Route Optimization in Mobile IP

David B. Johnson
Carnegie Mellon University

Charles Perkins
IBM Corporation

<draft-ietf-mobileip-optim-03.txt>
(with modifications)

34th IETF, Dallas, December 4–8, 1995

Mobile IP Route Optimization

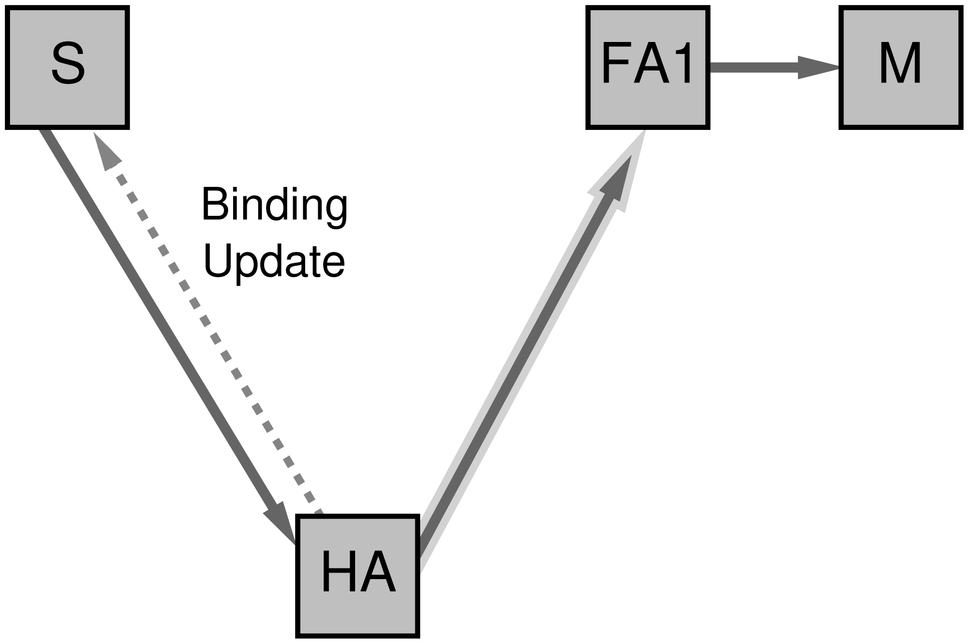
Route optimization allows a correspondent node to

- Learn current binding of mobile node,
- Cache this binding in a ***binding cache***, and
- Tunnel own packets directly there

General Route Optimization strategy:

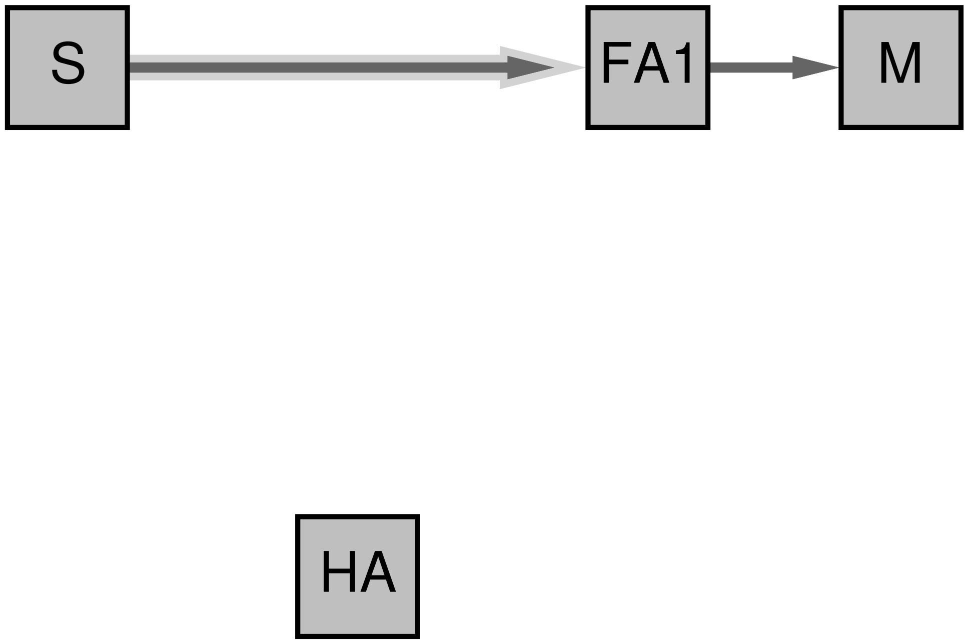
- Learn binding as a result of indirect routing
- Tunnel own packets based on binding cache entries
- If cache entry is out-of-date, get the packet there anyway and update the cache

