Background I: Internet Protocol (IP)

Internet Protocol IP, IPv4:

- Layer 3 Protocol (Network Layer)
- Packet (IP datagram) transmission between hosts (packet size up to 65535 bytes, often restricted by Layer 2 protocols)
- Routing using 32 bit addresses (v4)
- Most frequent transport protocols
  - Transmission Control Protocol TCP
  - User Datagram Protocol UDP
- Popular application layer protocols:
  - HyperText Transfer Protocol HTTP
  - File Transmission Protocol FTP
  - Simple Mail Transfer Protocol SMTP
Content

1. Background
   • Mobility & Handover Types
2. Mobile IP (v4)
   • Motivation, Principles, Messages, DHCP
3. MIP Performance aspects & improvements
   • HMIP, CIP
4. MIP Extensions/related topics
   • Security Aspects
   • Multi-homing/flow mobility
   • IPv6 and MIPv6
5. Mobility Support on higher layers
   • Transport layer mobility
   • Session Initiation Protocol and Mobility
6. Summary & Outlook
7. Experimental Measurements (optional)

Goal: Make students familiar with
• underlying problems
• solution approaches
• Overview on key technologies required to support mobility in IP-based networks

Background II: Mobility types

Assumption in this lecture: Infrastructure networks (only first hop wireless)

Different Levels of Mobility:
• Pico (e.g. within same radio cell)
• Micro (e.g. within same subnet)
• Macro (e.g. across subnets but within same administrative domain)
• Global (e.g. across different administrative domains)

‘Alternative’ classification:
• vertical mobility: changing access technology
**Background III: Handover & more mobility types**

Hand-over classification:
- Mobile initiated or network-initiated
- Backward or forward
- Mobile controlled or network controlled
- Mobile-assisted or network assisted or unassisted
- Proactive or reactive
- Make-before-break or break-before make
- Soft or hard
- fast (without 'noticable' delay)
- smooth (no loss of data)

More mobility types ...
- Host Mobility
- User Mobility
- Application Mobility
- Network Mobility

... and related identifiers
- IP address, hostname (DNS)
- User-name (e.g. SIP URL)
- address prefix / subnetmask

**Mobile IP Motivation: Host mobility & Routing**

Problem: IP address identifies host as well as topological location

Reason: IP Routing:
- Routes selected based on IP destination address
- network prefix (e.g. 129.13.42) determines physical subnet
- change of physical subnet → change of IP address to have a topological correct address

- Solution? Host-based routing: Specific routes to each host
  - Handover → change of all routing table entries in each (!) router
  - Scalability & performance problem

- Solution? Obtain new IP-address at hand-over
  - Problem: how to identify host after handover? DNS update → performance/scalability problem
  - Higher protocol layers (TCP/UDP/application) need to 'handle' changing IP address

→ Development of mobile IP
Mobile IP: Requirements (RFC 3344)

- **Transparency**
  - mobile end-systems keep their IP address
  - point of attachment to the fixed network can be changed
  - continuation of communication after handover possible (transparent to transport layer in mobile node as well as to correspondent node)

- **Compatibility**
  - support of the same layer 2 protocols as IP
  - no changes to correspondent nodes and routers required

- **Security**
  - authentication of all registration messages

- **Efficiency and scalability**
  - only small data volume for additional messages to/from the mobile node (connection typically via a low bandwidth radio link)
  - world-wide support of a large number of mobile nodes (via the whole Internet)

Mobile IP: Principles & Terminology

**Underlying Approach:** separate host identifier and location identifier

- **Terminology:**
  - **Mobile Node (MN)** with fixed IP address IP₁ (home address)
  - **Home Network:** subnet that contains IP₁
  - **Home Agent (HA):** node in home network, responsible for packet forwarding to MN
  - **Visited Network:** new subnet after roaming / handover
  - **Care-of Address (CoA):** temporary IP address within visited network
  - **Foreign Agent (FA):** node in visited network, responsible for packet forwarding to CoA
**Mobile IP: Tunneling & Triangle Routing**

1. CN sends packets to the MN using its Home Address IP1.
2. HA tunnels them to FA, using CoA1. FA forwards them to MN.
3. MN sends packets back to the CN using IP2 (without any tunneling).
   - Home Agent needs to contain mapping of care-of address to home address (location register).

