

SMALL NETWORK EXPANDED-SSH

Gtech want the ICT manager to be the one who should be able to access all network devices remotely securely.

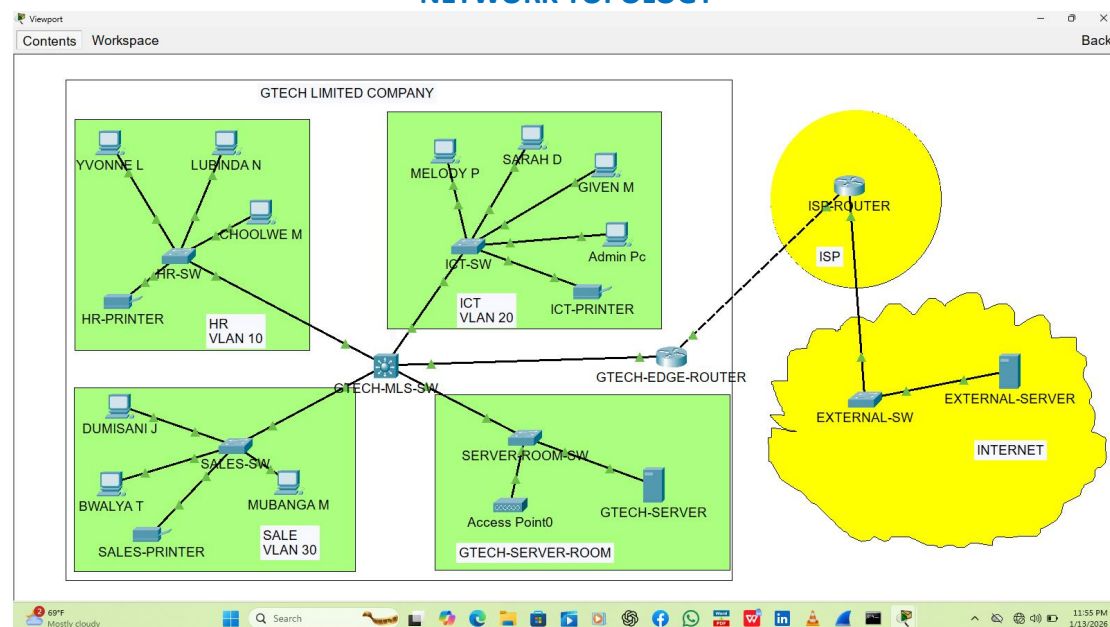
Remote secure access refers to managing network devices from a different location using encrypted management protocol. there are two methods to do this, thus telnet and ssh, telnet is not secure so we will use ssh. There are couple of things to consider this include;

- Username and secret.
- Domain name
- Ssh version
- Hostname
- Management vlan
- Gateway of management vlan
- Create crypto key rsa
- Access-list permitting the host(the PC to access the devices)
- Access-class on line vty
- Transport input SSH

In our case we already have hostname, username and domain name.

Network topology is still the same, I have just enabled the device names

NETWORK TOPOLOGY



Now lets start the configurations, they told us to make one change on the domain name

Instead of www.gtech.com but just gtech.local.

We will just make one change on our side as well on user password, we change it to secret.

On all devices(switches and router).

No username Admin password Admin123

No ip domain-name www.gtech.com

ip domain-name gtech.local

username Admin privilege 15 secret Admin123

crypto key generate rsa

ip access-list standard SSH-MGT

permit host 192.168.0.70

deny any

line vty 0 15

login local

transport input ssh

access-class SSH-MGT in

Exit

Now let us configure our management vlans on all switches

HR,ICT,SALES, MLS and SERVER ROOM SW.

Vlan 99

Name MGT

Ex

Next we configure switch virtual interface on the MLS

Int vlan 99

No shut

Ip add 192.168.0.65 255.255.255.240

Do wr

Ex

Let us now configure SVI for management vlan and gateway on all switches, we should keep in mind that the manager is in ICT dept

HR

Int vlan 99

No shut

Ip add 192.168.0.66 255.255.255.240

Ip default-gateway 192.168.0.65

Do wr

ICT

Here this is where we do the magic,

All the interface on this switch is in vlan 20, we just created vlan 99,the unassigned interface is gig0/2 that will be the interface for vlan 99.

