General Discussion on Networks for CISSP.

Introduction to Terms and OSI & TCP Models.

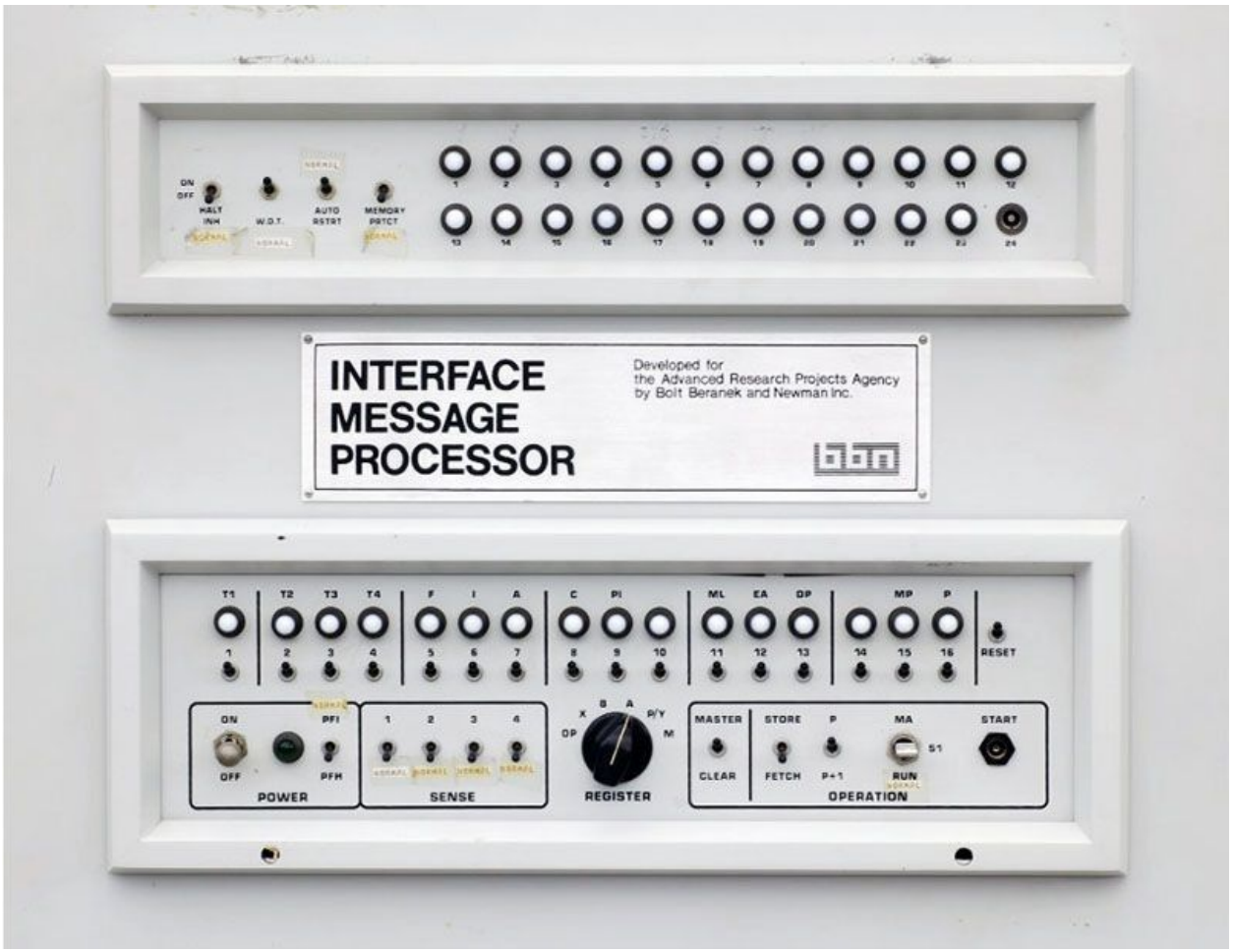
Session 1 10/17/2020 Classroom-1

NOTES

What is a Network?

