****

Remote Access Server using VPN

Computer Network Project

Submitted to: Sir Ayoub Kamal

Submitted by:

Abdur Rahman 20191-25972

Muhammad Haris 20191-26204

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **No.** | **Content** | **Page No.** |
| 1 | Acknowledgement | **3** |
| 2 | Abstract | **4** |
| 3 | Introduction | **5** |
| 4 | Components used | **6** |
| 5 | Technology used | **9** |
| 6 | Literature review | **14** |
| 7 | Methodology & Simulation | **17** |
| 7.1 | Campus Admin PC | **18** |
| 7.2 | Computer Lab PC | **20** |
| 7.3 | Server Admin PC | **21** |
| 7.4 | Main Server | **21** |
| 7.5 | Campus Router | **22** |
| 7.6 | Internet Router | **24** |
| 7.7 | Main Router | **26** |
| 7.8 | Main Server Configuration | **28** |
| 11 | Conclusion | **30** |
| 12 | References | **31** |

**Acknowledgement**

We express our sincere regard to Sir Ayoub Kamal for giving us the opportunity to work on this project. The project enhanced our skills in Cisco Packet Tracer and made us knowledgeable about IP (Internet Protocols), VPN (Virtual Private Network) and remotely accessed server systems.

**Abstract**

With the advancement of technology in universities, the demand for remote access to the campus network is becoming increasingly diverse. As a result, creating a secure and efficient network architecture is critical. In this study, we created a VPN access architecture based on a multi-ISP network, along with IPsec VPN technology to incorporate remote access into the solution, based on a multi-campus network environment. Campus network is the basis of daily teaching, scientific research and normal operation of schools. It is of great significance to strengthen the construction of campus network security. We have concentrated our efforts on VPN redundancy design, multi-campus interconnection and access management, and mobile worker remote access. The concept serves as a model for connecting other enterprise VPN networks. We have configured the campus network as such that only the admin PC can establish a successful connection between itself and the server that is located in the main campus. It is a cost-effective way to deploy multiple types of applications, second, it increases protection and security, and third, it can also reduce the network administrators' management of maintaining and managing the network as a whole, even if the two campuses are far away and maintain data transmission efficiency.

**Introduction**

We have combined Internet technologies to create a flexible, modular and easily extensible virtual server environment for both distance and local admin office to use in our networking and system administration classes. By combining the remote access technologies of Remote Desktop, the ability to share sessions of Remote Assistance. While others have been experimenting with different combinations of these technologies, we have aggressively developed and implemented this system, and we believe it has become a critical tool in our ability to provide computing infrastructure for local and distant students, as well as student and faculty research, at a low cost.

This set of measures is a complete list of measures which ensures security of remote connection to a corporate computer network using modern methods of cryptography and network administration technologies. It has been tested on the Cisco Packet Tracer and provides a high level of confidentiality and integrity of remote connection to a corporate computer network.

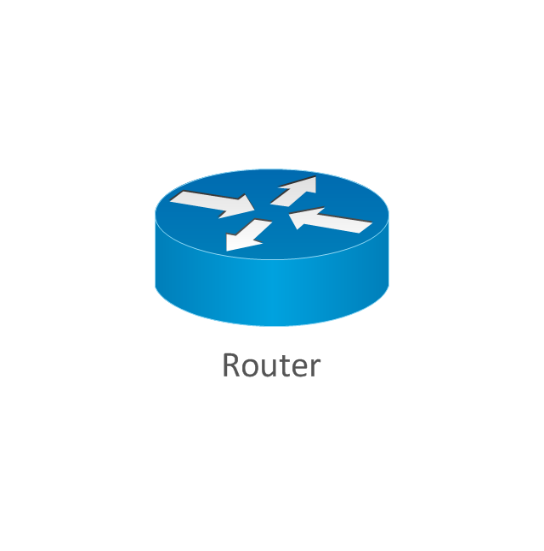
**COMPONENTS USED**

**ROUTER:**

A router is a piece of hardware that connects two or more packet-switched networks or subnetworks together. It has two basic functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing numerous devices to connect to the Internet at the same time.

There are many different types of routers, but the majority of them transfer data between LANs (local area networks) and WANs (wide area networks) (wide area networks). A single router is normally required for a LAN.

A router directs data packets to their destination IP address in the same manner that an air traffic controller guarantees that flights arrive at their destinations without getting lost or experiencing major disruptions along the way.

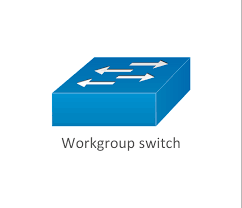


**SWITCH:**

A network switch is a device that connects devices in a network (such as computers, printers, and wireless access points) and allows them to communicate by exchanging data packets. Switches can be both hardware and software-based virtual devices that govern physical networks.

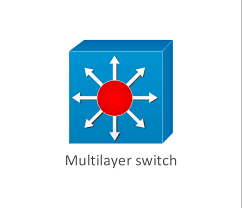
A network switch can be used in a variety of ways:

* Edge switches, also known as access switches, handle traffic entering and exiting the network. Edge switches are used to link devices such as PCs and access points.
* Switches for aggregation or dissemination are located within an optional intermediary layer. These link to edge switches, which can send traffic from switch to switch or up to core switches.
* Core switches: The network's backbone is made up of these switches. User or device edge networks to data centre networks, and enterprise LANs to routers are all connected by core switches, which connect aggregation or edge switches, user or device edge networks to data centre networks, and enterprise LANs to routers.



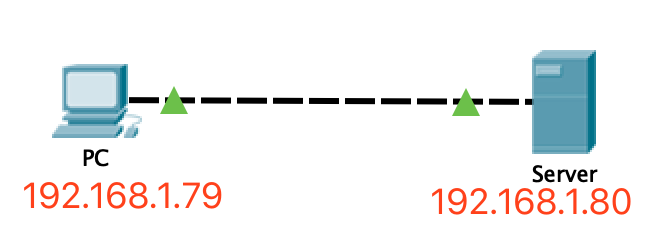
**MULTILAYER SWITCH:**

A multilayer switch, unlike regular switches, may operate at higher layers of the OSI reference model. A multilayer switch can fulfil the functions of both a switch and a router at breakneck rates. A switch inspects frames in the classic sense, whereas a multilayer switch looks deeper into the protocol description unit (at packet or even at segment level). ASIC hardware circuits are used in multilayer switches to accomplish routing functionalities. Typical routers, on the other hand, are based on a microprocessor and perform routing operations using software that run on it.



**SERVER:**

A server is a piece of computer hardware or software (computer programme) that offers functionality to other programmes or devices known as "clients" in the computing world. The client–server model is the name for this architecture. Servers can provide a variety of functions, referred to as "services," such as exchanging data or resources across several clients or executing computation on behalf of a client. Several clients can be served by a single server, while a single client can access multiple servers. A client process can run on the same device or connect to a server on a different device over a network.



**DNS SERVER:**

The Domain Name System (DNS) is the Internet's phone book. DNS is responsible for determining the correct IP address for domain names like 'google.com' or 'nytimes.com' when users type them into web browsers. The addresses are then used by browsers to communicate with origin servers or CDN edge servers in order to retrieve website data. DNS servers, which are dedicated machines that respond DNS queries, are responsible for all of this.

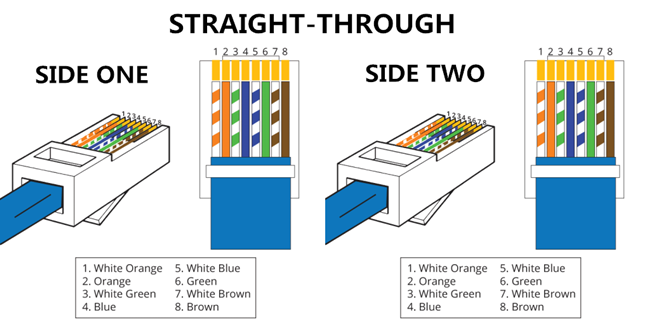
DNS resolution is the process of translating a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). Each device on the Internet is assigned an IP address, which is used to locate the proper Internet device, much way a street address is used to locate a specific residence. When a user requests a webpage, a translation must take place between the user's input (example.com) and the machine-friendly address required to locate the example.com webpage.

