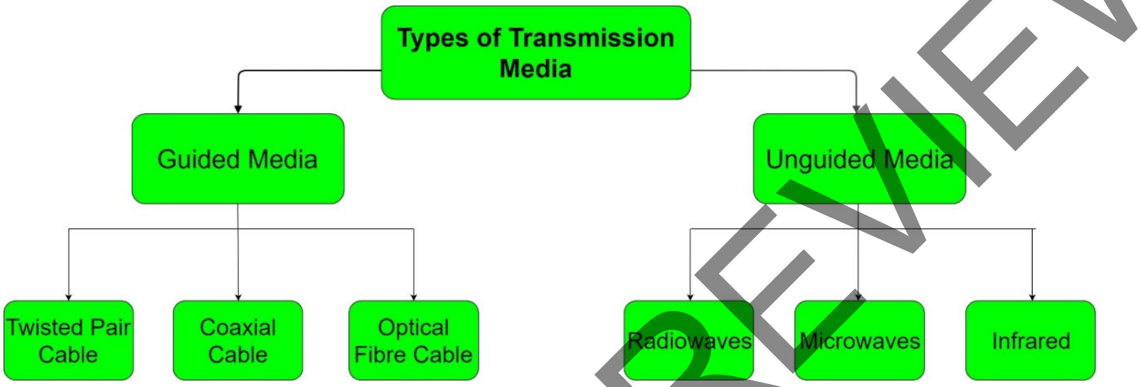
Contents

Chapter 2: Signal Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver. It is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types,



Guided Media

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

Twisted Pair

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. **Unshielded Twisted Pair (UTP):**
   This type of cable can block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

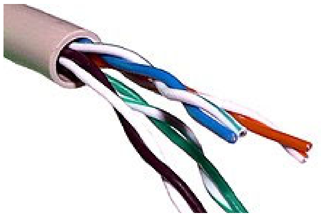


Figure 8: Unshielded twisted pair

Advantages of Unshielded Twisted Pair

Chapter 4: Connect Two Remote Devices

Computing devices have come a long way over the last years. The modern family now has become mobile in the sense that now they have smartphones, tablets and various other gadgets with rich networking capabilities. Now, it's easy for them to do home networking and remote access a computer with IP address.

Public Switched Telephone network (PSTN)

The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones.

The features of a PSTN are:

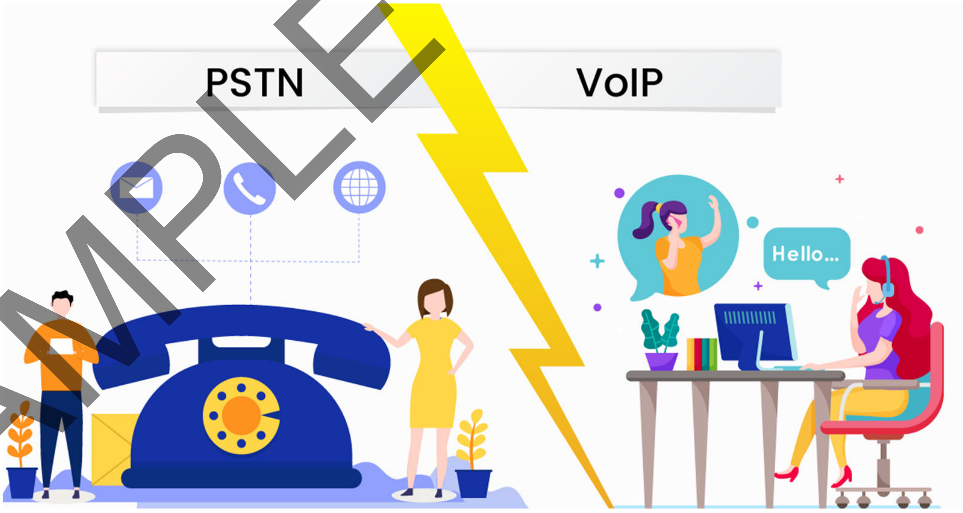


Figure 33: PSTN and VoIP

- Subscribers can be connected by entering telephone numbers
- The existing connections are primarily used to transmit speech information
- After hanging up the connection is closed and the resources used become available to other subscribers

