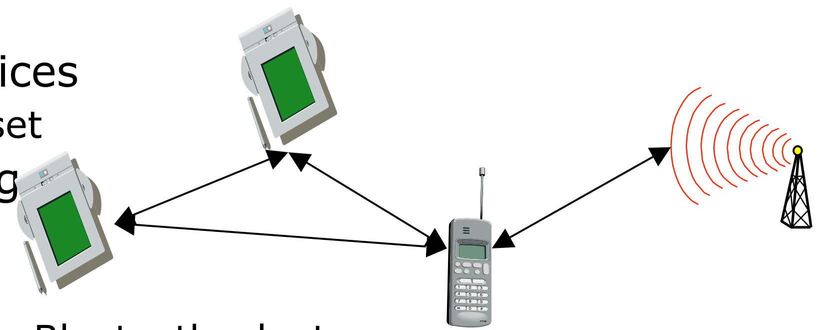
Bluetooth and Mobile IP

Wireless Networks Fall 2007

Bluetooth

- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba…
- Scenarios:
  - connection of peripheral devices
    - loudspeaker, joystick, headset
  - support of ad-hoc networking
    - small devices, low-cost
  - bridging of networks
    - e.g., GSM via mobile phone - Bluetooth - laptop



- Simple, cheap, replacement of IrDA, low range, lower data rates, low-power
  - Worldwide operation: 2.4 GHz
  - Resistance to jamming and selective frequency fading:
    - FHSS over 79 channels (of 1MHz each), 1600hops/s
  - Coexistence of multiple piconets: like CDMA
  - Links: synchronous connections and asynchronous connectionless
  - Interoperability: protocol stack supporting TCP/IP, OBEX, SDP
  - Range: 10 meters, can be extended to 100 meters
- Documentation: over 1000 pages specification: www.bluetooth.com

Bluetooth Application Areas

- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Low cost < $5
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range

Protocol Architecture

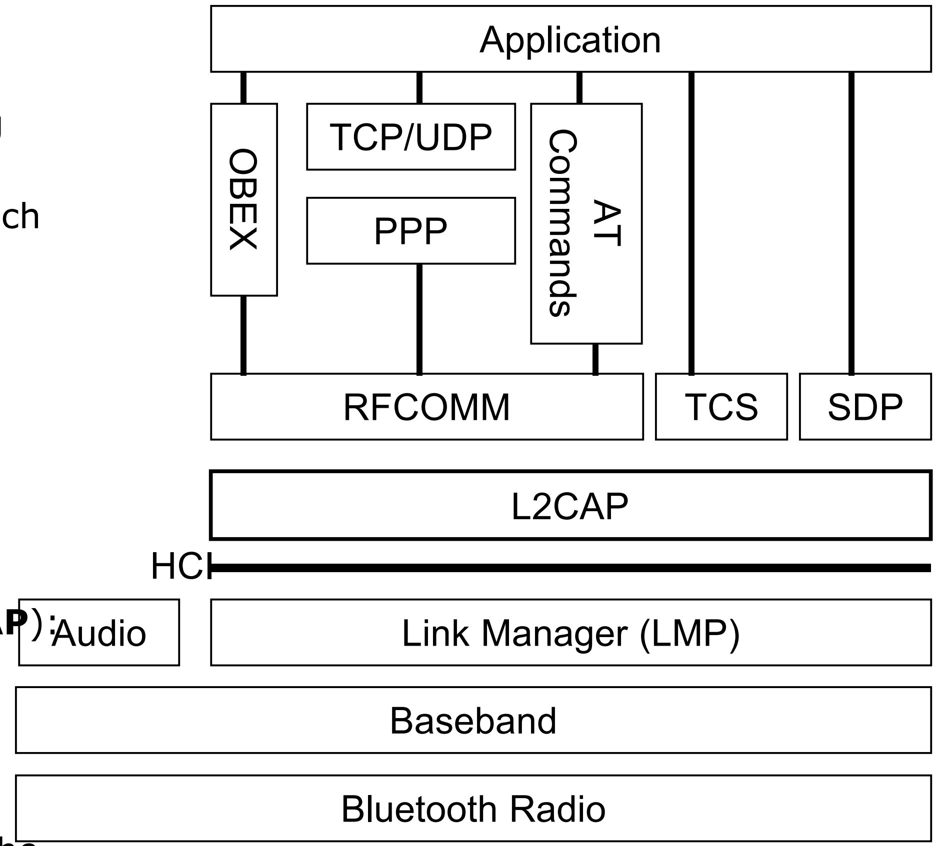
- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

Protocol Architecture

- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX
  - WAE/WAP

Protocol Architecture

- BT **Radio** (2.4 GHZ Freq. Band):
- Modulation: Gaussian Frequency Shift Keying
- **Baseband**: FH-SS (79 carriers), CDMA (hopping sequence from the node MAC address)
- **Audio**: interfaces directly with the baseband. Each voice connection is over a 64Kbps SCO link. The voice coding scheme is the Continuous Variable Slope Delta (CVSD)
- Link Manager Protocol (**LMP**): link setup and control, authentication and encryption
- Host Controller Interface: provides a uniform method of access to the baseband, control registers, etc through USB, PCI, or UART
- Logical Link Control and Adaptation Layer (**L2CAP**): higher protocols multiplexing, packet segmentation/reassembly, QoS
- Service Discover Protocol (**SDP**): protocol of locating services provided by a Bluetooth device
- Telephony Control Specification (**TCS**): defines the call control signaling for the establishment of speech and data calls between Bluetooth devices
- **RFCOMM**: provides emulation of serial links (RS232). Upto 60 connections



OBEX: OBject EXchange (e.g., vCard)

Usage Models

- File transfer
- Internet bridge
- LAN access
- Synchronization
- Three-in-one phone
- Headset