Before I answer that question.

- This is not a boot camp but think of it as an introductory class to the Network part of the Domain 4 for CISSP.
- This is a session for you to understand some of the basic terms and concepts.
- If you are a network expert, then this may seem like a refresher on networks.
- My goal is to give you a gateway drug into Domain 4. So when you pick up that OSG and read through some of the beginning chapters, there should not be any dropped packets or more questions but a smooth flow of information into your brain.



The **Interface Message Processor (IMP)** was the packet switching node used to interconnect participant networks to the ARPANET from the late 1960s to 1989. It was the first generation of gateways, which are known today as routers. An IMP required the connection to a host computer via a special bit-serial interface, The IMP software and the ARPA network

communications protocol running on the IMPs was discussed in RFC 1, the first of a series of standardization documents published by the Internet Engineering Task Force (IETF).

The first network that came online or switched ON, was in late October 1969, the ARPAnet is the first large-scale, general-purpose computer network to connect different kinds of computers together.

Birth of Internet: January 1, 1983
The ARPA projects and international working groups led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks, which produced various standards.

“A network consists of two or more computers that are linked in order to share resources”

For a CISSP, you should have a clear understanding of Fundamentals of Data Units.

Bit:

- a "bit" is atomic: the smallest unit of storage
- A bit stores just a 0 or 1
- "In the computer it's all 0's and 1's" ... bits
- Anything with two separate states can store 1 bit
- In a chip: electric charge = 0/1
- In a hard drive: spots of North/South magnetism = 0/1
- A bit is too small to be much use
- Group 8 bits together to make 1 byte

Byte:

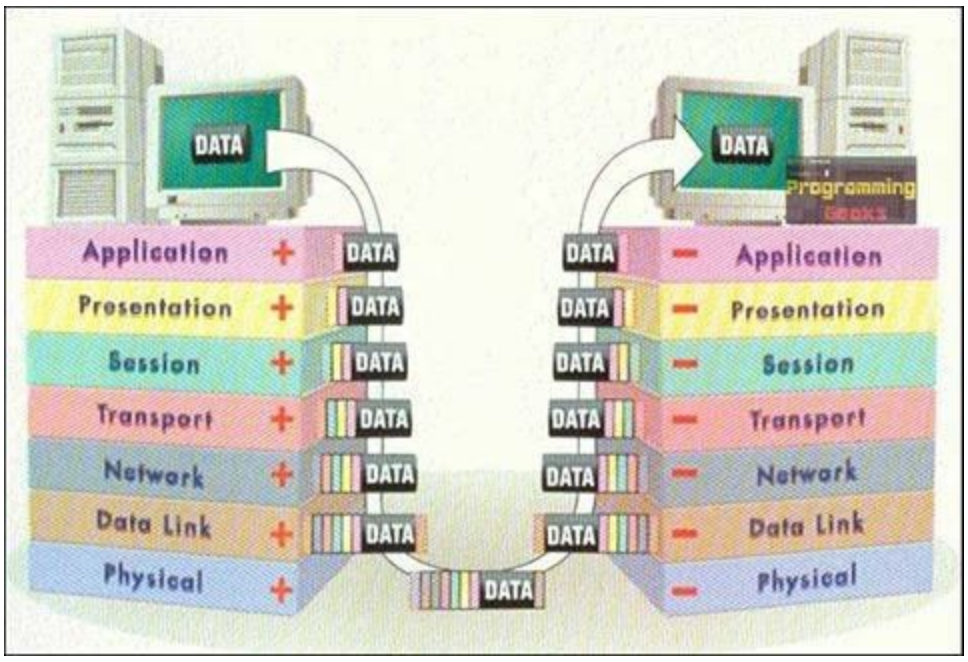
- One byte = collection of 8 bits
- e.g. 0 1 0 1 1 0 1 0
- One byte can store one character, e.g. 'A' or 'x' or '$'

For example,

ASCII characters are 1 byte. (American Standard Code for Information Interchange)
Unicode Character of UTD- 16 is 2 bytes. Encoding used by Windows Internally.

