Background Traffic to Network 39.0.0.0/8

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 39.0.0.0/8.

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 39.0.0.0/8 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 39.0.0.0/8.

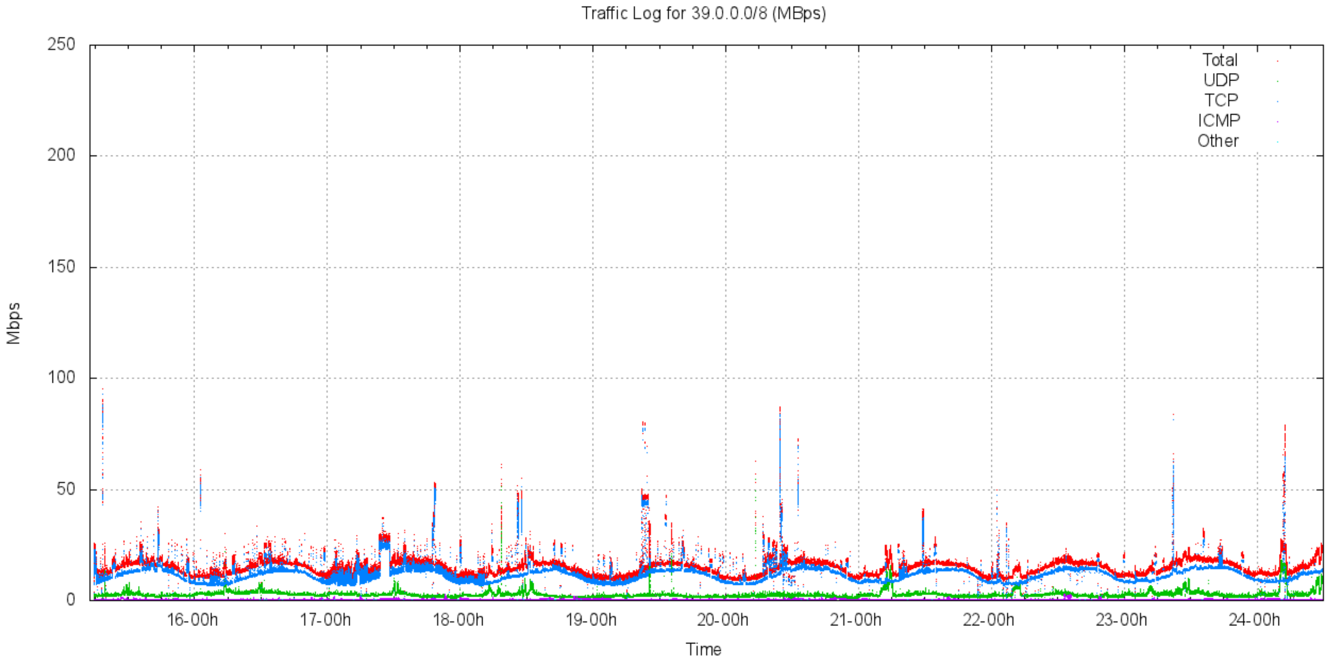


Figure 1 – Traffic profile for 39.0.0.0/8

(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 39.0.0.0/8 attracts some 12 – 25Mbps of incoming traffic. Of this, some 83% of the traffic is TCP and 15% 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.

Protocol	Proportion of Traffic					
	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	78.7%	82.8%	76.0%	81.5%	66.2%	71.4%
UDP	18.0%	14.5%	22.7%	17.4%	25.6%	27.6%
ICMP	2.5%	2.0%	0.9%	1.1%	8.0%	0.9%
Other	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.

