MIPv6 Generic Mechanisms

MIPv6 Basic Operation As noted, an MN is always addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to the MN within its home subnet prefix on its home link. While an MN is at home, packets addressed to its home address are routed to the MN's home link using traditional routing mechanisms. While an MN is attached to some foreign link away from home, it is also addressable at one or more CoAs. A CoA is an IP address associated with an MN that has the subnet prefix of a particular foreign link. The MN acquires its CoA using traditional IPv6 mechanisms, such as stateless or stateful autoconfiguration. As long as the MN stays in this location, packets addressed to this CoA will be routed to the MN. The MN may also accept packets from several CoAs, this being the case, for example, when it is moving to a new location but still reachable at the previous link. The MIPv6 specification requires that home and CoAs must be unicast routable addresses. The association between an MN's home address and CoA is known as a "binding" for the MN. While away from home, an MN registers its primary CoA with a router on its home link, requesting this router to function as the "HA" for the MN. The MN performs this binding registration by sending a BU message to the HA. The HA replies to the MN by returning a BA message. The exchange of BUs, BAs, and other control messages is referred to as "signaling." Note: In addition to the binding cache, each HA also maintains an HA list. This list has information about routers on the same link that is acting as an HA and is used by the HAAD mechanism—a router is known to be acting as an HA, if it sends 268 LAYER 3 CONNECTIVITY: TABLE Binding Cache Content Content Description Home address The home address of the MN for which this is the binding cache entry. This field is used as the key for searching the binding cache for the destination address of a packet being sent CoA The CoA for the MN indicated by the home address field in this binding cache entry Lifetime value The lifetime value indicates the remaining lifetime for this binding cache entry. The lifetime value is initialized from the lifetime field in the BU that created or last modified this binding cache entry Flag This flag indicates whether or not this binding cache entry is a home registration entry (applicable only on nodes that support HA functionality) Maximum value The maximum value of the sequence number field received in previous BUs for this home address. The sequence number field is 16 bits long (it uses modulo 216 math) Usage information Usage information for this binding cache entry. This is needed to implement the cache replacement policy in use in the binding cache. Recent use of a cache entry also serves as an indication that a BRR should be sent when the lifetime of this entry nears expiration a router advertisement in which the HA (H) bit is set. The HA maintains a separate HA list for each link on which it is serving as an HA. Any node communicating with an MN is referred to as a "correspondent node" of the MN and may itself be either a stationary device or a mobile device. MNs are also able to provide information about their current location to CNs. This happens through the correspondent registration. As a part of this procedure, a return-routability test is performed in order to authorize the establishment of the binding. There are two possible modes for communications between the MN and a CN, as previously noted, as follows: The first mode, "bidirectional tunneling," does not require MIPv6 support from the CN and is available even if the MN has not registered its current binding with the CN. Packets from the CN are routed to the HA and then tunneled to the MN. Packets to the CN are tunneled from the MN to the HA ("reverse tunneled") and then routed normally from the home network to the CN. In this mode, the HA uses proxy neighbor discovery to intercept any IPv6 packets addressed to the MN's home address on the home link. Each intercepted packet is tunneled to the MN's primary CoA. The second mode, "route optimization4" (also called above, "direct routing"), requires the MN to register its current binding at the CN. Packets from the CN can be routed directly to the CoA of the MN. When sending a packet to any IPv6 destination, the CN checks its cached bindings (see Table 8.3) for an entry for 4The acronym RO is also used by some practitioners. PROTOCOL DETAILS 269 the packet's destination address. If

