"Dark" Traffic in Network 101.0.0.0/8

September 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 "dark" traffic that is being directed to the address block 101.0.0.0/8.

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 101.0.0.0/8 for the period from 11 August 2010 until 19 August 2010. 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 101/8.

> *(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.)*

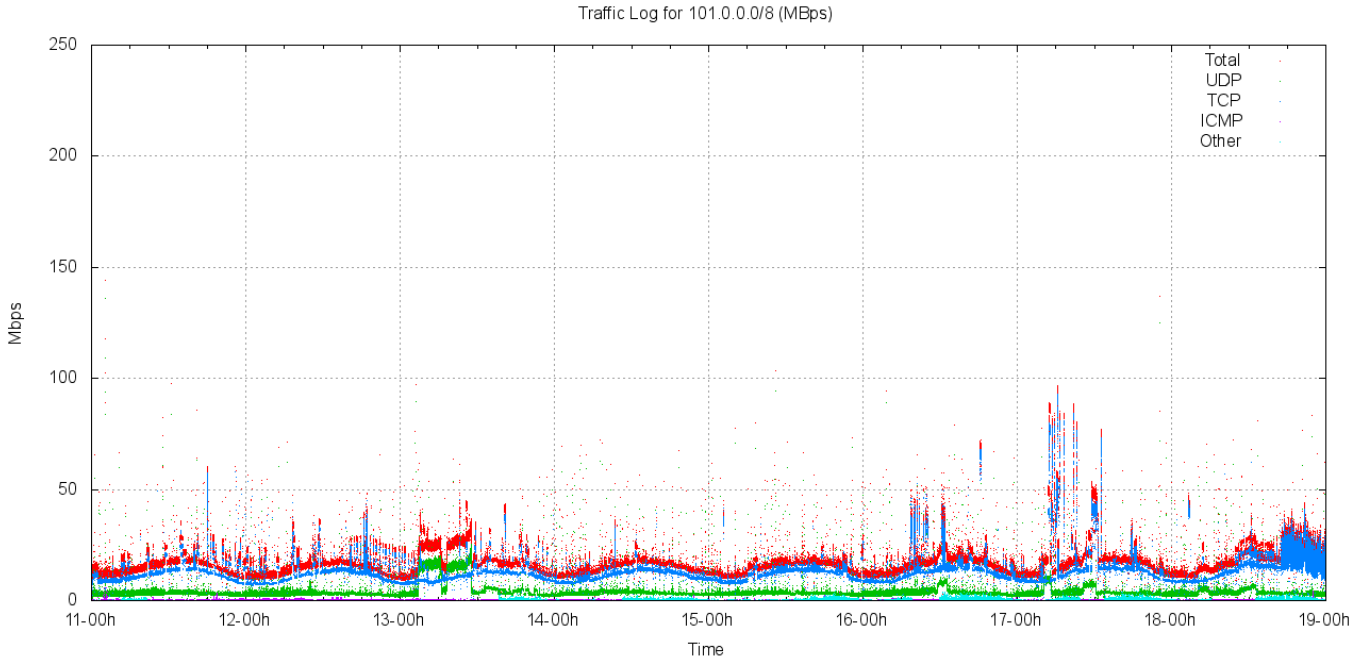

Figure 1 – Traffic profile for 101.0.0.0/8

This traffic profile is similar to the profile that was recorded for 49/8. The address block 101/8 attracts some 12 – 25Mbps of incoming traffic. Of this, some 60% of the traffic is TCP and 35% 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 49.0.0.0/8, 14.0.0.0/8 and 223.0.0.0/8.

