# INFO 6010 Lesson 7
# Communication & Network Security Part 1
# Domain 4

Revision 2

Information Security Management & Network Security and Architecture

FANSHAWE

# Discussion Topics

- **Part One**
  - OSI and TCP/IP models
  - Protocol types and security issues
  - LAN, WAN, MAN, intranet, and extranet technologies
  - Transmission media
  - Wireless technologies

- **Part Two**
  - Network components and services
  - Communications security management
  - Remote access technologies
  - Threats and attacks
  - Software-defined networks
  - Content distribution networks
  - Multilayer protocols
  - Convergent network technologies

# CISSP – Network domain (1)

- To secure a network architecture you must understand:
  - Various networking platforms involved
  - Network devices
  - How data flows through a network
  - Understand various protocols
  - Protocol purposes, their interactions with other protocols
  - How protocol may be exploitable or its vulnerabilities
  - Understand how to implement appropriate protocols in a given environment

# CISSP – Network domain (2)

- To secure a network architecture you must understand:
  - Different devices, protocols, and security mechanisms within an environment provide different functionality
  - Provide a layered approach to security
  - Layers are important, if an attacker penetrates one layer, another layer protects internal network

# OSI Model

- **Open Systems Interconnection Reference Model**
- **International Organization for Standardization** is a worldwide federation that works to provide international standards.
- In the early 1980s, ISO worked to develop a protocol set that would be used by all vendors throughout the world to allow the interconnection of network devices.
- OSI model was introduced in 1984, at which time the basics of the Internet had already been developed and implemented

# OSI Model

- The Transmission Control Protocol/Internet Protocol (TCP/IP) suite has own model that is used today when examining and understanding networking issues
- The OSI reference model, as described by ISO Standard 7498, provides important guidelines used by vendors, engineers, developers, and others
- The model segments the networking tasks, protocols, and services into different layers
- Each layer has its own responsibilities regarding how two computers communicate over a network

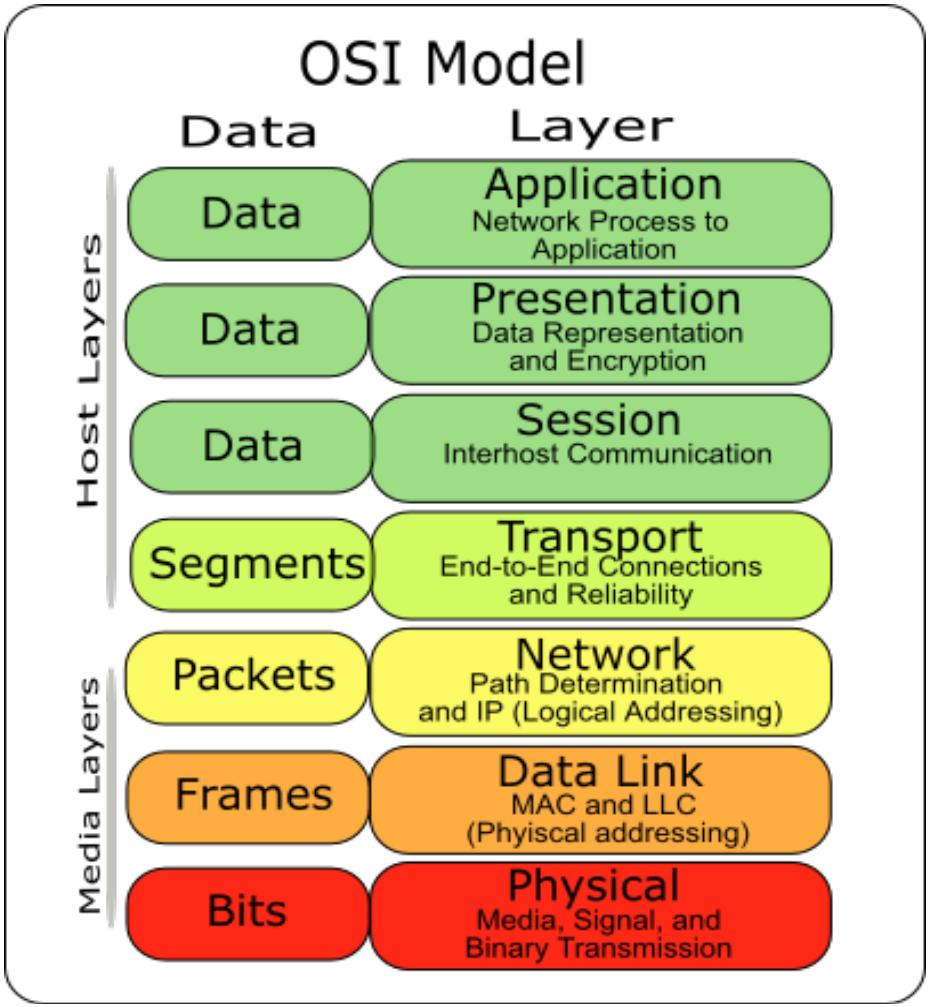
# OSI Model

- The OSI model's goal is to help others develop products that will work within an open network architecture
  - An open network architecture is one that no vendor owns, that is not proprietary, and that can easily integrate various technologies and vendor implementations of those technologies
  - Because vendors use the OSI model integration of products is easier
  - Less Interoperability issues than if each vendor had their own networking framework
- Each protocol at a specific OSI layer on one computer communicates with a corresponding protocol operating at the same OSI layer on another computer
- This communication at each OSI layer is done through **encapsulation**

