

SMALL NETWORK EXPANDED-SSH

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

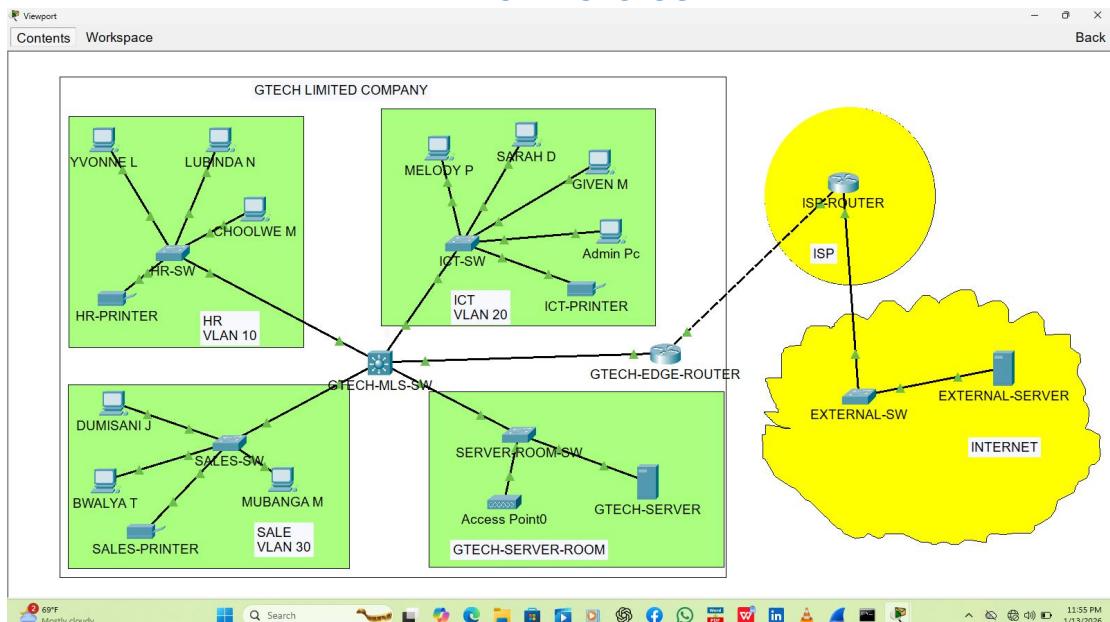
Remote secure access refers to managing network devices from a different location using encrypted management protocol. There are two methods to do this, thus telnet and ssh, telnet is not secure so we will use ssh. There are couple of things to consider this include;

- 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

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

We landed straight into an error, what's wrong here? let us troubleshoot

```
C:\>ssh -l admin 192.168.0.66
% Connection refused by remote host
C:\>tracert 182.168.0.66
Tracing route to 182.168.0.66 over a maximum of 30 hops:
 1  1 ms      0 ms      15 ms      192.168.0.66
 2  *          *          * Request timed out.
 3  *          *          * Request timed out.

C:\>tracert 192.168.0.66
Tracing route to 192.168.0.66 over a maximum of 30 hops:
 1  *          *          * Request timed out.
 2  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

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:\>
```

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

```
ADMIN'S ONLY
User Access Verification
Username: admin
Password:
HR-SW#show vlan brief
VLAN Name           Status     Ports
----- 
1  default          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2  management-vlan  active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
10   HR              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
98   NCT             active    Gig0/2
1002  fddi-default  active
1003  token-ring-default  active
1004  fddinet-default  active
1005  trinet-default  active
HR-SW#
```



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

No vlan 2

Ex

Do wr

```
Administrator: C:\Windows\system32\cmd.exe
Physical Config Desktop Programming Attributes
Command Prompt
Tracing route to 192.168.0.66 over a maximum of 30 hops:
  1  1 ms      0 ms      15 ms      192.168.0.65
  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:
  1  *          *          *          Request timed out.
  2  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

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