Sending the First Packet to a Mobile Node



Home agent returns authenticated ***binding update*** to sender

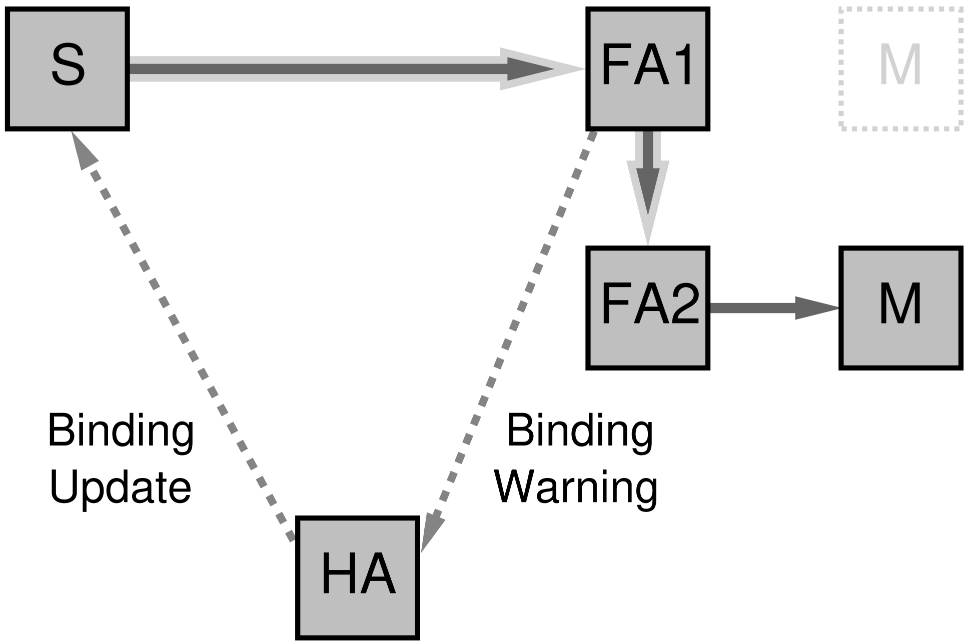
Once Sender Has a Binding Cache



Packets are tunneled directly to current foreign agent

(Minimal tunneling protocol adds only 8 bytes)

