# Advanced Topics in Computer Networks

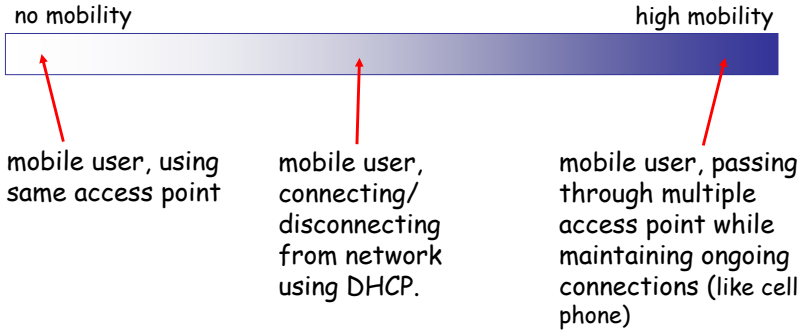
# Mobile IP

Chalermek Intanagonwiwat

Slides courtesy of James F. Kurose, Keith W. Ross, Golden G. Richard III, Mary Baker, Olaf Meyer, and Charles Perkins

# What is mobility?

- spectrum of mobility, from the *network* perspective:




# Mobility Impact on Protocol Stack

| Networking Layers | Standard Protocols |
|---|---|
| Applications | HTTP, NFS, SNMP, DNS, Telnet, FTP, … |
| Window Mgr | |
| Sockets | |
| Transport | TCP, UDP, RTP |
| Network | IP, ICMP, IGMP, IPSec, Mobile IP … (IPX, Appletalk) |
| Data Link | IEEE 802.*, PPP |
| Physical | Network adapter |

# Mobility Impact on Protocol Stack (cont.)

- Top layer (application layer)
  - Automatic configuration
  - Service discovery
  - Link awareness → adaptability
  - Environment awareness
- Layer 4 (transport layer)
  - Congestion control is based on packet loss
  - However, packet loss → congestion?
  - Other reasons for packet loss
    - Noisy wireless channel, During handoff process

# Mobility Impact on Protocol Stack (cont.)

- Layer 3 (network layer)
  - Changing the routing of datagrams destined for the mobile nodes
- Layer 2 (data link layer)
  - Collision detection → collision avoidance
  - Dynamic range of the signals is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmissions
  - Cell size (frequency reuse)

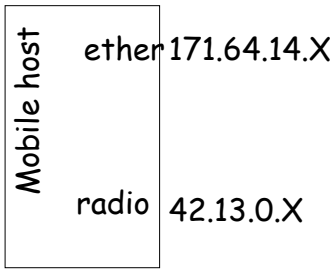
# Internet Protocol (IP) Review

- Network layer, "best-effort" packet delivery
- Supports UDP and TCP (transport layer protocols)
- IP host/interface addresses consist of two parts
  - **network id + host id**
- By design, IP host address is tied to home network address
  - Hosts are assumed to be wired, immobile
  - Intermediate routers look only at network address
  - Mobility without a change in IP address results in un-route-able packets

# Domains versus interfaces

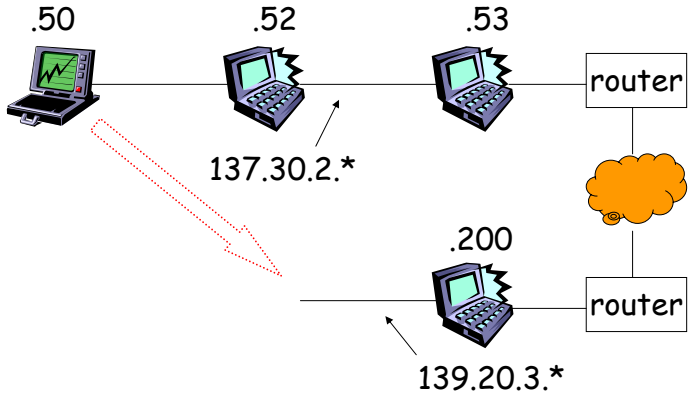
- Switching domains & switching interfaces are the same problem at the routing level

Network interfaces:



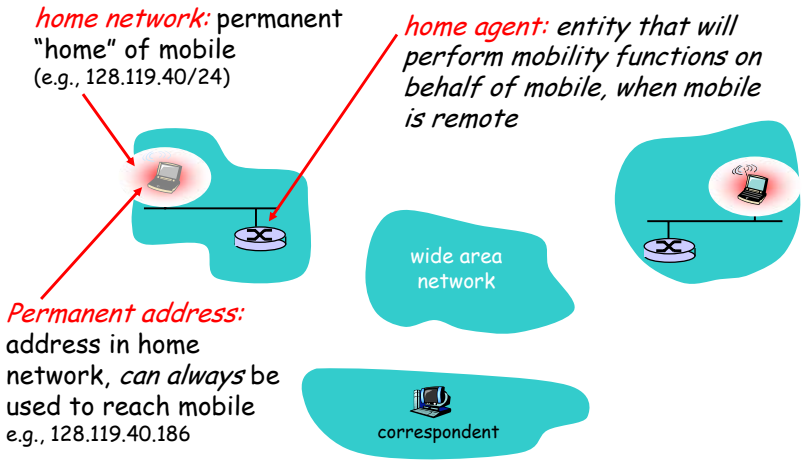

Administrative domains:


# IP Routing Breaks Under Mobility

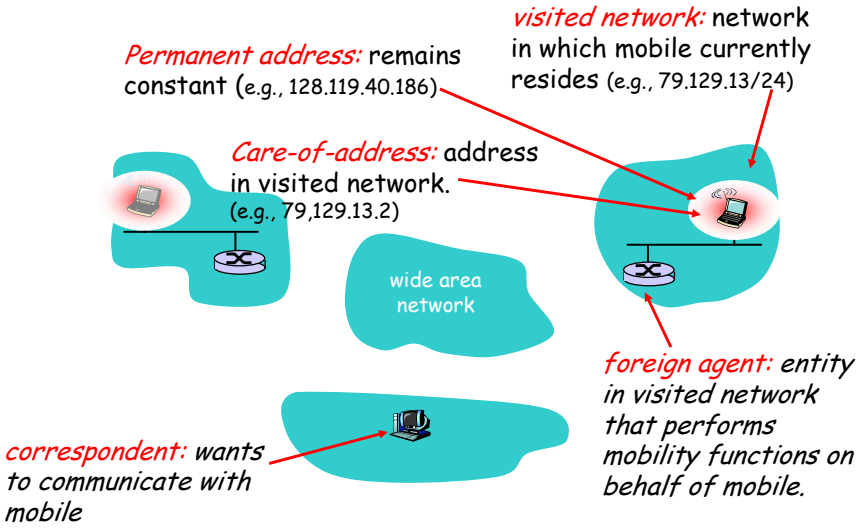



Why this hierarchical approach? Answer: **Scalability! Millions of network addresses, billions of hosts!**

# Mobility: Vocabulary




# Mobility: more vocabulary




# How do *you* contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?

- search all phone books?
- call her parents?
- expect her to let you know where he/she is?


# Mobility: approaches

- *Let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems

# Mobility: approaches (cont.)

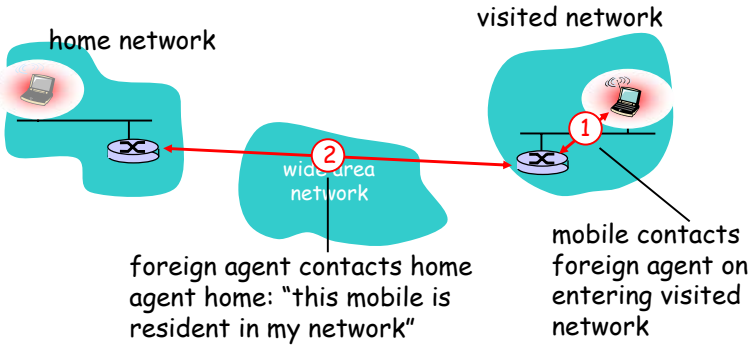
- *Let routing handle it:* routers advertise permanent addresses of mobile-nodes-in-residence via routing table exchange.
  - routing table indicates where each mobile located
  - no changes to end-systems

not scalable to millions of mobiles

# Mobility: approaches (cont.)

- *Let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

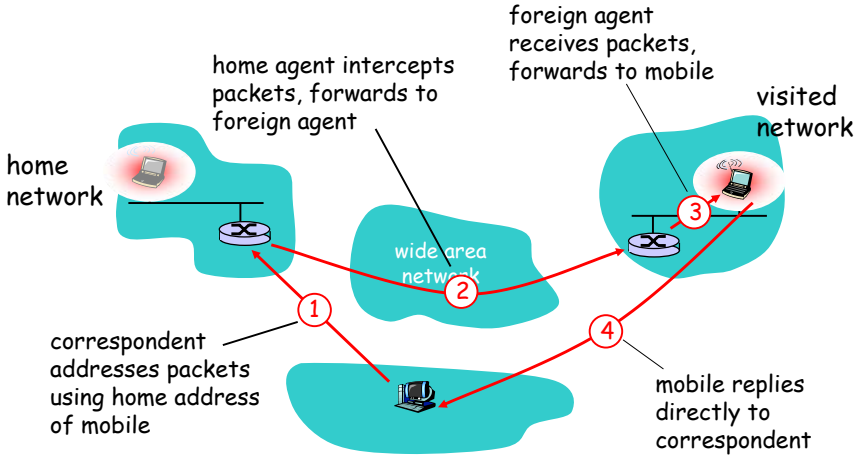
# Mobility: registration




End result:

- Foreign agent knows about mobile
- Home agent knows location of mobile

# Mobility via Indirect Routing

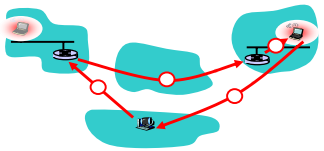


# Indirect Routing: comments

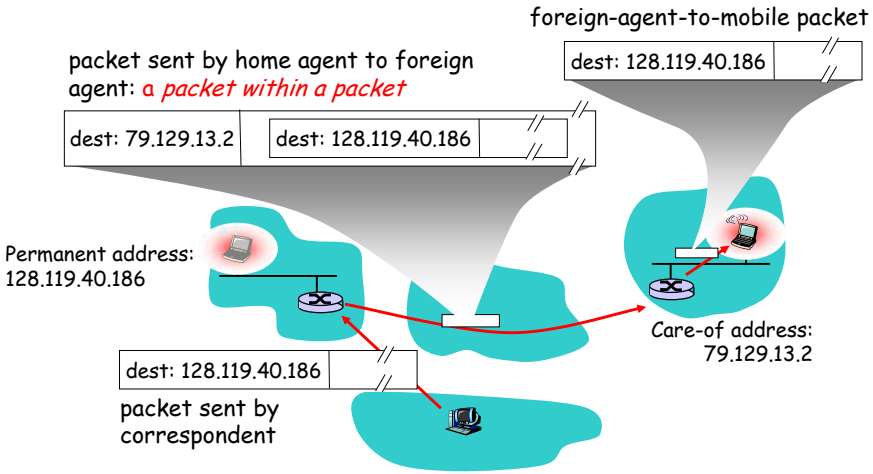
- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself

# Indirect Routing: comments (cont.)

- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



# Forwarding datagrams to remote mobile




# Packet addressing

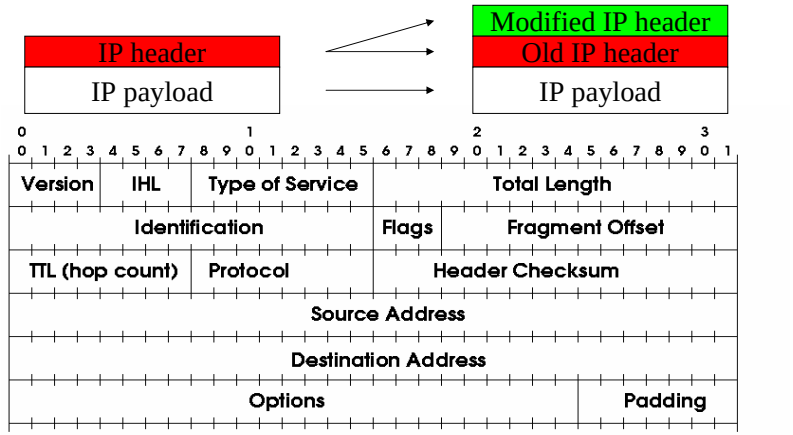
Packet from CH to MH

| Source address = address of CH |
|---|
| Destination address = home IP address of MH |
| Payload |

Home agent intercepts above packet and tunnels it

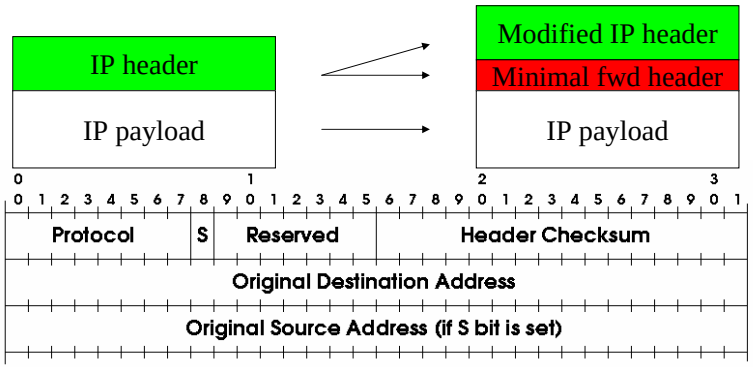
| Source address = address of HA |
|---|
| Destination address = care-of address of MH |
| Source address = address of CH |
| Destination address = home IP address of MH |
| Original payload |

