Project 1D:

Sandeep Kadagathur Vadiraj

ID: 8998-3394-34

Question 12 - (15 points) Other than the ASes shown in figure 2, there is a hidden network (AS 21) that is also connected to some of the ASes. You can use traceroutes from different ASes toward this hidden AS to infer the relationship between it and other ASes. You can also examine the BGP announcements you received as additional information. AS 21 AS and all other TA ASes have implemented no-valley and prefer-customer routing policies.

In your report, please describe (1) what are the ASes that connect to the hidden network, (2) what are the business relationship between the hidden AS and its neighbors, (3) what leads you to your answers in (1) and (2). To get full credit, you must indicate all the ASes that are connected to the hidden network. Also, notice that this hidden AS may not fall perfectly into tier1/tier2/tier3/stub categories.

Answer:

My assertion is that AS21 does not entirely fall into any of the clearly distinguished Tiers.

AS transit paths to AS21 (destination AS):

Autonomous System	**AS hop 1**	**AS hop 2**	**AS hop 3**	**AS hop 4**	**AS hop 5**	**AS hop 6**
AS 1	1	18	21			
AS 2	2	10	15	4	21	
AS 3	3	4	21			
AS 4	4	21				
AS 5	5	4	21			
AS 6	6	8	7	9	4	21
AS 7	7	9	4	21		
AS 8	8	7	9	21		
AS 9	9	4	21			
AS 10	10	15	4	21		
AS 11	11	12	4	21		
AS 12	12	4	21			
AS 13	13	18	21			
AS 14	14	5	4	21		
AS 15	15	4	21			
AS 16	16	1	18	21		
AS 17	17	15	18	21		
AS 18	18	21				
AS 19	19	21				
AS 20	20	21				

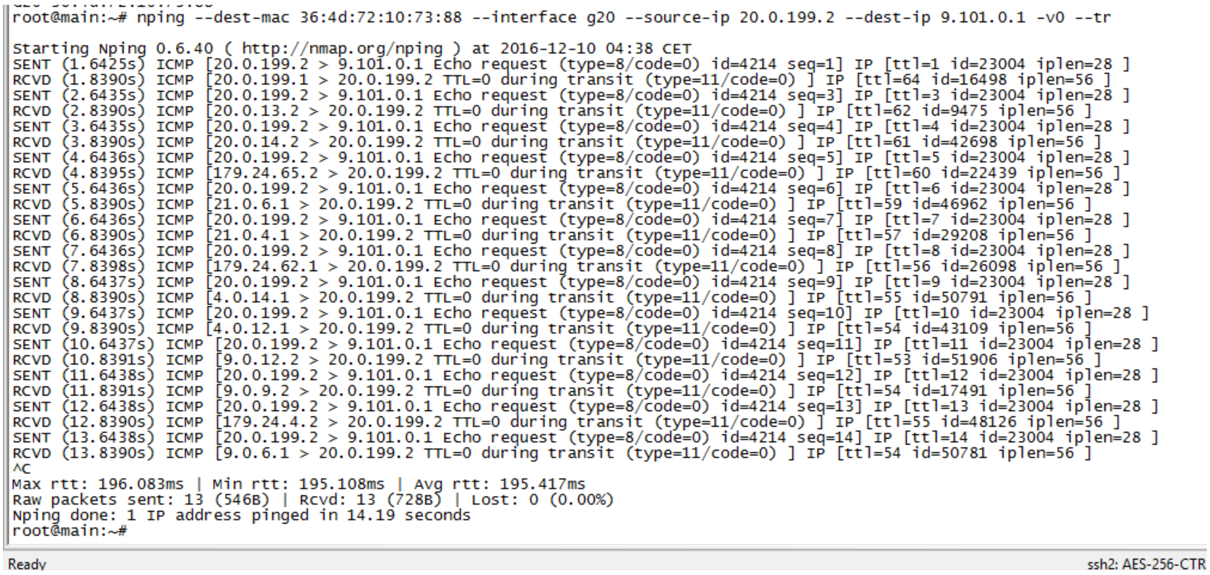
fig1

From, the above traceroute result, inference is that AS 21 has direct neighborship with AS4, AS18, AS19, and AS20. The real traceroutes are not provided so as to make the table comprehendible.

For establishing, the business relationships I use the traceroute from the AS's directly connected to the AS21 (hidden AS) and here are the results:

Autonomous System	AS hop 1	AS hop 2	AS hop 3
AS 20 to AS 4	20	21	4
AS 20 to AS 18	20	21	18
AS 20 to AS 19	20	21	19

The above example clearly shows that AS 21 is another (because we already have AS2 and AS14 as providers) **provider** for the stub AS20. Based on the BGP advertisements, the AS20 selects one of the providers. An example of traceroute is posted below:

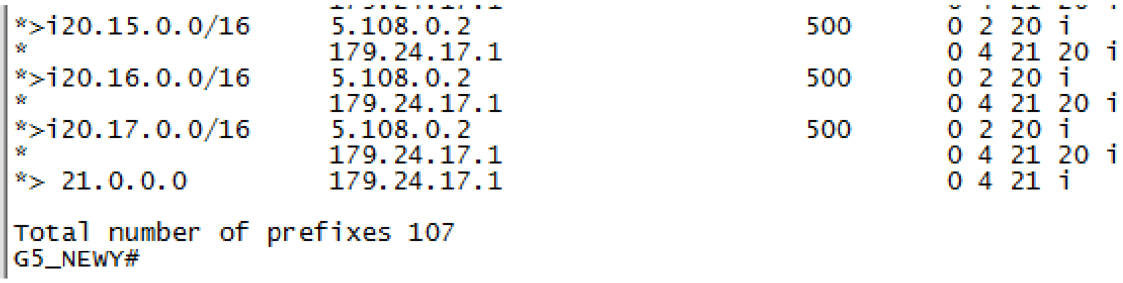


```
root@main:~# nping --dest-mac 36:4d:72:10:73:88 --interface g20 --source-ip 20.0.199.2 --dest-ip 9.101.0.1 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 04:38 CET
SENT (1.6425s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=1] IP [ttl=1 id=23004 iplen=28 ]
RCVD (1.8390s) ICMP [20.0.199.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=16498 iplen=56 ]
SENT (2.6435s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=3] IP [ttl=3 id=23004 iplen=28 ]
RCVD (2.8390s) ICMP [20.0.13.2 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=9475 iplen=56 ]
SENT (3.6435s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=4] IP [ttl=4 id=23004 iplen=28 ]
RCVD (3.8390s) ICMP [20.0.14.2 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=61 id=42698 iplen=56 ]
SENT (4.6436s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=5] IP [ttl=5 id=23004 iplen=28 ]
RCVD (4.8395s) ICMP [179.24.65.2 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=60 id=22439 iplen=56 ]
SENT (5.6436s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=6] IP [ttl=6 id=23004 iplen=28 ]
RCVD (5.8390s) ICMP [21.0.6.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=46962 iplen=56 ]
SENT (6.6436s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=7] IP [ttl=7 id=23004 iplen=28 ]
RCVD (6.8390s) ICMP [21.0.4.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=57 id=29208 iplen=56 ]
SENT (7.6436s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=8] IP [ttl=8 id=23004 iplen=28 ]
RCVD (7.8398s) ICMP [179.24.62.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=26098 iplen=56 ]
SENT (8.6437s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=9] IP [ttl=9 id=23004 iplen=28 ]
RCVD (8.8390s) ICMP [4.0.14.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=50791 iplen=56 ]
SENT (9.6437s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=10] IP [ttl=10 id=23004 iplen=28 ]
RCVD (9.8390s) ICMP [4.0.12.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=54 id=43109 iplen=56 ]
SENT (10.6437s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=11] IP [ttl=11 id=23004 iplen=28 ]
RCVD (10.8391s) ICMP [9.0.12.2 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=53 id=51906 iplen=56 ]
SENT (11.6438s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=12] IP [ttl=12 id=23004 iplen=28 ]
RCVD (11.8391s) ICMP [9.0.9.2 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=54 id=17491 iplen=56 ]
SENT (12.6438s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=13] IP [ttl=13 id=23004 iplen=28 ]
RCVD (12.8390s) ICMP [179.24.4.2 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=48126 iplen=56 ]
SENT (13.6438s) ICMP [20.0.199.2 > 9.101.0.1 Echo request (type=8/code=0) id=4214 seq=14] IP [ttl=14 id=23004 iplen=28 ]
RCVD (13.8390s) ICMP [9.0.6.1 > 20.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=54 id=50781 iplen=56 ]
^C
Max rtt: 196.083ms | Min rtt: 195.108ms | Avg rtt: 195.417ms
Raw packets sent: 13 (546B) | Rcvd: 13 (728B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 14.19 seconds
root@main:~#
```

An example of when the traffic might not flow through AS 21 would be when the destination is AS 5 and the source is AS 20.

If we see from the AS4 perspective AS21 is also acting as **customer**. "show ip bgp" command shows displays that AS21 prefix is advertised via AS4. Thereby, AS4 is **provider** also meaning AS 21 is also customer of AS4.

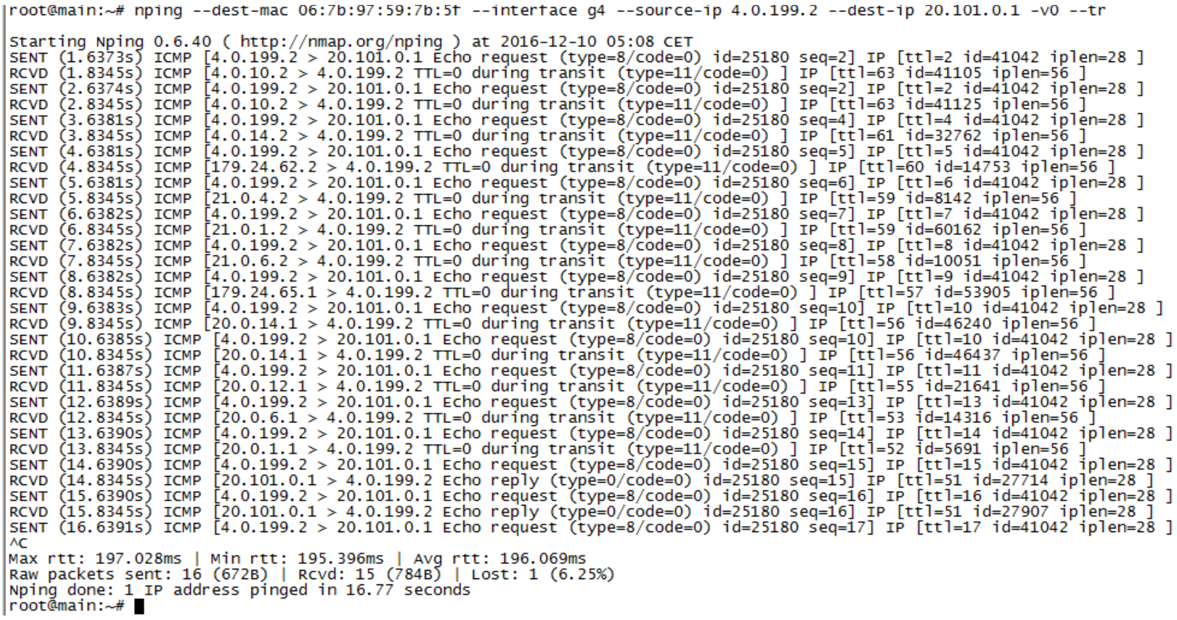


```
*>i20.15.0.0/16     5.108.0.2                      500      0 2 20 i
*                   179.24.17.1                             0 4 21 20 i
*>i20.16.0.0/16     5.108.0.2                      500      0 2 20 i
*                   179.24.17.1                             0 4 21 20 i
*>i20.17.0.0/16     5.108.0.2                      500      0 2 20 i
*                   179.24.17.1                             0 4 21 20 i
*> 21.0.0.0         179.24.17.1                             0 4 21 i

Total number of prefixes 107
G5_NEWY#
```

Another, way to verify this is to look at the tracerouting table attached above (fig1). When I issue a traceroute from my AS5 to AS21 path taken is AS5-AS4-AS21 . Thus, AS21 is also behaving as customer in some cases. AS21 also acts as a provider for AS20. If I traceroute from the AS4 to AS20 the path is via AS21. This shows that AS21 is also acting as provider. Thus, we can conclude that AS21 is basically a **transit AS** bridging between multiple tiers of AS's.

