FUKUOKA UNIVERSITY PUBLIC NTP SERVICE & BCP38

Information Technology Center, Fukuoka University, Japan
Sho FUJIMURA
fujimura@fukuoka-u.ac.jp

NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION
Fuminori -Tany- Tanizaki
fuminori.tanizaki@west.ntt.co.jp

福岡大學
FUKUOKA UNIVERSITY

Today's Content

Fukuoka University introduction

- Private university
  - 86th anniversary in May 2019
  - Connected to internet in 1993
- Location: Fukuoka City, JAPAN
  - The city we had APRICOT2015
- 9 faculties (31 departments)
- 10 graduate courses (33 specialties)
- Approximately 20,000 students
- Attached facilities
  - Hospital: 3
  - High school: 2
  - Junior high school: 1

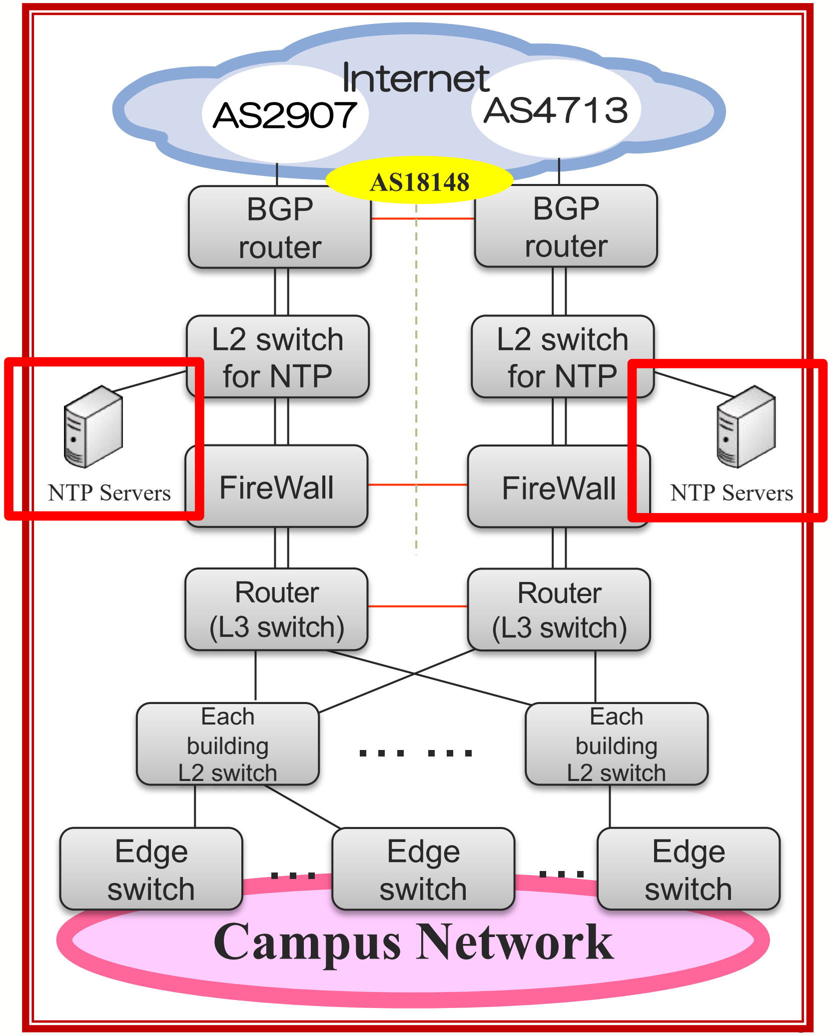
AS: 18148
Prefix: 133.100.0.0/16, 2405:be00::/32

Today's Presentation(Objective)

- Proceeding with BCP38
(Best Current Practice 38)measures

Fukuoka University NTP Service and Network Architecture

- Commenced Operations Oct 1993
- Japan's 1st open NTP Server
  - 133.100.9.2
  - 133.100.11.8
- NTP Server load distributed to 4 servers
- Multihomed internet connection to OCN and SINET