# IP within IP Encapsulation




- New header fields …
  - destination Address: "care-of address"
  - source Address: address of encapsulating host
  - protocol number: 4

# Minimal Encapsulation




- Modified header …
  - destination Address: "care-of address"
  - source Address: address of encapsulating host (opt.)
  - protocol number: 55
- adds less overhead but needs a **complete** IP packet before encapsulation

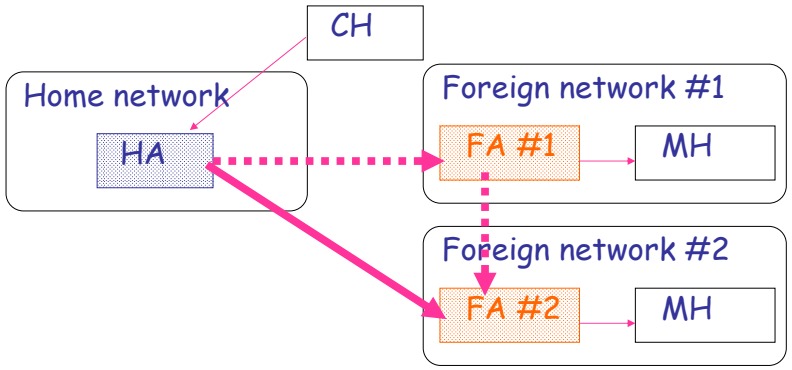
# Indirect Routing: moving between networks

- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)

# Indirect Routing: moving between networks (cont.)

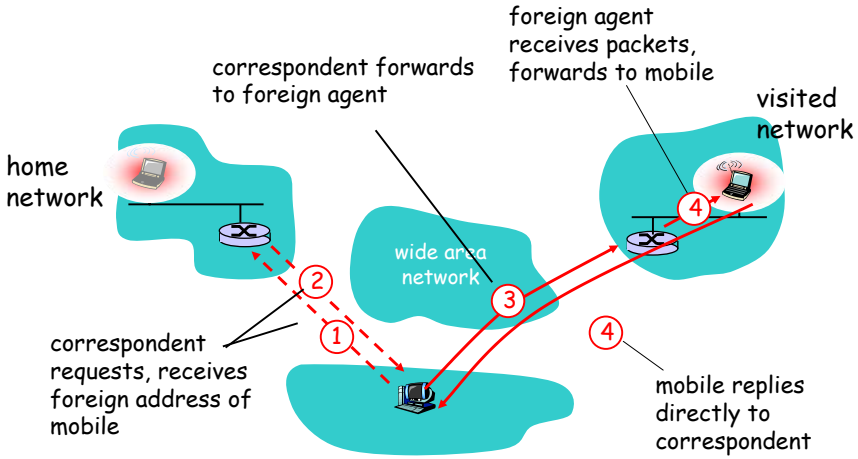
- Mobility, changing foreign networks transparent: *on going connections can be maintained!*

# When mobile host moves again



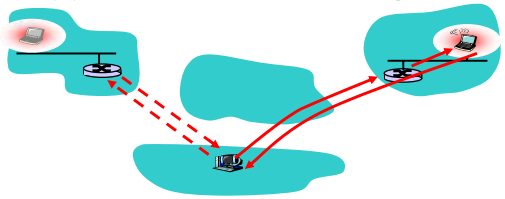

- MH registers new address (FA #2) with HA & FA #1
- HA tunnels packets to FA #2, which delivers them to MH
- Packets in flight can be forwarded from FA #1 to FA #2

# Mobility via Direct Routing




# Mobility via Direct Routing: comments

- overcome triangle routing problem
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - What happens if mobile changes networks?



# Mobile IP

- RFC 3220
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - agent discovery
  - registration with home agent
  - indirect routing of datagrams

# Why Mobile IP?

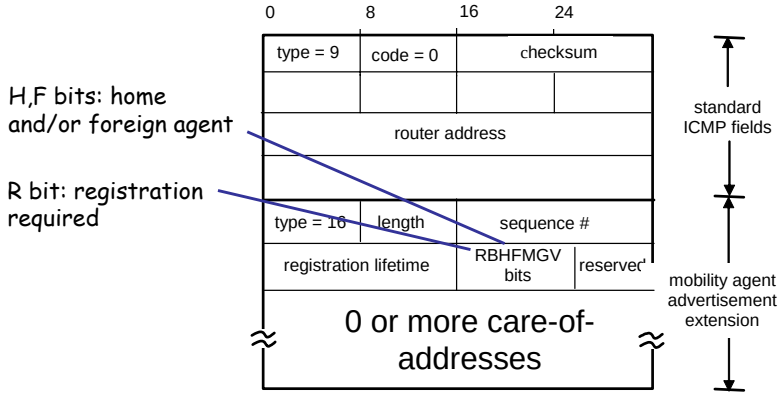
- Need a protocol which allows network connectivity across host movement
- Protocol to enable mobility must not require massive changes to router software, etc.
- Must be compatible with large installed base of IPv4 networks/hosts
- Confine changes to mobile hosts and a few support hosts which enable mobility

