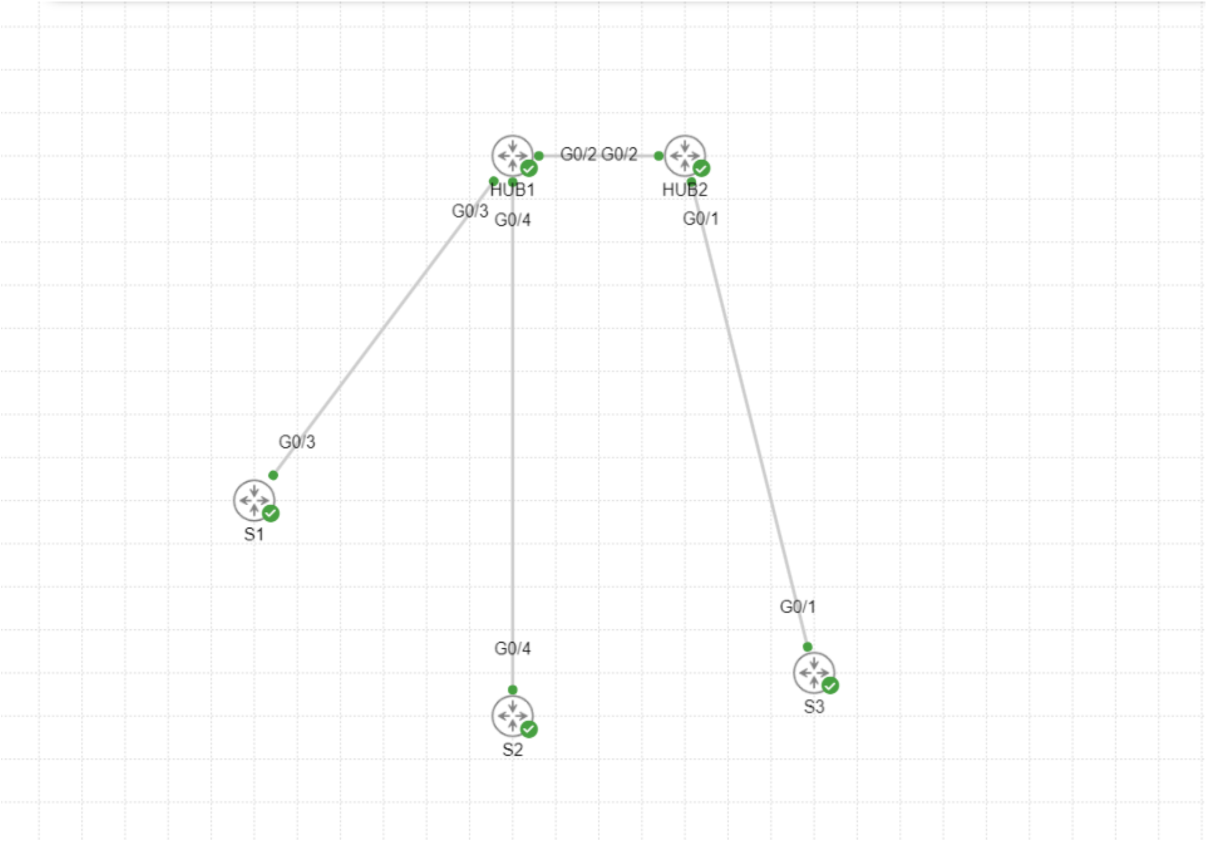
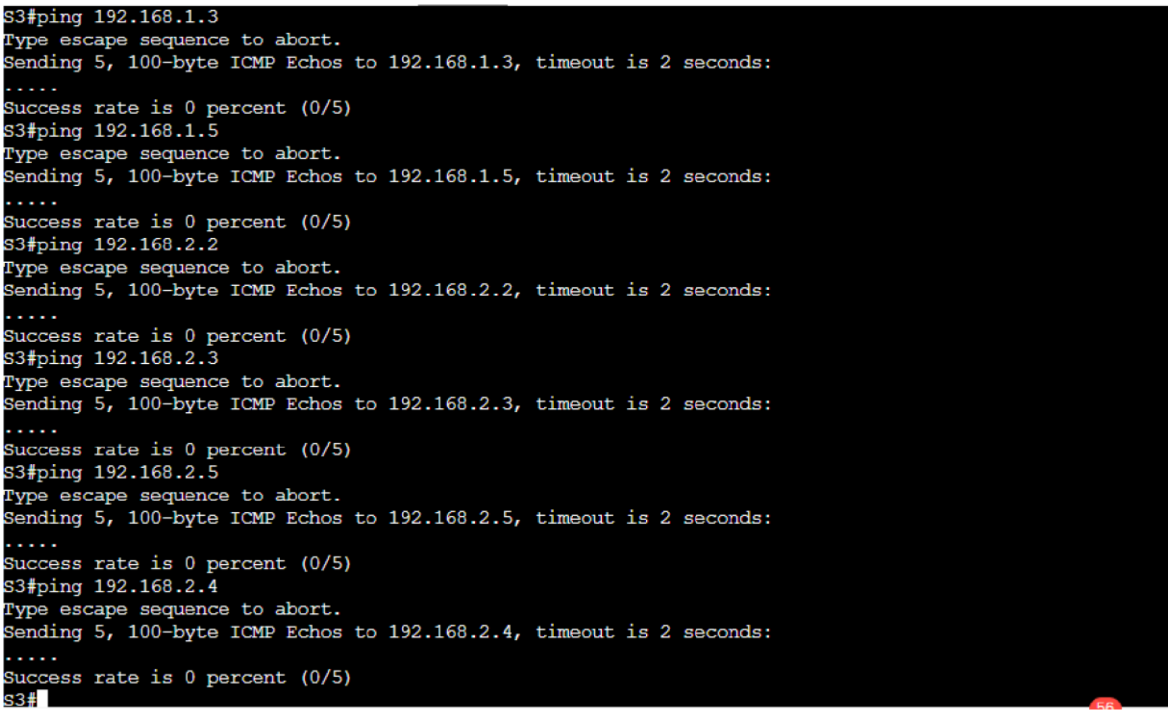


