

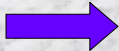
Course Overview

- Introduction
- Data in Wireless Cellular Systems
- Data in Wireless Local Area Networks
- **Internet Protocols**
- TCP over Wireless Link
- Ad-Hoc Networks, Sensor Networks
- Services and Service Discovery
- System Support for Mobile Applications

What is TCP/IP ?

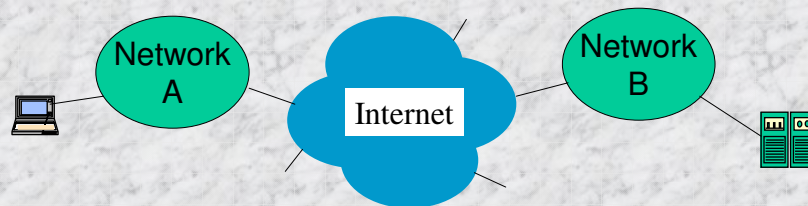
- TCP/IP is a collection of protocols that facilitates communications among servers and terminals that are hooked to different networks

TCP  Transport Control Protocol

IP  Internet Protocol

What is TCP/IP ? (continue)

- The TCP and IP are only two of several protocols, but the name stuck !!
- They are the most important ones



The Big Picture of TCP/IP

Application (Host-to-Host)	Ping	Telnet	FTP	SMTP	SNMP	Trace Route
	DNS	TFTP	BOOTP	RIP	OSPF	others
Transport	TCP		UDP		ICMP	
Network	IP					
Data Link	LLC		HDLC		PPP	
	Ethernet	802.3t	X.25	Token Ring	Frame Relay	ATM SMDS Etc.
Physical	Fiber Optics		UTP	Coaxial	Satellite	STP

- The most familiar Internet applications are
 - File Transfer (e.g. FTP)
 - Interactive request/response applications (e.g. Telnet)
 - Electronic mail (e.g. SMTP)



IETF: Internet Engineering Task Force

- Who develops protocols such as TCP/IP, Mobile IP, ...?
 - “standardized” by action of IETF
- IETF has over 70 *working groups* considering a broad range of protocol proposals for the Internet, tries to identify protocol needs in advance (?)
- IETF works with Internet Assigned Number Authority (IANA) to keep track of protocol number assignments and address allocations as required by various Internet protocols
- each protocol specified by a “Request for Comments”
 - working groups develop new RFCs by publishing Internet Drafts, building prototypes, and encouraging public debate
 - operational model: rough consensus and running code

IP Addresses

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
Class A	0	Network ID							Host ID																								
Class B	1	0	Network ID													Host ID																	
Class C	1	1	0	Network ID																						Host ID							
Class D	1	1	1	0	Multicast Address																												
Class E	1	1	1	1	0	Reserved																											

class	# of Nets	# of hosts
A	127	16,777,214
B	16,384	66,534
C	1,097,152	254

IP Addresses and Physical Addresses

- Map IP addresses into physical addresses
 - destination host
 - next hop router
- Techniques
 - encode physical address in host part of IP address
 - table-based
- ARP
 - table of IP to physical address bindings
 - broadcast request if IP address not in table
 - target machine responds with its physical address
 - table entries are discarded if not refreshed

IPv6

- Extended addressing capabilities: 128-bit address field and other improvements.
- Simplified header format: Some fields of IPv4 are dropped or turned into options
- Improved support for extensions and options: flexibility and ability to introduce new options
- Flow labeling
- Authentication and privacy

Why Worry About Mobility?

- mobile computing is on the rise
 - wireless communications technologies widely available
 - IEEE 802.11 finally standardized
 - MAC layer protocol with lots of features: power saving, ad-hoc networking support, maybe even isochronous communication
 - cellular telephony everywhere
 - AMPS and CDPD
 - GSM
 - wireless indoor equipment (IR and RF)
 - people expect the same from both desktop and laptop
 - high-resolution color display
 - 200 MHz processor
 - multi-gigabyte disk
 - with a docking station, the laptop is the desktop

Why Worry about Mobility?

