Local area network design

Course Project

New Bulgarian University

Subject : Local area network design

Course signature : NETB500

Autumn semester - 2023/2024

Faculty number : F95748

Name: Taner Karaibryam

Project Aim:

The primary aim of this network design project is to create a robust and secure laboratory environment for conducting classes on OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol). The design should cater to the networking needs of three classrooms located in different buildings on the same campus. The network should support both local and remote connectivity for students, ensuring effective communication, collaboration, and practical learning experiences. The network should also incorporate security measures and best practices for device management and monitoring.

1.Topology

Star Network Topology

Star topology is a kind of network topology in which every networking device is connected to one router/switch or a hub.

In a topology, the central hub acts sort of a server and also the connecting nodes act like clients. Once the central node receives a packet from a connecting node, it will pass the packet on to different nodes within the network. A star topology is additionally called a star network.

Star networks need a point-to-point affiliation between the central node and connecting devices. To improve communication between the devices on the network, the central node will offer signal reconditioning and amplification services.

Star topologies are usually utilized in home networks. the advantages of a star configuration embody the following:

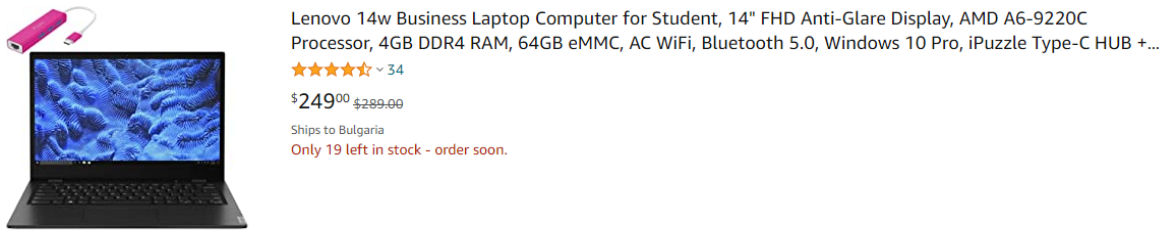
Limits the impact of one point of failure. In star networks, every connecting node is isolated from different connecting nodes. If one connecting node goes down, it'll not impact the performance of other connecting nodes within the network.

Facilitates adding or removing individual parts to and from a network. Star networks are typically kept small as a result of network performance will suffer once too much devices contend for access to the central node.

2. Necessary hardware and software

Before anything else I start with the PC’s, we would buy 15 pieces of those and they have almost all the peripherals built in like camera, monitor, speakers, webcam and keyboard but for this classroom to be efficient for a lot of different workloads I would add to every pc a headset with microphone and a mouse.

In this part my choices are based on budget but good quality things.



Lenovo 14w Business Laptop Computer for Student, 14" FHD Anti-Glare Display, AMD A6-9220C Processor, 4GB DDR4 RAM, 64GB eMMC, AC WiFi, Bluetooth 5.0, Windows 10 Pro, iPuzzle Type-C HUB +...

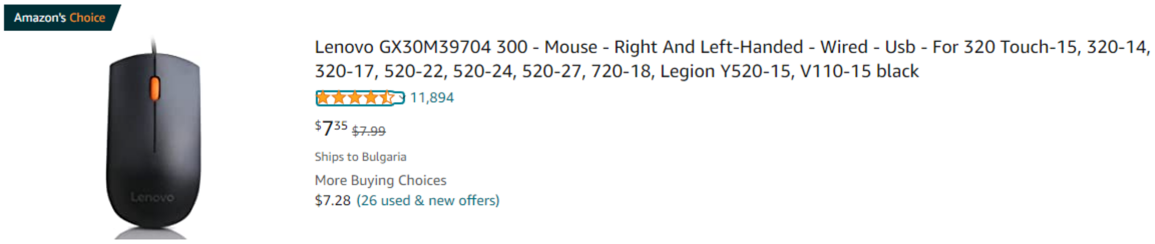
★★★★☆ 34

$^{\$}249^{00}$ ~~$289.00~~

Ships to Bulgaria

Only 19 left in stock - order soon.

