Fukuoka University Public NTP Service Deployment Use Case

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

Table of Contents

Fukuoka University introduction

- Private university
  - 85th anniversary in May 2019
  - Connected to internet in 1993
- Location: Fukuoka City,
  Fukuoka Prefecture, JAPAN
- 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

Objectives

- We would like to share the current status of Fukuoka University Public NTP Service
- Determine the cause of NTP traffic because we are troubled with much NTP traffic
- Reduce and stop NTP traffic

What is NTP

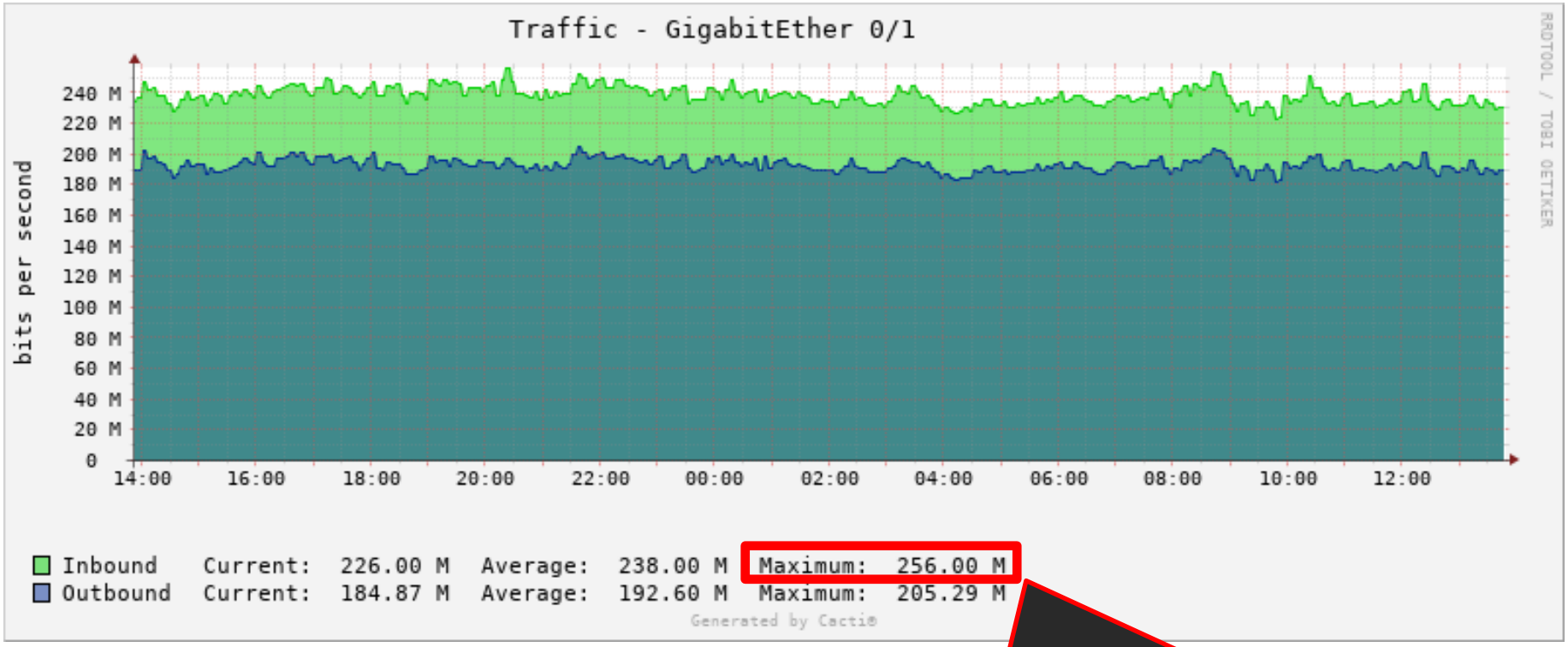
- Network Time Protocol
  - Synchronizes time over networks
  - UDP 123 Port
- Packet size normally 90 bytes
  - Send and receive packets basically the same size

Background

- Commenced a public NTP service in October 1993 at Fukuoka University
- First public NTP service using GPS in Japan
  - 133.100.9.2
  - 133.100.11.8 (already ceased the service)
    - Very little traffic compared to 133.100.9.2

NTP Traffic

- Only NTP



Maximum: 256 Mbps
340,000 Packet / s !!

