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
  - 83rd anniversary in May 2017
  - Connected to internet in 1993
- Location: Fukuoka City,
  Fukuoka Prefecture, JAPAN
  - The city we had APRICOT2015
- 9 faculties
  (31 departments)
- 10 graduate courses
  (33 specialties)
- Approximately 21,000 students
- Attached facilities
  - Hospital: 2
  - High school: 2
  - Junior high school: 1

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

Objectives

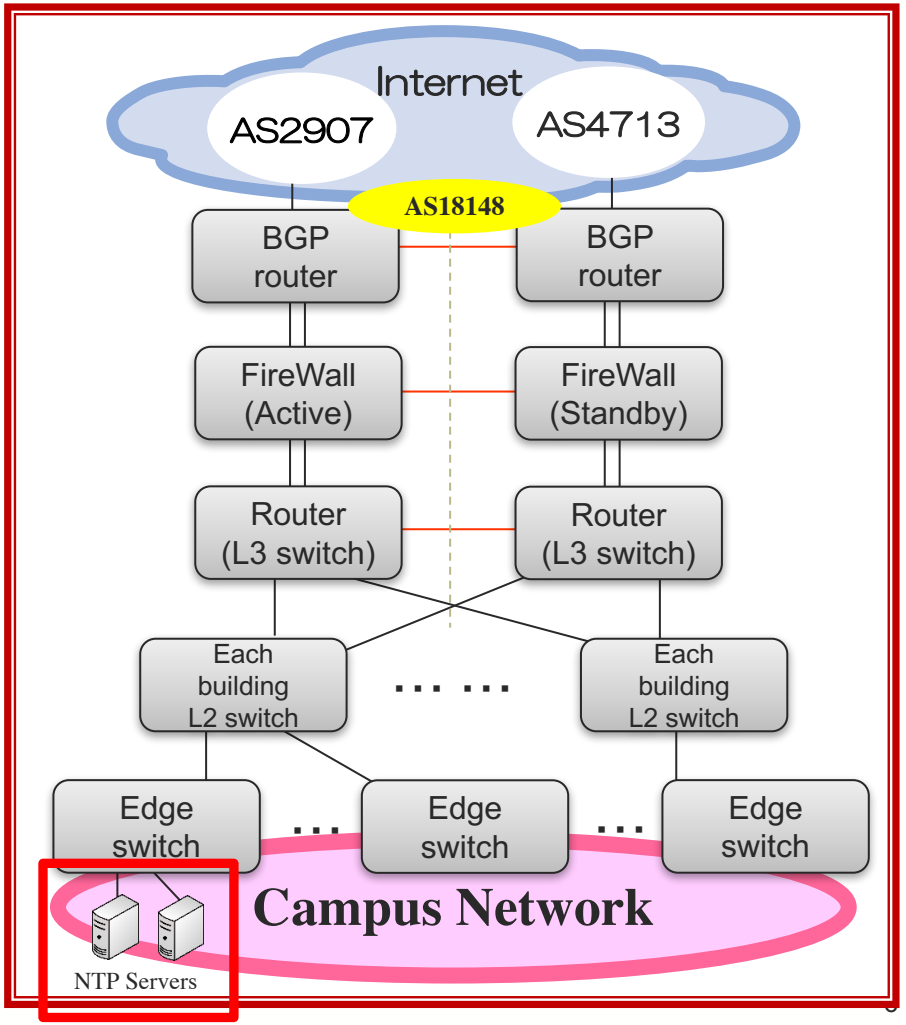
- Determine cause of NTP traffic
- Reduce NTP traffic

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
- Posted “Request of NTP traffic dispersion" to bulletin board named 2channel (Ni-channel: Japanese online forum) on January 20th 2005
  - Approximately 900 NTP requests per second
  - Bandwidth approximately 2Mbps