Piconets and Scatternets

- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

Wireless Network Configurations

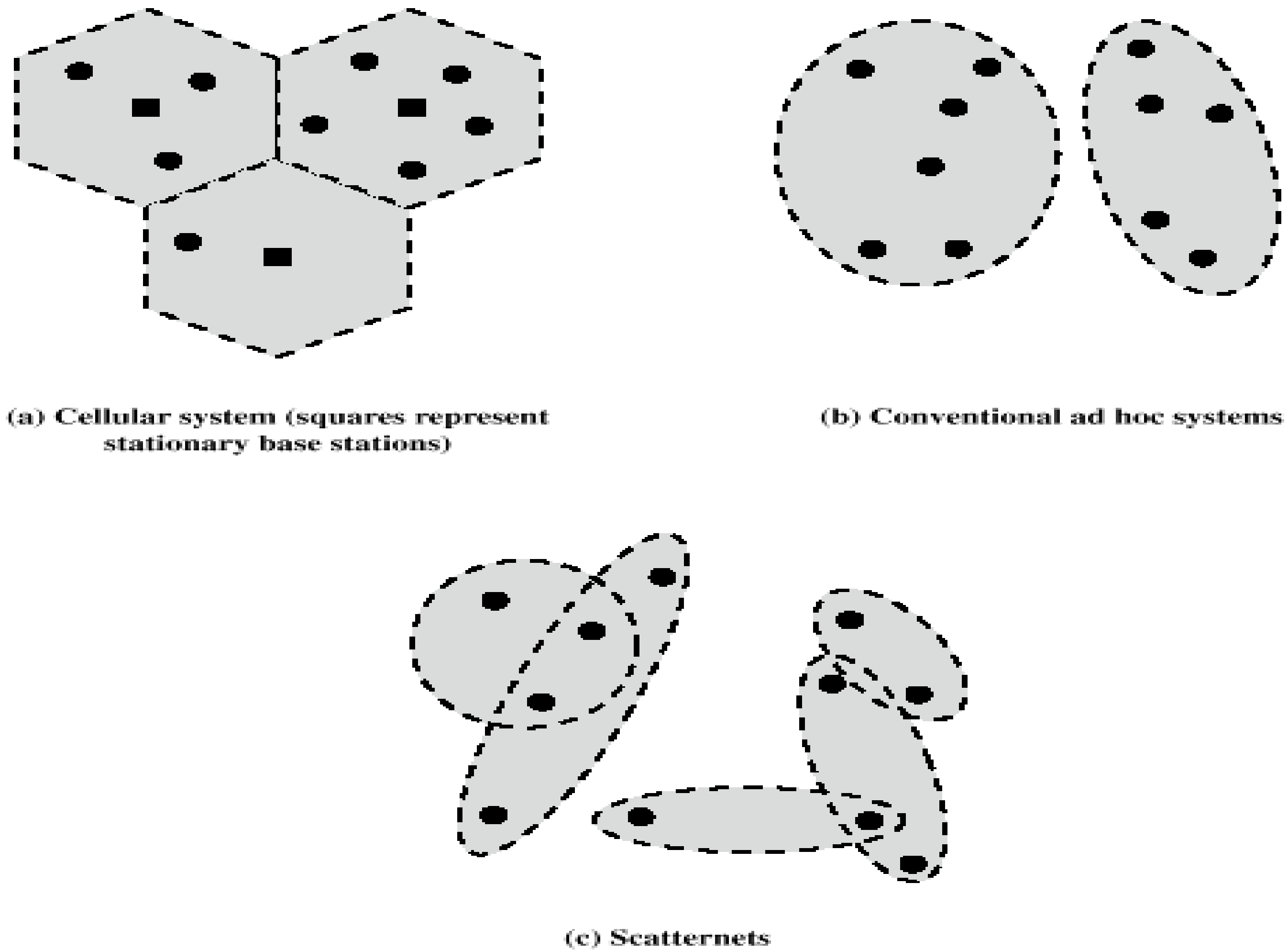
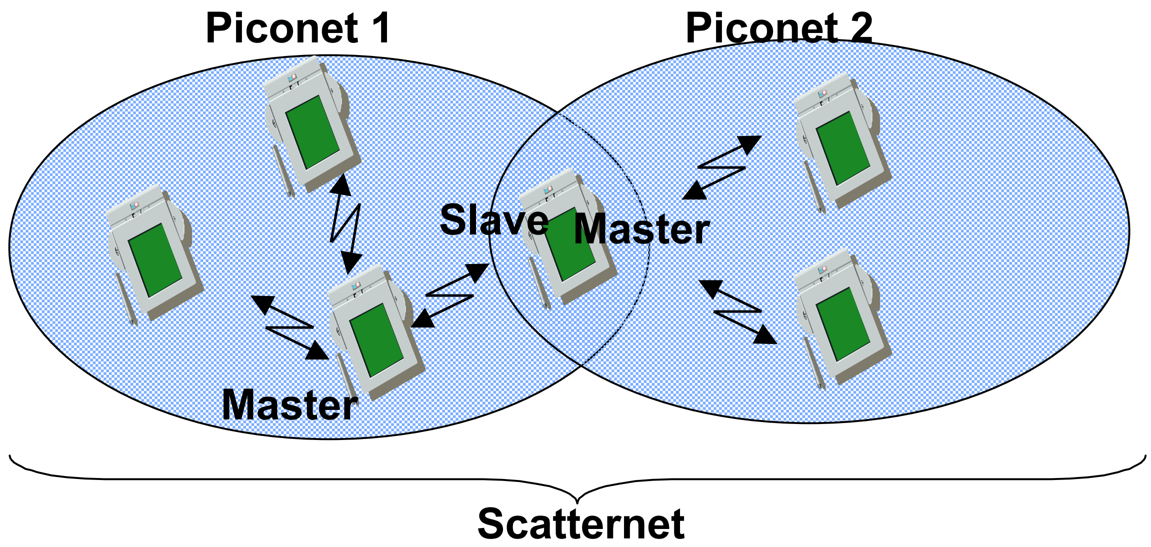


Figure 15.5 Wireless Network Configurations

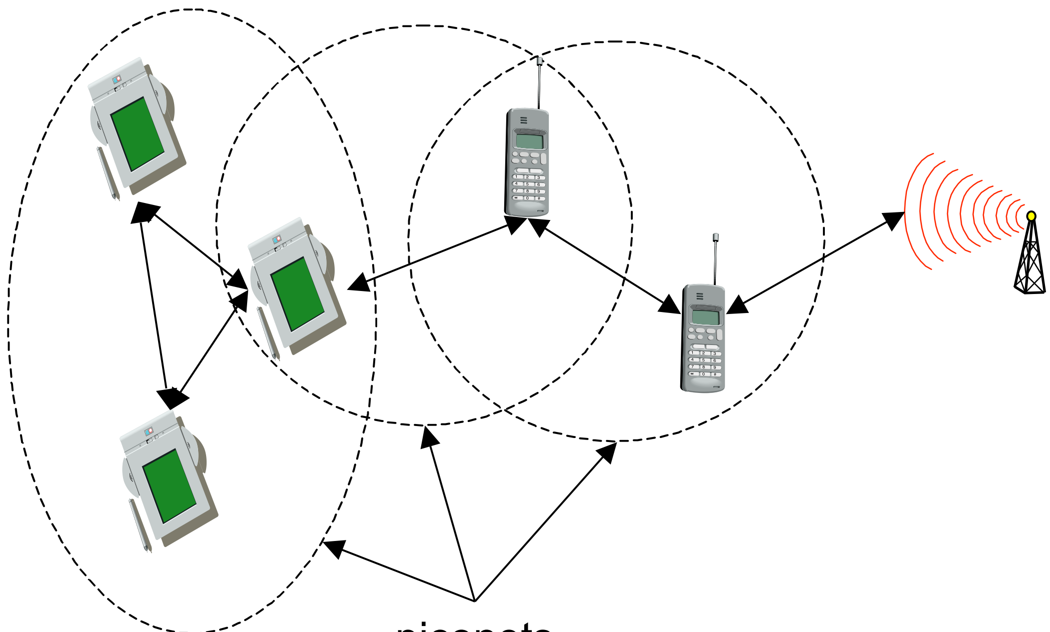
Network Topology



- Piconet = set of Bluetooth nodes synchronized to a master node
  - The piconet hopping sequence is derived from the master MAC address (BD_ADDR IEEE802 48 bits compatible address)
- Scatternet = set of piconet
- Master-Slaves can switch roles
- A node can only be master of one piconet. Why?

