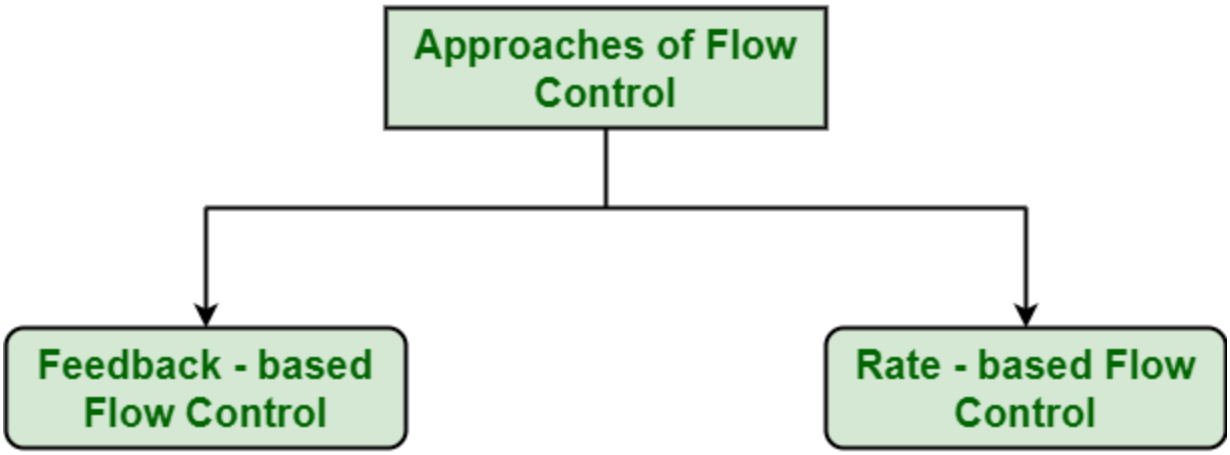
UNIT 2:

Cisco Basics, IOS & Basics Network Management

Flow Control and Describe the Three Basic Method Used in Networking.

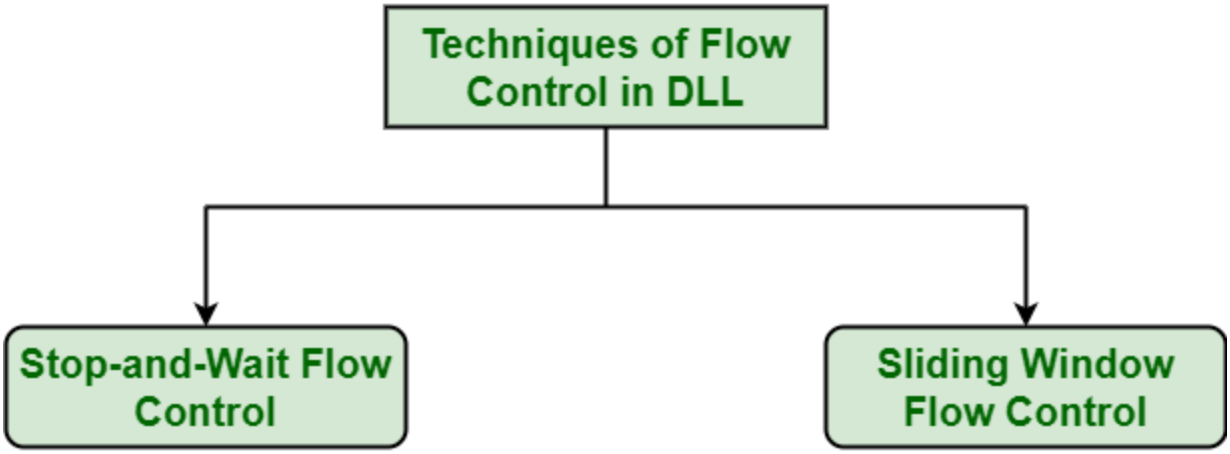
Flow control is design issue at Data Link Layer. It is a technique that generally observes the proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it. This can happen only if receiver has very high load of traffic as compared to sender, or if receiver has power of processing less as compared to sender. Flow control is basically a technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgement from receiver. Flow control is actually set of procedures that explains sender about how much data or frames it can transfer or transmit before data overwhelms receiver. The receiving device also contains only limited amount of speed and memory to store data. This is why receiving device should be able to tell or inform the sender about stopping the transmission or transferring of data on temporary basis before it reaches limit. It also needs buffer, large block of memory for just storing data or frames until they are processed.
flow control can also be understand as a speed matching mechanism for two stations.



