Mobility Management

Advanced Mobile Communication Networks
Motivation

• The Internet and mobile communication networks are experiencing an enormous growth

• Future networks will interconnect various heterogeneous networks by means of a common IP core, also referred to as All-IP

• Goals: always-on connectivity, higher bandwidth, reduced delay, lower cost, etc.

• Challenge: support mobility between cells connected through an IP core while satisfying real-time and QoS requirements
Mobility Management Approaches in the TCP/IP Reference Model
Which Layer Handles Mobility?

ISO/OSI

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer

TCP/IP

- Application layer mobility
- Session layer mobility
- Transport layer mobility
- Network layer mobility
- Link layer mobility
Which Layer Handles Mobility?

• Link layer mobility management is responsible for the establishment of a radio link between the Mobile Node (MN) and the new Access Point (AP)

• No more procedures are required if the old as well as the new AP belong to the same subnet

• If the new AP belongs to a new subnet, we need mobility support either
  – in the network layer, i.e. the Internet layer of the TCP/IP reference model,
  – in the transport layer or
  – in the application layer
Mobility Management in Different Layers, Why?

• Link layer mobility
  – Required when changing the point of attachment
  – Responsible for establishment of a wireless link

• Network layer mobility
  – Transparency to higher layer protocols, e.g. TCP and UDP
  – Applications on mobiles can further communicate with existing applications without any modifications
  – Change of network architecture is allowed

• Transport layer mobility
  – End-to-end mobility management while keeping the Internet infrastructure unchanged
  – End hosts take care of mobility, i.e. TCP and UDP are updated to support mobility
Mobility Management in Different Layers, Why?

- **Session layer mobility**
  - Migration of sessions between devices

- **Application layer mobility**
  - No changes to current networks
  - Example: extending IP telephony infrastructure to fulfill mobility requirements
  - Usage of SIP protocol and support for mobility by change of the mapping between a name of a user (e.g. mail address) and the IP address

- **Hybrid layer mobility**
  - Optimization of the performance of a certain layer mobility management approach using information from other layers or the integration of solutions from several layers
  - Synchronization between layers is essential
Tasks and criteria of mobility management

• Important tasks of mobility management
  − Find and address a mobile away from home
  − Support “continuous“ communication after change of location
  − Security: avoid misuse of mechanism
  − Privacy: hide location from others

• Important criteria to compare mobility protocols
  − Handover (HO) performance
    • Delay to update the route
    • Packet loss due to handover
  − Protocol overhead: consumption of network resources
  − Scalability: protocol overhead in large networks with large numbers of mobile nodes
  − Robustness: adaptability to different network conditions and failures
  − Ease of deployment: simplicity, suitability to different network scenarios
Link Layer Mobility Management
Link Layer Handoff

• This scenario considers handoffs between WLAN access points (APs) as an example!
  – Other communication systems use more sophisticated handoff mechanisms!

• Responsible for the establishment of a radio link between the MN and the AP

• The handoff comprises 4 phases
  – Recognizing the loss of the wireless connection
  – Search for and detection of a new adequate AP
  – Re-/Authentication with the new discovered AP
  – Re-/Association with the new discovered AP
Recognizing the Loss of the Wireless Connection

• Connection loss is detected based on
  – Weakness of the received signal or
  – Failed frame transmissions

• Weakness of the received signal
  – Most frequently used approach
  – A layer 2 handoff is prompted, if the received signal strength goes below a certain threshold

• Failed frame transmissions
  – Slower than received-signal-strength-based approach
  – The MN first assumes a collision as a reason for failed frame transmissions; if not, radio signal fading is assumed; if not, an out of range is declared
Search and Detection of a New Adequate AP

- Passive scanning

![Diagram showing the process of searching and detecting an adequate Access Point (AP) through passive scanning. The diagram illustrates the change of frequencies and the beacons transmitted at 100 milliseconds.]
Search and Detection of a New Adequate AP

- **Active scanning**

  - Change to frequency A
  - Probe request
  - No activities on this channel
  - Change to frequency B
  - Probe request
  - Probe delay
  - MinChannelTime
  - Probe delay
  - MinChannelTime
  - MaxChannelTime
  - Probe response

