Network Layer Protocols

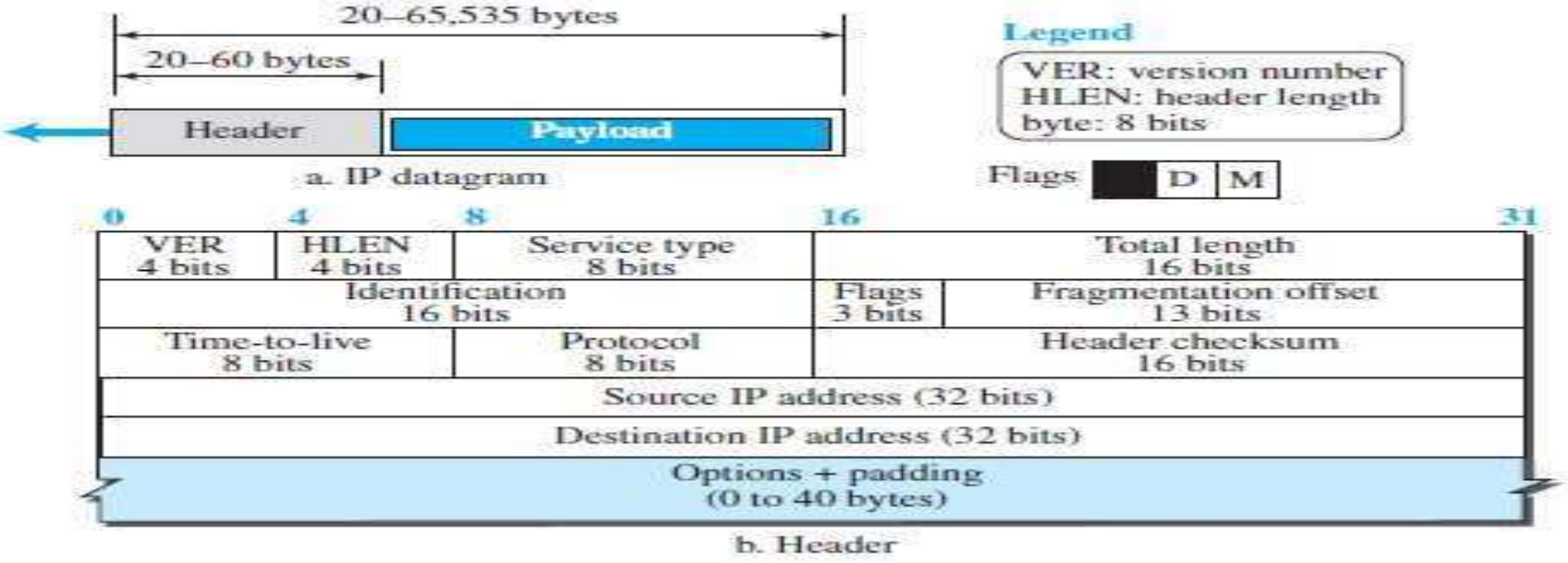
INTERNET PROTOCOL (IP)

- The main protocol, Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.
- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- The Internet Group Management Protocol (IGMP) is used to help IPv4 in multicasting.
- The Address Resolution Protocol (ARP) is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses.
- IPv4 is an unreliable datagram protocol—a best-effort delivery service. The term best-effort means that IPv4 packets can be corrupted, be lost, arrive out of order, or be delayed, and may create congestion for the network.
- IPv4 is also a connectionless protocol that uses the datagram approach.

Datagram Format

- Packets used by the IP are called **datagrams**.
- A datagram is a variable-length packet consisting of two parts: **header** and **payload (data).** The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

Figure 19.2 *IP datagram*



Continue…

- **Version Number:** The 4-bit version number (VER) field defines the version of the IPv4 protocol, i.e. 4
- **Header Length:**The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words.
- **Service Type:** In the original design of the IP header, this field was referred to as type of service (TOS), which defined how the datagram should be handled.
- **Total Length:** This 16-bit field defines the total length (header plus data) of the IP datagram in bytes.
- **Identification, Flags, and Fragmentation Offset:** These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.
- **Time-to-live:** The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field. This value is approximately two times the maximum number of routers between any two hosts.
- **Protocol:** In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.