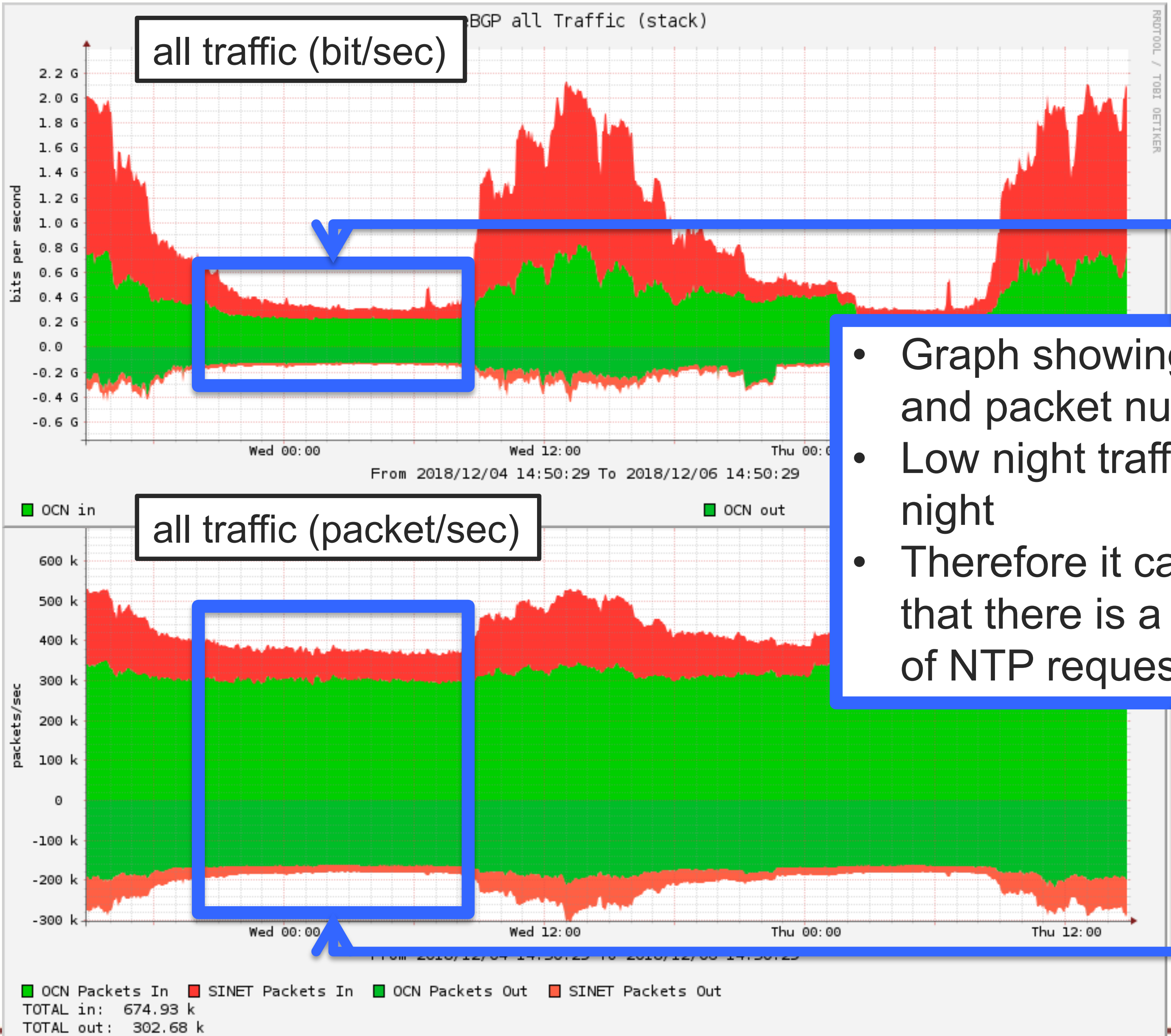


※ AS18148 … Fukuoka University
※ AS2907… Science Information NETwork（SINET）operated by National Institute of Informatics
※ AS4713 … Open Computer Network（OCN）operated by NTT Communications Corporation

What do these figures mean!?

270Mb/sec

350,000p/sec



- Graph showing router traffic and packet numbers
- Low night traffic at University at night
- Therefore it can be deduced that there is a high proportion of NTP request packets

If this is so...

- “High traffic volumes are a problem. So why not just shut down the NTP Server?”
- “Because if we shut down the NTP server the number of request packets increase!”

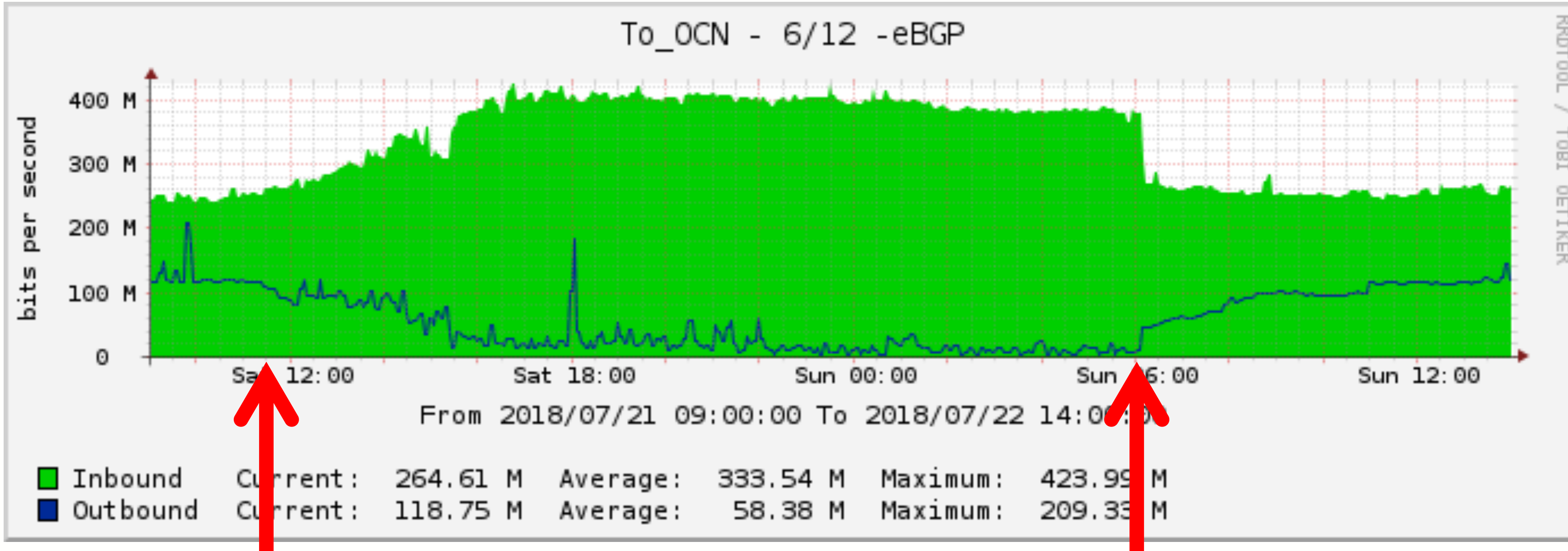
Outline of Experiment

- To confirm that request packets increase when the server disposes of NTP request packets
- Time of experiment： 2018/07/21 - 2018/07/22
- Subject：A specific AS (prefix no.：1361)

/17	/16	/15	/14	/19	/24	/18	/13	/20	/22	/21	/23	/12	/11	/10
576	220	118	66	65	60	58	52	35	32	25	24	24	5	1

- Method
- Direct NTP Server prefixes to blackhole
- Deactivate all server blackhole settings

The Experimental Result



Blackhole Setting Enabled

Blackhole Setting Disabled

- Straight after enabling the black hold, request packets (green) gradually began to increase
- The increase contiunued for 6 hours, then levelled off
- After disabling the black hole, the traffic immediately decreased.
- The range was over 160Mb/s

While investigating various issues in preparation for decommissioning the NTP Server

We discovered another troublesome issue!!

