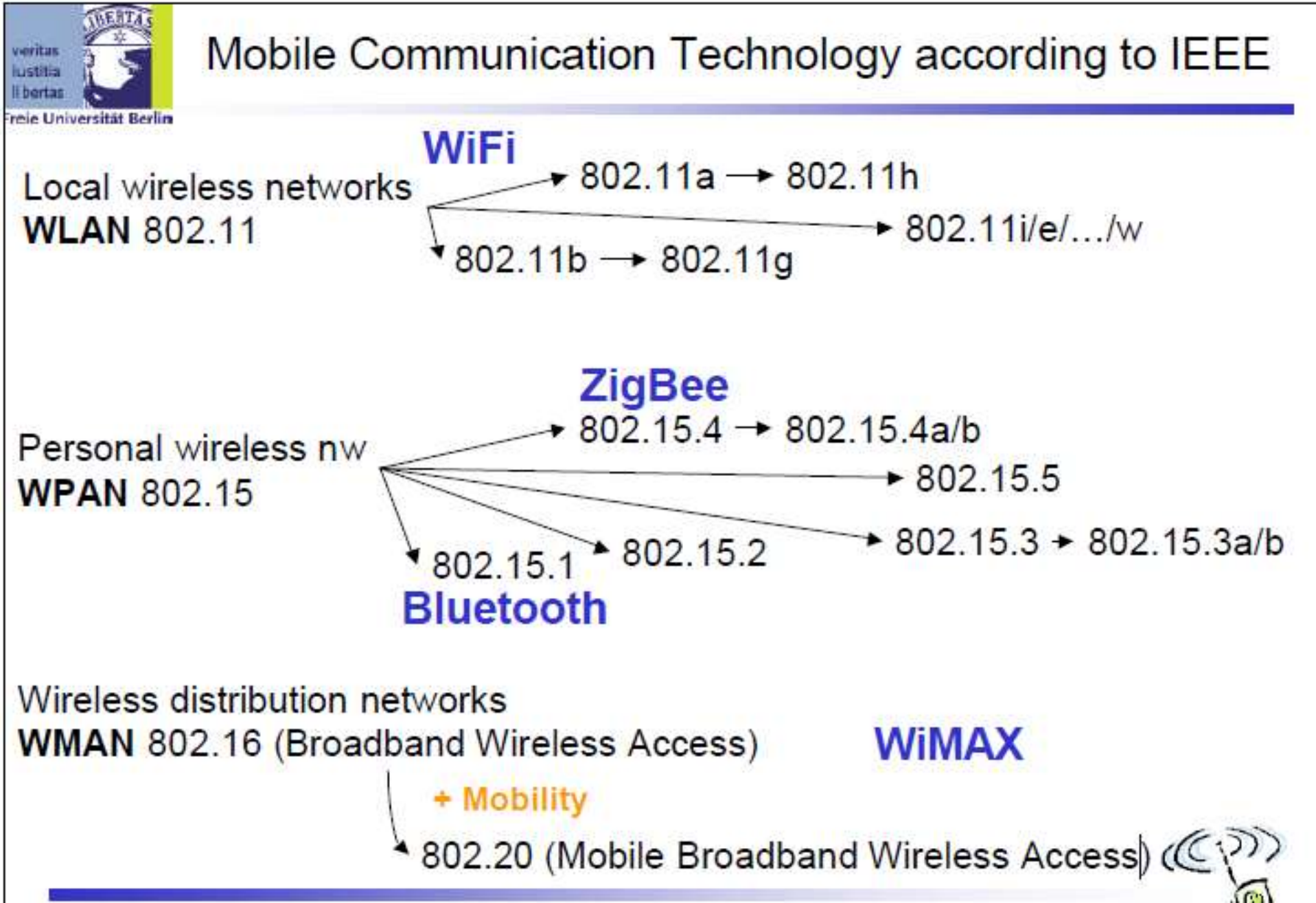
Wireless LAN (WLAN)

WLANs are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers.

The global goal of WLANs is to replace office cabling, to enable tetherless access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings.

Wireless LAN (WLAN)



Wireless LAN (WLAN)

Advantages:-

Flexibility: Very flexible within reception area
Within radio coverage, nodes can communicate without further restriction
Radio waves can penetrate walls, senders and receivers can be placed anywhere

No Planning: Ad-hoc networks do not need planning
No wiring difficulties

Robustness: Wireless networks can survive disasters, e.g., earthquakes
If the wireless devices survive, people can still communicate

Wireless LAN (WLAN)

Advantages:-

Flexibility

No Planning

Robustness

Design: Wireless networks allow for the design of small, independent devices which can for example be put into a pocket

Cost: After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost

Wireless LAN (WLAN)

Disadvantages :

Quality of service: WLANs typically offer lower quality
The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s)
Higher error rates due to interference
Higher delay/delay variation due to extensive error correction and detection mechanisms

Proprietary solutions: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features
However, these additional features only work when adapters from the same vendors are used for all wireless nodes

Wireless LAN (WLAN)

Disadvantages :

Quality of service
Proprietary solutions:
Restrictions: All wireless products have to comply with national regulations

Safety and security: Using radio waves for data transmission might interfere with other high-tech equipment
The open radio interface makes eavesdropping much easier in WLANs

Wireless LAN (WLAN)

Design goals for WLANs:

Global operation: should sell in all countries so, National and international frequency regulations have to be considered for WLAN products

Low power: Devices communicating via a WLAN are typically also wireless devices running on battery power

WAN design should take this into account and implement special power-saving modes and power management functions

License-free operation: WAN operators do not want to apply for a special license to be able to use the product

Equipment must operate in a license-free band, such as the 2.4 GHz ISM band

● **Robust transmission technology:**WLANs operate under difficult conditions Senders and receivers may move

Wireless LAN (WLAN)

Design goals for WLANs:

Easy to use: WLAN should not require complex management, but rather work on a plug-and-play basis

Safety and security: Wireless LANs should be safe to operate, especially regarding low radiation
Encryption mechanisms should be integrated
The networks should also take into account user privacy

Transparency for applications: Existing applications should continue to run over WLANs, the only difference being higher delay and lower bandwidth
The fact of wireless access and mobility should be hidden if it is not relevant, but the network should also support location aware applications, e.g., by providing location information

Types of Wireless LAN (WLAN)

I) Infrastructure based wireless networks
II) Ad-hoc wireless networks

I) Infrastructure based wireless networks:

Infrastructure networks provide access to other networks

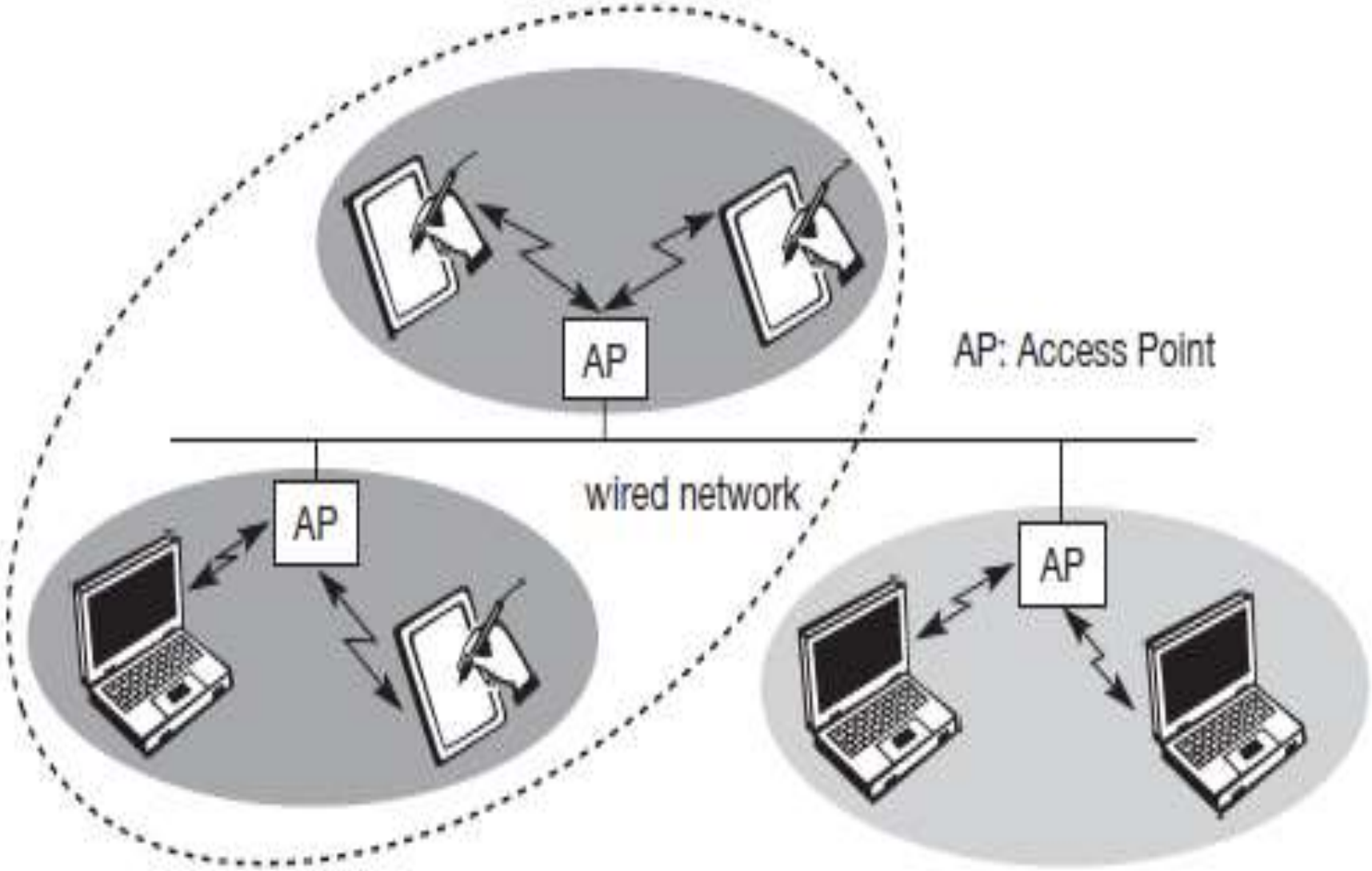
It includes forwarding functions,medium access control

In infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the **access point (AP)**, but not directly between the wireless nodes

The access point does not just control medium access, but also acts as a bridge to other wireless or wired networks

Types of Wireless LAN (WLAN)

I) Infrastructure based wireless networks:



Types of Wireless LAN (WLAN)

I) Infrastructure based wireless networks:

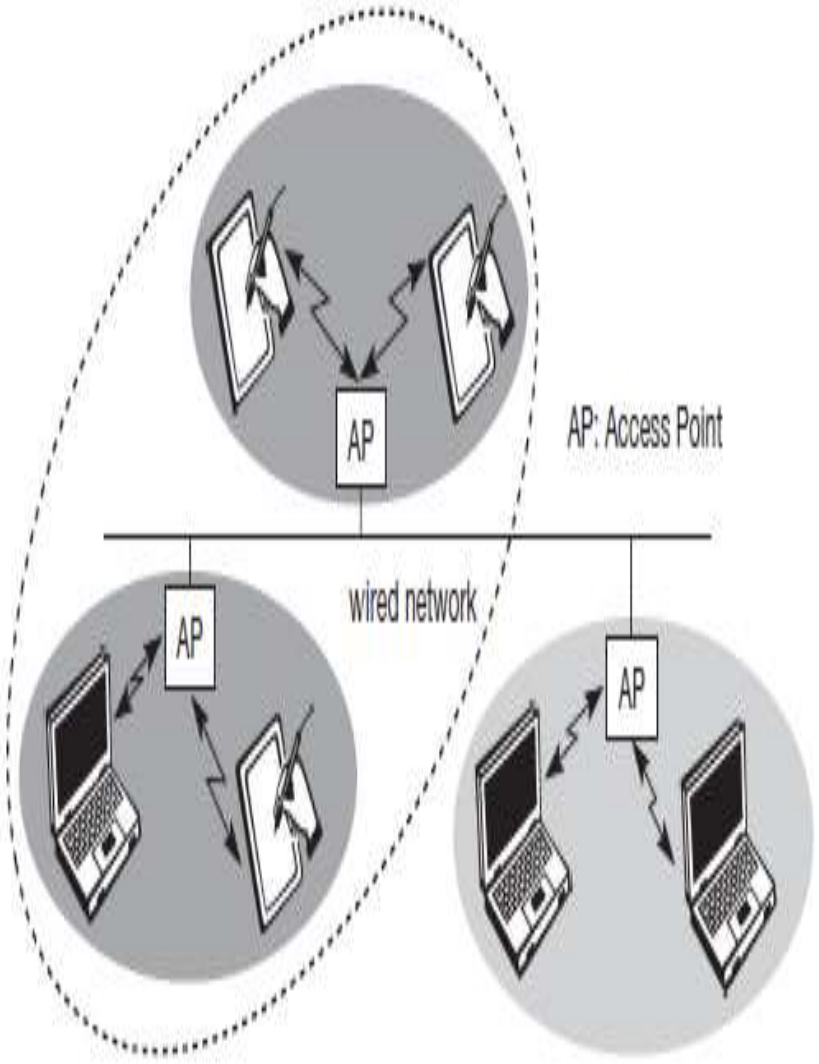


Figure shows three APs with their three wireless networks and a wired network

Several wireless networks may form one logical wireless network, so the access points together with the fixed network in between can connect several wireless networks to form a larger network beyond actual radio coverage

Types of Wireless LAN (WLAN)

I) Infrastructure based wireless networks:

The design of infrastructure-based wireless networks is simpler because most of the network functionality lies within the access point

If only the access point controls medium access, no collisions are possible

This setting may be useful for quality of service guarantees such as minimum bandwidth for certain nodes

The access point may poll the single wireless nodes to ensure the data rate

Types of Wireless LAN (WLAN)

I) Infrastructure based wireless networks:

Infrastructure-based networks lose some of the flexibility as they cannot be used for disaster relief in cases where no infrastructure is left

Typical cellular phone networks are infrastructure-based networks for a wide area

Satellite-based cellular phones have an infrastructure – the satellites

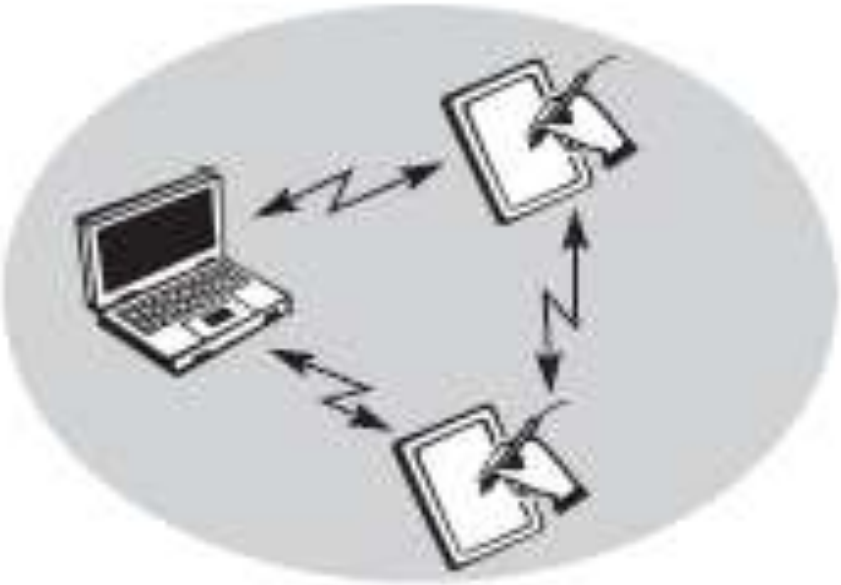
Infrastructure does not necessarily imply a wired fixed network

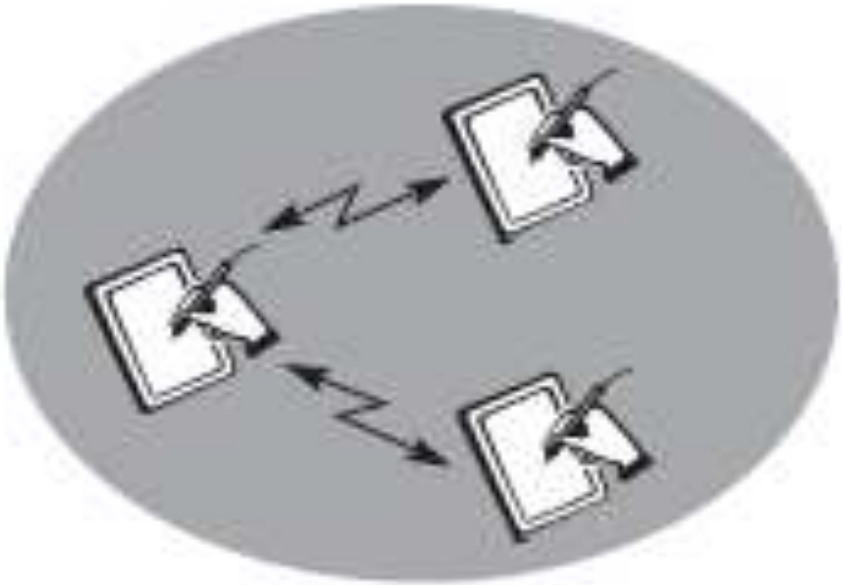
Types of Wireless LAN (WLAN)

II) Adhoc wireless networks:

Ad-hoc wireless networks, however, do not need any infrastructure to work

Each node can communicate directly with other nodes, so no access point controlling medium access is necessary





Types of Wireless LAN (WLAN)

II) Adhoc wireless networks:

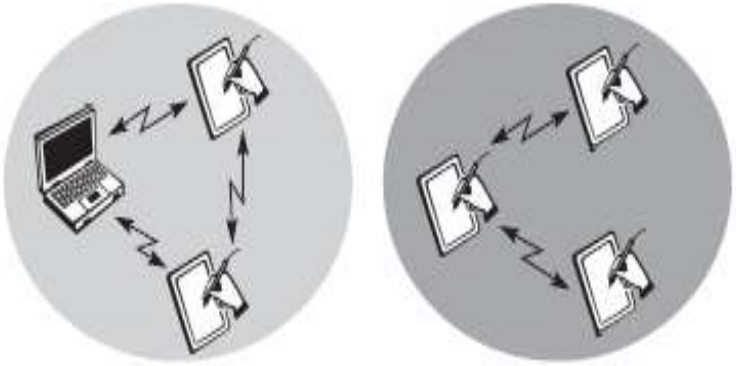


Figure shows two ad-hoc networks with three nodes each

Nodes within an ad-hoc network can only communicate if they can reach each other physically, i.e., if they are within each other's radio range or if other nodes can forward the message

Nodes from the two networks shown in Figure cannot, communicate with each other if they are not within the same radio range

Types of Wireless LAN (WLAN)

II) Adhoc wireless networks:

In ad-hoc networks, the complexity of each node is higher because every node in order to provide quality of service has to implement

- medium access mechanisms
- mechanisms to handle hidden / exposed terminal problems
- priority mechanisms

Adhoc wireless network exhibits the greatest possible flexibility

Adhoc networks only have selected nodes with the capabilities of forwarding data

Most of the nodes have to connect to such a special node first to transmit data if the receiver is out of their range

Eg.: Bluetooth is a typical wireless ad-hoc network

MAC belongs to layer 2, the **data link control layer (DLC)**

Layer 2 is subdivided into the

logical link control (LLC)	layer 2 b
MAC	layer 2 a

The main task of **DLC** is to

establish a reliable point to point

or

point to multi-point connection between different

devices over a wired or wireless medium.

Motivation for a specialized MAC

Whether it is possible to use MAC in wireless ?