- wireless communication and powerful portable devices lead to new computing paradigms:
 - mobile computing
 - ubiquitous computing
 - nomadic computing
- at the same time, the Internet and in particular the Web, are growing exponentially
 - timely news (and lots of it), user-friendly(?), lots of pretty pictures (70%-80% of Internet traffic is WWW traffic)
 - the “Information Superhighway” is where people want to be
 - certainly strong support by national governments to build and maintain this infrastructure
 - mobile computing seen as “on-ramp” to this infrastructure

Where to Solve Mobility Problem

- What model of mobility
 - “nomadic clients”: DHCP or similar solutions enough
 - Truly mobile: need to keep connections alive WHILE moving
- Where in the protocol stack
 - IP is common glue, solve it once and for all at IP layer
 - BUT: may be in contradiction to end-to-end argument
 - Other solutions/proposals exists, such as TCP connection migration

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 to long time
 - TCP connections break, security problems

Requirements to Mobile IP (RFC 3344, was: 3220, was: 2002)

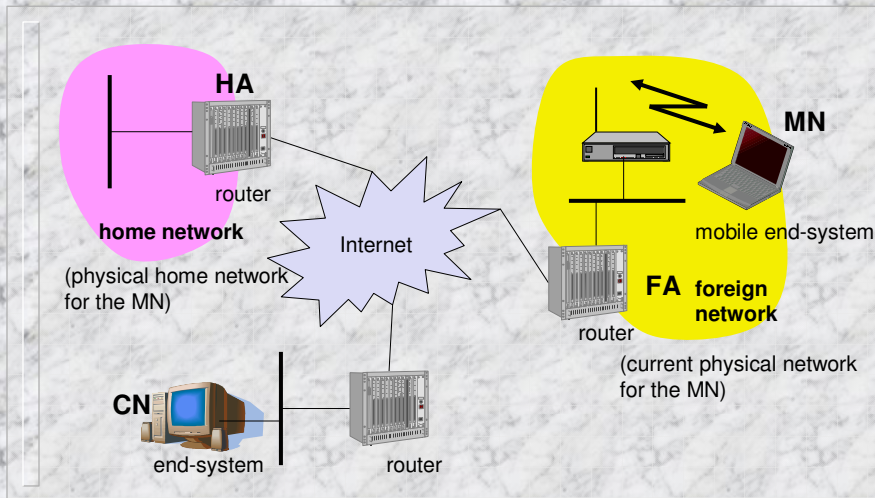
- Transparency
 - mobile end-systems keep their IP address
 - continuation of communication after interruption of link possible
 - point of connection to the fixed network can be changed
- Compatibility
 - support of the same layer 2 protocols as IP
 - no changes to current end-systems and routers required
 - 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

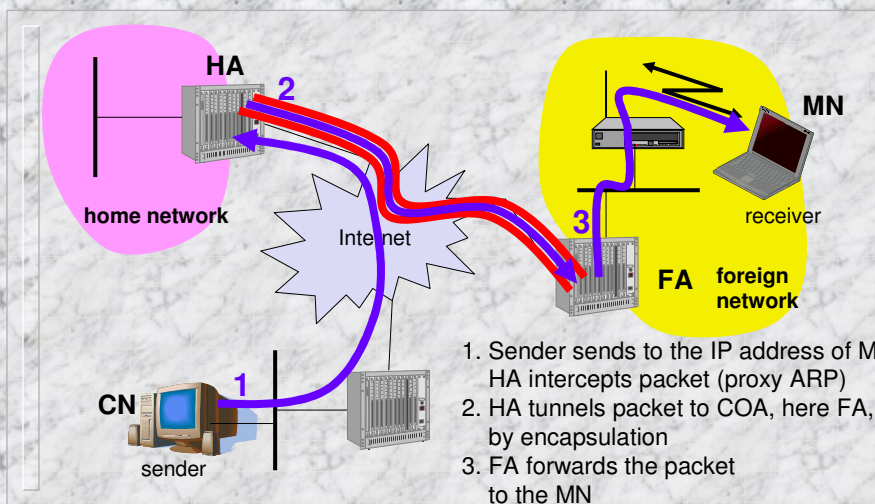
- Mobile Node (MN)
 - system (node) that can change the point of connection to the network without changing its IP address
- Home Agent (HA)
 - system in the home network of the MN, typically a router
 - registers the location of the MN, tunnels IP datagrams to the COA
- Foreign Agent (FA)
 - system 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