	G0/0	G0/1	G0/2	G0/3	G0/4	Loopback	VLAN	Tunnel
HUB 1	-	-	160.1.7.2/24	160.1.8.1/24	160.1.9.1/24	5.5.5.5/32	1	192.168.1.1
HUB 2	-	160.1.5.1/24	160.1.7.1/24	-	-	2.2.2.2/32	1	192.168.2.2
SITE 1 (S1)	-	-	-	160.1.8.2/24	-	6.6.6.6/32	1	192.168.1.3 192.168.2.3
SITE 2 (S2)	-	-	-	-	160.1.9.2/24	8.8.8.8/32	1	192.168.1.5 192.168.2.5
SITE 3 (S3)	-	160.1.5.2/24	-	-	-	3.3.3.3/32	1	192.168.1.4 192.168.2.4

The Topology is consisting of 5 routers representing 5 different locations with HUB1 and HUB2 being the 2 headquarters of the company and S1, S2 and S3 being branches of the company in other locations and they are also the spokes. The routers are running BGP for their routing protocol to send information across to each other. Routers HUB2 and Remote Site S3 are in the same autonomous system 600. HUB1 and Remote Sites S1, S2 and S3 are in the same autonomous system

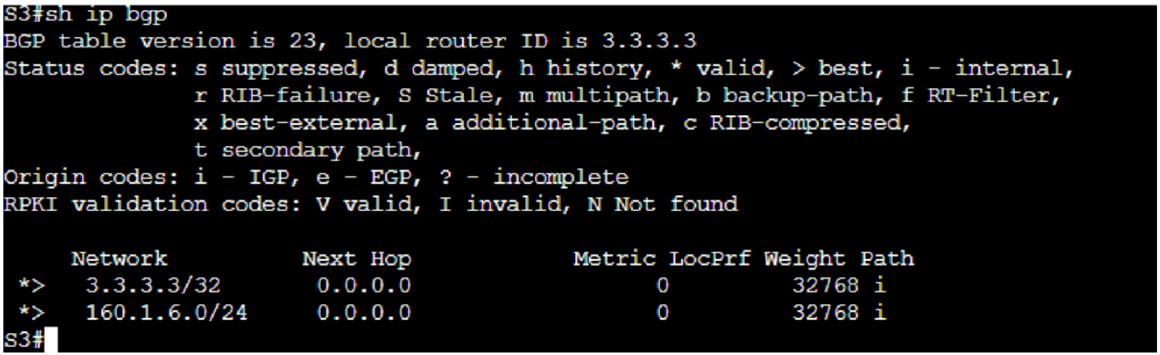
700 and that is to say that HUB1 and HUB2 are in different autonomous systems. IPsec is also configured on the routers to ensure security on the routers against a number of attacks.

Trouble Ticket	
Trouble Ticket TT-05-2024	No access to head office corporate resources or other remote sites.
Date	05/04/2024
Reporting User	On Site Technician at Site 3
Status	Open – passed to Networking and Remote Access Team
Priority	Very Urgent - High
Location	Remote Site S3
Affected Users	All users
Issue	Network down
Issue Description	A replacement router was sent in after the sudden breakdown of the previous one. The engineer the premises configured the router but doesn't seem to see or get any information from other remote site routers. Other sites confirm not being able to also reach Remote Site S3. This issue affects them with working with other sites and vice versa.
Action taken by Tier 1 engineer	Tier 1 logs the problem on the ticketing system for resolution and takes the following action: 1) Checks if the router is powered on and the power cables for any issue and confirms it is indeed turned on and no issues with the supply cables 2) Tests the network cables connected to the physical interfaces and also re-crimps the cable and sure enough they work well. 3) Pings the hub's IP and nothing shows.

