Digital Assignment-1

ALokam Nikhitha

19BCE2555

ISM - (CSE3502)

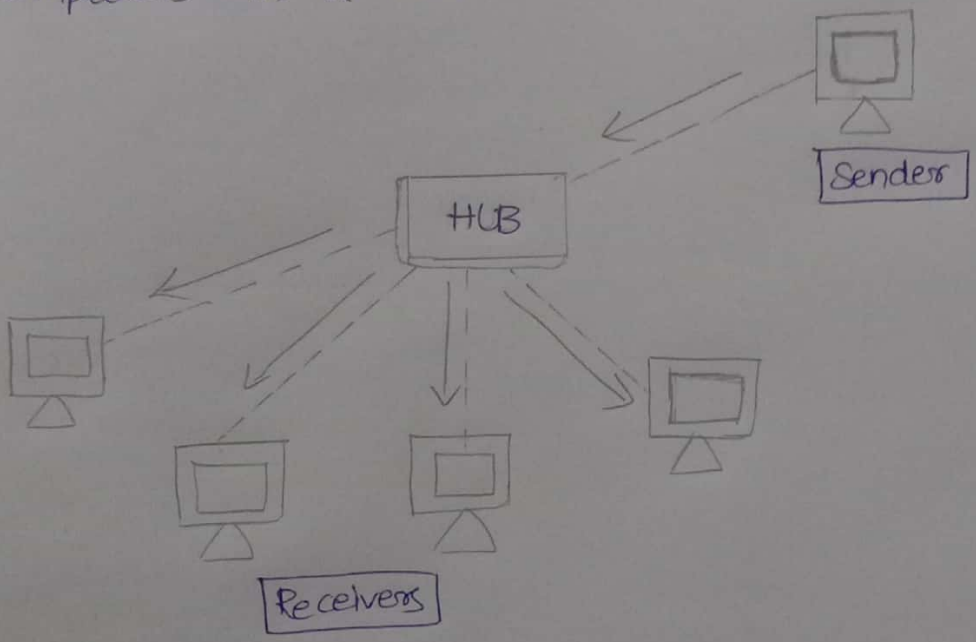
Digital Assignment

19BCE2555

Description of the listed devices.

Hub:

A Hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

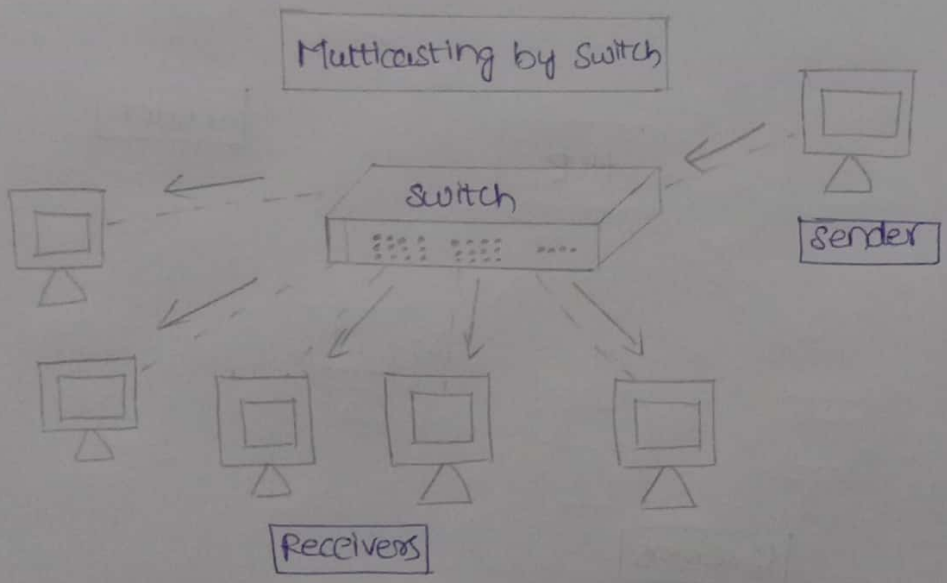


They operate in physical layer of the OSI model. It is an non-intelligent network device that sends message to all ports. It primarily broadcasts messages. Transmission models is half duplex. Collisions may occur during the setup of transmission when more than one computers place data simultaneously in the corresponding ports. They are passive devices, they don't have any software associated with it. They generally have fewer ports of 4/12.

19BCE2555

Switch:

Switches are networking devices operating at layer 2 or a datalink layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network



It uses MAC address to send packets to selected destination ports. It uses packet switching technique to receive and forward datapackets from source to the destination device. It supports unicast and broad cast communications. Transmission mode is full duplex Switches are active devices equipped with network software and network managment capabilities. The number of ports are higher - 24/48.

