1) Network Models

Thursday, May 16, 2024 11:40 AM

Open Systems Interconnection(OSI):
This is basically a model which simplifies the overall breakdown of networking process. It is created by the ISO. Let see the OSI Seven-Layer Model on a Simple Network.

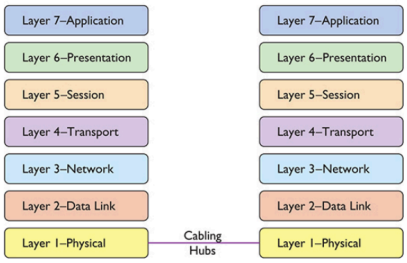
In this model, the individual layer doesn't have anything to do with the other layers but it affects a very little.

The seven layers of OSI are:

Layer 7 **Application**
Presentation
Session
Transport
Network
Data Link
Layer 1 **Physical**

Tip to learn the layers – **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

Network Hardware (Layers 1-2):
It includes the physical media through which the computers in a network are connected like UTP Cable, NIC etc.



The MAC-48 address is also known as **EUI-48(Extended Unique Identifier)**.

The data between two different NICs flow in frames. A typical frame looks like this:

Figure 1-18 Generic frame

FCS Stands for **Frame Check Sequence**.

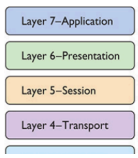
NOTE: Note that the data in each layer of the OSI model is measured through some protocol called **Protocol Data Unit(PDU)**.

For **Layer 2**, a **Frame** is PDU.

What happens when a frame is sent to the central box. Before, the central device was known as **Hub**. When a frame was sent to the hub, it would make same copies of it and then sends back them to each of the devices connected to it except the sender's device. The frame is then rejected by those devices for which it was not intended. However, it is received by those devices for which there is MAC address on it.

Nowadays, the central device is called **Switch**. A switch only sends the frame to the destined devices.

A broadcast address is sent to every device in case the MAC address of a receiver is unknown.



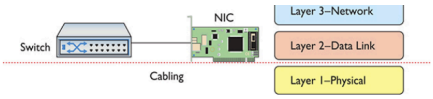


Figure 1-25 Layer 1 and Layer 2 are now properly applied to the network.

It can be seen that the NIC performs two functions, the first is that it moves the data between the cable connection and second is that it wraps and unwraps the data from and to the OS. These are categorized into two different jobs. The part where the NIC talks to the OS is called **LLC(Logical Link Control)**. The part which creates the NIC is called **MAC(Media Access Control)**.

NOTE: It is part of the second layer, called DATA LINK LAYER. It is the only layer which has two parts.

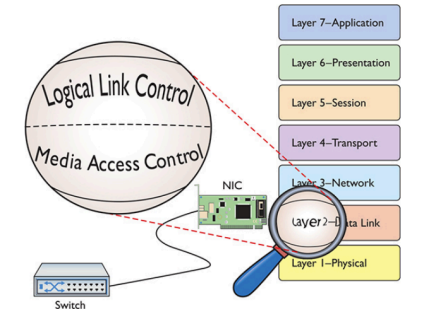


Figure 1-26 LLC and MAC, the two parts of the Data Link layer

NOTE that the fact NICs work at both the layer 1 and layer 2 is true because at some level, it is acting as a physical thing which is sending the data, hence counted in layer 1.

Network Software (Layers 3-7):
The small networks can share the data with the broadcasting technique. However, for large networks, where millions of network are interconnected it is impossible to broadcast. In that case, the **logical addressing** scheme is used. With this, the large network is divided into small groups called **subnets**.

A special software which is required to do the above is called a **Network Protocol**. A NP ensures that each system has a unique address(other than MAC), data is chopped up into pieces, data is reaching from the sender to the receiver etc.

IP – Playing on Layer 3, the Network Layer:
IP stands for **Internet Protocol**. On Layer 3, small **packets** are created and **addressed** for where they are supposed to go. The IP is the primary logical addressing protocol which gives each packet a unique **IP Address**.

NOTE: PDU for Layer 3 is packet.

Packets Within Frames:
An IP Packet is also included within the frame, which holds both the IP addresses and the data which needs to go. So, we can just say that the data is wrapped up in two bundles, the first one is the packet and later covered up by the frame.

Figure 1-30 IP packet

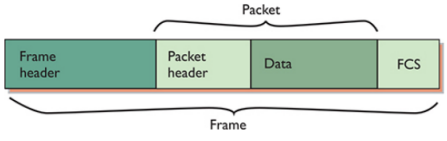
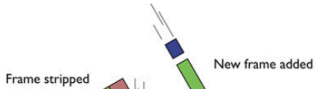


Figure 1-32 IP packet in a frame

When the data is sent to any router. It reads the IP as to where the packet is destined to go, based on that it remodifies the frame and send it further.



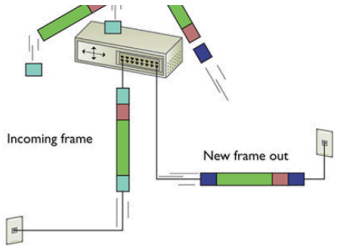


Figure 1-33 Router removing network frame and adding one for the outgoing connection

Segmentation and Reassembly – Layer 4, the Transport Layer:
Segmentation is the process of breaking up the data into chunks so that it can be send by the NIC into small pieces. **Reassembly** is the opposite. The segmentation of data is done in Layer 4.

The connection-oriented protocol is called **TCP(Transmission Control Protocol)** and connectionless protocol is called **User Datagram Protocol(UDP)**.

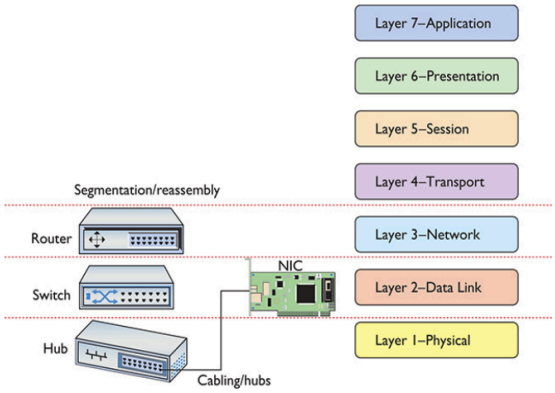


Figure 1-35 OSI updated

If we want to see the Transport layer in action, we first strip away the IP address from an IP packet. What remains the rest is called a **TCP Segment**. The TCP segment ensures that whatever data is there needs to get to the destination in the good order.

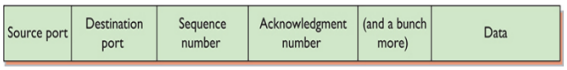


Figure 1-38 TCP segment

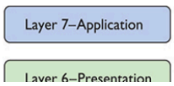
Port is basically a number between 1-65,536 which is given to either a particular service or application. The computer usually determines which TCP segment goes to which application. For example there is a lot of traffic on the web server but it listens for the **TCP segments from port 80-443.**

Similar to the TCP Segment, we also have **UDP Segment**

Figure 1-39 UDP datagram

Talking on a Network – Layer 5, The Session Layer:
In networking of computers, there are several things performed one after another. In such cases, we have small requests and sessions are created. The **Session Software** looks after all of these processes in the session layer.

The session layer initiates sessions, accepts incoming sessions and open/closes existing sessions.



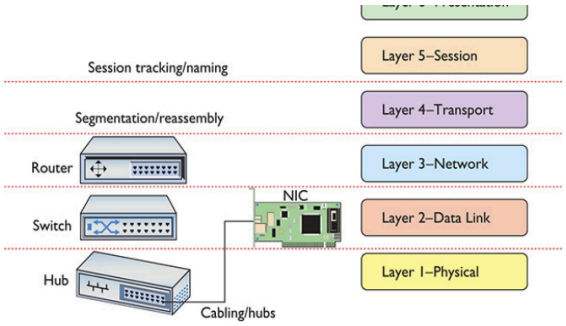


Figure 1-42 OSI updated

To see the sessions in a windows system, we can simply run **netstat**.

For example:

TCP 192.168.4.34:45543 11.12.13.123:80 Established

The above is a session where a web client with IP 192.168.4.34 and port number 45543 is in a TCP session with a web server using the IP address 11.12.13.123 and obviously the port is 80.

Translation – Layer 6, The Presentation Layer:
This layer transforms the data from lower layers into a format used by the Application layers and vice versa.

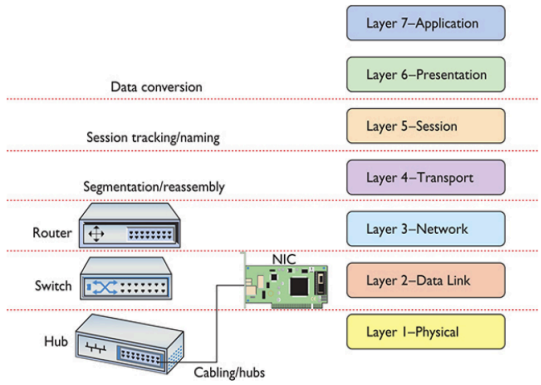


Figure 1-43 OSI updated

Network Applications – Layer 7, The Application Layer:
Application here doesn't refer to the software we use but it is the code built into all operating systems that enables network-aware applications. The application which we call is known as the **Application Programming Interface(API)**.

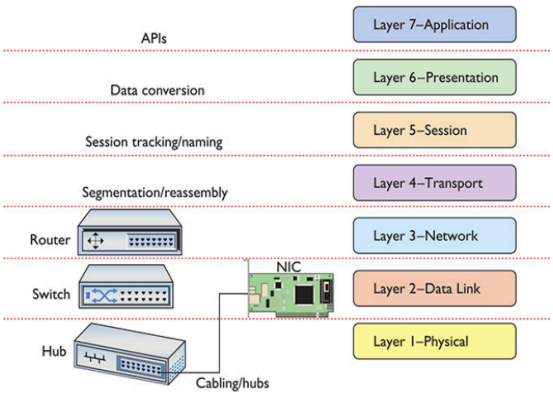


Figure 1-45 OSI updated

Encapsulation and Decapsulation:
Encapsulation is the process of preparing data to go on a network. This includes all the steps from Application to Physical layer. **Decapsulation** is its opposite.

2) Cabling and Topology

May 17, 2024 8:23 PM

Network Topologies:

Bus and Ring:
Star:
Hybrid:
If we talk about the topology today, it can be seen the **Physical Topology** is entirely different from **Logical Topology**. A form of network where the physical and logical topologies are combined is referred to as **Hybrid Topology**.

Mesh:

Cabling and Connectors:

Copper Cabling and Connectors:

Coaxial Cable:
Twin Axial:
It is similar to the coaxial cable which contains two central copper conductors. This is also known as **Direct Attached Cable(DAC)**.

Twisted Pair:
Shielded Twisted Pair:
Unshielded Twisted Pair:
Fiber Optical Cabling:
Fire Ratings:
This dictates what happens when a cable catches fire. The different fire ratings are **PVC-Rated Cable, Plenum-Rated Cable and Riser Rating**.

Networking Industry Standards – IEEE:
The IEEE defines the frames, speeds, distances and types of cabling used in a networking environment. There is basically a 802 Committee which has further created subcommittees for defining the standards in different sectors.

- The frequency (MHz) is the number of lanes on the highway.
- The bandwidth (Mbps) is how many cars (data) can pass through at the same time.
- A higher-rated cable (e.g., Cat 6) is like a highway with more lanes—it can handle more traffic and send data faster.

3) Ethernet Basics

May 18, 2024 7:08 AM

Sneakernet

Ethernet:
Xerox developed Ethernet(3mbps) but later engaged with **Digital Equipment Corporation(DEC)** and Intel and created a standard called **DIX(Digital/Intel/Xerox)** (10 Mbps). Then, this standard was transferred to **IEEE(Institute of Electrical and Electronics Engineers)** and was named 802.3.

802.3 Standards:
802.3i
802.3ab
802.3by
802.3cm
802.3cu

Ethernet Frames:
The transmission of a frame starts with a **preamble** and it sometimes also include what is called a **pad**.

Preamble:
It is either made up of either **8-byte** series of ones and zeros or **7-byte** ones and zeros with **1-byte start frame delimiter**. The use of it is to let the NIC know that a new frame is coming.

Pad:
The size of a frame is 64 bytes. If the data carried by the frame is not of this size then to make the frame of 64-bytes, an extra data is added which is called **Pad**.

Early Ethernet Standards:

10BASE-T:
1990 when this Ethernet became popular. Here, the number 10 refers to the speed, which is 10mbps , BASE stands for signal type, which is **Baseband**(carrying one signal in the cable) and T refers to the type of cable used: **Twisted Pair**.

UTP:
The 10BASE-T use **Cat3**, **two-pair UTP**. However, people had 4-pair installed which was for the intention that there will be good ethernet standards in future. The RJ-45 connector was also introduced in this type of cabling. The real name of RJ-45 was 8 position 8 contact (**8P8C**)

The 10BASE-T used two-pair cabling where the pins numbered **1, 2, 3** and **6** were used. Though, one of these pair was for sending data and the another one was for receiving but Hub was unable the send and receive at the same time. Which was because the NICs were half-duplex.

The **Telecommunications Industry Association/Electronics Industries Alliance(TIA/EIA)** defines the crimping standard for four-pair UTP. There were two major standards which were **TIA/EIA 568A** and **TIA/EIA 568B**.

NOTE: The trick to learn the difference between 568 A and 568 B is with the word **GO**, meaning only Green and Orange color are swapped.

Though the crimping standards used today are same but it has a different name **ANSI/TIA-568-D**.

10BASE-T Limits and Specs:
Distance was limited to **100meters** only. Not more than **1024** computers could be connected.

10BASE-FL:
It a the fiber-version of the 10BASE-T standard. It basically increased the distance to which the data can be carried, which was approximately 2kms and also it was more secure.

CSMA/CD:
In a bus topology and hybrid star-bus topology, the devices would share the same cable which would cause interference in the network due to collision of packets. Ethernet networks used a system called **Carrier-Sense Multiple Access with Collision Detection(CSMA/CD)** to determine which cable should use the cable at a given time. Here, the term carrier-sense means that every node must check the cable before sending the traffic and multiple-access means that all machines has equal access to the wire. If suppose two nodes saw that the cable was good to send data and both sent the data at the same time. In that case, there would be a collision and the data couldn't reach properly. Using the CSMA/CD model, the network would generate a random number and based on that, it would make the decision of which node should be given the chance to transmit data. Collision no longer exist today.

Enhancing and Extending Ethernet Networks:
Hubs were replaces with Switches. Switch is different from hub because it can create a point-to-point connection using the MAC address instead of sending data packets to every other node. The switch does this using **Port Mapping**. As soon as the networks are connected to the port, it creates a table of all the MAC addresses and later when the data is transmitted, it directly sends packet to the desired address.

Connecting Ethernet Segments:
When the networks get large, a single switch is not enough and hence more switches are added. To do so, there is a terminology called **Uplink Port**. In the switch itself, there existed a port called Uplink Port which was basically a port where we can connect another switch to the existing switch.

Modern systems have auto-sensing ports and the term used for it these days is **MDI-X(Auto-Medium-Dependent Interface Crossover)**.

Crossover Cable:

It was basically a cable which was used for **converting 568A to 568B**. The use for it was to interconnect two computers, thus a switch was not required.

Spanning Tree Protocol:
When there was the possibility of connecting two or more switches, we could connect the switches in any was possible. This interconnection of switches was termed as **Switching Loops** or **Bridge Loops**. It would create a loop and in turn would crash the network because the frame couldn't reach its destination.

There was a protocol created called **Spanning Tree Protocol (STP)**. In this type of protocol, the system would detect already if there is any potential loop in the system before it happen.

The STP process was done by sending the **BPDU(Bridge Protocol Data Units)** frames in the network. They would configure and find out if there is any switching loop in the setup. If there was any, certain ports were put to the **Blocking State**. When there was a need to open these ports if the device goes down, it was done by special type of BPDU frames called **TCN BPDUs (Topology Change Notification BPDUs)**.

While this happens, the ports which were connected to the computer were already put to the **Port Fast** setting, which means that there will no BPDU or TCN BPDU frames would go. **The BPDU Guard** ensures that no BPDU frame reaches to the **Port Fast** port. There is also another mechanism called **Root Guard** which stops the port fasted port from getting in switching loop state.

The current name for STP is **RSTP(Rapid STP)**.

4) Ethernet Standards

May 24, 2024 6:28 AM

10 BASE-T
100 BASE-T:
There were basically two standards under this standard, **100 BASE-T4(Cat 3)**and **100 BASE – TX(Cat 5 and Cat 5e)**. The T4 standard was not used because TX dominated the market hence, the standard is simply termed at **100 BASE-T**. Note that 100base required 100base NICs.

Note: Since this standard was used, **full-duplex** was already in use.

> 100 BASE – T
> **Speed:** 100 Mbps
> **Signal:** Baseband
> **Distance:** 100 meters
> **Node Limit:** 1024
> **Topology:** Star-Bus
> **Cable Type:** Cat 5 or better UTP or STP with RJ-45

100 BASE-FX:
Fiber cabling for high speed, greater distance and high security.

> 100BASE-FX
> **Speed:** 100 Mbps
> **Signal:** Baseband
> **Distance:** 2kms
> **Node:** 1024
> **Topology:** Star-Bus
> **Cable Type:** Multimode Fiber-optic with ST/SC connector

100 BASE-SX:
Similar to the 100BASE-FX standard and ran on **ST, SC** or **LC** connectors.

Gigabit Ethernet:
This is the most common type of Ethernet found on new NICs. There were two versions of this, **1000BASE-T(802.3ab)** and **1000BASE-X(802.3z)**. Ther latter is divided into a series of standards like 1000BASE-SX, LX etc.

> **1000 BASE-T** or **Gigabit Ethernet**
> **Speed:** 1000mbps
> **Distance:** 100m
> **Cable Type: Cat 5e or Cat 6** with **Four-Pair** UTP
>
> **1000 BASE-SX**
> **Speed:** 1000mbps
> **Distance:** 220-500m
> **Cable Type:** OM2 Multimode with ST, SC or LC connector.
> **Light:** 850-nm wavelength LED.
>
> **1000 BASE-LX**
> **Speed:** 1000mbps
> **Distance:** 5kms
> **Cable Type:** OS1 or OS2 Single-mode with ST, SC or LC connector.
> **Light:** 1300-nm wavelength LED.

The Small Form Factor fiber connectors used are **LC(Local Connector)** and **MT-RJ(Mechanical Transfer Registered Jack)**.

> **Mechanical Connection Variations:**
> When the fiber cables are connected to the PC, there remains a little gap between the point of connection, which causes interference in the light. For this reason, the old **Flat-Surface Connector** were replaced by **Physical Contact(PC) Connector** and later by **Ultra-Physical Contact(UPC)** and **Angular Physical Contact(APC)**.

> **Multiple Types of Gigabit Ethernet:**
> **Media Converters** can be used to connect any type of ethernet cabling together. The **Gigabit Interface Converter(GBIC)** is standard port for connecting Gigabit Ethernet to the

5) Installing a Physical Network

May 24, 2024 8:50 PM

Structured Cabling – Single Star Topology:
A successful implementation of a basic structured cabling(**horizontal cabling**) requires three basic components a **telecommunications room, horizontal cabling** and **a work area**.

Horizontal Cabling:
A cable runs from the telecommunications room to the work area. This cable is either **Cat 5e** or better UTP for copper-based standards. For ex **1000BASE-T**. It is recommended that **4-Pair** high-standard UTPs should be used in this cabling system.

Telecommunications Room:
Technically, this room is called **Intermediate Distribution Frame(IDF)**.

Equipment Racks:
19 inches wide. A height of unit **U** is **1.75** inches. Most of the devices are either **1U, 2U** or **4U**. A naming standard which exist but is not used by anyone is **ANSI/TIA-606-C**. **Patch Bays**. Common Punch Down Blocks are **66-Block** and **110-Block**.

The Work Area:
Jacks for wall outlets.

Structured Cabling - Beyond:
Connections from outside the world come into a building at a location called A Demarcation Point(**Demarc**). This is also called Service-Related Entry Point. On one side of the Demarc, it is our responsibility to take care of whatever happens, while another remains for the company. The device that acts as a Demarc is called **Network Interface Unit(NIU)**. These devices would come with the service called **Smartjack**, which would allow the ISPs to test their NIUs/Networks from distance.

Connections Inside the Demarc:
The first device in the building which is connected to the Demarc is called **Customer-Premises Equipment(CPE)**, a Switch is basically a CPE. The cable which connects this Demarc and CPE is called **Demarc Extension**.

The main Switch, which connects to the Demarc, is connected to a **Patch Panel** and this main panel is called **Vertical Cross-Connect**.

