Computer Networks

and

Computer Networking & Security

FTVETI

ICT @ FTVETI

Objectives

After completing this unit, you should be able to:

- Understand the concept of Layered Network architecture
- Know OSI Model and various TCP/IP Protocols
- Learn about various Network Devices
- Understand various Network security risks & know basic mitigation techniques

FTVETI

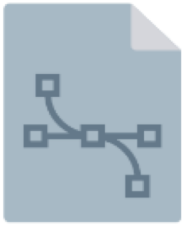
ICT @ FTVETI

Introduction To Computer Network

- Collection of nodes connected by some media link (wired or wireless connection) is called a **network**
- A **node** could be a device with a capability of sending and receiving data, such as computers, printers, tablets, mobile, IoT and so on
- **Internet** is great resultant of a large scale computer network
- Generally a **computer Network** meets the following characteristics:

Performance

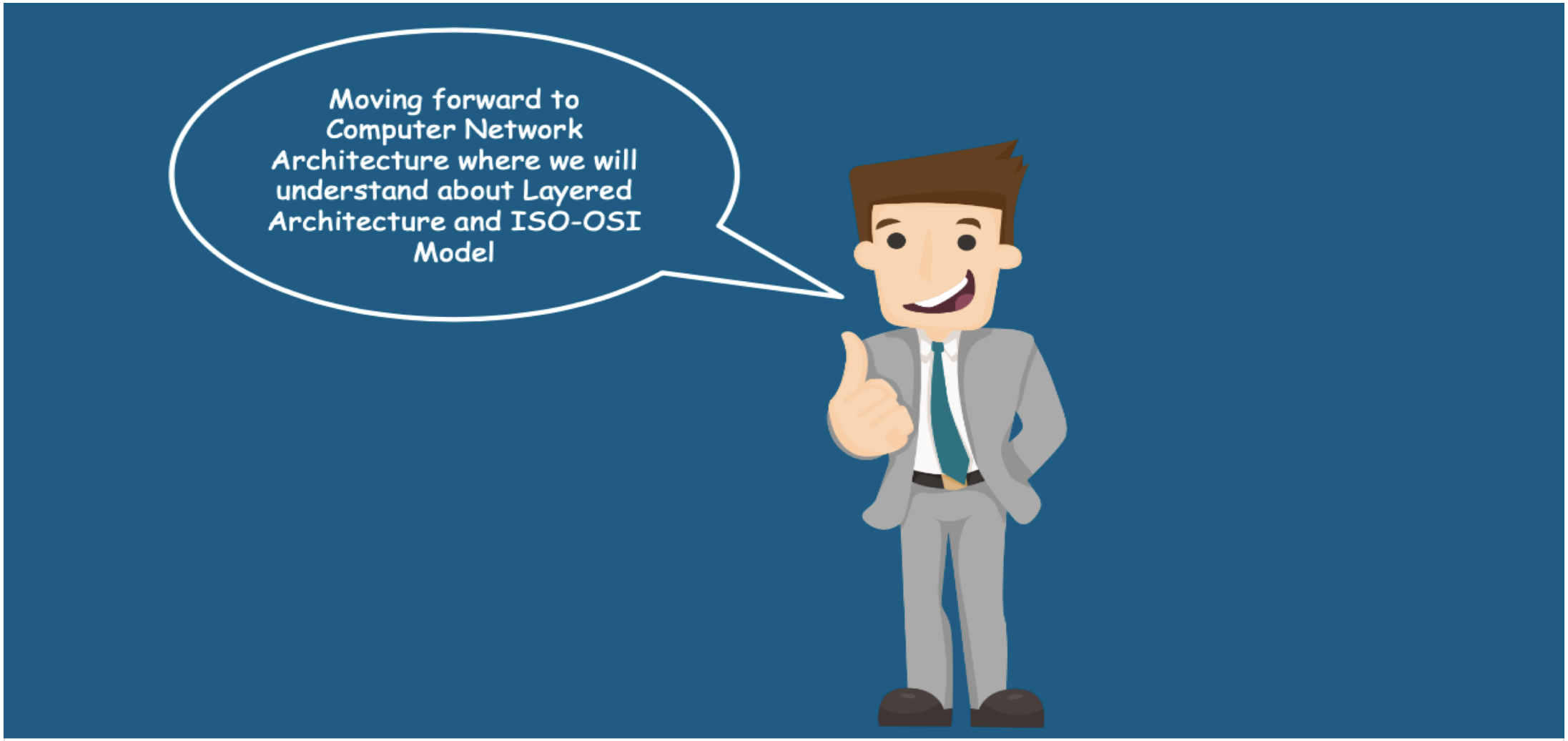
Reliability



Scalability

What Is A Computer Network?

A **computer network** is a group of computer systems and other hardware devices that are linked together by communication channels to facilitate communication and resource-sharing among a wide range of users


Moving forward to Computer Network Architecture where we will understand about Layered Architecture and ISO-OSI Model

Computer Networks – Architecture

FTVETI

ICT @ FTVETI

Layered Architecture

What is Layered Architecture ?

In a Layered Architecture data sequentially moves from one layer to the other

What does Layering mean ?

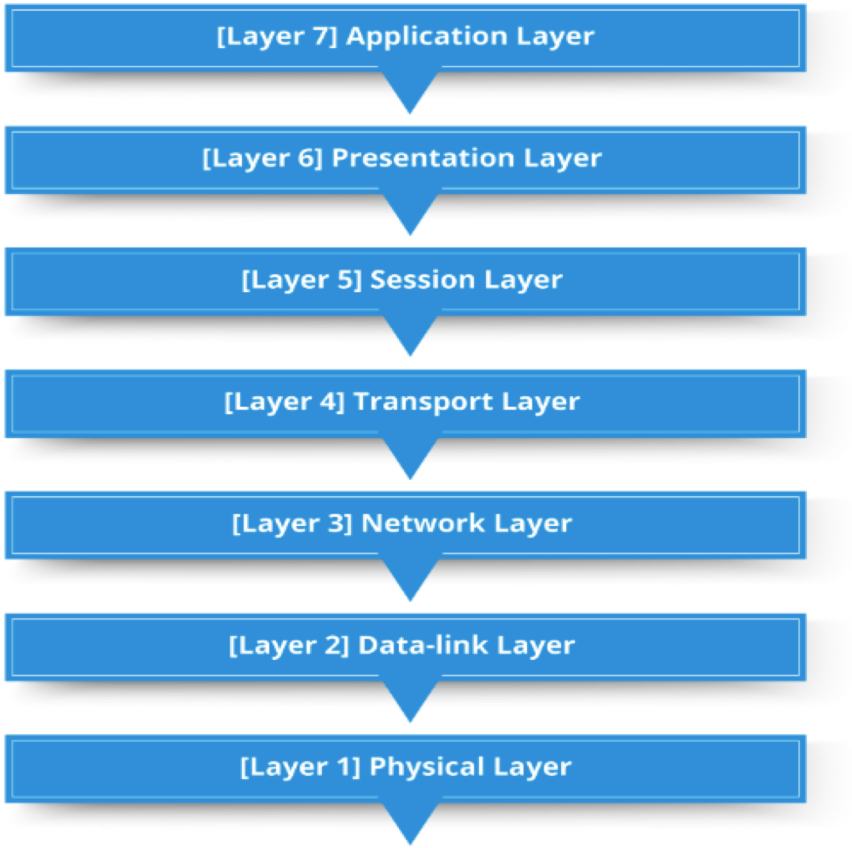
Each such level operates on the incoming data in a pre-defined way and passes on the data to the next level

Why does one need Layering ?