Network configuration diagram

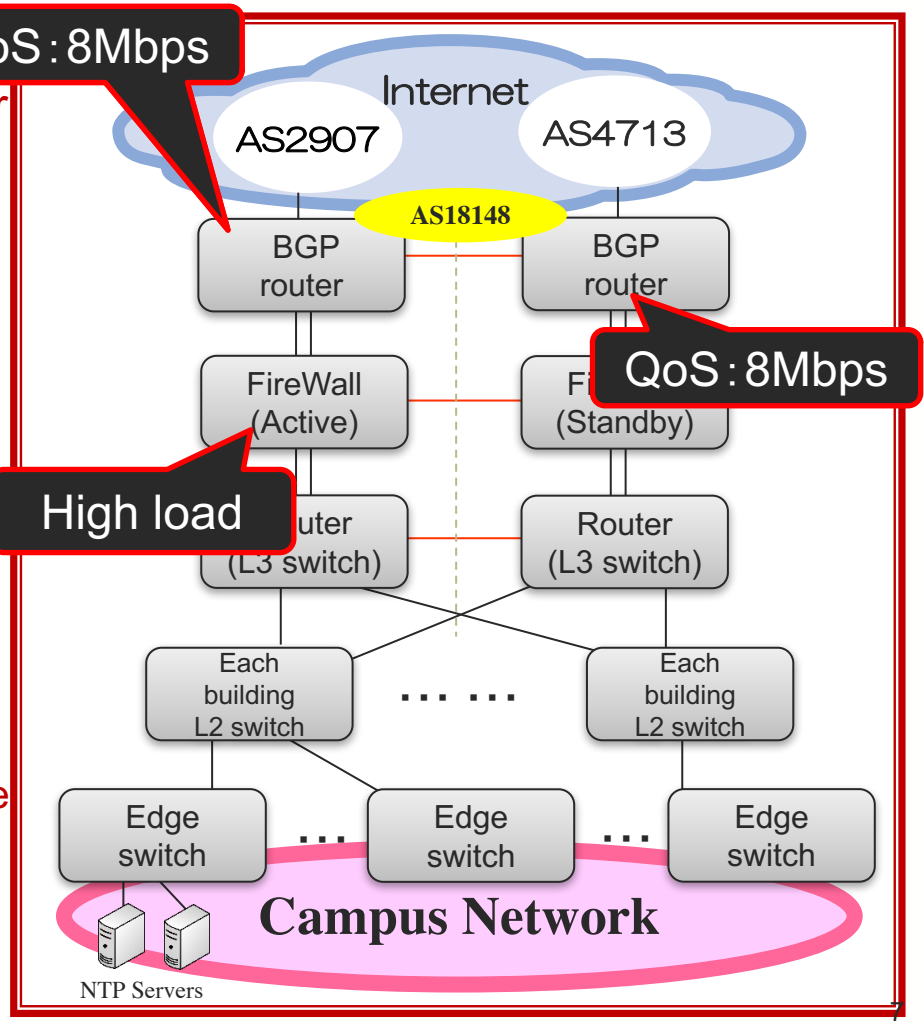
- Until August, 2015
- NTP servers were located in laboratory
  - Edge of campus network
  - Traffic increases momentarily every hour on the hour



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

Incident case

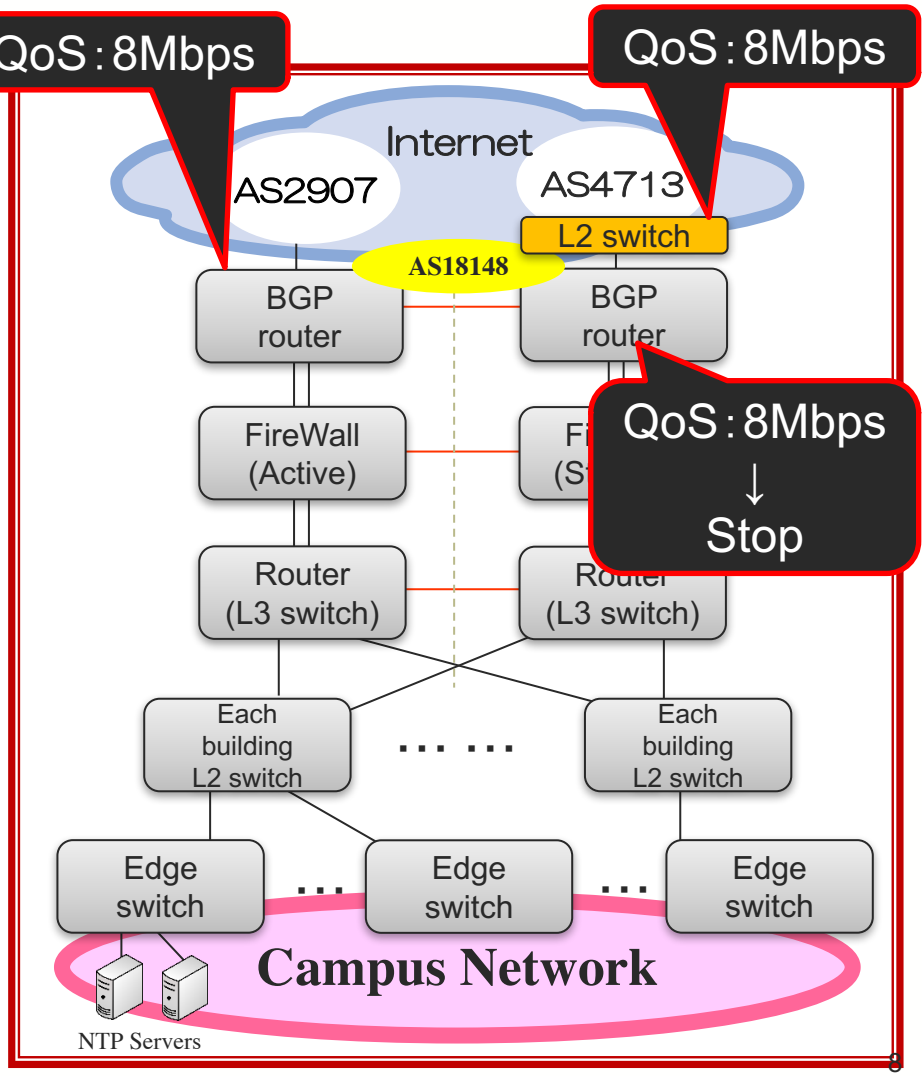
- 8Mbps rate-limiting for NTP was already configured at the BGP router connecting to AS4713
  - To address an issue of high CPU load on firewalls due to a huge number of NTP retry packets from clients while NTP servers were stopped for maintenance
  - No rate-limit at the BGP router connecting to AS2907
- Friday, February 14, 2014
  - Third incident related to the NTP service happened (total 4 troubles)
- NTP traffic through AS2907 was increased, and caused high CPU load on firewalls
  - Introduced 8Mbps rate-limiting at the BGP router connecting to AS2907
  - Internet connectivity was restored even though it's a bit slower than usual



