SUSTech CS305
IP over DNS

2019 fall

胡圣然 李文博 艾君达

Background

- TUN interface & TUN tunnel
  - TUN interface:
    - Virtual network interface supported entirely in software.
    - Allow userspace programs to see raw network traffic
    - Simulates a network layer device and operates in network layer carrying IP packets.
  - In our program we managed to route IP packets through TUN interfaces.

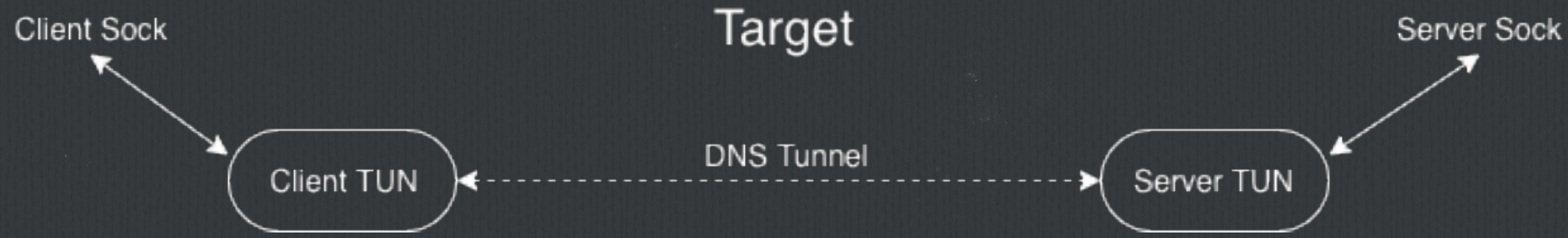
Background

- DNS tunnel
  - TUN devices at client and server are connected via DNS tunnel.
  - This can be used to breach network restriction by stuffing IP packet segments into DNS packets.