  AP operating in frequency B
  AP operating in frequency C
Re-/Authentication with the New Discovered AP

• The MN authenticates itself to the new AP

• Two authentication methods are defined for the IEEE 802.11 standard
  – Open system: null-authentication (default method)
  – Shared key authentication: none null-authentication

• Exchange of authentication request & authentication response messages

• More messages can be exchanged between the authentication request & response; details depend on the authentication method
Re-/Association With the New Discovered AP

• Exchange of association request & association response messages

• After this phase, the wireless link is established
Link Layer Handoff

- Large variation for the same hardware with same configuration mainly due to stochastic behavior of radio interface

- Scanning is the main factor for handoff latency, it accounts for
  - about 90% of the overall handoff delay
Research Issues

• Speeding up the layer 2 handoff requires accelerating the scanning phase
  – Periodic scanning
    • Scanning the medium while the MN is still connected to the old AP
    • When the signal strength of the current AP is decreasing, the MN switches to another frequency for a short time and scans for other available APs
  – Information about neighbors
    • Utilizing information about neighbor APs to reduce the number of channels that must be scanned
Network Layer Mobility Management
-
Basics
What is the problem and how to solve?
What is the problem and how to solve?

Communication disruption should be minimized or even eliminated
What is the problem and how to solve it?

• Routing
  – Forwarding is based on some destination address (a locator)
  – Change of location (due to mobility) requires change of destination address or needs an update of routing tables

• Ideas
  – Specific routes to end systems (per-host forwarding)
  – Multicast
  – Modification of the destination address
  – Tunneling
Specific routes to end systems

• Change of routing table entries to forward packets to the right destination
• Distribution of routing information for every mobile everywhere
Specific routes to end systems

- Change of routing table entries to forward packets to the right destination
- Distribution of routing information for every mobile (rather than subnets) everywhere
- Does not scale to a large network
- Security problems (routing table updates)
Multicast

- Building of a multicast tree
  - Security problem
  - Overhead
Modification of the destination address

• Adjust the host address depending on the current location
  - Problems to find a mobile host without a constant address
  - Problems with application due to change of address
  - Security problem
Tunneling

- Separation of a terminal/user identificator from a topological locator
  - Security problem
- Location update at HA

Tunnel data packets to the new location
Mobile IP

• Requirements for Mobile IP
  – Transparency
    – Mobile end-systems keep their IP address
    – Continuation of communication after interruption of link
    – Point of connection to the fixed network can be changed
  – Compatibility
    – Support of the same layer 2 protocols as IP
    – No changes to current end-systems and routers required
    – Mobile end-systems can communicate with fixed systems
  – Security
    – Authentication of all registration messages
  – Efficiency and scalability
    – Only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
    – World-wide support of a large number of mobile systems in the whole Internet
Mobile IP terminology

- **Mobile Node (MN)**
  - System (node) that can change the point of connection to the network without changing its IP address

- **Home Agent (HA)**
  - System in the home network of the MN, typically a router
  - Registers the location of the MN, tunnels IP datagrams to the CoA

- **Foreign Agent (FA)**
  - System in the current foreign network of the MN, typically a router
  - Forwards the tunneled datagrams to the MN, typically also the default router for the MN

- **Care-of Address (CoA)**
  - Address of the current tunnel end-point for the MN (at FA or MN)
  - Current location of the MN from an IP point of view
  - Can be chosen, e.g., via DHCP

- **Correspondent Node (CN)**
  - Communication partner
Mobile IP basics: example network

- **HA** (Home Agent)
- **Router**
- **Internet**
- **FA** (Foreign Agent)
- **MN** (Mobile Node)
- **CN** (Client Node)

**Home network: physical network for the MN**

**Foreign network: current physical network for the MN**
Mobile IP basics: data transfer to the mobile node

1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to CoA, here FA, by encapsulation
3. FA forwards the packet to the MN
Mobile IP basics: data transfer from the mobile node

1. Sender sends to the IP address of the receiver as usual, FA works as default route
Mobile IP basics: agent discovery (IPv4)