Let us consider **carrier sense multiple access with collision detection, (CSMA/CD)** which works as follows.

A sender senses the medium (a wire or coaxial cable) to see if it is free.

If it is busy, the sender waits until it is free.

If it is free, the sender starts transmitting data and continues to listen into the medium.

If the sender detects a collision while sending, it stops at once and sends a jamming signal.

CSMA/CD is not really interested in collisions at the sender, but rather in those at the receiver.

Sender is the one detecting collisions.

This is not a problem using a wire, as more or less the same signal strength can be assumed all over the wire.

If a collision occurs somewhere in the wire, everybody will notice it..

In wireless networks **the strength of a signal decreases proportionally to the square of the distance to the sender.**

Obstacles attenuate the signal even further.

The sender may now apply carrier sense and detect an idle medium.

The sender starts sending – but a collision happens at the receiver due to a second sender.

The sender detects no collision and assumes that the data has been transmitted without errors.

But a collision might actually have destroyed the data at the receiver.

Collision detection is very difficult in wireless scenarios

So, this common MAC scheme from wired network fails in a wireless scenario.

Hidden and exposed terminals

Consider the scenario with three mobile phones as shown in following figure .

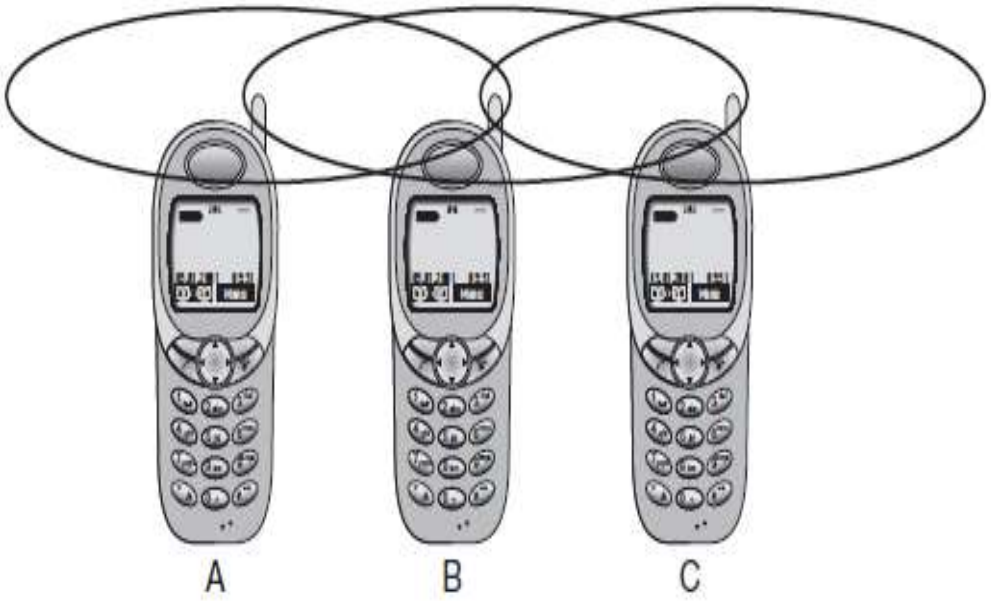


Figure 3.1
Hidden and exposed terminals

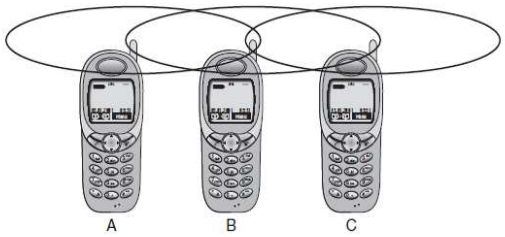


Figure 3.1
Hidden and
exposed terminals

The transmission range of A reaches B, but not C (the detection range does not reach C either).

The transmission range of C reaches B, but not A.

Finally, the transmission range of B reaches A and C.

A cannot detect C and vice versa.

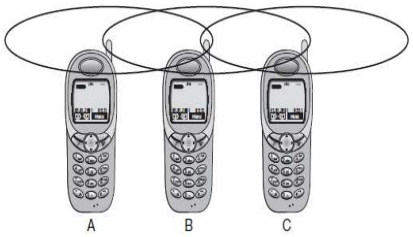


Figure 3.1
Hidden and exposed terminals

A starts sending to B, C does not receive this transmission.

C also wants to send to B and senses the medium.

Medium appears to be free, the carrier sense fails.

C also starts sending causing a collision at B.

But A cannot detect this collision at B and continues with its transmission.

A is **hidden** for C and vice versa.

Hidden terminals may cause collisions

B sends something to A and

C wants to transmit data to some other mobile phone outside the interference ranges of A and B.

C senses the carrier and detects that the carrier is busy (B's signal).

C postpones its transmission until it detects the medium as being idle again.

But as A is outside the interference range of C, waiting is not necessary

Causing a ‘collision’ at B does not matter because the collision is too weak to propagate to A.

In this situation, C is **exposed** to B.

Exposed terminal causes **unnecessary delay**

Near and far terminals

Consider the situation as shown in Figure

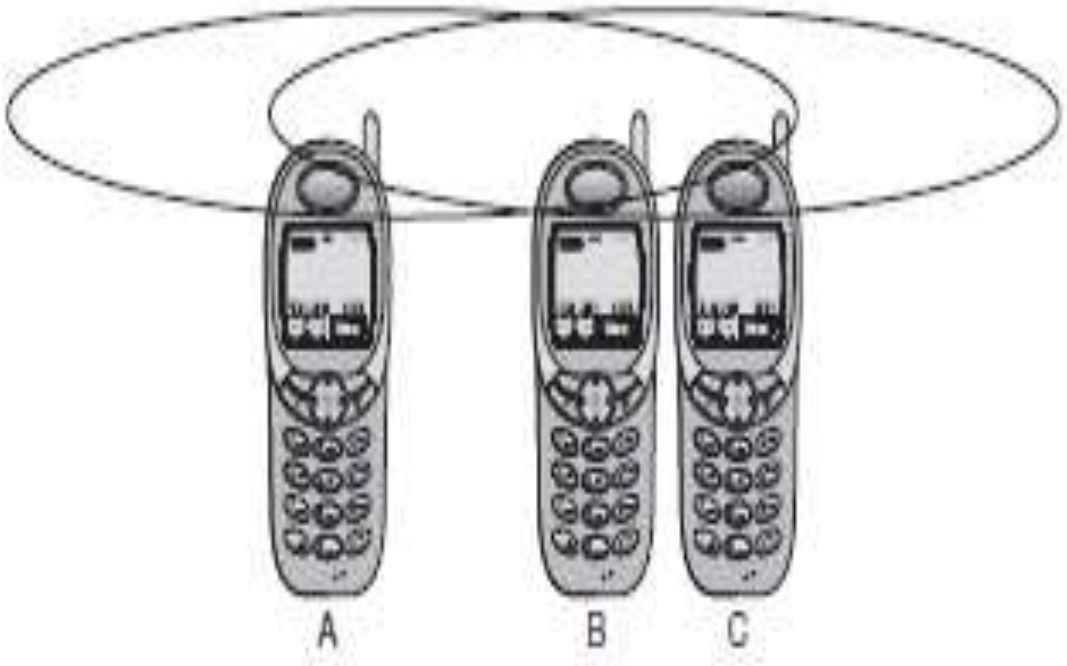


Figure 3.2
Near and far terminals

Near and far terminals

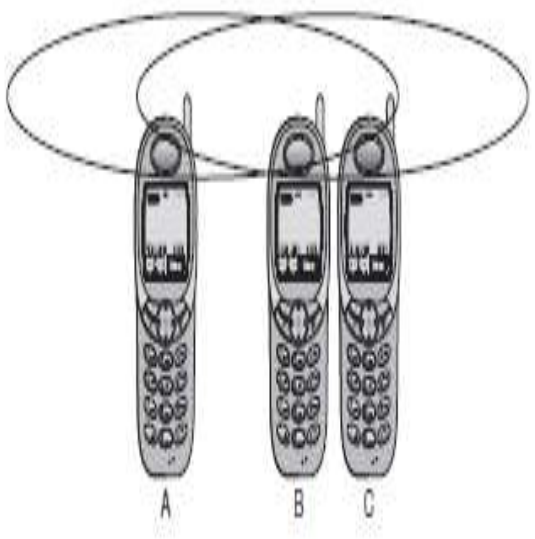


Figure 3.2
Near and far terminals

A and B are both sending with the same transmission power.

As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal.

As a result, C cannot receive A's transmission.

In this case, terminal B would already drown out terminal A on the physical layer.

C in return would have no chance of applying a fair scheme as it would only hear B.

The **near/far effect** is a severe problem of wireless networks using CDM.

All signals should arrive at the receiver with more or less the same strength.

Precise power control is needed to receive all senders with the same strength at a receiver.

Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks.

A typical application involves assigning an optimal base station to a mobile phone user.

The mobile phone may receive several base stations with different quality.

A MAC algorithm could decide which base station is best, taking into account which frequencies (FDM), time slots (TDM) or code (CDM).

Space Division Multiple Access (SDMA) SDMA is never used in isolation but always in combination with one or more other schemes.

Basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing **SDM**

Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the **frequency division multiplexing (FDM)**

Allocation can either be fixed or dynamic

Channels can be assigned to the same frequency at all times, i.e., **pure FDMA**,

or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA

Frequency division multiple access (FDMA)

FDMA combined with TDMA is the common practice to circumvent narrowband interference at certain frequencies, known as frequency hopping.

Sender and receiver have to agree on a hopping pattern.

Hopping patterns are typically fixed, at least for a longer period.

Frequency division multiple access (FDMA)

FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks.

Here the two partners typically establish a **duplex channel**, i.e., a channel that allows for simultaneous transmission in both directions.

Frequency division multiple access (FDMA).

Here the two partners typically establish a **duplex channel**, i.e., a channel that allows for simultaneous transmission in both directions.

The two directions, mobile station to base station and vice versa are now separated using different frequencies.

