# IPv4 Background Traffic

Geoff Huston

George Michaelson

APNIC R&D

Tomoya Yoshida

NTT Communications

Manish Karir

Merit

# Network “Background Radiation”

- Most network traffic is the result of some form of initial two-party rendezvous
- But there is a subset of network traffic that is completely unsolicited (and generally unanswered)
  - “leakage” from private networks
  - badly configured hosts
  - probes and scans
- This unsolicited traffic forms a constant background of network activity, or “background radiation”

# “Background Radiation” Questions

- How intense is this background radiation?
- Do some parts of the IPv4 address space attract consistently higher levels of background traffic than other parts?
- Are there “toxic hot spots” in the IPv4 address space?

# APNIC's Situation

As we get down to the last few /8s in IPv4 there is a concern that some parts of these networks have a history of prior use that add to the background traffic level

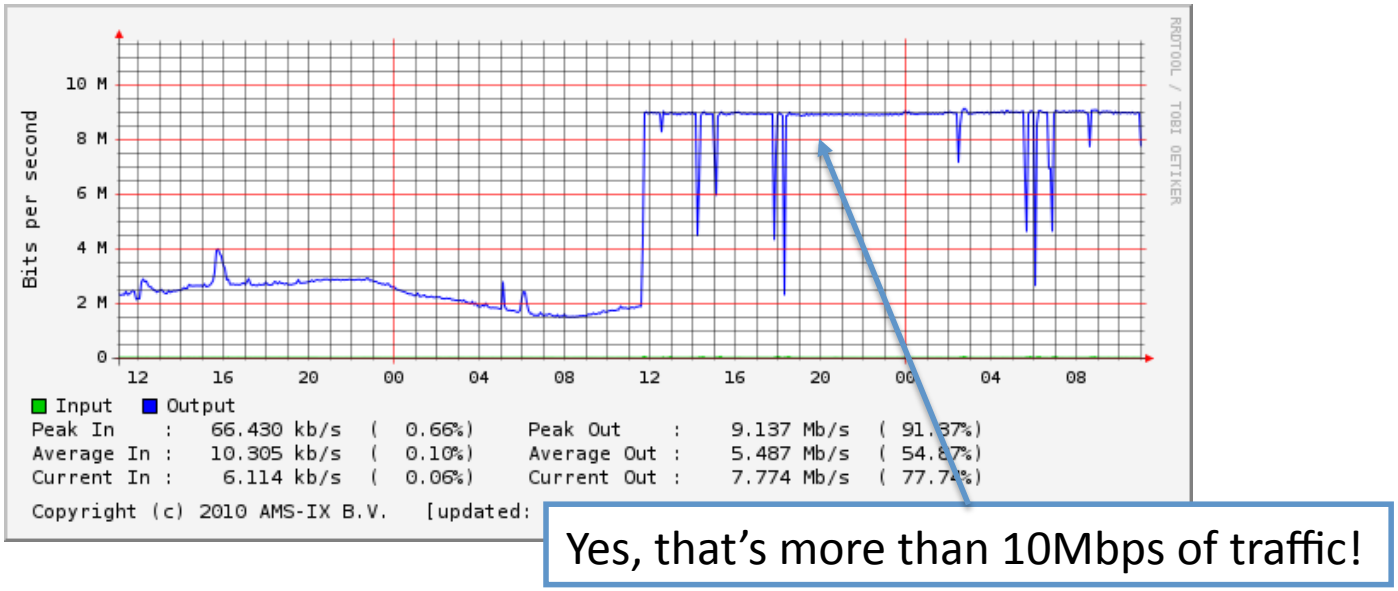
In 2010 APNIC has been allocated:

- **1.0.0.0/8** – often used in ad-hoc private contexts
- **14.0.0.0/8** – originally designated for use in interfacing to public X.25 networks
- **223.0.0.0/8** – used in ad hoc private contexts

# First Warnings

- 27 January 2010 RIPE NCC announces 1.1.1.0/24, 1.2.3.0/24, 1.50.0.0/22 and 1.255.0.0/16

http://labs.ripe.net/content/pollution-18

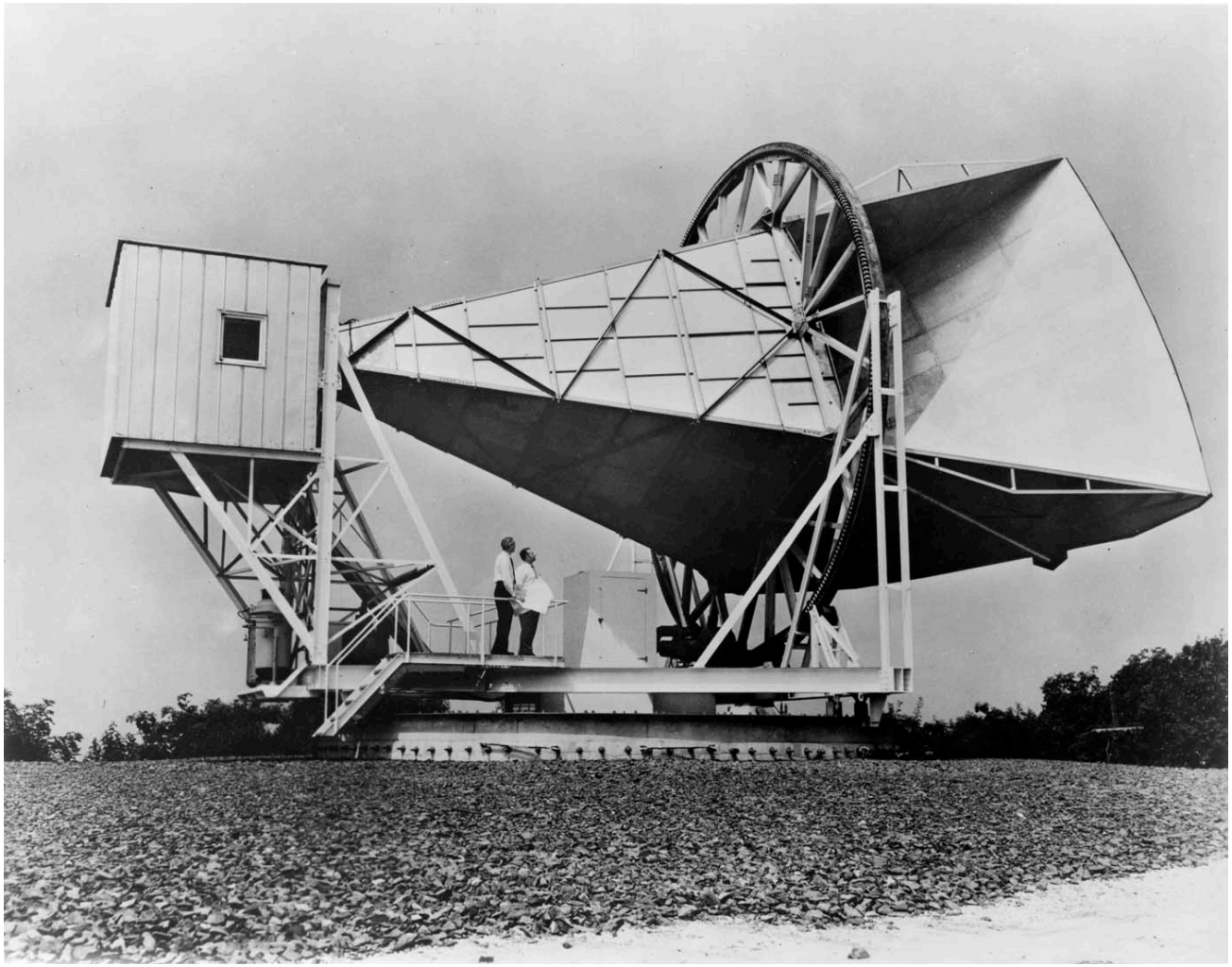



Yes, that's more than 10Mbps of traffic!

