MMU® MULTIMEDIA UNIVERSITY | FACULTY OF COMPUTING & INFORMATICS

TCS2351 (2210)

Network Security

Mdm. Siti Husna Binti Abdul Rahman

Group Members

NURHAKIM BIN HASBI	1211305696
WAN NASHRUL HAQEEM BIN WAN KAMAL	1191102618
AZMINA SHARAF	1181102970
MUHAMMAD AMINUR RASHID BIN MOHD JALIL	1201302477

FACULTY OF COMPUTING AND INFORMATICS

MULTIMEDIA UNIVERSITY

Table of Contents

Table of Contents 2

Secure Network Requirements 3

Proposed Design and Implementation 4

Topology Overview 4

Overview Discussion 5

Why Star Topology? 6

Username and Passwords 7

Implementation 8

VLAN Network 8

DHCP and DNS 11

Configuring SSH 12

Wireless Security 13

Layer 2 Security 15

Port Security 15

Layer 3 Security 16

Dynamic Host Configuration Protocol (DHCP) 16

OSPF Routing Protocol 17

Firewall 18

AAA Authentication 20

Default 20

TACACS+ 22

RADIUS 24

Intrusion Prevention System 26

Introduction 26

Additional Security Features 28

Security K9 Packages 28

Working Device Configurations 29

PC's 29

Printers 34

Server 42

Access Point 45

Wireless Devices 47

Switches 52

Router 54

References 62

Secure Network Requirements

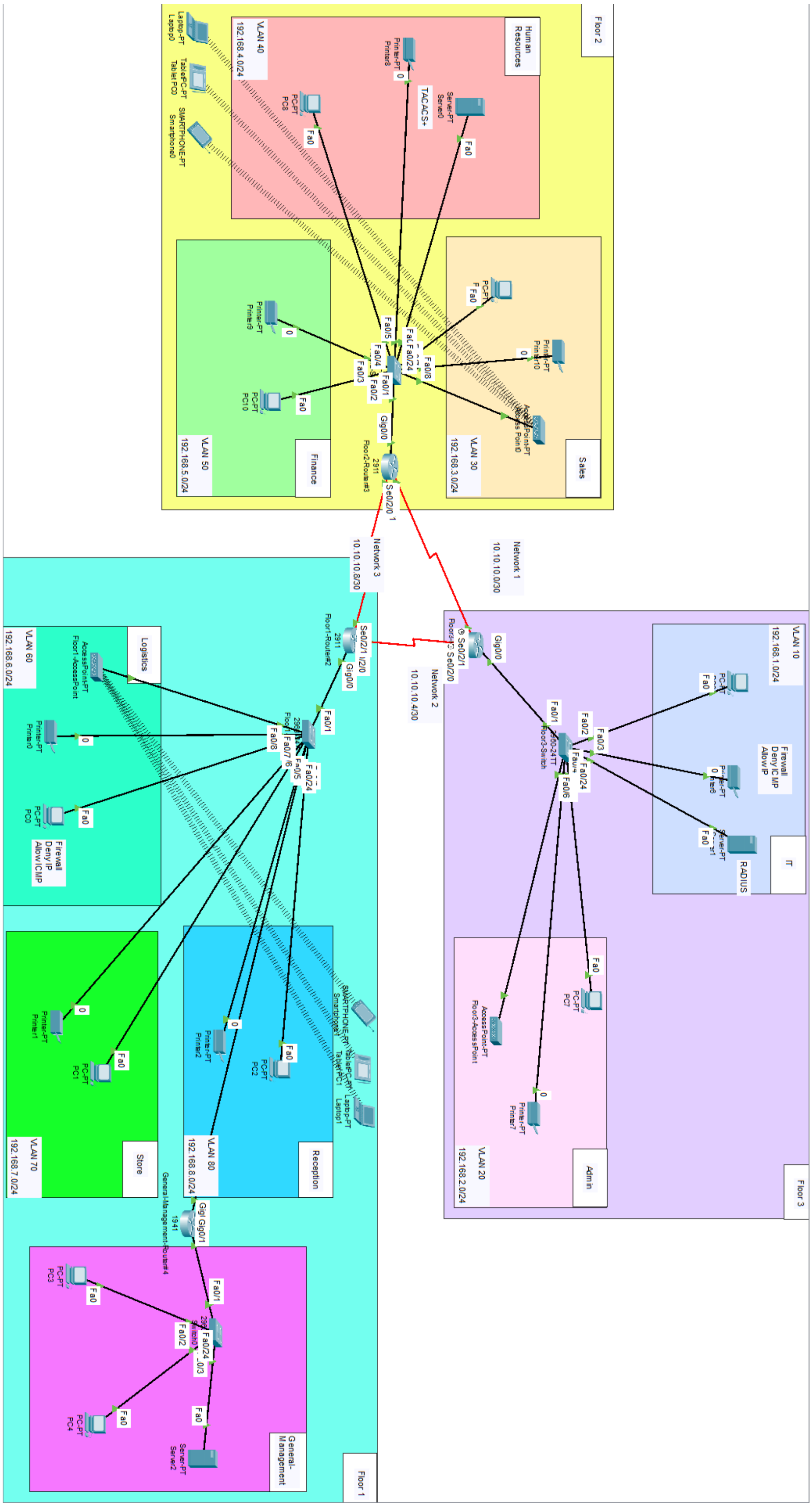
Security scenarios in today's enterprise network environment that should be addressed by security guidelines. Some of the salient aspects of this scenario are:

- Ubiquitous Access Location, Ubiquitous Hosting Location for Application Components, Also, multiple WAN transport protocols are changing the focus, goals, and objectives of security principle.
- Security focus is expanding from a network-centric orientation (ie, internal/intra-enterprise). network vs. external/public internet), users, devices, endpoints, service.
- New trust relationships need not be based solely on company identity or location. access, but extend it to validate each access request (not just the first). access session) and an appropriate set of contextual information associated with it with a user, device, or service.

To achieve this we have chosen a series of cohesive security choices which includes firewalls, Intrusion Prevention System , L2 Security, L3 Security, End devices security, AAA- Authentication, authorization, and accounting

Proposed Design and Implementation

Topology Overview



Overview Discussion

For our enterprise network, we decided to implement a network for an office building. This building will satisfy the various conditions and requirements we have placed on it.

1. Our office building will have 3 floors
2. Each floor will have their own departments unique to each floor
3. For Floor 1, it will have departments for Reception, Store, Logistics and General Management
4. For Floor 2, it will have departments for Sales, Human-Resources and Finance
5. For Floor 3, it will have departments for IT and Admin
6. For all departments, except for General Management, it will have its own VLAN network assigned to it
7. Both Floor 1 and Floor 2 will have an access point for connecting with Wireless Devices
8. Each department, except for General Management, will have at least 1 pc and 1 printer
9. The routers connecting each floor will be connected via LAN and through a VLAN Network

Using our method for creating the network for the office building, we could enjoy several key benefits such as the following.

1. Less congested network traffic between floors due to the VLAN networking
2. Other departments from different departments would not be able to view the data from other floors which is a key security feature in of itself
3. Extremely ease of use in adding new departments to the system as a new VLAN just needs to be assigned to it
4. Clear and concise paths for each PC to reach its destination the fastest due to the use of the Open Shortest Path First (OSPF) protocol

Why Star Topology?

There are several reasons why a star topology might be considered the best choice for a network:

1. Ease of installation and expansion: In a star topology, each device is connected to a central hub or switch, making it easy to add new devices or expand the network.
2. Improved fault tolerance: If one device fails, it will not bring down the entire network. Only the device that has failed and the connection to that device will be affected.
3. Easy to troubleshoot: It is easy to identify and fix problems in a star topology, as each device is connected to a central hub and can be isolated and tested individually.
4. High performance: A star topology can provide high performance, as each device has a dedicated connection to the central hub and does not have to compete with other devices for bandwidth.

However, it's important to note that there are also some potential drawbacks to using a star topology. For example, if the central hub fails, the entire network will go down. Additionally, a star topology can be more expensive to implement and maintain, as it requires more network infrastructure (e.g., hubs, switches, etc.) than other topologies.

Username and Passwords

All Router console passwords (Due note that for some routers, it is not able to be seen as AAA authentication cover over it)

→ **Assignmentconpw**

When wanting to enable

→ **Assignment123**

When accessing Telnet

→ **assignmentvtypw**

For AAA authentication:

General-Management Router#4:

Username → admin1
Password → admin1pw

Floor2-Router#3

Username → admin3
Password → admin3pw

Backup:

Username → user3
Password → user3pw

Floor3-Router#4

Username → admin4
Password → admin4pw

Backup:

Username → user4
Password → user4pw

Implementation

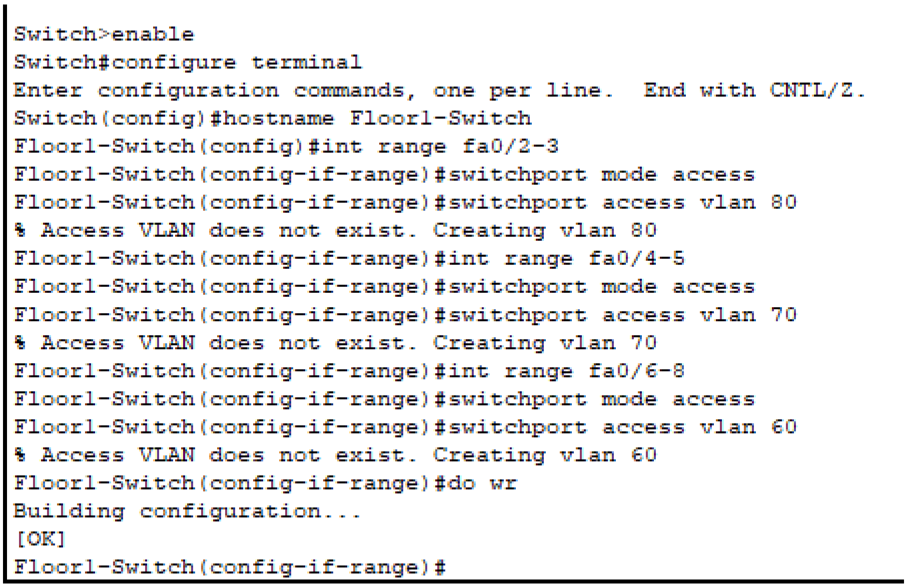
VLAN Network

We utilised a VLAN Network in our Enterprise Network. A VLAN by definition is a virtual local area network in any broadcast domain that is partitioned and isolated in a computer network at the data link layer.

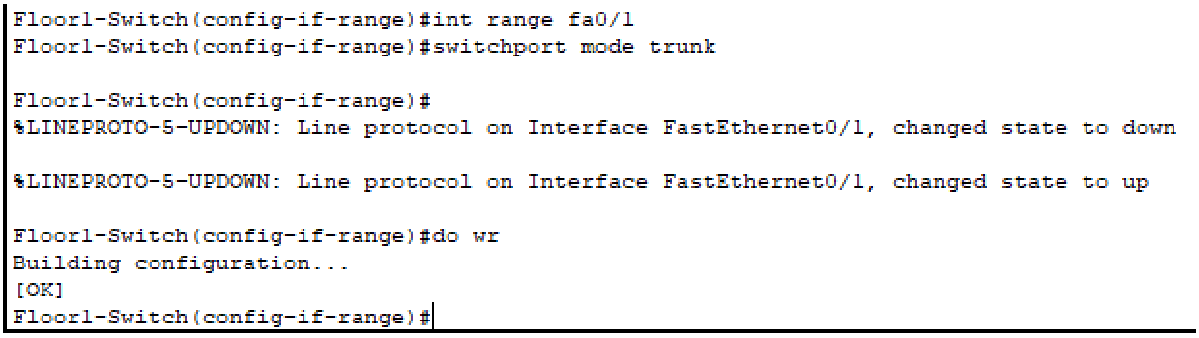
A VLAN network is beneficial for several reasons.

1. Improved Security
    a. Reduces both internal and external threats
    b. Internally, by separating users, we can improve both security and privacy by ensuring that users can only access the networks that apply to them
    c. Externally, if an attacker attacks a VLAN, they will be contained and trapped within that VLAN and the boundaries set by the moderators
2. Easier Fault Management
    a. Eases the process of troubleshooting as each network is isolated and segmented which makes the process simpler and more efficient
3. Improved Quality of Service
    a. VLANs are able to manage traffic much more efficiently which will in turn also boost the performance of the users
    b. Less latency issues
    c. More reliability for critical applications as it is easier to prioritise traffic towards that application
4. Simplified administration for the network manager
    a. Simplifies management by logically grouping users into the same virtual networks
    b. If users have to physically move locations or change their equipment, the same VLANs can still easily be used
    c. This also applies if an employee is moved to a different department, it is very easy to reassign them to the departments VLAN without issue which is important as our scenario is an office building

Below is the implementation of the VLAN within one of our routers



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Floor1-Switch
Floor1-Switch(config)#int range fa0/2-3
Floor1-Switch(config-if-range)#switchport mode access
Floor1-Switch(config-if-range)#switchport access vlan 80
% Access VLAN does not exist. Creating vlan 80
Floor1-Switch(config-if-range)#int range fa0/4-5
Floor1-Switch(config-if-range)#switchport mode access
Floor1-Switch(config-if-range)#switchport access vlan 70
% Access VLAN does not exist. Creating vlan 70
Floor1-Switch(config-if-range)#int range fa0/6-8
Floor1-Switch(config-if-range)#switchport mode access
Floor1-Switch(config-if-range)#switchport access vlan 60
% Access VLAN does not exist. Creating vlan 60
Floor1-Switch(config-if-range)#do wr
Building configuration...
[OK]
Floor1-Switch(config-if-range)#
```



```
Floor1-Switch(config-if-range)#int range fa0/1
Floor1-Switch(config-if-range)#switchport mode trunk

Floor1-Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Floor1-Switch(config-if-range)#do wr
Building configuration...
[OK]
Floor1-Switch(config-if-range)#
```

Here is the encapsulation process

```
Floor1-Router(config)#int gig0/0.80
Floor1-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.80, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.80, changed
state to up

Floor1-Router(config-subif)#encapsulation dot1Q 80
Floor1-Router(config-subif)#ip address 192.168.8.1 255.255.255.0
Floor1-Router(config-subif)#ex
Floor1-Router(config)#int gig0/0.70
Floor1-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.70, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.70, changed
state to up

Floor1-Router(config-subif)#encapsulation dot1Q 70
Floor1-Router(config-subif)#ip address 192.168.7.1 255.255.255.0
Floor1-Router(config-subif)#ex

Floor1-Router(config)#int gig0/0.60
Floor1-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed
state to up

Floor1-Router(config-subif)#encapsulation dot1Q 60
Floor1-Router(config-subif)#ip address 192.168.6.1 255.255.255.0
Floor1-Router(config-subif)#do wr
Building configuration...
[OK]
Floor1-Router(config-subif)#
```

DHCP and DNS

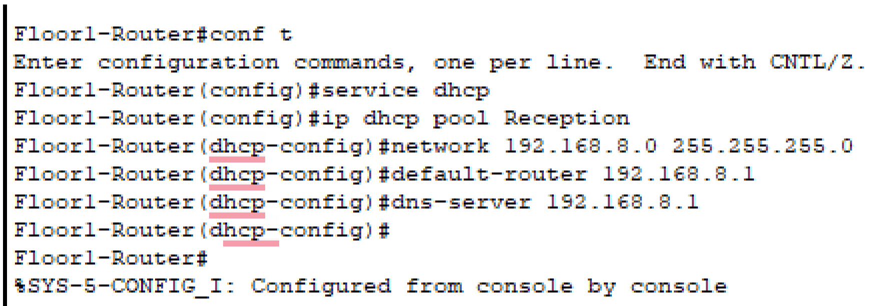
We have also utilised both DHCP and DNS in our network. As a brief introduction, DHCP sends out information that clients need to communicate with other devices or machines or services while DNS ensures that servers, clients and services can be found by their names.

DHCP, or Dynamic Host Configuration Protocol works by dynamically assigning IP addresses and other configuration options to devices in a network. This helps in scalability, as it is very easy to add new devices. DHCP is extremely key in an enterprise environment such as this as in a real life scenario, users from different departments will constantly be changing with their number constantly in flux as some get promoted and others fired.

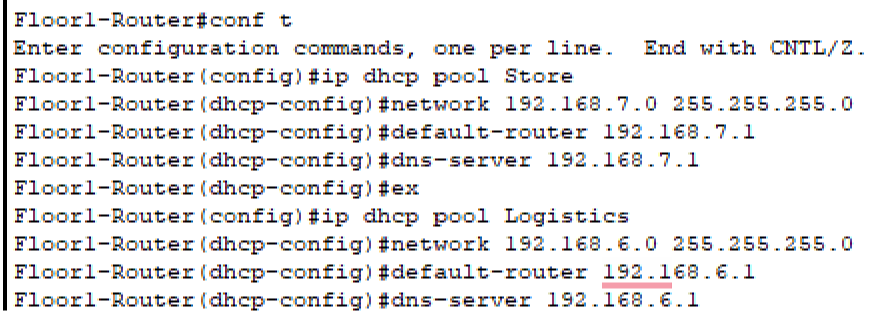
The DHCP server will distribute free IP addresses from an assigned pool. The clients will each get different IPs, which is very convenient when adding new people. The server also determines how long an IP address is valid and will automatically renew the lease time if it deems it expired.

DNS however, stands for Domain Name System and it is a hierarchical and decentralised naming system for computers, services and more connected to a private network. A DNS server in a private network is also responsible for the name resolution. It is aware of all IP addresses and names of the devices.

Below is an example on how we implemented DHCP and DNS in our routers



```
Floor1-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Floor1-Router(config)#service dhcp
Floor1-Router(config)#ip dhcp pool Reception
Floor1-Router(dhcp-config)#network 192.168.8.0 255.255.255.0
Floor1-Router(dhcp-config)#default-router 192.168.8.1
Floor1-Router(dhcp-config)#dns-server 192.168.8.1
Floor1-Router(dhcp-config)#
Floor1-Router#
%SYS-5-CONFIG_I: Configured from console by console
```



```
Floor1-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Floor1-Router(config)#ip dhcp pool Store
Floor1-Router(dhcp-config)#network 192.168.7.0 255.255.255.0
Floor1-Router(dhcp-config)#default-router 192.168.7.1
Floor1-Router(dhcp-config)#dns-server 192.168.7.1
Floor1-Router(dhcp-config)#ex
Floor1-Router(config)#ip dhcp pool Logistics
Floor1-Router(dhcp-config)#network 192.168.6.0 255.255.255.0
Floor1-Router(dhcp-config)#default-router 192.168.6.1
Floor1-Router(dhcp-config)#dns-server 192.168.6.1
```

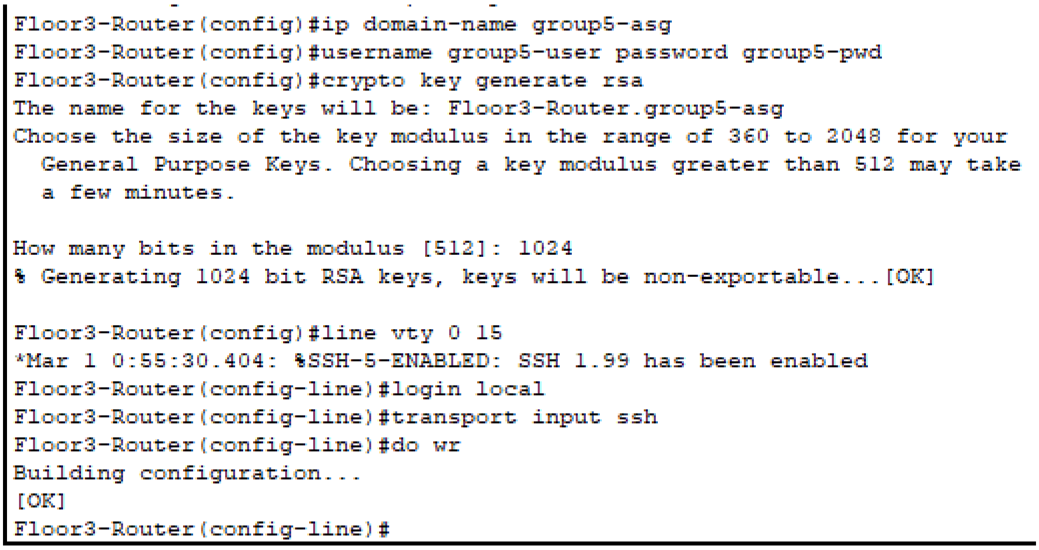
Configuring SSH

SSH or Secure Shell is a network communication protocol that enables two computers to communicate and share data. One key feature of SSH is that the communication between the two computers is also encrypted which adds an additional layer of security, especially over insecure networks.

SSH also allows for the tunnelling of other protocols such as FTP and can protect us from various attacks such as the below.

1. IP Source Rooting
2. IP Address Spoofing
3. DNS Spoofing
4. Data manipulation at routers
5. Eavesdropping or sniffing of transmitted data

Below is how we implemented SSH in one of our routers



```
Floor3-Router(config)#ip domain-name group5-asg
Floor3-Router(config)#username group5-user password group5-pwd
Floor3-Router(config)#crypto key generate rsa
The name for the keys will be: Floor3-Router.group5-asg
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Floor3-Router(config)#line vty 0 15
*Mar 1 0:55:30.404: %SSH-5-ENABLED: SSH 1.99 has been enabled
Floor3-Router(config-line)#login local
Floor3-Router(config-line)#transport input ssh
Floor3-Router(config-line)#do wr
Building configuration...
[OK]
Floor3-Router(config-line)#
```

Wireless Security

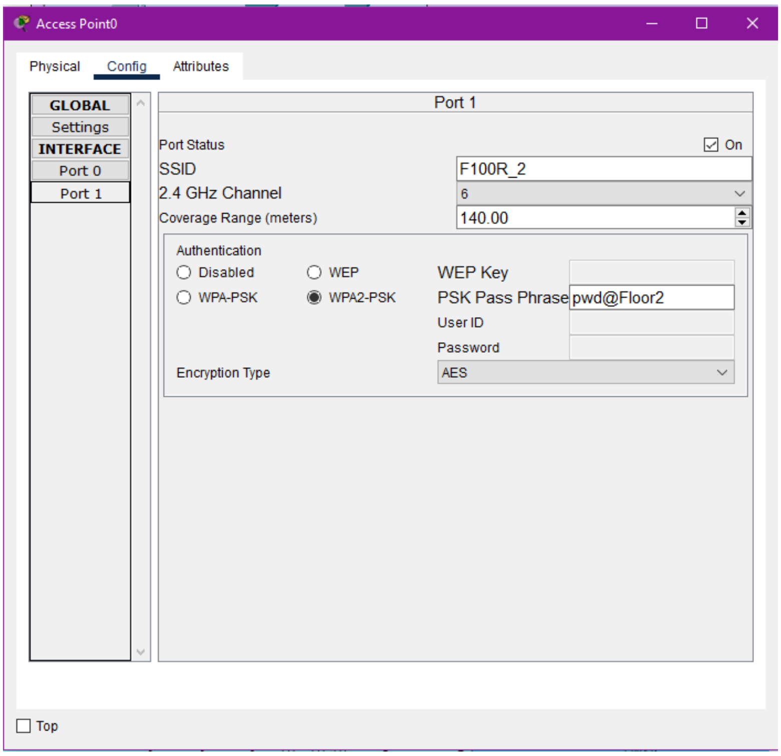
Floors 1 and 2 have access points within them in order to help in facilitating connections with wireless devices such as smartphones and tablets. However, we also need to implement a layer of security here so not just anyone out there can connect to our network.

First of all, we implemented an SSID for them. For the sake of the clarity for the assignment, we provided a pretty clear SSID naming scheme for both access points, however, in a real world scenario, this SSID should be a lot more cryptic.

Secondly, we also gave a password to this SSID. Similar to before, we used a relatively easy password for them, but in a real world scenario, a more cryptic one should be used.

Wireless security such as this is important to prevent eavesdropping, which is one of the biggest weaknesses of wireless devices. With this method, we can ensure only a select few number of people is able to access the wireless network.

Below shows the assignment of SSID and password in our Level 2 Access Point


Access Point0

Physical | Config | Attributes

Port 1

Port Status ☑ On

SSID F100R_2

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key

PSK Pass Phrase pwd@Floor2

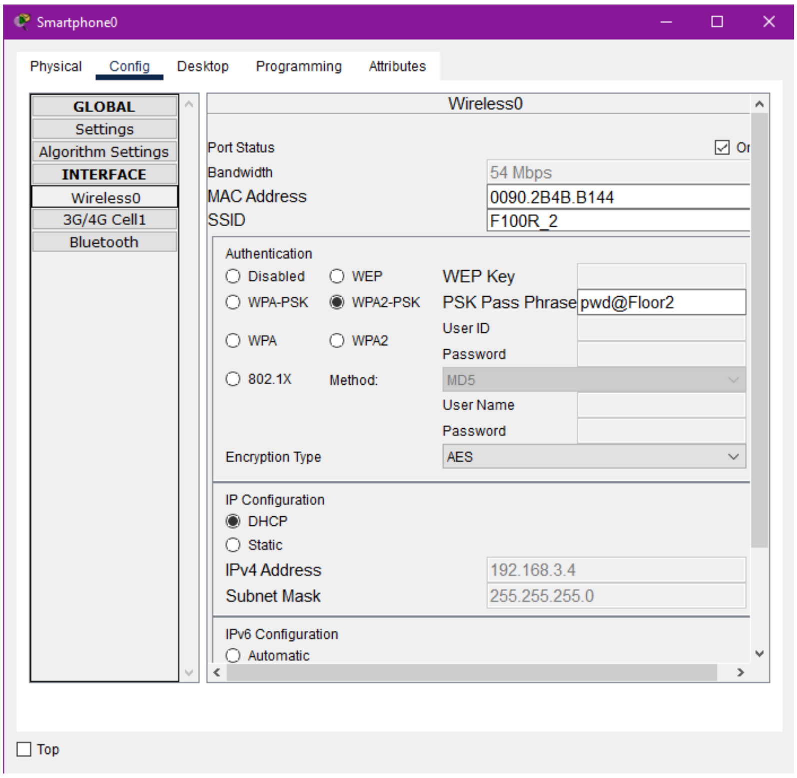
User ID

Password

Encryption Type AES

□ Top

Below shows the connection to that access point from a smartphone wireless device


Smartphone0

Physical | Config | Desktop | Programming | Attributes

Wireless0

Port Status ☑ On

Bandwidth 54 Mbps

MAC Address 0090.2B4B.B144

SSID F100R_2

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

○ WPA ○ WPA2

○ 802.1X Method: MD5

WEP Key

PSK Pass Phrase pwd@Floor2

User ID

Password

User Name

Password

Encryption Type AES

IP Configuration

● DHCP

○ Static

IPv4 Address 192.168.3.4

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

□ Top

Layer 2 Security

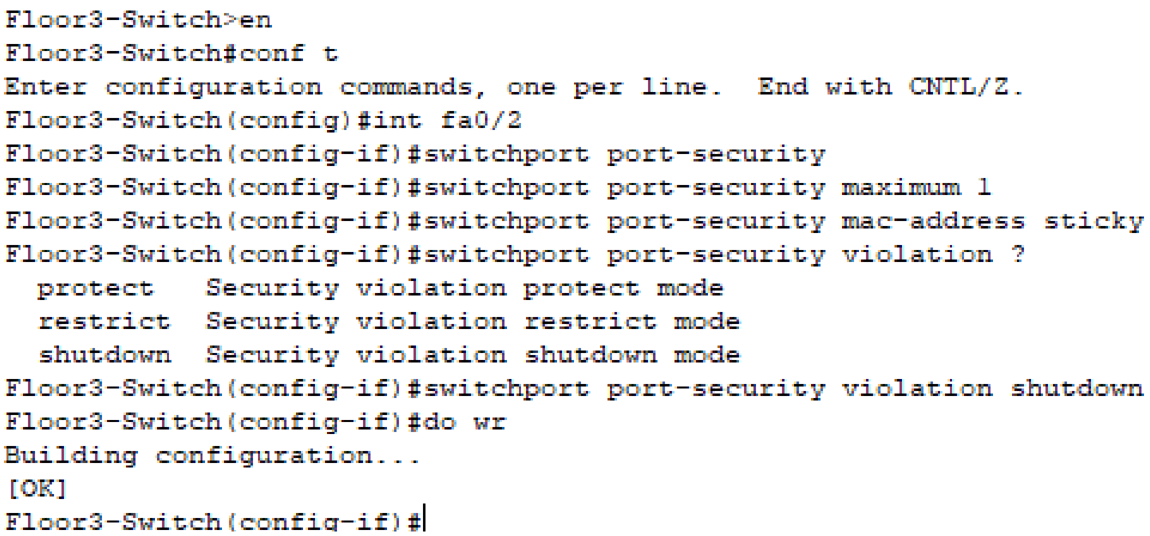
Port Security

Prevent unauthorised access By limiting the number of allowed MAC addresses on a switch port, we can also prevent unauthorised devices from accessing the network.

Not just that, by doing this, we can Prevent network attacks, because when we restrict the type of traffic thats allowed on a switch port, we can prevent network attacks such as ARP spoofing, which can compromise the security of our network.

ARP Spoofing is a man in the middle attack,

Finally, port security allows us to ensure network availability: By preventing unauthorised devices from accessing the network, we can save our network resources, and the network remains available to authorised devices.



