Mobile IP

Scalable Support for Transparent Host Mobility on the Internet

Olaf Meyer
University of Pennsylvania

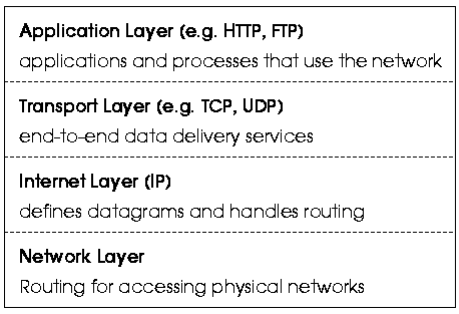
References

- **Mobile IP**, *Charles Perkins*, IEEE Communications Magazine, May 1997
- **Mobile IP - The Internet Unplugged**, James D. Solomon, Prentice Hall, 1998
- **Supporting Transparent Host Mobility on TCP/IP Internetworks**, *Vipul Gupta*, SUNY Binghamton, 1996

Organization

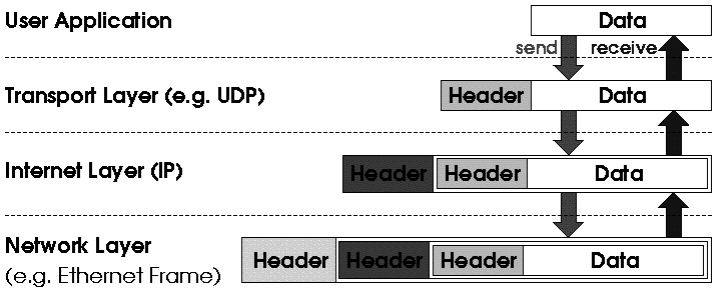
- Background on IP
- Motivation and Problem Description
- Mobile IP Overview for IPv4
- Mobility Support in IPv6 and Current Research

TCP/IP Protocol Architecture



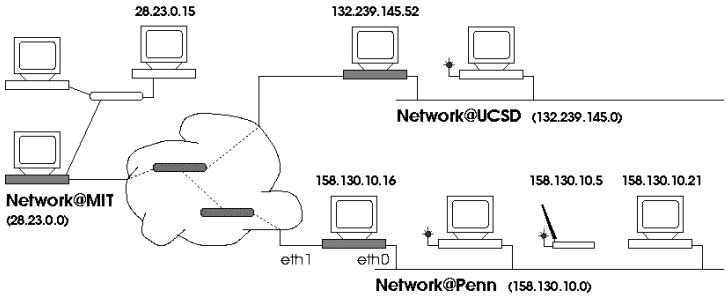
- define rules for exchanging data on the Internet
- layered approach provides a good way to manage complexity

Data Encapsulation



- Each layer
  - is unaware of the packet structure used by its layers above and below
  - is only concerned with the header meant for it
  - has its own header (depending on the type of protocol)

Internet Routing Basics

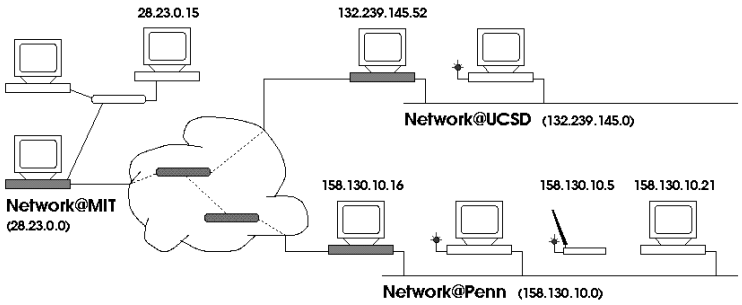


Routing table entries for 158.130.10.16

Destination	Gateway	Mask	Interface
158.130.10.0	158.130.10.16	255.255.255.0	eth0
0.0.0.0	x.y.w.z	0.0.0.0	eth1

- IP Packets are routed based on their Network Prefix (or Subnet Prefix)

Problem Description



- Host identifier (IP address) is topologically meaningful
- Similar situation as with PSTN
  Cannot receive calls for (215) 898-2222 in San Diego, CA

Options

- Retain Host Address => Routing fails
- Change Host Address => Lose established connections

