Towards an Internet Mobility Management Architecture

MobiArch Workshop
James Kempf
kempf@docomolabs-usa.com
December 1, 2006
Outline

- The Architectural Problem of IP Mobility
- A Sample of Existing Mobility Management Solutions
- NETLMM (NETwork based, Localized Mobility Management)
- Summary and Conclusions
The Architectural Problem of IP Mobility
What is an IP Address?

- An endpoint identifier, uniquely identifying a communication endpoint, particularly to the Transport Layer
- A topological locator, indicating where in the network topology a device interface is located
- A forwarding identifier, allowing routing intermediaries to forward packets to a device interface
- In practice, only first and third are causally active, second is a derivative of third
Why is Mobility an Architectural Problem?

- For mobile hosts, the attachment point to the Internet changes over time
- Mobile host movement splits the functions of an address
  - Forwarding identifier changes since the attachment point changes
  - Endpoint identifier remains the same since the mobile host is the same
  ➔ To maintain session continuity, forwarding must somehow track the topological change without changing the endpoint identifier
- Up until now, most applications have been nomadic and haven’t needed session continuity
  - User sits down, opens a laptop, works for a while, closes the laptop moves to a new location...
    - Laptop gets a new IP address using DHCP each time the user moves
  - VoIP, other new services now require session continuity when the user moves between different locations
  - Truly mobile applications require mobility management
Example

The Internet

endpoint identifier = forwarding identifier!

endpoint identifier ≠ forwarding identifier!
Why Isn’t Mobility Management More Widely Deployed?

- IP mobility solutions have been around for a long time
  - Mobile IP has been available for 10 years
  - Only available in a couple link layer specific cellular deployments,
- Most usage has been nomadic
  - User sits down, opens laptop, works, closes laptop and moves
  - Nomadic usage pattern doesn’t need session continuity
  - DHCP address configuration is sufficient
- Session based applications with longer session times need session continuity
  - Web browsing can be broken off and restarted after handover
  - VoIP session must survive a handover while the session is in progress
A Sample of Existing Mobility Management Solutions
Current Internet Architecture: Approaches to a Solution

- Split the identity and location function of the IP address
  - Use one IP address for identity, another for location
    - Mobile IP
- IP address is for location only
  - Create a separate identity name space
    - Host Identity Protocol (HIP)
- Change routing so that identity and location function remain equal on move
  - Overlay routing in the local topology
  - Proprietary solutions
    - GPRS
Mobile IP Basics

- **Internet Standards**
  - Mobile IPv4 – RFC 3344
  - Mobile IPv6 – RFC 3775
  - Widely deployed in cdma2000 cellular network (North America, Korea, some in China and Japan)

- **Basic Architectural Idea: split address functions**
  - **Forwarding identifier**
    - Care of address - address on the local subnet
    - Changes as the mobile host moves from subnet to subnet
  - **End node identifier**
    - Home address – address on a server (the home agent) in the home network
    - Bound to the mobile host’s Fully Qualified Domain Name (FQDN – DNS host name) and does not change
    - Identifies session endpoint to the Transport Layer

- **Global Rerouting Overlay**
  - Correspondent hosts send packets to the home address
  - Home agent reroutes the packets to the care of address using a tunneling overlay
  - Mobile host sends routing updates to the home agent when the care of address changes
    - Security handled by AAA between the mobile node, first hop router, and home agent for Mobile IPv4
    - Security handled by IPsec between home agent and mobile node for Mobile IPv6
Mobile IP Architecture
Problem: Two Japanese in America

- Long dogleg routes back to home agent in Japan
  - Could introduce substantial latency into VoIP
- Optimize routes by getting rid of overlay
  - Route optimization introduced into Mobile IPv6
- Mobile host signals directly to correspondent on movement
  - Sends new care-of address
  - Security complex: how can correspondent know that sender is authorized to change the IP address?
    - IPsec would require global authentication infrastructure
    - Return routability: new security protocol based on presumed security of routing infrastructure
- Correspondent switches to new address below transport layer
  - Home address still used as endpoint identifier
- Requires changes in all IPv6 stacks
  - Fixed servers (e.g. CNN.com) must do this too
Problem: Packet Delivery Latency

