Background Traffic to Unallocated Various Network Blocks administered by APNIC

March 2011

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 various network blocks that are now being administered by APNIC. These various networks blocks were part of the old "class B" network space under the previous Class-based address architecture. The complete list of these network blocks is provided in Appendix A of this report.

APNIC expresses its appreciation for the generous assistance provided by NTT Communications in undertaking this experiment.

Experiment Details

In collaboration with APNIC, AS38639 (NTT Communications) exclusively announced the set of /16s listed in Appendix A for the period from 3 February 2011 until 9 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 the aggregate of all these network blocks.

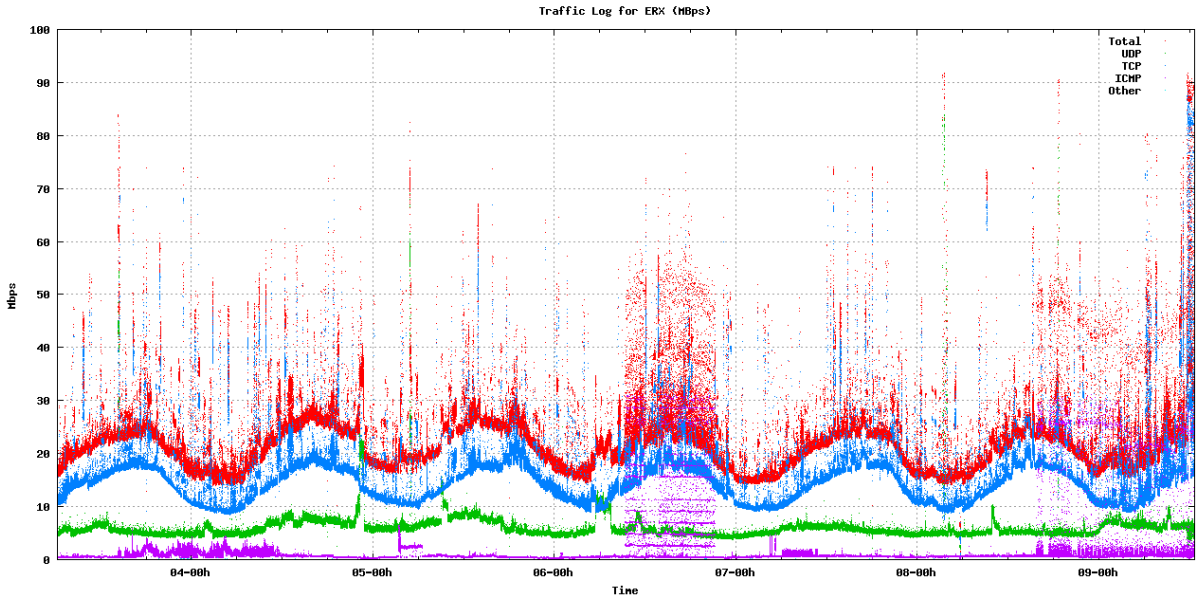


Figure 1 – Traffic profile for ERX network blocks

This traffic profile is similar to the profile that was recorded for other /8 address blocks recently allocated to APNIC. Of this traffic, some 80% of the traffic is TCP and 18% 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 42.0.0.0/8, 36.0.0.0/8,101.0.0.0/8, 49.0.0.0/8, 14.0.0.0/8 and 223.0.0.0/8.

Protocol	ERX	42.0.0.0.8	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	**68.9%**	79.7%	82.8%	76.0%	81.5%	66.2%	71.4%
UDP	**27.2%**	18.3%	14.5%	22.7%	17.4%	25.6%	27.6%
ICMP	**3.8%**	1.7%	2.0%	0.9%	1.1%	8.0%	0.9%
Other	**0.0%**	0.3%	0.7%	0.4%	0.0%	0.2%	0.1%

Table 1. Distribution of Traffic by Protocol

Distribution of Traffic Across /16s

The following figure shows the distribution of traffic across the /8 address block, divided up into each of the 392 /16 address blocks. Figure 4 shows this distribution for this set of /16s