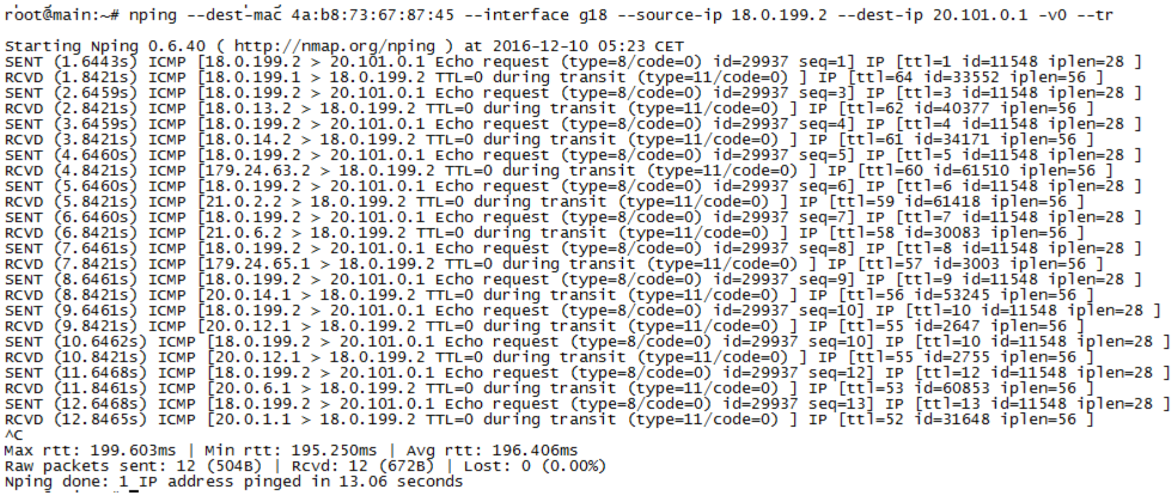
Traceroute from AS4 to AS20 shows AS21 as provider of AS20:



```
root@main:~# nping --dest-mac 06:7b:97:59:7b:5f --interface g4 --source-ip 4.0.199.2 --dest-ip 20.101.0.1 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 05:08 CET
SENT (1.6373s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=2] IP [ttl=2 id=41042 iplen=28 ]
RCVD (1.8345s) ICMP [4.0.10.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=63 id=41105 iplen=56 ]
SENT (2.6374s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=2] IP [ttl=2 id=41042 iplen=28 ]
RCVD (2.8345s) ICMP [4.0.10.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=63 id=41125 iplen=56 ]
SENT (3.6381s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=4] IP [ttl=4 id=41042 iplen=28 ]
RCVD (3.8345s) ICMP [4.0.14.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=61 id=32762 iplen=56 ]
SENT (4.6381s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=5] IP [ttl=5 id=41042 iplen=28 ]
RCVD (4.8345s) ICMP [179.24.62.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=60 id=14753 iplen=56 ]
SENT (5.6381s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=6] IP [ttl=6 id=41042 iplen=28 ]
RCVD (5.8345s) ICMP [21.0.4.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=8142 iplen=56 ]
SENT (6.6382s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=7] IP [ttl=7 id=41042 iplen=28 ]
RCVD (6.8345s) ICMP [21.0.1.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=60162 iplen=56 ]
SENT (7.6382s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=8] IP [ttl=8 id=41042 iplen=28 ]
RCVD (7.8345s) ICMP [21.0.6.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=10051 iplen=56 ]
SENT (8.6382s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=9] IP [ttl=9 id=41042 iplen=28 ]
RCVD (8.8345s) ICMP [179.24.65.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=57 id=53905 iplen=56 ]
SENT (9.6383s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=10] IP [ttl=10 id=41042 iplen=28 ]
RCVD (9.8345s) ICMP [20.0.14.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=46240 iplen=56 ]
SENT (10.6385s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=10] IP [ttl=10 id=41042 iplen=28 ]
RCVD (10.8345s) ICMP [20.0.14.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=46437 iplen=56 ]
SENT (11.6387s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=11] IP [ttl=11 id=41042 iplen=28 ]
RCVD (11.8345s) ICMP [20.0.12.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=21641 iplen=56 ]
SENT (12.6389s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=13] IP [ttl=13 id=41042 iplen=28 ]
RCVD (12.8345s) ICMP [20.0.6.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=53 id=14316 iplen=56 ]
SENT (13.6390s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=14] IP [ttl=14 id=41042 iplen=28 ]
RCVD (13.8345s) ICMP [20.0.1.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=52 id=5691 iplen=56 ]
SENT (14.6390s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=15] IP [ttl=15 id=41042 iplen=28 ]
RCVD (14.8345s) ICMP [20.101.0.1 > 4.0.199.2 Echo reply (type=0/code=0) id=25180 seq=15] IP [ttl=51 id=27714 iplen=28 ]
SENT (15.6390s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=16] IP [ttl=16 id=41042 iplen=28 ]
RCVD (15.8345s) ICMP [20.101.0.1 > 4.0.199.2 Echo reply (type=0/code=0) id=25180 seq=16] IP [ttl=51 id=27907 iplen=28 ]
SENT (16.6391s) ICMP [4.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=25180 seq=17] IP [ttl=17 id=41042 iplen=28 ]
^C
Max rtt: 197.028ms | Min rtt: 195.396ms | Avg rtt: 196.069ms
Raw packets sent: 16 (672B) | Rcvd: 15 (784B) | Lost: 1 (6.25%)
Nping done: 1 IP address pinged in 16.77 seconds
root@main:~# █
```

