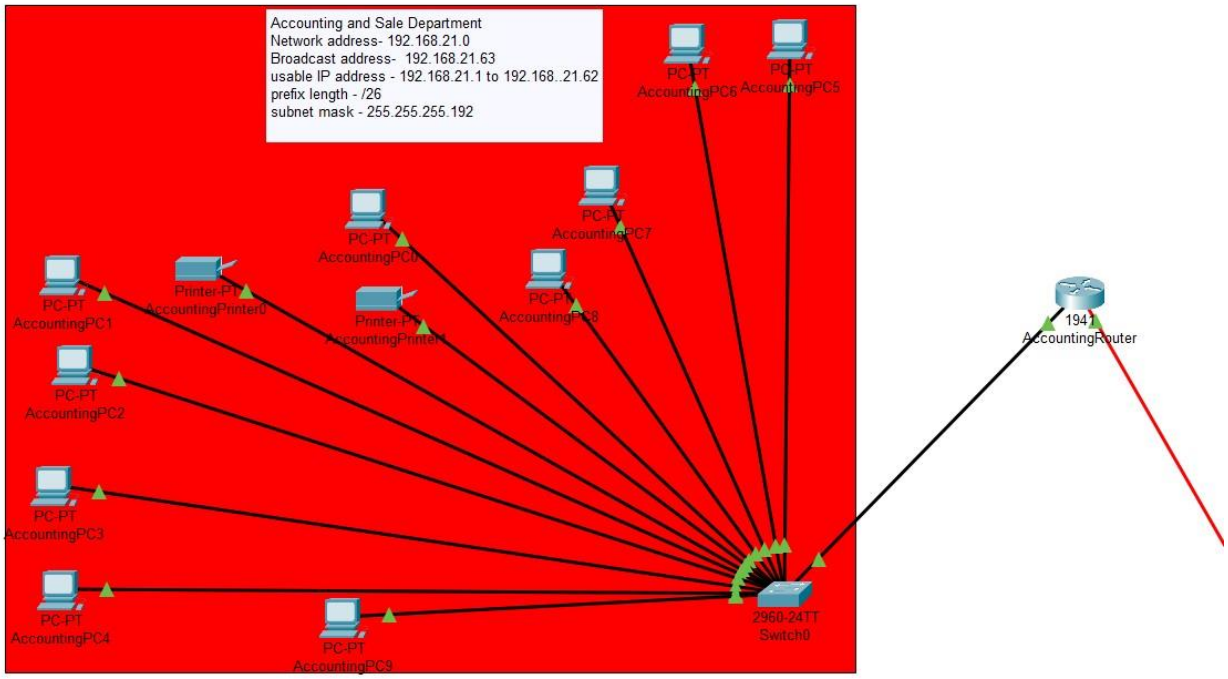
NETWORKING

Introduction

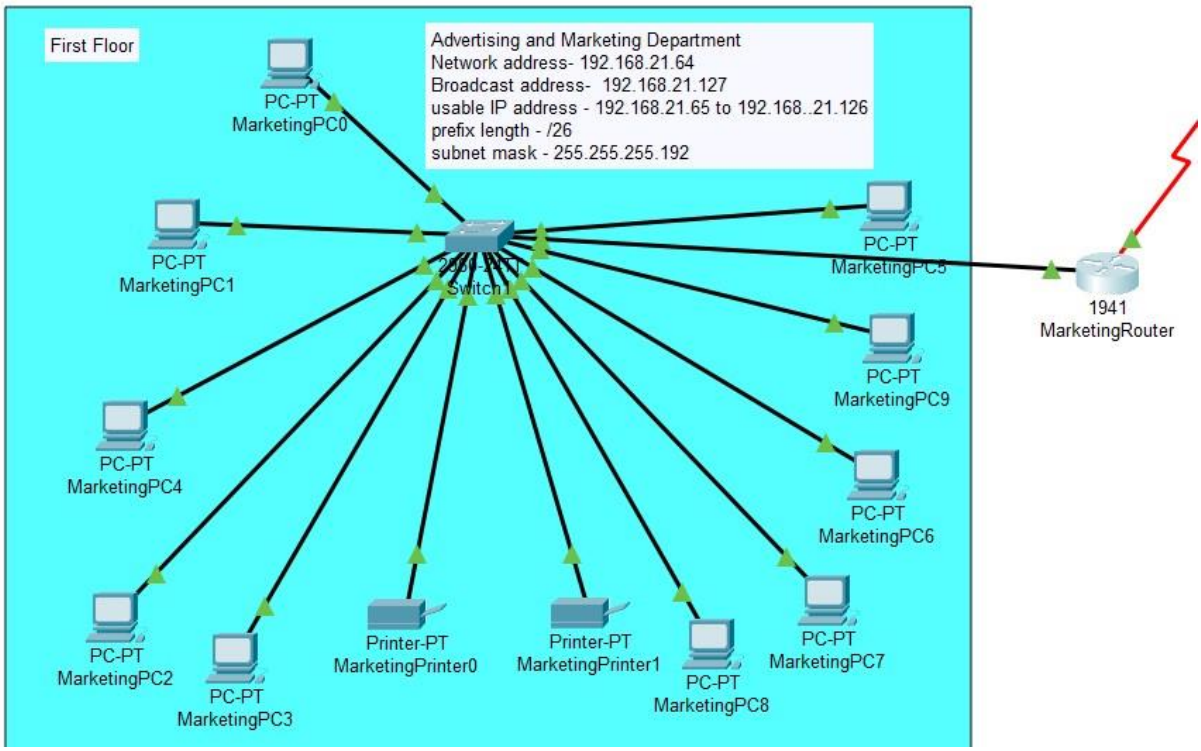
Explanation about networking fundamentals, focusing on cabling, DHCP versus static IP addressing, switches, routers, topologies, and company requirements. A design will be created to illustrate the network structure, highlighting the rationale for using static IP addresses, switches, and routers. The project will also include a test plan to evaluate network performance across departments and gather feedback from employees to ensure functionality and address any issues. Detailed explanations of each component and its role in the overall network will be provided.

