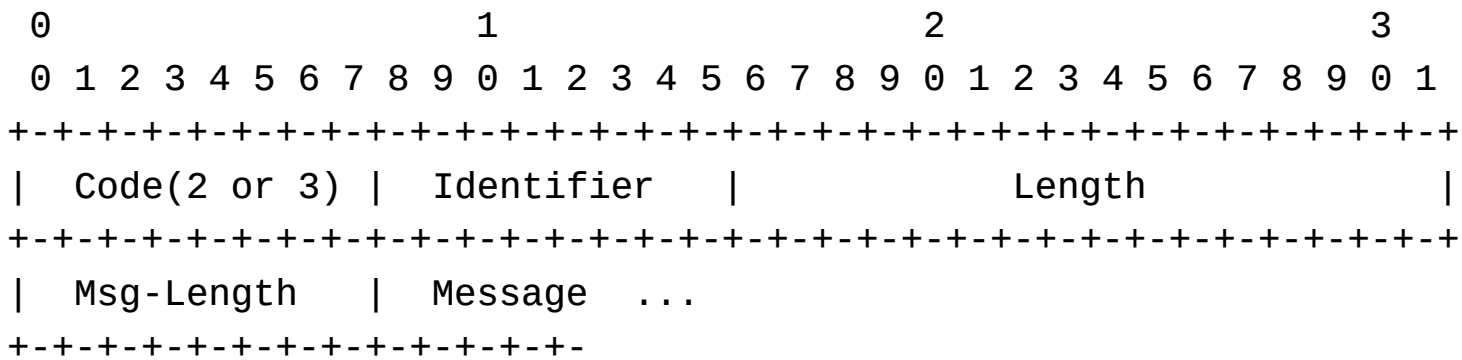



- Authenticate-Request

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code (1)  |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Peer-ID Length|  Peer-Id ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Passwd-Length |  Password  ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

# PAP – PPP Authentication Protocol

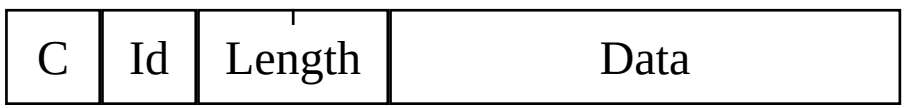
- Authenticate-Ack & Authenticate-Nak
  - Message can be any ASCII text



# CHAP – Challenge-Handshake Authentication Protocol

- Periodically verify peer's identity using a 3- way handshake.

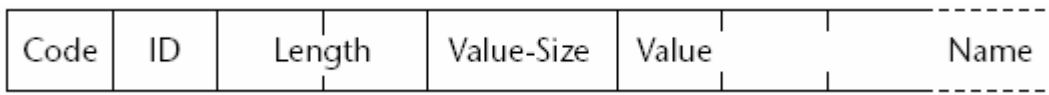
CHAP Negotiation Message



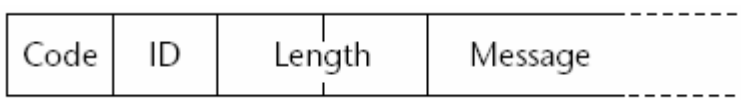

Code = 1 (Challenge)
2 (Response)
3 (Success)
4 (Failure)

# CHAP – Challenge-Handshake Authentication Protocol

- Challenge & Response
  - Challenge value MUST be changed each time a challenge is sent. (security reason)

