1. Introduction

1.1. Everything moves …

1.2. Mobility versus portability

1.3. Mobile devices

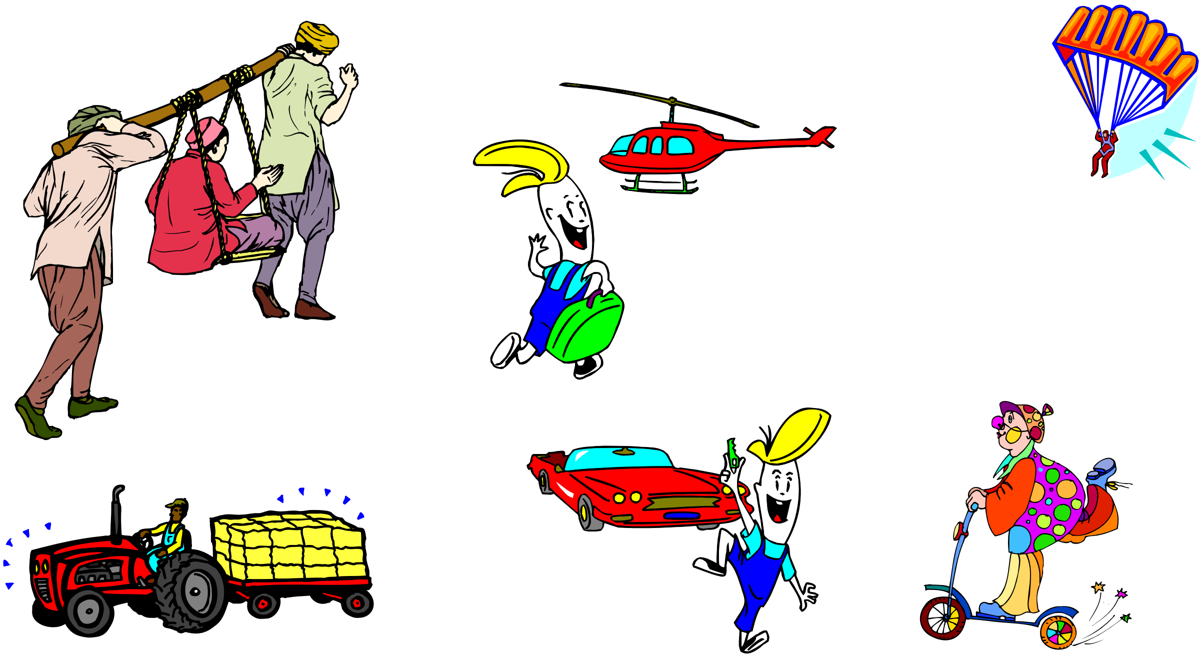
1.4. Wireless communication

1.5. Mobile communication and the layer model

1.1. Everything moves …

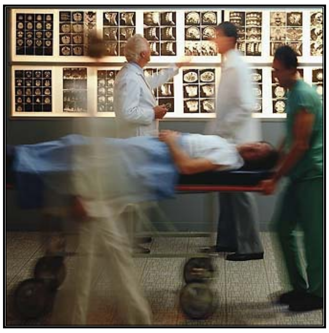
Mobility is one of the watchwords of our society:

Everything moves. Faster and more frequently.

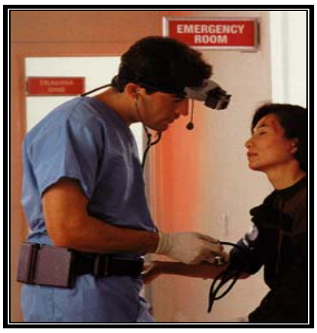


Wearable Applications (as discussed in IEEE 802 in March 1998)

Paint Inspection and Assembly Operation



Patient Monitoring using Sensors attached to the Patient



Assistance for medical and paramedical Personnel

Pilot Assistance

Automated Trading at the Stock Exchange

Enhancing the Guest Experience

Source: S. Case, „A Brief Survey of Wearable Applications“, doc.: IEEE 802.11-98/96, http://grouper.ieee.org/groups/802/15/pub/Tutorials.html

Wearable Applications (as discussed in IEEE 802 in March 1998)

War of the Cyborgs ?

Mortal combat: Steve confronts a rival technology.

Source: D. Braley, „Wearables Standards“, doc.: IEEE 802.11-98/96, http://grouper.ieee.org/groups/802/15/pub/Tutorials.html

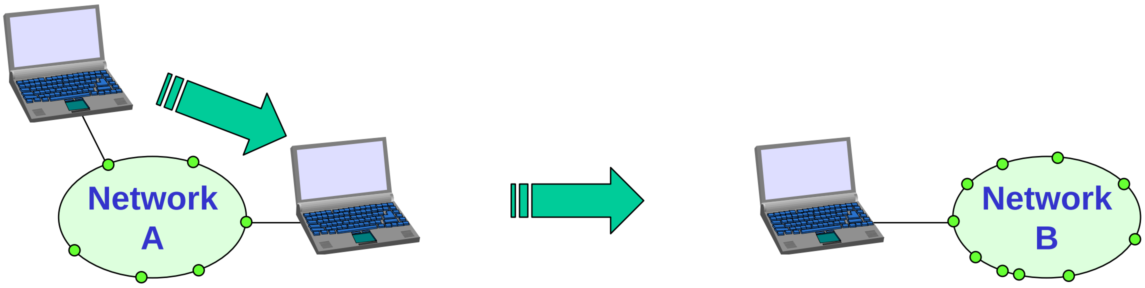
1.2. Mobility versus portability

Today, a lot of computer applications require network access.

Portable operation of a computer:

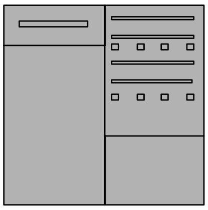
The computer
- can be operated **at any of a set of points of attachment**,
- usually **cannot be operated while being moved.**

⇨ **Network connections** are
- **shut down** and
- **re-initialized** at the new point of attachment



The client/server paradigm

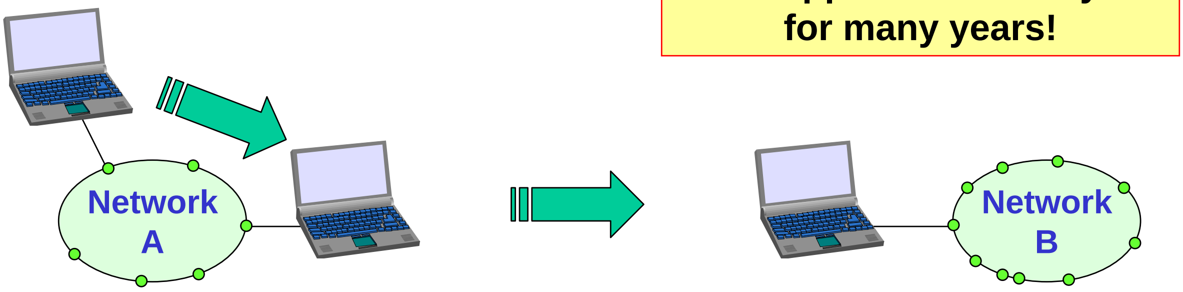
The **mobile device is the client** and uses client applications such as:



Central servers
in the Internet

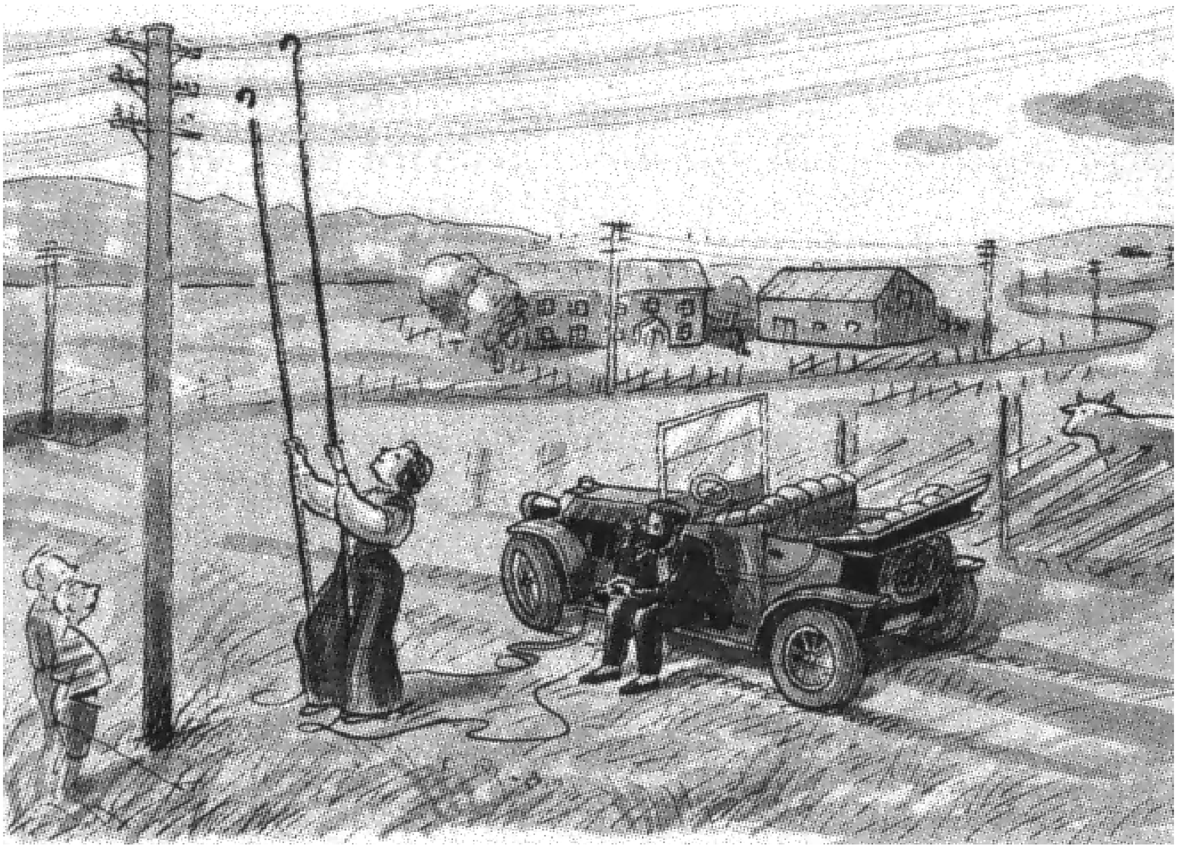
- E-Mail: access to centralised E-Mail servers via POP, IMAP, WWW
- browsing the WWW, download documents and files
- remote login (telnet, ssh)
- remote file transfer (ftp, scp)
- …

**This is no challenge
with the portability principle
as applicable already
for many years!**



The point of network attachment and
the client IP address are irrelevant for the server!