Mobile IP Features

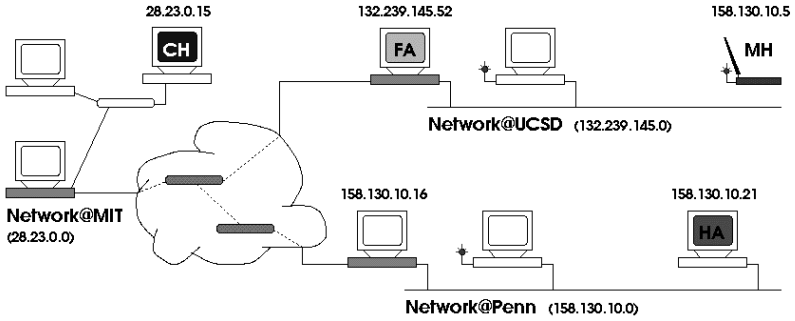
- Allows a host to be reachable at the same address, even as it changes its location
- makes it seem as one network extends over the entire Internet
- continuous connectivity, seamless roaming
  even while network applications are running
- fully transparent to the user

Mobile IP Implementations

various implementations use slightly different approaches

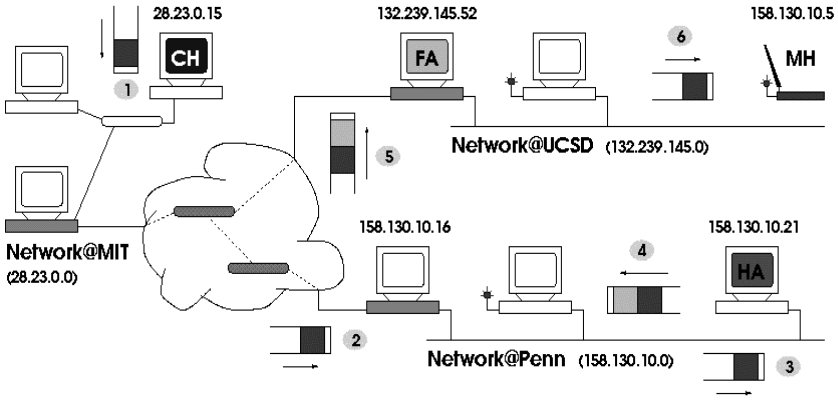
- Columbia ‘91
- Sony ‘91
- IBM ‘92
- Matsushita ‘92
- Harvard ‘94
- SUNY Binghamton ‘96 (Linux Mobile IP)

How Mobile IP works

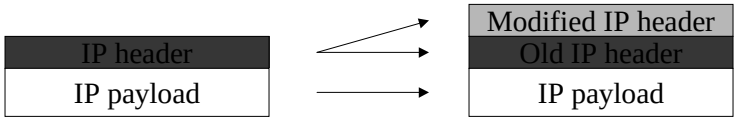


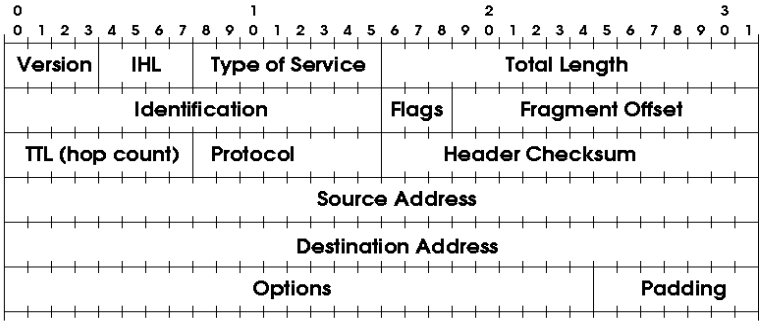
- When the Mobile Host is away from home its Home Agent picks up its IP packets, encapsulates them in a new IP packet and forwards them to the Foreign Agent
- intermediate routers are unaware of the inner IP header