Protocol	**Proportion of Traffic** **101.0.0.0/8**	**49.0.0.0/8**	**14.0.0.0/8**	**223.0.0.0/8**
TCP	76.0%	81.5%	66.2%	71.4%
UDP	22.7%	17.4%	25.6%	27.6%
ICMP	0.9%	1.1%	8.0%	0.9%
Other	0.4%	0.0%	0.2%	0.1%

Table 1. Distribution of Traffic by Protocol

Of note here is that the incoming traffic in network 101.0.0.0/8 has a slightly lower component of TCP traffic, and a corresponding higher UDP component compared to two of the other three network blocks, although it is most similar in profile to 14.0.0.0/8

Also of note in terms of traffic profile, incoming TCP traffic in network 101.0.0.0/8 shows a marked diurnal pattern, while the UDP traffic levels do not show such a marked diurnal pattern.

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.

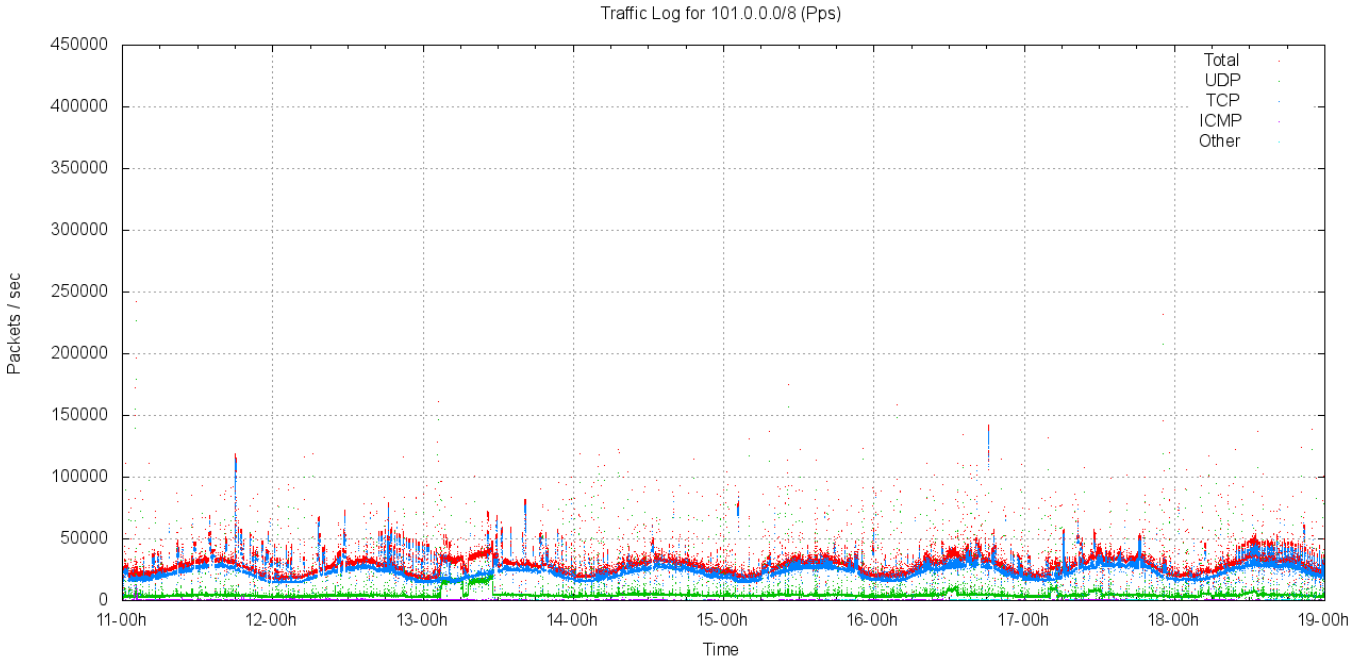

Figure 2 – Packet profile for 101.0.0.0/8

The 101/8 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**			
	101.0.0.0/8	**49.0.0.0/8**	**14.0.0.0/8**	**223.0.0.0/8**
TCP	83.1%	86.9%	50.0%	50.0%
UDP	16.0%	14.2%	36.5%	35.7%
ICMP	0.7%	6.1%	9.9%	13.9%
Other	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 (14,666M of the 16,437M TCP packets (89%) were TCP SYN packets).