Scatternets

- Each piconet has one master and up to 7 slaves
- Master determines hopping sequence, slaves have to synchronize
- Participation in a piconet = synchronization to hopping sequence
- Communication between piconets = devices jumping back and forth between the piconets



Radio Specification

- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power
- Frequency Hopping in Bluetooth
  - Provides resistance to interference and multipath effects
  - Provides a form of multiple access among co-located devices in different piconets

Frequency Hopping

- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA

Frequency Hopping

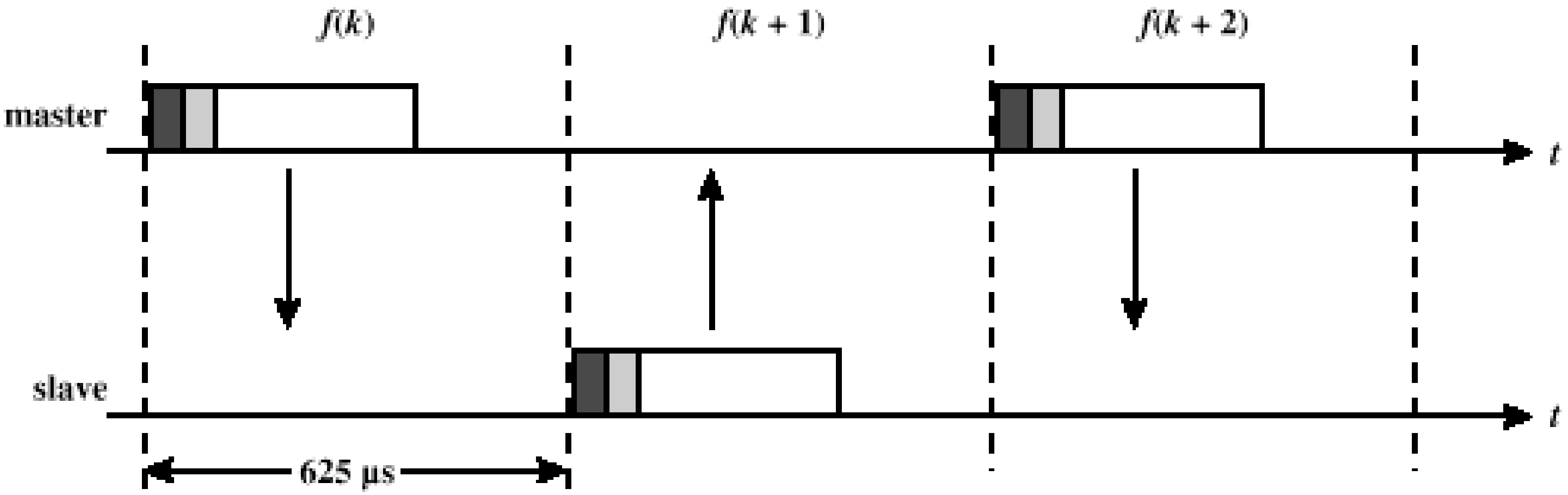


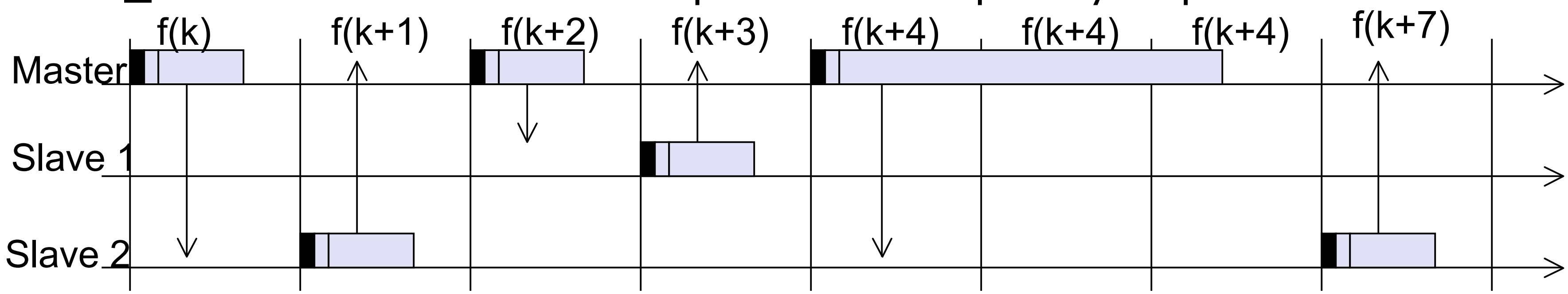
Figure 15.6 Frequency-Hop Time-Division Duplex

Physical Links

- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

Bluetooth Piconet MAC

- Each node has a Bluetooth Device Address (BD_ADDR). The master BD_ADDR determines the sequence of frequency hops

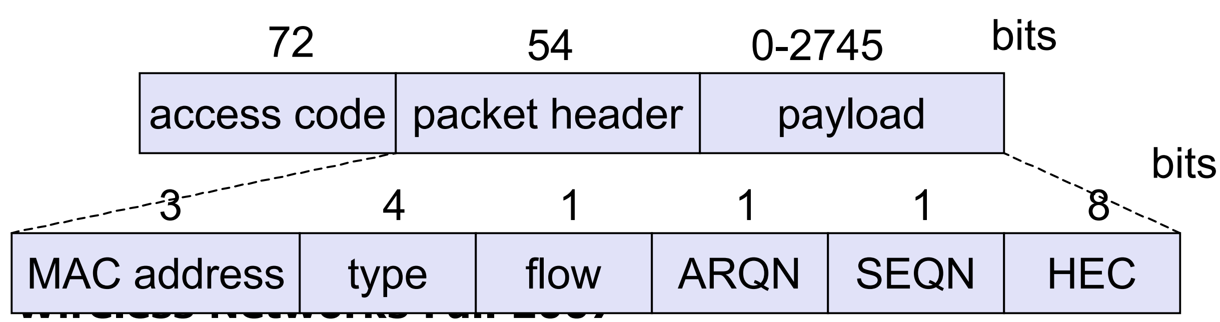


- Types of connections:

  Synchronous Connection-Oriented link (**SCO**) (symmetrical, circuit switched, point-to-point)

  Asynchronous Connectionless Link (**ACL**): (packet switched, point-to-multipoint, master-polls)

- Packet Format:
  - o Access code: synchronization, when piconet active derived from master
  - o Packet header (for ACL): 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



Types of Access Codes

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes
- Preamble+sync+trailer

Packet Header Fields

- AM_ADDR – contains "active mode" address of one of the slaves
- Type – identifies type of packet
  - ACL: Data Medium (DM) or Data High (DH), with different slot lengths (DM1, DM3, DM5, DH1, DH3, DH5)
  - SCO: Data Voice (DV) and High-quality voice (HV)
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

Payload Format

- Payload header
  - o L_CH field – identifies logical channel
  - o Flow field – used to control flow at L2CAP level
  - o Length field – number of bytes of data
- Payload body – contains user data
- CRC – 16-bit CRC code

Error Correction Schemes

- 1/3 rate FEC (forward error correction)
  - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
  - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
  - Used with DM and DH packets

ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits
- Bluetooth uses ACKs, NAKs, and a form of stop-and-wait ARQ

Types of packets

- SCO packets: Do not have a CRC (except for the data part of DV) and are never retransmitted. Intended for High-quality Voice (HV).

