TCP STATE TRANSITION DIAGRAM AND MOBILE IP

A TCP connection goes through a series of states during its lifetime. Figure 8.28 shows the state transition diagram. Each state transition is indicated by an arrow, and the associated label indicates associated events and actions. Connection establishment begins in the CLOSED state and proceeds to the ESTABLISHED state. Connection termination goes from the ESTABLISHED state to the CLOSED state. The normal transitions for a client are indicated by thick solid lines, and the normal transitions for a server are denoted by dashed lines. Thus when a client does an active open, it goes from the CLOSED state, to SYN_SENT, and then to ESTABLISHED. The server carry- ing out a passive open goes from the CLOSED state, to LISTEN, SYN_RCVD, and then to ESTABLISHED.

The client normally initiates the termination of the connection by sending a FIN. The associated state trajectory goes from the ESTABLISHED state, to FIN_WAIT_1 while it waits for an ACK, to FIN_WAIT_2 while it waits for the other side's FIN, and then to TIME_WAIT after it sends the final ACK. When the TIME_WAIT 2MSL period expires, the connection is closed and the transmission control block that stores all the TCP connection variables is deleted. Note that the state transition diagram does not show all error conditions that may arise, especially in relation to the TIME_WAIT state. The server normally goes from the ESTABLISHED state to the CLOSE_WAIT state after it receives a FIN, to the LAST_ACK when it sends its FIN, and finally to CLOSE when it receives the final ACK. **TCP STATE TRANSITION DIAGRAM AND MOBILE IP**

Mobile IP:

Mobile networking is a subject that is becoming increasingly important as por table devices such as personal digital assistants (PDAs) and notebook computers are becoming more powerful and less expensive, coupled with people's need to be connected whenever and wherever they are. The link between the portable device and the fixed communication network can be wireless or wired. Infrared channels are often used in shorter distances. A wireless connection enables a user to maintain its communication session as it roams from one area to another, providing a very powerful communication paradigm. In this section we look at a simple IP solution for mobile computers.

Mobile IP allows portable devices called mobile hosts (MHs) to roam from one area to another while maintaining the communication sessions. One require- ment in mobile IP is that a legacy host communicating with an MH and the intermediate routers should not be modified. This requirement implies that an MH must continuously use its permanent IP address even as it roams to another area. Otherwise, existing sessions will stop working and new sessions should be restarted when an MH moves to another area. The basic mobile IP solution is sketched in Figure 2.29.

The mobile IP routing operates as follows:

When a correspondent host (CH) wants to send a packet to an MH, the CH transmits the standard IP packet with its address as the source IP address and the MH's address as the destination IP address. This packet will be intercepted by the mobile host's router called the home agent (HA), which keeps track of the current location of the MH. The HA manages all MHs in its home network that use the same address prefix. If the MH is located in the home network, the HA simply forwards the packet to its home network.

When an MH moves to a foreign network, the MH obtains a care-of address from the foreign agent (FA) and registers the new address with its HA. The care-of address reflects the MH's current location and is typically the address of the FA. Once the HA knows the care-of address of the MH, the HA can forward the registration packet to the MH via the FA.

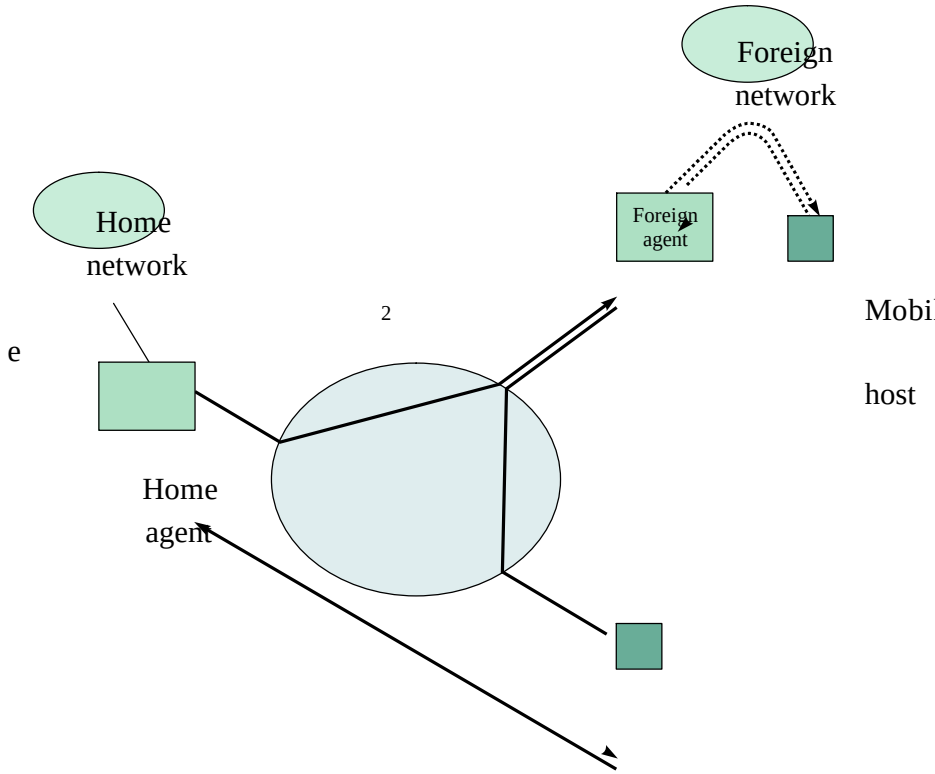

FIGURE 2.29 Routing for mobile hosts

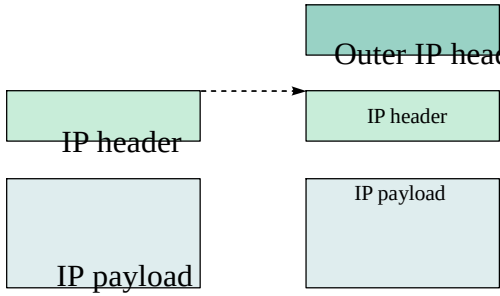

FIGURE 2.30 IP to IP

---------►

Unfortunately, the HA cannot directly send packets to the MH in a foreign network in a conventional way (i.e., by using the care-of address as the destina- tion address of the IP packet, the packet final destination will the FA rather than the MH). The solution is provided by a tunneling mechanism that essentially provides two destination addressesÐthe destination of the other end of the tunnel (i.e., the FA) and the final destination (i.e., the MH). The IP packet tunneled by the HA is encapsulated with an outer IP header (see Figure 8.30) containing the HA's address as the source IP address and the care-of address as the destination IP address. When the FA receives the packet, the FA decapsu-lates the packet that produces the original IP packet with the correspondent host's address as the source IP address and the MH's address as the destination IP address. The FA can then deliver the packet to the MH.