Background Traffic to Quarantined 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 that were previously identified by APNIC as receiving excessive levels of inbound traffic. 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 networks listed in Appendix A for the period from 5 March 2011 until 15 March 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.

The following networks were NOT tested in the testing setup:

1.0.0.0/24
1.1.1.0/24
1.2.3.0/24
1.3.0.0/16
1.4.0.0/24
1.10.10.0/24
36.37.38.0/24
101.101.101.0/24
101.102.103.0/24
223.255.255.0/24

Distribution of Traffic Across /16s

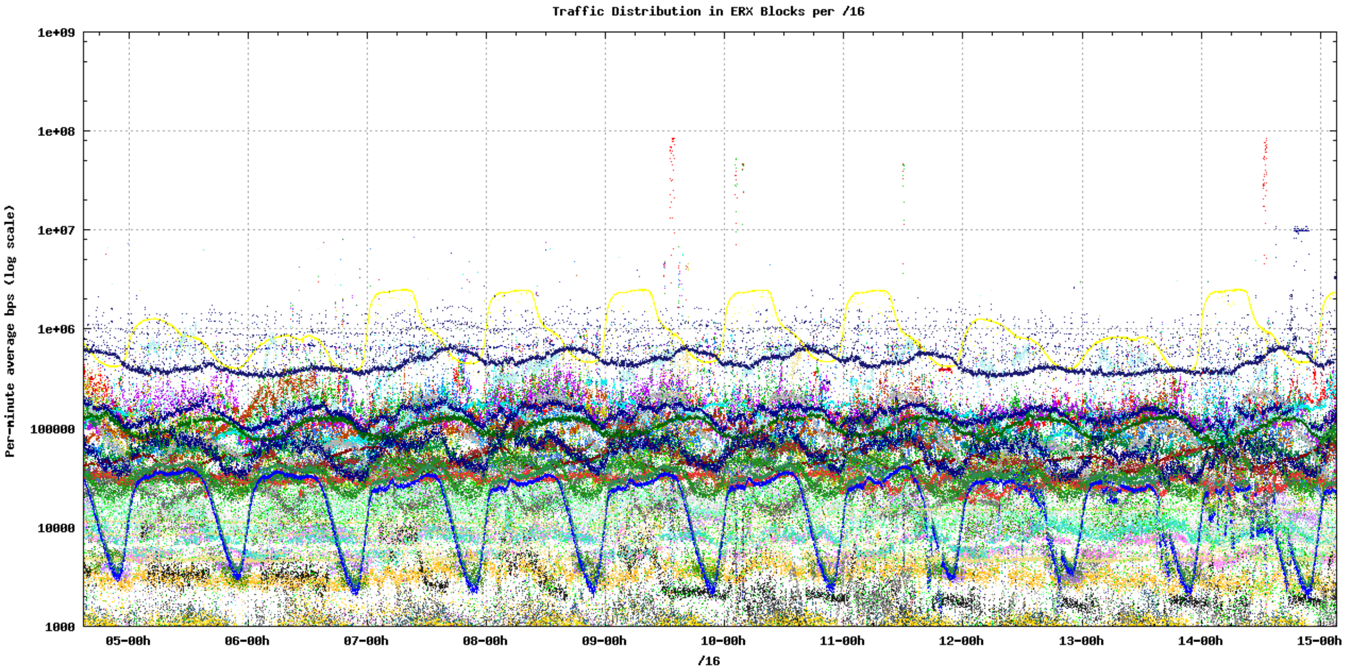

Figure 1 – Incoming traffic per /16 in reserved blocks

The following figures shows the distribution of traffic across each of the /8 address blocks, divided up into /16 segments.

