Jan

2021

CCNA Tutorial

For beginners, an exercise for those who wish to take the exam.

By: Eido Epstein

in

Eido Epstein

Glossary

Requirements 4
Instructions 5
Save Files 6
Topology 7
Basic Configurations 10
Naming A Switch \ Router 10
Setting Credentials 11
Line Console 11
Telnet 12
Privileged EXEC Mode 13
General Password Encryption 14
Setting A Banner 15
Setting A Messages Display Sync 16
Using "logging synchronous" 16
Using "no logging console" 17
Setting A Wrong Input Wait Prevention 18
VLAN 19
General Port Configuration 20
Trunk 22
Router On a Stick 23
DHCP 24
Relay Agent 24
DHCP Server Configuration 25
DHCP Router Configuration 26
LAN2 Setup 28
Router2 28
DNS Server 29
Web Server 32

Port Security 34
Disabling Interfaces 34
Limiting Interface Access 38
OSPF 40
Configuration 40
ACL 42
Device Interactions 42
NAT 44
NAT Overload (PAT) 44
Wireless LAN Controller 47
Device Settings 47
Switch Settings 48
DHCP Settings 48
Browser Settings 49
Endpoint Wireless Connection 53
SSH 54
Configuration 54
Verifying Connection 54
Conclusion 55

Requirements

In order to manually follow-up with this article, there are some prerequisites that needs be made;

- Installed CISCO Packet Tracer (Link to download).
- This CCNA tutorial .pkt file (Link to download).
- Basic familiarity with networks.

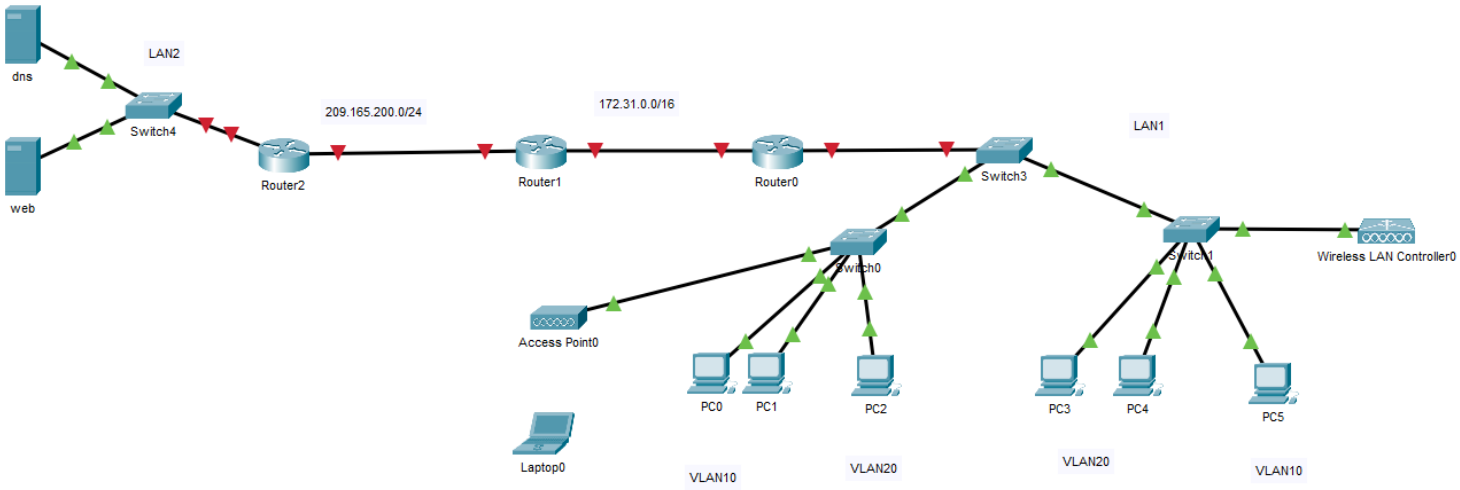
This guide can only serve as an additional exercise for the CISCO's CCNA exam. It cannot replace other studying tools or documentations, only enriching them.

Important; This tutorial can sometimes display specific commands on each section for training purposes. When possible, you can and should input all the series of commands you need for a single device in one configuration flow.

- Packet Tracer is a network simulator software. It simulates networking devices that are used to build CCNA practice labs. An average CCNA lab costs more than $300. With Packet Tracer you can learn how to configure routers and switches from the command line.

In order to begin this tutorial;

1) Open Packet Tracer; 
2) At the top left corner, press on "**file**".
3) Click on "**Open**" and choose the "**CCNA Tutorial.pkt**" file.
4) When picked the following network should be presented to you;



Instructions

First, we'll present what needs to be done for each section;

Basic Configurations

- Configure a name for each router/switch.
- Configure access passwords for the Console and Telnet on all devices.
- Configure a Privileged EXEC mode password for all devices.
- Encrypt all the password you entered and will enter in the future for all the devices.
- Configure a logon banner for all of the devices.
- Sync system messages so they won't interrupt you when you input commands.
- Prevent the system from being idle for 30 seconds when typing a wrong input.

VLAN

- Configure VLANs for Switches 0,1 and 3.
- Connect the VLANs to the relevant interfaces.

DHCP

- At the LAN1 network, configure Router0 as a DHCP server.
    - Create a pool that will be used by VLAN10.
    - Create a pool that will be used by VLAN20.
    - Configure the DHCP service in the router to also provide the Default Gateway and DNS server addresses.
    - Configure in the router a sub-interface for each VLAN.

❖ For this section we also provided details on configuring an ordinary DHCP server. This method is optional.

LAN2 Setup

- Configure the servers and router in the LAN2 network.
- Create an A record in the DNS server.

Port Security

- Use the Port Security feature for securing Switch4.
- Block all the interfaces that are not being used.
- Make sure the other devices will not be able to physically access the network.

OSPF

- Configure an OSPF routing between routers.
    - Configure IP addresses for all the routers.
    - Enable the LAN1 and LAN2 networks to communicate with each other.

ACL

- Use ACL in order prevent communication only between VLAN10 and VLAN20 endpoint devices.

NAT

- Configure NAT Overload (PAT) communication between LAN1 to LAN2.

Wireless LAN Controller

- Configure a WLC for the LAN1 Network.
- The wireless network needs to be connected to VLAN10.

SSH

- Enable only VLAN10 endpoint devices to connect via SSH to all the routers and switches.

Save Files

Use the save files in order to practice in a specific section or test your work;

0 - CCNA Tutorial

1 - Basic Configurations

2 - VLAN

3 - DHCP

4 - LAN2 Setup

5 - Port Security

6 - OSPF

7 - ACL

8 - NAT

9 - Wireless LAN Controller

10 - SSH

Topology

Headline	Hostname	User EXEC Password	Privileged EXEC Password	Network/s	Functionality
Switch0	sw0	abcd	1234	---	Switch
Switch1	sw1	abcd	1234	---	Switch
Switch3	sw3	abcd	1234	---	Switch
Switch4	sw4	abcd	1234	172.19.0.254/16	Switch
Router0	r0	abcd	1234	192.168.10.254/24 192.168.20.254/24 172.31.0.1/16	Router (DHCP)
Router1	r1	abcd	1234	172.31.0.2/16 209.165.200.1/24	Router
Router2	r2	abcd	1234	172.19.255.254/16 209.165.200.2/24	Router
PC0	---	---	---	192.168.10.0/24	Endpoint
PC1	---	---	---	192.168.10.0/24	Endpoint
PC2	---	---	---	192.168.20.0/24	Endpoint
PC3	---	---	---	192.168.20.0/24	Endpoint
PC4	---	---	---	192.168.20.0/24	Endpoint
PC5	---	---	---	192.168.10.0/24	Endpoint
dns	---	---	---	172.19.0.100/16	DNS
web	---	---	---	172.19.0.200/16	Web
WLC	WLC	Abcd1234 [Browser]		192.168.10.253/24	WLC
WPA	---	---	---	DHCP	WPA

Device	VLAN Name	ID	Interface	IP Range	Mode
Switch0	support	10	Fa0/1,2	192.168.10.0/24	Access
	product	20	Fa0/5	192.168.20.0/24	Access
	---	---	Gig0/1	---	Trunk
	support	10	Fa0/3	---	Access
Switch1	support	10	Fa0/5	192.168.10.0/24	Access
	product	20	Fa0/1,2	192.168.20.0/24	Access
	---	---	Gig0/1	---	Trunk
	support	10	Gig0/2	---	Access
Switch3	---	---	Gig0/1	---	Trunk
	---	---	Gig0/2	---	Trunk
	---	---	Fa0/24	---	Trunk
	support	10	---	---	---
	product	20	---	---	---
Switch4	blocked	13	Fa0/3-24	---	Access
			Gig0/2	---	Access
Router0	---	10	Gig0/0/0.10	192.168.10.254/24	---
	---	20	Gig0/0/0.20	192.168.20.254/24	---
	---	---	Gig0/0/1	172.31.0.1/16	---
Router1	---	---	Gig0/0/0	172.31.0.2/16	---
	---	---	Gig0/0/1	209.165.200.1/24	---
Router2	---	---	Gig0/0/1	172.19.255.254/16	---
	---	---	Gig0/0/0	209.165.200.2/24	---

- DHCP Pool Configurations [Optional];

Interface	Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Users
Fa0/1	serverPool [vlan10]	192.168.10.254	172.19.0.100	192.168.10.10	255.255.255.0	50
Fa0/1	Vlan20	192.168.20.254	172.19.0.100	192.168.20.20	255.255.255.0	50

- DNS Record Details;

Name	Record Type	Address
www.mysite.com	A	172.19.0.200

- OSPF

Router	Process ID	Networks	Wildcard	Area	Passive Interface
Router0	111	192.168.0.0	0.0.255.255	0	Gig0/0/0
		172.31.0.0	0.0.255.255	0	
Router1	111	172.31.0.0	0.0.255.255	0	---
		209.165.200.0	0.0.0.255	0	
Router2	111	209.165.200.0	0.0.0.255	0	Gig0/0/1
		172.19.0.0	0.0.255.255	0	

- ACL;

Router	Interface	ID	ACL Type	In / Out	Network	Wildcard	Action
Router0	Gig0/0/0.10	20	standard	Outbound	192.168.20.0	0.0.0.255	Deny
					permit	any	Permit
	Gig0/0/0.20	10	standard	Outbound	192.168.10.0	0.0.0.255	Deny
					permit	any	Permit
	---	13	standard	---	192.168.10.0	0.0.0.255	Permit
Router1	---	11	standard	---	192.168.10.0	0.0.0.255	Permit
					deny	any	Deny
	---	12	standard	---	192.168.20.0	0.0.0.255	Permit
					deny	any	Deny
	---	13	standard	---	192.168.10.0	0.0.0.255	Permit
Router2	---	13	standard	---	209.165.200.10	0.0.0.0	Permit
Switch0	---	13	standard	---	192.168.10.0	0.0.0.255	Permit
Switch1	---	13	standard	---	192.168.10.0	0.0.0.255	Permit
Switch3	---	13	standard	---	192.168.10.0	0.0.0.255	Permit
Switch4	---	13	standard	---	209.165.200.10	0.0.0.0	Permit

- NAT;

Router	Interface	Inside / Outside	ACL ID	Name	IP "From"	IP "To"	Subnet Mask
Router1	Gig0/0/1	Outside	---	vlan10	209.165.200.10	209.165.200.10	255.255.255.0
			---	vlan20	209.165.200.20	209.165.200.20	255.255.255.0
	Gig0/0/0	Inside	11	---	---	---	---
			12	---	---	---	---

- WLC;

Environment	IP	Subnet Mask	Default Gateway	DNS Server
WLC Device	192.168.10.253	255.255.255.0	192.168.10.254	172.19.0.100

Environment	User Name	Password
Login [Browser]	admin	Abcd1234

Environment	Network Name (SSID)	Security	Passphrase
System Settings [Browser]	WLC-1	WPA2 Personal	Abcd1234

- SSH;

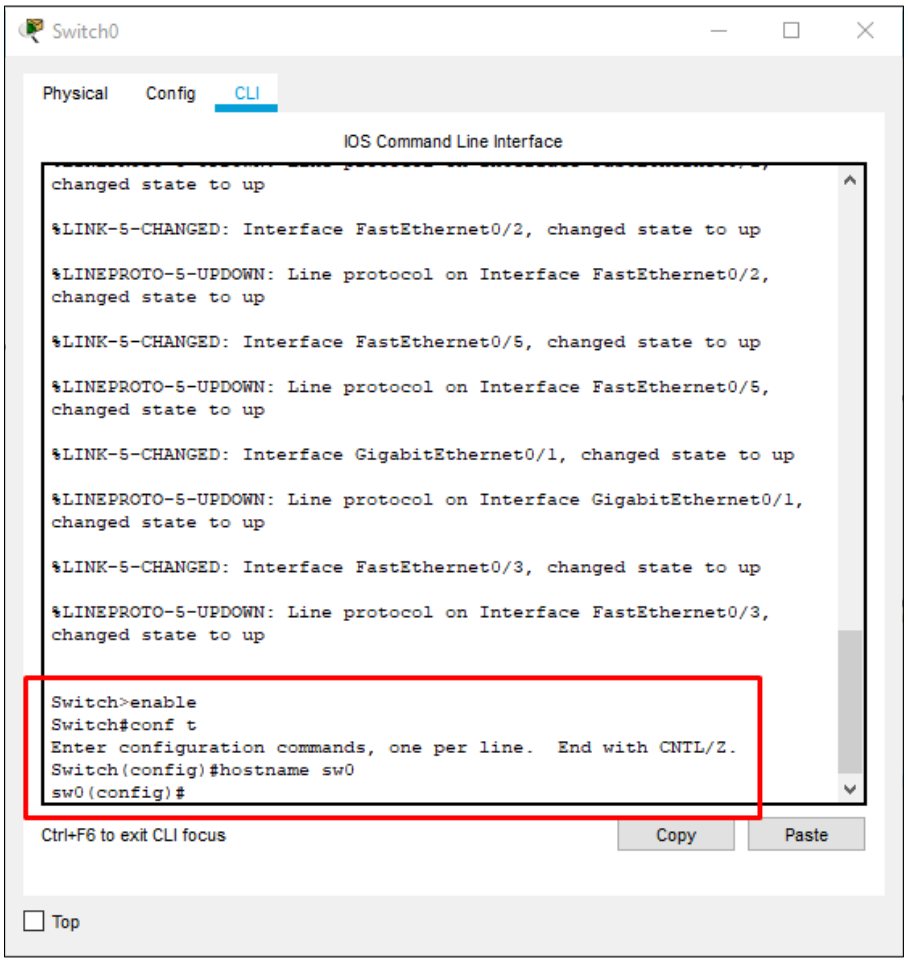
Environment	Domain	User Name	Password
All Routers & Switches	access.com	user	1234

Basic Configurations:

In this section we'll set some of the basic setting routers and switches have.

Naming A Switch\Router

1) Choose the relevant device you wish to configure.
2) Open the Command Line Input (CLI).
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**hostname *<NAME>***"



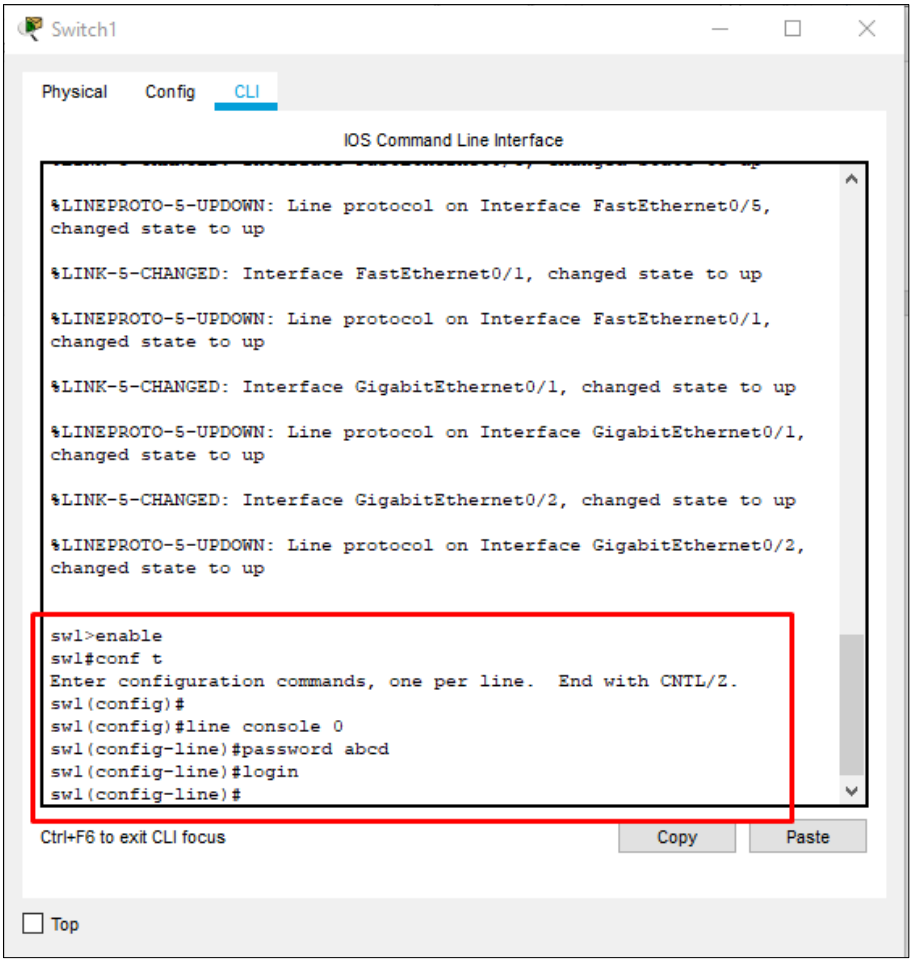
- If done correctly, you'll see that your device name changed.
- In order to correctly follow this tutorial, make sure to name all the Switches and Routers available in the following way;
  - "**Switch *X***" to "**sw*X***"
  - "**Router*X***" to "**r*X***"

Setting Credentials

Next, we'll set permissions passwords;

Setting a Line Console Password

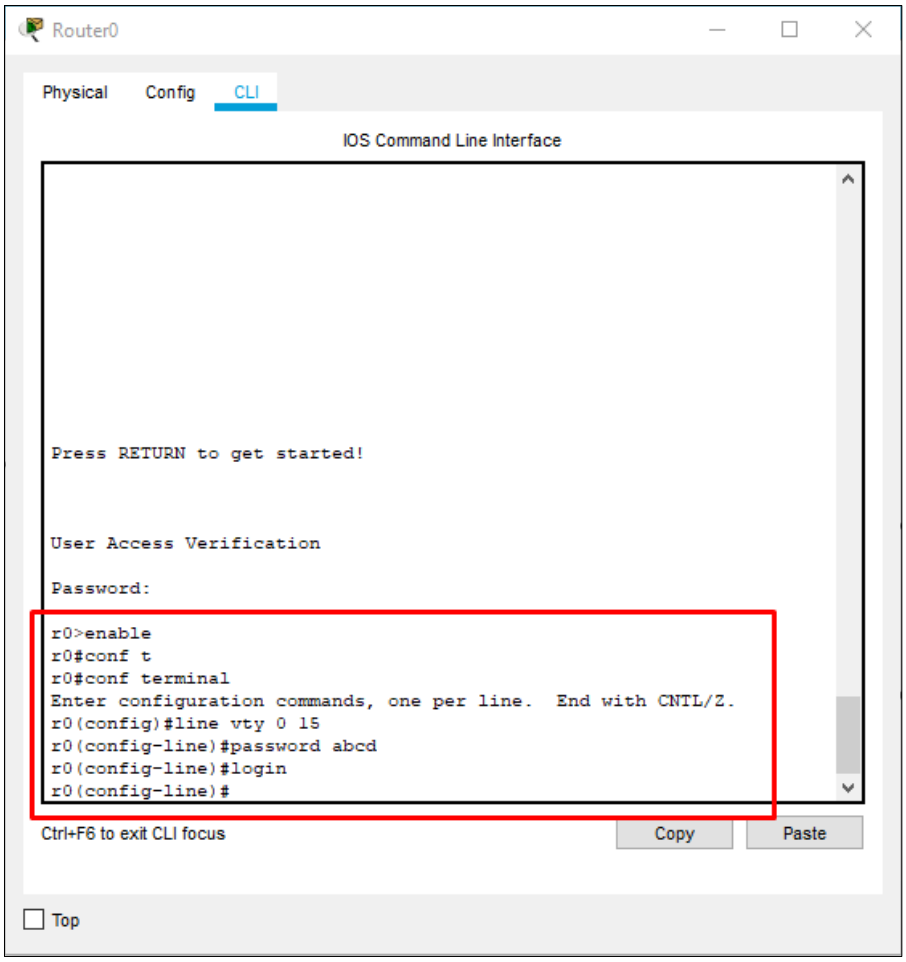
1) Choose the relevant device you wish to configure.
2) Open the CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**line console 0**".
6) Input "**password <*PASSWORD*>**".
7) Input "**login**".



