ICMP

ICMP

- ICMP is mainly used by operating systems of networked computers to send **error messages** indicating that a requested service is not available or that host/ router could not be reached.

Figure 9.1 *Position of ICMP in the network layer*

ICMP

MESSAGES

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

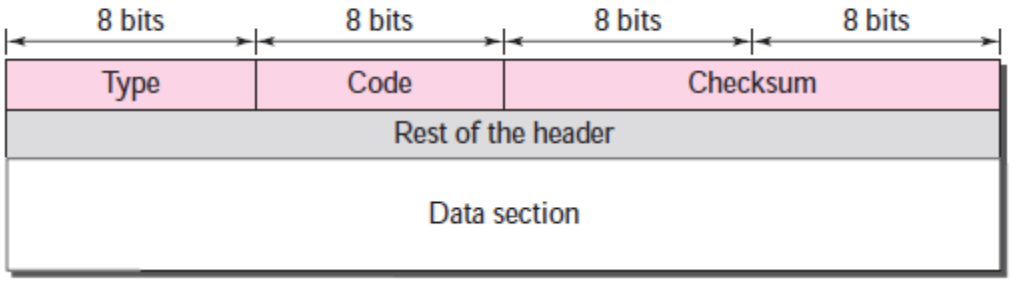
The error-reporting messages report **problems** that a router or a host (destination) may encounter when it **processes** an **IP packet**. The query messages, which occur in pairs, help a host or a network manager get **specific information** from a router or another host. For example, nodes can discover their neighbours.

Table 9.1 *ICMP messages*

Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

ICMP

Figure 9.3 *General format of ICMP messages*



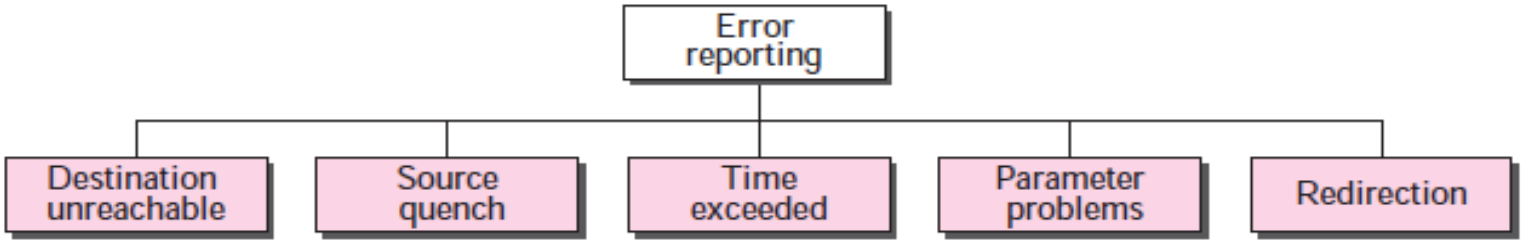
- **Message Format**

- 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.
- 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.**

ICMP

- **Error Reporting Messages**
- ICMP always reports error messages to the original source.
- The following are important points about ICMP error messages:
- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Figure 9.4 *Error-reporting messages*

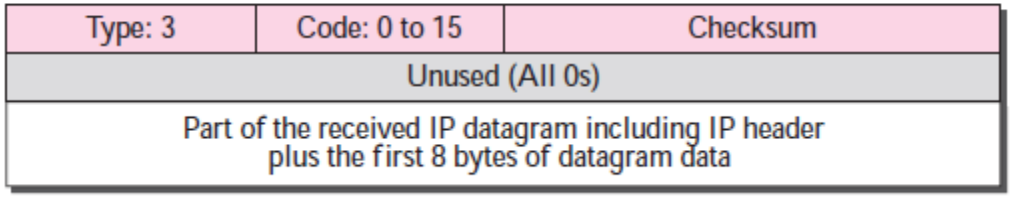


ICMP

- ***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.