Now let us take a look at the bigger picture of how data is transported or moved around. Remember, we use many different types of computers and hardware. In order to communicate we need common protocols. And thus comes the standardized protocols to communicate. There

are a couple of models that were introduced in the beginning to get a foothold on standardization of such protocols. While they served their purpose during the early stages of development of communication protocols. They are now used mainly to explain or learn about protocols and server very little or no purpose in modern day application development or communication design and architecture. In this session we will focus on the OSI Model.



Now remember there is also another model, called the TCP/IP model which is also called DoD Model. Which we will look at closely in the next session.

DoD model was **developed** in 1973 for the DARPA (**Defense Advanced Research Projects Agency)** Internetwork Project.
The Open Systems Interconnection (**OSI**) reference **model** was developed by the ISO (International Standards Organization (ISO) in 1984.

Why is it so confusing?
OSI Model is technically dead. No longer referenced. Then Would I say the TCP/IP Model is more relevant? I think that is dead too. Wait then how should you even start to understand this whole network stuff-
For academic and research purposes, even today ,the OSI and TCP/IP models are very relevant and help us understand the interconnections and help us reference various protocols and standards.

CISSP TIP:
Recollection of the Layer and its corresponding Number.

Alright. Who can tell me in a flash of a second the different layers and their associated numbers? In other words, If I were to give you a number, would you tell me what layer it is?

Let us try it. Write the corresponding number next to the layer.
.

Application Layer	
Physical Layer	
Data Layer	
Session Layer	
Presentation Layer	
Network Layer	
Transport Layer	

Did you all get it right? Lets see.
Application Layer is 7
Presentation Layer is 6
Session Layer is 5
Transport Layer 4
Network Layer is 3
Data Link Layer is 2
Physical Layer is 1

Watch the video here:
https://icsbits.com/go/osi

Or better yet let me show you something. Now this is just one of the hacks to quickly recollect the different layers and its corresponding number in the OSI Model.

Let us understand the OSI a little bit more. The OSI layers are basically a Protocol Entities. When data passes through them, they change, in the sense, more data parts are added when the data goes from Application down towards the Physical Layer and similarly the data parts are removed as the data units move from physical layer to Application Layer.