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

Incident case (2)

- Saturday, February 15 (the next day)
- The BGP router connecting to AS4713 went down
  - QoS handling on the router was software-based, caused high CPU load on the router
- Installed a new L2 switch to perform hardware-based QoS
  - restored the router without QoS
- Set 8Mbps rate-limiting for NTP traffic on both links



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

Traffic during network failure

- Traffic through AS2907 to AS18148 increased to approximately 135Mbps

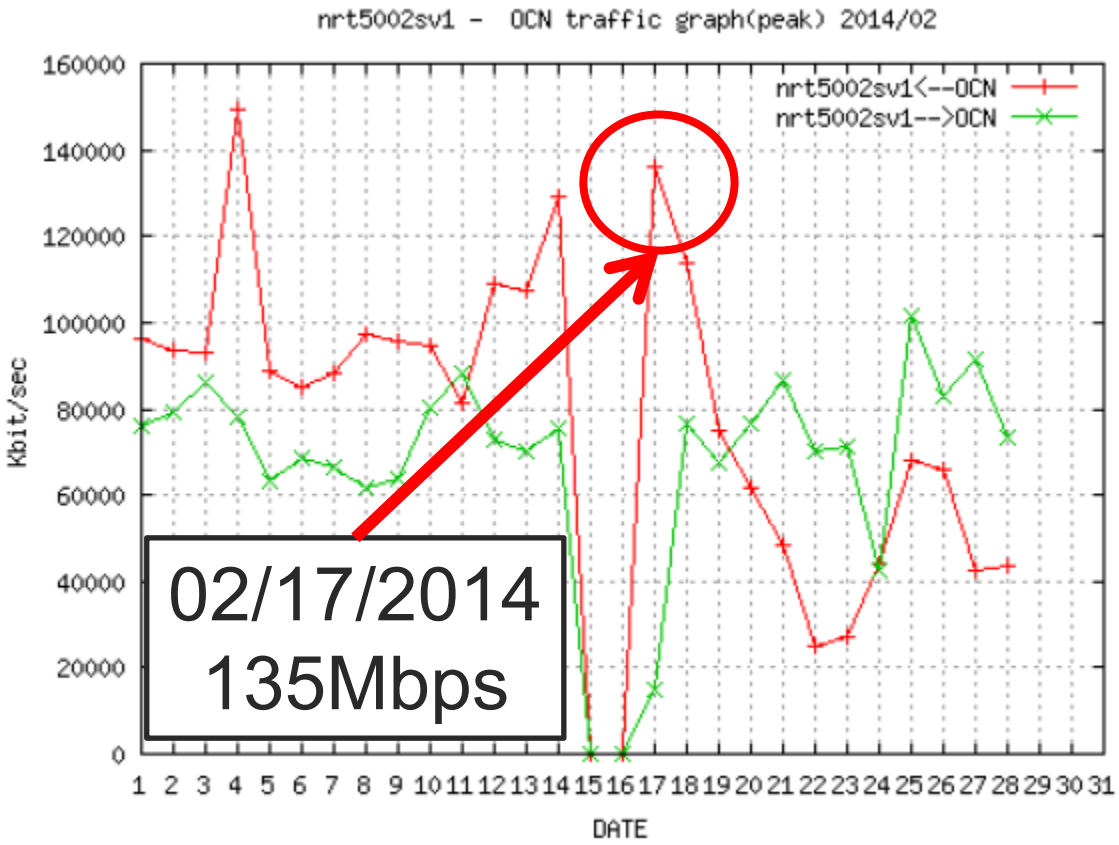


図 5.5 nrt5002sv1 GigabitEthernet0/2 (2014 年 2 月) (peak)

