INDEX

Experiment Name: RIP Server Configuration

Objective:

The objective of this experiment is to design and configure a network using the RIPv2 dynamic routing protocol to enable communication between four Local Area Networks (LANs) through two routers. The routers will act as default gateways for their respective LANs, and the RIPv2 protocol will dynamically update routing tables to ensure efficient data transmission.

Network Design:

In this experiment, we will set up a network with two routers, each responsible for two LANs. The RIPv2 dynamic routing protocol will be configured to enable communication between all LANs. Each LAN will have devices connected to it, and the routers will act as default gateways for their respective LANs.

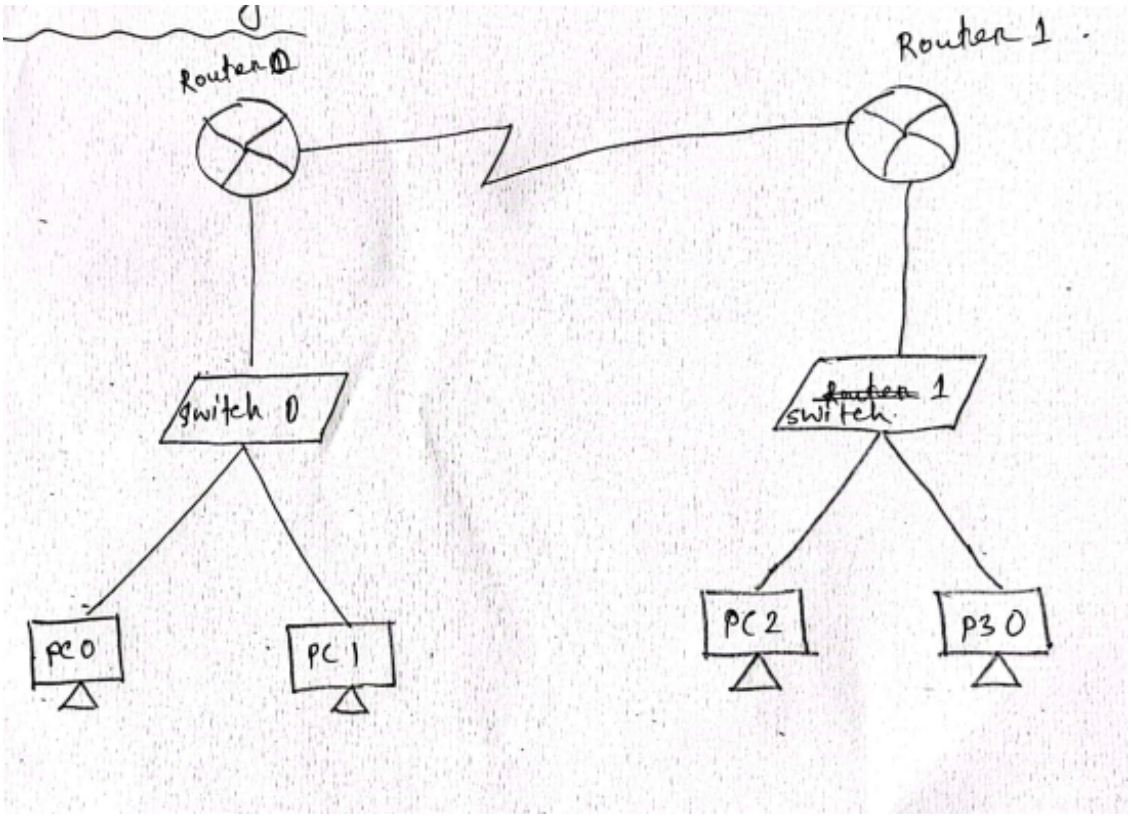


Fig: Network Diagram

IP Configure:

PC 0: 192.168.1.2	Default Getway 192.168.1.4
PC 1: 192.168.1.3	
PC 2: 192.168.2.2	Default Getway 192.168.2.4
PC 3: 192.168.2.3	

Router 0: F-0/0 = 192.168.1.4
F-0/1 = 192.168.1.4

Router 1: F-0/0 = 192.168.3.3
F-0/1 = 192.168.2.4

Procedure:

Step 1: Hardware and Software Setup:

- Set up two routers (R1 and R2) and configure the interfaces connected to each LAN with the specified IP addresses from the given subnets.
- Ensure that the routers are running a routing-enabled operating system, such as Cisco IOS

Step 2: Configure RIPv2 on Both Routers:

- Access the CLI of each router using a terminal emulator.
- Enter privileged EXEC mode by typing enable and providing the enable password.
- Enter global configuration mode by typing configure terminal.