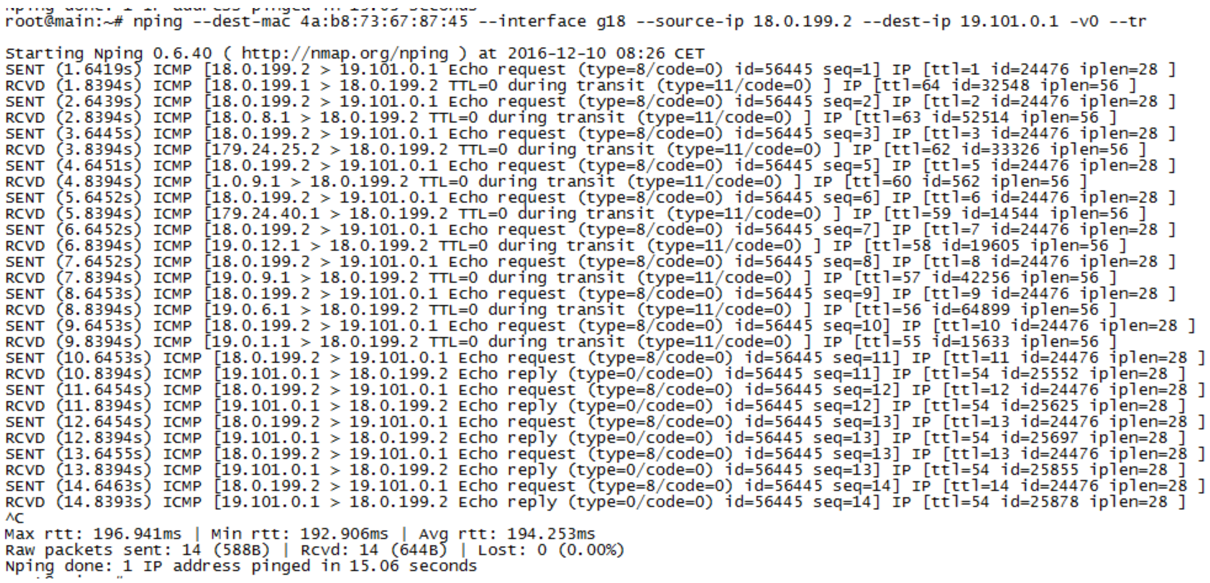
Traceroute to AS20 from AS16 shows that AS21 is acting as provider for AS20 and also as peer/provider for AS18.



```
root@main:~# nping --dest-mac 4a:b8:73:67:87:45 --interface g18 --source-ip 18.0.199.2 --dest-ip 20.101.0.1 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 05:23 CET
SENT (1.6443s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=1] IP [ttl=1 id=11548 iplen=28 ]
RCVD (1.8421s) ICMP [18.0.199.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=33552 iplen=56 ]
SENT (2.6459s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=3] IP [ttl=3 id=11548 iplen=28 ]
RCVD (2.8421s) ICMP [18.0.13.2 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=40377 iplen=56 ]
SENT (3.6459s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=4] IP [ttl=4 id=11548 iplen=28 ]
RCVD (3.8421s) ICMP [18.0.14.2 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=61 id=34171 iplen=56 ]
SENT (4.6460s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=5] IP [ttl=5 id=11548 iplen=28 ]
RCVD (4.8421s) ICMP [179.24.63.2 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=60 id=61510 iplen=56 ]
SENT (5.6460s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=6] IP [ttl=6 id=11548 iplen=28 ]
RCVD (5.8421s) ICMP [21.0.2.2 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=61418 iplen=56 ]
SENT (6.6460s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=7] IP [ttl=7 id=11548 iplen=28 ]
RCVD (6.8421s) ICMP [21.0.6.2 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=30083 iplen=56 ]
SENT (7.6461s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=8] IP [ttl=8 id=11548 iplen=28 ]
RCVD (7.8421s) ICMP [179.24.65.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=57 id=3003 iplen=56 ]
SENT (8.6461s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=9] IP [ttl=9 id=11548 iplen=28 ]
RCVD (8.8421s) ICMP [20.0.14.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=53245 iplen=56 ]
SENT (9.6461s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=10] IP [ttl=10 id=11548 iplen=28 ]
RCVD (9.8421s) ICMP [20.0.12.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=2647 iplen=56 ]
SENT (10.6462s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=10] IP [ttl=10 id=11548 iplen=28 ]
RCVD (10.8421s) ICMP [20.0.12.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=2755 iplen=56 ]
SENT (11.6468s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=12] IP [ttl=12 id=11548 iplen=28 ]
RCVD (11.8461s) ICMP [20.0.6.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=53 id=60853 iplen=56 ]
SENT (12.6468s) ICMP [18.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=29937 seq=13] IP [ttl=13 id=11548 iplen=28 ]
RCVD (12.8465s) ICMP [20.0.1.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=52 id=31648 iplen=56 ]
^C
Max rtt: 199.603ms | Min rtt: 195.250ms | Avg rtt: 196.406ms
Raw packets sent: 12 (504B) | Rcvd: 12 (672B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 13.06 seconds
```

Now, the decision is whether the AS18 is *peer or provider* of AS20. To make a conclusion, issue the traceroute from AS18 to AS19. If it is provider then the path must pass through AS21 else, we can say that AS18 is a peer of AS21.