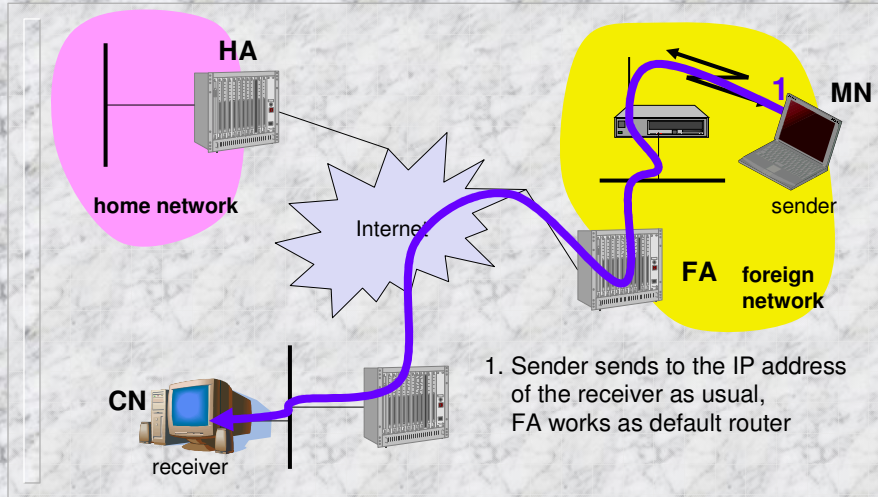
Data Transfer to the Mobile System



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



Data Transfer from the Mobile System



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

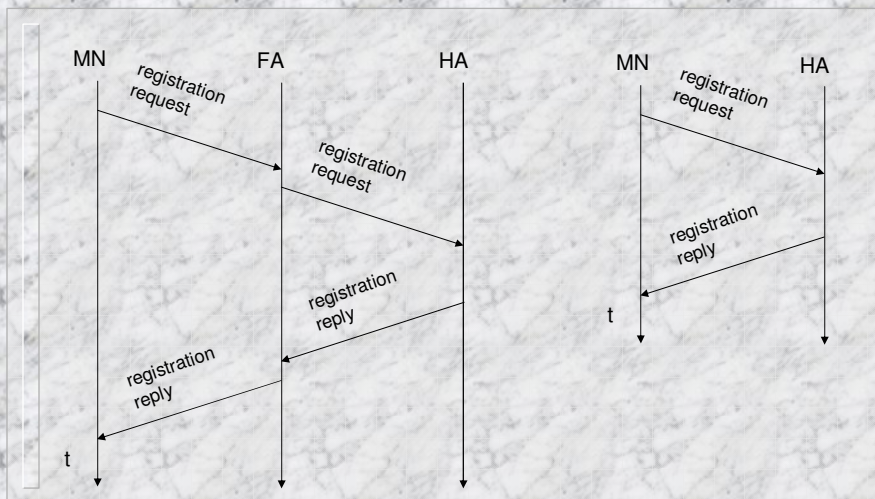
Agent Advertisement

type = 16
 length = 6 + 4 * #COAs
 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

0	7	8	15	16	23	24	31
type		code		checksum			
#addresses		addr. size		lifetime			
router address 1							
preference level 1							
router address 2							
preference level 2							
...							
type = 16		length		sequence number			
registration lifetime		R	B	H	F	M	G r T reserved
COA 1							
COA 2							



Registration



Mobile IP Registration Request

S: simultaneous bindings	0	7	8	15	16	23	24	31				
B: broadcast datagrams	type = 1		S	B	D	M	G	r	T	x	lifetime	
D: decapsulation by MN	home address											
M: minimal encapsulation	home agent											
G: GRE encapsulation	COA											
r: =0, ignored	identification											
T: reverse tunneling requested												
x: =0, ignored	extensions . . .											