PART 1

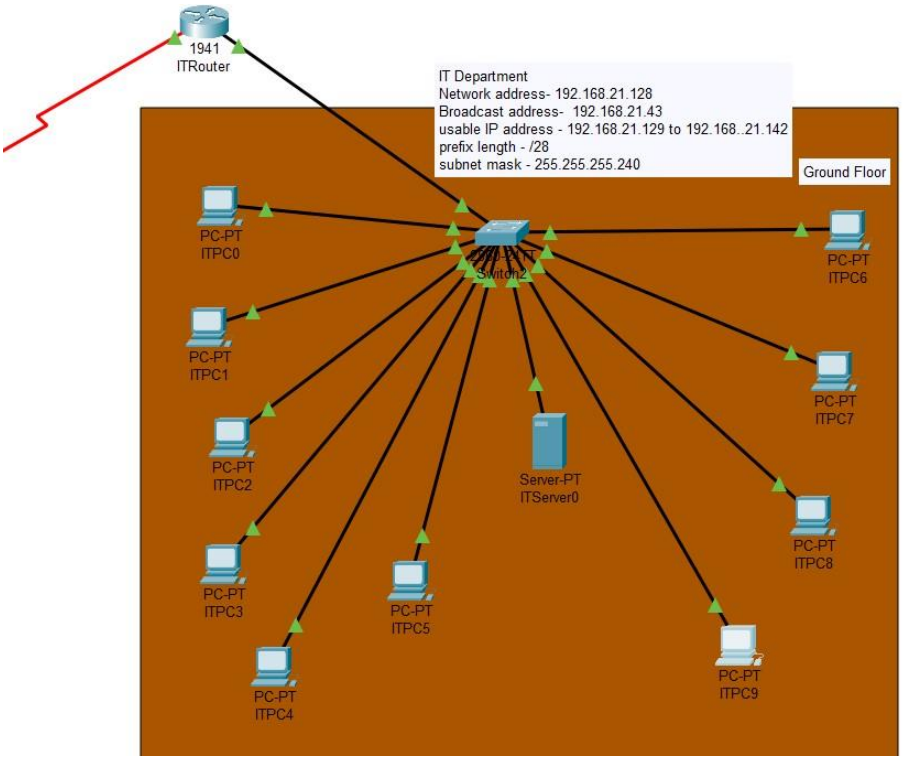
Accounting and sales departments



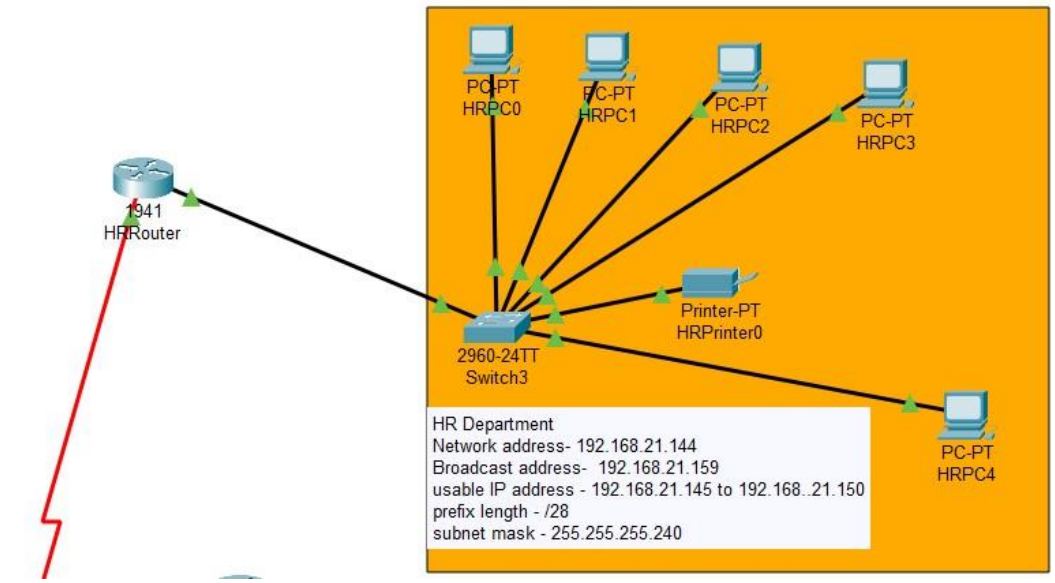
Advertising and marketing department



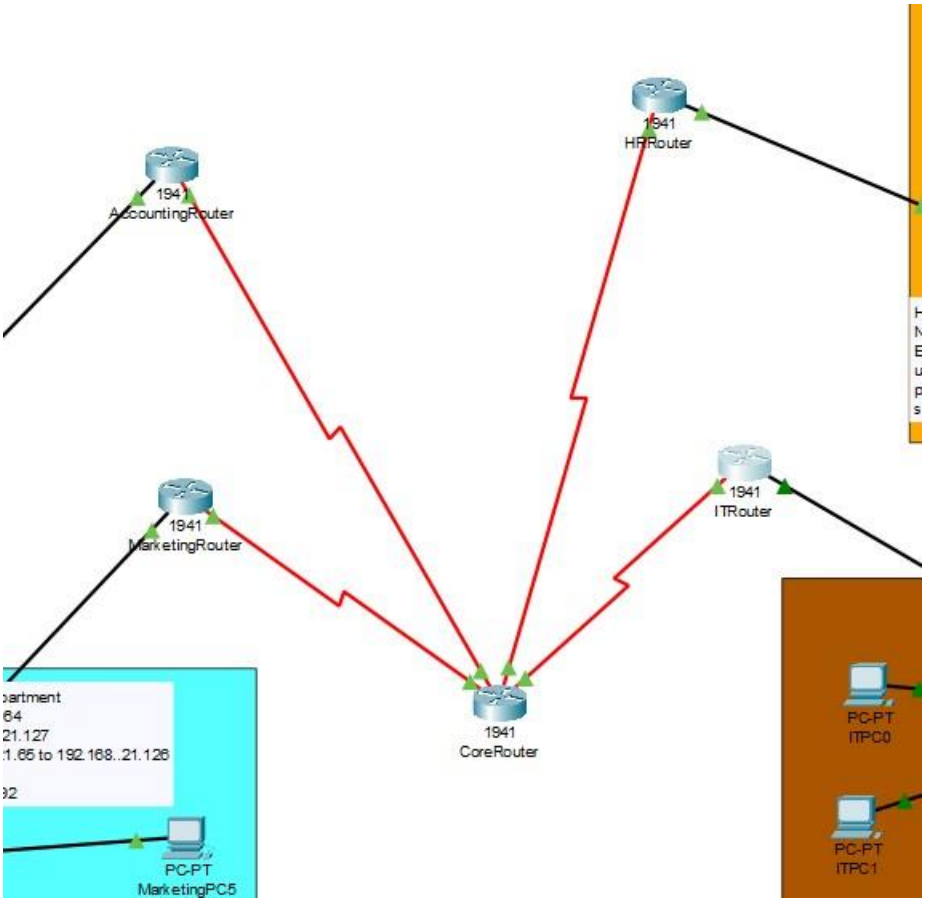
It department



HR department



Connect 4 departments router with core router



IP address

Department	Network Address	Broadcast Address	First IP Address	Last IP Address	Prefix Length	Subnet Mask

Accounting	192.168.21.0	192.168.21.63	192.168.21.0	192.168.21.62	/26	255.255.255.192
Advertising and marketing	192.168.21.64	192.168.21.127	192.168.21.64	192.168.21.126	/26	255.255.255.192
IT	192.168.21.128	192.168.21.43	192.168.21.128	192.168.21.142	/28	255.255.255.240
HR	192.168.21.144	192.168.21.159	192.168.21.144	192.168.21.159	/28	255.255.255.240

PART 2

Why we use static

Utilizing a Virtual Private Network (VPN) or other remote access software is simpler with a static IP address. More dependable communication: Using Audio over Internet Protocol (VoIP) for teleconferencing or other voice and video communications is made simpler by static IP addresses.

From accounting and sales department

From this local area network, we have 30 computer totals for the department and 2 printers all connected to switch 0. We gave IP address starting with 192.168.21.0 to 192.168.21.62 with subnet mark 255.255.255.192 and broadcast address with 192.168.2.63. the switch 0 is connected to accounting router.

From advertising and marketing department

From this local area network, we have 40 computers and 2 printers in the department all connected to switch 1 and that switch is connected with marketing

router. We have IP address starting with 192.168.21.64 to 192.168.21.126 with 255.255.1.92 subnet mark and 192.168.21.127 broadcast address.

From IT department

From this local area network, we have 10 computers and 1 server in IT department for the company which is connected to switch 2 and that switch connected to IT router. We gave IP address starting with 192.168.21.128 to 192.168.21.142 with 255.255.1255.40 subnet mark and 192.168.21.159 broadcast address.

From HR department

From this local area network, we have 2 computers with 1 printer for the department connected to switch 3 which is connected to router HR router. We gave IP address starting with 192.168.21.144 to 192.168.21.151 with 255.255.255.40 subnet mark and 192.168.21.159 broadcast address.