# Studying 1/8

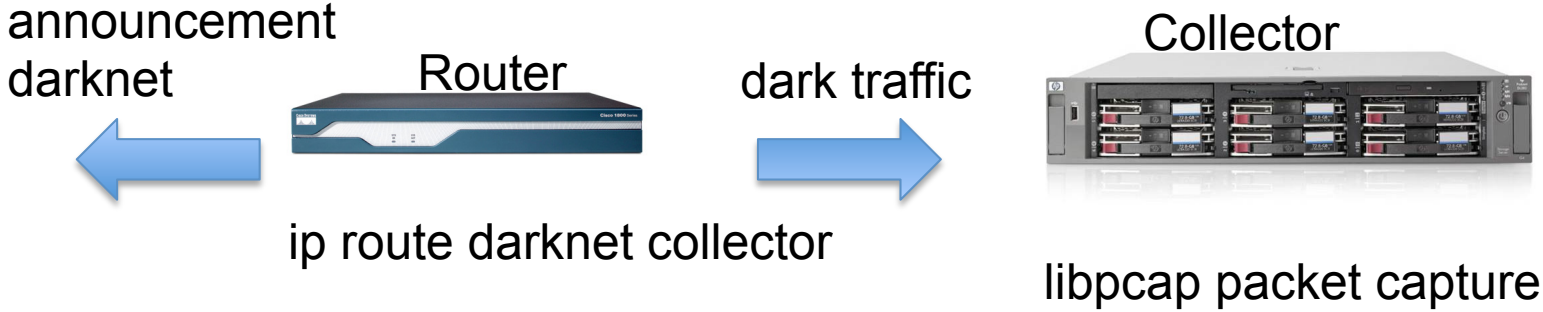
- There are some questions here:
  - Just how “bad” is 1.0.0.0/8?
  - Is this uniform, or are there “hot spots”?
  - Is this malign or private use leakage?
  - Is this “normal” when compared to other /8s?
- APNIC has commenced a program of analysis of the spectrum of “background” traffic in the /8s passed to APNIC by the IANA, prior to allocation to try and answer these questions

# Radiation Detection



The Holmdel Horn Antenna, at Bell Labs, on which Penzias and Wilson discovered the cosmic microwave background radiation

# IP Radiation Detector




Passive Detector: all incoming traffic is recorded
collector emits no traffic in response

Active Detector (Internet sink*): all incoming traffic recorded
ICMP, TCP and UDP responses generated
Application responses for HTTP, FTP, SMB,…

* "On the Design and Use of Internet Sinks for Network Abuse Monitoring",
Vinod Yegneswaran1 and Paul Barford1 and Dave Plonka2, University of Wisconsin, Madison
In *Proceedings of Symposium on Recent Advances in Intrusion Detection, 2004*
http://pages.cs.wisc.edu/~pb/isink_final.pdf

# Bigger, Badder, Faster

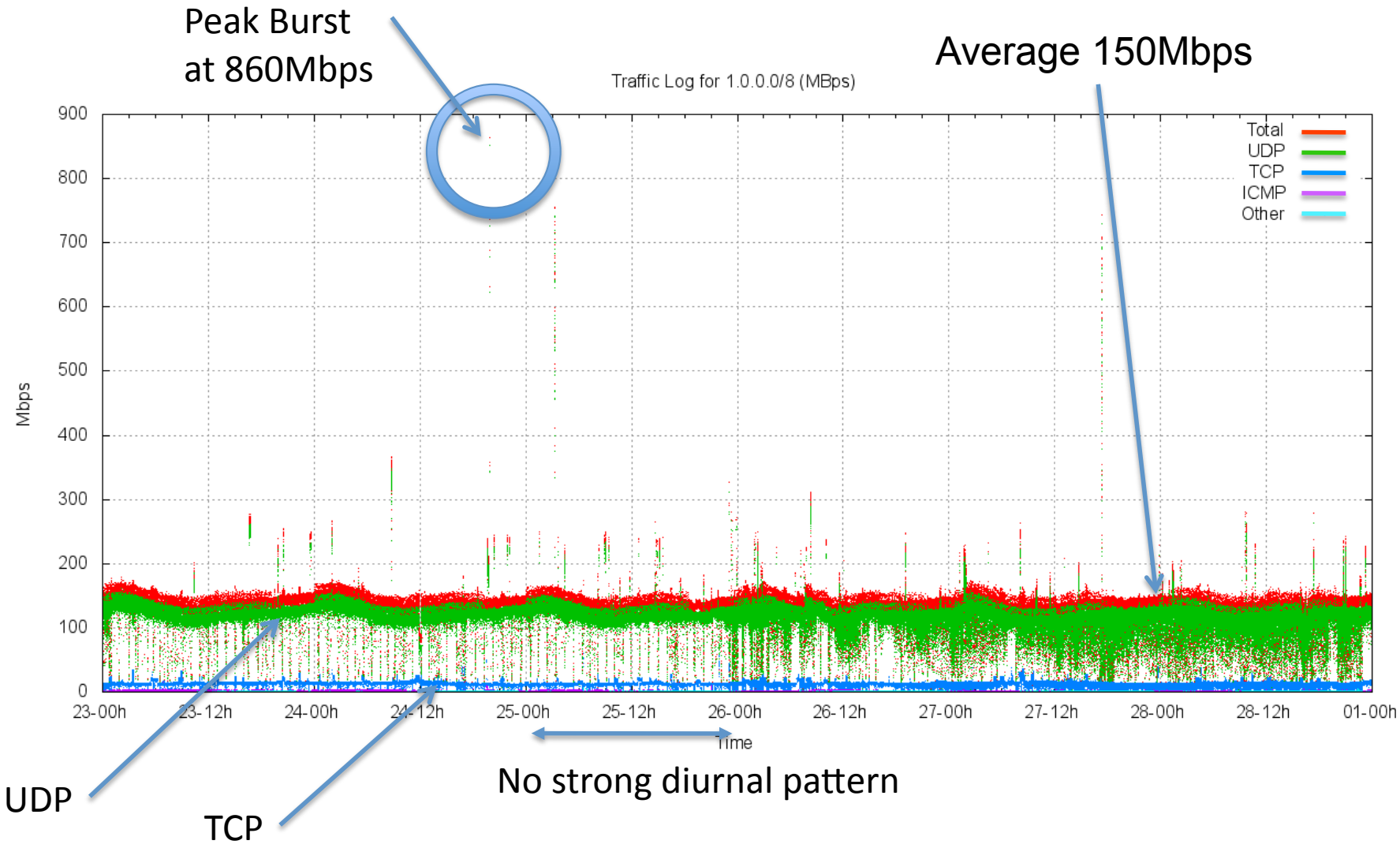
- To do this we needed multi-gig access and traffic collectors and multi-Tb disk space
  - this exceed's APNIC's lab systems and transit capacity
- We have sought collaborators in the R&D Ops community for assistance in this work
  - we had many responses, for which we are grateful
  - We have been working with Merit, NTT, AARNet, Google and You Tube

    all of whom have been fantastic collaborators – thanks!
- One week announcements of /8 address blocks
  - Then working through the resultant packet data

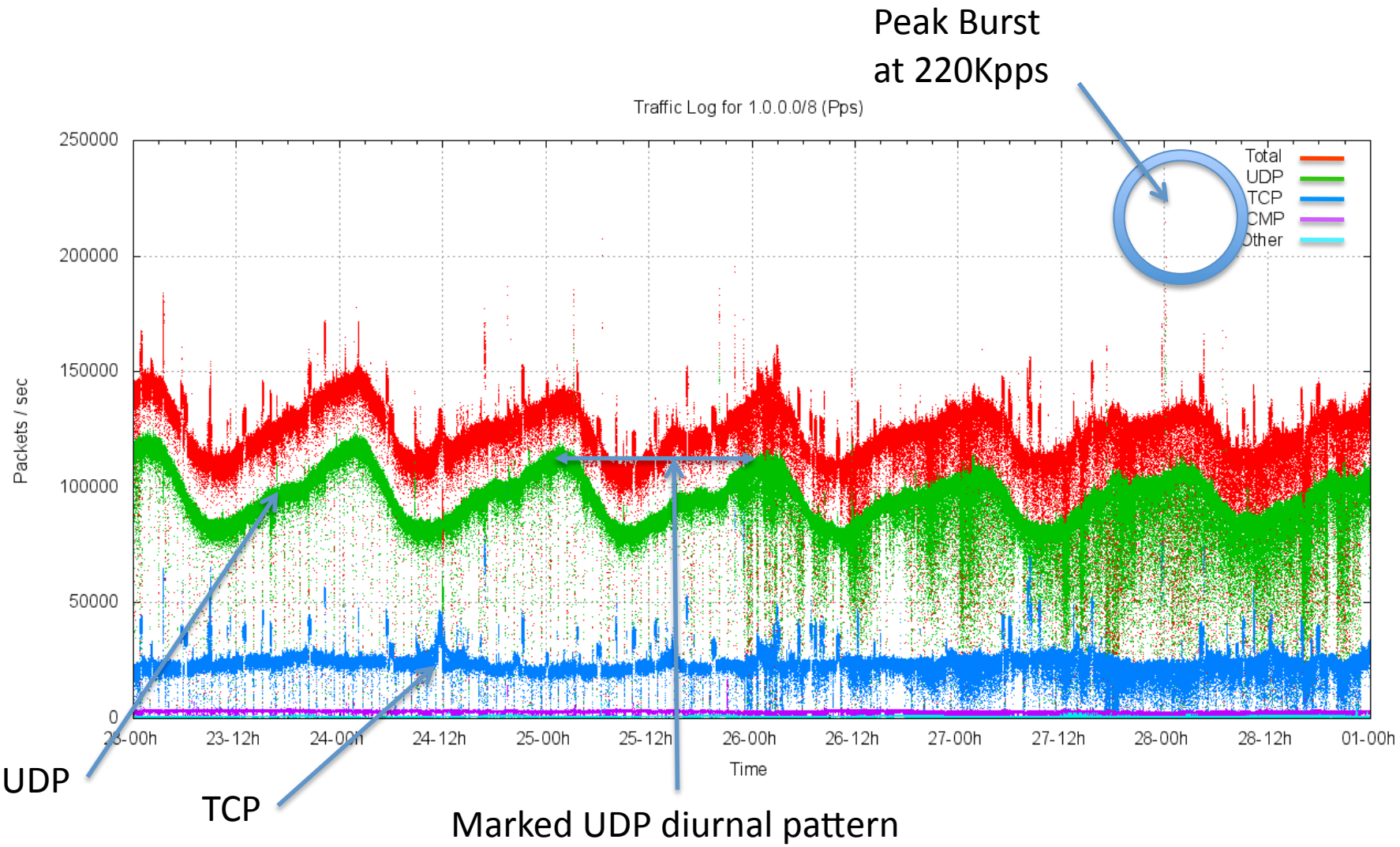
# Testing 1/8

- Merit (AS237) announced 1.0.0.0/8 from 23 Feb until 1 March 2010
  - Collected 7.9Tb of packet capture data