Figure 9.6 *Destination-unreachable format*

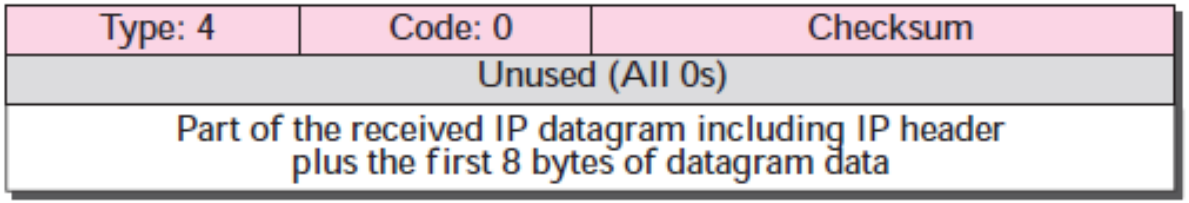


❑ Code 0. The network is unreachable, possibly due to hardware failure.
❑ Code 1. The host is unreachable. This can also be due to hardware failure.
❑ Code 2. The protocol is unreachable.
❑ Code 3. The port is unreachable.
❑ Code 4. Fragmentation is required, but the DF (do not fragment) field of the datagram has been set.

ICMP

- ***Source Quench***
- There is no flow-control or congestion-control mechanism in the IP protocol.
- The source-quench message in ICMP was designed to add a kind of flow control and congestion 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.

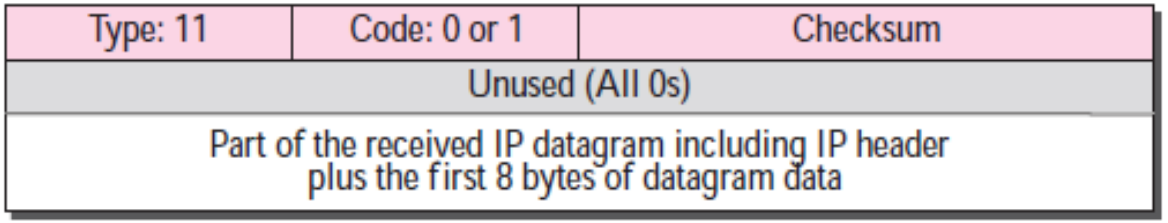
.7 Source-quench format



ICMP

- **Time Exceeded**
- The time-exceeded message is generated in two cases:
- Whenever a router decrements a datagram with a time-to-live value to zero, it discards the datagram and sends a time-exceeded message to the original source.
- 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.
- Code 0 is used when the datagram is discarded by the router due to a time-to-live field value of zero. Code 1 is used when arrived fragments of a datagram are discarded because some fragments have not arrived within the time limit.

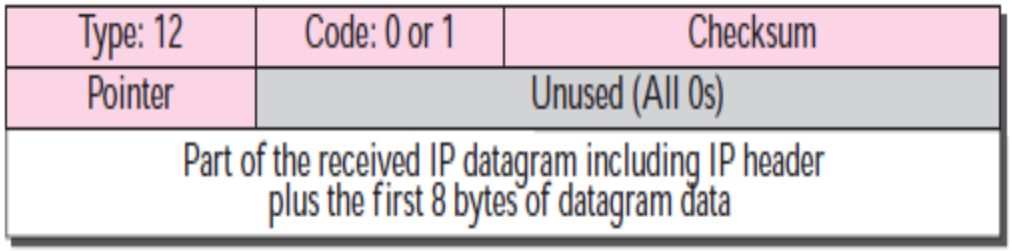
9.8 *Time-exceeded message format*



ICMP

- ***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.