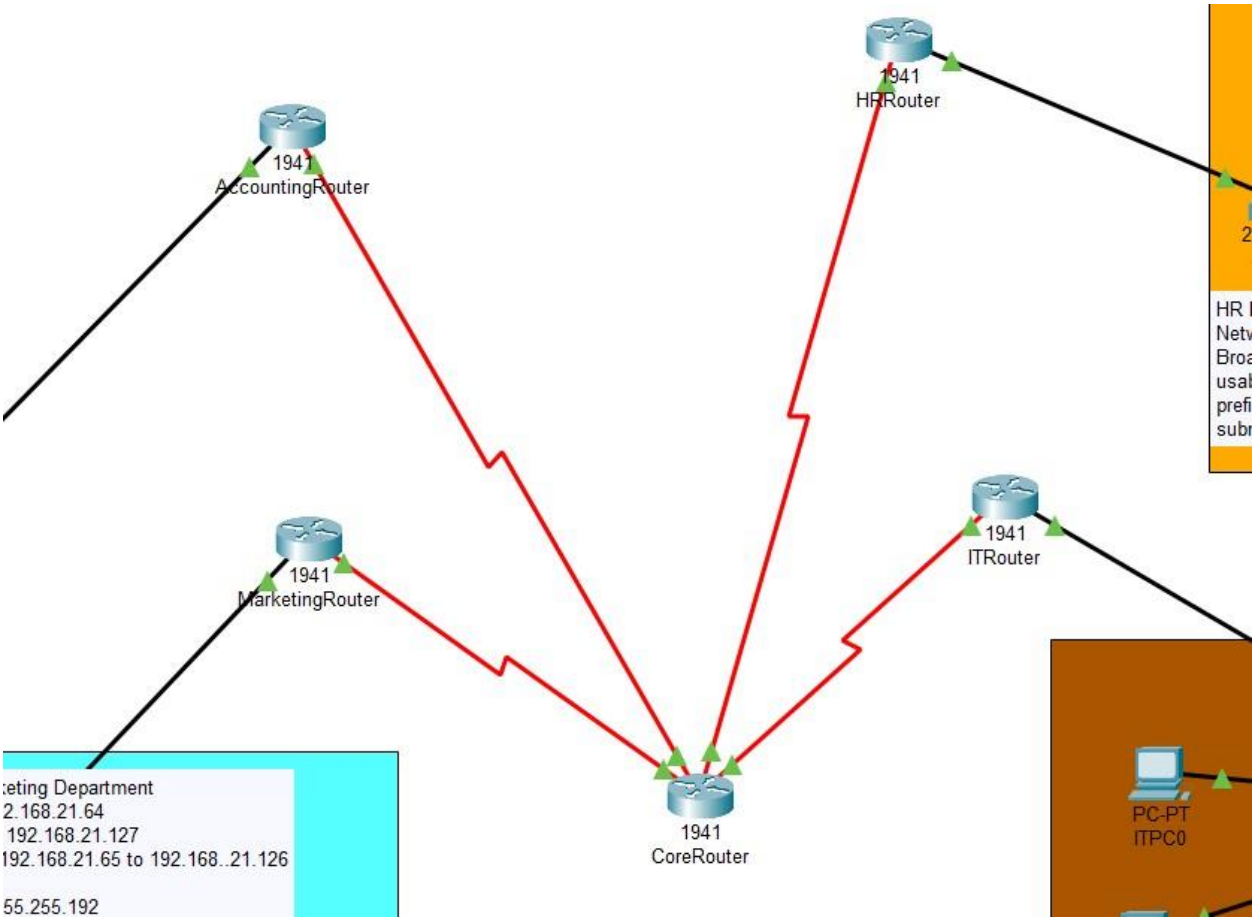
Connecting to all department router to core router

We have 4 routers in total from all the department and we connected the all the routers in core router and make network work all the departments.

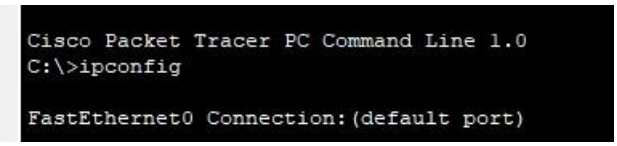
Cable

The cables that connect computers and switches are network cable and use it with copper straight-through and it look like photo from below.

The cables that connects switches to router is also the same cable as the cable use in connecting the computers and switches but for the department routers to the core routers is use as serial DCE cables for better network and it look like photo from below.

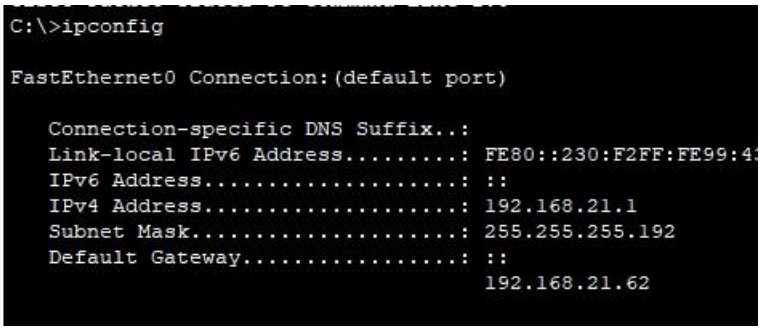


All the cables are default port as fast ethernet connection and to check the cable, we have to double click to any computer and go to desktop I the top bar and go to cmd and type "ipconfig" to check the cabling so it shows like this.



Server

There are total 2 servers in this design and to check the servers, we have to double clicked any computer like cable test and follow the steps till typing "ipconfig" in CMD and the program will show we are using the DNS server or DHCP server by showing like photo below.



Network maintenance plan

A network maintenance plan makes sure that all of your network's crucial components are routinely checked for any issues. A good maintenance strategy should be able to foresee issues before they arise and implement the appropriate countermeasures. By doing this, business continuity is ensured and downtime is decreased.

Hardware and software installation are among the chores that make up a good network maintenance strategy.

Plans for network maintenance include installing hardware and software to ensure that the tools and software we have are functional.

Maintenance plan

Server/System

Time	Details
Daily	❖ Physically inspect your tools. Make sure there are no red or amber lights, odd sounds, or
	odors emanating from your equipment each morning as you check your server room. ✞ Check the replications and backups. ✞ On each of your Windows servers, check the Windows services.

Months	✞ practice backups Make sure you can successfully restore a VM from scratch. ✞ Examine the system and application event logs. ✞ Verify and remove temporary files. ✞ Additionally, if you have roaming profiles for your remote desktop, remove any that did not properly unload. ✞ Purge away idle computers in your endpoint protection by going there. ✞ View your IIS logs, and if everything looks okay, you might want to consider securely purging them. ✞ Install any necessary Windows updates that you find. ✞ Verify that your SANS volumes are all in good condition and that you haven't overprovisioned. ✞ Check your UPS. Check that all of the batteries are in good shape and that you are not utilizing your capacity to the utmost by getting on the management console. Put the date of your battery replacement in your

	maintenance calendar. Batteries should typically be changed every three years.
6 monthlies	❖ Verify backup persistence
	✞ Restart all servers that haven't been started up in the last six months. ✞ For your gear and software that is essential to your business, check your warranties and support

	agreements. Review and comprehend the support contracts for Software and hardware
Annually	✞ methods and documentation for DR ✞ revisions to network diagrams ✞ Compare performance indicators to baselines. ✞ Review and restart keys for service accounts ✞ run DC tests on all domain controllers (DCs).

Network

- ✞ putting in place, updating, or changing both hardware and software
- ✞ maintaining, adjusting, and improving the network
- ✞ keeping network documentation and recording the network
- ✞ protecting the network from attacks both internal and external
- ✞ preparing for network additions, upgrades, or improvements
- ✞ setting up backups and recovering the network or services from backups
- ✞ ensuring adherence to company guidelines and regulatory requirements
- ✞ solving issues with reports
- ✞ upgrading and keeping up with device setups

Time	Details
Daily	✞ Examine the use and delay on your major WAN connections as well as on any VPN or remote site connections. ✞ Record WAN Connection speed and average utilization as performance benchmarks. Ping delay to distant offices. Throughput of NGFW
Quarterly	❖ Make that the date and time are still set correctly and that
	the firmware on your servers, switches, firewalls, raid controllers, and storage area networks is up to current.

