‏9/3/2021

eitan danon

Ccna final project

See security

Oriel kozaiev

Table of Contents

Basic configuration ………………………………………………………………………….2-5

Vlna, Vtp configuration …………………………………………………………………………….6-8

Dhcp server configuration …………………………………………………………………………9-10

Vlan 2 configuration………………………………………………………………………………….11-12

Port security configuration……………………………………………………………………….13-14

Static rout configuration …………………………………………………………………………...15-16

Ssh configuration ………………………………………………………………………………………17-18

Acl configuration ……………………………………………………………………………………...19-20

Web surfing …………………………………………………………………………………………… 21

**CCNA:**

he Cisco CCNA certification, which stands for **Cisco Certified Network Associate**, refers to a wide range of technical specializations that Cisco offers the IT world.

By this technology we can config and manage routing devices by our own needs, and make our own network and in this project ill explain by packet tracer by cisco

How to build this network.

Packet tracer is a cisco program that help us to simulate how the network and configuration of different type of devices work. So, let’s begin the project

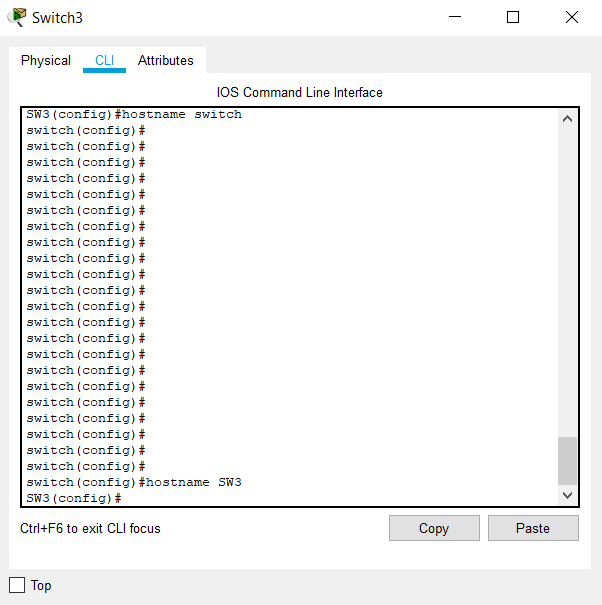
***Basic configuration***

First of all, before we begin configuration, we need to understand few things at first.

There are few types of configuration modes – the first mode is user mode that have no privilege to do anything, second mode is privilege executive mode that this mode gives us the privilege to see settings and policy’s, global configuration mode is the mode that we will use to configurate all the setting and policies on the devices we want and at last is interface configuration mode with this mode we can config specific interface at the device we want. So, after I explained about the types of the modes in the configuration, we can start use it.

1.config user name to all the devices:

To config the user’s name we will need to enter to global configuration mode by this way



Switch> enable …………………………….> means we are in user mode

Switch# configur terminal ………. #means we are in executive mode

Switch(config) # ……… (config)# means we are in global config mode

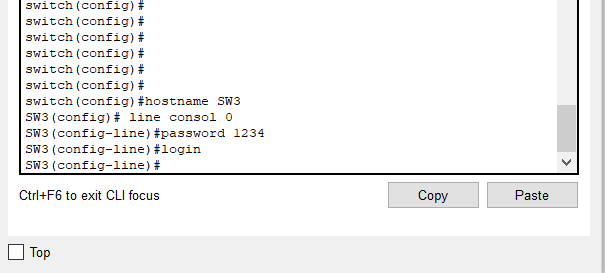
After we enter to the config mode we will use (hostname) command and after that we choose name like this

Switch(config)# hostname SW3

After we named all the devices, we need to secure them by passwords-

But the password can set when you enter the devices and when you go to privilege mode, and we will secure them both.

To put password on user mode (the first screen of the device) we will use

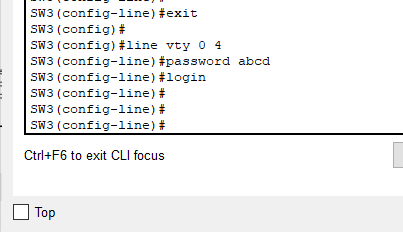


SW3(config) # line consol 0

SW3(config-line) # password 1234

SW3(config-line) # login / and that’s all

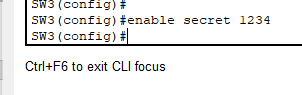
Now we need to put password to virtual terminal access by using (line vty 0 4) command



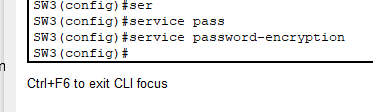
SW3(config)# line vty 0 4

SW3(config-line) #password abcd

SW3(config-line) login / and that’s all

Now to secure the privilege mode (enable) we need to use the (secret enable) command to get a secure password and encrypted that way we don’t need to use (enable password) command and then to encrypt it

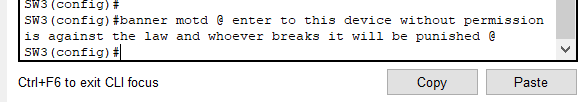
SW3(config)# enable secret 1234

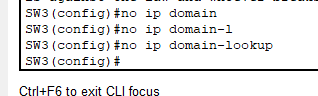
****Now to encrypt the user mode password for the attackers will be more difficult to find we will use (service password-encryption) command

SW#(config)#**service password-encryption**

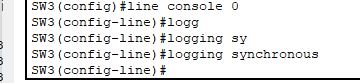
Now after we configure those settings (host names and password to the modes) , we will use banner warning for those who will try to enter the switch or the device without an promotion , we will use (banner motd) command

SW3(config)# banner motd @ enter to this device without permission Against the law and whoever breaks it will be punished@



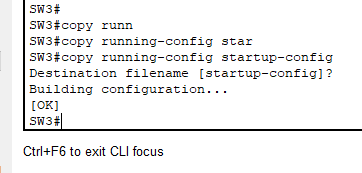
Now after we put an alert to all the people who will try to enter, we will setup some config to help us use the system configuration more confutable for us, first command for that is (no ip domain-lookup) this command helps us because sometimes we type some word wrong and the system try to find it a meaning and because there is not meaning the system freeze for 30sec and for to not make it freeze we will use no lookup

SW3(config)# no ip domain-lookup

The second command is (**logging synchronous)** this command helps us because sometimes when we write the system pops up a massage and it interferes us in the writing, so we will use this command to make it stop.