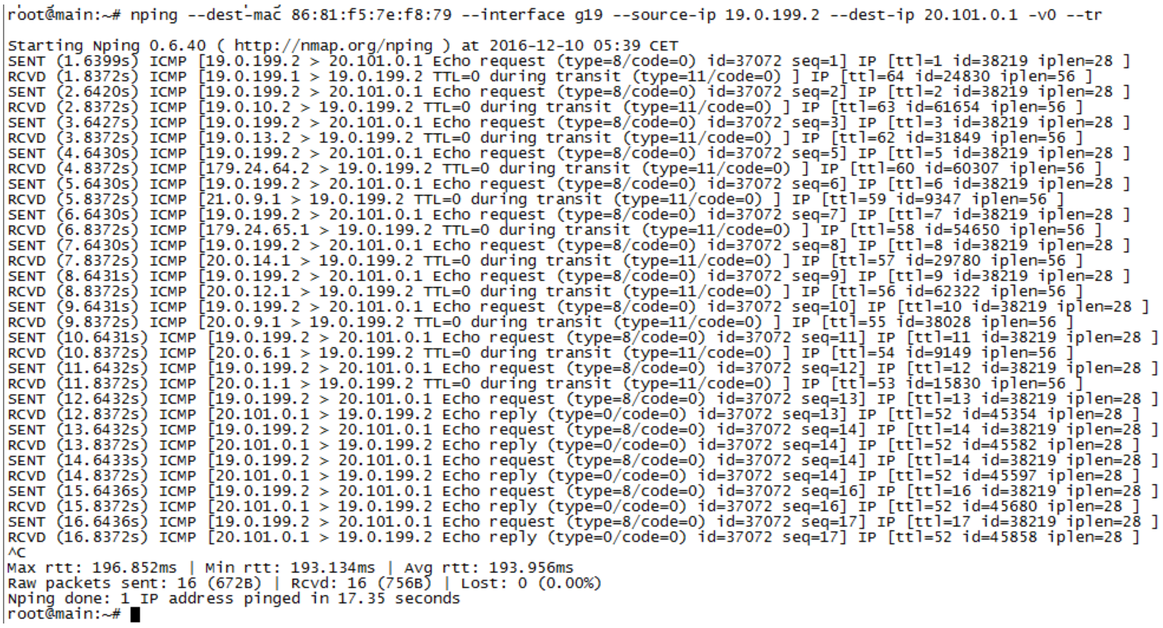


```
root@main:~# nping --dest-mac 4a:b8:73:67:87:45 --interface g18 --source-ip 18.0.199.2 --dest-ip 19.101.0.1 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 08:26 CET
SENT (1.6419s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=1] IP [ttl=1 id=24476 iplen=28 ]
RCVD (1.8394s) ICMP [18.0.199.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=32548 iplen=56 ]
SENT (2.6439s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=2] IP [ttl=2 id=24476 iplen=28 ]
RCVD (2.8394s) ICMP [18.0.8.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=63 id=52514 iplen=56 ]
SENT (3.6445s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=3] IP [ttl=3 id=24476 iplen=28 ]
RCVD (3.8394s) ICMP [179.24.25.2 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=33326 iplen=56 ]
SENT (4.6451s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=5] IP [ttl=5 id=24476 iplen=28 ]
RCVD (4.8394s) ICMP [1.0.9.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=60 id=562 iplen=56 ]
SENT (5.6452s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=6] IP [ttl=6 id=24476 iplen=28 ]
RCVD (5.8394s) ICMP [179.24.40.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=14544 iplen=56 ]
SENT (6.6452s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=7] IP [ttl=7 id=24476 iplen=28 ]
RCVD (6.8394s) ICMP [19.0.12.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=19605 iplen=56 ]
SENT (7.6452s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=8] IP [ttl=8 id=24476 iplen=28 ]
RCVD (7.8394s) ICMP [19.0.9.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=57 id=42256 iplen=56 ]
SENT (8.6453s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=9] IP [ttl=9 id=24476 iplen=28 ]
RCVD (8.8394s) ICMP [19.0.6.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=64899 iplen=56 ]
SENT (9.6453s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=10] IP [ttl=10 id=24476 iplen=28 ]
RCVD (9.8394s) ICMP [19.0.1.1 > 18.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=15633 iplen=56 ]
SENT (10.6453s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=11] IP [ttl=11 id=24476 iplen=28 ]
RCVD (10.8394s) ICMP [19.101.0.1 > 18.0.199.2 Echo reply (type=0/code=0) id=56445 seq=11] IP [ttl=54 id=25552 iplen=28 ]
SENT (11.6454s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=12] IP [ttl=12 id=24476 iplen=28 ]
RCVD (11.8394s) ICMP [19.101.0.1 > 18.0.199.2 Echo reply (type=0/code=0) id=56445 seq=12] IP [ttl=54 id=25625 iplen=28 ]
SENT (12.6454s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=13] IP [ttl=13 id=24476 iplen=28 ]
RCVD (12.8394s) ICMP [19.101.0.1 > 18.0.199.2 Echo reply (type=0/code=0) id=56445 seq=13] IP [ttl=54 id=25697 iplen=28 ]
SENT (13.6455s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=13] IP [ttl=13 id=24476 iplen=28 ]
RCVD (13.8394s) ICMP [19.101.0.1 > 18.0.199.2 Echo reply (type=0/code=0) id=56445 seq=13] IP [ttl=54 id=25855 iplen=28 ]
SENT (14.6463s) ICMP [18.0.199.2 > 19.101.0.1 Echo request (type=8/code=0) id=56445 seq=14] IP [ttl=14 id=24476 iplen=28 ]
RCVD (14.8393s) ICMP [19.101.0.1 > 18.0.199.2 Echo reply (type=0/code=0) id=56445 seq=14] IP [ttl=54 id=25878 iplen=28 ]
^C
Max rtt: 196.941ms | Min rtt: 192.906ms | Avg rtt: 194.253ms
Raw packets sent: 14 (588B) | Rcvd: 14 (644B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 15.06 seconds
```

This concludes that AS18 is a **peer** of AS21.

