BGP Bogon Defender

Team #7

Problem

```
                                   My traceroute  [v0.85]
XJTU-Lab-400-Ubuntu-Common (0.0.0.0)                                   Wed Dec  9 15:42:48 2015
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                          Packets               Pings
 Host                                                    Loss%   Snt   Last   Avg  Best  Wrst StdDev
 1.                                                       4.2%   120    0.8   1.1   0.7   6.4   0.7
 2.                                                       0.0%   120    2.9   2.2   1.7   8.8   0.9
 3.                                                       0.0%   120    0.5   1.1   0.4   5.7   0.7
 4.                                                       0.0%   120    0.4   2.6   0.4 220.0  20.1
 5. AS???    10.6.12.66                                   0.0%   120    0.5   0.5   0.3   2.9   0.3
 6. AS4837   113.200.58.65                               0.0%   120    1.3   1.6   1.3   8.3   0.7
 7. AS???    172.22.94.41                                 0.0%   120    7.0   7.8   2.4  14.5   1.3
 8. AS4837   123.139.2.137                                0.0%   119   25.6  40.7  17.1  75.7  13.3
 9. AS4837   221.11.0.37                                 57.1%   119   24.7  38.8  19.9  67.1  12.4
10. AS4837   219.158.24.253                               0.0%   119   71.2  85.7  62.5 126.8  14.4
11. AS4837   219.158.100.197                              2.5%   119   94.2 103.7  80.6 236.8  17.5
12. AS4565   192.168.1.2                                  0.0%   119  101.5 108.8  87.0 230.2  16.2
```