This scheme is then called **frequency division duplex (FDD)**.

Frequency division multiple access (FDMA).

In **FDD** both partners have to know the frequencies in advance.

Two frequencies are also known as **uplink**, i.e., from mobile station to base station or from ground control to satellite

and as **downlink**, i.e., from base station to mobile station or from satellite to ground control.

As for example FDM and FDD, following figure shows the situation in a mobile phone network based on the GSM standard for 900 MHz

The basic frequency allocation scheme for GSM is fixed

All uplinks use the band between **890.2 and 915 MHz**

All downlinks use band between **935.2 to 960 MHz**

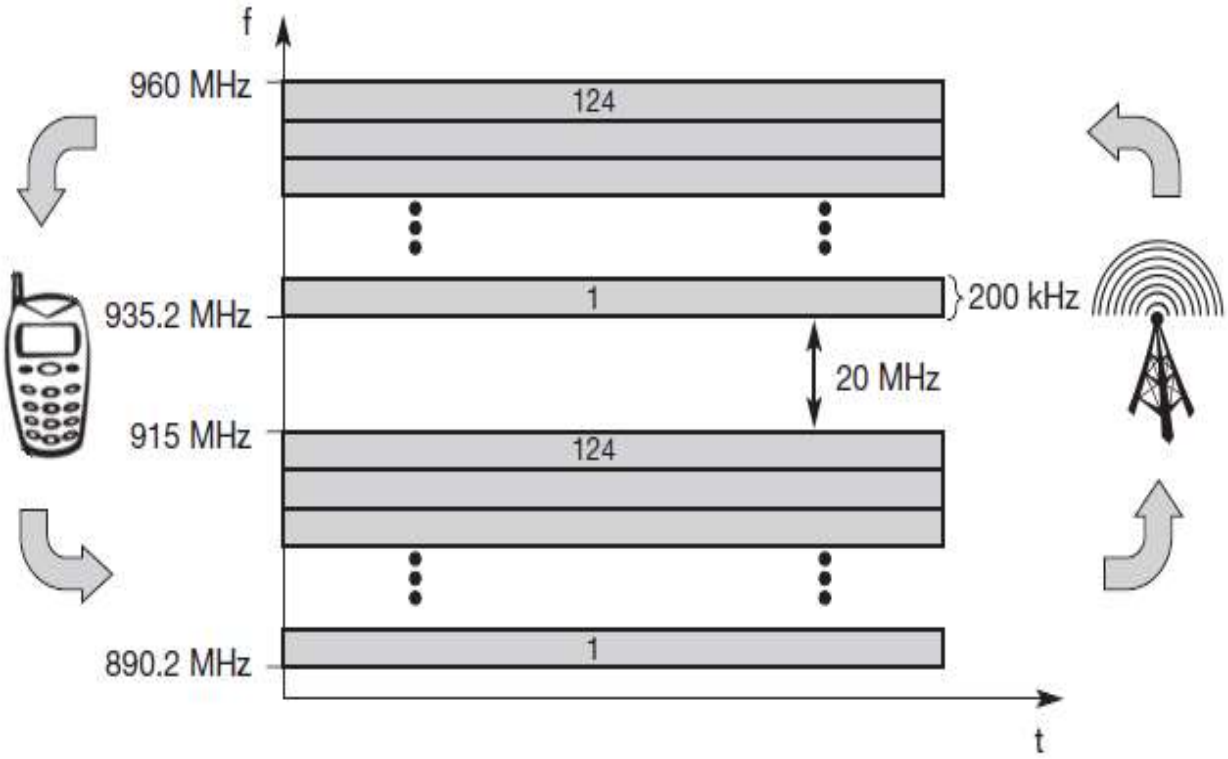


Figure 3.3
Frequency division multiplexing for multiple access and duplex

The base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone.

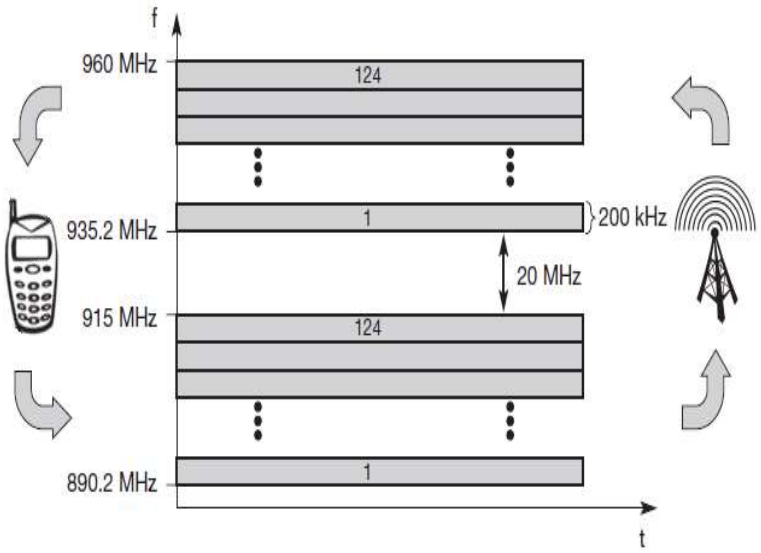


Figure 3.3
Frequency division multiplexing for multiple access and duplex

Up- and downlink have a fixed relation

For a certain channel n.

If uplink frequency is **fu = 890 MHz + n·0.2 MHz**

the downlink frequency is **fd = fu + 45 MHz**

i.e., **fd = 935 MHz + n·0.2 MHz**

The base station selects the channel

Each channel (uplink and downlink) has a bandwidth of 200 kHz.

The use of FDM for multiple access allows **124** channels per direction are available

Time division multiple access (TDMA)

TDMA comprises all technologies that allocate certain time slots for communication **TDM**

The receiver can stay at the same frequency the whole time

Using only one frequency, and thus very simple receivers and transmitters

Listening to many channels separated in time at the same frequency is simple.

Time division multiple access (TDMA)

Now synchronization between sender and receiver has to be achieved in the time domain.

This can be done by using a fixed pattern i.e., allocating a certain time slot for a channel

or by using a dynamic allocation scheme

Dynamic allocation schemes require an identification for each transmission e.g., sender address or the transmission has to be announced beforehand.

MAC addresses are quite often used as identification.

This enables a receiver in a broadcast medium to recognize if it really is the intended receiver of a message.

Fixed schemes do not need an identification, but are not as flexible considering varying bandwidth requirements.

The following sections present several examples for fixed and dynamic schemes as used for wireless transmission.

Typically, those schemes can be combined with FDMA to achieve even greater flexibility and transmission capacity.

Fixed TDM

The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern.

This results in a fixed bandwidth and is the typical solution for wireless phone systems.

MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment.

If this synchronization is assured, each mobile station knows its turn and no interference will happen.

The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.

Fixed access patterns (at least fixed for some period in time) fit perfectly well for connections with a fixed bandwidth.

Furthermore, these patterns guarantee a fixed delay – one can transmit, e.g., every 10 ms as this is the standard

TDMA schemes with fixed access patterns are used for many digital mobile phone systems like IS-54, IS-136, GSM, DECT, PHS, and PACS.

Figure 3.4 shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station.

Assigning different slots for uplink and downlink using the same frequency is called **time division duplex (TDD)**.

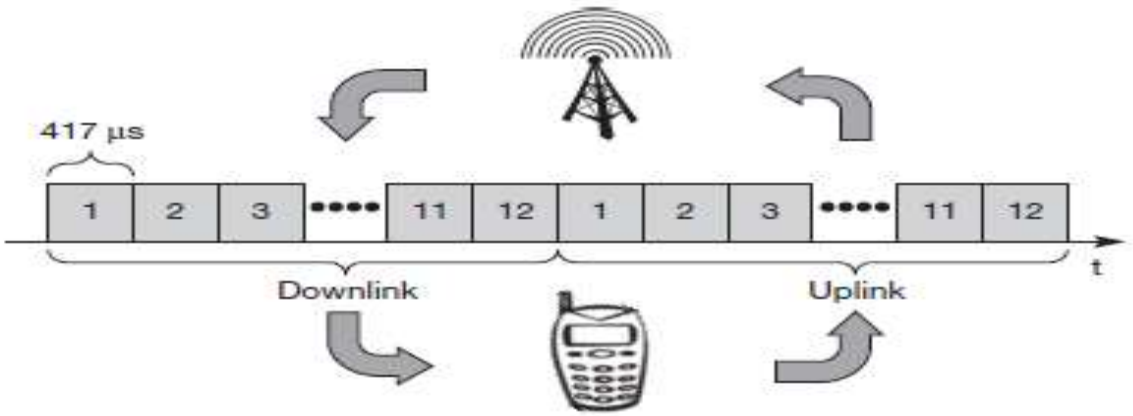


Figure 3.4 Time division multiplexing for multiple access and duplex

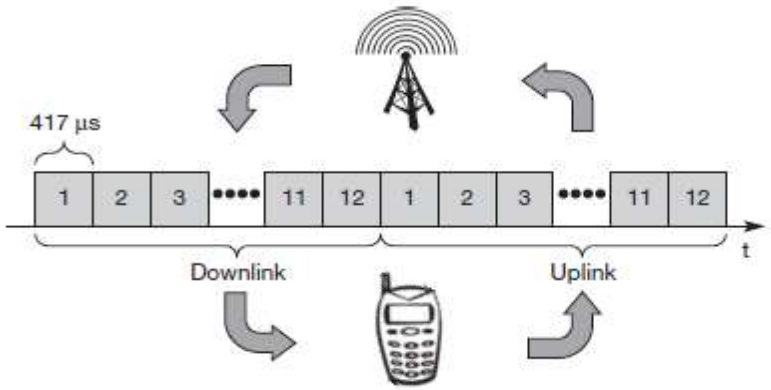


Figure 3.4
Time division multiplexing for multiple access and duplex

The base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink.

Uplink and downlink are separated in time.

Up to 12 different mobile stations can use the same frequency without interference using this scheme.

Each connection is allotted its own up- and downlink pair.