Mobile telephony in 1910



Source: Ericsson Connexion December 1994

Truly mobile operation

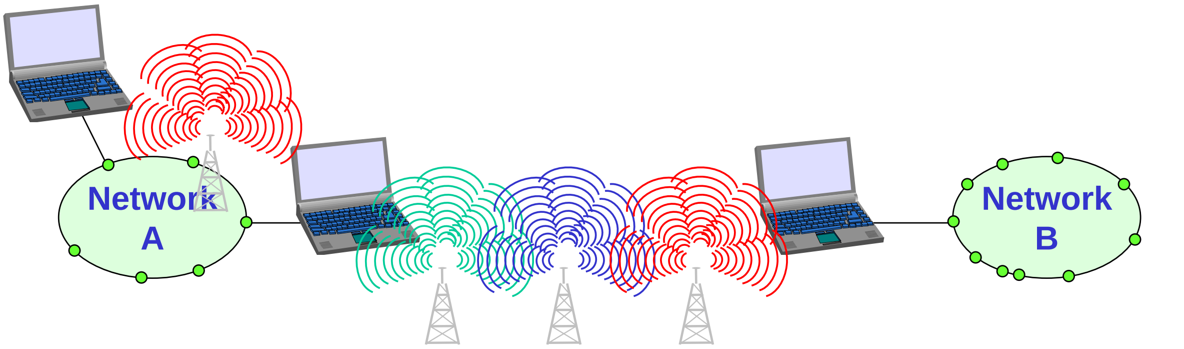
Truly mobile operation of a computer:

The computer

- can (at least almost) **continuously remain in contact** with the network resources required by the applications.

➡ **Neither the system nor the applications** running on the system need to be **re-initialized or restarted, ...**

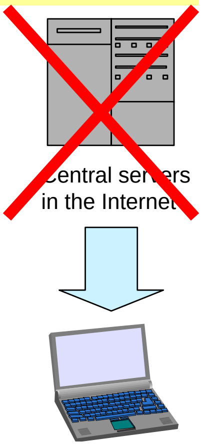
➡ **… even if the network connectivity is frequently broken and re-established at new points of attachment.**



A paradigm shift

The **mobile device becomes a server** and offers services to any other (mobile or fixed) device in the Internet:

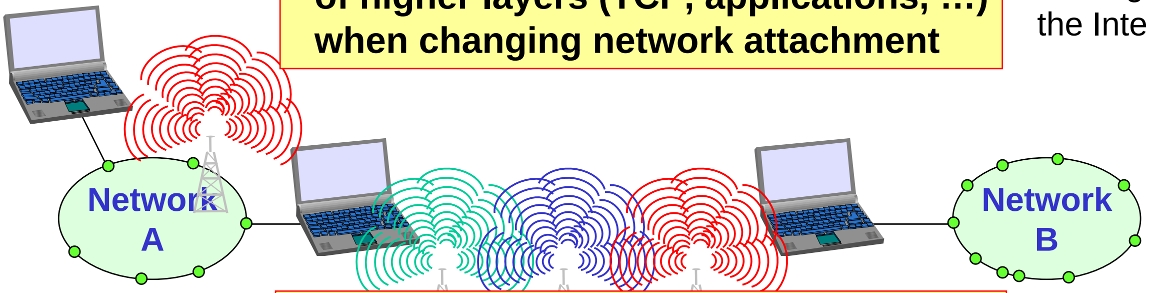
- resource sharing, peer to peer
- direct reachability, e.g. VoIP without server(s)
- …



Mobile server, moving within the Internet!

Important challenges of truly mobile operation:

- **reachability of the mobile device**
- **continuation of data connections of higher layers (TCP, applications, …) when changing network attachment**



A change of the IP address of the mobile device must be hidden for protocol layers above IP!

1.3. Mobile devices

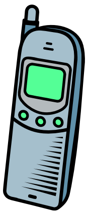
JS

Pager
- **receive only**
- tiny displays
- simple text messages

PDA
- simple graphical displays
- character recognition
- **simplified WWW**

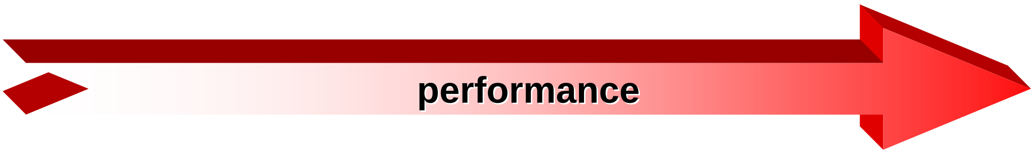
Laptop
- fully functional **standard applications**

Sensors, embedded controllers



Mobile phones
- **voice, data**
- simple graphical displays

Palmtop
- tiny keyboard
- **simple versions of standard applications**



Effects of device portability JS

- **Power consumption**
  - **limited computing power**, low quality displays, small disks due to **limited battery capacity**
  - **CPU: power consumption** ~ CV^2f
    - C: internal capacity, reduced by integration
    - V: supply voltage, can be reduced to a certain limit
    - f: clock frequency, can be reduced temporally
- **Loss of data**
  - **higher probability**, has to be included in advance into the design (e.g., defects, theft)
- **Limited user interfaces**
  - compromise between **size of fingers and portability**
  - integration of character/voice recognition, abstract symbols
- **Limited memory**
  - **limited value of mass memories with moving parts**
  - flash-memory or ? as alternative

1.4. Wireless communication

Obviously, user mobility is very limited in the wired world …

1.4.1. The electromagnetic spectrum

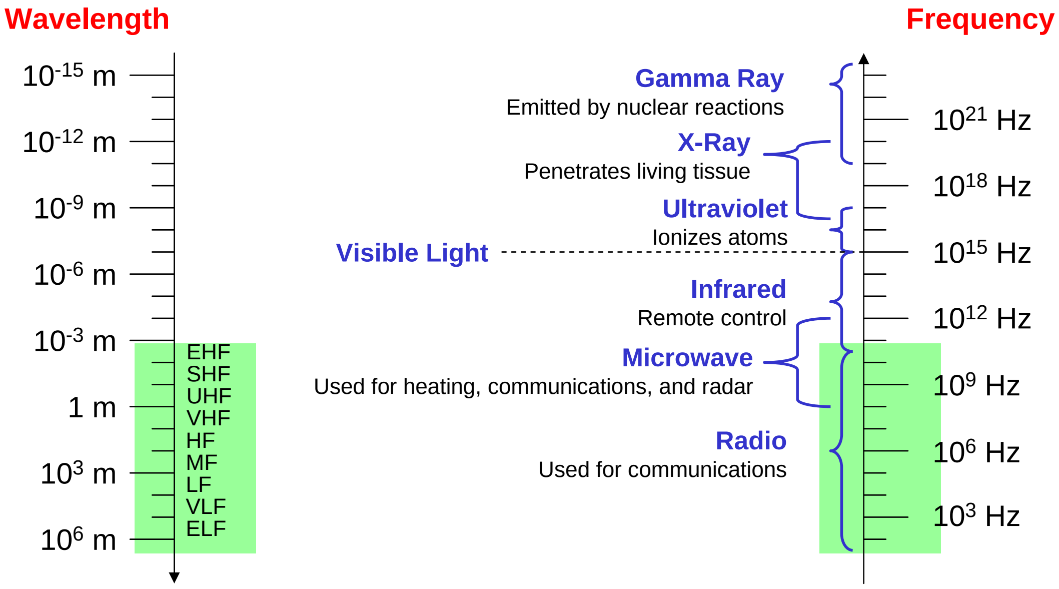
1.4.2. Early history of wireless communication

1.4.3. History of wireless communication

1.4.4. Wireless systems: Overview of the development

1.4.5. Wireless networks in comparison to fixed networks

1.4.1. The electromagnetic spectrum



Gamma Ray
Emitted by nuclear reactions

X-Ray
Penetrates living tissue

Ultraviolet
Ionizes atoms

Visible Light

Infrared
Remote control

Microwave
Used for heating, communications, and radar

Radio
Used for communications

Reminder: $\lambda = c/f$ where λ = wave length, $c \cong 3\text{x}10^8$m/s = speed of light, f = frequency

Radio wavebands

Wavelength	Frequency	Common Name	Main Purposes
Above 100 km	Below 3 kHz	Extremely Low Frequency (ELF)	Submarine communications
10 -100 km	3 – 30 kHz	Very Low Frequency (VLF)	Maritime communications
1 -10 km	20 – 300 kHz	Low Frequency (LF) or Long Wave (LW)	AM broadcasting
100 -1000 m	300 -3000 kHz	Medium Frequency (MF) or Medium Wave (MW)	AM broadcasting
10 -100 m	3 – 30 MHz	High Frequency (HF) or Short Wave (SW)	AM broadcasting, amateur radio
1 -10 m	30 -300 MHz	Very High Frequency (VHF)	FM broadcasting, TV
0,1 -1 m	300 – 3000 MHz	Ultra High Frequency (UHF)	TV, cell phones
10 -100 mm	3 -30 GHz	Super High Frequency (SHF)	Fixed wireless, satellites
1 -10 mm	30 – 300 GHz	Extra High Frequency (EHF)	Satellites, radar

Source: Andy Dornan, „The Essential Guide to Wireless Communications Applications“, Prentice Hall, 2001, p. 19, 20

Microwave wavebands

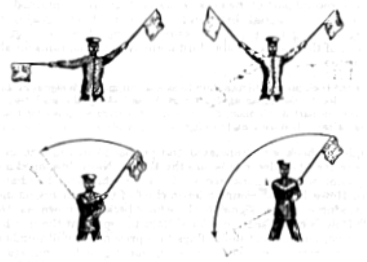
Wavelength	Frequency	Band	Main Communications Use
193 – 769 mm	0.4 – 1.5 GHz	L	Broadcasting and cellular
57.7 – 193 mm	1.5 – 5.2 GHz	S	Cellular
48.4 – 76.9 mm	3.9 – 6.2 GHz	C	Satellites
27.5 – 57.7 mm	5.2 – 10.9 GHz	X	Fixed wireless, satellite
8.34 – 27.5 mm	10.9 – 36 GHz	K	Fixed wireless, satellite
6.52 – 8.34 mm	36 – 46 GHz	Q	Fixed wireless
5.36 – 6.52 mm	46 - 56 GHz	V	Future satellite
3.00 – 5.36 mm	56 - 100 GHz	W	Future cellular

Source: Andy Dornan, „The Essential Guide to Wireless Communications Applications“, Prentice Hall, 2001, p. 20

1.4.2. Early history of wireless communication

JS

- **Many people in history used light for communication**
  - heliographs, flags („semaphore“), ...
  - 150 BC smoke signals for communication; (Polybius, Greece)
  - 1794, optical telegraph, Claude Chappe



- **Here electromagnetic waves are of special importance:**
  - 1831 **Faraday** demonstrates electromagnetic induction
  - **J. Maxwell** (1831-79): theory of electromagnetic Fields, wave equations (1864)
  - **H. Hertz** (1857-94): demonstrates with an experiment the wave character of electrical transmission through space (1888, in Karlsruhe, Germany, at the location of today’s University of Karlsruhe)

Heinrich Hertz
1889 – 1894 Professor University of Bonn
Chair of Physics (Physikalisches Institut)

1.4.3. History of wireless communication JS

- **1895 Guglielmo Marconi**
  - first demonstration of **wireless telegraphy** (digital!)
  - **long wave transmission**
    (high transmission power necessary, > 200kW)
- **1907 Commercial transatlantic connections**
  - **huge base stations** (30 100m high antennas)
- **1915 Wireless voice transmission New York - San Francisco**
- **1920 Discovery of short waves by Marconi**
  - **reflection at the ionosphere**
  - smaller sender and receiver, possible due to the invention of the vacuum tube (1906, Lee DeForest and Robert von Lieben)
- **1926 Train-phone on the line Hamburg - Berlin**
  - wires parallel to the railroad track

History of wireless communication (2) JS

- **1928 many TV broadcast trials** (across Atlantic, color TV, TV news)
- **1933 Frequency modulation** (E. H. Armstrong)
- **1958 A-Netz in Germany**
  - **analog**, 160MHz, connection setup only from the mobile station, no handover, 80% coverage, 1971 11000 customers
- **1972 B-Netz in Germany**
  - **analog**, 160MHz, connection setup from the fixed network too (but location of the mobile station has to be known)
  - available also in A, NL and LUX, 1979 13000 customer in D
- **1979 NMT at 450MHz** (Scandinavian countries)
- **1982 Start of GSM-specification**
  - goal: **pan-European digital mobile phone system with roaming**
- **1983 Start of the American AMPS** (Advanced Mobile Phone System, analog)
- **1984 CT-1 standard (Europe) for cordless telephones**

History of wireless communication (3)

JS

- **1986 C-Netz in Germany**
  - **analog** voice transmission, 450MHz, hand-over possible, digital signaling, automatic location of mobile device
  - Was in use until 2000, services: FAX, modem, X.25, e-mail, 98% coverage
- **1991 Specification of DECT**
  - Digital European Cordless Telephone
    (today: Digital Enhanced Cordless Telecommunications)
  - 1880-1900MHz, ~100-500m range, 120 duplex channels, 1.2Mbit/s data transmission, voice encryption, authentication, up to several 10000 user/km^2, used in more than 50 countries
- **1992 Start of GSM**
  - in D as D1 and D2, fully digital, 900MHz, 124 channels
  - **automatic location, hand-over**, cellular
  - roaming in Europe - now worldwide in more than 170 countries
  - services: data with 9.6kbit/s, FAX, voice, ...