- In your next login via CLI, you'll be required to input a password.
- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with the password – "***abcd***"

Setting a Telnet Password

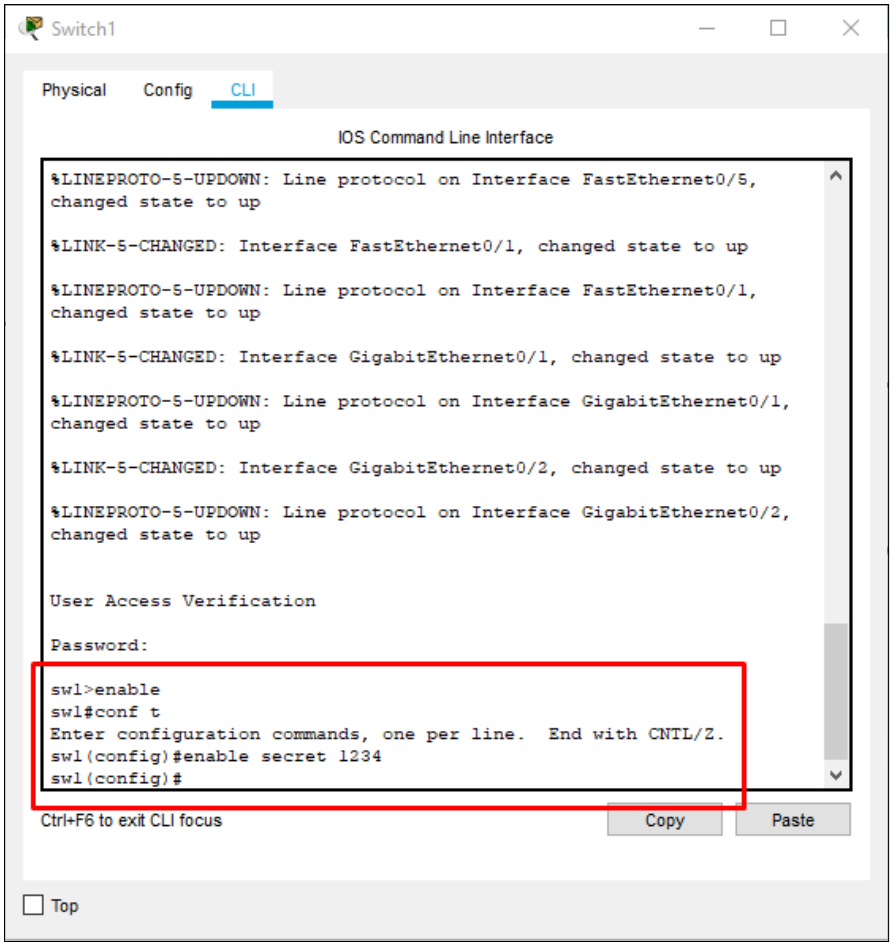
1) Choose the relevant device you wish to configure.
2) Open the CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**line vty 0 15**".
6) Input "**password <*PASSWORD*>**".
7) Input "**login**".



- When trying to simulate a Telnet connection, you'll be required to input a password.
- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with the password – "***abcd***"

Setting a Password for Privileged EXEC Mode (#)

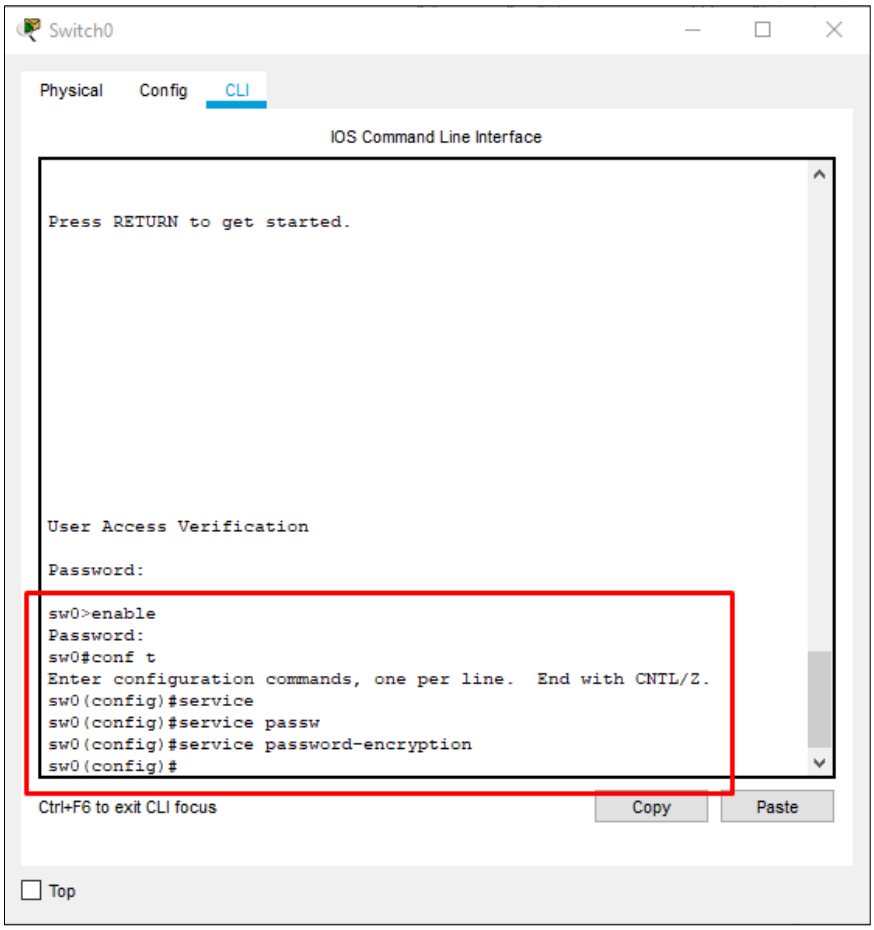
1) Choose the relevant device you wish to configure.
2) Open CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**enable secret *<PASSWORD>***".



- When trying to login to Privileged EXEC Mode, you'll be required to input a password.
- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with the password – "***1234***"

Setting a General Password Encryption

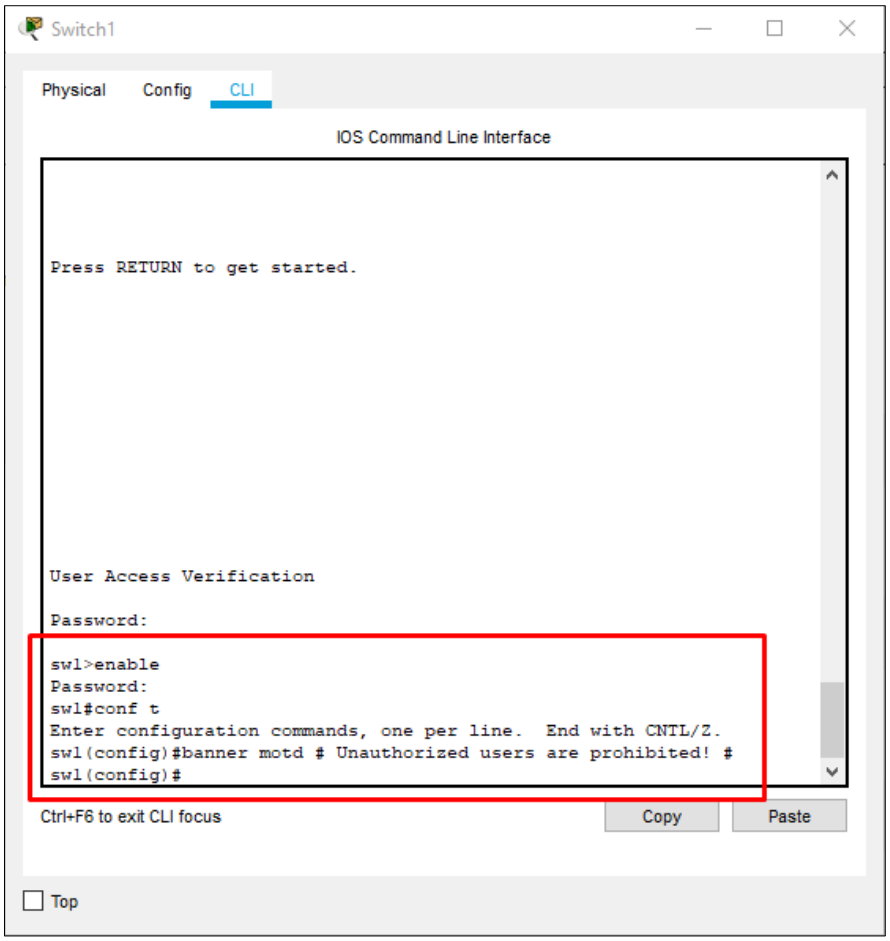
1) Choose the relevant device you wish to configure.
2) Open CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**service password-encryption**".



- When trying to review your passwords, you'll see they are all encrypted.
- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with this command.

Setting A Banner

1) Choose the relevant device you wish to configure.
2) Open CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**banner motd # *<CONTENT>* #**".



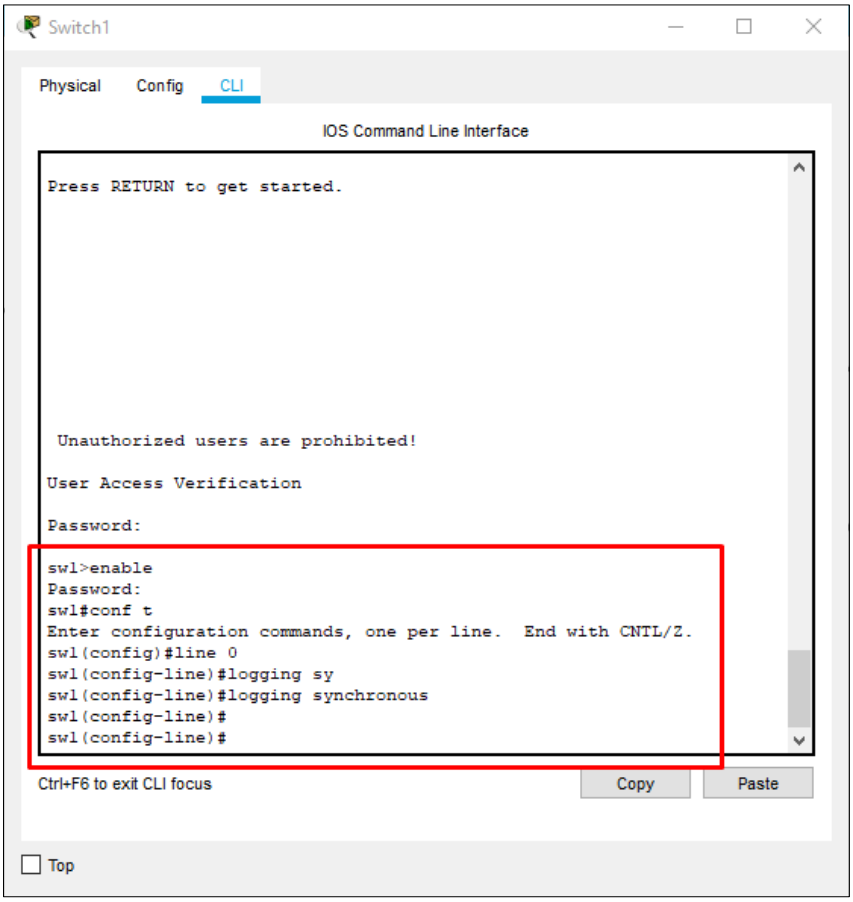
- When trying to login, you'll the message we configured.
- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with this message- "**Unauthorized users are prohibited!**"

Setting A Messages Display Sync

For this section you have two main options available;

Using "logging synchronous"

1) Choose the relevant device you wish to configure.
2) Open CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input a line command like "**line <vty/console/aux> *<NUMBER>***".
6) Input "**logging synchronous**"

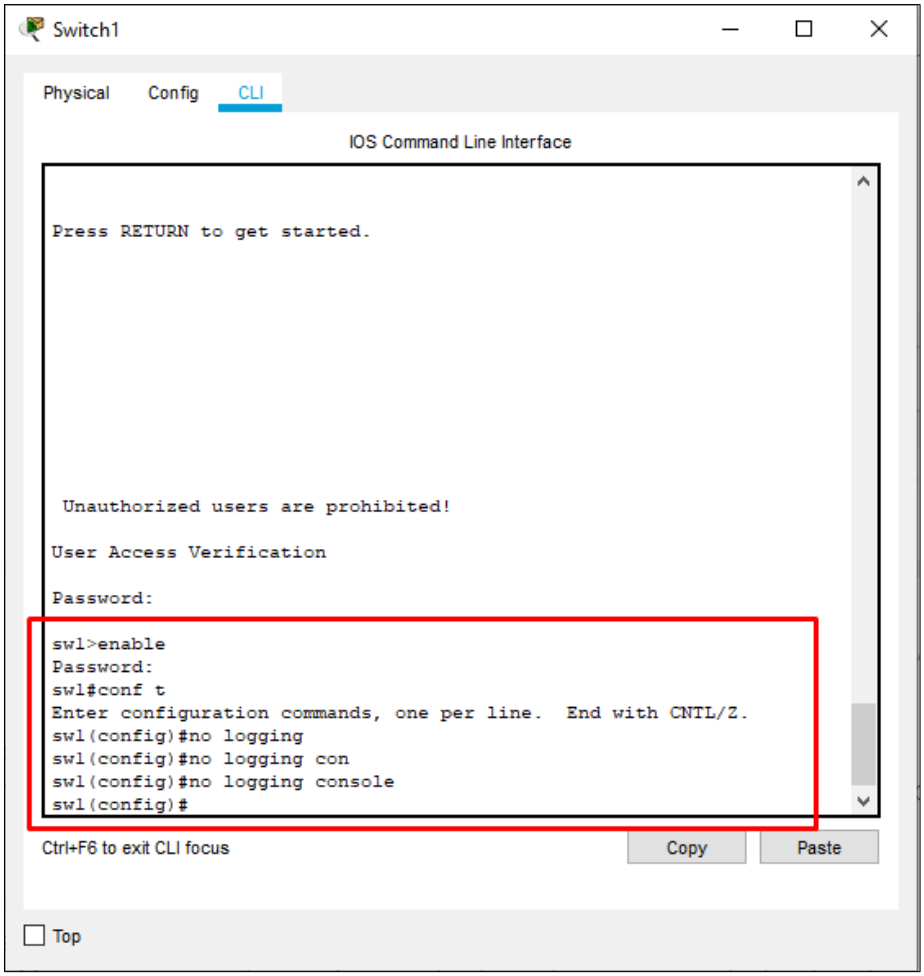


- This command will tell the router that if any informational items get displayed on the screen, your prompt and command line should be moved to a new line, so as not to confuse you. The informational line does not get inserted into the middle of the command you are trying to type. If you were to continue typing, the command would execute properly, even though it looks wrong on the screen.

- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with this command.

Using "no logging console"

1) Choose the relevant device you wish to configure.
2) Open the CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**no logging console**".

