Background Traffic to Network 103.0.0.0/8

April 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 103.0.0.0/8.

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 103.0.0.0/8 for the period from 3 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.

Traffic Profile

Figure 1 shows the traffic profile for network 103.0.0.0/8.

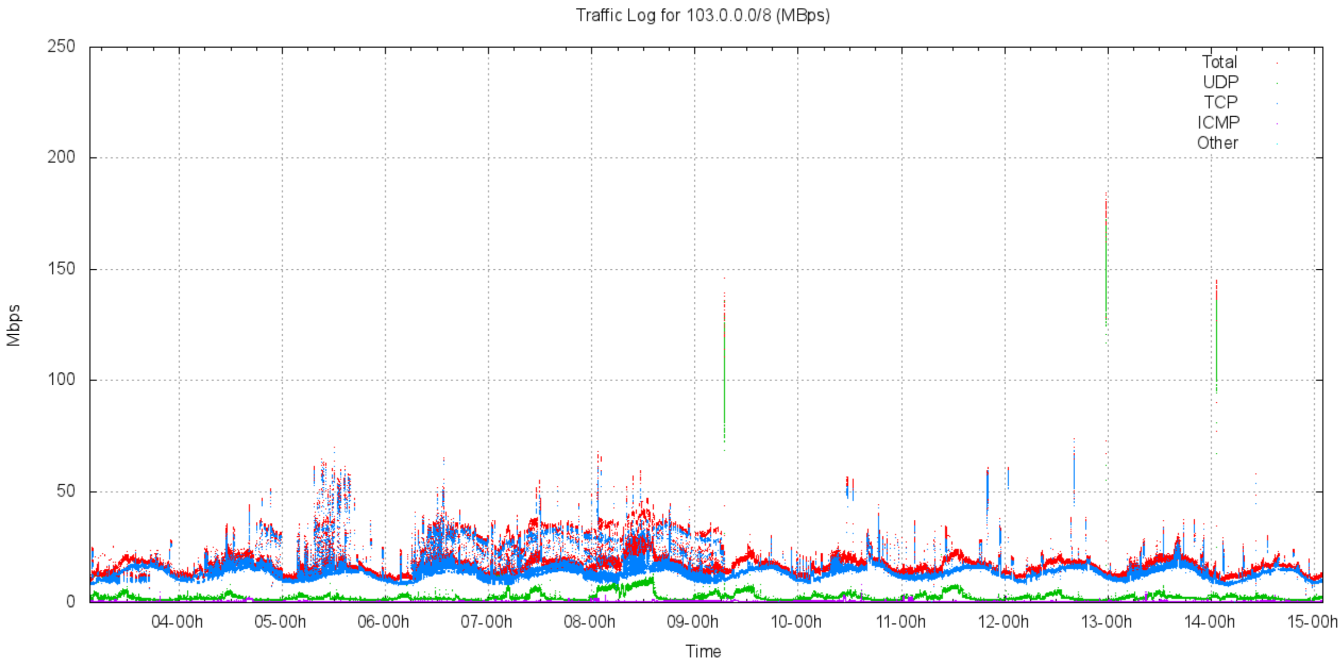


Figure 1 – Traffic profile for 103.0.0.0/8

(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 data.

Protocol	**Traffic**							
	103/8	**106/8**	**39/8**	**36/8**	**101/8**	**49/8**	**14/8**	**223/8**
TCP	83.1%	81.9%	78.7%	82.8%	76.0%	81.5%	66.2%	71.4%
UDP	14.8%	15.7%	18.0%	14.5%	22.7%	17.4%	25.6%	27.6%
ICMP	2.0%	2.2%	2.5%	2.0%	0.9%	1.1%	8.0%	0.9%
Other	0.1%	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.