Step 3: Enable Routing and Configure Interfaces:
Configure the interfaces of Router R1 connected to LANs A and C, and Router R2 connected to LANs B and D with IP addresses and subnet masks:

interface <interface_name>
ip address <ip_address> <subnet_mask>
no shutdown
Exit

Step 2: Configure RIPv2 on Both Routers:

Step 4: Configure RIPv2:
Enable RIPv2 routing protocol on both routers:

router rip
version 2
network <ip_address_of_interface>

Step 5: Set Default Gateways on Devices:
Configure devices in each LAN to use the IP address of their respective router as their default gateway.

Step 6: Testing:

- Connect devices to each LAN (A, B, C, D).
- Test connectivity between devices in different LANs and observe how RIPv2 dynamically updates routing tables.

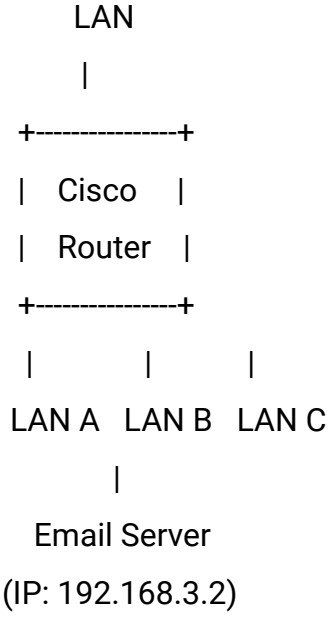
Note: While RIPv2 can be used for educational purposes, keep in mind that more advanced routing protocols like OSPF or EIGRP are recommended for larger, production networks due to their scalability and features. Additionally, ensure proper security measures are in place before conducting experiments.

Experiment Name: Design and Configure SMTP and POP3 Email Protocols using Cisco Router

Objective:

The objective of this experiment is to design and configure a Cisco router to enable the Simple Mail Transfer Protocol (SMTP) and Post Office Protocol version 3 (POP3) for email communication. The experiment aims to facilitate sending (SMTP) and receiving (POP3) of emails within a local network.

Network Design:



IP Configuration:

- Router IP (GigabitEthernet ports):
  - Port 0/0: 192.168.1.1/24
  - Port 0/1: 192.168.2.1/24
  - Port 0/2: 192.168.3.1/24

- Email Server IP: 192.168.3.2

Procedure:

Step 1: Hardware and Software Setup:

1. Set up the Cisco router and connect its GigabitEthernet ports to LANs A, B, and C.
2. Ensure that the router is running Cisco IOS and is accessible via a terminal emulator.

Step 2: IP Configuration:

1. Access the router's CLI using the terminal emulator.
2. Enter privileged EXEC mode: `enable`.
3. Enter global configuration mode: `configure terminal`.
4. Configure the IP addresses and subnet masks for each GigabitEthernet port:

```
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
```

interface GigabitEthernet0/2

ip address 192.168.3.1 255.255.255.0

no shutdown

exit

Step 3: SMTP Configuration:

1. Enable SMTP on the router:

```
ip smtp server
```

Step 4: POP3 Configuration:

1. Enable POP3 on the router:

```
ip pop3 server
```

Step 5: Email Server Configuration:

1. Configure the email server in LAN C with IP address 192.168.3.2.

Step 6: Testing:

1. Configure email clients in LANs A and B to use the email server's IP (192.168.3.2) for both SMTP (sending) and POP3 (receiving).
2. Send emails from LAN A to the email server using SMTP.
3. Receive emails in LAN B from the email server using POP3.

Step 7: Observations:

1. Observe successful sending and receiving of emails within the local network.
2. Monitor router logs for any SMTP and POP3 activity.

Step 8: Analysis:

1. Analyze the email communication process and the roles of SMTP and POP3 in sending and receiving emails.

Step 9: Conclusion:

Summarize the experiment's outcomes, emphasizing the successful configuration of the Cisco router to enable SMTP and POP3 protocols for email communication.

Note:

- This setup is for educational purposes and does not cover email security considerations, such as encryption or authentication.
- In a real-world scenario, professional email servers and security measures should be implemented.

Experiment Name: Designing and configuring a firewall for security in Windows.

Objective:

The objective of this task is to design and configure the Windows Firewall to enhance the security of a Windows-based system by controlling incoming and outgoing network traffic.