# Why Mobile IP? (cont.)

- Just hacking DNS won't work
  - DNS updates take time
  - Hooks for normal users to update DNS won't be accepted by administrators
  - After DNS lookup, raw IP address is used by TCP, UDP, …

# Mobile IP: agent discovery

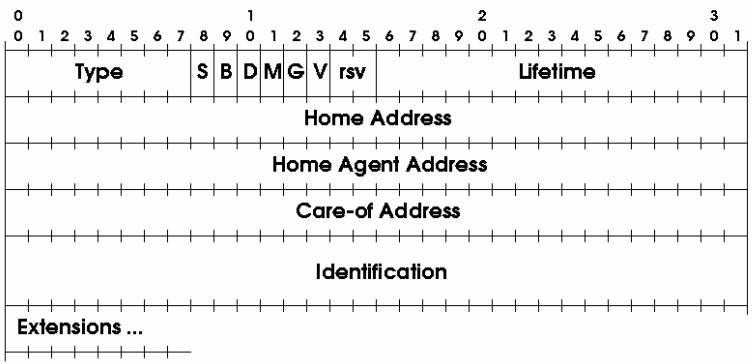
- agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (type field = 9)




# Mobile IP: registration

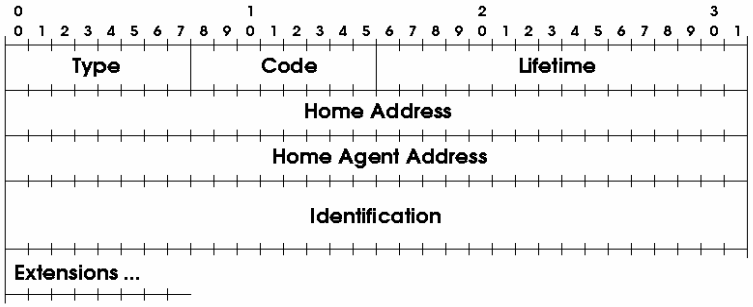
- Registration Request
  - Sent to home agent
  - New IP address
  - Flags to indicate whether broadcast traffic should be delivered
  - Security information to prevent remote redirects/replay attacks (more soon)
- Registration Reply
  - ACK or an error

# Registration Request



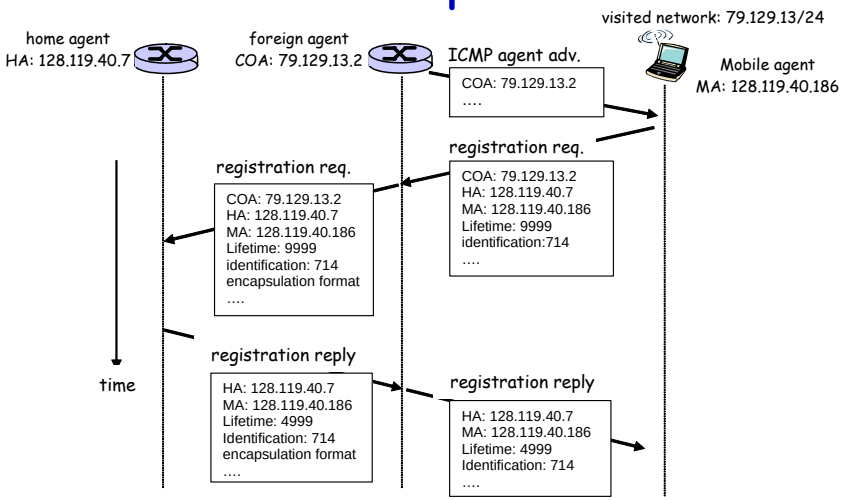

- *Mobile-Host* authentication extension required
- Identification used for replay protection
- Uses UDP messages

# Registration Reply




- *Code* field describes status information, e.g. why the registration failed. These include
  - authentication failed
  - ID mismatch (resynchronization needed)
  - unknown HA