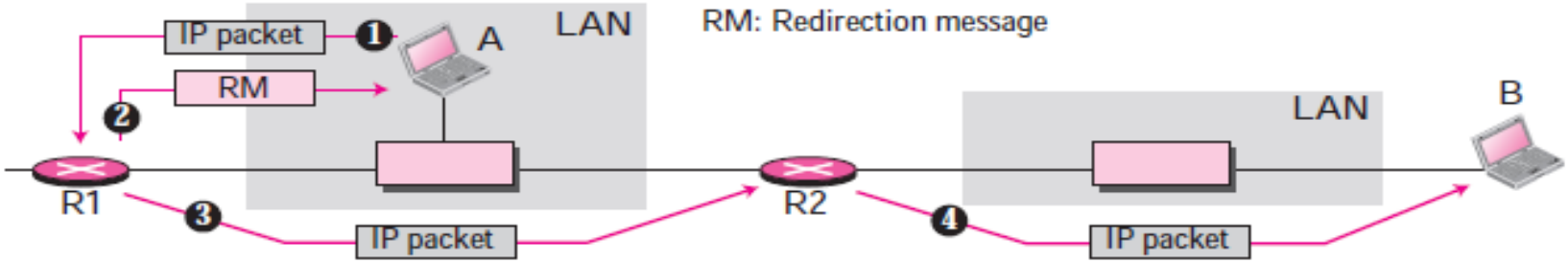
).9 *Parameter-problem message format*



ICMP

- **Redirection**
- The hosts usually use static routing. When a host comes up, its routing table has a limited number of entries. It usually knows only the IP address of 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.

Figure 9.10 *Redirection concept*



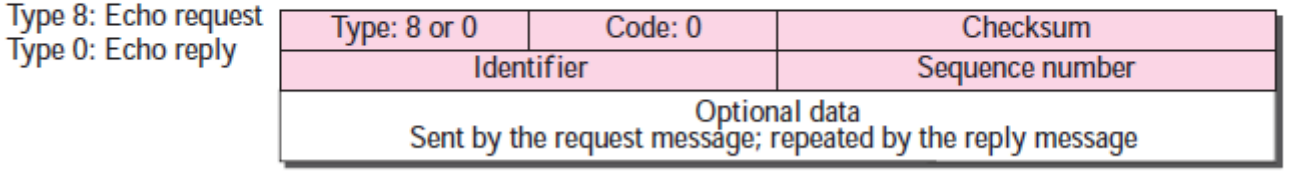
9.11 *Redirection message format*

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		

ICMP

- **Query Messages**
- ***Echo Request and Reply***
- The **echo-request and echo-reply messages are designed for diagnostic purposes. Network** managers and users utilize this pair of messages to identify network problems. The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.
- **An echo-request message can be sent by a host or router. An echo-reply message is sent by the host or router that 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 messages can test the reach-ability of a host.**

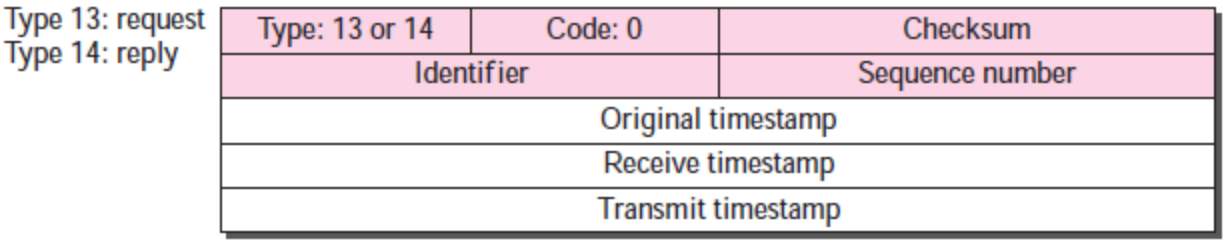
Figure 9.12 *Echo-request and echo-reply messages*



