POINT TO POINT PROTOCOL (PPP)

ECE422 – DATA COMMUNICATION & COMPUTER NETWORKS

Tuesday, 14 April 2026

DATA COMMMUNICATIONS & COMPUTER NETWORKS SYLLABUS

Course Content:

Introduction: Overview of Data Communications and Networking.

Physical Layer: Analog and Digital, Analog Signals, Digital Signals, Analog versus Digital, Data Rate Limits, Transmission Impairment, More about signals.

Digital Transmission: Line coding, Block coding, Sampling, Transmission mode.

Analog Transmission: Modulation of Digital Data; Telephone modems, modulation of Analog signals.

Multiplexing: FDM, WDM, TDM.

Transmission Media: Guided Media, Unguided media (wireless).

Data Link Layer: Error Detection and correction - Types of Errors, Detection, Error Correction; Data Link Control and Protocols-Flow and Error Control, Stop-and-wait ARQ. Go-Back-N ARQ, Selective Repeat ARQ, HDLC. Point-to-Point Access- Point–to-Point Protocol (PPP), PPP Stack, Multiple Access Random Access, Controlled Access, Channelization.

Network Layer: Host to Host Delivery: Internetworking, addressing and Routing Network Layer Protocols: ARP, IPV4, ICMP, IPV6 and ICMPV6

Transport Layer: Process to Process Delivery: UDP; TCP congestion control and Quality of service.

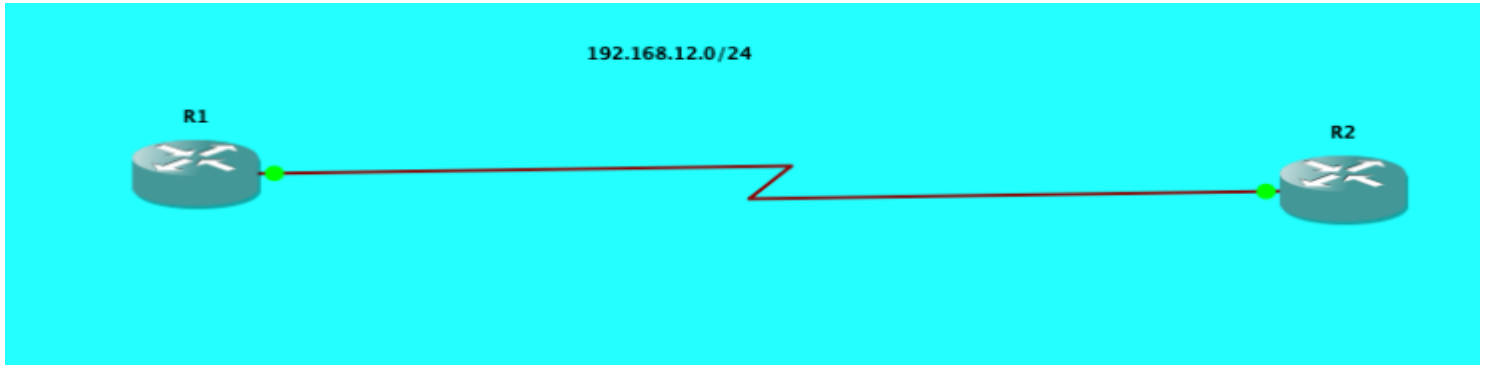
Application Layer: Client Server Model, Socket Interface, Domain Name System (DNS): Electronic Mail (SMTP) and file transfer (FTP) HTTP and WWW.

Local area Network: Ethernet - Traditional Ethernet, Fast Ethernet, Gigabit Ethernet; Token bus, token ring; Wireless LANs - IEEE 802.11, Bluetooth virtual circuits: Frame Relay and ATM.

Industrial Communication and Control Networks: Transmission methods, Network topology, Contemporary networks – Profibus, Controller Area Network (CAN), DeviceNet, CANopen, Actuator Sensor Interface (AS-1),Industrial Ethernet.