Continue…

- **Header checksum:** IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission. IP puts the burden of error checking of the payload on the protocol that owns the payload, such as UDP or TCP. The datagram header, however, is added by IP, and its error-checking is the responsibility of IP.
- **Source and Destination Addresses:** These 32-bit source and destination address fields define the IP address of the source and destination respectively.
- **Options:** A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.
- **Payload:** payload is the content of the package.

Fragmentation

- A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.
- **Maximum Transfer Unit (MTU):**
- when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network.
- The value of the MTU differs from one physical network protocol to another. For example, the value for a LAN is normally 1500 bytes, but for a WAN it can be larger or smaller.
- In order to make the IP protocol independent of the physical network, the designers decided to make the maximum length of the IP datagram equal to 65,535 bytes.
- for other physical networks, we must divide the datagram to make it possible for it to pass through these networks. This is called fragmentation.

Continue…

- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed. A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU.
- A datagram can be fragmented by the source host or any router in the path. The reassembly of the datagram, however, is done only by the destination host.

Security of IPv4 Datagrams

- There are three security issues that are particularly applicable to the IP protocol: packet sniffing,packet modification, and IP spoofing.
- **Packet Sniffing:** An intruder may intercept an IP packet and make a copy of it. Packet sniffing is a passive attack, in which the attacker does not change the contents of the packet. This type of attack is very difficult to detect because the sender and the receiver may never know that the packet has been copied. Although packet sniffing cannot be stopped, encryption of the packet can make the attacker's effort useless.
- **Packet Modification:** The second type of attack is to modify the packet. The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver. The receiver believes that the packet is coming from the original sender. This type of attack can be detected using a data integrity mechanism.
- **IP Spoofing:** An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer. This type of attack can be prevented using an origin authentication mechanism.

ICMPv4

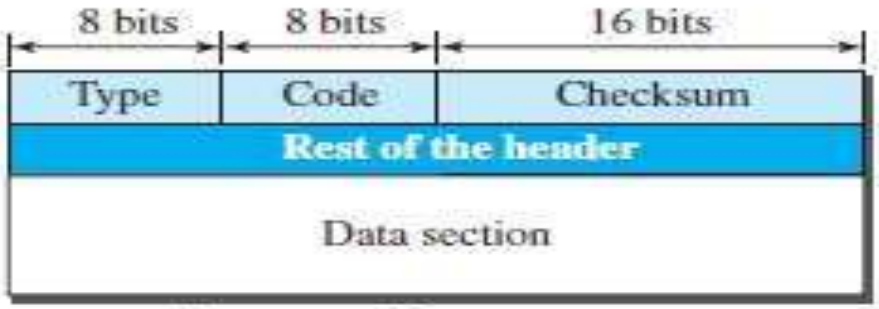
- The IPv4 has no error-reporting or error-correcting mechanism. The IP protocol has no built-in mechanism to notify the original host about the error that has occurred.
- The IP protocol also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive.
- The Internet Control Message Protocol version 4 (ICMPv4) has been designed to compensate for the above two deficiencies.
- It is a companion to the IP protocol. ICMP itself is a network-layer protocol. However, its messages are not passed directly to the data-link layer as would be expected. Instead, the messages are first encapsulated inside IP datagrams before going to the lower layer.
- When an IP datagram encapsulates an ICMP message, the value of the protocol field in the IP datagram is set to 1 to indicate that the IP payroll is an ICMP message.

Messages

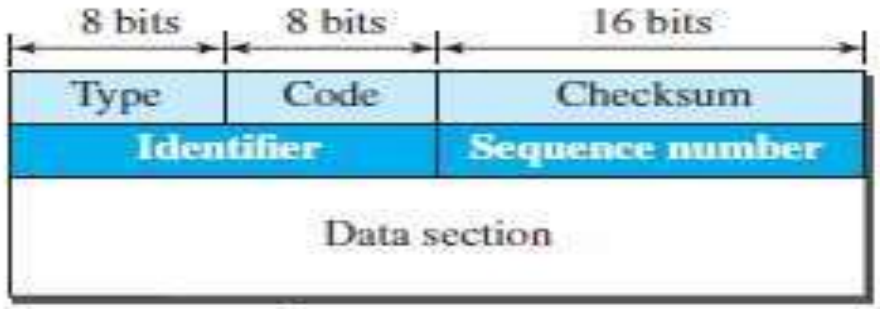
- ICMP messages are divided into two broad categories: **error-reporting messages** and **query messages**.
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.
- 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.