**Mobile IP: Tunneling**

**Default encapsulation:**
- IP-within-IP (RFC2003)

**Other Approaches:**
- Minimal encapsulation (RFC2004)
- Generic Routing Encapsulation (GRE) (RFC1702)
**Tunneling: IP in IP Encapsulation**

- IP-in-IP-encapsulation (support in MIP mandatory, RFC 2003)
  - tunnel between HA and COA

<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>flags</th>
<th>fragment offset</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP identification</td>
<td>IP-in-IP</td>
<td>IP checksum</td>
<td>COA [Care-of address]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TTL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Drawback of tunneling
  - Possibly long routes between CN and MN (many hops)
  - Increase of data volume increase (additional 20 bytes IP header) → possibly fragmentation

**Tunneling: Minimal Encapsulation**

- Minimal encapsulation (optional)
  - avoids repetition of identical fields (e.g. TTL, IHL, version, DS/TOS)
  - only applicable for un-fragmented packets (no space left for fragment identification)

<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>flags</th>
<th>fragment offset</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP identification</td>
<td>min. encaps</td>
<td>IP checksum</td>
<td>COA [Care-of address]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TTL</td>
<td>lay. 4 prot</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

|      | IP address of MN | IP address of CN | IP address of HA |
| lay. 4 prot. | S reserved | IP checksum | |
**Mobile IP: Agent Discovery & Registration**

- Mobile Node finds out about FA through **Agent Advertisements**
  - FAs broadcast Advertisements in periodic intervals
  - Advertisements can be triggered by an **Agent Solicitation** from the MN
- Care of Address of the MN is determined, either
  - Dynamically, e.g. using Dynamic Host Configuration Protocol (DHCP)
  - Or: use IP address of FA as CoA
- MN registers at FA and HA: **Registration Request & Reply**
  - MN signals CoA to the HA via the FA
  - HA acknowledges via FA to MN
- Registration with old FA simply expires (limited life-time, *soft-state*)

**MIP messages: Agent advertisement**

**Procedure:**
- HA and FA periodically broadcast advertisement messages into their subnets
- MN listens to these messages and detects, if it is in the home or a (new?) foreign network
- when new foreign network: MN reads a CoA from the advertisement (opt.)

**ICMP Router Discovery extension:**
- type = 16
  - R: registration required
  - B: busy, no more registrations
  - H: home agent
  - F: foreign agent
  - M: minimal encapsulation
  - G: GRE encapsulation
  - r: !=0, ignored (former Van Jacobson compression)
  - T: FA supports reverse tunneling
  - reserved: =0, ignored
**MIP messages: registration request & reply**

**Registration Request (via UDP)**

- S: simultaneous bindings
- B: broadcast datagrams
- D: decapsulation by MN
- M: minimal encapsulation
- G: GRE encapsulation
- r: =0, ignored
- T: reverse tunneling requested
- x: =0, ignored

```
0  7  8 15 16 23 24 31
type = 1  S  B  D  M

definition
  home address
  home agent
  COA
  identification
  extensions . . .

```

**Registration Reply (UDP)**

Example codes:

- registration successful
  - 0 registration accepted
  - 68 home agent failed authentication
  - 69 requested Lifetime too long
  - 129 registration denied by FA
  - 130 administrative prohibited
  - 133 registration Identification mismatch
  - 135 too many simultaneous mobility bindings

- registration denied by FA
  - 65 administratively prohibited
  - 66 insufficient resources
  - 67 mobile node failed authentication

```
0  7  8 15 16 31
type = 3  code  lifetime

definition
  home address
  home agent
  identification
  extensions . . .

```

**MIP: Care-of addresses**

MN obtains local care-of address either

- from FA Advertisement (see before)
- or via Dynamic Host Configuration Protocol (DHCP)
  - supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
  - Client/Server-Model: client sends request via L2 broadcast

![DHCP Diagram]

Wireless Networks I, Spring 2005: MM4, Advanced Mobility Support
Content

1. Background
   • IP, IETF, Mobility & Handover Types

2. Mobile IP (v4)
   • Motivation, Principles, Messages, DHCP

3. MIP Performance aspects & improvements
   • HMIP, CIP

4. MIP Extensions/related topics
   • Security Aspects
   • Multi-homing/flow mobility
   • IPv6 and MIPv6

5. Mobility Support on higher layers
   • Transport layer mobility
   • Session Initiation Protocol and Mobility

6. Summary & Outlook
   + Exercises

---

MIP Performance Aspects: Handover

Events during handover
• Loss of connectivity to AP (L2)
• Scan for new APs
• Obtain connectivity to new AP (L2)

