Traffic in Network 14.0.0.0/8 and 223.0.0.0/8

May 2010

Geoff Huston
George Michaelson
APNIC R&D

Following the recent study on the level of background traffic observed in network 1.0.0.0/8 (http://www.potaroo.net/studies/1slash8/1slash8.html), APNIC has been allocated two further IPv4 address blocks by the IANA, namely 14.0.0.0/8 and 223.0.0.0/8. An experiment has been undertaken with these address blocks by advertising routes to these two address blocks, and recording all incoming traffic received in response to the routing advertisements. This document reports on the results of this experiment.

APNIC expresses its appreciation for the generous assistance provided by NTT and Merit in undertaking these experiments.

Experiment Details

In collaboration with APNIC, AS38639 (NTT) announced routes to 14.0.0.0/8 and 223.0.0.0/8 from 16 April 2010 until 24 April 2010. These routes originated from an NTT facility located in Japan. AS237 (Merit) then announced these same /8 routes for the period from 27 April 2010 until 5 May 2010. These routes originated in the US, originating from their systems in the USA. In both cases these were the only routing advertisements within these address blocks. The data collectors in both cases were unfiltered, and the data collection system was entirely passive.

Traffic Profile

Figures 1 and 2 show the traffic profile for network 14/8.

> (The graph utility used here does not make this adequately clear, but in Figures 1 – 10 the red trace is the total traffic, the blue trace is TCP, the green trace is UDP, the violet trace is ICMP and the cyan trace is all other protocols.)

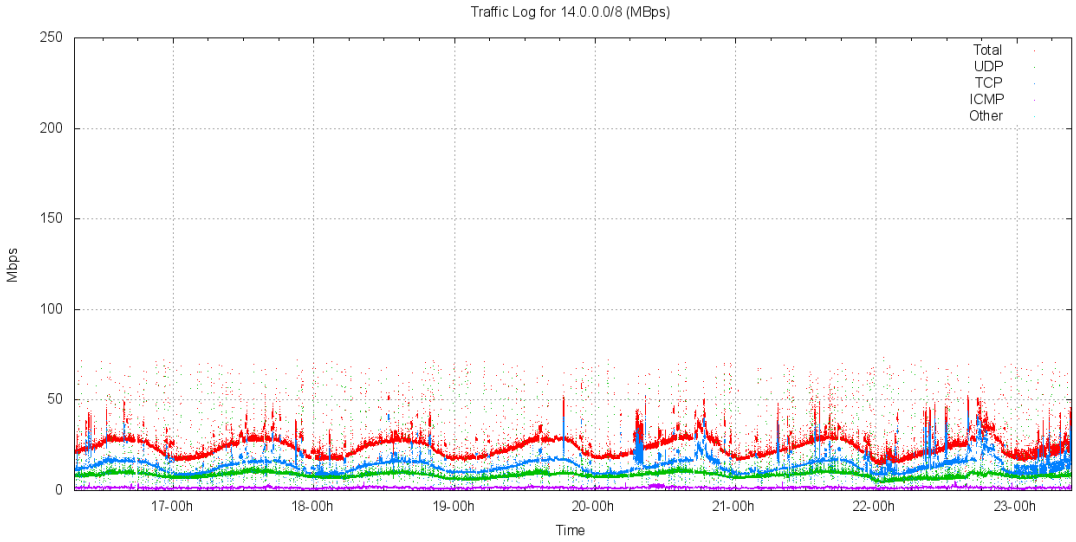

Figure 1 – Traffic profile for 14.0.0.0/8 advertised by AS38639

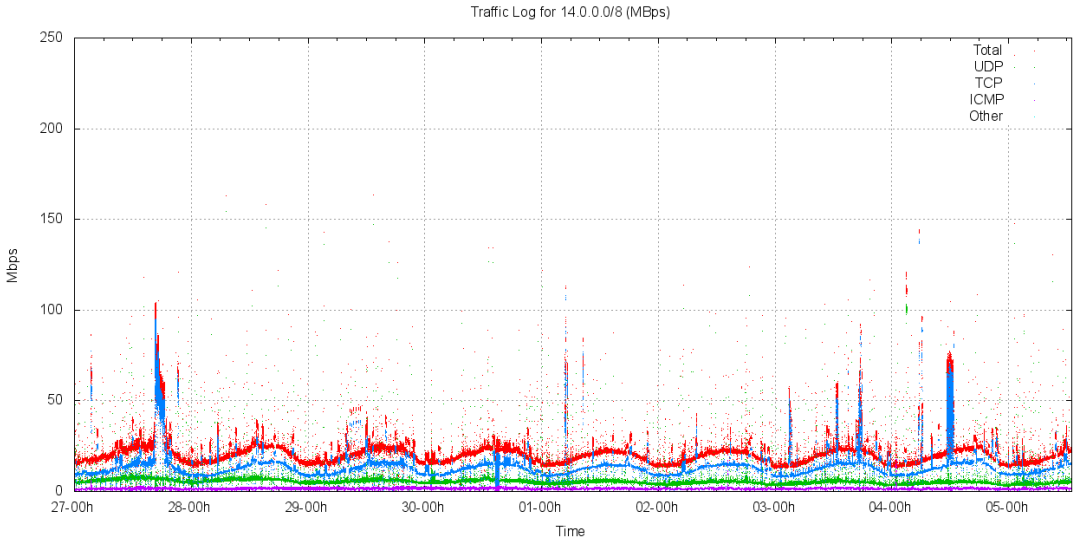

Figure 2 – Traffic profile for 14.0.0.0/8 advertised by AS237

The following two figures show the comparable data set for network 223.0.0.0/8

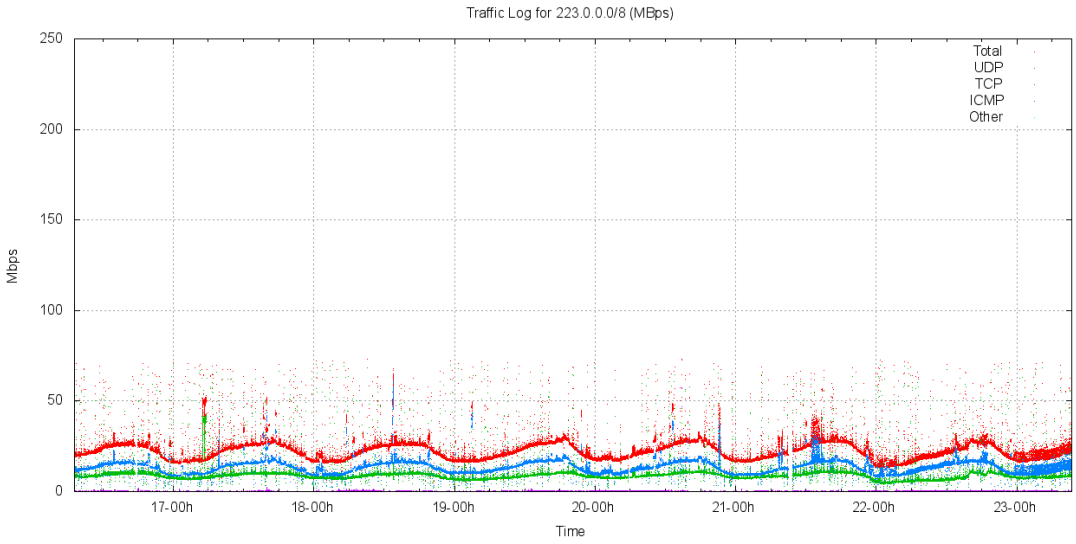

Figure 3 – Traffic profile for 223.0.0.0/8 advertised by AS38639

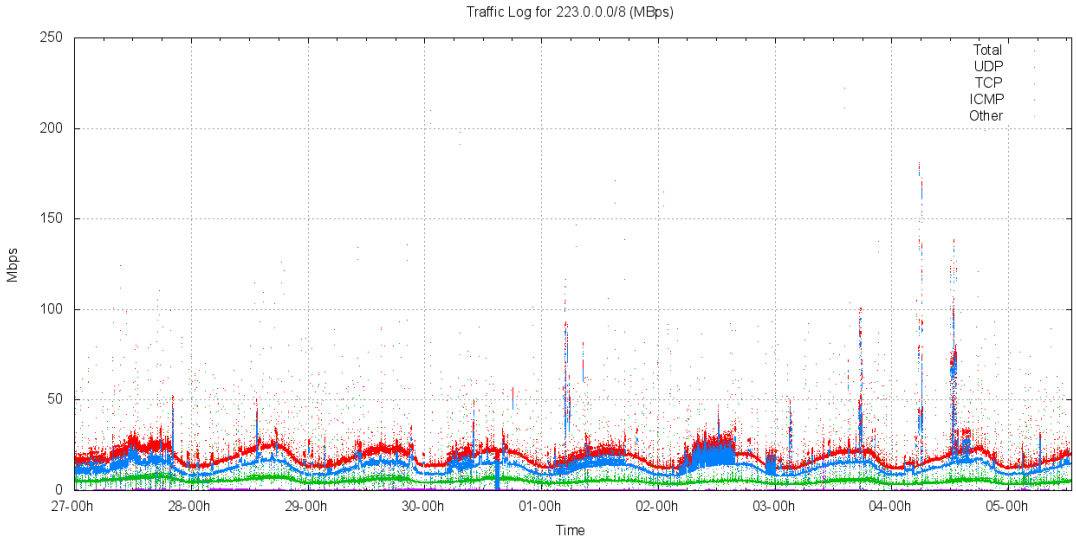

Figure 4 – Traffic profile for 223.0.0.0/8 advertised by AS3237

All four packet traces show a similar traffic pattern. Each /8 attracts some 17 – 25Mbps of incoming traffic. Of this, some 60% of the traffic is TCP and 35% is UDP, with the remainder being predominately ICMP.

