

NETWORK SECURITY 1 PROJECT

PROJECT

NAME: Ikem Mercy Ogechi

STUDENT ID: 8859960

COURSE CODE: INFO8491-23W

PROFESSOR NAME: Dr. Zara Hamid

DUE DATE: 16th April,2023.

Contents

SITE A	2
DESCRIPTION:	2
REQUIREMENTS:.....	2
DESIGN	2
IP ADDRESS ASSIGNMENT:.....	2
SCREENSHOT	3
SITE B	14
DESCRIPTION:	14
REQUIREMENTS:.....	14
DESIGN	14
SCREENSHOT	16
SITE C	23
DESCRIPTION:	23
REQUIREMENTS:.....	23
DESIGN	23
SCREENSHOT	24

NETWORK SECURITY 1 PROJECT

SITE A

DESCRIPTION:

Site A goal is to design and deploy a trustworthy network for a company using three layer 2 switches and two routers. The network requires a web server with a customized homepage, secure authentication, and EIGRP without auto-summary for routing updates between the access router and the edge router. For remote SSH connection to the access router and the edge router, a TACACS server is what I will use based on what I have been taught in this course.

REQUIREMENTS:

- A network design that is both secure and efficient
- Web server with personalized home page
- Secure authentication and encryption must be used for routing updates between the access router and edge router.
- EIGRP without auto summary
- Remote SSH login to access and edge routers must use TACACS server authentication.
- Three layer 2 switches connected to each other without causing network loops.
- A single IP address with a /28 CIDR will be used for the entire network.
- My subnet **10.150.136.0/28**
- The IP address between edge access and access router will be 10.150.136.48/28.

DESIGN

- **I will use 2 PT servers, 3-2960 layer 2 switches, 1- cisco 2911 Router, 1 Router PT router for this site.**
- I will use EIGRP for routing between the access router and edge router. Loopback addresses will be used for EIGRP updates.
- I will configure Vlan 1
- TACACS server will also be configured on this network to handle remote SSH login authentication for the access router and the edge router.
- I will configure a custom home page for my web server, I will activate the DNS service.
- STP will be configured on all switches to prevent network loops. SW2 will be configured as the root bridge, SW1 will have a root port on the interface connecting to SW2, and SW3 will have a root port on the interface connecting to SW1. All interfaces will be designated ports.
- I will connect the edge router in SITE A to SITE b using daisy chain manner which will also be connected to SITE C.

IP ADDRESS ASSIGNMENT:

- SW1: 10.150.136.2/28
- SW2: 10.150.136.3/28
- SW3: 10.150.136.4/28
- **Access Router:**

NETWORK SECURITY 1 PROJECT

- LAN: 10.150.136.1/28
- WAN: 10.150.136.49/28
- **Edge Router:**
- LAN: 10.150.136.50/28
- WAN: 10.150.136.160/28
- Tacacs server: 10.150.136.5/28
- Web server: 10.150.136.6/28

SCREENSHOT

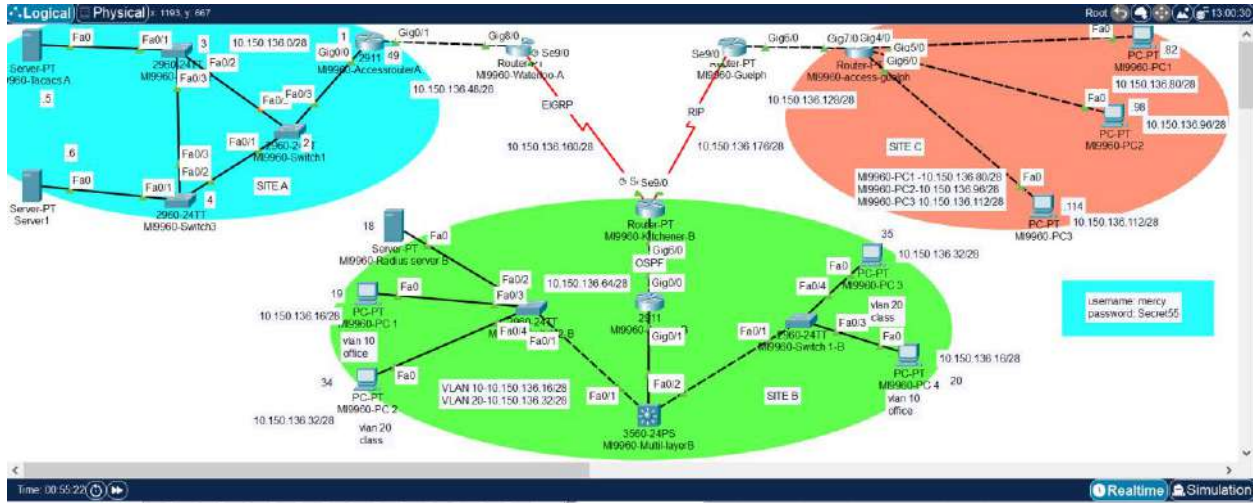


fig1 showing my topology showing different sites.

NETWORK SECURITY 1 PROJECT

The screenshot shows a network switch configuration window titled "MI9960-Switch3". The "CLI" tab is active, displaying the "IOS Command Line Interface". The command "sh spanning-tree" has been executed, showing the following output:

```
MI9960-Switch3>en
MI9960-Switch3#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0030.F28C.0543
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0030.F28C.0543
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/3	Desg	FWD	19	128.3	P2p

The output also shows the "Aging Time" as 20. The network diagram in the background shows a switch connected to three PCs (MI9960-PC1, MI9960-PC2, MI9960-PC3) and a server (MI9960-PC4) via a "vlan 20 class" and "Fa0" interface. The switch is labeled "MI9960-Switch3" and the server is labeled "MI9960-PC4".

Fig 2 showing that this is the root bridge, designated ports, and ports costs on switch 3. The ports cost 19.

NETWORK SECURITY 1 PROJECT

The screenshot displays the CLI of a switch (MI9960-Switch1) with the 'CLI' tab selected. The command 'sh spanning-tree' has been executed, showing the spanning tree configuration for VLAN0001. The output indicates that the spanning tree is enabled with the IEEE protocol. The root bridge is identified as 0030.F28C.0543 on port 1 (FastEthernet0/1). The bridge ID is 0060.70BA.326A. The output also shows the status of three interfaces: Fa0/1 (Root FWD), Fa0/3 (Desg FWD), and Fa0/2 (Altn BLK). The cost for all three interfaces is 19. The network diagram on the right shows a switch connected to three PCs (MI9960-PC1, MI9960-PC2, MI9960-PC3) and a PC-PT (MI9960-PC 4) in a green cloud labeled 'vlan 10 office'. The switch is also connected to a PC-PT (MI9960-PC 3) in a green cloud labeled 'vlan 20 class'. The switch is connected to a PC-PT (MI9960-PC 3) in a green cloud labeled 'vlan 20 class'. The switch is connected to a PC-PT (MI9960-PC 4) in a green cloud labeled 'vlan 10 office'.

```
MI9960-Switch1>en
MI9960-Switch1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0030.F28C.0543
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay
15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0060.70BA.326A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay
15 sec
             Aging Time  20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Root FWD 19        128.1   P2p
Fa0/3              Desg FWD 19        128.3   P2p
Fa0/2              Altn BLK 19        128.2   P2p

MI9960-Switch1#
MI9960-Switch1#
```

Copy Paste

Top

Diagram labels: Gig4/0, Gig5/0, Gig6/0, er-PT, ess-guolph, SITE C, MI9960-PC1 -10.150.136, MI9960-PC2-10.150.136, MI9960-PC3 10.150.136, 35, 10.150.136.32, PC-PT, 960-PC 3, vlan 20 class, Fa0, 10.150, PC-PT, MI9960-PC 4, 20, vlan 10 office.

Fig 3 showing the blocking ports, designated ports and ports cost is 19 on Switch 1.

NETWORK SECURITY 1 PROJECT

The screenshot shows the CLI of a switch named MI9960-Switch2. The user has entered the command `sh spanning-tree` in VLAN0001. The output displays the spanning tree configuration for VLAN0001, including the root ID, priority, address, cost, port, hello time, max age, and forward delay. The bridge ID and priority are also shown. The output then lists the interfaces and their roles in the spanning tree.

```
MI9960-Switch2>en
MI9960-Switch2#sh spannin
MI9960-Switch2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0030.F28C.0543
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay
15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0060.706C.0E97
             Hello Time  2 sec  Max Age 20 sec  Forward Delay
15 sec
             Aging Time  20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19       128.1    P2p
Fa0/3          Root FWD 19       128.3    P2p
Fa0/2          Desg FWD 19       128.2    P2p