Mobile IP Registration Reply

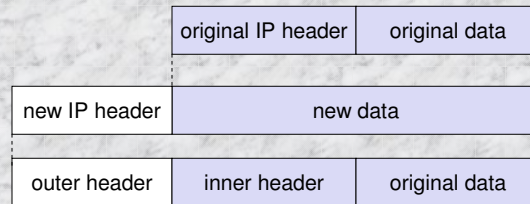
Example codes:

- registration successful
 - 0 registration accepted
 - 1 registration accepted, but simultaneous mobility bindings unsupported
- registration denied by FA
 - 65 administratively prohibited
 - 66 insufficient resources
 - 67 mobile node failed authentication
 - 68 home agent failed authentication
 - 69 requested Lifetime too long
- registration denied by HA
 - 129 administratively prohibited
 - 131 mobile node failed authentication
 - 133 registration Identification mismatch
 - 135 too many simultaneous mobility bindings

0	7	8	15	16	31
type = 3		code		lifetime	
home address					
home agent					
identification					
extensions					



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, RFC 2003)
 - tunnel between HA and COA

ver.	IHL	DS (TOS)	length	
IP identification		flags	fragment offset	
TTL	<i>IP-in-IP</i>		IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	DS (TOS)	length	
IP identification		flags	fragment offset	
TTL	lay. 4 prot.		IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ... payload				



Encapsulation II

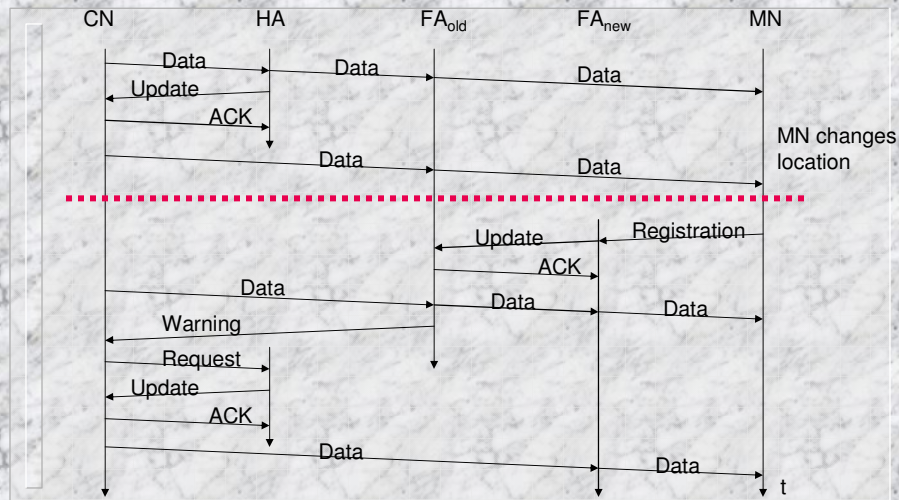
- Minimal encapsulation (optional)
 - avoids repetition of identical fields
 - e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
 - only applicable for unfragmented packets, no space left for fragment identification

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

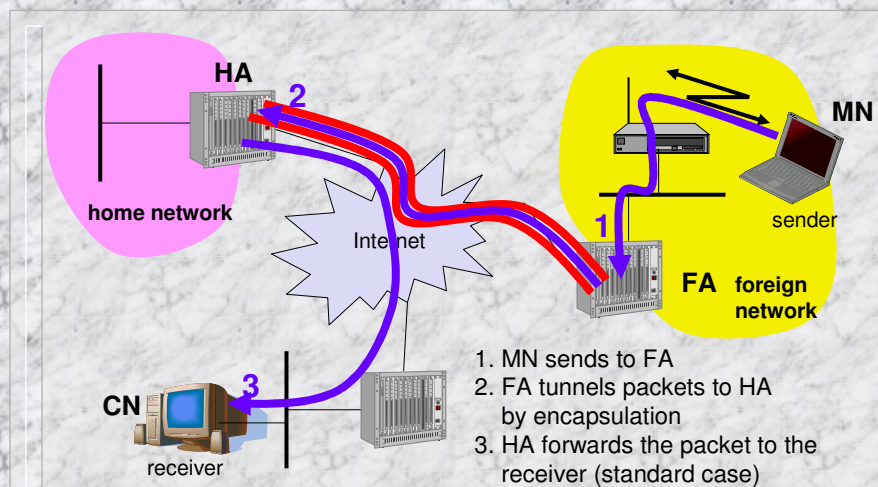
Optimization of Packet Forwarding

- 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 3024, was: 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 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)
- The standard is backwards compatible
 - the extensions can be implemented easily and cooperate with current implementations without these extensions
 - Agent Advertisements can carry requests for reverse tunneling

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; addresses are always co-located
 - 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!

