Wireless Networks: Network Protocols/Mobile IP

- Motivation
- Data transfer
- Encapsulation
- Security
- IPv6
- Problems
- DHCP
- Ad-hoc networks
- Routing protocols

Adapted from J. Schiller, "Mobile Communications"

Motivation for Mobile IP

Routing
- based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
- change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems?
- change of all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address?
- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take too much time
- TCP connections break, security problems

Requirements to Mobile IP (RFC 2002)

Transparency
- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- 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

Terminology

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

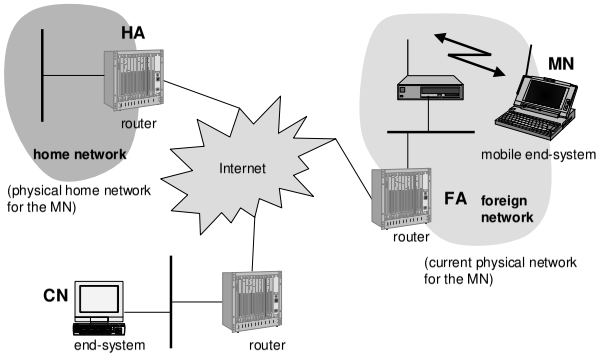
Home Agent (HA)
- system in the home network of the MN, typically a router
- registers the location of the MN, tunnels IP datagrams to the COA

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

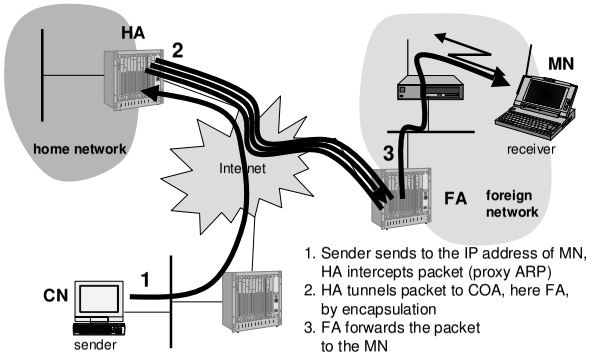
Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view
- can be chosen, e.g., via DHCP

Correspondent Node (CN)
- communication partner

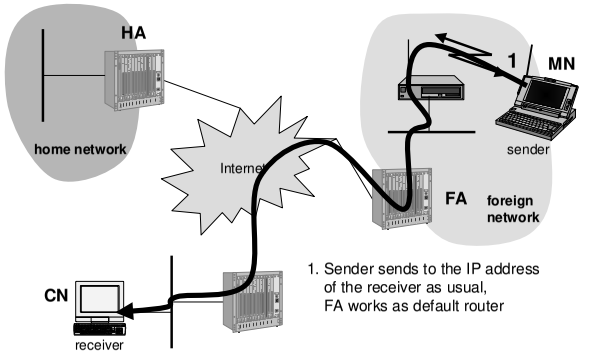
Example network



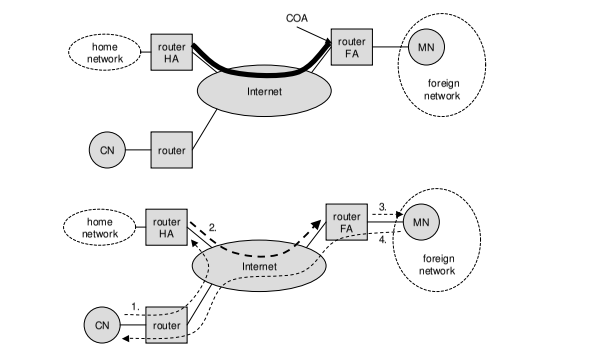
Data transfer to the mobile system



Data transfer from the mobile system



Overview



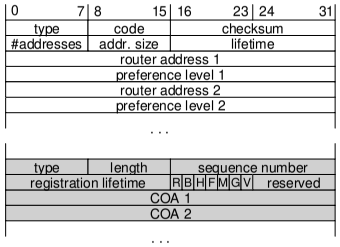
Network integration

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 (standard case for home network)
- MN reads a COA from the FA advertisement messages