ICMP

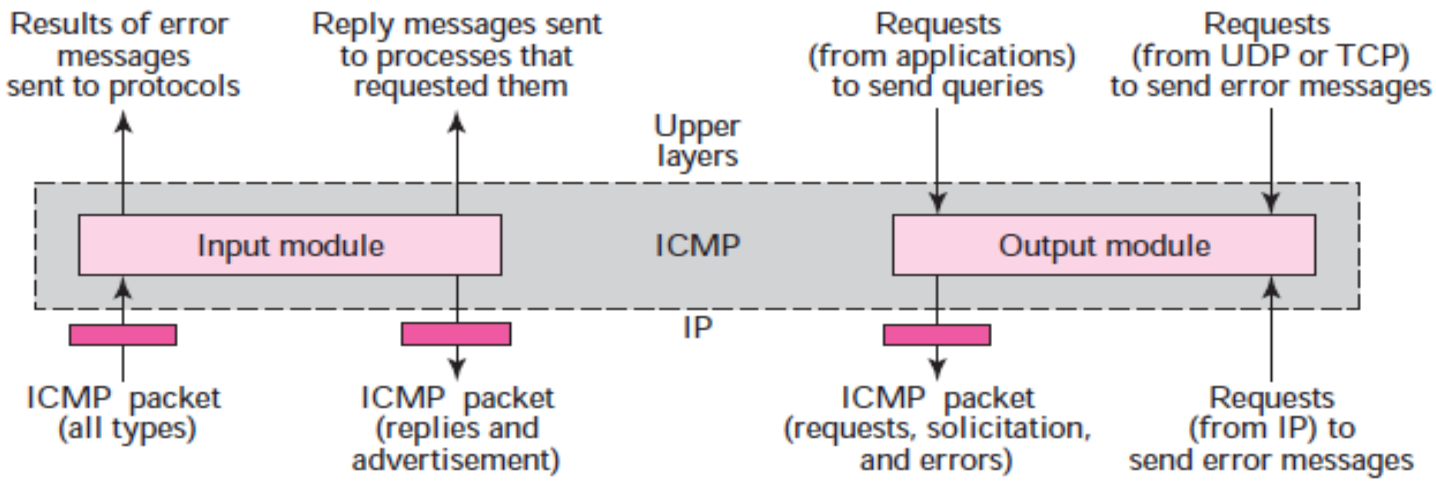
- **Query Messages**
- ***Timestamp Request and Reply***
- Two machines (hosts or routers) can use the timestamp-request and timestamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.

Figure 9.13 *Timestamp-request and timestamp-reply message format*



ICMP Package

Figure 9.16 *ICMP package*



- **Input Module**
- The input module handles all received ICMP messages. It is invoked when an ICMP packet is delivered to it from the IP layer. If the received packet is a request, the module creates a reply and sends it out. If the received packet is a redirection message, the module uses the information to update the routing table. If the received packet is an error message, the module informs the protocol about the situation that caused the error.

ICMP Package

- **Output Module**
- The output module is responsible for creating request, solicitation, or error messages requested by a higher level or the IP protocol. The module receives a demand from IP, UDP, or TCP to send one of the ICMP error messages.
- If the demand is from IP, the output module must first check that the request is allowed. Remember, an ICMP message cannot be created for four situations: an IP packet carrying an ICMP error message, a fragmented IP packet, a multicast IP packet, or an IP packet having IP address 0.0.0.0 or 127.X.Y. Z. The output module may also receive a demand from an application program to send one of the ICMP request messages.

Mobile IP

- **Stationary Hosts**
- The original IP addressing was based on the assumption that a host is stationary, attached to one specific network.
- The address is valid only when the host is attached to the network. If the network changes, the address is no longer valid.
- The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached.

- **Mobile Hosts**

• When a host moves from one network to another, the IP addressing structure needs to be modified.

• ***Changing the Address***

One simple solution is to let the mobile host change its address as it goes to the new network. The host can use DHCP to obtain a new address to associate it with the new network. This approach has several drawbacks.