History of wireless communication (4)

JS

- **1994 E-Netz in Germany**
  - **GSM** with 1800MHz, smaller cells
  - As Eplus in D (1997 98% coverage of the *population*)
- **1996 HiperLAN** (High Performance Radio Local Area Network)
  - **ETSI**, standardization of type 1: 5.15 - 5.30GHz, 23.5Mbit/s
  - recommendations for type 2 and 3 (both 5GHz) and 4 (17GHz) as wireless ATM-networks (up to 155Mbit/s)
- **1997 Wireless LAN - IEEE802.11**
  - **IEEE standard**, 2.4 - 2.5GHz and infrared, 2Mbit/s
  - already many (proprietary) products available in the beginning
- **1998 Specification of GSM successors**
  - for **UMTS** (Universal Mobile Telecommunication System) as European proposals for IMT-2000
- **Iridium**
  - 66 satellites (+6 spare), 1.6GHz to the mobile phone

History of wireless communication (5)

JS

- **1999 Standardization of additional wireless LANs**
  - **IEEE standard 802.11b**, 2.4-2.5GHz, 11Mbit/s
  - **Bluetooth** for piconets, 2.4Ghz, <1Mbit/s

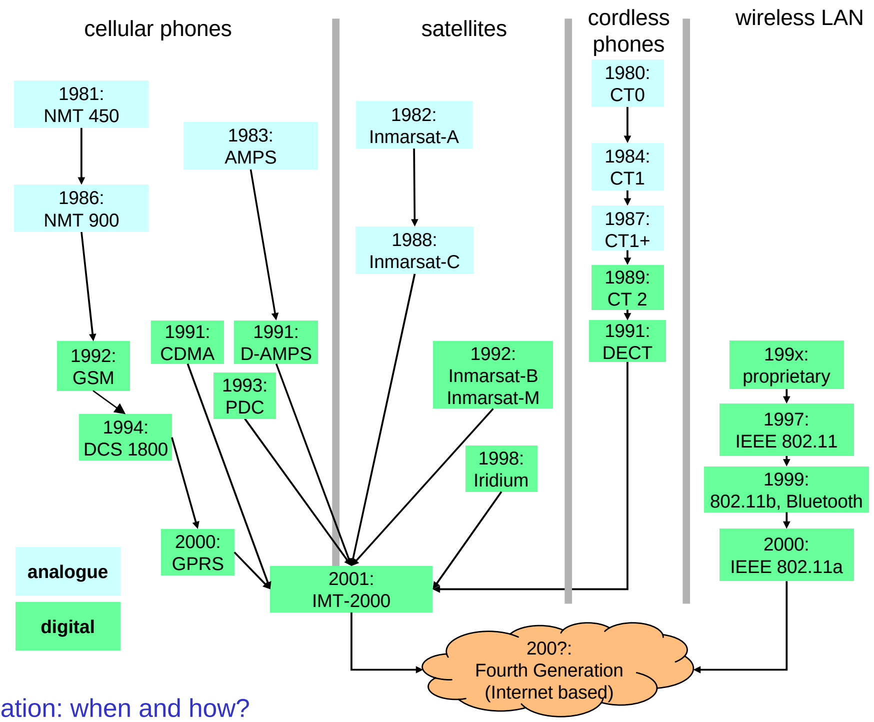
  Decision about IMT-2000
  - **Several “members” of a “family”:** UMTS, cdma2000, DECT, …

  Start of WAP (Wireless Application Protocol) and i-mode
  - **First step** towards a unified Internet/mobile communication system
  - Access to many services via the mobile phone
- **2000 GSM with higher data rates**
  - **HSCSD** offers up to 57,6kbit/s
  - First **GPRS** trials with up to 50 kbit/s (packet oriented!)

  UMTS auctions/beauty contests
  - **Hype** followed by **disillusionment**
    (approx. 50 B$ paid in Germany for 6 UMTS licences!)
- **2001 Start of 3G systems**
  - **Cdma2000** in Korea, **UMTS** in Europe, **Foma** (almost UMTS) in Japan

1.4.4. Wireless systems: Overview of the development

JS



cellular phones

satellites

cordless phones

wireless LAN

1981: NMT 450

1986: NMT 900

1983: AMPS

1991: CDMA

1991: D-AMPS

1992: GSM

1993: PDC

1994: DCS 1800

2000: GPRS

1982: Inmarsat-A

1988: Inmarsat-C

1992: Inmarsat-B Inmarsat-M

1998: Iridium

1980: CT0

1984: CT1

1987: CT1+

1989: CT 2

1991: DECT

199x: proprietary

1997: IEEE 802.11

1999: 802.11b, Bluetooth

2000: IEEE 802.11a

2001: IMT-2000

200?: Fourth Generation (Internet based)

analogue

digital

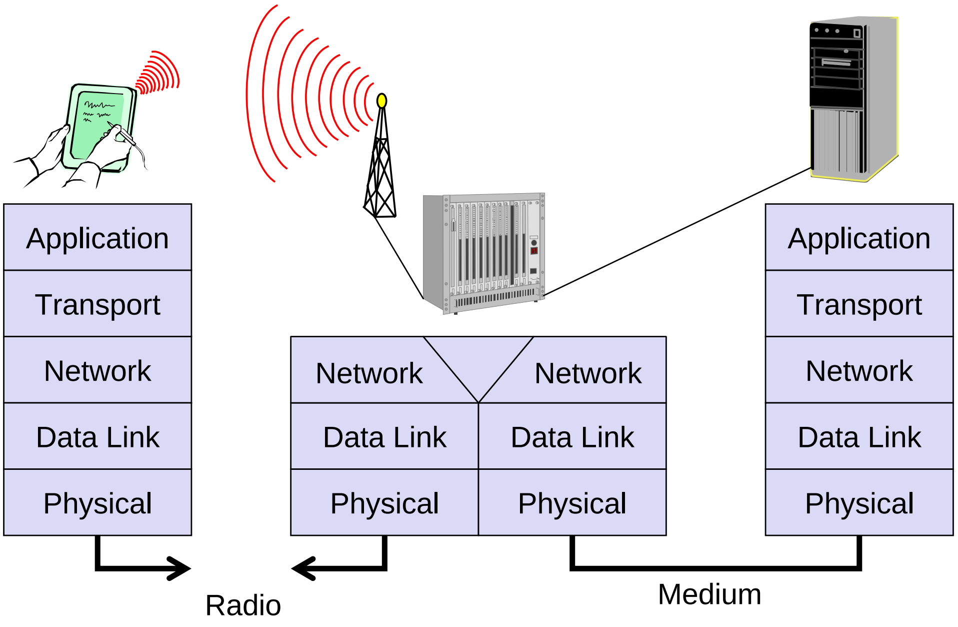
4G – fourth generation: when and how?

1.4.5. Wireless networks in comparison to fixed networks *JS*

- **Higher loss-rates due to interference**
  - **emissions of, e.g., engines**, lightning
- **Restrictive regulations of frequencies**
  - **frequencies have to be coordinated**, useful frequencies are almost all occupied
- **Low transmission rates**
  - local some Mbit/s, regional currently, e.g., **9.6kbit/s with GSM**
- **Higher delays, higher jitter**
  - **connection setup time** with GSM in the **second range**, several hundred milliseconds for other wireless systems
- **Lower security, simpler active attacking**
  - radio interface accessible for everyone, **base station can be simulated**, thus attracting calls from mobile phones
- **Always shared medium**
  - **secure access mechanisms important**

1.5. Mobile communication and the layer model *JS*

Wireless mobile communication obviously affects the **„last hop“.**
However, **tuning**, **changes** and/or **re-design** are also required in other places.



How mobile communication affects the layers

JS

Application layer	• service location • new applications, multimedia • adaptive applications
Transport layer	• congestion and flow control • quality of service
Network layer	• addressing, routing, • device location • hand-over
Data link layer	• authentication • media access • multiplexing • media access control
Physical layer	• encryption • modulation • interference • attenuation • frequency

2. Mobility across networks: Mobile IP

In this section, we study a **new mechanism**, which enables mobile devices to **move from one IP subnet to another … without changing** their **IP addresses**.

This mechanism, called **“Mobile IP”**,

- **solves** the **“macro” mobility management problem**
  Example: Change from one Ethernet segment to another or to WLAN or to UMTS or …
- is **less well suited** for **“micro” mobility management**
  Example: Handoff amongst wireless transceivers, each covering a small area.

2.1. Motivation for Mobile IP

2.2. Design goals, assumptions and outline of operation

2.3. Addressing with Mobile IP

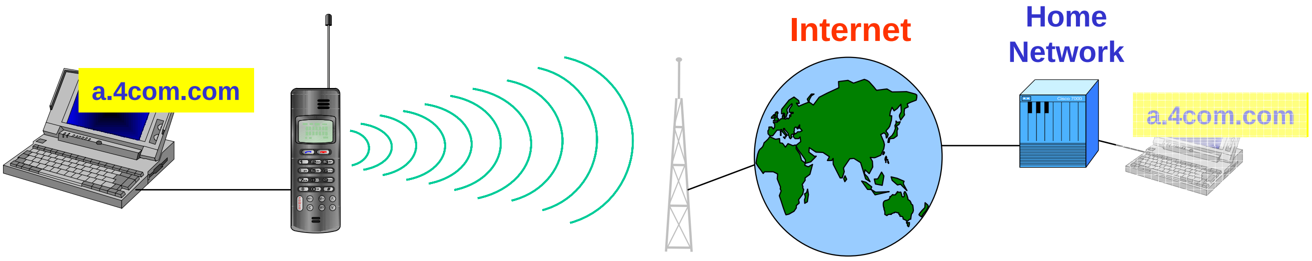
2.4. Routing with Mobile IP: Tunneling

2.5. Agent Advertisements

Note:

- We study **Mobile IPv4 only**: RFC 3344, Aug. 2002.
- Detailed information about Mobile IPv6 (RFC 3775, June 2004) is available at the IETF.