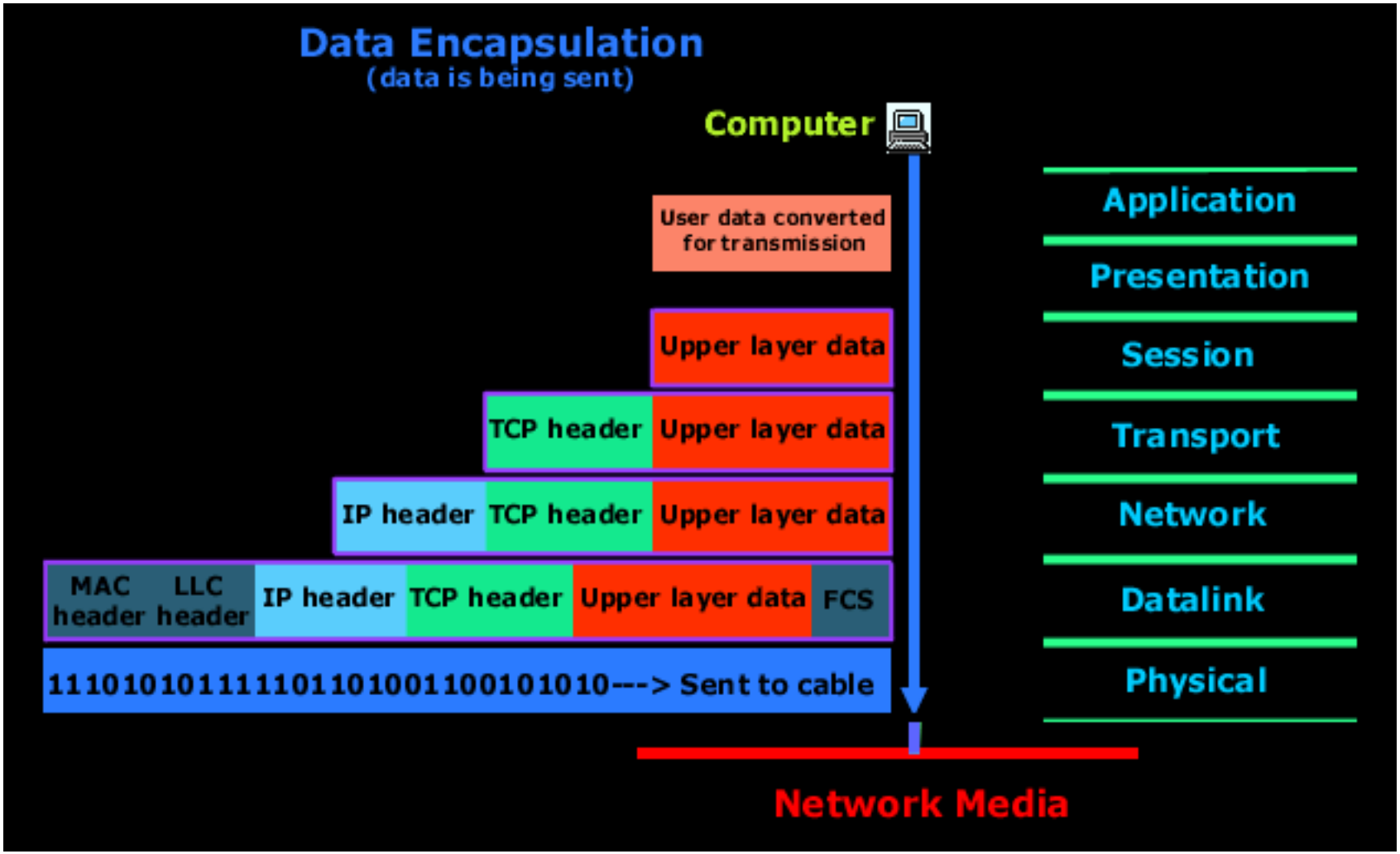
# Encapsulation

- A message is constructed within a program on one computer and then passed down through the OSI stack.
- A protocol at each OSI layer adds its own information to the message (Header)
- Message grows in size as it goes down the protocol stack
  - Data same size but headers added
- Message is then sent to the destination computer
- Process is reversed by taking the packet apart through the same steps in reverse
- At each OSI Layer ONLY the information pertaining to the layer is extracted and the remainder is passed to next layer

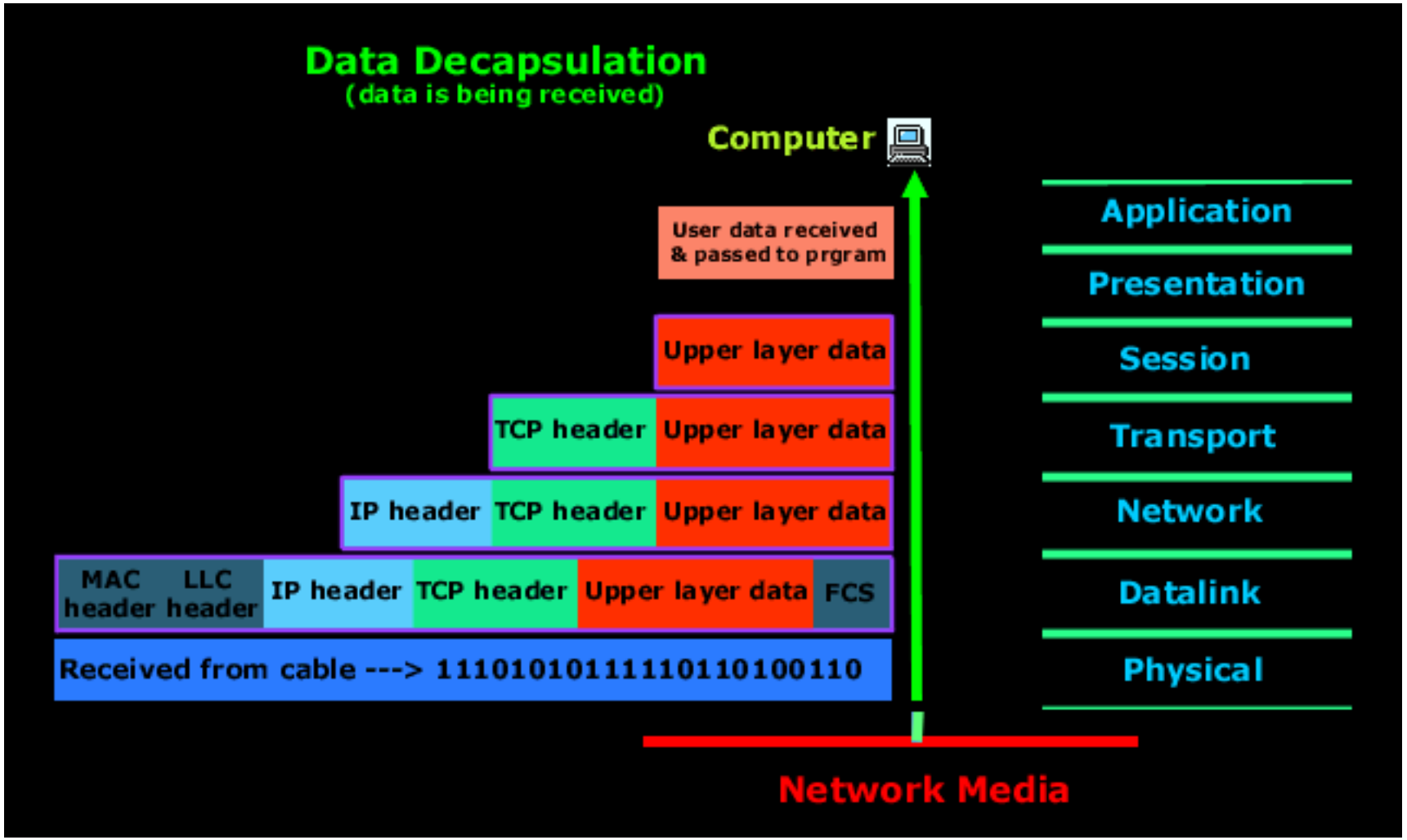
# OSI Model


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

# OSI Model


Data Encapsulation
(data is being sent)
Computer
User data converted for transmission
Upper layer data
TCP header
Upper layer data
IP header
TCP header
Upper layer data
MAC header
LLC header
IP header
TCP header
Upper layer data
FCS
11101010111110110100110010101010---> Sent to cable
Application
Presentation
Session
Transport
Network
Datalink
Physical
Network Media

# OSI Model


Data Decapsulation
(data is being received)
Computer
User data received & passed to prgram
Upper layer data
TCP header
Upper layer data
IP header
TCP header
Upper layer data
MAC header
LLC header
IP header
TCP header
Upper layer data
FCS
Received from cable ---> 11101010111110110100110
Application
Presentation
Session
Transport
Network
Datalink
Physical
Network Media

# OSI Model

- **Layer Seven – Application Layer**
  - The Application Layer of the OSI model is responsible for providing end-user services, such as file transfers, electronic messaging, e-mail, virtual terminal access, and network management. This is the layer with which the user interacts.
- **Layer Six - Presentation Layer**
  - Presentation Layer of the OSI model is responsible for defining the syntax which two network hosts use to communicate. Encryption and compression should be Presentation Layer functions.

# OSI Model

- **Layer Five – Session Layer**
  - The Session Layer of the OSI model is responsible for establishing process-to-process communications between networked hosts.
- **Layer Four – Transport Layer**
  - The Transport Layer of the OSI model is responsible for delivering messages between networked hosts. The Transport Layer  encapsulates the data segment

# OSI Model

- **Layer Three – Network Layer**
  - The Network Layer of the OSI model is responsible for establishing paths for data transfer through the network. Fragmentation and reassembly of packets
  - Routers operate at the Network Layer
- **Layer Two – Data-Link Layer**
  - The Data Link Layer of the OSI model is responsible for communications between adjacent network nodes. Hubs and switches operate at the Data Link Layer.
- **Layer One – Physical Layer**
  - The Physical Layer of the OSI model is responsible for bit-level transmission between network nodes. The Physical Layer defines items such as: connector types, cable types, voltages, and pin-outs.