- Agent discovery: How does the MN discover that it has moved?
  - Agent advertisement:
    - FAs and HAs advertise their presence periodically using special agent advertisement messages
      - For these advertisements Internet control message protocol (ICMP) messages are used with some mobility extensions
      - The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them
  - Agent solicitation:
    - If no agent advertisements are present or the inter-arrival time is too high, and an MN has not received a CoA by other means
    - The mobile node must send agent solicitations
      - A mobile node can send out three solicitations, one per second, as soon as it enters a new network
      - If a node does not receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network until it reaches a maximum interval between solicitations (typically one minute)
Mobile IP basics: agent discovery and registration (IPv4)

- Here the CoA denotes the address of the FA
  - The MN could also get it directly via DHCP (co-located care-off address)
- The binding update is a remote redirect and therefore needs authentication
- After the registration, the HA tunnels data for the MN to the CoA
Mobile IP basics: registration (IPv4)

- Registration (always limited lifetime!)
  - Having received a CoA, the MN has to register with the HA
  - The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets.

- There are two ways of registration:
  - CoA is at the FA:
    - The MN sends its registration request containing the CoA to the FA
    - FA forwards the request to the HA
    - HA now sets up a **mobility binding** containing the mobile node’s home IP address and the current CoA
    - After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN
  - CoA is co-located:
    - MN sends the request directly to the HA and vice versa
Mobile IP basics: registration (IPv4)

CoA is at the FA

CoA is co-located
Mobile IP basics: tunnel end points (IPv4)

- Home address: 10.10.0.10
- CoA:
  1. FA-CoA: 9.9.0.0 or
  2. Co-located CoA: 9.9.x.x

Destination is: 10.10.0.10
Mobile IP basics: tunnel end points (IPv4)

- Home address: 10.10.0.10
- CoA:
  1. FA-CoA: 9.9.0.0 or
  2. Co-located CoA: 9.9.0.2

De-tunneling by MN
Mobile IP basics: agent discovery and registration (IPv4)

- **Agent Advertisement**
  - HA and FA periodically send advertisement messages into their physical subnets
  - MN listens to these messages and detects, if it is in the home or a foreign network
  - MN reads a CoA from the FA advertisement messages
  
  Note: agent advertisement may be solicited by MN (agent solicitation msg)

- **Registration (always limited lifetime!)**
  - MN signals CoA to the HA via the FA, HA acknowledges via FA to MN
  - These actions have to be secured by authentication

- **Advertisement (ICMP extensions to RFC 1256)**
  - HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
  - Routers adjust their entries; these are stable for a longer time (HA responsible for a MN over a longer period of time)
  - Packets to the MN are sent to the HA, independent of changes in CoA/FA
Tunneling

- Tunneling ➔ sending a packet through a tunnel, is achieved by using encapsulation.
- **Encapsulation** is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.
- **Decapsulation** is the reverse operation, taking a packet out of the data part of another packet.

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>Original data</th>
</tr>
</thead>
<tbody>
<tr>
<td>new IP header</td>
<td>New data</td>
</tr>
<tr>
<td>Outer header</td>
<td>Inner header</td>
</tr>
</tbody>
</table>
Tunneling

- Encapsulation of one packet into another as payload
  - E.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
  - Here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)
- IP-in-IP encapsulation (mandatory, RFC 2003)
  - Tunnel between HA and CoA

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ver.</td>
<td>IHL</td>
<td>TOS</td>
<td>length</td>
<td></td>
</tr>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td><strong>IP-in-IP</strong></td>
<td>IP checksum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of HA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Care-of address COA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ver.</td>
<td>IHL</td>
<td>TOS</td>
<td>length</td>
<td></td>
</tr>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>lay. 4 prot.</td>
<td>IP checksum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of CN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of MN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TCP/UDP/ ... payload

MIP header

IP packet
Tunneling

- **Minimal encapsulation (optional)**
  - Avoids repetition of identical fields
    - E.g. TTL, IHL, version, TOS
  - Only applicable for unfragmented packets, no space left for fragment identification