The traffic shows a pronounced diurnal pattern, which most visible in the TCP component of the traffic. There is no clear weekday / weekend delineation.

In terms of protocol distribution, the distribution of incoming bytes in these two address blocks are shown in Table 1. This table also includes previously collected data concerning the protocol distribution in 1.0.0.0/8.

Protocol	**Proportion of Traffic 1.0.0.0/8**	**14.0.0.0/8**	**223.0.0.0/8**
TCP	9.8%	66.2%	71.4%
UDP	88.1%	25.6%	27.6%
ICMP	1.6%	8.0%	0.9%
Other	0.5%	0.2%	0.1%

Table 1. Distribution of Traffic by Protocol

Of note here is that the incoming traffic in network 1.0.0.0/8 was dominated by UDP traffic at a ratio of 10:1 (which was later analysed to be predominately SIP / RTP traffic directed to the address 1.1.1.1), while the incoming traffic in networks 14.0.0.0/8 and 223.0.0.0/8 is predominately TCP traffic, at a ratio of 5:2.

Also of note in terms of traffic profile, incoming TCP traffic in network 1.0.0.0/8 showed no marked diurnal pattern, while the TCP traffic in both 14.0.0.0/8 and 223.0.0.0/8 show a marked diurnal variation.

The second view of the overall traffic profile is by packet count rather than traffic (byte) counts. The packet profile of incoming traffic in these two network blocks is shown in the following two figures.

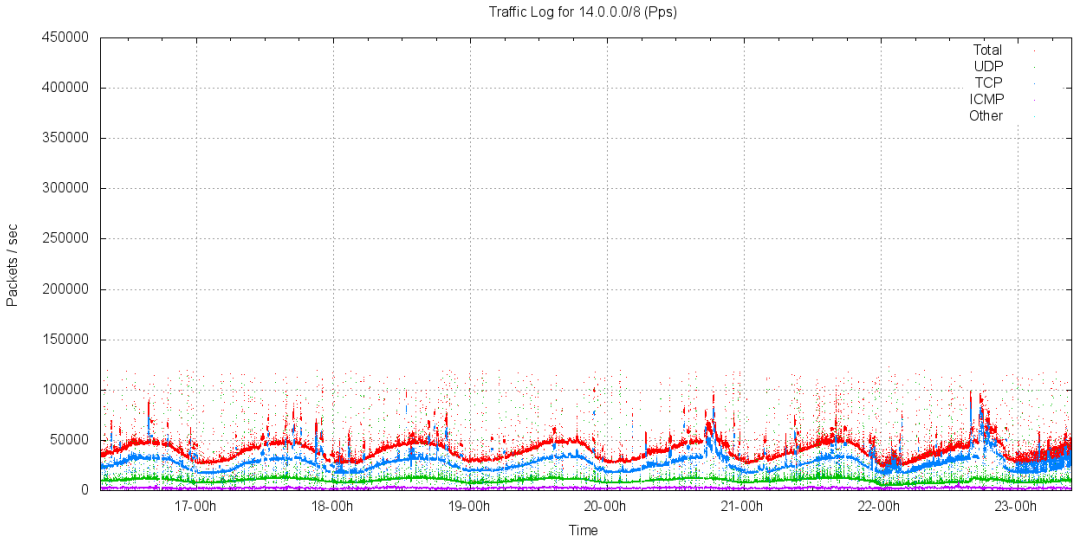

Figure 5 – Packet profile for 14.0.0.0/8 advertised by AS38639

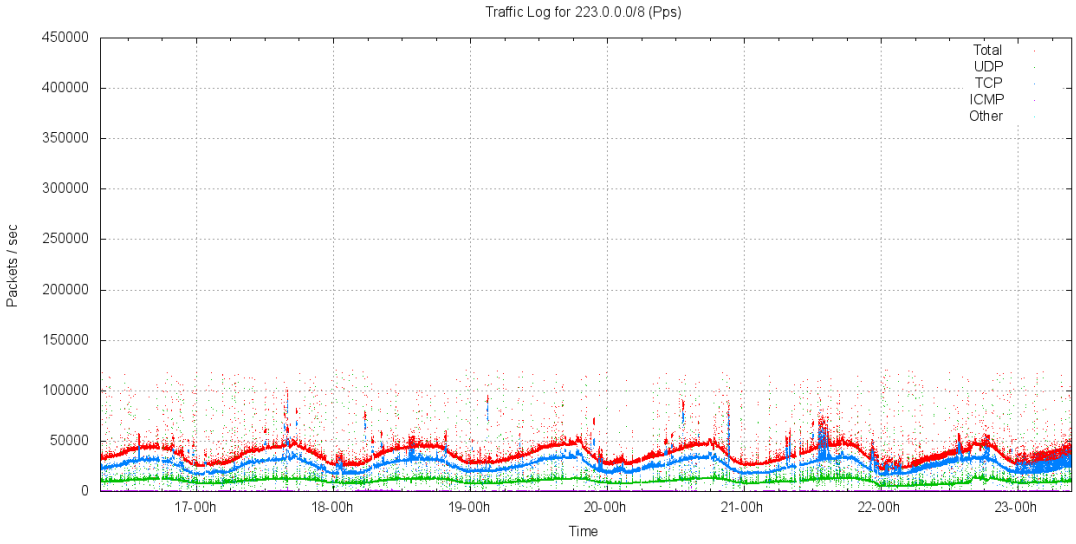

Figure 6 – Packet profile for 223.0.0.0/8 advertised by AS38639

Each /8 attracts between 3,500 and 5,000 packets per second, where between 66% (14/8) to 72% (223/8) of the incoming packets are TCP, between 25% (14/8) and 27% (223/8) are UDP and the remaining 10% being ICMP.

In terms of protocol distribution, the distribution of incoming bytes in these two address blocks are shown in Table 2. This table also includes previously collected data concerning the protocol distribution in 1.0.0.0/8.

Protocol	**Proportion of Packets**		
	1.0.0.0/8	**14.0.0.0/8**	**223.0.0.0/8**
TCP	19.8%	50.0%	50.0%
UDP	76.9%	36.5%	35.7%
ICMP	2.5%	9.9%	13.9%
Other	0.7%	3.6%	0.3%

Table 2. Distribution of Packets by Protocol

Again, there is a marked difference in the traffic profile in terms of packet counts, between network 1.0.0.0/8 and these other two network blocks, where networks 14.0.0.0/8 and 223.0.0.0/8 show a far higher proportion of TCP packets.

The third form of traffic profile is in terms of packet size distribution. TCP packets are predominately 62 octet SYN packets (18,873M of the 20,158M TCP packets (94%) were TCP SYN packets in the 14.0.0.0/8 data set collected by AS237).

