

**CISSP® Common Body of Knowledge
Review:**

**Telecommunications &
Network Security Domain –
Part 1**

Version: 5.9.2



CISSP Common Body of Knowledge Review by Alfred Ouyang is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Learning Objectives

Telecommunications & Network Security Domain – Part 1

“The Telecommunications and Network Security domain encompasses the structures, techniques, transport protocols, and security measures used to provide integrity, availability, confidentiality, and authentication for transmissions over private and public communication networks.”

“The candidate is expected to demonstrate an understanding of communications and network security as it relates to data communications in local area and wide area networks, remote access, internet/intranet/extranet configurations. Candidates should be knowledgeable with network equipment such as switches, bridges, and routers, as well as networking protocols (e.g., TCP/IP, IPSec,) and VPNs.”

Telecommunications & Network Security Domain – Part 1



Security Principles & Internet Protocol (IP) Architecture

- Terms & Definitions
 - Types of Data Network Structure
 - Methods & Modes of Data Network Communications
 - Types of Data Networks
 - Types of Data Networks Topology
- OSI Reference Model and TCP/IP Model
 - Physical Layer (Layer 1)
 - Data-Link Layer (Layer 2)
 - Network Layer (Layer 3)
 - Transport Layer (Layer 4)
 - Session Layer (Layer 5)
 - Presentation Layer (Layer 6)
 - Application Layer (Layer 7)

Telecommunications & Network Security Domain – Part 2

“The candidate is expected to demonstrate an understanding of communications and network security as relates to data communications in local area and wide area networks; remote access; Internet/intranet/extranet configurations, use of firewalls, network equipment and protocols (such as TCP/IP), VPNs, and techniques for preventing and detecting network based attacks.”

Reference: *CISSP CIB*, January 2012 (Rev. 2)

Telecommunications & Network Security Domain – Part 2

- Security Principles & Network Architecture
- Security Countermeasures and Controls
 - Physical Layer
 - Data-Link Layer
 - IP Network Layer
 - Transport Layer
 - Application Layer

Security Objectives

- Confidentiality
 - “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.” (44 USC Sec. 3542)
 - Network access control & data transport encryption, and network security protocols.
- Integrity
 - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.” (44 USC Sec. 3542)
 - Firewall, IDS, IPS Services, and network security management.
- Availability
 - “Ensuring timely and reliable access and use of information.” (44 USC Sec. 3542)
 - Fault tolerant network & services, and reliable network transport.

Security Implementation Principles

- Confidentiality, Integrity, Availability
- Need-to-know
 - Users should only have access to information (or systems) that enable them to perform their assigned job functions.
- Least privilege
 - Users should only have sufficient access privilege that allow them to perform their assigned work.
- Separation of duties
 - No person should be responsible for completing a task involving sensitive, valuable or critical information from the beginning to end.
 - No single person should be responsible for approving his/her own work.

Law, Regulations, and Policies:

- FISMA, SOX, GBL, National Security Act, USA PATRIOT ACT, etc.
 - OMB A-130, A-11, etc.
 - E.O. 13292, 12968, etc.
 - DoD 5200.1-R, etc.

Security Objectives:

- Confidentiality
 - Integrity
 - Availability

Standards and Best Practices

- NIST FIPS, SP 800-x, etc.
- COBIT, ITIL, Common Criteria
- ISO/IEC 27001, 21827, etc.
 - DoDI 8500.2, 8510.01

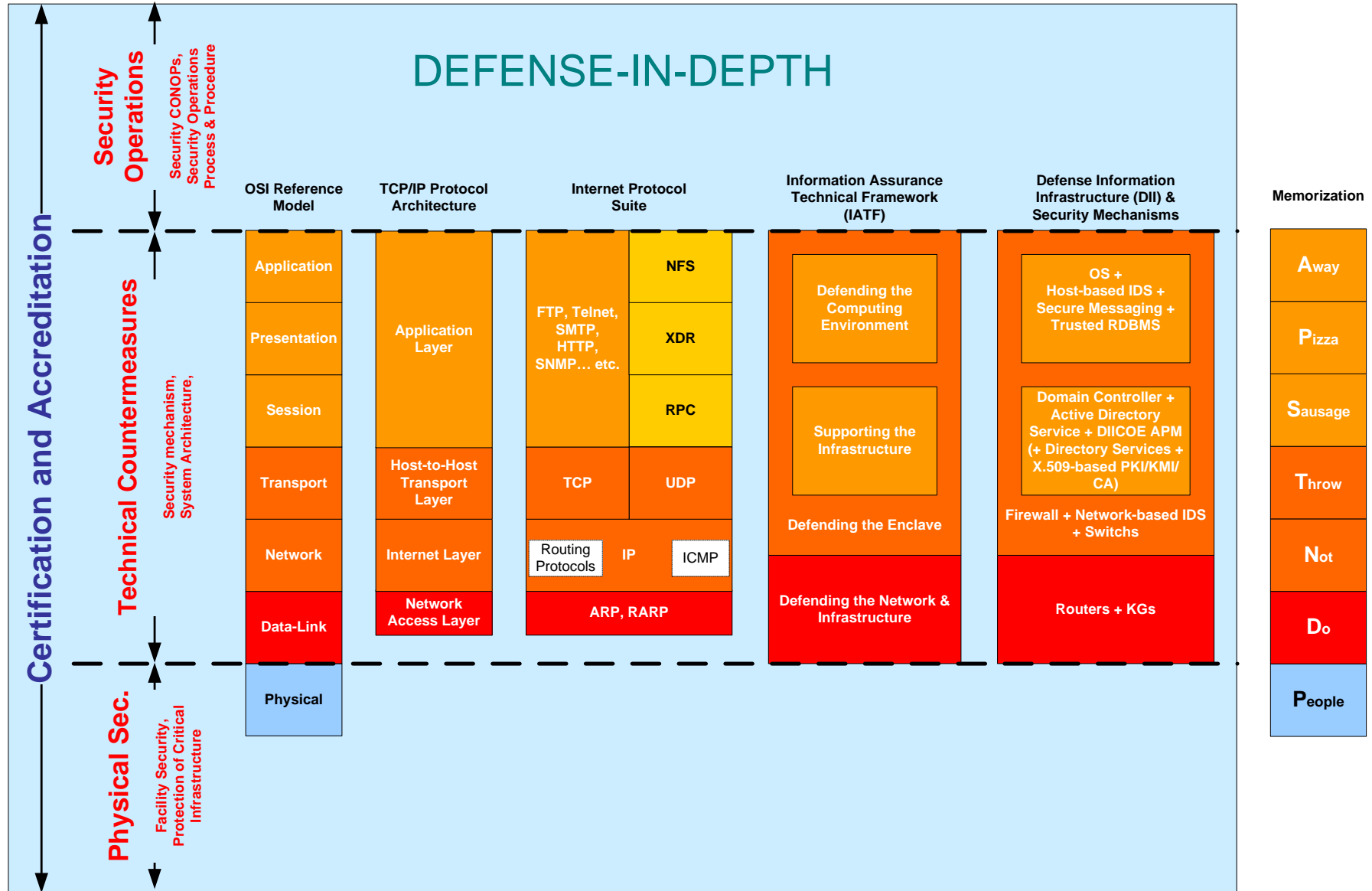
Security Implementation Principles:

- Confidentiality, Integrity, Availability
 - Need-to-Know
 - Least Privilege
 - Separation of Duties

Benchmarks and Guidelines:

- NIST National Checklist, DISA STIGs, CIS Benchmarks, etc.

OSI Reference Model & TCP/IP Protocol Architecture



Telecommunications & Network Security Domain – Part 1

- Security Principles & Internet Protocol (IP) Architecture



Terms & Definitions

- Types of Data Network Structure
 - Methods & Modes of Data Network Communications
 - Types of Data Networks
 - Types of Data Networks Topology
- OSI Reference Model and TCP/IP Model
 - Physical Layer (Layer 1)
 - Data-Link Layer (Layer 2)
 - Network Layer (Layer 3)
 - Transport Layer (Layer 4)
 - Session Layer (Layer 5)
 - Presentation Layer (Layer 6)
 - Application Layer (Layer 7)

Types of Data Network Structures

- Local Area Network (LAN). Primarily limited to a small geographical area or a single site (i.e. an office building).
- Personal Area Network (PAN). Data communications network for short distance (e.g. Bluetooth, Infra-Red).
- Wide Area Network (WAN). Data communications network to multiple long range geographic area.
- Metropolitan Area Network (MAN). Data communications network for a large city (e.g. Washington Metropolitan, New York City, or Boston, etc.)
- Campus Area Network. Data communications network for a campus of buildings (e.g. college campus, military base)
- Internet. Worldwide system of interconnected networks.
- Intranet. A type of network that services internal clients (/users) over diverse range of telecommunication networks.
- Extranet. A type of network that services to external clients (/customers) over diverse range of telecommunication networks.

Methods & Modes of Data Network Communications

- Methods of Data Network Communications
 - Analog Communications. A method of internetworking utilizing analog signal through combination of signal amplitude, frequency, and phase. (e.g. voice, fax, modem, analog radio, etc.)
 - Digital Communications. A method of internetworking utilizing digital signal through binary of 1/0s.
- Modes of Data Network Communications
 - Synchronous Communications. A mode of communication relying on a set of synchronized clocking systems to determine sender and receiver communication signals.
 - Asynchronous Communications. A mode of communication controlled by a set of start & stop bits at each end of data signals (headers & footers) to discretize pieces of data. (i.e. encapsulation)

Types of Data Network

- Circuit-switched network. Data is sent through a dedicated circuit between two endpoints. (e.g. public switched telephone network (PSTN))
- Packet-switched network. Data is segmented into packets and sent across a circuit shared by multiple subscribers.
 - Virtual circuit. Data is sent through a logical circuit created over a packet-switched network.
 - Switched virtual circuit (SVC).
 - Permanent virtual circuit (PVC).

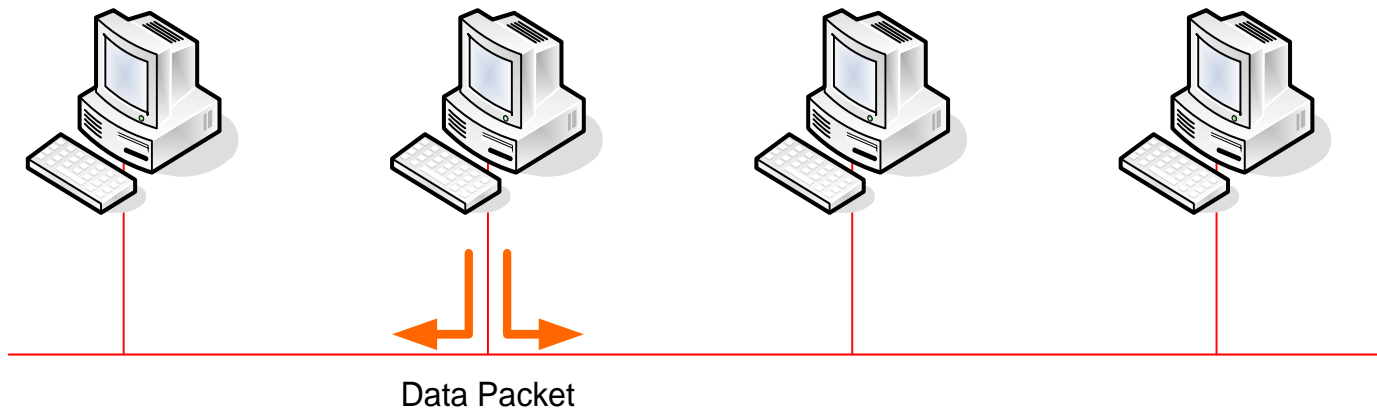
Types of Data Networks Topology

There are five types of physical network topologies:

- Bus Topology
- Tree Topology
- Star Topology
- Ring Topology
- Mesh Topology

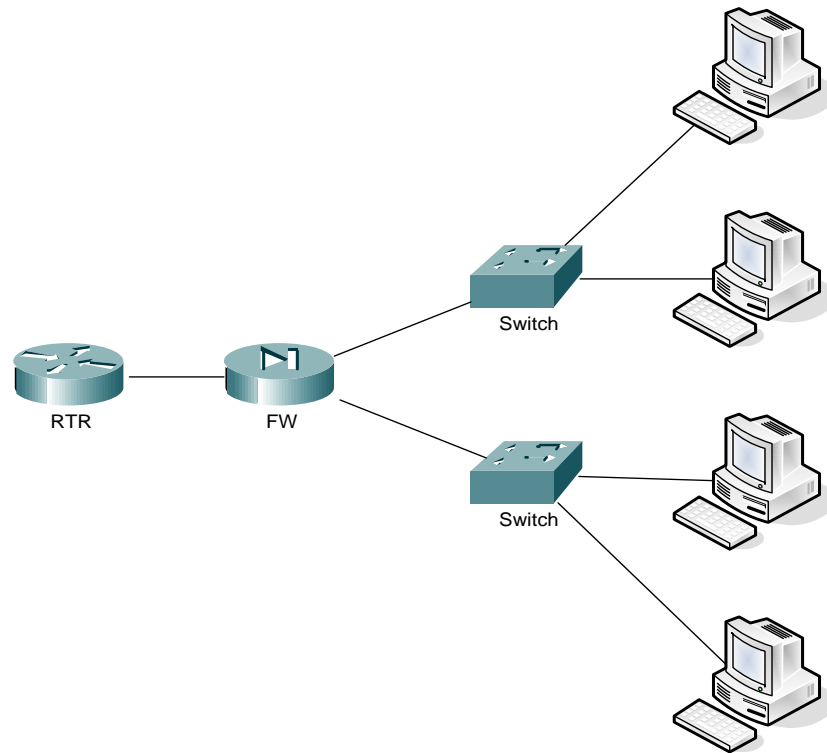
Types of Data Networks Topology – Bus Topology

- Bus Topology – Each device handles its own communications control. A bus is low cost and widely used in the start of PC era. (e.g. Thick-, Thin-Ethernet, and AppleTalk)



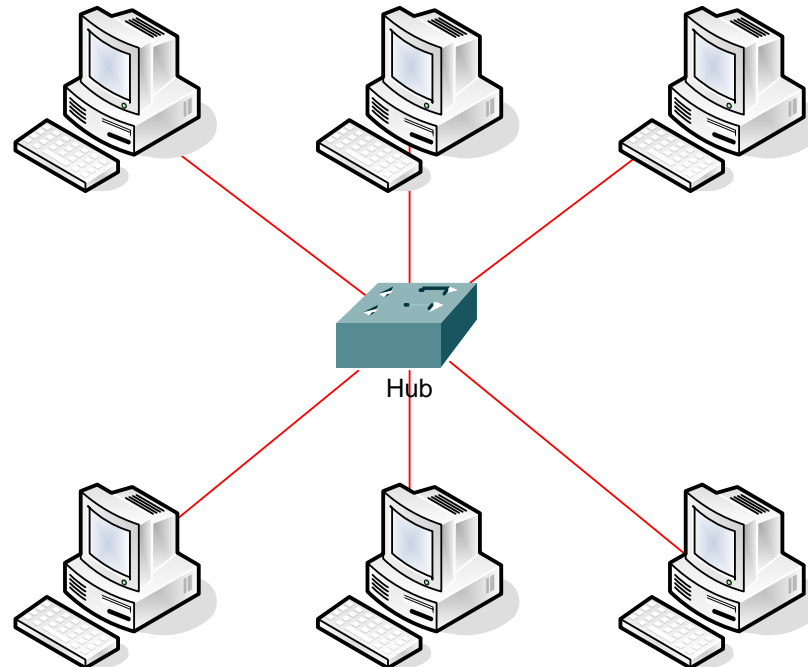
Types of Data Networks Topology – Tree Topology

- **Tree Topology** – Is a generalized bus topology. Tree root is the head-end. Cable starts at the head-end, each of which can have many branches. Branches may have additional branches which can form a complex structure.



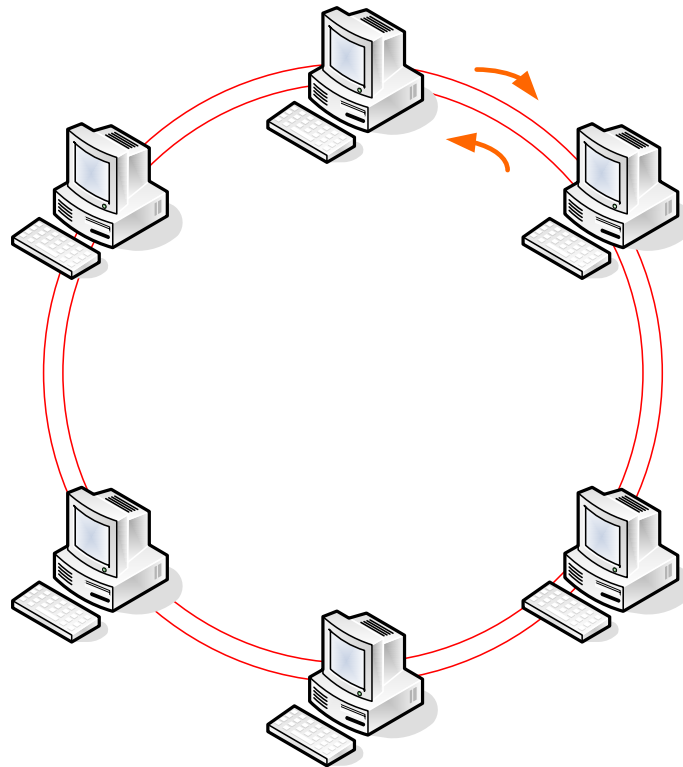
Types of Data Networks Topology – Star Topology

- Star Topology – Nodes are connected to a single host. All communications pass through this host which is usually a large mainframe or a network hub.



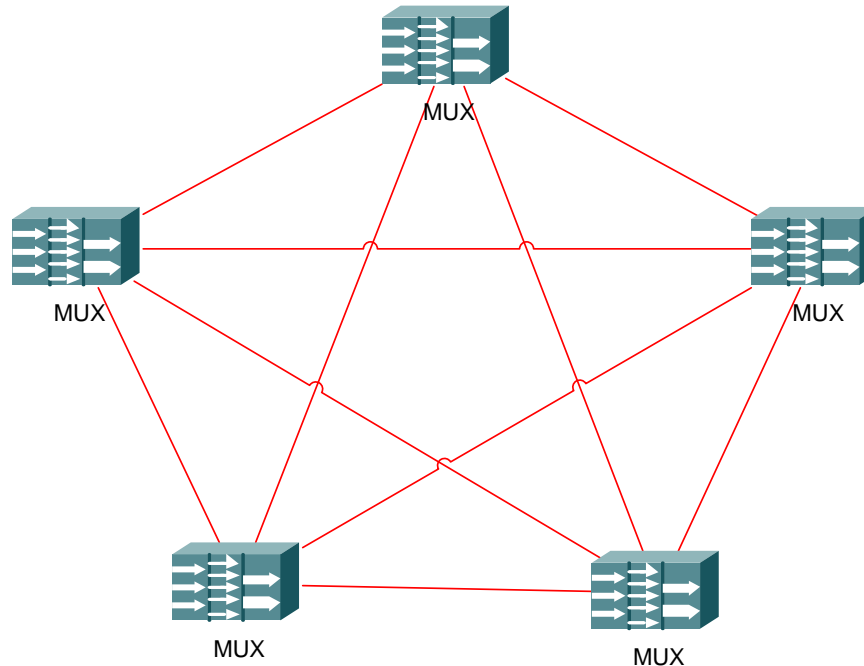
Types of Data Networks Topology – Ring Topology

- Ring Topology – A ring topology has all the network nodes connected by a unidirectional transmission link to form a closed loop. FDDI and Token Ring use this topology.



Types of Data Networks Topology – Mesh Topology

- Mesh Topology – A mesh topology has all the network nodes connected to each other. Network can be full mesh or partial mesh.
- Number of connections for a full mesh network = $n(n-1) / 2$.



Questions:

- Name the type of network is used primarily for short distance data communication?
–
- Name the type of network is used primarily for data communications at an office building?
–
- Name the type of network is used for data communications between multiple long range geographic area?
–

Answers:

- Name the type of network is used primarily for short distance data communication?
 - Personal Area Network (PAN)
- Name the type of network is used primarily for data communications at an office building?
 - Local Area Network (LAN)
- Name the type of network is used for data communications between multiple long range geographic area?
 - Wide Area Network (WAN)

Questions:

- A type of network that services to internal clients (/users) over diverse range of networks & services?
–
- A type of network that services to external clients (/customers) over diverse range of networks & services?
–
- What type of network topology has all the network nodes connected to each other?
–

Answers:

- A type of network that services to internal clients (/users) over diverse range of networks & services?
 - Intranet
- A type of network that services to external clients (/customers) over diverse range of networks & services?
 - Extranet
- What type of network topology has all the network nodes connected to each other?
 - Meshed Topology

Questions:

- What are the five types of physical network topologies?
 -
 -
 -
 -
 -
- What are two methods of data network communications?
 -
 -
- What are two modes of data network communications?
 -
 -

Answers:

- What are the five types of physical network topologies?
 - Bus Topology
 - Tree Topology
 - Star Topology
 - Ring Topology
 - Mesh Topology
- What are two methods of data network communications?
 - Analog
 - Digital
- What are two modes of data network communications?
 - Synchronous
 - Asynchronous

Telecommunications & Network Security Domain – Part 1

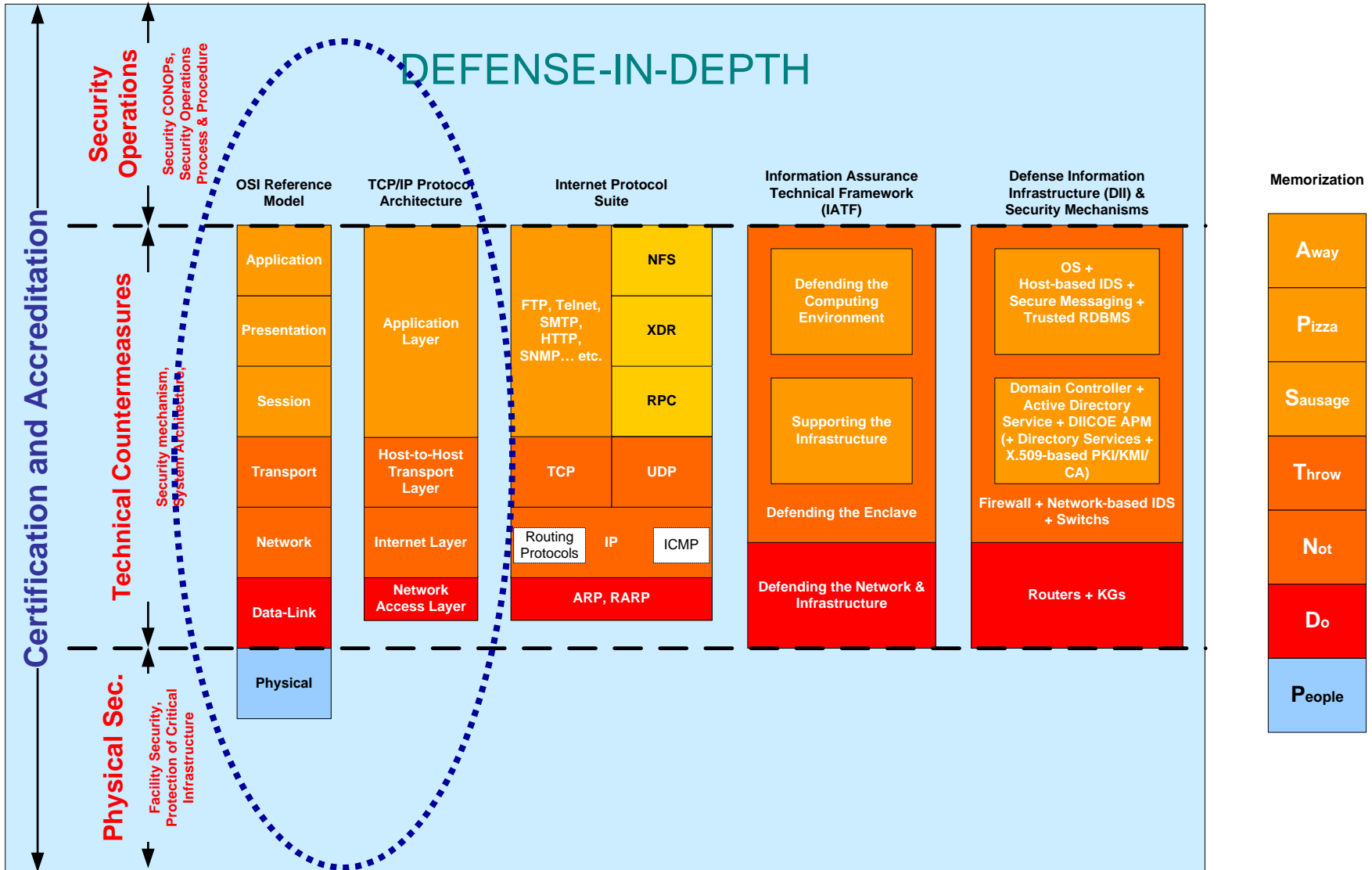
- Security Principles & Internet Protocol (IP) Architecture
- Terms & Definitions
 - Types of Data Network Structure
 - Methods & Modes of Data Network Communications
 - Types of Data Networks
 - Types of Data Networks Topology