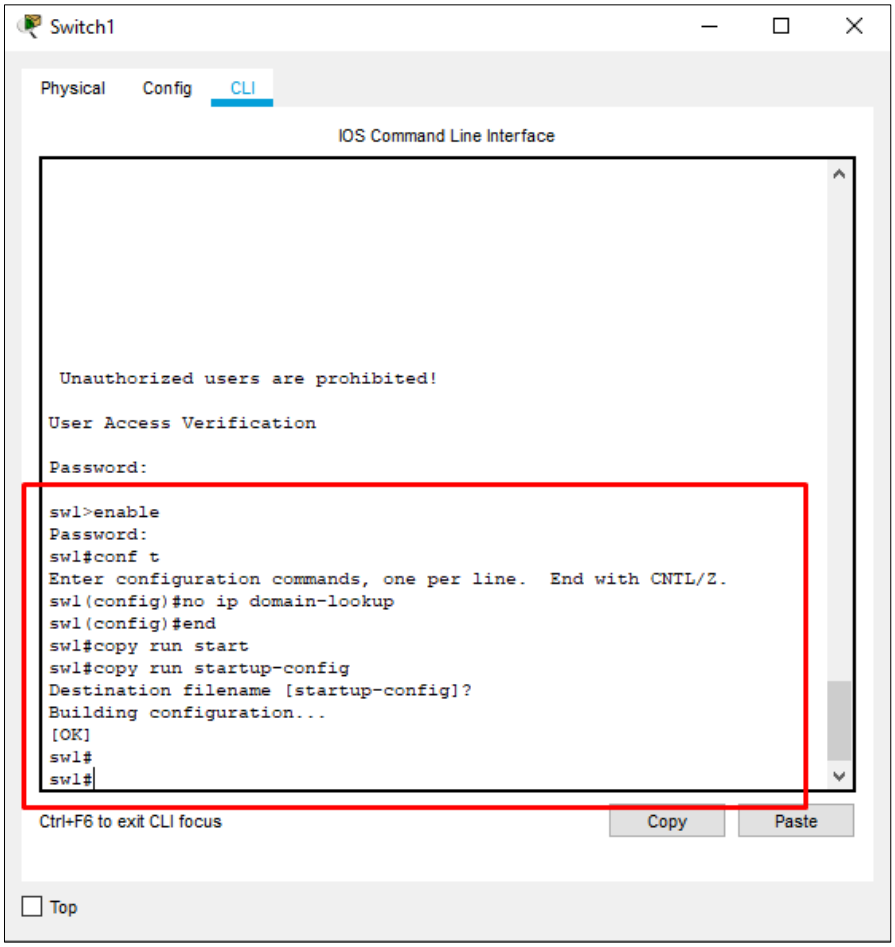


- This command turns off logging to the console connection and helps preventing security risks.

Setting A Wrong Input Wait Prevention

This command will prevent the wait from accidently input a wrong command in the CLI.

1) Choose the relevant device you wish to configure.
2) Open the CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**no ip domain-lookup**".
6) Input "**end**"
7) Input "**do w**".
8) Press enter until the process is complete.



- The "**no ip domain-lookup**" command disabled the auto domain lookup the router preforms by default when we type a wrong input.
- In order to correctly follow this tutorial, make sure to configure all the Switches and Routers available with this command.

VLAN:

In this section we'll set VLAN connections for our topology.

- Virtual Local Area Network (VLAN)- VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. VLAN can greatly simplify network design and deployment.

- Native VLAN- Also called VLAN1, is the default VLAN configuration for a port when it wasn't associated with a specific VLAN ID and Name. Some of the commands you'll see in this section can also be applied on Native VLAN, for additional information please refer to additional resources (Link1, Link2).

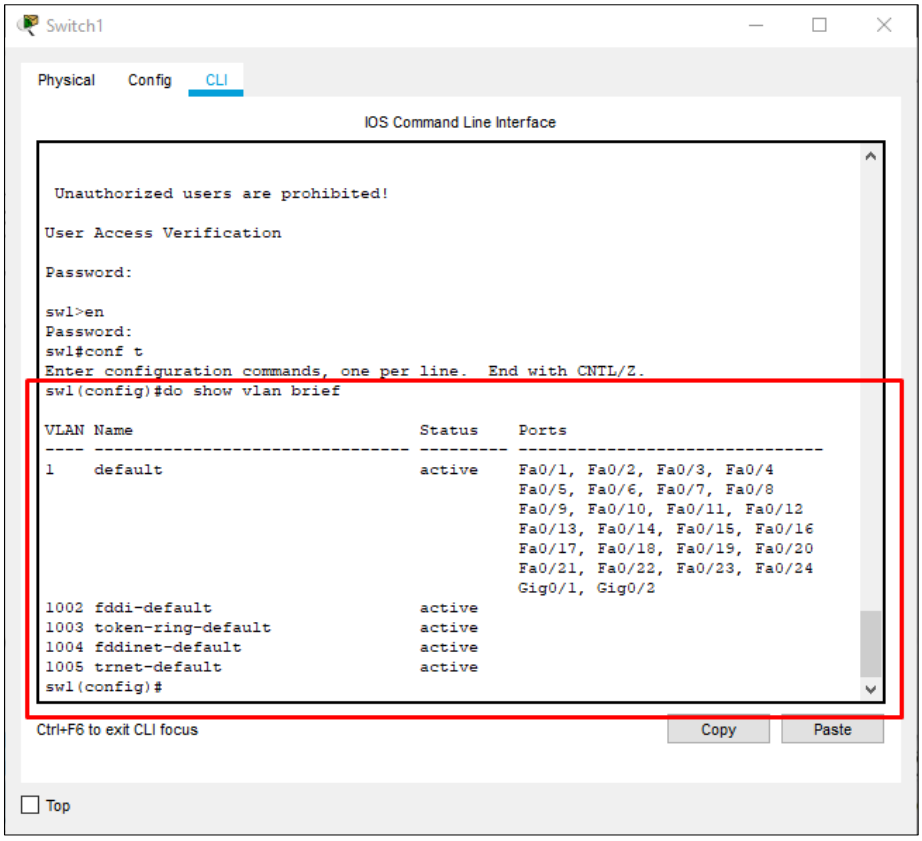
- Access- A connection mode for ports, can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.

- Trunk- A connection mode for ports, can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

- Router On a Stick (ROS)- A router that has a single physical or logical connection to a network. ROS is needed where one or more VLANs require routing between them.

General Port configuration

1) Choose the relevant Switch you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**do show vlan brief**".



- As default, all the interfaces are connected to VLAN1.
- This command will show you the connections.
- In this tutorial we already provided you with connections between devices.
- In order to view the ports for each connection;
  - i. In Packet Tracer, at the top left corner, press on "**Options**"
  - ii. Choose "**Preferences**"
  - iii. Mark "**Always Show Port Labels in Logical Workspace**"

6) Input "**vlan *<NUMBER>***"
   - This action will configure the VLAN ID.
7) Input "**name *<NAME>***"
   - This action will configure the VLAN Name.
   - Input "**exit**" once you are done.

8) Input "**interface range *<INTERFACE-NAME>* 0/*<RANGE>***"

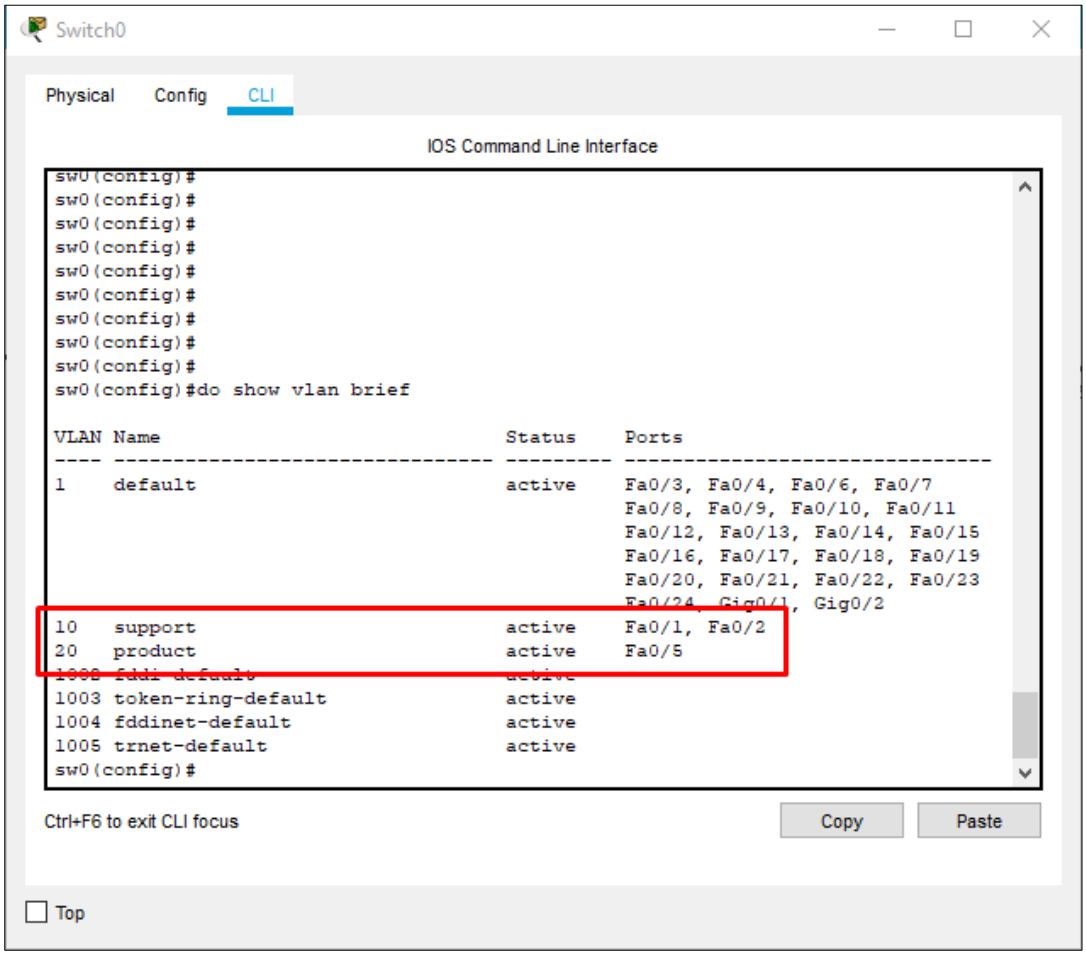
- You can also use the interface command for a single port.

9) Input "**switchport mode *<MODE>***"

- For this command, you can choose either "**access**"/"**trunk**"/"**vntag**"
- Generally, for "ordinary" connections we'll choose "**access**" mode.

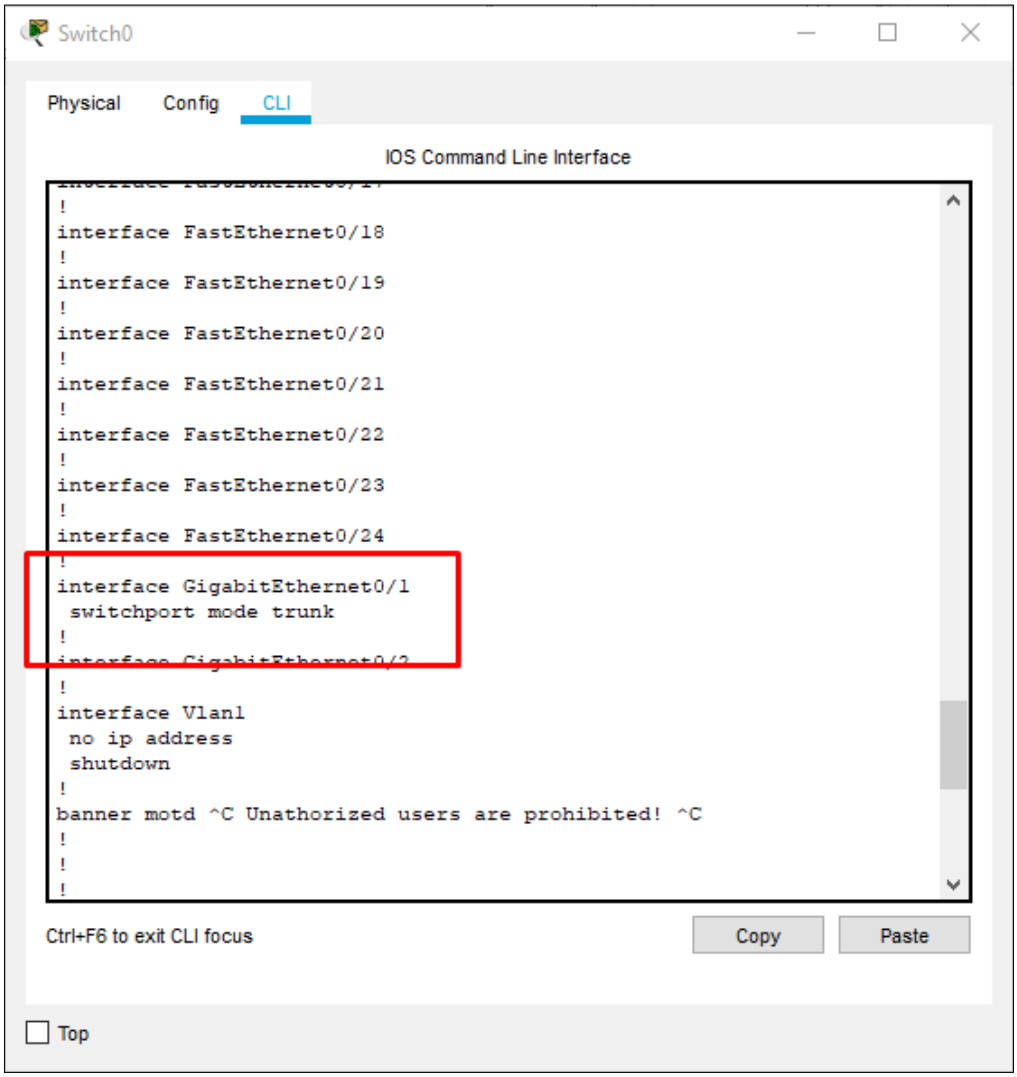
10) Input "**switchport *<MODE>* vlan *<ID>***"

- This command will assign the interface to the relevant VLAN.
- Use the "**do show vlan brief**" again to make sure the process was done correctly;



Trunk

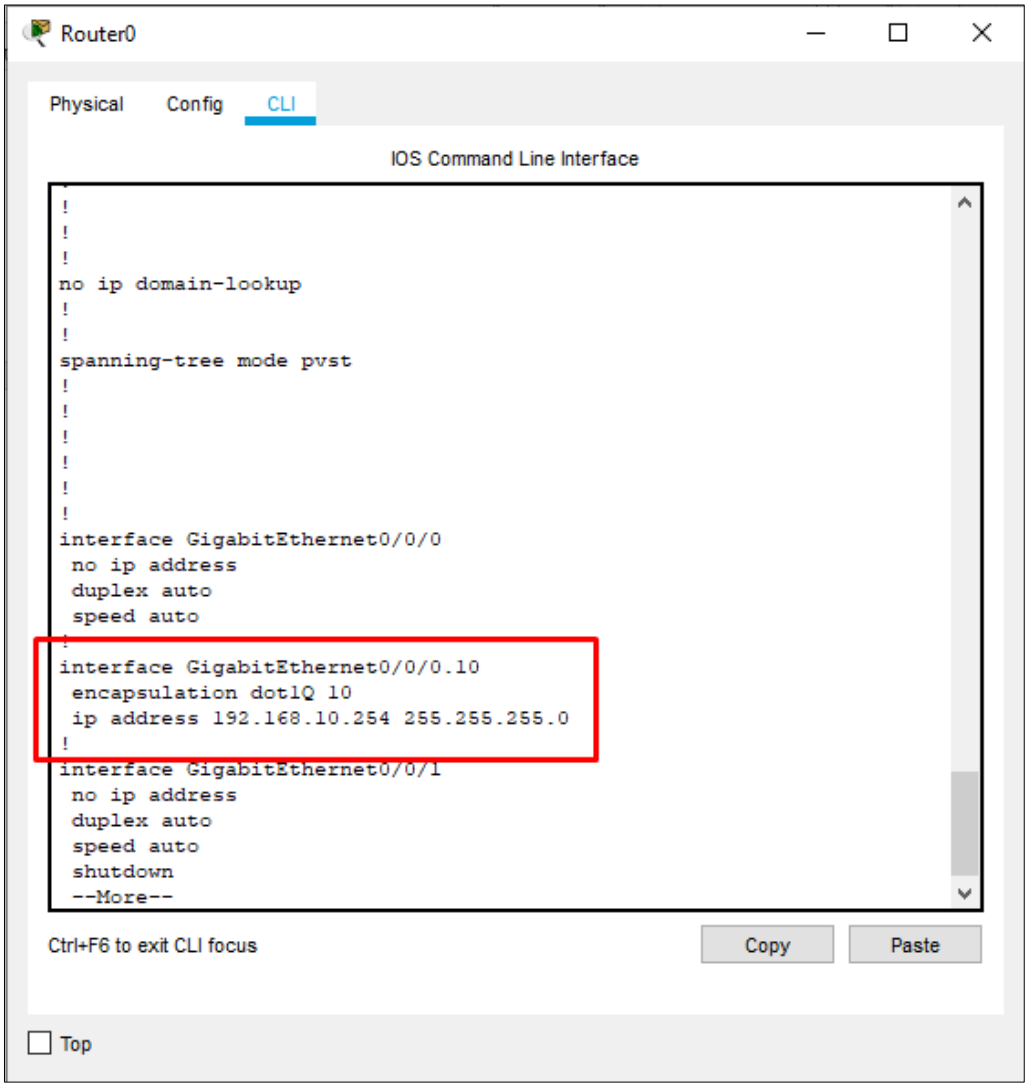
1) Choose the relevant device you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**interface *<INTERFACE-NAME>* 0/*<NUMBER>***"
6) Input "**switchport mode trunk**"
    - Trunk can be applied on a Port without a specific ID or Name to be used.
    - You can also make sure the native vlan is using Trunk by inputting; "**switchport *<Mode>* native vlan *<ID>***"
7) Input "**do show run**"
    - If you followed the process correctly, the following should be displayed;



Router On a Stick

1) Choose the relevant Router you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**interface *<INTERFACE-NAME>* 0/*<NUMBER>***"
6) Input "**no shutdown**"
7) Input "**exit**"
8) Input "**interface *<INTERFACE-NAME>* 0/*<NUMBER>*.*<ID>***"
9) Input "**encapsulation dot1q *<ID>***"
10) Input "**ip address *<IP>* *<SUBNET>***"
11) Input "**do show run**"

- If you followed the process correctly, the following should be displayed;



DHCP

In this section we'll apply the settings we need in order to make sure we have a proper DHCP usage for our network.