249 x 15 = 3735$



Amazon's Choice

Lenovo GX30M39704 300 - Mouse - Right And Left-Handed - Wired - Usb - For 320 Touch-15, 320-14, 320-17, 520-22, 520-24, 520-27, 720-18, Legion Y520-15, V110-15 black

★★★★☆ 11,894

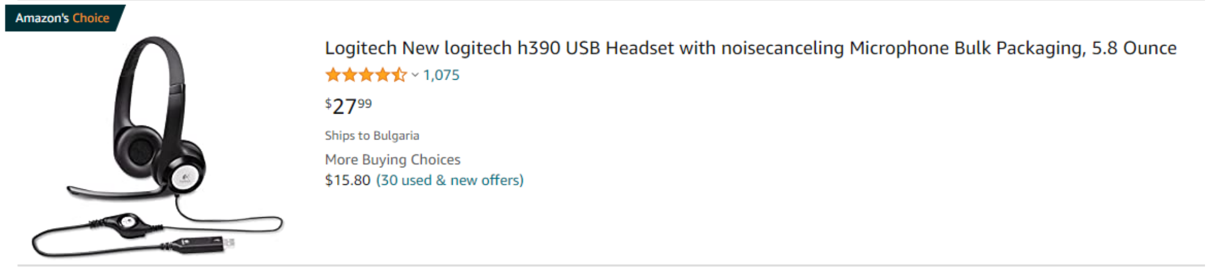
$^{\$}7^{35}$ ~~$7.99~~

Ships to Bulgaria

More Buying Choices

$7.28 (26 used & new offers)

7.35 x 15 = 110.25$



Amazon's Choice

Logitech New logitech h390 USB Headset with noisecanceling Microphone Bulk Packaging, 5.8 Ounce

★★★★☆ 1,075

$^{\$}27^{99}$

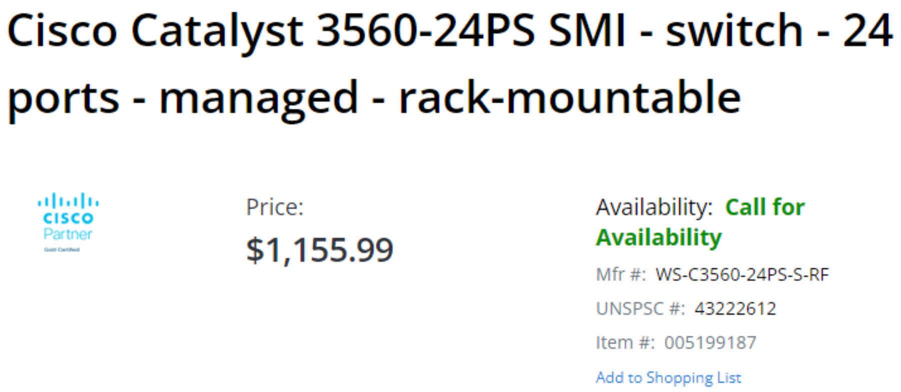
Ships to Bulgaria

More Buying Choices

$15.80 (30 used & new offers)

27 x 15 = 405$

The whole cost of the peripherals,computers and all the operating systems (already in the PC`s with licences) is 4250$ which is good for up to 15 PCs (some computers will be used remotely from the students) computer room.



Cisco Catalyst 3560-24PS SMI - switch - 24 ports - managed - rack-mountable

Price:

$1,155.99

Availability: Call for Availability

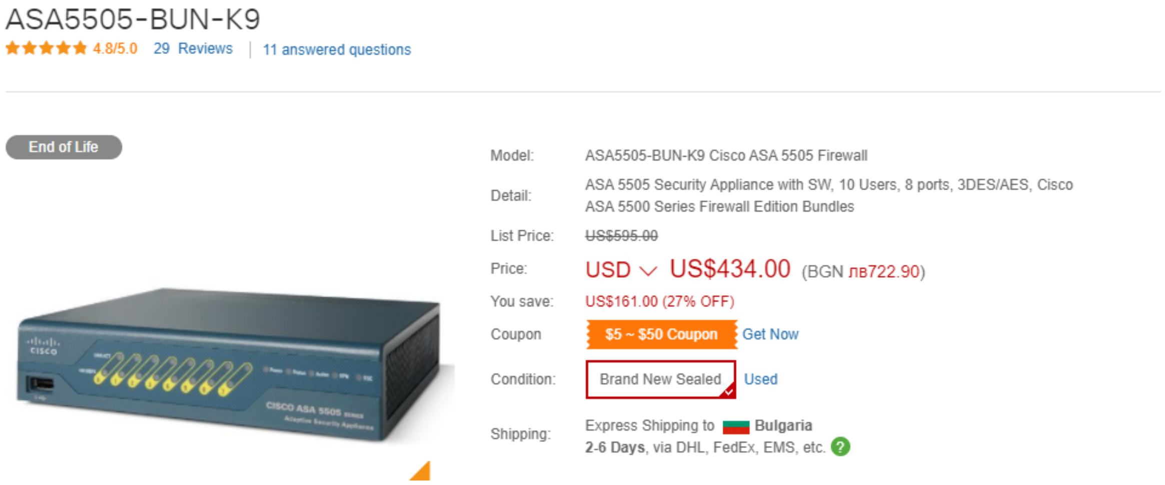
Mfr #: WS-C3560-24PS-S-RF

UNSPSC #: 43222612

Item #: 005199187

Add to Shopping List

And This is the price for a Catalyst 3560-24ps SMI switch.



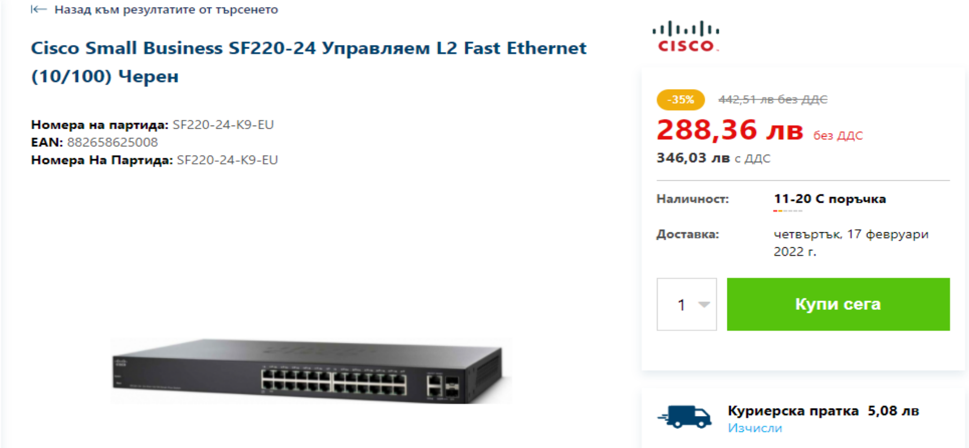
ASA5505-BUN-K9

★★★★★ 4.8/5.0 29 Reviews | 11 answered questions

End of Life

Model:	ASA5505-BUN-K9 Cisco ASA 5505 Firewall
Detail:	ASA 5505 Security Appliance with SW, 10 Users, 8 ports, 3DES/AES, Cisco ASA 5500 Series Firewall Edition Bundles
List Price:	~~US$595.00~~
Price:	USD US$434.00 (BGN лв722.90)
You save:	US$161.00 (27% OFF)
Coupon	$5 ~ $50 Coupon Get Now
Condition:	Brand New Sealed Used
Shipping:	Express Shipping to Bulgaria 2-6 Days, via DHL, FedEx, EMS, etc.

For the firewall we will use a standard 150 mbps firewall and for the price to performance ratio is very good.



