UNIT I
WIRELESS LAN

Introduction - WLAN technologies: Infrared, UHF narrowband, spread spectrum - IEEE802.11: System architecture, protocol architecture, physical layer, MAC layer, 802.11b, 802.11a – Hiper LAN: WATM, BRAN, HiperLAN2 – Bluetooth: Architecture, Radio Layer, Baseband layer, Link manager Protocol, security - IEEE802.16 - WIMAX: Physical layer, MAC, Spectrum allocation for WIMAX.

Introduction

A wireless LAN is a LAN that utilizes radio-frequency communication to permit data transmission among fixed, nomadic, or moving computers.

Wireless LANs can be divided into two operational modes based on the network formation:

- Infrastructure mode
- ad-hoc mode

1. ***Discuss the advantages and disadvantages of Wireless LAN in detail. [16m - Nov 2013]***
   Elucidate the advantages of WLAN techniques. (05m) [May 2018]
   Elucidate the advantages of WLAN techniques. (08m) [Nov 2018]

Advantages of WLANs:

- Flexibility: Within radio coverage, nodes can communicate without restrictions like walls.
- Planning: Only wireless ad-hoc networks allow for communication without previous planning.
- Design: Wireless networks allow the design of small, independent pocket size devices.
- Robustness (Strengthness): Wireless networks can survive disasters, e.g., earthquakes.
- 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.

Disadvantages:

- Quality of service: WLANs offer lower quality than their wired counterparts.
- Restrictions:
  - ✓ All wireless products have to obey with national regulations.
  - ✓ ***Restricted frequencies*** to minimize interference.
- Safety and security:
  - ✓ Senders and receivers are operated by laymen and, radiation has to be low.
  - ✓ All standards must offer (automatic) encryption, privacy mechanisms, support for secrecy etc.

Design goals have to be taken into account for WLANs to ensure their commercial success:

- Global operation
- Low power
- License-free operation
- Robust transmission technology
- Simplified spontaneous cooperation
- Easy to use

- Protection of investment

WLAN technologies:

Infrared Technology
UHF Narrowband Technology
Infrastructure and ad-hoc network
IEEE 802.11
- System architecture
- Protocol architecture
- Physical layer
- Medium access control layer
- MAC management
- 802.11 b
- 802.11 a

LANs support.

- Safety and security:
  - ✓ Wireless LANs should be safe to operate, especially at low radiation, e.g., in hospitals. Users cannot keep safety distances to antennas.

- Transparency for applications:
  - ✓ The fact of wireless access and mobility should be hidden if it is not relevant.
  - ✓ The network should also support location aware applications.

1.1 Infrared Technology:

2. Compare Infrared and Radio transmission.(08m) [Nov 2018]

- Infrared is an invisible band of radiation.
- It exists at the lower end of the visible electromagnetic spectrum.
- This type of transmission is most effective when a clear line-of-sight exists between the transmitter and the receiver.
- Two types of infrared WLAN solutions are available:
  - Diffused-beam, and
  - Direct-beam (or line-of-sight).

- Now, direct-beam WLANs offer a faster data rate than the diffused-beam networks.
- Direct-beam is more directional, since diffused-beam technology uses reflected rays to transmit/receive a data signal.
- It achieves lower data rates in the 1–2 Mbps range. Infrared is a short-range technology.

- In indoors, it can be limited by solid objects such as doors, walls, merchandise, or racking.
- Fluorescent lights also may contain large amounts of infrared.
- This problem may be solved by using
  - the high signal power, and
  - an optimal bandwidth filter (it reduces the infrared signals from an outside source).

- In an outdoor environment, snow, ice, and fog may affect the operation of an infrared based system.
- ***Table*** gives considerations for choosing infrared technology.

Table: Considerations for choosing infrared technology.

Advantages	No government regulations controlling use
	Immunity to electro-magnetic (EM) and RF interference
Disadvantages	Generally a short-range technology (30–50 ft radius under ideal conditions)
	Signals cannot penetrate solid objects
	Signal affected by light, snow, ice, fog
	Dirt can interfere with infrared

Advantages of infra red technology:

- Simple and extremely cheap senders and receivers, which are integrated into all mobile devices.
- PDAs, laptops, notebooks, mobile phones etc. have an infra red data association (IrDA) interface.
- Version 1.0 of this industry standard implements data rates of up to 115 kbit/s,
- IrDA 1.1 defines higher data rates of 1.152 and 4 Mbit/s.
- No licenses are needed for infrared technology and shielding is very simple.
- Electrical devices do not interfere with infra red transmission.

Disadvantages of infra red transmission:

- ✓ Low bandwidth compared to other LAN technologies.
- ✓ Typically, IrDA devices are limiting transfer rates to 115 kbit/s.
- ✓ Even 4 Mbit/s is not a particularly high data rate.
- ✓ The main disadvantage is that infra red is quite easily shielded.
- ✓ Infra red transmission cannot penetrate walls or other obstacles.
- ✓ For good transmission quality and high data rates a Line Of Sight is needed.

1.1. a UHF Narrowband Technology

- UHF wireless data communication systems have been available since the early 1980s.
- These systems normally transmit in the 430 to 470 MHz frequency range (rare systems use 800 MHz range).
- The lower portion of this band:
  - 430 to 450 MHz - It is referred to as the unprotected (unlicensed)
  - 450 to 470 MHz - It is referred to as the protected (licensed) band

- In the unprotected band, RF licenses are not granted for specific frequencies.
- Because independent narrowband RF systems cannot coexist on the same frequency, government agencies allocate specific RFs to users through RF site licenses.
- A limited amount of unlicensed spectrum is also available in some countries.

- RF signal is sent in a very narrow bandwidth, typically 12.5 kHz or 25 kHz.

- Power levels range from 1 to 2 watts for narrowband RF data systems.
- This narrow bandwidth combined with high power results in larger transmission distances.
- Following ***Table*** lists the advantages and disadvantages of UHF technology.

Table Considerations for choosing UHF technology.

Advantages	Longest range
	Low cost solution for large sites with low to medium data throughput requirements
Disadvantages	Large radio and antennas increase wireless client size
	RF site license required for protected bands
	No multivendor interoperability
	Low throughput and interference potential

- Many modern UHF systems are synthesized radio technology.
- This refers to the way channel frequencies are generated in the radio.

- Common equipment can be purchased and specific UHF frequency is used for each device, which can be tuned based upon specific location requirements.
- Additionally, synthesized UHF radios do not exhibit the frequency drift problem
    - But, frequency drift problem is experienced in crystal controlled UHF radios.

- Modern UHF systems allow APs to be individually configured for operation on one of the several preprogrammed frequencies.

Spread Spectrum Technology

- Most WLANs use spread spectrum technology.
- A wideband radio frequency technique that uses the entire allotted spectrum in a shared fashion.
- The spread spectrum system spreads the transmission power over the entire usable spectrum.
- This is a less efficient use of the bandwidth than the narrowband approach.
- The spread spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security.
- The bandwidth trade-off produces a signal that is easier to detect.
- If the receiver is not tuned to the right frequency, a spread spectrum signal looks like background noise.

- By operating across a broad range of radio frequencies, a spread spectrum device could communicate clearly despite interference from other devices

- In commercial applications, spread spectrum techniques currently offer data rates up to 2 Mbps.
- Two modulation schemes are commonly used to encode spread spectrum signals:
    - Direct Sequence Spread Spectrum (DSSS), and
    - Frequency Hopping Spread Spectrum (FHSS).

- FHSS
  - It uses a narrowband carrier
  - It changes frequency in a pattern known to both transmitter and receiver.
  - Properly synchronized, the net effect is to maintain a single logical channel.
  - To an unintended receiver, FHSS appears to be a short-duration impulse noise.

- DSSS
  - It generates a redundant bit pattern for each bit to be transmitted.
  - This bit pattern is called a spreading code.
  - The longer the code, the greater the probability that the original data can be recovered (and, of course the more bandwidth will be required).
  - To an unintended receiver DSSS appears as low-power, wideband noise and is rejected by most narrowband receivers.

1.3 IEEE 802.11

3. With a suitable block diagram, explain the IEEE 802 .11 Architecture. (16) (June/July 2013)
(or)
Explain the components of an Infrastructure of a, b and wireless part of an IEEE 802.11 standard Architecture system. (16) (Nov/ Dec 2013) ***(or)***
Compare the different versions of IEEE 802.11 standards respect to data rate , modulation techniques, operating frequency and applications (May/June 2014) ***(or)***
Explain in detail about the IEEE 802.11 protocol architecture and bridging with other networks. (16) (Nov 2017) ***(or)***
Draw the protocol architecture of WLAN (802.11). Explain the physical layer and MAC management of 802.11.(16m) [Nov 2018] ***(or)***
With neat sketch describe the architecture of IEEE 802.11vand explain the MAC management techniques. (11m) [May 2018]
Explain various WLAN technologies and describe them, with their applications. [Nov 2019]

- The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs.
- Many products are available in IEEE standard 802.11.
- As the standard's number indicates,
  - ✓ This standard belongs to the group of 802.x LAN standards
  - ✓ Some other examples are, e.g., 802.3 Ethernet *or* 802.5 Token Ring.
- This means, the standard specifies the ***physical and medium access layer*** adapted to the special requirements of wireless LANs.
- But offers the same ***interface to higher layers*** to maintain interoperability.

- The primary goal of the standard was ***the specification of a simple and robust WLAN***.
  - ✓ It offers time-bounded and asynchronous services.

- Additional features of the WLAN should include
  - ✓ the support of power management to save battery power,
  - ✓ the handling of hidden nodes, and

- ✓ the ability to operate worldwide.

- The 2.4 GHz ISM band, which is available in most countries around the world, was chosen for the original standard.
- Data rates predicted for the standard were 1 Mbit/s mandatory and 2 Mbit/s optional.

1.3.1 System architecture

- Wireless networks can exhibit two different basic system architectures such as
  - Infrastructure-based or
  - Ad-hoc.

Architecture of Infrastructure-based IEEE 802.11

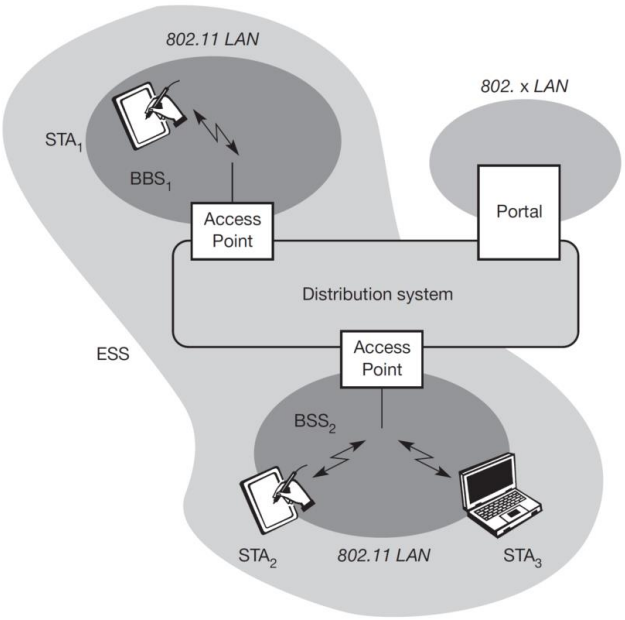


Figure 1.3 Architecture of an ***infrastructure-based IEEE 802.11***

- **Figure 1.3** shows the components of an infrastructure and a wireless part as specified for IEEE 802.11.
- Several nodes, called **Sta**tions (STA_i), are connected to **A**ccess **P**oints (**AP**).

- **STA$_i$**: Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.
- The stations and the AP within the same radio coverage form a **B**asic **S**ervice **S**et (**BSSi**).
  - Examples: Two BSSs – BSS1 and BSS2 – which are connected via a distribution system.

- A ***Distribution System*** connects several BSSs via the AP to form a single network and extends the wireless coverage area.
- This network is now called an **E**xtended **S**ervice **S**et (**ESS**) and has its own identifier, the **ESSID**.
- ***ESSID:***
  - The ESSID is the 'name' of a network and is used to separate different networks.
  - Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN.

- The distribution system connects the wireless networks via the APs with a **portal *(Gateway)***, which forms the interworking unit to other LANs.

- The architecture of the distribution system is not specified further in IEEE802.11.
- It could consist of bridged IEEE LANs, wireless links, or any other networks.

- But, distribution system services are defined in the standard.
- Stations can select an AP and associate with it.
- The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs.
- APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service.

Architecture of IEEE 802.11 ad-hoc wireless LAN

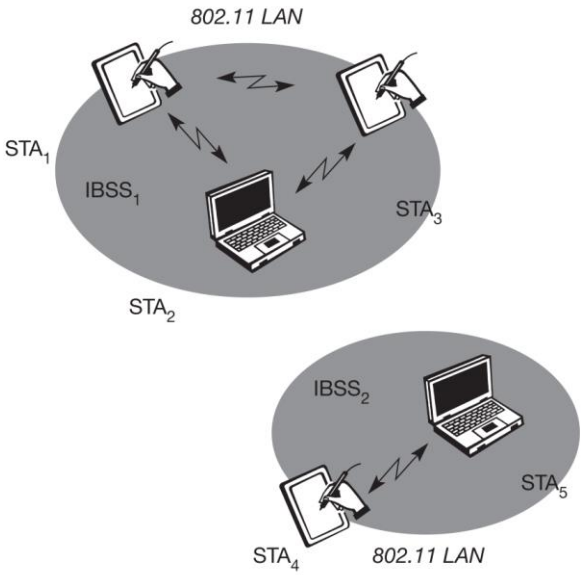


Figure 1.4 Architecture of IEEE 802.11 ad-hoc wireless LANs

- IEEE 802.11 allows the building of ad-hoc networks between stations.
- Thus forming one or more independent BSSs (IBSS) as in Figure 1.4.
- In this case, an IBSS comprises ***a group of stations using the same radio frequency***.
- Stations STA_1, STA_2, and STA_3 are in $IBSS_1$; STA_4 and STA_5 are in $IBSS_2$.

- This means for example that STA_3 can communicate directly with STA_2 but not with STA_5.
- IBSSs can be formed
  - via the distance between the IBSSs (Figure 1.4), (or)
  - by using different carrier frequencies (then the IBSSs could overlap physically).
- IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as, e.g., **HIPERLAN 1** or **Bluetooth**.

1.3.2 Protocol architecture

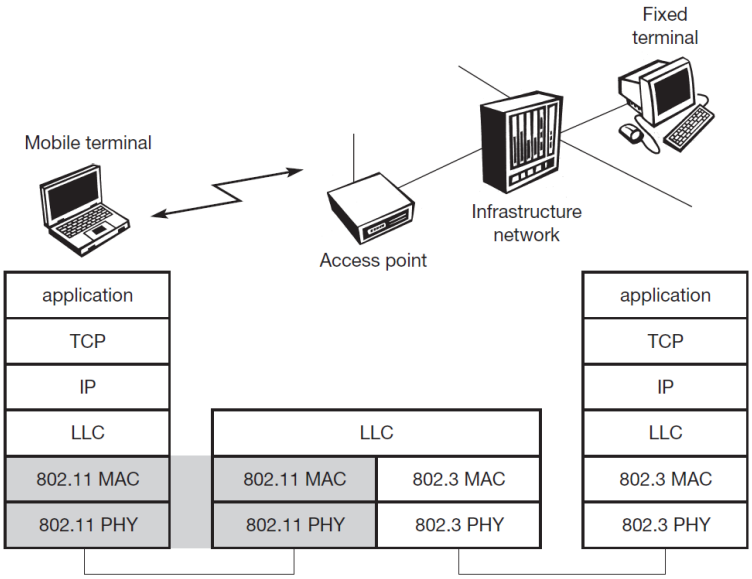


Figure 1.5 IEEE 802.11 protocol architecture and bridging

- IEEE 802.11 fits into the other 802.x standards for ***wired LANs***.
- Figure 1.5 shows the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge.

- The WLAN behaves like a slow wired LAN.
- The higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes.

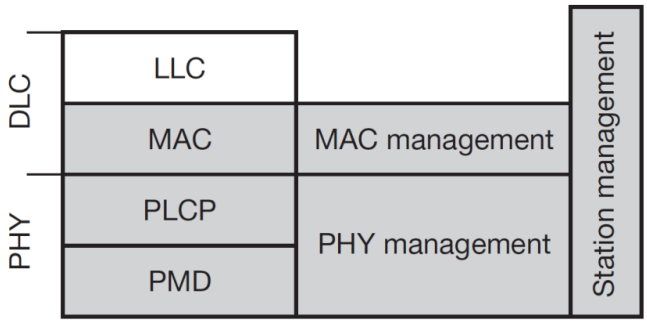


Figure 1.6 Detailed IEEE 802.11 protocol architecture and management

- ***LLC:***
  - LLC is the upper part of the data link control (DLC) layer.
  - The logical link control (LLC), covers the differences of the medium access control layers needed for the different media.

- The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do.

- The ***physical (PHY) layer*** is subdivided into

- the physical layer convergence protocol (PLCP), and
- the physical medium dependent sublayer (PMD).

The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.

- ***PLCP sublayer***
  - provides a carrier sense signal, called clear channel assessment (CCA), and
  - provides a common PHY service access point (SAP) independent of the transmission technology.

- ***PMD sublayer***
  - The PMD sublayer handles modulation and encoding/decoding of signals.

- Apart from the protocol sublayers, the standard specifies management layers and the station management.
  - **MAC management:**
    - The MAC management supports,
      - the association and re-association of a station to an access point and
      - roaming between different access points.
    - It also controls
      - authentication mechanisms, encryption, synchronization of a station with regard to an access point and
      - power management to save battery power.
    - MAC management also maintains the MAC management information base (MIB).

  - **PHY management:**
    - The main tasks of the PHY management include ***channel tuning*** and ***PHYMIB maintenance***.
- **Station Management:**
  - Station management interacts with both management layers
  - It is responsible for additional higher layer functions
    - Example: Control of bridging and interaction with the distribution system in the case of an access point.

****

1.3.3 (IEEE 802.11) Physical layer (*Subtopics:* *Frequency hopping spread spectrum, Direct sequence spread spectrum, Infra red*)

- IEEE 802.11 supports three different physical layers:
  - one layer based on infra red, and
  - two layers based on radio transmission (primarily in the ISM band at 2.4GHz, which is available worldwide).

- All the PHY variants include the provision of the clear channel assessment signal ***(CCA)***.
  - This is needed for
    - the MAC mechanisms controlling medium access, and
    - indicates if the medium is currently idle.

- The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer (basic version of the standard).

1.3.3.1 Frequency hopping spread spectrum

- FHSS allows the coexistence of multiple networks in the same area, by using different hopping sequences.

- The original standard defines
  - 79 hopping channels for North America and Europe, and
  - 23 hopping channels for Japan (each with a bandwidth of 1 MHz in the 2.4 GHz ISM band).
- The ***selection of a particular channel*** is achieved by using a pseudo-random hopping pattern.
- Maximum transmit power is
  - *1 W in the US, 100 mW EIRP in Europe,* and
  - *10 mW/MHz in Japan*.

  *Note: **EIRP** - **E**quivalent **I**sotropic **R**adiated **P**ower*

- The standard uses
  - ***Gaussian shaped FSK*** (frequency shift keying), ***GFSK***, as modulation for the FHSS PHY for 1 Mbit/s a 2 level GFSK is used (i.e., 1 bit is mapped to one frequency)
  - 4 level GFSK for 2 Mbit/s (i.e., 2 bits are mapped to one frequency).

- While sending and receiving at ***1 Mbit/s is mandatory*** for all devices and 2 Mbit/s is optional.
- Result:
  - Production of low-cost devices for the lower rate only
  - More powerful devices for both transmission rates in the early days of 802.11.

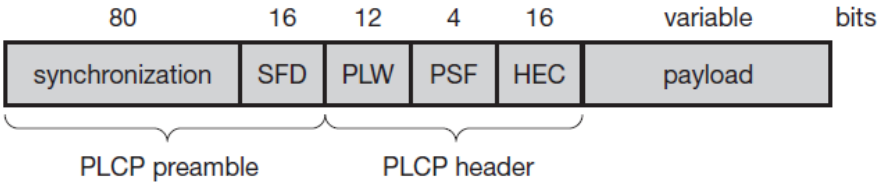


Figure 1.7 Format of an IEEE 802.11 PHY frame using FHSS

- **Figure 1.7** shows a frame of the physical layer used with FHSS.
- The frame consists of two basic parts,
  - the ***PLCP part*** (preamble and header), and
  - the ***payload part***.

- While the PLCP part is always transmitted at 1 Mbit/s, payload, i.e. MAC data, can use 1 or 2 Mbit/s.
- Additionally, MAC data is scrambled using the polynomial $s(z) = z^7 + z^4 + 1$ for DC blocking and whitening of the spectrum.

The fields of the frame fulfill the following functions:

- Synchronization:
  - The PLCP preamble starts with 80 bit synchronization, which is a 010101... bit pattern.
  - This pattern is used for synchronization of potential receivers and signal detection by the CCA.
- Start frame delimiter (SFD):
  - The following 16 bits indicate the ***start of the frame*** and provide ***frame synchronization***.
  - The SFD pattern is 0000110010111101.
- PLCP_PDU length word (PLW):
  - This first field of the PLCP header indicates ***the length of the payload in bytes*** including the 32 bit CRC at the end of the payload.
  - PLW can range between 0 and 4,095.
- PLCP signalling field (PSF):
  - This 4 bit field indicates the data rate of the payload following.
  - All bits set to zero (0000) indicates the lowest data rate of 1 Mbit/s.
  - The granularity is 500 kbit/s, thus 2 Mbit/s is indicated by 0010 and the maximum is 8.5 Mbit/s (1111).
  - This system obviously does not accommodate today's higher data rates.
- Header error check (HEC): Finally, the PLCP header is protected by a 16 bit checksum with the standard ITU-T generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$.

1.3.3.2 Direct sequence spread spectrum

- DSSS is the alternative spread spectrum method ***separating by code and not by frequency***.
- In IEEE 802.11 DSSS, spreading is achieved using the ***11-chip Barker sequence*** (+1, –1, +1, +1, –1,+1, +1, +1, –1, –1, –1).
- The key characteristics of this methods are
  - its robustness against interference, and
  - its insensitivity to multipath propagation (time delay spread).
- However, the implementation is more complex compared to FHSS.

- IEEE 802.11 DSSS PHY also uses the 2.4 GHz ISM band and offers both 1 and 2 Mbit/s data rates. ***(ISM** – **I**ndustrial, **S**cietific and **M**edical radio band)*
- Modulation Schemes
  - **D**ifferential **B**inary **P**hase **S**hift **K**eying (**DBPSK**) for 1 Mbit/s transmission, and
  - **D**ifferential **Q**uadrature **P**hase **S**hift **K**eying (**DQPSK**) for 2 Mbit/s transmission.
- ***Maximum transmit power:*** 1W in the US, 100 mW EIRP in Europe, and 10 mW/MHz in Japan.
- The ***symbol rate*** is ***1 MHz***, resulting in a chipping rate of 11 MHz.
  - All bits transmitted by the DSSSPHY are scrambled with the polynomial $s(z) = z^7 + z^4 + 1$.

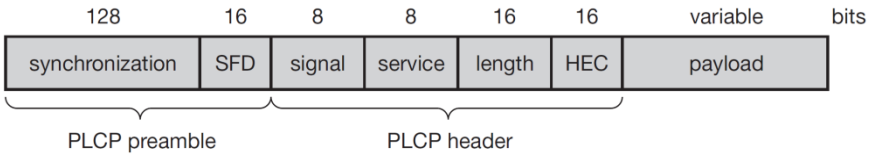


Figure 1.8 Format of an IEEE 802.11 PHY frame using DSSS

- The frame consists of two basic parts, ***the PLCP part*** (preamble and header) and the ***payload part***.
- The PLCP part is always transmitted at 1 Mbit/s,
- The payload, i.e., MAC data, can use 1 or 2 Mbit/s.

The fields of the frame have the following functions:

- ***Synchronization:***
  - The first 128 bits are used for synchronization, gain setting, energy detection and frequency offset compensation.
  - The synchronization field only consists of scrambled 1 bits.
- ***Start frame delimiter (SFD):***
  - This 16 bit field is used for synchronization at the beginning of a frame.
  - It consists of the pattern 1111001110100000.
- ***Signal:***
  - Originally, only two values are defined for this field, to indicate the data rate of the payload.
  - The value 0x0A indicates 1 Mbit/s (and thus DBPSK), 0x14 indicates 2 Mbit/s (and thus DQPSK).
  - Other values are reserved for future use, i.e., higher bit rates.
- ***Service:*** This field is reserved for future use; 0x00 indicates an IEEE 802.11 compliant frame.
- ***Length:*** 16 bits are used for length indication of the payload in microseconds.
- ***Header error check (HEC):*** Signal, service, and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

7.3.3.3 Infra red

- The PHY layer, which is based on infra red (IR) transmission.
- It uses ***near visible light*** at 850–950 nm.
- Infra red light is not regulated apart from safety restrictions (using lasers instead of LEDs).
- The standard ***does not require a line-of-sight*** between sender and receiver, but work with diffuse light ***(Reflected Light)***.

- This allows point-to-multipoint communication.
- The maximum range is about 10 m, if no sunlight or heat sources interfere with the transmission.

- This network will only work in buildings, e.g., classrooms, meeting rooms etc.
- Frequency reuse is very simple – a wall is enough to shield one IR based IEEE802.11 network from another.

- Today, no products are available that offer infra red communication based on 802.11.

- Proprietary products offer, e.g., up to 4 Mbit/s using diffuse infra red light.
- Alternatively, directed infra red communication based on IrDA can be used.

IEEE802.11 MAC sublayer

4.	**Why do you have the two divisions in the MAC layer itself for IEEE 802.11 and explain in detail about the MAC sub layer.**	**(16m)**	**Dec 2015**
	With suitable diagram, explain in detail about MAC sublayer of IEEE 802.11	**(16m)**	**Dec 2014**
	Describe the MAC layer features and functions and functionalities of IEEE 802.11 Wireless LAN.	**(10m)**	**May 2015**
	Explain the following corresponding to 802.11 MAC sublayer. **(1) Reliable data delivery** **(2) Access control** **(3) MAC Frame Format**	 **(04m)** **(04m)** **(04m)**	**Apr 2014**
	With suitable diagram, explain in detail about MAC sublayer of IEEE 802.11	**(16m)**	**May 2016**
	Explain and compare the medium access mechanism of DCF methods adopted in IEEE 802.11 WLAN.	**(16m)**	**May 2017**
	Write the sketch describe the architecture of IEEE 802.11 and explain the MAC Management techniques.	**(16m)**	**May 2018**
	Describe the IEEE 802.11 MAC data frame format with relevant diagram.	**(13m)**	**May 2019**

- In IEEE 802.11, the MAC sublayer is responsible for
  - ***asynchronous data service*** (e.g., exchange of **M**AC **S**ervice **D**ata **U**nits (MSDUs)),
  - ***security service*** (confidentiality, authentication, access control in conjunction with layer management), and
  - ***MSDU ordering***.
- The MAC sublayer accepts MSDUs from higher layers in the protocol stack and send them to the protocol stack in another station.
- The MAC adds information to the MSDU in the form of headers and trailers to generate a MAC protocol data unit (MPDU).
- The MPDU is then passed to the physical layer over the wireless medium to other stations.
- The MAC may fragment ***(pieces)*** MSDUs into several frames.
- It increases the probability of each individual frame being delivered successfully.

- The MAC frame contains addressing information, information to set the network allocation vector (NAV), and a frame check sequence to verify the integrity of the frame.
- The general IEEE 802.11 MAC frame format is shown in Figure 1.8a.

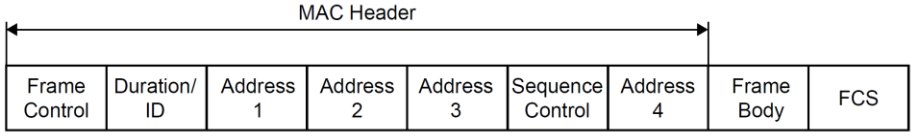


Figure 1.8a IEEE 802.11 MAC frame format.

- The MAC frame format contains four address fields.
- Any particular frame type may contain one, two, three, or four address fields.
- **Address Format:**
  - The address format in IEEE 802.11-1997 is a 48-bit address
  - It is used to identify the source and destination of MAC addresses contained in a frame.
  - In addition to ***source address (SA)*** and ***destination address (DA).***
  - Three additional address types are: ***the transmitter address***, ***the receiver address (RA)***, and ***the basic service set identifier*** (BSSID).
- **Transmitter address (TA):**
  - ✓ It is the address of the MAC, that transmitted the frame into the wireless medium.
  - ✓ This address is always an ***individual address***.
  - ✓ This address is used by stations receiving a frame to identify the transmitter MAC.
- **Receiver address (RA):**
  - ✓ This is the address of the MAC, to which the frame is sent over the wireless medium.
  - ✓ This address may be an ***individual*** or ***group address***.
- **Source Address (SA):**
  - ✓ This the address of the MAC, that originated the frame.
  - ✓ This address is always an ***individual address***.
  - ✓ This address does not match the address in the transmitter address field
  - ✓ It is the SA field that is used to identify the source of a frame.
- **Destination address (DA):**
  - ✓ This is the address of the final destination to which the frame is sent.
  - ✓ This address may be ***an individual*** or ***group address***.
  - ✓ This address does not match the address in the RA field.
- **Sequence Control Field (SCF):**
  - ✓ This is a 16-bit field that ***consists of two subfields***.
  - ✓ The subfields are a 4-bit fragment number and a 12-bit sequence number.
  - ✓ This field is used to allow a receiving station ***to eliminate duplicate received frames***.
  - ✓ The sequence number subfield contains ***numbers assigned sequentially by the sending station to each MSDU***.
  - ✓ This sequence number is ***incremented after each assignment*** and ***wraps back to zero when incremented from 4095***.
- **Frame Body Field:**
  - ✓ It contains the information specific to the particular data or management frames.
  - ✓ This field is variable in length.
  - ✓ It may be as long as 2034 bytes without encryption, or 2312 bytes when the frame body is encrypted.
- **Frame Check Sequence (FCS):**
  - ✓ This field is 32 bits in length.
  - ✓ It contains the result of applying the C-32 polynomial to the MAC header and frame body.

The following are some of the problems:

- ***Low data rate:***
  - The 802.11 protocol imposes very high overhead to all packets
    - It reduces real data rate significantly
- ***No QoS guarantees:***

- 802.11a, 802.11b, and 802.11g focus on higher data rates whereas 802.11e is aimed at providing QoS guarantees.

802.11b

5. Explain about 802.11b

1.3.6 802.11b

- IEEE 802.11b (IEEE 1999) was added as supplement to the original standard (Higher-speed physical layer extension in the 2.4 GHz band).
- This standard ***describes a new PHY layer*** and is the most successful version of IEEE 802.11 available today.
- As the name of the supplement implies, this standard only defines ***a new PHY layer***.

- All the MAC schemes, management procedures etc. explained above are used.
- Depending on the current interference and the distance between sender and receiver 802.11b systems offer 11, 5.5, 2, or 1 Mbit/s.
- Maximum user data rate is approx 6 Mbit/s.
- The lower data rates 1 and 2 Mbit/s use the 11-chip Barker sequence and DBPSK or DQPSK, respectively.

- The new data rates, 5.5 and 11 Mbit/s, use 8-chip **C**omplementary **C**ode **K**eying (**CCK**).
- The standard defines several packet formats for the physical layer.

- The ***mandatory format*** interoperates with the original versions of 802.11.
- The optional versions provide a ***more efficient data transfer*** due to shorter headers / different coding schemes.
- It can coexist with other 802.11 versions.

IEEE 802.11b PHY packet formats

- **Figure 1.22** shows ***two packet formats*** standardized for 802.11b.
- ***Long PLCP PPDU***
  - The mandatory format is called ***long PLCP PPDU*** and is similar to the format illustrated in **Figure 1.8**.
  - The difference is the rate encoded in the signal field, this is encoded in multiples of 100 kbit/s.
  - The preamble and the header are transmitted at 1 Mbit/s using DBPSK.

- ***Short PLCP PPDU format***
  - The optional ***short PLCP PPDU format*** differs in several ways.
  - The ***short synchronization field*** consists of ***56 scrambled zeros*** instead of scrambled ones.
  - **Short S**tart **F**rame **D**elimiter (SFD):
    - It consists of a mirrored bit pattern compared to the SFD of the long format:
      - 0000 0101 1100 1111 is used for the short PLCP PDU instead of 11110011 1010 0000 for the long PLCP PPDU.

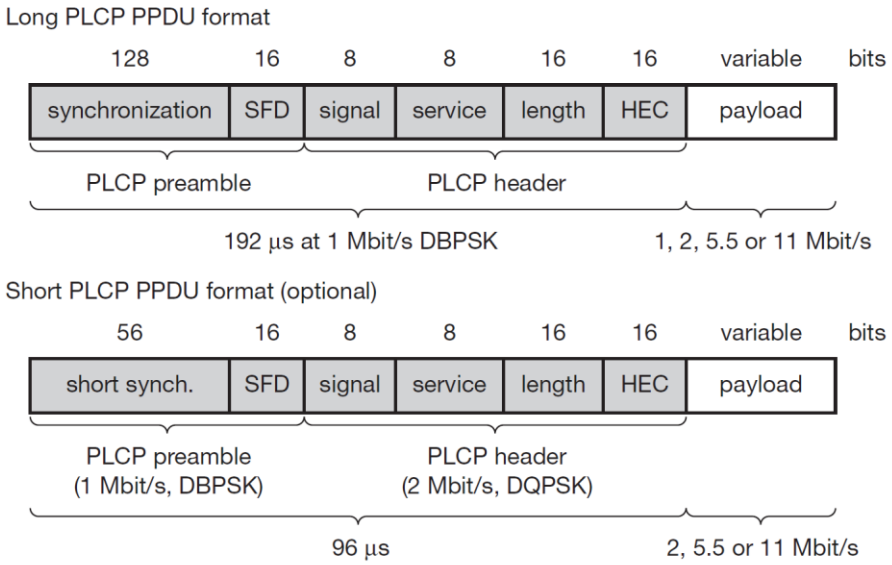


Figure 1.22 IEEE 802.11b PHY packet formats

- The preamble is transmitted at 1 Mbit/s, DBPSK.
- The following header is already transmitted at 2 Mbit/s, DQPSK, which is also the lowest available data rate.

- As ***Figure 1.22*** shows, the length of the overhead is only half for the short frames (96 µs instead of 192 µs).
- This is useful for, e.g., short, but time critical, data transmissions.
- The standards operates on certain frequencies in the 2.4 GHz ISM band.
- Figure 1.23 illustrates the non-overlapping usage of channels for an IEEE 802.11b installation with minimal interference in the US/Canada and Europe.
- The spacing between the center frequencies should be at least 25 MHz.
- This results in the channels 1, 6, and 11 for the US/Canada or 1, 7, 13 for Europe, respectively.
- It may be the case that, e.g., travellers from the US cannot use the additional channels (12 and 13)

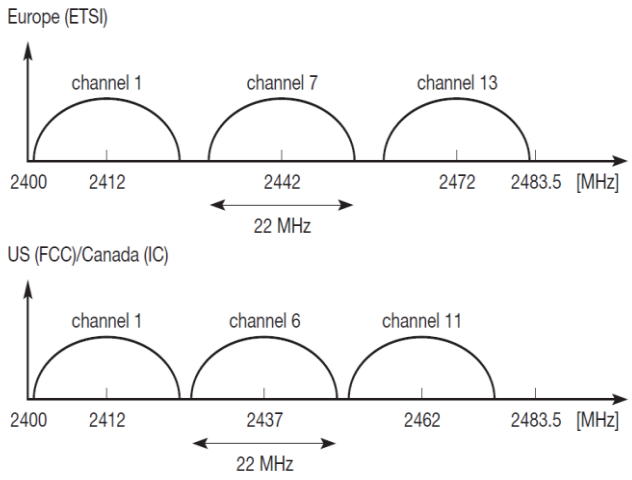


Figure 1.23 IEEE 802.11b non-overlapping channel selection

802.11a

6. Explain about 802.11a

1.3.7 802.11a

- The US 5 GHz U-NII (Unlicensed National Information Infrastructure) bands IEEE 802.11a offers up to ***54 Mbit/s using OFDM*** (IEEE,1999).
- The first products were available in 2001.
- The FCC (US) regulations offer ***three different 100 MHz domains*** for the use of 802.11a,
  - each with a different maximum power output: ***5.15–5.25 GHz/50 mW, 5.25–5.35 GHz/250 mW, and 5.725–5.825 GHz/1 W***.
- It requires two additional mechanisms for operation:
  - dynamic frequency selection (DFS), and
  - transmit power control (TPC)
- Maximum transmit power is
  - 200 mW EIRP for the lower frequency band (indoor use), and
  - 1 W EIRP for the higher frequency band (indoor and outdoor use).
- DFS and TPC are not necessary, if the transmit power stays below 50 mW EIRP and only 5.15–5.25 GHz are used.
- The physical layer of IEEE 802.11a and the ETSI standard HiperLAN2 has been jointly developed, so both physical layers are almost identical.
- Most explanations here are related to the transmission technology also valid for HiperLAN2.
- However, HiperLAN2 differs in the MAC layer, the PHY layer packet formats, and the offered services (quality of service, real time etc.).

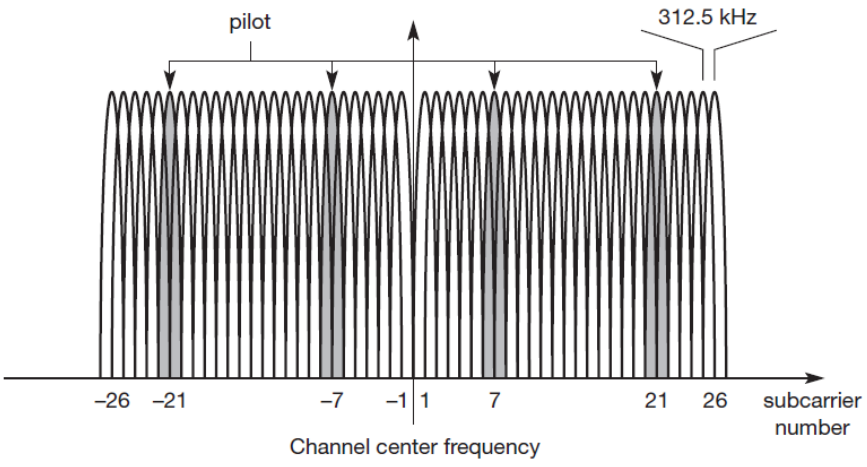


Figure 1.24 Usage of OFDM in IEEE 802.11a

- Figure 1.24 shows the usage of OFDM in IEEE 802.11a.
- Basic idea of OFDM (or MCM in general) was the ***reduction of the symbol rate*** by ***distributing bits over numerous subcarriers***.

- IEEE 802.11a uses a fixed symbol rate of 250,000 symbols per second independent of the data rate

- As Figure 1.24 shows, 52 subcarriers are equally spaced around a center frequency.
- The spacing between the subcarriers is 312.5 kHz.
- 26 subcarriers are to the left of the center frequency and 26 are to the right.
- The center frequency itself is not used as subcarrier.
- Subcarriers with the numbers –21, –7, 7, and 21 are used for ***pilot signals*** to make the signal detection robust against frequency offsets.

Channel layout for the US U-NII bands

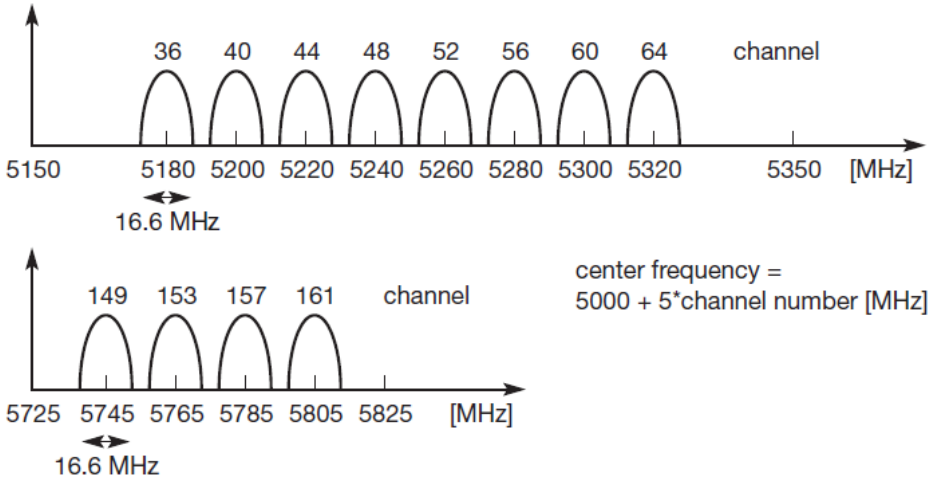


Figure 1.25 Operating channels of IEEE 802.11a in the U-NII bands

- Several operating channels have been standardized to minimize interference.
- Figure 1.25 shows the ***channel layout*** for the US U-NII bands.
- The ***center frequency of a channel*** is 5000 + 5*channel number [MHz].
- This definition provides a unique numbering of channels with 5 MHz spacing starting from 5 GHz.

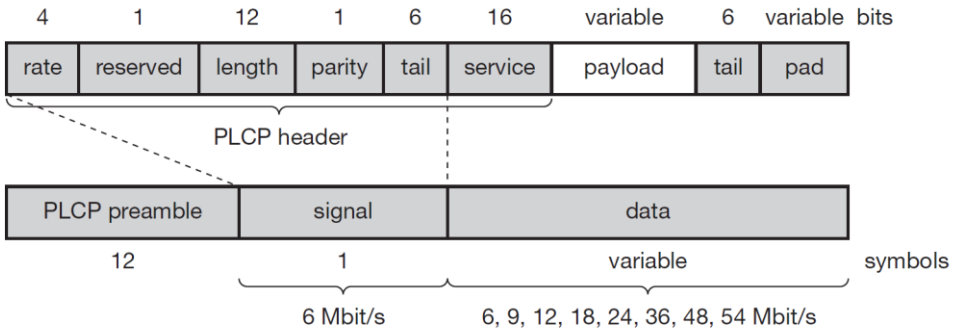


Figure 1.26 IEEE 802.11a physical layer PDU

- ***PLCP preamble:***
  - ✓ The PLCP preamble consists of 12 symbols.
  - ✓ It is used for frequency acquisition, channel estimation, and synchronization.
  - ✓ The duration of the preamble is 16 μs.
- ***Signal:*** The next ***OFDM symbol***, called ***signal***, contains the following fields and is BPSK-modulated.
  - ✓ ***Rate:*** The 4 bit rate field determines the data rate and the modulation of the rest of the packet (examples are 0x3 for 54 Mbit/s, 0x9for 24 Mbit/s, or 0xF for 9 Mbit/s).
  - ✓ ***Length:*** The length field indicates the *number of bytes in the payload field*.
  - ✓ ***Parity:*** It is an even parity for the first 16 bits of the signal field (rate, length and the reserved bit).
  - ✓ ***Tail:*** The six tail bits are set to zero.
- ***Data:***
  - ✓ The data field is sent with the rate determined in the rate field.
  - ✓ ***Service field*** is used to synchronize the descrambler of the receiver (the data stream is scrambled using the polynomial $x^7 + x^4 + 1$) and which contains bits for future use.
  - ✓ ***Payload:*** The payload contains the MAC PDU (1-4095byte).
  - ✓ ***Tail:*** The tail bits are used to reset the encoder.
  - ✓ ***Pad:*** Finally, the pad field ensures that the number of bits in the PDU maps to an integer number of OFDM symbols.

Compared to IEEE 802.11b working at 2.4 GHz IEEE 802.11a at 5 GHz offers much higher data rates. However, shading at 5 GHz is much more severe compared to 2.4 GHz and depending on the SNR, propagation conditions and the distance between sender and receiver, data rates may drop fast (e.g., 54 Mbit/s may be available only in an LOS or near LOS condition).

HIPERLAN
- **Historical: HIPERLAN 1**
- **WATM**
- **BRAN**
- **HiperLAN2**

HIPERLAN

7. Write short notes on HIPERLAN.	**(8m)**	**Dec 2014 May 2016**

- In 1996, the ETSI standardized HIPERLAN 1 as a WLAN.
- HIPERLAN stands for high performance local area network.
- It allows for ***node mobility*** and ***supporting ad-hoc and infrastructure-based topologies*** (ETSI,1996).

- HIPERLAN1 was originally one out of four HIPERLANs.
- The key feature of all four networks is their ***integration of time-sensitive data transfer services***.

- The names have changed and the HIPERLANs 2, 3, and 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK.
- The current focus is on HiperLAN2:
  - It is a standard that comprises many elements from ETSI's BRAN (**B**roadband **R**adio **A**ccess **N**etworks) and wireless ATM activities.

1.4.1 Historical: HIPERLAN 1

HIPERLAN 1

1.	**State the features and requirements of HIPERLAN standard.**	**(04m)**	**May 2015**
	Classify the HIPERLAN standard based on their architecture and protocol specification	**(12m)**	

- ETSI (1998b) describes HIPERLAN1 as a wireless LAN supporting priorities.
- The packet life time for data transfer at 23.5 Mbit/s.
- It includes forwarding mechanisms, topology discovery, user data encryption, network identification and power conservation mechanisms.
- HIPERLAN 1 should operate at 5.1–5.3 GHz.
- The range of HIPERLAN 1 is 50 m in buildings at 1W transmit power.
- The service offered by a HIPERLAN1 is compatible with the standard MAC services.
- Addressing is based on standard 48 bit MAC addresses.

- For power conservation, a node may set up a ***specific wake-up pattern***.
- This pattern determines at what time the node is ready to receive.
- At other times, the node can turn off its receiver and save energy.
- These nodes are called ***p-savers***.
- The ***p-supporters*** contains information about the wake-up patterns of all the ***p-savers*** they are responsible for.
- A ***p-supporter*** only forwards data to a ***p-saver*** at the moment the ***p-saver*** is awake.
- This action also requires buffering mechanisms for packets on ***p-supporting forwarders***.

Elimination-yield non-preemptive priority multiple access (EY-NPMA) is not only a complex acronym, but also the heart of the channel access providing priorities and different access schemes.

EY-NPMA divides the medium access of different competing nodes into three phases:

- ***Prioritization:*** Determine the highest priority of a data packet ready to be sent by competing nodes.
- ***Contention:*** Eliminate all but one of the contenders ***(competitors)***, if more than one sender has the highest current priority.
- ***Transmission:*** Finally, transmit the packet of the remaining node.

Prioritization:

- ***Channel access in synchronized channel condition:***
  - ✓ In a case where several nodes compete for the medium, here, all three phases are necessary.
- ***Channel access in channel-free condition:***

- ✓ If the channel is free for at least 2,000 so-called high rate bit-periods plus a dynamic extension.
- ✓ Here, only the third phase, i.e. transmission, is needed.

➢ ***Channel access in the hidden elimination condition:***

- ✓ HIPERLAN 1 also supports 'channel access in the hidden elimination condition'.
- ✓ It is to handle the problem of ***hidden terminals*** as in ETSI (1998b).

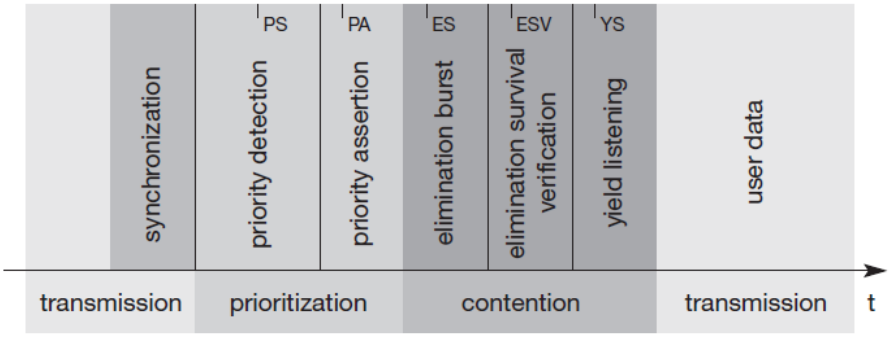


Figure 1.27 Phases of the HIPERLAN1 EY-NPMA access scheme

Contention phase:

- ➢ The contention phase is divided into an ***elimination phase*** and a ***yield phase***.
- ➢ ***Elimination phase:***
  - ▪ ***Purpose***: This phase ***eliminates as many contending (Competing) nodes*** as possible (but not all).
  - ▪ ***Result of elimination phase:*** More or less ***constant number of remaining nodes***.
- ➢ ***Yield phase:***
  - ▪ Finally, the yield phase completes the work of the elimination phase with the goal of ***only one remaining node***.

➢ Figure 1.27 gives an ***overview of the three main phases***.

- ✓ The first phase is prioritization.
- ✓ After that, the elimination and yield part of the contention phase follow.
- ✓ Finally, the remaining node can transmit its data.

Every phase has a ***certain duration*** which is ***measured in 'numbers of slots'*** and is determined by the variables I_{PS}, I_{PA}, I_{ES}, I_{ESV}, and I_{YS}.

1.4.1.1 Prioritization phase

➢ HIPERLAN 1 offers ***five different priorities*** for data packets ready to be sent.

➢ After one node has finished sending, many other nodes can contest for the ***right to send***.

➢ ***First objective:***

- o The prioritization phase is to make sure that ***no node with a lower priority gains access to the medium, while packets with higher priority are waiting at other nodes***.

➢ This mechanism, always

- o *allows the nodes with higher priority access to the medium, no matter* ***how high the load with lower priorities***.

- In the ***first step*** of the prioritization phase,
  - the priority detection, time is divided into ***five slots, slot 0 (highest priority)*** to ***slot 4 (lowest priority)***.
- Each slot has a duration of I_{PS} = 168 high rate bit-periods.
- If a node has the access priority ***p***, it has to listen into the medium for ***p slots*** (priority detection).

- If the ***node senses the medium is idle*** for the whole period of ***p*** slots, the node declares the priority by transmitting ***a burst*** for the duration I_{PA} = 168 high rate bit-periods (priority assertion).
- The burst consists of the following ***high rate bit sequence***, which is repeated as many times as necessary:

  111110101000100111000001100101110

- If the ***node senses activity in the medium***, it stops its attempt to send data in this transmission cycle and waits for the next one.
- The whole prioritization phase ends as soon as one node declares the access priority with a burst.

Example:

- Let us assume, for example,
  - there are three nodes with data ready to be sent,
  - the packets of node 1 and node 2 having the priority 2,
  - the packet of node 3 having the priority 4.
- Then
  - Nodes 1, 2 and 3 listen into the medium and senses slots 0 and 1 are idle.
  - Nodes 1 and 2 both send a burst in slot 2 as priority assertion.
  - Node 3 stops its attempt to transmit its packet.
- In this example, the prioritization phase has taken three slots.
- After this first phase at least one of the contending nodes will survive, the surviving nodes being all nodes with the highest priority of this cycle.

1.4.1.2 Elimination phase

- Several nodes now enter the ***elimination phase***.
- Again, time is divided into slots, using the elimination slot interval I_{ES} = 212 high rate bit periods.
- The length of an individual elimination burst is 0 to 12 slot intervals long.
- The probability $P_E(n)$ of an elimination burst to be ***n*** elimination slot intervals long is given by:

  $P_E(n) = 0.5^{n+1}$ for $0 \leq n < 12$

  $P_E(n) = 0.5^{12}$ for $n = 12$

- The elimination phase now resolves contention by means of ***elimination bursting*** and ***elimination survival verification***.
- Each contending node sends an elimination burst with length ***n***.
- Then, the contending node, listens to the channel during the ***survival verification interval*** I_{ESV} = 256 high rate bit periods.
- The burst sent is the same as for the priority assertion.

- A contending node survives this elimination phase if, and only if, it senses the channel is idle during its survival verification period.
- Otherwise, the node is eliminated and stops its attempt to send data during this transmission cycle.
- One or more nodes will survive this elimination phase, and can then continue with the next phase.

1.4.1.3 Yield phase

- During the yield phase, the remaining nodes *only* listen into the medium without sending any additional bursts.
- Again, time is divided into slots, called ***yield slots*** with a duration of I_{YS} = 168 high rate bit-periods.
- The length of an individual yield listening period can be 0 to 9 slots with equal possibility.
- The probability $P_Y(n)$ for a yield listening period to be n slots long is 0.1 for all $\boldsymbol{n}$, $0 \leq \boldsymbol{n} \leq 9$.

- Each node now listens for its yield listening period.
- If it senses the channel is idle during the whole period, it has survived the yield listening.
- Otherwise, it withdraws for the rest of the current transmission cycle.
- This time, the length of the yield phase is determined by the shortest yield-listening period among all the contending nodes.
- At least one node will survive this phase and can start to transmit data. This is what the other nodes with longer yield listening period can sense.

1.4.1.4 Transmission phase

- A node that has survived the prioritization and contention phase can now send its data, called a low bit-rate high bit-rate HIPERLAN 1 CAC ***Protocol Data Unit*** (LBR-HBR HCPDU).
- This PDU can either be multicast or unicast.
- In case of a unicast transmission, the sender expects to receive an immediate acknowledgement from the destination, called an acknowledgement HCPDU (AK-HCPDU).

1.4.1.5 Quality of service support and other specialties

- The specialty of HIPERLAN 1 is its QoS support.
- The quality of service offered by the MAC layer is based on three parameters (HMQoS-parameters).
- The user can set a priority for data, priority = 0 denotes a high priority, priority = 1, a low priority.
- The ***MSDU lifetime*** specifies the maximum time that can elapse between sending and receiving an MSDU.
- Beyond this, delivery of the MSDU becomes unnecessary.
- The MSDU lifetime has a range of 0–16,000 ms.

Table 1.4 Mapping of the normalized residual lifetime to the CAC priority

NRL	MSDU priority = 0	MSDU priority = 1
NRL < 10 ms	0	1
10 ms ≤ NRL < 20 ms	1	2
20 ms ≤ NRL < 40 ms	2	3
40 ms ≤ NRL < 80 ms	3	4
80 ms ≤ NRL	4	4

The final selection of the most important HMPDU (HIPERLAN 1 MAC PDU) is performed in the following order:

- HMPDUs with the highest priority are selected; from these, all HMPDUs with the shortest NRL are selected; from which finally any one without further preferences is selected from the remaining HMPDUs.

WATM

Motivation for WATM
Wireless ATM working group
WATM services
Generic reference model
Handover
Location management
Mobile quality of service

1.4.2 WATM

2. Explain in detail about WATM.

- Wireless ATM (WATM; sometimes also called wireless, mobile ATM, wmATM) describes a ***transmission technology***.

1.4.2.1 Motivation for WATM

Reasons led to the development of WATM:

- The need for integration of wireless terminals into an ATM network.
- Strategies are needed to extend ATM for wireless access in local and global environments.
- WATM could offer QoS for adequate support of multi-media data streams.

Specialty of WATM:

- The WATM is much more complex than most of the other wireless systems.
- IEEE 802.11 only covers local area access methods, Bluetooth only builds up piconets.
- Mobile IP only works on the network layer, but WATM tries to build up a complete system covering ***physical layer, media access, routing, integration*** into the fixed ATM network.

1.4.2.2 Wireless ATM working group

- The ATM Forum formed the Wireless ATM Working Group in 1996.
- This work group is to develop ***a set of specifications that expands the use of ATM technology*** to wireless networks.
- These wireless networks should cover many different networking scenarios, such as private and public, local and global, mobility and wireless access.

The following more general extensions of the ATM system also need to be considered for a mobile ATM:

- ***Location management:***
  - WATM networks must be able to locate a wireless terminal or a mobile user,
  - Location management is to find the current access point of the terminal to the network.
- ***Mobile routing:***
  - Each time a user moves to a new access point, the system must reroute traffic.
- ***Handover signaling:***
  - The network must provide mechanisms which
    - search for new access points
    - set up new connections between intermediate systems, and
    - signal the actual change of the access point.
- ***QoS and traffic control:***
  - WATM should be able to offer many QoS parameters.
  - To maintain these parameters, all actions such as rerouting, handover etc. have to be controlled.
  - The network must pay attention to the incoming traffic.
- ***Network management:***
  - All extensions of protocols or other mechanisms also require an extension of the management functions to control the network

To ensure wireless access, the working group discussed the following topics belonging to a radio access layer (RAL):

- ***Radio resource control:*** The radio frequencies, modulation schemes, antennas, channel coding etc. have to be determined.
- ***Wireless media access:*** Different media access schemes are possible.
  e.g., multi-media or voice applications.

Different centralized or distributed access schemes working on ATM cells can be imagined.

- ***Wireless data link control:***
  - The data link control layer offers header compression for an ATM cell.
  - It carries almost 10 per cent overhead using a 5 byte header in a 53 byte cell.
  - This layer can apply ARQ or FEC schemes to improve reliability.
- ***Handover issues:***
  - During handover, cells can be lost and also become out of sequence.
  - Cells must be ***re-sequenced*** and lost cells must be ***retransmitted*** if required.

1.4.2.3 WATM services

WATM systems had to be designed for transferring voice, classical data, video (from low quality to professional quality), multimedia data, short messages etc.

Several service scenarios could be identified, such as for example:

- ***Office environments:***
  - This includes all kinds of extensions for existing fixed networks.
  - ***Services:*** Internet/Intranet access, multi-media conferencing, online multi-media database access, and telecommuting.

- ***Universities, schools, training centers:***
  - ***Services:*** Distance learning, wireless and mobile access to databases, internet access, or teaching in the area of mobile multi-media computing.
- ***Industry:***
  - ***Services:*** Intranet supporting database connection, information retrieval, surveillance, real-time data transmission and factory management.
- ***Hospitals:***
  - WATM is best in reliable, high-bandwidth mobile and wireless networks.
  - ***Services:*** The transfer of medical images, remote access to patient records, remote monitoring of patients, remote diagnosis of patients at home or in an ambulance and tele-medicine.
- ***Home:***
  - ***Services:*** Many electronic devices at home (e.g., TV, radio equipment, CD-player, PC with internet access) could be connected using WATM technology.
  - Here, WATM would permit ***various wireless connections***, e.g., a PDA with TV access.
- ***Networked vehicles:***
  - All vehicles used for the transportation of people or goods will have a local network and network access in the future.
- ***Satellite ATM services:***
  - Future satellites will offer a large variety of TV, interactive video, multi-media, Internet, telephony and other services.

1.4.2.4 Generic reference model

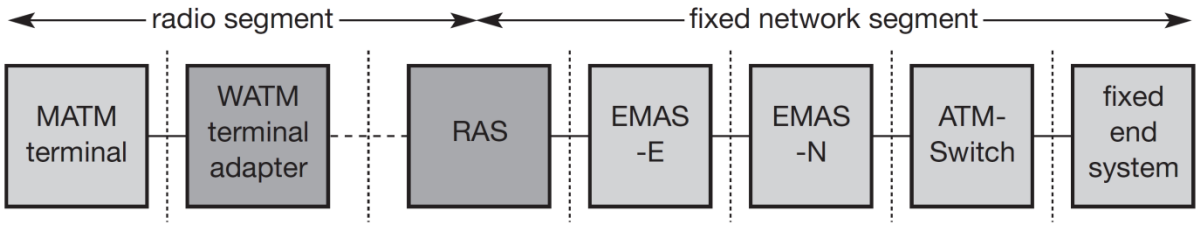


Figure 1.28 Example of a generic WATM reference model

- Figure 1.28 shows a common reference model for wireless mobile access to an ATM network.

- A mobile ATM (MATM) terminal uses a WATM terminal adapter to gain wireless access to a WATM **RAS** (**R**adio **A**ccess **S**ystem).

- MATM terminals could be represented by, e.g., laptops using an ATM adapter for wired access plus software for mobility.
- The WATM terminal adapter enables wireless access, i.e., it includes the transceiver etc., but it does not support mobility.
- The RAS with the radio transceivers is connected to a **M**obility **E**nhanced **A**TM **S**witch (EMAS-E).
- In turn, it connects to the ATM network with **M**obility **A**ware **S**witches (EMAS-N) and other standard ATM switches.

1.4.2.5 Handover

- Connectionless, best-effort protocols supporting handover, such as
  - ***mobile IP on layer 3*** and ***IEEE 802.11 with IAPP on layer 2***, do not have to take too much care about handover quality.
- In WATM, the main problem during the handover is ***rerouting all connections and maintaining connection quality***.
- Handover involves rerouting of connections.
- Handover, also involves ***reserving resources in switches, testing of availability of radio bandwidth, tracking of terminals to perform look-ahead reservations*** etc.

Many different requirements have been set up for handover:

- ***Handover of multiple connections:***
  - ✓ As ATM is a connection-oriented technology.
  - ✓ Here ***end-systems can support many connections at the same time***.
  - ✓ This results in the rerouting of every connection after handover.
- ***Handover of point-to-multi-point connections:***
  - ✓ WATM handover provides a perfect ***support of point-to-multi-point connections***.
- ***QoS support:***
  - ✓ Handover should aim to preserve the QoS of all connections during handover.
  - ✓ Due to limited resources, this is not always possible.
  - ✓ Functions for QoS re-negotiation and dropping of connections on a priority basis is required.
- ***Data integrity and security:***
  - ✓ WATM handover should ***minimize cell loss and avoid all cell duplication or re-ordering***.
  - ✓ ***Security associations*** between the terminal and the network should not be compromised by handover.
- ***Signaling and routing support:***
  - ✓ WATM must provide the resources
    - to identify mobility-enabled switches in the network,
    - to determine radio adjacent switches by another switch, and
    - to reroute partial connections in the handover domain.
- ***Performance and complexity:***
  - ✓ Modifications to the mobility-enabled switches should be extremely limited.
  - ✓ The functions required severe processing time requirements.

1.4.2.6 Location management

- Special functions are required to look up the current position of a mobile terminal.
- This is to provide the moving terminal with a permanent address, and for ensuring security features such as privacy, authentication, or authorization.
- These and more functions are grouped under the term location management.

Several requirements for location management have been identified (Bhat, 1998):

- ***Transparency of mobility:***
  - ✓ Transparent roaming between different domains (private/private, private/public, public/public) should be possible.

- ***Security:***
  - ✓ To provide a high level security a WATM system requires special features.
  - ✓ All location and user *information collected for location management and accounting* ***(bookkeeping)*** *should be protected*.
  - ✓ Essential security features include ***authentication*** of *users and terminals* and also the *access points*.
  - ✓ ***End-to-end Encryption*** is also necessary between terminal and access point.
- ***Efficiency and scalability:***
  - ✓ Imagine WATM networks with millions of users like today's mobile phone networks.
  - ✓ Every function and system involved in location management must be scalable and efficient.
- ***Identification:***
  - ✓ Location management must provide the resources to identify all entities of the network.
  - ✓ Radio cells, WATM networks, terminals, and switches need unique identifiers and mechanisms to exchange identity information.
  - ✓ In addition to the *permanent **A**TM **E**nd **S**ystem **A**ddress (**AESA**)*, a terminal also needs a ***routable temporary AESA*** as soon as it is outside its home network.
  - ✓ This temporary AESA must be forwarded to the terminal's home location.

- ***Inter-working and standards:***
  - ✓ Location management in WATM has to be coordinated with other location management schemes, such as (existing ATMs)
    - location management in GSM and UMTS networks,
    - the internet using Mobile IP, or Intranets with special features.
  - ✓ All protocols used in WATM for database updates, registration etc. have to be standardized to permit mobility across provider network boundaries.

1.4.2.7 Mobile quality of service

Quality of service (QoS) guarantees are one of the main advantages envisaged for WATM networks compared to, e.g., mobile IP working over packet radio networks.

While the internet protocol IP does not guarantee QoS, ATM networks do (at the cost of higher complexity). WATM networks should provide mobile QoS (M-QoS).

M-QoS is composed of three different parts:

- ***Wired QoS:***
  - ✓ WATM needs the same QoS properties as any wired ATM network.
  - ✓ Typical traditional QoS parameters are ***link delay, cell delay variation, bandwidth, cell error rate etc***.
- ***Wireless QoS:***
  - ✓ The QoS properties of the wireless part of a WATM network differ from those of the wired part.
  - ✓ Channel reservation and multiplexing mechanisms at the air interface strongly influence cell delay variation.
- ***Handover QoS:***
  - ✓ A new set of QoS parameters are introduced by handover.

- ✓ ***Critical factors of QoS:*** Handover blocking due to limited resources at target access points, cell loss during handover, or the speed of the whole handover procedure.

These protocols can support two different types of QoS during handover:

- ***Hard handover QoS:***
  - ✓ No QoS guarantees are given after the handover.
  - ✓ If a terminal can set up a connection, the connection's quality is guaranteed.
  - ✓ If there are no enough resources after handover, the system cuts off the connection.
- ***Soft handover QoS:***
  - ✓ Even for the current wireless segment, only statistical QoS guarantees can be given, and the applications have to adapt after the handover.
  - ✓ This assumes adaptive applications and allows some remaining QoS guarantees during periods of congestion or strong interference.

1.4.2.8 Access scenarios

Figure 1.29 shows possible access scenarios for WATM and illustrates what was planned during the specification of WATM.

Figure 1.29 shows the following components:

- ***T (terminal):*** A standard ATM terminal providing ATM services defined for fixed ATM networks.
- ***MT (mobile terminal):***
  - ✓ A standard ATM terminal with the additional capability of reconnecting after access point change.
  - ✓ The terminal can be moved between different access points within a certain domain.
- ***WT (wireless terminal):*** This terminal is accessed via a wireless link, but the terminal itself is fixed, i.e., the terminal keeps its access point to the network.
- ***WMT (wireless mobile terminal):***
  - ✓ The combination of a wireless and mobile terminal results in the WMT.
  - ✓ This is exactly the type of terminal presented throughout this WATM section.
  - ✓ It has the ability to change its access point and uses radio access.

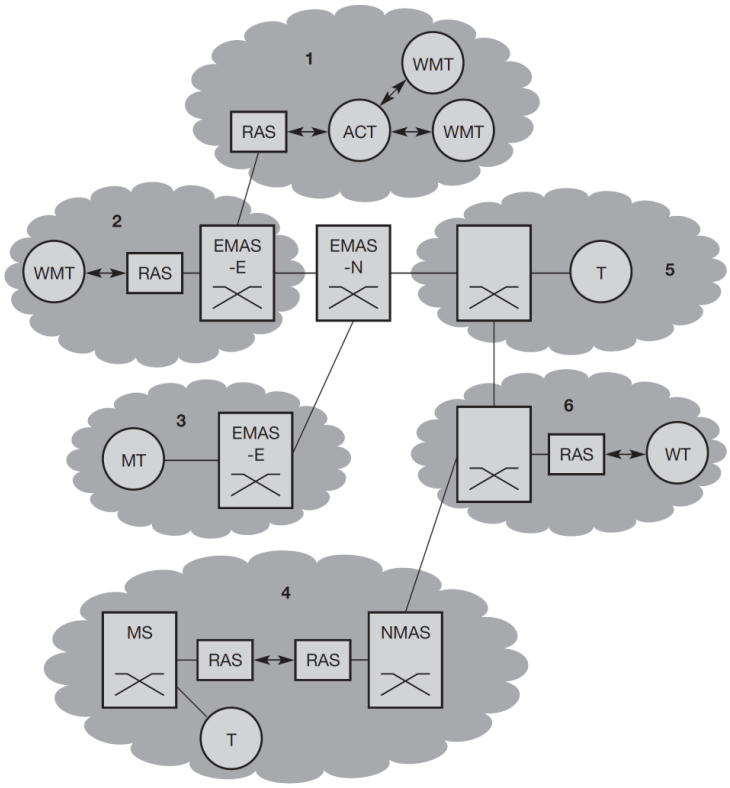


Figure 1.29 WATM reference model with several access scenarios

- ***RAS (radio access system):*** Point of access to a network via a radio link as explained in this chapter.
- ***EMAS (end-user mobility supporting ATM switch, -E: edge, -N: network):*** Switches with the support of end-user mobility.
- ***NMAS (network mobility-supporting ATM switch):*** A whole network can be mobile not just terminals. Certain additional functions are needed to support this mobility from the fixed network.
- ***MS (mobile ATM switch):*** ATM switches can also be mobile and can use wireless access to another part of the ATM network.
- ***ACT (ad-hoc controller terminal):***
  - ✓ For the configuration of ad-hoc networks, special terminal types are required in the wireless network.
  - ✓ These terminals could control wireless access without an RAS.