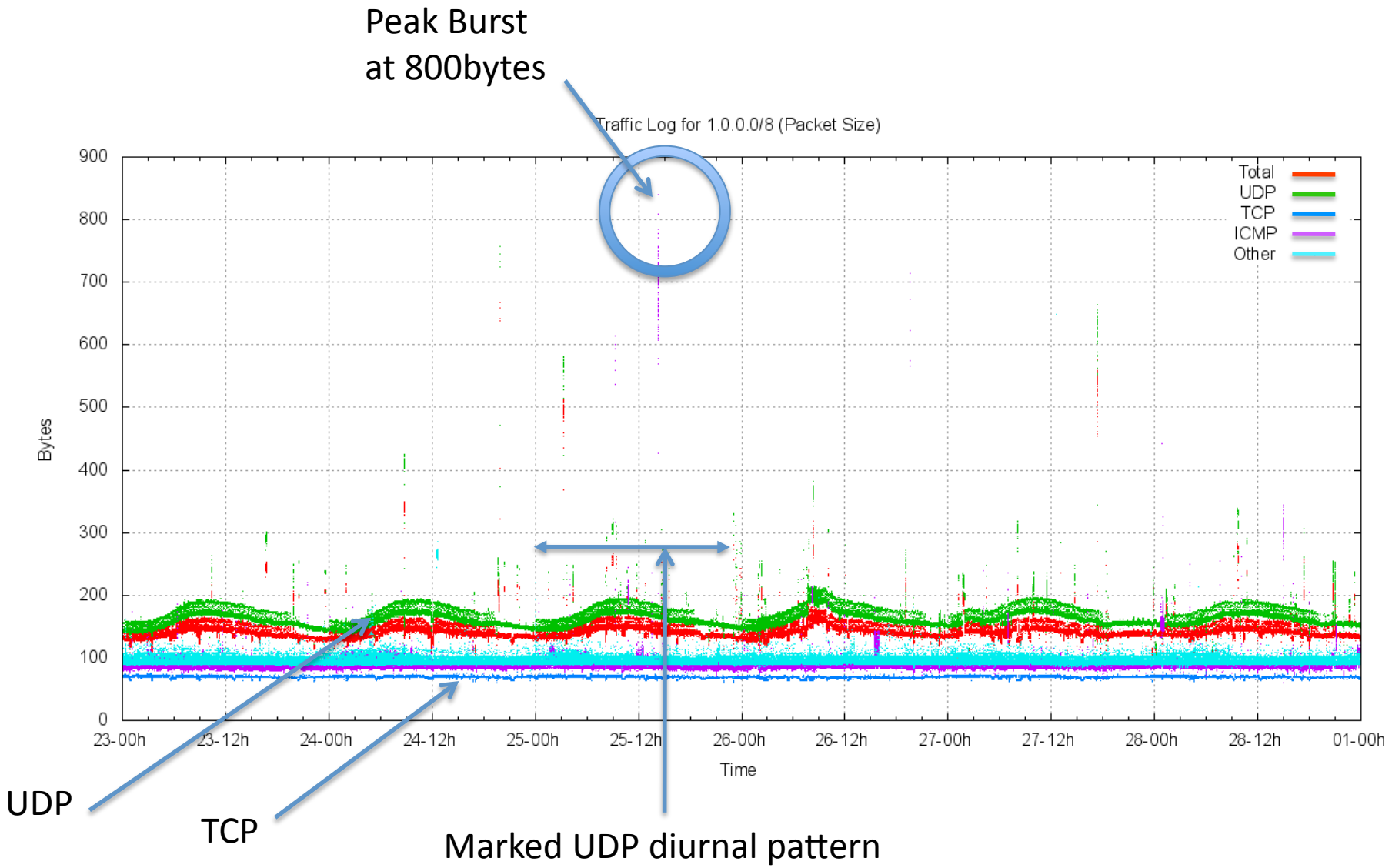
# Traffic to 1.0.0.0/8



# Packet Rate to 1.0.0.0/8



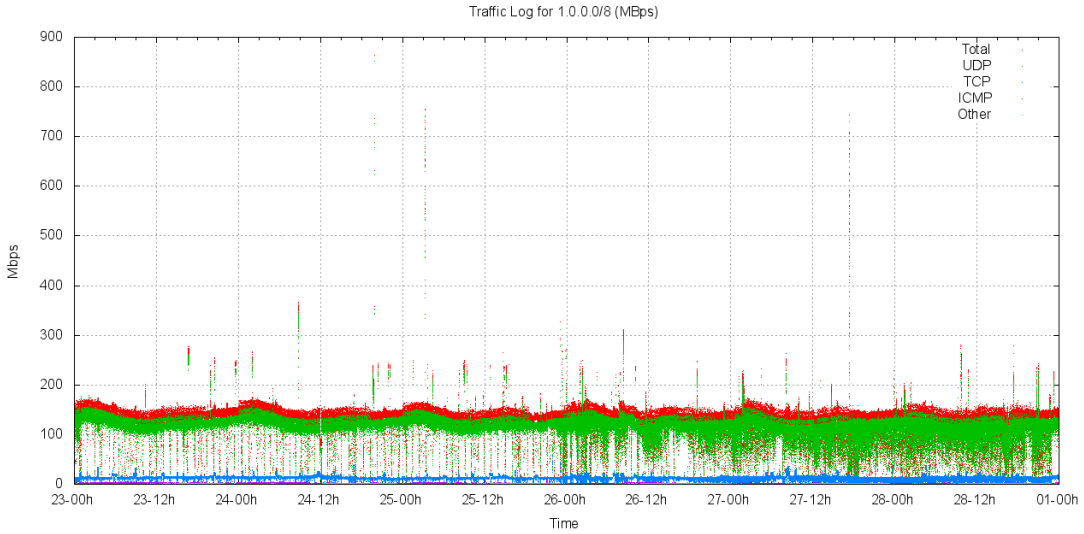
# Packet Size to 1.0.0/8

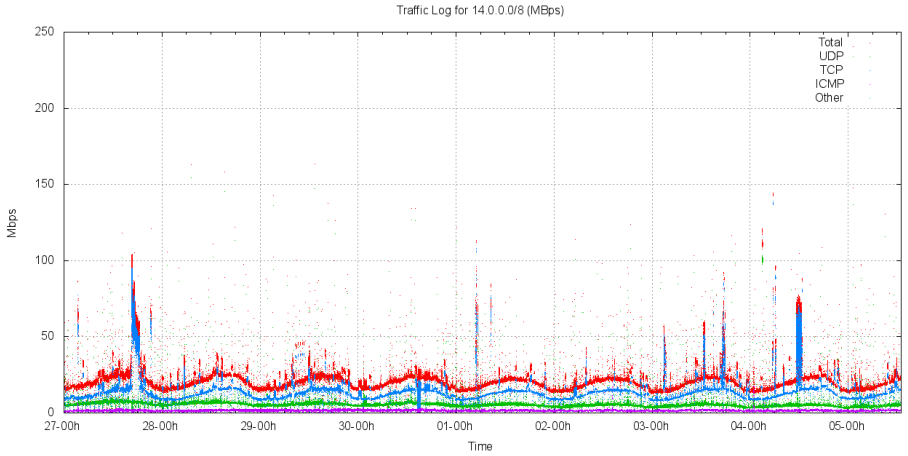


# Is this traffic “normal”?

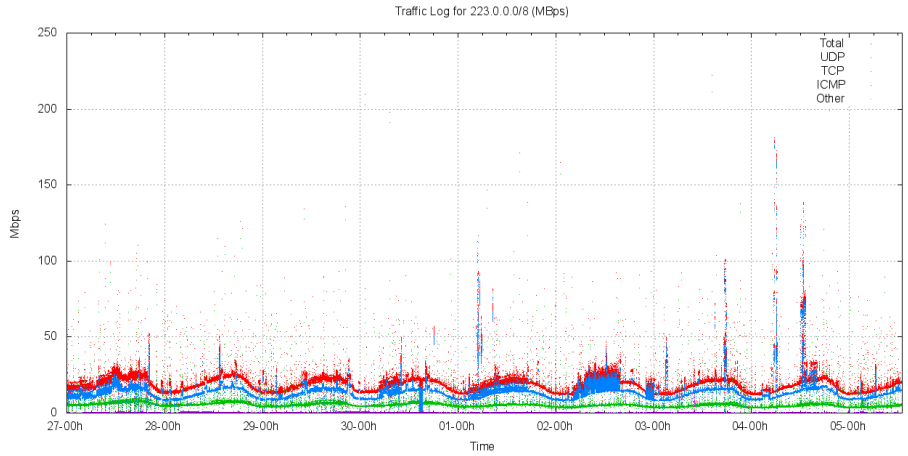
- We have also examined the traffic profile of two more address blocks: 14.0.0.0/8 and 223.0.0.0/8
  - similar experimental setup of a 7 day advertisement of the /8 address block using a passive collector