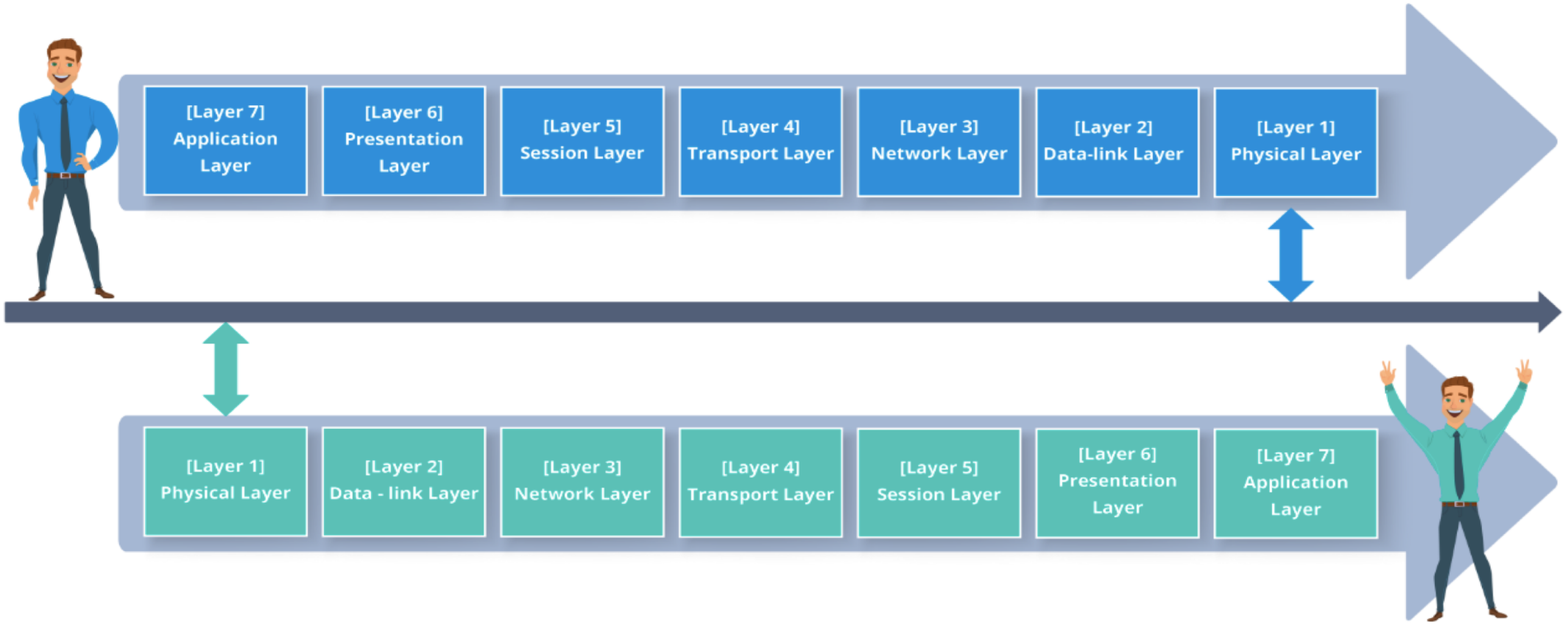
Layering helps by breaking a bigger complex task into smaller manageable units(Layers) of processing

ISO – OSI Reference Model – Overview

Open Systems Interconnection (OSI) is a set of internationally recognized, non-proprietary standards for networking & for operating system involved in networking purposes



OSI Reference Model – Flow



OSI – Model

FTVETI

ICT @ FTVETI

Layer 1 – Physical Layer

- **Physical Layer**
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Binary Transmission: Wires, Connectors, Voltages , Data Rates

- It is the first (lowest) layer of the OSI model
- Converts bits (0/1) into electronic-signals for outgoing messages
- Converts electronic signals into bits (0/1) for incoming messages
- Physical layer manages the interface between the computer and the physical medium of the network
- Physical layer constitutes the foundation for the driver software of the units such as NICs (Network Interface Cards)

Layer 2 – Data Link Layer

- Physical Layer
- **Data Link Layer**
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Media access: provides reliable data transfer via media; physical address, network topology, flow control & error notification

- Handles special data frames (packets) between the Network layer and the Physical layer
- At the receiving end, this layer converts raw-data coming from the physical layer (Layer1) into data frame format, to be passed on further to the Network layer
- At the sending end this layer converts the data frames into raw-data format which gets passed on further to the Physical layer (Layer1)

Layer 3 – Network Layer

- Physical Layer
- Data Link Layer
- **Network Layer**
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Addressing and best traversal path: Provides connectivity & path selection; routing domain

- Manages “addressing” for the messages to be delivered
- Performs transaction of logical network addresses & names into their physical equivalents
- Decides routing of network traffic between computers
- Manages packet switching & deals with network traffic congestion

Layer 4 – Transport Layer

- Physical Layer
- Data Link Layer
- Network Layer
- **Transport Layer**
- Session Layer
- Presentation Layer
- Application Layer

End to end connections: manages data transportation between hosts, establish, maintain & terminate virtual circuits; info flow control; error detection & recovery

- Enables transmission of data across a network
- Performs Segmentation of long data units into smaller segments called as packets (usually based on the bandwidth / allowed packet size for the involved medium of transmission)
- Assembles & performs sequencing of data chunks arriving at the receiver
- Provides confirmation of successful transmissions and signals for resending the erroneous data packets
- The transport layer enables the transfer of a message between the processes

Layer 5 – Session Layer

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- **Session Layer**
- Presentation Layer
- Application Layer

Communication between hosts: Establishes, maintains & terminates logical sessions between apps

- Helps in identifying and managing a communication channel (termed as a session) between two devices over a network
- Applications on either end of the session are able to communicate for the duration of the valid session
- Responsible for initiating, maintaining and terminating sessions
- Responsible for security and access control to session information (via session participant identification)
- Responsible for synchronization services, and for checkpoint services

Layer 6 – Presentation Layer

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- **Presentation Layer**
- Application Layer

Representation of data: Ensures that the data is readable by the receiving system; manages format of the data & its structure & syntax for application layer

- Manages data-format information (acts as a translator)
- For outgoing messages, it converts data into a generic format for network transmission; for incoming messages, it converts data from the generic network format to a format that the receiving application can understand
- Presentation layer is responsible for : protocol conversions, data encryption/decryption, or data compression/decompression
- A special software facility called a “redirector” operates at this layer . It determines if a request is network related or not and forwards network related requests to an appropriate network resource

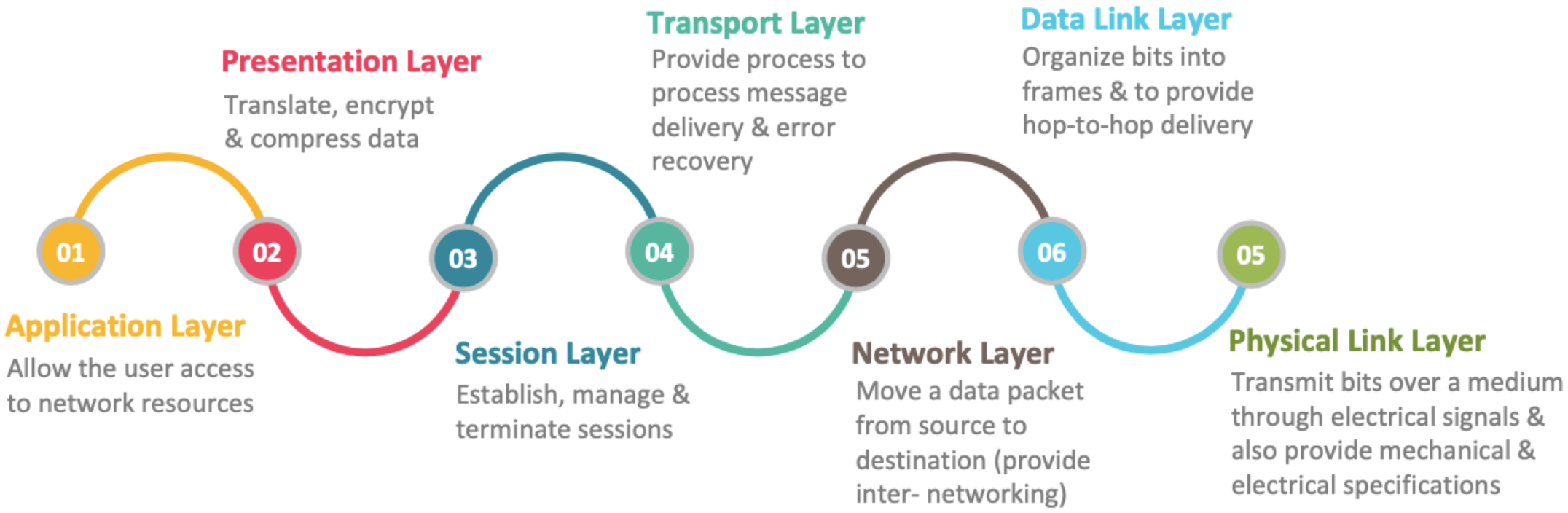
Layer 7 – Application Layer

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

Network Processes to Applications: Provides network services to application processes ex. Email, Terminal Emulation, File transfer and so on

- The top layer of the OSI model
- Provides a set of interfaces for sending and receiving applications & to use network services, such as:
  - Message handling
  - Database query processing
- Application layer is responsible for providing services to the end-user

Summary


01
Application Layer
Allow the user access to network resources
02
Presentation Layer
Translate, encrypt & compress data
03
Session Layer
Establish, manage & terminate sessions
04
Transport Layer
Provide process to process message delivery & error recovery
05
Network Layer
Move a data packet from source to destination (provide inter- networking)
06
Data Link Layer
Organize bits into frames & to provide hop-to-hop delivery
05
Physical Link Layer
Transmit bits over a medium through electrical signals & also provide mechanical & electrical specifications

Protocol Data Unit (PDU)

Data: This is a generic term that is often used in describing protocols that function at higher levels, usually the network layer and up

