Mobile IPv6

Raj Jain
Professor of Computer Science and Engineering
Washington University in Saint Louis
Saint Louis, MO 63130

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse574-10/
Overview

- 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 IPv6 (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:0200:0000:0000:0000:0012: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
Address Auto Configuration

- **Stateful:**
  - Using DHCP

- **Stateless:**
  - Hosts can make a global address using advertised network prefix
  - Interface identifier should be unique
  - Stateless $\implies$ No one needs to keep record of what address was allocated
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
   ⇒ Less overhead. Less state.
5. Neighbor discovery in place of ARP
   ⇒ More general L2
6. Dynamic home agent discovery returns a single reply
Binding Updates

- Binding Update ⇒ Registration
- New Mobility Header
- MH Type=5 ⇒ 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 ⇒ 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

**Diagram:**

1. Home Agent
2. Correspondent
3. Mobile Node

**Packets:**

- Upper layers:
  - CN | HoA | TCP Pkt
  - CN | HoA
  - CN | HoA | TCP Pkt

- On media:
  - CN | CoA | HoA | TCP Pkt
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.
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.

Mobile

- Home Adr Test Init (HOTI)
- Care-of Adr Test Init (COTI)
- COT: with one half of a key
- HOT: with another half of key
- Binding Update (Authenticated)
- Binding Ack

Correspondent

- HOTI
- HOT: Here is another nonce

Home Agent
Return Routability Procedure (Cont)

- Mobile starts this test. Sends HoTI via HA with a cookie.
- CN generates “Home Keygen Token”
  \[\text{= First}(64, \text{HMAC} _{\text{SHA1}}(Kcn, \text{HoA}|\text{nonce}|0))\]
- 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”
  \[\text{= First}(64, \text{HMAC} _{\text{SHA1}}(Kcn, \text{CoA}|\text{nonce}|1))\]
- CN returns CoT containing MN's cookie, Co Keygen Token, CN's nonce index
- Mobile constructs a key and sends an encrypted binding update
  - \[Kbm = \text{Sha1}(\text{Home Keygen Token}|\text{Care-of Keygen Token})\]
  - \[\text{Auth}_\text{data} = \text{First}(96, \text{MAC}(Kbm, \text{Mobility}_\text{data}))\]
  - Mobility_data = CoA|final dest address|Mobility Header data
  - Final Dest Address = CN's Home address if CN is mobile
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.
Who is the router for AP2?
Proxy Solicitation
AR2 is the router. N2 is prefix.
Proxy Advertisement
What Address Can I use?
Fast Binding Update
Use Adrx
Binding Ack
Hi! This is Adrx
Fast Neighbor Advertisement
Welcome to our network!
Neighbor Advertisement Ack

Mobile wants an Adr
Handover Initiate
Use Adrx
Handover Ack
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
Proxy Mobile IPv6

- Mobile nodes do not have any mobility software
- Access points register on behalf of mobile nodes
  ⇒ Easy to deploy
Proxy Mobile IPv6 (Cont)

- IPv6 nodes have 128 bit addresses = Subnet part + Host part
- PMIP enabled access points cache a database of home agents for all subnets that they support
- Authoritative AP keeps the latest copy. Other APs can ask authoritative AP for the correct info.
- When a node connects to the AP, it
  - looks at the subnet address of MN,
  - realizes that it is from a foreign network,
  - finds the home agent and registers its address with it.
  - All packets coming to home address will be forwarded to the AP and then to the mobile.
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
- Proxy Mobile IP allows APs to proxy for mobile nodes
Related Wikipedia Articles

- http://en.wikipedia.org/wiki/Mobile_virtual_private_network
Reading Assignment

- Configuring Proxy Mobile IP,

Key RFCs:
Homework 19

- Read RFC 3775 and make a list of 9 fields that are stored in the binding update list entries.
References: Mobile IPv6 RFCs (Cont)

Secondary RFCs:

References: Mobile IPv6 RFCs (Cont)

References: Mobile IPv6 RFCs (Cont)

References: Mobile IPv6 RFCs (Cont)

- RFC 5419 "Why the Authentication Data Suboption is Needed for Mobile IPv6 (MIPv6)," January 2009.
List of Acronyms

- AH: Authentication Header
- AR: Access Router
- ARP: Address Resolution Protocol
- CGA: Cryptographically Generated Address
- CN: Correspondent Node
- DA: Destination Address
- DAD: Duplicate Address Detection
- DHCP: Dynamic Host Control Protocol
- HA: Home Agent
- HMAC: Hierarchical Message Authentication Code
- ID: Identifier
- IP: Internet Protocol
- IPv4: Internet Protocol V4
- IPv6: Internet Protocol V6
- MAC: Message Authentication Code
List of Acronyms (Cont)

- MAP  Mobile Anchor Point
- MH   Mobility Header
- RFC  Request for Comment
- SA   Source Address
- SIP  Session Initiation Protocol
- TCP  Transmission Control Protocol