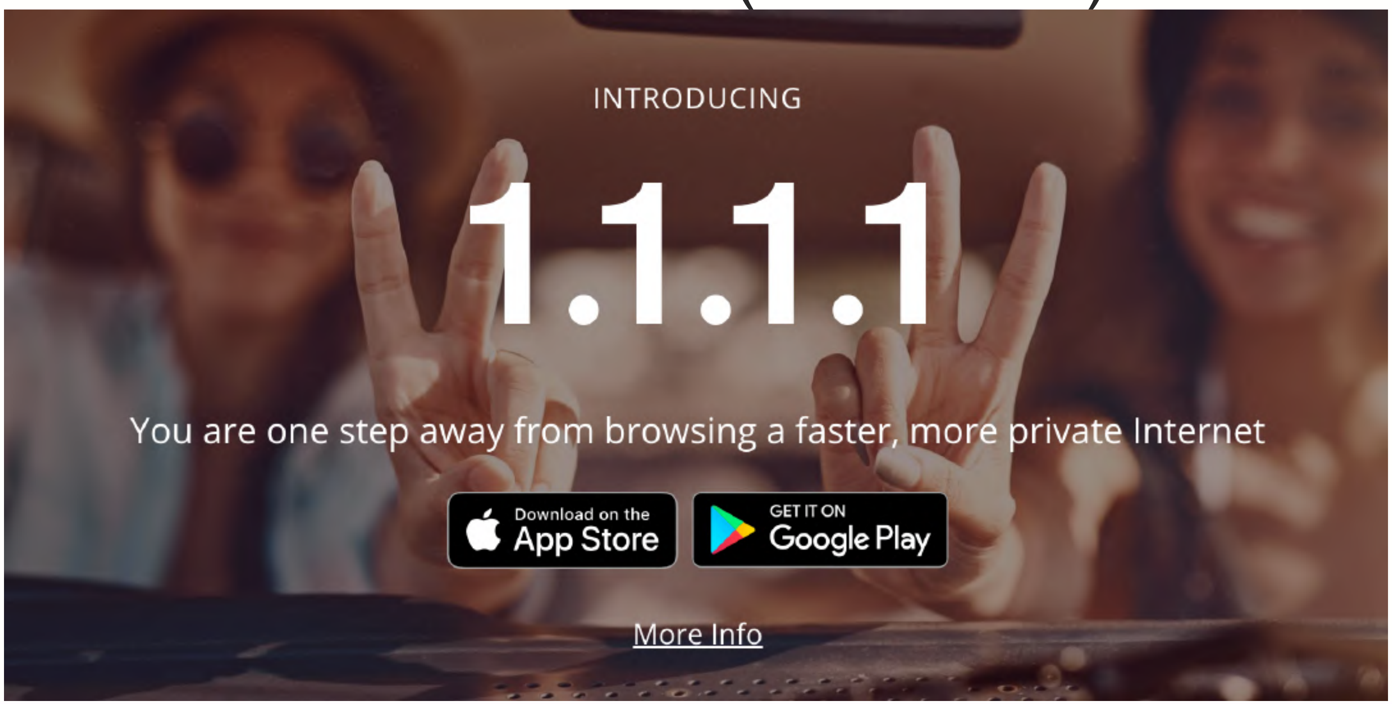
Request packets sent from 1.1.1.1

```
15:02:56.753073 IP 111.27.128.132.40335 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753222 IP 80.139.50.230.57285 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753224 IP 95.90.251.139.50935 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753225 IP 49.149.225.218.55957 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753250 IP 186.59.218.144.52437 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753308 IP 190.174.137.144.60873 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753310 IP 123.14.184.10.123 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753311 IP 112.134.243.117.51943 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753313 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753361 IP 213.80.209.242.33823 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753362 IP 95.39.184.203.60975 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753428 IP 109.173.208.67.48711 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753429 IP 87.21.2.56.58555 > 133.100.11.21.123: NTPv3, Client, length 48
15:02:56.753431 IP 183.200.171.184.46505 > 133.100.11.21.123: NTPv3, Client, length 48
```

- On closer inspection, the request packets were sent from 1.1.1.0/24 and 1.0.0.0/24
- Currently we are filtering them at the NTP Server

What is 1.1.1.1?

- It is a public DNS Resolution Service operated by Cloudflare
- Currently 1.0.0.0/24 and 1.1.1.0/24 are being advertised as AS13335(Cloudflare)



https://1.1.1.1/ or https://one.one.one.one/

Where is it coming from?

- (Of course)it is not coming from Cloudflare

> **Tom Paseka**
> @tompaseka
> フォローする
>
> hi @tanyorg . I am operator of #1dot1dot1dot1 . I can confirm that we do not send you NTP queries. You said these come from AS4713 or AS2907 networks. This means these networks are not doing BCP38 properly and should be alerted of this!