OSI Reference Model and TCP/IP Model

- Physical Layer (Layer 1)
- Data-Link Layer (Layer 2)
- Network Layer (Layer 3)
- Transport Layer (Layer 4)
- Session Layer (Layer 5)
- Presentation Layer (Layer 6)
- Application Layer (Layer 7)

OSI Reference Model & TCP/IP Protocol Architecture

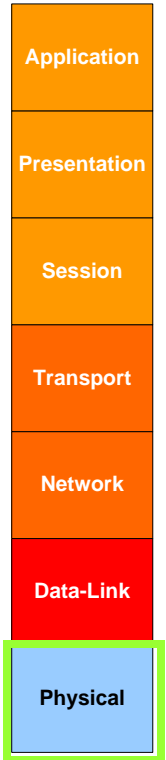


Physical Layer (Layer 1)

- Physical layer concerns the physical interface between devices and the rules by which bits are passed between devices.
 - Mechanical, Electrical, Functional, Procedural
 - Physical layer has two responsibilities sending and receiving bits.
- Examples of Cabling:
 - Twisted Pair
 - Coaxial Cable
 - Fiber Optical



OSI Reference Model



Network Cabling

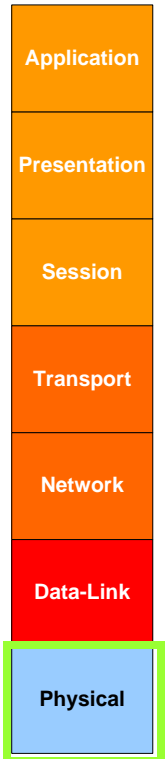
- Twisted Pair

- Inexpensive and very easy to install
- Consists of two copper wires twisted together which reduces electrical interference. Can be shielded or unshielded.
- Shielded is more expensive but has less crosstalk and more resistant to EMI.
- Can be used for analog or digital transmissions.
- Can be used up to 100 Mbps

- Six levels:

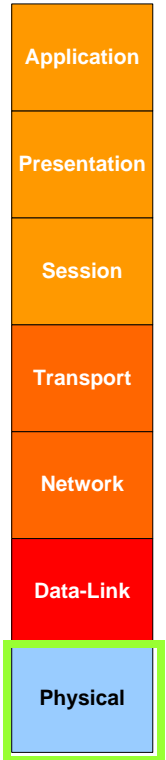
- Category 1: Analog and digital voice
- Category 2: ISDN and medium-speed data up to 4 Mbps
- Category 3: High-speed data and LAN traffic up to 10 Mbps
- Category 4: LAN traffic up to 16 Mbps
- Category 5: 100-Mbps UTP LAN technologies
- Category 5e: Enhanced performance spec. for CAT5
- Category 6: Gigabit Ethernet (1000-Mbps) and 10-Gigabit Ethernet

OSI Reference Model



Network Cabling

OSI Reference Model



- Coaxial Cable

- Provides a good combination of high bandwidth and excellent noise immunity but is more expensive.
- Two transmission methods are Baseband and Broadband.
 - Baseband carries only a single channel.
 - Broadband carries multiple channels, i.e. video, voice and data.

- Fiber Optics

- Fiber optic cable carries signals as light waves creating higher transmission speeds and greater distances.
- Very difficult to tap and is the most resistant to interference.
- Usually reserved for connections between backbone and devices in large networks.

Network Cabling

Media Type	Max Distance	Bandwidth	Advantages	Disadvantages
Thicknet Coax	500 meters	10 Mbps	Less susceptible to EMI than other copper media.	Difficult to work with and expensive.
Thinnet Coax	185 meters	10 Mbps	Less expensive than Thicknet or fiber; easy to install.	Limited bandwidth, limited application, damage to cable can bring down the network.
Shield Twisted Pair (STP)	100 meters	10 Mbps	Reduced cross talk. More resistant to EMI than UTP and thinnet.	Difficult to work with and more expensive than UTP.
CAT 3 UTP	100 meters	10 Mbps	Least expensive of all media.	Limited bandwidth, used primarily for voice.
CAT 5 UTP	100 meters	100 Mbps	Easy to use and widely available.	Susceptible to interference can only cover a limited distance.
Fiber – Multimode	2 kilometers	100 Mbps – 100Gbps	Support multiple transmissions, covers great distances, difficult to tap.	Expensive and difficult to terminate.

RF Network – International Telecommunication Union (ITU)

Radio Regulations

Band name	Abbr	ITU	Frequency	Wavelength	Example uses
Extremely low frequency	ELF	1	3 - 30 Hz	10,000 – 100,000 km	deeply-submerged submarine communication
Super low frequency	SLF	2	30 - 300 Hz	1000 – 10,000 km	submarine communication, AC power grids
Ultra low frequency	ULF	3	300 - 3 kHz	100 – 1000 km	earth quakes, earth mode communication
Very low frequency	VLF	4	3 - 30 kHz	10 – 100 km	near-surface submarine communication
Low frequency	LF	5	30 - 300 kHz	10 – 10 km	navigation, time signals, AM longwave broadcasting
Medium frequency	MF	6	300 - 3000 kHz	100 – 1000 m	AM broadcasts
High frequency	HF	7	3 - 30 MHz	10 – 100 m	Skywave long range radio communication
Very high frequency	VHF	8	30 - 300 MHz	1 – 10 m	FM radio broadcast, television broadcast, DVB-T, MRI
Ultra high frequency	UHF	9	300 - 3 GHz	10 – 100 cm	microwave oven, television broadcast, GPS, mobile phone communication (GSM, UMTS, 3G, HSDPA), cordless phones (DECT), WLAN (Wi-Fi), Bluetooth
Super high frequency	SHF	10	3 - 30 GHz	1 – 10 cm	DBS satellite television broadcasting, WLAN (Wi-Fi), WiMAX, radars
Extremely high frequency	EHF	11	30–300 GHz	1 – 10 mm	directed-energy weapon (Active Denial System), Security screening (Millimeter wave scanner), intersatellite links, WiMAX, high resolution radar

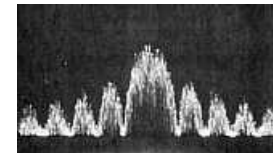
Reference: http://en.wikipedia.org/wiki/ITU_Radio_Bands

RF Network – Microwave

- Microwaves are electromagnetic waves:
 - Frequencies: 300MHz – 300GHz
 - Includes: ultra high frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF).
 - Wave lengths: 1 mm to 1 meter
- Usually used for:
 - Wide area communications: Satcom, TV broadcasts, etc.
 - Metropolitan area communications: [IEEE 802.16 \(WiMAX\)](#), cellular communications
 - Local area communications: [IEEE 802.11 a/b/g](#), etc.
 - Personal area communications: [Bluetooth](#)
- Line of sight (LOS) communication technology
 - Signal relay over long distance: land, sea, space.
 - Operating constrains: Ice, snow, heavy rain, and dust storm, solar flare, strong electro-magnetic interference (EMI), high altitude electro-magnetic pulse (HEMP), etc.

RF Network – Spread Spectrum

- Spread-spectrum is a communication method that spreads (or distributes) one or more discrete frequencies in time or frequency domains
- Two types of multiplex methods:
 - Circuit – Constant bandwidth
 - Statistical – Variable bandwidth
- Two popular methods:
 - Direct-sequence spread spectrum (DSSS)
 - Example: GPS, CDMA, IEEE 802.11b/g
 - Frequency-hopping spread spectrum (FHSS)
 - Example: TDMA – GSM, Dynamic TDMA – Bluetooth, IEEE 802.11a, IEEE 802.16a (WiMax)
 - Note: IEEE 802.11 uses both methods



RF Network – 3G Wireless Communications

- 3G – 3rd Generation
- International Mobile Telecommunications-2000 (IMT-2000) is the global standard for 3G wireless communications
- IMT-2000 specified six radio interfaces:
 - *IMT-DS* Direct-Sequence (a.k.a. W-CDMA)
 - *IMT-MC* Multi-Carrier (a.k.a. CDMA2000)
 - *IMT-TD* Time-Division (TD-CDMA and TD-SCDMA)
 - *IMT-SC* Single Carrier (a.k.a. EDGE)
 - *IMT-FT* Frequency Time (a.k.a. DECT)
 - *IMT-OFDMA TDD WMAN* (a.k.a. WiMAX)

RF Network – IEEE 802.11

- IEEE 802.11a
 - Operates in “open” 5 GHz band
 - Uses a 52-subcarrier orthogonal frequency-division multiplexing (OFDM)
 - Maximum data rate of 54 Mbps
 - Usually used as line-of-sight (LOS) RF communication, because of poor multi-path capability (5 GHz band)

- IEEE 802.11b/g
 - Operates in “open” but heavily used 2.4 GHz band. (e.g. cordless phones, Bluetooth, microwave oven, etc.)
 - Better multi-path capability (i.e. reflection)
 - 802.11b: 11 Mbps and 802.11g: 54 Mbps
 - 802.11b uses Direct-sequence spread spectrum (DSSS, a variation of CDMA)
 - 802.11g uses OFDM, so it’s just as fast as 802.11a

RF Network – Bluetooth

- Bluetooth is a RF network communications protocol design primarily for low power consumption
 - Operates in the open 2.4GHz band
 - Uses frequency-hopping spread spectrum (FHSS)
 - Bluetooth operating range are based on three power classes:

Class	Maximum Power mW (dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~ 100 meters
Class 2	2.5 mW (4 dBm)	~ 10 meters
Class 3	1 mW (0 dBm)	~ 1 meter

- Data rate varies:
 - Bluetooth 1.2: 1Mbit/sec.
 - Bluetooth 2.0 + EDR: 3 Mbit/sec.
- Usually used for personal area network (PAN) devices:
 - Hands-free headset for cell phones, mouse, keyboard, and printers
 - Game consoles: Nintendo Wii, Sony PlayStation 3

Questions:

- What are the two transmission methods for coaxial cable?
 -
 -
- What are the two modes of transmission for fiber optic cable?
 -
 -
- What are the two popular methods for spread spectrum radio frequency communications?
 -
 -

Questions:

- What are the two transmission methods for coaxial cable?
 - Baseband (single channel)
 - Broadband (multiple channels)
- What are the two modes of transmission for fiber optic cable?
 - Single-mode (single light spectrum)
 - Multi-mode (multiple light spectrums)
- What are the two popular methods for spread spectrum radio frequency communications?
 - Direct-sequence spread spectrum (DSSS)
 - Frequency-hopping spread spectrum (FHSS)

Telecommunications & Network Security Domain – Part 1

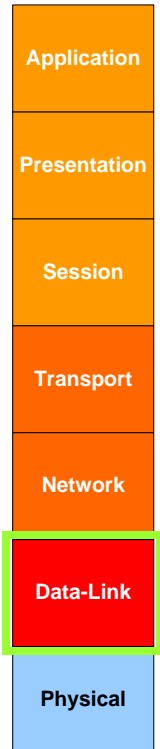
- Security Principles & Internet Protocol (IP) Architecture
- Terms & Definitions
 - Types of Data Network Structure
 - Methods & Modes of Data Network Communications
 - Types of Data Networks
 - Types of Data Networks Topology
- OSI Reference Model and TCP/IP Model
 - Physical Layer (Layer 1)
 - Data-Link Layer (Layer 2)
 - Network Layer (Layer 3)
 - Transport Layer (Layer 4)
 - Session Layer (Layer 5)
 - Presentation Layer (Layer 6)
 - Application Layer (Layer 7)



Data-Link Layer (Layer 2)