Installing, replacing and upgrading both hardware and software

Installation, replacement, and updates of hardware and software are frequent jobs in network maintenance. This could involve replacing outdated or broken hardware in a Cisco network, such switch line cards and supervisor modules in Catalyst 4500 and 6500 series switches, as well as updating Cisco IOS images to the most recent revision or patch level for both routers and switches.

Monitoring, tuning and optimizing the network

Proactive monitoring is one of the key enablers of a successful network maintenance solution or strategy. Through proactive monitoring, possible issues may be found and fixed before they disrupt service or have an adverse effect on

operation. Network monitoring and event logging can be utilized to: Proactively respond to network or system alarms by:

- ✞ Check the network's performance and that of all connected devices.
- ✞ Set a baseline for the network's performance.
- ✞ Recognize how much traffic goes in each direction on the network.
- ✞ Determine and address any network problems

Security

Data protection on your network is referred to as network security. This entails the usage of credentials for every worker, vendor, customer, and other collaborator that your business has. Your networks' continued operation is network security's primary goal. Additionally, your managed network provider must to be able to safeguard your network against nefarious cyberattacks, power outages, and natural catastrophes.

Time	Details
Weekly	❖ Endpoint security Monitor the dashboard and logs. Examine the logs and permits. Examine infected devices.
Monthly	❖ Endpoint security Monitor the dashboard and logs. Examine
	the logs and permits. Examine infected devices.
Quarterly	✞ Examine the access or NAT policies on the firewall. It could be necessary to clear up any that are redundant. It's possible that certain open ports are no longer required.

	✞ Examine the security groups in AD and confirm that the key groups are all members.

Documentation

Knowing the importance of documentation, which is sometimes disregarded as a minor aspect of network administration, is crucial to understanding your network as a whole. Documentation keeps we on track and clarifies the key goal of your network maintenance strategy.

Proactive monitoring is one of the key enablers of a successful network maintenance solution or strategy. Through proactive monitoring, possible issues may be found and fixed before they disrupt service or have an adverse effect on operation. Network monitoring and event logging can be utilized to: Proactively respond to network or system alarms by:

- ✞ Check the network's performance and that of all connected devices.
- ✞ Set a baseline for the network's performance.
- ✞ Recognize how much traffic goes in each direction on the network.
- ✞ Determine and address any network problems

Update and configuration

Software and hardware configuration and updates should be able to be planned by your managed network provider. This increases your overall network security by ensuring that both your software and hardware are in excellent condition.

Utilizing network monitoring, you may anticipate difficulties and prepare for prospective network upgrades or expansions, or capacity planning, based on the issues you anticipate. Effective planning may be used to specify the network maintenance activities that are necessary, priorities those tasks, and determine the sequence in which they will be carried out.

Trouble shooting

A fundamental aspect of network maintenance is problem solving. Troubleshooting is made easier by a structured network maintenance strategy, which includes documentation, backups, and some kind of proactive monitoring system. Troubleshooting approaches are explained in depth later in this guide.

Maintenance and updating devices and configuration

Because of routine transfers, additions, or changes (MACs) inside businesses, configuration modifications are frequent. Due to planned network modifications and periodic maintenance procedures, device configurations may also change. Maintaining and upgrading device settings is seen as a basic network management duty because of this. Every time a device's configuration changes, it should not only be recorded but also stored there and in a different place as a backup, such an FTP or TFTP server (if one is available).

Backup

Data is king nowadays. Your data should be regularly created and stored in backups by a managed network provider. Making ensuring your data is safe and secure guarantees that your firm is constantly up and functioning since data loss can impede a business' productivity.

Why we need network maintenance

Now, there are certain issues that are impossible to plan for. Using the interrupt-driven method to fix network problems is sometimes your only option. If a third-party maintenance company has we covered, we can relax knowing skilled experts are taking care of the issue as soon as it arises. When working with a customer, TPMs employ a hybrid approach to network hardware maintenance, working to avoid issues wherever feasible while being ready to deal with them when they arise. Although original equipment manufacturers (OEMs) sometimes offer comparable assistance, they are typically slow and more expensive than a TPM provider.

Feed back

Kim: I like your design since it is clear and understandable. Your design is excellent, and the wiring is clearly laid out but if we could do it with DHCP network, I think it will be a lot better for the company.

Marcus: I like your style. Your wire design and IP address distribution are flawless. I appreciate we providing accounting and sales department, accountant in particular. It is obviously meant to seem designed. However, I advise choosing a laptop over an accountant's computer.

Router 0 (Accounting Router)

```
!
interface Serial0/0/0
 ip address 192.168.22.1 255.255.255.252
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.21.0
 network 192.168.22.0
 no auto-summary
!
```

Router 1 (Marketing Router)

```
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.21.0
 network 192.168.23.0
 no auto-summary
!
```

Router 2 (IT Router)

```
!
interface Serial0/1/0
 ip address 192.168.24.1 255.255.255.252
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.21.0
 network 192.168.24.0
 no auto-summary
!
```

Router 3 (HR Router)

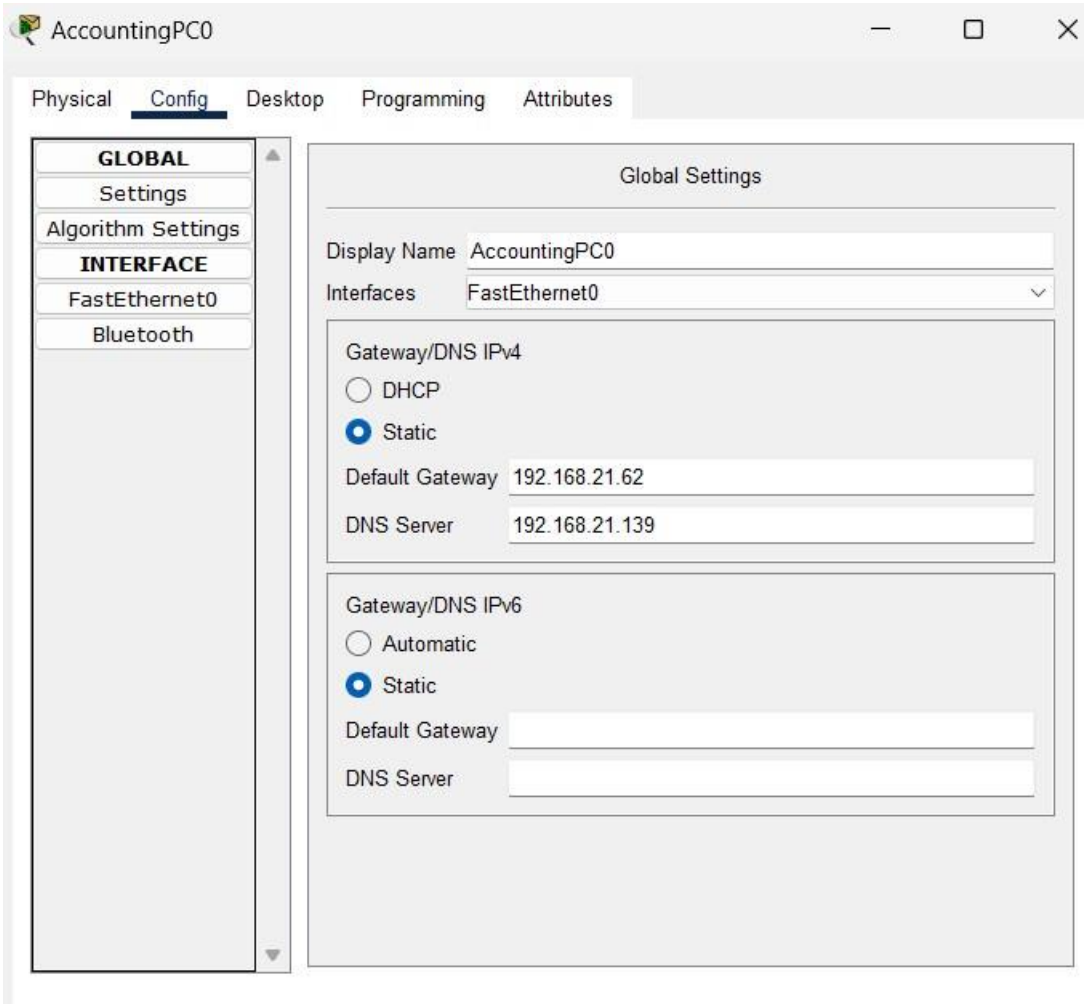
```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 ip address 192.168.25.1 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.21.0
 network 192.168.25.0
 no auto-summary
!
```

```
HRRouter>enable
HRRouter#
HRRouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HRRouter(config)#router rip
HRRouter(config-router)#
HRRouter(config-router)#end
HRRouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HRRouter(config)#
HRRouter(config)#
%SYS-5-CONFIG_I: Configured from console by console

HRRouter(config)#
HRRouter(config)#
```