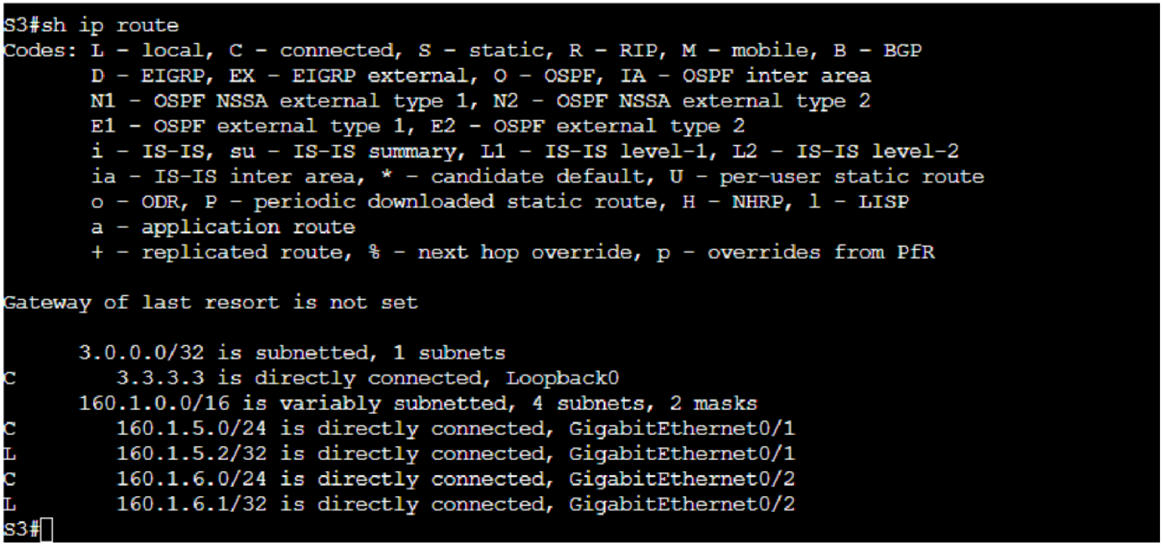
Test Ping done by Tier 1 engineer	

```
S3#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S3#ping 192.168.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S3#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S3#ping 192.168.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S3#ping 192.168.2.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S3#ping 192.168.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
S3#
```

<table>
<tr>
<td>BGP routes tests</td>
<td>



```
S3#sh ip bgp
BGP table version is 23, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   3.3.3.3/32       0.0.0.0                  0         32768 i
 *>   160.1.6.0/24     0.0.0.0                  0         32768 i
S3#
```

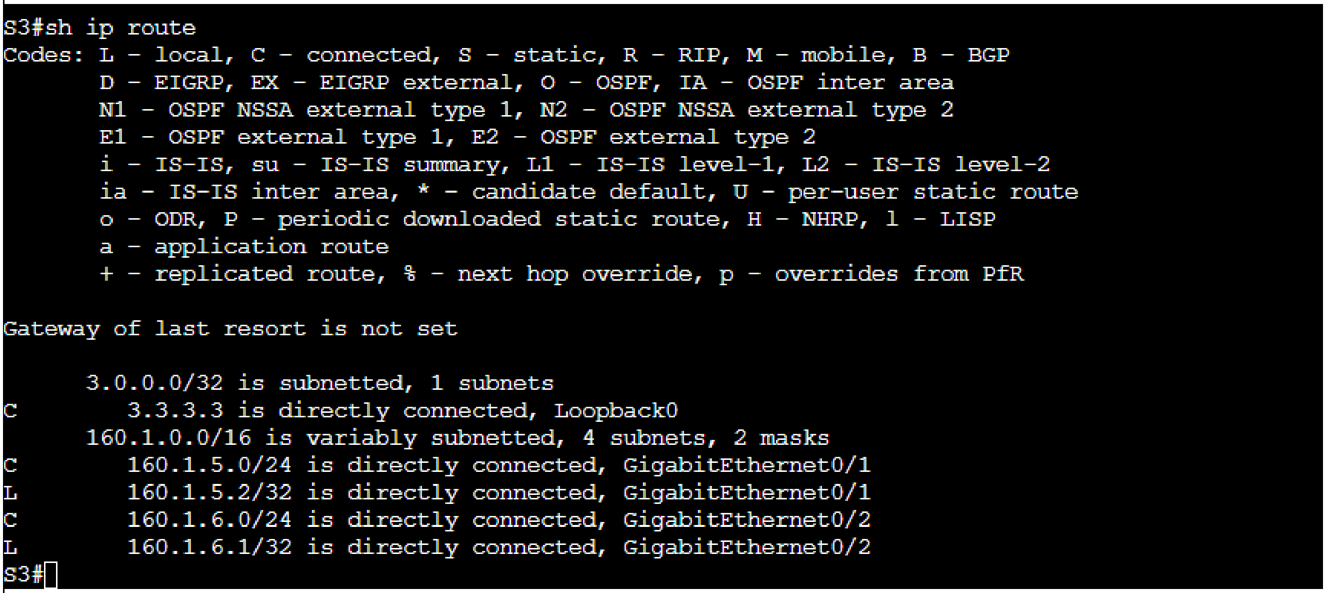


```
S3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3 is directly connected, Loopback0
      160.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        160.1.5.0/24 is directly connected, GigabitEthernet0/1
L        160.1.5.2/32 is directly connected, GigabitEthernet0/1
C        160.1.6.0/24 is directly connected, GigabitEthernet0/2
L        160.1.6.1/32 is directly connected, GigabitEthernet0/2
S3#
```