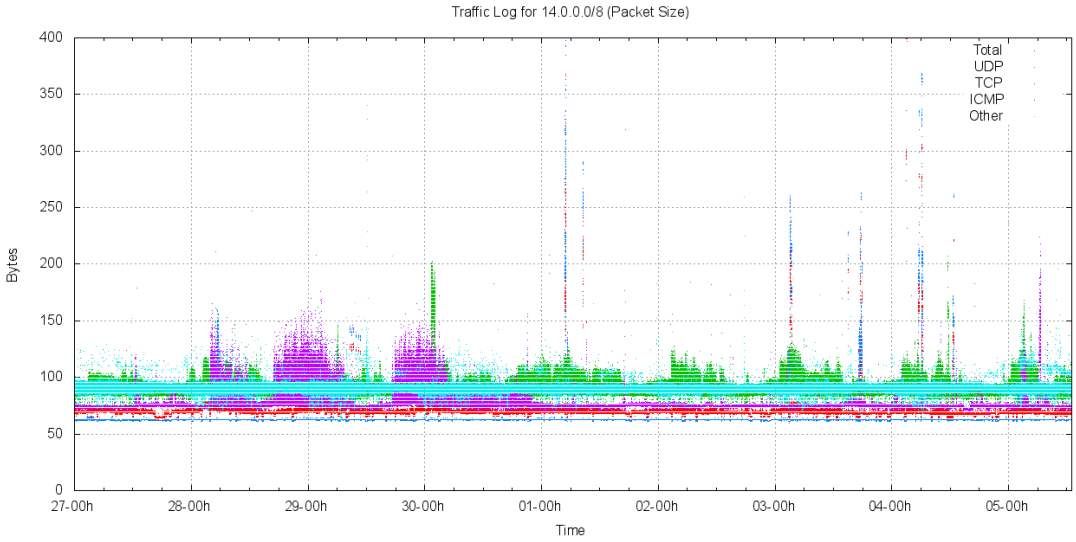

Figure 7 – Packet size distribution for 14.0.0.0/8 (AS237)

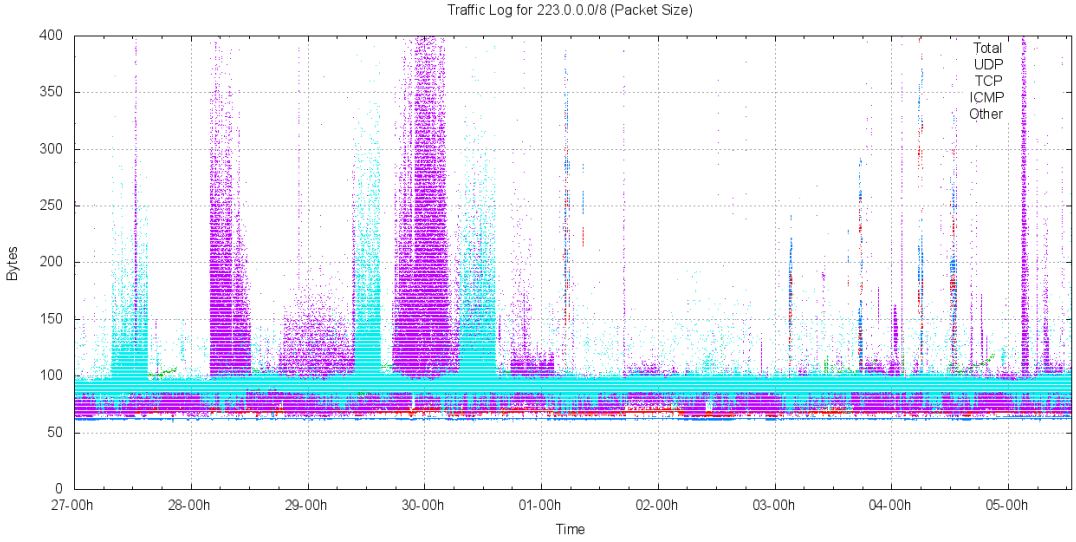

Figure 8 – Packet size distribution for 223.0.0.0/8 (AS237)

Of note in the data collected at AS237 is the ICMP and "other protocol" extended bursts of larger packet size collected at AS237. These bursts were not observed by AS38639 (Figures 9 and 10). In the AS38639 data set the ICMP packets directed as net 223.0.0.0/8 show a slightly larger degree of variance in size than those observed directed to 14.0.0.0/8.

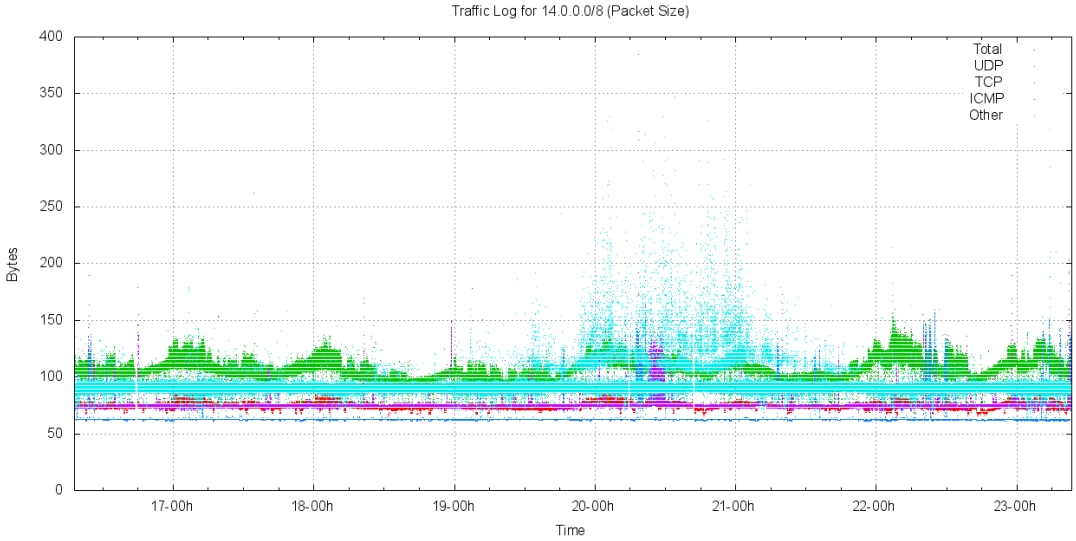

Figure 9 – Packet size distribution for 14.0.0.0/8 (AS38639)

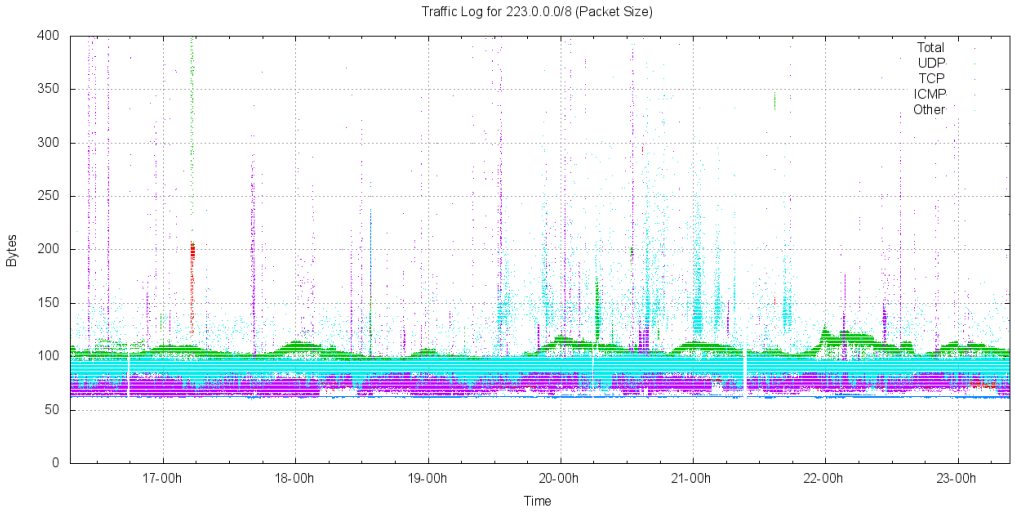

Figure 10 – Packet size distribution for 223.0.0.0/8 (AS38639)

Distribution of Traffic Across /16s

The following figures show the distribution of traffic across the two /8 address blocks, divided up into each of the 256 /16 address blocks. Figures 11 and 12 show this distribution for 14.0.0.0/8, and Figures 13 and 14 show the same distribution for network 223.0.0.0/8.

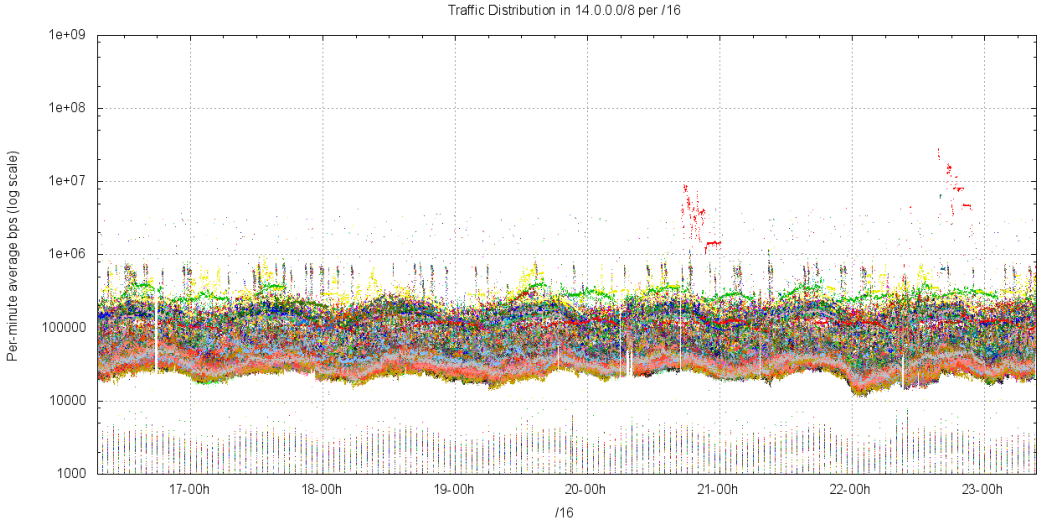

Figure 11 – Traffic distribution per /16 for 14.0.0.0/8 (AS38639)