Packet Analysis

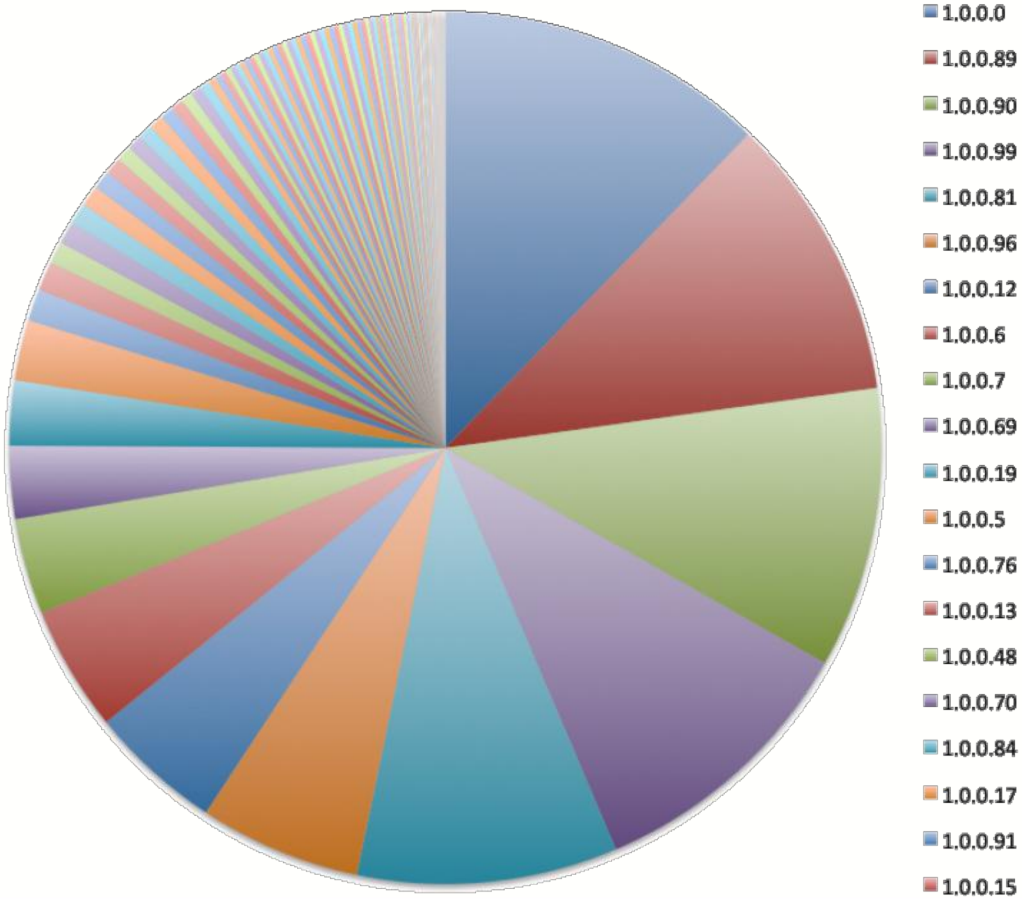
- We collected and analyzed NTP request packets
- Collection period 2018/11/30 8:26 - 2018/12/6 0:00
- Packets collected：1,408,390
- Traffic volumes approx.2.8pps

```
15:22:07.400541 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:12.956750 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:17.404660 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:23.557274 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:26.834715 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:27.401928 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:32.958544 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:33.557920 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:36.835301 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:42.544647 IP 1.1.1.1.10187 > 133.100.11.21.123: NTPv1, Client
15:22:42.959576 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:43.558565 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:46.840519 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:52.960485 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
15:22:57.405258 IP 1.1.1.1.123 > 133.100.11.21.123: NTPv3, Client,
```

NTP Version	Request no.
v1	410130
v2	0
v3	998232
v4	28

From what address?

