

Internet Packet Size Distributions: Some Observations

Rishi Sinha, Christos Papadopoulos, John Heidemann
University of Southern California
web page released October 5, 2005
republished as **ISI-TR-2007-643** May 2007

Abstract

This technical report captures the web page <http://netweb.usc.edu/~rsinha/pkt-sizes/>, summarizing our observations about packet sizes on the Internet in October 2005. Other than reformatting, the technical content has not been changed.

We were recently looking at packet size distributions in Internet traffic. We observed two surprising things. First, **current packet sizes seem mostly bimodal at 40B and 1500B** (at 40% and 20% of packets, respectively). This observation represents a change from common wisdom such as the pre-2000 data that reports tri-modal packet sizes around 40, 576, and 1500B.

Second, in some cases **we observe a strong mode around 1300B**. This represents a new phenomenon.

The first observation holds across all observations at five different network points, including Los Nettos (our regional ISP, carrying a mix of academic and commercial traffic), a USC Internet2 connection, and three connections monitored by NLANR. The second observation does not hold universally, but is very strong at Los Nettos and USC Internet2, and is noticeable in all traces.

The shift away from 576B packets is not surprising, since it is consistent with evolution of Oses and widespread use of Ethernet with a 1500B MTU.

The growth at 1300B packets (seen at Los Nettos and the USC Internet2 link) was surprising to us. We have tentatively identified 1300B packets as stemming from widespread use of VPN software, and possibly from recommendations from DSL providers.

We traced the recommendations for 1300B MTU to several sources. For example VPN MTU recommendations, see:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/4_6/admin/vcach8.htm#wp1153482

and

<http://www.rochester.edu/its/vpn/tutorials/mtu.html>

http://www.brown.edu/Facilities/CIS/Network_Services/vpnfaq.html

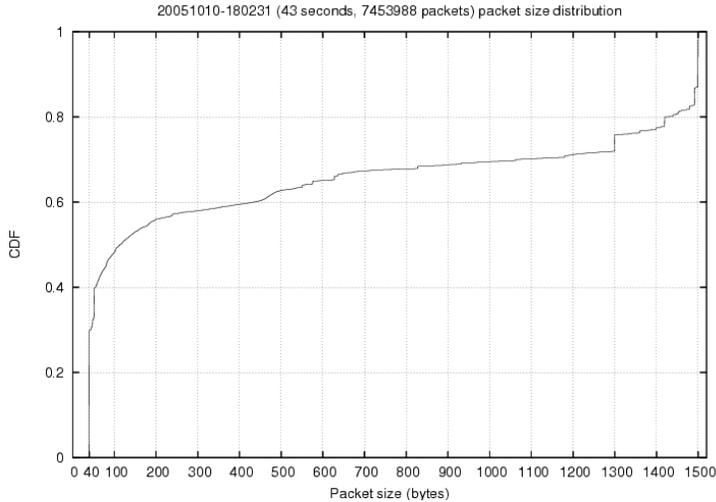


Figure 1: 43-second Los Nettos Level3 trace. (Unreleased Internet Trace Measurement dataset. Traces taken 2005-10-10. USC/LANDER project. <http://www.isi.edu/ant/lander>.)

http://www.shef.ac.uk/cics/services/internet/vpn/vpn_trouble.html

Also, the following URLs mention that 1300B is an MTU some ISPs recommend for DSL connections, but we haven't seen an official ISP recommendation to this effect.

<http://www.networkworld.com/newsletters/frame/2005/0613wan2.html>
<http://msn.pcworld.com/howto/article/0,aid,119267,pg,4,00.asp>

Our observations do not point to wide use of end-to-end VPN over WANs, but to VPN use at the edge network, since the 1300B size noted is presumably that of packets that have exited a VPN tunnel. This edge-network use is certainly true at USC, where most wireless traffic traverses a VPN over the wireless hop and then proceeds unencrypted over the rest of the Internet. This behavior explains why Los Nettos and USC Internet2 traffic shows the strongest 1300B modes of the sites we observe.