# Applications - 7

- The protocols at the application layer handle file transfer, virtual terminals, network management, and fulfilling networking requests of applications.
- A few of the protocols that work at this layer include:
  - File Transfer Protocol (FTP)
  - Trivial File Transfer Protocol (TFTP)
  - Simple Network Management Protocol (SNMP)
  - Simple Mail Transfer Protocol (SMTP)
  - Telnet
  - Hypertext Transfer Protocol (HTTP)

# Presentation - 6

- The services of the presentation layer handle translation into standard formats, data compression and decompression, and data encryption and decryption. No protocols work at this layer, just services. The following lists some of the presentation layer standards:
  - American Standard Code for Information Interchange (ASCII)
  - Extended Binary-Coded Decimal Interchange Mode (EBCDIC)
  - Tagged Image File Format (TIFF)
  - Joint Photographic Experts Group (JPEG)
  - Motion Picture Experts Group (MPEG)
  - Musical Instrument Digital Interface (MIDI)

# Session - 5

- The session layer protocols set up connections between applications, maintain dialog control, and negotiate, establish, maintain, and tear down the communication channel. Some of the protocols that work at this layer include:
  - Network File System (NFS)
  - NetBIOS
  - Structured Query Language (SQL)
  - Remote procedure call (RPC)

# Transport - 4

- The protocols at the transport layer handle end-to-end transmission and segmentation into a data stream. The following protocols work at this layer:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
  - Sequenced Packet Exchange (SPX)

# Network - 3

- The responsibilities of the network layer protocols include internetworking service, addressing, and routing. The following lists some of the protocols that work at this layer:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
  - Internet Group Management Protocol (IGMP)
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Novell Internetwork Packet Exchange (IPX)

# Data-Link - 2

- The protocols at the data link layer convert data into LAN or WAN frames for transmission, convert messages into bits, and define how a computer accesses a network. This layer is divided into the Logical Link Control (LLC) and the Media Access Control (MAC) sub layers. Some protocols that work at this layer include the following:
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)
  - Point-to-Point Protocol (PPP)
  - Serial Line Internet Protocol (SLIP)

# Data-Link

- Network interface cards and drivers convert bits into electrical signals and control the physical aspects of data transmission, including optical, electrical, and mechanical requirements. The following are some of the standard interfaces at this layer:
  - High-Speed Serial Interface (HSSI)
  - X.21
  - EIA/TIA-232 and EIA/TIA-449

# Physical Layer - 1

- The *physical layer*, layer 1, converts bits into voltage for transmission. Signals and voltage schemes have different meanings for different LAN and WAN technologies.
- Data  sent through dial-up software via a modem onto a telephone line, that data format, electrical signals, and control functionality are different to data  sent through a NIC and onto a unshielded twisted pair (UTP) wire for LAN communication.
- The mechanisms that control this data going onto the telephone line, or the UTP wire, work at the physical layer.
  - This layer controls synchronization, data rates, line noise, and transmission techniques.
  - Specifications for the physical layer include the timing of voltage changes, voltage levels, and the physical connectors for electrical, optical, and mechanical transmission.

# Functions and Protocols in the OSI Model

- **Application**
- The protocols at the application layer handle file transfer, virtual terminals, network management, and fulfilling networking requests of applications. A few of the protocols that work at this layer include
  - File Transfer Protocol (FTP)
  - Trivial File Transfer Protocol (TFTP)
  - Simple Network Management Protocol (SNMP)
  - Simple Mail Transfer Protocol (SMTP)
  - Telnet
  - Hypertext Transfer Protocol (HTTP)

# Functions and Protocols in the OSI Model

- **Presentation**
- The services of the presentation layer handle translation into standard formats, data compression and decompression, and data encryption and decryption. No protocols work at this layer, just services. The following lists some of the presentation layer standards:
  - American Standard Code for Information Interchange (ASCII)
  - Extended Binary-Coded Decimal Interchange Mode (EBCDIC)
  - Tagged Image File Format (TIFF)
  - Joint Photographic Experts Group (JPEG)
  - Motion Picture Experts Group (MPEG)
  - Musical Instrument Digital Interface (MIDI)

# Functions and Protocols in the OSI Model

- **Session**
- The session layer protocols set up connections between applications; maintain dialog control; and negotiate, establish, maintain, and tear down the communication channel. Some of the protocols that work at this layer include:
  - Network Basic Input Output System (NetBIOS)
  - Password Authentication Protocol (PAP)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Remote Procedure Call (RPC)

# Functions and Protocols in the OSI Model

- **Transport**
- The protocols at the transport layer handle end-to-end transmission and segmentation of a data stream. The following protocols work at this layer:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Sequenced Packet Exchange (SPX)

# Functions and Protocols in the OSI Model

- **Network**
- The responsibilities of the network layer protocols include internetworking service, addressing, and routing. The following lists some of the protocols that work at this layer:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
  - Internet Group Management Protocol (IGMP)
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Internetwork Packet Exchange (IPX)

# Functions and Protocols in the OSI Model

- **Data Link**
- The protocols at the data link layer convert data into LAN or WAN frames for transmission and define how a computer accesses a network. This layer is divided into the Logical Link Control (LLC) and the Media Access Control (MAC) sublayers. Some protocols that work at this layer include the following:
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)
  - Point-to-Point Protocol (PPP)
  - Serial Line Internet Protocol (SLIP)
  - Ethernet (IEEE 802.3)
  - Token Ring (IEEE 802.5)
  - Wireless Ethernet (IEEE 802.11)

# Functions and Protocols in the OSI Model

- **Physical**
- Network interface cards and drivers convert bits into electrical signals and control the physical aspects of data transmission, including optical, electrical, and mechanical requirements. The following are some of the standard interfaces at this layer:
  - RS/EIA/TIA-422, RS/EIA/TIA-423, RS/EIA/TIA-449, RS/EIA/TIA-485
  - 10Base-T, 10Base2, 10Base5, 100Base-TX, 100Base-FX, 100Base-T, 1000Base-T,1000Base-SX
  - Integrated Services Digital Network (ISDN)
  - Digital subscriber line (DSL)
  - Synchronous Optical Networking (SONET)

# Multilayer Protocol

- Not all protocols fit neatly within the layers of the OSI model e.g. devices and networks that were never intended to interoperate with the Internet.
  - Often lack robust security.
- SCADA (supervisory control and data acquisition) systems are vulnerable. Most SCADA systems use a multilayer protocol known as DNP3 which did not support networking.
- Rather than use the OSI seven-layer model, a simpler three-layer model was adopted - Enhanced Performance Architecture (EPA) that roughly corresponds to layers 2, 4, and 7 of the OSI model.
  - There was no encryption or authentication,

# TCP/IP

- Transmission Control Protocol/Internet Protocol is a suite of protocols that governs the way data travel from one device to another
- IP is a network layer protocol and provides datagram routing services
- IP's main task is to support internetwork addressing and packet routing
- TCP is a reliable and connection-oriented protocol
- It ensures packets are delivered to the destination computer

# TCP/IP

- TCP functions at the TRANSPORT Layer of the OSI Model
- IP functions at the NETWORK Layer of the OSI Model
- Two main protocols work at the **Transport** layer: **TCP** and **UDP**
  - TCP is a reliable and connection-oriented protocol
  - UDP is a best-effort and connectionless protocol

# TCP

- **TCP** is referred to as a connection-oriented protocol because:
- Before any data sent, a 3-Way handshake takes place between two systems that want to communicate
- Once handshake completes successfully a virtual connection is set up between hosts
- TCP has the ability to identify lost or corrupted packets
- TCP also supports packet sequencing and congestion controls

# UDP

- **UDP** is considered connectionless protocol because:
- No 3-Way handshake process
- UDP sends out messages without first contacting the destination computer and does not know if the packets were received properly or dropped