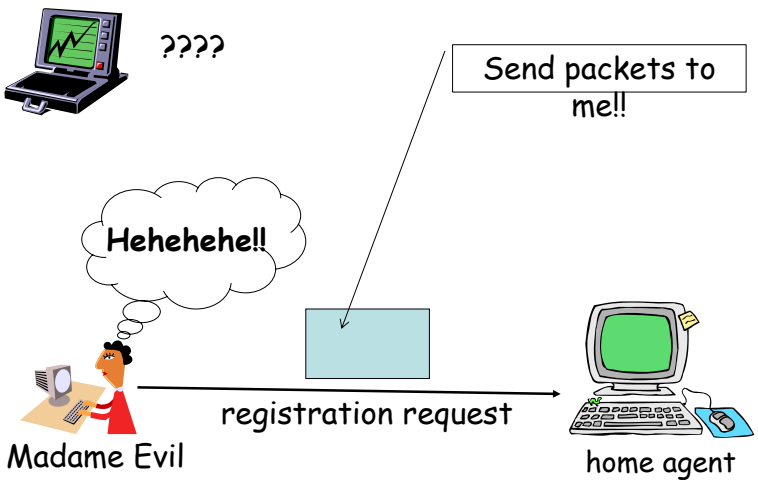
# Mobile IP: registration example




# Problem: Security

- Bogus registration (denial of service) attacks
  - Malicious host sends fake registration messages to home agent "on behalf" of the mobile host
  - Packets could be forwarded to malicious host

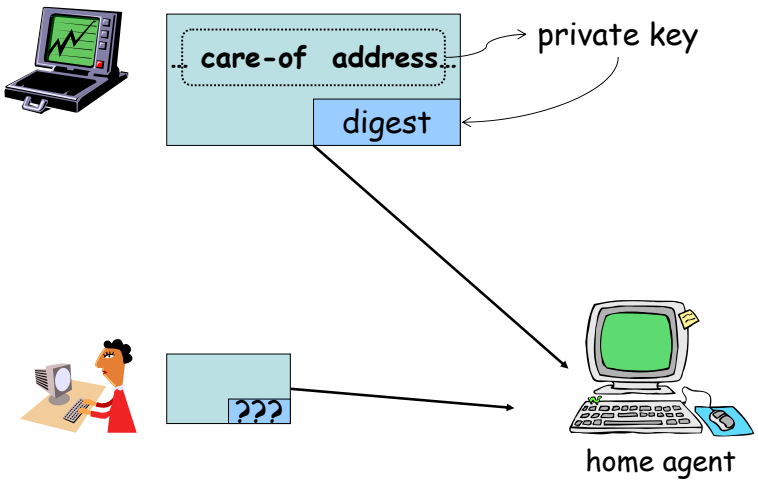
# Bogus Registration Attack



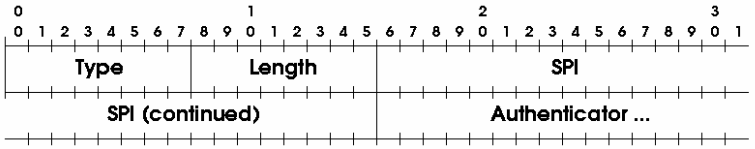

# Authentication

- To fix this problem, *authenticate* registration attempts
- Use keyed message hashing to generate a *message digest*
  - MD5: see RFC 1321
- Home agent generates hash using shared private key to message to see if message digest is identical

# Authentication (cont.)

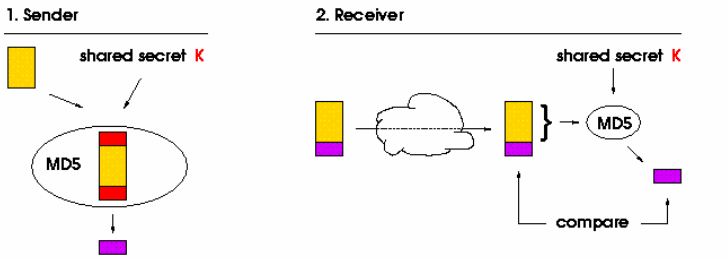



# Authentication Extension



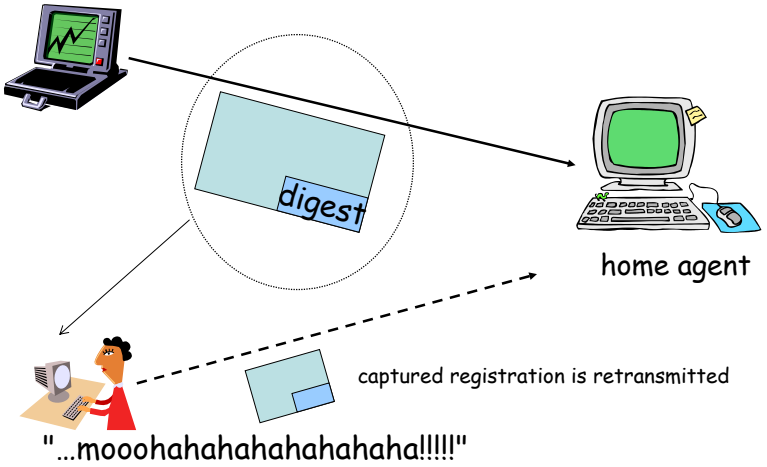

- *Type* field determines the entities involved in the authentication
  - Mobile-Home
    (required for all registration requests and replies)
  - Mobile-Foreign
  - Foreign-Home