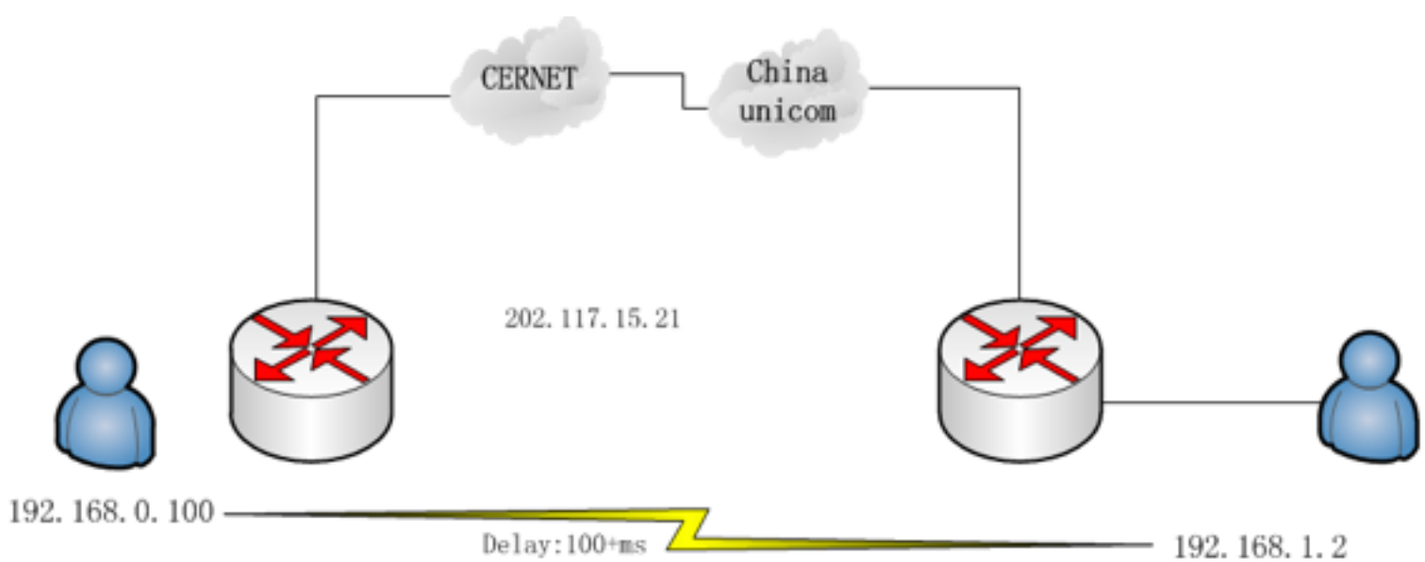
Local

ChinaUnicom

Unkown

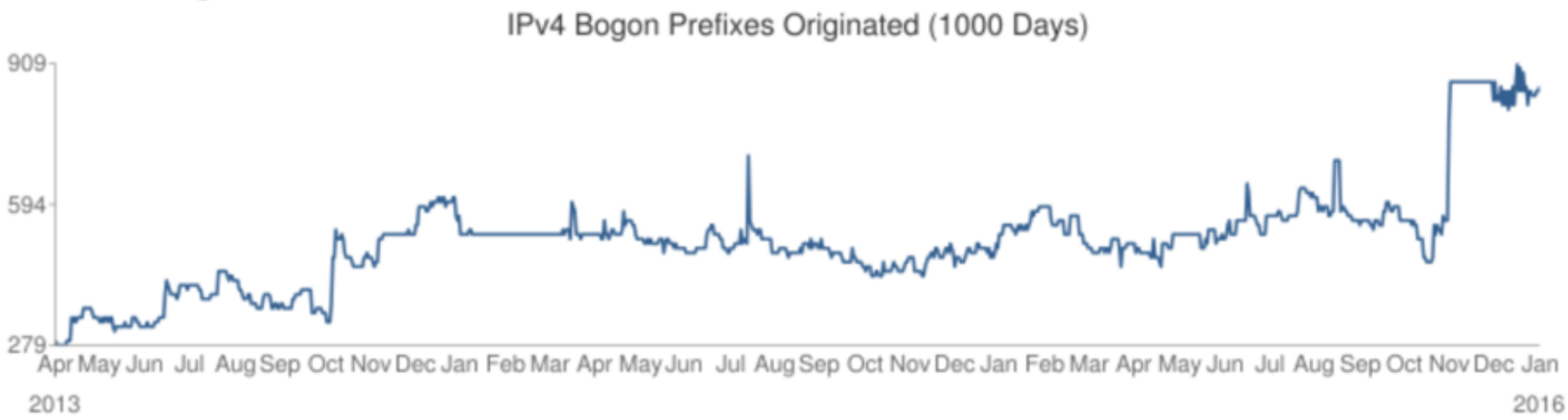
Problem

- Private IP addresses are announced wrongly to the other AS via BGP.
- In my experience:
  - I had set a local address:192.168.0.100/24 in my private LAN, then I ping ip:192.168.1.2, and this packet get response!
  - Traceroute: the packet was send to unknown network through ChinaUnicom
  - **Dangerous**: any others can find the local net easily, and do any thing!