# TCP Handshake

- TCP must set up a virtual connection between two hosts before any data is sent
  - **The TCP Handshake**
- Both hosts must agree on certain parameters, data flow, windowing, error detection and options

1. The host that initiates communication sends a synchronous (SYN) packet to the receiver.
2. The receiver acknowledges this request by sending a SYN/ACK packet “I have received your request and am ready to communicate with you”
3. The sending host acknowledges this with an acknowledgment (ACK) packet “I received your acknowledgment Let’s start transmitting our data”

# IP Addressing

- Each node on the same network must have a unique IP address
- Most commonly used version of IP is IP version 4 (IPv4)
- IP addresses (IPv4) are limited and will run out in the next few years
- IP version 6 (IPv6) was created to address this shortage
- IPv4 uses 32 bits for its addresses
- IPv6 uses 128 bits for its addresses
- Each address has a host portion and a network portion
- Addresses are grouped into classes and then into subnets
- Subnet mask differentiates the groups of addresses that define the subnets of a network

# IP Addressing

- **IPv4 address classes: (Classful Network Addressing)**
- Class A 0.0.0.0 to 127.255.255.255
  - First Byte is Network
- Class B 128.0.0.0 to 191.255.255.255
  - First 2 Bytes are Network
- Class C 192.0.0.0 to 223.255.255.255
  - First 3 Bytes are Network
- Class D 224.0.0.0 to 239.255.255.255
  - Used for Multicast addresses
- Class E 240.0.0.0 to 255.255.255.255
  - Reserved for Research
- Classless Internet Domain Routing (CIDR) introduced to make more efficient use of IPv4 addresses

# Internet Protocol v6

- IPv6 has a larger address space than IPv4 to support more IP addresses
- 128 bit address
- It has other capabilities that IPv4 does not
- IPv6 allows for scoped addresses, which enables an administrator to restrict specific addresses for file servers or file and print sharing
- IPv6 has IPSec integrated into the protocol stack which provides end-to-end secure transmission and authentication.
- IPv6 offers auto-configuration which makes administration easier
- IPv6 does not require network address translation (NAT) to extend its address space

# IPv6 cont.

- IPv6 is an Internet Protocol (IP) for packet-switched internetworking that specifies the format of packets and the addressing scheme across multiple IP networks. In comparing the two protocols IPv6 expands upon the addressing and routing capabilities of IPv4 in a number of ways including:
  - In IPv6 the IP address size is increased from 32 bits to 128 bits
  - IPv6 supports a greater number of addressable nodes
  - IPv6 provides more levels of addressing hierarchy
  - IPv6 offers simpler auto-configuration of addresses
  - Ipv6 also supports simplified header format

# Layer 2 Security Standards

- As frames pass from one network device to another device, attackers could:
  - Sniff the data; modify the headers; redirect the traffic; spoof traffic; carry out man-in-the-middle attacks, DoS attacks, and replay attacks; and indulge in other malicious activities.
- Secure Network traffic at the frame level, which is layer 2 of the OSI model.
  - *802.1AE* is the IEEE MAC Security standard (MACSec), which defines a security
  - infrastructure to provide data confidentiality, data integrity, and data origin authentication.
- Where a virtual private network (VPN) connection provides protection at the higher networking layers, MACSec provides hop-by-hop protection at layer 2.
- MACSec integrates security protection into wired Ethernet networks to secure LAN-based traffic. Only authenticated and trusted devices on the network can communicate with each other.

# Data Transmission

- **Types of Transmission**
- Data transmission can happen in different ways (analog or digital)
- Can use different controlling schemes (synchronous or asynchronous)
- Can use either one channel over a wire (baseband)
- Can use several different channels over one wire (broadband)

# Data Transmission

- **Analog**
  - Analog transmission signals are continuously varying electromagnetic waves that can be carried over air, water, twisted-pair cable, coaxial cable, or fiber-optic cable
  - Difficult to extract analog signals from background noise because the amplitudes and frequency of the waves slowly lose form
  - Uses '**modulation**'
- **Modulation -** data are combined with a carrier signal of a specific frequency
  - modulation of a signal differs in;
    - amplitude (height of the signal)
    - frequency (number of waves in a defined period of time)
  - Example: Dial-Up Modems (**mod**ulate/**dem**odulate)

# Data Transmission

- **Digital**
  - Digital signals represent binary digits as electrical pulses
  - Digital signals are more reliable than analog signals over a long distance
  - Efficient signaling because voltage is either ON (1) or OFF (0)
  - Digital signals can easily be extracted from noise and retransmitted
  - Digital signal is a square wave
  - Digital systems are superior to analog systems in that they can transport more calls and data transmissions on the same line at higher quality over longer distance
  - Today most communication is digitized
- **Bandwidth** in digital transmissions refers to the number of electrical pulses that can be transmitted over a link within a second

# Data Transmission

- **Asynchronous and Synchronous**
  - Two devices can communicate through asynchronous or synchronous means, depending on the type of communication and whether the two systems are synchronized in any way
- **Asynchronous** communication is when two devices are not synchronized in any way
  - The sender can send data at any time, and the receiving end must always be ready
  - Data can travel at any time and be any length
  - Stop and Start delimiters must be used to tell the receiving end when to start processing a request and when to stop
- **Synchronous** communication takes place between two devices that are synchronized, usually via a clocking mechanism
  - Synchronous communication transfers data as a stream of bits
  - Clocking used to determine where each byte is in the data stream

# Data Transmission

- **Broadband and Baseband**
- **Baseband** uses the entire communication channel for its transmission
- **Broadband** divides the communication channel into individual and independent channels so different types of data can be transmitted simultaneously
  - CATV – Cable TV
  - ADSL

# Cables

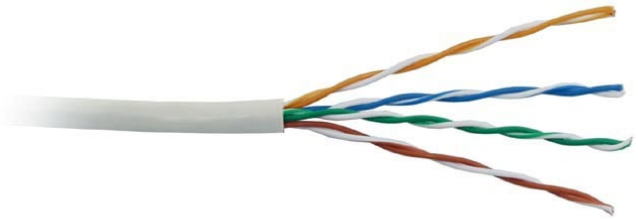
- **Coaxial Cable**
  - Copper core that is surrounded by a shielding layer and grounding wire
  - Encased within a protective outer jacket
  - More resistant to electromagnetic interference (EMI)
  - Provides a higher bandwidth
  - Supports the use of longer cable lengths
  - Can support Baseband or Broadband
  - Two main types of coaxial cable used within LAN environments
  - 50-ohm cable (used for digital signaling)
  - 75-ohm cable (used for high-speed digital signaling and analog signaling)

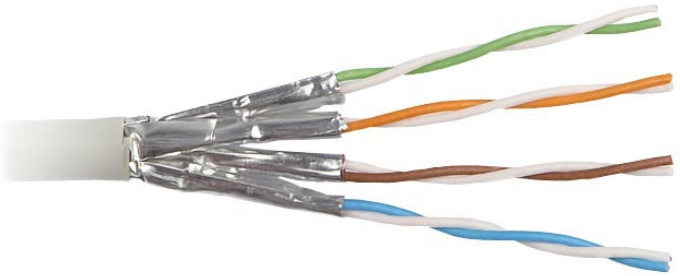
# Cables

- **Twisted-Pair Cable**
  - Insulated copper wires surrounded by an outer protective jacket
  - Copper wires that twist around each other
  - Twisting of the wires protects the signals from radio frequency and electromagnetic interference as well as crosstalk

# Cables

- **Twisted-Pair Cable**
  - Can have outer foil shielding (Shielded Twisted Pair (STP))
  - adds protection from radio frequency interference and electromagnetic interference.
  - Twisted-pair cabling without extra outer shielding is called (Unshielded Twisted Pair (UTP))