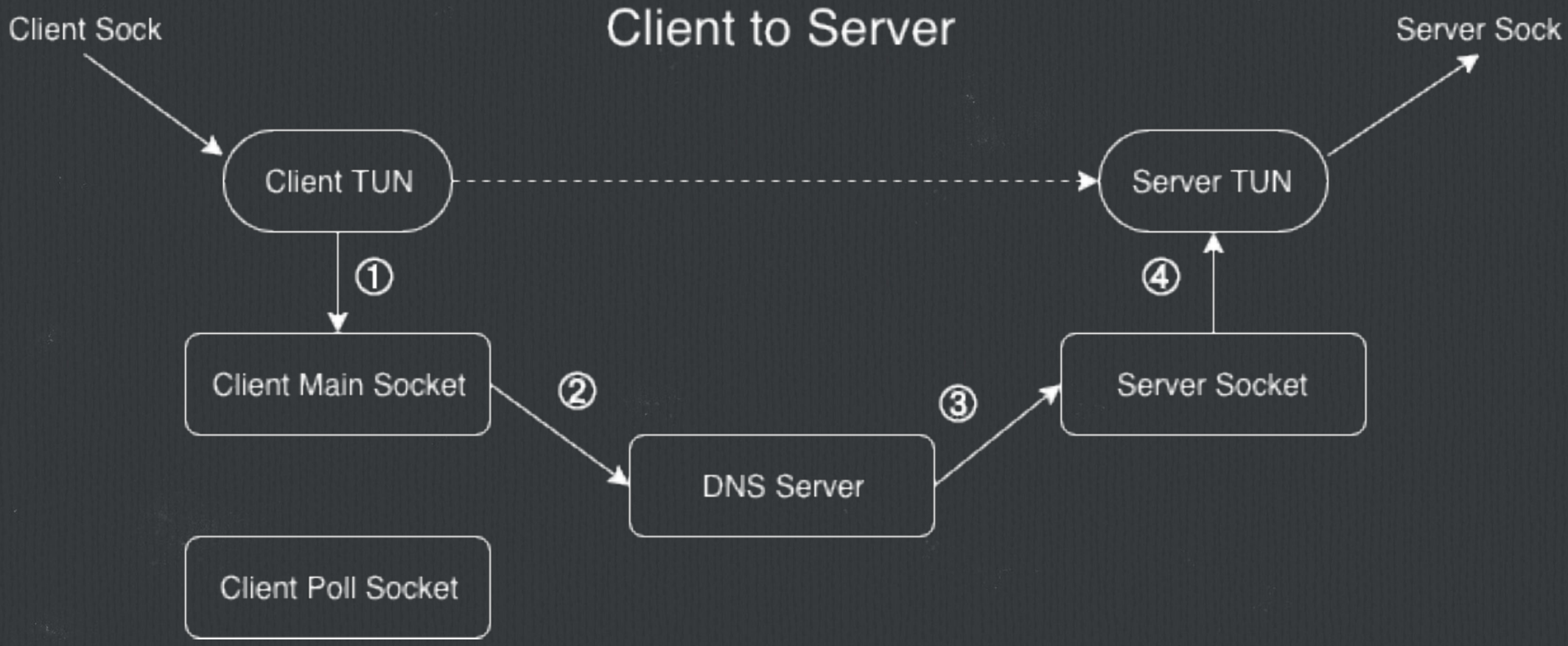
Implementation

- [ ] Network Topology
- [ ] Network Design

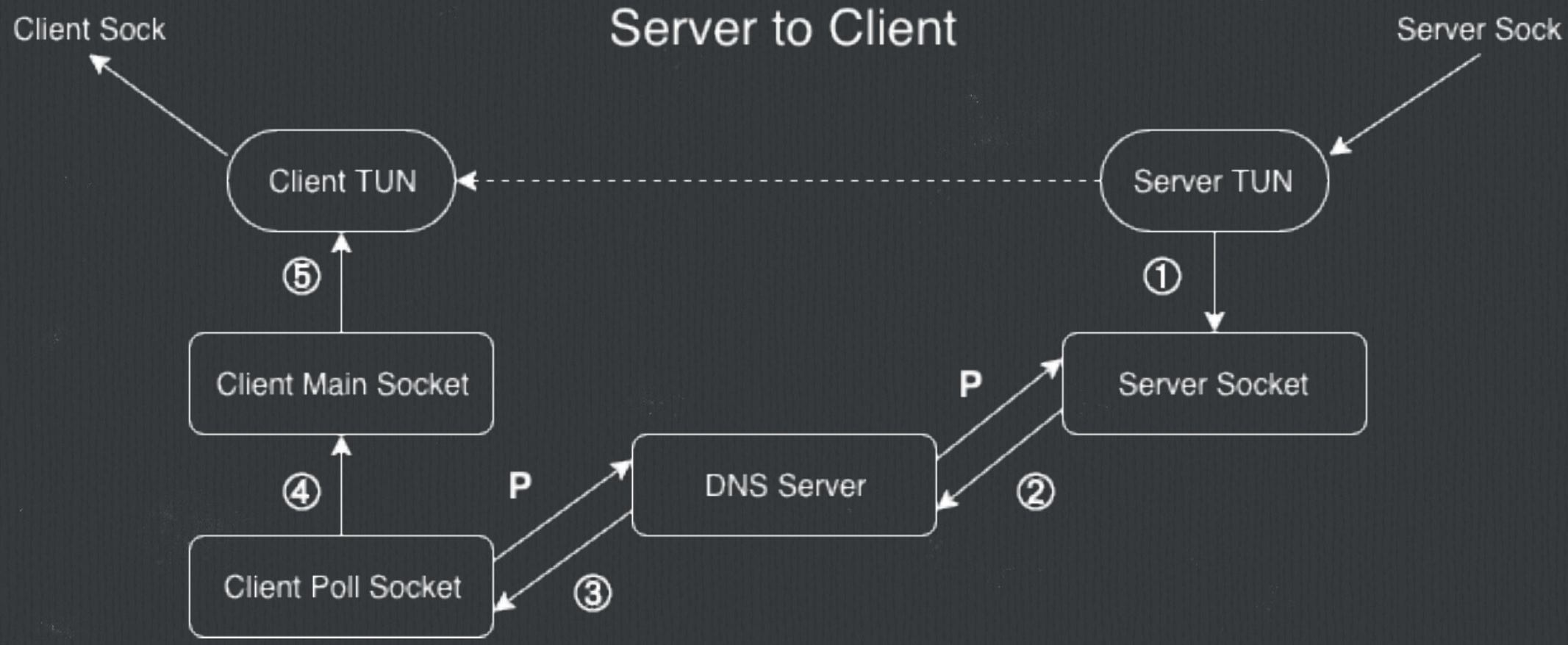
Network Topology



Network Topology



Network Topology



Network Design

- [ ] TUN Setup
  - [ ] Python-pytun
- [ ] Encode data
  - [ ] Base64 url safe

Network Design

