Alp Kural - 71959
Computer Engineering

Comp 416 – Network Layer Analysis and Simulations with Cisco Tracer

PART 1- Network Layer Analysis

PART 1.1 - ICMP Analysis

Question 01

```
alpku@alpku-VirtualBox:~$ traceroute -I www.sydney.edu.au
traceroute to www.sydney.edu.au (2.16.241.75), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.252 ms  0.197 ms  0.134 ms
 2  172.21.128.3 (172.21.128.3)  3.138 ms  3.295 ms  3.344 ms
 3  10.20.30.2 (10.20.30.2)  3.989 ms  4.313 ms  4.430 ms
 4  212.175.32.141.static.ttnet.com.tr (212.175.32.141)  5.637 ms  5.765 ms  5.911 ms
 5  212.174.167.209 (212.174.167.209)  6.057 ms  7.212 ms  7.255 ms
 6  00-gayrettepe-sr14s-t2-1---00-buyukdere-t3-1.statik.turktelekom.com.tr (212.156.121.72)  7.396 ms  4.190 ms  4.260 ms
 7  * 41-gebze-t2-1---34-acibadem-xrs-t2-1.statik.turktelekom.com.tr (81.212.220.238)  4.238 ms  4.494 ms
 8  10-balya-sr12-t4-1---10-balikesir-sr12e-t3-3.statik.turktelekom.com.tr (81.212.209.102)  4.680 ms  4.783 ms  4.926 ms
 9  305-vie-col-1---00-ebgp-gayrettepe-k.statik.turktelekom.com.tr (212.156.140.114)  29.793 ms  29.924 ms  29.913 ms
10  185.84.16.25 (185.84.16.25)  45.661 ms  45.770 ms  45.828 ms
11  ae-5.r20.vienat02.at.bb.gin.ntt.net (129.250.2.217)  51.053 ms  53.507 ms  53.474 ms
12  ae-1.r20.frnkge13.de.bb.gin.ntt.net (129.250.7.35)  67.136 ms  55.012 ms  55.152 ms
13  ae-0.a03.frnkge07.de.bb.gin.ntt.net (129.250.7.16)  57.609 ms  57.593 ms  57.787 ms
14  83.231.214.154 (83.231.214.154)  57.777 ms  56.720 ms  56.590 ms
15  ae34.r03.border101.fra03.fab.netarch.akamai.com (23.210.54.63)  48.174 ms  48.214 ms  48.187 ms
16  * * *
17  * * *
18  * * *
19  a2-16-241-75.deploy.static.akamaitechnologies.com (2.16.241.75)  49.872 ms  50.063 ms  50.055 ms
```

Fig. 1.

The maximum TTL less than which the traceroute messages do not reach to a destination is 15.