Encapsulation is the Key



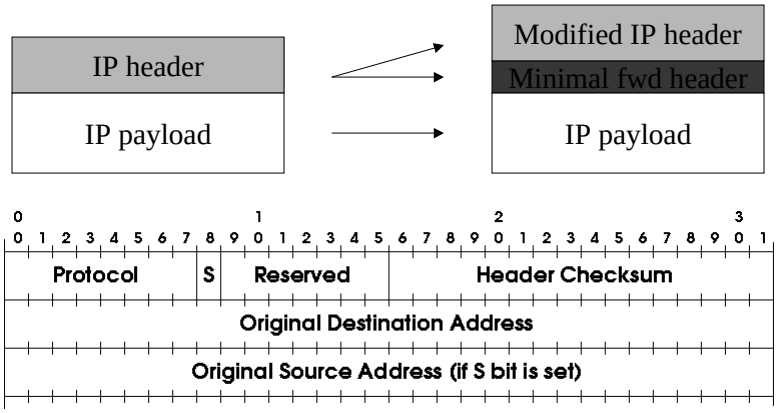
IP within IP Encapsulation





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

Minimal Encapsulation



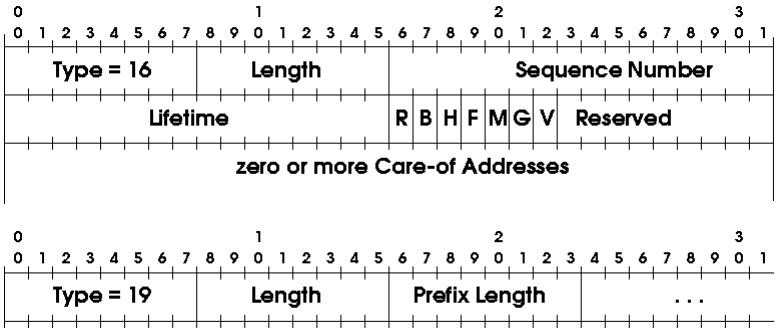
- Modified header …
  - destination Address: "care-of address"
  - source Address: address of encapsulating host (opt.)
  - protocol number: 55
- adds less overhead but needs a **complete** IP packet before encapsulation

Agent Advertisement and Discovery

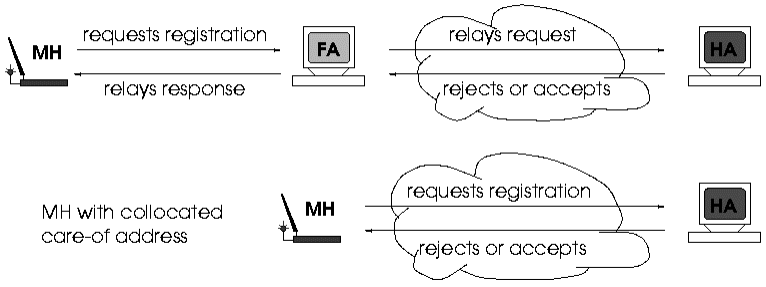
- *Mobility Agents* (HAs and FAs) periodically send out *agent advertisements* as link level broadcasts
- Sent as an extension to router advertisement ICMP messages using TLV encoding
- Advertisement includes care-of address, encapsulation type and lifetime
- Mobile Hosts listen to the routers advertising *mobility agents*
- If MH does not receive agent advertisements
  - send ICMP echo requests to default router (check if we're actually at our home network)
  - obtain care-of address via DHCP

How does a MH determine its Movement?

- Movement detection using *lifetimes*
- Movement detection using *network prefixes*

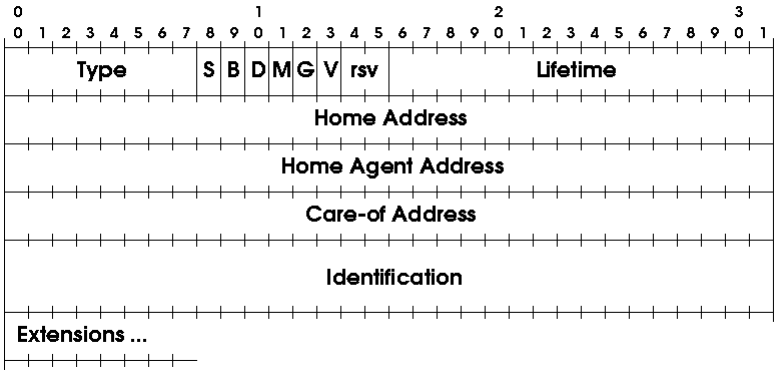


Mobile Host Registration



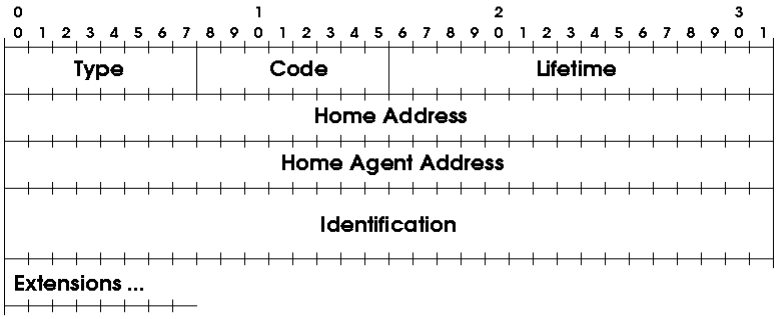
- Registration updates *binding*. A *binding* consists of:
  - mobile hosts address and the care-of address
  - message ID (nonce or timestamp) and a lifetime
- Authentication is needed to prevent misuse (e.g. denial-of-service attacks)

