Lab 5 Internet Control Messages Protocol (ICMP)

1. The Introduction of ICMP

The IP provides unreliable and connectionless datagram delivery. It was designed this way to make efficient use of network resources. The IP protocol is a best-effort delivery service that delivers a datagram from its original source to its final destination. However, it has two deficiencies: lack of error control and lack of assistance mechanisms. The Internet **Control Message Protocol** (**ICMP**) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol. ICMP messages are divided into two broad categories: **error-reporting messages** and **query messages (or informational messages)**. Like the Internet Protocol, ICMP is also unreliable and the message of ICMP may lose as well. For unlimited ICMP message, ICMP error-reporting message will not be sent if error happens during transmitting ICMP error messages.

2. The Format of ICMP Datagram

An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all. As Figure 4-1 shows, the first field, *ICMP type*, defines the type of the message. The *code* field specifies the reason for the particular message type. The last common field is the *checksum* field. The rest of the header is specific for each message type.

The data section in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the query.

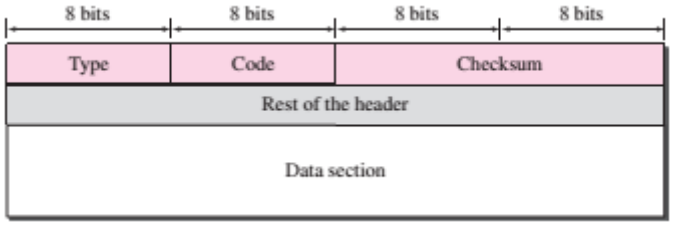

Figure 4-1 General format of ICMP messages

Type: 8-bits, used to define the type of the particular message

Code: 8-bits, used to specify the detailed illustration of ICMP packet

Checksum: 16-byte, used to verify this ICMP message

3. ICMP Encapsulation

An ICMP packet is encapsulated in an IP datagram as follows:

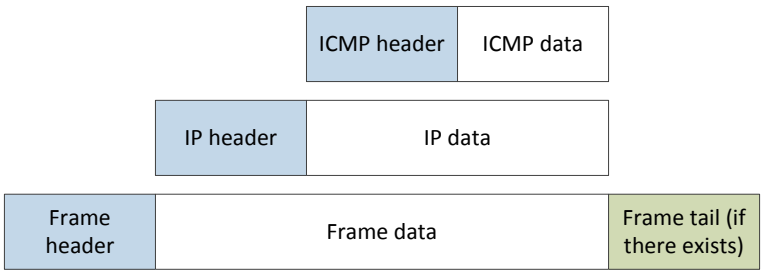

Figure 4-2 ICMP Encapsulation

4. Types of ICMP

ICMP messages are divided into two broad categories: *error-reporting messages* and *query messages*.

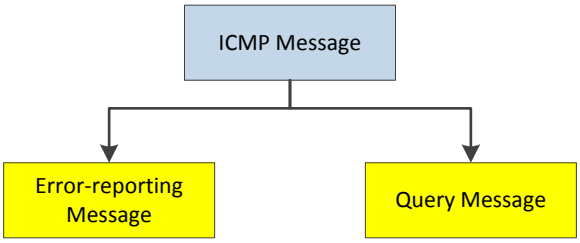

Figure 4-3 Types of ICMP

The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network, and routers can help a node redirect its messages.

Table 4-1 ICMP message

Category	Type	Message
Error-reporting message	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirect message
Query message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router advertisement or solicitation

5. ICMP Query Message

ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages, as shown in Figure 4-4. In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node. A query message is encapsulated in an IP packet, which in turn is encapsulated in a data link layer frame.

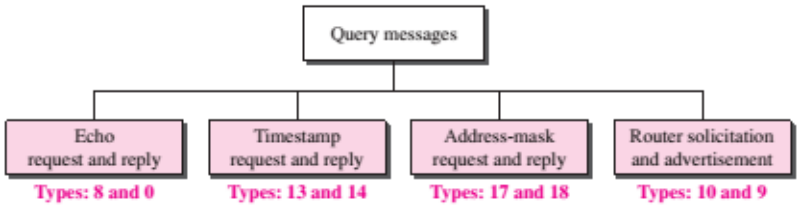

Figure 4-4 ICMP query message

5.1. Echo Request and Reply

The **echo-request** and **echo-reply** messages are designed for diagnostic purposes. The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other. Network managers and users utilize this pair of messages to identify network problems.