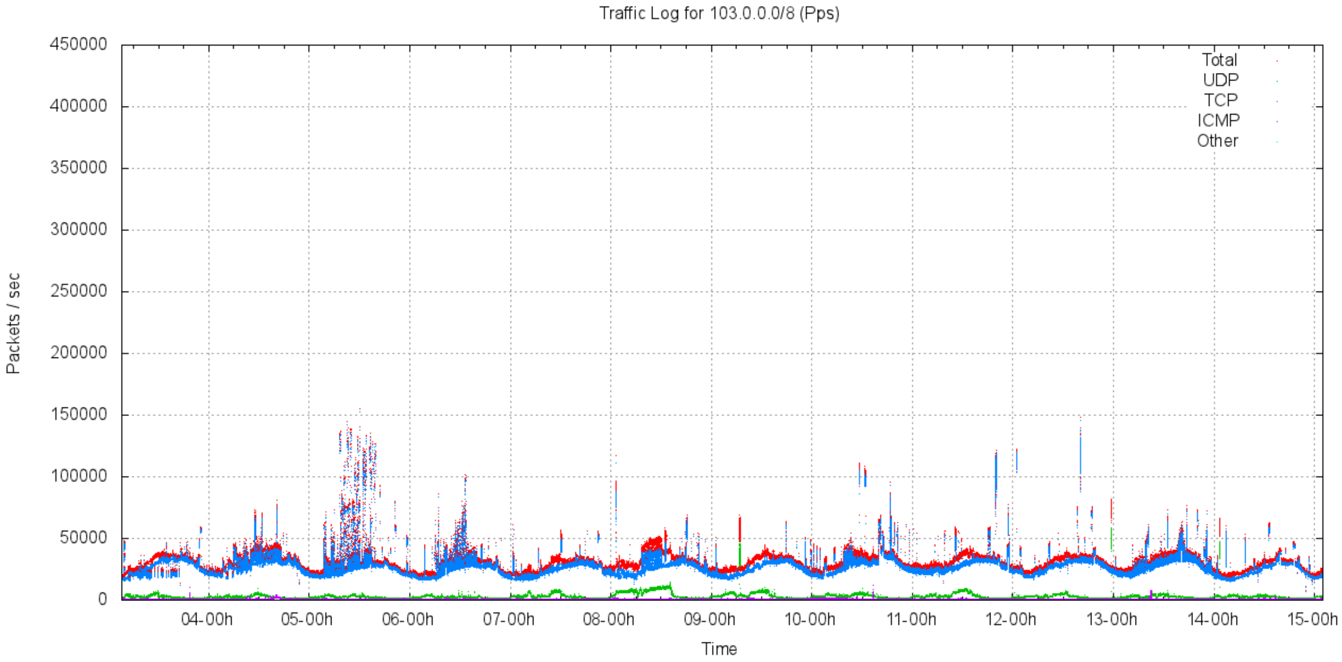


Figure 2 – Packet profile for 103.0.0.0/8

The 103.0.0.0/8 network block attracts between 25,000 and 45,000 packets per second, where 87.9% of the incoming packets are TCP, between 10.1% are UDP, 2.0% 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**							
	103/8	**106/8**	**39/8**	**36/8**	**101/8**	**49/8**	**14/8**	**223/8**
TCP	87.9%	86.5%	84.5%	88.4%	83.1%	86.9%	50.0%	50.0%
UDP	10.1%	11.1%	12.1%	9.2%	16.1%	14.2%	36.5%	35.7%
ICMP	2.0%	2.3%	2.4%	1.7%	0.7%	6.1%	9.9%	13.9%
Other	0.0%	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 (21,943M of the 27,182M TCP packets (80.7%) were TCP SYN packets).