Approaches to Flow Control : Flow Control is classified into two categories:

- **Feedback – based Flow Control :** In this control technique, sender simply transmits data or information or frame to receiver, then receiver transmits data back to sender and also allows sender to transmit more amount of data or tell sender about how receiver is processing or doing. This simply means that sender transmits data or frames after it has received acknowledgements from user.
- **Rate – based Flow Control :** In this control technique, usually when sender sends or transfer data at faster speed to receiver and receiver is not being able to receive data at the speed, then mechanism known as built-in mechanism in protocol will just limit or restricts overall rate at which data or information is being transferred or transmitted by sender without any feedback or acknowledgement from receiver.

Techniques of Flow Control in Data Link Layer : There are basically two types of techniques being developed to control the flow of data



1. Stop-and-Wait Flow Control : This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into

various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgement is received, then only sender will send or transfer the next frame. This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay and Ultimately In this method sender sent single frame and receiver take one frame at a time and sent acknowledgement(which is next frame number only) for new frame.

Advantages –

- This method is very easiest and simple and each of the frames is checked and acknowledged well.
- This method is also very accurate.

Disadvantages –

- This method is fairly slow.
- In this, only one packet or frame can be sent at a time.
- It is very inefficient and makes the transmission process very slow.

2. Sliding Window Flow Control : This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed. In this method, sender transmits or sends various frames or packets before receiving any acknowledgement. In this method, both the sender and receiver agree upon total number of data frames after which acknowledgement is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more than one unacknowledged packet “in-flight” at a time. This increases and improves network throughput. and Ultimately In this method sender sent multiple frame but receiver take one by one and after completing one frame acknowledge(which is next frame number only) for new frame.

Advantages –

- It performs much better than stop-and-wait flow control.
- This method increases efficiency.
- Multiples frames can be sent one after another.

Disadvantages –

- The main issue is complexity at the sender and receiver due to the transferring of multiple frames.

- The receiver might receive data frames or packets out the sequence.

Routing Protocols and Configuration; Access List, Operation and Membership in router.

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Once the access-list is built, then it should be applied to inbound or outbound of the interface:

- **Inbound access lists –**
  When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.

- **Outbound access lists –**
  When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

Types of ACL –

There are two main different types of Access-list namely:

1. **Standard Access-list –**
   These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.

2. **Extended Access-list –**
   These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Also, there are two categories of access-list:

1. **Numbered access-list –** These are the access list that cannot be deleted specifically once created i.e if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.

2. **Named access list –** In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

Rules for ACL –

1. The standard Access-list is generally applied close to the destination (but not always).
2. The extended Access-list is generally applied close to the source (but not always).
3. We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
4. We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule then the whole ACL will be removed. If we are using named access lists then we can delete a specific rule.

5. Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
6. As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
7. Standard access lists and extended access lists cannot have the same name.

Advantages of ACL –

- Improve network performance.
- Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of the network.

Congestion Problem :-

What is Network Congestion? Common Causes and How to Fix Them?

Network Congestion occurs when the traffic flowing through a network exceeds its maximum capacity. In most cases, congestion is a temporary issue with the network caused due to a sudden upsurge of traffic, however, sometimes, a network is continually congested, indicating a deeper problem. End-users perceive network congestion as Network Slowdown or a very large delay in processing requests. Network congestion is also a contributing factor in the following underlying issues:

- **High Latency –**
  In a congested network, the time taken by a packet to reach its destination increases significantly, hence a higher latency rate is observed.
- **Connection timeouts –**
  Ideally, the service should wait for the arrival of packets but in several cases, the connection terminates due to timeout.
- **Packet loss –**
  Many packets cannot reach their destination if the network is congested, and will be dropped eventually due to timeout.

Causes of network congestion :

1. **Excessive bandwidth consumption –**
   Certain users or devices on the network may occasionally utilize more bandwidth than the average user or device. This can put a strain on the network and its routing equipment (routers, switches, and cables), causing network congestion.