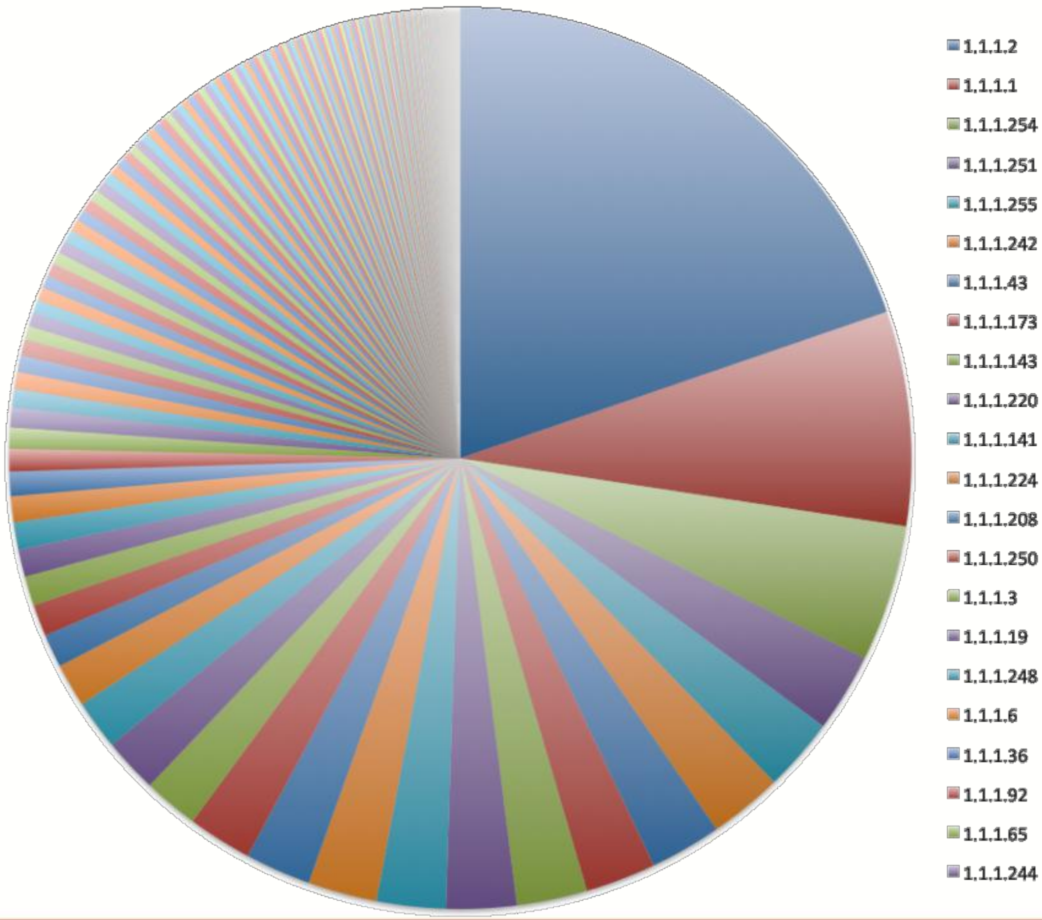
- 1.0.0.0/24



	Access※rigin	Access※o.	
1	1.0.0.0	19038	12.22%
2	1.0.0.89	16467	10.57%
3	1.0.0.90	16226	10.42%
4	1.0.0.99	16196	10.40%
5	1.0.0.81	15041	9.66%
6	1.0.0.96	9329	5.99%
7	1.0.0.12	7680	4.93%
8	1.0.0.6	7240	4.65%
9	1.0.0.7	5540	3.56%
10	1.0.0.69	4200	2.70%

From what address?

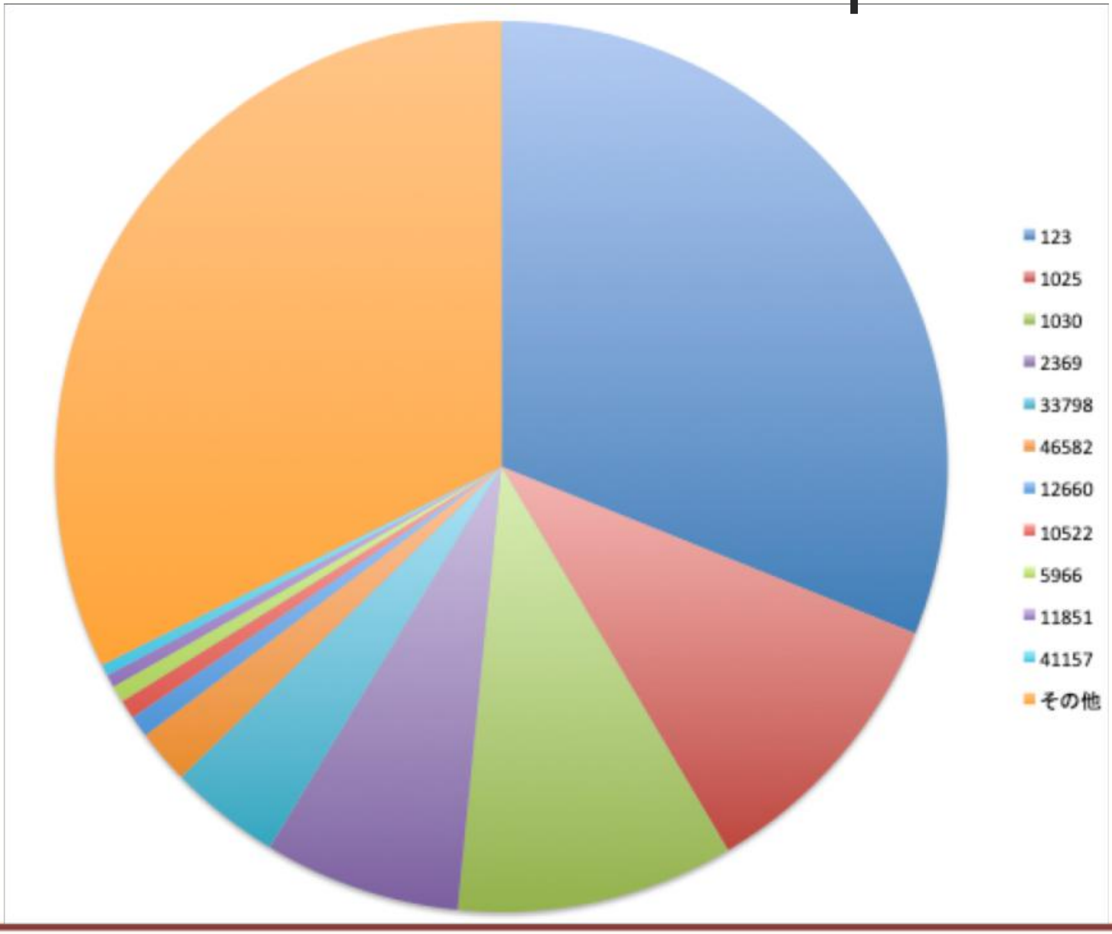
- 1.1.1.0/24



	Access※rigin	Access※o.	
1	1.1.1.2	247092	19.73%
2	1.1.1.1	96275	7.69%
3	1.1.1.254	61335	4.90%
4	1.1.1.251	35303	2.82%
5	1.1.1.255	32901	2.63%
6	1.1.1.242	32891	2.63%
7	1.1.1.43	32064	2.56%
8	1.1.1.173	31705	2.53%
9	1.1.1.143	31625	2.52%
10	1.1.1.220	31438	2.51%

What source port no.?

- Access from 2168 ports



Port no.	Request no.
123	3111
1025	1041
1030	1005
2369	713
33798	404
46582	196
12660	79
10522	68
5966	61
11851	46
41157	41
others	3235

Sample of NTP packets sent

```
▼ User Datagram Protocol, Src Port: 123, Dst Port: 123
    Source Port: 123
    Destination Port: 123
    Length: 56
    Checksum: 0xdf9a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
▼ Network Time Protocol (NTP Version 3, client)
  ▶ Flags: 0x1b, Leap Indicator: no warning, Version number: NTP Version 3, Mode: client
    Peer Clock Stratum: unspecified or invalid (0)
    Peer Polling Interval: invalid (0)
    Peer Clock Precision: 1.000000 sec
    Root Delay: 0 seconds
    Root Dispersion: 0 seconds
    Reference ID: NULL
    Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Origin Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Receive Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Transmit Timestamp: Jan  1, 1970 07:53:07.000000000 UTC
```

source port is not from inside 123 NAT

The time from when it was plugged in was 7hr 53 min?