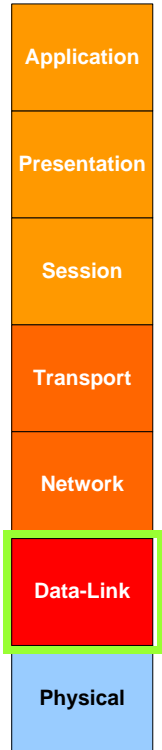
- Data-link layer defines the protocol that computers must follow in order to access the network for transmitting and receiving messages.
 - Protocols that control LAN transmission are:
 - MAC (Media Access Control)
 - LLC (Logical Link Control)
 - Popular protocols that control WAN transmissions are:
 - X.25
 - Frame Relay
 - ISDN (Integrated Services Digital Network)
 - SDLC (Synchronous Data Link Control)
 - HDLC (High-level Data Link Control)
 - ATM (Asynchronous Transfer Mode)
 - HSSI (High Speed Serial Interface)

OSI Reference Model



Media Access Control (MAC)

OSI Reference Model



- Data-Link layer addressing or a physical hardware address (MAC) is an unique address that is burned into each NIC card by the manufacturer
 - The hardware address is a 48-bit address expressed as 6 bytes. The first 3 bytes are the vendor code and the second 3 bytes are the serial numbers made up by the manufacturer
 - MAC sub-layer is responsible for media access. It controls how the workstations communicate over the network.
 - There are generally three types of media access.
 - Carrier Sense Multiple Access (CSMA)
 - Token Passing
 - Polling

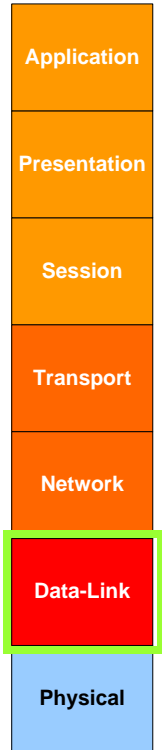


MAC Address of a NIC: **00-0F-1F-C1-21-B8**

Logical Link Control (LLC)

- The Logical Link Control (LLC) runs between the Network Layer (Layer 3) and MAC sub-layer
- Enables the network layer and physical layers to act independently. Network layer uses IP addresses and physical layer uses MAC addresses

OSI Reference Model

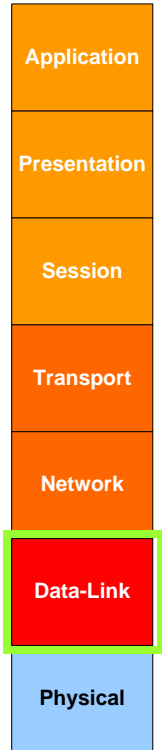


Media Access Methods

Three types of media access methods are used by packets to access the physical network medium:

- Carrier Sense Multiple Access (CSMA)
 - Carrier Sense: When an internetworking device connected to a network. It first checks to make sure the network interface has a carrier on which to send its data
 - Multiple Access: All internetworking devices on the network are free to use the network whenever they like so long as no one else is transmitting
 - With Collision Avoidance (CSMA/CA)
 - With Collision Detection (CSMA/CD)
- Polling
- Token Passing

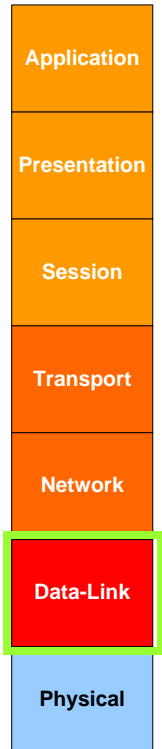
OSI Reference Model



CSMA/CD

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
 - Requires that all devices on the LAN listen before they transmit. This contention method is often known as Ethernet
 - If two devices transmit at the same time, a collision occurs
 - After the collision, devices on the LAN will wait a random amount of time before retransmitting data

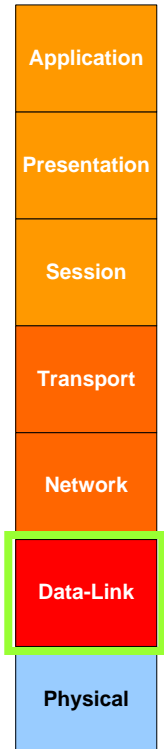
OSI Reference Model



CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
 - CSMA/CA is a network contention protocol that listens to a network in order to avoid collisions
 - Contributes to network traffic because, before any real data is transmitted, it has to broadcast a signal onto the network in order to listen for collision scenarios and to tell other devices not to broadcast
 - Example of CSMA/CA is IEEE 802.11b RF Network

OSI Reference Model



Polling & Token Passing

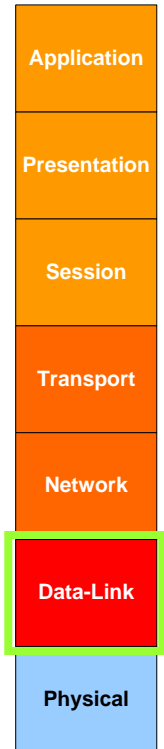
- Polling

- Primary station checks a secondary station regularly at predetermined times to see if it has data to transmit.
- Secondary stations are not permitted to transmit until given permission from the primary
- Used in large mainframe environments
- Polling is very inexpensive.

- Token Passing

- Stations in token passing networks cannot transmit unless they receive a special frame called a token.
- If the node does not have anything to transmit, it passes the token to the next station.
- Token Ring and IEEE 802.5 are examples of token passing networks
- Deterministic, transmission delay predictable, and robust

OSI Reference Model

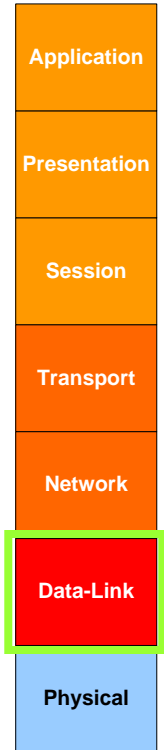


Wide Area Network (WAN)

- Circuit Switching

- Circuit-switching is a type of network switching in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection
- Ordinary voice phone service is circuit-switched.
- The telephone company reserves a specific physical path to the number you are calling for the duration of your call. During that time, no one else can use the physical lines involved
- Example: ISDN (Integrated Services Digital Network)

OSI Reference Model

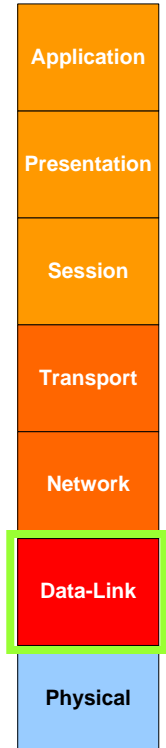


Wide Area Network (WAN)

- Packet Switching

- Packet-switching describes the type of network in which relatively small units of data called packets are routed through a network based on the destination address contained within each packet
- Breaking communication down into packets allows the same data path to be shared among many users in the network.
- Example: X.25, Frame Relay

OSI Reference Model

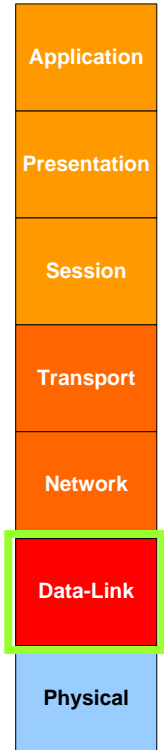


Wide Area Network (WAN)

- Virtual Circuit

- A virtual circuit is a circuit or path between points in a network that appears to be a discrete, physical path but is actually a managed pool of circuit resources from which specific circuits are allocated as needed to meet traffic requirements
- Permanent virtual circuit (PVC) – A PVC is a virtual circuit that is permanently available to the user just as though it were a dedicated or leased line continuously reserved for that user
- Switched Virtual Circuit. (SVC) – A SVC is a virtual circuit in which a connection can be dynamically established.

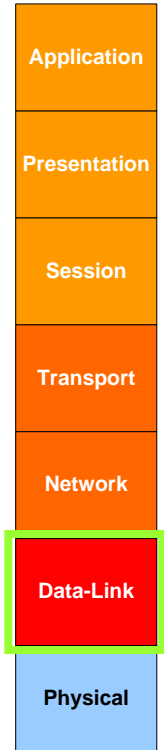
OSI Reference Model



WAN Protocols

- X.25
 - X.25 is a protocol standard that defines how WAN connections between user devices and network devices are established, maintained, and effectively operate
 - X.25 devices include DTEs, DCEs, and PSTNs. X.25 connections contain both SVCs and PVCs within the physical circuit
- Frame Relay
 - Frame relay is an upgrade from X.25 and a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model
 - Frame relay achieves high throughput with low delay by eliminating the overhead of error detection and correction

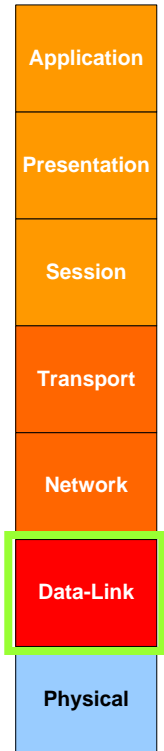
OSI Reference Model



WAN Protocols

- ISDN (Integrated Services Digital Network) is a world-wide standard for transmitting voice, video, data, or packets over the PSTN (public switched telephone network)
 - Carriers offers 2 types of services:
 - BRI (Basic Rate Interface)
 - 2 x 64kbps B channels for user data
 - 1 x 16kbps D channel for control & mgmt. signals
 - 144 kbps
 - PRI (Primary Rate Interface)
 - 23 x 64kbps B channels for user data
 - 1 x 64k bps D channel for control & mgmt. signals
 - 1.54 Mbps
 - B Channel = Bearer Channel (for user data)
 - D Channel = Data Channel (for control & mgmt signals)

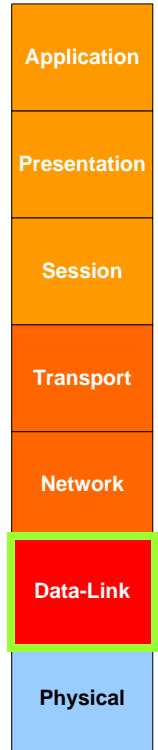
OSI Reference Model



WAN Protocols

- Asynchronous Transfer Mode (ATM)
 - ATM is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Requires a high speed medium like fiber optics
 - Carriers offer 4 types of services:
 - CBR (Constant Bit Rate)
 - VBR (Variable Bit Rate)
 - UBR (Unspecified Bit Rate)
 - ABR (Available Bit Rate)

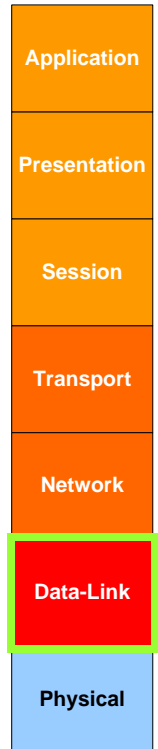
OSI Reference Model



WAN Protocols

- Synchronous Data Link Control (SDLC).
 - IBM developed the Synchronous Data Link Control (SDLC) protocol in the mid-1970's for use in Systems Network Architecture (SNA) environments. SDLC was the first link layer protocol based on synchronous, bit-oriented operation
- HDLC.
 - High-level Data Link Control (HDLC) was derived from SDLC.
 - HDLC specifies the data encapsulation method on synchronous serial links using frame characters and checksums.
- HSSI.
 - High Speed Serial Interface (HSSI) is a DTE/DCE interface that was developed by Cisco Systems.
 - Physical layer of the standard is defined by EIA-613 and EIA-612.

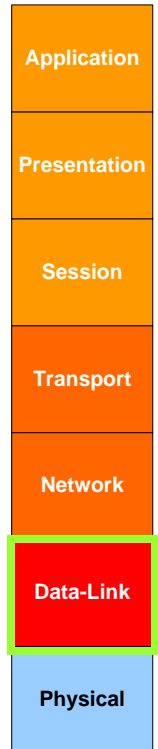
OSI Reference Model



Wireless Protocols

- WAP (Wireless Application Protocol)
 - For internetworking between IP and Cellular service.
 - WAP is a protocol suite from Data-Link to Application layers.
- Cellular
 - TDMA (Time Division Multiple Access). Supports data transmission
 - CDMA (Code Division Multiple Access). Supports data transmission
 - GSM (Global System for Mobile communications). Supports data transmission using GPRS (General Packet Radio Services)
- IEEE 802.11 a/b/g
 - Beacon frame announce its presence and provide Service Set Identification (SSID).