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

Traffic during network failure

- Traffic through AS4713 to AS18148 increased to approximately **900Mbps**

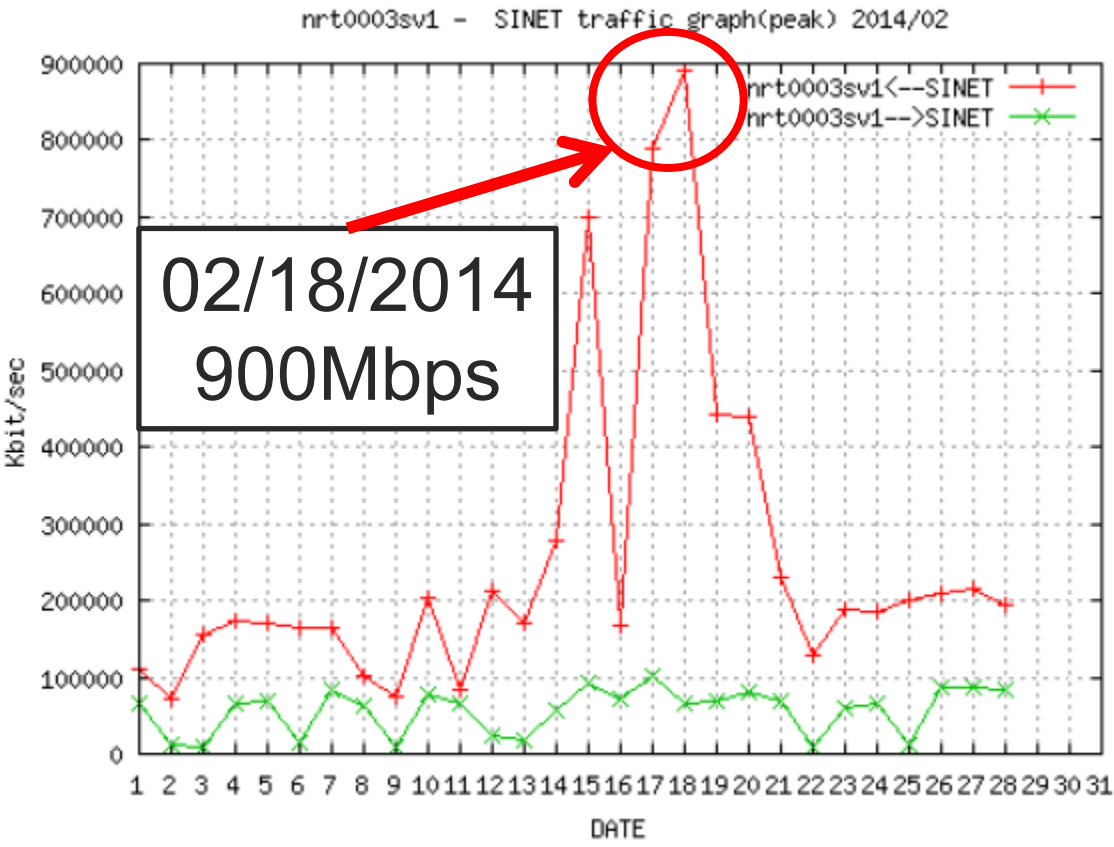


図 5.11 nrt0003sv1 TenGigabitEthernet1/4 (2014年2月) (peak)