Int vlan 99

Ip add 192.168.0.67

No shut

Ip default-gateway 192.168.0.65

Do wr

We need to configure static ip address on the Admin pc

!192.168.0.70 255.255.255.240

!Gateway 192.168.0.65

!Dns-server 8.8.8.8

SALES

Int vlan 99

No shut

Ip add 192.168.0.68 255.255.255.240

Ip default-gateway 192.168.0.65

Do wr

SERVER ROOM

Int vlan 99

No shut

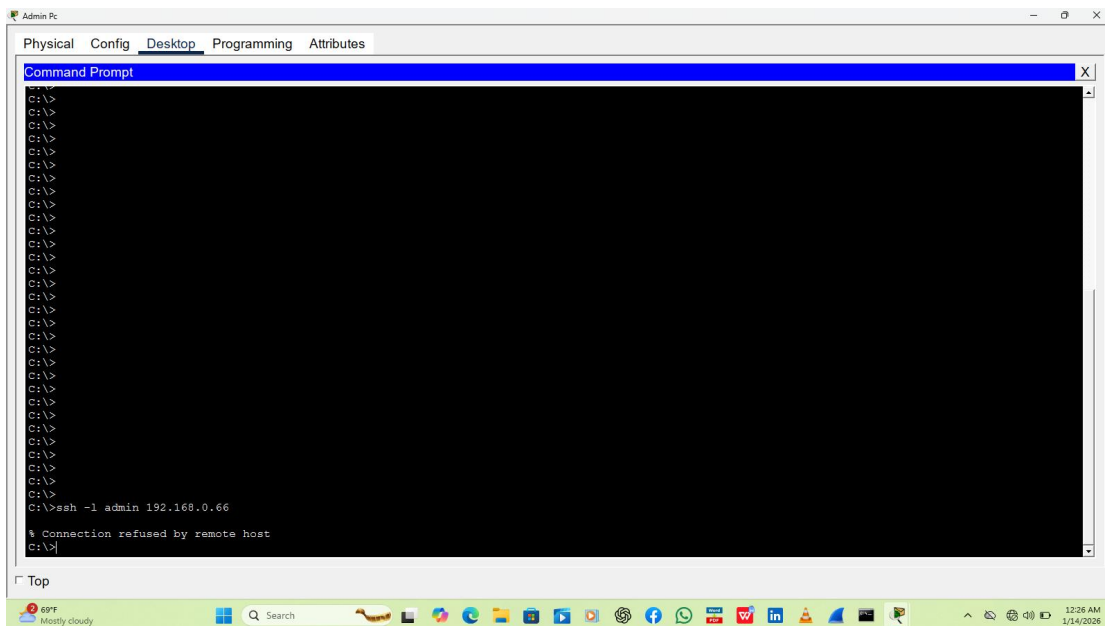
Ip add 192.168.0.69 255.255.255.240

Ip default-gateway 192.168.0.65

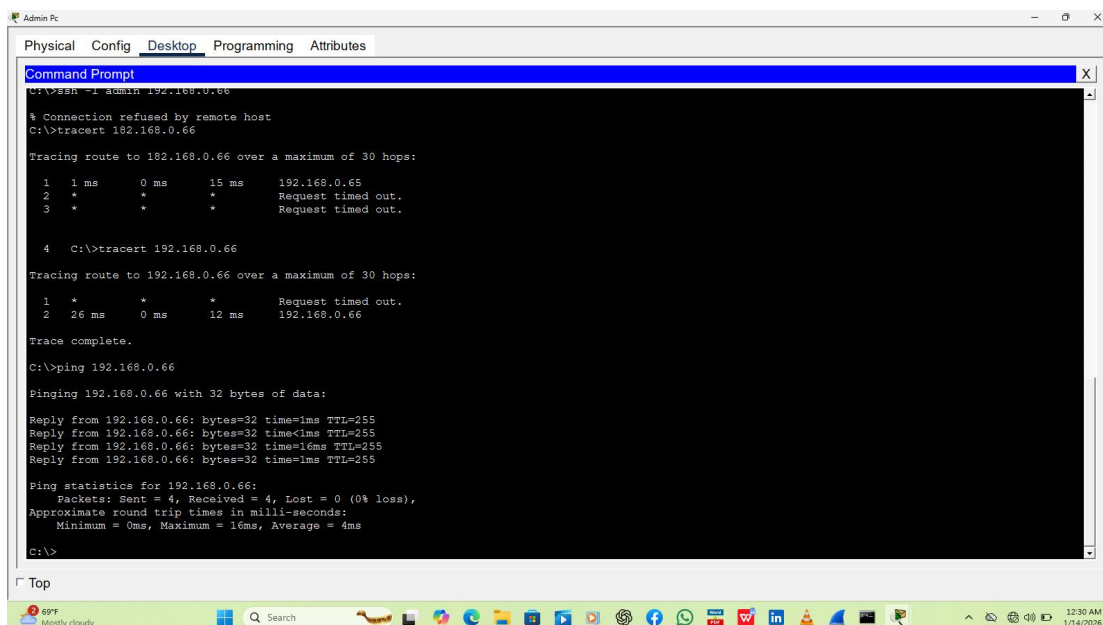
Do wr

We are partially done, let us test if Admin pc is able to access those devices

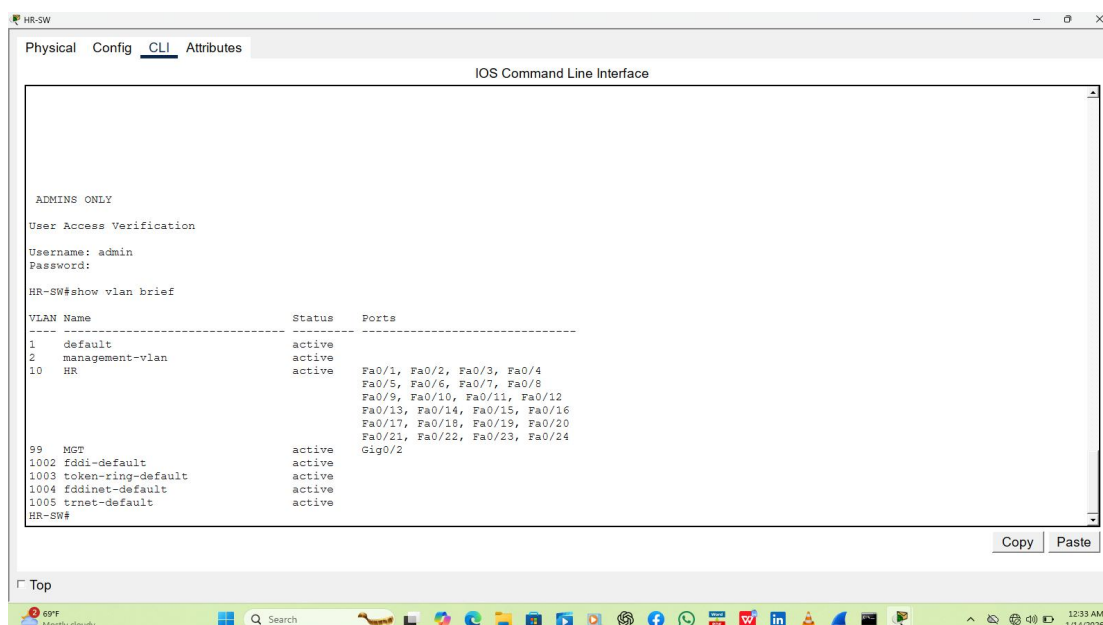
From Admin PC we go to command prompt we type "ssh -l admin 192.168.0.66(HR SW) if the configurations are okay we will be prompted to put password



We landed straight into an error, whats wrong here?let us troubleshoot



Ping is working, so this isn't connection issue,what does that mean? It means the problem we have is a layer 2 problem, let us go to HR sw and check the existing vlans
Show vlan brief

