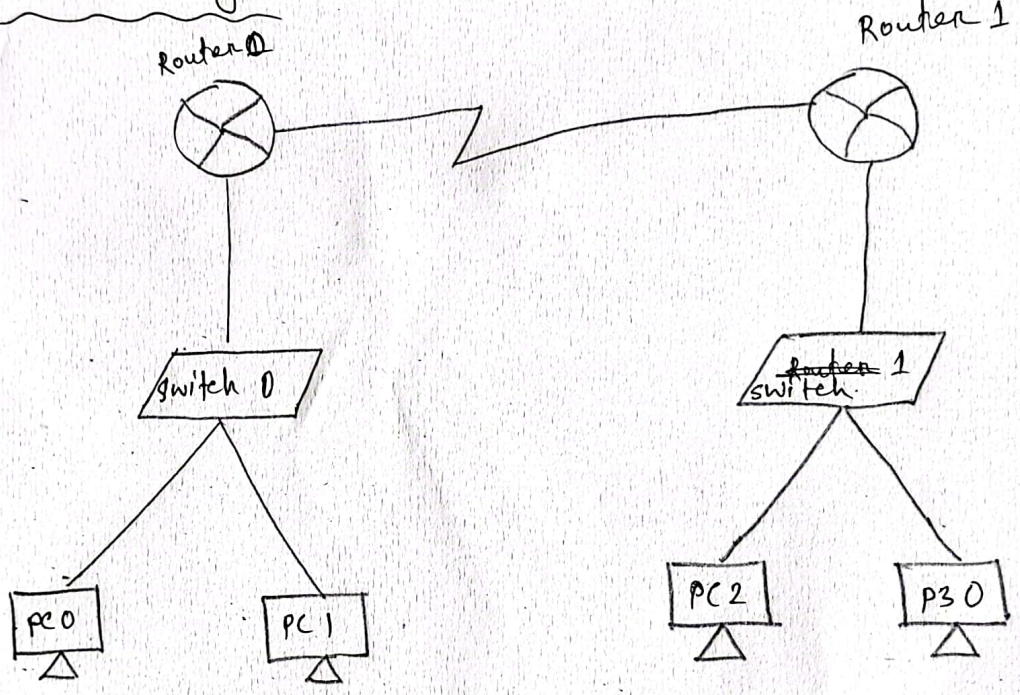
Experiment No: 01

Experiment Name: Design and configure a RIP server by using a RIPv1 or RIPv2 dynamic routing protocol also connect four LANs.

Network Design:



IP configuration:

PC 0 : 192.168.1.2
PC 1 : 192.168.1.3
} d.gateway = 192.168.1.4

PC 2 : 192.168.2.2
PC 3 : 192.168.2.3
} d. gateway = 192.168.2.4

Router0: F/0/0 = 192.168.1.4
F-0/1 = 192.168.3.2

Router 1:

F-0/0: 192.168.3.3

F-0/1: 192.168.2.4

procedure: (1.) Finst we will take 4 PCs.

(2) We will take 2 switches and 2 routers.

(3) We will configure the pcs and the routers.

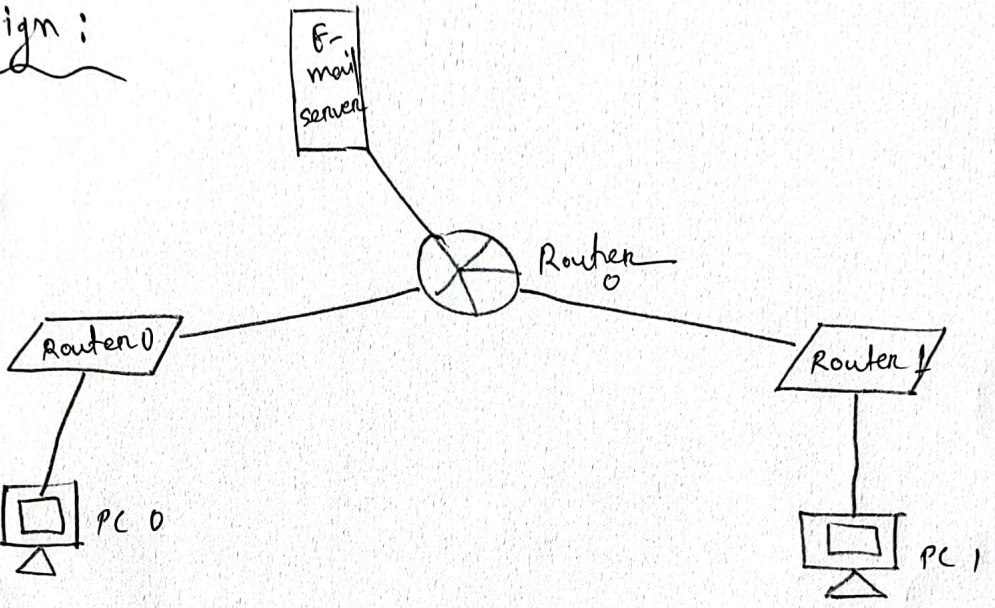
(4) We will ad RIP configuration of both routers.