Назад към резултатите от търсенето

Cisco Small Business SF220-24 Управляем L2 Fast Ethernet (10/100) Черен

Номера на партида: SF220-24-K9-EU
EAN: 882658625008
Номера На Партида: SF220-24-K9-EU

-35% ~~442,51 лв без ДДС~~

288,36 лв без ДДС

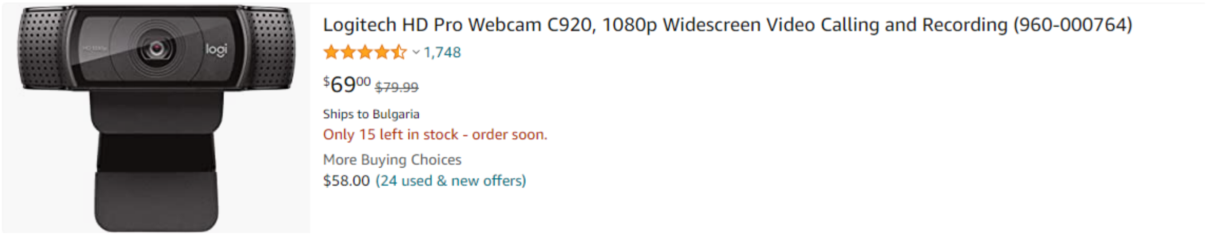
346,03 лв с ДДС

Наличност:	11-20 С поръчка
Доставка:	четвъртък, 17 февруари 2022 г.

1 Купи сега

Куриерска пратка 5,08 лв
Изчисли

We would need 4 of the **Cisco Small Business SF220-24** switch so we could connect all of our devices and have some room for experimentation and expansion.



Logitech HD Pro Webcam C920, 1080p Widescreen Video Calling and Recording (960-000764)

★★★★☆ 1,748

$69.00 ~~$79.99~~

Ships to Bulgaria
Only 15 left in stock - order soon.

More Buying Choices
$58.00 (24 used & new offers)

We would need 3 of those cameras so the lessons could be streamed and recorded for easier access by the students.

Remote connection

VPN

“Virtual private network **(VPN)** The process of securing communication between two devices whose packets pass over some public and unsecured network, typically the Internet. VPNs encrypt packets so that the communication is private, and authenticate the identity of the endpoints.” (Odom, 2019 p.756)

It`s gonna be used in the classroom so the lectures could be secure and all connection in and out of the network encrypted

Out of band configuration

RDP

We are gonna use RDP for the connection of the tutors to the student`s machines. Every PC, Linux machine or mac OS X machine would be set up so it can use RDP for remote control from the tutor. **Remote Desktop Protocol** (**RDP**) is a protocol developed by Microsoft in the beginning for Windows machines which provides a user with a GUI to connect with other computers over the network .The user would use RDP client software for this purpose, while the other computer will run RDP software for servers. Clients exist for most versions of Microsoft Windows (including Windows Mobile), Linux, Unix, macOS, iOS, Android, and other operating systems. RDP servers are built in almost all versions of the Windows operating systems; an RDP server for Linux/Unix and OS X also exists. In default settings, the server listens on TCP port 3389 and UDP port 3389.

SSH

For our purposes SSH would be used from the remote users and also, by students that are learning the basics of networking technologies and are gonna use for educational and practical purposes.

SSH was designed on unix-like OS`s as a replacement for Telnet and for unsecured remote Unix shell protocols, like the Berkeley Remote Shell (rsh) and therefore the connected rlogin and rexec protocols, that all use insecure, plaintext transmission of authentication tokens.

The Secure Shell Protocol (SSH) may be a cryptographic network protocol for operating network services firmly over Associate in Nursing unsecured network. Its most notable applications are remote login and command-line execution.

SSH applications are supported a client–server architecture, connecting an SSH client instance with an SSH server SSH operates as a superimposed protocol suite comprising 3 principal hierarchical components: the transport layer provides server authentication, confidentiality, and integrity; the user authentication protocol validates the user to the server; and also the affiliation protocol multiplexes the encrypted tunnel into multiple logical communication channels.

SSH was first designed in 1995 through Finnish computer scientist Tatu Ylönen. Subsequent improvement of the protocol suite proceeded in numerous developer groups, generating numerous versions of the implementation. The protocol specification distinguishes important versions, called SSH-1 and SSH-2. The maximum normally carried out software program tune is OpenSSH, launched in 1999 as open-supply software program through the OpenBSD developers.

Configuration

These are the configuration detail for all the network devices plus the routing table.