Question 02

The default number of probes used by the traceroute command is 3 in my Linux-based virtual machine.

```
alpku@alpku-VirtualBox:~$ traceroute -I --queries=4 www.sydney.edu.au
traceroute to www.sydney.edu.au (104.83.4.24), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  1.089 ms  1.067 ms  1.062 ms  1.057 ms
 2  172.21.128.3 (172.21.128.3)  4.338 ms  5.095 ms  5.018 ms  5.011 ms
 3  10.20.30.2 (10.20.30.2)  6.047 ms  6.027 ms  6.021 ms  5.905 ms
 4  212.175.32.141.static.ttnet.com.tr (212.175.32.141)  5.880 ms  5.855 ms  5.850 ms  6.570 ms
 5  212.174.167.209 (212.174.167.209)  5.152 ms  5.959 ms  5.955 ms  5.951 ms
 6  00-gayrettepe-sr14s-t2-1---00-buyukdere-t3-1.statik.turktelekom.com.tr (212.156.121.72)  4.383 ms  5.069 ms  5.063 ms  5.057 ms
 7  * * * *
 8  * * * *
 9  302-ams-col-2---00-ebgp-gayrettepe-k.statik.turktelekom.com.tr (212.156.102.136)  65.068 ms  66.112 ms  66.106 ms  66.100 ms
10  80.157.207.93 (80.157.207.93)  67.599 ms  67.585 ms  67.579 ms  68.500 ms
11  vie-sb5-i.VIE.AT.NET.DTAG.DE (217.239.43.242)  60.743 ms  60.865 ms  60.851 ms  60.847 ms
12  80.157.205.238 (80.157.205.238)  78.348 ms  79.305 ms  79.301 ms  78.399 ms
13  a104-83-4-24.deploy.static.akamaitechnologies.com (104.83.4.24)  78.362 ms  78.174 ms  78.162 ms  78.157 ms
alpku@alpku-VirtualBox:~$ traceroute -I --queries=5 www.sydney.edu.au
traceroute to www.sydney.edu.au (104.83.4.24), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.763 ms  0.740 ms  0.735 ms  0.730 ms  0.725 ms
 2  172.21.128.3 (172.21.128.3)  4.144 ms  4.139 ms  4.134 ms  4.129 ms  4.124 ms
 3  10.20.30.2 (10.20.30.2)  4.118 ms  4.112 ms  3.778 ms  3.787 ms  3.781 ms
 4  212.175.32.141.static.ttnet.com.tr (212.175.32.141)  4.705 ms  3.265 ms  4.094 ms  4.089 ms  4.084 ms
 5  212.174.167.209 (212.174.167.209)  4.852 ms  4.846 ms  6.047 ms  6.040 ms  6.033 ms
 6  00-gayrettepe-sr14s-t2-1---00-buyukdere-t3-1.statik.turktelekom.com.tr (212.156.121.72)  6.025 ms  6.018 ms  6.011 ms  6.003 ms  5.996 ms
 7  41-gebze-t2-1---34-acibadem-xrs-t2-1.statik.turktelekom.com.tr (81.212.220.238)  5.964 ms  6.831 ms  6.642 ms  7.405 ms  7.398 ms
 8  10-balya-sr12-t4-1---10-balikesir-sr12e-t3-3.statik.turktelekom.com.tr (81.212.209.102)  15.529 ms  16.548 ms  16.091 ms  16.079 ms  16.073 ms
 9  302-ams-col-2---00-ebgp-gayrettepe-k.statik.turktelekom.com.tr (212.156.102.136)  66.335 ms  67.132 ms  67.127 ms  74.222 ms  74.218 ms
10  80.157.207.93 (80.157.207.93)  77.703 ms  77.698 ms  77.694 ms  72.350 ms  71.572 ms
11  vie-sb5-i.VIE.AT.NET.DTAG.DE (217.239.43.242)  64.624 ms  58.713 ms  58.642 ms  60.449 ms  59.194 ms
12  80.157.205.238 (80.157.205.238)  82.442 ms  81.612 ms  83.147 ms  83.137 ms  81.547 ms
13  a104-83-4-24.deploy.static.akamaitechnologies.com (104.83.4.24)  78.003 ms  77.986 ms  78.152 ms  78.142 ms  77.084 ms
alpku@alpku-VirtualBox:~$ traceroute -I --queries=6 www.sydney.edu.au
traceroute to www.sydney.edu.au (104.83.4.9), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.785 ms  0.767 ms  0.762 ms  0.759 ms  0.755 ms  0.752 ms
 2  172.21.128.3 (172.21.128.3)  4.137 ms  4.134 ms  5.424 ms  5.421 ms  5.418 ms  5.414 ms
 3  10.20.30.2 (10.20.30.2)  5.410 ms  5.406 ms  6.182 ms  6.179 ms  4.022 ms  3.998 ms
 4  212.175.32.141.static.ttnet.com.tr (212.175.32.141)  3.973 ms  3.949 ms  3.945 ms  4.997 ms  4.507 ms  4.429 ms
 5  212.174.167.209 (212.174.167.209)  8.336 ms  8.329 ms  8.323 ms  8.317 ms  8.312 ms  8.304 ms
 6  00-gayrettepe-sr14s-t2-1---00-buyukdere-t3-1.statik.turktelekom.com.tr (212.156.121.72)  6.011 ms  6.003 ms  5.411 ms  5.378 ms  5.373 ms  5.350 ms
 7  * * * * * *
 8  * * * * * *
 9  302-ams-col-2---00-ebgp-gayrettepe-k.statik.turktelekom.com.tr (212.156.102.136)  64.934 ms  65.854 ms  65.848 ms  65.842 ms  65.894 ms  66.089 ms
10  80.157.207.93 (80.157.207.93)  66.902 ms  66.897 ms  66.549 ms  66.630 ms  65.806 ms  65.793 ms
11  vie-sb5-i.VIE.AT.NET.DTAG.DE (217.5.95.222)  62.165 ms  62.191 ms  62.173 ms  63.239 ms  62.240 ms  62.241 ms
12  80.157.205.238 (80.157.205.238)  76.776 ms  76.728 ms  79.126 ms  79.405 ms  82.669 ms  82.779 ms
13  a104-83-4-9.deploy.static.akamaitechnologies.com (104.83.4.9)  78.203 ms  78.348 ms  78.036 ms  77.906 ms  78.891 ms  78.773 ms
```