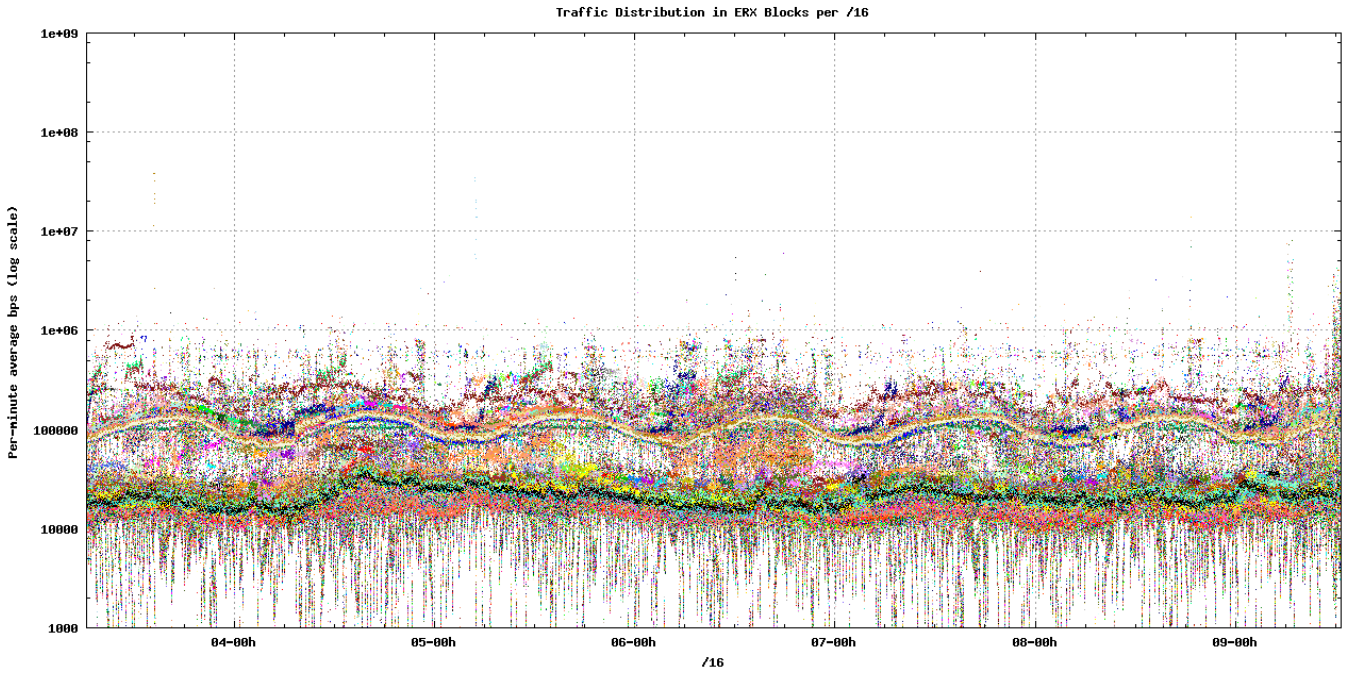


Figure 2 – Traffic distribution per /16 for ERX blocks

In almost all cases the level of incoming traffic lies between 10Kbps to 200Kbps, with a visible diurnal component. There is a "banding" into two traffic profiles: the low /9 of each /8 exhibits an average traffic level of some 110Kbps per /16, while the high /9 of each /8 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, which appears to limit itself to sending TCP SYN packets to addresses in the low /9 of each /8

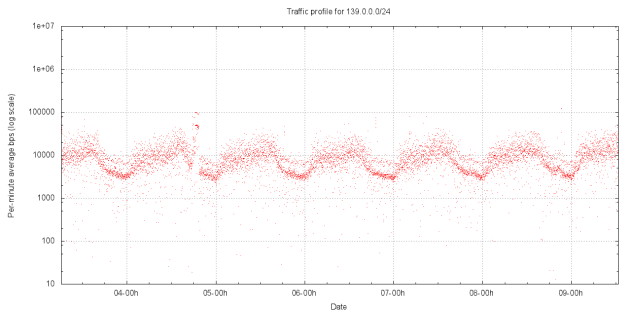
"Busy" networks

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 24 /24s in these address blocks that exceed this level of traffic.

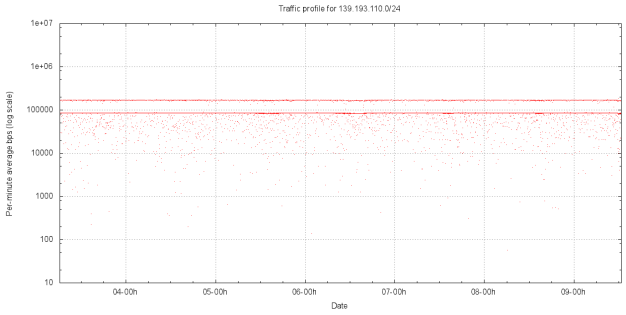
Prefix	Average Traffic
139.0.0.0/24	10 Kbps
139.193.110.0/24	91 Kbps
139.228.153.0/24	167 Kbps
139.255.238.0/24	15 Kbps
139.255.255.0/25	10 Kbps
140.0.0.0/24	15 Kbps
144.0.0.0/24	10 Kbps
144.0.240.0/24	25 Kbps
150.0.0.0/24	27 Kbps
150.0.1.0/24	38 Kbps
150.0.5.0/24	11 Kbps
150.0.11.0/24	8 Kbps
150.139.169.0/24	31 Kbps
153.0.88.0/24	16 Kbps
153.130.184.0/24	92 Kbps
157.0.0.0/24	8 Kbps
157.0.108.0/24	41 Kbps
163.0.0.0/24	10 Kbps
163.125.159.0/24	27 Kbps
163.222.55.0/24	14 Kbps
171.0.0.0/24	14 Kbps
171.3.19.0/24	25 Kbps
171.41.122.0/24	10 Kbps
171.80.59.0/24	38 Kbps
171.112.109.0/24	18 Kbps

Table 3 – Traffic profile for high traffic /24s in the ERX blocks

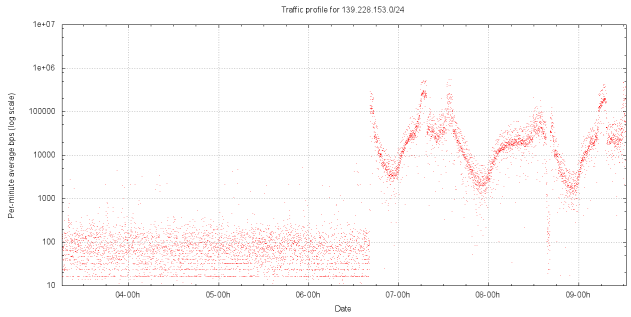
The traffic profile for each of these /24s is shown in the following figures.