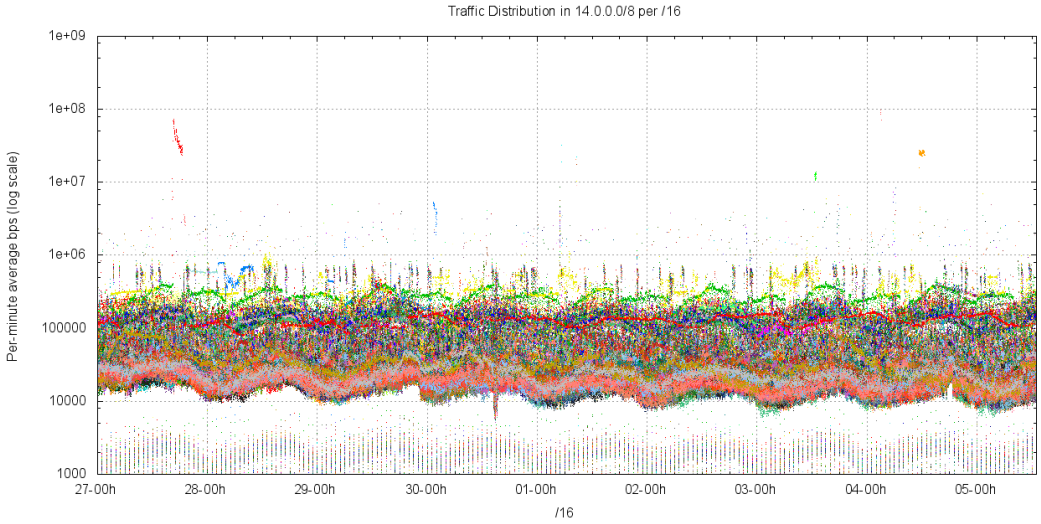

Figure 12 – Traffic distribution per /16 for 14.0.0.0/8 (AS237)

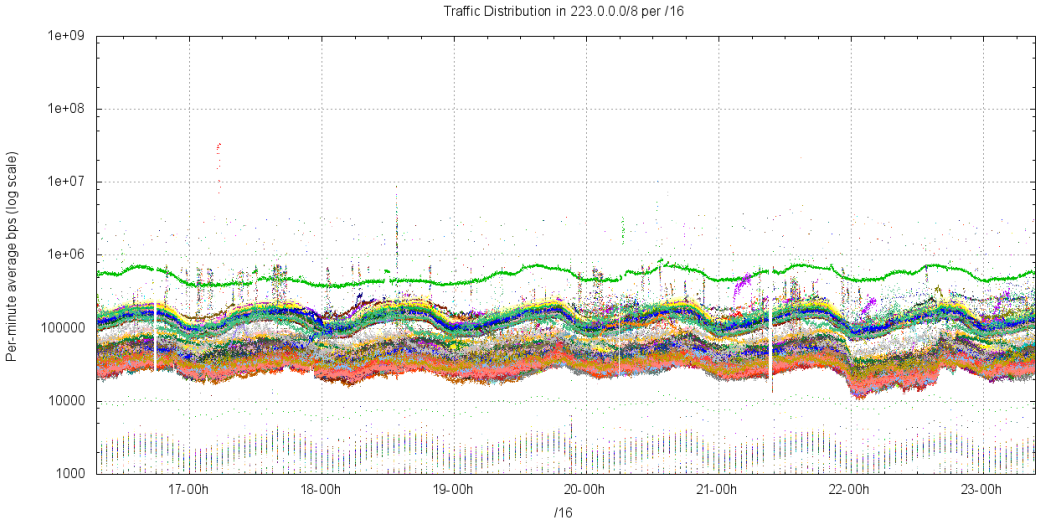

Figure 13 – Traffic distribution per /16 for 223.0.0.0/8 (AS38639)

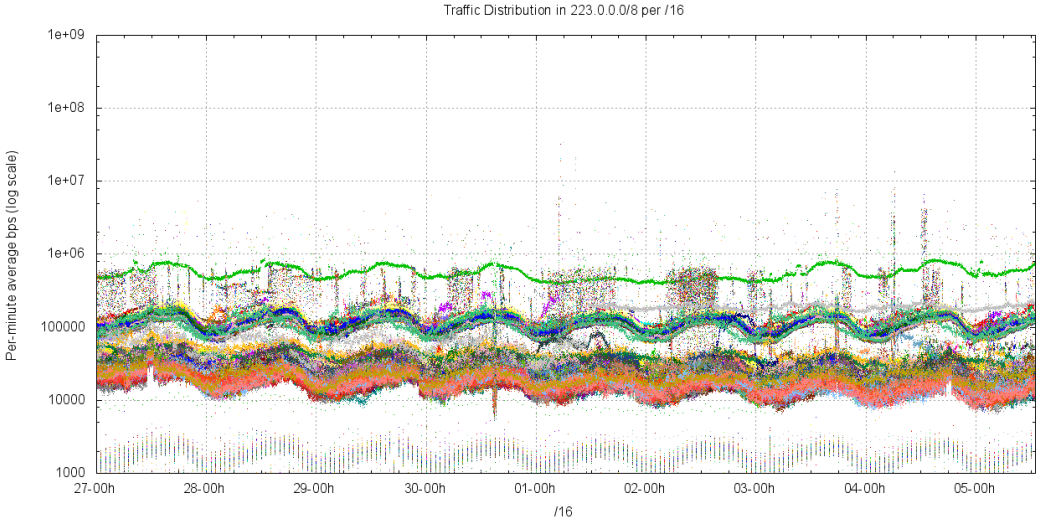

Figure 14 – Traffic distribution per /16 for 223.0.0.0/8 (AS237)

In all cases the level of incoming traffic lies between 10Kbps to 200Kbps, with a visible diurnal component. In the case of the block 14.0.0.0/8 no single /16 appears to attract an extraordinary level of traffic as compared to the remaining pool of /16 addresses. In the case of 223.0.0.0/8 a single /16, namely 223.1.0.0/16) appears to attract between 500Kbps and 800Kbps.

The distribution of average traffic levels for each of these /8s is shown in the following 4 figures.

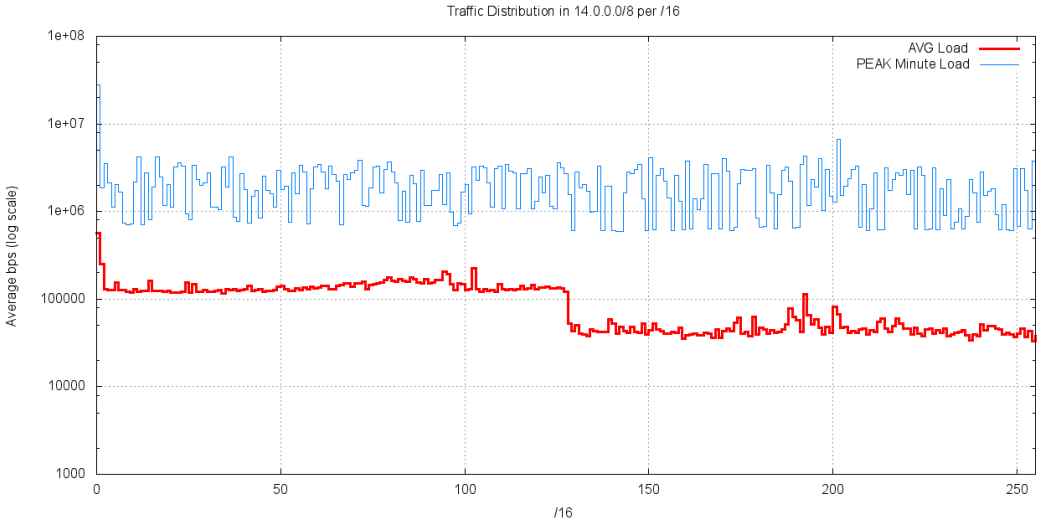

Figure 15 – Average Traffic load per /16 for 14.0.0.0/8 (AS38639)