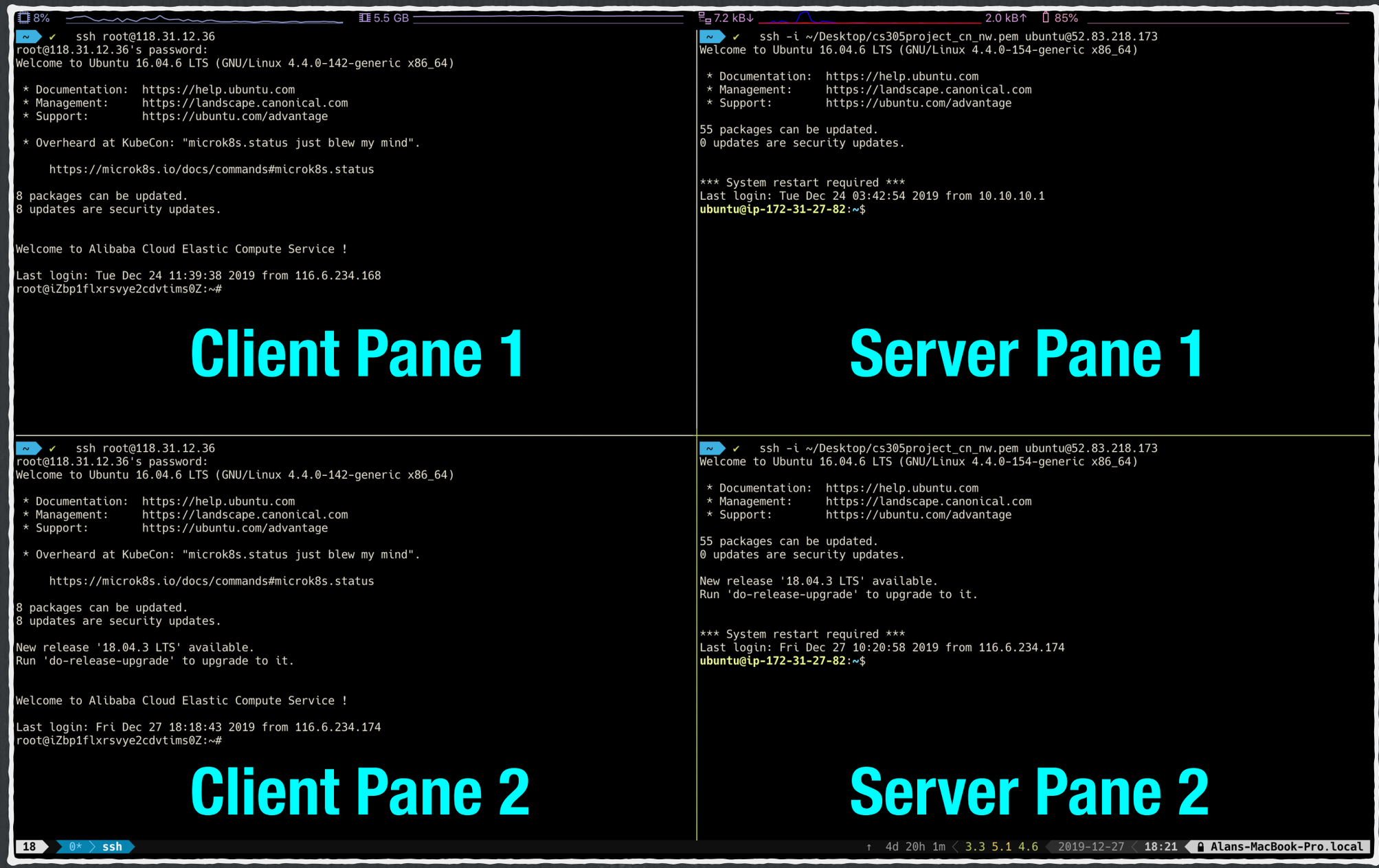
- [ ] Protocol-send (Client Main Socket -> Server Socket)
  - [ ] MTU: 150
  - [ ] Put encoded data to question-qname field
  - [ ] Client send: D.data1.data2.data3.data4.group-38.cs305 (QTYPE: TXT) 60 bytes each fragment. (D: data)
  - [ ] Server reply: Empty