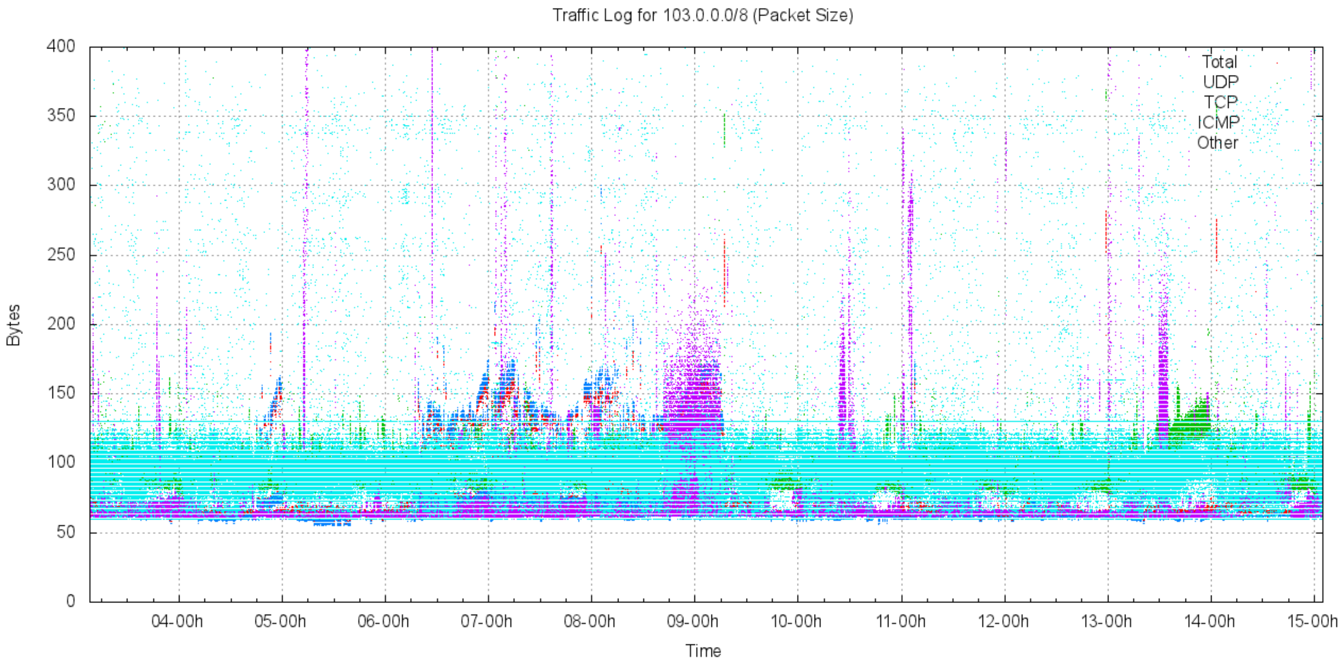


Figure 3 – Packet size distribution for 103.0.0.0/8

Of note in the data collected is the ICMP 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.

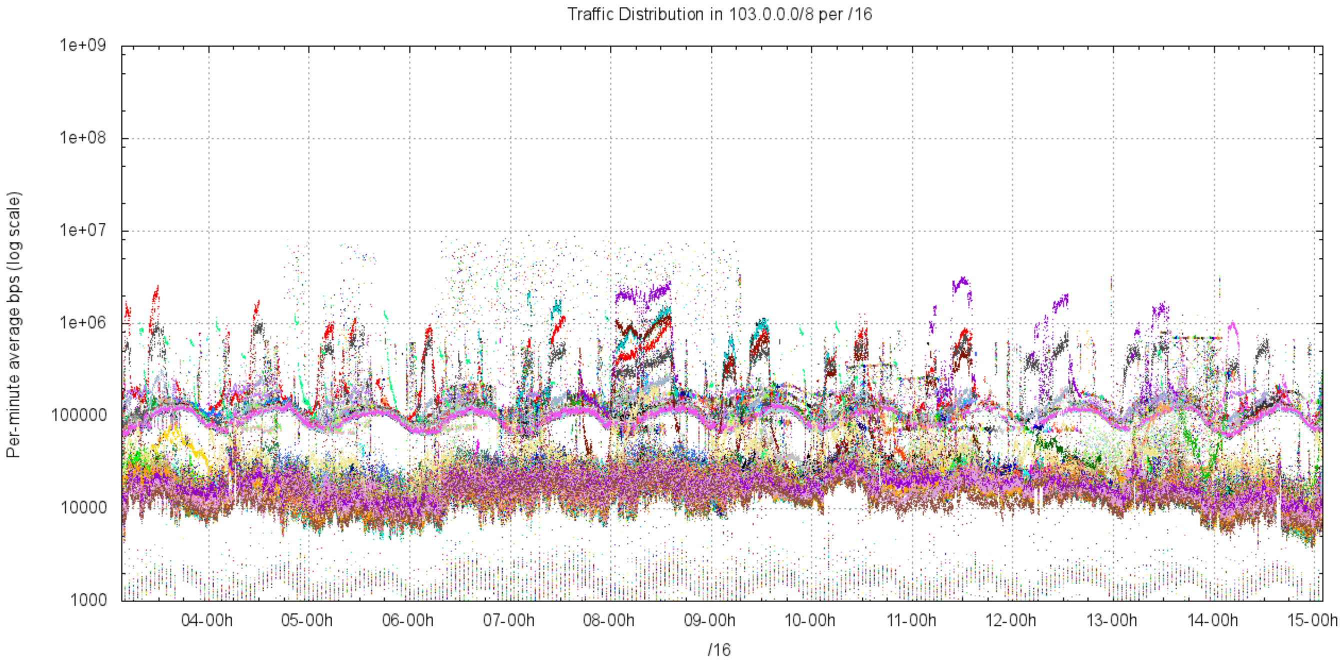


Figure 4 – Traffic distribution per /16 for 103.0.0.0/8

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 103.0.0.0/8 is shown in the following figure.

