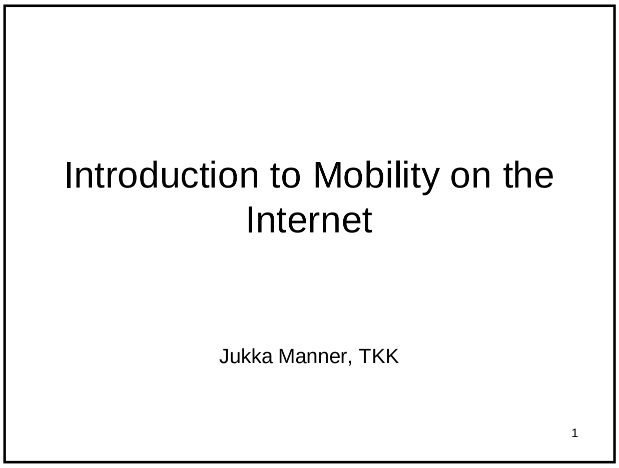
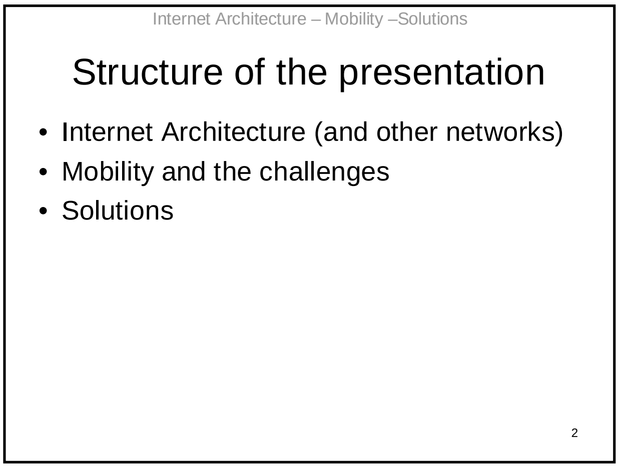


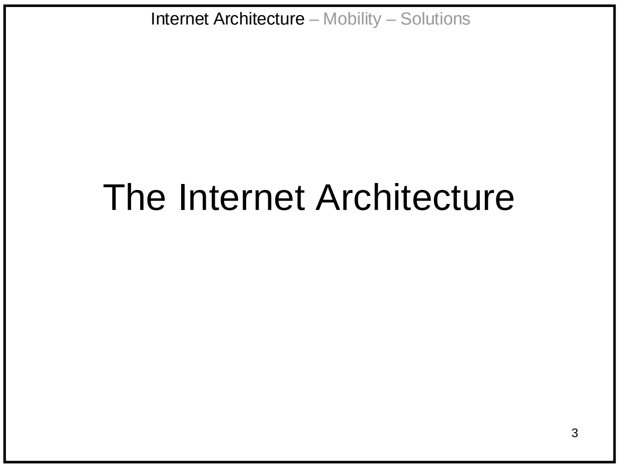
Introduction to Mobility on the Internet