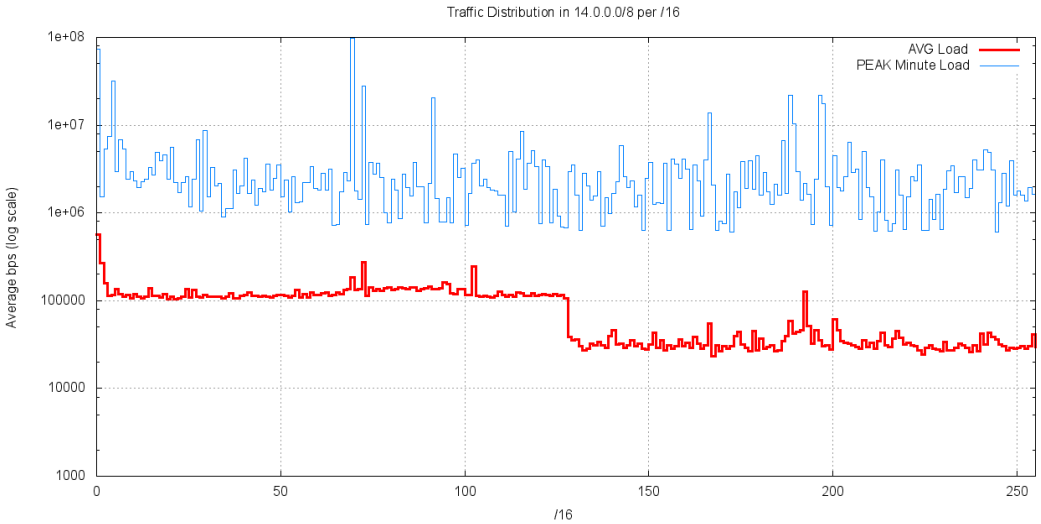

Figure 16 – Average Traffic load per /16 for 14.0.0.0/8 (AS237)

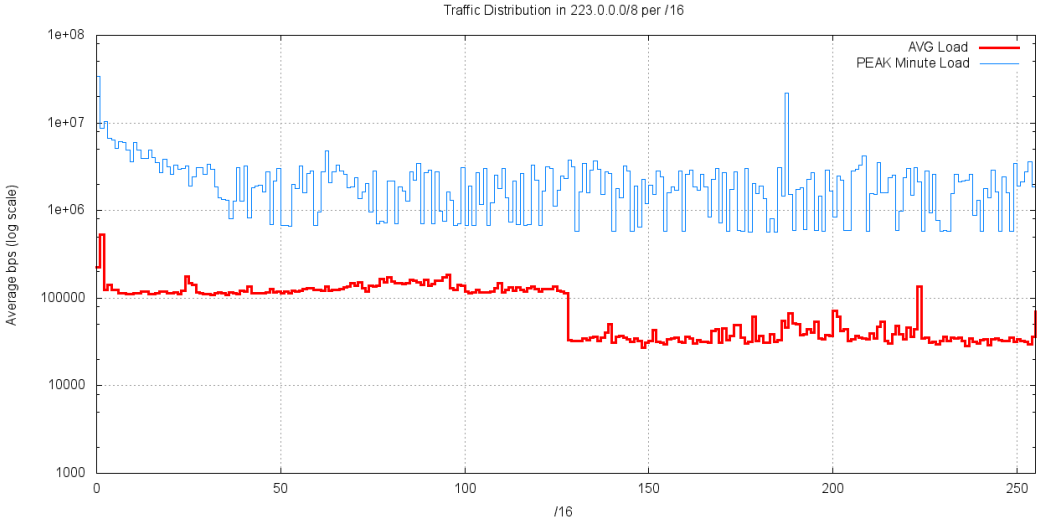

Figure 17 – Average Traffic load per /16 for 223.0.0.0/8 (AS38639)

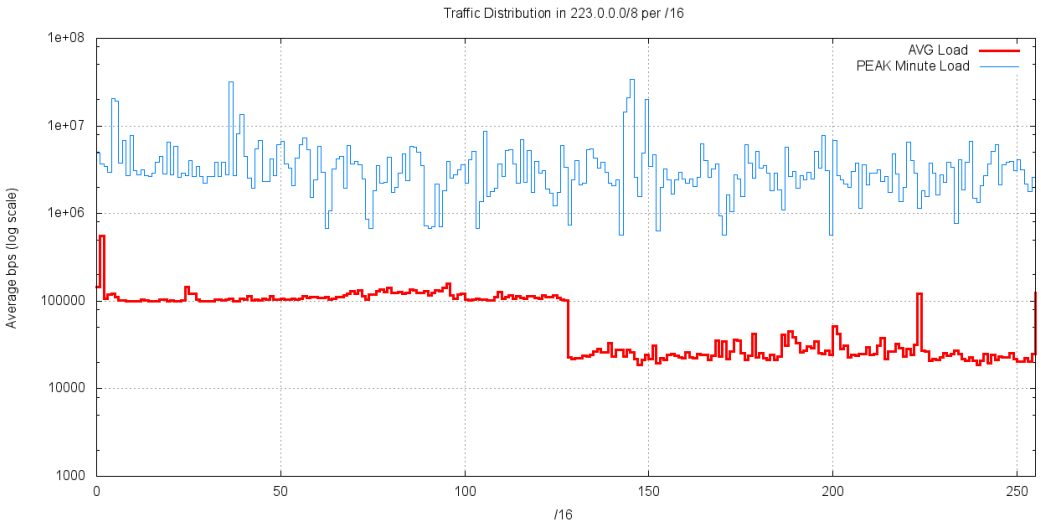

Figure 18 – Average Traffic load per /16 for 223.0.0.0/8 (AS237)

All four data collections show a pronounced break in the "middle" of the address block. The low half of the address blocks (14.0.0.0/9 and 223.0.0.0/9) have an average traffic load of 130Kbps per /16, while the upper half of the blocks (14.128.0.0/9 and 223.128.0.0/9) have an average traffic load of 30Kbps. This will be examined in the next section.

Differences in "low" and "high" /9s

Of the 20,581 million TCP packets directed to network 223 when advertised by AS237, some 14,447 million TCP packets were directed to port 445. TCP port 445 is used by Microsoft systems to support the Server Message Block (SMB) protocol, used for file sharing. It is also a very common vector for attacks on Microsoft Windows systems.

Taking a one hour sample period at 1800 UTC to 1900 UTC on 16 April, using the AS38639 data collected for net 223.0.0.0/8, there were a total of 153,821,993 packets received by the collector. Of these, 1,283,494 TCP packets were directed to port 445 in the "high" /9 of 223.128.0.0/9 (or 0.8% of the total packet count), as compared to 92,618,523 in the low /9 (or 60% of the total packet count).

Reports of the behaviour of the Conficker virus point to a outcome of the virus' random IP generation routine for port 445 scanning where bit 9 of the randomly generated IP address is always 0, as is bit 24 (http://www.caida.org/research/security/ms08-067/conficker.xml). The outcome of bit 9 being clear is that Conficker will only scan the "low" /9 of any /8 network block using the random IP generator.

This is the most likely reason for the disparity in incoming traffic levels between the "low" and "high" /9s in these network blocks. It also indicates that some 100Kbps per /16 in the bottom half of each of the address blocks is attributable to Conficker's port 445 scanning activity. The total traffic component of Conficker is some 40% of the total traffic load directed to these network blocks, and 60% of the total packet count, indicating the significant extent to which unpatched Windows systems continue to be vulnerable to this particular virus.

Distribution of Traffic

The following four figures show the distribution of traffic levels per /24 in network 14.0.0.0/8 (Figures 19 and 20) and network 223.0.0.0/8 (Figures 21 and 22).

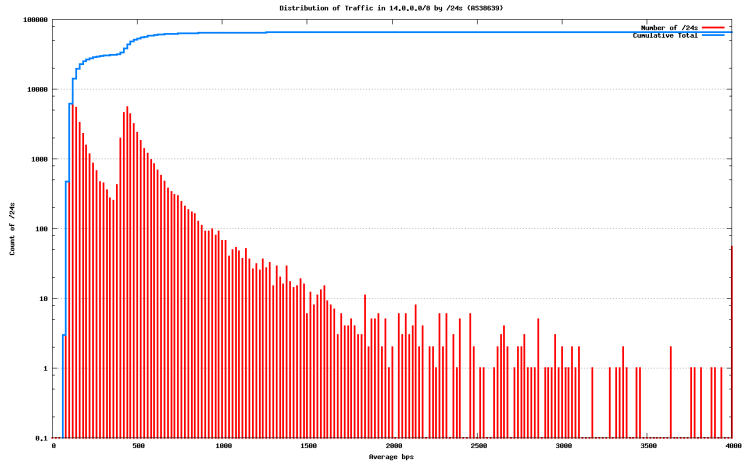

Figure 19 – Traffic profile for 14.0.0.0/8 by /24s (AS38639)