Shown here are packet size distributions computed from tcpdump traces collected at Los Nettos (Figure 1) and USC's Internet2 link (Figure 2) and from publicly available traces collected by NLANR (Figures 3 through 5). The Los Nettos traces are from October 10, 2005 and the USC Internet2 traces are from December 2, 2004. The NLANR traces are from September 13, 2005 and were obtained from <http://pma.nlanr.net/Traces/Traces/daily/20050913/> By "packet size" we mean the byte-count in the length field of the IP header.

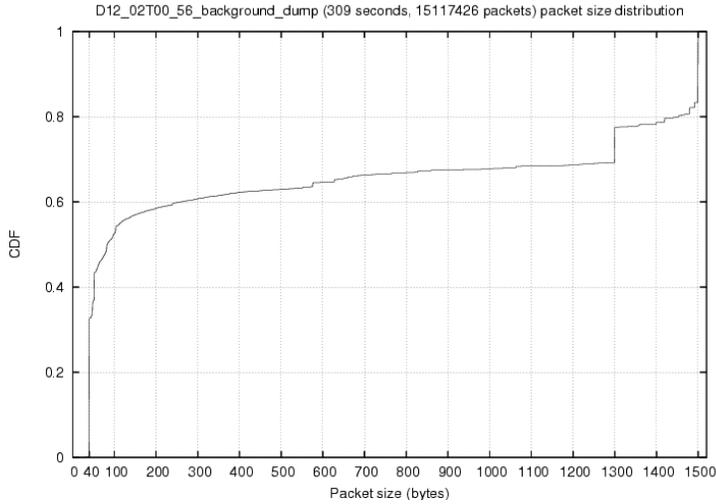


Figure 2: Five-minute USC Internet2 trace. (Scrambled Internet Trace Measurement dataset, PREDICT ID USC-LANDER/Bottleneck_traces-20041202. Traces taken 2004-12-02 to 2004-12-03. Provided by the USC/LANDER project. <http://www.isi.edu/ant/lander>.)

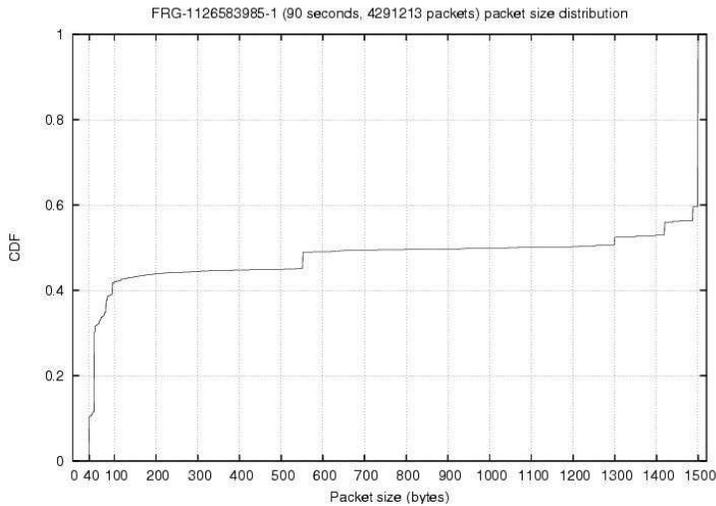


Figure 3: 90-second NLANR FRG (Front Range GigaPOP) trace. Traces taken 2005-09-13. Passive Measurement and Analysis, National Laboratory for Applied Network Research. <http://pma.nlanr.net>.