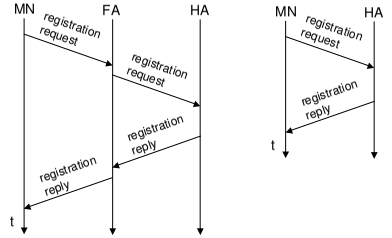
Registration (always limited lifetime!)
- MN signals COA to the HA via the FA, HA acknowledges via FA to MN
- these actions have to be secured by authentication

Advertisement
- 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

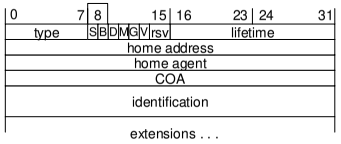
Agent advertisement



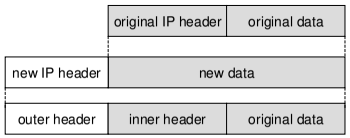
Registration



Mobile IP registration request



Encapsulation



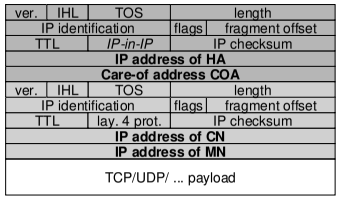
Encapsulation I

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 in RFC 2003)

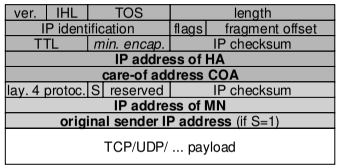
- tunnel between HA and COA



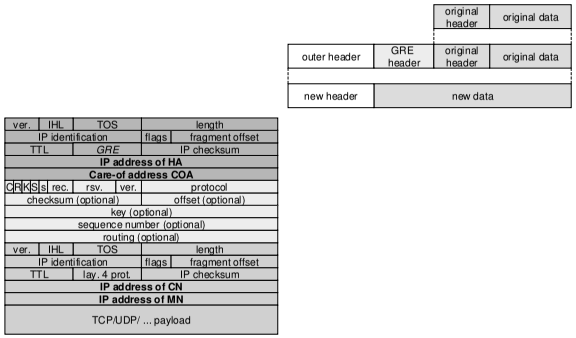
Encapsulation II

Minimal encapsulation (optional) [RFC2004]

- avoids repetition of identical fields
- e.g. TTL, IHL, version, TOS
- only applicable for unfragmented packets, no space left for fragment identification



Generic Routing Encapsulation [RFC 1701]



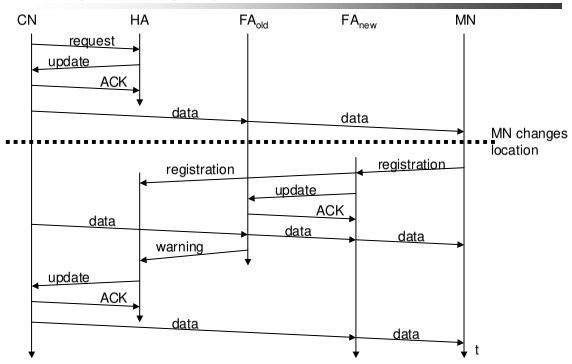
Optimization of packet forwarding

Triangular Routing
- sender sends all packets via HA to MN
- higher latency and network load

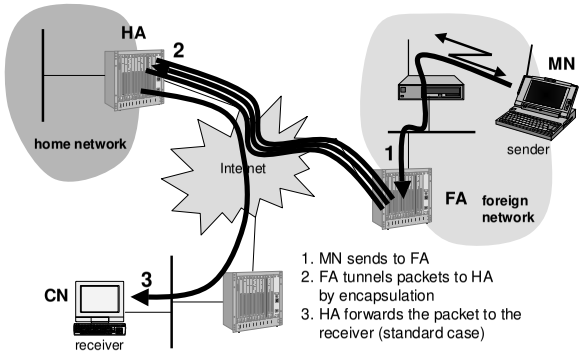
"Solutions"
- sender learns the current location of MN
- direct tunneling to this location
- HA informs a sender about the location of MN
- big security problems!