Traffic profile of 1/8




Traffic profile of 14/8

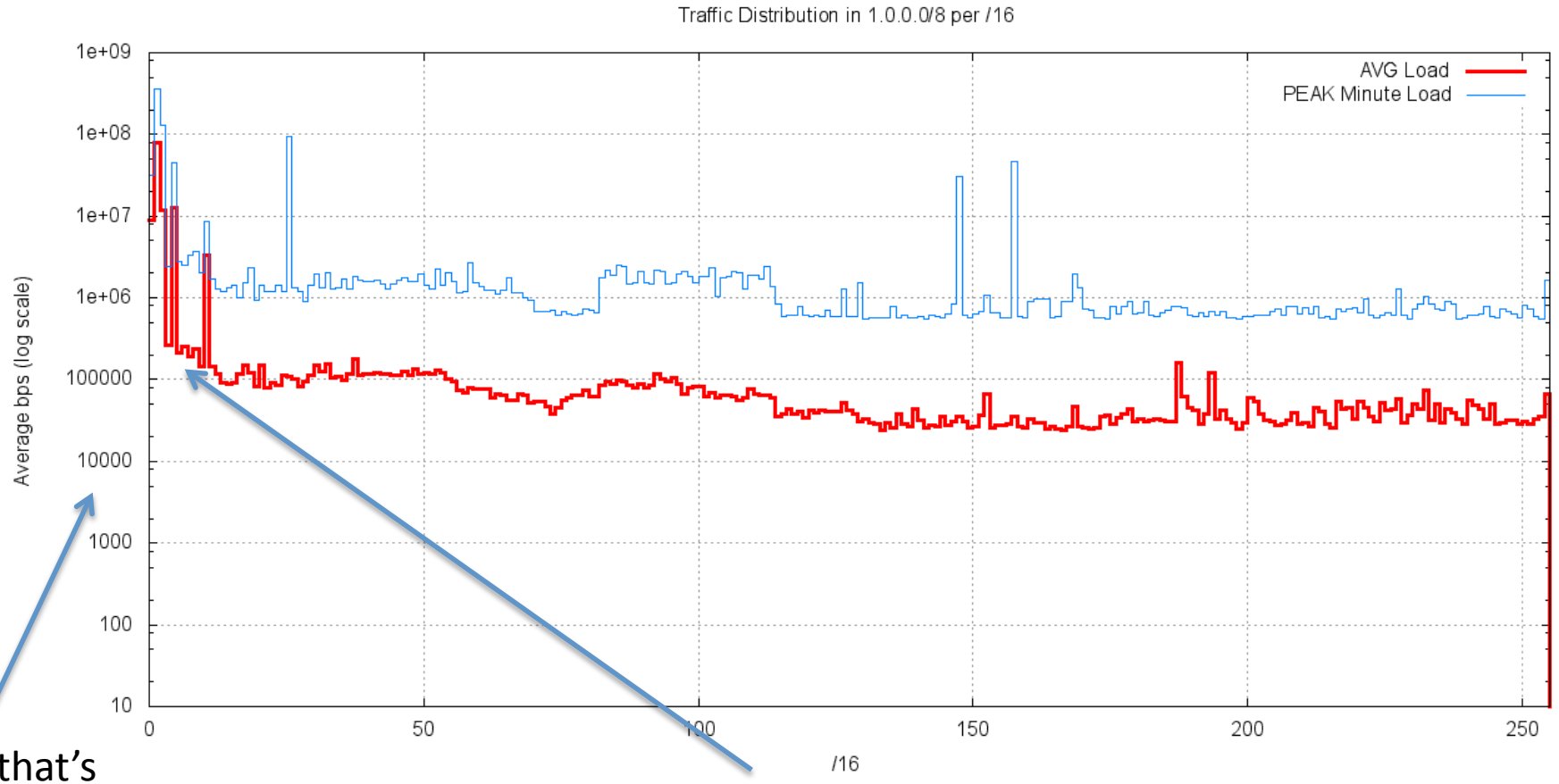



Traffic profile of 223/8

# 1.0.0.0/8 is *very* different

| | 1.0.0.0/8 | 14.0.0.0/8 & 223.0.0.0/8 |
|---|---|---|
| Average Traffic | 150Mbps | 25Mbps |
| UDP | 88% | 30% |
| TCP | 10% | 70% |
| Diurnal Variation | 4% | 45% |

# What's going on in 1/8?




Yes, that's a Log Scale!

The "hot spots" appear to lie in the low /16s

# 10 /24's receive 75% of packets

| Subnet /24 | Packets | % |
|---|---|---|
| 1.1.1.0 | 4797420185 | 44.5 |
| 1.4.0.0 | 1884458639 | 17.5 |
| 1.0.0.0 | 1069156477 | 9.9 |
| 1.2.3.0 | 199452209 | 1.8 |
| 1.1.168.0 | 62347104 | 0.5 |
| 1.10.10.0 | 26362000 | 0.2 |
| 1.0.168.0 | 18988771 | 0.1 |
| 1.1.0.0 | 18822018 | 0.1 |
| 1.0.1.0 | 14818941 | 0.1 |
| 1.2.168.0 | 12484394 | 0.1 |

# 1.1.1.1 – UDP port 15206

34.5% of all packets (and 50.1% of all bytes) received are UDP packets to 1.1.1.1, destination port 15206.

# UDP Port 15206?

- Most of the payloads looks like version 2 RTP packets
  - 75% of all bytes to this port have 0x8000 first 16 bits (first two bits is the version number and the next 14 all 0)
  - the majority of packets are 214 bytes in size (89.4%)
- Is this a small set of leaking devices?
  - All this coming from only 1036 /24s
  - And from only 1601 source ports seemingly unrelated to the ephemeral port ranges
  - Payload is PCMU – a compressed audio format
  - Is this a VOIP device with a configured default VOIP server setting of 1.1.1.1?

# An 860Mbps Peak…

Is 6 seconds of  UDP directed at 1.1.1.1

# That 6 second traffic burst …

- All these UDP packets are:
  - sourced from 206.225.8.22
  - sent to 1.1.1.1
  - total of 8192 bytes in length (pre fragmentation)
  - agile in source and destination ports
  - no “obvious” content in payload
- Some form of transient “leak” from inside a data centre?
- Or…

```
05:55:14.606498 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606568 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606642 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606856 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607031 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607268 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607500 IP 206.225.8.22.54295 > 1.1.1.1.767: UDP, length 8192
05:55:14.607905 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608174 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608466 IP 206.225.8.22.33462 > 1.1.1.1.5125: UDP, length 8192
05:55:14.608853 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.608926 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.609208 IP 206.225.8.22.53075 > 1.1.1.1.5175: UDP, length 8192
05:55:14.606498 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606568 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606642 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606856 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607031 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607268 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607500 IP 206.225.8.22.54295 > 1.1.1.1.767: UDP, length 8192
05:55:14.607905 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608174 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608466 IP 206.225.8.22.33462 > 1.1.1.1.5125: UDP, length 8192
05:55:14.608853 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.608926 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.609208 IP 206.225.8.22.53075 > 1.1.1.1.5175: UDP, length 8192
…
```

# Endian Confusion

- What is it with 1.1.168.0, 1.0.168.0, 1.2.168.0?
  - Most of the packets are going to: 1.1.168.192, 1.0.168.192, 1.2.168.192.

    Does anyone see anything familiar here?
- These IPs are really just 192.168.x.1, in host-byte order (little-endian)
  - someone is running some private network code and not doing a call to `htonl(ip_addr)`, and we are catching the data in network 1
  - Do other /8s see a similar leak? yes!

# 1.4.0.0

- For 1/8, 17.5% of all packets (and 10% of all bytes) received are UDP packets to 1.4.0.0, destination ports 33368, 514, 33527, 3072, 33493
  - Surprisingly most of these could be interpreted as DNS traffic
  - Most appear to be valid queries
  - leakage from a “private” DNS resolver configured on 1.4.0.0?

# What can we do about it?

- The following /24s are being withheld from general allocation by APNIC:
  - 1.0.0.0/24
  - 1.1.1.0/24
  - 1.2.3.0/24
  - 1.4.0.0/24
  - 1.10.10.0/24
- If further investigation reveals that the traffic to any of these /24s abates to a normal background level in the future, then these addresses would be returned to the APNIC unallocated address pool at that time.