VPN credentials

groupname - VPNgroup

groupkey vpnciscogroup

host IP 211.1.3.2 or 211.1.4.1

VPNuser

Vpnpassword

Routing table

multilayer switch

Vlan 1 192.168.40.1

Vlan 15 – 192.168.10.1

Vlan 25 – 192.168.11.1

Vlan 35 192.168.12.1

Vlan 45 192.168.13.1

Class 1 192.168.10.0 /24

Vlan 15

Computer 1-15 – 192.168.10.2 – 16

Switch 1 – vlan 15 – 192.168.10.25

Class 2 192.168.11.0/24

Computer 1-15 – 192.168.11.2-16

Switch 2 vlan 25 – 182.168.11.25

Gig 0/1 211.1.1.6 /24

Serial 0/1/1 211.1.4.1 /24

Class 3 192.168.12.0/24

Computer 1-15 – 192.168.12.2-16

Switch 3 vlan 25 – 182.168.12.25

IT management 192.168.13.0/24

Computer 1-15 – 192.168.13.2-16

Switch 4 vlan 25 – 182.168.13.25

Firewall

Inside configuration – vlan 1 – IP 192.168.40.2 /24

Outside configuration – vlan 2 211.1.1.1 /24

Cluster routers –

Router 0 – gig0/0 211.1.1.2

Gig0/1 10.1.1.1 / 24

Serial 0/1/0 211.1.3.2

Router 1

Gig 0/1 211.1.1.6 /24

Serial 0/1/1 211.1.4.1 /24

Gig0/0 10.1.1.2 / 24

Home PC – 192.168.1.2 / 24

Router connected to the Home PC gig0/0 192.168.1.1 /24

Serial 0/1/0 211.1.2.2 /24

ISP/Internet router

Seiral 0/1/0 211.1.2.1 /24

Serial 0/1/1 211.1.3.4 / 24

Here we've got the four distinct rooms linked to a switch for every room , a firewall which we can use to permit or deny any incoming or outgoing traffic and if want be to disclaim traffic to precise hosts/community If you've got got a dozen VLANs on a specific transfer, you don’t want extra cables or switches for every

A multi layer switch so as to act as a router as well that each one of the switches could be linked to it due to the fact it'll be additionally the default gateway for the four distinct rooms , and also a router a good way to be outside of the firewall in order that we are able to reach to the internet,

So first for configuration we can move over to the multi layer transfer , to configure it we are able to use a console cable from the IT control computer systems to configure it remotely and effectively even in case a ISP fault happens .

First we can add four vlans , one vlan for every room and a 5th vlan that will be the default vlan for the multilayer switch could be for the community among the multilayer switch and the firewall

To configure the vlan first we create them , to add the vlans we want to be in configuration terminal mode , to achieve this we want to apply the commands enable and afterwards use the command "configure terminal" afterwards as soon as we're in 'config term" mode we upload the vlans the usage of the command: vlan “number” as an example vlan 10 , vlan 20 ect. Can wager among 1-100

Once we've brought the vlans we then apply IP addresses due to the fact we're gonna use the multilayer switch as a router and a switch at the same time the IP’s could be default gateways for every network to accomplish that we first want to be at the interface vlan that we plan to assign the IP to , to do use we use the command” interface vlan “10 ”because of this that we're presently configuring vlan 10, then use the command: IP cope with “IP cope with” “subnet mask” to assign the IP to the vlan we're presently configuring. Once all of the vlans have their IP cope with configured we need to configure the trunks for the interfaces which can be going out of the multilayer switch , the motive behond why we need to achieve this is due to the fact a trunk port can transmit information for a couple of VLANS.

Since we've got a couple of VLANs on a specific transfer, we don’t want extra cables or switches for every VLAN—just a single link. A trunk port lets us in to ship all the ones signals for every switch or router through a single trunk link. In comparison to an access port, a trunk port should use tagging with a view to allow indicators to get to the right endpoint. Trunk ports normally provide better bandwidth and decrease latency than access ports.

To do thus we want to be inside the interfaces that our going out of the multilayer switch , 1st we wish to enter in the interfaces to set up them , to try {and do} so we tend to use an equivalent command accustomed configure every vlan , simply rather than the vlan we are going to use the interface name for instance – interface or int “interface name”.

Then we use the subsequent commands: switchport trunk encapsulation dot1q , that sets the encapsulation mode of the trunk interface to the business customary 802.1Q. 802.1Q is the networking standard that defines VLANS on an LAN network.