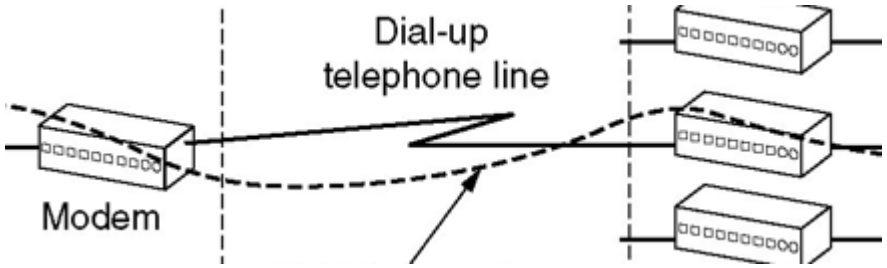
WHAT IS POINT-TO-POINT PROTOCOL?

1. **Point-to-Point Protocol (PPP)** is a data link layer (layer 2) communication protocol between two routers directly without any host or any other networking in between.
2. **PPP** can provide connection
   a) Authentication
   b) Transmission encryption
   c) Data compression.



FEATURES OF POINT-TO-POINT PROTOCOL

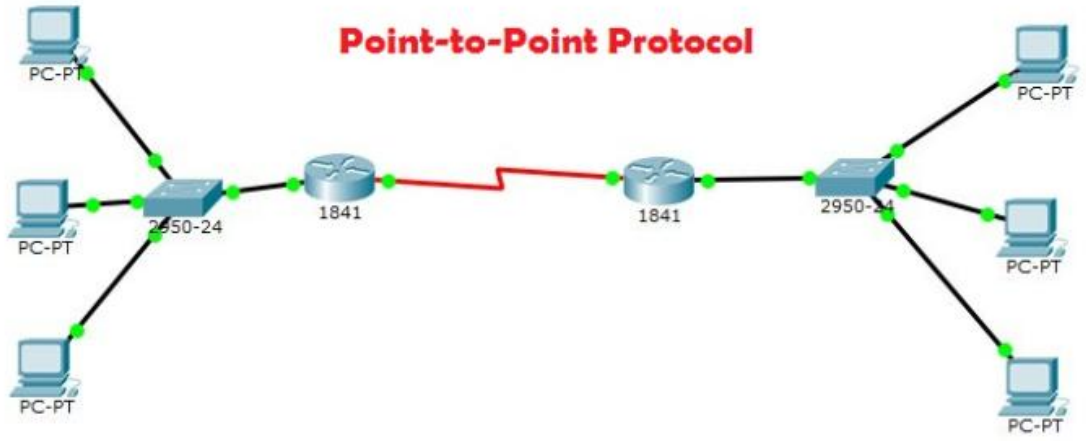
- **Point to Point Protocol (PPP)** links have one sender, one receiver, one link with the following features:
  - No Media Access Control
  - No need for explicit MAC addressing
  - Examples are dialup links, ISDN line



- Popular point-to-point and high-level DLC protocols:
  - PPP (point-to-point protocol)
  - HDLC (High Level Data Link Control). HDLC is also used in multi-point links (one station many receivers)
- These protocols can operate over other data link technologies providing best of both worlds
  - e.g., PPPoE, HDLC encapsulation by Ethernet