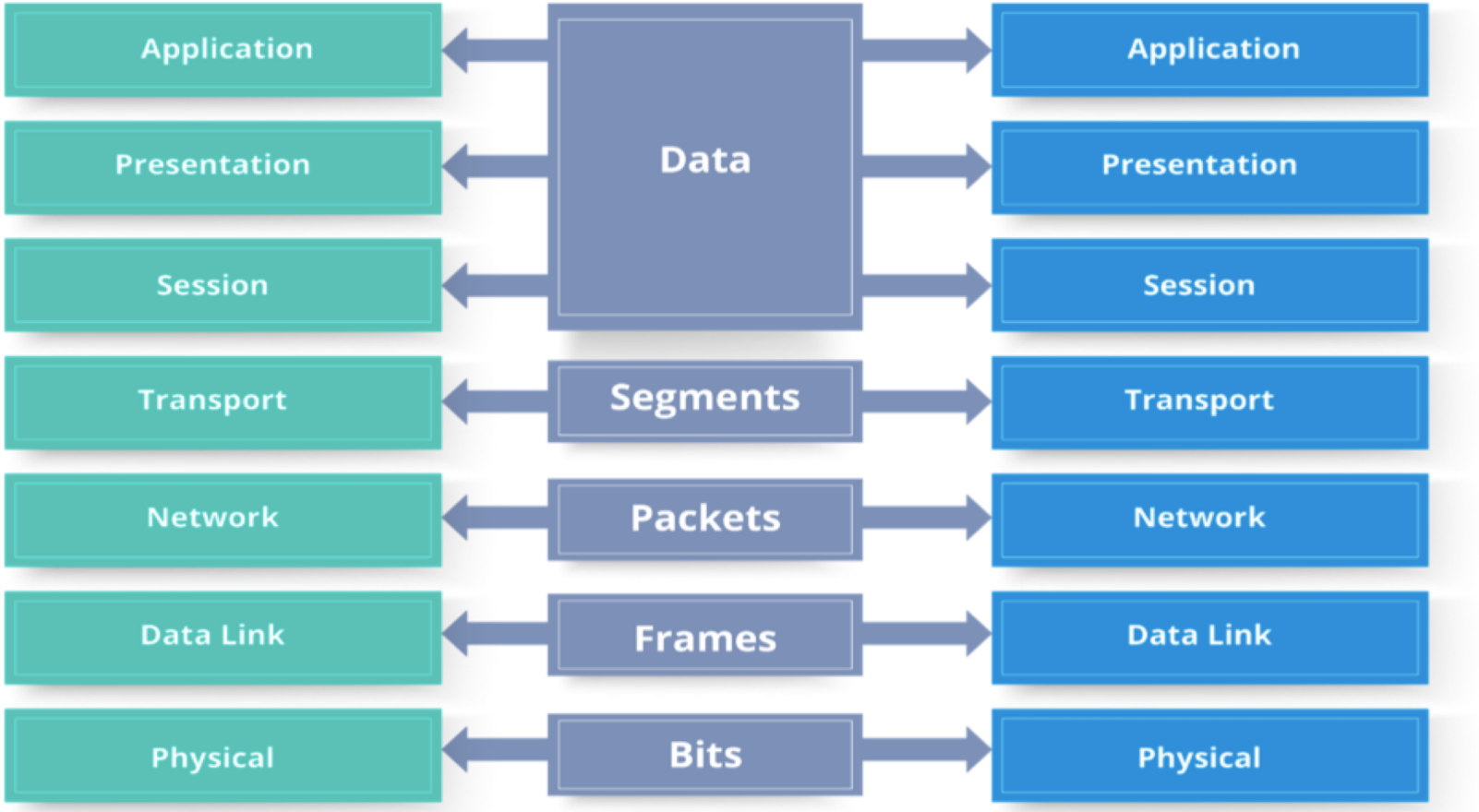
Segments: Chunk of data that has been prepared for transmission TCP (Transmission Control Protocol). Usually a segment is a chopped or manageable 'data stream'

Packets: Stream of binary octets of data of some arbitrary length, typically used to describe chunks of data created by software components

Frame: Bunch of data created by network communication hardware, ex: NIC (network interface cards), router interfaces at Data Link Layer

Bits: 0/1 - electronic signals

Peer To Peer Communication

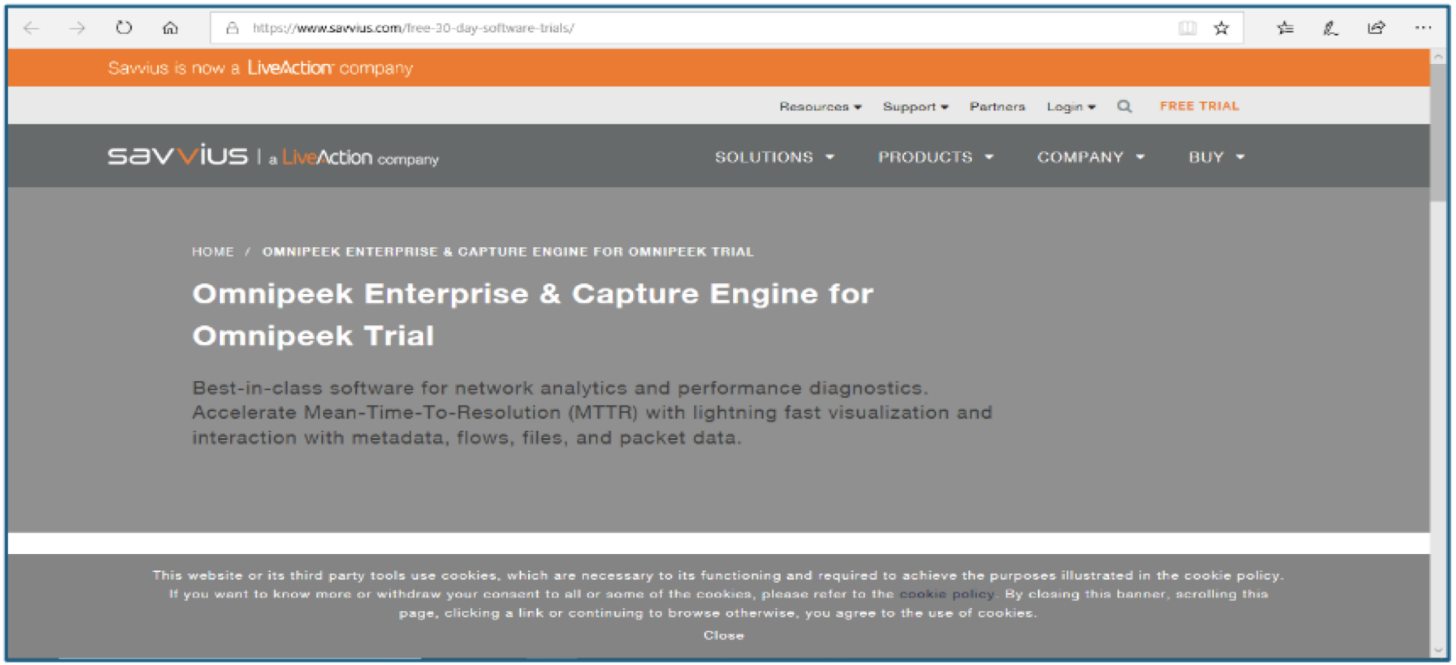


OSI Layer – Functions

OSI Layers	Function	Data Type	Protocols	Devices
Application Layer	Allows access to network services that support Applications, Handles network access, Flow control & error recovery	User Data	DNS, NFS, BOOTP, DHCP, SNMP, TFTP, HTTP	Gateway
Presentation Layer	All different formats from all sources are made into a common uniform format that the rest of the OSI model can understand	Encoded User Data	SSL, MIME	Gateway
Session Layer	Manages who can transmit data at a certain time and for how long	Sessions	NetBIOS, Sockets, Named Pipes, RPC	Gateway
Transport Layer	Additional connection below the session layer, manages the flow control of data between parties across the network, provides flow control and error-handling	Datagram/ Segments	TCP/UDP	Gateway, Brouter
Network layer	Translates logical network address and names to their physical address. Logical Addressing; Routing; Datagram Encapsulation; Fragmentation and Reassembly; Error Handling and Diagnostics	Datagram/ Packets	IPv4 , IPv6	Brouter, Router, Frame relay device
Data link layer	Handles data frames between the Network and Physical layers	Frames	Ethernet, IEEE 802.2 LLC , IEEE 802.11	Bridge, Switch
Physical Layer	Transmits Raw bitstream over Physical cable, Defines cables, cards, and physical Aspects, Defines NIC attachments to hardware, how cable is attached to NIC. Encoding and Signalling; Physical Data Transmission Hardware Specifications; Topology and Design	Bits	IEEE 802.2 , ISDN	Repeater, Multiplexer , Hub

Demo 1: Sniffer

- Sniff the network communication using **OmniPeek Network Analyzer** tool
- Scan the network, explore various options of the tool and generate a scan report
- Download and install OmniPeek Network Analyzer tool from the URL: https://www.savvius.com/free-30-day-software-trials/