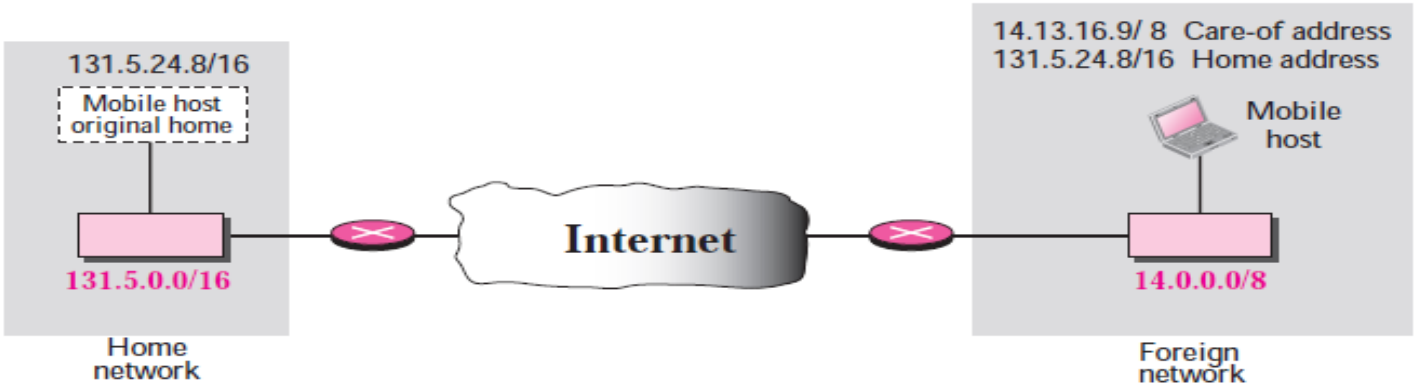
Mobile IP

- **Mobile Hosts**

Two Addresses

The approach that is more feasible is the use of two addresses. The host has its original address, called the **home address, and a temporary address, called the care-of address.**

Figure 10.1 *Home address and care-of address*



Mobile IP has two addresses for a mobile host: one home address and one care-of address. The home address is permanent; the care-of address changes as the mobile host moves from one network to another.

Mobile IP

- **AGENTS**

To make the change of address transparent to the rest of the Internet requires a **home agent and a foreign agent.**

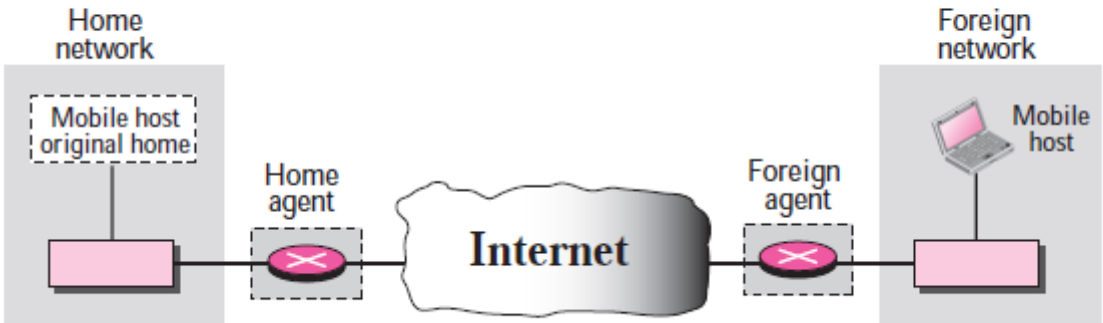
Home Agent

The home agent is usually a router attached to the home network of the mobile host. The home agent acts on behalf of the mobile host when a remote host sends a packet to the mobile host. The home agent receives the packet and sends it to the foreign agent.

Foreign Agent

The foreign agent is usually a router attached to the foreign network. The foreign agent receives and delivers packets sent by the home agent to the mobile host.

re 10.2 *Home agent and foreign agent*



Mobile IP

THREE PHASES

To communicate with a remote host, a mobile host goes through three phases: agent discovery, registration, and data transfer.

Agent Discovery

The first phase in mobile communication, **agent discovery, consists of two subphases.** A mobile host must discover (learn the address of) a home agent before it leaves its home network. A mobile host must also discover a foreign agent after it has moved to a foreign network. The discovery involves two types of messages: advertisement and solicitation.