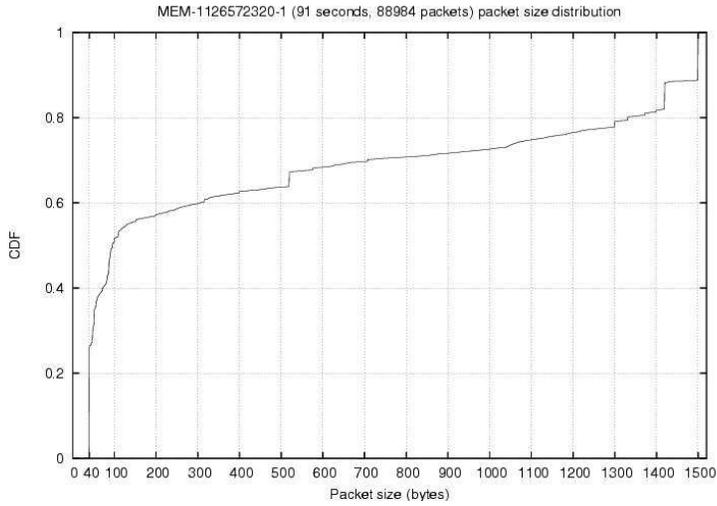


Figure 4: 90-second NLANR MEM (University of Memphis) trace. Traces taken 2005-09-13. Passive Measurement and Analysis, National Laboratory for Applied Network Research. <http://pma.nlanr.net>.

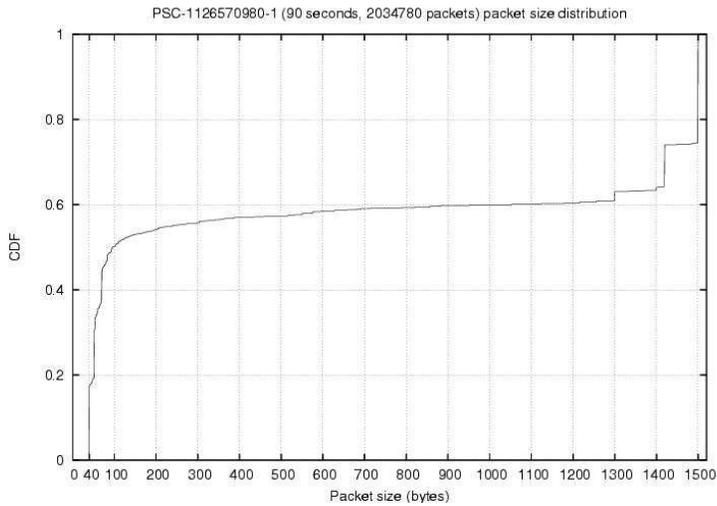


Figure 5: 90-second NLANR PSC (Pittsburgh Supercomputing Center) trace. Traces taken 2005-09-13. Passive Measurement and Analysis, National Laboratory for Applied Network Research. <http://pma.nlanr.net>.

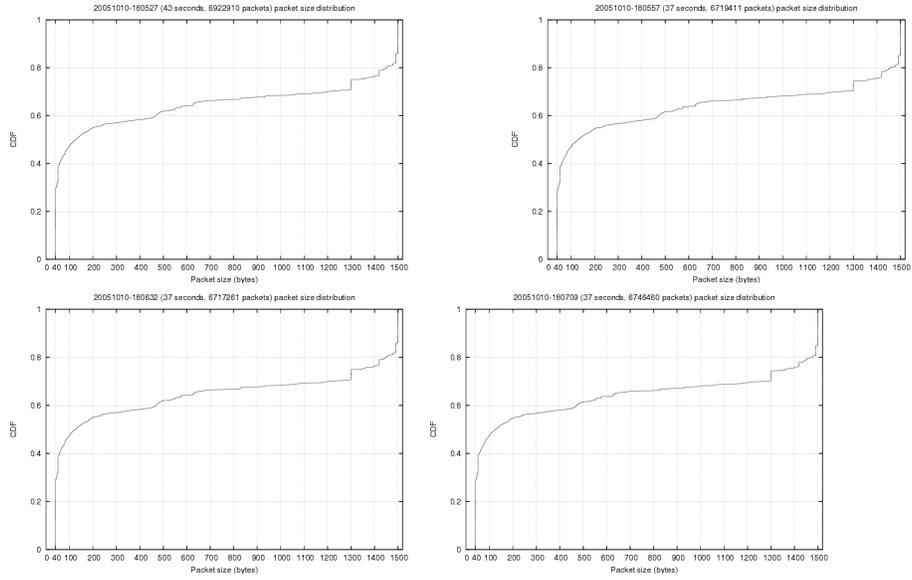


Figure 6: Supplementary traces from Los Nettos Level3 at other times.