Below is a **Fiber Patch Panel**

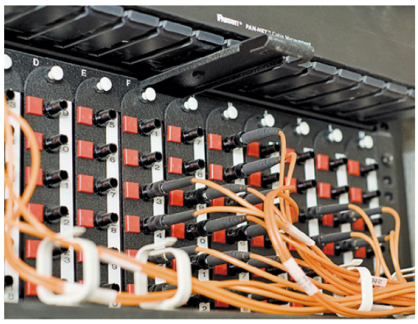


Figure 5-28 LAN vertical cross-connect

The room that stores Demarc, CPE, Cross-Connect etc. equipment is known as **Main Distribution Frame(MDF)**. The MDF if different from the IDF(Telecommunications Room) because IDF is for say, a floor whereas, MDF if for entire building.

Installing Structured Cabling:

Getting a Floor Plan:
Mapping the Runs:
A drop is basically a cable running from a tele room to some computer.

Location of the Tele Room:
It is based on Distance, Power, Humidity, Colling and Access.

Pulling Cable:
TIA, NEC and local codes, all have strict rules about how you pull cable in a ceiling.

Making Connections:

Connecting the Work Areas:
Rolling Your Own Patch Cables:
Connecting the Patch Panels:

Testing the Cable Runs:
Degradation, Interference and Connectivity. The testing standards are also defined by the TIA.

Copper Cable:
Continuity testing is also known as wire map and the devices used are Continuity Tester, **Microscanner**, Multimeter by putting it in continuous state etc., **TDR(Time Domain Reflector)** would tell the length of the wire, where is it broken from etc.

Crosstalk:
When we are send the signal from one pair of wires in the UTP, it is sometimes picked up by another wire and this is termed as **Crosstalk**.

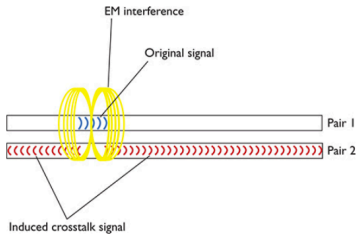


Figure 5-52 Crosstalk

There are **NEXT(Near-End Crosstalk)** and **FEXT(Far-End Crosstalk)** Crosstalk. In NEXT, we test for the crosstalk from the same end of the wire by which we are sending the signal and in FEXT, we test the signal at the opposite end of the wire.

The weakening of signal as it progresses through the wire is called **Attenuation**. **Jitter** is known as the delay in the transmission of frame. **Cable Certifiers** do a test on the cables installed and provide a paper with report on those cables. The loss of a signal in a cabling in defined in **Decibals(dB)**.

Fiber Cabling:
SFP/GBIC could cause signal loss. Dirty Optical Cables can also cause the same. Alike Attenuation, Fiber cables suffer from **Dispersion** or **Modal Dispersion**. The device used for detection is called **OTDR(Optical Time-Domain Reflectometer)**. The tool used for connecting two ends of a fiber is called a **Fusion Splicer**.

NICs:

Port Aggregation:
It is for connecting multiple NICs to a single machine. Another name for this is **Bonding** or **Link Aggregation**. This is not done for speed, but for adding another lane of equal speed.

Link Lights:
There is no standard for how lights flicker, but can be seen/read on user manual.

Diagnostics and Repair of Physical Cabling:

Checking Physical/Software Problem:
Checking Link Lights:
Checking the NIC:
Can be done using Software/Hardware Loopback test. For physical loopback test, there is a **loopback adapter**.
Cable Testing:
Coupler is basically a small device which has two female ports and is used to connect the broken UTP.
Telcommunication Room:

6) TCP/IP Basics

May 27, 2024 9:01 PM

The TCP/IP Protocol Suite:

Network Layer Protocols:
IP works on **Layer 3**, **Network Layer**. Other than IP4 and IP6, there is another protocol which works at this layer called **ICMP(Internet Control Message Protocol)**. This ICMP helps in error reporting and diagnostics. This protocol is mainly automatically setup by the application rather than the layer itself. However, this is sometimes intently triggered by the user like by running **ping** command.

There are 14 different fields in a IP4 header, but below is summary of them

Version:
- This defines the type of the IP address like IP4 or IP6

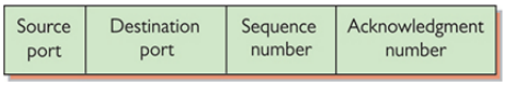
Total Length:
This defines the total size of the IP packet in octets.

Time To Live(TTL):
This is basically a counter which keeps on decreasing, it defines the number of routers the packet goes through. At most, a packet can travel only **255 routers**. So, the counter starts decreasing and goes to 0 as it progresses through the routers.

Protocol:
TCP or UDP is defined.

Transport Layer(Layer 4) Protocols:
The TCP/UCP is defined by the developer who makes the application. So, it is not in our control. Note that at layer 4, TCP gets the data divided into chunks called **segments** whereas UDP forms the entire data into a **datagram** and give it a header.

TCP:
The term **TCP/IP** indicates that the application uses the TCP protocol with IP. Since TCP is embedded in the application, it uses a way to communicate with the another device before sending any packet and verify its presence. The term defined for this is called **TCP Three-Way-Handshake**; **SYN, SYN-ACK** and **ACK**. Another function of TCP is that it also breaks the data into segments and gives them a **sequence number/acknowledgement number**. Furthermore, **Flags** in TCP help in giving both sides the status of their connection, whereas **Checksums** are helpful in checking the TCP header for errors.

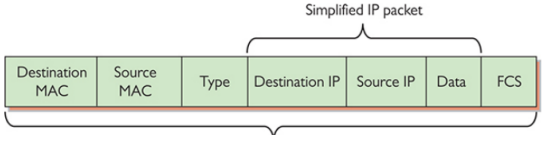


This is basically a TCP header. Here, the ports are basically the port number from which port to which port the packet is being sent.

UDP:
Its header doesn't contain much fields because the data sent/received doesn't need to be perfect. For this reason, it is very fast and used in connections where there is less chance of data loss during delivery. UDP is most commonly used by **DNS**(queries and response) and **DHCP**(for setting up initial connection).

Application Layer(Layer 7) Protocols:
TCP/IP Applications use TCP/IP for moving data back and forth between clients and servers. For example, web browsers use **HTTP** protocol which comes under the TCP/IP.

IP and Ethernet:
IP and MAC both work together while a frame is made. A common frame looks like this



Simplified Ethernet frame

When a computer is connected to a switch, it is given a MAC Address and an IP Address. Now, suppose one computer knows the IP address of the another which is in the same network and trying to connect to that computer using an IP Address. Here, the computer would need both an IP Address and MAC Address of another computer. But how would it know the MAC Address of another computer in the network. For this purpose, the ARP(Address Resolution Protocol) Protocol creates an **ARP Request** which is sent to the universal broadcasting address **FF-FF-FF-FF-FF-FF** and the IP Addressing belonging to that computer responds to it. The command **arp –a** will list all the current connections which has been made by the computer or which the computer already knows about.

IP Address:
IP Address in Action:

Network IDs:
Interconnecting LANs:
Routing Table defines which packet goes where.

Subnet Mask:
It is used to find out if a given IP address belong to the same Network ID or is it intended for different one. All the computers on the same network have the **same subnet mask**. Shorthand for Subnet is **CIDR**.

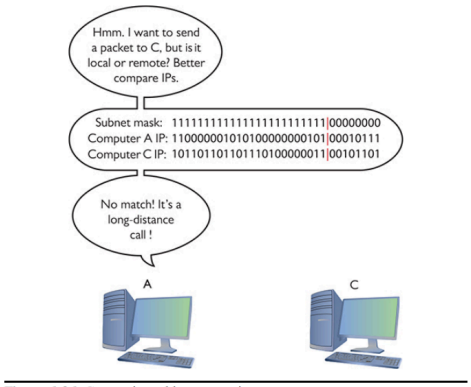


Figure 6-26 Comparing addresses again

NOTE: Note that when another computer, to which the data is being sent, is in the same network, the ARP gets to know the MAC but when it is in some another LAN then the ARP tries to find out the **Default Gateway's MAC**.

Class IDs:
RIR(Regional Internet Registries) is basically a registry which parcel out IP Addresses to the ISPs in different regions. The RIR is managed by a big organization called **IANA(Internet Assigned Numbers Authority)**. IANA is further managed by **PTI(Public Technical Identifiers)** and **ICANN(Internet Corporation for Assigned Names and Numbers)**.

The RIR for America is **ARIN(American Registry for Internal Numbers)**.

IANA manages the IP Addresses in some **network blocks** which are also called **Classes**.

	First Decimal Value	Addresses	Hosts per Network ID
Class A	1–126	1.0.0.0–126.255.255.255	16,777,216
Class B	128–191	128.0.0.0–191.255.255.255	65,534
Class C	192–223	192.0.0.0–223.255.255.255	254
Class D	224–239	224.0.0.0–239.255.255.255	Multicast
Class E	240–255	240.0.0.0–255.255.255.255	Experimental

The Subnet for Class A, B and C is 255, 255.255 and 255.255.255 respectively.

Multicast Addresses were used for **one-to-many communication** and **Experimental Addresses** were called **Reserved Addresses**, which were for occasional experiments.

Unicast- One computer to any other

Broadcast- Every computer hears the message
Anycast- Computers share same address and router sends to the closest computer
Multicast- A group of interested computers.

Now, the class system worked well for few years but then suppose a single organization has to use 2000 computers, it had to buy a single class, which would either waste the remaining IP addresses, if there are more or would either fell short if there are less. For this reason, a new method of **network blocks/class** was developed which was called **CIDR**.

Subnetting:

Now we know that the Network ID of a particular network is identified using subnet. Suppose we have a network in a café and we want to divide this single network into three different Network IDs which are used in the café. For doing this, we use a concept called **Subnetting**. Using this, we create more subnets, thus more Network IDs.

Let's now make a subnet. Suppose we have a /24 Network ID **192.168.4.0** that belong to our café. The subnet for this will look something like this, since it is a /24 subnet.

11111111.11111111.11111111.00000000

The idea how a subnet is created is by extending the 1s in a subnet to the right and name it accordingly. If we have 25 1s, we say it is sub netted to /25 Network ID. Now if we think, extending 1 to the right will give us two more extra Network IDs for this same network(Since the value corresponding to binary value 1 of subnet could be a 1 or 0 if compared to Network ID). And if we have extended n values, we will have 2 ^n more networks.

If we have a look at our example, we want to have three more networks at the café, for this matter, we need to convert the /24 subnet to /26 (since increasing 2 subnets to the right will have 4 more Network IDs).

Original network ID: 192.168.4.0 /24
Translates to this in binary:
11000000.10101000.00000100.00000000

11000000101010000000010000000000
11000000101010000000010001000000
11000000101010000000010010000000
11000000101010000000010011000000

Here, we can see that the /26 has given us four more Network IDs. We can now reserve them for different purposes in our network.

If we convert the above Network IDs into decimal, we have the following Network IDs with their corresponding hosts to the right. Note that host **63, 127, 191** and **255** are reserved for their **Broadcast Address**.

192.168.4.0	192.168.4.0 - 192.168.4.62
192.168.4.64	192.168.4.65 - 192.168.4.126
192.168.4.128	192.168.4.129 - 192.168.4.190
192.168.4.192	192.168.4.193 - 192.168.4.254

So, we can now say that a /24 Network ID has created four /26 Subnets. This concept is called Subnetting.

We saw that the /26 subnets have equal number of hosts. However, using **Variable-Length Subnet Masking(VLSM)**, we can divide them according to the needs. To calculate the number of hosts in a subnet, we do **2^n – 2** where n is the number of 0s in a Subnet.

Decimal to Binary Conversion:

Trick for any number. For example say **221**, we can place in the table like this and add later.

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1	1	0	1	1	1	0	1

IP Address in a PC:

Static:
Setting up IP in Windows, MacOS and Linux.

Dynamic IP Addressing:

DHCP:
Any computer which is connected to the network have **DHCP Clients** and **DHCP Server**. DHCP Server exists in SOHO Router or it could be a rack-mounted server.

Four-Way Handshake:
When a DHCP Client boots up, it broadcasts a **DHCP Discover message**, this message is like asking "are there any DHCP servers out there?". DHCP Server replies back by sending a **DHCP Offer message** which includes **IP, Subnet and Gateway**. The client then responds by sending out a **DHCP Request**, it is kind of confirming to the DHCP Offer. DHCP server then sends a **DHCP ACK (Acknowledgement)**. This four-step process of obtaining a Dynamic IP Address is called **Four-Way Handshake** also known as **DORA**.

Configuring DHCP:
DHCP Servers use UDP **Port 67** and **DHCP Client** use **Port 68**.

When the DHCP Server is setting up the IP addresses, it needs some configuration like; it needs a pool of IP addresses, it needs the subnet of the network, it needs to know the IP for the default gateway for the network.

DHCP Scope:
A technician installs a pool of IP Addresses and this is called a **DHCP Scope**.

DHCP Relay:
In some cases, the DHCP Server is a separate server instead of being in the same LAN. During that case, the router uses a **DHCP Relay** for sending out broadcast message to the separate server attached to the LAN using **UDP Forwarding**. This is done because broadcasting is usually done in the LAN only, broadcasting in router would cause Broadcasts all around the internet.

During the DHCP Relay, the relay is given the IP Address of the real DHCP server and this address is termed as **IP Helper Address** or **UDP Helper Address**.

Reservations:
Devices like Cameras, Printers and Servers have a fixed IP Address instead of dynamically assigning it an address every time. This is done either by reserving IPs for these devices using the term **MAC Reservations** or either by excluding some range of the IPs while creating the pool. This range is called **IP Exclusion Range**.

Living with DHCP:
When the DHCP fails to generate a DHCP address, the **APIPA** in Microsoft assigns a special kind of . Using this, the network couldn't get to the Internet but can talk to the devices in its network.

When a DHCP server fails, we can try something like renewing the lease.

Renew the lease in MacOS, Windows and Linux.

Multiple DHCP Servers:
If a bigger network is running DHCP server, there could be chances of network failure. For this reason, bigger networks have more than one DHCP servers running. **DHCP Failover** is the process of running two DHCPs together in case there is a network failure.

Rogue DHCP Server:
An unintentional server in a network can be termed as **Rogue DHCP Server**.

Special IP Addresses:
There are various types of special IP addresses used for different purposes. From them, one is 127.0.0.0. this address is called the loopback address. This is used with ping command to test computer's network stack if it can listen back to its packets. Some of the reserved IP Addresses are:

- 10.0.0.0 through 10.255.255.255 (1 Class A network block)
- 172.16.0.0 through 172.31.255.255 (16 Class B network blocks)
- 192.168.0.0 through 192.168.255.255 (256 Class C network blocks)

7) Routing

June 1, 2024 2:17 AM

How Routers Work:
Routers work at **Layer 3** or the OSI model. They forward packets based on their destination IP.

Usually, Switches work at layer 2 and routers at layer 3, but the Switches which work at Layer 3 or more are known as **Multilayer Switches(MLS)**.

Routing Tables:
It tells the router where to send the packets. Down below, there are some columns dedicated to a particular packets which defines the their route

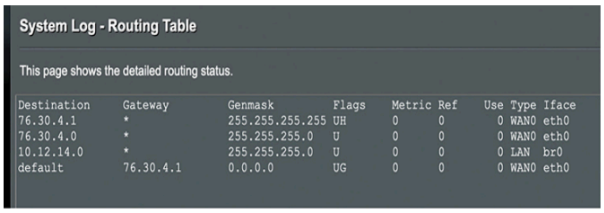


Figure 7-7 Routing table from a home router

Destination:
Defines where the packet needs to go.

Gateway:
It is for telling the router where to send the packet, if it is for some other device which is not connected to the router then the particular address is mentioned here. If the destined computer is connected to LAN, then there is either a * or **0.0.0.0 written**.

Gen mask:
It is basically the subnet which defines the Network ID.

Flags:
It is used for defining the destination like **U** for route's condition, **H** means the route is a host, **G** means the route is for gateway.

Type and I face:
Tell the router which ports to use for the packet.

Default Destination:
In the above table, if we observe the fourth row, it is basically a **default destination**, which means if there is no destination found we can use the default one. Here, it is forwarded to the 76.30.4.1 Gateway. Every router has this default destination address.

To print a routing table in CMD, we can run **route print**.
Print route table in Mac, Linux.

Metric:
It is a value which defines the desirability of a route. If a router has more than one route to the same network, we can assign different metrics to each route. **Dynamic Routing** defines the proper metric for each route. For some packet, the router would always choose the metric with the lowest value. For example, if we have Metric: 1 and Metric:10, the router would go for Metric 1 but since metric 1 is broken, metric 10 is taken.

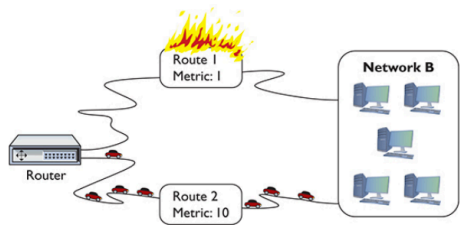


Figure 7-11 When a route no longer works, the router automatically switches.

For the snip below, the values could be defined as

```
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.12.14.1   10.12.14.201      25
```

(Any destination address) (with any subnet mask) (forward it to my default gateway) (using my NIC) (Metric of 25 to use this route).

Routing Table in Windows, MacOS and Linux - Understand.

Others Networks in the Router:
Routers not only connect Ethernet networks, but others types of networks that carry IP address as well. For example, some networks other than ethernet are- **Data-Over-Cable Service Interface Specification (DOCSIS)** and **Passive Optical Network (PON)**. To connect these to the router, we need different interface cards installed in the router.

Network Address Translation:
Many of the IP4 addresses are in use throughout the world and it is becoming harder to have a new IP. With the use of **NAT(Network Address Translation)** technology, we are conserving the IP addresses.

The Setup:
When a new network is being set-up, what is done is that the computers in the network are given a Private IP address which are connected to the router. The router has one **Public IP** provided by the ISP. This Public IP helps us in connecting to the internet. Here, we can see that only the router is using the Public IP, if all the computers in the LAN starts to use it, it could cause the public IPs to diminish. Hence, **Network Address Translation** is done to save those IPs.

Port Address Translation(PAT):
This is a type of NAT, where the router uses the port numbers to map the traffic of both the sender and the receiver. Suppose a user from the private IP makes a request to the web browser, he has to request it to the internet and through the gateway. In this case, the router uses a PAT. Using this, the router translates the private IP into the public IP using the port number. The port numbers have values ranging from 1 to 65535.

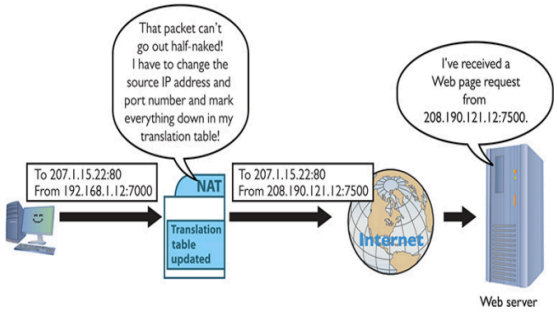
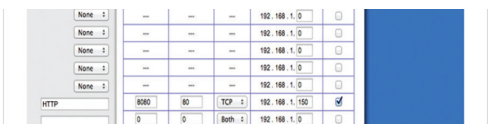
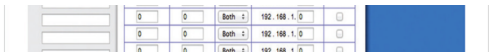


Figure 7-15 PAT in action—changing the source IP address and port number to something usable on the Internet

DNAT(Dynamic NAT):
It is also known as **Pooled NAT**. In this case, the computers in a network share some IP addresses, which are less than the computers, and when these computers have to access the resource on the internet, they dynamically use that address to translate their own address to some public IP.

Port Forwarding:
Suppose we have 10 devices in our network, every device shares a private IP. Now suppose one of the device is a server and computers outside our network wants to access the server. In this case, what is preferrable is that this one device should be given a routable IP address which helps to keep the connection one-to-one. This is called **Static NAT(SNAT)**. Static Translation is done using the Port Forwarding technology. Suppose we've set up that a traffic coming to port 8000 it is always forwarded to port 80. For this, we can say the port 8000 it forwarded to 80.





Dynamic Routing:
Dynamic Routing is a process that routers use to update routes automatically when they fail to update the routes.

Routing Metrics:
We know that routers use metric system to decide the route of a packet. There are some factors which are taken into consideration for setting up a metric value. These are:

Hop Count:
It is basically a count of the number of routers a packet has to pass through to get to its destination.

Bandwidth:
The amount of data carried in a given period of time.

Delay:
If the packet being sent is taking time. It can also be considered as latency.

Cost:
How a packet flows through a route and at what costs is also a factor. Like cost of higher or lower bandwidth also makes a difference.

Distance Vector and Path Vector:
Distance vector routing protocols are a type of network routing protocol where routers calculate the best path to a destination based on the metric, commonly the hop count. Routers share their entire routing tables with their immediate neighbors at regular intervals, allowing them to update their routes dynamically.