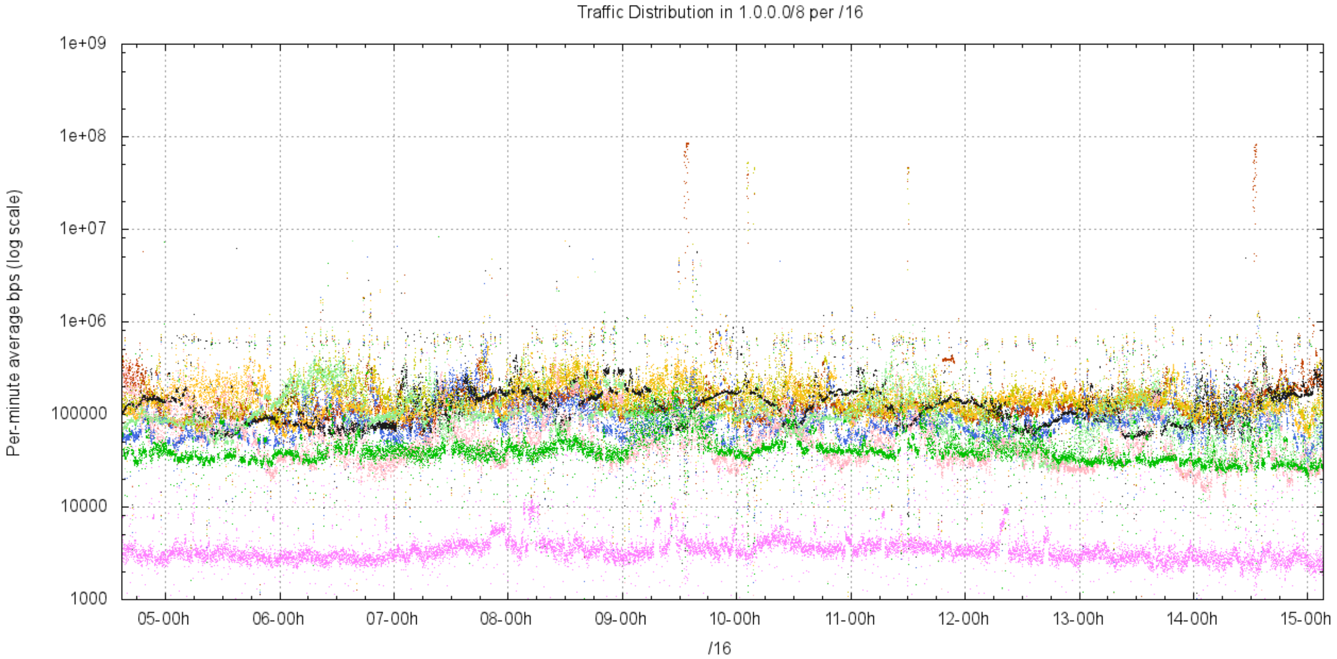

Figure 2 – Incoming traffic per /16 in reserved blocks of 1.0.0.0/8

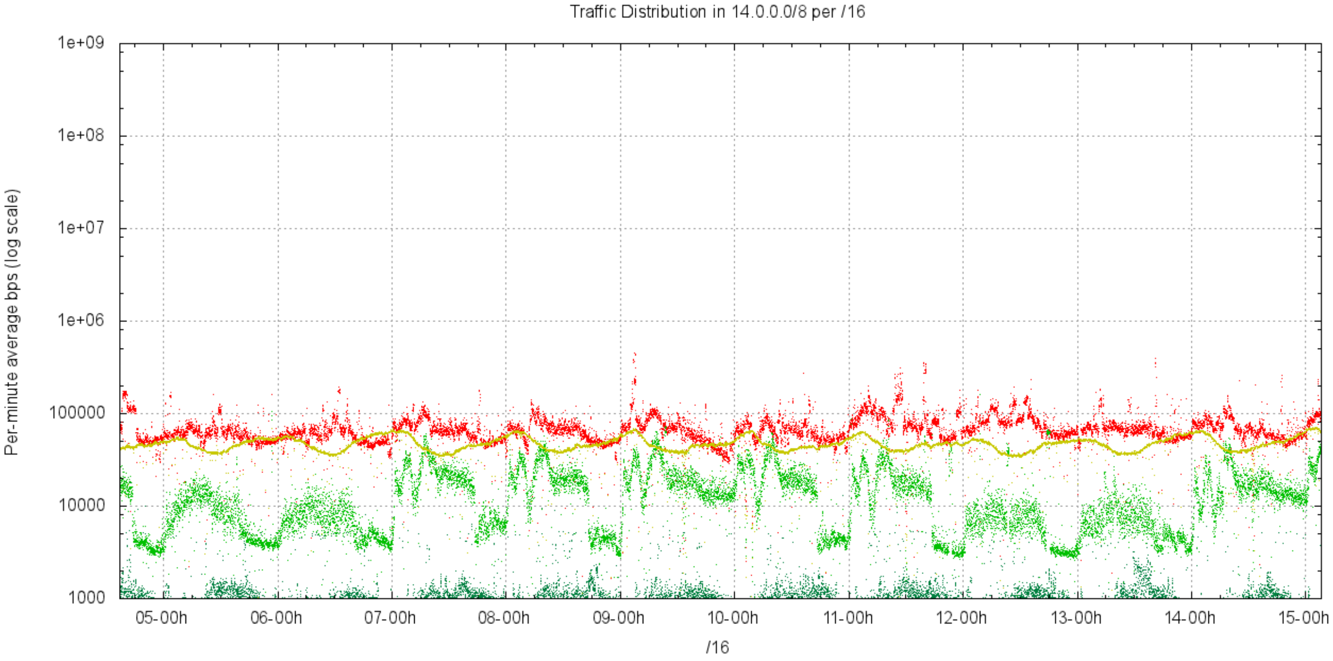

Figure 3 – Incoming traffic per /16 in reserved blocks of 14.0.0.0/8

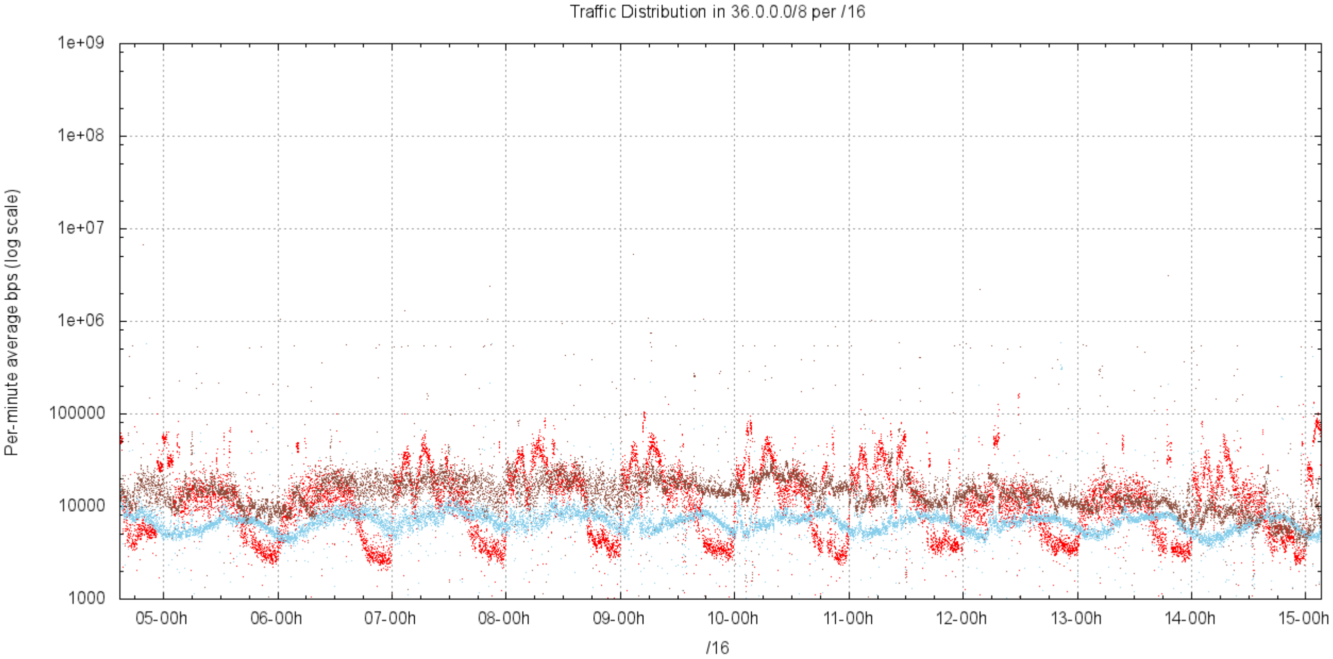

Figure 4 – Incoming traffic per /16 in reserved blocks of 36.0.0.0/8

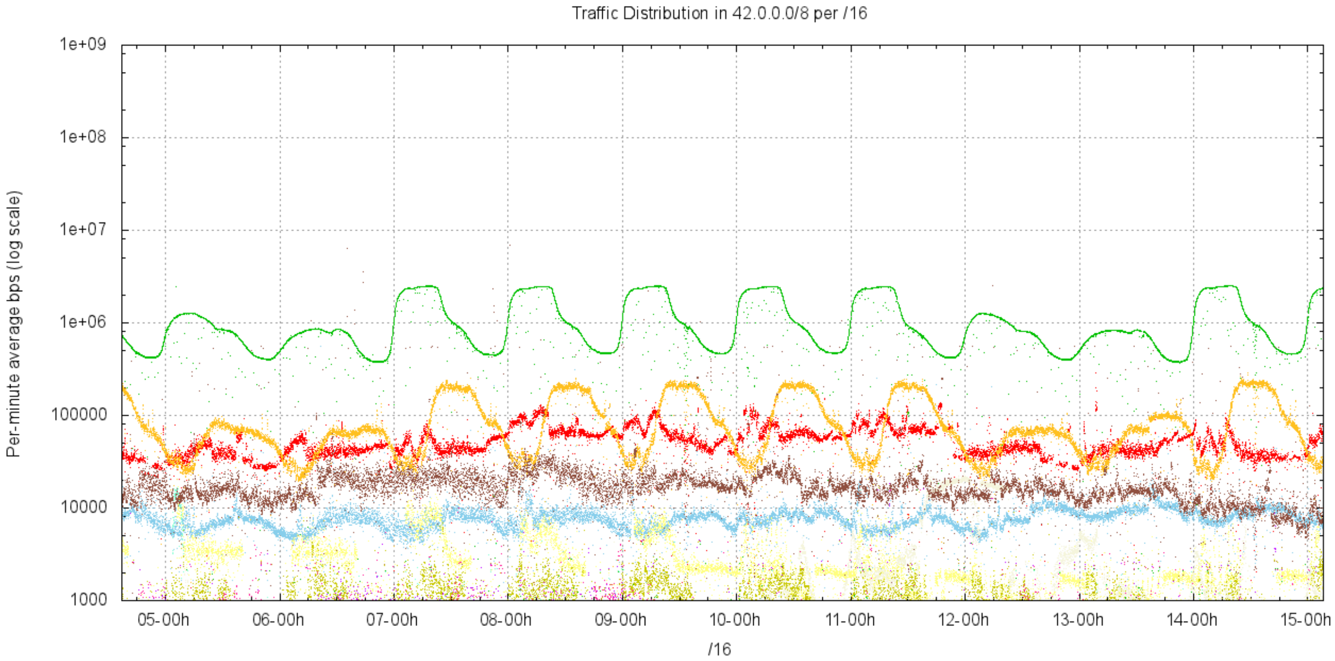

Figure 5 – Incoming traffic per /16 in reserved blocks of 42.0.0.0/8