Procedure:

Step 1: Access Windows Firewall Settings:

1. Open the Control Panel and navigate to "System and Security."
2. Click on "Windows Defender Firewall."

Step 2: Configure Inbound Rules:

1. Click on "Advanced settings" on the left pane.
2. In the "Windows Defender Firewall with Advanced Security" window, select "Inbound Rules."
3. Right-click on "Inbound Rules" and choose "New Rule."
4. Choose the rule type:
   - "Program" to allow or block specific programs.
   - "Port" to allow or block specific ports.
   - "Predefined" to choose from predefined rules.
   - "Custom" to define a custom rule.

Step 3: Configure Outbound Rules:

1. In the "Windows Defender Firewall with Advanced Security" window, select "Outbound Rules."
2. Follow the same process as in Step 2, but this time, you're configuring rules for outbound traffic.

Step 4: Define Rule Properties:

1. Follow the wizard to define properties such as program/path, action (allow/block), profiles (domain/private/public), and name.
2. Configure protocols and ports if setting up port-based rules.
3. For custom rules, specify criteria based on programs, services, ports, or IP addresses.

Step 5: Testing:

1. Test the rules by attempting network communication that falls under the configured rules.
2. Verify that allowed traffic is functioning as expected, and blocked traffic is indeed blocked.

Step 6: Monitoring and Adjustments:

1. Regularly monitor firewall logs to ensure that the rules are working effectively.
2. Adjust rules as needed based on changes in network requirements or security policies.

Best Practices:

1. Use the principle of least privilege: Only allow necessary traffic.
2. Keep rules up-to-date and remove unnecessary rules.
3. Block all incoming traffic by default and allow only essential services.
4. Regularly update the firewall rules based on new applications and services.
5. Consider enabling logging for rules to monitor traffic patterns and potential security risks.
6. Configure separate rules for different network profiles (domain, private, public).

Note:

- The above steps provide a basic overview of configuring the Windows Firewall. In an enterprise environment, consider more advanced firewall solutions for comprehensive security.
- Always follow security best practices and keep the system up to date with the latest security patches.

Experiment Name: Design and Configure a Network with 4 LANs Connected through PPTP using 2 Cisco Routers

Objective

The objective of this experiment is to design and configure a network with four LANs connected through PPTP (Point-to-Point Tunneling Protocol) using two Cisco routers. The network design involves setting up IP addresses for the routers and PCs, establishing connectivity between LANs, and configuring necessary routing commands.

Network Design:

```
          PC 0                    PC 1
          |                         |
          |                         |
        LAN 1 ---------------------- LAN 2
          |                         |
          |                         |
        Router 1                 Router 2
   FastEthernet0/0          FastEthernet0/0
     192.168.1.1               192.168.2.1
         |                           |
    Serial2/0 (shared)       Serial2/0 (shared)
      10.1.1.1                    10.1.1.2
         |                           |
         |                           |
        LAN 3 ---------------------- LAN 4
          |                         |
          |                         |
         PC 2                    PC 3
```

Equipment Used:

- 2 Cisco routers
- 4 PCs
- Ethernet cables
- Serial cables

Procedure:

1. Setting Up Router Interfaces:

- Connect FastEthernet0/0 of Router 1 to LAN 1 and assign IP address 192.168.1.1/24.
- Connect FastEthernet0/0 of Router 2 to LAN 2 and assign IP address 192.168.2.1/24.
- Configure Serial2/0 of Router 1 and Router 2 with IP addresses 10.1.1.1/30 and 10.1.1.2/30 respectively.

2. Configuring PCs:

- Configure PC 0 with IP address 192.168.1.2 and default gateway 192.168.1.1.
- Configure PC 1 with IP address 192.168.2.2 and default gateway 192.168.2.1.
- Configure PC 2 and PC 3 with IP addresses in their respective LAN ranges.

3. Routing Configuration:

- On Router 1:

```
enable
configure terminal
interface Serial2/0
ip address 10.1.1.1 255.255.255.252
exit
interface FastEthernet0/0
```

```
ip address 192.168.1.1 255.255.255.0
exit
ip route 192.168.2.0 255.255.255.0 10.1.1.2
```