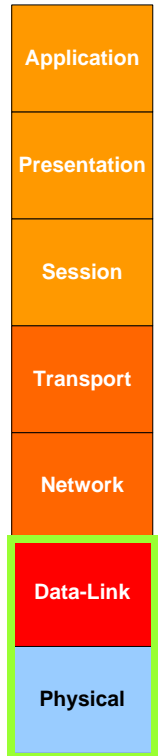
OSI Reference Model



Common Digital Network Services

- T Carrier Signals
 - T-1: 24 x voice or data channels
 - T-3: 672 voice or data channels
 - Typically used in large organizations to ISP
- ISDN (Integrated Services Digital Network)
 - BRI (Basic Rate Interface)
 - PRI (Primary Rate Interface)
- DSL (Digital Subscriber Line)
 - Unlike ISDN, DSL is an “always on” digital service
 - ADSL (Asymmetric DSL): uplink speed \neq downlink speed
 - SDSL (Symmetric DSL): uplink speed = downlink speed
- Frame Relay
 - A packet switched-based shared WAN service. Originally designed for ISDN, now it is also used in T-1, T-3 circuit switched network services
- ATM (Asynchronous Transfer Mode)
 - Cell Relay service (based on 53-Bytecells)
 - multiplex voice, video and data
- SONET (Synchronous Optical Network)
 - Up to 129k channels on a single fiber cable

OSI Reference Model



T Carrier Signal Levels vs. Digital Signal Levels

- Digital Signal (DS) Levels (e.g. DS-1, DS-3) defines the electrical characteristics of T-1 signal
- T Carrier Signals Levels (e.g. T1, T3), in U.S. uses Time Division Multiplexing (TDM) defining the speed and number of voice and data channels

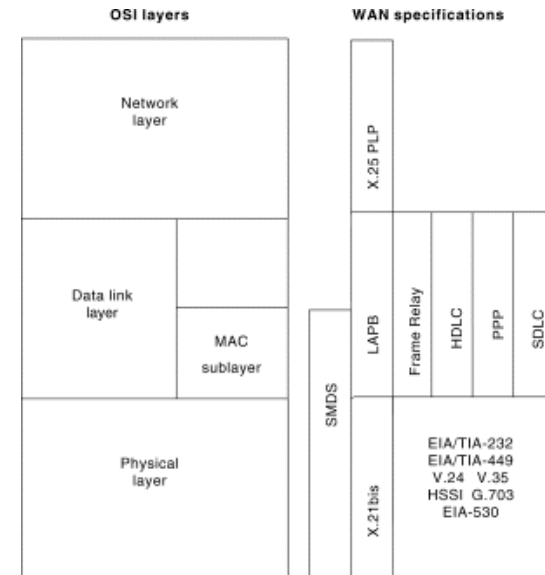
Level	U.S. / N. America	Europe
DS-1	T1 24 Circuits 1.544 Mbps	E1 30 Circuits 2.048 Mbps
DS-2	Not used in U.S.	E2 120 Circuits 34.368 Mbps
DS-3	T3 672 Circuits 44.7 Mbps	E3 480 Circuits 34.368 Mbps
DS-4	Not used in U.S.	E4 1920 Circuits 139.3 Mbps

Optical Carrier Levels

Optical Carrier (OC) Level	Megabits	# of 64kbps Channels	SONET Channels	SDH Channels (European)
OC-1	52Mbps	672	28 x DS-1 / 1 x DS-3	STM-0
OC-3	155Mbps	2,016	84 x DS-1 / 3 x DS-3	STM-1
OC-9	466Mbps	6,048	N/A	N/A
OC-12	622Mbps	8,064	336 x DS-1 / 12 x DS-3	STM-4
OC-18	933Mbps	12,096	N/A	N/A
OC-24	1,244Mbps	16,128	N/A	N/A
OC-36	1,866Mbps	24,192	N/A	N/A
OC-48	2,488Mbps	32,256	1344 x DS-1 / 48 x DS-3	STM-16
OC-96	4,976Mbps = 4.9Gbps	64,512	N/A	N/A
OC-192	10,000Mbps = 10Gbps	129,024	5376 x DS-1 / 192 DS-3	STM-64

WAN Devices

- Modem
 - A device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines
- Channel Service Unit/Digital Service Unit (CSU/DSU)
 - A digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for these two devices
- Multiplexer (MUX)
 - MUX allows more than one signal to be sent out simultaneously over a physical circuit
- WAN Switch
 - An internetworking device used in carrier networks. This device typically operates at the data-link layer
- Access Server
 - A concentration point for dial-in and dial-out connections.



WAN Devices

- Gateway
 - Allow different types of network to communicate
 - Three main types of gateways are: address, protocol, and application
 - Example: Gateway between RF and IP, Infrared and IP, etc.
- Multi-Service Switch
 - Layer 2/3 Devices that provide interoperability between data-link and network layers
 - Example:
 - WAN: MPLS (Multi-protocol Label Switching)
 - LAN: RSM (Route/Switch Module)
- Routers
 - Devices that operate at the network layer of the OSI model
 - A LAN or WAN devices determines the best path to send network traffic based on costs and other network information
 - A router also has to share information with other routers. (Static or dynamic routing.)

LAN Devices

- Repeaters (Layer 1)
 - Repeats electrical/radio signals to extend the length of the network
- Hubs (Layer 1)
 - Hubs are a central point of connection for cable segments in a physical star topology
- Bridges (Layer 2)
 - Bridges are intermediate systems, or switches, that forward MAC frames to destinations based on MAC addresses
- Switches (Layer 2 + Layer 3)
 - Essentially a multi-port bridges that function at the data link layer. Each port of the switch makes a decision to forward data packets to the attached network based on MAC addresses that maps to IP Addresses (i.e. ARP Table)
 - Each port on a switch is a separate collision domain reducing traffic on the network

Virtual Local Area Network (VLAN)

- VLANS
 - VLAN allows ports on a switch to be grouped into single broadcast domain. This allows devices to be logically configured as if they are on the same network without regard to their physical location
- Why Use a VLAN?
 - Performance – In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations
 - Formation of Virtual Workgroups – contain broadcasts and multicasts within the workgroup
 - Simplified Administration – 70% of network costs are a result of adds, moves, and changes of users in the network
 - Reduced Costs and Improve Security – Reduces and limits broadcasts

Virtual Local Area Network (VLAN)

- VLAN membership can be classified by port, MAC address, and protocol type
 - Membership by Port – The main disadvantage of this method is that it does not allow for user mobility. If a user moves to a different location away from the assigned VLAN, the network manager must reconfigure the VLAN
 - Membership by MAC Address – The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task
 - Membership by Protocol Type – The network IP subnet address can be used to classify VLAN membership users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses
 - VLAN membership can also be based on application or service, or any combination

Questions:

- What are the two data link layer protocols that control LAN transmissions:
 -
 -
- What are the three media access methods used by packets to access the network medium?
 -
 -
 -
- What are the two types of network switching commonly used in WAN?
 -
 -

Answers:

- What are the two data link layer protocols that control LAN transmissions:
 - Media Access Control (MAC)
 - Logical Link Control (LLC)
- What are the three media access methods used by packets to access the network medium?
 - Carrier Sensing Multiple Access (CSMA)
 - Token Passing
 - Polling
- What are the two types of network switching commonly used in WAN?
 - Circuit switching
 - Packet switching

Questions:

- What type of WAN device facilitates communications between two types of networks?
 -
- What type of WAN device enables multiple signals to be sent out simultaneously over a physical circuit?
 -
- VLAN membership can be organized by:
 -
 -
 -

Answers:

- What type of WAN device facilitates communications between two types of networks?
 - Gateway
- What type of WAN device enables multiple signals to be sent out simultaneously over a physical circuit?
 - Multiplexer (MUX)
- VLAN membership can be organized by:
 - Port
 - MAC Address
 - Protocol Type

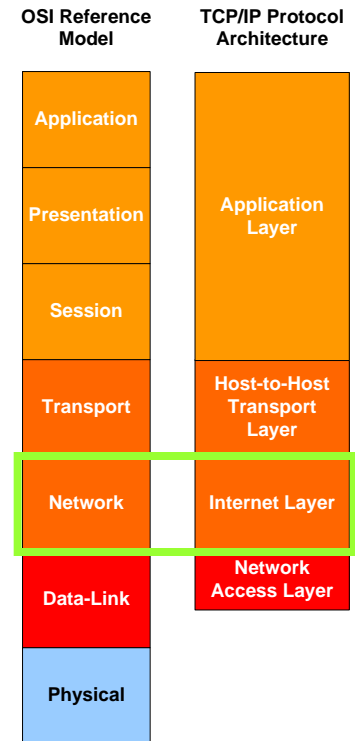
Telecommunications & Network Security Domain – Part 1

- Security Principles & Internet Protocol (IP) Architecture
- Terms & Definitions
 - Types of Data Network Structure
 - Methods & Modes of Data Network Communications
 - Types of Data Networks
 - Types of Data Networks Topology
- OSI Reference Model and TCP/IP Model
 - Physical Layer (Layer 1)
 - Data-Link Layer (Layer 2)
 - Network Layer (Layer 3)
 - Transport Layer (Layer 4)
 - Session Layer (Layer 5)
 - Presentation Layer (Layer 6)
 - Application Layer (Layer 7)



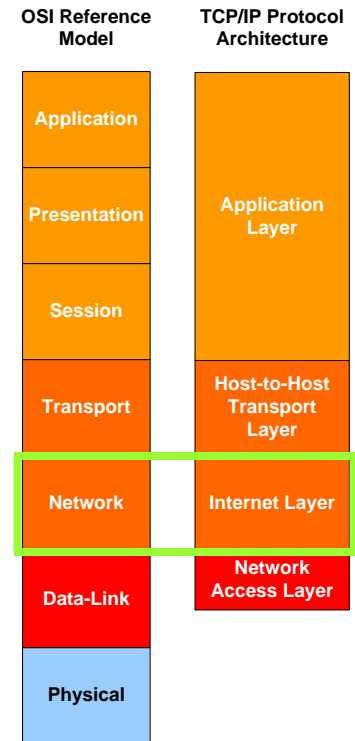
Network Layer (Layer 3)

- Network layer is responsible for the addressing and delivery of packets
 - Knows the address of the neighboring nodes in the network
 - Packages output with the correct network address information
 - Selects routes
 - Recognizes and forwards to the transport layer incoming messages for local host domains
 - Example: Internet Protocol (IP) and Netware



TCP/IP

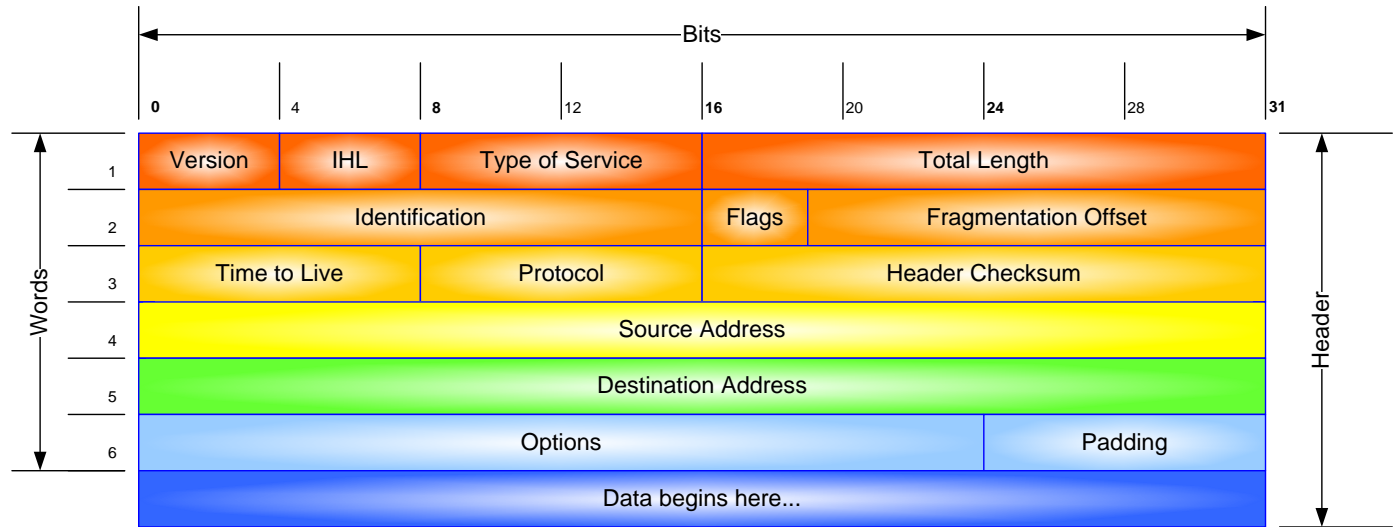
- DoD created TCP/IP to provide robust communication during wartime
- TCP/IP protocol suite is the standard for computer communications in today's networked world
- Internet Layer is the OSI Network layer (Layer 3) that contains:
 - Addressing information
 - Control information that enables packets to be routed
 - ICMP– Provides control and messaging capabilities
 - ARP– Determines MAC Address for known IP Address
 - Reverse ARP – Determines IP address from known MAC Address



Network Layer (Layer 3)

Structure of an IP

It is all about the “structured” **encapsulation** of data...