- Configuration of on a new subnet requires approximately 18 messages at the IP level depending on the address configuration mechanism used
  - IP level movement detection
  - Multicast listener discovery
  - Address configuration
    - Duplicate address configuration (DAD) if stateless
    - DHCP if stateful
  - Router address resolution
  - Binding update with the home agent
  - Return routability with the correspondent node for route optimization security
  - Binding update with the correspondent node for route optimization
- Depending on RTT this can considerably lengthen time before packets begin arriving at the new care of address
  - Packets delivered to the old care of address are dropped after the mobile node moves
- Some solutions to this problem (Fast Mobile IP, Optimistic DAD) but they require additional signaling and additional host to network security
  ➨ Performing Mobile IP handover on every link handover requires too much signaling overhead and may introduce too much packet delivery latency for some applications
HIP Basics

- Experimental
  - Architecture: RFC 4423
  - Protocol: draft-ietf-hip-base-05.txt (not yet published)
  - Experimental deployments, but not widely deployed commercially

- Basic Architectural Idea: Create a new host identifier name space
  - Contacting host establishes an IPsec ESP tunnel with correspondent
    - Special kind of tunnel - bound, end to end tunnel
    - Establishes security between two endpoints
  - Host Identifier Tag (HIT) constructed as hash of public key
  - Traffic packets have ESP authentication and encryption

- HIT Layer
  - Between Transport Layer and Network Layer
  - Maps HIT to/from current IP address
  - Transport Layer identifies connection endpoints using HIT

- When current IP address changes
  - Host signals correspondent with change using HIT to identify itself
  - IPsec ESP authentication ensures host has the right to claim the HIT
HIP Stack

<table>
<thead>
<tr>
<th>Application (e.g. HTTP, RTP, etc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport (e.g. TCP, UDP, etc)</td>
</tr>
<tr>
<td>HIP</td>
</tr>
<tr>
<td>IP</td>
</tr>
<tr>
<td>IPsec</td>
</tr>
<tr>
<td>L1/L2</td>
</tr>
</tbody>
</table>
HIP Architecture

Internet

Routing Update

Corresponding Host

Care of Address: CoA1

CoA2

CoA1
Problem: What if Correspondent is Also Mobile?

• If both move at the same time, signaling could get lost
  – More precisely, both move within RTT
  – Session fails

• Introduce a network functional elements to anchor mobility
  – Rendezvous server

• Rendezvous server acts as a fast name server
  – Dynamic DNS is too slow – 15 sec for change
  – Mobile host updates route to new address at the rendezvous server first
  – If correspondent loses the session, use rendezvous server to find new address

• Rendezvous server acts as a mobility anchor
  – Reroutes first HIP signaling packets through an overlay
  – No different from Mobile IP with route optimization

➡ HIP loses end to end character and much of its attraction over Mobile IP
GPRS Basics

- Proprietary protocol for cellular systems utilizing GSM signaling
  - Legacy circuit-switched signaling using SS7/MAP protocol
  - Extensive, world wide deployment on two cellular wireless technologies
    - GSM
    - WCDMA

- Basic architectural idea: keep the IP address the same when the host moves
  - Locator and endpoint identifier functions are not split
  - Locator function is updated by the network on movement to match current location

- Local Rerouting Overlay
  - A mobility anchor (GGSN) maintains host routes to/from mobile host’s current subnet
  - GGSN tunnels data plane traffic to/from last hop router (SGSN) on local subnet
  - Mobile host signals SGSN to detect movement but no change in IP address
  - SGSN signals host route updates to GGSN
  - GGSN updates tunnel endpoint
GPRS Stack
GPRS Architecture

- GGSN
- SGSN1
- SGSN2
- Internet
- Route Update
- Movement Detection
- Corresponding Host
Problems: Complex, Proprietary, and Limited

- Complex ties to legacy SS7 telephony signaling
  - GPRS also available on WLAN
    - Probably won't be deployed because there are simpler solutions
    - Many unnecessary hooks for QoS, charging, etc. that slow initial session establishment
- Proprietary to GSM Operators
  - Not a general solution for the Internet
- Limited topological scope for keeping address constant
  - Doesn't work when the mobile host changes to a different AS
    - BGP routed prefixes change
  - Also might not work for a service provider with a global network
- GSM Operators use a proprietary protocol to route from one GPRS network to another
  - No host involvement
  - Many technical flaws
  ➔ GPRS-like protocol with no SS7 legacy and confined to mobility management
Bottom Line