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

Change of foreign agent



Reverse tunneling (RFC 2344)



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 to 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)

The new standard is backwards compatible
- the extensions can be implemented easily and cooperate with current implementations without these extensions

Mobile IP and IPv6

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols

- security is integrated and not an add-on, authentication of registration is included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address autoconfiguration
- no need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
- „soft" hand-over, i.e. without packet loss, between two subnets is supported
  - MN sends the new COA to its old router
  - the old router encapsulates all incoming packets for the MN and forwards them to the new COA
  - authentication is always granted

Problems with mobile IP

Security

- authentication with FA problematic, for the FA typically belongs to another organization
- no protocol for key management and key distribution has been standardized in the Internet
- patent and export restrictions

Firewalls

- typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)

QoS

- many new reservations in case of RSVP
- tunneling makes it hard to give a flow of packets a special treatment needed for the QoS

Security, firewalls, QoS etc. are topics of current research and discussions!

Security in Mobile IP

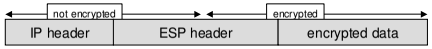
Security requirements (Security Architecture for the Internet Protocol, RFC 1825, RFC 1826, RFC 1827)

- Integrity
  any changes to data between sender and receiver can be detected by the receiver
- Authentication
  sender address is really the address of the sender and all data received is really data sent by this sender
- Confidentiality
  only sender and receiver can read the data
- Non-Repudiation
  sender cannot deny sending of data
- Traffic Analysis
  creation of traffic and user profiles should not be possible
- Replay Protection
  receivers can detect replay of messages

IP security architecture I

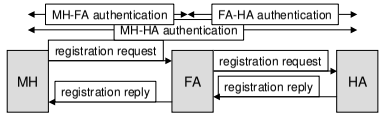
- Two or more partners have to negotiate security mechanisms to setup a security association
  - typically, all partners choose the same parameters and mechanisms
- Two headers have been defined for securing IP packets:
  - Authentication-Header
    - guarantees integrity and authenticity of IP packets
    - if asymmetric encryption schemes are used, some non-repudiation level can also be provided

  - Encapsulation Security Payload
    - protects confidentiality between communication partners



IP security architecture II

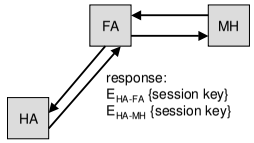
- Mobile Security Association for registrations
  - parameters for the mobile host (MH), home agent (HA), and foreign agent (FA)
- Extensions of the IP security architecture
  - extended authentication of registration



  - prevention of replays of registrations
    - time stamps: 32 bit time stamps + 32 bit random number
    - nonces: 32 bit random number (MH) + 32 bit random number (HA)

Key distribution

Home agent distributes session keys



- foreign agent has a security association with the home agent
- mobile host registers a new binding at the home agent
- home agent answers with a new session key for foreign agent and mobile node

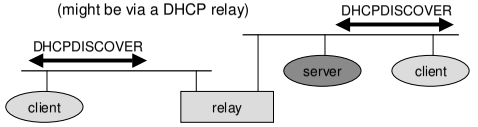
DHCP: Dynamic Host Configuration Protocol [RFC 2131]

Application

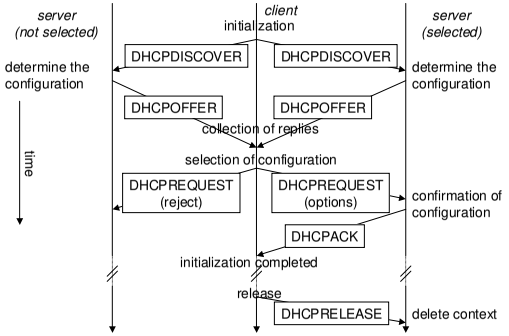
- simplification of installation and maintenance of networked computers
- supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
- enables automatic integration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP

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



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
- 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 yet

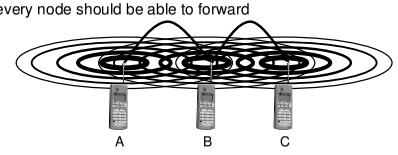
<draft-ietf-dhc-authentication-16.txt:2001>

Ad hoc networks

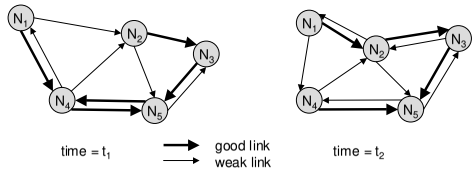
Standard Mobile IP needs an infrastructure
- Home Agent/Foreign Agent in the fixed network
- DNS, routing etc. are not designed for mobility

Sometimes there is no infrastructure!
- remote areas, ad-hoc meetings, disaster areas
- cost can also be an argument against an infrastructure!