Traffic analysis by country

- Top 20 ranking of NTP request by the country
  - Analysis results of June 2019
- Brazil, Argentina and Mexico account for Approx. 26% of traffic
- Access from 239 countries and territories from around the world

Rank	Country	PPS	Mbps	Percentage
1	Brazil	56,039	42.4	18.1%
2	China	39,468	29.7	12.7%
3	Argentina	20,688	15.8	6.7%
4	Spain	14,905	11.3	4.8%
5	Italy	12,042	9.8	3.9%
6	Germany	11,646	8.8	3.8%
7	United States	10,329	7.9	3.4%
8	Russian Federation	9,451	7.2	3.1%
9	Iraq	8,721	6.6	2.8%
10	Poland	6,613	5.0	2.1%
11	Viet Nam	6,274	4.7	2.0%
12	Greece	6,120	4.6	2.0%
13	Mexico	5,969	4.5	1.9%
14	Japan	5,595	4.2	1.8%
15	United Kingdom	5,054	3.8	1.6%
16	Portugal	3,545	2.7	1.1%
17	Indonesia	3,340	2.5	1.1%
18	India	3,261	2.5	1.1%
19	France	3,094	2.3	1.0%
20	Lebanon	2,979	2.2	1.0%
	others	73,832	56.0	24.0%
Total		308,965	235	100%

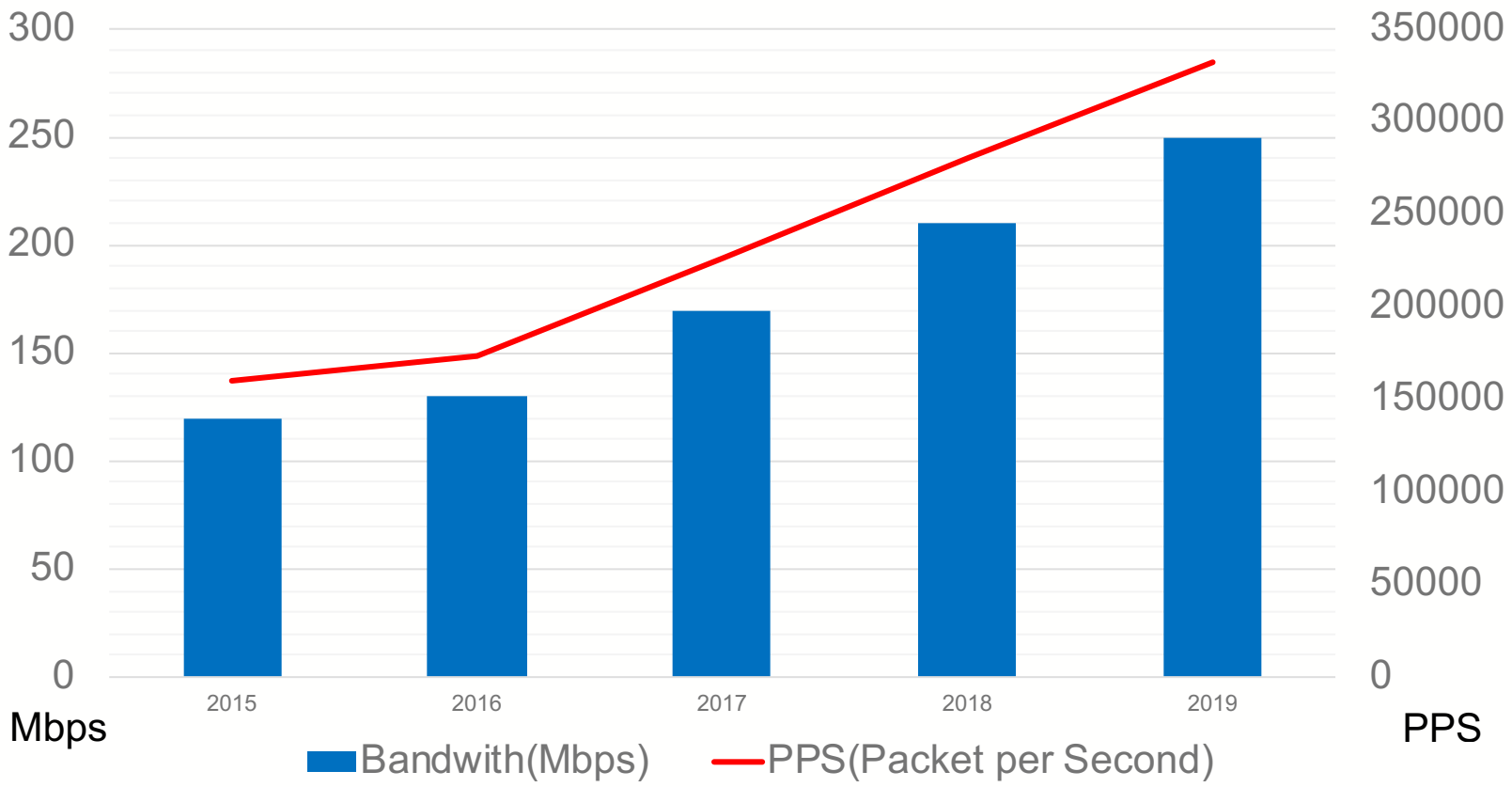
Traffic analysis by countries/regions participating in LACNIC

