Background Traffic to Network 106.0.0.0/8

March 2010

Geoff Huston
George Michaelson
APNIC R&D
research@apnic.net

APNIC is now regularly examining the unused state of IPv4 address blocks before they are passed over for general allocation. Experiments are undertaken with these address blocks by advertising a route to the address block, and recording all incoming traffic received in response to the routing advertisements. This document reports on the results of this experiment in the identification of the patterns of such "background" traffic that is being directed to the address block 106.0.0.0/8.

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

Experiment Details

In collaboration with APNIC, AS237 (Merit) exclusively announced 106.0.0.0/8 for the period from 15 February 2011 until 24 February 2011. The data collector was unfiltered, and the data collection system was entirely passive, and no packets were generated in response to the incoming traffic.

Traffic Profile

Figure 1 shows the traffic profile for network 106.0.0.0/8.

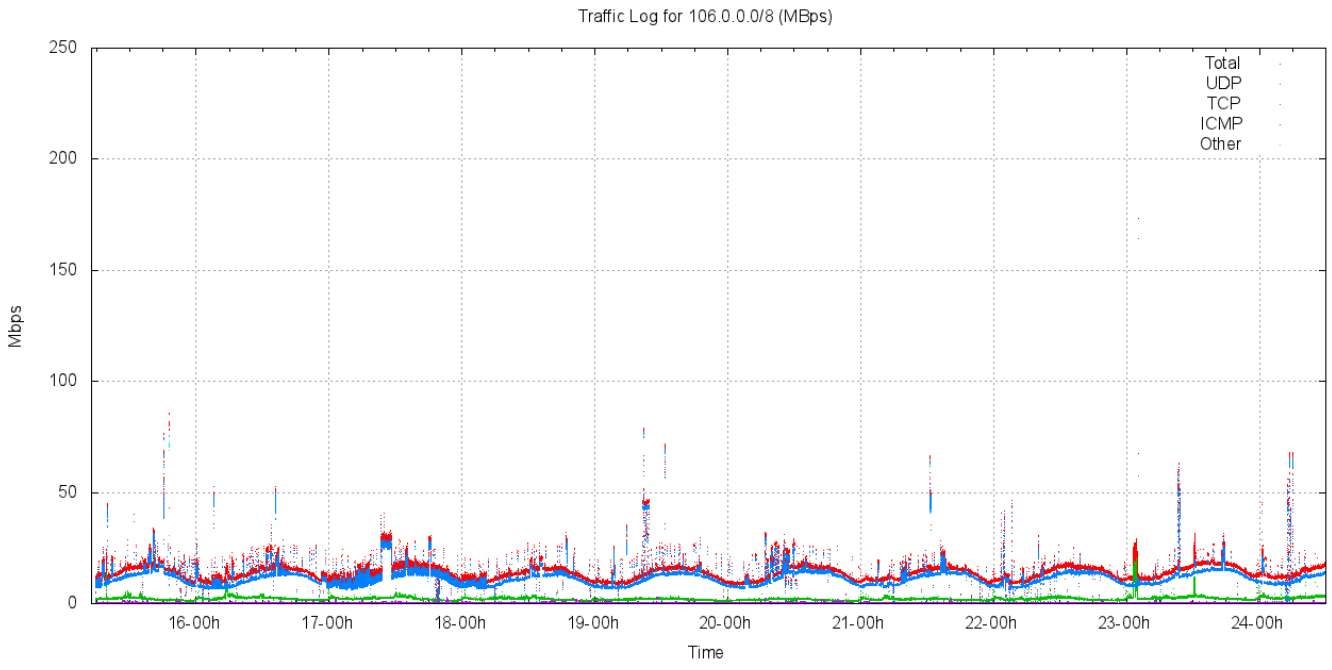


Figure 1 – Traffic profile for 106.0.0.0/8

(The graph utility used here does not make this adequately clear, but in the following figures 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.)