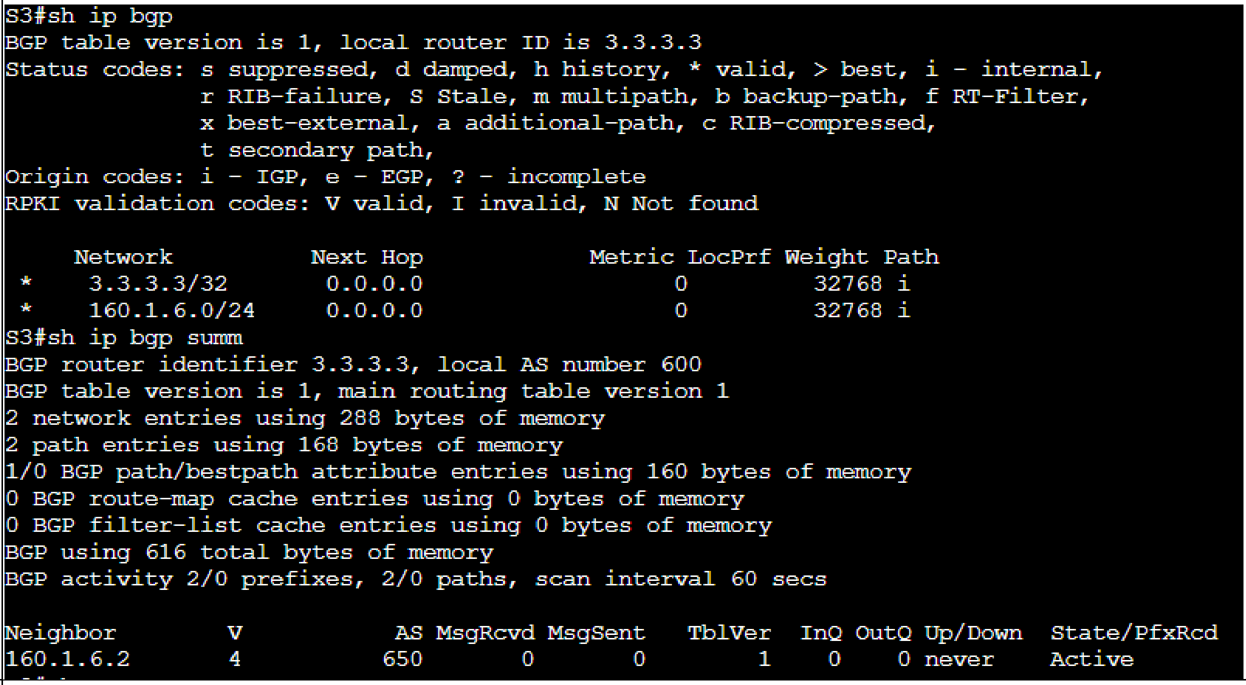
</td>
</tr>
<tr>
<td>The ticket is then escalated to a Tier 2 engineer for further troubleshooting</td>
<td>Time: 15:54, 05/04/2024
TT-05-2024
Re: Urgent- Network Down
Hello Victor,
The entire network is down and we cannot reach the other branches and headquarters and as such, all work has come to a halt. The first level has done the ping tests and no address is reachable. Please resolve the issue as soon as possible to enable resumption of operations. Best Regards,
Matt Hunnigan
Tier 1 Engineer
Remote Site 3</td>
</tr>
</table>

Resolution

Check for routing information and also bgp routing information to see what’s going on.

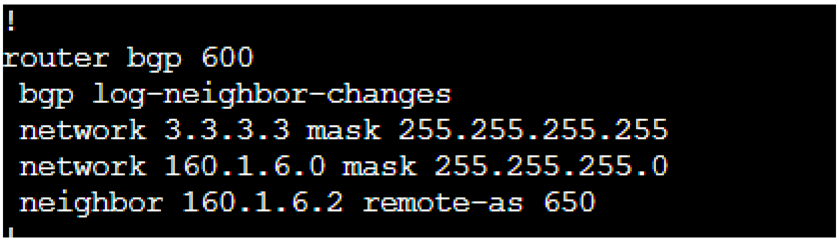


```
S3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3 is directly connected, Loopback0
      160.1.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        160.1.5.0/24 is directly connected, GigabitEthernet0/1
L        160.1.5.2/32 is directly connected, GigabitEthernet0/1
C        160.1.6.0/24 is directly connected, GigabitEthernet0/2
L        160.1.6.1/32 is directly connected, GigabitEthernet0/2
S3#
```



