CS307-f20
Computer Networks
Assignment 4

SYED ASAD ZAMAN
p180034(B)

January 28, 2020

Internet Control Message Protocol(ICMP)

1 Introduction and Overview

The Internet Protocol (IP) is used for host-to-host datagram service in a system of interconnected networks called the Catenet. The network connecting devices are called Gateways. These gateways communicate between themselves for control purposes via a Gateway to Gateway Protocol (GGP). Occasionally a gateway or destination host will communicate with a source host, for example, to report an error in datagram processing. For such purposes this protocol, the Internet Control Message Protocol (ICMP), is used. ICMP, uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module.
ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.

2 Application

2.1 Error Handling

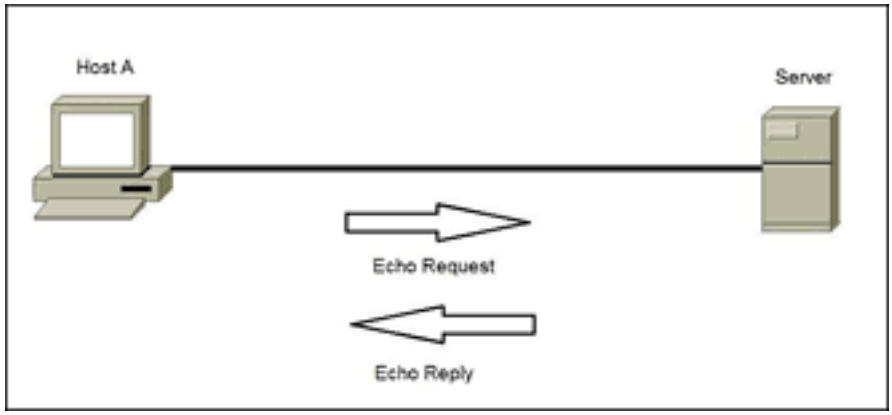
The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable. There are still no guarantees that a datagram will be delivered or a control message will be returned. Some datagrams may still be undelivered without any report of their loss. For that purpose the ICMP is used which send a message to the sender that the particular packet is undelivered provided with the information of which packet is discarded and by which router

2.1.1 Note:

The ICMP messages typically report errors in the processing of datagrams. To avoid the infinite regress of messages about messages etc., no ICMP messages are sent about ICMP messages. Also ICMP messages are only sent about errors in handling fragment zero of fragemented datagrams. (Fragment zero has the fragment offeset equal zero).

2.2 Request and Reply

The ICMP protocol is also used in the **Request and Reply** . It can be used either for requesting a specific packet or it can be used for **Ping** purpose inorder to check the connection.



2.2.1 Ping Responses

The ICMP echo request and the ICMP echo reply messages are commonly known as ping messages. Ping is a troubleshooting tool used by system administrators to manually test for connectivity between network devices, and also to test for network delay and packet loss. The ping command sends an ICMP echo request to a device on the network, and the device immediately responds with an ICMP echo reply. Sometimes, a company's network security policy requires ping (ICMP echo reply) to be disabled on all devices to make them more difficult to be discovered by unauthorized persons.

2.3 Source Quench

A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. If a gateway discards a datagram, it may send a source quench message to the internet source host of the datagram. A destination host may also send a source quench message if datagrams arrive too fast to be processed. The source quench message is a request to the host to cut back the rate at which it is sending traffic to the internet destination. The gateway may send a source quench message for every message that it discards. On receipt of a source quench message, the source host should cut back the rate at which it is sending traffic to the specified destination until it no longer receives source quench messages from the gateway. The source host can then gradually increase the rate at which it sends traffic to the destination until it again receives source quench messages

2.4 ICMP Header

The ICMP header looks like this:

```
    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             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           unused                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Internet Header + 64 bits of Original Data Datagram      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
Type

   3



Code

   0 = net unreachable;

   1 = host unreachable;

   2 = protocol unreachable;

   3 = port unreachable;

   4 = fragmentation needed and DF set;

   5 = source route failed.

Checksum

   The checksum is the 16-bit ones's complement of the one's
   complement sum of the ICMP message starting with the ICMP Type.
   For computing the checksum , the checksum field should be zero.
   This checksum may be replaced in the future.

Internet Header + 64 bits of Data Datagram

   The internet header plus the first 64 bits of the original
```

3 Mobile IP

Introduction

The standard communications protocol designed to allow mobile devices users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

Components

Following components that are used in **Mobile IP:**

Mobile Node:

A node running the Mobile IP protocol stack which moves between different IP subnets. This node is assigned a (permanent) IP address which defines where all its packets should be sent. When other nodes send packets to the mobile node, they only specify this home IP address in the packet, regardless of where the mobile node is physically located.

Home Network:

The subnet which corresponds to the home address of the mobile node as well as that of the home agent. It is considered the mobile node's "home" point of attachment

Home Agent:

A router on the home network that is responsible for intercepting packets destined for the mobile node when the mobile node is attached to a foreign network. The home agent is responsible for forwarding these packets to the mobile node.

Foreign Network

A network, other than the mobile node's home network, that a mobile node attaches itself to.

Foreign Agent

A router on the foreign network configured for Mobile IP. When the mobile node has a foreign agent care-of address all packets are relayed through this node. When using a collocated care-of address, the mobile node may still use a foreign agent for its default router or for registration with the foreign network

Correspondant Node

Any host which is communicating with the mobile node. This node could be located on the home network, foreign network, or any other place which is able to route packets to the mobile node's home network.

Tunneling

The process of encapsulating an IP packet within another IP packet for the purpose of routing it to a location other than the one specified in the original destination field. Specifically, when a packet is received by the home agent, it encapsulates the original packet inside a new packet, placing the mobile node's care-of address in the new destination address field before forwarding it to the appropriate router. The path that is followed by this new packet is called the *tunnel*.

Working

Correspondent node sends the data to the mobile node. Data packets contains correspondent node's address (Source) and home address (Destination). Packets reaches to the home agent. But now mobile node is not in the home network, it has moved into the foreign network. Foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.

Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

Now, home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on other side of the tunnel receives the data packets, decapsulates them and sends them to the mobile node. Mobile node in response to the data packets received, sends a reply in response to foreign agent. Foreign agent directly sends the reply to the correspondent node.

3.1 Applications

In many applications (e.g., VPN, VoIP), sudden changes in network connectivity and IP address can cause problems. Mobile IP was designed to support seamless and continuous Internet connectivity.

Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. Examples of use are in roaming between overlapping wireless systems, e.g., IP over DVB, WLAN, WiMAX and BWA.

Mobile IP is not required within cellular systems such as 3G, to provide transparency when Internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different packet data serving node (PDSN) domains.