This traffic profile is similar to the profile that was recorded for other /8 address blocks recently allocated to APNIC, including 36.0.0.0/8 and 101.0.0.0/8. The address block 106.0.0.0/8 attracts some 12 – 25Mbps of incoming traffic.

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.

Protocol	Traffic Ratio 106.0.0.0/8	39.0.0.0/8	36.0.0.0/8	101.0.0.0/8	49.0.0.0/8	14.0.0.0/8	223.0.0.0/8
TCP	81.9%	78.7%	82.8%	76.0%	81.5%	66.2%	71.4%
UDP	15.7%	18.0%	14.5%	22.7%	17.4%	25.6%	27.6%
ICMP	2.2%	2.5%	2.0%	0.9%	1.1%	8.0%	0.9%
Other	0.2%	0.7%	0.7%	0.4%	0.0%	0.2%	0.1%

Table 1. Distribution of Traffic by Protocol

The second view of the overall traffic profile is by packet count rather than traffic (byte) counts. The packet profile of incoming traffic in this network block is shown in the following figure.

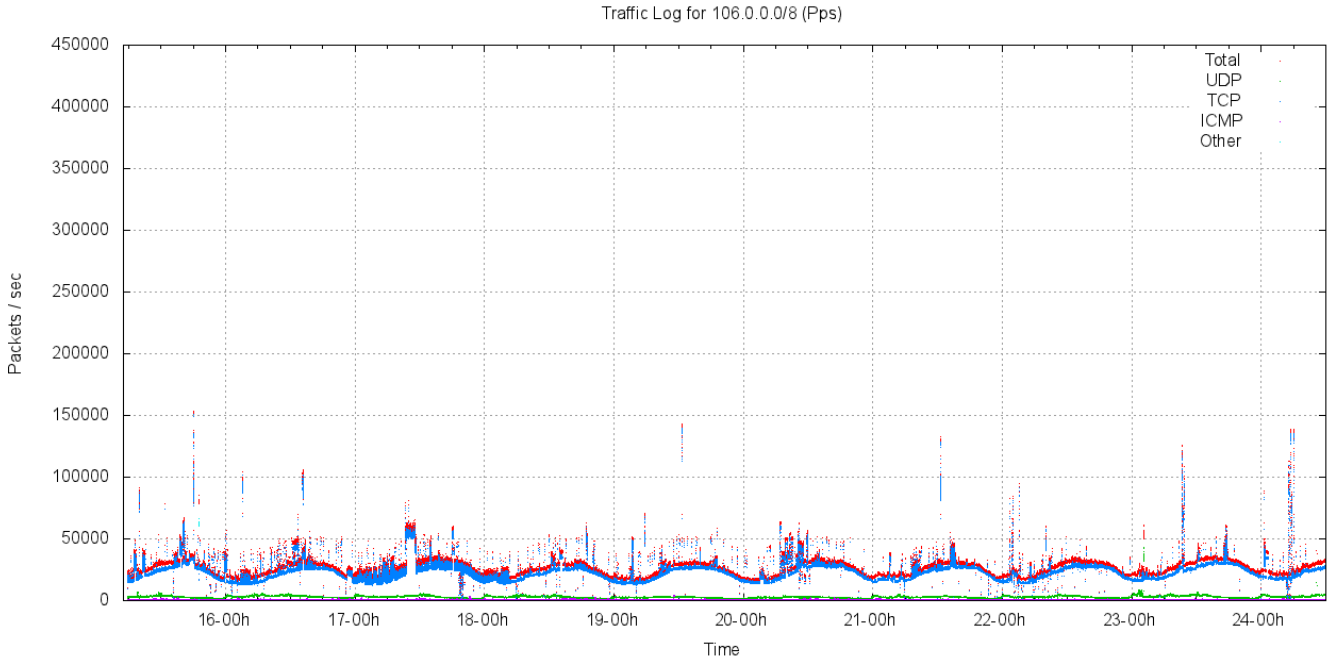


Figure 2 – Packet profile for 106.0.0.0/8

The 106.0.0.0/8 network block attracts between 25,000 and 45,000 packets per second, where 86.5% of the incoming packets are TCP, between 11.1% are UDP, 2.3% are 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 on other recently allocated /8s.