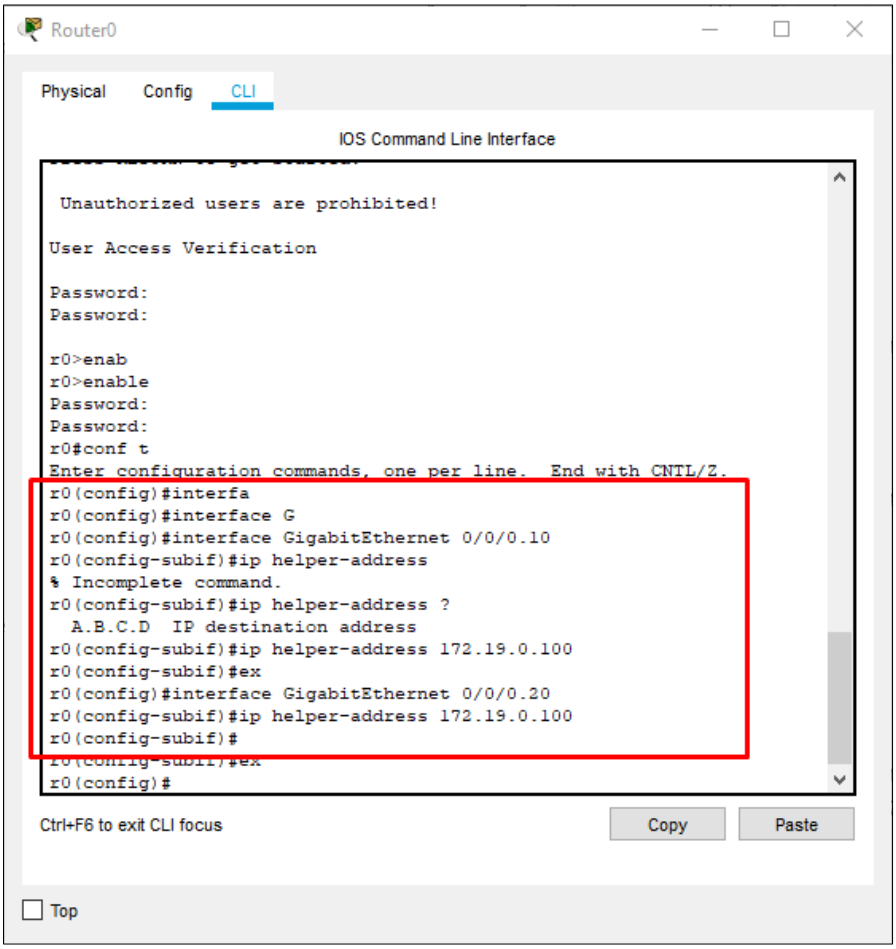
- Dynamic Host Configuration Protocol (DHCP)- A network protocol used on IP networks that automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

- DHCP Relay Agent- Sits between a DHCP server and DHCP clients and allows the DHCP clients to obtain IP addresses from the DHCP server that is not configured on the same LAN. The relay agent is being configured on Routers.

Relay Agent

Optional, if you are using the DNS server with a DHCP service;

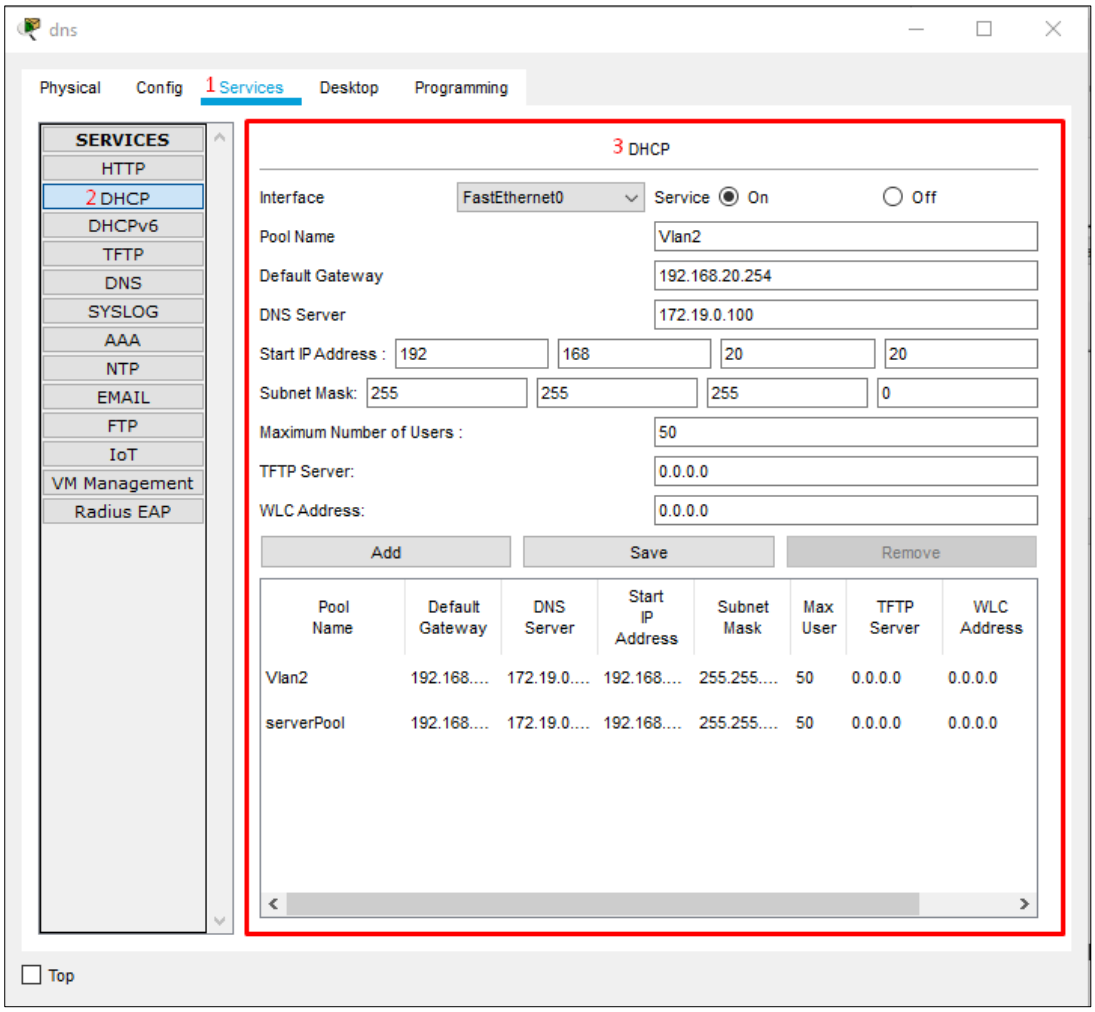
1) Choose the relevant Router you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**interface *<INTERFACE-NAME>* 0/*<NUMBER>*.*<ID>***"
6) Input "**ip helper-address *<DHCP-SERVER IP>***"



DHCP Server Configuration

Optional, if you are using the DNS server with a DHCP service;

1) Choose the relevant Server you wish to configure.
2) Under the "**Services**" tab, choose "**DHCP**" at the left options bar.
3) Input the pool details;

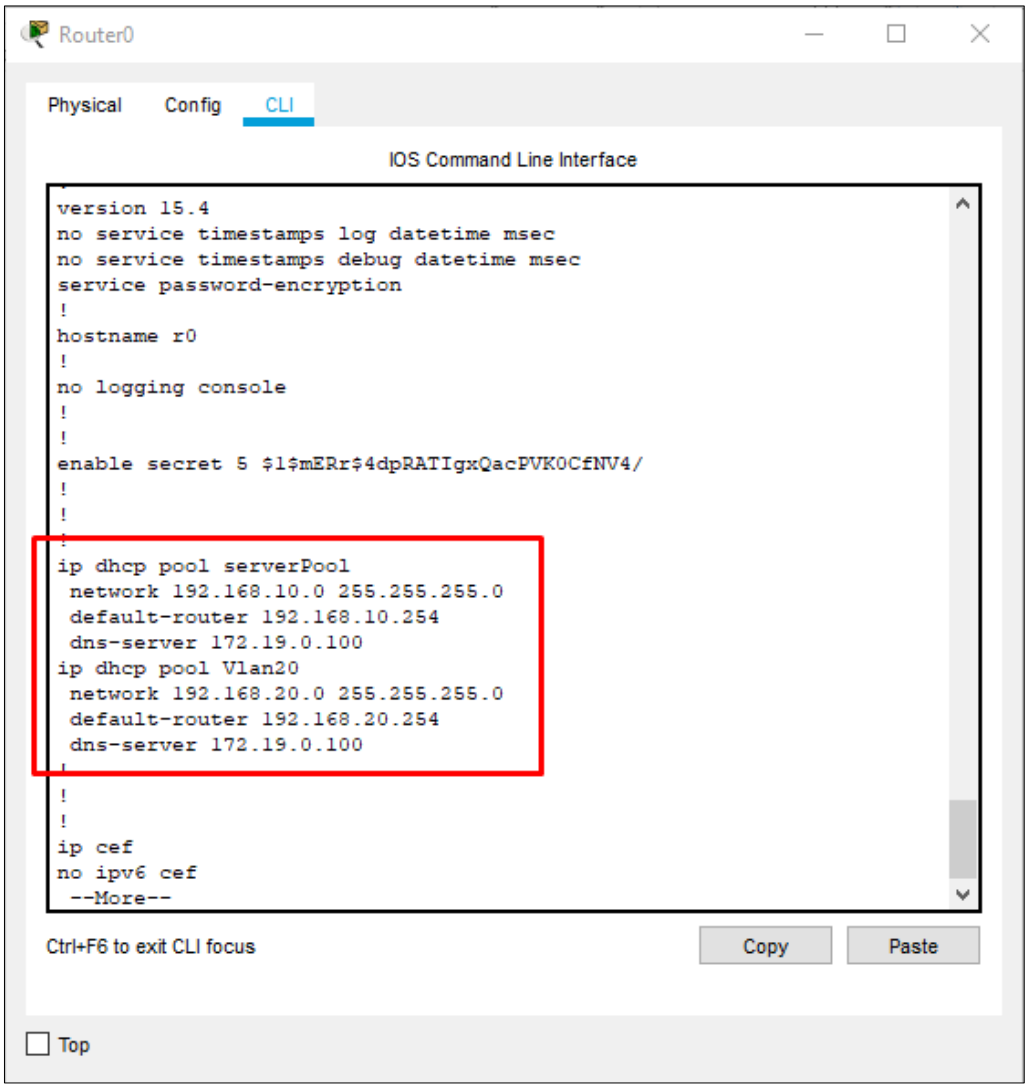


- The first Pool Name must remain "**serverPool**".
- Make sure the Service is marked as "**On**".

4) Press on "**Save**" when you are done or "**Add**" for adding a new pool configuration.

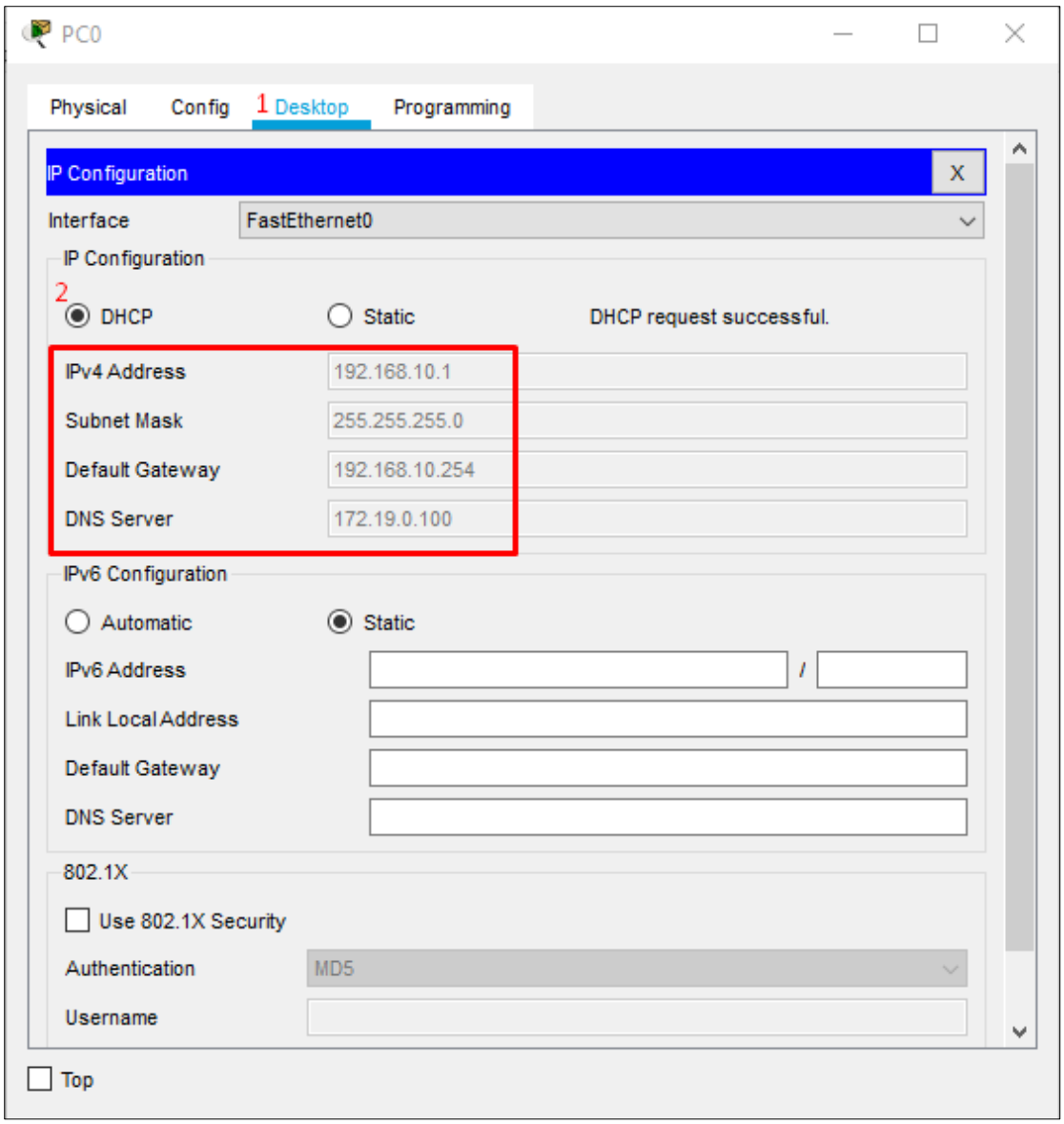
DHCP Router Configuration

1) Choose the relevant Router you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**"
5) Input "**service dhcp**"
6) Input "**ip dhcp pool *<POOL-NAME>***"
7) Input "**network *<IP> <SUBNET>***"
8) Input "**default-router *<GATEWAY>***"
9) Input "**dns-server *<DHCP-SERVER-IP>***"
    - Input "**exit**" when you are done.
10) Input "**do show run**"
    - If you followed the process correctly, the following should be displayed;



- If you correctly followed this tutorial until this point you should be able to get for all endpoint devices in the network an IP address;

  i. Choose an endpoint device.
  ii. Click on the "**Desktop**" tab.
  iii. Under the "**IP Configuration**", mark the "**DHCP**" option;



  - Before continuing with this tutorial, enable all endpoint devices are allocated with IP addresses.
  - For a more detailed review or in case of issues use the Simulation mode for troubleshooting.

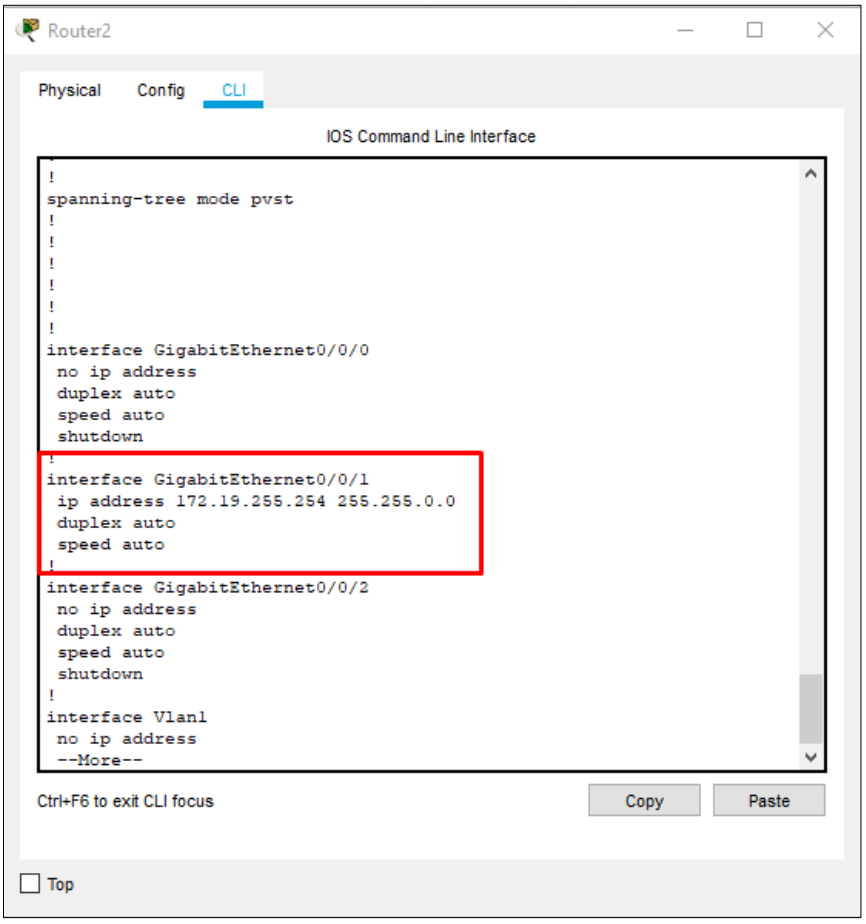
LAN2 Setup

In order to keep on with this tutorial, we'll need to apply some basic configuration in our LAN2 network first.