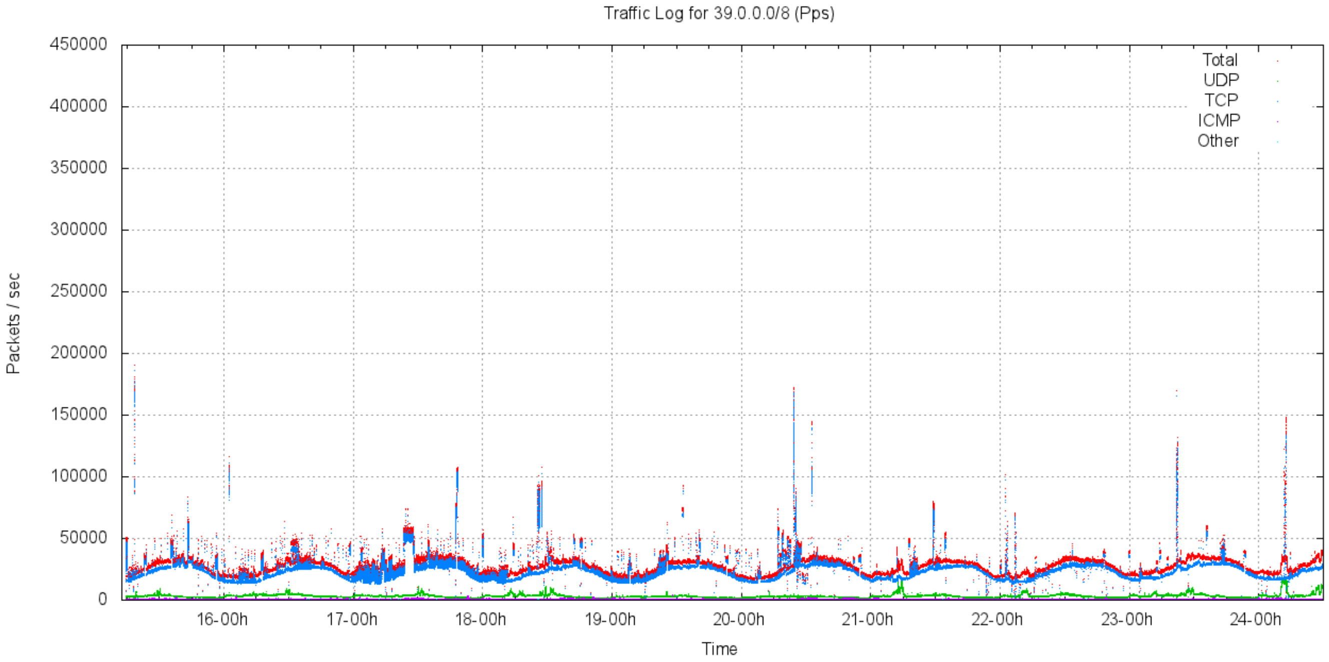


Figure 2 – Packet profile for 39.0.0.0/8

The 39.0.0.0/8 network block attracts between 25,000 and 45,000 packets per second, where 87% of the incoming packets are TCP, between 14.2% are UDP, 6.1% are ICMP and the remaining packets represent 4.6% of the total.

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 49/8, 14/8 and 223/8 for comparison.

Protocol	Proportion of Packets					
	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	84.5%	88.4%	83.1%	86.9%	50.0%	50.0%
UDP	12.1%	9.2%	16.1%	14.2%	36.5%	35.7%
ICMP	2.4%	1.7%	0.7%	6.1%	9.9%	13.9%
Other	0.5%		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 (16,098M of the 18,654M TCP packets (87%) were TCP SYN packets).

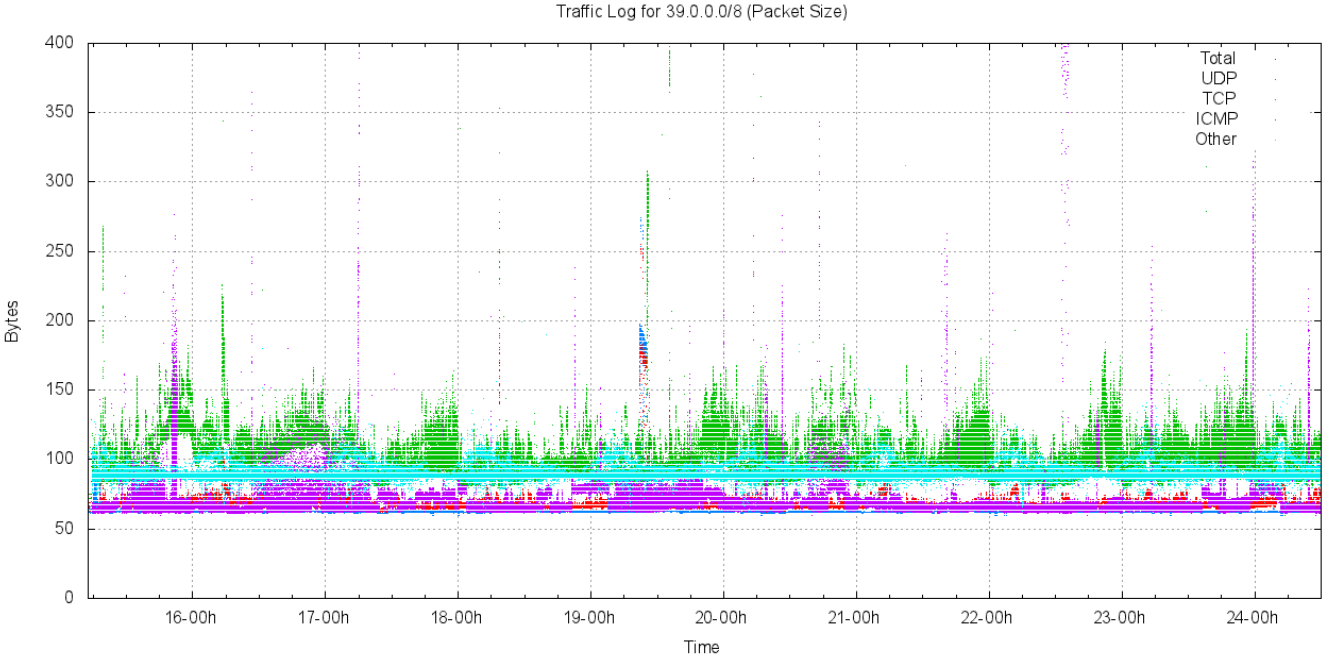


Figure 3 – Packet size distribution for 39.0.0.0/8

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 39.0.0.0/8.

