Efforts Against NTP Reflection Attacks in JP.

2014 Feb.

NTP-TALK WG (JANOG)
Miki Takata
Tomohiro Nakashima
Kaname Nishizuka

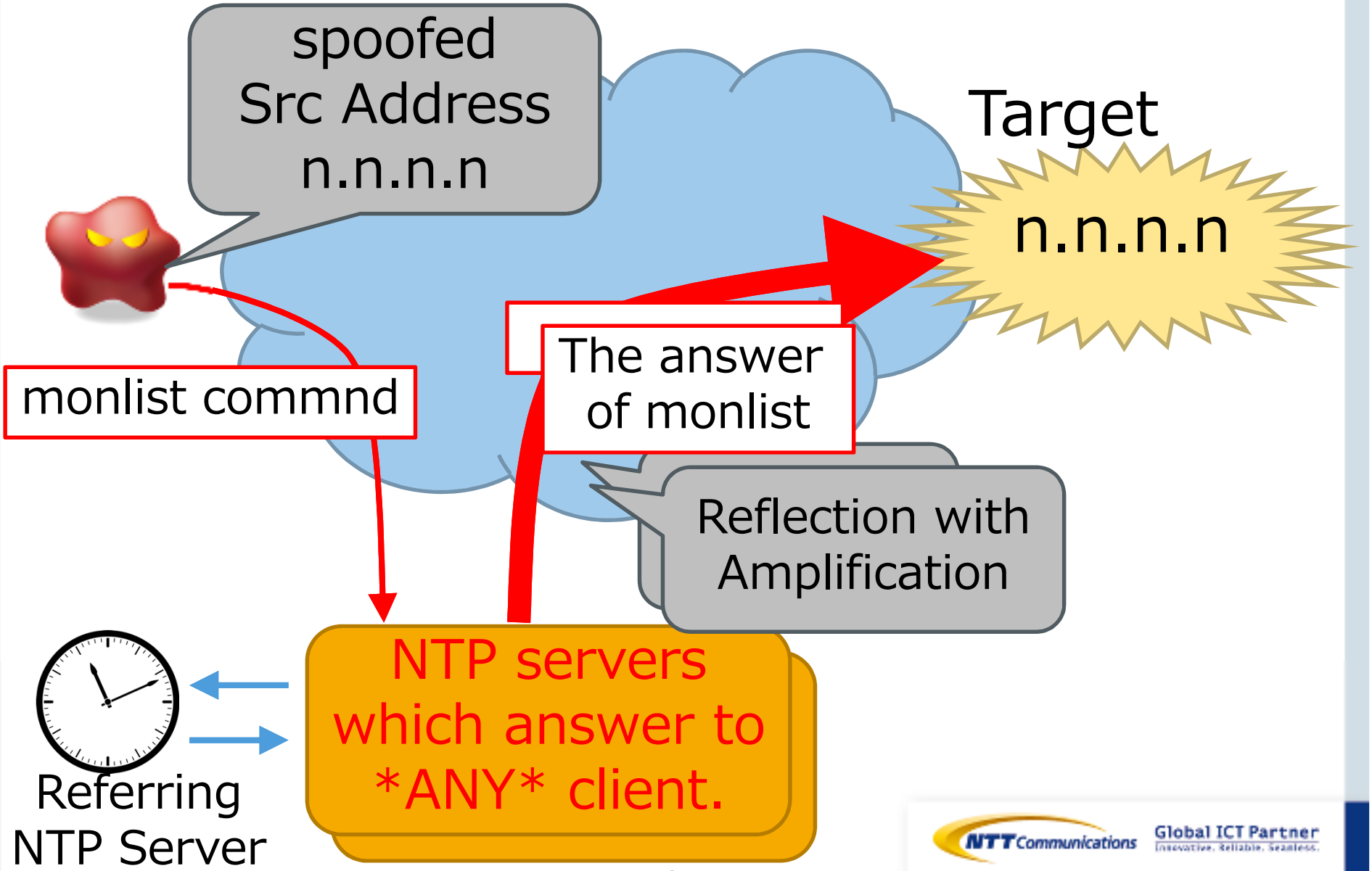
What is “NTP reflection attack”

- One of the methods of DDoS Attack
  - Just flooding target circuit.