Then we tend to use the command: switchport mode trunk to inform the interface that it'll be in trunk mode.

We are going to do therefore for every outgoing interface for the multilayer switch , we will additionally need to permit vlans – the command is : switchport trunk allowed vlan 1-50 , the rationale why we do it's as a result of The switchport trunk allowed vlan command is employed to specify the list of VLANs that are allowed on a trunk port. once a Layer two interface on a Cisco IOS device is organized to control in trunk mode, the default setting is for the interface to hold all of the VLANs outlined on the switch.

Additionally since the multilayer switch will be a layer three switch {we need|we'd like|we need} to modify the routing , to try and do so we tend to simply merely use the command : ip routing ,again we save configuration with privileged exec mode to the wr command.

Here we just want to permit these specific vlans , this configuration should be in serious trouble every outgoing interface , here we are through with the multilayer switch configuration , to save lots of the configuration we need to be in

Privileged executive department mode and use the command:wr.

Finally we are going to use the ip route on the multilayer switch to route to Traffic towards the firewall which is able to forward to the surface network, to try and do therefore we tend to use the command:

ip route 0.0.0.0 0.0.0.0 “IP address” the ip address is that the interface connects to the firewall

Currently we pass on to the computers to quickly set up each network for every area , since we've got in total forty eight devices , fifteen for each room them three for the IT management room , we will configure the IP’s for every host statically, to try and do therefore we simply merely visit ip configuration and add the

IP’s for the hosts , all masks are gonna be a 24 bit mask, the default gateway is that the 1st usable IP address in each network , the DNS server is the traditional 8.8.8.8 Google dns and that we just have to be compelled to confirm that the interfaces that may be used for all devices are on.

Once the configuration is completed for every end point , we will begin with the switches 1st we have a tendency to quickly substitute the names of the switches to have a a lot more easier time , class one switch are going to be named: class1-switch and also the same for the opposite switches then for all switches we enable passwords using the command: **enable password “password”** for further security. currently we add the vlans that we've got created at the multilayer switch then the interface that's connected to the multilayer switch will be used as a trunk, whereas the interfaces connected to the hosts are going to be used as an access mode , the distinction between access and trunk is that an access port may be a affiliation on a switch that transmits packets to and from a particular VLAN. as the result of an access port is simply assigned to one VLAN, it sends and receives frames that aren’t labeled and only have the access VLAN value. This won't cause signal problems because the frames stay among the same VLAN. If it does happen to receive a tagged packet, it'll simply avoid it. This is often an easier configuration, however not the foremost economical selection if the network is even moderately complex. therefore the interfaces for the hosts are going to be assigned to vlan fifteen , to try and do so we'd like to be in config t mode and enter into the interface that we tend to want to put together , the commands are as follows:

Int “**interface name**” – **switchport mode access** – **switchport access vlan 15** since classroom 1 will use vlan 15 we assigned vlan 15 for the interfaces. To save configuration we go into privileged EXEC mode and use the command: **wr**.

Before we're completed we want to feature an ip address for the vlans within switches we've simply added , to achieve this we simply input the vlan that's linked to the multilayer switch , we simply want to feature an IP that we aren't using for the switch and is a part of the vlan we determined to feature for the network.

To achieve this we simply input the interface of the vlan and from there we use the subsequent command to assign an IP: ip address “IP address “subnet mask” to keep the configuration whilst in config t mode we will use the command do copy run start. Once we've configured the transfer we're accomplished and we will go directly to the firewall.

Since the firewall vlan 1 is already preconfigured with an IP address we want to remove it in order to apply our own address , to do so we simply use the following command no dhcp address “IP addresses” inside .

Now we add an ip address to the inside firewall network , the ip that the network will be connected to the vlan 1 of the multilayer switch , first we will configure vlan 1 which is in the inside network ,to start with we go into interface vlan 1 or int vlan 1 then we add an IP address by doing the following command: ip address “IP address” “subnet mask” , name the inside network for example: name if “name” we will use the name – inside , then we set the security level as the highest one, since this is our inside network and we have full control over it and it is our most trusted network we will set the security for the maximum possible by inputting the following command: security-level 100

Then we exit and start configuring the vlan two for the outside network , we do it the it the same way we did with the inside network but here the IP will be for the outside that is connected to the router and also the security level will be zero – since it`s the outside network and the only control we have is what traffic is allowed or denied this is the most untrusted part of our network which will be at the lowest security level.