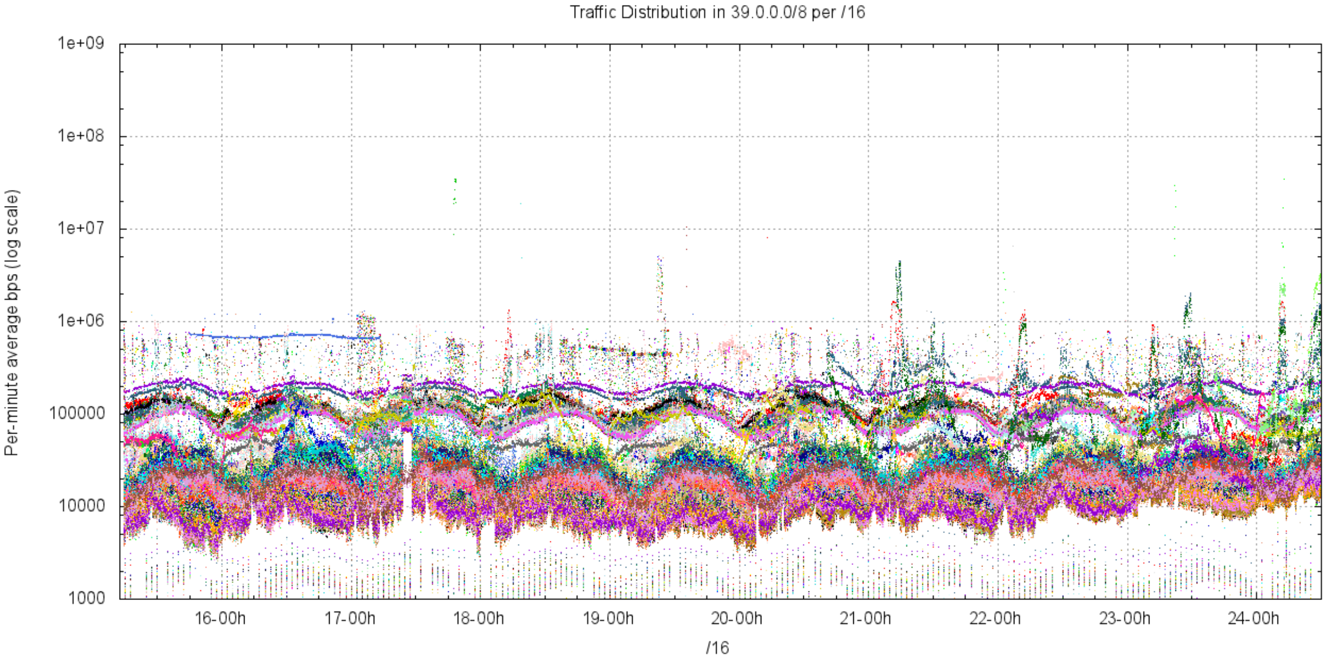


Figure 4 – Traffic distribution per /16 for 39.0.0.0/8

In almost all cases the level of incoming traffic lies between 5Kbps to 200Kbps, with a visible diurnal component. There is a "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 39.0.0.0/8 is shown in the following figure.

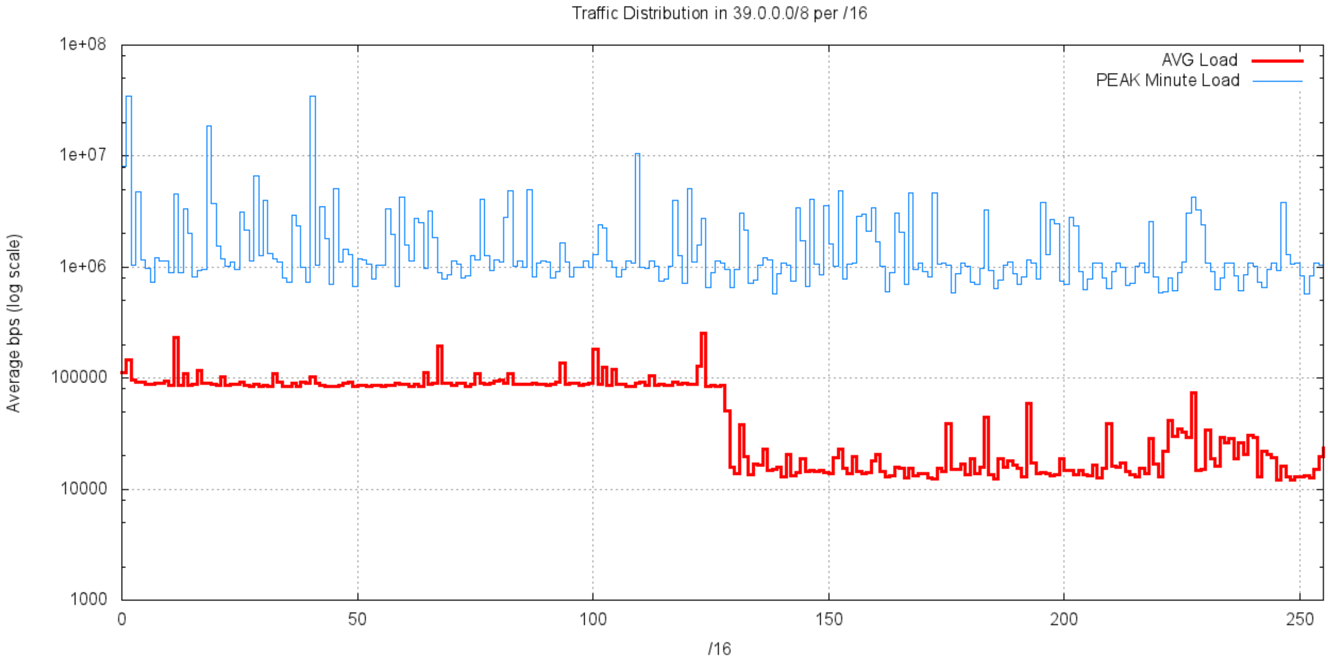


Figure 5 – Average Traffic load per /16 for 39.0.0.0/8

This data collection shows a pronounced break in the "middle" of the address block. The low half of the address block (39.0.0.0/9) has an average traffic load of 100Kbps per /16, while the upper half of the block (39.128.0.0/9) has an average traffic load of 20Kbps.

Distribution of Traffic

The following figure shows the distribution of traffic levels per /24 in network 39.0.0.0/8.