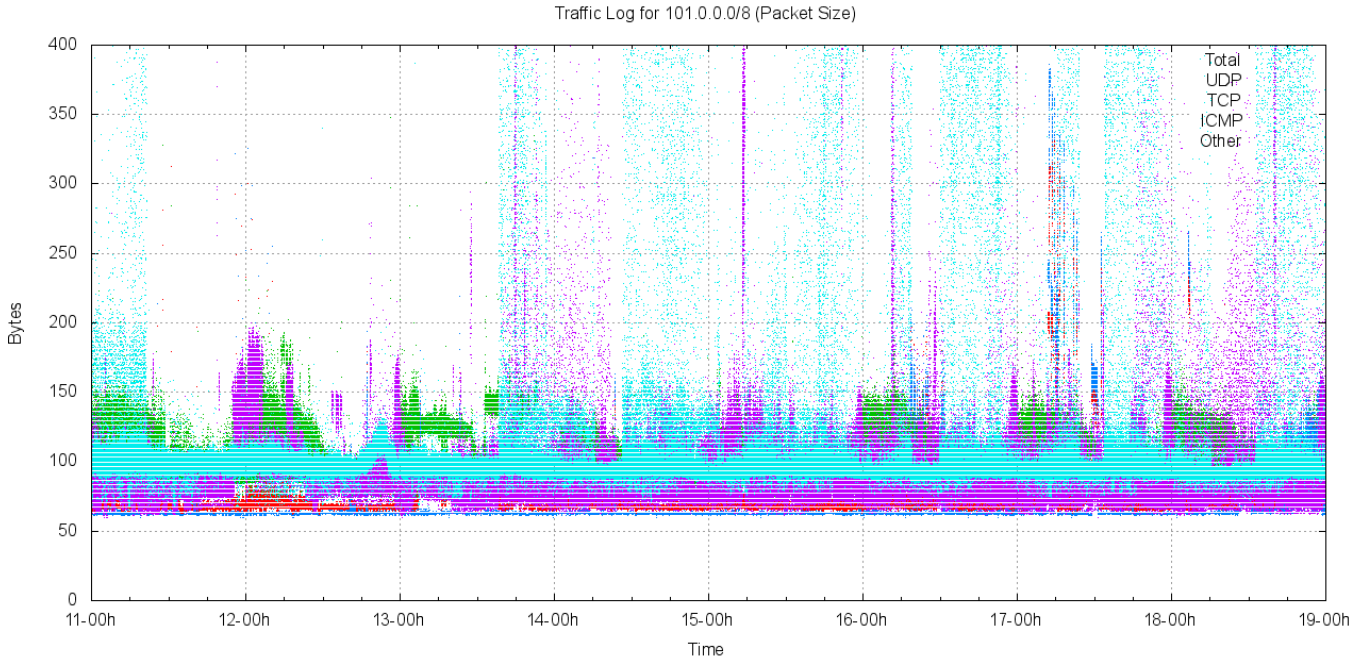

Figure 3 – Packet size distribution for 101.0.0.0/8

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 101.0.0.0/8.