Continue…

Figure 19.8 *General format of ICMP messages*



Error-reporting messages



Query messages

Type and code values

Error-reporting messages
03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages
08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Error Reporting Messages

- ICMP does not correct errors, it simply reports them.
- 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.
- To make the error-reporting process simple, ICMP follows some rules in reporting messages.

I. First, no error message will be generated for a datagram having a multicast address or special address (such as this host or loopback).

II. Second, no ICMP error message will be generated in response to a datagram carrying an ICMP error message.

III. Third, no ICMP error message will be generated for a fragmented datagram that is not the first fragment.

- 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 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.

Continue…

- **Destination Unreachable:** The most widely used error message is the destination unreachable (type 3). This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.
- **Source Quench:** Another error message is called the source quench (type 4) message, which informs the sender that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams.
- **Redirection Message:** The redirection message (type 5) is used when the source uses a wrong router to send out its message. The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future. The IP address of the default router is sent in the message.
- **Parameter Problem:** A parameter problem message (type 12) can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

Query Messages

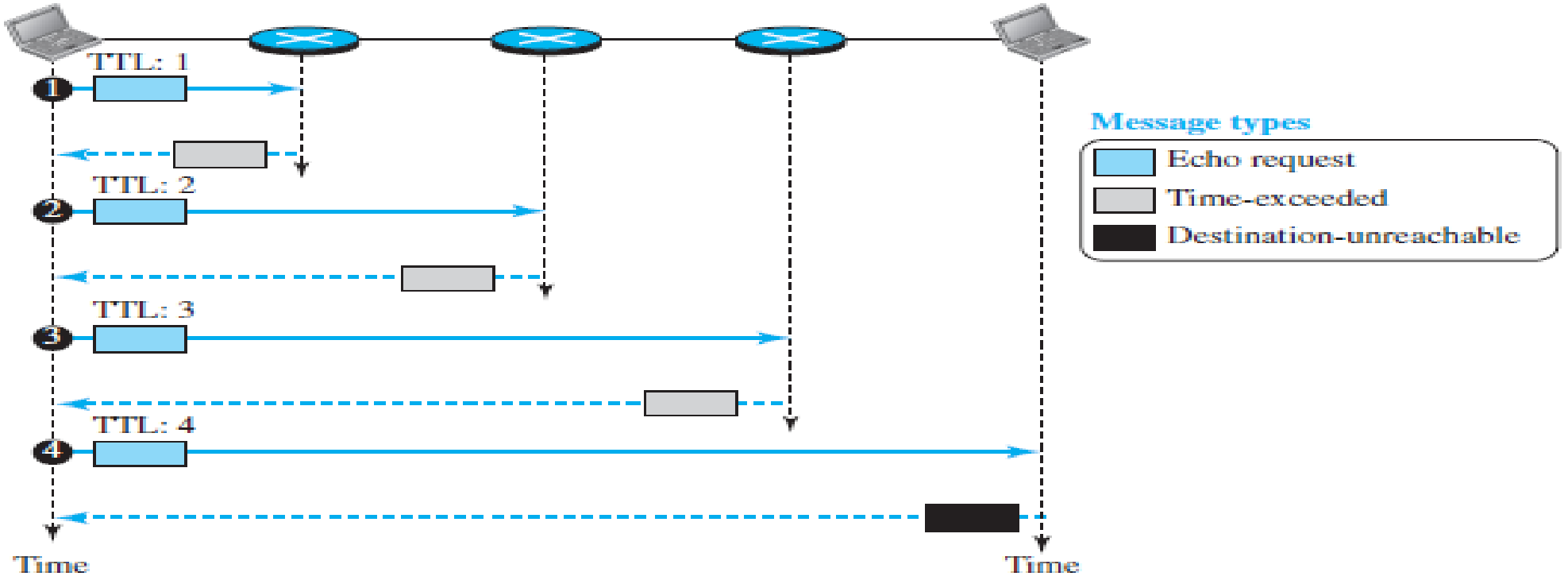
- Query messages in ICMP can be used independently without relation to an IP datagram.
- A query message needs to be encapsulated in a datagram, as a carrier.
- Query messages are used to probe or test the liveliness of hosts or routers in the Internet, find the one-way or the round-trip time for an IP datagram between two devices, or even find out whether the clocks in two devices are synchronized.
- Query messages come in pairs: **request and reply.**
- The echo request (type 8) and the echo reply (type 0) pair of messages are used by a host or a router to test the liveliness of another host or router. A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.