And again we make sure that the interface connected to the router is accessing the vlan for the outside network in our case it`s vlan two.

Now we want to forward the traffic onwards the router on the outside network to do so want to do the following command: route outside 0.0.0.0 0.0.0.0 “IP address” in our case it is 211.1.1.2 . 211.1.1.6 which will change our gateway of last resort to our assigned ip and network of 0.0.0.0 which means any network of any mask .

Now we will make a NAT so that when a packet comes from the inside network it will go to the outside and the mac address of the outside interface/global interface will be used which then will go back to the source IP that has requested the data to do we use the following commands:

We enter **config t mode – object network “name”**

Then we enter the network – subnet “network address” subnet mask” – nat(inside, outside) dynamic interface , now every ip in the network we have that wants to go out in the internet will have it’s private ip switched with the outside interface IP address , we do the same command for ever other network we have in our topology , the firewall asa will make a note of what PC is going out and will remember which so that it will be able to route back the traffic to the correct source that has requested it.

Now we end the configuration with the simple command: end

Now we can quick upload an access-list to accomplish that we go into config t mode after which use the following command: access-list in_to_internet extended permit tcp any any to allow all then access-listing in_to_internet prolonged allow icmp any any , now we upload the command: access-group in_to_internet in interface outside

For the router we want to configure the IP in order to be used for the outdoor network

To accomplish that we can use the subsequent commands: int “interface name” – the interface linked to the firewall then we upload an ip address by doing the subsequent : ip address “ip address” “ subnet mask”

And then save by doing : no shut

We have additionally delivered the ip routing to the router with a view to path lower back the visitors to the networks from which it got here from. The command is – in config it – ip path “community deal with” “subnetmask “ interface linked to the community of the router on the opposite device” – static routes

Also to permit remote connectivity we can need to configure a vpn on the main router and additionally at the cluster router that we've delivered as the main motive of cluster is toimprove overall performance and availability over that of a single computer

First we can want every other identical type of router for the cluster in our case it is the router 1941 then we upload the identical configuration this is determined on the principle router however right here as well we can need another community for the 2 routers. So in our case the IP 10.1.1.1 and 10.1.1.2 255.255.255. /24 is delivered

Between the 2.(in cisco packet tracer you pick out the 2 routers and at the top proper there may be an choice to press cluster)

Now we want to create vpn for our user’s at home so one can be linked remotely.(the identical settings can be implemented to the cluster router)

Here we determined to create a short vpn for class 1 now we pass back to the main router this is connected to all networks in our topology , First we will need to acquire the security characteristic license with a view to begin configuring ipsec vpn , to accomplish that we need to enter config mode and input the subsequent command:

license boot module c1900 technology-package securityk9 as soon as this is input we can be prompt to either input yes or no , we input yes to simply accept in any other case we can now no longer be able to configure the ipsec VPN, Now we quickly save the config with the command: copy running-config startup-config.

Then we reload to use the license that we've got we`ve have just added added. Now its time to configure the VPN phase 1

First we upload the local ip pool name and ip addresses so that it will be used for the VPN.

To achieve this we use the command(in config terminal mode):ip local pool "Poolname" "ip address ip address) ip addresses need to be available from the network of which we plan to authenticate to.

In our case the call for the vpn pool is PoolVPN the ip addresses are 192.168.10.25 192.168.10.30

Now we want to allow aaa so that it will authenticate to the VPN to achieve this we easy input the command: aaa new-model

Now we configure the serial linked to the net or in our case the only linked to the router patron with the static map

First we input the interface – int "int call" -> crypto map "Map call" (a reminder all letters are case sensitive. And now we simply clearly visit the patron and input the credentials had to authenticate.

