ICMP


1. ICMP is a protocol that is used by routers and hosts to report back an error in datagram processing
2. ICMP runs on top of IP
ICMP Types

Time exceeded Message

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0 or 1</td>
</tr>
</tbody>
</table>

code 0 - time to live exceeded in transit (sent by routers)

code 1 - fragment reassembly on the host exceeded the time limit (sent by end-hosts)
ICMP Types

Insufficient Buffer capacity -

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

A gateway discards a packet because it has insufficient capacity to queue the packet in its buffer.
ICMP Types

Destination Unreachable

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0 or 1 or 2 or 3 or 4 or 5</td>
</tr>
</tbody>
</table>

0 = net unreachable; 1 = host unreachable;
2 = protocol unreachable; 3 = port unreachable;
4 = fragmentation needed and DF set; 5 = source route failed.

Codes 0, 1, 4, and 5 may be received from a gateway.

Codes 2 and 3 may be received from a host.
traceroute

A tool/program that uses ICMP packets to discover a path to a host

The tool uses two types of ICMP messages to discover this path.

1. Message Type 11 and Code 0 to check if TTL expired
2. Message Type 3 and Code 3 to check if the host has been reached.
Homework 6

Write a traceroute program and find the route that packets take while traveling toward hosts such as -

- www.ucsd.edu
- www.cs.ucsd.edu
- www.utexas.edu
- www.vit.ac.in
- www.ntu.edu.sg
- www.ethz.ch
- www.google.com
- www.bing.com
- www.facebook.com
For each server find the IPs of all the hops and the number of hops. The source will be **AWS instances** in two different locations

1. US West (Oregon)
2. Seoul

Repeat the experiment after a day/few hours and see if the routes changed
Scapy

A library for packet manipulation -

1. traceroute
2. Probing - testing your end-hosts for vulnerabilities
3. Trying various attacks on your network by sending invalid frames, etc.

https://scapy.net/

Download using -

pip3 install scapy
Traceroute using scapy

```python
from scapy.all import *
hostname = "google.com"
for i in range(1, 28):
    pkt = IP(dst=hostname, ttl=i) / UDP(dport=33434)
    # Send the packet and get a reply
    reply = sr1(pkt, verbose=0)
    if reply is None:
        # No reply =(
        break
    elif reply.type == 3:
        # We've reached our destination
        print "Done!", reply.src
        break
    else:
        # We're in the middle somewhere
        print "%d hops away: " % i, reply.src
```

Source: [https://jvns.ca/blog/2013/10/31/day-20-scapy-and-traceroute/](https://jvns.ca/blog/2013/10/31/day-20-scapy-and-traceroute/)
Stacking

1. The `\` operator is used as a composition operator between two layers.
2. It allows you to define the packet in different layers

   full_packet = IP(dst="hackerschool.com", ttl=10) / UDP(dport=40000)

An IP packet with dst address, ttl etc.

A UDP packet on top with destination port = 40000

Send and Receive

1. The sr() function sends and receives packets.
2. sr1() - return only one packet that replied to the packet sent.

Internet Routes

The “End-to-End Routing Behavior in the Internet” paper measures several behaviours and pathologies about internet routes.

1. Prevalence - the overall likelihood that a particular route is encountered
2. Persistence - likelihood that a route remains unchanged over time

Pathologies

1. Routing Loops
2. Erroneous Routing
3. Infrastructure Failures
Questions?