# What can we do about it (cont)?

- The following /16s are temporarily marked as reserved and withheld from general allocation by APNIC:

| | | |
|---|---|---|
| 1.0.0.0/16 | 1.5.0.0/16 | 1.20.0.0/16 |
| 1.1.0.0/16 | 1.6.0.0/16 | 1.32.0.0/16 |
| 1.2.0.0/16 | 1.7.0.0/16 | 1.37.0.0/16 |
| 1.3.0.0/16 | 1.8.0.0/16 | 1.187.0.0/16 |
| 1.4.0.0/16 | 1.10.0.0/16 | |

# What about the other /8s?

- APNIC has also tested 14/8 and 223/8 prior to commencing allocation

Extract from Tomoya Yoshida's JANOG Report

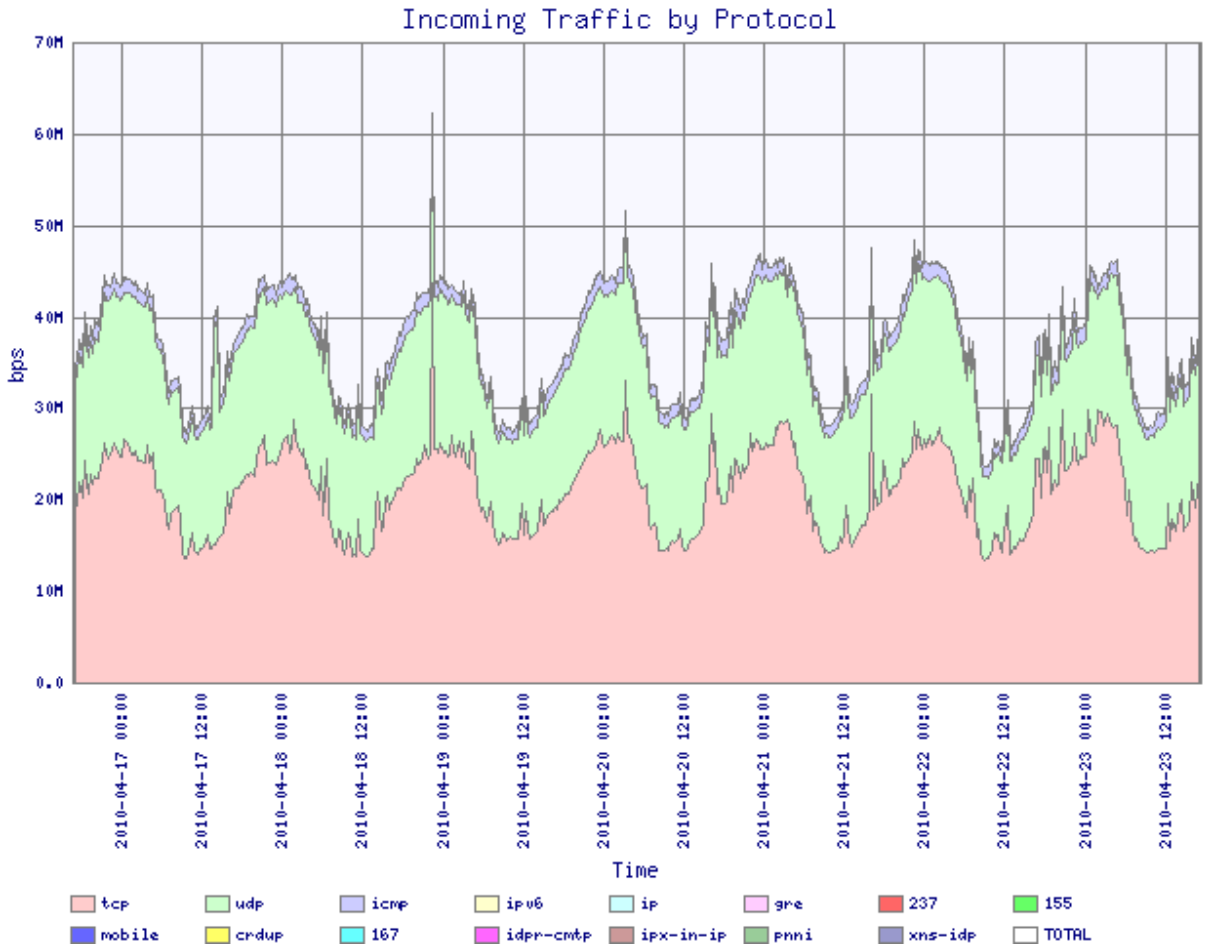
# One week advertisement of 14/8, 223/8

- Recently whole x/8 advertisement is observed more often just after the IANA allocated to the RIRs those blocks
  - Investigation 1/8 pollution at first
  - Other x/8s are also investigated for the situations and checking the trend
- Overview of Investigation
  - Period : 19th Apr 2010 ~ 26th (1 week)
    - Allocation from IANA to APNIC : 10th Apr 2010
  - Prefixes : 14/8, 223/8 from AS38639(NTTCom)
  - Packet collecting way : tcpdump + netFlow sampling (Samurai)
  - Reachability check for those two blocks using routeview (router server)

Extract from Tomoya Yoshida's JANOG Report

# Per Protocol

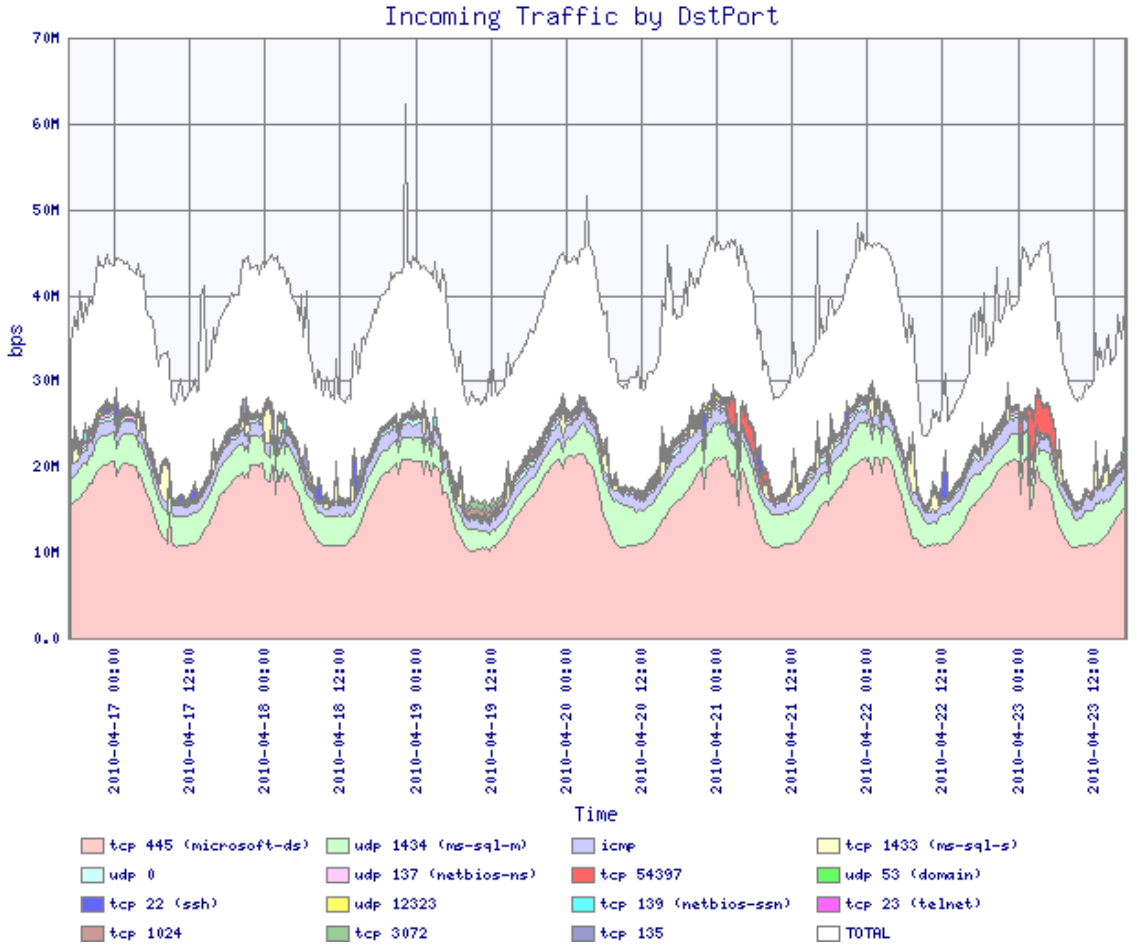
Normally 30Mbps ~ 50Mbps, it is like a normal traffic curve



