

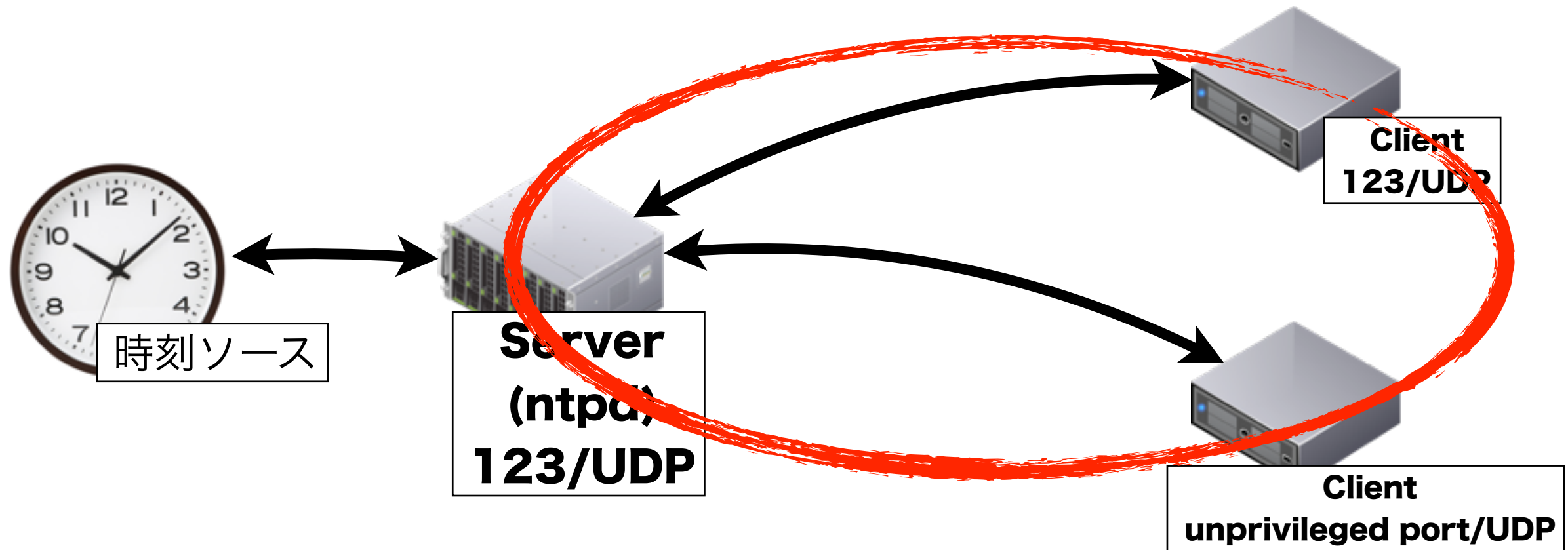


公開NTPサーバーの 運用と課題

Fuminori -Tany- Tanizaki
2017.10.27



おさらい：NTPについて



- ntpdは時刻ソースから時刻をもらい、正確な時刻を保持する。
- サーバーは**123/UDP**で待ち受け、クライアントは**123/UDP**、もしくは**非特権ポート/UDP**で、問い合わせを行う。
- サーバークライアント間でやり取りされるパケットは一般的に『**90byte**』である。
- ntpdがクライアント的に時刻を問い合わせに行くとき、サーバーから返答がないと、多量の問い合わせパケットを送りつける(場合がある)。

■NTPの話題：『正確な時刻』と『時刻を配信する』

福岡大学のNTPの歴史

■**1993/10**：福岡大学のある研究室で実験的に公開NTPサーバーとして運用開始

- **133.100.9.2**
- **133.100.11.8**
- 毎時0分にネットワークが重くなる。

■**2005/1**：アクセス過多問題(2chへの投稿)