It's necessary to learn about the many hardware components that a DNS query must pass through in order to comprehend the DNS resolution process. Apart from the initial request, the DNS lookup occurs "behind the scenes" in the web browser and requires no input from the user's computer. (1)



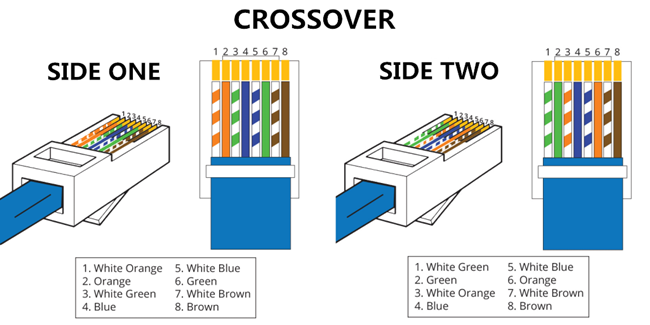
**COPPER STRIAGHT THROUGH CABLE:**

A straight through cable is a form of twisted pair connection that connects a computer to a network hub such as a router in a local area network. This sort of cable, also known as a patch cable, is a wired connection that allows one or more computers to connect to a router through a wireless signal. The wired pins of a straight through cable match. Straight through cable uses a single wiring standard on both ends: T568A or T568B.



**COPPER CROSSOVER CABLE:**

A crossover Ethernet cable is a form of Ethernet connection that is used to directly link computing devices. The RJ45 crossover cable, unlike straight through wire, uses two separate wiring standards: one end uses T568A wiring while the other end uses T568B wiring. The transmit and receive signals are reversed by the internal wiring of Ethernet crossover cables. It's most commonly used to connect two similar devices, such as two computers (through network interface controller) or two switches.



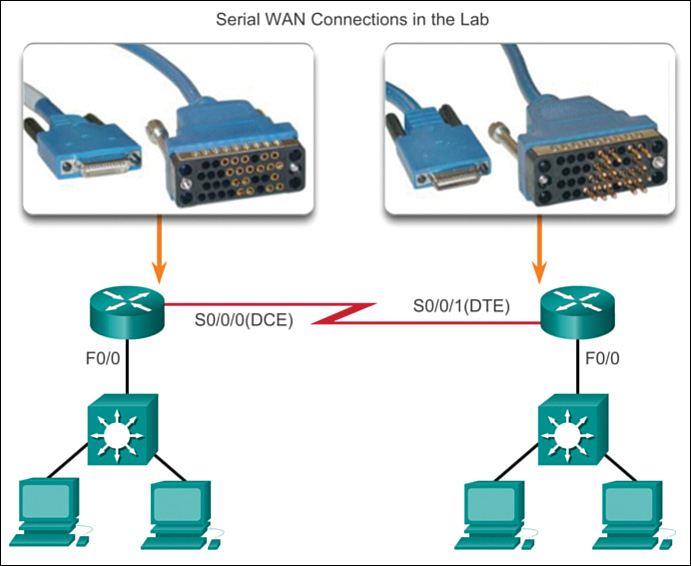
**SERIAL CABLE:**

DCE and DTE are the two types of serial devices that can communicate with each other. DTE stands for *Data Terminal Equipment*, and DCE stands for *Data Communications Equipment*.

DTE is typically either a dumb terminal or the serial port on a computer/workstation.

DCE is typically a modem A DCE is a device that connects to a network physically and forward’s traffic.

A DTE uses a DCE device to connect to a network. Rather than another DTE device, a DTE device is usually connected to a DCE device (or vice versa).



(2)

**Technology used**

**Cisco Packet Tracer:**

Cisco Packet Tracer is a Cisco-developed utility. This tool lets you practise simple and complicated networks using a network simulation. Cisco Packet Tracer's major goal is to help students learn networking principles through hands-on experience while also developing Cisco-specific abilities. This programme cannot replace hardware routers or switches because the protocols are implemented solely in software. Surprisingly, this utility includes not only Cisco hardware, but also a wide range of other networking devices.

**LAN:**

A local area network (LAN) is a computer network that uses access points, cables, routers, and switches to link devices to web servers and internal servers within a single building, campus, or home network, as well as to other LANs via Wide Area Networks (WAN) or Metropolitan Area Networks (MAN). Over a single Internet connection, devices on a LAN, typically personal PCs and workstations, can share files and be accessible by each other.

A router allocates IP addresses to each device on the network and allows all connected devices to share an Internet connection. A network switch connects to the router and allows connected devices to communicate, but it does not manage Local Area Network IP configuration or Internet connection sharing. Switches are excellent tools for expanding the number of LAN ports on a network.

Local Area Networks (LANs) are used to connect computers and offer shared access to printers, files, and other services. Peer-to-peer and client-server architectures are the two types of local area network architecture. Multiple client-devices are connected to a central server on a client-server local area network, which manages application access, device access, file storage, and network traffic.

Database access, document sharing, email, and printing are all provided by applications operating on the Local Area Network server. Without the use of a central server, devices on a peer-to-peer local area network share data directly with a switch or router.

LANs can communicate with one another using leased lines and services, or via virtual, private network technologies over the Internet. A Wide Local Area Network (WLAN) or a Metropolitan Area Network (MAN) is a network of connected LANs. The range of Local Area and Wide Area Networks is different. An Emulated Local Area Network (ELAN) permits the interchange of Ethernet and token ring network data by allowing routing and data bridging over an Asynchronous Transfer Mode (ATM) network. (4)

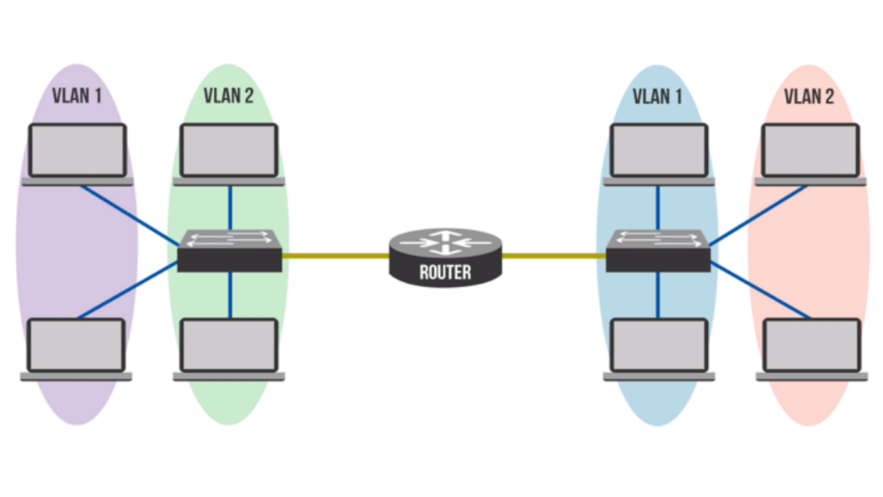
**VLAN:**

A VLAN is a customised network made up of one or more local area networks. It allows a set of devices from different networks to be merged into a single logical network. As a result, a virtual LAN that is managed similarly to a physical LAN emerges. VLAN stands for Virtual Local Area Network in its full form.

In networking, a VLAN is a virtual LAN extension. A local area network (LAN) is a collection of computers and peripheral devices connected in a specific area, such as a school, laboratory, home, or office building. It's a popular network for sharing resources such as files, printers, games, and other software.