Jukka Manner, TKK

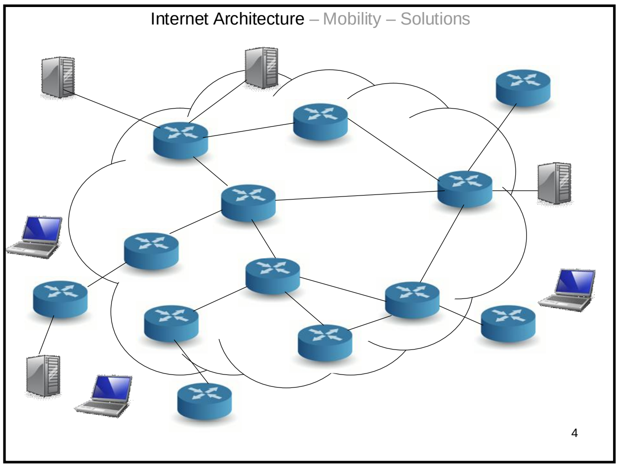


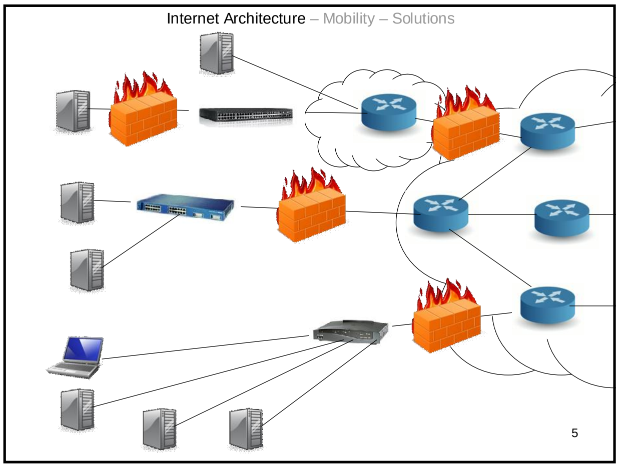
Structure of the presentation

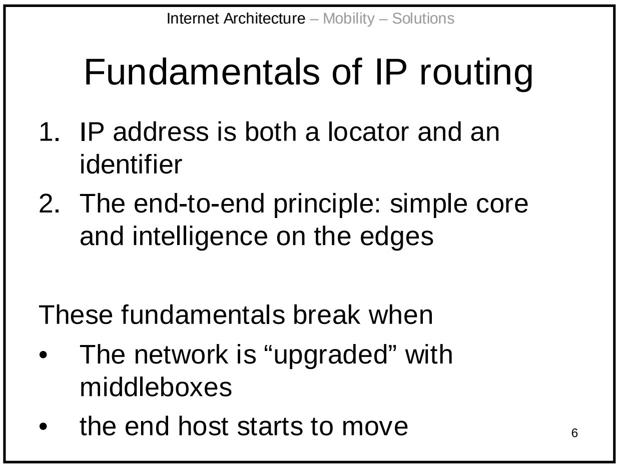
- Internet Architecture (and other networks)
- Mobility and the challenges
- Solutions



The Internet Architecture





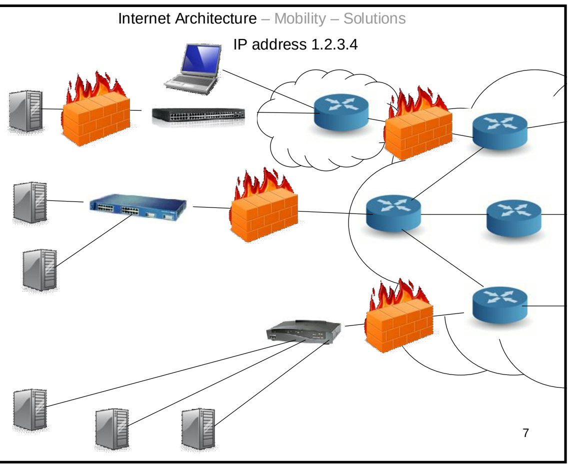


Fundamentals of IP routing

1. IP address is both a locator and an identifier
2. The end-to-end principle: simple core and intelligence on the edges

These fundamentals break when

- The network is “upgraded” with middleboxes
- the end host starts to move



Trust

- A further “problem” of the early Internet was mutual trust
- There was great joy in networking
  - Users trusted each other
  - Nodes could trust each other
  - Anyone doing harm would be identified
- This is no longer the case, and it has consequences on IP mobility, too

Ad-hoc networks

- Networks of equal nodes, moving around
- Wireless links, battery powered
- Dynamic topologies (very)
- Nodes route each others packets
- May have Internet connectivity
- Challenge: ability to route packets
- Examples: soldiers in battle field, fire fighters, cars

Sensor networks

- Small devices mainly used for sensing the environment
- Very limited processing power, battery, connectivity
- Typically more stable topologies
- An order of magnitude larger networks
- Challenge: power saving of the network
- Examples: sensors in agriculture, cities

Mobility

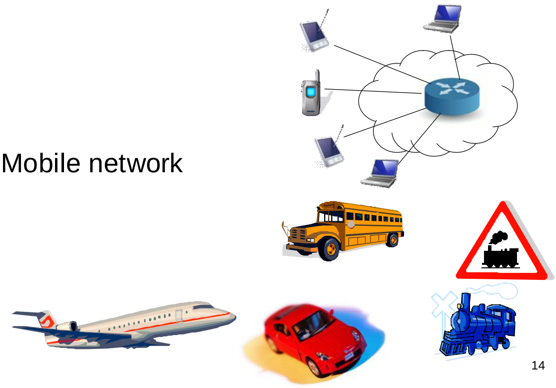
Mobility

What moves?