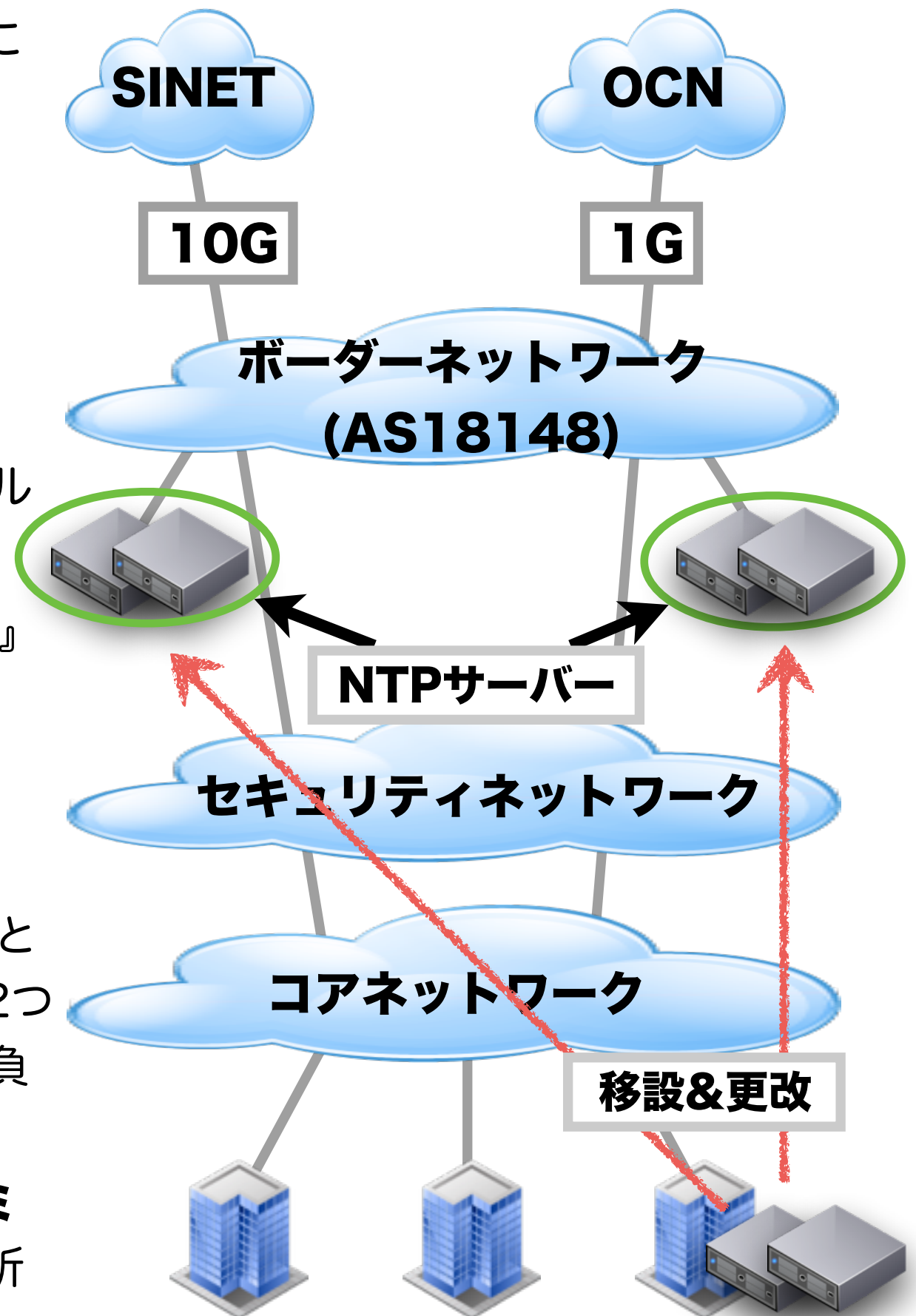
■**2012/12頃**から：NTPサーバー絡みのトラブルが数度発生

- 『**NTPサーバーの停止=ネットワークの停止**』
- **8Mb/s**で帯域制限