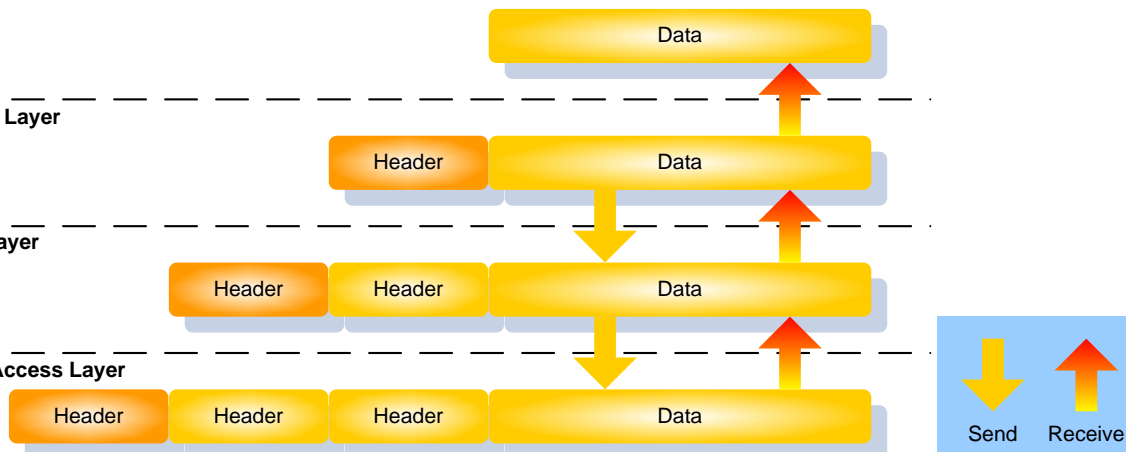


Application Layer

Transport Layer

Internet Layer

Network Access Layer



IP Addressing (IPv4)

- Internet Protocol Addresses (IPv4)
 - 32-bit IP Addresses are logical addresses and not physical
 - Includes a network ID and a host ID
 - Every host must have an unique IP address
 - IP addresses are assigned by a central authority

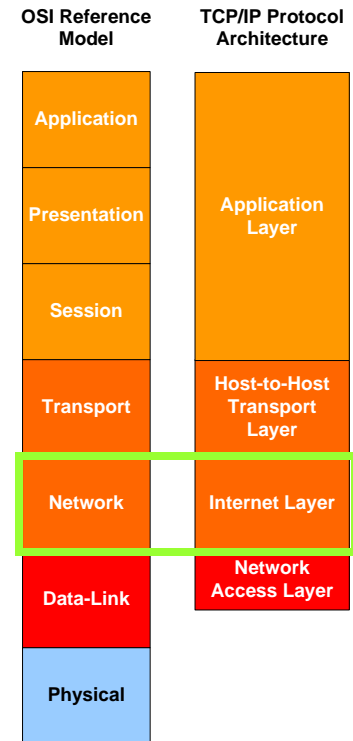
Class A (0) 1.0.0.0 – 127.255.255.255

Class B (10) 128.0.0.0 – 191.255.255.255

Class C (110) 192.0.0.0 – 223.255.255.255

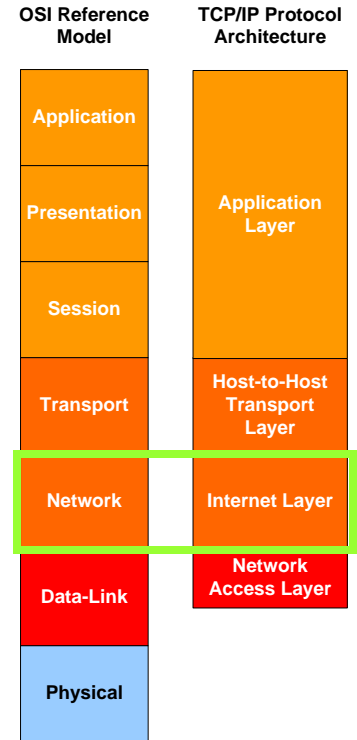
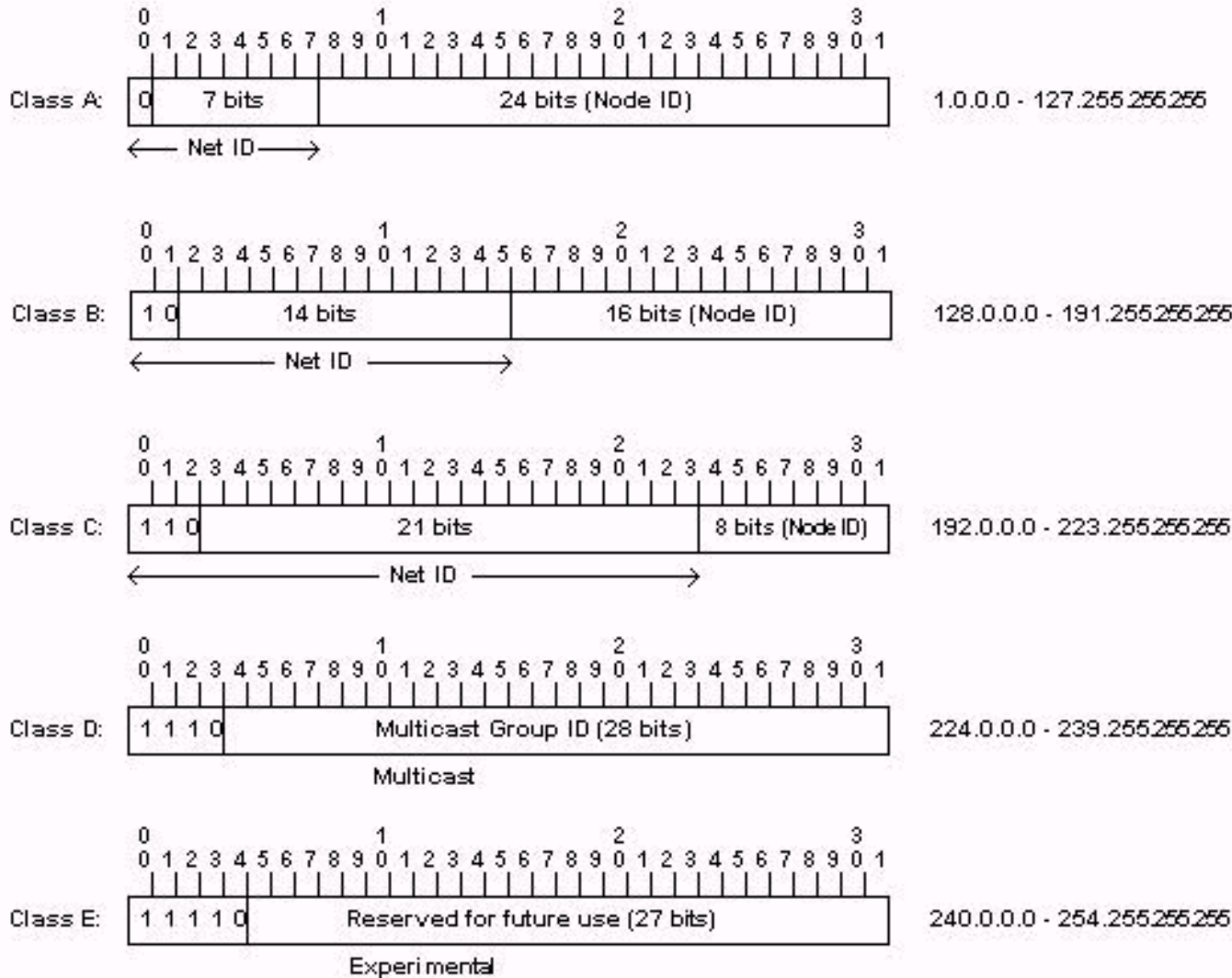
Class D (1110) 224.0.0.0 – 239.255.255.255 (Multicast)

Class E (11110) 240.0.0.0 – 254.255.255.255 (Experimental)



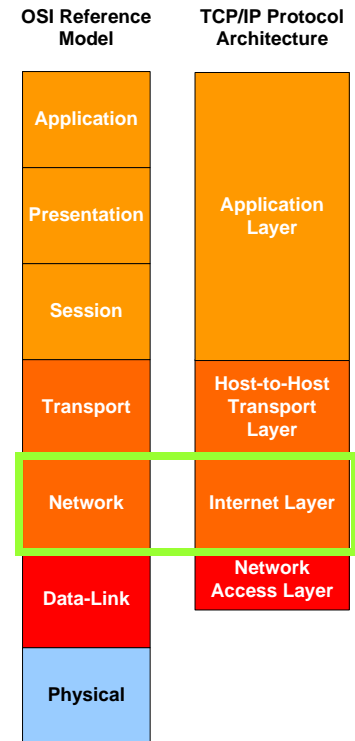
Network Layer (Layer 3)

IP Addressing (IPv4)



IP Addressing (IPv4)

- Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. (RFC 3022)
 - The increased use of NAT comes from several factors:
 - Shortage of IP addresses
 - Security needs
 - Ease and flexibility of network administration
 - RFC 1918 reserves the following private IP addresses for NAT
 - Class A: 10.0.0.0 – 10.255.255.255
 - Class B: 172.16.0.0 – 172.31.255.255
 - Class C: 192.168.0.0 – 192.168.255.255

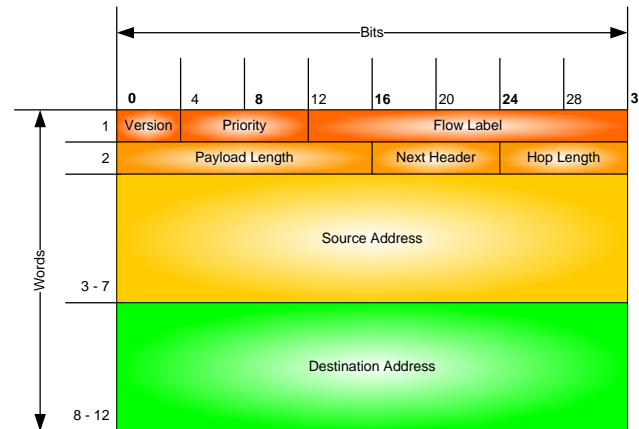


Internet Protocol Version 6 (IPv6)

- Internet Protocol Version 6 (IPv6) is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 (IPv4)
 - Larger IP Addressing Space. IPv6 is 128-bit, designed primarily to address shortage of IPv4 addresses
 - Auto configuration. With IPv6, a "stateless host auto configuration" mechanism is mandatory. This is much simpler than IPv4 DHCP
 - Security. With IPv6, IPsec support is mandatory
 - QoS flow label. IPv6 was designed to support for traffic engineering like diffserv. or intserv. (RSVP)
 - Multicast. Multicast is mandatory in IPv6. IPv4 uses IGMP

Internet Protocol Version 6 (IPv6)

- Priority: Enable a source to identify the desired delivery priority of the datagram
- Flow Label: Used by a source to label those products for which it requests special handling by the IPv6 router
- Payload Length: Length of payload (in octets)
- Next Header: Identifies the type of header immediately following the IPv6 header
- Hop Limit: An 8-bit integer decremented by one by each node that forwards the datagram
- Source & Destination Addresses: 128-bit IP addresses

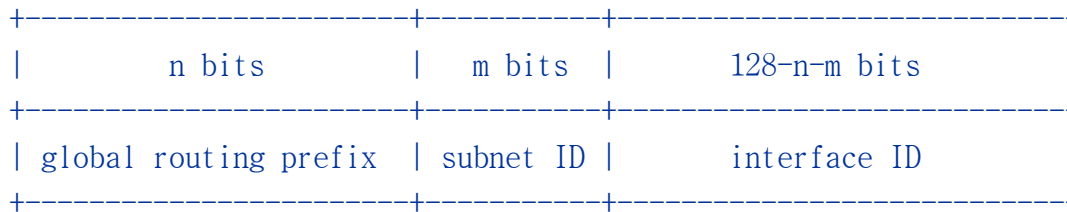


Internet Protocol Version 6 (IPv6) – Addressing

- RFC 4291 specifies the IPv6 addressing architecture

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local Unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

- The general format for IPv6 global unicast addresses:



where the global routing prefix is a (typically hierarchically-structured) value assigned to a site (a cluster of subnets/links), the subnet ID is an identifier of a link within the site.

