INFORMATION SECURITY ADVANCED

Chapter 3 | Network Security

Dr. Jamil Alagha

OUTLINE

- Authentication
- Access Control
- Networking Services Protocols
  - Internet protocol
  - TCP/IP
- Network Devices and Security

AUTHENTICATION, ACCESS CONTROL

- Security Services: Defined by X.800, OSI Security Architecture:
- a service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

- Defined by RFC 4949:
- a processing or communication service provided by a system to give a specific kind of protection to system resources

AUTHENTICATION, ACCESS CONTROL

- **Authentication** :
- Concerned with assuring that a communication is **authentic.**
- In the case of a single message, assures the recipient that the message is from the source that it claims to be from.

AUTHENTICATION, ACCESS CONTROL

- In the case of an ongoing interaction, two aspects are involved:
- ***First***, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be.
- ***Second***, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

AUTHENTICATION, ACCESS CONTROL

- **Access Control:**
- It is the ability to limit and control the access to host systems and applications via communications links.

- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Networking Services Protocols

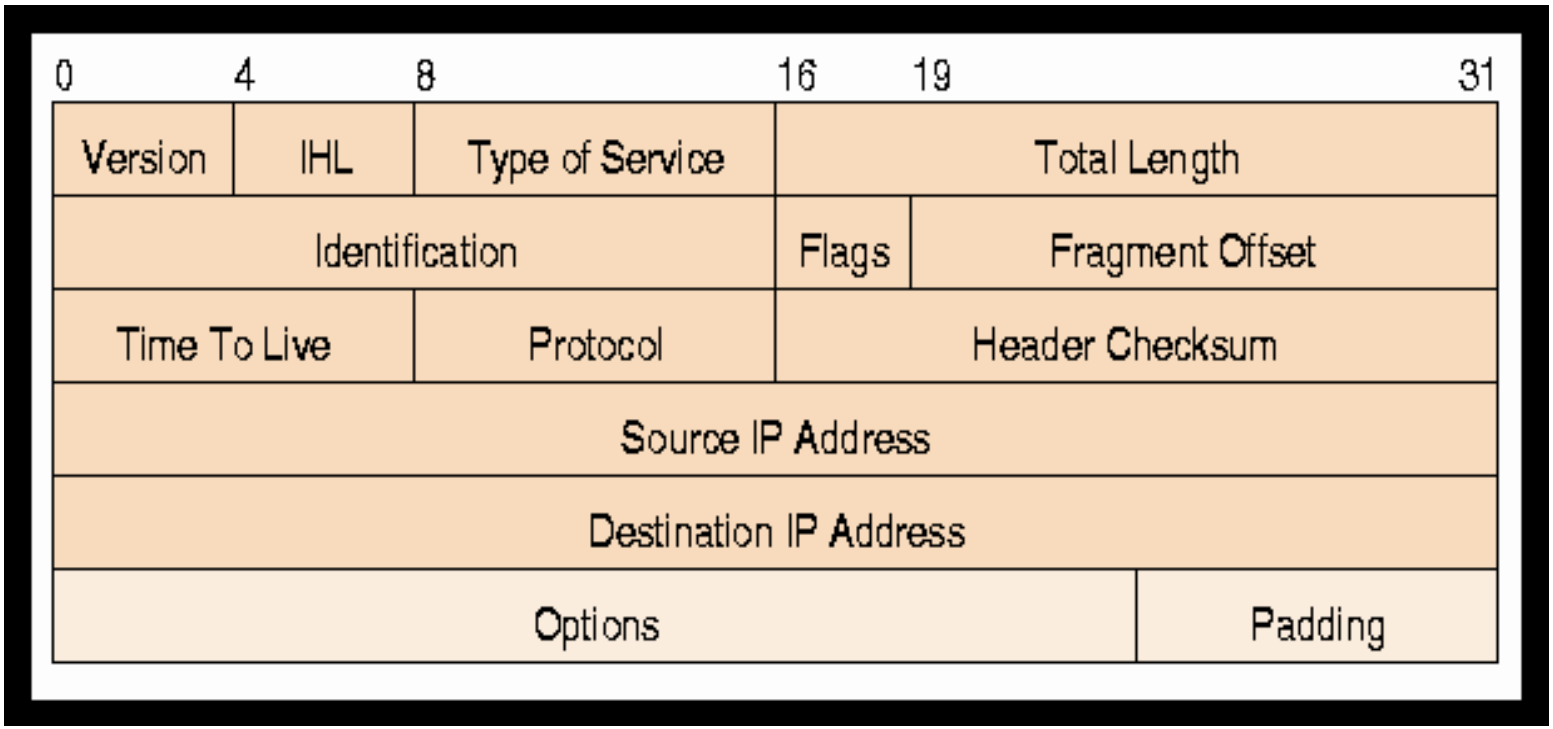
INTERNET PROTOCOLS

- Communication: A → B.
- Form of the communication.
  - meaning of an element has the same meaning to both (A,B).
- Medium of communication
  - Both parties must have access to the same communication medium.
  - Phone.

INTERNET PROTOCOLS

- With computers
  - Networks
    - is made connection possible by protocols.
  - Protocol
    - is a well-defined message format.
  - Message format
    - defines what each position in the message means.
    - One possible message format
      - the first 4 bits as the version number,
      - the next 4 bits as the length of the header, and
      - then 8 bits for the service being used.
    - both computers agree on this format
      - communication can take place.