```
Administrator: C:\Windows\system32\cmd.exe
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 192.168.0.69
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#show vlan brief
VLAN Name          Status    Ports
---- -----
1    default        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                      active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                      active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                      active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                      active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                      active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
99   MGT            active    Gig0/2
1002 fddi-default  active
1003 token-ring-default  active
1004 fdnet-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

```
HR-SW# config t
Enter configuration commands, one per line. End with CNTL/Z.
HR-SW(config)# int gig0/2
HR-SW(config-if)# no switchport access vlan 99
HR-SW(config-if)# do wr
^
% Invalid input detected at '^' marker.

HR-SW(config-if)#
HR-SW#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
HR-SW#show vlan brief

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 fddi-default  active
1003 token-ring-default  active
1004 fddinet-default active
1005 trnet-default  active

HR-SW#
```

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

```
Administrator:~ C:\>ssh -l admin 192.168.0.68
Connection to 192.168.0.68 closed by foreign host
Administrator:~ C:\>ssh -l admin 192.168.0.69
Connection to 192.168.0.69 closed by foreign host
Administrator:~ C:\>ssh -l admin 192.168.0.66
% Connection refused by remote host
Administrator:~ C:\>
```

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

No vlan 99

Ex

No int vlan 99

HR-SW

Physical Config CLI Attributes

IOS Command Line Interface

```

FastEthernet0/17 unassigned YES manual down
FastEthernet0/18 unassigned YES manual down
FastEthernet0/19 unassigned YES manual down
FastEthernet0/20 unassigned YES manual down
FastEthernet0/21 unassigned YES manual down
FastEthernet0/22 unassigned YES manual down
FastEthernet0/23 unassigned YES manual down
FastEthernet0/24 unassigned YES manual down
GigabitEthernet0/1 unassigned YES manual up
GigabitEthernet0/2 unassigned YES manual administratively down
Vlan1 unassigned YES manual administratively down
Vlan99 192.168.0.66 YES manual down
HR-SW#
$LINK-5-CHANGED: Interface Vlan99, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
sh vian brief

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 VLAN099 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
HR-SW#

```

Top

80°F Mostly cloudy  12:53 AM 1/14/2026

Let us ssh again

Admin Pc

Physical Config Desktop Programming Attributes

Command Prompt

```

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 192.168.0.69

Password:
ADMIN'S ONLY

SERVER-ROOM-SW#
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:\>ssh -l admin 192.168.0.66

* Connection refused by remote host
C:\>

```

Top

80°F Mostly cloudy  12:54 AM 1/14/2026

Still unable to ssh, let us check the SVI

Let check the running configurations

HR-SW

Physical Config CLI Attributes

IOS Command Line Interface

```

!
interface Vlan99
ip address 192.168.0.66 255.255.255.240
!
ip default-gateway 192.168.0.65
!
banner motd ^C ADMIN'S ONLY^C
!
!
!
access-list 1 permit host 192.168.0.22
ip access-list standard SSH-MGT
permit host 192.168.0.23
deny any
permit host 192.168.0.70
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

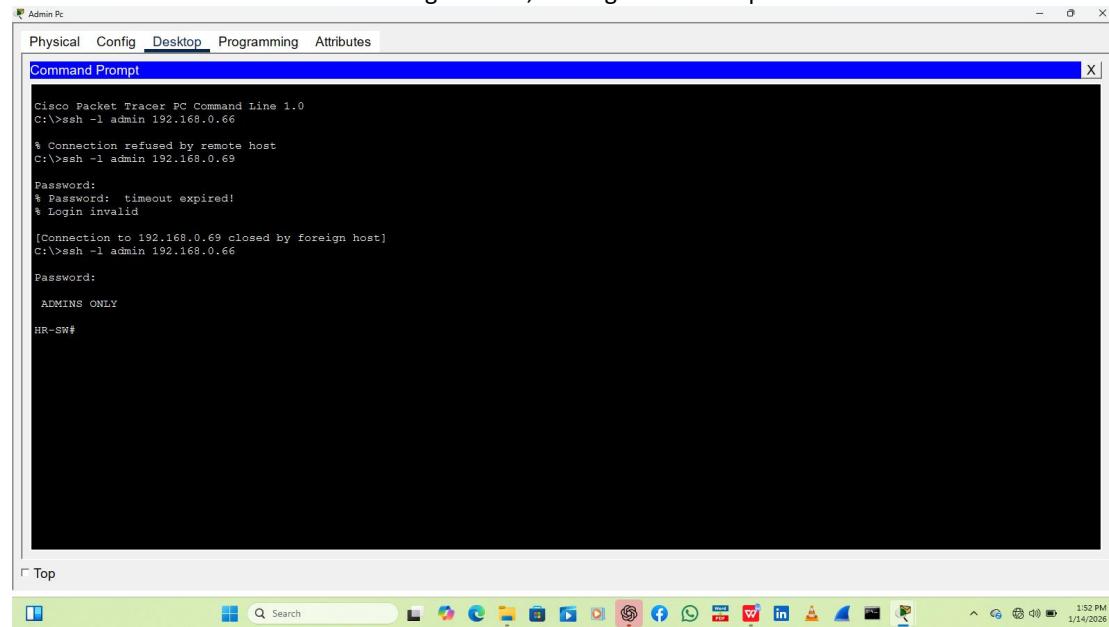
```