Scenarios:

Wireless ad-hoc ATM network (scenario 1):

- ✓ WMTs can communicate with each other without a fixed network.
- ✓ Communication can be set up without any infrastructure.
- ✓ Access control can be accomplished via the ACT.
- ✓ If the ad-hoc network needs a connection to a fixed network, this can be given by an RAS.

- ***Wireless mobile ATM terminals (scenario 2):***
  - ✓ In this configuration, a WMT cannot communicate without the support given by entities within the fixed network, such as an EMAS-E.
- ***Mobile ATM terminals (scenario 3):***

- ✓ This configuration supports device portability and simple network reconfiguration.
- ✓ Users can change the access points of their ATM equipment, without the need for reconfiguration by hand.
- ✓ This scenario needs support through entities in the fixed network (e.g., EMAS-E).

➢ ***Mobile ATM switches (scenario 4):***

- ✓ More complex configuration comprises mobile switches using wireless access to other fixed ATM networks.
- ✓ The entities supporting switch mobility are needed within the fixed network (NMAS).
- ✓ There are many applications for this scenario, e.g., networks in aircraft, trains, or ships.
- ✓ Within the mobile network either fixed, mobile, wireless, or mobile and wireless terminals can be used.
- ✓ This is the most complex configuration ever foreseen within an ATM environment.

➢ ***Fixed ATM terminals (scenario 5):***

- ✓ This configuration is the standard case.
- ✓ Terminals and switches do not include capabilities for mobility or wireless access.
- ✓ This is also the reference configuration for applications which work on top of an ATM network.

➢ ***Fixed wireless ATM terminals (scenario 6):***

- ✓ This is the ideal solution, to provide simple access to ATM networks without wiring.
- ✓ This scenario does not require any changes or enhancements in the fixed network.

1.4.3 BRAN

3. Explain in detail about BRAN.

➢ The ***Broadband Radio Access Networks*** (BRAN), which have been standardized by the ***European Telecommunications Standards Institute*** (ETSI).

➢ The main motivation behind BRAN is

- o the deregulation and privatization of the telecommunication sector in Europe.

➢ One possible technology to provide network access for customers is radio.

➢ The advantages of radio access are high flexibility and quick installation.

➢ Different types of traffic are supported, one can multiplex traffic for higher efficiency.

➢ BRAN includes private customers and small to medium-sized companies with Internet applications, multi-media conferencing, and virtual private networks.

➢ The BRAN standard and IEEE 802.16 (Broadband wireless access, IEEE, 2002b) have similar goals.

BRAN standardization has a rather large scope including indoor and campus mobility, transfer rates of 25–155 Mbit/s, and a transmission range of 50 m–5 km. Standardization efforts are coordinated with the ATM Forum, the IETF, other groups from ETSI, the IEEE etc.

BRAN has specified four different network types (ETSI, 1998a):

➢ ***HIPERLAN 1:***

- ✓ This high-speed WLAN supports mobility at data rates above 20 Mbit/s.

- ✓ Range is 50 m, connections are multi-point-to-multi-point using ad-hoc or infrastructure networks.

➢ ***HIPERLAN/2:***
- ✓ This technology can be used for wireless access to ATM or IP networks.
- ✓ It supports up to 25 Mbit/s user data rate in a point-to-multi-point configuration.
- ✓ Transmission range is 50 m with support of slow (< 10 m/s)mobility (ETSI, 1997).

➢ ***HIPERACCESS:***
- ✓ This technology used to cover the 'last mile' to a customer via a fixed radio link, so could be an alternative to cable modems or xDSL technologies.
- ✓ Transmission range is up to 5 km, datarates of up to 25 Mbit/s are supported.
- ✓ But, many proprietary products offer 155 Mbit/s and more, plus QoS.

➢ ***HIPERLINK:***
- ✓ To connect different HIPERLAN access points or HIPERACCESS nodes with a high-speed link, HIPERLINK technology can be chosen.
- ✓ HIPERLINK provides a fixed point-to-point connection with up to 155 Mbit/s.

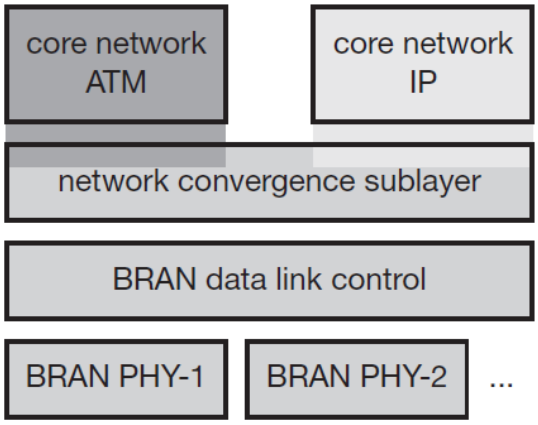


Figure 1.30 Layered model of BRAN wireless access networks

- ➢ BRAN technology, as an access network, is independent from the protocols of the fixed network.
- ➢ BRAN can be used for ***ATM and TCP/IP networks*** as illustrated in Figure 1.30.
- ➢ Based on different physical layers, the DLC layer of BRAN offers a common interface to higher layers.
- ➢ Network convergence sublayer:
  - o To cover special characteristics of wireless links, and
  - o To adapt directly to different higher layer network technologies.
  - o This layer can be used by a wireless ATM network, Ethernet, Firewire, or an IP network.

*****

1.4.4 HiperLAN2

Hiperlan2

Reference model and configurations
Physical layer
Data link control layer
Convergence layer

4. Explain the architecture and sublayers of HIPERLAN.	**(16m)**	**Apr 2014 May 2016**
5. Define Hiperlan-2. Discuss about the various operation modes and protocol stack in Hiperlan-2.	**(16m)**	**Nov 2017**
6. Explain the architecture of Hyperlan II protocol.	**(16m)**	**May 2018**

General features:

- This is also written as HIPERLAN/2, HiperLAN/2, H/2
- Official name: HIPERLAN Type 2.
- Standardized by ETSI (2000a) this wireless network works at 5 GHz
- It offers data rates of up to 54 Mbit/s including QoS support and enhanced security features.

Features of HIPERLAN2:

In comparison with basic IEEE 802.11 LANs, HiperLAN2 offers more features in the mandatory parts of the standard (HiperLAN2, 2002).

- ***High-throughput transmission:***
  - ✓ It uses OFDM in the physical layer and a dynamic TDMA/TDD-based MAC protocol.
  - ✓ HiperLAN2 offers up to 54 Mbit/s at the physical layer and about 35 Mbit/s at the network layer.
  - ✓ HiperLAN2 uses MAC frames with a constant length of 2 ms.
- ***Connection-oriented:***
  - ✓ HiperLAN2 networks establish logical connections between a sender and a receiver (e.g., mobile device and access point) before to data transmission.
  - ✓ All connections are time-division-multiplexed over the air interface (TDMA with TDD).
  - ✓ Bidirectional point-to-point and unidirectional point-to-multipoint connections are offered.
  - ✓ A ***broadcast channel*** is available ***to reach all mobile devices*** in the transmission range of an access point.
- ***Quality of service support:***
  - ✓ With the help of connections, support of QoS is much simpler.
  - ✓ Each connection has its own set of QoS parameters (bandwidth, delay, jitter, bit error rate etc.).
  - ✓ A more simplistic scheme using priorities only is available.
- ***Dynamic frequency selection:***
  - ✓ HiperLAN2 does not require frequency planning of cellular or IEEE 802.11 networks.
  - ✓ All access points have built-in support to automatically select an appropriate frequency within their coverage area.

- ✓ All APs listen to neighboring APs as well as to other radio sources in the environment.

- ***Security support:***
  - ✓ Authentication as well as encryption are supported by HiperLAN2.
  - ✓ Both, mobile terminal and access point can authenticate each other.
  - ✓ Additional functions (directory services, key exchange schemes etc.) are needed to support authentication.
  - ✓ All user traffic can be encrypted using DES, Triple-DES, or AES to protect against attacks.
- ***Mobility support:***
  - ✓ Mobile terminals can move around.
  - ✓ The transmission takes place between ***the terminal and the access point with the best radio signal***.
  - ✓ Handover between access points is performed automatically.
  - ✓ Some data packets may be lost during handover.
- ***Application and network independence:***
  - ✓ HiperLAN2 was not designed with a certain group of applications or networks in mind.
  - ✓ Interoperation with 3G networks is also supported.
- ***Power save:***
  - ✓ Mobile terminals can negotiate certain wake-up patterns to save power.
  - ✓ Depending on the sleep periods either ***short latency requirements*** or ***low power requirements*** can be supported.

The following sections show the reference model of HiperLAN2 and illustrate some more features.

1.4.4.1 Reference model and configurations

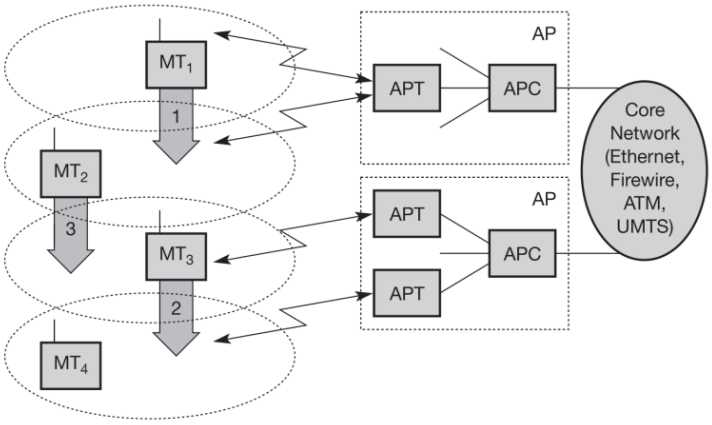


Figure 1.31 HiperLAN2 basic structure and handover scenarios

- ***Figure 1.31*** shows the standard architecture of an infrastructure-based HiperLAN2 network.
- In the example, two access points (AP) are attached to a core network.
- Core networks might be Ethernet LANs, Firewire (IEEE 1394) connections between audio and video equipment, ATM networks, UMTS 3G cellular phone networks etc.
- Each AP consists of an access point controller (APC) and one or more access point transceivers (APT).
- An APT can comprise one or more sectors (shown as cell here).

- Finally, four mobile terminals (MT) are also shown.
- MTs can move around in the cell area as shown.
- The system automatically assigns the APT/AP with the best transmission quality.
- ***Frequency planning*** is not necessary, because the APs automatically select the appropriate frequency by dynamic frequency selection.

Three handover situations may occur:

- ***Sector handover (Inter sector):***
  - ✓ If sector antennas are used for an AP, the AP shall support sector handover.
  - ✓ This type of handover is handled inside the DLC layer so is not visible outside the AP.
- ***Radio handover (Inter-APT/Intra-AP):***
  - ✓ This type too, is handled within the AP, no external interaction is needed.
  - ✓ In the example of Figure 1.31 the terminal MT3, moves from one APT to another of the same AP.
  - ✓ All ***context data*** for the connections are already in the AP ***(encryption keys, authentication, and connection parameters)***
  - ✓ .
- ***Network handover (Inter-AP/Intra-network):***
  - ✓ This is the most complex situation: MT2 moves from one AP to another.
  - ✓ In this case, the core network and higher layers are also involved.
  - ✓ This handover might be supported by the core network (similar to the IAPP, IEEE 802.11f).
  - ✓ Otherwise, the MT must provide the required information similar to the situation during a new association.

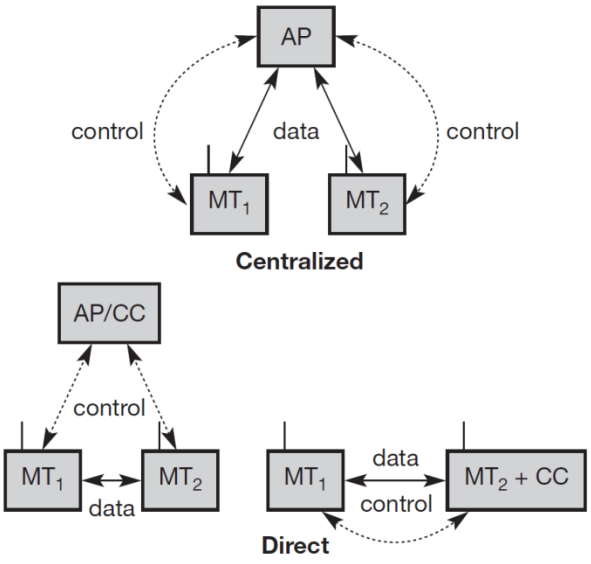


Figure 1.32 HiperLAN2 centralized vs direct mode

HiperLAN2 networks can operate in two different modes: (which may be used simultaneously in the same network).

- ***Centralized mode (CM):***

- ✓ This infrastructure-based mode is shown again in a more abstract way in ***Figure 1.32*** (left side).
- ✓ All APs are connected to a core network and MTs are associated with APs.
- ✓ Even if two MTs share the same cell, all data is transferred via the AP.
- ✓ In this mandatory mode the AP takes complete control of everything.

➢ ***Direct mode (DM):***

- ✓ The optional ad-hoc mode of HiperLAN2 is illustrated on the right side of ***Figure 1.32***.
- ✓ Data is directly exchanged between MTs if they can receive each other, but the network has to be controlled.
- ✓ This is done via an AP, that contains a central controller (CC).
- ✓ There is no real difference between an AP and a CC.
- ✓ The APs are always connected to an infrastructure but here only the CC functionality is needed.

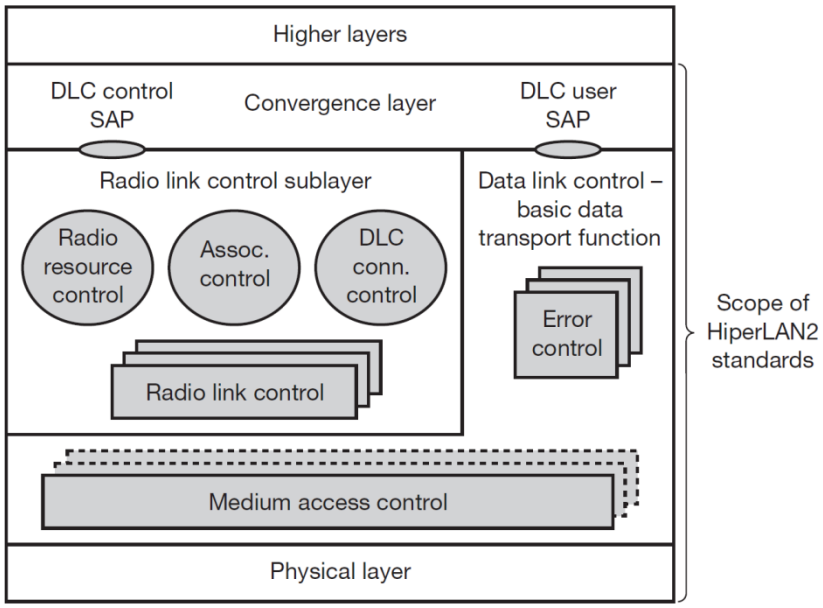


Figure 1.33 HiperLAN2 protocol stack

➢ ***Figure 1.33*** shows the HiperLAN2 protocol stack as used in access points.

➢ Protocol stacks in mobile terminals differ by ***the number of MAC and RLC instances*** (only one of each).

➢ ***Physical layer:***

- ✓ The lowest layer.
- ✓ It handles all the functions related to modulation, forward error correction, signal detection, synchronization etc.

➢ ***Data Link Control (DLC) layer :***

- ✓ The data link control (DLC) layer contains
  - the MAC functions,
  - the RLC sublayer, and
  - error control functions.
- ○ If an AP comprises several APTs then each APT requires an own MAC instance.

- ✓ The MAC of an AP assigns each MT a certain capacity to guarantee connection quality depending on available resources.
- ✓ Above the MAC, DLC is divided into a ***control and a user part***.
  - This separation is common in classical connection-oriented systems such as cellular phones or PSTN.
- ✓ The user part contains error control mechanisms.

Transmission

- HiperLAN2 offers reliable data transmission using acknowledgements and retransmissions.
- For broadcast transmissions a repetition mode can be used that provides increased reliability by repeating data packets.
- Additionally, unacknowledged data transmission is available.

- ***Radio Link Control (RLC):***
  - ✓ The radio link control (RLC) sublayer comprises most control functions in the DLC layer (the CC part of an AP).
  - ✓ The association control function (ACF) controls ***association and authentication*** of new MTs as well as synchronization of the radio cell via beacons.

- ***DLC user connection control (DCC or DUCC) service:***
  - ✓ It controls connection setup, modification, and release.

- ***Radio Resource Control (RRC):***
  - ✓ Finally, the radio resource control (RRC).
  - ✓ It handles handover between APs and within an AP.
  - ✓ These functions control the dynamic frequency selection and power save mechanisms of the MTs.

- ***Convergence layer:***
  - ✓ On top of the DLC layer there is the convergence layer.
  - ✓ This highest layer in HiperLAN2 standardization may comprise segmentation and reassembly functions and adaptations to fixed LANs, 3G networks etc.

The following sections give some more insight into the HiperLAN2 layers.

1.4.4.2 Physical layer

- Many functions and features of HiperLAN2's physical layer (ETSI, 2001a) served as an example for IEEE 802.11a.
- Both standards offer similar data rates and use identical modulation schemes.

- Figure 1.34 illustrates ***the reference configuration of the transmission chain*** of a HiperLAN2 device.

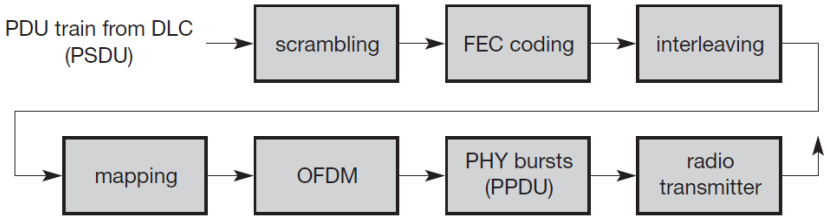


Figure 1.34 HiperLAN2 physical layer reference configuration

- After selecting one of the above transmission modes, the DLC layer passes a PSDU to the physical layer (PSDUs are called DLC PDU trains in the HiperLAN2 context).

- ***First step:***
  - ✓ The first step is scrambling of all data bits with the generator polynomial $x^7 + x^4 + 1$ for DC blocking and whitening of the spectrum.
  - ✓ The result of this first step are scrambled bits.
- ***Second step:***
  - ✓ The next step applies FEC coding for error protection.
  - ✓ Coding depends on the ***type of data*** (broadcast, uplink, downlink etc.) and the ***usage of sector or omni-directional antennas***.
  - ✓ The result of this step is an encoded bit.
- ***Third Step:***
  - ✓ For lessening of frequency selective fading, ***interleaving*** is applied.
  - ✓ Interleaving ensures that ***adjacent encoded bits*** are mapped onto ***non-adjacent subcarriers*** (48 subcarriers are used for data transmission).
  - ✓ Adjacent bits are mapped alternately onto less and more significant bits of the constellation.
- ***Mapping:***
  - ✓ The mapping process first divides the bit sequence in groups of 1, 2, 4, or 6 bits depending on the modulation scheme (BPSK, QPSK, 16-QAM, or 64-QAM).
  - ✓ These groups are mapped onto the ***appropriate modulation symbol*** according to the constellation diagrams.
  - ✓ The results of this mapping are ***subcarrier modulation symbols***.
- ***OFDM:***
  - ✓ The ***OFDM modulation step*** converts these symbols into a baseband signal, with the help of the inverse FFT.
  - ✓ The symbol interval is 4 µs with ***3.2 µs useful part*** and ***0.8 µs guardtime***.
  - ✓ Pilot sub-carriers (sub-carriers –21, –7, 7, 21) are added.
- ***PHY bursts:***
  - ✓ The last step before radio transmission is the ***creation of PHY bursts*** (PPDUs in ISO/OSI terminology).
  - ✓ Each burst consists of a preamble and a payload.
  - ✓ Five different PHY bursts have been defined: broadcast, downlink, uplink with short preamble, uplink with long preamble, and direct link (optional).
  - ✓ The bursts differ in their preambles.

- ***Radio Transmission:***
  - ✓ The final radio transmission shifts the baseband signal to a carrier frequency depending on the channel number.
  - ✓ All nominal carrier frequencies are spaced 20 MHz apart, resulting in a frequency allocation table for Europe as illustrated in Figure 1.35.

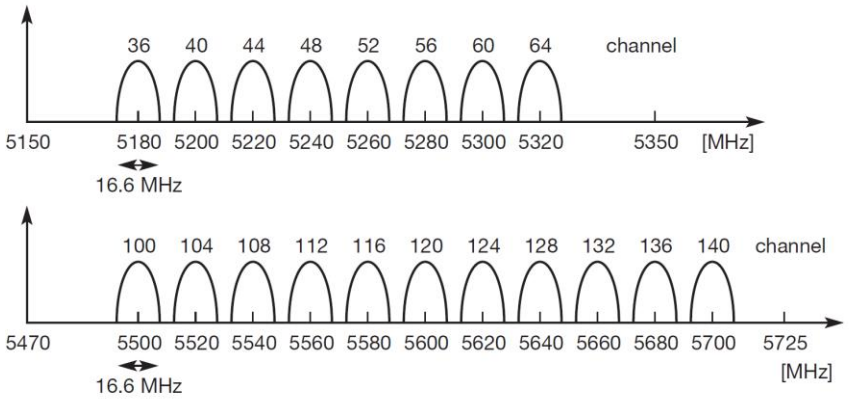


Figure 1.35 Operating channels of HiperLAN2 in Europe

Transmit Power:

- Maximum transmit power is
  - ✓ 200 mW EIRP for the lower frequency band (indoor use), and
  - ✓ 1 W EIRP for the higher frequency band (indoor and outdoor use).
- DFS and TPC are not necessary, if the transmit power stays below 50 mW EIRP.

1.4.4.3 Data link control layer

- The DLC layer is divided into MAC, control and data part (which would fit into the LLC sublayer according to ISO/OSI).
- ETSI (2001b) standardizes the basic data transport functions, i.e., user part with error control and MAC, while ETSI (2002a) defines RLC functionality.

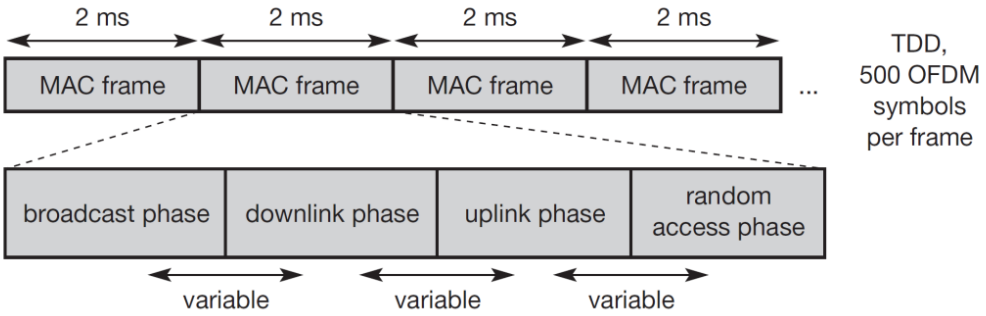


Figure 1.36 Basic structure of HiperLAN2 MAC frames

- The medium access control creates frames of 2 ms duration as shown in Figure 1.36.
- With a constant symbol length of four μs this results in 500 OFDM symbols.

Each MAC frame is further sub-divided into four phases with variable boundaries:

- ***Broadcast phase:***
  - ✓ The AP of a cell broadcasts the content of the current frame and information about the cell (identification, status, resources).
- ***Downlink phase:*** Transmission of user data from an AP to the MTs.
- ***Uplink phase:*** Transmission of user data from MTs to an AP.
- ***Random access phase:*** Capacity requests from already registered MTs and access requests from non-registered MTs (slotted Aloha).

HiperLAN2 defines six different so-called transport channels for data transfer in the above listed phases.

These transport channels describe the basic message format within a MAC frame.

- ***Broadcast channel (BCH):***
  - ✓ This channel conveys basic information for the radio cell to all MTs.
  - ✓ This comprises the identification and current transmission power of the AP.
  - ✓ Moreover,
    - the channel contains pointers to the FCH and RCH.
    - It allows for a flexible structure of the MAC frame.
    - The length is 15 bytes.

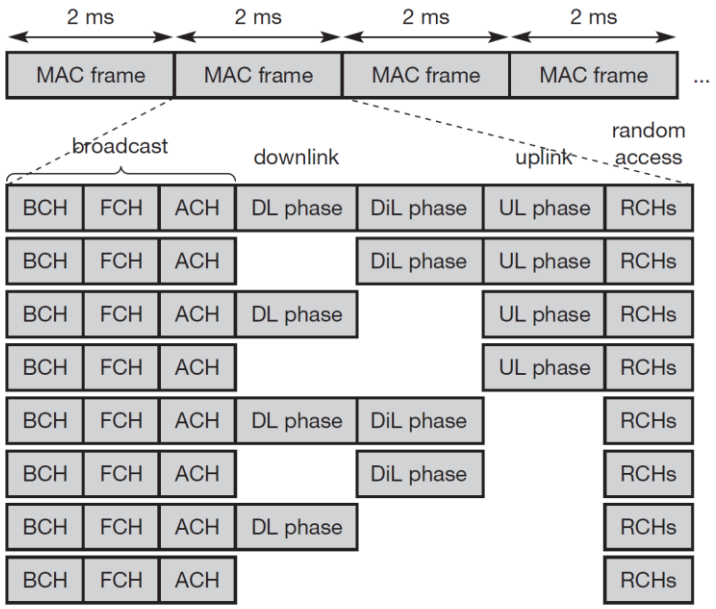


Figure 1.37 Valid configurations of MAC frames

- ***Frame channel (FCH):***
  - ✓ This channel contains a directory of the downlink and uplink phases (LCHs, SCHs, and empty parts).
  - ✓ This also comprises the PHY mode used.
  - ✓ The length is a multiple of 27 bytes.

- ***Access feedback channel (ACH):***
  - ✓ This channel gives feedback to MTs regarding the random access during the RCH of the previous frame.

- ✓ As the access during the RCHs is based on slotted Aloha, collision at the AP may occur.
- ✓ The ACH signals back, which slot was successfully transmitted.
- ✓ The length is 9 bytes.

- ***Long transport channel (LCH):***
  - ✓ This channel transports ***user and control data for downlinks and uplinks***.
  - ✓ The length is 54 bytes.

- ***Short transport channel (SCH):***
  - ✓ This channel transports control data for down links and uplinks.
  - ✓ The length is 9 bytes.
- ***Random channel (RCH):***
  - ✓ This channel is needed to give an MT the opportunity to send information to the AP/CC even without a granted SCH.
  - ✓ Access is via slotted Aloha so, collisions may occur.
  - ✓ Collision resolution is performed with the help of an exponential back-off scheme.
  - ✓ The length is 9 bytes.
  - ✓ A maximum number of 31 RCHs is currently supported.

Data between entities of the DLC layer are transferred over so-called logical channels (just another name for any distinct data path).

The type of a logical channel is defined by the type of information it carries and the interpretation of the values in the corresponding messages.

The following logical channels are defined in HiperLAN2 (logical channels use 4 letter acronyms):

- ***Broadcast control channel (BCCH):***
  - ✓ This channel on the downlink conveys a constant amount of broadcast information about the whole radio cell.
- ***Frame control channel (FCCH):***
  - ✓ The FCCH describes the structure of the remaining parts of the MAC frame.
  - ✓ This comprises resource grants for SCHs and LCHs belonging to certain MTs.
- ***Random access feedback channel (RFCH):***
  - ✓ This channel informs MTs that have used an RCH in the previous frame about the success of their access attempt.
- ***RLC broadcast channel (RBCH):***
  - ✓ This channel transfers information regarding RLC control information, MAC IDs during an association phase, information from the convergence layer.
- ***Dedicated control channel (DCCH):***
  - ✓ This channel carries RLC messages related to a certain MT and is established during the association of an MT.
- ***User broadcast channel (UBCH):***
  - ✓ A UBCH transfers broadcast messages from the convergence layer.
  - ✓ Transmission is performed in the unacknowledged or repetition mode.
- ***User multi-cast channel (UMCH):***
  - ✓ This channel performs unacknowledged transmission of data to a group of MTs.

- ***User data channel (UDCH):***
  - ✓ Point-to-point data between an AP and an MT(CM) or between two MTs (DM) use this channel.
  - ✓ Error protection via an ARQ scheme is possible.
- ***Link control channel (LCCH):***
  - ✓ This bi-directional channel conveys ARQ feedback.
  - ✓ It discards messages between the error control functions of an AP and an MT (CM) or between two MTs (DM).
  - ✓ A LCCH is typically assigned to a UDCH.
- ***Association control channel (ASCH):***
  - ✓ This channel is only used in the uplink and for currently non-associated MTs (related to a certain AP).
  - ✓ This is the case for a new association request (new MT in the network) or a handover request on behalf of the RLC.

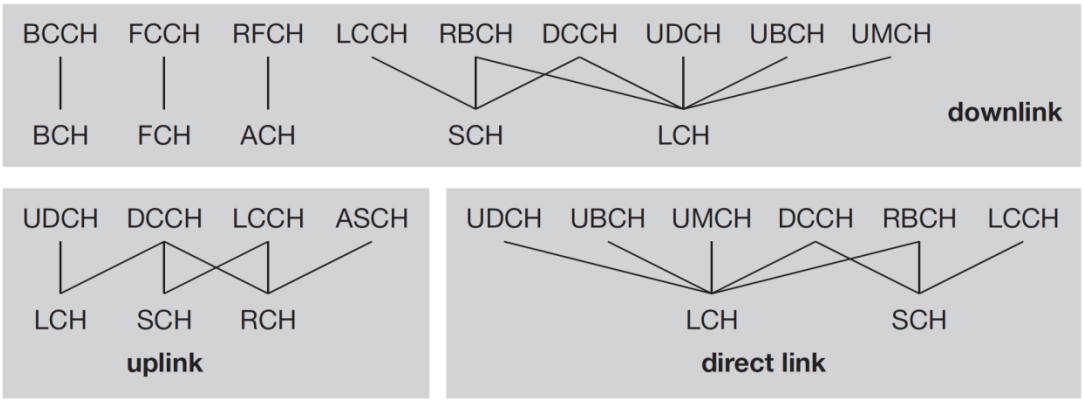


Figure 1.38 Mapping of logical and transport channels.

- ***Figure 1.39*** gives an example for mapping the logical channel UDCH to the transport channel LCH.
- The payload of the LCH is used for a sequence number plus the payload of the UDCH.

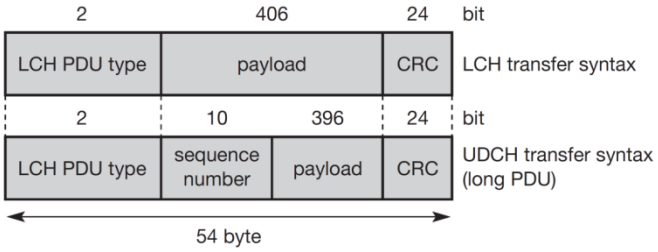


Figure 1.39 HiperLAN2 LCH and UDCH transfer syntax

The radio link control sublayer in connection oriented systems offering QoS like HiperLAN2 is quite complex and comprises many protocols, functions, and messages.

ETSI (2002a) defines three main services for the RLC sublayer:

- ***Association control function (ACF):***
  - ✓ ACF contains all procedures for association, authentication, and encryption.
  - ✓ An MT starts the association process.
  - ✓ The first step is the synchronization with a beacon signal transmitted in each BCCH of a MAC frame.
  - ✓ The network ID may be obtained via the RBCH.
  - ✓ The next step is the MAC ID assignment.
  - ✓ This unique ID is used to address the MT.
  - ✓ From this point on, all RLC control messages are transmitted via a DCCH.
  - ✓ During the following link capability negotiation, lists of supported convergence layers, authentication and encryption procedures are exchanged.
- ***Radio resource control (RRC):***
  - ✓ An important function of the RRC is handover support as already shown in ***Figure 1.31***.
  - ✓ Each associated MT continuously measures the link quality.
  - ✓ To find handover candidates the MT additionally checks other frequencies.
  - ✓ If only one transceiver is available the MT announces to the AP that it is temporarily unavailable (MT absence).
  - ✓ Based on radio quality measurements, an AP can change the carrier frequency dynamically (DFS). The RLC offers procedures to inform all MTs.
  - ✓ To minimize interference with other radio sources operating at the same frequency (HiperLAN2s or other WLANs) transmission power control (TPC) must be applied by the RRC.
- ***DLC user connection control (DCC or DUCC):***
  - ✓ This service is used for setting up, releasing, or modifying unicast connections.
  - ✓ Multi-cast and broadcast connections are implicitly set-up by a group/broadcast join during the association procedure.

1.4.4.4 Convergence layer

- The physical layer and the data link layer are independent of specific core network protocols.
- A special convergence layer (CL) is needed to adapt to the specific features of these network protocols.
- HiperLAN2 supports two different types of CLs: ***Cell-based and Packet-based.***
- ***Cell-based CL:*** The cell-based CL (ETSI, 2000b) expects data packets of fixed size (cells, e.g., ATM cells).
- ***Packet-based CL:***
  - ✓ The packet-based CL (ETSI, 2000d) handles packets that are variable in size (e.g., Ethernet or Firewire frames).

Three examples of convergence layers follow:

- ***Ethernet:***
  - ✓ This sublayer supports the ***transparent transport of Ethernet frames over a HiperLAN2*** wireless network (ETSI, 2001d).
  - ✓ This includes the ***mapping of Ethernet*** multicast and broadcast messages ***onto HiperLAN2*** multicast and broadcast messages.
  - ✓ The standard supports the traffic classes best effort, background, excellent effort, controlled load, video, voice, and network control.

- ***IEEE 1394 (Firewire):***
  - ✓ As a high-speed real-time bus for connecting, e.g., audio and video devices, timing and synchronization is of special importance for IEEE 1394.
  - ✓ ETSI (2001e) supports synchronization of timers via the air and treats isochronous data streams with special regard to jitter.

- ***ATM:***
  - ✓ The cell-based CL is used for this type of network (ETSI, 2000c).
  - ✓ As the payload of an ATM cell is only 48 byte, which fits into the 49.5 byte of a DLC-PDU, segmentation and reassembly is not necessary.
  - ✓ In this case, the sublayer only has to control connection identifiers and MAC IDs.

1.5 Bluetooth

BLUETOOTH

Architecture
Radio Layer
Baseband layer
Link manager Protocol
Security

- In 2001, the first products hit the mass market, and many mobile phones, laptops, PDAs, video cameras etc. are equipped with Bluetooth technology today.
- The Bluetooth development started, a study group within IEEE 802.11 discussed wireless personal area networks (WPAN) under the following five criteria:
  - ✓ ***Market potential:*** How many applications, devices, vendors, customers are available for a certain technology?
  - ✓ ***Compatibility:*** Compatibility with IEEE 802.
  - ✓ ***Distinct identity:*** Originally, the study group did not want to establish a second 802.11 standard. The topics such as, low cost, low power, or small form factor are not addressed in the 802.11 standard.
  - ✓ ***Technical feasibility:*** Prototypes are necessary for further discussion, so the study group would not rely on paper work.
  - ✓ ***Economic feasibility:*** Everything developed within this group should be cheaper than other solutions and allow for high-volume production.

1.5.1 User scenarios

Many different user scenarios can be imagined for wireless piconets or WPANs:

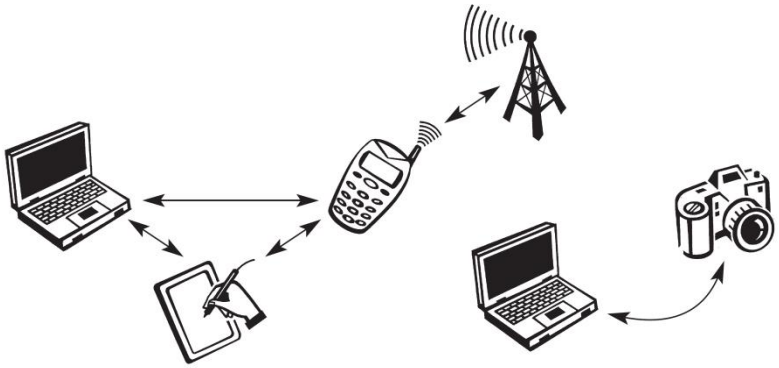


Figure 7.40 Example configurations with a Bluetooth-based piconet

- ***Connection of peripheral devices:***
  - ✓ Most devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers).
- ***Support of ad-hoc networking:***
  - ✓ Wireless networks can support the interaction between devices.
  - ✓ Small devices might not have WLAN adapters (IEEE 802.11 standard), but cheaper Bluetooth chips built in. Example: Students might join a lecture, with the teacher through their PDAs.
- ***Bridging of networks:***
  - ✓ Using wireless piconets, simply a mobile phone can be connected to a PDA or laptop.
  - ✓ Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip.
  - ✓ The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network.

1.5.2 Architecture

7.	**With neat diagrams explain the protocol and architecture of Bluetooth in detail**	**(16m)**	**Jun 2014**
	Draw and explain protocol architecture of Bluetooth	**(16m)**	**Dec 2014**
	With diagram explain the layered architecture of Bluetooth	**(10m)**	**May 2015**
	Explain the architecture and MAC layer details of Bluetooth system.	**(16m)**	**Apr 2014**
	Describe the user scenario architecture and protocol stack of Bluetooth technology.	**(16m)**	**Apr 2017**

- Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band.
- However, MAC, physical layer and the offered services are completely different.

Networking

Quick introduction to its key features is necessary:

- Bluetooth operates on ***79 channels*** in the ***2.4 GHz band*** with ***1 MHz carrier spacing***.
- Each device performs ***frequency hopping with 1,600 hops/s***, in a pseudo random fashion.

- Bluetooth applies FHSS for interference mitigation (and FH-CDMA for separation of networks).

Piconet:

- A very important term in perspective of Bluetooth is a piconet.
- A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence.

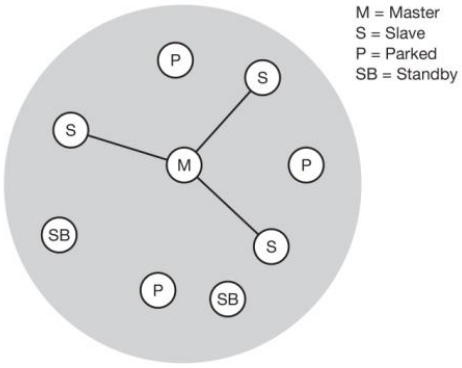


Figure 1.41 Simple Bluetooth piconet

- ***Figure 1.41*** shows, a collection of devices with different roles.
- ***Master:*** One device in the piconet can act as master (M)
- ***Slavs:*** All other devices connected to the master must act as slaves (S).
- ***Function of M and S:***
  - ✓ The master determines the hopping pattern in the piconet.
  - ✓ The slaves have to synchronize to this pattern.
- Each piconet has a unique hopping pattern.
- If a device wants to participate, it has to synchronize to this.
- Two additional types of devices are shown:
  - ✓ ***Parked devices (P):***
    - Parked devices can not actively participate in the piconet (i.e., they do not have a connection)
    - But are ***known and can be reactivated*** within some milliseconds.
  - ✓ ***Stand-by:***
    - Devices in stand-by (SB) do not participate in the piconet.
- ***Number of devices:***
  - ✓ Each piconet has exactly ***one master*** and up to ***seven simultaneous slaves***.
  - ✓ More than 200 devices can be parked.
  - ✓ The upper limit of ***eight active devices***, because the ***3-bit address used*** in Bluetooth.
- ***Parked state to Slave state:***
  - ✓ A parked device wants to communicate and there are already seven active slaves.
  - ✓ Then, one slave has to switch to park mode to allow the parked device to switch to active mode.

Forming a Bluetooth piconet:

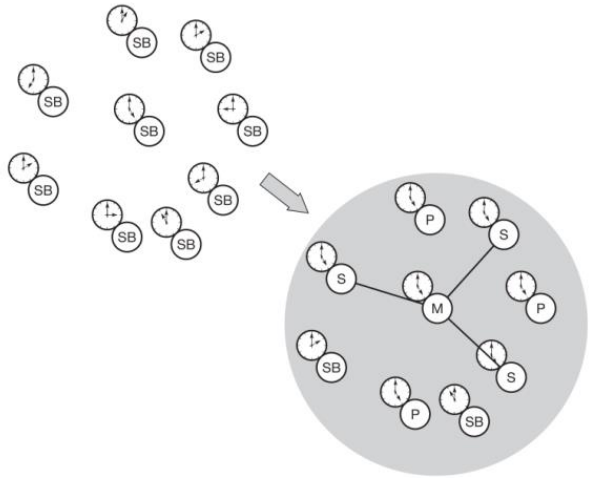


Figure 1.42 Forming a Bluetooth piconet

- ***Figure 1.42*** gives an overview of the formation of a piconet.
- ***Hopping sequence:***
  - ✓ As all active devices have to use the same hopping sequence they must be synchronized.
- ***Formation of network:***
  - ✓ The first step involves, ***a master sending its clock and device ID***.
  - ✓ ***All Bluetooth devices*** have the same networking capabilities, i.e., they ***can be master or slave***.
  - ✓ No distinction between terminals and base stations, so any two or more devices can form a piconet.
- ***Master and Slave:***
  - ✓ The unit establishing the piconet automatically becomes the master.
  - ✓ All other devices will be slaves.
- ***Hopping pattern:***
  - ✓ The hopping pattern is determined by the device ID (*a 48-bit worldwide unique identifier*).
  - ✓ The ***phase*** in the hopping pattern is ***determined by the master's clock***.
  - ✓ After adjusting the internal clock according to the master a device may participate in the piconet.
- ***Address:***
  - ✓ All active devices are assigned a 3-bit Active Member Address (AMA).
  - ✓ All parked devices use an 8-bit Parked Member Address (PMA).
  - ✓ Devices in stand-by do not need an address.

Limitations of piconet:

- All users within one piconet have the same hopping sequence and share the same 1 MHz channel.
- When more users join the piconet, the throughput per user ***drops*** quickly (a single piconet offers less than 1 Mbit/s gross data rate).
- To overcome this disadvantage: Forming groups of piconets called scatternet is performed.

Scatternet:

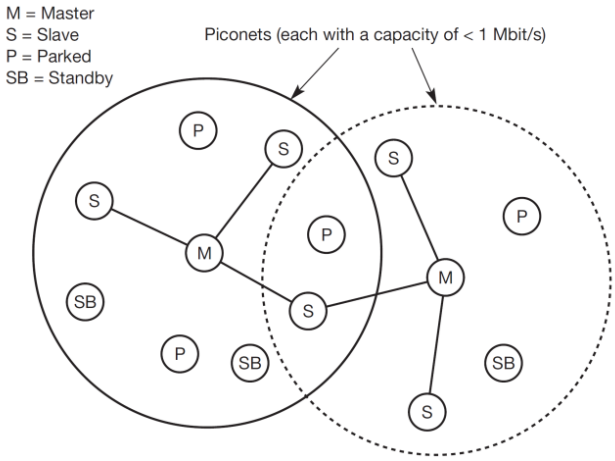


Figure 1.43 Bluetooth scatternet

- ***Figure 1.43*** gives an overview of the formation of a ***Scatternet***.
- Groups of piconets are called scatternet.
- The units which are in need of real data exchange share the same piconet, so that many piconets with overlapping coverage can exist simultaneously.

- In the example, the scatternet consists of two piconets.
- Here, one device participates in two different piconets.
- Both piconets use a different hopping sequence, it was determined by the master of the piconet.
- Bluetooth applies ***FH-CDMA for separation of piconets***.
- In an average sense, ***all piconets can share the total*** of 80 MHz ***bandwidth available***.

- Adding more piconets leads to a ***performance degradation*** of a single piconet, because more and more collisions may occur.
- A collision occurs if two or more piconets use the same carrier frequency at the same time.

- If a device wants to participate in more than one piconet, it must be synchronized to the hopping sequence of the piconet it wants to take part in.
- If a device acts as slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join.
- After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet.

- A master can also leave its piconet and act as a slave in another piconet.
- It is clearly not possible for a master of one piconet to act as the master of another piconet.

8. What are the functions of Bluetooth protocol stack? Explain (May / June 2014)

- As ***Figure 1.44*** shows, the Bluetooth specification already comprises many protocols and components.

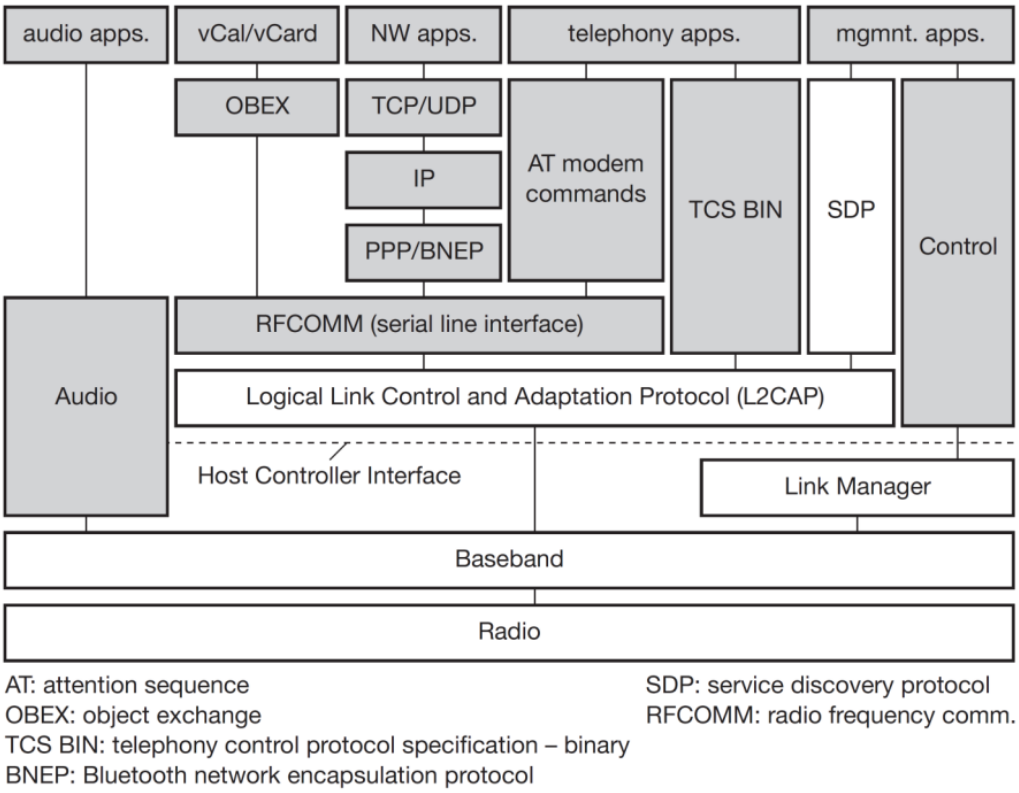


Figure 1.44 Bluetooth protocol stack

- The Bluetooth protocol stack can be divided into
  - ✓ **Core specification (Bluetooth, 2001a):** It describes ***the protocols from physical layer to the data link control*** together with ***management functions***.
  - ✓ **Profile specifications (Bluetooth, 2001b):** It describes many protocols and functions needed to adapt the wireless Bluetooth technology and new applications.

The core protocols of Bluetooth comprise the following elements:

- ***Radio:*** Specification of the air interface, i.e., frequencies, modulation, and transmit power.
- ***Baseband:*** Description of basic connection establishment, packet formats, timing, and basic QoS parameters.
- ***Link manager protocol:*** Link set-up and management between devices including security functions and parameter negotiation.
- ***Logical link control and adaptation protocol (L2CAP):*** Adaptation of higher layers to the baseband (connectionless and connection-oriented services).
- ***Service discovery protocol:*** Device discovery in close proximity plus querying of service characteristics.

Profile Specification Protocols:

(1) On the top of L2CAP is the cable replacement protocol RFCOMM
- ✓ This emulator a serial interface following the E/A-232 which was early called as RS-232.
- ✓ This allows a simple replacement of serial line cables and allows other protocols to run over Bluetooth.
- ✓ RFCOMM supports multiple serial ports.

(2) The telephony control protocol specification-binary (TCS BIN) specifies a bit oriented protocol which defines call control signal and establish voice and data calls between devices.

(3) The host control interface (HC1) between the base band and L2CAR provides the interface to the base band controller and link manager. Access to hardware status and control registers.
- ✓ The real difference between other protocols and that of this that blue tooth supports audio

***

1.5.3 Radio layer

- Radio layer define the carrier frequencies and output power
- Blue tooth devices will be integrated into mobile devices and rely on battery power.
- Hence small, low power chips are needed to build into hand held deices.
- Blue tooth has to support multimedia data.
- Blue tooth uses license free frequency band at 2.4 GHz.
- Hoping rate 1600 hops/sec. Time between two hops is called slot and interval is 625 ms.
- Blue tooth uses 79 hops.
- Transceivers use Gaussian FSK for modulation available in 3 classes :
  - Power Class 1 :
    - Maximum power is 100 MW Minimum power is 1 MW
    - Power control is mandatory
  - Power Class 2 :
    - Maximum power is 2.5 MW Nominal Power is 1 MW Minimum power is 0.25 MW
    - Power control is optional.
  - Power Class 3 : Maximum power is 1 MW

1.5.4 Baseband layer

- The functions of the baseband layer are quite complex.
- It performs frequency hopping for interference mitigation and medium access.
- It also defines physical links and many packet formats.

- ***Figure 1.45*** shows several examples of frequency selection during data transmission.
- ***Remember:*** each device participating in a piconet, hops at the same time to the same carrier frequency (f_i in Figure 1.45).
- If, for example, the master sends data at f_k, then a slave may answer at f_k+1.
- This scenario shows another feature of Bluetooth.
- TDD is used for separation of the transmission directions.

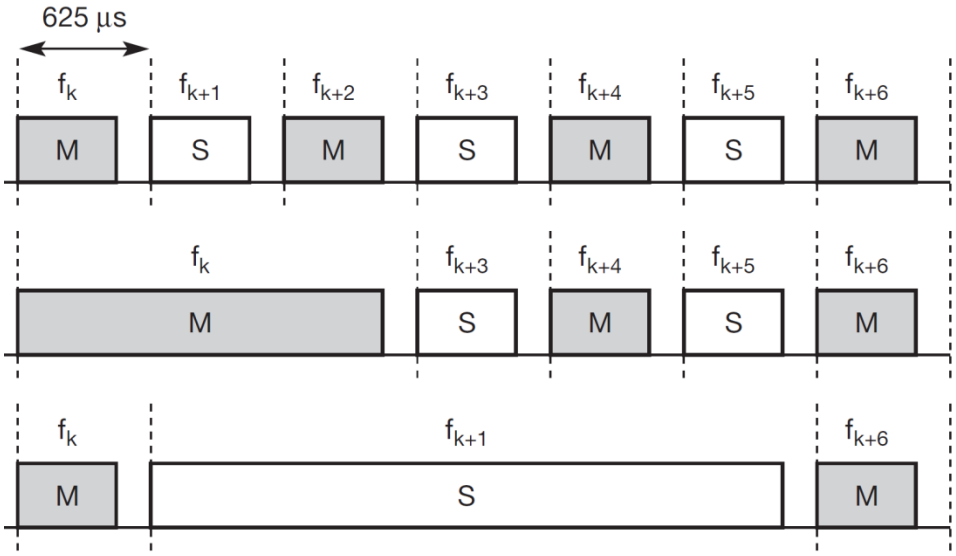


Figure 1.45 Frequency selection during data transmission (1, 3, 5 slot packets)

- The upper part of Figure 1.45 shows so-called 1-slot packets as the data transmission uses one 625µs slot.
- Within each slot the master or one out of seven slaves may transmit data in an alternating fashion.
- Bluetooth also defines 3-slot and 5-slot packets for higher data rates (multi-slot packets).

- *If a master or a slave sends a packet covering three or five slots, the radio transmitter remains on the same frequency.*
- *No frequency hopping is performed within packets.*
- *After transmitting the packet, the radio returns to the frequency required for its hopping sequence.*

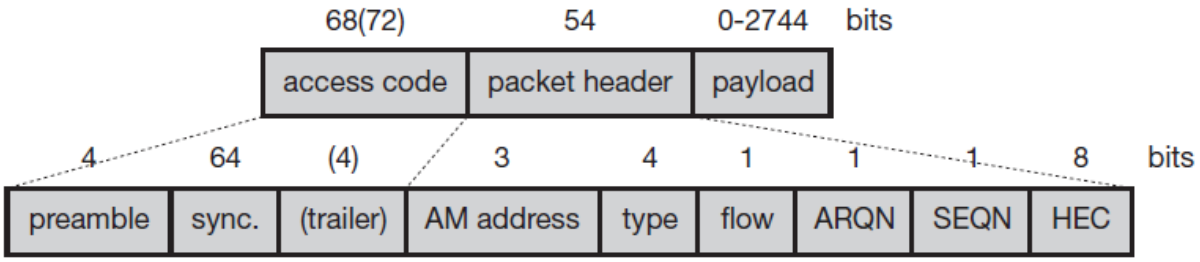


Figure 1.46 Baseband packet format

Figure 1.46 shows the components of a Bluetooth packet at baseband layer.

The packet typically consists of the following three fields:

- **Access code:**
  - ✓ This first field of a packet is needed for timing synchronization and piconet identification (channel access code, CAC).
  - ✓ It represent the special codes during paging (device access code, DAC) and inquiry (inquiry access code, IAC).

- ✓ The access code consists of a 4 bit preamble, a synchronization field, and a trailer (if a packet header follows).
- ✓ The 64-bit synchronization field is derived from the lower 24 bit of an address (lower address part, LAP).

➢ **Packet header:**

- ✓ This field contains typical layer 2 features: address, packet type, flow and error control, and checksum.
- ✓ ***AM address:***
  - The 3-bit active member address represents the active address of a slave.
  - Active addresses are temporarily assigned to a slave in a piconet.
  - If a master sends data to a slave, the address is interpreted as receiver address.
  - If a slave sends data to the master, the address represents the sender address.
  - As only a master may communicate with a slave this scheme works well.
  - Seven addresses may be used this way.
  - The zero value is reserved for a broadcast from the master to all slaves.
- ✓ ***Type** field:*
  - The 4-bit type field, determines the ***type of the packet***.
  - Examples for packet types are given in Table 1.6.
  - Packets may carry control, synchronous, or asynchronous data.
- ✓ ***Flow field:***
  - A simple flow control mechanism for asynchronous traffic.
  - It uses the 1-bit flow field.
  - If a packet is received with flow = 0 asynchronous data, transmission must stop.\
  - If a packet with flow = 1 is received, transmission may resume.
  - If an acknowledgement of packets is required, Bluetooth sends this ***in the slot following the data*** (using its time division duplex scheme).
- ✓ ***ARQN and SEQN:***
  - A simple alternating bit protocol with a single bit ***SEQuence Number*** (SEQN) and ***Acknowledgement Number*** (ARQN) can be used.
- ✓ ***HEC:***
  - It is an 8-bit Header Error Check (HEC).
  - It is used to protect the packet header.
  - The packet header is also protected by a one-third rate forward error correction (FEC) code.
  - Therefore, the 18-bit header requires 54 bits in the packet.

➢ **Payload:**

- ✓ Up to 343 bytes payload can be transferred.
- ✓ The structure of the payload field depends on the type of link.

1.5.4.1 Physical links

- ➢ Bluetooth offers two different types of links:
  - ✓ Synchronous connection-oriented link and
  - ✓ Asynchronous connectionless link

Synchronous connection-oriented link (SCO):

- ✓ Classical telephone (voice) connections require symmetrical, circuit-switched, point-to-point connections.
- ✓ For this type of link, the master reserves two consecutive slots (forward and return slots) at fixed intervals.

- ✓ A master can support up to three simultaneous SCO links to the same slave or to different slaves.
- ✓ A slave supports upto two links from different masters or up to three links from the same master.

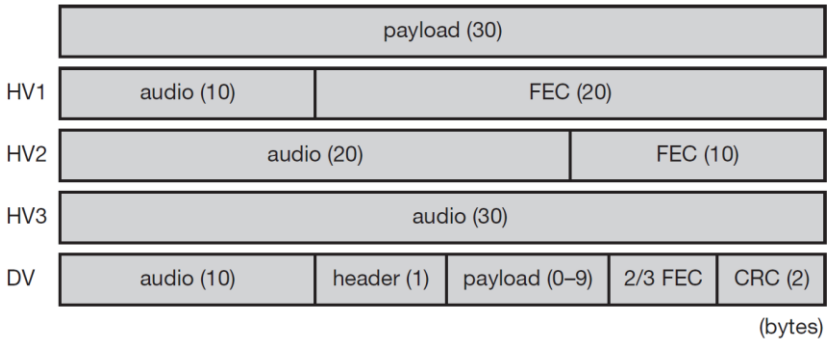


Figure 1.47 SCO payload types

- ✓ Using an SCO link, three different types of single-slot packets can be used (Figure 1.47).
- ✓ Each SCO link carries voice at 64 kbit/s, and no forward error correction (FEC), 2/3 FEC, or 1/3 FEC can be selected.
- ✓ Depending on the error rate of the channel, different FEC schemes can be applied.
- ✓ FEC always causes an overhead, but avoids retransmission of data with a higher probability.

- ✓ However, voice data over an SCO is never retransmitted.
- ✓ Instead, a very robust voice-encoding scheme, continuous variable slope delta (CVSD), is applied.

Asynchronous connectionless link (ACL):

- ✓ Some data applications require symmetrical or asymmetrical (e.g., web traffic), packet-switched, point-to-multipoint transfer scenarios (including broadcast).
- ✓ Here the master uses a polling scheme.

- ✓ A slave may only answer if it has been addressed in the preceding slot.
- ✓ Only one ACL link can exist between a master and a slave.
- ✓ For ACLs carrying data, 1-slot, 3-slot or 5-slot packets can be used (***Figure 1.48***).
- ✓ Additionally, data can be protected using a 2/3 FEC scheme.
- ✓ This FEC protection helps in noisy environments with a highlink error rate.

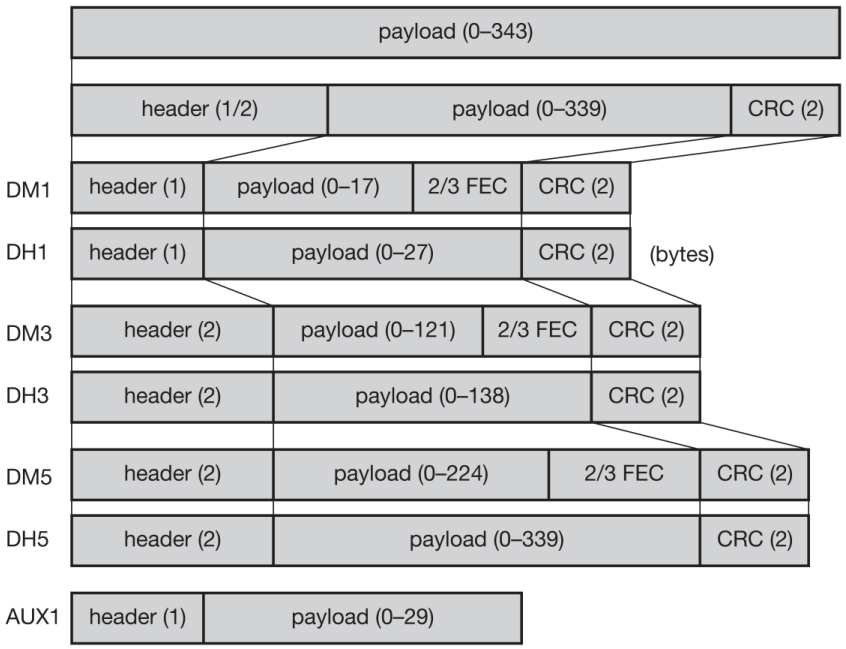


Figure 1.48 ACL payload types

- ✓ However, the overhead introduced by FEC might be too high.
- ✓ Bluetooth therefore offers a fast automatic repeat request (ARQ) scheme for reliable transmission.

9. Explain in detail about Link manager protocol in Bluetooth. (or) Give the strategy of logical link control and adaptation protocol (L2CAP). (Apr / May 2019)
Describe the need for Link Manager Protocol and illustrate with architecture. [Nov 2019]

1.5.5 Link manager protocol

- ➢ The link manager protocol (LMP) manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices.
- ➢ LMP enhances baseband functionality, but higher layers can still directly access the baseband.

The following groups of functions are covered by the LMP:

1. Authentication, pairing, and encryption:

- ✓ The basic authentication is handled in the baseband.
- ✓ Also, LMP has to ***control the exchange of random numbers and signed responses***.
- ✓ The pairing service is needed to establish an ***initial trust relationship between two devices*** that have ***never communicated before***. The result of pairing is a ***link key***.
- ✓ This may be changed, accepted or rejected.
- ✓ LMP sets the encryption mode (no encryption, point-to-point, or broadcast), key size, and random speed.

Synchronization

- ✓ The clock offset is updated each time a packet is received from the master.
- ✓ Additionally, special synchronization packets can be received.
- ✓ Devices can also exchange timing information related to the time differences (slot boundaries) between two adjacent piconets.

2. **Capability negotiation:**
   - ✓ The version of the LMP can be exchanged
   - ✓ The information about the supported features also changed.
3. **Quality of service negotiation:**
   - ✓ Different parameters control the QoS of a Bluetooth device at these lower layers.
   - ✓ The poll interval, *i.e., the maximum time between transmissions from a master to a particular slave*, controls the latency and transfer capacity.
   - ✓ The number of repetitions for broadcast packets can be controlled.
   - ✓ A master can limit the number of slots available for slaves'.
4. **Power control:**
   - ✓ A Bluetooth device can measure the received signal strength.
   - ✓ Depending on this signal level, ***the device can direct the sender*** of the measured signal ***to increase or decrease its transmit power***.
5. ***Link supervision:***
   - ✓ LMP has to control the activity of a link, it may set up new SCO links, or it may declare the failure of a link.
6. ***State and transmission mode change:***
   - ✓ Devices might switch the master/slave role, detach themselves from a connection, or change the operating mode.
   - ✓ The available modes will be explained together with ***Figure 1.51***.

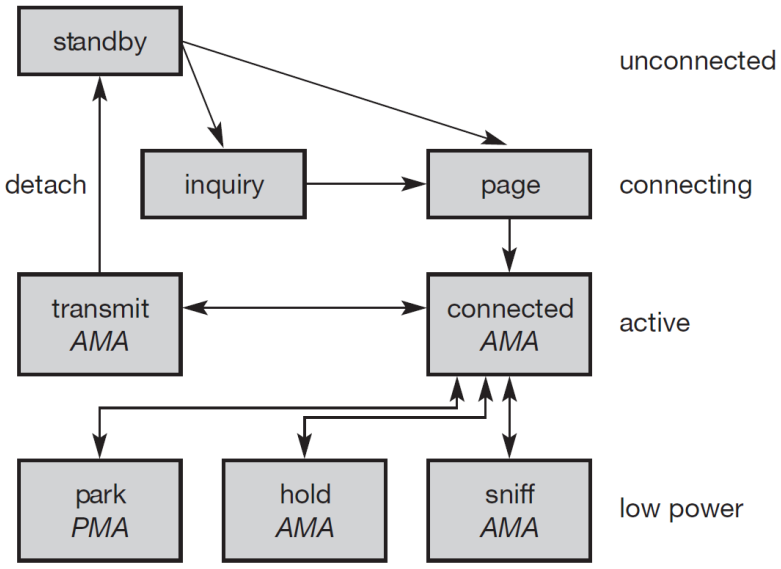


Figure 1.51 Major baseband states of a Bluetooth device

Either a device wants to establish a piconet or a device just wants to listen to see if something is going on.

- **A device wants to establish a piconet**:
  - ✓ A user of the device ***wants to scan for other devices*** in the radio range.
  - ✓ The device starts the inquiry procedure by sending an ***Inquiry Access Code*** (IAC).
  - ✓ This is common to all Bluetooth devices.
  - ✓ The IAC is ***broadcast over 32 so-called wake-up carriers*** in turn.

- **Devices in standby that listen periodically:**
  - ✓ Devices in standby may ***enter the inquiry mode periodically*** to search for IAC messages on the wake-up carriers.
  - ✓ When ***a device detects an inquiry***, it ***returns a packet containing its device address and timing information*** required ***by the master to initiate a connection***.
  - ✓ From that moment on, the device acts as slave.

To save battery power, a Bluetooth device can go into one of three low power states:

- ***Sniff state:***
  - ✓ The sniff state has the ***highest power consumption*** of the low power states.
  - ✓ Here, the device listens to the piconet at a reduced rate (not on every other slot as is the case in the active state).
  - ✓ The interval for listening into the medium can be programmed and is application dependent.
  - ✓ The master designates a reduced number of slots for transmission to slaves in sniff state.
  - ✓ However, the device keeps its AMA.
- ***Hold state:***
  - ✓ The device does not release its AMA but stops ACL transmission.
  - ✓ A slave may still exchange SCO packets.
  - ✓ If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.
- ***Park state:***
  - ✓ In this state the device has the lowest duty cycle and the lowest power consumption.
  - ✓ The device releases its AMA and receives a parked member address (PMA).
  - ✓ The device is still a member of the piconet, but gives room for another device to become active (AMA is only 3 bit, PMA 8 bit).
  - ✓ Parked devices are still FH synchronized and wake up at certain beacon intervals
  - ✓ for re-synchronization.
  - ✓ All PDUs sent to parked slaves are broadcast.

