RQA – Testing Address Blocks for Dark Traffic

Geoff Huston, George Michaelson

APNIC 31

23 February 2011

Resource Quality Assurance

Are all addresses the same?

As we get to the last few IPv4 address blocks, its possible that the addresses may have echoes of earlier use

Some addresses have been used “informally” for various uses already, such as:

1.1.1.1 used as a rendezvous address in many wifi hotspot networks

Resource Quality Assurance

Such addresses become “hot spots” over time

They attract large volumes of unsolicited incoming traffic when they are advertised on the public network

They would become highly problematical if they were assigned to an end user behind a low speed DSL line!

Can we test address blocks to see if there are “hot spots” within the address range?

Resource Quality Assurance

APNIC has worked with a number of collaborators to test /8 address blocks before they are passed into the allocation system

The testing involves adverting the /8 on the public Internet for an extended period, and recording all incoming packets that are being sent to this address block

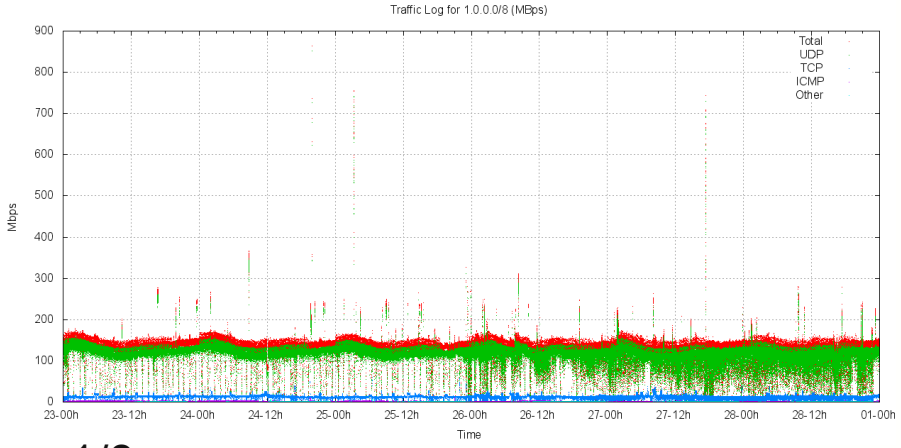
There are no packets sent in response – this is a “dark” network

We investigate the traffic profile and see if any prefixes are “unusual” in terms of incoming traffic levels

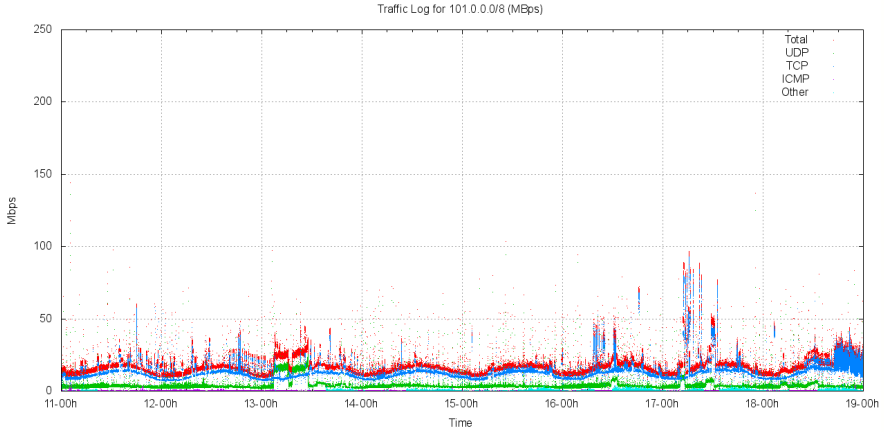
Testing Schedule

1.0.0.0/8	Feb 2010
14.0.0.0/8	May 2010
223.0.0.0/8	May 2010
49.0.0.0/8	Sep 2010
101.0.0.0/8	Sep 2010
42.0.0.0/8	Nov 2010
36.0.0.0/8	Nov 2010
39.0.0.0/8	Feb 2011
106.0.0.0/8	Feb 2011
ERX various	Feb 2011
103.0.0.0/8	Mar 2011

