Current Outlook for Mobile IP

Charles E. Perkins

Advanced Network Development

Sun Microsystems, Inc.

Palo Alto, CA 94303

cperkins@eng.sun.com

http://www.svrloc.org/~charliep

Outline of Presentation

Mobile IP

Mobile IPv6

Mobile IP and SLP

AAA and Mobile IP

Why Mobile Networking?

Wireless communications technologies are becoming widely available

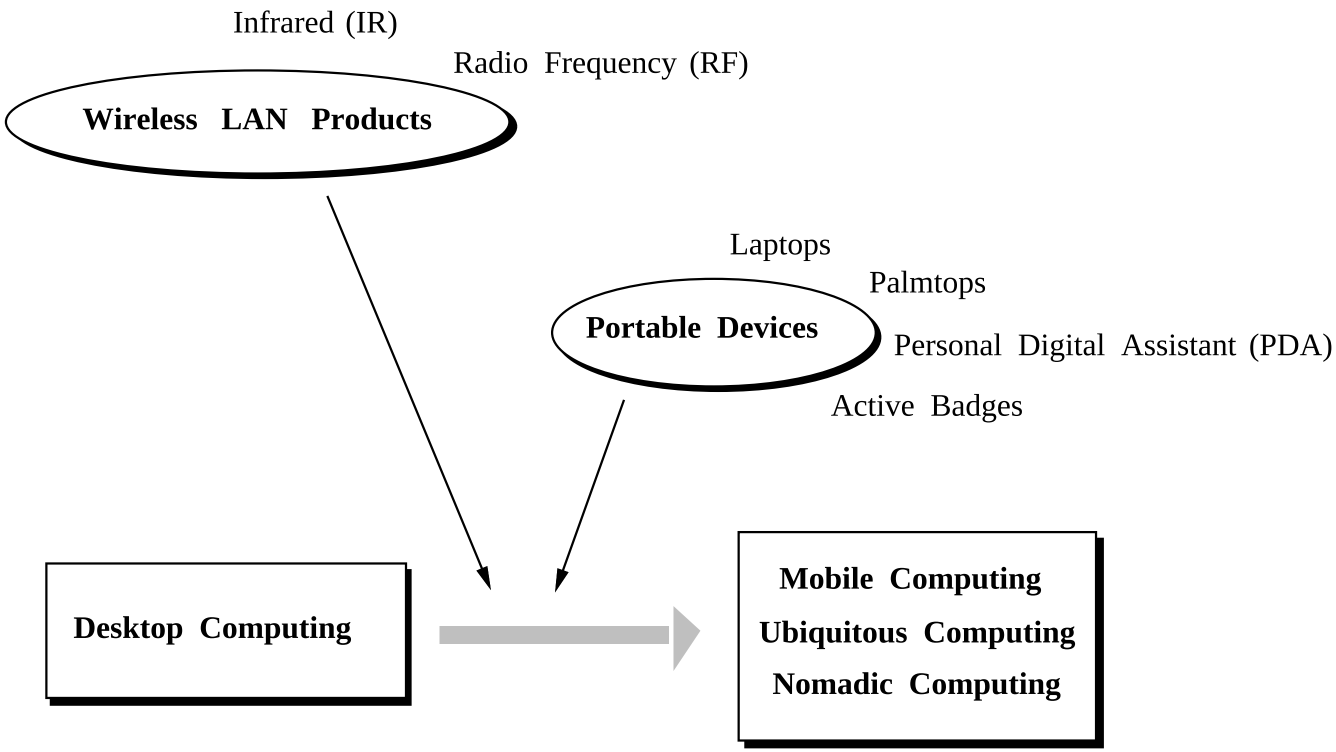
- 10+ Mb/s RF
- 4 Mb/s IRDA and Diffuse Infrared
- IEEE 802.11
- Battery life improved
- Bluetooth (www.bluetooth.com)

Why Mobile Networking? (cont.)

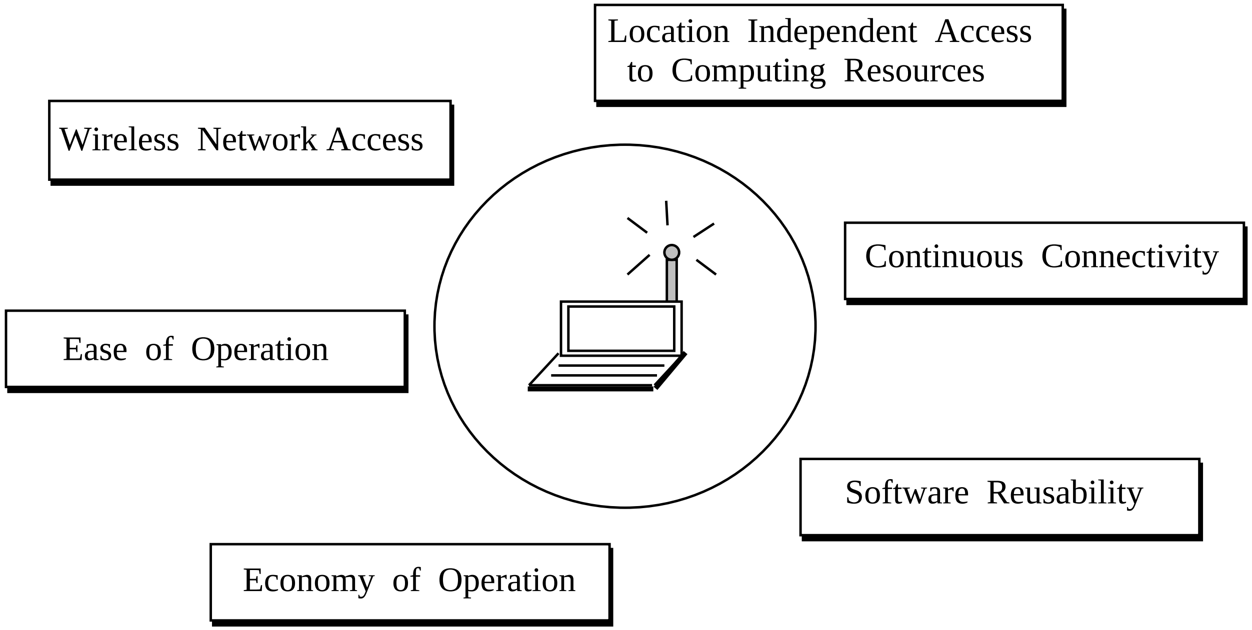
Laptops and even palmtops are sufficiently powerful

- High-resolution laptop color display
- 200 Mhz+ processor
- Hardware accelerators
- 8 gigabyte disk
- With a docking station, the laptop *is* the desktop
- JVM, TCP/IP running on Palm Pilot, plus many games