Top

80°F Mostly cloudy  1:45 PM 1/14/2026

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 so 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

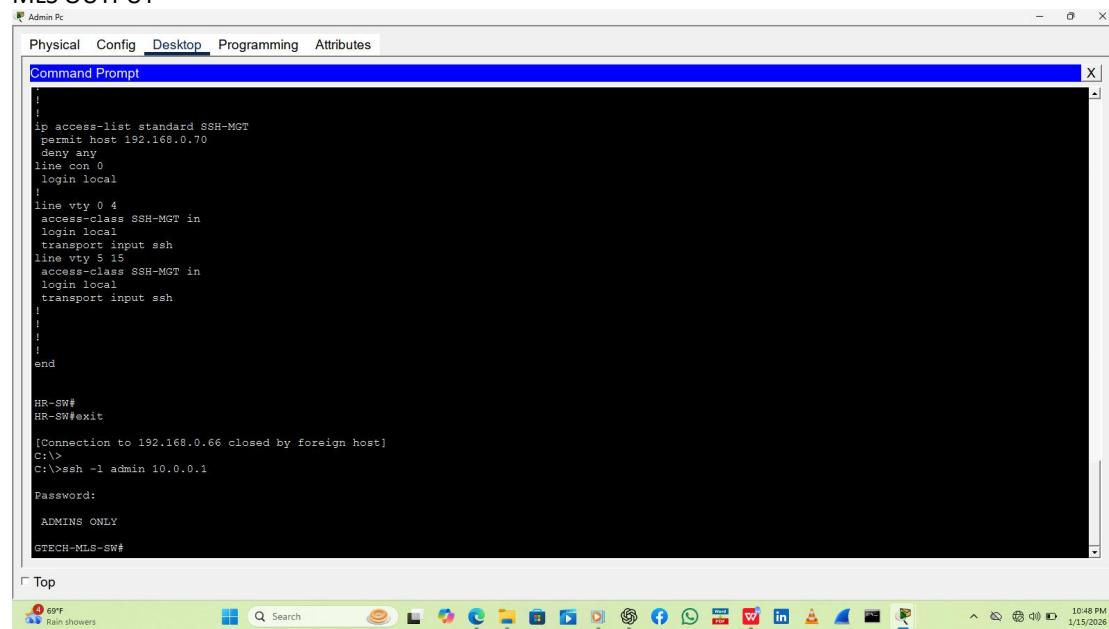


```
Cisco Packet Tracer PC Command Line 1.0
C:>ssh -l admin 192.168.0.66
% Connection refused by remote host
C:\>ssh -l admin 192.168.0.69
Password:
% Password: timeout expired!
% Login invalid
[Connection to 192.168.0.69 closed by foreign host]
C:>ssh -l admin 192.168.0.66
Password:
ADMINs ONLY
HR-SW#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

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



```
!
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

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

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

```
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:\>
```

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

ICT-SW

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
ADMINS ONLY

User Access Verification

Username: Admin
Password:

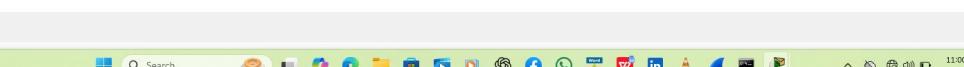
ICT-SW#en
Password:
ICT-SW#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 10.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ICT-SW#
```

[Copy](#) [Paste](#)

[Top](#)

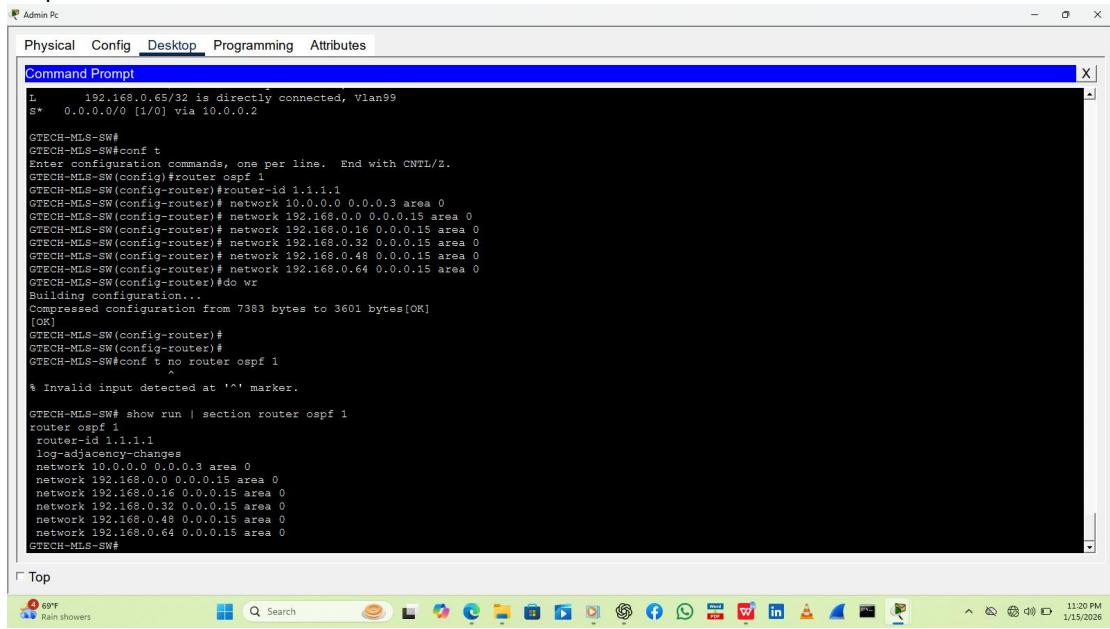


69°F Rain showers 11:00 PM 1/15/2026

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

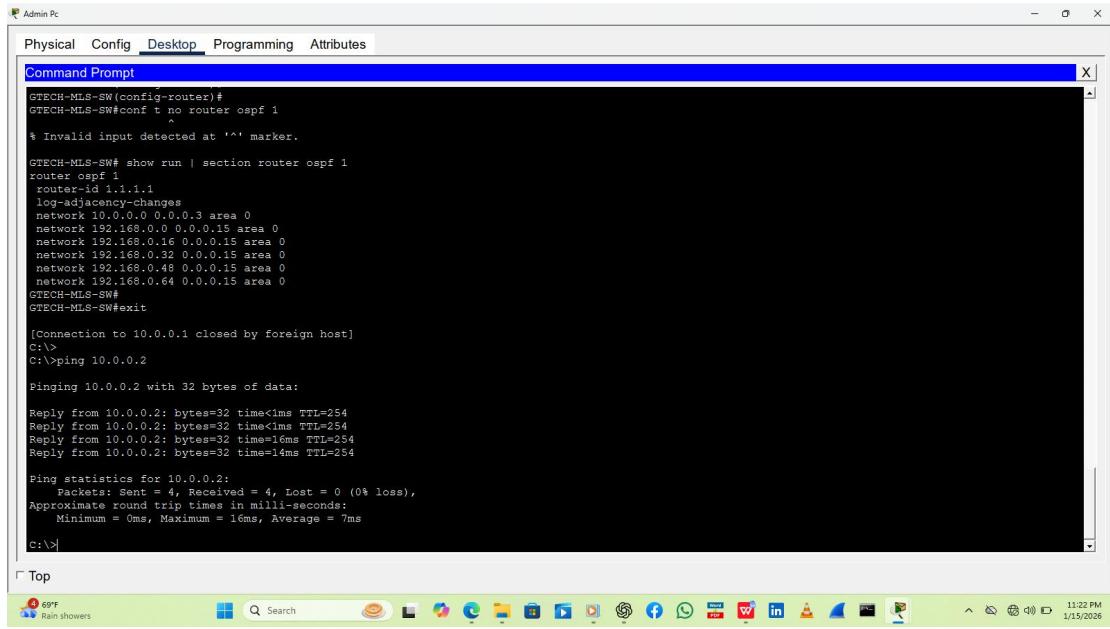