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

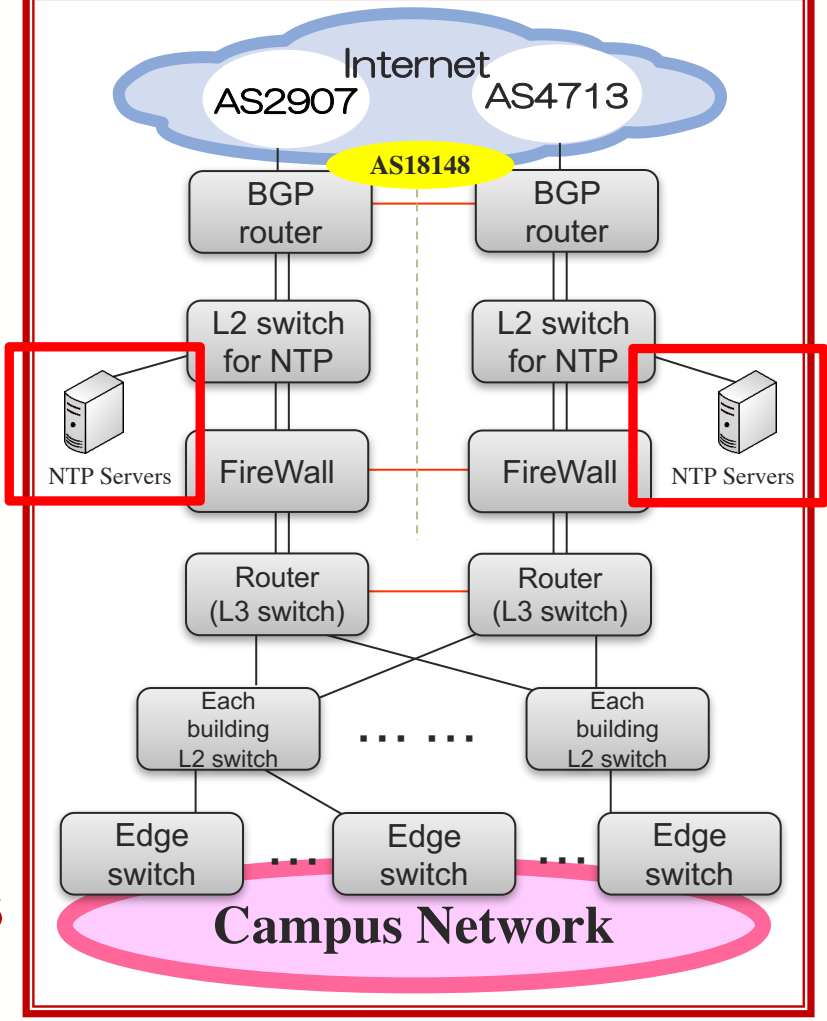
Summary until August, 2015

- NTP service failures cause a huge amount of retry packets, and that causes firewall failures
  - Must continue to reply NTP packets
- 8Mbps bandwidth limit for NTP traffic on both links to upstreams
  - The average NTP traffic subsequently exceeded 8Mbps
    - At that time, we were unable to ascertain what the bandwidth would be
  - Drop NTP packets or change bandwidth limit level, when trouble occurs

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

Current network diagram

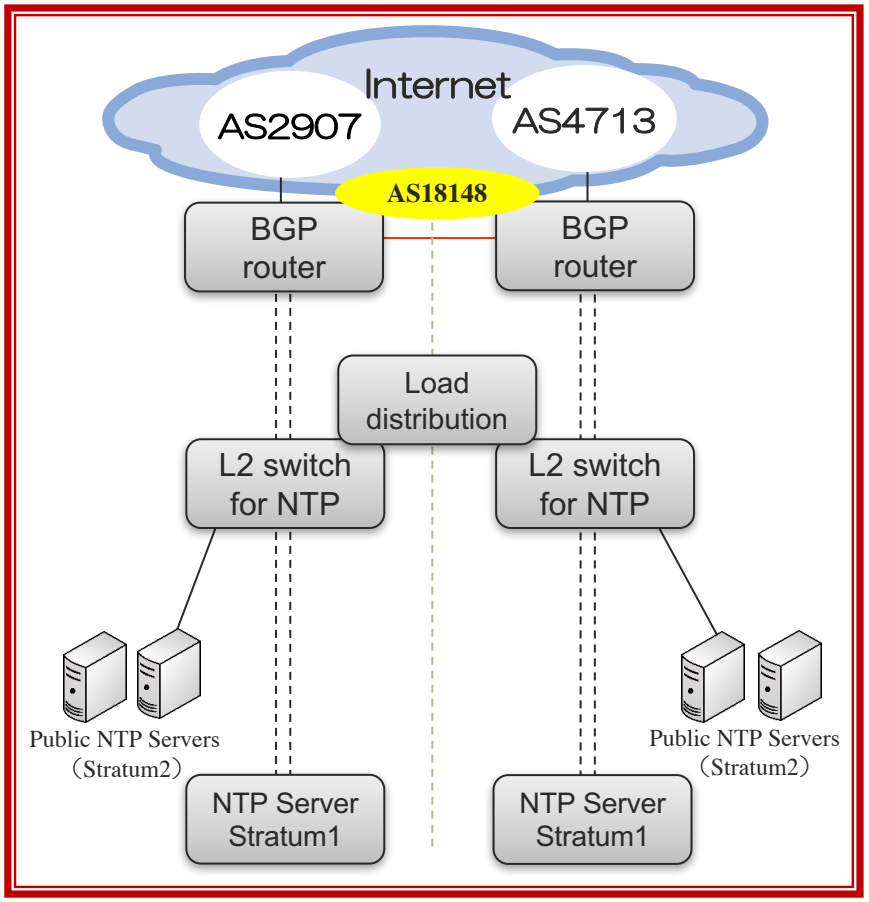
- Changed on September, 2015
- Operating NTP servers in Information Technology Center
  - To avoid high CPU load on firewalls, we moved NTP servers outside of the firewalls



