

Mobile IPv6

Raj Jain

Washington University in Saint Louis
Saint Louis, MO 63130

Jain@cse.wustl.edu

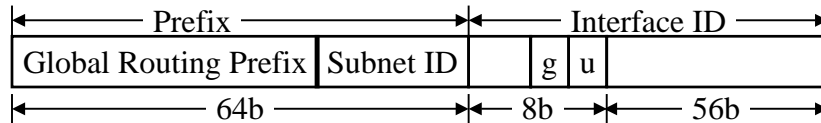
These slides are available on-line at:

<http://www.cse.wustl.edu/~jain/cse574-06/>



- IPv6: Overview, Extension Headers, Neighbor Discovery, Address Auto configuration
- Mobile IPv4 vs. IPv6
- Route Optimization
- Return Routability Procedure
- Cryptographically Generated Addresses (CGAs)
- Fast Handover
- Hierarchical Mobile IPv5 (HMIPv6)

IPv6: Overview



- ❑ 128 bit addresses: 64-bit Prefix + 64-bit Interface ID
lsb of MSB = u = universal or local interface ID
g = group ID
- ❑ Routers advertise network prefix
- ❑ Colon-hex notation:
3FFE:0200:0000:0000:0012:F0C8:79CA
3FFE:0200::0012:F0C8:79CA
:: ⇒ Unspecified Address
- ❑ Flow Label: SA-DA-Label ⇒ One flow
- ❑ Scoped Addresses: Link-Local, Site-Local
- ❑ Extension headers: Routing, Hop-by-Hop, Destination Options

Washington University in St. Louis

CSE574s

©2006 Raj Jain

13-3

Address Auto Configuration

- ❑ **Stateful:**
 - Using DHCP
- ❑ **Stateless:**
 - Hosts can make a global address using advertised network prefix
 - Interface identifier should be unique
 - Stateless ⇒ No one needs to keep record of what address was allocated

Washington University in St. Louis

CSE574s

©2006 Raj Jain

13-4

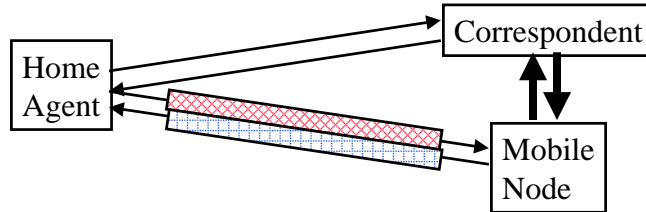
Mobile IPv4 vs. IPv6

1. No need for a foreign agent
2. Route optimization
3. Secure Route optimization
4. New extension header in place of tunneling \Rightarrow Less overhead. Less state.
5. Neighbor discovery in place of ARP \Rightarrow More general L2
6. Dynamic home agent discovery returns a single reply

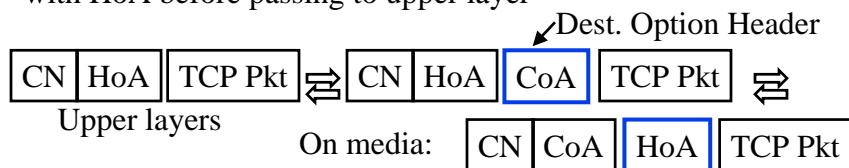
Binding Updates

- Binding Update \Rightarrow Registration
- New Mobility Header
- MH Type=5 \Rightarrow Binding Update
- Each binding update has a Sequence Number.
Mobile keeps track of last seq # for each destination
- Home agent performs Duplicate Address Detection (DAD), updates binding cache, sends binding ack
- New network prefix and default router unreachable
 \Rightarrow Network change

Route Optimization



- ❑ Shortest path in both directions
- ❑ Mobile sends a binding update to the correspondent
- ❑ New Destination Option: Home Address (HoA) Option
- ❑ HoA option is used in all packets. Correspondent replaces SA with HoA before passing to upper layer



Washington University in St. Louis

CSE574s

©2006 Raj Jain

13-7

Route Optimization (Cont)

- ❑ SA and destination option addresses are interchanged before transmission and after reception
- ❑ In the reverse direction:
 - New header type: “Routing Header type 2” contains home address
 - DA and Routing header type 2 addresses are interchanged before transmission and after reception
- ❑ Binding error message
 - ⇒ Sorry I don't have a binding for this HoA
- ❑ IP-in-IP tunneling will require 4 addresses instead of 3 with new headers

