Course Name: A Level (2nd Sem) Subject: DCN

Topic: PPP contd. Date: 17-04-20

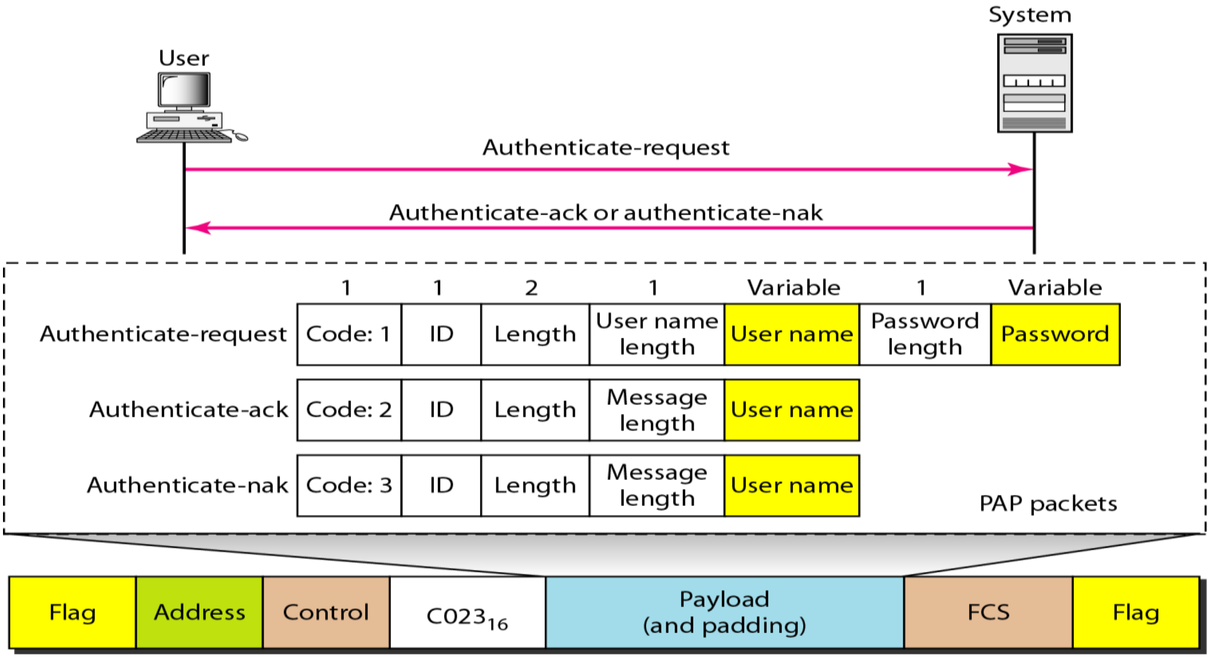
Password Authentication Protocol (PAP):

The **Password Authentication Protocol (PAP)** is a simple authentication procedure with a two-step process:

1. The user who wants to access a system sends authentication identification (usually the user name) and a password.

2. The system checks the validity of the identification and password and either accepts or denies connection.

Figure shows the three types of packets used by PAP and how they are actually exchanged. When a PPP frame is carrying any PAP packets, the value of the protocol field is OxC023. The three PAP packets are authenticate-request, authenticate-ack, and authenticate-nak. The **first** packet is used by the user to send the user name and password. The **second** is used by the system to allow access. The **third** is used by the system to deny access.