Router 2

For this Router, we'll be setting an IP address;

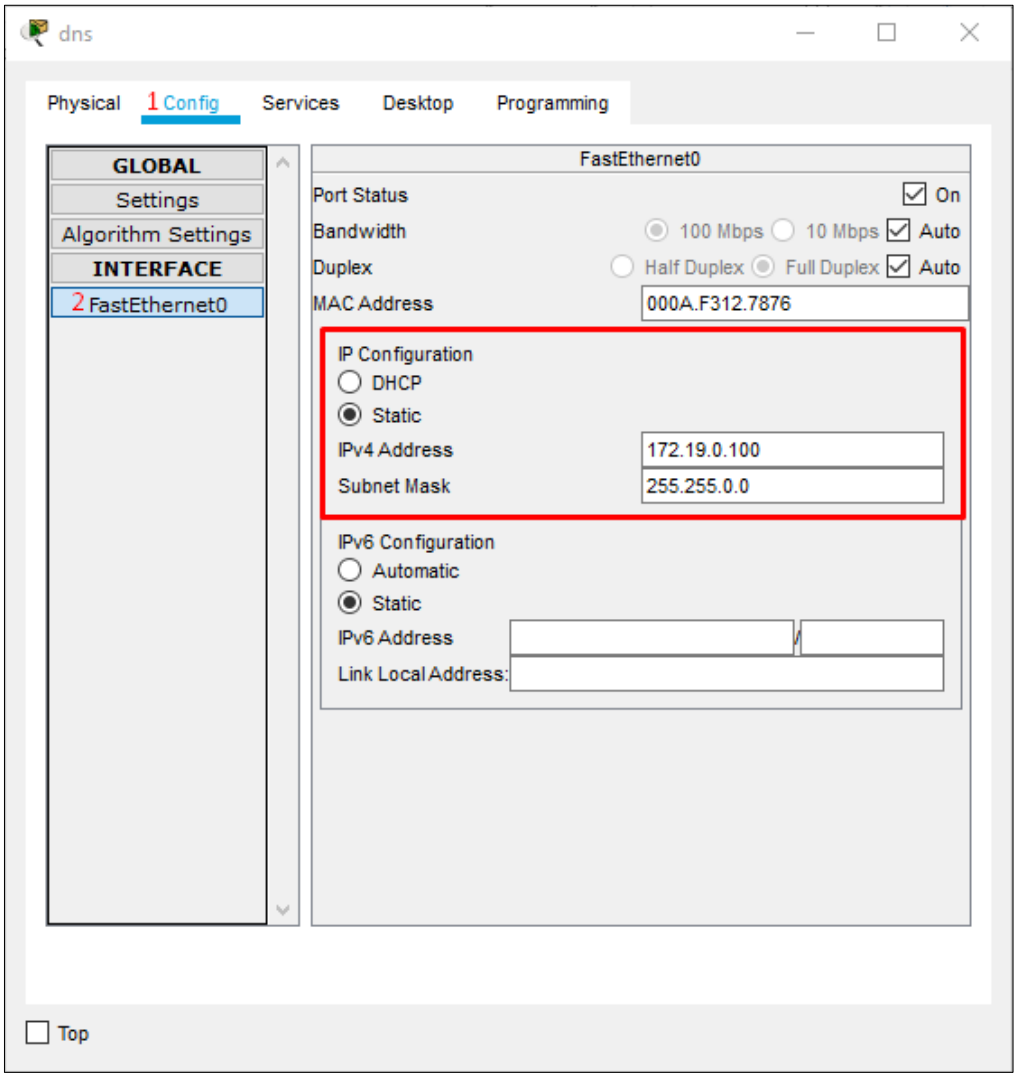
1) Click on Router2.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**"
5) Input "**interface gigabitEthernet 0/0/1**"
6) Input "**no shutdown**"
7) Input "**ip address *<IP> <SUBNET>***"
    - Input "**exit**" when you are done.
8) Input "**do show run**"
    - If you followed the process correctly, the following should be displayed;



DNS Server

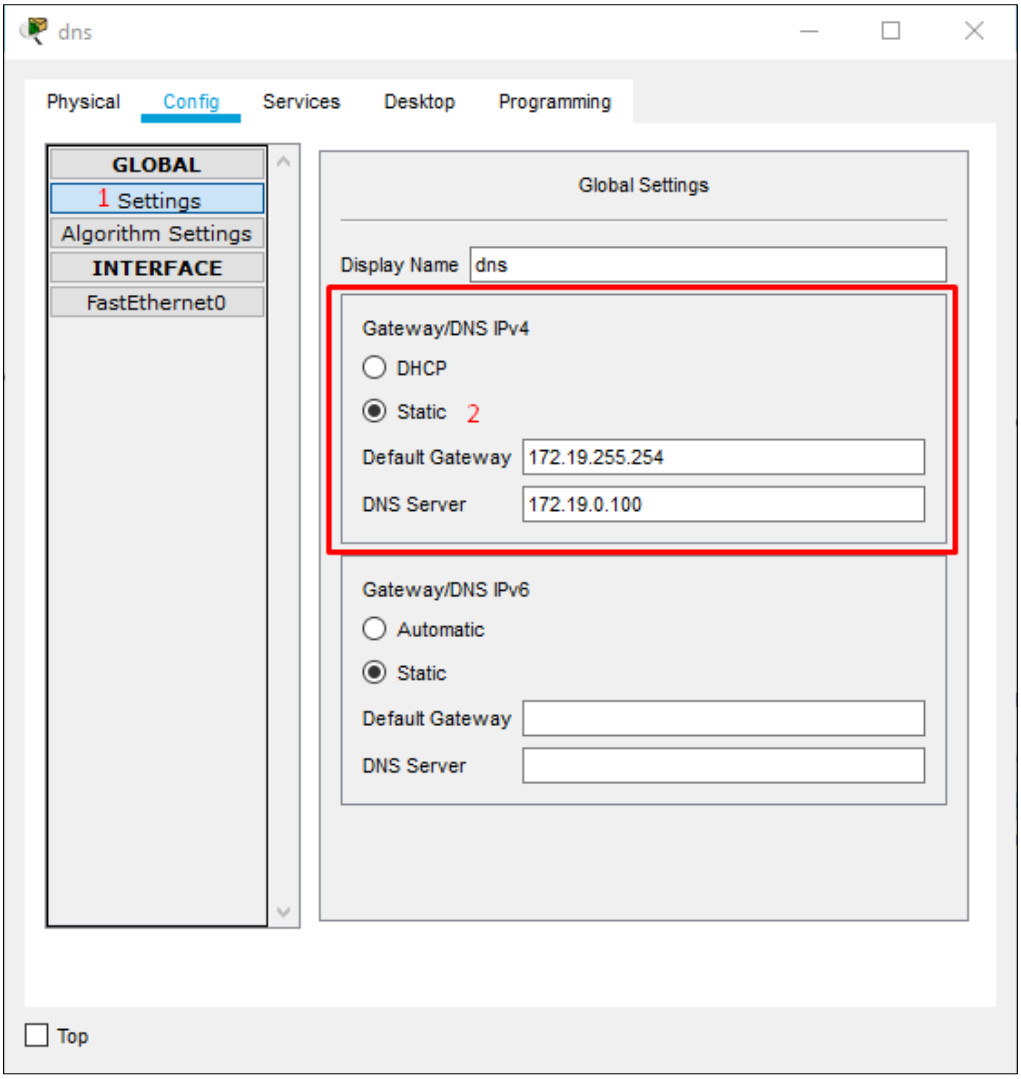
For this server we'll set network configurations and an A Record.

1) Click on the DNS server.
2) Under the "**Config**" tab, choose "**FastEthernet0**" at the left options bar.
3) Input the DNS IP address and Subnet according to the Topology section;



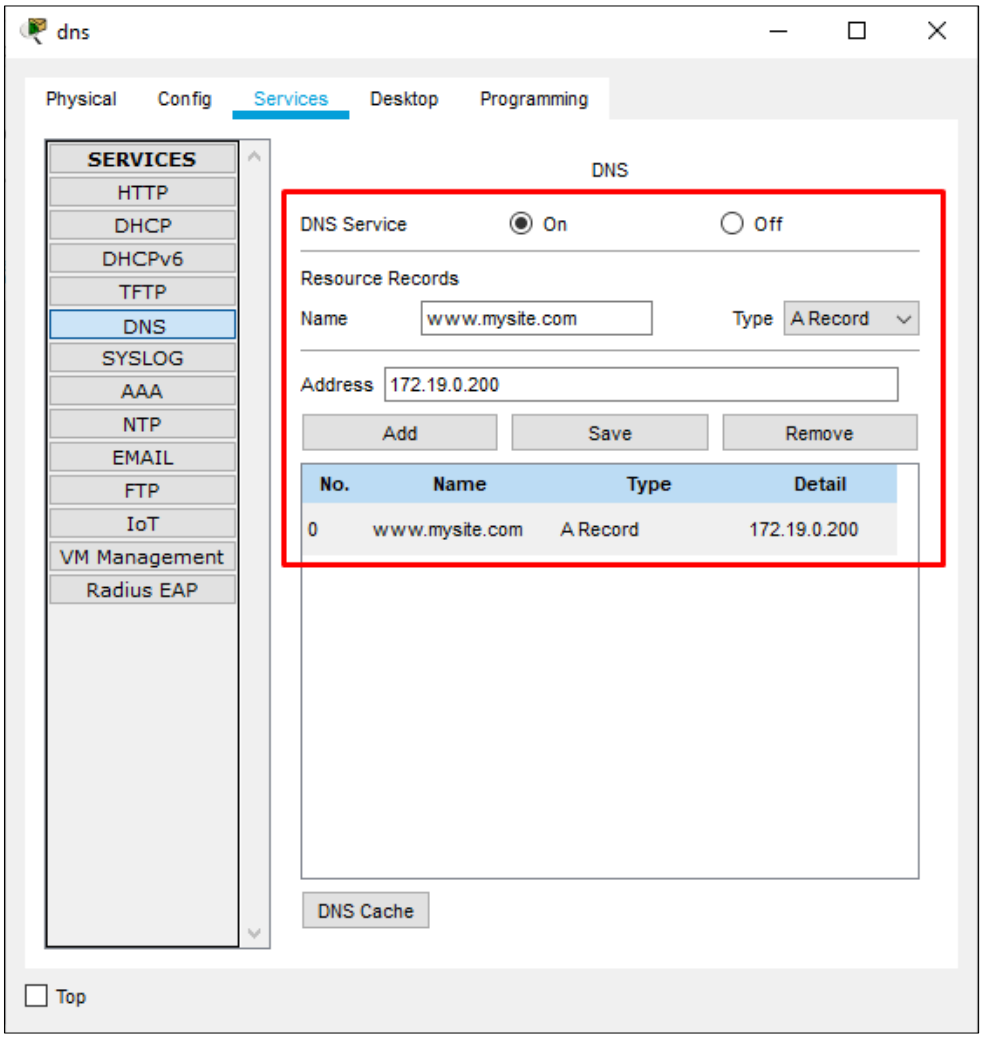
[Next Page]

4) At the left bar, press on "**Settings**" and input the Default Gateway and DNS Server according to the Requirements & Topology section;



[Next Page]

5) Next, under the "**Services**" tab, choose "**DNS**" at the left options bar.
6) Input the A Record credentials according to the Requirements & Topology section;

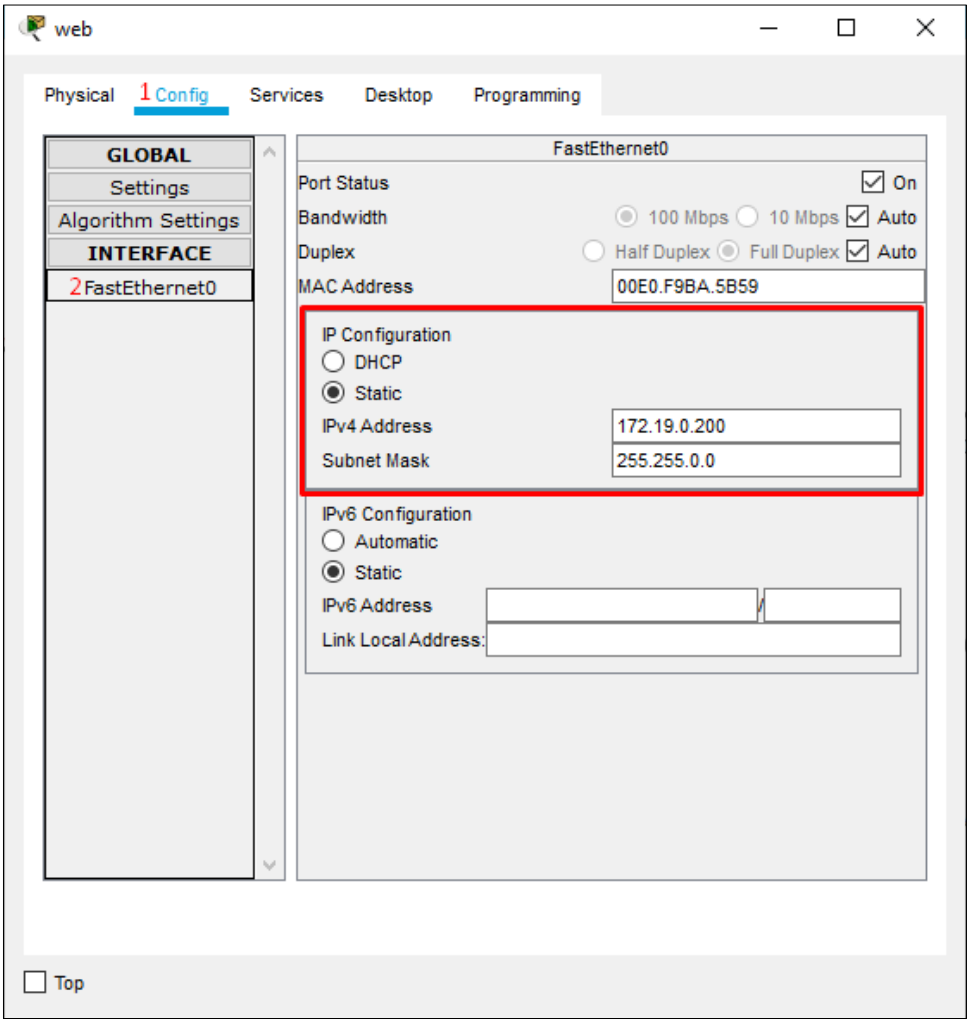


- Press on "**Save**" when you are done.

Web Server

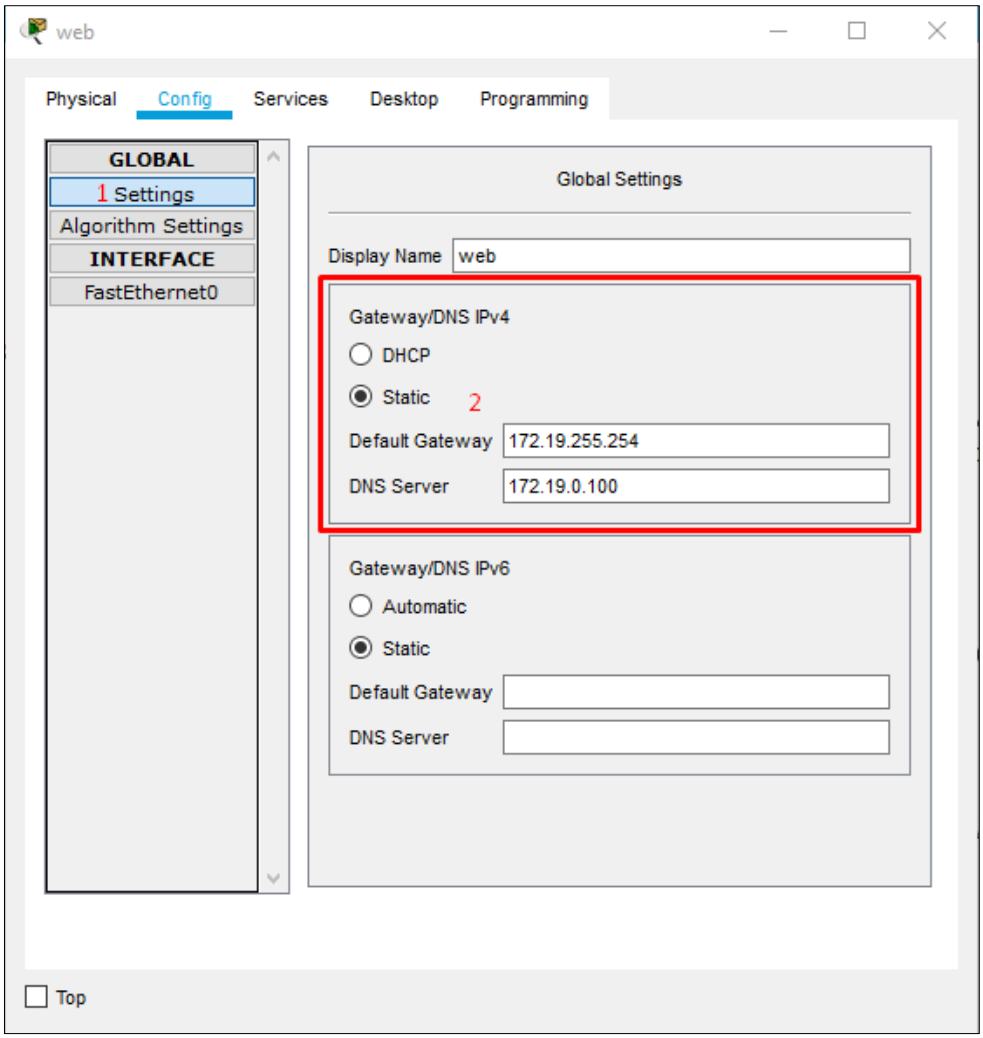
For this server we'll set network configurations

1) Click on the Web server.
2) Under the "**Config**" tab, choose "**FastEthernet0**" at the left options bar.
3) Input the Web IP address and Subnet according to the Requirements & Topology section;



[Next Page]

4) At the left bar, press on "**Settings**" and input the Default Gateway and DNS Server according to the Requirements & Topology section;

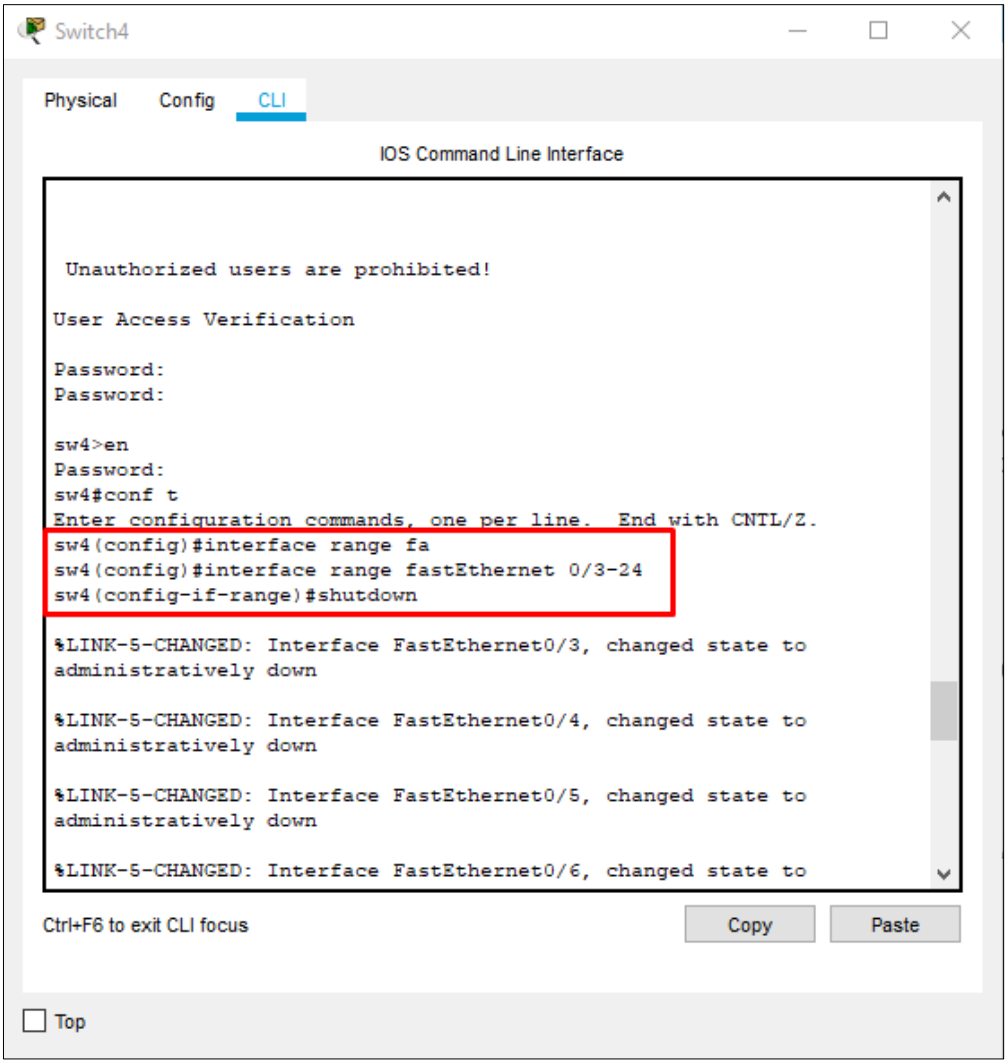


Port Security

In this section we'll secure our LAN2 network in order to make sure any 3rd party unwanted entities won't be able to access it.