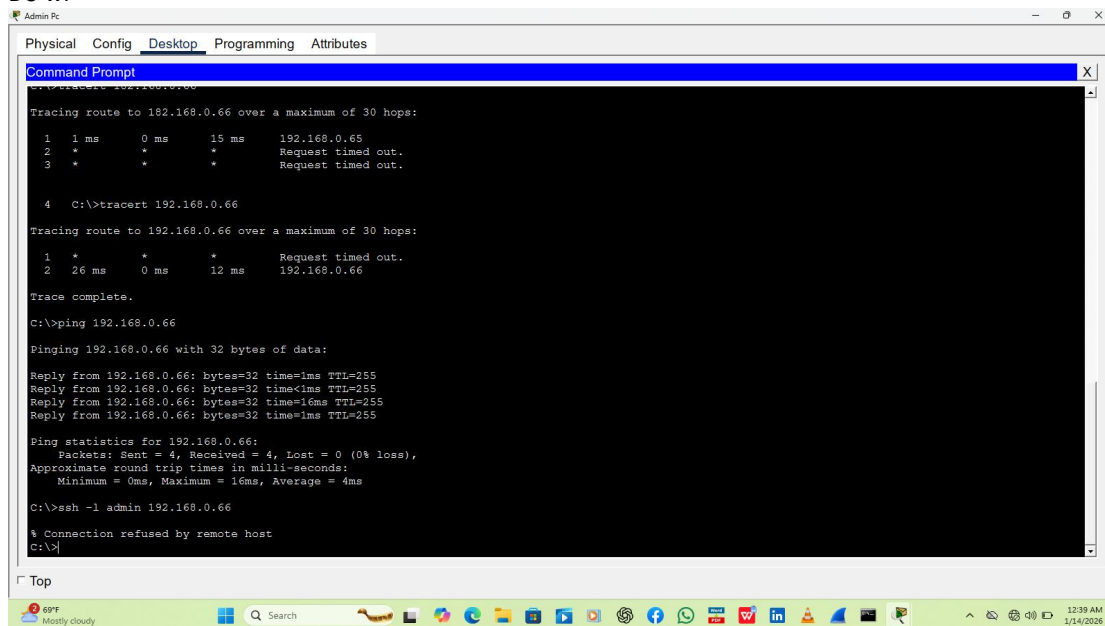


We can see that we have unwanted vlan which is vlan 2 let us remove vlan 2

No vlan 2

Ex

Do wr



```
Admin PC
Physical Config Desktop Programming Attributes
Command Prompt
C:\Users\Administrator>tracert 192.168.0.66
Tracing route to 192.168.0.66 over a maximum of 30 hops:
  0  1 ms    0 ms    15 ms   192.168.0.65
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.

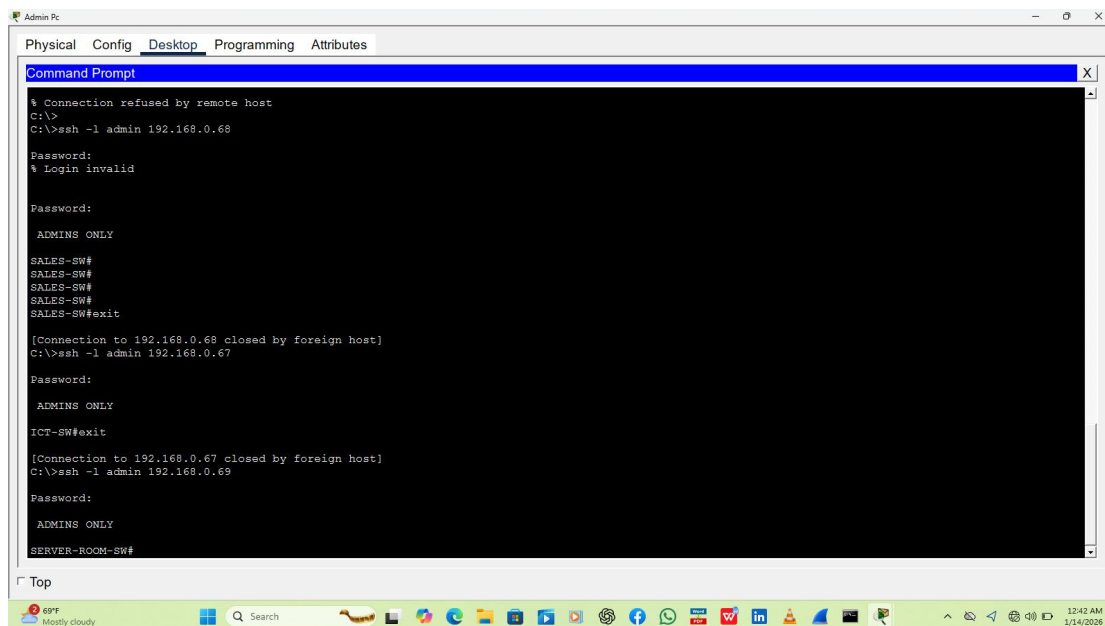
  4  C:\>tracert 192.168.0.66
Tracing route to 192.168.0.66 over a maximum of 30 hops:
  0  *      *      *      Request timed out.
  1  26 ms   0 ms    12 ms   192.168.0.66
Trace complete.

C:\>ping 192.168.0.66
Pinging 192.168.0.66 with 32 bytes of data:
Reply from 192.168.0.66: bytes=32 time=1ms TTL=255
Reply from 192.168.0.66: bytes=32 time<1ms TTL=255
Reply from 192.168.0.66: bytes=32 time=16ms TTL=255
Reply from 192.168.0.66: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.0.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>ssh -l admin 192.168.0.66
% Connection refused by remote host
C:\>
```

We still get an error, let us try to ssh other switches



```
Admin PC
Physical Config Desktop Programming Attributes
Command Prompt
% Connection refused by remote host
C:\>
C:\>ssh -l admin 192.168.0.68
Password:
% Login invalid

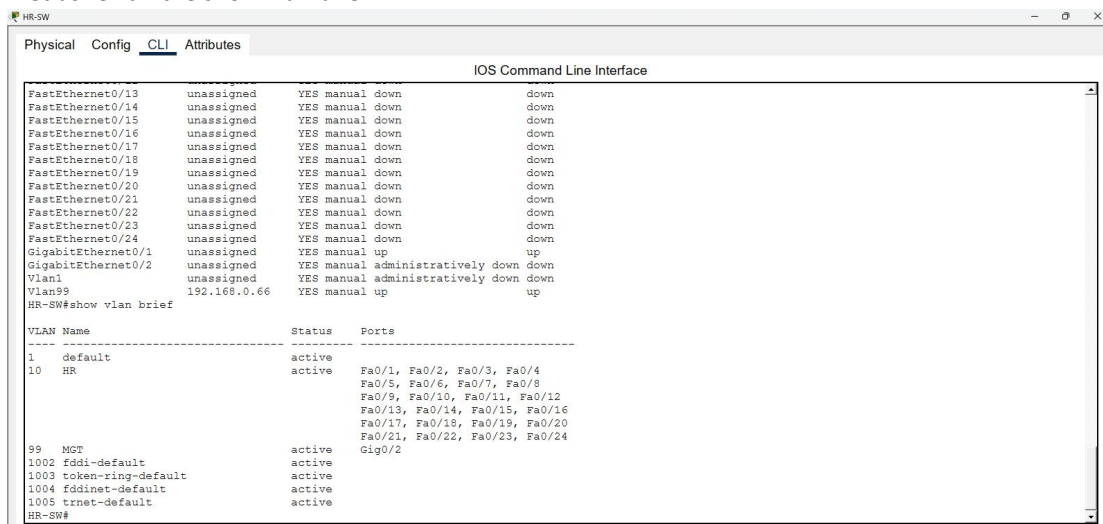
Password:
ADMIN'S ONLY
SALES-SW#
SALES-SW#
SALES-SW#
SALES-SW#
SALES-SW#exit

[Connection to 192.168.0.68 closed by foreign host]
C:\>ssh -l admin 192.168.0.67
Password:
ADMIN'S ONLY
ICT-SW#exit

[Connection to 192.168.0.67 closed by foreign host]
C:\>ssh -l admin 192.168.0.65
Password:
ADMIN'S ONLY
SERVER-ROOM-SW#
```

We are able to ssh other switches, let us continue to troubleshoot.