Registration Request



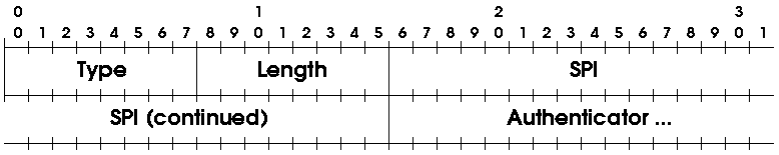
- *Mobile-Host* authentication extension required
- Identification used for replay protection
- Uses UDP messages

Registration Reply



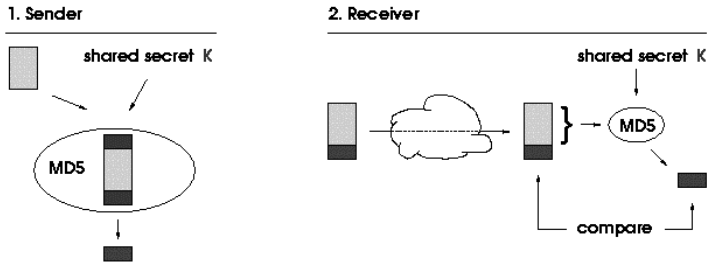
- *Code* field describes status information, e.g. why the registration failed. These include
  - authentication failed
  - ID mismatch (resynchronization needed)
  - unknown HA

Authentication Extension



- *Type* field determines the entities involved in the authentication
  - Mobile-Home
    (required for all registration requests and replies)
  - Mobile-Foreign
  - Foreign-Home
- The *Security Parameter Index (SPI)* identifies the security context

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

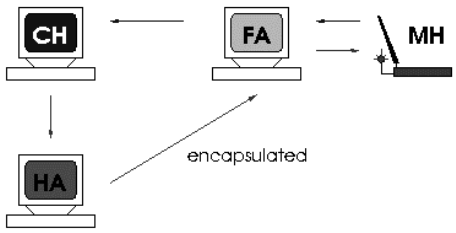
On the Home Network

- 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)

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

Triangle Routing



Triangle routing drawbacks:

- waste of network resources
- Home Agent is a bottleneck

Route Optimization

(work still in progress :-)

- *Idea:* Correspondent Host caches the current mobility binding
- updates have to be authenticated
- IP networking code at CH has to be modified

  => most hosts will not understand the optimization protocol

Creating and maintaining Mobility Bindings

- The HA sends *binding update* messages to the CHs from which it is receiving packets for a Mobile Host which is not at home
- A CH sends a *binding request* message to the HA of a MH if its binding is going stale (it knows the HA from the previous *binding update* message)

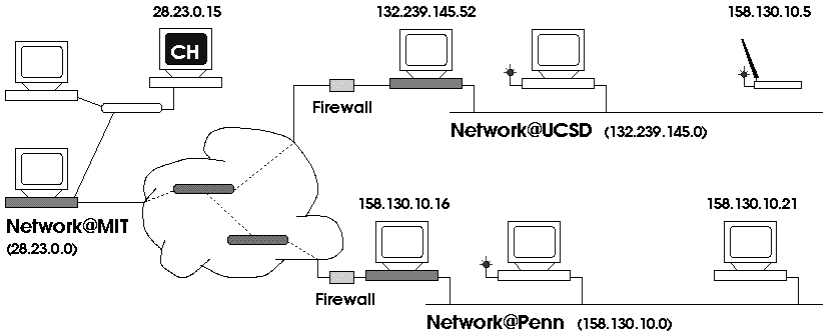
Smooth Handoffs

Problem: The MH leaves its current network and attaches to a network

=> IP packets in transit to the old FA (care-of address) might be dropped

Solution: The MH updates the mobility binding at the previous FA

Problems with Firewalls and packet filtering



- Firewalls may filter packets based on its source IP address and the interface on which it arrives
- Firewall must be made aware of the MH's location

TCP and Mobile IP

- TCP assumes that all packet losses are due to congestion. Upon packet loss detection TCP
  - drastically reduces the transmission rate
  - only recovers slowly
- wireless connections are more error prone than wired connections
- Mobility also causes packet loss (e.g. when a MH switches to another network and routes are temporarily lost)

Throttling the transmission is the the wrong approach

Improving TCP Throughput

- Fast Retransmit *(Caceres and Iftode 94)*
- Connection Segmentation *(Bakre and Badrinath 94)*
- Transmission and Timeout Freezing
  (when connection is temporarily broken)

Mobile IP and IPv6

- There is no need for Foreign Agents since the MH can use the *Address Autoconfiguration* protocol to obtain a dynamic care-of address
- Binding updates are supplied by encoding them as TLV destination options in the IP header
- IPv6 provides security protocols hence simplifying the authentication process

Current Research

- Route Optimization
- TCP improvements
- Location aware applications