Week 1 Portfolio

# TCP/IP:

TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.

TCP/IP functionality is divided into four layers, each of which include specific protocols.

*The application layer* provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol ([HTTP](http://searchwindevelopment.techtarget.com/definition/HTTP)), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol ([SMTP](http://searchexchange.techtarget.com/definition/SMTP)) and Simple Network Management Protocol ([SNMP](http://whatis.techtarget.com/definition/Simple-Network-Management-Protocol-SNMP)).

*The transport layer* is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol ([UDP](http://searchsoa.techtarget.com/definition/UDP)), which is sometimes used instead of TCP for special purposes.

*The network layer*, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol ([ICMP](http://searchnetworking.techtarget.com/definition/ICMP)), which is used for error reporting.

*The physical layer* consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol ([ARP](http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP)).

TCP/IP is nonproprietary and, as a result, is not controlled by any single company. Therefore, the internet protocol suite can be modified easily. It is compatible with all operating systems, so it can communicate with any other system. The internet protocol suite is also compatible with all types of computer hardware and networks.

# DNS:

Domain Name Servers (DNS) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses.  
This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.   
Information from all the domain name servers across the Internet are gathered together and housed at the Central Registry. Host companies and Internet Service Providers interact with the Central Registry on a regular schedule to get updated DNS information.   
When you type in a web address, e.g., www.jimsbikes.com, your Internet Service Provider views the DNS associated with the domain name, translates it into a machine friendly IP address (for example 216.168.224.70 is the IP for jimsbikes.com) and directs your Internet connection to the correct website.   
After you register a new domain name or when you update the DNS servers on your domain name, it usually takes about 12-36 hours for the domain name servers world-wide to be updated and able to access the information. This 36-hour period is referred to as propagation.

# Network Topology:

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

-BUS: Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

Advantages:

1. It is cost effective.
2. Cable required is least compared to another network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages:

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

-RING: It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Advantages:

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages:

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

-STAR: In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.

Advantages:

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages:

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

-MESH: t is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

Routing

Flooding

Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those nodes etc. We can even have routing logic, to re-configure the failed nodes.

Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of

**Partial Mesh Topology:**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

**Full Mesh Topology:**Each nodes or devices are connected to each other.

Advantages:

Each connection can carry its own data load.

It is robust.

Fault is diagnosed easily.

Provides security and privacy.

Disadvantages:

Installation and configuration is difficult.

Cabling cost is more.

Bulk wiring is required.

-TREE: It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Advantages:

Extension of bus and star topologies.

Expansion of nodes is possible and easy.

Easily managed and maintained.

Error detection is easily done.

Disadvantages:Heavily cabled.

Costly.

If more nodes are added maintenance is difficult.

Central hub fails, network fails.

-HYBRID: It is two different types of topologies which is a mixture of two or more topologies. For example, if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Advantages:

Reliable as Error detecting and troubleshooting is easy.

Effective.

Scalable as size can be increased easily.

Flexible.

Disadvantages:

Complex in design.

Costly.

# Subnet:

Subnetting is the process of stealing bits from the HOST part of an IP address to divide the larger network into smaller sub-networks called subnets. After subnetting, we end up with NETWORK SUBNET HOST fields. We always reserve an IP address to identify the subnet and another one to identify the broadcast address within the subnet. In the following sections you will find out how all this is possible.

**Conservation of IP addresses:** Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.

**Reduced network traffic:** The smaller networks created the smaller broadcast domains are formed hence less broadcast traffic on network boundaries.

**Simplification:** Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

STEP 1: Convert to Binary

STEP 2: Calculate the Subnet Address

To calculate the Subnets IP Address you need to perform a bit-wise AND operation (1+1=1, 1+0 or 0+1 =0, 0+0=0) on the host IP address and subnet mask. The result is the subnet address in which the host is situated.

 STEP 3: Find Host Range

We know already that for subnetting this Class C address we have borrowed 5 bits from the Host field. These 5 bits are used to identify the subnets. The remaining 3 bits are used for defining hosts within a subnet.

The Subnet address is identified by all 0 bits in the Host part of the address. The first host within the subnet is identified by all 0s and a 1. The last host is identified by all 1s and a 0. The broadcast address is the all 1s. Now, we move to the next subnet and the process is repeated the same way. The following diagram clearly illustrates this process:

STEP 4: Calculate the Total Number of Subnets and Hosts Per Subnet

Knowing the number of Subnet and Host bits we can now calculate the total number of possible subnets and the total number of hosts per subnet. We assume in our calculations that all-zeros and all-ones subnets can be used. The following diagram illustrated the calculation steps.

# FTP:

FTP may run in active or passivemode, which determines how the data connection is established. In both cases, the client creates a TCP control connection from a random, usually an unprivileged, port N to the FTP server command port 21.

# TFTP:

**Trivial File Transfer Protocol** (**TFTP**) is a simple [lockstep](https://en.wikipedia.org/wiki/Lockstep_(computing)) [File Transfer Protocol](https://en.wikipedia.org/wiki/File_Transfer_Protocol) which allows a [client](https://en.wikipedia.org/wiki/Client_(computing)) to get a file from or put a file onto a remote [host](https://en.wikipedia.org/wiki/Host_(network)). One of its primary uses is in the early stages of nodes booting from a [local area network](https://en.wikipedia.org/wiki/Local_area_network). TFTP has been used for this application because it is very simple to implement.

TFTP was first standardized in 1981[[1]](https://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol#cite_note-1) and the current specification for the protocol can be found in [RFC 1350](https://tools.ietf.org/html/rfc1350).

Uses port 21 like FTP but is based on UDTP that uses port 69