Note that distance vector routing protocols is an umbrella terms used, it compasses different protocols.

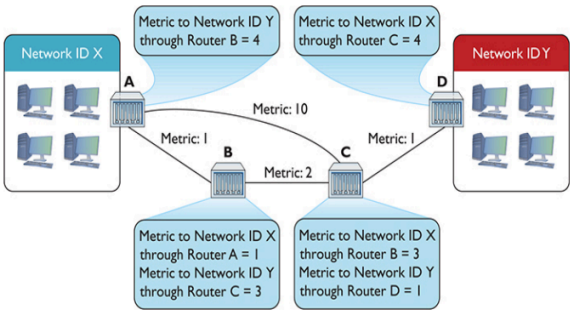


Figure 7-26 Last iteration

It is known that routers share their entire routing tables with each other for the purpose of calculating metrics. However, after a point of time, when they are done calculating, routers stop sharing and that state is known as **Convergence** or **Steady State**.

Distance vector routing is preferrable for smaller networks because for a larger network, convergence could take a lot of time.

There are different types of distance vector routing protocols:

RIPv1:
Routing Information Protocol is what comes under the term distance vector routing protocol. There are two versions of this, RIPv1 and RIPv2. Both the RIPs share not more than **15 hops**.

The drawbacks of V1 was that it didn't know how to use **VLSM(Variable Length Subnet Masking)** and it also didn't have any authentication, **less secure**.

RIPv2:
Solved the problems of VLSM and Security. Though it is still used in some routers like LAN but for larger networks, like WAN there was a need for better distance vector routing protocols.

BGP:

In 1980s, there was a need for the expansion of Internet and due to that reason, there was also a need for a **standard dynamic protocol**. Though this could have done but the problem was that smaller internet companies worked in a decentralized fashion like in smaller groups. These companies were **IANA(Internet Assigned Numbers Authority), Internet Society(ISOC), IETF(Internet Engineering Task Force)** etc. What these companies did was that they came up with a concept called **Autonomous Systems(AS)**. An autonomous system is basically a particular network or system of networks.

In AS networks, the admin of the network would assign it's network a policy which states how it is going to share traffic with another network. Each AS have its special number known as **Autonomous System Number(ASN)**, which is assigned by **IANA**.

ASN is a **32 bit** number with 16 bits separated by a dot. For ex **1.33457** is an ASN number. The router needs to be configured with ASN by IANA in order to be used.

When router on one AS communicates with another AS for the purpose of sharing router information, they use **Exterior Gateway Protocol(EGP)**. And the networks within networks use **Interior Gateway Protocols(IGPs)**. Though whatever protocol can be used for AS to AS communication but the internet uses **Border Gateway Protocol(BGP)** for this purpose. Current version of **BGP** is **BGP4**. BGP is also known as **Hybrid Protocol**.

Route Aggregation:
What BGP does is it supports **route aggregation**, using which, we can keep track of the shortest common network IDs rather than trying to keep track of every router on the Internet.

Link State:
With this type of protocol, instead of changing the route table, the routers were forwarding the change in the route. Two types of protocol fall under this category: **OSPF(Open Shortest Path First)** and **IS-IS (Intermediate System to Intermediate System)**.

OSPF:
This is the most commonly used protocol inside an AS even though on the edge router, BGP is used. It converges faster and much more efficient than RIP. It uses **Areas**, meaning a group of interconnected routers to control the reroute traffic. For the backbone of this setup, **Ared ID of 0** is defined.

In OSPF environment, an OSPF router initially send out a **Hello Packet** looking for an adjacent OSPF capable router. Once found, it then exchanges information via **Link State Advertisement(LSA) Packets**.

NOTE: OSPF Converges immediately whereas RIP does in 30-60secs.

IS-IS:
It is similar to the OSPF. The only advantage was that it worked with IPv6 address. It was based on the concept of **Areas** and send only the updates to the routing tables.

Hybrid:
The time when RIP was in demand and OSPF was not developed, cisco came up with a new version of **IGRP(Interior Gateway Routing Protocol)** which was **EIGRP(Enhanced IGRP)**. It was both a distance vector and link state protocol hence was termed hybrid.

Protocol	Type	IGP or EGP?	Notes
RIPv1	Distance vector	IGP	Old; only used variable subnets within an AS
RIPv2	Distance vector	IGP	Supports VLSM and discontiguous subnets
BGP	Path vector	EGP	Used on the Internet, connects Autonomous Systems
OSPF	Link state	IGP	Fast, popular, uses Area IDs (Area 0/backbone)
IS-IS	Link state	IGP	Alternative to OSPF
EIGRP	Hybrid	IGP	Cisco-developed; less common on non-Cisco routers

Table 7-2 Dynamic Routing Protocols

Route Distribution:
When a router has more than one protocol working and it learns a specific route of a path with one protocol and shares the same route with an another router through some another protocol, this is called **Route Distribution**.

Administrative Distance:

When a router has more than one choice of connecting to the same destination, it uses a feature called **Administrative Distance**, also known as **Route Preference**.

Working with Routers:

Connecting to Routers:

There are many ways by which we can connect the router to our PC and configure it before using. We can either create a physical connection using a cable known as a **Rollover Cable or Yost Cable** or we can use USB with settings of the router configured in it.

Once we have connected the router, we need to run some kind of program to set up router settings. This program is known as **Terminal Emulation**. Examples of this is **PuTTY, HyperTerminal, Cisco IOS (Internetwork Operating System)** etc.

Web Access:

Most routers nowadays come with a built-in Web Interface to enable us to set up everything on the router. For accessing the Web Interface, we must know the Router's IP, which exists by default or it can be given by accessing the Web Interface through other method.

Once we know the IP, what we do is we set the computer with a similar Network ID and connect to the router. Some of the Routers also carry a documentation while some are pre-configured with DHCP hence no need to set up IP or something.

Here, we have configured router for the PC we are connecting to but in the case of larger networks, the router needs a **Network Management Software (NMS)**. NMS are either OEMs or Third-Party.

Basic Router Configuration:

When we configuring the router, we need to make sure that every port is configured and also that routing table sends packet to the right destination.

WAN Side:

LAN Side:

Router Problems:

Routing Tables and Missing Routes:

MTUs and PDUs:

At each layer of the OSI model, the unit used for measurement is called PDU. There is always a defined size for this called **Maximum Transmission Unit (MTU)**. Sometimes, the frame exceeds the MTU and in such cases, fragmentation of frame is done which results in inefficiency. **Path MTU** refers to the largest packet size transmissible without fragmentation.

Tools:

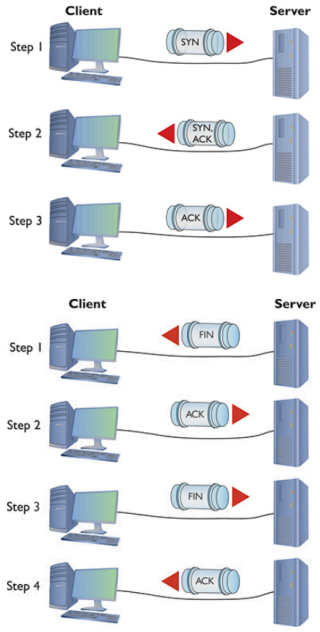
The **tracert** command in cmd.

8) TCP/IP Applications

June 8, 2024 5:33 AM

TCP:
It enables connection-oriented communication in networks. The three-way handshake works in TCP communication.

Any single communication between a computer and another computer is called a **session**. When a connection is made, it is done by sending SYN, SYN/ACK and ACK whereas for ending the connection, FIN, ACK, FIN and ACK is done.



UDP:
It is for the connection less stuff. It is for sessions of protocols like DNS, **DHCP, NTP/SNTP, TFTP** etc.

DNS:
DNS uses UDP on **Port 53** by default.

DHCP:
When it is being set-up, it doesn't know whether the other side of the network is ready, hence UDP.

For sending/receiving, DHCP clients use **Port 68** and servers use **Port 67**.

NTP/SNTP:
Network Time Protocol(NTP) and **SNTP(Simple NTP)** are used for synchronizing the clocks on the network.

NTP/SNTP servers use **Port 123**. And these servers have hierarchy from **Stratum 0** to **Stratum 15** in which the time is synchronized. Like Stratum 0 is very accurate and the later numbers not so much.

TFTP:
Trivial File Transfer Protocol(TFTP) also uses UDP.

TFTP uses **Port 69**.

ICMP:
UDP and TCP works at Layer 4 for sharing the data between different hosts. Similarly, there exists a protocol at Layer 3 called **ICMP(Internet Control Message Protocol)**, which doesn't transport data but communicates regarding the network information and errors.

ICMP works for low-level tasks like **host unreachable messages**, **router advertisements** etc. For example, ICMP works for the command **ping**. The ping utility sends an **echo request** to an IP address and the computers running TCP/IP will respond to this echo request with an **echo reply**. There are other responses as well like if the computer is unable to connect, it is responded by **destination host unreachable**. If the time for the request runs out, it is called **request timed out**.

Ping of death: Sending malicious packets to the users.

IGMP:
There exists the class of IPs which are intended for a particular group. The **Class D** group of IP is used for **multicasting**. When a multicast is done, it is not certain as to who wants to join the group and who doesn't. For this purpose, **Internet Group Management Protocol(IGMP)** works. IGMP enables routers to communicate with hosts and switches to determine as to who can join the multicast and create a **IGMP Group membership**. It works at **Layer 3**.

The Power of Port Numbers:
Port Number is basically a **16-bit** value ranging from 0-65535. It is used for the purpose of NAT.

Suppose we sent some packet to the server using our source IP and destination IP. We know the port to which we are sending the data but for the source part, the port number is always chosen randomly between **49125-65535**. These are known as **Dynamic Port(Ephemeral Ports/Private Ports)**. These numbers are decided by **IANA**. There are different categories of Port Number classification:

0–1023	Well-known ports
1024–49151	Registered ports
49152–65535	Dynamic, ephemeral, or private ports

Registered Ports:
When two computers are communicating or say are in a session, they store the information at a location called **Socket** or **Endpoint**. Sockets on both the ends is collectively called **Socket-Pair** or **Endpoints**.

To see all the active connections on the computer at a glance, we run **netstat** command.

Connection Status:
We can run netstat command to see the status of any connection in our system.

Any port which is ready to respond to any traffic is called **listening port** or **open port**. Usually, every application has a listening port. Every **web server** has a listening port on **Port 80**. To see all the listening ports, we can run **netstat –an**.

```
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
```

From this line, we can see that listening port 445 is ready to receive traffic. Since no one is connected, the **Foreign Address** is **0.0.0.0**.

ESTABLISHED ports are those which are already in a session.
CLOSE_WAIT ports are those where the web server requests a close.

Running **netstat –ano** will show all the connections with PIDs and running **netstat –anob** will show the programs as well.

TCP/IP Applications:
There are many applications which use the TCP/IP suite. Whenever it is asked which protocol is used by the x service, this means for the server side always.

Telnet and SSH:
E-mail:
SQL:
FTP:
Active vs. Passive FTP:
HTTP and HTTPS:
SSL(Secure Socket Layer)/TLS(Transport Layer Security):

9) Network Naming

June 10, 2024 8:49 PM

Before DNS:

> **NetBIOS:**
> It was developed by **Microsoft**. How this worked is that when every computer boots up, they would broadcast their **Name and MAC**. All the computers connected to this computer in the network would store this information in a **cache**. This was all done over the **NetBEUI (NetBIOS Extended User Interface) Protocol**. So we can say NetBIOS over NetBEUI.
>
> When the network enlarged, NetBIOS was no longer supported due to broadcasting issues. But Microsoft couldn't change this because all the systems were already using it. So, they came up with a different way of naming called **NetBIOS over TCP/IP** and this was known by the name **NetBT**.
>
> **TCP Ports** used were **137** and **139**. **UDP** were **137** and **138**.
>
> NetBIOS over TCP/IP alone couldn't share any resources and used another protocol called **SMB(Server Message Block)** to share files and folders. However, SMB today runs alone on **TCP Port 445**.
>
> **Hosts File** is basically a file that would store the naming resolution for computers in the network. This was developed when the ARPANET was used and still can be found in **C:\Windows\System32\drivers\etc**.

DNS(Domain Name System):
It relies on the delegation, meaning to pass-over, to make naming easy. Using this, the top level domain passes its job to its subsidiary DNS system and the process continues.

DNS Servers use **UDP Port 53** or **TCP Port 53**.

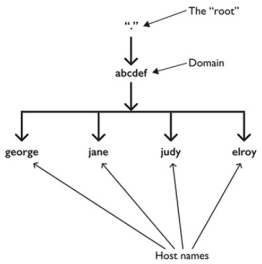
DNS servers divide the work in two ways, one is **resolver** and the another is **name servers**. Resolvers are basically used for querying the DNS Server. Namer servers are basically the **DNS Servers** from where the IP is queried. DNS Servers hold the **IP DNS Database** which is called a **Zone**. The name servers are arranged in a hierarchal manner, like one acting as a root and others it subsidiaries.

The root of the DNS Servers is a bunch of computers dispersed around the world and forms the **'root'**. These are basically called **Root DNS Servers** and are only **13** in number. The second Name Servers that come after this are called **Top-Level Domain Servers(TLDs)**. And then comes **Second-Level Domain Servers(SLDs)** and **Subdomains**.

Authoritative Name Servers are basically the servers which hold the **Zone** they are present at the organization which hosts the DNS.

ICANN takes care of adding the **TLDs**.

> **Name Spaces:**
> Networks which use DNS Names rely on using these names in an hierarchical manner called **Hierarchical Name Space**. For ex, a file in Windows could be as C:\Program1\Backup\Data.txt, DNS Name Space kindly works the same way.
>
> In DNS Hierarchy, we have **Root > TLD(or SLD) > Subdomain**. A complete DNS name which has all these values is called a **FQDN(Fully Qualified Domain Name)**.
>
> Let's see how the FQDN is written.



A **FQDN** is written from left to right by root side being on the right and separated by a period. For the above, it can be written as

george.abcdef
jane
judy
Elroy.abcdef

Since the root server is ".", there is no need to write it at the end because it is always presumed.

If we talk about a website, we write

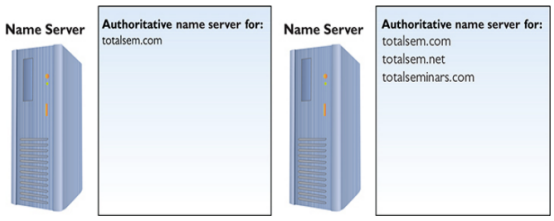
www.google.com

Here, **.com** is a TLD, **google** is a SLD and **www** is the subdomain.

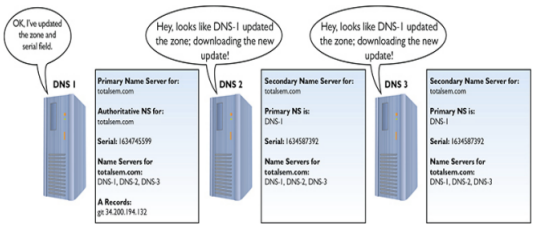
Name Servers:
DNS works on both small/private network and internet.

Record: A single piece of record which stores a name with an IP.
Zone: A collection of records
Name Server: Server which responds to resolvers

DNS Server can also be authoritative for more than one domains in case our network is using two or more domains.



Opposite to the above situation, a single domain can have multiple servers. For example, totalsem.com can have multiple DNS Servers. Large networks usually have a **Primary Name Server** and then one or more **Secondary Name Servers**. These servers share their zones to update and match records and this process is called **Zone Transfer**. The primary name server have a special value called **Serial Field**. If the update records, there is a change in this value. The secondary server regularly compares this value and if there is a difference, zone transfer is done.



Reverse Zones:
When we type a domain name and the DNS converts it into an IP is called a **Forward Lookup**. The reverse of this process, converting an IP into a particular DNS, is called **Reverse Lookup**.

A DNS server only allows Reverse Lookup if it is enabled. It is saved in the Zone by reversing the network ID and adding a unique domain **in-addr.arpa** to it. For example, all the Reverse Lookup addresses belonging to the Network ID **192.168.4.1** will be saved in the Zone **4.168.192.in-addr.arpa**.

Name Resolution:
When we type out an address in the web browser, this address is resolved into an IP address by some **Resolver**. First, the operating system would consult its local DNS server called **Resolver Cache**. This is basically the area where recently resolved addresses can be found.

To see these, we can run **ipconfig /displaydns**.

If the resolver cache couldn't resolve the name, it then makes a **Recursive Lookup** request to its external **DNS Resolver** for the IP. This external DNS Resolver is basically the DNS Server which we provide information in our PC while configuring the basic information like IP, Subnet, Default Gateway etc.

DNS Resolver makes a request to the root servers, root server will respond by providing the IP for the TLDs. Upon contact with TLDs, they provide the IP for Authoritative Name Server. This server provides our local DNS the IP which we are looking for and this whole process of looking is called **Iterative Lookup**.

Administering DNS Servers:
In Windows Server, the program that controls the domain naming is called **Windows DNS Server**. All the management of accounts and passwords of Windows Network is done in kind of a directory called **Active Directory**.

The meaning of **Domain** stands for a Domain name or something but for Windows DNS Server, it is used for calling out something specific in Active Directory. The system that manages an active directory is called a **Domain Controller**.

The most popular DNS Server used in UNIX/Linux systems is called **BIND**.

Windows DNS Server uses a folder analogy to show DNS zones and records and it is basically visible with three folder icons, **Forward Lookup Zones, Reverse Lookup Zones** and **Cached Lookup Zones**.

Caches Lookup Zones:
It is basically the practice of storing the recently visited DNS and keeping them in organized fashion. This helps in resolving the recent visited DNSes faster. How often a record is refreshed is based on the TTL(Time to Live) number. The less the number, the frequent the record updates and vice-versa. It is generally recommended that the TTL should be kept longer so just in case, if any hacker tries to make a difference, it could be solved with more TTL time.

Forward Lookup Zones:
The purpose of resolving a DNS name to specific IP. For a particular Domain in a network, we basically have a record and that record consists of three different fields, Name, Type and Data. Name is the name of the DNS, data is either IPv4 or IPv6 address and type is explained below.

DNS Record Types:
There are various record types used in DNS naming. The different record types help in resolving the DNS in different ways. Here are some record types, **SOA, NS, A, AAAA, CNAME, PTR, MX, SRV** and **TXT**.

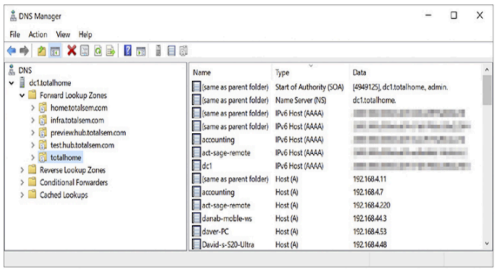


Figure 9-20 Forward lookup zone totalhome

SOA:
In every zone, there is always a record for which the zone is **SOA(Start of Authority)**. It is basically a record type which defines the primary name server in charge of the domain. For example, in the above, the first record is totalhome as SOA. This explains that for a domain called **totalhome**, the primary server is the server above.

NS:
An NS record points to the server that holds the primary name server for a particular DNS. For example, a record **ns1.example.com** will be responsible for handing the queries of the domain **example.com**.

A:

Each individual using a DNS will get an A record which resolves their DNS into an IPv4 address.

AAAA:
This is similar to the, but the host will get an IPv6 address. Since IPv6 is four times of IPv4, hence AAAA as four times of A.

CNAME:
It is known as Canonical Name. For example a domain mikemeyers.com can also be named as mike.com. So basically mikemeyers is a canonical name(original name) for mike and the cname record type will hold all these details.

PTR:
It stands for Pointer Record(PTR). This is generally seen in reverse lookup zones which acts opposite to the A and AAAA and helps resolve IPs to DNS.

MX:
It stands for **Mail Exchange(MX)**. This record holds the information of the email server belonging to that domain.

SRV:
These are similar to the MX records but the use of SRV records is to keep the information of servers which are responsible for a particular service. SRV stands for **Service Record(SRV)**.

TXT:
A text record is basically a record which is used to store text which is associated to a particular domain. The primary use of TXT record is for securing, verification, keys etc.

Public DNS Servers:
Publicly used by people for DNS Resolving purposes. However, Private ones are used for implementing security, performance, control, reliability etc.

Dynamic DNS:
Modern computers support DDNS to make automatic updates in the DNS servers.

DNS Security:
The DNSs have been made secure with the **DNSSEC(DNS Security Extension)** and **EDNS(Extension Mechanisms for DNS) Protocols**.

Troubleshooting DNS on Clients:
Whenever a problem occurs with the server not found error, we first flush the DNS using **ipconfig /flushdns** and then try to ping the address for some popular website and from there we need to see if the DNS name is successfully resolved into some IP address. If the name is not resolved into a proper IP, we need to see if the problem is in the local DNS or farther down the line. In this case, we need to ping using the IP address and if that worked, it states that there is a problem in the DNS.