2. **Poor subnet management –**
   For better resource management, a big network is divided into subnets. However, network congestion could arise if the subnets are not scaled according to usage patterns and resource requirements.

3. **Broadcast Storms –**
   A broadcast storm occurs when there is a sudden upsurge in the number of requests to a network. As a result, a network may be unable to handle all of the requests at the same time.

4. **Multicasting –**
   Multicasting occurs when a network allows multiple computers to communicate with each other at the same time. In multicasting, a collision can occur when two packets are sent at the same time. Such frequent collisions may cause a network to be congested.

5. **Border Gateway Protocol –**
   All traffic is routed by BGP via the shortest possible path. However, while routing a packet, it doesn't consider the amount of traffic present in the route. In such scenarios, there is a possibility all the packets are being routed via the same route which may lead to network congestion.

6. **Too many devices –**
   Every network has a limit on the amount of data it can manage. This capacity

establishes a limit on how much bandwidth and traffic your network can handle before performance degrades. If the network has too many devices linked to it, the network may become burdened with data requests.

7. **Outdated Hardware –**
   When data is transmitted over old switches, routers, servers, and Internet exchanges, bottlenecks can emerge. Data transmission can get hampered or slowed down due to outdated hardware. As a result, network congestion occurs.

8. **Over-subscription –**
   A cost-cutting tactic that can result in the network being compelled to accommodate far more traffic than it was designed to handle (at the same time).

Effects of network congestion :

1. Queueing delay
2. Packet Loss
3. Slow Network
4. Blocking of new connections
5. Low throughput

Test for network congestion :

- Run Command Prompt as administrator.
- Type **tracert google.com** in the CMD window.
- Take note of how many hops it takes to get to the final server.
- For every hop, check out the value of ping.

Congestion at the network layer is related to two issues, throughput and delay.

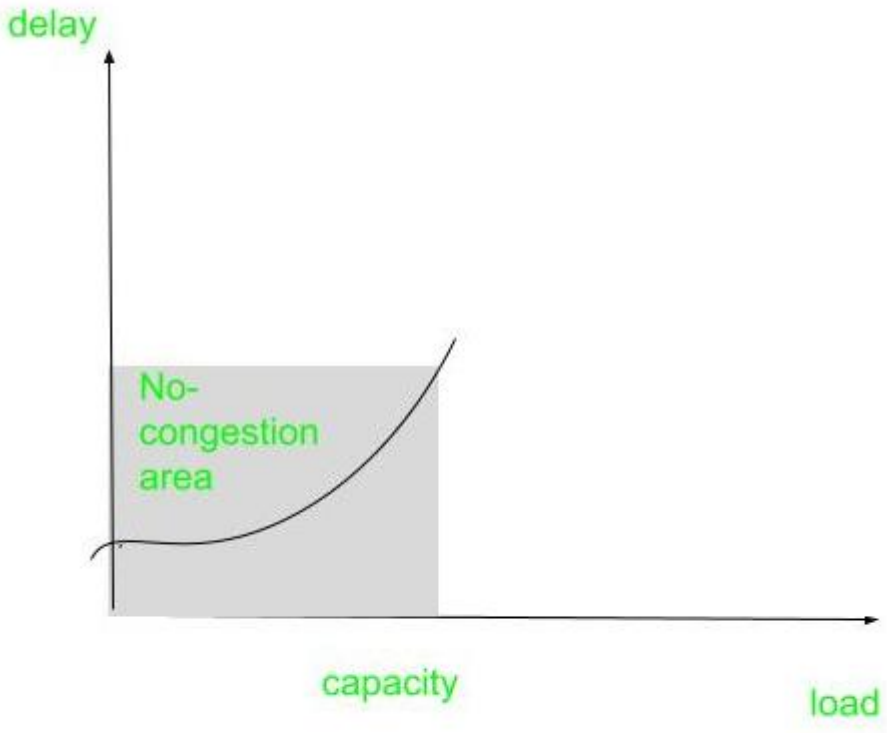
1. Based on delay

When the load is much less than the capacity of the network, the delay is at a minimum .

This minimum delay is composed of propagation delay and processing delay, both of which are negligible.

However, when the load reaches the network capacity ,the delay increases sharply because we now need to add the queuing delay to the total delay.