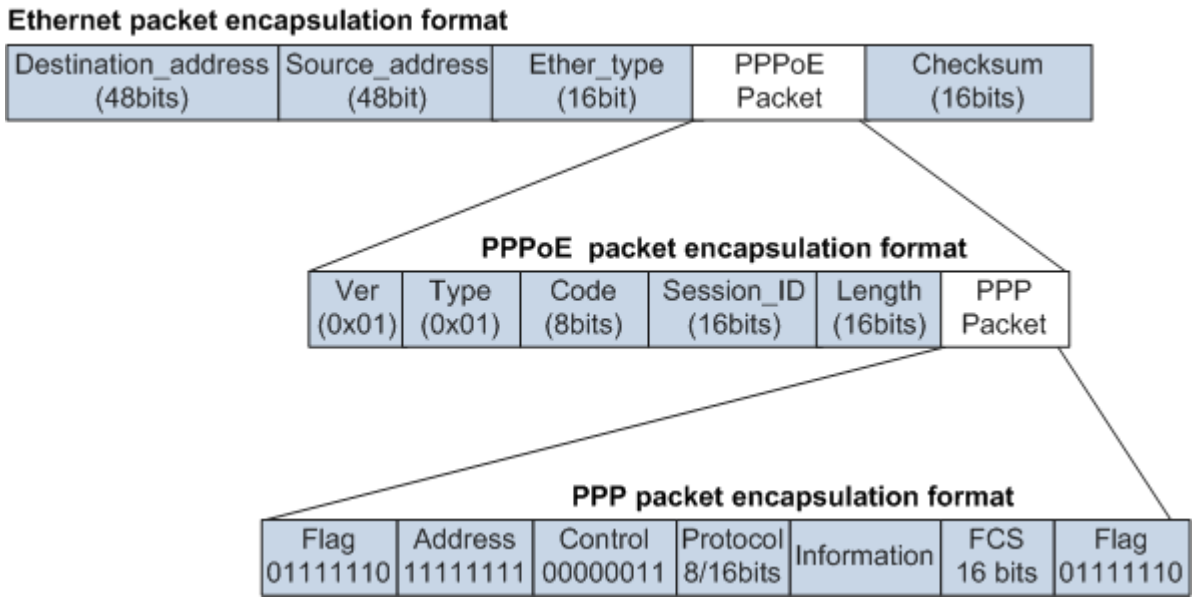
WHAT IS POINT TO POINT PROTOCOL(PPP)?

1. **Point-to-Point Protocol (PPP)** is a data link (layer 2) protocol used to establish a direct connection between two nodes.
2. **PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links.**
3. **PPP is also used over Internet access connections.** Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet.



WHAT IS PPPoE?

- **Point-to-Point Protocol over Ethernet (PPPoE)** facilitates communication between network endpoints.
- **PPPoE encapsulates Point-to-Point Protocol (PPP) frames inside Ethernet frames**, offering the same benefits as PPP, while providing connectivity across Ethernet networks.



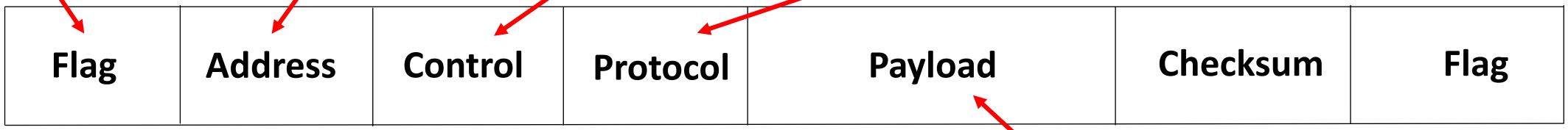
PPP FRAME FORMAT

Flag
1-byte with the bit pattern 01111110

Address
Usually set to 11111111 (broadcast address).

Control
Usually set to the constant value 11000000 (imitating unnumbered frames in HDLC)

Protocol
Defines what is being carried in the data field: either user data or control information.