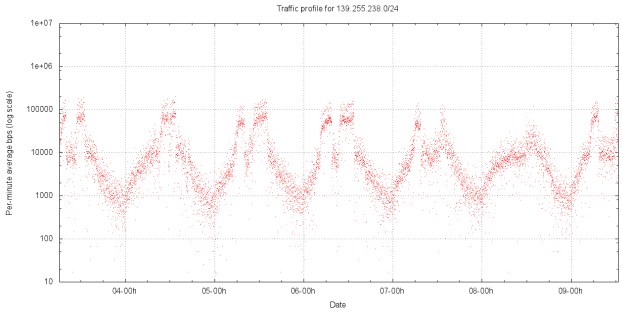
139.0.0.0/24



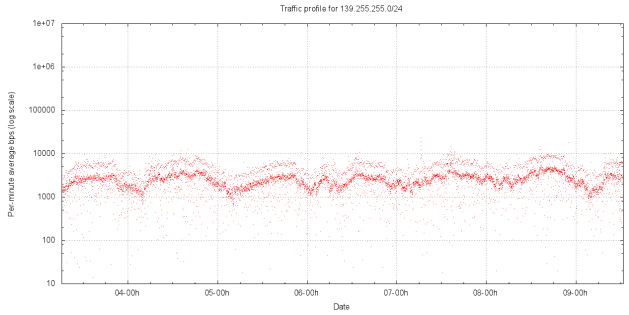
139.193.110.0/24



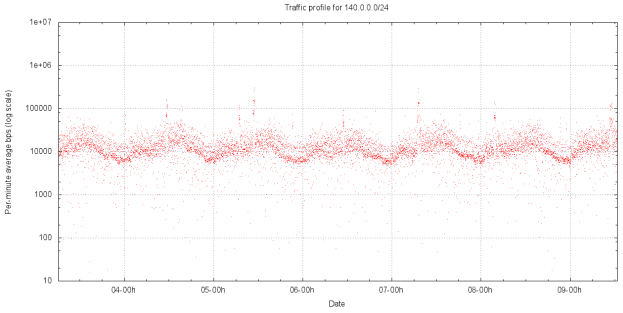
139.228.153.0/24



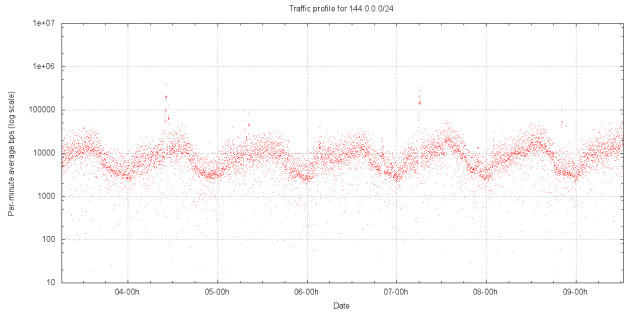
139.255.238.0/24



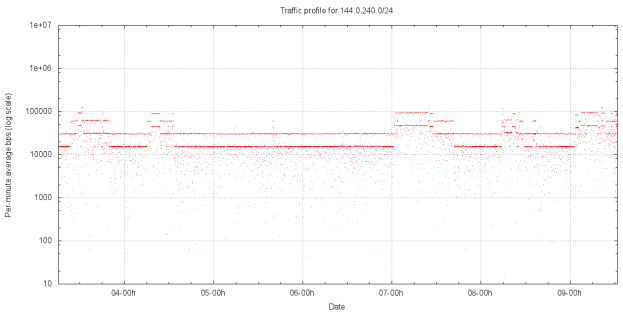
139.255.255.0/24



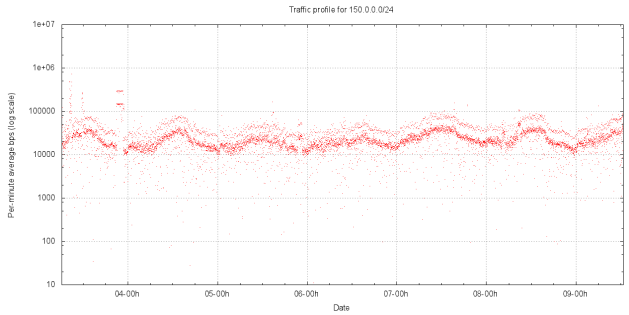
140.0.0.0/24



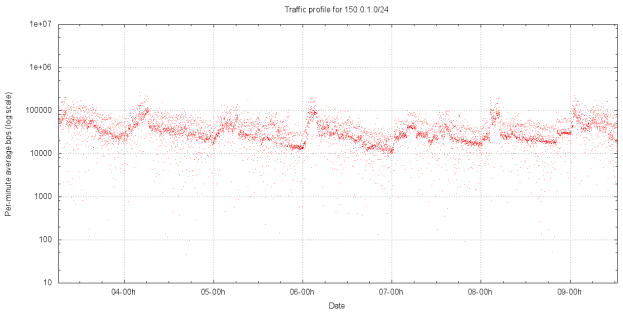
144.0.0.0/24



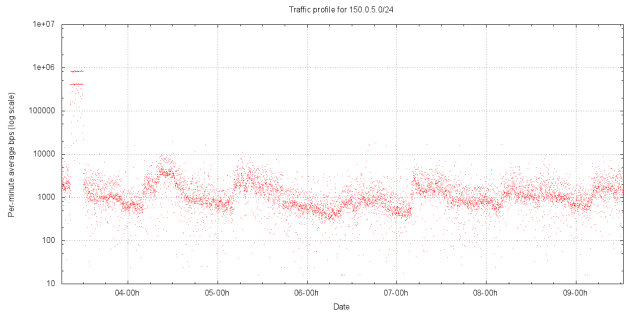
144.0.240.0/24



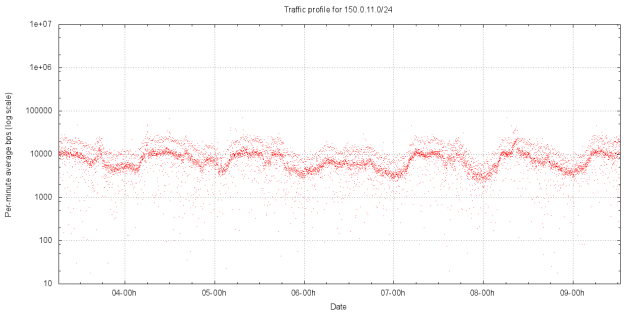
150.0.0.0/24



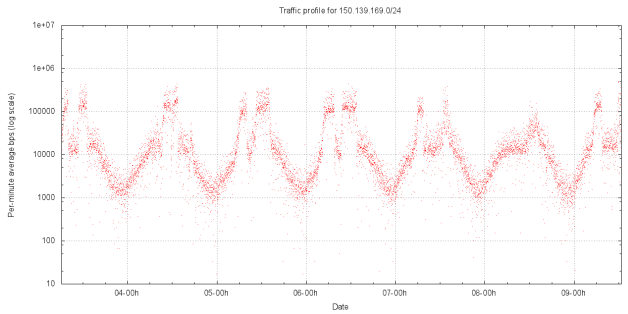
150.0.1.0/24



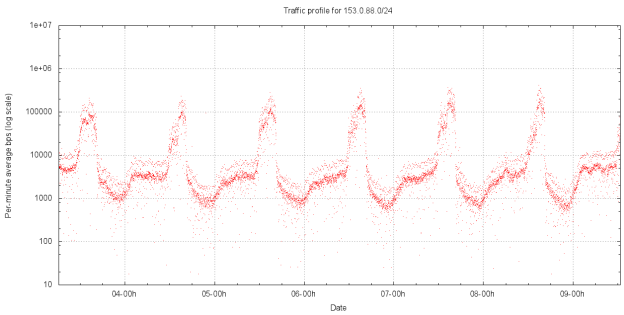
150.0.5.0/24



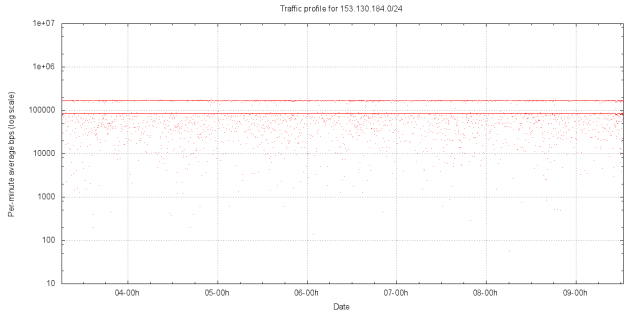
150.0.11.0/24



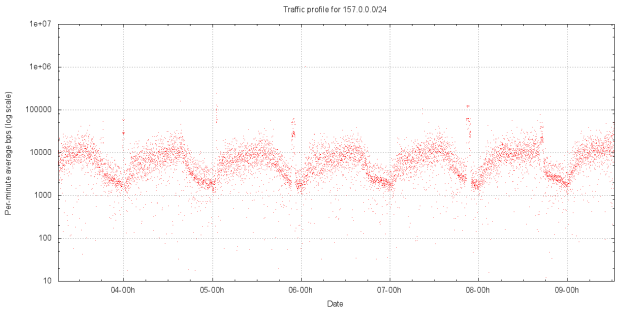