(5.) Then we will check the connection of message passing.

Experiment No : 02

Experiment Name: Design and configure Email protocol SMTP and POP using cisco routers.

Design :



IP configuration :

PC 0 : ip = 192.168.1.2
default gateway = 192.168.1.1

PC 1 : ip = 192.168.2.2
default gateway = 192.168.2.1

Router 0 : Gigabit Ethernet 0/0 = 192.168.1.1
Gigabit Ethernet 0/1 = 192.168.2.1
Gigabit Ethernet 0/2 = 192.168.3.1

Server : ip = 192.168.3.2
default gateway = 192.168.3.1

procedure:

After configure all the ip address:

server → service → EMAIL:

Domain name = gmail.com

user = shad password = 1234 → +

again.

user = bot password = 1234 → +

Then go to PC-0:

Desktop → Email →

your name = shad

Email add = shad@gmail.com

Incoming and Outgoing mail server = 192.168.3.2

User name = shad

password = 1234 → save

then go to PC 1 and same as PC 0 but name will be changed to "bot".

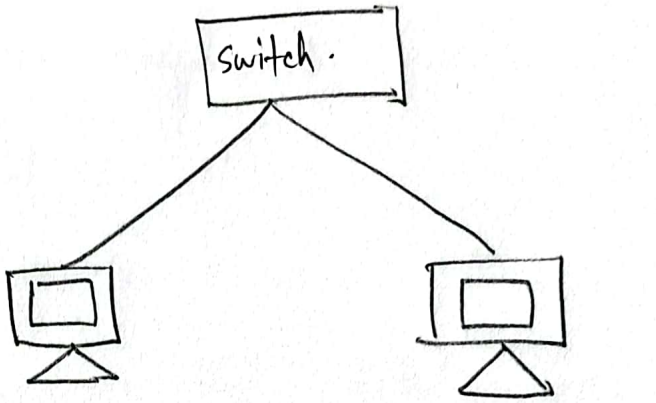
Then PC 0 or PC 1 choose anyone.

Then go to compose and receiver email and subject and message. Then go to another PC receiving the email and go to receive and you can see the email sent by another PC.

Experiment No: 03

Experiment Name: Design and configure firewall security in a windows.

Design:



Ip configuration:

PC-0 : 192.168.0.1

PC-1 : 192.168.0.2

procedure:

PC-0 → desktop → firewall → action → deny.
service → on.
protocol → ICMP. Remote ip = 0.0.0.0
Remote wireless mask: 255.255.255.255
the add.

Again, protocol → Ip, action → allow.

Remote ip : 0.0.0.0

Remote wireless mask : 255.255.255.255.

then "add".