To check the DNS, we first check if the entry of the DNS server is correct. This is done my matching the entry of the DNS Server with the ipconfig /all command outputs. If they do not match, we need to refresh the DHCP Settings.

If the DHCP is resolved, the further problems can be checked using **nslookup**. The nslookup command can be used in either **interactive** or **non-interactive mode**.

For the Unix/Linux systems, the command used for querying DNS is called **dig(domain information groper)**.

Diagnosing TCP/IP Network Issues:
The steps taken in diagnosing are:

Diagnosing the NIC
NIC's Driver
Diagnose Locally
Check IP and Subnet
Run Netstat
Diagnose the Gateway
Diagnose the Internet

10) Securing TCP/IP

July 2, 2024 8:32 PM

Let's understand the following terms
Encryption | Integrity | Nonrepudiation | Authentication | Authorization

Encryption:
When we run a **plaintext** data through a **cipher algorithm** using a key, we get the encrypted **ciphertext**.

- Cipher: The way of encrypting the data
- Algorithm: The underlying formula behind the cipher
- Ciphertext: The text received after it has been passed through cipher

Substitution:
It is also called **Caesar Cipher**. It worked on the principle of swapping alphabets.ch

Weaknesses are it could be broken by brute force by doing frequency analysis. Repetitive words, so easy to guess

XOR(Exclusive Operation):
In this method, we take a key and perform some math in some sequence. This is also called **Bitwise Operation**.

We use a key to encrypt & decrypt the data. When the key used for both these purposes is same, we call it **Symmetric-Key Encryption and Asymmetric** when the key-pair is different.

Symmetric-Key Encryption:
In Symmetric-Key Algorithms, there are two different kind of ciphers.

Block Cipher:
In this kind of algorithm, suppose we have a 1000 byte file, BC will split it into 128 byte and perform encryption systematically. A renowned block cipher is **AES(Advanced Encryption Standard)**.

Stream Cipher:
In this kind of algorithm, the encryption would be performed on individual byte

Asymmetric-Key Encryption(Also Public-Key Cryptography):
In Symmetric Enc, if a person gets to know the key, he/she has the access to data but if this key is encrypted inside some another container and that container would have two different keys or say asymmetric key-pair then it would enhance the security. This is the use of asymmetric-key encryption.

The two key-pairs used in this kind of cipher is called a **Public Key** and a **Private Key**. Now suppose two persons are in a session, Data encrypted with the public key, for example, must be decrypted with the private key, and **vice versa**.

RSA(Rivest, Shamir and Adleman), DSA(Digital Signature Algorithm) and ECC(Elliptic Curve Cryptography) are the ones used today.

Integrity:
It is the act of maintaining the integrity while the data is being carried.

Hash:
It is mathematical function which we perform on some binary digits of any given length and the resulting file is a value which is always same in length no matter how large the input is. The resulting file is called **Checksum or Message Digest**.

Hash is **one-way function**, which means that even if we have both Checksum and the algorithm used, we cannot get the string back out of the checksum, meaning irreversible. This is usually used in scenarios where, for ex, we need to match the file integrity like checking if the version of software we have installed is the same as it is on the reputable source.

MD5:
Message Digest, producing **128-bit** digest.

SHA(Secure Hash Algorithm):

SHA-1, producing 160-bit Digest
SHA-2, has six variants; **SHA-224, SHA-256, SHA-382, SHA-512, SHA-512/224, SHA-512/256**
SHA-3, also has six variants; **SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256**

Nonrepudiation:
This is the way of saying that a person cannot refuse what he/she has done. The way it is implemented in network security is by combining encryption and integrity(hashing) called **Digital Signatures**.

Digital Signatures:
To create a digital signature, the **sender hashes a message**, and this **hash is further encrypted with the sender's private key**. The receiver would **decrypt the hash with the public key** provided by the sender and **confirms the hash with message's hash**.

In this case, what ensures nonrepudiation is the fact that the hash is created by the sender using his private key, which only he has. So he cannot deny the fact that the digital signature associated with that message is created by him unless he claims that his private key was stolen.

The use of DSs in modern computers is to verify installed programs came from their registered developers, it is also used in verifying which websites are secure.

PKI(Public-Key Infrastructure):
The idea of issuing certificates is that it includes a public key, its own information and the digital signature of trusted authority. It also includes details like when it was issued, who issued it, who they are issuing it to, when will it expire etc. All this information tells us the resources we are using are legit.

Every browser we use have a list of **root certificates**, which are **pre-approved certificates** that come from **Certificate Authorities**. When a certificate is issued on a website, the browser confirms this certificate with the root certificate it is already carrying.

Now all this act of CAs issuing certificates and the browsers verifying it is called Public-Key Infrastructure, which is done to maintain nonrepudiation.

Authentication:
It is the method of verifying that you are actually the person who is using the system/resource. This verification can be done in several ways or **attributes**. Some of these are

Something you know
Something you have
Something you are
Somewhere you are
Something you do
Some when you are (Logging at a specific time)

Authorization:
This is the method of defining different levels of access and in order to do that we use an **Access Control List(ACL)**.

ACL defines the list of permissions that an authenticated user can do. When an ACL assign access to something, it used different ways/models for this use. These models are called **Access Models**. There are three different kinds of Access Models

Mandatory Access Control(MAC):
A user is assigned access if is meeting a certain security criteria

Discretionary Access Control(DAC):
A user is assigned access by his/her owner's decision

Role-Based Access Control(RBAC):
A user is assigned access based on his role. This is the most popular

Organizations use **NAC(Network Access Control)** methods for network security

TCP/IP Security Standards:

User Authentication Standards:
When the dial-up connection was used for accessing Internet, but the companies wouldn't want anyone to be dialing into their computers. To prevent this, they developed a security standard which was later adopted by TCP/IP. It was called **Point-to-Point Protocol**.

PPP(Point-to-Point Protocol):
It enables two devices to connect, authenticate with usernames and passwords. Both the devices will first decide their parameters like the protocol they are going to use, their medium, maximum transmission units etc. And then setup the connection.

There are two ways in which PPP authenticates password-

Password Authentication Protocol(PAP):
In this method, the username and password are shared in a plaintext file, which makes it less secure.

Challenge Handshake Authentication Protocol(CHAP):
This authentication relies on hashes and handshakes. At first, the initiator of the connection will make initial connection request to the authenticator, which responds back with some challenge or say nonce. The initiator will then create a hash which be based on the password, provided nonce and a hashing algorithm like MD5. Authenticator will store this hash and when the user log in back again, hash is matched.

When the dial-up connections back in 1990s boomed, Microsoft introduced its own **MS-CHAP**. The current version is **MS-CHAPv2**.

PPP is great for handling Point-To-Point connections but it has some limitations. What PPP assumes that all the usernames and passwords are stored at the endpoint (here endpoint refers to the computer to which the user is trying to connect). But in modern systems, we have multiple access points to a resource.

If we try to implement PPP in modern systems, suppose we have a modem and in this modem we can dial up any user's connection. Here, according to PPP, it considers that the username and password are stored in modem but that is not the case because we cannot store usernames/passwords in each modem. For this reason, we need a central database for username and passwords.

But if the data in Central Database is not protected, anyone can access the usernames/passwords. For this reason, a new philosophy was introduced called **AAA**.

AAA(Authentication, Authorization and Accounting):
It was designed for the idea of **port authentication**, meaning allowing remote user authentication to a particular port to another network.

Authentication
Authorization
Accounting:
The authenticating server **keeps record of events** such as logins, session actions, user bandwidth usage etc.

The two technologies based on it are RADIUS and TACACS+

RADIUS(Remote Authentication Dial-In User Service):
It created to support hundreds of modems to connect to a single central database but it is still used for several purposes today like Microsoft's Windows Server version uses **IAS(Internet Authentication Service)** which is based on RADIUS.

It consists of three devices, the server that has access to all the database of usernames and passwords, a number of **Network Access Servers(NASs),** which control the connection of modems, and a group of systems that connect to the network either via modem or modern wireless standards.

RADIUS – UDP Port 1812/13 or 1645/46

TACACS+(Terminal Access Controller Access Control System):
It was developed by CISCO to support AAA in networks with many routers and switches. It is similar to RADIUS but the **TCP port used is 49**.

Kerberos:
This protocol is not based on PPP but rather connecting clients to a single authentication server. This approach is even used by Microsoft in Domain Controller.

Kerberos uses **UDP or TCP port 88** by default.

KDC(Key Distribution Center), which is installed on Domain Controller, supplies services like session tickets, session keys etc. It relies on two components: the **Authentication Server** and the **Ticket-Granting Service**.

When a user logs onto the domain, a hash of the typed password is sent to the Authentication Server, it then matches the hash and responds back with **Ticket-Granting Ticket(TGT)** (or Ticket to Get Tickets) with a timestamp, which usually has a lifespan of **10 Hours**. The user then sends the timestamped TGT to the TGS for authorization. The TGS then sends a timestamped service ticket, which is also called a **Token**, back to the client.

The access token contains helps in accessing the resources. It contains **Security Identifier(SID)** for the user's account and for the groups of which the user is a member**.**

This token is used in accessing all the resources within the system and no reauthentication is required. This is called **Single Sign-On(SSO)**.

Limitations: If the KDC goes down, no one has access. Also, all the computers need to be synchronized within 2 minutes.

Encryption Standards:

SSH:
Telnet was an older protocol which was used for remote accessing and managing network devices but due to its lack of security, a new protocol was developed called **Secure Shell(SSH)**.

When the client first tries to log onto an **SSH server**, the server sends its **public key** to the client. The client then creates a **Session ID**, encrypts it using the public key and sends it back to the server. The server decrypts this session ID and uses it in all data transfers going forward. This session ID only stays between the client and the server. The type of encryption both the ends use is invisible to the client but it is generally **AES**. Until this point, only the connection is established, no authentication, nothing is done.

Now, since we have established a connection with the SSH server, how would the server know as to who is allowed to share the resources and not. For this reason, they **authenticate using the SSH Server's password** which the client has to enter.

Another method for SSH Authentication is using Public Key instead of passwords. Here's how it works:

The client first creates a **key-pair**. The **public key** is then shared with the server. This public key is added to the **server's authentication list** when the client is connected to the SSH Server via password authentication or it can be added when the client is trying to make a connection for the first time. Now, the server sends a **nonce**(some number) to the client. The client creates a **digital signature** of this nonce using his/her private key and sends it to the server. The server verifies this digital signature by decrypting it with the public key it has and if the **nonce matches**, the user is authenticated.

The key-pair can be generated using **PuTTY Key Generator** or **keygen**.

This way, Telnet was replaced by SSH. With SSH, applications can create a tunnel through **Tunneling**.

Tunneling:
It is the process of connecting two endpoints which are **end-to-end encrypted**. For ex, if the tunnel is SSH Tunnel, the client would send the data of an application through a tunnel to the server using SSH, the server would then decrypt this particular data only to the application it is intended to.

Combining Authentication and Encryption:

SSL/TLS(Secure Socket Layer and Transport Layer Security):
Netscape Navigator was the browser which introduced the concept of SSL. According to this, the SSH Server should have a certificate which is shown when the client **requests** something. When the client makes a request, the server responds back with a **certificate**. This certificate is further matches up with the **root certificates** in a browser. This way, both the sides(SSL Server and SSL Client) are now in a very secure encrypted tunnel.

TLS is almost the same but it supports more newer applications. Like **HTTPS, VoIP, VPNs** etc.

IPsec(Internet Protocol Security):
It is a protocol which works at the **Network Layer** of the OSI Model. This works in two ways, one which only encrypts the payload, called the **Transparent Mode** and the other which encrypts the entire IP packet, called the **Tunnel Mode**.

The two protocols which further works under IPsec are **AH(Authentication Header)** and **ESP(Encapsulating Security Payload)**. AH provides less authentication and ESP Provides more thus ESP is preferred.

Securing TCP/IP Applications:

HTTPS:
Uses TLS for actual authentication and encryption.

Securing E-Mail Protocols:
SMTP(Sending) and **POP/IMAP(Post Office Protocol and Internet Message Access Protocol - for Receiving)**. These are not secure and hence better protocols are used with TLS like **SMTPS(TCP Port 587)**, **POP3S(POP3 Over SSL – Port 995)**, **IMAPS(IMAP Over SSL – Port 993)** etc.

A command used to secure emails is called **STARTTLS** which makes a request to the server stating that the client wants to run the email service with TLS.

SCP(Secure Copy Protocol):
Alternative to FTP but not so much used instead, **SFTP** is preferred. Uses TCP Port 22.

SFTP(SSH FTP):
Not SSH over FTP but designed in a different manner and very secure as compared to FTP. Also, **FTPS** stands for **FTP with enhanced security of TLS**.

SNMP(Simple Network Management Protocol):
If the network devices are SNMP capable, we can query them regarding their status like CPU Usage, Network Utilization or even firewall hits.

The device which is SNMP Capable stores a server called **MIB(Management Information Base)** and information is shared from this.

Older versions **SNMPv1** and **SNMPv2** were not secure and **SNMPv3** is the current one. **UDP Ports used are 161 and 162**.

Zabbix is a SNMP Software.

LDAP(Lightweight Directory Access Protocol):
It is used in managing directory services in a network. It used **TCP/UDP Port 389** whereas **LDAPS(LDAP Over SSL)** uses **Port 636**.

11) Switch Features

September 28, 2024 6:00 PM

Switch Management:
The simple switches (**unmanaged switches**) which only handles the task of forwarding the traffic with the user being no control over it. They have embedded optimized hardware like **data plane** and **forwarding plane** which automatically looks after the traffic.

> **Managed Switches:**
> In managed switches, there is an operating system which enables device configuration.
>
> The device also uses the hardware and OS resources to run software which, in result, implement other features. This overall terminology is called **Control Plane**.
>
> We can connect to the switch using **Console Port**.

Setting up Unmanaged Switches:
An UM Switch needs an IP address for configuration on layer 3. A new switch comes with a default IP Address, username and password, but we can assign it an IP which is being used by our network.

The another thing which needs to be done is updating the firmware of the switch over the internet.

Access Management:
When we are accessing the configuration page of a switch, it is done in two different ways

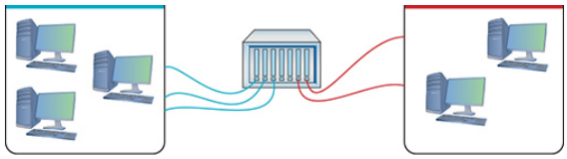
> **In-Band Management:**
> In this method, we connect the switch to our existing network and configure from there.
>
> **Out-Band Management:**
> In this method, we connect to the switch with a different dedicated port on it, which allows us to have a robust security as the management port is entirely different from the regular traffic flowing in the network.

Port Configuration:
Sometimes the ports in a switch require some configuration like speed, duplexity, flow control, frames, security etc. To see the current status/configuration of the ports, we can run command like **show config, show interface** and **show route**. Note these commands are not universal and can vary a/c to different vendor/OS for the switch.

> **Speed and Duplex:**
> The port speed in automatic in modern switches. However, we can setup the speed as per the circumstances. Same goes for the duplexity.
>
> **Flow Control:**
> If a host cannot keep up with the flow of the traffic, the speed can be controlled using **PAUSE** frames which are sent to the router to make a pause.
>
> **Frames:**
> One another use of port configuration is **Jumbo Frame**, which are basically frames larger than the standard frame size. These are used while reading/writing to a storage device.
>
> **Port Security:**
> This means locking the port to a specific MAC Address. In CISCO networks, this is also termed as **Sticky MAC** or **Persistent MAC**.

Virtual LANs:
A VLAN enables us to segment a physical network into multiple networks without having to add additional hardware. For CompTIA, VLAN is **data VLAN**, which is different from **voice VLAN**.

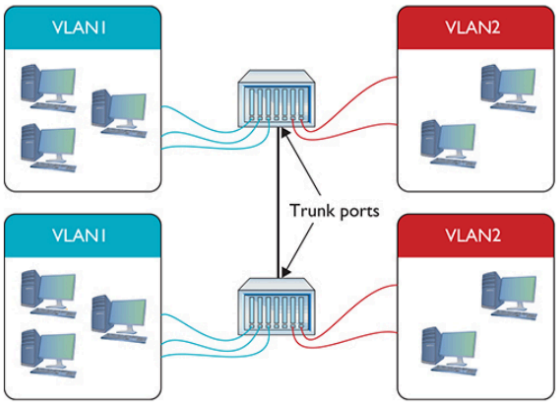
To convert a switch to VLAN-Capable, we take the single physical broadcast domain and chop it up into multiple broadcast domains. To do so, we first create two virtual broadcast and name them something using the programming in the Switch, say VLAN01 and VLAN02. Now, we can assign the ports in the switch to these specific VLANs.



NOTE: In a single broadcast domain, every LAN is VLAN01 by default.

Trunking:
Suppose we have two switches, which are interconnected to 5 computers each, this way we have 10 computers. We want to create VLANs in such a way that both the switches have the similar VLANs, say switch one has VLAN01 and switch two has VLAN02. This is usually achieved using Trunking.

We will assign VLANs to individual switches and then connect those switches using a specific port, called **Trunk Port** or **Tagged Port**. However, the port to which the host is connected is called **Access Port**. There is a trunk standard **IEEE 802.1 Q Trunk**



Configuring VLAN Switch:
We can access the Switch using **SSH** not Telnet. Every switch manufacturer has its own interface for configuring VLANs and their corresponding software for accessing. First, we create VLANs, then we assign them a port which is called **VLAN Assignment**.

Assigning VLANs and Tagging:
When we are sharing some resource to the same VLAN ID but which is connected to a different switch, we use **802.1Q Port Tagging**, which is basically a tag added to the frame.

How this happens; the host computer sends a frame and the switch verifies if the frame is associated with a VLAN ID in itself. If so, the frame is sent to the VLAN without a tag, otherwise, the frame is send to the Trunk Port.

Native VLAN is basically a default port setup in a switch which forwards untagged frames. So when the frame is sent to a different switch via trunk port, the receiving trunk port will check if the frame is intended for native VLAN, if so, it is sent without a tag. But if the frame is intended for a different VLAN, the trunk port forwards it to the respective VLAN with a **802.1Q Tag**.

NOTE: In modern systems, the Native VLAN is configured to a VLAN which is not used and even that is configured with a tagging scheme because hackers otherwise can get access to VLANs using **Double-Tagging Attack**.

VLAN Trunking Protocol:
Suppose we have a large network with multiple VLANs setup. In this case, if we want to modify the VLAN settings like adding/removing VLAN, there is a protocol dedicated for this purpose called **VTP(VLAN Trunking Protocol)**. With this protocol, we can put the switch in different states like **Server, Client** and **Transparent**. The server would act as the one who is **exchanging** the information on the network and the client would be helpful in **updating** the VLANs. Also, when a Switch is configured with Transparent mode, it is basically done when we don't want it to make changes in itself but rather **share** changes to other trunks.

Inter-VLAN Routing:
When we have to share the traffic between same VLANs, we can achieve it easily using 802.1Q Tagging Scheme. But, if we want to share the traffic between two different VLANs, we have to use the router because eventually these are two different networks. This sharing of traffic between different VLANs is called **Inter-VLAN Routing**.

How this is achieved is that a single physical port of the router is further broken into logical sub interfaces for each VLAN. This is achieved by adding the Router's Port to any existing Switch's trunk port, because eventually they are connected, and this is referred to as **Router-On-a-Stick** configuration.

If our network is big where we have lots of VLANs connected, then it is never a good idea to connect a router because all the traffic is going through the router. For this reason, **routing-capable switches** are made. Ex- **Juniper EX3400**, capable of working at both Layer 2 and Layer 3.

DHCP and VLANs:
Since the DHCP Discover message is a broadcast message, it cannot be sent to a different broadcast, or say a different VLAN. For this, we use **DHCP Relay**. For CISCO, Relay is implemented using a **IP helper** commands which generates an **IP Helper Address**. This address supports relaying for several protocols

DHCP Relay – PORT 67
TFTP – PORT 69
NTP – PORT 123
TACACS+ - PORT 49
DNS – PORT 53
NetBIOS – PORT 137
NetBIOS Datagram – PORT 138

Voice VLANs:
This is used for prioritizing Voice Traffic over Data Traffic

Private VLANs:
A private physical port on a Switch allows creating a private VLAN which is separated from the entire traffic on the network.

Troubleshooting VLANs:

Multilayer Switches:
These are the Switches which work at more than one layer of the OSI Model. If a port is working for Layer 2, it is called **Switch Port** and for Layer 3, it is called **Router Port**.

These can also be termed as **Advanced Networking Devices** or **Multifunction Network Devices**.

There are a several number of features which are handled by these devices, which are:

Load Balancing:
This is the feature through which, for ex case, we can say that a website has three server and handles thousands of requests per second.

