ICMP Protocol and Its Security

1 ICMP Protocol (Internet Control Message Protocol

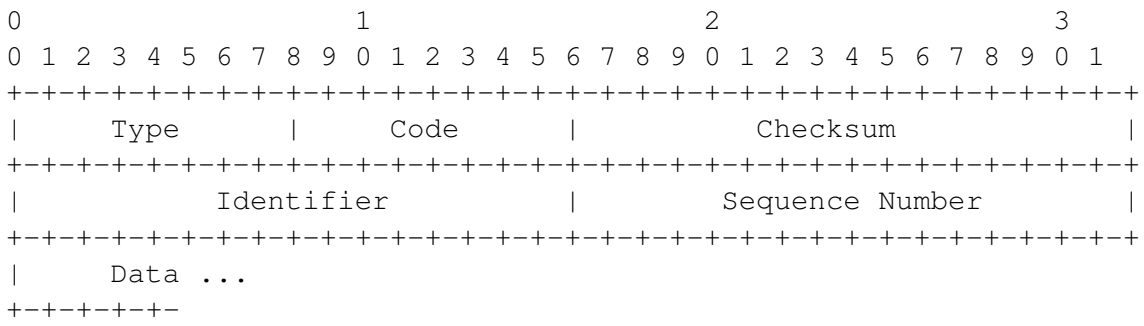
- Motivation
  - IP may fail to deliver datagrams because
    - the destination is not available
    - the time-to-live counter expires
    - routers become congested
  - We need to let the sender know what has happened
  - ICMP is a required part of IP
- Purpose
  - ICMP allows routers (and hosts) to send error or control messages to other routers or hosts
  - ICMP provides communication between the Internet Protocol software on one machine and the Internet Protocol software on another
- Restrictions
  - ICMP messages are not generated for errors that result from datagrams carrying ICMP error messages. Why?
  - ICMP is only sent to the original source. Why?
- ICMP Encapsulation
  - ICMP is encapsulated in an IP packet, but is considered part of the IP or Internet layer.

2 ICMP Messages

- The Common ICMP header
  - Each ICMP message has its own format, they all begin with the same three fields
  - TYPE (8-bit): identifies the message
  - CODE (8-bit): provides further information about the message type
  - CHECKSUM (16-bit)
  - In addition, ICMP messages that report errors always include the header and the first 64 data bits of the datagram causing the problem.
- ICMP Message TYPE
  - 0: Echo Reply
  - 3: Destination Unreachable
  - 4: Source Quency

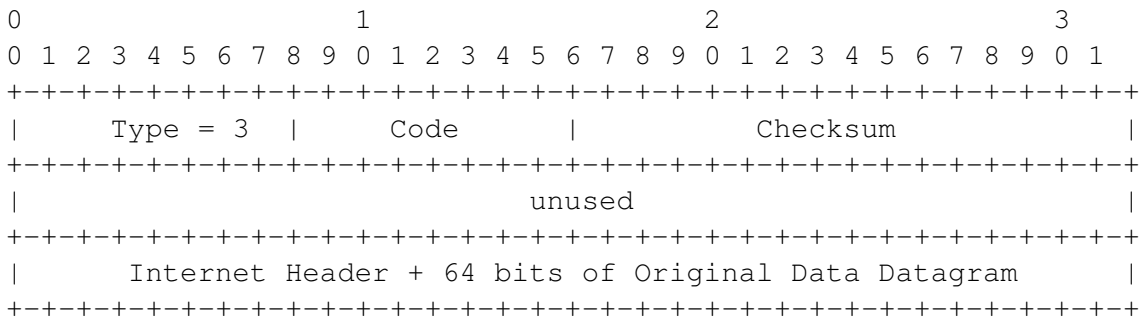
  - 5: Redirect (chage a route)
  - 8: Echo Request
  - 9: Router Advertisement
  - 10: Router Solicitation
  - 11: time Exceeded for a Datagram
  - 12: Parameter Problem on a Datagram
  - 13: timestamp Request
  - 14: Timestamp Reply
  - 17: Address Mask Request
  - 18: Address Mask Reply

- Echo request and reply message (TYPE = 8 and TYPE = 0)
  - Used to test reachability
  - The format of echo request/reply packets is the following:



  - An echo request can also contain optional data (the content does not matter).
  - An echo reply always returns exactly the same data as was received in the request.
  - ICMP echo request/reply messages are used by the `ping` program.