Let us re-run the show vlan brief



```
HR-SW
Physical Config CLI Attributes
IOS Command Line Interface
FastEthernet0/13 unassigned YES manual down down
FastEthernet0/14 unassigned YES manual down down
FastEthernet0/15 unassigned YES manual down down
FastEthernet0/16 unassigned YES manual down down
FastEthernet0/17 unassigned YES manual down down
FastEthernet0/18 unassigned YES manual down down
FastEthernet0/19 unassigned YES manual down down
FastEthernet0/20 unassigned YES manual down down
FastEthernet0/21 unassigned YES manual down down
FastEthernet0/22 unassigned YES manual down down
FastEthernet0/23 unassigned YES manual down down
FastEthernet0/24 unassigned YES manual up up
GigabitEthernet0/1 unassigned YES manual administratively down down
GigabitEthernet0/2 unassigned YES manual administratively down down
Vlan1 unassigned YES manual administratively down down
Vlan99 192.168.0.66 YES manual up up
HR-SW#show vlan brief

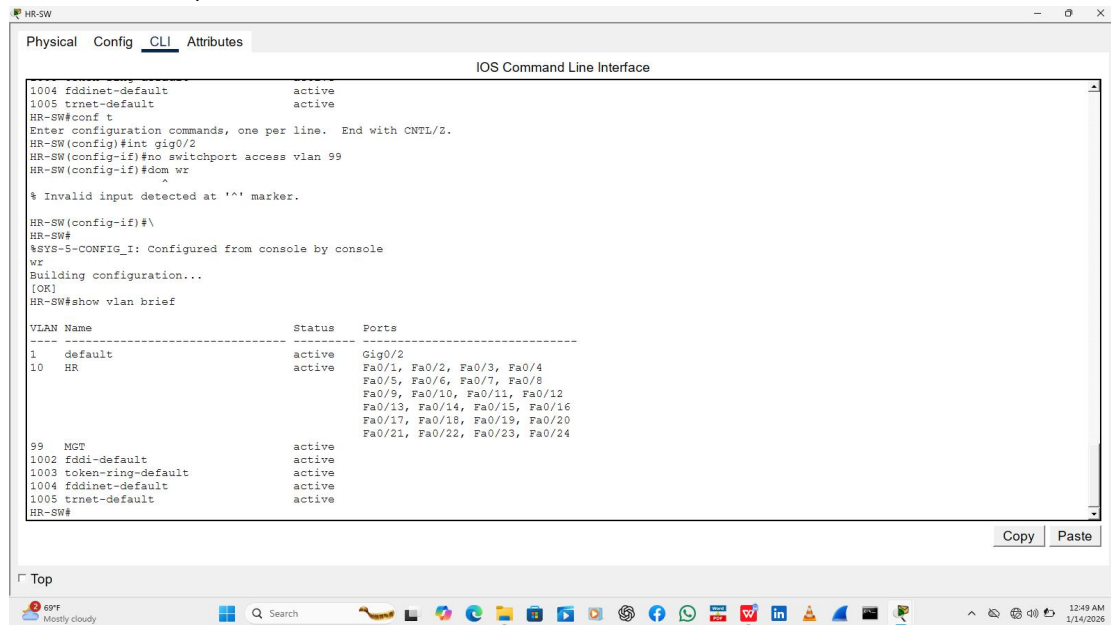
VLAN Name                Status    Ports
-----
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
10   HR                    active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14,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

If we look very closer we can see that vlan 99 is assigned to interface e gig0/2 which is not connected to anything, let us remove that.

Int gig0/2

No switchport access vlan 99

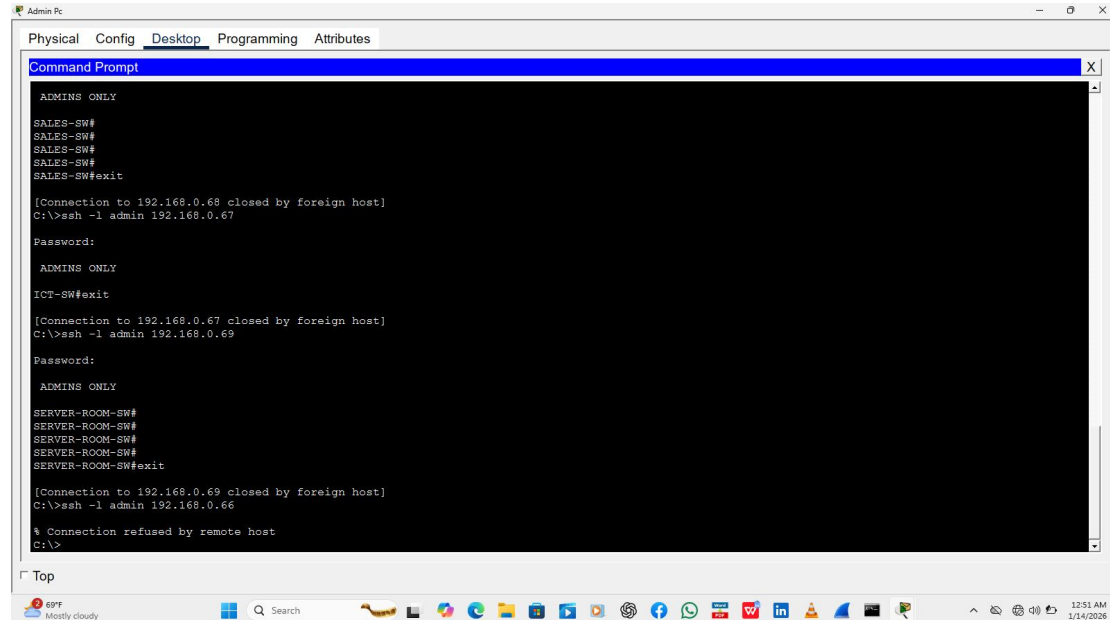
Let us see the output from the show vlan brief



The screenshot shows the HR-SW CLI interface. The user has entered the command `show vlan brief`, and the output is displayed as follows:

VLAN	Name	Status	Ports
1	default	active	Gig0/2
10	HR	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, 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
99	MGT	active	
1002	fdi-default	active	
1003	token-ring-default	active	
1004	fdinet-default	active	
1005	trinet-default	active	

that's what we wanted, let us try to ssh hr switch



The screenshot shows the Admin PC Command Prompt. The user has attempted to SSH into the HR-SW switch using the command `ssh -l admin 192.168.0.67`. The output shows that the connection was refused by the remote host.

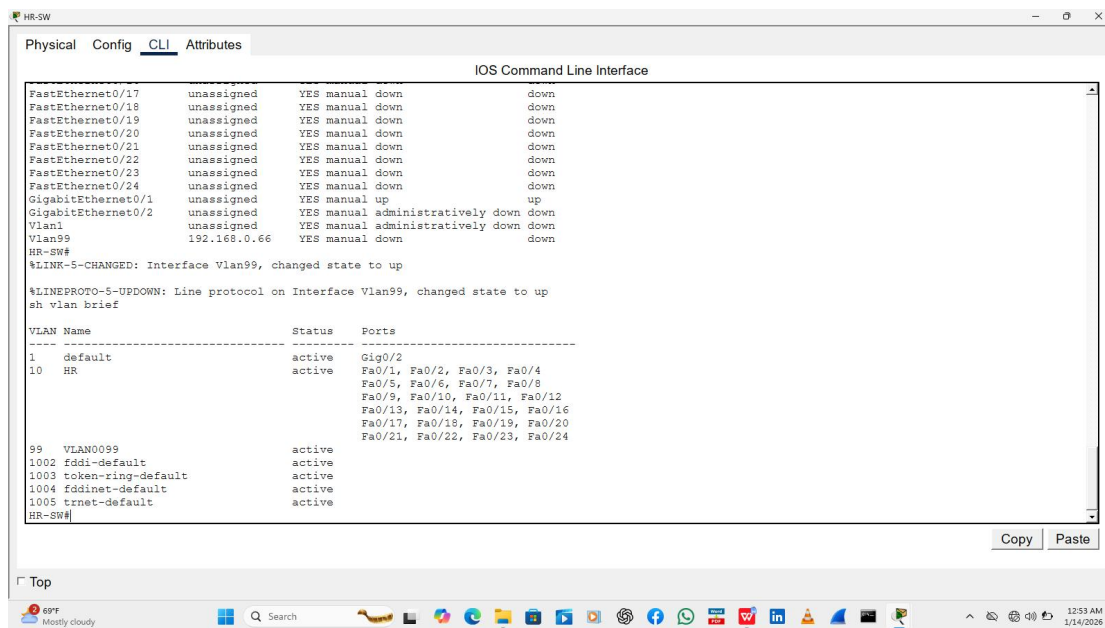
```
ADMIN ONLY
SALES-SW#
SALES-SW#
SALES-SW#
SALES-SW#exit
[Connection to 192.168.0.68 closed by foreign host]
C:\>ssh -l admin 192.168.0.67
Password:
ADMIN ONLY
ICT-SW#exit
[Connection to 192.168.0.67 closed by foreign host]
C:\>ssh -l admin 192.168.0.69
Password:
ADMIN ONLY
SERVER-ROOM-SW#
SERVER-ROOM-SW#
SERVER-ROOM-SW#
SERVER-ROOM-SW#exit
[Connection to 192.168.0.69 closed by foreign host]
C:\>ssh -l admin 192.168.0.66
* Connection refused by remote host
C:\>
```

We still unable to ssh it, let us remove the vlan configuration and svi

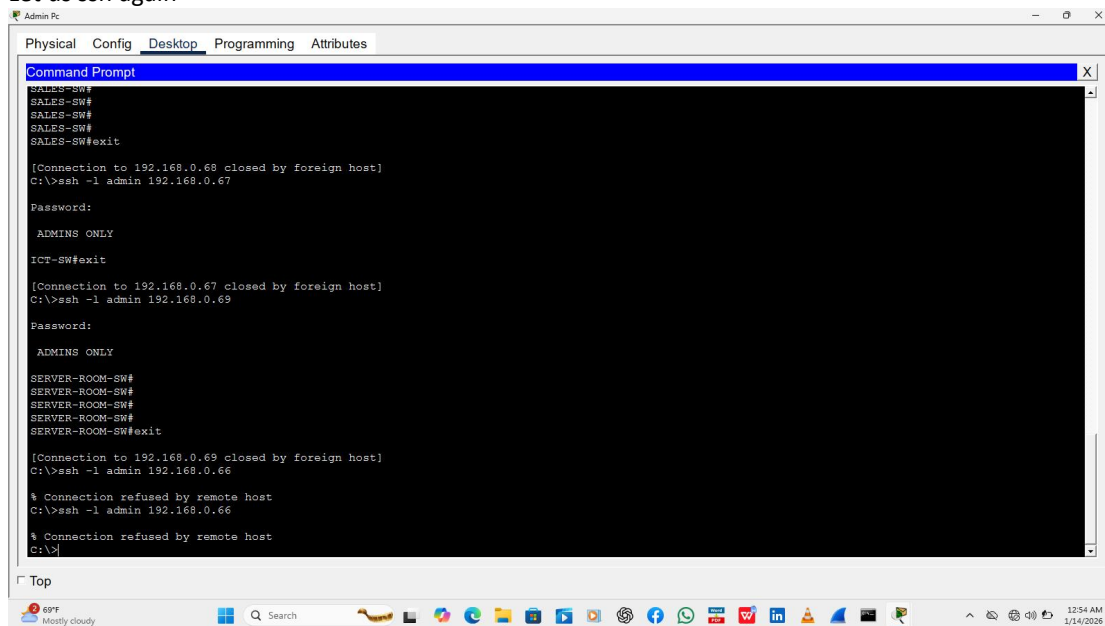
No vlan 99

Ex

No int vlan 99

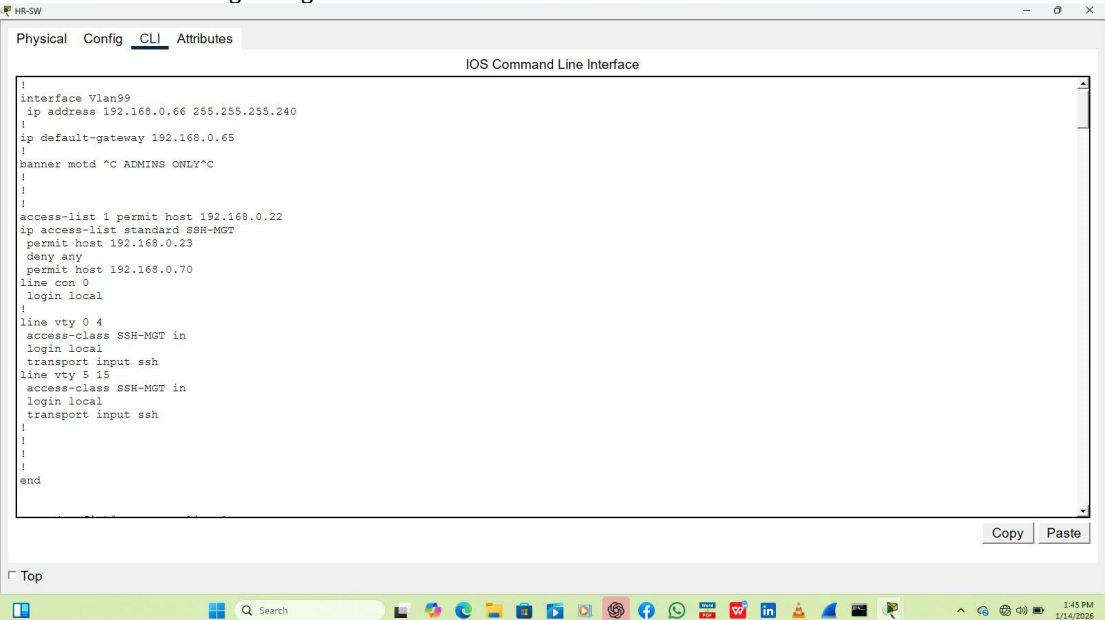


Let us ssh again



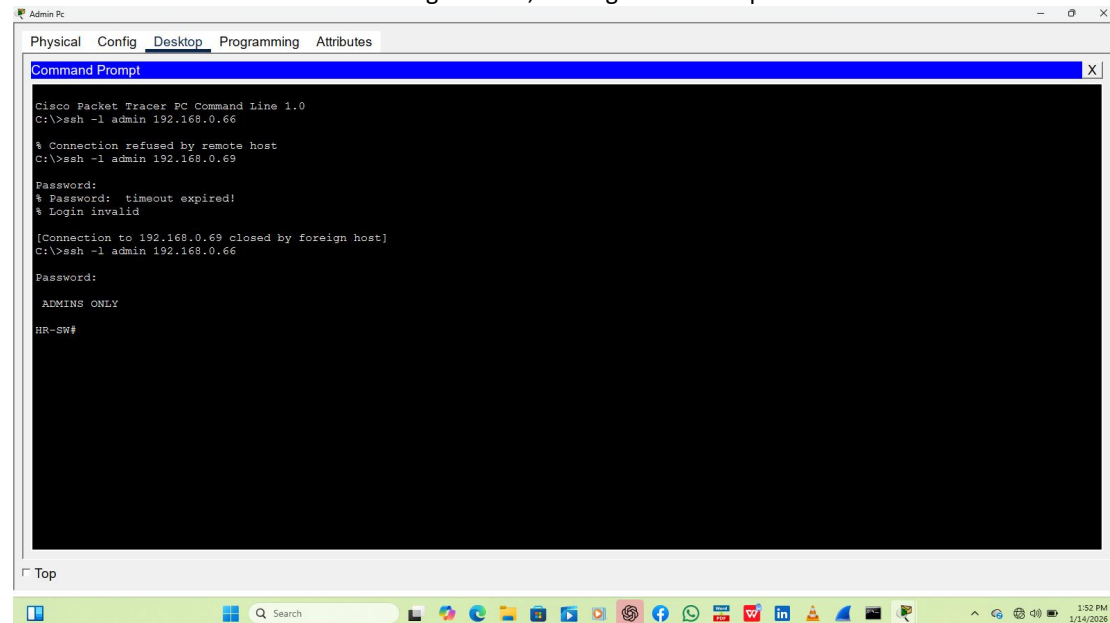
Still unable to ssh, let us check the SVI

Let check the running configurations



We can see that there were three access list, one permitting 192.168.0.22, 192.168.0.23 and 192.168.0.70 that's where the problem is, let us remove the unwanted access list as we only want 192.168.0.70

Now that we have done the new configurations, let us go on Admin pc and ssh 192.168.0.66

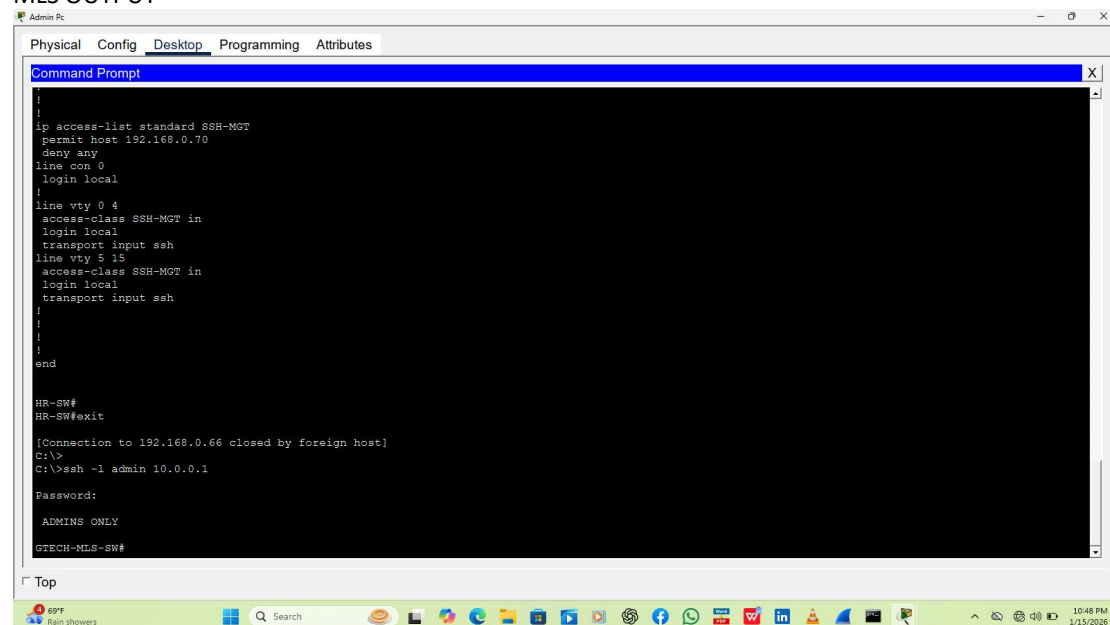