Core Router

```
!
router rip
 version 2
 network 192.168.22.0
 network 192.168.23.0
 network 192.168.24.0
 network 192.168.25.0
 no auto-summary
!
```

Using DNS Iv4



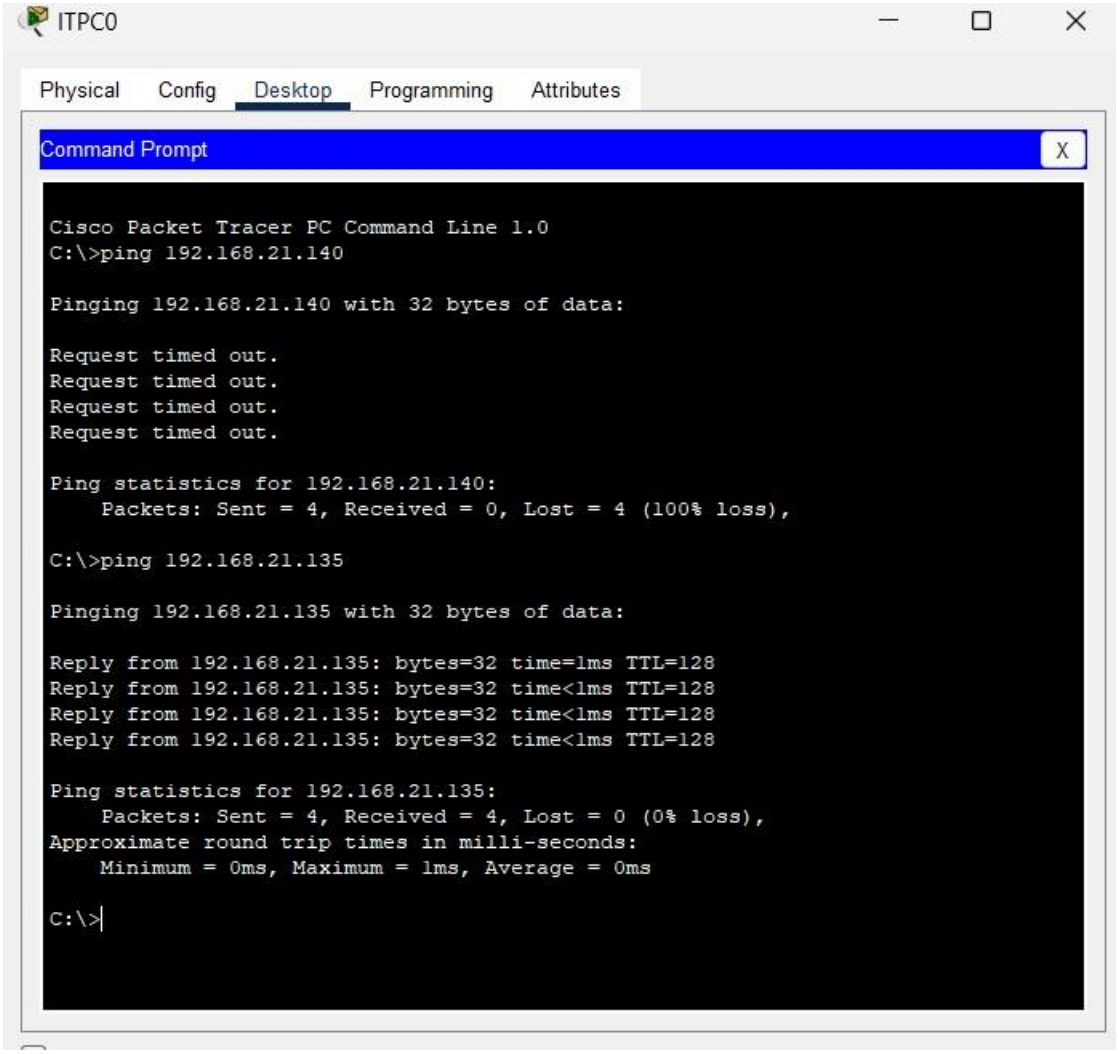
why use iv4 instead of iv6

While IPv4 is restricted to 4.3 billion IP addresses, IPv6 utilizes a 128-bit address and may generate 340 undecillion IP addresses. However, the adoption of IPv6 by ISPs and/or network administrators may result in a number of leaks and security problems. Your personal information may be compromised in this way.

Test plan

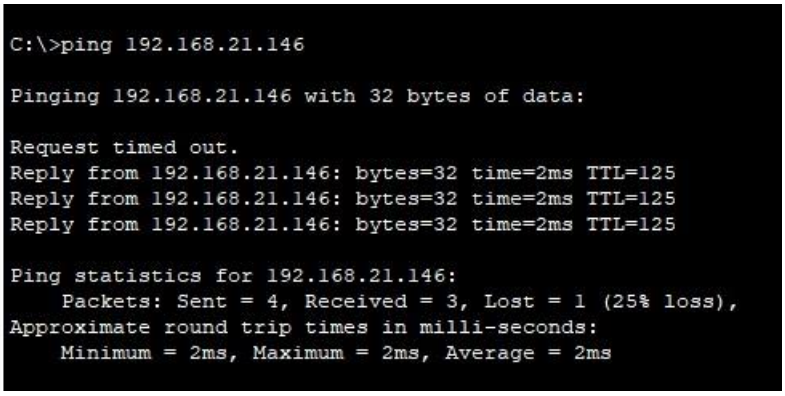
Pinging IT department to IT department

IP address-192.168.21.135



Pinging IT department to HR department

IP address- 192.168.21.146



Pinging IT department to Accounting and sales department

IP address- 192.168.21.9

```
C:\>ping 192.168.21.9

Pinging 192.168.21.9 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.9: bytes=32 time=48ms TTL=125
Reply from 192.168.21.9: bytes=32 time=25ms TTL=125
Reply from 192.168.21.9: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.21.9:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 48ms, Average = 25ms
```