SW3(config)#line console 0

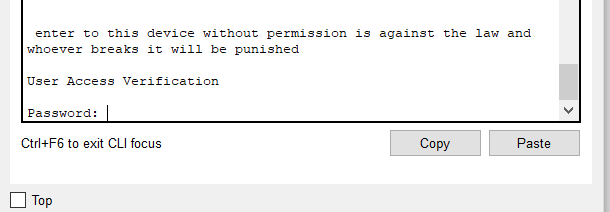
SW3(config-line) #logging synchronous

Now after we finish with the configuration like every system, we need to save the data because when we will restart the switch all the data will be deleted. So, for that we will use simple command (copy running-config startup-config) like you can read its says to copy the running configuration we did to the startup configuration when the router will be rest, we will do it at enable mode (privilege)

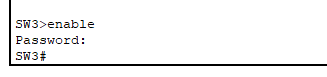
Switch# copy running-config startup-config

Destination filename [startup-config]? [Enter]

And now after we finish let’s check all the configuration if it’s working.



Like we see there is the banner warning and the user mode password (1234)



And here we can see the enable secret password (abcd) and is all working.

So, what we learned?

How to put name to a host device.

How to put a password to different types of modes and how to encrypt it.

How to put a banner warning.

How to config the system not to freeze if we don’t write right a word.

How to config non pops ups massages.

How to save the configuration stats so they will be not deleted.

***Vtp – vlan***

Before we start working with the vtp – vlan configuration we need to understand what those 2 words mean.

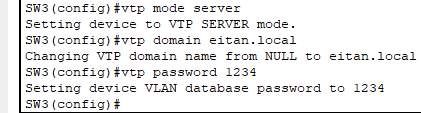
Vlan: (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs), One or more network switches may support multiple, independent VLANs, creating Layer 2 (data link) implementations of subnets. A VLAN is associated with a broadcast domain.

Vtp:( VLAN Trunking Protocol) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks on the whole local area network. To do this, VTP carries VLAN information to all the switches in a VTP domain.

So, after we understand what those words mean let’s start config them to our network.

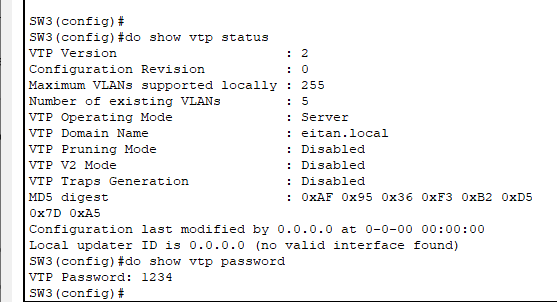
First, we need to set vtp server by using (vtp mode server) command. And after we setup a server we will setup a clints.

Vtp server:

SW3(config)#vtp mode {server/client/transparent}

SW3(config)#vtp domain {domain-name}

SW3(config)#vtp password {password}



To check the setup, we will use:

We can use (do show) if we are in config mode

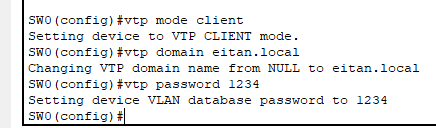
Switch# show vtp password

Switch# show vtp status

Vtp clint:

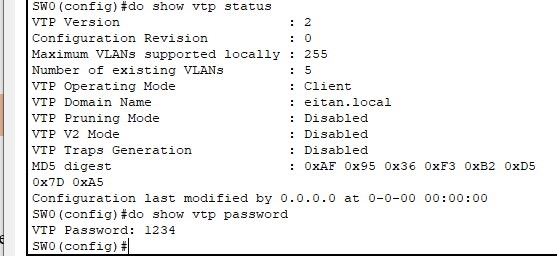
To setup Vtp clint we will use the same command but we will choose clint instead of server.

SW0(config)#vtp mode {server/client/transparent}

SW0(config)#vtp domain {domain-name}

SW0(config)#vtp password {password}

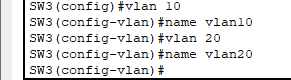
Now let’s check if the setup worked by using those commands:

SW0# show vtp password

SW0# show vtp status

Now after we setup an IP address to the switch we need to create a vlan so we can add to him devices and we will use those commands:

We need to create the Vlans on the server Vtp in our case is SW3

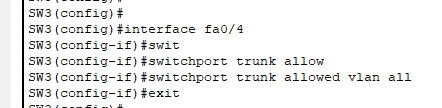
SW3(config)#vlan {vlan-id}

SW3(config-vlan) #name {vlan-name} (not necessary)

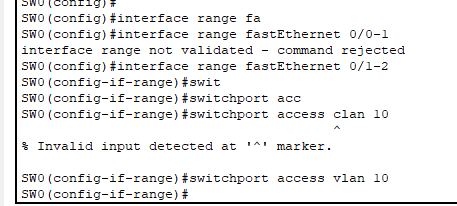
After we created the vlans we need to trunk the clients and the router so the server can assist the Vlan without making all the switches as servers, so we will use those commands:



Switch(config-if) #switchport mode trunk



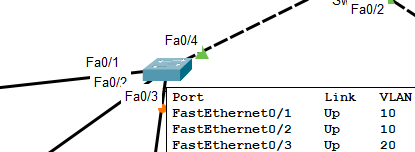
Switch(config-if) #switchport trunk allowed vlan

So, after we allowed the Vlan trunk we can add host to the vlan by using those commands:

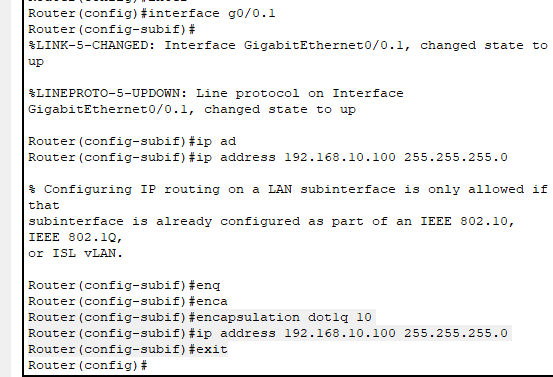
Switch(config)#interface range fastethernet 0/(number)-(number)

Switch(config-if-range) #switchport access vlan (number)

The numbers are the interfaces of the device we choose to add.

and like we see the configuration worked, we succeeded to manage the Vlans by interfaces from the client SW0 by using trunk mode allow from server switch SW3

after we organized the VLANS we need to go to the router and create an sub interfaces of our VLANS and give them an network id, we are going to use encapsulation dot1q command. So let’s create sub inter face for vlan 10 :

R0(config)#interface g0/0.1

R0(config-subif)#

Router(config-subif)#ip address 192.168.10.100 255.255.255.0

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.10.100 255.255.255.0

Router(config-subif)#exit

And that’s how we create a sub interface, and now we need to create another one for vlan 20

***Dynamic host configuration protocol (DHCP)***

(**DHCP**) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to **use** network services such as DNS, NTP, and any communication protocol based on UDP or TCP.

So basically, the DHCP protocol gives our hosts IP address so they can communicate in the network, so after we understand what is this protocol, we will start to config it in our network. This protocol can be setup on router so we will practice on our router that is connected with the switches we already configure. The command we will use are:

R0(config)#ip dhcp excluded-address {low IP} {high IP} – this command excluded IP addresses we don’t want to be give away by the dhcp server.

R1(config)#**ip dhcp pool** {pool name} – putting us in the dhcp config mode

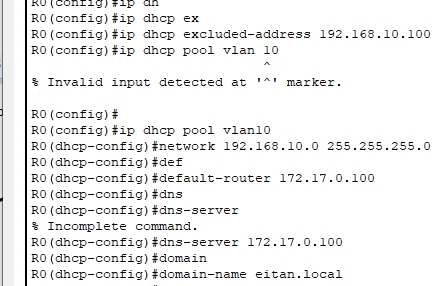
R1(dhcp-config) #**network** {network-id} {subnet-mask} – setup the ip network that gives ip

R1(dhcp-config) #**default-router** {ip address} the default getaway ip

R1(dhcp-config) #**dns-server** {ip address} the DNS server ip

R1(dhcp-config) #**lease** {days} {hours} {minutes} how much time until the ip will change