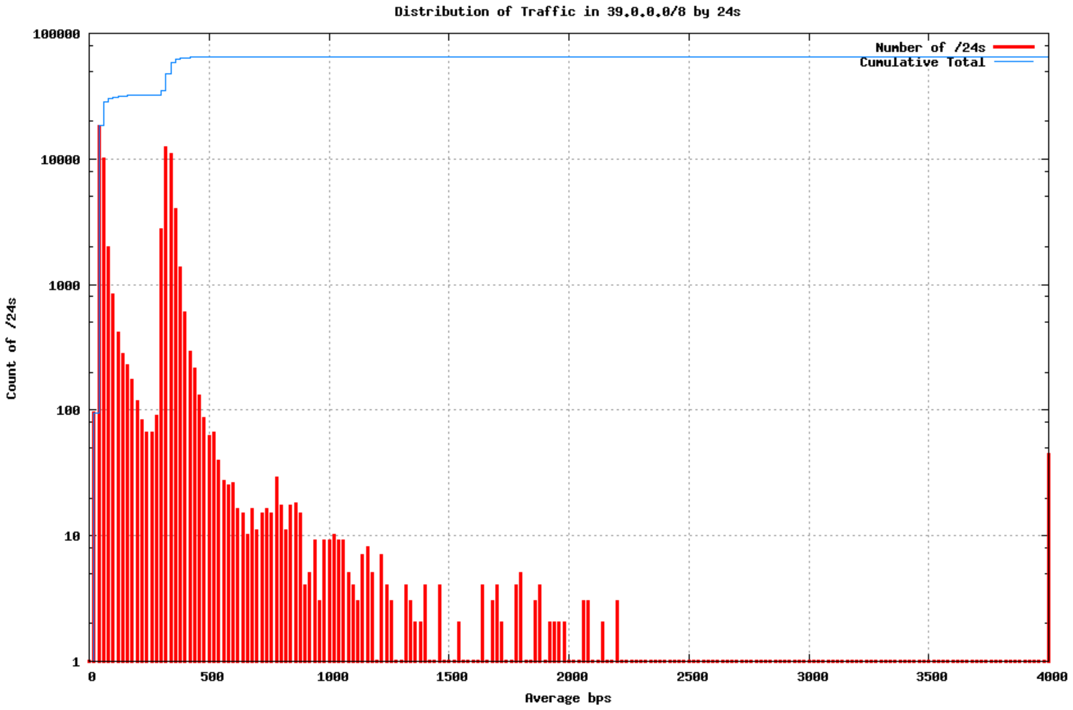


Figure 6 – Traffic profile for 39.0.0.0/8 by /24s

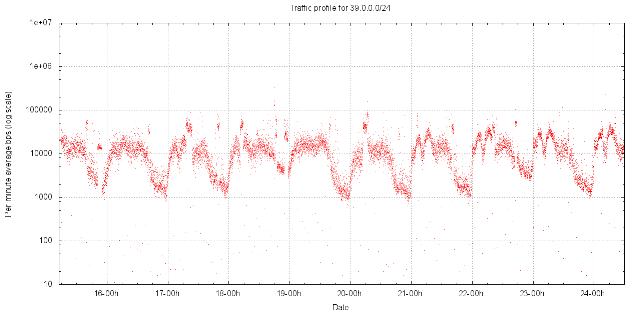
The second peak in this distribution at 400bps per /24 is due to *conficker* scanning across the low /9 of the address block. It appears that the *conficker* scanning traffic element is common across the entire IPv4 address range, and this additional traffic component directed to TCP port 445 in the 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 there are 5 /24s in 39.0.0.0/8 that exceed this level of traffic.

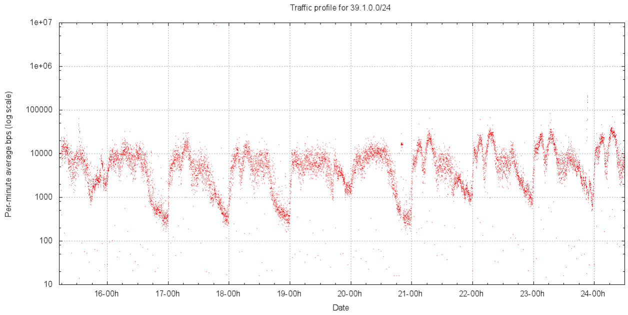
/24 Prefix	Avg Traffic Level
39.0.0.0/24	13.3 kbps
39.1.0.0/24	55.7 kbps
39.11.110.0/24	85.7 kbps
39.11.160.0/24	60.6 kbps
39.13.229.0/24	26.7 kbps
39.16.232.0/24	16.9 kbps
39.21.82.0/24	11.8 kbps
39.32.231.0/24	17.2 kbps
39.40.1.0/24	14.6 kbps
39.64.234.0/24	16.9 kbps
39.67.24.0/24	108.0 kbps
39.75.12.0/24	21.9 kbps
39.82.135.0/24	11.2 kbps
39.93.118.0/24	46.4 kbps
39.100.5.0/24	97.4 kbps
39.102.221.0/24	34.6 kbps
39.104.19.0/24	34.7 kbps
39.112.233.0/24	13.9 kbps
39.122.91.0/24	44.7 kbps
39.123.0.0/24	154.4 kbps
39.123.218.0/24	16.6 kbps
39.128.71.0/24	22.5 kbps
39.131.254.0/24	21.7 kbps
39.175.16.0/24	25.0 kbps
39.183.40.0/24	32.5 kbps
39.192.231.0/24	18.1 kbps
39.192.235.0/24	16.9 kbps
39.209.31.0/24	26.0 kbps
39.218.182.0/24	16.1 kbps
39.227.235.0/24	58.9 kbps