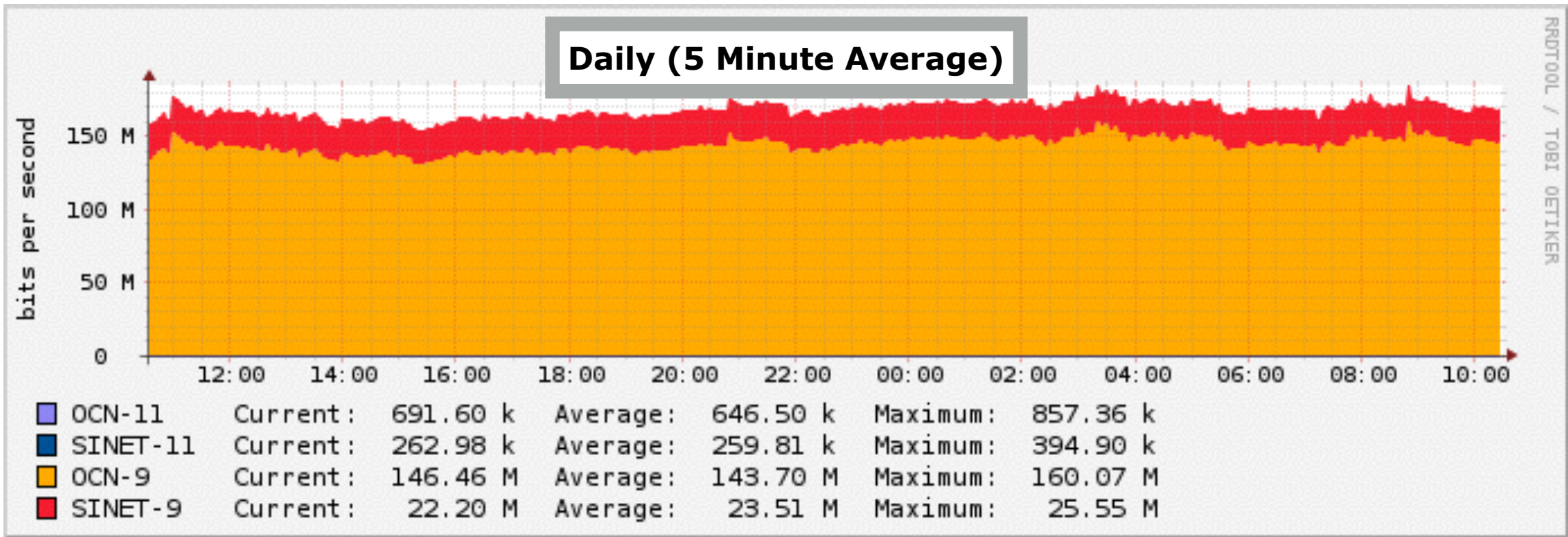
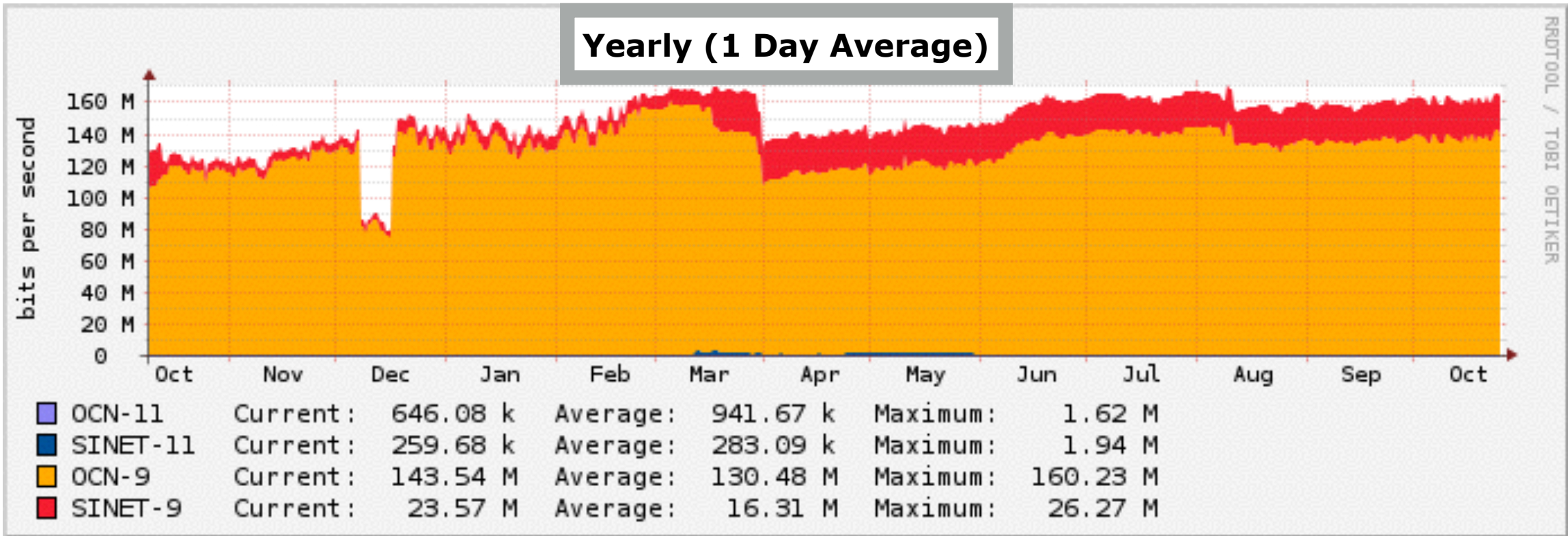
■**2015/4頃**：新NTPシステムの検討開始