• [send Agent solicitation (L2 trigger)]
• receive Agent advertisement/obtain new IP address
• send registration
• receive registration reply

MN can receive 'new' data packets from CN, when registration request is successfully processed by HA
→ Handover delay,
possible loss of data-packets (sent to old 'FA' during handover)

Qu.: When can MN send packets again?
**Link-Layer Hand-over: Measurements 802.11b**

Scenario

- Hard Handover in 802.11b
- Both APs use same SSID
- HO initiated by pulling cable from AP1 ('Istanbul')

Source: Master Thesis, Rui Martins

---

**Measurements II: Hard Hand-over**

<table>
<thead>
<tr>
<th>Downlink Connection</th>
<th>Uplink Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="chart1" alt="Downlink Throughput" /></td>
<td><img src="chart2" alt="Uplink Throughput" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Handover Time [s]</th>
<th># Lost Packets during HO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average (10 meas.)</td>
<td>Handover Time [s]</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>0.6273</td>
<td>316.8</td>
</tr>
<tr>
<td>0.1701</td>
<td>4.2</td>
</tr>
</tbody>
</table>
Measurements III: Soft Hand-over Scenario

General Setup

- Both AP’s set with the same SSID
- 10 measurements for UL and DL

Test-bed

Distance: 33m  
Speed: 1.5 m/s  
Average Time: 11s

Measurements IV: Soft Handover Results

Uplink connection

<table>
<thead>
<tr>
<th></th>
<th>% Lost Packets before HO</th>
<th>% Lost Packets due to HO</th>
<th>% Lost Packets during HO</th>
<th>HO time [s]</th>
<th>% Lost Packets after HO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Connection</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0.114891</td>
<td>0</td>
</tr>
</tbody>
</table>

Downlink connection

<table>
<thead>
<tr>
<th></th>
<th>% Lost Packets before HO</th>
<th>% Lost Packets due to HO</th>
<th>% Lost Packets during HO</th>
<th>HO time [ms]</th>
<th>% Lost Packets after HO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Connection</td>
<td>10.7</td>
<td>2366.9</td>
<td>0</td>
<td>3.5969</td>
<td>0</td>
</tr>
</tbody>
</table>
**Intermission: Handover classification (Exercise)**

MIP handover is ...
- Mobile initiated or network-initiated?
- backward or forward?
- mobile controlled or network controlled?
- Mobile-assisted or network assisted or unassisted?
- Proactive or reactive?
- Make-before-break or break-before make?
- Soft or hard?
- fast (without noticeable delay)?
- smooth (no loss of data)?

**MIP: Performance Enhancements**

Techniques to achieve fast and/or smooth handover:
- Layer 2 triggers (agent solicitations)
- Handover prediction & multicast (simultaneous bindings)
- Bidirectional edge tunnels & buffering
- Route Optimization (avoid triangular routing)
- Regional Registrations
Hierarchical Approaches

- Optimization for:
  - long registration delay
  - inefficient routing paths
  - Frequent re-registration at HA (even though mostly 'local' mobility

- Example (Hierarchical Mobile IPv4):
  - Hierarchy of Foreign Agents
  - Every FA re-tunnels the packets to the next FA until it reaches the MN
  - When a handoff occurs, the MN sends a regional registration request to the lowest level FA
  - FAs can also re-direct up-stream packets, if the destination (home-address) is registered within their domain

Similar Approach using ‘local Home Agents’ (called Mobility Anchor Points) in HMIPv6
draft-ietf-mobileip-hmipv6-08.txt (June2003)

Hybrid Approaches: Cellular IP

- Solutions to the local management of micro-mobility events
- Mobile IP is used for global mobility
- A gateway (GW) acts as foreign agent for each domain (all MNs use GW address as c/o)
- Within the domain: host-based routing
  - routing cache entries using soft-state
  - routing cache updated by upstream packets
  - separate paging cache for in-active nodes
  - routers within domain have to be CIP aware