This is achieved by making a bunch of servers look like a single server, creating a **server cluster**. These servers distribute the requests evenly and with many methods

DNS Load Balancing:
How this works is that a same website will have multiple web servers, each with their own **Public IP Addresses**. Every time we make a request, the DNS Server resolves the request by addressing us to that particular DNS. In our case, our DNS server will store all the IPs corresponding to the FQDN. Meaning, a FQDN can be accessed via various different IP addresses or different web servers.

In the DNS Record, the record will be saved in such a way that several copies of **A Type** record will be saved for that particular FQDN. When we will try to access the FQDN, the DNS will use different IP every time and this is known as **Round Robin**.

Content Switching:
In case of Layer 2 and Layer 3 based Switches, the load is handled by inspecting the Frames/Packets but there are network devices called **Content Switches** which handle traffic on **Layer 7** by inspecting the data like URLs, type of file etc. And balance load according to it.

QoS and Traffic Shaping:
Quality of Service is basically a policy which we can use to prioritize traffic based on certain rules like bandwidth, PC, user, VLAN etc. There is also an another terminology called **Traffic Shaping** which controls the flow of traffic in and out.

Port Bonding:
This is basically the act of joining two ports and treating them as one for the purpose of achieving high speed by multiplying the throughout. Usually done in data centers.

Other names are: **Link Aggregation, NIC Bonding, NIC Teaming, Port Aggregation etc.**

Port Aggregation Protocol(PAgP) and Link Aggregation Control Protocol(LACP)

Network Protection:

Intrusion Detection/Intrusion Prevention:
And **IDS(Intrusion Detection System)** is basically an application running on dedicated IDS Box which inspects packets, look for active intrusions by working inside a network.

There are two kinds of IDSes, **Host-Based IDS and Network-Based IDS(NIDS)**.

Intrusion Prevention System(IPS) works on the network and actively monitors traffic.

Port Mirroring:
This is the act of copying all the ports or a single port to some other port for the purpose of seeing the traffic all at once.

There is one more method instead of Port Mirroring called **Network Tap** also known as **Traffic Access Port or Test Access Port**. This is better than Port Mirroring.

Proxy Serving:
It is like a mediator between the client and the web server. Whenever a request is made by the client to a server, it is first sent to the proxy server and the proxy server then itself handles this request further. Similarly, if the web server responds to the request, it is filtered by the proxy.

We have to setup our proxy server in the network settings.

A good use case of using proxy is that it keeps the cached data, hence results are quicker. There are various public proxy servers available.

In **Forward Proxy Service**, the client makes a request to the Server where the proxy checks only checks if we are allowed to do so, based on that it allows and deny, but we know the server we are interacting with.

In **Reverse Proxy Service**, when a client makes a request, the proxy not only decides if we are allowed to access that resource but also hides the server it is going to use and the response we get is from **anonymous server**.

AAA(Triple AAA):
Port Authentication is a way which gives us a way to protect our network from unwanted people trying to access the network.

Suppose a person comes up to a port and try plugging into the ethernet. In this case, we can setup several settings before the person gets to the network like,

12) IPv6

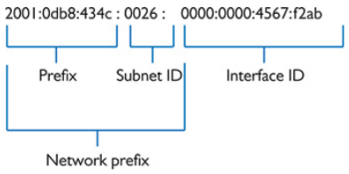
September 30, 2024 9:48 PM

Understanding | Implementation | Deployment

IPv6 Concepts:

IPv6 Address Notation:

Length	**128 bit**
Groups of	**16 bits (Hextet)**
Writing Form	**Hexadecimal**
Parts	**Network Prefix, Interface ID**
Net Prefix Part	**Routing Prefix, Subnet ID**
No. Of bits for Network Prefix	**/x**
Loopback Address	**::1**
Values	**Can not be entirely 1 or 0**
Notation	**Zeros Could Be Skipped, only once**



Link Local Address:
When the computer boots up, it assigns itself an IPv6 address without internet and this address is termed as **Link-Local Address**

Note that for IPv4, zeroconfig address is assigned using the **APIPA-Addressing** whereas for IPv6, it is assigned by **Link-Local Addressing**

First 64 bits(Network Prefix):	**fe80::/10** This states that the first 10 bits of the Link Local are reserved and will be used as Network ID of the address. The remaining **54 bits** in the prefix are always equal to **0**
Last 64 bits(Identifier ID):	It is referred as **Identifier** which is generated in two ways 1) A 64-bit **random number** called **Privacy Extension** 2) Using MAC address, called **EUI(Extended Unique Identifier)** If it shows us that our address is temporary, this means **privacy extension** is being using for the identifier which we can switch to EUI

Global Unicast Address:
A **Unicast Address** is the one which is not routable and used for internal communication in the network. When a computer get connected to the internet, an another type of address is assigned to it called **Global Unicast Address**.

Multicast Address:
In IPv4, we have broadcast but in IP6, we have only **Multicast**, not broadcast. Meaning, sending the data to interested group of computers.

These type of addresses are built from independent parts like a single IP6 multicast address will have different values/parts which will tell its characteristics

ff02 : : 2 - In this example, the first **"2"** indicates the independent part of the address, meaning that the scope of this message is **Local Network Segment**. The second **"2"** indicates that this message is destined for any **routers** belonging to that scope

When we send data to a user, we are usually concerned with the MAC Address. But that is an address which cannot be changed. In the similar way, we also have a **Multicast MAC Address**. This is basically a virtual address rather than the physical one and keeps on **changing** based on **Multicast Grouping**.

A multicast group is created on one computer and another computers, who want to be a part of this group, joins it. Once joined, all the computers are assigned with a **Multicast MAC Address**. The nature of Multicast MAC is that its first **16-bits** are always **33:33 Hex**., and the rest **32-bits** are **derived** from the **Multicast** Address Itself.

ff02 : : 2 is an address destined for Routers
ff02 : : 1 is destined for nodes in the network

Anycast Address:

Note that in IPv4, the number of addresses a system can hold is usually one whereas in IPv6, a computer could have different type of addresses like Link-Local, Unicast, Multicast, Anycast etc.

So, in anycast addressing, several computers are pre-configured with the same **Anycast Address**. Routers are configured in such a manner that they are going to forward traffic to that address based on the highest routing metrics or say the closest distance.

A use case of Anycast Address is in **Content Delivery Network(CDN)**. CDN allows to connect to the closest servers for faster connections. For ex: Netflix Servers could be connected to the closest for faster streaming

Neighbour Discovery:
Alike the ARP in IPv4, we have **NDP(Neighbour Discovery Protocol)** for IPv6 Networks. It works using **ICMPv6** and has five control message types which comes under the term **Packet Type**: Neighbor Solicitation | Neighbour Advertisement | Router Solicitation | Router Advertisement | Redirect

Neighbour Solicitation:
Solicited-Node Multicast Address is a type of multicast addressing in IPv6 which is used in discovering other nodes in the Network.

ff02 : : 1 : ffxx : xxxx

This is a Solicited-Node Multicast Address where the **last 6 x** denotes the last 6 digits of the **Unicast IPv6** for which we want to find the MAC.

So when NDP works, it first sends out an NS packet to the Solicited-Node Multicast Address, requesting to search for the MAC of corresponding Unicast Address.

Neighbour Advertisement:
When the user is requesting for the MAC using Neighbour Solicitation Packet, it also adds an another packet called **Neighbour Advertisement**, through which it dictates that, "I am reachable to my MAC Address" and adds its MAC address in the **Neighbor Discovery Cache**. This way, the receiving system can directly reach-out to the host via Unicast IPv6.

Router Solicitation:
This message is sent by the host in the network to find any routers on the network. These packets are sent to the **All-Routers Multicast Address**

Router Advertisement:
These contains important information about routers available on a local network like Router's MAC, their Link-Local Address, information about getting a Global Unicast Address etc. Routers send a RA packet in response to RS. An RA is sent to **All-Nodes Multicast Address** or to **Unicast**

IPv6 Implementations:

Stateless Address Autoconfiguration (SLAAC):
It is one of the methods by which computers in a network get their IPv6 addresses. It relies on the **NDP protocol**, where hosts assign themselves their own **link-local** address. Once assigned, it the sends a **neighbor solicitation** message on the same address, just to make sure it is **not already taken**.

An IPv6 user have **multiple global-unicast addresses** assigned at a time because they are temporary and keeps on changing because if the original global-unicast address is used there is a privacy concern. If the interface identifier is shared in the network, the host could be traced back to a specific device.

The key things a host needs from the router is the **Address Prefix**. It is usually achieved from the router advertisements that are sent by the router. Once received, this address prefix is **added to interface identifier** of the link-local address we are already having.

The router advertisement that a host receives, there could be multiple things derived from it like Default Gateway, DNS, Server Address etc.

DHCPv6:
In IPv6, DHCP Server works in two different ways, one is letting the user decide its own address and the second is giving it a DHCP generated global unicast.

> **Stateless:**
> Using Stateless DHCPv6, the DHCPv6 server lets the host pick its own address using **SLAAC**. DHCPv6 is needed to give clients other information like DNS Server IP, Time Server etc.
>
> **Stateful:**
> In Stateful DHCP assignment, the DHCPv6 server tell the host 128-bit address similar to IPv4.

When the DHCPv6 used by ISPs is called **DHCPv6-PD**. It works on prefix-delegation. Meaning, they rely on just passing the Network Prefix. For this to work, prefix delegation setting should be turned on.

NOTE: SLAAC is not widely used as not many networks have their own DHCP server so this is mostly common among special needs like data centers.

Default-Free Zone:
When multiple routers are interconnected, they have a default route. The use of this route in the router is to forward the packet incase the router doesn't know the router. Same process happens until the destination is found.

Now this doesn't happen in the routers of Tier 1 because they are the highest tier routers and know almost all the routes of the network so they doesn't need to forward it. The area of these routers is referred to as **Default-Free Zone(DFZ)**.

Aggregation:
If we talk about a single router in the DFZ, it would have almost 850,000 routes. If we organize these routes into a subnet, the size and complexity of routing tables will be reduced. This process of creating subnets is termed as **Aggregation**.

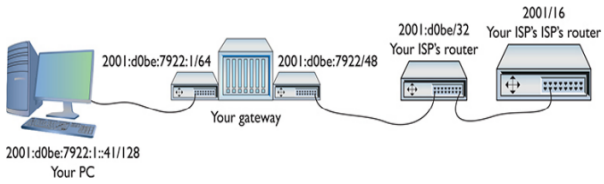


Figure 12-11 An IPv6 group of routers

Here, we can see that the Tier 1(RIR) router is /16 whack, Tier 2(ISP) is /32 and Tier 3(Our Router) is /48 which later adds up to /64 to the end users. Note that even though ISP provides us with /48, the person setting up the gateway further divides it to /64 by adding **16 bits(:0001)** to make it compatible several addresses. If the Tier 1 router tries to change the prefix, the routers **downstream** to it will share an router advertisement to **all-node multicast address** and all the clients eventually get a new prefix.

DNS with IPv6:
It works similar to IPv4 but we need to make sure the DHCPv6 is properly configured and if we are using SLAAC, we should be taking care of the **properly configuring** our DNS Server.

In DNS for IP6, we use **AAAA** type record to point to IPv6, which is **four times** to IPv4.

Moving to IPv6:
Usually, a computer is set up with both IPv4 and IPv6 which is called a **Dual-Stack**.

If we talk about the IPv6 address transition, it can be seen that almost all the **DNS Servers** and **Tier 1 Routers** almost **completely support** IPv6 address translation. But what is stopping us from transitioning to IPv6 completely is that suppose we are configured with IPv6 already but the computers to which we like to connect are not yet enabled. Once every computer is IPv6 enabled, we can say that the we have completely transitioned to IPv6. To achieve this, we can use some transition mechanisms.

Transitioning mechanisms are basically the tunneling standards which are set-up by the IPv6 folks for converting an IPv4 packet to IPv6 and vice-versa. Some of the standards are:

4to6:
It works like any other tunnel, **encapsulating** one type of data into another. For example, all the IPv4 traffic can be encapsulated into IPv6 packets. To make this work, we can download a **tunneling client** and install it on our computer.

6to4:
It works **opposite** to 4to6

Tunnel Brokers:
When a network with IPv4 is transitioning to IPv6, it needs to implement a tunneling protocol and this protocol is usually provided by **Tunnel Brokers**. Note that the above two 4to6 and 6to4 are transitioning mechanisms, not protocols. The protocols used are **TSP(Tunnel Setup Protocol) and TIC(Tunnel Information and Control Protocol)**

The biggest tunnel broker is **Hurrican Electric**

Overlay Tunnels:
It is the method of connecting two IPv6 networks over the existing IPv4 network. This way, the same existing physical connection can be used for the IPv6 packets.

NAT64:
This type of Network Address Translation is helpful in letting the IPv6 enabled computer to communicate with IPv4 servers. How this works is we have a **NAT64 Gateway** which handles the traffic between the IPv4 and IPv6 segments. This NAT64 Gateway can either be installed on the Server Side(**Stateless Mapping**) for automatic translation or on the Client Side(**Stateful Mapping**) for manual translation. The another system that works with it is **DNS64**, which helps in **resolving queries** of IPv6 and IPv4

13) WAN Connectivity

Sunday, November 03, 2024 5:28 PM

Before the Internet, faraway systems were **privately interconnected** using their own technologies but as the internet and WAN Connectivity(Wide Area Network) developed, those same connections became the way for internet

SONET:
Before, the international standard for **American** fiber-optic cable carrier was called **Synchronous Optical Network(SONET)** and for **Europe** it was **Synchronous Digital Hierarchy(SDH)**.

The physical traits of SONET like speed and bandwidth were defined by a standard called **OC Standard(Optical Carrier)**. There were various categories of OC like OC-1, OC-2, OC-3 etc.

The good thing about SONET was that it supported ring-topology in such a way that it is fault tolerable so that if a part of the ring breaks, data can still be sent.

BWDM, DWDM and CWDM:
These are basically the technologies which enable a single fiber line to carry multiple signals

BWDM(Bidirectional Wavelength Division Multiplexing):
Allows a light signal in fiber to travel in multiple directions using different wavelength, thus no need to have two separate fibers to create a connection

DWDM(Dense WDM):
Allows a single fiber to carry multiple signal by changing the color of the light

CWDM(Coarse WDM):
Just a simpler form of DWDM

Private WAN:
There are companies which need private WAN connectivity, for preserving their data from hackers and faster connectivity. They **lease lines** from telecommunication companies. Some of the private WAN technologies are: MPLS, SD-WAN, Metro Ethernet etc

MPLS:
The data is always carried in IP packets, but the route which this packet is going to take is decided by the router. If packets go through long distances, multiple routers have to make a decision

In a private connection, this process can be simplified by using a different switching technology at a few destinations. **Multiprotocol Label Switching(MPLS)** provides this facility. The idea is to provide routers a header information to route packets quickly instead of providing them with the entire routing table. MPLS adds an **MPLS Label** between layer 2 and layer 3, which looks like this

Label:
A unique ID for routers to move data more efficiently

Experimental Bits(Exp):
A value to prioritize some packets over the other

Bottom of Label Stack(S):
If a single packet have multiple labels, the first one will be assigned by 1 and followed

TTL:
Number of hops the label can go through

MPLS routers use their own dynamic protocols to send messages about the status of their data and resources

Some of the terms used in a MPLS environment are:

FEC(Forwarding Equivalence Class):
It is a group of packets which always follow the same path, hence no need for route lookup every time they pass through a router. This makes the routing process fast and efficient

LSR(Label Switching Router):
An MPLS router is called an LSR

LER(Label Edge Router):
It is basically a router which adds MPLS labels to the incoming packets which doesn't have any MPLS label before. These have the real power because they are the exit and entry points for a packet

LDP(Label Distribution Protocol):
It is basically a protocol used by LSRs and LERs for communication

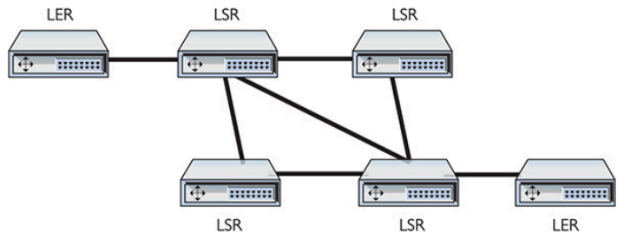


Figure 13-5 Sample MPLS network

SD-WAN(Software-Defined Wide Area Networking):
It is a private networking technology which enables traffic over the Internet. It relies of virtualization technologies. It also uses features of MPLS

Metro Ethernet:
It is a way of creating a secure, private network connection with a city using fiber-optic or ethernet technology. It is also known as **Metro-Optical or Metropolitan Arean Network(MAN)**

Last-Mile Technologies:
These refer to the connection from a telecommunications company central office to the premises

DSL(Digital Subscriber Line):
Internet connection over telephone line. It is the only one using PPP protocols

ISDN(Integrated Services Digital Network)
PSTN(Public Switched Telephone Network): Telephone lines

SDSL and ADSL(Asymmetric and Symmetric):
Symmetric provides equal upload and download. Asymmetric doesn't provide equal uploading and downloading speeds

DSL Features:
Same internet connection line can be used for telephone communications. There are smart NIC used at the user's end and for the office part it is **DSLAM(DSL Access Multiplexer)**

Installing DSL:
We can set-up a DSL connection over the existing telephone cable. Though the telephone will not be working anymore. To enable both the internet and the telephone communication, we have to further add a **POTS Filter**, which stands for **Plain Old Telephone Line**. We connect the DSL Modem to gateway and to the computer. However, for the telephone, POTS Filter to the gateway and the telephone

Broadband Cable:
Coaxial Cable > Cable Modem > PC. Similar to a DSLAM in DSL, offices here have **Headend**. Protocol used is **DOCSIS(Data Over Cable Service Interface Specification)**

Satellite:
One-way and Two-way. Ex: **Starlink**

Fiber:
Companies providing these are **AT&T** and **Verizon**

PON(Passive Optical Network):
Installing a fiber in the neighborhood switch and then individual fiber runs to each final destination

Cellular WAN:

GSM(2G):
GSM(Global System for Mobile Communication) relied on **TDMA(Time Division Multiple Access)** which enabled multiple users to share the same channel more or less at the same time. It also introduced SIM Card. The further advanced version of GSM was **EDGE(Enhanced Data Rates for GSM)**

CDMA(2G):
Code-Division Multiple Access also relied on TDMA but instead it had multiple channels. It relied on the embedded connection, rather than using SIM

HSPA+(3G):
ITU in 2000 requested for covering shortcomings in the telecommunications industry by drafting an IMT-2000 standard. These were later fulfilled by **HSPA(Evolved High-Speed Packet Access)**

LTE(4G):
Long Term Evolution technology started in something 2010. We can run LTE radios on any device. If we want to access any LTE, we can just plug-and-play LTE NIC

5G:
Just advanced version of the above generations

Remote Access:
There are two ways to connect to a remote machine, Remote Machine and VPN

Remote Terminal:
We can access any remote server using **Terminal Emulation** programs. **Citrix** runs a TE program called **Citrix Virtual Apps and Desktop**

Remote Terminal programs require both a server and a client to run. For this, Citrix made a standard called **Independent Computing Architecture(ICA)**. A similar version created by Microsoft is called RDP and the program was **RDC(Remote Desktop Connection)**. The server version of Windows runs **RDG(Remote Desktop Gateway)**

VNC(Virtual Network Computing) and SSH allows **in-band management**, meaning direct control over the resources but it cannot until a connect has been initialized like firing up the initial system. To address this issue, there are also **Lights-Out-Management(LOM)** technologies introduced in many servers

Virtual Private Networks:
The way to create a VPN connection is to create two endpoints at both the ends. They would have a central tunnel which would carry the data. For this to work, both the connections should be on the same network(same IP). If we are running internet, we would have two different IPs in case we are using a VPN client software. One would be the IP provided by the DHCP. The another would be the one created by the client software for VPN and in this way the VPN Tunnel is created. There are several ways to implement this:

PPTP VPNs(Point to Point Tunneling Protocol):
Microsoft uses PPTP at both the end of the VPN Connection and makes it work. The server endpoint is a program called **Routing and Remote Access Service(RRAS)**, which runs in Windows Server. On the client side, we can simply add a VPN connection in settings. This kind of connection is called **Host-To-Site VPN Connection**

Before, setting up a VPN in windows would create a new virtual NIC, which would get the IP from the private DHCP

L2TP VPNs(Layer 2 Tunneling Protocol):
It is made from the **PPTP and L2F(Layer 2 Forwarding)** protocols. The server endpoint here is called **VPN Concentrator** or **VPN Headend**.