- There are too many ways to handle mobility management
- Many are specific to particular wireless link technologies
- Service application writers can never know whether mobility management will be available in the deployment environment
- Wanted: mobility management just works, everywhere, like routing does
NETLMM (NETwork based, Localized Mobility Management)
Three Tiered Mobility Management

• Layer 2 Mobility
  – Allows movement within an IP subnet
  – Movement from one wireless access point/base station to another
  – Causes a node’s basic link to the network to move
    • Without it, a node loses link connectivity and basic networking fails

• Global Mobility
  – Movement between two IP subnets
  – Requires change in the identity to locator mapping
  – Causes a node’s IP routing to move
    • Without it, a node loses forwarding service and packet delivery for existing sessions fails

• Localized Mobility
  – Movement between links within a locally contained network topology
  – Extent of the containment depends on the deployment
    • But it does not span the Internet
  – No change in IP address
  – Node may change to a new access router as it moves but won’t change subnet
  – Causes a node’s IP routing to move without node involvement
    • Without it, a node experiences handover delays due to IP subnet configuration signaling
What is NETLMM?

- IETF Working Group developing a network based mobility management protocol for IPv6
- Network based: no involvement on the part of the host
  - Other than possibly simple IP level movement detection
- Localized Mobility Management: mobility management service is provided over a restricted chunk of topology not the entire Internet
  - Need another protocol for global mobility management
    - Global mobility management: session continuity between NETLMM domains and roaming
    - Provided by Client Mobile IP, HIP, etc.
- Mobility management just works if global mobility management isn’t needed
  - Provided network operators deploy NETLMM
Proxy Mobile IP

- IETF NETLMM WG has selected Proxy Mobile IP for mobility management
  - 3GPP2 requested IETF to standardize
  - Excellent deployment prospects
  - 3GPP is also considering
- Mobile IP client functions move to a proxy node at the access router
  - No localized mobility management functions on the terminal
  - Still need global mobility management (Client Mobile IP, HIP, etc.)
- Local home agent allocated in access network
- Home agent protocol changes from RFC 3775
  - RFC 3775 has strong end to end security, changes needed for Proxy Mobile IP
  - Possible addition of aggregated tunneling to improve prospects for traffic management
  - Other...
Proxy Mobile IP Overview

**Prefix**
- **CAFÉ::/64**
- **BABA::/64**

**Mobile IP Tunnel**
A IPinIP tunnel HA and PMA.

**Home Network**
Mobile’s Home Network (Topological Anchor Point)

**Home Agent**

**Access Router**

**Care of Address (CoA)**
The address of the Proxy Mobile Agent. That will be the tunnel end-point.

**Proxy Binding Update (PBU)**
Control message sent out by PMA to HA to register its correct location.

**LMM Network**
Why Not Use Proxy Mobile IP for Global Mobility Management Too?

- Proxy Mobile IP could support network-based global mobility management
  - Don’t allocate a local home agent
  - Use home agent in home network
- But network-based Global Mobility Management may be harmful for Internet...
- Mobile terminals must be “access network-agile”
  - If access network doesn’t have mobility management, terminals must still be able to move
  - Client-side mobility management is essential for this
- Tussle between large operators and small
  - Large operators could form closed roaming consortia with all members globally linked
    - “Mobility Walled Gardens”
  - Client side mobility management enables small operators to preserve a niche
  - Large operators benefit too
    - Small market roaming partner choice more competitive
- Protocol design to support local mobility management only???
  - Doubtful
Summary and Conclusions
Three Tiered Mobility Management Architecture

- Layer 2 mobility for movement within an IP subnet
  - All Layer 2 protocols support some kind of Layer 2 mobility management protocol
- Network-based, localized mobility management for movement within a constrained topological and geographical area
  - Local IP address doesn’t change
  - Host involvement at IP level limited to movement detection
- Host-based, global mobility management for roaming and large topological movements
  - Change in local IP address due to service provider change or movement outside of localized mobility management domain
  - Host required to sense wireless on a new interface and move sessions to the interface