Disabling Interfaces

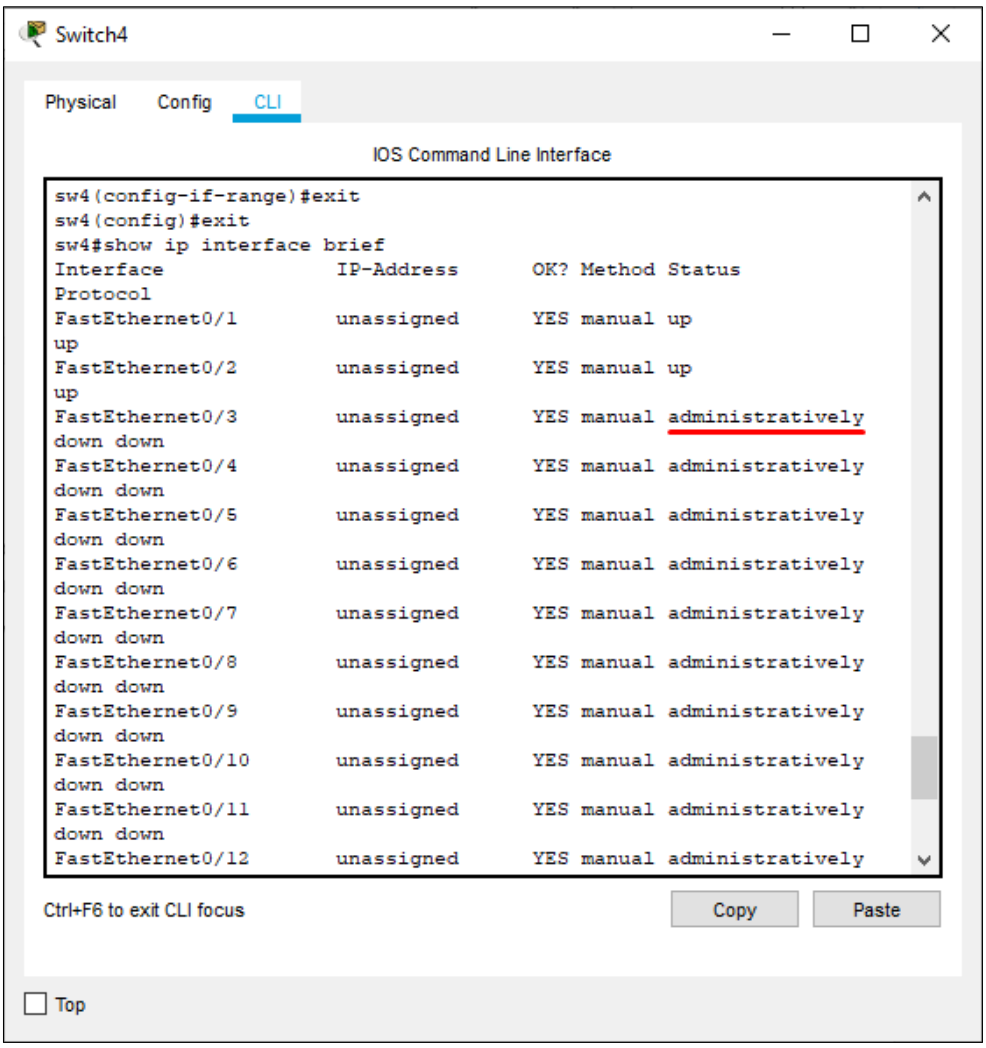
1) Choose the relevant Switch you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**interface range *<INTERFACE>* 0/*<RANGE>***"
6) Input "**shutdown**"



[Next Page]

7) Input "**exit**" until you reach Privileged EXEC mode.
8) Input "**show ip interface brief**"

- If you followed the process correctly, the following should be displayed;



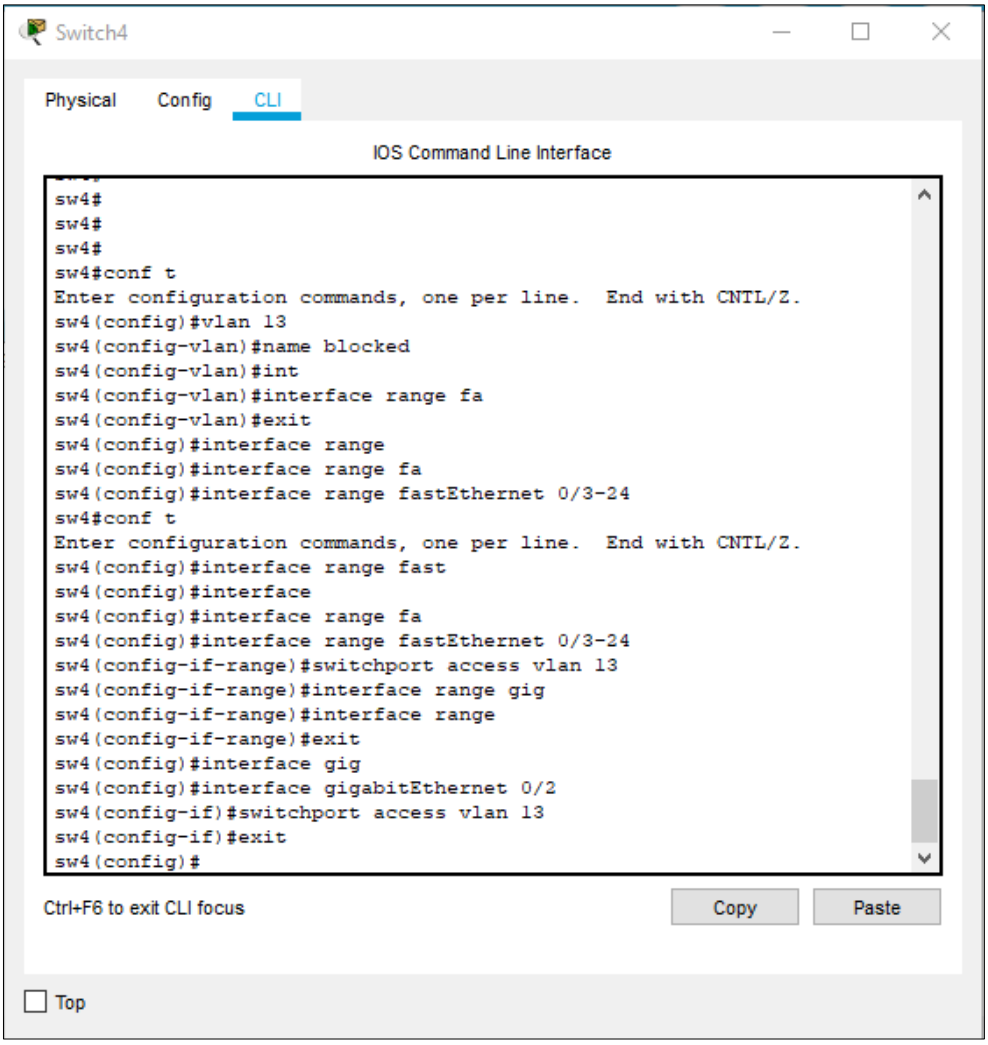
- In order to correctly follow this tutorial, make sure that all the inactive interfaces on Switch4 are disabled.

[Next Page]

9) Re-enter Global mode by pressing "**conf t**"
10) Input "**valn *<NUMBER>***"
11) Input "**name *<NAME>***"

- Input "**exit**" when you are done

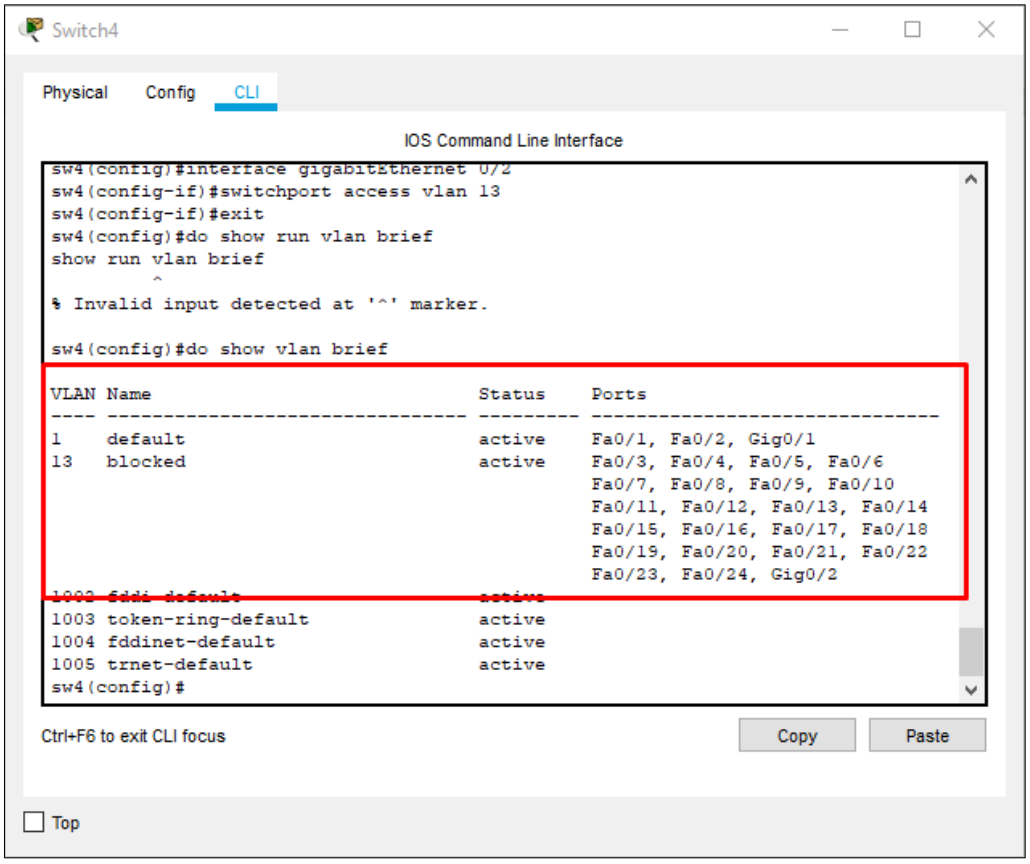
12) Input "**interface range *<INTERFACE>* 0/*<RANGE>***"
13) Input "**switchport access vlan 13**"



[Next Page]

14) Input "**do show vlan brief**"

- If you followed the process correctly, the following should be displayed;



Limiting Interface Access

1) Choose the relevant Switch you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**interface *<INTERFACE>* 0/*<NUMBER>***"
6) Input "**switchport mode access**"
    - The interface must be in access mode in order for port security to be active.
7) Input "**switchport port-security**"
8) Input "**switchport port-security violation *<shutdown/restrict/protect>***"
    - For this tutorial, we'll be using the restrict option.
9) Input "**switchport port-security maximum *<NUMBER>*"**
    - This command limits the number of devices that can use the interface.
10) Choose the method in which you would like the devices using the switch will be recorded;
    a) Input "**switchport port-security mac-address sticky"**
        - This command ensures that the MAC addresses that are accessing through the relevant interface will be saved by the switch.
    b) Input "**switchport port-security mac-address *<MAC>*"**
        - This command will enable specific MAC address/es to use the interface.
11) After finishing with the configurations, input "**copy running-config startup-config**" in order to save your work.
12) Input "**show port-security interface *<INTERFACE>* 0/*<NUMBER>***"
    - If you followed the process correctly, the following should be displayed;

[Next Page]

Switch4

Physical Config CLI

IOS Command Line Interface

```
sw4#show port-security interface gigabitEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

sw4#show port-security interface fa
sw4#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

sw4#show port-security interface fastEthernet 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

sw4#
```

Ctrl+F6 to exit CLI focus Copy Paste

Top

- Any unauthorized device, will not be able to access the LAN2 network. In order to test this, connect another device to the network and try sending a ping to other devices in Simulation mode.

OSPF

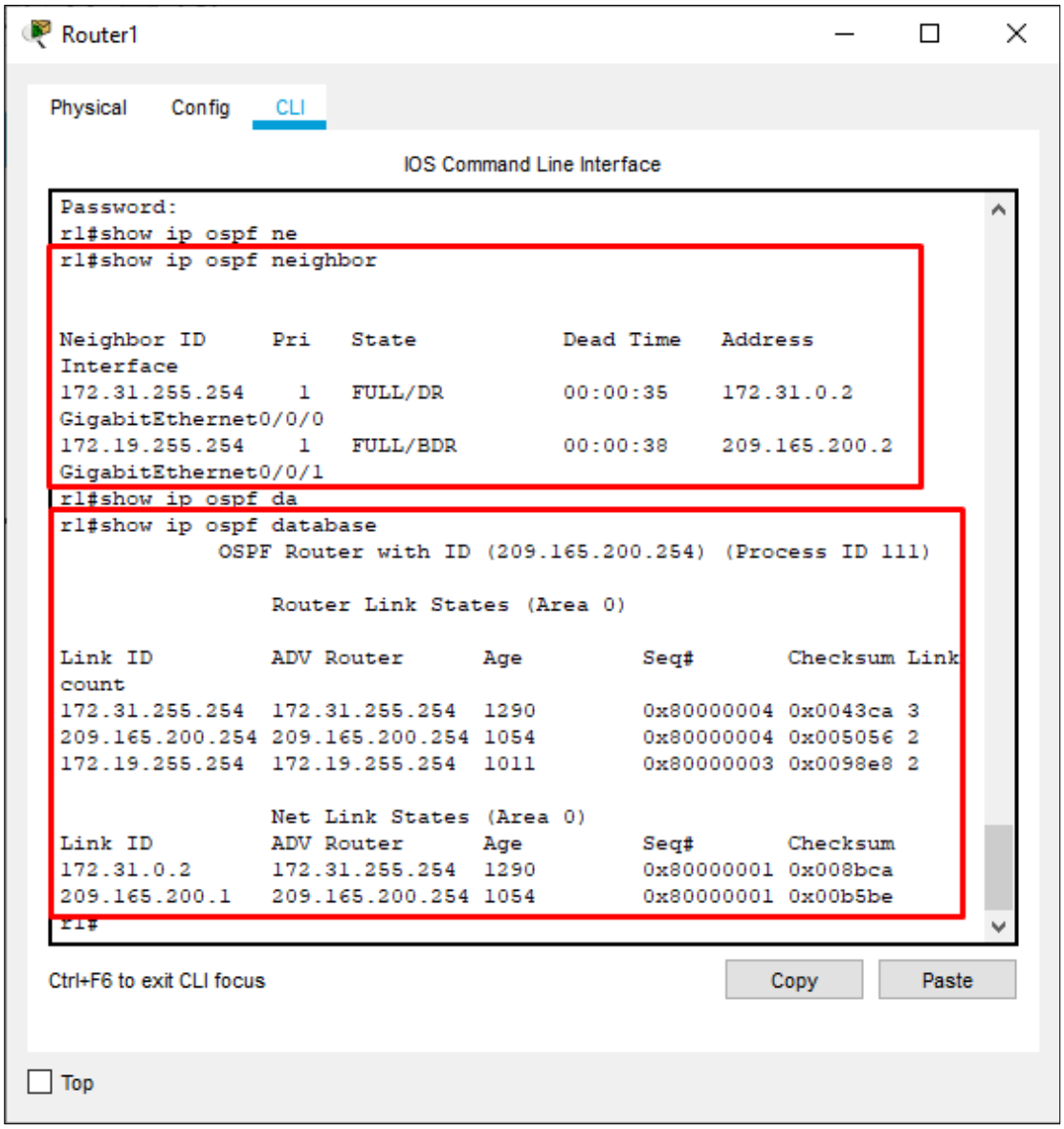
In this section we'll use the OSPF protocol in order to make sure all of our routers are familiar with the available networks.

- Open Shortest Path First (OSPF)- A protocol that is being based on the Link State routing protocol which enables routers in a network to build a "map" of all the connected networks.