The following is a step-by-step explanation of how VLAN works:

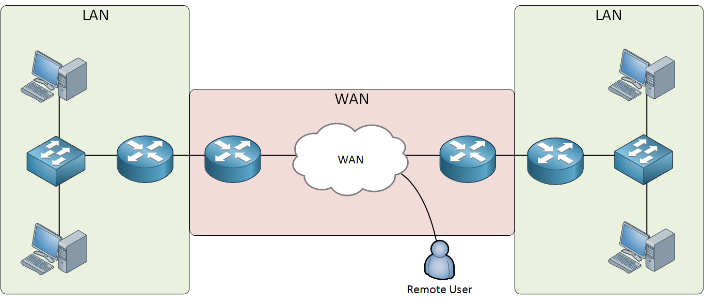
* A number is used to identify VLANs in networking.
* 1-4094 is a valid range. You assign the right VLAN number to ports on a VLAN switch.
* The switch then permits data to be transmitted between ports that are part of the same VLAN.
* There should be a means to transport traffic between two switches because practically all networks are larger than a single switch.
* Assigning a VLAN to a port on each network switch and running a cable between them is one simple and easy approach to do this. (5)



**WAN:**

A WAN is a computer network that connects smaller campus and metropolitan area networks in different locations into a single, distributed network covering a large geographical area using various links such as private lines, Multiprotocol Label Switching (MPLS), virtual private networks (VPNs), wireless (cellular), and the Internet. It doesn't matter if the locations are a few miles away or halfway around the world. A wide area network is used by businesses to connect regional and branch offices, as well as individual distant workers, to centralised resources.

WANs are generally reliant on physical connections provided by telecommunications carriers, whereas LANs are usually managed by an organization's own IT team. The construction of your WAN architecture will be guided by decisions about what kind of connections or communications protocols to utilise and how to install them.



**IP Addressing:**

On a network, IP (Internet Protocol) addresses are used to identify hardware devices. These addresses enable these devices to communicate with one another over a local network or the internet.

Each address consists of a series of integers separated by commas. There are a total of four numbers, each of which can range from 0 to 255. 506.457.14.512 is an example of an IP address.

To identify every computer, router, and website on the internet, we need billions of IP addresses. We will run out of unique addresses at some point, and a new IPv6 protocol has been created to solve this need. (6)

* **DYNAMIC IP ADDRESS:**

The majority of internet users have a dynamic IP address that changes on a regular basis. This is more convenient for internet service providers who must deal with clients joining and leaving the service, as well as address changes.

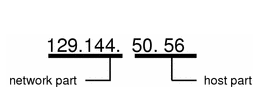
* **STATIC IP ADDRESS:**

The majority of websites use a static IP address that does not change. This is significant because when someone visits your site or sends you an email, the DNS system uses your website's IP address.

**IPV4:**

The IPv4 address is a 32-bit number that identifies a machine's network interface. In most cases, an IPv4 address is represented in decimal digits, with four 8-bit fields separated by periods. Each byte of the IPv4 address is represented by an 8-bit field. The dotted-decimal format is the most common way of encoding the bytes of an IPv4 address.

The network component and the host part of an IPv4 address are further divided into two sections. The components of a typical IPv4 address, 129.144.50.56, are shown in the diagram below.



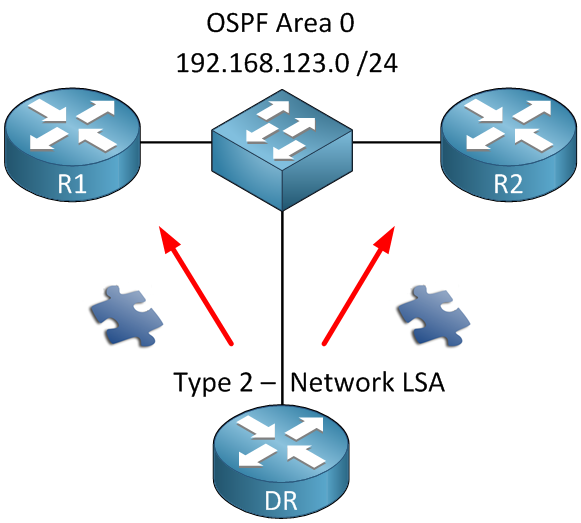
**OSPF:**

OSPF (Open Shortest Path First) is a link-state routing protocol based on the Shortest Path First (SPF) algorithm that was created for IP networks. OSPF stands for Open Shortest Path First (IGP).

In an OSPF network, routers or systems in the same area share the same link-state database, which represents the area's topology. Each router or system in the region creates its own link-state database by combining the link-state advertisements (LSAs) it receives from other routers or systems in the area with the LSAs it generates. An LSA is a packet that includes information about neighbours as well as path costs. The SPF algorithm produces a shortest-path spanning tree with itself as the root based on the link-state information.

The following are the main benefits of OSPF:

* OSPF is more suited to service big, heterogeneous internetworks than distance-vector routing technologies like the Routing Information Protocol (RIP). When the topology of the network changes, OSPF can quickly recalculate the routes.
* To reduce OSPF routing traffic and the size of each area's link-state database, divide an Autonomous System (AS) into areas and maintain area topologies independent using OSPF.
* Equal-cost multipath routing is provided by OSPF. Duplicate routes can be added to the TCP stack with differing next hops. (7)



**VPN:**

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and hide your true identity on the internet. Third parties will have a harder time tracking your online activities and stealing data as a result. Encryption is done in real time.

A VPN connection hides your online data transmission and protects it from prying eyes. Anyone with network access and a desire to see unencrypted data can do so. Hackers and cyber thieves can't decipher this data if you use a VPN.

**Secure encryption:**

An encryption key is required to read the data. In the event of a brute force attack, a computer would take millions of years to decrypt the code without one. Even on public networks, your online activities are masked with the help of a VPN.

**Disguising your whereabouts:**

VPN servers work as proxies for you on the internet. Your exact location cannot be established since the demographic location data comes from a server in another nation. Furthermore, most VPN providers do not keep track of your activity. Some providers, on the other hand, keep track of your actions but do not share them with third parties. This means that any possible record of your user behaviour will be completely erased.

**Access to regional content:**

It is not always possible to access regional web content from anywhere. Content on services and websites is frequently restricted to various regions of the globe. To establish your location, standard connections use local servers in the nation. This means you won't be able to access content from your home while on the road, and you won't be able to access overseas content from your home. With VPN location spoofing, you may practically "alter" your location by switching to a server in another country.

**Secure data transfer:**

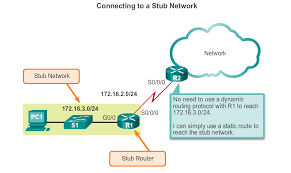
You may need to access important files on your company's network if you operate remotely. This type of information necessitates a secure connection for security reasons. A VPN connection is frequently required to obtain access to the network. To limit the risk of data leakage, VPN services connect to private servers and employ encryption techniques.

**STATIC ROUTING:**

We can communicate with remote networks using static routes. Static routes are typically used in production networks to route traffic from a specific network to a stub network.

Stub networks are networks that can only be accessed from a single location or through a single interface.

The 192.168.1.0/24 and 192.168.4.0/24 networks are stub networks in the situation above. This means that hosts in these network segments only have one route to connect with other hosts, which is R1 for the 192.168.1.0/24 network and R3 for the 192.168.4.0/24 network.