Network Design

- [ ] Protocol-receive (Server Socket -> Client Poll Socket)
  - [ ] MTU: 150, Poll frequency: 0.01s
  - [ ] Poll send: P.32byte-random.group-38.cs305.fun (QTYPE: TXT)
  - [ ] Server reply: answer section txt type
  - [ ] Poll socket cc server reply to client main socket

Testing

Testing Window Layout



Two-way TUN Device Ping Test

TUN client.py running output

```
8%  5.4 GB
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.5D22FC2E57B0E911AF45DB2DAC2C6F89.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKEhQAB
AAXFxCgoKAgoKCgEIAF2YCb4AAkbcBV4AAAAAfZoIAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVPtQAABAAVdCCgoKAQoKCgIAAGWYCb4AAkbcBV4AAAAAfZoIAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.26FDE81C702086E7442AEB6144F0BE48.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKF5QAB
AAXEZCgoKAgoKCgEIAB6SCb4AA0fcBV4AAAAAu58IAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVPtaAABAAVc4CgoKAQoKCgIAACaSCb4AA0fcBV4AAAAAu58IAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.00007C2C0A2D68A12D4BA583DF02017D.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKJEQAB
AAXBOCgoKAgoKCgEIAIeJCb4ABEjcBV4AAAAAUacIAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVPuIAABAAVcKCgoKAQoKCgIAAI-JCb4ABEjcBV4AAAAAUacIAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.69A39BD2781F4EA51C228CFF76434FED.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKK1QAB
AAW_dCgoKAgoKCgEIAA2CCb4AAUscBV4AAAAA70IAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVPuIAABAAVcKCgoKAQoKCgIAABWCCb4AAUscBV4AAAAA70IAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.C400911C21DAB486EEA14AE9BE855C6B.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKLUQAB
AAW--CgoKAgoKCgEIAKN7Cb4ABkrcBV4AAAAAM7MIAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVPymAABAAVXsCgoKAQoKCgIAAKt7Cb4ABkrcBV4AAAAAM7MIAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.7D851257F8437CB8662F40969D005E04.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKOFQAB
AAW8NCgoKAgoKCgEIAItzCb4AB0vcBV4AAAAASroIAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVPy8AABAAVXWCgoKAQoKCgIAAJNzCb4AB0vcBV4AAAAASroIAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
recv:  P.862184D93AA39F5D63B78251FB18FC7D.group-38.cs305.fun. 0       IN      TXT     "E" "RQAAVKOtQAB
AAW7lCgoKAgoKCgEIAAJrCb4ACEzcBV4AAAAA0sEIAAAAAAAQERITFBUWFxgZGhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3"
send:  ;E.RQAAVP2aAABAAVT4CgoKAQoKCgIAAAprCb4ACEzcBV4AAAAA0sEIAAAAAAAQ.ERITFBUWFxgZGhscHR4fICEiIyQlJic
oKSorLC0uLzAxMjM0NTY3.group-38.cs305.fun. IN      TXT
```

Client host ping server

```
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:14989 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14989 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:3655293 (3.6 MB)  TX bytes:3655293 (3.6 MB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.10.10.2  P-t-P:10.10.10.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@iZbp1flxrsvye2cdvtims0Z:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=66.8 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=67.9 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=102 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=99.2 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=64 time=106 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=64 time=82.6 ms
64 bytes from 10.10.10.2: icmp_seq=7 ttl=64 time=64.6 ms
64 bytes from 10.10.10.2: icmp_seq=8 ttl=64 time=111 ms
64 bytes from 10.10.10.2: icmp_seq=9 ttl=64 time=76.5 ms
^C
--- 10.10.10.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 64.625/86.487/111.306/17.521 ms
root@iZbp1flxrsvye2cdvtims0Z:~#
```

