"Dark" Traffic in Network 49.0.0.0/8

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 49.0.0.0/8.

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 49.0.0.0/8 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 49/8.

> *(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.)*

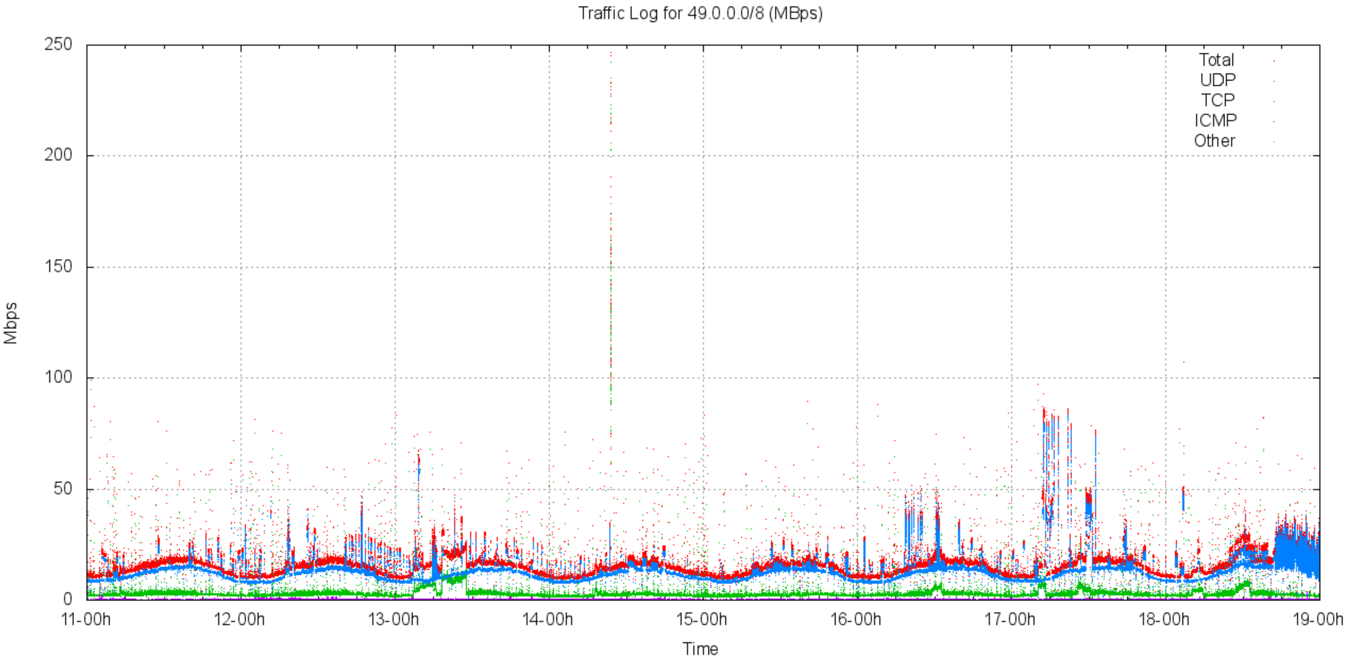

Figure 1 – Traffic profile for 49.0.0.0/8

This traffic profile is similar to the profile that was recorded for 14/8 and 223/8 in May 2010. The address block 49/8 attracts some 17 – 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 14.0.0.0/8 and 223.0.0.0/8.

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

Table 1. Distribution of Traffic by Protocol

Of note here is that the incoming traffic in network 49.0.0.0/8 has a slightly higher component of TCP traffic, and a corresponding lower UDP component.

Also of note in terms of traffic profile, incoming TCP traffic in network 49.0.0.0/8 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.