Type	Payload (bytes)	FEC	CRC	max-rate kbps
HV1	10	1/3	No	64
HV2	20	2/3	No	64
HV3	30	No	No	64
DV	10+(1-10)D	2/3D	Yes D	64+57.6D

- ACL packets: Data Medium-rate (DM) and Data High-rate (DH)

Type	Payload (bytes)	FEC	CRC	Sym. max-rate	Asymm. max-rate (DL/UL)
DM1	0-17	2/3	Yes	108.8	108.8/108.9
DM3	0-121	2/3	Yes	258.1	387.2/54.4
DM5	0-224	2/3	Yes	286.7	477.8/36.3
DH1	0-27	No	Yes	172.8	172.8/172.8
DH3	0-183	No	Yes	390.4	585.6/86.4
DH5	0-339	No	Yes	433.9	723.2/185.6

Channel Control

- Major states
  - Standby – default state
  - Connection – device connected
- Interim substates for adding new slaves
  - Page – device issued a page (used by master)
  - Page scan – device is listening for a page
  - Master response – master receives a page response from slave
  - Slave response – slave responds to a page from master
  - Inquiry – device has issued an inquiry for identity of devices within range
  - Inquiry scan – device is listening for an inquiry
  - Inquiry response – device receives an inquiry response

Inquiry Procedure

- Potential master identifies devices in range that wish to participate
  - Transmits ID packet with inquiry access code (IAC)
  - Occurs in Inquiry state
- Device receives inquiry
  - Enter Inquiry Response state
  - Returns FHS (Frequency Hop Synchronization) packet with address and timing information
  - Moves to page scan state

Inquiry Procedure Details

- Goal: aims at discovering other neighboring devices
- Inquiring node:
  - Sends an inquiry message (packet with only the access code: General Inquiry Access Code: GIAC or Dedicated IAC: DIAC). This message is sent over a subset of all possible frequencies.
  - The inquiry frequencies are divided into two hopping sets of 16 frequencies each.
  - In inquiry state the node will send up to $N_{INQUIRY}$ sequences on one set of 16 frequencies before switching to the other set of 16 frequencies. Upto 3 switches can be executed. Thus the inquiry may last upto 10.24 seconds.
- To be discovered node:
  - Enters an inquiry_scan mode
  - When hearing the inquiry_message (and after a backoff procedure) enter an inquiry_response mode: send a Frequency Hop Sync (FHS) packet (BD_ADDR, native clock)
- After discovering the neighbors and collecting information on their address and clock, the inquiring node can start a page routine to setup a piconet

Page Procedure

- Master uses devices address to calculate a page frequency-hopping sequence
- Master pages with ID packet and device access code (DAC) of specific slave
- Slave responds with DAC ID packet
- Master responds with its FHS packet
- Slave confirms receipt with DAC ID
- Slaves moves to Connection state

Page Procedure Details

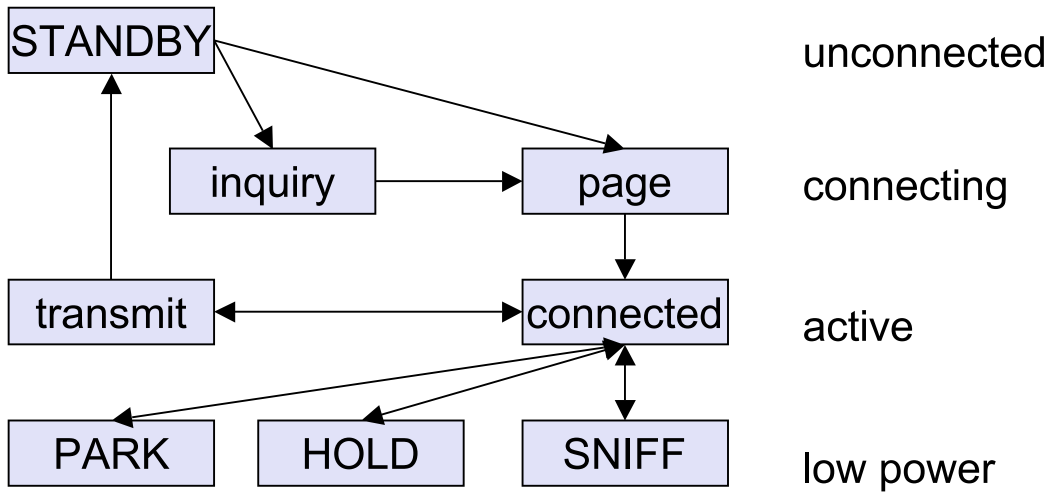
- Goal: e.g., setup a piconet after an inquiry
- Paging node (master):
  - Sends a page message (i.e., packet with only Device Access Code of paged node) over 32 frequency hops (from DAC and split into 2*16 freq.)
  - Repeated until a response is received
  - When a response is received send a FHS message to allow the paged node to synchronize
- Paged node (slave):
  - Listens on its hopping sequence
  - When receiving a page message, send a page_response and wait for the FHS of the pager

Slave Connection State Modes

- Active – participates in piconet
  - Listens, transmits and receives packets
- Sniff – only listens on specified slots
- Hold – does not support ACL packets
  - Reduced power status
  - May still participate in SCO exchanges
- Park – does not participate on piconet
  - Still retained as part of piconet

States of a Bluetooth Device

ACTIVE (connected/transmit): the device is uniquely identified by a 3bits AM_ADDR and is fully participating
SNIFF state: participates in the piconet only within the SNIFF interval
HOLD state: keeps only the SCO links
PARK state (low-power): releases AM_ADDR but stays synchronized with master



BT device addressing:
- BD_ADDR (48 bits)
- AM_ADDR (3bits): ACTIVE, HOLD, or SNIFF
- PM_ADDR (8 bits): PARK Mode address (exchanged with the AM_ADDR when entering PARK mode)
- AR_ADDR (8 bits): not unique used to come back from PARK to ACTIVE state

Bluetooth Audio

- Voice encoding schemes:
  - Pulse code modulation (PCM)
  - Continuously variable slope delta (CVSD) modulation
- Choice of scheme made by link manager
  - Negotiates most appropriate scheme for application

Bluetooth Link Security

- Elements:
  - Authentication – verify claimed identity
  - Encryption – privacy
  - Key management and usage
- Security algorithm parameters:
  - Unit address
  - Secret authentication key (128 bits key)
  - Secret privacy key (4-128 bits secret key)
  - Random number

Link Management

- Manages master-slave radio link
- Security Service: authentication, encryption, and key distribution
- Clock synchronization
- Exchange station capability information
- Mode management:
  - switch master/slave role
  - change hold, sniff, park modes
  - QoS

L2CAP

- Provides a link-layer protocol between entities with a number of services
- Relies on lower layer for flow and error control
- Makes use of ACL links, does not support SCO links
- Provides two alternative services to upper-layer protocols
  - Connectionless service
  - Connection-oriented service: A QoS flow specification is assigned in each direction
- Exchange of signaling messages to establish and configure connection parameters