Technological Advances enabling Mobility



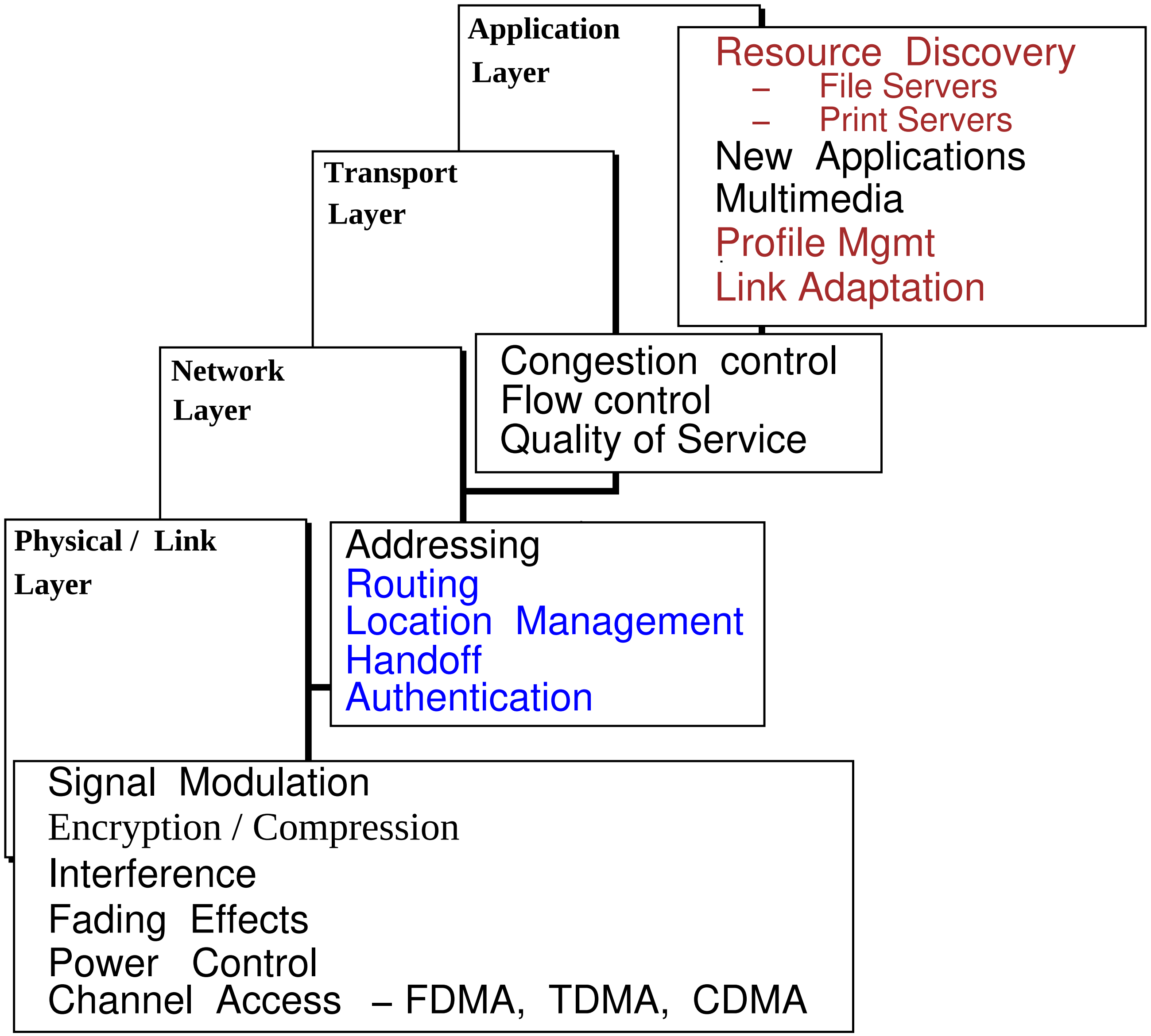
Why Network-Layer mobility (Mobile-IP)?



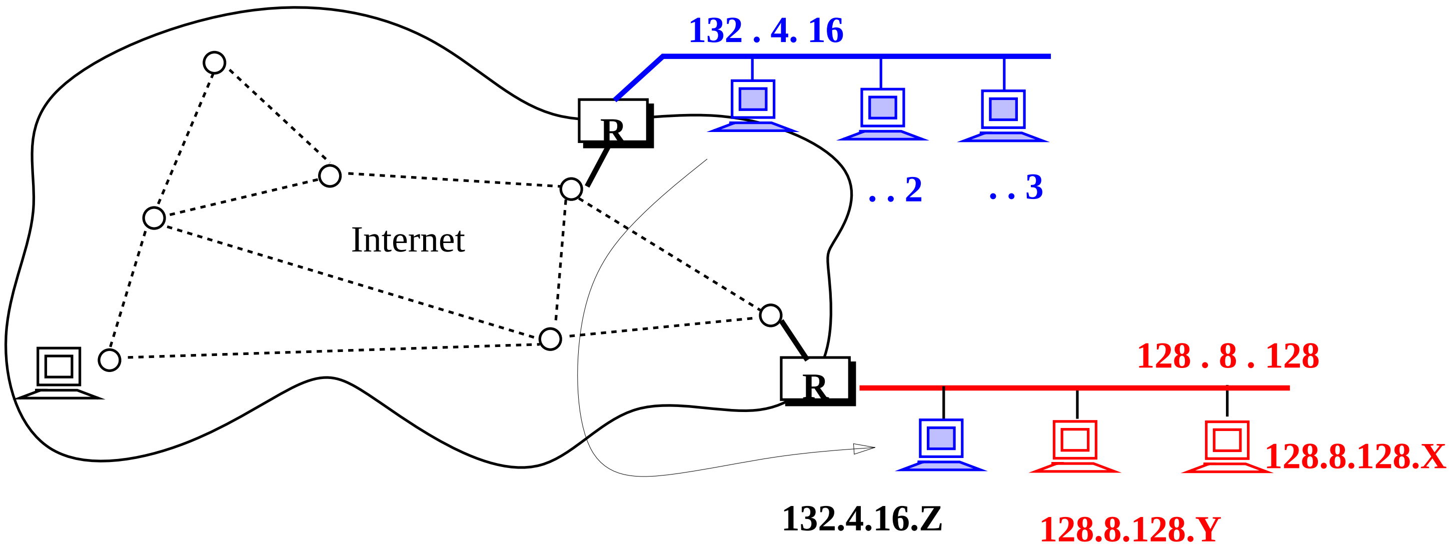
Can even change physical media without breaking connections

Provides *application transparency*, by way of a (possibly virtual) *home network* extending over the entire Internet.

The ***network*** is the "computer"


Application Layer
Resource Discovery
– File Servers
– Print Servers
New Applications
Multimedia
Profile Mgmt
Link Adaptation
Transport Layer
Congestion control
Flow control
Quality of Service
Network Layer
Addressing
Routing
Location Management
Handoff
Authentication
Physical / Link Layer
Signal Modulation
Encryption / Compression
Interference
Fading Effects
Power Control
Channel Access – FDMA, TDMA, CDMA

IP's Routing Model



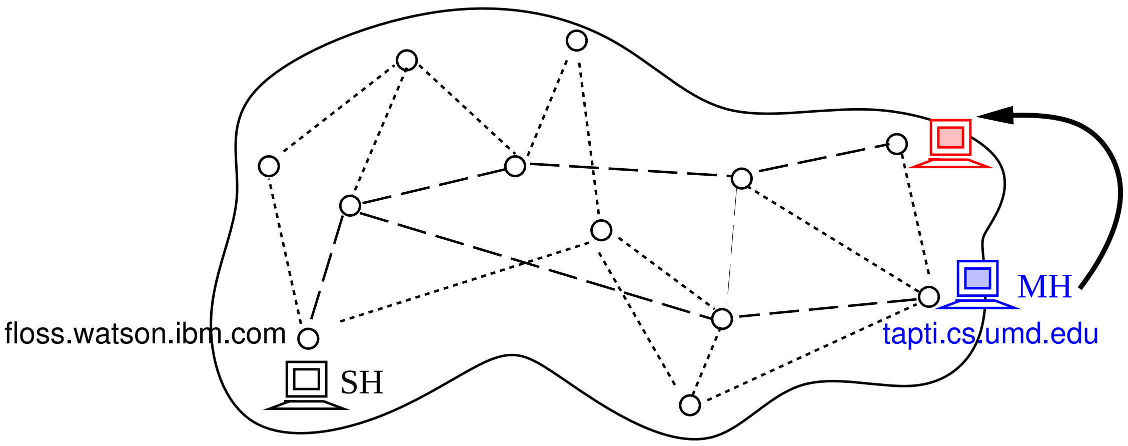
1. Every host has a unique 32-bit IP address.