So, the OSI concept is clear now. In order to enable computers to share resources across a network we require a collection of multiple protocols, which is know as TCP/IP. Let's see it in detail

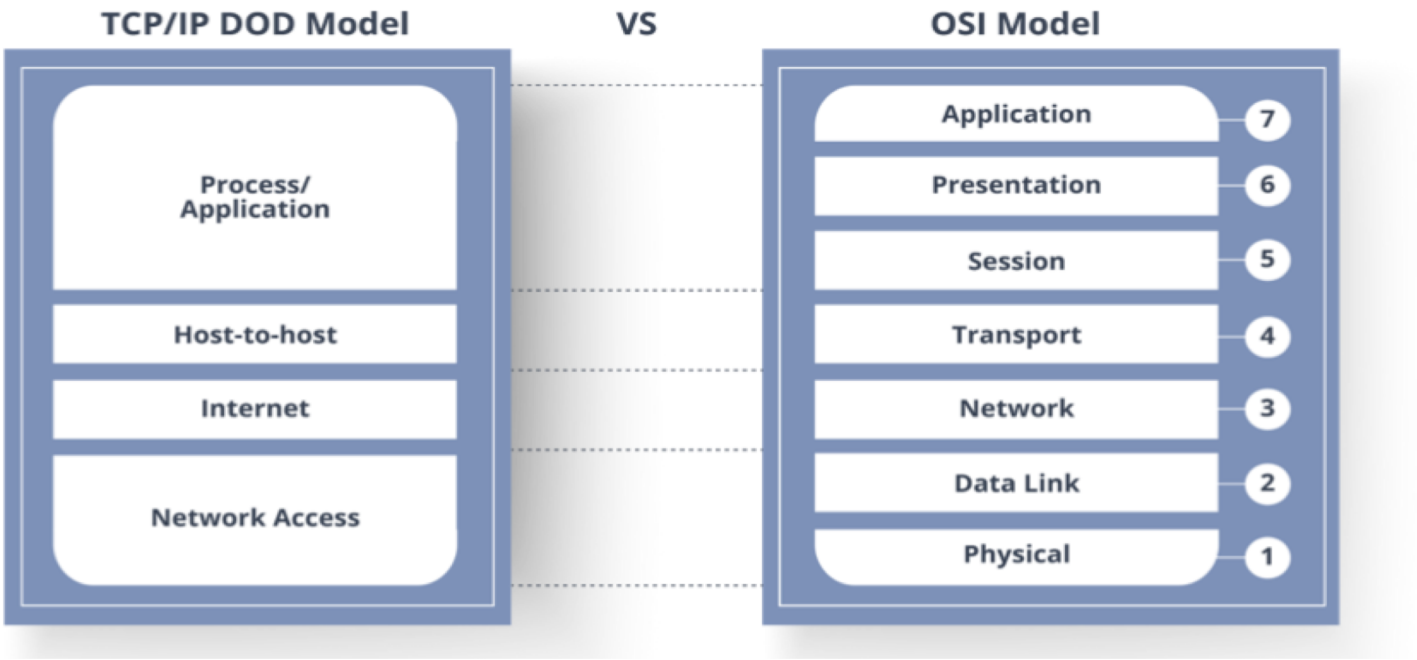
TCP/IP

What Is TCP/IP

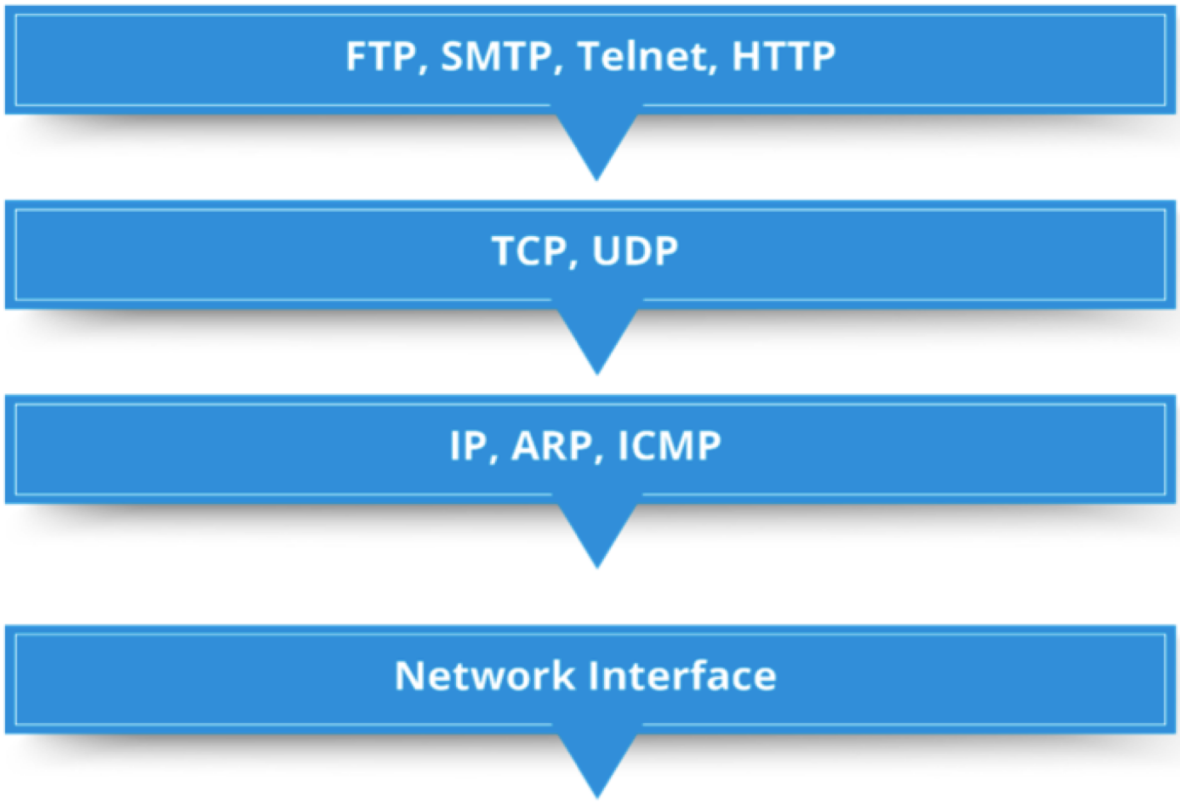
- TCP/IP is a collection of multiple protocols, which collectively enable computers to share resources across a network
- TCP stands for “Transmission Control Protocol”. IP stands for “Internet Protocol”
- They are Transport layer and Network layer protocols respectively of the protocol suite
- The most well known network that adopted TCP/IP is Internet – the biggest WAN in the world
- TCP/IP was developed very early & widely available to the public for free via RFC
- TCP/IP was developed earlier than the OSI 7-layer reference model , it does not have 7 layers but only 4 layers

TCP/IP – OSI layers (mapping)

The diagram shows a mapping (equivalence) of TCP/IP layers with corresponding OSI model



TCP/IP Stack



TCP/IP: Application Layer

- The protocols at this layer, help defining the rules for implementation of network applications
- This layer is dependent on lower layers for accuracy and efficiency of delivered data

FTP – File Transfer Protocol	• For file transfer
Telnet – Remote terminal protocol	• For remote login on any other computer on the network
SMTP – Simple Mail Transfer Protocol	• For mail transfer
HTTP – Hypertext Transfer Protocol	• For web browsing

TCP/IP: Transport Layer

- Transport layer forms a set of protocols in IP suite
- The protocols within the transport layer offer host to host communication services, for applications
- Services provided by it are : reliability, multiplexing, connection-oriented communication and flow control

TCP : Transmission Control Protocol

- TCP is a connection-oriented protocol
- TCP provides the function to allow a connection that virtually exists – also called virtual circuit
- TCP provides the functions:
  - Division of data into smaller pieces
  - Reassembly segments into the original chunk
  - Provide further the functions such as reordering and data resend
  - Offering a reliable byte-stream delivery service

UDP : User Datagram Protocol

- UDP provides datagrams & is transaction-oriented
- UDP is suitable for simple query-response protocols
- UDP is simple and powers trivial protocols such as the DHCP and FTP
- UDP is usually not meant for reliable and sequential communication
- Lack of reliability burden qualifies UDP for real time applications such as VOIP, online streaming
- UDP is most suitable for in unidirectional communication & for unidirectionally broadcasting information

TCP/IP: Internet Layer

- Internet Layer is a collection of specifications, methods & protocols in the IP suite primarily responsible for transportation of packets from one host to another (over network boundaries)
- Internet layer protocols use IP-based packets.