The echo-request and echo-reply messages can be used to determine if there is communication at the IP level. Because ICMP messages are encapsulated in IP datagrams, the receipt of an echo-reply message by the machine that sent the echo request is proof that the IP protocols in the sender and receiver are communicating with each other using the IP datagram. Also, it is proof that the intermediate routers are receiving, processing, and forwarding IP datagrams.

Echo request and reply can be used to check whether another host is reachable. Today, most systems provide a version of the ***ping*** command that can create a series (instead of just one) of echo-request and echo-reply messages, providing statistical information.

We can also use echo request and reply to check whether a node works normally. We send echo-request message to the tested host, whose data field contains a segment of message. If this message is repeated correctly by the tested host through the echo-reply message, it proves that the tested host works normally. Otherwise, there is problem with the tested host. The following figure gives the format of echo-request and echo-reply message. The type of echo-request is 8, while the type of echo-reply is 0. There are no definitions of "Identification" and "Sequence" in the protocol and thus senders can use them randomly.

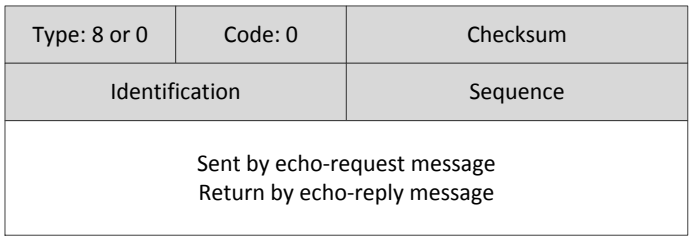

Figure 4-5 ICMP echo request and reply message

5.2. Timestamp Request and Reply

Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the *round-trip time* needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.

Type: 13 or 14	Code: 0	Checksum
Identification		Sequence
Originate timestamp		
Receive timestamp		
Transmit timestamp		

Figure 4-6 ICMP timestamp request and reply message

The type of timestamp request is 13, while the type of timestamp reply is 14.

The lengths of three timestamps are all 32-bit. Each field stores an integer, representing the number of milliseconds since midnight Universal Time (UT).

The source host fills the field of "originate timestamp" with the UT which its clock displays. Other two fields are filled with 0.

After receiving the timestamp request message, the ending host will generate reply message. It will copy the originate timestamp from the request message to the reply message, filling the same field. Then it writes the field of "Receive timestamp". Finally, the field of "Transmit timestamp" will be filled with the sending timestamp.

Timestamp request and reply messages can be used to calculate the time spent from the source to the destination as well as back to the source.

5.3. Address-Mask Request and Reply

A host may know its IP address, but it may not know the corresponding mask. To obtain its mask, a host sends an address-mask-request message to a router on the LAN. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message. The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host. This can be applied to its full IP address to get its subnet address.

The format of address-mask request and reply messages are shown as follows. Type of value 17 represents the address-mask request message, while value 18 represents the address-mask reply message. The field of "Address mask" in the request message is filled with all 0s. When the router replies the host, this field will be filled with real address mask.

Type: 17 or 18	Code: 0	Checksum
Identification		Sequence
Address mask		

Figure 4-7 ICMP address mask request and reply message

When the *diskless workstation* startups, address mask is required. It uses RARP to find out the complete IP address. After that, it searches the address mask by sending address mask request message to determine which is the network ID as well as the host ID.

5.4. Router Solicitation and Advertisement (路由器询问和通告)

A host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. The router-solicitation and router-advertisement messages can help in this situation. A

host can broadcast (or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message. A router can also periodically send router-advertisement messages even if no host has solicited. Note that when a router sends out an advertisement, it announces not only its own presence but also the presence of *all routers on the network of which it is aware*. The following figure gives the format of router solicitation message.

Type: 10	Code: 0	Checksum
Identification		Sequence

Figure 4-8 ICMP router solicitation message

The format of router advertisement message is shown as follows. The field of "Lifetime" indicates how long this message is available. Each router item consists of two fields: Router address and Preference level. The preference level defines the level of router, which is used to choose a router as the default router. If the "Preference Level" is 0, then this router is set as default router. If it is 0x80000000, this router will never be the default router.

Type: 9	Code: 0	Checksum
Number of Addresses	Address Entry Size	Lifetime
Router Address #1		
Preference Level #1		
Router Address #2		
Preference Level #2		
...		