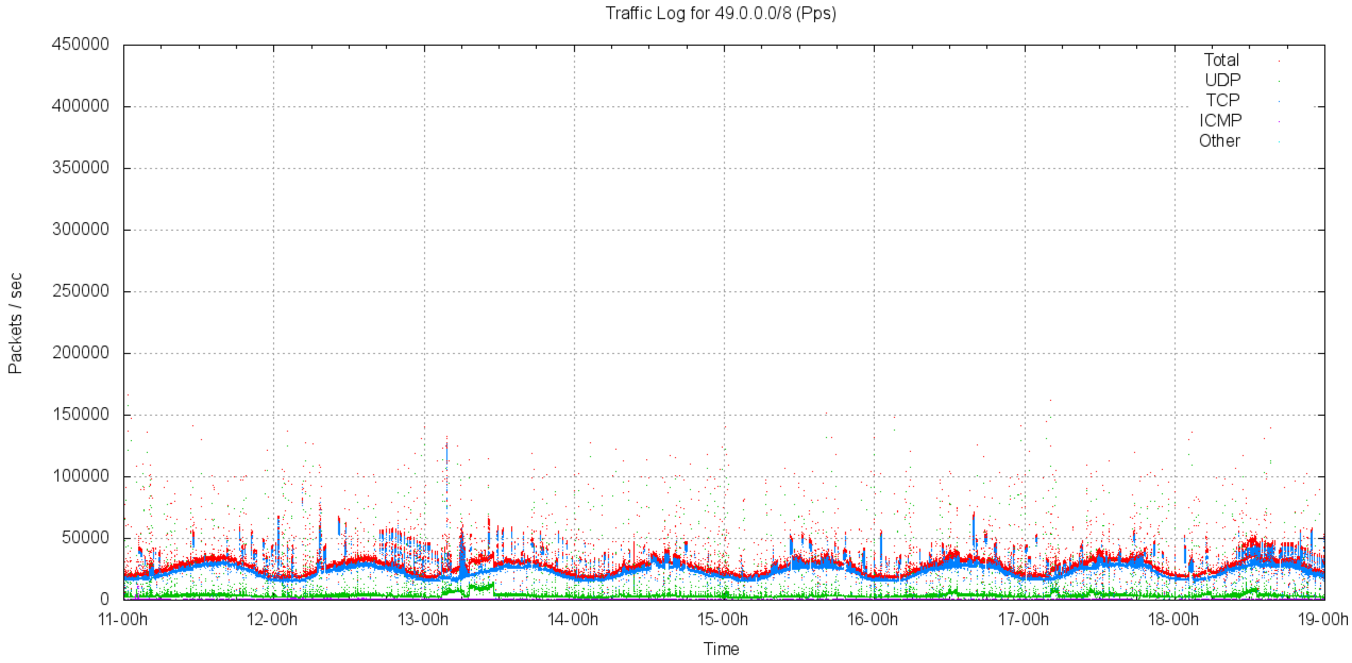

Figure 2 – Packet profile for 49.0.0.0/8

The 49/8 network block attracts between 35,000 and 50,000 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 14/8 and 223/8 for comparison.

Protocol	**Proportion of Packets**		
	49.0.0.0/8	**14.0.0.0/8**	**223.0.0.0/8**
TCP	86.9%	50.0%	50.0%
UDP	14.2%	36.5%	35.7%
ICMP	6.1%	9.9%	13.9%
Other	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 (14,892M of the 16,689M TCP packets (89%) were TCP SYN packets).

