Route Optimization

Charles E. Perkins

David B. Johnson

cperkins@eng.sun.com

dbj@cs.cmu.edu

Route Optimization

new draft available:

draft-ietf-mobileip-optim-06.txt

Basic parts reflected in reorganized draft:

- Overview
- Binding Cache Maintenance
- Smooth Handoff
- Registration Key
- Special Tunnels

Binding Cache Maintenance

- Binding Warning
- Binding Request
- Binding Update
- Binding Acknowledgement

Home Agent typically supplies a Binding Update to Correspondent Node after Binding Warning

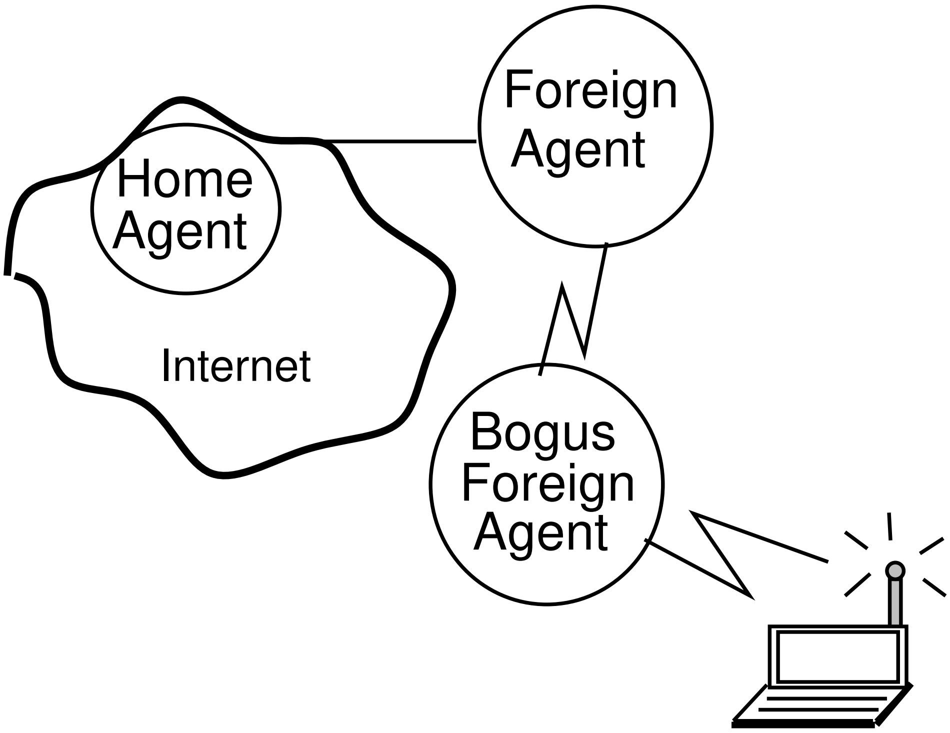
Binding Warning may be supplied to Correspondent Node by any node – especially previous foreign agent

Smooth Handoffs

Mobile Node supplies Binding Update to previous FA to enable previous FA to forward ”packets in flight”.

- Short timeout
- Registration Key required for secure operation

Registration Key Acquisition



- Want to use SA's or public keys when available
- Want to use Diffie-Hellman as a last resort
- Man-in-the-middle attacks
- Let HA be KDC, or consult a KDC

Algorithm at Foreign Agent

Set 'S' bit in advertisements.

```
if (previous foreign agent notification) {
        /* build the binding update and authentication extension */
}

/* Set up registration key */
if (have security association with HA) {
        /* Append FA key request to registration request */
}
else if (have a public key) {
        /* append FA Public Key request to registration request */
}
else if (have mobile node's public key) {
        /* pick a good key */
        /* append FA public key reply to registration request */
}
else if (want D-H exchange) {
        /* do the computation */
        /* append it to the registration key request */
else {
        /* do nothing */
        /* Home agent can approve the registration request anyway */
}
```

Special Tunnels

- Problem: an old FA *could* send stray MN packets to Home Network, but routing loops would be created if HA thinks that the MN is still using the care-of address at the old FA.
- Solution: the old FA *tunnels* the packet to the MN's Home address. Then:
  - inner source = Correspondent Node
  - outer source = old FA
  - inner dest = Mobile Node
  - outer dest = Mobile Node
- If Home Agent detects that inner_dest == outer_dest and the mobile node is *NOT* at the old FA's care-of address, then it can tunnel the packet again