Configuration

1) Choose the relevant Router you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**"
    - If needed, activate any interfaces that are currently shutdown and assign IP addresses to them according to the Topology section.
5) Input "**router ospf *<NUMBER>***"
    - Sets a process ID that's being identified by all the routers who use the same ID for sharing networks data.
6) Input "**passive-interface *<INTERFACE>* 0/*<NUMBER>***"
    - If required, this command excludes the selected interface from receiving requests that contain the networks that are affiliated with the router.
7) Input "**network *<NETWORK>* *<WILDCARD>* area *<NUMBER>***"
8) In Privileged EXEC mode, input "**show ip ospf ?**" in order to make sure the configurations were set correctly for the relevant router:

[Next Page]




```
Password:
r1#show ip ospf ne
r1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.31.255.254    1   FULL/DR         00:00:35    172.31.0.2
GigabitEthernet0/0/0
172.19.255.254    1   FULL/BDR        00:00:38    209.165.200.2
GigabitEthernet0/0/1
r1#show ip ospf da
r1#show ip ospf database
            OSPF Router with ID (209.165.200.254) (Process ID 111)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.31.255.254  172.31.255.254  1290        0x80000004 0x0043ca 3
209.165.200.254 209.165.200.254 1054        0x80000004 0x005056 2
172.19.255.254  172.19.255.254  1011        0x80000003 0x0098e8 2

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.31.0.2      172.31.255.254  1290        0x80000001 0x008bca
209.165.200.1   209.165.200.254 1054        0x80000001 0x00b5be
r1#
```

- Any request being currently sent from our devices in LAN1 will be able to reach LAN2 devices. In order to test this, switch a device to a IP configuration to DHCP and send a ping request to a device in LAN2, in Simulation mode.

ACL

In this section we'll apply some restrictions for our end devices.

- Access Control List (ACL)- provides basic traffic filtering capabilities with access control lists. You are able to configure it for all routed network protocols (IP, AppleTalk, and so on) to filter protocol packets when these packets pass through a device. Access lists can prevent certain traffic from entering or exiting a network.

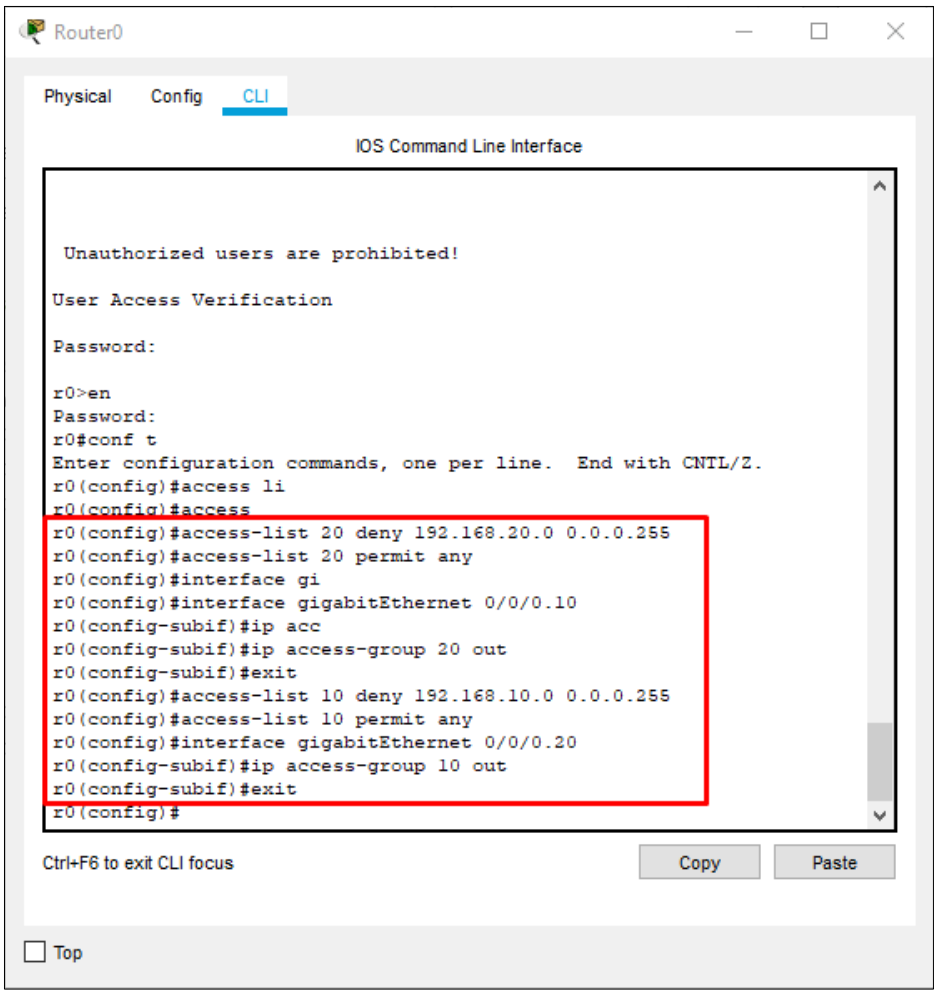
Device Interactions

1) Choose the relevant Router you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**"
5) Input "**access-list *<NUMBER> <ACTION> <NETWORK> <WILDCARD>***"
    - The above syntax is meant only for one type of ACL.
    - For this tutorial, use this command as many times as you need before continuing.
    - In the *<ACTION>* option, you can type: deny, permit or remark.
6) Input "**interface *<INTERFACE>* 0/*<NUMBER>***"

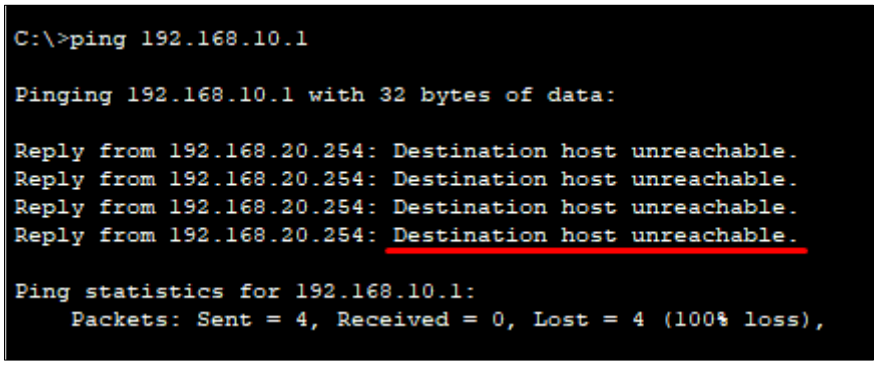
[Next Page]

7) Input "**ip access-group <NUMBER> <IN/OUT>**"

- Input "**exit**" once you are done.



8) If done correctly, when trying to ping an opposite device's IP network to the one you are currently using. The following message will be shown;



NAT

In this section we'll establish a NAT connection to our LAN2 environment.

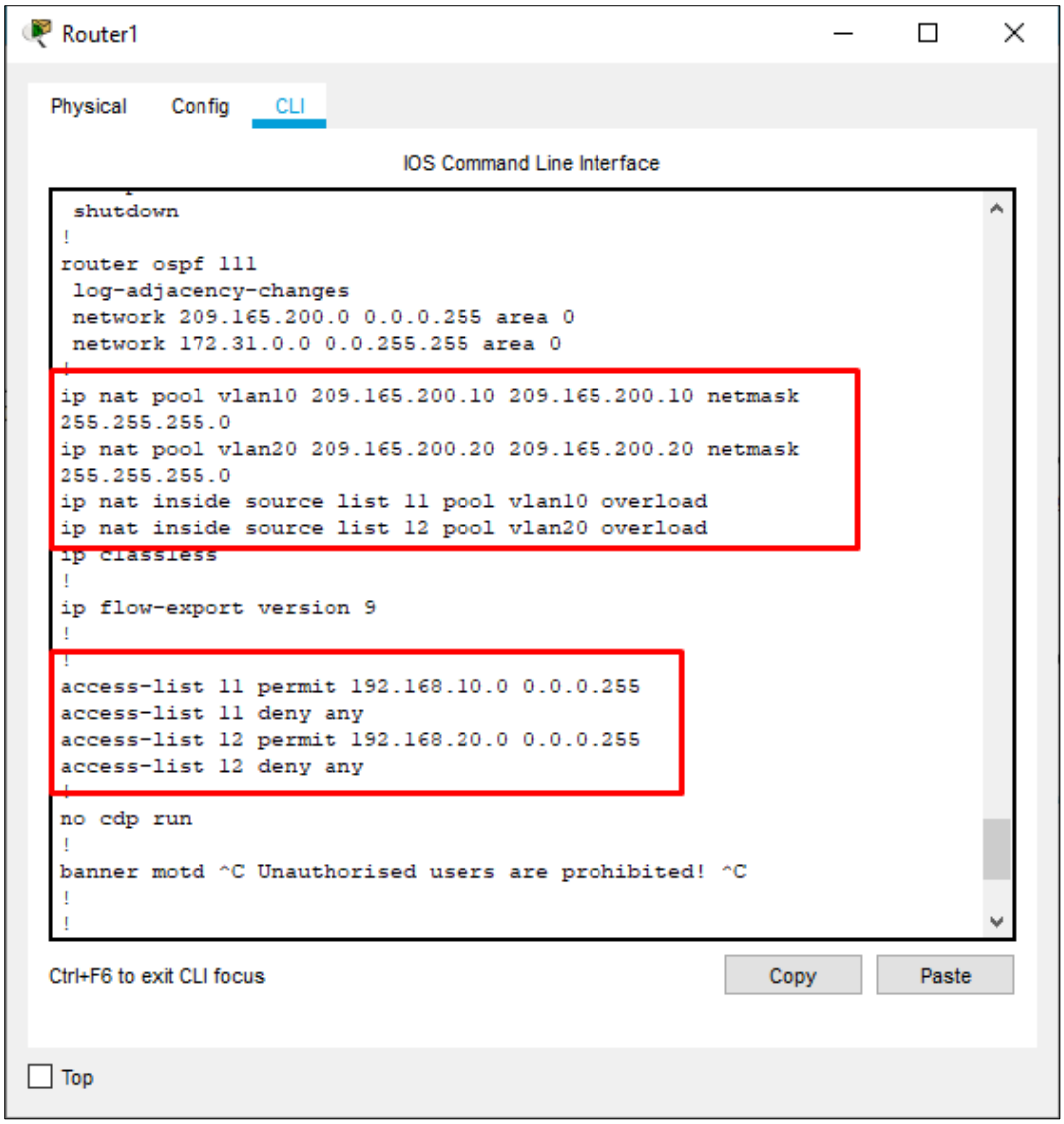
- Network Address Translation (NAT)- The process where a network device assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

NAT Overload

- NAT Overload- Also sometimes referred to as Port Address Translation (PAT), is an extension to NAT that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

1) Choose the relevant Router you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**"
5) Input "**interface *<INTERFACE>* 0/*<NUMBER>***"
6) Input "**ip nat *<outside/inside>***"
    - Make sure to repeat steps 5 and 6, both 'inside' and 'outside' environments need to be configured for a single router.
    - Type "**exit**" each time you are done with an interface.
7) Input "**access-list *<NUMBER> <ACTION> <NETWORK> <WILDCARD>***"
    - For this tutorial, use this command as many times as you need before continuing.
8) Input "**ip nat pool *<NAME> <IP-FROM> <IP-TO>* netmask *<SUBNET-MASK>***"
    - You can also enable NAT Overload (PAT) without defining a pool.
9) Input "**ip nat inside source list *<NUMBER>* pool *<NAME>* overload**"
10) Input "**do show run"**
    - If you followed the process correctly, the following should be displayed;

[Next Page]



In order to test the NAT Overload, ping a device in LAN2 from LAN1.
Then, input "**show ip nat translations"** in Privileged EXEC mode in order to review the actual conversion;

[Next Page]