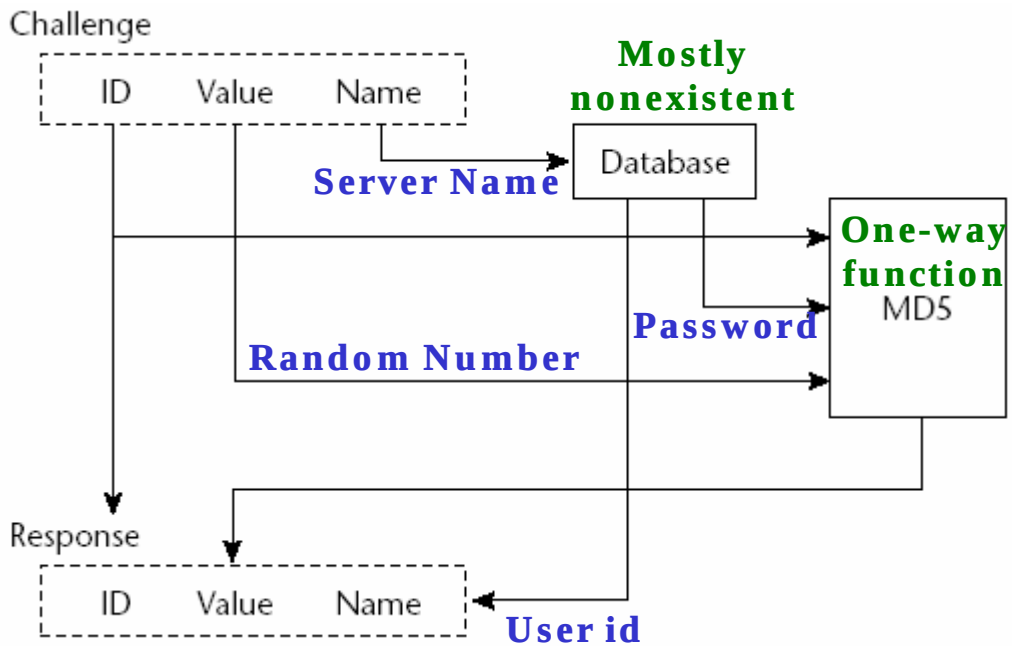



- Success & Failure



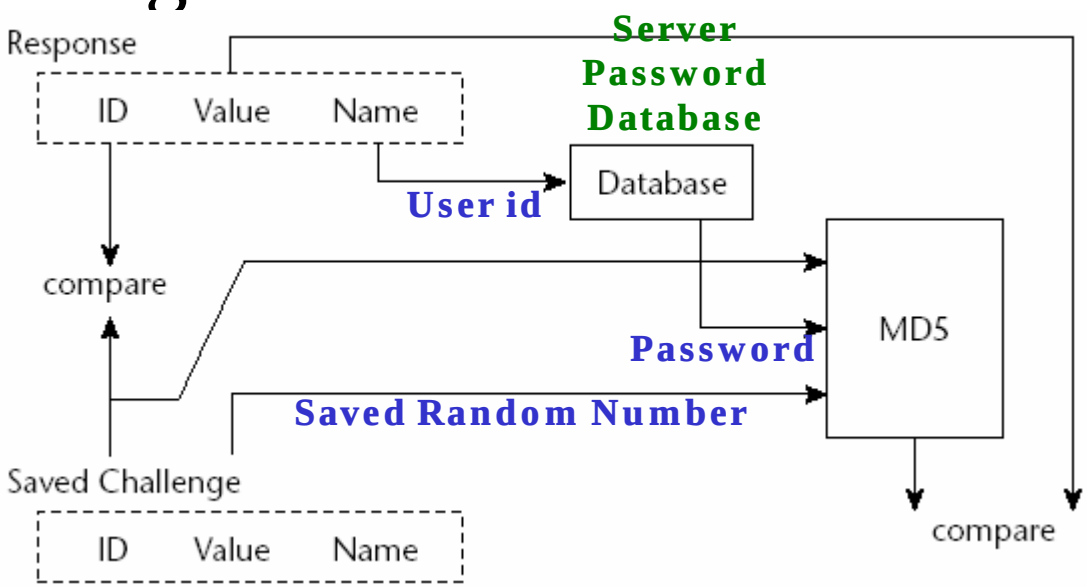
# CHAP – Challenge-Handshake Authentication Protocol