IP Micro-Mobility Support

- Micro-mobility support:
 - Efficient local handover inside a foreign domain without involving a home agent
 - Reduces control traffic on backbone
 - Especially needed in case of route optimization
- Example approaches:
 - Cellular IP
 - HAWAII
 - Hierarchical Mobile IP (HMIP)
- Important criteria:
Security Efficiency, Scalability, Transparency, Manageability

Cellular IP

■ Operation:

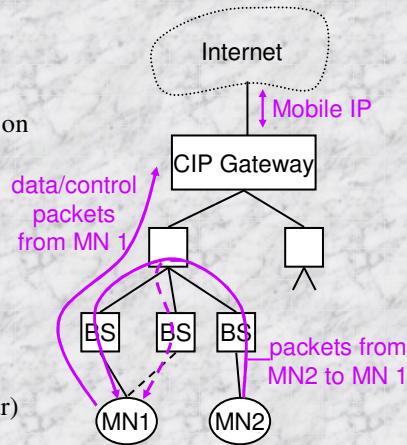
- „CIP Nodes“ maintain routing entries (soft state) for MNs
- Multiple entries possible
- Routing entries updated based on packets sent by MN

■ CIP Gateway:

- Mobile IP tunnel endpoint
- Initial registration processing

■ Security provisions:

- all CIP Nodes share „network key“
- MN key: MD5(net key, IP addr)
- MN gets key upon registration



Cellular IP: Evaluation

■ Advantages:

- Simple and elegant architecture
- Mostly self-configuring (little management needed)
- Integration with firewalls / private address support possible

■ Potential problems:

- Not transparent to MNs (additional control messages)
- Public-key encryption of MN keys may be a problem for resource-constrained MNs
- Multiple-path forwarding may cause inefficient use of available bandwidth

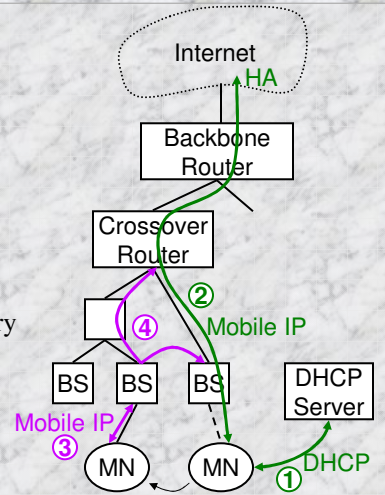
HAWAII

■ Operation:

- MN obtains co-located COA and registers with HA
- Handover: MN keeps COA, new BS answers Reg. Request and updates routers
- MN views BS as foreign agent

■ Security provisions:

- MN-FA authentication mandatory
- Challenge/Response Extensions mandatory



HAWAII: Evaluation

■ Advantages:

- Mostly transparent to MNs (MN sends/receives standard Mobile IP messages)
- Explicit support for dynamically assigned home addresses

■ Potential problems:

- Mixture of co-located COA and FA concepts may not be supported by some MN implementations
- No private address support possible because of co-located COA

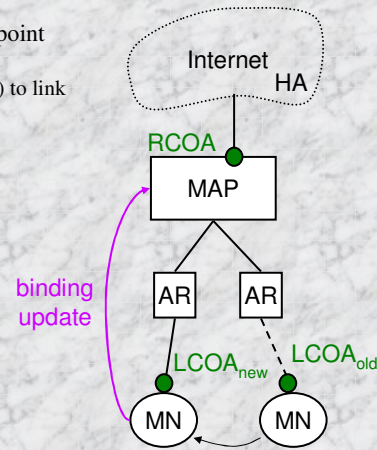
Hierarchical Mobile IPv6 (HMIPv6)

■ Operation:

- Network contains mobility anchor point (MAP)
 - mapping of regional COA (RCOA) to link COA (LCOA)
- Upon handover, MN informs MAP only
 - gets new LCOA, keeps RCOA
- HA is only contacted if MAP changes

■ Security provisions:

- no HMIP-specific security provisions
- binding updates should be authenticated



Hierarchical Mobile IP: Evaluation

■ Advantages:

- Handover requires minimum number of overall changes to routing tables
- Integration with firewalls / private address support possible

■ Potential problems:

- Not transparent to MNs
- Handover efficiency in wireless mobile scenarios:
 - Complex MN operations
 - All routing reconfiguration messages sent over wireless link