2. Addresses are assigned in a topologically significant manner.

3. Routing based on address prefixes.

A mobile host must be assigned a new address when it moves

Connections between Internet computers

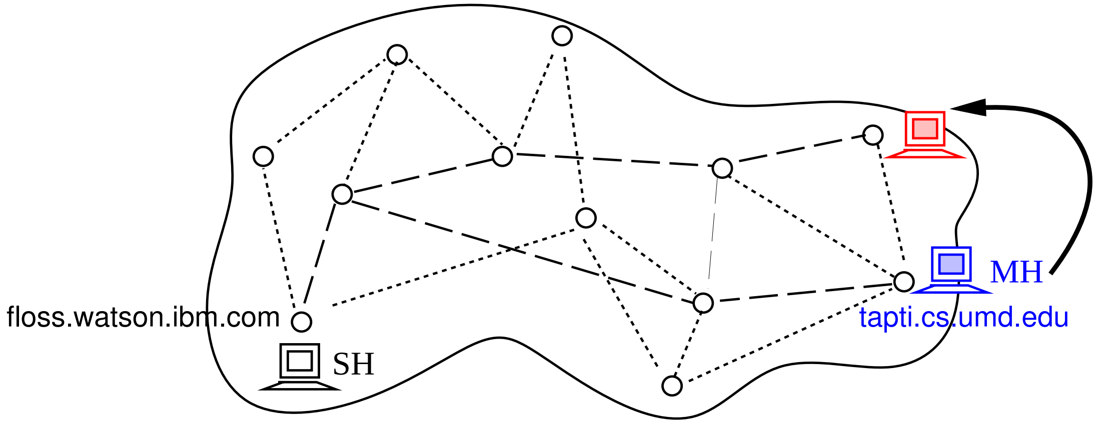


Connection := <129.34.16.43, sh_port #, 128.8.128.45, mh_port #>

TCP connections are defined by source and destination IP addresses and port numbers.

Mobile computers violate the assumption that the IP addresses define the topological relationship of the "connected" computers.

Mobility Problem : The Internet Viewpoint

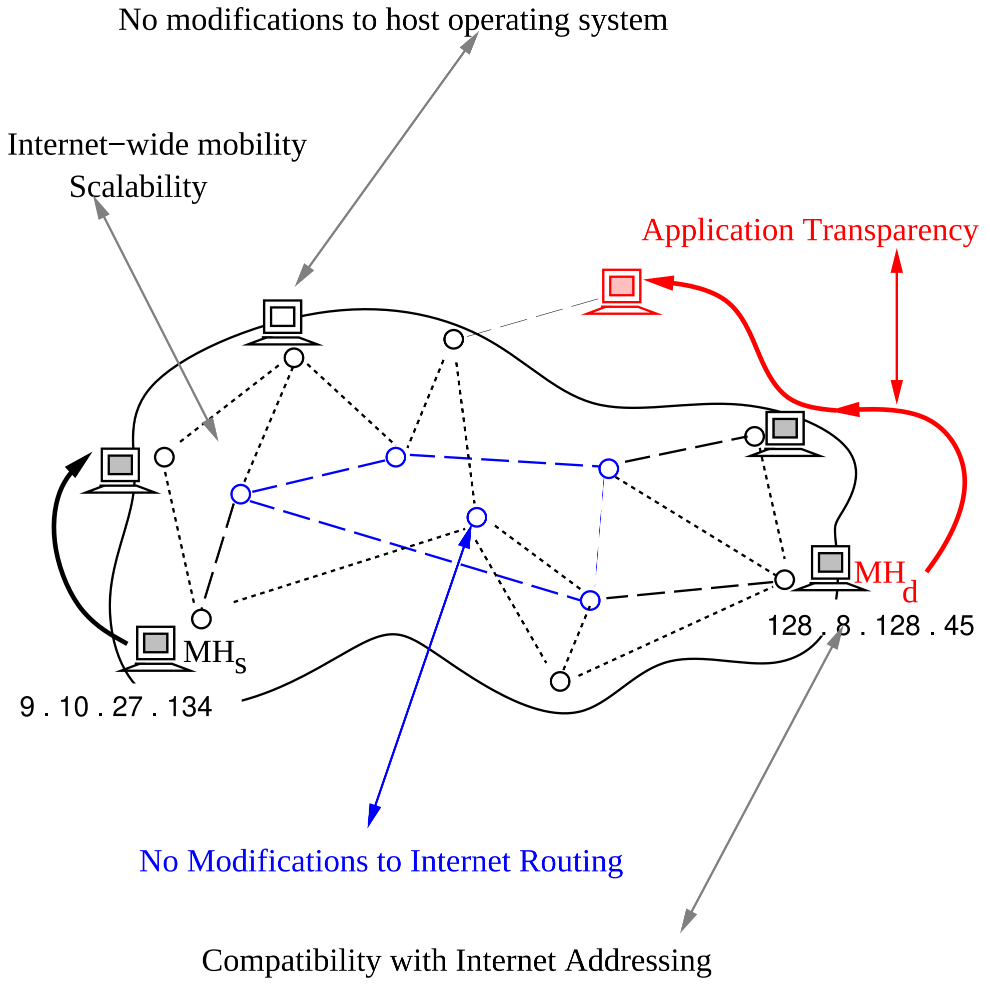


Connection := <129.34.16.43, sh_port #, 128.8.128.45, mh_port #>

- Change host address → Connection breaks
- Retain host address → Routing fails

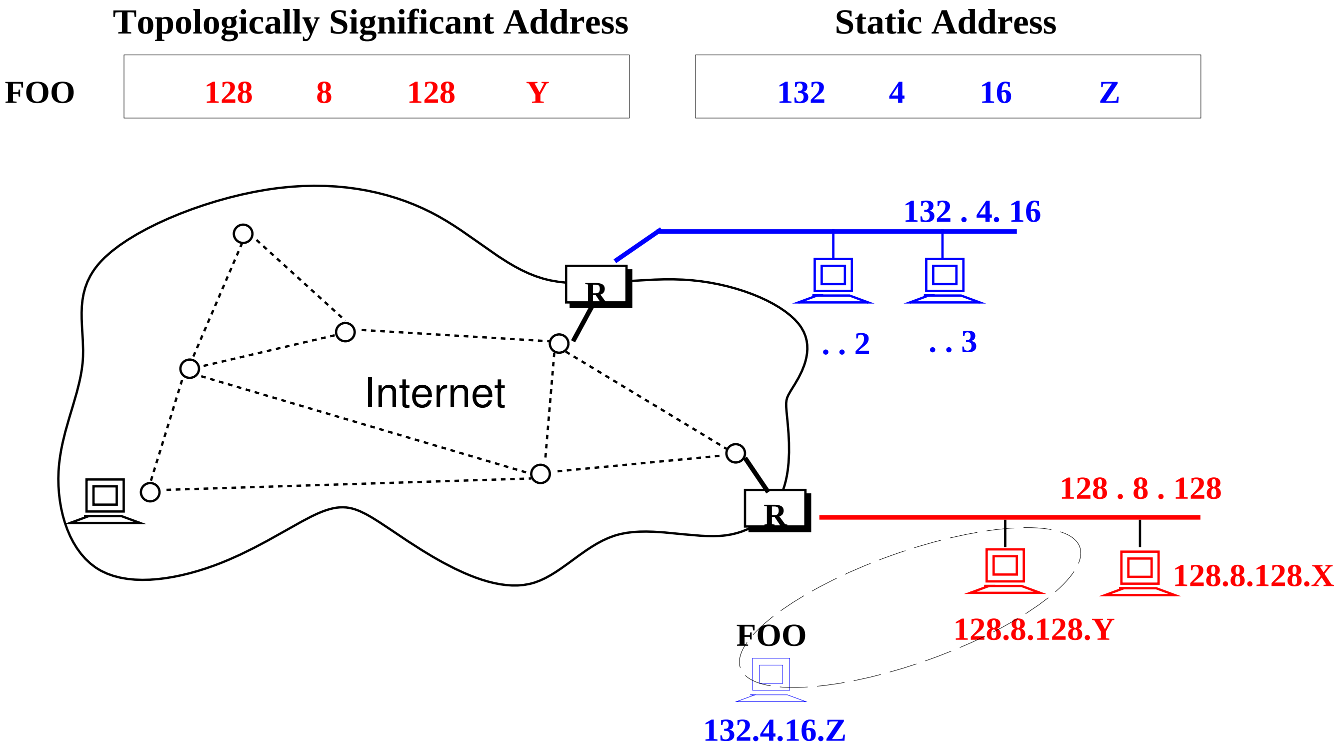
> Host address must be preserved regardless of its location