■**2015/12頃**：新NTPシステム運用開始

- **対外接続ルータの直下**にロードバランサ(2台)と**NTPサーバー(4台)**を設置し、サービス用の2つのIPv4アドレスに対するNTPトラフィックを負荷分散
- NTPサーバーのうちの**1台のトラフィックをミラー**し、**ntopng**、**Elasticsearch**で分析



現在のトラフィック(イン側)



180Mb/s 210,000query/s

ntopng+ElasticSearchによる分析

イン側パケット数を地図にプロット

国別TOP10

ntop

ntop

elastic

kibana

CN

BR

US

DE

ES

AR

IT

NL

GB

RU



AS別TOP8

ntop

AS number	Hosts▼	Alerts	Name
56042	4,015	0	China Mobile communications corporation
28573	3,325	0	CLARO S.A.
4134	2,890	0	Chinanet
6830	1,689	0	Liberty Global Operations B.V.
3320	1,565	0	Deutsche Telekom AG
3352	1,204	0	Telefonica De Espana
27699	955	0	TELEFÔNICA BRASIL S.A
7922	1,013	0	Comcast Cable Communications, LLC

なぜこんなことに？

■製品マニュアルやweb上の記事に**設定例**として書かれている。

- ネットワーク機器、複合機、IP電話…
- 『ntpを設定しました！』的なweb上の記事

■ググればそんなのがたくさん出てくる。

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
```

Google

"133.100.9.2" pdf

すべて

ニュース

画像

動画

地図

もっと見る

設定

ツール

約 2,160 件 (0.33 秒)

ヒント: 日本語の検索結果のみ表示します。検索言語は [表示設定] で指定できます。

[PDF] TL-SG2424P 24-Port Gigabit Smart PoE Switch with 4 ... - Ne...

images10.newegg.com/.../TL_SG2424P_V1_CLI_Reference_Gu14... このページを訳す

2012/02/14 - ... the time zone is GMT-12, 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-SG2424P(config)# system-time ntp GMT-12 133.100.9.2 139.79.100.163.



TP-LINK
TL-SG3210/TL-SG3216/TL-SG3424/TL-SG3424P
JetStream L2 Managed Switch

なぜこんなことに？

■機器のファームウェアにNTPサーバーのIPv4アドレスが埋め込まれている。

- ・家庭向けブロードバンドルータ
- ・無線LAN AP
- ・Webカメラ

```
%ls -l libshared.so
-rw-r--r--  1 tany  staff  69612  3 28 18:49 libshared.so
%strings libshared.so | grep 133.100.9.2
192.5.41.40 192.5.41.41 133.100.9.2
```

■Linux(busybox)ベース

- OpenWRTもしくはBroadcomのリファレンスコードに関係あり？
- ntpdもしくはntpdate相当で時刻同期をしている？

■設定変更できない！！



 tp-link TL-WR740N



Tenda®
W309R

FAQとと思っていること

■これってDDoSみたいなもんだよね？

- **そう思います！！！！！！しかも、ほっとくとずーっとこのままかも？**

■NTPサーバーを止めればいいじゃん！or 大学側のBGPルータでフィルタすれば？

- 世界中からリクエストパケットを多量に送りつけられて、対外接続が埋め尽くされる可能性があります…orz

■じゃあ、**上流のISPでフィルタ**してもらえばいいじゃん！

- 技術的には可能ですが、その**フィルタを維持し続けて**もらえるのでしょうか？
- **数年後にふと削除**されたりすると、えらいことになりそう…。

■最終的にはサービスをやるべく模索中

- **みなさん使わないで！！！！！！**
- 自分たちで**nullに捨てる、流量を観測**し続ける。
- 今のトラフィック解析は全体の25%、**全体を解析**したい。

■トラフィックを減らす努力をしないと！

- **中国のISP**の人と話がしたい！
- **ブロードバンドルータを作っている人**と話がしたい！
- **多くの人**に知ってもらいたい！



Fukuoka University Public NTP Service
Deployment Use case.
APRICOT2017
Sho Fujimura/Fukuoka University

QUNOG

九州沖縄ネットワーク・オペレーターズ・グループ

QUNOG10

2018/2/9

鹿児島県鹿児島市

<https://www.facebook.com/QUNOG/>