150.139.169.0/24



153.0.88.0/24

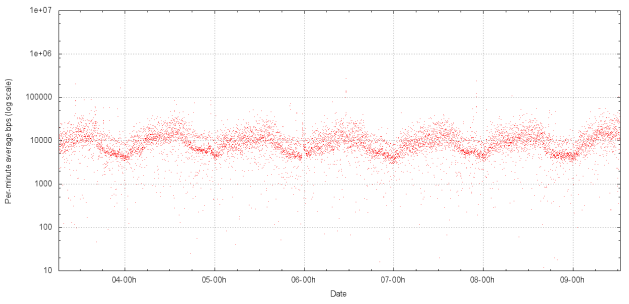


153.130.184.0/24

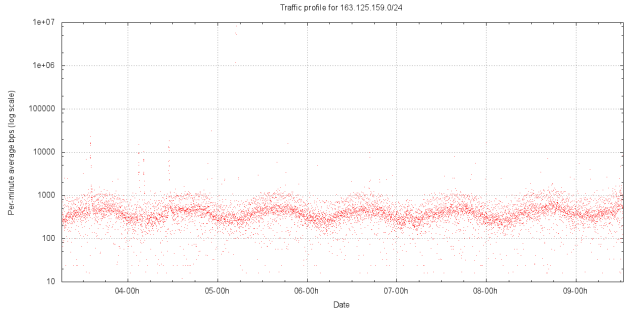


157.0.0.0/24

157.0.108.0/24

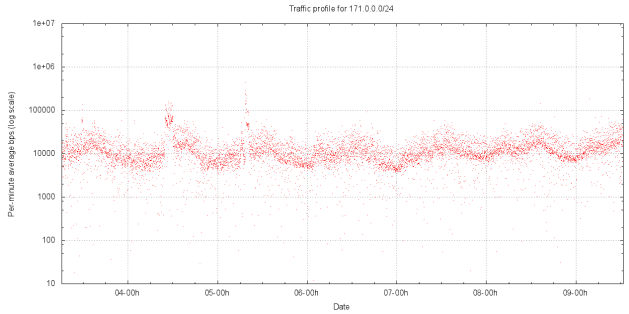


163.0.0.0/24

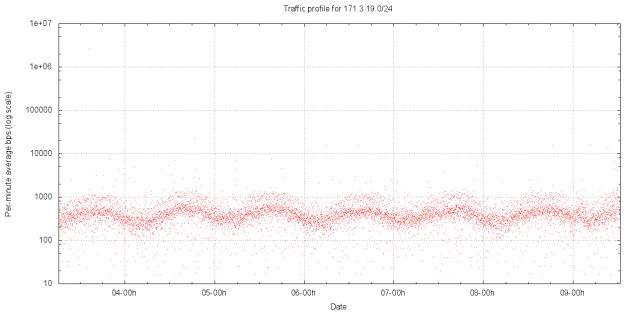


163.125.159.0/24

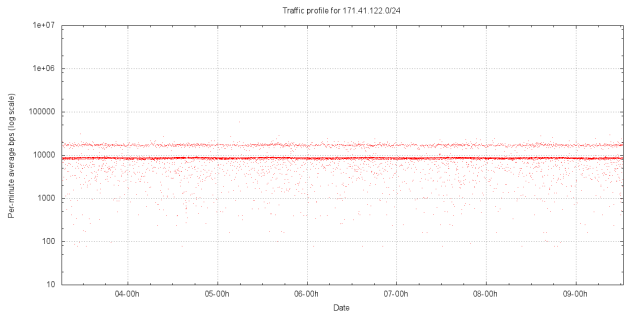
163.222.55.0/24



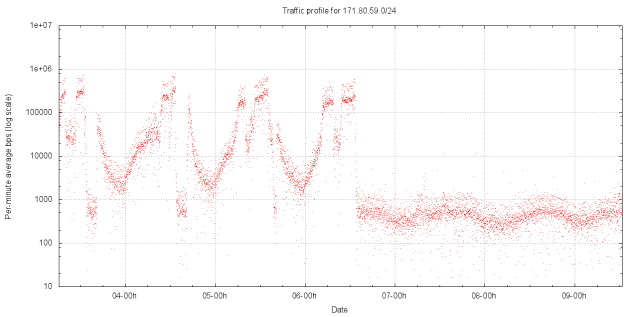
171.0.0.0/24



171.3.19.0/24



171.41.122.0/24



171.80.59.0/24

171.112.109.0/24

The network 139.0.0.0/24 does not appear to attract significantly higher levels of incoming traffic as compared to other /24 networks, and there is insufficient grounds to recommend quarantining of this network.

Similarly, the network 139.255.255.0/24 appears to have a traffic profile that is not overly different to other adjacent networks, and given that the traffic profile is generally below 10Kbps for the period, there is insufficient grounds to recommend quarantining of this network.

Network 144.0.0.0/24 shows only intermittent bursts of incoming traffic, and therefore is not a candidate network for quarantining.

Network 150.0.5.0/24 is marginal in terms of potential quarantine actions. There is one significant traffic flow detected in this network block, from source 198.203.136.248 UDP port 14000 to 150.0.5.2, UDP port 5000. Given that the traffic profile is generally below 10Kbps for the period, there is insufficient grounds to recommend quarantining of this network.