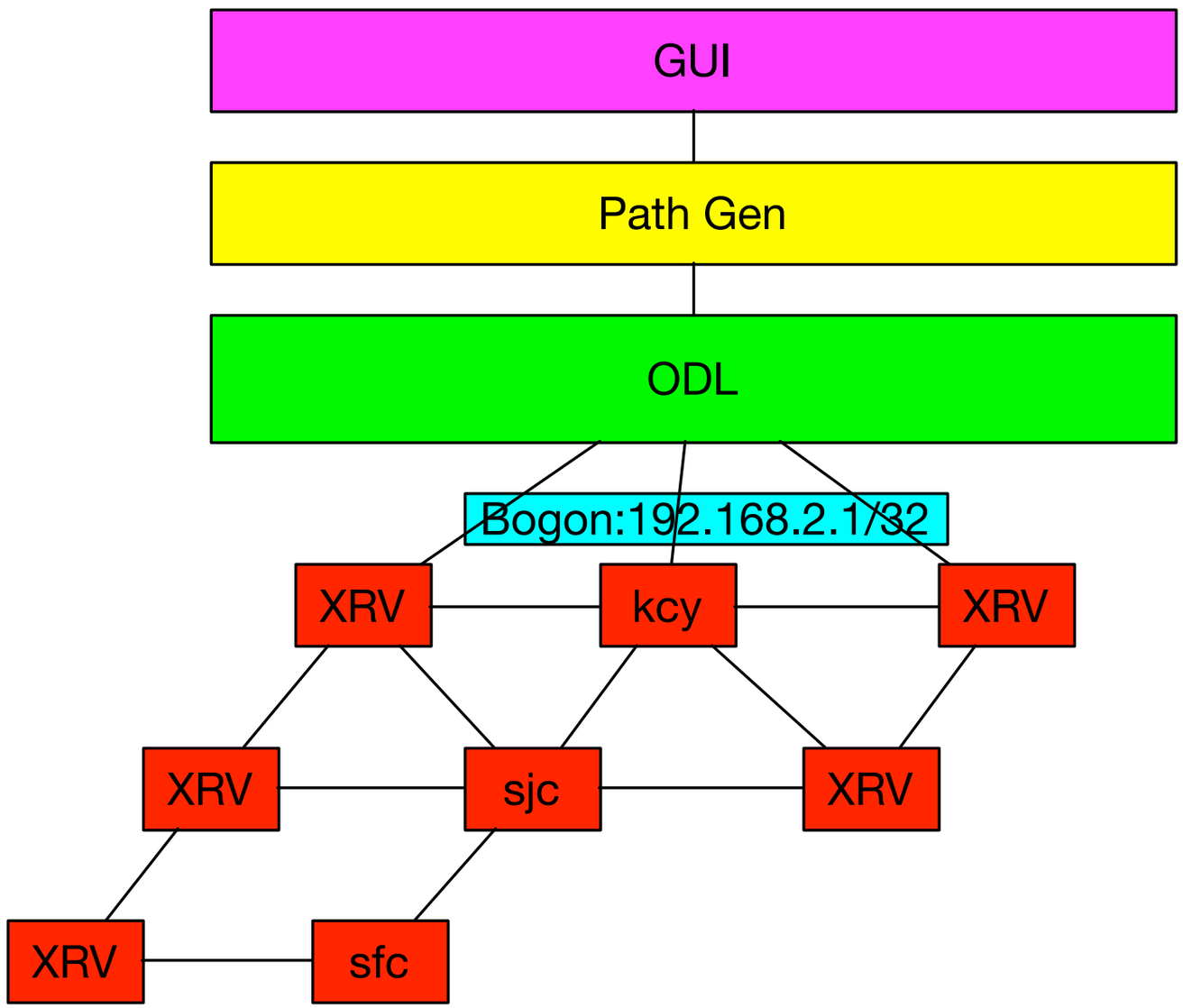


BGP Bogon Routes

865 IPv4 Bogon Routes



Architecture



How it works?

- Use the topology in d-cloud.
- Get BGP Configuration from every XRV node.
- Find the bogons according to list.
- Delete the bogons.