<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>TOS</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>min. encap.</td>
<td>IP checksum</td>
<td></td>
</tr>
<tr>
<td>IP address of HA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>care-of address COA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lay. 4 protoc.</td>
<td>S</td>
<td>reserved</td>
<td>IP checksum</td>
</tr>
<tr>
<td>IP address of MN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>original sender IP address (if S=1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/UDP/ ... payload</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MIP header**

**Minimized IP packet**
Optimization of packet forwarding

• Triangular Routing
  – CN sends all packets via HA to MN
    • Higher latency and network load

• Ideas for Solutions
  – CN learns the current location of MN
  – Direct tunneling to this location
  – HA informs a sender about the location of MN
  – Security problems with binding updates

• Change of FA
  – Packets on-the-fly during the change can be lost
  – New FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
  – This information also enables the old FA to release resources for the MN
Tunneling and route optimization (IPv4)

- The home agent can either use IP-within-IP or minimal encapsulation to reduce the header overhead
- **Route optimization** can be done if the HA sends a Binding Update to the CN
  - Subsequent packets can be tunneled directly from the CN to the FA
- In the reverse direction normal standard IP routing mechanisms are used to deliver IP datagrams from the MN
- Problems if the MN moves to another FA!
After having moved to the new FA, the MN can also communicate its new care-of address to the previous FA.

Note that most of the Binding Update messages are not emitted by the MN, thus they are not going over the wireless link.

Problem if FA1 does not know the new care-of address of the MN:
- FA1 must re-route the traffic to the HA, which again handles it via a new tunnel to FA2.
Change of foreign agent (IPv4)
Reverse tunneling (RFC 3024)

1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)
Mobile IP with reverse tunneling

• Router accept often only “topological correct“ addresses (firewall!)
  – A packet from the MN encapsulated by the FA is now topological correct
  – Furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is too far away from the receiver)

• Reverse tunneling does not solve
  – Problems with *firewalls*, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
  – Optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)

• MIP reverse tunneling is backwards compatible
  – The extensions can be implemented easily and cooperate with current implementations of Mobile IP without these extensions
  – Agent advertisements can carry requests for reverse tunneling
Mobile IP and IPv6

- Huge address space with IPv6 address renumbering scheme
- Better mobility support
  - Mobile IP was designed as add-on to IPv4
  - Majority of IPv4 nodes do not support Mobile IP
- MN can use **Address Autoconfiguration** which eliminates the need of a Foreign Agent
  - **Stateless**: to configure its care-of address from a NW prefix of the foreign NW and a MN interface identifier. The needed information is published by neighboring routers through the Neighbor Discovery protocol in the foreign network (combined ARP/ICMP)
  - **Stateful**: by using a centralized DHCP server
- **Source Routing**: Instead of tunneling packets using “IP in IP”, IPv6 Routing Headers are used
- IPv6 does work smoothly with **ingress filtering**
  - In IPv4 a border router may discard IP packets not originating from its own subnet, and MN use their home address always as source address
- Every IPv6 node will have implemented IPv6 **authentication headers** to be used with binding updates
Mobile IPv6 (MIPv6)

Home Agent (HA)

Access Router (AR)

Periodic broadcast of Router Advertisements (RA)

Corresponding Node (CN)

Internet

No support for mobility (standard IPv6 router)

Mobility support; use of two IP addresses (Home Address (HoA) & Care of Address (CoA))
MIPv6 - Handoff

Binding Acknowledgements (BAs)
Uplink data packets are dealt with as standard IP packets.
MIPv6 - Pros & Cons

• Pros
  – End-to-end mobility
  – Transparency to upper layer protocols
  – Proper integration with IP

• Cons
  – Handoff latencies (traffic interruption) due to contacting the HA and the CN each time the MN changes the point of attachment
  – Overhead due to encapsulation
  – Signaling load due to frequent BUs especially when MNs move at high speeds
  – Sub-optimal routing and increased end-to-end delay due to triangular routing where CN is not MIPv6 enabled (binding updates) or due to lack of security
Dynamic Host Configuration Protocol (DHCP)

• Application
  – Simplification of installation and maintenance of networked computers
  – Supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
  – Enables automatic integration of systems into an Intranet or the Internet
  – Can be used to acquire a CoA for Mobile IP (co-location of MN and FA)