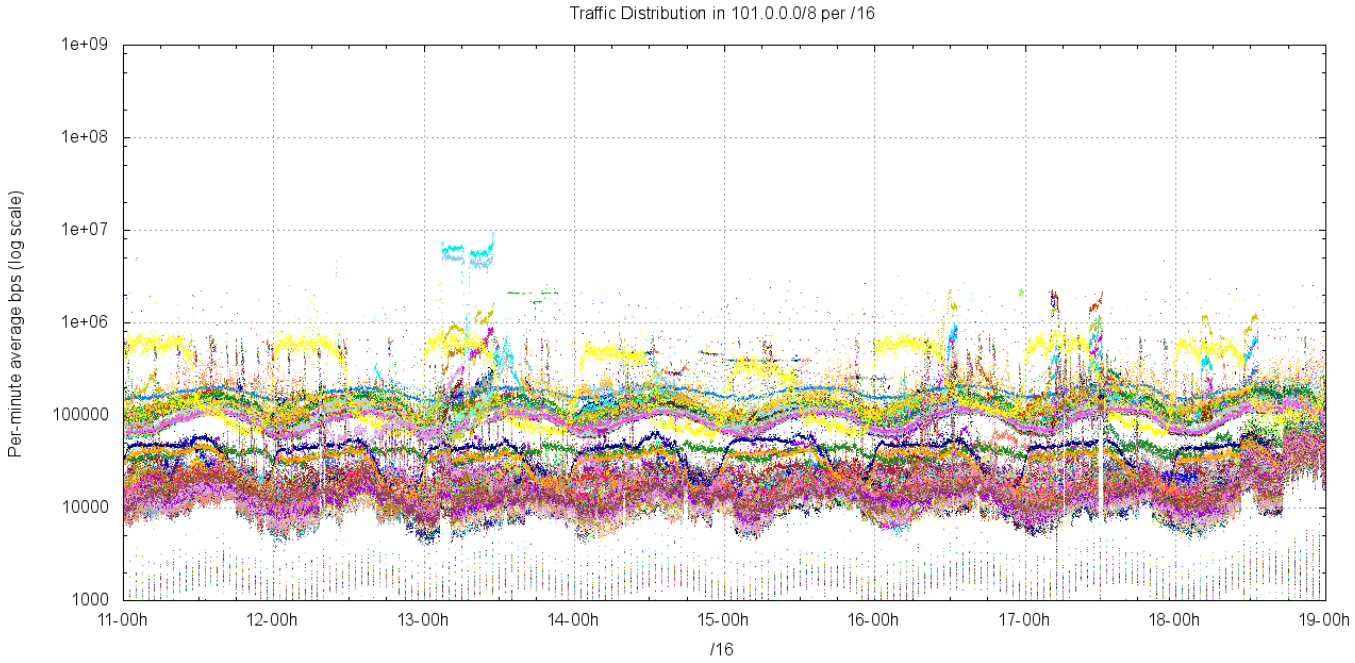

Figure 4 – Traffic distribution per /16 for 101.0.0.0/8

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 exhibits an average traffic level of some 110Kbps per /16, while the high /9 exhibits an average traffic level of 20Kbps, consistent with the scanning behaviour of the conficker virus.

The distribution of average traffic levels for each of the /16s in net 101 is shown in the following figure.