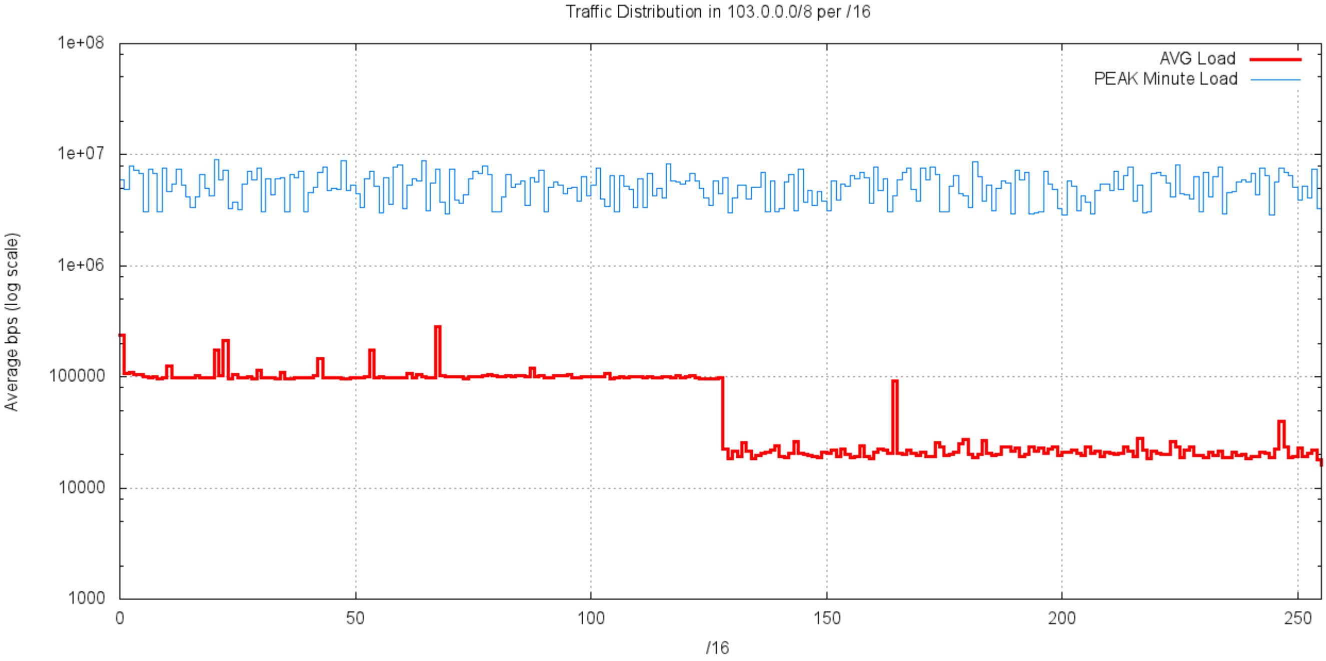


Figure 5 – Average Traffic load per /16 for 103.0.0.0/8

This data collection shows a pronounced break in the "middle" of the address block. The low half of the address block (103.0.0.0/9) has an average traffic load of 100Kbps per /16, while the upper half of the block (103.128.0.0/9) has an average traffic load of 20Kbps.

Distribution of Traffic

The following figure shows the distribution of traffic levels per /24 in network 103.0.0.0/8.