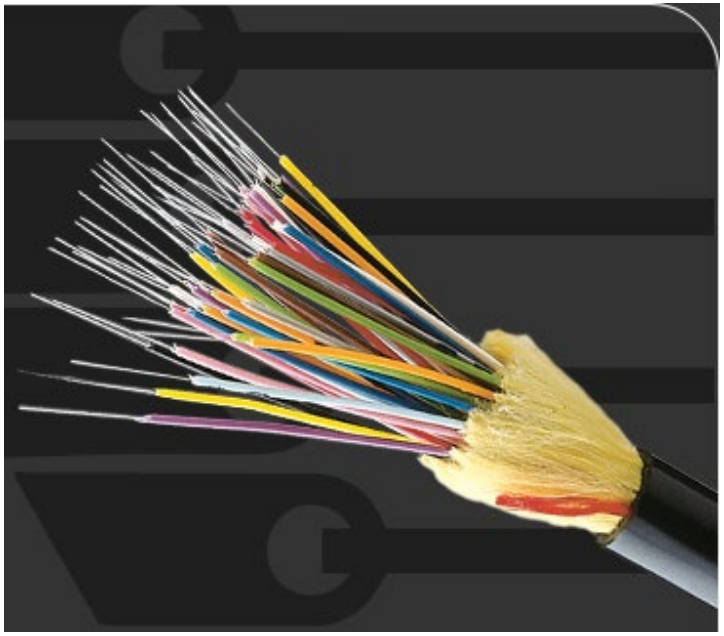


# Cables

- **Fiber-Optic Cable**
- Uses a type of glass that carries light waves
- Light waves represent the data being transmitted
- The glass core is surrounded by a protective cladding which in turn is encased within an outer jacket
- Higher transmission speeds that allow signals to travel over longer distances

# Cables

- **Fiber-Optic Cable**
- Not as affected by attenuation and EMI
- Does not radiate signals
- Difficult to eavesdrop
- Extremely expensive and difficult to work with
- Usually used in backbone networks



FANSHAWE

# Cabling Problems

- Cables are extremely important within networks, and when they experience problems, the whole network could experience problems
- **Noise**
  - Caused by surrounding devices or by characteristics of the wiring's environment. Noise can be caused by motors, computers, copy machines, fluorescent lighting, and microwave ovens
- **Attenuation**
  - Loss of signal strength as it travels
  - The longer a cable the more attenuation is introduced
  - Causes the signal carrying the data to deteriorate
- **Crosstalk**
  - Occurs when electrical signals of one wire spill over to another wire

# Wireless Communications

- Wireless communication involves transmitting signals via radio waves through air and space which alters airwaves
- Signals are measured in frequency and amplitudes
- The frequency of a signal dictates the amount of data that can be carried and how far
- The higher the frequency the more data the signal can carry

# Wireless Communications

- **Problem:**
- The higher the frequency the more susceptible the signal is to atmospheric interference
- A number of technologies have been developed to allow wireless devices to access and share this limited amount of medium for communication purposes
- Goal of each of these wireless technologies is to split the available frequency into usable portions

# Wireless Communications

## Spread Spectrum

- Something is distributing individual signals across the allocated frequencies
- Sender spreads its data across the frequencies over which it has permission to communicate
- More effective use of the available bandwidth because the sending system can use more than one frequency at a time
- Serial communications vs. Parallel (Parallel is faster because it transmits more at the same time)
- Two types of spread spectrum:
  - **Frequency hopping spread spectrum (FHSS)**
  - **Direct sequence spread spectrum (DSSS)**

# Wireless Communications

## Frequency hopping spread spectrum (FHSS)

- Takes the total amount of bandwidth (spectrum) and splits it into smaller sub- channels
- The sender and receiver work at one of these channels for a specific amount of time and then move to another channel
- The sender puts the first piece of data on one frequency, the second on a different frequency, and so on
- The FHSS algorithm determines the individual frequencies that will be used and in what order (referred to as **hop sequence**)
- Interference is a large issue in wireless transmissions because it can corrupt signals as they travel
- FHSS hopping between different frequencies reduces interference
- Hopping approach also makes it much more difficult for eavesdroppers

# Wireless Communications

## Direct sequence spread spectrum (DSSS)

- Applies sub-bits to a message
- The sub-bits are used by the sending system to generate a different format of the data before the data are transmitted
- The receiving end uses these sub-bits to reassemble the signal into the original data format
- The sub-bits are called “**chips**“and the sequence of how the sub-bits are applied is referred to as the “**chipping code**”
- Sender’s data are combined with the chip
- Anyone who does not know the chipping sequence signals appear as random noise

# Wireless Communications

## WLAN Components

- A wireless LAN (WLAN) uses a transceiver called an access point (AP) which connects to an Ethernet cable that links wireless devices to wired network
- APs are in fixed locations throughout a network and work as communication beacons
- When APs are used to connect wireless and wired networks this is called an "**infrastructure WLAN**"
- For a wireless device and AP to communicate they must be configured for the same channel
- Hosts that wish to participate in a particular WLAN must be configured with the proper **Service Set ID (SSID)**
- An "**ad hoc WLAN**" has no APs, the wireless devices communicate with each other through their wireless NICs instead of going through a centralized device

# Wireless Authentication

- Wireless device can authenticate to the AP in two main ways:
  - **Open System Authentication (OSA)**
  - **Shared Key Authentication (SKA)**
- **OSA** does not require cryptographic key, all transaction are sent in clear text
- All that's required is SSID
- **SKA** requires cryptographic key
- AP sends a random value to the wireless device
- Device encrypts this value with its cryptographic key and returns it
- This method is based on the **Wired Equivalent Privacy (WEP)** protocol

# Wireless Standards

- **Wireless Standards**
- Standards are developed so that many different vendors can create various products that will work together seamlessly
- Standards are usually developed on a consensus basis among the different vendors in a specific industry
- The Institute of Electrical and Electronics Engineers (IEEE) develops standards for a wide range of technologies including wireless

# Wireless Standards

- **IEEE802.11b**
  - This standard was the first extension to the 802.11 WLAN standard
  - 802.11b provides a transfer rate of up to 11 Mbps and works in the 2.4GHz frequency range
  - Uses DSSS and is backward-compatible with 802.11 implementations
- **IEEE802.11a**
  - Provides a transfer rate of up to 54 Mbps and works in the 5GHz frequency range
  - OFDM slits data over several narrow channels of different frequencies
  - Not compatible with 802.11b or 802.11g

# Wireless Standards

- **IEEE802.11e**
  - This standard provides QoS and support of multimedia traffic in wireless transmissions.
  - Multimedia and other types of time-sensitive applications have a lower tolerance for delays in data transmission.
- **IEEE802.11f**
  - For a user to move around in a WLAN, the device needs to communicate with different APs. An AP can cover only a certain distance, and as the user moves out of the range of the first AP, another AP needs to pick up and maintain the signal to ensure network connectivity is not lost.
  - The first AP would need to be able to convey this information to the second AP. The conveying of this information between the different APs during roaming is what 802.11f deals with.
- **IEEE802.11g**
  - The 802.11g standard provides for higher data transfer rates up to 54 Mbps
  - Speed extension for current 802.11b products
  - If a product meets the specifications of 802.11b and is based on 802.11g it is backward-compatible with older equipment
  - 802.11g works in the 2.4GHz range (increasingly crowded)

# Wireless Standards

## IEEE802.11h

- 802.11a works in the 5-GHz range, which is not necessarily available in every country, for this type of data transmission. The 802.11h standard builds upon the 802.11a specification to meet the requirements of European wireless rules so products working in this range can be properly implemented in European countries.