Table 3 – Traffic profile for highest traffic /24s in 39.0.0.0/8

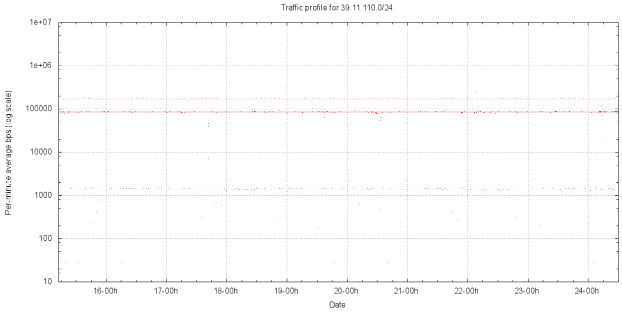
The traffic profile for each of these /24s is show in the following figures



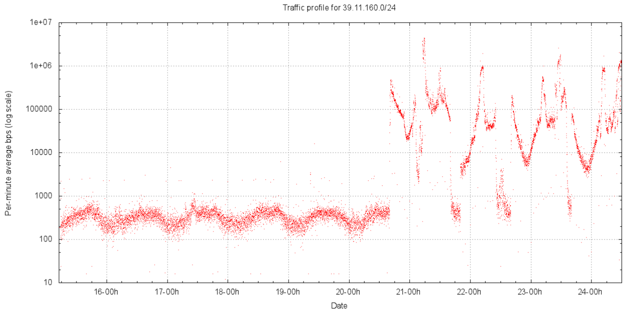
39.0.0.0/24



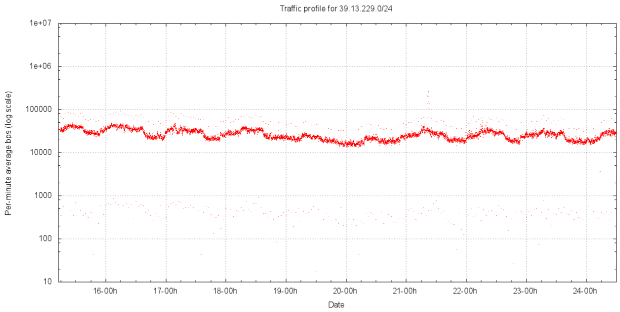
39.1.0.0/24



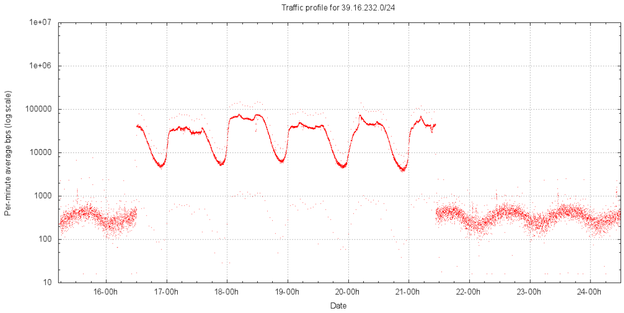
39.11.110.0/24



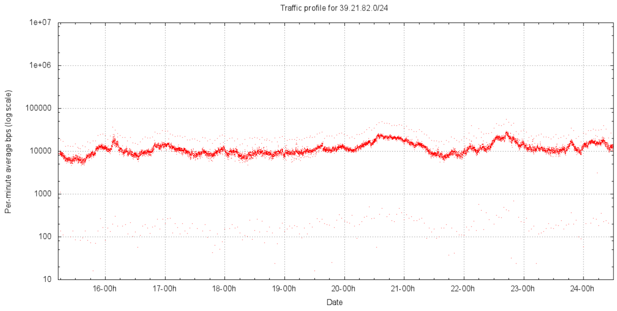
39.11.160.0/24



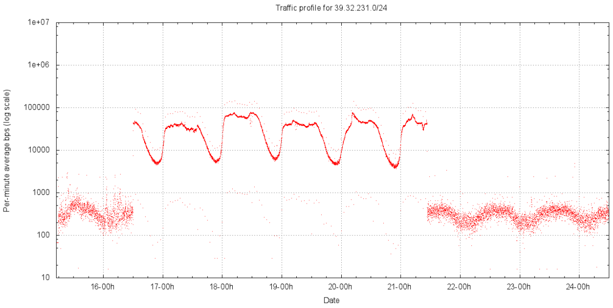
39.13.229.0/24



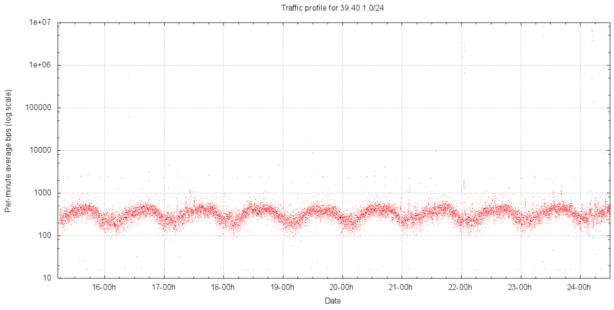
39.16.232.0/24



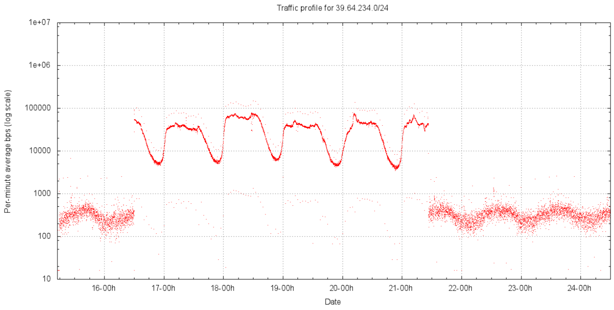
39.21.82.0/24



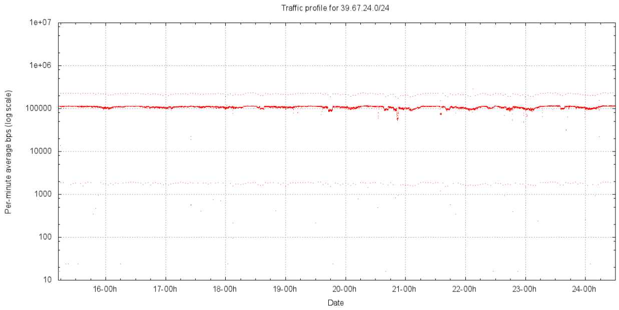
39.32.231.0/24



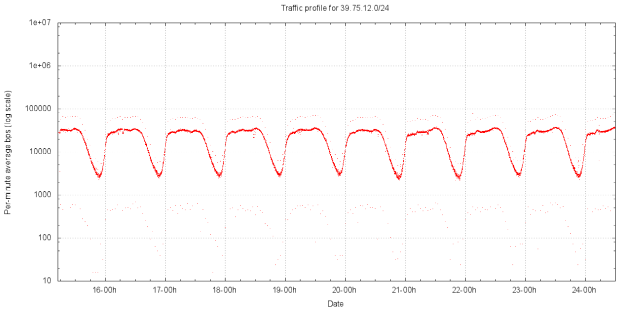
39.40.1.0/24



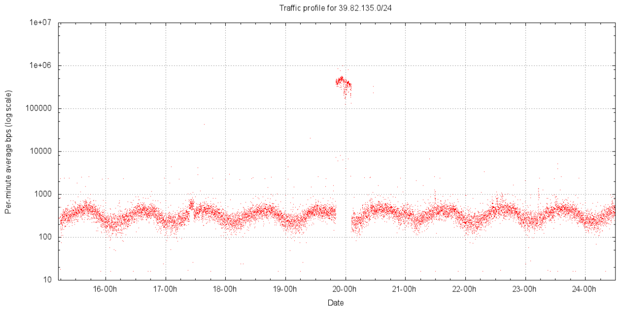
39.64.234.0/24



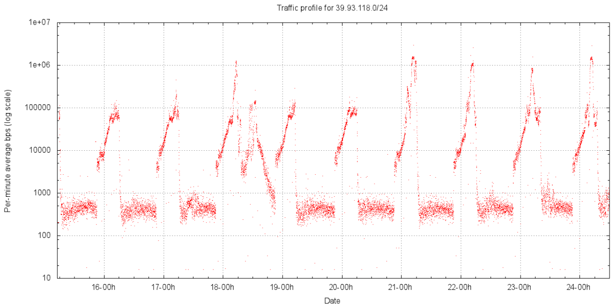
39.67.24.0/24



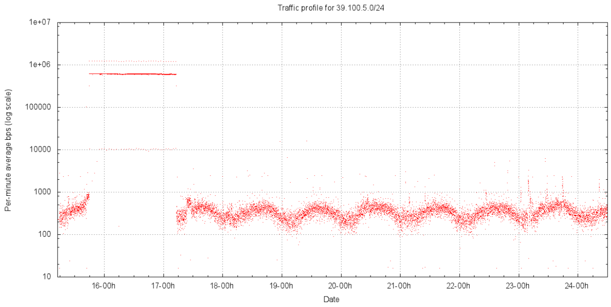
39.75.12.0/24



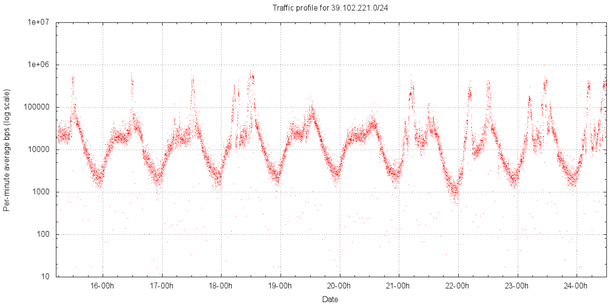
39.82.135.0/24



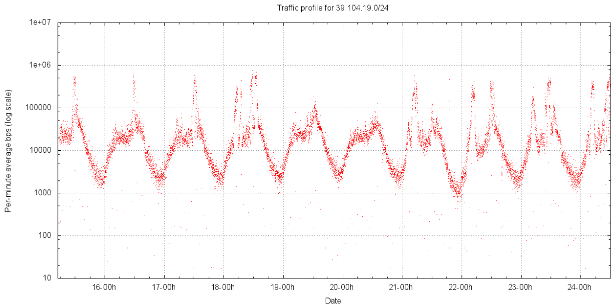
39.93.118.0/24



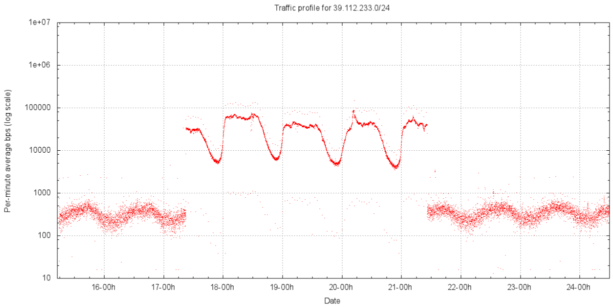
39.100.5.0/24



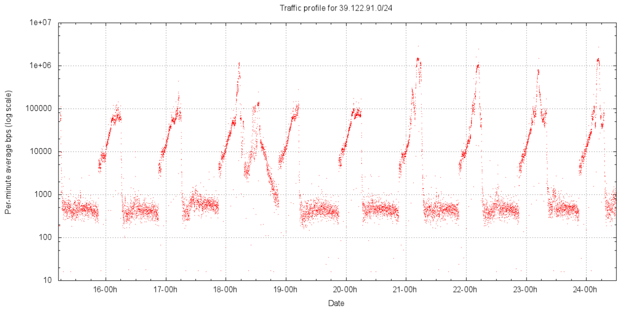