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

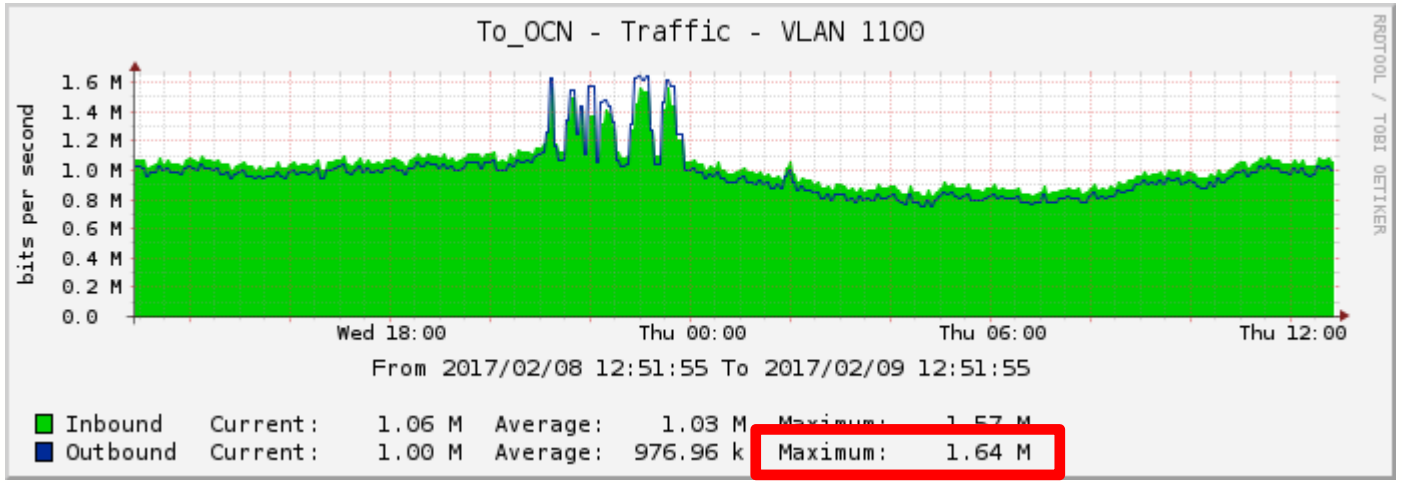
NTP Network configuration diagram

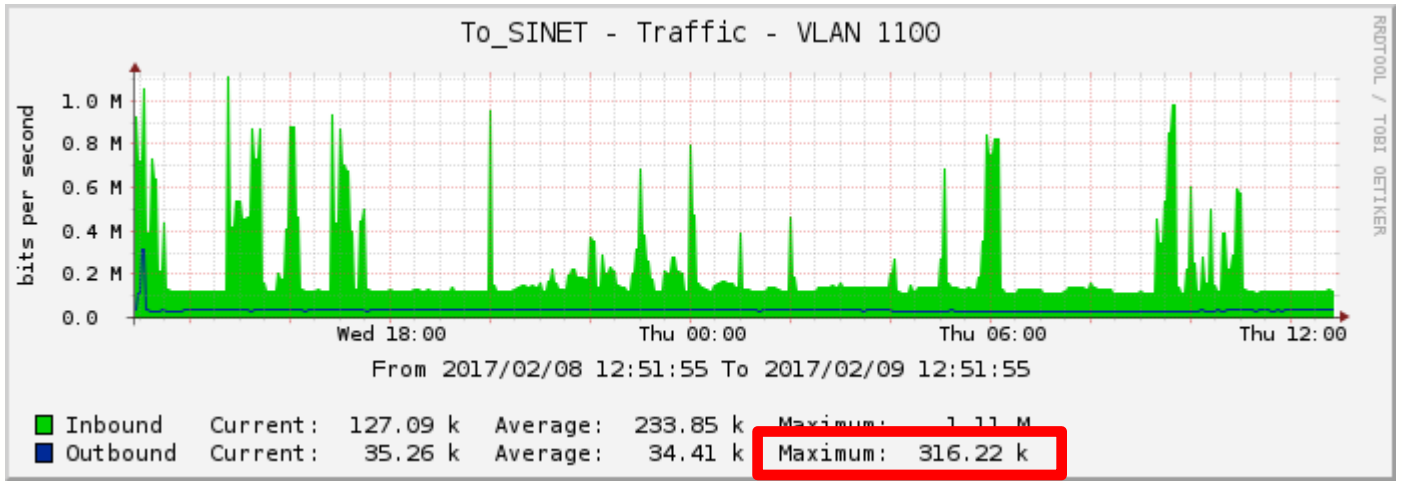
- load distribution by load balancers
- Increased public NTP servers from 2 to 4 in consideration of load and redundancy
- 2 ‘stratum 1’ servers
  - These are not open to public, serving for clients in the campus only



