**Assignment – 7**

**Module-3**

1. The Cisco Wireless Network is an infrastructure that permits wireless devices to link with a wired network. You'll be able to use network resources and services from anywhere in the coverage area.
2. The Institute of Electrical and Electronics Engineers (IEEE) develops and publishes numerous standards covering a wide range of topics in the fields of electrical engineering, electronics, telecommunications, and computer science. Here is a list of some notable IEEE standards:

IEEE 802.3: Ethernet

IEEE 802.11: Wi-Fi (Wireless LAN)

IEEE 802.15: Wireless Personal Area Network (WPAN)

IEEE 802.16: WiMAX (Worldwide Interoperability for Microwave Access)

IEEE 802.1Q: VLAN (Virtual LAN) tagging

IEEE 802.1X: Port-based Network Access Control (PNAC)

IEEE 802.3af/IEEE 802.3at: Power over Ethernet (PoE/PoE+)

IEEE 802.3ad: Link Aggregation (EtherChannel)

IEEE 802.1D: Spanning Tree Protocol (STP)

IEEE 802.1Q: VLAN trunking (Inter-VLAN communication)

IEEE 802.1p: Quality of Service (QoS) prioritization

IEEE 802.1ab: Link Layer Discovery Protocol (LLDP)

IEEE 802.11i: Wi-Fi Protected Access 2 (WPA2)

IEEE 802.1Qav: Audio-Video Bridging (AVB)

IEEE 802.1ah: Provider Backbone Bridges (PBB)

IEEE 802.11ac: High-Efficiency Wireless (Wi-Fi 5)

IEEE 802.11ax: High-Efficiency Wireless (Wi-Fi 6)

IEEE 802.3bz: 2.5G/5GBASE-T Ethernet

IEEE 802.1X-2010: Port-based Network Access Control (PNAC) revision

IEEE 802.11ah: Wi-Fi HaLow (Low-Power, Long-Range Wi-Fi)

1. The topology of a wireless network is simply the way network components are arranged. It describes both the physical layout of devices, routers, and gateways, and the paths that data follows between them.

Wireless Security Protocols:

WEP (Wired Equivalent Privacy):

WEP was the first wireless security protocol introduced and provides basic encryption for wireless networks.

However, WEP is vulnerable to several security flaws and is no longer considered secure. It's easily crackable with readily available tools.

WPA (Wi-Fi Protected Access):

WPA was introduced as a replacement for WEP and provides stronger security through improved encryption and authentication mechanisms.

WPA uses TKIP (Temporal Key Integrity Protocol) for encryption and includes mechanisms for key management and integrity checking.

While WPA improved upon WEP's security, it is still vulnerable to certain attacks.

WPA2 (Wi-Fi Protected Access 2):

WPA2 is the successor to WPA and is currently the most widely used wireless security protocol.

WPA2 provides stronger encryption using AES (Advanced Encryption Standard) instead of TKIP, which significantly enhances security.

WPA2 also supports stronger authentication methods such as 802.1X/EAP (Extensible Authentication Protocol) and pre-shared keys (PSKs).

WPA3 (Wi-Fi Protected Access 3):

WPA3 is the latest iteration of the Wi-Fi Protected Access protocol, designed to address vulnerabilities found in WPA2.

WPA3 introduces stronger encryption methods, such as Opportunistic Wireless Encryption (OWE) and Enhanced Open, providing better protection against brute-force attacks and offline dictionary attacks.

WPA3 also enhances security for devices with limited or no display capability, such as IoT devices.

Encryption Methods:

TKIP (Temporal Key Integrity Protocol):

TKIP was introduced with WPA as a replacement for the weak encryption used in WEP.

TKIP dynamically generates encryption keys for each data packet, providing improved security compared to WEP.

However, TKIP has been deprecated in favor of AES due to vulnerabilities discovered over time.

AES (Advanced Encryption Standard):

AES is a symmetric encryption algorithm used in WPA2 and WPA3 for encrypting wireless data.

AES is highly secure and widely adopted as the standard encryption algorithm for protecting sensitive data.

AES uses a block cipher with key lengths of 128, 192, or 256 bits, making it extremely difficult to crack through brute-force attacks.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol):

CCMP is the encryption protocol used with WPA2 and is based on AES.

CCMP provides data confidentiality, integrity, and authentication for wireless communications.

