Mobile IPv6 Update

David B. Johnson

The Monarch Project

Carnegie Mellon University

`http://www.monarch.cs.cmu.edu/`

`dbj@cs.cmu.edu`

47th IETF, Adelaide, Australia

March 26–31, 2000

Carnegie Mellon

Overview of Recent Changes

I submitted ***draft-ietf-mobileip-ipv6-10.txt*** on February 10:

- Issues raised at last IETF meeting (Washington, DC)
- Some issues raised on mailing list and private email

I submitted ***draft-ietf-mobileip-ipv6-11.txt*** on March 10:

- Issues raised by implementors at Mobile IPv6 interoperability testing at ***Connectathon 2000*** that week
- A few more issues raised on mailing list and private email

Areas of changes since last IETF meeting:

- IPsec processing
- Duplicate Address Detection
- Movement detection
- Dynamic Home Agent Address Discovery
- Miscellaneous

Interaction with Outbound IPsec Processing

Added in version 09 of the draft (October 1999):

- Packet is created by higher layers as if at home, with IP header Source Address set to home address
- As part of outbound packet processing in IP, packet is compared against the IPsec Security Policy Database (SPD)
- Special case for Mobile IP:
  - If a Binding Update or Acknowledgement is included, authentication and replay protection MUST be applied
  - If already required by SPD, this is sufficient
  - Otherwise, create temporary SPD entry for handling this packet
- If IPsec processing is required, find SA or create new SA
- Insert Home Address option in packet and change addresses
- Add a Binding Update to the packet if needed
- Finally, any necessary authentication/encryption is computed

Use of IKE

Problems in normal use of IKE for making SA for Binding Updates:

- Need the SA to authenticate the Binding Update
- Nodes that we need to communicate with (e.g., responder or DNS) may need binding to reply to us

Luckily, IKE has an existing solution that we can reuse here:

- ISAKMP ***Identification Payload*** defined to tell responder who we are so it can find our public key
- Used, for example, by security gateways

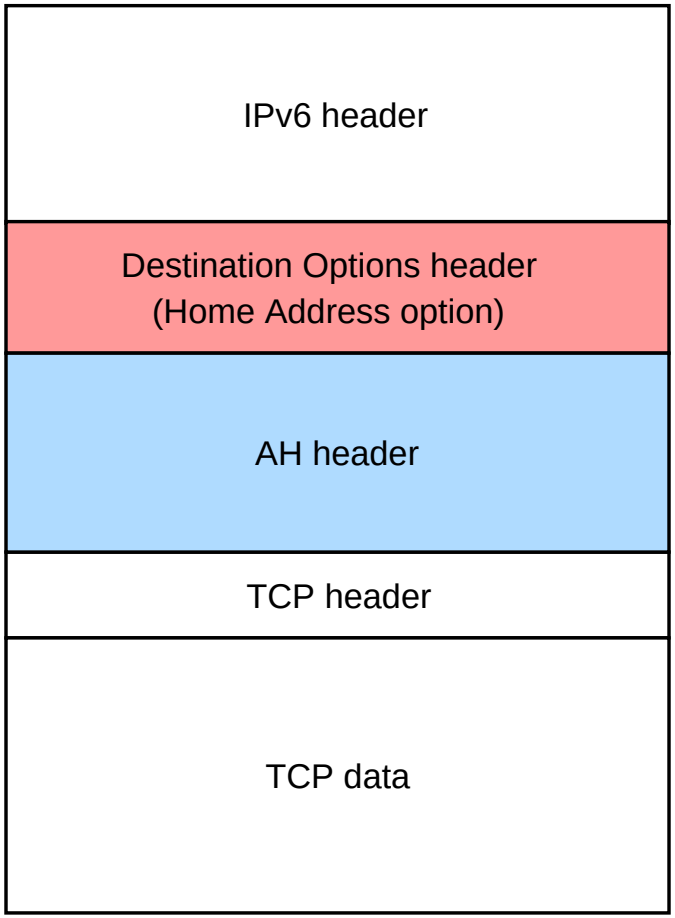
For Mobile IP, in effect pretend that mobile node is a security gateway running IKE on behalf of mobile node:

- Mobile node must use its care-of address as the Source Address of all packets part of SA setup
- Must not include Home Address option (no use of Mobile IP)
- Must include an ISAKMP Identification Payload in IKE exchange, giving mobile node's home address as SA initiator

Order of Headers and Processing with AH

Home Address option must appear ***above*** AH header:

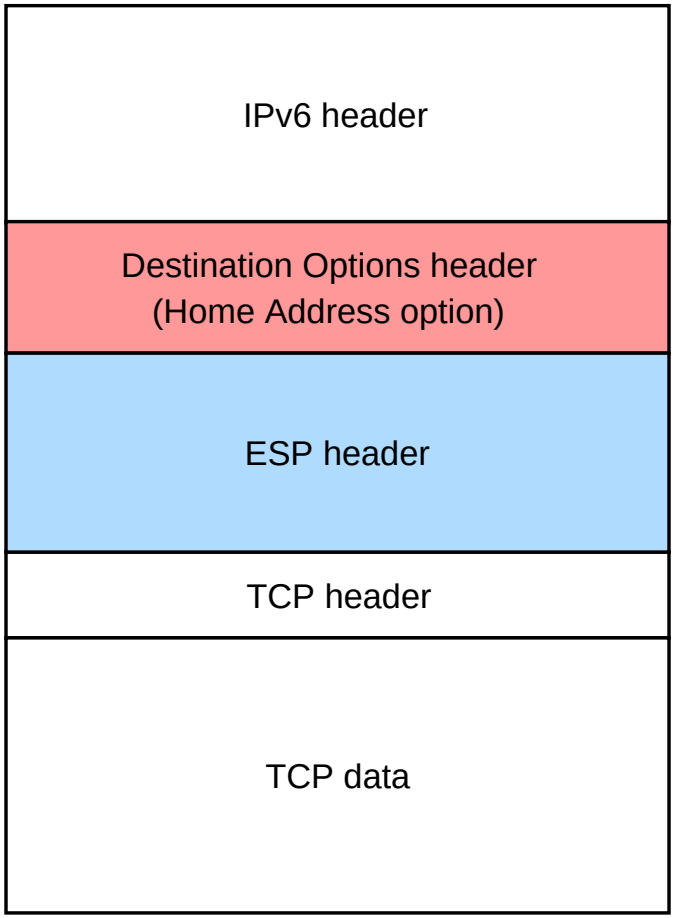
- Outbound Home Address option addition is done ***after*** SA selection
- Inbound Home Address option processing is done ***before*** SA selection
- SA thus always sees only the home address
- No need to establish new SA for each new care-of address
- ***AH protects the entire packet, even the part above the AH header***
- Any needed Binding Update can go above or below AH header



Order of Headers and Processing with ESP

Home Address option must still appear ***above*** AH header:

- Don’t want to establish new SA for each new care-of address
- Thus Home Address option again must appear ***above*** ESP header
- ***But ESP protects only the part of the packet below the ESP header!***
- Binding Update should go ***below*** ESP header
- But home address for binding is not protected!
- Normal care-of address is also not protected but can already put it in Binding Update



Possible Solutions to ESP Problem

Use only AH, not ESP, for authentication of Binding Updates:

- This is what is specified now (version 11 of the draft)
- It's simple, and it works
- ESP can be used too, for example if data needs to be encrypted
- But that means overhead for space of extra header: AH is 24 bytes plus size of Authentication Data (I think minimum total is 36 bytes)
- And overhead of extra crypto transform on packet

Or repeat critical fields inside the Binding Update:

- Can already put care-of address in Binding Update (overrides IP header Source Address)
- Could add sub-option to be able to put home address there too
- This is all protected by ESP if below ESP header
- On receipt, verify that it is same as Home Address option

Duplicate Address Detection for Home Address

While away from home:

- Added a Duplicate Address Detection (D) bit in the Binding Update
- Requests mobile node's home agent to perform DAD on the mobile node's home link for the home address in this binding
- Returns new Status value of 138 (Duplicate Address Detection failed) in Binding Acknowledgement, if failure

When returning home:

- Mobile node needs to send a Binding Update to its home agent
- But home agent is defending mobile node's home address for DAD
- Home agent also is set to tunnel home address to care-of address
- Mobile node Neighbor Solicitation for home agent would be detected by home agent as duplicate use of home address
- Mobile node may already know home agent link-layer address, for example from Router Advertisements
- If Neighbor Solicitation needed, must set Solicitation source address to the unspecified address
- Mobile node must not perform DAD on its own address

Performing DAD for Care-of Addresses

IPv6 says perform DAD before assigning a new address:

- Defined in RFC 2462 (IPv6 Stateless Address Autoconfiguration)
- Used for all addresses, whether stateless or stateful
- For stateless, can test only link-local address if all others use the same interface identifier

Problem for Mobile IPv6:

- Mobile node would need to perform DAD for each new care-of address, ***each time it moves!***
- DAD takes a “long” time:
  - Mobile node sends DupAddrDetectTransmits (default: 1) Neighbor Solicitations, each separated by RetransTimer (default: 1 second)
  - If first message to be sent from an interface after interface (re)initialization, should random delay between 0 and MAX_RTR_SOLICITATION_DELAY (1 second)

Can We Avoid This?

Is DAD for each address really required?

- RFC 2462 is ambiguous and contradictory on this
- “Duplicate Address Detection MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration”
- “For safety, all addresses must be tested for uniqueness prior to their assignment to an interface”
- “Each individual unicast address SHOULD be tested for uniqueness”

Can we optimize the use of DAD in any way?

- For example, random delay for MAX_RTR_SOLICITATION_DELAY should be safe to skip
- Designed to randomize many hosts all booting at the same time
- But in a foreign network, we aren’t booting
- Also, can we perform DAD in parallel with normal use?

Movement Detection for Mobile Nodes

Mobile node's must be able to detect when they move:

- For example, wireless movement out of range of access point
- Need to detect this and configure a new care-of address from some new router from which you hear Router Advertisements
- Defined mechanism is deliberately flexible, to allow choice by implementors
- But an incorrect implementation at Connectathon made us think more about the defined mechanism

Planning to define a more specific movement detection mechanism:

- Want something that allows quick movement detection
- Want something that works with non-mobile-aware local routers
- Need to detect new and missed Router Advertisements, plus expiration of Default Router List and Prefix List entries
- But its hard to know when you've missed a Router Advertisement
- Can also supplement with lower layer information on some links

Dynamic Home Agent Address Discovery

Originally specified use of anycast Binding Update is awkward:

- All Binding Updates must be authenticated
- But this one can't be, since destination is anycast address
- And it really is very different than normal Binding Update processing

New mechanism defined in version 11 of draft:

- Mobile node sends ***ICMP Home Agent Address Discovery Request*** to home agent anycast group
- Some home agent on home link responds with ***ICMP Home Agent Address Discovery Reply***
- Reply contains ordered list of home agents
- Removed Home Agents List Sub-Option definition and Binding Acknowledgement option Status value of 135 (dynamic home agent address discovery response)
- Still need ICMP type code assignments from IANA (I've requested them)

Miscellaneous

Slight change to description of the Home Agents List:

- Each mobile node must maintain a Home Agents List (in addition to all home agents)
- Needed by mobile node, to be able to send Binding Update to a home agent on previous link after moving

Sequence numbers in Binding Updates:

- For retransmitted Binding Updates, Sequence Number field must be greater than in previous transmission
- Change is needed in order to handle case in which original Binding Update was received but Binding Acknowledgement (instead of the Binding Update) was lost
- Changing the Sequence Number also avoids any ambiguity about when binding lifetime starts

Fixed a few more typos here and there in the draft