Mobile IP

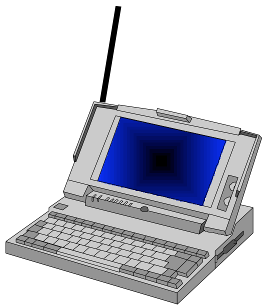
Motivation for Mobile IP

- 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

Mobile IP Requirements

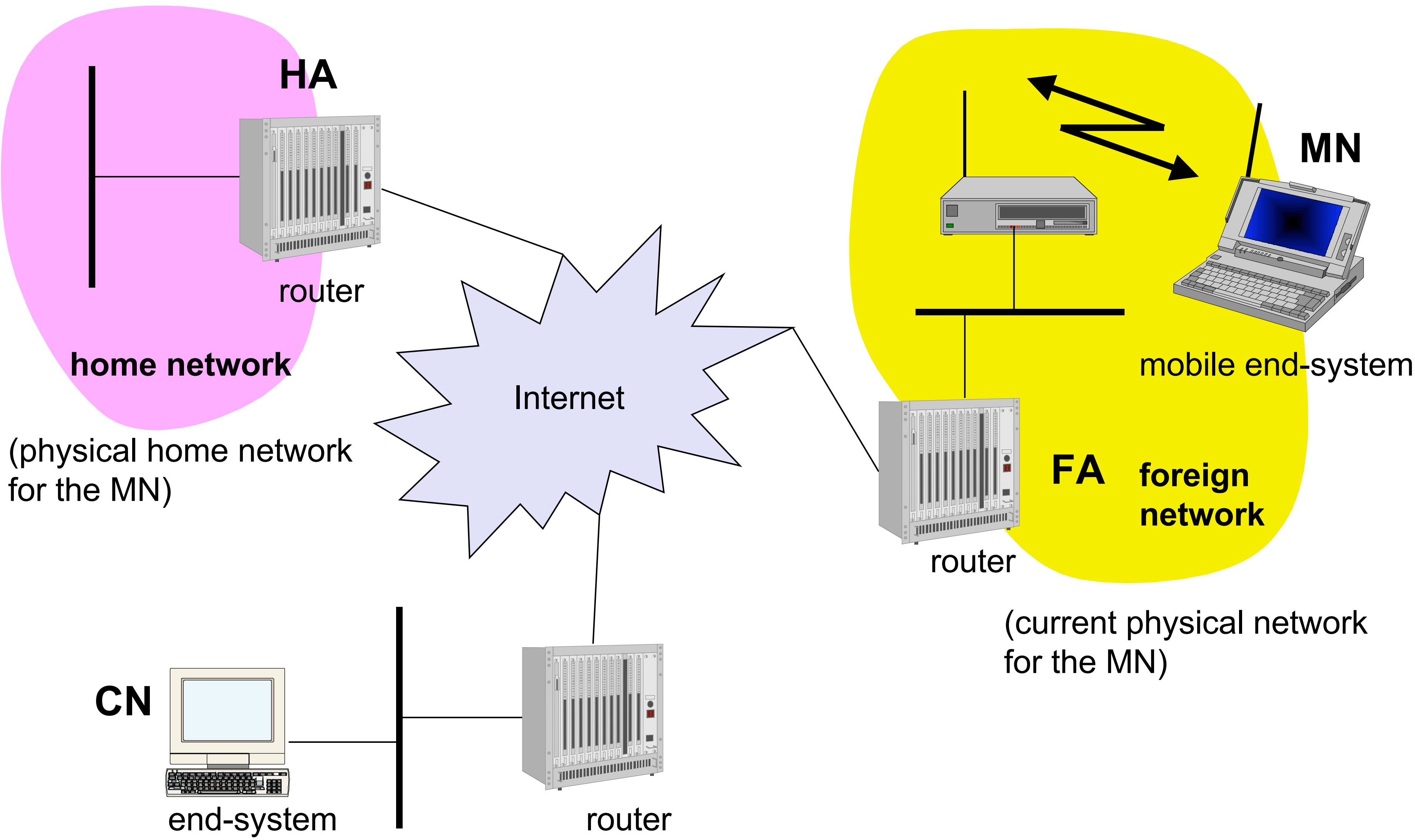
- Transparency
  - mobile end-systems keep their IP address
  - continuation of communication after interruption of link possible
  - point of connection to the fixed network can be changed
- Compatibility
  - support of the same layer 2 protocols as IP
  - no changes to current end-systems and routers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

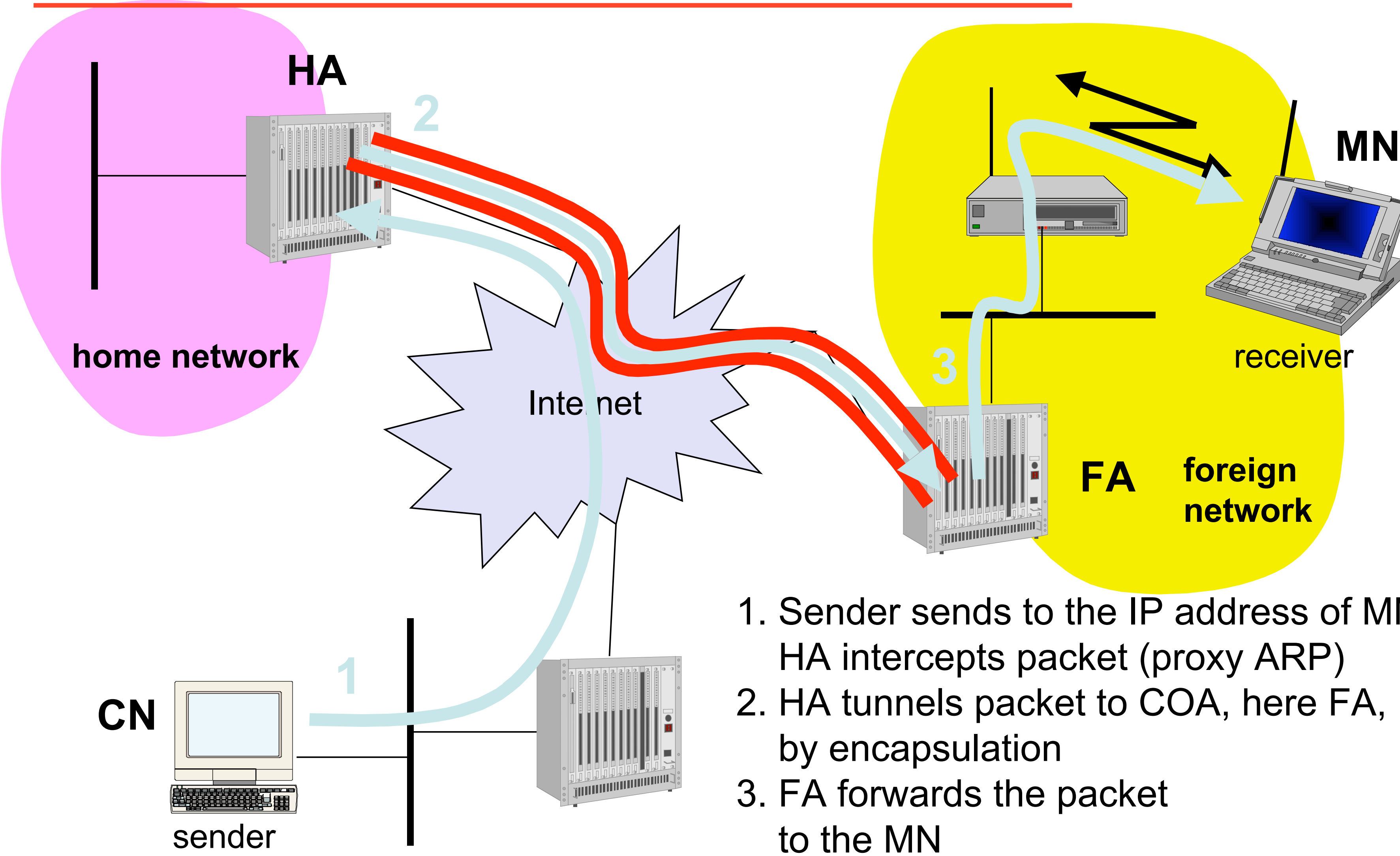


- Mobile Node (MN)
  - system (node) that can change the point of connection to the network without changing its IP address
- Home Agent (HA)
  - system in the home network of the MN, typically a router
  - registers the location of the MN, tunnels IP datagrams to the COA
- Foreign Agent (FA)
  - system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