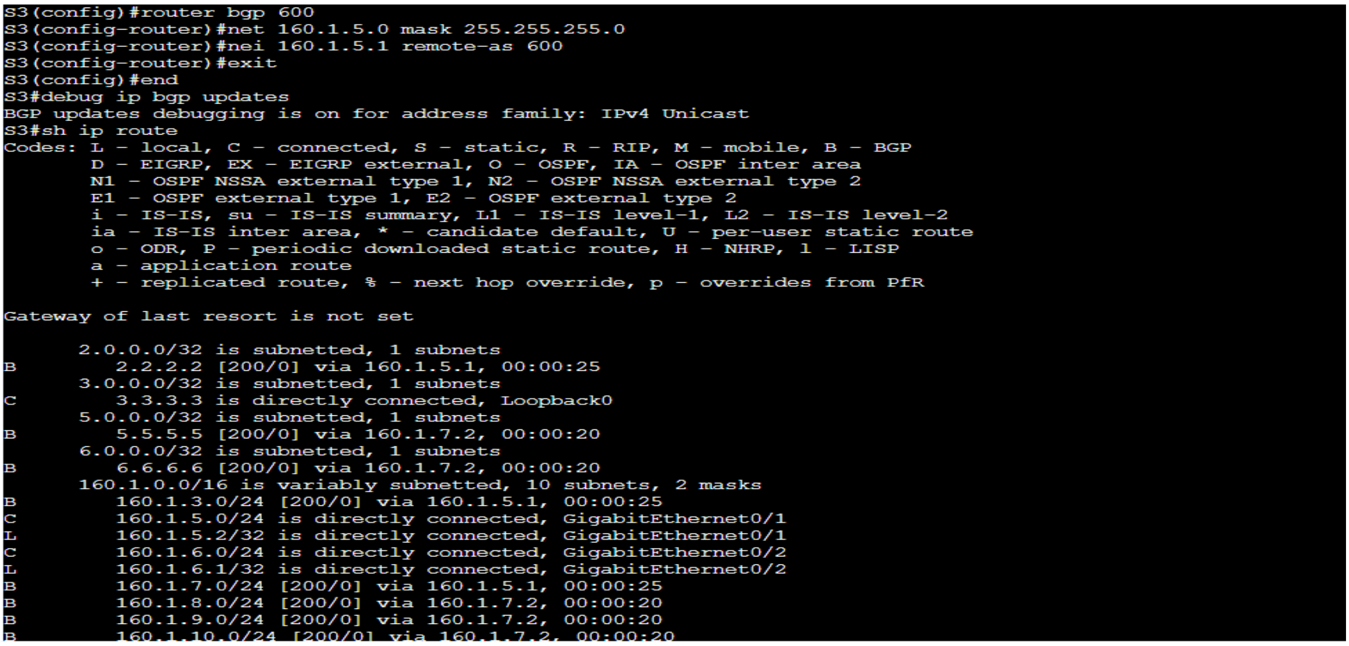
```
S3#sh ip bgp
BGP table version is 1, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *    3.3.3.3/32       0.0.0.0                  0         32768 i
 *    160.1.6.0/24     0.0.0.0                  0         32768 i
S3#sh ip bgp summ
BGP router identifier 3.3.3.3, local AS number 600
BGP table version is 1, main routing table version 1
2 network entries using 288 bytes of memory
2 path entries using 168 bytes of memory
1/0 BGP path/bestpath attribute entries using 160 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 616 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
160.1.6.2       4          650       0       0        1    0    0 never    Active
```

We can see that there is no route except the ones directly connected via the physical interfaces. We check the bgp Section of the running configuration and we see that there are no routes defined which means the engineer who did it forgot to put the right route.

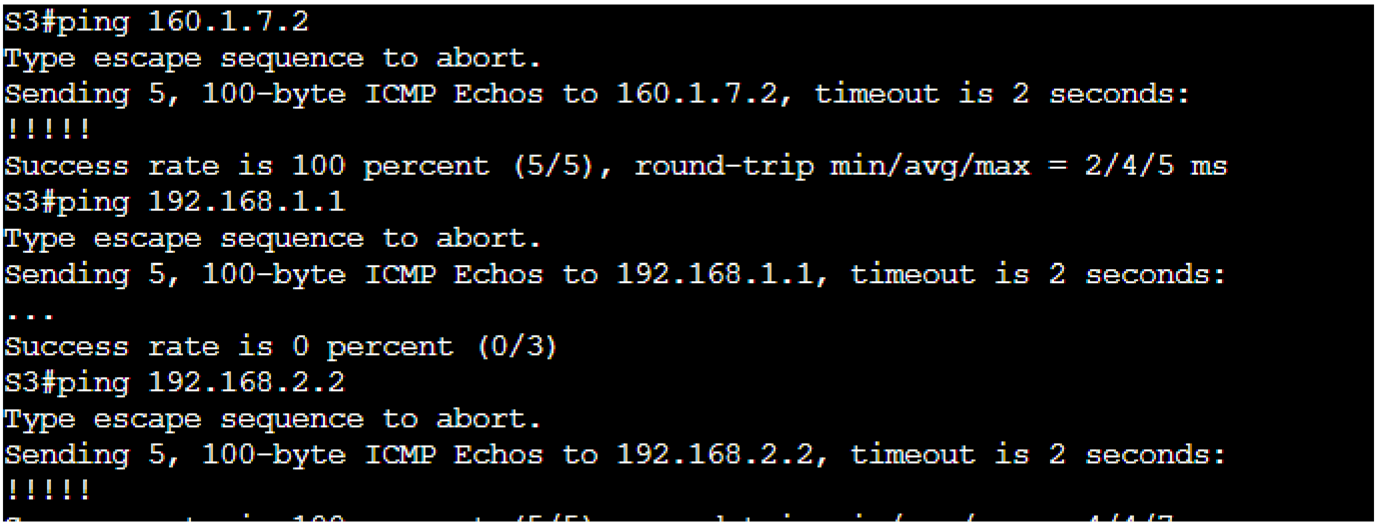


```
!
router bgp 600
 bgp log-neighbor-changes
 network 3.3.3.3 mask 255.255.255.255
 network 160.1.6.0 mask 255.255.255.0
 neighbor 160.1.6.2 remote-as 650
```

