**Assignment-4**

1. **List of IP services Types and Examples of HSRP ?**

IP services are network services that use Internet Protocol (IP) to facilitate communication, security, and management in a network. Here are some common types of IP services:

1. DHCP (Dynamic Host Configuration Protocol)  
   * Assigns dynamic IP addresses to devices in a network.
   * Example: A router automatically assigning IPs to client devices.
2. DNS (Domain Name System)  
   * Translates domain names into IP addresses.
   * Example: Resolving "[www.google.com](http://www.google.com/)" to its IP address.
3. NAT (Network Address Translation)  
   * Maps private IP addresses to a public IP for internet access.
   * Example: A home router translating multiple devices to a single public IP.
4. VPN (Virtual Private Network)  
   * Provides secure communication over a public network.
   * Example: A remote worker connecting securely to an office network.
5. QoS (Quality of Service)  
   * Manages bandwidth and prioritizes network traffic.
   * Example: Prioritizing VoIP traffic over web browsing.
6. VoIP (Voice over IP)  
   * Enables voice communication over IP networks.
   * Example: Skype or Zoom calls.
7. FTP (File Transfer Protocol)  
   * Transfers files between client and server.
   * Example: Uploading files to a web server.
8. IPSec (Internet Protocol Security)  
   * Encrypts and secures IP communications.
   * Example: Securing VPN connections.
9. BGP (Border Gateway Protocol)  
   * Manages routing between large networks (autonomous systems).
   * Example: Internet Service Providers (ISPs) exchanging routing information.
10. HSRP (Hot Standby Router Protocol)

* Provides high availability by allowing a standby router to take over in case of failure.
* Example: Configuring multiple routers for failover in enterprise networks.

### Example of HSRP Configuration

Hot Standby Router Protocol (HSRP) is used to provide redundancy for a default gateway in a network. Below is an example of configuring HSRP on two routers:

#### Router 1 (Active)

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

standby 1 ip 192.168.1.254

standby 1 priority 110

standby 1 preempt

standby 1 authentication mypassword

#### Router 2 (Standby)

interface GigabitEthernet0/0

ip address 192.168.1.2 255.255.255.0

standby 1 ip 192.168.1.254

standby 1 priority 100

standby 1 preempt

standby 1 authentication mypassword

### Explanation:

* standby 1 ip 192.168.1.254 → This is the virtual IP that clients use as the default gateway.
* priority 110 (Router 1) and priority 100 (Router 2) → Higher priority router becomes active.
* standby 1 preempt → Allows a router to take back the active role if it recovers.
* authentication mypassword → Secures HSRP messages between routers.

### HSRP Failover Scenario:

* If Router 1 goes down, Router 2 (Standby) takes over.
* Clients continue using the virtual IP (192.168.1.254) without interruption.
* When Router 1 recovers, it preempts and becomes the Active router again.

1. **Example of Backup and restore Router managing IOS?**

### Backup and Restore Cisco Router IOS

Backing up and restoring the Cisco IOS is crucial for network device management. Here’s how to do it using TFTP (Trivial File Transfer Protocol).

## 1. Backup Cisco Router IOS to TFTP Server

### Step 1: Verify the Current IOS Version

Before backing up, check the IOS version running on the router:

show version

Look for the System Image file location (e.g., flash:c1900-universalk9-mz.SPA.157-3.M5.bin).

### Step 2: Ensure Connectivity to the TFTP Server

Make sure the router can reach the TFTP server by pinging it:

ping 192.168.1.100

*(Assume 192.168.1.100 is the TFTP server's IP address.)*

### Step 3: Backup the IOS to the TFTP Server

Use the following command to copy the IOS to a TFTP server:

copy flash: tftp:

* When prompted, enter the source file name (the IOS filename).
* Enter the TFTP server IP address.
* Specify the destination filename (or press Enter to keep the same name).

