SMALL NETWORK EXPANDED-SSH

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

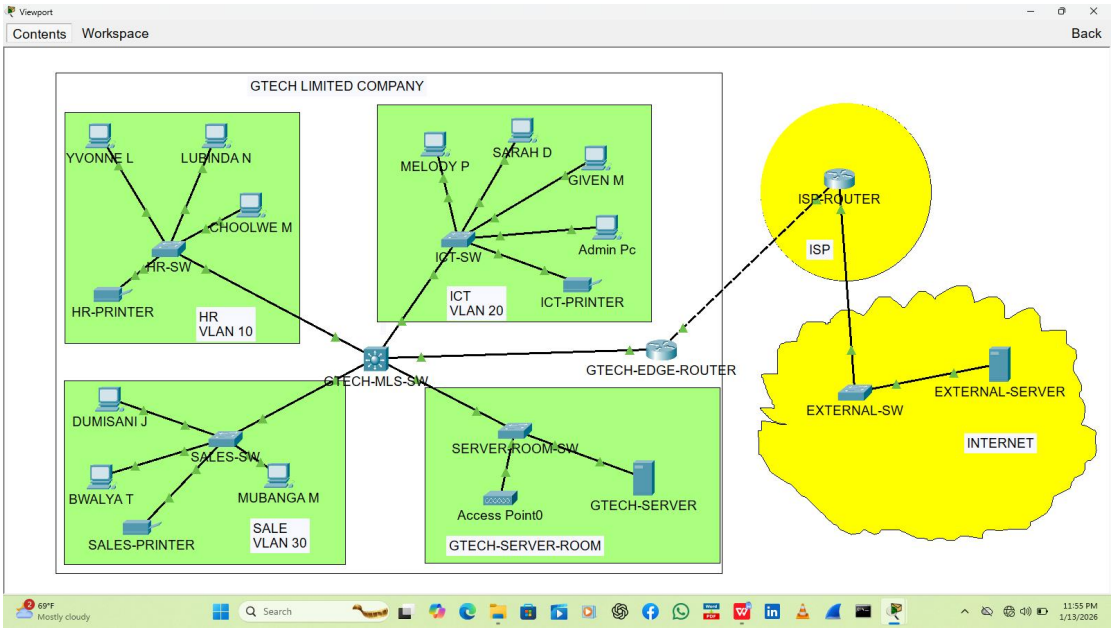
Remote secure access refers to managing network devices from a different location using encrypted management protocol.there are two methods to do this, thus telnet and ssh, telnet is not secure so we will use ssh. There are couple of things to consider this include;

- 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 changes 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