Implementing IPv6 – Compatibility to IPv4

- IPv6 can be compatible to IPv4 in two ways:

- IPv4-compatible IPv6 address



where the IPv4 address must be a globally unique IPv4 unicast address

- IPv4-mapped IPv6 address



- See RFC 4038 for IPv6 transition.

Implementing IPv6 – IPsec

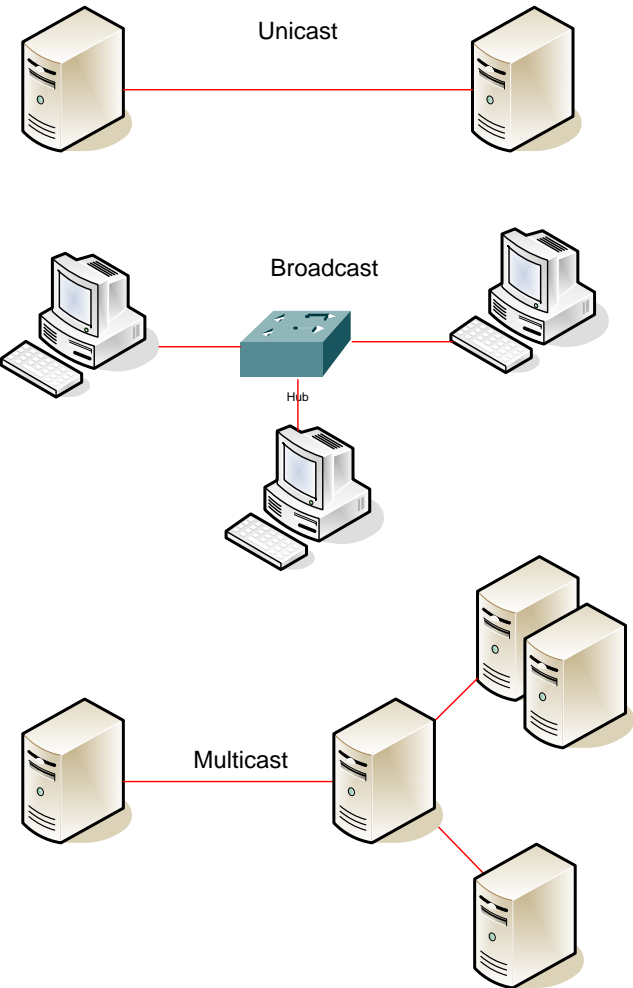
- IPsec is “mandatory” in IPv6, but biggest implementation challenges were:
 - Updating key exchange protocols and ciphers (IKEv2):
RFC 2409 → RFC 4306 → RFC 5996
 - Establishing security associations on a “Internet” scale:
RFC 2401 → RFC 4301
- RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*, September 2010
 - Two phase: IKE-SA and Child-SA, to better facilitate IPsec deployment
 - [IKEv2 is not backward compatible to IKEv1](#)
- RFC 4301, *Security Architecture for IP*, December 2005
 - Added [Peer Authorization Database \(PAD\)](#) to provide a link between an SA management protocol and the Security Policy Database (SPD)

Reference:

- *Design Rationals for IKEv2* (<http://tools.ietf.org/html/draft-ietf-ipsec-ikev2-rationale-00>)
- S. Hagen, *IPv6 Essentials, 2nd. Edition*, 2006.

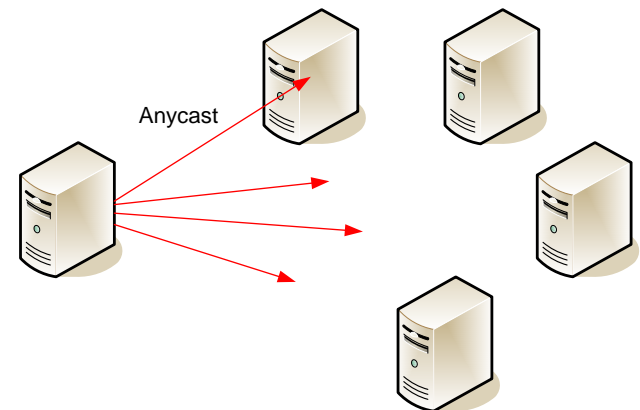
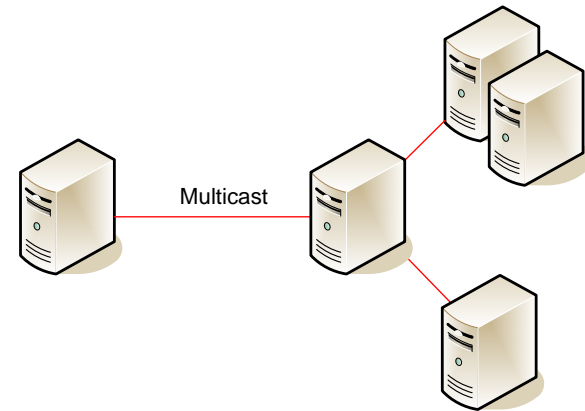
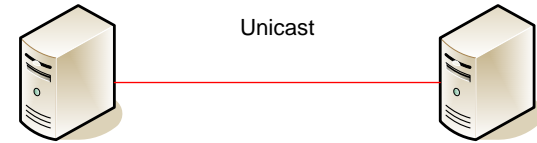
IP Transmission Methods (in IPv4)

- **Unicast:** Packet is sent from a single source to a single destination
- **Broadcast:** The packet is copied and sent to all of the nodes on the network
- **Multicast:** Source packet is copied and then sent to a group of destinations on a network



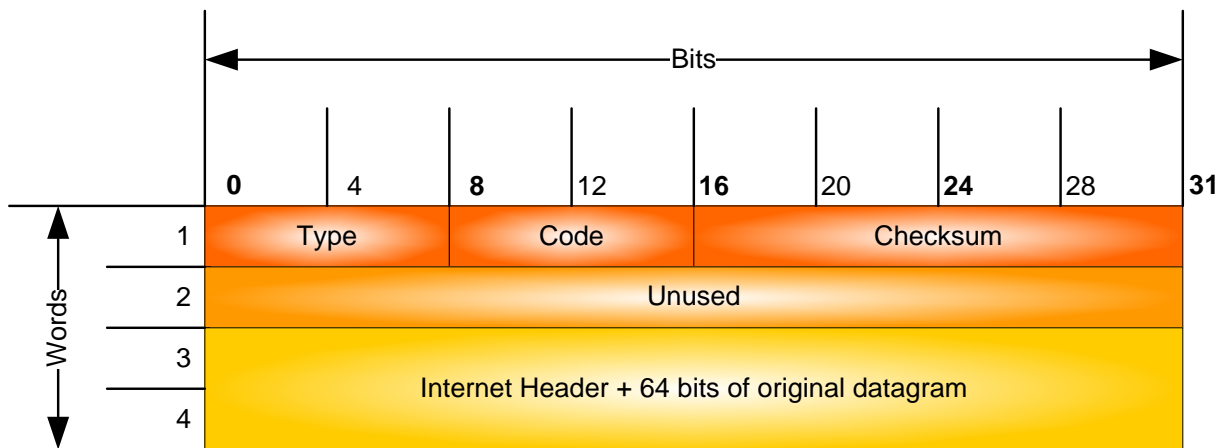
IP Transmission Methods (in IPv6)

- **Unicast:** Packet is sent from a single source to a single destination
- **Multicast:** A multicast address identifies a group of IPv6 interfaces. Source packet is copied and then sent to a group of destinations on a network
- **Anycast:** An anycast address is assigned to multiple interfaces. Source packet is delivered to the nearest interface.



Internet Control Message Protocol (ICMP)

- ICMP (Internet Control Message Protocol)
- Used to exchange control messages between gateways and hosts regarding the low-level operations of the Internet
 - Ping
 - Traceroute
- ICMP is encapsulated within the IP packet

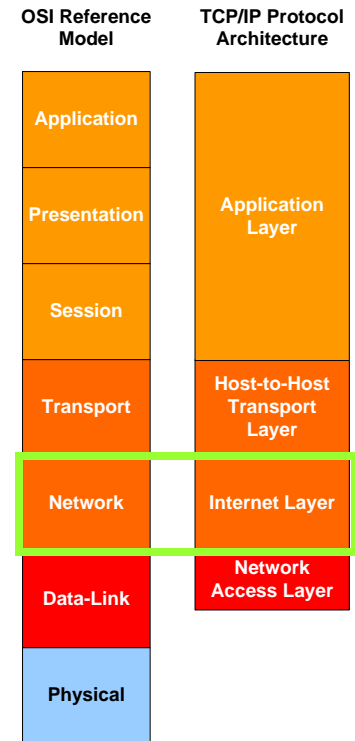


Internet Group Management Protocol (IGMP)

- IGMP (Internet Group Management Protocol)
- Created because IPv4 only supports unicast and broadcast
- When a message is sent to a particular multicast group, all computers in that group will get a copy of the message
- It is used by hosts to report multicast group members to neighboring multicast routers

Routing vs. Routed Protocols

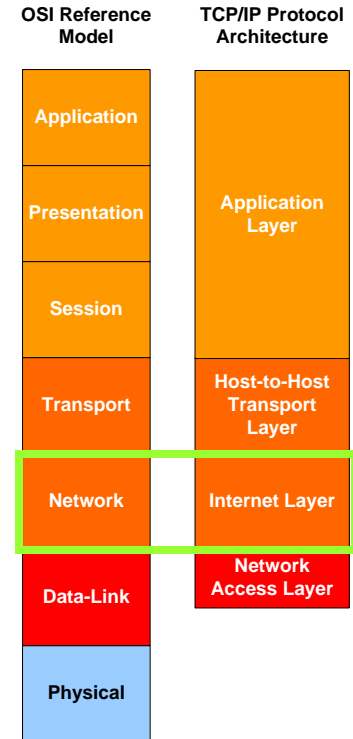
- Routing Protocols
 - Interior Routing Protocols
 - Routing Information Protocol (RIP)
 - Interior Gateway Routing Protocol (IGRP) (proprietary to Cisco Systems)
 - Open Shortest Path First (OSPF) Protocol
 - Integrated IS-IS (ISO 10589 Intermediate system to intermediate system)
 - Extended Interior Gateway Routing Protocol (EIGRP) (proprietary to Cisco Systems)
 - Exterior Routing Protocols
 - Border Gateway Protocol (BGP)
- Routed Protocols
 - Protocols that are encapsulated within the routing protocols and being routed by the routing protocols
 - Example: HTTP, FTP, Telnet, SNMP, etc.



Static Routing

Routing can be either static or dynamic

- Static routing is performed using a preconfigured routing table which remains in effect indefinitely, unless it is changed manually by the user
 - This is the most basic form of routing, and it usually requires that all machines have statically configured addresses. If there is a change, the user must manually alter the routing tables on one or more machines to reflect the change in network topology or addressing
 - Static routing does not scale well. Calculation of static routing grows exponentially to the number of static routes in the route table



Dynamic Routing

- Dynamic routing uses special routing information protocols to automatically update the routing table with routes known by peer routers
 - These protocols are grouped according to whether they are Interior Gateway Protocols (IGP's) or Exterior Gateway Protocols (EGP's)
 - IGP's are used to distribute routing information inside of an Autonomous System (AS). An AS is a set of routers inside the domain administered by one authority. Examples of interior gateway protocols are OSPF and RIP
 - EGP's are used for inter-AS routing, so that each AS may be aware of how to reach others throughout the Internet. Examples of exterior gateway protocols are EGP and BGP

Dynamic Routing – Interior Gateway Protocols (IGP's)

- Distance-Vector Routing Protocols
 - Routing Information Protocol version 2 (RIP-2), has routers exchanging routing table information using a distance-vector algorithm
 - With RIP, neighboring routers periodically exchange their entire routing tables
 - RIP uses hop count as the metric of a path's cost, and a path is limited to **15 hops**
 - RIP Protocol version 2 is described in RFC2453

Note: Think “road sign”

Dynamic Routing – Interior Gateway Protocols (IGP's)

- Link-State Routing Protocols
 - Open Shortest Path First (OSPF) protocol is a link state routing algorithm that is more robust than RIP
 - OSPF converges faster, scales to larger enterprise networks
 - Requires less network bandwidth. Using OSPF, a router broadcasts only changes in its links' status rather than entire routing tables
 - OSPF Version 2, is described in RFC 1583, and is rapidly replacing RIP in the Internet

Note: Think “roadmap”