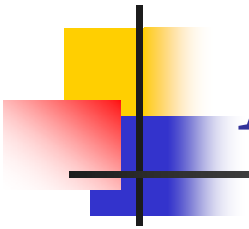
- Responsing a challenge



# CHAP – Challenge-Handshake Authentication Protocol

- Verify a response with saved challenge





# Agenda

- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

# Network Control Protocol

- PPP has a family of network control protocol to establishing and configuring different network-layer protocols.
- ** protocol no. + 8000 = ** CP
  - Ex: 0021 (IP) + 8000 = 8021 (IPCP)

| PPP Protocol Number | Description | RFC |
|---|---|---|
| 8021 | IP Control Protocol | 1332 |
| 8029 | AppleTalk Control Protocol | 1378 |
| 802B | IPX Control Protocol | 1552 |
| 8057 | IPV6 Control Protocol | 2472 |
| 8281 | MPLS Control Protocol | -- |

# IPCP – Internet Protocol Control Protocol

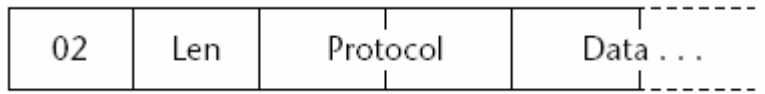
- Local IP address and TCP/IP header compression protocol are negotiated in IPCP.
- Sending IP datagrams
  - Exactly one IP packet is encapsulated in the information field of PPP frame.
  - IP packet size is limited by receiver's MRU.
  - Avoid IP fragmentation
    - TCP MSS option
    - Path MTU discovery

# IPCP Negotiation Message Types

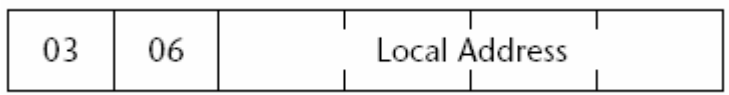
- Only codes 1 – 7 are used
  - Configure-Request
  - Configure-Ack
  - Configure-Nak
  - Configure-Reject
  - Terminate-Request
  - Terminate-Ack
  - Code-Reject

# IPCP Configuration Options

- IP Compression Protocol
  - VJ Compression




    - Can reduce TCP/IP headers from 40 octets to 3 octets.
    - Protocol: 002d
    - RFC 1144
- IP Address




  - Configuring local IP address
  - Local address field:

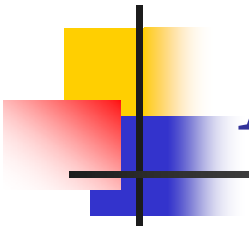
Subnet mask, IP of DNS **should be** assigned via DHCP protocol

    - Can be sender's self assigned address.
    - Can be be all zero (remote address assign)
      - peer use Configure-Nak to assign a address for the sender.

# IPCP Configuration Options

- DNS and NBNS Address
  - Microsoft proposed these options in RFC 1877
  - DNS and NBNS are application level service, they are negotiated at wrong level.
  - These options duplicate services of BOOTP and DHCP.

