**ICMP**

**Internet Control Message Protocol**

* Error reporting protocol for nodes
* Contains a large amount of error messages
  + Commonly used for ping

**Common error responses**

* Echo reply/request
* Destination unreachable
  + Router can’t find dst or IP
* Redirect message
* Router advertisement
* Time exceeded
* Timestamp
* Traceroute

**Ping**

* Commonly used to test if an IP is online
* Client will send the Echo request ICMP packet
* Server/End-node will respond with Echo Reply if its available
* The router will reply Destination Unreachable if the IP is not alive
* Cmd (Windows & Linux): ping IPADDRESS

Data *is* sent over a ping though

HW – find out what data this is

**Traceroute**

Commonly used to trace a packet through hops on a network

Client will send an outdated ICMP traceroute packet to its dst

* This type of message will keep track of each hop it hits before it reaches the end
  + An outdated packet will get ‘kickbacked’
  + For the second hop, it’ll send 2 outdated packets to get kicked back
  + A packet will be kicked back at every hop the packet makes
  + When it finally reaches its end hop, it will be printed and a traceroute showing all hops (that in initiated a kickback) in the path of the packet
* Note that a missing IP or hostname normally indicates a firewall of some kind