```
Floor3-Switch>en
Floor3-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Floor3-Switch(config)#int fa0/2
Floor3-Switch(config-if)#switchport port-security
Floor3-Switch(config-if)#switchport port-security maximum 1
Floor3-Switch(config-if)#switchport port-security mac-address sticky
Floor3-Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Floor3-Switch(config-if)#switchport port-security violation shutdown
Floor3-Switch(config-if)#do wr
Building configuration...
[OK]
Floor3-Switch(config-if)#
```

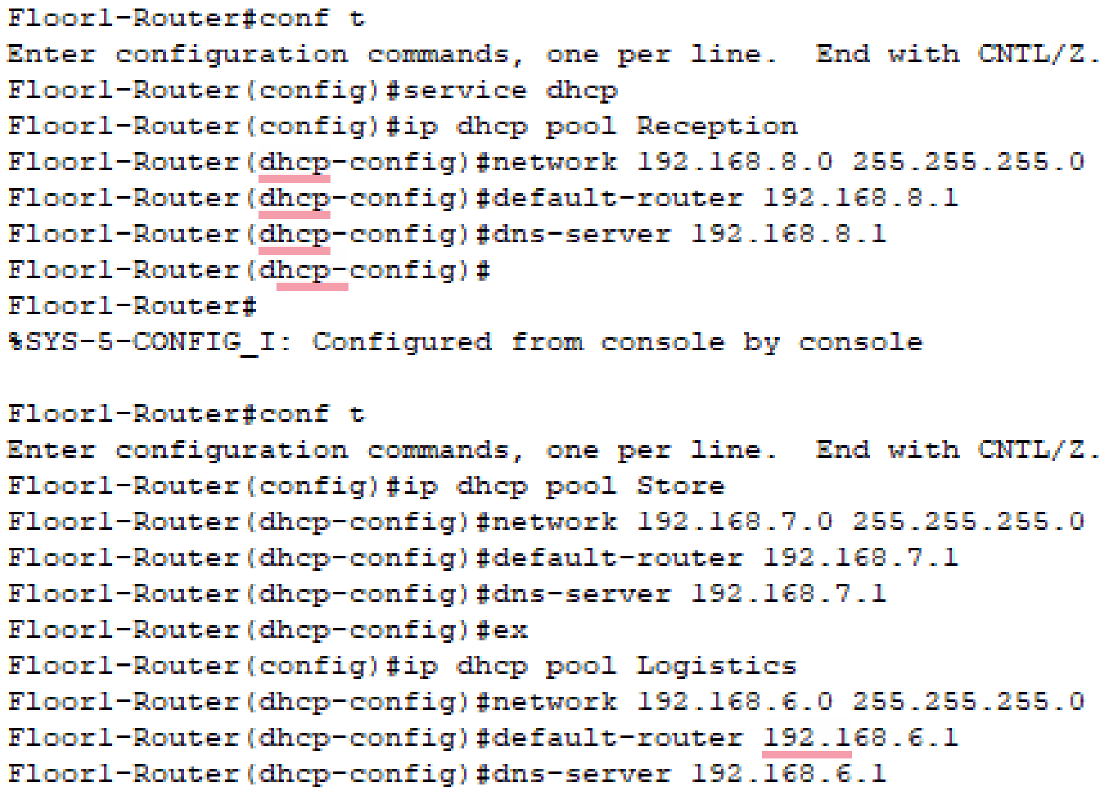
Figure above shows how to apply port security

Layer 3 Security

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol. DHCP is applied when we want to automatically assign IP addresses to devices on our network. DHCP simplifies the task of configuring IP addresses on devices and ensures that each device on the network has a unique IP address.

When we use DHCP, we don't have to manually assign IP addresses to each device on the network. Instead, the DHCP server assigns IP addresses dynamically to devices as they join the network. This makes it easier to add or remove devices from the network without having to manually reconfigure IP addresses.



```
Floor1-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Floor1-Router(config)#service dhcp
Floor1-Router(config)#ip dhcp pool Reception
Floor1-Router(dhcp-config)#network 192.168.8.0 255.255.255.0
Floor1-Router(dhcp-config)#default-router 192.168.8.1
Floor1-Router(dhcp-config)#dns-server 192.168.8.1
Floor1-Router(dhcp-config)#
Floor1-Router#
%SYS-5-CONFIG_I: Configured from console by console

Floor1-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Floor1-Router(config)#ip dhcp pool Store
Floor1-Router(dhcp-config)#network 192.168.7.0 255.255.255.0
Floor1-Router(dhcp-config)#default-router 192.168.7.1
Floor1-Router(dhcp-config)#dns-server 192.168.7.1
Floor1-Router(dhcp-config)#ex
Floor1-Router(config)#ip dhcp pool Logistics
Floor1-Router(dhcp-config)#network 192.168.6.0 255.255.255.0
Floor1-Router(dhcp-config)#default-router 192.168.6.1
Floor1-Router(dhcp-config)#dns-server 192.168.6.1
```

Figure above shows the commands to implement DHCP

OSPF Routing Protocol

OSPF is a routing protocol that is used to distribute routing information in a network. The main purpose of OSPF is to find the best path to a destination and to ensure that all routers in the network have the same view of the network.

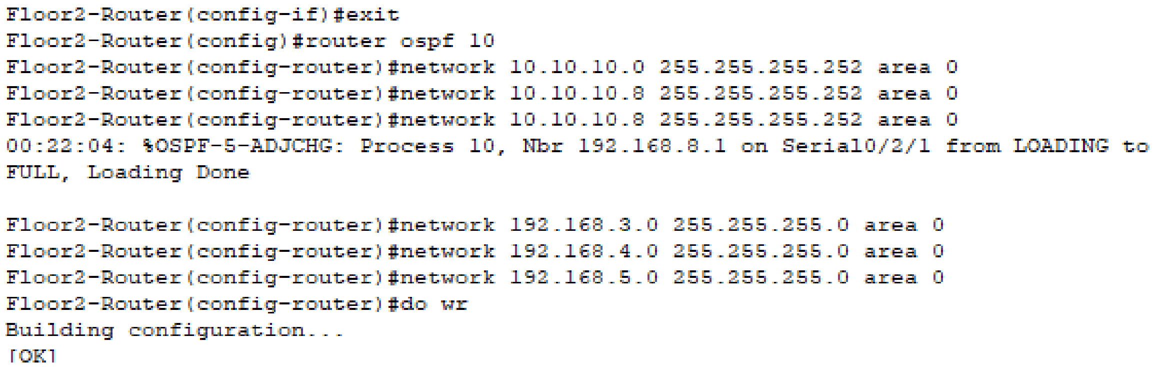
How OSPF works is by having each router maintain a map of the network and its topology. Each router then calculates the shortest path to each destination based on this information. The routers will then exchange this information with each other to ensure that all routers have the same view of the network.

OSPF has a few benefits such as :

Scalability: OSPF is capable of handling large networks and can scale to accommodate growth.

Reliability: OSPF provides fast convergence times in the event of network changes and can automatically route around network failures.

Finally, By using OSPF in a network, we can ensure that all routers have a consistent view of the network, that traffic is routed along the best path, and that the network is scalable and reliable.



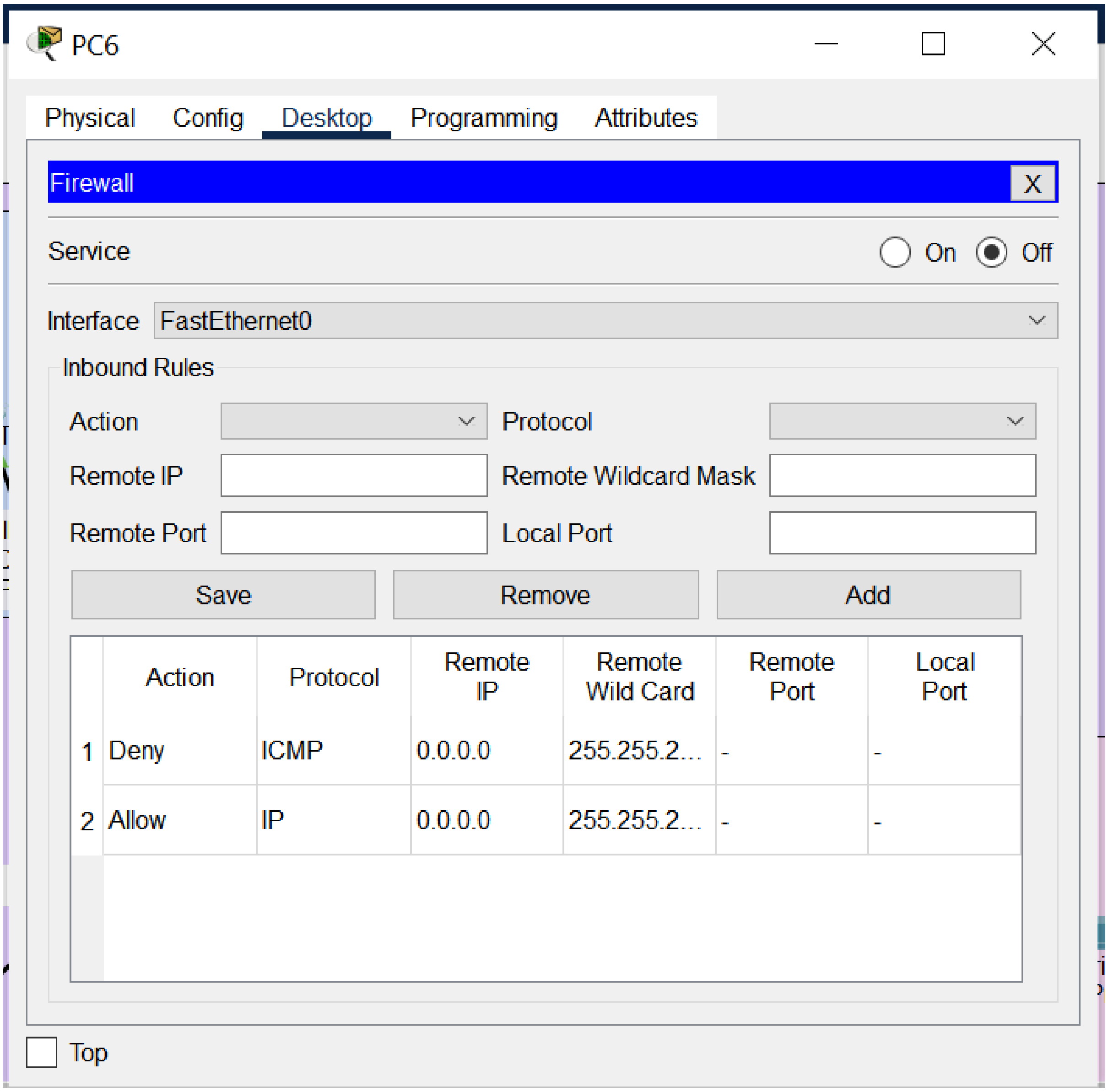
```
Floor2-Router(config-if)#exit
Floor2-Router(config)#router ospf 10
Floor2-Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
Floor2-Router(config-router)#network 10.10.10.8 255.255.255.252 area 0
Floor2-Router(config-router)#network 10.10.10.8 255.255.255.252 area 0
00:22:04: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.8.1 on Serial0/2/1 from LOADING to
FULL, Loading Done

Floor2-Router(config-router)#network 192.168.3.0 255.255.255.0 area 0
Floor2-Router(config-router)#network 192.168.4.0 255.255.255.0 area 0
Floor2-Router(config-router)#network 192.168.5.0 255.255.255.0 area 0
Floor2-Router(config-router)#do wr
Building configuration...
[OK]
```

Figure above shows the command to implement OSPF Routing

Firewall

Firewalls are an essential part of any network security strategy. They act as a barrier between an organisation's internal network and the outside world, enabling organisations to control what traffic can access their systems.

Firewalls can protect against malicious software, viruses, and hackers by creating rules for which traffic can access the organisation's systems. They can also block access from outside sources that have not been authorised. Implementing a firewall is essential to protect critical data, systems, and networks from malicious attacks.



Service ○ On ● Off

Interface FastEthernet0

Inbound Rules

Action

Protocol

Remote IP

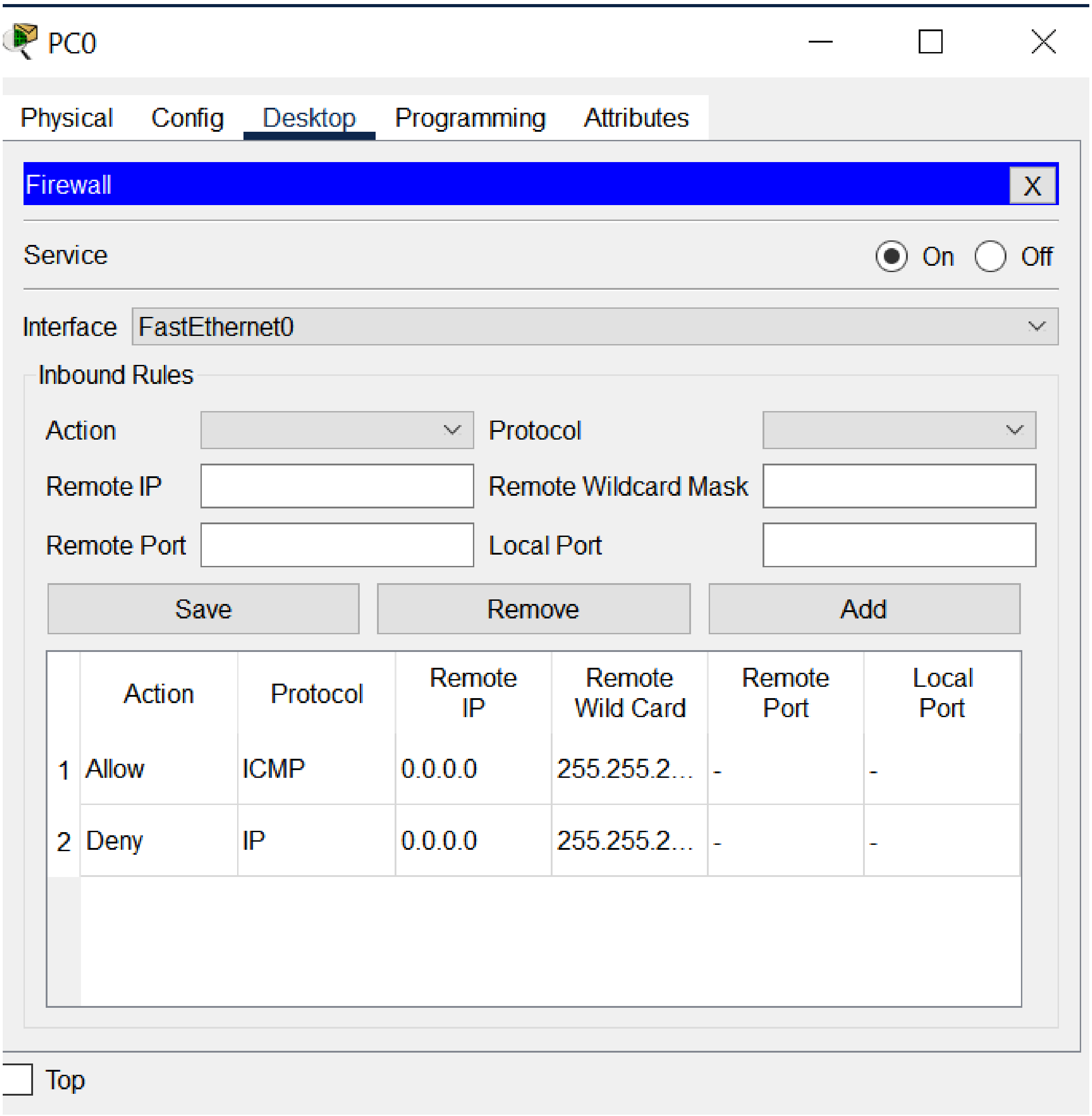
Remote Wildcard Mask

Remote Port

Local Port

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Deny	ICMP	0.0.0.0	255.255.2...	-	-
2	Allow	IP	0.0.0.0	255.255.2...	-	-

□ Top



Service ● On ○ Off

Interface FastEthernet0

Inbound Rules

Action
Protocol
Remote IP
Remote Wildcard Mask
Remote Port
Local Port

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	ICMP	0.0.0.0	255.255.2...	-	-
2	Deny	IP	0.0.0.0	255.255.2...	-	-

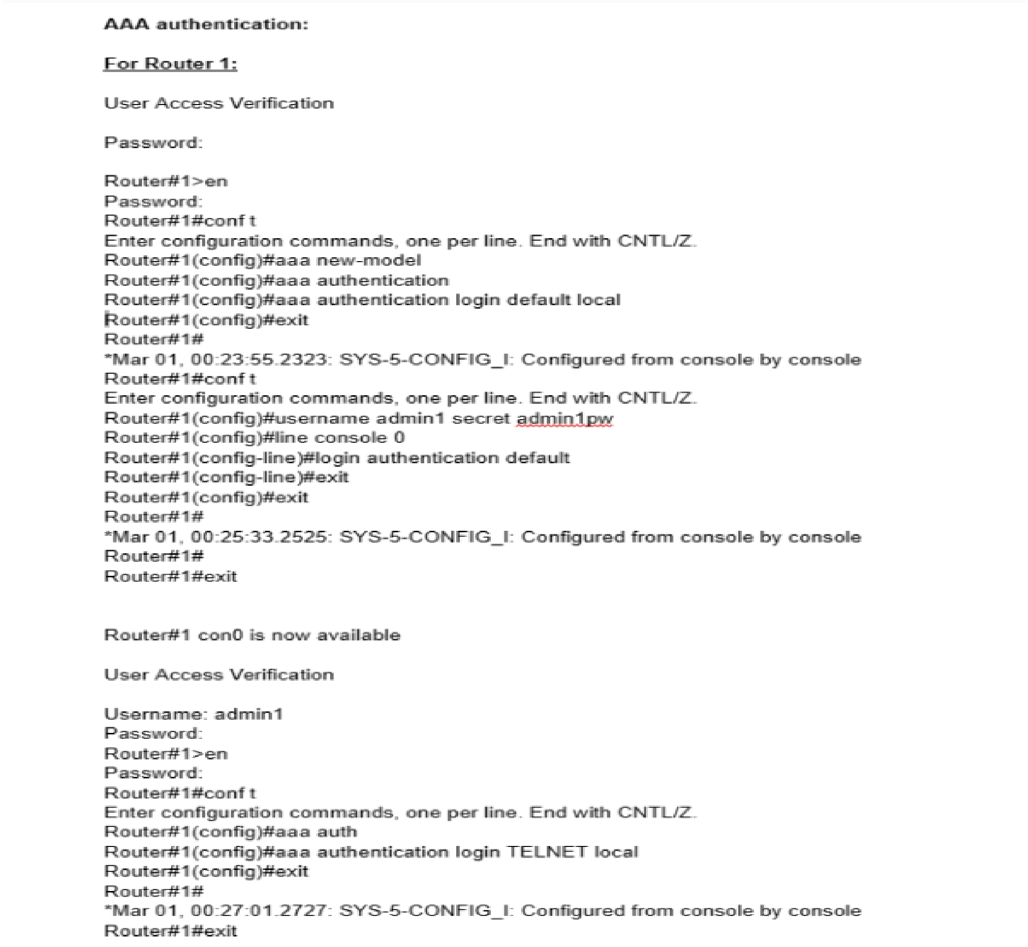
□ Top

AAA Authentication

Default

AAA authentication can be a valuable security measure to protect routers from unauthorised access. By requiring users to enter their credentials, AAA authentication can help prevent unauthorised access to the router and its features. Additionally, AAA authentication can be used to ensure that only users with appropriate credentials can access certain features, making it easier to maintain network security and control who has access to the router.

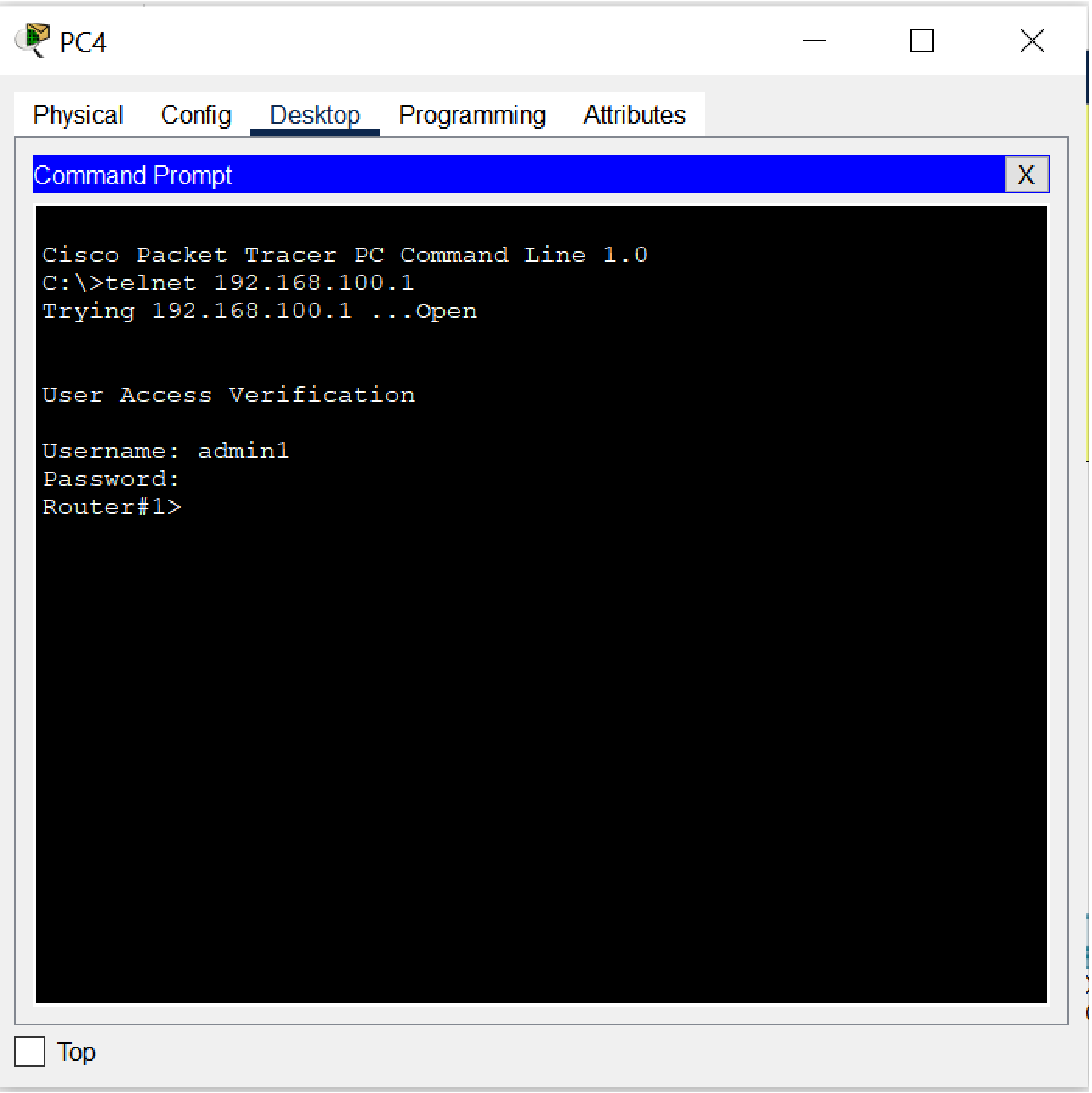
Furthermore, AAA authentication can help guarantee that only authorised users can make changes to the router, preventing it from being tampered with or misconfigured. Lastly, AAA authentication can help provide a more secure connection when using remote access to the router, ensuring that only authorised users are able to access the router.



AAA authentication:

For Router 1:

```
User Access Verification

Password:

Router#1>en
Password:
Router#1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router#1(config)#aaa new-model
Router#1(config)#aaa authentication
Router#1(config)#aaa authentication login default local
Router#1(config)#exit
Router#1#
*Mar 01, 00:23:55.2323: SYS-5-CONFIG_I: Configured from console by console
Router#1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router#1(config)#username admin1 secret admin1pw
Router#1(config)#line console 0
Router#1(config-line)#login authentication default
Router#1(config-line)#exit
Router#1(config)#exit
Router#1#
*Mar 01, 00:25:33.2525: SYS-5-CONFIG_I: Configured from console by console
Router#1#
Router#1#exit


Router#1 con0 is now available

User Access Verification

Username: admin1
Password:
Router#1>en
Password:
Router#1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router#1(config)#aaa auth
Router#1(config)#aaa authentication login TELNET local
Router#1(config)#exit
Router#1#
*Mar 01, 00:27:01.2727: SYS-5-CONFIG_I: Configured from console by console
Router#1#exit
```

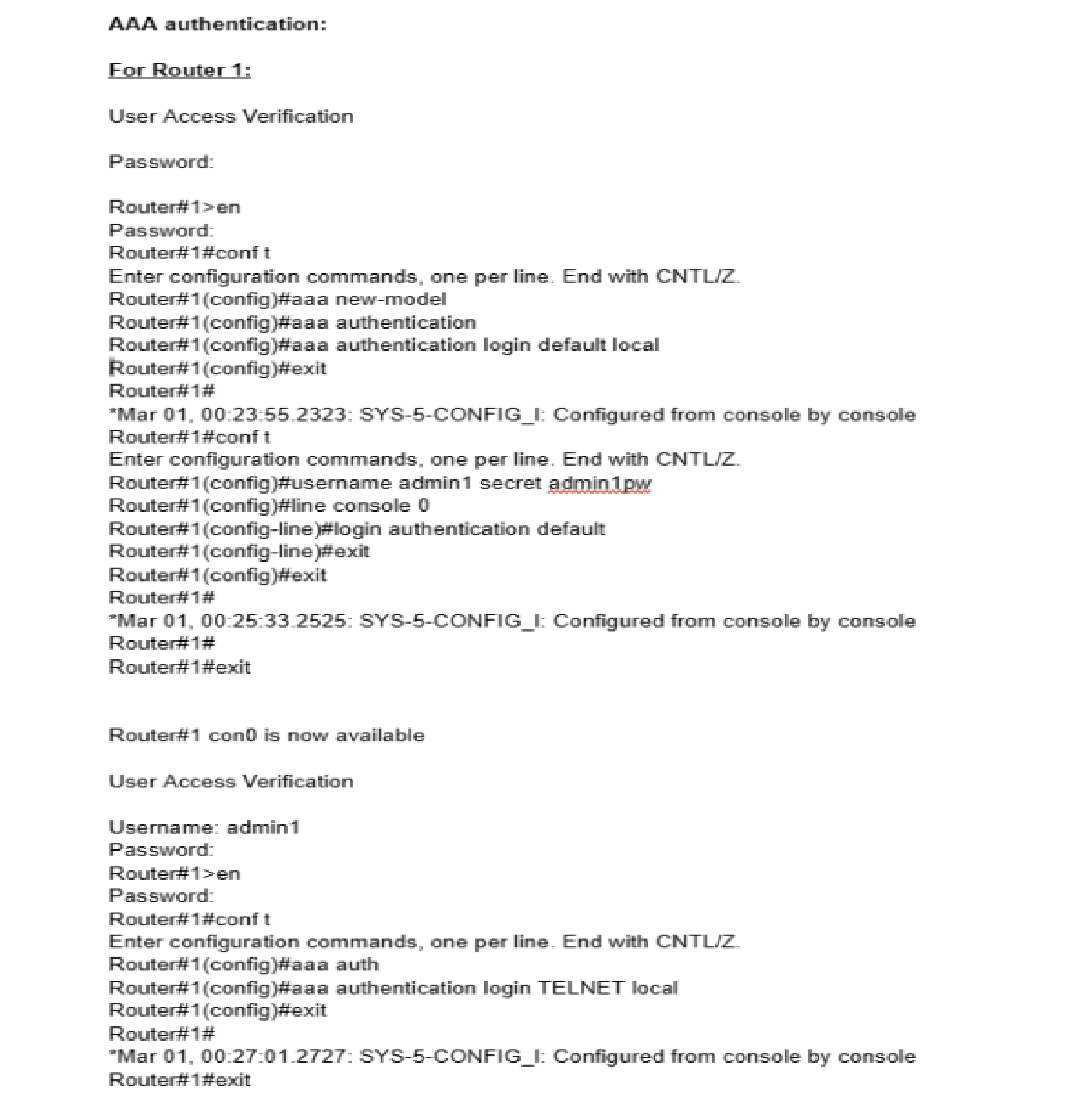


```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.100.1
Trying 192.168.100.1 ...Open


User Access Verification

Username: admin1
Password:
Router#1>
```

TACACS+

AAA authentication is a security protocol used to validate any user attempting to access a router or network access server. It stands for Authentication, Authorization, and Accounting and is used to manage access to network resources.

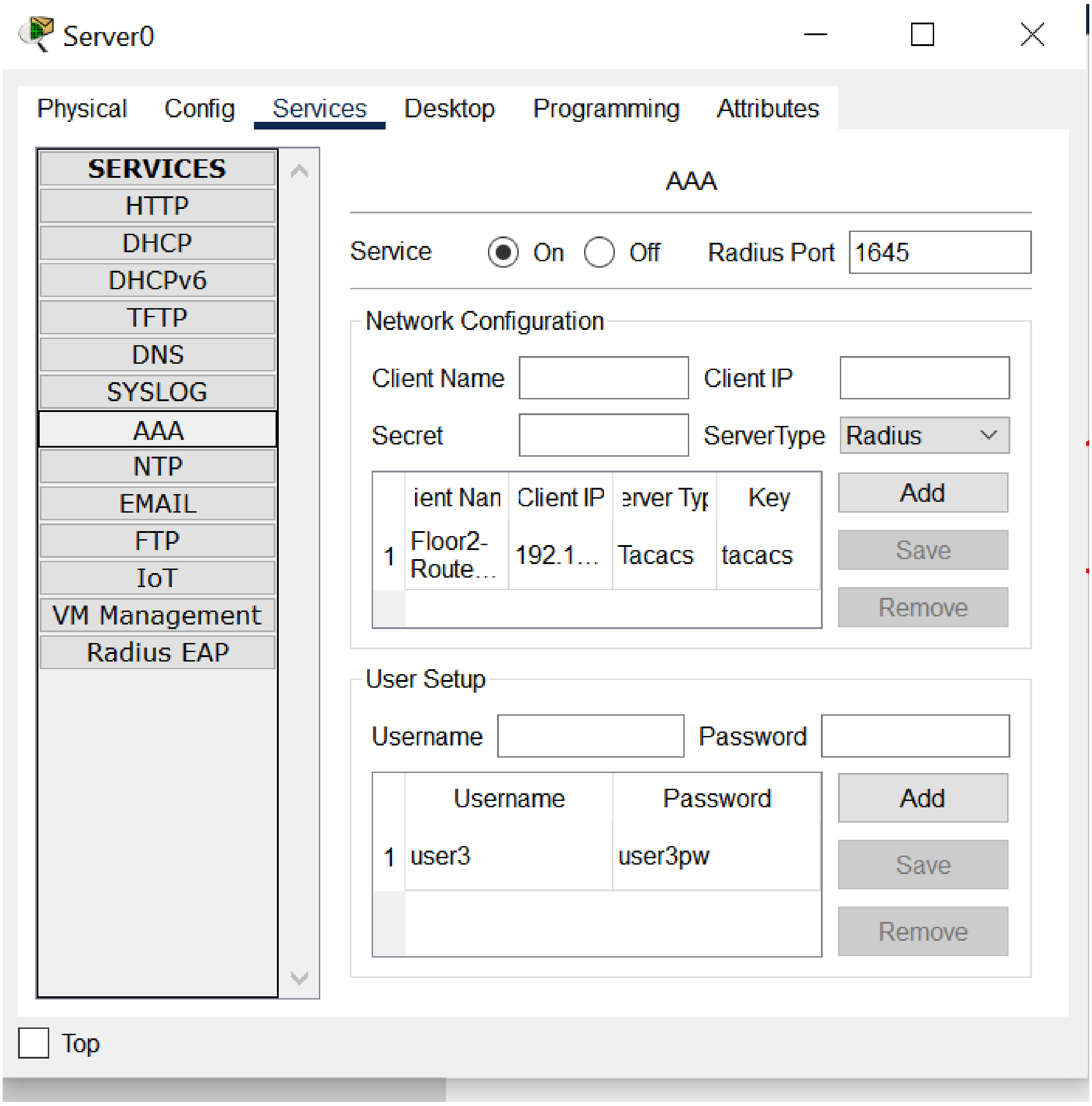
TACACS+ is an open standard security protocol used for AAA authentication. It provides separated authentication, authorization and accounting services, and enables you to manage administrator authorization through your directory via Vendor-Specific Attributes (VSAs).



AAA authentication:

For Router 1:

```
User Access Verification

Password:

Router#1>en
Password:
Router#1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router#1(config)#aaa new-model
Router#1(config)#aaa authentication
Router#1(config)#aaa authentication login default local
Router#1(config)#exit
Router#1#
*Mar 01, 00:23:55.2323: SYS-5-CONFIG_I: Configured from console by console
Router#1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router#1(config)#username admin1 secret admin1pw
Router#1(config)#line console 0
Router#1(config-line)#login authentication default
Router#1(config-line)#exit
Router#1(config)#exit
Router#1#
*Mar 01, 00:25:33.2525: SYS-5-CONFIG_I: Configured from console by console
Router#1#
Router#1#exit


Router#1 con0 is now available

User Access Verification

Username: admin1
Password:
Router#1>en
Password:
Router#1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router#1(config)#aaa auth
Router#1(config)#aaa authentication login TELNET local
Router#1(config)#exit
Router#1#
*Mar 01, 00:27:01.2727: SYS-5-CONFIG_I: Configured from console by console
Router#1#exit
```



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name

Client IP

Secret

ServerType Radius

	ient Nan	Client IP	erver Typ	Key
1	Floor2- Route…	192.1…	Tacacs	tacacs

User Setup

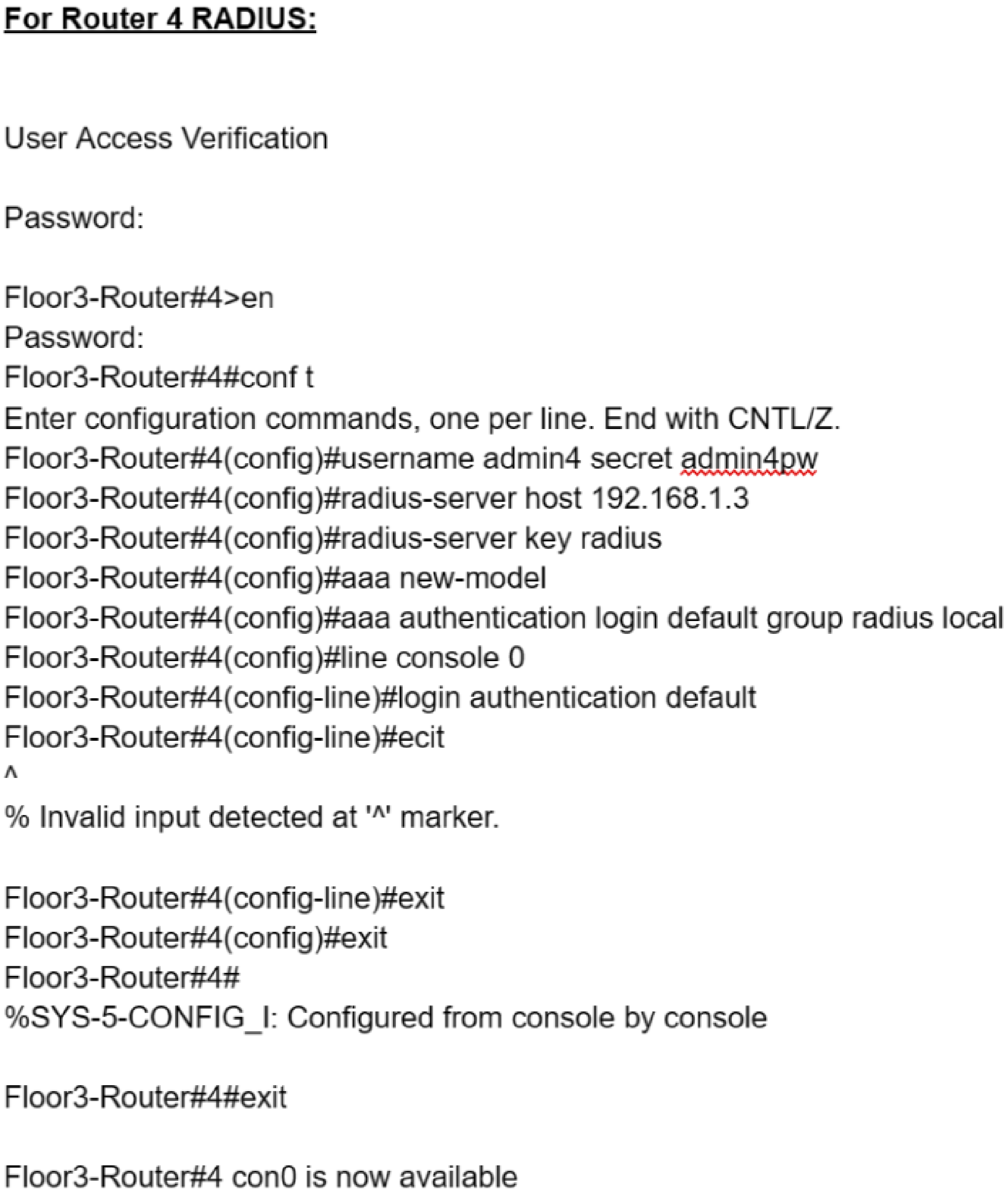
Username

Password

	Username	Password
1	user3	user3pw

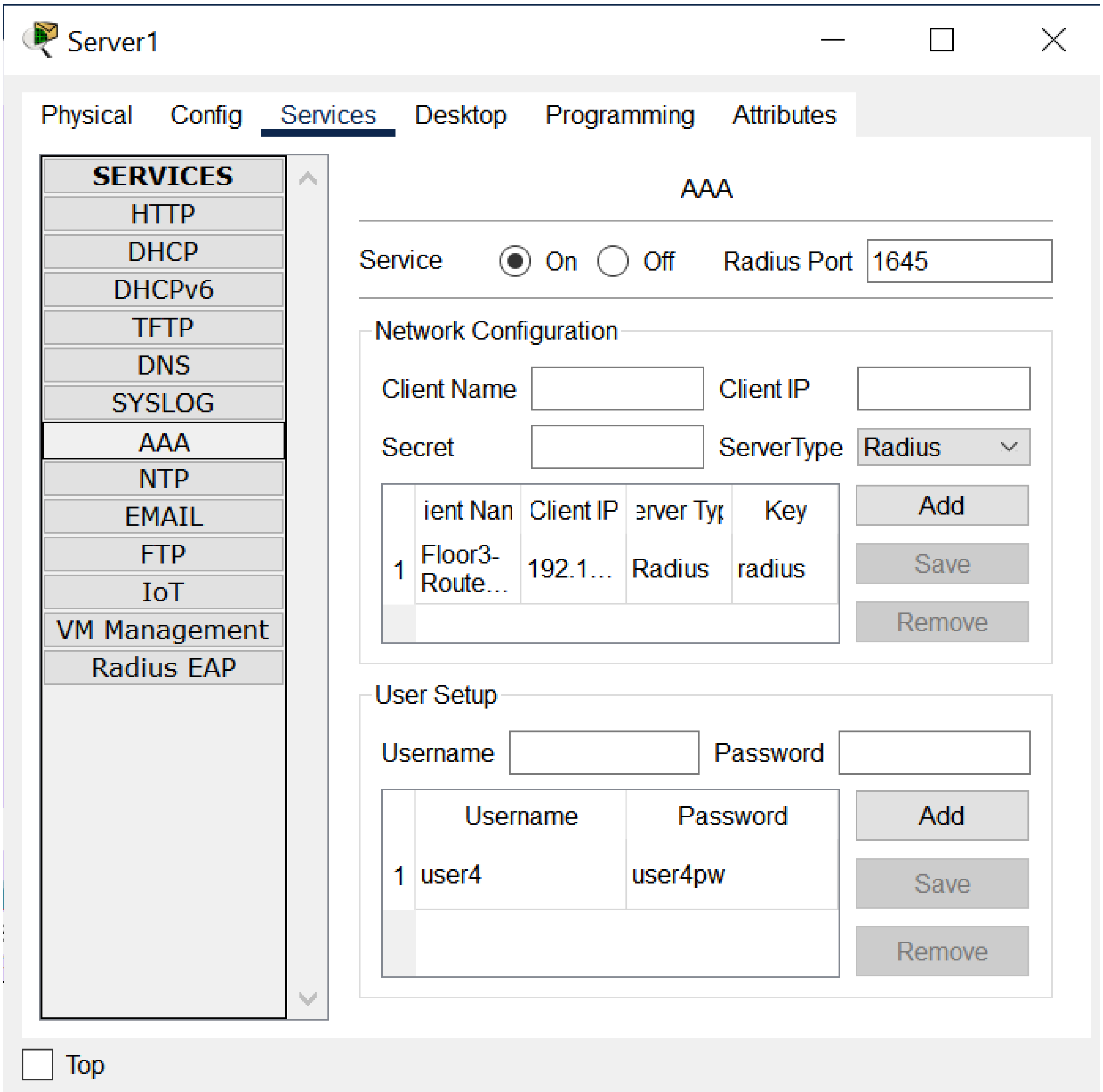
RADIUS

RADIUS (Remote Authentication Dial In User Service) is an authentication and authorization protocol used to provide centralised AAA (Authentication, Authorization, and Accounting) management for users connecting to a network. RADIUS functions as a client-server protocol, authenticating each user with a unique encryption key when access is granted. It is used to authenticate and authorise users and track their activity on a network. It also provides security for wireless hotspots and remote access, and for billing users for their network usage.



For Router 4 RADIUS:

```
User Access Verification

Password:

Floor3-Router#4>en
Password:
Floor3-Router#4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Floor3-Router#4(config)#username admin4 secret admin4pw
Floor3-Router#4(config)#radius-server host 192.168.1.3
Floor3-Router#4(config)#radius-server key radius
Floor3-Router#4(config)#aaa new-model
Floor3-Router#4(config)#aaa authentication login default group radius local
Floor3-Router#4(config)#line console 0
Floor3-Router#4(config-line)#login authentication default
Floor3-Router#4(config-line)#ecit
^
% Invalid input detected at '^' marker.

Floor3-Router#4(config-line)#exit
Floor3-Router#4(config)#exit
Floor3-Router#4#
%SYS-5-CONFIG_I: Configured from console by console

Floor3-Router#4#exit

Floor3-Router#4 con0 is now available
```



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	ient Nan	Client IP	erver Typ	Key
1	Floor3-Route...	192.1...	Radius	radius

User Setup

Username Password

	Username	Password
1	user4	user4pw

□ Top

Intrusion Prevention System

Introduction

The terms intrusion detection and prevention system and intrusion prevention system are interchangeable.It is a network security tool that checks system or network activity for suspicious behaviour. The main duties of intrusion prevention systems are to spot harmful activity, gather data on it, report it, and make an effort to block or stop it.

In this topology , the Intrusion Prevention System(IPS) is being used in the form of Host-based intrusion prevention system (HIPS) which is an inbuilt software package which operates a single host (General-Management-Router#4) for doubtful activity by scanning events that occur within that host. The HIPS in this case is signature-based which operates by comparing packets in the network and compares with pre-built and preordained attack patterns known as signatures.

The IPS is implemented in the devices in the purple square in the figure below and is isolated from the rest of the topology by ensuring that it can communicate with each other but they cannot communicate with the rest of the topology.

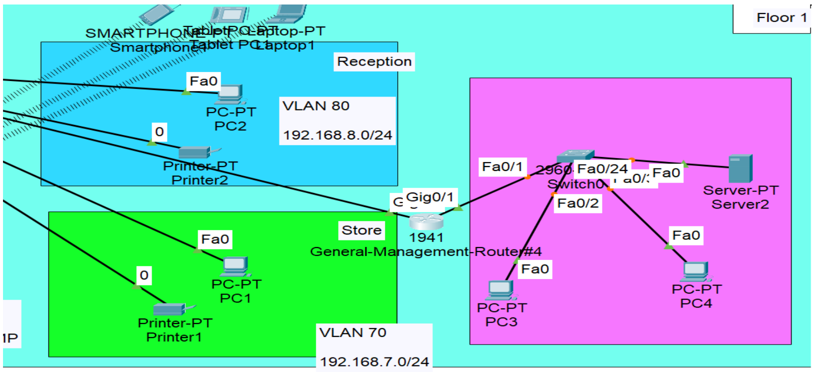
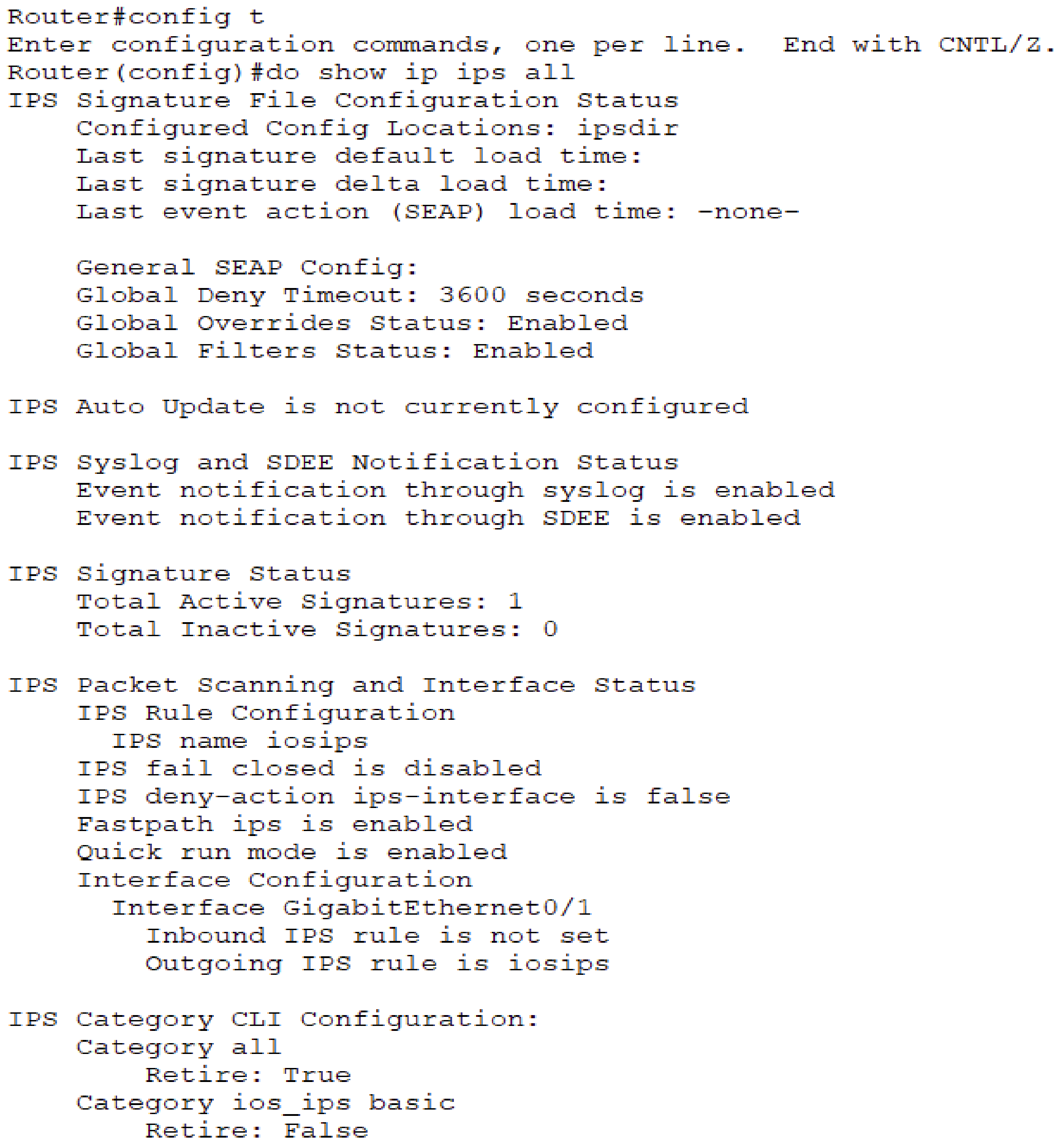


Figure above show the Floor 1 section of the proposed topology



```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#do show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
        Retire: True
    Category ios_ips basic
        Retire: False
```

Figure above shows the settings of the enabled IPS

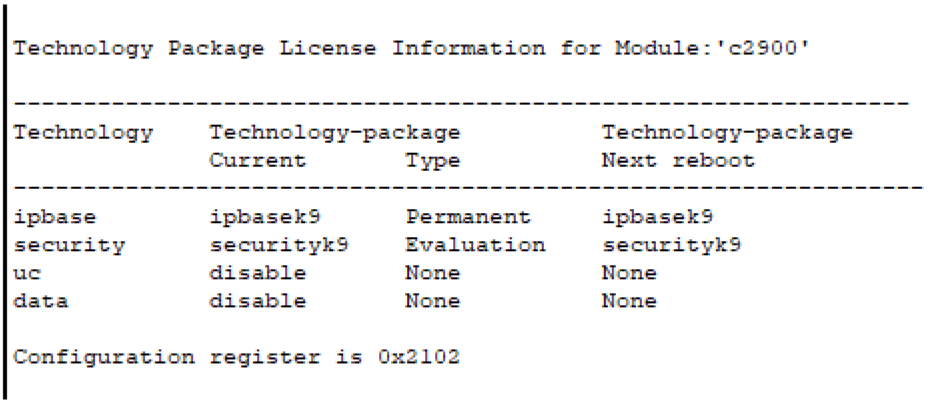
Additional Security Features

Security K9 Packages

Security K9 has been installed to each router using the command :

Router(config)#license boot module c2900 technology-package securityk9
(For routers 2911)

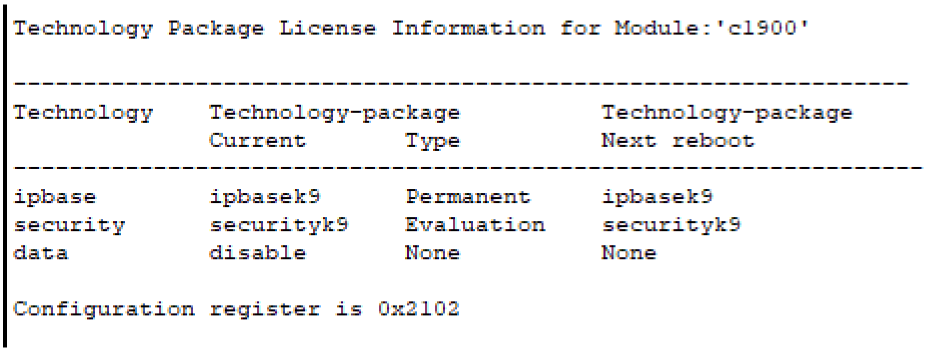
Proof : (From Show Version after reloading router)



```
Technology Package License Information for Module:'c2900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
uc            disable       None           None
data          disable       None           None

Configuration register is 0x2102
```

Router(config)#license boot module c1900 technology-package securityk9
(For routers 1911)

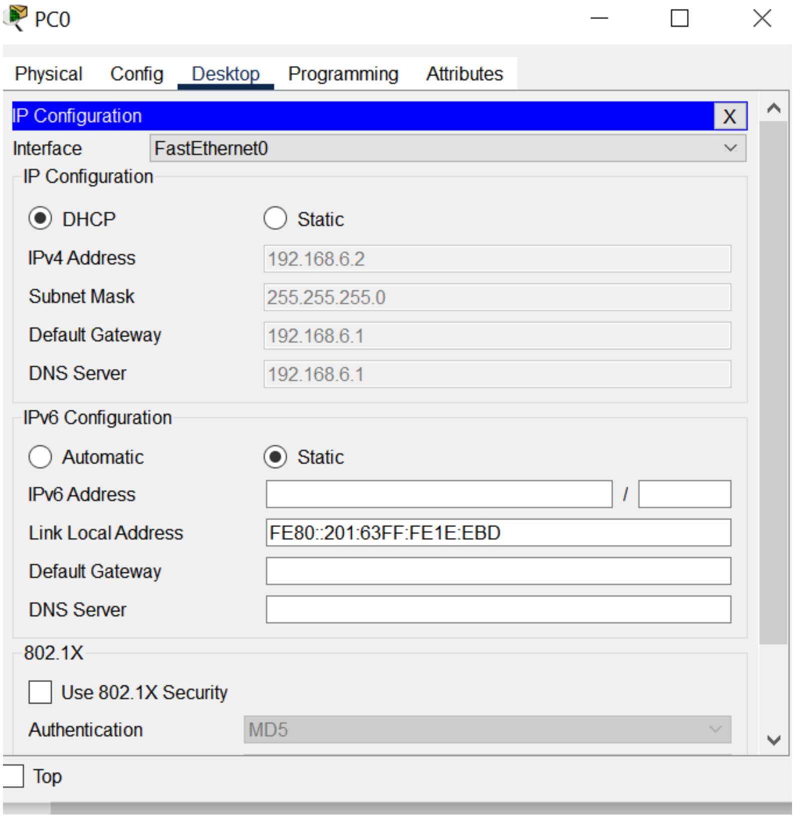
Proof : (From Show Version after reloading router)