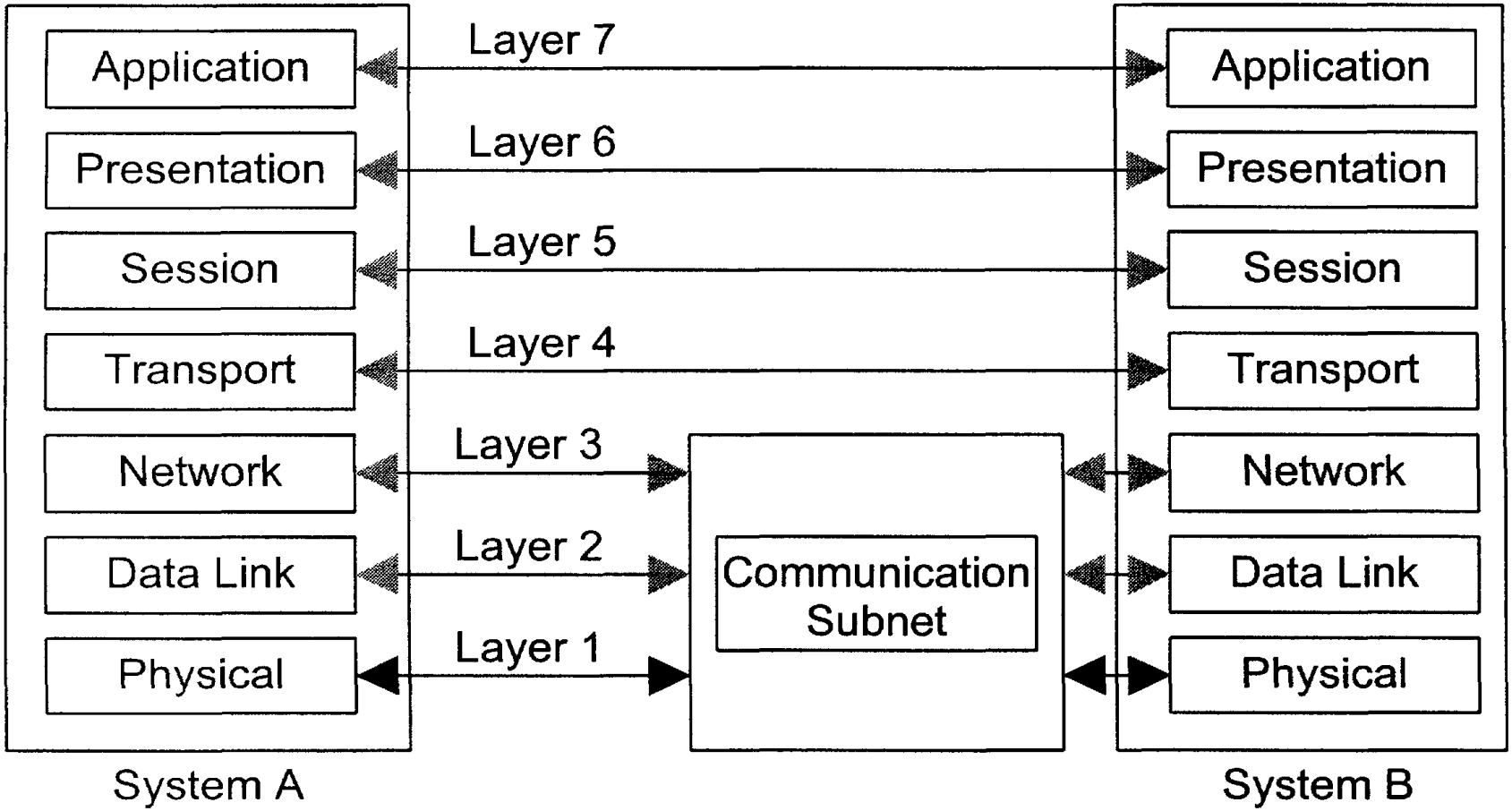
MESSAGE BLOCK



INTERNET PROTOCOLS

- Protocol Suites
  - More than one protocol
  - layered protocols.
  - Transport Control Protocol/ Internet Protocol (TCP/IP) suite.
    - It is based on the International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model.

INTERNET PROTOCOLS



INTERNET PROTOCOLS

- Reference Model 7 layers

1. Physical Layer I
   - lowest layer in the protocol stack.
   - consists of the "physical" connection.
     - This may be copper wire or fiber-optic cables and the associated connection hardware.
   - to transfer the bits from one location to another.

INTERNET PROTOCOLS

2. Data-Link Layer
   - provides for the reliable delivery of data across the physical link.
   - creates a checksum of the message that can be used by the receiving host to ensure that the entire message was received.

INTERNET PROTOCOLS

3. Network Layer
   - manages the connections across the network for the upper four layers .
   - isolates them from the details of addressing and delivery of data.

4. Transport Layer
   - provides the end-to-end error detection
   - correction function between communicating applications.