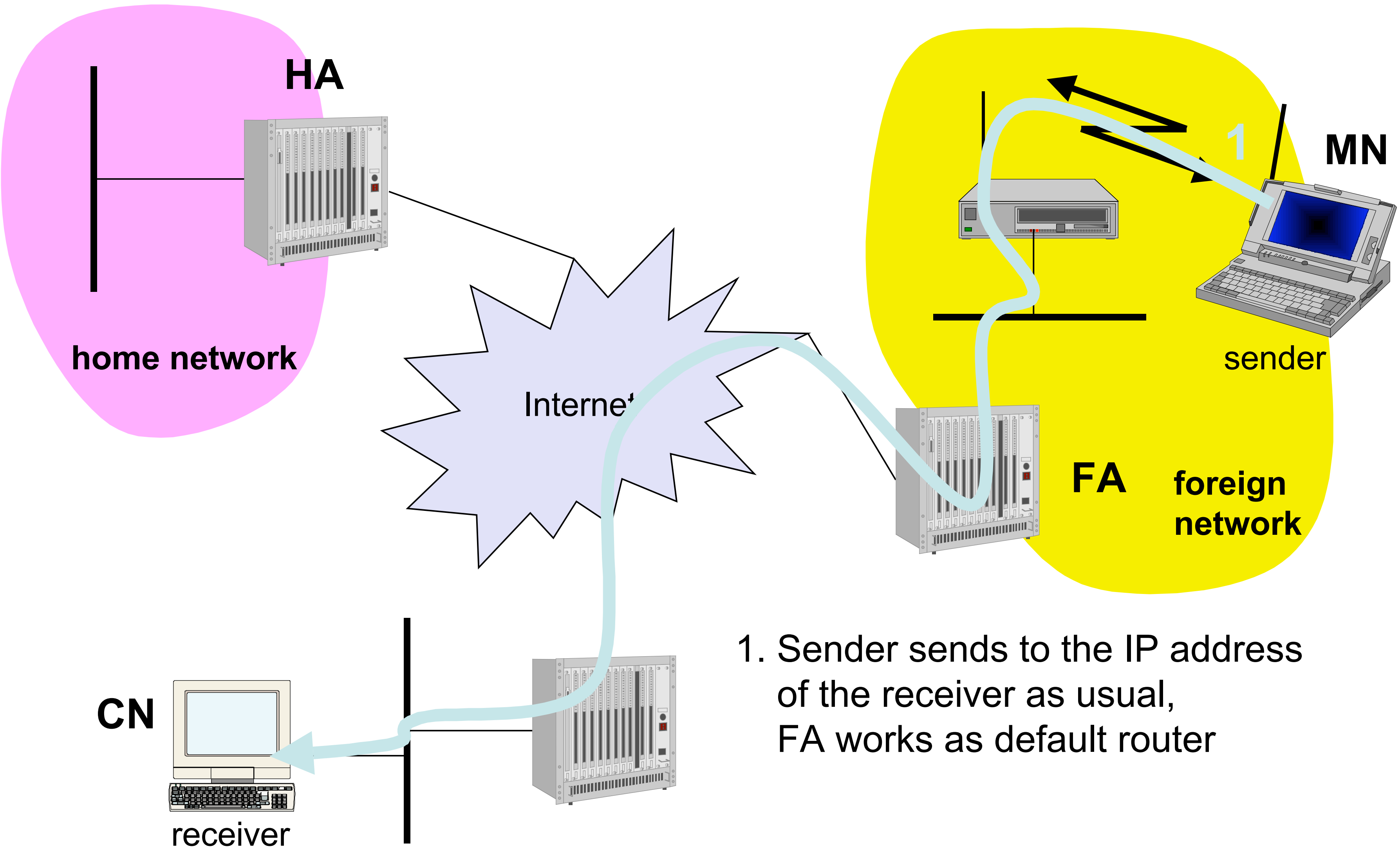


Data transfer to the mobile



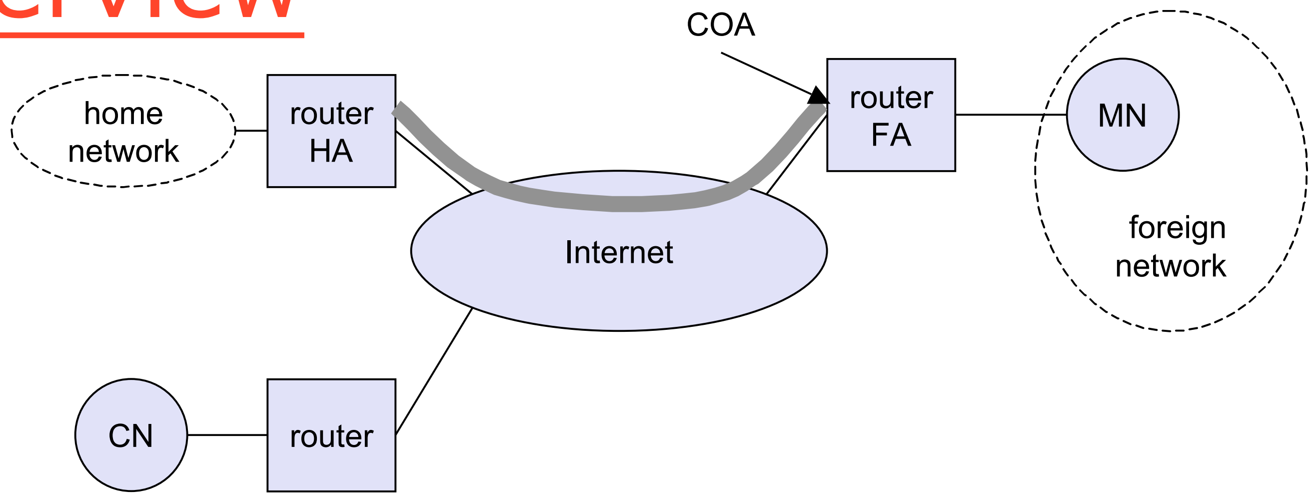
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile

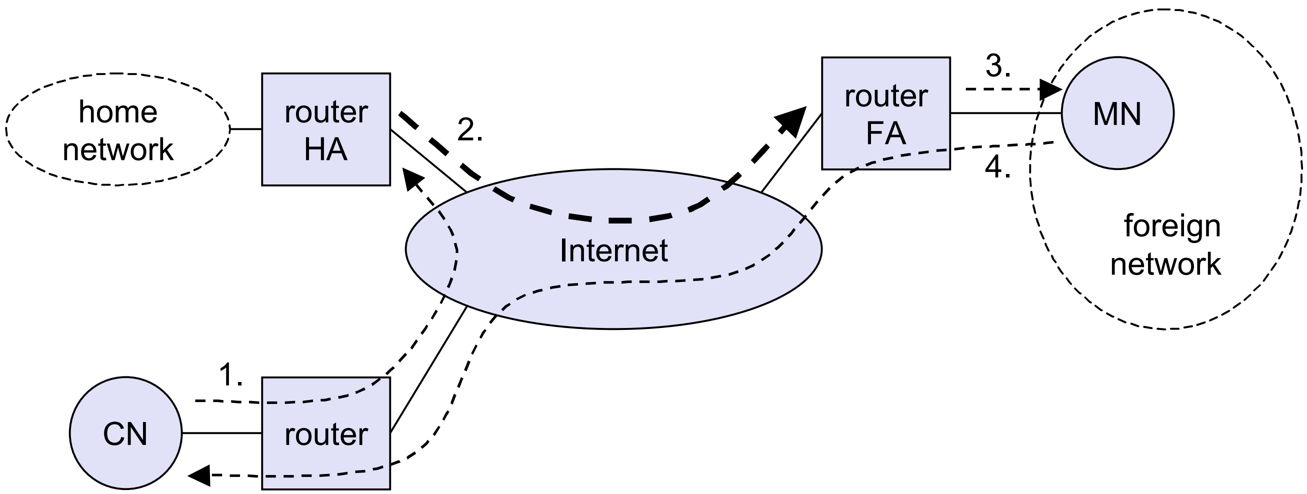


1. Sender sends to the IP address of the receiver as usual, FA works as default router

Overview



COA
home network
router HA
router FA
MN
Internet
foreign network
CN
router



home network
router HA
2.
router FA
3.
MN
4.
Internet
foreign network
1.
CN
router