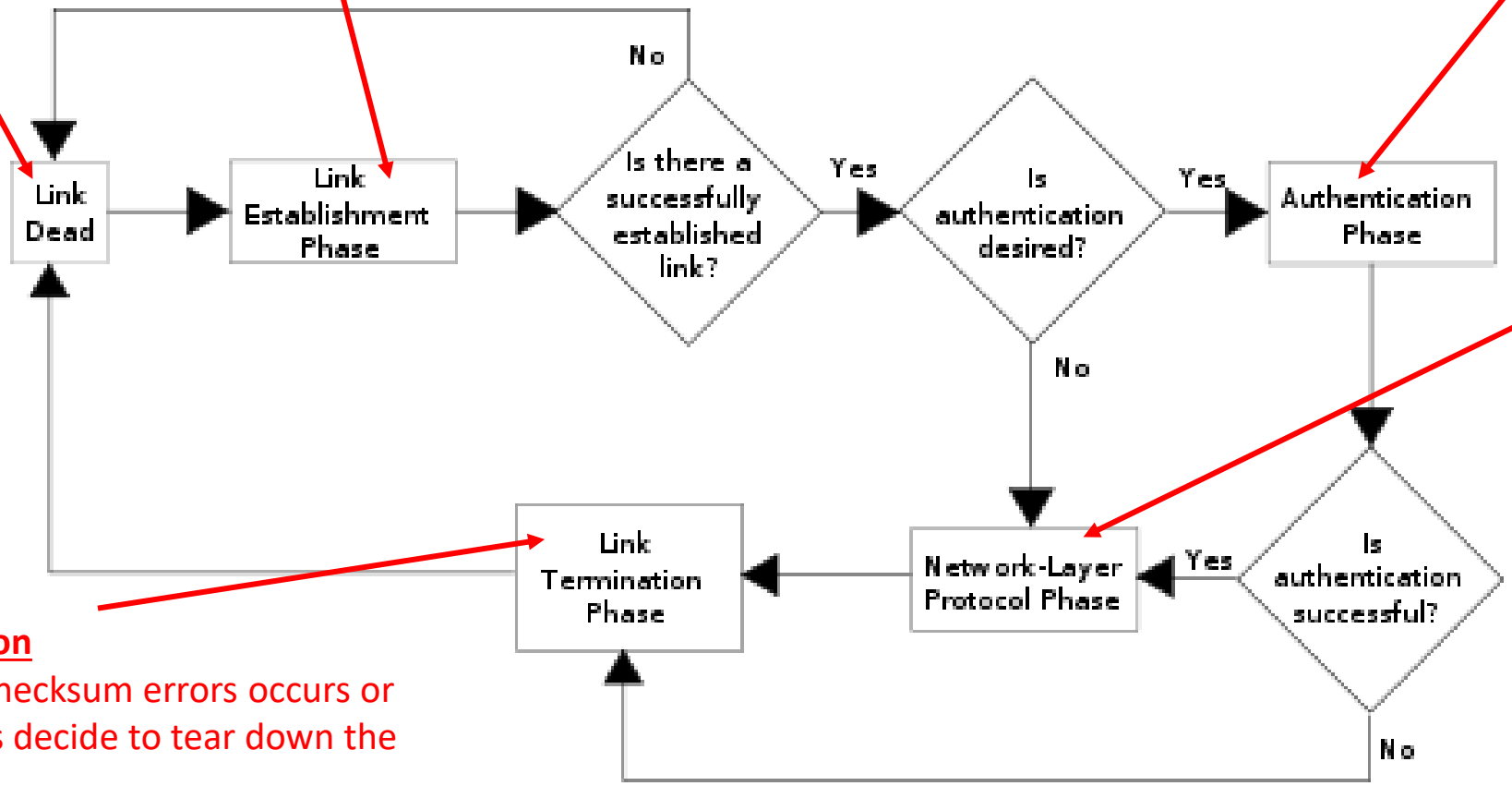
Payload
carries user data or other information

PPP LINE ACTIVATION PHASES

LINK DEAD PHASE
Occurs when the link fails, or one side has been told to disconnect.

LINK ESTABLISHMENT
Link Control Protocol negotiation is attempted

AUTHENTICATION PHASE
Allows both sides to verify each others identity before a connection is established

