

Duplicate packets

Pinging some hosts causes multiple responses for a ping echo request. This is reported by the Linux and Mac OSX ping command but not by Windows. For iPhones the results depend on the app, e.g. NetAnalyzer and Ping Lite do not show the DUPs, whereas Ping does. Typically from a RHEL6-64 Linux host (pinger.slac.stanford.edu, not using multicast, the interfaces are not bonded) at SLAC it appears as:

```
290cottrell@pinger:~$ping www.cern.ch
PING webrlb02.cern.ch (188.184.9.235) 56(84) bytes of data.
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=1 ttl=109 time=163 ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=1 ttl=109 time=163 ms (DUP!)
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=1 ttl=109 time=163 ms (DUP!)
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=2 ttl=109 time=163 ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=2 ttl=109 time=163 ms (DUP!)
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=2 ttl=109 time=163 ms (DUP!)
```

On a SunOS host it appears as:

```
290cottrell@flora04:~>ping -s www.cern.ch
PING www.cern.ch: 56 data bytes
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=0. time=166. ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=0. time=308. ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=0. time=308. ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=1. time=166. ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=1. time=166. ms
64 bytes from webrlb02.cern.ch (188.184.9.235): icmp_seq=1. time=166. ms
```

More examples of duplicate pings

Duplicate packets should never occur when pinging a unicast address, and seem to be caused by inappropriate link-level retransmissions. Duplicates may occur in many situations and are rarely (if ever) a good sign, although the presence of low levels of duplicates may not always be cause for alarm. Duplicates are expected when pinging a broadcast or multicast address, since they are not really duplicates but replies from different hosts to the same request. From <http://www.gsp.com/cgi-bin/man.cgi?section=8&topic=ping#4>

For a discussion of the reasons for duplicate pings see <http://unix.stackexchange.com/questions/13254/what-could-dup-mean-when-using-ping>. For PingER data several of the possibilities such as multicast, wireless network, promiscuous mode are unlikely to be the cause.

Duplicate ping responses can be seen for example from SLAC to [CERN](http://www.cern.ch) or www.realbroadband.co.sz. They can be caused by:

- More than one host has the same IP address, so all these hosts will respond to the ICMP echo request.
- The IP address pinged may be a broadcast address.
- The host has multiple TCP stacks bound to an Ethernet adaptor (see http://www.doxpara.com/read.php/tcp_chorusing.html).
- A router believes it has two routes by which it can reach the end host and (presumably mistakenly) forwards the ICMP echo requests by both routes, thus the end host sees two echo requests and responds twice.
- There maybe two or more (non-routed) paths to the end host and each request is forwarded by more than one path.
- It may be caused by NIC bonding (see <http://slashzeroconf.wordpress.com/2008/04/29/duplicate-ping-error-with-network-bonding-driver-in-linux/>).
- A misbehaving NAT box.

Some tests that may help include:

- Pinging the routers along the route to see if any of them respond with duplicates. Examples: Duplicate pings from SLAC to realimage.realnet.co.sz, www.lonab.bf.
- Capture the ping packets and look to see if all the packets are returned from the same Ethernet address. See the examples using [tcpdump](#) of [SLA C to CERN](#) and [SLAC to www.lonab.bf](#) where in both cases all responses are from the same IP address.
- Do multiple hosts at a site/network domain/subnet return duplicate packets? For example www.cern.ch (137.138.144.16) gives 3 pings in response to each one sent, while ping.cern.ch (137.138.28.176) and pinger.cern.ch (192.91.244.6) see no duplicate pings. CERN has a /16 IP network space 137.138.*.*

An example of the prevalence of duplicate ping packets comes from [PingER measurements on March 31st 2012](#) from SLAC to 703 hosts in over 160 countries. Of these hosts 15 responded with duplicate pings. For 13 of the 15 hosts it occurred on both 100 and 1000 Byte pings. Out of 10 pings sent:

- 6 hosts had 1 ping duplicated,
- 5 had 2 pings duplicated,
- 2 had 4 pings duplicated,
- 1 had 3 pings duplicated and
- 1 returned 12 pings for each ping sent.