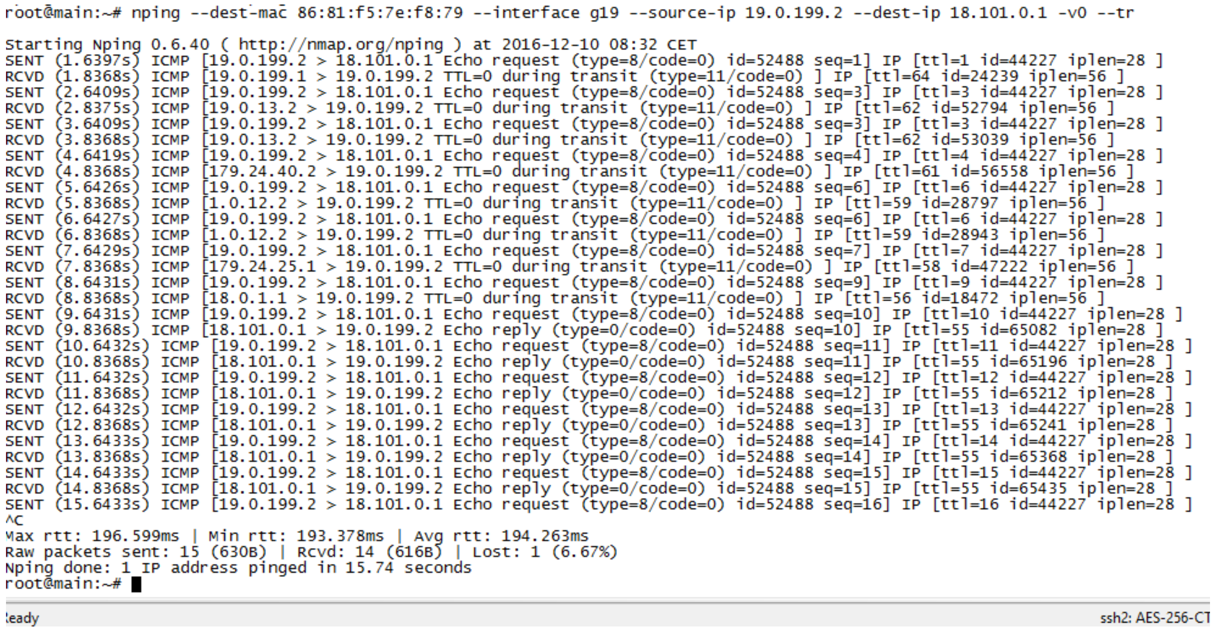
For AS19 the AS21 is a provider, this is by the fact that AS19 is a stub AS and do not advertise the customers. But, our network violates the standard stub rule. So, the evidence for this is the traceroute from AS19 to AS20 passes through AS21. So AS21 again can be peer or provider as in the above case. To draw the inference we issue the traceroute to another AS18 which is directly connected to AS21.



```
root@main:~# nping --dest-mac 86:81:f5:7e:f8:79 --interface g19 --source-ip 19.0.199.2 --dest-ip 20.101.0.1 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 05:39 CET
SENT (1.6399s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=1] IP [ttl=1 id=38219 iplen=28 ]
RCVD (1.8372s) ICMP [19.0.199.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=24830 iplen=56 ]
SENT (2.6420s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=2] IP [ttl=2 id=38219 iplen=28 ]
RCVD (2.8372s) ICMP [19.0.10.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=63 id=61654 iplen=56 ]
SENT (3.6427s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=3] IP [ttl=3 id=38219 iplen=28 ]
RCVD (3.8372s) ICMP [19.0.13.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=31849 iplen=56 ]
SENT (4.6430s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=5] IP [ttl=5 id=38219 iplen=28 ]
RCVD (4.8372s) ICMP [179.24.64.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=60 id=60307 iplen=56 ]
SENT (5.6430s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=6] IP [ttl=6 id=38219 iplen=28 ]
RCVD (5.8372s) ICMP [21.0.9.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=9347 iplen=56 ]
SENT (6.6430s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=7] IP [ttl=7 id=38219 iplen=28 ]
RCVD (6.8372s) ICMP [179.24.65.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=54650 iplen=56 ]
SENT (7.6430s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=8] IP [ttl=8 id=38219 iplen=28 ]
RCVD (7.8372s) ICMP [20.0.14.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=57 id=29780 iplen=56 ]
SENT (8.6431s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=9] IP [ttl=9 id=38219 iplen=28 ]
RCVD (8.8372s) ICMP [20.0.12.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=62322 iplen=56 ]
SENT (9.6431s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=10] IP [ttl=10 id=38219 iplen=28 ]
RCVD (9.8372s) ICMP [20.0.9.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=55 id=38028 iplen=56 ]
SENT (10.6431s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=11] IP [ttl=11 id=38219 iplen=28 ]
RCVD (10.8372s) ICMP [20.0.6.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=54 id=9149 iplen=56 ]
SENT (11.6432s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=12] IP [ttl=12 id=38219 iplen=28 ]
RCVD (11.8372s) ICMP [20.0.1.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=53 id=15830 iplen=56 ]
SENT (12.6432s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=13] IP [ttl=13 id=38219 iplen=28 ]
RCVD (12.8372s) ICMP [20.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=37072 seq=13] IP [ttl=52 id=45354 iplen=28 ]
SENT (13.6432s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=14] IP [ttl=14 id=38219 iplen=28 ]
RCVD (13.8372s) ICMP [20.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=37072 seq=14] IP [ttl=52 id=45582 iplen=28 ]
SENT (14.6433s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=14] IP [ttl=14 id=38219 iplen=28 ]
RCVD (14.8372s) ICMP [20.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=37072 seq=14] IP [ttl=52 id=45597 iplen=28 ]
SENT (15.6436s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=16] IP [ttl=16 id=38219 iplen=28 ]
RCVD (15.8372s) ICMP [20.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=37072 seq=16] IP [ttl=52 id=45680 iplen=28 ]
SENT (16.6436s) ICMP [19.0.199.2 > 20.101.0.1 Echo request (type=8/code=0) id=37072 seq=17] IP [ttl=17 id=38219 iplen=28 ]
RCVD (16.8372s) ICMP [20.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=37072 seq=17] IP [ttl=52 id=45858 iplen=28 ]
^C
Max rtt: 196.852ms | Min rtt: 193.134ms | Avg rtt: 193.956ms
Raw packets sent: 16 (672B) | Rcvd: 16 (756B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 17.35 seconds
root@main:~# █
```

The traceroute result below shows the AS19 to AS18 relationship:



```
root@main:~# nping --dest-mac 86:81:f5:7e:f8:79 --interface g19 --source-ip 19.0.199.2 --dest-ip 18.101.0.1 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 08:32 CET
SENT (1.6397s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=1] IP [ttl=1 id=44227 iplen=28 ]
RCVD (1.8368s) ICMP [19.0.199.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=24239 iplen=56 ]
SENT (2.6409s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=3] IP [ttl=3 id=44227 iplen=28 ]
RCVD (2.8375s) ICMP [19.0.13.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=52794 iplen=56 ]
SENT (3.6409s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=3] IP [ttl=3 id=44227 iplen=28 ]
RCVD (3.8368s) ICMP [19.0.13.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=62 id=53039 iplen=56 ]
SENT (4.6419s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=4] IP [ttl=4 id=44227 iplen=28 ]
RCVD (4.8368s) ICMP [179.24.40.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=61 id=56558 iplen=56 ]
SENT (5.6426s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=6] IP [ttl=6 id=44227 iplen=28 ]
RCVD (5.8368s) ICMP [1.0.12.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=28797 iplen=56 ]
SENT (6.6427s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=6] IP [ttl=6 id=44227 iplen=28 ]
RCVD (6.8368s) ICMP [1.0.12.2 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=28943 iplen=56 ]
SENT (7.6429s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=7] IP [ttl=7 id=44227 iplen=28 ]
RCVD (7.8368s) ICMP [179.24.25.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=47222 iplen=56 ]
SENT (8.6431s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=9] IP [ttl=9 id=44227 iplen=28 ]
RCVD (8.8368s) ICMP [18.0.1.1 > 19.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=56 id=18472 iplen=56 ]
SENT (9.6431s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=10] IP [ttl=10 id=44227 iplen=28 ]
RCVD (9.8368s) ICMP [18.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=52488 seq=10] IP [ttl=55 id=65082 iplen=28 ]
SENT (10.6432s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=11] IP [ttl=11 id=44227 iplen=28 ]
RCVD (10.8368s) ICMP [18.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=52488 seq=11] IP [ttl=55 id=65196 iplen=28 ]
SENT (11.6432s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=12] IP [ttl=12 id=44227 iplen=28 ]
RCVD (11.8368s) ICMP [18.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=52488 seq=12] IP [ttl=55 id=65212 iplen=28 ]
SENT (12.6432s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=13] IP [ttl=13 id=44227 iplen=28 ]
RCVD (12.8368s) ICMP [18.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=52488 seq=13] IP [ttl=55 id=65241 iplen=28 ]
SENT (13.6433s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=14] IP [ttl=14 id=44227 iplen=28 ]
RCVD (13.8368s) ICMP [18.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=52488 seq=14] IP [ttl=55 id=65368 iplen=28 ]
SENT (14.6433s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=15] IP [ttl=15 id=44227 iplen=28 ]
RCVD (14.8368s) ICMP [18.101.0.1 > 19.0.199.2 Echo reply (type=0/code=0) id=52488 seq=15] IP [ttl=55 id=65435 iplen=28 ]
SENT (15.6433s) ICMP [19.0.199.2 > 18.101.0.1 Echo request (type=8/code=0) id=52488 seq=16] IP [ttl=16 id=44227 iplen=28 ]
^C
Max rtt: 196.599ms | Min rtt: 193.378ms | Avg rtt: 194.263ms
Raw packets sent: 15 (630B) | Rcvd: 14 (616B) | Lost: 1 (6.67%)
Nping done: 1 IP address pinged in 15.74 seconds
root@main:~# █
```

Again, the path is not via AS21 and therefore as in the previous case we prove that AS19 is **peer** for the AS21.