Table 3.1 Comparison of SDMA, TDMA, FDMA, and CDMA mechanisms

Approach	SDMA	TDMA	FDMA	CDMA
Idea	Segment space into cells/sectors	Segment sending time into disjoint time-slots, demand driven or fixed patterns	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes
Terminals	Only one terminal can be active in one cell/one sector	All terminals are active for short periods of time on the same frequency	Every terminal has its own frequency, uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted
Signal separation	Cell structure directed antennas	Synchronization in the time domain	Filtering in the frequency domain	Code plus special receivers
Advantages	Very simple, increases capacity per km^2	Established, fully digital, very flexible	Simple, established, robust	Flexible, less planning needed, soft handover
Disadvantages	Inflexible, antennas typically fixed	Guard space needed (multi-path propagation), synchronization difficult	Inflexible, frequencies are a scarce resource	Complex receivers, needs more complicated power control for senders
Comment	Only in combination with TDMA, FDMA or CDMA useful	Standard in fixed networks, together with FDMA/SDMA used in many mobile networks	Typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	Used in many 3G systems, higher complexity, lowered expectations; integrated with TDMA/FDMA

MCC PT2 Question Bank

1 Explain UTMS Architecture
2 Write Note on Handover in UTMS
3 Explain GPRS architecture Reference Model
4 Explain Advantages and Disadvantage of Wireless LAN
5 Write Note on UTRAN
6 Write Note on Infrastructure and Ad-hoc wireless network
7. Write short notes on Hidden and exposed terminals.
8. Write short notes on Near and far terminals.
9. Write short notes on SDMA.
10. Write short notes on FDMA.
11. Write short notes on TDMA.
12. Compare SDMA ,TDMA,FDMA and CDMA.
13. Explain how Multiple Access with collision avoidance (MACA) solve hidden terminals problem.
14. Explain how Multiple Access with collision avoidance (MACA) solve exposed terminals problem.
15. Explain agent discovery process.
16. Explain agent registration process.

Mobile IP

Entities and terminology

- **Mobile node (MN):**

A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP.

The MN keeps its IP address and can continuously communicate with any other system in the internet as long as link-layer connectivity is given.

MN : laptops with antennas ,mobile phones; a router onboard an aircraft

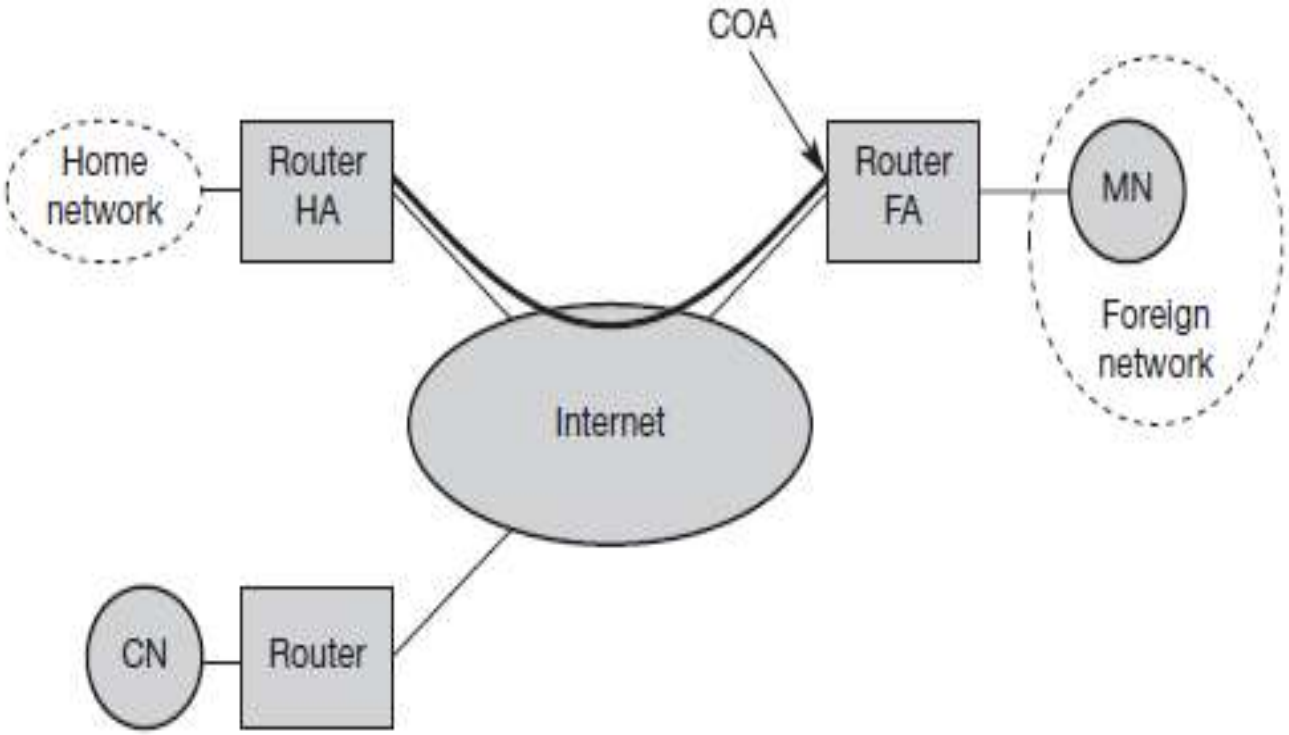


Figure 8.1
Mobile IP example network

Mobile IP (Entities and terminology)

Correspondent node (CN): At least one partner is needed for communication.

The CN can be a fixed or mobile node.

- **Home network:** The home network is the subnet the MN belongs to with respect to its IP address.

No mobile IP support is needed within the home network.

Mobile IP (Entities and terminology)

Foreign network: The FN is the current subnet the MN visits and which is not the home network.

Foreign agent (FA): The FA can provide several services to the MN during its visit to the FN

FA can have the COA acting as tunnel endpoint and forwarding packets to the MN.

FA - default router

FA - **security services**

FA is implemented on a router for the subnet the MN attaches to

Mobile IP (Entities and terminology)

- **Care-of address (COA):** The COA defines the current location of the MN from an IP point of view.

IP packets - to - MN –COA- not IP address of the MN

Packet delivery toward the MN is done using a tunnel

COA - tunnel endpoint - address where packets exit

There are two different possibilities for the location of the COA:

Mobile IP (Entities and terminology)

- **Care-of address (COA):** There are two different possibilities for the location of the COA:

- **Foreign agent COA: -**

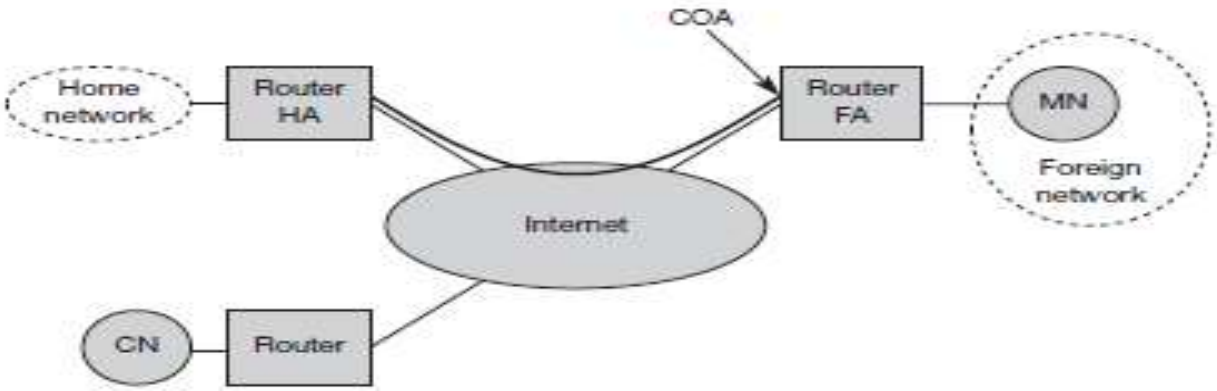
located at the FA, i.e., the COA - IP address of the FA

The FA - tunnel end-point – forwards packets to MN

Many MN using the FA can share this COA as common COA.

- **Co-located COA:**

The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA.



Home agent (HA):

HA - several services - MN – located in the home network

The tunnel for packets toward the MN starts at the HA

HA -a location registry, i.e., it is informed of the MN's location by the current COA

Home agent (HA):

3 alternatives for the implementation of an HA exist

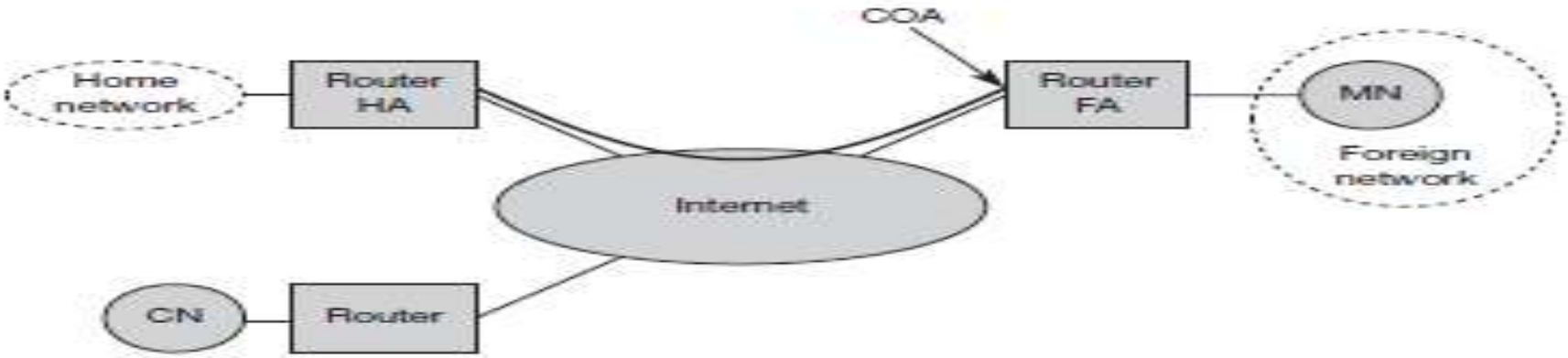
- The HA - on a router - for the HN

This - best position - because without optimizations to mobile IP, all packets for MN -through the router anyway.