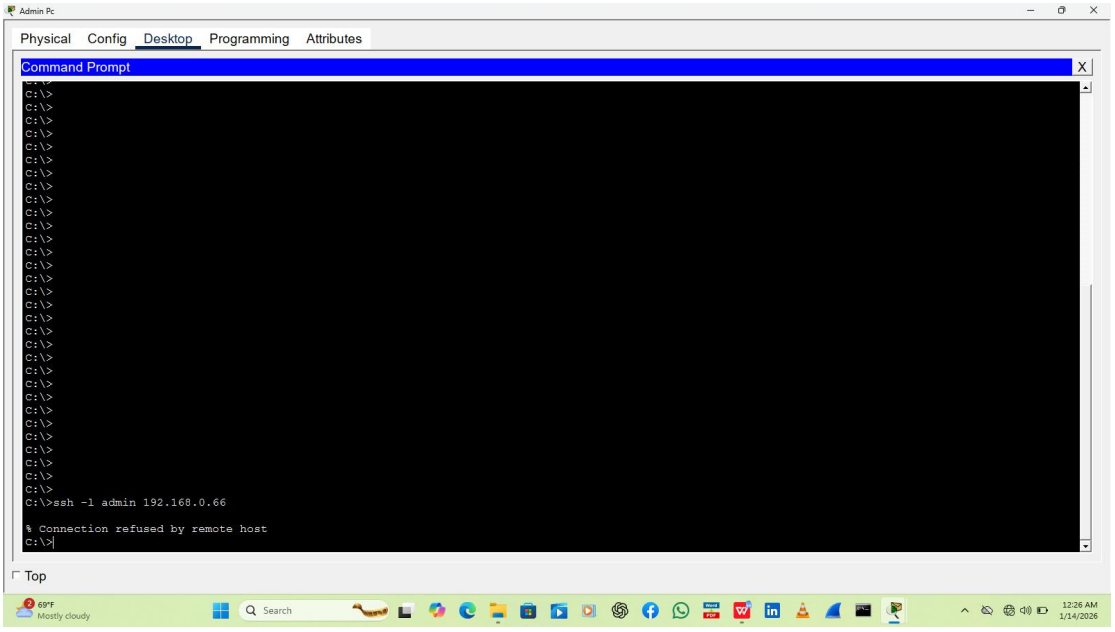
transport input ssh

access-class SSH-MGT in

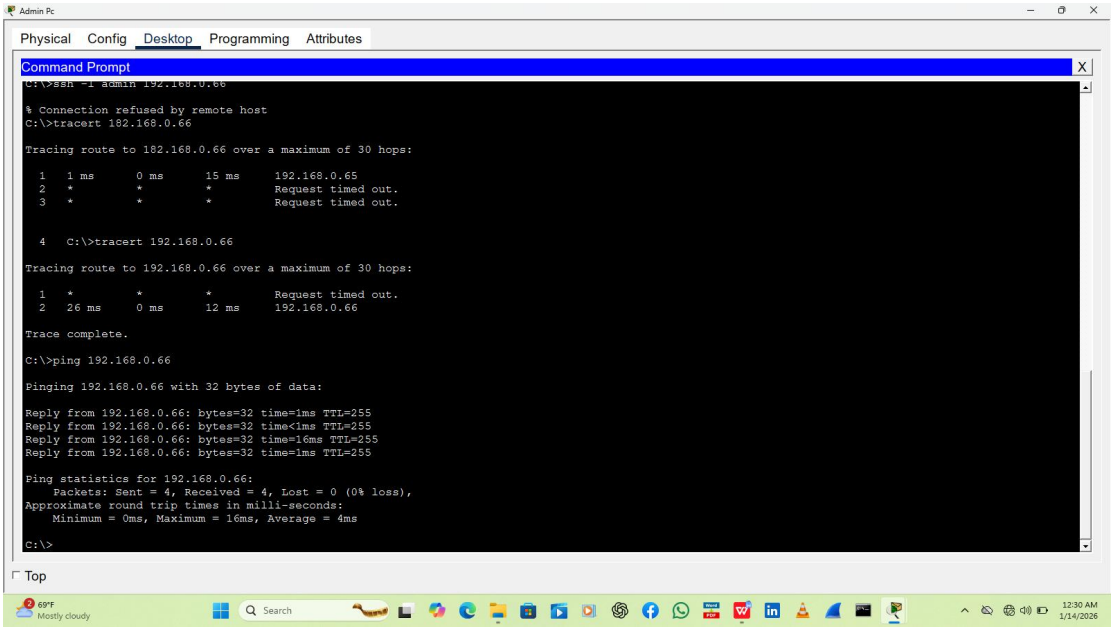
Exit

Now let us configure our management vlans on all switches

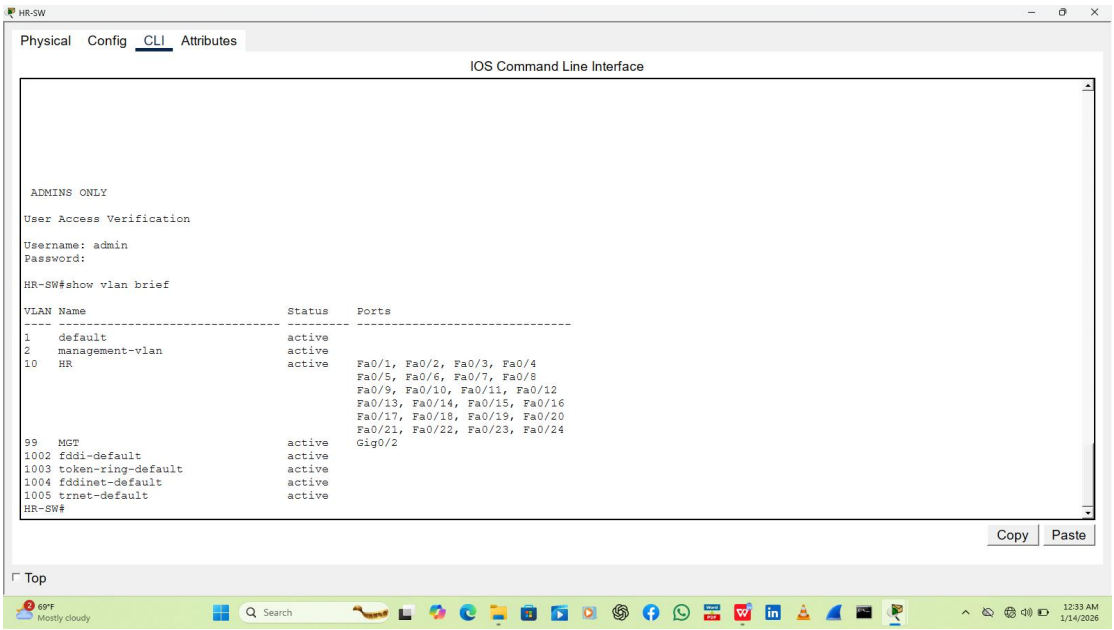
HR,ICT,SALES, MLS and SERVER ROOM SW.
Vlan 99
Name MGT
Ex
Next we configure switch virtual interface on the MLS
Int vlan 99
No shut
Ip add 192.168.0.65 255.255.255.240
Do wr
Ex
Let us now configure SVI for management vlan and gateway on all switches, we should keep in mind that the manager is in ICT 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



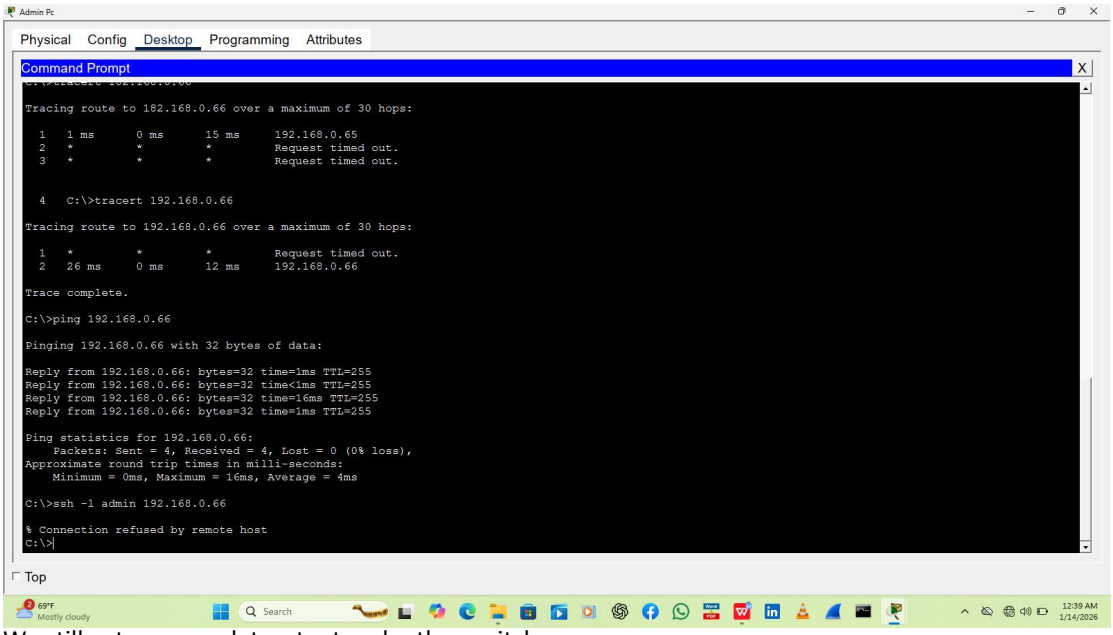
We landed straight into an error, whats wrong here?let us troubleshoot