# Wireless Standards

- **IEEE802.11n**
- Replaces the current mix of various Wi-Fi technologies
- 802.11n is designed to be much faster with throughput at 100 Mbps, and it works at the same frequency range of 802.11a (5GHz)
- Intent is to maintain some backward-compatibility with current Wi-Fi standards
- This standard uses a concept called multiple input, multiple output (MIMO) to increase the throughput
- This will necessitate the use of two receive and two transmit antennas to broadcast in parallel using a 20MHz channel

# Wireless Standards

- **IEEE802.11ac**
- The IEEE 802.11ac WLAN standard is an extension of 802.11n. It also operates on the 5-GHz band, but increases throughput to 1.3 Gbps.
- 802.11ac is backward compatible with 802.11a, 802.11b, 802.11g and 802.11n, but if in compatibility mode it slows down to the speed of the slower standard.
- Another benefit of this newer standard is its support for *beamforming*, which is the shaping of radio signals to improve their performance in specific directions. In simple terms, this means that 802.11ac is better able to maintain high data rates at longer ranges than its predecessors.

# Wireless Standards

- **Bluetooth Wireless**
- Bluetooth wireless technology is actually a portion of the 802.15 standard
- It has a 1 to 3 Mbps transfer rate and works in a range of approximately ten meters
- Bluetooth works in the frequency range of other 802.11 devices (2.4GHz)
- Real security risks exist when transferring unprotected data via Bluetooth in a public area, because any device within a certain range can capture this type of data transfer
- Attacks:
  - **Bluejacking** - someone sends an unsolicited message to a device that is Bluetooth-enabled

# Wireless

- **WLAN Best practices:**
- Change default SSID
- Disable “broadcast SSID” on the AP
- Implement another layer of authentication (RADIUS, Kerberos)
- Physically put the AP at the center of the building
- Logically put the AP in a DMZ with a firewall between the DMZ and internal network.
- Allow the firewall to investigate the traffic before it gets to the wired network

# Wireless

- **WLAN Best practices:**
- Implement VPN for wireless devices to use. This adds another layer of protection for data being transmitted
- Configure the AP to allow only known MAC addresses into the network
- Assign static IP addresses to wireless devices and disable DHCP. If an attacker gains access and DHCP is enabled, you have just given the attacker a valid working IP address to use
- Carry out penetration tests on the WLAN

# Satellites

- For two different locations to communicate via satellite links, they must be within the satellite's line of sight and *footprint* (area covered by the satellite).
- The sender of information (ground station) modulates the data onto a radio signal that is transmitted to the satellite. A transponder on the satellite receives this signal, amplifies it, and relays it to the receiver.
- The receiver must have a type of antenna, dish-like. The antenna contains one or more microwave receivers, depending upon how many satellites it is accepting data from.

# Mobile Wireless Communications

- A device that can send voice and data over wireless radio links. It connects to a cellular network, which is connected to the PSTN.
- A cellular network distributes radio signals over delineated areas, called cells. Each cell has at least one fixed-location transceiver (base station) and is joined to other cells to provide connections over large geographic areas.

# Mobile Wireless Communications

- Multiple Access technologies allow for a finite number of radio frequencies to be employed:
- Frequency division multiple access (FDMA)
  - The available frequency range is divided into sub-bands (channels), and one channel is assigned to each subscriber (cell phone).
- Time division multiple access (TDMA)
  - increases the speed and efficiency of the cellular network by taking the radio-frequency spectrum channels and dividing them into time slots. At various time periods, multiple users can share the same channel; the systems within the cell swap from one user to another user, in effect, reusing the available frequencies.
- Code division multiple access (CDMA)
- Orthogonal frequency division multiple access (OFDMA)

# Mobile Wireless Communications

- Code division multiple access (CDMA)
  - CDMA assigns a unique code to each voice call or data transmission to uniquely identify it from all other transmissions sent over the cellular network. In a CDMA “spread spectrum” network, calls are spread throughout the entire radio-frequency band. CDMA permits every user of the network to simultaneously use every channel in the network. At the same time, a particular cell can simultaneously interact with multiple other cells.

- Orthogonal frequency division multiple access (OFDMA)
  - Each of the channels is subdivided into a set of closely spaced orthogonal frequencies with narrow bandwidths (sub channels).
  - Each of the different sub channels can be transmitted and received simultaneously in a multiple input, multiple output (MIMO) manner.
  - The use of orthogonal frequencies and MIMO allows signal processing techniques to reduce the impacts of any interference between different sub-channels and to correct for channel impairments, such as noise and selective frequency fading. 4G requires that OFDMA be used.

# Mobile Technology Generations

**First generation (1G):**
- Analog services
- Voice service only

**Second generation (2G):**
- Primarily voice, some low-speed data (circuit switched)
- Phones were smaller in size
- Added functionality of e-mail, paging, and caller ID

**Generation 2½ (2.5G):**
- Higher bandwidth than 2G
- “Always on” technology for e-mail and pages

**Third generation (3G):**
- Integration of voice and data
- Packet-switched technology, instead of circuit-switched

**Generation 3.5 G (3GPP)**
- Higher data rates
- Use of OFDMA technology

**Fourth generation (4G)**
- Based on an all-IP packet-switched network
- Data exchange at 100 Mbps to 1 Gbps

# Network Foundations

FANSHAWE

# LAN Networking

- **LAN Networking**
- The following are the four main reasons to have a network:
  - To allow communication between computers
  - To share information
  - To share resources
  - To provide central administration

# Network Topology

- **LAN Media Access Technologies**
  - A LAN is a network that provides shared communication and resources in a relatively small area
  - The term “local” in the context of a LAN refers to the limitations of a LAN and the number of devices and computers that can be connected to it
  - Poorly designed LAN’s can have performance limitations
  - Administration of poorly designed large LAN’s can be a nightmare
  - Errors, Collisions and Security Holes
  - These limitations are defined by the data link layer protocols

# Network Topology

- The physical arrangement of computers and devices is called a network topology
- **Topology** refers to the manner in which a network is physically connected and shows the layout of resources and systems
- Network can be configured as a physical star but work logically as a ring as in the Token Ring technology

# Network Topology

- **Ring Topology**
  - A ring topology has a series of devices connected by unidirectional transmission links
  - These links form a closed loop and do not connect to a central system
  - Physical ring formation
  - Each node is dependent upon the preceding nodes

# Network Topology

- **Bus Topology**
  - Single cable runs the entire length of the network
  - Nodes are attached to the network through drop points on this cable
  - Data communications transmit the length of the medium
  - Each packet transmitted has the capability of being “looked at” by all nodes
  - Each node decides to accept or ignore the packet
  - If one workstation fails other systems can be negatively affected
  - Cable itself becomes a potential single point of failure
  - Ethernet uses bus and star topologies.
- Two main types: Linear and Tree
  - The linear bus topology has a single cable with nodes attached.
  - A tree topology has branches from the single cable, and each branch can contain many nodes

# Network Topology

- **Star Topology**
  - All nodes connect to a central device such as a switch
  - Each node has a dedicated link to the central device
  - Central device can be a bottleneck to network performance
  - Central device is a single point of failure
  - One Workstation failure does not affect network or other workstations
  - Star topology typically requires less cabling

# Network Topology

- **Mesh Topology**
  - All systems and resources are connected to each other
  - This arrangement is usually a network of interconnected routers and switches that provides multiple paths to all the nodes on the network
  - Full mesh topology every node is directly connected to every other node
  - Provides a great degree of redundancy
- The Internet is an example of a partial mesh topology

# Media Access Technologies

- **Media Access Technologies**
  - Rules how systems and devices communicate over media and are usually represented in protocols, NIC drivers, and interfaces
  - Rules how errors are handled
  - Rules what physical medium is to be used
  - Rules that define the maximum transmission unit (MTU) which is the size of frames

# Token Ring

- Token Ring is a LAN technology originally developed by IBM and is now defined by the IEEE 802.5 standard
- It uses a token-passing technology with a star-configured topology
- Ring is a logical ring
- Each computer is connected to a central hub called a Multistation Access Unit (MAU)