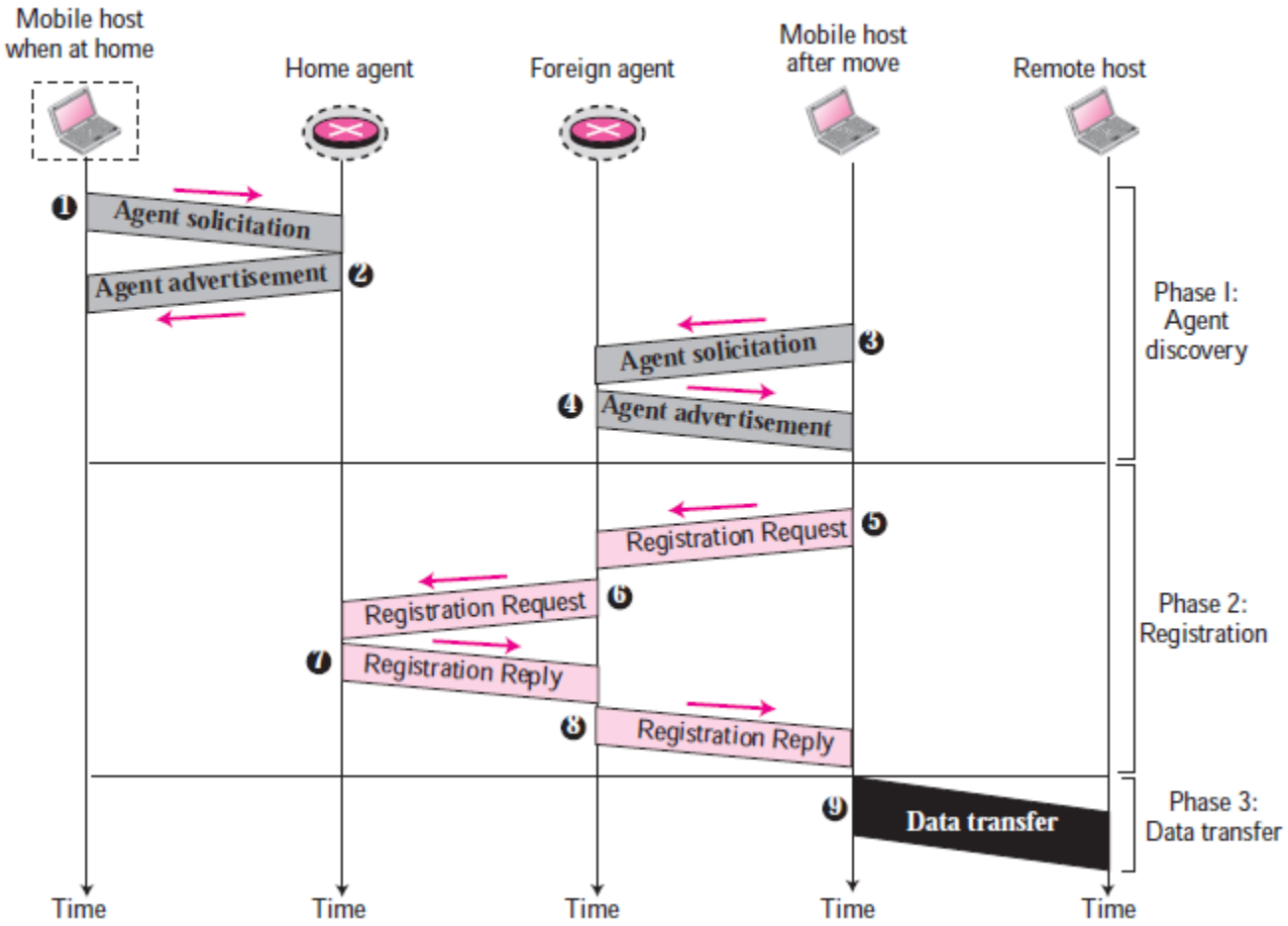
Agent Advertisement

Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message.

Agent Solicitation

It can use the ICMP solicitation message to inform an agent that it needs assistance.