Main topic: routing
- no default router available
- every node should be able to forward



Routing examples for an ad-hoc network



Traditional routing algorithms

Distance Vector
- periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
- selection of the shortest path if several paths available

Link State
- periodic notification of all routers about the current state of all physical links
- router get a complete picture of the network

Example
- ARPA packet radio network (1973), DV-Routing
- every 7.5s exchange of routing tables including link quality
- updating of tables also by reception of packets
- routing problems solved with limited flooding

Problems of traditional routing algorithms

Dynamic of the topology
- frequent changes of connections, connection quality, participants

Limited performance of mobile systems
- periodic updates of routing tables need energy without contributing to the transmission of user data, sleep modes difficult to realize
- limited bandwidth of the system is reduced even more due to the exchange of routing information
- links can be asymmetric, i.e., they can have a direction dependent transmission quality

Problem
- protocols have been designed for fixed networks with infrequent changes and typically assume symmetric links

DSDV (Destination Sequenced Distance Vector)

Routing Protocols: DSDV

Destination-Sequenced Distance Vector:
- Each node maintains a routing table listing:
  <dest, next-hop, metric, SeqNum>:
  The favored route is changed if a new route with higher SeqNum is received, or if the new route has equal SeqNum and lower metric
- Nodes send advertisement with evenly increased SeqNum
- When a node detects a broken link he sends an advertisement with ∞ metric and SeqNum=PrevSeqNum+1
- Damping fluctuations:
  - Fluctuations are due to out-of-order arrival of route advertisement
  - Proposed solution: maintain a settling time estimation for routes
  - Route with an ∞ metric are advertised without delay

Dynamic source routing I <draft-ietf-manet-dsr-05.txt:2001>

Split routing into discovering a path and maintaining a path

Discover a path
- only if a path for sending packets to a certain destination is needed and no path is currently available

Maintaining a path
- only while the path is in use, one has to make sure that it can be used continuously

No periodic updates needed!

Dynamic source routing II

Path discovery
- broadcast a *Route Request* packet with destination address and unique ID
- if a station receives a broadcast packet
  - if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet): *Route Reply*
  - if the packet has already been received earlier (identified via ID) then discard the packet
  - otherwise, append own address and broadcast packet
- sender receives packet with the current path (address list)

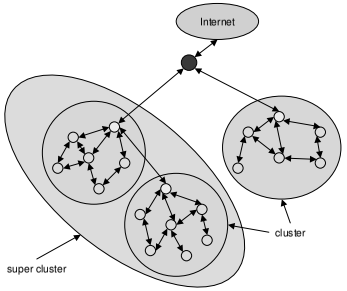
Optimizations
- limit broadcasting if maximum diameter of the network is known
- caching of address lists (i.e. paths) from passing packets (overhearing)
  - stations can use the cached information for path discovery (own paths or paths for other hosts)

Dynamic Source Routing III

Maintaining paths

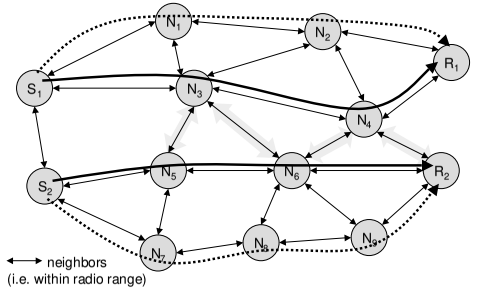
- after sending a packet
  - wait for a layer 2 acknowledgement (if applicable)
  - listen into the medium to detect if other stations forward the packet (if possible)
  - request an explicit acknowledgement
- if a station encounters problems it can inform the sender of a packet or look-up a new path locally

Clustering of ad-hoc networks



Interference-based routing

Routing based on assumptions about interference between signals



Examples for interference based routing

Least Interference Routing (LIR)

- calculate the cost of a path based on the number of stations that can receive a transmission

Max-Min Residual Capacity Routing (MMRCR)

- calculate the cost of a path based on a probability function of successful transmissions and interference

Least Resistance Routing (LRR)

- calculate the cost of a path based on interference, jamming and other transmissions

LIR is very simple to implement, only information from direct neighbors is necessary