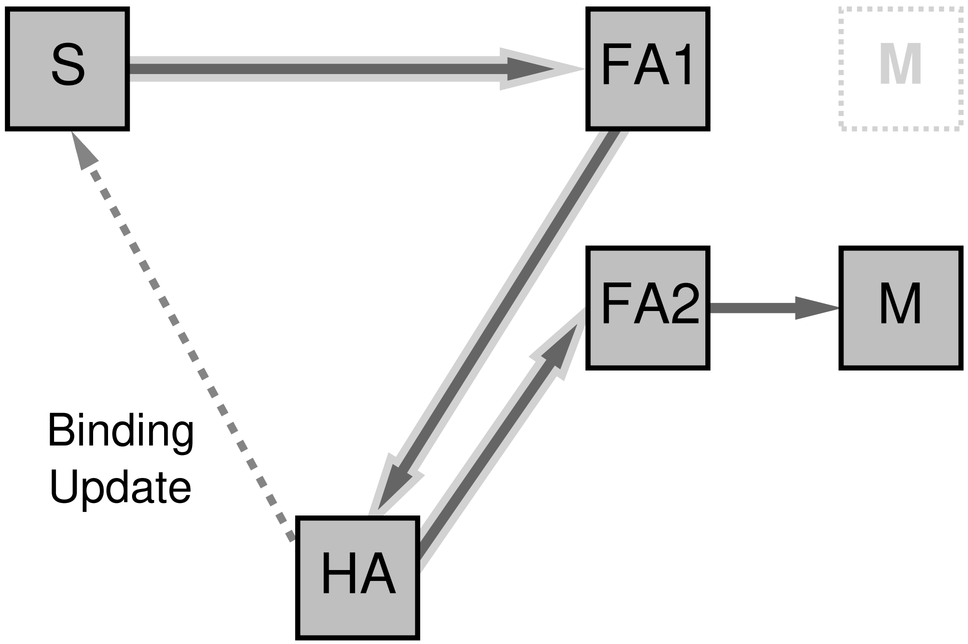
Sending First Packet After Movement



Previous foreign agent cache acts is forwarding pointer

Binding warning tells home agent to send authenticated binding update

If Previous Foreign Agent Cache Is Dropped



Previous foreign agent forwards as a ***special tunnel***:
Inner and outer destination is mobile host home address

Home agent can avoid tunneling back to same foreign agent

Foreign Agent Registration Keys

Optionally establish ***registration key*** during registration

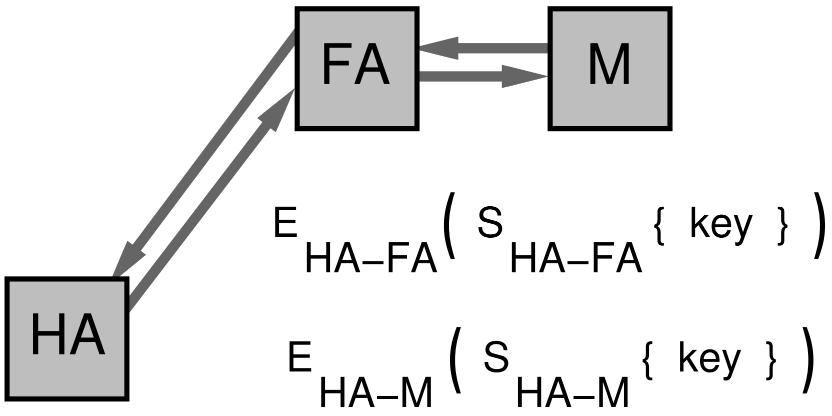
Secret shared between mobile node and current foreign agent:

- Use to authenticate notification to foreign agent of move to next care-of address
- Could also use to encrypt packets between mobile node and its current foreign agent

Two alternative methods for establishing:

- Using the home agent as a ***Key Distribution Center***
- Using ***Diffie-Hellman*** key exchange protocol
- Using mobile node ***RSA public key*** to send registration key

