CSC465 – Computer Networks

Dr. J. Harrison

These slides were produced almost entirely from material by Behrouz Forouzan for the text "TCP/IP Protocol Suite (2nd Edition)", McGraw Hill Publisher

Chapter 9

Internet Control Message Protocol (ICMP)

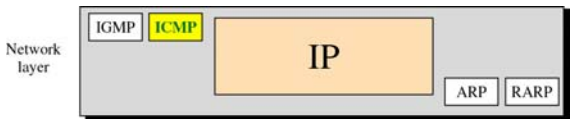
CONTENTS

ICMP

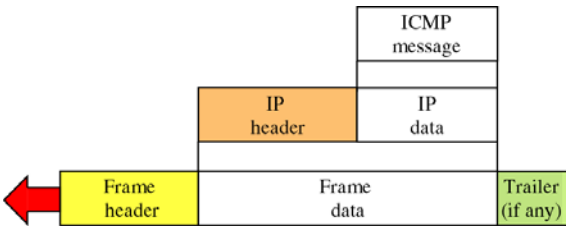
- IP unreliable, connectionless datagram delivery
  - Efficient use of network resources
  - Best effort service to send from source to destination
- No error control
  - What if router must discard datagram because it cannot find route to final destination?
  - What if final destination must discard all fragments because some don't arrive within time limit?
  - Error has occurred and IP Protocol has no built-in mechanism to notify the original host
- No method to obtain node information
  - Is router or host alive?

ICMP

ICMP addresses IP deficiencies



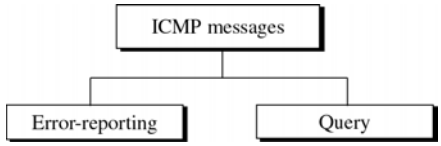
Encapsulation of ICMP packet



Value of protocol field in IP datagram is 1 to indicate data is ICMP

9.1 TYPES OF MESSAGES

ICMP messages

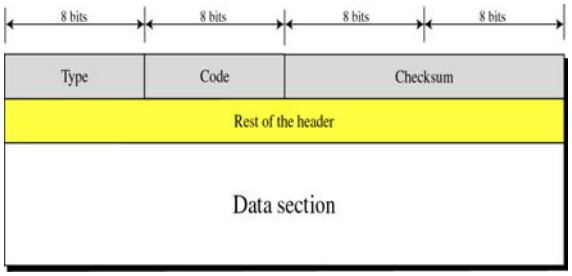


3 Dest Unreachable
4 Source Quench
11 Time Exceeded
12 Parameter Problem
5 Redirection

8 / 0 Echo Request/Reply
13 / 14 Timestamp Req/Reply
17 / 18 Address Mask
10 / 9 Router Solicitation

9.2 MESSAGE FORMAT

General format of ICMP messages



First 4 bytes common to all ICMP messages

Code specifies reason for particular message type

9.3 ERROR REPORTING

ICMP

- ICMP reports errors
- Higher protocols must correct them
- ICMP always reports error messages to the original source
- Source address within IP datagram

Error-reporting messages

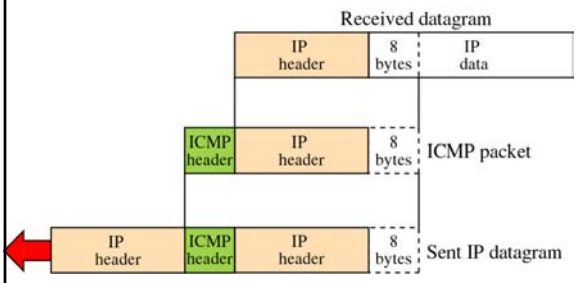
ICMP handles five (5) types of errors

- Destination unreachable
- Source Quench
- Time exceeded
- Parameter Problem
- Redirection

Important points about ICMP error messages:

1. ***No ICMP error message for a datagram carrying an ICMP error message.***
2. ***No ICMP error message for a fragmented datagram that is not the first fragment.***
3. ***No ICMP error message for a datagram having a multicast address.***
4. ***No ICMP error message for a datagram with a special address such as 127.0.0.0 or 0.0.0.0.***

Contents of data field for error messages



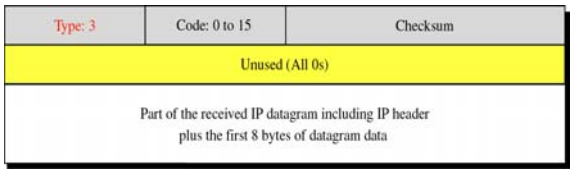
8 bytes UDP (TCP) header

(Source/Dest ports, length, checksum)

Destination-unreachable format

When a **router cannot route a datagram** the datagram is discarded and the router sends a "destination unreachable" message back to source host.