• Client/Server-Model
  – The client sends via a MAC broadcast a request to the DHCP server (might be via a DHCP relay)
DHCP – protocol mechanisms

Server (not selected) → Initialization → DHCPDISCOVER → DHCPOFFER → DHCPREQUEST (Reject) → DHCPACK → Initialization completed

Client → Collection of replies → DHCPOFFER → DHCPREQUEST (Options) → DHCPACK

Server (selected) → Confirmation of configuration

Determine the configuration

Delete context
DHCP characteristics

• Server
  – Several servers can be configured for DHCP, coordination not yet standardized (i.e. manual configuration)

• Renewal of configurations
  – IP addresses have to be requested periodically, simplified protocol

• Options (RFC 2132)
  – Available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)

• Big security problems!
  – No authentication of DHCP information specified
Network Layer Mobility Management

- Advanced Solutions
Approaches for Network Layer Mobility Management

Terminal-based mobility management

- Mobility support in the network and MNs
- MNs participate in mobility procedures
- Disadvantages
  - SW update to MNs needed

Network-based mobility management

- Mobility support in the network only (terminals with legacy IP stack can be mobile)
- No interaction between the network and MNs
- Disadvantages
  - Many features are hard to realize, e.g. route optimization
  - Focus is on support of global mobility
Macro and Micro Mobility Management

Movements between different domains are typically handled by MIP, also called macro or inter-domain mobility.

HA is not aware of each change in the point of attachment.

Movements inside the domain are controlled by the intermediate node, also called micro or intra-domain mobility.

Internet

HA

Intermediate node

Administrative domain

Administrative domain
Macro and Micro Mobility Management

• Macro mobility management approaches
  – Aim at global mobility support
  – Base protocols: Mobile IPv4 (RFC 3344) & Mobile IPv6 (RFC3775)

• Micro mobility management approaches
  – Performance improvements through localizing the mobility processing inside administrative domains
  – Introduction of new intermediate nodes to the network
  – Hierarchical network topology is typically required
Proxy Agent Approaches (PAA)

• Extend the principle of MIP to provide micro mobility

• Introduce new intermediate nodes to the network to process the mobility inside an administrative domain locally

• Data packets destined to the MN are forwarded to the intermediate node, which tunnels them towards the MN’s current point of attachment

• Examples
  – Hierarchical MIPv6 (HMIPv6), Anchor Foreign Agent (AFA), Seamless MIP (S-MIP), etc.
Improved Micro Mobility: Hierarchical MIPv6

MN registers a Regional CoA (RCoA), i.e. a CoA in the MAP’s subnet, in its HA as the MN’s CoA; the location of the MN inside the domain is defined by the local CoA (LCoA), which is a CoA in the current AR subnet.

HA is not aware of the MN’s mobility as long as the RCoA is not changed.
HMIPv6 – Handoff

The MN configures a new LCoA
HMIPv6 – Data Communication

Internet

HA

MAP

AR1

AR2

AR3

AR4

AR5

AR6

CN
HMIPv6 – Pros & Cons

• Pros
  – Localizing of mobility management inside administrative domains
  – Improving the performance: reduced handoff latency compared to MIPv6, reduced packet loss, etc.
  – Reducing the signaling load traveling towards the HA

• Cons
  – Restrictions on the network topology
  – Single point of failure (all traffic passes through the MAP)
  – Increased signaling and packet forwarding overhead inside the domain
  – Security issues: how to authenticate arriving MNs?
Localized Enhanced Routing Schemes (LERS)

• Similar principle as PAA approaches

• Typically introduce a new dynamic layer 3 routing protocol inside the domain (per-hop routing)

• Data packets destined for the MN are forwarded to the intermediate node controlling the domain, which forwards them hop per hop towards the MN

• All nodes in the domain should be mobility-aware

• Examples
  – Cellular IP, HAWAII
Improved Micro Mobility: Cellular IP

The gateway controls the domain

IP-based routing of data packets inside the domain is replaced by a special CIP routing and location management

The MN registers the address of the gateway as its CoA; inside the domain, the MN uses its HoA

Beacon messages flooded periodically → all BSs know how to route packets towards the gateway
Cellular IP – Hard Handoff

Update its routing cache and starts forwarding data packets towards the new location of the MN.
Cellular IP – Semi-Soft Handoff

The MN detects a handoff in the near future \( \Rightarrow \) it switches for a short time to the radio of the new BS.