Switch

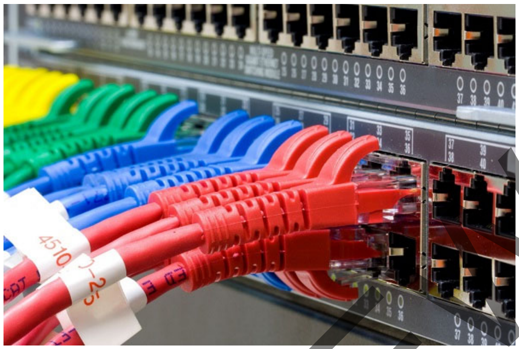


Figure 47: Network cables connected to a switch

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Figure 48: Switch

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. You can think of a switch as a device that has some of the best capabilities of routers and hubs combined. A switch can work at either the Data Link layer or the Network layer of the OSI model. A multilayer switch is one that can operate at both layers, which means that it can operate as both a switch and a router. A multilayer switch is a high-performance device that supports the same routing protocols as routers.

Switches can be subject to distributed denial of service (DDoS) attacks; flood guards are used to prevent malicious traffic from bringing the switch to a halt. Switch port security is important so be sure to secure switches: Disable all unused ports and use DHCP snooping, ARP inspection and MAC address filtering.

Router

Figure 49: Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking

Subnetting Questions

Question 1:

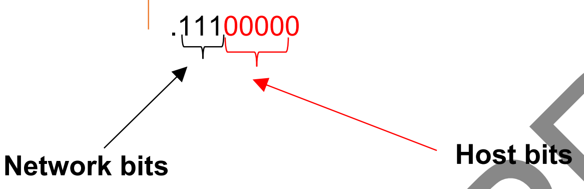
Class C network 192.168.10.0 with subnet mask 255.255.255.224. Calculate the followings

1. Number of subnets

First write the default subnet mask of class C subnetworks and then write the subnet mentioned in the questions as shown below.

255.255.255.0

255.255.255.224



Number of subnet bits (network bits) = 3

If you know number of subnet bit you can find number of subnets using following equation.

$\boldsymbol{Number\ of\ Subnets = 2^s}$ (s = number of subnet bits)

Therefore,

$$\boldsymbol{Number\ of\ subnets = 2^3 = 8}$$

2. Number of hosts per network

Number of host bits = 5

If you know the number of host bits you can find the number of hosts using the following equation.

$\boldsymbol{Number\ of\ Hosts = 2^h - 2}$ (h = number of host bits)

Therefore,

$$Number\ of\ hosts = 2^5 - 2 = 30\ hosts$$

3. Valid IP address range

First, we find the 2 to the power of number of host bits. (here the number of host bits = 5, already calculated in the above section)

$$2^5 = 32$$

Here the IP address is given as 192.168.10.31. The first address range can write as follows.

192.168.10.0 – 192.168.10.31

Network address **Broadcast address**

First address range → 192.168.10.0 – 192.168.10.31

Second address range → 192.168.10.32 – 192.168.10.63

Third address range → 192.168.10.64 – 192.168.10.95

4. What is the network address and broadcast address of the first range?

192.168.10.0 – 192.168.10.31

Network address is first address in the network and it is used for identification network segment.

Network address = 192.168.10.0

Broadcast address is the last address in the network, and it is used for addressing all the nodes in the network at the same time.

Broadcast address = 192.168.10.31

5. What are the first and last usable addresses in the first address range?

192.168.10.0 and 192.168.10.31 are used for network address and broadcast address. Therefore, those addresses cannot assign to a host. Then the next address after the network address is the first usable address in here.