Router1

Physical Config CLI

IOS Command Line Interface

```
!
!
!
line con 0
 password 7 08204E4D0D
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password 7 08204E4D0D

r1(config)#XIT
           ^
% Invalid input detected at '^' marker.

r1(config)#exit
r1#
%SYS-5-CONFIG_I: Configured from console by console

r1#show ip nat tra
r1#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
udp 209.165.200.10:1026192.168.10.1:1026  172.19.0.100:53     172.19.0.100:53
tcp 209.165.200.10:1026192.168.10.1:1026  172.19.0.200:80     172.19.0.200:80

r1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Wireless LAN Controller

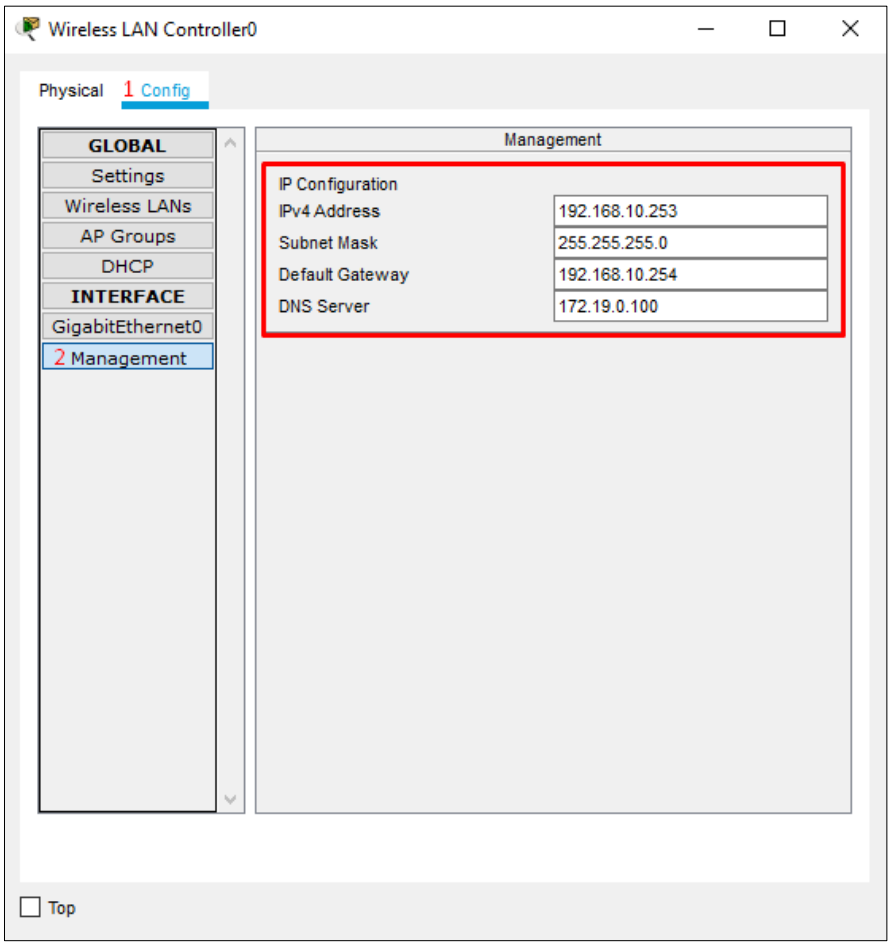
In this section we'll set configurations for establishing wireless connections foe end devices.

- Wireless LAN Controller (WLC)- A device that manages wireless network access points in terms deployment, performance, scalability, security and more.

- Wireless Access Point (WAP)- A networking hardware device that allows other Wi-Fi devices to connect to a wired network. As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself.

Device Settings

1) Click on the WLC device.
2) Under the "**Config**" tab, choose "**Management**".
3) Input the relevant credentials according to what is being listed in the Topology section.



Switch Settings

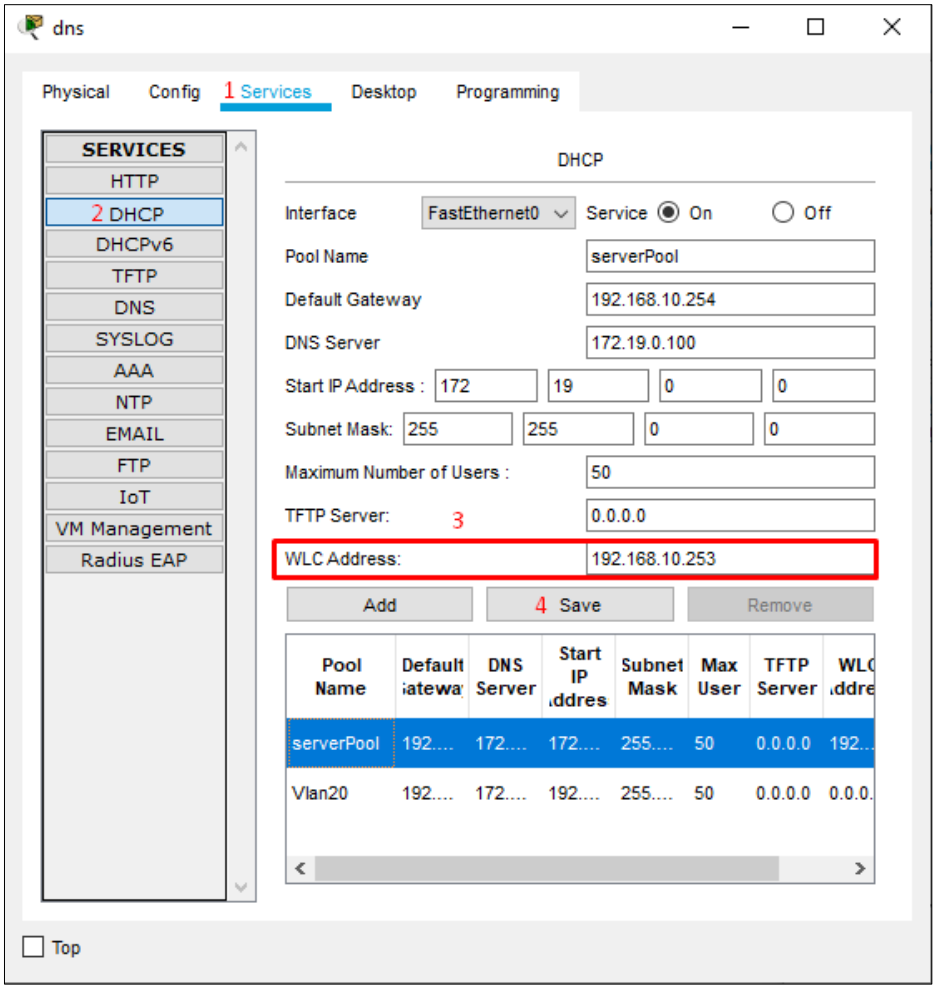
1) Choose the relevant Switch you wish to configure.
2) Open CLI Input.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**"
5) Input "**interface *<INTERFACE>* 0/*<NUMBER>***"
6) Input "**switchport mode *<MODE>***"
7) Input "**switchport *<MODE>* vlan *<NUMBER>***"

    - Repeat this process, for configuring all the interfaces that are connected to the WLC and WPA.

DHCP Settings

Optional, if you are using the DNS server with a DHCP service;

1) Choose the relevant Server you wish to configure.
2) Under the "**Services**" tab, click on "**DHCP**" at the left bar.
3) In the "**WLC Address**" field, input the WLC IP address;



- Press on the "**Save**" button once you are done.

Browser Settings

In order to begin this section, you must first send a ping request from PC5 to WLC in order to update the network ARP tables and to make sure you'll be able to send TCP request to the WLC;

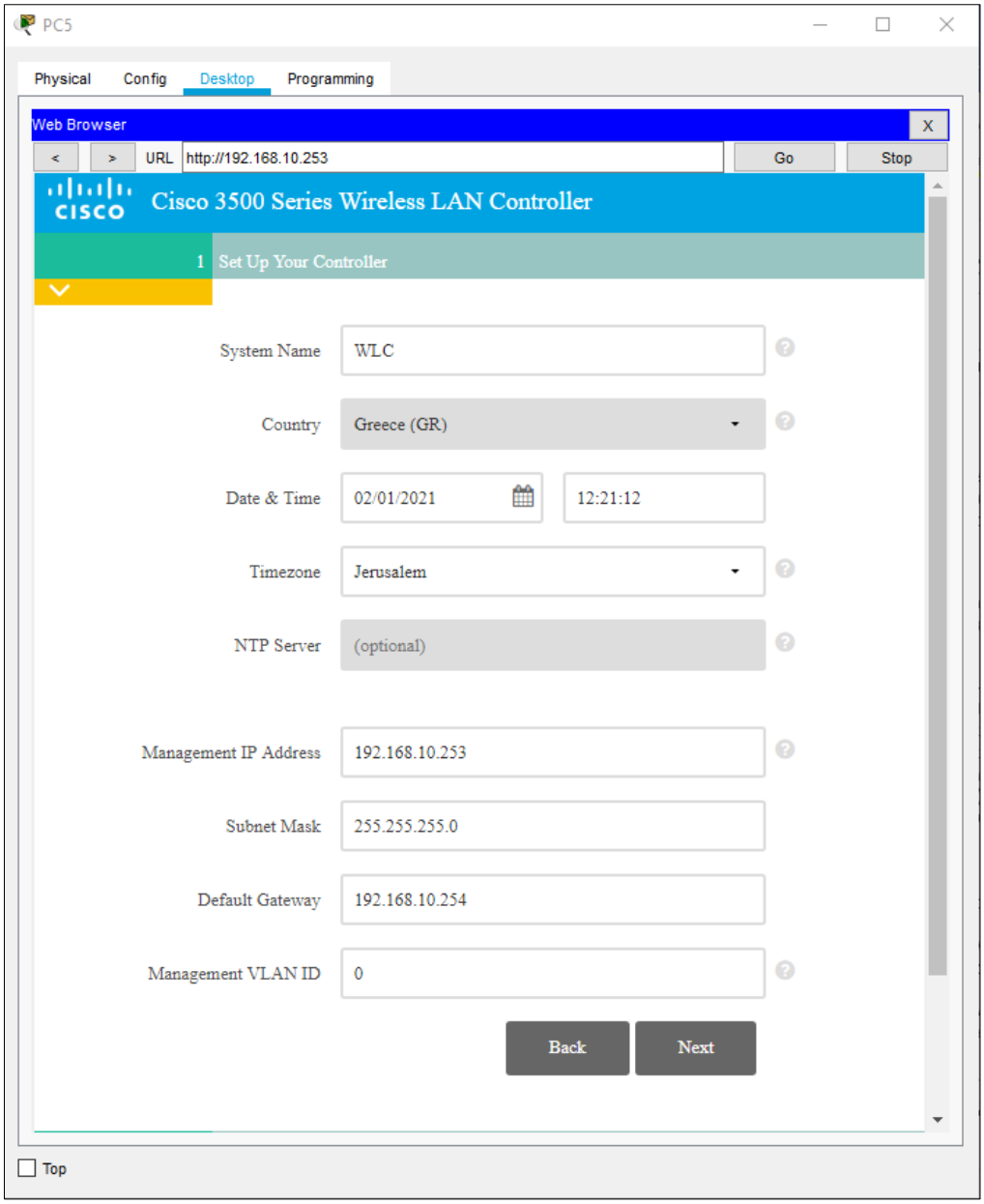
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.253

Pinging 192.168.10.253 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.253: bytes=32 time<1ms TTL=255
Reply from 192.168.10.253: bytes=32 time<1ms TTL=255
Reply from 192.168.10.253: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.253:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1) Choose a device that is on the same network as the WLC.
2) Under the "**Desktop**" tab, pick the "**Web Browser**" application at the right.
3) Input the WLC IP address
4) Set your login credentials;

- Press on "**Start**" when you are done.

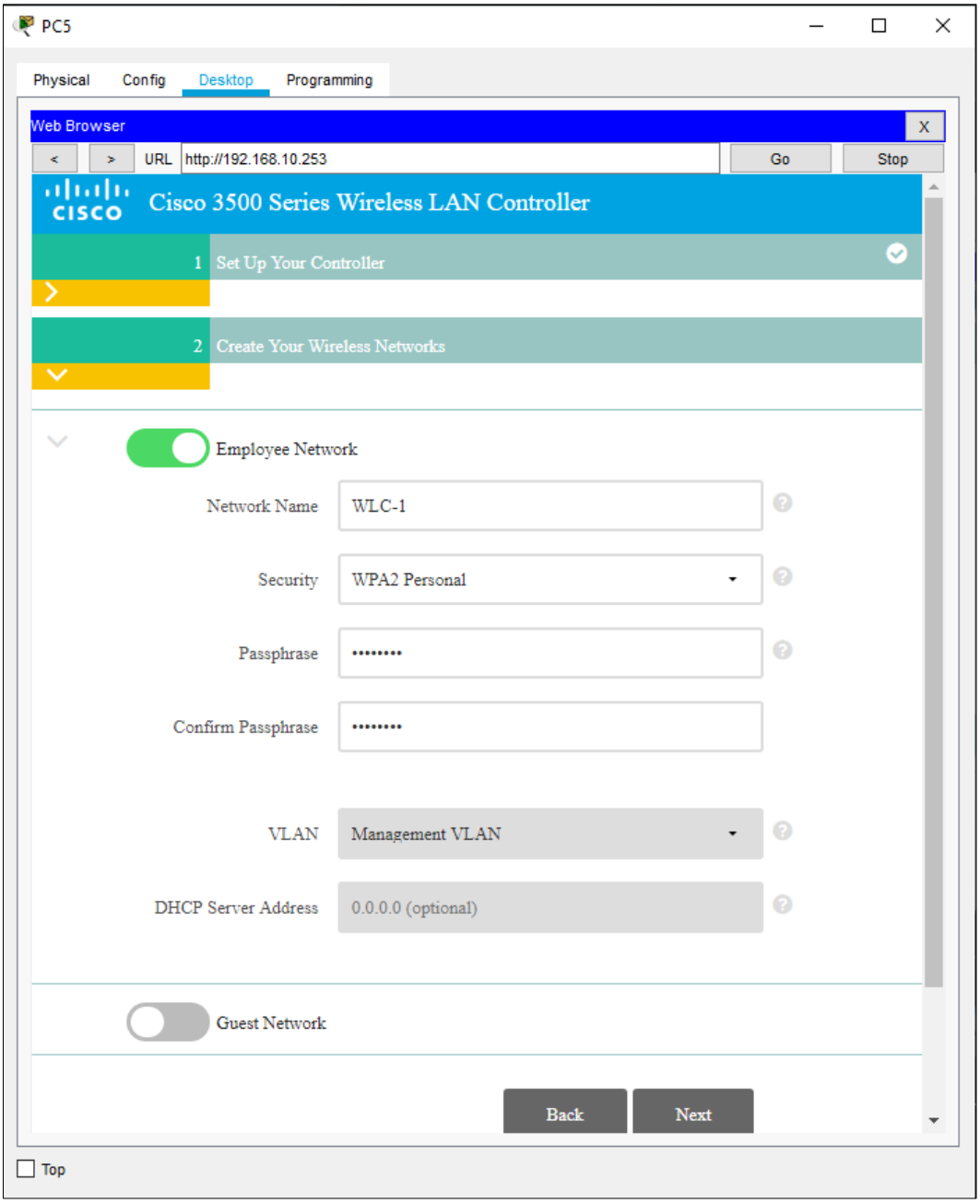
[Next Page]

5) Input the relevant credentials for the "**Set Up You Controller**" section;



[Next Page]

6) Input the relevant credentials for the "**Create Your Wireless Networks**" section;

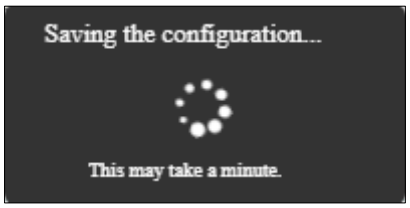


[Next Page]

7) At the "**Advanced Settings**" section, press on "**Next**".
8) At the bottom of the summary page, press on "**Apply**".

- Pay attention that the info you configured is correct, in some cases you won't be able to relog to the system otherwise.

9) The configuration process will begin and may take up to 2 minutes;



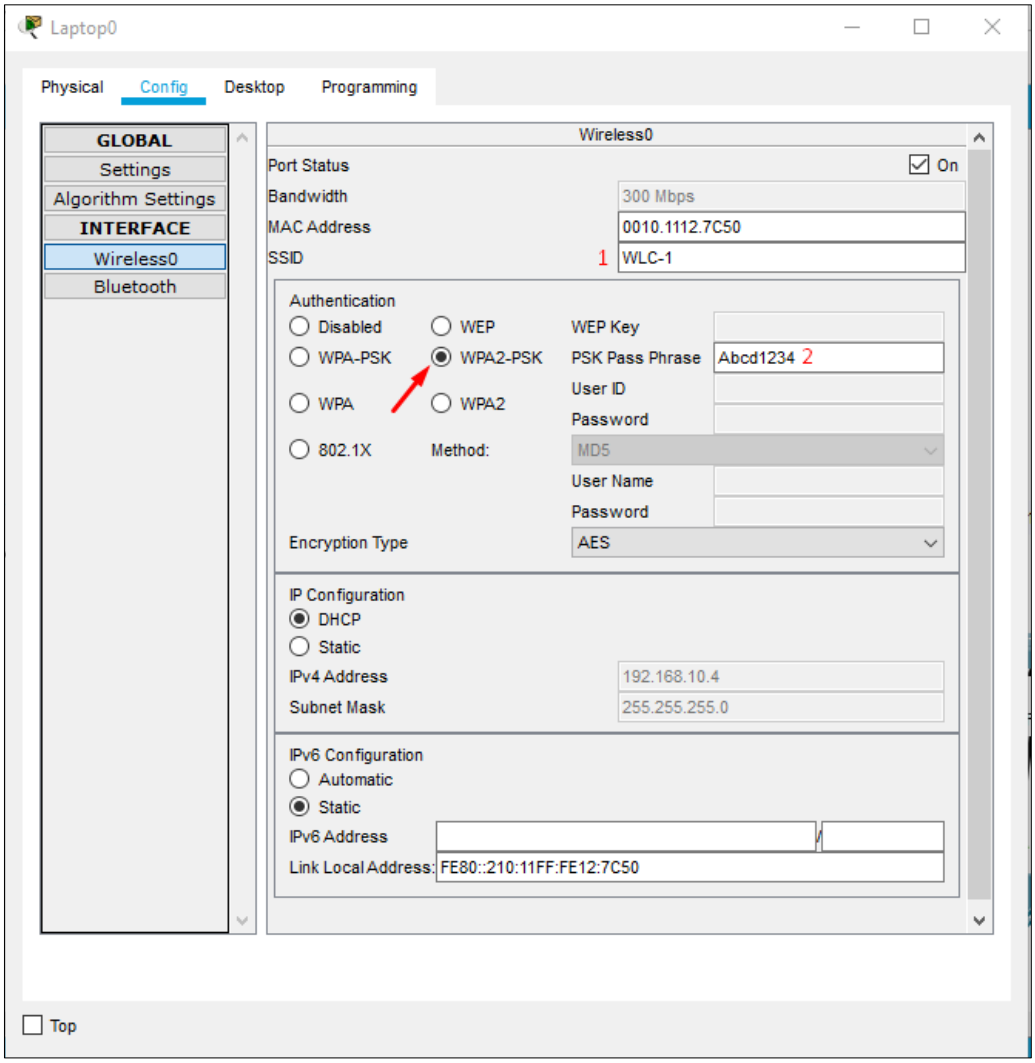
- If you correctly followed this tutorial, you should be able to see CAPWAP packets being sent and received between the WLC and WAP in Simulation mode.

10) Close the browser window and open a new one.
11) Input "**https:// *<WLC-IP>***"

- Login to the WLC with your credentials in order to review the WLC configurations.

Endpoint Wireless Connection

1) Make sure that any relevant physical modules are connected to their respected devices;
    - For the WPA, a Power Adapter.
    - For the Laptop, a WPC300N module.
2) Make that the WPAs and the endpoint devices that will use the wireless connection are set to receive their IP address with DHCP.
3) Click on the endpoint device you wish to connect via the wireless network.
4) Under the "**Config**" tab, pick "**Wireless0**" at the left bar.
5) Input credential for the "**SSID**" and "**WPA2-PSK**" fields;



SSH

In this section we'll apply access to all of our routers only to users that belong to the vlan10 network, via an encrypted connection called SSH.

- Secure Shell (SSH)- A cryptographic network protocol for operating services securely over an unsecured network. SSH provides a secure channel over an unsecured network by using a client–server architecture.

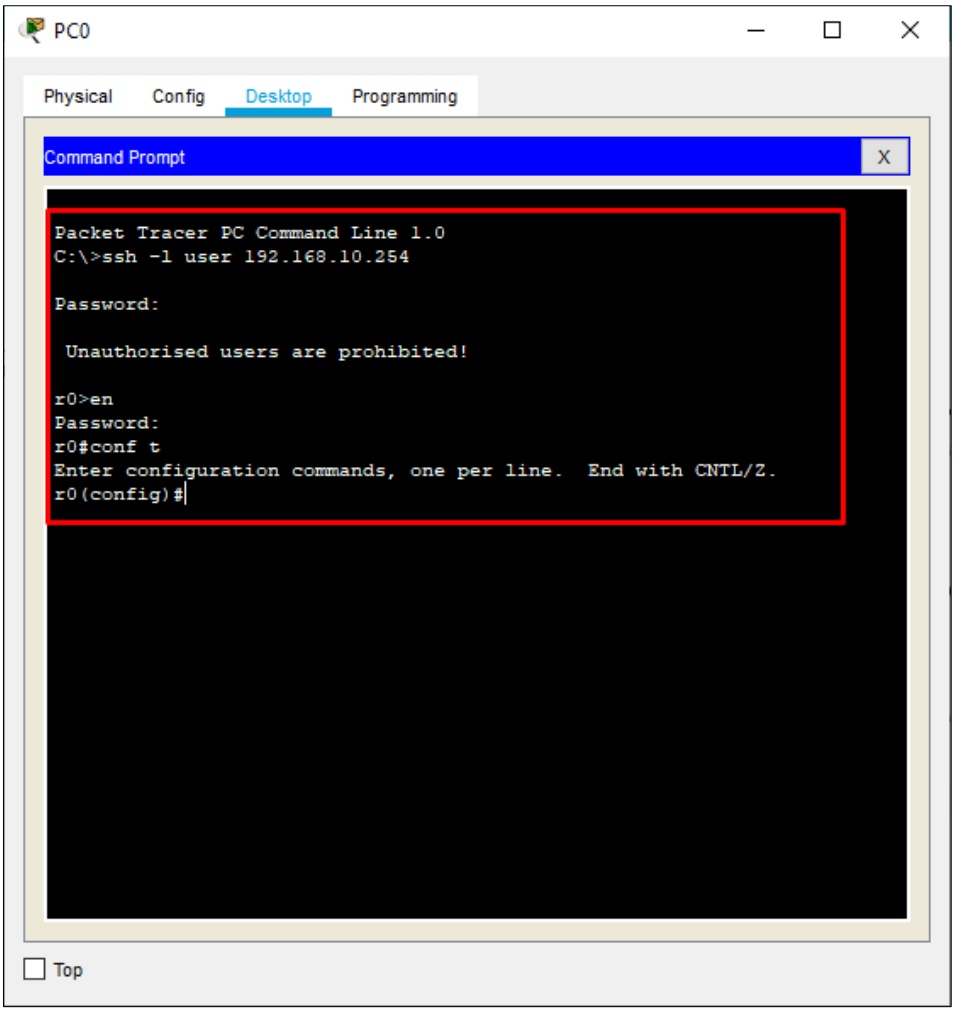
Configuration

1) Choose the relevant device you wish to configure.
2) Open the CLI.
3) Input "**enable**".
4) Input "**configure terminal**" or "**conf t**".
5) Input "**ip domain-name *<DOMAIN>***"
6) Input "**username *<USER-NAME>* secret *<PASSWORD>***"
7) Input "**crypto key generate rsa**"
    - For best practice, apply a 2048-bit encryption.
8) Input "**ip ssh version 2**"
9) Input "**line vty 0 15**"
10) Input "**transport input *<METHOD>***"
    - For this command, you can choose either '**ssh**'/'**telnet**'/'**all**'/'**none**'
    - Input "**exit**" when you are done.
11) Create an ACL for vlan10 according to the Topology section.
12) Input "**line vty 0 15**"
13) Input "**access-class *<NUMBER>* in**"

Verifying Connection

1) Open an endpoint device that is associated with vlan10.
2) Under the "**Desktop**" tab, pick the "**Command Prompt**" application.
3) Input "**ssh -l *<USER-NAME>* <DESTINATION-IP>**
    - If you followed the process correctly, the following should be displayed;

[Next Page]



Conclusion

I hope you enjoyed this tutorial for the CCNA exam and that it helped you in your studies. I would like to encourage the reader to keep on learning and developing himself on the subjects that involved this tutorial. We only covered some of the basic configurations for routers and switches and there is much more to learn.

Mail: eidoepstein@gmail.com
Phone: (+972) 507-513-270
LinkedIn: www.linkedin.com/in/eido-epstein