Table 1.7 Example power consumption(CSR, 2002)

Operating mode	Average current [mA]
SCO, HV1	53
SCO, HV3, 1 s interval sniff mode	26
ACL, 723.2 kbit/s	53
ACL, 115.2 kbit/s	15.5
ACL, 38.4 kbit/s, 40 ms interval sniff mode	4
ACL, 38.4 kbit/s, 1.28 s interval sniff mode	0.5
Park mode, 1.28 s beacon interval	0.6
Standby (no RF activity)	0.047

- The effect of the low power states is shown in Table 1.7.
- This table shows the typical average power consumption of a Bluetooth device (BlueCore2, CSR, 2002).
- It is obvious that higher data rates also require more transmission power.
- The intervals in sniff mode also influence power consumption.
- Typical IEEE802.11b products have an average current in the order of 200 mA while receiving, 300 mA while sending, and 20 mA in standby.

Logical link control and adaptation protocol (L2CAP)

L2CAP is used within the Bluetooth protocol stack. It passes packets to either the Host Controller Interface (HCI) or, on a hostless system, directly to the Link Manager/ACL link.

L2CAP's functions include:

- Multiplexing data between different higher layer protocols.
- Segmentation and reassembly of packets.
- Providing one-way transmission management of multicast data to a group of other Bluetooth devices.
- Quality of service (QoS) management for higher layer protocols.

- L2CAP is used to communicate over the host ACL link.
- Its connection is established after the ACL link has been set up.
- In basic mode, L2CAP provides packets with a payload configurable up to 64 kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU.
- In retransmission and flow control modes, L2CAP can be configured for reliable or asynchronous data per channel by performing retransmissions and CRC checks.
- Reliability in either of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets).
- In-order sequencing is guaranteed by the lower layer.

10. Explain in detail about Security in Bluetooth.

1.5.7 Security

- A radio interface is by nature easy to access.
- Bluetooth devices can transmit private data, e.g., schedules between a PDA and a mobile phone.
- A user clearly does not want another person to ***eavesdrop*** (***spy***) the data transfer.
- The security algorithms use the public identity of a device, a secret private user key, and an internally generated random key as input parameters.
- For each transaction, a new random number is generated on the Bluetooth chip. Key management is left to higher layer software.

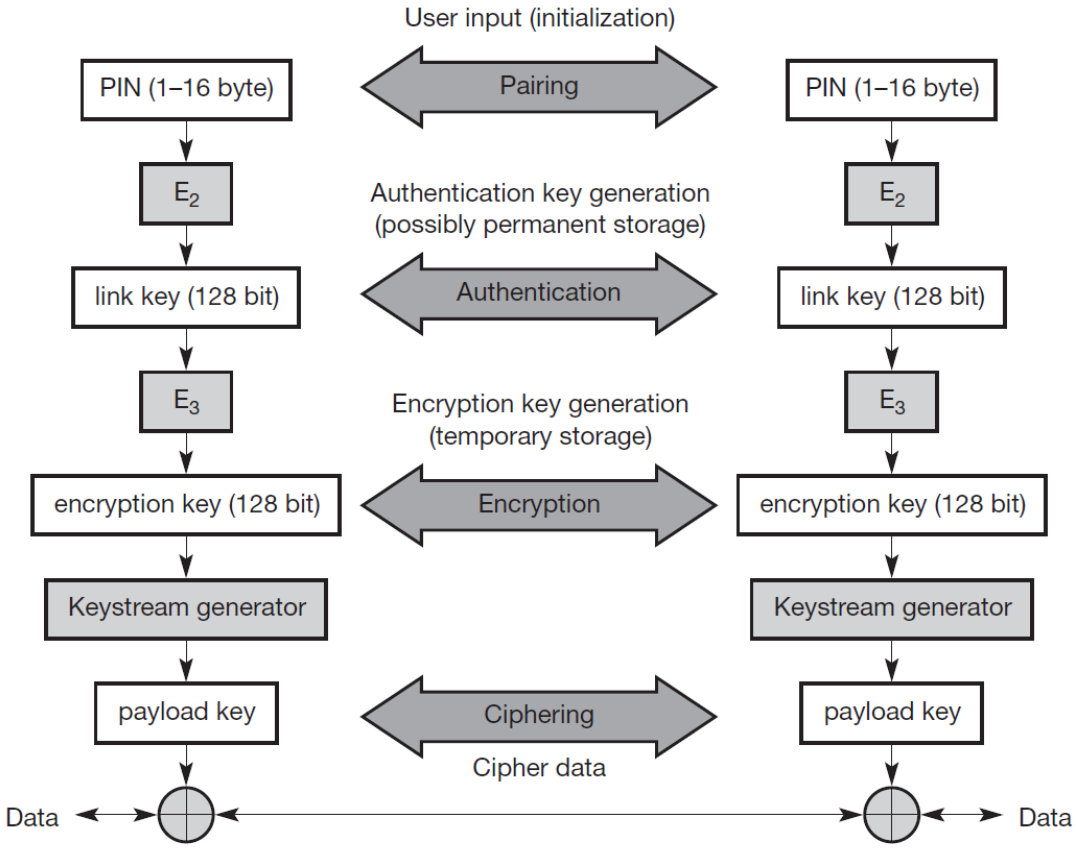


Figure 1.54 Bluetooth security components and protocols

- Figure 1.54 shows several steps in the security architecture of Bluetooth.

- Pairing:
  - The first step, called pairing, is necessary if two Bluetooth devices have never met before.
  - To set up trust between the two devices a user can enter a secret PIN into both devices.
  - This PIN have a length of up to 16 byte. Most devices limit the length to four digits.
  - Based on the PIN, the device address, and random numbers, several keys can be computed which can be used as link key for authentication.
  - ***Link keys*** are typically stored in a persistent storage.
- Authentication:
  - The authentication is a challenge-response process based on the link key.
  - ***Link key***: a random number generated by a verifier (the device that requests authentication), and the device address of the claimant (the device that is authenticated).
- Ciphering:
  - Based on the link key, again an encryption (a random number) key is generated during the encryption stage of the security architecture.
  - Based on the ***encryption key*** (maximum size of 128 bits), the device address and the current clock a ***payload key*** is generated for ciphering user data.
  - The payload key is a stream of pseudo-random bits. The ciphering process is a simple XOR of the user data and the payload key.

- Compared to WEP in 802.11, Bluetooth offers a lot more security.
- However, Bluetooth, too, has some weaknesses when it comes to real implementations.
- The PINs are quite often fixed. Some of the keys are permanently stored on the devices and the quality of the random number generators has not been specified.

- If Bluetooth devices are switched on they can be detected unless they operate in the non-discoverable mode.

- Either a user can use all services as intended by the Bluetooth system, or the devices are hidden to protect privacy.
- Either roaming profiles can be established, or devices are hidden and, thus many services will not work.

IEEE 802.16

- The IEEE 802.16 standard delivers performance comparable to traditional cable, DSL, or T1 offerings.
- The principal advantages of systems based on 802.16 are multifold:
  - faster provisioning of service, even in areas that are hard for wired infrastructure to reach;
  - lower installation cost; and
  - ability to overcome the physical limitations of the traditional wired infrastructure.
  - 802.16 technology provides a flexible, cost-effective, standard-based means of filling gaps in broadband services not envisioned in a wired world.

- The 802.16a is an extension of the 802.16 originally designed for 10–66 GHz.
- It covers frequency bands between 2 and 11 GHz and enables non line-of-sight (NLOS) operation.

- The 802.16a has a range of up to 30 miles with a typical cell radius of 4 to 6 miles.

- Within the typical cell radius NLOS performance and throughputs are optimal.
- In addition, the 802.16a provides an ideal wireless backhaul technology to connect 802.11 WLAN and commercial 802.11 hotspots with the Internet.

- Applications of the 802.16 are cellular backhaul, broadband on-demand, residential broadband, and best-connected wireless service (see Figure 21.22).

- The 802.16 delivers high throughput at long ranges with a high spectral efficiency.
- Dynamic adaptive modulation allows base stations to trade off throughput for range.
- The 802.16
  - Supports flexible channel bandwidths to accommodate easy cell planning in both licensed and unlicensed spectra.
  - Includes robust security features, and

- QoS needed to support services that require low latency, such as voice and video.

- The 802.16 voice service can either be TDM voice or voice over IP (VoIP).
- Privacy and encryption features are also included to support secure transmission and data encryption.
- The worldwide interoperability for microaccess inc. (WiMAX) forum, an industry group, focused on creating system profiles and conformance programs

Table Road-map of IEEE 802.16 standard.

Standard	Features
802.16 (2001)	Air interface for fixed broadband wireless access system, MAC and PHY specification for 10–66 GHz (LOS)
802.16a (January 2003)	Amendment to 802.16; MAC modifications and additional PHY specifications for 2–11 GHz (NLOS); three physical layers—OFDM, OFDMA, single carrier; additional MAC functions; mesh topology support; ARQ
802.16d (July 2004)	Combine 802.16 and 802.16a, some modification to MAC and PHY
802.16e (December 2005)	Amendment to 802.16d, MAC modifications for limited mobility

WIMAX: Physical layer, MAC, Spectrum allocation for WIMAX

11. Write short notes on WiMAX Standard	**(8m)**	**Dec 2014**
What is the need of Wireless MAN? With schematic explain MAC layer details of WiMax	**(10m)**	**May 2014**
In detail, explain the physical and MAC layer details of WiMax network.	**(16m)**	**Apr 2014**
Depict a treatise on spectrum allocation of WiMax in detail	**(15m)**	**Nov 2019**

World Interoperability for MicroAccess, Inc. (WiMAX)

- WiMAX is an advanced technology solution based on an open standard.
- Designed to meet the need for very high speed wide area Internet access, and to do so in a low-cost, flexible way.
- It aims to provide business and consumer broadband service on the scale of the metropolitan area network (MAN).

- WiMAX networks are designed for high-speed data and will spur innovation in services, content, and new mobile devices.

- WiMAX is optimized for IP-based high-speed wireless broadband which will provide for a better mobile wireless broadband Internet experience.

- With its large range and high transmission rate, WiMAX can serve as a backbone for 802.11 hotspots for connecting to the Internet.
- Alternatively, users can connect mobile devices such as laptops and handsets directly to WiMAX base stations without using 802.11.
- Mobile devices connected directly can achieve a range of 4 to 6 miles, because mobility makes links vulnerable.

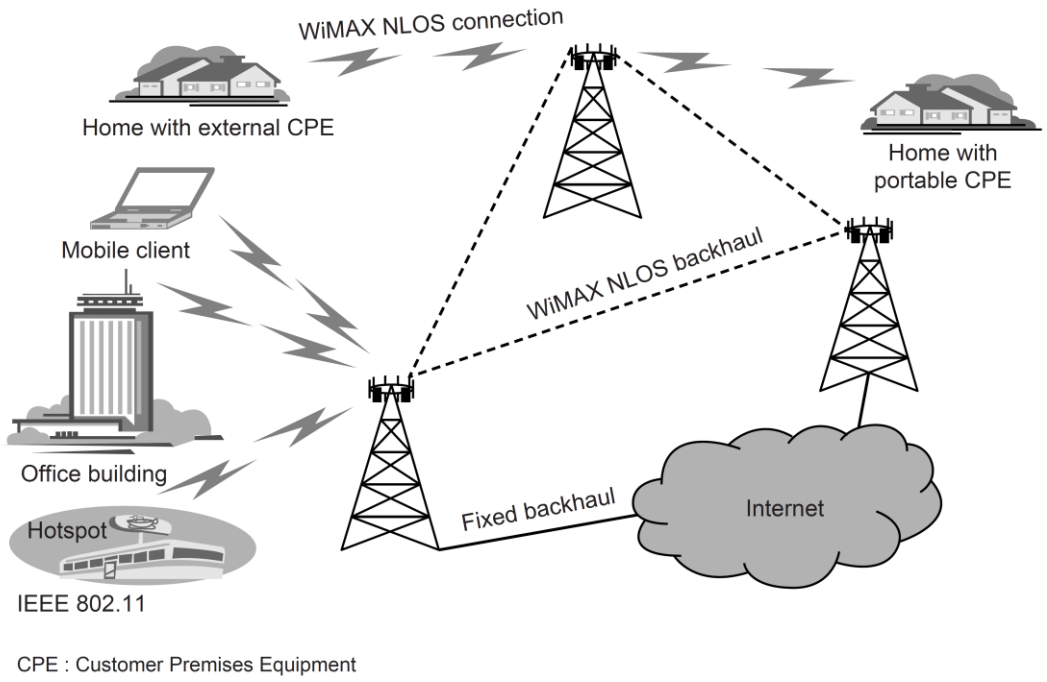


Figure 21.22 Applications of IEEE 802.16 (WiMax).

- WiMAX can be used in disaster recovery scenes where the wired networks have broken down. It can be used as backup links for broken wired links.
- WiMAX can typically support data rates from 500 kbps to 2 Mbps.
- A cellular architecture similar to that of mobile phone systems can be used with a central base station controlling downlink/uplink traffic (see ***Figure 21.22***).

- WiMAX is a family of technologies based on IEEE 802.16 standards.
- There are two main types of WiMAX today,
  - fixed WiMAX (IEEE 802.16d — 2004), and
  - mobile WiMAX (IEEE 802.16e — 2005).
- Fixed WiMAX: It is a point-to- multipoint technology, whereas
- Mobile WiMAX: It is a multipoint-to-multipoint technology, similar to a cellular infrastructure.

- Scalable OFDMA (SOFDMA) has been introduced in IEEE 802.16e to support scalable channel bandwidths from 1.25 to 20 MHz.

- Release 1 of mobile WiMAX will cover 5, 7, 8.75, and 10 MHz channel bandwidths for licensed worldwide spectrum allocations in 2.3 GHz, 2.5 GHz, 3.3 GHz, and 3.5 GHz frequency bands.

Table 21.19 provides comparisons of Wi-Fi and WiMAX.

Wi-Fi	WiMAX
802.11a—OFDM, maximum rate = 54 Mbps 802.11b—DSSS, maximum rate = 11 Mbps 802.11g—OFDM, maximum rate = 54 Mbps	802.16—OFDM, maximum rate = 50 Mbps 802.16e—OFDM, maximum rate ~ 30 Mbps
Range <100 m	A few km's non-line-of-sight, more with line of sight
Indoor environment	Outdoor environment
No admission control, no load balancing	Admission control and load balancing
No quality of service (QoS)	Five QoS classes enforced by base station

- WiMAX does not require stations to listen to one another because they encompass a larger area.

- The mesh mode can help relax the line-of-sight requirement and ease the deployment costs for high frequency bands by allowing subscriber stations to relay traffic to one another.
- In this case, a station that does not have line-of-sight with the base station can get its traffic from another station (see ***Figure 21.23***).

- ***Quality of service (QoS).***
  - The fundamental premise of the IEEE 802.16 MAC architecture is QoS.
  - It defines service flows which can map to DiffServ code points or MPLS flow labels that enable end-to-end IP based QoS.
- ***Scalability.***
  - Mobile WiMAX is designed to be able to scale to work in different channelization from 1.25 to 20 MHz to achieve spectrum harmonization in the longer term.
- ***Security.***
  - Support for a diverse set of user credentials exists including SIM/USIM cards, smart cards, digital certificates, and user name/password schemes.
- ***Mobility.***
  - Mobile WiMAX supports optimized handoff schemes with latencies less than 50 ms.
  - This ensures that real-time applications such as VoIP can be performed without service degradation.
  - Flexible key management schemes assure that security is maintained during handoff.

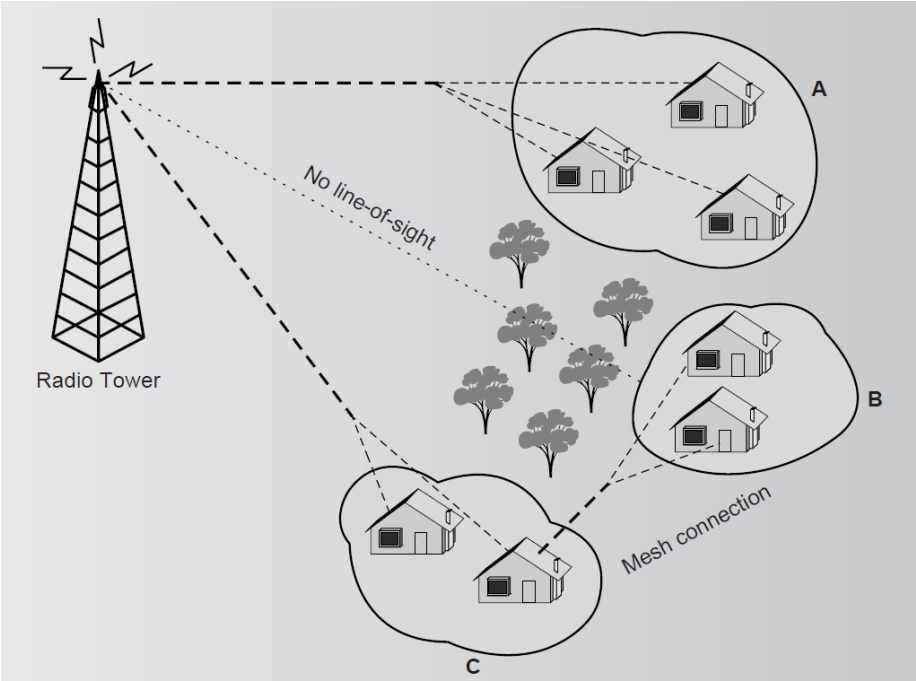


Figure 21.23 Mesh mode in IEEE 802.16 (WiMAX).

WiMAX Physical Layer (PHY)

- The 802.16 PHY supports TDD and full and half duplex FDD operations.
- Other advanced PHY features include
  - adaptive modulation and coding (AMC),
  - hybrid automatic repeat request (HARQ), and
  - fast channel feedback (CQICH)

  to enhance coverage and capacity of WiMAX in mobile applications.

- For the bands in the 10–66 GHz range, 802.16 defines one air interface called Wireless MAN — SC.

- The PHY design for the 2–11 GHz range (both licensed and unlicensed bands) is more complex because of interference.
- Hence, the standard supports burst-by-burst adaptability for modulation and coding schemes and specifies three interfaces.
- The adaptive features at the PHY allow trade-off between robustness and capacity.
- The three air interfaces for the 2–11 GHz range are:
  - Wireless MAN — SC uses single carrier modulation.
  - Wireless MAN — OFDM uses a 256-carrier OFDM. This air interface provides multiple access to different stations through time-division-multiple access.
  - Wireless MAN — OFDM uses a 2048-carrier OFDM scheme. The interface provides multiple access by assigning a subset of the carriers to an individual receiver.

- Support for QPSK, 16-QAM, and 64-QAM are mandatory in the downlink with mobile WiMAX. In the uplink 64-QAM is optional. Both convolutional code and turbo code with variable code rate and repetition coding are supported.

- The combinations of various modulation and code rates provide a fi ne resolution of data rates.
- The frame duration is 5 ms.
- Each frame has 48 OFDM symbols with 44 OFDM symbols available for data transmission.

- The base station (BS) scheduler determines the appropriate data rate for each burst allocation based on the buffer size, channel propagation conditions at the receiver, etc.
- A channel quality indicator (CQI) channel is used to provide channel state information from the user terminals to the BS scheduler.

- WiMAX provides signaling to allow fully asynchronous operation.
- The asynchronous operation allows variable delay between retransmissions which gives more flexibility to the scheduler at the cost of additional overhead for each retransmission.

WiMAX Media Access Control (MAC)

- The IEEE 802.16 MAC is significantly different from that of IEEE 802.11b Wi-Fi MAC.
- In Wi-Fi, the MAC uses ***contention access*** — all subscribers wishing to pass data through an access point compete for the access point's (AP's) attention on a random basis.
- This can cause distant nodes from the AP to be repeatedly interrupted by less sensitive, closer nodes, greatly reducing their throughput.
- The MAC layer of 802.16 is designed to serve sparsely distributed stations with high data rates.

- The 802.16 MAC is a scheduling MAC where the subscriber only has to compete once (for initial entry into the network).
- After that it is allocated a time slot by the base station.

- This scheduling algorithm is stable under overload and oversubscription.
- It is also more bandwidth efficient.

- Duplexing, a station's concurrent transmission and reception, is possible through time division duplex (TDD) and frequency division duplex (FDD).
- In TDD, a station transmits then receives (or vice versa) but not at the same time.
- This option helps reduce subscriber station costs, because the radio is less complex.
- In FDD, a station transmits and receives simultaneously on different channels.

- The 802.16 MAC protocol is connection-oriented and performs link adaptation and ARQ functions to maintain target bit error rate while maximizing the data throughput.
- It supports different transport technologies such as IPv4, IPv6, Ethernet, and ATM.

Spectrum Allocation for WiMAX

- The IEEE 802.16 specification applies across a wide swath of RF spectrum.
- There is no uniform global licensed spectrum for WiMAX in the United States.

- The biggest segment available is around 2.5 GHz.

- Elsewhere in the world, the most likely bands used will be around 3.5 GHz, 2.3/2.5 GHz, or 5 GHz, with 2.3/2.5 GHz probably being most important in Asia.

- There are several variants of 802.16, depending on local regulatory conditions.
- Mobile WiMAX based on the 802.16e standard will most likely be in 2.3 GHz and 2.5 GHz frequencies — low enough to accommodate the NLOS conditions between the base station and mobile devices.

- The key technologies in 802.16e on PHY level are OFDMA and SOFDMA. OFDMA uses a multicarrier modulation in which the carriers are divided among users to form subchannels (see ***Figure 21.24***).

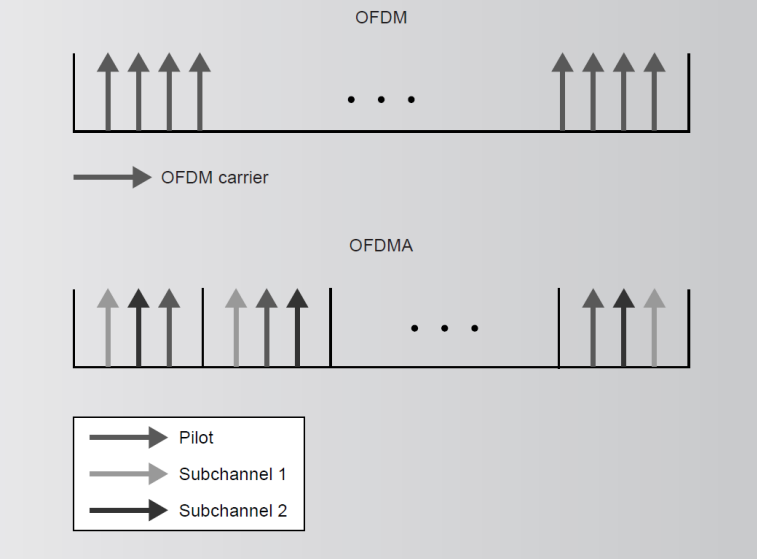


Figure 21.24 OFDM and OFDMA in 802.16e.

- For each subchannel, the coding and modulation are adapted separately, allowing channel optimization on a smaller scale (rather than using the same parameters for the whole channel).
- This technique optimizes the use of spectrum resources and enhances indoor coverage by assigning a robust scheme to vulnerable links.
- 802.16e includes power-saving and sleep modes to extend the battery life of mobile devices.
- 802.16e also supports hard and soft handoff to provide users with seamless connections as they move across coverage areas of adjacent cells.

*****

TWO MARKS
UNIT I
WIRELESS LAN

1. What are the two types of transmission technologies used to set up WLANs?

- Two different basic transmission technologies can be used to set up WLANs.
  - Based on the transmission of infra red light (e.g., at 900 nm wavelength),
  - Uses radio transmission in the GHz range (e.g., 2.4 GHz in the license-free ISM band).

2. What is the principle behind infrared technoogy? What are the advantages and disadvantages of infrared technology? [Nov 2018] *(combine the answers of Q. No. 3 & 4)*

- Infrared is an invisible band of radiation.
- It exists at the lower end of the visible electromagnetic spectrum.
- This type of transmission is most effective when a clear line-of-sight exists between the transmitter and the receiver.
- Two types of infrared WLAN solutions are available:
  - Diffused-beam, and
  - Direct-beam (or line-of-sight).

3. What are the advantages of InfraRed Technology? [Apr/May 2017] [Nov 2018]

The main advantages of infra red technology are

- Version 1.0 of this industry standard implements data rates of up to 115 kbit/s, while IrDA 1.1 defines higher data rates of 1.152 and 4 Mbit/s.
- No licenses are needed for infra red technology and shielding is very simple.
- Electrical devices do not interfere with infra red transmission.

4. What are the disadvantages of IR Technology? [Nov 2018]

The disadvantages of infra red transmission are

- Low bandwidth compared to other LAN technologies.
- Infra red is quite easily shielded.
- Infra red transmission cannot penetrate walls or other obstacles.
- For good transmission quality and high data rates a Line of sight i.e., direct connection, is needed.

5. State the significance of radio transmission over infrared. [Apr/May 2017]

The advantages of radio transmission include

- The long-term experiences made with radio transmission for wide area networks.
- Radio transmission can cover larger areas and can penetrate (thinner) walls, furniture, plants etc. Additional coverage is gained by reflection
- Radio typically does not need a LOS if the frequencies are not too high.

6. What are the disadvantages of Radio waves?

The disadvantages of radio transmission are

- Shielding is not so simple.
- Radio transmission can interfere with other senders, or electrical devices can destroy data transmitted via radio.

7. What is meant by Infrastructure networks? (May/June 2013)

Infrastructure networks

- Infrastructure networks provide access to other networks.
- Also include forwarding functions, medium access control etc.
- Communication typically takes place only between the wireless nodes and the access point.

8. Write about the infrastructure-based networks with diagram.

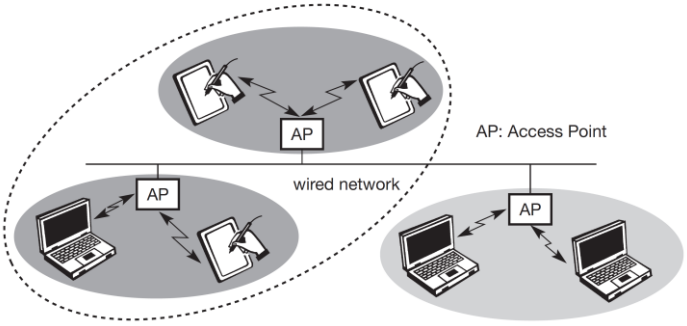


Figure: Example of three infrastructure-based wireless networks

- Figure shows three access points 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.

9. What is meant by Ad-hoc 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.
- Figure shows two ad-hoc networks with three nodes each.

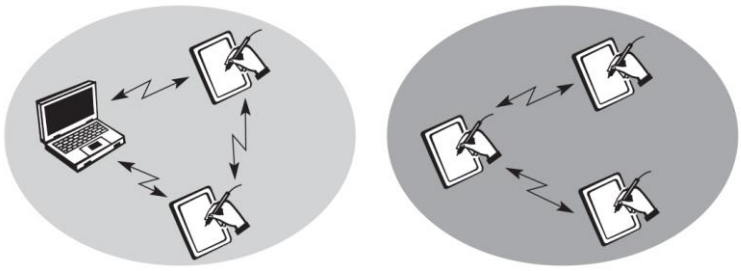


Figure: Example of two ad-hoc wireless networks

IEEE 802.11 STANDARD-ARCHITECTURE
System architecture

10. What are the components of infrastructure network?

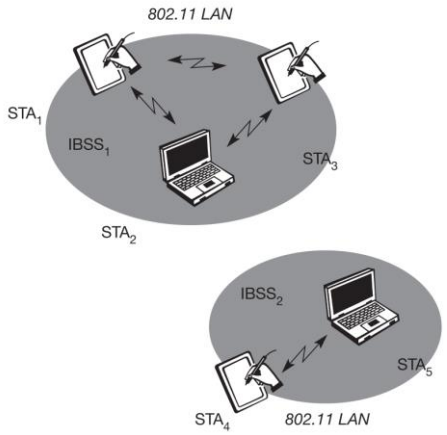
The components of infrastructure network are

- Stations (STAi)
- Access points (AP)
- Basic service Set (BSSi).
- Extended Service Set (ESS)

11. Draw the architecture of IEEE 802.11 ad-hoc wireless LANs.

Architecture of IEEE 802.11 ad-hoc wireless LANs

- Direct communication within a limited range



Station (STAi): terminal with access mechanisms to the wireless medium,
Independent Basic Service Set (IBSS): group of stations using the same radio frequency

Protocol architecture

12. **Draw how could we connect an IEEE 802.11 wireless LAN to a switched IEEE 802.3 Ethernet. (Or) Draw the architecture of IEEE 802.11. [*June 2012*]**

Architecture of IEEE 802.11

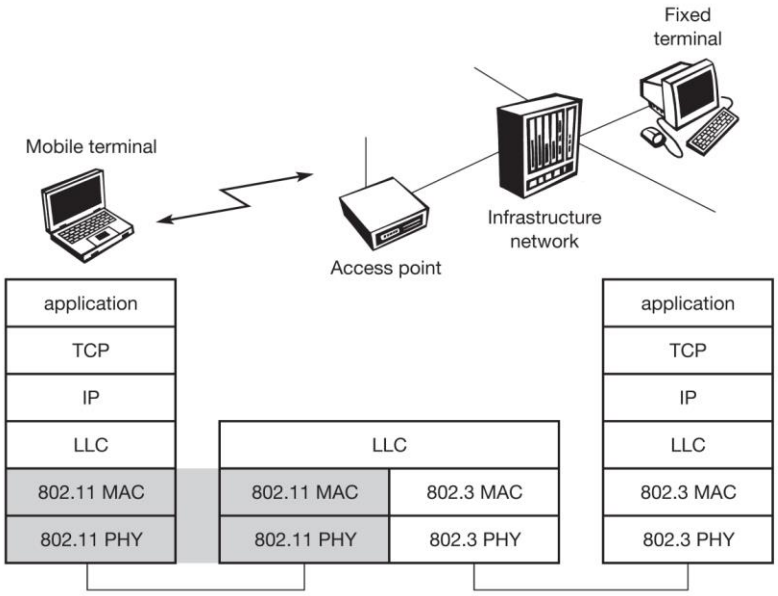


Figure: IEEE 802.11 protocol architecture and bridging

Where,

TCP - Transmission Control Protocol
IP - Internet Protocol
LLC - Logical Link Control
MAC - Medium Access Control layer
PHY –PHYsical Layer

13. **Draw the diagram of Detailed IEEE 802.11 protocol architecture and management.**

IEEE 802.11 protocol architecture and management

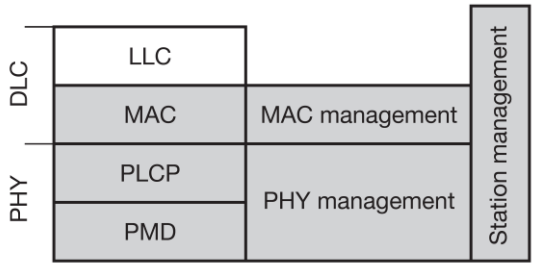


Figure: Detailed IEEE 802.11protocol architecture and management

where,

PHY - PHYsical Layer
- PLCP - Physical Layer Convergence Protocol
- PMD - Physical Medium Dependent
- PHY Management (PMD+PLCP)

DLC - Data Link Control
- LLC - Logical Link Control
- MAC - Medium Access Control layer

14. What is the task of PLCP?

Tasks of PLCP are

- PLCP - Physical Layer Convergence Protocol: Clear Channel Assessment signal (carrier sense signal) provides a common PHY service access point (SAP).

15. What is the task of PMD and PHY Management?

Tasks of PMD and PHY Managements are

- PMD Physical Medium Dependent modulation: Encoding and Decoding.
- PHY Management (PMD+PLCP) channel (tuning) selection, MIB Management.

16. What is the task of Station Management in IEEE 802.11protocol management?

Tasks of Station Management in IEEE 802.11 protocol management

- Coordination of all management functions
- Additional higher layer functions
  - Control of bridging
  - Interaction with the distribution system in the case of an access point

17. What are the tasks of MAC and MAC Management? (Or) What are the responsibilities of MAC management sub layer in 802.11? ***(Dec 2014, Nov 2017)***

MAC is the Medium access mechanisms for fragmentation of user data and encryption

MAC Management deal with

- Association and re-association of a station to an access point
- Roaming between different access points
- Synchronization, Roaming, Power management
- Maintains: MIB (Management Information Base (MIB)

18. What are the three different physical layers supported by IEEE 802.11?

IEEE 802.11 supports three different physical layers:

- One layer based on infra red
- Two layers based on radio transmission (primarily in the ISM band at 2.4 GHz, which is available worldwide).

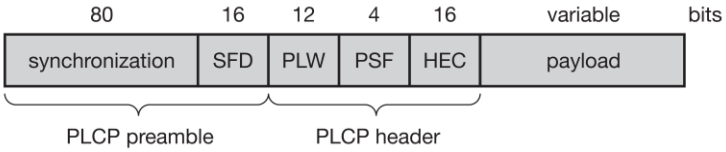
19. What are the specifications of Frequency hopping spread spectrum version of Physical layer?

Specifications of Frequency hopping spread spectrum version of Physical layer

- Spreading, despreading, signal strength, typ. 1 Mbit/s
- Minimum 2.5 frequency hops/s (USA), two-level GFSK modulation

20. Draw and write about FHSS PHY packet format.

FHSS PHY packet format

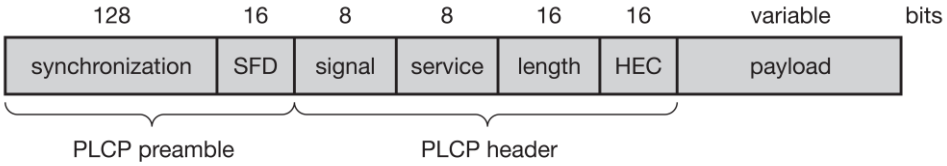


- Synchronization
  - PLCP preamble starts with 80 bit synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern (16 bits)
- PLW (PLCP_PDU Length Word) Protocol Data Unit
  - length of payload incl. 32 bit CRC of payload, PLW range o to 4095
- PSF (PLCP Signaling Field)
  - Data rate of the payload {0000→lowest 1Mbps, 0010 → 2Mbps, 1111 → 8.5Mbps
  - data of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)
  - CRC with $G(x) = x^{16}+x^{12}+x^5+1$; 16-bit Check sum

21. What do you know about Direct Sequence spread spectrum version of Physical layer?

- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK).
- Preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s.
- Chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code).
- Maximum radiated power 1 W (USA), 100 mW (EU), min. 1mW.

22. Draw and write about FHSS PHY packet format.



- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service Length
  - future use, 00: 802.11 compliant
  - length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length, $x^{16}+x^{12}+x^5+1$

23. Write about the Infra red version of Physical layer.

The physical layer, which is based on infra red (IR) transmission, uses near visible light at 850–950 nm.

- Infra red light is not regulated apart from safety restrictions (using lasers instead of LEDs).
- The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission.
- The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission.

24. What are the basic services provided by the MAC layer?

The basic servicesprovided by MAC layer are

a. Asynchronous Data Service (mandatory)
   i. exchange of data packets based on "best-effort"
   ii. support of broadcast and multicast

b. Time-Bounded Service (optional)
    i. implemented using PCF (Point Coordination Function)

25. What are the basic access mechanisms have been defined for IEEE 802.1?

Access methods defined for IEEE 802.11 are

a. DFWMAC-DCF CSMA/CA (mandatory)
    i. collision avoidance via randomized „back-off“ mechanism
    ii. minimum distance between consecutive packets
    iii. ACK packet for acknowledgements (not for broadcasts)
b. DFWMAC-DCF w/ RTS/CTS (optional)
    i. Distributed Foundation Wireless MAC
    ii. avoids hidden terminal problem
c. DFWMAC- PCF (optional)
    i. access point polls terminals according to a list

26. What are the different parameters that define the priorities of medium access?

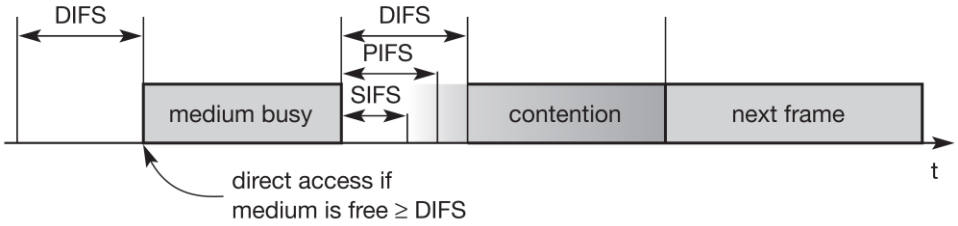


Figure: Medium access and inter-frame spacing

a. SIFS (Short Inter Frame Spacing)
    i. highest priority, for ACK, CTS, polling response
b. PIFS (PCF Inter-Frame Spacing)
    i. medium priority, for time-bounded service using PCF
c. DIFS (DCF inter-frame spacing)
    i. lowest priority, for asynchronous data service

MAC management

27. What are the functional groups of MAC Management?

Synchronization

a. try to find a LAN, try to stay within a LAN
b. timer etc.

Power management

a. sleep-mode without missing a message
b. periodic sleep, frame buffering, traffic measurements

Association/Reassociation

a. integration into a LAN
b. roaming, i.e. change networks by changing access points
c. scanning, i.e. active search for a network

MIB - Management Information Base

a. managing, read, write

28. Draw the diagramatic representation of Beacon transmission ina busy 802.11infrastructure network.

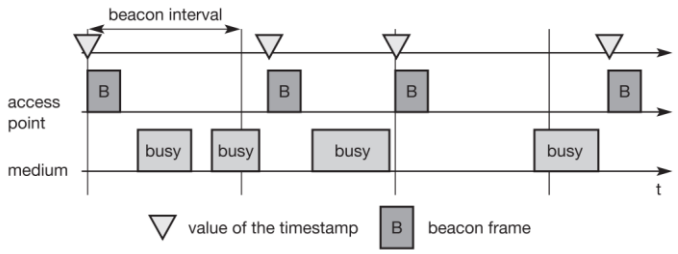


Figure: Beacon transmission in a busy 802.11 infrastructure network

29. Draw the diagramatic representation of Beacon transmission in a busy 802.11 ad-hoc network.

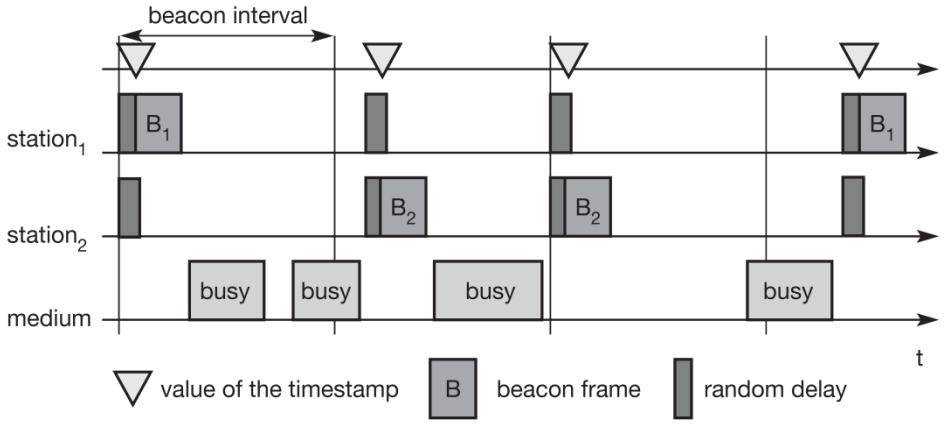


Figure: Beacon transmission in a busy 802.11 ad-hoc network

30. Draw the Power management in IEEE 802.1infrastructure networks

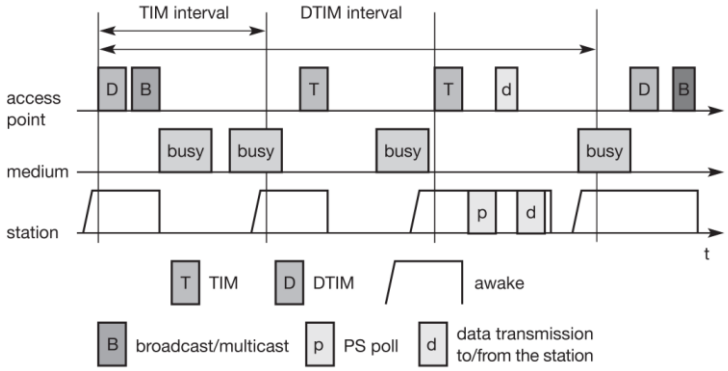


Figure: Power management inIEEE 802.11infrastructure networks

31. Draw the Power management in IEEE 802.11ad-hoc networks

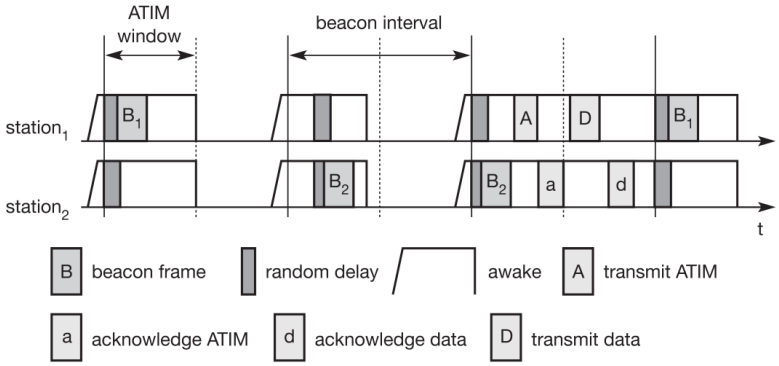


Figure: Power managementin IEEE 802.11ad-hoc networks

32. What is scanning in roaming between access points in IEEE 802.11?

Scanning: Scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

33. What are the types of scanning in roaming between access points in IEEE 802.11?

- Passive scanning
- Active scanning

34. What is meant by Reassociation Request and Reassociation Response?

Reassociation Request

a. station sends a request to one or several AP(s)

Reassociation Response

a. success: AP has answered, station can now participate
b. failure: continue scanning

35. What is Access Point accepting the Reassociation Request?

AP accepts Reassociation Request

a. signal the new station to the distribution system
b. the distribution system updates its data base (i.e., location information)
c. typically, the distribution system now informs the old AP so it can release resources

36. What is IEEE 802.11? [May 2018] *(Combine 36 & 37)*

Write in short about IEEE 802.11a.

IEEE 802.11a

- compatible MAC, but now 5 GHz band
- transmission rates up to 20 Mbit/s
- close cooperation with BRAN (ETSI Broadband Radio Access Network)

37. Write in short about IEEE 802.11b.

IEEE 802.11b

- higher data rates at 2.4 GHz
- proprietary solutions already offer 10 Mbit/s

38. Write in short about the newer developments in IEEE 802.11.

- 802.11e (MAC enhancements)
- 802.11f (Inter-Access Point Protocol)
- 802.11g (Data rates above 20 Mbit/s at 2.4 GHz)
- 802.11h (Spectrum managed 802.11a)
- 802.11i (Enhanced Security mechanisms)

HIPERLAN

39. What is HIPERLAN?

- HIPERLAN stands for high performance local area network.
- HIPERLAN1 was originally one out of four HIPERLANs envisaged, as ETSI decided tohave different types of networks for different purposes.
- The key feature of all four networks is their integration of time-sensitive data transfer services.
- Overtime,names have changed and the former HIPERLANs 2, 3, and 4 are nowcalled HiperLAN2, HIPERACCESS, and HIPERLINK.

Historical: HIPERLAN 1

40. What is HIPERLAN1?

- ETSI (1998b) describes HIPERLAN 1 as a wireless LAN supporting priorities and packet life time for data transfer at 23.5 Mbit/s.
- It includes forwarding mechanisms,topology discovery, user data encryption, network identification and power conservation mechanisms.
- HIPERLAN 1 should operate at 5.1–5.3 GHz with a range of 50 m in buildings at 1W transmit power.

41. What are the three phases in medium acces divided by EY-NPMA? ***(Nov/ Dec 2013)***

EY-NPMA (Elimination-yield non-preemptive priority multiple access) divides the medium access of different competing nodes into three phases:

- Prioritization: Determine the highest priority of a data packet ready to besent by competing nodes.
- Contention: Eliminate all but one of the contenders, if more than onesender has the highest current priority.
- Transmission: Finally, transmit the packet of the remaining node.

42. Give the diagramatic representation of Phases of the HIPERLAN 1 EY-NPMA access scheme.

***EY-NPMA** - **E**limination-**Y**ield Non-preemptive **P**riority **M**ultiple **A**ccess

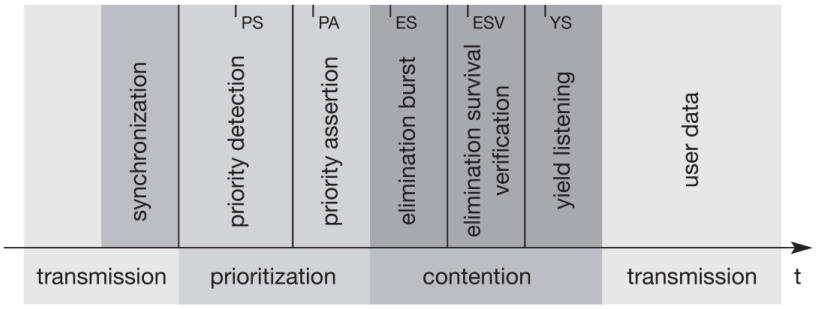


Figure: Phases of the HIPERLAN 1 EY-NPMA access scheme

43. What are the channel access conditions involve with EY-NPMA?

- Synchronized channel condition
- Channel-free condition
- Hidden elimination condition

44. What is meant by synchronized channel condition?

In a case where several nodes compete for the medium, all three phases arenecessary (called 'channel access in synchronized channel condition').

45. What is meant by Channel-free condition?

If the channel is free for at least 2,000 so-called high rate bit-periods plus a dynamic extension, only the third phase, i.e. transmission, is needed (called 'channel access in channel-free condition').

46. What is meant by Hidden elimination condition?

HIPERLAN 1 also supports 'channel access in the hidden elimination condition' to handle the problem of hidden terminals asdescribed in ETSI (1998b).

47. Write about Dynamic extension.

- The dynamic extension is randomly chosen between 0 and 3 times 200 high rate bit-periods with equal likelihood.
- This extension minimizes the probability of collisions accessing a free channel if stations are synchronized on higher layers and try to access the free channel at the same time.

48. What are the subphases of Contention Phase?

- Elimination phase
- Yield phase

49. What is the function of elimination phase?

Elimination phase:The purpose of the elimination phase is to eliminate as many contending nodes as possible (but surely not all). The result of the elimination phase is a more or less constant number of remaining nodes, almost independent of the initial number of competing nodes.

50. What is the function of yield phase?

Yield phase: Finally, the yield phase completes thework of the elimination phase with the goal of only one remaining node.

WATM

51. What is called WATM? (May/June 2013)

- Wireless ATM (WATM; sometimes also called wireless mobile ATM, (WATM) describe a transmission technology and tries to specify a complete communication.
- Many aspects of the IEEE WLANs originate from the data communication community, many WATM aspects come from the telecommunication industry.

Motivation for WATM

52. Write any two reasons led to the development of WATM.(or) Identify the need of WATM systems. (Apr/May 2019)

- The need for seamless integration of wireless terminals into an ATM network.
- For ATM to be successful, it must offer a wireless extension. Otherwise it cannot participate in the rapidly growing field of mobile communications.

53. What are the general extensions of the ATM system also need to be considered for a mobile ATM?

- Location management.
- Mobile routing
- Handover signalling
- QoS and traffic control.
- Network management

All extensions of protocols or other mechanisms also require an extension of the management functions to control the network.

WATM services

54. Give any two services provided by WATM.

- **Office environments:** Multi-media conferencing, online multi-media database access, and telecommuting.
- **Universities, schools, training centres:** Distance learning, wireless and mobile access to databases, internet access, or teaching in the area of mobile multi-media computing.

Generic reference model

55. Draw the diagramatic representation of an example of a generic WATM reference model.

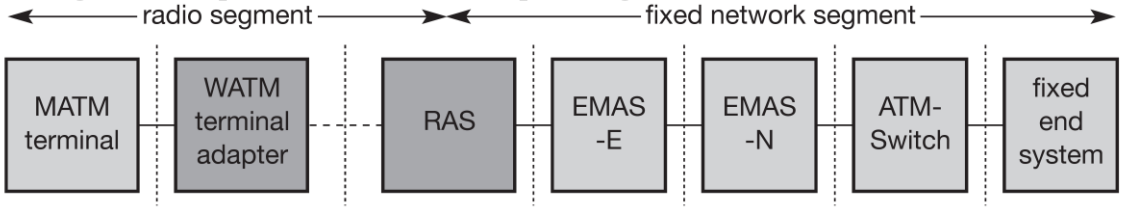


Figure: Example of a genericWATM reference model

Where,

MATM : mobile ATM (MATM)
WATM : Wireless ATM (MATM)
RAS : Radio Access System
EMAS-E : End-user Mobility-supporting ATM Switch - Edge
EMAS-N : End-user Mobility-supporting ATM Switch - Network
ATM-Switch: Asynchronous Transfer Mode - Switch

Handover

56. What are the process involved during handover in WATM?

- The main problem for WATM during the handover is rerouting all connections and maintaining connection quality.
- Handover involves rerouting of connections and also involves reserving resources in switches, testing of availability of radio bandwidth, tracking of terminals to perform look-ahead reservations etc.

57. What are the different requirements should be set up for handover?

The following list presents some of the requirements

- Handover of multiple connections
- Handover of point-to-multi-point connections
- QoS support

- Data integrity and security
- Signaling and routing support
- Performance and complexity

Location management

58. What are the several requirements for location management?

- Transparency of mobility
- Security
- Efficiency and scalability
- Identification
- Inter-working and standards

Mobile quality of service

59. Write short notes on Mobile quality of service.

- Quality of service (QoS) guarantees are one of the main advantages envisaged for WATM networks compared to, e.g., mobile IP working over packet radio networks.
- While the internet protocol IP does not guarantee QoS, ATM networksdo (at the cost of higher complexity).

60. What are the three important parts of MQoS?

- Wired QoS
- Wireless QoS
- Handover QoS

61. What are the two different types of QoS during handover?

- Hard handover QoS
- Soft handover QoS

62. What is Hard handover QoS?

- ***Hard handover QoS:*** While the QoS with the current RAS may be guaranteed due to the current availability of resources, no QoS guarantees are given after the handover.
- This is comparable to the traditional approach for,e.g., GSM networks with voice connections.
- If a terminal can set up a connection,the connection's quality is guaranteed.
- If there are not enough resources after handover (too many users are already in the target cell), thes ystem cuts off the connection.

63. What is Soft handover QoS?

- ***Soft handover QoS:*** Even for the current wireless segment, only statistical QoS guarantees can be given, and the applications also have to adapt after the handover.
- This assumes adaptive applications and at least allows for some remaining QoS guarantees during, e.g., periods of congestion or strong interference.

Access scenarios

64. Draw the diagramatic representation of WATM reference modelwith several accessscenarios.

In figure,

T (terminal)
MT (mobile terminal
WT (wireless terminal)
WMT (wireless mobile terminal)
RAS (radio access system):
EMAS (end-user mobility supporting ATM switch, -E: edge, -N: network)
NMAS (network mobility-supporting ATM switch)
MS (mobile ATM switch)

ACT (ad-hoc controller terminal)

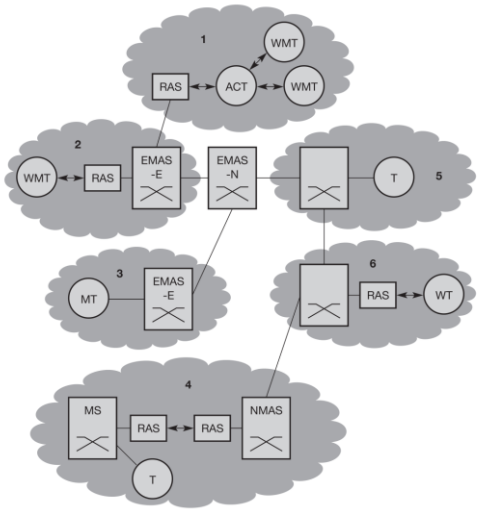


Figure: WATM reference model with several access scenarios

65. Give the several scenarios which should be supported by WATM if fully specified.

- Wireless ad-hoc ATM network (scenario 1)
- Wireless mobile ATM terminals (scenario 2)
- Mobile ATM terminals (scenario 3)
- Mobile ATM switches (scenario 4)
- Fixed ATM terminals (scenario 5)
- Fixed wireless ATM terminals (scenario 6)

BRAN

66. What is meant by BRAN ?

- The broadband radio access networks (BRAN), which have been standardized by the EuropeanTelecommunications Standards Institute (ETSI), could have been an RAL for WATM (ETSI, 2002b).
- The main motivation behind BRAN is the deregulation and privatization of the telecommunication sector in Europe.
- The advantages of radio access are high flexibility and quick installation.

67. What are the different types of networks specified by BRAN?

BRAN has specified four different network types(ETSI, 1998a):

- HIPERLAN 1
- HIPERLAN/2
- HIPERACCESS
- HIPERLINK

HiperLAN2

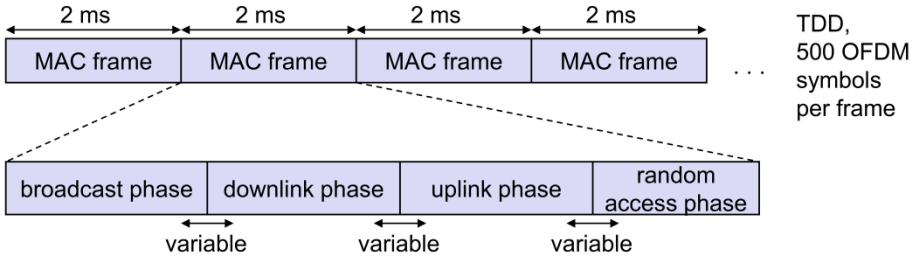
68. What are the basic characteristics of HiperLAN2?

- High data rates for users up to 54 Mbps
- 5 GHz band (Europe: 5.15-5.35 GHz and 5.47-5.725 GHz license exempt bands)
- Connection oriented
- Quality of service support
- Dynamic frequency selection
- Security support
- Mobility support
- Network and application independent
- Power save modes
- Plug and Play

69. Differentiate the IEEE 802.11 from the Hiperlan MAC protocol.

Characteristic	IEEE 802.11	HIPERLAN/2
Spectrum	2.4 GHz	5 GHz
Max. physical rate	2 Mbps	54 Mbps
Max. data rate, layer 3	1.2 Mbps	32 Mbps
Medium access control/ Media sharing	CSMA/CA	Central resource control, TDMA/TDD
Access scheme	DCF/PCF	Elimination yield-non preemptive priority multiple access
Connectivity	Connectionless	Connection oriented
Multicast	Yes	Yes
QoS support	PCF	ATM/802.1p/Rsource reSerVation Protocol/Differential service (full control)
Frequency selection	Frequency hopping or DSSS	Single carrier with dynamic frequency selection
Authentication	No	Network access identifier/IEEE address/ X.509
Encryption	40-bit RC4	Data Encryption Standard (DES), triple DES
Handover support	No	No
Fixed network support	Ethernet	Ethernet, IP, ATM, UMTS, Firewire, PPP
Management	802.11 MIB	HIPERLAN/2 MIB
Radio link quality control	No	Link adaptation

70. Draw the basic structure of HiperLAN2 MAC frames.



MAC: creates frames of 2 ms duration

Each MAC frame is further sub-divided into four phases

- broadcast phase: The AP sends inf of the current frame
- downlink phase: AP to MTs
- uplink phase: MTs to AP
- random access phase: for registered MTs – capacity requestsfor new MTs access requests (slotted ahloha)

BLUE TOOTH

71. What is called Bluetooth?

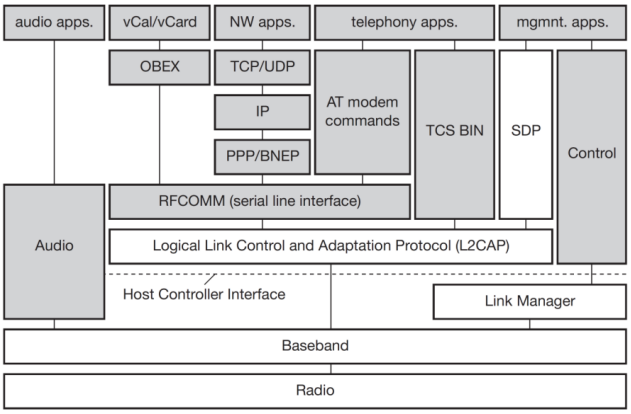
Bluetooth is the wireless technology for short-range voice and data communication.

72. What are the different user scenarios imagined for wireless piconets or WPANs?

a. **connection of peripheral devices**
   i. loudspeaker, joystick, headset
b. **support of ad-hoc networking**
   i. small devices, low-cost
c. **bridging of networks**

i. e.g., GSM via mobile phone - Bluetooth – laptop

73. Draw the protocol stack of Bluetooth. [*Dec 2013*] *(Or)*
Give the protocol stack involved for Bluetooth communication. *]Dec 2012]*



74. What are the technology characteristics of Bluetooth? (or) List out the main features of Bluetooth. [Nov 2019]

- Low-cost
- Low-power
- Small-sized
- Short-range
- Robust wireless technology

75. What are the General Characteristics of Blue tooth? (or)
List any four important features of bluetooth technology. (May 2015)

- Universal wireless interface
- Ad-hoc networking architecture
- 80 Mhz in unlicenced ISM band at 2.45 Ghz
- Gross bitrate 1 Mbps
- Simultaneous voice and high speed data support
- Evolves from cable replacement → networking solution

70. Define piconet and scatternet.(or) What are Piconet and Scatternet? (Apr/May 2019)

Piconet is the basic unit of Bluetooth networking. Master and one to seven slave devices are used.Master determines channel and phase

Scatternet is the device in one piconet may exist as master or slave in another piconet. It allows many devices to share same area and makes efficient use of bandwidth

Networking

71. Write about the different devices with different roles in Bluetooth. *(May/June 2012)*
Name the four state of Bluetooth. *(Dec 2014)*

Master:

- One device in the piconet can act as master (M)
- determines the hopping pattern in the piconet

Slaves:

- All other devices connected to the master must act as slaves (S).
- the slaves have to synchronize to the pattern determined by the master

Parked devices (P):

- Can not actively participate in the piconet (i.e., they do not have a connection)
- More than 200 devices can be parked.
- But are known and can be reactivated within some milliseconds
- More than 200 devices can be parked.

Stand-by (SB) Devices:

- do not participate in the piconet.

76. Write in short about Piconet.

- Each piconet has exactly one master and up to seven simultaneous slaves.
- The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth.

Protocol stack

77. What are the elements comprised in core protocols of Bluetooth?

- Radio
- Baseband
- Link manager protocol
- Logical link control and adaptation protocol (L2CAP)
- Service discovery protocol

78. What is the functionality of L2CAP? List the different types of logical channels. [Nov 2017]

Logical link control and adaptation protocol (L2CAP) governs the adaptation of higher layers to the baseband (connectionless and connection-oriented services).

Different types of logical channels:

- Broadcast control channel (BCCH)
- Frame control channel (FCCH)
- Random access feedback channel (RFCH)
- RLC broadcast channel (RBCH)
- Dedicated control channel (DCCH)
- User broadcast channel (UBCH)
- User multi-cast channel (UMCH)

WiMAX

79. Write the expansion for WiMax and features of the system. [April 2014]

What is WiMax? Mention its features. [Nov 2018]

- WiMAX is a family of technologies based on IEEE 802.16 standards.
- There are two main types of WiMAX today,
  - fixed WiMAX (IEEE 802.16d — 2004), and
  - mobile WiMAX (IEEE 802.16e — 2005).
- Fixed WiMAX: It is a point-to- multipoint technology, whereas
- Mobile WiMAX: It is a multipoint-to-multipoint technology, similar to a cellular infrastructure.

80. What is the frequency band channel bandwidth specification of WiMax standard? [April 2014]

- There is no uniform global licensed spectrum for WiMAX in the United States.
- The biggest segment available is around 2.5 GHz.
- There are several variants of 802.16, depending on local regulatory conditions.
- Mobile WiMAX based on the 802.16e standard will most likely be in 2.3 GHz and 2.5 GHz frequencies — low enough to accommodate the NLOS conditions between the base station and mobile devices.

81. OFDM uses a set of orthogonal subcarriers for transmission of data. OFDM is used in WLANs. Consider an OFDM system that uses 52 sub-carriers out of which 48 are pilot subcarriers. System bandwidth is 20MHz and OFDM symbol duration including cyclic prefix is 4 μs . If code rate is ¾ and 64 QAM is used, find the data rate. [Apr/Mar 2017]

Solution:

The 64 QAM corresponds to 6 bits per symbol. Total number of data bits transmitted per OFDM symbol is $4\,\mu s$ is $4\times 68\times \frac{3}{4} = 216.$

Therefore the data rate is $216\times \frac{1000000}{4} = 54 Mbps$.

*****

71. Compare Wi-Fi, Wimax, Optical and 3G Technologies	**08m**	**2015**

Feature	WiMax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
Mobility	Mobile WiMax (802.16e)	In development	In development

Mesh	Yes	Vendor Proprietary	Vendor Proprietary
Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

72. Compare the features of different WLAN standards.	**(12m)**	**2015**
Compare the medium access mechanism of DCF methods adopted in IEEE 802.11 WLAN.	**(16m)**	**May 2017**

Table Comparison of wireless networks

Criterion	IEEE 802.11b	IEEE 802.11a	HiperLAN2	Bluetooth
Frequency	2.4 GHz	5 GHz	5 GHz	2.4 GHz
Max. trans. rate	11 Mbit/s	54 Mbit/s	54 Mbit/s	< 1 Mbit/s
User throughput	6 Mbit/s	34 Mbit/s	34 Mbit/s	< 1 Mbit/s
Medium access	CSMA/CA	CSMA/CA	AP centralized	Master centralized
Frequency management	None	802.11h	DFS	FHSS
Authentication	None/802.1x	None/802.1x	X.509	Yes
Encryption	WEP, 802.11i	WEP, 802.11i	DES, 3DES	Yes
QoS support	Optional (PCF)	Optional (PCF)	ATM, 802.1p, RSVP	Flow spec, isochronous
Connectivity	Connectionless	Connectionless	Connection-oriented	Connectionless + connection-oriented
Available channels	3	12 (US)	19 (EU)	Soft – increasing interference
Typ. transmit power	100 mW	0.05/0.25/1W, TPC with 802.11h	0.2/1W, TPC	1/2.5/100 mW
Error control	ARQ	ARQ, FEC (PHY)	ARQ, FEC (PHY)	ARQ, FEC (MAC)

73. List the IEEE 802 working groups.

IEEE 802 working groups

	Working group
802.1	Higher Layer LAN Protocol
802.2	Logical Link Control (LLC)
802.3	Ethernet
802.11	WLAN
802.15	WPAN
802.16	Broadband Wireless Access (BWA)
802.17	Resilient Packet Ring
802.18	Radio Regulatory TAG
802.20	Mobile Broadband Wireless Access (MBWA)
Link Security	Executive Committee Study Group
802 Handoff	Executive Committee Study Group

74. **Explain Primary IEEE 802.11 specifications and their comparisons.**

Primary IEEE 802.11 specifications and their comparisons:

	802.11a	802.11b	802.11g	802.11n
Approval date	July 1999	July 1999	June 2003	August 2006
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz or 5 GHz
Number of spatial streams	1	1	1	1, 2, 3, or 4
Channel width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz

75. Compare *HIPERLAN/2 and IEEE 802.11*

A comparison of HIPERLAN/2 and IEEE 802.11:

Characteristic	IEEE 802.11	HIPERLAN/2
Spectrum	2.4 GHz	5 GHz
Max. physical rate	2 Mbps	54 Mbps
Max. data rate, layer 3	1.2 Mbps	32 Mbps
Medium access control/ Media sharing	CSMA/CA	Central resource control, TDMA/TDD
Access scheme	DCF/PCF	Elimination yield-non preemptive priority multiple access
Connectivity	Connectionless	Connection oriented
Multicast	Yes	Yes
QoS support	PCF	ATM/802.1p/Rsource reSerVation Protocol/Differential service (full control)
Frequency selection	Frequency hopping or DSSS	Single carrier with dynamic frequency selection
Authentication	No	Network access identifier/IEEE address/ X.509
Encryption	40-bit RC4	Data Encryption Standard (DES), triple DES
Handover support	No	No
Fixed network support	Ethernet	Ethernet, IP, ATM, UMTS, Firewire, PPP
Management	802.11 MIB	HIPERLAN/2 MIB
Radio link quality control	No	Link adaptation

76. Compare various WLAN standards.

Give any three differences between HIERLAN1 and HIERLAN 2. [May 2018]

Comparisons of various WLAN standards:

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g	HIPERLAN/1	HIPERLAN/2	MMAC HiSWAN
Rectification	June 1997	Sept. 1999	Sept. 1999	June 2003	early 1993	Feb. 2000	April 1997
RF bandwidth (GHz)	2.4	2.4	5.0	2.4	5	5	5
Max. data rate (Mbps)	2	11	54	54	23.5	54	27
Physical layer (PHY)	FHSS, DSSS, IR	DSSS	OFDM	OFDM	GMSK	OFDM	OFDM
Range (m)	50–100	50–100	50–100	50–100	50	50 indoor, 300 outdoor	100–150

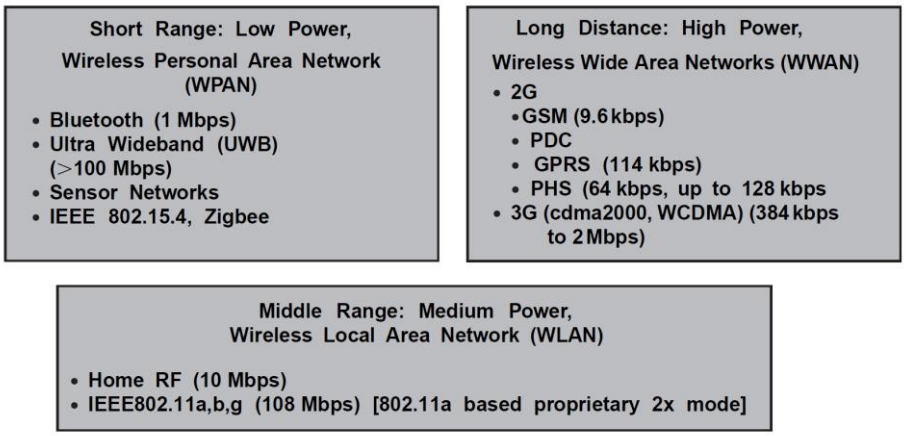
77. Compare Wi-Fi and WiMAX.