#### Example Output:

Router# copy flash:tftp:

Source filename []? c1900-universalk9-mz.SPA.157-3.M5.bin

Address or name of remote host []? 192.168.1.100

Destination filename [c1900-universalk9-mz.SPA.157-3.M5.bin]? (Press Enter)

If the transfer is successful, you should see:

!!

[OK - 33554432 bytes]

The IOS is now backed up on the TFTP server.

## 2. Restore IOS from TFTP to Router

If the router’s IOS is corrupted or missing, you can restore it.

### Step 1: Boot into ROMmon Mode

If the router is stuck in ROMmon mode (due to a corrupted/missing IOS), connect via console and type:

rommon 1 > IP\_ADDRESS=192.168.1.2

rommon 2 > IP\_SUBNET\_MASK=255.255.255.0

rommon 3 > DEFAULT\_GATEWAY=192.168.1.1

rommon 4 > TFTP\_SERVER=192.168.1.100

rommon 5 > TFTP\_FILE=c1900-universalk9-mz.SPA.157-3.M5.bin

rommon 6 > tftpdnld

This downloads the IOS from the TFTP server and loads it into flash.

### Step 2: Copy the IOS from TFTP to Flash (If in Normal Mode)

If the router is still functional but needs an IOS restore, use:

copy tftp: flash:

Then provide:

* TFTP server IP
* Source IOS filename
* Destination filename (press Enter to keep it the same)

#### Example Output:

Router# copy tftp: flash:

Address or name of remote host []? 192.168.1.100

Source filename []? c1900-universalk9-mz.SPA.157-3.M5.bin

Destination filename [c1900-universalk9-mz.SPA.157-3.M5.bin]? (Press Enter)

Once the file transfer completes, verify it:

show flash:

### Step 3: Set the Boot Image and Reload

Set the router to boot from the new IOS:

configure terminal

boot system flash:c1900-universalk9-mz.SPA.157-3.M5.bin

exit

write memory

reload

After rebooting, verify the router is running the correct IOS:

show version

1. **Explain Security Threat.**

A security threat is any potential danger or vulnerability that could harm an organization's or individual's data, systems, or network infrastructure. These threats can lead to data breaches, financial loss, reputational damage, or system failure.

## Types of Security Threats

### 1. Cyber Threats (Digital Threats)

These threats target computer systems, networks, and digital information.

* Malware (Malicious Software)  
  + Includes viruses, worms, trojans, ransomware, and spyware.
  + Example: Ransomware encrypts files and demands a ransom for decryption.
* Phishing Attacks  
  + Cybercriminals use fake emails or websites to trick users into providing sensitive information.
  + Example: A fake email pretending to be from a bank asking for login credentials.
* Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks  
  + Overloads a network or website with excessive traffic, making it unavailable.
  + Example: A botnet floods a company's website, causing downtime.
* Man-in-the-Middle (MITM) Attacks  
  + An attacker intercepts communication between two parties to steal or manipulate data.
  + Example: Capturing login credentials on an unsecured Wi-Fi network.
* Zero-Day Exploits  
  + Attacks that exploit unknown software vulnerabilities before a patch is available.
  + Example: A hacker discovers and exploits a flaw in a new web browser update.

### 2. Insider Threats

Threats from employees, contractors, or partners with access to internal systems.

* Malicious Insider  
  + A disgruntled employee stealing or damaging data.
  + Example: An IT admin selling confidential company data.
* Negligent Insider  
  + Unintended mistakes that cause security risks.
  + Example: An employee clicking on a phishing email.

### 3. Physical Security Threats

Threats that involve direct physical damage to systems.

* Theft of Devices  
  + Unauthorized access due to stolen laptops, USB drives, or smartphones.
  + Example: A stolen company laptop containing sensitive client data.
* Unauthorized Access  
  + Someone physically accessing a restricted area or server room.
  + Example: An outsider gaining entry to a data center.
* Natural Disasters  
  + Earthquakes, floods, or fires destroying data centers.
  + Example: A flood damaging on-premise servers, leading to data loss.