IPv4

IPv4 uses 32-bit addresses which limits the address space to 2^32 = 4,294,967,296 addresses

IPv6

IPv6 uses 128bit addressing scheme. Hence the total address space is 2^128 = Approx. 3.4×10^38 addresses

TCP/IP: Link Layer

- Link layer is the lowest layer in the Internet Protocol (IP) Suite (which is the networking architecture of the Internet)
- The link layer comprises of functions & communication protocols that only operate on the connected physical link for a given host
- The link layer is used to interconnect nodes or hosts in the network
- Link protocol is a suite of methods & standards that operate only between adjacent network nodes of a LAN segment or a WAN connection
- Link layer corresponds to a combination of the data link layer (layer 2) and the physical layer (layer 1) in the OSI model
- The layers of TCP/IP are high level enumerations of operating scopes (application, hosttohost, network, link) & not the underlying details of networking technologies, operating procedures, data formats and so on

TCP/IP: Link Layer

ARP – Address Resolution Protocol

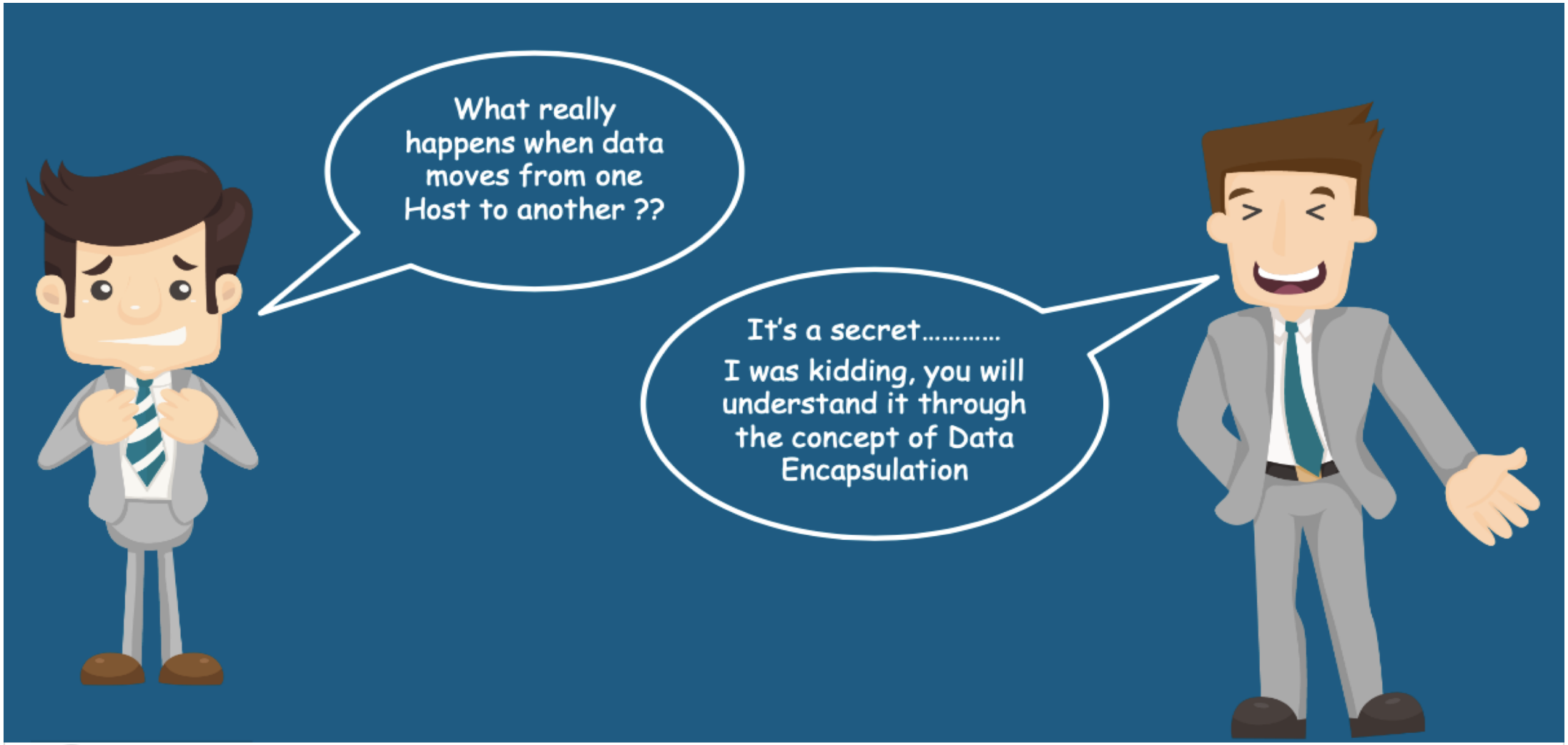
- **ARP** looks for the hardware address (Media Access Control (MAC) address) of a host – from its known IP address
- ARP maintains a cache (table) in which a mapping of MAC addresses to IP addresses is stored

BGP – Border Gateway Protocol

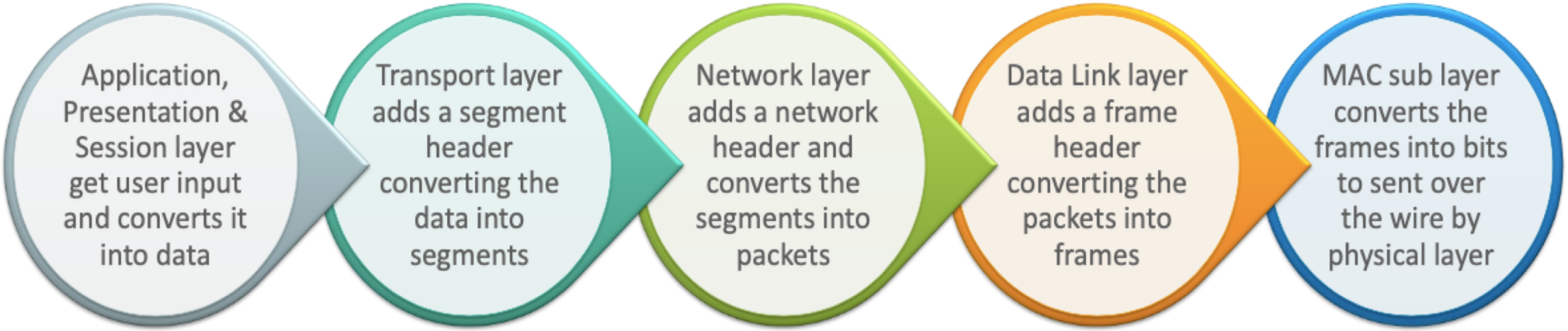
- **Border Gateway Protocol** (BGP) is a routing protocol used to exchange data & information between different networked systems
- BGP maintains routes to various hosts, networks & gateway routers on which the routing decisions are made
- BGP is often referred to as a "reachability protocol"

Demo 2: IP Address

- Monitor your public and local IP address using **IP watcher**
- Check online statues of IP address
- Generate an alert for change in IP address
- Download IP Watcher tool from the link below: https://www.gearboxcomputers.com/products/ip-watcher/


What really happens when data moves from one Host to another ??
It's a secret.....
I was kidding, you will understand it through the concept of Data Encapsulation

Data Encapsulation

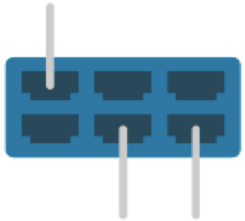


There are various network devices which operates at various levels, let's go through that

Network Devices

Network Devices

Repeater



Hub

Bridge

Router

Gateway

Switch

FTVETI

ICT @ FTVETI

Repeater

- Repeater
- Hub
- Bridge
- Router
- Gateway
- Switch

Layer of Operation: Physical

- Revives the weakening signal over the network
- Repeaters do not usually amplify (enlarge) the signal
- Weak signals get bitwise copied & regenerated at original strength
- It is typically a 2 ports device

Layer 2 – Data Link Layer

- Repeater
- **Hub**
- Bridge
- Router
- Gateway
- Switch

Layer of Operation: Physical

- Fundamentally it is a repeater with multiple ports
- It usually can not find the best route to be used for data packets
- Types of Hubs:
  - **Active Hub:** Possesses inbuilt power supply. It cleans up (de-noise) , enhances & transmits the signal along the network. Typically, used to extend the net distance between networked nodes
  - **Passive Hub:** Hubs which get lines from nodes and power supply from active hub; no cleaning and enhancement of signals and can not typically be used for the purpose of extending the distance between the nodes

Layer 3 – Network Layer

- Repeater
- Hub
- Bridge
- Router
- Gateway
- Switch

Layer of Operation: Data-Link

- A bridge is similar to a repeater and has an ability to filter just the required content based on 'MAC addresses' of the source & destination
- Used for bridging 2 different LANs typically operating on the same protocol.
- A bridge has one input and output port each (2 port device)
- Types of Bridges
  - Transparent Bridges
  - Source Routing Bridges