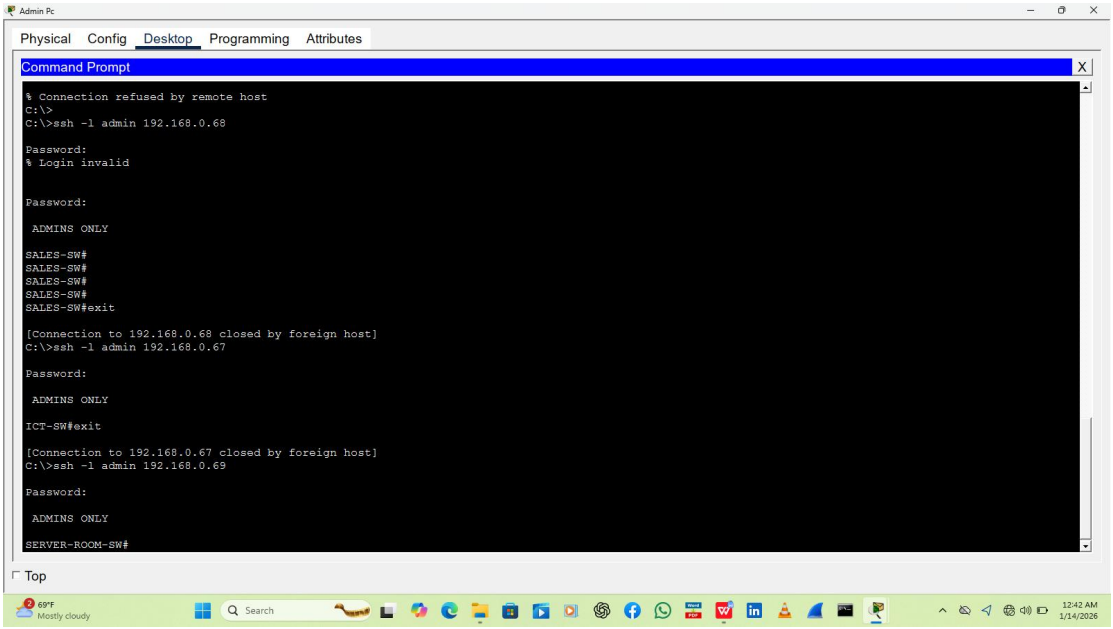
Ping is working, so this isn't connection issue,what does that mean? It means the problem we have is a layer 2 problem, let us go to HR sw and check the existing vlans
Show vlan brief



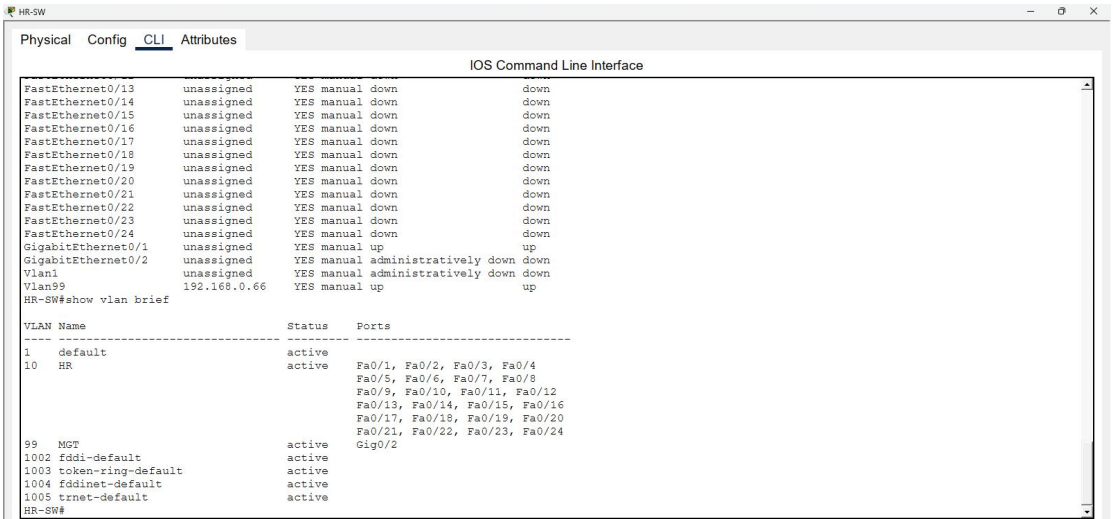
We can see that we have unwanted vlan which is vlan 2 let us remove vlan 2
No vlan 2
Ex
Do wr



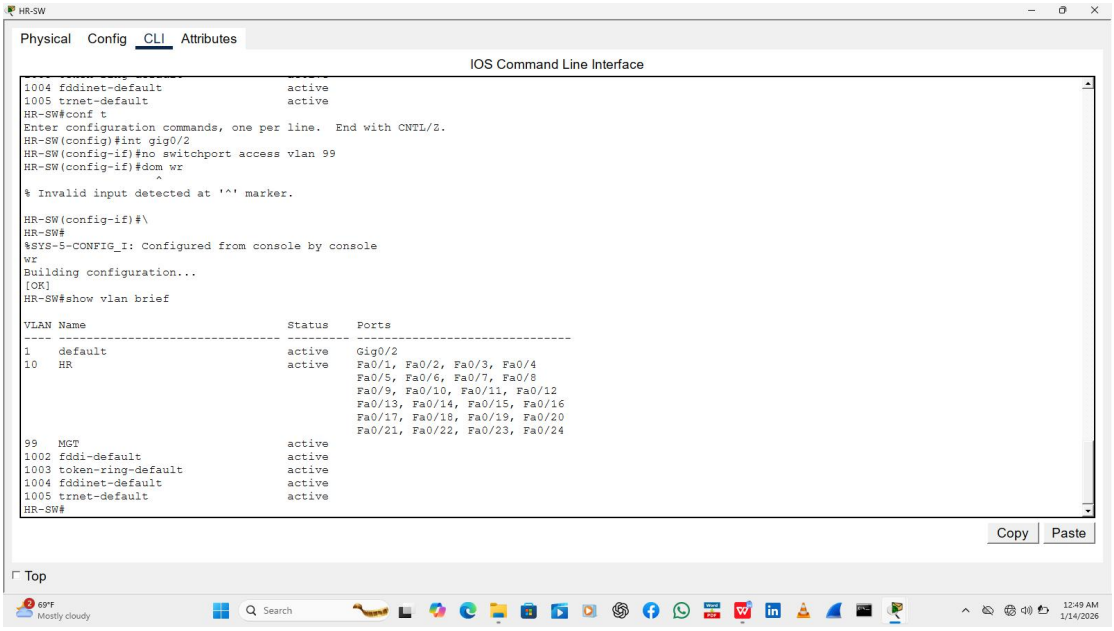
We still get an error, let us try to ssh other switches