Characteristics of allowable solutions



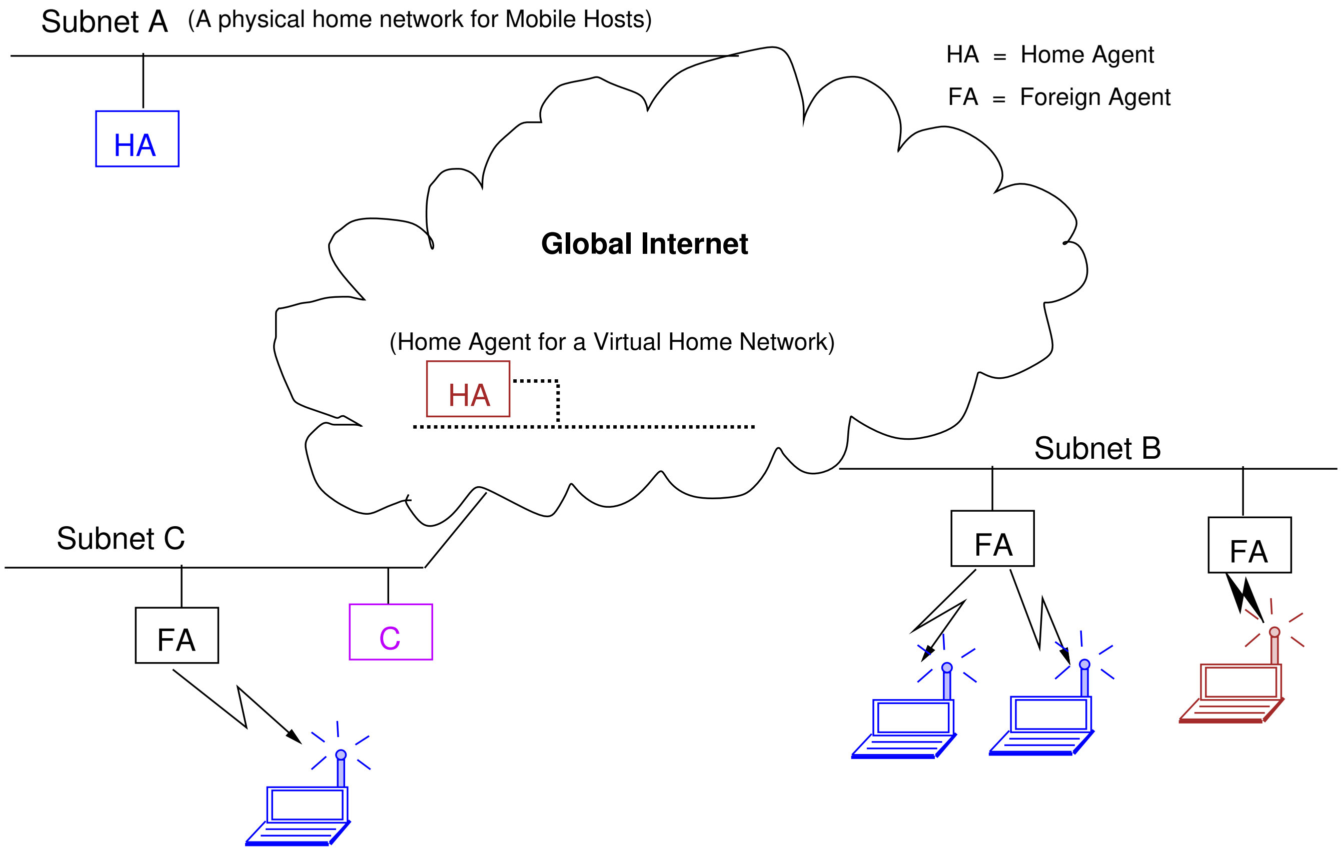
Compatibility (in all respects) with existing Internet computers, applications

Solution: two-tier IP addressing



- The mobile computer keeps its static IP address, but borrows the service of a *care-of address* on whatever IP subnet it happens to be visiting
- A care-of address, if offered by a mobility agent, can be shared by visiting mobiles