R1(dhcp-config) #**domain-name** {domain name} the domain name of the network

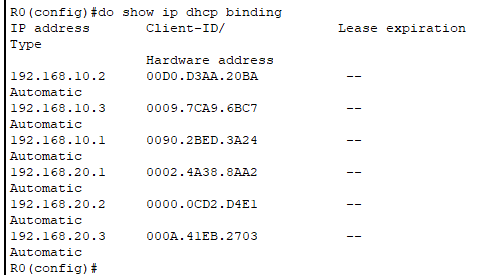


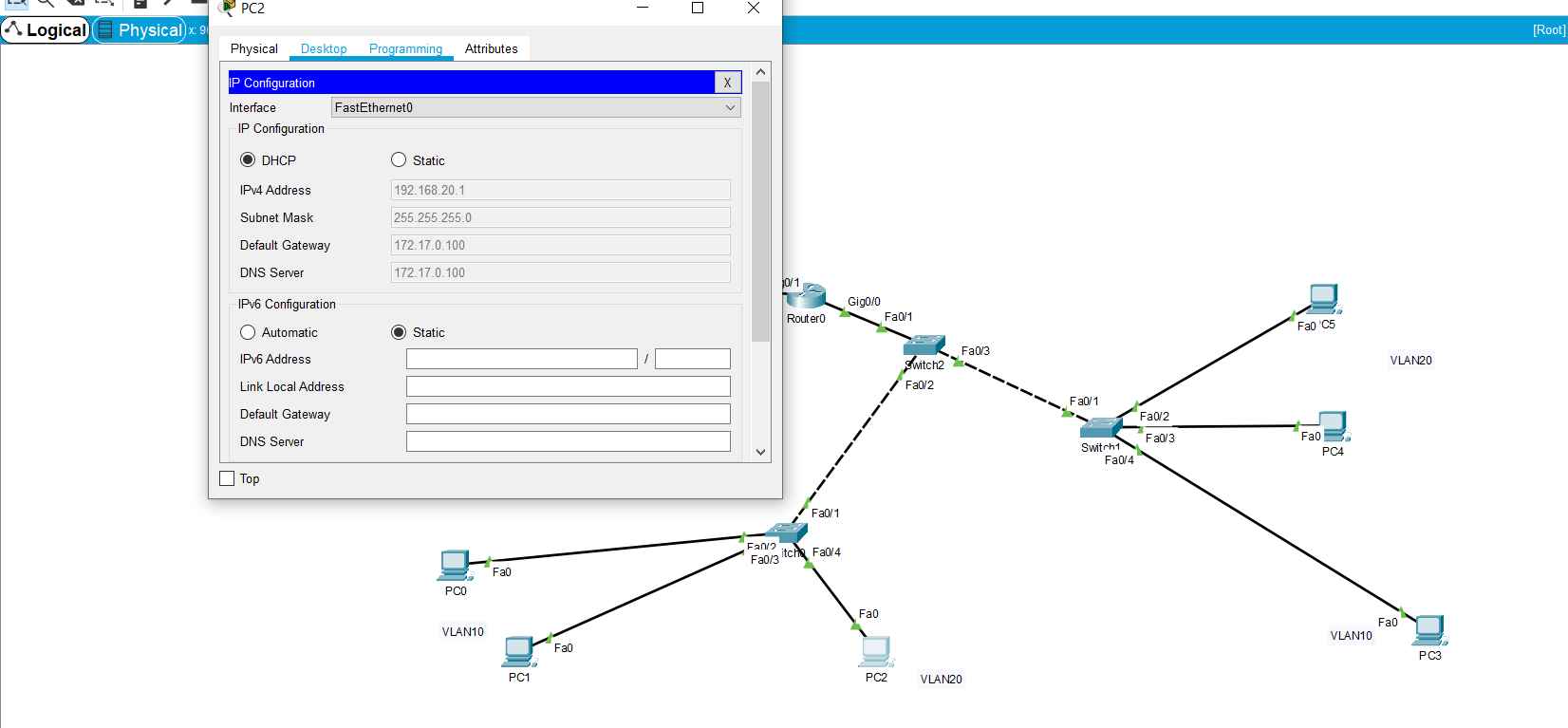
192.168.0.254

172.19.0.200

Like we see in the pic I excluded the switch IP address and setup the DHCP configuration, now for checking if the IP addresses are given like its spouse to be we will use this command:

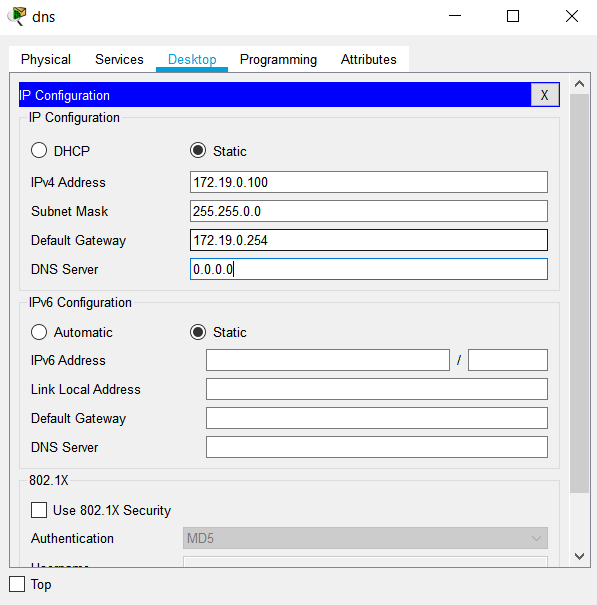
R0#show ip dhcp binding or R0(config)# do show ip dhcp binding



like we see every VLAN has his ip address and VLAN even when they aren’t in the same network 

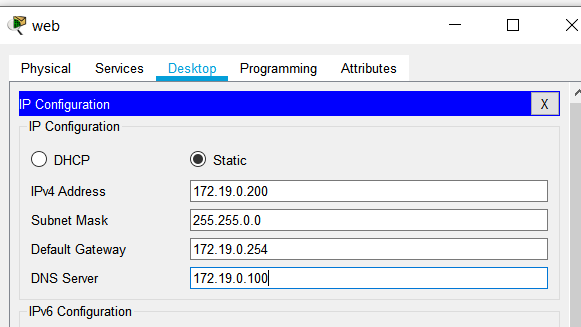
here we can see that pc2 got the DG and DNS by what we write, and we see here that in one network we have 2 VLANS but we splinted them earlier but their interfaces so we checked and every this is working property.

**LAN2 configuration**



LAN2 is going to be our web server and we will customize it manually.

First, we will setup the DNS IP address 172.19.0.100 255.255.0.0---- tap the DNS device—desktop---- IP configuration:

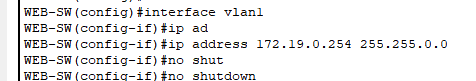


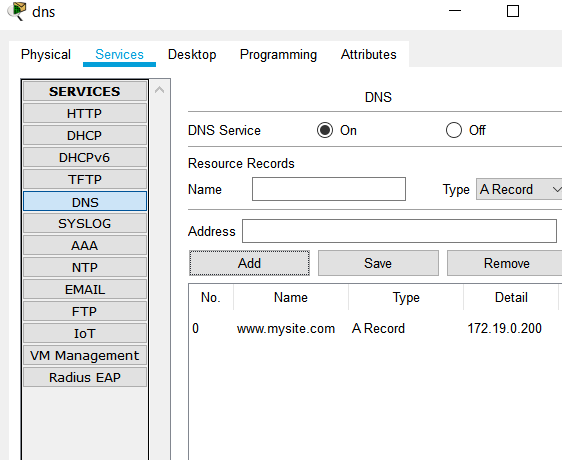
Now we will setup the web server IP address as 172.19.0.200 255.255.255.0.0 by the same way:

Now we will setup the switch the IP address 172.19.0.254 255.255.0.0 by this command