- On Router 2:

```
enable
configure terminal
interface Serial2/0
ip address 10.1.1.2 255.255.255.252
exit
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
exit
ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

4. Testing Connectivity:

- Ping from PC 0 to PC 1 (192.168.2.2) to test inter-LAN connectivity.
- Ping from PC 2 to PC 3 to test connectivity within the same LANs.

Conclusion:

In this experiment, a network with four LANs connected through PPTP using two Cisco routers was successfully designed and configured. The routers' interfaces and routing tables were configured to ensure proper communication between LANs. Inter-LAN and intra-LAN connectivity were tested using ping commands, confirming the functionality of the network setup.

Experiment Name: Analysis of Firewall Features in Providing Network Security

Objective:

The primary objective of this experiment is to comprehensively examine the various features of a firewall in strengthening network security. This analysis will cover critical firewall functionalities, including packet filtering, application inspection, intrusion prevention systems, virtual private networks (VPNs), bandwidth management, sandboxing, data loss prevention (DLP), cloud security, along with discussing the benefits and limitations of using firewalls for network protection.

Introduction:

Firewalls play a crucial role in safeguarding networks from unauthorized access, cyber threats, and data breaches. They act as barriers between a trusted internal network and untrusted external networks, controlling the flow of data and enforcing security policies.

Discussion of Firewall Features:

1. Packet Filtering:

- Packet filtering is the initial layer of defense in a firewall.
- It examines incoming and outgoing data packets based on pre-defined rules.
- Packets are either allowed or blocked based on criteria such as source and destination IP addresses, port numbers, and protocols.

2. Application Inspection:

- Application layer firewalls go beyond packet filtering and understand the context of network traffic.
- They inspect the content of packets to identify and block malicious or unauthorized applications and services.

3. Intrusion Prevention System (IPS):

- IPS monitors network traffic for signs of known attacks or unusual behavior.
- It can detect and block intrusion attempts in real-time, adding an extra layer of security.

4. Virtual Private Network (VPN):

- VPNs provide secure remote access to networks over the Internet.
- Firewalls with VPN capabilities encrypt data transmissions, ensuring confidentiality.

5. Bandwidth Management:

- Firewalls can manage network bandwidth by prioritizing or limiting data traffic.
- This ensures critical applications receive sufficient bandwidth while preventing congestion.

6. Sandboxing:

- Sandboxing creates isolated environments to execute suspicious files or applications.
- This allows the firewall to analyze their behavior without endangering the network.

7. Data Loss Prevention (DLP):

- DLP features monitor data leaving the network to prevent sensitive information leakage.
- It identifies and blocks unauthorized transfers of confidential data.

8. Cloud Security:

- Firewalls extend their protection to cloud environments by controlling access to cloud resources and data.
- Cloud-based firewalls can inspect traffic between the cloud and on-premises systems.

Benefits of Firewall:

- Network Segmentation: Firewalls help partition networks into zones, limiting the impact of breaches.
- Unauthorized Access Prevention: Firewalls block unauthorized users and connections.
- Malware Defense: Firewalls can prevent malware from entering the network.
- Policy Enforcement: They enforce security policies, ensuring compliance.
- Traffic Monitoring: Firewalls monitor traffic for abnormal behavior or patterns.
- Centralized Management: Firewalls offer a central point for managing security settings.

Conclusion:

Firewalls are a cornerstone of network security, offering a range of features to protect against threats and vulnerabilities. From packet filtering to advanced application inspection, intrusion prevention, and beyond, firewalls provide essential defense mechanisms. While offering numerous benefits, they also have limitations, such as not being able to prevent all advanced threats. Organizations must carefully design their firewall strategies and combine them with other security measures for comprehensive network protection.

Experiment Name: Analysis of Security Vulnerabilities in Email Applications

Objective

The main objective of this experiment is to comprehensively analyze the security vulnerabilities commonly found in email applications. This analysis will cover crucial topics related to email security vulnerabilities, including their types, potential risks, and mitigation strategies.

Introduction

Email applications are widely used for communication and information exchange. However, their popularity also makes them prime targets for cyberattacks. Security vulnerabilities in email applications can lead to data breaches, malware infections, phishing attacks, and unauthorized access to sensitive information.

Topics and Details:

1. Phishing Attacks:

- Description: Phishing is a social engineering attack where attackers impersonate trusted entities to trick users into revealing sensitive information.
- Risks: Phishing emails can lead to unauthorized data access, credential theft, financial losses, and malware infections.
- Mitigation: User awareness training, email filtering, and adopting strong authentication methods.

2. Malware Attachments:

- Description: Malicious attachments, such as infected documents or executables, can be sent via email to compromise systems.
- Risks: Opening malware attachments can lead to malware infection, data theft, and system compromise.
- Mitigation: Implementing email attachment scanning, using up-to-date antivirus software, and educating users about safe practices.