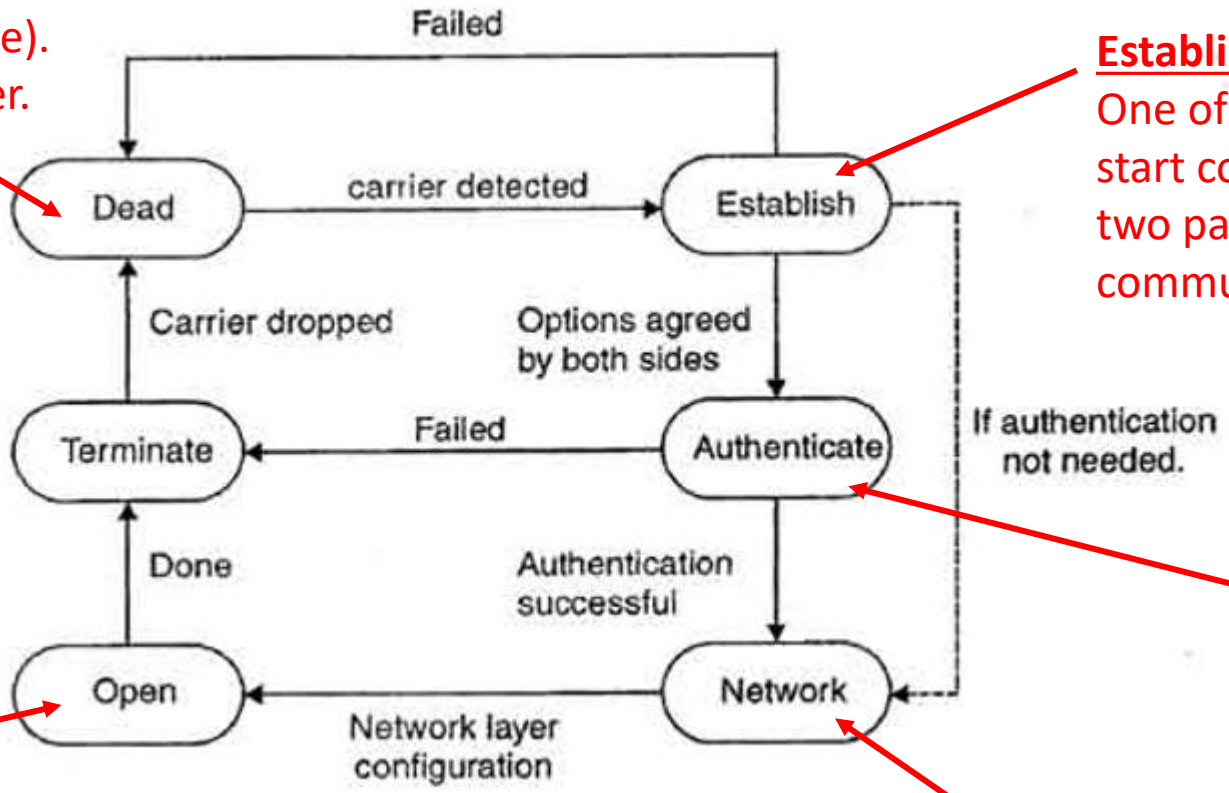


Network Layer Protocol
The Network Control Protocols are invoked

Link Termination
Occurs when checksum errors occurs or the two parties decide to tear down the link.

PPP TRANSITION PHASES

Dead State
Link is not used(or is idle).
There is no active carrier.



Establish Phase
One of the nodes wishes to start communication. The two parties negotiate the communication options