Host-to-Site or Client-to-Site or Host-to-Gateway:
Connecting host to the server

Host-to-Host:
Connecting hosts

Site-to-Site:
Connecting two LANs or say two headend to act as one

Split Tunnel:
Even though the client is connected to the VPN, some of the traffic will still be connecting to the Internet Connection

Full Tunnel:
All the traffic goes through the LAN or say remote connection

Protocol used for security in L2TP is **IPsec**. Together, it is termed as **L2TP/IPsec**

SSL/TLS VPNs:
This kind of VPN allows us to get rid of any client software for running the VPN and instead we can run it directly through the browser. The traffic will be secured using SSL/TLS. The two kinds of SSL VPNs are:

SSL Portal VPN:
Client accesses the VPN and the page is made secure

SSL Tunnel VPN:
The client runs some kind of controlling software and gains further access to the VPN. Rather than accessing the sites/links, the user has a broader access to the network

DTLS VPNs(Datagram TLS):
Using Datagram over TCP to optimize delay-sensitive applications like VoIP. Ex is **Cisco AnyConnect DTLS VPN**

DMVPN(Dynamic Multipoint VPN):
This enables direct VPN connections between locations thus, no need to reroute traffic between the central VPN Concentrator. Cisco's DMVPN runs on IPsec

Alternative VPNs:
OpenVPN and SSH. These mostly rely on IPsec. Another examples are **Cisco IOS Easy VPN**. Cisco also developed **Generic Routing Encapsulation(GRE)** Protocol. Multipoint GRE for enabling DMVPN is **mGRE**

WAN Troubleshooting:

Loss of Internet Connectivity:
Ping, ipconfig, netstat, nslookup. Items needed for a connection are: IP, Subnet, Default Gateway and DNS

Interface Errors:
Errors while in a private connections

Local Ethernet Interface/LAN Interfaces:
Make sure cables are connected

Modem Interface:
Make sure Optical Network Terminal(ONT) or CPE or any form of modem is upright and working. Also, get to know about the lights

DNS Issues:
We get the DNS from the ISPs, it can fail and thus we get an error. We would better get a public DNS like the one from the **Google, Quad9**

Interference:
Could be caused by EMI on the client side between the LAN and the Demarc or any other kind of interference

14) Wireless Networking

Saturday, November 23, 2024 12:47 PM

Wi-fi Standards

802.11:
This standard was developed in 1997 and several features were defined under this like network cards, configuration software etc.

Hardware:
The wireless networking NICs perform the same work as wired devices, the only difference is devices transmitting and receiving radio waves

To connect a wireless network to a wired network, a **Wireless Access Point(WAP)** is required

Software:
There are two kinds of software involved in wireless networking. One which acts as a **driver** and talks to the wireless NIC and the another which looks after the **configuration** of the wireless network, like setting up the state of the device, managing connectivity etc.

Wireless Network Modes:

Ad Hoc Mode(Peer-to-Peer):
Decentralized, only one to one connection forming an **Independent Basic Service Set(IBSS)**

Infrastructure Mode:
A centralized network, which can also be termed as **WLAN(Wireless LAN)**. This forms a **Basic Service Set(BSS)** if we add more access point to these, it is termed as **Extended Service Set(ESS)**

BSSID & SSID:
The MAC address of an infrastructure network is called **BSSID**. However, in case of an Ad-Hoc mode, the MAC address is randomly generated.
SSID(Service Set ID) is an another level of naming which is a 32-bit string MAC Address for either BSS or IBSS

When in an ESSID, clients connect to WAPs with the strongest signal and as they move through, the connection happens seamlessly and this is called **Roaming**

Transmission Frequency:
To get rid of Interference from other devices in the network, wireless frequencies operate in the same wireless band, which was either **2.4GHz or 5GHz** for **802.11** standard

NOTE: Wireless Network are **Half-Duplex**, they cannot listen and respond at the same time

Transmission Methods:
There were three different spread-spectrum transmission methods which were defined in the 802.11 standard:

Direct-Sequence Spread-Spectrum(DSSS):
Sending out different frequencies at the same time

Frequency-Hopping Spread-Spectrum(FHSS):
One frequency at a time

Orthogonal Frequency-Division Multiplexing(OFDM):
Same like FHSS, but uses more bandwidth

Channel:
Every Wi-Fi network communicates on a channel and these channels may vary according to the frequencies, bandwidths, environment etc.

CSMA/CA:
For wired, we have CSMA/CD but here, CA stands for **Collision Avoidance**

In a wired network, when the device is sending a frame, it checks if the wire is clear to send the data. Typically, the wait is around the length of the frame plus a predefined silence period called **Interframe Gap(IFG)**. Also, if a collision happens somehow, each sending nodes generates a timeout for itself in which it doesn't try to send any more data on the network. This is called **Backoff Period**.

Now, for wireless networks, C/CD doesn't work because wireless networks are half-duplex so they cannot listen and send at the same time. For these networks, there is basically a DCF Standard

DCF(Distributed Coordination Function):
It defines if the network is found busy, **there is a backoff period on top of the normal IFG wait period**. Also, it requires the receiving node to send an **ACK flag** for every frame they are receiving. This ACK packet also consists of a value which tells the other users to wait a certain period before trying to access the media. The waiting period generally depends on the length of the frame and data rate

Wireless Networks sends out many packets which do nothing more than just advertising their existence and maintaining connections. For real, the number of useful bits per second is called the **Goodput** of wireless network

802.11b:
Widely adopted, but downside was its frequency, which was only 2.4GHz, creating interference

802.11a:
It came after 802.11b, the main change was its frequency range, running in a 5GHz frequency, thus less interference from other devices

802.11g:
It ran on 2.4GHz, but it had a better speed and was backward compatible with 802.11b. It could run in two modes, one is **native mode**, meaning running the main 802.11g standard and the another one is **mixed mode**, making it backward compatible with 802.11b

802.11n(Wifi-4):
It was named as Wi-Fi 4 and brought significant changes to the Wi-Fi. They would be using antennas to implement channel bonding, combining two different frequencies to achieve excellent speeds etc.

Though these networks were backward compatible with .g and .b but the problem was that they had to overlap the frames in the same packets they were using, this would cause some kind of slowdown in the network. To address this, WAPs would transmit in three different modes, **legacy, mixed and greenfield**.

Legacy:
Running .b connections

Mixed:
Running .a and .g with high-throughput. It would use names like **802.11a-ht & 802.11g-ht**, meaning for high-throughput

Greenfield:
.n only

802.11ac(Wifi-5):
Same like .n with increased channels and streams for higher speed

802.11ax(Wifi-6 or Wifi6E):
For high density areas like stadiums and conference halls. Wi-fi 6 runs at 2.4GHz and 5GHz whereas Wi-Fi 6Et runs at 6GHz.

WPS:

As soon as 802.11 got popular, non-PC devices were using it but it was hard to configure the wi-fi network in those devices. For an easy setup, a newer standard was introduced **WPS(Wi-Fi Protected Setup)**, which would work in two modes. One is the **push button** and the another one is using a **PIN** for the connection

Wi-fi Security:

Wired Equivalent Privacy(WEP):
Provides very low security with only 64-bit and 128-bit encryption

Wi-fi Protected Access(WPA):
A full implementation of WEP was called 802.11i but before that several intermediate fixes were there in the market. WPA was the one and it would be running on the EAP Authentication

Extensible Authentication Protocol(EAP):
A single standard to allow devices to authenticate using the PPP protocol. It would better be regarded as a wrapper for PPP rather than standard. There were several versions of this:

EAP-PSK(Pre-Shared Key):
A secret code lying on both the connected devices and encrypted using the powerful AES encryption

EAP-TLS(Transport Layer Security):
Works on a requiring certificates on both the server and the client side

EAP-TTLS(Tunneled TLS):
Using only a server side certificate

EAP-MS-CHAPv2 or PEAP(Protected EAP):
Password version(MS-CHAPv2) with the addition of EAP-TLS

802.1x:
In WPA, we had everything wrapped inside the PPP but for .1x, everything was wrapped inside an Ethernet Frame

I was a complete authentication standard designed to force devices to go through a full AAA process to get anywhere on the wireless network. Before this, the hackers could get access to system's another port where they would be granted access to the network but it wasn't happening anymore in 802.1x standard. For WPA-Enterprise Networks, authentication happens through the RADIUS

WPA2:
It implemented the full IEEE 802.11i standard

WPA3:
Enhanced some of the security features of WPA2 and also added SAE(Simultaneous Authentication of Equals). By 2018, Wi-Fi alliance had started certifying devices that use WPA3

Additional Security Measures:

Disabling SSID Broadcast:
Hiding the SSID, but eventually wireless sniffing tools will almost immediately discover it. Downside is even legitimate users won't be able to access wi-fi easily

MAC Filtering:
Only allowing limited users kind of creating an **Access Control List(ACL)**. There could also be a blacklist for blocking certain MAC Addresses

Isolation:
This would block the client from everything else, like accessing the WLAN, and gives only the access to the Internet

Geofencing:
Giving access based on the several things like location, Bluetooth, cellular network etc. of the device

Enterprise Wireless:
Firing up a simple SOHO network is quite easy but getting into an Enterprise Wireless takes along several things

Robust Device Construction:
Better material, antennas, etc.

Enterprise Wireless Administration:
Wireless network is entirely managed by Wireless switches, which can also be referred to as **Thin Client**. If we are manually configuring it using cables then it would be referred to as **Thick Client**. As there were two modes for connection, there would be an issue in configuring these devices. Today, most of the manufacturers use **Lightweight Access Point Protocol(LWAPP)**, which ensures interoperability of devices

Several organizations also offer this cloud facility of managing the features using web-based browser utility like **Cisco's Meraki**.

VLAN Pooling:
Some of the problems a network would be setting up the same SSID for a larger network. Before, different broadcast domains would be categorized and thus create individual SSIDs for that but nowadays, a pool of VLANs for a single SSID is created and this is called **VLAN Pooling**.

Power over Ethernet:
Using electric cords as ethernet. The original standard for it was **802.3af**. Later, 802.3at, 802.3bt etc. There is term called POE/POE+

Implementing Wi-Fi:

Performing a Site Survey:
Floor plan of the area we wish to survey, site survey tools etc.

What Wireless Is Already There?
Search around for interferences so that networks doesn't overlap. **Wireless Analyzer** can be used for this purpose. This is, however, automatically achieved these days using specific built-in algorithms in WAPs. The map generated by Wireless Analyzers is called a **Heat Map**, which shows a graphical representation of the **RF sources** around us

Interference Sources:
This includes sketching out Refrigerators, Reinforced Walls, Metal Plumbing, Microwave Ovens etc.

Installing the Client:
Installing like wireless NICs, though mobile have built-in wireless clients.

Setting Up an Ad Hoc Network:
There are four things which needs to be configured for setting up an Ad-Hoc network. **SSID, IP Addresses, Channel** and **Sharing**

Modern computers would generally be connecting in Ad-Hoc Networks by using Command-Line only because there is not specific way of achieving this

Setting Up an Infrastructure Network:

Placing the Access Points/Antennas:
Antenna placement if very important, some of them have only one and another more than one. Some of them might be having them hidden inside the chassis. There are basically three different types of antennas in 802.11 Networks: **Omnidirectional, Unidirectional and Patch**.

Omnidirectional:
Antennas which radiate signal outward from the WAP in all the directions. The standard antennas which are used inside these are called **Dipole Antennas**

An antenna basically strengthens the RF output from a WAP. The ratio of increase is called **Gain**, which is measured in **Decibels(dB)**

Unidirectional:

If we do not want to broadcast to the outside world, there are antennas to create a focused network. They come in various forms like Parabolic, Yagi, Dish etc. These are used in cases suppose where we want to connect to a straight hallway faraway

Patch Antennas:
They are like flat, plate-shaped which form an half-sphere beam. Ideal for using in a room

Polarization and Antenna Alignment:
The polarization property of the signal tells the orientation of the radio waves. Like vertically, horizontally and slanted. The more there is an alignment between the transmitter and the receiver, the more strong is signal and the more there is misalignment, weaker it gets

Configuring a Consumer Access Point:

Configuring the SSID and Beacon:
There is a thing called **Beacon**. It is basically a frame which is at sent by the WAP at regular intervals and this makes the networks function. It is usually configured in **milliseconds(MS)**. For a typical connection, it is usually 100ms

Configuring MAC Address Filtering:

Configuring Encryption:

Configuring Channel and Frequency:
We can set it up in regards to the other channels and fqs around

Configuring the Client:
On non-broadcasting networks, we have to manually type the SSID for connection

Extending the Network:

Adding a WAP:
Just add a cable and a new WAP

Wireless Bridges:
These are used to connect two wired networks wirelessly. Comes in two different forms

Point-to-Point:
Used for connecting only two wired network segments

Point-to-Multipoint:
Used to connect more than one bridge at a time and connect multiple network segments

Troubleshooting Wi-Fi:

No Connection:

Channel Problems:
Channels overlapping

Security Type Mismatch:

Signal/Power Levels:
Insufficient wireless coverage. The **RSSI(Received Signal Strength Indication)** is used to measure the quality of a signal. It is usually represented by **Bars** in many connections. Sometimes the strength is caused due to low power as well. Other reasons could be Concrete Walls, Metals, **RF-Blocking Window Films**. When cranking up a Wi-Fi speed, we should be make sure of the surroundings and legal limits too. **ERP(Effective Radiated Power)** is the signal strength coming out of an antenna

Slow Connection:
There could be several reasons behind the WAP being running slow

Overworked WAPs:
If we add too many devices in a single SSID, there gets a **device saturation**. There is also a bandwidth issue when a particular band/channel is being used too much

and this is termed as **Bandwidth Saturation**

Physical Issues:
Items being placed in the straight-line path between a WAP and a wireless client

> **Absorption:**
> This is when solid things like bricks, wood etc. absorb the signal
>
> **Reflection:**
> Metals like pipes, radiators, doors, window frames, etc. Would bounce back the signals
>
> **Refraction:**
> Glass bends the radio waves as they pass through it which would cause a problem called **RF Attenuation**

Either the place affecting the signals could be resolved or there could be multiple antennas installed and a **Multipath** could be created

Captive Portal:
This is a page which is opened up when a public Wi-Fi is being accessed and the page prompts to ask for accepting use policy

Interference:
RFI(Radio Frequency Interference) basically comes from two source, one is non-Wi-fi sources(CFL, LED lighting, Bluetooth, Zigbee, Cordless Phones, Microwaves etc.) and the another is Wi-Fi sources. An **spectrum analyzer** can be used to scan the signals around

Weird Connection:
The event log of an AP could be seen to check what has recently happened with its connection

> **Open Networks:**
> Are unsecure
>
> **Wrong SSID:**
> Selecting an evil twin SSID
>
> **Untested Updates/Incompatibilities:**
> Run updates and test networks first
>
> **Rogue Access Point:**
> Evil Twin
>
> **Client Disassociation Issues:**
> A device is forced with **De-auth Attack** to force a device off

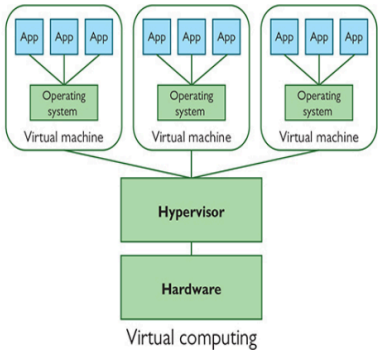
15) Virtualization and Cloud Computing

Friday, November 08, 2024 1:40 AM

Virtualization:
The process of creating Virtual Machine on a computer

> **Hardware Underutilization:**
> This means that a machine is not being used to its capability

Hardware Virtualization comes into play when we want to get rid of underutilization. The program used to create and run a VM is called **Hypervisor**



There are two types of Hypervisors, one which is installed in the place of an Operating System and the another which is installed on top of the OS

> **Aspects of Virtualization:**
>
> **Abstraction:**
> Abstract means to remove or separate. In networking, it means to separate the programs/processes of the machine in such a way that they are easy to manage. The discrete part which we get after abstraction are called **abstracts**. For example, by installing an OS in the VM Ware, we have separated it from the physical hardware, thus not directly affecting the physical system
>
> When virtualizing, the physical devices of a machine are converted into some form of software versions which the hypervisor controls and use them according to the currently running VM. For ex, for a virtual machine, RAM is treated as a physical hardware but the hypervisor treats it as a software and uses it according to the current VM it is running
>
> In Networking, the idea of virtualization can be seen in such a way that instead of having dedicated servers for DNS, Firewall etc., we have a single hypervisor managing these services.
>
> Another different example of abstraction, other than VMs is the idea that IP packets can work with applications regardless of whether the network uses Ethernet or not. This states that the IP Packets are standalone thing or an **abstract**
>
> > **Containerization:**
> > With this, the operating system creates a separate space for applications to run. This space has all the things which are required in order to run that application and the environment(container) is treated in such a manner as if it were the only application running on the system. This is different from virtualization, where the entire OS is given a different environment and here, only the applications are given a container
>
> **Flexibility:**
> Since we convert the physical hardware into some form of software, we have flexibility in using that virtual hardware
>
> **Scaling:**
> At a very large scale, like data centers, virtualization can save millions of dollars for even a very small tweak

Cloud Computing:
It is like a cafeteria of computing and networking resources which is enhanced by layers of powerful services and software

Infrastructure as Code(IaC):
It is a practice where infrastructure management, such as servers, networks, and other resources, is automated and managed through code rather than manual processes. This approach enables the configuration of physical hardware using code

Automation:
It is the way of managing and configuring the tasks automatically using scripts

Some of the popular and powerful tools for managing servers are **Vagrant, Ansible, Terraform** etc.

Orchestration:
It is similar to automation but instead of running a specific task, it includes a streamlines of processes to achieve a larger output. These chain of processes are called **Pipeline** or **Workflow**

CI/CD(Continuous Integration/Continuous Deployment) is a specific kind of orchestration which is used in applications

Virtual Networking:
In virtual networking, software performs the classic network functions. Here, network functions are referred to the physical devices like Switch, Router, Firewall etc. This physical infrastructure is written with some code and turned into some kind of software-versions. Such that, we have like Virtual Switches, Virtual Routers, Virtual Firewalls etc.yut6 But note that we would still have some form of physical medium to connect cables and all. These virtual versions are called **Virtual Network Functions(VNFs)**

VNFCs(VNF Components):
Suppose there is a virtual firewall which compromises of things like Inspection, Logging, Policy Management etc. These components of VNFs are termed as VNFCs

Virtual Networking Inside the VM Host:
When we have a virtual networking, most of the networking needs are covered with in-built features of hypervisors but if it don't cover then we can create a new VM which would be treated as a network function like Router VM, Switch VM, Firewall VM etc.

Distributed Switches:
Since larger networks requires management of large number of switches. In such cases, these are managed centrally and this is called **Distributed Switching**.

Network Function Virtualization:
It is basically a pattern of defining as to how to design the virtual network in order to get achieve a specific set of goals

Network Function Virtualization Infrastructure(NFVI):
It is basically the physical layer in the NFV which compromises of the virtual devices like Switch, Router, Servers etc.

Software Defined Networking:
In classic networking, the router, for ex, were defined with two different parts: a Control Plane and a Data Plane

Control Plane:
This part of the router stands for the structure and management of the traffic. It deals with protocols like OSPF and BGP. For ex, it makes the routing table for the packets to flow

Data Plane:
This part of the router stands for the flow of the data. For ex, it will already have a routing table from the control plane and it will just decide as to where the packets will go. This is also called **Forwarding Plane**

Since virtualization is done to achieve some form of abstraction, so in virtual networking, what is done is that this control plane is abstracted and instead a new **Network Controller** is made which manages these VNFs. And this is achieved with **Software Defined Networking**.