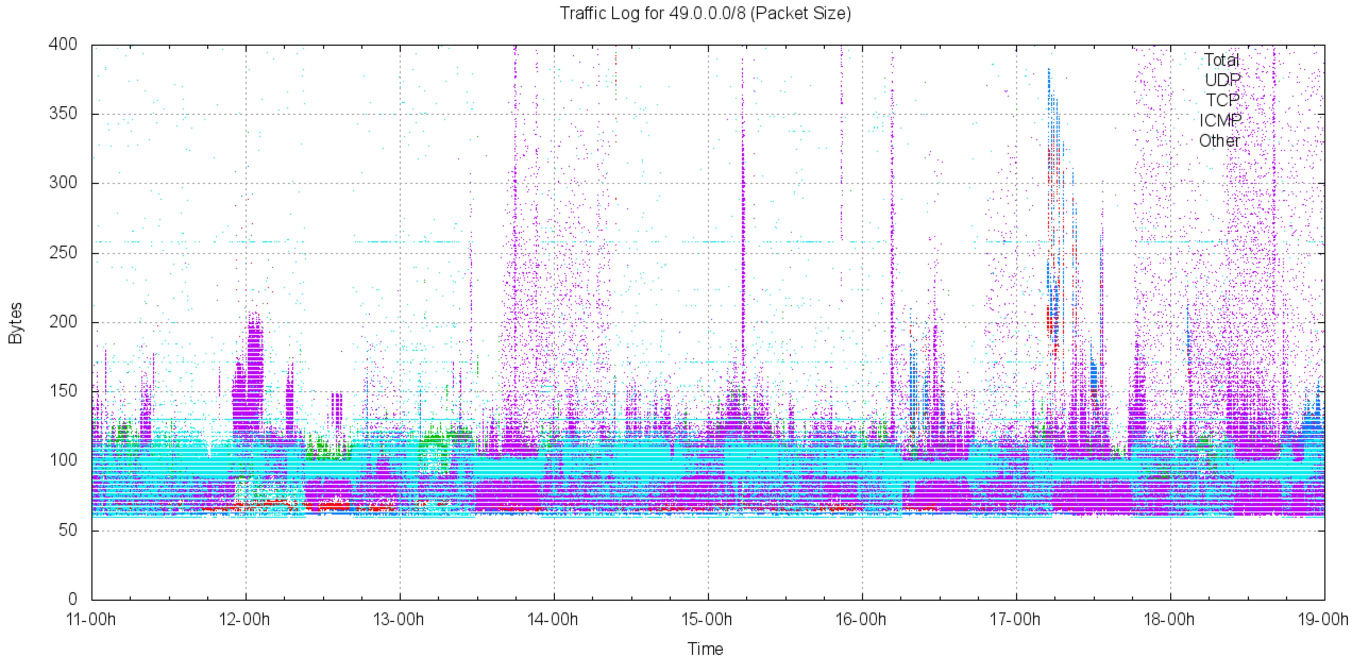

Figure 3 – Packet size distribution for 49.0.0.0/8

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 49.0.0.0/8.

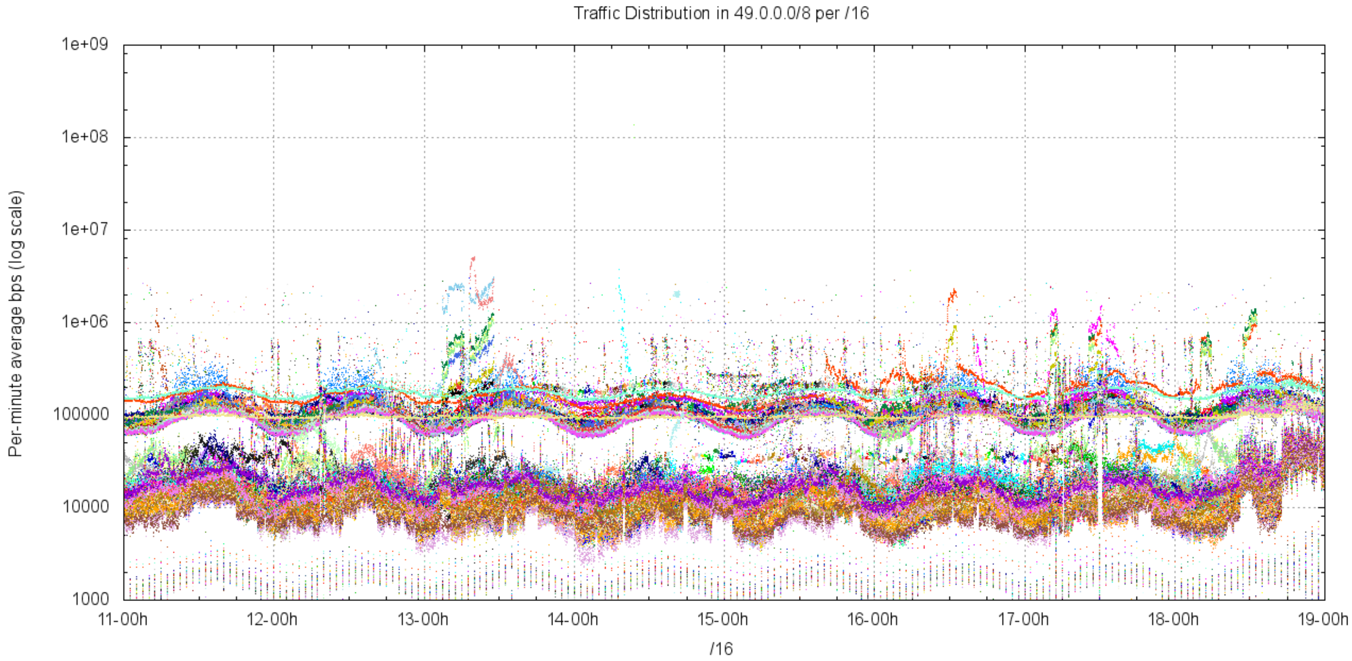

Figure 4 – Traffic distribution per /16 for 49.0.0.0/8

In 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 100Kbps per /16, while the high /9 exhibits an average traffic level of 15Kbps, consistent with the scanning behaviour of the conficker virus.