### 4. Social Engineering Attacks

Manipulating people into revealing confidential information.

* Pretexting  
  + Attacker pretends to be someone trustworthy to gather information.
  + Example: A hacker posing as IT support asking for a password.
* Baiting  
  + Luring victims into downloading malware.
  + Example: A free USB drive infected with malware left in a public area.

### 5. Supply Chain Attacks

Hackers target weak links in a company's supply chain to gain access to sensitive systems.

* Example:
  + Attackers compromise a software vendor to infect clients using their products.
  + Real-world Case: The SolarWinds attack in 2020, where hackers injected malware into software updates.

## How to Mitigate Security Threats?

🔹 Use Strong Passwords & Multi-Factor Authentication (MFA)  
 🔹 Keep Software & Systems Updated (Patch vulnerabilities)  
 🔹 Use Firewalls & Antivirus Software  
 🔹 Train Employees on Cybersecurity Awareness  
 🔹 Regular Security Audits & Penetration Testing  
 🔹 Encrypt Sensitive Data & Use Secure Backups  
 🔹 Limit Access Based on User Roles (Zero Trust Security Model)

1. **List of Basic security of Password – Example with apply password in Router.**

### Basic Security Guidelines for Passwords

To ensure security, passwords must be strong, unique, and well-protected. Below are basic security rules for passwords:

### 1. Password Security Best Practices

Use Strong Passwords – At least 8-12 characters with a mix of uppercase, lowercase, numbers, and special characters.  
 Avoid Common Passwords – Do not use "123456," "password," or "admin."  
 Enable Multi-Factor Authentication (MFA) – Adds an extra layer of security.  
 Change Passwords Regularly – Update them every 60-90 days.  
 Do Not Reuse Passwords – Use unique passwords for different accounts.  
 Store Passwords Securely – Use a password manager instead of writing them down.  
 Disable Unused Accounts – Remove old or inactive user accounts.  
 Monitor for Breaches – Use services like Have I Been Pwned to check for leaks.

## Applying Password Security in a Cisco Router

Here’s how to secure a Cisco router with different password protection methods.

### 1. Set a Password for Console Access

Router(config)# line console 0

Router(config-line)# password cisco123

Router(config-line)# login

Router(config-line)# exit

🔹 This requires a password when accessing the router via the console port.

### 2. Set a Password for VTY (Telnet/SSH) Access

Router(config)# line vty 0 4

Router(config-line)# password strongVTYpass

Router(config-line)# login

Router(config-line)# exit

🔹 This secures remote access (Telnet/SSH) by requiring a password.

### 3. Enable a Privileged EXEC Mode Password (Enable Password)

Router(config)# enable password myEnablePass

🔹 Secures privileged EXEC mode but stores the password in plain text (not recommended).

### 4. Secure Privileged EXEC Mode with Encrypted Password (Enable Secret)

Router(config)# enable secret StrongSecretPass!

🔹 More secure than enable password because it is stored as an encrypted hash.

### 5. Encrypt All Plain Text Passwords

Router(config)# service password-encryption

🔹 Encrypts all passwords stored in the running configuration to prevent plain-text visibility.

### 6. Use Local Username and Password Instead of Line Password

Router(config)# username admin privilege 15 secret AdminPass123!

Router(config)# line vty 0 4

Router(config-line)# login local

Router(config-line)# exit

🔹 This requires users to log in with a username and password, instead of just a password.

### 7. Set a Password for Auxiliary (AUX) Access

Router(config)# line aux 0

Router(config-line)# password auxSecurePass!

Router(config-line)# login

Router(config-line)# exit

🔹 Protects access through the AUX (modem) port.