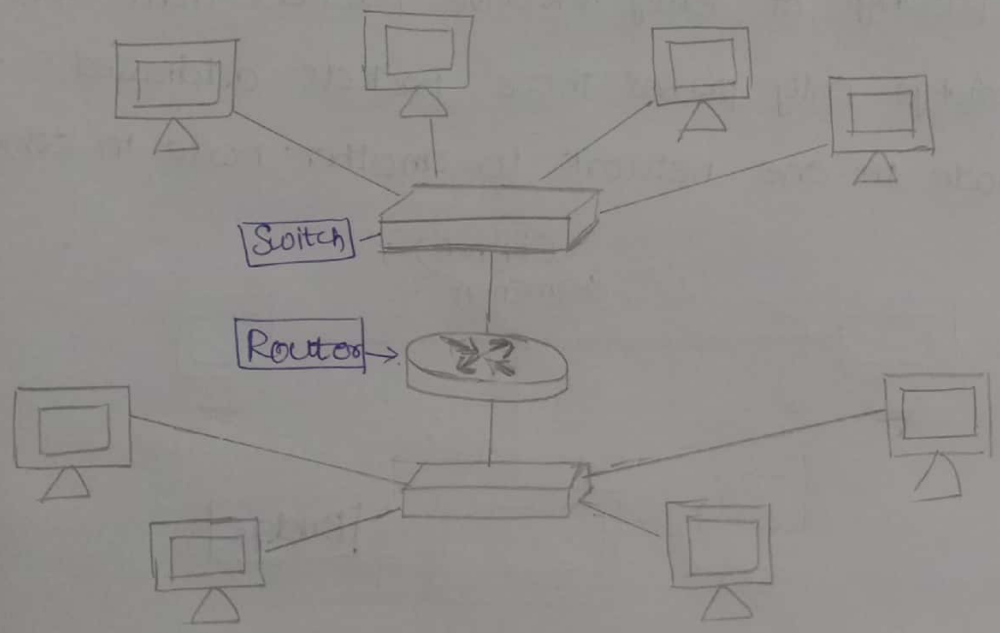
Different types of switches:

Unmanaged switches, Managed switches, LAN switch, PoE switch are different types.

19BCE2555

Router:

A router is a switching device for networks, which is available to route network packets, based on their address, to other networks or devices. Among other things, they are used for Internet acess, for coupling network or for connecting branch offices to a central office via VPN (Virtual Private Network)



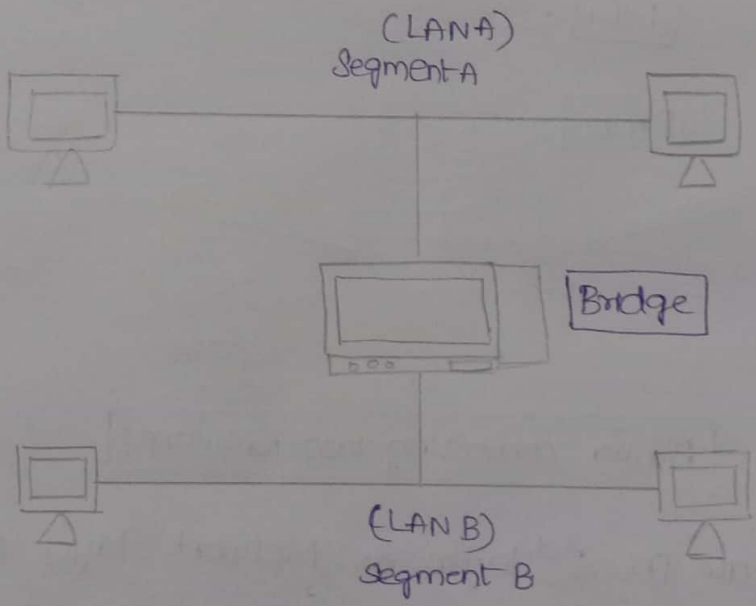
Router connecting two Networks

Routers operate in 3rd layer or Network layer of OSI. It can be used in both LANs and WANs. It transfer data in the form of IP packets. Routers provide protection against the broadcast storms. Routers have routing tables in that it is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.