MI9960-Switch2#
```

The output shows that Fa0/1 and Fa0/2 are designated ports (Desg) with a cost of 19, while Fa0/3 is the root port (Root) with a cost of 19. The status is FWD (Forwarding) for all ports. The priority is 128.1 for Fa0/1, 128.3 for Fa0/3, and 128.2 for Fa0/2. The type is P2p (Point-to-point) for all ports.

Fig 4 showing the designated ports and ports cost 19 on switch 2.

NETWORK SECURITY 1 PROJECT

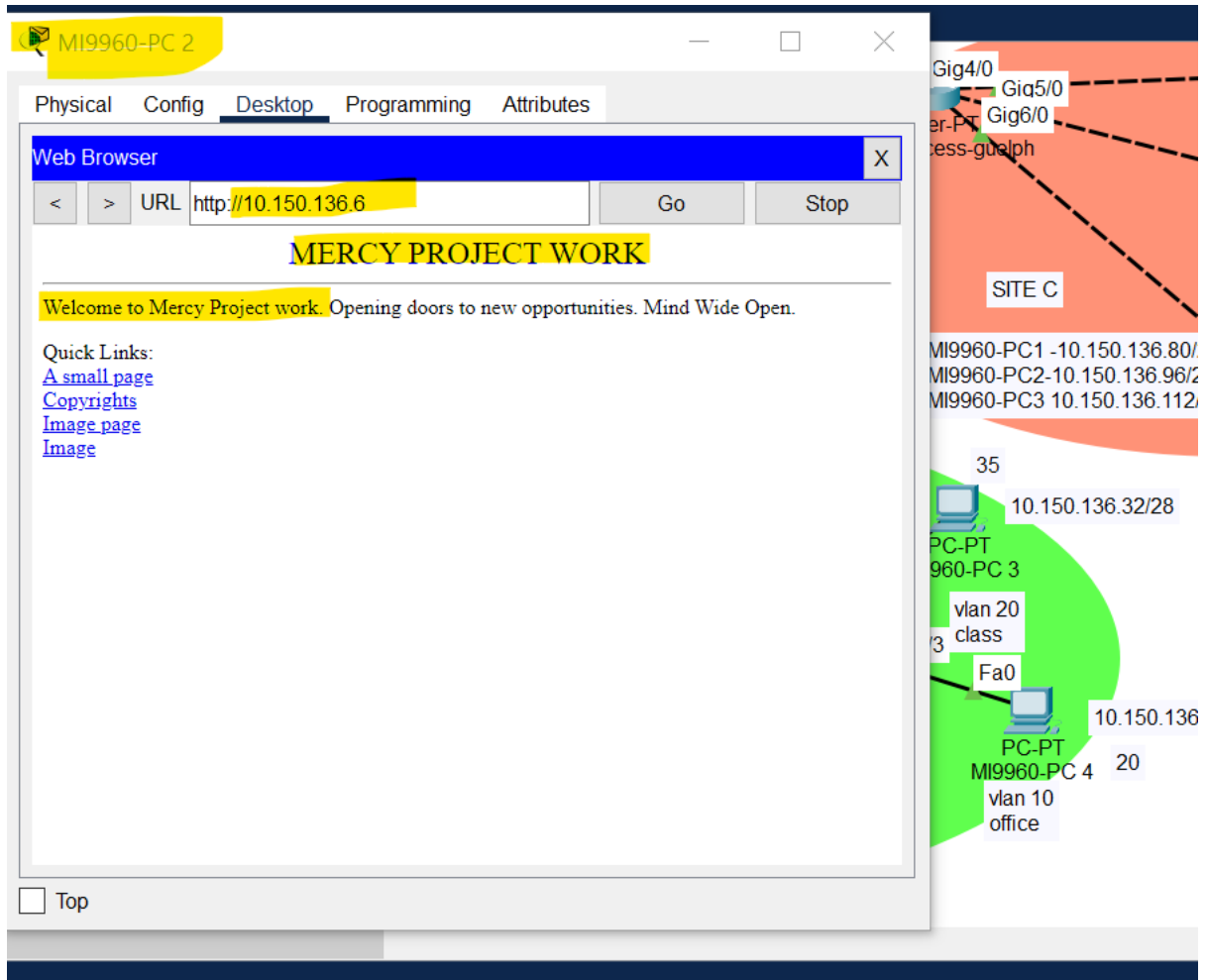


Fig 5 showing my customized home page.

NETWORK SECURITY 1 PROJECT

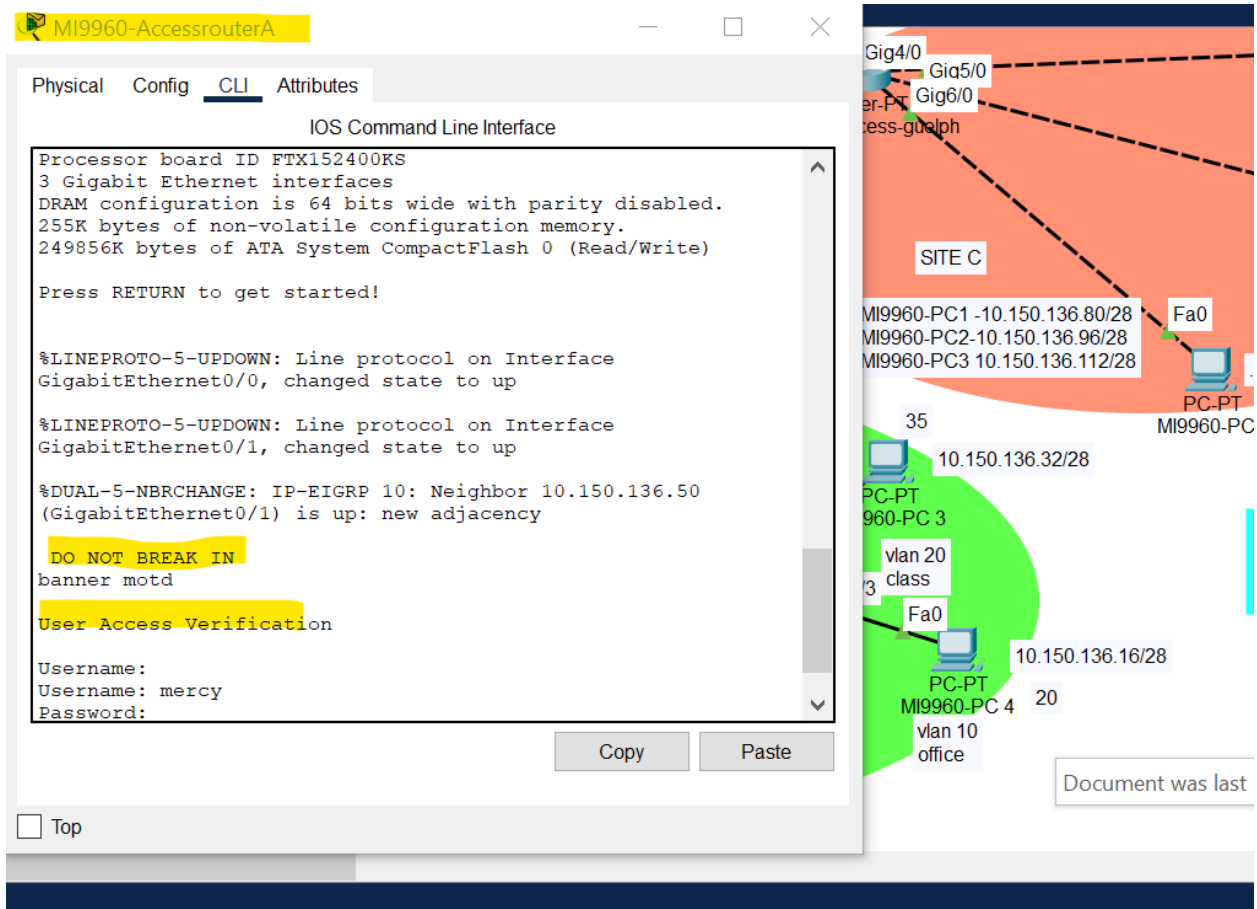


Fig 6 showing that I have configured banner of the day and I have enforced login.

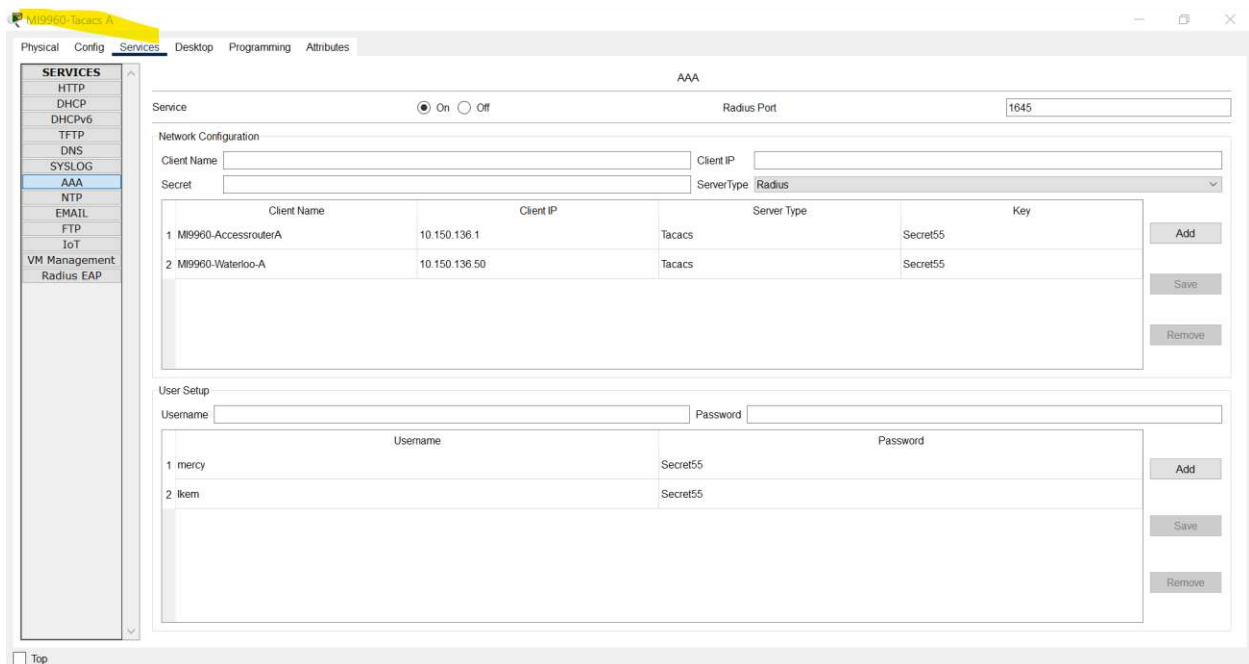


Fig 7 showing that I am using tacacs authentication for my access router and edge router.

NETWORK SECURITY 1 PROJECT

```
MI9960-AccessrouterA#
MI9960-AccessrouterA(config)#do sh run
Building configuration...

Current configuration : 1348 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MI9960-AccessrouterA
!
!
enable secret 5 $1$mRr$J8n8/unf2$zzhbVJzoq8D/
!
!
!
!
!
!
aaa new-model
!
aaa authentication login default group tacacs+
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username meccy password 7 0812494d1b1c114247
!
!
license udi pld C18C02911/R3 sn FTX152451X-
!
!
!
--More--
```

Fig 8 showing the configuration I made on my waterloo access router.

```
MI9960-AccessrouterA#
MI9960-AccessrouterA#
ip sah version 2
ip domain-name meccy.com
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.150.136.1 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.150.136.49 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 10
passive-interface GigabitEthernet0/0
network 10.150.136.0 0.0.0.15
network 10.150.136.48 0.0.0.15
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
--More--
```

Fig 9 showing the running configuration I made on access router.

NETWORK SECURITY 1 PROJECT



Fig 10 showing the configuration I made on the access router.

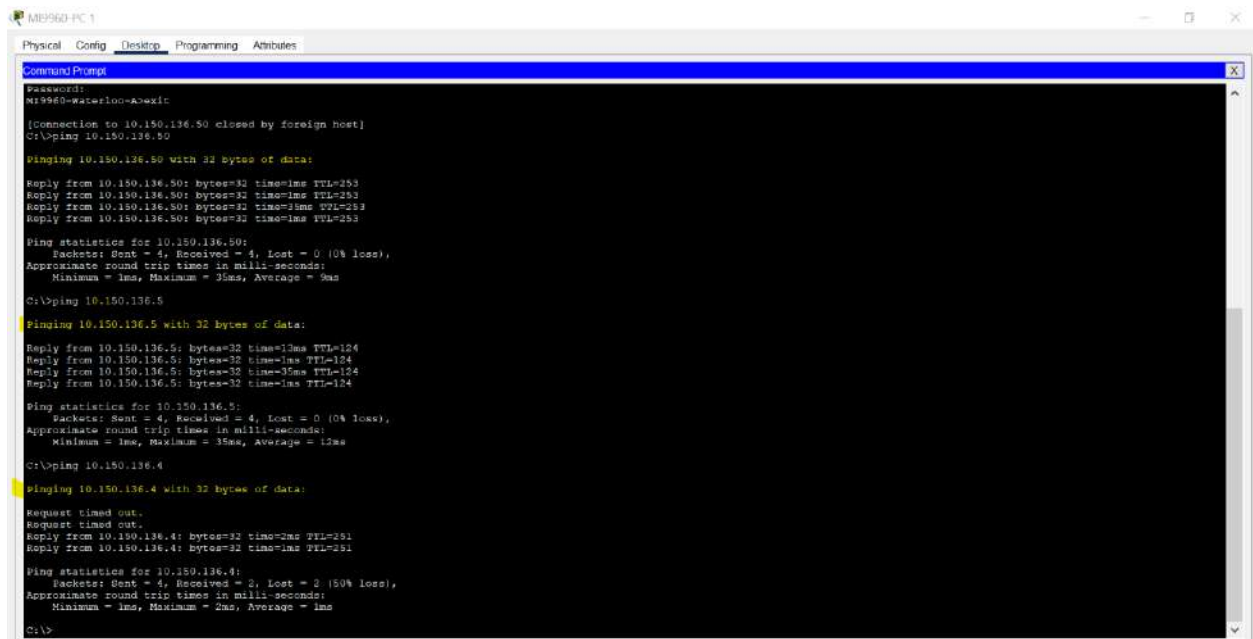
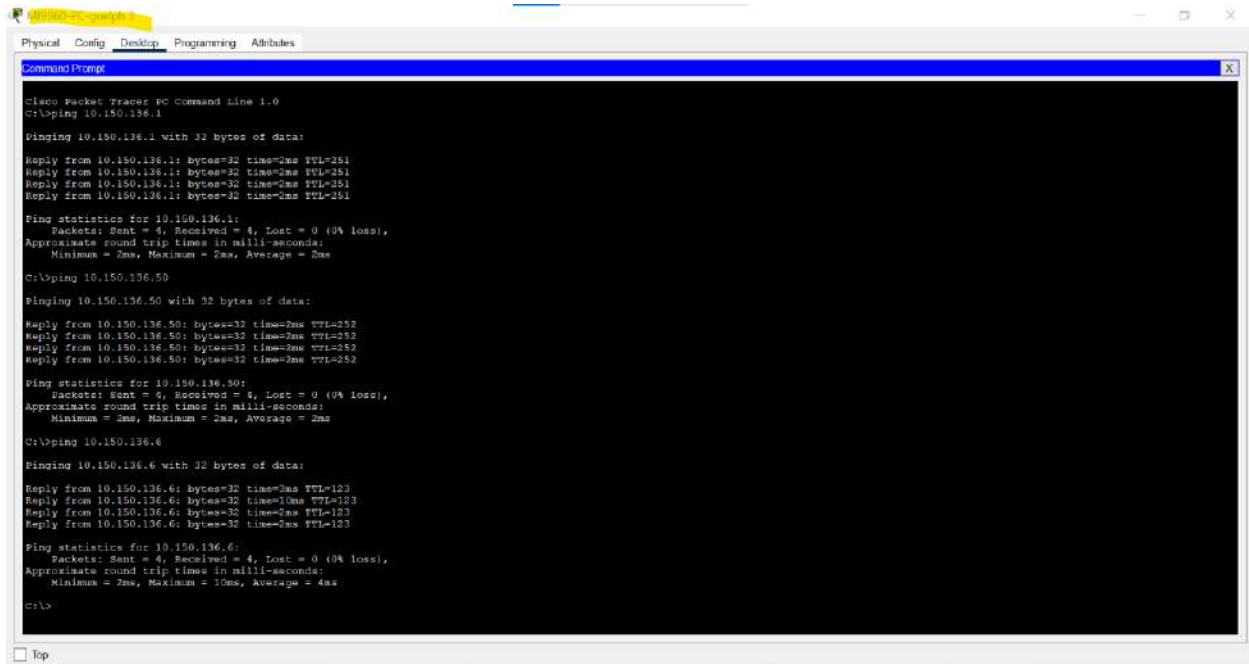


Fig 11 showing that the pc in site b can communicate with the router, switch and the server in site A.

NETWORK SECURITY 1 PROJECT