Network 157.0.108.0/24 shows incoming traffic at excessive levels for the first part of the test period. This traffic was UDP traffic directed to the address 157.0.108.46 from various sources, which abated midway through the test period. There is insufficient grounds to recommend quarantining of this network.

Network 163.125.159.0/24 shows only intermittent bursts of incoming traffic, and therefore is not a candidate network for quarantining.

Network 171.3.19.0/24 shows only intermittent bursts of incoming traffic, and therefore is not a candidate network for quarantining.

Network 171.80.59.0/24 shows incoming traffic at excessive levels for the first part of the test period. This traffic was UDP traffic directed to the address 171.80.59.26 from various sources, which abated midway through the test period. There is insufficient grounds to recommend quarantining of this network.

Conclusions

The following network blocks should be withheld from allocation at present, and rechecked in 3 months time, unless the identified source of the unwanted traffic can be isolated and switched off.

139.193.110.0/24

This is a single UDP stream from 221.153.208.183, UDP port 9018, directed to 39.193.110.179, UDP port 36428, of a sustained rate of some 90Kbps. If this individual address were quarantined, the remained of this network would be useable.

139.228.153.0/24

A large number of sources are sending a 115 octet UDP packet to 139.228.153.109, port 62275. It appears that all the packets have the same 87 octet UDP payload. Aside from this single address, the remainder of the /24 is unremarkable in terms of incoming traffic. If this individual address were quarantined, the remained of this network would be useable.

139.255.238.0/24

A large number of sources are sending a 115 octet UDP packet to 139.255.238.145, port 32164. It appears that all the packets have the same 87 octet UDP payload. Aside from this single address, the remainder of the /24 is unremarkable in terms of incoming traffic. If this individual address were quarantined, the remained of this network would be useable.

140.0.0.0/24

A significant proportion of the traffic into this net is UDP traffic directed to 140.0.0.0, from various sources. If

this individual address were quarantined, the remained of this network would be useable.

144.0.240.0/24

This traffic is directed to the single destination address, 144.0.240.252, UDP port 10000. The traffic is sourced from two addresses: 80.62.60.102, UDP port 11897 (an address located in Denmark), and 91.154.240.41, UDP port 1075 (an address located in Finland). If this individual address were quarantined, the remained of this network would be useable.

150.0.0.0/24

There is a significant level of incoming traffic directed to the single destination address 150.0.0.0, a major proportion of which appears to be DNS queries directed to high numbered UDP ports from end sources that are located in Brazil. This appears to be part of some form of customized DNS setup for an ISP operating in that country. Other traffic streams appear to be directed to 150.0.0.10, 150.0.0.50, 150.0.0.53, 150.0.0.101 and 150.0.0.255.

150.0.1.0/24

The traffic to this network is from various sources and is directed to various addresses in 150.0.1.0/24. A significant proportion of traffic is being directed to 150.0.1.216, UDP port 8640. If this individual address were quarantined, the remained of this network would be useable.

150.0.5.0/24

There are four addresses in this block that attract most of the incoming traffic: 150.0.11.15 and 150.0.11.184 are the highest two addresses, and 150.0.5.114 and 150.0.5.176 are at the next level of incoming traffic.

150.139.169.0/24

There is a single address in this network block at appears to attract the overall majority of incoming traffic:150.139.169.194, UDP port 23052. There are a variety of sources, where each source sends between 4 and 11 packets to this address. If this individual address were quarantined, the remained of this network would be useable.

153.0.88.0/24

There is a single address in this network block at appears to attract the overall majority of incoming traffic: 153.0.88.76, TCP port 4984. There are a variety of sources, sending TCP SYNs to this address. If this individual address were quarantined, the remained of this network would be useable.

153.130.184.0/24

The traffic in this network is a single UDP stream directed at 153.130.184.27, UDP port 5563. The single source is 58.143.131.134, UDP port 9020, located in Korea. The traffic is a sustained level of 100Kbps. If this individual address were quarantined, the remained of this network would be useable.

157.0.0.0/24

The single address 157.0.0.0 attracts the overall majority of the incoming traffic to this network block. If this individual address were quarantined, the remained of this network would be useable.

163.0.0.0/24

The single address 163.0.0.0 attracts the overall majority of the incoming traffic to this network block (80%). If this individual address were quarantined, the remained of this network would be useable.

163.222.55.0/24

The single address 163.222.55.80 attracts the overall majority of the incoming traffic to this network block (98%), which is UDP traffic addressed to port 4583, from various sources. If this individual address were quarantined, the remained of this network would be useable.

171.0.0.0/24

The address 171.0.0.0 attracts the majority of the incoming traffic to this network (65%), and 171.0.0.1 attracts a further 15% of the traffic and 171.0.0.73 attracts a further 10% of the incoming traffic. The sources are distributed. If these three individual address were quarantined, the remained of this network would be useable.

171.41.122.0/24

The address 171.41.122.194 is receiving a constant stream of SIP packets, sourced from the single address 67.78.178.166. If this individual address were quarantined, the remained of this network would be useable.