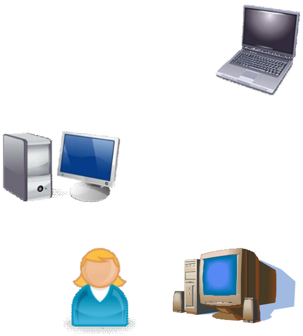
Mobile end-host

(what people usually think about)

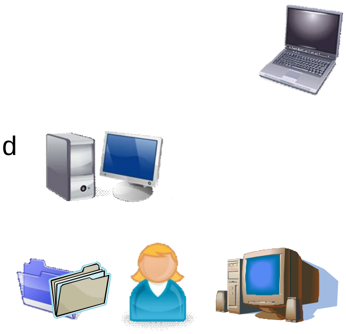
Mobile network



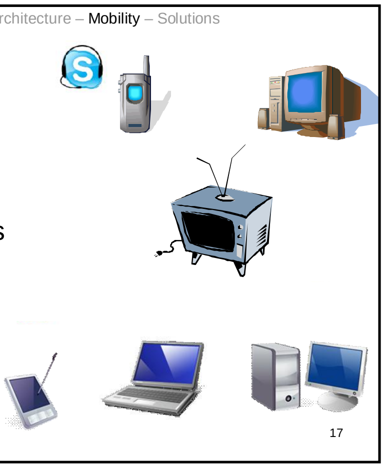
User moves



User’s profiles and files move



A session moves



Mobile applications

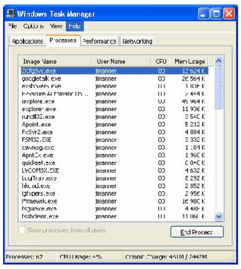


Image Name	User Name	CPU	Mem Usage
ZCfgSvc.exe	jmanner	00	13 624 K
googletalk.exe	jmanner	00	26 564 K
exshowWh.exe	jmanner	00	1 836 K
F-Secure Automatic Up...	jmanner	00	2 444 K
iexplore.exe	jmanner	00	45 964 K
explorer.exe	jmanner	00	11 936 K
rundll32.exe	jmanner	00	3 540 K
Apoint.exe	jmanner	00	5 212 K
FxSvr2.exe	jmanner	00	4 884 K
FSM32.EXE	jmanner	00	3 332 K
cswmsg.exe	jmanner	00	1 104 K
ApntEx.exe	jmanner	00	1 960 K
quickset.exe	jmanner	00	6 040 K
LVCOMSX.EXE	jmanner	00	4 632 K
LogiTray.exe	jmanner	00	8 292 K
hkcmd.exe	jmanner	00	2 852 K
igfxpers.exe	jmanner	00	2 956 K
IFrmewrk.exe	jmanner	00	16 980 K
fsguiexe.exe	jmanner	00	4 488 K
fsshclient.exe	jmanner	00	11 060 K

□ Show processes from all users

Processes: 67 CPU Usage: 4% Commit Charge: 451M / 2442M

Moving entities on the Internet

- End host,
- A network,
- A user,
- A session,
- Personal files and profiles, or
- An application process

Two primary questions

1. How does the mobility affect IP addresses?
2. Is the address topologically correct?

What must be updated?

1. *When* can mobility happen
   - Before a communication session, or
   - During the session?
2. *Where* is this movement happening
   - *local* to an administrative domain,
   - or Internet wide (*global*)?
3. *What* is the network like?