There is one anomaly at the /16 level, namely 49.153.0.0/16, which shows a steady traffic level of 100Kbps. Over 90% of this traffic in the /16 block is a single UDP stream sourced from port 9004 of 119.201.109.xxx and directed to 49.153.62.235:36428, where the remote system is sending a single 200 byte UDP packet every 20ms.

The distribution of average traffic levels for each of the /16s in net 49 is shown in the following figure.

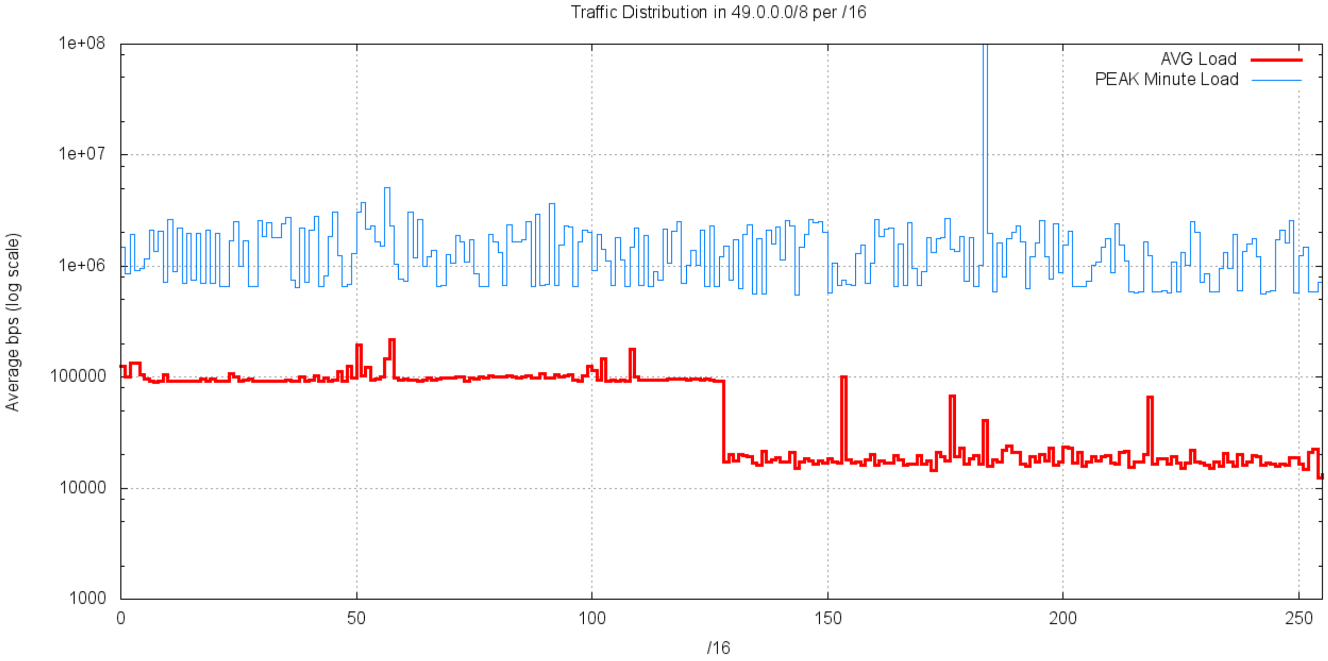

Figure 5 – Average Traffic load per /16 for 49.0.0.0/8

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.

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

Of the 16,698 million TCP packets directed to network 49.0.0.0/8 over the 8 day period when advertised by AS237, some 13,308 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 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 49.0.0.0/8.