Figure 4-9 ICMP router advertisement message

6. ICMP Error Reporting Message

One of the main responsibilities of ICMP is to report errors. Although technology has produced increasingly reliable transmission media, errors still exist and must be handled. IP is an unreliable protocol. This means that error checking and error control are not a concern of IP. ICMP was designed, in part, to compensate for this shortcoming. However, ICMP does not correct errors—it simply reports them. Error correction is left to the higher-level protocols. Error messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses. ICMP uses the source IP address to send the error message to the source (originator) of the datagram.

Five types of errors are handled: destination unreachable, source quench, time exceeded, parameter problems, and redirection (see Figure 21.9).

Figure 4-10 ICMP Error Reporting Message

Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram. The original datagram header is added to give the original source, which receives the error message, information about the datagram itself. The 8 bytes of data are included because, the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCP or UDP) about the error. ICMP forms an error packet, which is then encapsulated in an IP datagram.

6.1. Destination Unreachable

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram. Note that destination-unreachable messages can be created by either a router or the destination host. The following figure gives the format of Destination Unreachable message, whose field of "Code" indicates the reason why the packet is dropped.

Type: 3	Code: 0 ~ 15	Checksum
Un-used (all 0)		
Part of received IP datagram, including IP header and the first 8 bytes of payload		

Figure 4-11 ICMP Destination Unreachable Message

6.2. Source Quench

The IP protocol is a connectionless protocol. There is no congestion control (拥塞控制) between the source host, which produces the datagram, the routers, which forward it, and the destination host, which processes it. The source-quench message in ICMP was designed to add a kind of *flow control* to the IP. When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram. This message has two purposes. *First*, it informs the source that the datagram has been discarded. *Second*, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process. The format of ICMP source quench message is shown as follows:

Type: 4	Code: 0	Checksum
Un-used (all 0)		
Part of received IP datagram, including IP header and the first 8 bytes of payload		

Figure 4-12 ICMP Source Quench Message

6.3. Time Exceeded

The time-exceeded message is generated in two cases:

- When the *time-to-live* value reaches 0, after decrementing, the router discards the datagram.

However, when the datagram is discarded, a time-exceeded message must be sent by the router to the original source.

- Second, a time-exceeded message is also generated when *not all fragments* that make up a message arrive at the destination host within a certain time limit. The format of Time Exceeded message is shown as follows:

Type: 11	Code: 0 or 1	Checksum
Un-used (all 0)		
Part of received IP datagram, including IP header and the first 8 bytes of payload		

Figure 4-13 ICMP Time Exceeded Message

6.4. Parameter Problem

Any ambiguity in the header part of a datagram can create serious problems as the datagram travels through the Internet. If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source. The following figure shows the format of ICMP Parameter Problem Message. The field of "Code" indicates

Type: 12	Code: 0 or 1	Checksum
Pointer	Un-used (all 0)	
Part of received IP datagram, including IP header and the first 8 bytes of payload		

Figure 4-14 ICMP Parameter Problem Message

"Code" 0 indicates that there is error or ambiguity in some fields of header. "**Pointer"** points to the byte with problem.

"Code" 1 indicates that the missing option. In this case, "**Pointer**" is useless.

6.5. Redirection

For efficiency, hosts do not take part in the routing update process because there are many more hosts in an internet than routers. Updating the routing tables of hosts dynamically produces unacceptable traffic. The hosts usually use static routing. When a host comes up, its routing table has a limited number of entries. It usually knows the IP address of only one router, the default router. For this reason, the host may send a datagram, which is destined for another network, to the wrong router. In this case, the router that receives the datagram will forward the datagram to the correct router. However, to update the routing table of the host, it sends a redirection message to the host. The format of ICMP Redirection Message is shown in Figure 4-15.

Type: 5	Code: 0 or 3	Checksum
IP address of destination router		
Part of received IP datagram, including IP header and the first 8 bytes of payload		

Figure 4-15 ICMP Redirection Message

7. ICMP Checksum

The calculation of ICMP checksum **covers the whole ICMP message**, including header and data.

7.1. Calculating checksum

The senders use ones' complement code arithmetic operation to calculate the checksum as follows:

1) Set checksum as 0;
2) Fragment the message by the length of 16 bits and use ones' complement arithmetic operation to calculate the sum of all fragmentations;
3) Flip the sum and then get the checksum;
4) Store the checksum into the field of "**Checksum**".

7.2. Verifying checksum

Receivers use ones' complement arithmetic operation as follows to verifying the checksum:

1) Fragment the message by the length of 16 bits and use ones' complement arithmetic operation to calculate the sum of all fragmentations;
2) Flip the sum and then get the checksum;
3) If the result is 0, then receive the message, otherwise reject this message.