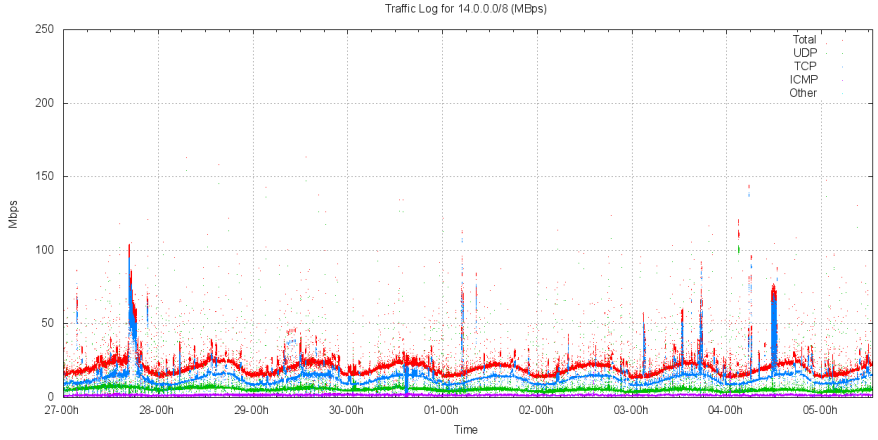
Some Traffic Profiles



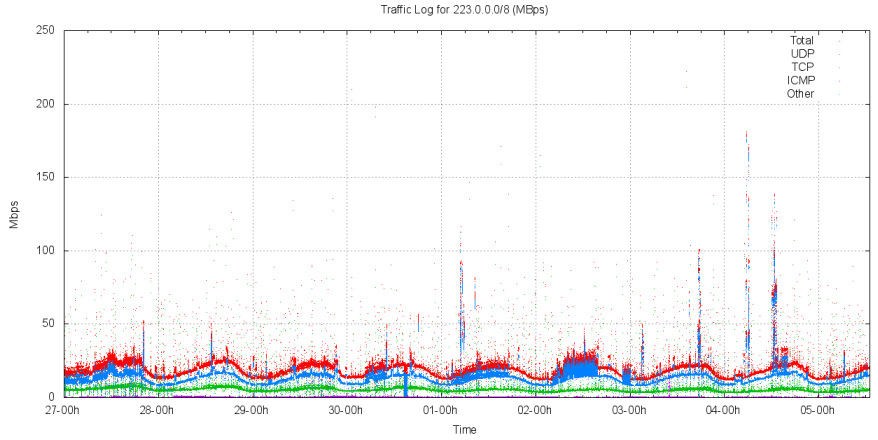