171.112.109.0/24 17728 - yes

The address 171.112.109.68 is receiving regular bursts of UDP traffic, directed to port 31663, from various

sources. If this individual address were quarantined, the remained of this network would be useable.

In all these cases if the individual addresses noted in the comments were not used for customer assignments, then the entire set of network blocks cvan be made available for allocation.

Appendix A

Unallocated /16 Addresses Administered by APNIC in the Various Network Blocks

139.0.0.0/16	139.226.0.0/16	153.118.0.0/16
139.9.0.0/16	139.227.0.0/16	153.119.0.0/16
139.101.0.0/16	139.228.0.0/16	153.120.0.0/16
139.129.0.0/16	139.255.0.0/16	153.121.0.0/16
139.148.0.0/16	140.0.0.0/16	153.122.0.0/16
139.150.0.0/16	140.75.0.0/16	153.123.0.0/16
139.155.0.0/16	140.143.0.0/16	153.124.0.0/16
139.159.0.0/16	140.149.0.0/16	153.125.0.0/16
139.170.0.0/16	140.205.0.0/16	153.126.0.0/16
139.176.0.0/16	140.206.0.0/16	153.127.0.0/16
139.183.0.0/16	140.207.0.0/16	153.128.0.0/16
139.186.0.0/16	140.210.0.0/16	153.129.0.0/16
139.189.0.0/16	140.213.0.0/16	153.130.0.0/16
139.190.0.0/16	140.224.0.0/16	153.131.0.0/16
139.192.0.0/16	140.237.0.0/16	153.132.0.0/16
139.193.0.0/16	140.240.0.0/16	153.133.0.0/16
139.194.0.0/16	140.243.0.0/16	153.134.0.0/16
139.195.0.0/16	140.246.0.0/16	153.135.0.0/16
139.196.0.0/16	140.249.0.0/16	153.136.0.0/16
139.197.0.0/16	140.250.0.0/16	153.137.0.0/16
139.198.0.0/16	140.255.0.0/16	153.138.0.0/16
139.199.0.0/16	144.0.0.0/16	153.139.0.0/16
139.200.0.0/16	144.7.0.0/16	153.140.0.0/16
139.201.0.0/16	144.12.0.0/16	153.141.0.0/16
139.202.0.0/16	144.52.0.0/16	153.142.0.0/16
139.203.0.0/16	144.123.0.0/16	153.143.0.0/16
139.204.0.0/16	144.255.0.0/16	153.144.0.0/16
139.205.0.0/16	150.0.0.0/16	153.145.0.0/16
139.206.0.0/16	150.115.0.0/16	153.146.0.0/16
139.207.0.0/16	150.116.0.0/16	153.147.0.0/16
139.208.0.0/16	150.117.0.0/16	153.148.0.0/16
139.209.0.0/16	150.121.0.0/16	153.149.0.0/16
139.210.0.0/16	150.122.0.0/16	153.150.0.0/16
139.211.0.0/16	150.138.0.0/16	153.151.0.0/16
139.212.0.0/16	150.139.0.0/16	153.152.0.0/16
139.213.0.0/16	150.223.0.0/16	153.153.0.0/16
139.214.0.0/16	150.255.0.0/16	153.154.0.0/16
139.215.0.0/16	153.0.0.0/16	153.155.0.0/16
139.216.0.0/16	153.3.0.0/16	153.156.0.0/16
139.217.0.0/16	153.34.0.0/16	153.157.0.0/16
139.218.0.0/16	153.35.0.0/16	153.158.0.0/16
139.219.0.0/16	153.36.0.0/16	153.159.0.0/16
139.220.0.0/16	153.37.0.0/16	153.160.0.0/16
139.221.0.0/16	153.99.0.0/16	153.161.0.0/16
139.224.0.0/16	153.101.0.0/16	153.162.0.0/16