Sample of NTP packets sent

source port 1030 packet

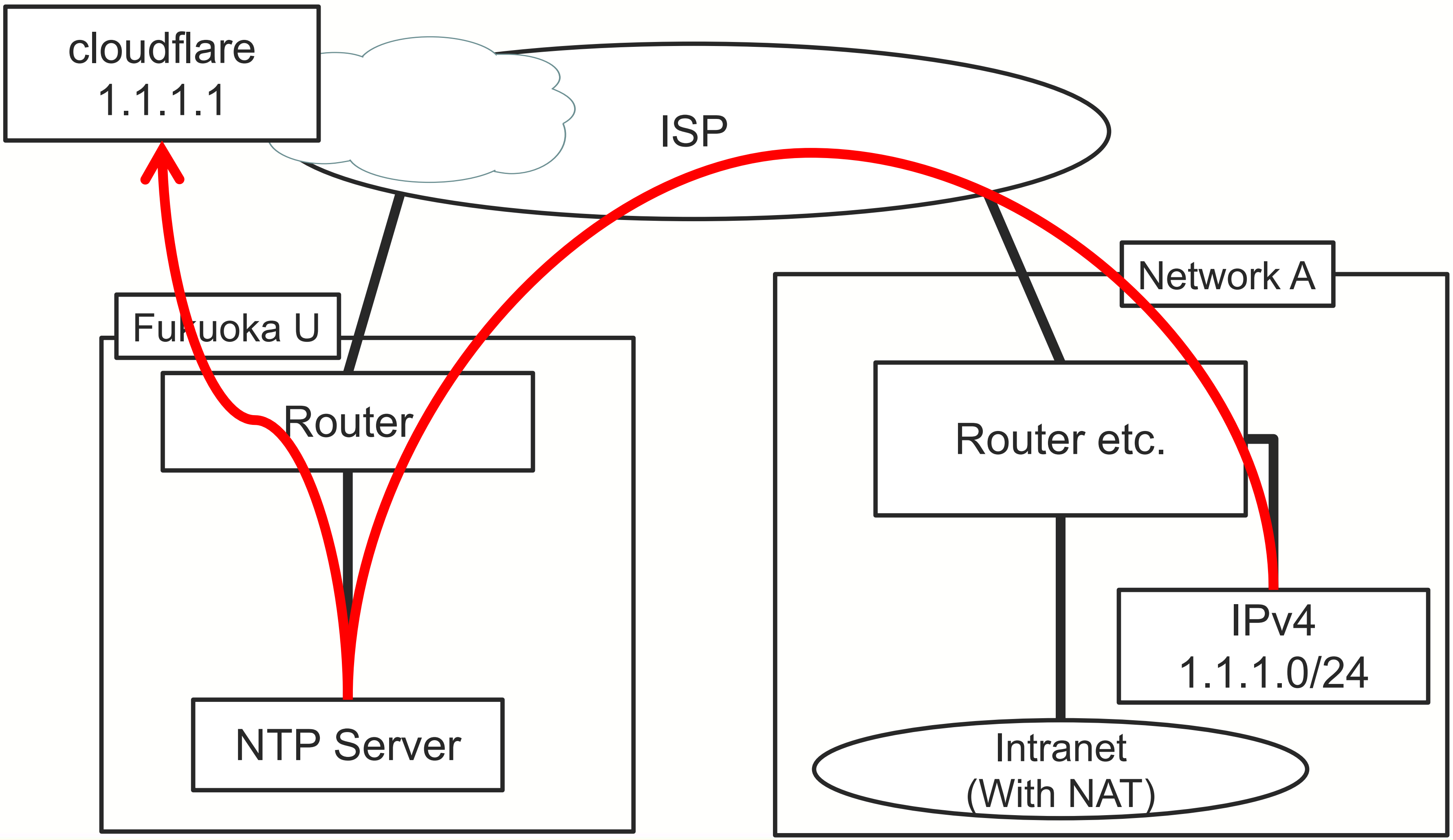
```
14:41:08.935090 IP 1.1.1.220.1030 > 133.100.11.22.123: NTPv3, Client, length 48
14:41:18.938156 IP 1.1.1.220.1030 > 133.100.11.22.123: NTPv3, Client, length 48
14:41:28.935795 IP 1.1.1.220.1030 > 133.100.11.22.123: NTPv3, Client, length 48
14:41:38.935938 IP 1.1.1.220.1030 > 133.100.11.22.123: NTPv3, Client, length 48
14:41:48.936329 IP 1.1.1.220.1030 > 133.100.11.22.123: NTPv3, Client, length 48
```

