Networking

Networking Fundamentals

1.1.2 - Encapsulation and Decapsulation

What is encapsulation and decapsulation and how does it work with the OSI model?

Overview

The student will be able to compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 1.1

- Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
    - Data encapsulation and decapsulation within the OSI model context
        - Ethernet header
        - Internet Protocol (IP) header
        - Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) headers
        - TCP flags
        - Payload
        - Maximum transmission unit (MTU)

Encapsulation and Decapsulation

Within the OSI model, ***encapsulation*** adds information to a packet, such as the header and the footer, as it travels down the OSI model. It is also the process of transforming the data from the application layer's human-readable data to 0's and 1's. ***Decapsulation*** reverses the process by removing the added information, so a destination device can read what was originally sent. It is the process of transforming from 0's and 1's back to the application layer's human-readable data all while losing the header and footer data.

The process starts at the Application layer where the user interface exists. The data is passed to the Presentation layer and then to the Session layer, each adding a small amount of additional information before passing it off to the Transport layer. The data is broken into smaller pieces and a ***TCP header*** is added. The Transmission Control Protocol (TCP) header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. We refer to this data as a segment. (We also have ***User Datagram Protocol headers*** but they do not guarantee data arrival or error-checking like TCP does).

TCP flags are various types of flag bits present in the TCP header. They initiate connections, carry the data, and even tear down connections. Some common TCP flags are syn, ack, rst, fin, urg, psh.

Teacher Notes:

Each segment is passed to the Network layer for network addressing and routing through the Internet. At this point, the data is called a packet. The Network layer adds its IP header and sends it off to the Datalink layer. An ***IP header*** is simply header information at the beginning of an Internet Protocol (IP) packet.

At this point, we call the data a frame. A frame includes the ***ethernet header***, the original data/***payload*** itself, and a trailer. The ethernet header contains a preamble, the start frame delimiter, the destination MAC address, the source MAC address, and the type. A ***maximum transmission unit*** (MTU) is the largest packet or frame size, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network such as the internet. The internet's transmission control protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission.

From the Datalink layer, the frame is sent to the destination computer via digital signal at the Physical layer. Once received, the process is simply reversed so the receiver can read the data.