Comparison of Wi-Fi and WiMAX:

Wi-Fi	WiMAX
802.11a—OFDM, maximum rate = 54 Mbps 802.11b—DSSS, maximum rate = 11 Mbps 802.11g—OFDM, maximum rate = 54 Mbps	802.16—OFDM, maximum rate = 50 Mbps 802.16e—OFDM, maximum rate ~ 30 Mbps
Range <100 m	A few km's non-line-of-sight, more with line of sight
Indoor environment	Outdoor environment
No admission control, no load balancing	Admission control and load balancing
No quality of service (QoS)	Five QoS classes enforced by base station

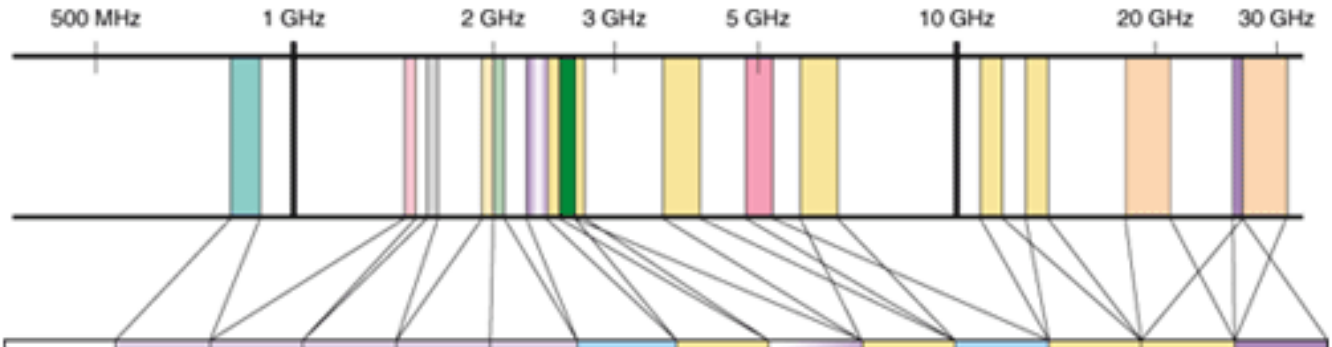
78. Explain the range of wireless networks.

Range of Wireless networks



PDC: Personal Digital Cellular (Japan)
GPRS: General Packet Radio Service
PHS: Personal Handy Phone System (Japan)

79. Draw the frequency spectrum for wireless operation. [Nov 2019]



System	PDC	PDC	FOMA	PHS	FOMA	WiFi 11b/11g	Fixed satellite	BWA	Fixed satellite	WiFi 11a/11j	Fixed satellite	Fixed satellite	WiPAS
Frequency	800 MHz	1.5 GHz	1.7 GHz	1.9 GHz	2.0 GHz	2.4 GHz	2.4 GHz 2.6 GHz	2.5 GHz	4 GHz 6 GHz	5 GHz	12 GHz 14 GHz	20 GHz 30 GHz	26 GHz
Bandwidth	29 MHz ×2	5.5 MHz ×2	10 MHz ×2	35.1 MHz	15 MHz ×2	97 MHz	35 MHz ×2	70 MHz	800 MHz 635 MHz	616 MHz	550 MHz 750 MHz	3.5 GHz ×2	1.7 GHz
Application	MWA	MWA	MWA	MWA	MWA	WLAN NWA	MWA	MWA FWA NWA	FWA	WLAN NWA FWA	FWA MWA		FWA
NTT operator	DoCoMo	DoCoMo	DoCoMo	DoCoMo	DoCoMo	East, West, Coms, DoCoMo	DoCoMo	Undecided	East, West, DoCoMo	East, West, Coms, DoCoMo	East, West, Coms		East, West
Remarks		CITIPHONE	Tokyo, Nagoya, Osaka areas			Interference with other systems		Four systems including 802.16e					

PDC: personal digital cellular
FOMA: freedom of mobile multimedia access
PHS: personal handyphone system
BWA: broadband wireless access
WiPAS: wireless Internet protocol access system

ANNA UNIVERSITY, CHENNAI
AFFILIATED INSTITUTIONS
R-2013
B.E. ELECTRONICS AND COMMUNICATION ENGINEERING
SYLLABUS
SEMESTER- VIII

		L	T	P	C
EC6802	**WIRELESS NETWORKS**	**3**	**0**	**0**	**3**

OBJECTIVES:

- To study about Wireless networks, protocol stack and standards.
- To study about fundamentals of 3G Services, its protocols and applications.
- To study about evolution of 4G Networks, its architecture and applications.

UNIT I WIRELESS LAN 9

Introduction - WLAN technologies: Infrared, UHF narrowband, spread spectrum - IEEE802.11: System architecture, protocol architecture, physical layer, MAC layer, 802.11b, 802.11a – Hiper LAN: WATM, BRAN, HiperLAN2 – Bluetooth: Architecture, Radio Layer, Baseband layer, Link manager Protocol, security - IEEE802.16 - WIMAX: Physical layer, MAC, Spectrum allocation for WIMAX.

UNIT II MOBILE NETWORK LAYER 9

Introduction - Mobile IP: IP packet delivery, Agent discovery, tunneling and encapsulation, IPV6- Network layer in the internet - Mobile IP session initiation protocol - mobile ad-hoc network: Routing, Destination Sequence distance vector, Dynamic source routing.

UNIT III MOBILE TRANSPORT LAYER 9

TCP enhancements for wireless protocols - Traditional TCP: Congestion control, fast retransmit/fast recovery, Implications of mobility - Classical TCP improvements: Indirect TCP, Snooping TCP, Mobile TCP, Time out freezing, Selective retransmission, Transaction oriented TCP - TCP over 3G wireless networks.

UNIT IV WIRELESS WIDE AREA NETWORK 9

Overview of UTMS Terrestrial Radio access network-UMTS Core network Architecture: 3G-MSC, 3GSGSN, 3G-GGSN, SMS-GMSC/SMS-IWMSC, Firewall, DNS/DHCP-High speed Downlink packet access (HSDPA)- LTE network architecture and protocol.

UNIT V 4G NETWORKS 9

Introduction – 4G vision – 4G features and challenges - Applications of 4G – 4G Technologies: Multicarrier Modulation, Smart antenna techniques, OFDM-MIMO systems, Adaptive Modulation and coding with time slot scheduler, Cognitive Radio.

TOTAL: 45 PERIODS

OUTCOMES:

Upon completion of the course, the students will be able to

- Conversant with the latest 3G/4G and WiMAX networks and its architecture.
- Design and implement wireless network environment for any application using latest wireless protocols and standards.
- Implement different type of applications for smart phones and mobile devices with latest network strategies.

TEXT BOOKS:

1. Jochen Schiller, “Mobile Communications”, Second Edition, Pearson Education 2012.(Unit I,II,III)
2. Vijay Garg, “Wireless Communications and networking”, First Edition, Elsevier 2007.(Unit IV,V)

REFERENCES:

1. Erik Dahlman, Stefan Parkvall, Johan Skold and Per Beming, "3G Evolution HSPA and LTE for Mobile Broadband”, Second Edition, Academic Press, 2008.
2. Anurag Kumar, D.Manjunath, Joy kuri, “Wireless Networking”, First Edition, Elsevier 2011.
3. Simon Haykin , Michael Moher, David Koilpillai, “Modern Wireless Communications”, First Edition, Pearson Education 2013.

UNIT II

MOBILE NETWORK LAYER

Introduction - Mobile IP: IP packet delivery, Agent discovery, tunneling and encapsulation, IPV6-Network layer in the internet - Mobile IP session initiation protocol - mobile ad-hoc network: Routing, Destination Sequence distance vector, Dynamic source routing.

2.1 Mobile IP
- 2.1.1 Motivation for Mobile IP
- 2.1.2 Requirements to Mobile IP (RFC 2002)
- 2.1.3 Operation of Mobile IP
  - 2.1.3.1 IP packet delivery
- 2.1.4 Discovery
- 2.1.5 Registration
- 2.1.6 Tunneling
- 2.1.7 Encapsulation

2.2 IPV6
- 2.2.1 Features of IPv6
- 2.2.2 IP micro-mobility support
- 2.2.3 Cellular IP
- 2.2.4 Hawaii
- 2.2.5 Hierarchical mobile IPv6 (HMIPv6)

2.3 Dynamic Host Configuration Protocol (DHCP)
- 2.3.1 Configuration/Model
- 2.3.2 Client Initialization via DHCP

2.4 Mobile ad-hoc network
- 2.4.1 Routing,
- 2.4.2 Routing Algorithms
  - 2.4.2.1 Destination Sequence distance vector
  - 2.4.2.2 Dynamic source routing.
  - 2.4.2.3 Other Routing Protocols
    - 2.4.2.3.1 Flat ad hoc routing
    - 2.4.2.3.2 Hierarchical Ad hoc routing
    - 2.4.2.3.3 Geographic position assisted Ad hoc routing
    - 2.4.2.3.4 Greedy perimeter stateless routing

2.5 Network layer in the internet

2.6 Mobile IP session initiation protocol

2.1 MOBILE IP

- Mobile IP was developed to enable computers ***to maintain Internet connectivity while moving*** from one Internet attachment point to another.
- Mobile IP can work with wired connections, but it is particularly ***suited to wireless connections***.
- The term ***mobile*** in this context involves
  - a user connected to applications across the Internet
  - the user's point of attachment changes dynamically, and
  - All connections are automatically maintained even with the change.

- In ISP (Internet service provider) case, in contrast, the user's Internet connection is terminated each time the user moves and a new connection is initiated when the user dials back.

- In Mobile IP, with each new Internet connection establishment, software in the point of attachment is used to obtain a new, temporarily assigned IP address.
- This ***temporary IP address*** is used by the user's correspondent for each application-level connection (e.g., FTP, Web connection). A better term for this kind of use is ***nomadic*** ***(roaming)***.

2.1.1 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 long time
- TCP connections break, security problems

2.1.2 Requirements to Mobile IP (RFC 2002)

1. ***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

2. ***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
3. ***Security***
   - ✓ Authentication of all registration messages
4. ***Efficiency and scalability***
   - ✓ Only little additional messages to the mobile system required.
   - ✓ World-wide support of a large number of mobile systems in the whole Internet.

2.1.3 Operation of Mobile IP

1. State the entities and terminologies used in Mobile IP along with tunneling and also explain the three types of encapsulation mechanisms used in triangle routing	***(16m)***	***Apr 2017***
2. Explain mobile management in Mobile IP. What is meant by triangle routing?	***(16m)***	***Nov 2013***
3. Explain the Mobile IP session initiation protocol for IP packet delivery is mobile IP networks.	***(16m)***	***May 2018***
4. Discuss the entities and terminology of mobile IP networks.	***(08m)***	***Nov 2018***
5. What is Mobile IP? State the properties and explain in detail.	***(13m)***	***Nov 2019***

2.1.3.1 IP packet delivery

- Routers make use of the IP address in an IP datagram to perform routing.
- The ***network portion*** of an IP address is used by routers to move a datagram from the source computer to the network, to which the target computer is attached.
- Then the final router on the path, which is attached to the same network as the target computer, uses the ***host portion*** of the IP address to deliver the IP datagram to the destination.
- This IP address is known to the next higher layer in the protocol architecture.

- Most applications over the Internet are supported by TCP connections.
- When a TCP connection is set up, the TCP entity on each side of the connection knows the IP address of the correspondent host.

- When a TCP segment is handed down to the IP layer for delivery, TCP provides the IP address, and IP creates an IP datagram with that IP address in the IP header and sends the datagram out for routing and delivery.
- With a mobile host, the IP address may change while one or more TCP connections are active.

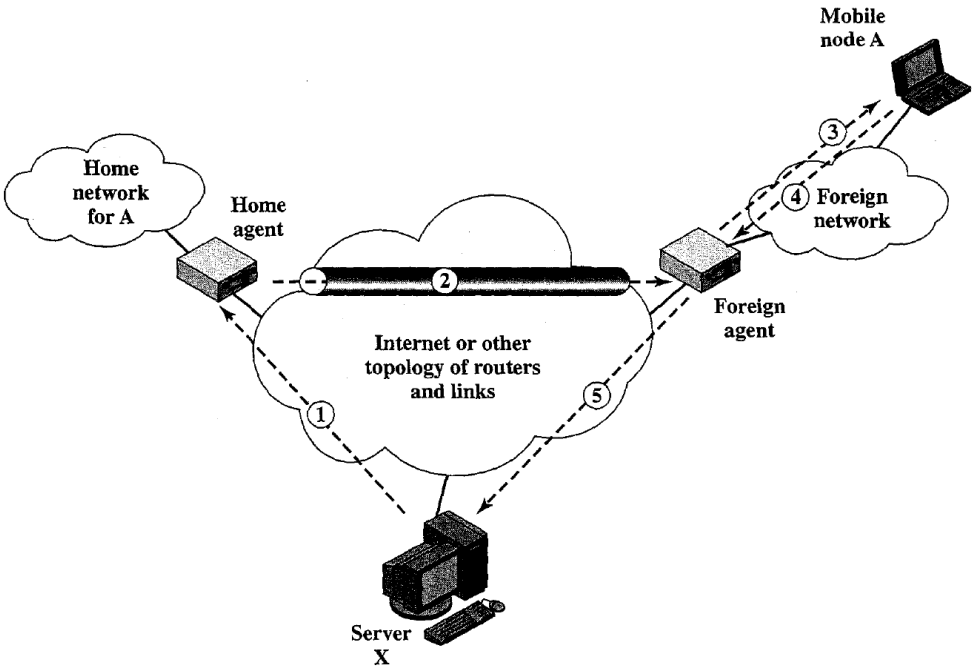


Figure 2.1 Mobile IP Scenario

Figure 2.1 shows in general terms how Mobile IP deals with the problem of dynamic IP addresses.

- ***Home network:*** A mobile node is assigned to a particular network, known as its ***home network.***
- ***Home address:*** Its IP address on that network, known as its ***home address,*** is static.
- ***Foreign network:*** When the mobile node moves its attachment point to another network, that network is considered as a foreign network for this host.
- ***Foreign agent:*** Once the mobile node is reattached, it indicates its presence by registering with a network node (a router) on the foreign network known as a foreign agent.
- ***Home agent:*** The mobile node then communicates with a similar agent on the user's home network, known as a home agent, giving the home agent the care-of address of the mobile node; the care-of address identifies the foreign agent's location.
- Typically, one or more routers on a network will implement the roles of both home and foreign agents.

When IP datagrams are exchanged over a connection between the mobile node and another host (a server in Figure 2.1), the following operations occur:

1. Server X transmits an IP datagram destined for mobile node A, with A's home address in the IP header. The IP datagram is routed to A's home network.

2. At the home network, the incoming IP datagram is intercepted by the home agent.
   - ✓ The home agent encapsulates the entire datagram inside a new IP datagram that has the A's care-of address in the header, and retransmits the datagram.
   - ✓ The use of an outer IP datagram with a different destination IP address is known as tunneling.
   - ✓ This IP datagram is routed to the foreign agent.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network-level PDU (e.g., a LAN LLC frame), and delivers the original datagram to A across the foreign network.
4. When A sends IP traffic to X, it uses X's IP address. In our example, this is a fixed address; that is, X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network for routing to X. Typically, this router is also the foreign agent.
5. The IP datagram from A to X travels directly across the Internet to X, using X's IP address.

1. Explain in detail about the underlying protocol support for the Mobile IP. (Or) Discuss the concept of agent discovery in Mobile IP

To support the operations illustrated in Figure 2.1, Mobile IP includes three basic capabilities:

- ***Discovery:*** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- ***Registration:*** A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.
- ***Tunneling:*** Tunneling is used to forward IP datagrams from a home address to a care-of address.

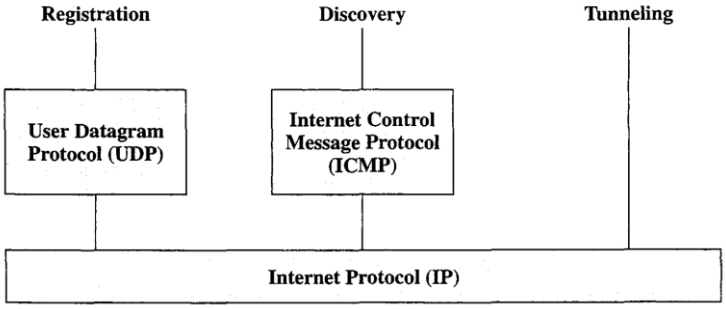


Figure 2.2 Protocol Support for Mobile IP

- Figure 2.2 indicates the underlying protocol support for the Mobile IP capability.

- The ***registration protocol*** communicates between an application on the mobile node and an application in the home agent and hence uses a transport-level protocol.
- Because ***registration is a simple request-response transaction***, the overhead of the connection-oriented TCP is not required, and therefore UDP is used as the transport protocol.

- ***Discovery*** makes use of the existing ***ICMP (Internet Control Message Protocol)*** by adding the appropriate extensions to the ICMP header.
- ICMP is a connectionless protocol well suited for the discovery operation.

- Finally, ***tunneling*** is performed at the IP level. Mobile IP is specified in a number of RFCs. The basic defining document is RFC 2002. Table 2.1 lists some useful terminology from RFC 2002.

2.1.4 Discovery

- The ***discovery process*** in Mobile IP is very ***similar to*** the ***router advertisement process*** defined in ICMP.
- ***Agent discovery*** makes use of ICMP router advertisement messages, with one or more extensions specific to Mobile IP.

- The ***mobile node*** is responsible for an ***ongoing discovery process***.
- If the ***mobile node*** is attached to its home network (then, the IP datagrams may be received without forwarding).
- If the mobile node is attached to a foreign network then IP datagram needs forwarding.

- A transition from the home network to a foreign network can occur at any time without notification to the network layer (i.e., the IP layer).
- Thus, discovery for a mobile node is a continuous process.

- For the purpose of discovery, a router (agent) periodically ***issues a router advertisement*** ICMP message with an advertisement extension.
- The router advertisement portion of the message includes the ***IP address of the router***.
- The ***advertisement extension*** includes ***additional information about the router's role as an agent***.
- A ***mobile node listens*** for these agent advertisement messages.

- The mobile node must compare the network portion of the router's IP address with the network portion of its own home address.
- If these network portions do not match, then the mobile node is on a foreign network.

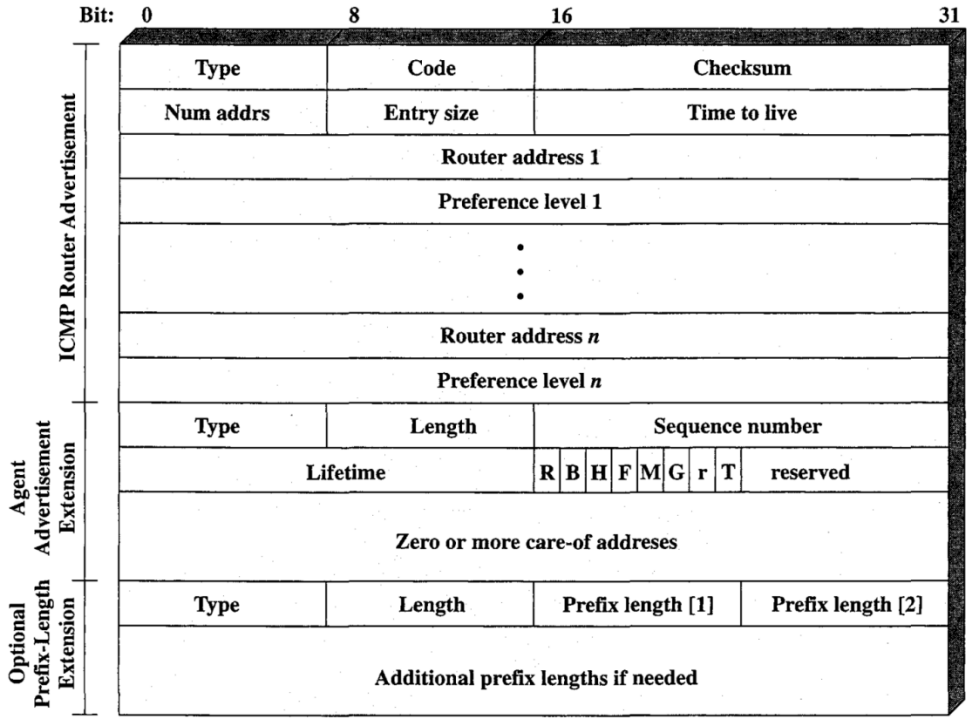


Figure 2.3 Mobile IP Agent Advertisement Message

The agent advertisement extension following the ICMP router advertisement fields consists of the following fields (Figure 2.3):

- ✓ ***Type:*** 16, indicates that this is an agent advertisement.
- ✓ ***Length:*** Number of bytes in the extension, excluding the Type and Length fields. The value is (6 + *4N)*, where N is the number of care-of addresses advertised.
- ✓ ***Sequence Number:*** The count of agent advertisement messages sent since the agent was initialized.
- ✓ ***Lifetime:*** The longest lifetime, in seconds, that this agent is willing to accept a registration request from a mobile node.
- ✓ ***R:*** Registration with this foreign agent is required (or another foreign agent on this network). Even those mobile nodes that have already acquired a care-of address from this foreign agent must re-register.
- ✓ **B:** Busy. The foreign agent will not accept registrations from additional mobile nodes.
- ✓ **H:** This agent offers services as a home agent on this network.
- ✓ **F:** This agent offers services as a foreign agent on this network.
- ✓ **M:** This agent can receive tunneled IP datagrams that use minimal encapsulation.
- ✓ **G:** This agent can receive tunneled IP datagrams that use GRE encapsulation.
- ✓ **r:** reserved.
- ✓ **T:** Foreign agent supports reverse tunneling.

- ✓ **Care-Of Address:**
  - The care-of address or addresses supported by this agent on this network.
  - There must be at least one such address if the F bit is set. There may be multiple addresses.

Optional prefix-length extension

- There may also be an optional **prefix-length extension** following the advertisement extension.
- This extension ***indicates the number of bits in the router's address*** that define the ***network number***.
- The mobile node uses this information ***to compare the network portion*** of its own IP address with the network portion of the router.

The fields are as follows:

- ✓ **Type:** 19, indicates that this is a prefix-length advertisement.
- ✓ **Length:** N, where N is the value of the ***Num Addrs*** field in the ICMP router advertisement portion of this ICMP message. In other words, this is the number of router addresses listed in this ICMP message.
- ✓ **Prefix Length:** The number of bits defines the ***network number*** of the corresponding router address listed in the ICMP router advertisement portion of this message. The number of Prefix Length fields matches the number of router address fields (N).

Agent Solicitation: Foreign agents are expected to issue agent advertisement messages periodically. If a mobile node needs agent information immediately, it can issue an ICMP router solicitation message. Any agent receiving this message will then issue an agent advertisement.

Move Detection As was mentioned, a mobile node may move from one network to another due to some handoff mechanism, without the IP level being aware of it.

- The agent discovery process is intended to enable the agent to detect such a move.

The agent may use one of two algorithms for this purpose:

- ✓ Use of ***lifetime field:*** When a mobile node receives an agent advertisement from a foreign agent and it records the lifetime field as a timer.
  - If the timer expires before the mobile node receives another agent advertisement from the agent, then the node assumes that it has lost contact with that agent.

- If, in the meantime, the mobile node has received an agent advertisement from another agent and that advertisement has not yet expired, the mobile node can register with this new agent.
  - Otherwise, the mobile node should use agent solicitation to find an agent.

✓ Use of ***network prefix:***

- The mobile node checks whether any newly received agent advertisement is on the same network as the node's current care-of address.
- If it is not, the mobile node assumes that it has moved and may register with the agent whose advertisement the mobile node has just received.

Co-Located Addresses

- The discussion so far has involved the care-of address is an IP address for the foreign agent.
- This foreign agent will receive datagrams at this care-of address, intended for the mobile node, and then forward them across the foreign network to the mobile node.

- In some cases, a mobile node may move to a network that has no foreign agents or on which all foreign agents are busy.
- As an alternative, the mobile node may act as its own foreign agent by using a co-located care-of address.

- A ***co-located care-of address*** is an ***IP address obtained by the mobile node*** that is associated with the mobile node's ***current interface to a network***.

- Two ways to obtan ***Co-Located Addresses:***
  - ✓ ***Dynamically <u>acquire</u> a temporary IP address through an Internet service*** such as DHCP (Dynamic Host Configuration Protocol).
  - ✓ ***Co-located address may be <u>owned</u> by the mobile node as a long-term address*** for use only while visiting a given foreign network.

2.1.5 Registration

2. Explain the process of Registration and authentication in Mobile IP.

Once a mobile node is on a foreign network and has acquired a care-of address, it needs to ***alert a home agent*** on its home network and ***request that the home agent forward its IP traffic***.

The registration process involves four steps:

1. The mobile node ***requests the forwarding service*** by sending a registration request to the foreign agent that the mobile node wants to use.
2. The ***foreign agent relays*** this request to ***the mobile node's home agent***.
3. The ***home agent either accepts or denies*** the request and sends a ***registration reply to the foreign agent***.
4. The ***foreign agent relays this reply to the mobile node***.

If the mobile node is using a co-located care-of address, then it registers directly with its home agent, rather than going through a foreign agent.

The registration operation uses two types of messages, carried in UDP segments (Figure 2.4).

The registration request message consists of the following fields:

- ✓ **Type**: 1, indicates that this is a registration request.
- ✓ **S**: Simultaneous bindings. The mobile node is requesting that the home agent retain its prior mobility bindings.
  - When simultaneous bindings are in effect.
    - the home agent will forward multiple copies of the IP datagram,
    - one to each care-of address currently registered for this mobile node.
  - Multiple simultaneous bindings can be useful in wireless handoff situations, to improve reliability.
- ✓ **B**: ***Broadcast datagrams***. Indicates that the mobile node would like to receive copies of broadcast datagram.
- ✓ **D**: ***Decapsulation by mobile node***. The mobile node is using a co-located care-of address and will decapsulate its own tunneled IP datagrams.
- ✓ **M**: Indicates that the home agent should use minimal encapsulation.
- ✓ **G**: Indicates that the home agent should use GRE encapsulation.
- ✓ **r**: Reserved.
- ✓ **T**: Reverse tunneling requested.
- ✓ **x**: Reserved.

- ✓ **Lifetime**: The number of seconds before the registration is considered expired. A ***value of zero*** is a ***request for de-registration***.

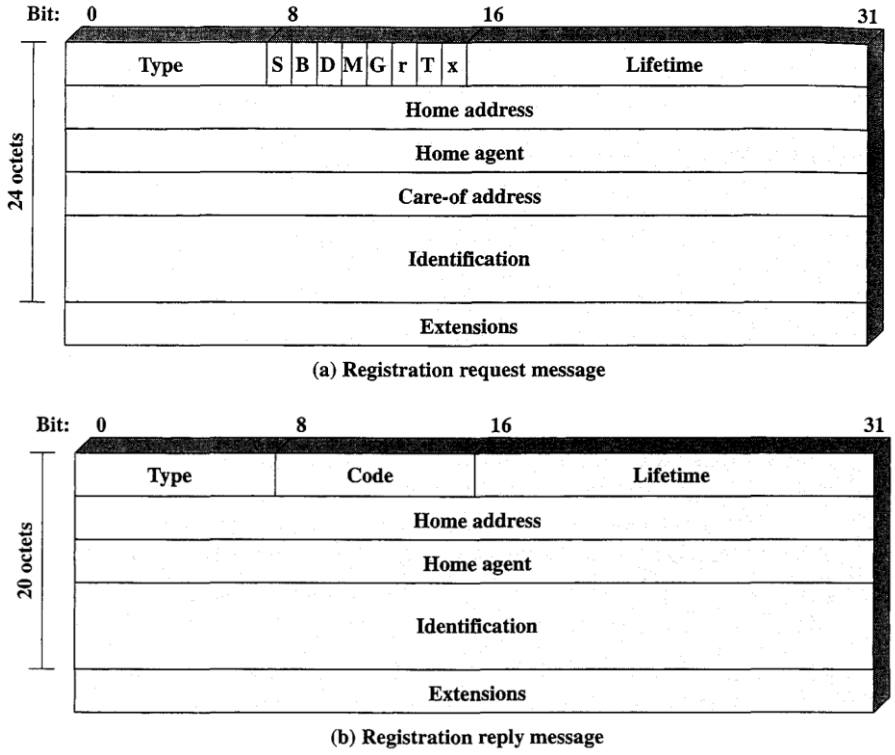


Figure 2.4 Mobile IP Registration Messages

- ✓ **Home Address:**
  - The home IP ***address of the mobile node***.
  - The home agent can expect to receive IP datagrams with this as a destination address, and must forward those to the care-of address.
- ✓ **Home Agent:**
  - The IP address of the ***mobile node's home agent***.
  - This informs the foreign agent of the address to which this request should be relayed.
- ✓ **Care-Of Address:**
  - The IP address at this ***end of the tunnel***.
  - The home agent should forward **IP** datagrams that it receives with mobile node's home address to this destination address.
- ✓ **Identification:**
  - A 64-bit number generated by the mobile node.
  - It is used to ***match registration requests to registration replies*** and for ***security purposes***.
- ✓ **Extensions:**
  - The only extension so far defined is the authentication extension.

The **registration reply message** consists of the following fields:

- ✓ **Type:** 3, indicates that this is a registration reply.
- ✓ **Code:** Indicates result of the registration request (Table 2.2).
- ✓ **Lifetime:** A value of zero indicates that the mobile node has been de-registered.
- ✓ **Home Address:** The home **IP** address of the mobile node.
- ✓ **Home Agent: The IP** address of the mobile node's home agent.
- ✓ **Identification:** A 64-bit number used for matching registration requests to registration replies.
- ✓ **Extensions:** The only extension so far defined is the authentication extension, explained subsequently.

Table 2.2 Code Values for a Mobile IP Registration Reply

Registration Successful	
0	registration accepted
1	registration accepted, but simultaneous mobility bindings unsupported
Registration Denied by the Home Agent	
128	reason unspecified
129	administratively prohibited
130	insufficient resources
131	mobile node failed authentication
132	foreign agent failed authentication
133	registration Identification mismatch
134	poorly formed Request
135	too many simultaneous mobility bindings
136	unknown home agent address
Registration Denied by the Foreign Agent	
64	reason unspecified
65	administratively prohibited
66	insufficient resources
67	mobile node failed authentication
68	home agent failed authentication
69	requested Lifetime too long
70	poorly formed Request
71	poorly formed Reply
72	requested encapsulation unavailable
73	requested Van Jacobson compression unavailable
77	invalid care-of address
78	registration timeout
80	home network unreachable (ICMP error received)
81	home agent host unreachable (ICMP error received)
82	home agent port unreachable (ICMP error received)
88	home agent unreachable (other ICMP error received)

Securing the Registration Procedure: A key concern with the registration procedure is security. Mobile IP is designed to resist two types of attacks:

1. A node may pretend to be a foreign agent and send a registration request to a home agent so as to divert traffic intended for a mobile node to itself.
2. A malicious agent may replay old registration messages, effectively cutting the mobile node from the network.

The technique that is used to protect against such attacks involves the use of message authentication and the proper use of the identification field of the registration request and reply messages (Figure 2.4).

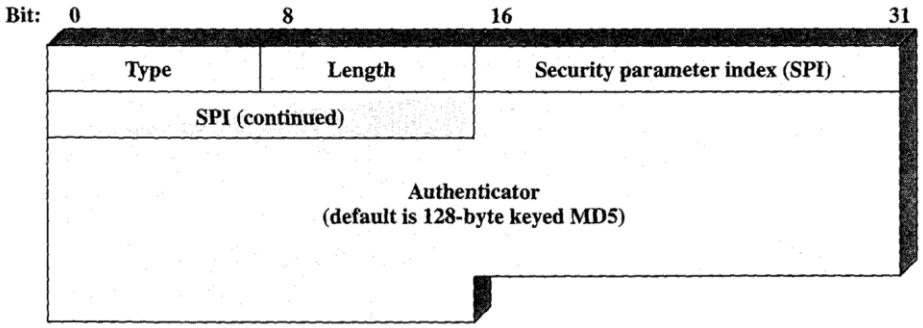


Figure 2.5 Mobile IP Authentication Extension

For purposes of message authentication, each registration request and reply contains an authentication extension (Figure 2.5) with the following fields:

- ***Type:*** Used to designate the type of this authentication extension.
- ***Length:*** 4 plus the number of bytes in the authenticator.
- ***Security Parameter Index (SPI):***
  - An index that identifies a security context between a pair of nodes.
  - Configuration: The two nodes share a secret key and parameters relevant to this association (e.g., authentication algorithm).
- .**Authenticator:**
  - ✓ A code used to authenticate the message.
  - ✓ The sender inserts this code into the message using a shared secret key.
  - ✓ The receiver ***uses the code*** to *ensure that the message has not been* ***altered or delayed***.
  - ✓ The authenticator protects the entire registration request or reply message, any extensions prior to this extension, and the type and length fields of this extension.

The default authentication algorithm is HMAC-MD5, defined in RFC 2104, which produces a 128-bit message digest. HMAC-MD4 is an example of what is known as a ***keyed hash code***.

Three types of authentication extensions are defined:

- **Mobile-home:**
  - It must be present.
  - It provides for ***authentication of the registration messages*** between ***the mobile node and the home agent***.
- **Mobile-foreign:**
  - The extension may be present when a security association exists between the mobile node and the foreign agent.

- The foreign agent will strip this extension off before ***relaying a request message to the home agent*** and ***add this extension to a reply message coming from a home agent***.

- **Foreign-home:**
  - The extension may be present when a security association exists between the foreign agent and the home agent.

2.1.6 Tunneling

6. State the entities and terminologies used in Mobile IP along with tunneling and also explain the three types of encapsulation mechanisms used in triangle routing	**(16m)**	**Apr 2017**
7. Explain how tunneling works in general and especially for mobile IP using IP in IP, minimal and generic routing encapsulation respectively. Discuss the advantages and disadvantages of these three methods.	**(16m)**	**Nov 2017**
8. How the Tunneling and IP – in – IP encapsulation occur in the mobile IP?	**(13m)**	**May 2019**

- Once a mobile node is registered with a home agent, the home agent must be able to capture IP datagrams sent to the mobile node's home address so that these datagrams can be forwarded via tunneling.
- The standard references ARP (Address Resolution Protocol) is a possible mechanism.
- The home agent needs to inform other nodes on the same network (the home network) that IP datagrams with a destination address of the mobile node in question should be delivered (at the link level) to this agent.
- In effect, the home agent steals the identity of the mobile node in order to capture packets destined for that node that are transmitted across the home network.

- For example, suppose that R_3 in Figure 2.6 is acting as the home agent for a mobile node that is attached to a foreign network elsewhere on the Internet.
- That is, there is a host H whose home network is LAN Z that is now attached to some foreign network.
- If host D has traffic for H, it will generate an IP datagram with H's home address in the IP destination address field.

- The IP module in D recognizes that this destination address is on LAN Z and so passes the datagram to the link layer with instructions to deliver it to a particular MAC-level address on Z.

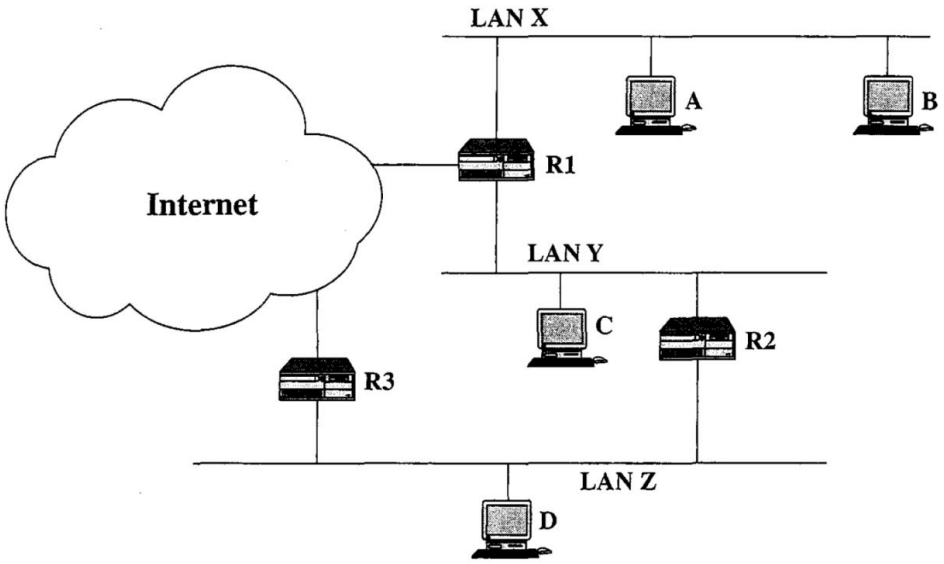


Figure 2.6 A Simple Internetworking Example

- Prior to this time, R3 has informed the IP layer at D that datagrams destined for that particular address should be sent to R3.
- Thus, D inserts the MAC address of R3 in the destination MAC address field of the outgoing MAC frame.
- Similarly, if an IP datagram with the mobile node's home address arrives at router R2, it recognizes that the destination address is on LAN Z and will attempt to deliver the datagram to a MAC-level address on Z.
- Again, R2 has previously been informed that the MAC-level address it needs corresponds to R3.

- For traffic that is routed across the Internet and arrives at R3 from the Internet, R3 must simply recognize that for this destination address, the datagram is to be captured and forwarded.
- To forward an IP datagram to a care-of address, the home agent puts the entire IP datagram into an outer IP datagram.
- This is a form of encapsulation, just as placing an IP header in front of a TCP segment encapsulates the TCP segment in an IP datagram.

2.1.7 Encapsulation

- Three options for encapsulation are allowed for Mobile IP:
  - ✓ **IP-within-IP encapsulation:** This is the simplest approach, defined in RFC 2003.
  - ✓ **Minimal encapsulation:** This approach involves fewer fields, defined in RFC 2004.
  - ✓ **Generic routing encapsulation (GRE):** This is a generic encapsulation procedure that was developed prior to the development of Mobile IP, defined in RFC 1701.

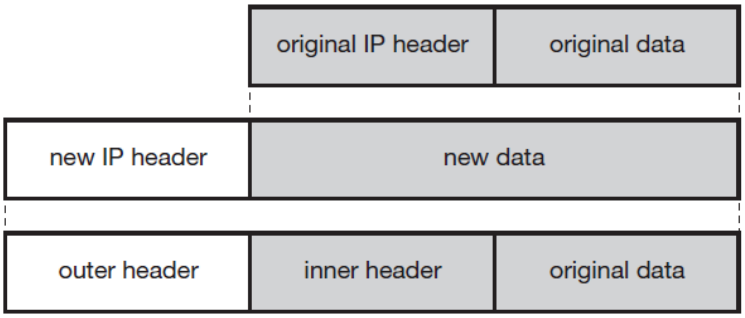


Fig 2.7a IP encapsulation

IP-within-IP Encapsulation

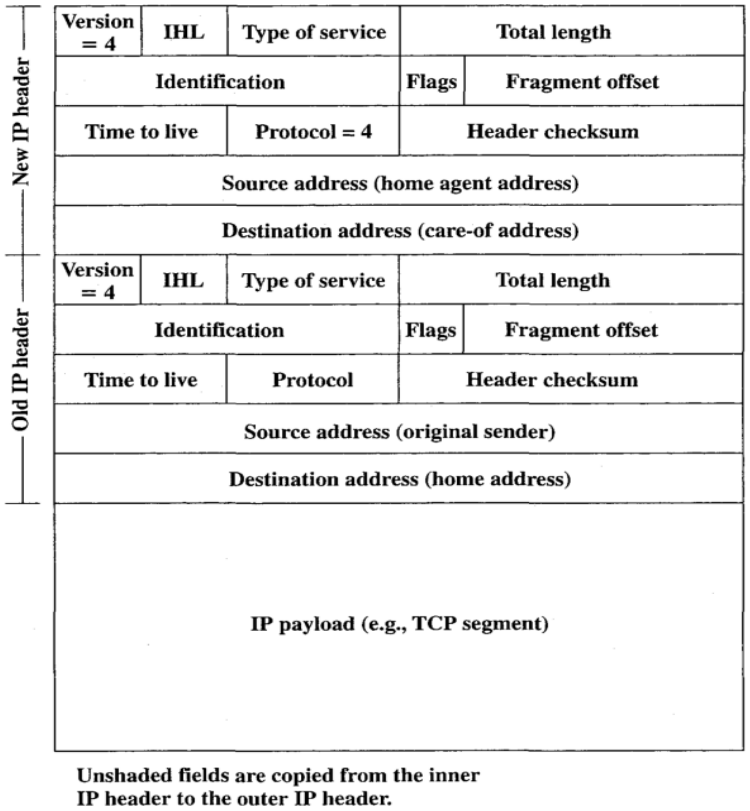
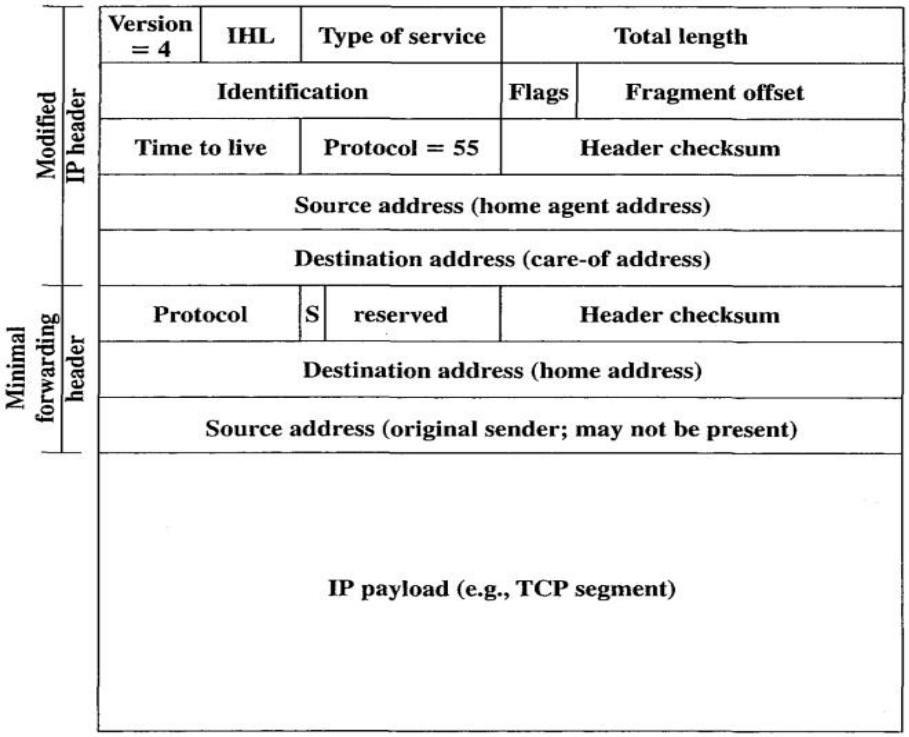


Figure 2.7b IP-in-IP encapsulation

- With this approach, the entire IP datagram becomes the payload in a new IP datagram (Figure 2.7b).
- The inner, original IP header is unchanged except to decrement TTL by 1.
- The outer header is a full IP header. Two fields (indicated as unshaded in the figure) are copied from the inner header:
- The version number is 4, which is the protocol identifier for IPv4, and the type of service requested for the outer IP datagram is the same as that requested for the inner IP datagram.
- In the ***inner IP header***, the source address refers to the host that is sending the original datagram, and the destination address is the home address of the intended recipient.
- In the ***outer IP header***, the source and destination addresses refer to the entry and exit points of the tunnel.
- Thus, the source address typically is the IP address of the home agent, and the destination address is the care-of address for the intended destination.

Minimal Encapsulation

- Minimal encapsulation results in ***less overhead*** and can be used if the mobile node, home agent, and foreign agent all agree to do so.



Unshaded fields in the inner IP header are copied from the original IP header. Unshaded fields in the outer IP header are modified from the original IP header.

Figure 2.7c Minimal encapsulation

- With minimal encapsulation, the new header is inserted between the original IP header and the original IP payload (Figure 2.7b). It includes the following fields:
  - ✓ ***Protocol:*** Copied from the destination address field in the original IP header. This field ***identifies the protocol type of the original IP payload and thus identifies the type of header*** than begins the original IP payload.
  - ✓ ***S:*** If 0, the original source address is not present, and the length of this header is 8 octets. If 1, the original source address is present, and the length of this header is 12 octets.
  - ✓ ***Header Checksum:*** Computed over all the fields of this header.
  - ✓ ***Original Destination Address***: Copied from the destination address field in the original IP header.
  - ✓ ***Original Source Address:***
    - Copied from the source address field in the original IP header.
    - This field is present only if the S bit is 1.
    - The field is not present if the encapsulator is the source of the datagram (i.e., the datagram originates at the home agent).

The following fields in the original IP header are modified to form the new outer IP header:

- ✓ ***Total Length:*** Incremented by the size of the minimal forwarding header (8 or 12).
- ✓ ***Protocol:*** 55; this is the protocol number assigned to minimal IP encapsulation.
- ✓ ***Header Checksum:*** Computed over all the fields of this header; because some of the fields have been modified, this value must be recomputed.
- ✓ ***Source Address:*** The IP address of the encapsulator, typically the home agent.
- ✓ ***Destination Address:***
  - The IP address of the exit point of the tunnel.
  - This is the care-of address and may either be the IP address of the foreign agent or the IP address of the mobile node (in the case of a co-located care-of address).

- ✓ The processing for minimal encapsulation is as follows. The encapsulator (home agent) prepares the encapsulated datagram with the format of Figure 2.7c.
- ✓ This datagram is now suitable for tunneling and is delivered across the Internet to the care-of address.
- ✓ At the care-of address, the fields in the minimal forwarding header are restored to the original IP header and the forwarding header is removed from the datagram.
- ✓ The total length field in the IP header is decremented by the size of the minimal forwarding header (8 or 12) and the header checksum field is recomputed.

Generic routing encapsulation

While IP-in-IP encapsulation and minimal encapsulation work only for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP.

- ✓ **Generic routing encapsulation** (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

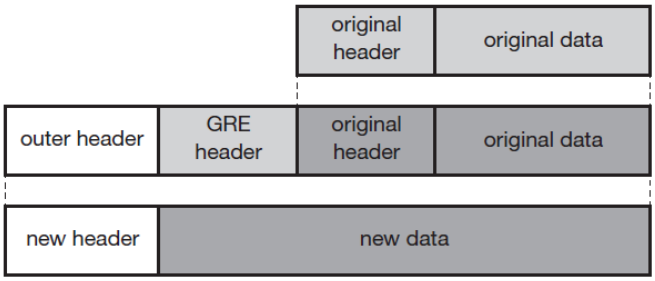


Fig 2.8a Generic routing encapsulation

Figure 2.8a shows this procedure.

- ✓ The packet of one protocol suite with the original packet header and data is taken and a new GRE header is prepended.
- ✓ Together this forms the new data part of the new packet. Finally, the header of the second protocol suite is put in front.

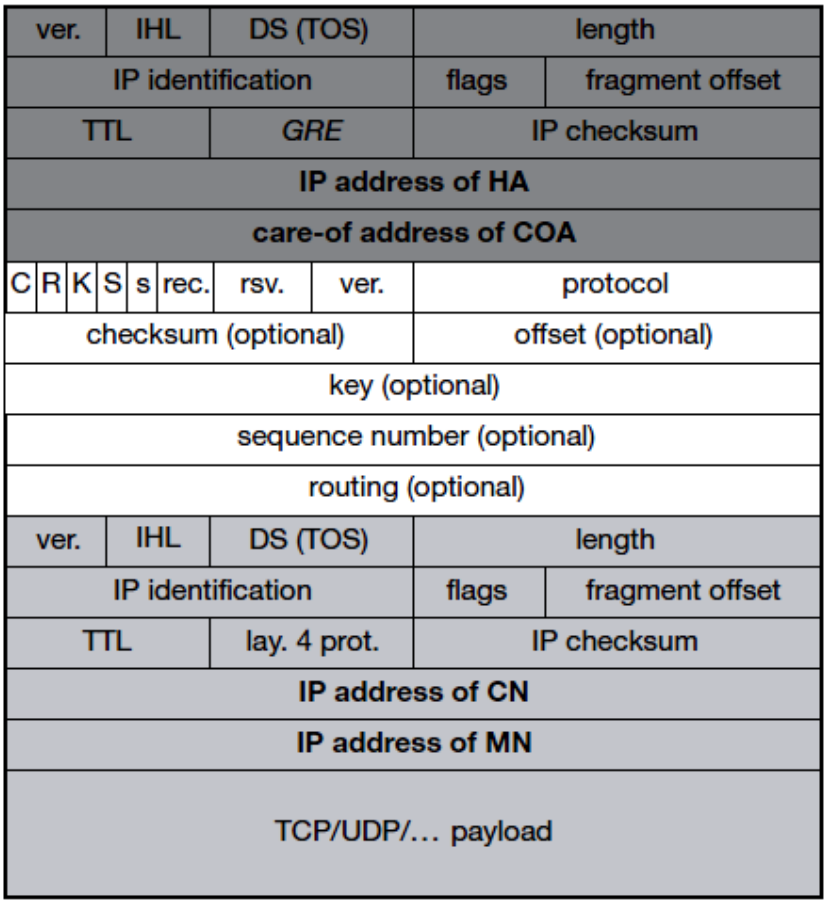


Fig 2.8b Protocol fields for GRE according to RFC 1701

Figure 2.8b shows on the left side the fields of a packet inside the tunnel between home agent and COA using GRE as an encapsulation scheme according to RFC 1701.

- ✓ The outer header is the standard IP header with HA as source address and COA as destination address. The protocol type used in this outer IP header is 47 for GRE.
- ✓ The other fields of the outer packet, such as TTL and TOS, may be copied from the original IP header. However, the TTL must be decremented by 1 when the packet is decapsulated to prevent indefinite forwarding.
- ✓ The GRE header starts with several flags indicating if certain fields are present or not. A minimal GRE header uses only 4 bytes; nevertheless, GRE is flexible enough to include several mechanisms in its header.
- ✓ The **C** bit indicates if the checksum field is present and contains valid information. If **C** is set, the **checksum** field contains a valid IP checksum of the GRE header and the payload.

- ✓ **R:** The **R** bit indicates if the offset and routing fields are present and contain valid information.
- ✓ **Offset *(Optinal)*:** The **offset** represents the offset in bytes for the first source **routing** entry.

- ✓ **Routing field *(Optimal)*:** The ***routing field***, if present, has a variable length and contains fields for source routing.
- ✓ **C** and **R**: If the ***C*** bit is set, the ***offset field is also present*** and, vice versa, if the ***R*** bit is set, the ***checksum field*** must be present. The only reason for this is to align the following fields to 4 bytes.
- ✓ ***Checksum field (Optimal):*** The ***checksum field*** is valid only if C is set.
- ✓ ***Offset field (Optimal):*** The offset field is valid only if R is set respectively.
- ✓ ***Key (Optimal)****:* GRE also offers a **key** field which may be used for authentication. If this field is present, the **K** bit is set. However, the authentication algorithms are not further specified by GRE.
- ✓ ***S (Sequence number):***
    - o It indicates if the **sequence** number field is present.
    - o If the **S** bit is set, strict source routing is used.
    - o Sequence numbers may be used by a decapsulator ***to restore packet order***.
    - o This can be important, if a protocol guaranteeing in-order transmission is encapsulated and transferred using a protocol which does not guarantee in-order delivery, e.g., IP.
    - o Now the decapsulator at the tunnel exit must restore the sequence to maintain the characteristic of the protocol.

- ✓ ***Recursion Control:***
    - ▪ The **recursion control** field ***(rec.)*** is an important field.
    - ▪ It distinguishes GRE from IP-in-IP and minimal encapsulation.
    - ▪ This field represents a ***counter that shows the number of allowed recursive encapsulations***.
    - ▪ When the packet arrives at an encapsulator, it checks whether this field equals zero.
    - ▪ If the field is not zero, additional encapsulation is allowed – the packet is encapsulated and the field decremented by one.
    - ▪ Otherwise the packet will most likely be discarded.
    - ▪ This mechanism ***prevents indefinite recursive encapsulation.***
    - ▪ Recursive encapsulation occurs in other schemes if tunnels are set up improperly (e.g., several tunnels forming a loop).
    - ▪ The default value of this field should be 0, thus allowing only one level of encapsulation.

- ***Reseved (rsv.):*** The following **reserved** fields must be zero and are ignored on reception.
- ✓ ***Version (ver.):*** The **version** field contains 0 for the GRE version.
- ✓ ***Protocol:*** The following 2 byte **protocol** field represents the protocol of the packet following the GRE header.

- ✓ Several values have been defined, e.g., 0 × 6558 for transparent Ethernet bridging using a GRE tunnel.
- ✓ In the case of a mobile IP tunnel, the protocol field contains 0 × 800 for IP. T
- ✓ The standard header of the original packet follows with the source address of the correspondent node and the destination address of the mobile node.

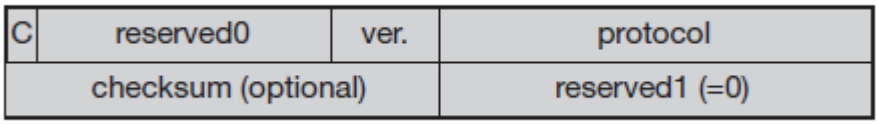


Fig. 2.8c Protocol fields for GRE according to RFC 2784

Figure 2.8c shows the simplified header of GRE following RFC 2784, which is a more generalized version of GRE compared to RFC1701.

- ✓ This version does not address mutual encapsulation and ignores several protocol-specific nuances on purpose. The field **C** indicates again if a checksum is present.
- ✓ The next 5 bits are set to zero, then 7 reserved bits follow. The **version** field contains the value zero.
- ✓ The **protocol** type, again, defines the protocol of the payload following RFC 3232.
- ✓ If the flag C is set, then **checksum** field and a field called reserved1 follows. The latter field is constant zero set to zero follow.
- ✓ RFC 2784 deprecates several fields of RFC 1701, but can interoperate with RFC 1701-compliant implementations.

1. **Imagine the following scenario. A Japanese and a German meet at a conference on Hawaii. Both want to use their laptops for exchanging data, both run mobile IP for mobility support. Explain the optimizations used in this mobile IP networks. [Nov 2018]**

Optimizations

Imagine the following scenario.

- A Japanese and a German meet at a conference on Hawaii. Both want to use their laptops for exchanging data, both run mobile IP for mobility support
- If the Japanese sends a packet to the German, his computer sends the data to the HA of the German, i.e., from Hawaii to Germany.
- The HA in Germany now encapsulates the packets and tunnels them to the COA of the German laptop on Hawaii.
- ✓ The packets have to travel around the world.
- ✓ This inefficient behavior of a non optimized mobile IP is called **triangular routing**.

Disadvantages:

- ✓ Unnecessary overheads.
- ✓ To optimize the route is to inform the correspondent node of the current location of the mobile node.
- ✓ Correspondent node can learn the location by caching it in a binding cache.
- ✓ Binding cache is a part of routing tabe.

The optimized mobile IP protocol needs four additional messages.

- **Binding request:**
  - Any node that wants to know the current location of an MN can send a binding request to the HA.
  - The HA can check if the MN has allowed dissemination of its current location.
  - If the HA is allowed to reveal the location it sends back a binding update.
- **Binding update:**
  - This message sent by the HA to CNs reveals the current location of an MN.
  - The message contains the fixed IP address of the MN and the COA.
  - The binding update can request an acknowledgement.
- **Binding acknowledgement:** If requested, a node returns this acknowledgement after receiving a binding update message.
- **Binding warning:** If a node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends a binding warning.

- The warning contains MN's home address and a target node address, i.e., the address of the node that has tried to send the packet to this MN.
- The recipient of the warning then knows that the target node could benefit from obtaining a fresh binding for the MN.

- The recipient can be the HA, so the HA should now send a binding update to the node that obviously has a wrong COA for the MN.

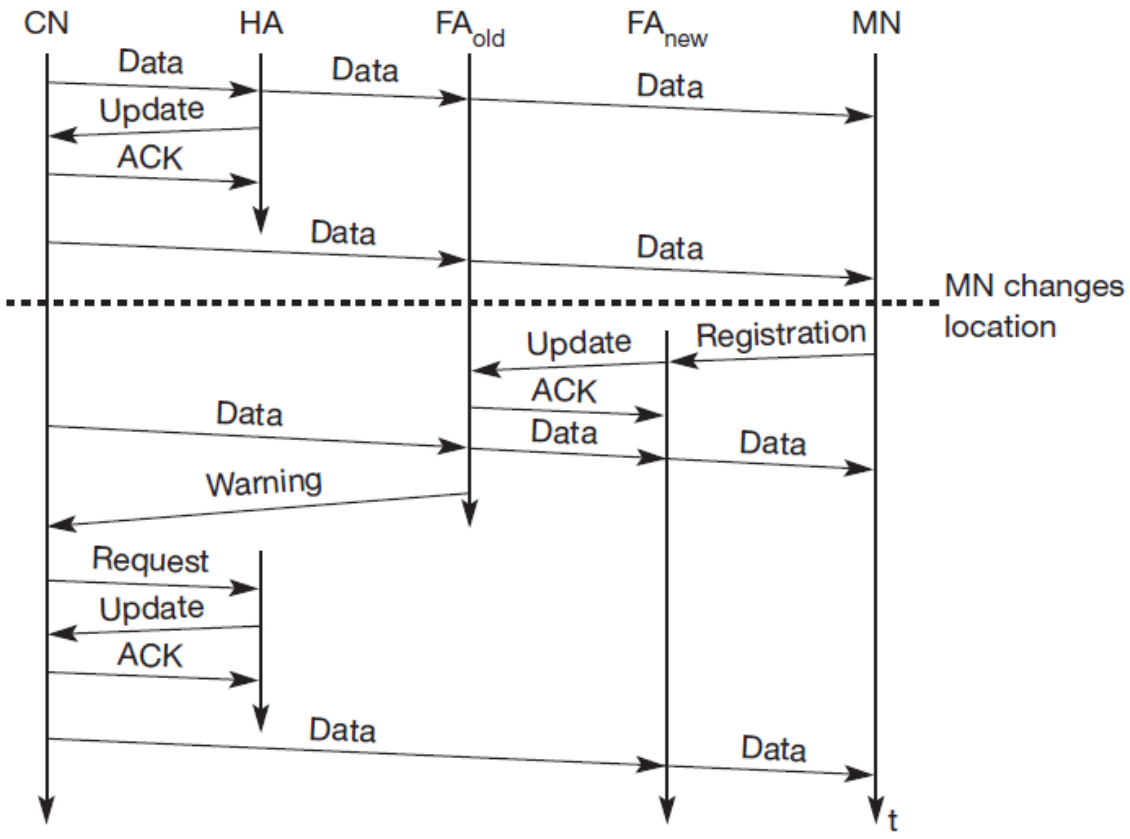


Fig 2.9 Change of the foreign agent with an optimized mobile IP

Figure 2.9 explains these additional four messages together with the case of an MN changing its FA.

- The CN can request the current location from the HA. If allowed by the MN, the HA returns the COA of the MN via an update message.
- The CN acknowledges this update message and stores the mobility binding. Now the CN can send its data directly to the current foreign agent FAold. FAold forwards the packets to the MN.
- This scenario shows a COA located at an FA. Encapsulation of data for tunneling to the COA is now done by the CN, not the HA.
- The MN might now change its location and register with a new foreign agent, FAnew. This registration is also forwarded to the HA to update its location database. Furthermore, FAnew informs FAold about the new registration of MN.
- MN's registration message contains the address of FAold for this purpose.

- Passing this information is achieved via an update message, which is acknowledged by FAold.
- Registration replies are not shown in this scenario. Without the information provided by the new FA, the old FA would not get to know anything about the new location of MN.
- In this case, CN does not know anything about the new location, so it still tunnels its packets for MN to the old FA, FAold.
- This FA now notices packets with destination MN, but also knows that it is not the current FA of MN.
- FAold might now forward these packets to the new COA of MN which is FAnew in this example.
- This forwarding of packets is another optimization of the basic Mobile IP providing **smooth handovers**.

- Without this optimization, all packets in transit would be lost while the MN moves from one FA to another.
- With TCP as the higher layer protocol this would result in severe performance degradation.
- To tell CN that it has a stale binding cache, FAold sends, in this example, a binding warning message to CN. CN then requests a binding update. (The warning could also be directly sent to the HA triggering an update).
- The HA sends an update to inform the CN about the new location, which is acknowledged. Now CN can send its packets directly to FAnew, again avoiding triangular routing.
- Unfortunately, this optimization of mobile IP to avoid triangular routing causes several security problems (e.g., tunnel hijacking) as discussed in Montenegro (1998).
- Not all users of mobile communication systems want to reveal their current 'location' (in the sense of an IP subnet) to a communication partner.

Reverse tunnelling

2. Explain in detail about reverse tunnelling.

- At first glance, the return path from the MN to the CN shown in Figure 2.1.
- The MN can directly send its packets to the CN as in any other standard IP situation.
- The destination address in the packets is that of CN.
- But there are several severe problems associated with this simple solution.
  - **Firewalls:** Almost all companies and many other institutions secure their internal networks (intranet) connected to the internet with the help of a firewall.
    - All data to and from the intranet must pass through the firewall.

- Besides many other functions, firewalls can be set up to filter out malicious addresses from an administrator's point of view.
- Quite often firewalls only allow packets with topologically correct addresses to pass.
- This provides at least a first and simple protection against misconfigured systems of unknown addresses.
- Firewalls often filter packets coming from outside containing a source address from computers of the internal network.
- This avoids other computers that could use internal addresses and claim to be internal computers.
- The **network address translation** is used by many companies to hide internal resources (routers, computers, printers etc.) and to use only some globally available addresses.

- **Multi-cast:** Reverse tunnels are needed for the MN to participate in a multicast group.
  - While the nodes in the home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel.
  - The foreign network might not even provide the technical infrastructure for multi-cast communication (multi-cast backbone, Mbone).
- **TTL:** Consider an MN sending packets with a certain TTL while still in its home network.
  - The TTL might be low enough so that no packet is transmitted outside a certain region.
  - If the MN now moves to a foreign network, this TTL might be too low for the packets to reach the same nodes as before.
  - Mobile IP is no longer transparent if a user has to adjust the TTL while moving.
  - A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from the foreign to the home network.

2.2 IPv6

3. Discuss in detail about IPv6. (or)

Analyse all possible solutions to be adopted for giving mobility support in the network layer such that both delay constraints along with throughput levels are achieved. (Apr / May 2019)

Explain the features of IPV6. Illustrate the features, for a Mobile IP session initiation protocol. [Nov 2019]

2.2.1 Features of IPv6:

- ✓ One issue is security with regard to authentication, which is now a required feature for all IPv6 nodes.
- ✓ Every IPv6 node masters address auto configuration – the mechanisms for acquiring a COA are already built in.
- ✓ Neighbour discovery is a mechanism mandatory for every node, special foreign agents are no longer needed to advertise services.
- ✓ The ***neighbour 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 the MN can send its current COA directly to the 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 the old router encapsulates all incoming packets for the MN and forwards them to the new COA.
- ✓ 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. The MN itself has to be able to decapsulate 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. However, IPv6 does not solve any firewall or privacy problems.

2.2.2 IP micro-mobility support

- ➢ Mobile IP exhibits several problems regarding the duration of handover and the scalability of the registration procedure.
- ➢ Assuming a large number of mobile devices changing networks quite frequently, a high load on the home agents as well as on the networks is generated by registration and binding update messages.
- ➢ IP micro-mobility protocols can complement mobile IP by offering fast and almost seamless handover control in limited geographical areas.

Consider a client arriving with his or her laptop at the customer's premises.

- ➢ The home agent only has to know an entry point to the customer's network, not the details within this network.
- ➢ The entry point acts as the current location.
- ➢ Changes in the location within the customer's network should be handled locally to minimize network traffic and to speed-up local handover.

Principle: The Home Agent needs to be informed only when the node changes a region. Three IP micro mobility approaches are:

1. Cellular IP
2. Hawaii
3. Hierarchical mobile IPv6

2.2.3 Cellular IP

- Cellular IP provides local handovers without renewed registration.
- This is achieved by installing a single **cellular IP gateway (CIPGW)** for each domain
- This CIPGW acts as a foreign agent, to the outside world.
- Inside the cellular IP domain, all nodes collect routing information for accessing MNs.
- The routing information is based on the origin of packets sent by the MNs towards the CIPGW.
- Soft handovers are achieved by allowing simultaneous forwarding of packets.
- These packets were intended for a mobile node along multiple paths.
- A mobile node moving between adjacent cells will be able to receive packets ***via both old and new base stations (BS).***

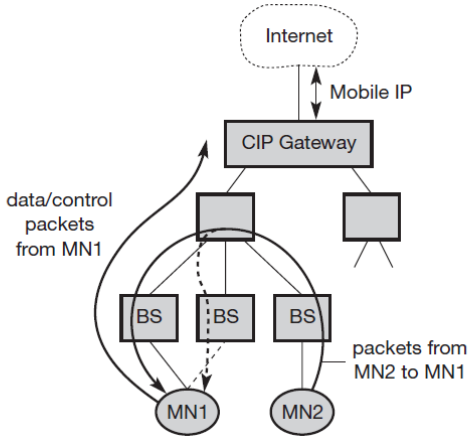


Fig 2.10 Basic architecture of cellular IP

- This ***Cellular IP approach*** has a simple and smart architecture and is mostly ***self-configuring***.
- The mobile IP tunnels are controlled more easily.
- Cellular IP requires changes to the basic mobile IP protocol.
- Cellular IP is not transparent to existing systems.
- The foreign network's routing tables are changed based on messages sent by mobile nodes.
- In enterprise scenarios which require basic communications security, this may not be acceptable.

Advantage

● ***Manageability:*** Cellular IP is mostly self-configuring, and integration of the CIPGW into a firewall would facilitate administration of mobility-related functionality.

Disadvantages

● ***Efficiency:*** Additional network load is induced by forwarding packets on multiple paths.

● ***Transparency:*** Changes to MNs are required.

● ***Security:***

- Routing tables are changed based on messages sent by mobile nodes.
- Additionally, all systems in the network can easily obtain a copy of all packets intended for an MN by sending packets with the MN's source address to the CIPGW.

2.2.4 Hawaii

- HAWAII (**H**andoff-**A**ware **W**ireless **A**ccess **I**nternet **I**nfrastructure, Ramjee, 1999) tries to keep micro-mobility support as transparent as possible for both home agents and mobile nodes (which have to support route optimization).
- Its concrete goals are
  - performance and reliability improvements, and
  - support for quality of service mechanisms.

- On entering an HAWAII domain, a mobile node obtains a co-located COA (step 1) and registers with the HA (step 2).
- Additionally, when moving to another cell inside the foreign domain, ***the MN sends a registration request to the new base station*** as to a foreign agent (step 3), thus mixing the concepts of co-located COA and foreign agent COA.
- The base station intercepts the registration request and sends out a handoff update message, which reconfigures all routers on the paths from the old and new base station to the so-called crossover router (step 4).