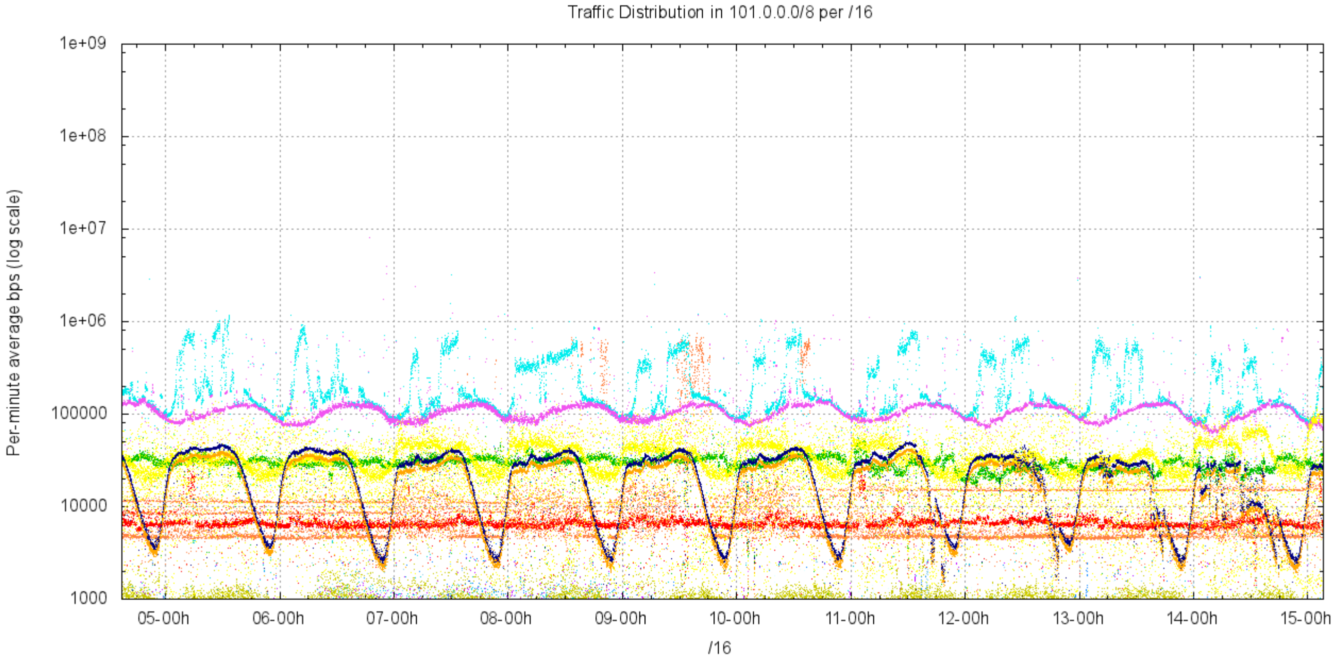

Figure 6 – Incoming traffic per /16 in reserved blocks of 101.0.0.0/8

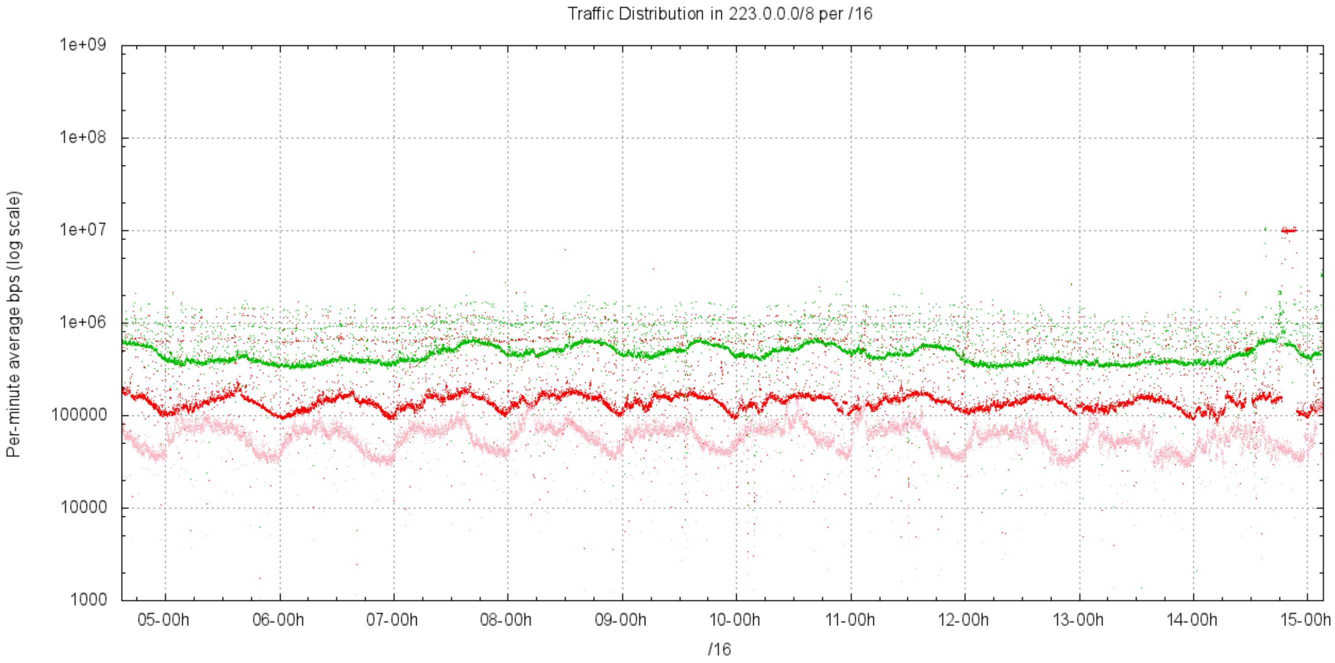

Figure 7 – Incoming traffic per /16 in reserved blocks of 223.0.0.0/8

"Busy" networks

Using a threshold value of a average incoming traffic rate of more than 8Kbps per /24, corresponding to 32 bits per second per address, or approximately 1 packet on average every 24 seconds per address, then the following /24's exceed this level of traffic.