```
class packet tracer PC Command Line 1.0
C:\>ping 10.150.136.1

Pinging 10.150.136.1 with 32 bytes of data:

Reply from 10.150.136.1: bytes=32 time=2ms TTL=251
Reply from 10.150.136.1: bytes=32 time=2ms TTL=251
Reply from 10.150.136.1: bytes=32 time=2ms TTL=251
Reply from 10.150.136.1: bytes=32 time=2ms TTL=251

Ping statistics for 10.150.136.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\>ping 10.150.136.50

Pinging 10.150.136.50 with 32 bytes of data:

Reply from 10.150.136.50: bytes=32 time=2ms TTL=252
Reply from 10.150.136.50: bytes=32 time=2ms TTL=252
Reply from 10.150.136.50: bytes=32 time=2ms TTL=252
Reply from 10.150.136.50: bytes=32 time=2ms TTL=252

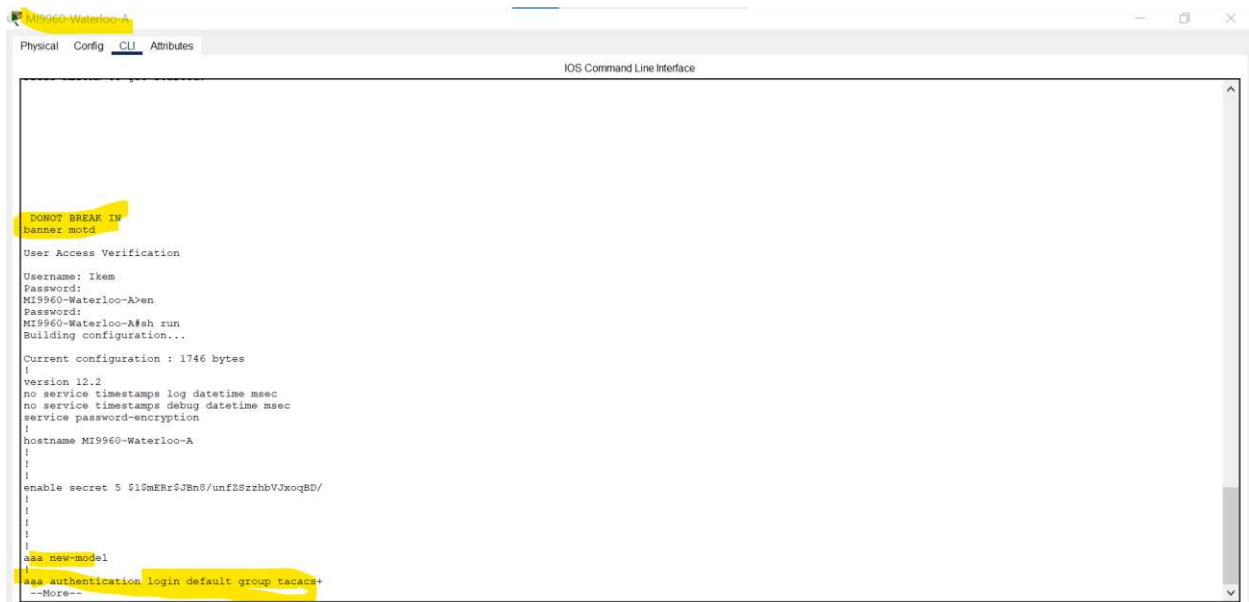
Ping statistics for 10.150.136.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\>ping 10.150.136.6

Pinging 10.150.136.6 with 32 bytes of data:

Reply from 10.150.136.6: bytes=32 time=2ms TTL=123
Reply from 10.150.136.6: bytes=32 time=2ms TTL=123
Reply from 10.150.136.6: bytes=32 time=2ms TTL=123
Reply from 10.150.136.6: bytes=32 time=2ms TTL=123

Ping statistics for 10.150.136.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 4ms
C:\>
```

Fig 12 shows that site c can communicate with site A.



```
Physical Config CLI Attributes
IOS Command Line Interface

DONT BREAK IN
banner motd

User Access Verification

Username: ikem
Password:
MI9960-Waterloo-A>en
Password:
MI9960-Waterloo-A#sh run
Building configuration...