Fig. 2.

Observations regarding the resolution of the route:

Consistent Initial Hops: The early hops (1-6) remain relatively consistent across different queries, representing the local network and initial routers.

Varying Intermediate Hops: There is variability in the number of intermediate hops, with some routers responding and others not. This variability can be attributed to network conditions and configurations.

Consistent Final Hops: The final hops (11-13) leading to the destination IP address (104.83.4.24) are relatively consistent, indicating stability in the path to the destination.

Increased Latency: Latency generally increases as the traceroute progresses, reflecting the cumulative time taken for packets to traverse multiple routers and cover a larger geographic distance.

Unresponsive Hops: Some hops do not respond to probes, denoted by asterisks. This is a common behavior and can be due to routers configured not to respond to ICMP requests.

Path Stability: Despite variations in intermediate hops, the overall path to the destination remains stable, and the traceroute consistently reaches the destination through the same set of final hops.

Question 03

All the experiments in Question 2 & 3 are conducted with traceroute version that uses ICMP packets.

Question 04

A Routing Blackhole refers to a situation in a computer network where network traffic is directed to a destination for which there is no valid route or forwarding information. Essentially, it's a condition where data packets are sent into the network, but due to misconfigurations, errors, or other issues, they end up getting dropped or lost because there is no proper path for them to reach their intended destination.

In a DDoS protection scenario, a routing blackhole can be beneficially used to mitigate the impact of a DDoS attack. By configuring a blackhole route for the targeted IP address, malicious traffic is directed to a non-existent path, preventing it from reaching the intended destination and minimizing the impact on the network. This intentional use of a routing blackhole is a common strategy in DDoS mitigation to protect essential services during an attack.

PART - 1.2 Network Interface Analysis

Command #1: ip -s -d link show

```
alpku@alpku-VirtualBox:~$ ip -s -d link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 promiscuity 0 minmtu 0 maxmtu 0 addrgenmode eui64 numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso
_max_segs 65535
    RX:  bytes packets errors dropped  missed   mcast
         15817     205      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
         15817     205      0       0       0       0
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:11:22:33:44:55 brd 02:11:22:33:44:55 permaddr 08:00:27:71:75:ee promiscuity 0 minmtu 46 maxmtu 16110 addrgenmode none numtxqueues 1 numrxque
ues 1 gso_max_size 65536 gso_max_segs 65535 parentbus pci parentdev 0000:00:03.0
    RX:  bytes packets errors dropped  missed   mcast
          9076      68      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
         15817     157      0       0       0       0
```

Fig. 3.

The command is used in Linux to display detailed information about network interfaces.

"-s": This option stands for "statistics" and is used to display additional statistics for network interfaces.

"-d": This option stands for "details" and is used to show detailed information about the specified network interfaces.