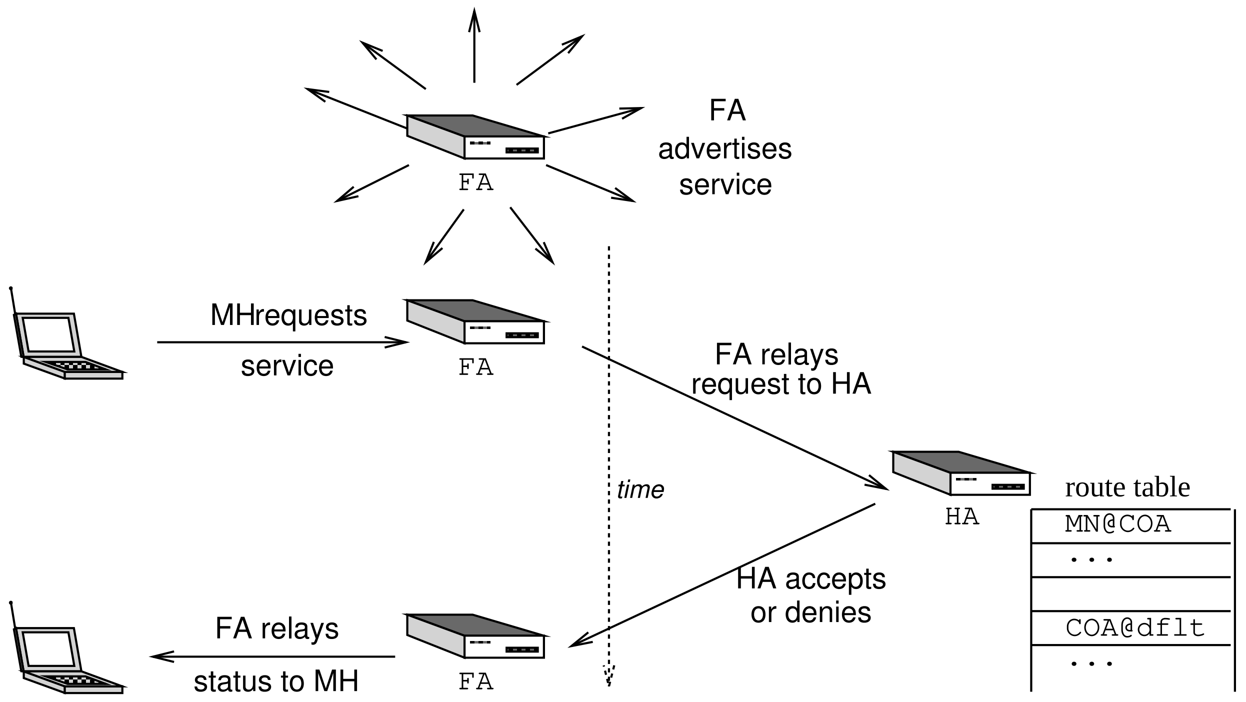
Overall Picture



1. *Service Advertisement*
2. *Registration*
3. *Tunneling*

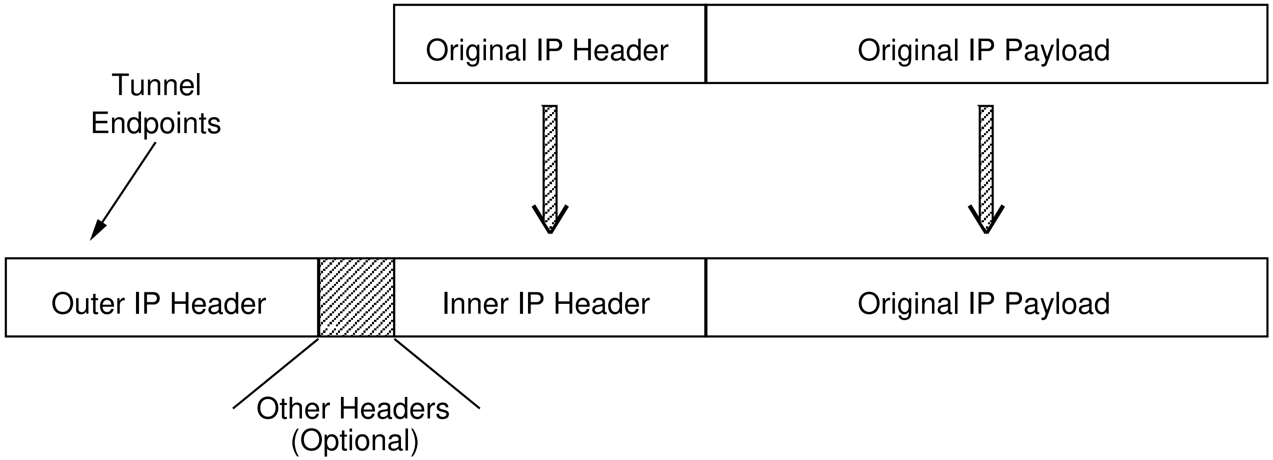
Mobile-IP transforms the mobility problem into a routing problem.

Registration: a four-step process



- A *binding* is the tuple (mobile, care-of address, lifetime)
- Registration means updating the binding
- Registration is a *remote redirect*; authentication required

IP within IP



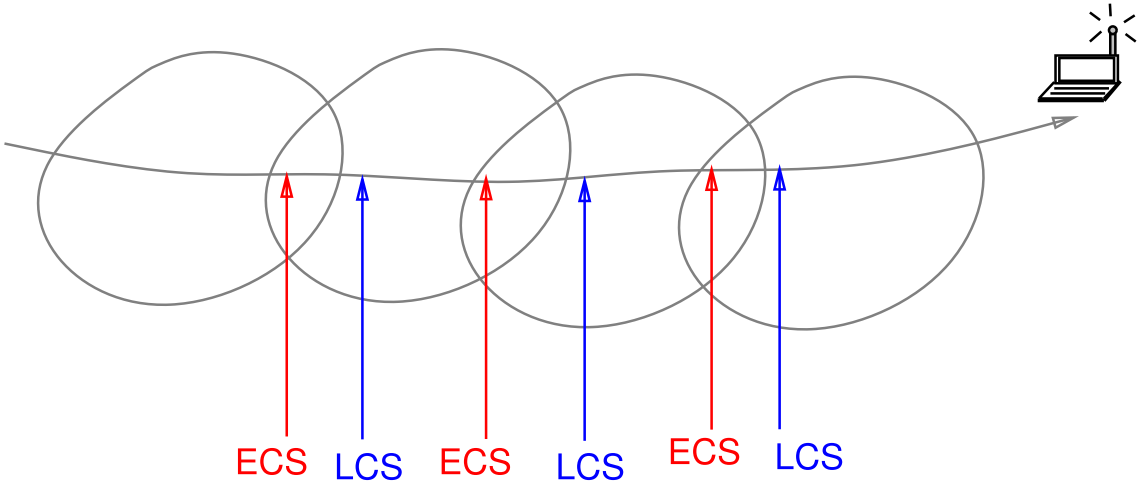
Handles incoming fragmentation

New IP Header uses protocol number 4

ICMP error returns (Datagram Too Big, Time Exceeded, Destination Unreachable) may require *soft state* for correct handling.

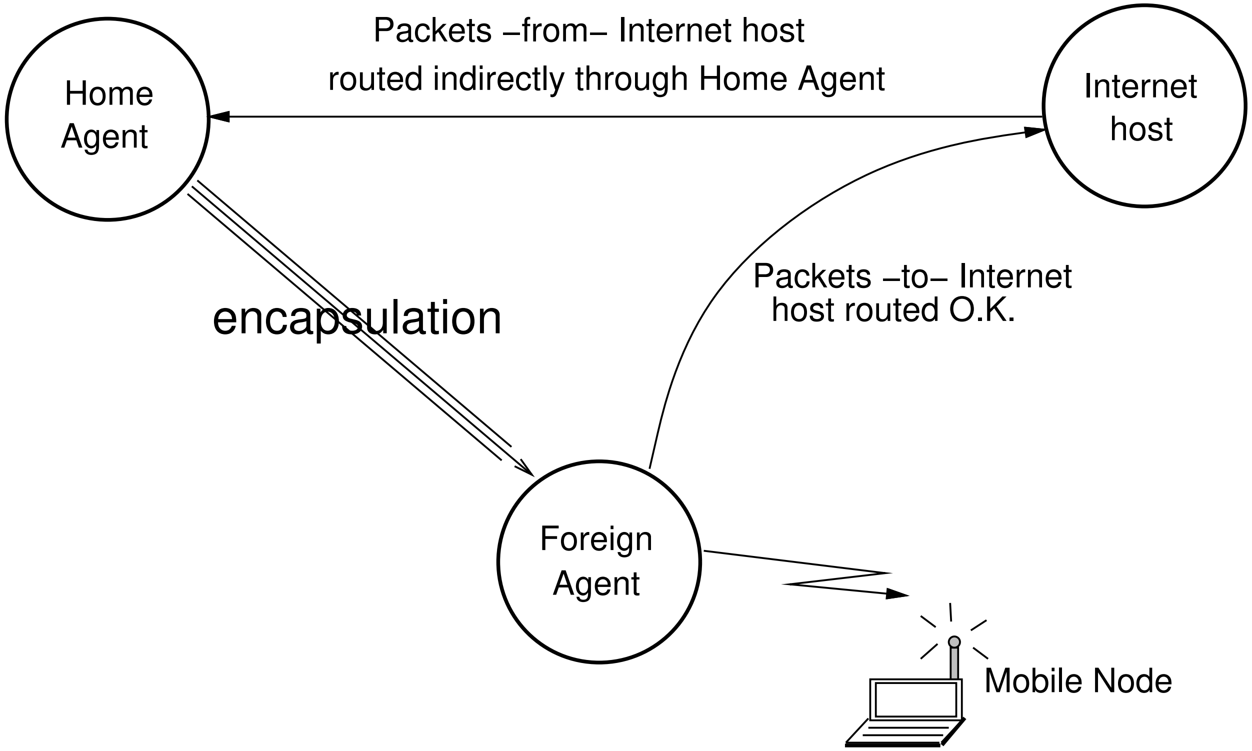
Home agent can maintain tunnel soft state, and return ICMP errors without encapsulating the packet

Algorithms for Motion Detection



- Lazy Cell Switching (LCS) (switch on BLUE)
- Eager Cell Switching (ECS) (switch on RED)
- Prefix Comparison (switch on RED) (requires more subnets)
- Link-Layer notification (can include signal-strength, etc.)
- Performance depends upon pattern of user mobility, frequency of advertisement, and whether mobile node can respond to multiple IP addresses
- LCS w/signal strength measurement can outperform ECS

Triangle (Non-Optimal) Routing



Triangle routing is undesirable:

- Home Agent bottleneck
- Increased network utilization
- Increased sensitivity to network partition

Route Optimization in Four Parts

Current solution requires modified correspondent, and security associations with home agents

Idea: Allow correspondent hosts to know the care-of address of the mobile node – i.e, to get a *binding update*.