Layer 4 – Transport Layer

- Repeater
- Hub
- Bridge
- Router
- Gateway
- Switch

Layer of Operation: Network

- Routers directs data packets on the basis of their IP addresses.
- Interconnects LANs & WANs with each other
- Consists of a routing table which gets updated on the fly (dynamically)
- The routing table is referred to for making data routing decisions by a Router

Layer 5 – Session Layer

- Repeater
- Hub
- Bridge
- Router
- **Gateway**
- Switch

Layer of Operation: Any Layer from layers 3 – 7

- Gateway connects 2 networks, that may be working on different underlying networking models
- Performs the role of an interpreter between two systems
- Often referred to as 'protocol converters'
- Typically capable of operate at most of the network layers
- Gateways possess more complexity as compared to switches / routers

Layer 6 – Presentation Layer

- Repeater
- Hub
- Bridge
- Router
- Gateway
- Switch

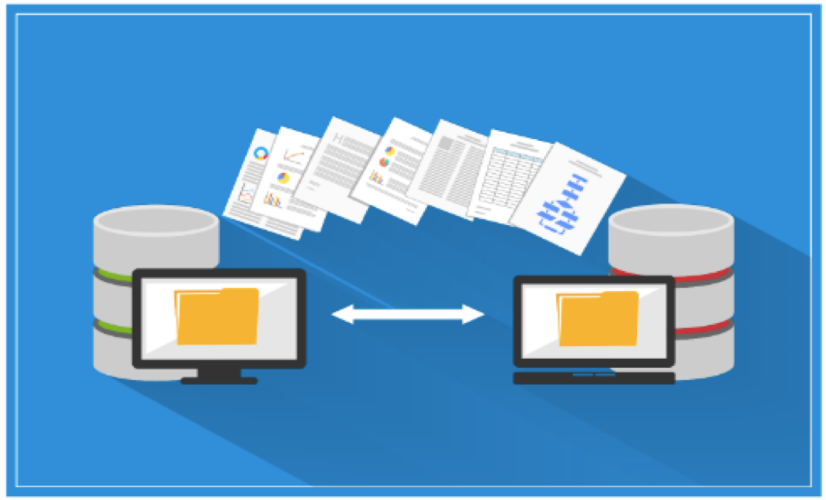
Layer of Operation: Data-Link

- Switch is fundamentally a bridge with multiple ports
- It has a buffer and designed in a way that elevates its efficiency & performance.
- Usually is capable to perform error-checking before forwarding the input data ahead.
- Switches are efficient due to the quality of blocking the erroneous packets & capability of selective forwarding of good packets

Network Protocols & Security Viewpoint

ICT @ FTVETI

What Is A ‘Protocol’ ?



- A protocol is a collection of rules, procedure, sequence etc. for two devices to communicate and exchange information
- A protocol typically also specifies the format in which the data gets exchanged

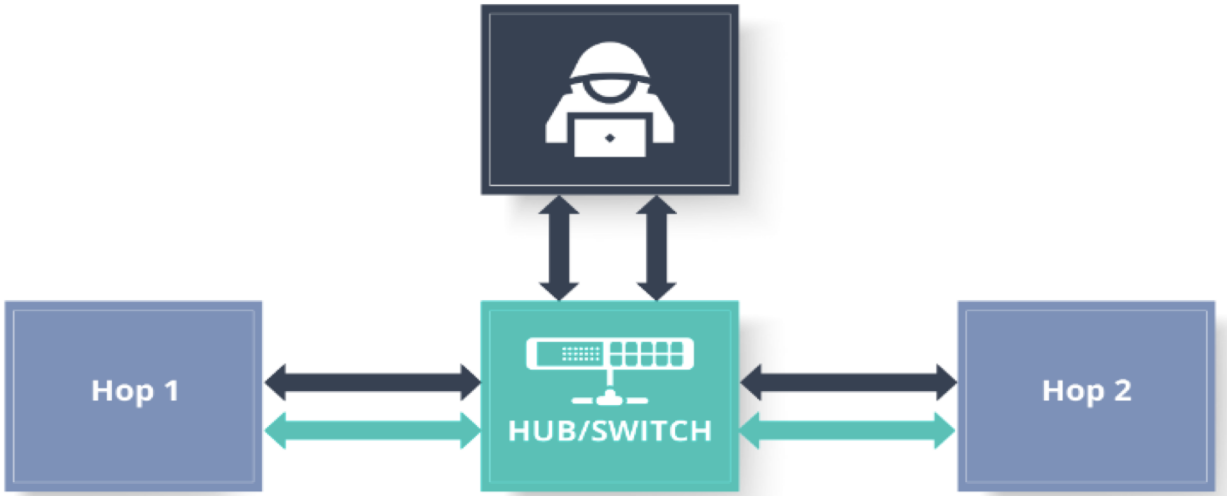
OSI Model Layers & Information Exchange

- The 7 OSI layers use different forms of “control information” (consisting of specific requests & instructions) to exchange information with their adjacent layers
- Control information typically has two formats: **headers** and **trailers**
- Headers & Trailers are respectively attached to data chunks that needs to be passed down from upper layers
- **Example:** At the network layer, an information unit comprises of a Layer3 header & data. Further (at the data link layer i.e. Layer 2), all the information sent by the network layer (combination of the Layer 3 control information along with the data) is deliberated as a ‘data unit’

ARP (Address Resolution Protocol)

- ARP is responsible for IP – MAC (Media Access Control) resolution
- Sender's Data Link Layer Invokes ARP. It gives "destination IP address" to ARP protocol
- ARP broadcasts a frame requesting "MAC ID" of the required destination with it's destination IP address
- The correct destination computer responds with it's own MAC ID [Uses RARP – Reverse ARP]
- The Sender can use the shared "MAC ID" for sending data
- ARP cacheing is done & stored temporarily (in ARP table locally)

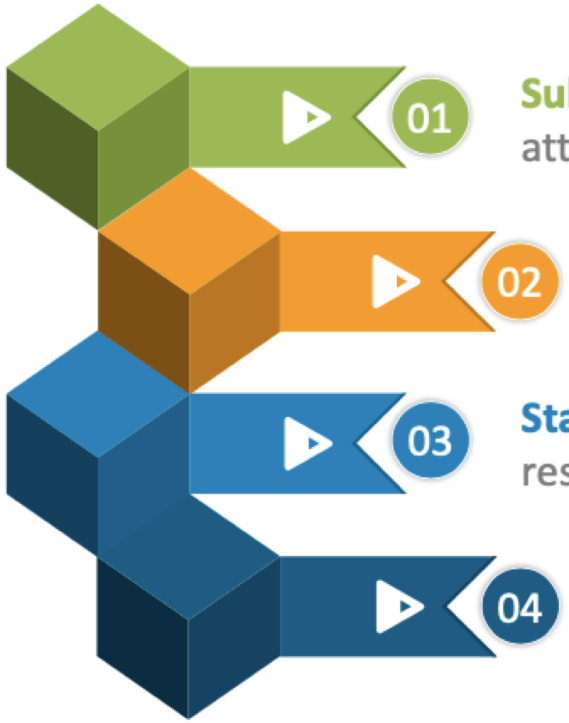
ARP – Attacker's View



Attacker's View

- An attacker may alter ARP table this is called as ARP poisoning
- Attacker's goal is to receive packets intended to be received by an another computer (MITM: Man in the middle)

ARP – Solution To Attacker's View



Subnetting: A well designed & segregated network is effective against an ARP poison attack to prevent the attack on the local LAN communication

Encryption: It is possible to sniff (obtain) Encrypted traffic but being encrypted it can not be deciphered

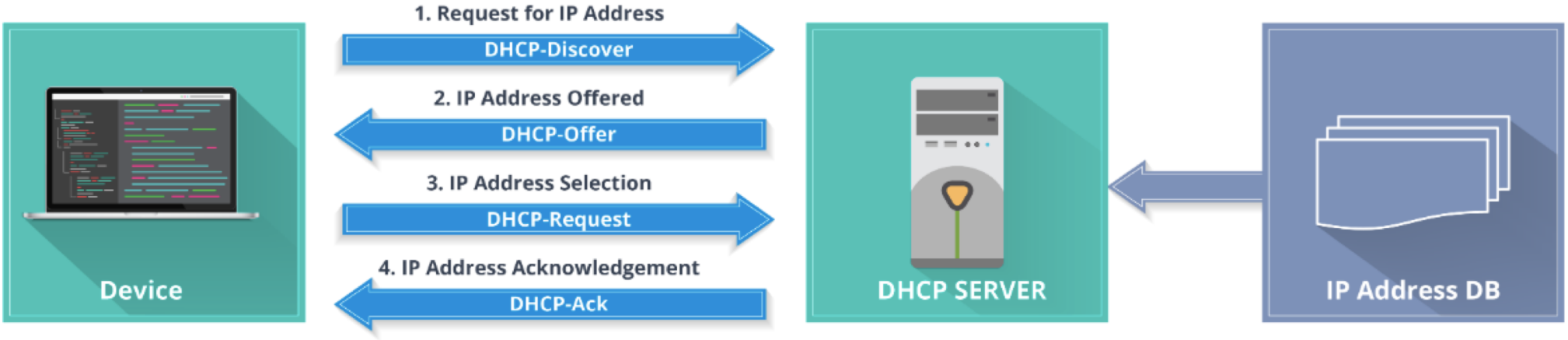
Static ARPs: ARP table written statically doesn't need to be updated through request/ response