The next step is to put in a correct route that will help establish communications with other routers. Once that is done, we can see the routes show up to all other devices on the underlay network and we do a series of ping to the underlay network to confirm connectivity.



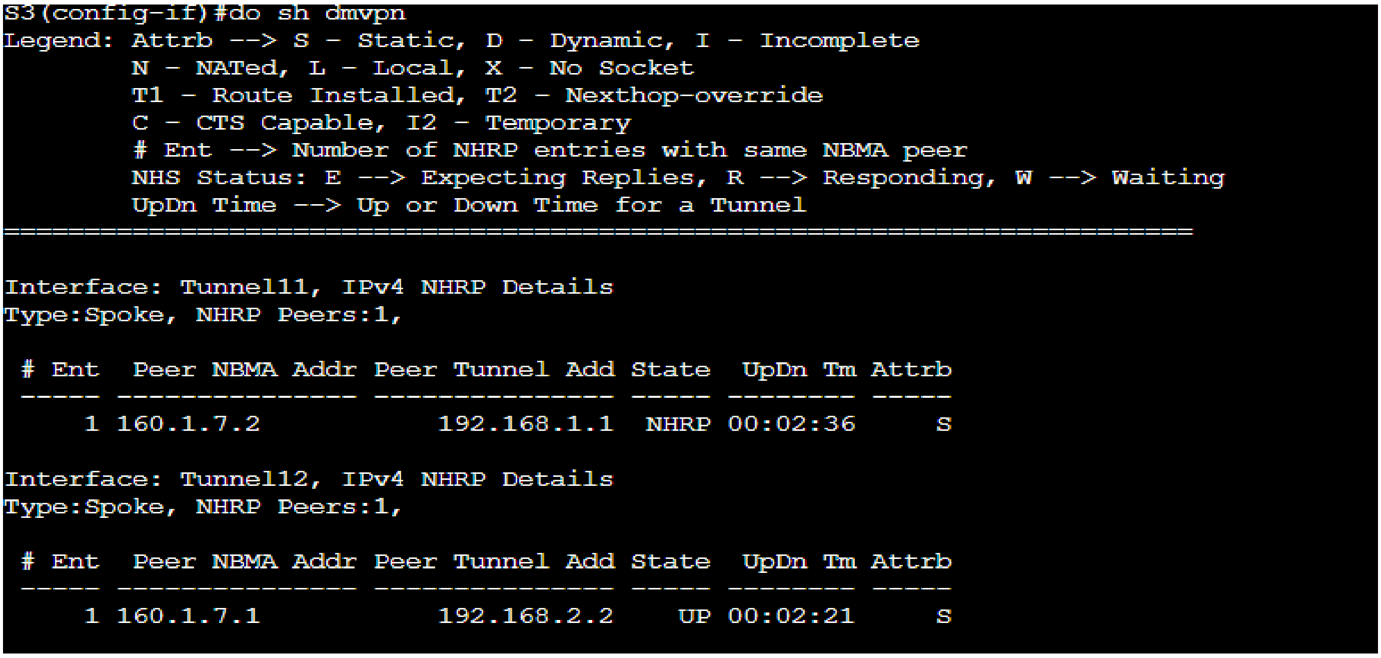
```
S3(config)#router bgp 600
S3(config-router)#net 160.1.5.0 mask 255.255.255.0
S3(config-router)#nei 160.1.5.1 remote-as 600
S3(config-router)#exit
S3(config)#end
S3#debug ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
S3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
B        2.2.2.2 [200/0] via 160.1.5.1, 00:00:25
      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3 is directly connected, Loopback0
      5.0.0.0/32 is subnetted, 1 subnets
B        5.5.5.5 [200/0] via 160.1.7.2, 00:00:20
      6.0.0.0/32 is subnetted, 1 subnets
B        6.6.6.6 [200/0] via 160.1.7.2, 00:00:20
      160.1.0.0/16 is variably subnetted, 10 subnets, 2 masks
B        160.1.3.0/24 [200/0] via 160.1.5.1, 00:00:25
C        160.1.5.0/24 is directly connected, GigabitEthernet0/1
L        160.1.5.2/32 is directly connected, GigabitEthernet0/1
C        160.1.6.0/24 is directly connected, GigabitEthernet0/2
L        160.1.6.1/32 is directly connected, GigabitEthernet0/2
B        160.1.7.0/24 [200/0] via 160.1.5.1, 00:00:25
B        160.1.8.0/24 [200/0] via 160.1.7.2, 00:00:20
B        160.1.9.0/24 [200/0] via 160.1.7.2, 00:00:20
B        160.1.10.0/24 [200/0] via 160.1.7.2, 00:00:20
```



```
S3#ping 160.1.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 160.1.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/5 ms
S3#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
...
Success rate is 0 percent (0/3)
S3#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
```