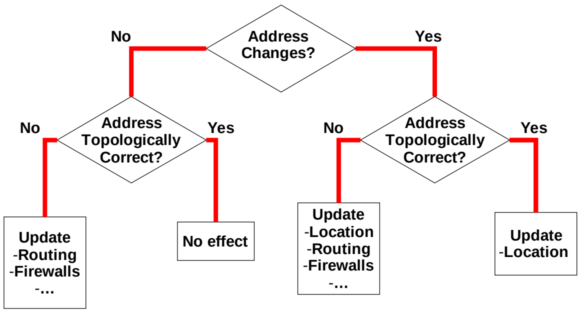
When and Where

- If mobility can happen only *before* a communication is initiated, mobility only requires a location service to be maintained and updated.
- Example: User mobility, I change devices and register my new location, e.g., to an IM service.

When and Where

- If mobility can happen *during* a session, we need to either
  - *Hide* the mobility from other nodes, or
  - *Update* our location information with them.
- Other nodes may include:
  - Our communication partners
  - Routers (local, global)
  - Home network location service

IP mobility diagram



Address Changes?

No

Yes

Address Topologically Correct?

No

Yes

Update -Routing -Firewalls -…

No effect

Address Topologically Correct?

No

Yes

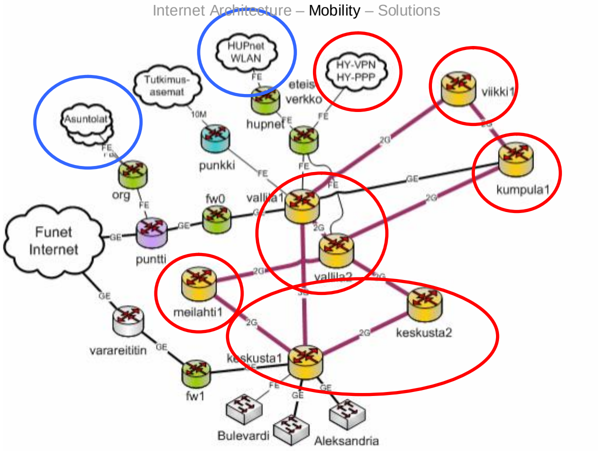
Update -Location -Routing -Firewalls -…

Update -Location

What is the network like?

- Is the network
  - built with link layer technologies, or
  - Is it a full-blown IP network?
- For example, GSM, 3G, WLAN, WiMAX, and other similar networks will effectively hide the mobility from the IP layer.
- The only effect will be a sudden break in the connectivity (which may be interpreted as congestion by IP transport protocols)

VIIKKI
KUMPULA
VALLILA
MEILAHTI
KLUUVI
KRUUNUNHAKA
KAMPPI



Some challenges

- How can the other nodes trust my new location to be real?
- Does the location matter?
- How about my privacy (location tracking)?
- How to do these updates fast?
- Which nodes must be upgraded to support my mobility?

Deployment?

- An important question to ask when designing mobility schemes: what nodes must be upgraded, e.g.,
  - Mobile client devices
  - Correspondent nodes (user devices, servers)
  - Visiting access network routers
  - Home access network nodes
  - Backbone routers
  - DNS and other infrastructure services

Solutions

Fundamental problems

- All solutions to IP mobility are often unnecessary complex
- One reason is the dual meaning of IP addresses:
  1. Identifier of the recipient node
  2. Information for routing the packet, location of the node in the topology
- Signalling performance is a challenge
- Security is a major practical problem

Solutions

- There exists tens (100s?) of solutions:
  - For global end-to-end mobility
  - Localized mobility within a single network
  - Faster handover schemes
  - Alternatives to the identifier/locator issue
  - Ad-hoc and sensor network routing
  - User mobility

Solutions: Global mobility

- The most well-known and popular scheme is *Mobile IP*
- The first specifications date from the mid 90's
- There are separate designs for IPv4 and v6
- Mobile IP provides constant mobility and across domains
- There also exist schemes, e.g., based on DNS updates