Dynamic Routing – Exterior Gateway Protocols (EGP)

- Border Gateway Protocol version 4 (BGP-4) is an *exterior gateway protocol* because it is used to provide routing information between Internet routing domains (i.e. inter-AS)
 - BGP is a path vector protocol, unlike other distance vector protocols, BGP tables store the actual route to the destination network
 - BGP-4 also supports policy-based routing, which allows a network administrator to create routing policies based on political, security, legal, or economic issues rather than technical ones

Questions:

- Why IPv4 requires Class D IP addresses and IGMP, but IPv6 does not?
 -
- What is the length of an IPv4 address?
 -
- What is the length of an IPv6 address?
 -
- What is the difference between routing and routed protocols?
 -

Answers:

- Why IPv4 requires Class D IP addresses and IGMP, but IPv6 does not?
 - Multicast is build-in to IPv6
- What is the length of an IPv4 address?
 - 32-bit
- What is the length of an IPv6 address?
 - 128-bit
- What is the difference between routing and routed protocols?
 - Routing protocols instruct a router where and how to send the routed protocols

Questions:

- What is the difference between static routing and dynamic routing?
 -
- Name the two types of routing protocols?
 -
 -
- What is the default routing protocol for Internet?
 -

Answers:

- What is the difference between static routing and dynamic routing?
 - Routing table changes in dynamic routing
- Name the two types of routing protocols?
 - Interior routing protocols
 - Exterior routing protocols
- What is the default routing protocol for Internet?
 - Border Gateway Protocol (BGP)

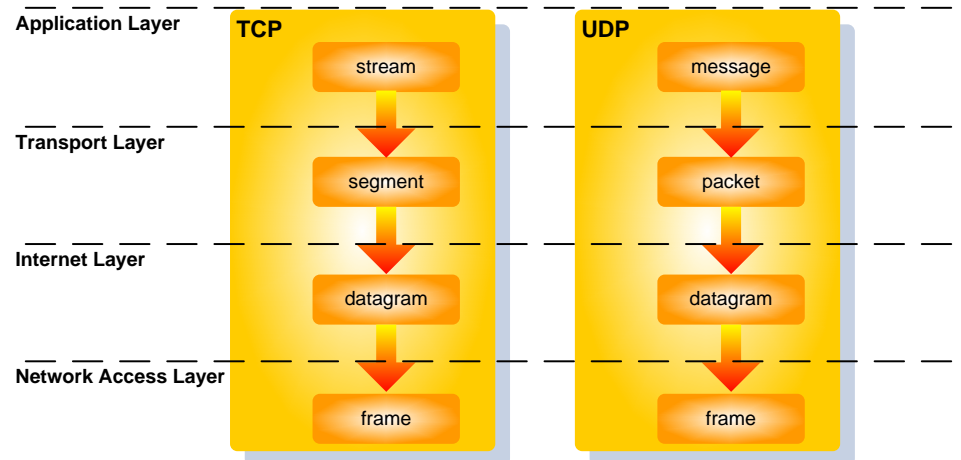
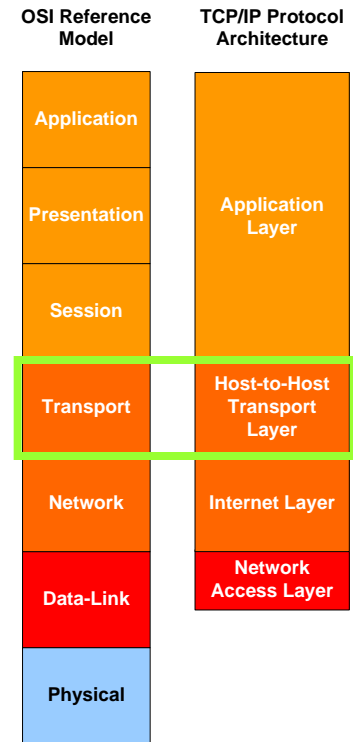
Telecommunications & Network Security Domain – Part 1

- Security Principles & Internet Protocol (IP) Architecture
- Terms & Definitions
 - Types of Data Network Structure
 - Methods & Modes of Data Network Communications
 - Types of Data Networks
 - Types of Data Networks Topology
- OSI Reference Model and TCP/IP Model
 - Physical Layer (Layer 1)
 - Data-Link Layer (Layer 2)
 - Network Layer (Layer 3)
 - Transport Layer (Layer 4)
 - Session Layer (Layer 5)
 - Presentation Layer (Layer 6)
 - Application Layer (Layer 7)



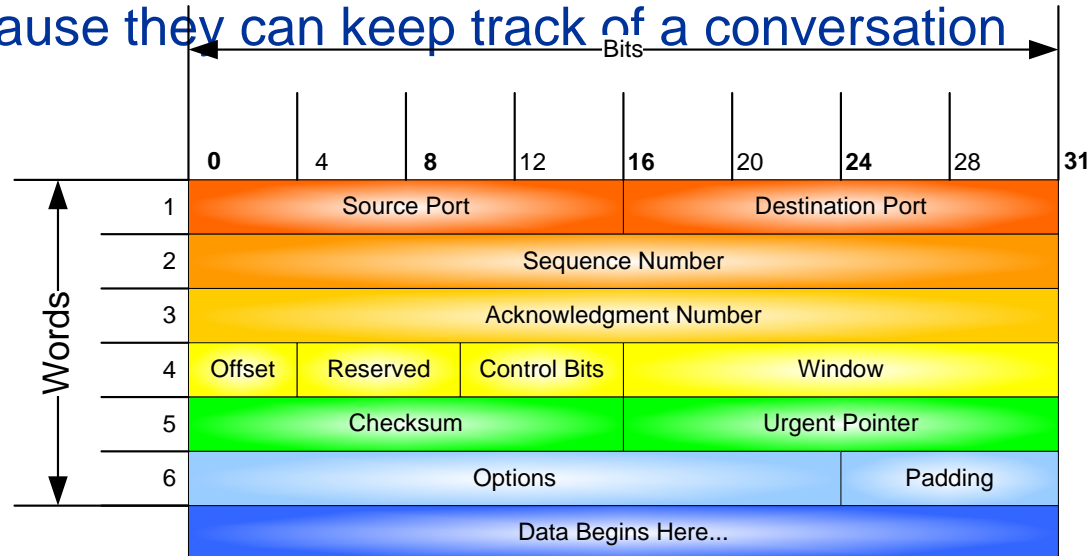
Transport Layer (Layer 4) – TCP vs. UDP

- Transmission Control Protocol (TCP)
 - Provide reliable data transmission
 - Connection-oriented with flow control
 - Maintains status and state: Stateful
- User Datagram Protocol (UDP)
 - Provide best effort data transmission
 - Connection-less without flow control
 - Does not maintain status and state
 - Does not offer error correction, nor retransmission



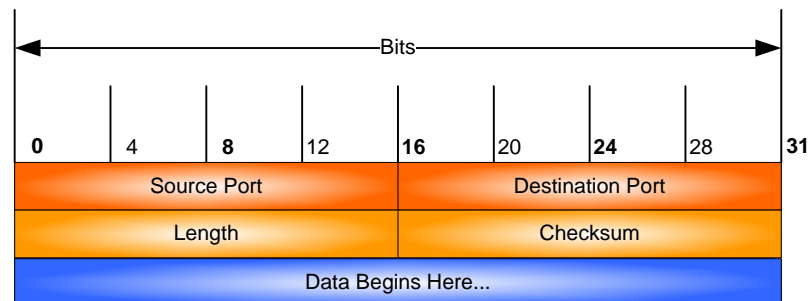
Transmission Control Protocol (TCP)

- **TCP** is a **connection-oriented** transmission that maintains status and state information of each user data stream flowing into and out of the TCP module
 - Connection-oriented data management
 - Reliable **stream-oriented** data transfer
 - Segments are resent if a segment is unrecognizable or is not received
 - Connection-oriented protocols are sometimes described as **stateful** because they can keep track of a conversation



User Datagram Protocol (UDP)

- UDP is a connectionless transmissions do not require the receiver to acknowledge receipt of a packet, instead the sending device assumes that the packet arrived
 - Much faster. Less overhead than TCP
 - Less reliable. UDP does not offer error correction, retransmission or protection from lost, duplicated, or re-ordered packets
 - Connectionless protocols are usually described as stateless because each end has no protocol-defined way to remember where they are in a "conversation" of message exchanges



TCP/UDP Examples

Transmission Control Protocol

Higher communication protocols that use TCP

- FTP (File Transfer Protocol)
- Telnet
- SMTP (Simple Mail Transfer Protocol)
- SSH (Security Shell)
- SSL (Secure Socket Layer)
- HTTP (Hyper Text Transfer Protocol)

User Datagram Protocol

Higher communication protocols that use UDP

- RPC (Remote Procedural Call)
- XDR (eXternal Data Representation)
- NFS (Network File System)
- TFTP (Trivial FTP)
- SNMP (Simple Network Management Protocol)
- DNS (Domain Name System)

Session Layer (Layer 5)

Session Layer provides services to establish a session-connection between two presentation entities and support orderly data exchange interactions, and to release the connection in an orderly manner.

- Connections: duplex, half-duplex mode
- Session-connection synchronization
- (For CISSP...) Examples of Session Layer protocols are:
 - Network File System (NFS)
 - Remote Procedure Call (RPC)
 - Network Basic Input/Output System (NetBIOS) names
 - Structured Query Language (SQL)

Reference:

- ISO/IEC 7498-1:1994(E), *Open Systems Interconnection – Basic Reference Model: The Basic Model*, 1996.
- *CISSP All-in-One Exam Guide*, S. Harris, 2008.

Presentation Layer (Layer 6)

Presentation Layer ensures that the communications passing through are in the appropriate form for the recipient. Programs in the presentation layer address three aspects of presentation:

- Syntactical compatibility. Data coding and conversion send from the application layer of one system will be readable by the application layer of another system
- Encapsulation of data into message "envelopes" for transmission through the network. (i.e. EBCDIC binary → ASCII.)
- (For CISSP...) Example of data formats are:
 - ASCII (American Standard Code for Information Interchange)
 - EBCDIC (Extended Binary Coded Decimal Interchange Code)
 - Tagged Image File Format (TIFF)
 - Joint Photographic Experts Group (JPEG)
 - Motion Picture Experts Group (MPEG)

Reference:

http://en.wikipedia.org/wiki/Presentation_layer

- ISO/IEC 7498-1:1994(E), *Open Systems Interconnection – Basic Reference Model: The Basic Model*, 1996.
- *CISSP All-in-One Exam Guide*, S. Harris, 2008.

Application Layer (Layer 7)

Application Layer provides services for application program that ensure that communication is possible.

- Makes sure that necessary communication resources exist
- Ensures agreement at both ends about error recovery procedures, data integrity, and privacy
- Determines protocol and data syntax rules at the application level
- (For CISSP...) Example of application services are:
 - File Transfers Protocol (FTP)
 - Trivial File Transfer Protocol (TFTP)
 - Simple Mail Transfer Protocol (SMTP)
 - Simple Network Management Protocol (SNMP)
 - Telnet
 - Hypertext Transfer Protocol (HTTP)

Reference:

- ISO/IEC 7498-1:1994(E), *Open Systems Interconnection – Basic Reference Model: The Basic Model*, 1996.
- *CISSP All-in-One Exam Guide*, S. Harris, 2008.

Summary

OSI Layers	Protocols
Application	FTP, TFTP, SNMP, SMTP, Telnet, HTTP
Presentation	ASCII, EBCDIC, TIFF, JPEG, MPEG, MIDI
Session	TCP: SQL, NetBIOS; UDP: NFS, RPC
Transport	TCP, UDP, SSL, SPX
Network	IP: Address, Routing, Broadcast methods; ICMP; IGMP
Data Link	Data-Link Protocols: LAN, WAN
Physical	Network Cables, RF, Infrared, Optical Fiber, etc.

Validation Time... 😊

1. Class Exercise
2. Review Answers

Exercise #1: Routing Architecture

- Please provide a list of recommended ways to :
 - Control where the packets go?
 - Define how packets are being routed?
 - Preserve integrity of routing table?

Exercise #2: L2 Switching

- Please provide a list of recommended ways to:
 - Control the information flow?
 - Control the network broadcasts from Ethernet?
 - Control the network interfaces?
 - Preserve the configuration of a ARP table?

Telecommunications & Network Security Domain – Part 2

- Security Principles & Network Architecture
- Security Countermeasures and Controls
 - Physical Layer
 - Data-Link Layer
 - IP Network Layer
 - Transport Layer
 - Application Layer