- Similar approach: Hand-off Aware Wireless Access Internet Infrastructure (HAWAII)
Content

1. Background
   • IP, IETF, Mobility & Handover Types

2. Mobile IP (v4)
   • Motivation, Principles, Messages, DHCP

3. MIP Performance aspects & improvements
   • HMIP, CIP

4. MIP Extensions/related topics
   • Security Aspects
   • Multi-homing/flow mobility
   • IPv6 and MIPv6

5. Mobility Support on higher layers
   • Transport layer mobility
   • Session Initiation Protocol and Mobility

6. Summary & Outlook
   + Exercises

MIP Security Aspects I: Basics (optional)

• General security requirements (Security Architecture for the Internet Protocol, RFC 1825)
  – Authentication
    the origin of the data can be determined
  – Integrity
    messages cannot be modified by a third party
  – Confidentiality
    only authorized partners (e.g. sender & receiver) can read the data
  – Non-Repudiation
    sender cannot deny sending of data
  – Prevention of Traffic Analysis
    creation of traffic and user profiles should not be possible
  – Replay Protection
    replay of earlier messages by an attacker can be detected
• Additionally: Availability (Prevent Denial of Service Attacks)
MIP security aspects II: Security associations

- Security Association (SA) for registrations (optional)
  - extended authentication of registration

- SA contains the following parameters
  - Destination IP address
  - Cryptographic method for encryption/authentication
  - Encryption/authentication key
  - Lifetime of key
  - Specific parameters depending on crypticographic method

MIP security aspects III: Registration (optional)

Identification field: protection against replay attacks
- time stamps: 32 bit time-stamp + 32 bit random number
- Nonces: 32 bit random number (MH) + 32 bit random number (HA)
MIP security aspects IV: Authentication extension (optional)

- Part of Registration Messages: MN <-> HA, MN<->FA, FA<->HA

  0 1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 9 0 1
  +---------------------------------------------+
  | Type | Length | SPI ... |
  +---------------------------------------------+
  ... SPI (cont.) | Autenticator ...
  +---------------------------------------------+

- Computation of Autenticator: cryptographic keyed Hash function (e.g. HMAC-MD5 Algorithm) covering
  - UDP payload
  - All earlier extensions
  - Type, length and SPI of authentication extension
  Using the shared, secret key

- SPI (security parameter index)
  - determines algorithm, mode, and key

MIP security aspects V: Firewall traversal

- Ingress Filtering
  - Problem: MN sends packets to CN with source address = Home Address (and not c/o address)
  - Firewalls at domain boundaries suspect IP Spoofing discard packets
- Solution: Reverse Tunneling
**Multi-homing and flow mobility**

- **Multi-homing:** Host supports multiple interfaces with potentially different IP addresses
  - E.g. for redundancy purposes (e.g. SCTP)
  - Simultaneous, multiple wireless access techniques

- Goal: redirect different data-streams via ‘appropriate’ interfaces
  - only one home address (as host identifier)
  - multiple c/o addresses (one per interface)

→ **Flow Mobility**
  
  e.g. extension of mobile IP (IETF draft):
  - HA contains mapping [home address, flow identifier] → c/o address
  - Flows identified by (ranges of)
    - Source IP addresses (CNs)
    - Protocol type (TCP, UDP, etc.)
    - Port Numbers
    - DiffServ CodePoints
    - ... 

**MIP extensions: Context Transfer (I)**

- Routing-related service: extension of default ‘routing’ treatment (e.g. Packet discarding, scheduling, etc.)
- Context: information on the current state of routing-related service
  - Configuration context: unchanged during session
  - State context: changing over time
- Context Hierarchy:

  ![Context Hierarchy Diagram]

  Feature context examples:
  - Header compression
  - Quality of service
  - Security

- Context Transfer: re-establish routing related service on a new AP/router
**MIP Extensions: Context Transfer (II)**

Framework (expired seamboby draft):

![Diagram showing handover signalling](image)

- **SHIN**: Seamless Handover Initiate
- **SHREQ**: Seamless Handover Request
- **SHREP**: Seamless Handover Reply

**Basic Handover Signalling**

**Fast Handover Signalling**

---

**IP Version 6 (IPv6)**

**IPv6**
- Basic Header 40 Bytes
- 128-bit Network Addresses
- Flow label (QoS)
- No fragmentation in the network
- ‘Built-in’ Security
- Neighbor Discovery
- Extension Headers: Routing, Fragmentation, Authentication, Encryption