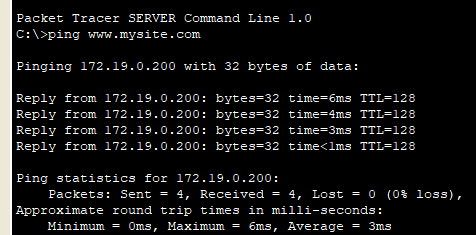
WEB-SW (conifg)# interface VLAN1

WEB-SW (config-if) # IP address 172.19.0.254 255.255.0.0

WEB-SW (config-if) # no shutdown

Now we will setup on the DNS server lookup for the web server: [www.mysite.com](http://www.mysite.com) (172.19.0.200): by going to the DNS---- services----- DNS------

And now lets check it if it works:



And that’s all, every thing is working

**Port security configuration**

Port security is a layer two traffic control feature on Cisco Catalyst switches. It enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port.

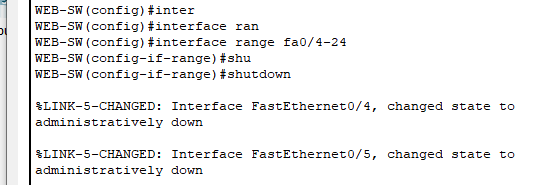
Port security help us secure better our switches from people we don’t what to have access to the switch.

First, we will secure all the interfaces are not in use by those commands:

WEB-SW>enable

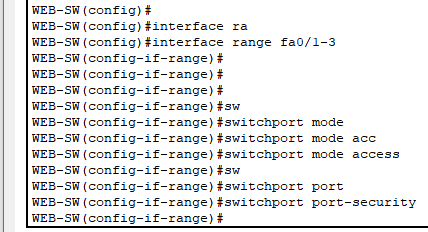
WEB-SW#show ip interface brie

WEB-SW#configure terminal

WEB-SW (config)#interface range {fastEthernet}(0/3-24)

WEB-SW (config-if-range) #shutdown

After we shut down the interfaces, there is no access to the switch with does interfaces but, if some one will disconnect the FA 0/1-3 cable and connect it to other pc and try to control the switch?

****For this we have the switchport security that only a pc with a mac that it is saved in the switch can access, but we need to remember that even a mac address can be change so port security in only the first line of defence. So, to activate this security mode we will use those commands:

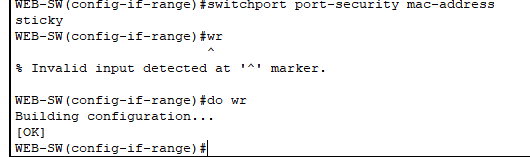
WEB-SW (config-if) #**switchport mode access**

WEB-SW (config-if) #**switchport port-security**

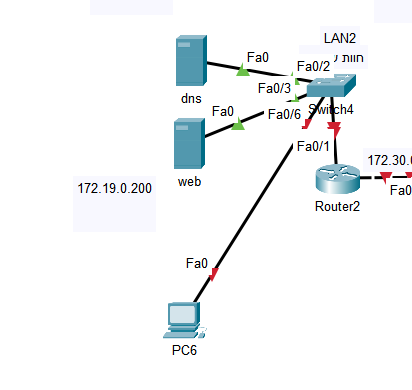
After we secure the ports, we need to learn the switch what mac address are available

By using this command:

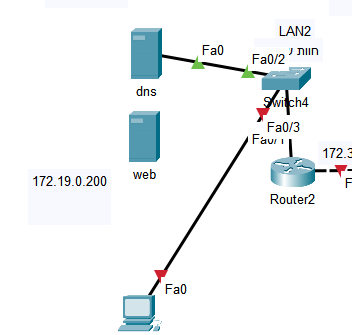
Switch(config-if) #**switchport port-security mac-address sticky**

****

After we finish to secure we will check if all the setup works for the ports:

First, we will try to connect to shutdown interface like fa0/6

Like we see the fa0 pc can’t connect to the switch with the interface, but let’s try to connect him instead of DNS server.



Doesn’t work, the interface fa0/1 immediately shutdown as default, so the pc will not try to connect to the switch.

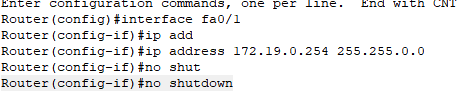
**Static rout configuration**

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.

The static rout provides a way to transfer packets between different types of networks, by finding the best path to use and split the network to different broadcast domain.

So the network is 172.30.0.0/16 and we need to connect all the routers between them by using those commands