- Using spoofing and reflection.
  - The victim’s IP address is spoofed.
  - Reflector: Inappropriately configured NTP servers
  - The most effective reflection is NTP monlist command
    - ✓ Amplitude (=Answer/Query) is over hundreds (!)

- The mechanism is basically same as DNS amp.

An illustration of NTP reflection attack



NTP Attacks in Our(ntt.net) Network

- NTP attacks happen everyday
- attack size is usually around 1Gbps
- not all of them were contacted by customers
- a lot of servers have been observed with NTP batch / fixes but still there are a lot of vulnerable devices out there

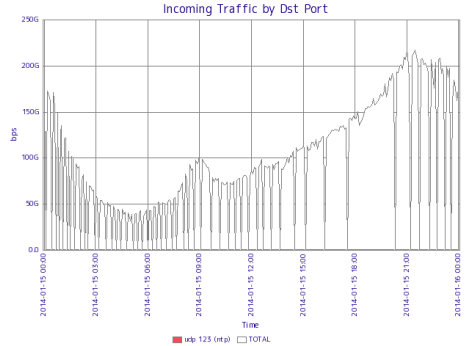
alert from US-CERT (2014/01/13)

Alert (TA14-013A)

NTP Amplification Attacks Using CVE-2013-5211

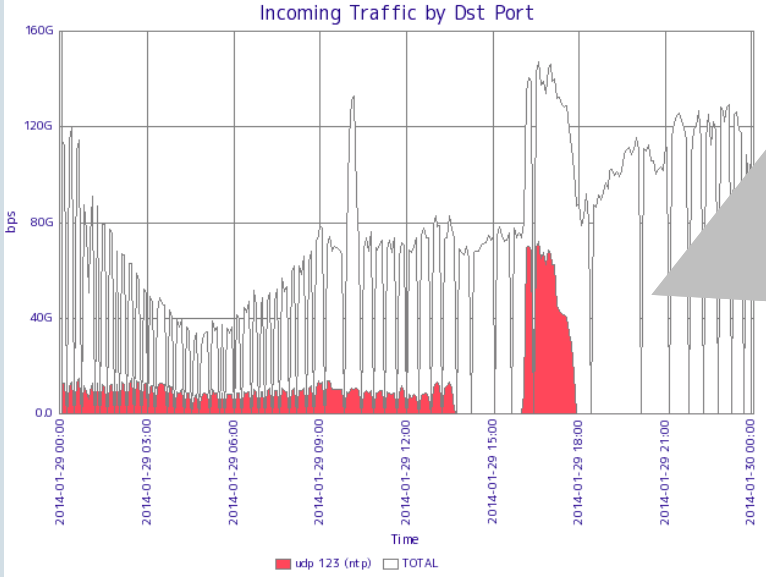
Original release date: January 13, 2014 | Last revised: February 05, 2014

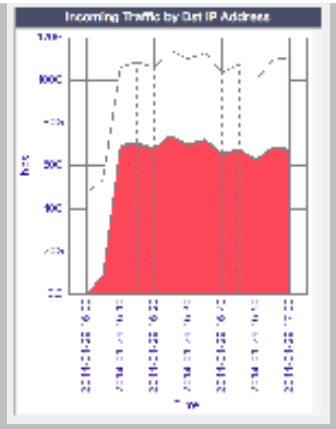
NTP traffic for 1 of our customer



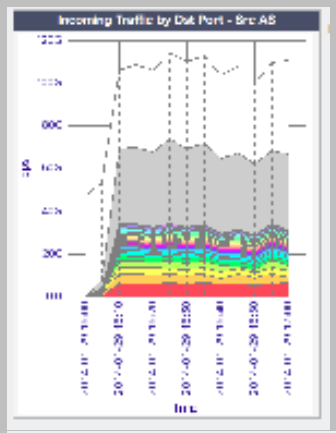
← almost nothing

2 weeks after that … (2014/01/29)