```
Admin PC
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.0.66
% Connection refused by remote host
C:\>ssh -l admin 192.168.0.69
Password:
% Password: timeout expired!
% Login invalid
[Connection to 192.168.0.69 closed by foreign host]
C:\>ssh -l admin 192.168.0.66
Password:
ADMINS ONLY
HR-SW#
```

There we go , finally. What was the main reason? SSH access to HR switch initially failed due to multiple access-list permit statements applied to the VTY line. Although the Admin PC was permitted, the overlapping ACL entries caused unexpected behaviour. Re-configuring the ACL to permit only the Admin PC resolved the issue. We aren't completely done, we didn't test admin PC to the MLS and to the edge router, so let us try it.

On admin PC - ssh -l admin 10.0.0.1 (for MLS) and 10.0.0.2 (for edge router)

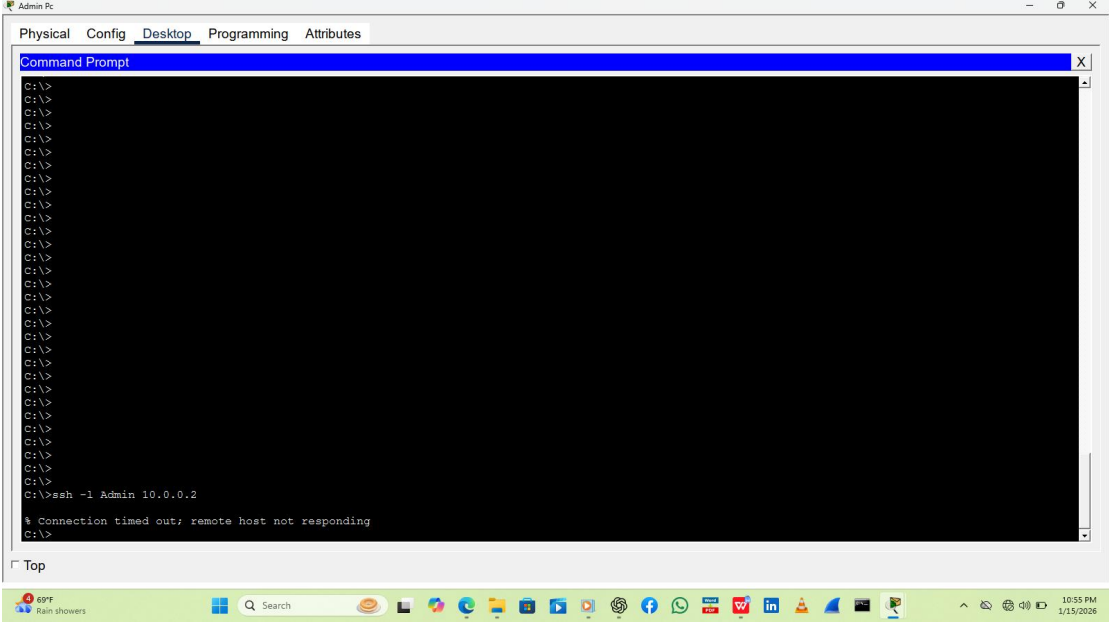
MLS OUTPUT