Command #2: ip -h -c addr show

```
alpku@alpku-VirtualBox:~$ ip -h -c addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:11:22:33:44:55 brd 02:11:22:33:44:55 permaddr 08:00:27:71:75:ee
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 84734sec preferred_lft 84734sec
    inet6 fe80::b255:580c:d8cc:a2a4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Fig. 4.

The command is used to display information about network interfaces and their addresses on a Linux system.

-c: This option stands for "color." It enables colorized output, making it visually more appealing and easier to distinguish different parts of the information.

-h: This option is used for human-readable output, making the information more understandable for users.

Command #3: ip -j -p route show table main

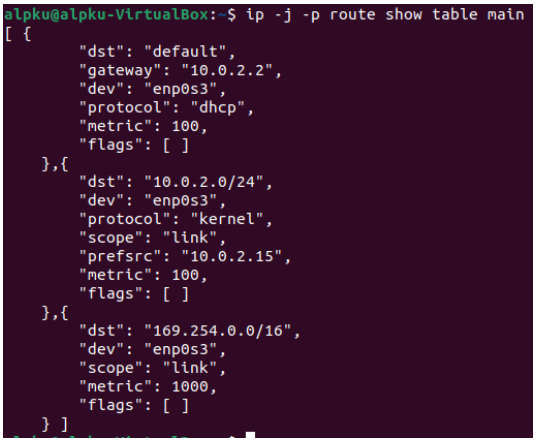

Fig. 5.

The command is used to display the routing table for the "main" table in a JSON format.

-j: This option specifies that the output should be in JSON format.

-p: The default JSON format is compact and more efficient to parse but hard for most users to read. This flag adds indentation for readability.

PART 2 – Understanding IP and Subnetting

Question 01

The IP address of the network that I am connected to is 172.21.177.47

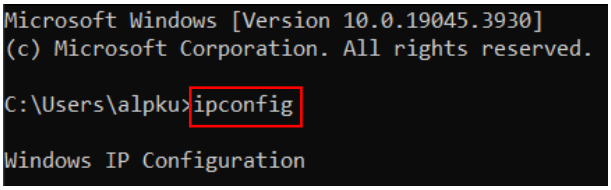

Fig. 6.

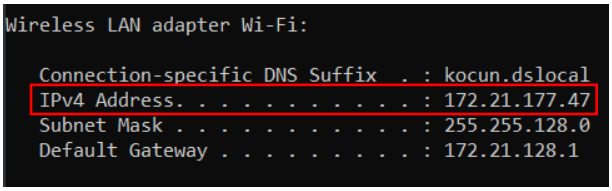

Fig. 7.

Question 02

A subnet mask is a 32-bit number that divides an IP address into network and host portions.

Question 03

Bitmask -> 11111111.11111111.10000000.00000000 (255.255.128.0)

Deriving the subnet address from IPv4 address by preserving the first 17 bits according to bitmask:

Subnet -> 172.21.128.0/17

The network address is 172.21.128.0

Question 04

The broadcast address is 172.21.255.255