The delay becomes infinite when the load is greater than the capacity.



delay as a function load

2. Based on Throughout

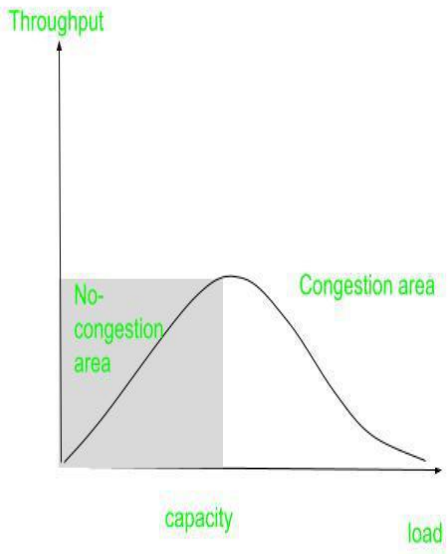
When the load is below the capacity of the network, the throughput increases proportionally with the load.

We expect the throughput to remain constant after the load reaches the capacity, but instead the throughput declines sharply.

The reason is the discarding of packets by the routers.

When the load exceeds the capacity, the queues become full and the routers have to discard some packets.

Discarding packets does not reduce the number of packets in the network because the sources retransmit the packets, using time-out mechanisms, when the packets do not reach the destinations.



throughput as a function of delay

How to fix network congestion?

1. Divide your network into subnets that can be resized to meet traffic.
2. TCP/IP settings should be adjusted to balance packet send/request speeds.
3. Use a CDN (Content Delivery Network) to save time by directing more requests to edge servers.
4. Choke packets are used to reduce the output of sender devices, which helps to avoid network congestion.
5. In case the default route becomes congested, you can employ multi-hop routing so that traffic can be managed.

6. Upgrade your Internet plan to allow for more devices and increased bandwidth. Check to see if your devices are up to date and not outdated (even the cables).

A good practice is to monitor your network for any abnormal changes in the traffic. This helps in identifying the issue in advance and planning out improvements.

Elements:-

Elements of Computer Network

Computer Network
is a system in which multiple nodes are connected to each other to share information and resources. A computer network allows sharing of resources between different nodes connected within it.

Computer Network Elements: The objects basically used in a computer network are known as Computer Network Elements (CNEs). There are basically 4 computer networking elements:

1. Computers
2. Transmission medium (wired or wireless)
3. Protocols
4. Network software

All the elements of a computer network are described below:

1. Computers:
A computer is a digital device that is able to accept data as input, a process that data using predefined algorithms and data structures, and perform tasks as output – that includes the transformation of raw data into information, then knowledge, and finally insight about the data's domain. The output also takes the form of the performance of physical tasks along with data storage, data transformation, and data retrieval. The network is also formed by computers for the purposes of data interchange and leveraging a distributed programming model for parallel processing.

2. Transmission medium:
The means through which we send our data from one place to another is known as the Transmission medium.
Signals are used to represent data by computers and other telecommunication

devices. The signals (i.e., data or information) are transmitted in the form of electromagnetic energy from one device to another. These signals travel through a vacuum, air, or other transmission mediums to move from one point to another (from sender to receiver).
The transmission medium is of two types:

- **(i) Wired or Guided:** For example, Twisted Pair Cable, Coaxial Cable, and Optical Fiber Cable.
- **(i) Wireless or Unguided:** For example, Radiowaves, Microwaves, and Infrared.

3. Protocols:
There are some defined rules and conventions for communication between network devices.
These are called Protocols. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into sent and received messages.
Protocols may be of 3 types:

1. Internet Protocols
2. Wireless Network Protocols
3. Network Routing Protocols

4. Network Software:
Network software is a foundational element for any network. This type of software helps administrators deploy, manage and monitor a network. The traditional networks are made up of specialized hardware, such as routers and switches, that bundle the networking software into the solution.
Such types of software encompasses a broad range of software used for the design, implementation, and operation, and monitoring of computer networks. Traditional networks were hardware-based with software embedded. When software like Defined Networking (SDN) emerged, the software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

Boot Sequence in router:-

Router Boot Sequence

A Router is a networking device that forwards data packets between computer networks. Router Boot sequence involves the following memory elements:

- **Read-Only Memory (ROM):** ROM stores the bootstrap startup program of the router along with the operating system software and other test programs like POST programs (Power On Self Test).
- **Flash Memory:** Flash memory generally called flash holds the IOS images. The flash content is used by the router at the time of reload. Flash is erasable and reprogrammable ROM.
- **Random Access Memory (RAM):** RAM stores information such as routing tables and running configuration files. RAM is volatile hence, its content is lost during router power down and reload.
- **Non-volatile RAM (NVRAM):** NVRAM stores the startup configuration files. It is non-volatile RAM; hence contents are not lost during router power down and reload.