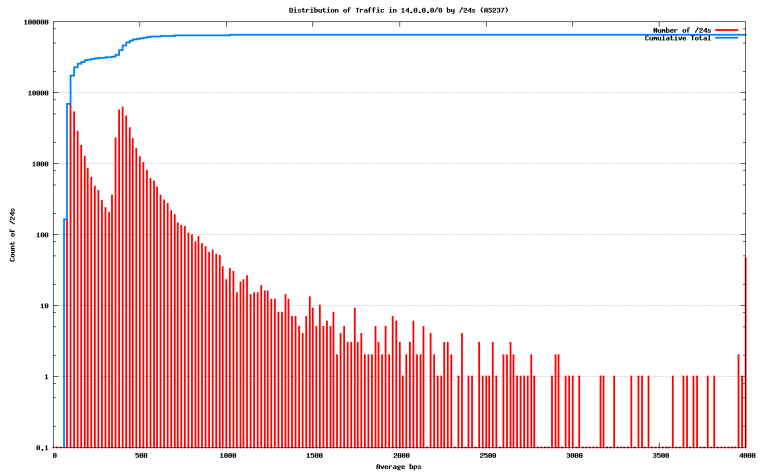

Figure 20 – Traffic profile for 14.0.0.0/8 by /24s (AS237)

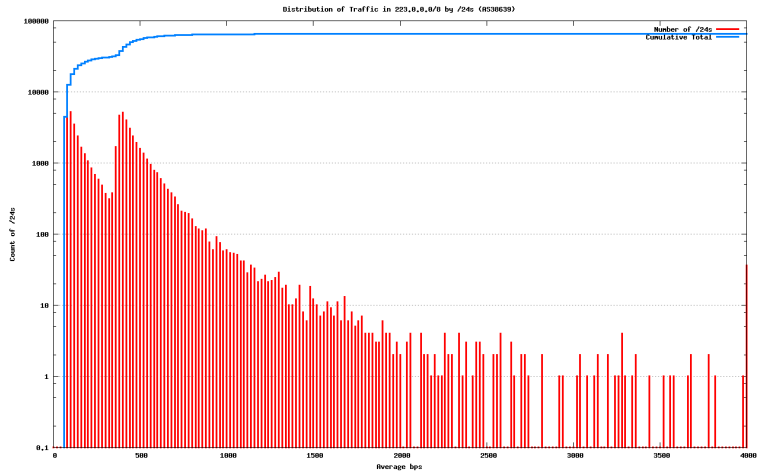

Figure 21 – Traffic profile for 223.0.0.0/8 by /24s (AS38639)

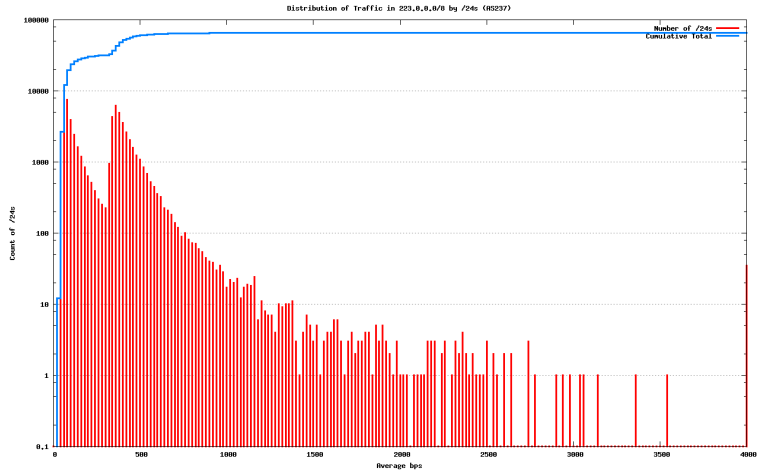

Figure 22 – Traffic profile for 223.0.0.0/8 by /24s (AS237)

The two peaks in all these distributions are evidently due to Conficker scanning across the low /9 of the address block. It appears that the Conficker scanning traffic element is common across the entire IPv4 address range, and this additional traffic component of some 500bps per /24 directed to TCP port 445 in the low /9 of these two address blocks is not an anomaly that warrants any particular action in terms of reservation of addresses from allocations or assignments.

High Traffic Prefixes in 14.0.0.0/8

In terms of potentially anomalous /16s in 14.0.0.0/8, outside of this division into the lower and upper halves, the blocks 14.0.0.0/16, 14.1.0.0/16 and 14.102.0.0/16 appear to have a higher level of incoming traffic in both experiments. The average measurements of incoming traffic for these three /16s are shown in Table 3.

	AS38639	AS237
14.0.0.0/16	561Kbps	567Kbps
14.1.0.0/16	250Kbps	265Kbps
14.102.0.0/16	226Kbps	244Kbps

Table 3 – Most active /16s in 14.0.0.0/8

A more detailed examination of the load for these three /16s using the AS237 data set is shown in Figures 23, 24 and 25.

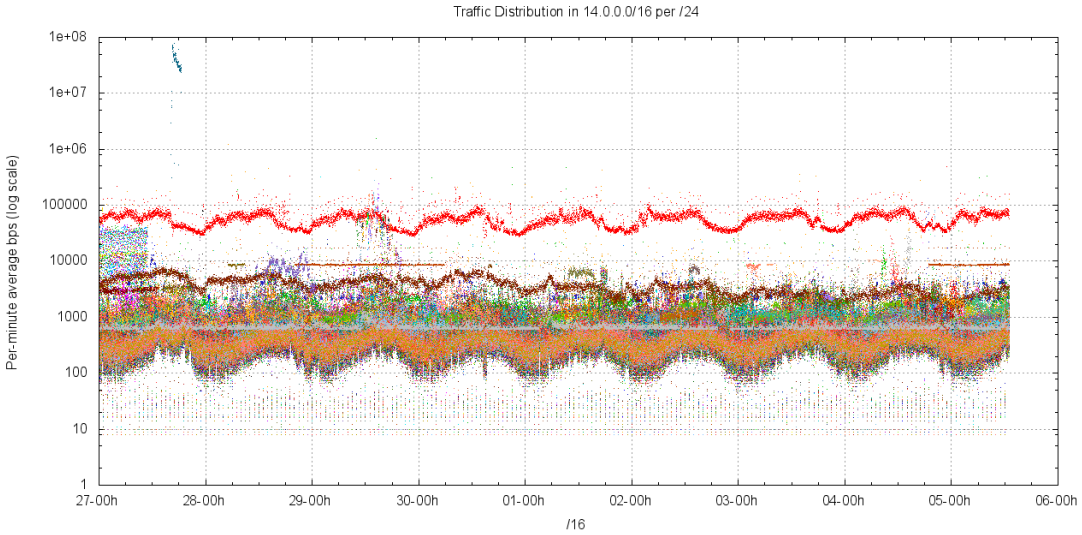

Figure 23 – Traffic profile for 14.0.0.0/16 (AS237)

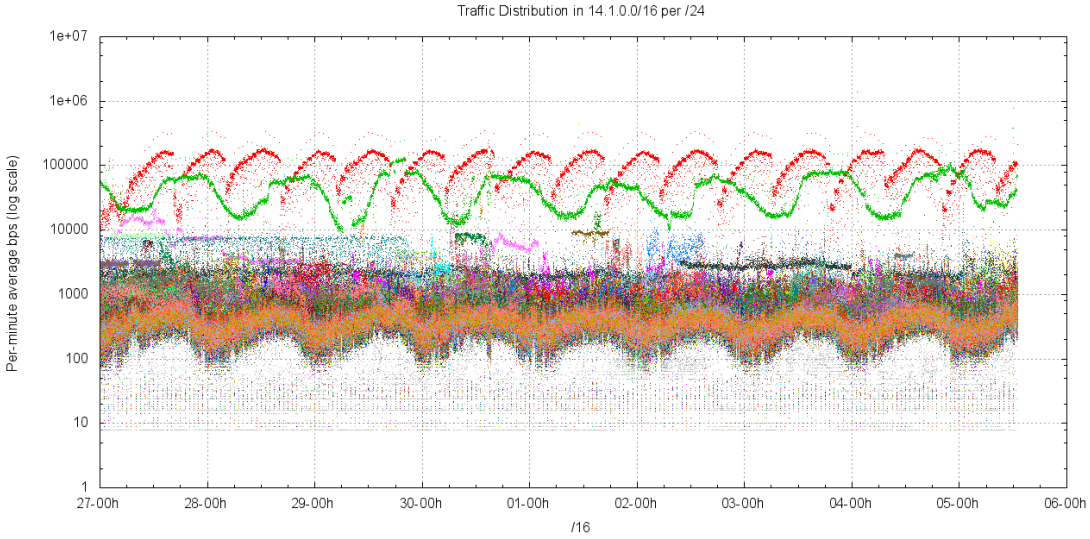

Figure 24 – Traffic profile for 14.1.0.0/16 (AS237)

