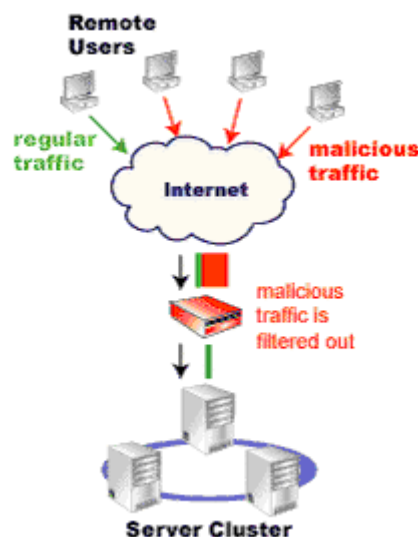


## Ping Flood (ICMP Echo) Detection



Ping Flood attacks attempt to saturate a network by sending a continuous series of ICMP echo requests (pings) over a high-bandwidth connection to a target host on a lower-bandwidth connection to cause it to send back an ICMP echo reply for each request. Ping Flood attacks can slow down a network or even disable network connectivity. Rate limiting ICMP traffic on customer access connections and at peering points are steps service providers can take to reduce Denial of Service (DoS) attacks that make use of ICMP messages.

Pinging involves one computer sending a signal to another computer expecting a response back. Responsible use of pinging provides information on the availability of a particular service. Ping Flooding is the extreme of sending thousands or millions of pings per second. Ping Flooding can cripple a system or even shut down an entire site.

A Ping Flooding Attack floods the victim's network or machine with IP Ping packets. At least 18 operating systems are vulnerable to this attack, but the majority can be patched. There are also numerous routers and printers that are vulnerable. Patches cannot currently be applied throughout a global network easily.

### Procedure

- Using a routing protocol, such as BGP-4, advertise a range of network prefixes on the destination test port.
- On the source test port, build a Ping Flood attack stream of IP packets containing ICMP echo request messages. (Optionally, the source IP address of the packets could also be spoofed.)



## Verify DUT's ability to block or limit attack stream

- Send a unicast Ping Flood attack stream to the DUT interface connected to the source test port, and verify that the DUT drops the packets. (Some routers may choose to forward ICMP echo messages at a limited rate instead.)
- Repeat the test, but send the attack traffic to the loopback address of the DUT.
- Repeat the test again, sending the traffic through the DUT to one of the addresses advertised behind the destination test port (i.e., the target host).

## Measure performance impact on background stream

- After ensuring that the router can block all three-attack streams, send a background stream containing normal traffic from the source test port, through the DUT, to the addresses advertised on the destination test port. Use a rate at which no packet loss is observed.
- Measure the total number of background packets transmitted and received, and their latency.
- In parallel with the background traffic, send a Ping Flood attack stream at an initial load to the target host on the destination test port.
- Measure the total number of background packets transmitted and received, and the latency or delay (if packet loss) during this attack.
- Increase the offered load of the Ping Flood attack stream by a user-defined increment and repeat the last two steps until the final load is reached.

## Variables

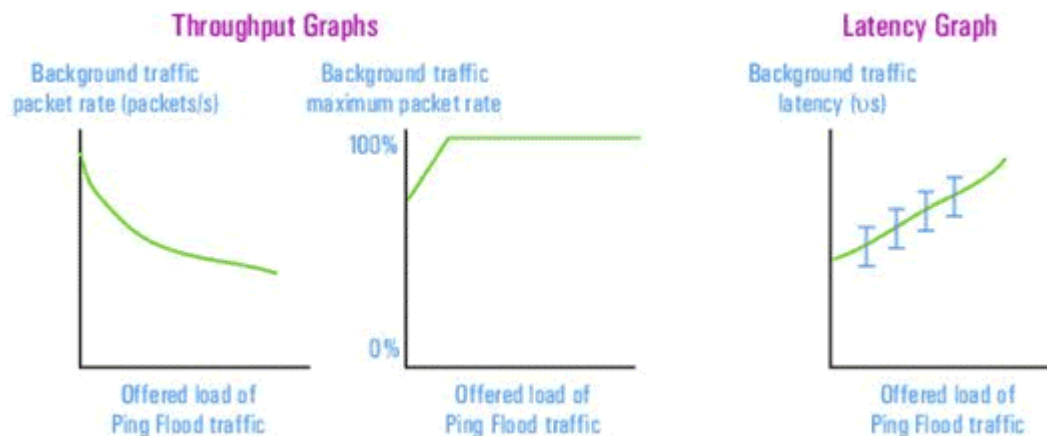
- Initial load of Ping Flood attack traffic.
- Increment by which Ping Flood attack load is increased.
- Final load of Ping Flood attack traffic.
- Background traffic load.
- Packet length of background traffic.
- Number of routes advertised.
- Number of hosts attacked.

## Results

For each test iteration, record the throughput, and the minimum, maximum, and average latency.

## Graphs

A sample Graph throughput and latency of the background traffic as functions of the Ping Flood traffic load is shown below.



**Dax Product Offering:**

Some of the Dax products that support "Ping Flood Detection" are listed below:

Dax BTI-0524GT/ BTI-0524GT-D:

[https://www.daxnetworks.com/Dax/Products/Switch/DTS\\_T5C\\_24G\\_24GT.htm](https://www.daxnetworks.com/Dax/Products/Switch/DTS_T5C_24G_24GT.htm)

Dax BTI-0524T/0548T/ 0548T-D-L3:

[https://www.daxnetworks.com/Dax/Products/Switch/DTS\\_T5C\\_24T\\_48T.htm](https://www.daxnetworks.com/Dax/Products/Switch/DTS_T5C_24T_48T.htm)

Dax BTI-0530 RN -L3:

[https://www.daxnetworks.com/Dax/Products/Switch/DTS\\_T5R.htm](https://www.daxnetworks.com/Dax/Products/Switch/DTS_T5R.htm)

Dax BTI-T6 Pro:

<https://www.daxnetworks.com/Dax/Products/switch/T6%20Pro%20Routing%20Switch.htm>

[CLICK HERE TO MAIL YOUR QUERY OR ORDER](#)

---

For complete Dax Product information, please visit: <https://www.daxnetworks.com/PFF.htm>

**GO PLACIDLY AMID THE NOISE AND HASTE**

If you have been forwarded this e-mail and wish to **recommend** this Newsletter, please [click here](#).

To **unsubscribe** to this Newsletter, please [click here](#).

[www.daxnetworks.com](http://www.daxnetworks.com)

© 2003 Dax Networks. All rights reserved.