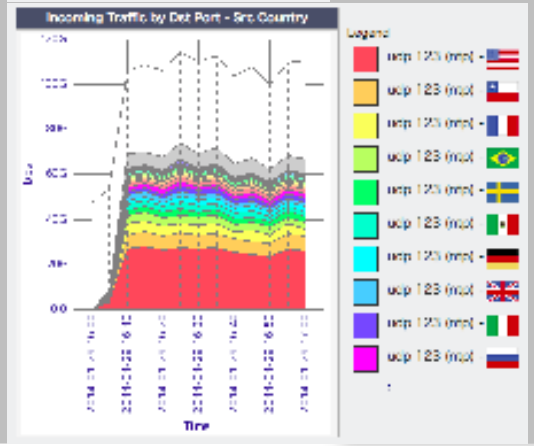




sorted by Destination IP



sorted by Destination AS



Why NTP ?

■ Comparing Reflection Protocols

Protocol	Amplitude	The Size of Request	The Size of Response
echo	1	–	–
chargen	～25	～20Byte	～512Byte
DNS	～25	～20Byte	～512Byte
DNS(EDNS0)	～75	～20Byte	～1500Byte
NTP(monlist)	～200	～18Byte	～44,000Byte
snmp(GET BULK)	?	100Byte	depends

- Moreover, there are many vulnerable NTP servers in wild.