```
Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None

Configuration register is 0x2102
```

Working Device Configurations

PC's



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.6.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.6.1

DNS Server: 192.168.6.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:63FF:FE1E:EBD

Default Gateway:

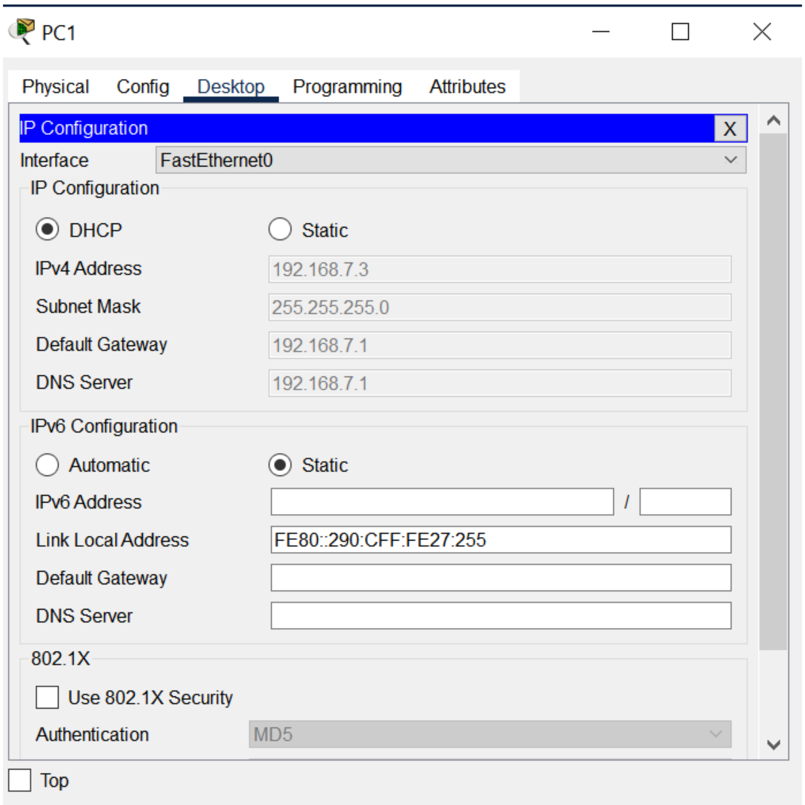
DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.7.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.7.1

DNS Server: 192.168.7.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::290:CFF:FE27:255

Default Gateway:

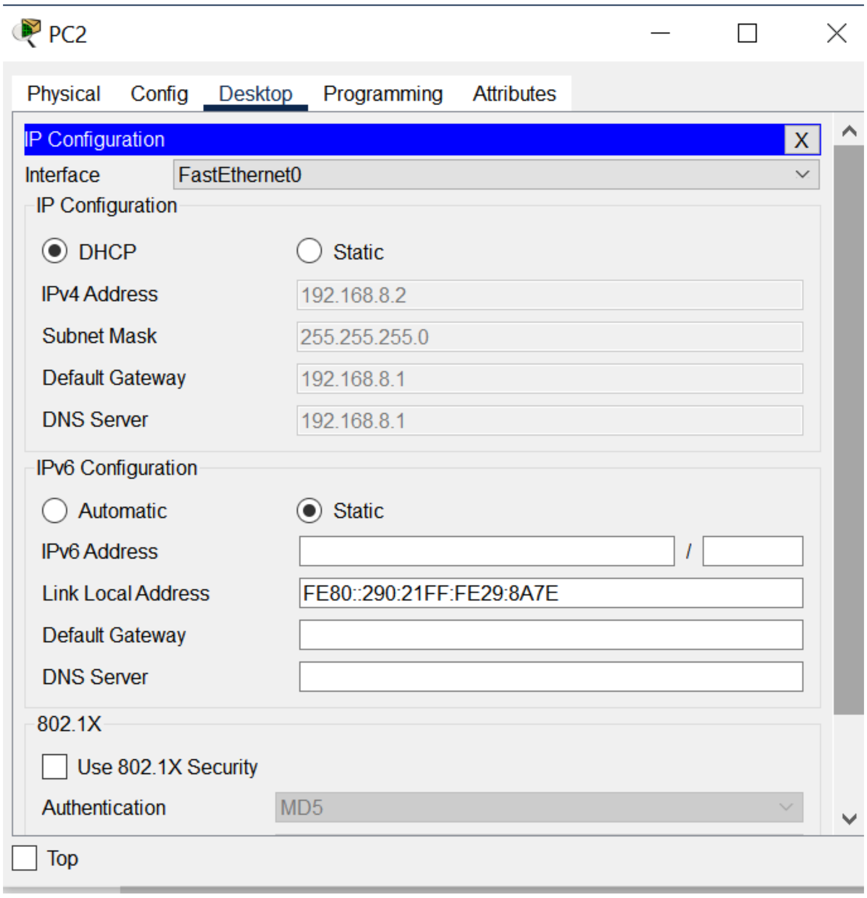
DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.8.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.8.1

DNS Server: 192.168.8.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::290:21FF:FE29:8A7E

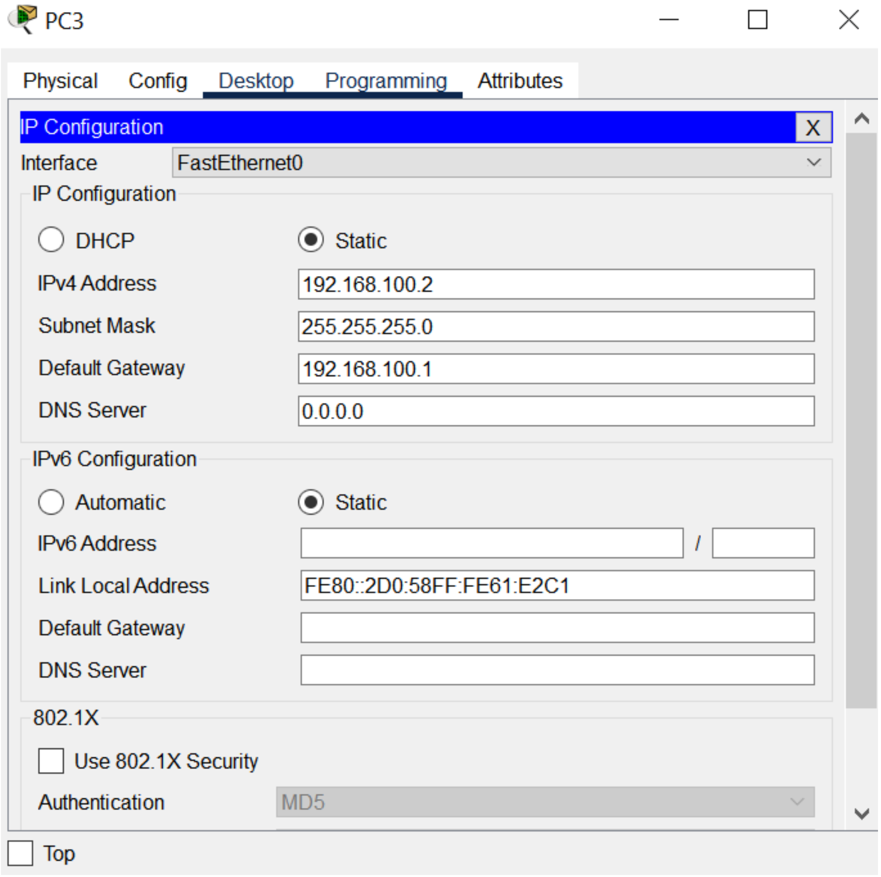
Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.100.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.100.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:58FF:FE61:E2C1

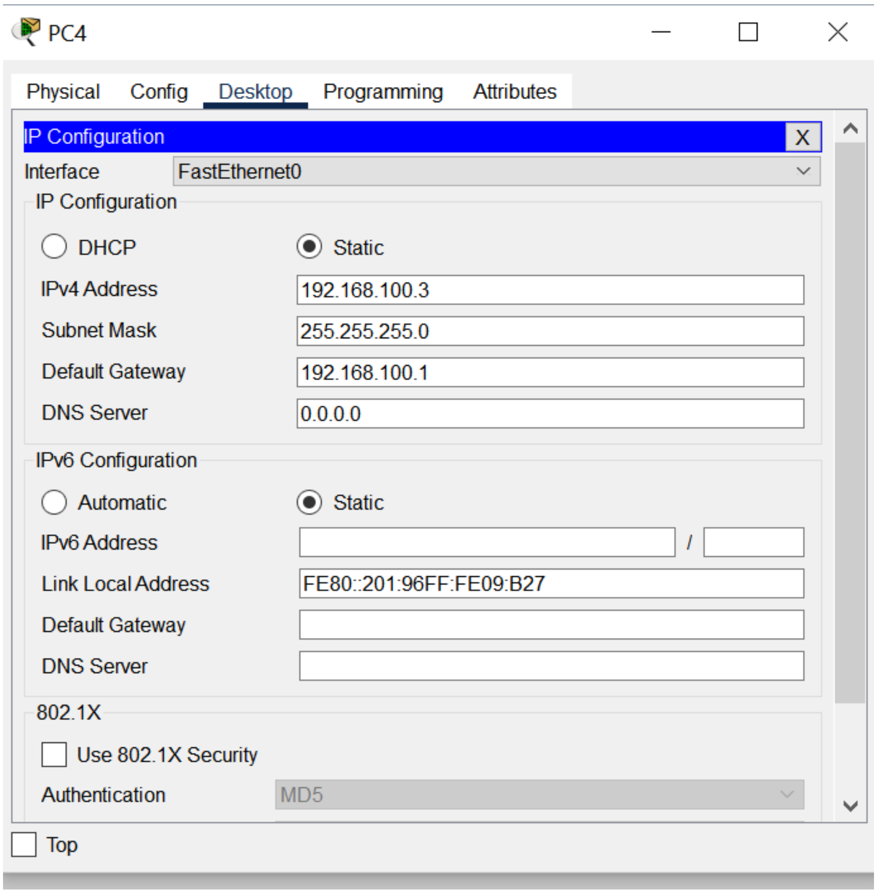
Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5



PC4

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.100.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.100.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:96FF:FE09:B27

Default Gateway:

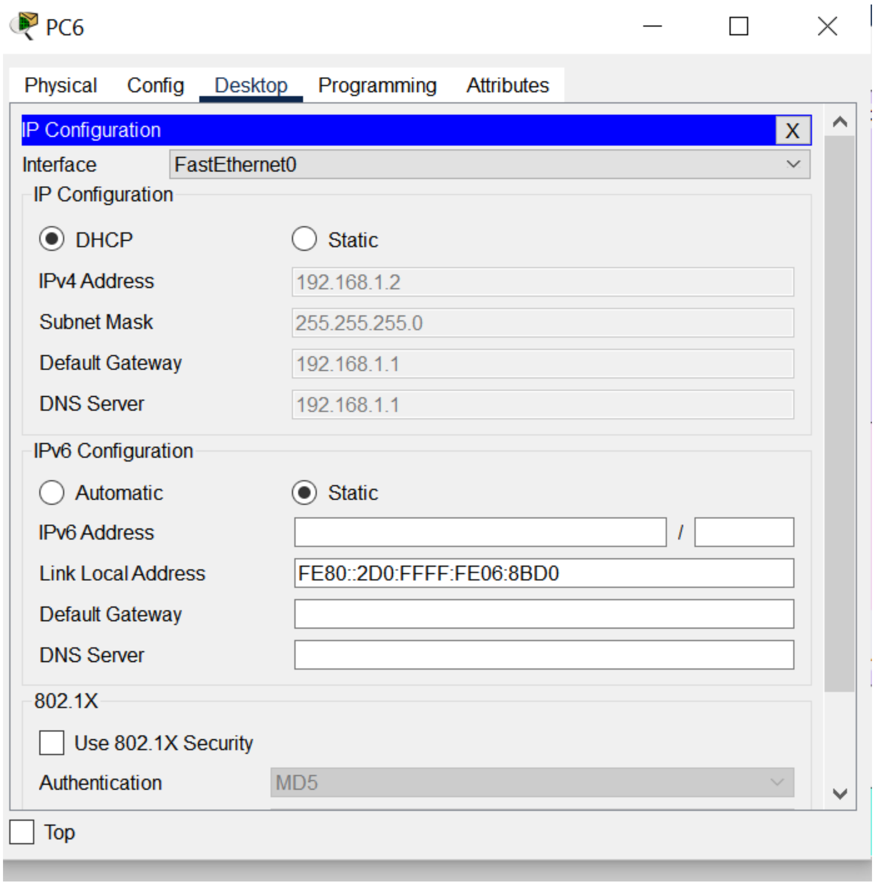
DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top



PC6

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:FFFF:FE06:8BD0

Default Gateway:

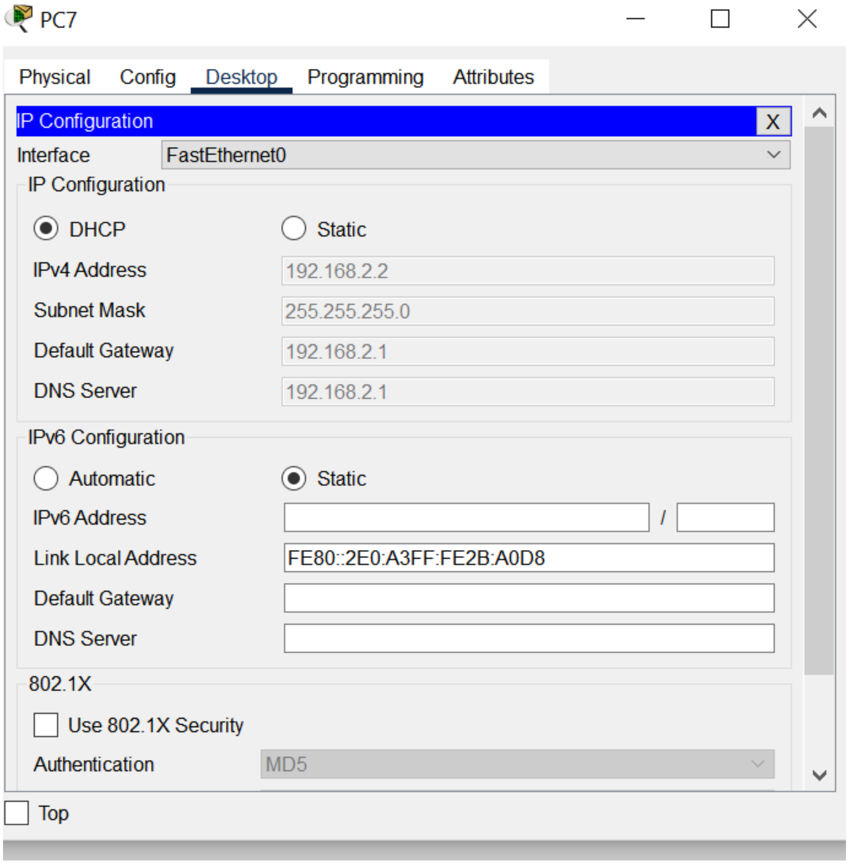
DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 192.168.2.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:A3FF:FE2B:A0D8

Default Gateway:

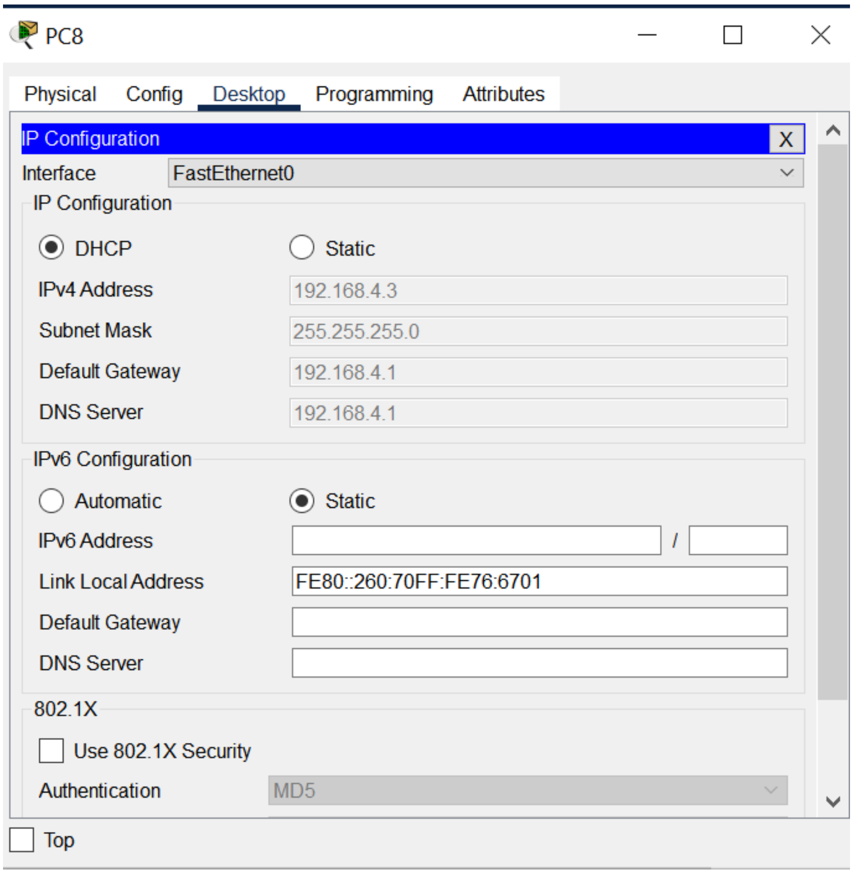
DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.4.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 192.168.4.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::260:70FF:FE76:6701

Default Gateway:

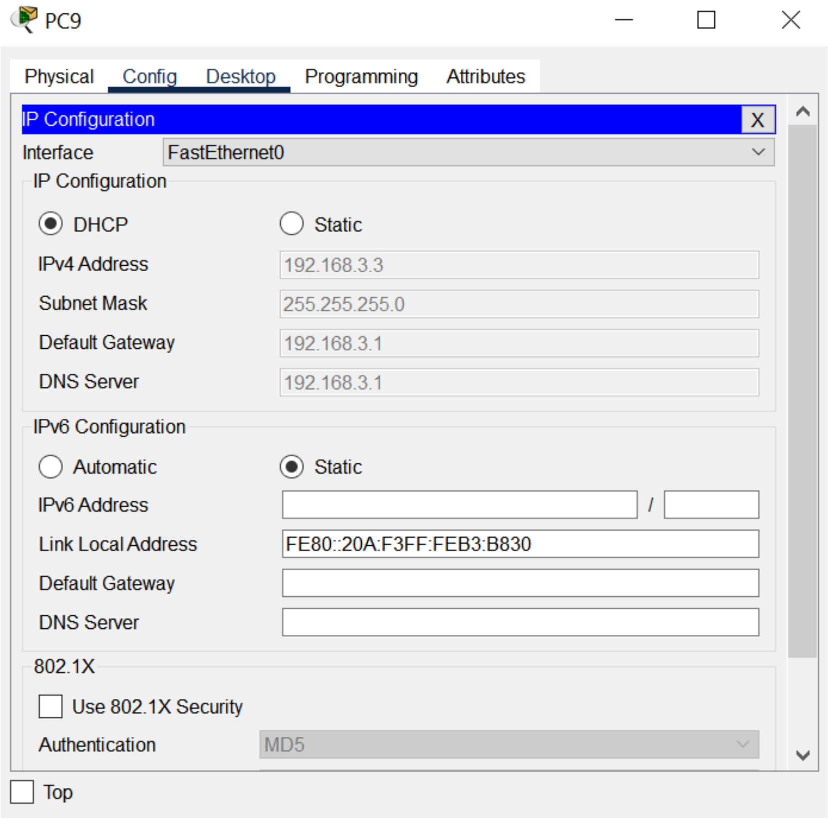
DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.3.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.3.1

DNS Server 192.168.3.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::20A:F3FF:FEB3:B830

Default Gateway

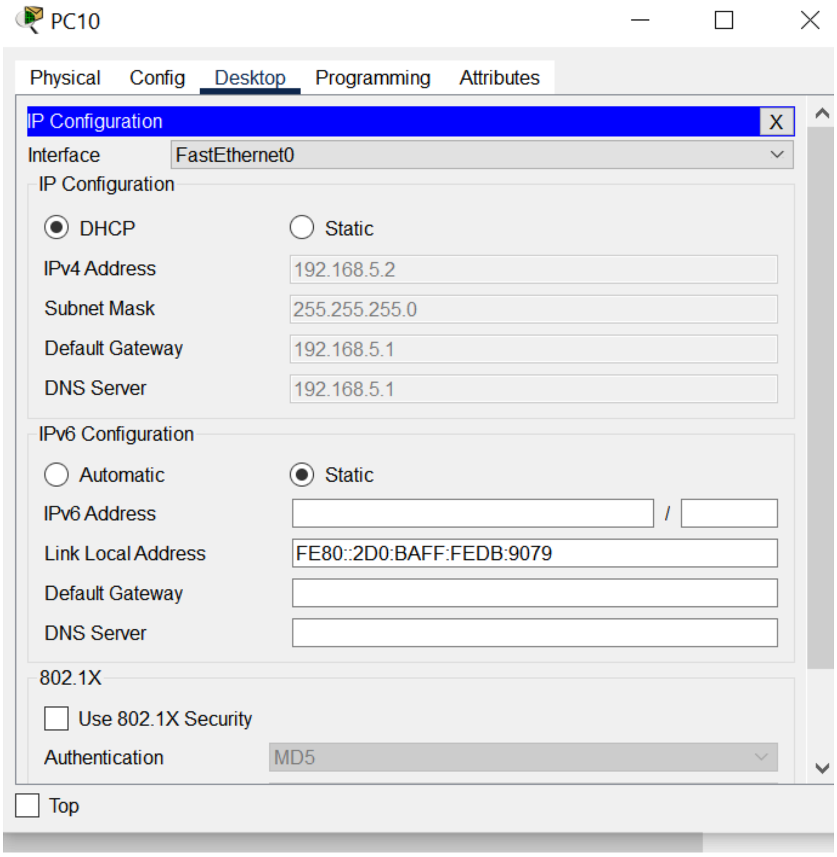
DNS Server

802.1X

□ Use 802.1X Security

Authentication MD5

□ Top



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.5.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.5.1

DNS Server 192.168.5.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::2D0:BAFF:FEDB:9079

Default Gateway

DNS Server

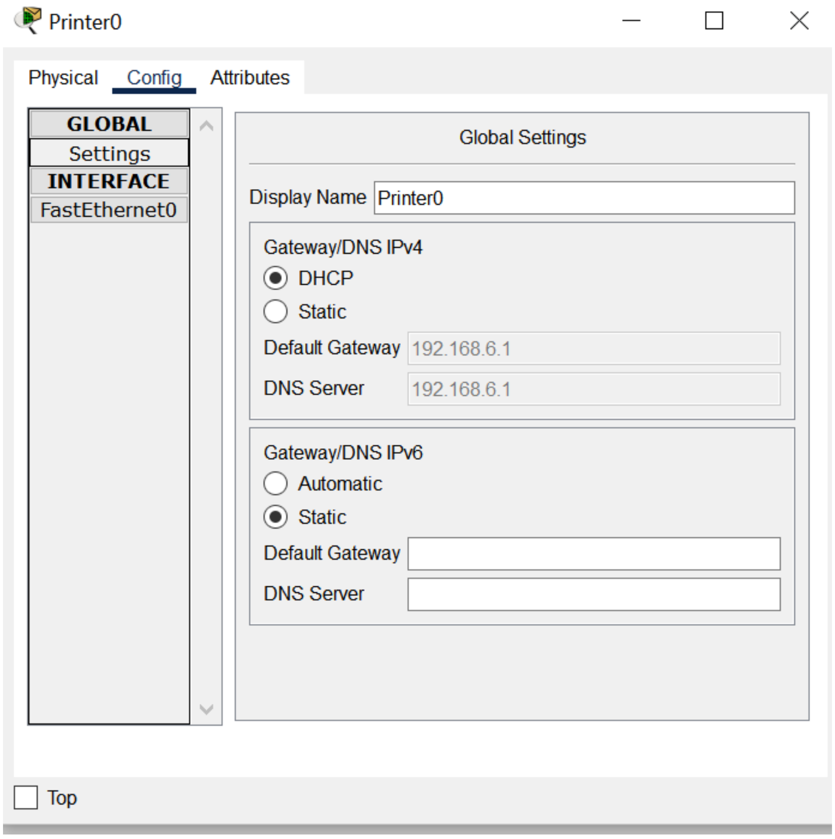
802.1X

□ Use 802.1X Security

Authentication MD5

□ Top

Printers

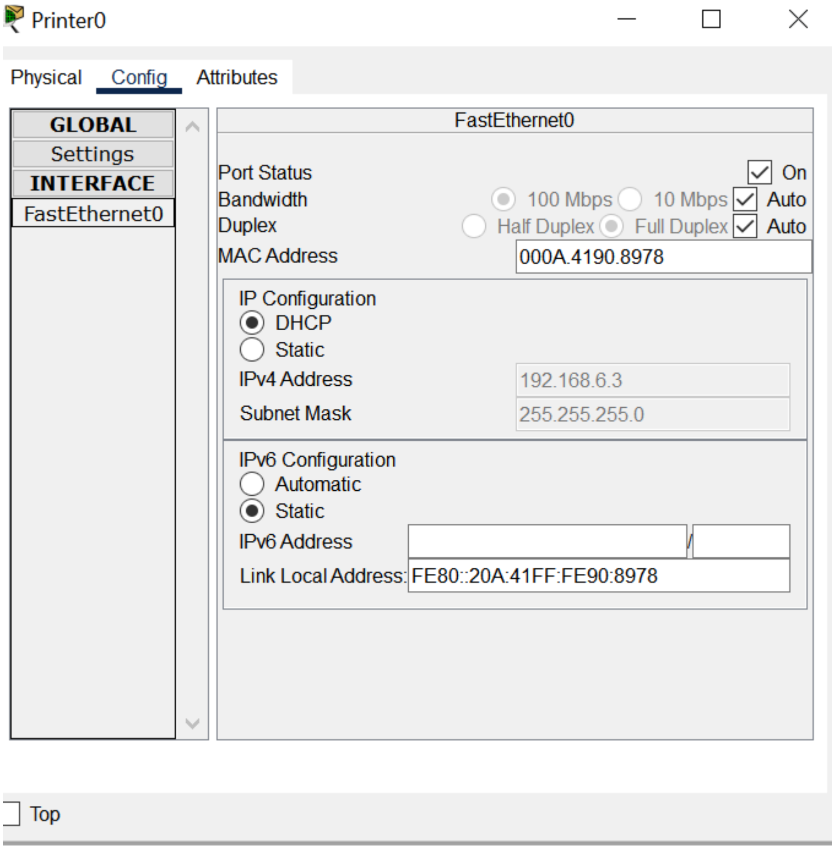


Global Settings

Display Name: Printer0

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway: 192.168.6.1
DNS Server: 192.168.6.1

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

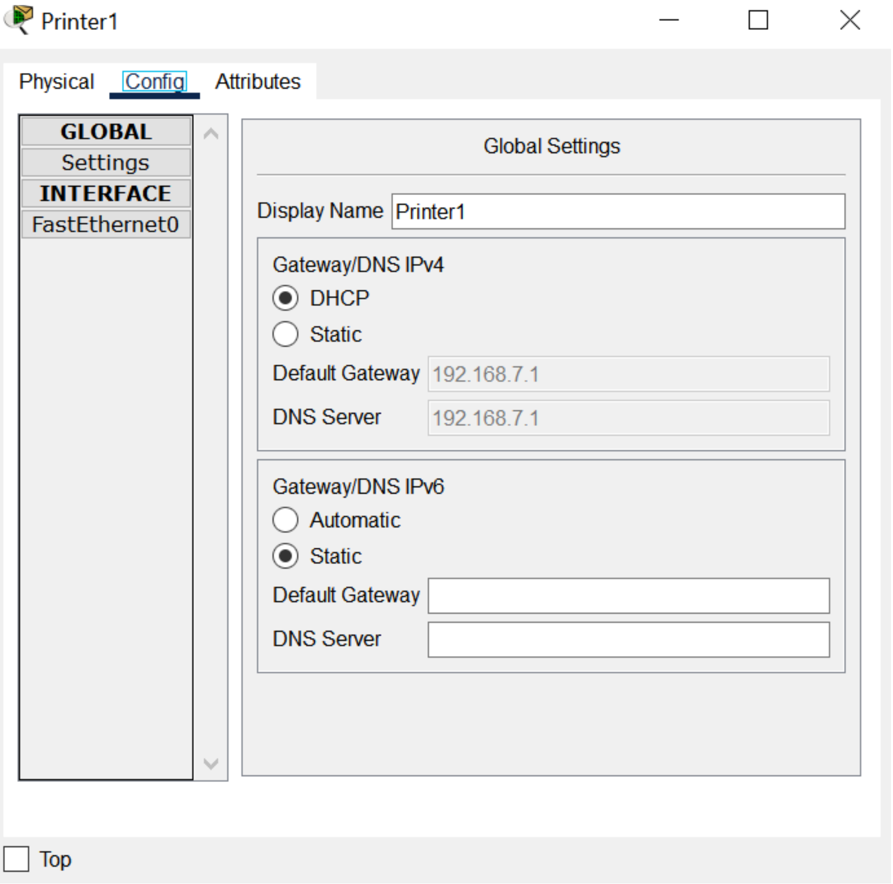


FastEthernet0

Port Status: ☑ On
Bandwidth: ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex: ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 000A.4190.8978

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.6.3
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::20A:41FF:FE90:8978



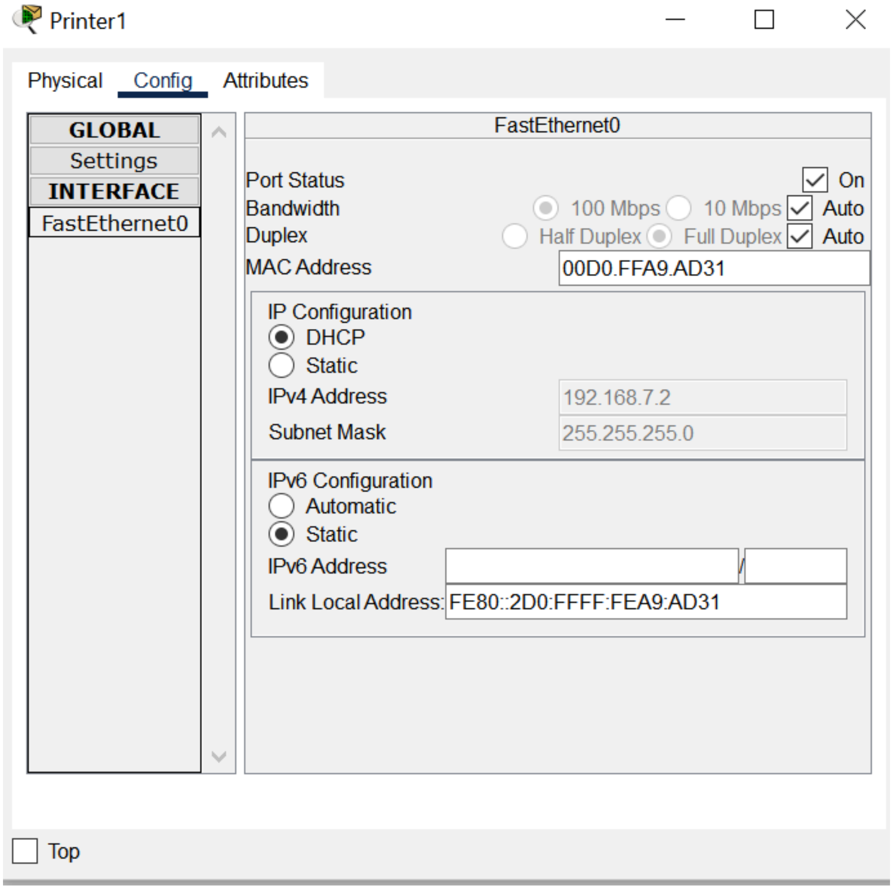
Global Settings

Display Name: Printer1

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway: 192.168.7.1
DNS Server: 192.168.7.1

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

□ Top



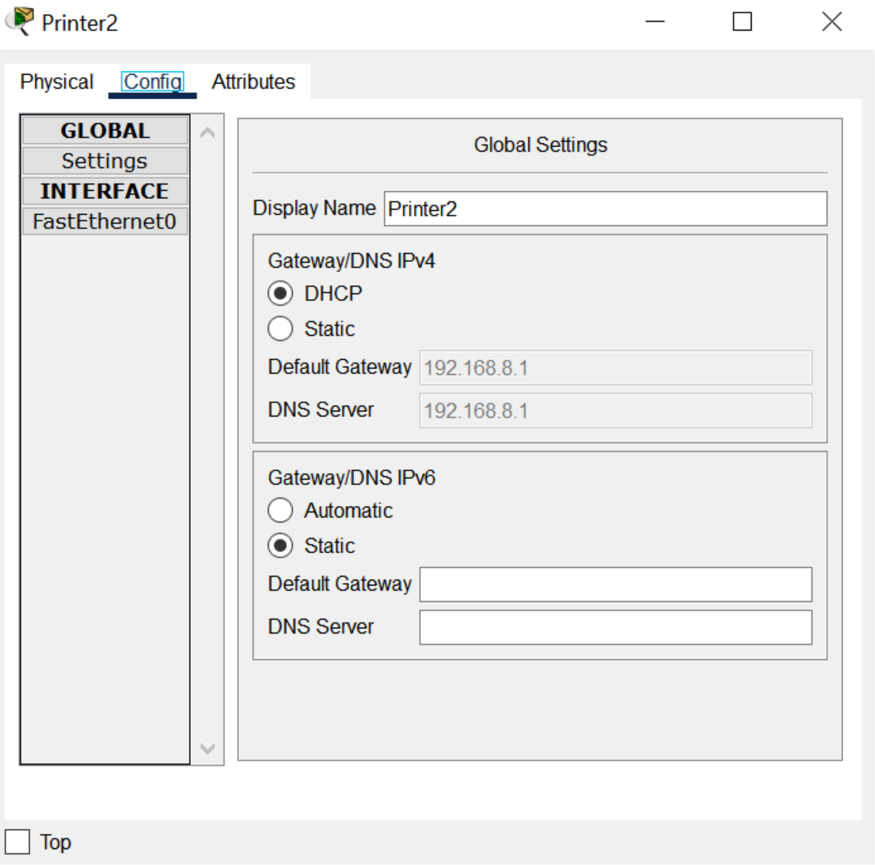
FastEthernet0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 00D0.FFA9.AD31

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.7.2
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::2D0:FFFF:FEA9:AD31

□ Top



Printer2

Global Settings

Display Name: Printer2

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.8.1

DNS Server: 192.168.8.1

Gateway/DNS IPv6

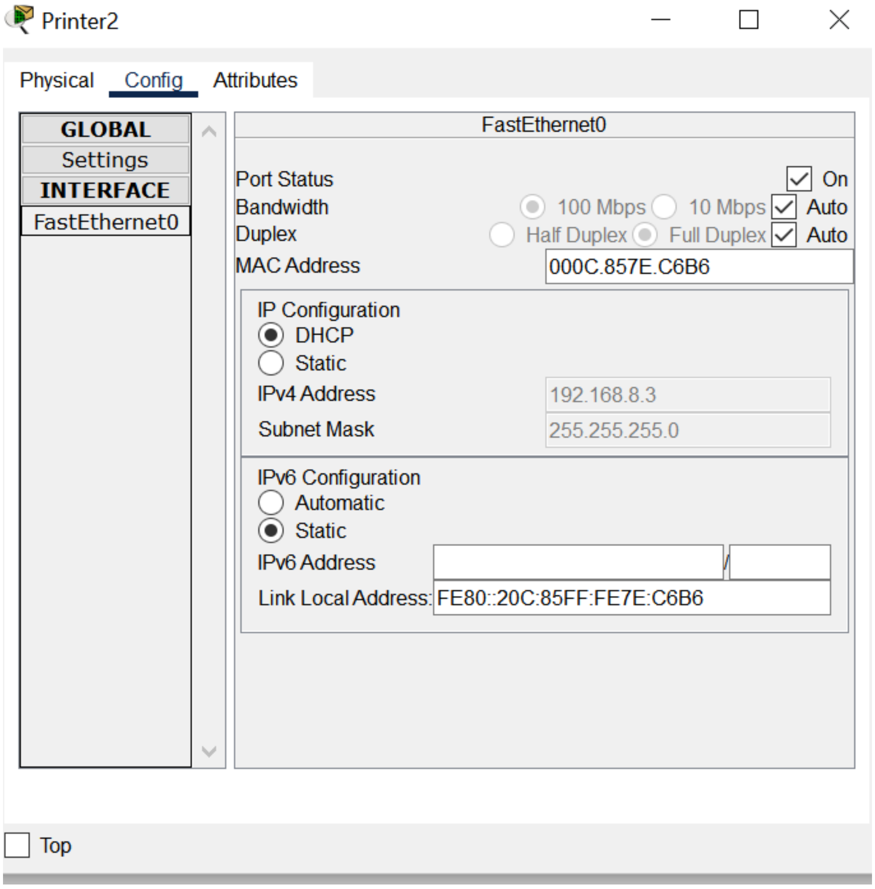
○ Automatic

● Static

Default Gateway:

DNS Server:

□ Top



Printer2

FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address: 000C.857E.C6B6

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.8.3

Subnet Mask: 255.255.255.0

IPv6 Configuration

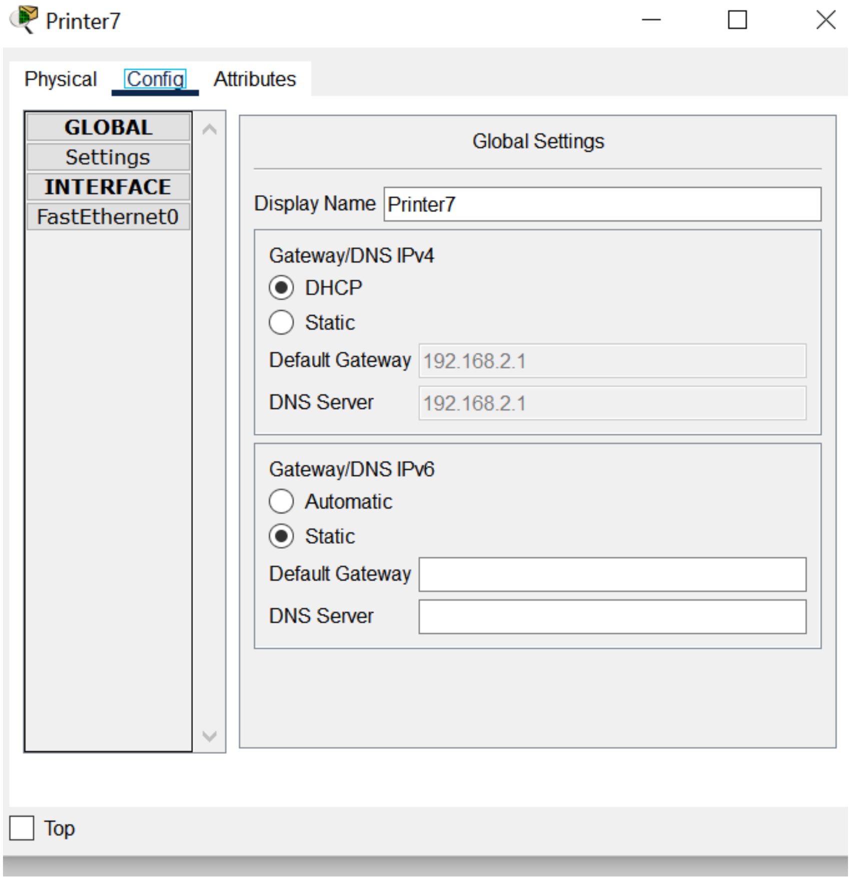
○ Automatic

● Static

IPv6 Address: /

Link Local Address: FE80::20C:85FF:FE7E:C6B6

□ Top

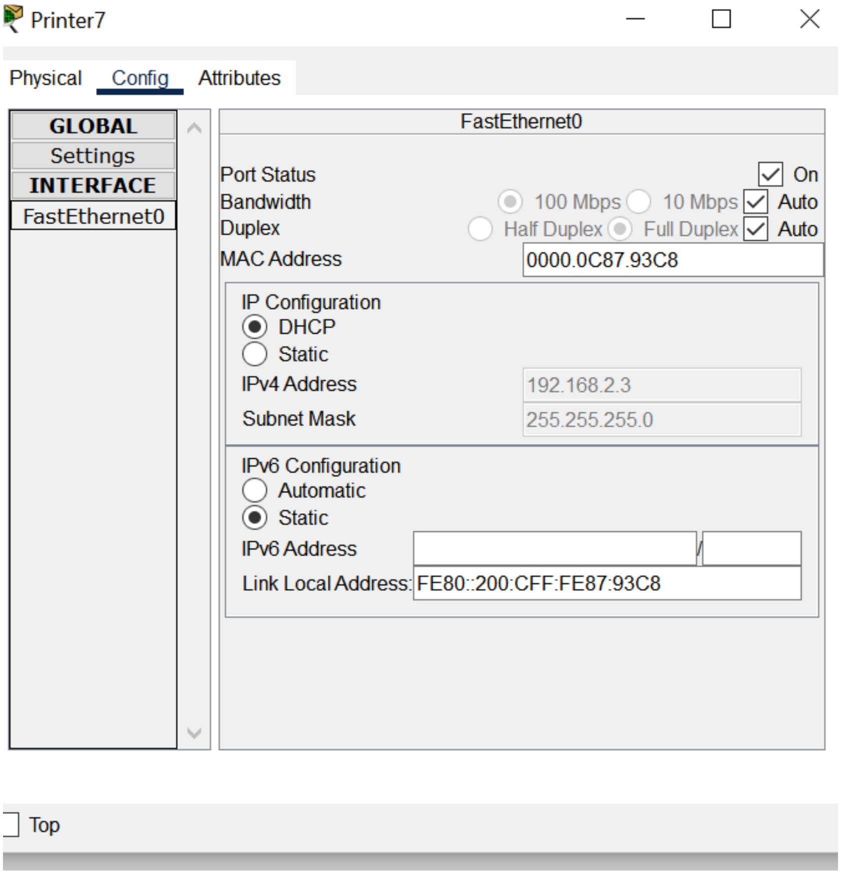


Global Settings

Display Name: Printer7

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway: 192.168.2.1
DNS Server: 192.168.2.1

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

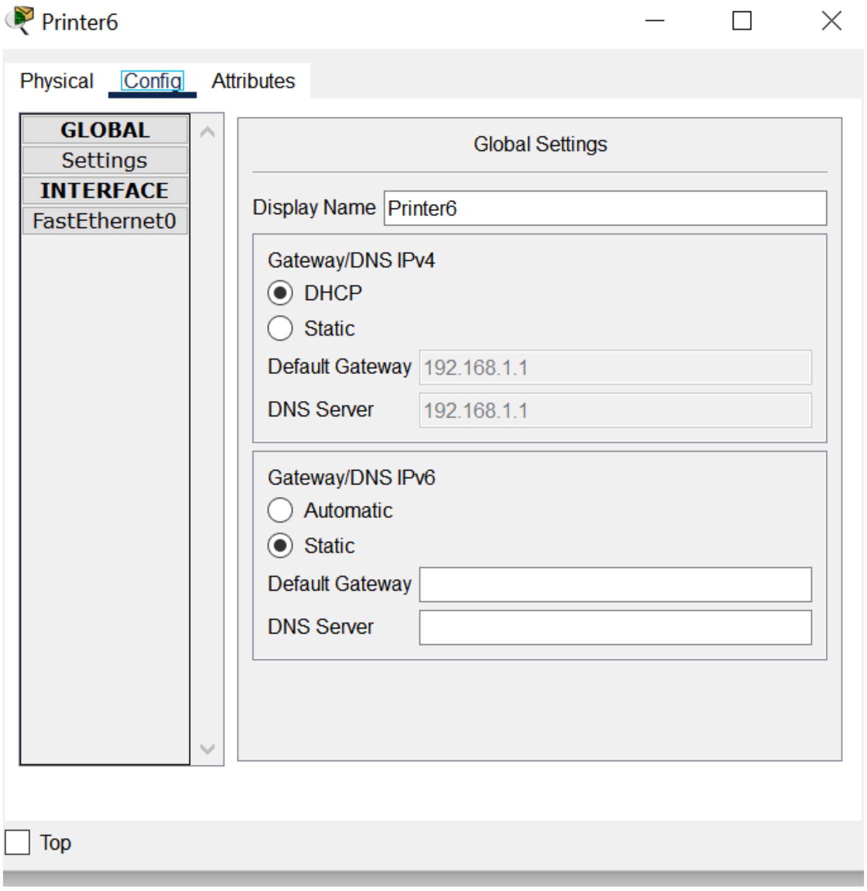


FastEthernet0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 0000.0C87.93C8

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.2.3
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::200:CFF:FE87:93C8



Printer6

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
FastEthernet0

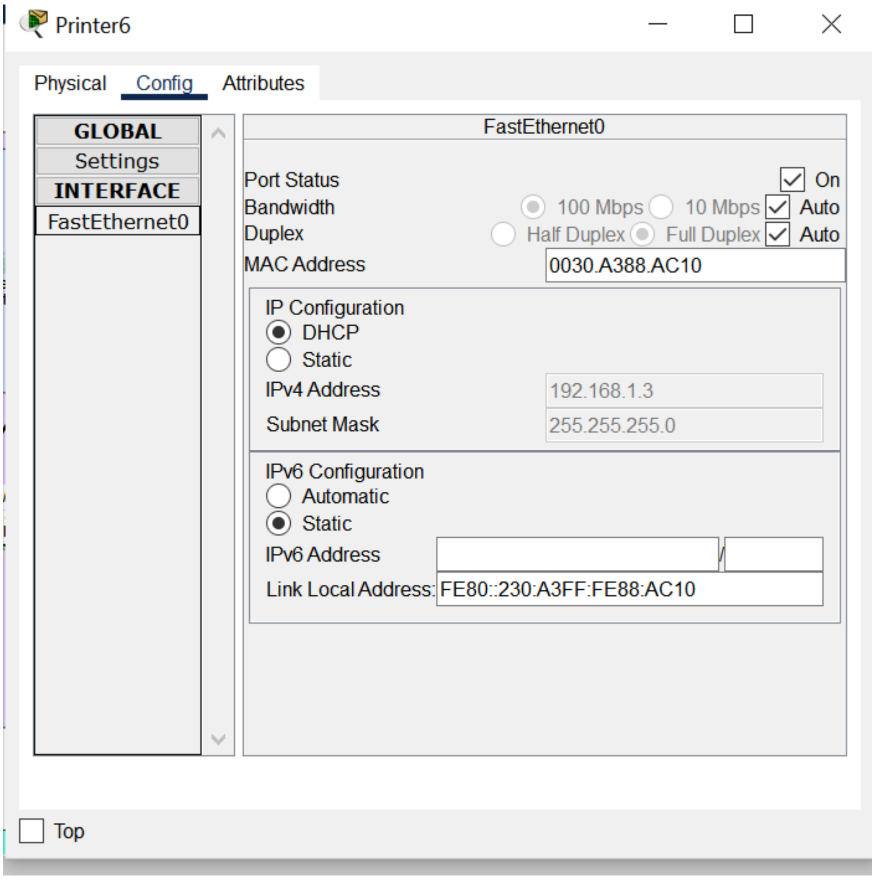
Global Settings

Display Name: Printer6

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway: 192.168.1.1
DNS Server: 192.168.1.1

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

□ Top



Printer6

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
FastEthernet0

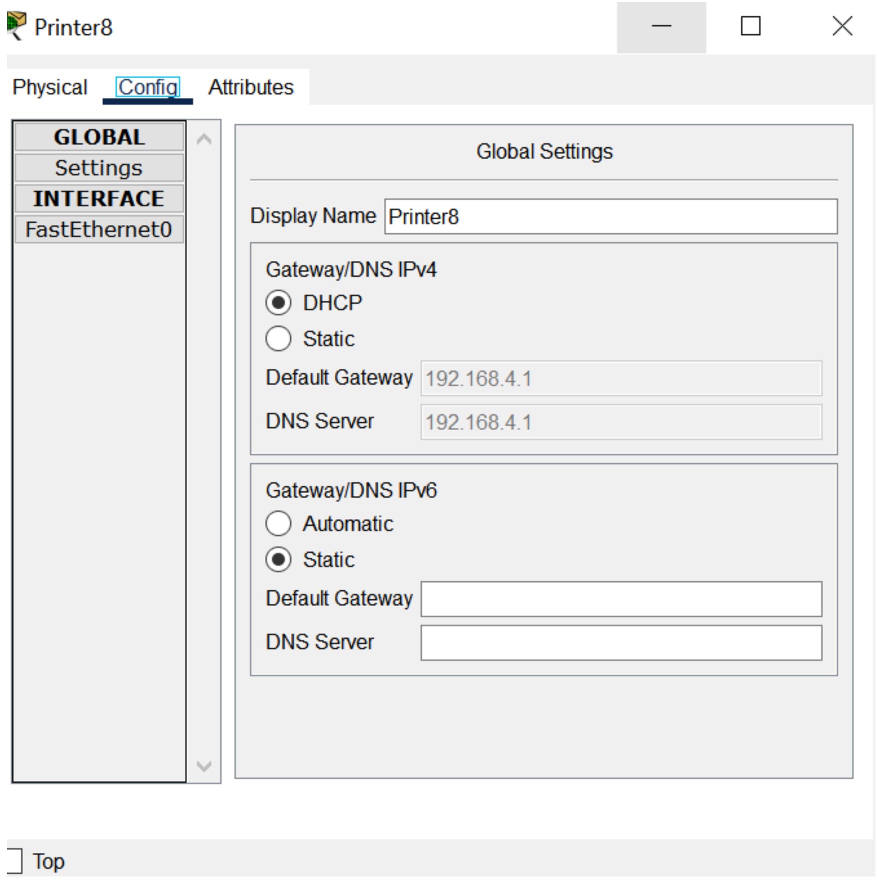
FastEthernet0

Port Status: ☑ On
Bandwidth: ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex: ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 0030.A388.AC10

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.1.3
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::230:A3FF:FE88:AC10

□ Top



Printer8

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
FastEthernet0

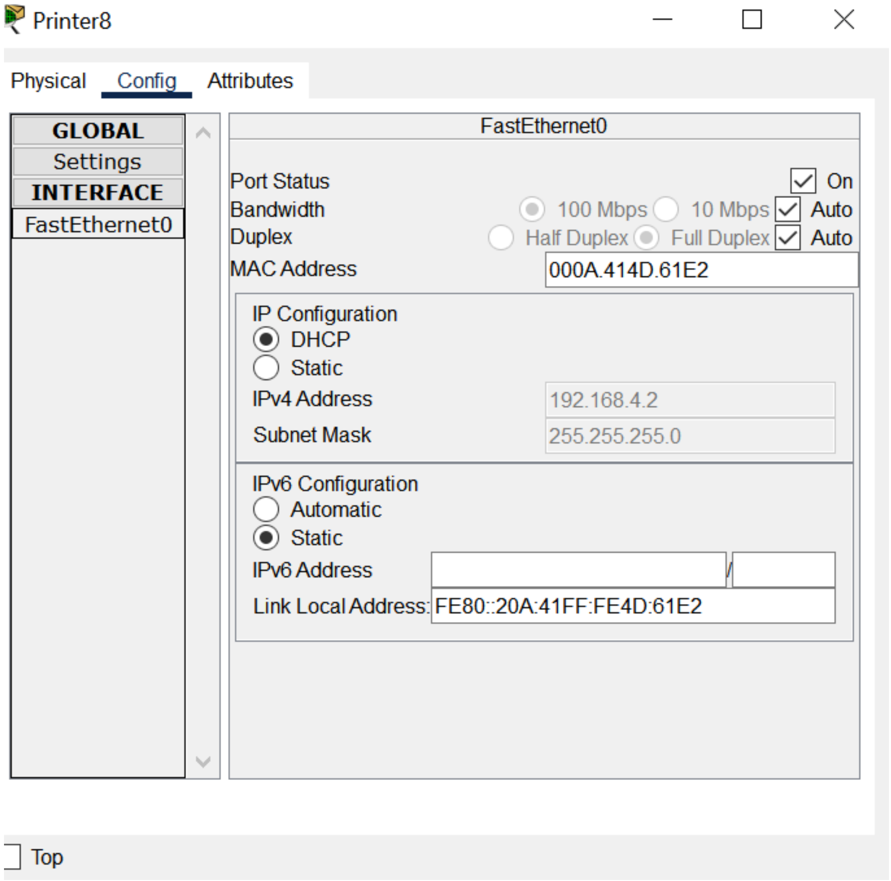
Global Settings

Display Name: Printer8

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway: 192.168.4.1
DNS Server: 192.168.4.1

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

□ Top



Printer8

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
FastEthernet0

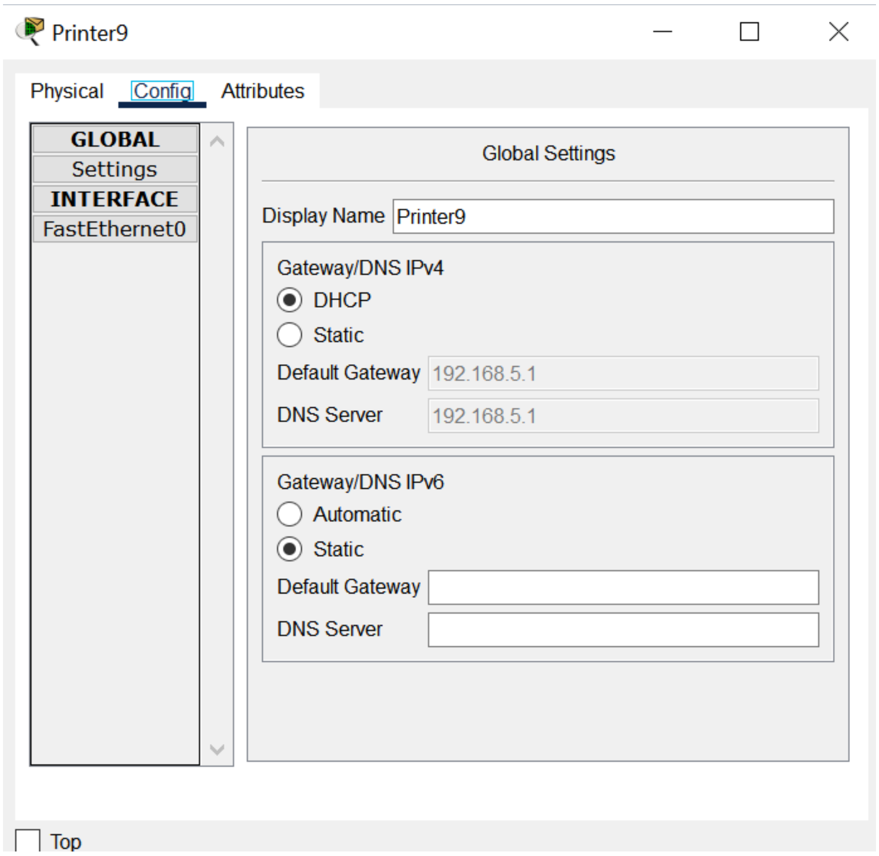
FastEthernet0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 000A.414D.61E2

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.4.2
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::20A:41FF:FE4D:61E2

□ Top



Printer9

Global Settings

Display Name: Printer9

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.5.1

DNS Server: 192.168.5.1

Gateway/DNS IPv6

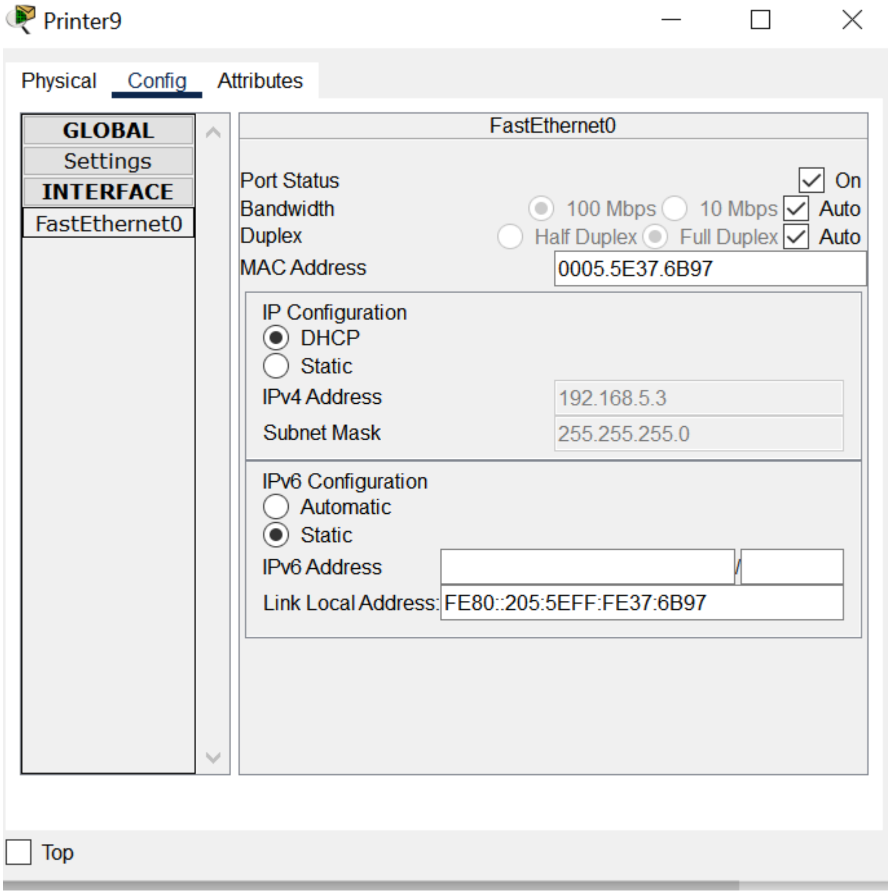
○ Automatic

● Static

Default Gateway:

DNS Server:

□ Top



Printer9

FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 0005.5E37.6B97