INTERNET PROTOCOLS

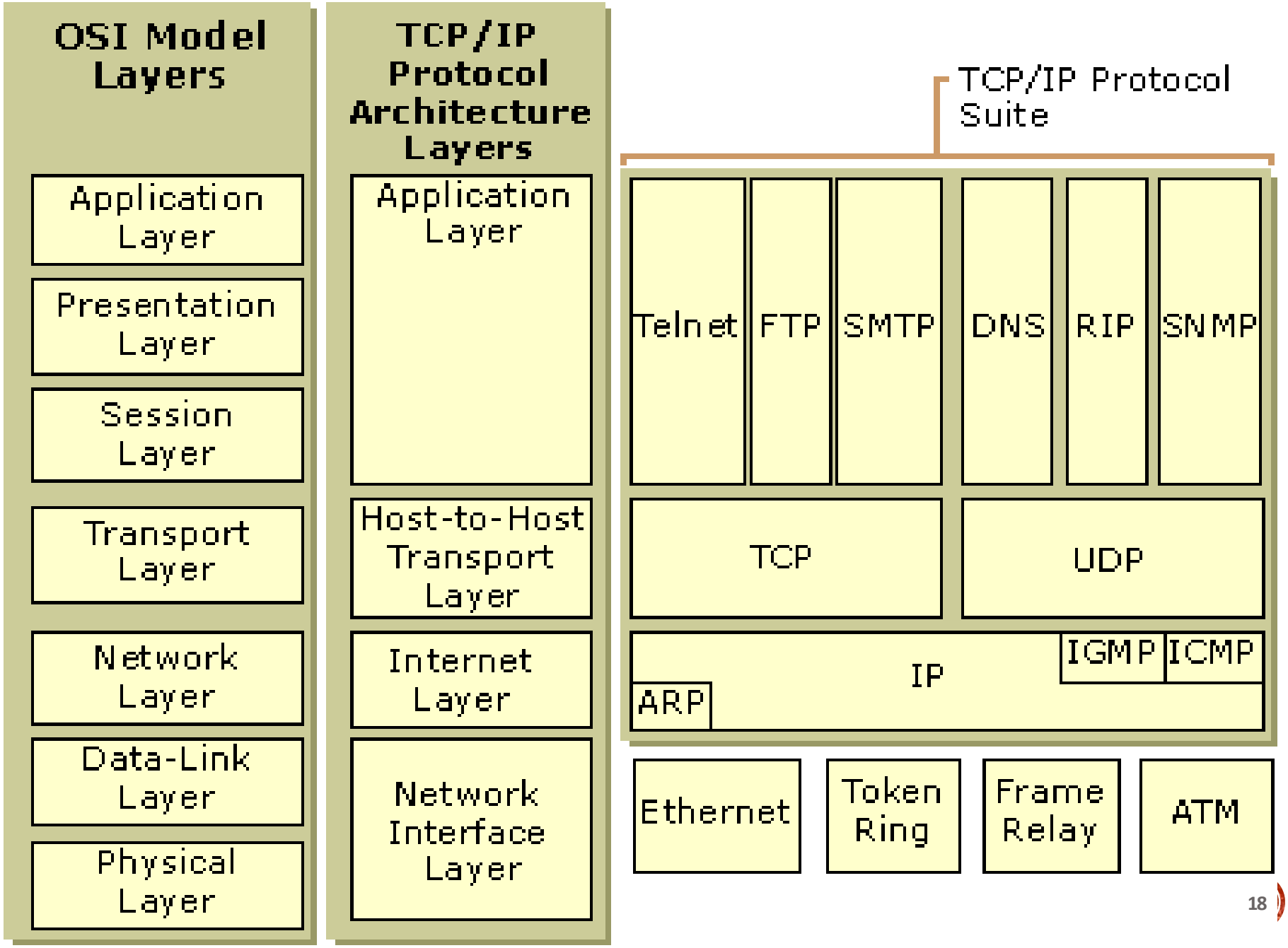
5. Session Layer
   - manages the sessions between communicating applications.

6. Presentation Layer
   - standardizes the data presentation to the application level.

7. Application Layer
   - consists of application programs that communicate across the network.
   - This is the layer with which most users interact.

TCP/IP PROTOCOL ARCHITECTURE.

- Transmission Control Protocol/Internet Protocol (TCP/IP)
  - is based on the ISO model
  - it groups the seven layers of the ISO model into four layers


OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IP
IGMP
ICMP
ARP
Ethernet
Token Ring
Frame Relay
ATM

TCP/IP PROTOCOL ARCHITECTURE.

Application Layer consists of applications and processes that use the network.
Host-to-Host Transport Layer provides end-to-end data delivery service.
Internet Layer Defines the datagram and handles the routing of data.
Network Access Layer consists of routines for accessing physical networks.

TCP/IP PROTOCOL ARCHITECTURE.

- Network Access Layer:
- encapsulate the datagrams and maps the IP addresses to the physical addresses
  - the lowest layer of the TCP/IP protocol stack.
  - provides the means of delivery
  - has to understand how the network transmits data from one IP address to another.

TCP/IP PROTOCOL ARCHITECTURE.

- basically provides the functionality of the first three layers of the ISO model.
- TC/IP provides a scheme of IP addressing that uniquely defines every host connected to the Internet.
- The Network Access Layer
  - provides the functions that **encapsulate the datagrams and maps the IP addresses to the physical addresses used by the network**.