19BCE2555

Bridge:

Bridges are used to connect two subnetworks that use interchangeable protocols. It combines two LANs to form an extensible LAN. A bridge accepts all packets and amplifies all of them to other side. The bridges are intelligent devices that allows the passing of only selective packets from them. A bridge only passes those packets addressed from a node in one network to another node in other network

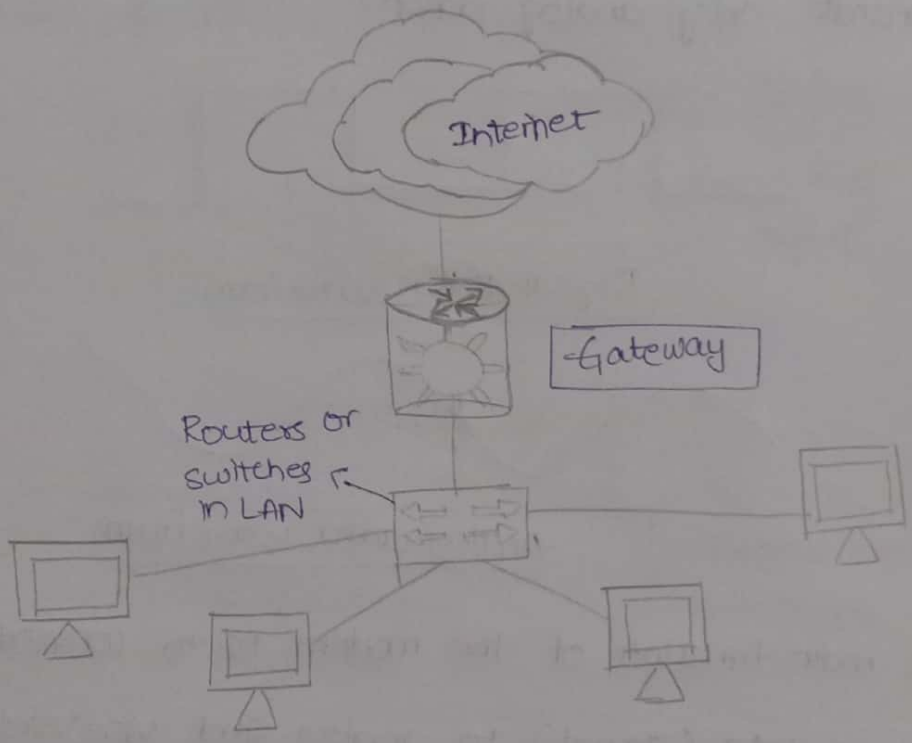


A Bridge can perform aspects like building a table of addresses from which it can identify that the packets are sent from which LAN to which LAN. The bridge reads the send and discards all packets from LANA sent to a computer on LANA and the packets from LANA send to a computer on LANB are retransmitted to LAN B.

Gateway:

19BCE2555

A gateway is a network node that performs a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at Network layer in OSI model.



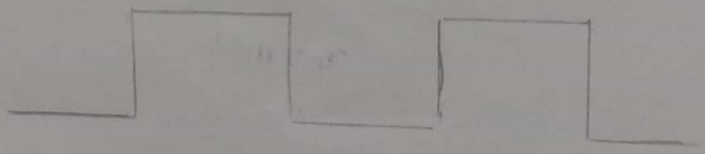
Gateway b/w a LAN and Internet

Gateway is located at the boundary of a network and manages all data that inflows or outflows of the network. It operates as a protocol converter providing compatibility between different protocols used in two different networks. It also store information about the routing paths of the communicating networks. There are 2 types of gateways based on direction of data flow. Unidirectional gateway and Bidirectional gateway.

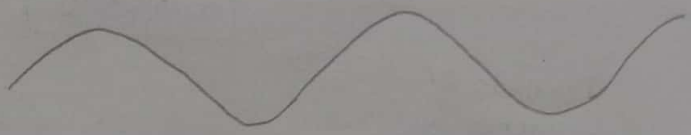
19BCE2555

Modem:

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digitalized whereas a telephone line or cable wire can transmit only analog data.



Digital Data waveform



Analog data waveform

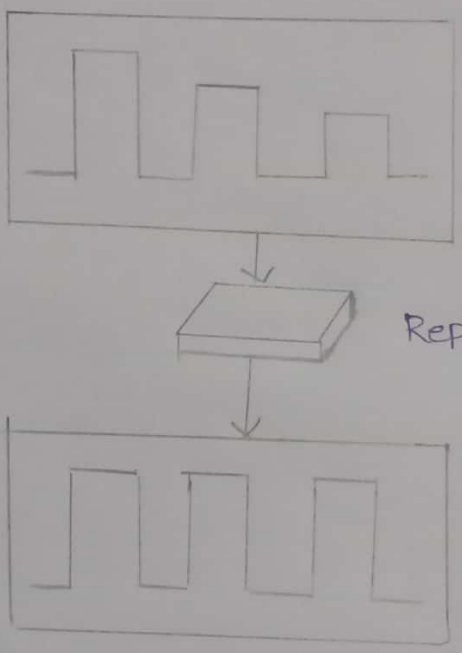
The main function of the modem is to convert digital data (signal) to analog and vice versa. Modem is a combination of two devices- modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by computer. The demodulator converts analog data signals in to digital signals when it is being received by the computer.