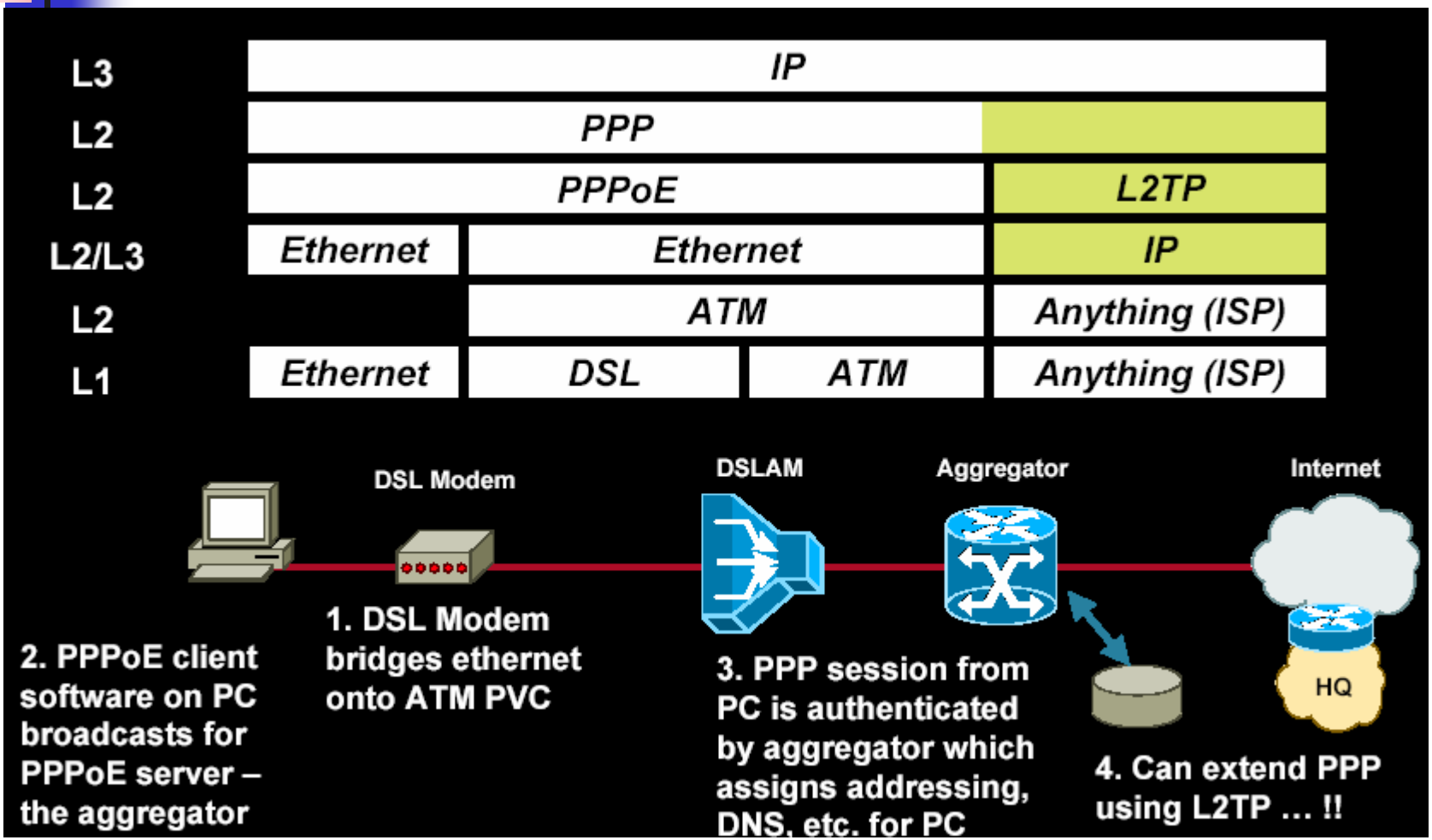
| Option No. | Description |
|---|---|
| 0x81 | Primary DNS Address |
| 0x82 | Primary NBNS Address |
| 0x83 | Secondary DNS Address |
| 0x84 | Secondary NBNS Address |