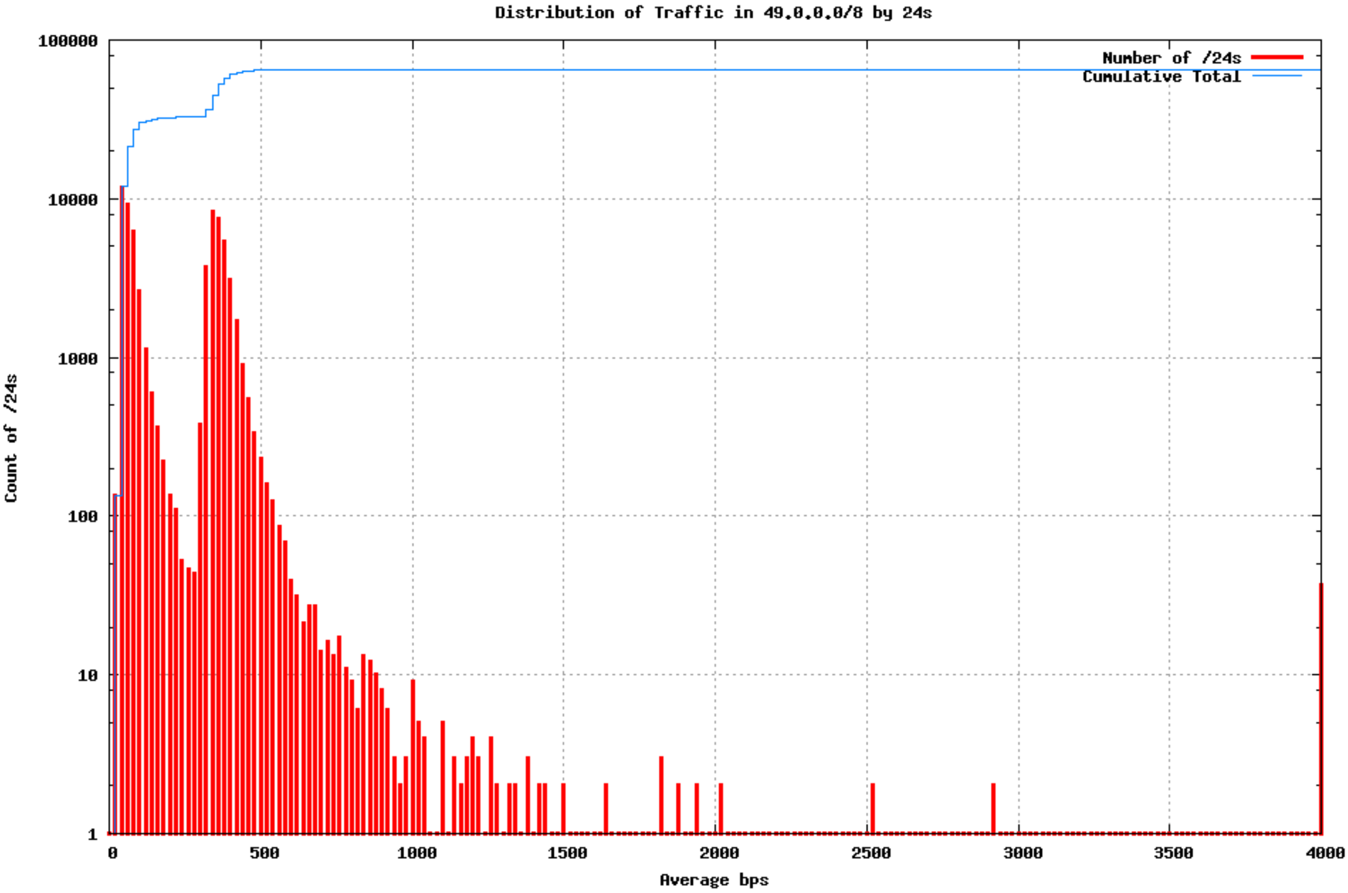

Figure 6 – Traffic profile for 49.0.0.0/8 by /24s

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.

Conclusions

Using a threshold value of 250Kbps per /16, corresponding to 3 bits per second per address, or approximately 1 packet on average every 5 per individual address, then no /16 address blocks in 49.0.0.0/8 can be regards as anomalous to the extent that they should be held over for further examination due to sustained high incoming traffic levels.

At the /24 level a similar conclusion can be drawn, that there is no address block that consistently attracts an anomalously high level of traffic.

It is recommended that no /24s be withheld from regular allocation or assignment from 49.0.0.0/8