Debugging Tools

- We introduce two tools that use ICMP for debugging: **ping** and **traceroute**.
- **Ping:**
- We can use the ping program to find if a host is alive and responding. We use ping here to see how it uses ICMP packets. The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages. The ping program sets the identifier field in the echo-request and echo-reply message and starts the sequence number from 0; this number is incremented by 1 each time a new message is sent.
- **Traceroute or Tracert:**
- The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination. It can find the IP addresses of all the routers that are visited along the path. The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- The ping program gets help from two query messages; the traceroute program gets help from two error-reporting messages: time-exceeded and destination-unreachable.

Continue…

Figure 19.10 *Use of ICMPv4 in traceroute*



MOBILE IP

- Mobile IP, the extension of IP protocol that allows mobile computers to be connected to the Internet at any location where the connection is possible.
- **Addressing:**
- **Stationary Hosts:** The original IP addressing was based on the assumption that a host is stationary, attached to one specific network. A router uses an IP address to route an IP datagram.
- **Mobile Hosts:** When a host moves from one network to another, the IP addressing structure needs to be modified. Several solutions have been proposed.

I. **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.

Drawbacks:

The configuration files would need to be changed.

Device needs to be rebooted.

DNS table entries need to be revised.

The data exchange will be interrupted.

Continue…

II. Two Addresses:

- The host has its original address, called the **home address**, and a temporary address, called the **care-of address.**