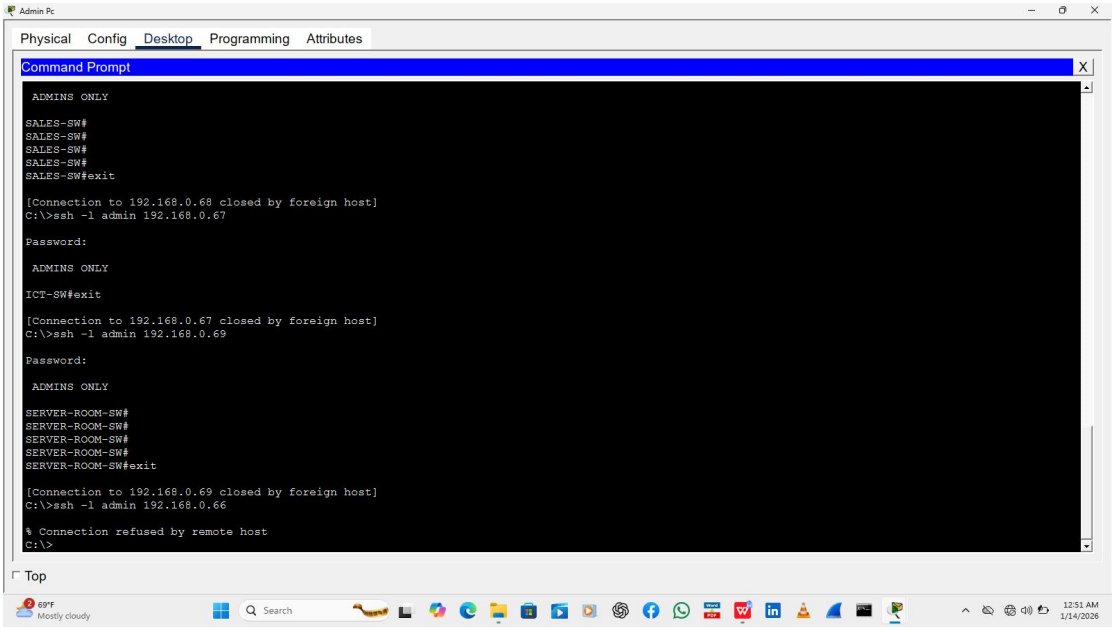
We are able to ssh other switches,let us continue to troubleshoot.
Let us re-run the show vlan brief



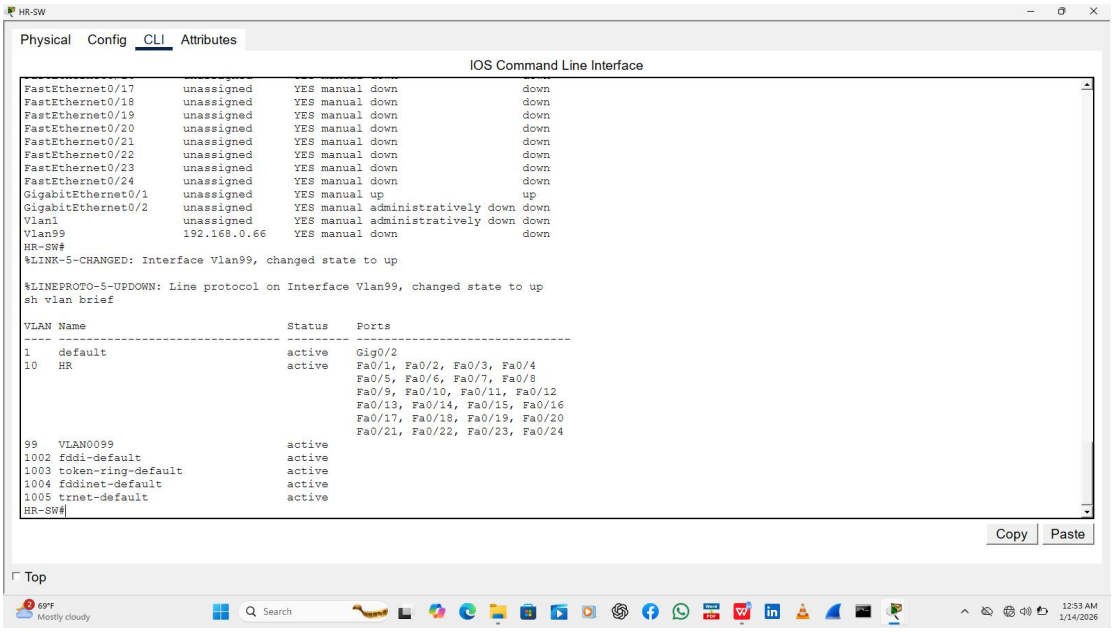
If we look very closer we can see that vlan 99 is assigned to interface e gig0/2 which is not connected to anything, let us remove that.
Int gig0/2
No switchport access vlan 99
Let us see the output from the show vlan brief



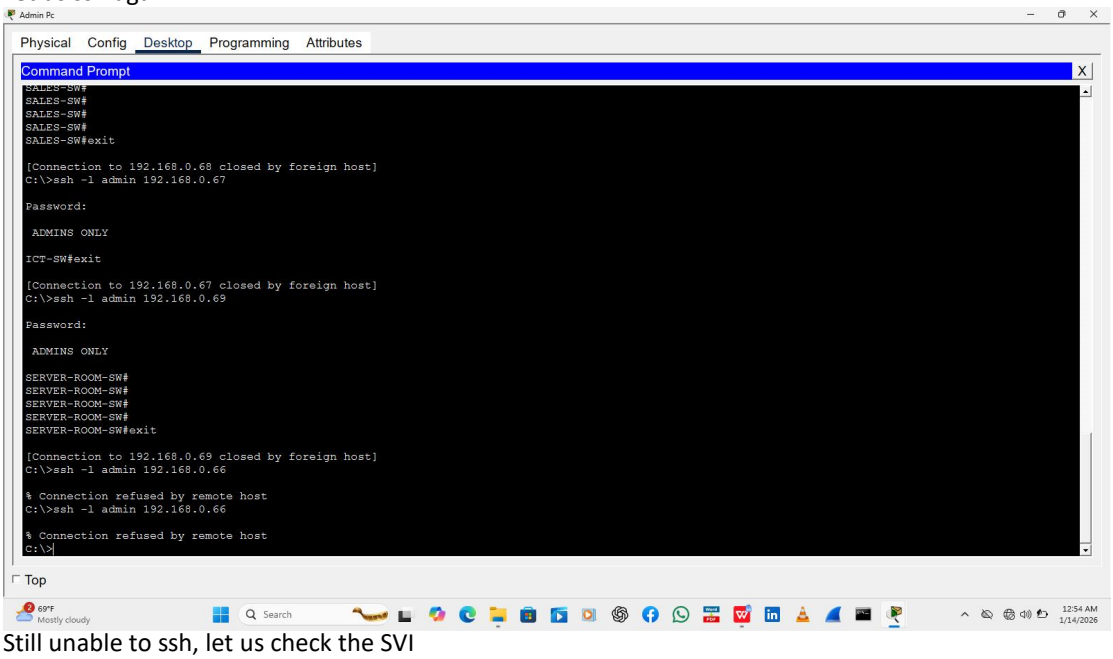
that's what we wanted, let us try to ssh hr switch



We still unable to ssh it, let us remove the vlan configuration and svi
No vlan 99
Ex
No int vlan 99