source port 1025 packet

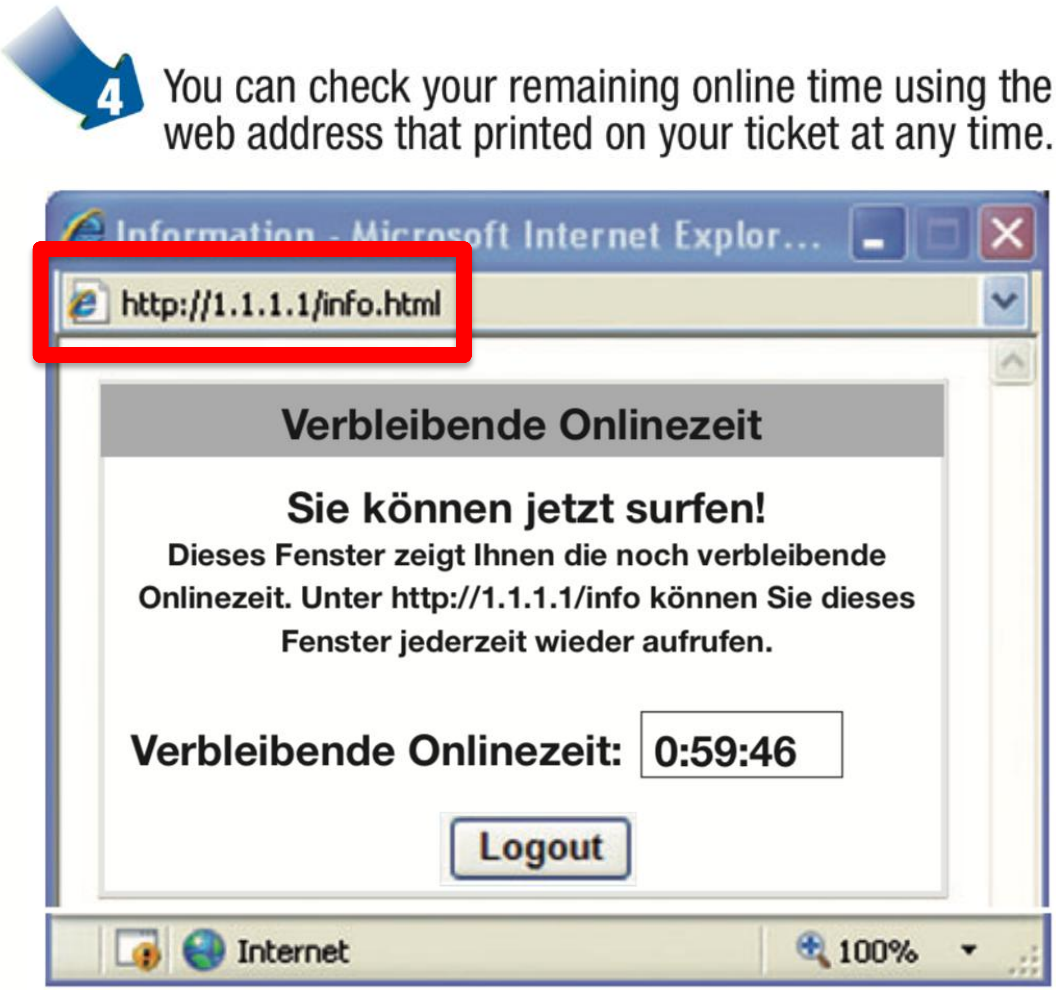
```
14:25:27.066895 IP 1.1.1.141.1025 > 133.100.11.22.123: NTPv3, Client, length 48
14:25:37.000614 IP 1.1.1.141.1025 > 133.100.11.22.123: NTPv3, Client, length 48
14:25:47.069840 IP 1.1.1.141.1025 > 133.100.11.22.123: NTPv3, Client, length 48
14:25:56.993226 IP 1.1.1.141.1025 > 133.100.11.22.123: NTPv3, Client, length 48
14:26:07.003478 IP 1.1.1.141.1025 > 133.100.11.22.123: NTPv3, Client, length 48
```

- It appears that one request is sent every 10 seconds until time synchronization is reached
  - Synchronization not possible as IPv4 is incorrect

Presumed connection structure and packet flow



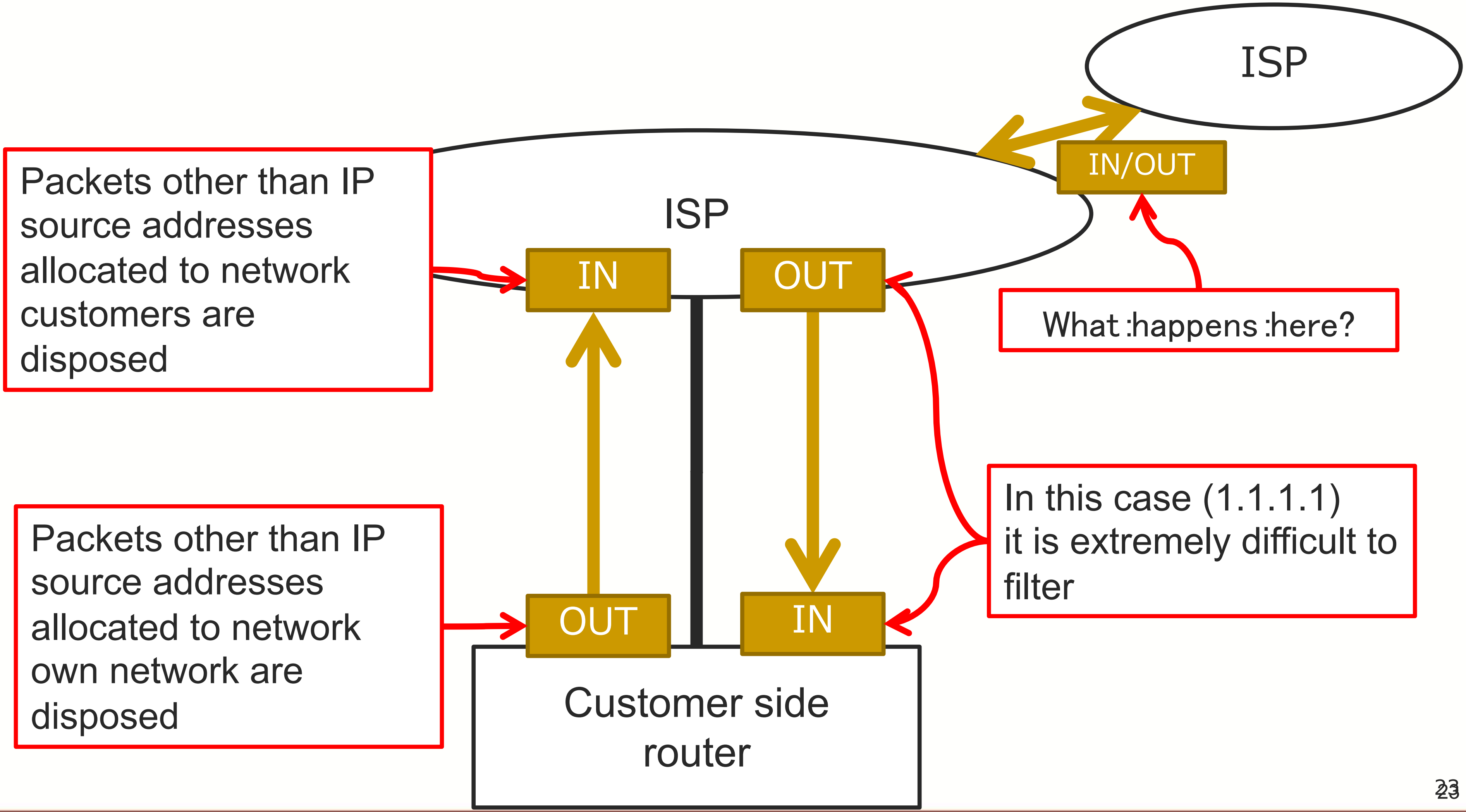
What are these packets?