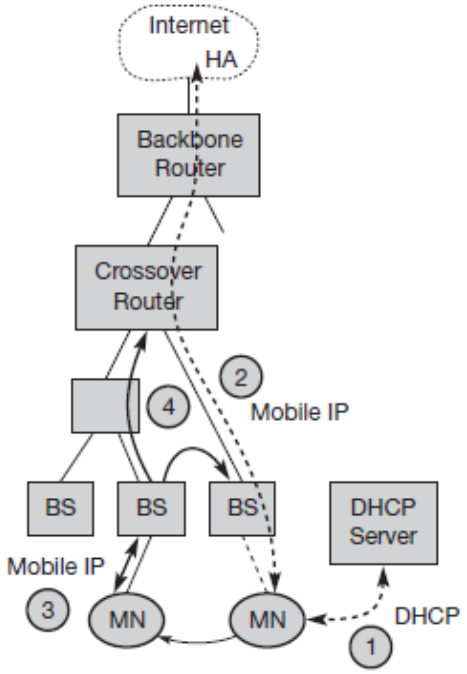


Fig: 2.11 Basic architecture of HAWAII

- When routing has been reconfigured successfully, the base station sends a registration reply to the mobile node, again as if it were a foreign agent.
- The use of challenge-response extensions for authenticating a mobile node is mandatory.
- In contrast to cellular IP, routing changes are always initiated by the foreign domain's infrastructure, and the corresponding messages could be authenticated, e.g., by means of an IPSec authentication header, reducing the risk of malicious rerouting of traffic initiated by bogus mobile hosts.
- HAWAII claims to be mostly transparent to mobile nodes.

Advantages

● ***Security:*** Challenge-response extensions are mandatory. In contrast to Cellular IP, routing changes are always initiated by the foreign domain's infrastructure.

● ***Transparency:*** HAWAII is mostly transparent to mobile nodes.

Disadvantages

● Security: There are no provisions regarding the setup of IPSec tunnels.

● Implementation: No private address support is possible because of co-located COAs.

2.2.4 Hierarchical mobile IPv6 (HMIPv6)

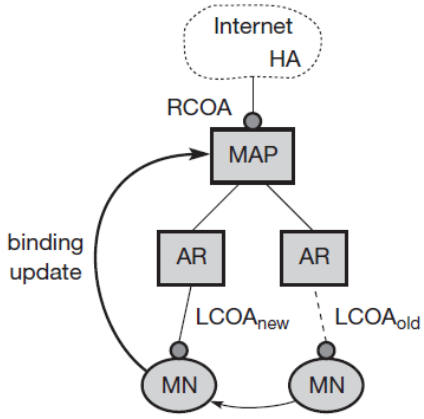


Fig: 2.12 Basic architecture of hierarchical mobile IP

- HMIPv6 provides micro-mobility support by installing a **mobility anchor point (MAP)**.
- This **MAP** is responsible for a certain domain.
- MAP acts as a local HA within this domain for visiting MNs.

- The MAP receives all packets on behalf of the MN.
- It encapsulates and forwards them directly to the MN's current address (link COA, **LCOA**).
- As long as an MN stays within the domain of a MAP, the globally visible COA (regional COA, **RCOA**) does not change.
- A MAP domain's boundaries are defined by the **access routers (AR)** advertising the MAP information to the attached MNs.
- A MAP assists with local handovers and maps RCOA to LCOA.
- MNs register their RCOA with the HA using a binding update.
- When a MN moves locally it must only register its new LCOA with its MAP. The RCOA stays unchanged.
- To support smooth handovers between MAP domains, an MN can send a binding update to its former MAP.

- It should be mentioned as a security benefit that mobile nodes can be provided with some kind of limited location privacy because LCOAs on lower levels of the mobility hierarchy can be hidden from the outside world.
- However, this applies only to micro mobility, that is, as long as the mobile node rests in the same domain. A MN can also send a binding update to a CN who shares the same link.

- This reveals its location but optimizes packet flow (direct routing without going through the MAP). MNs can use their RCOA as source address.
- The extended mode of HMIPv6 supports both mobile nodes and mobile networks.

Advantages

● ***Security:*** MNs can have (limited) location privacy because LCOAs can be hidden.

● ***Efficiency:*** Direct routing between CNs sharing the same link is possible

Disadvantages

● ***Transparency:*** Additional infrastructure component (MAP).

● ***Security:*** Routing tables are changed based on messages sent by mobile nodes. This ***requires strong authentication and protection against denial of service attacks***. Additional security functions might be necessary in MAPs

2.3 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

4. Explain the dynamic host configuration protocol.

1. The aim of DHCP is to simplify the installation and maintenance of network computer.
2. When a new computer is added to the network, DHCP can provide with all necessary information for integration.
3. DHCP provides IP address.

2.3.1 Configuration/Model

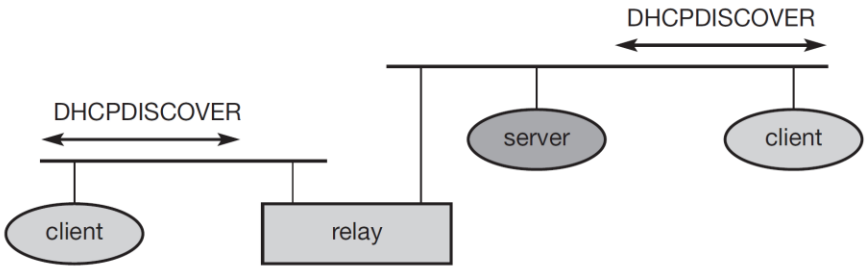


Figure Basic DHCP configuration

- DHCP is based on client server model.
- DHCP client sends a request To the server using DHCP Discover, which is broadcasted.
- The server responds.
- The relay is needed to forward across the interworking units to a server.

2.3.2 Client Initialization via DHCP

Initialization phase:

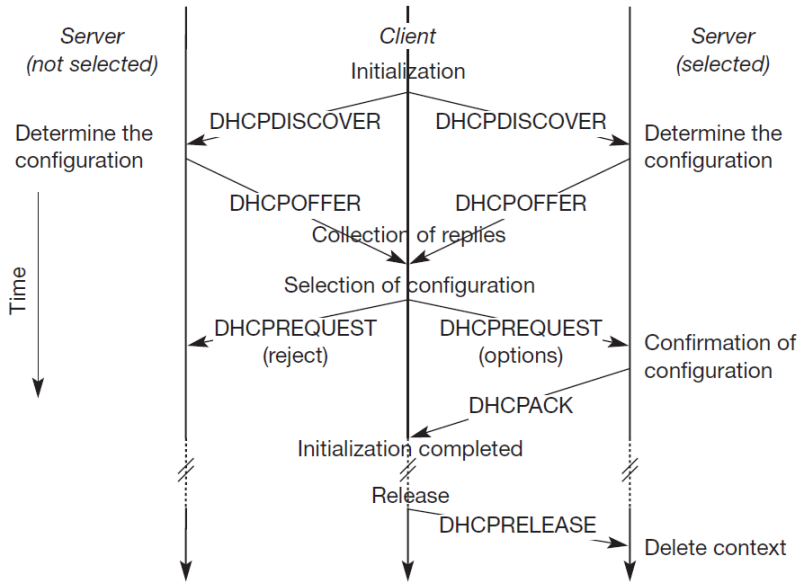


Figure Client initialization via DHCP

- The client broadcasts a DHCP discover to the subnet. There may be a relay to forward this broad.
- In the above figure two servers receive this broadcast and determine the configuration they can offer to the client.
- Server's reply to the client's request with DHCP OFFER and offers a list of configuration parameters.
- The client can choose one of the configurations offered.
- The client replies to the servers either accepting or rejecting using DHCP REQUEST for rejection the client sends DHCP REQUEST with a reject.
- The rejected server releases the reserved configuration.
- The accepted server sends back DHCP acknowledgement.

Release :

- When the client leaves the subnet, it should release the configuration received from the server.
- It does using the DHCP RELEASE.
- The period of service is fixed.
- If the client dose not reconfirm within that duration the server will free the configuration. Thus the DHCP supports the acquisition of COA for the mobile modes.

2.4 Mobile and Adhoc Networks

Adhoc Networks : The networks devices which are mobile and use wireless communication are called as Adhoc Networks.

Examples :

1. Instant Infrastructure: Unplanned events cannot rely on infrastructure. Infrastructure takes a longer time. Hence adhoc is used
2. Disaster Relief: During the time of hurricanes, flood the infrastructure break down. In military activities the Adhoc networks can be used.
3. Remote Areas: Setting up of infrastructure is costly in remote areas where the Adhoc Networks can be used.
4. Effectiveness: Services will be too expensive for certain applications where adhoc network can be used.

Concepts and terminologies of adhoc network

- At a certain time t_1 the topology looks as at the left side.
- Nodes N_1 to N_5 are connected.
- N_1 can receive info over a weak link from N_4 but N_4 can receive over a strong link from N_1.
- The links can be strong or weak depending upon the antenna characteristics or transmit power. N_1 cannot receive from N_2.

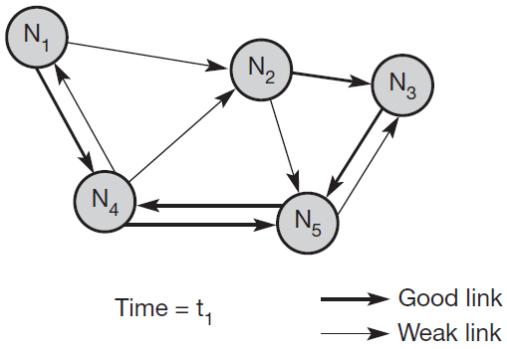


Figure: Example of Adhoc Network

- After some time at time t_2 the topology looks as at the right side.
- N_1 cannot receive from N_4 etc.
- Hence in adhoc wireless the topology changes.

Differences Between Wired and Wireless Network Related to Routing

1. ***Asymmetric Links:***

- ✓ Routing information for one direction is not the same in the other direction in wireless (i.e.) A Node can receive signal from B.
- ✓ This does not tell about the reverse connection between B to A (i.e.,) B to A link can be either strong/weak or No link routing also for the wired depends upon symmetric scenario.

2. ***Redundant Links:***
   - ✓ There is no control for the redundant link in the wireless.
   - ✓ But the network admin controls the redundancy in wired.
   - ✓ High redundancy leads to heavy computational overhead for routing tables.
3. ***Interference:***
   - ✓ In adhoc the links, come and go depending upon the transmission char, (i.e.) one transmission can interfere with other or overhear.
   - ✓ Interference has a disadvantage. If two close by nodes and forward, transmissions they might interfere and destroy each other.

Advantage:

- ✓ Node can learn the topology with the help of overhearing.

Dynamic Topology:

- ✓ The greatest problem for routing is due to dynamic topology.
- ✓ Frequent changes in the topology.
- ✓ Routing algorithm face many problems because they rely upon the topology.

2.4.1 Routing:

5. Discuss in detail about various routing algorithms.

- ➢ Routing is to find a path between source and destination and to forward the packets appropriately.

- ➢ Due to the above discussed difficulties in adhoc networks, the following observations are made:
  1. In adhoc environment the traditional routing algorithms cannot work because these algorithms cater to symmetric and static network topology.
  2. Routing cannot rely on layer three knowledge alone.
  3. Centralized approach will not work, because the network is in dynamic.
  4. Algorithms need to consider the limited battery power of the nodes.
  5. Nodes need to make local decision to forward the packets.
  6. Hooding is to done forward the packets. This mechanisms works when the load is low.

2.4.2 ROUTING ALGORITHMS

The routing algorithms discussed are :

1. Destination Sequence Distance Vector.
2. Dynamic Source Routing.
3. Other Routing Algorithm.

6. Expalin with neat diagram and example the destination sequence distance vector algorithm of AdHoc networks. [May 2018]
Explain the destination sequence distance vector routing protocol. Mention its features. (16m) [Nov 2018]

2.4.2.1 Destination Sequence Distance Vector (DSDV)

- This DSDV is an enhancement to Distance Vector Routing.
- **Distance Vector Concept:** Each node exchanges with its neighbor , the adjacency information (i.e.) hop count changes at one node in the network

To the existing also DSDV adds two concepts:

- Sequence Number: Each routing advertisements comes with a sequence number. The advertisement travel in many paths. The sequence number is used to see the order of advertisements.
- Damping Advantage: Avoid loops, when the topology remains the same.

Damping (breaking):

- Changes in the topology which is of short duration should not destabilize the routing.
- Advertisements containing such transient changes are not disseminated further. A node waits with destination if these changes are unstable.
- Waiting time depends on the time between the first and best announcement of a path to a destination.

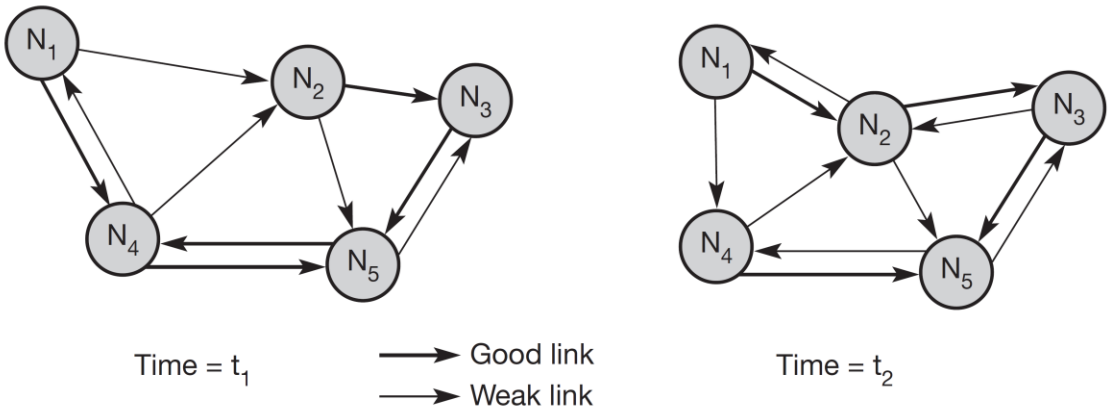


Figure Example ad-hoc network

The routing table is for N_1 is

Destination	Next hop	Metric	Sequence no.	Instal time
N_1	N_1	0	S_1–321	T_4–001
N_2	N_2	1	S_2–218	T_4–001
N_3	N_2	2	S_3–043	T_4–002
N_4	N_4	1	S_4–092	T_4–001
N_5	N_4	2	S_5–163	T_4–002

The Destination is the other nodes in the network.

- ***Next hop:*** From starting node to which node, it will move in the next hop to reach the destination path to reach the destination is the next hop.
- ***Metric:*** Metric is the hop count.
- ***Sequence No:*** Sequence number of the last advertisement for this node.
- ***Install Time:*** The time at which path was installed first.

Advantages:

- Low memory needed.
- Quick convergence.
- Maintain routes between all nodes.

2.4.2.2 Dynamic Source Routing (DSR)

9. How does dynamic source routing handle routing? What is the motivation behind dynamic source routing compared to other routing algorithms for fixed networks?	**(16m)**	**Apr 2017**
10. Describe the Dynamic source routing with example.	**(13m)**	**May 2019**

In the DSDV, all nodes maintain path to all the other nodes.

Due to this there is heavy traffic.

To save the battery power DSR is considered.

This DSR divides the routing into 2 sub problems

- Route Discovery : Here a node tries to discover a route to a node (i) Only if there is information to send (ii) and no routes are known.
- Route Maintenance : If a node is continuously using this route to transmit a packet, then the route should be without problems. But if the node detects that the route is with problem, then it has to determine alternate route.

Working Principle : If a node reads a route to a destination, it broadcasts a route request with a unique identifier and the destination address as parameters.

The node which receives the (Route Request Message) does the following:

1. If the node has already received the request, it drops the request packet.
2. If the node recognizes own address as the destination, the request has reached the target.
3. Otherwise the node appends its own address in the route, and broadcasts this updated route request.

Principle :

- The route request collects the list of address representing a possible path on its way towards the destination. When the request reaches the destination, it can return the request packet to the source.
- When the link is bi-directional the route list is sent in the reverse order to the destination.
- When the link is unidirectional the destination does not maintain the route. It needs to discover the route.

Example to find a route from N_1 to N_3 at t_1,

1. N1 broadcasts the Request ((N1), id=42, target=N3). N2 and N4 receive the packet.
2. N2 broadcasts ((N1, N2), id=42, target=N3).N4 broadcasts ((N1, N4), id=42, target=N3). N3 and N5 receive N2's broadcasts. N1, N2, N5 receives N4's broadcasts.
3. N3 itself is the target.
4. N5broadcasts ((N1, N2, N5), id=45, target=N3). N3, N4 receive this broadcast.
5. N1, N2, N5 drop this N4's broadcast, because it has already received.
6. N4 drops N5's broadcast.

   N3 finds (N1, N2 and N5) as an alternate route but a longer route.

7. N3 has to return the path (N1, N and N3) to N1 . N3 can do the reverse forwarding because symmetric link is assumed.
8. When the links are uni-directional the algorithm needs to be applied again with N3 as source and. Nj as destination.

Optimization

1. To avoid too many broad cast route requests should contain a counter. For every rebroad cast the counter is incremented. When the counter exceeds the number of nodes in the network, the nodes can drop the request.
2. Node can Cache the path fragments from recent requests. This fragments can be used to find other route.
3. A node can update the Cache while forwarding the packets.
4. The node can update the Cache when it overhears the transmission from other nodes.

Maintenance of the Route: When the routes are discovered they need to be maintained. Approaches to maintain the route are as follows :

1. If the link layer uses acknowledgement this ack can be considered as an interact route.
2. The node can overhear the next hop which is passive acknowledgement.
3. A node can ask for explicit acknowledge.

When the links are bi-directional, no problem for maintenance. If not the situation is complicated. If there is connectivity problem, detected by a node, it has to inform the sender, to find a new route from the sender.

***

2.4.2.2 Other Routing Protocols

11. Explain the following protocols.

a) Flat ad hoc routing
b) Hierarchical Ad hoc routing
c) Geographic position assisted Ad hoc routing
d) Greedy perimeter stateless routing

1. Flat ad hoc routing
2. Hierarchical Ad hoc routing
3. Geographic position assisted Ad hoc routing
4. Greedy perimeter stateless routing

2.4.2.3.1 Flat ad hoc routing

- This protocol does not set up in any hierarchies with nodes,
- All the nodes have an equal role in routing.
- Addressing Scheme is flat.
- Protocols is of two types :

  (1) Proactive protocols

  (2) Reactive protocols.

(1) Proactive Protocols

Sets up tables for routing (e g.,) DSDV. The Algorithm is based on link state algorithm.

Link State Algorithm : Such algorithm floods the information to the neighbors periodically. This algorithm cannot be used in mobile ad hoc environment due to too much of updates/too few updates which reduces the traffic.

To achieve both (i.e.) update without traffic:

- ✓ Fisheye State Routing.
- ✓ Fuzzy Sighted Link State is used.

The concept is to transmit for away destination at a lower frequency.

Some algorithms attacks:

- ✓ Topology Broadcast based on reverse path forwarding.
- ✓ Optimized link state routing.

Advantage of Proactive Protocol:

- QOS guarantees
- Routing table reflect the current topology with certain precision.

Disadvantage:

- Overhead in lightly loaded networks.

(2) Reactive Protocols

A path between source and destination is set only if there is a necessity (e.g.) DSR, AODV (Ad hoc on Demand Distance Vector) on demand.

Advantages:

- Scalability.
- Devices can use longer low power periods because they wakeup only when needed.

Disadvantages:

- Initial search latency.

- Route casting is useful only when there is high mobility.

2.4.2.3.2 Hierarchical Ad hoc routing

For larger networks, clustering of nodes needs to be done. This algorithm is scalable.

Concept: Locality properties, (i.e.) if a cluster can be established nodes remain in the cluster (grouping) with minor changes. When the topology changes only the cluster is to be informed. Nodes of other cluster needs to know how to reach the cluster.

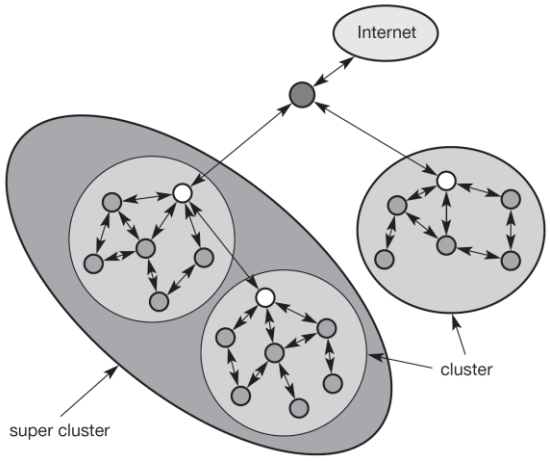


Figure: Building hierarchies in ad-hoc networks

Advantage:

- Lesser number of message transfers.
- Cluster can be combined to form super cluster.
- One node can act as cluster head.
- This cluster head is used as router for Inter Cluster Communication.

Three protocols based on this concept are

1. Cluster Head Gateways Switch Routing.
2. Hierarchical State Routing.
3. Zone Routing Protocol.

2.4.2.3.3 Geographic position assisted Ad hoc routing

- Here the mobile modes should know their geographical position.
- To get the position we can use Global Positioning System (GPS).
- Geocast allows the messages to be sent to all nodes in a specific region.
- This is done based on the address of (geographic information).
- The location aided routing protocol similar to DSR, can be used.
- But it is restricted to use in certain geographic only.

2.4.2.3.4 Greedy perimeter stateless routing:

- This method uses the location of neighbors that are exchanged via a periodic beacon messages or in a piggy banking.
- This follows the greedy method where by the packets are forwarded to the geographically closest neighbor via which the destination can be reached.
- Once when it reaches a dead end hash tracking should be done.

Metrics:

1. Traditionally hop count is considered as Metrics. This hop count is best choice for fixed network.
2. Other metric can be Bandwidth.
3. Least Interference Routing can be considered as other metric.

Consider the topology

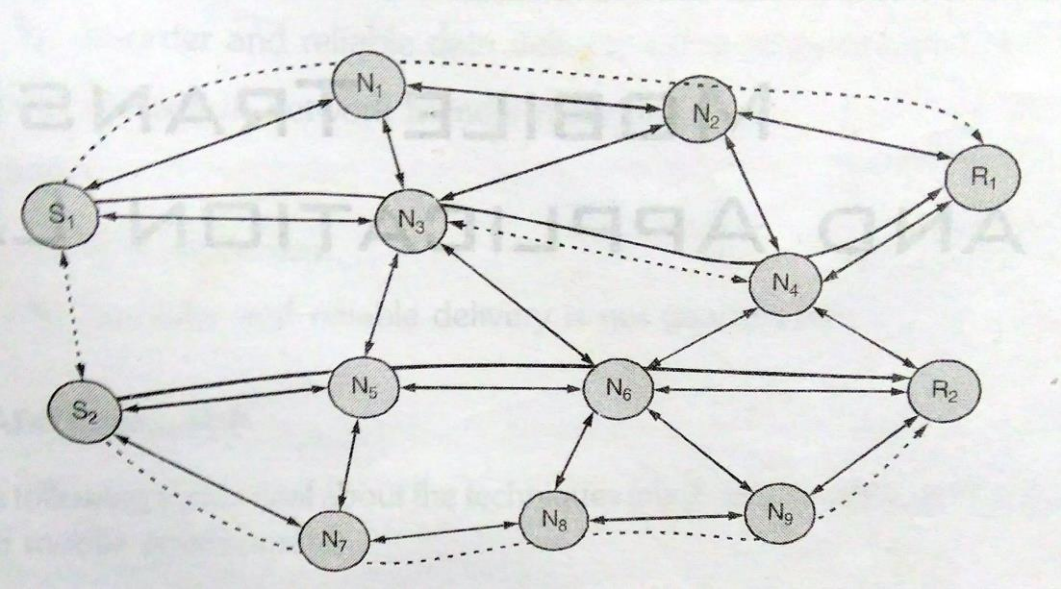


Figure: Example for Least Interference routing

S_1 is the sources and R_1 is the receiver. Possible paths are :

1. S_1, N_3, N_4, R_1 = Number of hops = 4 I = 16
2. S_1, N_3, N_2, R_1 = Number of hops = 4 I = 15
3. S_1, N_1, N_2, R_1 = Number of hops = 4 I = 12
4. S_1, N_1, N_2, N_3, N_4, R_1, committed due to number of hops = 6 (I is the Inference).

This method calculates the Interference of a path. Interference is defined as number of neighbors that can over hear a transmission. Hence the route S_1, N_1, N_2, R_1 is selected.

2.5 Network layer in the internet

7. *Discuss about the network layers in the internet.*

- The IP provides the basis for the interconnections of the Internet.
- IP is a ***datagram protocol***.
- The packets contain an ***IP header***.
- The basic header, without options, is shown in Figure 2.24.
- ***Version:*** The version field contains the version of IP—IPv4 or IPv6.
- ***Internet header length*** (IHL):
  - ✓ The ***internet header length*** (IHL) field specifies the actual length of the header in multiples of 32-bit words.
  - ✓ The minimum length is 5.
  - ✓ The maximum permissible length is 15.

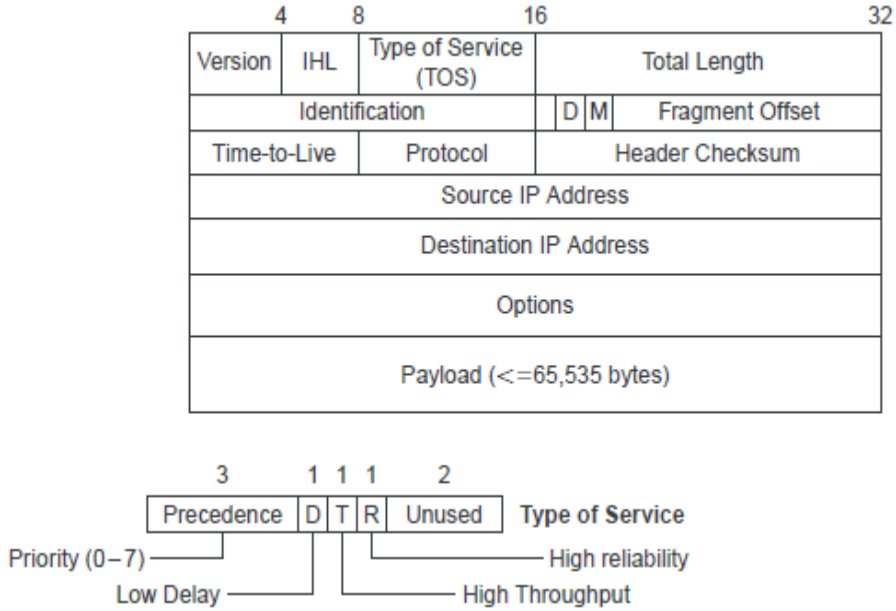


Fig:2.24 IP Header

- ***Type of service (TOS)*** :
  - ✓ The ***type of service (TOS)*** field allows an application protocol/process to specify the relative priority of the application data and the preferred attributes associated with the path to be followed.
  - ✓ It is used by each gateway and router ***during the transmission and routing*** of the packet to transmit packets of higher priority first and to select a line/route that has the specified attributes should a choice be available.

- ***Total length field:***
  - ✓ The total length field defines the total length of the initial datagram including the header and payload parts.
  - ✓ When the contents of the initial datagram need to be transferred in multiple packets, then the value in this field is used by the destination host to ***reassemble the payload*** contained within each smaller packet — known as a fragment — into the original payload.
- ***Identification field:***
  - ✓ The identification field enables the destination host to relate each received packet fragment to the same original datagram.
- ***Don't fragment (or)D-bit:***
  - ✓ Don't fragment or D-bit is set by a source host and is examined by routers.
  - ✓ A D-bit indicates that the packet should not be fragmented.
- ***More fragment or M-bit:***
  - ✓ More fragment or M-bit is used during the reassembly procedure associated with data transfers involving multiple smaller packets/fragments.
  - ✓ It is set to 1 in all but the last packet/fragment in which it is set to 0.
- ***Fragment offset:***
  - ✓ The fragment offset field is used to indicate the position of the first byte of the fragment contained within a smaller packet in relation to the original packet payload.
- All fragments except the last one are in multiples of 8 bytes.
- ***Time-to-live field:***
  - ✓ The time-to-live field defines the maximum time for which a packet can be in transit across the Internet.
  - ✓ The value is in seconds and is set by the IP in the source host.
  - ✓ It is decremented by each gateway and router by a defined amount and should the value become zero, the packet is discarded.
- ***Protocol field:***
  - ✓ The protocol field is used to enable the destination IP to pass the payload within each received packet to the same (peer) protocol that sent the data.
  - ✓ This can be an internal network layer protocol such as the ICMP or a higher-layer protocol such as TCP or UDP.
- ***Header checksum:*** The header checksum applies just to the header part of the datagram and is a safeguard against corrupted packets being routed to incorrect destinations.
- ***Source and Destination Internet addresses:***
  - ✓ The source and destination Internet addresses indicate the sending host and the intended recipient host for this datagram.
- ***Options field:***

- ✓ The options field is used in selected datagrams to carry additional information relating to security, source routing, loose source routing, route recording, stream identification, and time-stamp.

- ***Payload:*** The last field is the payload.

- A symbolic address, or name, of the form user@domain can be used instead of an Internet address.
- It is translated into an Internet address by directory tables that are organized along the same hierarchy as the addressing.
- Typically, the domain is of the form machine, institution, type, country.
- The type is ***edu*** for educational institutions, ***com*** for companies, ***gov*** for governmental agencies, ***org*** for nonprofit organizations, and ***mil*** for military.
- The country field is omitted for the United States and is a two-letter country code for the other countries (e.g., fr for France). For instance, the author's address is vgarg@uic.edu.

- With best-effort delivery service (optional quality of service (QoS)), IP packets may be lost, corrupted, delivered out-of-order, or duplicated.
- The upper layer entities should anticipate and recover on an end-to-end basis.

Internet Addresses

Three classes of Internet addresses (unicast) are used (see Figure 2.25):

- Class A — 7 bits for netid and 24 bits for hostid, they are used with networks having a large number of hosts (224)
- Class B — 14 bits for netid and 16 bits for hostid, they are used with networks having a medium number of hosts (216)
- Class C — 21 bits for netid and 8 bits for hostid, they are used with networks having a small number of hosts (28)

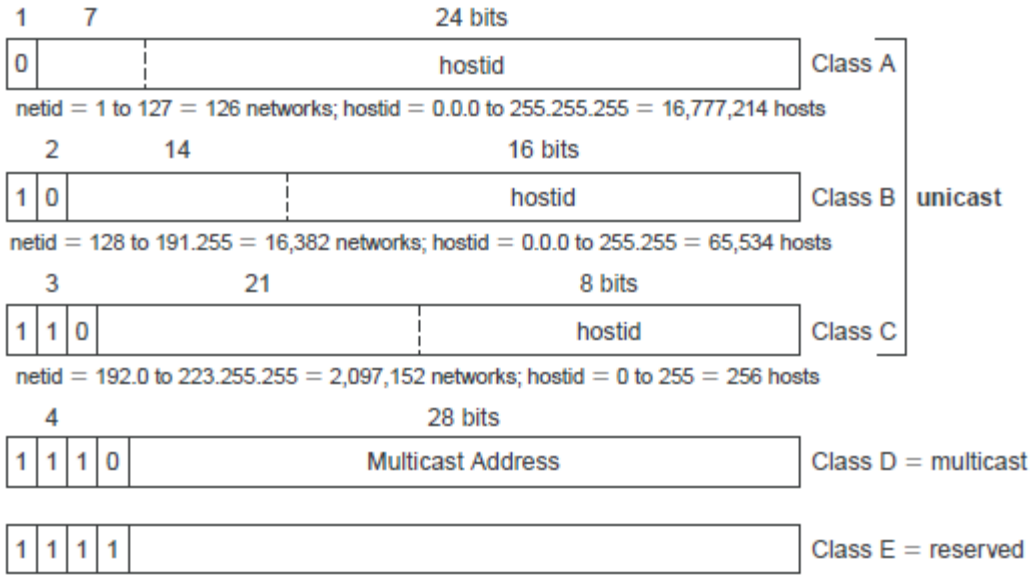


Fig: 2.25 Internet addresses.

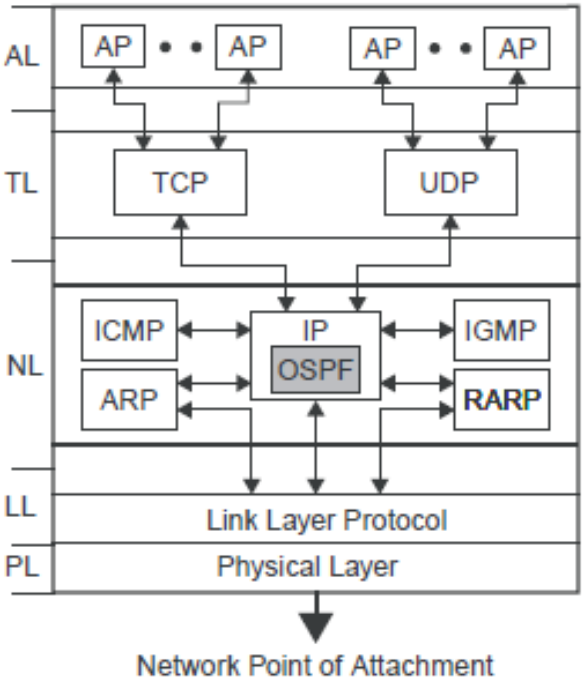
- It should be noted that the netid and hostid with all 0s or all 1s have special meaning.
  - An address with hostid of all 0s is used to refer to the network in netid part rather than a host
  - An address with a netid of all 0s implies the same network as the source network/netid
  - An address of all 1s means broadcast the packet over the source network
  - An address with a hostid of all 1s means broadcast the packet over the destination network in netid part
  - A class A address with a netid of all 1s is used for test purposes within the protocol stack of the source host. It is known as the loop-back address.

IP Adjunct Protocols

Figure 2.26 shows the IP adjunct protocols.

- ***Address resolution protocol (ARP)*** and R***everse ARP (RARP)*** are used by IP in hosts that are attached to a broadcast LAN (such as Ethernet or token ring)
  - ✓ To determine the physical MAC address of a host or gateway given its IP address (ARP), and, in case of the RARP, the reverse function.

- ***Open shortest path first (OSPF):***
  - ✓ Open shortest path first (OSPF) protocol is a routing protocol used in the global internetwork.
  - ✓ Such protocols are present in each internetwork router.
  - ✓ They are used to build up the contents of the routing table used to route packets across the global internetwork.



AP: Application Protocol/process
ARP: Address Resolution Protocol
RARP: Reverse ARP
ICMP: Internet Control Message Protocol
IGMP: Internet Group Message Protocol
OSPF: Open Shortest Path First
UDP: User Datagram Protocol
TCP: Transmission Control Protocol

Figure 2.26 Adjunct protocols.

- ***Internet control message protocol (ICMP)*** is used by the IP in a host or gateway to exchange errors and other control messages with IP in another host or gateway.
- ***Internet group message protocol (IGMP)*** is used with multicasting to enable a host to send a copy of a datagram to the other hosts that are part of the same multicast group.

- The ICMP forms an integral part of all IP implementations.
- It is used by hosts, routers, and gateways for a variety of functions, and especially by network management.
- The main functions associated with the ICMP are as follows:
  - ✓ Error reporting
  - ✓ Reachability testing
  - ✓ Congestion control
  - ✓ Route-change notification
  - ✓ Performance measuring
  - ✓ Subnet addressing

- The standard way to send an IP packet over any point-to-point link is either dial-up modems (e.g., async framing), leased lines (e.g., bit synchronous framing), or ISDN, IS-99 CDMA (e.g., octet-synchronous framing).
- ***The link control protocol (LCP)*** runs during initial link establishment and negotiates link-level parameters (e.g., maximum frame size, etc.).
- ***The IP control protocol (IPCP)*** establishes the IP address of the client (the point-to-point (PPP) server, allocates a temporary address, or the client notifies the server of the fixed address) and negotiates for the use of TCP/IP header compression.

QoS Support in the Internet

- QoS requirements include a defined minimum mean packet throughput rate and a maximum end-to-end packet transfer delay.
- To meet the varied set of QoS requirements, two schemes have been standardized:
  - ✓ Integrated Services (IntServ)
  - ✓ Differentiated Services (DiffServ)
- Packets relating to different types of call/session are each allocated a different value in the precedence bits of the type of service (TOS) field of the IP packet header.
- This is used by routers within the Internet to differentiate between the packet flows relating to different types of calls.

2.6 Session Initiation Protocol (SIP)

8. Explain in detail about session initiation protocol.

Explain the mobile IP session initiation protocol for IP packet delivery in I networks. (16m) [May 2018]

Illustrate the features, for a Mobile IP session initiation protocol. [Nov 2019]

- SIP is used for provisioning services in IP-based mobile networks.
- SIP specifications ***define an architecture of user agents and servers*** (proxy server, redirect server, register) that ***support communications*** between SIP peers through user tracking, call routing, and so on.
- In SIP, each user is uniquely identified by an ***SIP universal resource indicator***.

- This is used as the identifier to address the called user when the sending session initiation requests.

- An IP address is associated with the user in order to route SIP signaling from the SIP register.

- A SIP user registers with the ***SIP register*** to indicate its presence in the network and its willingness to receive incoming session initiation requests from other users.
- A typical session in SIP begins with a user sending an INVITE message to a peer through SIP proxies.

- When the recipient accepts the request and the initiator is notified, the actual data flow begins, usually taking a path other than the one taken by the SIP signaling messages.
- An INVITE message typically carries a description of the session parameters. In particular, each media component of the SIP session is described in terms of QoS parameters.

- The user can modify the parameters regarding an existing session by adding or removing media components or modifying the current QoS using a re-INVITE message.
- SIP also supports personal mobility by allowing a user to reregister with an SIP register on changing its point of attachment to the network, in particular on changing its IP address.
- A user could also change point of attachment during an active session provided the user re-invites the session providing the new parameters.

****

UNIT II

MOBILE NETWORK LAYER

TWO MARKS

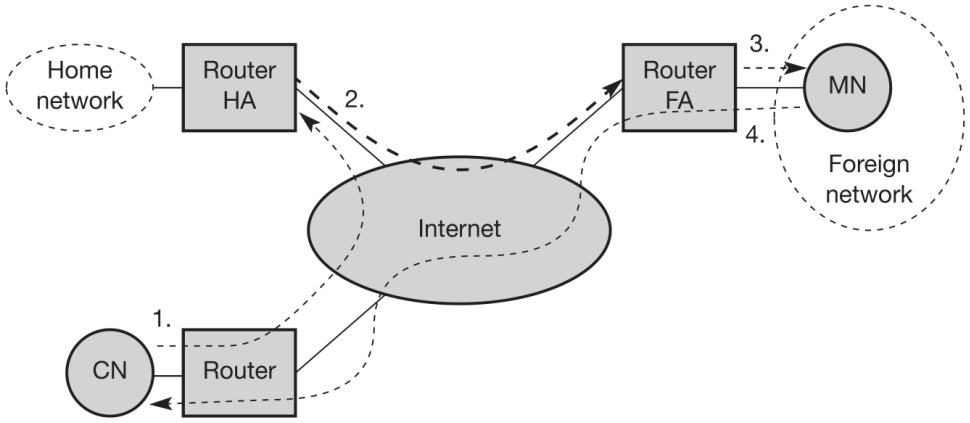
MOBILE IP

1. **Define mobile IP.**
   What is mobile IP? What are the entities of mobile IP? [May 2018] *(Combine Qn. No.: 3)*
   Mobile IP was developed to enable computers to maintain Internet connectivity while moving from one Internet attachment point to another. Although Mobile IP can work with wired connections, in which a computer is unplugged from one physical attachment point and plugged into another, it is particularly suited to wireless connections

2. **What are the requirements accompanied the development of the Mobile IP standard?**
   - Compatibility
   - Transparency
   - Scalability and efficiency
   - Security
3. **What are the entities and terminologies associated with Mobile IP?**
   - Mobile node (MN)
   - Correspondent node (CN)
   - Home network (HN)
   - Foreign network (FN)
   - Foreign agent (FA)
   - Care-of address (COA) - Foreign agent COA, Co-located COA
   - Home agent (HA)

IP packet delivery

4. **Draw the schematic diagram representation of Packet delivery to and from the mobile node.**



Agent discovery

5. **What is meant by agent discovery?**
   Agent discovery consists of two steps agent advertisement and agent solicitation, which are in fact router discovery methods plus extensions of an MN to find a foreign agent

Agent advertisement

6. What is called Agent advertisement.?

Foreign agents and home agents advertise their presence periodically using special agent advertisement messages.These advertisement messages can be seen as a beacon broadcast into the subnet. For these advertisements Internet control message protocol (ICMP) messages accordding to RFC1256 are used with some mobility extensions. Routers in the fixed network implementing this standard also advertise their routing service periodically to the attached links.

7. What is Agent solicitation? [Nov/ Dec 2016] (or)
When the agent solicitation message has to be sent by mobile node? [Nov 2017]

If no agent advertisements are present or the inter-arrival time is too high, and an MN has not received a COA by other means, e.g., DHCP, the mobile node must send agent solicitations.These solicitations are again based on RFC 1256 for router solicitations. Care must be taken to ensure that these solicitation messages do not flood the network, but basically an MN can search foran FA endlessly sending out solicitation messages.

Registration

8. What is the purpose of registration?

Having received a COA, the MN has to register with the HA. The main purposeof the registration is to inform the HA of the current location for correct forwardingof packets.

9. Give the diagramatic representation of Registration of a mobile node via the FA or directly with the HA.

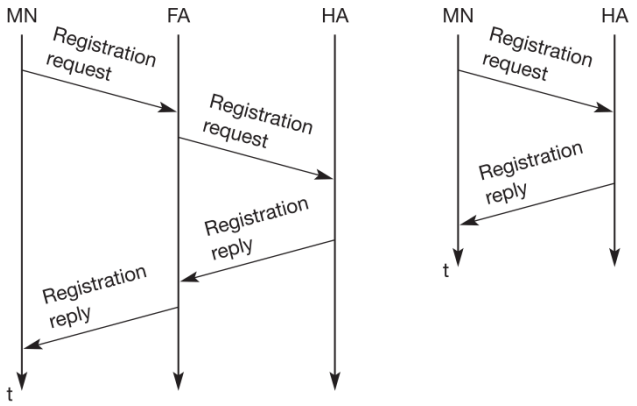


Figure: Registrationof a mobile node via theFA or directly with the HA

10. Draw and give details about the diagram of Registration request (UDP Packets).

Figure: Registration request

- UDP packets are used for registration requests.
- The IP source address of the packet is set to the interface address of the MN, the IP destination address is thatof the FA or HA (depending on the location of the COA).
- The UDP destinationport is set to 434.
- UDP is used because of low overheads and better performancecompared to TCP in wireless environments.
- The fields relevantfor mobile IP registration requests follow as UDP data.

11. Give the example for registration reply codes.

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

Tunneling and encapsulation

12. What are the mechanisms used for forwarding packets between the HA and the COA?

- Tunneling
- Encapsulation

13. Define tunneling.

- A **tunnel** establishes a virtualpipe for data packets between a tunnel entry and a tunnel endpoint.
- Packets entering a tunnel are forwarded inside the tunnel and leave the tunnelunchanged.
- Tunneling, i.e., sending a packet through a tunnel, is achieved byusing encapsulation.

14. Define encapsulation and decapsulation. [Nov/ Dec 2012] (or)
What is encapsulation in Mobile IP? [Apr 2017]

- Encapsulation is the mechanism of taking a packet consisting of packetheader and data and putting it into the data part of a new packet.
- The reverse operation, taking a packet out of the data part of another packet, is called decapsulation.
- Encapsulation and decapsulation are the operations typicallyperformed when a packet is transferred from a higher protocol layer to a lowerlayer or from a lower to a higher layer respectively. Here these functions areused within the same layer.

15. What is IP encapsulation?

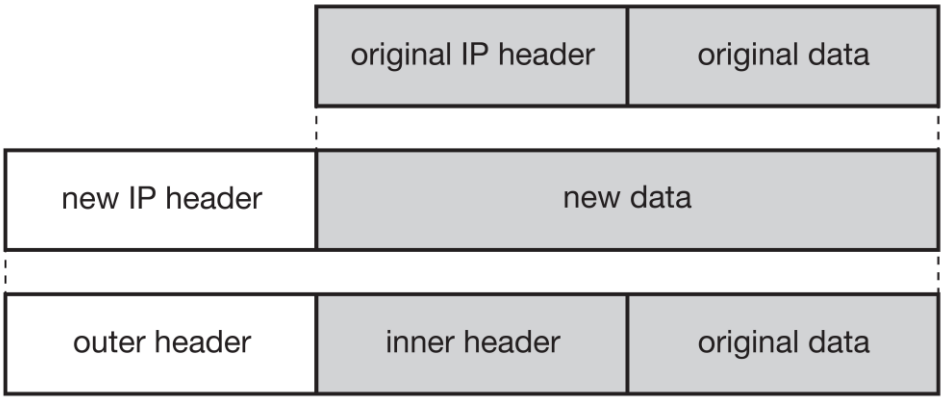
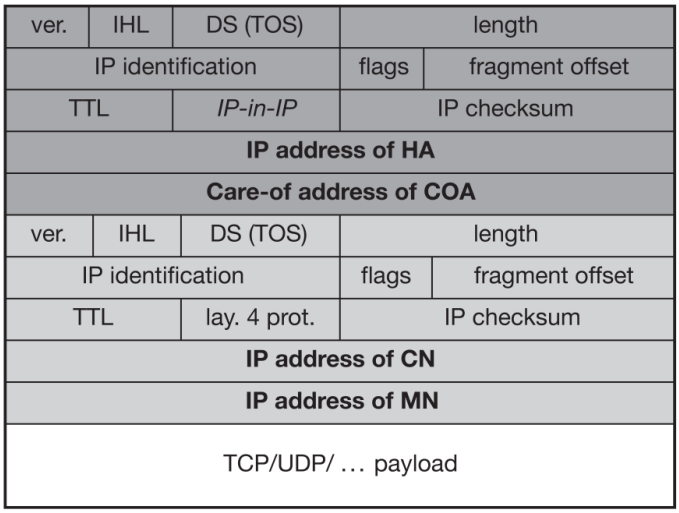


Figure:IP encapsulation

The HA takes the original packet with the MN as destination,puts it into the data part of a new packet and sets the new IP header insuch a way that the packet is routed to the COA.The new header is also calledthe **outer header** for obvious reasons. Additionally, there is an **inner header**which can be identical to the original header as this is the case for IP-in-IPencapsulation, or the inner header can be computed during encapsulation.

IP-in-IP encapsulation

16. Define IP-in-IP encapsulation and give its format.



- There are different ways of performing the encapsulation needed for the tunnelbetween HA and COA. Mandatory for mobile IP is **IP-in-IP encapsulation** asspecified in RFC 2003.

- Figure shows a packet inside the tunnel. The fields follow the standard specification of the IP protocol as definedin RFC 791 and the new interpretation of the former TOS, now DS field in the context of differentiated services (RFC 2474).

17. Define Binding request.

Any node that wants to know the current location of anMN can send a binding request to the HA. The HA can check if the MN hasallowed dissemination of its current location. If the HA is allowed to revealthe location it sends back a binding update.

18. Define Binding update.

This message sent by the HA to CNs reveals the currentlocation of an MN. The message contains the fixed IP address of the MNand the COA. The binding update can request an acknowledgement.

19. Define Binding warning.

If a node decapsulates a packet for an MN, but it is not thecurrent FA for this MN, this node sends a binding warning. The warning containsMN's home address and a target node address, i.e., the address of thenode that has tried to send the packet to this MN.

The recipient of the warning then knows that the target node could benefit from obtaining a freshbinding for the MN. The recipient can be the HA, so the HA should now senda binding update to the node that obviously has a wrong COA for the MN.

20. What are additional messages needed by optimized Mobile IP?

The optimized mobile IP protocol needs four additional messages.

- Binding request
- Binding update
- Binding acknowledgement
- Binding warning

IPv6

21. What are the advantages and disadvantages if Cellular IP?

Advantage

- Manageability: Cellular IP is mostly self-configuring, and integration of theCIPGW into a firewall would facilitate administration of mobility-relatedfunctionality.

Disadvantages

- Efficiency: Additional network load is induced by forwarding packets onmultiple paths.
- Transparency: Changes to MNs are required.
- Security: Routing tables are changed based on messages sent by mobilenodes. Additionally, all systems in the network can easily obtain a copy ofall packets destined for an MN by sending packets with the MN's sourceaddress to the CIPGW.

22. What are the advantages and disadvantages of Hierarchical mobile IPv6 (HMIPv6)?
Hierarchical mobile IPv6 (HMIPv6)

Advantages

- Security: MNs can have (limited) location privacy because LCOAs can be hidden.
- Efficiency: Direct routing between CNs sharing the same link is possible.

Disadvantages

- Transparency: Additional infrastructure component (MAP) needed.

Dynamic Host Configuration Protocol

21.What is the use of DHCP protocol?

The dynamic host configuration protocol is mainly used to simplifiy the installation and maintenance of networked computers.If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network, e.g., addressesof a DNS server and the default router, the subnet mask, the domain name, and anIP address. Providing an IP address, makes DHCP very attractive for mobile IP as a source of care-of-addresses.

23. Give the configuration of DHCP.

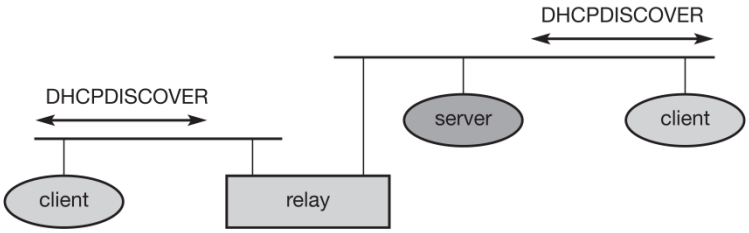


Figure: Basic DHCPconfiguration

- DHCP is based on a client/server model as shown in Figure. DHCP clients send a request to a server (DHCPDISCOVER in the example) to which the server responds.A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.

24. What is meant by Dynamic Source Routing? [Nov 2019]
Dynamic Source Routing (**DSR**) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

25. Write about the two different problems in DSR (Dynamic source routing).
Dynamic source routing (DSR), divides the task of routing into two separate problems

- **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- **Route maintenance:** If a node is continuously sending packets via a route,it has to make sure that the route is held upright. As soon as a node detectsproblems with the current route, it has to find an alternative.

26. List some Mobile ad-hoc routing protocols.

- Flat ad-hoc routing
- Hierarchical ad-hoc routing
- Geographic-position-assisted ad-hoc routing

27. Define security parameter index. (May/Dec 2013)

Security Parameter Index (SPI) is an index that identifies a security contextbetween a pair of nodes. This security context is configured so that the twonodes share a secret key and parameters relevant to this association (e.g.,authentication algorithm).

28. What are the two different types of destination addresses that can be assigned to a mobile node while it is attached to a foreign network? (or)
What is care of address in Mobile IP? (or) Define the term care of address in mobile IP. [Apr/Mar 2017][Apr/May 2019]

The protocol can use two different types of care of addresses:
Foreign agent care of address-is an address of a foreign agent with which the **mobile** node is registered.
Co- located care of address - A co-located care-of address is an IP address obtained by the mobile node that is associated with the mobile node's current interface to a network.

29. What are the different types of message authentication extensions in mobile IP?

Three types of authentication extensions are defined:

- **Mobile-home:** This extension must be present and provides for authentication of the registration messages between the mobile node and the home agent.
- **Mobile-foreign:** The extension may be present when a security association exists between the mobile node and the foreign agent. The foreign agent will strip this extension off before relaying a request message to the home agent and add this extension to a reply message coming from a home agent.
- **Foreign-home:** The extension may be present when a security association exists between the foreign agent and the home agent.

30. Distinction between a mobile user and a nomadic user. [Nov/ Dec 2014]

- **Mobile user**-The user is connected to one or more applications across the Internet, that the user's point of attachment changes dynamically, and that all connections are automatically maintained despite the change.
- **Nomadic user-**the user's Internet connection is terminated each time the user moves and a new connection is initiated when the user dials back in. Each time an Internet connection is established, software in the point of attachment (typically an ISP) is used to obtain a new, temporarily assigned IP address. This temporary IP address is used by the user's correspondent for each application-level connection (e.g., FTP, Web connection). A better term for this kind of use is *nomadic.*

31. Draw and explain thePerformance enhancing proxy.

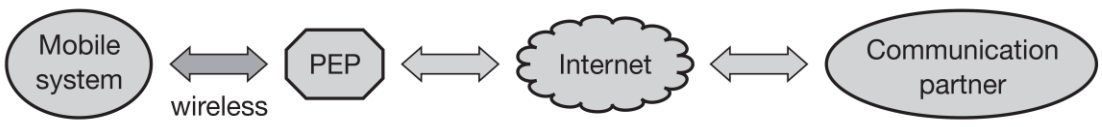


Figure: Performance enhancingproxy

Performance-enhancing proxies (PEPs) are network agents designed to improve the end-to-end performance of some communications protocol. Performance-enhancing proxies standards are defined in RFC 3135 (performance-enhancing proxies intended to mitigate link-related degradations) and RFC 3449 (TCP performance implications of network path asymmetry).

Mobile Adhoc Networks

32. What are the difference between Proactive and Reactive Routing protocols? (or) Differeentiate proactive and reactive routing protocols. Write examples for each. [Nov 2018]

Sl. No.	Reactive(On-demand)	Proactive(Table driven)
1.	Average end-to-end delay or the time taken by the data to reach the destination from the source is variable in Reactive Protocols.	Average end-to-end delay or the time taken by the data to reach the destination from the source is Constant in proactive Protocols.
2.	The delivery of packet data is much more efficient.	The delivery of packet data is less efficient.
3.	Reactive Protocols are much faster in performance.	Proactive protocols are slower in performance.
4.	It is more adaptive and work much better in different topographies.	It is less adaptive.

33. What are the characteristics of a Ideal Routing protocol for Adhoc wireless networks? (Nov/ Dec 2014)

- Fully distributed.
- Adaptive tp frequent topology changes.
- Minimum connection setup time is desired.
- Loop free and free from state routes.
- Provide QOS and support for time sensitive traffic

34. List the issues in designing Routing protocol for Adhoc wireless networks.

- Bandwidth efficiency.
- QOS support
- Mobility
- Bandwidth constraints.
- Hidden terminal problem

35. What are the parameters included in Routing Protocols?

- High dynamic topology.
- No infrastructure for centralized administration.
- Bandwidth constraints.
- Energy constraints.

36. What is DSDV protocol?

- **DSDV**-Destination Sequenced Distance-Vector Routing Protocols are the first protocols proposed for Adhoc wireless networks, It is an enhanced version of the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest and the first node on the shortest path to every other node in the network.

37. Write the advantages and disadvantages of CGSR.

CGSR-Cluster-Head Gateway Switch Routing protocol

Advantages:

- Better bandwidth utilization is possible.
- Easy to implement priority scheduling schemes with token scheduling and gateway code scheduling.

Disadvantages:

- Increase in path length and instability in the system at high mobility when the rate of change of cluster-heads is high.

38. Write the use of Hierarchical Routing protocols and its types. (Nov/ Dec 2014)

- The use of routing hierarchy has several advantages, the most important ones being reduction in the size of routing tables and better scalability,

Types:

- HSR-Hierarchical State Routing Protocol
- FSR-Fisheye State Routing Protocol

39. What are the metrices of Power Aware Routing Protocols?

- Minimal Energy Consumption per packet
- Maximize Network Connectivity
- Minimum Variance in Node Power Levels
- Minimum Cost per packet
- Minimize Maximum Node Cost

40. Which Topologies are used in Routing protocols?

- Flat Topology routing protocol
- Hierarchical Topology Routing Protocol

41. What is the function of Power aware Routing protocol?

Power aware routing protocols is used for minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power. The routing decisions are based on minimizing the power consumption either locally or globally in the network.

42. List the tables maintained by a node in WRP.

- Distance Table (DT)
- Routing Table (RT)
- Link Cost Table (LCT)
- Message Retransmission List (MRL)

43. Write the advantages and disadvantages of WRP.

WRP-Wireless Routing Protocol

Advantages:

It has faster convergence and involves fewer table updates. But the complexity of maintenance of multiple tables demands a larger memory and greater processing power from nodes.

Disadvantages:

At high mobility, the control overhead involved in updating table entries is almost the same as that of DSDV and hence is not suitable for highly dynamic and also for large ad hoc wireless networks.

44. Write the advantages and disadvantages of DSDV.

DSDV-Destination Sequenced Distance Vector Routing Protocol

Advantage:

The availability of routes to all destinations at all times implies that much less delay is involved in the route setup process.

Disadvantage:

Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth. Hence, this protocol suffers from excessive control overhead that is proportional to the number of nodes in the network and therefore is not scalable in adhoc wireless networks, which have limited bandwidth and whose topologies are highly dynamic.

45. Write the advantages and disadvantages of STAR.

STAR-Source-Tree Adaptive Routing Protocol

Advantage:

STAR has very low communication overhead among all the table-driven routing protocols.

Disadvantage:

The use of the LORA approach in this table-driven routing protocol reduces the average control overhead compared to several other pm-demand routing protocols.

46. Write the advantages and disadvantages of DSR.

DSR-Dynamic Source Routing Protocol

Advantages:

- The protocol uses a reactive approach which eliminates the need to periodically find the network with table update messages which are required in a table-driven approach.
- The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

Disadvantages:

- The route maintenance mechanism does not locally repair a broken link.
- The connection setup delay is higher than in table-driven protocols. Even though the protocol performs will in static and low mobility environments, the performance degrades rapidly with increasing mobility.

47. Write the advantages and disadvantages of AODV.

AODV-Ad Hoc On-Demand Distance-Vector Routing Protocol

Advantage:

Routes are established on demand and destination sequence numbers are used to fine the latest to the destination. The connection setup delay is less.

Disadvantage:

The intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.

48. Write the advantages and disadvantages of TORA. (May/June 2013)

TORA - Temporally-Ordered Routing Algorithm

Advantage

By limiting the control packets for route reconfigurations to a small region, TORA incurs less control overhead.

Disadvantage

Concurrent detection of partitions and subsequent deletion of routes could result in temporary oscillations and transient loops.

49. Write the advantages and disadvantages of HSR.

HSR - Hierarchical State routing

Advantages:

- Reduces the routing table size by making use of hierarchy information.
- The storage required is O (n x m) compared to O (n^m) that is required for a flat topology link state routing protocol.

Disadvantages:

- Though the reduction in the amount of routing information stored at nodes is appreciable, the overhead involved in exchanging packets containing information about the multiple levels of hierarchy and the leader election process make the protocol unaffordable in the ad hoc wireless networks context.

50. Write the advantages and disadvantages of FSR.

FSR - Fisheye State Routing

Advantage:

- The notion of multi-level scopes employed by FSR significantly reduces the bandwidth consumed by link state update packets.
- Hence, FSR is suitable for large and highly mobile ad hoc wireless networks.

Disadvantage:

- The choice of the number of hops associated with each scope level has a significant influence on the performance of the protocol at different mobility values, and hence must be carefully chosen.

51. What is an ad hoc wireless network? (May/June 2013)

- An ad hoc wireless network is a collection of two or more devices equipped with wireless communication and networking capability. Such devices can communicate with another node that is immediately within their radio range or one that is outside their radio range.
- An ad hoc network is self-organizing and adaptive.

52. List out the several issues of the multicast routing protocol.

There are several issues involved in multicast routing,

- Robustness
- Efficiency
- Control overhead
- Quality of service
- Dependency on the unicast routing protocol
- Resource management

53. Distinguish Hidden & exposed terminal problems in adhoc wireless network.

- If both nodes S1 & S2 transmit to the receiving node R1 at the same time their packets collide at node R1. This is because both nodes S1 & S2 are hidden from each other as they are not within the direct transmission range of each other, it is known as **hidden terminal problem.**
- If the transmission from the node S1 to the another node receiver R1 is already in progress. Node S3 cannot transmit to the node R2 as it concludes that its neighbor node S1 is in transmitting node & hence it should not interfere with ongoing transmission. This effect is known as **exposed terminal problem.**

54. State exposed terminal problems in adhoc wireless network.

- If the transmission from the node S1 to the another node receiver R1 is already in progress. Node S3 cannot transmit to the node R2 as it concludes that its neighbor node S1 is in transmitting node & hence it should not interfere with ongoing transmission. This effect is known as **exposed terminal problem.**

55. State Hidden terminal problems in adhoc wireless network. (Nov 2014)

- If both nodes S1 & S2 transmit to the receiving node R1 at the same time their packets collide at node R1. This is because both nodes S1 & S2 are hidden from each other as they are not within the direct transmission range of each other, it is known as **hidden terminal problem.**

56. What are the different categories of the multicast routing protocols? (May/June 2012)

- Flooding
- Source based multicast tree(SBT)
- Core based multicast tree(CBT)
- Multicast mesh
- Group based multicast forwarding

57. Why ad hoc network is preferred for?

- It does not need backbone infrastructure support
- Are easy to deploy
- Useful when infrastructure is absent, destroyed or impractical

58. What are the Applications of ad hoc network?

- **Personal area networking**
  cell phone, laptop, ear phone, wrist watch
- **Military environments**
  soldiers, tanks, planes
- **Civilian environments**
  taxi cab network, meeting rooms, sports stadiums, boats, small aircraft.
- **Emergency operations**
  search-and-rescue
  policing and fire fighting

59. Distinguish between adhoc wireless network and wireless sensor network. [May 2015, Nov 2013]

General Ad Hoc Networks	Sensor Networks
Unreliable communication	Unreliable communication
Require self-configuration	Require self-configuration
Constrained energy and bandwidth	Very constrained energy and bandwidth
Small-scale	Large-scale
Typically mobile	Typically immobile
Competitive	Cooperative
One-to-one traffic pattern	Many-to-one traffic pattern
Address-centric	Data-centric
QoS: delay, etc	Application-specific QoS

60. What are the characteristics of MANET? (or) Outline the characteristics of MANET. (Nov 2014, Nov 2013) (Apr/May 2019)

Characteristics of MANET:

- In MANET each node acts as both host and router.
- High user density and large level of user mobility.
- Centralized system or firewall is absent here.

61. What are the ways available for deletion of the multicast tree ?

The deletion of the multicast tree can be performed in two ways,

- Explicit broadcast of a tree deletion message
- Route entry expiration upon timeout(soft state)

62. Define SIP. Write the functions of SIP.

- SIP is used for provisioning services in IP-based mobile networks.
- SIP specifications ***define an architecture of user agents and servers*** (proxy server, redirect server, register) that ***support communications*** between SIP peers through user tracking, call routing, and so on.
- In SIP, each user is uniquely identified by an ***SIP universal resource indicator***.
    - This is used as the identifier to address the called user when the sending session initiation requests.
- An IP address is associated with the user in order to route SIP signaling from the SIP register.

63. Why is routing in multi-hop ad-hoc networks complicated? [Nov 2017]

Routing is complicated because of frequent topology changes, different capabilities of the nodes, varying propagation characteristics. Furthermore, no central instance can support routing.

64. Differentiate an ad-hoc network and a cellular network with respect to (a) Bandwidth usage (b) cost effectiveness. [May 2018]

Sl. No.	Particulars	Cellular network	Adhoc Network
1.	Bandwidth	The allocation of BW is guaranteed and easy	The allocation of BW is based on shared channel using complex MAC algorithms
2.	Cost and time for installation	Higher cost and takes more time for deployment.	Lower cost and does not take more time for deplment.

65. Compare tunneling and encapsulation. [Nov 2019]

TUNNELING	**ENCAPSULATION**
An IP tunnel is an Internet Protocol (IP) network communications channel between two networks.	Data Encapsulation is a process of adding header to wrap the data flows through OSI model.
It creates a tunnel when it uses a high level transport delivery service to send datagrams from one point to another	IP encapsulates each datagram in a packet when it uses hardware directly

*****

UNIT III

MOBILE TRANSPORT LAYER

TCP enhancements for wireless protocols - Traditional TCP: Congestion control, fast retransmit/fast recovery, Implications of mobility - Classical TCP improvements: Indirect TCP, Snooping TCP, Mobile TCP, Time out freezing, Selective retransmission, Transaction oriented TCP - TCP over 3G wireless networks.

3.1 Transmission Control Protocol

- The TCP is the connection-oriented transport layer protocol designed to operate on the top of the datagram network layer IP.
- The two widely used protocols are known under the collective name TCP/IP.
  - TCP provides a ***reliable end-to-end byte stream transport***.
  - The ***segmentation and reassembly of the messages*** are handled by IP, not by TCP.

1. Explain in detail about TCP enhancements for wireless networks.
2. Discuss various approaches suggested to improve end-to-end TCP performance over wireless links.

3.1.1 TCP Enhancements for Wireless Networks

TCP/IP in wire networks:

- TCP was primarily designed for wired networks.
- Its parameters were selected to maximize its performance on wired networks.
- Here, the packet delays and losses are caused mainly by ***congestion***.
- In wired networks, random bit error rate is negligible.

TCP/IP in wireless networks:

- In a wireless network, ***packet losses*** occur due to ***handoff or fading*** and can be random.
- In wireless network, when TCP responds to packet losses by invoking congestion control or avoidance algorithm, results in a degraded end-to-end performance.
- A wireless environment violates many of the assumptions made by TCP.
- Several approaches have been suggested to improve end-to-end TCP performance over wireless links

- They can be classified into three categories.
  1. ***End-to-end TCP protocols***, where loss recovery is performed by the sender, such as ***Explicit Loss Notification (ELN) option***.
  2. ***Link-layer protocols*** that provide local reliability using techniques such as
     - ✓ Forward error correction (FEC), and
     - ✓ Retransmission of lost packets in response to automatic repeat request (ARQ) messages
  3. ***Split TCP connection protocol*** that breaks the end-to-end TCP connection into two parts at the base station,
     a. One between the sender and the base station.
     b. Other between the base station and the receiver.

- All wireless networks face a ***high bit error rate***.

- In heterogeneous networks, the primary goal of TCP design is to differentiate clearly the ***cause of packet loss***.

- Such efforts aim to find a clear way ***to inform the sender about the cause of packet loss***, be it congestion or random errors.
- Thus, the sender is able to make appropriate decisions on ***how to adjust the congestion window***.
- In ***the End-to-end TCP protocols*** case
    - The link-layer ARQ mechanism is used to improve the error rate faced by TCP.
    - The IS-95 CDMA data stack uses this approach.

- In the ***Link-layer protocols*** case,
    - Network layer software is modified at the base station, to monitor every passing packet in either direction.
    - Cache packets at the base station are used and local retransmissions across wireless links are performed.

- In ***the Split TCP connection protocol*** case,
    - The TCP mode wireless portion is separated from the fixed portion.
    - With split TCP, TCP may get ACK even before the packet is successfully delivered to the receiver.
    - It also involves software overhead.