Pinging IT department to Advertising and sales department

IP address- 192.168.21.70

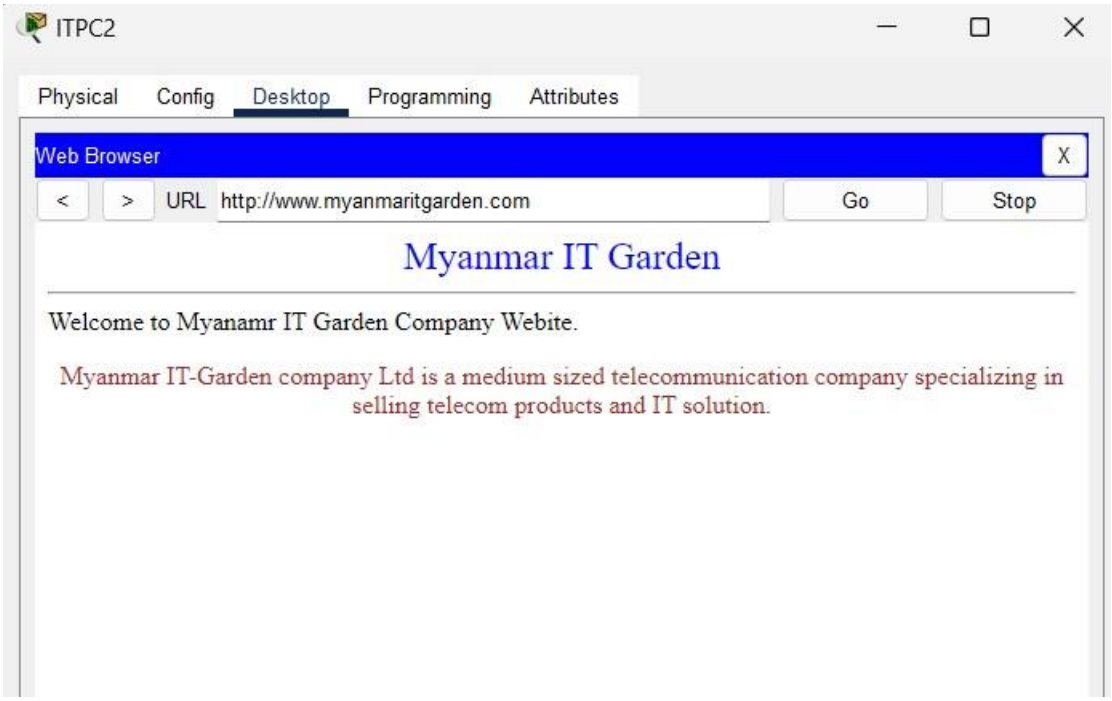
```
Pinging 192.168.21.7 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.7: bytes=32 time=2ms TTL=125
Reply from 192.168.21.7: bytes=32 time=18ms TTL=125
Reply from 192.168.21.7: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.21.7:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 7ms

C:\>
```

Ping Department	Reply department	IP address	Success or fail
IT	IT	192.168.21.135	success
IT	HR	192.168.21.146	success
IT	Advertising and marketing	192.168.21.9	success
IT	Accounting and sales	192.168.21.70	success