In SDN, since there is a lot of complexity in management, SDN makes it easy by defining some layers-

Management Plane:
Responsible for setting up the network devices

Application Plane:
It does jobs like load balancing, flow optimization etc

NOTE: The difference between SDN and NFV is that the former focuses on virtualizing the control plane whereas for latter, the entire infrastructure is virtualized. In some way, NFV uses SDN too

Managing Cloud Resources:

Scaling:
There are two ways in which a VM is scaled, on is method is **Scalability**, which means taking up the machine and putting it on a bigger system and the another one is **Elasticity**, meaning taking the instances of the VM and putting them into an entirely new VM

Security Implications:
There are many security issues in a cloud resource-

Account Security:
Cloud providers rely on various methods to log, monitor and fire alerts based on account activity

Privacy:
In some cases, the cloud provider might have access to our data due to some of their policies so in such cases, the organization prefers to keep the data encrypted

Multitenancy:
It is ability of the cloud to support multiple customers on the same infrastructure. This is both good and bad. The reason this is good is that everyone can use the shared resource. The reason it is not good is because suppose the cloud has one more server running other than ours but that server, say, is a bad guy which is demanding more energy from that cloud. In such way, the cloud not only affects us in terms of power but there could be a potential risk of security

Intrusion:
There could be a possible risk for the organization if anyone using the cloud resource compromises security

Logging:
The company produces many logs through all kinds of devices which are helpful in debugging or looking into a security incident. So, the company needs to make sure that they are sharing them without violating and policy because they contain very sensitive information

Desktop as a Service(DaaS):
This enables users to access virtual desktops from remote devices, such as PCs and laptops without needing to have powerful hardware locally

The infrastructure of running OS on a remote VM is called **Virtual Desktop Infrastructure(VDI)**

The protocols used by Azure and Amazon for DaaS are **Remote Desktop Protocol(RDP)** and **PC over IP(PCoIP)**

Interconnecting Local and Cloud Resources:
There are a certain number of cases where we want to connect our LAN to the cloud but it is less secure and the connection can't stay permanent. There are usually two methods of achieving it: VPN and Private Direct Connection

Virtual Private Network:
The most convenient way to connect to a network to the public cloud is through a VPN which uses the **IPsec** mechanism

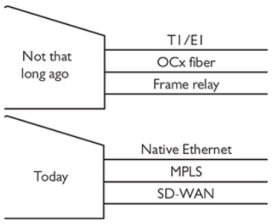
So think of it as if your computer is running some kind of file-server which in turn is connected to a bigger AWS. People use your desktop as DaaS by connecting to your computer using VPN

Private Direct Connection:

16) Data Centers

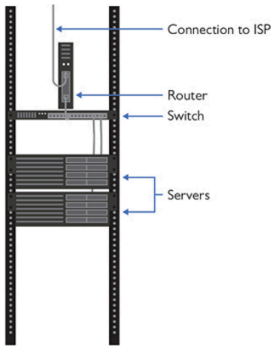
Sunday, November 10, 2024 8:58 PM

Classic Data Center Architecture and Design:
In small organizations, the data center is located at the same facility. But in larger organizations, it is located in a separate building. External connection technologies back in the days are different from modern ones

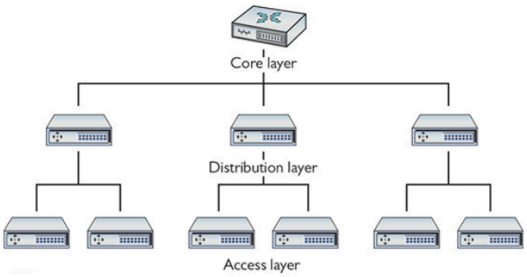


But before connecting to the outer world, the data center in itself requires a well-planned inner connection

Tiers:
A simple architecture of the data center might have a server, a switch, a router and an ISP which kind of looks very simple

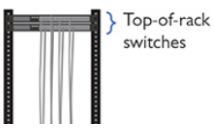


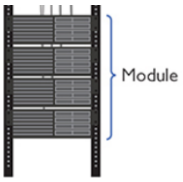
But as the number of servers begin to grow, a structured approach is needed to organize these servers. After decades of different architectures, the most commonly adopted by data centers is **Cisco's Three-Tiered Architecture**. It consists of three layers: **Access Layer, Distribution Layer** and **Core Layer**



Access Layer(Edge Layer):
The first thing to note is that the **servers** in a data center are referred to as **Users**. So basically, the access layer is the first layer which interacts with the users(servers). The **Access Switches(also, Dedicated Switches)** are the switches of the access layer.

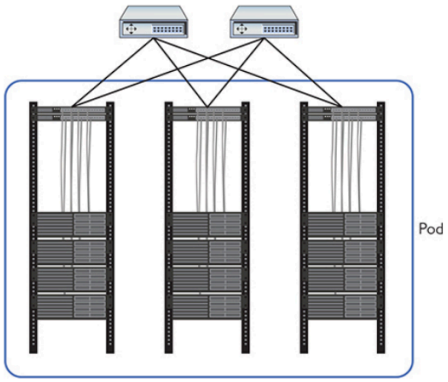
In a racking, the access switches sit at the very top of the racking and the users(servers) sit at the bottom of the racking. A collection of users(servers) connected to the same access switch is called a **Module**





Distribution Layer(Aggregation Layer):
A data center could have a huge number of racking(access switches), ranging from 10-100. There needs to be some kind of way to interconnect these racking. The interconnection of these is done through the **Distribution Layer**.

To connect multiples access switches, it is generally preferred to have more than one distribution switches in case of failure of one. Also, distribution switches are **multilayer switches** which work both as Layer 2 and Layer 3 switches. Suppose there are 4-6 different distributed switches, any group of access switches which are connected to same switches is referred to as **Pod**

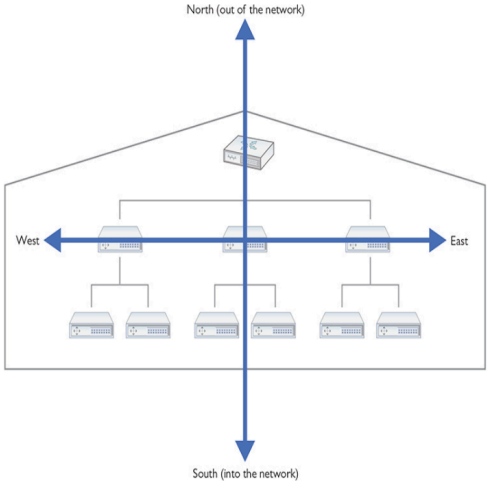


Core Layer:
It is the core switch which connects to the distribution layer and to all the external connections. There could be more than one core switches. These are also multilayer switches

Traffic Flows:
Since the data center is made to flow data in and out, there are established terms to define the movement of the data around the center. These are called **Traffic Flows**

North-South:
It describes the data moving in/out of the data center. **Northbound Traffic** leaves the data center and **Southbound Traffic** enter the data center

East-West:
It describes all the data moving inside the data center. There is no specific direction in this. Examples might include Backups, Detection Systems, Alerts etc.



Data Storage:

One type of storage media is called the **boot drive**, which is attached directly to the motherboard and helps booting up the system. And for the actual data storage, there is a centralized bank of mass storage devices and this is connected to the systems using a network called **Storage Area Network(SAN)**

SAN is different from **NAS**, because NAS is usually a smaller dedicated network appliances with 2,4 or 6 hard drives and is generally preferred for smaller network usage. It will be treated like an attached storage media in the network

In SAN, since there is virtual networking involved, the system would treat the storage as **Virtual Disk**. These type of storage spaced can be mapped to any form of storage devices

There are basically two ways of connecting to a SAN:

Fiber Channel(FC):
It is a type of connection which has its own type of cables, protocols and switches. Some of the more recent versions of it are **Fiber Channel over Ethernet(FCoE)**

Internet Small Computer System Interface(iSCSI):
It is made from TCP/IP it is preferred to reduce processing cost for the data

Where Is the Classic Data Center?

On-Premises:
Creating a small data-center room at the facility itself

Co-Location:
A big data center where people can place their server

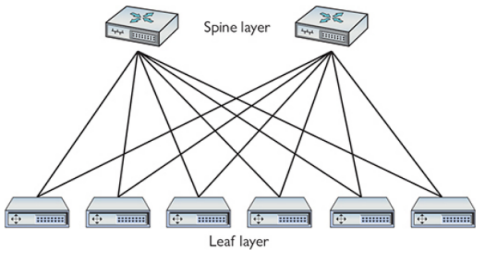
Branch Offices:
One central data server and then connecting that to the small server located in the branch office

The Modern Data Center:

Virtualization:
Physical servers running several virtual servers

Software-Defined Networking:
More flexible and powerful data center architectures

Spine and Leaf:
It is a two-tier network architecture which replaces three-tiered architecture. The two layer which acts here are: **Spine Layer** and **Leaf Layer**. **Spine Switches** would connect to the world, these could be 2 or 3, which further connects to each and every **Leaf Switches**. These are the ones which connect to the users(servers).



The removal of the central layer(distribution layer), would aid in reducing latency, predictable connection, making STP unneeded etc. Also, in modern days traffic flowing from EAST-WEST happens a lot, so this would make it faster

ECPM(Equal-Cost Multipath) protocol in spine and leaf help in load balancing

High Availability in the Data Center:
Since the data in the data center needs to be provided to the right host at the right time, it needs to make sure that there is a **High Availability(HA)** of the system running it

Load Balancing:
It is the act of dividing the load among two systems to enable some process to work. This is can be achieved using **Clustering**(treating two servers to act as one logical device)

There could be two types of availability: **Active Active**(where both the machines would be available the same way) and **Active Passive**(where the backup machine would server only if the primary one fails)

Clustering is an Active Active availability

Redundancy:
Creating backup options if one fails to serve

If there are multiple redundant devices then this is done by treating the devices in such a manner that they will seem to have the same MAC and IP but for their own communication, they would need their own MACs and IPs

There are protocols like **First Hop Redundancy Protocols(FHRPs), Virtual Router Redundancy Protocol(VRRP), Hot Standby Router Protocol(HSRP), Gateway Load Balancing Protocol(GLBP)**, help in treating all the virtual routers as one with a **Virtual IP(VIP)**

VRRP and HSRP are examples of Active Passive availability

When the data centers are connected to an ISP, **Path Diversity** is followed, meaning they connect to the ISPs with different ways in order to keep redundancy

Facilities and Infrastructure Support:
Data Center requires proper power, clean cool air, emergency procedures etc

Power:
Using UPSs and Power Generators

Environment:
HVAC – Average is **68 Fahrenheit and 50% Humid**. Also, **fire suppression systems**

Emergency Procedures:
Building Layout, Fire Plan, Safety/Emergency Exits, Fail Open/Fail Close and Emergency Alert System

Documenting the Data Center:
It includes documenting electrical structure, physical layout, networking standards, installation, climate control etc. The documentation is actually done in three different categories: Network Diagrams, Baseline Configurations and Assessments

Network Diagrams:

Physical Network Diagrams:

Floor Plans:
Locations of rooms, racks, hot and cold aisles, raised floors, ceiling heights, air conditioning units, ductwork etc

IDF(Intermediate Distribution Frame also Tele Room):
A point where all the wires come to a point

NOC(Network Operations Center):
Where all the engineers and techinicians work

Server Farm:
Where racks and servers exist

MDF(Main Distribution Frame):
The main point of connection to the outwise world

Rack Diagrams:
Detailed Rack Diagrams with tons of details. A detailed information like firmware version, date of purchase, upgrade history, service history, techincian assigned, vendor contact, etc

MDF/IDF Documentation:
As these are the frames which actually move sthe data inside and outside the center, they are very well documented with documentation on specific things. An example of MDF can be seen below, it shows us the demarc, patch panels, switches etc.

Logical Network Diagram:
It is kind of a line drawing listing connectivity among many devices

Wiring Diagrams:

Baseline Configurations:
A **network baseline** configuration describes all the pieces, servers, switches, routers, all the software installed on everything. Then comes the **performance baseline**. A baseline configuration can be defined as the foundation for the center, if any upgrade happens, baseline is also upgraded so that the center can be used/optimized to its potential

Assessments:
Every data center should be assessed periodically for overall efficiency and effectiveness. It could be conducted internally or externally

Site Surveys:
Periodic site surveys which records overall assessment

Audit and Assessment Reports:
An audit is done anually to assess compliance with every applicable law and regulation for the industry. The several standards and laws are **ISO 27001, ISO 27002, HIPAA(Health Insurance Portability and Accountability Act), PCIDSS(Payment Card Industry Data Security Standard)**

17) Integrating Network Devices

Sunday, November 24, 2024 1:08 PM

Unified Communication:
Before, PBX-Style phone systems would be used for communication, but this has been replaced by Cisco's **UC(Unified Communication)**, where the communication happens with TCP/IP

VoIP:
To enable both internet and phone VoIP, two different kind of RJs were used, 45 and 11. These would run to different ports and switches and form a **Computer Telephony Integration(CTI)**

All the VoIP were running on **RTP(Real-time Transport Protocol)** and **SIP(Session Initiation Protocol)**. RTP uses UDP from **6970 to 6999** whereas SIP was running on **5060(TCP) and 5061(UDP)** respectively

Since, a separate setup for early VoIP was required and even video conferencing with text messaging was inaccessible. For this reason, Cisco came up with its own **Unified Communications** family of products

Unified Communcation Features:
Real-Time Services(RTS) tell a user's presence for some form of communication. **Video Teleconferencing(VTC)** enables VC with audio

UC Network Components:
There are three core components, Devices, Servers and Gateways

UC Devices:
VoIP Telephone which handles voice, video and more

UC Server:
UC services handler

UC Gateway:
Router with UC Gateway as well as PSTN systems

UC Protocols:
RTP uses UDP, often the IETF-recommended ports 6970 to 6999

SIP uses TCP or UDP ports 5060 and 5061

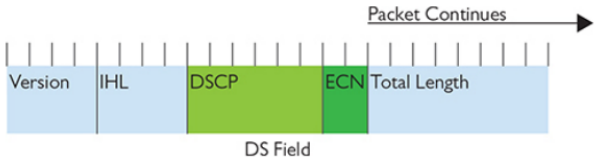
H.323 uses TCP port 1720

MGCP(Media Gateway Control Protocol) uses ports 2427 and 2727

VTC and Medianets:

Medianet is basically a type of network which provides services, like QoS, that are efficient to run VTC. It could either be a huge company or a small setup of high edge routers.

For a QoS, the underlying architecture is referred to as **Differentiated Services(DiffServ)**. In DiffServ, every IP header is sent with two pieces of data, **DSCP(Differentiated Services Code Point)** and **ECN(Explicit Congestion Notification)**. These two are together placed in such a way that they are cumulatively referred to as **DS Field(Diff Serv Field)**, spanning 8 bits of the header.



The first six bits of DS Field,**DSCP** , are further classified into 8 different **Class of Service(CoS)**. A CoS is basically a value which can be assigned to either ports, services or any device involved in QoS. It is like setting up a priority value for something

The last 2 bits of DS Field are defined as ECN. It is a value which is used to tell the sender/receiver information about traffic congestion in a QoS environment. These values are:

00: Not QoS aware
01: QoS aware, no congestion
10: Same 01
11: QoS aware, congestion encountered

UCaaS:
Unified Communication As A Service(UCaaS) covers all the communication needs of an organization like calls, meetings, messaging etc. Ex is Microsoft Teams

ICS(Industrial Control System):

DCS(Distributed Control System):
A DCS is where control is evenly distributed to individual machines instead of having a central control on the machines. To control the DCS, an centralized ICS server is connected. Operators would control controllers using **Human-Machine Interface(HMI)**. These are not general-purpose and hence we won't be able to run anything else on these machines. Though some of the machines doesn't even allow to change interface.

PLC(Programmable Logic Controller):
It is basically a computer that would control the machine according to a set of ordered steps.

SCADA(Supervisory Control and Data Acquistion):
It functions similar to the ICS but the difference is that it is designed for large-scale processes like Power-Grids, Pipelines and Railroads

Remote Terminal Unit(RTU):
These are very similar to DCS but the main difference is that an RTU system have some kind of autonomy in case it loses the connection. Also, RTU is capable of making long-distance communication like telephony, fiber optic or WAN.

Network Segmentation:
Since SCADA system are incredibly crucial for certain needs of everyday living, they should have a high security do get rid of network failure. Also, the need a good amount of performance to work. For this reason, their network is segmented. It is done by using VPNs, creating several separate physical connections, VLANs, and also using different IPs, SSIDs etc.

18) Network Operations

Tuesday, November 26, 2024 2:16 PM

Risk Management:

Hardening and Security Policies:
A Security Policy is going to define how an organization will protect its infrastructure. There are several different kinds of policies

Acceptable Use Policies(AUP):
This defines what and what shouldn't be done on company devices.

Ownership
Network Access
Privacy/Consent to monitoring
Illegal Use

Network Access Policies:
It defines who can access the network, what they can access and how they access. Here, the principle of least privilege works where defining the permission based on role works

Password Policy
Data loss prevention Policy
Remote Access Policy

Mobile Deployment Models:

BYOD(Bring Your Own Device):

COBO(Corporate-Owned Business Only):
Owned by the corporate and issued to employees

COPE(Corporate-Owned Personally Enabled):
Similar to COBO but employees can install some whitelisted applications

CYOD(Choose Your Own Device):
Similar to COPE, but we can choose

Onboarding and Offboarding Policies:
There is a system in an organization which handles mobile devices called **Mobile Device Management(MDM)**. When any onboarding/offboarding happens, some of the devices might have to be registered and some have to be de-registered. This happens both manually and automatically depending upon MDM system

Enternally Imposed Policies:
These policies cover as to what kind of data is allowed to be carried onto a device. Several export control officers also do watch this thing

Adherence to Policies:
It is also important for an organization to adhere to its policies strictly

Change Management:
There is a dedicated team for change management, Change Management Team. There are two kinds of changes, one which is made by the organization and one which is understood by the people working and done upon their request. We are focusing on the latter

Initiating the Change:
A good change request will include the following

Type of Change:
Configuration Procedures:
What is it going to take, who will help and how long is it going to take

Rollback Process:
What is it going to take to roll-back to previous configuration

Potential Impact:
Impact, time, money, efficiency, perception, how will they be affected

Dealing with the Change Management Team:

Making the Change Happen:

Documenting the Change:
All the changes must be clearly documented

Updating SOP:
Standard Operating Procedures must be updated

Patching and Updates:

What Do We Update:
OS updates are the most common types of update. Since October of 2003, Microsoft has sent out patches that have been in development and are ready for deployment on the second Tuesday of the month. This has become known as **Patch Tuesday**. There are both scheduled patches and update-based patches

How to Patch:

Research:
Before patching, it is critical to search what is happening with the patch which has already been released.

Test:
Test, if possible on another system

Configuration Backups:
Backup is important

Tracking the updates is also good because sometimes we need to roll-back to the previous Patch.

Training:
Employees need to be trained on the IT resources

Security Policies:
Users need to read, understand and sign

Passwords:
Maintain complexity

Physical workplace and system security:
Not leaving written passwords, shredding off documents, reporting suspicious behaviors

Social engineering:
Recognize typical social-engineering and how to counter them

Malware:
Teach users to recognize malware attacks

Common Agreements:
When dealing with third-party vendors, there are basically five types of agreements

Service-Level Agreement(SLA):
It is a common agreement where services, equipment, tech support etc. are defined. For ex: an ISP might be providing services and defining their bandwidth, downtime, equipment they are providing, type of connection, troubleshooting support etc.