First usable address → 192.168.10.1

The address before the broadcast address is the last usable address in this range

Last usable address → 192.168.10.30

6. The last usable address in the first address range

We have to assign last address of a range for the Broadcast address. Therefore after allocating last IP address, the IP address before the last is 199.100.10.62

The last usable IP address of the range $199.100.10.0 - 199.100.10.63$ is,

199.100.10.62

7. The broadcast IP address

The first address range is ,

$$199.100.10.0 - 199.100.10.63$$

The Broadcast address is the last address of the given address range. Therefore,

$$\boldsymbol{Broadcast\ address} \rightarrow \mathbf{199.100.10.63}$$

Question 3

Calculate the following for a network which is having 120 hosts

1. Subnet mask

Here we need 120 hosts for the network. Then we need to find the actual number of required hosts by adding 2 to the hosts. 120+2 = 122 hosts. (The two is added for the network address and the broadcast address)

Then we need to get the nearest power of two greater than 122. It is simple and easy. The nearest value is 128. To write 128 as a binary number we need 7 bits. Then we allocate 7 bits as 0000000 in the subnet. The rest of the bits are mentioned as 1s.

$$11111111.11111111.11111111.1\underbrace{0000000}_{\text{7 bits are allocated to the hosts}}$$

Now let's write above value in decimal form,

$$255.255.255.128$$

Therefore the subnet mask equals to $\mathbf{255.255.255.128}$

- It can be used to establish a connection between two computers.

Disadvantages of TCP/IP

Here, are few drawbacks of using the TCP/IP model:

- TCP/IP is a complicated model to set up and manage.
- The shallow/overhead of TCP/IP is higher-than IPX (Internetwork Packet Exchange).
- In this, model the transport layer does not guarantee delivery of packets.
- Replacing protocol in TCP/IP is not easy.
- It has no clear separation from its services, interfaces, and protocols.