Update its routing cache and starts forwarding data packets towards the MN via the old and new BS.
Cellular IP – Semi-Soft Handoff

Update its routing cache and stops forwarding to the old BS

After the layer 2 handoff, the MN sends a route-update packet to stop the bicast
Cellular IP – Data Communication

Uplink packets are forwarded hop by hop towards the gateway; they are used to refresh the routing caches.

Routed using IP towards their destination.
Cellular IP – Pros & Cons

• Pros
  – Localizing of mobility management inside administrative domains
  – Improving the performance: reduced handoff latency, less lost packets, etc.
  – Reducing the signaling towards the HA
  – Mobile to mobile communication within the domain has to be routed via the gateway

• Cons
  – Every node in the domain has to be mobility-aware
  – Restrictions on the network topology
  – Single point of failure (all traffic travels through the gateway)
  – Signaling and packet forwarding overhead inside the domain
  – Reduced TCP throughput due to new layer 3 dynamic routing protocol
  – Security issues: authentication of arriving MNs, authentication of route-update messages, etc.
Network-based MM: Proxy MIPv6

Support of mobility is required in the MAGs; each MAG emulates the home network of each MN served by it.

MN does not have to understand mobility; from the MN’s point of view, it is located in its home network and the whole domain represents a single point of attachment.

Unicast RA with the Home Network Prefix (HNP) of the MN.
Proxy MIPv6 – Handoff

Start a timer to delete the mobility binding of the MN

Proxy Binding Acknowledgement (PBAck)

De-Registration Proxy Binding Update (DeReg PBU)

The MAG detects a detach event
Proxy MIPv6 – Handoff

Accepts the binding, allocates MN-HNP and sets up a tunnel to the MAG

The MAG detects an attach event & acquires the MN-ID and profile, from AAA server for example

A unicast RA with the MN-HNP → the MN assumes that it is located in its home network and thus there is no need for a re-configuration of its IP address
Proxy MIPv6 – Data Communication

[Diagram of Proxy MIPv6 network highlighting components such as LMA, CN, MAGs, and Internet connections.

Integrated Communication Systems Group

Advanced Mobile Communication Networks, Master Program
Proxy MIPv6 – Pros & Cons

• **Pros**
  – Transparency to MNs (MN\s with no mobility support can be mobile)
  – Protocol is robust against control messages dropping (no control messages are sent on wireless links)
  – Reduced signaling cost
  – Terminating the tunnel in the MAG instead of MN\s reduces the data traffic volume sent over the wireless link

• **Cons**
  – Triangular routing \(\rightarrow\) increased end-to-end delay
  – Overhead due to the encapsulation
  – Handoff latency due to contacting the LMA each time the MN moves from one point of attachment to another \(\rightarrow\) communication disruption
  – Route optimization is not possible
Conclusions

• Mobility management in future networks is IP-based

• Mobility can be implemented in different layers of the TCP/IP reference model; each layer has positive and negative impacts

• Network layer mobility approaches are the most deployed solutions
  – Terminal-based approaches interact with MNs to support mobility
  – Network-based approaches do not involve MNs in mobility support
  – Both approaches are categorized into macro and micro mobility management approaches
    • Macro mobility approaches aim at supporting global mobility
    • Micro mobility approaches aim at accelerating the mobility management through processing of mobility locally
References

- Jochen Schiller: Mobile Communications (German and English), Addison-Wesley, 2000 (chapter 9 provides an overview on Mobile IP)
- Wisely, Eardley, Burness: IP for 3G: Networking Technologies for Mobile Communications, Wiley, 2002 (chapter 5 provides classification of mobility mechanisms and overview on protocols, including session-layer mobility)

Important standards:
- Mobile IP: RFC 3220, formerly: RFC 2002
- Reverse tunneling: RFC 3024, formerly: 2344
- DHCP: RFC 2131, RFC 2132
- ICMP: RFC 1256