Thus, in summary the business relationships are and evidence that lead me to my conclusion:

Autonomous System	**Business Relationship with AS21**	**Evidence**
AS 20	Is a customer	Traceroute to any other BGP peer of AS21 passes through AS21
AS 4	Is a provider	1. show ip bgp table and 2. Trace Path from AS5 to AS20 goes via AS21
AS 18	Is a peer	1. Trace route from AS16 to AS20 goes via AS21 2. Traceroute to AS19 is not via AS21 (as that would indicate provider)
AS 19	Is a peer	1. Trace route from AS19 to AS20 goes via AS21 2. Traceroute to AS18 is not via AS21 (as that would indicate provider)

As described in the question it does not strictly fall into any particular AS tier category. It appears as a transit AS for different tiers.

Question 13 - (15 points) For this question, you will study the impact of prefix hijacking. You are allowed to hijack one or more prefixes within the subnets 4.X.0.0/16, 10.X.0.0/16, 18.X.0.0/16, 19.X.0.0/16, 20.X.0.0/16, with X being your AS number. AS 4/10/18/19/20 will also advertise the corresponding /16 prefixes at the same time; they are considered to be the valid owners of the ASes.

Important: DO NOT hijack any prefixes that is not listed above. You will receive penalty on the project if you do that.

Use traceroutes from different ASes to the destinations that you hijacked to verify that you can intercept some traffic successfully.

In your report, please describe (1) what are the prefixes that you hijacked and where do you make these hijacking announcements, (2) the evidences to support that you have successfully hijacked some traffic, (3) explanation about how to interpret the evidence. Also, discuss (4) whether your hijacking attack captures the traffic to the hijacked prefix(es) from all ASes. If yes, why is that? If no, what are the cases you fail (illustrate with real traceroute examples)? What are the cases you succeed? Be sure to list every AS as either failed or successful. And what is the reason for such difference?

Solution:

1.

I am hijacking AS4 and the prefix that I have hijacked from AS4 is 4.5.5.0/24. I am making the announcements from my SEAT routers. The commands that I used were:

router bgp 5

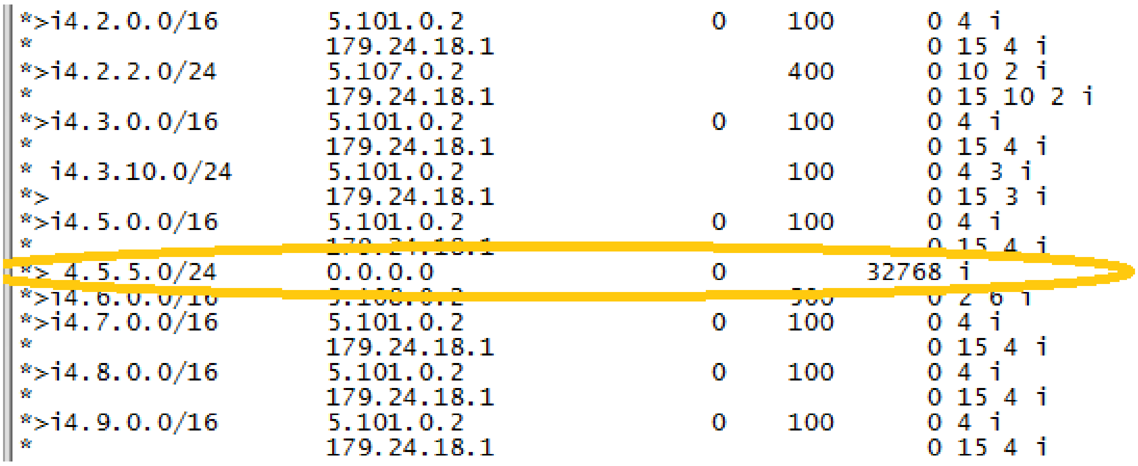
network 4.5.5.0/24

access-list 20 permit 4.5.5.0 0.0.0.255

This access-list is tagged with the community of 5:20 and already permitted in the route-map to be advertised.

2.

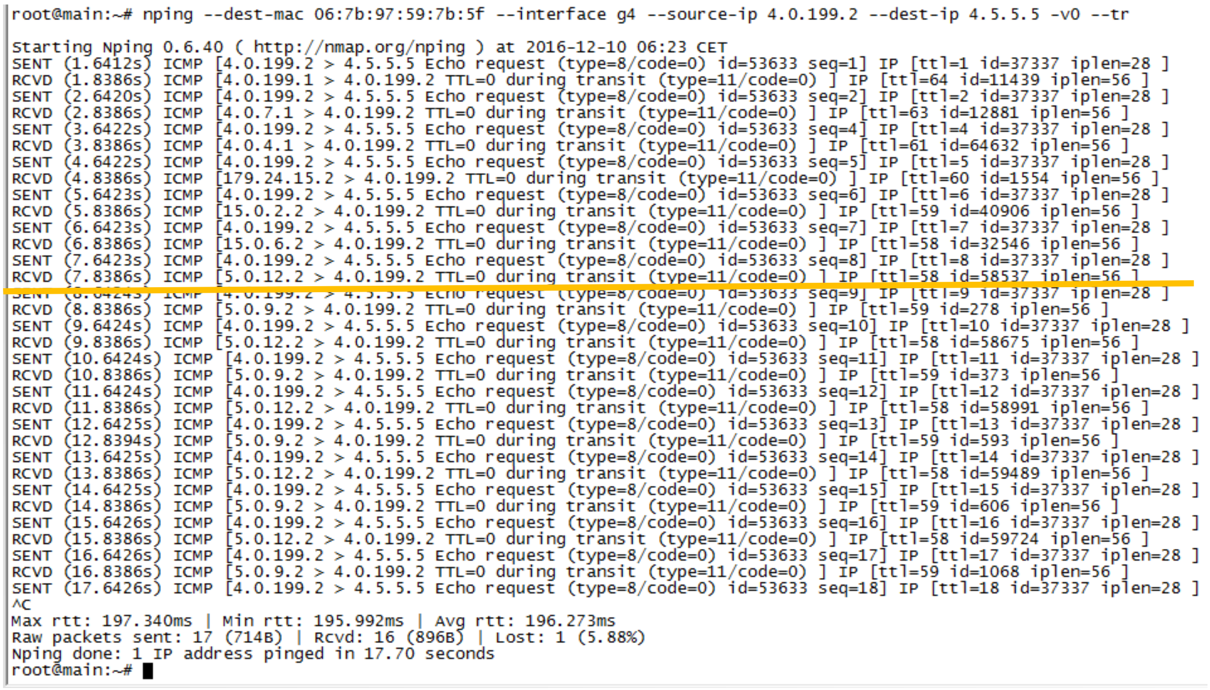
On SEAT show ip bgp command resulted in this-



```
*>i4.2.0.0/16       5.101.0.2           0    100      0 4 i
*                   179.24.18.1                       0 15 4 i
*>i4.2.2.0/24       5.107.0.2                400      0 10 2 i
*                   179.24.18.1                       0 15 10 2 i
*>i4.3.0.0/16       5.101.0.2           0    100      0 4 i
*                   179.24.18.1                       0 15 4 i
*  i4.3.10.0/24     5.101.0.2                100      0 4 3 i
*>                  179.24.18.1                       0 15 3 i
*>i4.5.0.0/16       5.101.0.2           0    100      0 4 i
*                   179.24.18.1                       0 15 4 i
*> 4.5.5.0/24       0.0.0.0             0         32768 i
*>i4.6.0.0/16       5.108.0.2                300      0 2 6 i
*>i4.7.0.0/16       5.101.0.2           0    100      0 4 i
*                   179.24.18.1                       0 15 4 i
*>i4.8.0.0/16       5.101.0.2           0    100      0 4 i
*                   179.24.18.1                       0 15 4 i
*>i4.9.0.0/16       5.101.0.2           0    100      0 4 i
*                   179.24.18.1                       0 15 4 i
```