Protocol	Ratio 106.0.0.0/8	39.0.0.0/8	36.0.0.0/8	101.0.0.0/8	49.0.0.0/8	14.0.0.0/8	223.0.0.0/8
TCP	86.5%	84.5%	88.4%	83.1%	86.9%	50.0%	50.0%
UDP	11.1%	12.1%	9.2%	16.1%	14.2%	36.5%	35.7%
ICMP	2.3%	2.4%	1.7%	0.7%	6.1%	9.9%	13.9%
Other	0.1%	0.5%	0.7%	0.2%	4.6%	3.6%	0.3%

Table 2. Distribution of Packets by Protocol

The third form of traffic profile is in terms of packet size distribution. TCP packets are predominately 62 octet SYN packets (15,665M of the 18,175M TCP packets (86%) were TCP SYN packets).

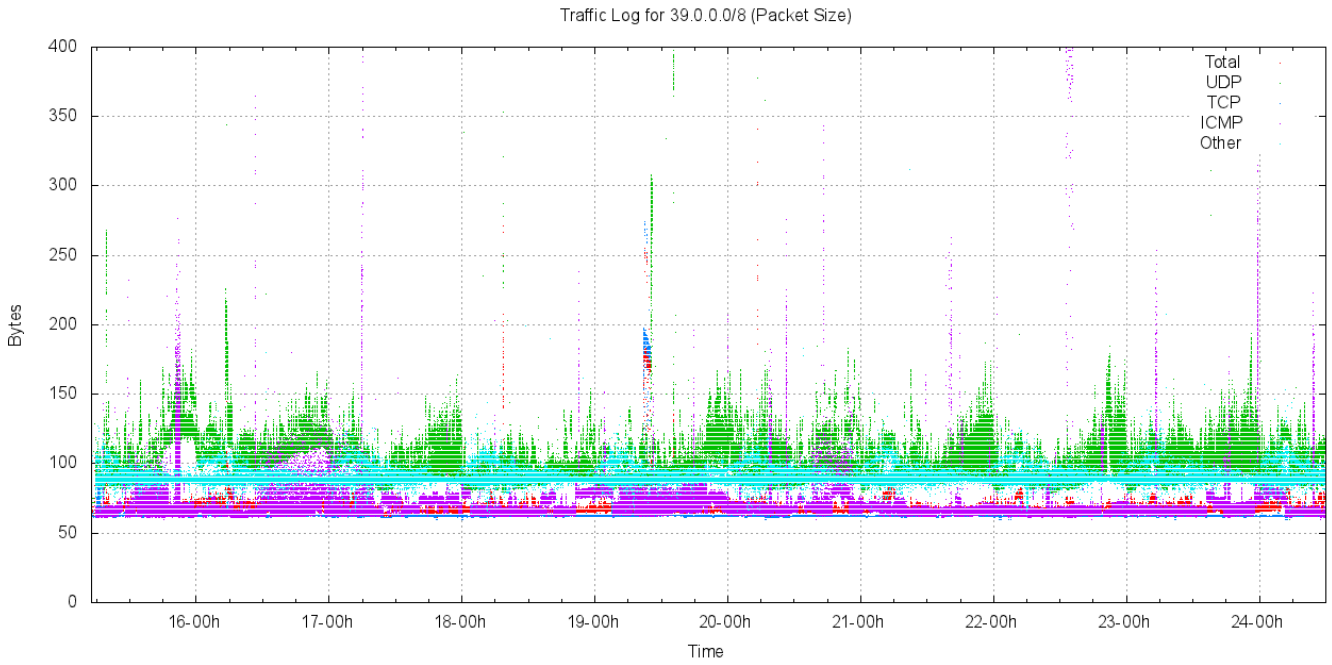


Figure 3 – Packet size distribution for 106.0.0.0/8

Of note in the data collected is the ICMP and "other protocol" extended bursts of larger packet sizes.