TUN server.py running output

```
9.2 kB↓  0.0 kB↑  84%
x00\x00\x00Q\xa7\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\
x1f !"#$%&\'()*+,-./01234567'
recv b'E\x00\x00T\xfb\x88\x00\x00@\x01W\n\n\n\n\x01\n\n\n\x02\x00\x00\x8f\x89\t\xbe\x00\x04H\xdc\x05^
\x00\x00\x00\x00\x00Q\xa7\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d
\x1e\x1f !"#$%&\'()*+,-./01234567'
send:  b'E\x00\x00T\xa2\xb5@\x00@\x01o\xdd\n\n\n\x02\n\n\n\x01\x08\x00\r\x82\t\xbe\x00\x05I\xdc\x05^\
x00\x00\x00\x00\x00\xca\xad\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x
1d\x1e\x1f !"#$%&\'()*+,-./01234567'
recv b'E\x00\x00T\xfcH\x00\x00@\x01VJ\n\n\n\x01\n\n\n\x02\x00\x00\x15\x82\t\xbe\x00\x05I\xdc\x05^\x00
\x00\x00\x00\x00\xca\xad\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\
x1e\x1f !"#$%&\'()*+,-./01234567'
send:  b'E\x00\x00T\xa2\xd4@\x00@\x01o\xbe\n\n\n\x02\n\n\n\x01\x08\x00\xa3{\t\xbe\x00\x06J\xdc\x05^\x
00\x00\x00\x00\x00\x003\xb3\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x
1e\x1f !"#$%&\'()*+,-./01234567'
recv b'E\x00\x00T\xfd\x00\x00@\x01U\xd6\n\n\n\x01\n\n\n\x02\x00\x00\x93s\t\xbe\x00\x07K\xdc\x05^\
x00\x00\x00\x00\x00J\xba\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\
x1e\x1f !"#$%&\'()*+,-./01234567'
send:  b'E\x00\x00T\xa3\x85@\x00@\x01o\r\n\n\n\x02\n\n\n\x01\x08\x00\x8bs\t\xbe\x00\x07K\xdc\x05^\x00
\x00\x00\x00\x00J\xba\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e
\x1f !"#$%&\'()*+,-./01234567'
recv b'E\x00\x00T\xfe\xbc\x00\x00@\x01U\xd6\n\n\n\x01\n\n\n\x02\x00\x00\x93s\t\xbe\x00\x07K\xdc\x05^\
x00\x00\x00\x00\x00J\xba\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\
x1e\x1f !"#$%&\'()*+,-./01234567'
send:  b'E\x00\x00T\xa3\xad@\x00@\x01n\xe5\n\n\n\x02\n\n\n\x01\x08\x00\x02k\t\xbe\x00\x08L\xdc\x05^\x
00\x00\x00\x00\xd2\xc1\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1
d\x1e\x1f !"#$%&\'()*+,-./01234567'
recv b'E\x00\x00T\xfd\x9a\x00\x00@\x01T\xf8\n\n\n\x01\n\n\n\x02\x00\x00\nk\t\xbe\x00\x08L\xdc\x05^\x0
0\x00\x00\x00\xd2\xc1\x08\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d
\x1e\x1f !"#$%&\'()*+,-./01234567'
```