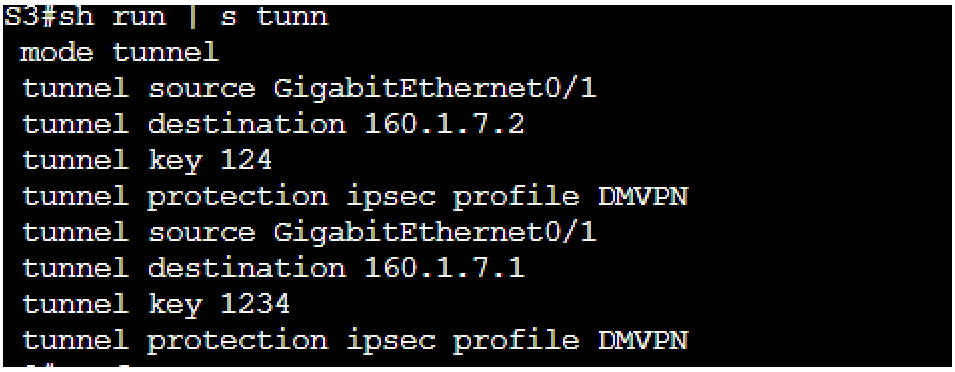
The ping test to HUB1 underlay interface is successful but the overlay isn't and also, the overlay for HUB2 is reachable which means that something may be wrong with the dmvpn configuration.

We check the dmvpn status using the ‘sh dmvpn’ command to see what is going on and we find out that tunnel 11 is in NHRP state which means that there is a configuration issue somewhere which I would try to look for.



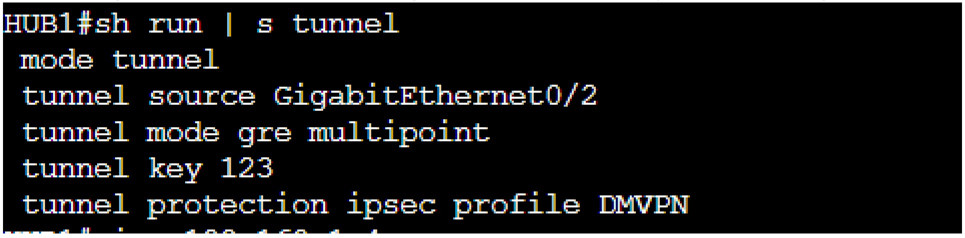
```
S3(config-if)#do sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 160.1.7.2           192.168.1.1  NHRP 00:02:36     S

Interface: Tunnel12, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 160.1.7.1           192.168.2.2    UP 00:02:21     S
```

Using the ‘sh run’ command, we look at the dmvpn running configuration on the router.



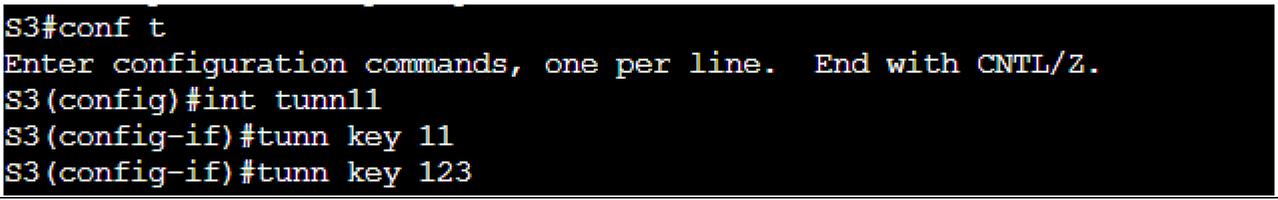
```
S3#sh run | s tunn
 mode tunnel
 tunnel source GigabitEthernet0/1
 tunnel destination 160.1.7.2
 tunnel key 124
 tunnel protection ipsec profile DMVPN
 tunnel source GigabitEthernet0/1
 tunnel destination 160.1.7.1
 tunnel key 1234
 tunnel protection ipsec profile DMVPN
```

The configuration seems to be alright at first so I will try to check it against the hub’s dmvpn tunnel configuration.