3. Compare various schemes used to improve TCP's performance in wireless and mobile environment.

- Some of the schemes used to improve TCP's performance in wireless and mobile environment are:
    - ✓ Indirect TCP (I-TCP) (see Figure 3.1)
    - ✓ Snooping TCP (see Figure 3.2)
    - ✓ Mobile TCP (M-TCP)
    - ✓ Fast retransmit/fast recovery
    - ✓ Transmission/time-out freezing
    - ✓ Selective retransmission

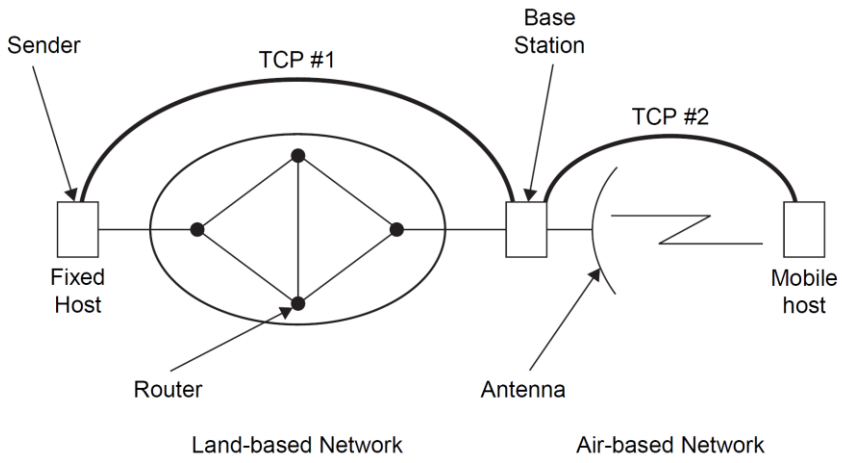


Figure 3.1 Split connection (indirect) TCP in wireless environment.

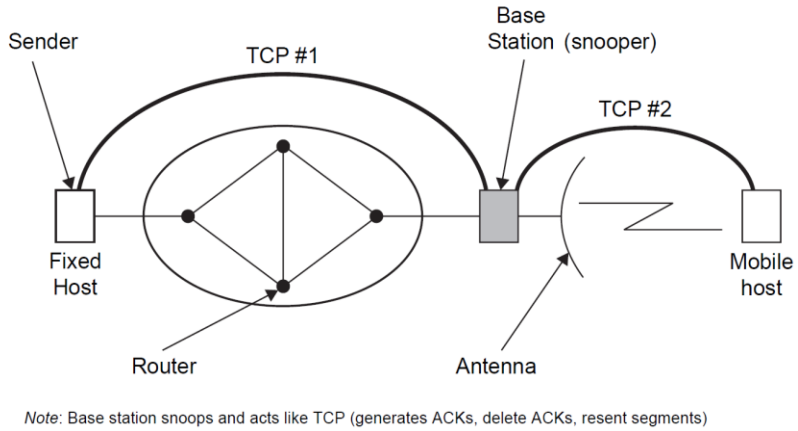


Figure 3.2 Snooping agent TCP in wireless environment.

Table 3.1 Comparison of TCP enhancements for mobility.

Approch	Mechanism	Advantages	Disadvantages
I-TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handoff security problem
Snooping TCP	Snoops data and ACKs, local retrans-mission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problem
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles longterm and frequent disconnections	Bad isolation of wire-less link, overhead due to bandwidth management, security problem
Fast retransmit/fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnecting	Independent of content, works for longer interruptions	Changes in TCP required, MAC independent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space required

- The ***current TCP*** for 2.5G/3G wireless networks describes a profile to ***optimize TCP for Wireless Wide-Area Networks (WWANs)*** such as GSM/GPRS, UMTS, or cdma2000.

4. Discuss about the characteristics to be considered in deploying applications over 2.5/3G wireless links. [May 2018]

- The following characteristics are considered in deploying applications over 2.5/3G wireless links:
  - ✓ Data rates
  - ✓ Latency
  - ✓ Jitter
  - ✓ Packet loss

Based on these characteristics, the following configuration parameters for TCP in a wireless environment have been suggested:

- ***Large window size:***
  - ✓ In wireless systems, TCP should use ***large window sizes*** based on the ***bandwidth delay***.
  - ✓ A large initial window size (more than the typical 1 segment) of ***2 to 4 segments*** may increase performance, particularly for short transmissions.

- ***Limit transmit:***
  - ✓ This is an extension of fast retransmission/fast recovery.
  - ✓ It is useful when small amounts of data are to be transmitted.

- ***Large Maximum Segment Size (MSS):***
  - ✓ The ***larger the MSS*** the ***faster TCP increases the congestion window***.
  - ✓ Link-layers piece the ***Packet Data Units (PDUs)*** for transmit, according to their needs.
    - A large MSS may be used to increase performance.
  - ✓ ***MSS path discovery*** should be used for larger segment sizes.

- ***Selective ACK (SACK):***
  - ✓ SACK allows the ***selective retransmission of packets***.
  - ✓ It is beneficial compared to the standard cumulative scheme.
  - ✓ ***Explicit congestion notification (ECN):***
    - On receiving an IP packet that has experienced congestion,
      - It allows a receiver to inform a sender about congestion in the network
        - ***by setting the ECN-echo flag***,.
  - ✓ This scheme makes it easier to ***distinguish the packet loss <u>due to retransmission errors</u>*** from ***packet loss <u>due to congestion</u>***.

- ***Time-stamp:***
  - ✓ Higher delay spikes can be tolerated by TCP with the help of time-stamps, without experiencing a spurious time-out.
  - ✓ The effect of bandwidth oscillation *(i.e., throughput degradation)* is also reduced.

- ***No header compression:***
  - ✓ ***Header compression**** mechanism does not perform well in the presence of packet losses.
  - ✓ It should not be used.

5. Explain in detail about the following traditional TCPs. **(a) Congestion control** **(b) Slow start** **(c) Fast retransmit / Fast Recovery** **(d) Implications on mobility**	**(16m)**	
6. Describe the working mechanism of traditional TCP.	**(16m)**	**Apr 2017**
7. Describe the basic concepts of congestion control. What are the implications on mobility in traditional TCP?	**(16m)**	**Nov 2017**
8. Explain in detail about traditional TCP and its significance.	**(10m)**	**May 2018**
9. Explain the Congestion control, Slow start and Fast retransmit / Fast Recovery in traditional TCPs.	**(13m)**	**May 2019**

3.2 Traditional TCP

- This section highlights several mechanisms of the transmission control protocol (TCP).
- It influences the efficiency of TCP in a mobile environment.

3.2.1 Congestion control

- The transport layer protocol TCP has been designed for ***fixed networks with fixed end-systems***.
- ***Data transmission*** takes place using network adapters, fiber optics, copper wires, special hardware for routers etc.

- This hardware typically works ***without introducing transmission errors***.
- If the software is good enough, it will not drop packets or flip bits.
- So, if a packet is lost during transmission in a fixed network, it is not because of hardware or software errors.

- ***Congestion at a node:*** The possible reason for a packet loss in a fixed network is a ***temporary overload*** at some point in the transmission path, i.e., a state of congestion at a node.

Scenario for the occurrence of congestion:

- Congestion may appear from time to time.
- It happens even in carefully designed networks.

- The ***packet buffers**** of a router are filled and the router cannot forward the packets fast enough.
- Because the sum of the input rates of packets designed for one output link is higher than the capacity of the output link.
- Now, a router can drop packets.

- A dropped packet is ***lost for the transmission***.
- Then, the ***receiver notices*** a gap in the packet stream.
- Now the receiver does not directly tell the sender which packet is missing
- But, the receiver continues to acknowledge ***all in-sequence packets up to the missing one***.

- The ***sender notices the missing acknowledgement*** for the lost packet and ***assumes a packet loss*** due to congestion.
- ***Retransmitting the missing packet*** and continuing at full sending rate would now be risky. Because this will increase the congestion.
- To mitigate ***(lessen)*** congestion, TCP ***slows down the transmission rate*** dramatically ***(severely)***.

- All other TCP connections experiencing the same congestion do exactly the same, so the congestion is soon resolved.
- This cooperation of TCP connections in the internet is one of the main reasons for its survival.

Compare UDP and TCP

- Using UDP is not a solution.
- Because the throughput is higher compared to a TCP connection.
- As soon as everyone uses UDP, this advantage disappears.

- After that, congestion is standard and data transmission quality is unpredictable.
- Even under heavy load, TCP guarantees at least sharing of the bandwidth.

5.1 Discuss the mechanisms to alter the transmission rate when congestion occurs.

Mechanisms to alter the transmission:

Mechanisms to alter the transmission rate when congestion has resulted are:

Slow start

Fast retransmits and fast recovery

3.2.2 Slow start

- TCP's reaction to a missing acknowledgement is quite drastic ***(severe)***, but it is necessary to get rid ***(clear)*** of congestion quickly.
- The behavior of TCP shown after the detection of congestion is called ***slow start***.

It proceeds as follows:

- The sender always calculates a congestion window for a receiver.
- The start size of the congestion window is one segment (TCP packet).
- The sender sends one packet and waits for acknowledgement.
- If this acknowledgement arrives, the sender increases the congestion window by one, now sending two packets (congestion window = 2).
- After arrival of the two corresponding acknowledgements, the sender again ***adds 2*** to the congestion window, one for each of the acknowledgements.
- Now the congestion window equals 4.
- This scheme doubles the congestion window every time the acknowledgements come back, which takes one ***round trip time*** (RTT).
- This is called the ***exponential growth of the congestion window*** in the slow start mechanism.

Effect of doubling the congestion window:

- It is too dangerous to double the congestion window each time.
  - ✓ Because the steps might become too large.
- The exponential growth stops at the ***congestion threshold***.
- When the congestion window reaches the congestion threshold,
  - ✓ the increase of the transmission rate is linear by adding 1 to the congestion window, each time the acknowledgements come back.

- Linear increase continues
  - ✓ until a time-out at the sender occurs, due to a missing acknowledgement (or)
  - ✓ until the sender detects a gap in transmitted data, because of continuous acknowledgements for the same packet.

3.2.3 Fast retransmit / Fast Recovery

- Two things lead to a reduction of the congestion threshold.
- Sender receiving continuous acknowledgements for the same packet.

This informs the sender of two things.

- The receiver got all packets up to the acknowledged packet in sequence.
- In TCP, a receiver sends acknowledgements only if it receives any packets from the sender.

Fast retransmit:

- Receiving acknowledgements from a receiver also shows that the receiver continuously receives something from the sender.
- The gap in the packet stream is not due to severe congestion, but a simple packet loss due to a transmission error.
- The sender can now retransmit the missing packet(s) before the timer expires.
- This behavior is called ***fast retransmit***.

Fast recovery:

- The receipt of acknowledgements shows that there is no congestion to justify a slow start.
- The sender can continue with the current congestion window.
- The sender performs a ***fast recovery*** from the packet loss.
- This mechanism can improve the efficiency of TCP dramatically.

- The other reason for activating slow start is a time-out due to a missing acknowledgement.
- TCP using fast retransmit/fast recovery interprets this congestion in the network and activates the slow start mechanism.

5.2. Briefly discuss about the implications on mobility.

3.2.4 Implications *(suggestions)* on mobility:

- Slow start is useful mechanism in ***fixed networks***.
- But, if it is used jointly with ***mobile receivers or senders***, it drastically decreases the efficiency of TCP.
- ***Reason:*** The use of *slow start* under the wrong assumptions.
  Example:
  - From a missing acknowledgement, TCP concludes a congestion situation.
  - Missing acknowledgement may also happen in networks with *mobile and wireless end-systems.*

- But, here congestion will not be the main reason for packet loss.

- Error rates on wireless links are ***orders of magnitude**** higher compared to fixed fiber or copper links.
- Packet loss is much more common and cannot be always compensated by layer 2 retransmissions (ARQ) or error correction (FEC).

- Trying to retransmit on layer 2, for example, trigger TCP retransmission if it takes too long.
- Layer 2 now faces the problem of transmitting the same packet twice over a bad link.
- Detecting these duplicates on layer 2 is not an option, because more and more connections use end-to-end encryption, making it impossible to look at the packet.

- Mobility itself can cause packet loss.
- There are many situations where a soft handover from one access point to another is not possible for a mobile end system.
- For example, when using mobile IP, there could still be some packets in transit to the old foreign agent while the mobile node moves to the new foreign agent.
- The old foreign agent may not be able to forward those packets to the new foreign agent or even buffer the packets if disconnection of the mobile node takes too long.
- This packet loss has nothing to do with wireless access but is caused by the problems of rerouting traffic.

- The TCP mechanism detecting missing acknowledgements via time-outs and concluding packet loss due to congestion cannot distinguish between the different causes.

- This is a fundamental design problem in TCP: An error control mechanism (missing acknowledgement due to a transmission error) is misused for congestion control (missing acknowledgement due to network overload).
- In both cases packets are lost (either due to invalid checksums or to dropping in routers). However, the reasons are completely different.TCP cannot distinguish between these two different reasons.
- Explicit congestion notification (ECN) mechanisms are currently discussed and some recommendations have been already given (RFC 3168).
- However, RFC 3155 states that ECN cannot be used as surrogate for explicit transmission error notification.
- Standard TCP reacts with slow start if acknowledgements are missing, which does not help in the case of transmission errors over wireless links and which does not really help during handover.
- This behavior results in a severe performance degradation of an unchanged TCP if used together with wireless links or mobile nodes.

- However, one cannot change TCP completely just to support mobile users or wireless links.
- The same arguments that were given to keep IP unchanged also apply to TCP.
- The installed base of computers using TCP is too large to be changed and, more important, mechanisms such as slow start keep the internet operable.
- Every enhancement to TCP, has to remain compatible with the standard TCP and must not jeopardize (risk) the cautious behavior of TCP in case of congestion.

10. Explain the classical TCP improvement methods to increase TCP's performance in wireless and mobile environments.	**(16m)**	
Discuss the classical TCP improvement methods.	**(16m)**	
Write your understanding on indirect TCP, Snooping TCP, Mobile TCP and transaction oriented TCP.	**(16m)**	**Apr 2017**
Explain any two classical TCP improvements for mobility.	**(08m)**	**Nov 2018**
Draw the overview of classical enhancements to TCP mobility.	**(06m)**	**May 2018**
Describe the basic concepts of Classical TCP and Indirect TCP.	**(13m)**	**Nov 2019**

3.3 Classical TCP improvements

- Several research projects were started with the goal to increase TCP's performance in wireless and mobile environments.
- The methods used in this are:
  - ✓ Indirect TCP
  - ✓ Snooping TCP
  - ✓ Mobile TCP
  - ✓ Fast retransmit/fast recovery
  - ✓ Transmission/time-out freezing
  - ✓ Selective retransmission
  - ✓ Transaction-oriented TCP

10.1. Explain the Indirect TCP method to increase TCP Performance.

3.3.1 Indirect TCP

- Two competing approaches led to the development of indirect TCP (I-TCP) (Bakre, 1995).
- They are:
  - ✓ TCP performs poorly together with wireless links.
  - ✓ TCP within the fixed network cannot be changed.

Concepts:

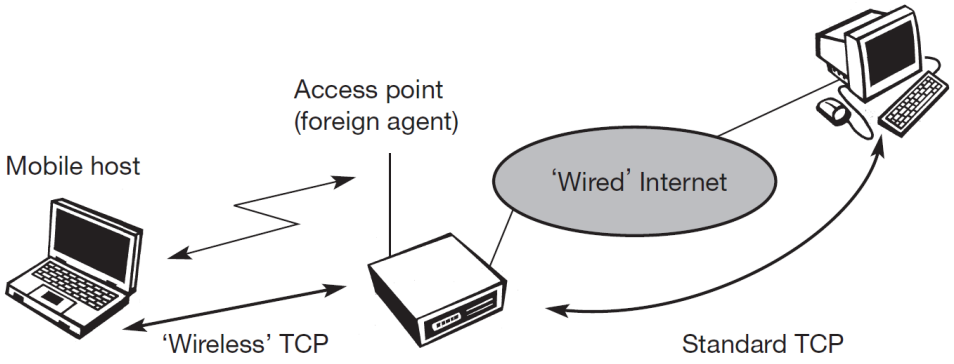


Figure 3.3 Indirect TCP segments a TCP connection into two parts

- I-TCP segments a TCP connection into a fixed part and a wireless part.

- ***Figure 3.3*** shows an example:
  - ✓ The mobile host connected via a wireless link.
  - ✓ An access point to the 'wired' internet where the correspondent host exists.

- ***Standard TCP*** (***i.e., wired TCP***) is used between the fixed computer and the access point.
- No computer in the internet recognizes any changes to TCP.

- Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy.
- The access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host.
- Between the access point and the mobile host, a special TCP, adapted to wireless links, is used.
- However, changing TCP for the wireless link is not a requirement.

- Even an unchanged TCP can benefit from the much shorter round trip time, starting retransmission much faster.
- ***The correct place for segmenting the connection*** between mobile host and correspondent host ***is at the foreign agent of mobile IP***.

- The foreign agent controls the mobility of the mobile host.
- It can also, hand over the connection to the next foreign agent when the mobile host moves on.
- However, one can also imagine separating the TCP connections at a special server, e.g., at the entry point to a mobile phone network (e.g., IWF in GSM, GGSN in GPRS).

Working principle:

- The ***correspondent host*** in the fixed network does not notice the wireless link or the segmentation of the connection.
- The foreign agent acts as a proxy and relays all data in both directions.
- If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host.
- If the mobile host receives the packet, it acknowledges the packet.
- However, this acknowledgement is only used by the foreign agent.

- If a packet is lost on the wireless link due to a transmission error, the correspondent host would not notice this.
- In this case, the foreign agent tries to retransmit this packet locally to maintain reliable data transport.

- Similarly, if the mobile host sends a packet, the foreign agent acknowledges this packet and tries to forward it to the correspondent host.
- If the packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet.
- Packet loss in the wired network is now handled by the foreign agent.

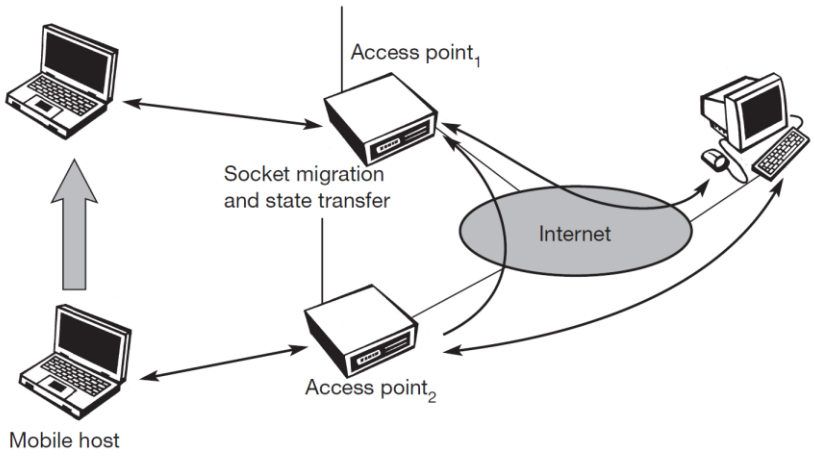


Figure 3.4 Socket and state migration after handover of a mobile host

- I-TCP requires several actions as soon as a handover takes place.
- As ***Figure 3.4*** demonstrates, not only the packets have to be redirected using, e.g., mobile IP.

- In the example shown, the ***access point acts as a proxy*** buffering packets for retransmission.
- After the handover, the old proxy must forward buffered data to the new proxy because it has already acknowledged the data.
- After registration with the new foreign agent, this new foreign agent can inform the old one about its location to enable packet forwarding.
- Besides buffer content, the sockets of the proxy, too, must migrate to the new foreign agent located in the access point.

- The socket reflects the current state of the TCP connection, i.e., sequence number, addresses, ports etc.
- No new connection may be established for the mobile host, and the correspondent host must not see any changes in connection state.

Advantages with I-TCP:

- I-TCP does not have any changes on the TCP protocol.
- Transmission errors on the wireless link cannot propagate in the fixed network, *due to strict partitioning into 2 connections.*
- Short delay between the mobile host and Foreign Agent can be determined, and it was independent of other traffic streams.
- The connection is partitioned, so different transport layer protocol can be used, between the FA and mobile or FA and correspondent node.
    - FA acts as a gate way to translate between different protocols.

Disadvantages:

- End to end semantics TCP is lost due to partitioning.
- If FA crashes, the source will think that the ***correspondent node*** has received the packet it has the acknowledgement from FA.
- Handover will be problematic. The entire packet sent by the correspondent is before handover are buffered by FA and also forwards the packet to mobile.
- At the same time of handover many packets may arrive. All these packets must be forwarding the new packets redirected to it.
- The FA should be trusted entity.

3.3.2 Snooping TCP

8.2. Explain the Snooping TCP method to increase TCP Performance.

What is meant by snooping TCP? (08m – Nov 2017)

Describe the snooping TCP and points out the advantages and disadvantages. (Apr / May 2019)

- One of the drawbacks of I-TCP is ***the segmentation of the single TCP connection into two TCP connections***. This loses the original end-to-end TCP semantic.

- The following TCP enhancement works completely transparently and leaves the TCP end-to-end connection intact ***(in one piece)***.

Main function of the enhancement:

- To buffer data close to the mobile host ***to perform fast local retransmission*** in case of packet loss.
- A good ***place for the enhancement of TCP*** could be ***the foreign agent*** in the Mobile IP context (see **Figure 3.5**).

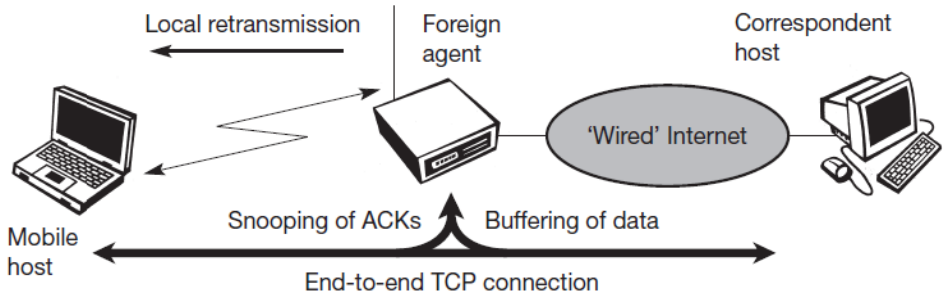


Figure 3.5 Snooping TCP as a transparent TCP extension

Functions of Foreign Agent (FA):

- In this approach, the foreign agent
  - Buffers all packets with destination mobile host.
  - Additionally 'snoops' the packet flow in both directions to recognize acknowledgements.

- Reason for buffering packets toward the mobile node is ***to enable the foreign agent to perform a local retransmission*** in case of packet loss on the wireless link.
- The foreign agent ***buffers every packet until it receives an acknowledgement*** from the mobile host.

- If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, ***either the packet or the acknowledgement has been lost***.

- Alternatively, the foreign agent could receive a ***duplicate ACK***, it also shows the loss of a packet.

- Now the ***foreign agent retransmits the packet*** directly from the buffer, performing a much ***faster retransmission*** compared to the correspondent host.

- To remain transparent, the foreign agent must not acknowledge data to the correspondent host.
- This would make the correspondent host believe that the mobile host had received the data and would violate the end-to-end semantic in case of a foreign agent failure.
- However, the foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host.

- If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission.
- The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host.
- This avoids unnecessary traffic on the wireless link.

- Data transfer from the mobile host with destination correspondent host works as follows.
- The foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP.
- As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host.
- The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the correspondent host by TCP.

Advantages:

- End to end TCP Segments are preserved.
- As the enhancements are done in Foreign Agent, CN need not be changed. No concept of handover is needed.
- It does not need all the Foreign Agent to use enhancements. If not done, the scheme follows the standard TCP concept.

Disadvantages:

- Snooping TCP does not isolate the behavior of the wireless link as well as ITCP.
- Retransmitting data from the foreign agent may not work because many security schemes prevent replay attacks.
- Security schemes are needed: Encrypting end-to-end is the way many applications work so it is not clear how this scheme could be used in the future.

3.3.3 Mobile TCP

8.3 Explain the Mobile TCP method to increase TCP Performance. (Or)
How the mobile TCP is playing the important role in mobile transport layers? Explain with overview of the classical enhancements to TCP for mobility and compare with 2./3G wireless networks. [5+5+6m] [May 2018] (Or)
How does mobile TCP play an important role in Mobile transport layer? Discuss in detail. (08m) [Nov 2018]

- Dropping packets due to a handover or higher bit error rates is not the only phenomenon of wireless links and mobility.
- The occurrence of ***lengthy and/or frequent disconnections*** is another problem.
- Quite often mobile users cannot connect at all.
- One example is islands of wireless LANs inside buildings but no coverage of the whole campus.

What happens to standard TCP in the case of disconnection?

- A TCP ***sender tries to retransmit data*** controlled by a ***retransmission timer***.
- The timer doubles with each unsuccessful retransmission attempt, up to a maximum of one minute (the initial value depends on the round trip time).
- This means that the sender tries to retransmit an unacknowledged packet every minute and will give up after 12 retransmissions.

What happens if connectivity is back earlier than this?

- No data is successfully transmitted for a period of one minute.
- The retransmission time-out is still valid and the sender has to wait.

- The sender also goes into slow-start because it assumes congestion.

What happens in the case of I-TCP if the mobile is disconnected?

- The proxy has to buffer more and more data, so the longer the period of disconnection, the more buffer is needed.
- If a handover follows the disconnection, even more state has to be transferred to the new proxy.
- The snooping approach also suffers from being disconnected.
- The mobile will not be able to send ACKs so, snooping cannot help in this situation.

Concept:

- The 'M-TCP (mobile TCP) 1' approach has the same goals as I-TCP and snooping TCP
- The goal is 'to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems'.
- M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover.
- Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.

Functions of SH:

- M-TCP splits the TCP connection into two parts as I-TCP does.
- An unmodified TCP is used on the ***Standard Host-supervisory host*** (SH) ***connection***, while an optimized TCP is used on the SH-MH connection.
- The supervisory host is responsible for exchanging data between both parts similar to the proxy in ITCP (see Figure 3.3).
- The M-TCP approach assumes a relatively low bit error rate on the wireless link.
- Therefore, it does not perform caching/retransmission of data via the SH.
- If a packet is lost on the wireless link, it has to be retransmitted by the original sender.
- This maintains the TCP end-to-end semantics.

- The ***SH monitors all packets sent to the MH and ACKs returned from the MH***.
- If the ***SH does not receive an ACK*** for some time, it assumes that the MH is disconnected.
- It then chokes the sender by ***setting the sender's window size to 0***.

- ***Setting the window size to 0 forces the sender to go into persistent mode, i.e., the state of the sender will not change no matter how long the receiver is disconnected.***
- ***This means that the sender will not try to retransmit data.***
- ***As soon as the SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value.***
- The sender can continue sending at full speed.
- This mechanism does not require changes to the sender's TCP.

Wireless side connections

- The wireless side uses an adapted TCP that can recover from packet loss much faster.
- This modified TCP does not use slow start, thus, M-TCP needs a bandwidth manager to implement fair sharing over the wireless link.

Advantages:

- It maintains the TCP end-to-end semantics.
  - The SH does not send any ACK itself, but forwards the ACKs from the MH.
- If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections ***by simply shrinking the sender's window to 0***.
- Lost packets will be automatically retransmitted to the new SH.

Disadvantages:

- SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender.
- A modified TCP on the wireless link requires
  - modifications in the ***MH protocol software***, and
  - new network elements like the ***bandwidth manager***.

3.4 Explain the Fast retransmit/fast recovery method to increase TCP Performance.

3.3.4 Fast retransmit/fast recovery

- ***Moving to a new foreign agent*** can ***cause packet loss or time out*** at mobile hosts or corresponding hosts.
- TCP concludes this as congestion and goes into slow start, although there is no congestion.

- *It is already discussed about the mechanisms of fast recovery/fast retransmit a host can use after receiving duplicate acknowledgements, thus concluding a packet loss without congestion.*
- The idea presented by Caceres (1995): Artificially force the fast retransmit behavior on the mobile host and correspondent host side.

- The mobile host registers at a new foreign agent using mobile IP,
  - immediately it starts to send duplicated acknowledgements to correspondent hosts.
- The proposal is to send three duplicates.
- This forces the corresponding host to go ***into fast retransmit mode*** and ***not to start slow start***, i.e., the correspondent host continues to send with the same rate, it did before the mobile host moved to another foreign agent.

- As the mobile host may also go into slow start after moving to a new foreign agent, this approach ***additionally*** puts the mobile host into fast retransmit.
- The mobile host retransmits all unacknowledged packets using the current congestion window size without going into slow start.

Advantages:

- ✓ Simplicity.
- ✓ Only minor changes in the mobile host's software already result in a performance increase.
- ✓ No foreign agent or correspondent host has to be changed.

Disadvantages:

- ✓ The insufficient isolation of packet losses.
- ✓ Forcing fast retransmission ***increases the efficiency***, but ***retransmitted packets have to cross the whole network*** between correspondent host and mobile host.
- ✓ The approach focuses on ***loss due to handover***. But, packet loss due to wireless link problems is not considered.
- ✓ This approach ***requires more cooperation between the mobile IP and TCP layer***, so it is harder to change one without manipulating the other.

3.5 Explain the Transmission/time-out freezing method to increase TCP Performance.

3.3.5 Transmission/time-out freezing

- The approaches presented so far can handle
  - short interruptions of the connection,

- either due to handover or transmission errors on the wireless link,

- Some approaches designed for longer interruptions of transmission.

- Examples are the use of mobile hosts in a car driving into a tunnel, which loses its connection to, e.g., a satellite (however, many tunnels and subways provide connectivity via a mobile phone), or a user moving into a cell with no capacity left over.
- In this case, the mobile phone system will interrupt the connection.
- The reaction of TCP would be a disconnection after a time out.

- The MAC layer will ***already notice the connection problems***, before ***the connection is actually interrupted*** from a TCP point of view.
- Additionally, the MAC layer ***knows the real reason for the interruption***, and
  - it does not assume congestion as in the TCP.
- The MAC layer can inform the TCP layer
  - about the upcoming loss of connection ***or*** that the current interruption is not caused by congestion.
- TCP can now stop sending and 'freezes' the current state of its congestion window and further timers.

- If the MAC layer notices the upcoming interruption soon enough, both the mobile and correspondent hosts will be informed.
- With a fast interruption of the wireless link, ***additional mechanisms in the access point are needed*** to inform the correspondent host about the reason for interruption.
- Otherwise, the correspondent host goes into slow start assuming congestion and finally breaks the connection.

- When the MAC layer detects connectivity again, it signals to TCP that it can resume operation, exactly at the same point where it was forced to stop.
- For TCP time simply does not advance, so no timers expire.

Advantages:

- ✓ It offers a way to resume TCP connections even after longer interruptions of the connection.
- ✓ It is independent of other TCP mechanisms, *such as acknowledgements or sequence numbers*, so it can be used together with encrypted data.

Disadvantages:

- ✓ Changing the software on the mobile host is not enough. For more effectiveness the correspondent host must also be changed.
- ✓ All mechanisms depend on the capability of the MAC layer, to detect future interruptions.
- ✓ Freezing the state of TCP does not help ***in case of some encryption schemes that use time-dependent random numbers***.
- ✓ These schemes need resynchronization after interruption.

3.6 Explain the selective retransmission method to increase TCP Performance.
Illustrate the basic principles of selective retransmission. When such situations are warranted? Discuss. [Nov 2019]

3.3.6 Selective retransmission

- A very useful extension of TCP is ***selective retransmission***.
- TCP acknowledgements are cumulative, i.e., they acknowledge in-order receipt of packets up to a certain packet.
- If a single packet is lost, the sender has to retransmit everything starting from the lost packet (go-back-n retransmission).
- This wastes bandwidth, not just in the case of a mobile network, but for any network.
- Using RFC 2018, TCP can indirectly request a selective retransmission of packets.
- The ***receiver can acknowledge single packets***, not only trains of in-sequence packets.
- The sender can now ***determine precisely which packet is needed*** and can ***retransmit*** it.

Advantages:

- ✓ A sender retransmits only the lost packets.
- ✓ This reduces the bandwidth requirements and is extremely helpful in slow wireless links.
- ✓ The gain in efficiency is not restricted to wireless links and mobile environments.
- ✓ Using selective retransmission is also beneficial in all other networks.

Disadvantages:

- ✓ More complex software on the receiver side, because now more buffers are necessary to resequence the data and to wait for filling the gaps.
- ✓ But while memory sizes and CPU performance permanently increase, but the bandwidth *of the air interface* remains almost the same.

3.7 Explain the Transaction oriented TCP method to increase TCP performance.

3.3.7 Transaction-oriented TCP

- Assume an application running on the mobile host that sends a short request to a server from time to time, which responds with a short message.
- If the application requires reliable transport of the packets, it may use TCP

- Using TCP will require several packets over the wireless link.
- First, TCP uses a three-way handshake to establish the connection.
- At least one additional packet is usually needed for transmission of the request.
- It requires three more packets to close the connection *via a three-way handshake*.

- Assuming connections with a lot of traffic or with a long duration, this overhead is negligible.
- But in an example of only one data packet, TCP may need seven packets altogether.

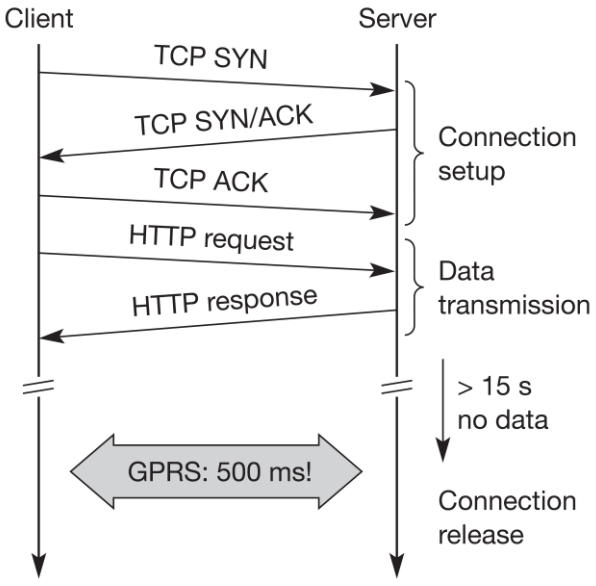


Figure 3.6 Example TCP connection setup overhead

- Figure 3.6 shows an example for the overhead introduced by using TCP over GPRS in a web scenario.
- Web services are based on HTTP which requires a reliable transport system. In the internet, TCP is used for this purpose.
- The TCP connection has to be established before a request can be transmitted. This already requires three messages.
- If GPRS is used as wide area transport system, one-way delays of 500 ms and more are common.
- The setup of a TCP connection already takes more than a second.

Concept:

- This led to the development of a transaction-oriented TCP (T/TCP, RFC 1644).
- T/TCP can combine packets for ***connection establishment and connection release*** with user data packets.
- This can reduce the number of packets to 2 instead of 7.
- Similar considerations led to the development of a transaction service in WAP.

Advantage:

- The ***reduction in the overhead*** *than the* ***standard TCP consists*** for the purpose of ***connection setup and connection release***.

Disadvantage:

- The T/TCP is not the original TCP, so ***it requires changes*** in the mobile host and all correspondent hosts.
- T/TCP exhibits several security problems.

3.4 Overview of classical enhancements to TCP for mobility

4 Compare various classical enhancements to TCP for mobility.

- Table 3.2 shows an overview of the classical mechanisms presented together with some advantages and disadvantages.
- ***Approaches can be combined:***
  - ✓ The approaches are not all exclusive, but can be combined.
  - ✓ ***For example:*** Selective retransmission can be used together with the others. Even it can be applied to fixed networks.

  An ***additional scheme*** that can be used to reduce TCP overhead is header compression.

- ***Larger headers:***
  - ✓ Using tunneling schemes *as in mobile IP* together with TCP, results in protocol headers of 60 byte in case of IPv4 and 100 byte for IPv6 due to the larger addresses.
  - ✓ Many fields in the IP and TCP header remain unchanged for every packet.
  - ✓ Just transmitting the differences is often sufficient.
  - ✓ Header compression experiences difficulties when error rates are high.

- With the new possibilities of wireless wide area networks (WWAN) and their tremendous success, the focus of research has shifted more and more towards these 2.5G/3G networks.
- Up to now there are no final solutions to the problems arising when TCP is used in WWANs. However, some guidelines do exist.

Table 3.2 Overview of classical enhancements to TCP for mobility

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover, security problems
Snooping TCP	Snoops data and acknowledgements, local retransmission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problems
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management, security problems
Fast retransmit/ fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnection	Independent of content, works for longer interruptions	Changes in TCP required, MAC dependent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space needed
Transaction-oriented TCP	Combines connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent, security problems

3.3 TCP over 2.5/3G wireless networks

5 Discuss the TCP over 2.5/3G networks. (or)

Explain in detail about the basic concepts of TCP over 2.5/3G wireless network. (08m - Nov 2017)

Explain in detail about the TCP over 3G wireless networks. (16m) [Nov 2018]

How the mobile TCP is playing the important rate in mobile transport layer? Explain with overview of the classical enhancements to TCP for mobility and compare with 2.3G wireless networks. (05+05+05m) [May 2018]

- The current internet draft for TCP over 2.5G/3G wireless networks describes a profile for optimizing TCP over today's and tomorrow's wireless WANs such as GSM/GPRS, UMTS, or CDMA2000.
- The configuration optimizations recommended in this draft can be found in most of today's TCP implementations so this draft does not require an update of millions of TCP stacks.
- The focus on 2.5G/3G for transport of internet data is important as already more than 1 billion people use mobile phones.
- It is obvious that the mobile phone systems will also be used to transport arbitrary internet data.

The following characteristics have to be considered when deploying applications over 2.5G/3G wireless links:

- ***Data rates:***
  - ✓ Typical data rates
    - 2.5G systems are 10–20 Kbit/s uplink and 20–50 Kbit/s downlink
    - 3G and future 2.5G systems:
      - Uplink data rates 64 Kbit/s and Downlink data rates 115–384 Kbit/s.
  - ✓ Typically, data rates are asymmetric as it is expected that users will download more data compared to uploading. Uploading is limited by the limited battery power.

- ***Latency:***
  - ✓ All wireless systems comprise complicated algorithms for error correction and protection.
    - ***Example:*** Forward Error Correction (FEC), check summing, and interleaving.
  - ✓ FEC and interleaving allow the round trip time (RTT) grow to several hundred milliseconds up to some seconds.
  - ✓ The current GPRS standard specifies an average delay of less than two seconds for the transport class with the highest quality.

- ***Jitter:***
  - ✓ Wireless systems suffer from large ***delay variations*** or ***'delay spikes'***.
  - ✓ Reasons for sudden increase in the latency are:
    - link outages due to temporal loss of radio coverage,

- blocking due to high-priority traffic, or
- handovers.

✓ Handovers are quite often only virtually seamless with outages reaching from some 10 ms (handover in GSM systems) to several seconds (intersystem handover).

➢ ***Packet loss:***

✓ Packets might be lost during handovers or due to corruption.

✓ Recovery at the link layer appears as jitter to the higher layers.

Characteristics of the following configuration parameters to adapt TCP to wireless environments:

➢ ***Large windows:***

- TCP should support large enough window sizes based on the ***bandwidth delay product*** faced in wireless systems.
- Accomplished through: Windows scale option (RFC 1323) and larger buffer sizes. (typical buffer size settings of 16 Kbyte are not enough).
- Larger initial window (more than the typical one segment) of 2 to 4 segments will increase the performance in short transmissions (a few segments in total).

➢ ***Limited transmit:***

- This mechanism, defined in RFC 3042 is an extension of Fast Retransmission/Fast Recovery
- It is useful small amount data transmission (e.g., web service requests).

➢ ***Large MTU:***

- The larger the MTU (Maximum Transfer Unit) the TCP increases the congestion window faster.
- Link layers fragment the PDUs for transmission according to their needs.
- Large MTUs may be used to increase performance.

➢ ***Selective Acknowledgement (SACK):***

- SACK (RFC 2018) allows the selective retransmission of packets.
- It is always beneficial compared to the standard cumulative scheme.

➢ ***Explicit Congestion Notification (ECN):***

- ECN as defined in RFC 3168.
- It allows a receiver to inform a sender about the congestion in the network, by setting the ECN-Echo flag ***on receiving an IP packet*** that has experienced congestion.
- This mechanism is useful to ***distinguish packet loss due to transmission errors from packet loss due to congestion***.
- This can only be achieved when ECN capable routers are deployed in the network.

- ***Timestamp:***
  - TCP connections with large windows get benefit from more frequent RTT samples provided with timestamps.
  - With the help of timestamps the higher delay spikes can be tolerated by TCP without experiencing a spurious timeout.
  - The effect of bandwidth oscillation is also reduced.

- ***No header compression:***
  - The TCP header compression mechanism according to RFC 1144 does not perform well in the presence of packet losses, so this mechanism should not be used.
  - Header compression according to RFC 2507 or RFC 1144 is not compatible with TCP options such as SACK or timestamps.

Note: These recommendations are still at the draft-stage, they are already used in i-mode running over FOMA as deployed in Japan and are part of the WAP 2.0 standard (aka TCP with wireless profile).

Header compression: Headers of typical UDP or TCP packets can be compressed down. This largely removes the negative impact of large IP headers and allows efficient use of bandwidth on low and medium speed links.

Packet Buffer: A packet buffer is memory space set aside for storing packets awaiting transmission over networks or storing packets received over networks.

Orders of Magnitude: The scientific notation of very large numbers in which each order of magnitude is ten times the previous one.

Intersystem handover: *Example:* From a WLAN to a cellular system using Mobile IP without using additional mechanisms such as multicasting data to multiple access points

UNIT III
MOBILE TRANSPORT LAYER

TWO MARKS

1. Define Transmission Control Protocol (TCP).

The TCP is the connection-oriented transport layer protocol designed to operate on the top of the datagram network layer IP.

2. Give the two widely used protocols in TCP/IP.

The two widely used protocols are known under the collective name TCP/IP.

- TCP provides a ***reliable end-to-end byte stream transport***.
- The ***segmentation and reassembly of the messages*** are handled by IP, not by TCP.

3. Define TCP/IP in wire networks.

TCP/IP in wire networks:

- TCP was primarily designed for wired networks.
- Its parameters were selected to maximize its performance on wired networks.
- Here, the packet delays and losses are caused mainly by ***congestion***.
- In wired networks, random bit error rate is negligible.

4. Describe TCP/IP in wireless networks.

TCP/IP in wireless networks:

- In a wireless network, ***packet losses*** occur due to ***handoff or fading*** and can be random.
- In wireless network, when TCP responds to packet losses by invoking congestion control or avoidance algorithm, results in a degraded end-to-end performance.
- A wireless environment violates many of the assumptions made by TCP.

5. List out the classification of TCP.

They can be classified into three categories.

1. Explicit Loss Notification (ELN) option.
2. Link-layer protocols
3. Split TCP connection protocol

6. What are the techniques used to provide reliability in Link layer protocols?

Link-layer protocols provides local reliability using techniques such as

- ✓ Forward error correction (FEC)
- ✓ Retransmission of lost packets in response to automatic repeat request (ARQ) messages

7. What is meant by Split TCP connection protocol?

Split TCP connection protocol that breaks the end-to-end TCP connection into two parts at the base station,

a. One between the sender and the base station.
b. Other between the base station and the receiver

8. List out the cases of End-to-end TCP protocols.

In ***the End-to-end TCP protocols*** case

- The link-layer ARQ mechanism is used to improve the error rate faced by TCP.
- The IS-95 CDMA data stack uses this approach.

9. How to adjust the congestion window in case of Link-layer protocols?

In the ***Link-layer protocols*** case,

- Network layer software is modified at the base station, to monitor every passing packet in either direction.
- Cache packets at the base station are used and local retransmissions across wireless links are performed.

10. How to adjust the congestion window in case of Split TCP connection protocol?

In ***the Split TCP connection protocol*** case,

- The TCP mode wireless portion is separated from the fixed portion.
- With split TCP, TCP may get ACK even before the packet is successfully delivered to the receiver.
- It also involves software overhead.

11. What are the schemes used to improve TCP's performance in wireless and mobile environment?

The schemes used to improve TCP's performance in wireless and mobile environment are:

- ✓ Indirect TCP (I-TCP)
- ✓ Snooping TCP
- ✓ Mobile TCP (M-TCP)
- ✓ Fast retransmit/fast recovery
- ✓ Transmission/time-out freezing
- ✓ Selective retransmission

12. Draw the Split connection (indirect) TCP in wireless environment.

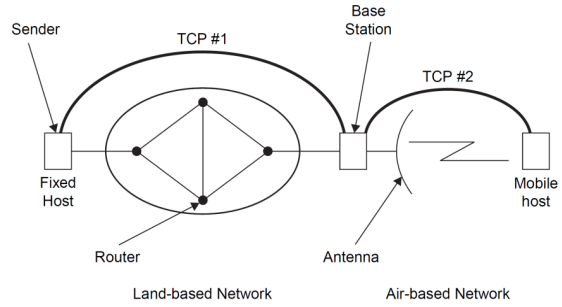


Figure Split connection (indirect) TCP in wireless environment.

13. Draw the Snooping agent TCP in wireless environment.

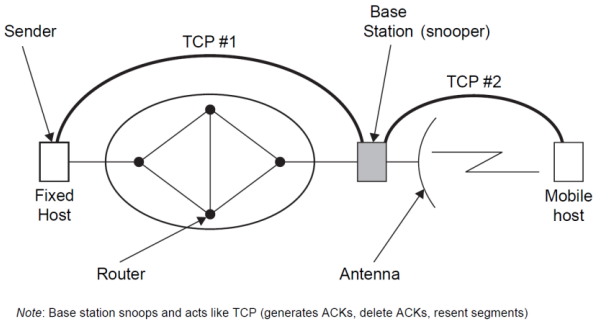


Figure Snooping agent TCP in wireless environment.

14. Compare TCP enhancements for mobility.

Approch	Mechanism	Advantages	Disadvantages
I-TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handoff security problem
Snooping TCP	Snoops data and ACKs, local retrans-mission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problem
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles longterm and frequent disconnections	Bad isolation of wire-less link, overhead due to bandwidth management, security problem
Fast retransmit/fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnecting	Independent of content, works for longer interruptions	Changes in TCP required, MAC independent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space required

15. Write the characteristics that are deploying applications over 2.5 / 3G wireless inks.

The following characteristics are considered in deploying applications over 2.5/3G wireless links:

- ✓ Data rates
- ✓ Latency
- ✓ Jitter
- ✓ Packet loss

16. List out the configuration parameters for TCP in a wireless environment.

Configuration parameters for TCP in a wireless environment have been suggested:

- Large window size
- Limit transmit
- Large Maximum Segment Size (MSS)
- Selective ACK (SACK)
- Time-stamp
- No header compression

17. Define Large window size.

Large window size:

- ✓ In wireless systems, TCP should use ***large window sizes*** based on the ***bandwidth delay***.
- ✓ A large initial window size (more than the typical 1 segment) of ***2 to 4 segments*** may increase performance, particularly for short transmissions.

18. Define Limit transmit.

Limit transmit:

- ✓ This is an extension of fast retransmission/fast recovery.
- ✓ It is useful when small amounts of data are to be transmitted.

19. Define Large Maximum Segment Size (MSS).

Large Maximum Segment Size (MSS):

- ✓ The ***larger the MSS*** the ***faster TCP increases the congestion window***.
- ✓ Link-layers piece the ***Packet Data Units (PDUs)*** for transmit, according to their needs.
  - A large MSS may be used to increase performance.
- ✓ ***MSS path discovery*** should be used for larger segment sizes.

20. Define Selective ACK (SACK).

Selective ACK (SACK):

- ✓ SACK allows the ***selective retransmission of packets***.
- ✓ It is beneficial compared to the standard cumulative scheme.
- ✓ ***Explicit congestion notification (ECN):***
  - On receiving an IP packet that has experienced congestion,
    - It allows a receiver to inform a sender about congestion in the network
      - ***by setting the ECN-echo flag***,.
- ✓ This scheme makes it easier to ***distinguish the packet loss <u>due to retransmission errors</u>*** from ***packet loss <u>due to congestion</u>***.

21. What is Time-stamp?

Time-stamp:

- ✓ Higher delay spikes can be tolerated by TCP with the help of time-stamps, without experiencing a spurious time-out.
- ✓ The effect of bandwidth oscillation *(i.e., throughput degradation)* is also reduced.

22. Define Congestion control.

Congestion at a node: The possible reason for a packet loss in a fixed network is a ***temporary overload*** at some point in the transmission path, i.e., a state of congestion at a node.

23. What is congestion avoidance algorithm? [Nov 2018]

Mechanisms to alter the transmission rate when congestion has resulted are:

Slow start

Fast retransmits and fast recovery

24. Briefly write about the scenario for the occurrence of congestion.

Scenario for the occurrence of congestion:

- The ***packet buffers**** of a router are filled and the router cannot forward the packets fast enough.
- Because the sum of the input rates of packets designed for one output link is higher than the capacity of the output link.
- Now, a router can drop packets. A dropped packet is ***lost for the transmission***.

25. What are the mechanisms followed to alter the transmission rate when congestion occurred?

Mechanisms to alter the transmission rate when congestion has resulted are:

- Slow start
- Fast retransmits and fast recovery

26. What is meant by slow start mechanism?

Slow start

- ✓ The behavior of TCP shown after the detection of congestion is called ***slow start***.
- ✓ The sender always calculates a congestion window for a receiver.
- ✓ This scheme doubles the congestion window every time the acknowledgements come back, which takes one ***round trip time*** (RTT).
- ✓ This is called the ***exponential growth of the congestion window*** in the slow start mechanism.

27. Define the term slow start mechanism and fast retransmit algorithm in TCP. [May 2018]

(Combine with Qn. 28)

What is the effect of doubling the congestion window?

Effect of doubling the congestion window:

- ➢ It is too dangerous to double the congestion window each time.
  - ✓ Because the steps might become too large.
- ➢ The exponential growth stops at the ***congestion threshold***.
- ➢ When the congestion window reaches the congestion threshold,
  - ✓ The increase of the transmission rate is linear by adding 1 to the congestion window, each time the acknowledgements come back.

Fast retransmit / Fast Recovery

28. What is meant by fast retransmit? (or) Define fast retransmit. (Nov 2017)

Fast retransmit:

If the gap in the packet stream is not due to severe congestion and a simple packet loss due to a transmission error then sender can now retransmit the missing packet(s) before the timer expires. This behavior is called ***fast retransmit***.

29. What is meant by fast recovery?

Fast recovery:

The receipt of acknowledgements shows that there is no congestion to justify a slow start. The sender can continue with the current congestion window. The sender performs a ***fast recovery*** from the packet loss. This mechanism can improve the efficiency of TCP dramatically.

Implications *(suggestions)* **on mobility:**

30. Mention the various implications of mobility. [Nov 2019]

- ➢ Slow start is useful mechanism in ***fixed networks***.
- ➢ But, if it is used jointly with ***mobile receivers or senders***, it drastically decreases the efficiency of TCP.

31. What the situations for the use of slow starts under wrong assumptions?

The use of *slow start* under the wrong assumptions.

- o From a missing acknowledgement, TCP concludes a congestion situation.
- o Missing acknowledgement may also happen in networks with *mobile and wireless end-systems.* But, here congestion will not be the main reason for packet loss.

Classical TCP improvements

32. What are the methods used to increase TCP's performance in wireless and mobile environments? (or) Give any four schemes to improve the TCPs performance in wireless networks. (Apr/May 2019)

- The methods used to increase TCP's performance in wireless and mobile environments are:
  - ✓ Indirect TCP
  - ✓ Snooping TCP
  - ✓ Mobile TCP
  - ✓ Fast retransmit/fast recovery
  - ✓ Transmission/time-out freezing
  - ✓ Selective retransmission
  - ✓ Transaction-oriented TCP

Indirect TCP

33. What are the two competing approaches led to the development of indirect TCP? (Or) What is I-TCP? List its merits and demerits. [Nov 2018] *(combine Qn. No. 33 & 34)*

- Two competing approaches led to the development of indirect TCP (I-TCP) (Bakre, 1995).
- They are:
  - ✓ TCP performs poorly together with wireless links.
  - ✓ TCP within the fixed network cannot be changed.

34. What are the advantages of I-TCP?

Advantages with I-TCP:

- I-TCP does not have any changes on the TCP protocol.
- Transmission errors on the wireless link cannot propagate in the fixed network, *due to strict partitioning into 2 connections.*
- Short delay between the mobile host and Foreign Agent can be determined, and it was independent of other traffic streams.
- The connection is partitioned, so different transport layer protocol can be used, between the FA and mobile or FA and correspondent node.
  - o FA acts as a gate way to translate between different protocols.

35. What are the disadvantages of Indirect TCP? [Apr 2017]

Disadvantages:

- End to end semantics TCP is lost due to partitioning.
- If FA crashes, the source will think that the ***correspondent node*** has received the packet it has the acknowledgement from FA.
- Handover will be problematic. The entire packet sent by the correspondent is before handover are buffered by FA and also forwards the packet to mobile.

Snooping TCP

36. What are the functions of Foreign agent?

Functions of Foreign Agent (FA):

- In this approach, the foreign agent
  - Buffers all packets with destination mobile host.
  - Additionally 'snoops' the packet flow in both directions to recognize acknowledgements.

37. What are the advantages of snooping TCP?

Advantages Snooping TCP:

- End to end TCP Segments are preserved.
- As the enhancements are done in Foreign Agent, CN need not be changed. No concept of handover is needed.
- It does not need all the Foreign Agent to use enhancements. If not done, the scheme follows the standard TCP concept.

38. What are the disadvantages of snooping TCP?

Disadvantages Snooping TCP:

- Snooping TCP does not isolate the behavior of the wireless link as well as ITCP.
- Retransmitting data from the foreign agent may not work because many security schemes prevent replay attacks.
- Security schemes are needed: Encrypting end-to-end is the way many applications work so it is not clear how this scheme could be used in the future.

39. What happens to standard TCP in the case of disconnection?

- A TCP ***sender tries to retransmit data*** controlled by a ***retransmission timer***.
- The timer doubles with each unsuccessful retransmission attempt, up to a maximum of one minute (the initial value depends on the round trip time).
- This means that the sender tries to retransmit an unacknowledged packet every minute and will give up after 12 retransmissions.

40. What happens if connectivity is back earlier than this?

- No data is successfully transmitted for a period of one minute.
- The retransmission time-out is still valid and the sender has to wait.
- The sender also goes into slow-start because it assumes congestion.

41. What happens in the case of I-TCP if the mobile is disconnected?

- The proxy has to buffer more and more data, so the longer the period of disconnection, the more buffer is needed.
- If a handover follows the disconnection, even more state has to be transferred to the new proxy.
- The snooping approach also suffers from being disconnected.
- The mobile will not be able to send ACKs so, snooping cannot help in this situation.

42. What is the concept of M-TCP?

- The 'M-TCP (mobile TCP) 1' approach has the same goals as I-TCP and snooping TCP

- The goal is 'to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems'.
- M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover.
- Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.

43. What are the functions of SH (*Standard Host-supervisory host* (SH) *connection*)? (Or) How the destination correspondent host works? [May 2018]

Functions of SH:

- The ***SH monitors all packets sent to the MH and ACKs returned from the MH***.
- If the ***SH does not receive an ACK*** for some time, it assumes that the MH is disconnected.
- It then chokes the sender by ***setting the sender's window size to 0***.

44. Mention the advantages of Mobile TCP? [Apr 2017]

Advantages of M-TCP:

- It maintains the TCP end-to-end semantics.
  - The SH does not send any ACK itself, but forwards the ACKs from the MH.
- If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections ***by simply shrinking the sender's window to 0***.
- Lost packets will be automatically retransmitted to the new SH.

45. What are the advantages of M-TCP?

Disadvantages of M-TCP:

- SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender.
- A modified TCP on the wireless link requires
  - modifications in the ***MH protocol software***, and
  - new network elements like the ***bandwidth manager***.

Fast retransmit/fast recovery

46. Write about fast recovery/fast retransmit.

- The idea presented by Caceres (1995): Artificially force the fast retransmit behavior on the mobile host and correspondent host side.
- The mobile host registers at a new foreign agent using mobile IP,
  - immediately it starts to send duplicated acknowledgements to correspondent hosts.
- This forces the corresponding host to go ***into fast retransmit mode*** and ***not to start slow start***, i.e., the correspondent host continues to send with the same rate, it did before the mobile host moved to another foreign agent.

47. What are the advantages of Fast retransmit/fast recovery?

Advantages of Fast retransmit/fast recovery:

- ✓ Simplicity.
- ✓ Only minor changes in the mobile host's software already result in a performance increase.

- ✓ No foreign agent or correspondent host has to be changed.

48. What are the disadvantages of Fast retransmit/fast recovery?

Disadvantages of Fast retransmit/fast recovery:

- ✓ The insufficient isolation of packet losses.
- ✓ Forcing fast retransmission ***increases the efficiency***, but ***retransmitted packets have to cross the whole network*** between correspondent host and mobile host.
- ✓ The approach focuses on ***loss due to handover***. But, packet loss due to wireless link problems is not considered.
- ✓ This approach ***requires more cooperation between the mobile IP and TCP layer***, so it is harder to change one without manipulating the other.

Transmission/time-out freezing

49. Write the concept of transmission/time-out freezing.

- ➢ The MAC layer will ***notice the connection problems***, before ***the connection is actually interrupted*** from a TCP point of view.
- ➢ The MAC layer can inform the TCP layer about the loss of connection ***or*** that the current interruption is not caused by congestion.
- ➢ TCP can now stop sending and 'freezes' the current state of its congestion window and further timers.

50. What are the advantages of transmission/time-out freezing?

Advantages:

- ✓ It offers a way to resume TCP connections even after longer interruptions of the connection.
- ✓ It is independent of other TCP mechanisms, *such as acknowledgements or sequence numbers*, so it can be used together with encrypted data.

51. What are the disadvantages of transmission/time-out freezing?

Disadvantages:

- ✓ Changing the software on the mobile host is not enough. For more effectiveness the correspondent host must also be changed.
- ✓ All mechanisms depend on the capability of the MAC layer, to detect future interruptions.
- ✓ Freezing the state of TCP does not help ***in case of some encryption schemes that use time-dependent random numbers***.
- ✓ These schemes need resynchronization after interruption.

Selective retransmission

52. Write the concept of selective retransmission.

- ➢ Using RFC 2018, TCP can indirectly request a selective retransmission of packets.
- ➢ The ***receiver can acknowledge single packets***, not only trains of in-sequence packets.
- ➢ The sender can now ***determine precisely which packet is needed*** and can ***retransmit*** it.

53. What are the advantages of selective retransmission?

Advantages:

- ✓ A sender retransmits only the lost packets.
- ✓ This reduces the bandwidth requirements and is extremely helpful in slow wireless links.
- ✓ The gain in efficiency is not restricted to wireless links and mobile environments.
- ✓ Using selective retransmission is also beneficial in all other networks.

54. What are the disadvantages of selective retransmission?

Disadvantages:

- ✓ More complex software on the receiver side, because now more buffers are necessary to resequence the data and to wait for filling the gaps.
- ✓ But while memory sizes and CPU performance permanently increase, but the bandwidth *of the air interface* remains almost the same.

Transaction-oriented TCP

55. What is the concept behind transaction-oriented TCP?

Concept of transaction-oriented TCP:

- ➢ This led to the development of a transaction-oriented TCP (T/TCP, RFC 1644).
- ➢ T/TCP can combine packets for ***connection establishment and connection release*** with user data packets.
- ➢ This can reduce the number of packets to 2 instead of 7.
- ➢ Similar considerations led to the development of a transaction service in WAP.

56. What is the advantage of transaction-oriented TCP?

Advantage of transaction-oriented TCP:

- ➢ The ***reduction in the overhead*** *than the* ***standard TCP consists*** for the purpose of ***connection setup and connection release***.

57. **What are the disadvantages of transaction-oriented TCP?**

Disadvantages of transaction-oriented TCP:

- ➢ The T/TCP is not the original TCP, so ***it requires changes*** in the mobile host and all correspondent hosts.
- ➢ T/TCP exhibits several security problems.

Overview of classical enhancements to TCP for mobility

TCP over 2.5/3G wireless networks

58. What is the consideration regarding data rates when deploying applications over 2.5G/3G wireless links? (or)

Identify the characteristics to be considered while deploying applications over 3G wireless links. (Apr/May 2019)

- ➢ ***Data rates:***
  - ✓ Typical data rates

- 2.5G systems are 10–20 Kbit/s uplink and 20–50 Kbit/s downlink
- 3G and future 2.5G systems:
  - Uplink data rates 64 Kbit/s and Downlink data rates 115–384 Kbit/s.

✓ Typically, data rates are asymmetric as it is expected that users will download more data compared to uploading. Uploading is limited by the limited battery power.

59. What is latency in deploying applications over 2.5G/3G wireless links?

Latency:

✓ All wireless systems comprise complicated algorithms for error correction and protection.
- ***Example:*** Forward Error Correction (FEC), check summing, and interleaving.

✓ FEC and interleaving allow the round trip time (RTT) grow to several hundred milliseconds up to some seconds.

✓ The current GPRS standard specifies an average delay of less than two seconds for the transport class with the highest quality.

60. What is the consideration regarding jitter when deploying applications over 2.5G/3G wireless links?

Jitter:

✓ Wireless systems suffer from large ***delay variations*** or ***'delay spikes'***.

✓ Reasons for sudden increase in the latency are:
- link outages due to temporal loss of radio coverage,
- blocking due to high-priority traffic, or
- handovers.

✓ Handovers are quite often only virtually seamless with outages reaching from some 10 ms (handover in GSM systems) to several seconds (intersystem handover).

61. What is the consideration regarding packet loss when deploying applications over 2.5G/3G wireless links?

Packet loss:

✓ Packets might be lost during handovers or due to corruption.

✓ Recovery at the link layer appears as jitter to the higher layers.

Characteristics of the following configuration parameters to adapt TCP to wireless environments:

62. Why large windows are used when deploying applications over 2.5G/3G wireless links?

Large windows:

o TCP should support large enough window sizes based on the ***bandwidth delay product*** faced in wireless systems.

o Accomplished through: Windows scale option (RFC 1323) and larger buffer sizes. (typical buffer size settings of 16 Kbyte are not enough).

o Larger initial window (more than the typical one segment) of 2 to 4 segments will increase the performance in short transmissions (a few segments in total).

63. What are the characteristics of the large windows when deploying applications over 2.5G/3G wireless links?

Limited transmit:

- This mechanism, defined in RFC 3042 is an extension of Fast Retransmission/Fast Recovery
- It is useful small amount data transmission (e.g., web service requests).

64. Write about Maximum Transfer Unit when deploying applications over 2.5G/3G wireless links.

Large MTU:

- The larger the MTU (Maximum Transfer Unit) the TCP increases the congestion window faster.
- Link layers fragment the PDUs for transmission according to their needs.
- Large MTUs may be used to increase performance.

65. Write about selective acknowledge when deploying applications over 2.5G/3G wireless links.

Selective Acknowledgement (SACK):

- SACK (RFC 2018) allows the selective retransmission of packets.
- It is always beneficial compared to the standard cumulative scheme.

66. Write about Maximum Transfer Unit when deploying applications over 2.5G/3G wireless links.

- ***Explicit Congestion Notification (ECN):***
  - ECN as defined in RFC 3168.
  - It allows a receiver to inform a sender about the congestion in the network, by setting the ECN-Echo flag ***on receiving an IP packet*** that has experienced congestion.
  - This mechanism is useful to ***distinguish packet loss due to transmission errors from packet loss due to congestion***.
  - This can only be achieved when ECN capable routers are deployed in the network.

67. What is meant by timestamp?

- ***Timestamp:***
  - TCP connections with large windows get benefit from more frequent RTT samples provided with timestamps.
  - With the help of timestamps the higher delay spikes can be tolerated by TCP without experiencing a spurious timeout.
  - The effect of bandwidth oscillation is also reduced.

68. Why header compression is not preferred when deploying applications over 2.5G/3G wireless links?

- ***No header compression:***
  - The TCP header compression mechanism according to RFC 1144 does not perform well in the presence of packet losses, so this mechanism should not be used.

- Header compression according to RFC 2507 or RFC 1144 is not compatible with TCP options such as SACK or timestamps.

69. What is meant by header compression?

Header compression: Headers of typical UDP or TCP packets can be compressed down. This largely removes the negative impact of large IP headers and allows efficient use of bandwidth on low and medium speed links.

70. What is packet buffer?

Packet Buffer: A packet buffer is memory space set aside for storing packets awaiting transmission over networks or storing packets received over networks.

71. Define Orders of Magnitude.

Orders of Magnitude: The scientific notation of very large numbers in which each order of magnitude is ten times the previous one.

72. Give an example for Intersystem handover.

Intersystem handover: *Example:* From a WLAN to a cellular system using Mobile IP without using additional mechanisms such as multicasting data to multiple access points

73. Compare various approaches with their respective mechanisms advantages and disadvantages.

Comparison of classical enhancements to TCP for mobility

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover, security problems
Snooping TCP	Snoops data and acknowledgements, local retransmission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problems
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management, security problems
Fast retransmit/ fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnection	Independent of content, works for longer interruptions	Changes in TCP required, MAC dependent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space needed
Transaction-oriented TCP	Combines connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent, security problems

*****

UNIT IV
WIRELESS WIDE AREA NETWORK

Overview of UMTS Terrestrial Radio access network - UMTS Core network Architecture: 3G-MSC, 3GSGSN, 3G-GGSN, SMS-GMSC/SMS-IWMSC, Firewall, DNS/DHCP-High speed Downlink packet access (HSDPA) - LTE network architecture and protocol.

1. Explain in detail about UMTS Terrestrial Radio Access Network (UTRAN).

4.1 UMTS Terrestrial Radio Access Network (UTRAN) Overview

- The UTRAN consists of a set of ***Radio Network Subsystems*** (***RNS***s) (see ***Figure 4.1***).
- The RNS has two main logical elements: ***Node B*** and an ***RNC***.
- The RNS is responsible for the ***radio resources*** and ***transmission/reception in a set of cells***.
- A ***cell*** (sector) is one coverage area served by a broadcast channel.

RNC (Radio Network Controller)

- An RNC (Radio Network Controller) is responsible for the use and allocation of all the radio resources of the RNS to which it belongs.
- The RNC also handles
  - ✓ The user voice and packet data traffic, performing the actions on the user data streams that are necessary to access the radio bearers.
- The responsibilities of an RNC are:
  - ✓ Intra UTRAN handover
  - ✓ Macro diversity combining/splitting of I_{ub} data streams
  - ✓ Frame synchronization
  - ✓ Radio resource management
  - ✓ Outer loop power control
  - ✓ Iu interface user plane setup
  - ✓ Serving RNS (SRNS) relocation
  - ✓ Radio resource allocation (allocation of codes, etc.)

- ✓ Frame selection/distribution function necessary for soft handover (functions of UMTS radio interface physical layer)
- ✓ UMTS radio link control (RLC) sublayers function execution
- ✓ Termination of MAC, RLC, and RRC protocols for transport channels, i.e., DCH, DSCH, RACH, FACH
- ✓ I_{ub}'s user plane protocols termination

Node B

- ➢ A Node B is responsible for radio transmission and reception in one or more cells to/from the user equipment (UE).
- ➢ The logical architecture for Node B is shown in ***Figure 4.2***.