# Authentication using MD5




- MD5 algorithm computes a one-way cryptographic hash code (128-bit fingerprint)
- communicating parties share a secret key
- secret key is not sent as part of the communication
- Mobile IP draft requires default support of keyed MD5

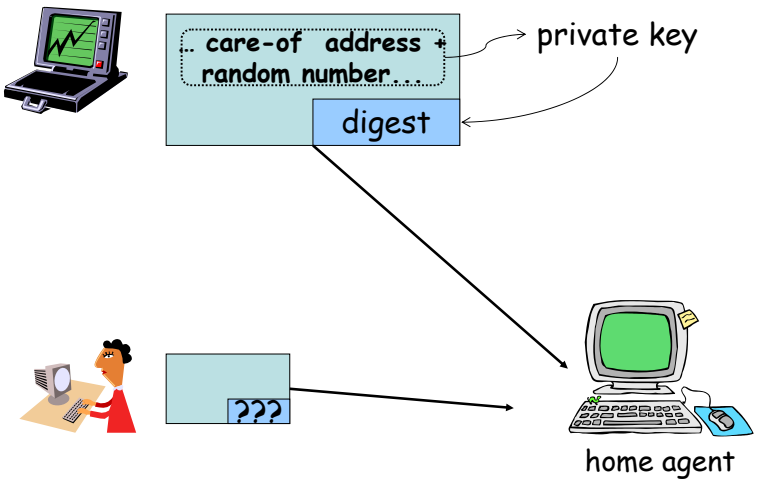
# Ooops. Replay Attacks!




# Avoiding Replay Attacks

- Avoid replay attacks by making registration requests unique
- Add time or a pseudo-random number to registration request/reply
- If time or random number is out of sync, provide info to resync in rejection
- Insufficient information to help malicious host
- Counter instead of time/random number not as good
- Would allow storing a 'set' of registration requests

# Random Number Avoids Replay



## ARP Problem: On the Home Network

- If the HA is the gateway host then picking up packets destined for the MH is trivial
- If the HA is **not** the gateway host then the proxy ARP must be used
- The HA pretends to be MH and responds to requests for MH's physical address (e.g. Ethernet address) with its own physical address
- ARP caches on all hosts have to be updated upon registration of the MH (gratuitous ARP)

## ARP Problem: On the Foreign Network

- The "care-of" address used for encapsulation may belong to the FA or may be a temporary address acquired by the Mobile Host (e.g. via DHCP)
- The MH must never send ARP frames on a foreign network
- The MH can obtain the FAs link-layer address from the *agent advertisement* messages

## Problems with Foreign Agents

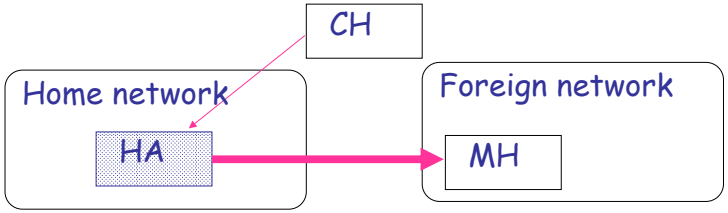
- Assumption of support from foreign networks
  - A foreign agent exists in all networks you visit?
  - The foreign agent is robust and up and running?
  - The foreign agent is trustworthy?

## Problems with Foreign Agents (cont.)

- Correctness in security-conscious networks
  - We'll see that "triangle route" has problems
  - MH under its own control can eliminate this problem
- Other undesirable features
  - Some performance improvements are harder with FAs
- We want end-to-end solution that allows flexibility

# Solution

•Mobile host is responsible for itself
-(With help from infrastructure in its home network)
-Mobile host decapsulates packets
-Mobile host sends its own packets
-"Co-located" FA on MH




⇒MH must acquire its own IP address in foreign network
This address is its new "care-of" address
Mobile IP spec allows for this option

# Obtaining a foreign IP address

- Can we expect to obtain an IP address?
  - DHCP becoming more common
  - Dynamic IP address binding like some dial-up services
  - Your friend can reserve an IP address for you
  - More support for dynamic IP address binding in IPv6
- This assumes less than getting others to run a FA