- The HA - on an arbitrary node in the subnet

One disadvantage - double crossing of the router by the packet if the MN is in a foreign network

The HA - on the ‘router’ but - as a manager for MNs belonging to a virtual home network.



CN - via a router to the internet, as are the **HN** and **FN**

HA - on the router connecting the **HN**

FA -on the router to the **FN**

MN is currently in foreign network

The tunnel for packets toward the MN starts at the HA and ends at the FA, for the FA has the COA in this example.

IP packet delivery

Fig 8.2 illustrates packet delivery to and from the MN

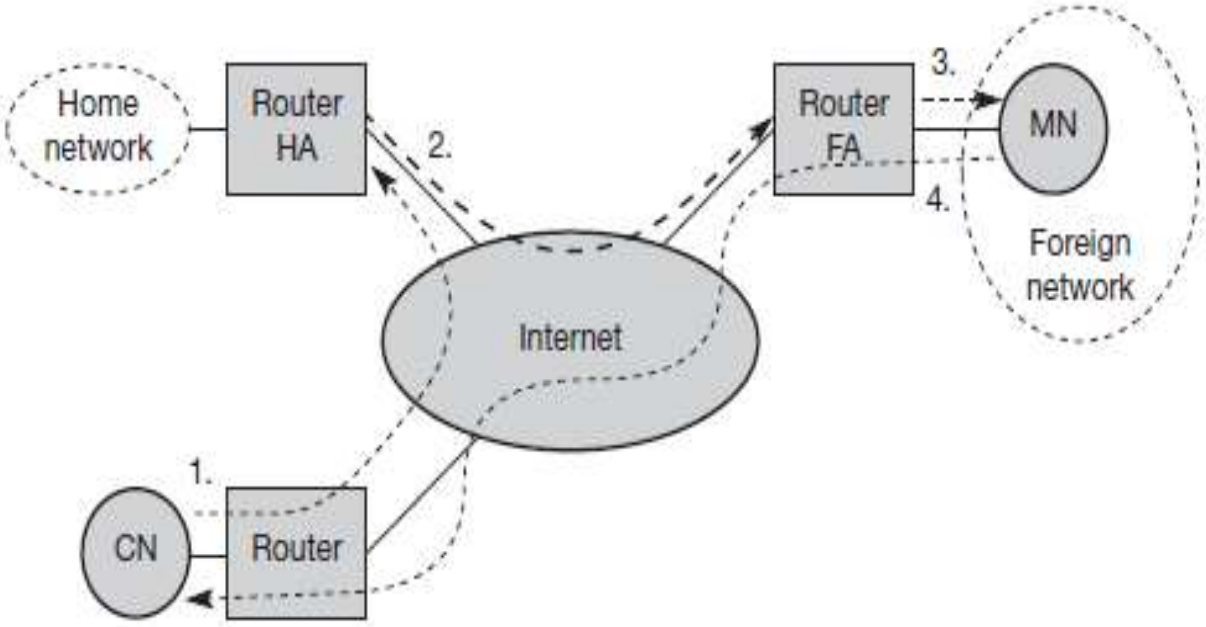


Figure 8.2
Packet delivery to and from the mobile node

A correspondent node CN wants to send an IP packet to the MN

CN – doesn’t - MN’s current location - sends packet as usual to the IP address of MN (step 1)

CN sends an IP packet with MN as a destination address and CN as a source address

The internet routes the packet to the router responsible for the home network of MN

The HA now intercepts the packet, knowing that MN is currently not in its home network.

The packet is not forwarded into the subnet,

but encapsulated and tunneled to the COA

A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet (step 2)

The foreign agent now de-capsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN (step 3)

Again, for the MN mobility is not visible
It receives the packet with the same sender and receiver address as it would have done in the home network.

The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination (step 4).

If CN were also a **mobile node** residing in **FN**, then steps 1 through 3 would apply now in the other direction.

Agent discovery

Initial problem - MN - to find a foreign agent

How - MN discover that it has moved?

1) **Agent advertisement**
2) **Agent solicitation**

Agent discovery

1) Agent advertisement

FA and HA -advertise their presence periodically using special **agent advertisement** messages

For these advertisements Internet control message protocol (**ICMP**) messages are used

The agent advertisement packet according to RFC 1256 with the extension for mobility is shown in Figure 8.3

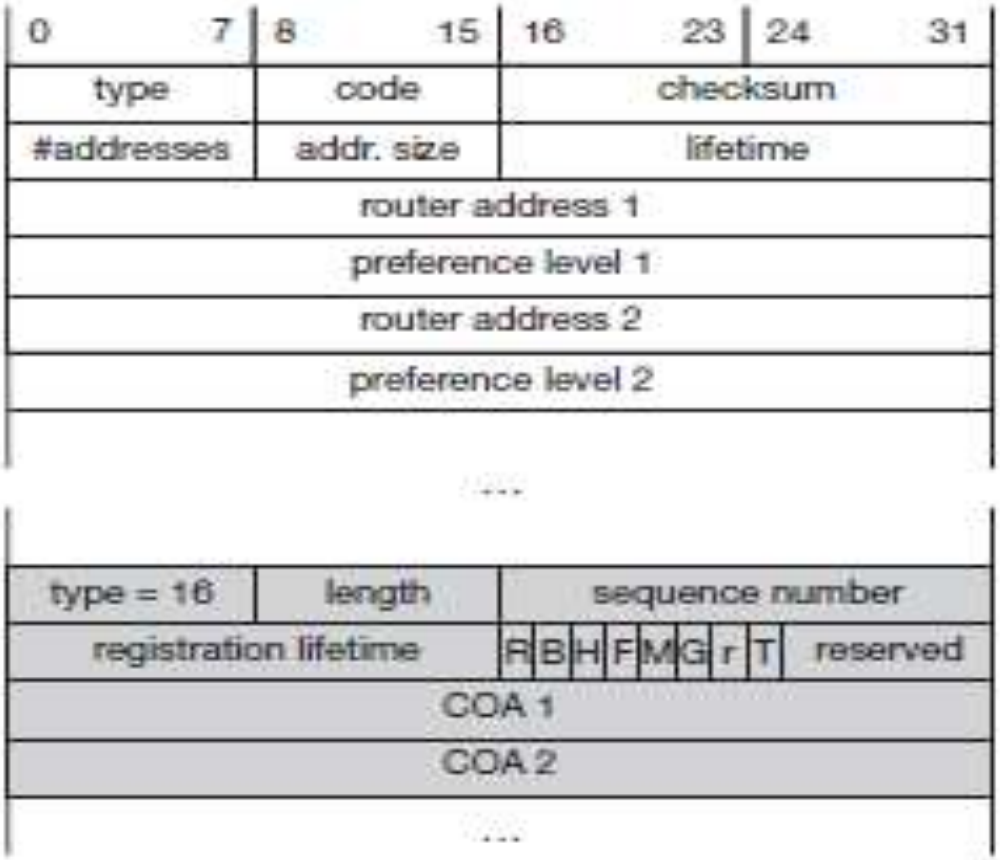
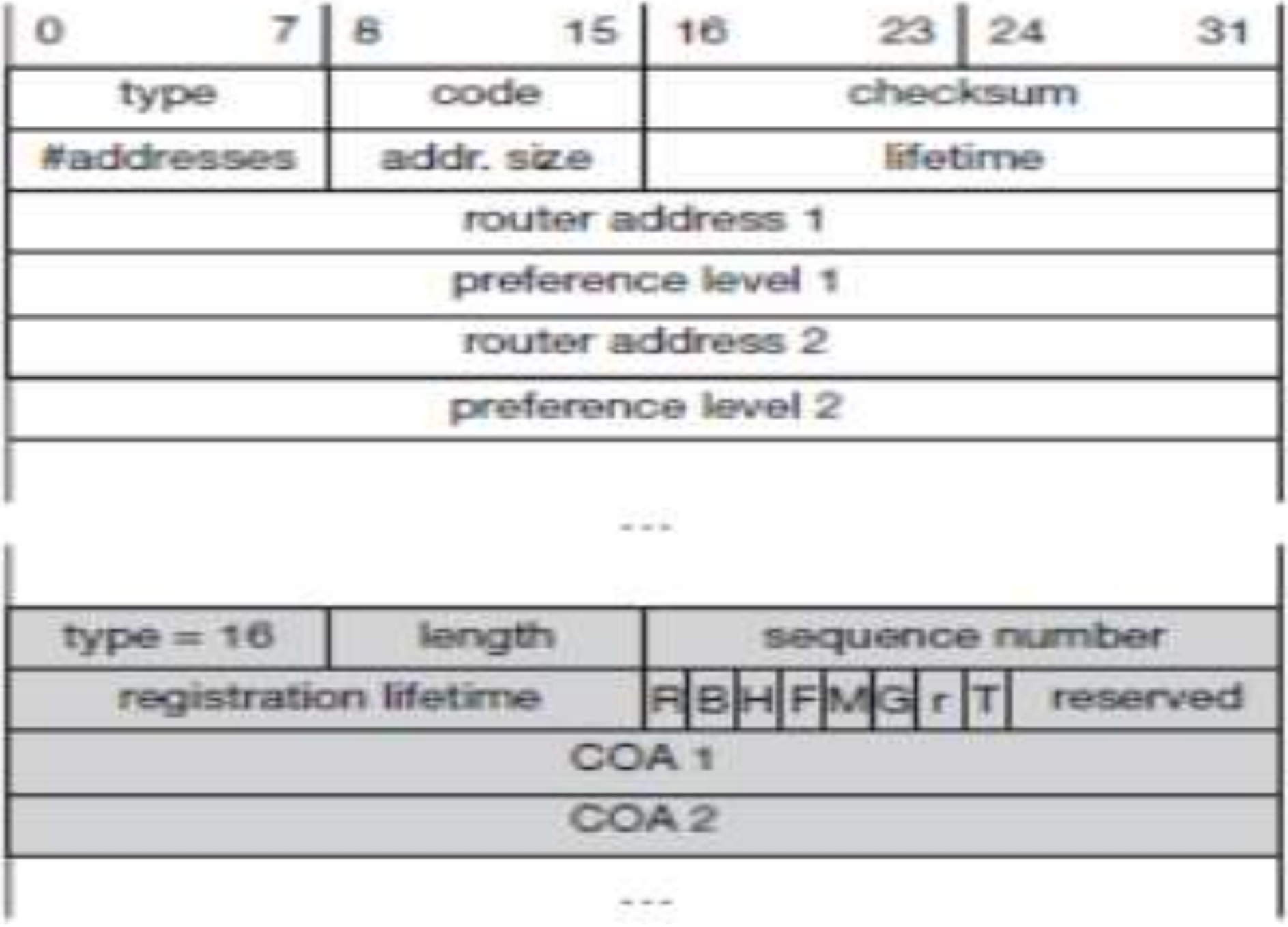


Figure 8.3
Agent advertisement packet (RFC 1256 + mobility extension)

The upper part represents the ICMP packet while the lower part is the extension needed for mobility.