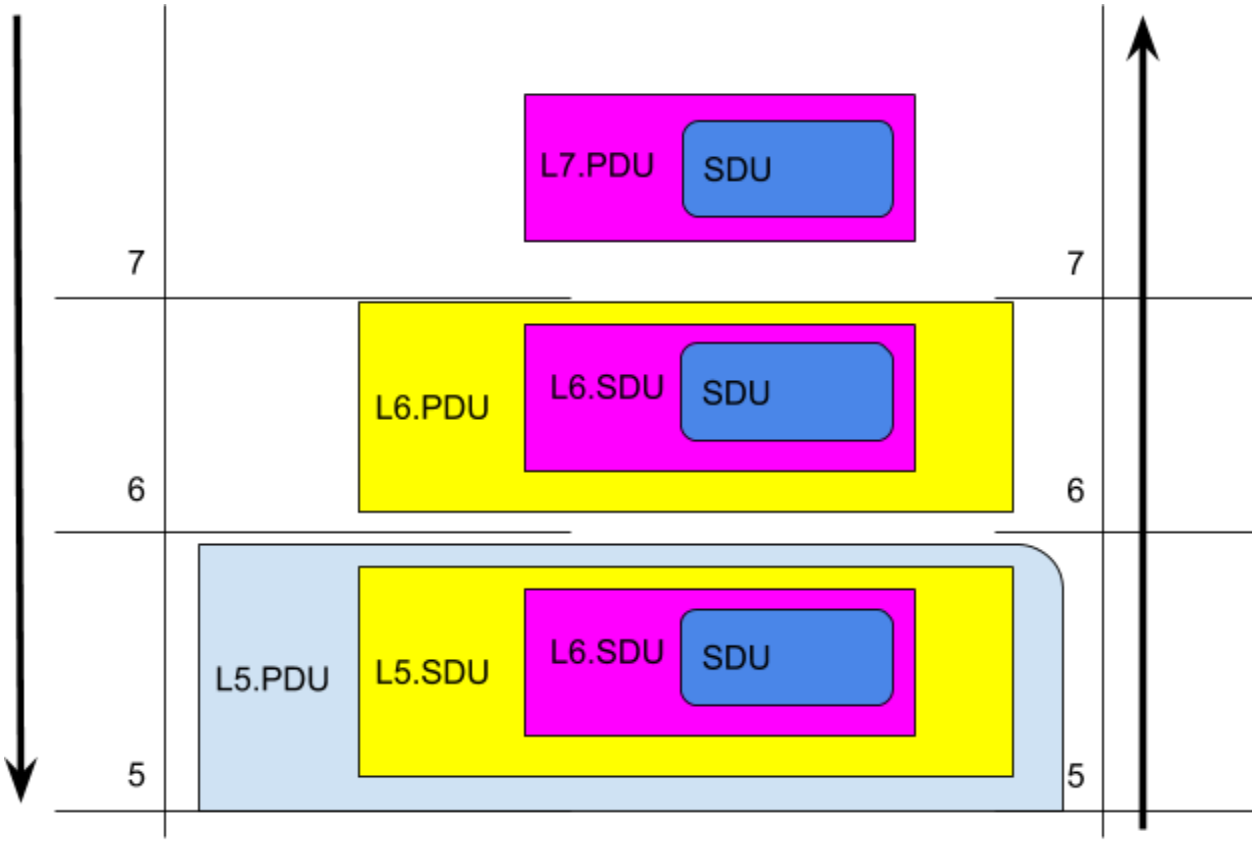
Encapsulation and Opposite of Encapsulation - Reveal (Decapsulation**)**

Service Data Unit (SDU)

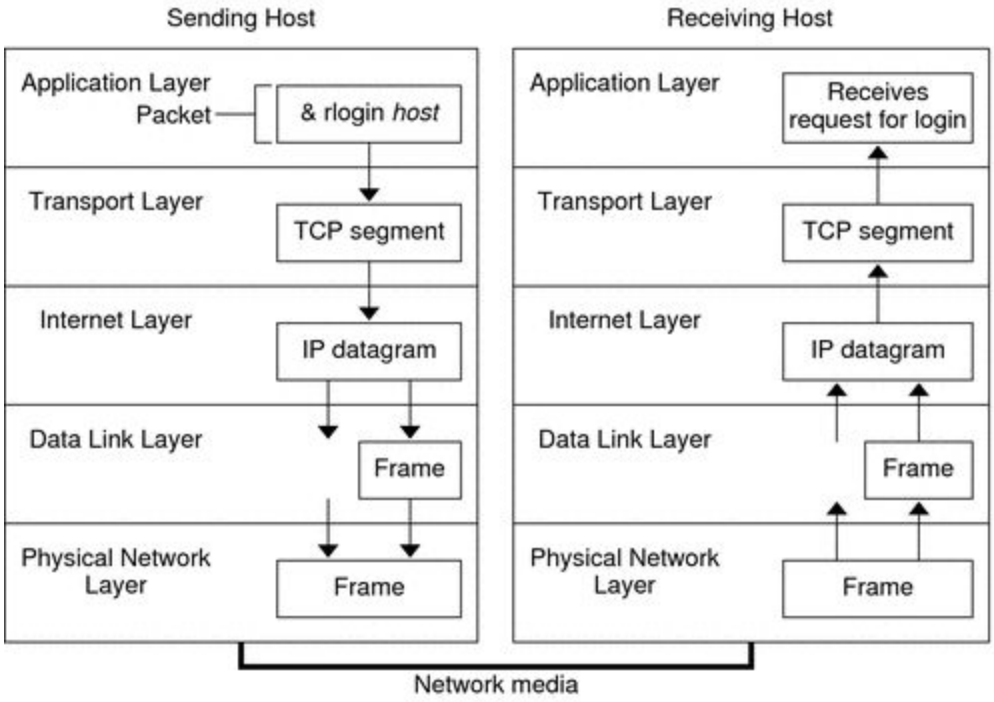
SDU stands for **Service Data Unit** - this is the input data form that gets into a particular protocol entity to be processed.