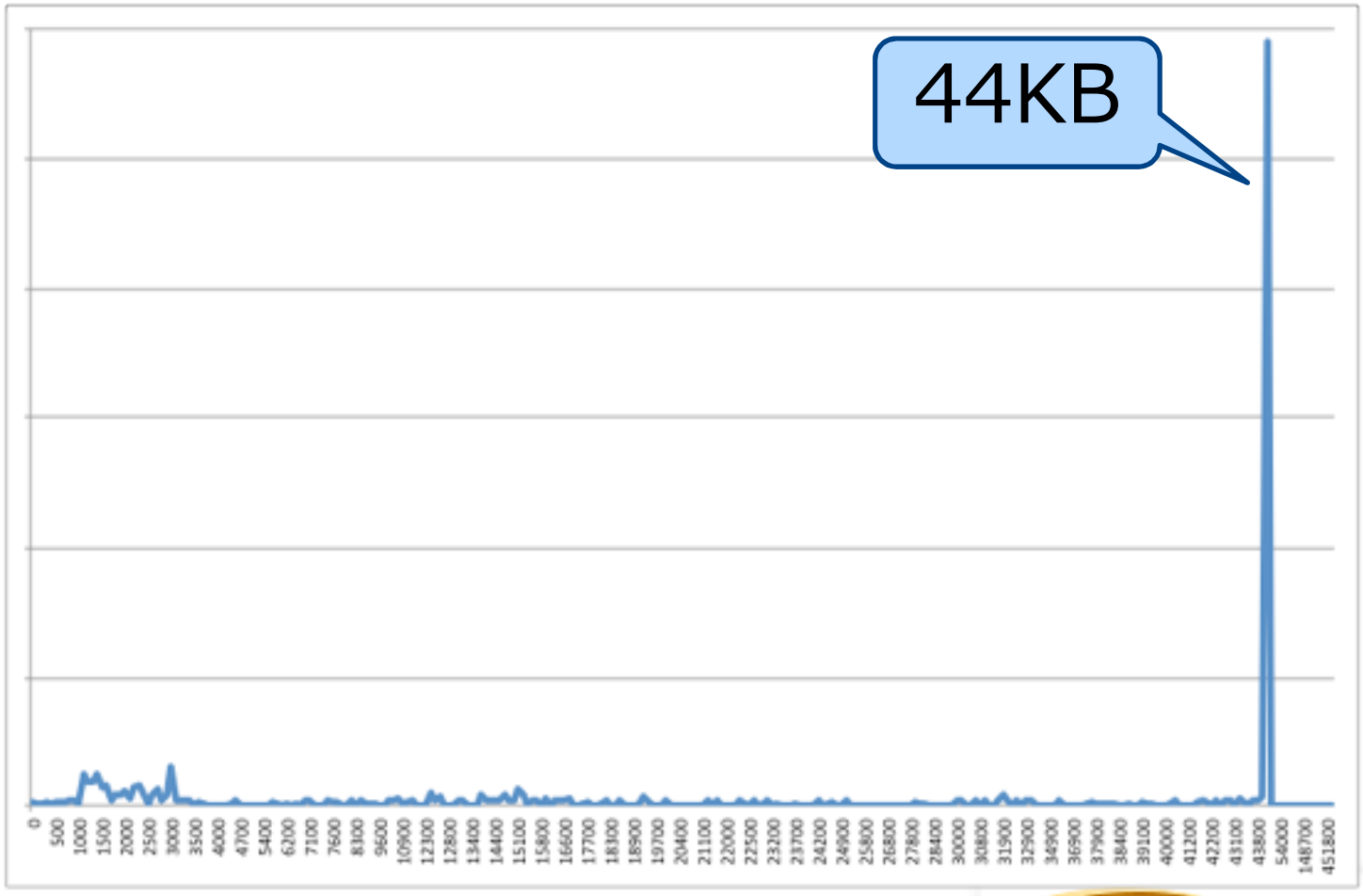
monlist

- What is monlist command
  - Getting list of NTP client addresses and other management information.
  - Max 600 lines => 44KB => 100packets
    - ✓ Depends on version of NTPd
  - It's super effective! in case the number of NTP clients is large.
- Example
  - ntpdc –n –c monlist <NTP server IP address>

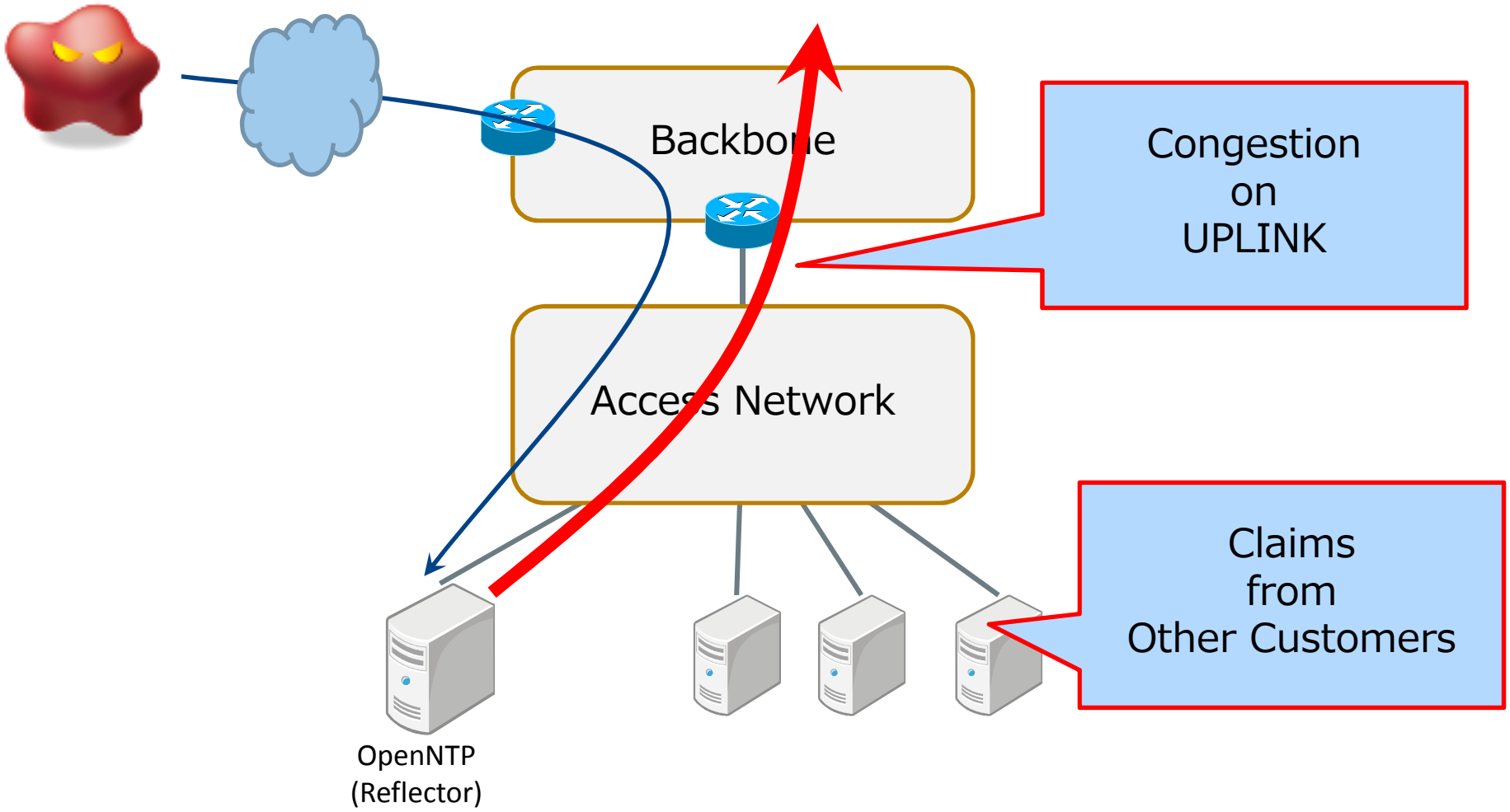
```
$ /usr/sbin/ntpdc -n -c monlist 192.0.2.123
remote address          port local address      count m ver code avgint  lstint
===============================================================================
192.0.2.70           57124 192.0.2.123            3 7 2     0   3194      0
192.0.2.51             123 192.0.2.123         3387 4 4     0   1008     39
192.0.2.69           38323 192.0.2.123           11 7 2     0  27441  63313
192.0.2.2            60947 192.0.2.123            2 7 2     0 554028 101944
   :                   :                  :          :
192.0.2.27           58440 192.0.2.123            1 7 2     0      0  244503
```