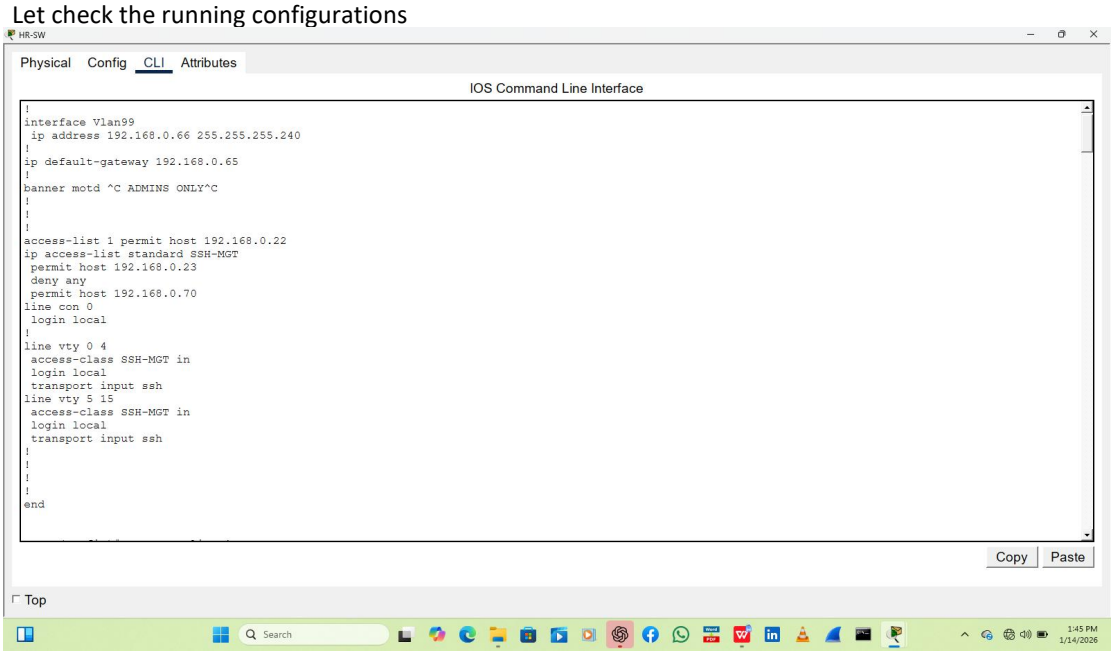


Let us ssh again



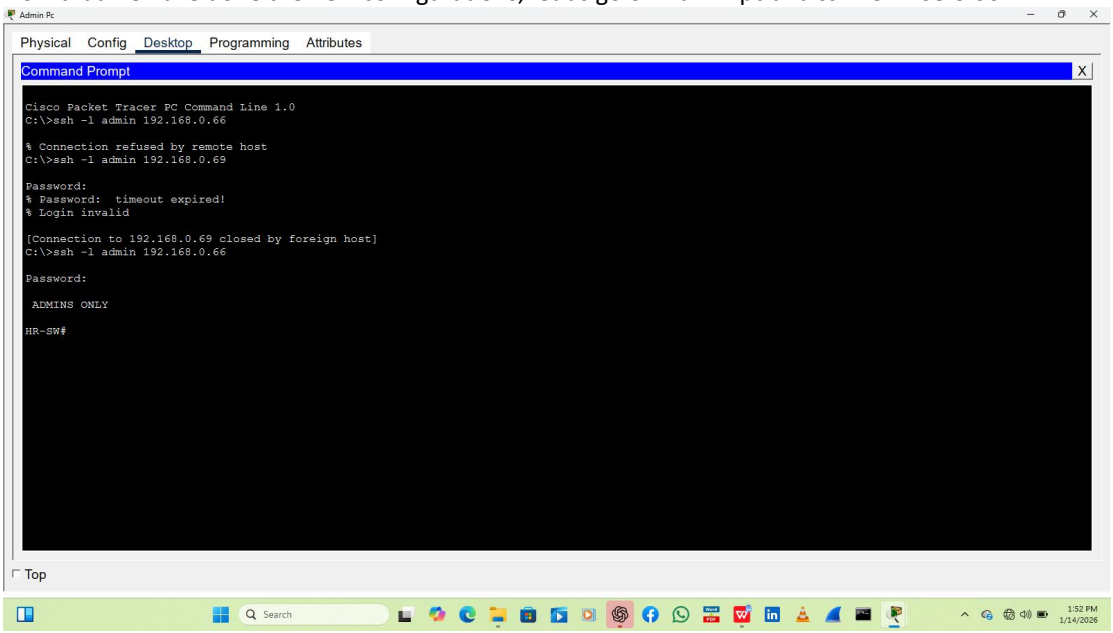
Still unable to ssh, let us check the SVI

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 us we only want 192.168.0.70

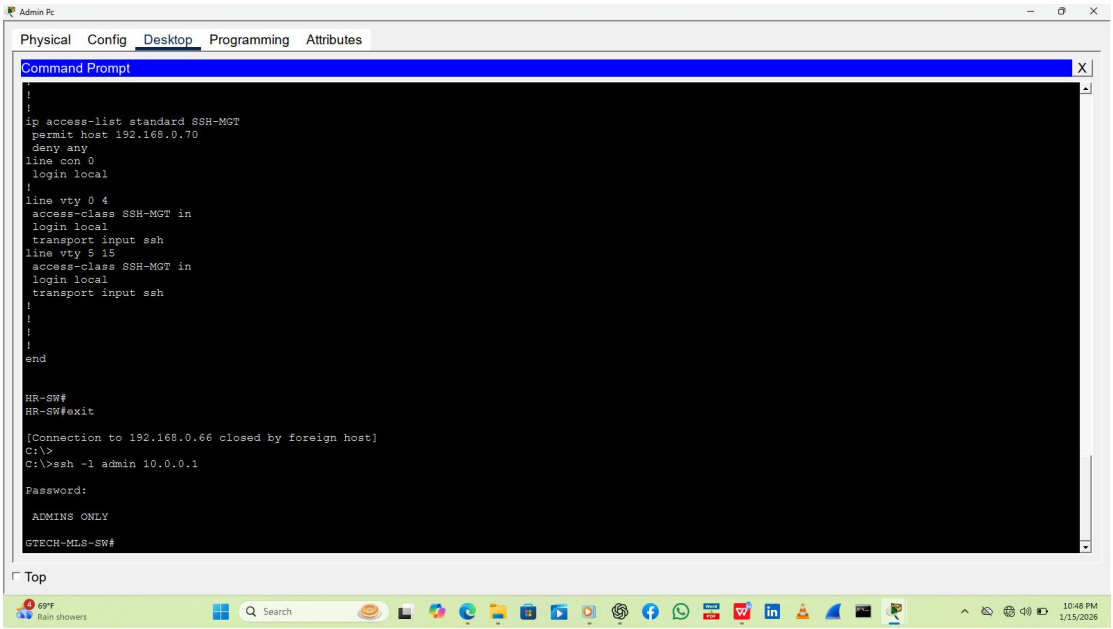
Now that we have done the new configurations, let us go on Admin pc and ssh 192.168.0.66



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.