Differences between OSI and TCP/IP Models

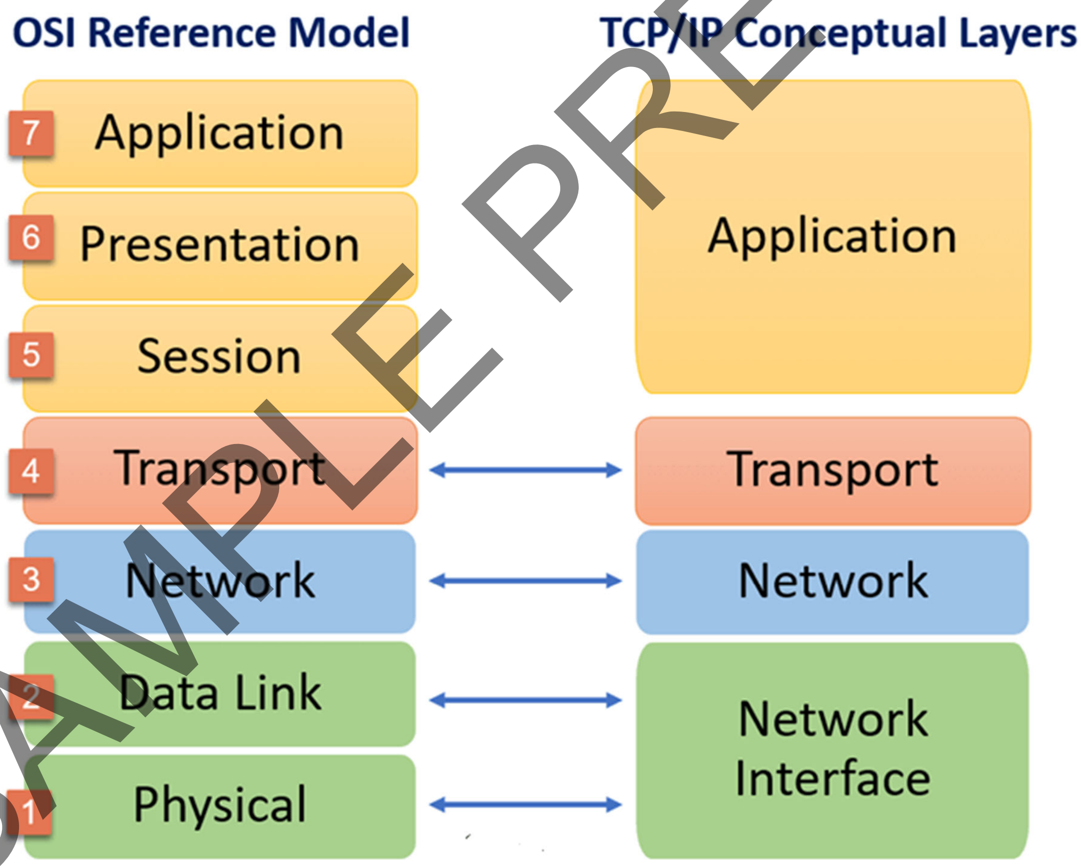


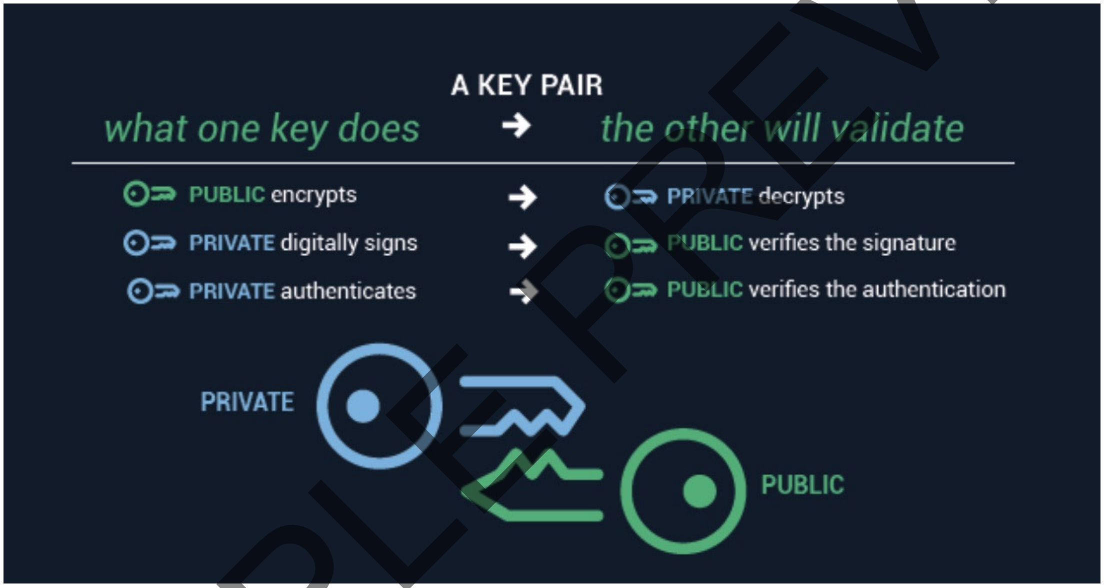
Figure 99: OSI vs TCP/IP

The above diagram depicts how the layers of OSI Reference Model and TCP/IP Reference Model Maps. Now let's discuss some major differences between OSI Reference Model and TCP/IP Reference Model.

- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Private Key

Unlike the publicly accessible public key, the private key is a secret key known only by its owner, with the private key and public key paired such that the recipient can use the corresponding key to decrypt the cipher text and read the original message.



A KEY PAIR

what one key does → the other will validate

PUBLIC encrypts → PRIVATE decrypts

PRIVATE digitally signs → PUBLIC verifies the signature

PRIVATE authenticates → PUBLIC verifies the authentication

Figure 104: Private Key

Private keys are generated using the same algorithms that create public keys to create strong keys that are bonded mathematically.