2.1. Motivation for Mobile IP



- Manager **X** of company 4com works in a hotel room and wants to **access documents on the company server** to finish a report. The hotel offers Internet access.

Transparency: X can work on his laptop like he does in his office.

- **Colleague Y** wants to **work on** parts of the **report**. He needs access to special software running in **X's** Laptop. How does **Y reach X's Laptop**?

• Transparency: The Laptop can always be reached using the same address.
• A static DNS name is possible !

- **X** needs to go to a meeting, **Y** is not ready yet. For this reason, **Y** wants to **download the document.** With the **download still active**, **X needs to go**.
- **X** starts the **Internet access via his mobile** (phone) and takes the laptop with him.

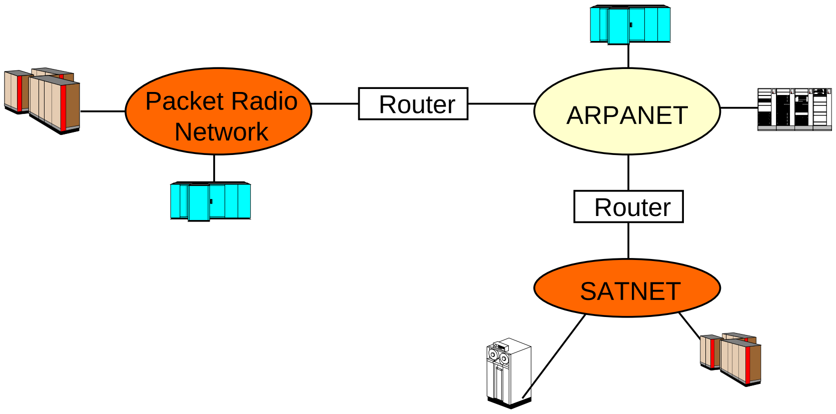
No interruption of active connections in case of network change !

Mobility in the Internet

... is as old as the Internet itself !

Spring 1973: Bob Kahn and Vint Cerf discuss about the interconnection of networks.

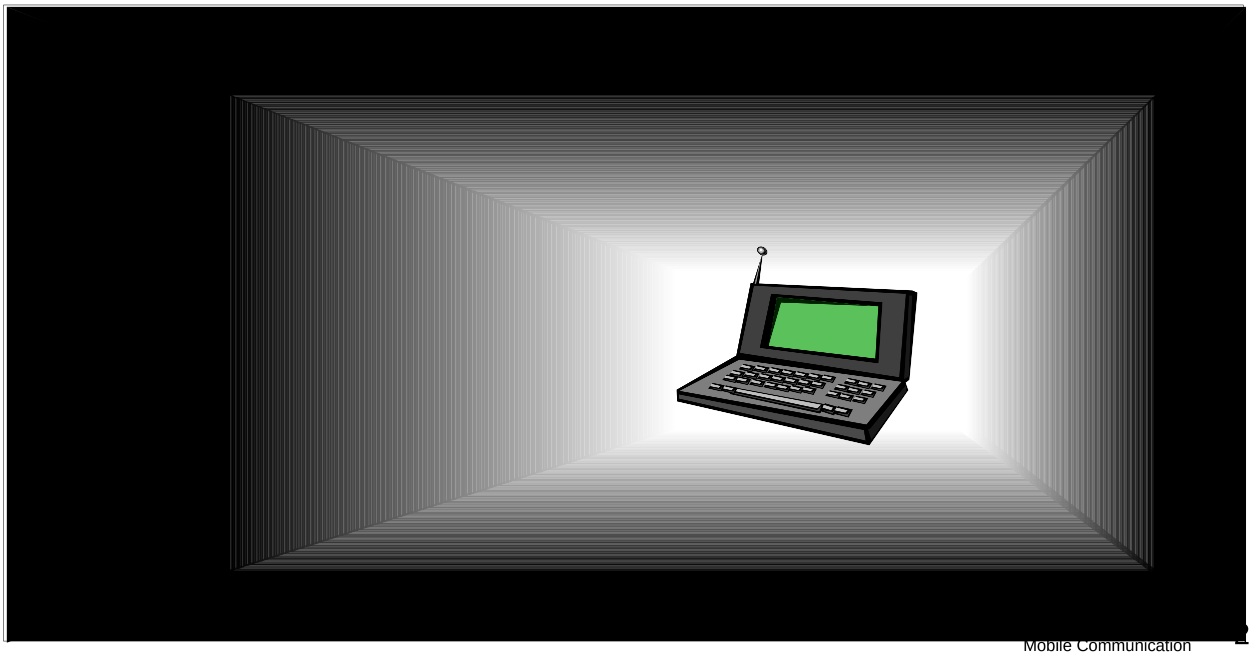
October 1977: The first 3-network-system (Packet Radio Network, SATNET, ARPANET).



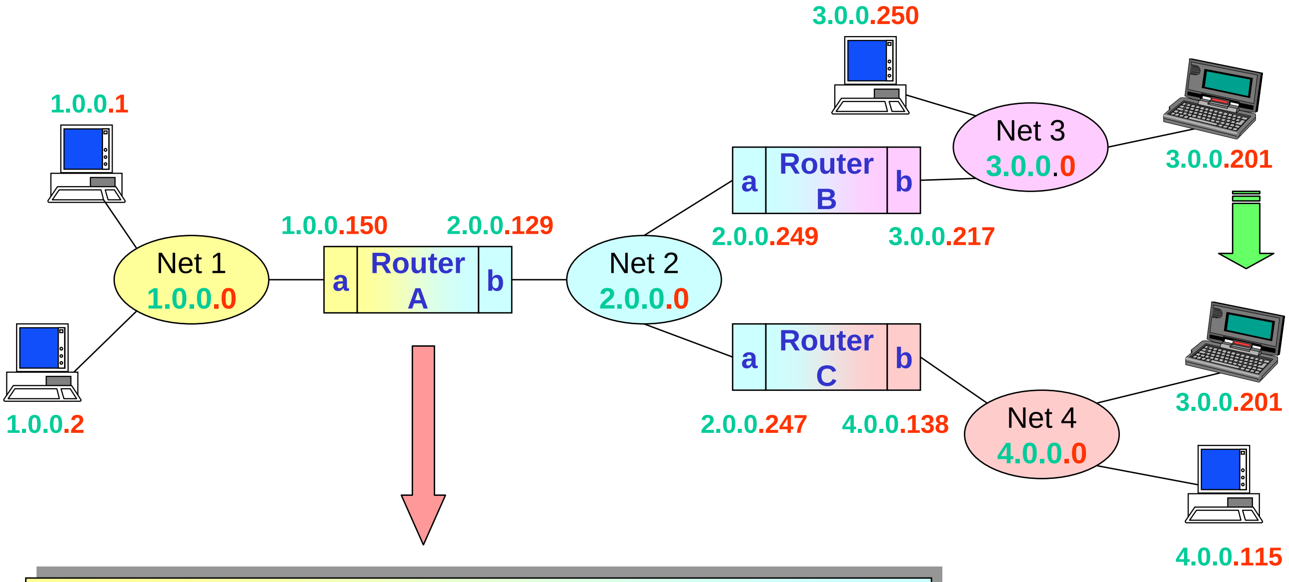
What‘s new in „Mobile IP“ ?

The Internet Engineering Steering Group (IESG) passed RFC 2002 „IP Mobility Support“ in June 1996. It was published in November 1996. The current version is RFC 3344.

Mobile IP supports mobility with transparent routing across networks.



Mobility across networks without Mobile IP ?

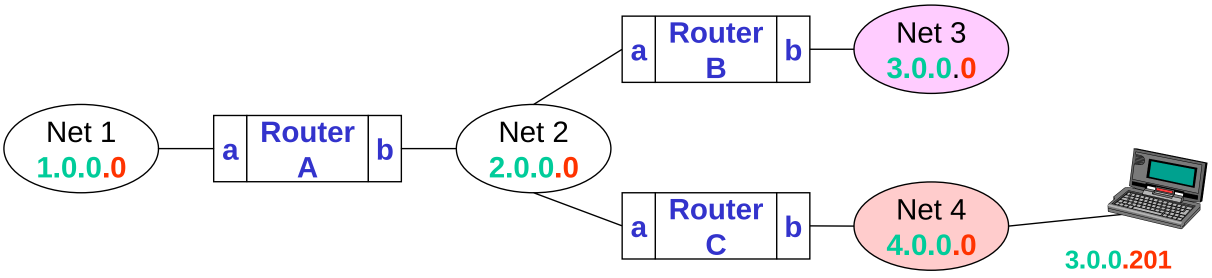


routing table

router A

Dest/Prefix	Send to	interface
1.0.0.0/24	Direct to dest	a
2.0.0.0/24	Direct to dest	b
3.0.0.0/24	2.0.0.249	b
4.0.0.0/24	2.0.0.247	b

Mobility across networks without Mobile IP (2) ?



a) Use the home address in the foreign network:

- **Station is not reachable**
  - IP address are structured hierarchically: (**netid**, **hostid**).
  - Routing across networks usually is based on the **netid** (efficiency !)
  - In this case, the mobile station is not reachable in the foreign network if using the home address !
- **Host-specific routing does not scale**
- **Risk of "confusion" in the foreign network**
  - Transmitting packets with foreign source-**netid** may cause unpredictable reactions.
    (A lot of protocols are based on the assumption of consistent netids inside subnetworks).

b) Use a new (foreign) address in the foreign network:

- **Station is not reachable**
  - Nobody knows the new address. For this reason, nobody sends messages to this address.
- **Interruption of TCP connections when changing the network**
  - TCP connections are identified by: (Source **IP-Address+Port**, Destination **IP-Address+Port**).

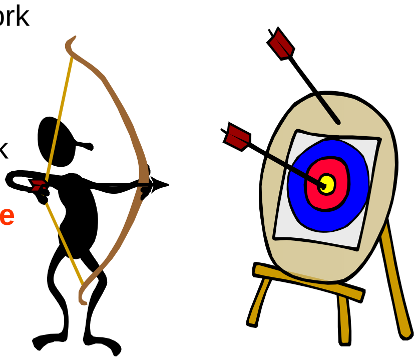
2.2. Design goals, assumptions and outline of operation

Mobility without IP address change

- **No change of IP address** when changing to a different network
  (e.g. when changing from Ethernet to Wireless LAN)

Mobility with active connections

- **Active TCP connections survive** change to different network



Smooth integration into the existing wired network structure

- **No change to hosts** in existing networks;
  however: full connectivity to these "conventional" stations.
- **No change to** existing **routers**;
  except where desired.

Protection against deviation attacks

- **Authentication** of all messages with location updates.

Optimization for wireless communication

- Significantly **reduced throughput** and **higher error rates** when compared to wired world.