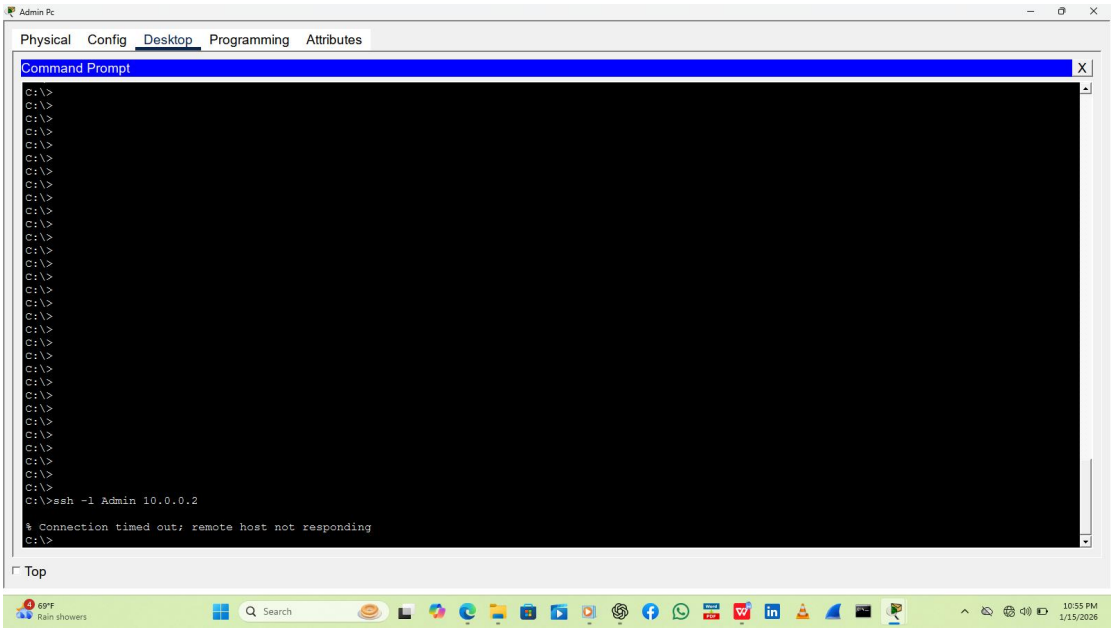
On admin PC - ssh -l admin 10.0.0.1 (for MLS) and 10.0.0.2 (for edge router)