When a **host cannot deliver a datagram**, the datagram is discarded and the destination host sends a "destination unreachable" message back to source host.



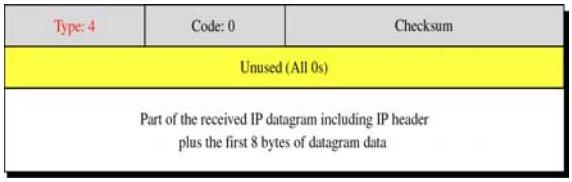
- 0: Net Unreachable
- 1: Host Unreachable
- 2: Protocol Unreachable
- 3: Port Unreachable
- 4: Frag Needed but "Don't Frag" was Set
- 5: Source Route Failed
- 6: Dest. Net Unknown
- 7: Dest. Host Unknown
- 8: Source Host Isolated
- 9: Communication with Dest Net is Admin Prohibited
- 10: Communication with Dest Host is Admin Prohibited
- 11: Dest Net Unreachable for Type of Service
- 12: Dest Host Unreachable for Type of Service
- 13: Communication Administratively Prohibited
- 14: Host Precedence Violation
- 15: Precedence cutoff in effect

Destination-unreachable messages with codes 2 or 3 can be created only by the destination host. Some destination-unreachable messages can be created only by routers.

Source Quench

- IP offers no inherent support to guide flow control
- The source host does not know if the routers or dest host have been overwhelmed with datagrams
- Lack of flow control can create congestion in routers or destination host
  - Router forwarding buffers may overflow
  - Host processing buffers may overflow
- Source Quench messages in ICMP
- Routers or hosts that discard packets sends SQ
  - Informs source of discarding; warns source of speed

Source-quench format



Note

A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host.

The source must slow down the sending of datagrams until the congestion is relieved.

One source-quench message should be sent, from router or destination host for each datagram that is discarded due to congestion.

- There is no mechanism for telling source that congestion is relieved and transmission can resume at previous rate.
- Source continues to send at reduced rate.
- If transmission is many-to-one, the destination may drop packets from slower sending host but not those from faster (congestion causing) senders.

Time Exceeded Message

Sent in two cases:

Case 1:

Whenever a router receives a datagram with a time-to-live value of zero, it discards the datagram and sends a time-exceeded message to the original source.

Time Exceeded Message

Sent in two cases:

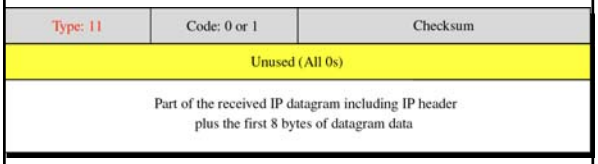
Case 2:

When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.

Time Exceeded Message

In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero. Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time.

Time-exceeded message format



Code 0: Time to live
Code 1: Fragmentation

Parameter-problem message format

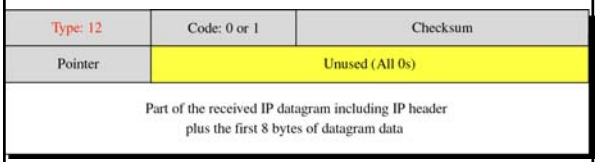
Error or ambiguity in one of the header fields (Code 0)

Required part of an IP option is missing

(Code 1)

A parameter-problem message can be created by a router or the destination host.

Parameter-problem message format



Code 0: Ptr field points to problem byte
Code 1: Ptr field unused

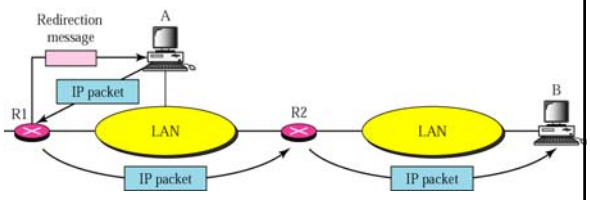
ICMP Redirection

- Router's routing tables updated dynamically using routing protocols
  - Hosts don't participate (for efficiency) since many more hosts than routers
- Hosts usually use static routing
  - Can result in misrouted datagram
  - In this case the recipient router forwards datagram to correct router
  - Sends ICMP "redirection" message to sending host to update its routing table

Note

A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.

Redirection concept



A redirection message is sent from a router to a host on the same local network.