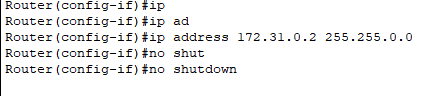
Router2

Router(config)#interface fa0/1

Router(config-if)#ip address 172.19.0.254 255.255.0.0

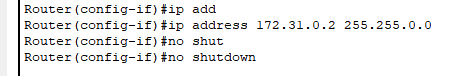
Router(config-if)#no shutdown

And now for the other side of the router fa0/0



Router1

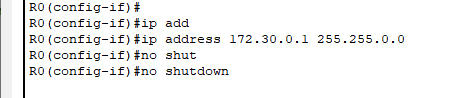
Fa0/0

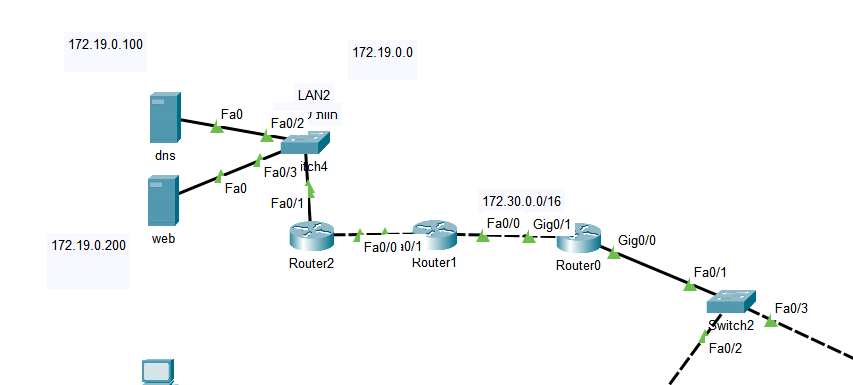


Fa0/1



Router0G0/0

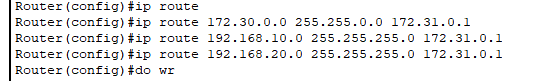




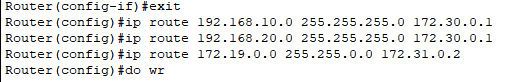
After we connected all the routers and switches, we need to static rout the routers so they can transfer packets between each other by using

Router2

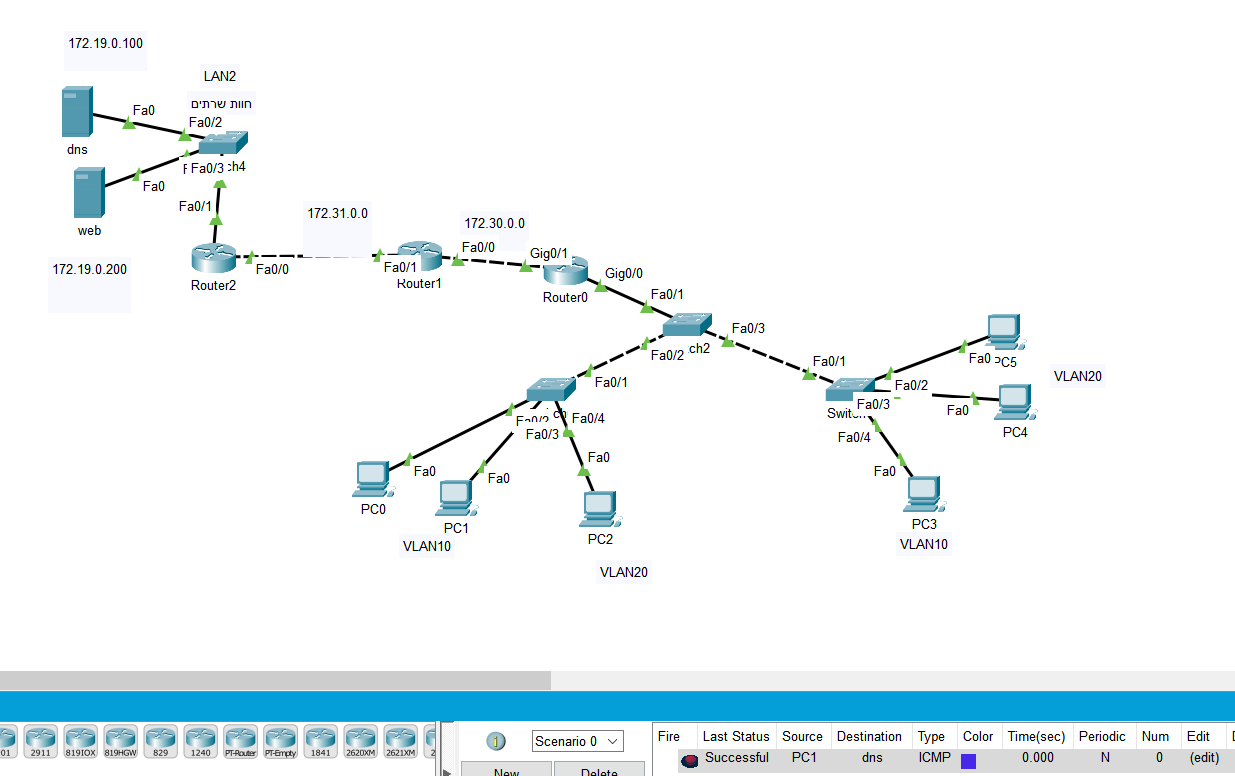
Router(config)#ip route {destination\_network} {subnet\_mask} {gateway\_address}

****

**Router1**

****

****Router0

****After we rout every router at the network we will test if we did it correctly, like we see there is an ping from pc1(LAN1) to DNS server(LAN2)

**SSH configuration**

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH

So, to configure on the switch SSH configuration we will use those protocols:

SW (config)#username {name} password/secret {1234}

SW (config)#ip domain-name {name. local}

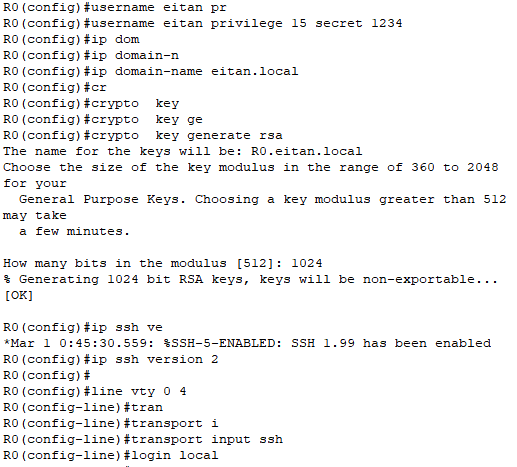
SW (config)#crypto key generate rsa

SW (config)#ip ssh version 2

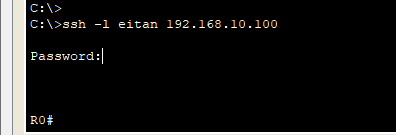
SW (config)#line vty 0 4

SW (config-line) #transport input {ssh/telnet/all/none}

SW (config-line) #login local

****

Now let’s check form the pc(VLAN10) if we have connection : and we have and its working