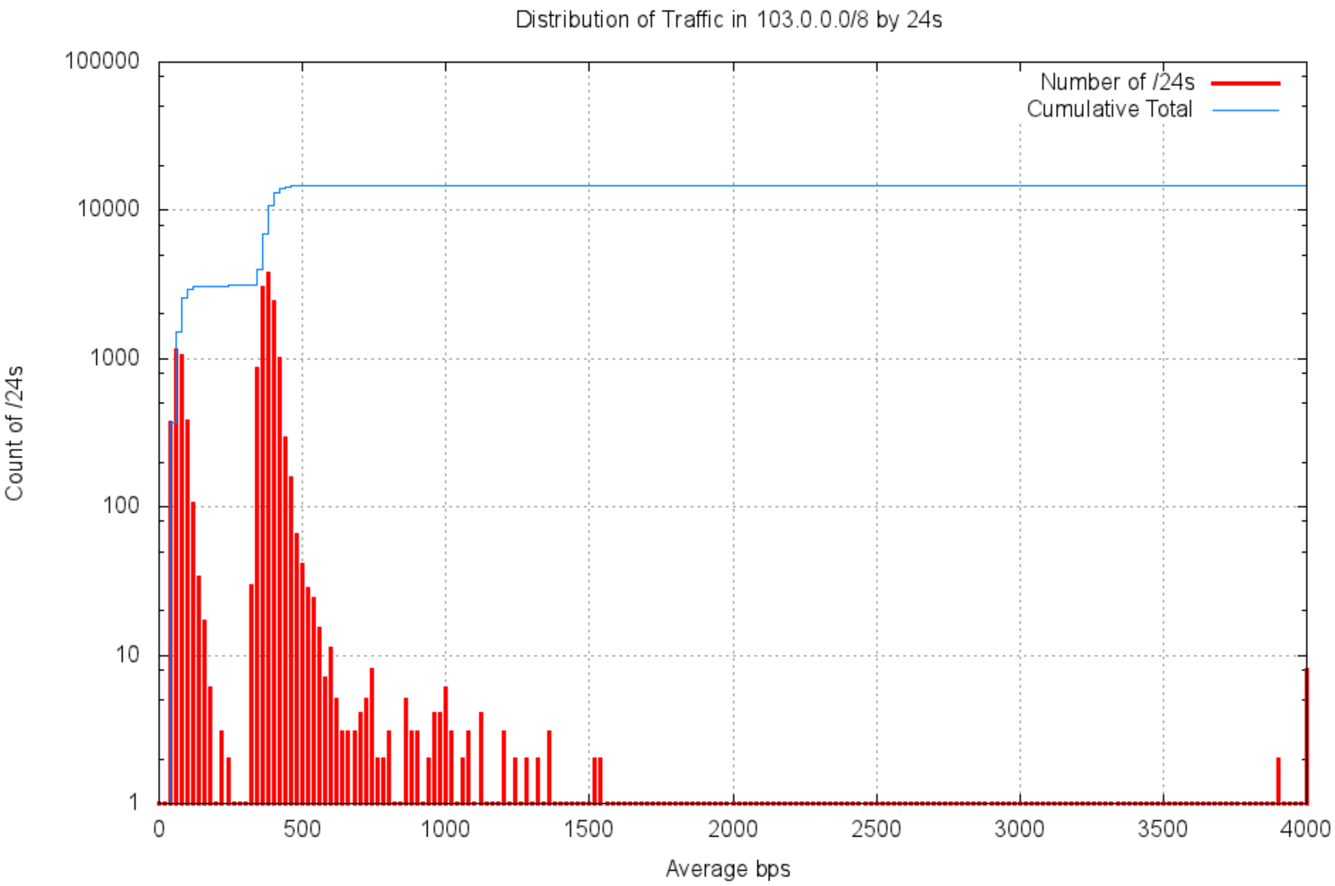


Figure 6 – Traffic profile for 103.0.0.0/8 by /24s

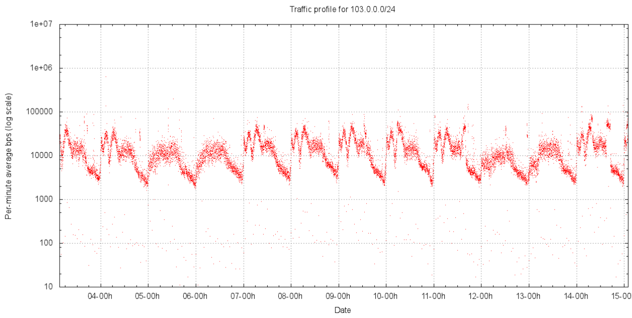
The second peak in this distribution at 400bps per /24 is due to *conficker* scanning across the low /9 of the address block. It appears that the *conficker* scanning traffic element is common across the entire IPv4 address range, and this additional traffic component directed to TCP port 445 in the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