Extract from Tomoya Yoshida's JANOG Report

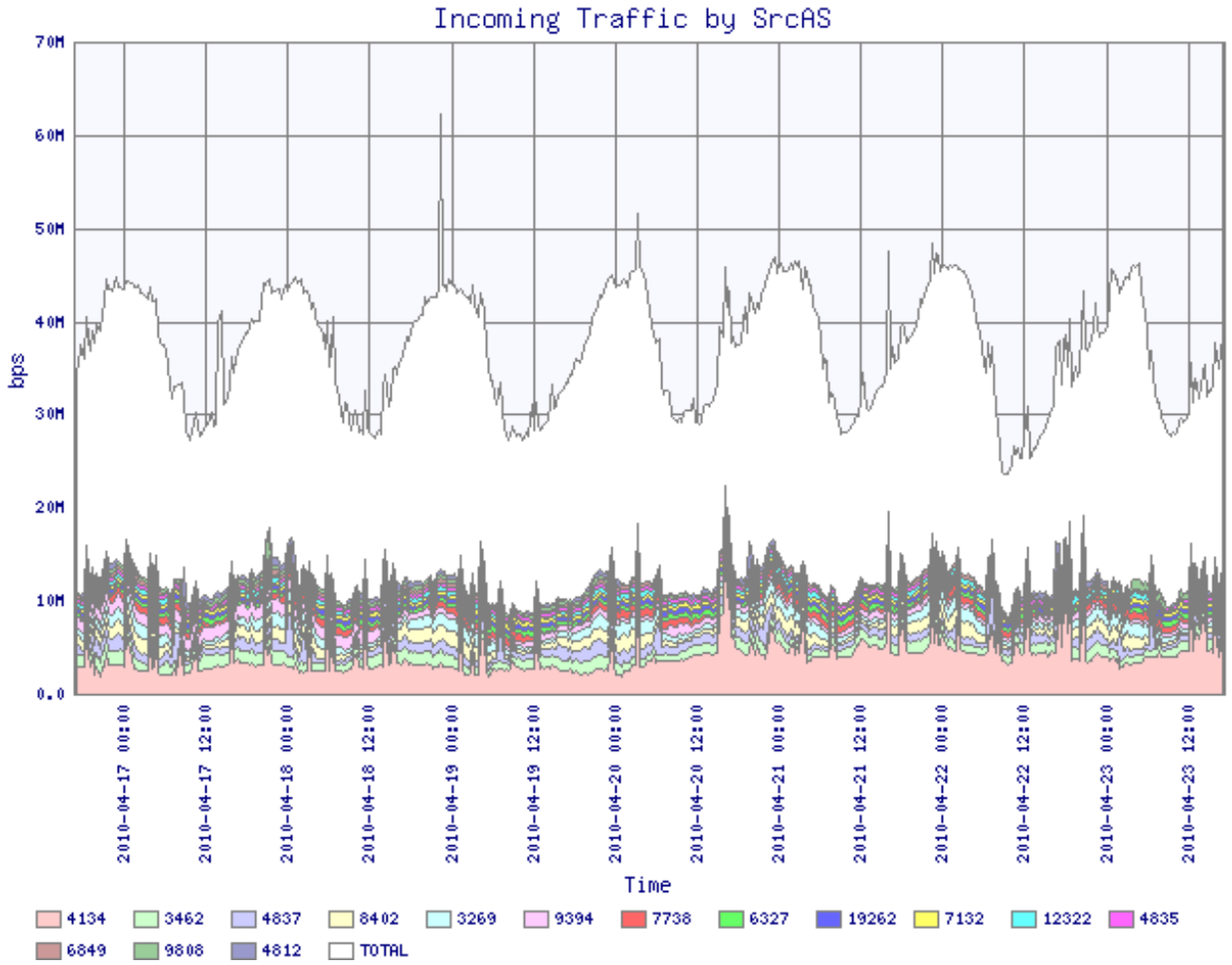
# Per Protocol and Port

A half is tcp/445(Conficker , Downadup), second udp/1434(sql-slammer)



Extract from Tomoya Yoshida's JANOG Report

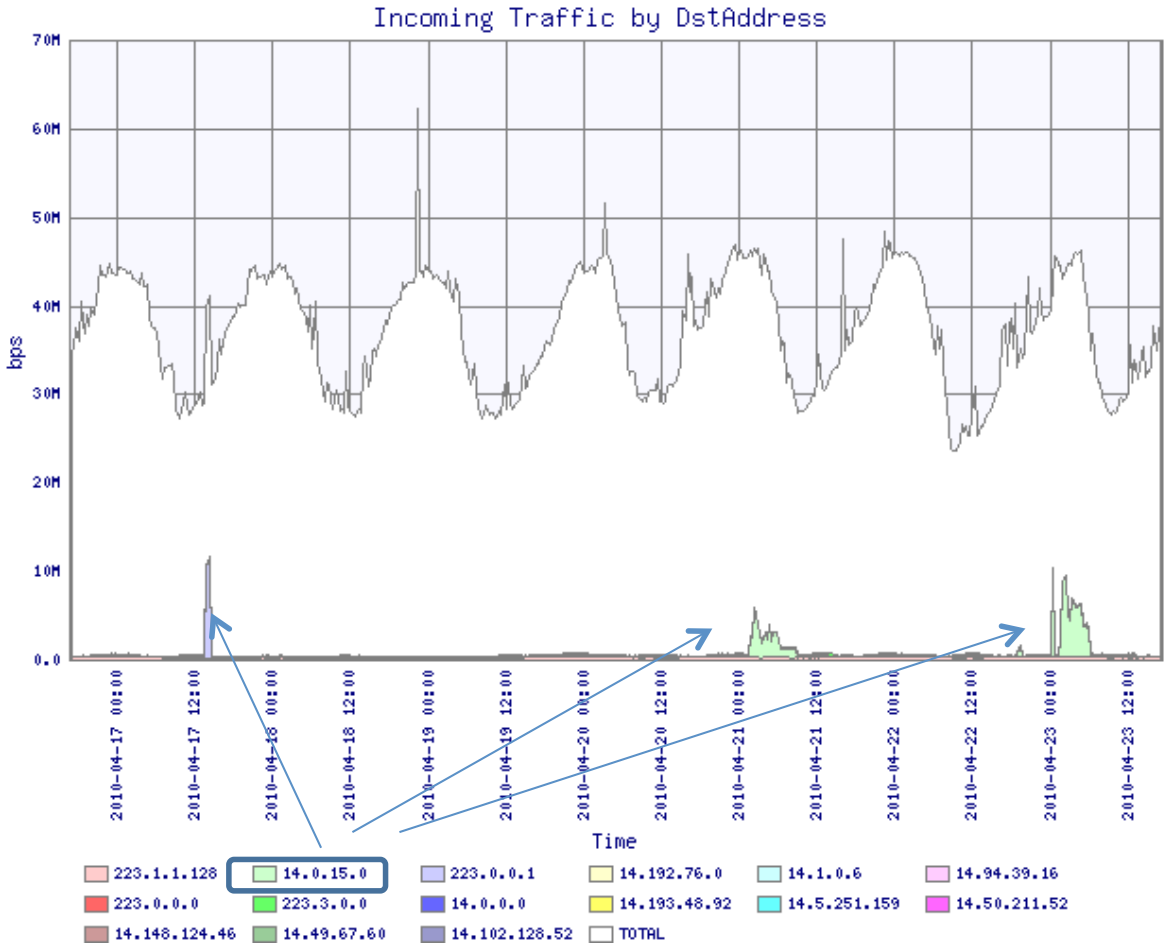
# Per Origin_AS




AS4134:ChinaNet
AS3462:Hinet
AS4837:CNCG
AS8402:Corbina Tel
AS3269:Telecom Italy

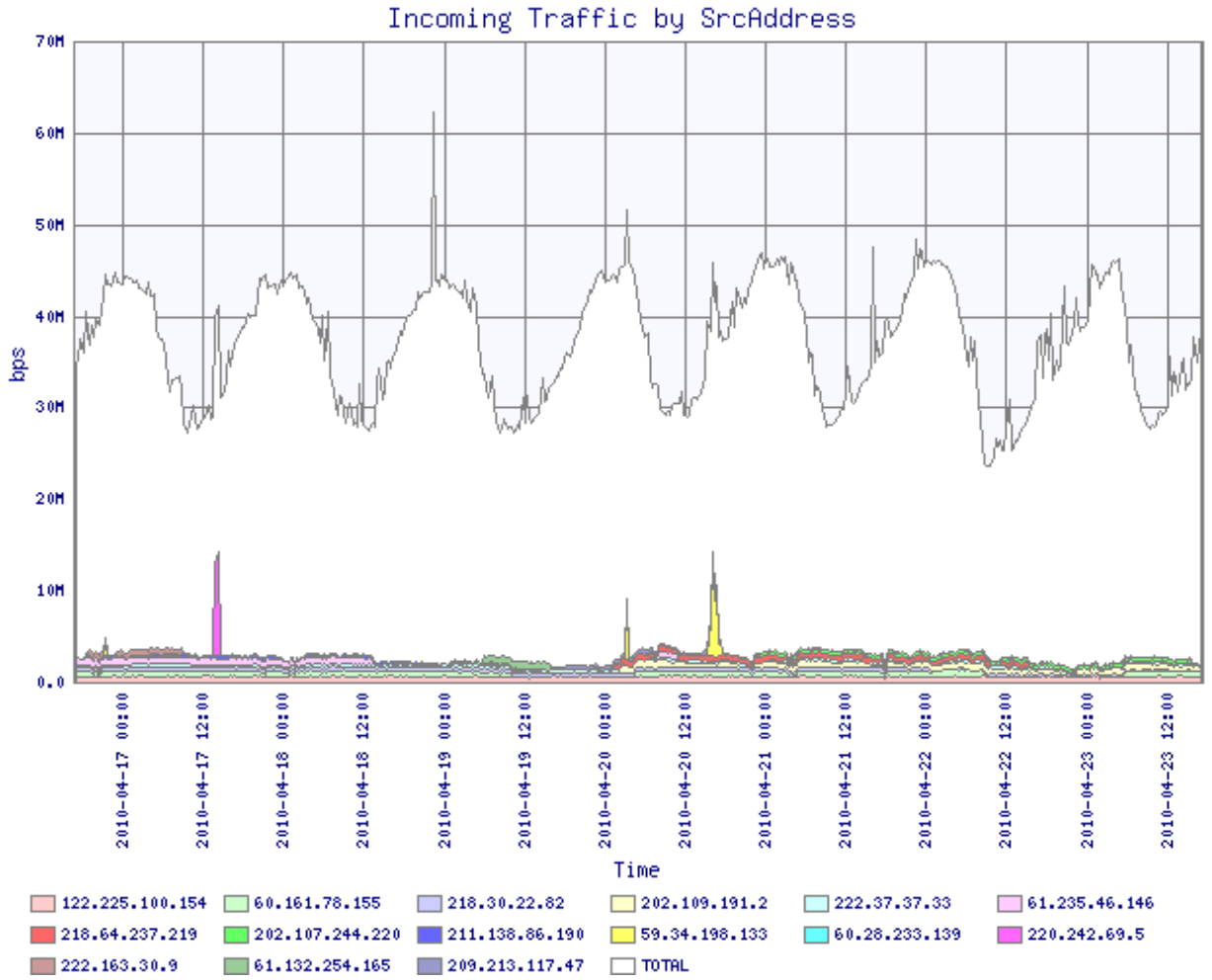
Extract from Tomoya Yoshida's JANOG Report