## Verifying and Saving Password Configuration

After setting up passwords, use these commands:

Check Current Configuration (without revealing passwords):  
 show running-config | include password|secret

Save Configuration to Prevent Loss After Reboot:  
 write memory

OR  
 copy running-config startup-config

### Conclusion

To enhance Cisco Router Security, follow these steps:

1. Use enable secret instead of enable password for encryption.
2. Apply strong passwords on all access points (Console, VTY, AUX).
3. Use local usernames/passwords instead of line passwords.
4. Enable service password-encryption to encrypt plain-text passwords.
5. Regularly update passwords and limit access where necessary.
6. **Describe threat defense technologies.**

Threat defense technologies are security solutions designed to protect networks, systems, and data from cyber threats. These technologies detect, prevent, and mitigate security risks such as malware, phishing, data breaches, and unauthorized access.

## 1. Firewall Protection

🔹 Definition: A firewall acts as a security barrier between trusted and untrusted networks, filtering traffic based on predefined rules.  
 🔹 Types:

* Packet Filtering Firewall – Blocks or allows traffic based on IP addresses and ports.
* Stateful Firewall – Tracks active connections and decides which packets are allowed.
* Next-Generation Firewall (NGFW) – Includes deep packet inspection, intrusion prevention, and application control.  
   🔹 Example: Cisco ASA, Fortinet FortiGate, Palo Alto Firewalls.

## 2. Intrusion Detection and Prevention Systems (IDS/IPS)

🔹 IDS (Intrusion Detection System): Monitors network traffic for suspicious activity and alerts administrators.  
 🔹 IPS (Intrusion Prevention System): Actively blocks detected threats.  
 🔹 Example: Snort (Open-source IDS/IPS), Cisco Firepower IPS, Palo Alto Threat Prevention.

## 3. Endpoint Security (Antivirus & EDR)

🔹 Protects individual devices (PCs, servers, mobile) from malware, ransomware, and unauthorized access.  
 🔹 Types:

* Antivirus Software: Scans files for malware (e.g., Windows Defender, McAfee, Norton).
* EDR (Endpoint Detection & Response): Uses AI and behavior analysis to detect advanced threats (e.g., CrowdStrike, SentinelOne).

## 4. Virtual Private Network (VPN)

🔹 Encrypts internet traffic, securing remote access.  
 🔹 Types:

* SSL VPN (Secure Sockets Layer VPN) – Secure remote access via web browsers.
* IPSec VPN – Encrypts network communication between two sites.  
   🔹 Example: Cisco AnyConnect, OpenVPN, Fortinet VPN.

## 5. Network Access Control (NAC)

🔹 Ensures that only authorized and compliant devices can access the network.  
 🔹 Example: Cisco Identity Services Engine (ISE), Aruba ClearPass.

## 6. Zero Trust Security

🔹 Concept: "Never trust, always verify." Every user and device must be authenticated before accessing resources.  
 🔹 Example Technologies:

* Multi-Factor Authentication (MFA)
* Role-Based Access Control (RBAC)
* Microsegmentation (e.g., VMware NSX, Cisco TrustSec)

## 7. Security Information and Event Management (SIEM)

🔹 Centralized system that collects, analyzes, and correlates security logs from multiple sources.  
 🔹 Example: Splunk, IBM QRadar, Microsoft Sentinel.

## 8. Threat Intelligence Platforms

🔹 Provides real-time information about emerging cyber threats to enhance security defenses.  
 🔹 Example: FireEye, Cisco Talos, Palo Alto Unit 42.

## 9. Data Loss Prevention (DLP)

🔹 Prevents unauthorized data sharing or leakage.  
 🔹 Example: Symantec DLP, Microsoft Purview DLP.

## 10. Cloud Security Technologies

🔹 Protects cloud-based applications and data.  
 🔹 Example:

* Cloud Access Security Broker (CASB): Monitors and controls cloud app usage (e.g., McAfee MVISION, Netskope).
* Cloud Security Posture Management (CSPM): Identifies misconfigurations (e.g., Prisma Cloud, Microsoft Defender for Cloud).