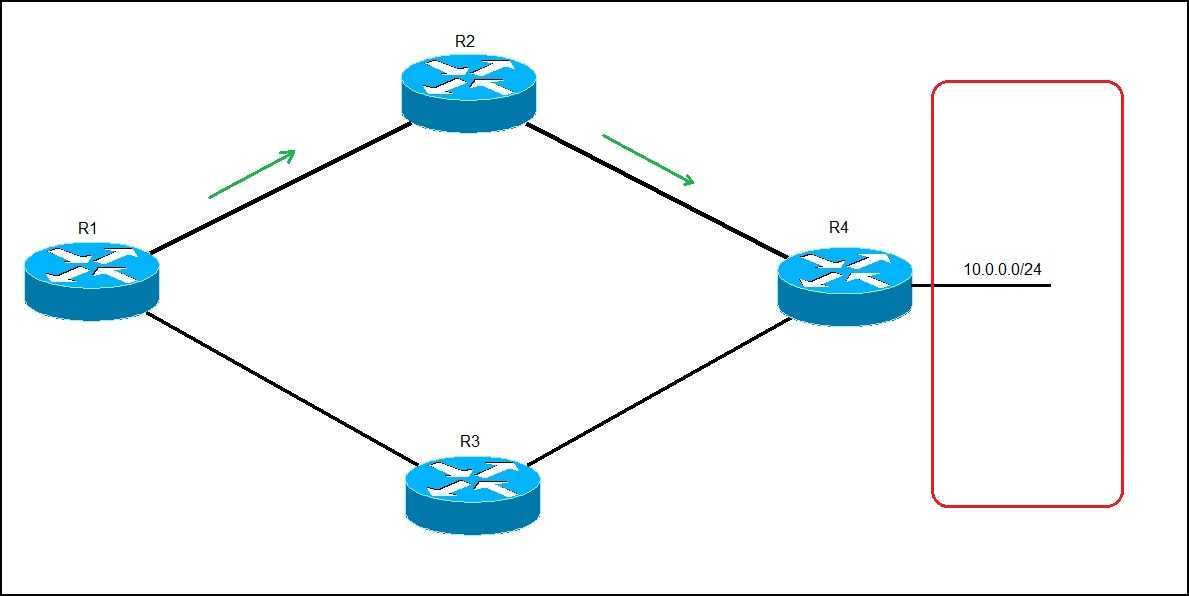


**DYNAMIC ROUTING:**

The routers in dynamic routing display the path between two routers, which can be modified automatically. The paths are updated automatically. There is no need to manually update routing paths if changes occur on the network side; routing paths will be changed automatically. Routing pathways are the connections between routers. When the network changes, it sends messages to a router to notify it of the changes. The router updates the modifications and calculates and updates the routing paths in the database using routing algorithm routes. Because it adopts the route path automatically, dynamic routing is also known as adaptive routing.

Dynamic paths or dynamic routes are the routes or paths on which dynamic routing is accomplished.

in this path; the information responds to network changes in order to dynamically update the changes. It's responsive, which means it adapts to changes in the network. It modifies itself in response to changes in the network. (8)



**Literature review**

**Cisco Packet Tracer:**

Cisco Packet Tracer is a valuable visual simulation programme for networking certifications like the CCNA. Students can use this tool to explore with network behaviour. As a result, they can ask a wide range of questions and investigate many scenarios for better results. Cisco Packet Tracer is a key aspect of the Networking Academy, and it gives students a lot of opportunities to study. It also provides various visualisation, simulation, evaluation, collaboration, and authoring features that make studying and teaching complicated IT concepts a breeze.

Packet Trace is commonly used in the curriculum for courses like as CCNA and CCENT, where faculty use it to demonstrate technical topics and networking systems. Students use this tool to accomplish homework, either alone or in groups.

Engineers prefer to use Cisco Packet Tracer to evaluate protocols before deploying them. Engineers that want to deploy any modification in the production network prefer to utilise Cisco Packet Tracer to test the changes first and then deploy if and only if everything works as planned. (3)

Engineers can use a command line interface and a drag-and-drop user interface to add or remove virtual network devices, making their job easier.

***Characteristics Of Cisco Packet Tracer:***

There are no restrictions on how many devices you can have

* E-learning
* Customize activities for a single or several users.
* Environment that is interactive
* Network Visualization
* Real-time and simulation modes are available.
* Self-paced
* Most networking protocols are supported.
* Language assistance on a global scale
* Compatibility between platforms



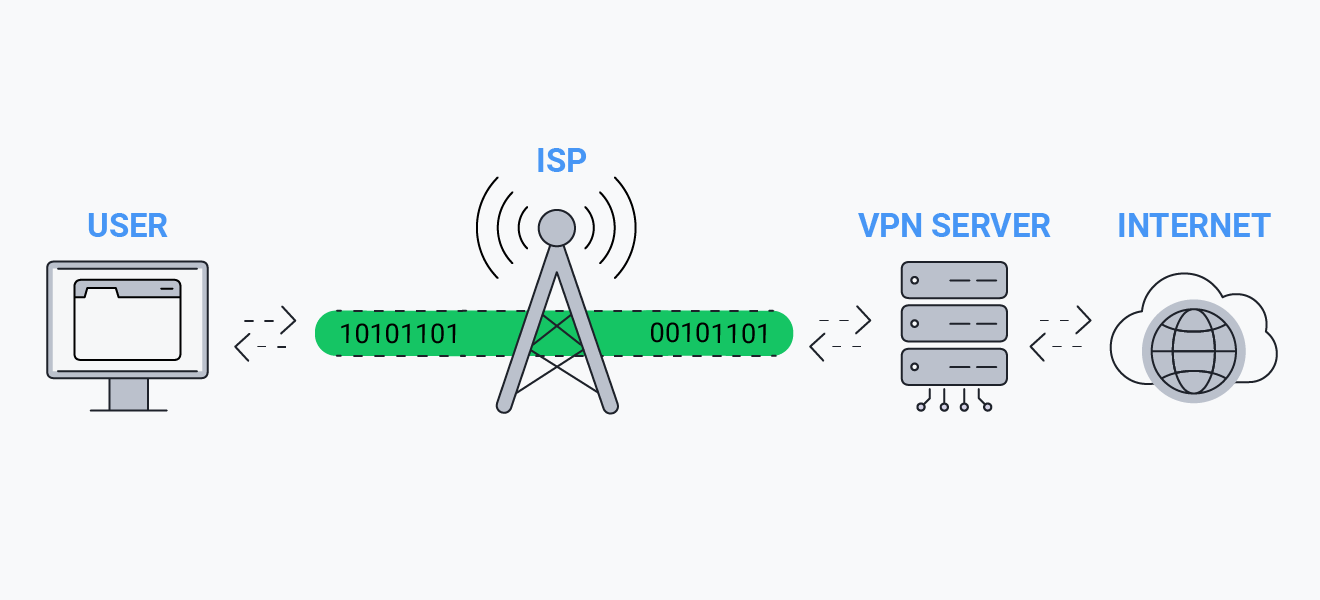
**VPN:**

VPN (Virtual Private Network) is a type of technology that leverages a public network to create a private network that is "in the line." Data is disseminated over the public network via a secure "encrypted tunnel." Building a special communication connection to connect the Internet between two or more enterprises Intranets located in separate sections is the same as constructing a special line. It does not, however, need the construction of a genuine physical line, such as an optical cable. Businesses merely need to hire a local special data line and connect it to the local Internet in order for institutions to communicate with one another.

Through the integrated use of Internet technology, access of interview technology, encryption technology, and certain user management mechanism, the user can make use of the existing public Internet to safely, securely, and undisturbedly interview the remote internal network resources. Compared with the traditional private network, VPN technology greatly reduces the cost. It is convenient, safe, standard, and becomes the main technology in achieving enterprises’ cross-regional secure network interconnection. VPN can be divided into three categories: **(1)** *Internal virtual network (Intranet VPN):* the safe connection between the headquarters and branches; **(2)** *Remote Access to virtual network (Remote Access VPN)*: employees’ remote access to the company network server. Generally, it should have encryption, identity authentication, filtering, and other functions; **(3)** *Enterprises expanding virtual network (Extranet VPN):* providing security for the enterprise's business partners, suppliers and customers, mainly ensuring the data not being modified in the process of transmission and protecting the network resources from external damage.