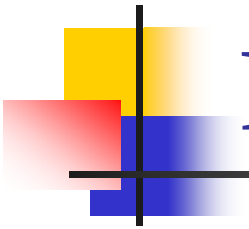


# Agenda

- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

# PPP over Ethernet

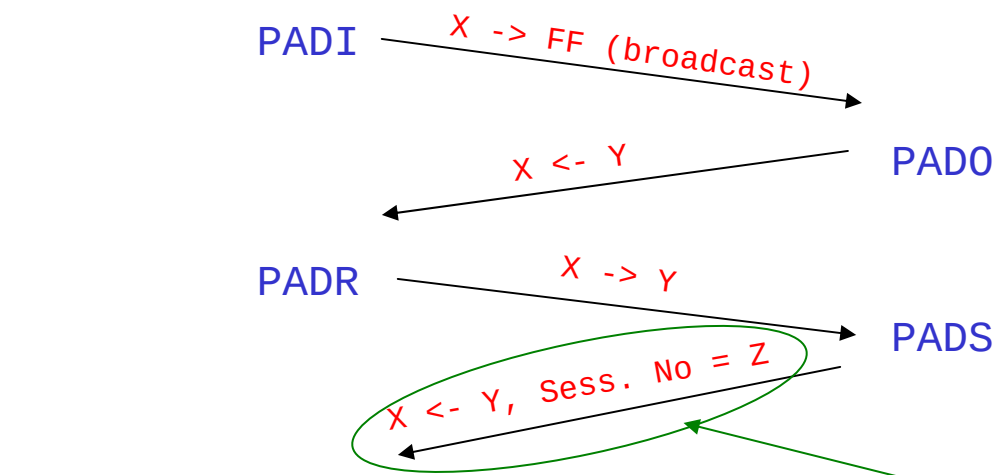




# PPP over Ethernet

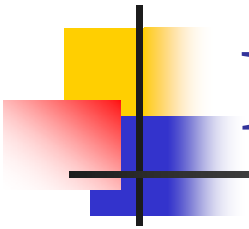
- Provide point-to-point connection over Ethernet
- PPPoE stages
  - Discovery stage
    - Discover the Ethernet address of access concentrator (server)
    - Negotiate a PPPoE session number for session stage
  - Session stage
    - PPP packets are transferred in this stage.

# PPPoE Discovery Stage




| | |
|---|---|
| PADI | PPPoE Active Discovery Initiation |
| PADO | PPPoE Active Discovery Offer |
| PADR | PPPoE Active Discovery Request |
| PADS | PPPoE Active Discovery Session-confirmation |
| PADT | PPPoE Active Discovery Terminate |

The session number, combined with source and destination Ethernet addresses, uniquely identifies a PPPoE session.



# PPPoE Session Stage

- PPP packet are transmitted in PPPoE session stage.
- PPP Ethernet framing
  - No escape bytes are required because frame boundaries are explicit in Ethernet encapsulation.
  - 6 bytes of overhead are added in addition to the Ethernet header.
  - No PPP FCS is required because Ethernet has its own CRC.