39.102.221.0/24



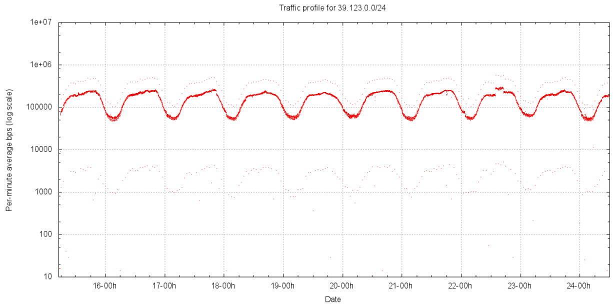
39.104.19.0/24



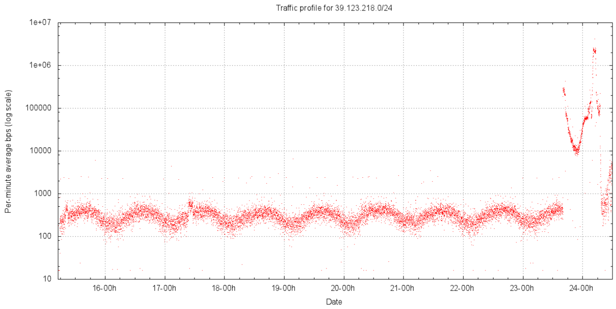
39.112.233.0/24



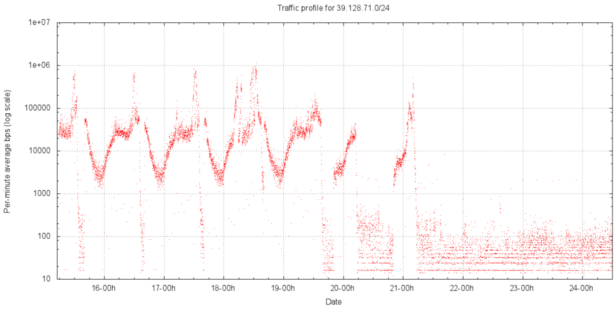
39.122.91.0/24



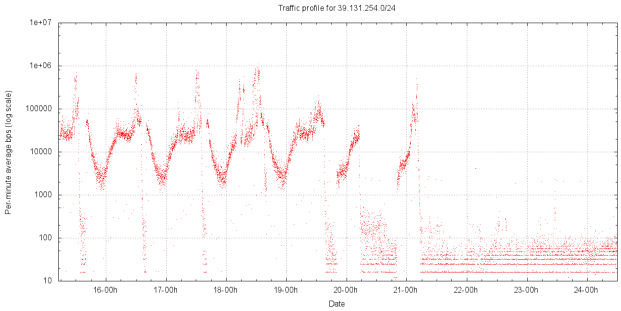
39.123.0.0/24



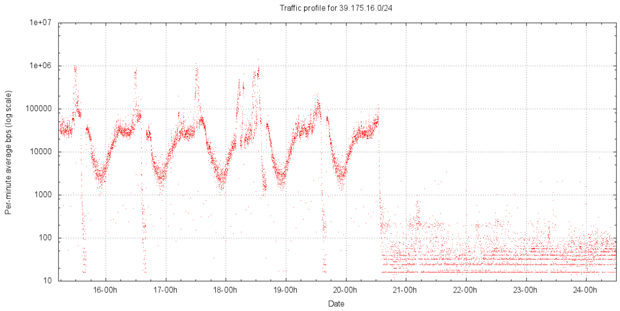
39.123.218.0/24



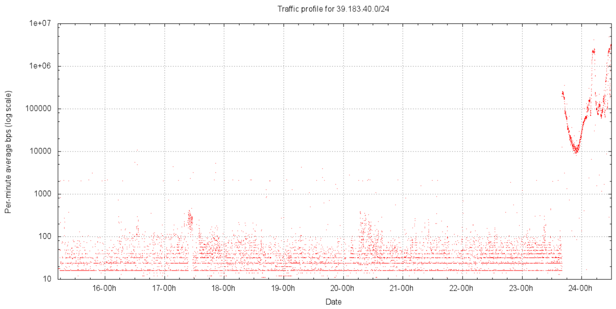
39.128.71.0/24



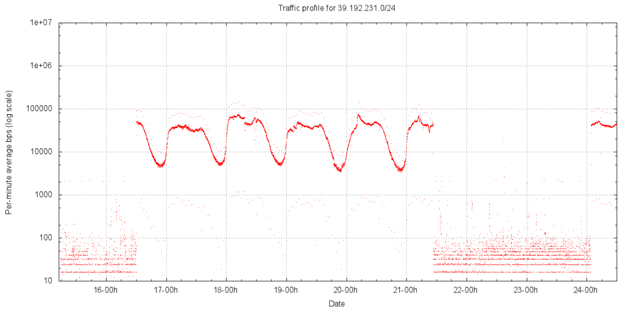
39.131.254.0/24



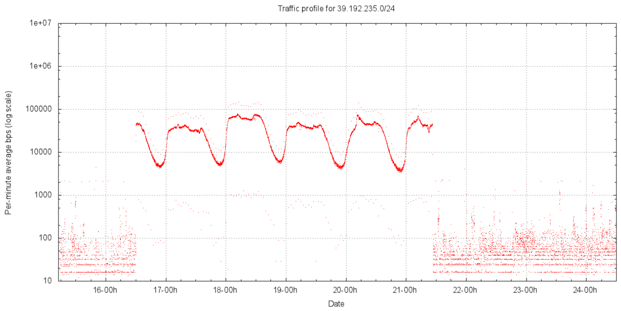
39.175.16.0/24



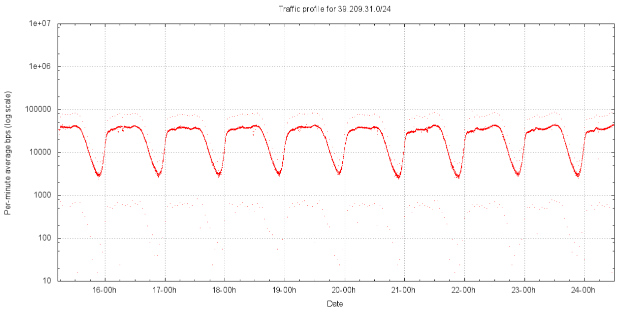
39.183.40.0/24



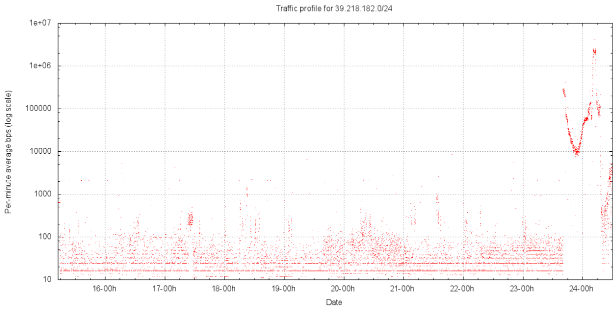
39.192.231.0/24



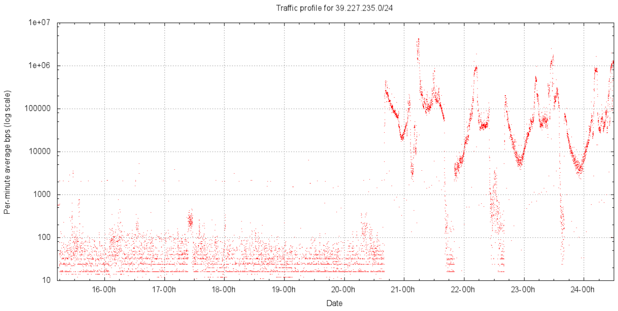
39.192.235.0/24



39.209.31.0/24



39.218.182.0/24



39.227.235.0/24

As can be seen from these traces, not all prefixes see a sustained load pattern, and where the incoming traffic is intermittent, it is likely that the traffic is the product of a form of address scanning that "walks" through the address space, and that a scan of traffic at another date would see a different result.

Conclusions