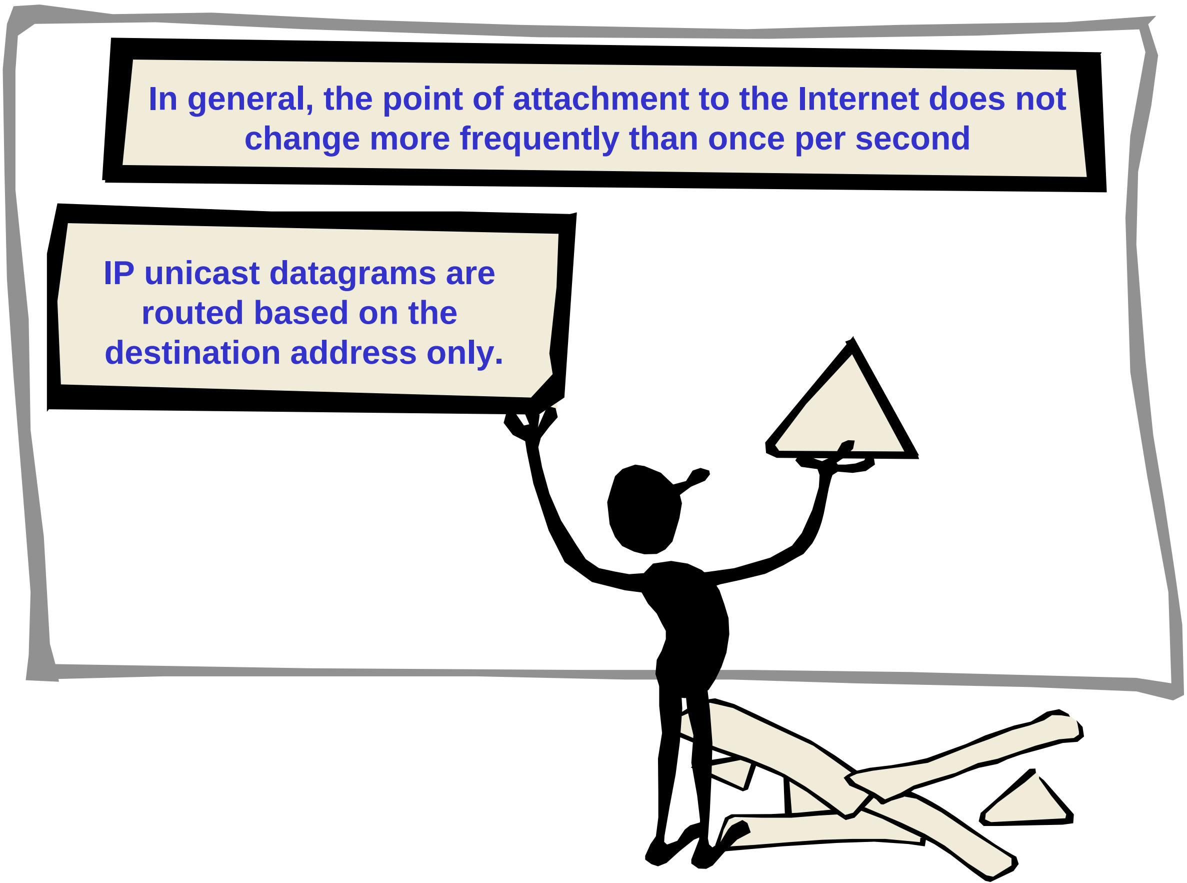
Optimization for end stations working on battery

- Keep the number and the length of **management messages to a minimum**!

Optimization for "macro-mobility"

- High overhead ok for **mobility across networks** (macro mobility).
- **Less suitable for handover** between cells (micro mobility).

Assumptions (RFC 3344)



In general, the point of attachment to the Internet does not change more frequently than once per second

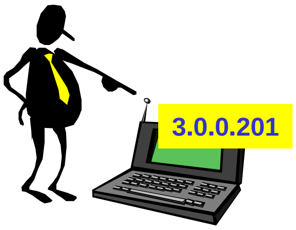
IP unicast datagrams are routed based on the destination address only.

Outline of operation (RFC 3344, pp. 10, 11)

- **Mobility agents** (i.e., foreign agents and home agents) **advertise their presence** via Agent Advertisement messages (Section 2). A mobile node may optionally solicit an Agent Advertisement message from any locally attached mobility agents through an Agent Solicitation message.
- A **mobile node** receives these Agent Advertisements and **determines whether** it is on its **home network or a foreign network**.
- **When** the mobile node detects that it is located **on its home network**, it operates **without mobility services**. **If returning to its home** network from being registered elsewhere, the mobile node **deregisters with its home agent**, through exchange of a Registration Request and Registration Reply message with it.
- When a **mobile node detects that it has moved to a foreign network**, it **obtains a care-of address** on the foreign network. The care-of address can either be determined from a foreign agent's advertisements (a foreign agent care-of address), or by some external assignment mechanism such as DHCP [13] (a co-located care-of address).
- The mobile node operating away from home then **registers its new care-of address with its home agent** through exchange of a Registration Request and Registration Reply message with it, possibly via a foreign agent (Section 3).
- **Datagrams sent to the mobile node's home address** are **intercepted by its home agent**, **tunneled** by the home agent **to** the mobile node's **care-of address**, received at the tunnel endpoint (either at a foreign agent or at the mobile node itself), and **finally delivered to the mobile node** (Section 5.2.3).
- In the **reverse direction**, datagrams sent by the mobile node are generally delivered to their destination using **standard IP routing mechanisms**, not necessarily passing through the home agent.

2.3. Addressing with Mobile IP

1. Each mobile station gets a **home IP address**.
   This is the identification independent from the current location.



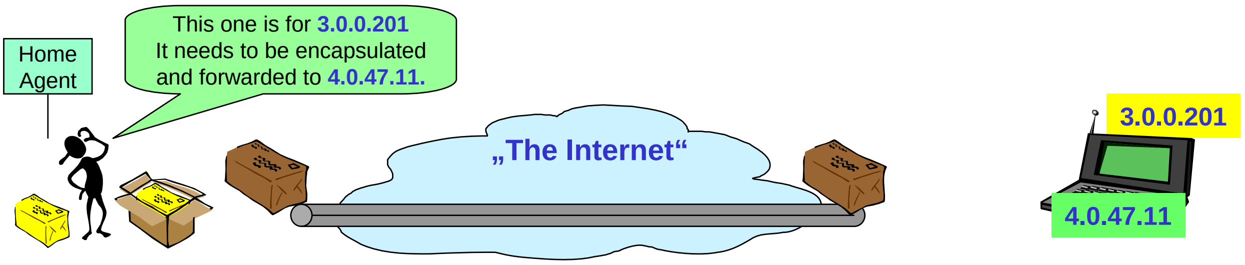
2. Whenever visiting a **foreign network**, the mobile station is additionally assigned a **care-of address (CoA)**.
   The CoA reflects the **current Internet access.**

3.0.0.201
4.0.47.11

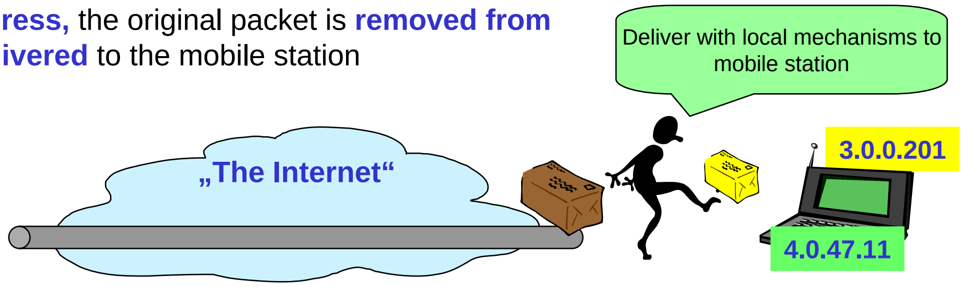
3. Mobile IP makes sure that the **care-of address** is communicated to the „**Home Agent**“.

Transparent routing to mobile stations

4. The **Home Agent forwards** IP packets destined to the mobile station **via** a **tunnel to** the **care-of address.**


Home Agent
This one is for 3.0.0.201
It needs to be encapsulated
and forwarded to 4.0.47.11.
„The Internet“
3.0.0.201
4.0.47.11

5. At the **care-of address,** the original packet is **removed from the tunnel** and **delivered** to the mobile station



Home Agent and Foreign Agent

A Home Agent

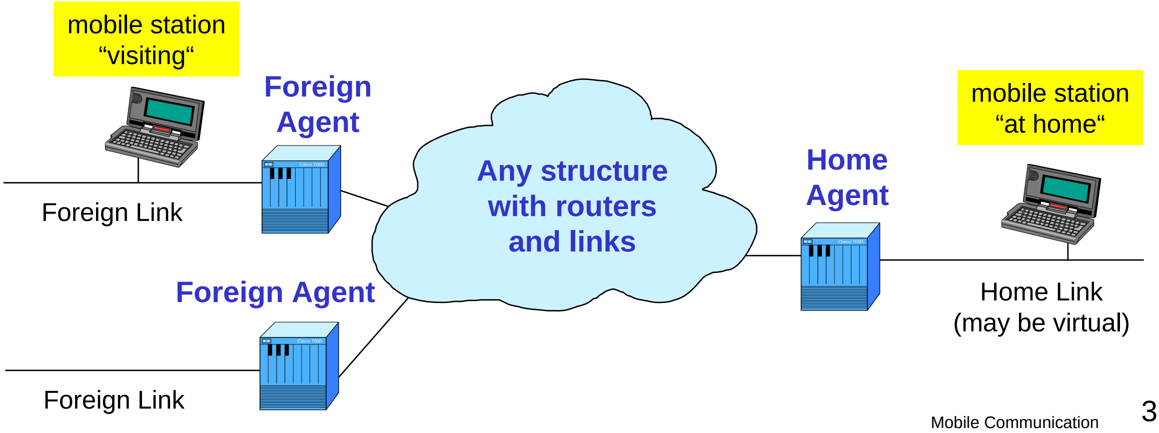
is a **router** interconnected to the home link of the mobile station which

- **knows** the **current care-of address** of the mobile station,
- **intercepts packets** destined to the home address of the mobile station and **tunnels** these packets to the care-of address.

A Foreign Agent

is a **router** interconnected to the foreign link of the mobile station which

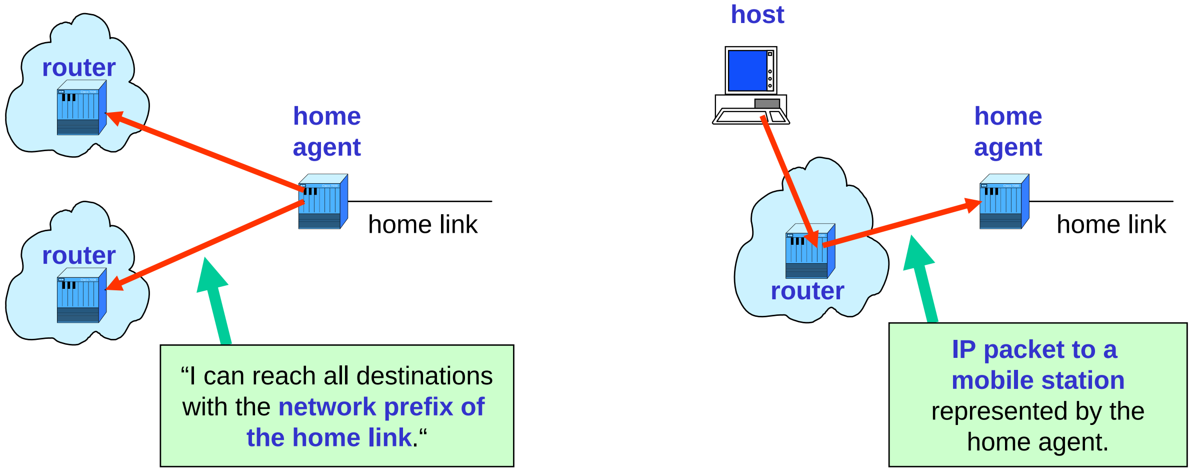
- **supports** the mobile station when communicating its **care-of address**,
- may allocate the **care-of address** and
- **decapsulates** tunneled packets to the mobile station.