---

**IPv4**
- Basic Header 20 Bytes
- 32-bit Network Addresses
- Type of Service field
- Router may fragment packets
- IPsec as an enhancement
- ARP (Address Resolution Protocol)
- Options

---

**IP datagram**

<table>
<thead>
<tr>
<th>Offset</th>
<th>Version</th>
<th>Header Length</th>
<th>IP ID</th>
<th>Flags</th>
<th>Fragment Offset</th>
<th>Data Length (in bytes)</th>
<th>Protocol</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Next Header</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IPv6 in mobile settings

- Large number of IP addresses (each device needs at least two addresses!)
- Stateless autoconfiguration (can replace DHCP)
- Extension headers (selection)
  - 43 Routing Header
  - 44 Fragment Header
  - 51 Authentication Header
  - 50 Encrypted Security Payload
  - 60 Destination Options Header
  - 0 Hop-by-hop header
- Advantages for MIPv6
  - Route Optimisation (via binding updates) → no triangular routing
  - No foreign agent needed
  - Security easier to implement
  - Reverse tunneling can be avoided (c/o address as source address, home address in destination header)

Content

1. Background
   - IP, IETF, Mobility & Handover Types
2. Mobile IP (v4)
   - Motivation, Principles, Messages, DHCP
3. MIP Performance aspects & improvements
   - HMIP, CIP
4. MIP Extensions/related topics
   - Security Aspects
   - Multi-homing/flow mobility
   - IPv6 and MIPv6
5. Mobility Support on higher layers
   - Transport layer mobility
   - Session Initiation Protocol and Mobility
6. Summary & Outlook
+ Exercises
Transport Layer Protocols

Goal: data transfer between application (processes) in end-systems

- support of multiplexing/de-multiplexing
  e.g. socket API

  data stream/connection identified by:
  two IP addresses, protocol number, two port numbers

Overview: Transport Protocols

- User Datagram Protocol UDP (RFC 768)
  - Connectionless
  - Unreliable
  - No flow/congestion control

- Transmission Control Protocol TCP (RFC 793, 1122, 1323, 2018, 2581)
  - Connection-oriented (full duplex)
  - Reliable, in-order byte-stream delivery
  - Flow/congestion control

- Stream Control Transport Protocol SCTP (see later)

- Real-Time Transport Protocol RTP
  - Uses UDP
  - Provides: Time-stamps, sequence numbers
  - Supports: codecs, codec translation, mixing of multi-media streams
Streaming Control Transmission Protocol (SCTP)

- Defined in RFC2960 (see also RFC 3257, 3286)
- Purpose initially: Signalling Transport
- Features
  - Reliable, full-duplex unicast transport (performs retransmissions)
  - TCP-friendly flow control (+ many other features of TCP)
  - Multi-streaming, in sequence delivery within streams
    $\rightarrow$ Avoid head of line blocking (performance issue)
  - Multi-homing: hosts with multiple IP addresses, path monitoring (heart-beat mechanism), transparent failover to secondary paths
    - Useful for provisioning of network reliability

Transport Layer Handover in SCTP

1. MN communicates with CN via established SCTP association (From IP1 to IP CN)
2. When MN comes in Range of AP B
   - MN obtains new IP address IP2
   - MN adds IP2 to the existing SCTP association
     Address configuration Change (ASCONF) Chunk
3. When connection should be transferred to new AP B
   - MN sets primary address to IP2
   - MN deletes old IP1 from SCTP association (ASCONF chunk)
**SCTP Mobility support: Discussion**

- SCTP Handover transparent for network
  - No additional network infrastructure needed
  - Possible use-case: switch to peer-to-peer mode without network support
- avoids tunneling and tri-angular routing
- Endpoints need to support SCTP (with dynamic control of IP addresses)
- Signalling to every correspondent node necessary (for every established SCTP association)
  - for high number of parallel connections, large signalling volume over air interface
- Dynamic Naming Service for connection set-up from CN required (to establish the initial SCTP association)
  - Dynamic DNS
  - Other location mechanisms (e.g. based on SIP URLs)
- Only usable for traffic without real-time requirements (due to SCTP flow/congestion control)
  - but similar approaches, e.g. for RTP, possible
- Simultaneous Handover (Mobile Node and Correspondent Node) can lead to loss of connection