Memorandum of Understanding(MOU):
It is an agreement between two parties where the individual parties need to perform their duties mentioned in the MOU. For ex, suppose there is a fire in a hospital so if this generates an MOU, it would request for hospital in its surroundings to accept their patients for the time frame of their MOU

Multi-Source Agreement(MSA):
Companies agreeing on the fact that their hardware will be working with different components. For ex, an NIC manufacturer might claim that their NIC would be supportable with both Cisco and Juniper

Statement of Work(SOW):

It defines the services and products which vendor agrees to provide and the time frame for which they are going to provide

Nondisclosure Agreement(NDA):

Security Preparedness:

Security Risk Assessments:
To protect a company's asset, they have categorized aspects of risk assessments

Threat Assessment:
This is analyzing what's out there that could be a threat actor to an asset. It could be an employee, organization or even a nation state

Vulnerability Assessment:
Looking for vulnerabilities in the network. This could be done by running a vulnerability scanner. Popular vulnerability scanner tool is **NMAP(Network Mapper)**, can run on **Zenmap** GUI. More advanced ones are **Nessus, OpenVAS**

Note that vulnerability scanning is a part of vulnerability management

Penetration Testing:
Assigning a White-Hat to check for the exploits and vulnerabilities. Tools can be **Aircrack-ng** and **Metasploit**(Massive library of attacks)

Posture Assessment:
It covers the overall aspects to which the company is vulnerable including negative events like disasters and death of a personnel

Business Risk Assessments:
This is more focused on operations in the organization. This looks for overall risks faced by an organization

Process Assessment:
This involves assessing all the process in the company from manufacturing to sales. For ex: Looking for a new hire if he/she is vulnerable to the company in any way

Vendor Assessment:
Looking for potential risks from a vendor

Contingency Planning:
Contingency plans cover documentation about limiting the damage and recovering quickly afterwards. There are basically three different categories of these: **Incident Response(Damage), Disaster Recovery(Recoverable Damage) and Business Continuity(Recovering Damage Outside Organization)**

Incident Response:
Incident Response Team looks after it. Organizations have detailed incident response policies and plans

Disaster Recovery:
There is a disaster recovery team which looks after things like what kind of data can be backed up, how often backups should be made, making sure backups are available in case of emergencies

Network Device Backup/Restore:
A network devices have two things to be backed up, **Configuration Data and State Data**. Configuration looks after the settings like Router, Switch, Load Balancer, IDS/IPS etc. State Data includes things like Active Directory

Backup Plan Assessments:
A proper assessment of a backup plan records how much data might be lost and how long would it take to restore it. A **Recovery Point Objective(RPO)** defines how much lost data the organization can tolerate if it must restore from a backup point and this also decides how often the backups should be performed. Real-time backup is also a thing in servers. **Recovery Time Objective(RTO)** defines how long the organization can tolerate without system being restored. There are some of the terms

MTBF	**Mean time between failures:** how long it is going to take for a part to fail after one is failed

MTFF	**Mean time to failure:** how long the device is going to last in case of a failure
MTTR	**Mean time to repair:** The amount of time it takes to fix a system after it fails

Business Continuity:
This is dealt with Business Continuity Plan. There is a concept of backup sites, continuing the business at different sites. There are four different kind of sites

Cold Site:
It has all the infrastructure necessary to run a faulted site

Warm Site:
Similar to the Cold one but it make sure that the systems are functioning with loaded software and servers

Hot Site:
Similar to the Warm one but it also has a backup ready already which could be made ready pretty soon

Cloud Site:
A site available on the cloud with everything into place to run remotely as a backup

Forensics:
At the very basic, if we are the first responder, we can do the following

Secure the Area:
Document the Scene:
Collect Evidence:

Three top certifications are:

Certified Forensic Computer Examiner(CFCE)
Certified Computer Examiner(CCE)
GIAC Certified Forensic Analyst(GCFA)

19) Protecting Your Network

Saturday, November 30, 2024 7:23 PM

Security Concepts:

CIA(Confidentiality, Integrity and Availability):
Every security technique, practice and mechanism that is implemented to protect systems and data ensures at least one goat of the CIA

Confidentiality:
Integrity:
There shouldn't be any unauthorized modification, alteration, creation or deletion of data

Availability:
Ensuring systems and data are available for authorized users whenever needed. An extremely secure system that's not functional is not available in practice

Zero Trust:
Meaning that every resource should be treated as if it's hostile and proper authentication/authorization should be performed

Defense in Depth:
It says that the security posture should be designed with the assumption that every single defense can be beaten and also that every specific thing like physical security, network segmentation, separation of duties, strong passwords, patch management etc. should be considered very important

Separation of Duties:
It is about trying to identify what are the potential corners needed altogether to misuse and system and then separating those areas so that people alone cannot do anything

Network Threats:
It is the action of using vulnerabilities to harm a system. **CVE(Common Vulnerabilities and Exposures)** database holds a list of known vulnerabilities. **Exploit** is an actual procedure for taking advantage of a vulnerability whereas, **Attack** simply means trying to compromise CIA for an organization or its systems

Spoofing:
The process of pretending to be someone or something you are not. Not basically a threat but tool to make threats

MAC Spoofing
IP Spoofing: To make you think a packet come from somewhere
ARP Spoofing: To make you think a message is from a trusted source
E-mail Spoofing
Web Address Spoofing
Username Spoofing

DNS Poisoning: Poisoning a DNS cache to point clients to an evil web server. To prevent this, **DNSSEC(DNS Security Extension)** can be used

Packet/Protocol Abuse:
Using protocols in an improper way

NTP(Network Time Protocol)	This protocol is designed for each NTP server to correct its time by querying its peer servers. If a user puts the **ntpdc** command, it puts him in the interactive mode and later further queries can be made into that mode. One of the queries is **monlist**. This will list all the traffic which is going on between the queried NTP and its peers with a lot of other information A hacker can hit multiple NTP servers with the same command with a spoofed source IP. This will put the source IP into target with tons of requests and there would be a **DOS Attack**

	Further, this system can be compromised by hacker by putting **malformed packets** using **Scapy** tool

Zero-Day Attacks:
There are still a lot of vulnerabilities which are unknown in the market and get traded off in black-market

When a new vulnerability is discovered as an attack and given a very short amount of time to fix, this is termed as Zero-Day attack

Rogue Devices:
Tricking the clients in believing that the devices they are using are legitimate

DHCP Snooping:
It is a way of keeping the DHCP Servers safe from attack. This is usually enabled by Network Admins in a protected environment

DHCP Snooping	This creates a **DHCP Snooping Binding Database** of all the trusted ports and monitors the traffic on all untrusted ports. If someone tries to send untrusted DHCP Messages, the snooper identifies it and informs the client

RA-Guard:
It is similar to DHCP Snooping but well suited for **IPv6** networks. What it does is that it looks after the false **Router Advertisements** from untrusted ports

ARP Cache Poisoning:
This is the act of poisoning either the host's ARP cache or MAC Tables on Switches

ARP Cache Poisoning	In general, ARP enables any device any time to announce their MAC without first creating a request. Since ARP has no security, it enables anybody to create ARP Requests and Responses unstoppably. This way, an hacker can create a rogue ARP Broadcast claiming itself to be the router. Any software which isn't patched well and hears the ARP Request might try to respond to it. Once the system has been poisoned, it could be treated as a **Man-In-The-Middle** attack

Dynamic ARP Inspection(DAI):
This is a technology which makes the use of DHCP Snooping to protect a switch port. The DAI technology would look for the good-known IP and MAC Addresses in the **DHCP Snooping Binding Database**. If the ARP Information is untrusted it would be blocked right away and this is a good practice of **Switch Port Protection**. Another tool used for switch protection is **Flood Guards**

Denial of Service(DOS):
It is a targeted attack on a server with the goal of making that service unable to process anything. This is usually done when a particular service/weakness is unable to exploit. **Physical DOS** is attacking the server in-person

The main way to make a DOS work is by getting help from other users to make more requests. This is called a **DDOS(Distributed Denial Of Service)**. A single computer performing the attack is called **Zombie or Bot** and a group of these is called **Botnet**

Reflection is the method of spoofing target's IP Address as Source IP address and use it to aim at the target

Amplification is the process that comes under reflection and it focuses on sending very small requests to trigger a very big response

RUDY	**R U Dead Yet** attack is where the hacker tries to keep the target engaged for as long as possible until he is not done with his work
Deauth Attack	It is a form of DOS attack where wi-fi networks are targeted by creating a rogue access point. This connects the client to it and data is collected

DHCP Starvation Attack	When a DHCP client runs out of DHCP addresses after distributing all its leases, it is termed as **DHCP Scope Exhaustion**. An hacker intentionally does this to encourage clients to switch to a rogue DHCP server and this is called **DHCP Starvation Attack**
Unintentional Dos	When a DOS attack is unintentional, say the site literally gets super busy this is termed as **Slashdotting** or **Hug of Death**

On-Path Attack:
Also man-in-the-middle attack. This is usually done by ARP Poisoning or **SSID Spoofing**

Session Hijacking:
This is similar to man-in-the-middle attack but instead of listening to the ongoing traffic, the hacker tries to get the authentication information

Password Attacks:
The ways of discovering password

Brute Force:
Trying out password permutations and combinations

Dictionary:
Advanced form of Brute-Forcing

Physical/Local Access:

Insider Threats:
Malicious Employees

Trusted and Untrusted Users:
Sometimes an untrusted user is given some trusted permission which are intended to finish some work and it later becomes a threat to the organization

Malicious Users:
Sometimes users try to gain further access to the data by using packet sniffing

Packet Sniffing	Hackers try to gain access to the system by probing a user's ports as to which one is open which one is closed. The tool used can be **Nmap or Netcat**. Once an open port if found, the user might try to learn details about running services. This is called **Banner Grabbing**. For ex: A user might found an exposed SSH port, he can then connect to this port using SSH. Now, user can learn more about the product using SSH and take advantage of the vulnerabilities
Zombified IOT	In NIC devices, the first 24-bits of a MAC are vendor specific called **Organizationally Unique Identifier(OUI)**. A user in the organization might try to grab all these OUIs using common lookup tools and can perform several DDOS. For IOT devices, these attack can be termed as **Zombified IOT**

VLAN Hopping:
In this type of attack, the user in the VLAN tries to convince the switch by sending command in such a way that it wants itself to be treated as another switch and create a **Trunk Link**(connection between switches)

Administrative Access Control:
The admin accounts in Windows is **Administrator**, **Linux** and **MacOS** is **Root**

Unused Components and Devices:
Organizations make sure the proper use/destroy of unused items and resources

Malware:
It is a program designed to do something that is not good for the system

Crypto-malware/Ransomware:
Locking a user out of a system using cryptographic code and in-return asking for the cryptocurrency

Any form of malware which makes a user pay some amount is called **Ransomware**. The above can be termed as **Crypto-Ransomware**

Virus:
It is a type of malware which can do two things, **Replication and Activation**. Replication is when some executable file runs and the virus is attached to its end. Activation is like wiping out a drive or boot sector etc.

Worm:
A virus which actions in networks. Unlike virus, it doesn't need to get activated by anybody but gets to work as soon as the computer is connected to the network

Macro:
It is type of virus which works inside applications which run some kind of **macro programs**. For ex: A macro could be attached to an excel file and later, running that file can cause a big problem

Logic Bomb:
It is a form of code which is written to execute when certain conditions are met. For ex: A company has planted a logic bomb which would delete all the user files as soon as the user leaves the company

Trojan Horse:
It is a form of malware that pretends to do something else but deep inside it is doing something evil. It could be game or anything

Rootkit:
A rootkit is a type of malware which would make itself hide in the system in such a way that it is undetectable even to the best of anti-malware programs

Adware/Spyware:
Adware are the fake-looking ads on a website that would track websites we use often and based on them, prompt us to use deceptive-looking software/services/website in order to gain access

Spyware is a program installed in the system that would send the user's information over to the person controlling it. It could be keystrokes, contacts, list of software/services we are using etc.

Social Engineering:
Manipulating people to gain information like network login, credit card, company customer data etc. The most classic example if telephone scam

Phishing:

Shoulder Surfing:
Monitoring people while they are using passwords

Physical Intrusion:
Breaking into the server room etc.

Common Vulnerabilities:

Unnecessary Running Services:
Some of the services inside a system are not of any use so they should be disabled. Sometimes, the TCP/UDP ports are left open to listen but they are potentially the way for hackers to attack

Make sure that the ports are **not excessively blocked/filtered** because that would cause several network service issues inside the network

Unpatched/Legacy Systems:
Patching and Firmware Management should be done in order to make systems more secure. For the older systems inside the network, we can either isolate them with heavy firewalls or just completely remove if not used

Unencrypted Channels:
Using proper protocols for protection and not just getting insecure at several areas

Cleartext Credentials:
Make sure everything is well encrypted

RF Emanation:
TEMPSET are a set of technologies which allows to protect walls from **RF Emanation**

Hardening Your Network:
There are three aspects of hardening network security, Physical Security, Network Security and Host Security

Physical Security:

Prevention and Control:
Only giving the access to trusted personnel. **Tailgating** is coming through an open door without letting anybody know. **Piggybacking** is the same but the difference is that some authorized personnel help him in doing this intentionally

Smart Lockers:
Company assigning lockers via networking

Monitoring:
CCTV cameras can be used to watch for the people coming in and out of the building

Network Security:

Controlling User Accounts:
Controlling what users can and cannot do. **Improper Access** means though the user is authorized but he is accessing things in a different way

Edge:
These are the devices which are installed on like security doors, cameras etc. For security purpose and they are centrally managed

Posture Assessment:
Network Access Control(NAC) is a way of verifying that a node meets certain criteria before connecting to the network. However, Cisco also implements **Posture Assessment** as a part of NAC. Using this, it wants to check certain things for the connecting host like type and version of anti-malware, level of QoS, and type/version of operating system etc.

Persistent and Non-Persistent Agents:
Whenever a user is requested to respond to a posture assessment, the user answers this using an **Agent**. It is basically a program or piece of software in a computer which gathers all the information in a computer like configuration, assets, resources and then responds to the assessment accordingly. Now there are two different kind of Agents in a computer

Persistent Agent:
It is a basically an agent which is made when the computer **boots up**. It captures all the information as soon as booting up is finished. Though answers to posture assessment queries are made by Non-Persistent Agents but, when it is not available, node is permitted to respond with Persistent Agent

Non-Persistent Agents:
These types of agents are created for a temporary period of time and are made destroyed as soon as the work is done. **For ex:** a user might be connecting to the secure VPN. In this case, the user will try to search for queries at the other end. The endpoint device will then create an agent and made it available on the user computer. This will only create the answer to queries which are requested and as soon as the connection ends, the agents are made disappear

Network Segmentation:
This could be termed as creating separate parts in a network such that even when someone is trying to fiddle with the network, it could be separated or say make other systems safer. For ex: For a coffeeshop, the private wi-fi is separated from the public wi-fi

When someone in Guest Network is denied to get into the Private Network, he is kind of considered suspicious and got put into a **Quarantine Network**

Device Hardening:
Change default passwords, keep update, disabling unnecessary services, using secure network protocols, using QOS filter, **Control Plane Policy** helps in securing the control plane of the network devices

Host Security:
It is preventing dangerous things that users do like propagating to the rest of the network

Malware Prevention and Recovery:

Malware Prevention:
The symptoms of a malware can be seen early like some kind of wonkiness in the system. If our system doesn't let us Patch new updated, there could be a problem. It can also be seen if some configuration tool is showing Access Denied error

Symptoms of a Compromised System:
The most common is general sluggishness and random crash. Website might be redirecting and outgoing traffic would be spiking.

Top Talkers are systems with very high network output

Dealing with Malware:
Anti-malware programs, user awareness, patch management and remediation

Anti-Malware Programs:
A **Signature** is basically a coding pattern in which a Malware is written. Anti-Malware programs have a lot of existing signatures and they compare the executable files with these signatures and if they match, virus is detected

Also, these programs scan the **boot sector** of a system and compare it with a standard boot sector. If there's a change, it would reflect the viruses

Firewalls:
The most basic job of a firewall is to decide packets based on the rules of firewall whether to block or allow the inbound/outbound traffic

Types of Firewalls:

Software vs. Hardware Firewalls:
A **Hardware** firewall can be treated as the one which is installed in the networking device, it could be either Switch, Router anything. It is sometimes also referred as **SOHO Firewall**

A **Software** firewall is the one which is installed on the host computer. Ex is **Windows Defender Firewall**

Advanced Firewall Techniques and Features:
Stateful Inspection is a feature in firewall which would tell if the packet flowing is part of the current connection or no. Before we had **Stateless Inspection** but now it is upgraded

There is a kind of Firewall called **Application/Context Aware Firewall**. This works at OSI Layer 7 and filters according to the use of application/context. This is sometimes invaluable because services like BitTorrent run on **port-hopping**(changing ports dynamically) and hence the firewalls wouldn't be able to stop them.

There comes a **Next-Generation Firewall(NGFW)** which would work at multiple layers of the OSI Model and filters at individual layers. For ex: It would be filtering packets based on IP on layer 3, port numbers on layer 5 and protocols on layer 7

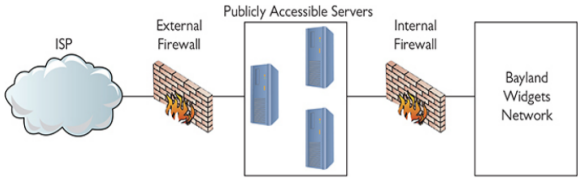
Web Filtering is filtering based on websites. **Content Filtering** is filtering based on signatures and keywords. **IP Filtering** is IP Add filtering. **Port Filtering** is blocking on specific ports

Implementing and Configuring Firewalls:

To protect the internal network from the external, **Cisco's Adaptive Security Appliance(ASA)** device can be used which comes with a hardware-based firewall. Some of the Routers and Switches comes with built-in ports for firewalls, it is similar to connecting other physical devices in the network

Restricting Access via ACLs:
Once we have configured our firewall physically, we need to defined what rules as to what kind of traffic is allowed and what kind of traffic is not allowed. For doing so, we define rules in the **Access Control List**. Certain rules need to be defined like whether it is for the outbound traffic or for the inbound traffic etc.

DMZ and Firewall Placement:
A Demilitarized Zone(DMZ) is basically a zone of network devices which are arranged in a special way for enhancing the security. Suppose our network has a web server which is accessible by the public. Since it is accessible by a lot of people, there could be chances of people getting into our network. In such cases we want to secure the network in a manner that though both the networks will have their individual firewalls but we want our systems to be completely secure or say some kind of enhanced firewall. Here, the picture of DMZ comes into play. It is also known as **Screened Subnet** or **Perimeter Network**. It would look something like this:



Honeypots and Honeynets:
To kill hackers time into accessing a system is what some of the network admins want. They want to increase the roadblocks and make it hard for them to enter into the system or network. Infact, sometimes admins want hackers to check their potential and intentionally challenge them to get into the system in order to check vulnerabilities and get reward

For the roadblock reasons, admins implement some kind of fake systems or say traps to get those hackers waste their time in those systems. These systems too fake, with fake data and everything. Such systems are called **Honeypots** and a collection of these systems or say a network is called a **Honeynet**. This is usually done either with network segmentation or running in virtual machines

Firewall Troubleshooting:
There could be incorrect ACL settings, misconfigured applications etc. We need to make sure if the rules assigned in ACL are working in order, especially for a newly installed Firewall.

Also, when we are talking about **network-based firewall**, we need to make sure that we are also checking is applications are being filtered well from the firewalls because sometimes these applications are treated as Protocols by these firewalls.

In case of an **host-based firewall**, though it is well aware of the applications and filters the inbound/outbound traffic. In some cases, the applications are accidentally listed in the ACL as Deny which we need to check

Sometimes when it is encountered that a certain Service/Port or Address is blocked, Firewalls could be checked

20) Network Monitoring

Sunday, December 01, 2024 5:51 PM

SNMP(Simple Network Management Protocol):
It is a network management protocol for **TCP/IP**

Components of SNMP:
It is basically made up of three main components **Managed Devices, SNMP Manager** and **SNMP Agent**

Managed Devices:
Printers, Workstations, etc

SNMP Agent:
Software which runs on managed devices

SNMP Manager:
Request and processes information from the agent software. Also known as **Network Management System(NMS)**

SNMP uses mainly 8 different kind of PDUs(Protocol Data Units) for querying and responding to the managed devices. Four of them are:

Get:
Sending **GetRequest** or **GetNextRequest** for the query

Response:
Agent responds to the query

Set:
If there needs a change in the query response, NMS sends **SetRequest**

Trap:
A trap is basically a notification/alert sent by the managed device irrespective of any query made

Net-SNMP package in Linux contains a command called **snmpwalk** which is for troubleshooting SNMP related issues. SNMP has three versions, SNMPv1, SNMPv2c and SNMPv3

NOTE that SNMP categorizes data using **MIB(Management Information Base)**, depending upon the type/format of data being queried

SNMP protocol is **UDP** on port **161 and 162**. With TLS, ports are **10162 and 10161**

Monitoring Tools:

Packet Sniffer:
A program that queries a NIC and stores all the captured packets in a file called **Capture File**. These programs can run on computers, dedicated hardware or routers etc. A packet sniffer is usually connected to a **mirrored port**

Protocol Analyzers:
It is a program for reading the **Capture File**. It performs **packet/traffic** analysis like IP and MAC of a packet etc.

NOTE: Filtering in Wireshark is a very good paying skill

NetFlow:
It is basically a tool for monitoring, developed by Cisco. It is based on the idea of the type of flow we want to track

- A **flow** is a sequence of packets from one specific place to another. These flow are stored in a **Flow Cache**

Top Talkers are the devices sending the most data and **Top Listeners** are the opposite

Sensors:
For controlling things like temperature, device/chassis etc.

Interface Monitors:
Tracks the bandwidth and utilization of ports in a network. Some of the terms that can be seen in a interface monitor are: Link State, Speed/Duplex, Send/Receive Traffic, CRC Errors, Protocol Packet and Byte Counts, Giants, Runts, Encapsulation Errors, Uptime/Downtime etc.

Performance Monitors:
It basically tracks the performance for some part of the OS like how much the web server is putting, etc. **Syslog** is a tool in Linux and **perfmon** is a tool in Windows

Logs:
These are basically the system log file to track performance

Baselines:
It is basically a baseline for as to how the optimal network should perform so that if networks breaks down or boosts up, the baseline could be compared

Log Management:
The log files should be secured and managed well. The protection and management of it is called **Log Management**

Log files are **cyclical**, means that if they grow to a certain size, the older ones are deleted. **Also, there are many laws according to which the log files should be kept for a certain period of time**

Putting It All Together:

Monitoring and Managing:
A centralized location for tech and admins to manage the network in an environment is called **NOC(Network Operations Center)**. Some of the tools used are **Cacti, Grafana, Zabbix, SolarWinds, etc.**

SIEM(Security Information and Event Managment):
It is basically a term used for calling out monitoring and management of network. It is made-up of two different processes, **SEM(Security Event Managment) and SIM(Security Information Management)**.

SEM:
It is the real-time monitoring of security events and saving them in a single viewing point say, a log file. What is also does is that it centralizes the other security monitors and event logs

SIM:
It reviews and analyzes log file things like file size, configuration values, content, credentials, hash values etc. Are seen as to what changes have been made and usually compared to the baseline. This is also known as **File Integrity Monitoring(FIM)**. These are either self-implemented or managed by an admin under contract by **Managed Security Service Provider(MSSP)**