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.5.3

Subnet Mask: 255.255.255.0

IPv6 Configuration

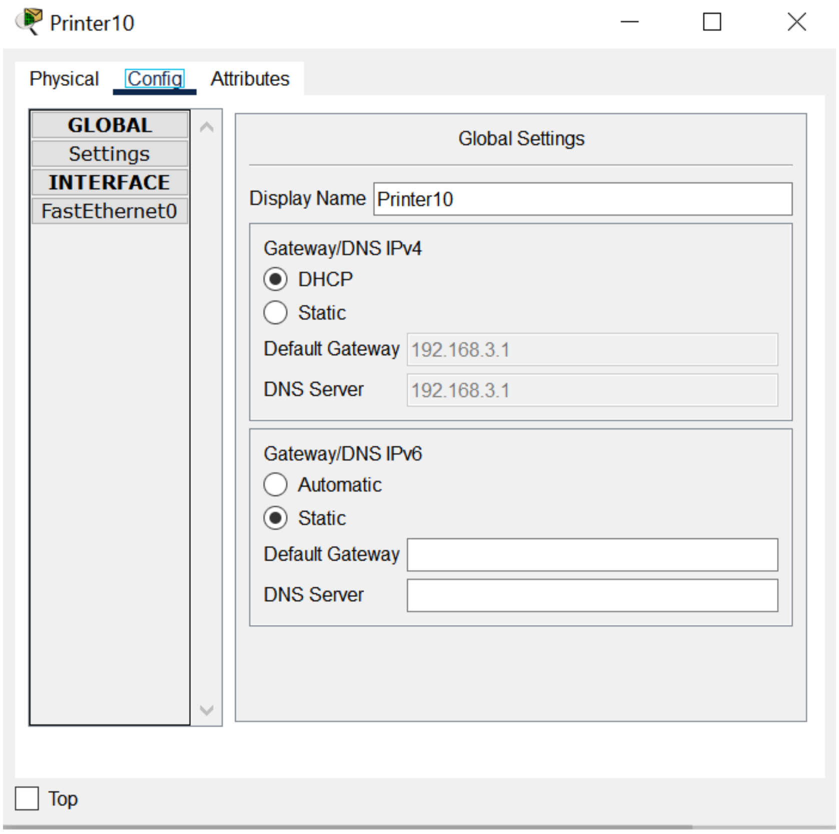
○ Automatic

● Static

IPv6 Address: /

Link Local Address: FE80::205:5EFF:FE37:6B97

□ Top



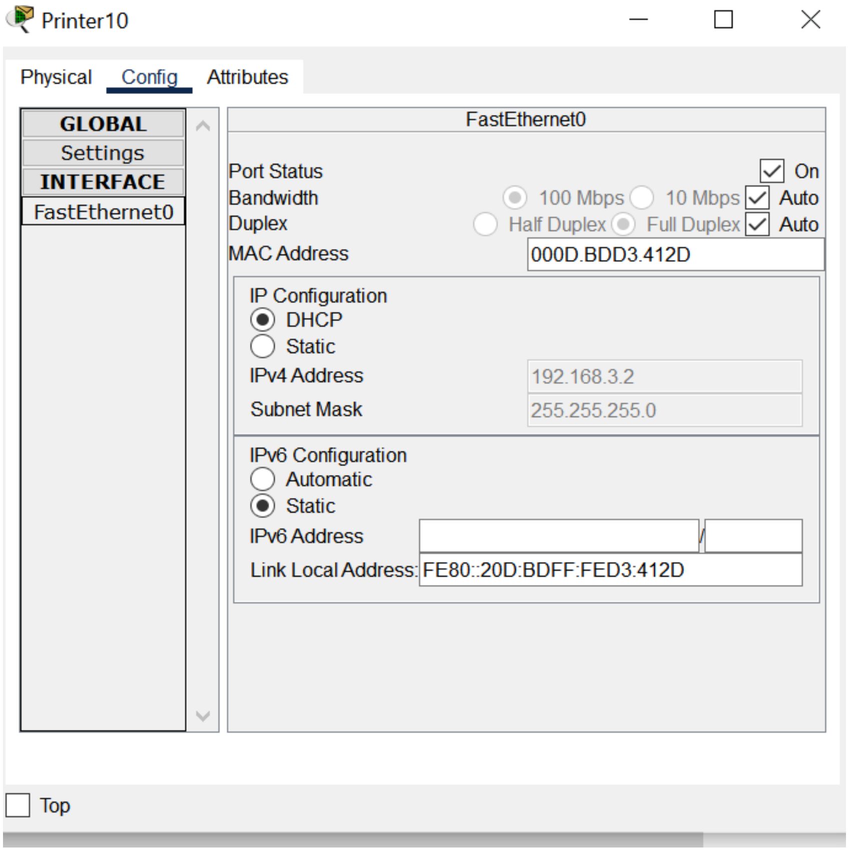
Global Settings

Display Name: Printer10

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway: 192.168.3.1
DNS Server: 192.168.3.1

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

□ Top



FastEthernet0

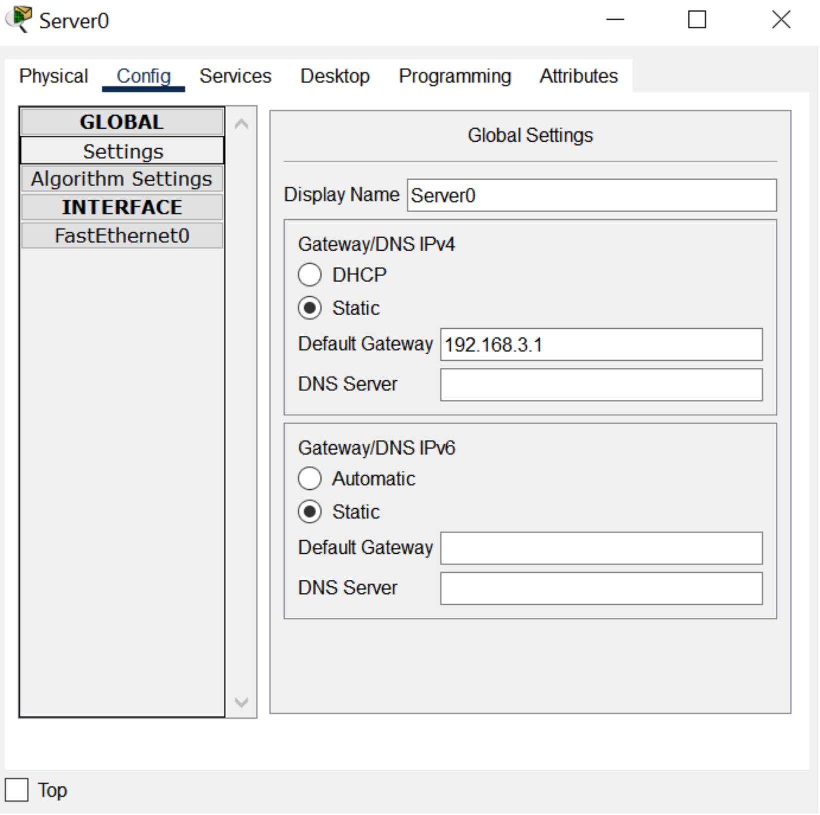
Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 000D.BDD3.412D

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.3.2
Subnet Mask: 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::20D:BDFF:FED3:412D

□ Top

Server



Global Settings

Display Name: Server0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway: 192.168.3.1

DNS Server:

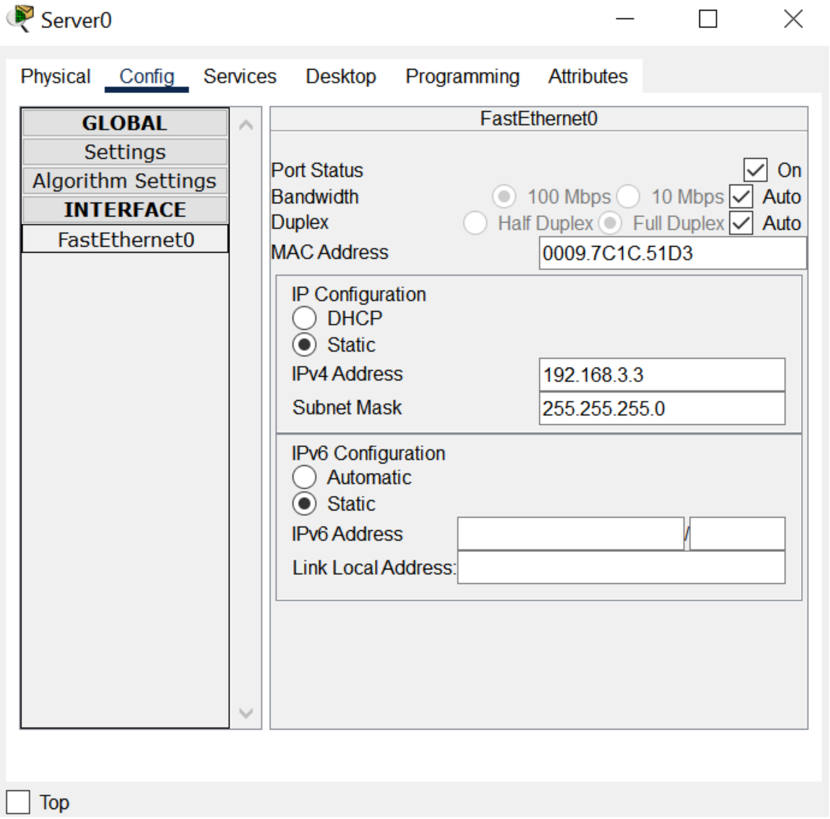
Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway:

DNS Server:



FastEthernet0

Port Status: ☑ On

Bandwidth: ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex: ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address: 0009.7C1C.51D3

IP Configuration

○ DHCP

● Static

IPv4 Address: 192.168.3.3

Subnet Mask: 255.255.255.0

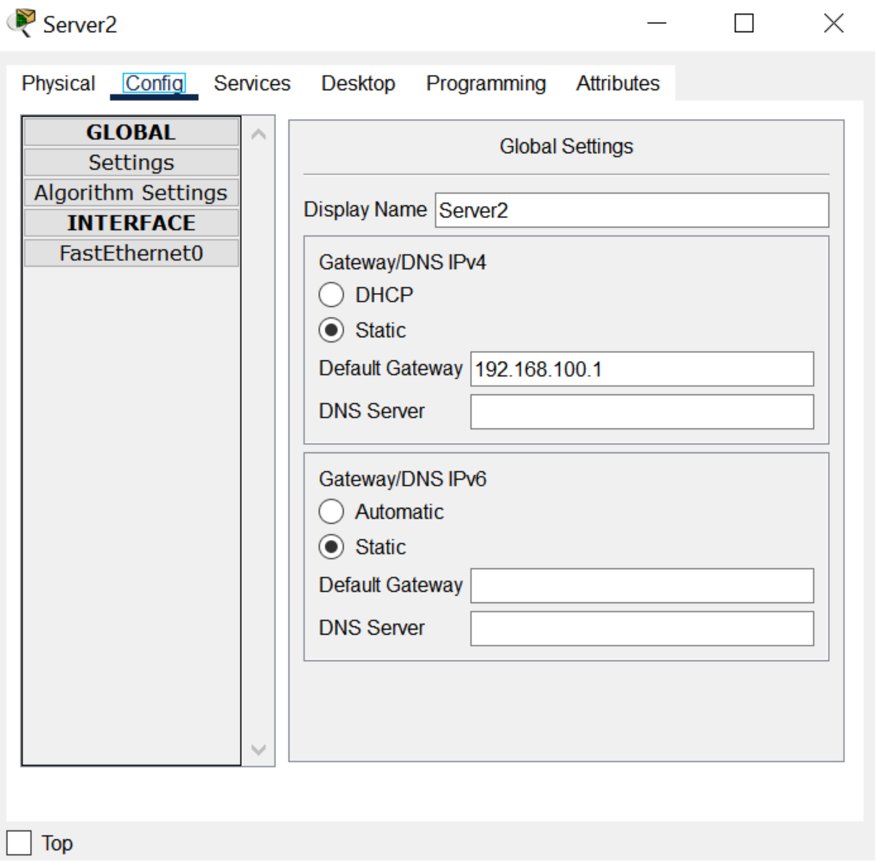
IPv6 Configuration

○ Automatic

● Static

IPv6 Address: /

Link Local Address:



Global Settings

Display Name: Server2

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway: 192.168.100.1

DNS Server:

Gateway/DNS IPv6

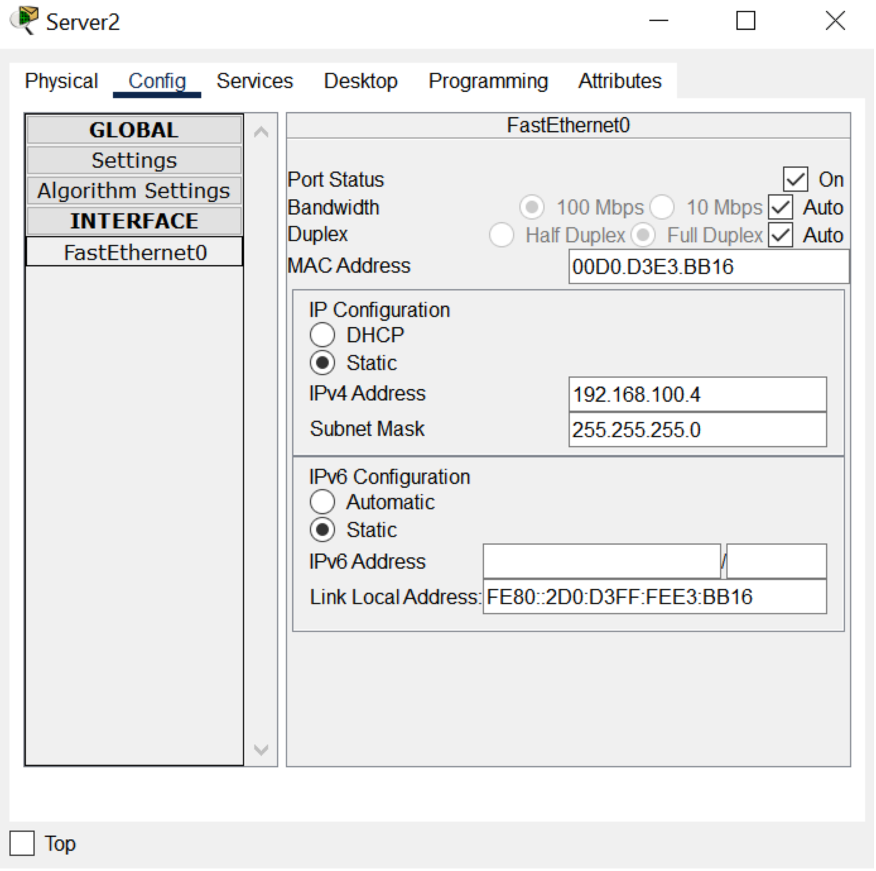
○ Automatic

● Static

Default Gateway:

DNS Server:

□ Top



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 00D0.D3E3.BB16

IP Configuration

○ DHCP

● Static

IPv4 Address: 192.168.100.4

Subnet Mask: 255.255.255.0

IPv6 Configuration

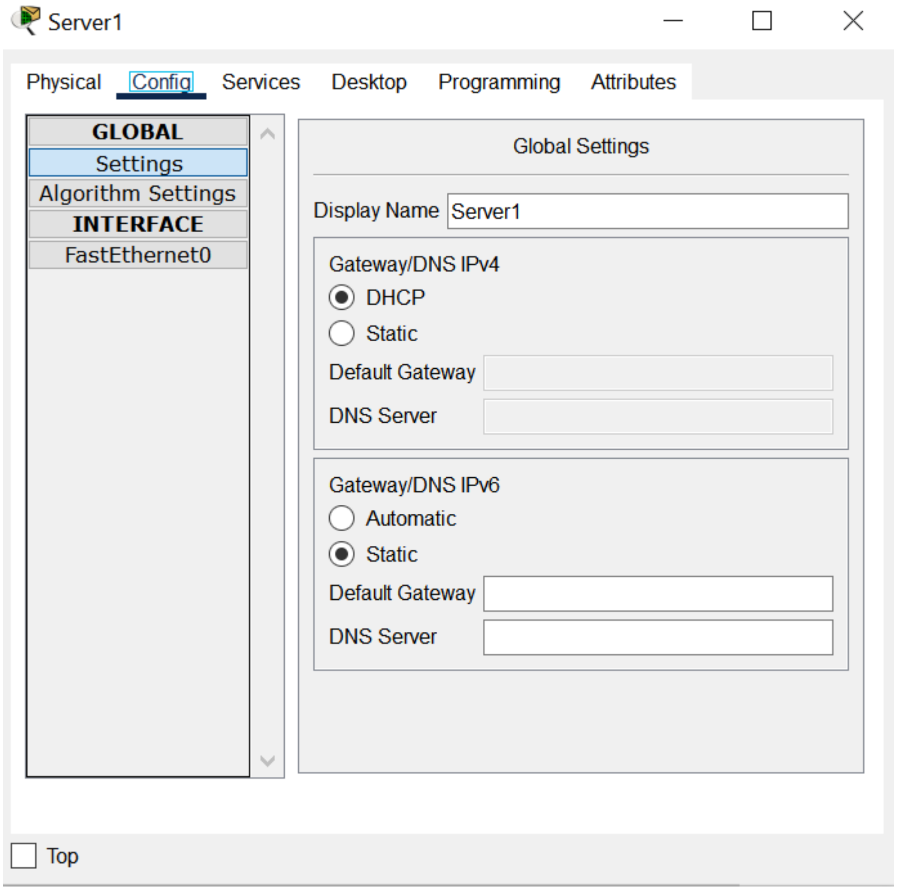
○ Automatic

● Static

IPv6 Address: /

Link Local Address: FE80::2D0:D3FF:FEE3:BB16

□ Top



Server1

Physical | Config | Services | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0

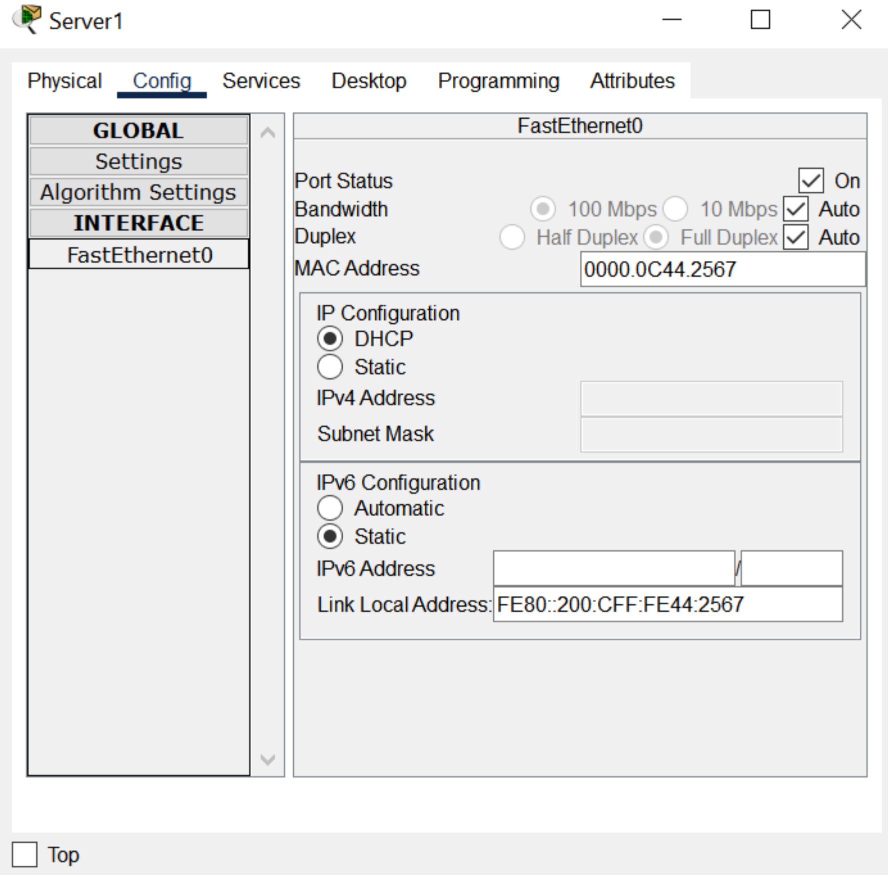
Global Settings

Display Name: Server1

Gateway/DNS IPv4
● DHCP
○ Static
Default Gateway:
DNS Server:

Gateway/DNS IPv6
○ Automatic
● Static
Default Gateway:
DNS Server:

□ Top



Server1

Physical | Config | Services | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0

FastEthernet0

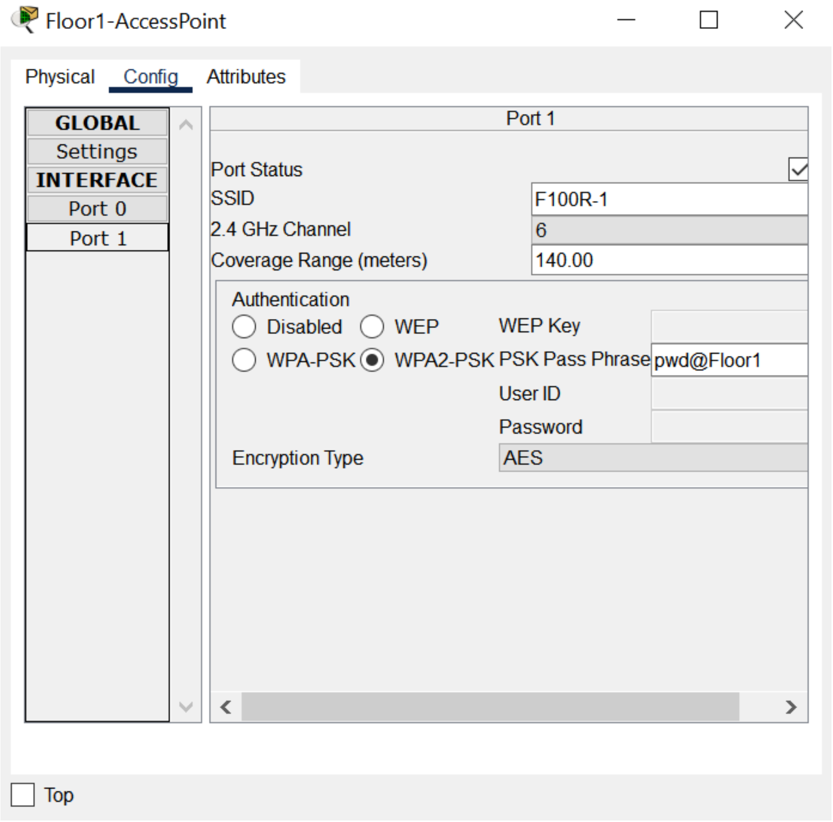
Port Status: ☑ On
Bandwidth: ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex: ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address: 0000.0C44.2567

IP Configuration
● DHCP
○ Static
IPv4 Address:
Subnet Mask:

IPv6 Configuration
○ Automatic
● Static
IPv6 Address: /
Link Local Address: FE80::200:CFF:FE44:2567

□ Top

Access Point


Floor1-AccessPoint

Port 1

Port Status ☑

SSID F100R-1

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP WEP Key

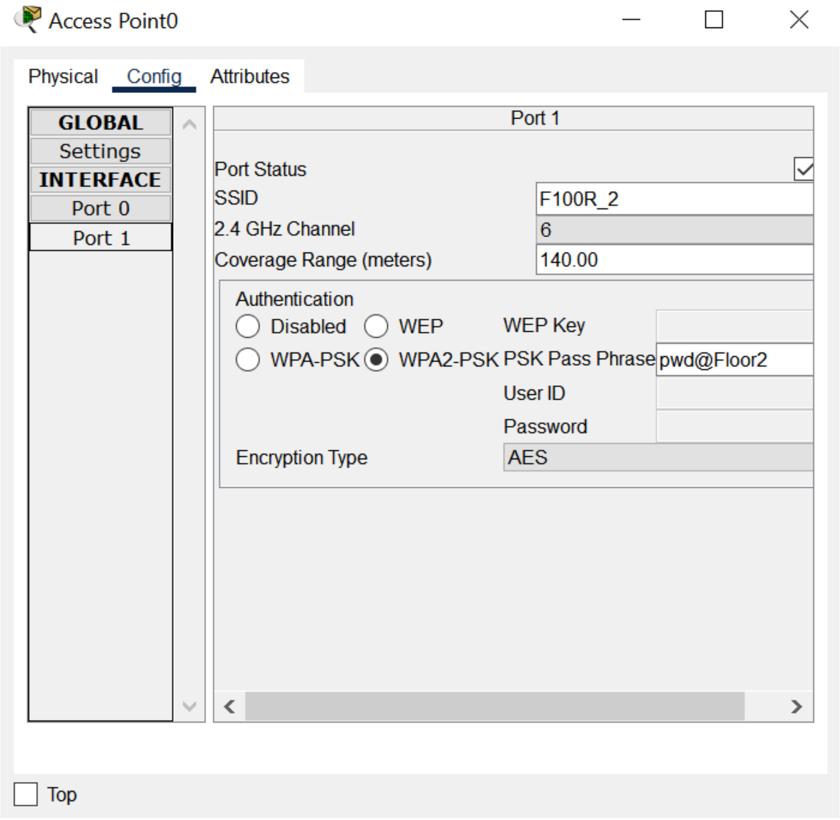
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase pwd@Floor1

User ID

Password

Encryption Type AES

□ Top


Access Point0

Port 1

Port Status ☑

SSID F100R_2

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP WEP Key

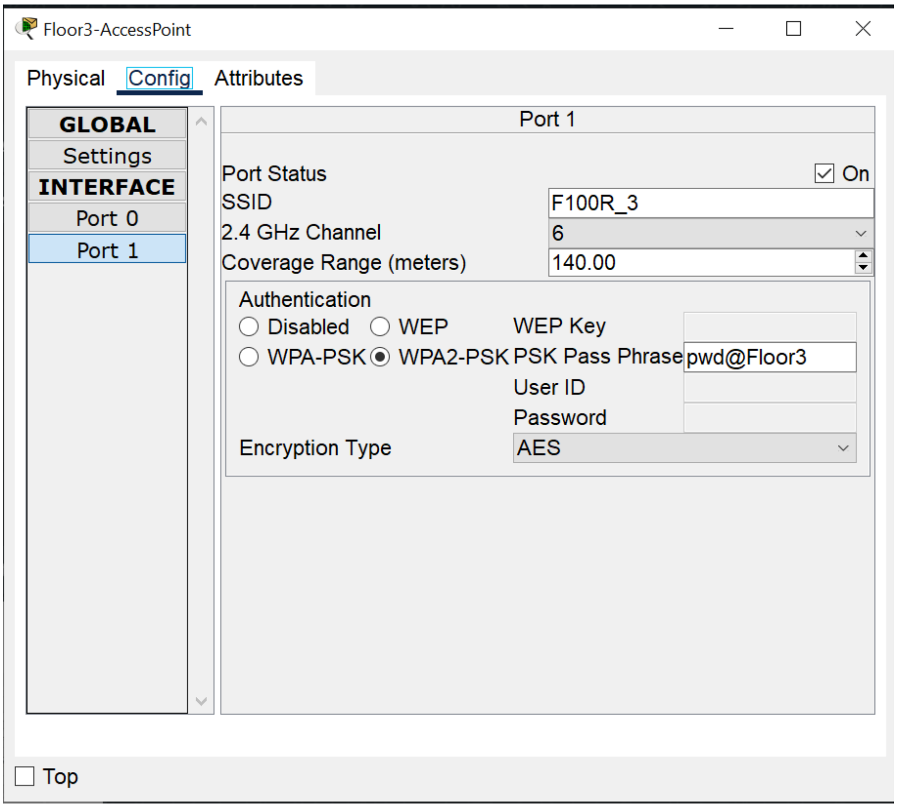
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase pwd@Floor2

User ID

Password

Encryption Type AES

□ Top



Floor3-AccessPoint

Port 1

Port Status ☑ On

SSID F100R_3

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase pwd@Floor3

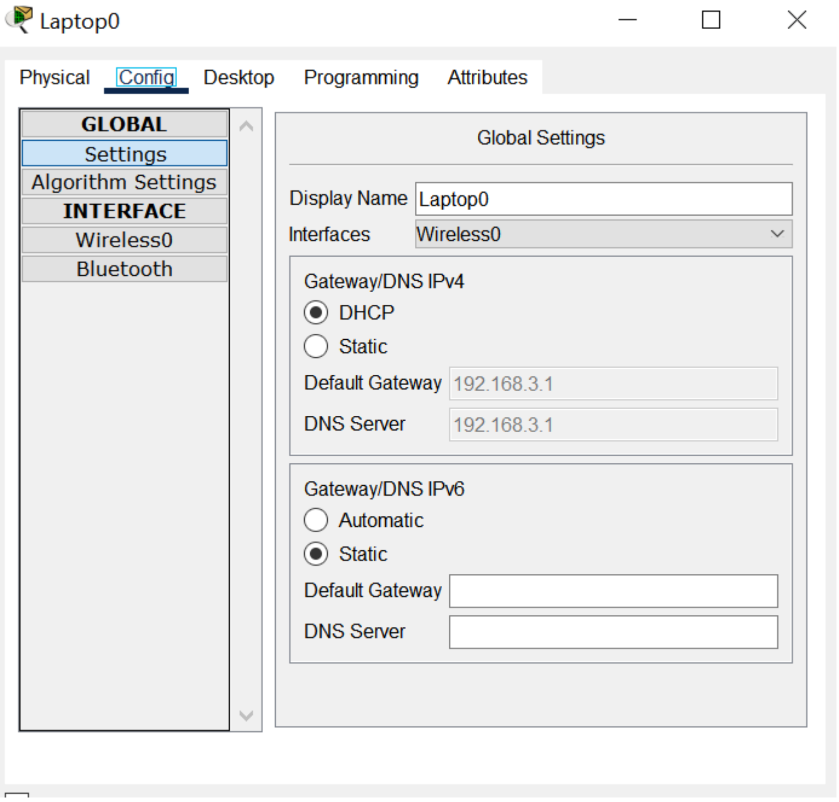
User ID

Password

Encryption Type AES

□ Top

Wireless Devices



Global Settings

Display Name: Laptop0

Interfaces: Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.3.1

DNS Server: 192.168.3.1

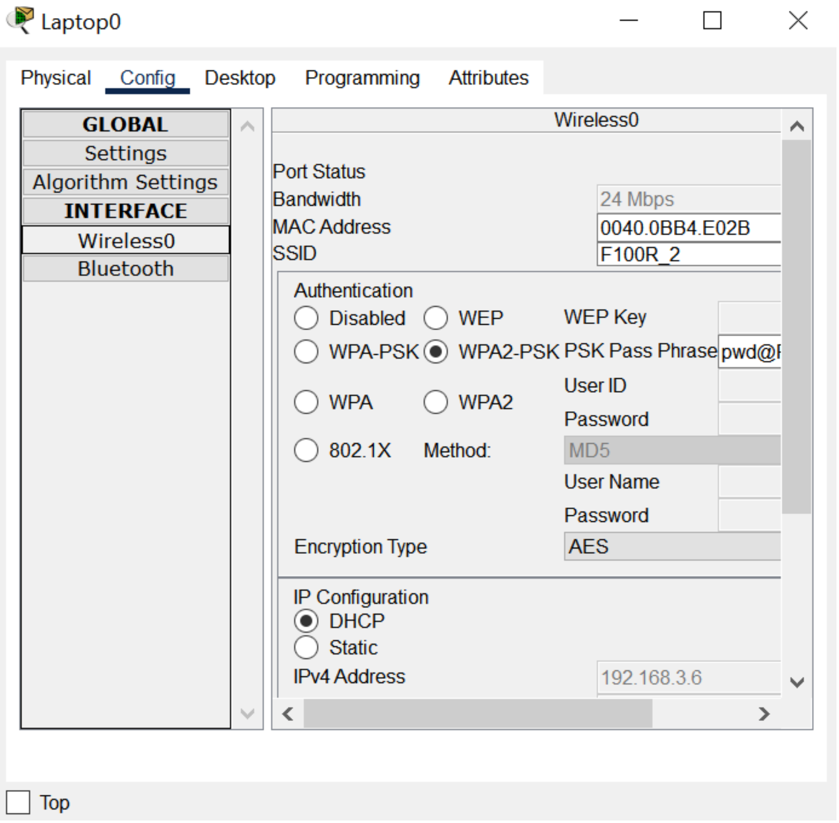
Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway:

DNS Server:



Wireless0

Port Status

Bandwidth: 24 Mbps

MAC Address: 0040.0BB4.E02B

SSID: F100R_2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase: pwd@F

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

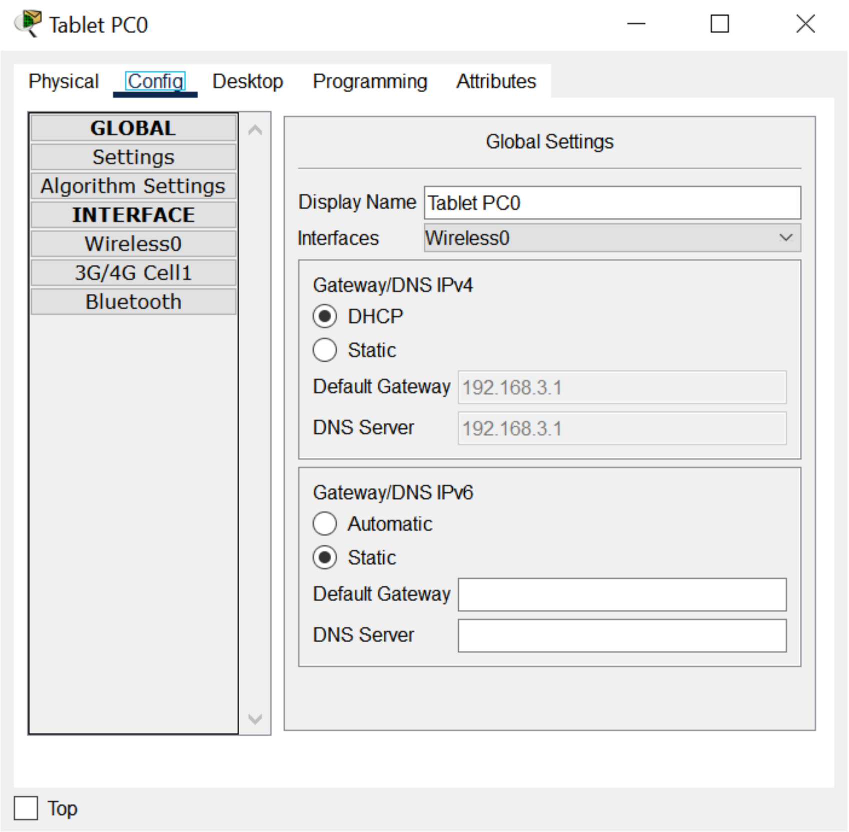
Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.3.6



Global Settings

Display Name: Tablet PC0

Interfaces: Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.3.1

DNS Server: 192.168.3.1

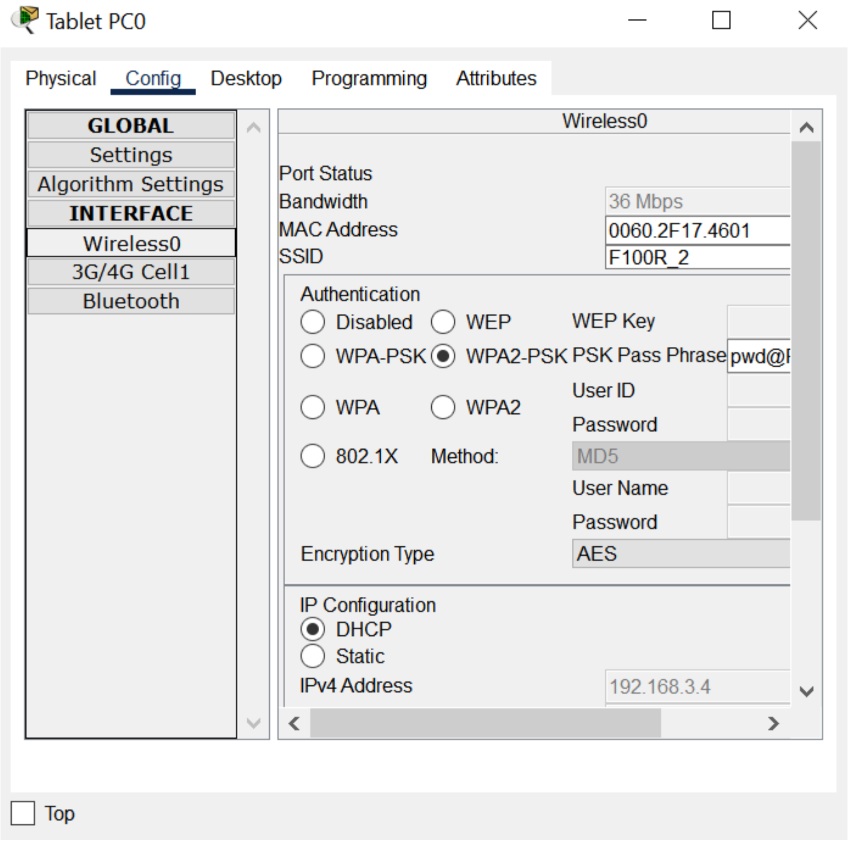
Gateway/DNS IPv6

○ Automatic

● Static

Default Gateway:

DNS Server:



Wireless0

Port Status

Bandwidth: 36 Mbps

MAC Address: 0060.2F17.4601

SSID: F100R_2

Authentication

○ Disabled ○ WEP — WEP Key:

○ WPA-PSK ● WPA2-PSK — PSK Pass Phrase: pwd@F

○ WPA ○ WPA2 — User ID: / Password:

○ 802.1X — Method: MD5 — User Name: / Password:

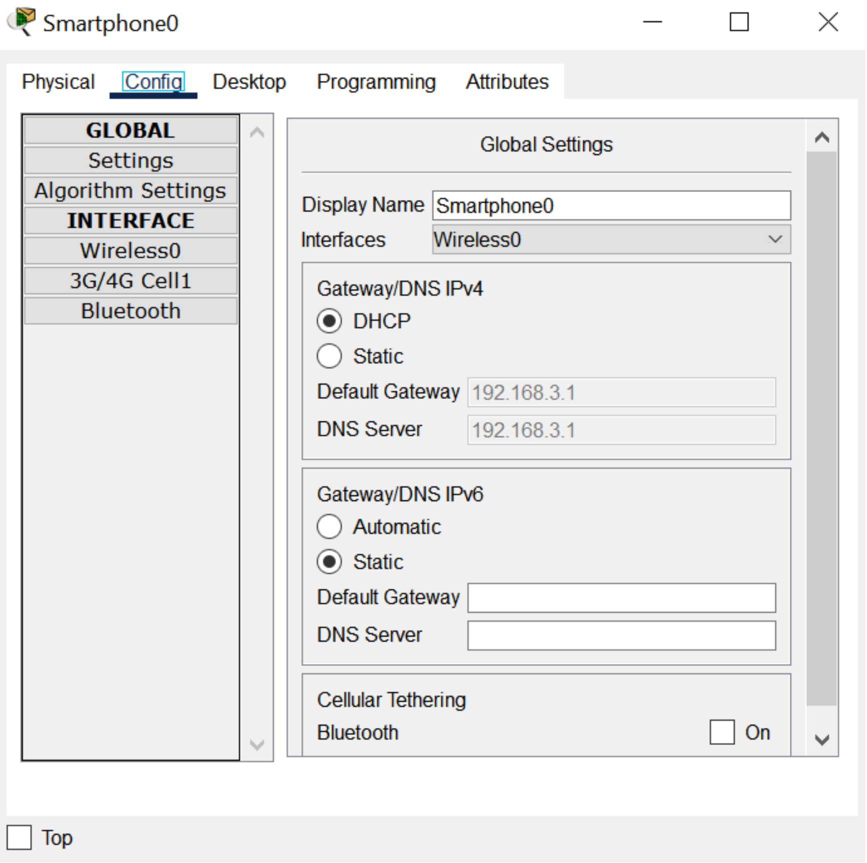
Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.3.4



Global Settings

Display Name: Smartphone0

Interfaces: Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.3.1

DNS Server: 192.168.3.1

Gateway/DNS IPv6

○ Automatic

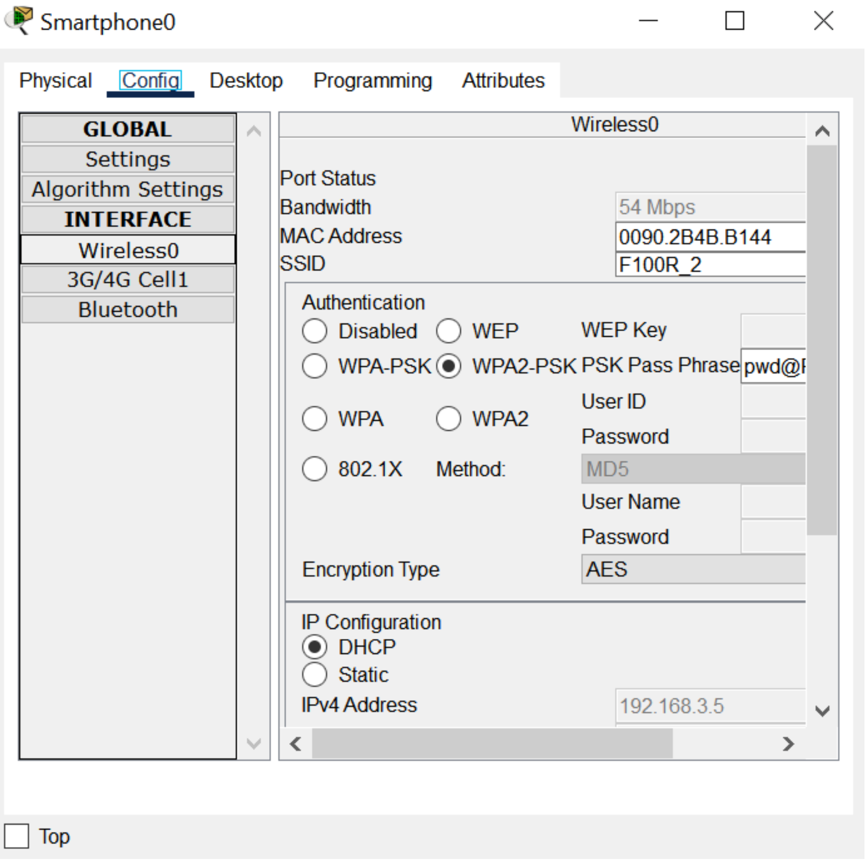
● Static

Default Gateway:

DNS Server:

Cellular Tethering

Bluetooth □ On



Wireless0

Port Status

Bandwidth: 54 Mbps

MAC Address: 0090.2B4B.B144

SSID: F100R_2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase: pwd@I

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

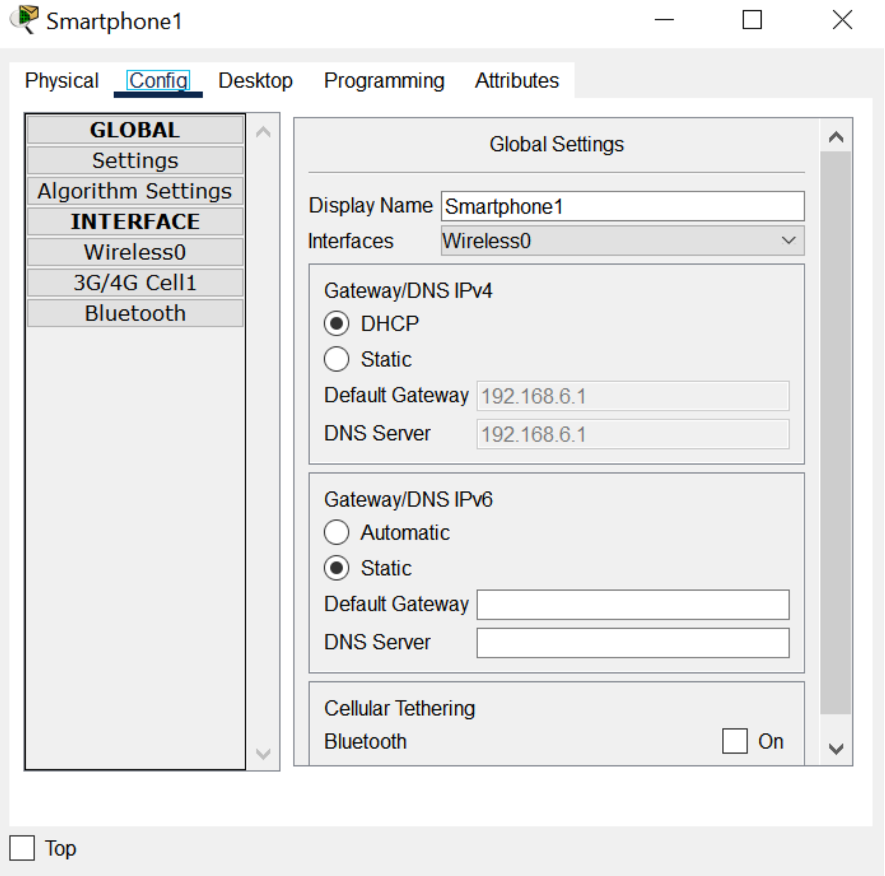
Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.3.5



Smartphone1

Global Settings

Display Name: Smartphone1

Interfaces: Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.6.1

DNS Server: 192.168.6.1

Gateway/DNS IPv6

○ Automatic

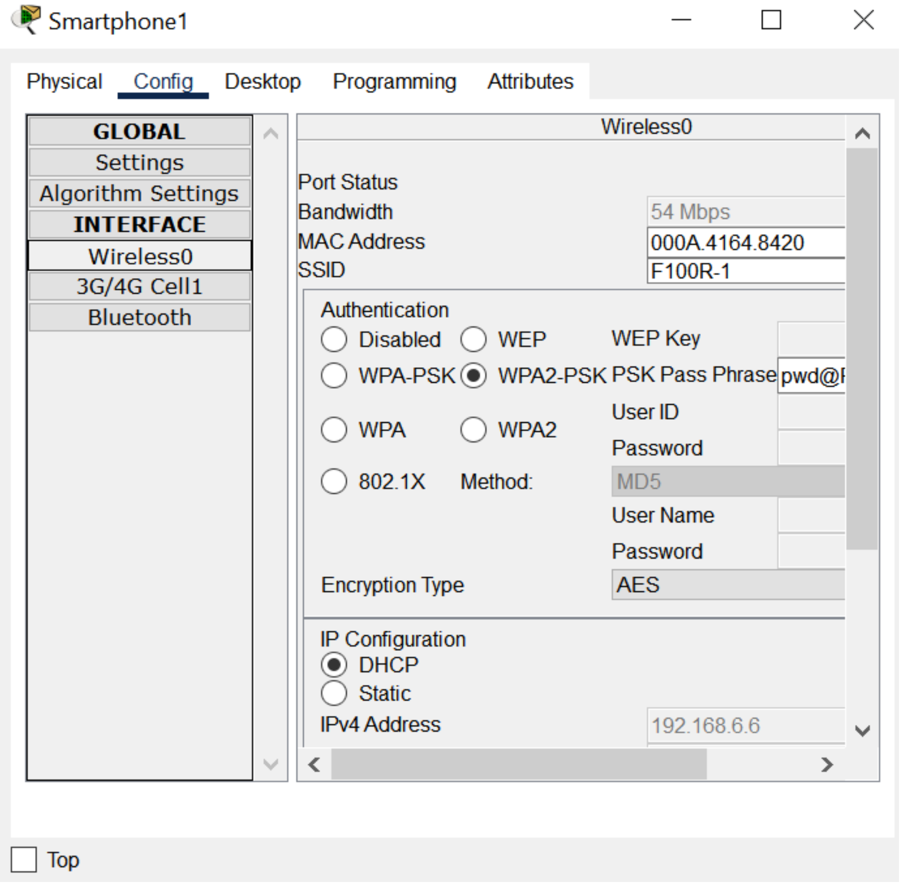
● Static

Default Gateway:

DNS Server:

Cellular Tethering

Bluetooth □ On



Smartphone1

Wireless0

Port Status

Bandwidth: 54 Mbps

MAC Address: 000A.4164.8420

SSID: F100R-1

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase pwd@P

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

User Name

Password

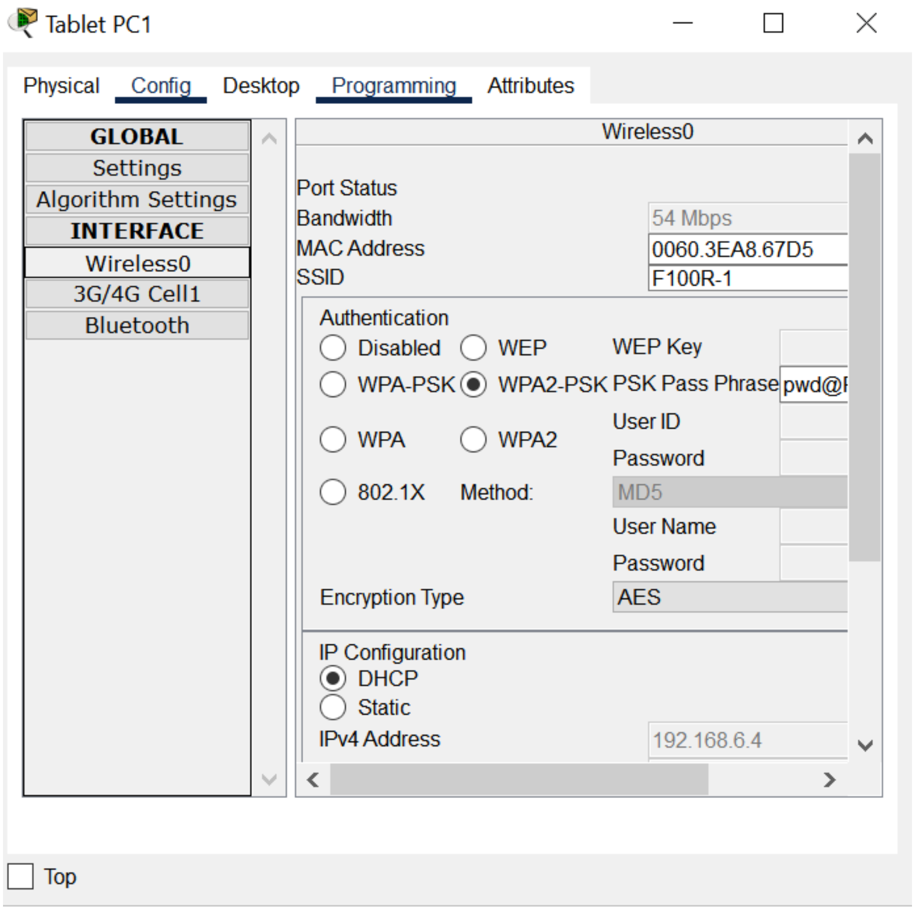
Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.6.6



Wireless0

Port Status

Bandwidth: 54 Mbps

MAC Address: 0060.3EA8.67D5

SSID: F100R-1

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase: pwd@F

User ID

○ WPA ○ WPA2

Password

○ 802.1X Method: MD5

User Name

Password

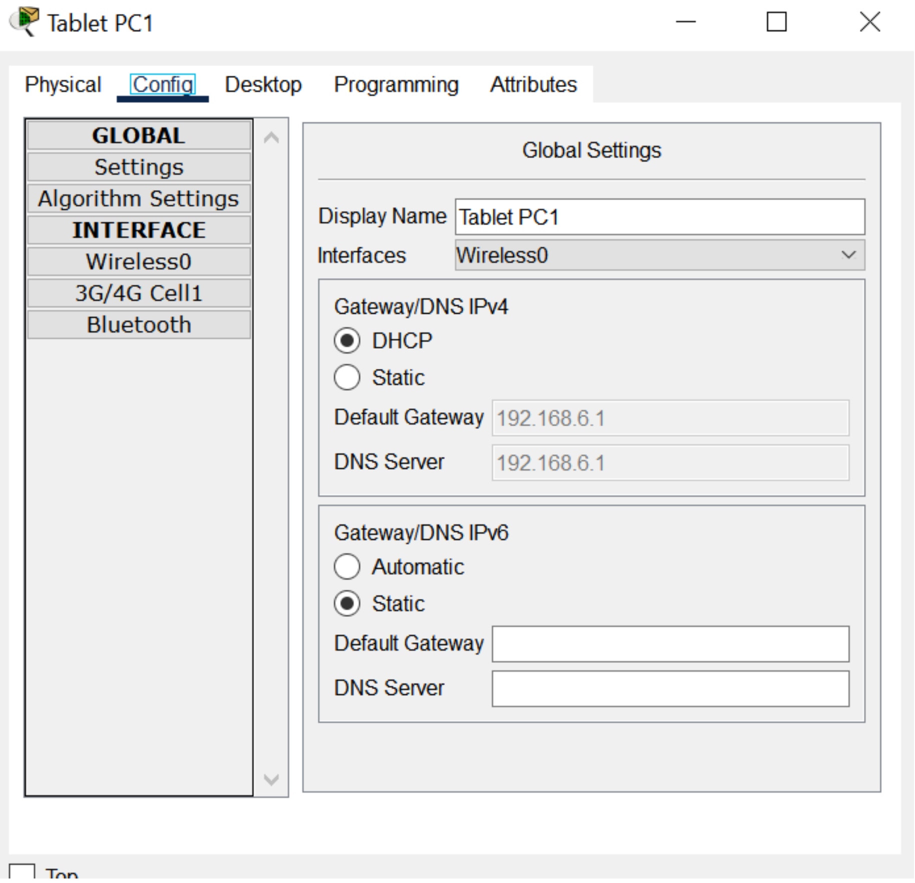
Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.6.4



Global Settings

Display Name: Tablet PC1

Interfaces: Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 192.168.6.1

DNS Server: 192.168.6.1

Gateway/DNS IPv6

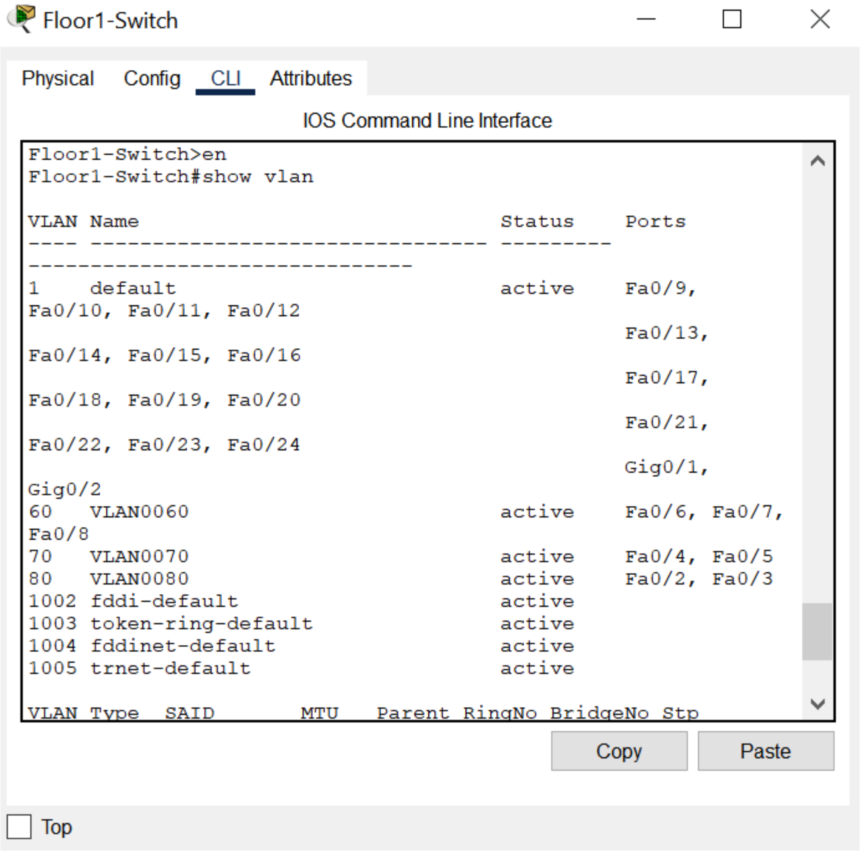
○ Automatic

● Static

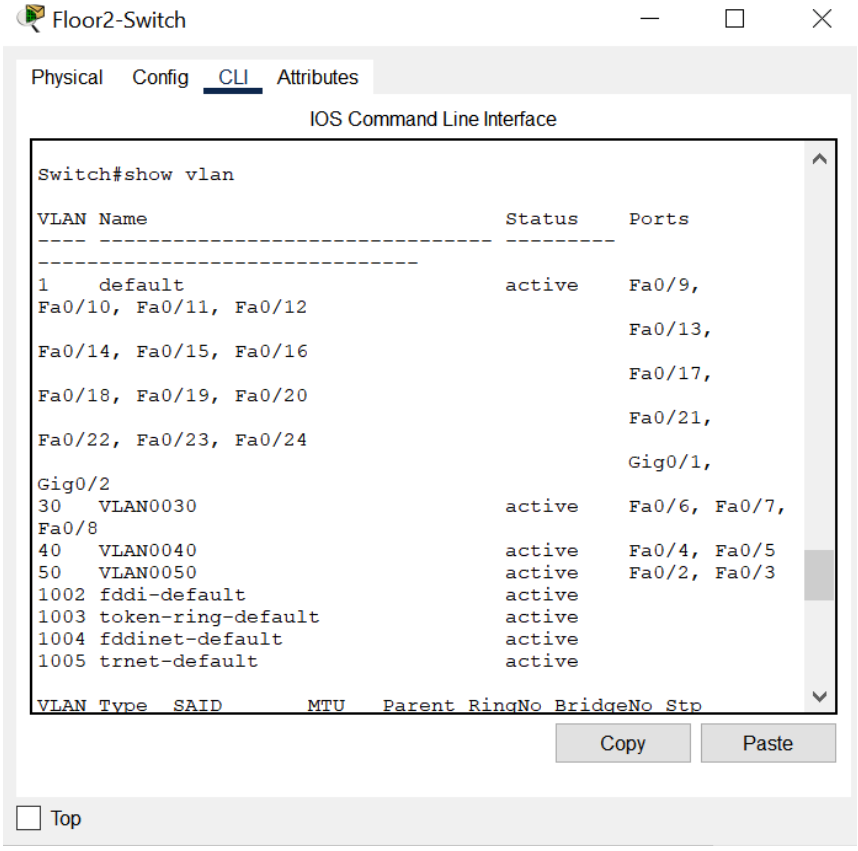
Default Gateway

DNS Server

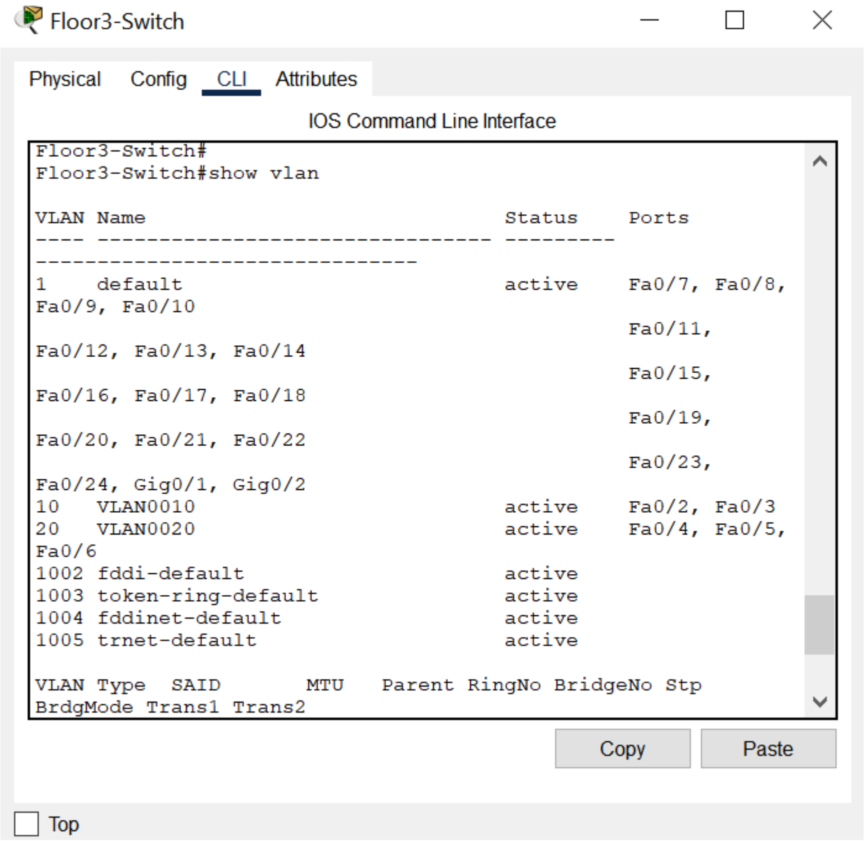
Switches