then, we can check by go to PC-0 and terminal →

ping 192.168.0.2

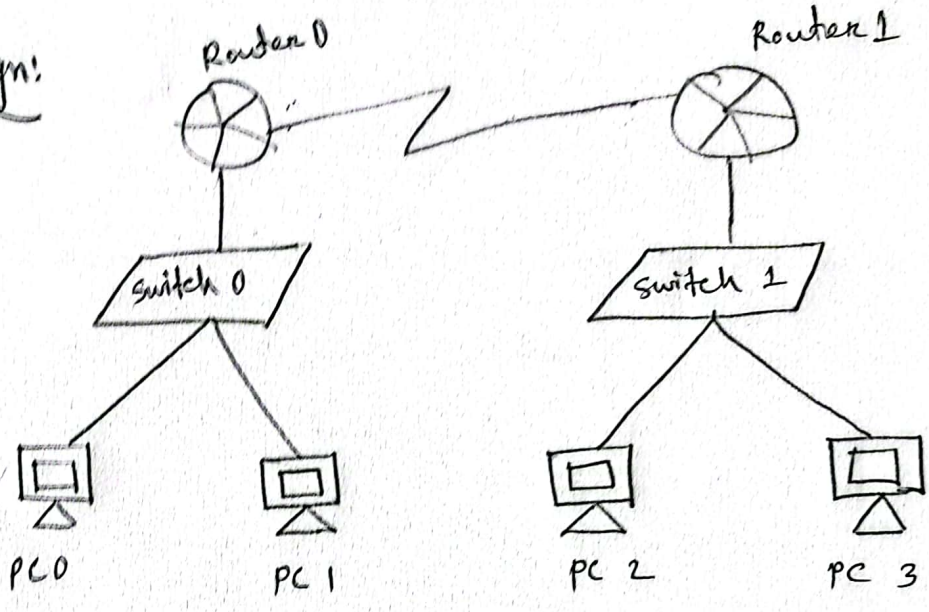
we can see that data/message is not going to PC-A.

So, firewall is working.

Experiment No: 04

Experiment Name: Design and configure a network with 4 LAN connected through PPT connection by using 2 cisco routers.

Design:



Configuration:

Router 0:

FastEthernet 0/0 = 192.168.1.1

serial 2/0 = 10.1.1.1

Router 1: FastEthernet 0/0 = 192.168.2.1

serial 2/0 = ~~10.0~~ 10.1.1.2

PC 0: ip = 192.168.1.2

dg = 192.168.1.1

4.(ii).

PC 1: ip = 192.168.2.2
dg = 192.168.1.1

PC 2: ip = 192.168.3.2
dg = 192.168.2.1

PC 3: ip = 192.168.4.2
dg = 192.168.2.1

procedure: We will add 3 ip address both Router 0 and 1 in RIP section.

Router-0

192.168.1.0
192.168.2.0
10.0.0.0

Router-1

192.168.3.0
192.168.4.0
10.0.0.0

Then,

Router-0 → CLI:

Router > enable
Router # configure terminal
Router (config) # hostname R1.
R1 (config) # username R2 password cisco
R1 (config) # interface serial2/0
R1 (config-if) # ip address 10.1.1.1 255.255.255.252

R1(config-if)# encapsulation ppp

R1(config-if)# ppp authentication chap

R1(config-if)# clock rate ?

R1(config-if)# clock rate 64000

R1(config-if)# end

R1# copy run start

R1#

Router (1) CLI

Router> enable

Router# configure terminal.

Router(config)# hostname R2

R2(config)# username R1 password cisco

R2(config)# interface serial 2/0

R2(config-if)# ip address 10.1.1.2 255.255.255.252

R2(config-if)# no shutdown.

R2(config-if)# encapsulation ppp

R2(config-if)# ppp authentication chap.

R2(config-if)# end

R2# copy run start.

R2# .....

Experiment No: (05)

Experiment Name: Analysis the features of firewall in providing network security.

Discussion:

Firewall: Firewall is a type of software or firmware that prevent unauthorized users from accessing a network as a part of broader network security strategy.

There are many different features of that firewalls offer to provide network security. Some of the most common features include:

* Packet filtering: This is the basic function of a firewall, and it allows you to control which types of traffic are allowed to pass through the firewall. You can create rules to allow or block traffic based on source and destination IP address, ports and protocols.

* Application layer inspection: Allows firewall to inspect traffic at the application layer, which can help to identify and block malicious traffic. For example, a firewall can inspect HTTP traffic to look for signs of phishing or malware.

* Instruction prevention system: Allows firewall to actively block malicious traffic. IPS use signature to identify known malicious traffic, and they can also use anomaly detection to identify suspicious traffic.

* Virtual private networks (VPN): VPN allows you to create secure tunnel between two networks. This can be used to allow remote users to connect to your internal network securely, or to connect two different networks securely.

* Bandwidth management: Can be used to manage bandwidth usage on your network. This can be helpful for preventing congesting and ensuring

that critical applications have enough bandwidth.

Some firewalls also provide addition features like.

(i) Sandboxing.
(ii) Data loss preventing (DLP).
(iii) Cloud security.

Benefits of using firewalls:

preventing of unauthorized access.
protection from malicious traffic
Improve network performance.
Increase security awareness etc.