Prefix	Average Traffic
1.5.0.0/24	9.4 Kbps
1.5.6.0/24	9.0 Kbps
1.6.128.0/24	32.7 Kbps
1.20.2.0/24	16.2 Kbps
1.32.0.0/24	8.8 Kbps
1.32.14.0/24	27.3 Kbps
1.37.111.0/24	8.0 Kbps
14.0.0.0/24	62.0 Kbps
14.1.0.0/24	14.3 Kbps
14.192.76.0/24	48.3 Kbps
36.0.0.0/24	15.4 Kbps
42.0.0.0/24	51.5 Kbps
42.1.56.0/24	985.1 Kbps
42.1.57.0/24	135.3 Kbps
42.123.39.0/24	25.1 Kbps
42.194.10.0/24	91.7 Kbps
101.1.1.0/24	30.2 Kbps
101.78.2.0/24	23.9 Kbps
101.97.49.0/24	119.3 Kbps
101.110.116.0/24	23.6 Kbps
101.203.172.0/24	37.1 Kbps
101.234.78.0/24	23.4 Kbps
101.251.0.0/24	19.7 Kbps
223.0.0.0/24	30.6 Kbps
223.1.1.0/24	330.3 Kbps
223.223.223.0/24	62.6 Kbps

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

Conclusions

The following network blocks should continue 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.

1.0.0.0/24
1.1.1.0/24
1.2.3.0/24
1.3.0.0/16
1.4.0.0/24
1.10.10.0/24
36.37.38.0/24
101.101.101.0/24
101.102.103.0/24
223.255.255.0/24

The following network blocks can be returned to the free pool:

1.5.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

1.5.0.0
1.5.0.3
1.5.6.8 intermittent high volume bursts of SNMP query traffic from 194.90.124.233

1.6.0.0/16

The following /32s should be noted as a potential problem, and should not be assigned to end customers. These addresses are attracting a high level of incoming Teredo and 6to4 connection attempts:

1.6.128.102
1.6.128.104
1.6.128.109
1.6.128.114
1.6.128.124
1.6.128.131
1.6.128.136
1.6.128.141
1.6.128.160
1.6.128.165
1.6.128.170
1.6.128.174

1.7.0.0/16

1.8.0.0/16

1.20.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

1.20.2.10 UDP traffic from 161.38.221.246 addressed to 1.20.2.10 UDP port 80
1.20.41.10 UDP traffic from 161.38.221.246 addressed to 1.20.41.10 UDP port 80
1.20.89.10 UDP traffic from 161.38.221.159, addressed to 1.20.89.10 UDP port 80
1.20.92.10 UDP traffic from 12.54.215..166, addressed to 1.20.92.10 UDP port 80
1.20.95.10 UDP traffic from 66.192.234.74 addresses to 1.20.95.10 UDP port 80
1.20.111.10 UDP traffic from 65.123.114.126 addresses to 1.20.111.10 UDP port 80
1.20.128.10 UDP traffic from 161.38.221.231 addressed to 1.20.128.10 UDP port 80
1.20.248.10 UDP traffic from 161.38.221.189 addressed to 1.20.248.10 UDP port 80

1.32.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

1.32.14.10 UDP traffic from various sources in 148.100.0.0/16 addressed to 1.32.14.10 UDP port 80

1.37.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

1.37.57.161 TCP SYN traffic from various sources
1.37.57.171 TCP SYN traffic from various sources

1.187.0.0/16

1.200.0.0/20

14.0.0.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

14.0.0.0 There is a significant proportion of SIP traffic directed to this address, from various sources

14.0.0.144 There is a significant component here of Teredo ICMP6 packets being sent to the equivalent 6to4 IPv6 address of this address, all encapsulated in IPv4 protocol 41 (IPv6-in-IPv4). The teredo packets have a diverse set of IPv4 end addresses in the Teredo packet

14.0.0.254 ICMP backscatter from source address spoofing of 14.0.0.254

14.0.0.255 Various sources sending to UDP port 40002

14.0.1.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

14.1.0.0 There is a significant proportion of UDP traffic from 218.4.143.91, UDP source port 16145 directed to 14.1.0.0 port 4605

14.1.0.2 There is a stream of TCP SYN packets from the single source address 94.91.24.244 directed to port 25000

14.1.0.37 This is a single stream of SYSLOG packets from 201.12.72.140, possibly due to some form of malconfiguration

14.0.2.0/24

14.0.3.0/24

14.0.4.0/24

14.0.15.0/24

14.1.0.0/24

14.102.128.0/23

14.192.76.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

14.192.76.0 There is a significant proportion of UDP traffic from various sources directed to UDP port 4567 at this address.

36.0.0.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

36.0.0.0 There is a significant proportion of UDP traffic from various sources to directed to UDP port 4605 at this address.

36.0.1.0/24

36.50.0.0/20

36.255.0.0/16

42.0.0.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

42.0.0.0 There is a significant proportion of UDP traffic from various sources to directed to UDP port 4605 at this address.

42.0.0.1 There is a significant proportion of UDP NetBIOS traffic from 20 sources to directed to this address.

42.0.1.0/24

42.0.25.0/24

42.1.56.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

42.1.56.100 There is a significant proportion of TCP SYN traffic from various sources directed to TCP Port 20006 at this address.

42.1.57.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

42.1.57.137 There is a significant proportion of UDP traffic from various sources directed to Port 15001 at this address.