a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the MN by way of the CoA indicated in this binding. Routing packets directly to the MN's CoA allows the shortest communications path to be used. It also eliminates congestion at the MN's HA and home link. In addition, the impact of any possible failure of the HA or networks on the path to or from it is reduced. When routing packets directly to the MN, the CN sets the destination address in the IPv6 header to the CoA of the MN. A new type of IPv6 routing header is also added to the packet to carry the desired home address. Similarly, the MN sets the source address in the packet's IPv6 header to its current CoAs. The MN adds a new IPv6 "home address" destination option to carry its home address. The inclusion of home addresses in these packets makes the use of the CoA transparent above the network layer (e.g., at the transport layer). Note: MIPv6 requires the MN to know its HA address, its own home address, and the cryptographic materials (e.g., shared keys or certificates) needed to set up IPsec SAs with the HA in order to protect MIPv6 signaling. The MIPv6 base protocol does not specify any method to automatically acquire this information, which means that network administrators are normally required to manually set configuration data on MNs and HAs. However, in real deployments, manual configuration does not scale as the MNs increase in number (6). A bootstrapping process can be beneficial. Also, according to the latest RFCs, the only SA that is preconfigured is a shared secret between the MN and the home AAA server; this is in contrast with an earlier version of the MIPv6 model. 8.2.1.2 IPv6 Protocol Extensions MIPv6 defines a new IPv6 protocol, using the mobility header. This header is used to carry the messages summarized in Table 8.4. 8.2.1.3 New IPv6 Destination Option MIPv6 defines a new IPv6 destination option, the home address destination option. This option is described in more detail in Section 8.2.2. 8.2.1.4 New IPv6 ICMP Messages As alluded to earlier, MIPv6 also introduces four new ICMPv6 message types, two for use in the dynamic HAAD mechanism and two for renumbering and mobile configuration mechanisms. HAAD request. The ICMP HAAD request message is used by an MN to initiate the dynamic HAAD mechanism. The MN sends the HAAD request message to the MIPv6 HA anycast address for its own home subnet prefix. HAAD reply. The ICMP HAAD reply message is used by an HA to respond to an MN that uses the dynamic HAAD mechanism. Mobile prefix solicitation. The ICMP mobile prefix solicitation message is sent by an MN to its HA while it is away from home. The purpose of the message is to solicit a mobile prefix advertisement from the HA, which will allow the MN 270 LAYER 3 CONNECTIVITY: MOBILE IPv6 TECHNOLOGIES FOR THE IoT

TABLE 8.4 Mobility Header Messages Message Description HoTi HoT These messages are used to perform the return-routability procedure from the MN to a CN Care-of test init Care-of test BU Message is used by an MN to notify a CN or the MN's HA of its current binding. The BU sent to the MN's HA to register its primary CoA is marked as a "home registration" BA Message is used to acknowledge receipt of a BU, if an acknowledgement was requested in the BU, the BU was sent to an HA, or an error occurred BRR Message is used by a CN to request an MN to re-establish its binding with the CN. This message is typically used when the cached binding is in active use, but the binding's lifetime is close to expiration. The CN may use, for instance, recent traffic and open transport layer connections as an indication of active use Binding error Message is used by the CN to signal an error related to mobility, such as an inappropriate attempt to use the home address destination option without an existing binding to gather prefix information about its home network. This information can be used to configure and update home address(es) according to changes in prefix information supplied by the HA. Mobile prefix advertisement. An HA will send a mobile prefix advertisement to an MN to distribute prefix information about the home link while the MN is traveling away from the home network. This occurs in response to a mobile prefix solicitation with an advertisement, or by an unsolicited advertisement. 8.2.1.5 Mobile IPv6 Security MIPv6 incorporates a number of security features. These include the protection of BUs both to HAs and to CNs, the protection of mobile prefix discovery, and the protection of the mechanisms that MIPv6 uses for transporting data packets: BUs are protected by the use of IPsec extension headers, or by the use of the binding authorization data option

(this option employs a binding management key, Kbm, which can be established through the return-routability procedure). Mobile prefix discovery is protected through the use of IPsec extension headers. Mechanisms related to transporting payload packets—such as the home address destination option and type 2 routing header—have been specified in a manner that restricts their use in attacks. Although these basic security mechanisms are adequate for some environments and applications, there are limitations with these for other environments.