Intercepting packets to the mobile station

The **conventional routing mechanisms** used in the Internet make sure that packets sent to the home address of a mobile station are forwarded to the home link, i.e. to the home agent.

The **home agent intercepts** the packets **and "tunnels"** them to the care-of address.



"I can reach all destinations with the **network prefix of the home link**."

IP packet to a mobile station represented by the home agent.

Home address und home link

The „home address“

- is the **home IP address** of a mobile station,
- **does not change** when the network attachment of the mobile station is changed,
- **changes** as often and for the same reasons as the IP address of immobile stations,
- is **closely related to the home agent** and to the home link,
- is the **IP source address of** (almost) **all data packets** sent by the mobile station,
- is the **IP destination address of all data packets** destined to the mobile station.

The home link

- is **defined by** the **network prefix** of the IP address **of the mobile station**,
- may be **real** (a corresponding physical medium exists),
- may be **virtual** (there is nothing but software in the Home Agent).

  → In this case, the mobile station is never at home.

Care-of address

A „care-of address“

- is an **IP address** allocated to the mobile station **in the foreign network**,
- is **specific for** the currently visited **foreign network**,
- **changes** when changing the **visited network**,
- identifies the **end of a mobile IP tunnel**,
- is **not the source address of “ordinary” data packets** sent by the mobile station (but: source address of Mobile IP specific packets),
- is **not known to DNS.**

A Foreign Agent care-of address

- is an **IP address of a Foreign Agent** (identifying a specific network attachment),
- may be allocated to **many mobile stations at the same time.**

A Co-located care-of address

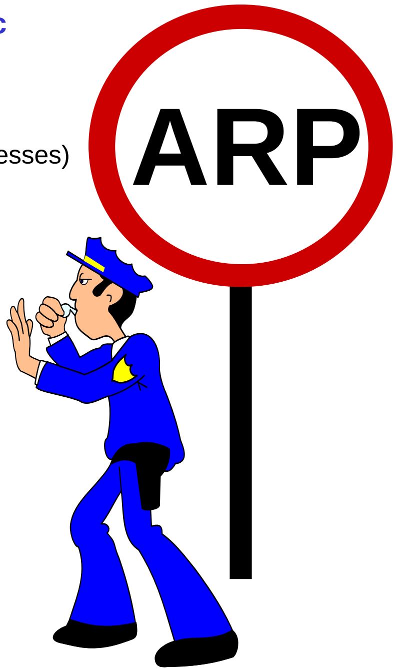
- is an **IP address currently allocated to** a network attachment of the mobile station,
- must have the same **network prefix as the corresponding foreign link**,
- may be allocated **manually** or via **DHCP** (Dynamic Host Configuration Protocol).

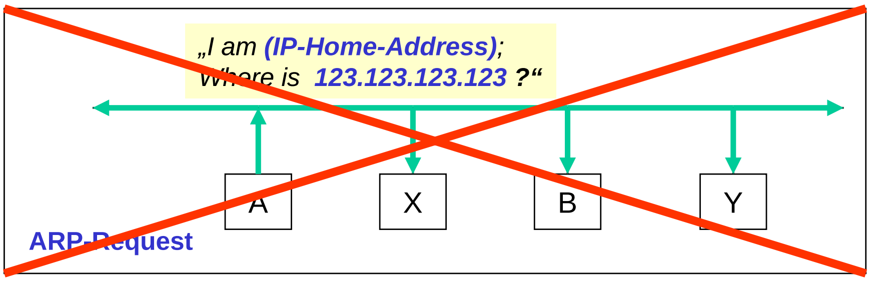
Addressing in the foreign network

The foreign link usually requires the mapping of **network-specific addresses.**

Challenge: **Address Translation / Address Mapping**
(Mapping of IP addresses to network-specific addresses)

How about … : **ARP** (Address Resolution Protocol) ?





„I am ***(IP-Home-Address)****;*
Where is ***123.123.123.123*** ***?“***

A X B Y

ARP-Request

But: This is **forbidden** !!!!

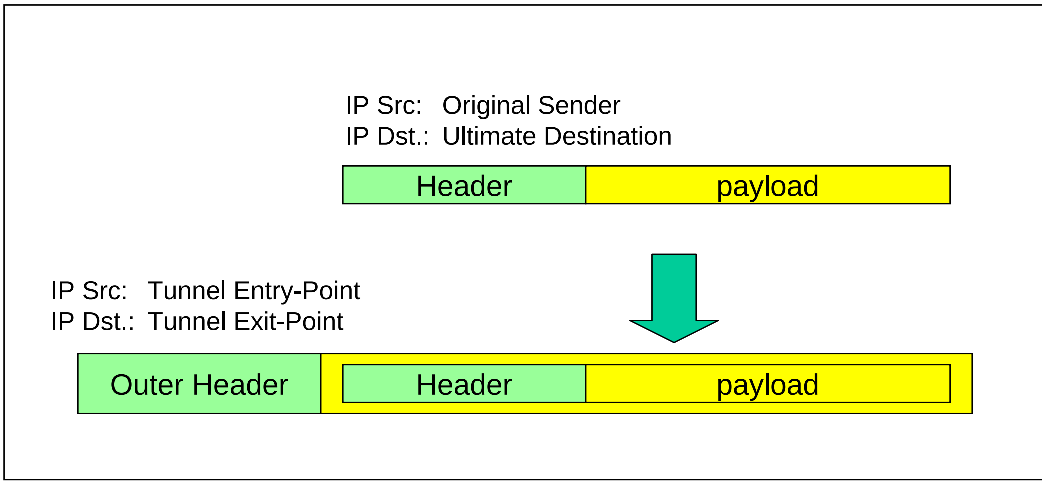
Why ? An ARP-Request with foreign IP source address may result in **significant confusion**.

While the mobile node is away from home,
it MUST NOT transmit any broadcast ARP Request or ARP Reply messages.
RFC 3344, IP Mobility Support for IPv4, Aug. 2002

2.4. Routing with Mobile IP: Tunneling

A tunnel

is a **path** followed by an IP packet while **encapsulated**.
Tunnels have well-defined starting and termination points.

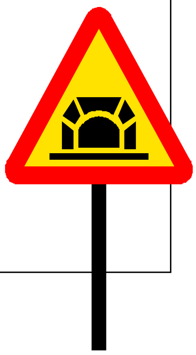


IP Src: Original Sender
IP Dst.: Ultimate Destination

Header	payload

IP Src: Tunnel Entry-Point
IP Dst.: Tunnel Exit-Point

Outer Header	Header	payload



Tunneled packets carry the “IP”-ID in the **„protocol“ field of the IP-Header: ”IP in IP“**.

Tunnel en-/decapsulation using a virtual interface

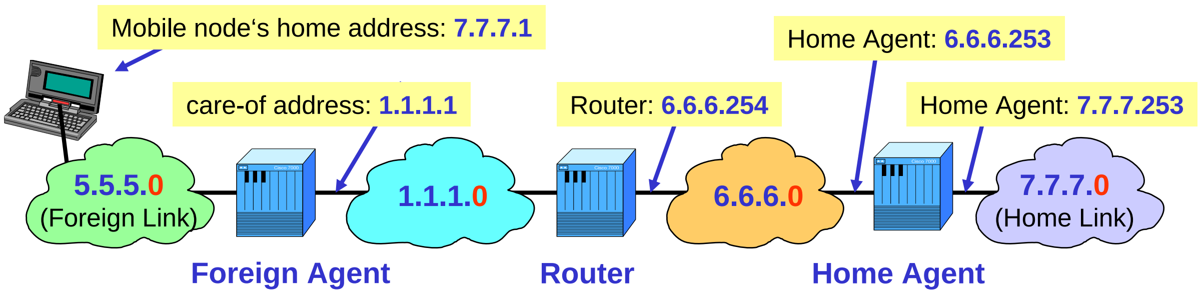
Tunnel encapsulation may be done using a virtual interface:

Encapsulation: The original packet is encapsulated into a packet to the care-of address.

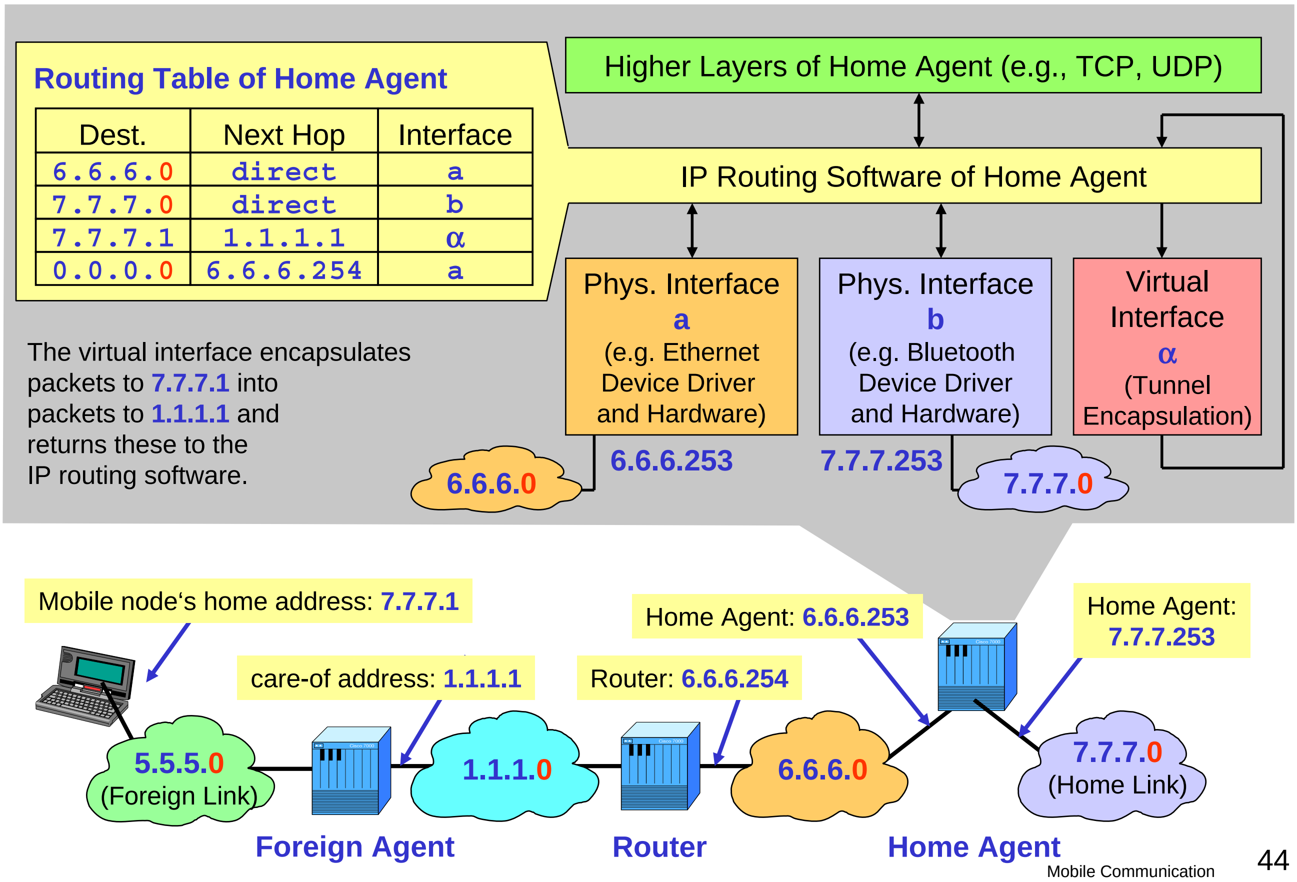
Decapsulation: The virtual interface at the care-of address unpacks the original packet.