- Top 20 ranking of NTP request by the countries/regions participating in LACNIC
- Analysis result of June 2019

Rank	Countries / regions participating in LACNIC	PPS	Mbps	Percentage
1	Brazil	56,039	42.40	58.66%
2	Argentina	20,688	15.80	21.65%
3	Mexico	5,969	4.50	6.25%
4	Ecuador	2,788	2.10	2.92%
5	Chile	2,196	1.70	2.30%
6	Bolivarian Republic of Venezuela	1,698	1.30	1.78%
7	Costa Rica	995	0.75	1.04%
8	Colombia	948	0.73	0.99%
9	Uruguay	887	0.68	0.93%
10	Paraguay	769	0.59	0.80%
11	Dominican Republic	638	0.48	0.67%
12	Peru	513	0.39	0.54%
13	Guatemala	397	0.31	0.42%
14	Plurinational State of Bolivia	380	0.29	0.40%
15	Panama	194	0.15	0.20%
16	Honduras	188	0.14	0.20%
17	Guyana	45	0.03	0.05%
18	Curaçao	39	0.03	0.04%
19	El Salvador	36	0.03	0.04%
20	Nicaragua	35	0.03	0.04%
	others	96	0.08	0.10%
Total		95,538	72.50	100%

Increase in traffic volumes

- Traffic continues to increase



Why is it so popular in the world?

- written in manual as setting example
  - Network devices such as L2, L3 switch
  - Multifunction device, etc.

Example

Configure the system time mode as NTP, the time zone is UTC-12:00, the primary NTP server is 133.100.9.2 and the secondary NTP server is 139.78.100.163, the fetching-rate is 11 hours:

TL-SG3424(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

Why is it so popular? (2)

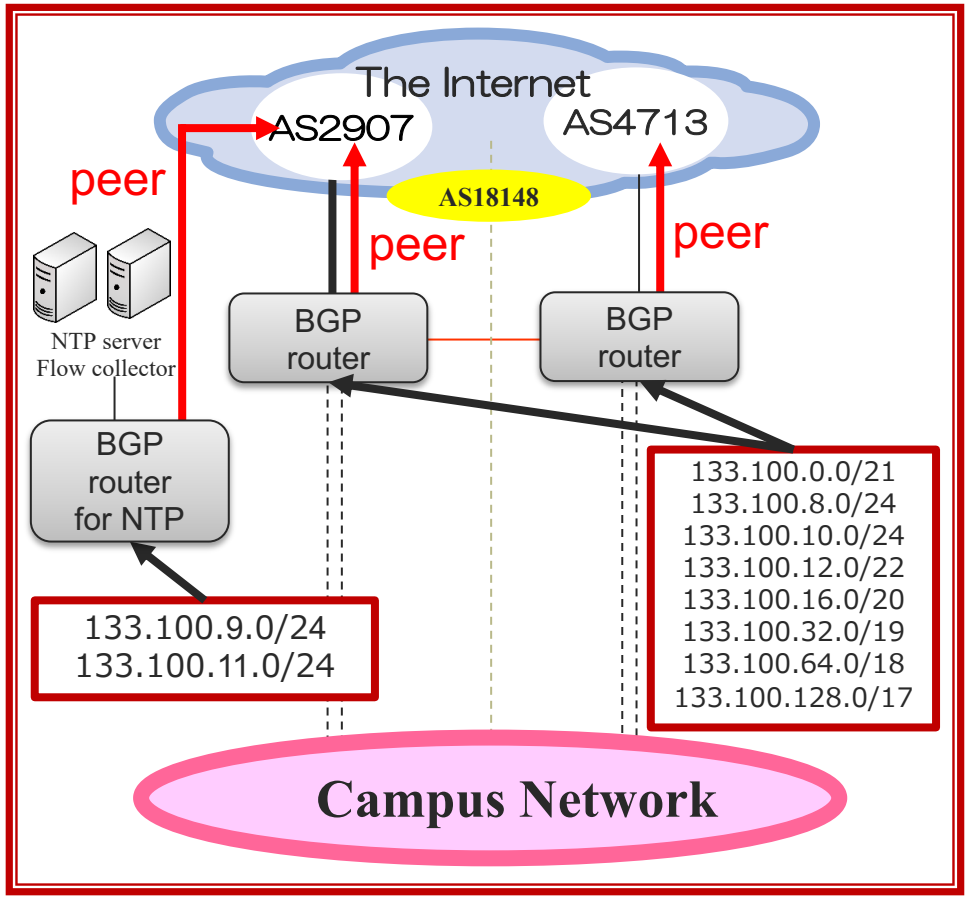
- It's embedded as default setting
- But this is just the tip of the iceberg. We believe that this is not the only reason for the increase in traffic.