**Session Initiation Protocol -- SIP**

SIP: Application layer signalling protocol (RFC 3261)

- Provides call control for multi-media services
  - initiation, modification, and termination of sessions
  - terminal-type negotiation and selections
  - call holding, forwarding, forking, transfer
  - media type negotiation (also mid-call changes)
    - using Session Description Protocol (SDP)
- Properties
  - Independent of transport protocols (TCP, UDP, SCTP,...)
  - ASCII format SIP headers
  - Separation of call signalling and data stream

**Basic Messages (Methods)**

- **INVITE**: initiate call
- **ACK**: confirm final response (after 'invite')
- **BYE**: terminate call
- **CANCEL**: cancel pending requests
- **OPTIONS**: queries features supported by other side
- **REGISTER**: register with location service

**Responses**

- 1xx Intermediate results
e.g. *180 Ringing*
- 2xx Successful Responses
  - e.g. *200 OK*
- 3xx Redirections
  - e.g. *302 Moved Temporarily*
- ...
SIP Call Signalling: Example

SIP: Mobility support

User/Session/Application Mobility (change of terminal)
- Registration via SIP ‘REGISTER’
- Initial connection set-up between MN1 and CN through ‘INVITE’
- mid-session mobility (application mobility): call transfer, SIP method ‘REFER’ (RFC3515)
- Application state could be contained in the message body (‘proprietary’ extension)

Host Mobility (change of IP address)
- Pre-call: re-register, routing of ‘INVITE’ based on SIP-URL
- mid-call: re-invite
Summary

1. **Background**: IP, IETF, Mobility & Handover Types
2. **Mobile IP (v4)**: Motivation, Principles, Messages, DHCP
3. **MIP Performance** aspects & improvements: HMIP, HAWAII, CIP
4. **MIP Extensions**: Security Aspects (Authentication, Firewall Traversal), Multi-homing/flow mobility, IPv6 and MIPv6
5. **Mobility support on higher layers**: Transport Layer Mobility, Session Initiation Protocol (SIP)

**Approaches**:  
- Separation of host identifier and location identifier  
- Tunnelling  
- Soft-state  
- Performance optimisations: hierarchical/hybrid approaches  
- [Security requirements and solutions (MACs, encryption, sequence numbers, timestamps, nonces)]

**Key Technologies/Protocols**:  
(see left column)

---

Outlook: research topics, IP Mobility

- Network Mobility  
- Application Mobility (SIP method 'refer'?)  
- Mobility and QoS (IETF WG NSIS)  
- Cross layer optimization (L2 triggers, …)  
- MIP and NAT/FW  
- Location-based services and location privacy  
- ‘all IP’ mobile networks
Outlook: Host Identity Protocol (HIP)

- Underlying ideas for mobility support
  - Separate host identifier (HI, 'name') and locator ('IP address')
  - Dynamic name service or rendezvous server for pre-session mobility
  - Update of mapping of host identifier → locator at handovers
  - Mechanism works between transport and network layer: additional HIP header as IPv6 extension header
- In combination with security mechanisms
  - Host Identity Name space based on public keys
  - Hash of HI → 128bit Host Identity Tag attached to packets
  - 4-packet basic exchange (cookies, Diffie-Hellman Key Exchange)

References

- IETF Working groups (see also for RFCs and drafts):
  - Others: nemo, mip4, dhcp, seamoby
- Seok Joo Koh, 'mSCTP: Use of SCTP for IP Mobility Support', Presentation, IT Forum, Korea, 2003
Acknowledgements

- Lecture notes: Mobile Communications, Jochen Schiller, [www.jochenschiller.de](http://www.jochenschiller.de)
- Student work (TU Munich, AAU)
  - Stefan Rank (Master Thesis)
  - Michael Zech (Seminar)
  - Krasimir Dzhigovechki (Seminar)
  - Wolfgang Thomas (Seminar)
  - Rui Martins (Master Thesis)
- Lecture notes: Wireless communication protocols (R. Prasad, TKM)
- Tutorial: IP Technology in 3rd Generation mobile networks, Siemens AG (J. Kross, L. Smith, H. Schwefel)