```
Floor1-Switch>en
Floor1-Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/9,
Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13,
Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17,
Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21,
Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1,
Gig0/2
60   VLAN0060                         active    Fa0/6, Fa0/7,
Fa0/8
70   VLAN0070                         active    Fa0/4, Fa0/5
80   VLAN0080                         active    Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp
```

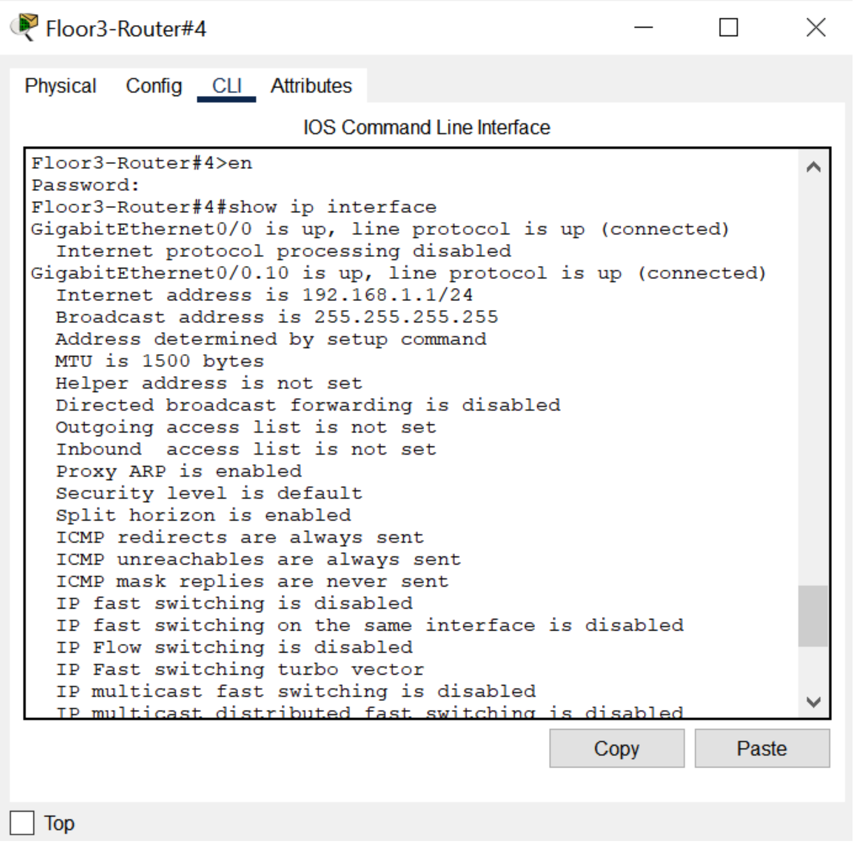