Overall, firewall is an essential component of network security. They provide a number of benefits, including prevention of unauthorized access, protection from malicious traffic, improved network performance, and increased security awareness.

Experiment No: 06.

Experiment Name: Analysis the security vulnerabilities of E-mail applications.

Discussion: E-mail applications are common target for cyber attacks because they are widely used and often contains sensitive information. Some of them are:

phishing: Is a type of social engineering attack that uses email to trick users into revealing sensitive information, such as password or credit-card numbers.

Malware: Can be attached to email or embedded in links in emails. When user opens the attachment or click on the link, the malware can be installed on their computer.

spoofing: Is a technique that can be used to make emails appear to come from a legimate source. This can be use to trick users

into opening emails that they would not otherwise open.

Weak password: Weak passwords are common vulnerability that can be exploited by attackers. If users have weak passwords, attackers can easily gain access to their email accounts.

Configuration errors: can allow attackers to gain access to email systems. These errors can be caused by misconfiguration of email servers or by users making changes to their email settings.

To protect against these ~~vult~~ vulnerabilities, best practices are

- Educating users about phishing and malware.
- Using strong password.
- keeping email applications up to date.
- Using a firewall.

Here are some additional tips for improving the security of email-applications:

- Use a spam filter.
- Enable two factor authentication.
- Be careful what you click on and
- Scan attachments for malware etc.

By following these tips, we can help to protect email applications from cyberattacks and keep sensitive information safe.

Experiment no: 07

Experiment Name: Analysis different computer network components and features of any of the mobile security apps.

Discussion: Avast Mobile Security is a comphensive mobile security apps that offers a variety of features to protect your android device from malware, viruses, and other threads. Some of them:

Firewall: The firewall in Avast Mobile Security can help to protect your device from unauthorized access and malicious traffic. The firewall can block traffic from unauthorized sources and can also filter traffic to prevent malicious from reaching your device.

Anti-virus: The anti-virus engine in Avast Mobile Security can help you to protect your device for malware and viruses. If any malware or viruses are found, Avast Mobile Security can remove them from your device.

*Web-shield: The web shield can help to protect your from malicious websites. The web shield can scan websites for malware and viruses before you visit them. If any malicious websites are found. It will block you from visiting them.

*App lock: Can help you from sensetive application of unauthorized access. Simple you can use PIN, Password to protect.

*privacy advisor: The privacy advisor can help you to protect your privacy. It can scan your device for privacy settings that you may not be aware of. If any privacy settings are found that could be compromise your privacy, the privacy advisor will warn you about them.

*Anti theft: Can help you to track and recover your lost or stolen device. If the device is stolen then simply you can find

your device or you can earse all the data of that device with the help of it.

Here are some additional tips for improving the security of mobile device.

- keep device up to date.
- Use a strong password.
- Be ~~cause~~ careful about downloading.
- Use a VPN etc.

Experiment No: 08

Experiment Name: Analysis the security vulnerabilities of e-commerce services.

Discussion: E-commerce services are common target for cyber attacks, as they offer wealth of personal and financial data that can be exploid by cyber-criminals. some of the most common security vulnerabilities are:

- SQL injection: This is a types of that injects malicious code into a web application's SQL ~~queries~~ queries. This can be used to steal data, modify data, or even take control of application.

- Cross-site scripting: It injects malicious code into a web page. This can be executed by victim's browser, which can lead to the thefit of cookies, session tokens, or other sensitive data.

- Information disclosure: Allows unauthorized users to view sensitive information, such as customer data or

financial information. This can be caused by a variety of factors, such as week passwords, insecure file permissions, or improper error handling.

- payment fraud: Used to steal money from e-commerce customers. This can be done through a variety of methods, such as credit card fraud, chargeback fraud or friendly fraud.

- Botnets: These are networks infected computers that are controlled by cybercriminals. Botnets can be used to launch a variety of attacks against e-commerce services, such as -: denial-of-services, click fraud or spam campaigns.

Some steps to protect customers & data by implementing security measures such as:

→ Using strong password and security practices.

→ keeping software up to date.

→ Using a web application firewall (WAF).

→ Monitoring your website for suspicious activity.

In adding to the above, some other security best practices for e-commerce :-

Encrypt all sensitive data.

Use a secure payment gateway.

Have a clear privacy policy.

Educate your employees ~~and~~ about security.

By following these security best practices, e-commerce businesses can help to protect their customers and their data from cyberattacks.