# Per Destination IP

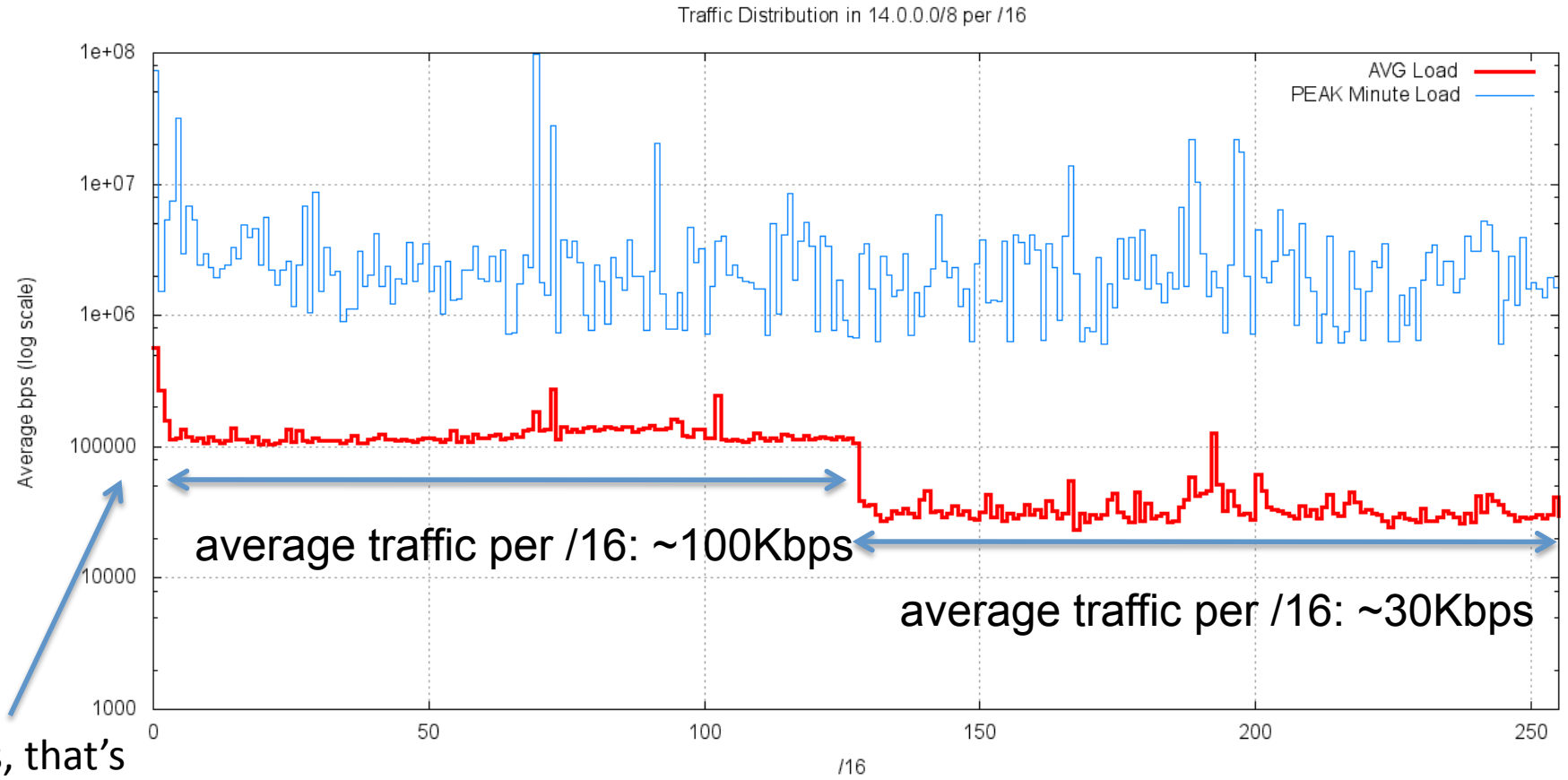


Extract from Tomoya Yoshida's JANOG Report

# Per Source IP

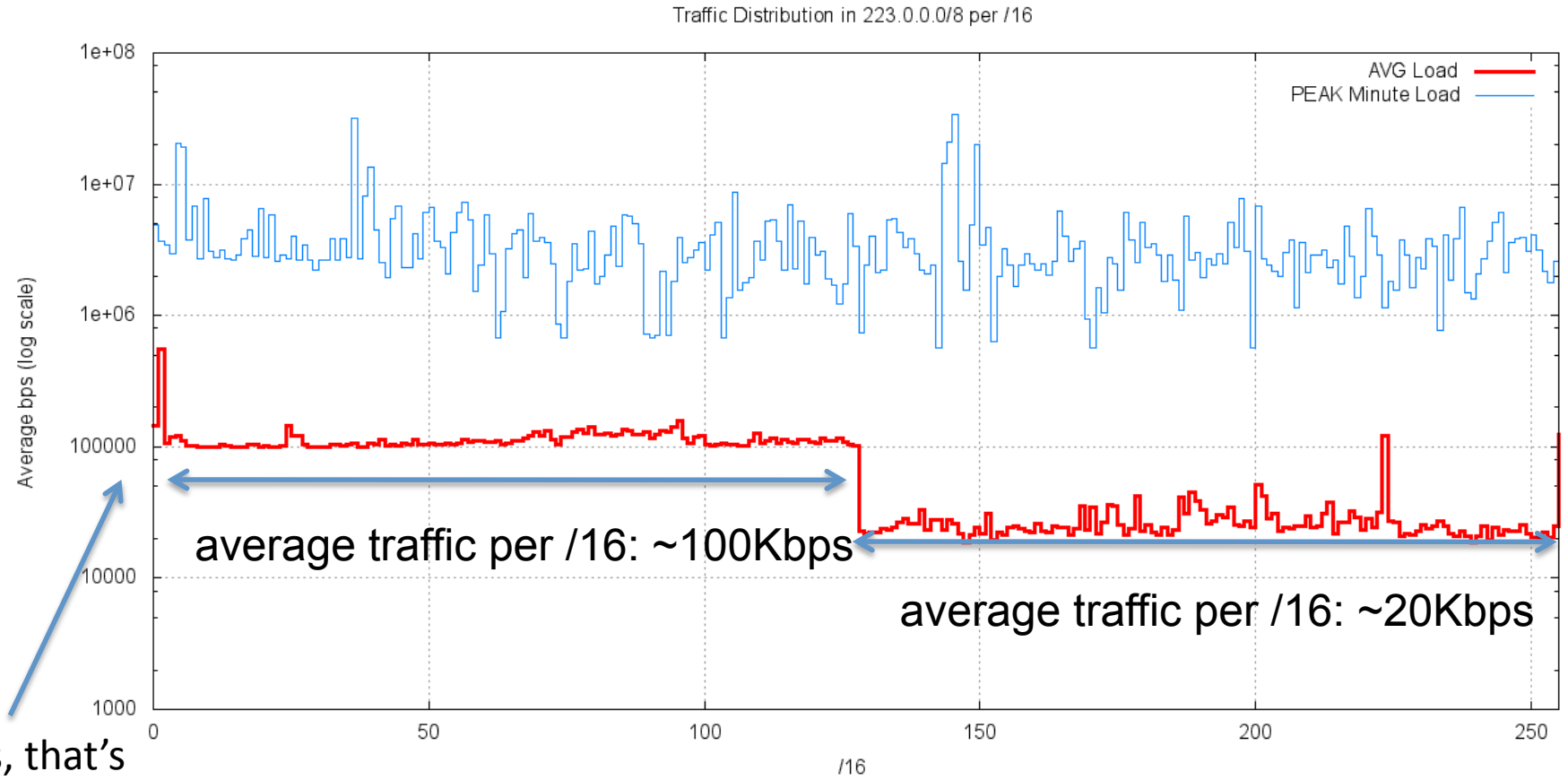


# 14.0.0.0/8 Profile




Yes, that's a Log Scale!

# 223.0.0.0/8 Profile




Yes, that's a Log Scale!