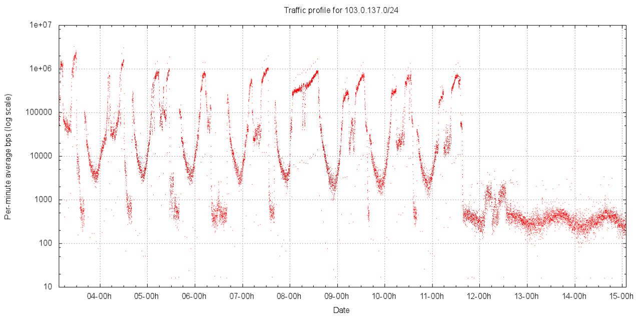
/24 Prefix	**Avg Traffic Level**
103.0.0.0/24	14.0 kbps
103.0.137.0/24	119.4 kbps
103.10.10.0/24	23.1 kbps
103.20.114.0/24	79.3 kbps
103.22.208.0/24	117.1 kbps
103.29.42.0/24	17.5 kbps
103.34.50.0/24	11.5 kbps
103.53.20.0/24	77.7 kbps
103.67.241.0/24	186.9 kbps
103.87.219.0/24	19.9 kbps
103.164.32.0/24	73.4 kbps
103.216.62.0/24	8.0 kbps
103.246.105.0/24	18.8 kbps

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

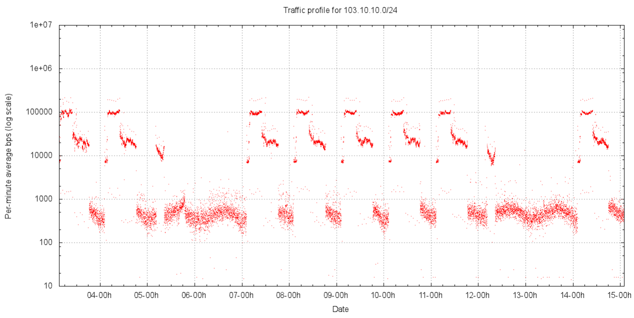
The traffic profile for each of these /24s is show in the following figures