93	77.44401	192.168.2.2	133.100.9.2	NTP	90	NTP Version 3, client
94	77.65878	133.100.9.2	192.168.2.2	NTP	90	NTP Version 3, server
95	88.761313	192.168.2.2	192.168.2.1	DNS	78	Standard query 0x04d2
96	88.762061	192.168.2.1	192.168.2.2	DNS	94	Standard query respons

```
▶ Frame 93: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_ae:ee:53 (30:b5:c2:ae:ee:53), Dst: MS-NLB-PhysServer-32_05:4b:2d:72:64
▶ Internet Protocol Version 4, Src: 192.168.2.2, Dst: 133.100.9.2
▶ User Datagram Protocol, Src Port: 42336 (42336), Dst Port: 123 (123)
▼ 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: 4 (16 sec)
    Peer Clock Precision: 0.015625 sec
    Root Delay:    1.0000 sec
    Root Dispersion:    1.0000 sec
    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, 2014 00:01:16.005072000 UTC
```

NTP Network configuration diagram

- The Campus Network is detached from the Public NTP Server
- So the NTP traffic does not affect the campus network
- The public NTP Service Network only is connected to the BGP



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

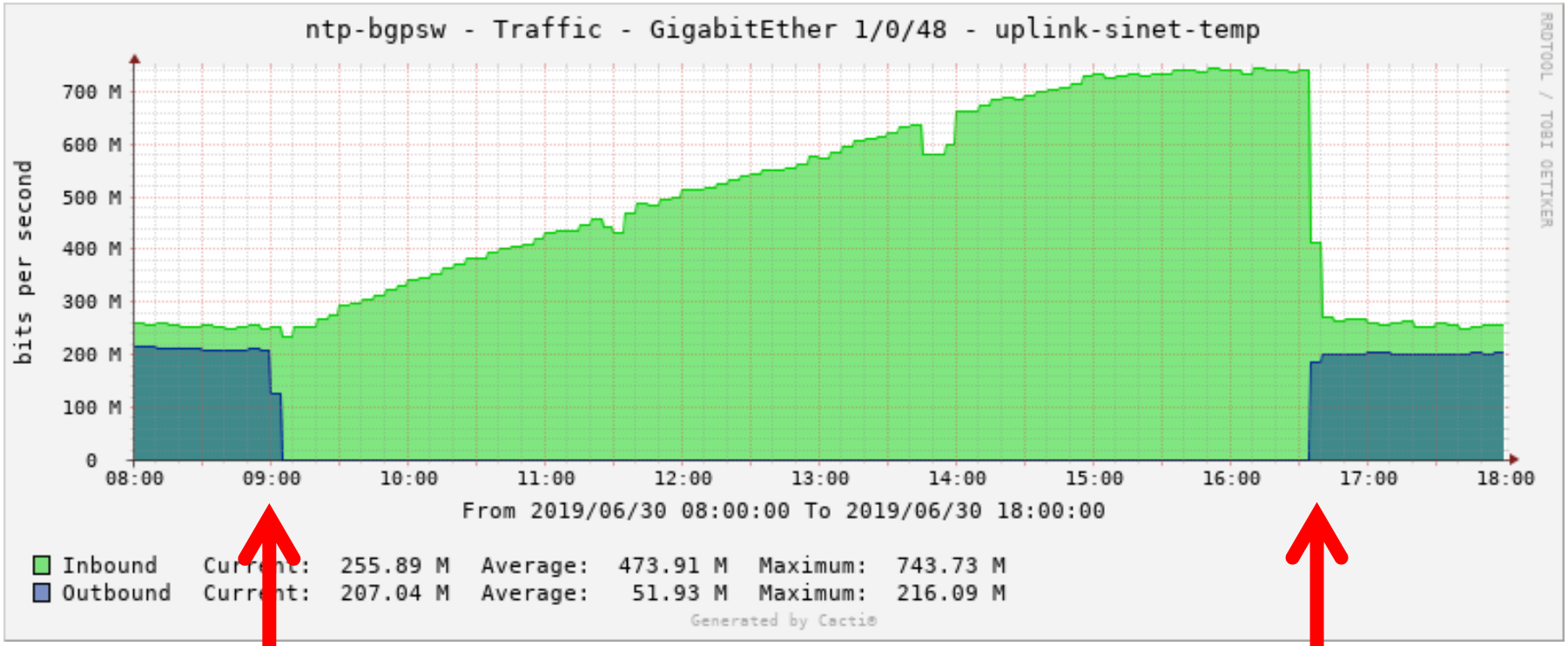
Why not stop the service or filter it?