Option 1: Home Agent as KDC

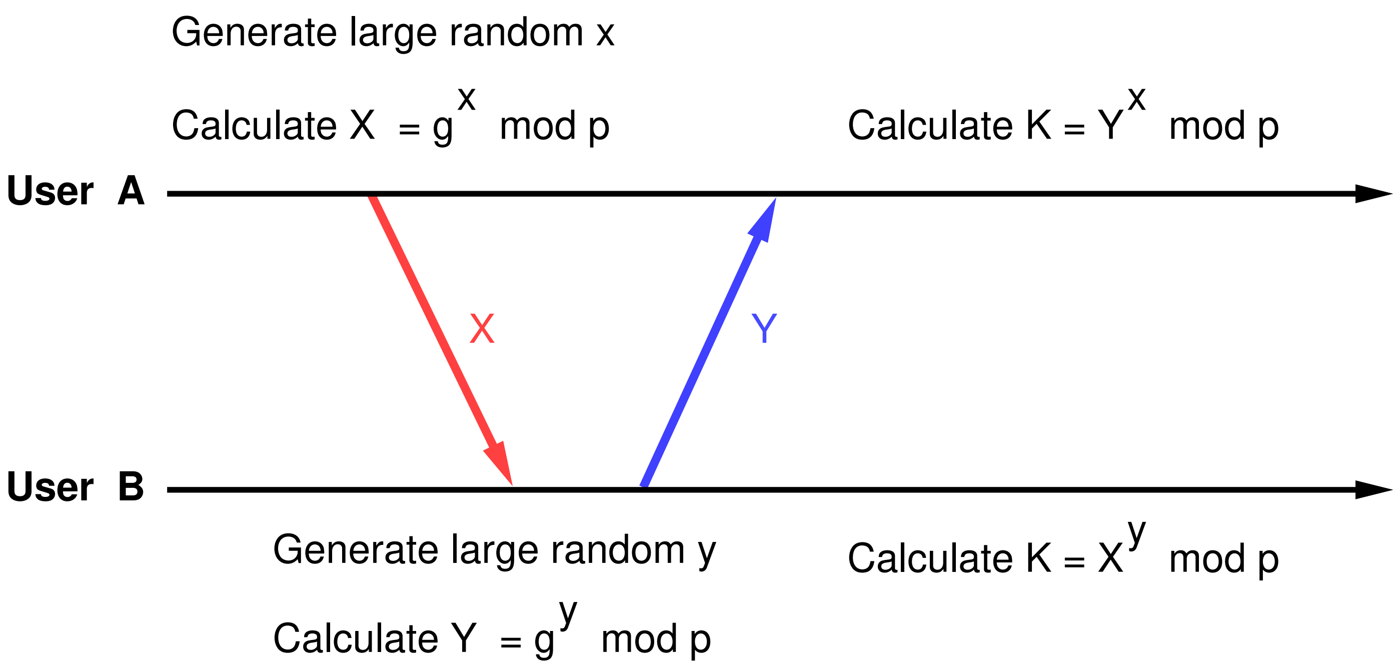


Foreign agent must have security association with home agent

Mobile node registers new binding with home agent

Home agent returns new registration key to both

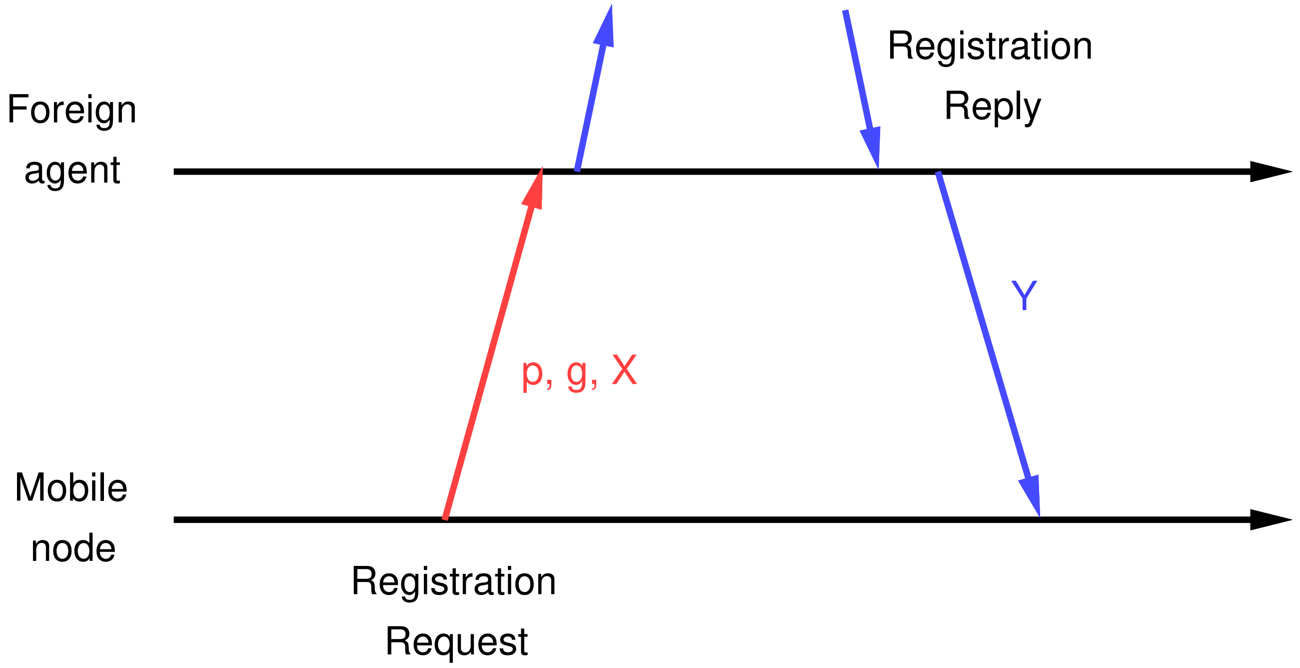
Option 2: Diffie-Hellman Key Exchange



Public values: a large ***prime*** number p, and ***generator*** g $<$ p

K is resulting shared secret key

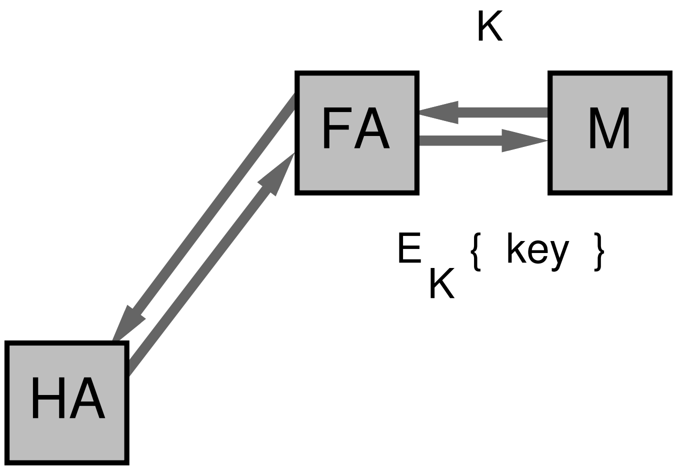
Diffie-Hellman with Foreign Agent



Mobile node sends prime, generator, X in Registration Request