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

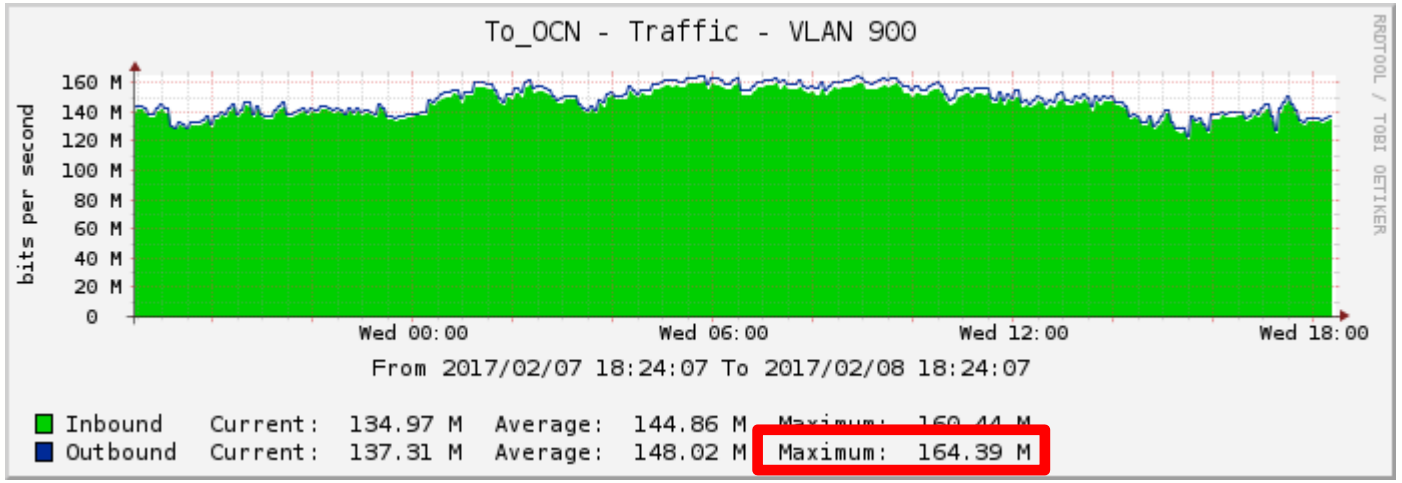
133.100.11.8 Traffic

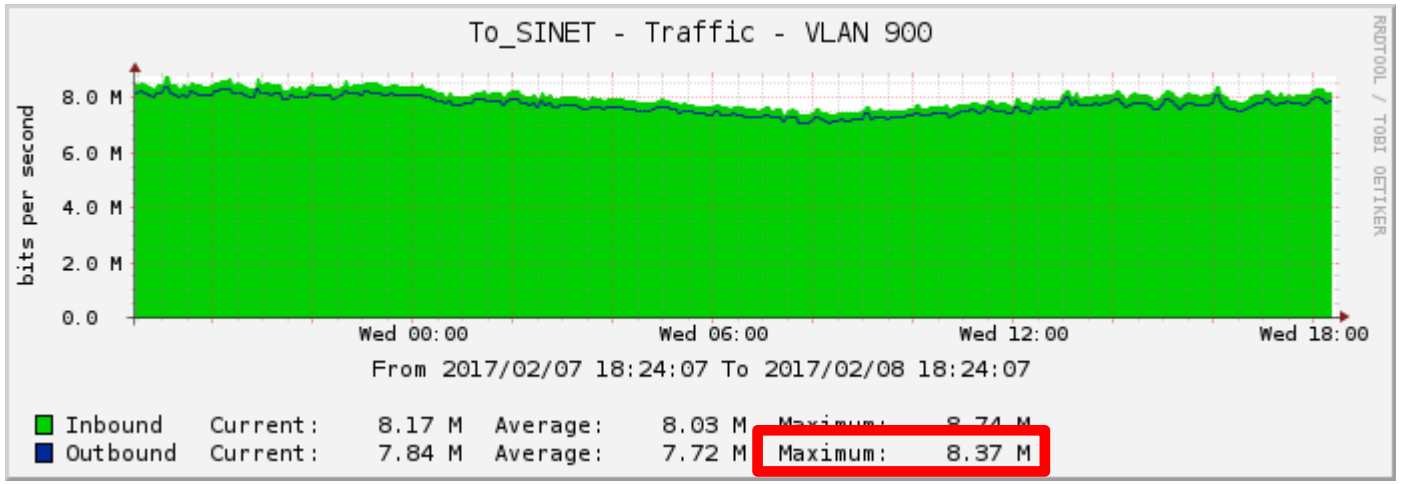




※ AS18148 … Fukuoka University
※ AS2907… Science Information NETwork（SINET）operated by National Institute of Informatics
※ AS4713 … Open Computer Network（OCN）operated by NTT Communications Corporation