```
L 192.168.0.65/32 is directly connected, Vlan99
S* 0.0.0.0/0 [1/0] via 10.0.0.2

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...
[Processor processed configuration from 7383 bytes to 3601 bytes](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.

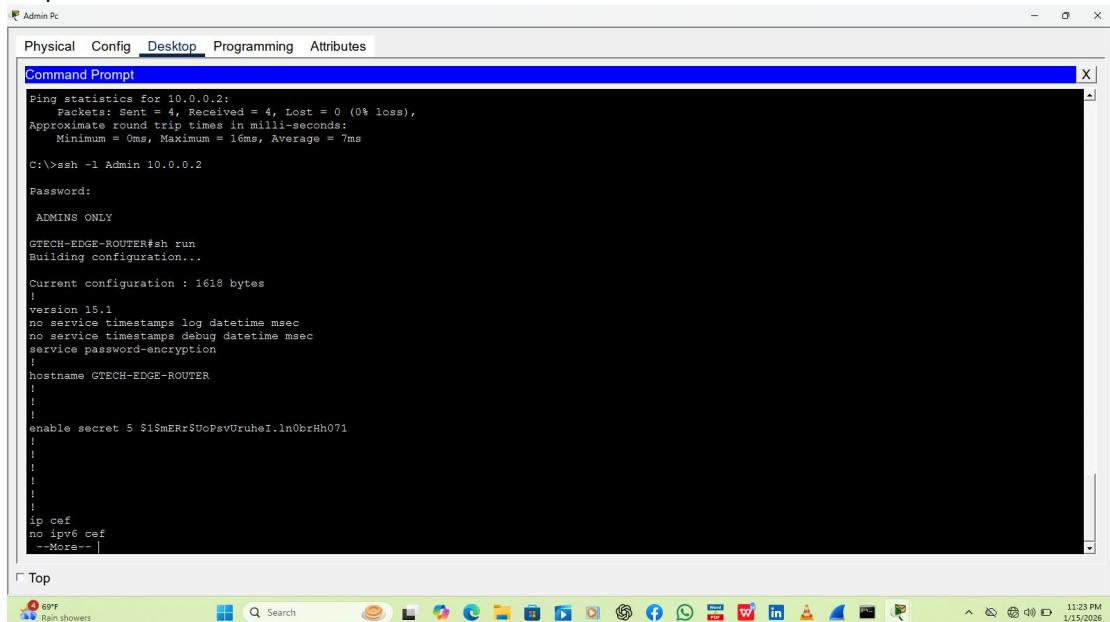
GTECH-MLS-SW# show run | section router ospf 1
router ospf 1
  router-id 1.1.1.1
    log adjacency-changes
  network 10.0.0.0 0.0.0.3 area 0
  network 192.168.0.0 0.0.0.15 area 0
  network 192.168.0.16 0.0.0.15 area 0
  network 192.168.0.32 0.0.0.15 area 0
  network 192.168.0.48 0.0.0.15 area 0
  network 192.168.0.64 0.0.0.15 area 0
GTECH-MLS-SW#exit
[Connection to 10.0.0.1 closed by foreign host]
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=1ms 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



```
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:\>ssh -l Admin 10.0.0.2
Password:
ADMIN'S ONLY
GTECH-EDGE-ROUTER#sh run
Building configuration...
Current configuration : 1618 bytes
!
version 15.1
no service timestamp log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname GTECH-EDGE-ROUTER
!
!
!
enable secret 5 $1$MERR$UoPsvUruHe1.ln0brHh071
!
!
!
ip cef
no ipv6 cef
--More--
```