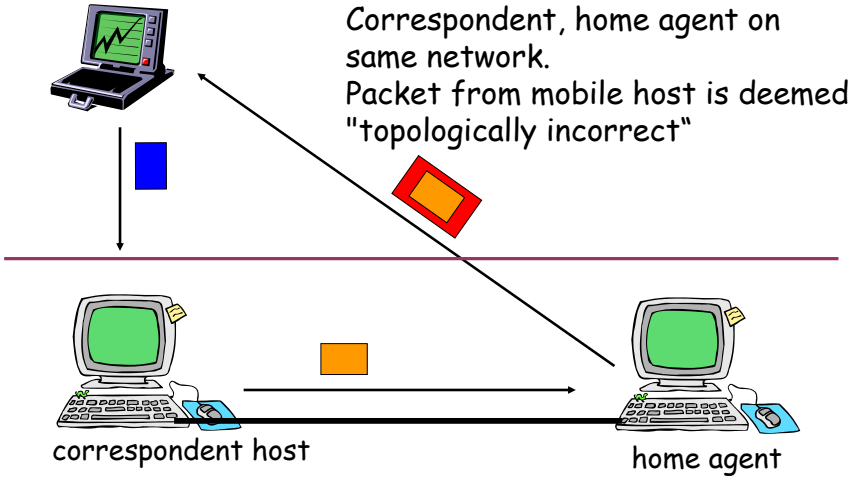
# Design implications

- New issues: the mobile host now has two roles:
  - Home role
  - Local role
- More complex mobile host
- Loss of in-flight packets?
  - This can happen anyway

# Problems with ingress filtering

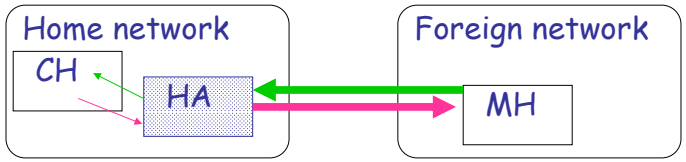
- Mobile host uses its home IP address as source address
- Security-conscious boundary routers will drop this packet
  - Routers which see packets coming from a direction from which they would not have routed the source address are dropped

# Packets Dropped: "Ingress" Filtering




# Solution: bi-directional tunnel

•Provide choice of "safe" route through home agent both ways



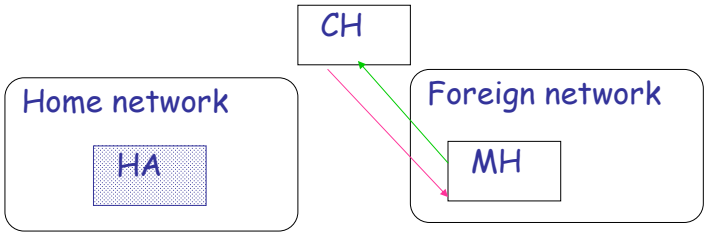

•This is the slowest but most conservative option

At the other extreme…

# Problem: performance

- Example: short-lived communication
  - When accessing a web server, why pay for mobility?
  - Do without location-transparency
  - Unlikely to move during transfer; can reload page
  - Works when CH keeps no state about MH

# Solution: yet more flexibility




•Use current care-of address and send packet directly
-This is regular IP!

•More generally:
-MH should have flexibility to adapt to circumstances
-A range of options: from slow-but-safe to regular IP
-Should be an end-to-end packet delivery decision (no FA)

# Routing options

- Allow MH to choose from among all routing options
- Options:
  - Encapsulate packet or not?
  - Use home address or care-of address as source address?
  - Tunnel packet through home agent or send directly?

# Routing options (cont.)

- Choice determined by:
  - Performance
  - Desire for transparent mobility
  - Mobile-awareness of correspondent host
  - Security concerns of networks traversed
- Equivalent choices for CH sending packets to MH

# Mobility 4x4

| | Outgoing Indirect, Encapsulated | Outgoing Direct, Encapsulated | Outgoing Direct, Home Address | Outgoing Direct, Temp. Address |
|---|---|---|---|---|
| Incoming Indirect, Encapsulated | Most reliable, least efficient | Requires decapsulation on CH | No security-conscious routers on path | |
| Incoming Direct, Encapsulated | | Requires fully mobile-aware CH | No security-conscious routers on path | |
| Incoming Direct, Home Address | | | Requires both hosts to be on same net. seg. | |
| Incoming Direct, Temp. Address | | | | Most efficient, no mobility support |

# Figuring out which to use

- With bidirectional tunneling
  - Probe destination using triangle route
  - If it works, switch to that option
- With triangle route
  - If packets aren't getting through after some number of tries, switch to bidirectional tunneling

# Mobile IP: Conclusions...

- Great potential for mobile application deployment using Mobile IP
- Minimizes impact on existing Internet infrastructure
- Security issues are important
- Several working implementations (e.g., Monarch project at CMU)