Washington University in St. Louis

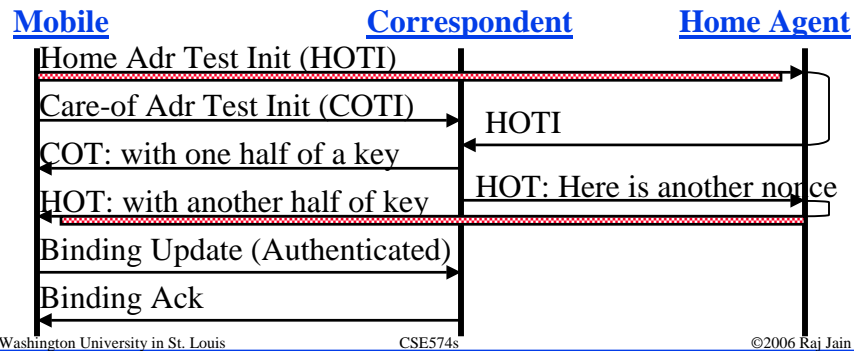
CSE574s

©2006 Raj Jain

13-8

Return Routability Procedure

- ❑ Mobile must prove to correspondent that it owns both HoA and CoA
- ❑ Mobile does not share any secret with correspondent
- ❑ Correspondent send messages to HoA and CoA. Mobile responds correctly if it receives both.



13-9

Return Routability Procedure (Cont)

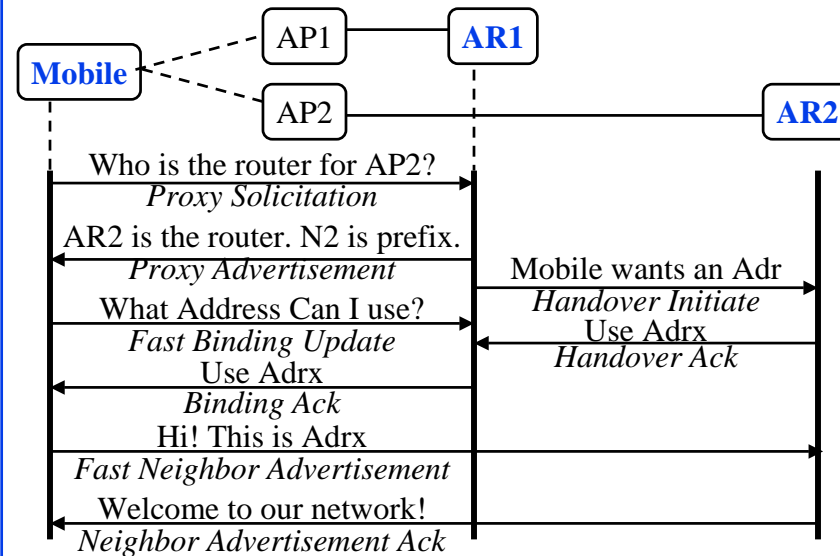
- ❑ Mobile starts this test. Sends HoTI via HA with a cookie.
 - ❑ CN generates “Home Keygen Token”
= $\text{First}(64, \text{HMAC_SHA1}(\text{Kcn}, \text{HoA}|\text{nonce}|0))$
 - ❑ CN returns HoT containing MN's cookie, Home keygen token, and CN's nonce index
 - ❑ Mobile sends CoTI directly to CN with another cookie
 - ❑ CN generates “Care-of Keygen Token”
= $\text{First}(64, \text{HMAC_SHA1}(\text{Kcn}, \text{CoA}|\text{nonce}|1))$
 - ❑ CN returns CoT containing MN's cookie, Co Keygen Token, CN's nonce index
 - ❑ Mobile constructs a key and sends an encrypted binding update
 - $\text{Kbm} = \text{Sha1}(\text{Home Keygen Token}|\text{Care-of Keygen Token})$
 - $\text{Auth_data} = \text{First}(96, \text{MAC}(\text{Kbm}, \text{Mobility_data}))$
 - $\text{Mobility_data} = \text{CoA}|\text{final dest address}|\text{Mobility Header data}$
 - $\text{Final Dest Address} = \text{CN's Home address if CN is mobile}$
- Washington University in St. Louis CSE574s ©2006 Raj Jain

13-10

Cryptographically Generated Addresses

- ❑ IPv6 address includes 64 bit interface id
- ❑ A node can generate Interface ID using its public key on network prefix
- ❑ 64-bit Interface ID = First(64, Hash(home_prefix|public key|context) & 0xFCFF FFFF FFFF FFFF)
- ❑ C ⇒ Universal and group bits on the interface id are zero
- ❑ Mobile node can sign the binding update using its private key.