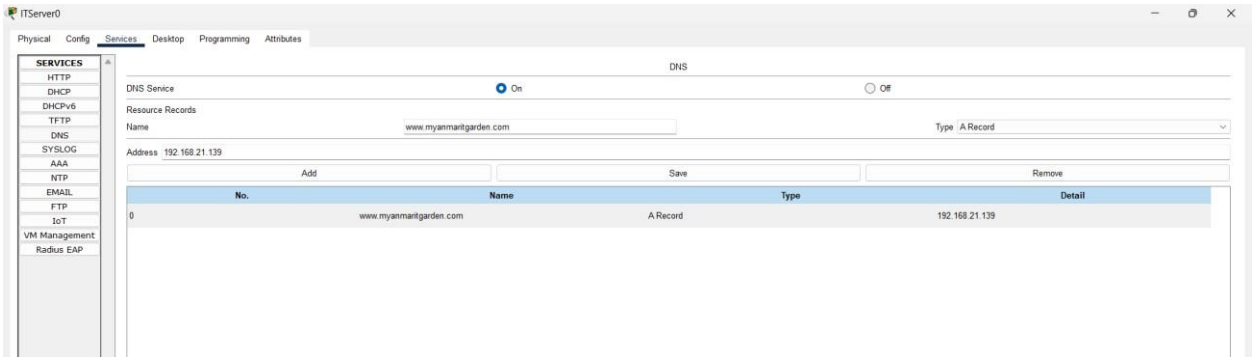
Server IP ping from marketing

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.21.139

Pinging 192.168.21.139 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.139: bytes=32 time=4ms TTL=125
Reply from 192.168.21.139: bytes=32 time=3ms TTL=125
Reply from 192.168.21.139: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.21.139:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\>
```

Web from IT server

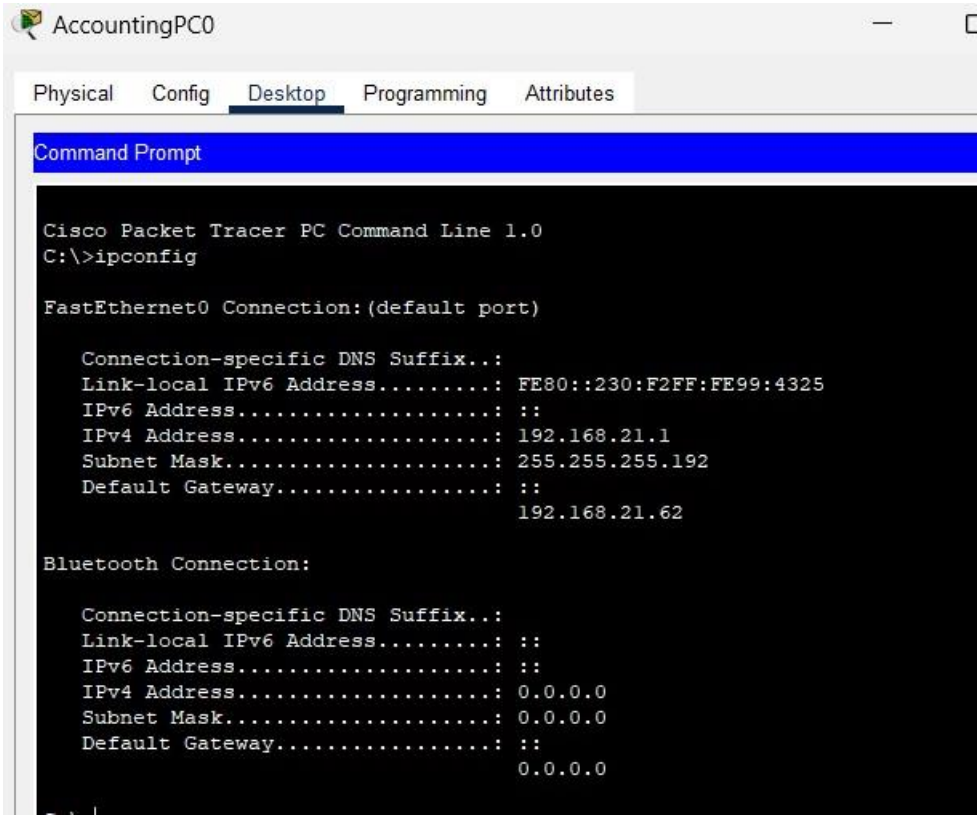


DNS



Checking IP CONFIG

Accounting PC0



PART 3

Network services needed for company in future

1. Installation of a network

Businesses rely significantly on networks for day-to-day operations, so they must be dependable and secure. A certified managed service provider (MSP) may assist firms in replacing their antiquated network with one that supports their current business strategies. Professional network installation services are available.

Network security, wireless network services, computer cabling, support for mobile devices, network integration services, and software and hardware installation are just a few of the essential network installation services that managed network service providers provide. An MSP may assist with the design and configuration of a quick and effective corporate network.

2. Network Engineers verifying Server Maintenance two Support services for fixing and improving server hardware are included in server maintenance.

This might involve diagnosing and changing different server parts such CPUs, motherboards, hard drives, and memory. Organizations may concentrate on their operations with the aid of a managed network service provider (MSP), who will also maintain their server software up to date and functioning properly.

Additionally, server maintenance services may assist businesses in preventing data loss, expensive downtime, and partial or total network failure. When a company server does experience issues, an MSP will deal with the situation right away to avoid a big catastrophe that affects regular business activities.

3.Services for Structured Cabling

A system of wires, cables, and other hardware known as "structured cabling" links various communication systems into a single, cohesive unit. Numerous advantages can result from building a thorough communications infrastructure, including more adaptability, lessened clutter, and expedited system problems and other bug diagnostics.

Businesses can benefit from enhanced connectivity, security, and audiovisual applications. Fiber optic cables, CAT6, and CAT6A cables are just a few of the numerous types of cables that managed network service providers employ to supply structured cabling services. These cables may increase the connection speed between the server and other devices and are very compatible with many kinds of network equipment.

Devices

Other recommended devices

Hub

Why use hub

The connecting point for all devices on a local area network is a hub, often known as a network hub (LAN). Open Systems Interconnection (OSI) Layer 1, the initial and most fundamental layer, is where hubs function (also called the physical layer). They link network equipment including servers, workstations, printers, scanners, etc. via an RJ45 socket and twisted-pair wiring.

How It work

All devices on a local area network are connected to one another through a hub, also known as a network hub (LAN). Hubs function at Layer 1, the initial and base layer of the Open Systems Interconnection (OSI) protocol (also called the physical layer). They employ twisted-pair cabling and often link network equipment including servers, workstations, printers, scanners, etc. via an RJ45 socket.

Repeater

Why use repeater

Star topology describes a LAN's ability to allow any individual unit to interface directly with the hub or central device. Topology is the physical configuration used to create a network connection point. The term "multiport repeater" also applies to this central device. This repeater's function is to enable signal transmission across greater distances. To make up for the shortcomings of star topology cabling, multiple ports Ethernet repeaters are employed.

We use star topology for the company in assignment 1 and with repeater star topology is very useful and very easy and good to use for network. Star topology in a LAN is when each individual unit is given access to interact directly with the hub or central device. The physical configuration used to create a network connection point is known as topology. The multiport repeater is another name for this core device. This repeater's function is to enable the signal to reach farther distances. Ethernet repeaters with many ports are used to make up for the shortcomings of star topology cabling.

How it works

In computer networks, repeaters are used to increase the network's coverage area, replicate a weak or damaged signal, and/or support faraway nodes. Repeaters boost the input/received signal to a higher frequency range, making it more useable, scalable, and accessible.

VPN

Why use VPN

Staff's access to internal IP addresses, regional servers, shared files, and remote access to devices are all made possible through a VPN. Remote workers may more easily access the tools they need to accomplish their jobs thanks to a secure network without endangering the organizations.

The corporate perimeter of an organization's headquarters provides direct access to the corporate network for employees, negating the requirement for a business VPN connection. For secure network access while they operate remotely, branch office personnel, remote employees, or staff going beyond the locked corporate boundary require a business VPN.

Remote users can securely access the network infrastructure of their company via a remote access VPN. Additionally, it encrypts all data that remote workers transmit to and receive from the network infrastructure, allowing a company's remote workforce to safely access and utilize tools, services, and applications that are housed in the corporate data center and headquarters.

Companies with several offices in various regions that require continuing access to and usage of the corporate network commonly employ site-to-site VPNs. A corporation may securely link its corporate network with its remote offices using a site-to-site VPN so that they can interact and share resources as one network.

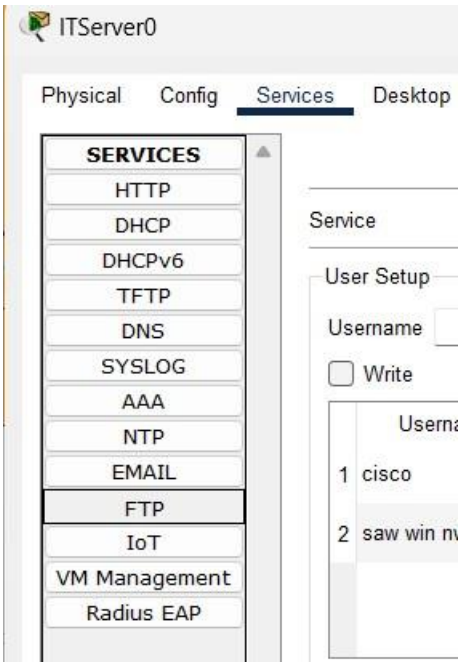
File server

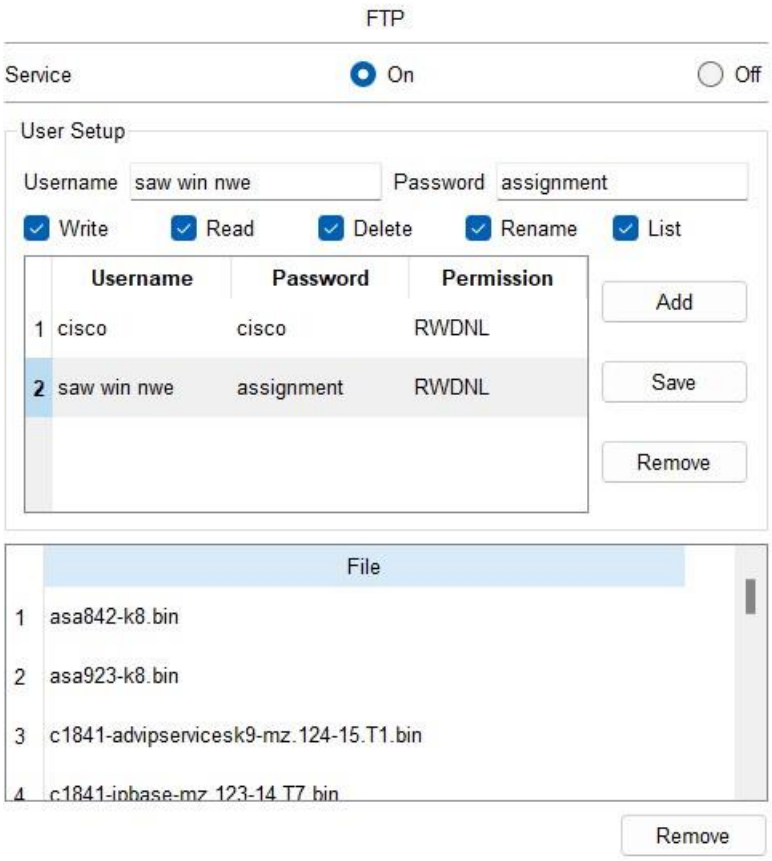
Why we use file server

For the creation of a website, FTP is necessary. It makes it possible for the web developer to transfer data from their computer to the server that hosts the website they are developing. The primary access method to the FTP server, where all of the essential components of the website are kept, is FTP.

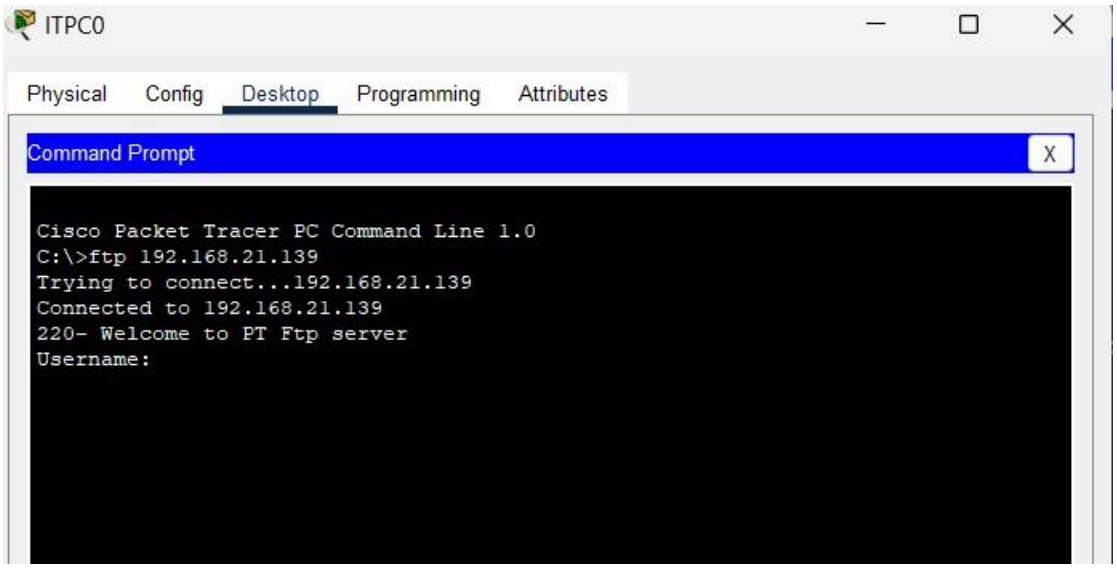
Inserting file server FTP in IT department

First, we put new FTP with username and password by doubling clicking the ITserver0 and clicked services and go to FTP and we clicked “on” and we create new FTP by putting username “saw win nwe” and passwords
“assignment” and give permission on write, read, delete, rename and list the FTP and save it as the photo below.

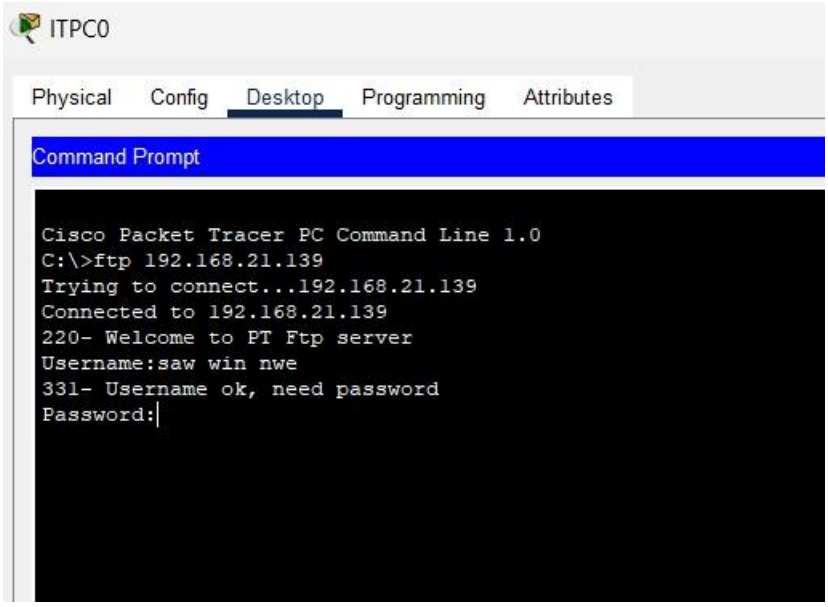




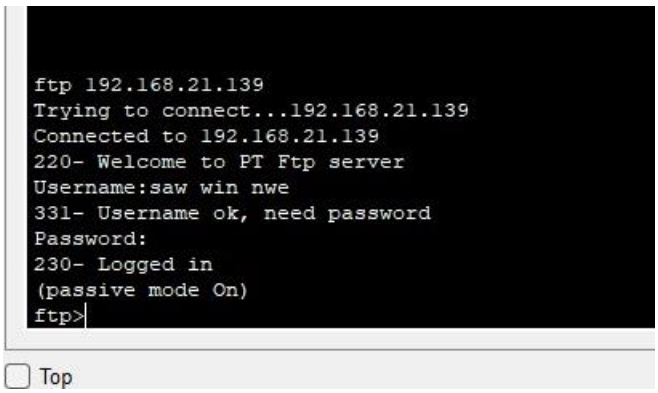
Then we clicked and desktop and go to CMD to check the FTP by typing ftp and server IP address like photo below.



We type the username we created in the above process and the result shown below.



We type password same as username we created from above process and the result shown below.



We type “DIR” to check the FTP and the result shown below.