Ports:

Cisco routers have two types of ports: Interfaces and lines. Interfaces connect routers to other devices. Data travels through these ports in the network. Interfaces are identified by their name and number. Some common interfaces are:

- Serial Interface
- Ethernet Interface
- Fast Ethernet Interface

We can configure routers by connecting them with other types of ports called lines. Like interfaces, lines are also identified by line name and number. Some common lines are:

- Console Ports
- Auxiliary Ports
- VTY Ports

Command Line Interface:

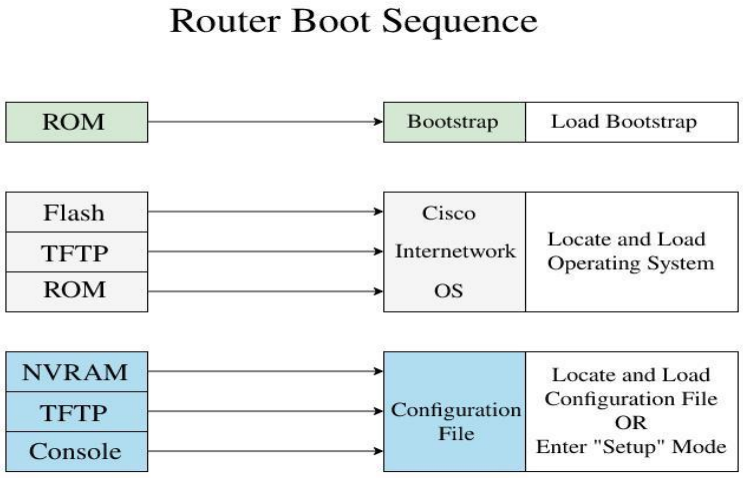
IOS provides a command line interface to interact with the Cisco router. The command line interface is first used to configure and manage Cisco devices. It can be accessed through modem, console, and telnet connection. In CLI, we can type a command and execute it.

Router Boot Sequence:

The series of steps performed by the router during the booting process is called the router boot sequence. The router boot sequence defines the sequence in which the booting process takes place in a router.

Steps of Router Boot Sequence:

1. When the router is turned on it performs the POST (Power On Self Test) program. The POST program tests the present hardware and checks it is operational or not. The POST programs are stored and run from the ROM.
2. The bootstrap program present in the ROM checks the Configuration Register value to find where to load the IOS. The default value of configuration register 0x2102 indicates that the router should load the Cisco IOS Operating System software image from the flash memory and load the startup configuration.
3. The Bootstrap Program looks for and loads the IOS program to the configuration register. This program is also responsible for initializing the hardware and finding the IOS program location and loading the IOS image from the flash memory.
4. If the Bootstrap program does not find the IOS image it will act as ROM Monitor. It supports a command line that is used to perform configuration tasks.
5. The IOS finds the valid configuration file stored in NVRAM. This file is called startup-config.
6. If the Startup configuration(startup-config) is present in NVRAM the router loads the file into RAM and applies the startup-config file. If the file is not present in NVRAM it tries to load a file from TFTP. If no TFTP server responds it enters the Setup mode.
7. When the Startup Configuration is loaded IOS will display CLI mode in user mode.



Router Booting Process Example:

The router goes through the above steps during the booting process.

- The router is powered on.
- POST is performed which checks the hardware components including memory and interfaces.
- The bootstrap program is loaded and executed.
- Bootstrap reads the configuration register value which identifies how the router will boot up.
- Depending on the value of the configuration register, the bootstrap program finds and locates the IOS image.
- If bootstrap fails to load the IOS it will drop the boot sequence to ROMMON (ROM Monitor) mode for troubleshooting.
- If IOS is loaded it finds and loads the configuration.
- If the configuration is not present, the system configuration dialog would be launched.
- If the configuration is loaded, you would be presented in the CLI interface.