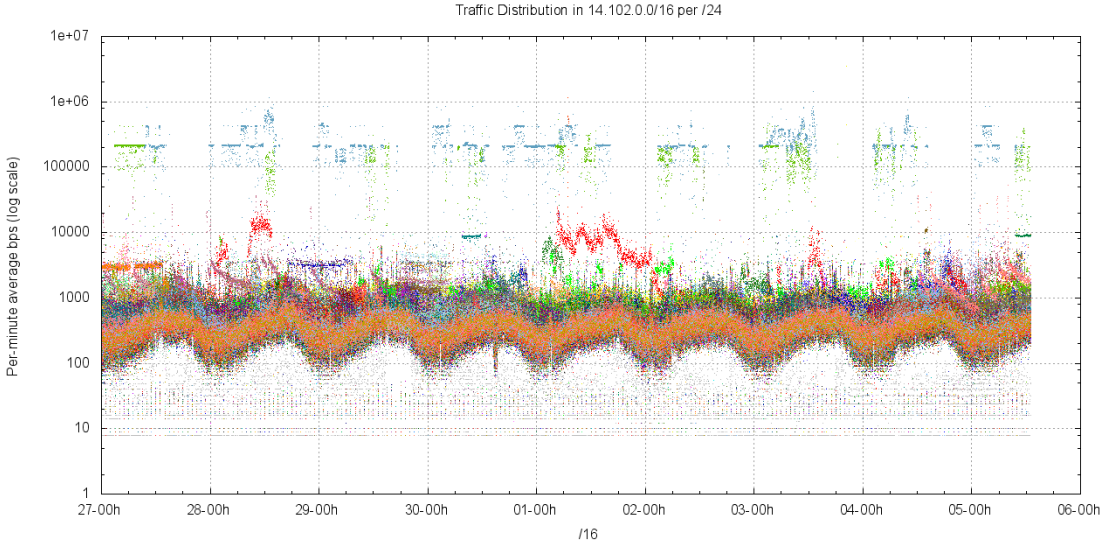

Figure 25 – Traffic profile for 14.102.0.0/16 (AS237)

There are also a further /16 that has a highly active /24, namely 14.192.0.0/16, whose traffic profile as seen by AS237, is shown in Figure 26.

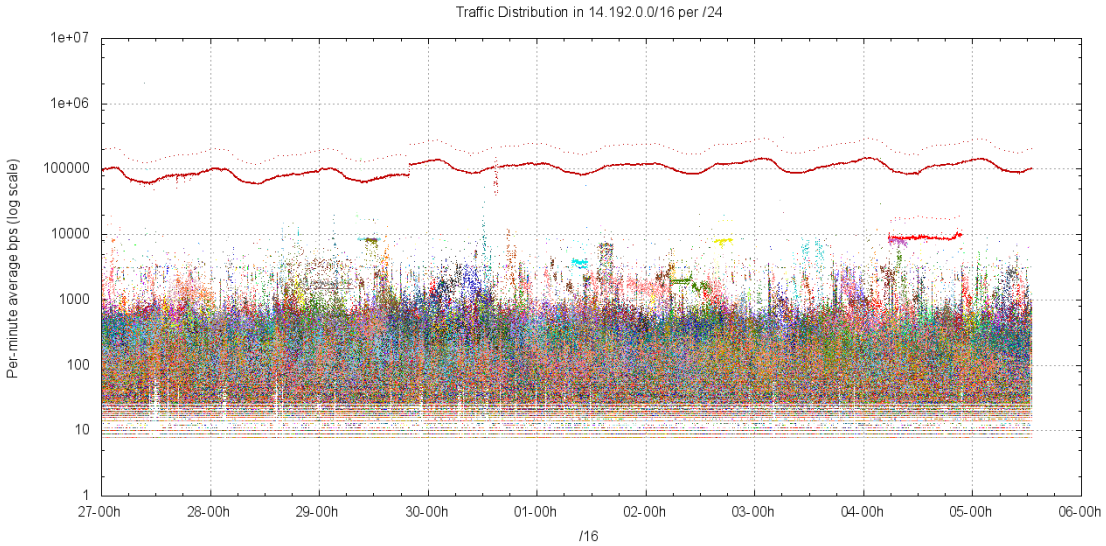

Figure 26 – Traffic profile for 14.192.0.0/16 (AS237)

Closer inspection of the entire 14.0.0.0/8 data at a level of granularity of individual /24's in 14.0.0.0/8 across the two experiments shows that there are 4 individual /24s that appear to consistently receive traffic in excess of 50Kbps in both experiments, and a further 2 /24s that received higher than normal volumes in one experiment, but not in the other.

/24 Prefix	AS38639	AS237
14.0.15.0/24	369Kbps	386Kbps
14.1.0.0/24	78Kbps	99Kbps
14.192.76.0/24	73Kbps	101Kbps
14.0.0.0/24	56Kbps	56Kbps
14.102.129.0/24	54Kbps	27Kbps
14.102.128.0/24	48Kbps	109Kbps

Table 4 – Most active /24s in 14.0.0.0/8

High Traffic Prefixes in 223.0.0.0/8

The traffic profile for 223.0.0.0/8 (Figures 17 and 18) indicates anomalous traffic directed to networks in 223.0.0.0/16 and 223.1.0.0/16. These address blocks can be further broken into its constituent /24s, as shown in Figures 27 through 30.

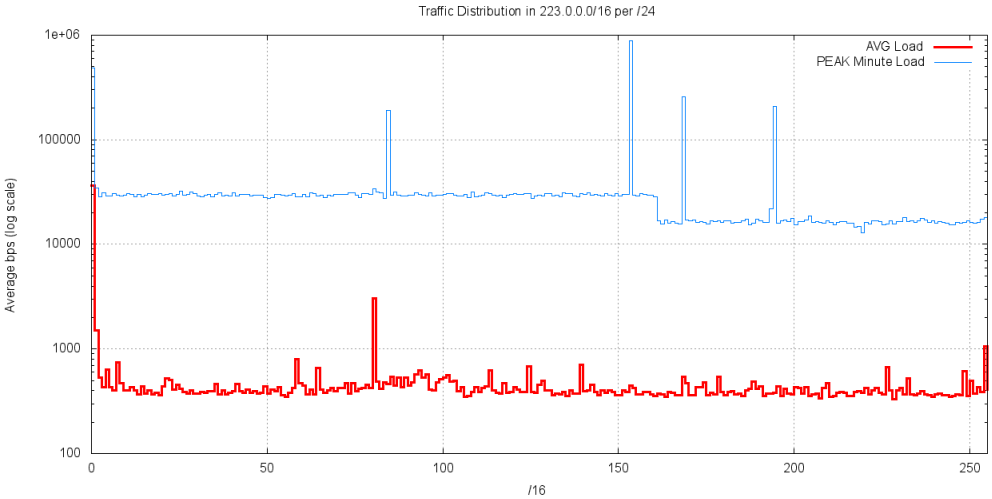

Figure 27 – Traffic profile for 223.0.0.0/16 (AS237)

It is evident that the major component of this traffic is directed at 223.0.0.0/24, and within that /24 some 60% of the packets are directed to 223.0.0.0 and 11% are directed to 223.0.0.1.

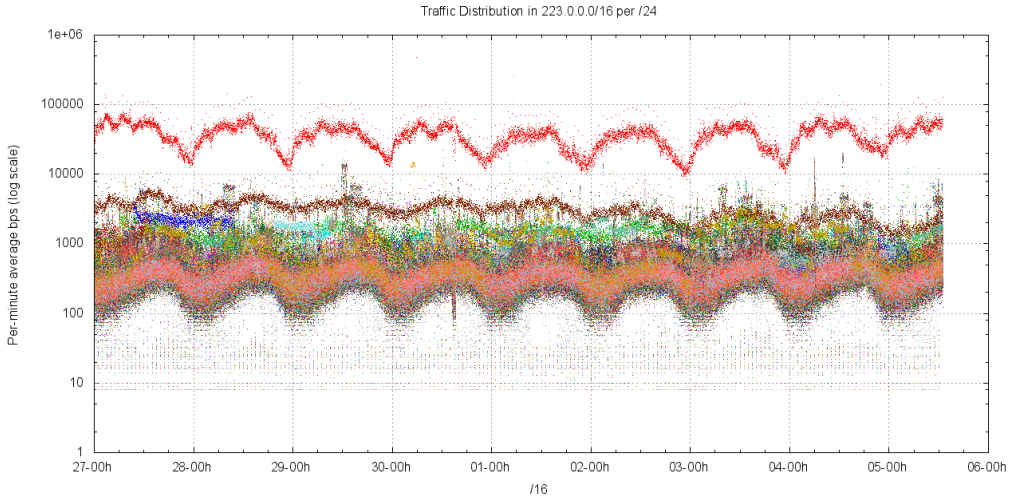

Figure 28 – Traffic profile for 223.0.0.0/16 (/24s) (AS237)

There is a somewhat different profile for 223.1.0.0/16 (Figures 29 and 30).