```

Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/9,
Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13,
Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17,
Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21,
Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1,
Gig0/2
30   VLAN0030                         active    Fa0/6, Fa0/7,
Fa0/8
40   VLAN0040                         active    Fa0/4, Fa0/5
50   VLAN0050                         active    Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp
```

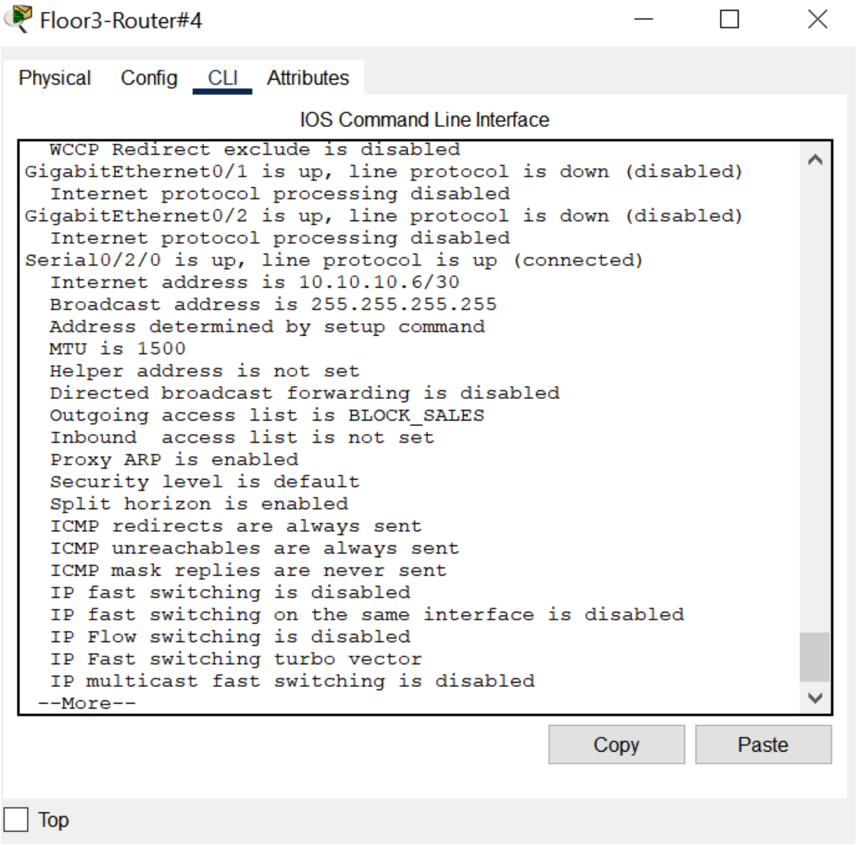