Background, Importance, National & International Scenario of Information Security:

Background:

Information security has evolved as a crucial discipline in response to the increasing reliance on digital technologies and the interconnectedness of modern systems. As the world becomes more digitally connected, the risks associated with cyber threats have grown exponentially. The roots of information security can be traced back to the early days of computing when simple measures were taken to safeguard data and systems. However, with the proliferation of the internet and advancements in technology, information security has become a complex and dynamic field.

Importance:

Information security is of paramount importance as it ensures the confidentiality, integrity, and availability of sensitive data and critical systems. It protects individuals, organizations, and nations from a wide range of cyber threats, including unauthorized access, data breaches, identity theft, financial fraud, and cyber espionage. A strong information security posture is crucial for maintaining the trust of customers, safeguarding intellectual property, and ensuring the smooth functioning of government and critical infrastructure.

National & International Scenario:

Governments worldwide have recognized the significance of information security and have established national cybersecurity strategies and agencies to protect their interests. These initiatives focus on enhancing cyber defense capabilities, promoting cybersecurity awareness, and fostering collaboration between the public and private sectors to counter cyber threats effectively.

At the international level, various organizations and initiatives play a pivotal role in addressing global cybersecurity challenges. For instance, the United Nations (UN) has recognized the importance of cybersecurity and advocates for the responsible use of information and communication technologies. Additionally, regional bodies like the European Union Agency for Cybersecurity (ENISA) and the Asia-Pacific Economic Cooperation (APEC) have developed frameworks to facilitate cybersecurity cooperation among member countries.

Furthermore, international conventions and agreements, such as the Budapest Convention on Cybercrime, aim to harmonize cybercrime legislation and foster cooperation in investigating and prosecuting cybercriminals across borders.

However, the information security landscape is continuously evolving, and the sophistication of cyber threats continues to grow. Nation-states engage in cyber-espionage and cyberwarfare, criminal organizations conduct ransomware attacks, and hacktivists target websites for ideological purposes. As technology advances, new challenges arise, such as securing the Internet of Things (IoT), protecting critical infrastructure from cyber-physical attacks, and addressing the implications of artificial intelligence and quantum computing on cybersecurity.

In conclusion, information security is a critical aspect of the digital age. Its importance is recognized at national and international levels, with various efforts being made to enhance cybersecurity measures and cooperation. As technology advances, information security professionals and policymakers face the ongoing challenge of staying ahead of emerging cyber threats to safeguard individuals, organizations, and nations in an increasingly interconnected world.

Upgrade and Restore Cisco IOS image:-

Upgrading and restoring the Cisco IOS image on a Cisco router or switch is essential for keeping the device up-to-date with the latest features, bug fixes, and security patches. The process involves copying the new IOS image to the device and configuring the device to boot from the new image. Below are the steps to upgrade and restore the Cisco IOS image:

1. **Prepare for the Upgrade:**

   - Before proceeding with the upgrade, ensure that you have the correct IOS image for your device model and version. Download the appropriate IOS image from the Cisco website or obtain it from a trusted source.

   - Make a backup of the current configuration using the "copy running-config" command to a TFTP server or USB flash drive.

2. **Copy the New IOS Image:**

   - Transfer the new IOS image file to the device. You can use TFTP, FTP, or SCP to copy the image from a server to the device.

   - For example, to copy via TFTP, use the following command:

     ```
     copy tftp://<TFTP-server-IP>/<IOS-image-file> flash:
     ```

3. **Verify the Integrity of the IOS Image:**

   - After copying the image, verify its integrity using the MD5 checksum provided by Cisco. This helps ensure that the image is not corrupted during the transfer.

4. **Configure the Boot System:**

- Set the new IOS image as the default boot option by configuring the "boot system" command in the device's configuration mode.

- For example:

```
config t
boot system flash:<IOS-image-file>
```

5. **Save Configuration and Reboot:**

- Save the configuration using the "write memory" or "copy running-config startup-config" command to persist the boot system configuration.

- Reboot the device to load the new IOS image as the active operating system.

- You can use the "reload" command to initiate the reboot:

```
reload
```

6. **Verify the Upgrade:**

- After the device reboots, verify that the new IOS image is running using the "show version" command:

```
show version
```

Restoring the Cisco IOS image is a similar process but involves copying the backup IOS image from a TFTP server or USB flash drive back to the device's flash memory. If you encounter issues with the new IOS image, you can use the backup image to restore the device's previous working state.