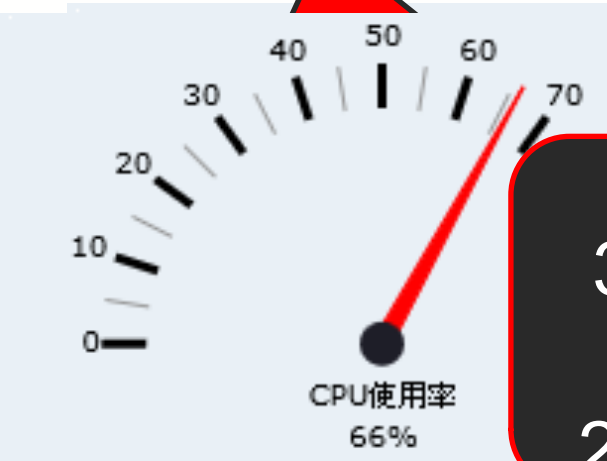
133.100.9.2 Traffic





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

Current traffic (Number of packets)



Total Throughput:
342,539,104 bits / s
L4 Connections:
221,250 Packet / s !!

パフォーマンス

全体のスループット Bits/sec:	342539104
L4 Conns/sec:	221250
L7 Conns/sec:	0
L7 Trans/sec:	0
SSL Conns/sec:	0
IP NAT Conns/sec:	0
全体の新規コネクション毎秒:	221250
現在の全コネクション数:	418361

Analyze using ntopng

- Capturing data from one of the 4 public NTP servers
- Real-time analysis at a dedicated server by “ntopng”

ntop

Flows | Hosts

Hosts by Country

Name	Hosts
CN	4,995
BR	2,239
US	657
VE	674
IT	383
ES	365
AR	371
IN	374
DE	244
RU	165

Autonomous Systems

AS number	Hosts	Alerts	Name
56042	6,318	0	China Mobile communications corporation
28573	5,954	0	S.A.
4134	5,168	0	Chinanet
8048	2,917	0	Servicios, Venezuela
4837	2,877	0	CNCGROUP China169 Backbone
9808	2,086	0	Guangdong Mobile Communication Co.Ltd.
27699	1,169	0	TELEFÃNICA BRASIL S.A
18881	1,317	0	Global Village Telecom
10481	1,044	0	Prima S.A.
6830	858	0	Liberty Global Operations B.V.
11830	725	0	Instituto Costarricense de Electricidad y Telecom.
3320	685	0	Deutsche Telekom AG
7303	667	0	Telecom Argentina S.A.
1267	628	0	Wind Telecomunicazioni SpA
8151	590	0	Uninet S.A. de C.V.
22927	525	0	Telefonica de Argentina
3269	522	0	Telecom Italia S.p.a.
8167	521	0	Brasil Telecom S/A - Filial Distrito Federal
7738	513	0	Telemar Norte Leste S.A.
7018	473	0	AT&T Services, Inc.

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
- TL-WR740N(TP-LINK) is one of devices

```
   93 77.444013   192.168.2.2      133.100.9.2      NTP      90 NTP Version 3, client
   94 77.658785   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
```

Why is it so popular? (3)

- was in source codes of OpenWRT (2005)
  - It's fixed now [0-3].openwrt.pool.ntp.org
  - Cannot connect to two other NTP servers
  - Other vendors might reuse the code and there might be commercial products that are embedded 'default NTP setting'

{ "ntp_server" , "192.5.41.40 192.5.41.41 133.100.9.2" , 0}

Summary

- Statistics of our public NTP servers
  - Approximately 190,000 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
  - At this moment, there is no way to terminate the service

Request: Please do not use our NTP servers

- 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
- If you have contacts of them
  - Please pass the above information
- We would like to take measures by determining the cause of NTP traffic. So if you know particular product or site which uses our NTP servers, please introduce the contact to us.

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

Conclusion

- Would like to determine cause of NTP traffic
- Because of the concentrated nature of NTP traffic we would like to reduce it.

We sincerely appreciate your cooperation.

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

福岡大学

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。
福岡大学