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
...

Agent discovery

1) Agent advertisement

The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding

The IP destination address according to standard router advertisements can be either set to **224.0.0.1,** which is the multicast address for all systems on a link

or to the broadcast address **255.255.255.255**

The fields in the ICMP part are defined as follows

type - 9

code - 0, if agent routes traffic from non-mobile nodes
or
code -16, if it routes traffic from mobile nodes

#addresses -Number of addresses advertised

Lifetime - length of time advertisement is valid

Preference levels - for each address help a node to choose the router that is the most eager one to get a new node.

Extension for mobility has following fields:

type - 16

length -depends on number of COAs provided with the message and equals 6 + 4*(number of addresses)

Sequence number - total number of advertisements sent since initialization by the agent

registration lifetime the agent can specify the maximum lifetime in seconds a node can request during registration

The following bits specify the characteristics of an agent in detail.

R bit (registration) - if a registration with this agent is required even when using a co-located COA at MN

B bit - Agent is currently too busy to accept new registrations

H bit - the agent offers services as a home agent

F bit - the agent offers services as an foreign agent

M bit - minimal encapsulation

G bit - generic routing encapsulation

r bit - set to zero and must be ignored

T bit - indicates that reverse tunneling

2) Agent solicitation

If no agent advertisements are present or
the inter-arrival time is too high,
and
an MN has not received a COA
the mobile node must send **agent solicitations**

Solicitation messages do not flood the network

MN can search for an FA endlessly sending out solicitation messages

Mobile node can send out three solicitations, one per second, as soon as it enters a new network

2) Agent solicitation

If a node doesn't receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network

After these steps of advertisements or solicitations the MN can now receive a COA, either one for an FA or a co-located COA

The MN knows its location (HN or FN) and the capabilities of the agent

The next step for the MN is the registration with the HA if the MN is in a foreign network

Registration

Having received a COA, MN has to register with HA

Main purpose of the registration is to inform HA of the current location for correct forwarding of packets

Registration can be done in two different ways depending on the location of the COA

- If the COA is at the FA, registration is done as illustrated in Figure (left)

The MN sends its registration request containing the COA (see Figure) to the FA which is forwarding the request to the HA.

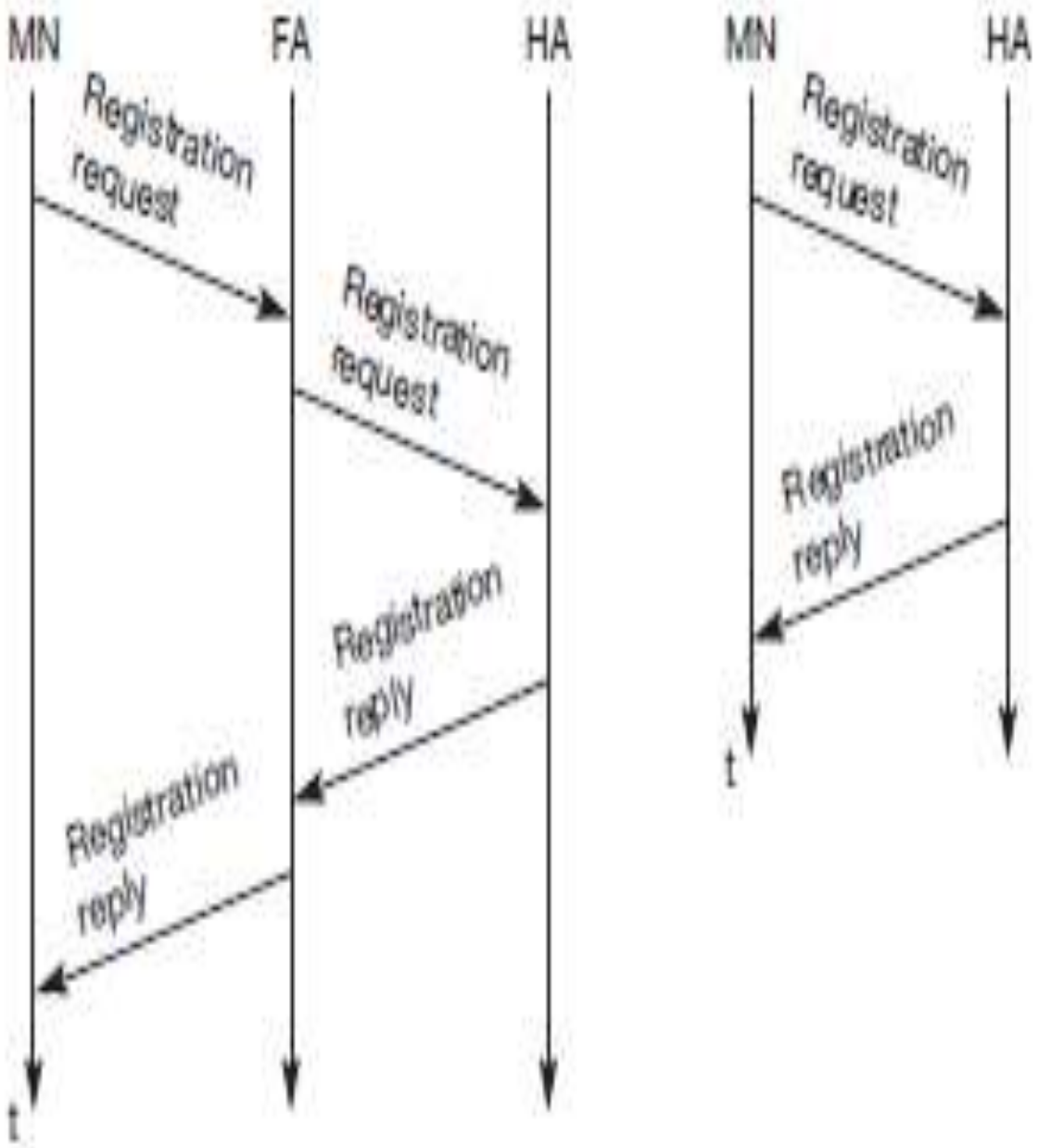


Figure 8.4 Registration of a mobile node via the FA or directly with the HA

Figure 8.5
Registration request

Registration

The HA now sets up a **mobility binding** containing the MN's home IP address and the current COA

Additionally, it contains the lifetime of the registration

MN should reregister before expiration

After setting up the mobility binding, HA sends a reply message back to the FA which forwards it to the MN.

- If the COA is co-located, registration can be simpler, as shown in Figure (right)

The MN may send the request directly to the HA and vice versa. This is also the registration procedure for MNs returning to their home network.

Registration

Here they also register directly with the HA

If MN received agent advertisement from FA it should register via this FA if R bit is set in the advertisement

UDP packets are used for **registration requests**

IP source address is set to interface address of the MN

IP destination address is that of the FA or HA

UDP destination port is set to **434**

Fields relevant for mobile IP registration requests follow as UDP data are defined as follows

Registration request

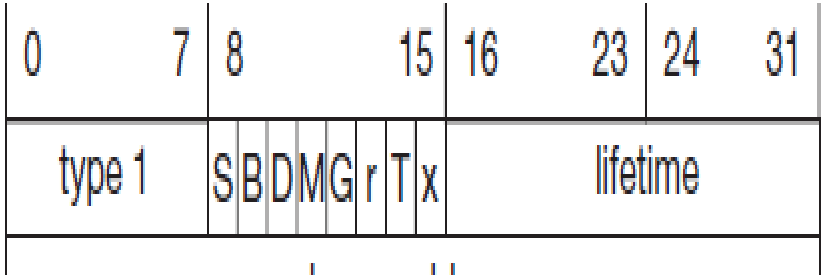
type is set to 1 for a registration request

S bit – MN can specify if it wants the HA to retain prior mobility bindings

B bit - an MN also wants to receive the broadcast packets which have been received by the HA in HN

D bit - If MN uses a co-located COA, it also takes care of the de-capsulation at the tunnel endpoint

M and **G** denote the use of minimal encapsulation or generic routing encapsulation



T indicates reverse tunneling

r and **x** are set to zero.

Lifetime denotes validity of registration in seconds Value of zero indicates deregistration

home address is the fixed IP address of the MN

home agent is the IP address of the HA

COA represents the tunnel endpoint. The 64 bit **identification** is generated by the

A **registration reply**, which is conveyed in a UDP packet, contains a **type** field set to 3

code indicating the result of the registration request.