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

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	length	sequence number							
registration lifetime		R	B	H	F	M	G	V	reserved
COA 1									
COA 2									

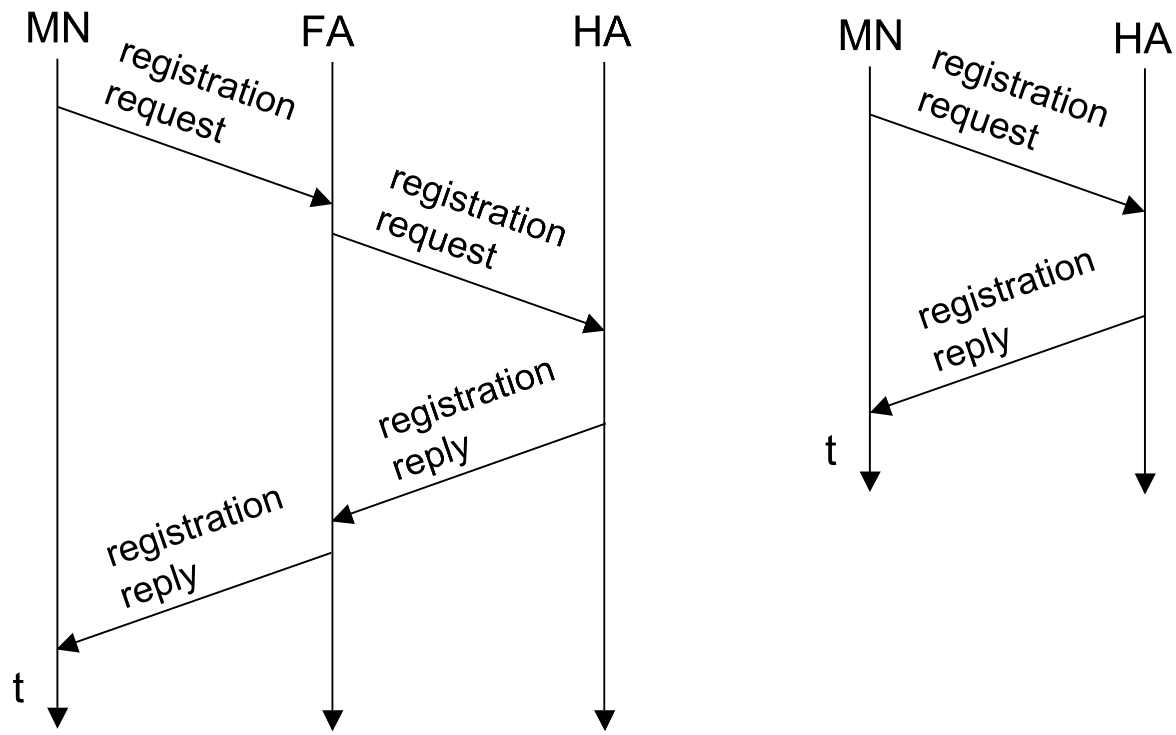
. . .

R: registration required
B: busy
H: home agent
F: foreign agent
M: minimal encapsulation
G: generic encapsulation
V: header compression

ICMP-Type = 0; Code = 0/16; Extension Type = 16

TTL = 1 Dest-Adr = 224.0.0.1 (multicast on link) or 255.255.255.255 (broadcast)

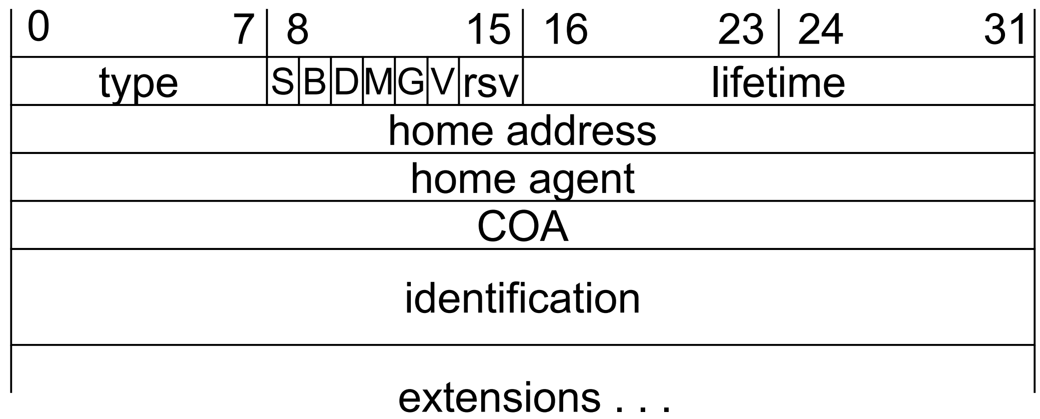
Registration



Goal: inform the home agent of current location of MN (COA-FA or co-located COA)

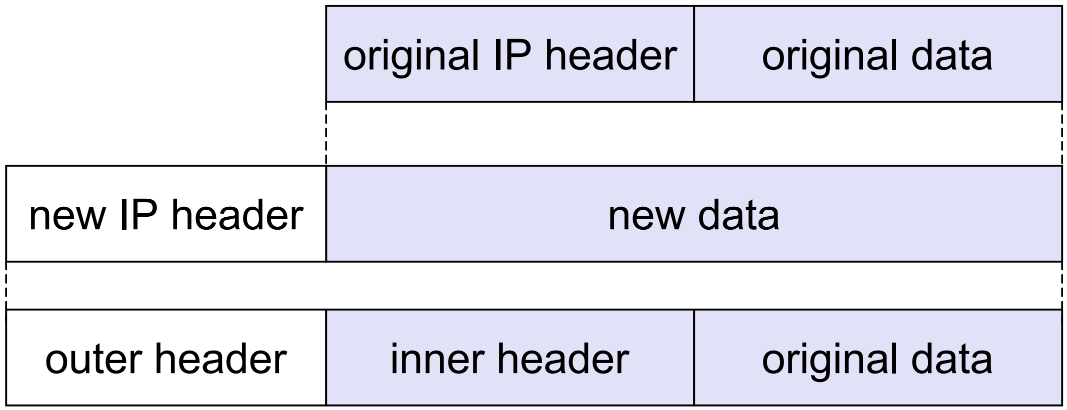
Registration expires automatically (lifetime)
Uses UDP port 434

Mobile IP registration request



UDP packet on port 343
Type = 1 for registration request
S: retain prior mobility bindings
B: forward broadcast packets
D: co-located address=> MN decapsulates packets

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

ver.	IHL	TOS	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP*	IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	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