```
Admin PC
Physical Config Desktop Programming Attributes
Command Prompt
ip access-list standard SSH-MGT
 permit host 192.168.0.70
 deny any
line con 0
 login local
!
line vty 0 4
 access-class SSH-MGT in
 login local
 transport input ssh
line vty 5 15
 access-class SSH-MGT in
 login local
 transport input ssh
!
!
!
end
HR-SW#
HR-SW#exit
[Connection to 192.168.0.66 closed by foreign host]
C:\>
C:\>ssh -l admin 10.0.0.1
Password:
ADMINS ONLY
GTECH-MLS-SW#
```

Let us check to our edge router

EDGE ROUTER OUTPUT

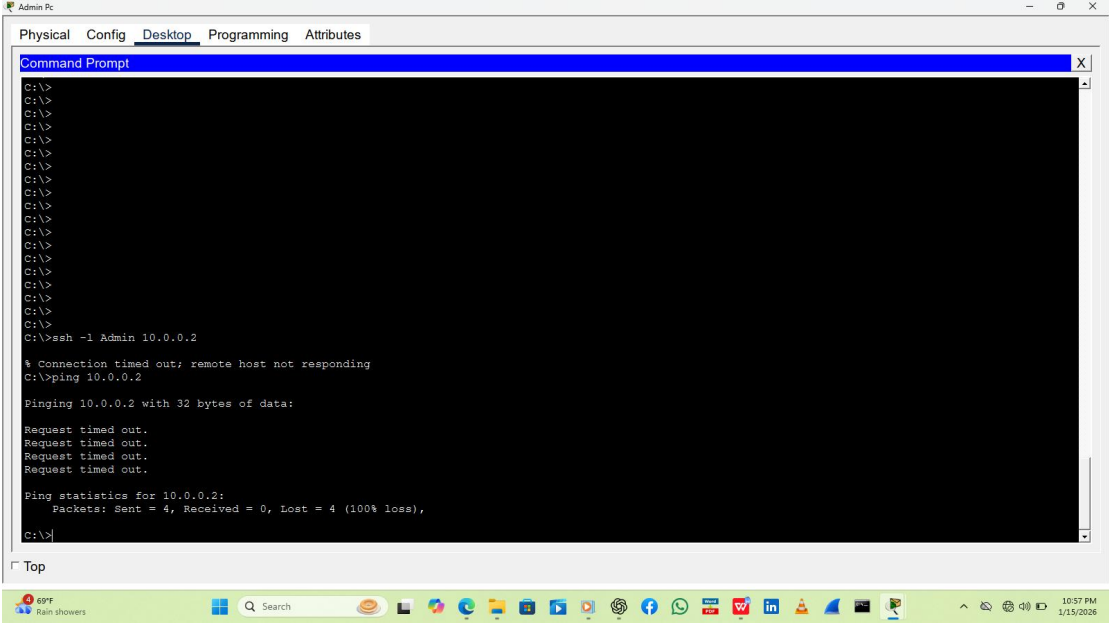


The screenshot shows a Windows desktop environment with a taskbar at the bottom. A 'Command Prompt' window is open, displaying the following text:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ssh -l Admin 10.0.0.2
% Connection timed out; remote host not responding
C:\>
```

The window title bar indicates it is an 'Admin Pc' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The taskbar shows various application icons and a system tray with the date '1/15/2026' and time '10:55 PM'.

We unable to SSH the edge router, let us try to ping first,



The screenshot shows the same Windows desktop environment as the previous one. The 'Command Prompt' window now displays the following text:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ssh -l Admin 10.0.0.2
% Connection timed out; remote host not responding
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

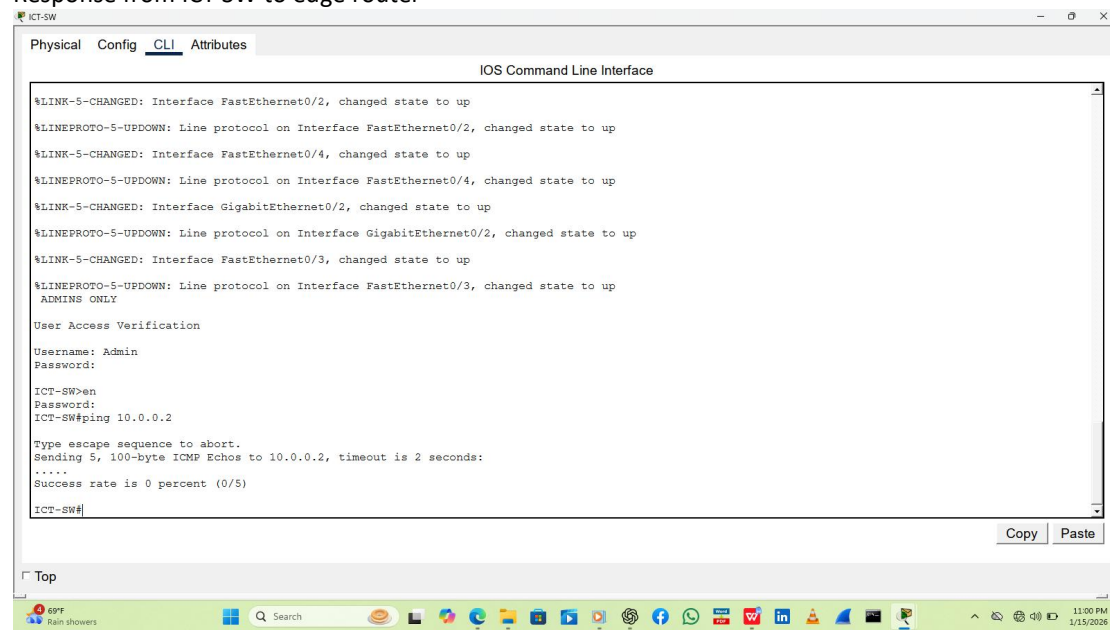
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