HIDS (Host based Intrusion Detection Systems): IDS embedded in routers, are likely to detect massive ARP requests thereby assisting in blocking the attack

DHCP (Dynamic Host Configuration Protocol)

- The Dynamic Host Configuration Protocol (DHCP) is a protocol meant for network management (addressing)
- A DHCP server dynamically allocates an IP address along with a few other network configuration parameters to the requesting device on a network
- The DHCP server creates & maintains a database of IP addresses and provides an address to a DHCP-enabled client while it comes up on a network
- As the IP addresses are dynamically leased, they no longer remain in use and get automatically assigned back to the database for further re-assignment when requested

DHCP Process



DHCP – Attacker's View & Solution

Attacker's View

- An attacker may attempt to respond to DHCP requests and trying to list himself (spoof) as the "default gateway" or "DNS server". Hence, initiating a man in the middle attack
- This is called as DNS Spoofing Attack
- Rogue DHCP servers usually get exploited for "man in the middle" (MITM) or "denial of service" (DOS) attacks
- One of the most common attack scenarios is - an insider plugging in a consumer-grade router at his desk, without being mindful of the fact that the device being connected in a DHCP server itself

Solution

- **DHCP snooping :** It is a security mechanism working at Layer2, typically embedded into the OS (operating system) of a good network switch. It is effective in dropping undesirable DHCP traffic
- DHCP snooping primarily prevents an unauthorized (rogue) DHCP server to offer IP addresses to the DHCP clients connected onto the network

ICMP (Internet Control Message Protocol)

- ICMP is included in the IP (Internet Protocol) suite
- Network devices (including routers) use ICMP to send operational & error messages. For example, messages for situations while a demanded service remains inaccessible or a host or router being pinged remains not reachable
- ICMP is deliberated a part of the IP layer. In the context of TCP/IP – based layered network, ICMP is usually considered as Layer – 3 protocol
- Since IP suite does not have a way for sending error/ control messages, ICMP is relied upon to provide an error control
- ICMP is used for reporting – errors & queries for network management
- Messages: Source quench | Time exceeded | Parameter problem | Destination un-reachable | Redirection message

ICMP – Attacker's View & Solution

Attacker's View

- **Smurf Attack**
  - A hacker typically spoofs(changes) the source address of an ICMP packet
  - It then transmits it over to all the devices over that network
  - In case the networking devices fail to filter this traffic, such a malicious traffic is broadcast to all computers in the network
  - The victim's network becomes overloaded with traffic, which affects the productivity of the entire network
- **Fraggle Attack:** Fraggle attack is analogous to the Smurf attack, except the fact that in Fraggle attack, UDP protocol is used whereas ICMP is used in Smurf

Solution

- Usage of filters on routers & firewall to counteract address spoofing:
  - An IP address should be assigned to a LAN segment, and if the IP address of the source machine is not in the range of IP address that is assigned to the segment, then the traffic should be dropped
  - Put filters on Layer3 devices so that it does not reply to broadcast address

Common Network Threats/Attacks

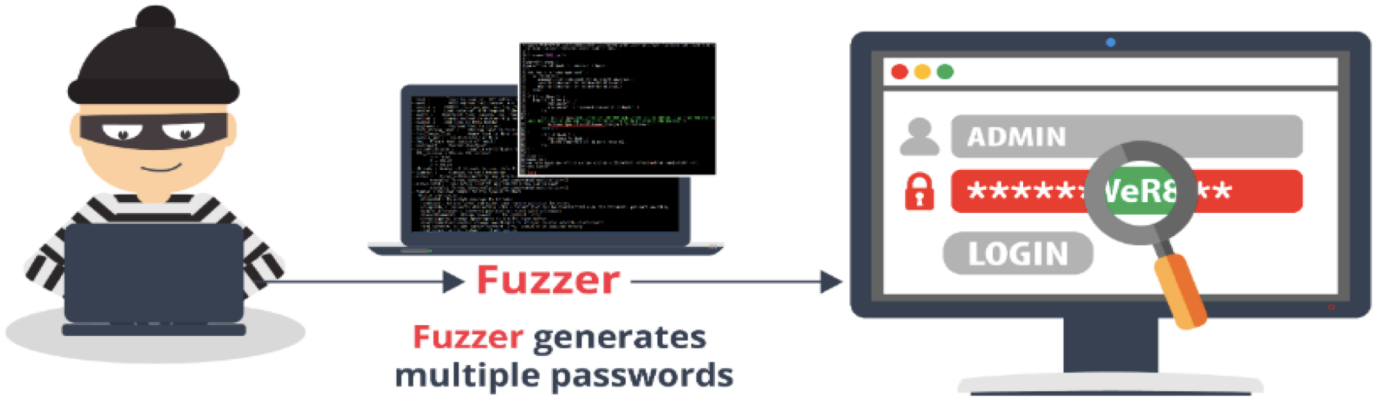
FTVETI

ICT @ FTVETI

Browser Based Attacks

- In such attacks, a machine is compromised through a web browser which being most commonly used way for accessing internet
- These attacks are often performed via authentic websites which have known vulnerabilities (especially to the attacker)
- Attackers breach the site and infect it with malicious scripts or processes
- When users try to access the infected website via the web browser, it attempts to run the malicious code onto the users' systems by taking advantage of the vulnerabilities in their browsers
- Common mitigations include regular security patching of browsers, system & browser hardening , wise usage of browser extensions & addons and usage of a reputed and updated anti-malware solution

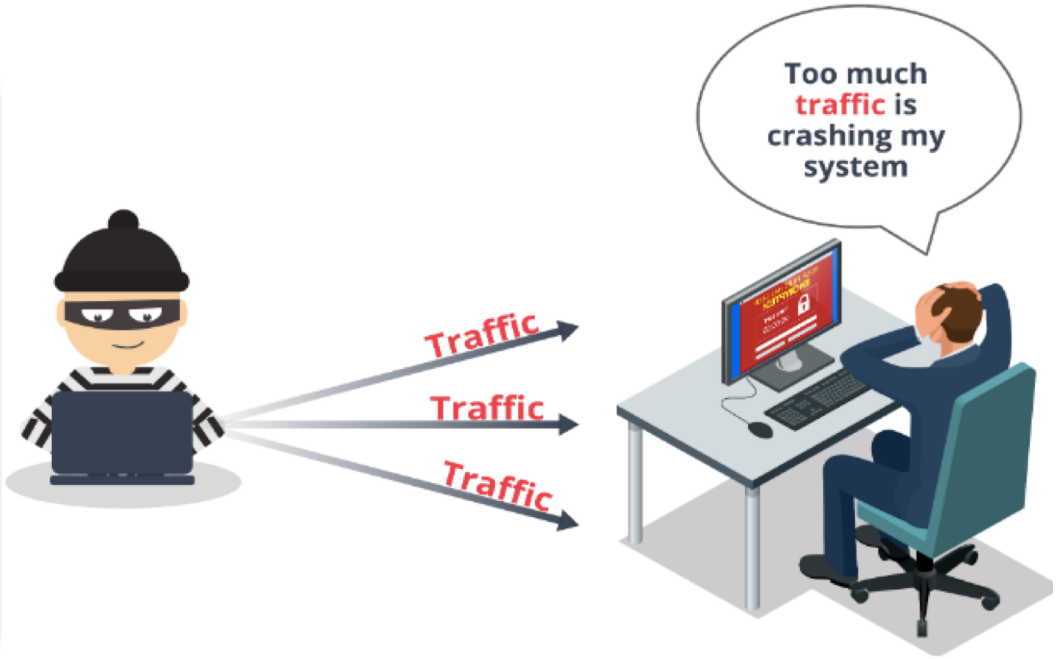
Brute Force Attacks



- Here, the attacker tries to determine the password for a target (service/system/device) through a permutation or fuzzing process
- As it is a lengthy task, attackers usually employ a software such as fuzzer, to automate the process of creating numerous passwords to be tested against a target
- In order to avoid such attacks – password best practices should be followed, mainly on critical resources like servers, routers, exposed services and so on

Denial-of-Service (DoS) Attacks

- DoS attacks primarily try to "overwhelm" a target – such as websites, FTP / DNS / NTP servers and so on – with floods of traffic. These attacks aim at slowing down or crashing the target, thereby impacting its availability
- **DDOS (Distributed Denial of Service)** is a special form of DOS where the attack could be performed through multiple attack points. However, the goal is the same. DDOS is more effective and difficult to mitigate
- DDoS is sometimes used as a distraction mechanism to divert the security team's focus from an additional major attack being covertly carried out
- Network Segmentation, Implementation of Load balancers, Firewalls and DDOS protection solutions are some of the ways to keep DOS attacks at bay