Location cache, part of route table

Main ideas:

- Get *bindings* to the correspondent nodes that need them
- Allow *smooth updates* from one foreign agent to another
- Provide *registration keys* for the latter operation
- Define *special tunnels* for additional robustness

IP version 6

Reasons for creation:

- Exponential route table expansion (BUT: CIDR has helped)
- Rapid address space exhaustion

Major points of difference from IPv4:

- 128 bit addresses (denoted in format `XXXX:XXXX:....:XXXX`)
- *flow id* field
- Improved option handling
- Authentication services assumed universal
- Source route reversal not required
- Fragmentation only at endpoints
- No checksum
- Address autoconfiguration
- Some level of multi-homing guaranteed

Mobility for IP version 6

- Mobile nodes create their Care-of Address using link-local address and automatic (*stateless* or *stateful*) address configuration.
- Mobile Node may notify its correspondents when it moves (no *triangle routing*!)
- Correspondents put care-of address in routing headers
- Home Agent encapsulates packets if it gets them (e.g., from correspondents having no current care-of address)
- Binding updates are carried in a Destination Option
- Acknowledgments (usually only sent by a home agent) in another Destination Option, with status codes
- Mobile nodes should be able to receive packets at multiple addresses

Sending Binding Updates

Each mobile node maintains a *Binding Update* list:

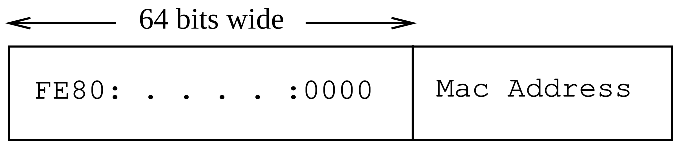
- All nodes to which it has sent a Binding Update, for which the lifetime has not expired

The mobile node sends a Binding Update to nodes on its list when it acquires a new care-of address:

- Can be included in any existing packet (eg: TCP ack)
- Or, in a packet by itself

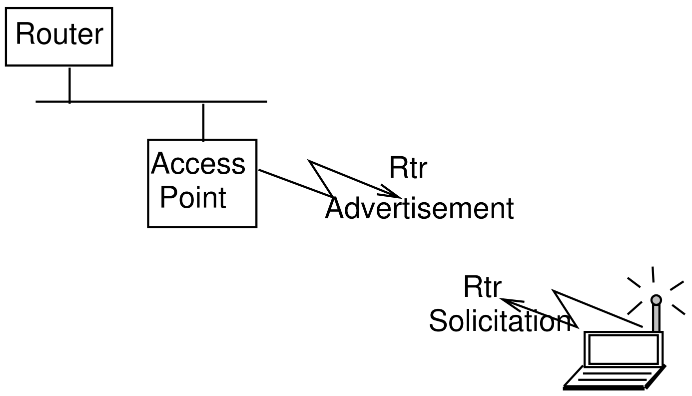
All packets with a Binding Update must also include an IPv6 *Authentication Header*

Establishing the Link – Stateless Address Autoconfiguration (RFC1971)



- Provides means for creating a *unique* link-local address
- Specifies algorithms for *Duplicate Address Detection*(DAD),
- Stateless and idempotent

Router and Neighbor Discovery (RFC1970)



These processes (and Mobile IP) only expect appropriate broadcast behavior on link.

- Provides means for creating a unique globally routable address
- Defines router advertisements, host advertisements, solicitations
- Replaces and improves upon ARP
- Proxy advertisement specified
- 'M' bit allows for stateful autoconfiguration (i.e., DHCPv6)

IP version 6 mobility - Conclusion

Support for mobility is *far* simpler

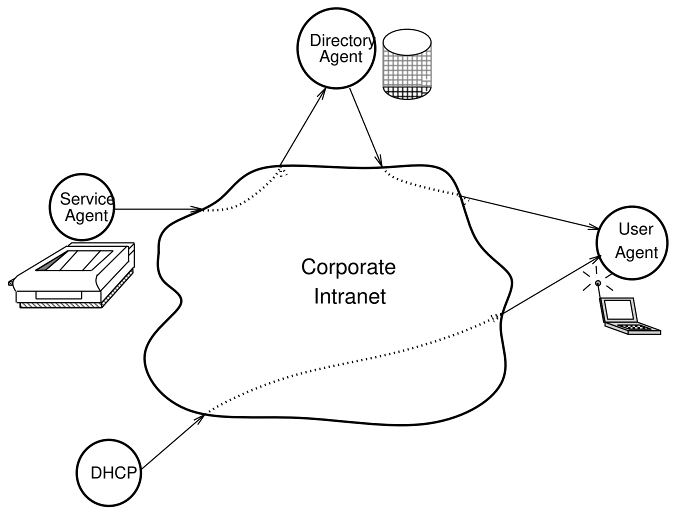
- Address autoconfiguration for care-of addresses eliminates need for foreign agents
- Neighbor Discovery works well for maintaining even wireless links
- Mobile Node issues binding updates to correspondents and home agent
- Using *destination option* distributes bindings with small overhead
- IPv6 routers handle Destination options and Routing headers much faster than possible with IPv4 options
- Universal security deployment avoids problems with *remote redirects*

IPv6 isn't yet fully deployed, so all correspondent nodes should be able to support mobility

Introduction to Service Location Protocol (SLP)

SLP allows:

- Clients to find Servers by *type* and desired *attributes*
- Services to advertise themselves
- *Scopes* to organize services, using arbitrary policies
- Hierarchy of services not artificially imposed
- Support for internationalization



Introduction to SLP (cont.)

SLP is:

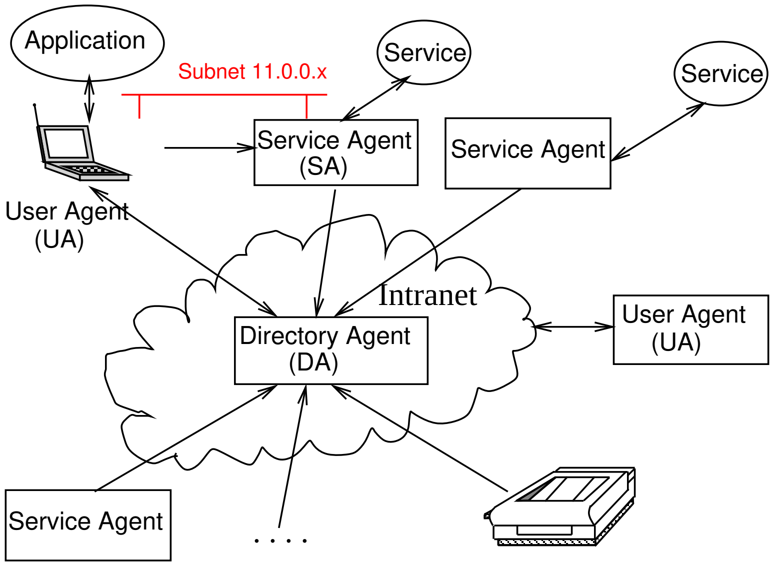
- Low-cost administration and effortless extension to new services
- Decentralized and (after creation) self-administered availability
- Compatible with browser, existing applications, and services (URLs)
- featherweight
- Replacement/supplement for proprietary protocols such as:
  - ⋆ Appletalk NBP
  - ⋆ NetWare SAP
  - ⋆ Microsoft CIFS browsing protocol

Protocol Characteristics

- distributed and self-managing, with numerous service agents
- compatible with other administrative protocols and mobile networking protocols
- string-based (reduced parser complexity)
- easily implemented
- uses existing standards where possible
- expressive query grammar – LDAPv3 query syntax
- *Scalability* a prime motivation, given future explosion of network services and the crowded nature of of enterprise networks

Service Location Discovery Framework

- User Agents (UAs) intercede for applications
- Service Agents (SAs) intercede for services
- UAs and SAs on *nearby* networks can communicate
- Larger deployments use Directory Agents (DAs) (transparent)