Distribution of Traffic Across /16s

The following figure shows the distribution of traffic across the /8 address block, divided up into each of the 256 /16 address blocks. Figure 4 shows this distribution for 106.0.0.0/8.

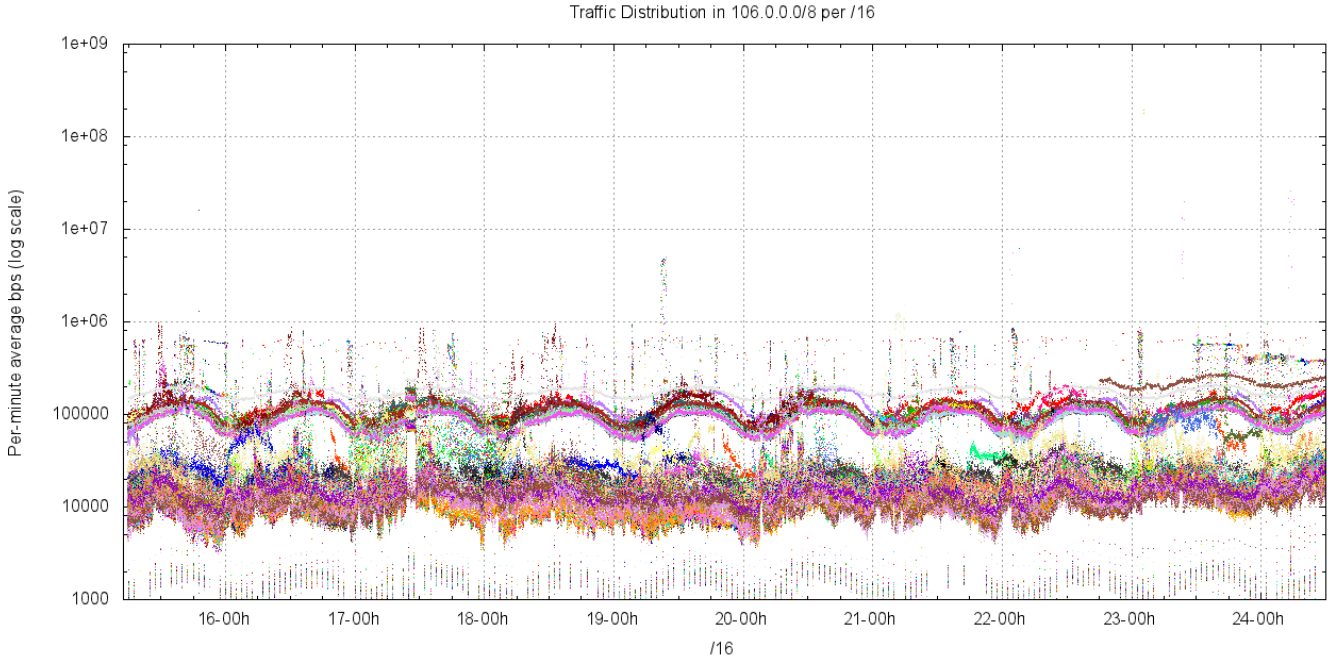


Figure 4 – Traffic distribution per /16 for 106.0.0.0/8

In almost all cases the level of incoming traffic lies between 5Kbps to 200Kbps, with a visible diurnal component. There is a clear "banding" into two traffic profiles: the low /9 exhibits an average traffic level of some 110Kbps per /16, while the high /9 exhibits an average traffic level of 15kbps, consistent with the scanning behaviour of the *conficker* virus, as seen in other /8s tested in 2010 by APNIC.