VPN mainly uses two technologies: tunnel and security. Three protocols are currently supported by tunnel technology: PPTP, L2TP, and IPsec. Tunnel technology's major goal is to complete the secondary encapsulation of IP packets in order to transmit an enterprise's private address over the public Internet. To preserve the privacy and integrity of the data, a safe means of encryption should be used to assure the security of transmission. MPPE, IPsec, and other encryption algorithms are examples of security technology. IPsec is a security protocol that protects IP traffic. In terms of tunnel and encryption technology, IPsec has already established itself as a widely used and open VPN security protocol that ensures TCP/IP protocol and VPN compatibility. IPsec is a set of standard protocols that protects the privacy and integrity of data and supports encryption algorithms such as DES 3 DES. It verifies the integrity of data packet transmission to ensure that the data has not been tampered with. Its purpose is to authenticate the source data.

***ADVANTAGES OF IPSEC VPN:***

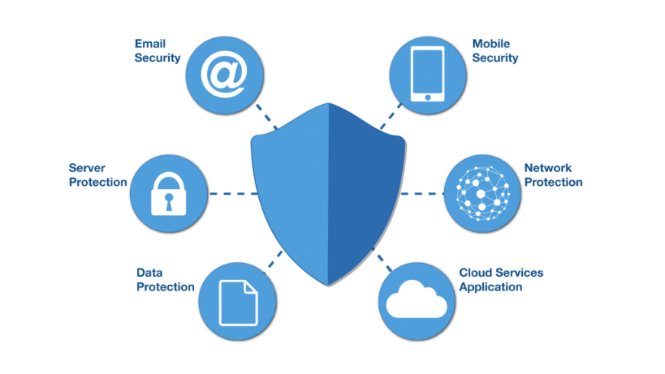
The advantages and applications of IPsec VPN in the workplace network are becoming more apparent. On the IP transmission side, the IPsec VPN technology uses an encrypted tunnel to send information from the internal private network to the public network while still ensuring the security of the internal data, allowing data, voice, and video to travel freely between corporate headquarters and branches. Many businesses now consider VPN to be a primary tool for connecting remote branches and mobile users in order to create a virtual service network. This strategy is being considered by a large number of domestic businesses, and it is even being implemented gradually. The following are some of the benefits of using the Internet to create) your own IPsec VPN. (9

**NETWORK SECURITY:**

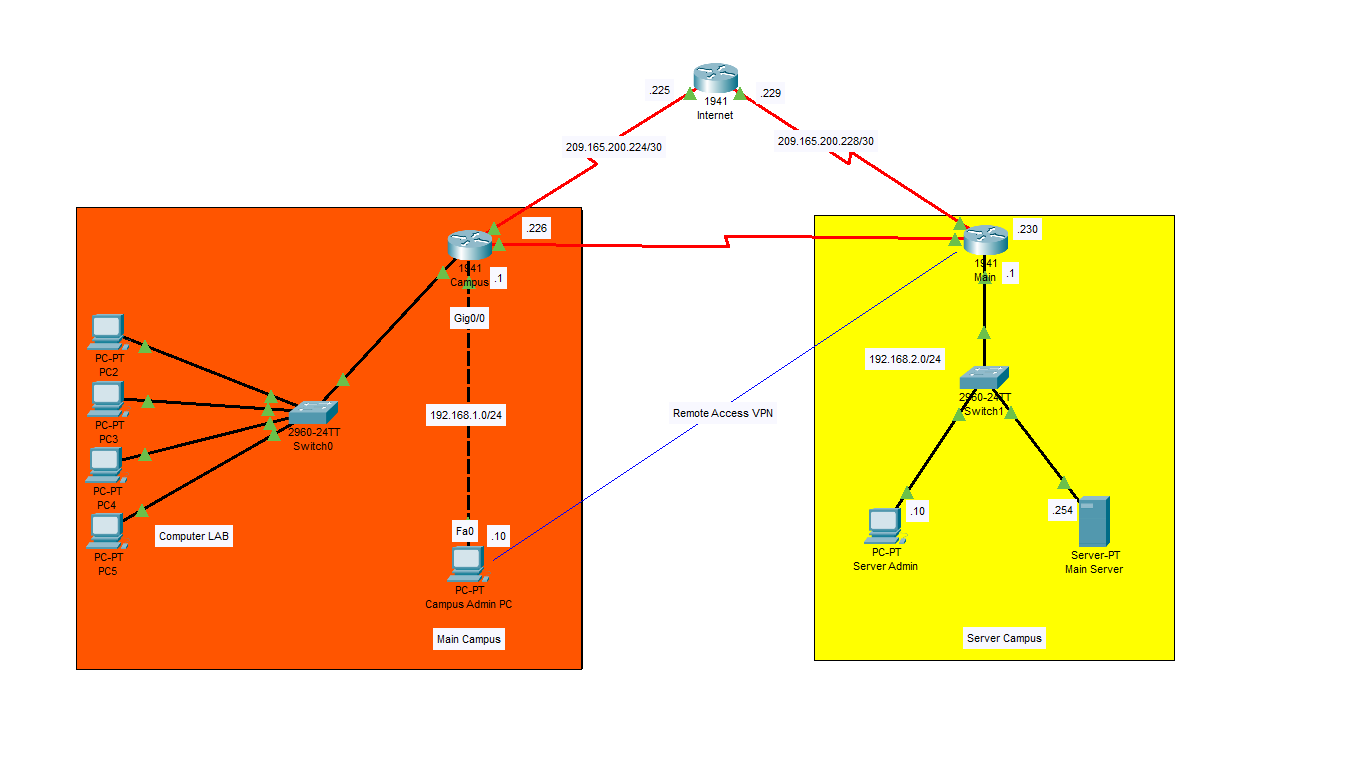
The security of the underlying networking infrastructure against illegal access, misuse, or theft is known as network security. It entails establishing a secure infrastructure that allows devices, applications, users, and applications to operate safely.

Multiple layers of defences at the edge and throughout the network make up network security. Policies and controls are implemented at each network security layer. Access to network resources is granted to authorised users, but bad actors are prevented from carrying out attacks and threats.

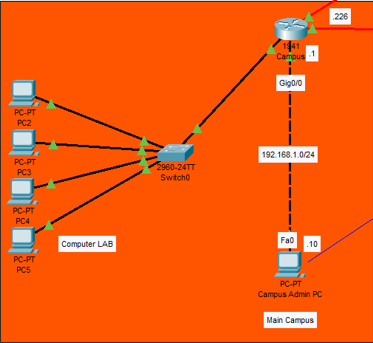
Our world has changed as a result of digitization. Everything about how we live, work, play, and learn has altered. Every company that wants to provide the services that their consumers and workers expect must safeguard their network. Network security also aids in the protection of confidential information. In the end, it safeguards your reputation.



**Methodology & Simulation**

**Architecture:**

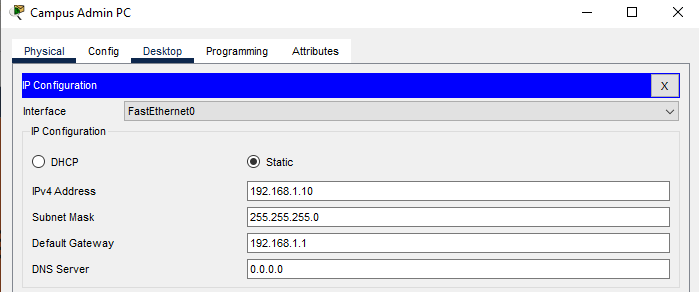
* ***Main Campus:***

****

The main Campus includes 5 PCs in which four of them are setup in LAN and one is PC of the campus Administrator.

The PC of the Campus Admin is secure which is connected directly to the router via a copper-crossover cable.