Current configuration : 1746 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MI9960-Waterloo-A
!
!
!
enable secret 5 $1$mERr$JbN9/unfZ8zrhbVJxoq8D/
!
!
!
!
!
aaa new-model
!
aaa authentication login default group tacacs+
--More--
```

Fig 13 showing the configuration I made on the edge router.

NETWORK SECURITY 1 PROJECT



Fig 14 showing the configuration I made on the edge router.

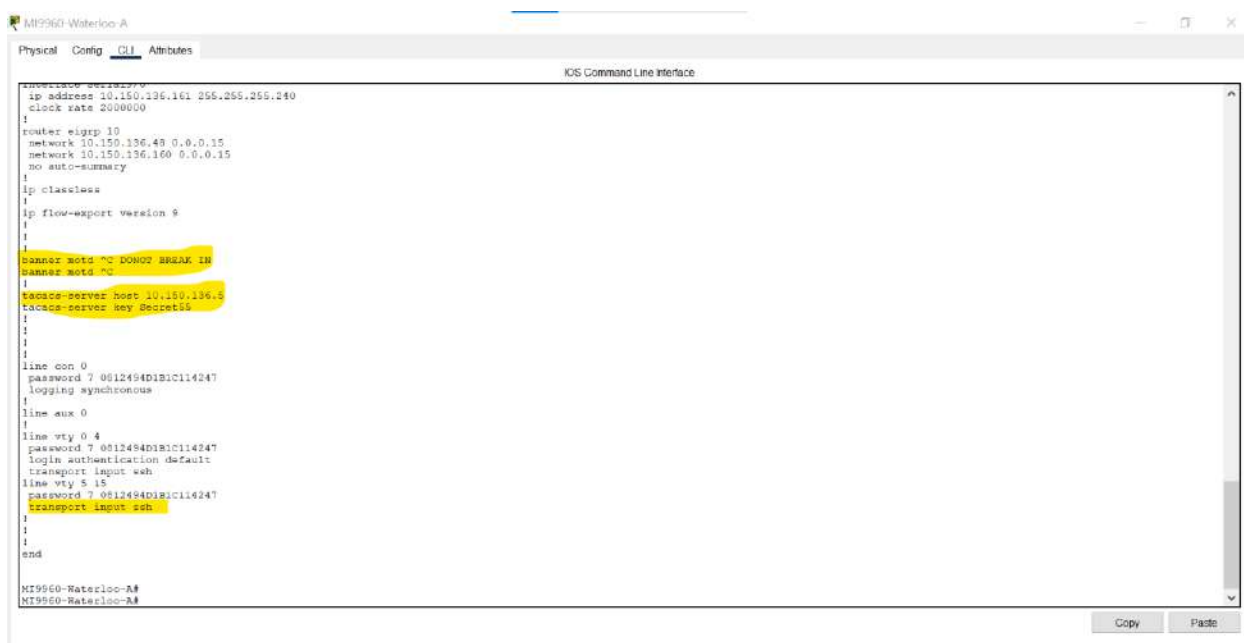


Fig 15 showing the configuration I made on the edge router.

NETWORK SECURITY 1 PROJECT

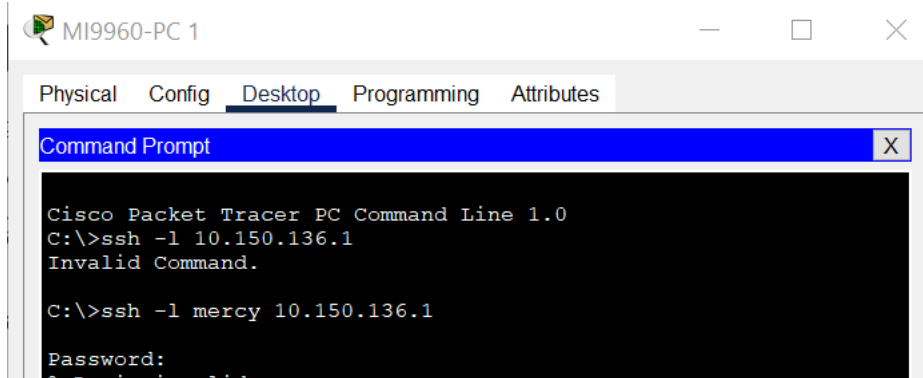


Fig 16 showing that I can ssh into the access router in site A using the pc in site b

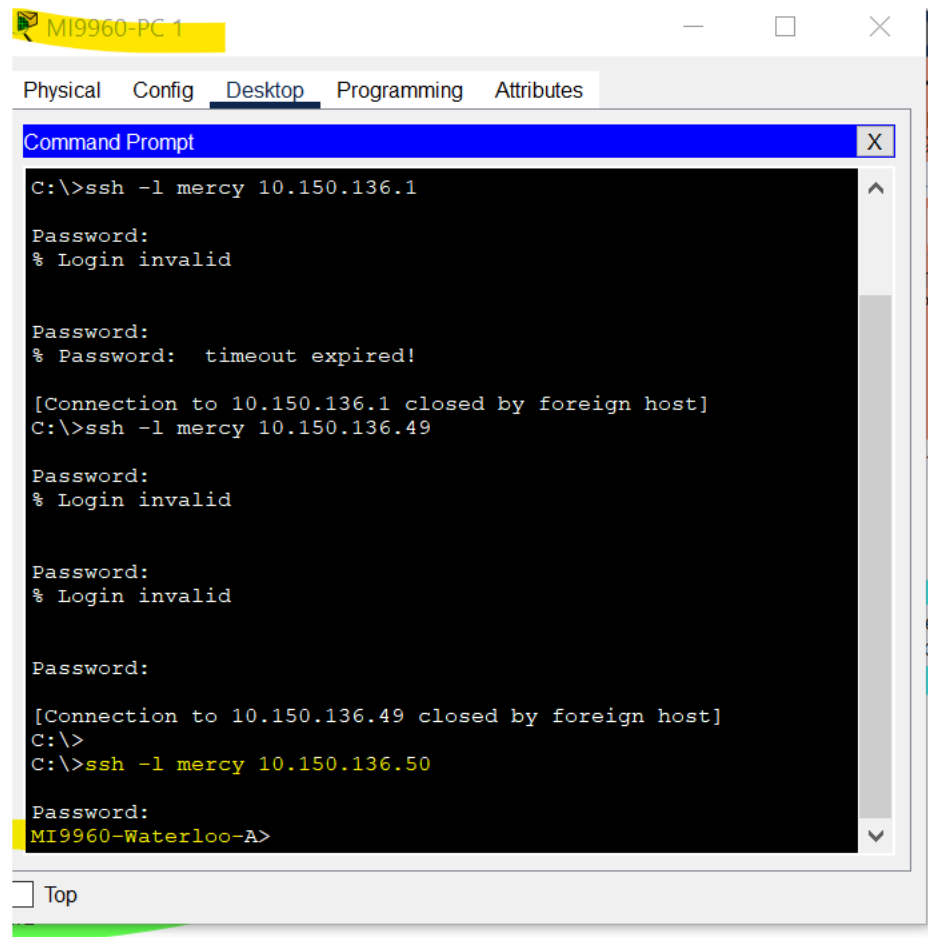


Fig 17 showing that I ssh into the edge router on site A using the pc in site b.

NETWORK SECURITY 1 PROJECT

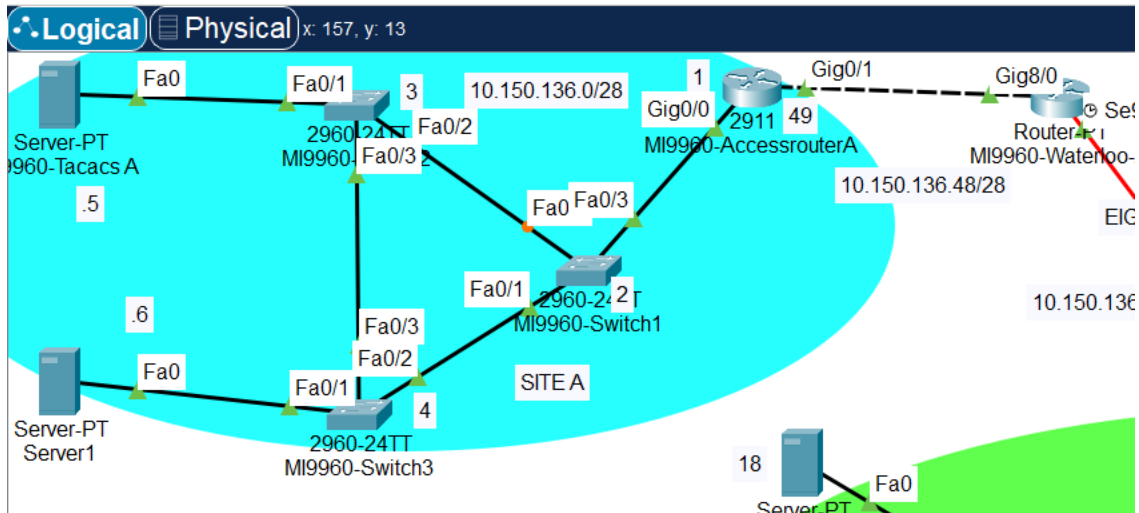


Fig 18 showing my Topology for site A.

SITE B

DESCRIPTION:

The goal for site B is to create a network that contains several switches, routers, and PCs that must be connected to provide secure remote access, inter-VLAN routing, and device connectivity.

REQUIREMENTS:

I will configure site B to do the following.

- I will configure the access router and edge router to authenticate using RADIUS server and remote using ssh.
- The radius server will be connected to one of the Vlans.
- Each of my switches in site b will have two identical vlans.
- Two pcs will be connected to each of the layer 2 switches, and they will be on separate vlans.
- I will connect the two-layer 2 switch to a layer 3 switch and configure VLAN Trunking and Inter VLAN routing.
- The computer connected to the switch must be able to communicate with each other.

DESIGN

To meet the requirements I mentioned above, I must make sure that my design will be implemented like this:

- My network will have several devices, including switches, routers, and computers. The network will have two VLANs, VLAN 10 and 20.