It operates in Counter Mode (CTR) for encryption and Cipher Block Chaining (CBC) mode for authentication.

GCMP (Galois/Counter Mode Protocol):

GCMP is the encryption protocol used with WPA3 and is also based on AES.

GCMP is designed to provide similar security features as CCMP but with improved efficiency and resistance against certain attacks.

It combines the Galois/Counter Mode for encryption and Message Authentication Code (MAC) for authentication.

1. Example DHCP Configuration:

Router(config)# ip dhcp pool LAN

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.1

Router(dhcp-config)# dns-server 8.8.8.8

1. Access Control List (ACL) is a set of rules or conditions that determine whether a network device (such as a router or firewall) allows or denies traffic based on criteria such as source IP address, destination IP address, port numbers, and protocols. ACLs are commonly used to control traffic flow, filter packets, and enhance network security.

Types of ACL:

Standard ACL:

Extended ACL:

Example of Extended ACL:

Router(config)# access-list 101 permit tcp any host 192.168.1.100 eq 80

Router(config)# access-list 101 deny udp any host 192.168.2.200 eq 53

Router(config)# access-list 101 permit ip any any

1. By using the sticky command, the user provides static Mac address security without typing the absolute Mac address. For example, if user provides a maximum limit of 2 then the first 2 Mac addresses learned on that port will be placed in the running configuration.
2. Several WAN protocols have been developed over time, including Packet over SONET/SDH (PoS), Multiprotocol Label Switching (MPLS), ATM, and Frame Relay.
3. frame relay:-

Frame relay is a protocol that defines how frames are routed through a fast-packet network based on the address field in the frame.

ppp:-

A Public-Private Partnership (PPP) is a partnership between the public sector and the private sector for the purpose of delivering a project or a service traditionally provided by the public sector.

1. Network Address Translation (NAT) is a process used in networking to modify network address information in packet headers while in transit through a router or firewall. NAT enables multiple devices on a local network to share a single public IP address for communication with devices on the internet. It helps conserve public IP addresses and provides an additional layer of security by hiding internal IP addresses from external networks.

Example of NAT:

Router: The router connects the internal office network to the internet and has a public IP address assigned to its external interface.

Internal Devices: Multiple devices (e.g., computers, printers) within the office network using private IP addresses (e.g., 192.168.1.x)

1. HDLC stands for High-Level Data Link Control. It is a synchronous data link layer protocol used for communication between network devices, typically in wide area networks (WANs). HDLC is a bit-oriented protocol that provides both connection-oriented and connectionless modes of operation.

Command to Show HDLC Configuration:

show interface serial <interface>

1. Encapsulation refers to the process of enclosing data packets within a specific protocol header as they traverse a network. This header provides necessary information for transmitting the packet across the network and delivering it to the correct destination.

Example of GRE (Generic Routing Encapsulation) Tunnel:

A GRE tunnel is a type of virtual private network (VPN) that encapsulates packets from one network protocol within packets from a different protocol and sends them over an intermediate network. Here's how encapsulation works in a GRE tunnel:

Original Packet:

Suppose we have two remote networks, Network A and Network B, connected via the internet. A router at each network's edge serves as the tunnel endpoints.

Encapsulation:

A packet from Network A destined for Network B is encapsulated by adding a GRE header to it.

The GRE header includes information such as source and destination IP addresses, protocol type, and optional fields.

Transmission:

The encapsulated packet (now containing the original packet and the GRE header) is transmitted over the internet as a standard IP packet.Since the intermediate network (the internet) only understands IP packets, the encapsulated packet is treated as regular IP traffic.

Decapsulation:

When the encapsulated packet reaches the router at Network B's edge, it is decapsulated by removing the GRE header.

The original packet is then forwarded to its destination within Network B.

**Module- 4**

1. List of IP Services Types:

IP services encompass a variety of protocols and technologies designed to support and enhance network functionality and communication. Here are some common types of IP services:

DNS (Domain Name System):

Translates domain names (e.g., www.example.com) into IP addresses (e.g., 192.168.1.1).

DHCP (Dynamic Host Configuration Protocol):

Automatically assigns IP addresses and other network configuration parameters to devices on a network.

NAT (Network Address Translation):

Modifies IP address information in packet headers while in transit, allowing multiple devices on a local network to share a single public IP address.

VPN (Virtual Private Network):

Creates a secure connection over a public network (e.g., the internet) by encrypting traffic between two points.