```
Floor3-Switch#
Floor3-Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/7, Fa0/8,
Fa0/9, Fa0/10
                                                Fa0/11,
Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15,
Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19,
Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23,
Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                         active    Fa0/2, Fa0/3
20   VLAN0020                         active    Fa0/4, Fa0/5,
Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp
BrdgMode Trans1 Trans2
```

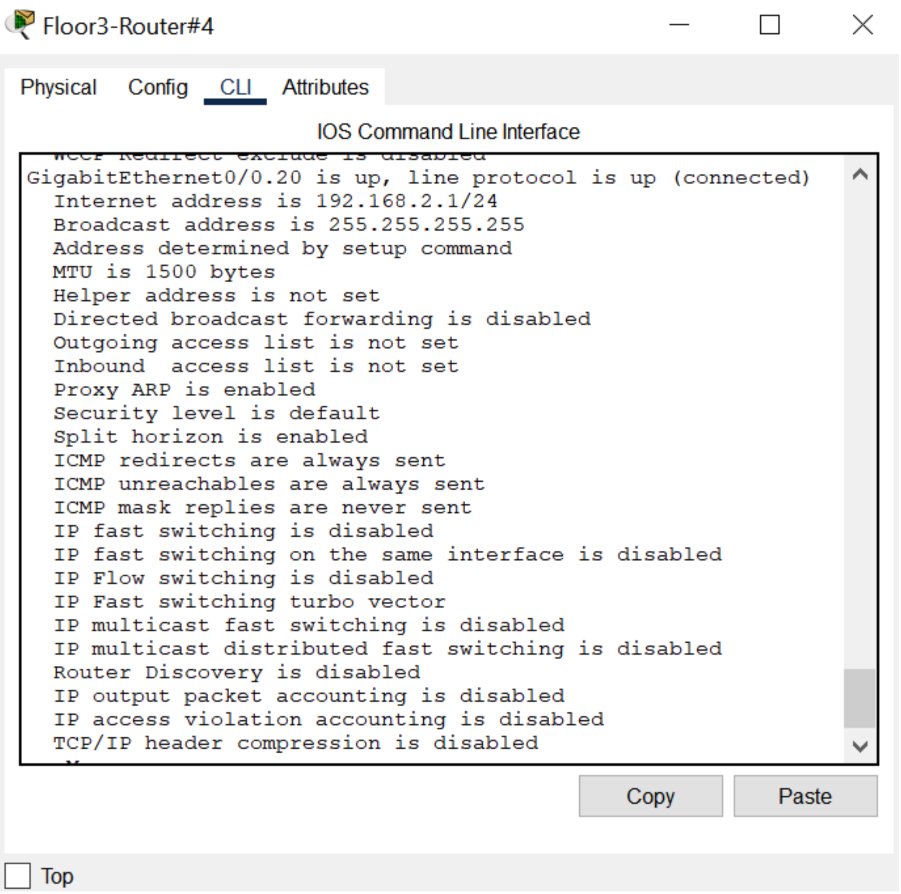
Router



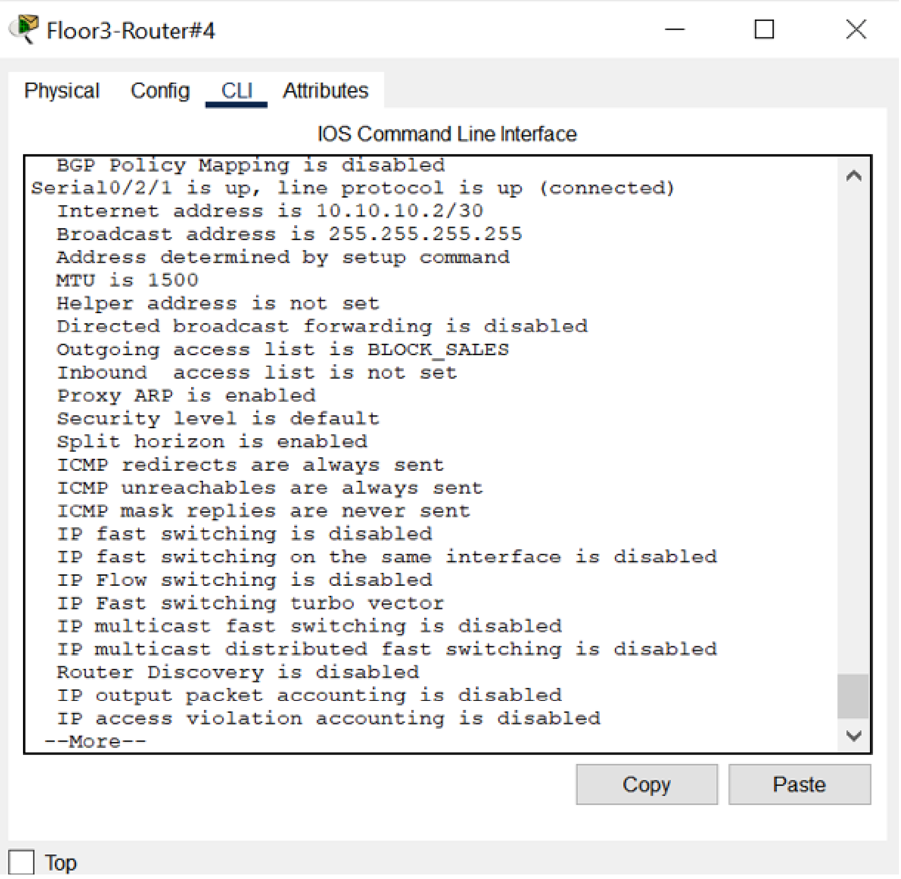
```
Floor3-Router#4>en
Password:
Floor3-Router#4#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet protocol processing disabled
GigabitEthernet0/0.10 is up, line protocol is up (connected)
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
```



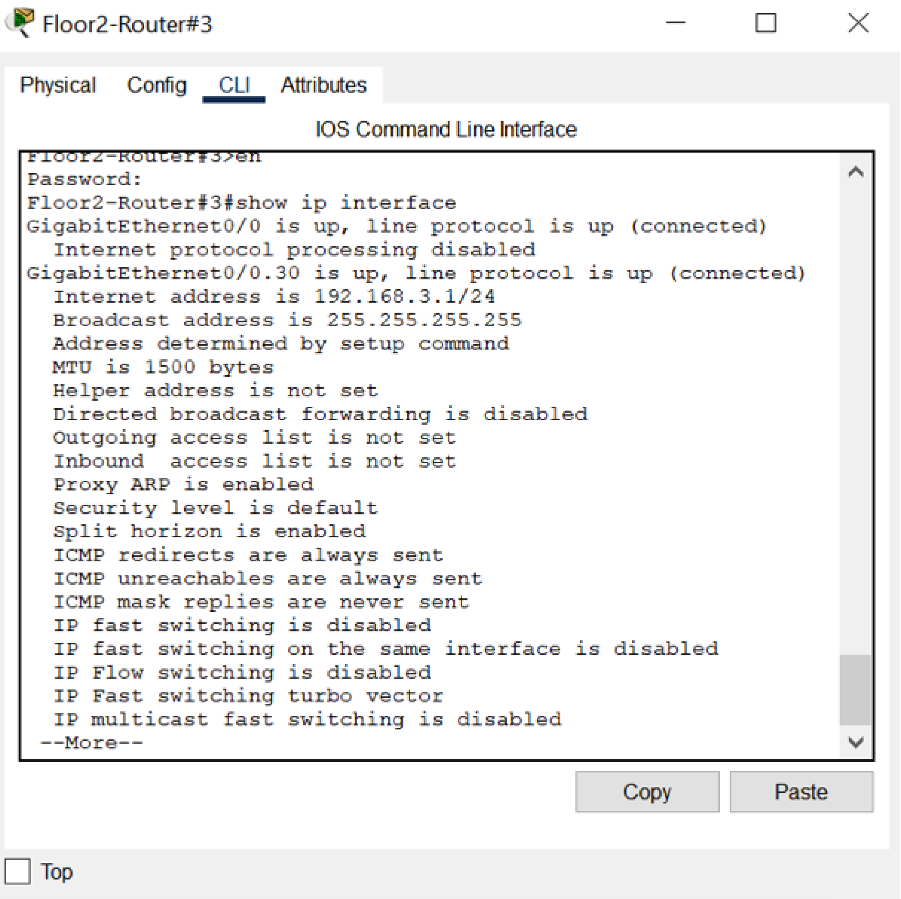
```
  WCCP Redirect exclude is disabled
GigabitEthernet0/1 is up, line protocol is down (disabled)
  Internet protocol processing disabled
GigabitEthernet0/2 is up, line protocol is down (disabled)
  Internet protocol processing disabled
Serial0/2/0 is up, line protocol is up (connected)
  Internet address is 10.10.10.6/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is BLOCK_SALES
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
 --More--
```



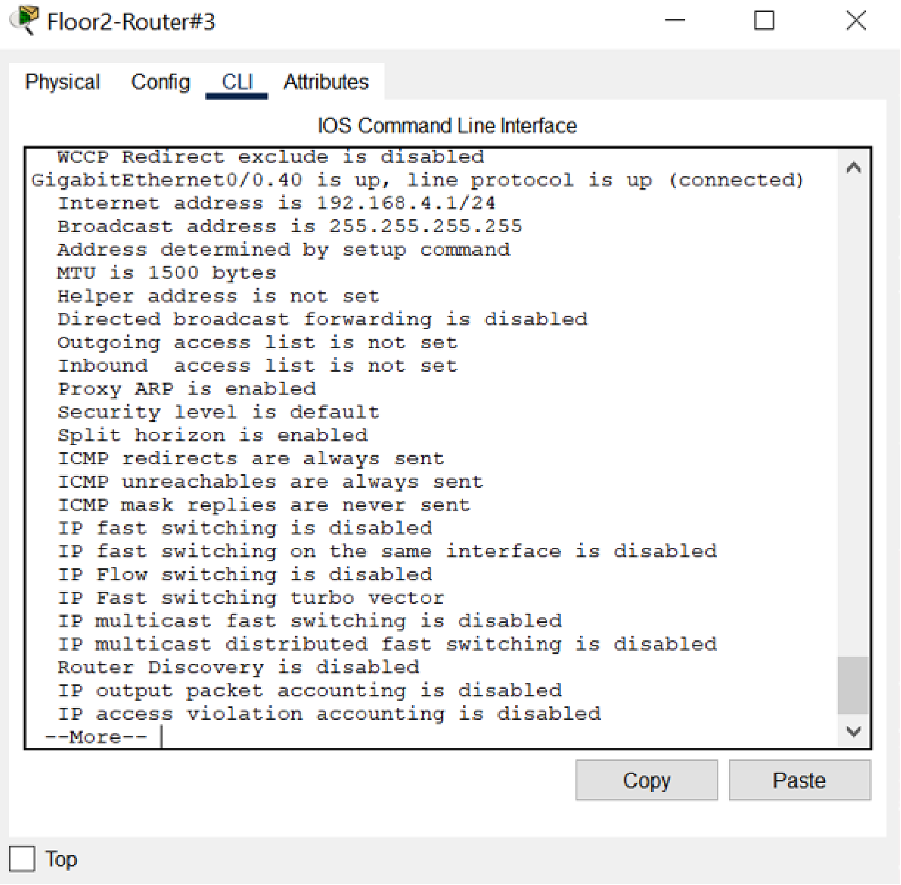
```
  WCCP Redirect exclude is disabled
GigabitEthernet0/0.20 is up, line protocol is up (connected)
  Internet address is 192.168.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
```



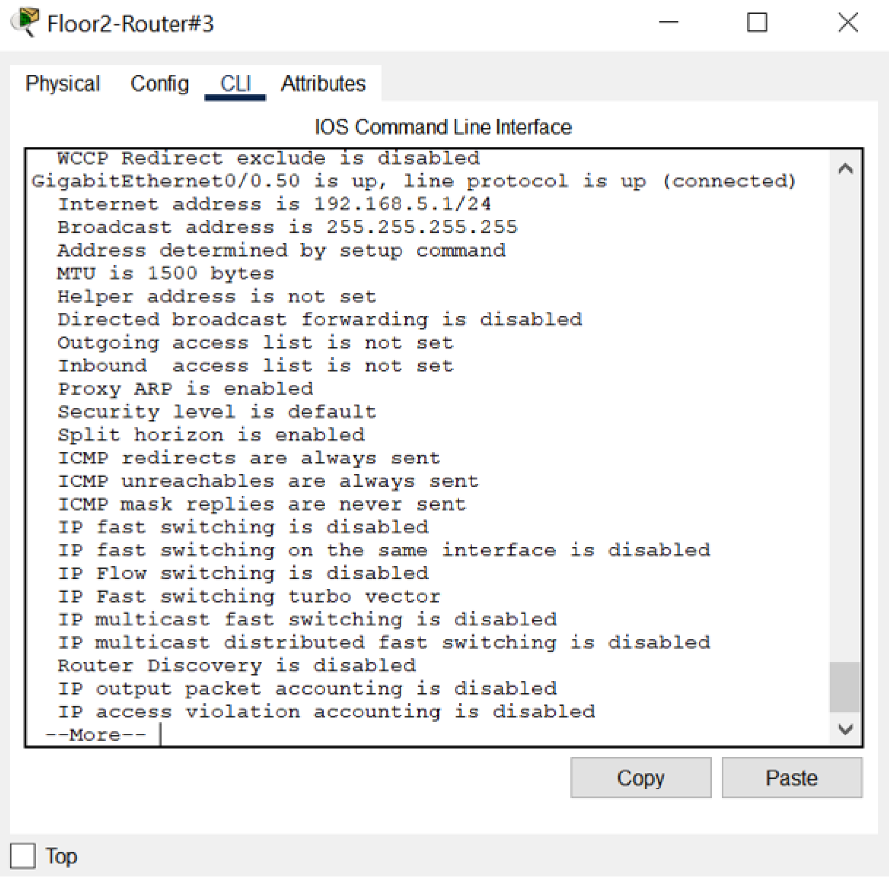
```
  BGP Policy Mapping is disabled
Serial0/2/1 is up, line protocol is up (connected)
  Internet address is 10.10.10.2/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is BLOCK_SALES
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 --More--
```



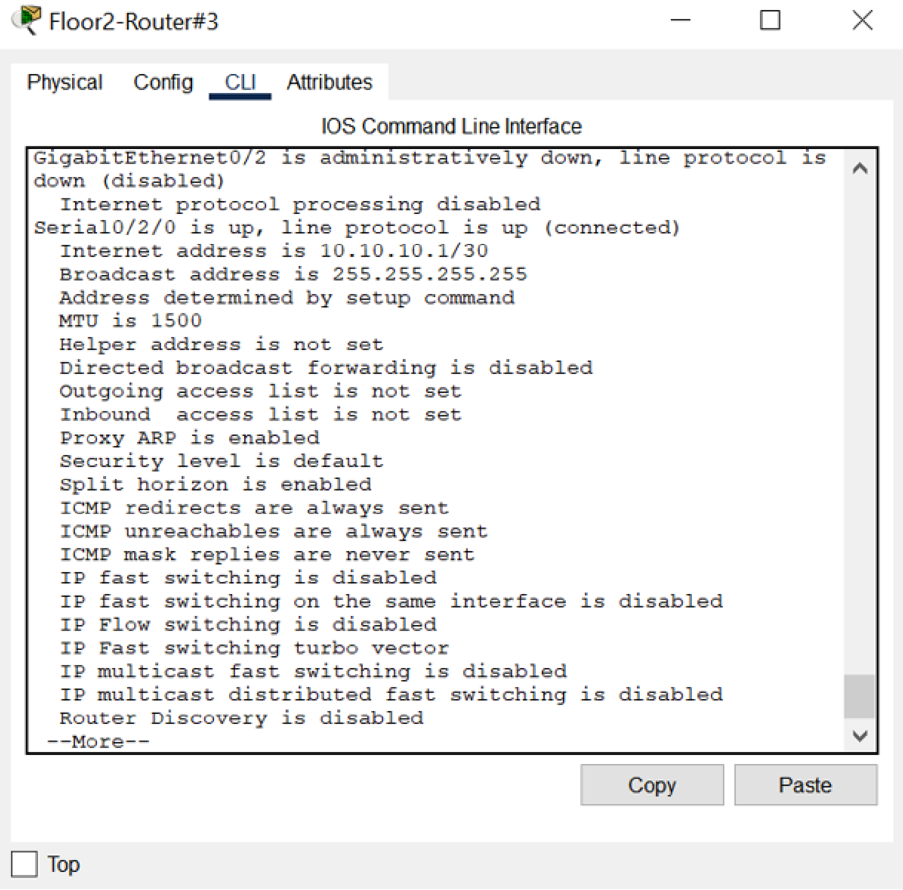
```
Floor2-Router#3>en
Password:
Floor2-Router#3#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet protocol processing disabled
GigabitEthernet0/0.30 is up, line protocol is up (connected)
  Internet address is 192.168.3.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
 --More--
```



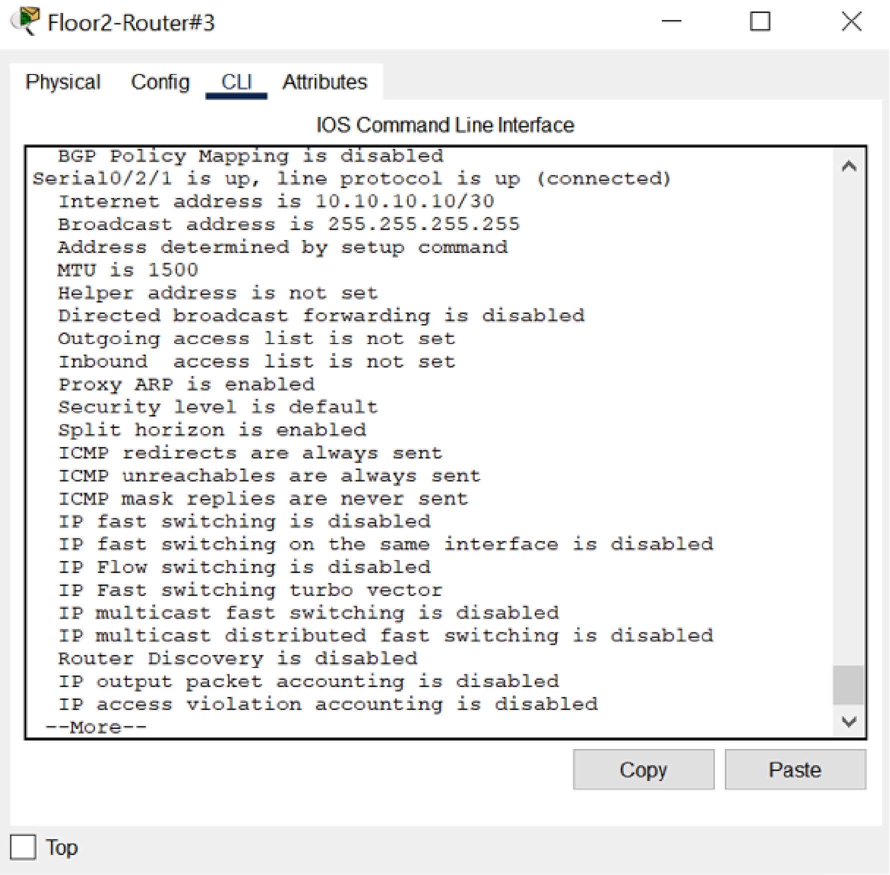
```
  WCCP Redirect exclude is disabled
GigabitEthernet0/0.40 is up, line protocol is up (connected)
  Internet address is 192.168.4.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 --More--
```



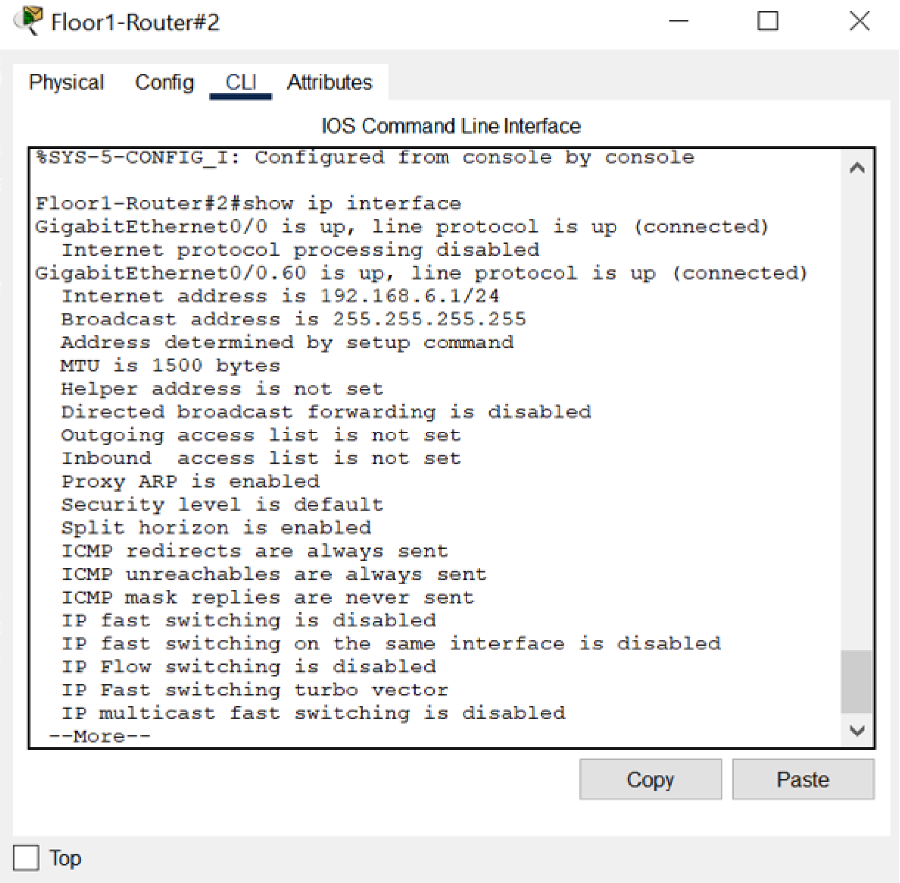
```
  WCCP Redirect exclude is disabled
GigabitEthernet0/0.50 is up, line protocol is up (connected)
  Internet address is 192.168.5.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 --More--
```



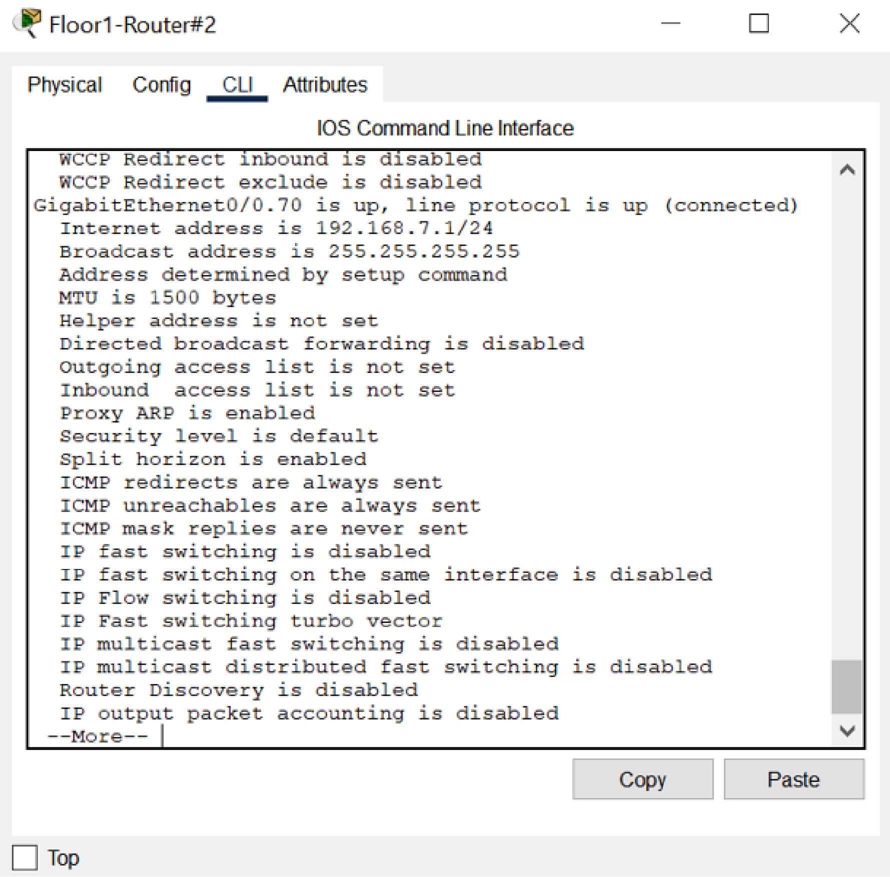
```
GigabitEthernet0/2 is administratively down, line protocol is
down (disabled)
  Internet protocol processing disabled
Serial0/2/0 is up, line protocol is up (connected)
  Internet address is 10.10.10.1/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
 --More--
```



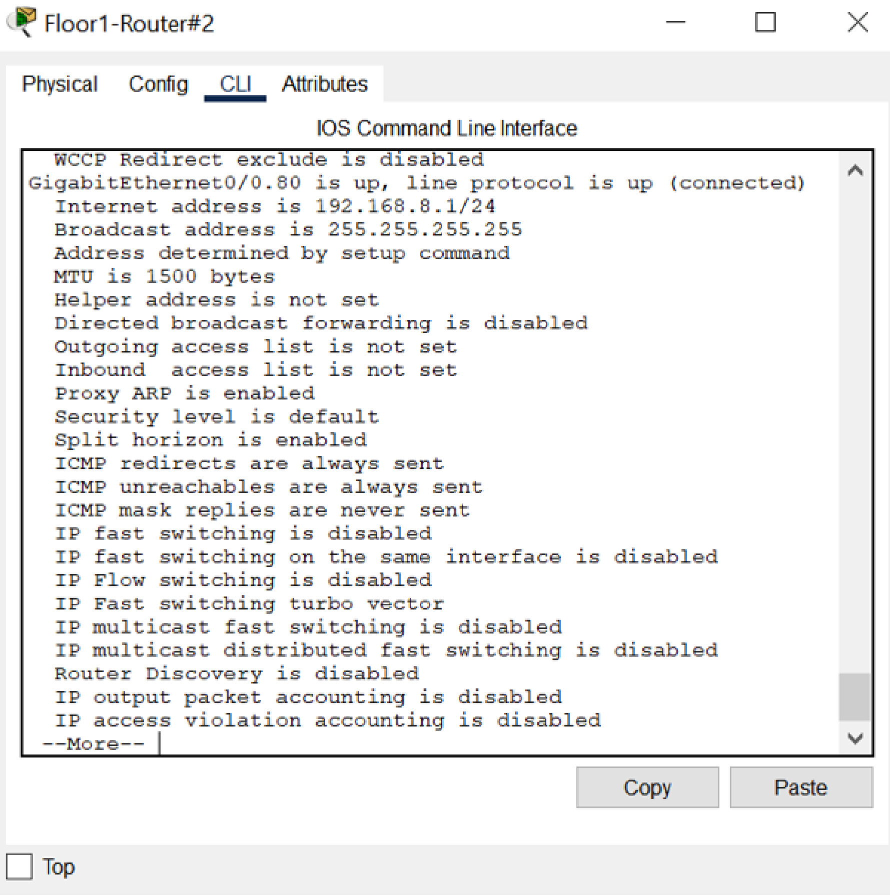
```
  BGP Policy Mapping is disabled
Serial0/2/1 is up, line protocol is up (connected)
  Internet address is 10.10.10.10/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 --More--
```



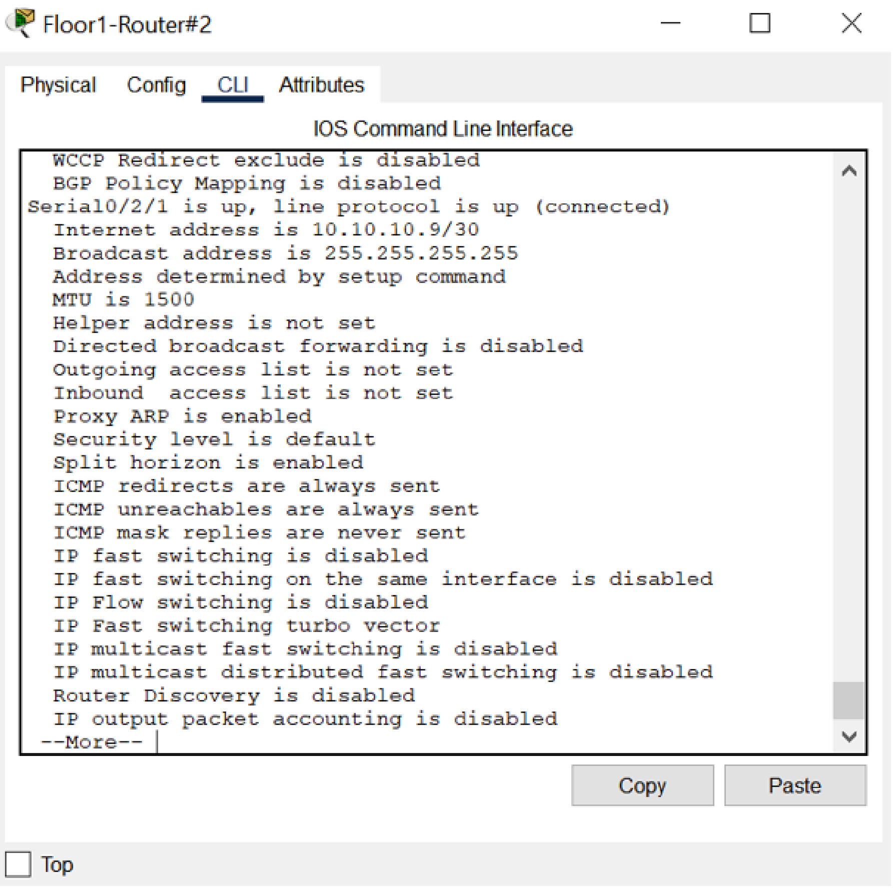
```
%SYS-5-CONFIG_I: Configured from console by console

Floor1-Router#2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet protocol processing disabled
GigabitEthernet0/0.60 is up, line protocol is up (connected)
  Internet address is 192.168.6.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
 --More--
```



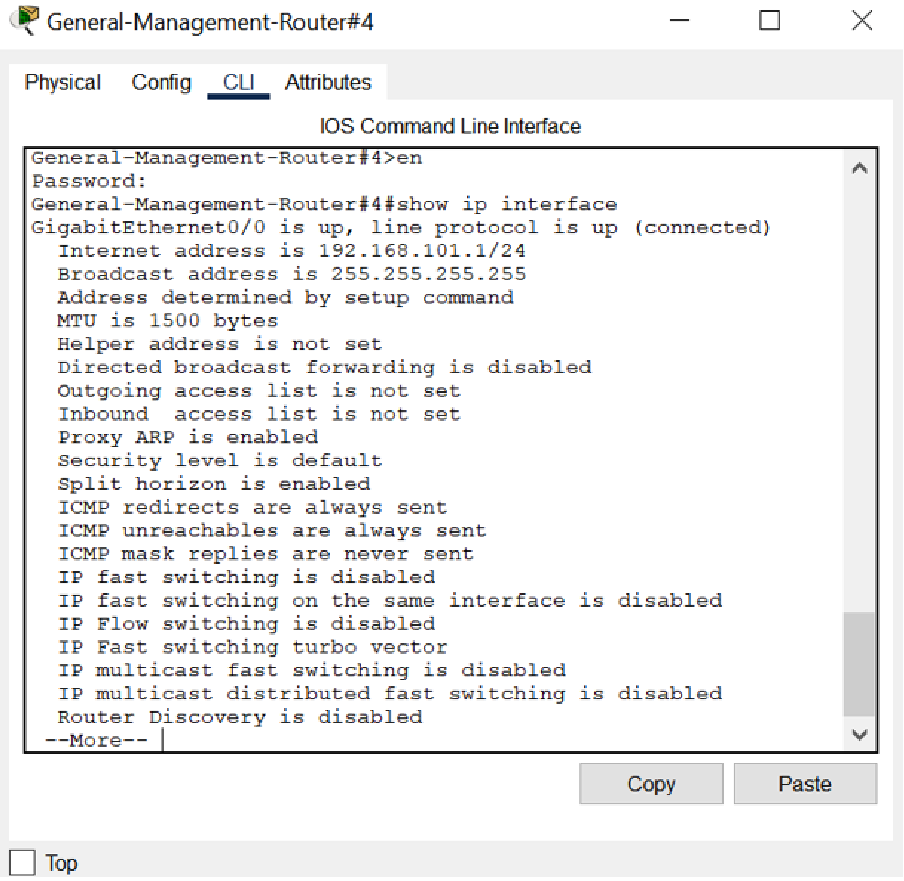
```
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
GigabitEthernet0/0.70 is up, line protocol is up (connected)
  Internet address is 192.168.7.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
 --More--
```



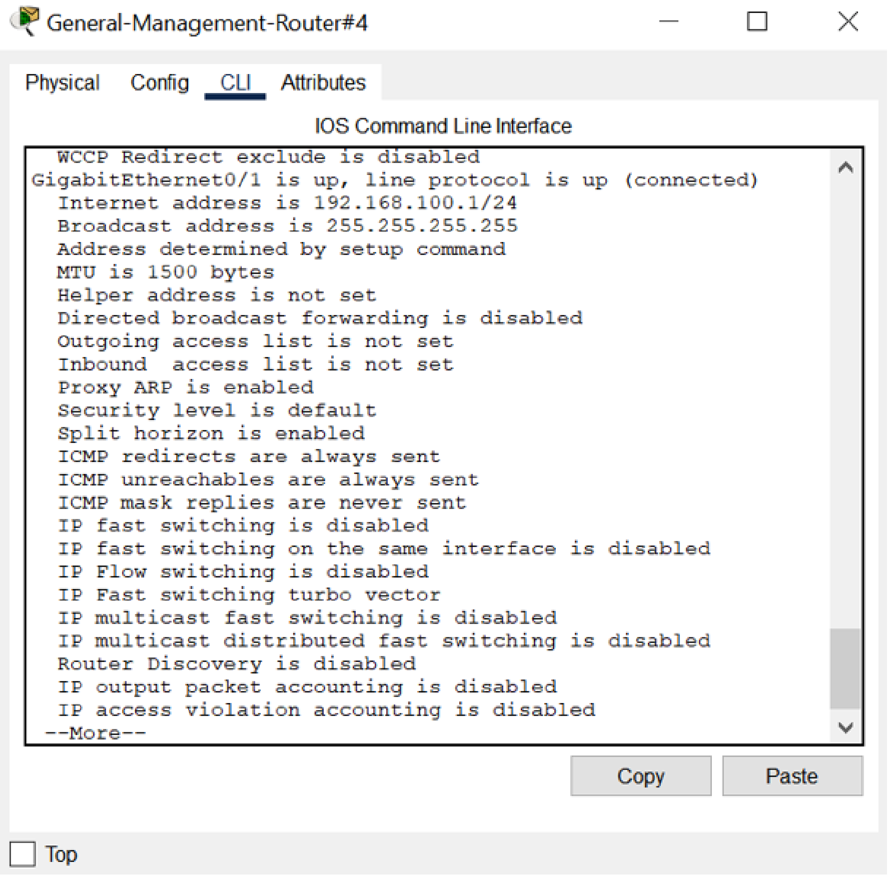
```
  WCCP Redirect exclude is disabled
GigabitEthernet0/0.80 is up, line protocol is up (connected)
  Internet address is 192.168.8.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 --More--
```



```
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
Serial0/2/1 is up, line protocol is up (connected)
  Internet address is 10.10.10.9/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
 --More--
```



```
General-Management-Router#4>en
Password:
General-Management-Router#4#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.101.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
 --More--
```



```
  WCCP Redirect exclude is disabled
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.100.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 --More--
```

References

- Ramaswamy Chandramouli (2022) (U.S. Department of Commerce, Washington, D.C.) ,Guide to a Secure Enterprise Network Landscape, Change Notice 11/17/22: November 17, 2032. https://csrc.nist.gov/publications/detail/sp/800-215/final

- *What is an Intrusion Prevention System?* (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

- GeeksforGeeks. (2021, August 31). *Intrusion Prevention System IPS*. https://www.geeksforgeeks.org/intrusion-prevention-system-ips/

- *Configuring Port Security*. (2015, March 21). Cisco. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/sec_port.html

- Taylor, C. (2022, January 13). *Layer 2 Network*. CyberHoot. https://cyberhoot.com/cybrary/layer-2-network/

- Cisco Packet Tracer Labs. (2016, December 30). *CCNA Security Lab 5.4.1.2: Configure IOS Intrusion Prevention System (IPS) Using CLI* [Video]. YouTube. https://www.youtube.com/watch?v=KBELcaBveNI

- A. (2023, February 2). *General Layer 3 Security Considerations - Routing and Switching*. Cisco Certified Expert. https://www.ccexpert.us/routing-switching-2/general-layer-3-security-considerations.html

- GeeksforGeeks. (2021b, October 28). *Computer Network AAA Authentication Authorization and Accounting*. https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/