Types of Modem are categorized based on direction of transmission of data. They are Simplex, Half duplex and Full duplex.

19BCE2555

Repeater:

A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than that would be capable with original signal.



Repeaters were introduced in wired data communication networks due to the limitation of a signal in propogating over a longer distance and now are common installation in cordless networks for expanding cell size.

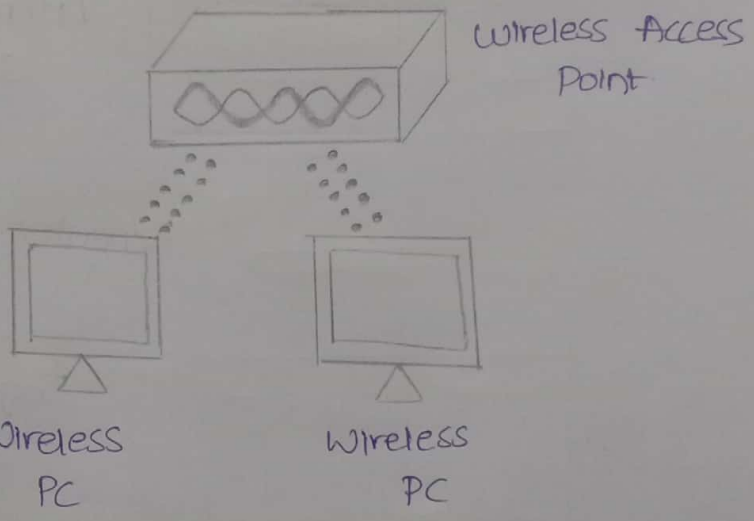
Repeaters are also known as boosters.

Different types of Repeaters are Analog Repeaters, Digital Repeaters, Wired Repeaters, Wireless Repeaters, Local Repeaters and Remote Repeaters.

19BCE2555

Access point:

An accesspoint is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch or hub via an Ethernet cable and projects a wifi signal to designated area.



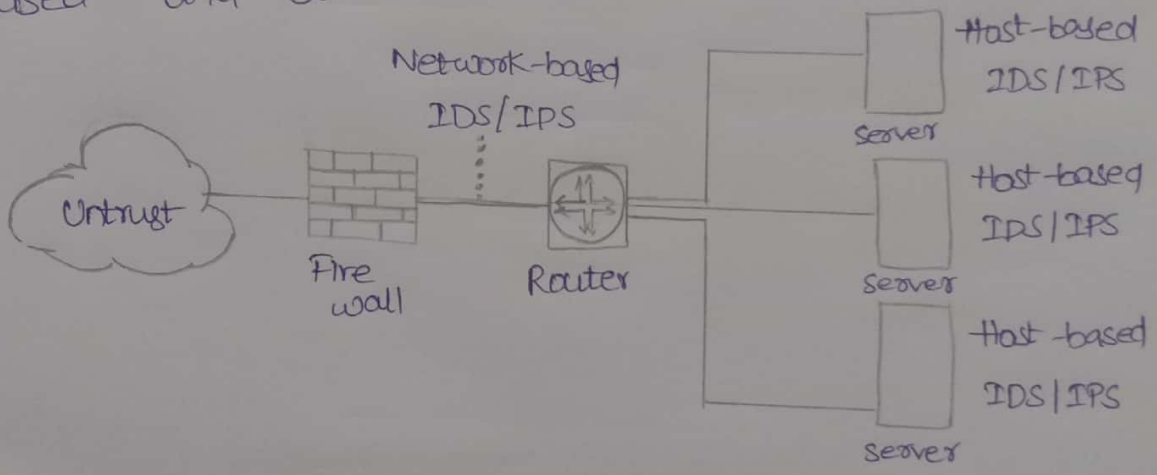
A wireless access point (wireless AP) is a network device that transmitts and receives data over a wireless local area network (WLAN). The wireless access point serves as the interconnection point between the WLAN and a fixed wire network. Conceptually, AP is like Ethernet hub, but instead of relaying LAN frames only to other 802.3 stations, an AP relays 802.11 frames to all other 802.11 and 802.3 stations in same subnet.