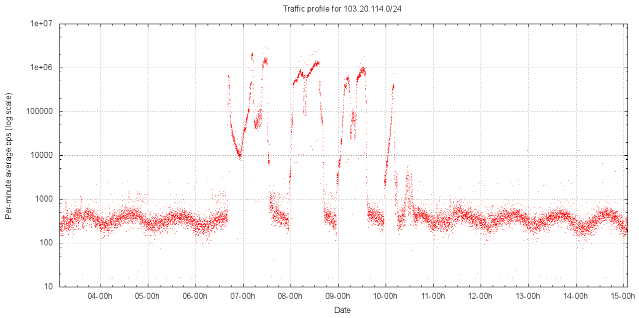
103.0.0.0/24



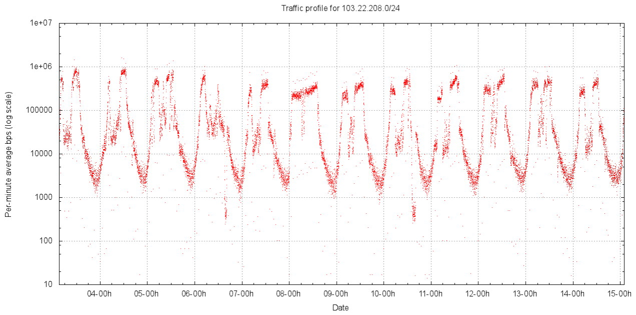
103.0.137.0/24



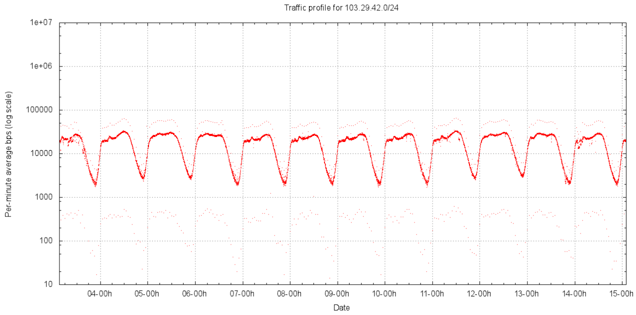
103.10.10.0/24



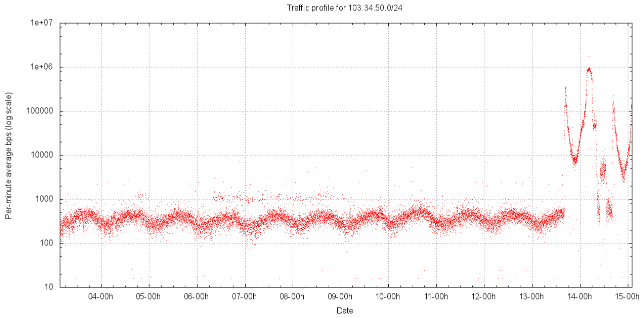
103.20.114.0/24



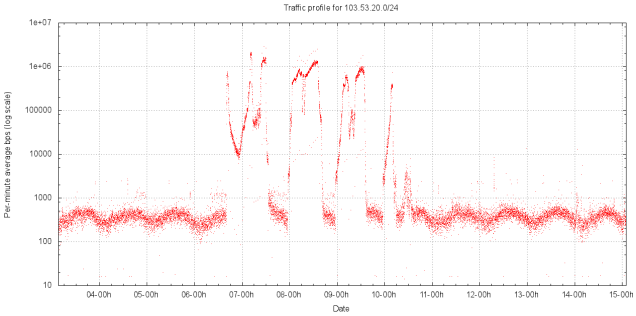
103.22.208.0/24



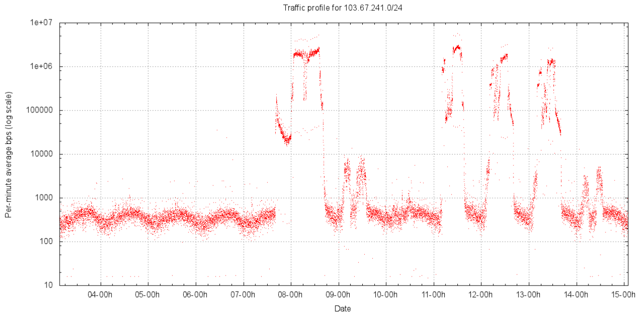
103.29.42.0/24



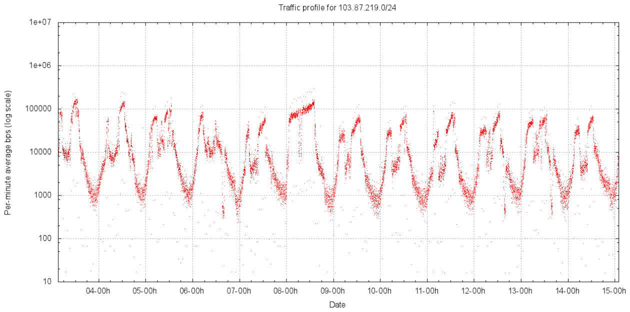
103.34.50.0/24



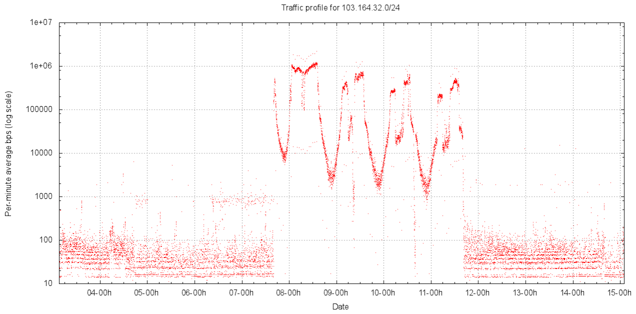
103.53.20.0/24



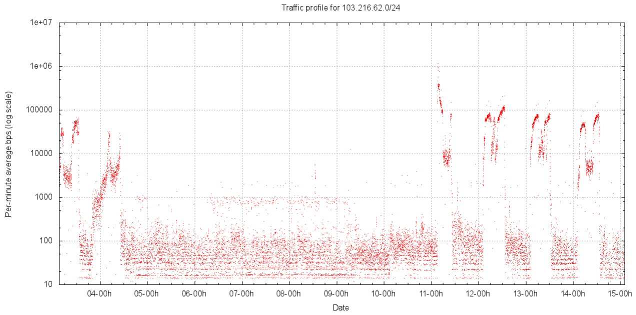
103.67.241.0/24



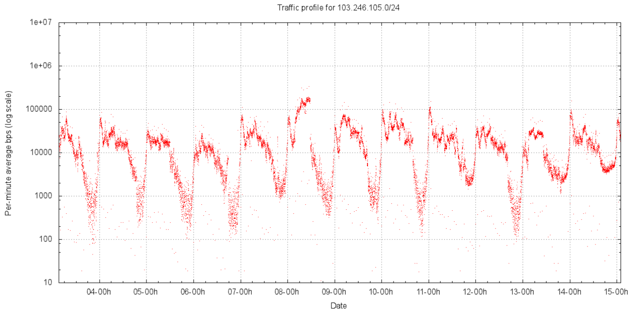
103.87.219.0/24



103.164.32.0/24



103.216.62.0/24



103.246.105.0/24

A number of these prefixes are seeing transient scanning traffic, and as such are not candidate networks for withholding from allocation. The likely explanation of these bursts is that many online games attempt to connect a new client to the "closest" game server, where "closeness" is defined as the server with the minimum delay from the client's perspective. The client establishes this by sending a set of packets to all listed game servers and then ranking them in order of round trip delay. It appears that if there is a typo in the DNS, or a typo in an IP address server list, then the incorrect address is the subject of potentially high volumes of traffic from game clients. This pattern of traffic is evident for a number of addresses in network 103.0.0.0/8