The Size of Reflected Answer

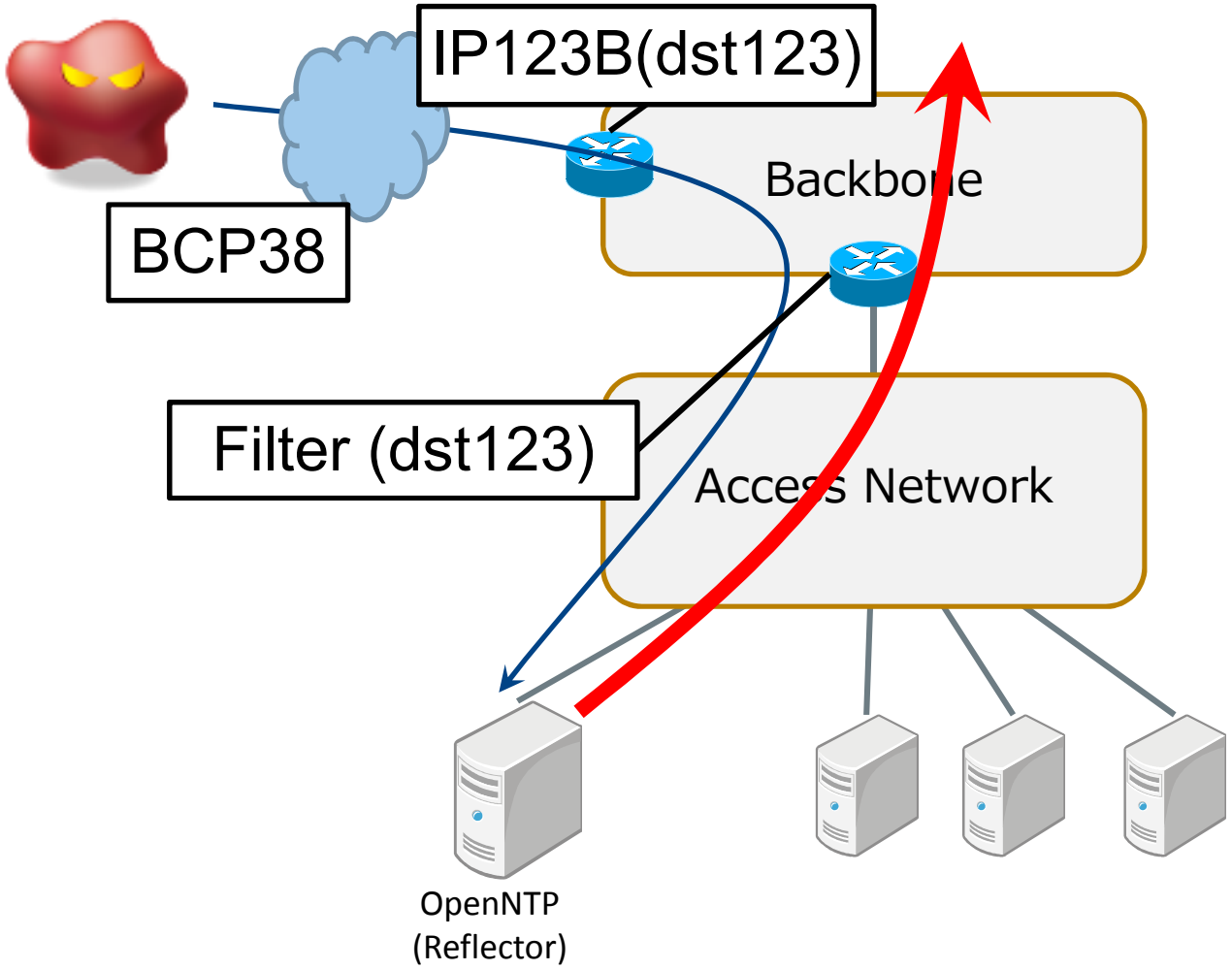
- Most of the answer is 44KB = 600lines
  - they could be injected false NTP clients.