IDS/IPS

19BCE2555

IDS: Intrusion Detection Systems are those systems that explore and watch all traffic of the network, looking for symptoms that indicate any cyber threat to the network for infiltrating or stealing data from the network.

The 3 IDS detections methodologies are typically used to detect incidents: Signature-Based, Anomaly-Based and Stateful Protocol analysis.

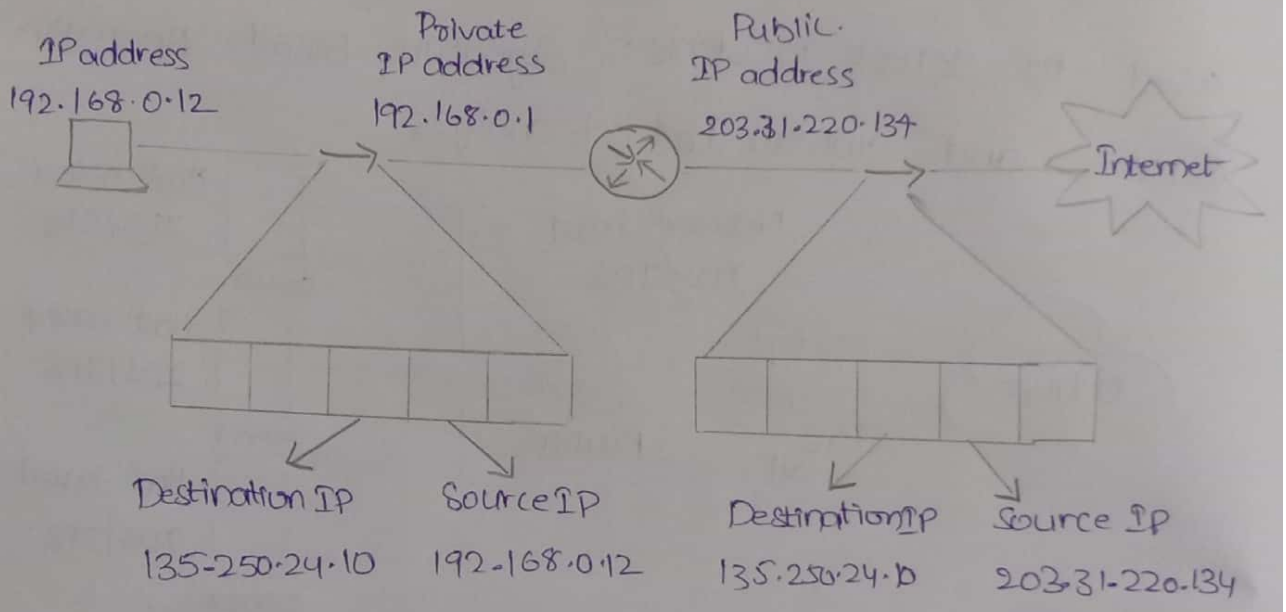


IPS: Intrusion prevention system is a network security tool to continously monitor a network for malicious activities and take action to prevent it, including reporting, blocking or dropping it, when it does occur. It is classified in to 4 types. They are Network based Intrusion Prevention System (NIPS) Wireless intrusion prevention system (WIPS). Network behaviour analysis (NBA) and Host-based intrusion prevention system (HIPS).

19BCE2555

NAT:

Network Address Translation is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.



Packet before NAT

Packet after NAT

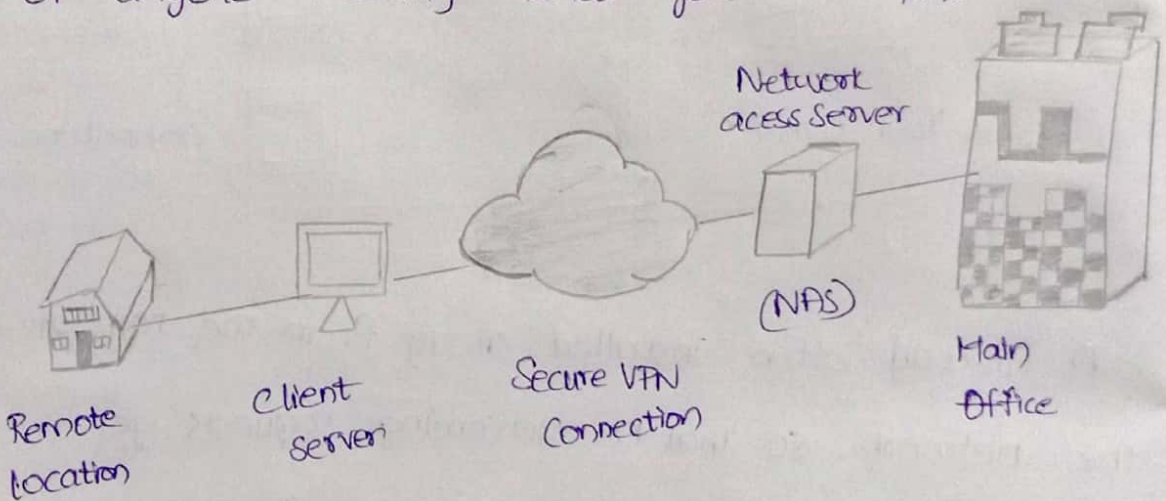
Network ROUTER (Gateway) with NAT Enabled.