Foreign agent replies with Y in Registration Reply

Option 3: Using a Mobile Node RSA Public Key

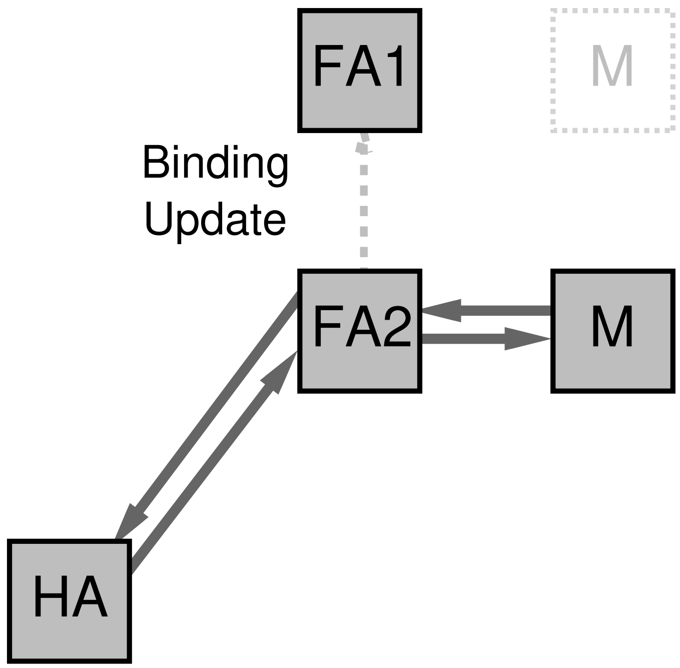


Mobile node sends its RSA public key in Registration Request

Foreign agent chooses a registration key

Foreign agent encrypts and returns it in Registration Reply

Notifying Previous Foreign Agent



Include authenticated notification in new Registration Request:

- New foreign agent just forwards to previous foreign agent
- Mobile node gets acknowledgement, does retransmissions