# Token Ring

- A token-passing technology is one in which a device cannot put data on the network wire without having possession of a token
- A Token is a control frame that travels in a logical circle and is “picked up” when a system needs to communicate
- Token Ring does not have collisions unlike Ethernet
- Maximum Transmission Speed 4Mbps later upgraded to 16Mbps

# Token Passing (1)

- A token is a 24-bit control frame used to control which computers communicate at what intervals
- Token is passed from computer to computer
- The computer that has the token can actually put frames onto the wire
- Token grants a computer the right to communicate
- Token contains the data to be transmitted and source and destination address information
- Computer then connects its message to the token and puts it on the wire

# Token Passing (2)

- Each computer checks this message to determine whether it is addressed to it
- Destination computer makes a copy of the message and flips a bit to tell the source computer it did indeed get its message
- Destination computer makes a copy of the message, but only the originator of the message can remove the message from the token and the network

# Collision Detection/Avoidance

- **Collision Domains**
  - A collision occurs on Ethernet networks when two computers transmit data at the same time
  - The more devices on a contention-based network the more likely collisions will occur
  - Collisions increase network latency (data transmission delays)
  - A '**collision domain**' is a group of computers that are contending, or competing, for the same shared communication medium
  - High collisions can be caused by a highly populated network, or
    - Damaged cable or connector
    - Too many repeaters
    - Cables that exceed the recommended length

# Collision Detection/Avoidance

- '**Contention**' means that the nodes have to compete for the same shared medium.
- '**Collision**' happens when two or more frames collide, which most likely corrupts both frames
- Nodes will execute a random collision timer to force a delay before they attempt to transmit data
- This random collision timer is called the '**back-off algorithm**'

# Collision Detection/Avoidance

- There are two distinct types of CSMA: CSMA/CD and CSMA/CA
  - Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- **CSMA/CD**
  - Hosts or devices monitor the transmission activity, or carrier activity on the wire so they can determine when would be the best time to transmit data
  - Each node monitors the wire continuously and waits until the wire is free before it transmits its data
  - If two computers transmit data at the same time contention and a collision can take place

# Collision Detection/Avoidance

- **CSMA/CA**
  - Access method in which each computer signals its intent to transmit data before it actually does so
  - Systems listen to the shared medium to determine whether it is busy or free
  - Once a node determines it can put its data on the wire it sends out a broadcast to all other systems telling them it is going to transmit information
  - Each system will wait a period of time before attempting to transmit data
- **Example:**
  - 802.11 WIFI uses CSMA/CA for its media access

# Polling

- In an environment where a *polling* LAN media access and sharing method is used, some systems are configured as primary stations and others are configured as secondary stations.
  - At predefined intervals, the primary station asks the secondary station if it has anything to transmit. This is the only time a secondary station can communicate.
- Polling is a method of monitoring multiple devices and controlling network access transmission. If polling is used to monitor devices, the primary device communicates with each secondary device in an interval to check its status. The primary device then logs the response it receives and moves on to the next device. If polling is used for network access, the primary station asks each device if it has something to communicate to another device. Network access transmission polling is used mainly with mainframe environments.

# Ethernet

- Ethernet is a LAN-sharing technology that enables several devices to communicate on the same network
- Ethernet usually uses a bus or star topology
- Ethernet has seen quite an evolution from purely coaxial cable installations to Twisted Pair cabling
- Ethernet Bandwidth ranges from 10 Mbps, 100 Mbps, 1,000 Mbps (1 Gbps) and 10 Gbps

# Ethernet

- Shared media
- Uses broadcast and collision domains
- Uses the carrier sense multiple access with collision detection (CSMA/CD) access method
- Supports full duplex on twisted-pair implementations
- Can use coaxial or twisted-pair media
- Is defined by standard IEEE 802.3

# Ethernet

- Ethernet runs at 10 Mbps over twisted-pair
  - CAT3
  - Ethernet uses the traditional CSMA/CD
- **Fast Ethernet**
  - Fast Ethernet is regular Ethernet except that it runs at 100 Mbps over twisted-pair
  - CAT5
  - Fast Ethernet uses the traditional CSMA/CD
  - **10GBase-T 10 Gigabit Ethernet** allows the transmitting at a rate of 10 gigabits per second. It was first defined by the IEEE 802.3ae-2002 standard. It is only full-duplex point-to-point links which are generally connected by network switches.

# Ethernet 10BaseT

- Uses twisted-pair copper wiring instead of coaxial cabling
- Twisted-pair wiring uses one wire to transmit data and the other to receive data Implemented in a star topology
- All systems are connected to centralized devices
- Use RJ-45 connector faceplates to which the computer connects.
- Wires usually run behind a wall and connect the faceplate to a punchdown block within a wiring closet
- The punchdown block is often connected to a 10Base-T hub that serves as a doorway to the network's backbone cable or to a central switch

# FDDI

- **Fiber Distributed Data Interface** (FDDI) technology, developed by the American National Standards Institute (ANSI)
- High-speed token-passing media access technology with maximum speed of 100 Mbps
- Typically used as backbone network using fiber-optic cabling
- Provides fault tolerance by using a second counter-rotating fiber ring

# FDDI

- Primary ring has data traveling clock-wise and is used for regular data transmission
- The second ring transmits data in a counterclockwise fashion and is invoked only if the primary ring goes down
- IEEE Standard 802.8

# Network Protocol and Services

## Address Resolution Protocol

- Each computer and network device requires a unique IP address and a unique physical hardware address
- Each NIC has a unique physical address that is programmed into the ROM chips on the card by the manufacturer
- Physical address is called the Media Access Control (MAC) address
- MAC and IP addresses must be properly mapped so they can be correctly resolved This happens through the Address Resolution Protocol (ARP)
- The data link layer works with and understands physical MAC addresses

# ARP

- **Why is ARP important?**
  - When a piece of Data starts at the application layer encapsulation process
  - Moves it down to the transport layer for sequence numbers and session establishment
  - Then data is passed to the network layer for routing information like source and destination IP addresses
  - Then it moves down to the data link layer which adds MAC address to the header
  - When frame hits the wire it is routed based on MAC address
  - If a computer cannot resolve the IP address passed down from the network layer to the corresponding MAC address it cannot communicate with other hosts

# ARP

- **Why is ARP important?**
  - MAC and IP addresses must be properly mapped so they can be correctly resolved
  - This happens through the Address Resolution Protocol (ARP)
  - When data link layer receives a frame the network layer has already attached the destination IP address to it
  - The problem is data link layer cannot understand IP address and thus invokes ARP for help

# DHCP

- **Dynamic Host Configuration Protocol**
  - A computer be assigned an IP address in different ways
    1. Assigned statically
    2. Assigned dynamically by Dynamic Host Configuration Protocol (DHCP) server
  - At boot up host makes a request to the DHCP server
  - The DHCP server assigns the IP address from a preconfigured pool of addresses

# DHCP

- **DHCP Process**
  - Client computer broadcasts a DHCPDISCOVER message on the network in search of the DHCP server
  - DHCP server receives the DHCPDISCOVER request and responds with a DHCPOFFER packet offering the client an IP address
  - Client receives Server's DHCPOFFER
  - Client responds with a DHCPREQUEST packet confirming it accepted
  - DHCP Server now acknowledges with a DHCPACK packet which includes validity period (lease) for given IP address

# ICMP

- **Internet Control Message Protocol**
  - Internet Control Message Protocol (ICMP) is IP's "messenger boy"
  - ICMP delivers status messages
  - ICMP Reports errors
  - ICMP replies to certain requests
  - ICMP reports routing information
  - ICMP is used to test connectivity and troubleshoot problems on IP networks
- Most common use of ICMP is through the PING utility
- Testing connectivity to another system can be achieved by sending ICMP ECHO REQUEST frames
- ICMP ECHO REPLY frames are sent