Protocol Data Unit (PDU)

PDU stands for **Protocol Data Unit** - this is the output data form from a protocol entity



Segments, **Packets** and **Frames**.



LAYER # - OSI NAME	- COMMON PROTOCOL OR USE	- PDU NAME
Layer 1 - Physical	- Transceiver	- bits, or a physical signal
Layer 2 - Datalink	- Ethernet	- frame
Layer 3 - Network	- IP	- packet
Layer 4 - Transport	- TCP	- segment
Layer 5 - Session	- SIP	- data, request, or response
Layer 6 - Presentation	- Encryption/compression	- data, request, or response
Layer 7 - Application	- HTTP	- data, request, or response

OSI-TCP/IP Reference Table

OSI Layers	Terms	Network Equipment	Protocols	Application (Example)	Standards	TCP/IP Layers
7 - APP	SEGMENT	Gateways	SMTP, POP, HTTP, FTP, VOIP, DNS, DHCP, NTP	Web Servers	RFC 821	4 APP
6 - PRE	SEGMENT	Gateways	TLS. SSL, FTP, IMAP	Email Access	RFC 959	4 APP
5 - SES	SEGMENT	Gateways	API	Database Access		4 APP
4 - TRA	DATA STREAM ← → Segment	Firewalls, Gateways	TCP, UDP	Client-Server Communication	RFC 793, RFC 768	3 TRA
3 - NET	SEGMENT ← → Packet	Routers, Firewalls	IP. ICMP	IPSec (VPN)	RFC 1112	2 INTERNET
2 - DAT	PACKET ← → Frame	NIC, Layer 2 Switch, Bridges	PPP	Ethernet	IEEE (802.2, 802.11x)	1 NET ACC
1 - PHY	Frame ← → Electrical	Hubs, Repeaters		Coax, Fiber	ITU, IEC, IEEE	1 NET ACC

ITU: International Telecommunication Union
IEC: International Electrotechnical Commission
IEEE: Institute of Electrical and Electronics Engineers
RFC: Request for Comments → Standard

Multi-Layer Switching

Multi-Layer Switch means, It can route traffic using the Layer 2, 3 and 4

Multi-layer switching can make routing and switching decisions based on the following

- MAC address in a data link frame
- Protocol field in the data link frame
- IP address in the network layer header
- Protocol field in the network layer header
- Port numbers in the transport layer header

Ethernet:
The term Ethernet refers to a whole family of closely related protocols characterized by their raw data rates (10 Mbps, 100 Mbps, 1 Gbps or 10 Gbps)

The term Ethernet refers to a whole family of closely related protocols characterized by their raw data rates

- 10 Mbps,
- 100 Mbps,
- 1 Gbps,
- 10 Gbps

Ethernet also refers to the physical medium on which they operate. Ethernet now runs on a wide variety of physical media.
Among the most common are:

- Coaxial cable (thick or thin),
- Many types of copper cable called twisted pair,
- Several types of fiber-optic cables using a variety of signalling methods and light wavelengths.

Next Session:

- Detailed OSI Model Review
- Introduction to TCP/IP - Four Layers of TCP/IP and the protocols
- TCP and UDP Protocols (TCP Three way handshake)
- IP Classes (CIDR Classless Inter Domain Routing)