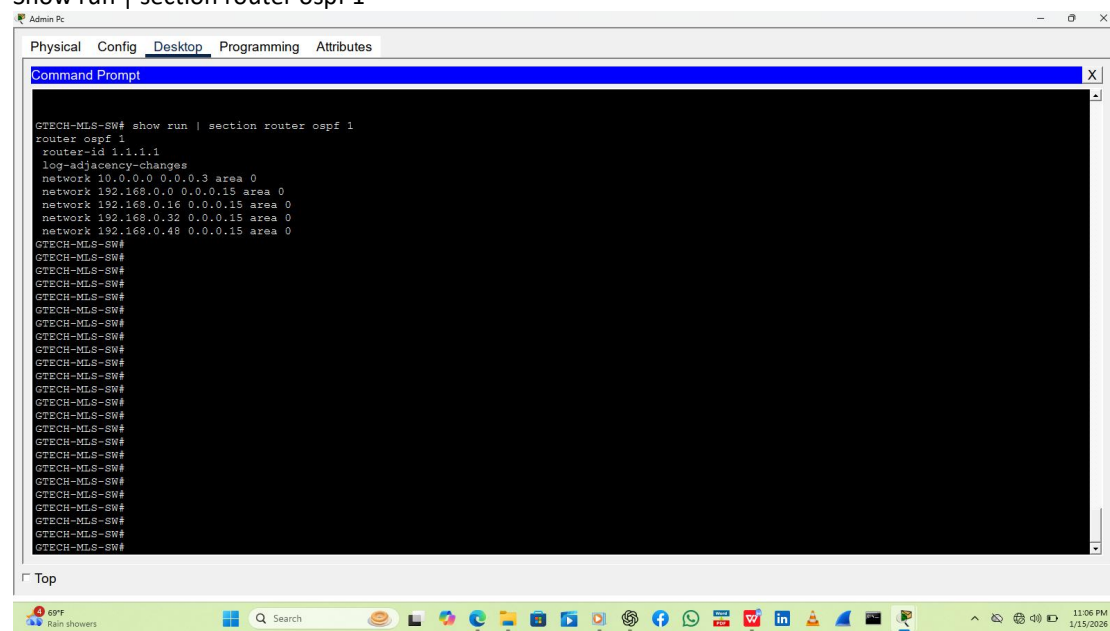
The window title bar and taskbar are identical to the previous screenshot, showing the same desktop environment and system information.

We can't even ping that must tell us the story, before we continue, we have to try to ping from any access switch to see if there is connectivity

Response from ICT SW to edge router

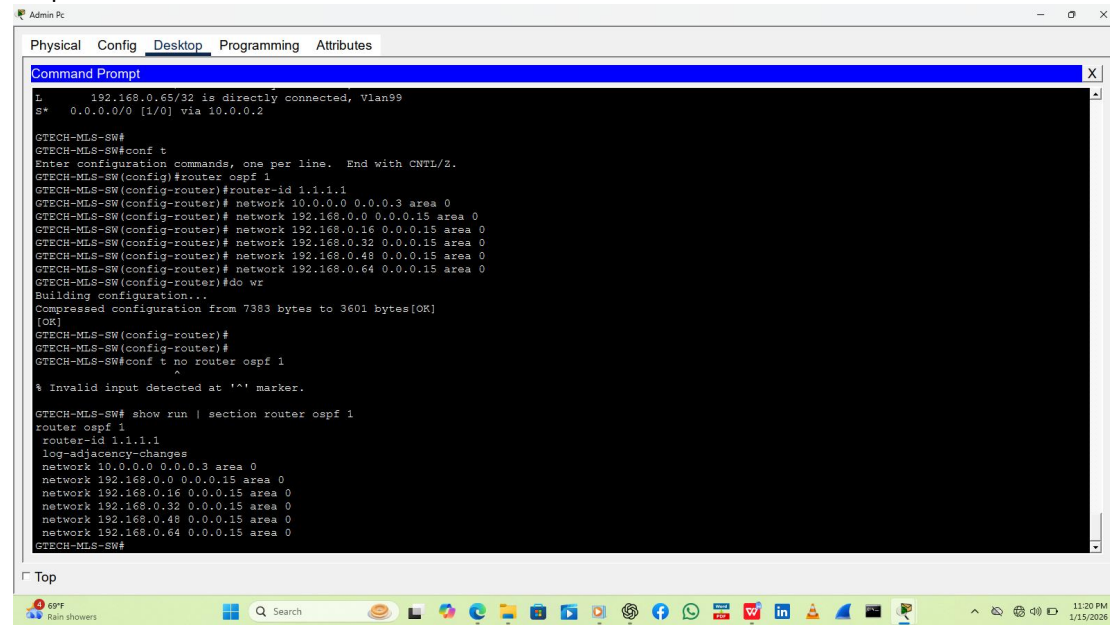


Let us start troubleshooting, first we check the routing protocol on the MLS
Show run | section router ospf 1



We can see that subnet 192.168.0.64/28 isn't advertised, better still we can still do a show ip route. Am on Admin PC since it can ssh the MLS no need of going to the device. Let us advertise it and check again with the Show run | section router ospf 1

Response



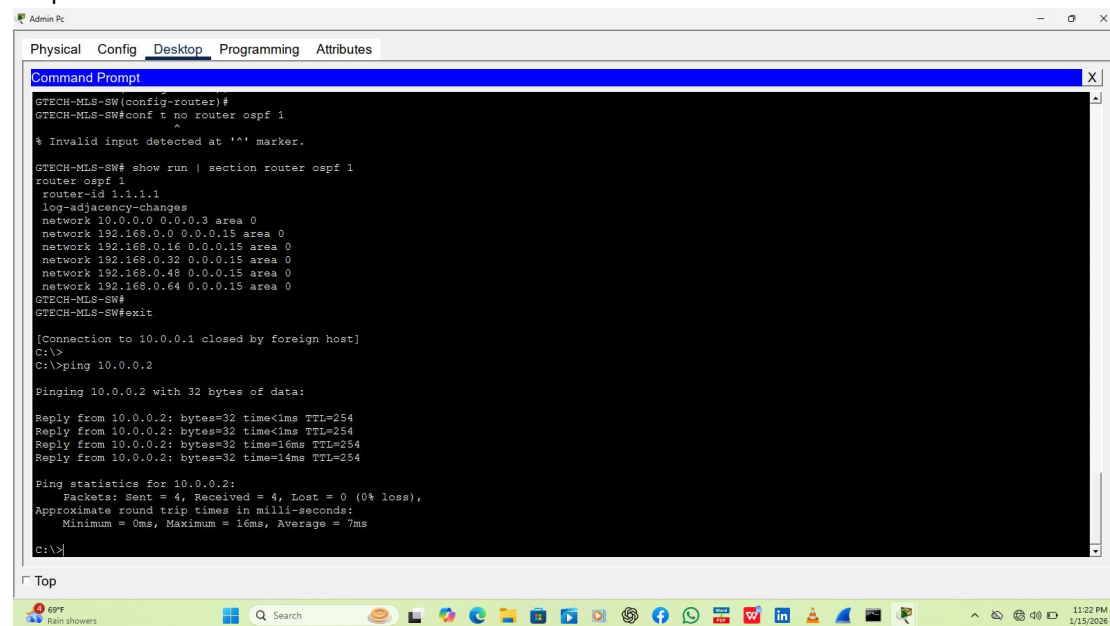
```
1 192.168.0.65/32 is directly connected, Vlan99
S* 0.0.0.0/0 [1/0] via 10.0.0.2

GTECH-MLS-SW#
GTECH-MLS-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
GTECH-MLS-SW(config)#router ospf 1
GTECH-MLS-SW(config-router)#router-id 1.1.1.1
GTECH-MLS-SW(config-router)# network 10.0.0.0 0.0.0.3 area 0
GTECH-MLS-SW(config-router)# network 192.168.0.0 0.0.0.15 area 0
GTECH-MLS-SW(config-router)# network 192.168.0.16 0.0.0.15 area 0
GTECH-MLS-SW(config-router)# network 192.168.0.32 0.0.0.15 area 0
GTECH-MLS-SW(config-router)# network 192.168.0.48 0.0.0.15 area 0
GTECH-MLS-SW(config-router)# network 192.168.0.64 0.0.0.15 area 0
GTECH-MLS-SW(config-router)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
GTECH-MLS-SW(config-router)#
GTECH-MLS-SW(config-router)#
GTECH-MLS-SW#conf t no router ospf 1
^
% Invalid input detected at '^' marker.

GTECH-MLS-SW# show run | section router ospf 1
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 10.0.0.0 0.0.0.3 area 0
network 192.168.0.0 0.0.0.15 area 0
network 192.168.0.16 0.0.0.15 area 0
network 192.168.0.32 0.0.0.15 area 0
network 192.168.0.48 0.0.0.15 area 0
network 192.168.0.64 0.0.0.15 area 0
GTECH-MLS-SW#
```