The sites of the hosts range from national labs (CERN, IHEP SU), developed countries (Israel), developing countries (Burkina Faso, Malawi, Mauritius, Sierra Leone, Swaziland, Zambia), and educational sites (SDSC). Only the www.cern.ch address was consistent in the number and frequency of duplicate pings.

PingER simply reports whether there were duplicates or not. A useful metric is to report the *number of pings received/number pings sent*. The number received may depend on the ping command options. One option will send a given number of pings until it receives that many back or times out. Another option will send 10 pings and wait (or time out) until they are received. So the metric value may also depend on the ping command.

CERN

For each ping sent to www.cern.ch from pinger.slac.stanford.edu or ping.desy.de, perfsonar-unimas.myren.net.my (but not from pinger-host.fnal.gov, netmon.physics.carleton.ca) it responds with ~3 pings consistently. Using the normal traceroute www.cern.ch from SLAC does not respond. Using the ICMP traceroute it does respond (twice). [Pinging each node along the route](http://pingroute.pl) using pingroute.pl (<http://http://www-dev.slac.stanford.edu/cgi-wrap/scriptdoc.pl?name=pingroute.pl>) (unfortunately mtr does not report duplicates), it is seen that only www.cern.ch responds with duplicate packets. Also looking at the cpdump output is seen that only one IP address is responding.

A possible source is the Load Balancing of the CERN www server. SLAC also load balances (via F5s) its www server. However, the SLAC Load Balancer only forwards the http/https requests to the web servers, the pings are responded to by the F5 load balancer itself. Thus though we pinged www.slac.stanford.edu from ping.desy.de, we do not see any duplicate pings.

Analysis of data in Jan 2015

We have data capable of detecting duplicate pings from PingER, going back to 2005 which I have mined to look for DUP's. The input data is one line per set of pings made from SLAC to a remote host. The line indicates whether there were DUP's. Each line is for a remote host monitored from SLAC with up to 10 successful (with a cut off at 30 tries) 100 Byte pings each 30 mins.

We wrote a perl script (dupes.pl) to analyze the data.

The monitoring host (pinger.slac.stanford.edu) is not using multicast, the interfaces are not bonded. It is running Linux:

Linux pinger 2.6.32-279.19.1.el6.i686 #1 SMP Sat Nov 24 14:42:18 EST 2012 i686 i686 i386 GNU/Linux

- The current number of countries with remote hosts being monitored is 171.
- The number of remote hosts being monitored in 2014 is 836.
- Of these, 81 recorded 1 or more lines (samples) with duplicate pings.
- Of the 128 S. E. Asian hosts monitored from SLAC (number of hosts with DUPs / number of hosts monitored in country)

BN	IN	KH	LA	MM	MY	PH	SG	TH	VN
0/5	1/50	0/1	1.4	0/3	0/40	0/10	0/7	1/11	1/4

- The major contributor since 2006 has been www.cern.ch, each year we see about 60 different hosts responding with DUPs.
- A list of the hosts responding with DUP pings in 2014 is below, followed by a summary of the annual DUP pings.