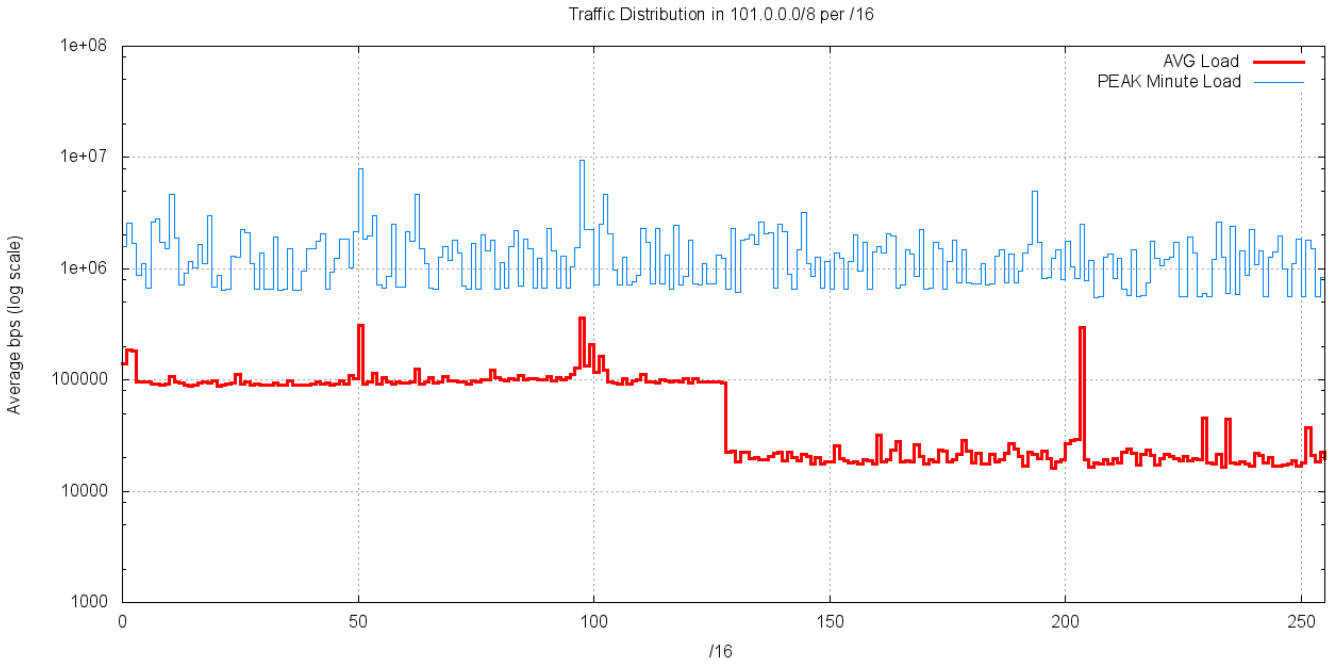

Figure 5 – Average Traffic load per /16 for 101.0.0.0/8

This data collection shows a pronounced break in the "middle" of the address block. The low half of the address block (49.0.0.0/9) has an average traffic load of 100Kbps per /16, while the upper half of the block (49.128.0.0/9) has an average traffic load of 20Kbps. This will be examined in the next section.

There are a number of /16s that appear to show anomalously high levels of traffic, with 10 /16s receiving average incoming traffic levels of in excess of 125Kbps.

Differences in "low" and "high" /9s

Of the 16,437 million TCP packets directed to network 101.0.0.0/8 over the 8 day period when advertised by AS237, some 12,317 million TCP packets were directed to port 445. TCP port 445 is used by Microsoft systems to support the Server Message Block (SMB) protocol, used for file sharing. It is also a very common vector for attacks on Microsoft Windows systems. This skew of traffic distribution, where the low /9 is dominated by TCP SYN traffic to port 445, while the high /9 has no counterpart, and is instead dominated by UDP traffic is typical of what has been previously observed in 49.0.0.0/8, 14.0.0.0/8 and 223.0.0.0/8

Distribution of Traffic

The following figure shows the distribution of traffic levels per /24 in network 101.0.0.0/8.