The distribution of average traffic levels for each of the /16s in net 106.0.0.0/8 is shown in the following figure.

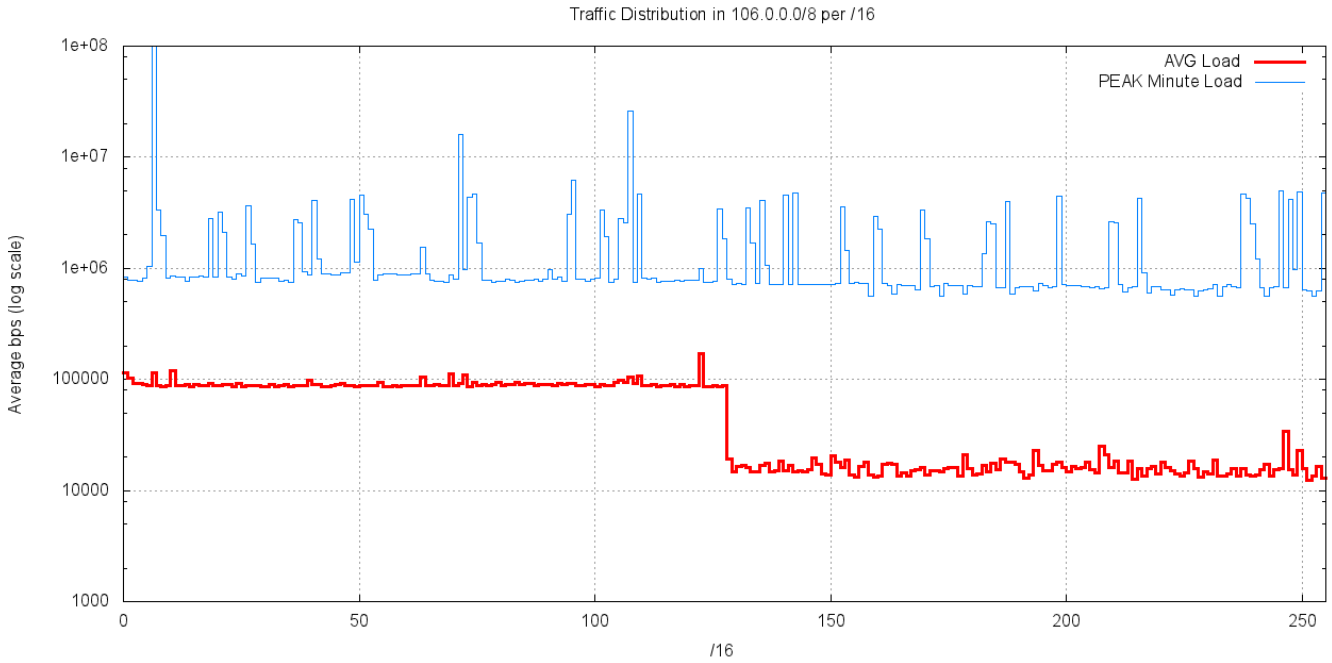


Figure 5 – Average Traffic load per /16 for 106.0.0.0/8

This data collection shows a pronounced break in the "middle" of the address block. The low half of the address block (106.0.0.0/9) has an average traffic load of 100Kbps per /16, while the upper half of the block (106.128.0.0/9) has an average traffic load of 20Kbps.

Distribution of Traffic

The following figure shows the distribution of traffic levels per /24 in network 106.0.0.0/8.