Finding Directory Agents

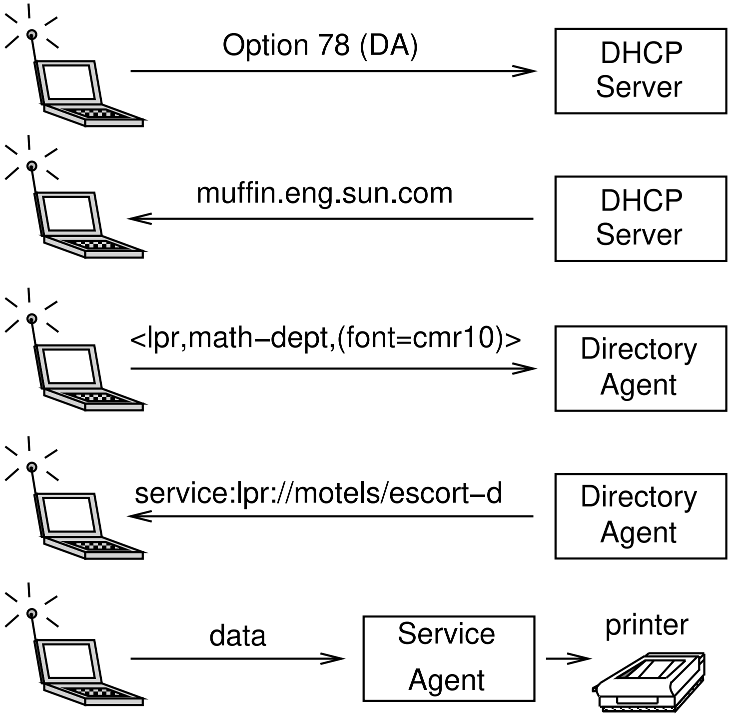
There are four ways to find Directory Agents:

- Listening for Directory Agent Advertisements
- Multicast/broadcast Service Request for small/moderately-sized installations
- Request option 78 from DHCP
- Manual configuration

Note that even the last choice is ***much*** better than having to configure each service manually time and again.

Option 78 going through working group Last Call, responding to DHCP group comments

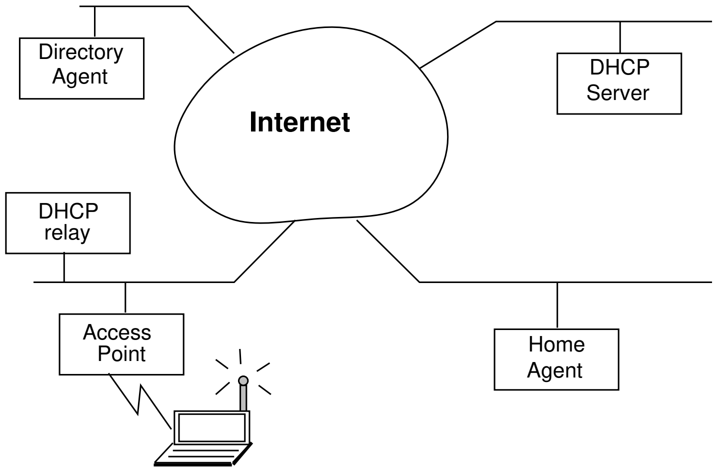
Discovering a Print Service



- Query *DHCP* for IP address of a Directory Agent
- get back `muffin.eng.sun.com`
- contact `muffin` for URL of printer
- receive unicast Service Reply `service:lpr://motels/queuename`
- send print jobs to IP address of printer service agent, `motels`

Mobile Networking and Service Location

- The growth of wireless communications is driving mobile networking
- Mobility is driving the need for automatic resource discovery
- Need to access local resources without preconfiguration
- Mobile users should not have to become system administrators
- While DHCP is useful, it is in no way required for use of SLP either in general or for mobile computers



Operating Service Location with Mobile-IP

- Mobile discovers that a cell switch is needed
- Mobile queries DHCP for a *Care-of Address*, and includes the Directory Agent (DA) option 78
- Mobile registers new Care-of Address with home agent
- Mobile queries Directory Agent for local resources

Issues with Mobile IP and DHCP

- Often, the mobile node should use the *care-of address*, instead of its *home address*
- Mobile SAs have to worry about multicast tree maintenance vs. performance of tunnels to home network
- Some DHCP servers only handle optional requests at boot time

SLP Today

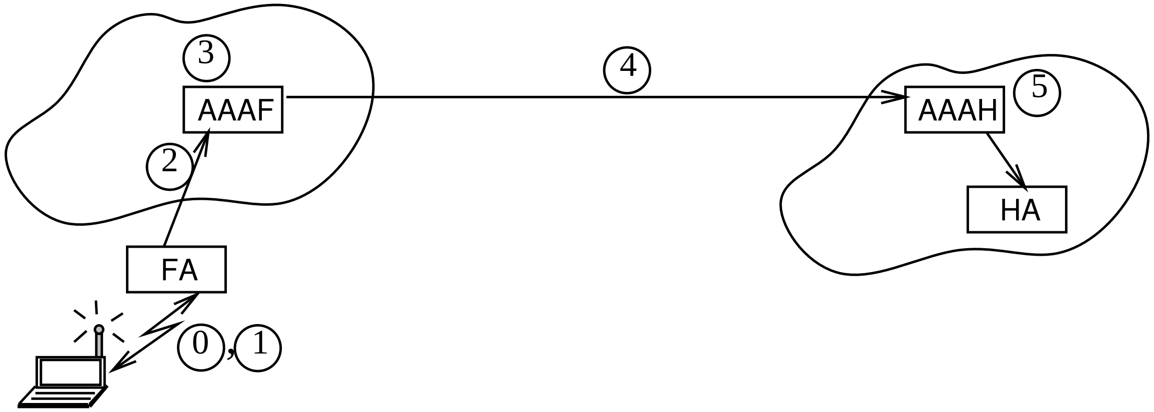
- Locating services and resources is a big problem area for mobile computing
- Service Location Protocol is here now, and can become immediately useful.
- SLP is a natural, standardized scheme (RFC 2165) for finding services
- Using browser technology is appropriate and synergistic for Service Location
- Implementation and deployment can be very simple or much more sophisticated

AAA - Authentication, Authorization, and Accounting

DIAMETER (a follow-on to RADIUS) is used by Mobile IP agents to handle

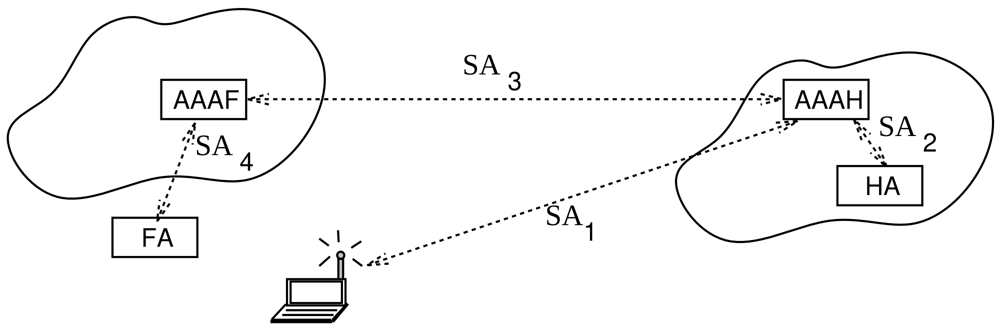
- Mobile Nodes authenticated by trusted agents in their home domain
- Connectivity authorized by administrative agents in the foreign domain
- Accounting initiated by foreign agents, which are trusted by the administrative agents in the foreign domain

Protocol Overview



0. Foreign agent (FA) advertises challenge
1. Mobile node (MN) adds NAI, Challenge Response etc., to Mobile IP registration request
2. FA sends DIAMETER AVPs with registration request to Foreign AAA (AAAF)
3. AAAF ("proxy") looks up NAI, finds MN's home server address (AAAH)
4. AAAF sends DIAMETER request, awaits approval by AAAH
5. AAAH authenticates request; it *may* allocate a HA and IP address for MN