1/8



101/8

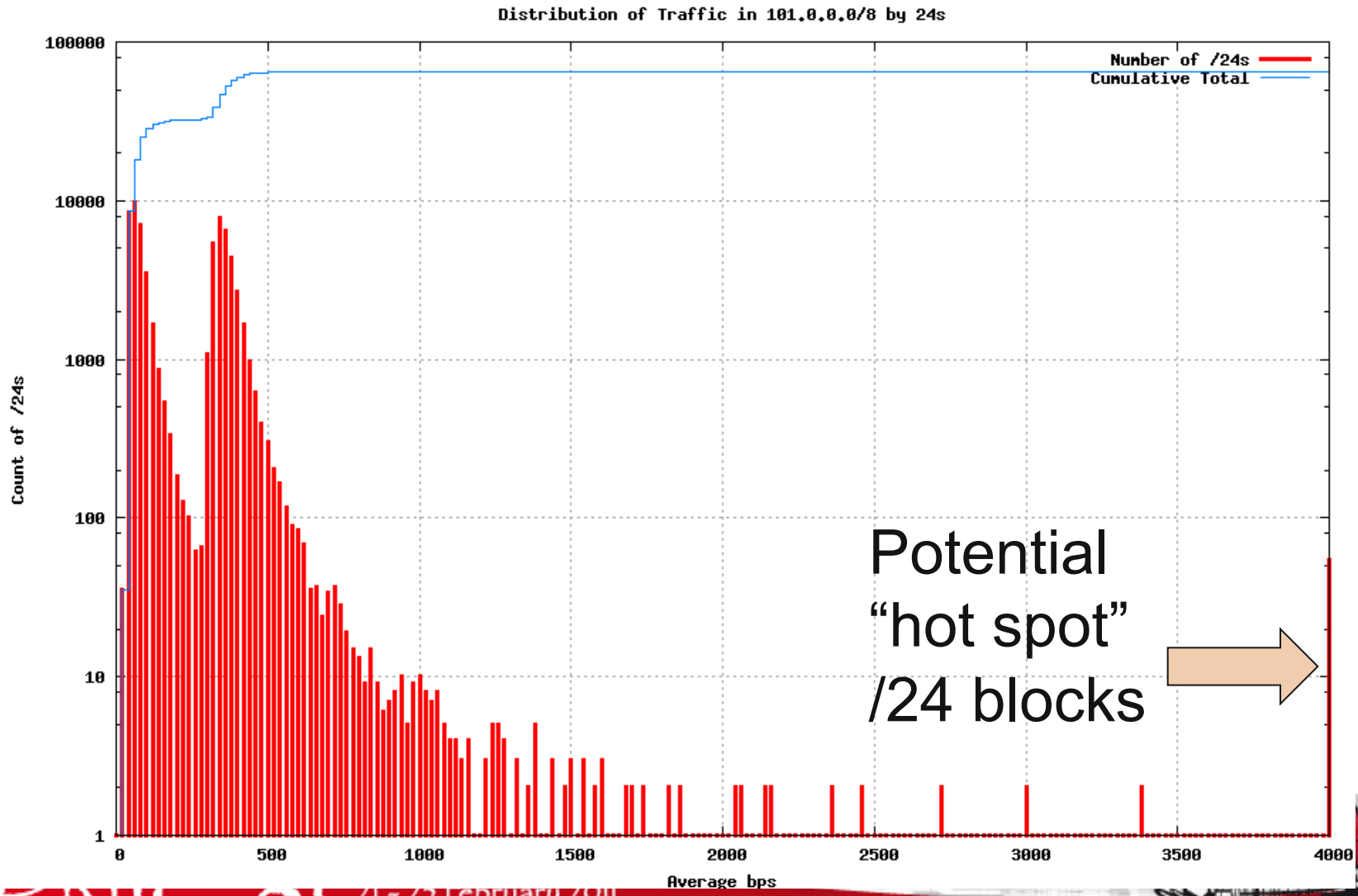


14/8



223/8