It is recommended that /24 prefixes listed below be withheld from regular allocation or assignment from 39.0.0.0/8 for a period of 3 months, allowing a second round of testing of these particular prefixes at that time.

39.11.110.0/24
The traffic is a single UDP stream from 222.99.116.11 directed to 39.11.110.108

39.13.229.0/24
This traffic is all DNS traffic, directed to 39.13.229.241. The source addresses are varied, and the DNS queries are varied, so this address is possibly being used in the context of a bogus root server, or a DNS forwarder.

39.67.24.0/24
This is a single traffic stream directed to the single address 39.67.24.0, TCP port 80, incoming SYNs. The source address is 72.45.1.117, source port 4976, sending at a rate of some 200 TCP SYN packets per second.

39.75.12.0/24
This is UDP traffic, directed to the single address 39.75.12.77, UDP port 57607. There are a large number of source addresses involved. Each unique source appears to send a single packet.

39.93.118.0/24
This is UDP traffic, directed to the single address 39.93.118.247, UDP port 6861. There are a number of source addresses involved. All the UDP packets are identical in format with one byte value varying.

39.102.221.0/24
This is UDP traffic, directed to the single address 39.102.221.38, UDP port 15100. The traffic is in all other respects the same as is being directed to 39.93.118.247.

39.104.19.0/24
This is UDP traffic, directed to the single address 39.104.19.193, UDP port 32416. The traffic is in all other respects the same as is being directed to 39.93.118.247.

39.122.91.0/24
This is UDP traffic, directed to the single address 39.122.91.182, UDP port 32721. The traffic is in all other respects the same as is being directed to 39.93.118.247.

39.123.0.0/24
This is UDP traffic, directed to 39.123.0.0, UDP port 137 (NETBIOS name service). It is possible that this is an address that is configured as a secondary WINS server in some DSL modem equipment configurations (this appears to relate some versions of the ZyXEL DSL modem software)

39.209.31.0/24
This is UDP traffic, directed to 39.209.31.159, UDP port 56541, all with a UDP payload of length 2 bytes. This is identical to the traffic that is being directed to 39.75.12.77.