Status

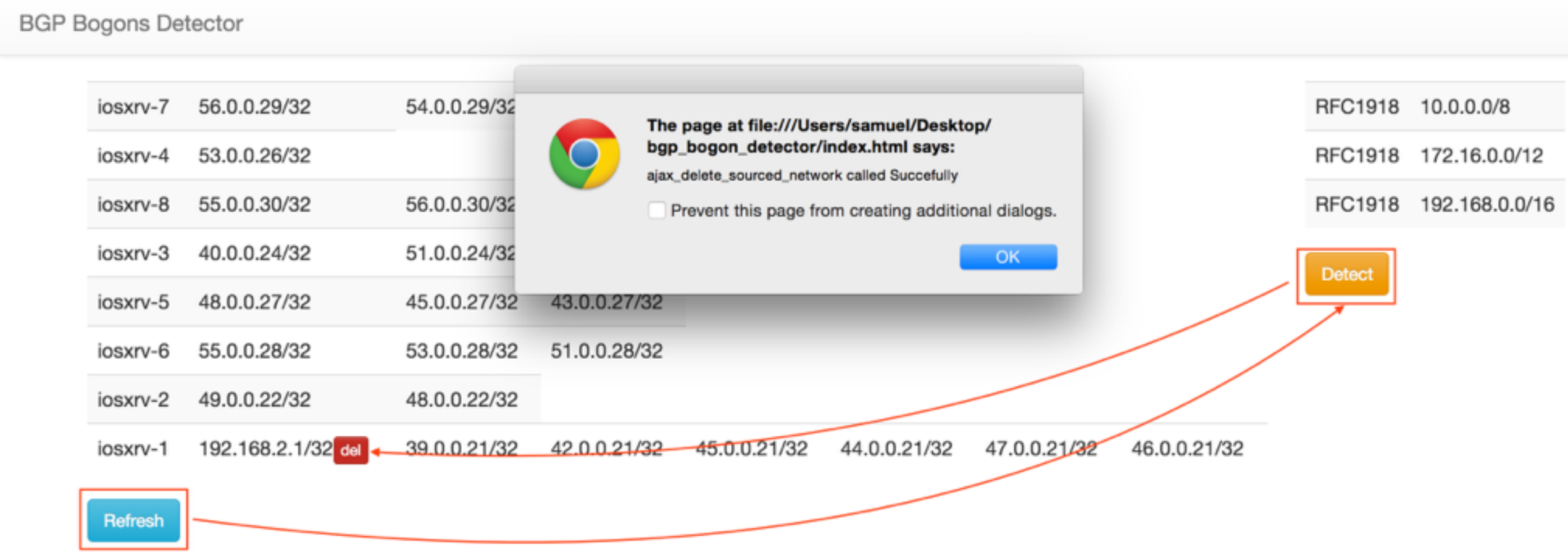
- Config a private ip address and announce it by BGP.
- Ping the ip address, responsed.

```
RP/0/0/CPU0:sea#show route bgp
Fri Jan 22 14:13:12.962 UTC

B    39.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    40.0.0.24/32 [200/0] via 24.24.24.24, 1d03h
B    42.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    43.0.0.27/32 [200/0] via 27.27.27.27, 1d03h
B    44.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    44.0.0.24/32 [200/0] via 24.24.24.24, 1d03h
B    45.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    45.0.0.27/32 [200/0] via 27.27.27.27, 1d03h
B    46.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    46.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    47.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    48.0.0.22/32 [200/0] via 22.22.22.22, 1d03h
B    48.0.0.27/32 [200/0] via 27.27.27.27, 1d03h
B    49.0.0.22/32 [200/0] via 22.22.22.22, 1d03h
B    49.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    51.0.0.24/32 [200/0] via 24.24.24.24, 1d03h
B    53.0.0.26/32 [200/0] via 26.26.26.26, 1d03h
B    54.0.0.29/32 [200/0] via 29.29.29.29, 1d03h
B    55.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    56.0.0.29/32 [200/0] via 29.29.29.29, 1d03h
B    56.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    192.168.2.1/32 [200/0] via 21.21.21.21, 00:02:41
RP/0/0/CPU0:sea#ping 192.168.2.1
Fri Jan 22 14:13:38.481 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
RP/0/0/CPU0:sea#
```

Status

- Run the application.



Status

- The routes is deleted and can not get the responsed of ping packet.

```
RP/0/0/CPU0:sea#show route bgp
Fri Jan 22 14:14:34.157 UTC

B    39.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    40.0.0.24/32 [200/0] via 24.24.24.24, 1d03h
B    42.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    43.0.0.27/32 [200/0] via 27.27.27.27, 1d03h
B    44.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    44.0.0.24/32 [200/0] via 24.24.24.24, 1d03h
B    45.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    45.0.0.27/32 [200/0] via 27.27.27.27, 1d03h
B    46.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    46.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    47.0.0.21/32 [200/0] via 21.21.21.21, 1d03h
B    48.0.0.22/32 [200/0] via 22.22.22.22, 1d03h
B    48.0.0.27/32 [200/0] via 27.27.27.27, 1d03h
B    49.0.0.22/32 [200/0] via 22.22.22.22, 1d03h
B    49.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    51.0.0.24/32 [200/0] via 24.24.24.24, 1d03h
B    53.0.0.26/32 [200/0] via 26.26.26.26, 1d03h
B    54.0.0.29/32 [200/0] via 29.29.29.29, 1d03h
B    55.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
B    56.0.0.29/32 [200/0] via 29.29.29.29, 1d03h
B    56.0.0.30/32 [200/0] via 30.30.30.30, 1d03h
RP/0/0/CPU0:sea#ping 192.168.2.1
Fri Jan 22 14:14:42.206 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
RP/0/0/CPU0:sea#
```

Thanks

Q&A