153.163.0.0/16
153.164.0.0/16
153.165.0.0/16
153.166.0.0/16
153.167.0.0/16
153.168.0.0/16
153.169.0.0/16
153.170.0.0/16
153.171.0.0/16
153.172.0.0/16
153.173.0.0/16
153.174.0.0/16
153.175.0.0/16
153.176.0.0/16
153.177.0.0/16
153.178.0.0/16
153.179.0.0/16
153.180.0.0/16
153.181.0.0/16
153.182.0.0/16
153.183.0.0/16
153.184.0.0/16
153.185.0.0/16
153.186.0.0/16
153.187.0.0/16
153.188.0.0/16
153.189.0.0/16
153.190.0.0/16
153.191.0.0/16
153.192.0.0/16
153.193.0.0/16
153.194.0.0/16
153.195.0.0/16
153.196.0.0/16
153.197.0.0/16
153.198.0.0/16
153.199.0.0/16
153.200.0.0/16
153.201.0.0/16
153.202.0.0/16
153.203.0.0/16
153.204.0.0/16
153.205.0.0/16
153.206.0.0/16
153.207.0.0/16
153.208.0.0/16
153.209.0.0/16
153.210.0.0/16
153.211.0.0/16
153.212.0.0/16
153.213.0.0/16
153.214.0.0/16
153.215.0.0/16
153.216.0.0/16
153.217.0.0/16
153.218.0.0/16
153.219.0.0/16
153.220.0.0/16
153.221.0.0/16
153.222.0.0/16
153.223.0.0/16
153.224.0.0/16
153.225.0.0/16
153.226.0.0/16
153.227.0.0/16
153.228.0.0/16
153.229.0.0/16
153.230.0.0/16
153.231.0.0/16
153.232.0.0/16
153.233.0.0/16
153.234.0.0/16
153.235.0.0/16
153.236.0.0/16
153.237.0.0/16
153.238.0.0/16
153.239.0.0/16
153.240.0.0/16
153.241.0.0/16
153.242.0.0/16
153.243.0.0/16
153.244.0.0/16
153.245.0.0/16
153.246.0.0/16
153.247.0.0/16
153.248.0.0/16
153.249.0.0/16
153.250.0.0/16
153.251.0.0/16
153.252.0.0/16
153.253.0.0/16
153.254.0.0/16
153.255.0.0/16
157.0.0.0/16
157.18.0.0/16
157.61.0.0/16
157.122.0.0/16
157.148.0.0/16
157.156.0.0/16
157.255.0.0/16
163.0.0.0/16
163.125.0.0/16
163.142.0.0/16
163.177.0.0/16
163.179.0.0/16
163.204.0.0/16
163.213.0.0/16
163.222.0.0/16
163.229.0.0/16
163.255.0.0/16
171.0.0.0/16
171.1.0.0/16
171.2.0.0/16
171.3.0.0/16
171.4.0.0/16
171.5.0.0/16
171.6.0.0/16
171.7.0.0/16
171.8.0.0/16
171.9.0.0/16
171.10.0.0/16
171.11.0.0/16
171.12.0.0/16
171.13.0.0/16
171.14.0.0/16
171.15.0.0/16
171.34.0.0/16
171.35.0.0/16
171.36.0.0/16
171.37.0.0/16
171.38.0.0/16
171.39.0.0/16
171.40.0.0/16
171.41.0.0/16
171.42.0.0/16
171.43.0.0/16
171.44.0.0/16
171.45.0.0/16
171.46.0.0/16
171.47.0.0/16
171.48.0.0/16
171.49.0.0/16
171.50.0.0/16
171.51.0.0/16
171.52.0.0/16
171.53.0.0/16
171.54.0.0/16
171.55.0.0/16
171.56.0.0/16
171.57.0.0/16

171.58.0.0/16
171.59.0.0/16
171.60.0.0/16
171.61.0.0/16
171.62.0.0/16
171.63.0.0/16
171.76.0.0/16
171.77.0.0/16
171.78.0.0/16
171.79.0.0/16
171.80.0.0/16
171.81.0.0/16
171.82.0.0/16
171.83.0.0/16
171.84.0.0/16
171.85.0.0/16
171.86.0.0/16
171.87.0.0/16
171.88.0.0/16
171.89.0.0/16
171.90.0.0/16
171.91.0.0/16
171.92.0.0/16
171.93.0.0/16
171.94.0.0/16
171.95.0.0/16
171.96.0.0/16
171.97.0.0/16
171.98.0.0/16
171.99.0.0/16
171.100.0.0/16
171.101.0.0/16
171.102.0.0/16
171.103.0.0/16
171.104.0.0/16
171.105.0.0/16
171.106.0.0/16
171.107.0.0/16
171.108.0.0/16
171.109.0.0/16
171.110.0.0/16
171.111.0.0/16
171.112.0.0/16
171.113.0.0/16
171.114.0.0/16
171.115.0.0/16
171.116.0.0/16
171.117.0.0/16
171.118.0.0/16
171.119.0.0/16
171.120.0.0/16
171.121.0.0/16
171.122.0.0/16
171.123.0.0/16
171.124.0.0/16
171.125.0.0/16
171.126.0.0/16
171.127.0.0/16
171.207.0.0/16
171.208.0.0/16
171.209.0.0/16
171.210.0.0/16
171.211.0.0/16
171.212.0.0/16
171.213.0.0/16
171.214.0.0/16
171.215.0.0/16
171.216.0.0/16
171.217.0.0/16
171.218.0.0/16
171.219.0.0/16
171.220.0.0/16
171.221.0.0/16
171.222.0.0/16
171.223.0.0/16
171.224.0.0/16
171.225.0.0/16
171.226.0.0/16
171.227.0.0/16
171.228.0.0/16
171.229.0.0/16
171.230.0.0/16
171.231.0.0/16
171.232.0.0/16
171.233.0.0/16
171.234.0.0/16
171.235.0.0/16
171.236.0.0/16
171.237.0.0/16
171.238.0.0/16
171.239.0.0/16
171.240.0.0/16
171.241.0.0/16
171.242.0.0/16
171.243.0.0/16
171.244.0.0/16
171.245.0.0/16
171.246.0.0/16
171.247.0.0/16
171.248.0.0/16
171.249.0.0/16
171.250.0.0/16
171.251.0.0/16
171.252.0.0/16
171.253.0.0/16
171.254.0.0/16
171.255.0.0/16