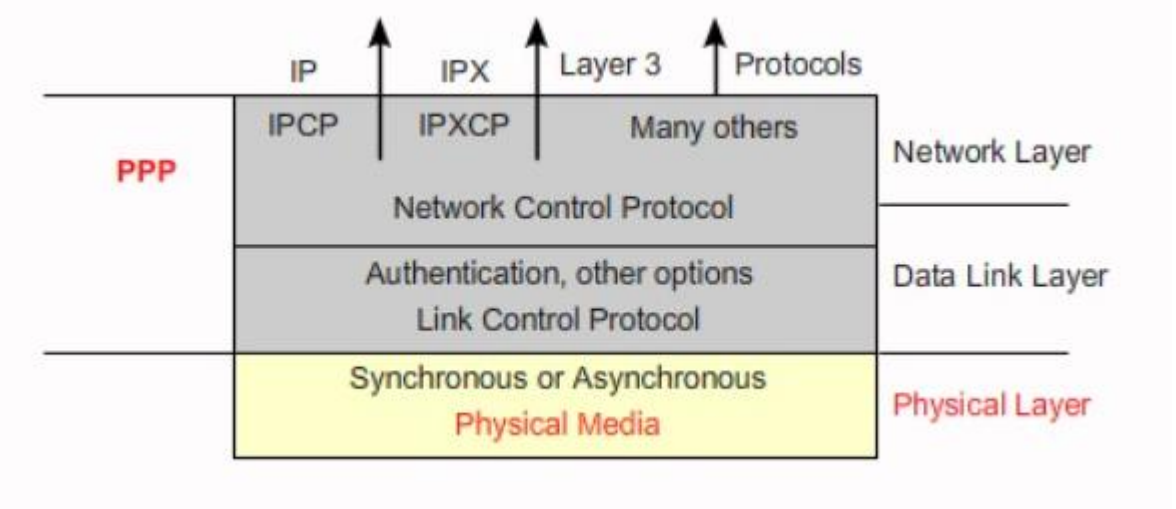
Authentication Phase
The parties send several authentication packets to verify their identities.

Open Phase
Data transfer takes place. The connection remains in this phase until one party requests for termination.

Network Phase
Negotiation for the network layer protocols takes place

POINT TO POINT PROTOCOL STACK

1. PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.
2. The various protocols used are:
   a) Link Control Protocol
   b) Authentication Protocol
   c) Network Control Protocol



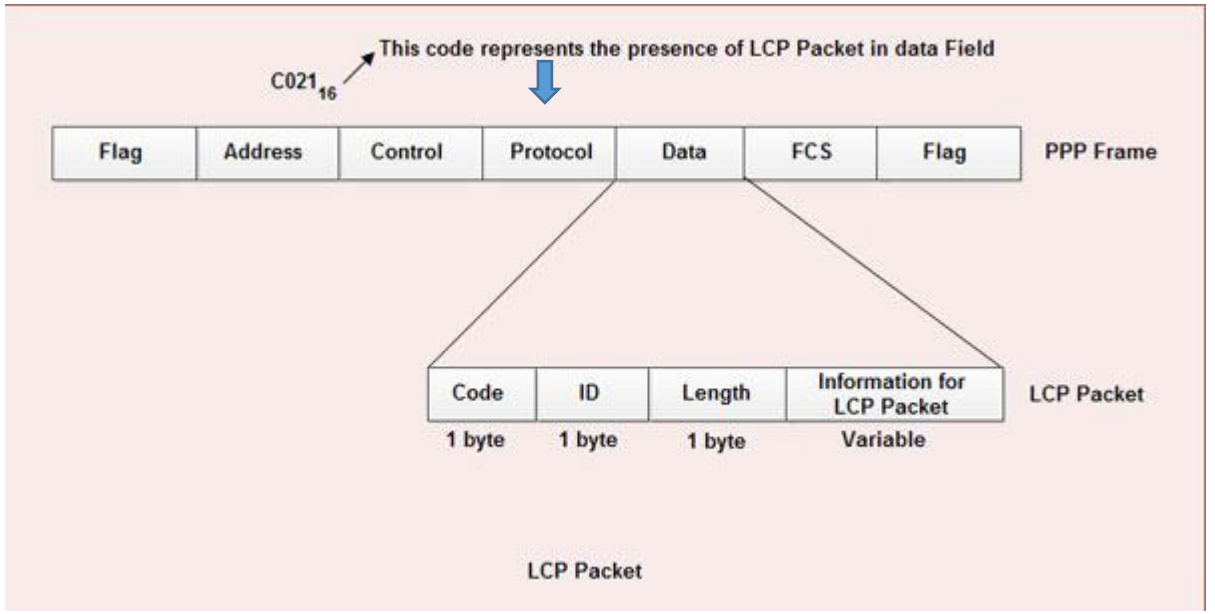
LINK CONTROL PROTOCOL

1. **Link Control Protocol LCP)** is responsible for establishing, maintaining, configuring and terminating the link.