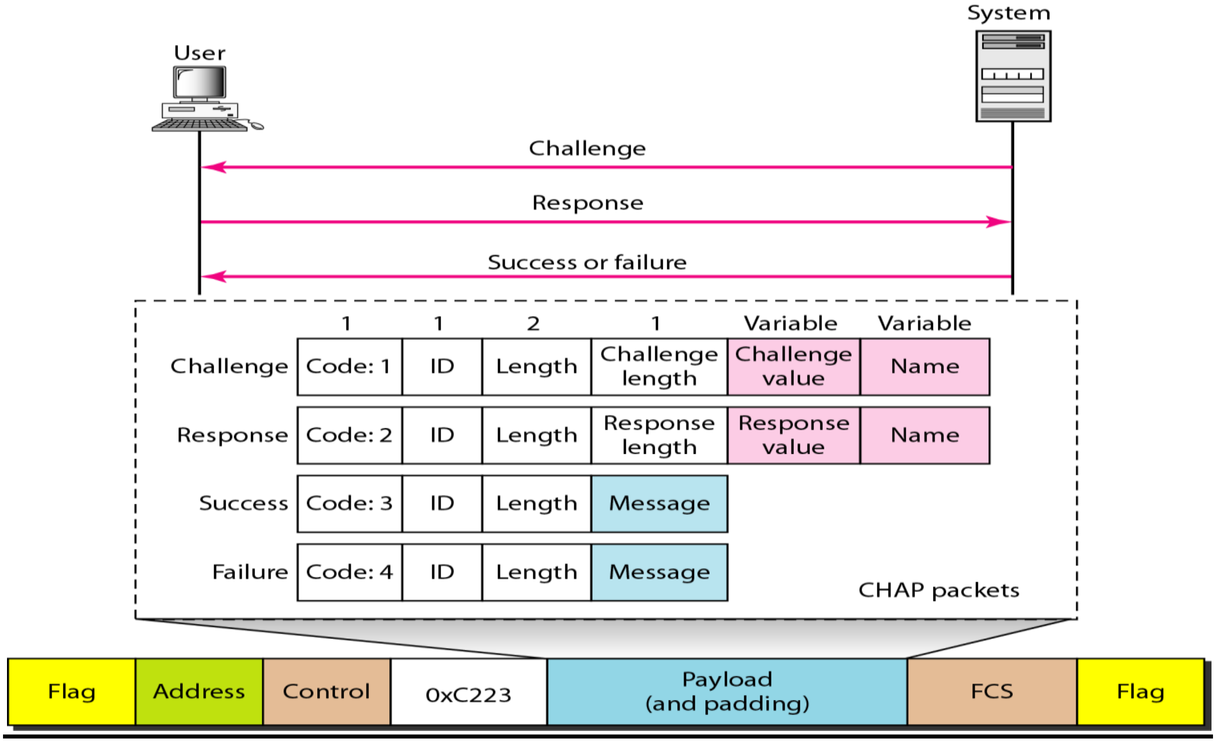
Challenge Handshake Authentication Protocol (CHAP):

The Challenge Handshake Authentication Protocol (CHAP) is a three-way hand-shaking authentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent online.

1. The system sends the user a challenge packet containing a challenge value, usually a few bytes.

2. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.

3. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied. CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret. Figure shows the packets and how they are used.



	1	1	2	1	Variable	Variable
Challenge	Code: 1	ID	Length	Challenge length	Challenge value	Name
Response	Code: 2	ID	Length	Response length	Response value	Name
Success	Code: 3	ID	Length	Message		
Failure	Code: 4	ID	Length	Message		

CHAP packets are encapsulated in the PPP frame with the protocol value C223 in hexadecimal. There are four CHAP packets: challenge, response, success, and failure. The first packet is used by the system to send the challenge value. The second is used by the user to return the result of the calculation. The third is used by the system to allow access to the system. The fourth is used by the system to deny access to the system.

Network Control Protocols:

PPP is a multiple-network layer protocol. It can carry a network layer data packet from protocols defined by the Internet, OSI, Xerox, DECnet, AppleTalk, Novel, and so on. To do this, PPP has defined a specific Network Control Protocol for each network protocol. For example, IPCP (Internet Protocol Control Protocol) configures the link for carrying IP data packets. Xerox CP does the same for the Xerox protocol data packets, and so on. None of the NCP packets carry network layer data; they just configure the link at the network layer for the incoming data.

Exercises:

A. **Compare and Contrast PPP and CHAP?**

B. **“CHAP is more secure than PPP”? Justify the comment.**