List of hosts responding with DUPLICATE pings as seen from SLAC in 2014

- 2014: cbinet.bi seen duping 35 times
- 2014: internet.fo seen duping 6 times
- 2014: ms01.linea.gov.br seen duping 1 times
- 2014: ns.conacyt.gob.sv seen duping 3 times
- 2014: ping.cern.ch seen duping 450 times
- 2014: pinger.daffodilvarsity.edu.bd seen duping 2 times
- 2014: pinger.ictp.it seen duping 1 times
- 2014: pinger.numl.edu.pk seen duping 96 times
- 2014: pingerqta.pern.edu.pk seen duping 1 times
- 2014: www.acgrc.am seen duping 2 times
- 2014: www.afribone.net.gn seen duping 2 times
- 2014: www.afrinet.cd seen duping 8 times
- 2014: www.aic.ac.nz seen duping 1 times
- 2014: www.alard.ps seen duping 1 times
- 2014: www.bonesha.bi seen duping 73 times
- 2014: www.boz.zm seen duping 4 times
- 2014: www.cern.ch seen duping 14026 times
- 2014: www.cnrst.bf seen duping 43 times
- 2014: www.cyfronet.krakow.pl seen duping 1 times
- 2014: www.drtvnet.cg seen duping 12 times
- 2014: www.eritel.com.er seen duping 373 times
- 2014: www.gov.bw seen duping 635 times
- 2014: www.granma.cu seen duping 9 times
- 2014: www.hraparak.am seen duping 1 times
- 2014: www.ihep.su seen duping 1 times
- 2014: www.kcn.unima.mw seen duping 118 times
- 2014: www.lanl.gov seen duping 1 times
- 2014: www.lonab.bf seen duping 394 times
- 2014: www.lsx.com.la seen duping 1 times
- 2014: www.minzdrav.uz seen duping 12 times
- 2014: www.ml.refer.org seen duping 1 times
- 2014: www.nomad.mu seen duping 1 times
- 2014: www.rmutsy.ac.th seen duping 4 times
- 2014: www.rub.edu.bt seen duping 1 times
- 2014: www.stmaryuniversitycollege.edu.et seen duping 1 times
- 2014: www.uniswafoundation.org.sz seen duping 1 times
- 2014: www.univ-koudougou.bf seen duping 632 times
- 2014: www.univ-ouaga.bf seen duping 7 times
- 2014: www.uns.ac.id seen duping 2 times
- 2014: www.vnu.edu.vn seen duping 26 times
- 2014: www.vnuhcm.edu.vn seen duping 1 times

Summary of yearly data of DUP pings seen from SLAC

See [spreadsheet](#).

Year	DUPs	Hosts DUPing	Hosts monitored	Samples	%	CERN	Diff	% CERN
2005	93	27	481	11408092	0.0008%	0	93	0.00%
2006	9228	40	514	13715929	0.0673%	5751	3477	62.32%
2007	35673	42	541	16315320	0.2186%	34721	952	97.33%
2008	39262	57	592	19680482	0.1995%	34249	5013	87.23%
2009	42356	52	663	17889767	0.2368%	27469	14887	64.85%
2010	74638	51	623	19862304	0.3758%	19693	54945	26.38%
2011	30769	79	659	22889278	0.1344%	22518	8251	73.18%
2012	85217	50	797	23786399	0.3583%	34402	50815	40.37%
2013	74128	76	774	25475771	0.2910%	34916	39212	47.10%
2014	16990	41	836	29933696	0.0568%	14026	2964	82.55%
2015	164	4		514773	0.0319%	104	60	63.41%

Jan 1-Feb 14 2015

This data is for all monitors monitoring their set of remote sites every 30 minutes for the dates above. There are roughly 70 active monitors of which ~ 50% saw at least one remote host giving duplicate pings responses. There were 22 remote hosts responding with duplicate ping responses. There were roughly 720 remote hosts being probed with pings in over 170 countries. The remote hosts seen providing duplicate pings ordered in frequency of being seen is given in the table below. It is seen that apart from CERN (duplicates seen only from SLAC) the remote hosts with duplicate responses are outside N. America, Europe and Australia with the top 3 three being in Africa. For E. Asia the host in Taiwan (.tw) is seen once by pingermt.n.pern.edu.pk. the host in China (.cn) is seen once by SLAC.

Times remote host seen w 1 or more dups	Remote host
1099	www.univ-koudougou.bf
315	www.univ-ouaga.bf
263	www.gov.bw
235	shinjiru.com.my
70	pinger-ncp.ncp.edu.pk
68	www.kcn.unima.mw
44	www.multinet.af
37	www.cern.ch
24	www.kist.ac.rw
12	www.granma.cu
6	pinger.lcwu.edu.pk
2	ms01.linea.gov.br
2	www.ml.refer.org
2	www.stmaryuniversitycollege.edu.et
1	namunu.learn.ac.lk
1	cad.zju.edu.cn
1	www.unilag.edu.ng
1	dns.sinica.edu.tw
1	www.global.net.pg
1	www.nren.net.np
1	www.ubd.edu.bn
2186	Sum

[Spreadsheet](#)

Spreadsheet

