ICMP

Used by ping and traceroute

Level 3 protocol that must ride on an IP header

Frame Header|IP Header|ICMP info|FCS

ICMP messages

To support ICMP requests, the devices along the path to the target device must allow ICMP requests to be forwarded.

Query messages

See if a service is available at an endpoint

The numbers below are ICMP numbers (types).

There are 256 numbers

Most are deprecated

1-2, 4, 6-7, 9-10, 12, 15-254

If you see these, you may be under attach

ICMP requests and responses can be tied together by sequence.

The response seqno will match the initial request seqno.

For each successive ping request, the seqno will increment by 1

Echo

Hey device, are you there?

Request - 8

Reply - 0

Used in ping

Timestamp

Hey, what’s your time? (UTC time)

Request - 13

Reply - 14

Error messages

A device may not be able to forward a request to target device

The device may respond with an ICMP error message if ICMP is enabled on that device.

Three types

Dest unreachable(3)

16 diff subcodes

4 most used

0 network unreachable

No route path to that device

1 host unreachable

Self generated by our workstation itself, so not usually seen in the network

Happens when the ip requested doesn’t exist

ARP request can’t be resolved to a hardware address.

Doesn’t typically show up in wireshark since it’s not actually sent from the network.

2 protocol unreachable

Layer 3

A device doesn’t support the request protocol

3 port unreachable

Layer 4 protocol

4-15 Uncommon

Redirect (5)

Informational thing telling your workstation that in the future, start sending requests directly to the router from which this message was sent.

Sent when a client sends a message to one router, but the router has no routes to the target but has a route to another router that does have a route to the target.

Time exceeded (11)

Allows a receiving router to send message back to requesting device telling the client that the router is throwing away the message since the ttl has expired.

Ttl is the number of routers a message has passed through

Indicative of a routing loop or purposeful generation of a ttl to force this message.

We may want a low ttl to support displaying devices through which messages are flowing.

Many routers / firewalls are configured not to support throwing ECMP messages

Triggered when message is received having ttl = 0

## Traceroute Utilities

A utility that makes use of ICMP features, specifically ICMP error messages

Windows : ICMP messages

Mac / Linus : Sends UDP messages

Router receiving a message having ttl 1 will reduce it to 0 and respond with a time exceeded message containing the src ip address (address on the router that received the message) and the time it took

Traceroute sends incrementally increasing ttl messages, generating a consecutive list of error messages containing the src ip and time received

Default ttl is 128

Good for

Determining a path through your network

Identifying routing loops

Bad for

Determining whether or not a device is online

Better to use ping

Not always useful since ICMP isn’t always turned on on all points in a network

### Discover networks

IP

Network layer protocol

Data is wraped in frames

Wireshark

Filter traffic to only include certain protocols

Add a filter named icmp

If you select a frame, Wireshark displays headers for all protocol layers

For ICMP, displays physical, data-link, and ip, then following that, the ICMP-specific header info

Terms

ICMP

Internet control message protocol

ARP Request

Used by IP to map an ip address to a hardware address

Ttl

Number of routers a message can hop across