NTP Service Stop Experiment

- This experiment aims to confirm the movement of request packets when the NTP Service goes offline
- Time of experiment (UTC+0900)
  - 30 June 2019 (Sun) 9am to 5pm
- Target
  - All NTP requests sent to 133.100.9.2 were disposed of in the NTP's BGP router

Results of Experiment

- Increased to 740Mbps, 950,000pps
- Increase in bandwidth approx. 500Mbps, 500,000pps



Service stopped

Service resumed

Traffic Patterns

- On concentrating on a specific IP address during the stoppage experiment the analysis showed there were the following 3 patterns:
- Requests at 5 and 10 minute intervals
  - crontab: 5/* * * * * ntpdate 133.100.9.2
- Access at a specific interval (e.g.1024 sec)
  - ntpd or similar software
- During the stoppage the requests increased, and decreased after the service was resumed
  - Why is this?
  - Causes of increased traffic

Results of the experiment

- Traffic increased when the NTP service stops
  - Some installation causing the extreme increase exists
- We do not know how far the traffic will increase will continue
  - This experiment was only over a short period of time, we will conduct a longer experiment in the future
- We cannot simply stop the service

Frequently Asked Questions(1)

- Why don't you get it filtered upstream?
- This is technically possible, however it will be difficult to maintain this filter over a long period of time
  - It is embedded in firmware packets of numerous devices so we predict that it will continue for a long time
  - For example, if the filter was inadvertently deleted, there would be huge volumes of requests flooding Fukuoka University

Frequently Asked Questions(2)

- Why don’t you send an erroneous time?
- This is technically possible,
  but we worry about the ramifications
  - Access comes from various types of NTP clients, and we cannot predict what ramifications an erroneous time would have
  - For example, if a device could not operate due to the erroneous time, the end user would be the first to be adversely affected

Frequently Asked Questions(3)

- How are you considering terminating the service?
- We are considering using the following method using routes such as BGP
  - Gathering request packets in a specific location in our network and dumping them in a black hole.
  - Stop advertising prefixes that include our NTP Server
- We intend to constantly monitor and analyze traffic

Summary

- Statistics of our public NTP servers
  - Approximately 340,000 requests per second
  - Presently statistics shows gradual increase
- Origin of the NTP clients
  - Throughout the world
- Implications for the Fukuoka University network...
  - Further increasing is not desirable
- What happens if we stop the NTP service now...
  - Retry packets will naturally DoS to our network

Request

- Please do not use our NTP servers
  - Even if it is in the manual do not use it
  - We would like you to check the NTP settings of your broadband router and IoT devices
- To firmware developers
  - Please confirm you do not have 133.100.9.2 nor 133.100.11.8 as default NTP servers
  - If you do, please change them
- To manual authors
  - Please do not list 133.100.9.2 and 133.100.11.8 as NTP servers

Contact information: Sho FUJIMURA (ntp-admin@fukuoka-u.ac.jp)

Conclusion

- We would like to take measures by determining the cause of NTP traffic
- Reduce NTP traffic because of its concentrated nature
- Stop public NTP service to the world

We sincerely appreciate your cooperation.

Contact information: Sho FUJIMURA (ntp-admin@fukuoka-u.ac.jp)

Active 福岡大學

福岡大學

FUKUOKA UNIVERSITY

Thank you very much for your kind attention.

Contact information: Sho FUJIMURA (ntp-admin@fukuoka-u.ac.jp)

人をつくり、時代を拓く。 福岡大學