Solutions: Mobile IPv4

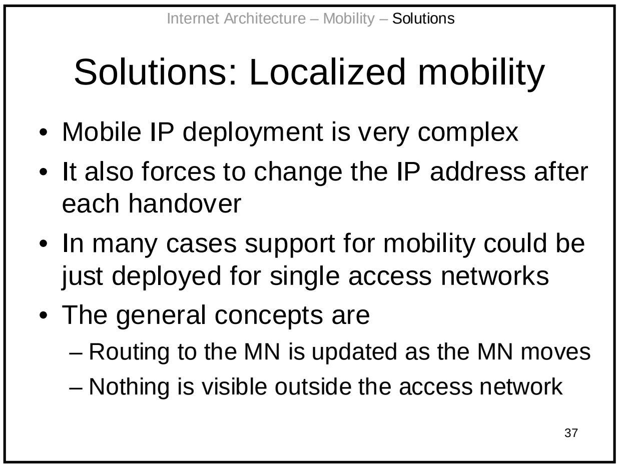
- Architecture based on three components:
  - Mobile Node (MN)
  - Home Agent (HA) in the home network
  - Foreign Agent (FA) to support visiting MNS
- When MN moves, it registers its new IP address with its own HA
- HA then tunnels packets to the FA or MN
- Packets from MN go directly or via HA

Solutions: Mobile IPv6

- Basic principle is similar to Mobile IPv6
- Most differences:
  - Supports route optimization
  - No need for Foreign Agents
  - Uses IPv6 functions, e.g., ND
  - Uses IPv6 header extensions instead of tunneling

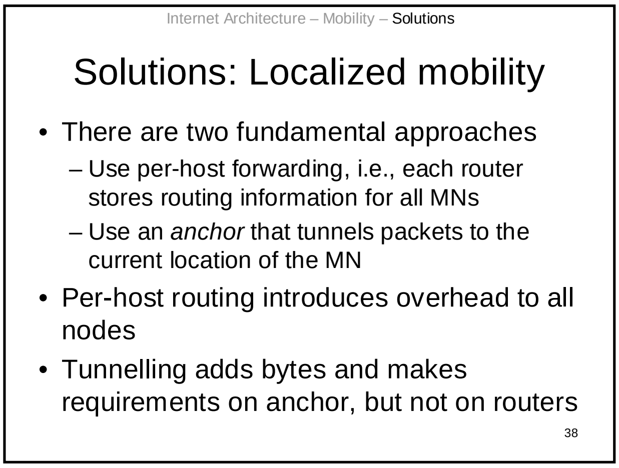
Solutions: NEMO

- Basic MIP solves end-host mobility
- A whole network could also move
- NEMO is a solution based on Mobile IPv6
- A *Mobile Router* (MR) communicates with a home agent as the network moves
- The nodes inside the network do not see the mobility
- MR and HA have a bi-directional tunnel



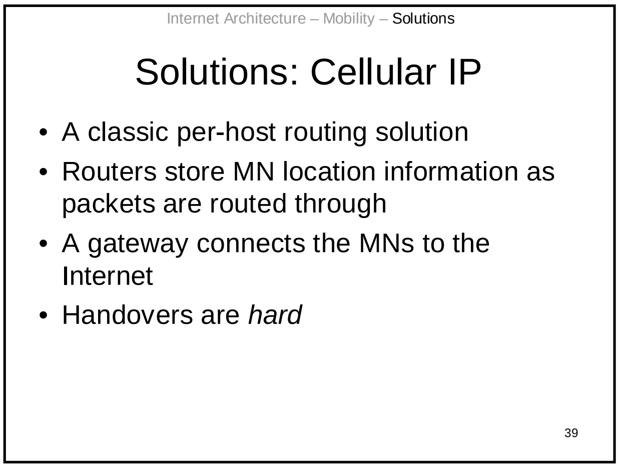
Solutions: Localized mobility

- Mobile IP deployment is very complex
- It also forces to change the IP address after each handover
- In many cases support for mobility could be just deployed for single access networks
- The general concepts are
  - Routing to the MN is updated as the MN moves
  - Nothing is visible outside the access network