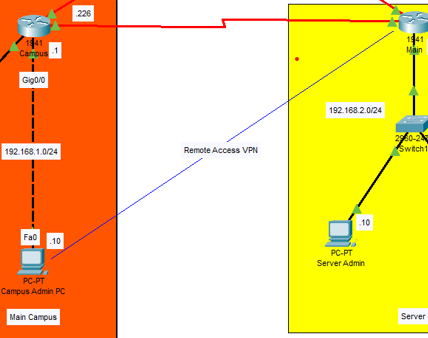
1. **Campus Admin PC:**

****

The Admin PC is assigned IPv4 address: **192.168.1.10**

Along with the Gateway: **192.168.1.1**

The main feature of our Admin PC is our established VPN connection which is accessed remotely via a secure VPN connection with the Main router that is established in the other server campus building.



**VPN:**

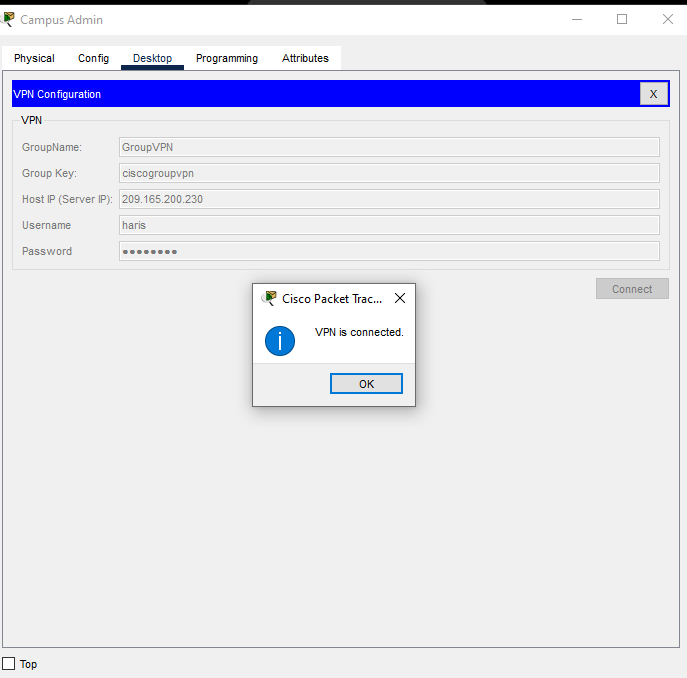
**GroupName:** GroupVPN

**Group Key:** ciscogroupvpn

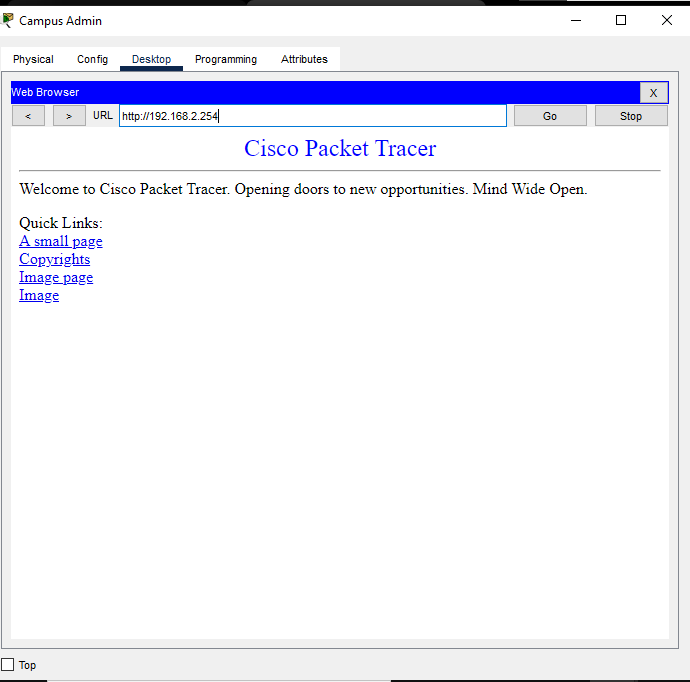
**Host IP (Main Router):** 209.165.200.230

**Username:** haris

**Password:** harisvpn



Through this established VPN connection that was configure in the Main server router, this PC has access to the Server and can ping and even login and browse websites from the server.



* **LAN:**

1. **Computer LAB PCs:**
   1. **PC-2:**

The PC is assigned IPv4 address: **192.168.3.2**

Along with the Gateway: **192.168.1.1**

* 1. **PC-3:**

The PC is assigned IPv4 address: **192.168.3.3**

Along with the Gateway: **192.168.1.1**

* 1. **PC-4:**

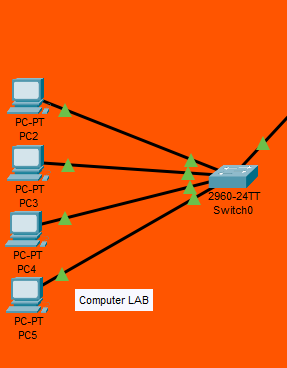
The PC is assigned IPv4 address: **192.168.3.4**

Along with the Gateway: **192.168.1.1**

* 1. **PC-5:**

The PC is assigned IPv4 address: **192.168.3.5**

Along with the Gateway: **192.168.1.1**

****

* ***Server Campus:***

1. **Server Admin PC:**

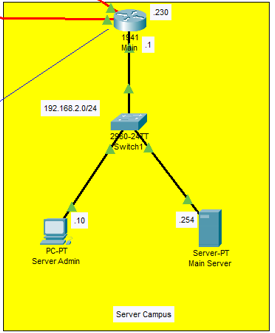
The PC is assigned IPv4 address: **192.168.2.10**