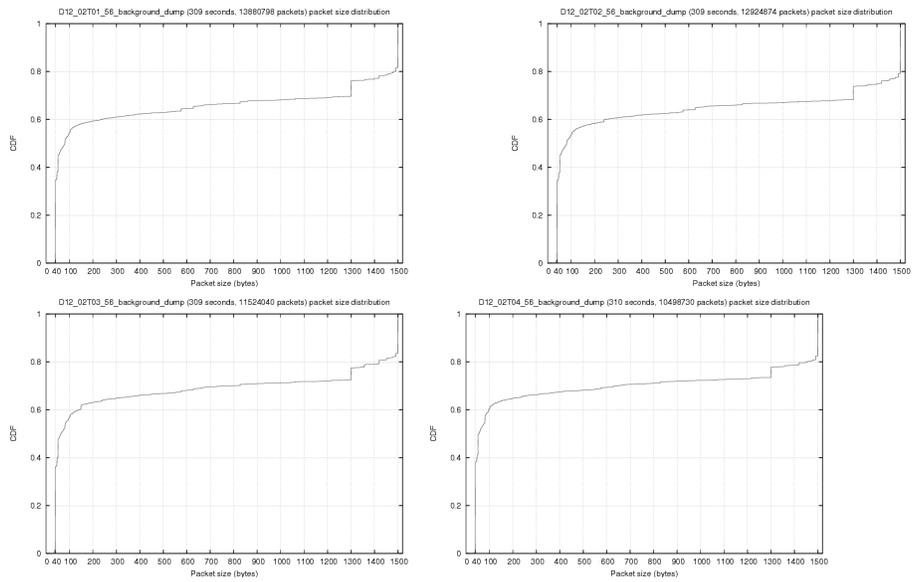


Figure 7: Supplementary traces from USC Internet2 at other times.

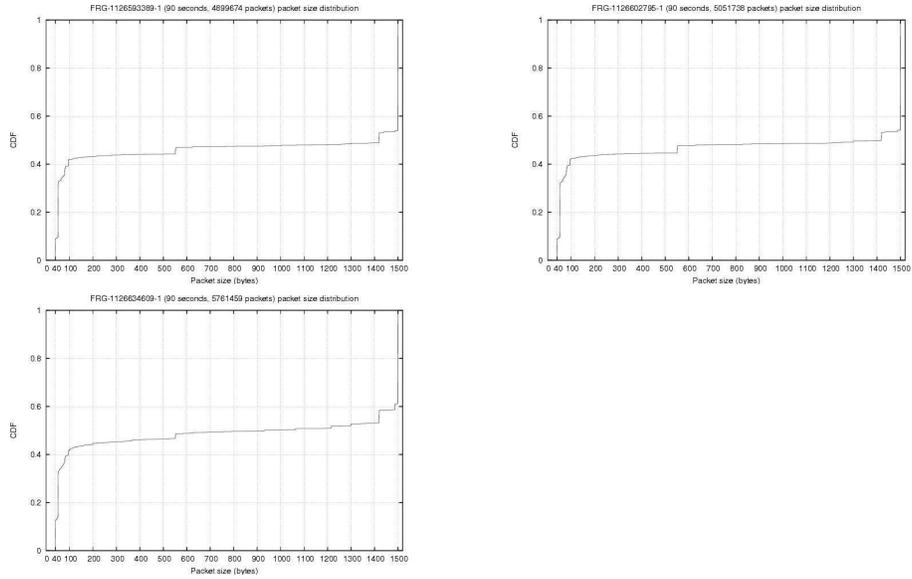


Figure 8: Supplementary traces from NLANR FRG (Front Range GigaPOP) at other times.