"A symmetric encryption method that uses the same secret key to encrypt and decrypt data. See also encryption, key, public key encryption, and security."

Summary Public key cryptography

Public key cryptography provides the basis for securely sending and receiving messages with anyone whose public key you can access.

Public keys enable:

- Users to encrypt a message to other individuals on the system direct access to the internet. Therefore, an email server will be built or placed inside the DMZ in order to interact with and access the email database without directly exposing it to potentially harmful traffic.

- FTP servers: These can host critical content on an organization's site, and allow direct interaction with files. Therefore, an FTP server should always be partially isolated from critical internal systems.

A DMZ configuration provides additional security from external attacks, but it typically has no bearing on internal attacks such as sniffing communication via a packet analyzer or spoofing via email or other means.

DMZ Designs

There are numerous ways to construct a network with a DMZ. The two major methods are a single firewall (sometimes called a three-legged model), or dual firewalls. Each of these system can be expanded to create complex architectures built to satisfy network requirements:

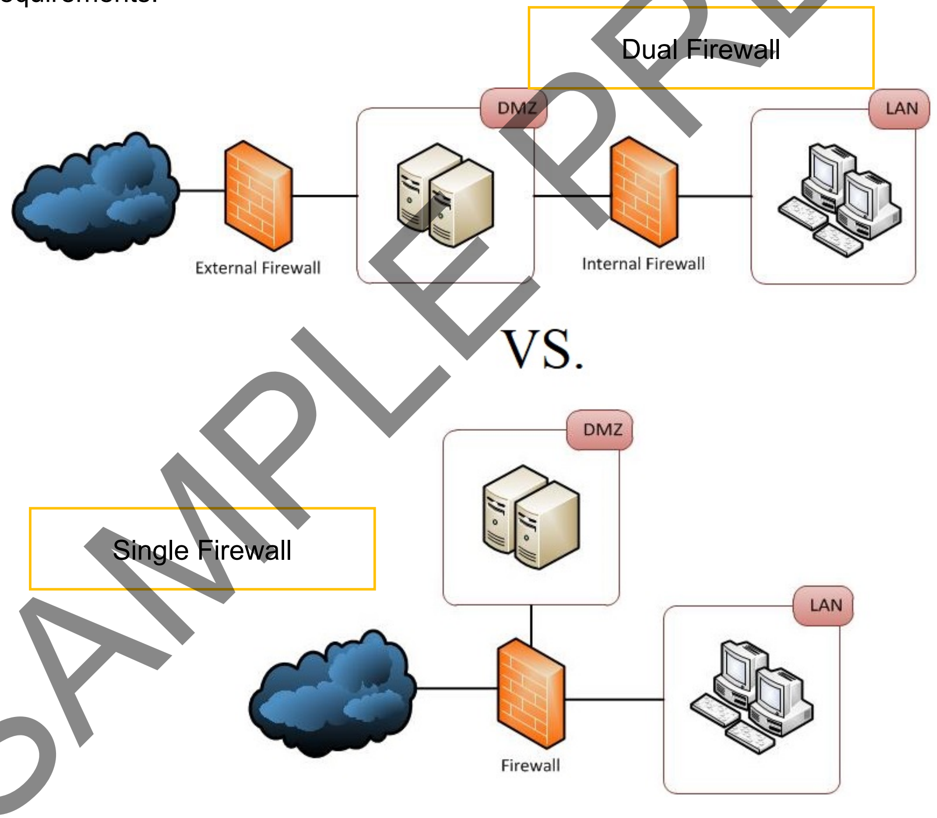


Figure 118: Single Firewall vs Dual Firewall

- Single firewall: A modest approach to network architecture involves using a single firewall, with a minimum of 3 network interfaces. The DMZ will be placed Inside of this firewall. The tier of operations is as follows: the external network device makes