- Destination Unreachable (TYPE = 3)
  - When a router cannot forward or deliver an IP datagram, it sends a destination unreachable message back to the original source.
  - The format of the packet is the following:



  - The CODE field specifies details

    - 0: network unreachable
    - 1: host unreachable
    - 2: protocol unreachable
    - 3: port unreachable
    - 4: fragmentation needed and DF (dont fragment) 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.
  - The IP header plus the first 64 bits of the original packet is attached in this ICMP packet.

- Source Quench
  - To deal with congestion and datagram flow control
  - When routers are overrun with traffic, it is called congestion.
  - A machine uses ICMP source quench messages to report congestion to the original source
  - There is no ICMP message to reverse the effect of a source quench. Usually the host gradually increases the rate when no further source quench requests are received.

- Route Redirect
  - The format of the ICMP route redirect message:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Gateway Internet Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Internet Header + 64 bits of Original Data Datagram      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

  - Routers exchange routing information periodically to accommodate network changes and keep their routes up-to-date. However, hosts do not do this.
  - A general rule:
    Routers are assumed to know correct routes; hosts begin with minimal routing information and learn new routes from routers.
  - IP hosts are typically only configured with an IP address of a default router (also called a default gateway). Any remote traffic from the IP host is forwarded to the default IP router.
  - When a router detects a host using a nonoptimal route, it sends the host an ICMP redirect message, requesting that the host change its route. This way, the host learn a new route, and add the route to its routing table.
  - The gateway sends a redirect message to a host in the following situation. A gateway, G1, receives an internet datagram from a host on a network to which the gateway is attached. The gateway, G1, checks its routing table and obtains the address of the next gateway, G2, on the route to the datagram's internet destination network, X. If G2 and the host identified by the

internet source address of the datagram are on the same network, a redirect message is sent to the host. The redirect message advises the host to send its traffic for network X directly to gateway G2 as this is a shorter path to the destination. The gateway forwards the original datagram's data to its internet destination.

- Limited to interactions between a router and a host on a directly connected network.

3 Attacks Using ICMP Messages

- Mapping Network Topology
  - Mapping a target network is a very strategic part of most intelligently planned attacks. This initial step in reconnaissance attempts to discover the live hosts in a target network. An attacker then can direct a more focused scan or exploit toward live hosts only.
  - Sending individual ICMP echo: this is what the ping command does.
  - Sending ICMP echo requests to the broadcast addresses of a network.
  - Sending ICMP echo requests to network and broadcast address of subdivided networks
  - Sending an ICMP address mask request to a host on the network to determine the subnet mask to better understand how to map efficiently.
- Smurf Attack
  - Ping an IP-directed broadcast address, with the (spoofed) IP of a victim as the source address.
  - IP-directed broadcast addresses are usually network addresses with the host portion of the address having all one bits. For example, the broadcast address for subnet `192.168.10.0` is `192.168.10.255`).
  - Until 1999, standard required routers to forward such packets.
  - Impact: All hosts on the network will respond to the victim, and thus overwhelm the victim. This is a denial-of-service attack.
  - ICMP echo just used for convenience. All ICMP messages can be abused this way.
  - The key idea of this attack: Amplification and IP spoofing
  - This is a protocol vulnerability. To solve this problem, we can do the following:
    - Disable IP-directed broadcasts at the router.
    - Configure the operating system to prevent the machine from responding to ICMP packets sent to IP broadcast addresses.
- ICMP Redirect Attack
  - Send an ICMP redirect packet to the victim, asking it to send its packets to another "router", which can be a malicious machine.
  - Impact: man-in-the-middle attacks or denial-of-service attacks.
  - Host Requirements RFC states that system MUST follow ICMP redirects unless it's a router.
  - Winfreez(e): in Windows.
    - ICMP Redirect: Yourself is the quickest link to host Z.
    - The victim changes its routing table for Z to itself.

    - Host sends packets to itself in an infinite loop.

- Ping of Death
  - ICMP echo request with fragmented packets
  - Maximum legal size of an ICMP echo request packet:
    65535 - 20 - 8 = 65507
  - Fragmentation allows the bypass of the maximum size. For the last piece of the fragment, the following is possible:
    (offset + size) $>$ 65535
  - Reassembled packet would be larger than 65535 bytes.
  - Impact: some operating systems will crash.
  - Same attack with different IP protocols.
- ICMP attacks on TCP connections (more will be covered in the TCP lectures).