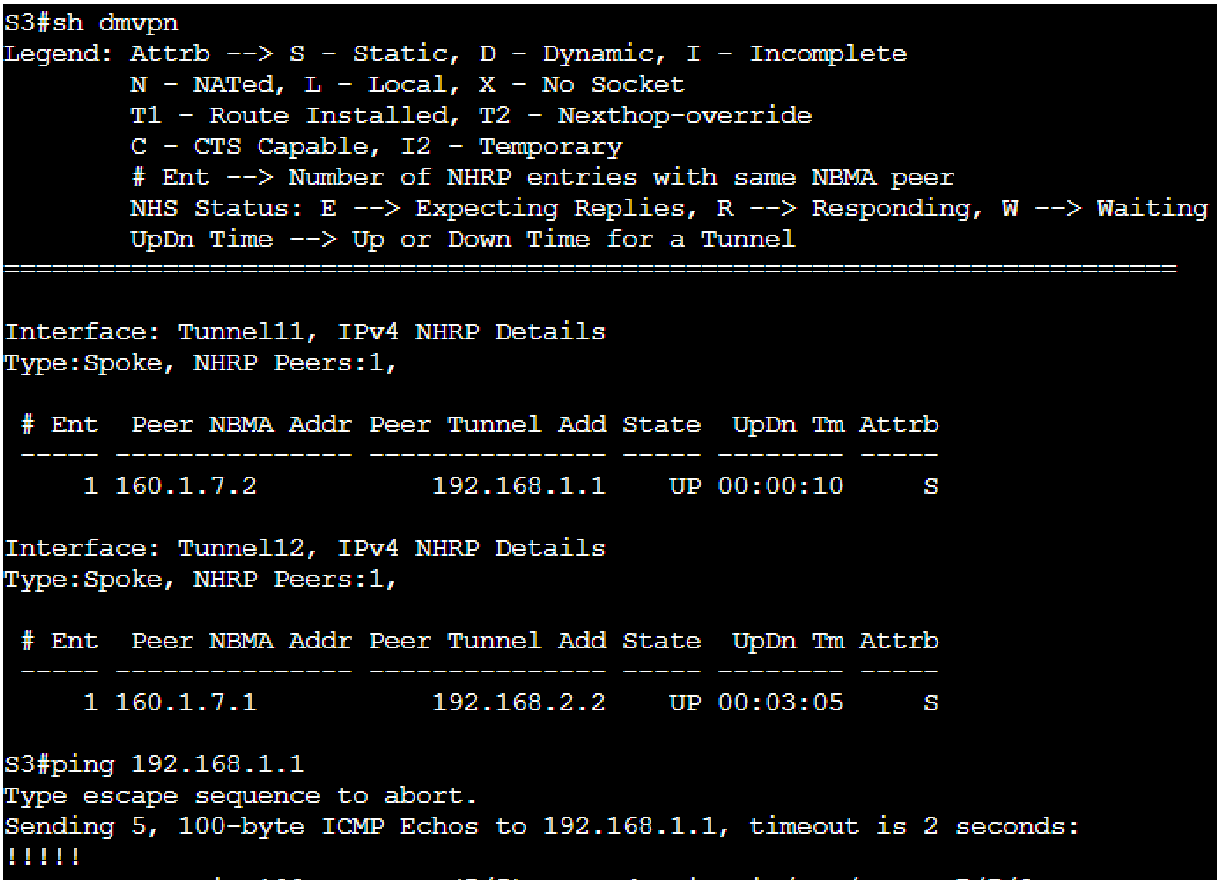
```
HUB1#sh run | s tunnel
 mode tunnel
 tunnel source GigabitEthernet0/2
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile DMVPN
```

The issue looking at it seems to be a tunnel key mismatch which should be the issue causing the tunnel not to be able to resolve the next hop. So we change the tunnel key to what it is on the hub.



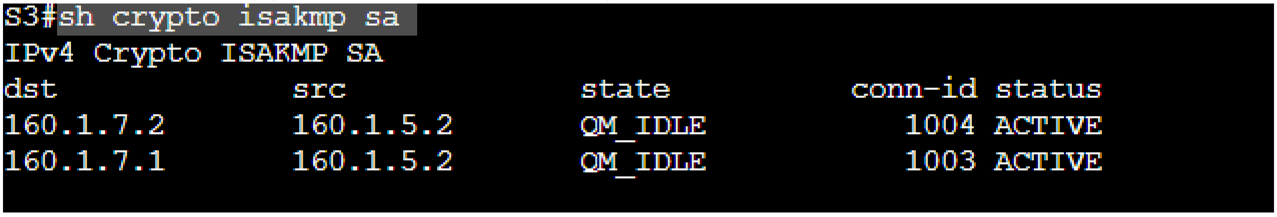
```
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#int tunn11
S3(config-if)#tunn key 11
S3(config-if)#tunn key 123
```

After changing the tunnel key of the spoke router, the state of the tunnel has come up and pings to the hub is going through.



```
S3#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 160.1.7.2           192.168.1.1    UP 00:00:10     S

Interface: Tunnel12, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 160.1.7.1           192.168.2.2    UP 00:03:05     S

S3#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
```

After I check the iskamp status to check IKE security association.



```
S3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
160.1.7.2       160.1.5.2       QM_IDLE           1004 ACTIVE
160.1.7.1       160.1.5.2       QM_IDLE           1003 ACTIVE
```

End of Ticket	Time: 16:15, 05/04/2024 TT-05-2024 Re: Urgent- Network Down Hello Matt, I an pleased to report that the network is back and running properly as I have taken care of the root cause of the problem and work can continue as normal. Best Regards, Victor Ndukwe Tier 2 Engineer Headquarters 1 Site