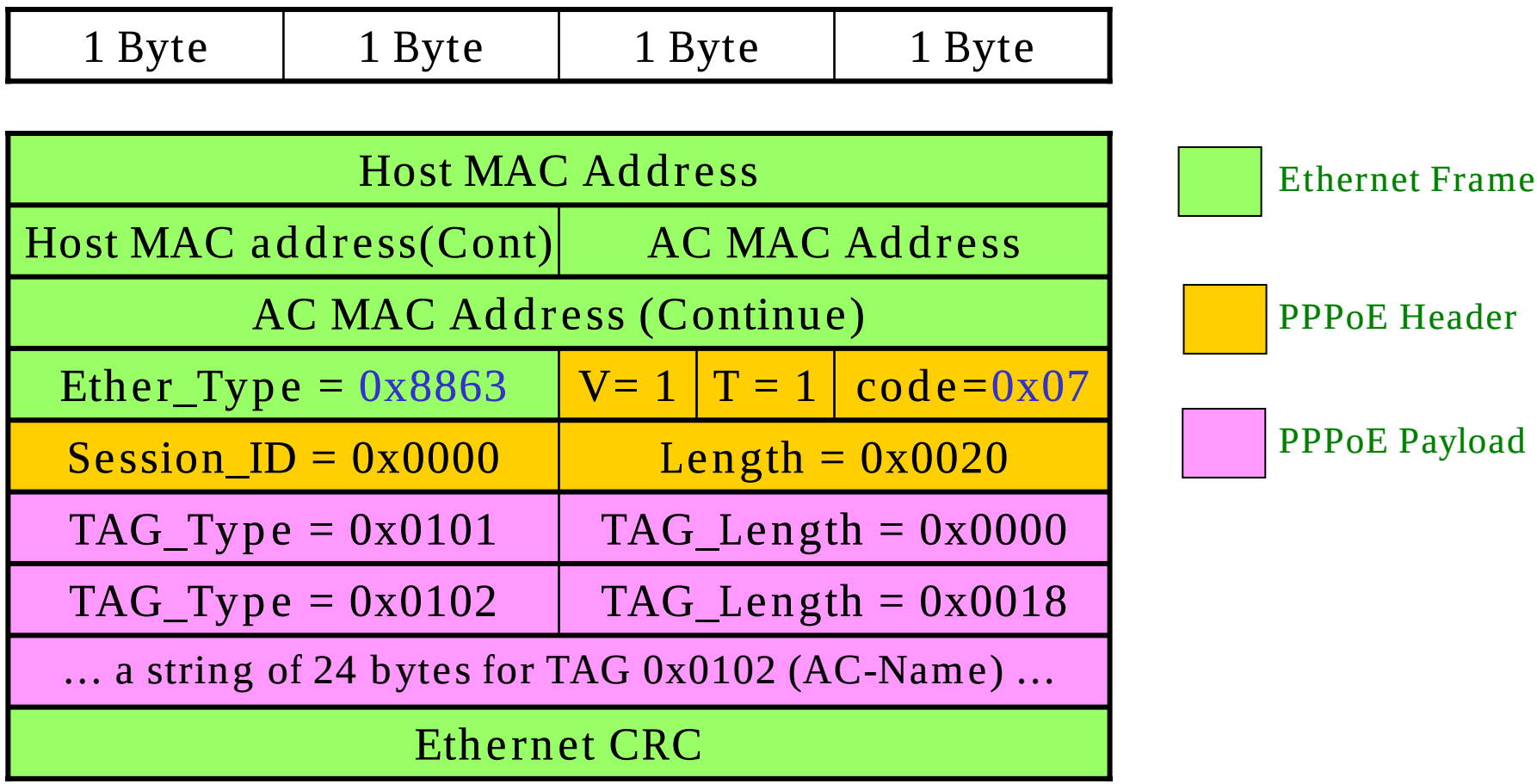
# Example PADI packet

| 1 Byte | 1 Byte | 1 Byte | 1 Byte |
|---|---|---|---|

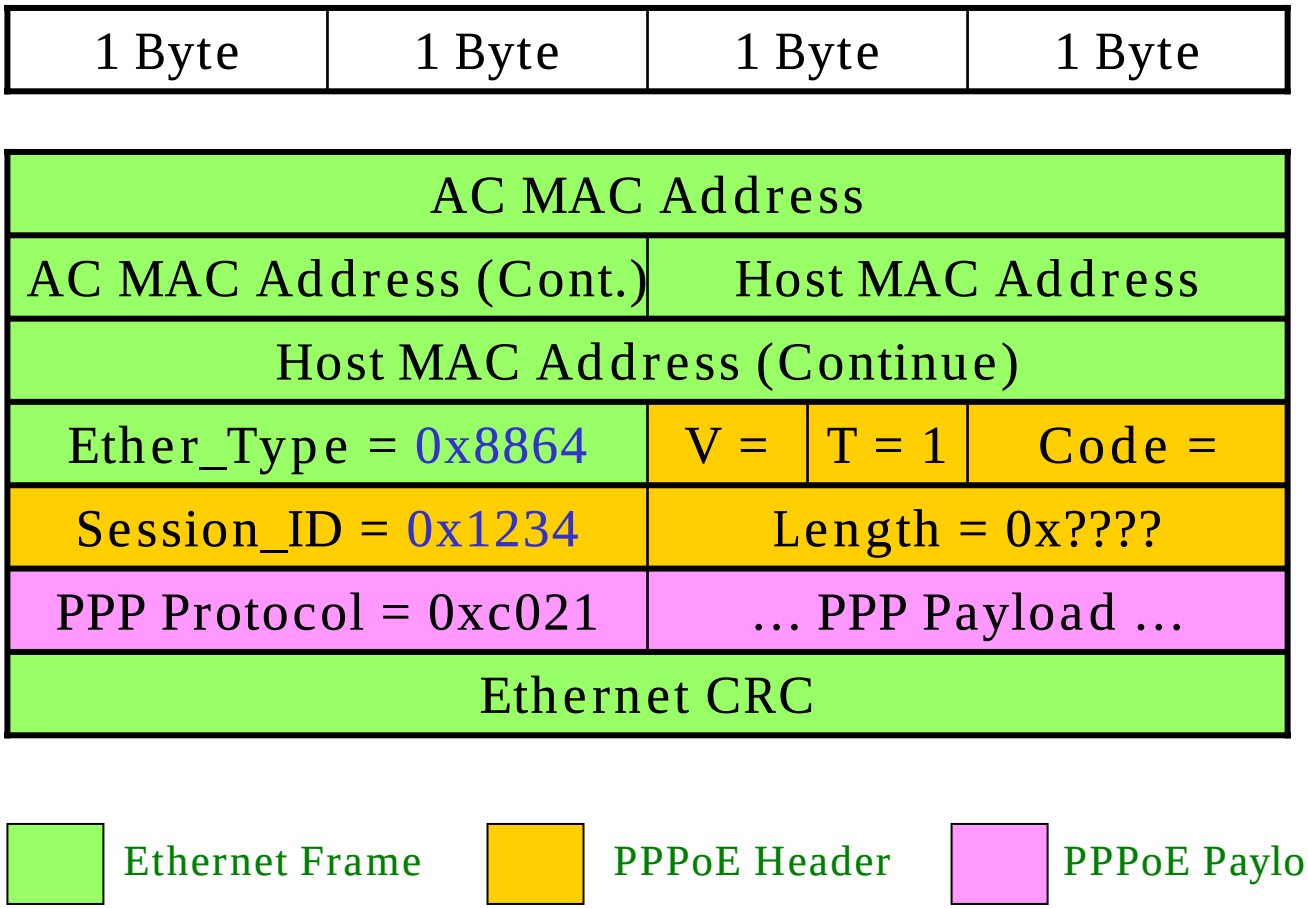
| 0xFFFFFFFF | | | |
|---|---|---|---|
| 0xFFFF | Host MAC Address | | |
| Host MAC Address (Continue) | | | |
| Ether_Type = 0x8863 | V= 1 | T = 1 | code=0x09 |
| Session_ID = 0x0000 | Length = 0x0004 | | |
| TAG_Type = 0x0101 | TAG_Length = 0x0000 | | |
| Ethernet CRC | | | |

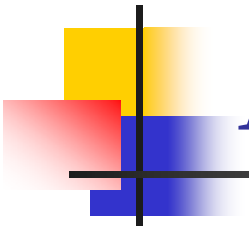
Ethernet Frame  PPPoE Header  PPPoE Payload

# Example PADO packet



# Example PPPoE Session Packet



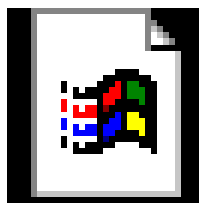


# Agenda

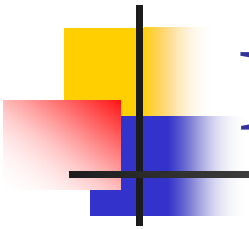
- PPP Overview
- PPP Negotiation Automaton
- Link Control Protocol
- Authentication Protocol
- Network Control Protocol
- PPP over Ethernet
- Packet Analysis of A Real Example

# Packet Analysis of A Real Example

- PPPoE link with SEEDNET ADSL on D-Link DI-713P
- Open the following file with Sniffer Pro



DI-713P to SEEDNET ADSL.cap



# Reference

- Book
  - James Carlson, PPP Design, Implementation and Debugging, 2nd Edition
  - W. Richard Steven, TCP/IP Illustrated, Volume 1
  - Andrew S. Tanenbaum, Computer Networks, 3rd Edition
- RFC
  - PPP: RFC 1661, 1662
  - IPCP: RFC 1332
  - PAP, CHAP: RFC 1334, 1994