MLS OUTPUT

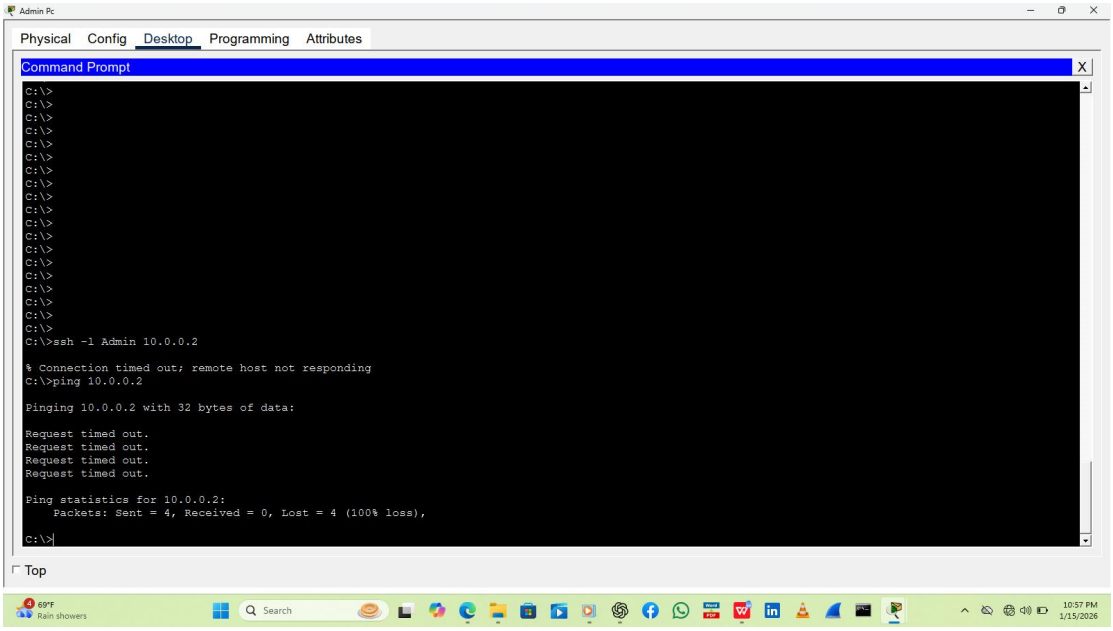


Let us check to our edge router

EDGE ROUTER OUTPUT

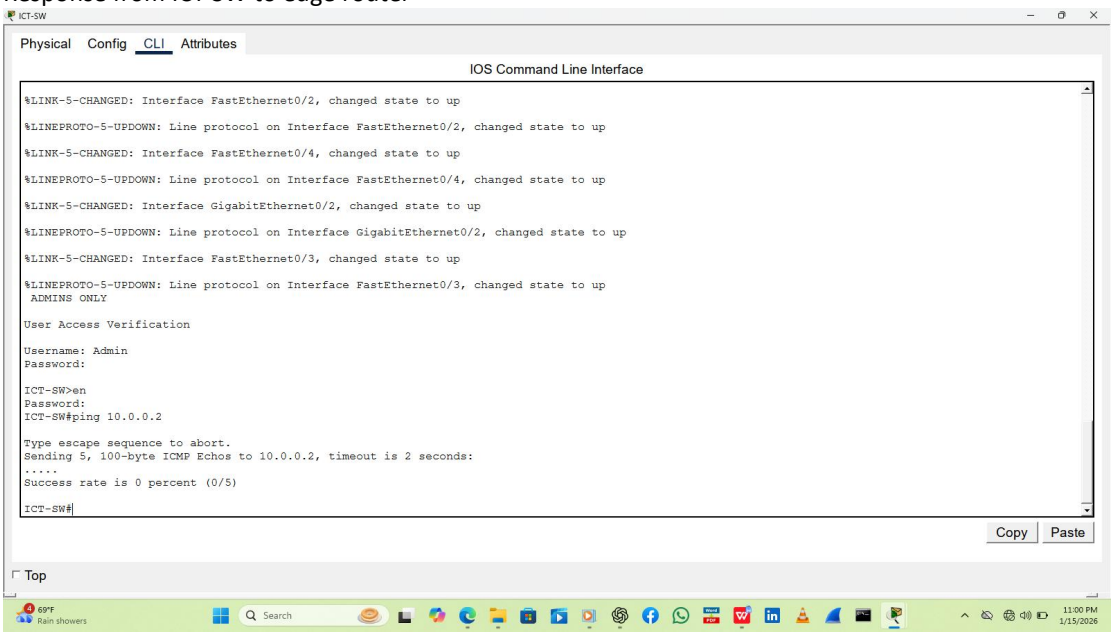


We unable to SSH the edge router, let us try to ping first,

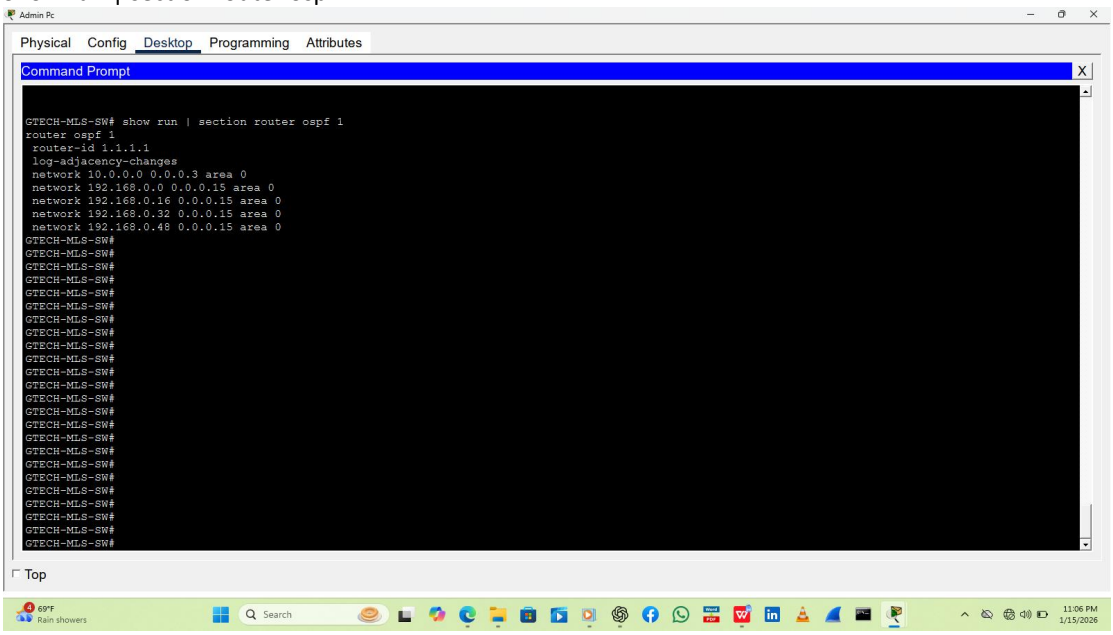


We can't even ping that must tell us the story, before we continue, we have to try to ping from any access switch to see if there is connectivity

Response from ICT SW to edge router

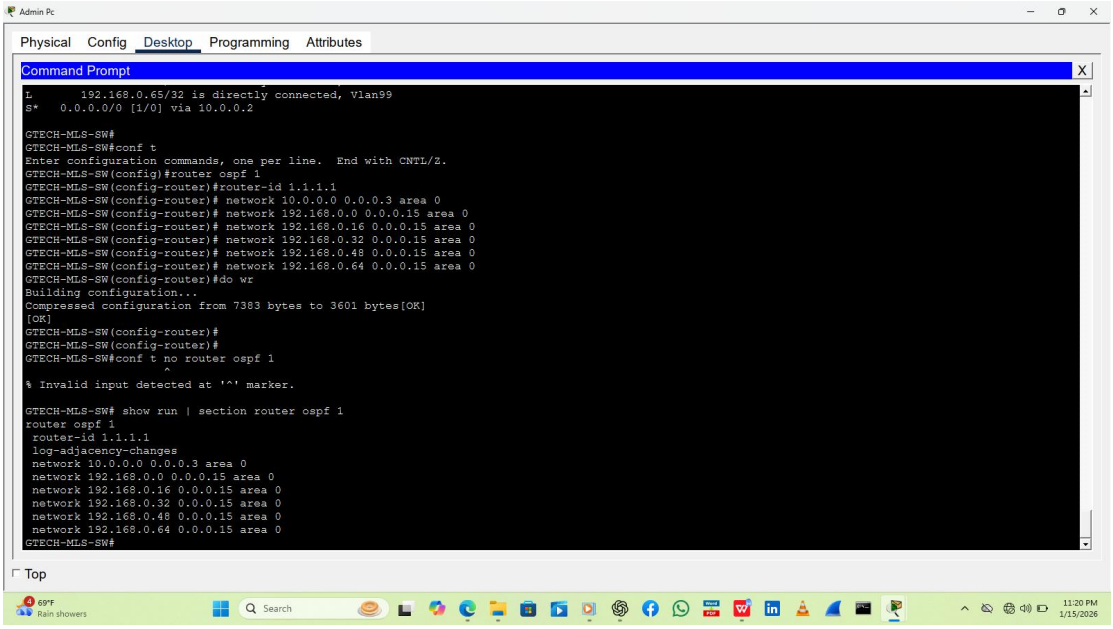


Let us start troubleshooting,first we check the routing protocol on the MLS
Show run | section router ospf 1