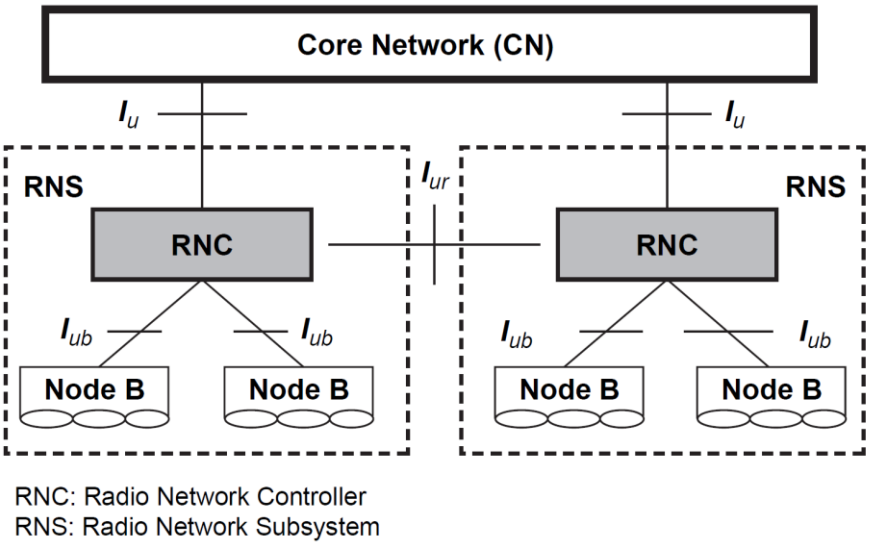


Figure 4.1 UTRAN logical architecture.

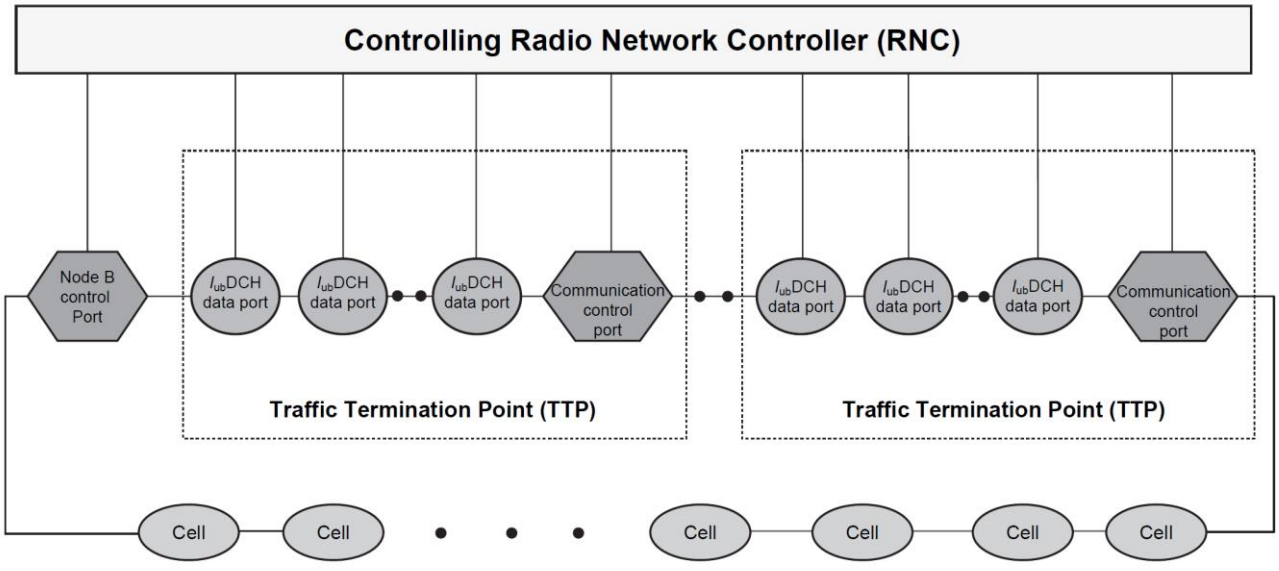


Figure 4.2 Node B logical architecture.

The following are the responsibilities of the Node B:

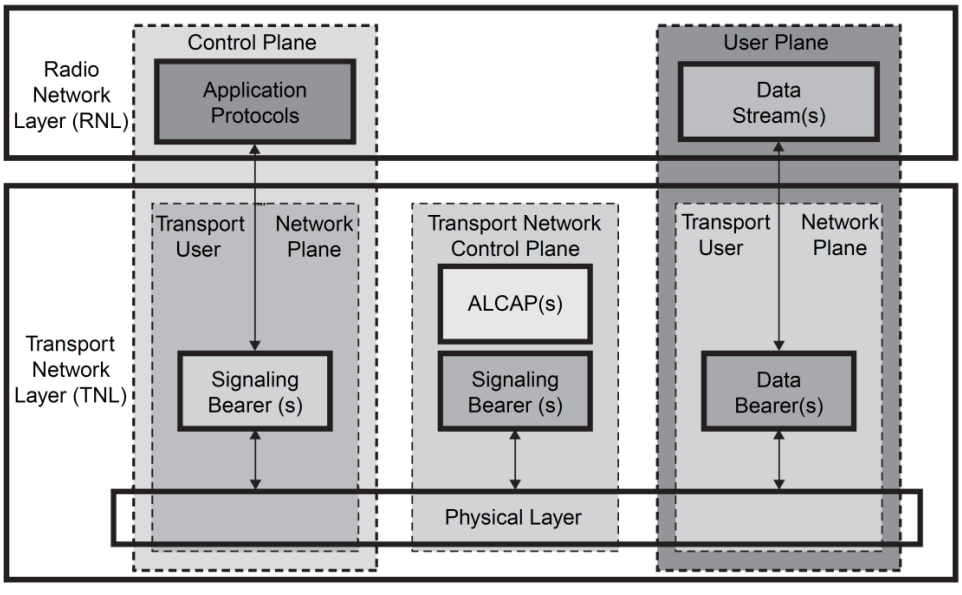
- ✓ Termination of I_{ub} interface from RNC
- ✓ Termination of MAC protocol for transport channels RACH, FACH
- ✓ Termination of MAC, RLC, and RRC protocols for transport channels: BCH, PCH

- ✓ Radio environment survey (BER estimate, receiving signal strength, etc.)
- ✓ Inner loop power control
- ✓ Open loop power control
- ✓ Radio channel coding/decoding
- ✓ Macro diversity combining/splitting of data streams from its cells (sectors)
- ✓ Termination of U_u interface from **UE**
- ✓ Error detection on transport channels and indication to higher layers
- ✓ FEC encoding/decoding and interleaving/deinterleaving of transport channels
- ✓ Multiplexing of transport channels and demultiplexing of coded composite transport channels
- ✓ Power weighting and combining of physical channels
- ✓ Modulation and spreading/demodulation and despreading of physical channels
- ✓ Frequency and time (chip, bit, slot, frame) synchronization
- ✓ RF processing

2. Discuss in detail about logical interfaces of UTRAN. (or)
Discuss the role of the access link control application part (ALCAP) in the UMTS. (16m – Nov 2017)

4.1.1 UTRAN Logical Interfaces

- ➢ Design of UTRAN protocol structure
  - ✓ The layers and planes are logically independent of each other.
  - ✓ If required, parts of protocol structure can be changed in the future without affecting other parts.
- ➢ The protocol structure contains two main layers:
  - ✓ the radio network layer (RNL)
  - ✓ the transport network layer (TNL).
- ➢ In the RNL, all UTRAN-related functions are visible/
- ➢ The TNL deals with transport technology selected to use for UTRAN but without any UTRAN-specific changes.
- ➢ A general protocol model for UTRAN interfaces is shown in ***Figure 4.3***.



ALCAP: Access Link Control Application Part

Figure 4.3 General protocol model for UTRAN interfaces.

- ***Control Plane:***
  - ✓ The control plane is used for all UMTS-specific control signaling.
  - ✓ It includes the
    - ***application protocol***
      - Radio Access Network Application Part (RANAP) in I_u
      - Radio Network Subsystem Application Part (RNSAP) in I_{ur} and
      - Node B Application Part (NBAP) in I_{ub}.
  - ✓ The application protocol is used for setting up bearers to the UE.

In the three-plane structure the bearer parameters in the application protocol are not directly related to the ***user plane technology***, but rather they are ***general bearer parameters***.

- ***User Plane:***
  - ✓ User information is carried by the user plane.
  - ✓ The user plane includes ***data stream(s)***, and ***data bearer(s) for data stream(s)***.
  - ✓ Each data stream is characterized by one or more ***frame protocols*** specified for that interface.
- ***Transport Network Control plane:***
  - ✓ The transport network control plane carries all control signaling within the transport layer.
  - ✓ It does ***not include radio network layer information***.
  - ✓ It contains ***Access Link Control Application Part (ALCAP)***
    - ALCAP is required to set up the transport bearers (data bearers) for the user plane.
  - ✓ It also includes the ***signaling bearer*** needed for the ALCAP.
  - ✓ The transport plane lies between the control plane and the user plane.
  - ✓ The addition of the transport plane in UTRAN allows the application protocol in the radio network control plane to be totally independent of the technology selected for the data bearer in the user plane.

- With the transport network control plane, the transport bearers for data bearers in the user plane are set up in the following way.
- There is a signaling transaction by application protocol in the control plane that initiates set-up of the data bearer by the ALCAP protocol specific for the user plane technology.
- The independence of the control plane and user plane assumes that an ALCAP signaling occurs.
- The ALCAP may not be used for all types of data bearers.
- If there is no ALCAP signaling transaction, the transport network control plane is not required.
- This situation occurs when preconfigured data bearers are used.
- Also, the ALCAP protocols in the transport network control plane are not used to set up the signaling bearer for the application protocol or the ALCAP during real-time operation.

2(a) Discuss various protocol architecture on I_u interface.

I_u Interface The UMTS I_u interface is the open logical interface that interconnects one UTRAN to the UMTS core network (UCN). On the UTRAN side the Iu interface is terminated at the RNC, and at the UCN side it is terminated at U-MSC.

- The Iu interface consists of three different protocol planes — the radio network control plane (RNCP), the transport network control plane (TNCP), and the user plane (UP).

The RNCP performs the following functions:

- ✓ It carries information for the general control of UTRAN radio network operations.
- ✓ It carries information for control of UTRAN in the context of each specific call.
- ✓ It carries user call control (CC) and mobility management (MM) signaling messages.

- The control plane serves two service domains in the core network, the packet-switched (PS) domain and circuit-switched (CS) domain.
- The CS domain supports circuit-switched services. Some examples of CS services are voice and fax.
- The CS domain can also provide intelligent services such as voice mail and free phone.
- The CS domain connects to PSTN/ISDN networks.
- The CS domain is expected to evolve from the existing 2G GSM PLMN.

- The PS domain deals with PS services. Some examples of PS services are Internet access and multimedia services.
- Since Internet connectivity is provided, all services currently available on the Internet such as search engines and e-mail are available to mobile users.
- The PS domain connects to IP networks. The PS domain is expected to evolve from the GPRS PLMN.
- The I_u circuit-switched and packet-switched protocol architecture are shown in ***Figures 4.4 and 4.5.***

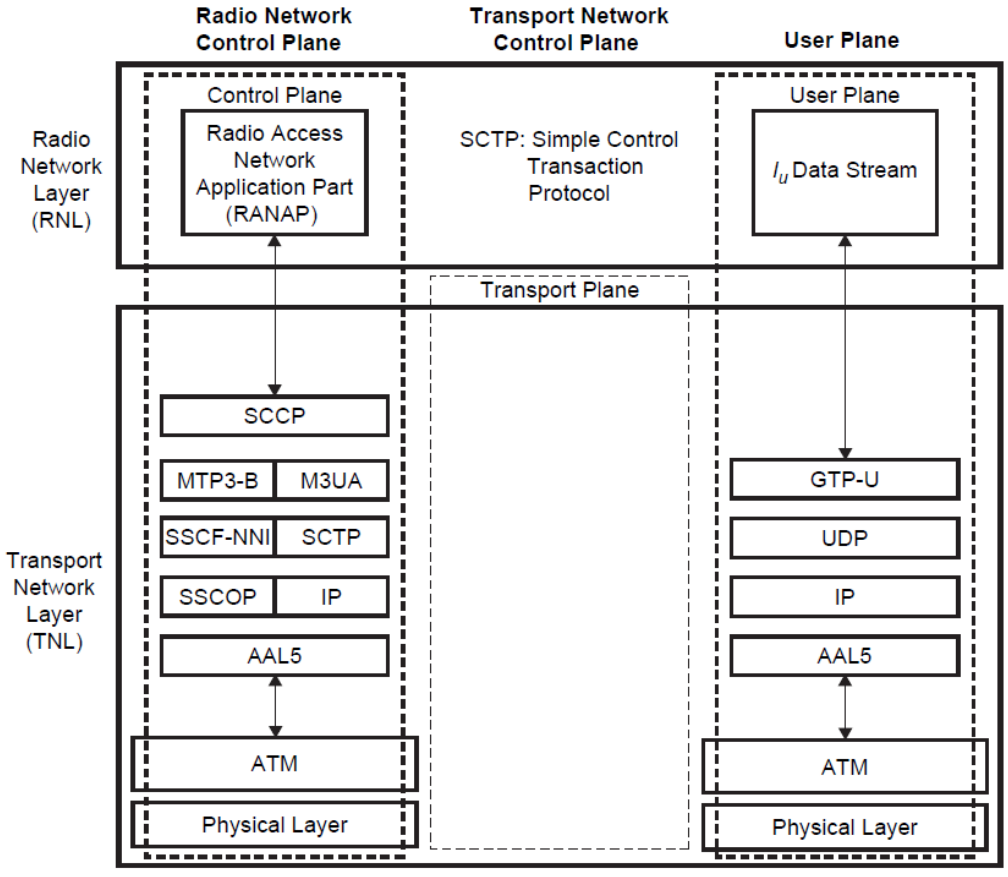


Figure 4.4 PS protocol architecture on lu interface.

- The control plane protocol stack consists of RANAP on the top of signaling system 7 (SS7) protocols.
- The protocol layers are the signaling connection control part (SCCP), the message transfer part (MTP3-B), and signaling asynchronous transfer mode (ATM) adaptation layer for network-to-network interface (SAAL-NNI).
- The SAAL-NNI is divided into service-specifi c coordination function (SSCF), the service-specific connection-oriented protocol (SSCOP), and ATM adaptation layer 5 (AAL5) layers.
- The SSCF and SSCOP layers are specifically designed for signaling transport in ATM networks, and take care of signaling connection management functions.
- AAL5 is used for segmenting the data to ATM cells.
- As an alternative, an IP-based signaling bearer is specified for the Iu PS control plane.
- The IP-based signaling bearer consists of SS7-MTP3—user adaptation layer (M3UA), simple control transmission protocol (SCTP), IP, and AAL5.
- The SCTP layer is specifically designed for signaling transport on the Internet.

- The transport network control plane (TNCP) carries information for the control of transport network used within UCN.

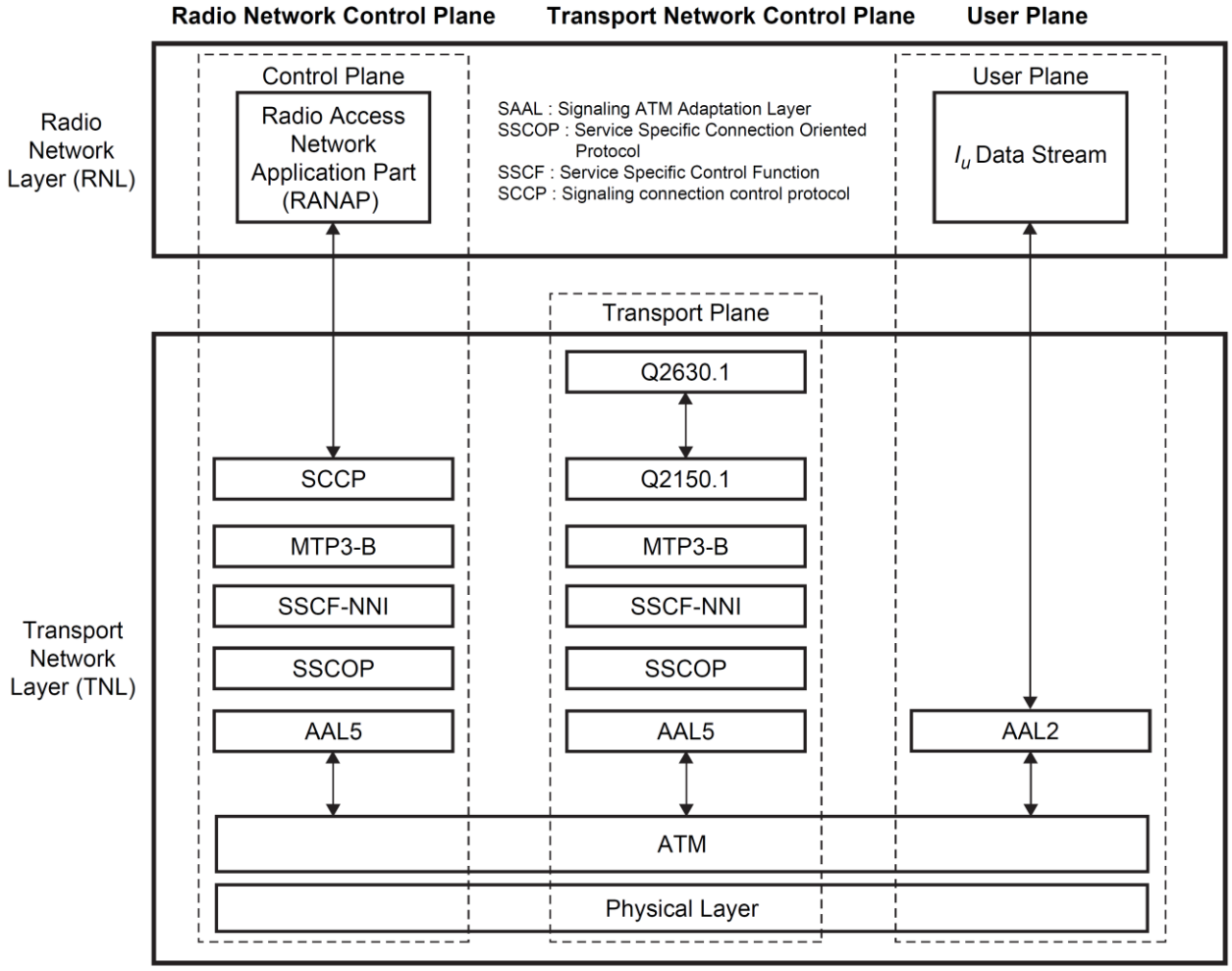


Figure 4.5 CS protocol architecture on lu interface.

- The user plane (UP) carries user voice and packet data information.

- AAL2 is used for the following services: narrowband speech (e.g., EFR, AMR); unrestricted digital information service (up to 64 kbps, i.e., ISDN B channel); any low to average bit rate CS service (e.g., modem service to/from PSTN/ISDN). A
- AL5 is used for the following services: non-real-time PS data service (i.e., best effort packet access) and real-time PS data.

2(b) Explain in detail about I_{ur} interface protocol architecture.

I_{ur} Interface

- The connection between two RNCs (serving RNC (SRNC) and drift RNC (DRNC)) is the Iur interface.
- It is used in soft handoff scenarios when different macro diversity streams of one communication are supported by Node Bs that belong to different RNCs.
- Communication between one RNC and one Node B of two different RNCs are realized through the ***I_{ur}*** interface.
- Three different protocol planes are defined for it:
  - ✓ Radio network control plane (RNCP)
  - ✓ Transport network control plane (TNCP)
  - ✓ User plane (UP)

  The I_{ur} interface is used to carry:
  - ✓ Information for the control of radio resources in the context of specific service request of one mobile on RNCP
  - ✓ Information for the control of the transport network used within UTRAN on TNCP
  - ✓ User voice and packet data information on UP

  The protocols used on this interface are:
  - ✓ Radio access network application part (RANAP)
  - ✓ DCH frame protocol (DCHFP)
  - ✓ RACH frame protocol (RACHFP)
  - ✓ FACH frame protocol (FACHFP)
  - ✓ Access link control application part (ALCAP)
  - ✓ Q.aal2
  - ✓ Signaling connection control part (SCCP)
  - ✓ Message transfer part 3-B (MTP3-B)
  - ✓ Signaling ATM adaptation layer for network-to-network interface (SAALNNI) (SAAL-NNI is further divided into service specific coordination function for network to network interface (SSCF-NNI), service specific connection oriented protocol (SSCOP), and ATM adaptation layer 5 (AAL5))
  - ✓ The bearer is AAL2. The protocol structure of the ***I_{ur}*** interface is shown in ***Figure 4.6***.

Initially, this interface was designed to support the inter-RNC soft handoff, but more features were added during the development of the standard.

The ***I_{ur}*** provides the following four functions:

1. Basic inter-RNC mobility support
   - ✓ Support of SRNC relocation
   - ✓ Support of inter-RNC cell and UTRAN registration area update

- ✓ Support of inter-RNC packet paging
- ✓ Reporting of protocol errors

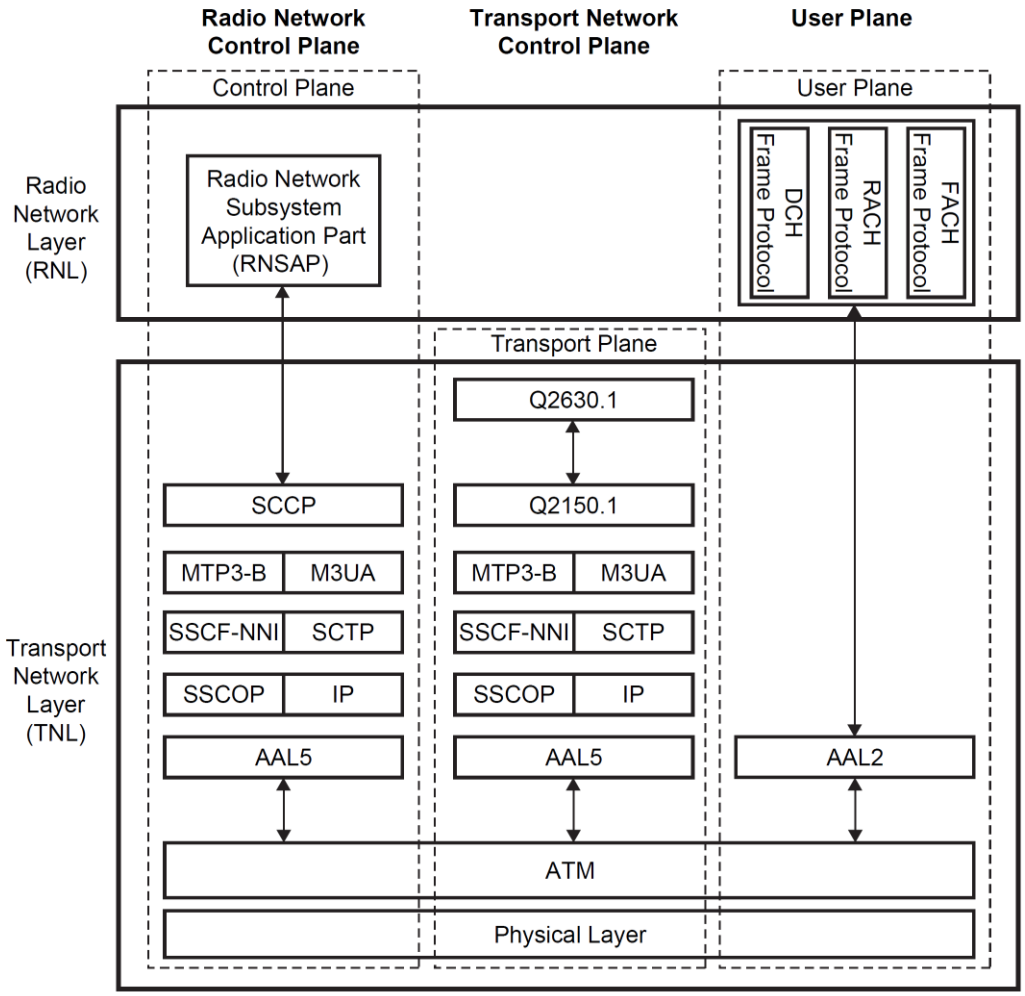


Figure 4.6 Protocol structure of I_{ur} interface.

2. Dedicated channel traffic support
   - ➢ Establishment, modification, and release of a dedicated channel in the DRNC due to hard and soft handoff in the dedicated channel state
   - ➢ Setup and release of dedicated transport connections across the I_{ur} interface
   - ➢ Transfer of DCH transport blocks between SRNC and DRNC
   - ➢ Management of radio links in the DRNS via dedicated measurement report procedures and power setting procedures
3. Common channel traffic support
   - ➢ Setup and release of the transport connection across the I_{ur} for common channel data streams
   - ➢ Splitting of the MAC layer between the SRNC (MAC-d) and DRNC
   - ➢ (MAC-c and MAC-sh); the scheduling for downlink data transmission is performed in the DRNC
   - ➢ Flow control between the MAC-d and MAC-c/MAC-sh
4. Global resource management support
   - ➢ Transfer of cell measurements between two RNCs
   - ➢ Transfer of Node B timing between two RNCs

2(c) Explain in detail about I_{ub} interface protocol architecture.

I_{ub} Interface

The connection between the RNC and Node B is the ***I_{ub}*** interface. There is one ***I_{ub}*** interface for each Node B. The ***I_{ub}*** interface is used for all of the communications between Node B and the RNC of the same RNS.

Three different protocol planes are defined for it.

- Radio network control plane (RNCP)
- Transport network control plane (TNCP)
- User plane (UP)

The ***I_{ub}*** interface is used to carry:

- Information for the general control of Node B for radio network operation on RNCP
- Information for the control of radio resources in the context of specific service request of one mobile on RNCP
- Information for the control of a transport network used within UTRAN on TCNP
- User CC and MM signaling message on RNCP
- User voice and packet data information on UP

The protocols used on this interface include:

- Node B application part protocol (NBAP)
- DCH frame protocol (DCHFP)
- RACH frame protocol (RACHFP)
- FACH frame protocol (FACHFP)
- Access link control application part (ALCAP)
- Q.aal2
- SSCP or TCP and IP
- MTP3-B
- SAAL-UNI (SSCF-UNI, SSCOP, and AAL5)

When using multiple low-speed links in the Iub interface, Node B supports inverse multiplexing for ATM (IMA).

The bearer is AAL2. The protocol structure for the interface Iub is shown in ***Figure 4.7***.

U_u Interface

The UMTS ***U_u*** interface is the radio interface between a Node B and one of its UE. The ***U_u*** is the interface through which UE accesses the fixed part of the system.

4.1.2 Distribution of UTRAN Functions

Located in the RNC

- Radio resource control (L3 Function)
- Radio link control (RLC)
- Macro diversity combining
- Active cell set modification
- Assign transport format combination set (centralized data base function)
- Multiplexing / demultiplexing of higher layer PDUs into/from transport block delivered to/from the physical layer on shared dedicated transport channels (used for soft handover)
- L1 function: macro diversity distribution/combining (centralized multipoint termination)

- Selection of the appropriate transport format for each transport channel depending upon the instantaneous source rate — collocate with RRC
- Priority handling between data flows of one user

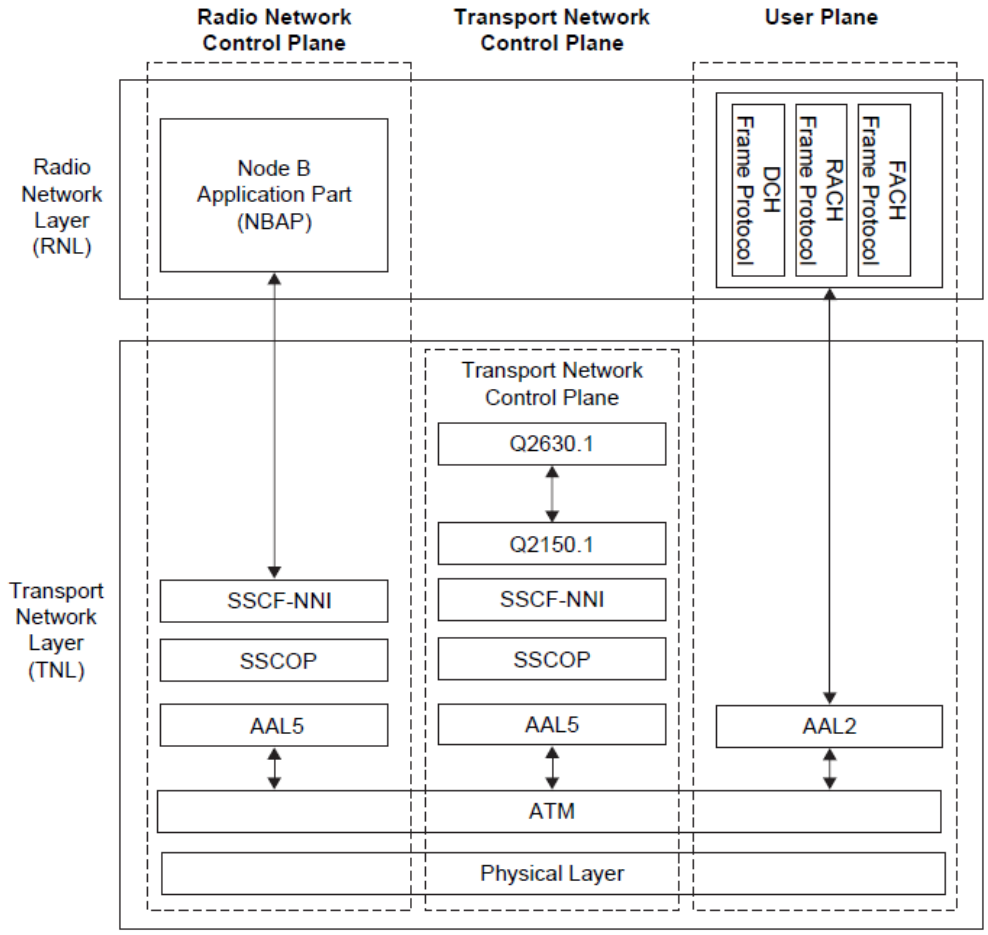


Figure 4.7 Protocol structure of I_{ub} interface.

Located in Node B

- Scheduling of broadcast, paging, and notification messages; location in Node B — to reduce data repetition over I_{ub} and reduce RNC CPU load and memory space
- Collision resolution on RACH (in Node B — to reduce nonconstructive traffic over I_{ub} interface and reduce round trip delay)
- Multiplexing / demultiplexing of higher layer PDUs to/from transport blocks delivered to / from the physical layer on common transport channels

******

3. Explain UMTS Core Network (UCN) Architecture. (16m - April 2017)

4.2 UMTS Core Network Architecture

Figure 15.28 shows the UMTS core network (UCN) in relation to all other entities within the UMTS network and all of the interfaces to the associated networks.

- The UCN consists of a CS entity for providing voice and CS data services and a PS entity for providing packet-based services.
- The logical architecture offers a clear separation between the CS domain and PS domain.

- The CS domain contains the functional entities: mobile switching center (MSC) and gateway MSC (GMSC) (see ***Figure 4.8***).

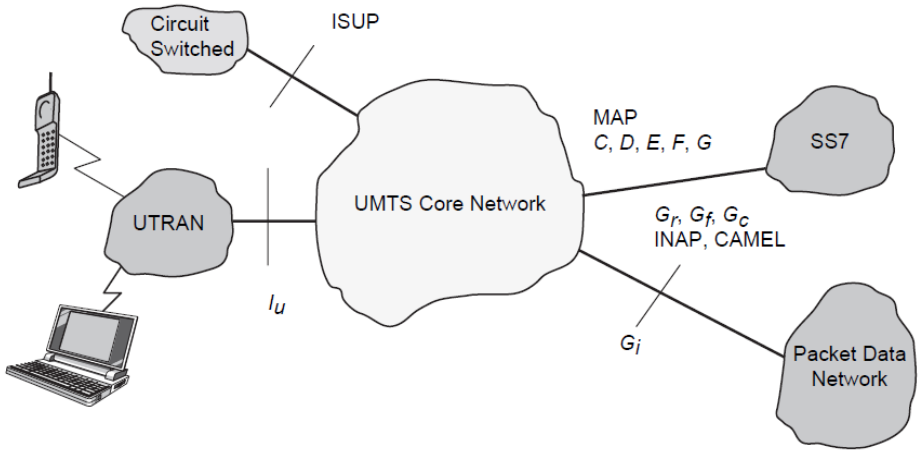


Figure 4.8 UMTS core network architecture.

- The PS domain comprises the functional entities:
  - serving GPRS support node (SGSN),
  - gateway GPRS support node (GGSN),
  - domain name server (DNS),
  - dynamic host configuration protocol (DHCP) server,
  - packet charging gateway, and
  - Firewalls.

The core network can be split into the following different functional areas:

- ✓ Functional entities needed to support PS services (e.g. 3G-SGSN, 3G-GGSN)
- ✓ Functional entities needed to support CS services (e.g. 3G-MSC/VLR)
- ✓ Functional entities common to both types of services (e.g. 3G-HLR)

Other areas that can be considered part of the core network include:

- ✓ Network management systems (billing and provisioning, service management, element management, etc.)
- ✓ IN system (service control point (SCP), service signaling point (SSP), etc.)
- ✓ ATM/SDH/IP switch/transport infrastructure

Figure 4.9 shows all the entities that connect to the core network — UTRAN, PSTN, the Internet and the logical connections between terminal equipment (MS, UE), and the PSTN/Internet.

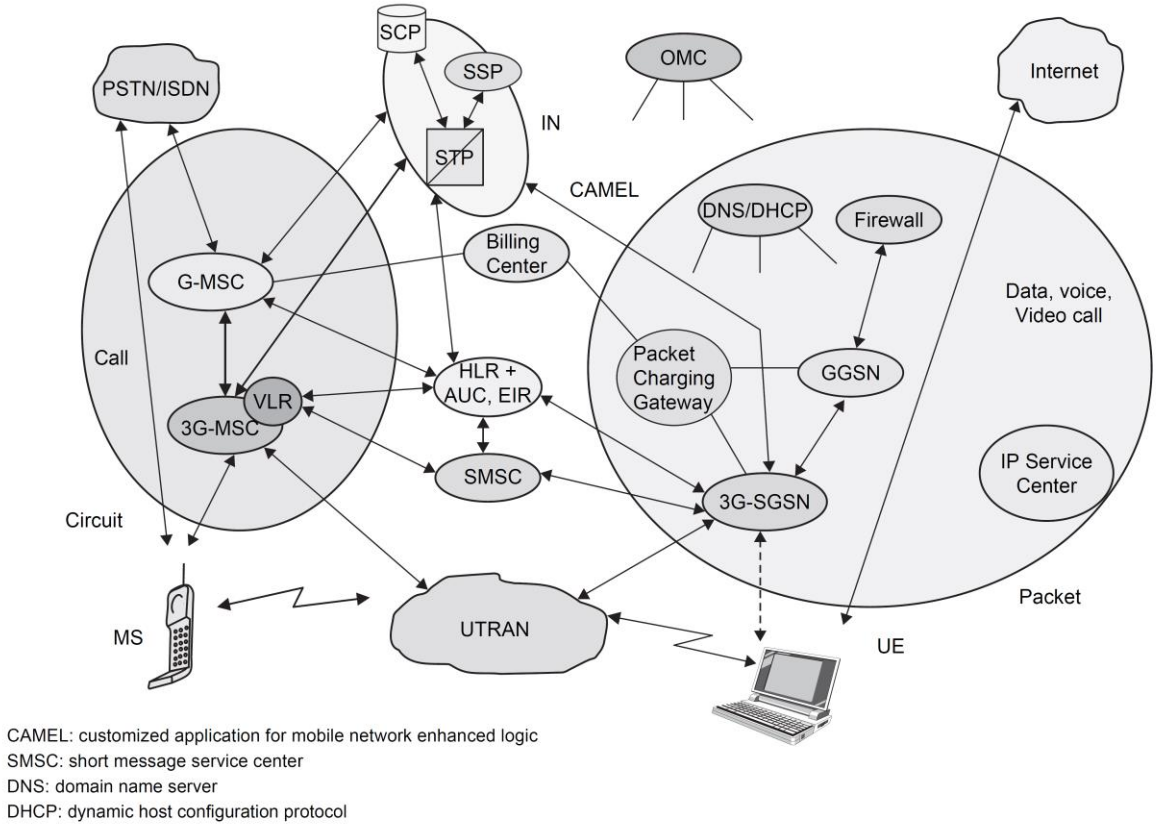


Figure 4.9 Logical architecture of the UMTS core network.

4.2.1 3G-MSC

- The 3G-MSC is the main CN element to provide CS services.
- The 3G-MSC also provides the necessary control and corresponding signaling interfaces including SS7, MAP, ISUP (ISDN user part), etc.
- The 3G MSC provides the interconnection to external networks like PSTN and ISDN.

The following functionality is provided by the 3G-MSC:

- ✓ ***Mobility management:*** Handles attach, authentication, updates to the HLR, SRNS relocation, and intersystems handover.
- ✓ ***Call management:*** Handles call set-up messages from/to the UE.
- ✓ ***Supplementary services:*** Handles call-related supplementary services such as call waiting, etc.
- ✓ ***CS data services:*** The IWF provides rate adaptation and message translation for circuit mode data services, such as fax.
- ✓ ***Vocoding***
- ✓ ***SS7, MAP and RANAP interfaces:*** The 3G-MSC is able to complete originating or terminating calls in the network in interaction with other entities of a mobile network, e.g., HLR, AUC (Authentication center). It also controls/communicates with RNC using RANAP which may use the services of SS7.
- ✓ ***ATM/AAL2 Connection to UTRAN*** for transportation of user plane traffic across the I_u interface. Higher rate CS data rates may be supported using a different adaptation layer.

- ✓ ***Short message services (SMS):*** This functionality allows the user to send and receive SMS data to and from the SMS-GMSC/SMS-IWMSC (Inter working MSC).
- ✓ ***VLR functionality:*** The VLR is a database that may be located within the 3G-MSC and can serve as intermediate storage for subscriber data in order to support subscriber mobility.
- ✓ ***IN and CAMEL***.
- ✓ ***OAM*** (Operation, Administration, and Maintenance) agent functionality.

4.2.2 3G-SGSN

- ➢ The 3G-SGSN is the main CN element for PS services.
- ➢ The 3G-SGSN provides the necessary control functionality both toward the UE and the 3G-GGSN.
- ➢ It also provides the appropriate signaling and data interfaces including connection to
  - ✓ an IP-based network toward the 3G-GGSN,
  - ✓ SS7 toward the HLR/EIR/AUC, and
  - ✓ TCP/IP or SS7 toward the UTRAN.

The 3G-SGSN provides the following functions:

- ✓ ***Session management:*** Handles session set-up messages from/to the UE and the GGSN and operates Admission Control and QoS mechanisms.
- ✓ ***I_u and G_n MAP interface:*** The 3G-SGSN is able to complete originating or terminating sessions in the network by interaction with other entities of a mobile network, e.g., GGSN, HLR, AUC. It also controls/communicates with UTRAN using RANAP.
- ✓ ATM/AAL5 physical connection to the UTRAN for transportation of user data plane traffic across the ***I_u*** interface using GPRS tunneling protocol (GTP).Connection across the ***G_n*** interface toward the GGSN for transportation of user plane traffic using GTP. Note that no physical transport layer is defined for this interface.
- ✓ ***SMS:*** This functionality allows the user to send and receive SMS data to and from the SMS-GMSC /SMS-IWMSC.
- ✓ ***Mobility management:*** Handles attach, authentication, updates to the HLR and SRNS relocation, and intersystem handover.
- ✓ ***Subscriber database functionality:*** This database (similar to the VLR) is located within the 3G-SGSN and serves as intermediate storage for subscriber data to support subscriber mobility.
- ✓ ***Charging:*** The SGSN collects charging information related to radio network usage by the user.
- ✓ ***OAM agent functionality***.

4.2.3 3G-GGSN

- ➢ The GGSN provides interworking with the external PS network.
- ➢ It is connecte with SGSN via an IP-based network.
- ➢ The GGSN may optionally support an SS7 interface with the HLR to handle mobile terminated packet sessions.

The 3G-GGSN provides the following functions:

- ✓ Maintain information locations at SGSN level (macro-mobility)
- ✓ Gateway between UMTS packet network and external data networks (e.g. IP, X.25)
- ✓ Gateway-specific access methods to intranet (e.g. PPP termination)

- ✓ Initiate mobile terminate Route Mobile Terminated packets
- ✓ User data screening/security can include subscription based, user controlled, or network controlled screening.
- ✓ ***User level address allocation:*** The GGSN may have to allocate (depending on subscription) a dynamic address to the UE upon PDP context activation. This functionality may be carried out by use of the DHCP function.
- ✓ ***Charging:*** The GGSN collects charging information related to external data network usage by the user.
- ✓ OAM functionality

4.2.4 SMS-GMSC/SMS-IWMSC

- ➢ The overall requirement for these two nodes is to handle the SMS from point to point. The functionality required can be split into two parts.

- ➢ The SMS-GMSC is an MSC capable of
  - ✓ receiving a terminated short message from a service center,
  - ✓ interrogating an HLR for routing information and SMS information, and
  - ✓ delivering the short message to the SGSN of the recipient UE.

- ➢ The SMS-GMSC provides the following functions:
  - ✓ Reception of short message packet data unit (PDU)
  - ✓ Interrogation of HLR for routing information
  - ✓ Forwarding of the short message PDU to the MSC or SGSN using the routing information

The SMS-IWMSC is an MSC capable of receiving an originating short message from within the PLMN and submitting it to the recipient service center.

The SMS-IWMSC provides the following functions:

- ✓ Reception of the short message PDU from either the 3G-SGSN or 3G-MSC
- ✓ Establishing a link with the addressed service center
- ✓ Transferring the short message PDU to the service center

Note: The service center is a function that is responsible for relaying, storing, and forwarding a short message. The service center is not part of UCN, although the MSC and the service center may be integrated.

4.2.5 Firewall

- ➢ This entity is used to protect the service providers' backbone data networks from attack from external packet data networks.
- ➢ The security of the backbone data network can be ensured by applying packet filtering mechanisms based on access control lists or any other methods deemed suitable.

4.2.6 DNS/DHCP

- ➢ The DNS server is used, as in any IP network, to translate host names into IP addresses, i.e., logical names are handled instead of raw IP addresses.

- Also, the DNS server is used to translate the access point name (APN) into the GGSN IP address.
- It may optionally be used to allow the UE to use logical names instead of physical IP addresses.
- A dynamic host configuration protocol server is used to manage the allocation of IP configuration information by automatically assigning IP addresses to systems configured to use DHCP.

4. Discuss a bout High-Speed Downlink Packet Access (HSDPA).

4.3 High-Speed Downlink Packet Access (HSDPA)

- In third-generation partnership project (3GPP) standards, Release 4 specifications,
  - provide efficient IP support which enables provision of services through an all-IP core network (see ***Figures 4.10 and 4.11***).
- Release 5 specifications focus on HSDPA
  - to provide data rates up to approximately 8–10 Mbps
  - So that it can support packet-based multimedia services.
- Multi input and multi output (MIMO) systems are the work item in Release 6 specifications, which will support even higher data transmission rates of up to 20 Mbps.
- HSDPA is evolved from and backward compatible with Release 99 WCDMA systems.
- HSDPA is based on the same set of technologies as high data rate (HDR) to improve spectral efficiency for data services such as
  - shared downlink packet data channel and high peak data rates — *using high-order modulation and adaptive modulation and coding*,
  - hybrid ARQ (HARQ) retransmission schemes,
  - fast scheduling, and
  - shorter frame sizes.
- HSDPA marks a similar boost for WCDMA, that EDGE does for GSM.
- It provides
  - a two-fold increase in air interface capacity, and
  - a five-fold increase in data speeds in the downlink direction.
- HSDPA also
  - shortens the round-trip time between the network and terminals, and
  - Reduces the variance in downlink transmission delay.

4 (a). List the improvements in performance are achieved by HSDPA.

The improvements in performance are achieved by:

- ✓ ***Bringing some key functions***, such as
  - Scheduling of data packet transmission and processing of retransmissions (*in case of transmission errors*) into the base station — that is, closer to the air interface.
- ✓ ***Using a short frame length*** to further accelerate packet scheduling for transmission.
- ✓ ***Employing incremental redundancy*** for minimizing the air-interface load caused by retransmissions.

- ✓ ***Adopting a new transport channel type***, known as **H**igh-**S**peed **D**ownlink **S**hared **Ch**annel (HSDSCH), to facilitate air interface channel sharing between several users.
- ✓ ***Adapting the modulation and coding scheme*** according to the quality of the radio link

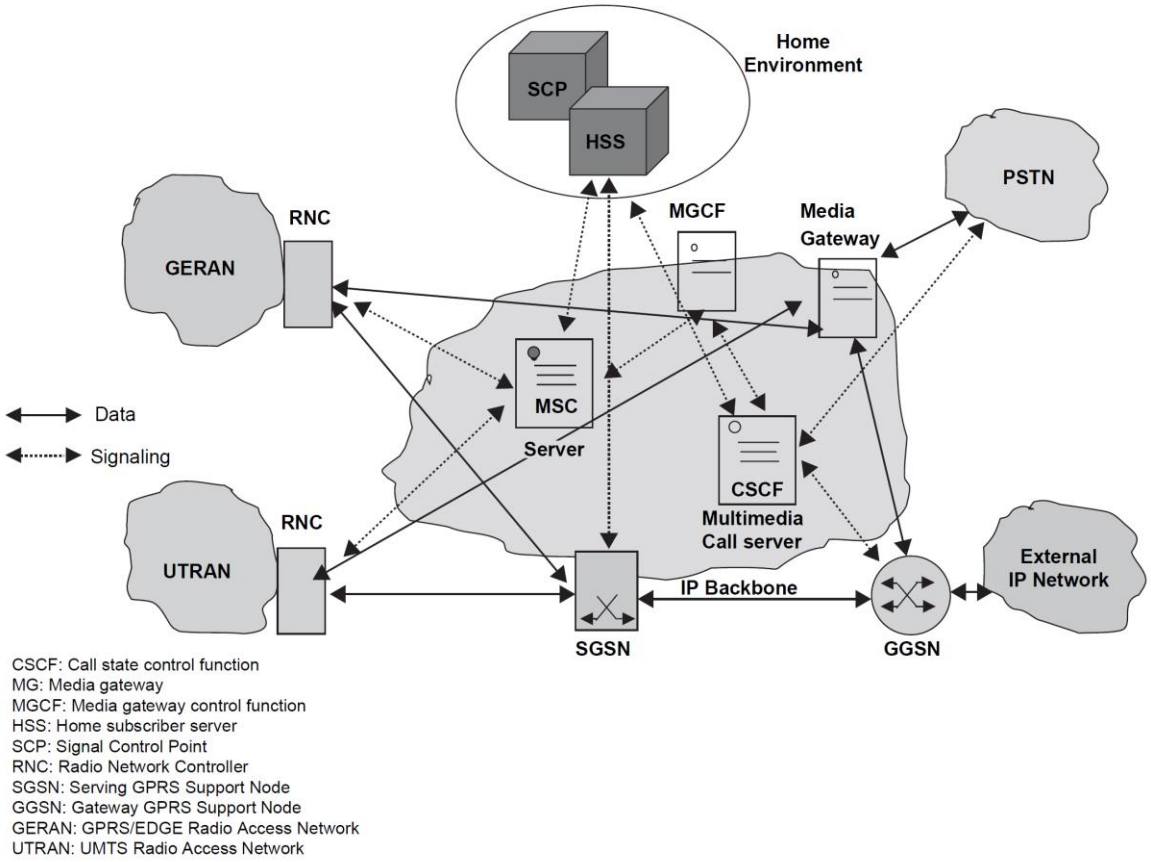


Figure 4.10 A simplified all-IP UMTS architecture.

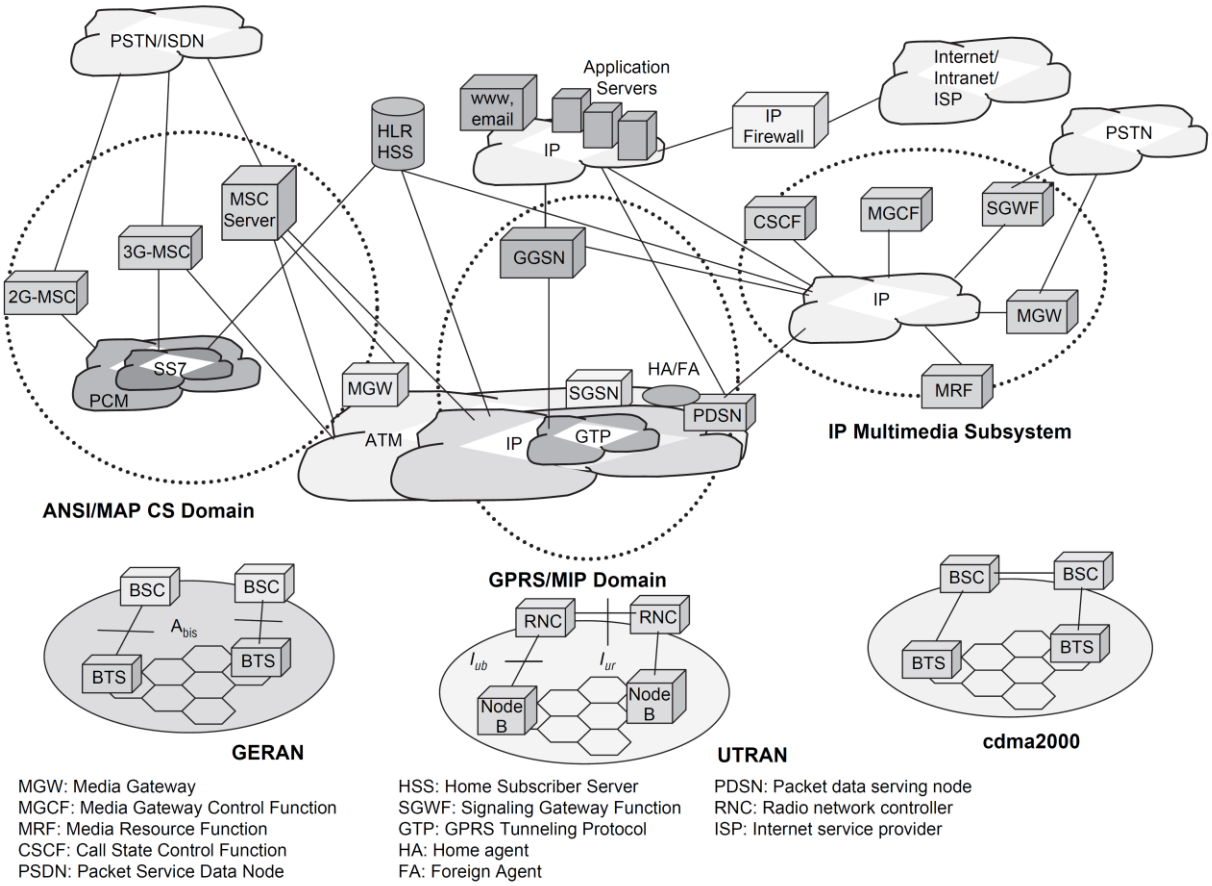


Figure 4.11 All-IP core network architecture for UMTS.

- The ***primary objective*** behind HSDPA is to provide a ***cost-effective, high bandwidth, low-delay, packet-oriented service*** within UMTS.
- Backward compatibility is critical, so the HSDPA architecture adheres to an evolutionary philosophy.

- From an architectural perspective,
  - HSDPA is a ***straightforward enhancement of the UMTS Release '99 (R99)*** architecture,
  - The addition is, a repetition scheduling entity within the Node B that resides below the R99 media-access control (MAC) layer.

- From a cellular-network perspective, all R99 techniques can be supported in a network supporting HSDPA, since HSDPA mobile terminals (UEs) are designed to coexist with R99 UEs.
- HSDPA is particularly suitable for ***extremely asymmetrical data services***,
  - Which require significantly higher data rates for the transmission from the network to the UE, than they do for the transmission from the UE to the network.
- HSDPA introduces ***enablers*** for the high-speed transmission at the physical layer
- **HS-DPCCH** is used ***to carry the acknowledgment signals*** to Node B for each block.
- It is also used to indicate channel quality (CQI - Channel Quality Indicator) used for adaptive modulation and coding.
- HS-DSCH uses 2 ms TTI (transmission time interval)
  - to reduce trip time,

- to increase the granularity in the scheduling process, and
- to track the time varying radio channel better.

4 (b). Explain the Basic operational principles behind HSDPA.

Basic operational principles behind HSDPA

- Principles are relatively simple.
- **RNC:** The RNC routes data packets destined ***(assigned)*** for a particular UE to the appropriate Node B.
- **Node B:**
  - ***takes the data packets*** and ***schedules their transmission*** to the mobile terminal over the air interface
    - by matching the user's priority and estimated channel operating environment
      - with an appropriately chosen coding and modulation scheme (that is, 16-QAM vs. QPSK).
- **UE:**
  - It is ***responsible for acknowledging receipt of the data packet***.
  - It also providing Node B with information regarding ***channel condition, power control,*** and so on.
  - Once it (i.e., Node B) sends the data packet to the UE, the Node B waits for an acknowledgment.
  - If it does not receive one within a prescribed time, it assumes that the data packet was lost and retransmits it.

- ***Bandwidth:*** With some constraints, HSDPA continuously tries to give the ***maximal bandwidth*** to the user with the best channel conditions.
- ***Data Rate:*** Data rates with HSDPA are more than enough for supporting multimedia streaming services (refer to ***Table 3.1***).

Table 3.1 HSDPA data rates.

Chip rate = 3.84 Mcps, frame size = 3 slots				
Modulation	**Coding rate**	**Throughput with 5 codes**	**Throughput with 10 codes**	**Throughput with 15 codes**
16-QAM	1/2	2.4 Mbps	4.8 Mbps	7.2 Mbps
16-QAM	3/4	3.6 Mbps	7.2 Mbps	10.8 Mbps
16-QAM	4/4	4.8 Mbps	9.6 Mbps	14.4 Mbps
QPSK	1/4	600 kbps	1.2 Mbps	1.8 Mbps
QPSK	1/2	1.2 Mbps	2.4 Mbps	3.6 Mbps
QPSK	3/4	1.8 Mbps	3.6 Mbps	5.4 Mbps

4 (c). Discuss in detail about implementation issues or architectural issues of HSDPA.

Implementation Issues:

Architectural issues:

- HSDPA is conceptually simple, but implementation within the perspective of a Node B raises some architectural issues for the designer.

- ***Network deployment***:
  - The Node B radio cabinet sits in closeness to the radio tower and the power cabinet.
  - For indoor deployments the radio cabinet may be a simple rack, while in outdoor deployments it may be an environmental-control unit.

The backbones of the radio cabinet are

- an antenna interface section (filters, power amplifiers, and the like),
- core processing chassis (RF transceivers, combiner, high performance channel cards, network interface and system controller card, timing card, back-plane, and so on),
- mechatronics (power supply, fans, cables, etc.), and
- other miscellaneous elements.

- ***Core processing chassis:***
  - The ***core processing chassis*** is the foundation stone of Node B and bears most of the cost.
  - It contains the RF transceiver, combiner, network interface and system controller, timing card, channel card and backplane.
  - Of the core processing chassis elements, only the channel card needs to be modified to support HSDPA.

- The typical UMTS channel card comprises a
  - ✓ ***general-purpose processor*** that handles the miscellaneous control tasks,
  - ✓ a pool of ***digital signal processor (DSP) resources*** to handle symbol-rate processing and chip-rate assist functions, and
  - ✓ a ***pool of specialized ASIC*** (application specific integrated circuit) devices to handle intensive chip-rate operations
    - such as spreading, scrambling, modulation, rake receiving, and preamble detection.

Changes in Channel card

- To support HSDPA, ***two changes*** must be made to the channel card.
- First change:
  - ✓ the downlink chip-rate ASIC must be modified to support the new 16-QAM modulation schemes and new downlink slot formats associated with HSDPA.
  - ✓ In addition, the downlink symbol-rate processing section must be modified to support HSDPA extensions.

- Second change:
  - ✓ It requires a new processing section, called the MAC-hs.
  - ✓ The MAC-hs must be added to the channel card to support the scheduling, buffering, transmission, and retransmission of data blocks that are received from the RNC.
  - ✓ It requires the introduction of a programmable processing entity together with a retransmission buffer.

4 (d). Explain about New channels introduced in HSDPA.

New channels introduced in HSDPA:

- ***Three New channels introduced in HSDPA:***
  - ✓ High-speed downlink shared channel (HS-DSCH)
  - ✓ High-speed shared control channel (HS-SCCH), and
  - ✓ High speed dedicated physical control channel (HS-DPCCH).

HS-DSCH

- ✓ The HS-DSCH is the primary radio bearer.
- ✓ Its resources can be shared among all users in a particular sector.
- ✓ The primary channel multiplexing occurs in a time domain, where each TTI consists of three time slots (each 2 ms).
- ✓ TTI is also referred to as a sub-frame.
- ✓ Within each 2 ms TTI, a constant spreading factor (SF) of 16 is used for code multiplexing, with a maximum of 15 parallel codes allocated to HS-DSCH.
- ✓ Codes may all be assigned to one user, or may be split across several users.
- ✓ The number of codes allocated to each user depends on cell loading, QoS requirements, and UE code capabilities (5, 10, or 15 codes).

HS-SCCH

- ✓ The HS-SCCH (a fixed rate 960 kbps, SF = 128).
- ✓ It is used to carry downlink signaling between Node B and UE before the beginning of each scheduled TTI.
- ✓ It includes UE identity, HARQ-related information and the parameters of the HS-DSCH transport format selected by the link-adaptation mechanism.
- ✓ Multiple HS-SCCHs can be configured in each sector to support parallel HS-DSCH transmissions.
- ✓ A UE can be allocated a set of up to four HS-SCCHs, which need to be monitored continuously.

HS-DPCCH

- ✓ The HS-DPCCH (SF = 256) carries ACK/NACK signaling to indicate whether the corresponding downlink transmission was successfully decoded, as well as a channel quality indicator (CQI) to be used for the purpose of link adaptation.
- ✓ The CQI is based on a common pilot channel (CPICH)
  - It is used to estimate the transport block size, modulation type, and number of channelization codes
  - The codes support for reliability level in downlink transmission.
- ✓ The feedback cycle of CQI can be set as a network parameter in predefined steps of 2 ms.

4 (e). List out UE capabilities and Tabulate UE categories in HSDPA.

- UE capabilities include
  - ✓ the maximum number of HS-DSCHs supported simultaneously (5, 10, or 15),

- ✓ minimum TTI time (minimum time between the beginning of two consecutive transmissions to the UE),
- ✓ the maximum number of HS-DSCH transport block (TB) bits received within an HS-DSCH TTI,
- ✓ the maximum number of soft channel bits over all HARQ and supported modulations (QPSK only or both QPSK and 16-QAM).

➢ **Table 3.2** gives UE categories.

Table 3.2 HSDPA UE categories.

Category	Codes	Inter-TTI	TB size (bits)	Total soft bits	Modulation	Data rate (Mbps)
1	5	3	7300	19,200	QPSK/QAM	1.2
2	5	3	7300	28,800	QPSK/QAM	1.2
3	5	2	7300	28,800	QPSK/QAM	1.8
4	5	2	7300	38,400	QPSK/QAM	1.8
5	5	1	7300	57,600	QPSK/QAM	3.6
6	5	1	7300	67,200	QPSK/QAM	3.6
7	10	1	14,600	115,200	QPSK/QAM	7.2
8	10	1	14,600	134,400	QPSK/QAM	7.2
9	15	1	20,432	172,800	QPSK/QAM	10.2
10	15	1	28,776	172,800	QPSK/QAM	14.4
11	5	2	3650	14,400	QPSK	0.9
12	5	1	3650		QPSK	1.8

LTE network architecture and protocol

LTE Network Architecture

5. Explain in detail about LTE network architecture.

The high-level network architecture of LTE is comprised of following three main components:

- The User Equipment *UE*
- The Evolved UMTS Terrestrial Radio Access Network *E−UTRAN*
- The Evolved Packet Core *EPC*

➢ The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem.

➢ The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below:

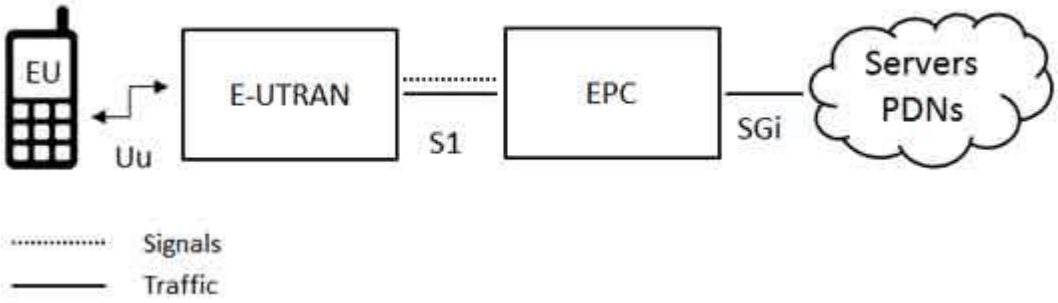


Figure 4.12 LTE network architecture

The User Equipment *UE*

The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment *ME*

The mobile equipment comprised of the following important modules:

Mobile Termination *MT*

- This handles all the communication functions.

Terminal Equipment *TE*

- This terminates the data streams.

Universal Integrated Circuit Card *UICC*

- This is also known as the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module *USIM*

A **USIM** stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

The E-UTRAN *The access network*

The architecture of evolved UMTS Terrestrial Radio Access Network *E−UTRAN* has been illustrated below.

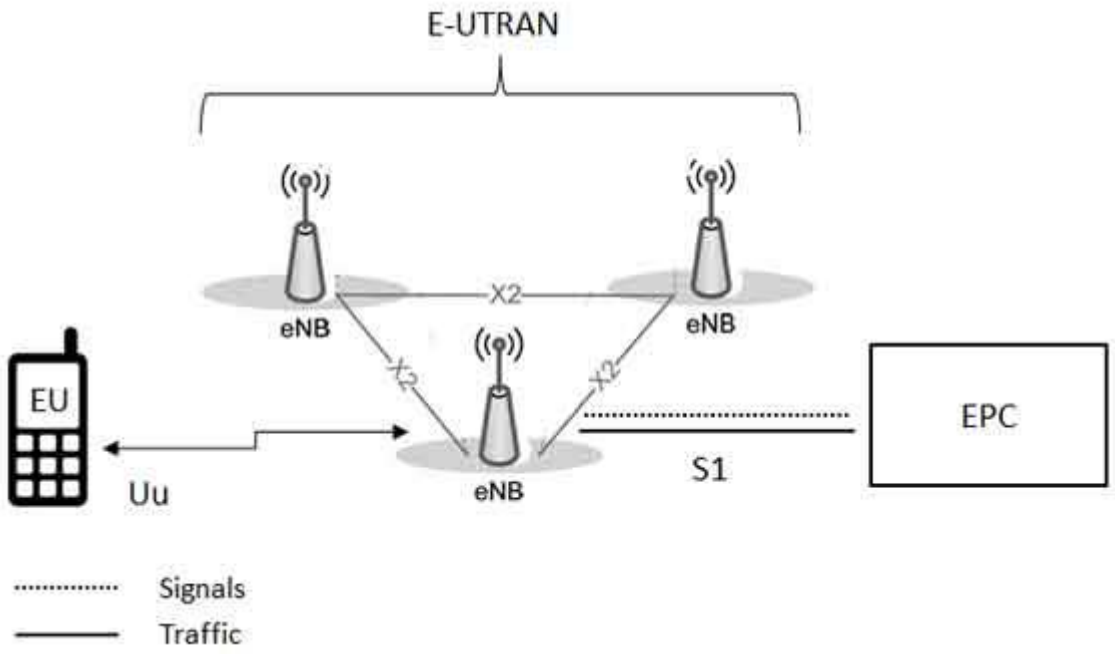


Figure 4.13: The E-UTRAN *The access network*

The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called **eNodeB** or **eNB**. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

LTE Mobile communicates with just one base station and one cell at a time and there are following two main functions supported by eNB:

- The eNB sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
- The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

Each eNB connects with the EPC by means of the S1 interface and it can also be connected to nearby base stations by the X2 interface, which is mainly used for signalling and packet forwarding during handover.

A home eNB *HeNB* is a base station that has been purchased by a user to provide femtocell coverage within the home. A home eNB belongs to a closed subscriber group *CSG* and can only be accessed by mobiles with a USIM that also belongs to the closed subscriber group.

The Evolved Packet Core *EPC*

The core network

The architecture of Evolved Packet Core *EPC* has been illustrated below. There are few more components which have not been shown in the diagram to keep it simple. These components are

like the Earthquake and Tsunami Warning System *ETWS*, the Equipment Identity Register *EIR* and Policy Control and Charging Rules Function *PCRF*

.

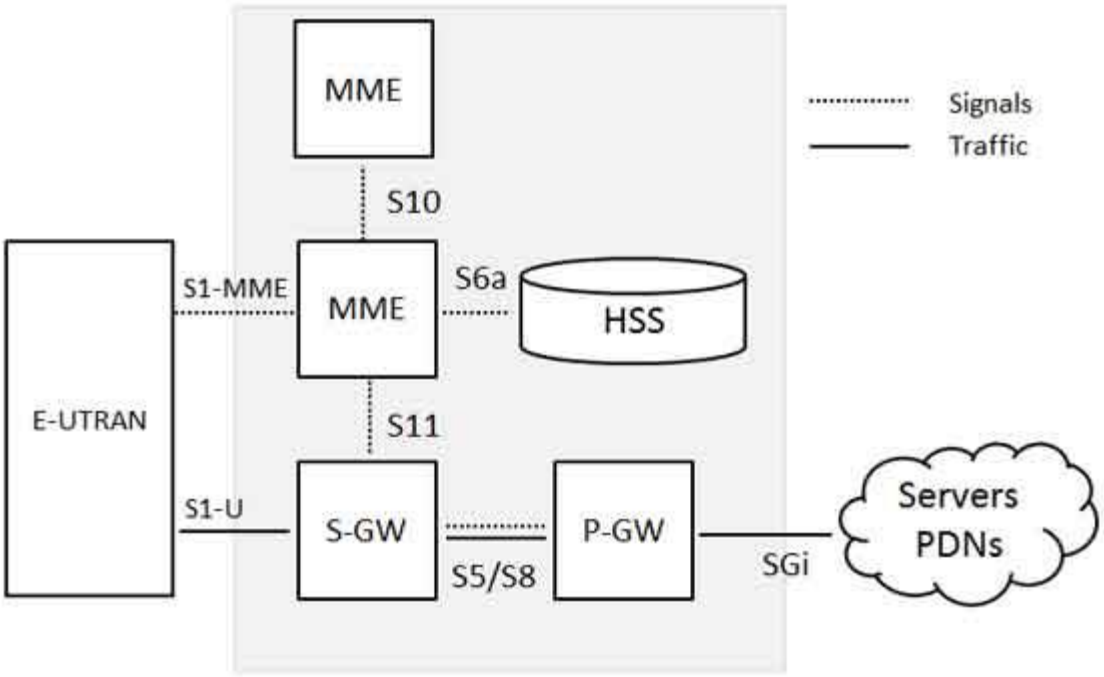


Figure 4.14:

Below is a brief description of each of the components shown in the above architecture:

- The Home Subscriber Server *HSS* component has been carried forward from UMTS and GSM
- and is a central database that contains information about all the network operator's subscribers.
- The Packet Data Network *PDN* Gateway *P−GW* communicates with the outside world ie. packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name *APN*. The PDN gateway has the same role as the GPRS support node *GGSN* and the serving GPRS support node *SGSN* with UMTS and GSM.
- The serving gateway *S−GW* acts as a router, and forwards data between the base station and the PDN gateway.
- The mobility management entity *MME* controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server *HSS*
- The Policy Control and Charging Rules Function *PCRF* is a component which is not shown in the above diagram but it is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function *PCEF*, which resides in the P-GW.