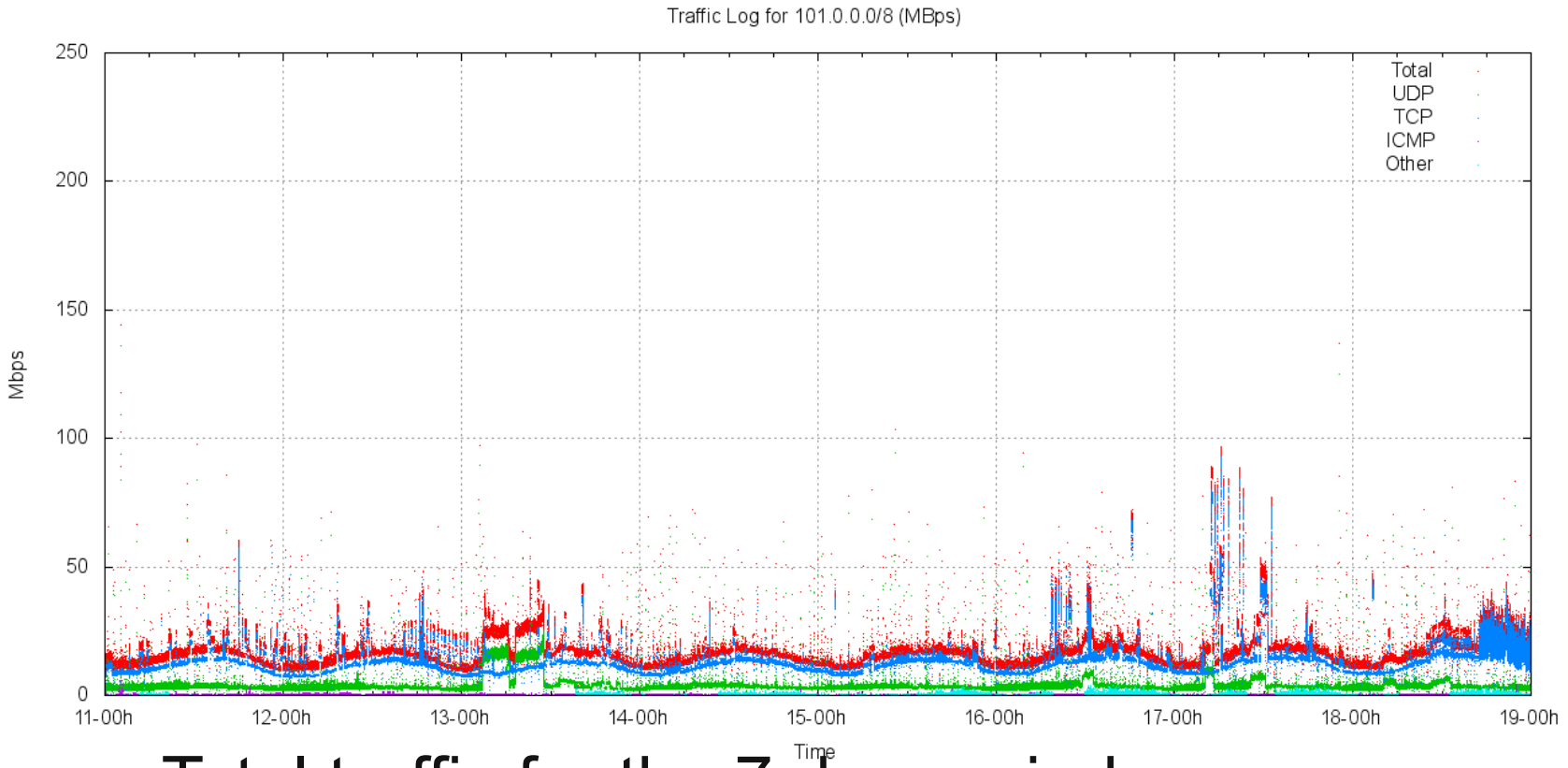
Looking for “Hot Spots”



Normal vs “Hot”