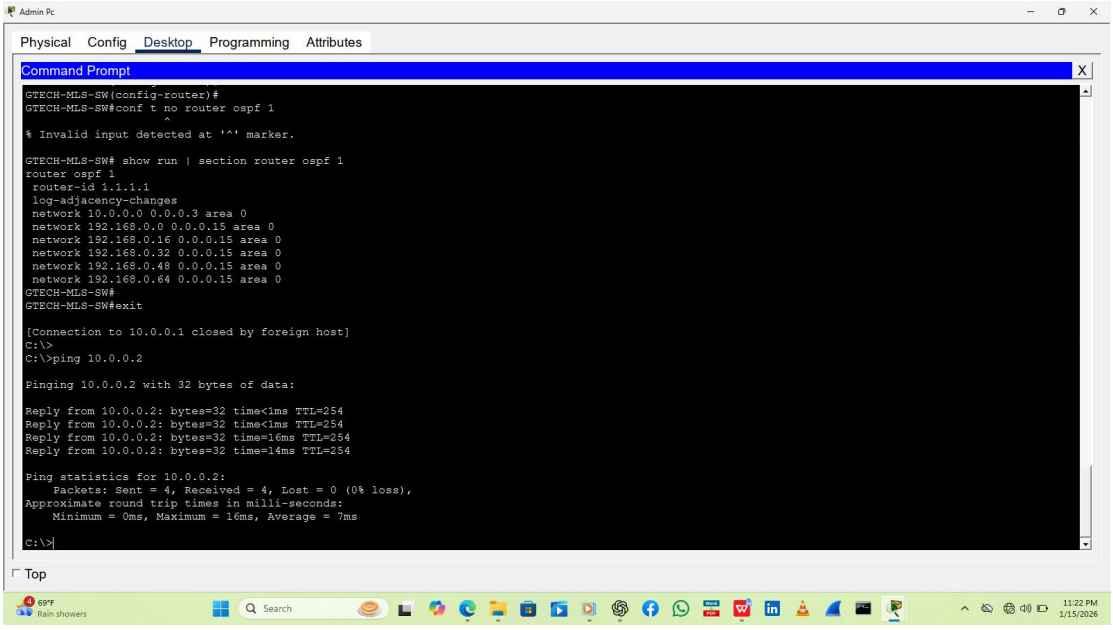
We can see that subnet 192.168.0.64/28 isnt advertised, better still we can still do a show ip route. Am on Admin PC since it can ssh the MLS no need of going to the device. Let us advertise it and check again with the Show run | section router ospf 1

Response



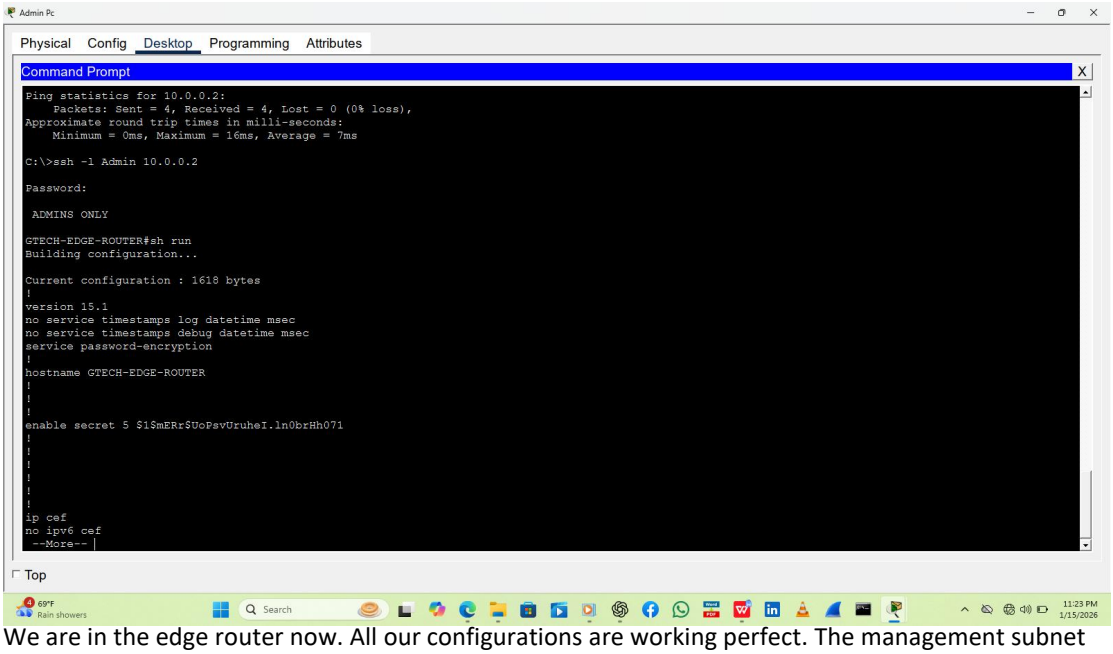
Let us try to ping the edge router again from the admin PC

Response



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

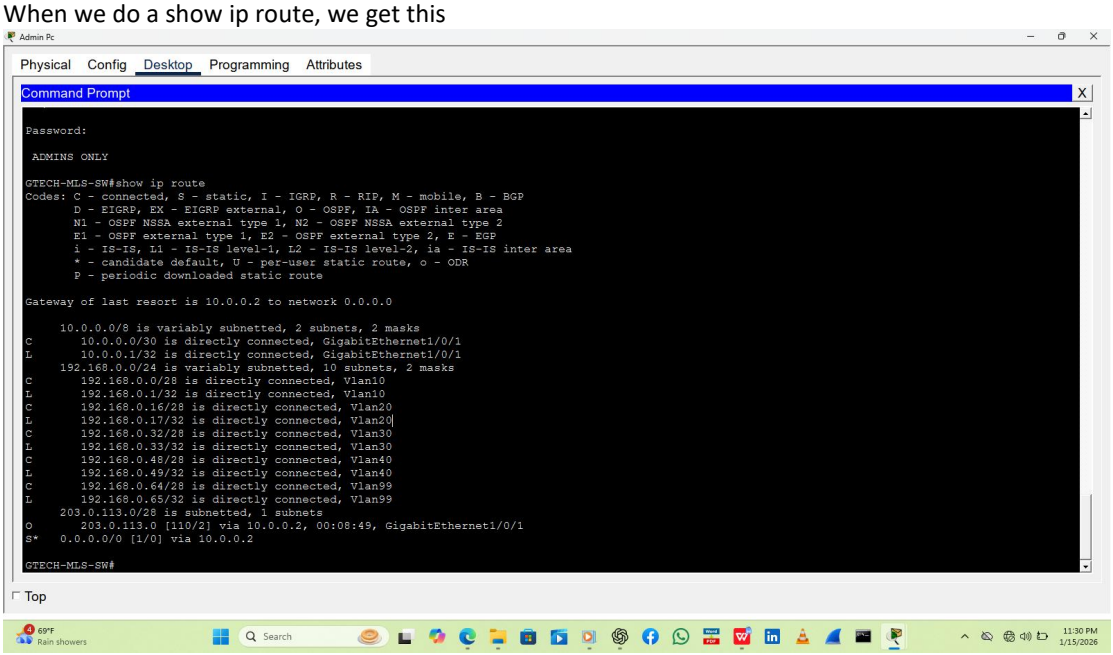
Response



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.