The 4.5.5.0/24 is displayed with an internal (i), meaning that this AS is the originator of the prefix.

The traceroute from the AS4:



```
root@main:~# nping --dest-mac 06:7b:97:59:7b:5f --interface g4 --source-ip 4.0.199.2 --dest-ip 4.5.5.5 -v0 --tr

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2016-12-10 06:23 CET
SENT (1.6412s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=1] IP [ttl=1 id=37337 iplen=28 ]
RCVD (1.8386s) ICMP [4.0.199.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=64 id=11439 iplen=56 ]
SENT (2.6420s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=2] IP [ttl=2 id=37337 iplen=28 ]
RCVD (2.8386s) ICMP [4.0.7.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=63 id=12881 iplen=56 ]
SENT (3.6422s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=4] IP [ttl=4 id=37337 iplen=28 ]
RCVD (3.8386s) ICMP [4.0.4.1 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=61 id=64632 iplen=56 ]
SENT (4.6422s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=5] IP [ttl=5 id=37337 iplen=28 ]
RCVD (4.8386s) ICMP [179.24.15.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=60 id=1554 iplen=56 ]
SENT (5.6423s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=6] IP [ttl=6 id=37337 iplen=28 ]
RCVD (5.8386s) ICMP [15.0.2.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=40906 iplen=56 ]
SENT (6.6423s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=7] IP [ttl=7 id=37337 iplen=28 ]
RCVD (6.8386s) ICMP [15.0.6.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=32546 iplen=56 ]
SENT (7.6423s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=8] IP [ttl=8 id=37337 iplen=28 ]
RCVD (7.8386s) ICMP [5.0.12.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=58537 iplen=56 ]
SENT (8.6424s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=9] IP [ttl=9 id=37337 iplen=28 ]
RCVD (8.8386s) ICMP [5.0.9.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=278 iplen=56 ]
SENT (9.6424s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=10] IP [ttl=10 id=37337 iplen=28 ]
RCVD (9.8386s) ICMP [5.0.12.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=58675 iplen=56 ]
SENT (10.6424s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=11] IP [ttl=11 id=37337 iplen=28 ]
RCVD (10.8386s) ICMP [5.0.9.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=373 iplen=56 ]
SENT (11.6424s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=12] IP [ttl=12 id=37337 iplen=28 ]
RCVD (11.8386s) ICMP [5.0.12.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=58991 iplen=56 ]
SENT (12.6425s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=13] IP [ttl=13 id=37337 iplen=28 ]
RCVD (12.8394s) ICMP [5.0.9.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=593 iplen=56 ]
SENT (13.6425s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=14] IP [ttl=14 id=37337 iplen=28 ]
RCVD (13.8386s) ICMP [5.0.12.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=59489 iplen=56 ]
SENT (14.6425s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=15] IP [ttl=15 id=37337 iplen=28 ]
RCVD (14.8386s) ICMP [5.0.9.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=606 iplen=56 ]
SENT (15.6426s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=16] IP [ttl=16 id=37337 iplen=28 ]
RCVD (15.8386s) ICMP [5.0.12.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=58 id=59724 iplen=56 ]
SENT (16.6426s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=17] IP [ttl=17 id=37337 iplen=28 ]
RCVD (16.8386s) ICMP [5.0.9.2 > 4.0.199.2 TTL=0 during transit (type=11/code=0) ] IP [ttl=59 id=1068 iplen=56 ]
SENT (17.6426s) ICMP [4.0.199.2 > 4.5.5.5 Echo request (type=8/code=0) id=53633 seq=18] IP [ttl=18 id=37337 iplen=28 ]
^C
Max rtt: 197.340ms | Min rtt: 195.992ms | Avg rtt: 196.273ms
Raw packets sent: 17 (714B) | Rcvd: 16 (896B) | Lost: 1 (5.88%)
Nping done: 1 IP address pinged in 17.70 seconds
root@main:~# █
```

The transit is happening to the AS5 network or network from where the false advertisement originated.

This is true for all the AS’s. Please find all the traceroute results showing the transit for the 4.5.5.0/24 prefix happens via AS5. The above traceroute concludes that the longest prefix match (/24) over rules the prefix (/16) even on the originator of AS4 prefix for the falsified prefix originated from AS5.

All the traceroute results for the 4.5.5.0/24 is provided in an additional file as evidence.

4.

Please see the other file for all the traceroute results in the zipped folder.

As per the evidence provided in the additional file my prefix hijacked is advertised to all the routers because, I am advertising only a sub prefix of what I am supposed to advertise and not competing with any other routing advertisement. Thus, only longest prefix match rule is applied and the hijacking works.