QoS (Quality of Service):

Manages network traffic to reduce latency and improve bandwidth utilization, ensuring reliable and predictable performance for critical applications.

VoIP (Voice over IP):

Delivers voice communications and multimedia sessions over IP networks.

FTP (File Transfer Protocol):

Transfers files between a client and server on a network.

TFTP (Trivial File Transfer Protocol):

A simplified version of FTP used for transferring smaller files, such as configurations and firmware updates.

HTTP/HTTPS (Hypertext Transfer Protocol/Secure):

HTTP is the foundation of data communication on the World Wide Web, while HTTPS provides encrypted communication for secure data transfer.

SMTP (Simple Mail Transfer Protocol):

Used for sending and receiving email between email servers and clients.

SNMP (Simple Network Management Protocol):

Used for managing devices on IP networks, such as routers, switches, servers, and workstations.

Example of HSRP (Hot Standby Router Protocol):

HSRP is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. HSRP allows two or more routers to work together to present the appearance of a single virtual router to the hosts on a LAN.

1. Backing up and restoring the IOS (Internetwork Operating System) on a Cisco router is an essential task for network administrators to ensure that router configurations and the IOS itself can be recovered in case of a failure or upgrade. Here are the steps and examples for both backing up and restoring the IOS on a Cisco router:

Example of Backup IOS:

Step 1: Prepare for Backup

Ensure you have access to a TFTP server where the backup will be stored. The TFTP server should be reachable from the router.

Step 2: Verify the Current IOS Filename

Use the following command to determine the current IOS filename and location:

Example of Restore IOS:

Step 1: Prepare for Restoration

Ensure the TFTP server has the backup IOS image file and that the router can reach the TFTP server.

Step 2: Copy the IOS Image from TFTP Server to the Router

Use the following command to copy the IOS image from the TFTP server to the router's flash memory:

1. Security Threats, by definition, are any type of malicious activity or attack that could potentially cause harm or damage to an organization, its data or its personnel.

Basic Security of Passwords on a Router

To secure a Cisco router, it is essential to implement strong passwords and follow best practices for password management. Here are some basic security measures and an example of how to apply passwords on a router:

Basic Security Measures:

Enable Password: Secures access to the router's privileged EXEC mode.

Console Password: Secures access to the router's console port.

Auxiliary Password: Secures access to the router's auxiliary port.

VTY (Virtual Terminal) Passwords: Secures remote access to the router via Telnet or SSH.

Service Password Encryption: Encrypts all plain text passwords in the router configuration file.

User Accounts with Privilege Levels: Creates user accounts with specific privilege levels for better access control.

1. Mobile Threat Defense tools are security tools specifically designed to detect and protect mobile devices against cyber threats. They analyze application characteristics and respond to threats in real-time while providing visibility of the risk level of all devices connected to the network.

**Module -5**

1. Automation in network management significantly impacts the efficiency, reliability, and scalability of network operations. Here are some key ways in which automation transforms network management:
2. Increased Efficiency and Productivity.

Task Automation: Routine tasks such as configuration changes, software updates, and network provisioning can be automated, reducing the manual effort required by network administrators. This frees up time for more strategic activities.

Faster Response Times: Automated systems can quickly respond to network issues and changes, reducing downtime and improving overall network performance.

2. Improved Accuracy and Consistency

Error Reduction: Manual configuration and management are prone to human errors. Automation ensures that tasks are performed consistently and accurately every time.

Standardization: Automation enforces standardized procedures and configurations across the network, which is crucial for maintaining a uniform and predictable environment.

3. Enhanced Network Visibility and Monitoring

Real-Time Monitoring: Automated tools can continuously monitor network performance, providing real-time insights and alerts for any anomalies or potential issues.

Data Analytics: Automation systems can analyze vast amounts of network data to identify trends, forecast issues, and optimize network performance proactively.

4. Scalability

Handling Growth: Automation allows network infrastructure to scale efficiently without a proportional increase in manual management efforts. This is essential for organizations experiencing rapid growth or seasonal spikes in demand.

Resource Allocation: Automated systems can dynamically allocate resources based on current network demands, ensuring optimal performance and utilization.

5. Enhanced Security

Consistent Security Policies: Automation ensures that security policies are consistently applied across the network, reducing the risk of vulnerabilities caused by inconsistent configurations.