NETWORK SECURITY 1 PROJECT

- The access router will be the default gateway for the switches and the PC.
- I will use OSPF authentication to route between my Access and Edge router. The Edge router will securely **redistribute** routing information between site A and site B.
- I will include the following devices.
- **Access router-** 1 2911 router
- **Edge router-** 1 router PT
- **Layer 3 switch -1** 3560-24PS
- **Two-layer 2 switch -2960** Switches.
- **Radius server**
- **two pcs on both sides.**
- Access router will be connected to the edge router through serial link.
- The Edge router will be connected to layer 3 switch through a link and to the access router.
- I will connect the layer 3 switch to layer 2 switches through a trunk link.
- My radius server will be connected to one of my vlan (VLAN 10).
- My two PCs will be connected to the Vlans. (VLAN 10 and 20).

I will assign the following IP addresses to my devices.

- Access router-se9/0-10.150.136.162/28 gig6/0 10.150.136.66/28 se2/0 10.150.136.177/28
- Edge router- VLAN 10 (10.150.136.17/28) VLAN 20 (10.150.136.33/28)
- Layer 3 switch-VLAN 10 (10.150.136.21/28) VLAN 20 (10.150.136.37/28)
- MI9960-PC 1-10.150.136.19/28(VLAN 10)
- MI9960-PC 2-10.150.136.34/28(VLAN 20)
- MI9960-PC3-10.150.136.35/28(VLAN 20)
- MI9960-PC4-10.150.136.20/28(VLAN 10)
- Radius server-10.150.136.18/28(VLAN 10)

SCREENSHOT

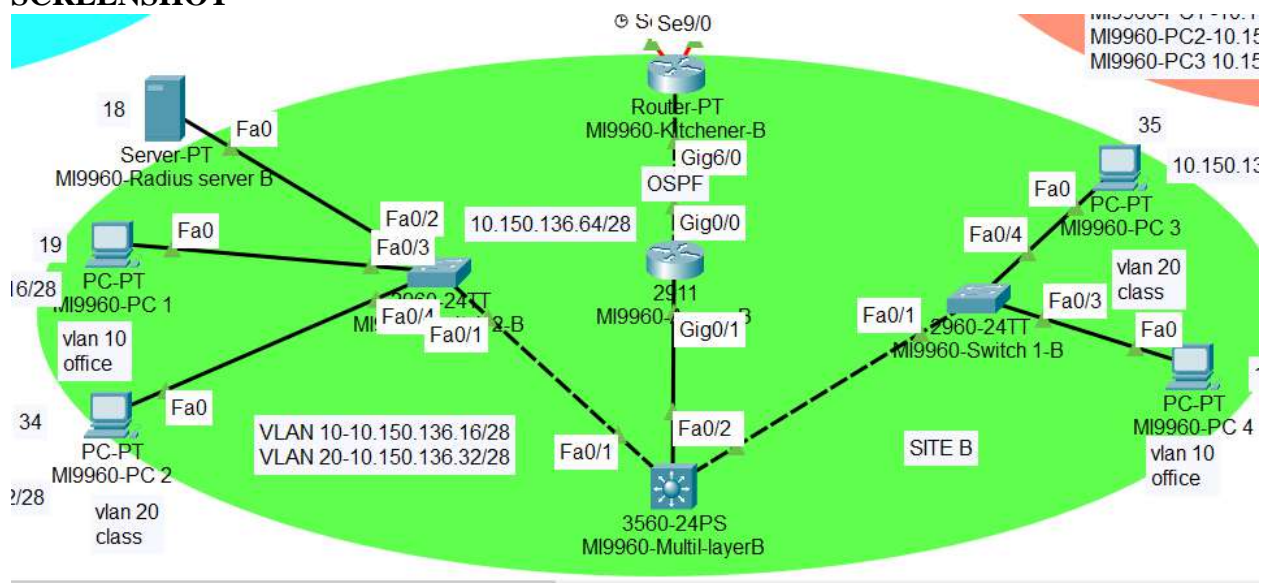


Fig 19 shows my Site B topology.

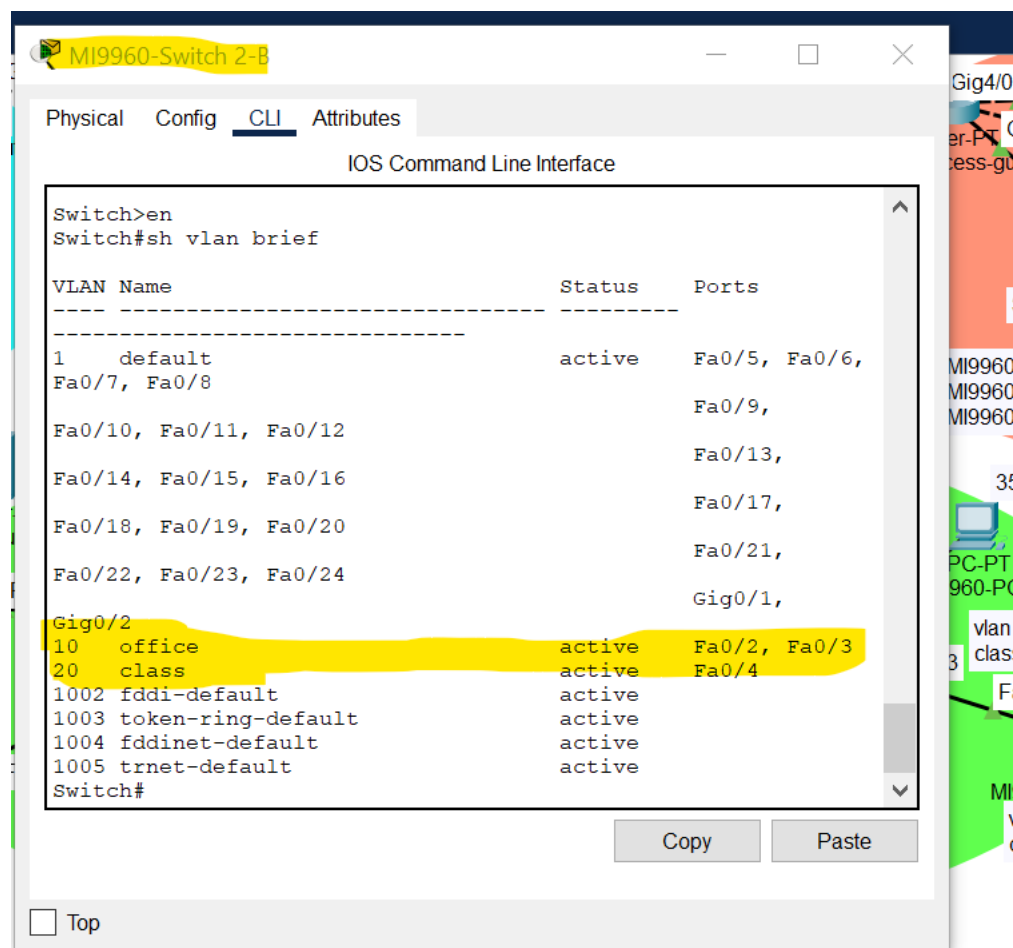


Fig 20 showing my vlan in switch 2 in site B.

NETWORK SECURITY 1 PROJECT

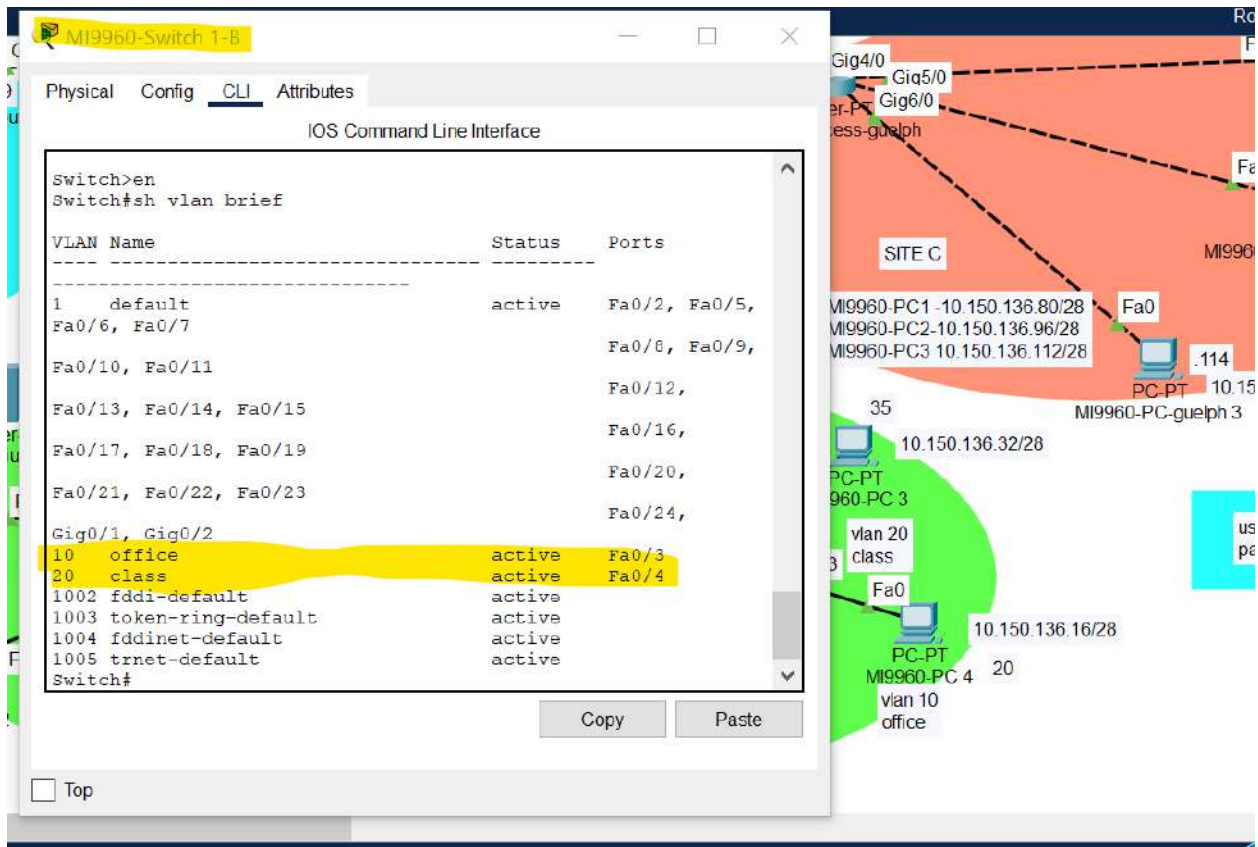


Fig 21 shows my vlan in switch 1 in site B.

NETWORK SECURITY 1 PROJECT

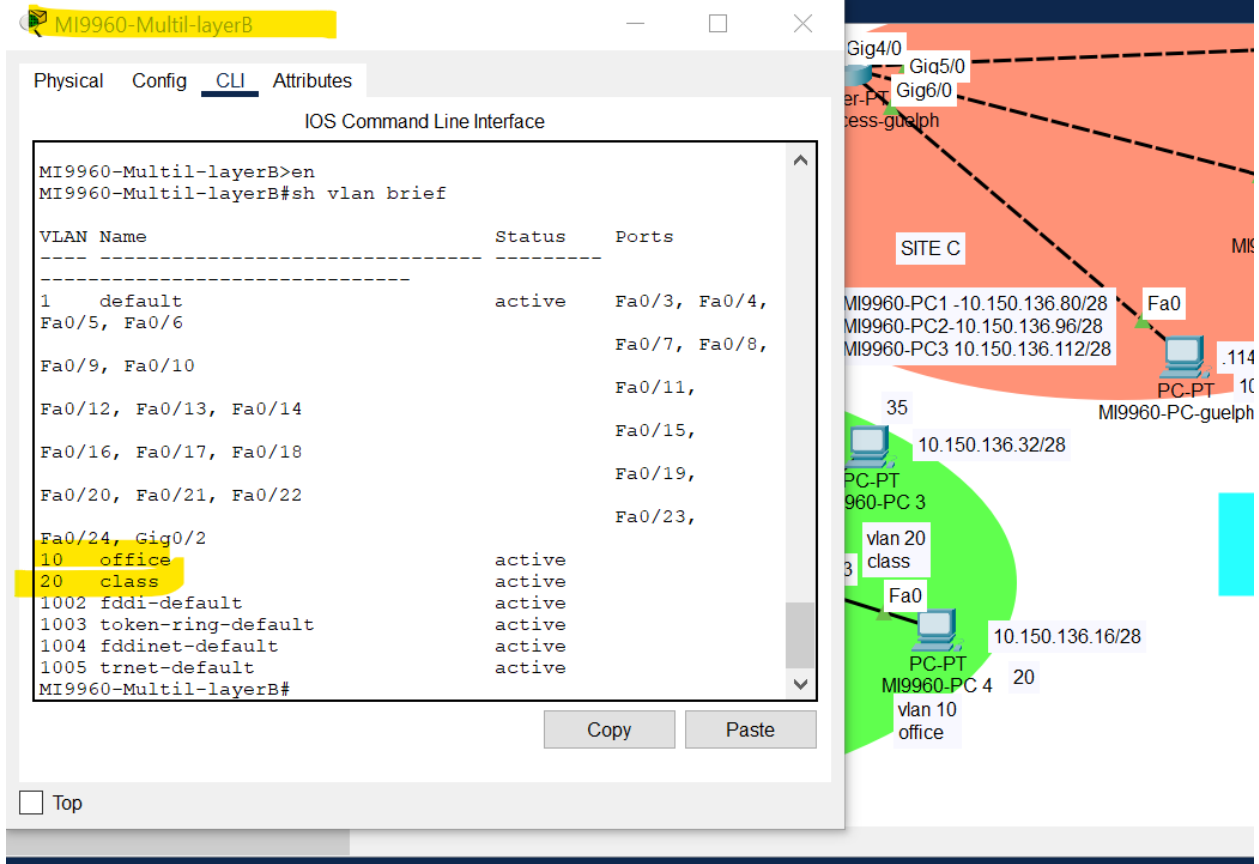


Fig 22 showing my vlan in my multilayer switch.

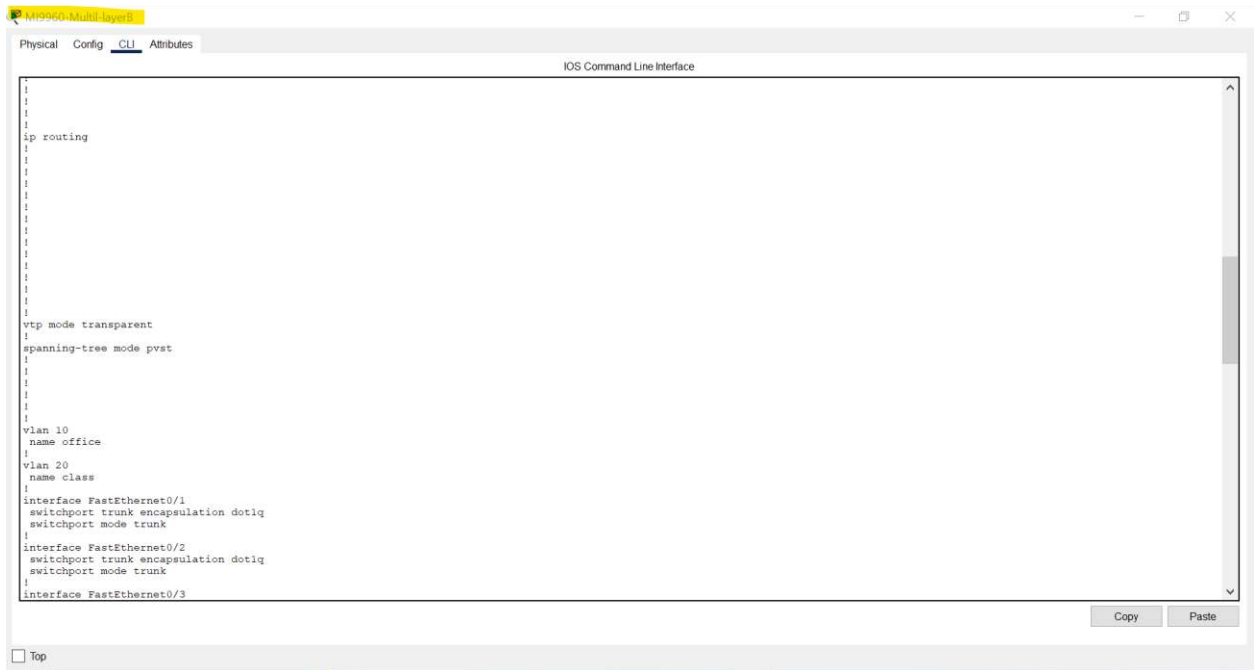
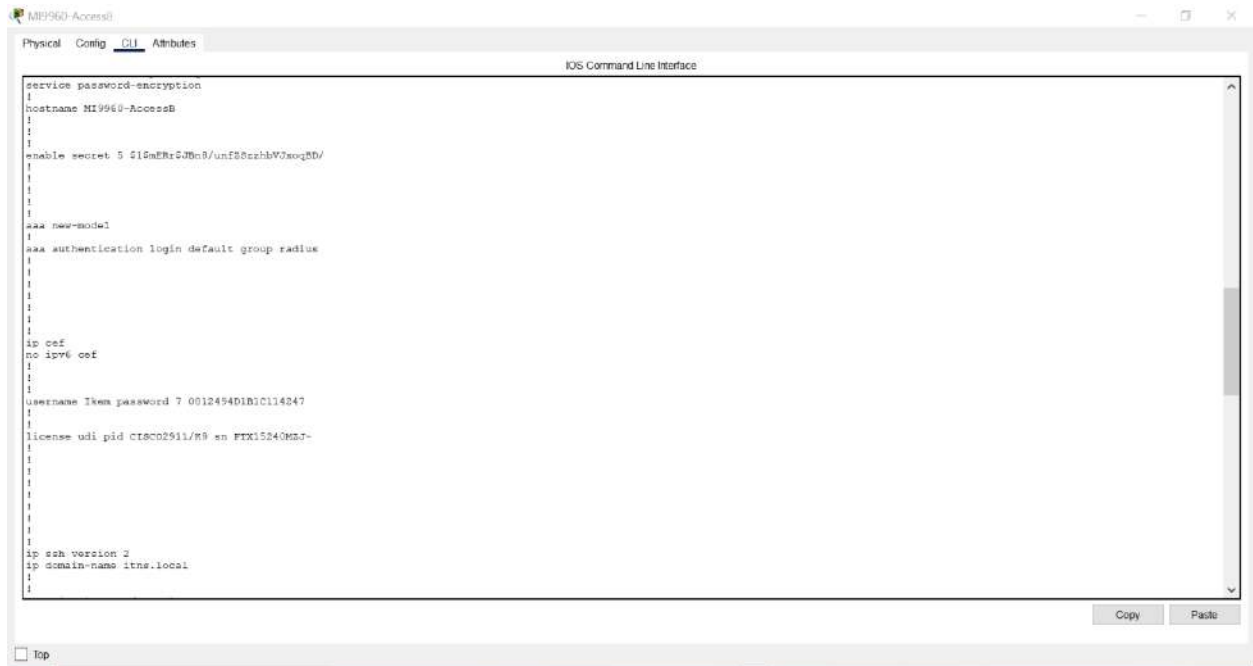


Fig 23 showing the configuration I made in my multilayer switch.

NETWORK SECURITY 1 PROJECT