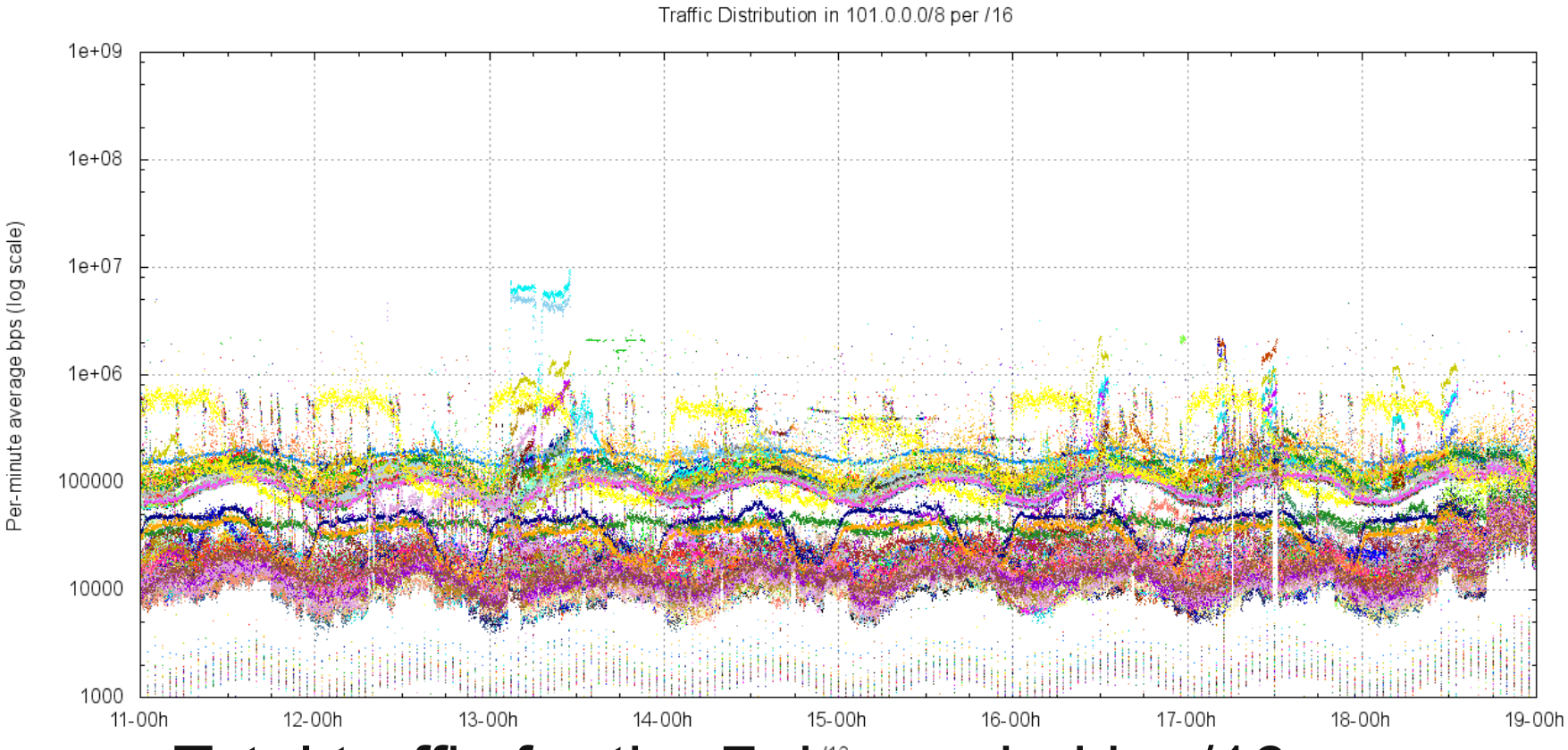
- Average incoming traffic per /24 is between 80 – 500 bps of incoming traffic
- Anomalous “hot” /24s attract more than 10kbps of incoming traffic