Example:

7.7.7.0 the home link of a mobile station
6.6.6.0 an additional IP subnetwork to which the Home Agent is attached
7.7.7.1 the Home Address of a mobile station
1.1.1.1 the care-of address of the same mobile station
6.6.6.254 the IP address of the Default Router of the Home Agent
6.6.6.253 the IP address of the Home Agent in IP subnetwork 6.6.6.0
7.7.7.253 the IP address of the Home Agent in IP subnetwork 7.7.7.0



Encapsulation by virtual interface



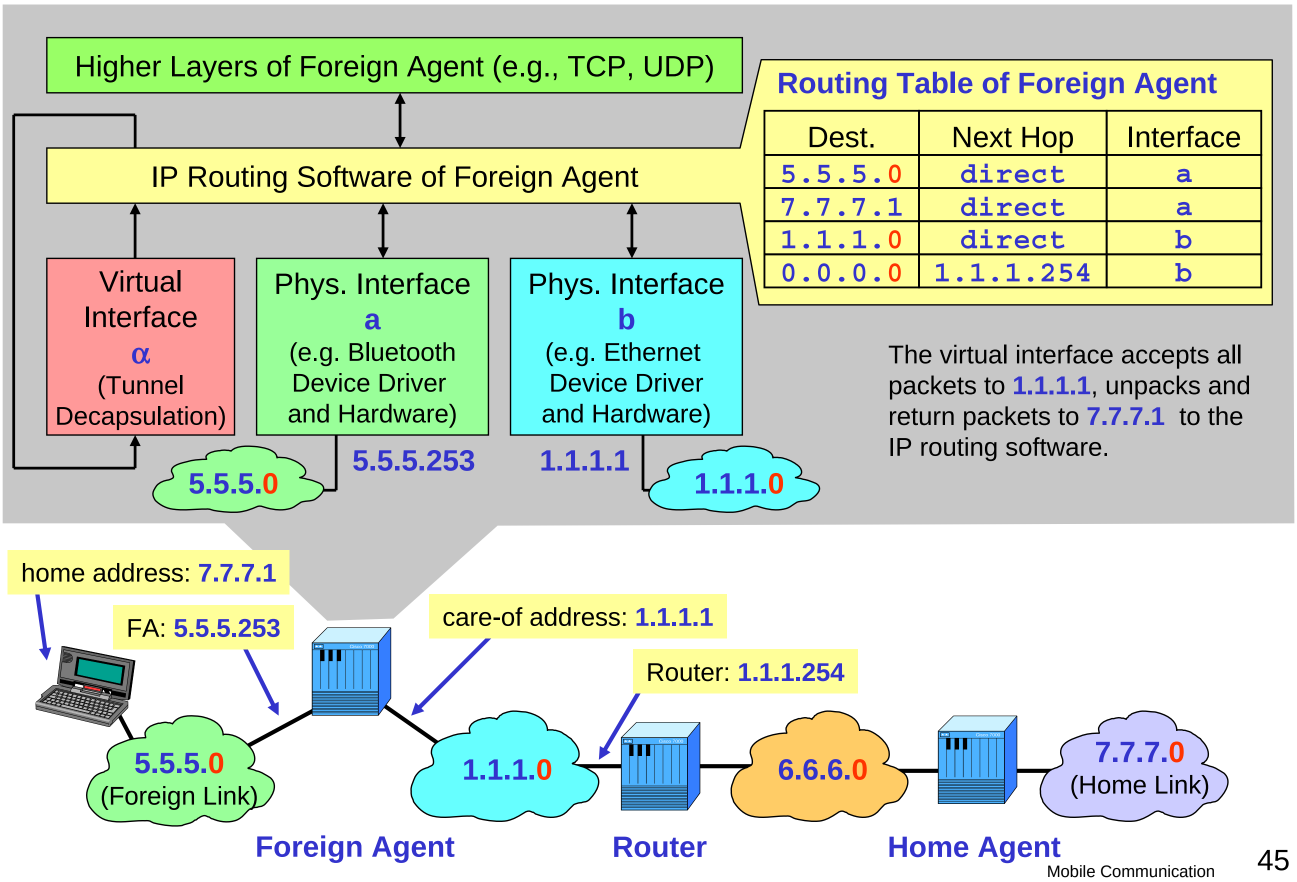
Routing Table of Home Agent

Dest.	Next Hop	Interface
6.6.6.0	direct	a
7.7.7.0	direct	b
7.7.7.1	1.1.1.1	α
0.0.0.0	6.6.6.254	a

The virtual interface encapsulates packets to 7.7.7.1 into packets to 1.1.1.1 and returns these to the IP routing software.

Higher Layers of Home Agent (e.g., TCP, UDP)
IP Routing Software of Home Agent
Phys. Interface a (e.g. Ethernet Device Driver and Hardware)
Phys. Interface b (e.g. Bluetooth Device Driver and Hardware)
Virtual Interface α (Tunnel Encapsulation)
6.6.6.253
7.7.7.253
6.6.6.0
7.7.7.0
Mobile node‘s home address: 7.7.7.1
care-of address: 1.1.1.1
Router: 6.6.6.254
Home Agent: 6.6.6.253
Home Agent: 7.7.7.253
5.5.5.0
(Foreign Link)
1.1.1.0
6.6.6.0
7.7.7.0
(Home Link)
Foreign Agent
Router
Home Agent

Decapsulation by virtual interface

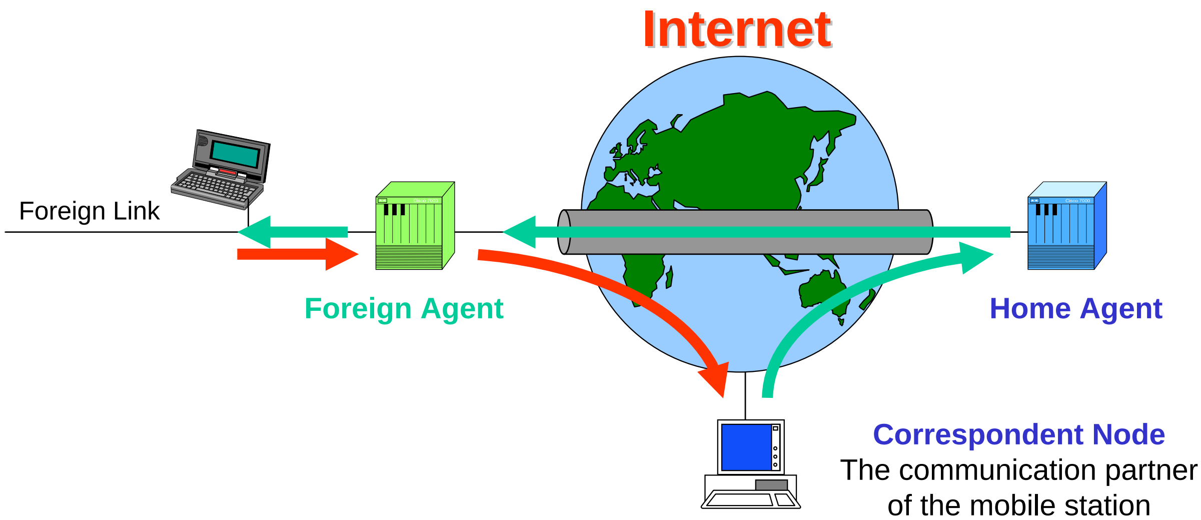

Higher Layers of Foreign Agent (e.g., TCP, UDP)
IP Routing Software of Foreign Agent
Virtual Interface α (Tunnel Decapsulation)
Phys. Interface a (e.g. Bluetooth Device Driver and Hardware)
Phys. Interface b (e.g. Ethernet Device Driver and Hardware)
5.5.5.0
5.5.5.253
1.1.1.1
1.1.1.0
home address: 7.7.7.1
FA: 5.5.5.253
care-of address: 1.1.1.1
Router: 1.1.1.254
5.5.5.0 (Foreign Link)
1.1.1.0
6.6.6.0
7.7.7.0 (Home Link)
Foreign Agent
Router
Home Agent

Routing Table of Foreign Agent

Dest.	Next Hop	Interface
5.5.5.0	direct	a
7.7.7.1	direct	a
1.1.1.0	direct	b
0.0.0.0	1.1.1.254	b

The virtual interface accepts all packets to **1.1.1.1**, unpacks and return packets to **7.7.7.1** to the IP routing software.

Triangle Routing



Correspondent Node
The communication partner
of the mobile station
In the Internet

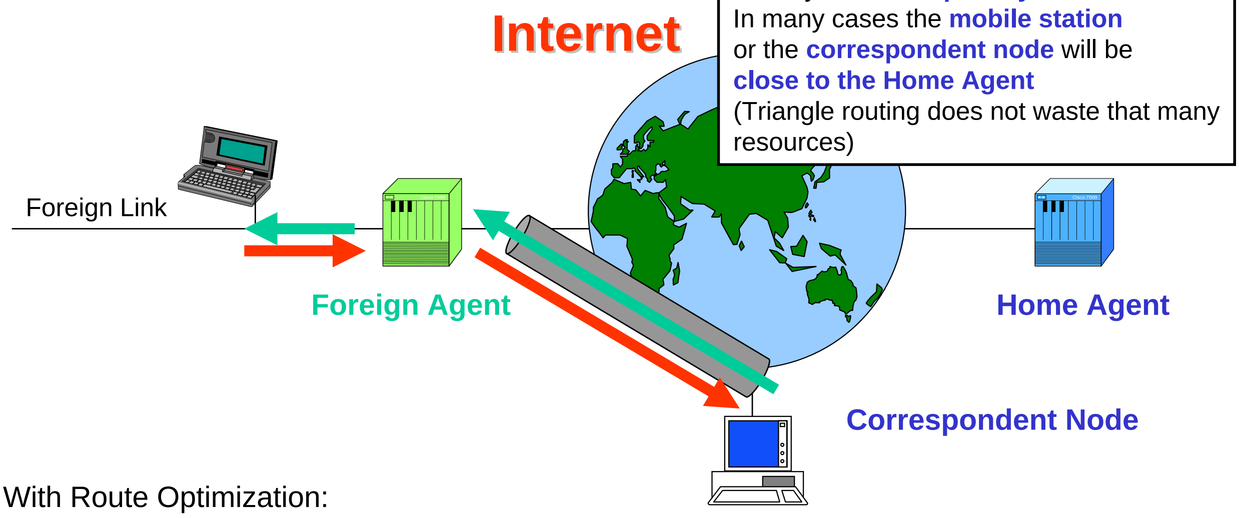
According to Mobile IP

- all packets are **sent directly from the mobile station to the correspondent node**,
- all packets **to the mobile station are sent to the Home Agent first** and tunneled from there to the mobile station.

For **security reasons** (location hiding) the IETF did not want to make other stations (= stations other than the Home Agents) aware of the care-of address (route optimization has later been added).