```
service password-encryption
!
hostname MI9960-AccessB
!
!
enable secret 5 215aEkr5Jbn8/unf88znhbW0xog8D/
!
!
!
aaa new-model
!
aaa authentication login default group radius
!
!
!
!
ip cef
no ipv6 cef
!
!
username Iken password 7 0012494D1B1C114247
!
!
license udi pid CISC02911/R9 sn FTX15240M2J-
!
!
!
!
!
ip ssh version 2
ip domain-name itns.local
!
!
```

Fig 24 showing the configuration I did in MI9960 Access Router.



```
!
spanning-tree mode pvst
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.150.136.65 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 10.150.136.17 255.255.255.240
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 10.150.136.33 255.255.255.240
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 10
router-id 2.2.2.2
log-adjacency-changes
passive-interface GigabitEthernet0/1
network 10.150.136.0 0.0.0.15 area 0
network 10.150.136.16 0.0.0.15 area 0
network 10.150.136.32 0.0.0.15 area 0
```

Fig 25 showing the configuration I did in MI9960 Access Router.

NETWORK SECURITY 1 PROJECT

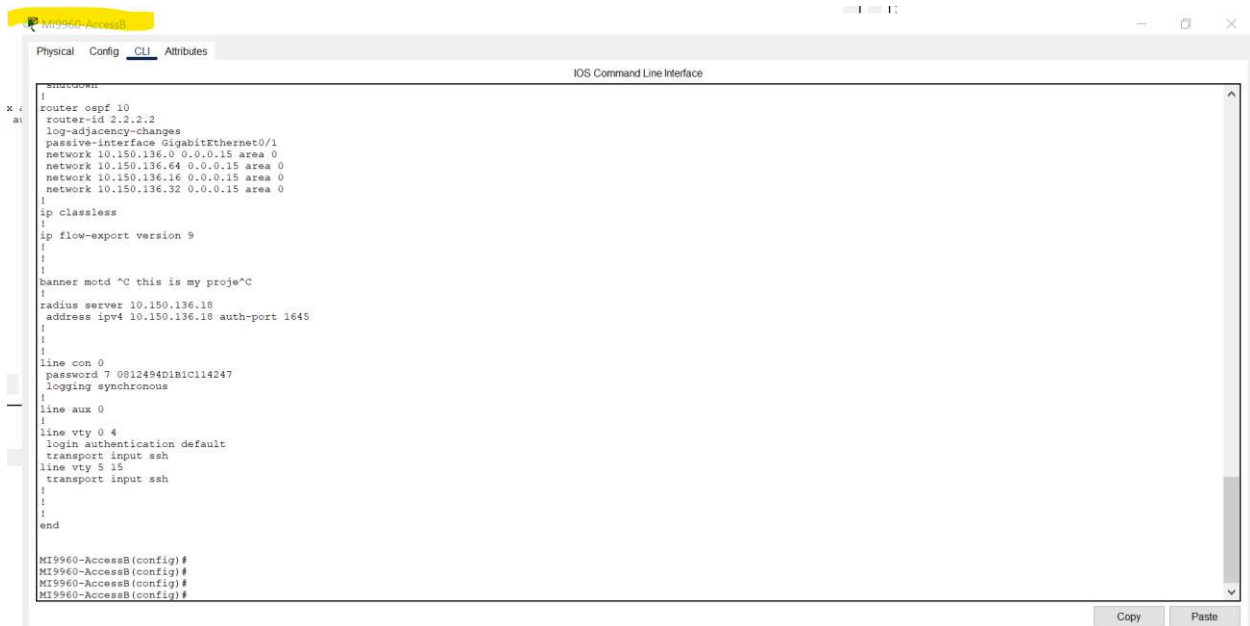


Fig 26 showing the configuration I did in MI9960 Access Router.

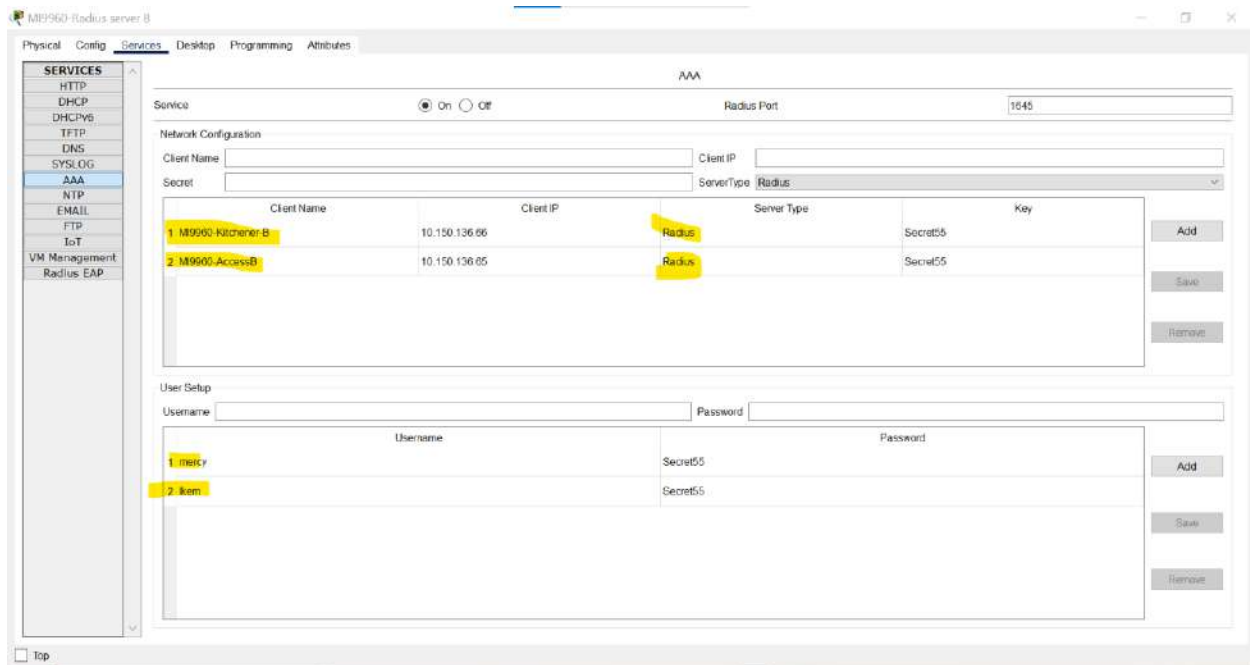
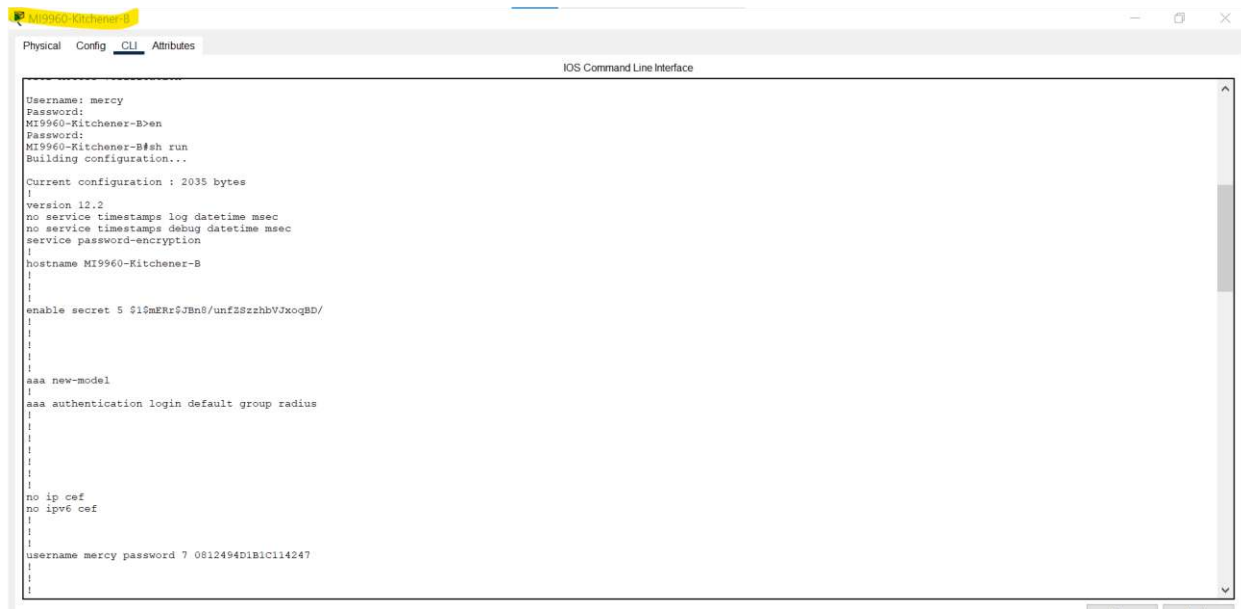


Fig 27 showing that I am using radius authentication for my access router and edge router.

NETWORK SECURITY 1 PROJECT



```
Username: mercy
Password:
MI9960-Kitchener-B>en
Password:
MI9960-Kitchener-B#sh run
Building configuration...

Current configuration : 2035 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MI9960-Kitchener-B
!
!
enable secret 5 $1$mEr$Jbn8/unf2SzshbVJaoqBD/
!
!
!
aaa new-model
!
aaa authentication login default group radius
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username mercy password 7 0812494D1B1C114247
!
!
```

Fig 28 showing the configuration I made in my edge router.



```
!
!
username mercy password 7 0812494D1B1C114247
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name mercy.com
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial12/0
ip address 10.150.136.177 255.255.255.240
clock rate 2000000
!
interface Serial13/0
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet4/0
no ip address

```

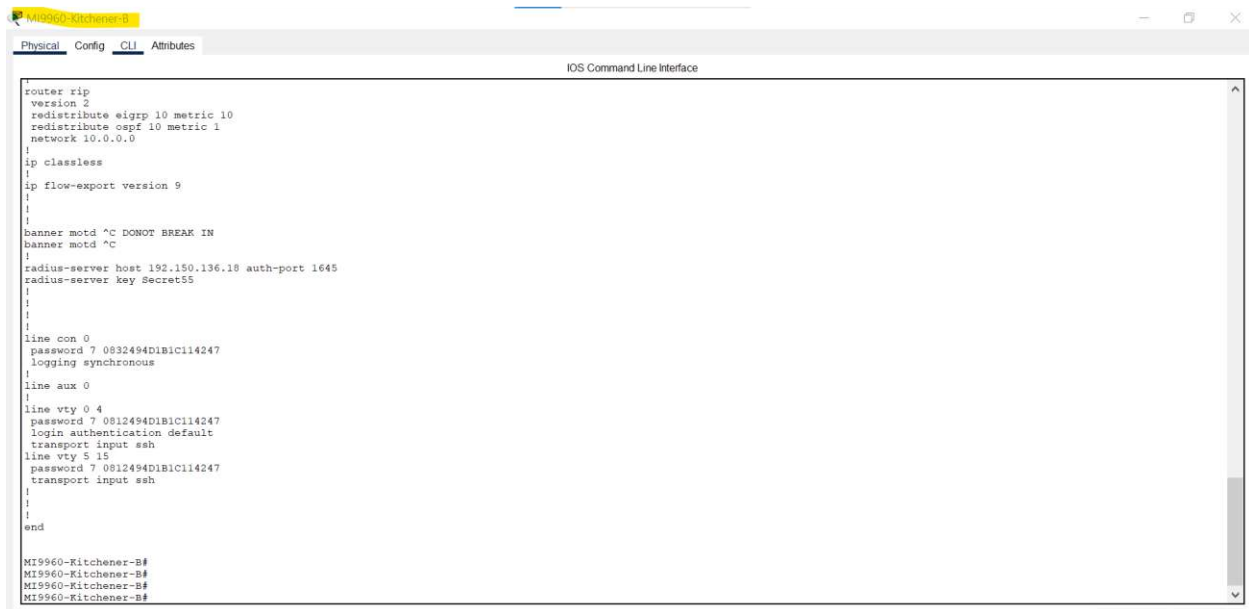
Fig 29 showing the configuration I made in my edge router.

NETWORK SECURITY 1 PROJECT



```
interface FastEthernet0/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface GigabitEthernet6/0
ip address 10.150.136.66 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet7/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet8/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial9/0
ip address 10.150.136.162 255.255.255.240
!
router eigrp 10
 redistribute rip metric 10000 0 255 100 1000
 redistribute ospf 10 metric 1 1 1 1
 network 10.150.136.160 0.0.0.15
 no auto-summary
!
router ospf 10
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute rip metric 1 subnets
 redistribute eigrp 10 subnets
 network 10.150.136.64 0.0.0.15 area 0
!
router rip
 version 2
 redistribute eigrp 10 metric 10
 redistribute ospf 10 metric 1
```

Fig 30 shows that my edge router is the main point for my redistribution to take place.