Rapid Threat Response: Automated security systems can quickly detect and respond to security threats, mitigating potential damage and reducing the time to resolution.

6. Cost Savings

Reduced Operational Costs: By automating routine tasks, organizations can reduce the need for extensive manual labor, leading to significant cost savings.

Reduced Downtime: Faster problem detection and resolution minimize network downtime, which can result in substantial cost savings, especially for businesses where network availability is critical.

7. Support for Advanced Technologies

Integration with AI and ML: Automation often incorporates artificial intelligence (AI) and machine learning (ML) to enhance network management. These technologies can predict and resolve issues before they impact the network.

Support for IoT and Edge Computing: As the number of connected devices grows, automation helps manage the complexity and scale of IoT networks and edge computing environments efficiently.

8. Disaster Recovery and Business Continuity

Automated Backups and Recovery: Automation ensures regular backups and can quickly restore network functions in case of a failure, enhancing business continuity.

Failover Mechanisms: Automated systems can implement failover mechanisms that switch to backup systems in case of a primary system failure, ensuring continuous network availability.

1. The main differences between traditional networks and controller-based networks include: 1. Management: In traditional networks, each network device is managed independently, whereas in controller-based networks, all network devices are managed centrally through the controller.
2. Virtualization is technology that you can use to create virtual representations of servers, storage, networks, and other physical machines. Virtual software mimics the functions of physical hardware to run multiple virtual machines simultaneously on a single physical machine.
3. Automation in network management significantly impacts the efficiency, reliability, and scalability of network operations. Here are some key ways in which automation transforms network management:

1. Increased Efficiency and Productivity

Task Automation: Routine tasks such as configuration changes, software updates, and network provisioning can be automated, reducing the manual effort required by network administrators. This frees up time for more strategic activities.

Faster Response Times: Automated systems can quickly respond to network issues and changes, reducing downtime and improving overall network performance.

2. Improved Accuracy and Consistency

Error Reduction: Manual configuration and management are prone to human errors. Automation ensures that tasks are performed consistently and accurately every time.

Standardization: Automation enforces standardized procedures and configurations across the network, which is crucial for maintaining a uniform and predictable environment.

3. Enhanced Network Visibility and Monitoring

Real-Time Monitoring: Automated tools can continuously monitor network performance, providing real-time insights and alerts for any anomalies or potential issues.

Data Analytics: Automation systems can analyze vast amounts of network data to identify trends, forecast issues, and optimize network performance proactively.

4. Scalability

Handling Growth: Automation allows network infrastructure to scale efficiently without a proportional increase in manual management efforts. This is essential for organizations experiencing rapid growth or seasonal spikes in demand.

Resource Allocation: Automated systems can dynamically allocate resources based on current network demands, ensuring optimal performance and utilization.

5. Enhanced Security

Consistent Security Policies: Automation ensures that security policies are consistently applied across the network, reducing the risk of vulnerabilities caused by inconsistent configurations.

Rapid Threat Response: Automated security systems can quickly detect and respond to security threats, mitigating potential damage and reducing the time to resolution.

6. Cost Savings

Reduced Operational Costs: By automating routine tasks, organizations can reduce the need for extensive manual labor, leading to significant cost savings.

Reduced Downtime: Faster problem detection and resolution minimize network downtime, which can result in substantial cost savings, especially for businesses where network availability is critical.

7. Support for Advanced Technologies

Integration with AI and ML: Automation often incorporates artificial intelligence (AI) and machine learning (ML) to enhance network management. These technologies can predict and resolve issues before they impact the network.

Support for IoT and Edge Computing: As the number of connected devices grows, automation helps manage the complexity and scale of IoT networks and edge computing environments efficiently.

8. Disaster Recovery and Business Continuity

Automated Backups and Recovery: Automation ensures regular backups and can quickly restore network functions in case of a failure, enhancing business continuity.

Failover Mechanisms: Automated systems can implement failover mechanisms that switch to backup systems in case of a primary system failure, ensuring continuous network availability.

1. What is Cisco DNA Center? Cisco DNA Center allows network administrators to receive advanced insights into network performance. No more guesswork as to the root cause of slow downs, or issues - DNA provides analytics to troubleshoot as the network environment changes.
2. Software-Defined Networking (SDN) is a network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed,' using software applications. This helps operators manage the entire network consistently and holistically, regardless of the underlying network technology.