```
ftp>dir

Listing /ftp directory from 192.168.21.139:
0    : asa842-k8.bin                                5571584
1    : asa923-k8.bin                                30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
3    : c1841-ipbase-mz.123-14.T7.bin                13832032
4    : c1841-ipbasek9-mz.124-12.bin                 16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin       33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
7    : c2600-i-mz.122-28.bin                        5571584
8    : c2600-ipbasek9-mz.124-8.bin                  13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin     50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin      33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin              5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin       33591768
14   : c2950-i6q412-mz.121-22.EA4.bin               3058048
15   : c2950-i6q412-mz.121-22.EA8.bin               3117390
16   : c2960-lanbase-mz.122-25.FX.bin               4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin             4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin             4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin      8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin       10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin         33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin        83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin       505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG          159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG          184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin     160968869
27   : ir800-universalk9-mz.SPA.155-3.M             61750062
28   : ir800-universalk9-mz.SPA.156-3.M             63753767
29   : ir800_yocto-1.7.2.tar                        2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar           6912000
31   : pt1000-i-mz.122-28.bin                       5571584
32   : pt3000-i6q412-mz.121-22.EA4.bin              3117390
ftp>
```

We use file server in this company because as we explain in assignment 1, file server FTP is allowing many files and folders to be transferred. Resuming a transfer after a connection loss ability to add things to a queue for download or upload. enables we to plan transfers. FTP is also better in security and better network and work faster than any other than DNS or web server.

Conclusion

In this assignment 2, we create the design as the company asked, 4 departments 10 computers in each departments, 5 printers, 1 server, 4 switches and 5 routers in total all connected to as statics IP address method and all printers and computers in each department connected to their switch from the department which connected to the router and all these router from all departments connected to the core router which is main router and from any computer in any department can ping any IP address given in each computers. We create the test plan to test and network and as an example, we test the

network from IT department to its own and all the other departments as well. For the maintenance plan, we write down possible issues in page 8 and ask feed back from the employees in the company. Details about our IP address in each computer in each department are shown in above including routers. We also create which services will be better for the company as our suggestion or any different usable devices for company and why should we use it and why should we use VPN and etc. We create the FTP server because we wrote about using FTP server in assignment 1 and according to the assignment 1, we used it as it planned and test it and example will be above and all the references of this assignment 2 will be below.

Reference

https://blog.etech7.com/what-is-a-network-maintenance-plan
https://mglobalservices.com/knowledge-center/blog/what-is-network-maintenance https://www.seaglasstechnology.com/5-types-of-managed-network-services/ https://www.ftptoday.com/blog/why-do-people-still-use-ftp-sites https://openvpn.net/blog/3-reasons-your-business-needs-a-vpn/
https://planetechusa.com/why-use-a-hub/#:~:text=Hub%20Applications&text=To%20monitor%20networks,available%20throughout%20the%
20entire%20network

https://freewimaxinfo.com/network-repeaters.html#:~:text=Repeater%20is%20a%20poyourful%20network,used%20to%20establish%20Ethe rnet%20network.

https://www.paloaltonetworks.com/cyberpedia/what-is-a-business-vpn-understand-its-uses-andlimitations#:~:text=A%20VPN%20makes%20an%20internet,for%20protection%20against%20data%20int erception.
https://supertechman.com.au/server-and-network-maintenance-checklist/
https://www.howtonetwork.org/tshoot/module-1/network-maintenance-tasks/