103.0.0.0/24

The traffic here is directed to 103.0.0.0. The traffic is predominately UDP traffic directed to ports 4605 (this is a possibly a UDP server port used for online games) and 18499 from various sources. There are smaller quantities of RADIUS access requests and DNS queries, arising from leakage from private networks who appear to have the address 103.0.0.0 configured into their environment. With the exception of this single address, the remainder of this /24 is useable.

103.0.137.0/24

The address 103.0.137.120 was attracting high volumes of UDP traffic directed to port 27486 for the first half of the test period. The traffic appears to be rendezvous attempts with an online game server. The traffic cleared during the test period and it appears that the entire /24 is useable for allocation.

103.10.10.0/24

This is a stream of 1K UDP packets from 103.10.10.2 directed to 103.10.10.255, with the traffic occurring only on weekdays, sustained at 100Kbps for some 8 hours, then tapering off to 1Kbps for a further 6 hours, then shutting down. This traffic suggests a leakage from a private corporate network, possibly from a video device. The address 103.10.10.255 should not be used for end user allocations, but the remainder of the /24 appears useable for allocation.

103.20.114.0/24

There was a 3 day traffic burst for this network, peaking at 1Mbps for the /24. The traffic is UDP traffic, directed to 103.20.114.48, port 26487. The packets are uniformly 87 bytes in payload size and appear to be an online game server connection attempts from various sources. It appears that an incorrect server address was circulated within an online game context, and subsequently corrected. The entire /24 address block appears to be useable.

103.22.208.0/24

This traffic is 87 byte UDP packets directed to port 64544 at 103.22.208.205. The packets are uniformly 87 bytes in payload size and appear to be an online game server connection attempts from various sources. The traffic rate to 103.22.208.205 peaks at between 0.5Mbps and 0.7 Mps. The address 103.22.208.205 should not be used for end user allocations, but the remainder of the /24 appears to be normal in terms of its background traffic profile.

103.29.42.0/24

This traffic is a stream of 2 byte payload UDP packets directed to port 17982 at 103.29.42.126 from a large set of sources. The address 103.29.42.126 should not be used for end user allocations, but the remainder of the /24 appears to be normal in terms of its background traffic profile.

103.34.50.0/24

There is a burst of 87 byte UDP packets directed to port 62727 at 103.34.50.16. The packets are uniformly 87 bytes in payload size and appear to be an online game server connection attempts from various sources. The packet burst started near the end of the testing period and is likely to be a temporary burst , as the address is unresponsive.

103.53.20.0/24

There is a burst of 87 byte UDP packets directed to port 62954 at 103.50.20.174. The packets are uniformly 87 bytes in payload size and appear to be an online game server connection attempts from various sources. The packet burst lasted for 3 days during the testing period and is likely to be a temporary burst , as the address is unresponsive.

103.164.32.0/24

There is a burst of 87 byte UDP packets directed to port 9596 at 103.164.32.217. The packets are uniformly 87 bytes in payload size and appear to be an online game server connection attempts from various sources. The packet burst lasted for 4 days during the testing period and is likely to be a temporary burst, as the address is unresponsive.

103.216.62.0

There is a burst of 87 byte UDP packets directed to port 39273 at 103.216.62.13. The packets are uniformly 87 bytes in payload size and appear to be an online game server connection attempts from various sources. The packet burst lasted for 5 days during the testing period and is likely to be temporary, as the address is unresponsive.

103.246.105.0

There is a sustained load of 30 byte UDP packets directed to various UDP ports at the address 103.246.105.113. The packets appear to be an online game server connection attempts from various sources. The packet burst lasted across the entire testing period. The address 103.246.105.113 should not be used for end user allocations, but the remainder of the /24 appears useable for allocation.

Conclusions

The entire address block is useable for allocations, but the following individual addresses should be used with caution, and preferably withheld from any form of end client allocation as they attract large quantities of unsolicited traffic on a sustained basis:

103.0.0.0
103.10.10.255
103.22.208.205
103.29.42.126
103.246.105.113