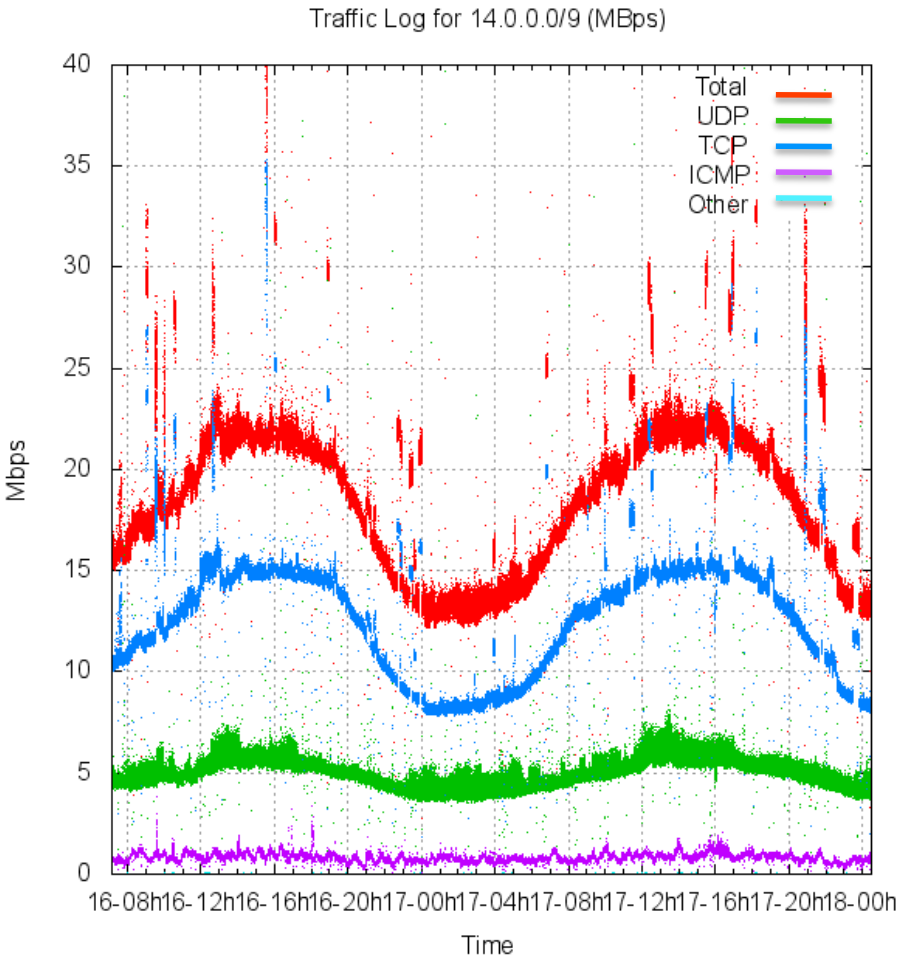
# What's in the low half?

Conficker!

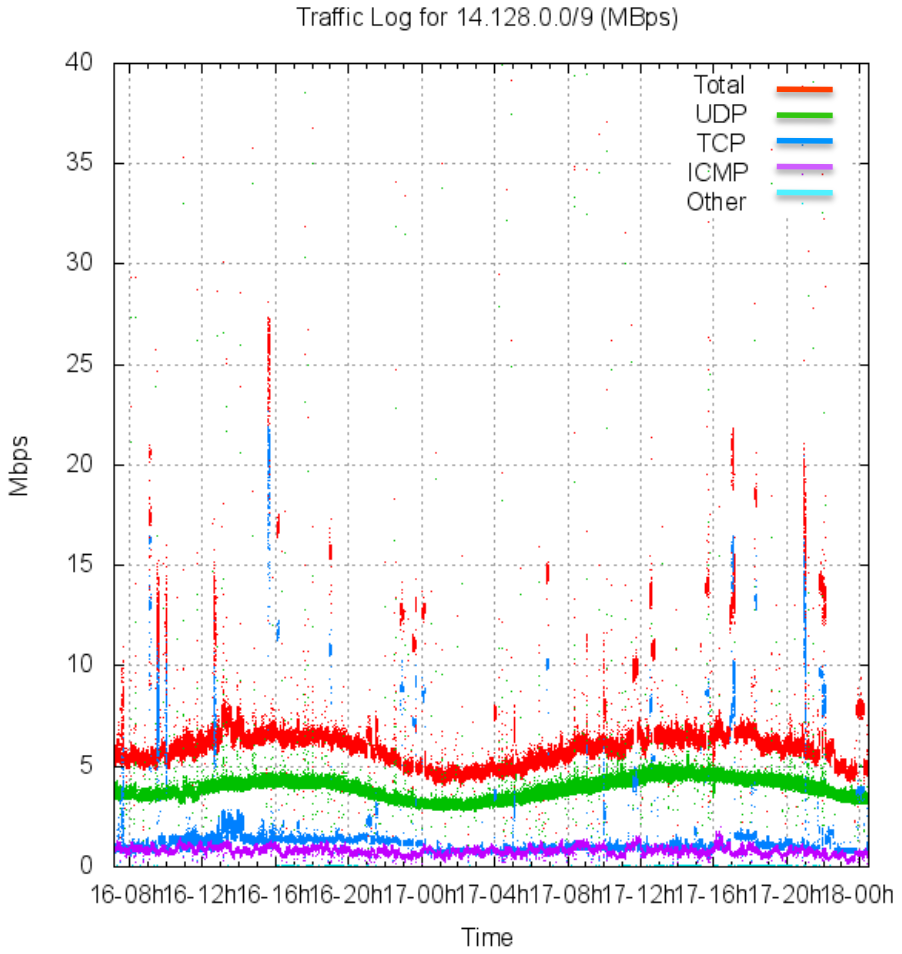
- conficker will not scan addresses with bit 9 set
- the "low" half of the /8 is scanned by conficker at a rate of ~24,000 packets per second

# comparing /9s in 14/8

Low Half




High Half



# TCP destination ports in 14/8

Low Half

| TCP Port | % | Packet Count |
|---|---|---|
| 445 | 82.9% | 3132836308 |
| 1433 | 1.7% | 63876218 |
| 22 | 0.6% | 22555596 |
| 139 | 0.5% | 19185536 |
| 23 | 0.4% | 15325619 |
| 135 | 0.4% | 14307267 |
| 25 | 0.3% | 9723041 |
| 9415 | 0.2% | 8536035 |
| 1755 | 0.2% | 8416185 |
| 4899 | 0.2% | 8392818 |

High Half

| TCP Port | % | Packet Count |
|---|---|---|
| 1433 | 13.0% | 61352758 |
| 22 | 4.0% | 18769025 |
| 445 | 3.9% | 18341810 |
| 135 | 3.8% | 18092100 |
| 23 | 3.2% | 15304995 |
| 139 | 2.8% | 13192532 |
| 25 | 2.0% | 9619182 |
| 4899 | 1.8% | 8500798 |
| 9415 | 1.8% | 8408492 |
| 1755 | 1.8% | 8408303 |

# Toxic Radiation in 14.0.0.0/8

| TCP Port | % | Port / Attack |
|---|---|---|
| 445 | 73.65% | MS Server / conficker |
| 1433 | 1.5% | SQL Server / various |
| 22 | 0.5% | ssh / probes |
| 139 | 0.5% | netbios / various |
| 23 | 0.4% | telnet / probes |
| 135 | 0.4% | MS RPC / Blaster |
| 25 | 0.3% | SMTP |
| 9415 | 0.2% | koobface proxies |
| 1755 | 0.2% | MS media streaming |
| 4899 | 0.2% | radmin |

Conficker appears to be the most virulent current Internet virus by far, with a total traffic profile of 12Mbps per /8, or 2.5 Gbps in total across the entire IPv4 address space.

# What can we do about it?

- Temporary reservations of the “hot spots” in 14.0.0.0/8 and 223.0.0.0/8

| Prefix |
|---|
| 14.0.0.0/24 |
| 14.0.15.0/24 |
| 14.1.0.0/24 |
| 14.192.72.0/24 |
| 14.102.128.0/24 |
| 14.102.129.0/24 |

| Prefix |
|---|
| 223.0.0.0/24 |
| 223.1.0/24 |
| 223.223.223.0/24 |
| 223.255.255.0/24 |

# IPv4 Background Radiation

- We understand that the IPv4 address space is now heavily polluted with background traffic
  - Background levels of traffic associated with scanning, backscatter, mis-configuration and leakage from private use contexts contributing to the traffic volume
  - Average background traffic level in IPv4 is around 300 – 600 bps per /24
  - There is a “heavy tail” to this distribution, with some /24s attracting well in excess of 1Mbps of continuous traffic
  - The “hottest” point in the “dark” IPv4 network appears to be 1.1.1.0/24. This prefix attracts some 100Mbps as a constant incoming traffic load

# IPv4 Background Radiation

- Most of this traffic is port scanning for well known vulnerabilities:
  - predominately scanning for and by Windows systems
  - exploiting vulnerabilities where patches already exist
  - where the scanning sources are well distributed – these are bot-scanners
  - TCP Port 445 / Conficker is the most virulent scanner in today's IPv4 Internet

# IPv4 Background Radiation

- Total background traffic level across the entire IPv4 address range is some 5.35Gbps
- On average, every IPv4 address will receive one packet every 69 seconds
  - addresses in the “high” /9 of each /8 will receive a packet every 120 seconds
  - address in the “low” /9 will receive a packet every 20 seconds

# Thank You

Questions?