Redirection message format

Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Code 0: Network specific
Code 1: Host specific
Code 2: Network specific (specified service)
Code 3: Host specific (specified service)

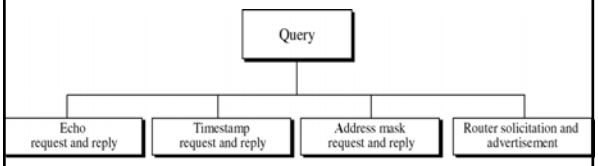
9.4

QUERY

Query messages

In addition to error detection, ICMP can also diagnose some network problems

Uses query/response system



Echo Request / Reply

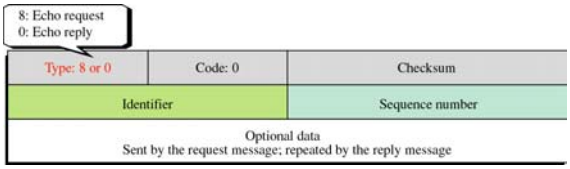
- Used by network managers and users for diagnosing network problems
- Tests if IP stack functioning on destination and routers in between
- Tests for the "reachability" of a host
- Used to implement the PING command
  - **Packet INternet Groper**

An echo-request message can be sent by a host or router.

An echo-reply message is sent by the host or router which receives an echo-request message

Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol..

Echo-request and echo-reply message format



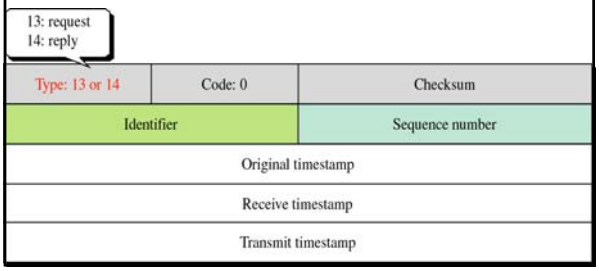
- Optional Data must be returned exactly as sent
- Identifier and Sequence # not formally defined
- Identifier often Process ID of sender
- Sequence # keeps track of particular request/reply

Timestamp Request/Reply

- Used by two machines to determine the roundtrip time for an IP datagram to travel between them
- Also used to synchronize the clocks in two machines
- Format contains three timestamps, each 32-bits
- Represents time (in milliseconds) from midnight in Universal Time (formerly GMT)

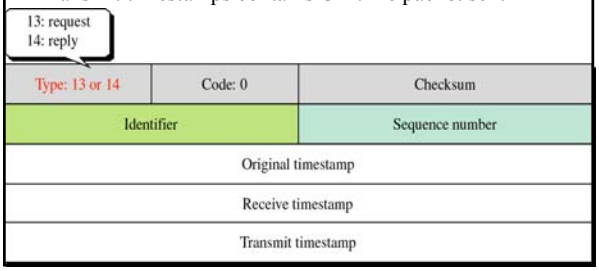
Timestamp-request format

- Original Timestamp receives Univeral Time shown by clock at departure time
- Receive/Transmit timestamps initialized to 0s



Timestamp-reply format

- Original Timestamp receives value copied from request
- Receive timestamp contains UT time dest received packet
- Transmit timestamps contains UT time packet sent



Sending time = value of receive timestamp – value of original timestamp

Receiving time = time the packet returned – value of transmit timestamp

Round-Trip Time = Sending time + Receiving time

The Round-Trip Time computation correct even if their clocks are not synchronized.

Mask-request and mask-reply message format

- Used by Host to obtain its IP address mask
- Host sends request to router if it knows IP of router
- If not, host broadcasts request and then router replies
- Diskless workstations use RARP to first get IP
- Then use ICMP Mask-request to get address mask

Router solicitation message format

Hosts need to know addresses of routers

Request broadcast by host to obtain the operating routers

Routers reply with all routers they are aware of including themselves (Sometimes reply without request)

Type: 10	Code: 0	Checksum
Identifier		Sequence number

Router advertisement message format

Preference level is used to select default router

If pref level is 0 then it is default. If level is 0x80000000 never selected as default

Type: 9	Code: 0	Checksum
Number of addresses	Address entry size	Lifetime
Router address 1		
Address preference 1		
Router address 2		
Address preference 2		
• • •		

9.5 CHECKSUM

Example of checksum calculation

8	0	0
1		9
TEST		

8 and 0	→	00001000 00000000
0	→	00000000 00000000
1	→	00000000 00000001
9	→	00000000 00001001
T & E	→	01010100 01000101
S & T	→	01010011 01010100
Sum	→	10101111 10100011
Checksum	→	01010000 01011100

9.6 ICMP PACKAGE

ICMP package