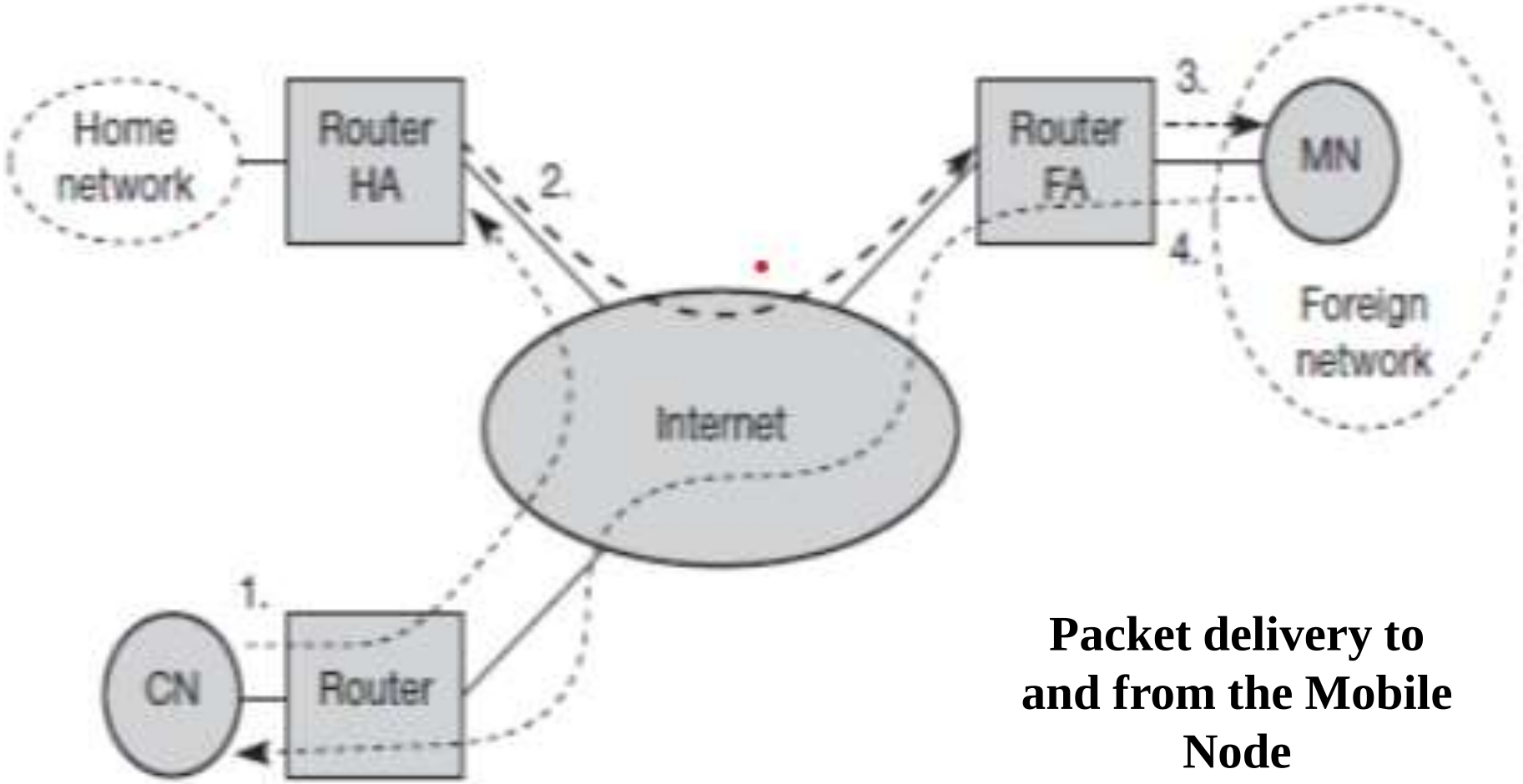
Registration Reply

Registration	Code	Explanation
successful	0	registration accepted
	1	registration accepted, but simultaneous mobility bindings unsupported
denied by FA	65	administratively prohibited
	66	insufficient resources
	67	mobile node failed authentication
	68	home agent failed authentication
	69	requested lifetime too long
denied by HA	129	administratively prohibited
	130	insufficient resources
	131	mobile node failed authentication
	132	foreign agent failed authentication
	133	registration identification mismatch
	135	too many simultaneous mobility bindings

Example Registration Reply Codes

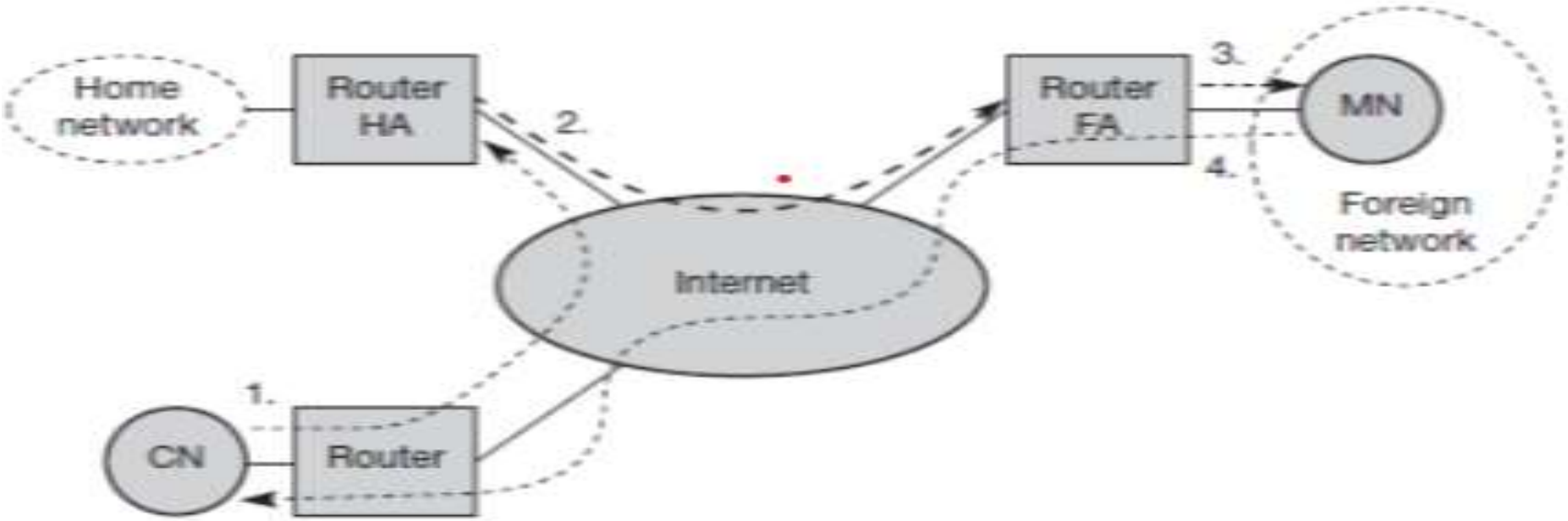
Tunneling and encapsulation

In the Figure below, step 2, describes the mechanisms used for forwarding packets between the HA and the COA



Packet delivery to and from the Mobile Node

Tunneling and encapsulation



A **tunnel establishes a virtual** pipe for data packets between a tunnel entry and a tunnel endpoint

Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged

Tunneling and encapsulation (contd.)

Tunneling is achieved by using encapsulation.

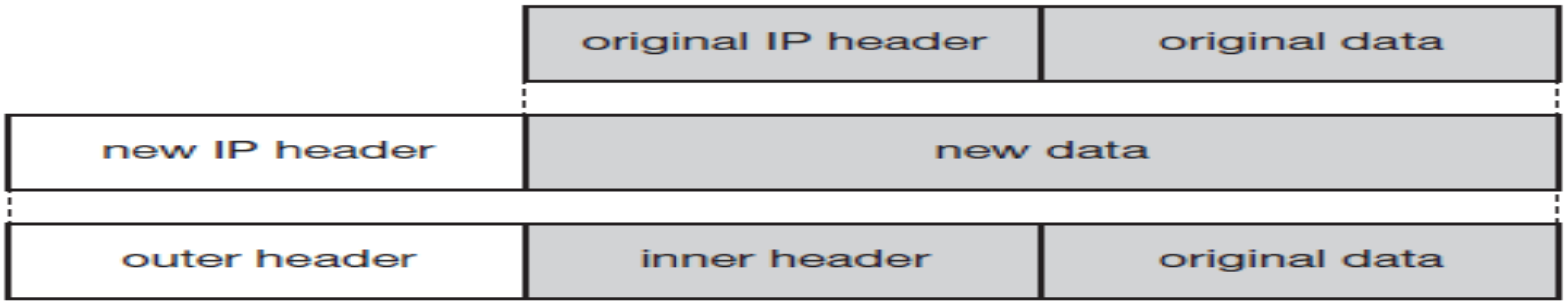
Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.

The reverse operation or **de-capsulation** is taking a packet out of the data part of another packet**.**

Encapsulation and de-capsulation operations are performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively

Tunneling and encapsulation (contd.)

This mechanism is shown in the figure below



IP Encapsulation HA takes original packet with the MN as destination, puts it into the data part of a new packet and Sets new IP header in such a way that the packet is routed to the COA

New header is called **outer header**

Inner header which can be identical to the original header

This is the case for **IP-in-IP encapsulation**

IPv6

Features

Security with regard to authentication

No special mechanisms are needed for securing mobile IP registration

Every IPv6 node masters address auto configuration – the mechanisms for acquiring a COA are already built in

Neighbor discovery as a mechanism mandatory for every node is also included in the specification;
it means special FAs are no longer needed to advertise services

IPv6 Features (contd.)

Combining the features of auto configuration and neighbor discovery means that every mobile node is able to create or obtain a topologically correct address for the current point of attachment.

Every IPv6 node can send binding updates to another node, so MN can send its current COA directly to CN and HA.

A soft handover is possible with IPv6

The MN sends its new COA to the old router servicing the MN at the old COA, and old router encapsulates all incoming packets for MN and forwards them to the new COA.

IPv6 Features (contd.)

The FA is not needed any more

A CN only has to be able to process binding updates, i.e., to create or to update an entry in the routing cache

MN itself has to be able to de-capsulate packets, to detect when it needs a new COA, and to determine when to send binding updates to the HA and CN.

A HA must be able to encapsulate packets