An example: 101/8



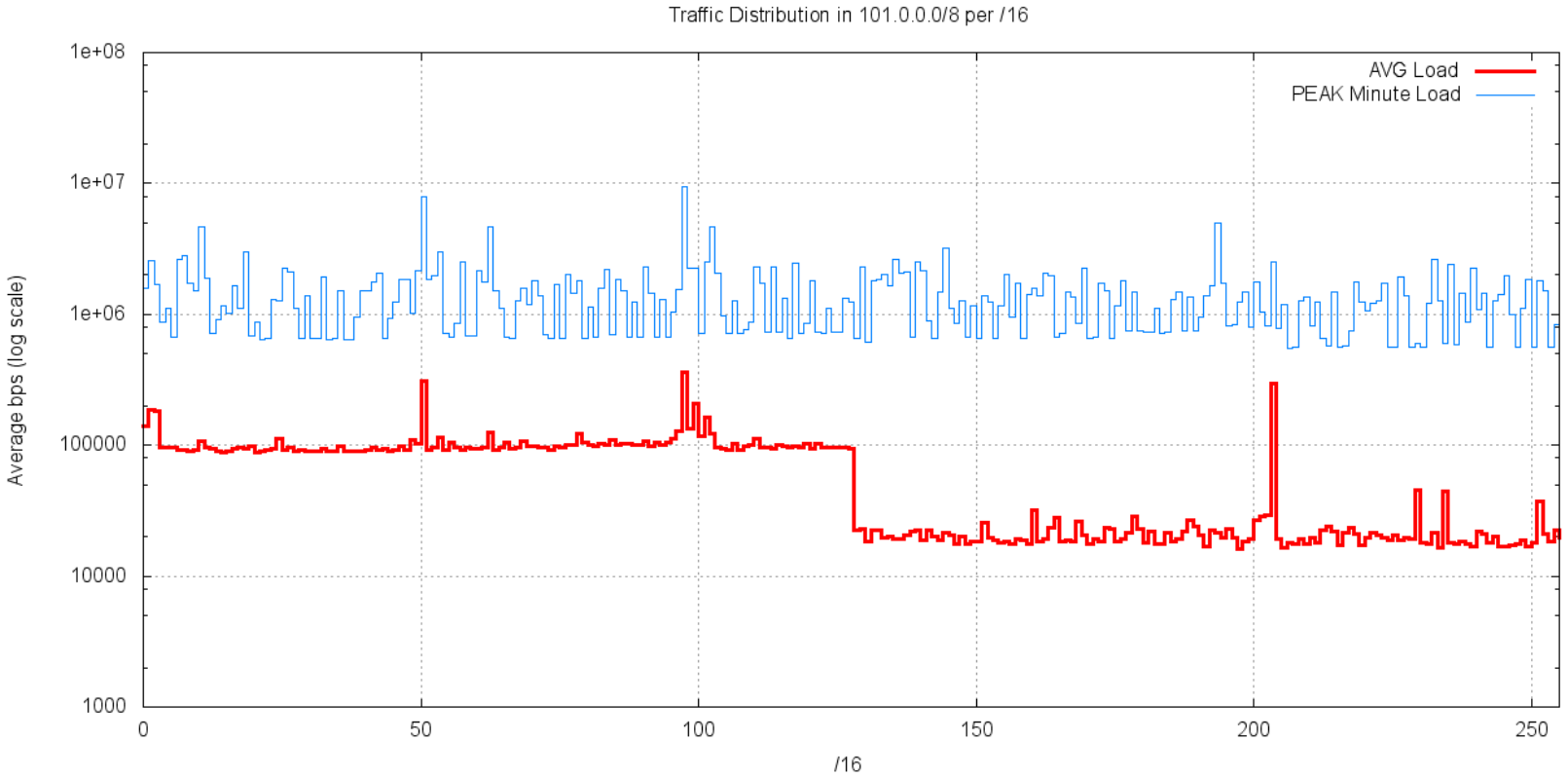
Total traffic for the 7 day period

Looking at /16s in 101/8

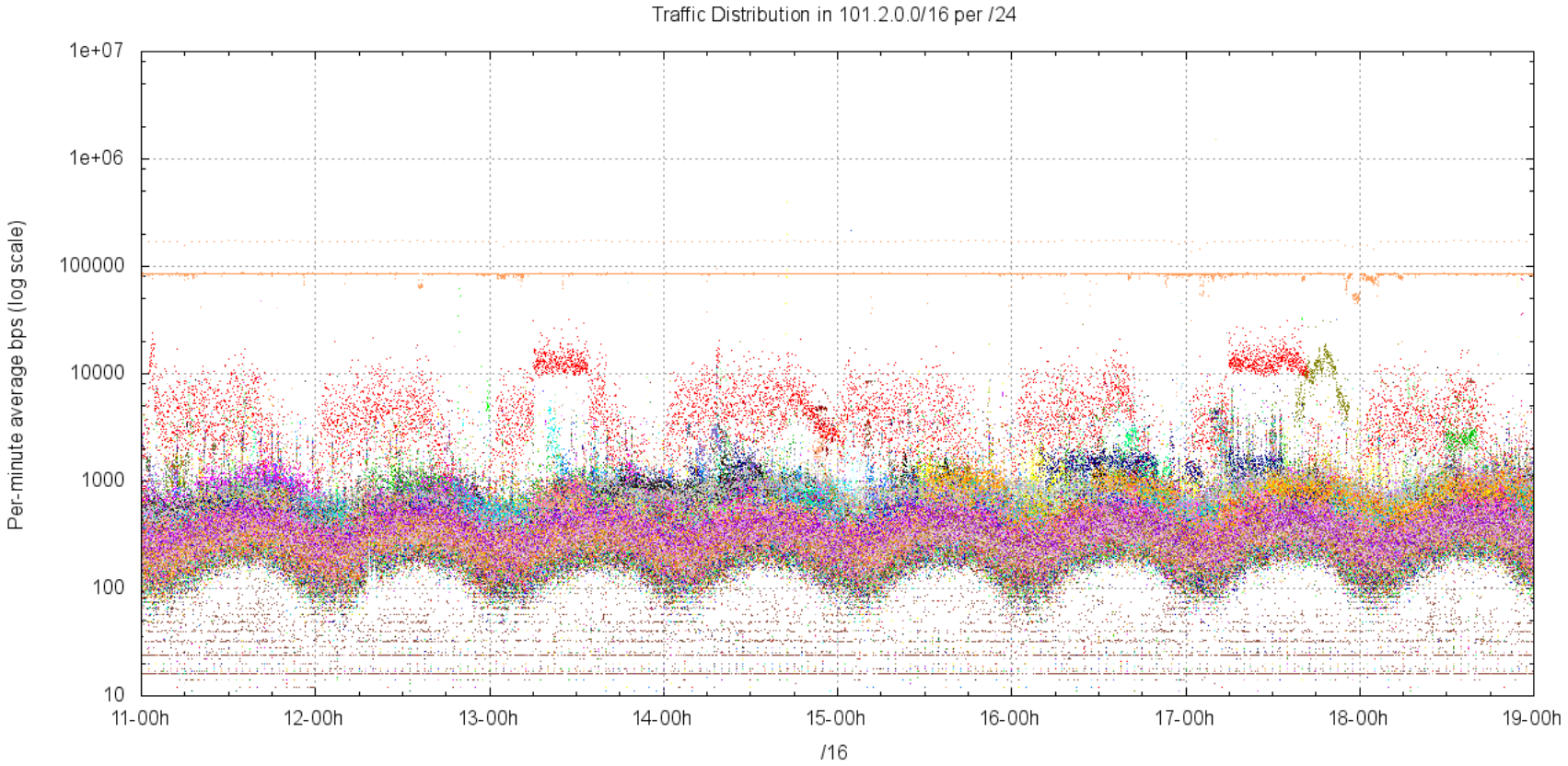


Total traffic for the 7 day period by /16

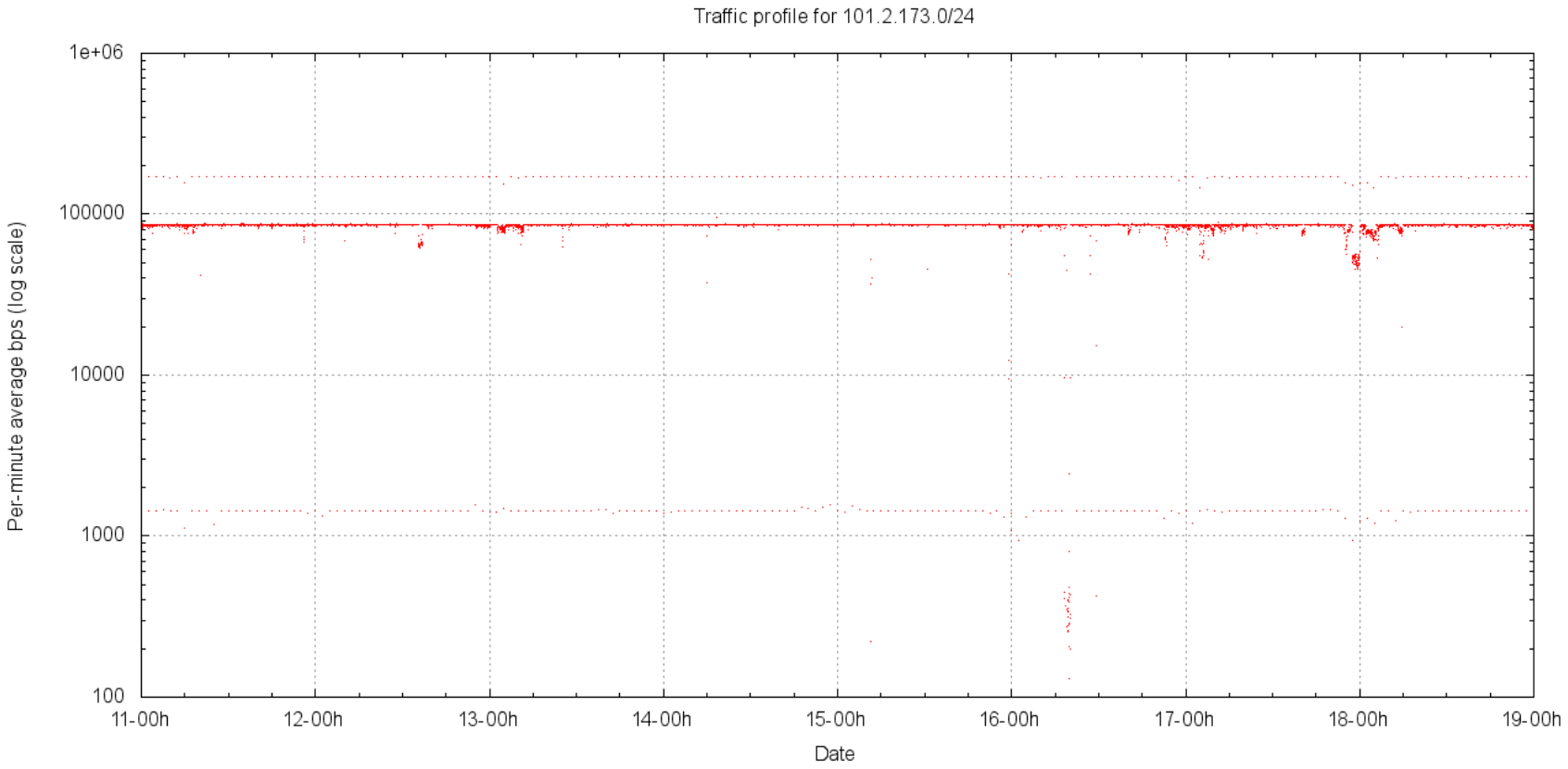
/16 Traffic Distribution in 101/8



/24 Traffic Distribution in 101.2/16



Hot Spot /24 – 101.2.173.0/24



Hot Spot Management

- Hold “hot spot” prefixes for quarantine
- Recheck regularly to see if the traffic profile has dissipated
- Next check scheduled for March 2011