```
router rip
version 2
 redistribute eigrp 10 metric 10
 redistribute ospf 10 metric 1
 network 10.0.0.0
!
ip classless
!
ip flow-export version 9
!
!
banner motd ^C DONOT BREAK IN
banner motd ^C
!
radius-server host 192.150.136.10 auth-port 1645
radius-server key Secret55
!
!
!
line con 0
password 7 0812494D1B1C114247
logging synchronous
!
line aux 0
!
line vty 0 4
password 7 0812494D1B1C114247
login authentication default
transport input ssh
line vty 5 15
password 7 0812494D1B1C114247
transport input ssh
!
!
!
end

M19960-Kitchener-B#
M19960-Kitchener-B#
M19960-Kitchener-B#
M19960-Kitchener-B#
```

Fig 31 showing the configuration I made in my edge router.

NETWORK SECURITY 1 PROJECT

SITE C

DESCRIPTION:

The aim for my site C is to design and implement a network infrastructure for a multi-site organization. I will include three different networks and subnets.

REQUIREMENTS:

- I will ensure that all my computers can communicate with each other.
- I will ensure that all devices in the network can be remotely managed using local authentication.
- I will configure RIP routing protocol between Access and edge router.
- I will configure **redistribution** of routing information between site A and site C.
- I will configure local authentication on my network devices.

DESIGN

- 1 router PT, 1 router PT, 3 PC-PT.
- My three computers will have their own subnets and they will be connected to the access router.
- The access router will be responsible for routing between the different networks. I will configure RIP routing protocol to communicate with the edge router.
- I will configure remote access using local authentication.
- I will use daisy chain connection for SITE C and SITE B.

IP Addressing

- MI9960-PC Guelph 1- 10.150.136.82/28
- MI9960-PC Guelph 2- 10.150.136.98/28
- MI9960-PC Guelph 3- 10.150.136.112/28
- MI9960-Access Guelph – gig4/0 10.150.136.81/28 gig5/0 10.150.136.97/28 gig6/0 10.150.136.113/28 gig7/0 10.150.136.130/28
- MI9960-Edge Guelph- gig6/0 10.150.136.129/28 se9/0 10.150.136.178/28

NETWORK SECURITY 1 PROJECT

SCREENSHOT

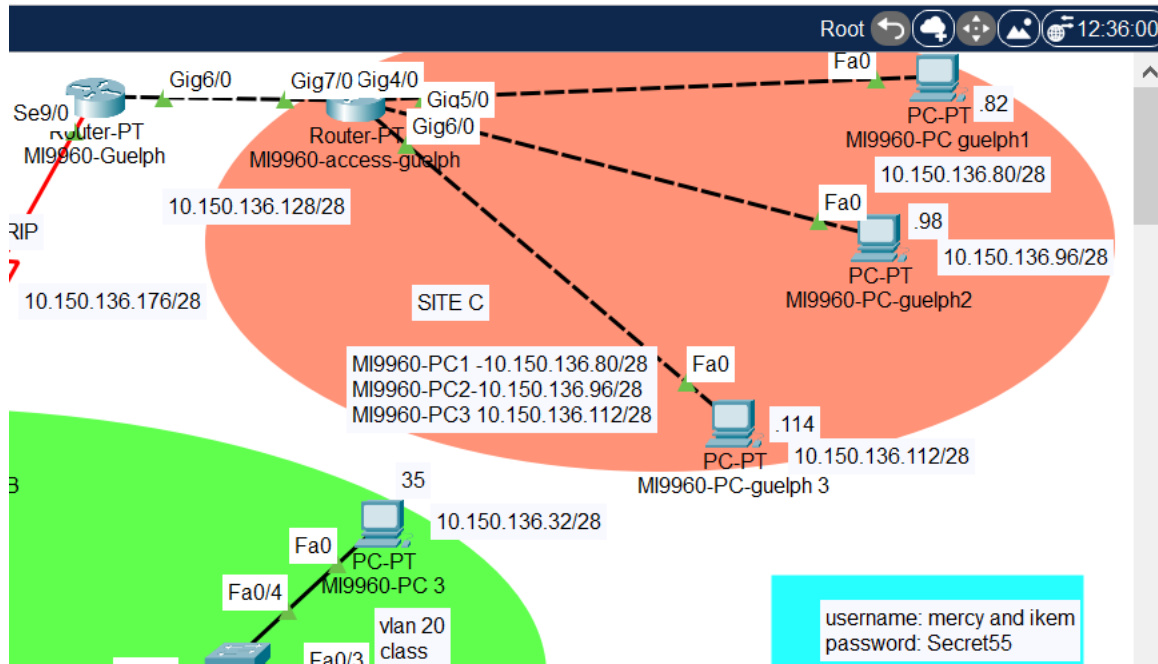


Fig 32 showing the topology for site C.

```
MI9960-access-guelph>en
Password:
MI9960-access-guelph#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MI9960-access-guelph(config)#do sh run
Building configuration...

Current configuration : 1600 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MI9960-access-guelph
!
enable secret 5 $1$mERt$JBn6/unf28zshbVJxoq8D/
!
!
aaa new-model
!
!
!
no ip cef
no ipv6 cef
!
username mercy password 7 0812494D1B1C114247
!
!
```

Fig 33 shows the configuration I made in my access router.

NETWORK SECURITY 1 PROJECT

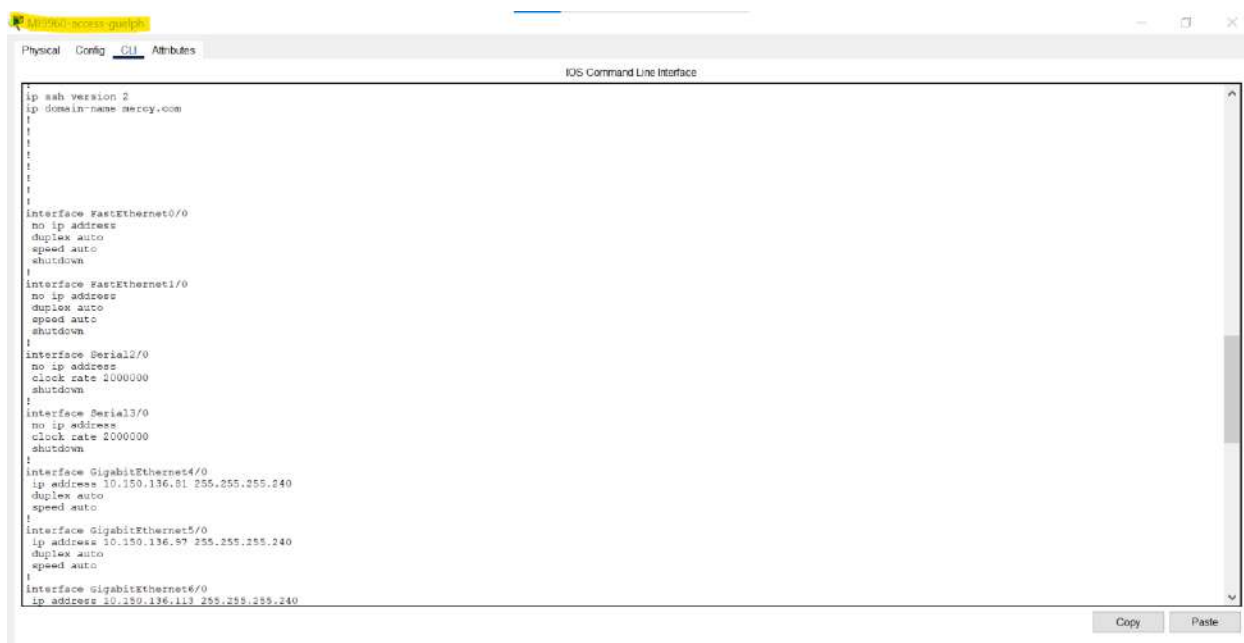


Fig 34 shows the configuration I made in my access router.

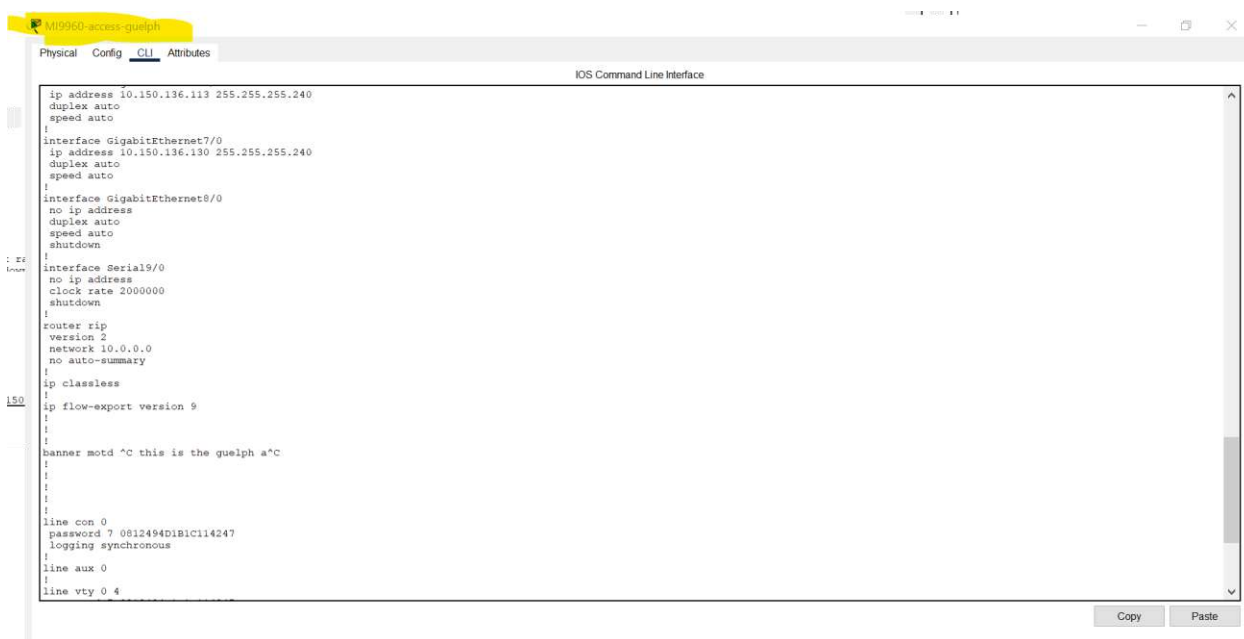


Fig 35 shows the configuration I made in my access router.

NETWORK SECURITY 1 PROJECT

[illegible]

Fig 36 shows the configuration I made in my access router.

Physical Config CLI Attributes

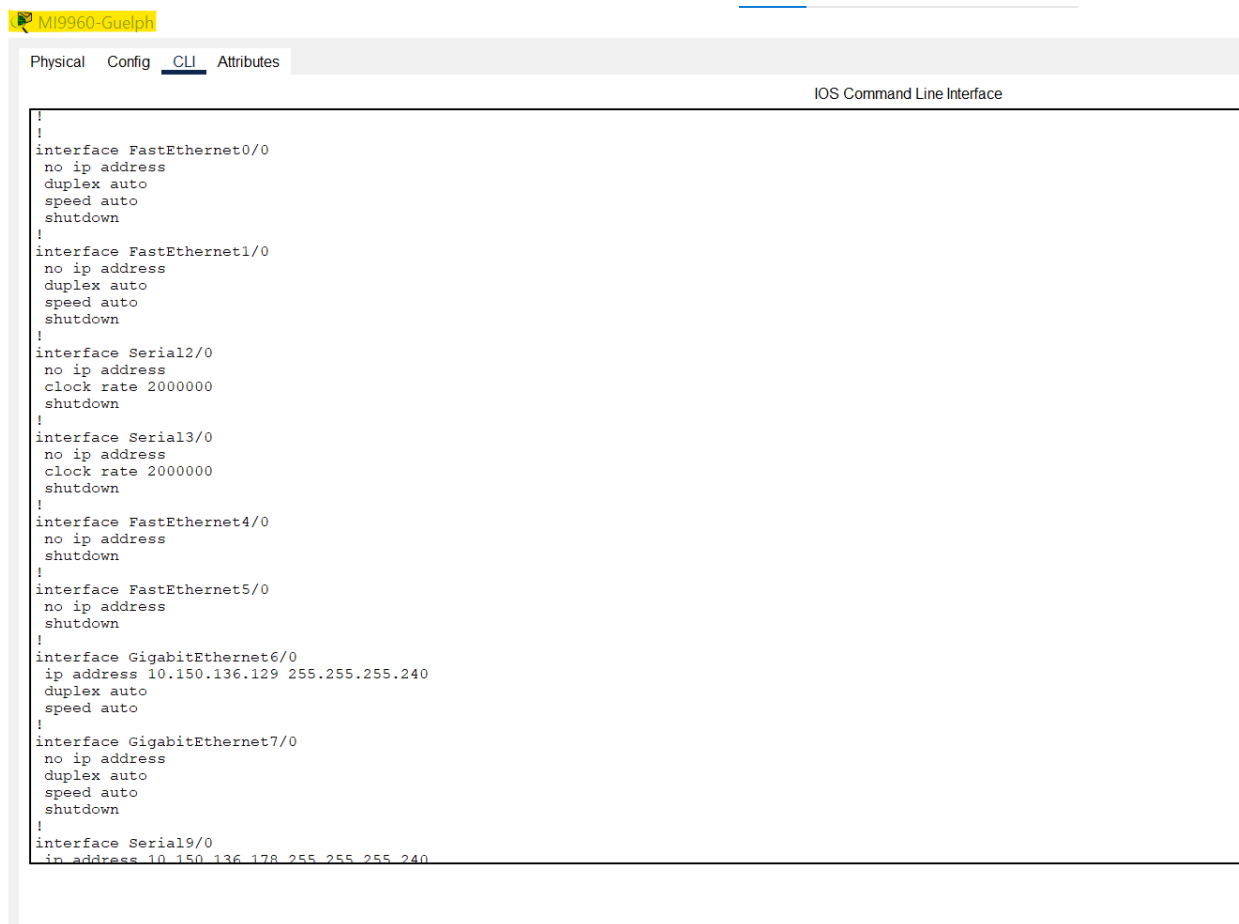
IOS Command Line Interface