TCP/IP PROTOCOL ARCHITECTURE.

- The Internet Layer: Moving Data (RFC 791)
  - its core - Internet Protocol (**IP**)
  - IP provides
    - the basic building blocks of the Internet.
    - Datagram definition scheme
    - Internet addressing scheme
    - Means
      - of moving data between the Network Access Layer and the Host-to-Host Layer
      - for datagrams to be **routed** to remote hosts

TCP/IP PROTOCOL ARCHITECTURE.

- **The Internet Layer**
  - Function of breaking apart and reassembling packets for transmission
  - a connectionless protocol.
    - relies on TCP to provide the connection-oriented services.
    - take care of the handshake — the exchange of control information.
  - The IP Layer contains the Internet Control Message Protocol (ICMP).

TCP/IP PROTOCOL ARCHITECTURE.

- Transport Layer (Host-to-Host)
  - deliver messages
    - between the Application Layer and the Internet Layer.
  - houses two protocols
    - Transport Control Protocol (TCP)
      - a reliable protocol.
      - contains error detection and correction features.
    - User Datagram Protocol (UDP).
      - unreliable.
      - For shorter messages, where it is easier to resend the message than worry about the overhead involved with TCP, UDP is used.

TCP/IP PROTOCOL ARCHITECTURE.

- Application Layer
  - contains
    - various services that users will use to send data.
    - user programs as
      - the Network Terminal Protocol (Telnet),
      - File Transfer Protocol (FTP),
      - Simple Mail Transport Protocol (SMTP).
    - protocols not directly used by users, but required for system use
      - Domain Name Service (DNS)
      - Routing Information Protocol (RIP)
      - Network File System (NFS)

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

- **ICMP**
  - A major component of the TCP/IP Internet Layer
  - is used for
    - flow control, detecting unreachable destinations, redirection routes, and checking remote hosts.
  - Most users are interested in.
    - Checking a remote host
      - is accomplished by (**PING**)- sending an ICMP Echo Message.

Network Devices and Security

NETWORK DEVICES AND SECURITY

- To build a Network we need hardware devices
  - **can provide different levels of security,**
  - **depending on how far up the stack they can read.**
    - **Repeaters + Bridge**
    - **Routers and gateways**
    - **Switch Vs Hub**

REPEATERS + BRIDGE

- Repeaters
  - to connect two Ethernet segments.
  - simply copies the electrical transmission and sends it on to the next segment of the network (**forward**).
  - Because the repeater only reads up through the Data-Link Layer, no security can be added by its use.

REPEATERS + BRIDGE

- Bridge
  - a computer that is used to connect two or more networks.
  - can **store** and forward entire packets. (!like repeater)
  - Because it reads up through the Network Layer of the packet, the bridge can add some security.
    - It could allow the transfer of only packets with local addresses.
  - uses
    - physical addresses — not IP addresses.
    - physical address = the Ethernet address
    - is the actual address of the Ethernet hardware. It is a 48-bit number.

Router

- determine which of the many possible paths a packet will take to get to the destination device. (Layer 3)
- read up through the Transport Layer and can read IP addresses, including port numbers.
  - dynamically via routing protocols
  - manually via administratively defined static routes.
    - a firewall to be inform.
- They can be programmed to
  - allow, disallow, and reroute IP datagrams determined by the IP address of the packet.

SWITCH VS HUB

- Switch Vs Hub
  - layer two device
  - Hub (***Broadcast***)
    - were dumb devices
    - used to
      - transmit packets between devices connected to them,
    - functioned by retransmitting each and every packet received on one port out through all of its other ports.
    - Problem - collusion
    - Problem – sniff - Workstation see all traffic

SWITCH VS HUB

- Switch Vs Hub
  - Switch (***switching***)
    - intelligent device
    - learn the various MAC (Media Access Control) addresses of connected devices
    - Transmit packets to the devices they are specifically addressed to.
    - provide a security benefit by
      - reducing the ability to monitor or "sniff" another workstation's traffic.

END

Questions