NAT conserves legally registered IP addresses. It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden. It eliminates address renumbering when a network evolves.

VPN:

19BCE2555

VPN (Virtual Private Network) is a technology that encrypts your internet traffic on unsecured networks to protect your online identity, hide your IP address, and shield your online data from third parties. VPN uses a real-time encryption and send your internet data through a secure virtual tunnel to minimize the possibility of anyone tracking what you do online.



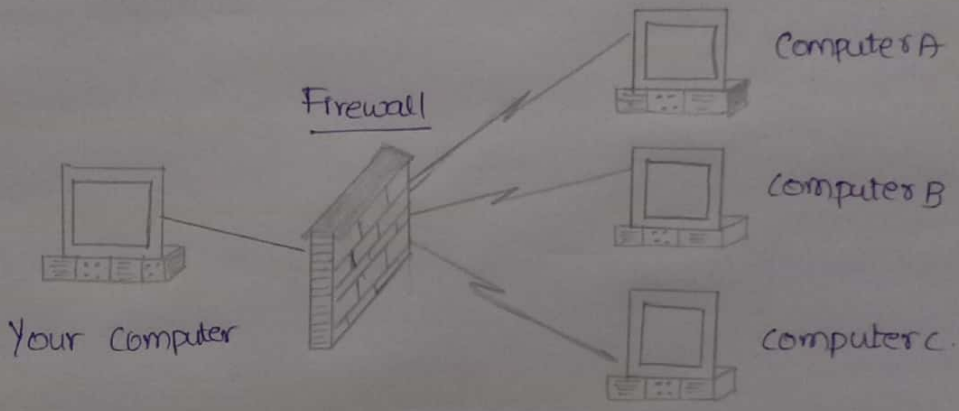
There are many different types of VPNs, mainly we have 3 types: SSL VPN, Site-to-Site VPN and Client-to-Server VPN. When we connect a VPN service it authenticates your client with a VPN server and applies an encryption protocol to all your internet data. The VPN service then creates an encrypted tunnel over the internet.

Here I have choosen the topic "Firewall". Description, Architecture and configuration of it is explained for 2nd part of the Question.

19BCE2555

Firewall:

A Firewall is a device installed between the internal network on organisation and the rest of the network. It is designed to forward some packets and filter others. Firewalls are set of tools that monitors the flow of traffic between networks.



A firewall often installed away from the rest of the network so that no incoming requests get directly to private network resource. If it is configured properly, systems on one side of the firewall are protected from systems on the other side. They generally filter traffic based on 2 methodologies

A firewall can allow any traffic except what is specified as restricted.

A firewall can deny any traffic that doesnot meet the specific criteria based on the network layer on which firewall operates.

19BCF2555

Here I choose the device "Firewall" and analyzing on it.

Working Architecture of Firewall:

- A firewall can allow only traffic except what is specified as restricted. It relies on type of firewall used, the source, the destination address and the ports.
- A firewall can deny any traffic that does not meet the specified criteria based on the network layer on which firewall operates.

The type of criteria used to determine whether traffic should be allowed through varies from one type to another. A firewall may be concerned with the type of traffic or with source or destination address and ports.

Firewall Architecture Implementation:

There are 4 common architectural implementations of firewall. widely in use.

Packet filtering routers: This router is placed at the perimeter between the organization's internal networks and internet service provider.

These can accept or reject packets based on rules of the organization.

Screened host firewalls:

This firewall combines a packet-filtering router with a discrete firewall such as an application proxy server. In this approach, the router screens the packet before entering the internal network and minimizes the traffic and network load on internal proxy.

Dual home hosted firewalls:

In this architecural approach, the bastion host accomodates two NICS in the bastion host configuration. This makes use of Network Address Translation. NAT is a method of mapping external IP addresses to internal IP addresses, thus forming a barrier to intrusion from external attackers.