Quarantine Pen Contents

Current list of quarantined hot spot prefixes:

1.0.0.0/13
1.8.0.0/16
1.10.0.0/16
1.20.0.0/16
1.32.0.0/16
1.37.0.0/16
1.187.0.0/16
14.0.0.0/24
14.0.15.0/24
14.1.0.0/24
14.192.76.0/24
14.102.128.0/24
14.102.129.0/24

36.0.0.0/24
36.37.38.0/24
42.240.51.0/24

42.0.0.0/24
42.0.25.0/24
42.1.56.0/24
42.1.57.0/24
42.62.181.0/24
42.83.80.0/24
42.96.111.0/24
42.99.114.0/24
42.123.39.0/24
42.156.39.0/24
42.187.123.0/24
42.194.10.0/24
42.201.36.0/24

101.0.0.0/24
101.1.1.0/24
101.2.173.0/24
101.50.56.0/24
101.53.100.0/24
101.55.225.0/24
101.78.2.0/24
101.96.8.0/24
101.97.51.0/24
101.99.97.0/24
101.99.100.0/24
101.101.101.0/24
101.102.103.0/24
101.110.116.0/24
101.203.172.0/24
101.234.78.0/24
101.251.0.0/24

223.0.0.0/24
223.1.1.0/24
223.223.223.0/24
223.255.255.0/24

Plus:
39.0.0.0/8
103.0.0.0/8
106.0.0.0/8
ERX Various Holes

Collaborators

Our warm thanks to our collaborators in this work, who have been generous with their time, systems and network in assisting us:

- Merit
- NTT Communications
- AARNet
- YouTube
- Google