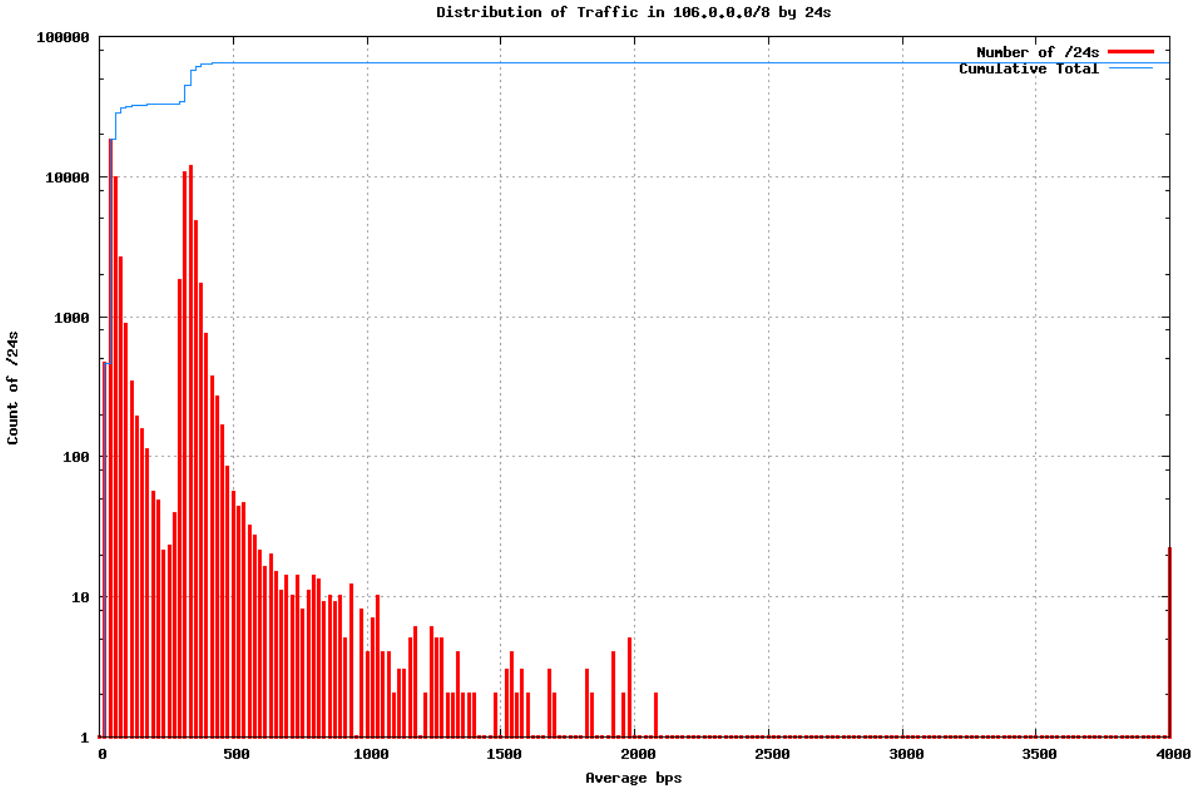


Figure 6 – Traffic profile for 106.0.0.0/8 by /24s

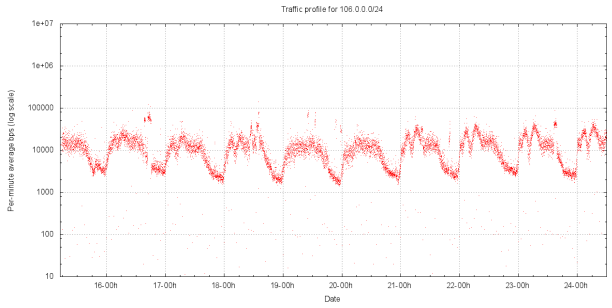
The second peak in this distribution at 400bps per /24 is due to *conficker* scanning across the low /9 of the address block. It appears that the *conficker* scanning traffic element is common across the entire IPv4 address range, and this additional traffic component directed to TCP port 445 in the low /9 of this two address block is not an anomaly that warrants any particular action in terms of reservation of addresses from allocations or assignments.

Using a threshold value of a average incoming traffic rate of more than 10Kbps per /24, corresponding to 40 bits per second per address, or approximately 1 packet on average every 20 seconds per address, then the following /24s in 106.0.0.0/8 that exceed this level of traffic.