3. Spoofing and Email Forgery:

- Description: Attackers forge the sender's email address to make their emails appear legitimate, leading to trust exploitation.
- Risks: Email spoofing can result in unauthorized access, financial fraud, and spreading malware.
- Mitigation: Implementing email authentication protocols (SPF, DKIM, DMARC) to verify sender authenticity.

4. Man-in-the-Middle (MitM) Attacks:

- Description: Attackers intercept communication between sender and recipient, gaining access to sensitive data.
- Risks: MitM attacks can expose confidential information, including passwords and personal data.
- Mitigation: Using encryption (TLS), secure authentication methods, and avoiding unsecured networks.

5. Email Header Manipulation:

- Description: Attackers modify email headers to deceive recipients or bypass security measures.
- Risks: Header manipulation can lead to miscommunication, unauthorized access, and phishing.
- Mitigation: Employing email security gateways, verifying email origins, and using SPF/DKIM/DMARC.

6. Cross-Site Scripting (XSS) in Webmail:

- Description: Vulnerabilities in webmail interfaces can allow attackers to inject malicious scripts into emails viewed by recipients.
- Risks: XSS can lead to data theft, session hijacking, and spreading malware.
- Mitigation: Regular security assessments, input validation, and secure coding practices for webmail applications.

7. Email Account Compromise:

- Description: Weak passwords or credential leaks can lead to unauthorized access to email accounts.
- Risks: Compromised accounts can be used for spreading malware, launching attacks, and stealing sensitive data.
- Mitigation: Enforcing strong password policies, enabling multi-factor authentication, and monitoring account activity.

Conclusion:

The security vulnerabilities inherent in email applications pose significant risks to individuals and organizations. Understanding these vulnerabilities and their potential impacts is crucial for implementing effective security measures. By adopting strategies such as user awareness training, email filtering, encryption, and authentication protocols, users and organizations can significantly enhance their email security posture and mitigate the risks associated with these vulnerabilities.

Experiment Name: Analysis of Computer Network Components and Features of Mobile Security Apps

Objective

The primary objective of this experiment is to analyze various components that constitute a computer network and explore the essential features of mobile security applications. This analysis covers critical topics related to network components, their functions, and the features provided by mobile security apps for safeguarding mobile devices.

Analysis of Computer Network Components:

1. Network Devices:

- Description: Identify and explain various network devices like routers, switches, hubs, and access points.
- Functions: Routers connect different networks, switches manage data traffic, hubs pass data to all connected devices, and access points provide wireless network access.

2. Network Topologies:

- Description: Discuss common network topologies, including star, bus, ring, and mesh.
- Functions: Different topologies determine how devices are connected and communicate within a network.

3. Networking Protocols:

- Description: Explain network protocols like TCP/IP, HTTP, HTTPS, and FTP.
- Functions: Protocols define rules for data communication, ensuring seamless interaction between devices.

4. IP Addressing:

- Description: Explore IPv4 and IPv6 addressing, subnetting, and IP classes.
- Functions: IP addresses uniquely identify devices on a network and enable data routing.

5. Network Security Measures:

- Description: Discuss security mechanisms like firewalls, intrusion detection systems, and virtual private networks (VPNs).
- Functions: Security measures protect networks from unauthorized access, data breaches, and cyber threats.

Features of Mobile Security Applications:

1. Antivirus and Malware Protection:

- Description: Explore how mobile security apps offer real-time scanning and protection against malware.
- Features: Malware detection, app scanning, and removal of malicious software.

2. Privacy Protection:

- Description: Discuss features that safeguard personal data, such as app permission control and data encryption.
- Features: App permission management, data encryption, and secure browsing.

3. Anti-Theft and Device Tracking:

- Description: Explain how mobile security apps aid in locating lost or stolen devices.
- Features: Remote device tracking, lock, and wipe functionalities.

4. App Scanning and Behavior Analysis:

- Description: Explore how security apps analyze app behavior and identify potential threats.
- Features: Scanning for malicious apps, behavior analysis, and anomaly detection.

5. Safe Browsing and Phishing Protection:

- Description: Discuss features that protect users from unsafe websites and phishing attempts.
- Features: Safe browsing mode, URL filtering, and phishing detection.

6. Secure Wi-Fi Connection:

- Description: Explain how security apps ensure safe connections to public Wi-Fi networks.
- Features: Wi-Fi network scanning, secure connection establishment, and VPN integration.

7. Backup and Restore:

- Description: Discuss features that allow users to back up and restore their data.
- Features: Data backup, restore, and synchronization across devices.

Conclusion:

Understanding the components of computer networks and the features provided by mobile security applications is crucial for maintaining a secure and efficient digital environment. By comprehending network devices, topologies, protocols, and security measures, individuals and organizations can build robust networks. Similarly, mobile security apps play a vital role in protecting sensitive data, privacy, and devices from a wide range of threats. Implementing these security measures ensures a safer and more resilient digital experience for users.