After we setup the ssh I want to only VLAN10 will have access to the switches with SSH

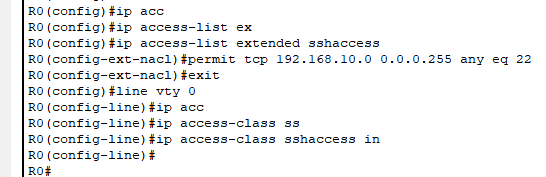
For that we will use ACL: and ill use those commands

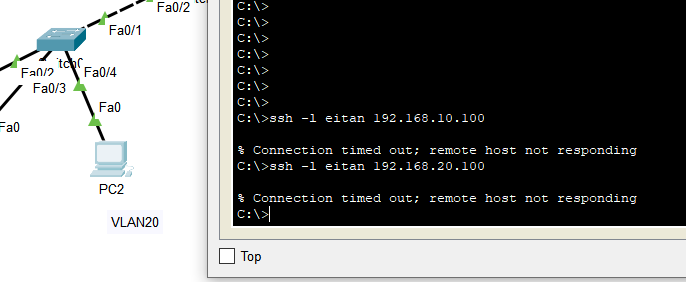
R0(config)#ip access-list extended (name)

R0(config-ext-nacl)#permit tcp (ip address) any eq 22

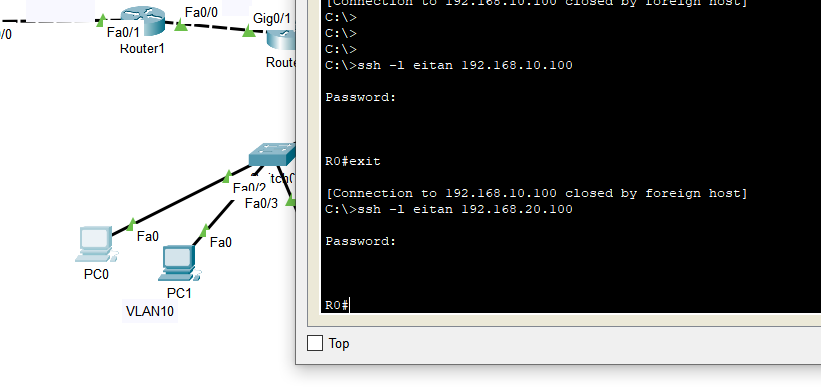
R0(config)#line vty 0

R0(config-line)#ip access-class (name) in





Now after we setup lets check if it is working Like we see pc from VLAN20 cant access to ssh, that means the ACL is working good

and here we see that VLAN 10 can access to both switches from the both networks

that’s.

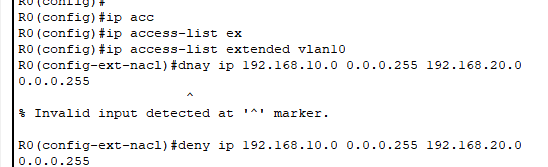
**Access control list configuration**

Access control list is an access list that organize the network by our commands and tell the pc what it can and can’t do. For example: vlan1 to not communicate with vlan2 or only this pc can access with SSH to this pc. To use this protocol, we will use those commands

R0(config)#ip access-list extended (name of the list)

R0(config-ext-nacl)#deny ip (the ip we want to set the list) ( the destination ip)

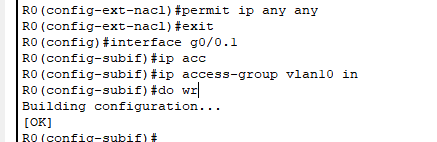
R0(config-ext-nacl)#permit ip any any

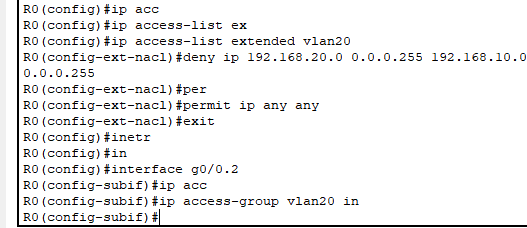


And to set the list in to the VLAN we want or the network we want we will use the interface we want and the sub interface we need: and setup and list by those commands.

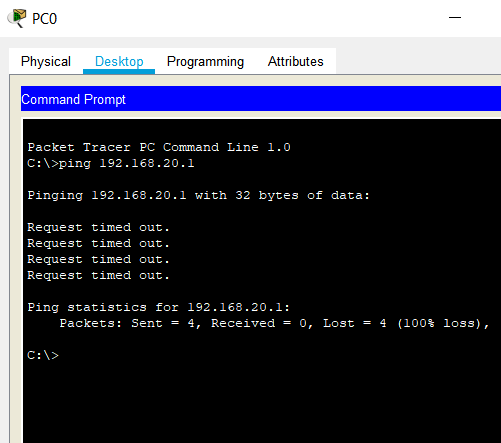
R0(config)#interface g0/0.1 – the interface we want to put the list

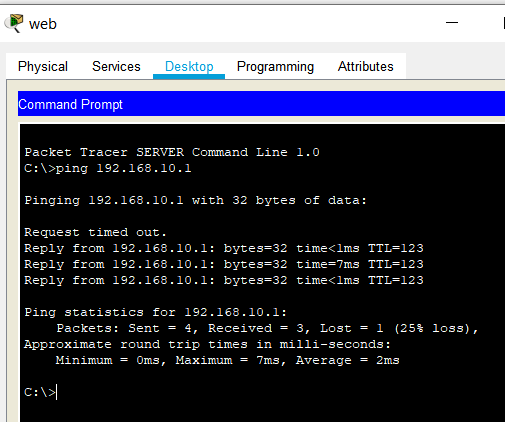
R0(config-subif) #ip access-group (name of the list) in