(Will ship a further image from the snapping device to expose that the VPN has correctly been linked to)

To upload SSH protocol configuration withinside the cisco router we want to go into some instructions , first we are able to configure thru the IT control PC

The instructions are as follows first I modified the hostname – config t – hostname "hostname"

Then I delivered an ip domain call through doing the subsequent command" ip area-call "call" in this example it's miles nbu.com , then I did line vty zero four then enabled ssh through inputing the command shipping enter ssh ,

Now we exit the road interface and do the subsequent instructions: crypto key generate rsa I selected 1024 bits right into a username router1 password cisco , I did the command two times after the router informed me that ssh has been enabled.

Now we move into line vty 0 15 into command: login local then we press do copy run start to keep configuration , Now to connect through the command line ssh we go to the PC , we input the subsequent command ssh -l router1 211.1.1.2 (ip address of the router) after which we input the password , we've passwords as we enabled a password to go into privileged EXEC mode which offers us every other layer of security.

Now the identical may be finished for the switches

Now for the authentication approach command: aaa authentication login “name of the vpn” local we're the use of local as the nearby records base in this case and now no longer an ldap for AD,

Now we want a call for the vpn organization: aaa authorization community “organization call” nearby

Now to create consumer call and password: username “username” mystery “password”

For our topology the groupname is groupVPN , the username and password are – username: uservpn mystery ciscovpn

Secret will permit the password to be encrypted and now no longer simply be out in simple text

Now we circulate into the isakmp coverage - Internet Security Association and Key Management Protocol (ISAKMP) is a protocol described via way of means of RFC 2408 for setting up Security association (SA) and cryptographic keys in an Internet environment.

The command is as follows: crypto isakmp coverage one hundred . we selected one hundred in our instance as priority

Now we want to encrypt to guard the records to achieve this we use the command: encryption aes 256.

;0000000000000

We enter the command crypto isakmp purchaser configuration group “groupname” groupname is the name we brought withinside the authorization network section , in our case it is “groupVPN”

Now need want to feature the important thing for the group – password for the organization command is:

Key “password” in our case the password for the group now no longer consumer is “ciscogroupvpn”

Now we assign a pool for the group the group could be the only we brought earlier:

Pool “Poolname” in our case it's miles PoolVPN. Now go out the isakmp group.

Now to configure the rework set that is a mixture of protection protocols and algorithm which must be matched on the peer router:

crypto ipsec remodel-set “setname” esp-des esp-md5-hmac . in our case the call is SetVPN.

Now to create the dynamic map the dynamic crypto map command statements are used for determining whether or not or now no longer site visitors have to be protected:

Crypto dynamic-map “Mapname” one hundred in our case the name is “DynamicMAP”

Now we set the rework set: set rework-set “setname” or in our case it's miles “SetVPN”

Reverse-route –Reverse route injection (RRI) is also enabled to offer the capacity for simplest the lively tool withinside the HSRP institution to be marketing and marketing itself to internal gadgets as the following hop VPN gateway to the far flung proxies. If a failover occurs, routes are deleted on the previous lively tool and created on the brand new lively tool. go out the map.

Now we configure the router to answer to mode configuration requests from far flung clients:

Crypto map “mapname´patron configuration cope with respond – in our case it's miles StaticMap.

Conclusion

This project is like a guide for how to configure and make a medium LAN and for the final part we assess how much it costs. The cost is 5495$ (USD) for all the hardware equipment. For most operations like this one year costs around 10% so we can add it to the overall cost.

The training of network administration (CCNA) is around 680$ per person.

We dont need any software because the software that we need is included in the price of the equipment (Windows OS RDP included, Included Windows firewall etc.)

So from my rough estimates the final cost is 7850$.

I would also add Around 5000$ for the licenses for all the cisco equipment for the forceable years. So, The total Rough cost is around 12 850$. With everything in check and ready to go.

References:

- *Emil Stoilov, Lecture Notes on Network Hardware, Module NETB356, Moodle System,
NBU*
- *Shinder Debra, Computer Networking Essentials, Cisco Press, 2002.*
- *Tannenbaum, Andrew, Witherall, David, Computer Networks, Pearson Publ. House,
Fifth edition, 2011*
- *Sam Halabi, Internet Routing Architectures, Cisco Press, 2000*