Let us try to ping the edge router again from the admin PC

Response



```
GTECH-MLS-SW(config-router)#
GTECH-MLS-SW#conf t no router ospf 1
^
% Invalid input detected at '^' marker.

GTECH-MLS-SW# show run | section router ospf 1
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 10.0.0.0 0.0.0.3 area 0
network 192.168.0.0 0.0.0.15 area 0
network 192.168.0.16 0.0.0.15 area 0
network 192.168.0.32 0.0.0.15 area 0
network 192.168.0.48 0.0.0.15 area 0
network 192.168.0.64 0.0.0.15 area 0
GTECH-MLS-SW#
GTECH-MLS-SW#exit

[Connection to 10.0.0.1 closed by foreign host]
C:\>
C:\>ping 10.0.0.2

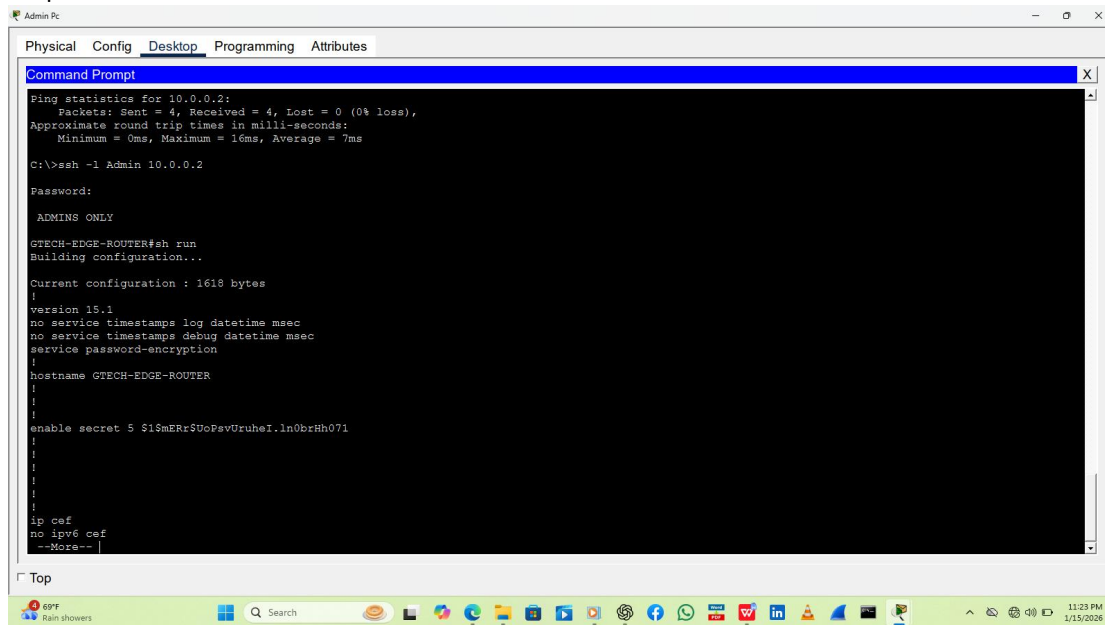
Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time=16ms TTL=254
Reply from 10.0.0.2: bytes=32 time=14ms TTL=254

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 7ms
C:\>
```

Ping is now successful, let us try ssh. We should be able to ssh the edge router now, let us try now

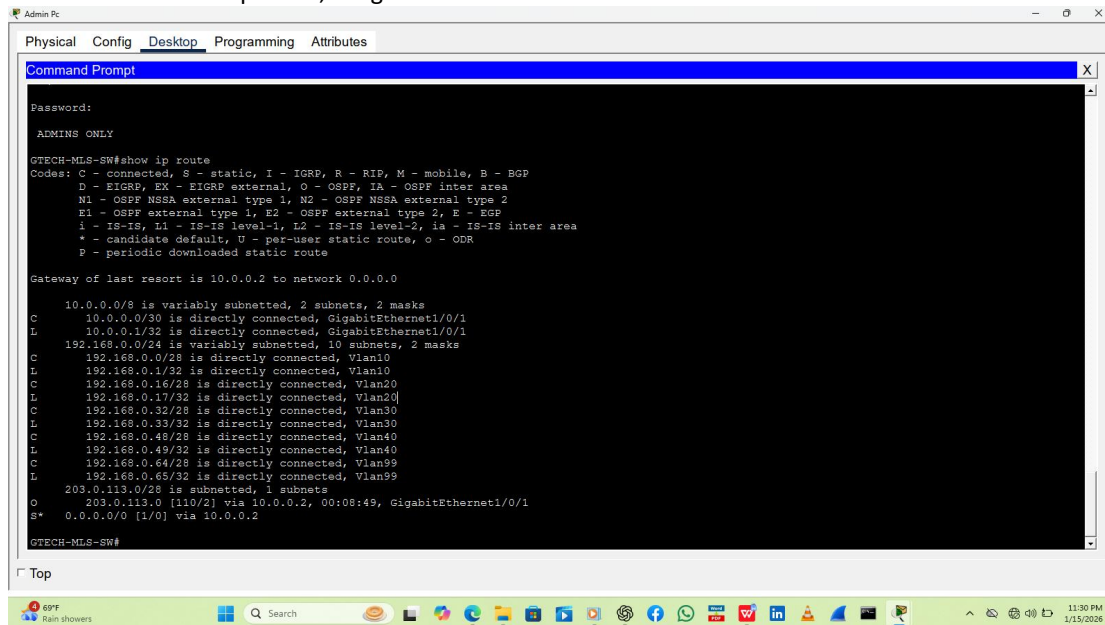
Response



We are in the edge router now. All our configurations are working perfect. The management subnet (192.168.0.64/28) did not appear as an OSPF route on the MLS because it is directly connected and therefore installed as a connected route. However, it was initially reachable from the edge router because it was not advertised into OSPF. Once the subnet was included in the OSPF process, full connectivity and SSH access to the edge router were achieved

Why we were unable to ssh the edge router? We were unable to ssh the edge router because there was no connectivity between the Subnet where the admin PC belong to (192.168.0.64) this was connected directly but was not being advertised by the MLS the fix was to advertise it.

When we do a show ip route, we get this



Why didn't our subnet made it into the OSPF routes? The subnets did not appear as OSPF routes because they are directly connected to the MLS and are installed as connected routes; only remote subnets learned from OSPF neighbors appear in the routing table as OSPF routes. Only remote subnets learned from OSPF neighbors appear in the routing table as OSPF route.