And the same thing we need to do the other side of the network for us is VLAN 2 

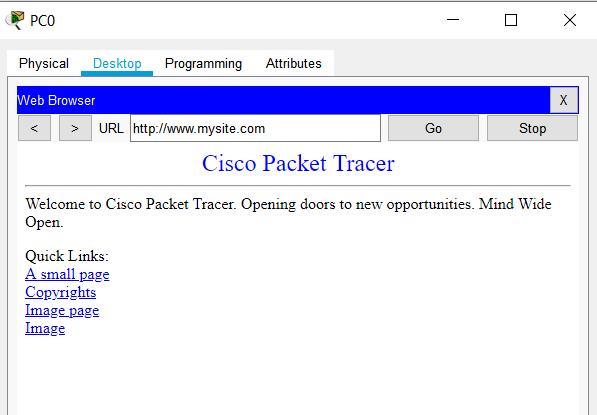
And now after we setup all the rules we will check if they are working by try to ping from vlan1 to VLAN 2 : like we see no respond, and that mean the rule is working

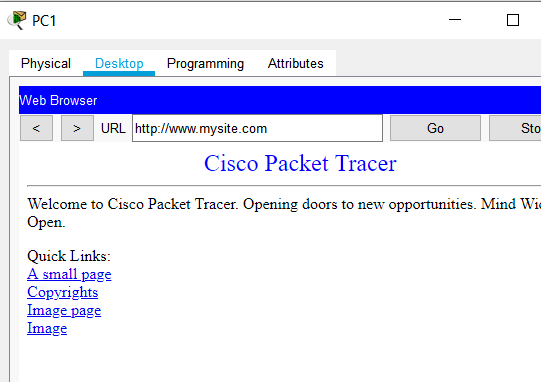


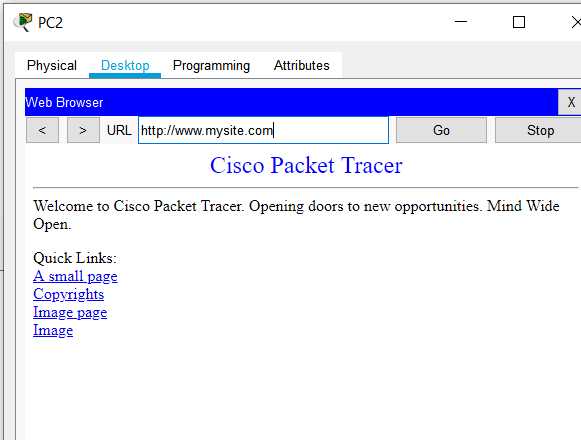
And now we will check if we will get ping from the LAN2 to LAN1 for example VLAN10 to LAN2 : and like we see we have an ping and everything is working correctly

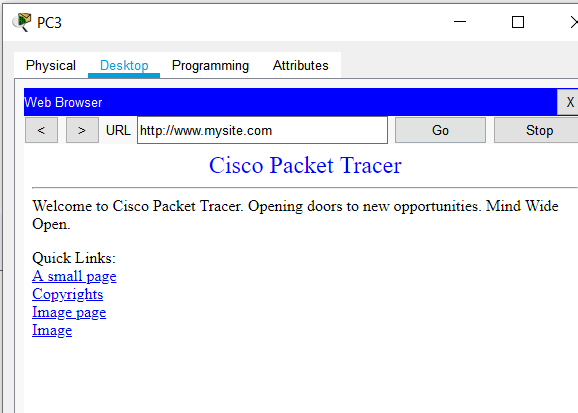
**Web surfing**

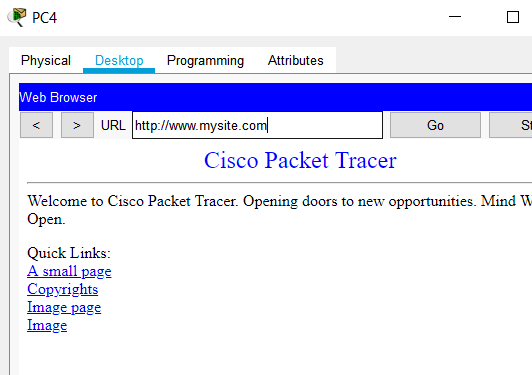
Now for our final step we will see if all the pcs have the access to the we server by entering every pc web and type www.mysite.com .

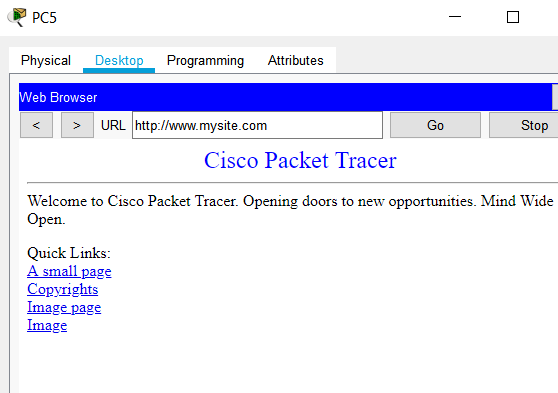
PC0-VLAN10 PC1-VLAN10



PC2-VLAN20 PC3-VLAN10



PC4-VLAN20 PC5-VLAN20



And every thing is working well and that was the final step.

thanks to Uriel of being the pest teacher that because of him I understand it better