Question 05

Since bitmask contains 17 leadings 1s 15 bits are reserved to the subnet.

2^{15} – 2 edge devices can be connected to the subnet as one IP address is reserved as network address and one as the broadcast address.

PART 3 – Simulations with Cisco Packet Tracer

Question 01

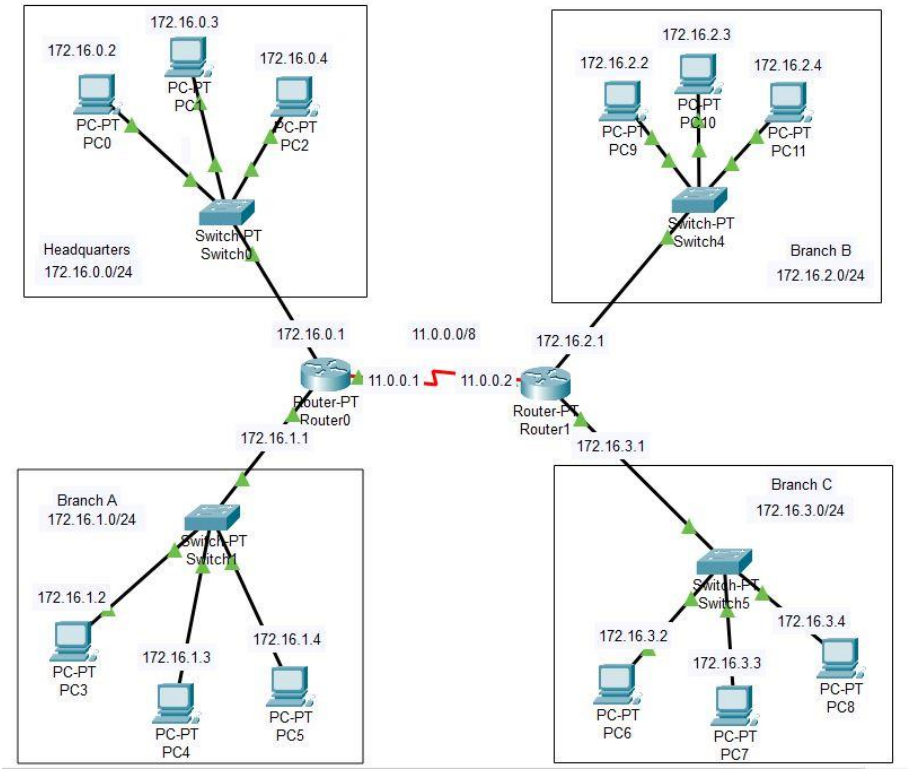

Fig. 8.

Question 02

I selected the Option III (172.16.0.0/20) because I wanted to allocate at most 16 subnets and 126 edge device addresses allocated for each of the subnet. Even though, there exist 4 subnets in the given scenario and the maximum number of edge device in a subnet is given as 30, in case of future scalability I designed the network architecture with higher allocation of resources.

Question 03

My network architecture supports up to 16 branches and each branch supports at most 126 edge devices.

21st, 22nd, 23rd, and 24th bits of the 172.16.0.0/20 IP address are allocated to branches. Therefore, the subnet mask of the branches becomes 255.255.255.0 and using these four bits up to (2^4) 16 branches can be represented. The trailing 8 bits are reserved to the addresses of the edge devices in the subnet. (2^8 – 2) 126 edge devices are supported due to the fact that one address is reserved for the network address and the one is reserved for the broadcast address.

Question 04

Process	Command
privileged EXEC mode	enable
global configuration mode	configure terminal
router interface selection	interface FastEthernet0/0
assignment of an IP address and subnet mask to an interface	ip address 172.16.1.1 255.255.255.0
move from the current configuration mode to the next higher mode	exit
configuration of a static route	ip route 172.16.2.0 255.255.255.0 11.0.0.2

Question 05

Router 01