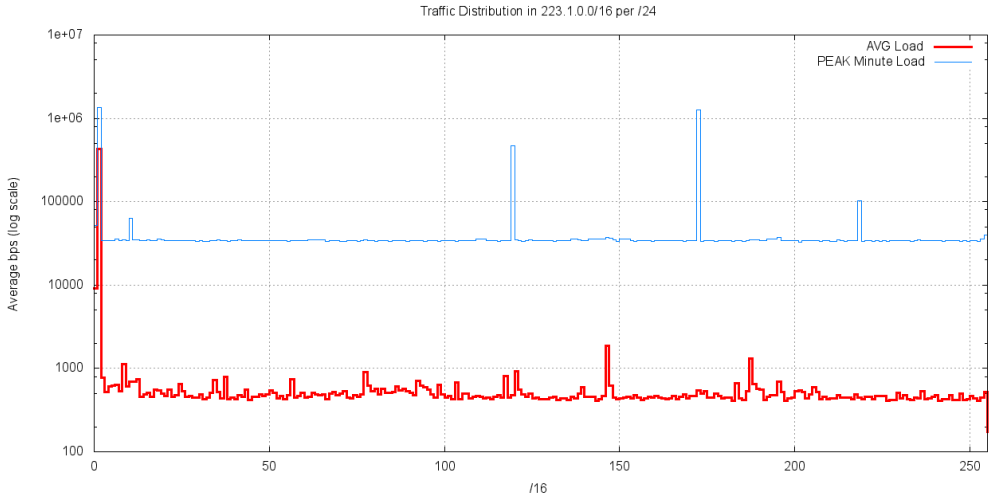

Figure 29 – Traffic profile for 223.1.0.0/16 (/24s) (AS237)

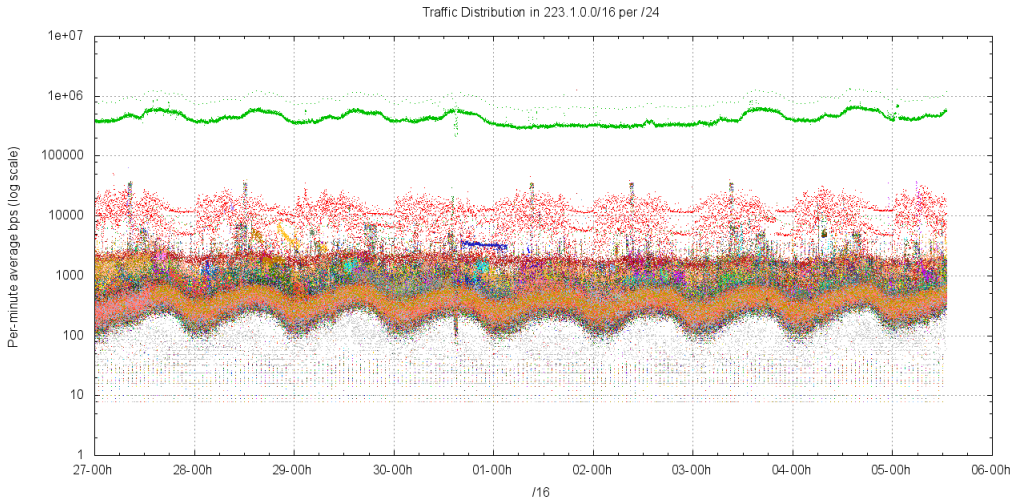

Figure 30 – Traffic profile for 223.1.0.0/16 (/24s) (AS237)

It is evident that the major component of this traffic in 223.1.0.0/16 is being directed to 223.1.1.0/24. Within this /24, the overall majority of the traffic is being directed to the single address 223.1.1.128. A web search for this address

reveals that a possible cause for unsolicited traffic being directed is traffic leakage from a commercial "secure" VPN client package. It appears that this VPN product uses 223.1.1.128 as a default network adapter interface. What is being observed here appears to be leakage of traffic into the public network from this default configuration state where VPN traffic is being directed to the address 223.1.1.128. The traffic level of this leakage of VPN traffic into the public Internet is between 300Kbps and 500Kbps.

There are two further /16s that have individual /24s that are attracting abnormally high traffic levels, namely 223.223.0.0/16 and 223.255.0.0/16 (Figures 31 and 32).

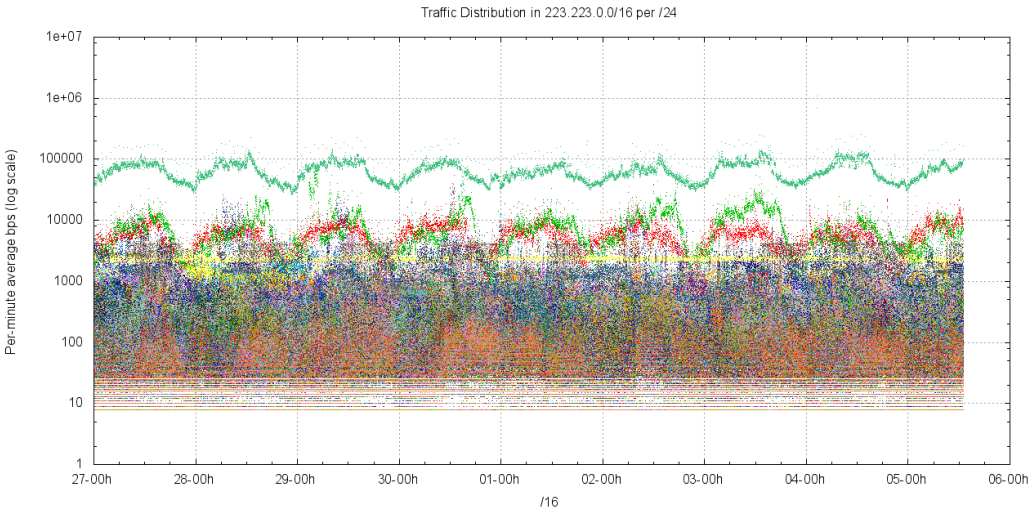

Figure 31 – Traffic profile for 223.223.0.0/16 (AS237)

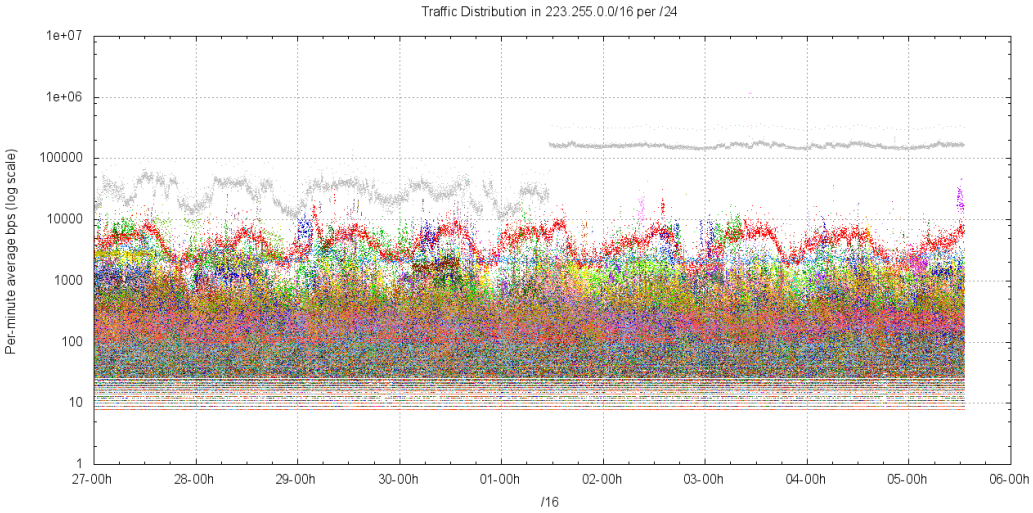

Figure 32 – Traffic profile for 223.223.0.0/16 (AS237)

In summary, there are 2 /24's in 223.0.0.0/8 that were measured as receiving more than 50Kbps of traffic in both experiments. A further 2 /24's had more than 50Kbps of incoming traffic in one experiment, but not in the other. These results are summarized in Table 4.

/24 Prefix	AS38639	AS237
223.1.1.0/24	392Kbps	433Kbps
223.223.223.0/24	65Kbps	65Kbps
223.0.0.0/24	101Kbps	36Kbps
223.255.255.0/24	27Kbps	92Kbps

Table 5 – Most active /24s in 223.0.0.0/8

Conclusions

There are four /24s in network 14 that appear to consistently attract more than 50Kbps of incoming traffic level. These are:

14.0.0.0/24
14.0.15.0/24
14.1.0.0/24
14.192.76.0/24

Two further /24s appear anomalous at this stage:

14.102.128.0/24
14.102.129.0/24

It is recommended that these six /24s be withheld from regular allocation or assignment for a period of six months, to allow for more detailed testing of the extent to which this incoming traffic profile is sustained.

There are two /24s in network 223 that also appear to attract significantly higher levels of traffic than the remainder of the address block. These are:

223.0.0.0/24
223.1.1.0/24

Two further /24s appear anomalous at this stage:

223.223.223.0/24
223.255.255.0/24

It is recommended that these four /24s be withheld from regular allocation or assignment for a period of six months, to allow for more detailed testing of the extent to which this incoming traffic profile is sustained.