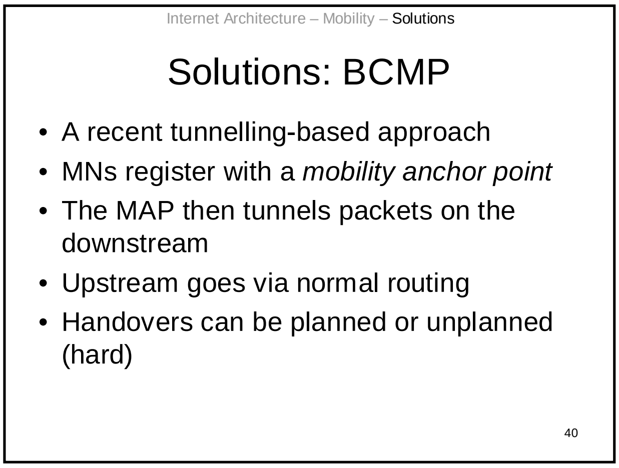
Solutions: Localized mobility

- There are two fundamental approaches
  - Use per-host forwarding, i.e., each router stores routing information for all MNs
  - Use an *anchor* that tunnels packets to the current location of the MN
- Per-host routing introduces overhead to all nodes
- Tunnelling adds bytes and makes requirements on anchor, but not on routers



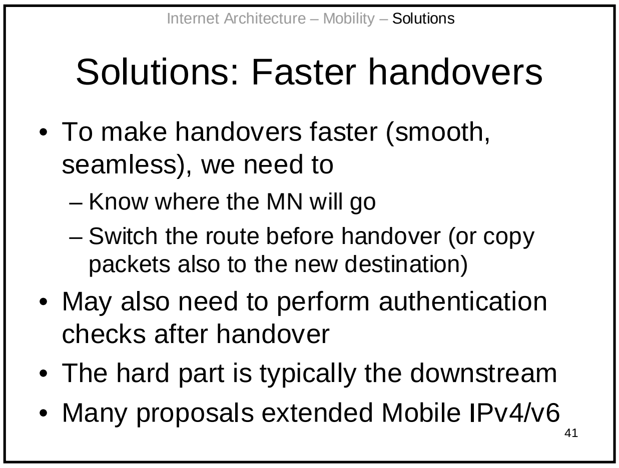
Solutions: Cellular IP

- A classic per-host routing solution
- Routers store MN location information as packets are routed through
- A gateway connects the MNs to the Internet
- Handovers are *hard*



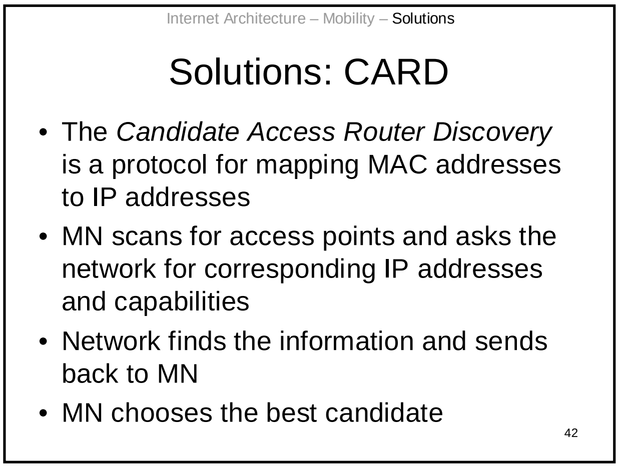
Solutions: BCMP

- A recent tunnelling-based approach
- MNs register with a *mobility anchor point*
- The MAP then tunnels packets on the downstream
- Upstream goes via normal routing
- Handovers can be planned or unplanned (hard)



Solutions: Faster handovers

- To make handovers faster (smooth, seamless), we need to
  - Know where the MN will go
  - Switch the route before handover (or copy packets also to the new destination)
- May also need to perform authentication checks after handover
- The hard part is typically the downstream
- Many proposals extended Mobile IPv4/v6



Solutions: CARD

- The *Candidate Access Router Discovery* is a protocol for mapping MAC addresses to IP addresses
- MN scans for access points and asks the network for corresponding IP addresses and capabilities
- Network finds the information and sends back to MN
- MN chooses the best candidate

Solutions: CTP

- The *Context Transfer Protocol* allows an MN to provide different context information to a new access router (AR)
  - The MN can ask the current AR to send the information to the new AR, or
  - After handover the MN tells the new AR where the information is available (old AR)
- Context can be e.g. security information, header compression, QoS, multicast group