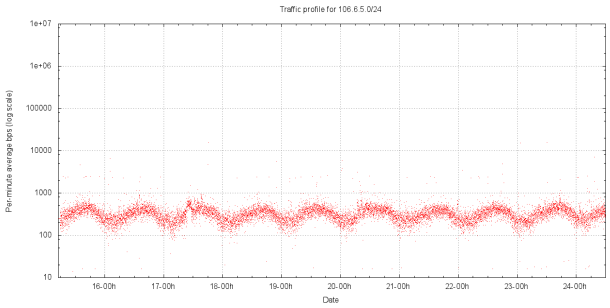
/24 Prefix	Avg Traffic Level
106.0.0.0/24	12.5 kbps
106.6.5.0/24	28.1 kbps
106.10.1.0/24	30.6 kbps
106.63.99.0/24	20.0 kbps
106.69.121.0/24	24.9 kbps
106.72.154.0/24	21.6 kbps
106.105.190.0/24	10.0 kbps
106.107.1.0/24	19.3 kbps
106.122.237.0/24	85.7 kbps
106.246.105.0/24	17.8 kbps

Table 3 – Traffic profile for highest traffic /24s in 106.0.0.0/8

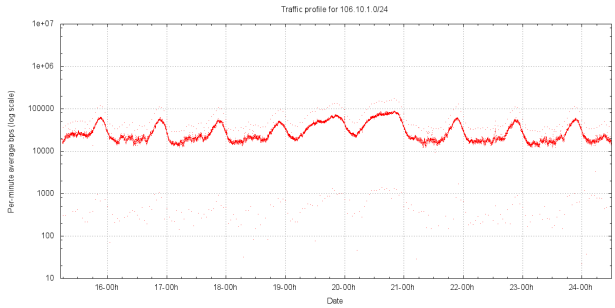
The traffic profile for each of these /24s is show in the following figures