# Simple Network Management Protocol

- **Simple Network Management Protocol** (**SNMP**) used for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers.
- SNMP is used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.
- Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

# DNS

- **Domain Name Service**
- The Domain Name Service (DNS) is a method of resolving hostnames to IP addresses so names can be used instead of IP addresses when referencing unique hosts on the Internet
- DNS namespaces are split up administratively into zones
- DNS server that holds the files for one of these zones is said to be the authoritative name server for that particular zone
- DNS server contains records that map hostnames to IP addresses which are referred to as resource records
- Recommended that a primary and a secondary DNS server be placed in each zone
- Primary and Secondary DNS servers synchronize their information through a zone transfer

# DNS

- **Internet DNS and Domains**
- Networks on the Internet are connected in a hierarchical structure
- If one DNS server does not know which DNS server holds the necessary resource record to resolve a hostname, it can pass the request up to a DNS server above it
- Naming scheme of the Internet resembles an inverted tree with the root servers at the top

# DNS

- **Internet DNS and Domains**
- Lower branches of this tree are divided into top-level domains
  - COM Commercial
  - EDU Education
  - MIL U.S. military organization
  - INT International treaty organization
  - GOV Government
  - ORG Organizational
  - NET Networks

# Directory Services

- A directory service has a hierarchical database of users, computers, printers, resources, and attributes of each
- The directory is mainly used for lookup operations
- Enables users to track down resources and other users easily to facilitate access
- Most directory service databases are built on the X.500 model

# Directory Services

- Use Lightweight Directory Access Protocol (LDAP) to access the directory database
- Directory itself uses classes of objects and subclasses
- Each directory follows a specific schema
- Schema provides structure to the directory repository and defines how objects and their relationships are to be represented
- Two examples of directory services are Microsoft Active Directory and Novell Directory Services (NDS)

# Directory Services

- **Lightweight Directory Access Protocol**
- Lightweight Directory Access Protocol (LDAP) is a client/server protocol used to access network directories such as Microsoft Active Directory or NDS
- LDAP specification works with directories that organize their database in a hierarchical tree structure
- LDAP tree has leaves (entries) with unique distinguished names (DNs)
- DN names are hierarchical and describe the object's place within the tree
- Entries can define network resources, computers, people, wireless devices, and more
- Attributes are like the columns in a relational database and provide descriptive information about the entry

# E-mail Services - SMTP

- SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. It is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server.

- Users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.

# E-mail Services

- *Post Office Protocol (POP)* is an Internet mail server protocol that supports incoming and outgoing messages. A mail server that uses POP, apart from storing and forwarding e-mail messages, works with SMTP to move messages between mail servers.
- *Internet Message Access Protocol (IMAP)* is also an Internet protocol that enables users to access mail on a mail server.
- IMAP is a store-and-forward mail server protocol. It also gives administrators more capabilities when it comes to administering and maintaining the users' messages.

# E-mail Security

- **E-mail Relaying**
- Sending legitimate or forged email through a 3rd party email server
- Sometimes companies need to implement different types of mail servers and services within the same network, which can become a bit overwhelming and a challenge to secure
- Mail servers in the DMZ are in this protected space because they are directly connected to the Internet
- These servers should be tightly locked down and their relaying mechanisms should be correctly configured
- DMZs that have loosely configured relaying mechanisms and use these computers to send their spam

# E-mail Threats

- It is very easy to spoof e-mail messages, which means to alter the name in the From field
- This type of activity is rampant today, and has become more of a social-engineering tactic. Another variant is referred to as **phishing**
- Phishing is the act of sending spoofed messages that pretend to originate from a source the user trusts and has a business relation with (Think Fake Online Banking Notices)
- Companies that regard security as one of their top priorities should implement an e-mail protection application that can digitally sign messages, like Pretty Good Privacy (PGP), or use a public key infrastructure (PKI)

# Network Address Translation

- **Network address translation** (**NAT**) allows the remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
- One Internet-routable IP address of a NAT gateway can be used for an entire private network.
- The following lists current private IP address ranges:
  - 10.0.0.0–10.255.255.255 Class A networks
  - 172.16.0.0–172.31.255.255 Class B networks
  - 192.168.0.0–192.168.255.255 Class C networks

# Network Address Translation

Three basic types of NAT implementations can be used:

- **Static mapping** The NAT software has a pool of public IP addresses configured. Each private address is statically mapped to a specific public address.
- **Dynamic mapping** The NAT software has a pool of IP addresses, but instead of statically mapping a public address to a specific private address, it works on a first-come, first-served basis.
- **Port address translation (PAT)** One public IP address for all systems that need to communicate outside the internal network is used.
  - When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number.

# Routing Protocols

- Individual networks on the Internet are referred to as autonomous systems (ASs)
- These ASs are independently controlled by different corporations and organizations
- An AS is made up of routers which are administered by a single entity and use a common Interior Gateway Protocol (IGP) within the boundaries of the AS
- The Internet is just a network made up of ASs and routing protocols
- Routing protocols can be dynamic or static

# Routing Protocols

- A dynamic routing protocol can discover routes and build a routing table
  - Routers use these tables to make decisions on the best route for the packets they receive
- A dynamic routing protocol can change the entries in the routing table based on changes that take place to the different routes
- When a router finds out that a route has gone down or is congested it sends an update message to other routers around it
- A static routing protocol requires the administrator to manually configure the router's routing table

# Routing Protocols

- **Route flapping** refers to the constant changes in the availability of routes
- **Black hole** a router does not receive an update that a link has gone down and continue to forward packets to that route
- Two main types of routing protocols are used:
  - **Distance-vector**
  - **Link-state routing**

# Routing Protocols

- **Distance-vector**
  - Distance-vector routing protocols make their routing decisions based on the distance (or number of hops) and a vector (a direction)
  - Distance-vector routing protocol use an algorithm to determine the best route for a packet
- **Link-state routing**
  - Link-state routing protocols build a more accurate routing table
  - They build a topology database of the network
  - Look at more variables than just the number of hops between two destinations
  - Use packet size, link speed, delay, loading, and reliability as the variables in their algorithms to determine the best routes for packets to take

# RIP

- Routing Information Protocol
  - RIP is a standard that outlines how routers exchange routing table data and is considered a distance-vector protocol
- It calculates the shortest distance between the source and destination
- Considered a legacy protocol because its slow performance and lack of functionality
- Should only be used in small networks
- RIP version 1 has no authentication
- RIP version 2 sends passwords in clear text or hashed with MD5

# OSPF: Open Shortest Path First

- Uses link-state algorithms to send out routing table information
  - These algorithms allow for smaller more frequent routing table updates
- Provides a more stable network than RIP
- Requires more memory and CPU resources to support this extra processing
- OSPF has a hierarchical routing network that has a backbone link connecting all subnets together
- OSPF has replaced RIP in many networks
- Authentication can take place with clear text passwords or hashed passwords

# Interior Gateway Routing Protocol - GRP

- Interior Gateway Routing Protocol (IGRP)
- Distance-vector routing protocol that was developed by Cisco Systems
- Proprietary protocol used only by Cisco devices
- IGRP uses five criteria to make a “best route” decision
- Network administrator can set weights on these different metrics so that the protocol works best in that specific environment
- No longer promoted by Cisco
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Cisco routing protocol
- Some features of link state

# Homework

- Read the relevant chapter (first half) in the set book ‘All In One CISSP Exam Guide’ – by Shon Harris.

- Communication & Network Security
- Go through the Quick Tips at the end of the chapter

- Then identify and do the practice m/c questions relating to this subject, these will either be at the end of the chapter if you are using the current edition or spread between different chapters in earlier editions.

# Questions

- ?