2. LCP provides negotiation mechanism to set options between two endpoints.

3. LCP packets are carried in the data field of the PPP frame.

4. The presence of a value $C021_{hex}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.



AUTHENTICATION PROTOCOL

Authentication protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

1. Password Authentication Protocols (PAP)
2. Challenge Handshake Authentication Protocol (CHAP)

PASSWORD AUTHENTICATION PROTOCOL(PAP)

1. **Password Authentication Protocol (PAP)** provides two step authentication procedure as follows:

   Step 1: Username and password is provided by the user who wants to access a system.

   Step 2: The system checks the validity of username and password and either accepts or denies the connection.

2. PAP packets are carried in the data field of PPP frames.
3. The presence of PAP packet is identified by the value $C023_{16}$ in the protocol field of PPP frame.
4. There are three PAP packets.

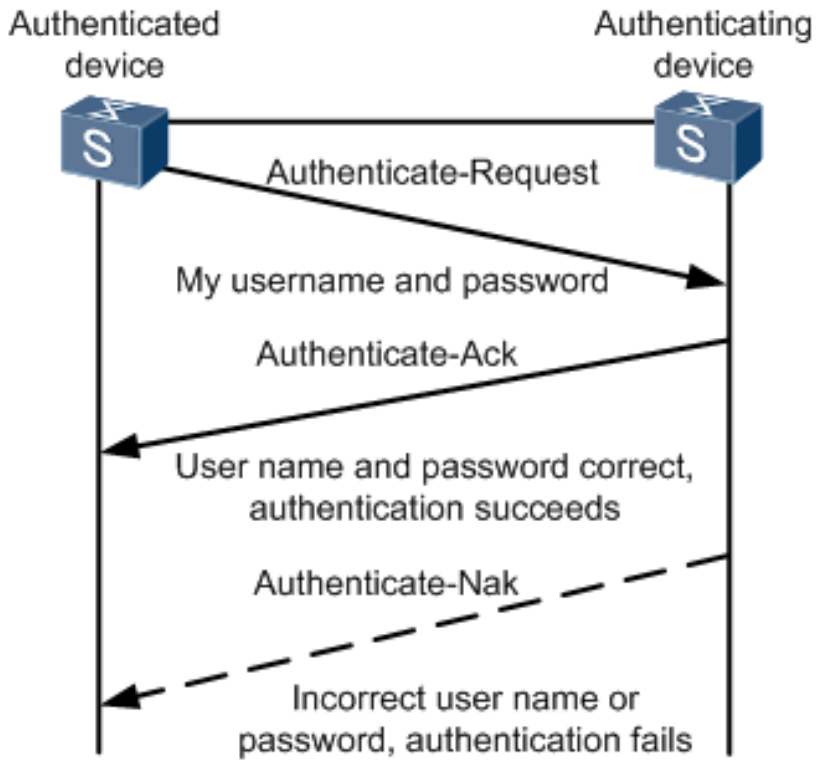
   Authenticate-request: used to send username & password.

   Authenticate-ack: used by system to allow the access.

   Authenticate-nak: used by system to deny the access.

WHAT IS THE PROBLEM WITH PAP?

Password Authentication Protocol (PAP) not a strong authentication method because passwords are transmitted in clear form over the link and there is no protection from repeated attacks during the life of the link.



WHEN SHOULD ONE USE PASSWORD AUTHENTICATION PROTOCOL (PAP)?