Agents

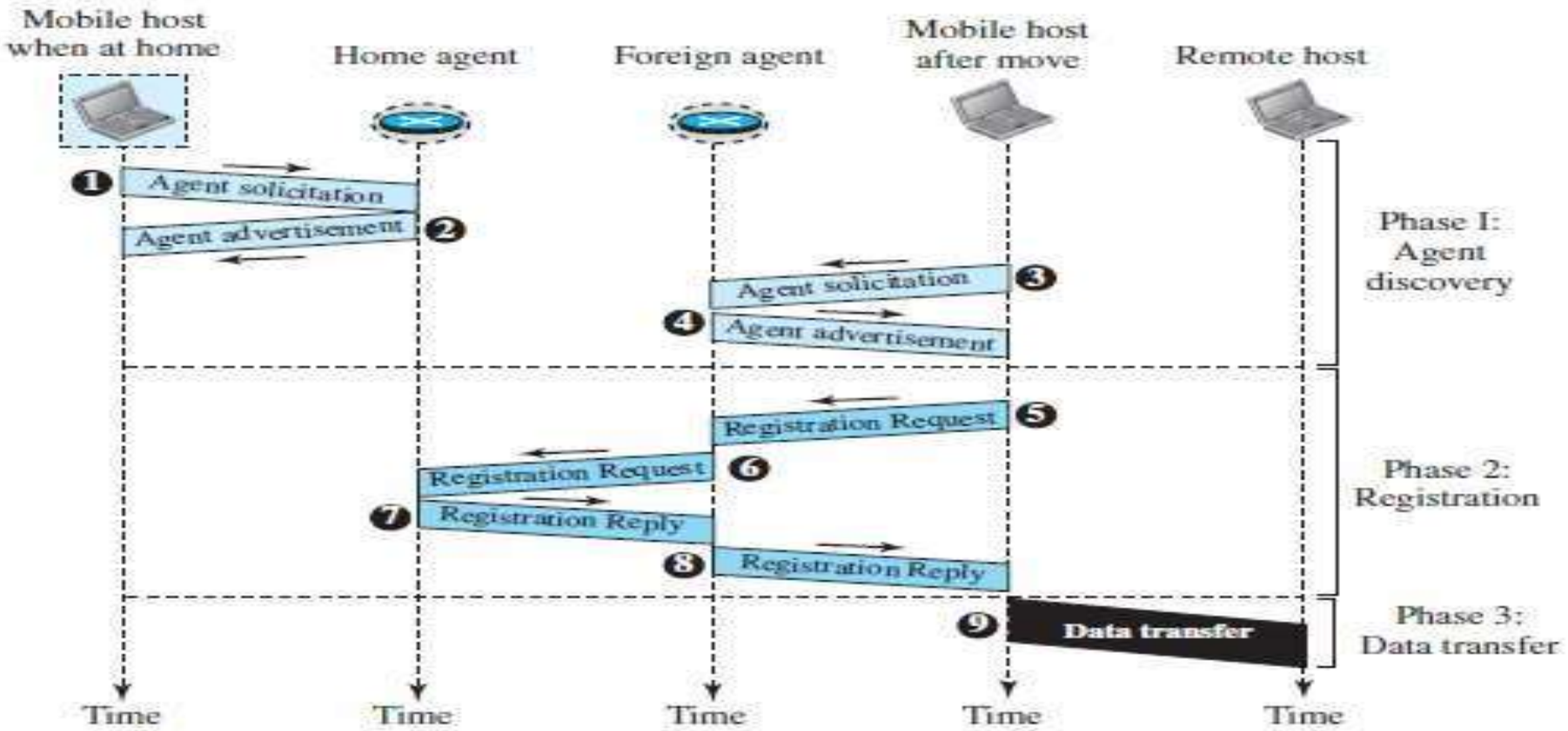
- To make the change of address transparent to the rest of the Internet requires a **home agent** and a **foreign agent.**

I. **Home Agent:** The home agent is usually a router attached to the home network of the mobile host. The home agent receives the packet and sends it to the foreign agent.

II. **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.

Three Phases

Figure 19.14 *Remote host and mobile host communication*



Continue…

- **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**.

I. **Agent Advertisement:** When a router advertises its presence on a network using an ICMP router advertisement, it can append an agent advertisement to the packet if it acts as an agent.

II. **Agent Solicitation:** When a mobile host has moved to a new network and has not received agent advertisements, it can initiate an agent solicitation. It can use the ICMP solicitation message to inform an agent that it needs assistance.

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

I. **Registration Request:** A registration request is sent from the mobile host to the foreign agent to register its care-of address and also to announce its home address and home agent address. The foreign agent, after receiving and registering the request, relays the message to the home agent.

Continue…

II. **Registration Reply:** A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host. The reply confirms or denies the registration request.

- **Data Transfer:** After agent discovery and registration, a mobile host can communicate with a remote host.

I. **From Remote Host to Home Agent:** When a remote host wants to send a packet to the mobile host, it uses its address as the source address and the home address of the mobile host as the destination address.

II. **From Home Agent to Foreign Agent:** After receiving the packet, the home agent sends the packet to the foreign agent. The home agent encapsulates the whole IP packet inside another IP packet using its address as the source and the foreign agent's address as the destination.

III. **From Foreign Agent to Mobile Host:** When the foreign agent receives the packet, it removes the original packet. However, since the destination address is the home address of the mobile host, the foreign agent consults a registry table to find the care-of address of the mobile host. The packet is then sent to the care-of address.

Continue…

IV. **From Mobile Host to Remote Host:** When a mobile host wants to send a packet to a remote, it sends as it does normally. The mobile host prepares a packet with its home address as the source, and the address of the remote host as the destination. Although the packet comes from the foreign network, it has the home address of the mobile host.

V. **Transparency:** In this data transfer process, the remote host is unaware of any movement by the mobile host. The remote host sends packets using the home address of the mobile host as the destination address; it receives packets that have the home address of the mobile host as the source address. The movement is totally transparent.