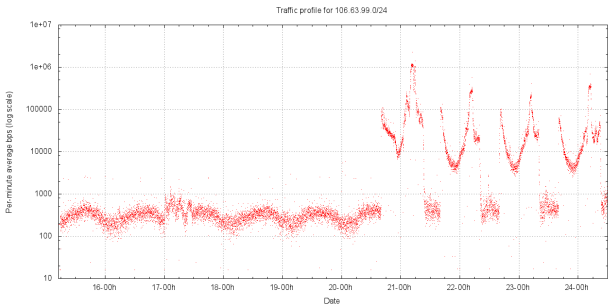
106.0.0.0/24



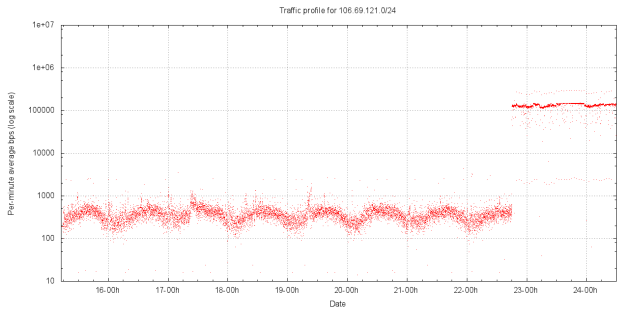
106.6.5.0/24



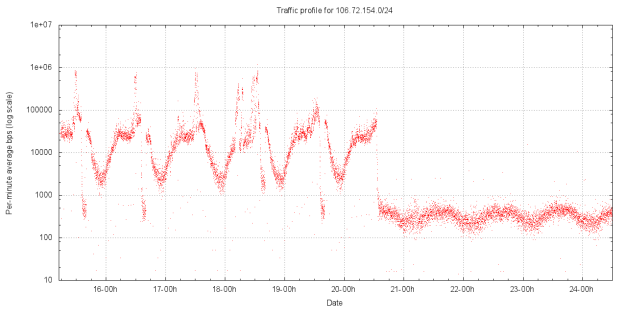
106.10.1.0/24



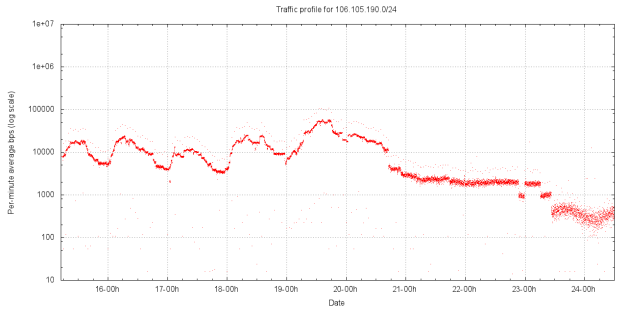
106.63.99.0/24



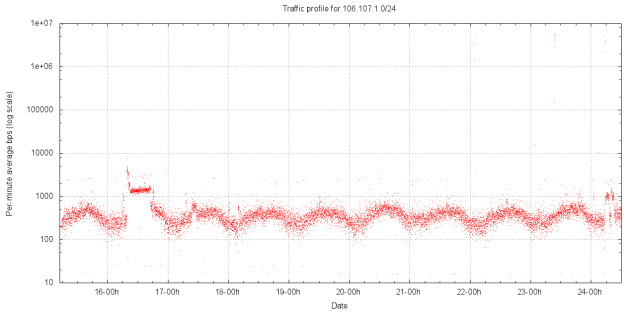
106.69.121.0/24



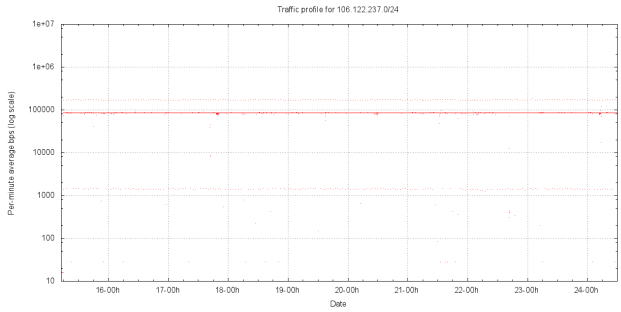
106.72.154.0/24



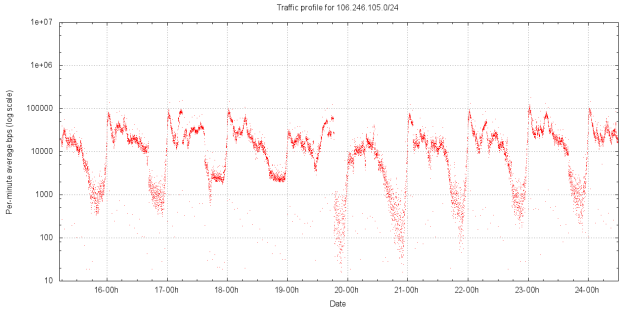
106.105.190.0/24



106.107.1.0/24



106.122.237.0/24



106.246.105.0/24

Conclusions

It is recommended that /24 prefixes listed below be withheld from regular allocation or assignment from 106.0.0.0/8 for a period of 3 months, allowing a second round of testing of these particular prefixes at that time.

106.10.1.0/24

The traffic directed at 106.10.1.0/24 is predominately directed to the two addresses: 106.10.1.180, UDP port 15035 and 106.10.1.229, UDP port 15001. The traffic comes from various source addresses

106.122.237.0/24

The traffic directed at 106.122.237.0/24 is predominately directed to the single address 106.122.237.61, and is sourced from a single IP address.

106.246.105.0/24

The traffic directed at 106.122.237.0/24 is predominately UDP traffic directed to the single address 106.246.105.113. The UDP ports, both in source and destination, are varied, as are the source addresses sending this traffic. The UDP payload is constant across both the ports used and the source addresses.