Solutions: ID/Locator split

- The problem with IP mobility is that the IP address is used as an identifier
- When the IP address changes after movement, the identifier changes, too
- This causes problems with authentication and security protocols
- An important feature would be to separate routing and node identifiers

Solutions: ID/Locator split

- There exists many proposals that aim at adding a new identifier to communication
- This identifier should be cryptographically generated, i.e., easily verified
- IP addresses would then be used just for packet routing
- When the IP address changes, the receiver just verifies the “other” identifier

Solutions: HIP

- The *Host Identity Payload* (HIP) is one solution to the problem
- It adds an identifier to all IP packets
- The *Host Identity Tag* (HIT) is based on a nodes public key
- Packet content is also encrypted with IPsec ESP
- Provides secure communication through IP address changes

Solutions: i3

- The *Internet Indirection Infrastructure* is essentially a rendez-vous based approach
- It uses a proxy-like scheme, where packets are sent to a well-known *identifier*
- Nodes register theirs identifiers with the infrastructure
- The infrastructure receives the packets and sends them to the current location
- The location can be updated any time

Solutions: Ad-hoc networks

- Routing in ad-hoc networks is very challenging
  - The topology and routes change all the time
  - Nodes can enter and leave any time
- Keeping up-to-date routing paths is difficult
- We also must optimize the signalling to minimize overhead
- Routing loops must be avoided

Solutions: Ad-hoc networks

- There are two primary solutions
  - Reactive, on-demand protocols: routes are queries when packets need to be sent
  - Proactive, table-driven protocols: routes are set up and updated constantly in the background
- The overheads of these schemes depend very much on the network dynamics and amount of traffic

Solutions: AODV

- The *Ad-hoc On-demand Distance Vector* is a classic on-demand protocol
- Sends broadcast messages through the network to find a packet destination
- Routes are then built and the sender can choose the most optimal route

Solutions: OLSR

- The *Optimized Link State Routing* protocol is based on periodic dissemination of topology information
- Nodes tell who they can route to
- This information is used by senders to calculate a good route to the destination
- OLSR signaling messages are sent between *Multipoint Relays*
- This minimizes the signaling overhead

Solutions: User mobility

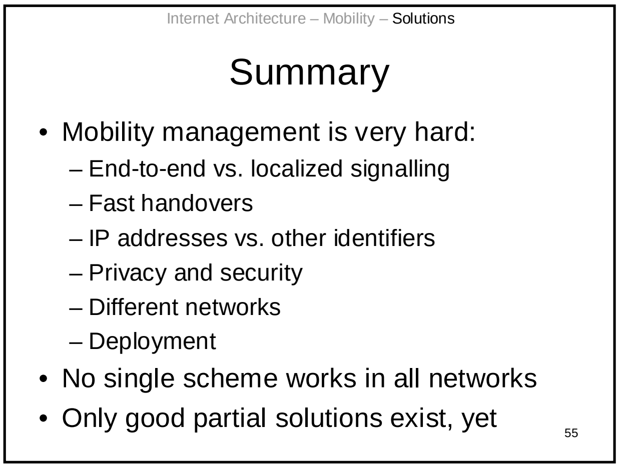
- The previous solutions were meant for device mobility
- A user could also move in the network, e.g., change devices
- Currently, the only viable solution is the *Session Initiation Protocol* (SIP)

Solutions: User mobility

- SIP provides control signalling primarily for multimedia sessions, including messaging
- Message forwarding is based on an overlay network of SIP servers
- The initiator sends an INVITE towards the recipient
- The recipient answers if it wants to start the communication

Solutions: User mobility

- The SIP *REFER* message can be used to move a session to another location
- It can be
  - The same device with a new IP address, or
  - A completely physically separate device, i.e., a call transfer as in the PSTN



Summary

- Mobility management is very hard:
  - End-to-end vs. localized signalling
  - Fast handovers
  - IP addresses vs. other identifiers
  - Privacy and security
  - Different networks
  - Deployment
- No single scheme works in all networks
- Only good partial solutions exist, yet