Remember to exercise caution when upgrading or restoring the IOS image, as a failed upgrade could render the device inoperable. Always follow Cisco's guidelines and best practices for performing IOS upgrades and backups.

Configuration of router:-

Router setup steps

Step 1: Decide where to place the router

The best place for a wireless business router is in an open area of the workplace, as you'll benefit from even coverage. However, sometimes it's not easy to find a space out in the open because you must connect the router to a broadband gateway from your ISP (Internet service provider), which is usually attached to a cable near an outside wall.

Step 2: Connect to the Internet

Attach the router to a cable - or choose a mesh router

To solve the "long-distance" problem when connecting a router, you can use a CAT5e or CAT6 cable to connect the router to the ISP gateway's Ethernet port. Another option is to run Ethernet cables through the walls of your office to the chosen central location for the router.

Yet another option is to install a mesh network with a router. A mesh network allows you to place multiple Wi-Fi transmitters across your home or office, all on one network. Unlike extenders, which can be used with any wireless router, mesh networks require a router with this capability built-in.

No matter which option you choose, you'll use a basic Ethernet cable, plugged into the router's wide-area network (WAN) or Internet port. The Internet port is typically set apart from other ports by a different color.

Check the router's LED lights

Your router's LED lights tell you if you've successfully made an active Internet connection. If you don't see lights confirming such a connection, make sure you've plugged the cable into the correct port.

Test the connection with a device

Confirm that your router has a working connection by plugging a laptop computer into one of the device ports on the back of the router. If all goes well, you should be able to begin a wired connection, just as you did when confirming an active Internet connection.

Step 3: Configure the wireless router gateway

In some cases, ISPs offer customers gateways with built-in routers. In most cases, these combined devices are not built for business environments, nor do they have extra ports, security, and other options that allow you to add services and expand networks as the business grows.

If you have a gateway with an integrated router, you'll have to configure the gateway to disable the router and pass the WAN IP address—the unique Internet protocol address that the Internet provider assigns to your account—and all network traffic through to your new router.

If you don’t take this step, you may run into conflicts that prevent devices from working properly. You may need to contact your ISP for help with this step.

Step 4: Connect gateway to router

First, turn off the gateway. If there is already an Ethernet cable plugged into the gateway's local-area network (LAN) port, unplug the cable and plug it into your router's WAN port. Turn the gateway back on and wait a few minutes for it to boot up. Plug in the router's power supply and turn it on, again waiting a few minutes.

Step 5: Use app or web dashboard

The easiest way to continue with router setup is to use a mobile app if the router maker provided one. If there is no app, or you'd rather use the router's web-based dashboard, connect the router to a computer via an Ethernet cable.

You might find the router's IP address printed on the back of device itself; if not, type 192.168.1.1, a common router address, into the browser search bar.

Step 6: Create a username and password

To configure the router, you'll need to log in, using its default admin name and password. You can usually find this information printed on the router itself, or in an accompanying user manual.

Next, enter the required credentials. Once you're in, you should immediately create a new username and password. The defaults are usually something like "admin" and "password1234," which are obviously not secure—so make sure to change them at the first opportunity.

Step 7: Update the router's firmware

Your router may need an update of the "firmware," or software that operates it. Update it as soon as possible, since the new firmware might fix bugs or offer new security protections.

Some routers may download new firmware automatically, but many do not. You may need to check for updates through the app or the browser interface.

Step 8: Create a Wi-Fi password

Just as most routers come with preassigned admin usernames and passwords, most also come with preset Wi-Fi usernames and passwords. You'll likely be prompted to change the Wi-Fi username and password, but even if you don't see such a prompt, plan to do so quickly.

Step 9: Use auto-configuration tools where possible

If your router is equipped with auto-install features, rely on them to help complete setup. For example, you should be able to use auto-configuration to manage IP addresses with the Dynamic Host Configuration Protocol (DHCP), which automatically assigns IP addresses to devices. You can always change these addresses later.

Step 10: Set up security

Many router manufactures provide security functionality to safeguard network and user privacy. You can login into the web dashboard and enabling added security features such as firewall, web filtering, and access controls to protect yourself from malicious traffic. You can also set up virtual private networks (VPNs) for privacy.