Figure 10.3 *Remote host and mobile host communication*



Mobile IP

Registration

The second phase in mobile communication is **registration. After a mobile host has** moved to a foreign network and discovered the foreign agent, it must register. There are four aspects of registration:

1. The mobile host must register itself with the foreign agent.

2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.

3. The mobile host must renew registration if it has expired.

4. The mobile host must cancel its registration (deregistration) when it returns home.

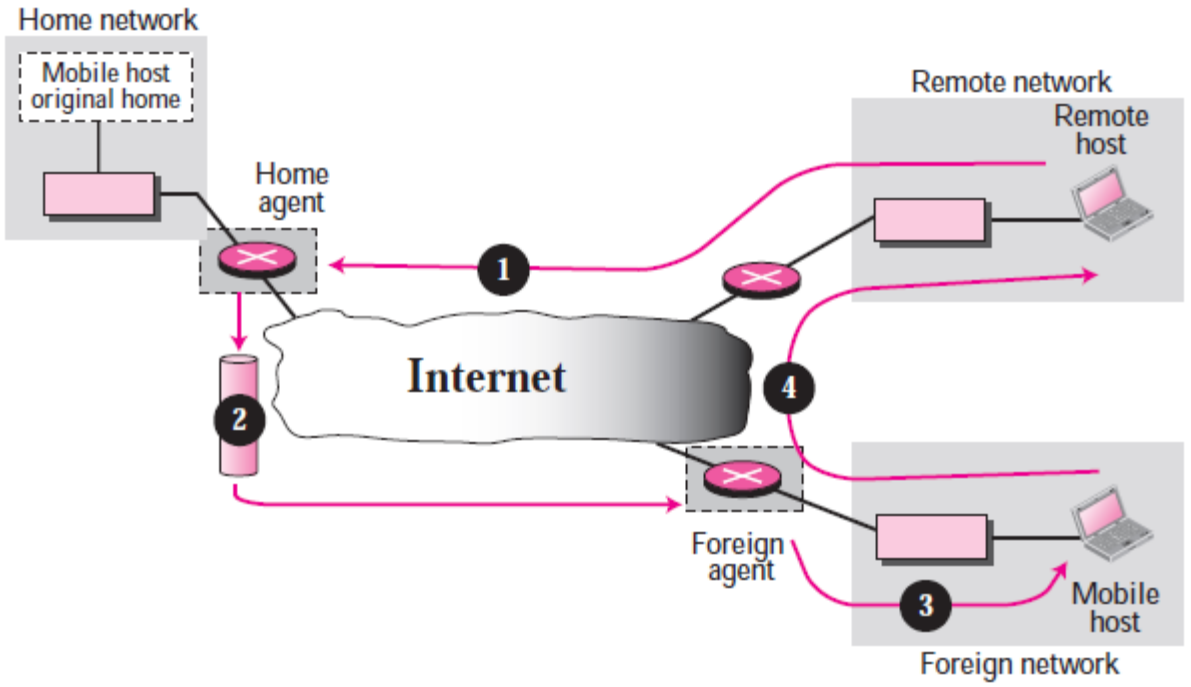
Request and Reply

To register with the foreign agent and the home agent, the mobile host uses a **registration request and a registration reply.**