Malware Attacks

- Usually malwares are triggered out of some user activity such as
  - Plugging in a malicious USB device
  - Inadvertently downloading a malicious attachment over the email
  - Browsing infected or phished websites
- Malware is (bad) software application that has been created to harm, hijack, lock or spy on the infected systems
- Three common ways in which it spreads include: **Phishing emails**, **malicious websites**, **malvertising**
- Use of Anti-phishing solutions, Email Security Gateways, Email Sandboxing solutions, Browser integrated Anti-malware solutions etc prevents Malware attacks to some extent. However in addition appropriate system hardening and user awareness is vital for keeping Malware attacks at bay

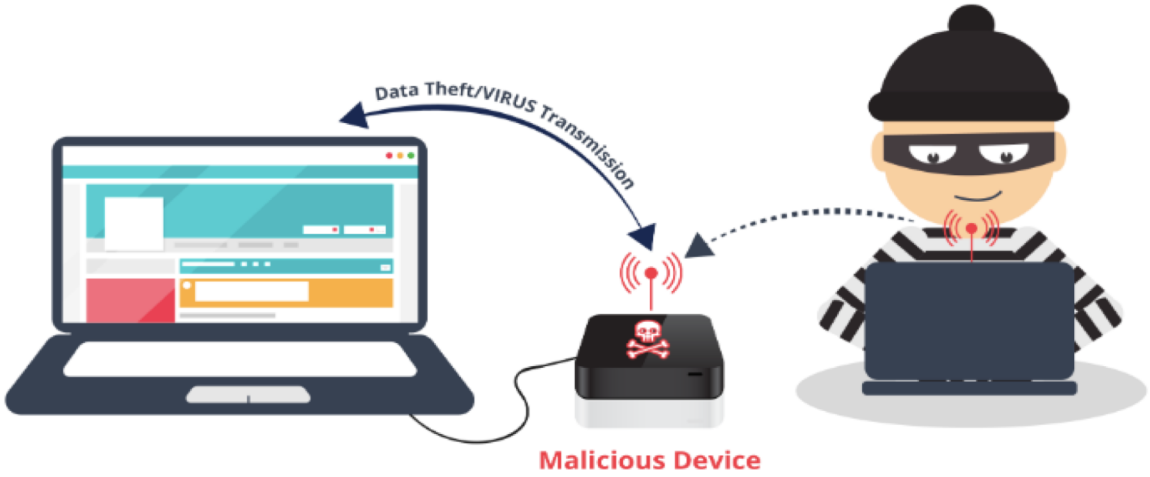
Worm Attacks

- Malwares with a capability of propagate by themselves and do not require a user activity for getting triggered are known as **Worms**
- Usually, worms take advantage of system vulnerabilities in order to proliferate over networks
- **Ex:** WannaCry, a famous Ransomware outbreak in Year 2017, swiftly attacked multiple machines globally by exploiting a rampant Windows vulnerability. Once a machine got infected, the malware recursively searched the connected network to locate and attack other connected vulnerable machines
- To prevent or contain an outbreak of work attacks a combination of preventive techniques such as System Hardening, Security Patching, Usage of HIDS / HIPS, Anti-Malware, Process monitoring systems and sound network design via proper segmentation and firewalls is the key

Web Application Attacks

- Public facing web services, such as web-applications & databases are very common victims of network security attacks
- Most common web application attacks apart from **DOS & DDOS** are:
  - Cross-Site Scripting (XSS)
  - SQL Injection (SQLi)
  - Path Traversal

Physically Triggered Attacks



- Attempts to steal systems physically. Ex: Theft of devices such as laptops or tablets for unauthorized usage
- Insertion of Rogue malicious devices into corporate network for either inserting a malware, running scans or finding vulnerabilities
- Placing rogue network enabled webcams into corporate network with an intension of espionage Or reputation damage in public. Such attacks usually are performed by an insider who already has some trust & access within the target system

Scan Attacks

- Attackers typically use opensource tools for scanning & finding public-facing systems in order to gather details about the services along with the security controls in place
- This is often a reconnaissance phase carried out before actual attack
- **Usage of Port scanner:** Port Scanner is a tool employed to decipher open network ports on a target system. Different types of port scanners are available out of which some allow going silent
- **Usage of Vulnerability scanner:** This tool scans & gathers information on a target. It then compares the obtained information with a set of known security vulnerabilities thereby resulting in a list of known vulnerabilities found on the system along with their severity
- Scanning is a recon activity which from preventive angle should minimize the revelation of data / configuration / vulnerabilities of a given system /service /network. This can be achieved to some extent by appropriate system configuration hardening , firewalls and usage of honeypots (Deception Technique)

Quiz #1

- HTTPS is a secured protocol working at which TCP/IP Layer?
  a. Link Layer
  b. Internet Layer
  c. Application Layer
  d. Transport Layer

Answer #1

- HTTPS is a secured protocol working at which TCP/IP Layer?
  a. Link Layer
  b. Internet Layer
  c. **Application Layer**
  d. Transport Layer

Answer c:
Explanation: HTTPS works on Application Layer!

Quiz #2

- A component (software/hardware) that checks information coming from the Internet & depending on the applied filters and configuration settings either allows or prevents it to pass through is called:
  a. Router
  b. Firewall
  c. Intrusion detection system
  d. Anti-Virus

Answer #2

- A component (software/hardware) that checks information coming from the Internet & depending on the applied filters and configuration settings either allows or prevents it to pass through is called:
  a. Router
  b. Firewall
  c. Intrusion detection system
  d. Anti-Virus

Answer b:
Explanation: Only Firewall does the said job

Quiz #3

- A network service which allows clients to make indirect network connections to other network services is called as:
  a. NAC (Network Access Control)
  b. Proxy
  c. Network Load balancer
  d. C&C Backdoor

Answer #3

- A network service which allows clients to make indirect network connections to other network services is called as:
  a. NAC (Network Access Control)
  b. Proxy
  c. Network Load balancer
  d. C&C Backdoor

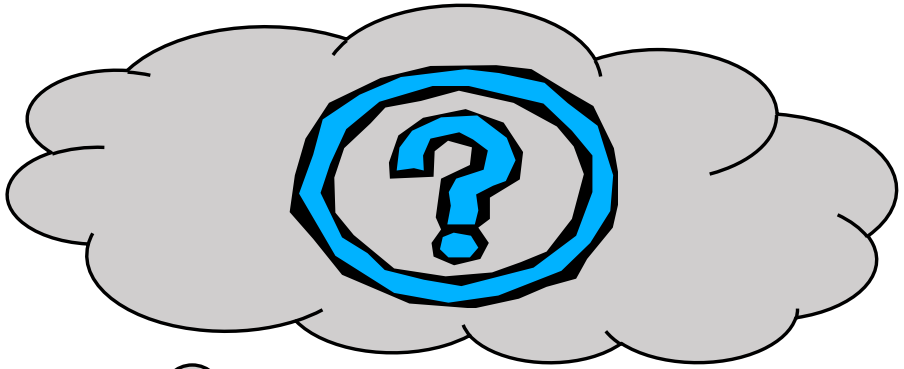
Answer b:
Explanation: A proxy is used to make indirect network connections. Usually it is a legitimate device-in-the-middle & works as a silent watchman. Proxy logs are thus very useful for various security incident response processes

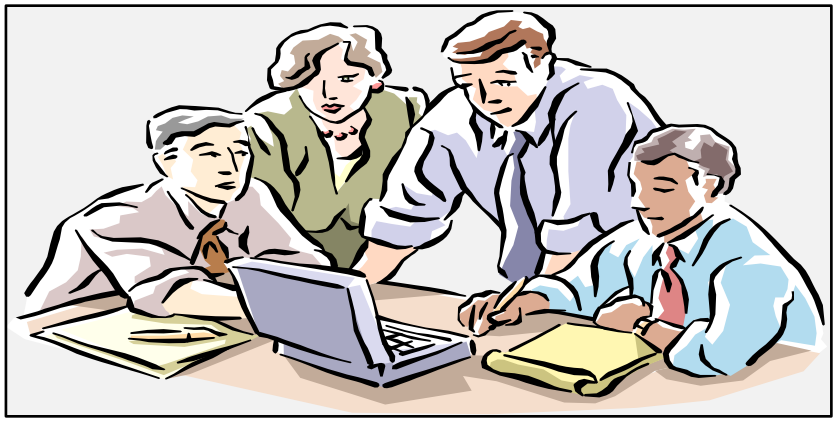
Summary

In this unit, you should have learnt:

- Layered Network architecture
- OSI Model and various TCP/IP Protocols
- Network Devices
- Network security risks & basic mitigation techniques

QUESTIONS PLEASE ☺





FTVETI

ICT @ FTVETI