Fast Handover

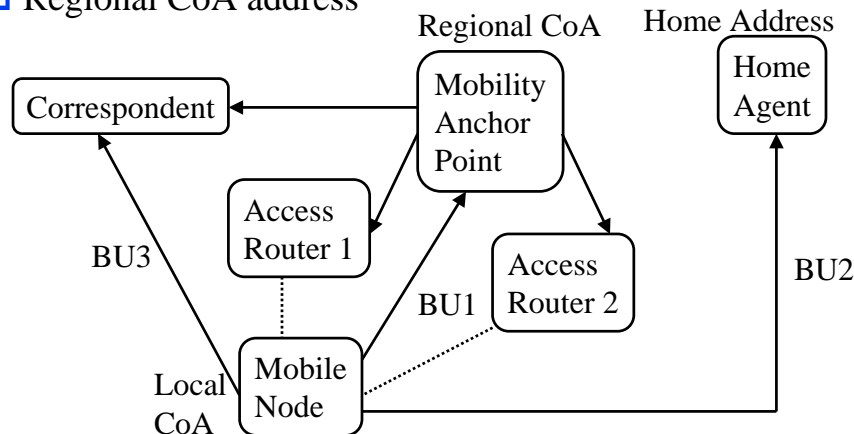


Fast Handover (Cont)

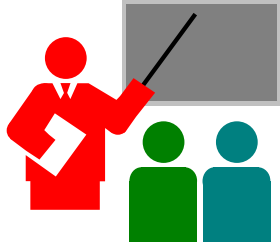
- ❑ Ask AR1 about router for AP2
⇒ *Router Solicitation for Proxy* w list of Access Points
- ❑ AR1 returns *Proxy Router Advertisement* w at least one prefix
- ❑ AR1 sends *Handover initiate* (HI) message to AR2 and sets up a tunnel
- ❑ AR2 does *DAD* and send *Handover Ack* (Hack)
- ❑ Mobile sends *Binding update* to AR1
- ❑ AR1 sends *Binding Ack* to old CoA or new CoA
- ❑ Mobile sends *Fast Neighbor Advertisement* (F-NA) to AR2
- ❑ AR2 returns *Fast Neighbor Advertisement Ack* to Mobile
- ❑ Mobile can use CGA to avoid HI/Hack

Hierarchical Mobile IPv6 (HMIPv6)

- ❑ Regional Home Agent: Mobile Anchor Point (MAP)
- ❑ Regional CoA address



Summary



- ❑ IPv6 has a new "mobility" extension header.
- ❑ Two-way optimal route using binding updates with correspondent
- ❑ Security using Return Routability procedure
- ❑ Fast handover using local mobility
- ❑ Hierarchical anchors to minimize mobile overhead

Reading Assignment

Text Books:

- ❑ Dixit and Prasad, Chapter 16, pp. 335-439.
- ❑ Murthy and Manoj, Section 4.3, pp. 158-172

Other Books:

- ❑ Hesham Soliman, "Mobile IPv6," Addison-Wesley, 2004, ISBN:0201788977
- ❑ **Key RFCs:**
 - RFC 3775 Mobility Support in IPv6
 - RFC 4068 Fast Handovers for Mobile IPv6
 - RFC 4260 Mobile IPv6 Fast Handovers for 802.11 Networks
 - RFC 4140 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)

Reading Assignment (Cont)

□ Secondary RFCs:

- RFC 1688 IPng Mobility Considerations
- RFC 3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents
- RFC 4225 Mobile IP Version 6 Route Optimization Security Design Background
- RFC 4283 Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4285 Authentication Protocol for Mobile IPv6