```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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, 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 not set

C    11.0.0.0/8 is directly connected, Serial2/0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.0.0 is directly connected, FastEthernet1/0
C       172.16.1.0 is directly connected, FastEthernet0/0
S       172.16.2.0 [1/0] via 11.0.0.2
S       172.16.3.0 [1/0] via 11.0.0.2
```

Fig. 9.

Router 02

```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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, 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 not set

C    11.0.0.0/8 is directly connected, Serial2/0
     172.16.0.0/24 is subnetted, 4 subnets
S       172.16.0.0 [1/0] via 11.0.0.1
S       172.16.1.0 [1/0] via 11.0.0.1
C       172.16.2.0 is directly connected, FastEthernet0/0
C       172.16.3.0 is directly connected, FastEthernet1/0
```

Fig. 10.

Question 06

Headquarters -> Branch C

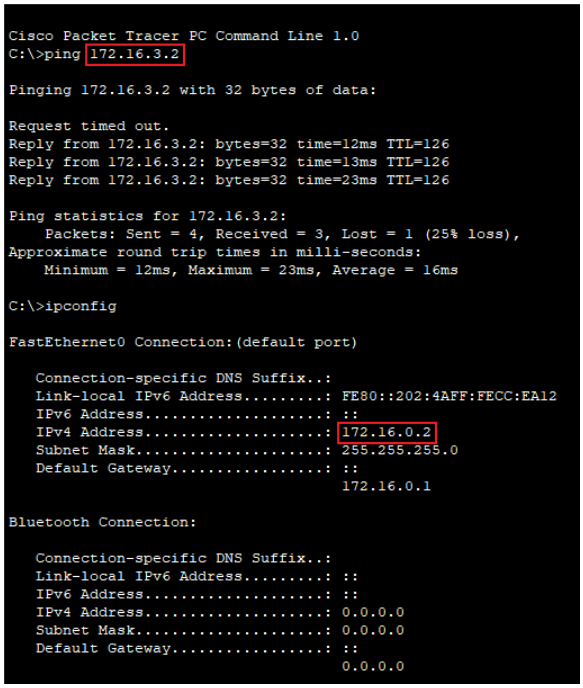

Fig. 11.

Branch A -> Branch B

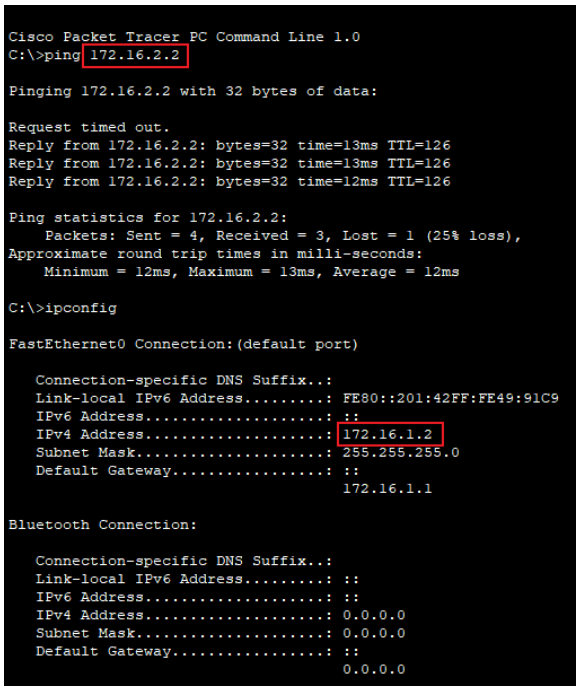

Fig. 12.

Branch B -> Branch C

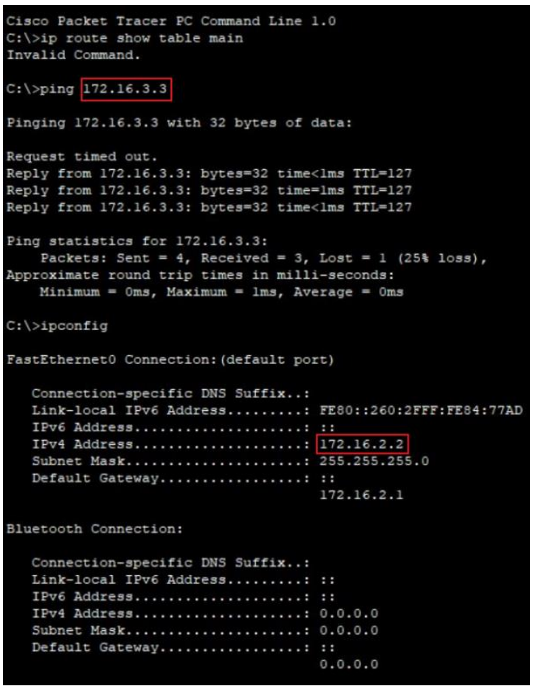

Fig. 13.

Branch C -> Branch B

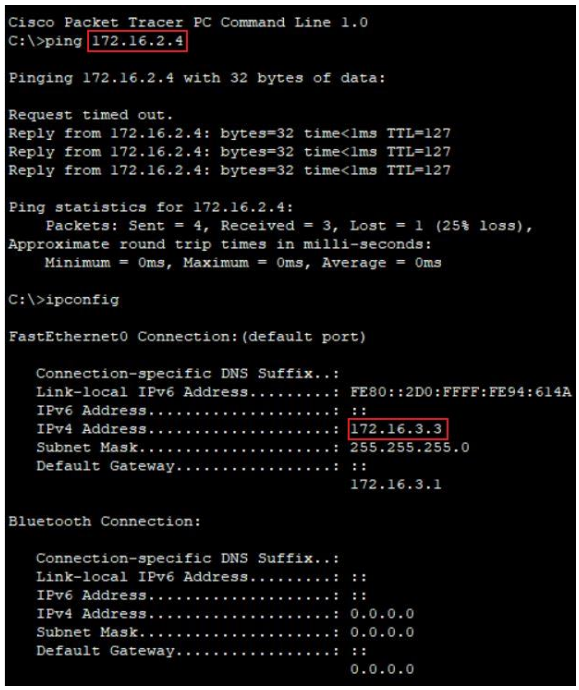

Fig. 14.