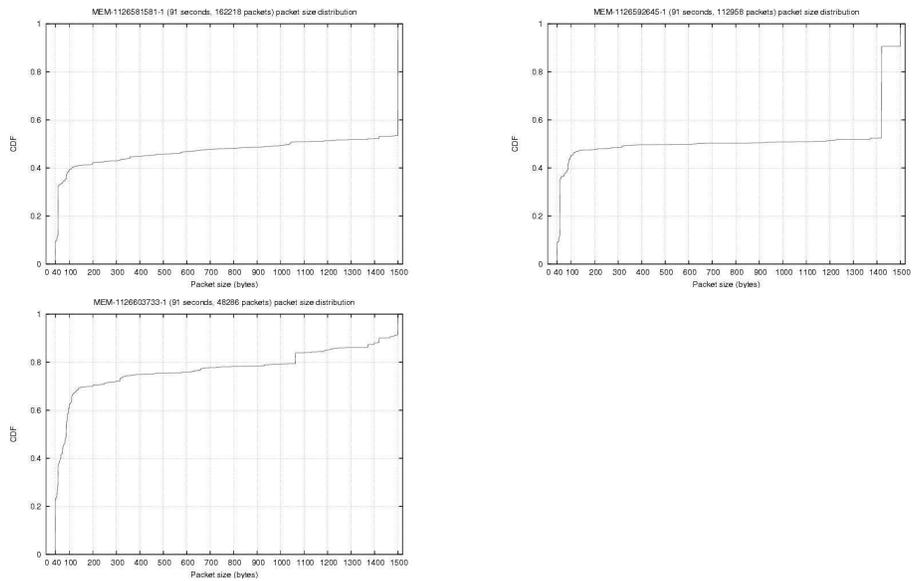


Figure 9: Supplementary traces from NLANR MEM (University of Memphis) at other times.

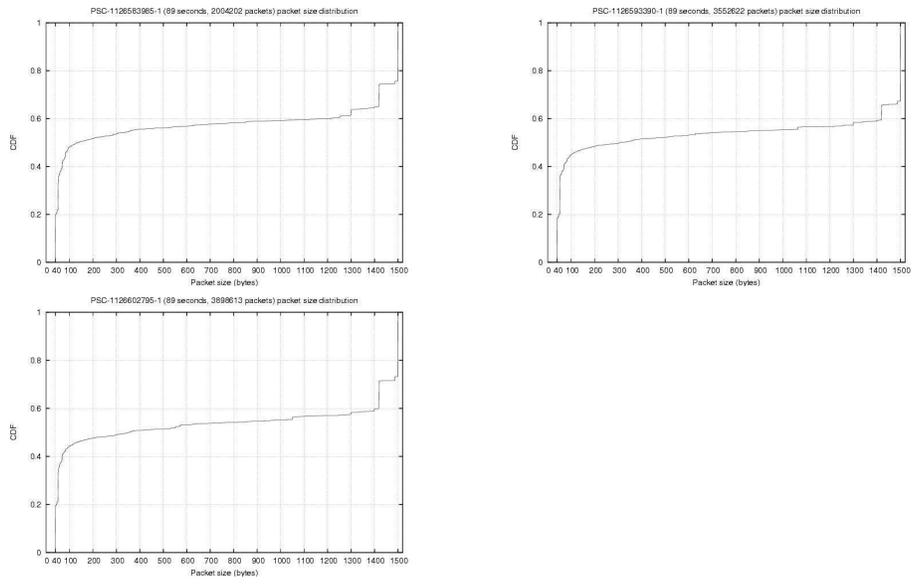


Figure 10: Supplementary traces from NLANR PSC (Pittsburgh Supercomputing Center) at other times.