Screened subnet firewalls:

It is widely used and implemented in corporate networks. Screened subnet firewalls as the name suggests uses DMZ and are a combination of dual-homed gateways and screen host firewalls.

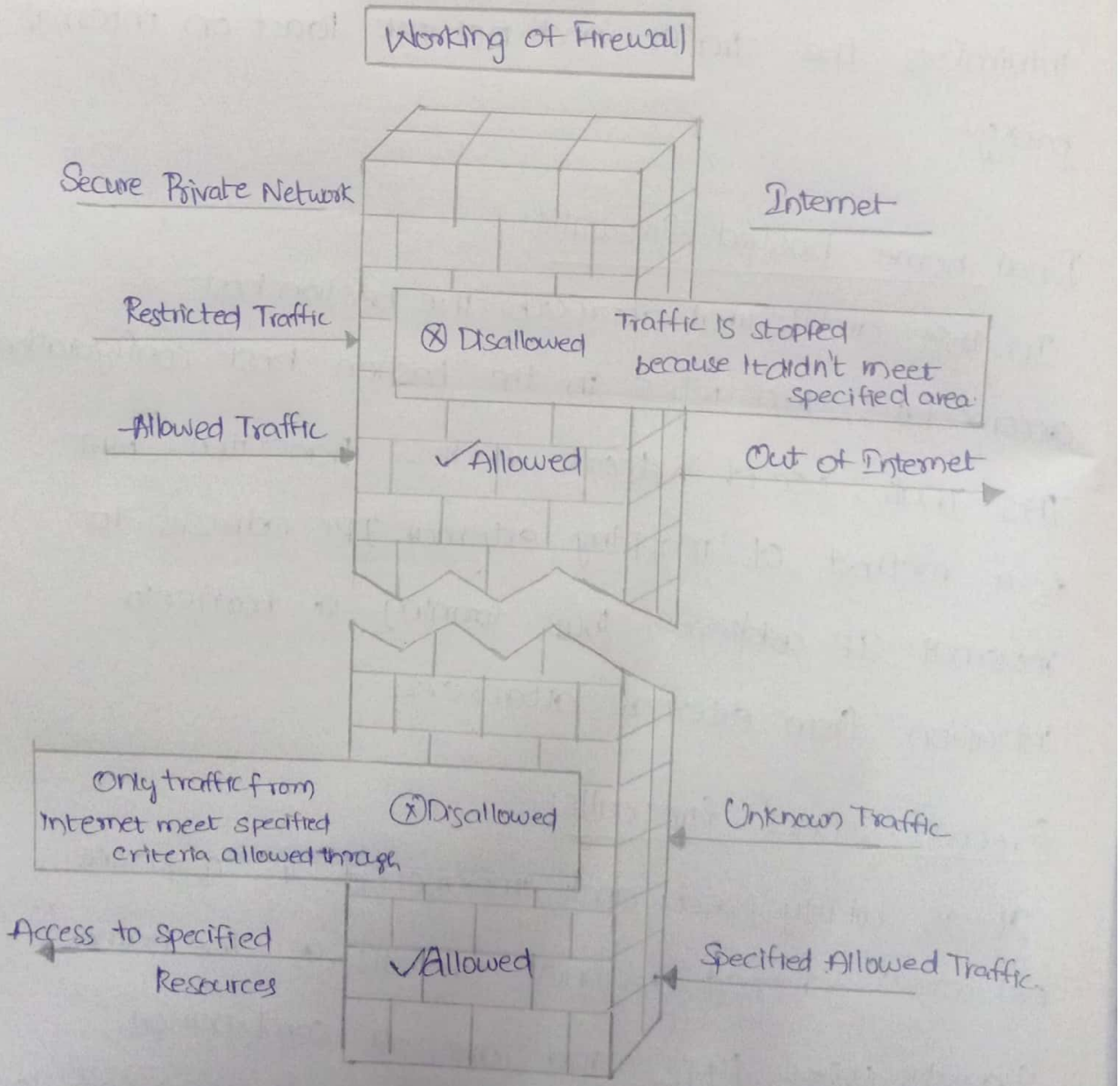
19BCE2555

The network architecture has 3 components:

1st component: This acts as a public interface and connects to the Internet.

2nd component: This is a middle zoned called demilit-arized zone. It act as buffer between 1st & 2nd compos

3rd component: This connects to an intranet or other local architecture.



19BCE2555

Configuring Firewall

Firewalls use one or more of three methods to control traffic flowing in and out of network

Packet Filtering:

Packets are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.