- 『1.1.1.1』is used in 『**Captive Portal**』 in public Wi-Fi, hotel routers, University wireless LAN etc.
  - The setup by the administrator of hotel and cafe free Wi-Fi forces mandatory web access

https://www.k-bit.de/wireless_lan/kb_easy-hotspot-userguide.pdf

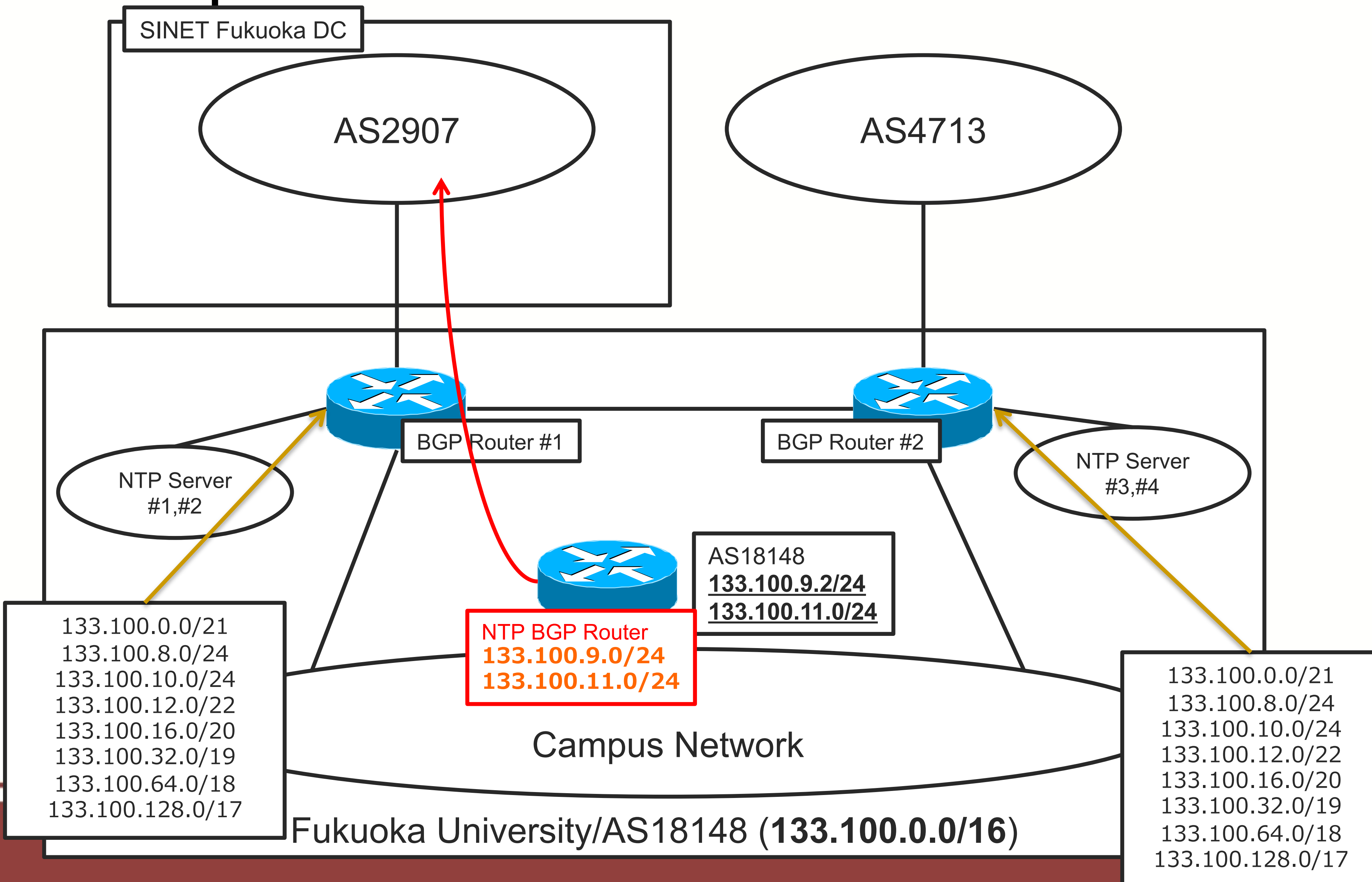
Should a filter be created? (BCP38)



The future of Fukuoka-U NTP Service

- We plan to collect all of these NTP Server directed packets, including BGP routed packets sent to the NTP Server, collect them in a designated router and null them
- We plan to analyze the dispose packets with netflow/sflow

Proposed new network architecture



Conclusion

- We should establish a filter based on BCP38
  - Let's not send out disguised packets and private address block packets

References

- BCP38
  - http://www.bcp38.info/
  - https://tools.ietf.org/html/bcp38
- Fukuoka University Public NTP Service Deployment Use case (APRICOT 2017)
  - https://2017.apricot.net/program/schedule/#/day/8/apops-1

Thank you for your kind attention