Case: Congestion on UP-LINK of Access Network



Defense in many ways.



Ask customer
to check configuration

Countermeasures

- Stopping customers and myself from becoming Reflector
  - Review my own equipment.
  - Contact customers to change their configuration with harmless NTP configuration template.
  - Filter UDP/123 by ACLs
- Protecting customers and myself from reflected attack
  - Filter UDP/123 by ACLs
  - Buy mitigation devices and services...
- Make the Internet without any reflection attack
  - BCP38 / BCP84 (Source Address Validation)

WG for talking about NTP related issues

- NTP-talk WG in JANOG
  - Chair: Miki Takata, Tomohiro Nakashima
  - Term: 2014 Jan.24 – 2014 Jul. 31
  - Target:
    - ✓ Coping with NTP related issues
    - ✓ Especially about NTP Reflection Attack
  - Output:
    - ✓ Experiments on NTP
    - ✓ Documentation about NTP and NTP Reflection Attack

- What is WG in JANOG ?
  - Discuss about specific issues in short term

Stop NTP Attacks. Save NTP Service.

Your cooperation is important

- To clarify technical problems.
  - Recent Attacks and Future Threats
  - Problematic Implementation
    - ✓ Make a guideline.
- To make useful references about various countermeasures
  - Configuration templates for many platforms
  - How to filter it.
  - Caution points of dealing with customers.
- The targets are:
  - Stopping NTP Attacks immediately.
  - Avoiding from turning off all NTP services.
- Contact: ntp-talk-wg@janog.gr.jp

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

References(1)

- Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks
  - http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks
- NTP reflection attack
  - https://isc.sans.edu/forums/diary/NTP+reflection+attack/17300
- NTP DoS reflection attacks
  - https://cert.litnet.lt/en/docs/ntp-distributed-reflection-dos-attacks
- New DoS attacks taking down game sites deliver crippling 100Gbps floods
  - http://arstechnica.com/security/2014/01/new-dos-attacks-taking-down-game-sites-deliver-crippling-100-gbps-floods/
- Configuration template
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-endrun-template.html

References(2)

- JPCERT/CC
  - https://www.jpcert.or.jp/at/2014/at140001.html
  - http://jvn.jp/cert/JVNVU96176042/
- @Police
  - https://www.npa.go.jp/cyberpolice/detect/pdf/20140117.pdf

- Amplification Hell: Revisiting Network Protocols for DDoS Abuse
  - Christian Rossow. 2014 Network and Distributed System Security Symposium, NDSS 2014, San Diego, CA, USA
  - http://www.internetsociety.org/ndss2014/programme#session1
    - ✓ We revisit 14 popular UDP-based protocols of network services, online games, P2P filesharing networks and P2P botnets, all of which are vulnerable to amplification DDoS attacks. We leverage traffic analysis to detect attack victims and amplifiers, showing that attackers already started to abuse amplification-vulnerable protocols other than DNS.