Step 6: Key Generation



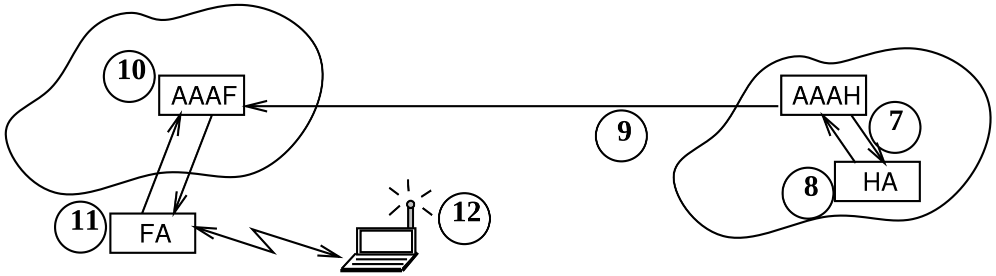
AAAH generates:

- K_1: MN $\leftrightarrow$ FA
- K_2: MN $\leftrightarrow$ HA
- K_3: FA $\leftrightarrow$ HA

AAAH encrypts:

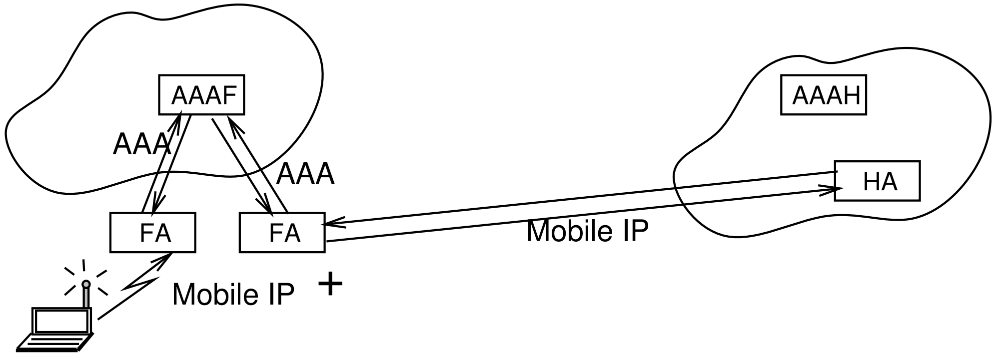
- K_1 & K_2 using $SA_1 \rightarrow$ MN
- K_1 & K_3 using $SA_3 \rightarrow$ FA
- K_2 & K_3 using $SA_2 \rightarrow$ HA

Protocol Overview, continued



7. AAAH issues DIAMETER request to HA with K_2, K_3
8. HA creates registration reply using K_2, and K_3 for FA.
9. HA sends results to AAAH, which proxies request to AAAF
10. AAAF decrypts K_1 & K_3 using SA_3, re-encrypts using SA_4
11. FA decrypts K_1 & K_3 using SA_4, checks registration reply and FA↔HA authentication, adds MN↔FA using K_1
12. MN decrypts K_1 & K_2 using SA_1, checks registration reply, and MN↔FA authentication

Local Handoff



FA advertises NAI as well as challenge

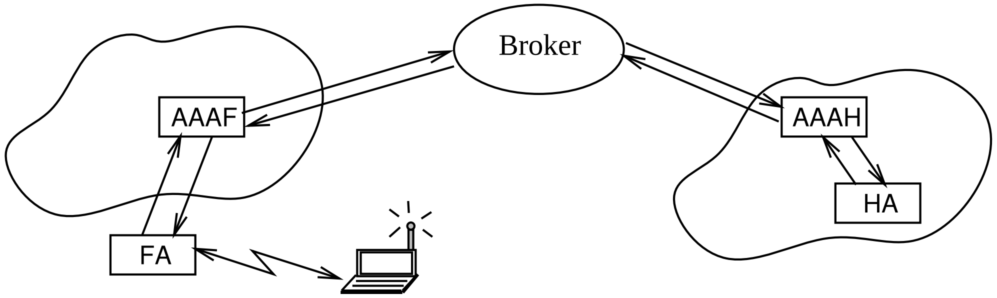
Mobile Node checks whether new NAI is in same domain as old NAI

Mobile Node supplies previous FA as well as unforgeable response

FA sends request to AAAF

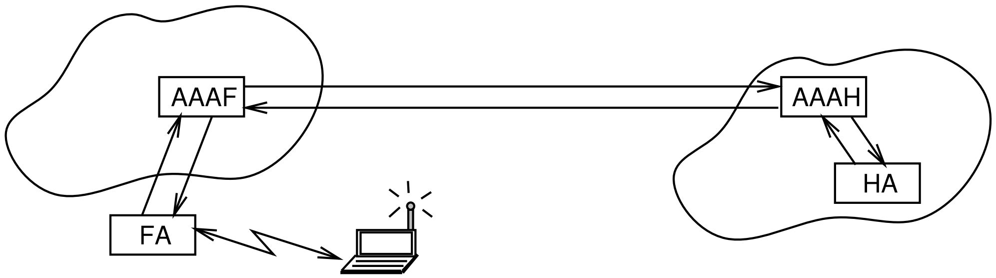
AAAF *may* re-encrypt previous registration key and send it to new FA, without contacting AAAH

Using Brokers



It is possible to use a broker, if the AAAF and AAAH do not already share a security association SA_3

AAAF↔AAAH Accounting



- After successful registration reply, FA sends Accounting Start Record to AAAF
- AAAF proxies Start Record to AAAH.
- Foreign Agent MAY send interim Accounting Records (perhaps every 5 minutes) containing cumulative information.
- Foreign Agent sends Accounting Stop Record upon receipt of notification from new FA.

Features

Generates session keys for Mobile Node and Mobility Agents

Eliminates unnecessary Internet traversals

Challenge/Response integrated with Registration Request

Centralizes AAA functions in administrated services

Broker certification (e.g., IPASS, GRIC), to eliminate need for so many bilateral service agreements (see DIAMETER Proxy draft)

How does Mobile IP compare?

- Seamless Roaming
- Internet Standard connectivity
- PPP Dialin compatibility (RFC 2290)
- DHCP compatibility, without need for dynamic DNS
- Route Optimization
- Low-cost implementation
- Can provide other services for nomadic applications

IETF status

- Mobile-IP interoperability testing has been quite successful
- Base document, two encapsulation drafts, and MIB are RFCs 2002-2006.
- Draft Standard status possible within a year.
- IPv6 mobility meandering through last call
- Route Optimization updated using feedback from IPv6 mobility.
- RFC 2267 for Reverse Tunneling
- RFC 2290 for PPP configuration option
- RFC 2356 for Firewall Traversal using SKIP
- `manet` working group for *ad hoc* networking,
- `roamops` working group for *roaming*
- `svrloc` working group for *Service Location*
- Service Location has gone to Proposed Standard.

Freeware

- http://www.monarch.cs.cmu.edu/ (Dave Johnson)
- http://www.cs.pdx.edu/research/SMN (Portland State)
- http://mip.ee.nus.sg (University of Singapore)
- http://www.mcl.cs.columbia.edu/source.html (JI's Mach code)
- ftp://ftp.it.kth.se/pub/klemets/klemets.tar.gz ("MINT")
- http://anchor.cs.binghamton.edu/ mobileip/ (Linux MH and "agent")
- http://mosquitonet.stanford.edu/software/mip.html (MosquitoNet)
- http://mip-nt.aii.pub.ro (NT freeware)
- http://www.cs-ipv6.lancs.ac.uk/MobileIP (Linux Mobile IPv6)
- ftp://playground.sun.com/pub/mobile-ip/ (Linux/Solaris)

Mailing Lists

Check out www.ietf.org for more information

mobile-ip join:	`mobile-ip-request@SmallWorks.com`
mobile-ip contribute:	`mobile-ip@SmallWorks.com`
IPng join:	`ipng@sunroof.eng.sun.com`
IPng contribute:	`majordomo@sunroof.eng.sun.com`
	in body: `subscribe ipng`
srvloc join:	`srvloc-request@srvloc.org`
srvloc contribute:	`srvloc@srvloc.org`
AAA join:	`ietf-aaa-request@external.cisco.com`
AAA contribute:	`ietf-aaa@external.cisco.com`