Server host ping client

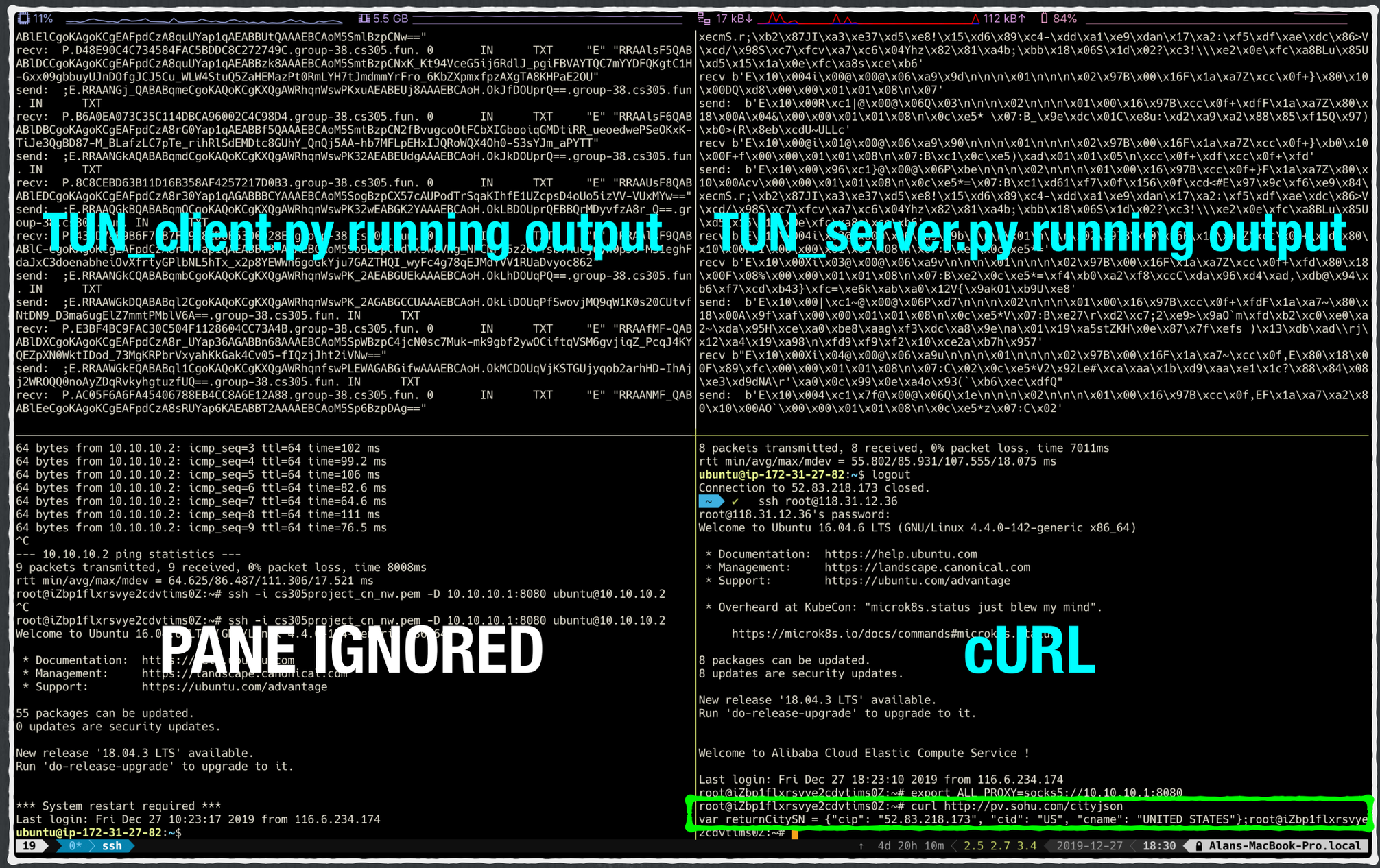
```
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

55 packages can be updated.
0 updates are security updates.

New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Fri Dec 27 10:23:15 2019 from 116.6.234.174
ubuntu@ip-172-31-27-82:~$ ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=95.3 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=62.1 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=55.8 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=107 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=64 time=106 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=64 time=84.7 ms
64 bytes from 10.10.10.1: icmp_seq=7 ttl=64 time=96.8 ms
64 bytes from 10.10.10.1: icmp_seq=8 ttl=64 time=78.7 ms
^C
--- 10.10.10.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 55.802/85.931/107.555/18.075 ms
ubuntu@ip-172-31-27-82:~$
```

```
19  0* ssh   ↑ 4d 20h 6m  1.1 2.9 3.7  2019-12-27  18:26  Alans-MacBook-Pro.local
```

SSH SOCKS Proxy Establishment

Export All Traffic to Proxy Port

cURL pv.sohu.com/cityjson



cURL www.baidu.com

Conclusion

- Gained deeper understanding of DNS protocol, IP package exchange, and proxy
- Problem:
  - Fragmentation of IP package. Finally we limit MTU to avoid Fragmentation.
  - Asymmetry of connection. Use polling on client side to let server send message to client
  - Ubuntu environment setting for TUN and Proxy.

Contribution

- □ 胡圣然 33%： DNS tunnel implementation
  TUN setup/configuration

- □ 艾君达 33%： Proxy setup/configuration
  DNS packet encapsulation

- □ 李文博 33%： Proxy setup/configuration
  Poll implementation