```
Current configuration : 1533 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MI9960-Guelph
!
!
enable secret 5 $1$mErR$JBn8/unfZSzzhbVJxoqBD/
!
!
!
!
!
aaa new-model
!
aaa authentication login SSH-LOGIN local
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username mercy password 7 0812494D1B1C114247
!
!
!
!
!
!
ip ssh version 2
ip domain-name mercy.com
!
```

☐ Top

Fig 37 shows the configuration I made in my edge router.

NETWORK SECURITY 1 PROJECT

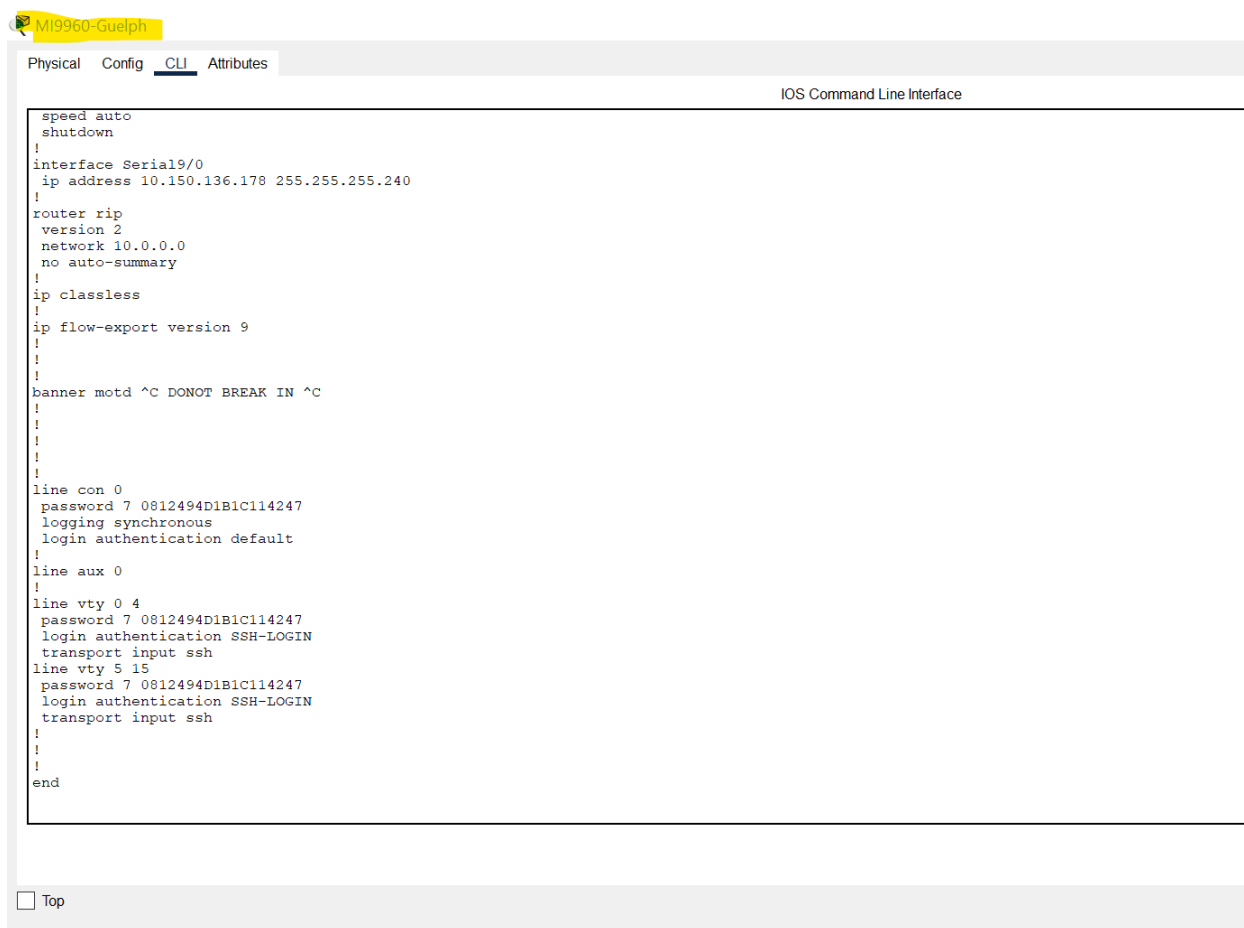


The screenshot shows a network configuration window with a yellow header bar containing a small icon and the text "M19960-Guelph". Below the header is a tabbed interface with four tabs: "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected and highlighted. The main area displays the "IOS Command Line Interface" with a list of configuration commands for an edge router. The commands are as follows:

```
!  
!  
interface FastEthernet0/0  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface FastEthernet1/0  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial2/0  
no ip address  
clock rate 2000000  
shutdown  
!  
interface Serial3/0  
no ip address  
clock rate 2000000  
shutdown  
!  
interface FastEthernet4/0  
no ip address  
shutdown  
!  
interface FastEthernet5/0  
no ip address  
shutdown  
!  
interface GigabitEthernet6/0  
ip address 10.150.136.129 255.255.255.240  
duplex auto  
speed auto  
!  
interface GigabitEthernet7/0  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial9/0  
ip address 10.150.136.178 255.255.255.240
```

Fig 38 shows the configuration I made in my edge router.

NETWORK SECURITY 1 PROJECT



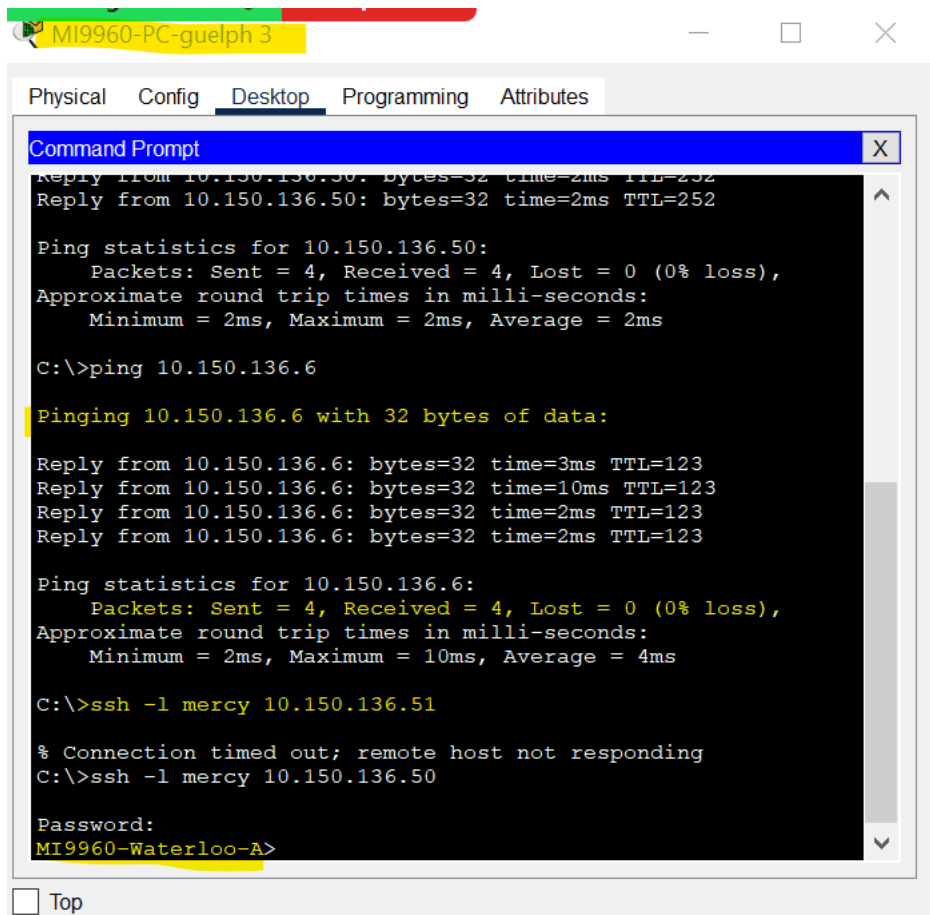
The screenshot shows a web-based configuration interface for a network device. At the top, there are tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is selected. Below the tabs, the title 'IOS Command Line Interface' is displayed. The main area contains a text box with the following configuration commands:

```
speed auto
shutdown
!
interface Serial19/0
ip address 10.150.136.178 255.255.255.240
!
router rip
version 2
network 10.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C DONOT BREAK IN ^C
!
!
!
!
line con 0
password 7 0812494D1B1C114247
logging synchronous
login authentication default
!
line aux 0
!
line vty 0 4
password 7 0812494D1B1C114247
login authentication SSH-LOGIN
transport input ssh
line vty 5 15
password 7 0812494D1B1C114247
login authentication SSH-LOGIN
transport input ssh
!
!
!
end
```

At the bottom left of the interface, there is a checkbox labeled 'Top'.

Fig 39 shows the configuration I made in my edge router.

NETWORK SECURITY 1 PROJECT



The screenshot shows a network configuration interface with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the results of a ping command to 10.150.136.50, followed by a ping command to 10.150.136.6, and then an attempt to connect via ssh to 10.150.136.51, which timed out. The user then attempts to connect via ssh to 10.150.136.50, and the prompt asks for a password. The user enters 'MI9960-Waterloo-A'.

```
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.150.136.50: bytes=32 time=2ms TTL=252
Reply from 10.150.136.50: bytes=32 time=2ms TTL=252

Ping statistics for 10.150.136.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ping 10.150.136.6

Pinging 10.150.136.6 with 32 bytes of data:

Reply from 10.150.136.6: bytes=32 time=3ms TTL=123
Reply from 10.150.136.6: bytes=32 time=10ms TTL=123
Reply from 10.150.136.6: bytes=32 time=2ms TTL=123
Reply from 10.150.136.6: bytes=32 time=2ms TTL=123

Ping statistics for 10.150.136.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 4ms

C:\>ssh -l mercy 10.150.136.51

% Connection timed out; remote host not responding
C:\>ssh -l mercy 10.150.136.50

Password:
MI9960-Waterloo-A>
```

Fig 37 showing that I can ssh into the edge router in site A