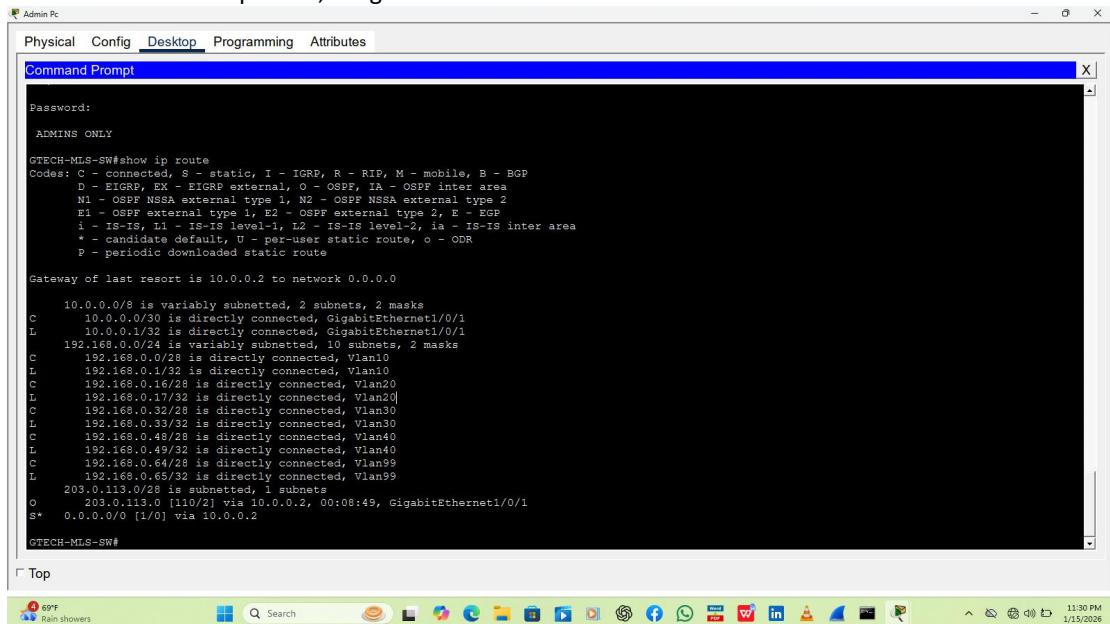
Top



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



```
Physical Config Desktop Programming Attributes
Command Prompt
Password:
ADMIN'S ONLY
GTECH-MLS-SW#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       EIGRP, EX - EIGRP external, OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       p - periodic downloaded static route

Gateway of last resort is 10.0.0.2 to network 0.0.0.0

          10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/30 is directly connected, GigabitEthernet1/0/1
L    10.0.0.1/32 is directly connected, GigabitEthernet1/0/1
          192.168.0.0/24 is variably subnetted, 10 subnets, 2 masks
C    192.168.0.0/28 is directly connected, Vlan10
L    192.168.0.1/32 is directly connected, Vlan10
C    192.168.0.16/30 is directly connected, Vlan20
L    192.168.0.17/32 is directly connected, Vlan20
C    192.168.0.32/30 is directly connected, Vlan30
L    192.168.0.33/32 is directly connected, Vlan30
C    192.168.0.48/28 is directly connected, Vlan40
L    192.168.0.49/32 is directly connected, Vlan40
C    192.168.0.64/28 is directly connected, Vlan99
L    192.168.0.65/32 is directly connected, Vlan99
          203.0.113.0/28 is subnetted, 1 subnets
O    203.0.113.0 [110/2] via 10.0.0.2, 00:08:49, GigabitEthernet1/0/1
S*   0.0.0.0/0 [1/0] via 10.0.0.2

GTECH-MLS-SW#
```

Top



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.