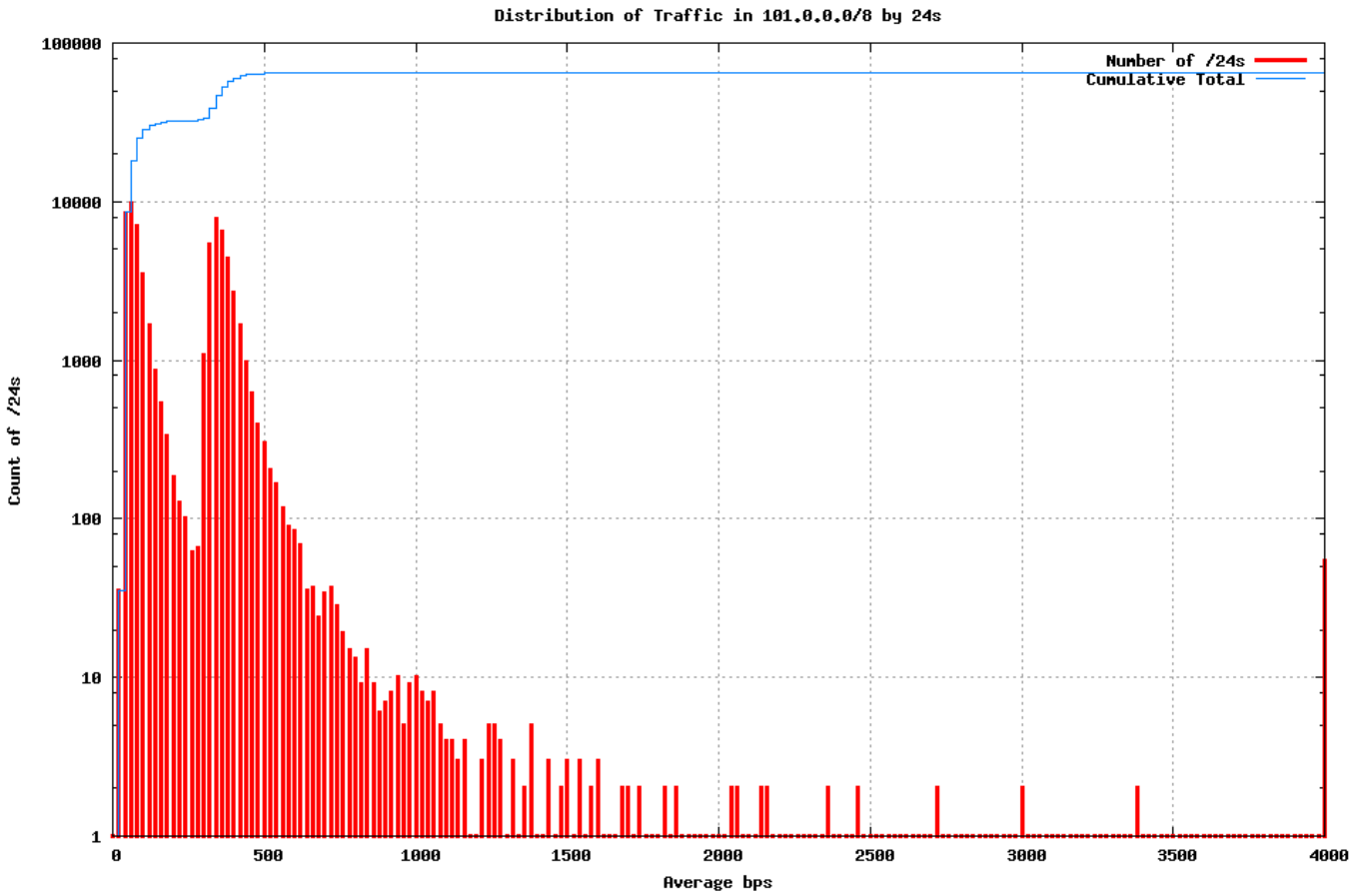

Figure 6 – Traffic profile for 101.0.0.0/8 by /24s

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.

The list of /24s with sustained average traffic levels greater than 10Kbps for the 8 day period are:

101.0.0.0/24	34Kbps
101.1.1.0/24	75Kbps
101.2.173.0/24	85Kbps
101.50.56.0/24	21Kbps
101.53.100.0/24	22Kbps
101.55.225.0/24	12Kbps
101.78.2.0/24	22Kbps
101.96.8.0/24	35Kbps
101.97.51.0/24	213Kbps
101.99.97.0/24	45Kbps
101.99.100.0/24	59Kbps
101.101.101.0/24	53Kbps

101.102.103.0/24	22Kbps
101.110.116.0/24	13Kbps
101.203.172.0/24	278Kbps
101.234.78.0/24	27Kbps
101.251.0.0/24	19Kbps

Conclusions

Using a threshold value of a sustained 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 17 /24s in 101.0.0.0/8 that exceed this level of traffic on a sustained basis.

It is recommended that these 17 /24s be withheld from regular allocation or assignment from 101.0.0.0/8 for a period of 3 months, allowing a second round of testing of these particular prefixes at that time.