Route Optimization

In cases where there is no need for location hiding, routing may be optimized:



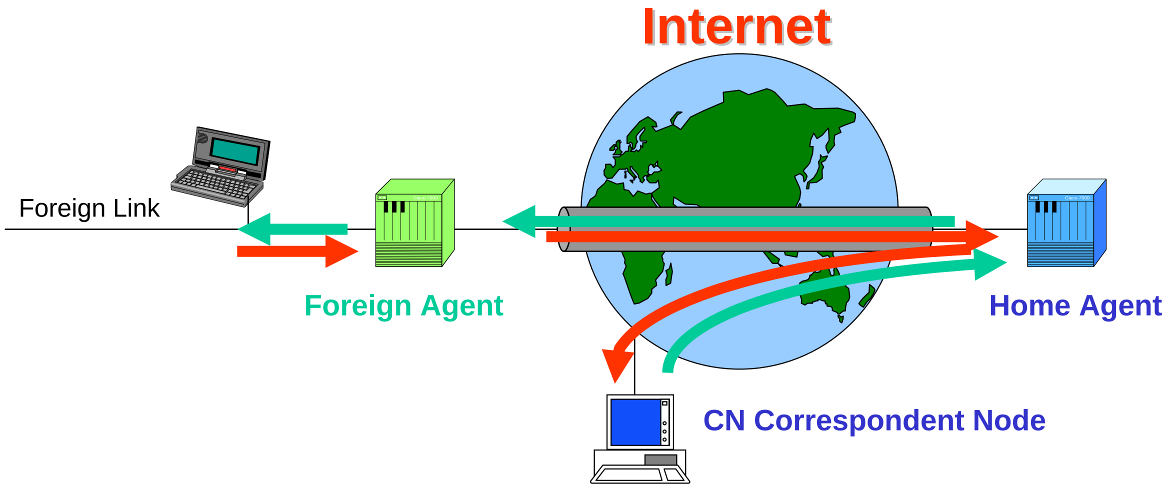
In early work: **low priority issue**:
In many cases the **mobile station** or the **correspondent node** will be **close to the Home Agent**
(Triangle routing does not waste that many resources)

With Route Optimization:

- the **care-of address** is **communicated to the communication partner,**
- this **“correspondent node” tunnels** directly to the care-of address,
- there could be a **significant vulnerability** (remote redirection) if the care-of address registration would not be authenticated.

Mobile IPv4 as specified in RFC 3344 does **not include** route optimization.

Reverse Tunneling (RFC 3024)

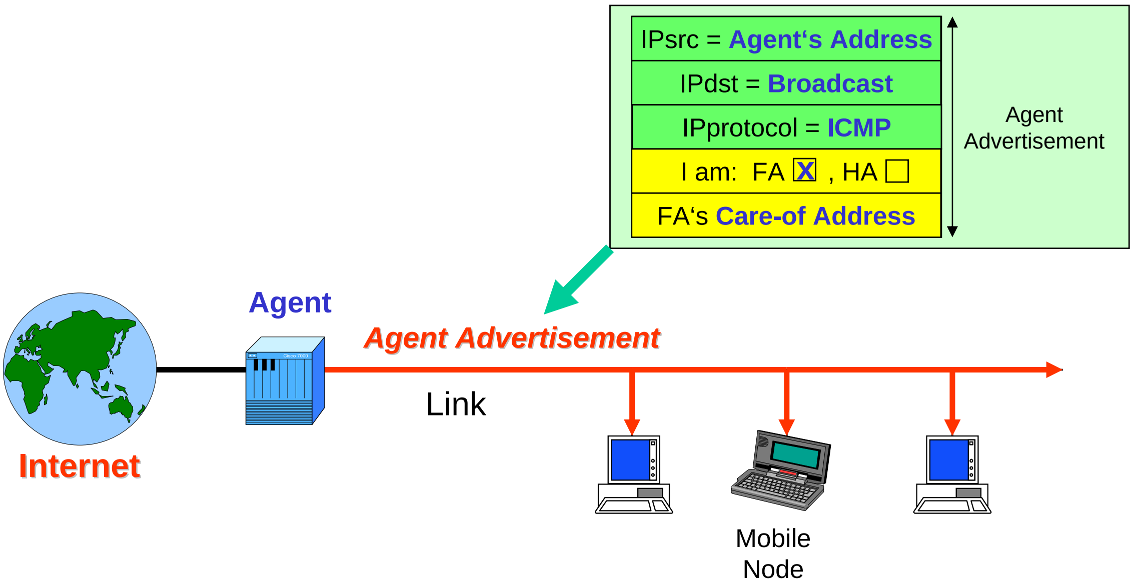


Many routers implement security policies such as „**ingress filtering**“ and “**egress filtering**” that do not allow forwarding of packets with a **Source Address** which appears **topologically incorrect**.

In these environments, mobile nodes may use “reverse tunneling” with the **care-of address as the Source Address.**

2.5. Agent Advertisements

Mobility agents transmit "Agent Advertisements" to advertise their services on the link.



Mobile devices analyze these Agent Advertisements. This way they

- **determine whether** they are **at home or on a foreign link**,
- **learn care-of addresses** of the corresponding Foreign Agents.

Reminder: IP datagrams

Network layer PDUs (OSI layer 3) are called "packets". In case of IP they are also called *Internet datagram*, short: *IP datagram*; even shorter: *datagram*.

Length in bytes				
1	Version		IHL	
1	type of service			
2	total length			
2	identification			
1	0	DF	MF	offset
1	offset (continued)			
1	time to live			
1	protocol			
2	header checksum			
4	source address			
4	destination address			
variable	options			
variable	padding			
	data			

precedence	D	T	R	unused

IPv4 datagrams

Reminder: Protocols identified by IP

In the “protocol” field, (among others) the following protocols are identified:

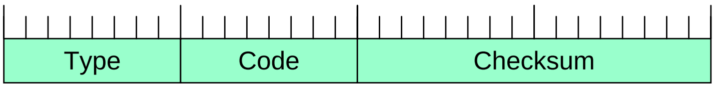
Decimal	Keyword	Protocol
0		Reserved
1	**ICMP**	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	**TCP**	Transmission Control
8	EGP	Exterior Gateway
17	**UDP**	User Datagram
29	ISO-TP4	ISO Transport Protocol Class 4
38	IDPR-CMTP	IPDR Control Messenger Transport Protocol
80	ISO-IP	ISO Internet Protocol (CLNP)
88	IGRP	IGRP (proprietary CISCO routing protocol)
89	**OSPF**	Open Shortest Path First
255		Reserved

Reminder: ICMP PDUs

It is desirable to allow routers and hosts to notify other stations about special events, errors etc. Here is where the

Internet Control Message Protocol (ICMP)

enters the scene. After the first 32 bits, the structure of the ICMP PDU strongly depends on the type field.



Type	ICMP Message
0	Echo Reply
3	**Destination Unreachable** (Datagram cannot be delivered, eg. destination host unknown)
4	**Source Quench** (Notification to the sender that the path to the destination is congested)
5	Redirect (A router tells a host to change the route)
8	**Echo Request** (“Ping“; testing the path to the destination and back to the sender)
9	**Router Advertisement** (A router tells about its existence)
10	**Router Solicitation** (A host looks for a router)
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request (Synchronization of clocks)
14	Timestamp Reply
15	Information Request
16	Information Reply

Mobility Agent Advertisement Extension (RFC 3344)

Originally, the IP addresses of routers in a specific subnetwork had to be configured manually. Then “ICMP Router Advertisement“ was specified in RFC 1256.
„Mobile IP“ is an extension of ICMP Router Advertisement.

1 Byte	1 Byte	1 Byte	1 Byte	
Vers = 4 IHL	Type of Service	Total Length		RFC 791: IP-Header
Identification		Flags Offset		
Time to Live **= 1**	Protocol **= ICMP**	Header Checksum		
Source Address **= address of home and/or foreign agent on this link**				
Dest. Add. **= 255.255.255.255 (broadcast) or 224.0.0.1 (multicast)**				
Type **= 9**	Code	Checksum		RFC 1256: ICMP Router Advertisement
Num Addrs	**Addr Entry Size**	**Lifetime (of this Advertisement)**		
Router Address [1]				
Preference Level [1]				
Router Address [2]				
Preference Level [2]				
...				
Type **= 16**	Length	Sequence Number		RFC 3344: Mobility Agent Advertisement Extension
(maximum) Registration Lifetime		R B H F M G r T	reserved	
Care-of Address [1]				
Care-of Address [2]				
...				
Type **= 19**	Length	Prefix-Length [1]	Prefix-Length [2]	Optional Prefix Length Extension
...				

Configuration for Mobile IP

“Everything” apart data transport:

1.a **Agent Advertisement**
Home and Foreign Agents periodically broadcast Agent Advertisements which are received by all nodes on the link

1.b **Agent Solicitation**
“Impatient” mobile nodes may “trigger” an Agent Advertisement

2. Mobile nodes (MN) **“examine” the Agent Advertisement** (home or foreign link?)

3. MN on foreign link **obtain care-of address (COA)**
(Foreign Agent COA from Advertisement, co-located COA manually/DHCP)

4. MN **registers the COA with its Home Agent** (possibly via Foreign Agent)

Now, **data transport** from and to MN is possible (previous slides).

When the **MN moves** to other foreign links or back to the home link:

5.a MN performs steps 1 - 4 to **register new location (new COA).**
Simultaneous binding of several COAs/several locations is possible.

5.b Returning to the **home link, MN “de”-registers** with Home Agent

Terminology (RFC 2002, RFC 3344)

RFC 2002 (Mobile IP) defines the following **new functional entities**:

Mobile Node

A host or router that **changes** its point of **attachment from one network** or subnetwork **to another.** A mobile node may change its location without changing its IP address; it **may continue to communicate** with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available.

Home Agent:

A router on a mobile node’s home network which **tunnels datagrams** for delivery **to the mobile node** when it is away from home, and **maintains current location information** for the mobile node.

Foreign Agent:

A router on a mobile node’s visited network which provides routing services to the mobile node while registered. The foreign agent **detunnels and delivers** datagrams to the mobile node that were tunneled by the mobile node’s home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

Terminology (2)

RFC 2002 (Mobile IP) defines the following important terms:

Agent Advertisement:

An advertisement message constructed by attaching a **special extension to a router advertisement** message.

Care-of Address:

The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of address: a “**foreign agent care-of address**” is an address of a foreign agent with which the mobile node is registered, and a “**co-located care-of address**” is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

Foreign Network:

Any network other than the mobile node’s **Home** Network.

Home Address:

An **IP address** that is assigned for an **extended period of time** to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Home Network:

A network, possibly virtual, having a **network prefix matching** that of a mobile node’s home address. Note that **standard IP routing** mechanisms will **deliver** datagrams destined **to** a mobile node’s Home Address to the mobile node’s **Home Network**.

Terminology (3)

Link:

A **facility or medium** over which nodes can communicate at the link layer. A link underlies the network layer.

Link-Layer Address:

The address used to identify an **endpoint of** some **communication over a physical link.** Typically, the Link-Layer address is an interface’s Media Access Control (MAC) address.

Mobility Agent:

Either a **home agent** or a **foreign agent.**

Mobility Binding:

The **association** of a **home address with a care-of address**, along with the **remaining lifetime** of that association.

Tunnel:

The **path** followed by a datagram **while** it is **encapsulated**. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

Virtual Network:

A network with **no physical instantiation beyond a router** (with a physical network interface on another network). The **router** (e.g., a home agent) generally **advertises reachability** to a virtual network using conventional routing protocols.

Visited Network:

A network other than a mobile node’s Home network, to which the mobile node is currently connected.