Proxy Service:

Information from the internet is retrieved by the firewall and then sent to the requesting system and vice versa.

Stateful Inspection:

A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information.

Information travelling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics.

19BCE2555

Firewall Software Configuration

Firewalls are customizable. This means that you can add or remove filters based on several conditions. They are:

IP address, Domain Names and Protocols

Why Firewall Security?

There are many creative ways that unscrupulous people use to access or abuse unprotected computer.

→ Remote Login
→ Application backdoors
→ SMTP session hijacking
→ Operating system bugs
→ Denial of Service
→ Email Bombs
→ Macros
→ Viruses
→ Spam
→ Redirect Bombs
→ Source routing.

19BCE2555

Configure Access Lists:

Step1

command

access-list-number {deny | permit} protocol
Source source-wild card [operator[port]]
destination.

Example

Router (config)# access-list 103 permit host 206.1.1.1 eq eqisakmp any

Router (config)#

To create an acesslist which prevent Internet-initiated traffic from reaching local network of router.

Step2:

command

acess-list number {deny | permit} protocol
Source source-wild card destination-wildcard

Example

Router (config)# access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255255

Router (config)#

Creates an access list that allow network to pass freely between the coorporate network and local network.

19BCE2555

Configure Inspection Rules

perform these steps to configure firewall inspection rules for all TCP and UDP traffic, as well as specific application protocols as defined in security policy, beginning in global configuration mode:

Step 1

Command

ip inspect name inspection-name protocol

Example

Router(config)# ip inspect
name firewall tcp
Router (config)#

Purpose: Defines an inspection rule for particular protocol.

Apply Acess lists and Inspection Rules to Interface

Perform these steps to apply ACLs and inspection rules to the network interfaces, beginning in global configuration mode:

Step 1

Command

Interface type number

Example

Router (config) # interface vlan 1

Router (config) #

purpose: Enters interface configuration mode for inside network interface on your router.

Step2

Command :

ip inspect inspection-name {in|out}

Example:

Router (config-if) # ip inspect firewall in

Router (config-if) #

purpose: Assigns the set of firewall inspection rules to the inside interface on router.

Step3

Command:

Exit

Example:

Router (if config-if) # exit

Router (config) #

Returns to global configuration mode.

Step4

Command

Interface type number

Example

Router(config)# interface fastethernet 0

Router (config-if)#

Enters the interface configuration mode for the outside network interface on your router.

Step5

Command

ip access-group {access-list-number | access-list-name} {in | out}

Example

Router (config-if)# ip acess-group 103 in

Router (config-if)#

Assigns defined ACLs to outside interface on router.

Step6

Command

exit

example

Router (config-if)# exit

Router (config)#

19BCE2555

Configure Inspection rules

Step2:

command

Ip inspect name inspection-name protocol

Example

Router (config) # ip inspect name firewall rtsp.

Router (config) # ip inspect name firewall h323

Router (config) # ip inspect name firewall netshow

Router (config) # ip inspect name firewall ftp

Router (config) # ip inspect name firewall sqlnet

Router (config) #

Repeat this command for each inspection rule that you wish to use.

Security Policies

policies Based on IP Addresses and Protocols

Firewall policies should only allow necessary IP protocols through. Fire wall policies should only permit appropriate source and destination IP addresses to be used Specific recommendations for IP address include:

- Traffic with invalid source (or) destination should always be blocked, regardless of firewall location.
- The firewall should be able to use IPV6 address in all filtering rules that use IPV4 addresses.
- The firewall needs to be able to filter ICMPV6, as specified in RFC 4890, Recommendations for filtering ICMPV6 Messages in firewalls.
- Firewalls that enforce policies based on user identity should be able to reflect these policies in their logs That is, it is probably not useful to only log the IP addresses from which a particular user connected If the user was allowed in by a user-specific policy; it is also important to log user's identity as well

Policies based on Network Activity

Many firewalls allow the administrator to block established connections after a certain period of inactivity. Time based policies are useful in thwarting attacks caused by a logged-in user walking away from computer and someone is sitting down on established connections.

19BCE2555

List of policies:

- An organization's firewall policy should be based on comprehensive risk analysis.
- Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.
- Policies should take into account the source and destination of the traffic in addition to the content.
- Many types of IPV4 traffic, such as that with invalid or private addresses, should be blocked by default.
- Organizations should have policies for handling incoming and outgoing IPV6 traffic
- An organization should determine which applications may send traffic into or out of the network and make firewall policies to block traffic rules for the other applications.