PAP may be used in the following situations:

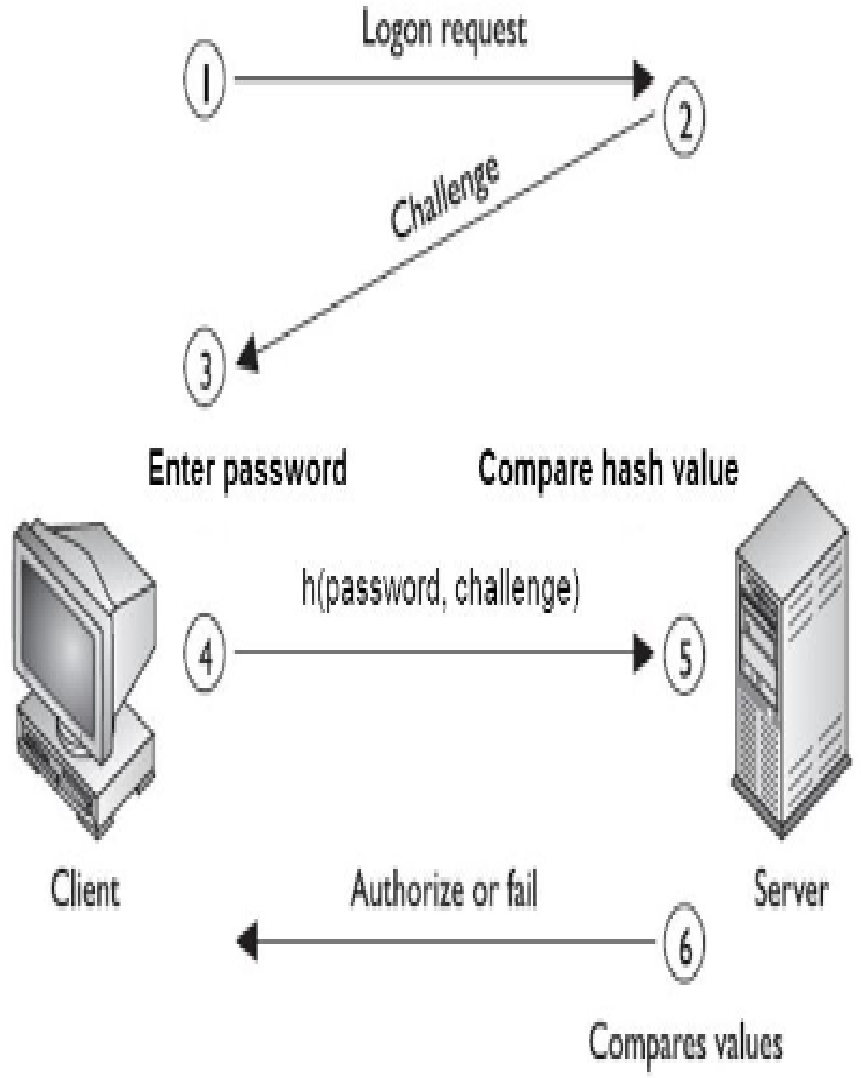
1. When an installed network application does not support **Challenge Handshake Authentication Protocol(CHAP)**
2. Incompatibilities between different vendor implementations of CHAP
3. Circumstances where a plain text password must be available to simulate a login at the remote host

CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL(CHAP)

Challenge Handshake Authentication Protocol(CHAP) is a three-way handshaking authentication protocol:

1. User sends to the system a login request.
2. System sends a challenge packet(random) to the user.
3. Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.
4. System applies the same function to the password of the user and challenge value and creates a result.

If result is same as the result sent in the response packet, access is granted, otherwise, it is denied.



TYPES OF CHAP PACKETS

There are 4 types of CHAP packets:

1. **Challenge**-used by system to send challenge value.
2. **Response**-used by the user to return the result of the calculation.
3. **Success**-used by system to allow access to the system.
4. **Failure**-used by the system to deny access to the system.

NETWORK CONTROL PROTOCOL (NCP)

1. Point-to-Point Protocol (PPP) can carry a network layer data packet from protocols defined by the Internet, Apple Talk, Novell, etc.

2. **Network Control Protocol (NCP)** is a set of control protocols that allow the encapsulation of the data coming from network layer.

3. After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.

Internet Protocol Control Protocol(IPCP) Network Control Protocol for establishing and configuring Internet Protocol over a Point-to-Point Protocol link.

IPX (Internetwork Packet Exchange) A networking protocol from Novell that interconnects networks that use Novell's NetWare clients and servers.