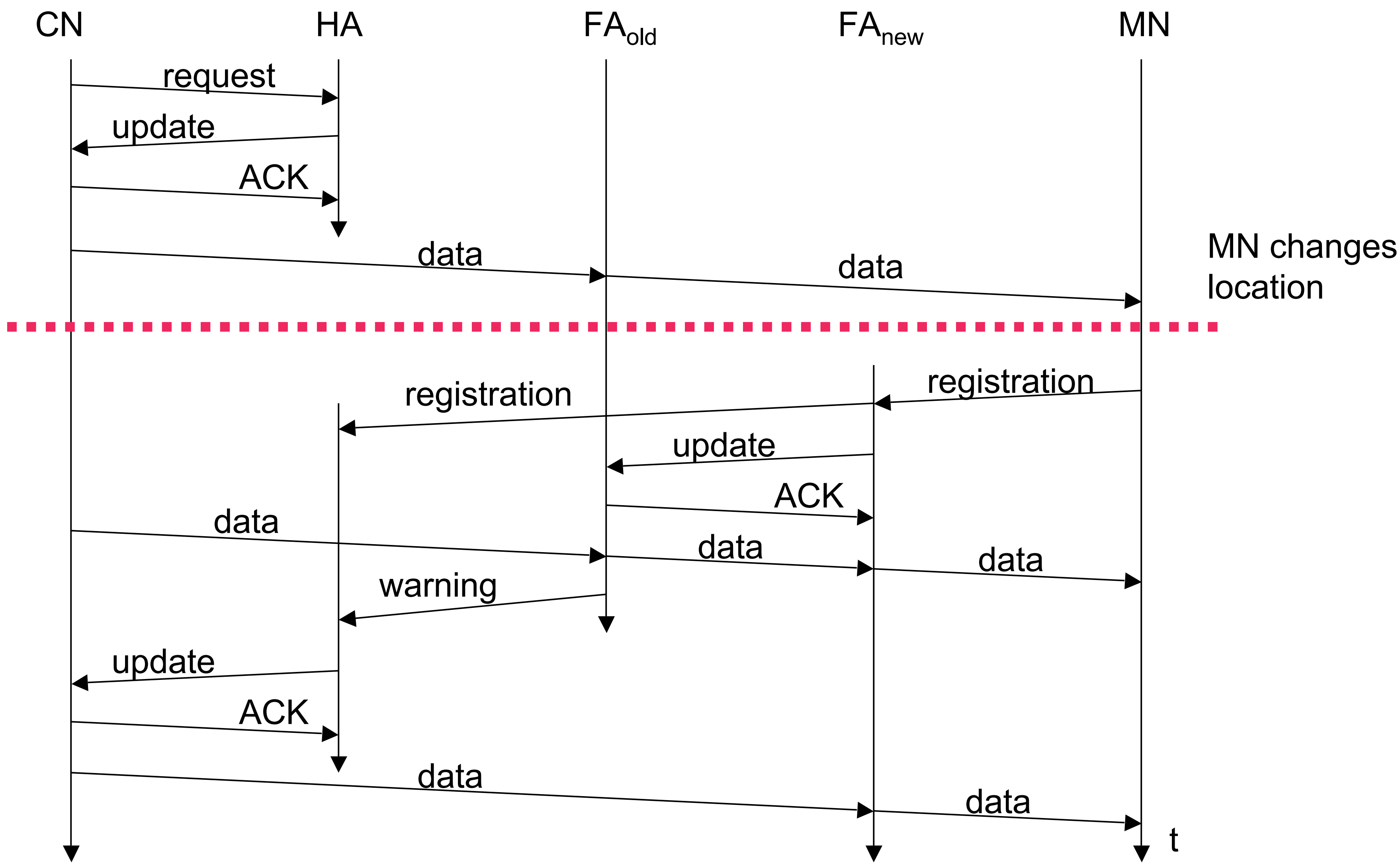
- Minimal encapsulation (optional) [RFC2004]
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, TOS
  - only applicable for unfragmented packets, no space left for fragment identification

<table>
<tr><td>ver.</td><td>IHL</td><td colspan="2">TOS</td><td colspan="2">length</td></tr>
<tr><td colspan="4">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">min. encap.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of HA</td></tr>
<tr><td colspan="6">care-of address COA</td></tr>
<tr><td colspan="2">lay. 4 protoc.</td><td>S</td><td>reserved</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of MN</td></tr>
<tr><td colspan="6">original sender IP address (if S=1)</td></tr>
<tr><td colspan="6">TCP/UDP/ ... payload</td></tr>
</table>

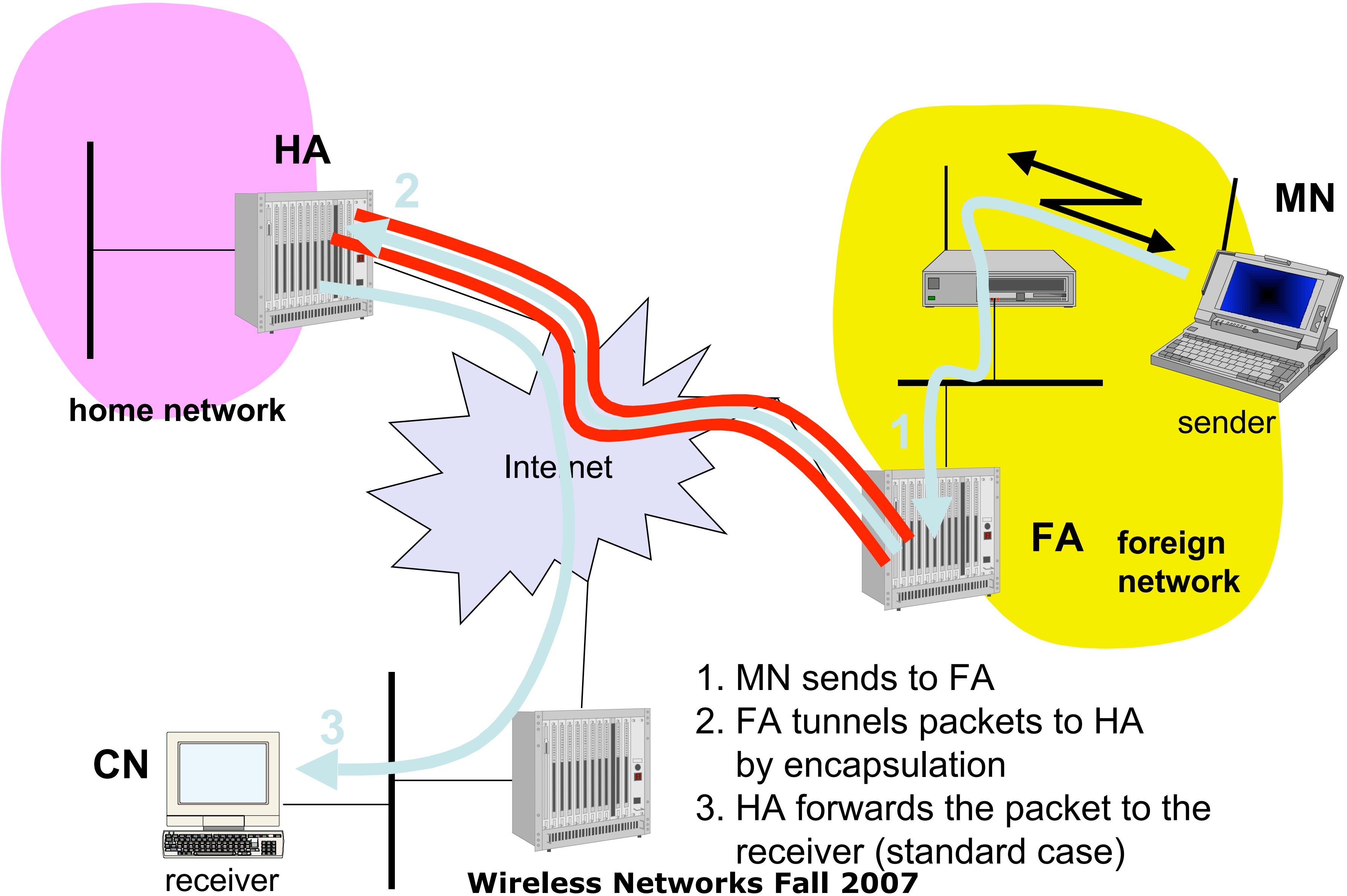
Optimization of packet forwarding

- 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)



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

- Routers 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

- 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!