42.1.57.156 This network receives a significant flow of TCP SYN packets from various sources directed to port 2186

42.1.57.157 This network receives a significant flow of TCP SYN packets from various sources directed to port 2186

42.1.57.158 This network receives a significant flow of TCP SYN packets from various sources directed to port 2186

42.1.57.159 This network receives a significant flow of TCP SYN packets from various sources directed to port 2186

42.50.0.0/20

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

The following /32s should be noted as a potential problem and should not be assigned to end customers:

42.123.39.80 There is a significant proportion of UDP traffic from various sources directed to various UDP ports at this address

42.156.39.0/24

42.187.123.0/24

42.194.10.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

42.194.10.99 There is a single stream of 1416 octet UDP packets being sent from 195.212.15.244, UDP port 9912 to 42.194.10.99, UDP port 2055

42.201.36.0/24

42.240.51.0/24

42.255.0.0/16

49.0.1.0/24

49.51.0.0/16

49.127.0.0/16

49.128.0.0/24

101.0.1.0/24

101.1.1.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.1.1.1 There is a single stream of UDP packets being sent from 188.248.246.156, UDP port 1199 to 101.1.1.1 UDP port 1101. This address is also attracting DNS query traffic to UDP port 53 from various sources.

101.1.1.2 There is a single stream of SYN+ACK packets being sent from 124.120.245.66, which may be in response to source-spoofed TCP SYN packets being sent to this address. This address is also attracting DNS query traffic to UDP port 53 from various sources.

101.1.1.255 There is a stream of NetBIOS UDP traffic being sent to this address. The source of these packets is 101.1.1.200 and 101.1.1.201, which are spooed sources..

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

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.78.2.125 There is a single stream of UDP SYSLOG packets being sent from 203.246.255.158

101.96.8.0/24

101.97.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.97.49.50 Various sources send bursts of 3 – 4 UDP packets to port 26160 to this address.

101.99.97.0/24

101.99.100.0/24

101.110.116.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.110.116.83 Various sources send bursts of UDP packets to port 3478 to this address. The major sources appear to be 221.234.19.162, 58.52.199.133, 58.52.199.136, and 116.209.240.116, but other sourvces were also observer.

101.127.0.0/16

101.128.0.0/24

101.203.172.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.203.172.20 There is a single stream of UDP SYSLOG packets being sent from 61.33.239.67

101.234.78.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.234.78.244 A large number of source addresses send minimal size UDP packets to port 6693 at this address.

101.251.0.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

101.251.0.203 A large number of source addresses send minimal size UDP packets to port 43266 at this address.

223.0.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

223.0.0.0 A large number of source addresses send UDP packets to port 4605 at this address, and, in addition, DNS query packets are being sent to UDP port 53 at this address

223.1.0.0/16

The following /32s should be noted as a potential problem and should not be assigned to end customers:

223.1.1.128 A large number of source addresses send both UDP and TCP packets to this address, including NetBIOS and NTP UDP packets.

223.223.223.0/24

The following /32s should be noted as a potential problem and should not be assigned to end customers:

223.223.223.0 A large number of sources use this address to direct their DNS queries.
223.223.223.1 A large number of sources use this address to direct their DNS queries.
223.223.223.223 A large number of sources use this address to direct their DNS queries.

Appendix A

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

1.0.0.0/24
1.1.1.0/24
1.2.3.0/24
1.3.0.0/16
1.4.0.0/24
1.5.0.0/16
1.6.0.0/15
1.8.0.0/16
1.10.10.0/24
1.20.0.0/16
1.32.0.0/16
1.37.0.0/16
1.187.0.0/16
1.200.0.0/20
14.0.0.0/24
14.0.1.0/24
14.0.2.0/23
14.0.4.0/24
14.0.15.0/24
14.1.0.0/24
14.102.128.0/23
14.192.76.0/24
36.0.0.0/24
36.0.1.0/24
36.37.38.0/24
36.50.0.0/20
36.255.0.0/16
42.0.0.0/24
42.0.1.0/24
42.0.25.0/24
42.1.56.0/23
42.50.0.0/20
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
42.240.51.0/24
42.255.0.0/16
49.0.1.0/24
49.51.0.0/16
49.127.0.0/16
49.128.0.0/24
101.0.1.0/24
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
101.97.0.0/16
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
101.127.0.0/16
101.128.0.0/24
101.203.172.0/24
101.234.78.0/24
101.251.0.0/24
223.0.0.0/15
223.223.223.0/24
223.255.255.0/24