Mobile IP

Data Transfer

Figure 10.7 *Data transfer*



Inefficiency in Mobile IP

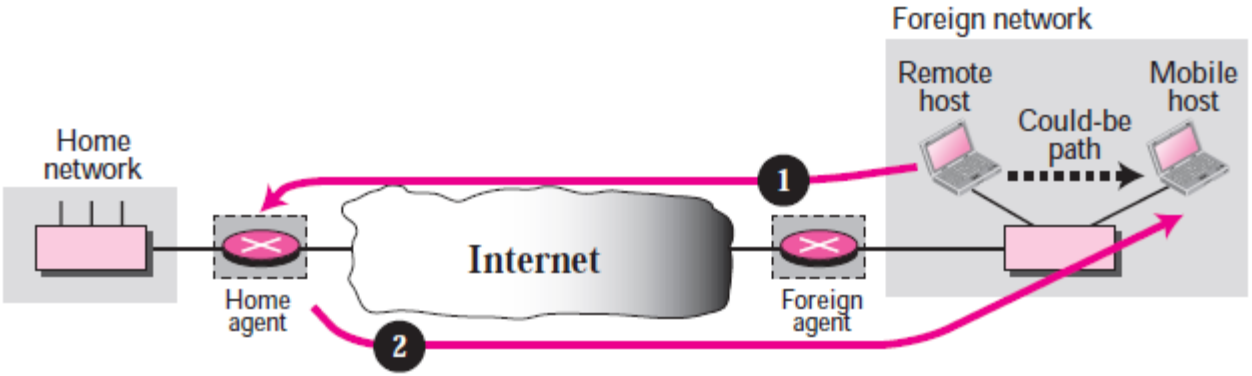
Communication involving mobile IP can be inefficient. The inefficiency can be severe or moderate. The severe case is called *double crossing or 2X. The moderate case is* called *triangle routing or dog-leg routing.*

Double Crossing

Double crossing occurs when a remote host communicates with a mobile host that has moved to the same network (or site) as the remote host.

When the mobile host sends a packet to the remote host, there is no inefficiency; the communication is local. However, when the remote host sends a packet to the mobile host, the packet crosses the Internet twice.

Figure 10.8 *Double crossing*



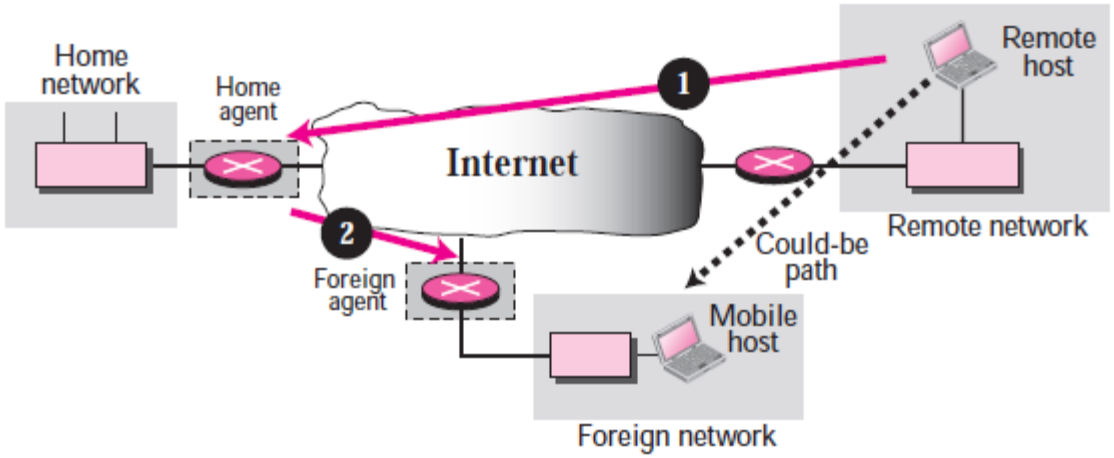
Inefficiency in Mobile IP

Triangle Routing

Triangle routing, the less severe case, occurs when the remote host communicates with a mobile host that is not attached to the same network (or site) as the mobile host.

When the mobile host sends a packet to the remote host, there is no inefficiency. However, when the remote host sends a packet to the mobile host, the packet goes from the remote host to the home agent and then to the mobile host.

Figure 10.9 *Triangle routing*



Inefficiency in Mobile IP

Solution

One solution to inefficiency is for the remote host to bind the care-of address to the home address of a mobile host. For example, when a home agent receives the first packet for a mobile host, it forwards the packet to the foreign agent; it could also send an **update binding packet to the remote host so that future packets to this host could** be sent to the care-of address. The remote host can keep this information in a cache.

The problem with this strategy is that the cache entry becomes outdated once the

mobile host moves. In this case the home agent needs to send a **warning packet to the** remote host to inform it of the change.