Along with the Gateway: **192.168.2.1**

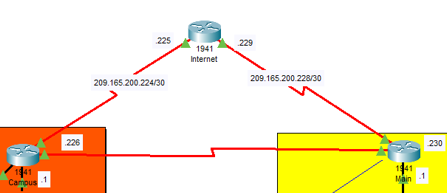
1. **Main Server:**

The PC is assigned IPv4 address: **192.168.2.1**

Along with the Gateway: **192.168.2.254**

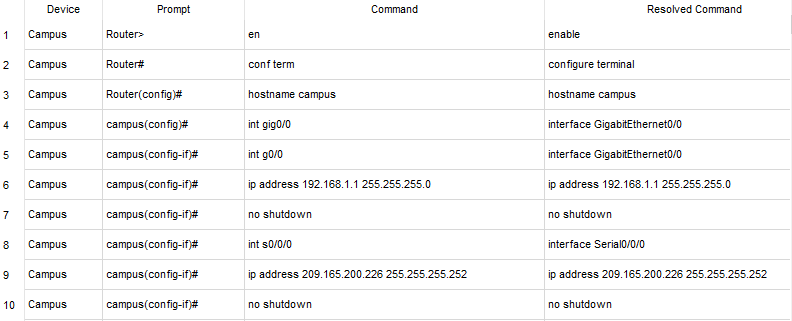
****

* ***Routers:***

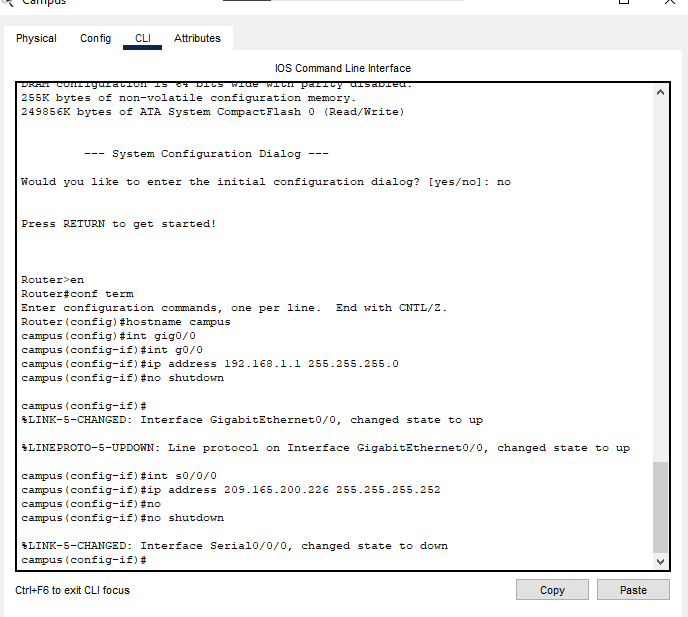
****

1. ***Campus Router:***

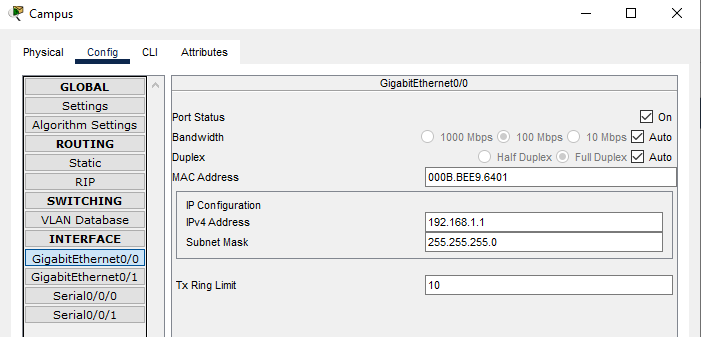
The following CLI commands were given to enable and setup our campus router:

******

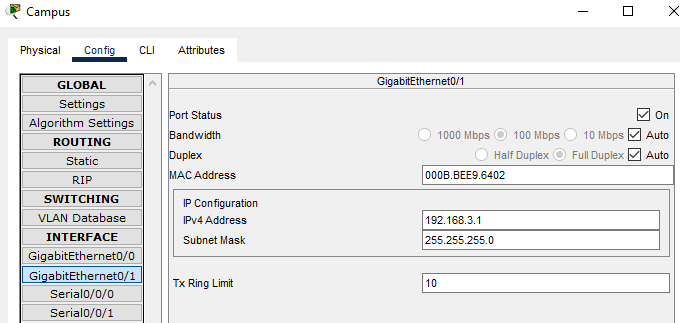
It did the following function:



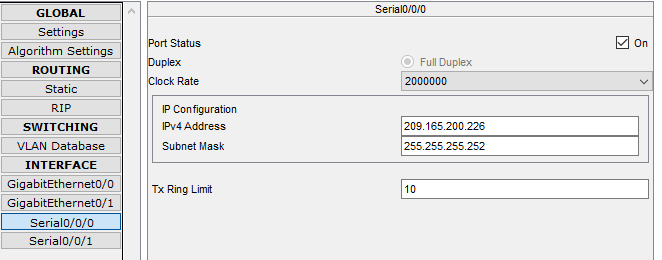
Campus router on g0/0:



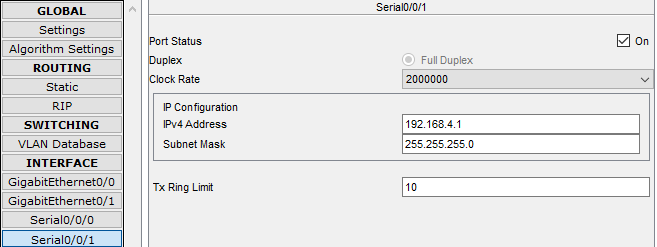
Campus Router on g0/1:



Campus Router on s0/0/0:

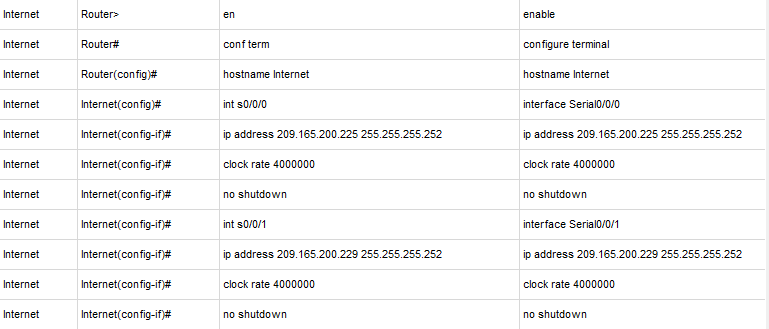


Campus Router on s0/0/1:

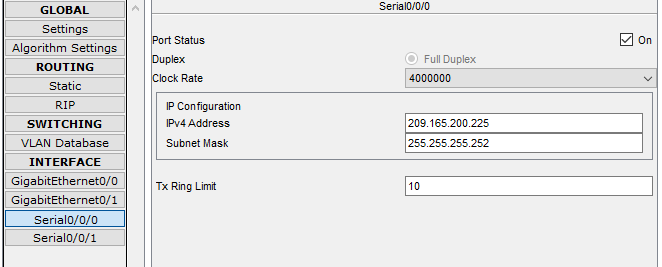


1. ***Internet Router:***

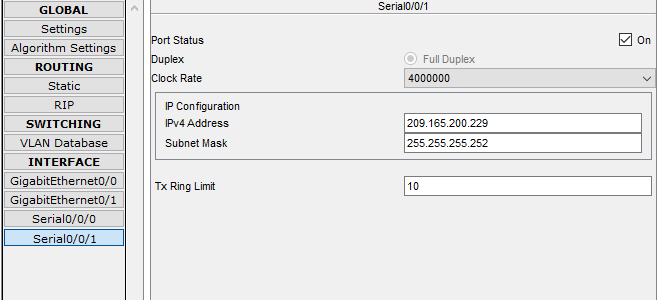
The following CLI commands were given to enable and setup our Internet Router:

******

Internet Router on s0/0/0:



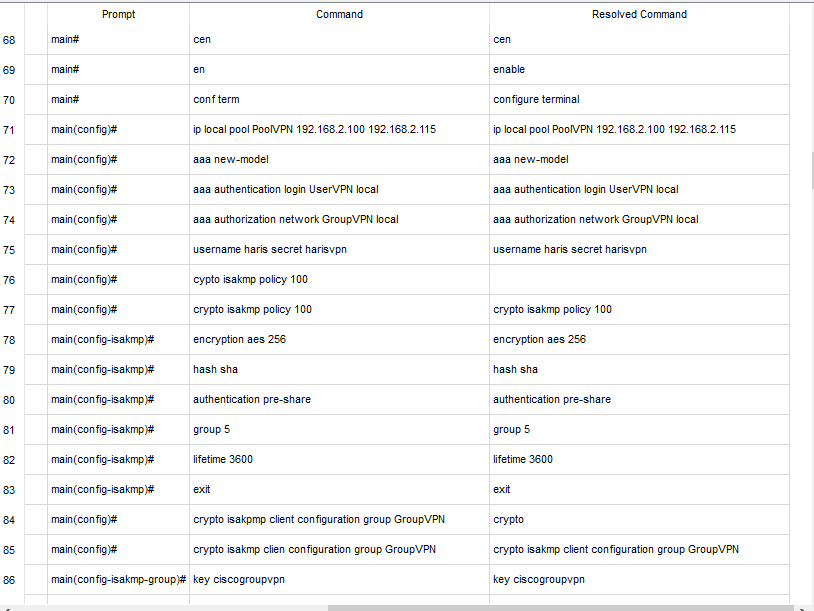
Internet Router on s0/0/1:

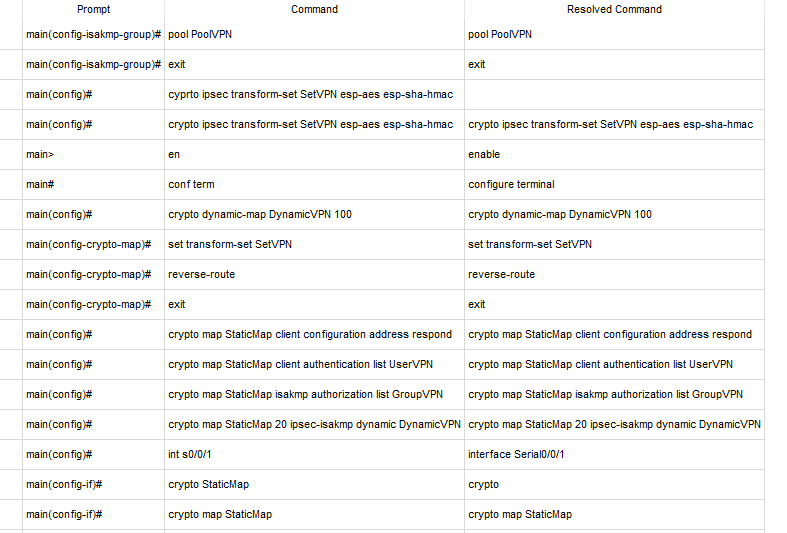


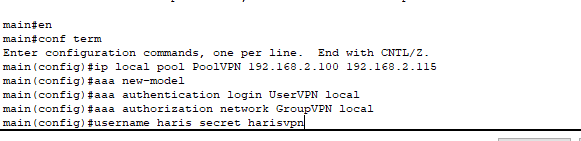
1. ***Main Router:***

This is a very important router configuration because this enabled us to setup our VPN network on this router in order to give remote access to it’s client PC which was the Campus Admin PC

The following commands were fed through CLI:



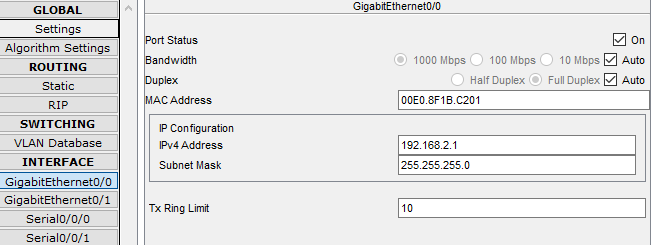
****



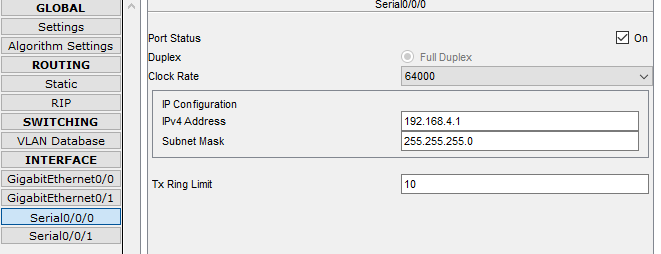
This is where we created a new network group named as GroupVPN.

We authorized the router to establish connection with the username haris and its password as harisvpn so the connection can be secured

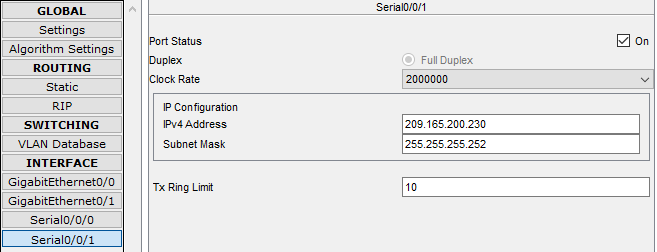
Main Router on g0/0:



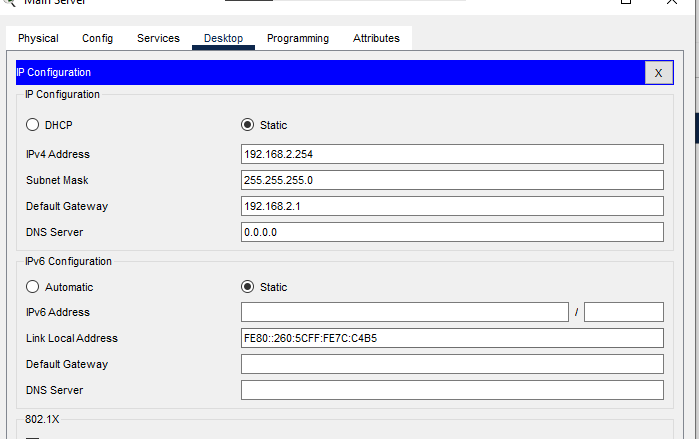
Main Router on s0/0/0:



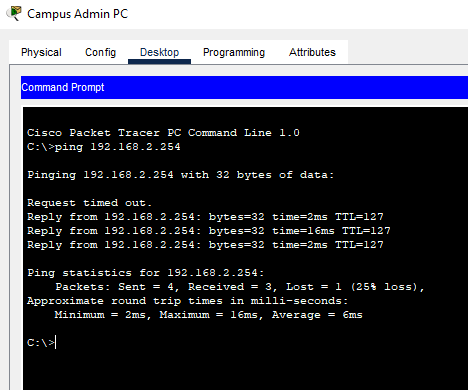
Main Router on s0/0/1:

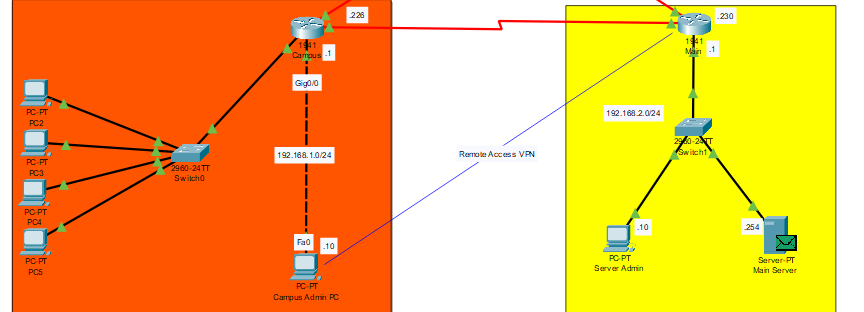
****

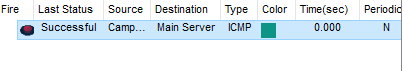
1. **Main Server:**



* **Simulation:**
  + - * + **Campus Admin PC (via VPN) to Main Server:**



****

****

**Conclusion**

To increase the security level in the network’s system especially on campuses, we proposed a secure campus network (SCN) scenario designing and simulating using the cisco packet tracer program. This presents a topology that contains two differently located buildings, with different networks and different types of devices. In each building, we separate the end devices into different LANs for security purposes. We connected a client pc named Admin and gave it administrator rights via creating a new VPN. Also, we applied security techniques for the routers that connect the networks and for switches that connect the end devices with each other to prevent outside or unauthorized accesses. Moreover, it also shows the real weight of some protocols in connecting and securing the entire campus system. It is a cost-effective way to deploy multiple types of applications, second, it increases protection and security, and third, it can also reduce the network administrators' management of maintaining and managing the network as a whole, even if the two campuses are far away and maintain data transmission efficiency.

**References**

(1) <https://f60host.com/support/what-is-dns-how-dns-works/>

(2)<https://www.ciscopress.com/articles/article.asp?p=2202412&seqNum=4>

(3)<https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/>

(4)<https://www.heavy.ai/technical-glossary/local-area-network#:~:text=What%20is%20a%20Local%20Area,Metropolitan%20Area%20Network%20(MAN).>

(5)<https://www.guru99.com/vlan-definition-types-advantages.html#1>

(6)<https://www.wpbeginner.com/glossary/ip-address/>

(7)<https://www.ibm.com/docs/en/i/7.4?topic=routing-open-shortest-path-first#:~:text=Open%20Shortest%20Path%20First%20(OSPF,Interior%20Gateway%20Protocol%20(IGP).>

(8)<https://www.educba.com/static-routing-vs-dynamic-routing/>

(9)[file:///C:/Users/HAJI%20LAPTOP/Downloads/12845.pdf](C://Users/HAJI%20LAPTOP/Downloads/12845.pdf)