The interface between the serving and PDN gateways is known as S5/S8. This has two slightly different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.

Functional split between the E-UTRAN and the EPC

Following diagram shows the functional split between the E-UTRAN and the EPC for an LTE network:

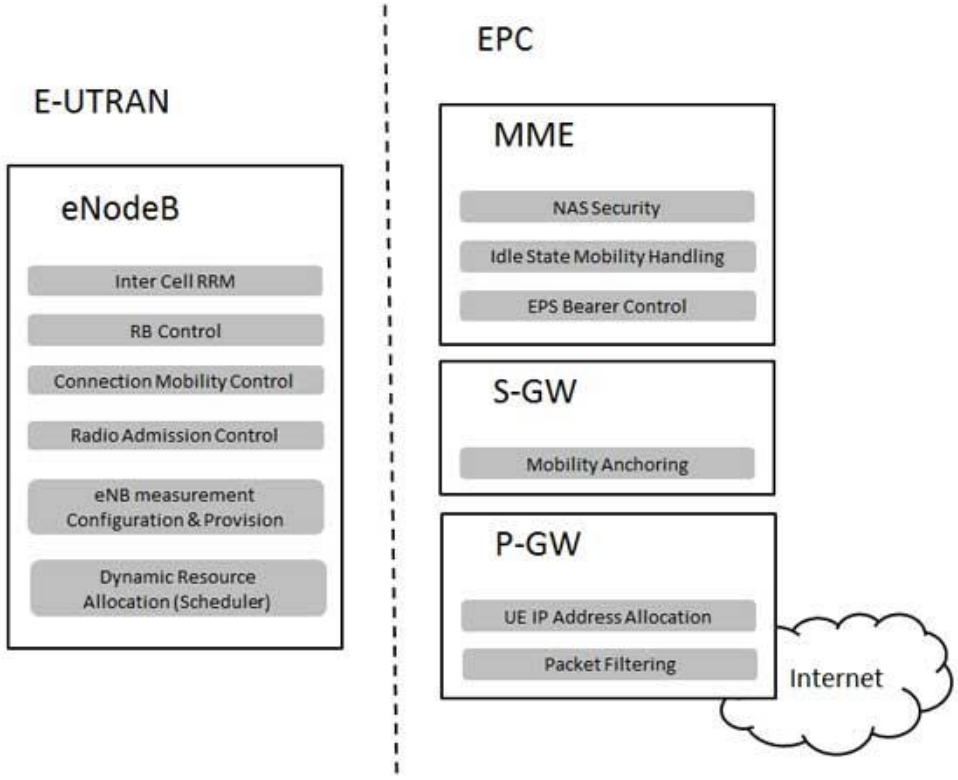


Figure 4.15:

6. Distinguish between 2G/3G and LTE.

2G/3G versus LTE

Following table compares various important Network Elements & Signaling protocols used in 2G/3G and LTE.

2G/3G	**LTE**
GERAN and UTRAN	E-UTRAN
SGSN/PDSN-FA	S-GW
GGSN/PDSN-HA	PDN-GW
HLR/AAA	HSS
VLR	MME
SS7-MAP/ANSI-41/RADIUS	Diameter

DiameterGTPc-v0 and v1	GTPc-v2
MIP	PMIP

7. Discuss briefly about LTE Radio Protocol Architecture.

LTE Radio Protocol Architecture

The radio protocol architecture for LTE can be separated into **control plane** architecture and **user plane** architecture as shown below:

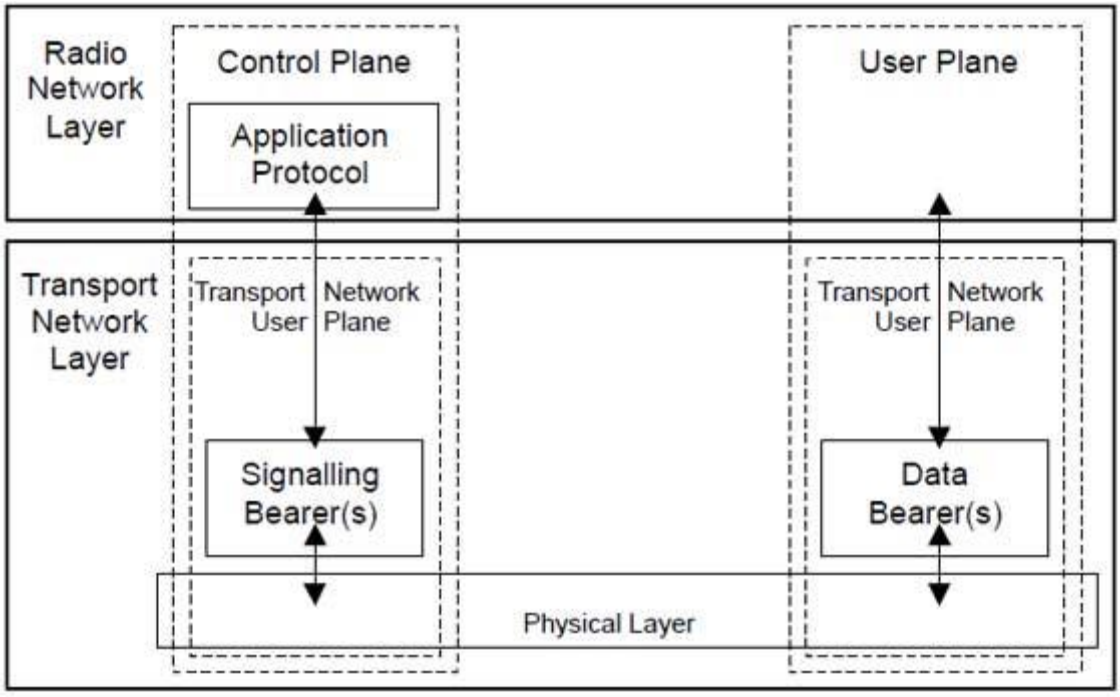


Figure 4.16: Radio Frequency Protocol

- At user plane side, the application creates data packets that are processed by protocols such as TCP, UDP and IP, while in the control plane, the radio resource control (RRC) protocol writes the signalling messages that are exchanged between the base station and the mobile.
- In both cases, the information is processed by the packet data convergence protocol (PDCP), the radio link control (RLC) protocol and the medium access control (MAC) protocol, before being passed to the physical layer for transmission.

User Plane

The user plane protocol stack between the e-Node B and UE consists of the following sub-layers:

- PDCP (Packet Data Convergence Protocol)
- RLC (radio Link Control)
- Medium Access Control (MAC)

- On the user plane, packets in the core network (EPC) are encapsulated in a specific EPC protocol and tunneled between the P-GW and the eNodeB. Different tunneling protocols are used depending on the interface.

- GPRS Tunneling Protocol (GTP) is used on the S1 interface between the eNodeB and S-GW and on the S5/S8 interface between the S-GW and P-GW.

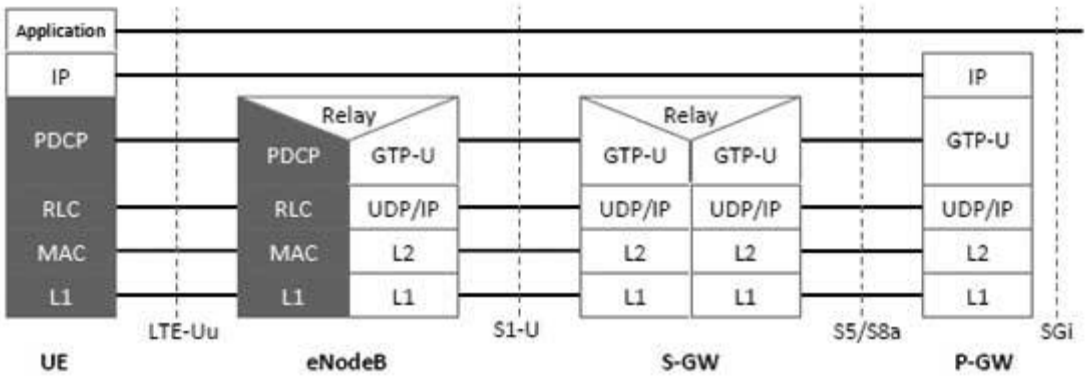


Figure 4.17: User plane

- Packets received by a layer are called Service Data Unit (SDU) while the packet output of a layer is referred to by Protocol Data Unit (PDU) and IP packets at user plane flow from top to bottom layers.

Control Plane

- The control plane includes additionally the Radio Resource Control layer (RRC) which is responsible for configuring the lower layers.
- The Control Plane handles radio-specific functionality which depends on the state of the user equipment which includes two states: idle or connected.

Table: Control plane

Mode	Description
Idle	The user equipment camps on a cell after a cell selection or reselection process where factors like radio link quality, cell status and radio access technology are considered. The UE also monitors a paging channel to detect incoming calls and acquire system information. In this mode, control plane protocols include cell selection and reselection procedures.
Connected	The UE supplies the E-UTRAN with downlink channel quality and neighbour cell information to enable the E-UTRAN to select the most suitable cell for the UE. In this case, control plane protocol includes the Radio Link Control (RRC) protocol.

- The protocol stack for the control plane between the UE and MME is shown below.
  - The grey region of the stack indicates the access stratum (AS) protocols.
  - The lower layers perform the same functions as for the user plane with the exception that there is no header compression function for the control plane.

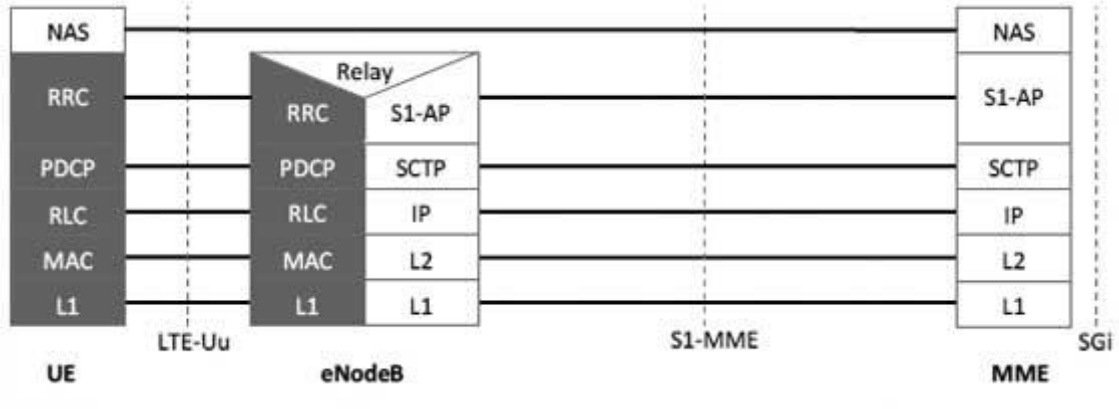


Figure 4.18

8. Explain about LTE Protocol Stack Layers.

LTE Protocol Stack Layers

Diagram of E-UTRAN Protocol Stack:

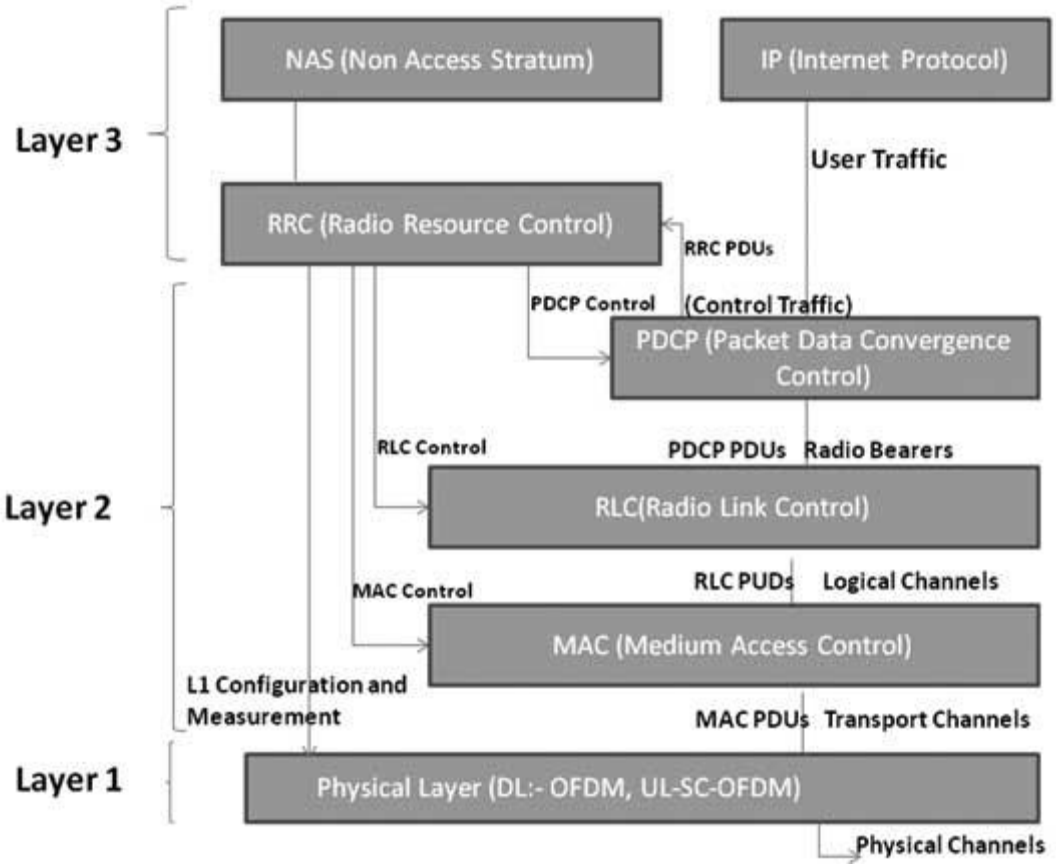


Figure 4.19

Physical Layer (Layer 1)

- Physical Layer carries all information from the MAC transport channels over the air interface.

- Takes care of the link adaptation (AMC), power control, cell search (for initial synchronization and handover purposes) and other measurements (inside the LTE system and between systems) for the RRC layer.

Medium Access Layer (MAC)

MAC layer is responsible for

- Mapping between logical channels and transport channels,
- Multiplexing of MAC SDUs from one or different logical channels onto transport blocks (TB) to be delivered to the physical layer on transport channels,
- Demultiplexing of MAC SDUs from one or different logical channels from transport blocks (TB) delivered from the physical layer on transport channels,
- Scheduling information reporting,
- Error correction through HARQ,
- Priority handling between UEs by means of dynamic scheduling,
- Priority handling between logical channels of one UE,
- Logical Channel prioritization.

Radio Link Control (RLC)

RLC operates in 3 modes of operation:

- Transparent Mode (TM)
- Unacknowledged Mode (UM)
- Acknowledged Mode (AM)
- RLC Layer is responsible for transfer of upper layer PDUs, error correction through ARQ (Only for AM data transfer), Concatenation, segmentation and reassembly of RLC SDUs (Only for UM and AM data transfer).

RLC is also responsible for

- re-segmentation of RLC data PDUs (Only for AM data transfer),
- reordering of RLC data PDUs (Only for UM and AM data transfer),
- duplicate detection (Only for UM and AM data transfer),
- RLC SDU discard (Only for UM and AM data transfer),
- RLC re-establishment, and
- protocol error detection (Only for AM data transfer).

Radio Resource Control (RRC)

The main services and functions of the RRC sublayer include

- broadcast of System Information related to the non-access stratum (NAS),
- broadcast of System Information related to the access stratum (AS),
- Paging, establishment, maintenance and release of an RRC connection between the UE and E-UTRAN,

- Security functions including key management, establishment, configuration, maintenance and release of point to point Radio Bearers.

Packet Data Convergence Control (PDCP)

PDCP Layer is responsible for

- Header compression and decompression of IP data,
- Transfer of data (user plane or control plane),
- Maintenance of PDCP Sequence Numbers (SNs),
- In-sequence delivery of upper layer PDUs at re-establishment of lower layers,
- Duplicate elimination of lower layer SDUs at re-establishment of lower layers for radio bearers mapped on RLC AM,
- Ciphering and deciphering of user plane data and control plane data,
- Integrity protection and integrity verification of control plane data,
- Timer based discard,
- duplicate discarding,
- PDCP is used for SRBs and DRBs mapped on DCCH and DTCH type of logical channels.

Non Access Stratum (NAS) Protocols

- The non-access stratum (NAS) protocols form the highest stratum of the control plane between the user equipment (UE) and MME.
- NAS protocols support the mobility of the UE and the session management procedures to establish and maintain IP connectivity between the UE and a PDN GW.

9. Discuss two evolution paths for the GSM to offer 3G services. [16m, Dec 2017]

- GSM operators have two nonexclusive options for evolving their networks to 3G wideband multimedia operation:
  (1) using GPRS and EDGE in the existing radio spectrum, and in small amounts of the new spectrum; or
  (2) using WCDMA in the new 2 GHz bands, or in large amounts of the existing spectrum.

- Both approaches offer a high degree of investment flexibility because roll-out can proceed in line with market demand with the extensive reuse of existing network equipment and radio sites.
- In the new 2 GHz bands, 3G capabilities are delivered using a new wideband radio interface that offers much higher user data rates than are available today — 384 kbps in the wide area and up to 2 Mbps in the local area.
- Of equal importance for such services is the high-speed packet switching provided by GPRS and its connection to public and private IP networks.

- GSM and digital (D)AMPS (IS-136) operators can use existing radio bands to deliver some of the 3G services, even without the new wideband spectrum by evolving current networks and deploying GPRS and EDGE technologies.
- In the early years of 3G service deployment, a large proportion of wireless traffic will still be voice-only and low-rate data.
- So whatever the ultimate capabilities of 3G networks, efficient and profitable ways of delivering more basic wireless services are still needed.
- The significance of EDGE for today's GSM operators is that it increases data rates up to 384 kbps and potentially even higher in a good quality radio environment using current GSM spectrum and carrier structures more efficiently.
- EDGE is both a complement and an alternative to new WCDMA coverage. EDGE also has the effect of unifying the GSM, D-AMPS and WCDMA services through the use of dual-mode terminals.

****

10. Explain the UMTS network architecture with GSM, 3G and also explain the reference architecture.

Third-Generation (3G) Wireless Systems

- The International Telecommunication Union (ITU) began studies on the globalization of personal communications in 1986 and identified the long-term spectrum requirements for the future *third-generation* (*3G*) mobile wireless telecommunications systems.
- In 1992, the ITU identified 230 MHz of spectrum in the 2 GHz and to implement the IMT-2000 system on a worldwide basis for satellite and terrestrial components.
- The aim of IMT-2000 is to provide universal coverage enabling terminals to have seamless roaming across multiple networks.
- The ITU accepted the overall standardization responsibility of IMT-2000 to define radio interfaces that are applicable in different radio environments including indoor, outdoor, terrestrial, and satellite.
- Figure 4.20 provides an overview of the IMT family.
- *IMT-DS* is the direct spread (DS) technology and includes WCDMA systems.
- This technology is intended for UMTS terrestrial radio access (UTRA)-FDD and is used in Europe and Japan.
- *IMT-TC* family members are the UTRA-TDD system that uses time division (TD) CDMA, and the Chinese TD-synchronous CDMA (TD-SCDMA).
- Both standards are combined and the third-generation partnership project (3GPP) is responsible for the development of the technology.
- *IMT-MC* includes multiple carrier (MC) cdma2000 technology, an evolution of the ***cdmaOne*** family.

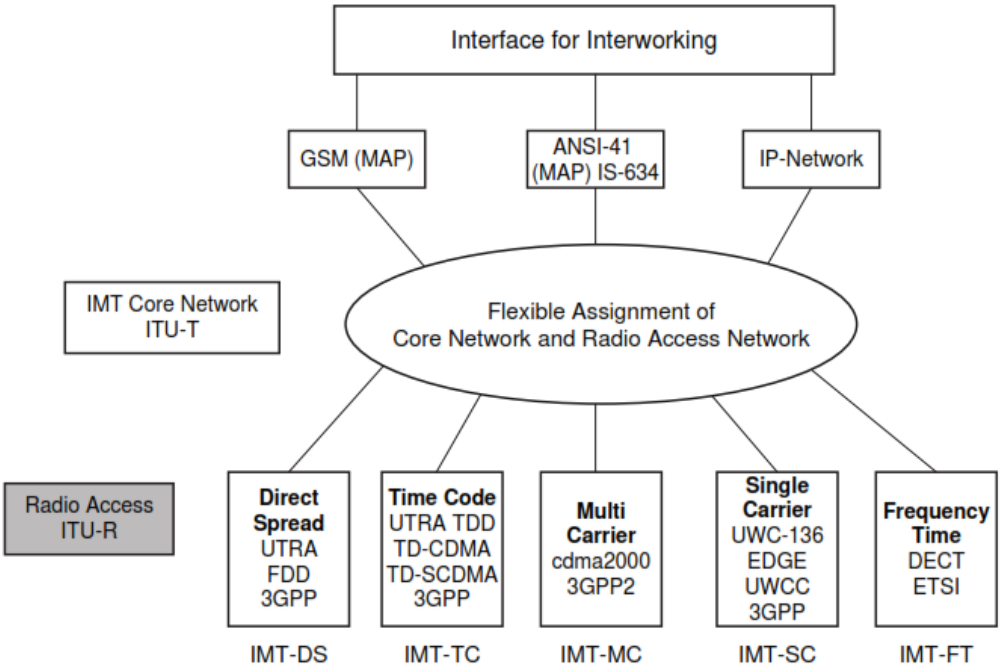


Figure 4.20 IMT family.

- 3GPP2 is responsible for standardization. *IMT-SC* is the enhancement of the US TDMA systems.
- UWC-136 is a single carrier (SC) technology.
- This technology applies EDGE to enhance the 2G IS-136 standard.
- It is now integrated into the 3GPP efforts.
- *IMT-FT* is a frequency time (FT) technology.
- An enhanced version of the cordless telephone standard digital European cordless technology (DECT) has been selected for low mobility applications.
- The ETSI has the responsibility for standardization of DECT.

- A primary assumption for UMTS is that it is based on an evolved GSM core network.
- This provides backward compatibility with GSM in terms of network protocols and interfaces (MAP, ISUP (ISDN user part), etc.)
- The core network supports both GSM and UMTS/IMT-2000 services, including handoff and roaming between the two (see Figure 4.21 15.10).
- The proposed W-CDMA based UMTS terrestrial radio access network (UTRAN) is connected to the GSM-UMTS core network using a new multi-vendor interface (*Iu*).
- The transport protocol within the new radio network and the core network will be IP.

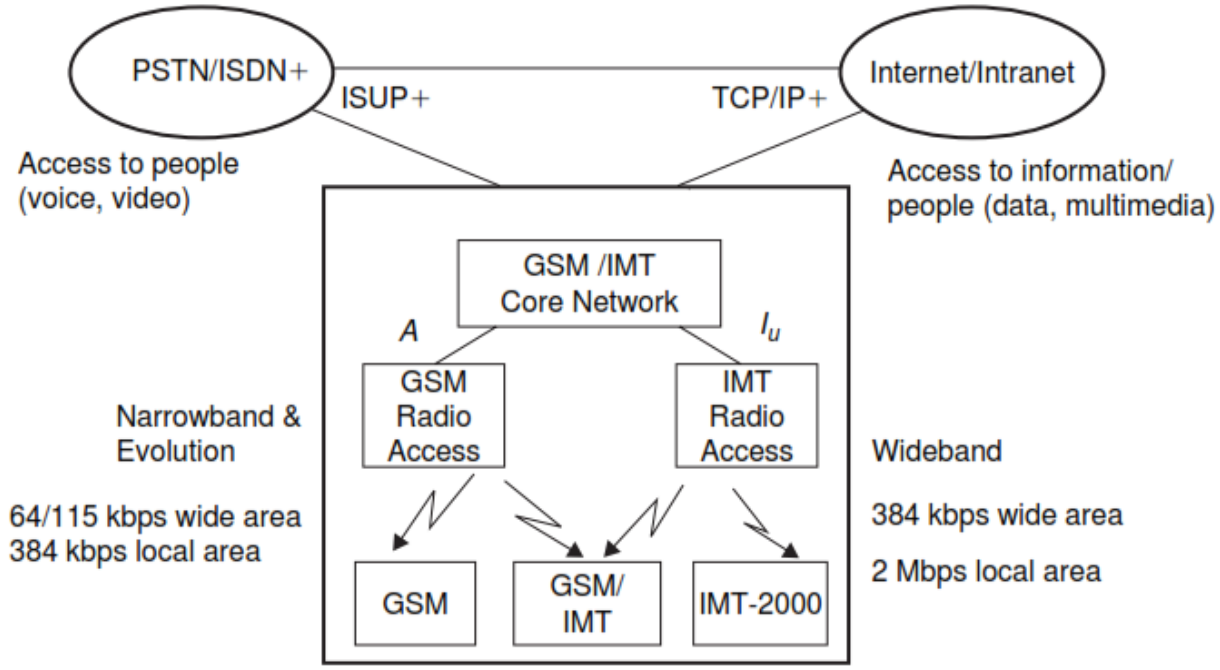


Figure 4.21 Evolution to UMTS/IMT-2000 in a GSM environment.

- There is a clear separation between the services provided by UTRAN and the actual channels used to carry these services.
- All radio network functions (such as resource control) are handled within the radio access network and clearly separated from the service and subscription functions in the UMTS core network (UCN).

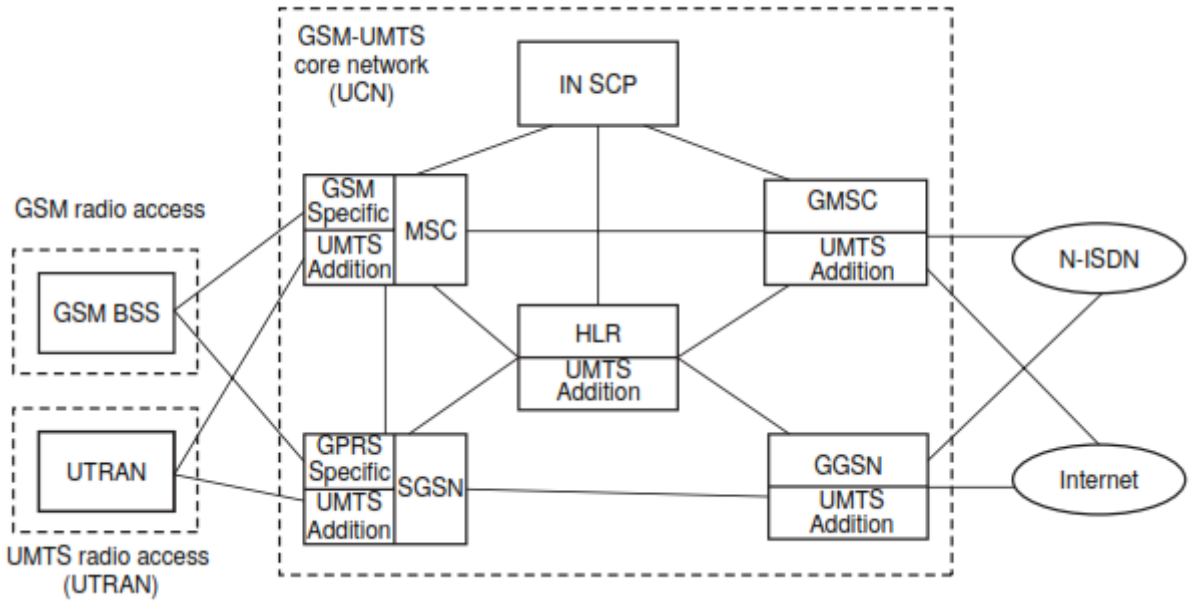


Figure 4.22 General GSM-UMTS network architecture.

- The GSM-UMTS network, shown in Figure 4.22 , consists of three main entities:
  - GSM-UMTS core network (UCN)
  - UMTS terrestrial radio access network (UTRAN)
  - GSM base station subsystem (BSS)

- Like the GSM-GPRS core network, the GSM-UMTS core network has two different parts: a circuit-switched MSC and a packet-switched GRPS support node (GSN).
- The core network access point for GSM circuit-switched connections is the GSM MSC, and for packet-switched connections it is the SGSN.

- GSM-defined services (up to and including GSM Phase 2+) are supported in the usual GSM manner.
- The GSM-UMTS core network implements supplementary services according to GSM principles (HLR-MSC/VLR).
- New services, beyond Phase 2+ are created using new service capabilities.
- These service capabilities may be seen as building blocks for application development and include:

    - Bearers defined by QoS
    - Mobile station execution environment (MExE)
    - Telephony value-added services (TeleVAS)
    - Subscriber identity module (SIM) toolkit
    - Location services
    - Open interfaces to mobile network functions
    - Down-loadable application software
    - Intelligent Network/Customized Applications for Mobile Enhanced Logic (IN/CAMEL) and service nodes.

- In addition to new services provided by the GSM-UMTS network itself, many new services and applications will be realized using a client/server approach, with servers residing on service local area networks (LANs) outside the GSM-UMTS core network.
- For such services, the core network simply acts as a transparent bearer.
- This approach is in line with current standardization activities, and is important from a service continuity point of view.
- The core network will ultimately be used for the transfer of data between the end-points, the client and the server.

****

15.4 UMTS Network Reference Architecture

- A UMTS system can be divided into a set of domains and the reference points that interconnect them.

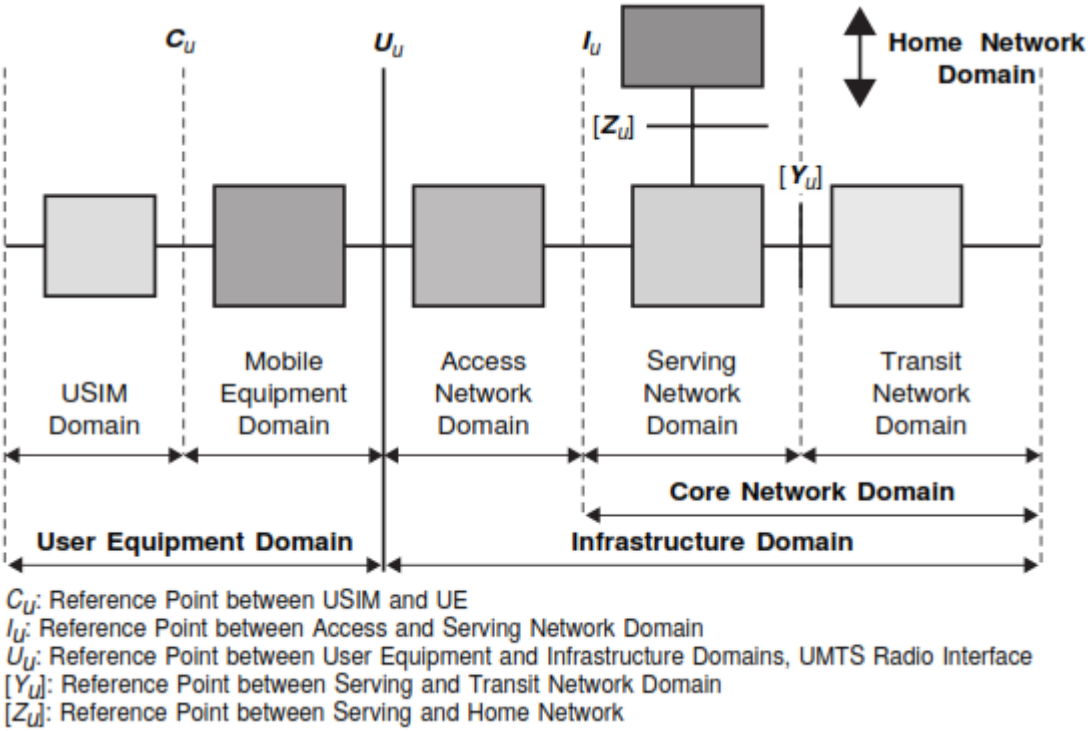


Figure 4.23 UMTS domains and reference points.

- Note that this is a reference model and does not represent any physical architecture.
- The *Iu* is split functionally into two logical interfaces, *I ups* connecting the packet switched domain to the access network and the *Iucs* connecting the circuit switched domain to the access network.
- The standards do not dictate that these are physically separate, but the user plane for each is different and the control plane may be different.
- The *Iur* logically connects radio network controllers (RNCs) but could be physically realized by a direct connection between RNCs or via the core network.

- Figures 4.23 and 4.24 show these domains and reference points.
- A simplified mapping of functional entities to the domain model is shown in Figure 15.25.

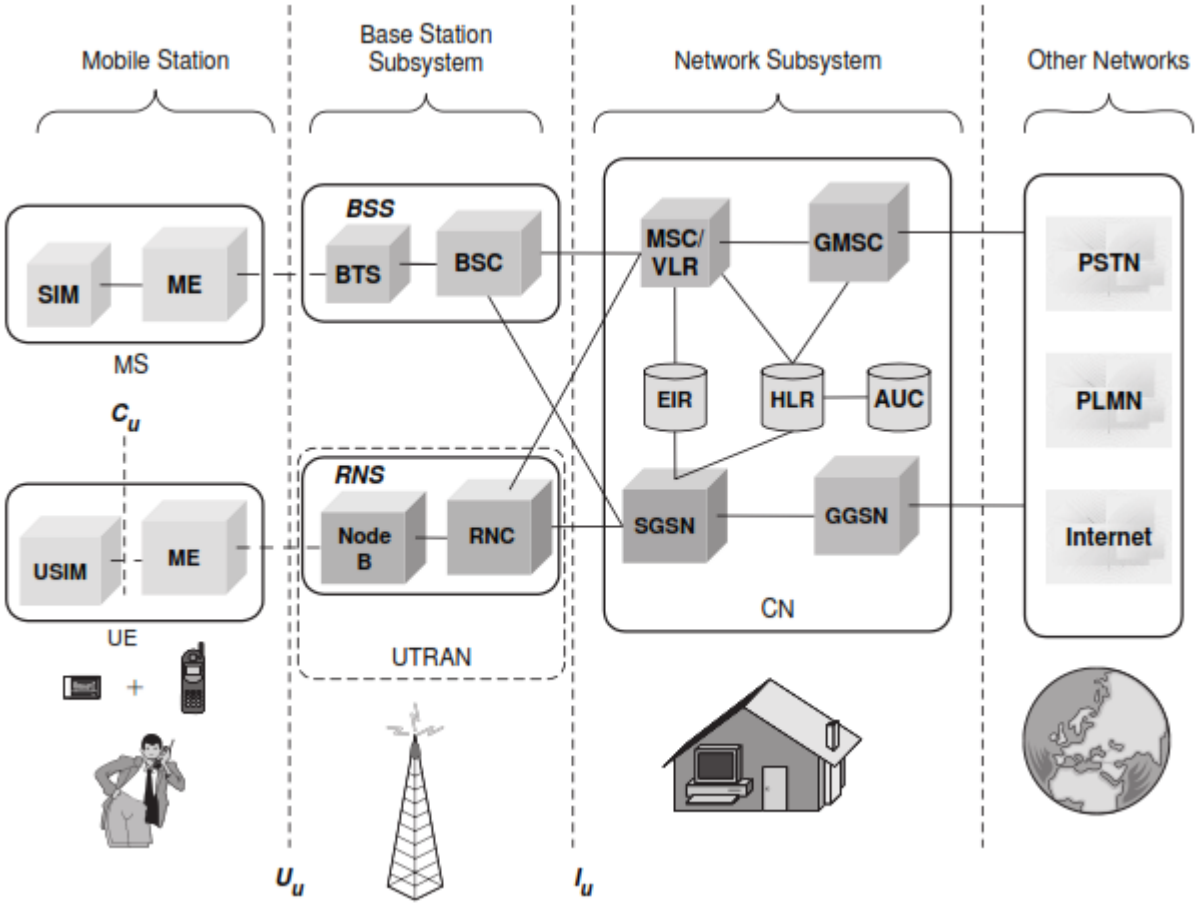


Figure 4.24 UMTS — 3G reference architecture.

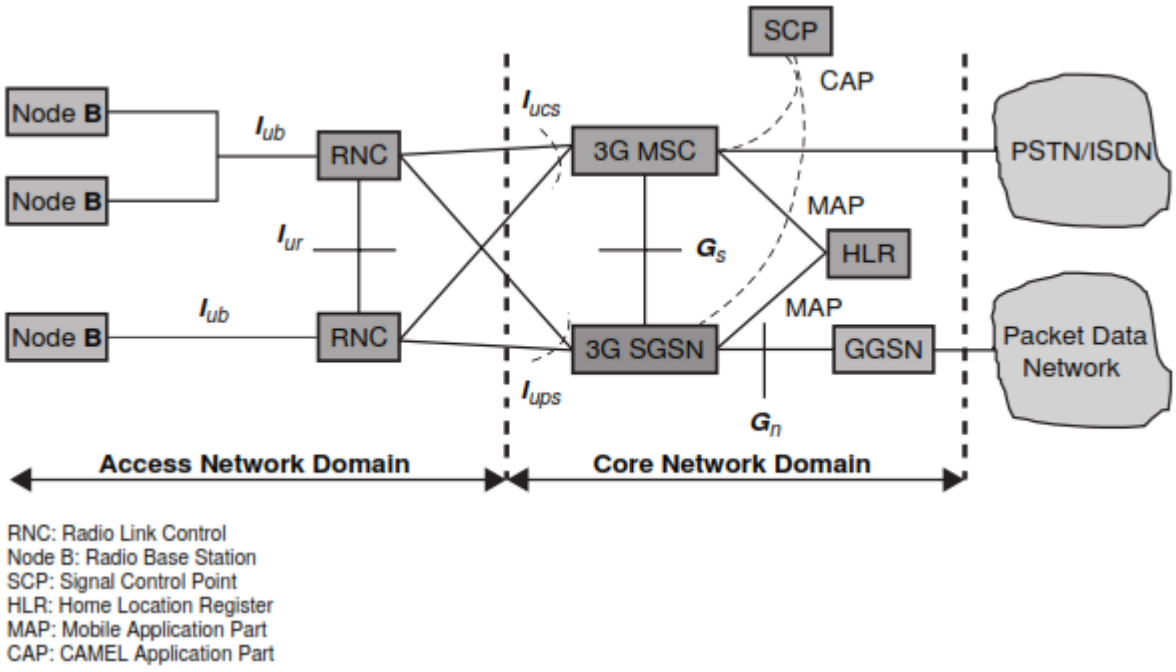


Figure 4.25 Simplified UMTS network reference model.

****

UNIT IV
WIRELESS WIDE AREA NETWORK

TWO MARKS

1. **Expand the following UMTS, UTRAN, RNS, RNC.**
   UMTS – Universal Mobile Telecommunications System
   UTRAN - UMTS Terrestrial Radio Access Network
   RNS - Radio Network Subsystem
   RNC - Radio Network Controller

UMTS Terrestrial Radio Access Network (UTRAN) Overview

1. **What does UTRAN consist? List the main logical elements of RNS.**
   The UTRAN consists of a set of ***Radio Network Subsystems*** (***RNS***s).
   The RNS has two main logical elements: ***Node B*** and an ***RNC***.

2. **Mention the responsibility of RNS.**
   The RNS is responsible for the ***radio resources*** and ***transmission/reception in a set of cells***.

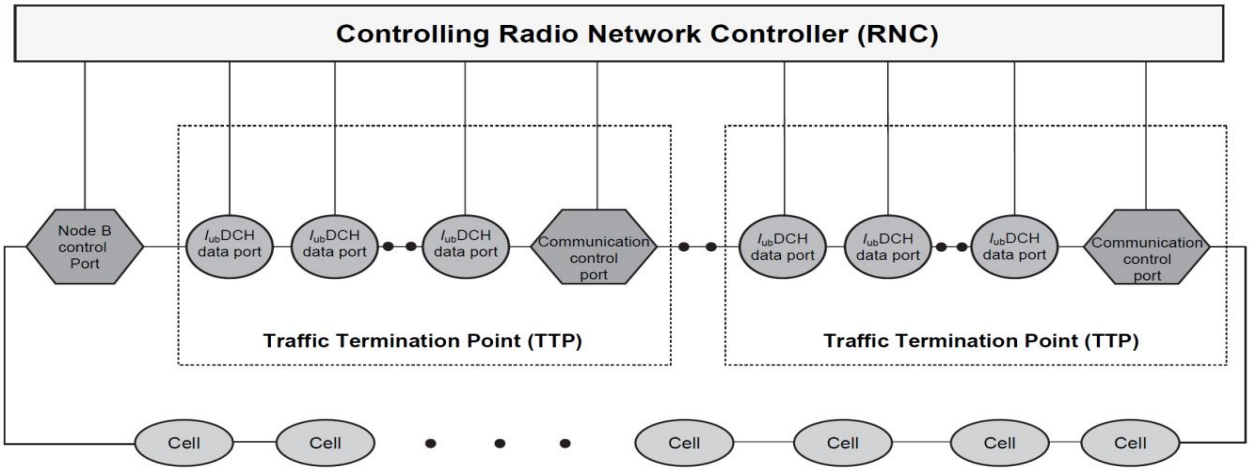
3. **What is a cell?**
   A ***cell*** (sector) is one coverage area served by a broadcast channel.

RNC (Radio Network Controller)

4. **Mention the responsibility of RNC.**
   The responsibilities of an RNC are:
   - ✓ Intra UTRAN handover
   - ✓ Macro diversity combining/splitting of Iub data streams
   - ✓ Frame synchronization
   - ✓ Radio resource management
   - ✓ Outer loop power control
   - ✓ Iu interface user plane setup
   - ✓ Serving RNS (SRNS) relocation

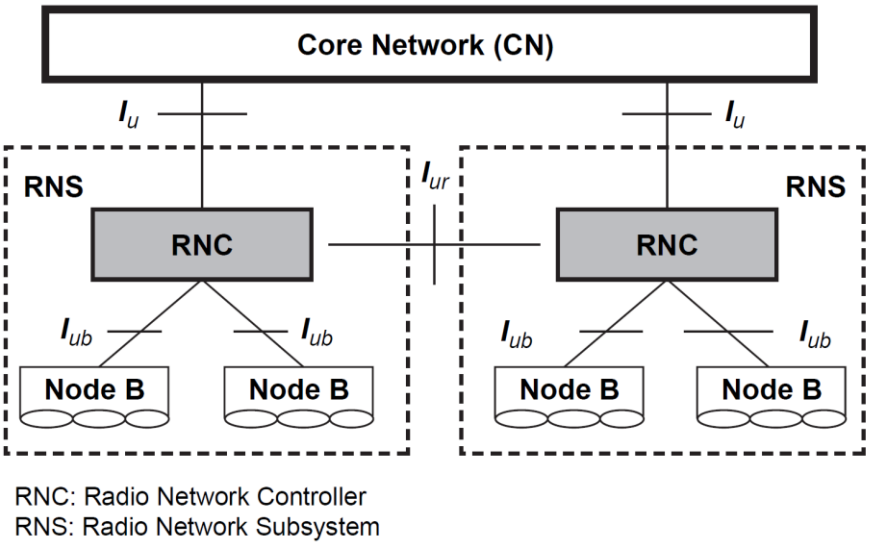
5. **What is Node B?**
   A Node B is responsible for radio transmission and reception in one or more cells to/from the user equipment (UE).

6. **Draw the logical architecture for Node B.**
   The logical architecture for Node B is shown,



7. Draw the logical architecture for UTRAN.

UTRAN logical architecture is shown,



RNC: Radio Network Controller
RNS: Radio Network Subsystem

8. Mention the responsibilities of Node B.

The following are the responsibilities of the Node B:

- ✓ Termination of Iub interface from RNC
- ✓ Termination of MAC protocol for transport channels RACH, FACH
- ✓ Termination of MAC, RLC, and RRC protocols for transport channels: BCH, PCH
- ✓ Radio environment survey (BER estimate, receiving signal strength, etc.)
- ✓ Inner loop power control
- ✓ Open loop power control
- ✓ RF processing

UTRAN Logical Interfaces

9. Design protocol structure of UTRAN.

- ✓ The layers and planes are logically independent of each other.
- ✓ If required, parts of protocol structure can be changed in the future without affecting other parts.

10. What do main layers of UTRAN protocol structure contains?

The protocol structure contains two main layers:

- ✓ Radio Network Layer (RNL)
- ✓ Transport Network Layer (TNL).

11. What is meant by RNL and TNL?

- ➢ In the RNL, all UTRAN-related functions are visible
- ➢ The TNL deals with transport technology selected to use for UTRAN but without any UTRAN-specific changes.

12. List the plane in UTRAN interface.

- ✓ Control Plane
- ✓ User plane
- ✓ Transport network control plane
- ✓ Transport network user plane

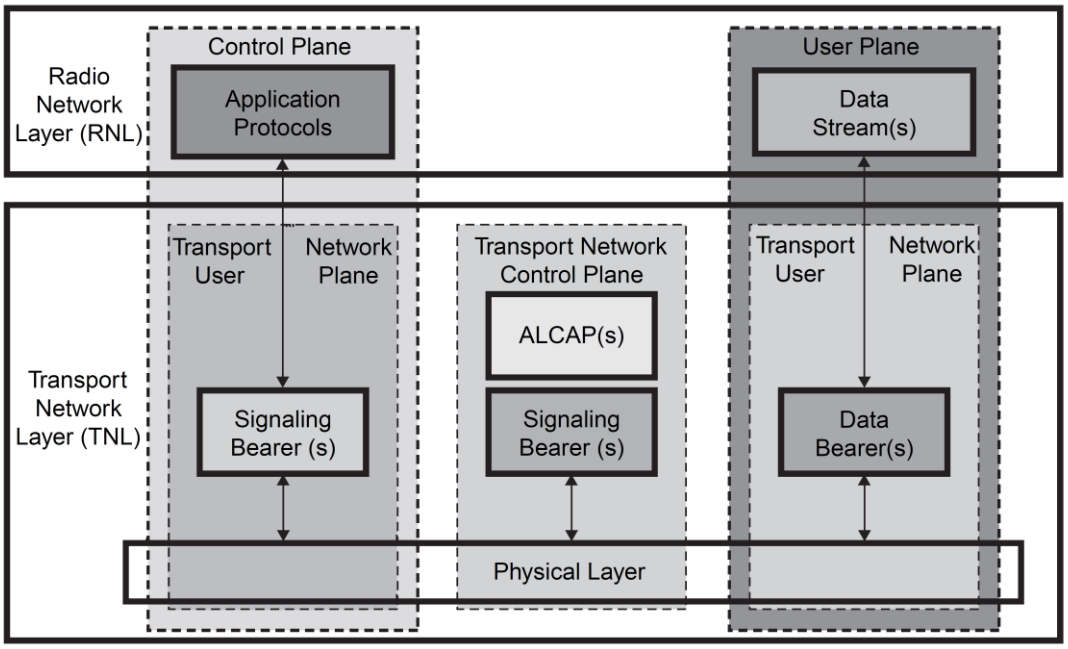
13. What is meant by Control plane in UTRAN interface?

The control plane is used for all UMTS-specific control signaling.

- ✓ It includes the
  - ***Application protocol***
    - Radio Access Network Application Part (RANAP) in I_u
    - Radio Network Subsystem Application Part (RNSAP) in I_{ur} and
    - Node B Application Part (NBAP) in I_{ub}.

14. Draw a general protocol model for UTRAN interfaces.

A general protocol model for UTRAN interfaces is shown,



ALCAP: Access Link Control Application Part

15. Define application protocol.

The application protocol is used for setting up bearers to the UE. In the three-plane structure the bearer parameters in the application protocol are not directly related to the ***user plane technology***, but rather they are ***general bearer parameters***.

16. What is meant by User plane in UTRAN interface?

- ✓ User information is carried by the user plane.
- ✓ The user plane includes ***data stream(s)***, and ***data bearer(s) for data stream(s)***.
- ✓ Each data stream is characterized by one or more ***frame protocols*** specified for that interface.

17. What does Transport Network Control plane in UTRAN interface carry?

The transport network control plane carries all control signaling within the transport layer.

- ✓ It does ***not include radio network layer information***.
- ✓ It contains ***Access Link Control Application Part (ALCAP)***
  - ALCAP is required to set up the transport bearers (data bearers) for the user plane.
- ✓ It also includes the ***signaling bearer*** needed for the ALCAP.
- ✓ The transport plane lies between the control plane and the user plane.
- ✓ The addition of the transport plane in UTRAN allows the application protocol in the radio network control plane to be totally independent of the technology selected for the data bearer in the user plane.

18. How does Transport Network User plane in UTRAN interface implemented?

With the transport network control plane, the transport bearers for data bearers in the user plane are set up in the following way.

- ➢ There is a signaling transaction by application protocol in the control plane that initiates set-up of the data bearer by the ALCAP protocol specific for the user plane technology.
- ➢ The independence of the control plane and user plane assumes that an ALCAP signaling occurs.
- ➢ The ALCAP may not be used for all types of data bearers.
- ➢ If there is no ALCAP signaling transaction, the transport network control plane is not required.
- ➢ This situation occurs when preconfigured data bearers are used.
- ➢ Also, the ALCAP protocols in the transport network control plane are not used to set up the signaling bearer for the application protocol or the ALCAP during real-time operation.

I_u **Interface**

19. What do you understand by UMTS Iu interface?

The UMTS ***Iu*** interface is the open logical interface that interconnects one UTRAN to the UMTS core network (UCN).

- ✓ On the UTRAN side the Iu interface is terminated at the RNC, and at the UCN side it is terminated at U-MSC.
- ✓ The Iu interface consists of three different protocol planes — the radio network control plane (RNCP), the transport network control plane (TNCP), and the user plane (UP).

20. What are the functions of RNCP?

The RNCP performs the following functions:

- ✓ It carries information for the general control of UTRAN radio network operations.
- ✓ It carries information for control of UTRAN in the context of each specific call.
- ✓ It carries user call control (CC) and mobility management (MM) signaling messages.

21. What are the service domains of control plane in the core network?

The control plane serves two service domains in the core network, the packet-switched (PS) domain and circuit-switched (CS) domain. The CS domain supports circuit-switched services. Some examples of CS services are voice and fax.

22. What are the services provided in CS domain?

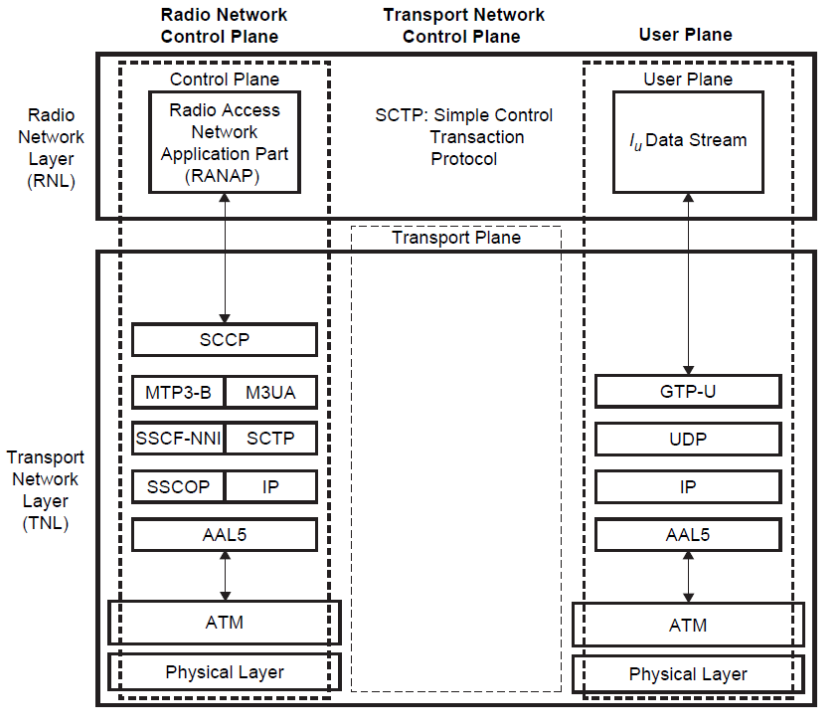
- ✓ The CS domain can also provide intelligent services such as voice mail and free phone.
- ✓ The CS domain connects to PSTN/ISDN networks.
- ✓ The CS domain is expected to evolve from the existing 2G GSM PLMN.

23. What are the services provided in PS domain?

- ✓ The PS domain deals with PS services.
- ✓ Some examples of PS services are Internet access and multimedia services.
- ✓ Since Internet connectivity is provided, all services currently available on the Internet such as search engines and e-mail are available to mobile users.
- ✓ The PS domain connects to IP networks. The PS domain is expected to evolve from the GPRS PLMN.

24. Draw I_u packet-switched protocol architecture.

The Iu packet-switched protocol architecture is shown,



I_u packet-switched protocol architecture

25. What does control plane protocol stack in Iu packet-switched consist?

The control plane protocol stack consists of RANAP (Radio Access Network Application Part) on the top of signaling system 7 (SS7) protocols.

26. What are the protocol layers of control plane protocol stack in Iu packet-switched?

The protocol layers are,

- ✓ Signaling Connection Control Part (SCCP),
- ✓ Message Transfer Part (MTP3-B),
- ✓ Signaling Asynchronous Transfer Mode (ATM) Adaptation Layer for Network-To-Network Interface (SAAL-NNI).

27. What is meant by SAAL – NNI?

The SAAL-NNI is divided into service-specific coordination function (SSCF), the service-specific connection-oriented protocol (SSCOP), and ATM adaptation layer 5 (AAL5) layers.

- ➢ The SSCF and SSCOP layers are specifically designed for signaling transport in ATM networks, and take care of signaling connection management functions.
- ➢ AAL5 is used for segmenting the data to ATM cells.

28. What does an IP-based signaling bearer consist?

The IP-based signaling bearer consists of SS7-MTP3—user adaptation layer (M3UA), simple control transmission protocol (SCTP), IP, and AAL5.

- ➢ The SCTP layer is specifically designed for signaling transport on the Internet.
- ➢ The transport network control plane (TNCP) carries information for the control of transport network used within UCN.

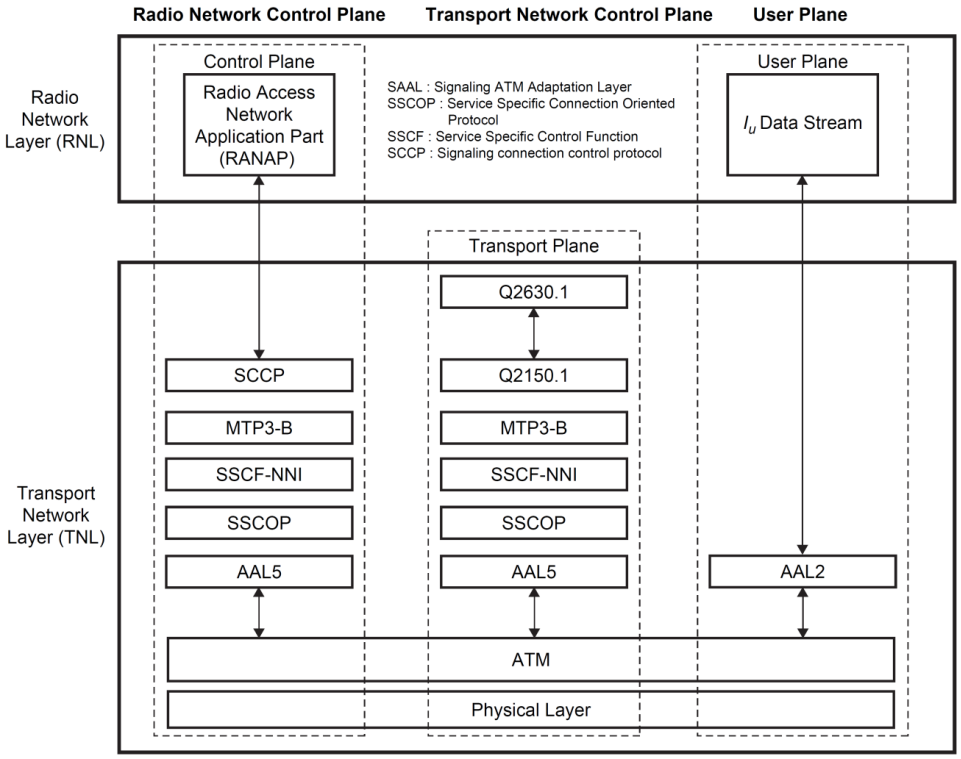
29. What does user plane carry in Iu circuit-switched protocol architecture?

The user plane (UP) carries user voice and packet data information.

- ➢ AAL2 is used for the following services: narrowband speech (e.g., EFR, AMR); unrestricted digital information service (up to 64 kbps, i.e., ISDN B channel); any low to average bit rate CS service (e.g., modem service to/from PSTN/ISDN). A
- ➢ AL5 is used for the following services: non-real-time PS data service (i.e., best effort packet access) and real-time PS data.

30. Draw I_u circuit-switched protocol architecture.

The I_u circuit-switched protocol architecture is shown,



***I_u* circuit-switched protocol architecture**

I_{ur} Interface

31. What is Iur interface?

The connection between two RNCs (serving RNC (SRNC) and drift RNC (DRNC)) is the I_{ur} interface.

- It is used in soft handoff scenarios when different macro diversity streams of one communication are supported by Node Bs that belongs to different RNCs.
- Communication between one RNC and one Node B of two different RNCs are realized through the ***I_{ur}*** interface.

32. What are the different protocol planes in Iur and Iub interface?

Three different protocol planes are defined for it:

- ✓ Radio network control plane (RNCP)
- ✓ Transport network control plane (TNCP)
- ✓ User plane (UP)

33. What does *I_{ur}* interface carry?

The Iur interface is used to carry:

- ✓ Information for the control of radio resources in the context of specific service request of one mobile on RNCP
- ✓ Information for the control of the transport network used within UTRAN on TNCP
- ✓ User voice and packet data information on UP

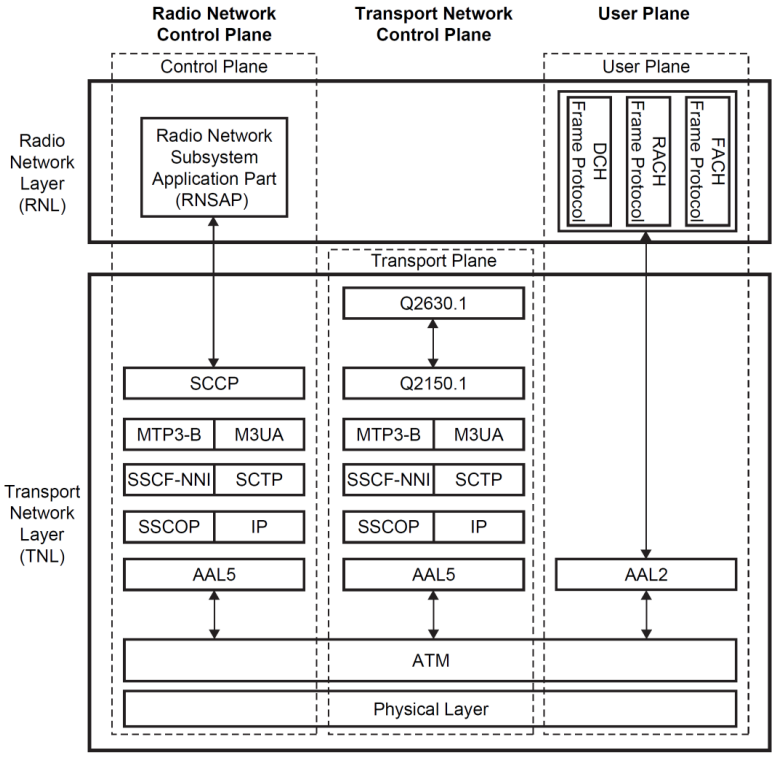
34. List the uses of protocol in Iur interface.

The protocols used on this interface are:

- ✓ Radio access network application part (RANAP)
- ✓ DCH frame protocol (DCHFP)
- ✓ RACH frame protocol (RACHFP)
- ✓ FACH frame protocol (FACHFP)

35. Draw the protocol structure of the I_{ur} interface.

The protocol structure of the I_{ur} interface is shown.



36. Mention the functions of I_{ur} interface.

The I_{ur} provides the following four functions:

- ✓ Basic inter-RNC mobility support
- ✓ Dedicated channel traffic support
- ✓ Common channel traffic support
- ✓ Global resource management support

37. What are the functions of Basic inter-RNC mobility in I_{ur} interface?

Basic inter-RNC mobility supports,

- ✓ Support of SRNC relocation
- ✓ Support of inter-RNC cell and UTRAN registration area update
- ✓ Support of inter-RNC packet paging
- ✓ Reporting of protocol errors

38. What are the functions of Dedicated channel traffic in I_{ur} interface?

Dedicated channel traffic supports,

- ➢ Establishment, modification, and release of a dedicated channel in the DRNC due to hard and soft handoff in the dedicated channel state
- ➢ Setup and release of dedicated transport connections across the I_{ur} interface
- ➢ Transfer of DCH transport blocks between SRNC and DRNC
- ➢ Management of radio links in the DRNS via dedicated measurement report procedures and power setting procedures.

39. What are the functions of Common channel traffic in I_{ur} interface?

Common channel traffic supports,

- ➢ Setup and release of the transport connection across the I_{ur} for common channel data streams

- Splitting of the MAC layer between the SRNC (MAC-d) and DRNC
- (MAC-c and MAC-sh); the scheduling for downlink data transmission is performed in the DRNC
- Flow control between the MAC-d and MAC-c/MAC-sh.

40. Briefly give a note on how Global resource management support in Iur interface

Global resource management supports,

- Transfer of cell measurements between two RNCs
- Transfer of Node B timing between two RNCs

I_{ub} Interface

41. What is I_{ub} interface and what is the function of the same?

The connection between the RNC and Node B is the I_{ub} interface. There is one I_{ub} interface for each Node B. The I_{ub} interface is used for all of the communications between Node B and the RNC of the same RNS.

42. What does I_{ub} interface carry?

The I_{ub} interface is used to carry:

- ✓ Information for the general control of Node B for radio network operation on RNCP
- ✓ Information for the control of radio resources in the context of specific service request of one mobile on RNCP
- ✓ Information for the control of a transport network used within UTRAN on TCNP
- ✓ User CC and MM signaling message on RNCP
- ✓ User voice and packet data information on UP

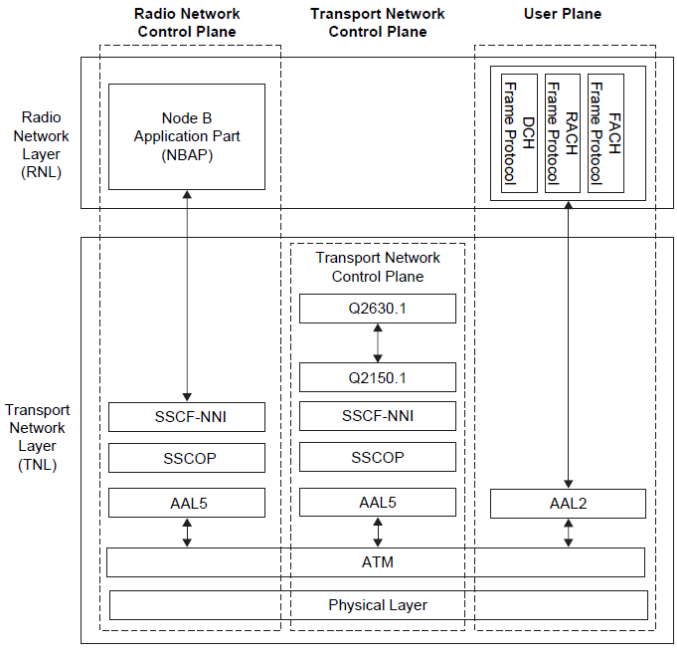
43. List the uses of protocol in Iub interface.

The protocols used on this interface include:

- ✓ Node B application part protocol (NBAP)
- ✓ DCH frame protocol (DCHFP)
- ✓ RACH frame protocol (RACHFP)
- ✓ FACH frame protocol (FACHFP)
- ✓ Access link control application part (ALCAP)
- ✓ Q.aal2
- ✓ SSCP or TCP and IP
- ✓ MTP3-B
- ✓ SAAL-UNI (SSCF-UNI, SSCOP, and AAL5)

44. Draw the protocol structure for the interface Iub.

The protocol structure for the interface Iub is shown.



U_u Interface

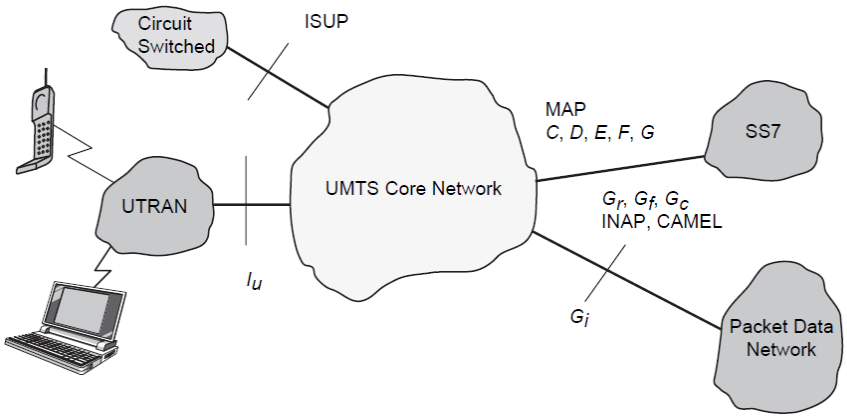
45. Define Uu interface.

The UMTS ***U_u*** interface is the radio interface between a Node B and one of its UE. The ***U_u*** is the interface through which UE accesses the fixed part of the system.

UMTS Core Network Architecture

46. Draw UMTS Core Network Architecture.

UMTS core network architecture is shown,



47. What does UCN consist?

The UCN consists of a CS entity for providing voice and CS data services and a PS entity for providing packet-based services. The logical architecture offers a clear separation between the CS domain and PS domain.

48. Mention the functions of CS domain in UCN.

The CS domain contains the functional entities: mobile switching center (MSC) and gateway MSC (GMSC).

49. Mention the functions of PS domain in UCN.

The PS domain comprises the functional entities:

- serving GPRS support node (SGSN),

- gateway GPRS support node (GGSN),
- domain name server (DNS),
- dynamic host configuration protocol (DHCP) server,
- packet charging gateway, and
- firewalls.

50. What are the different functional areas of UCN?

The core network can be split into the following different functional areas:

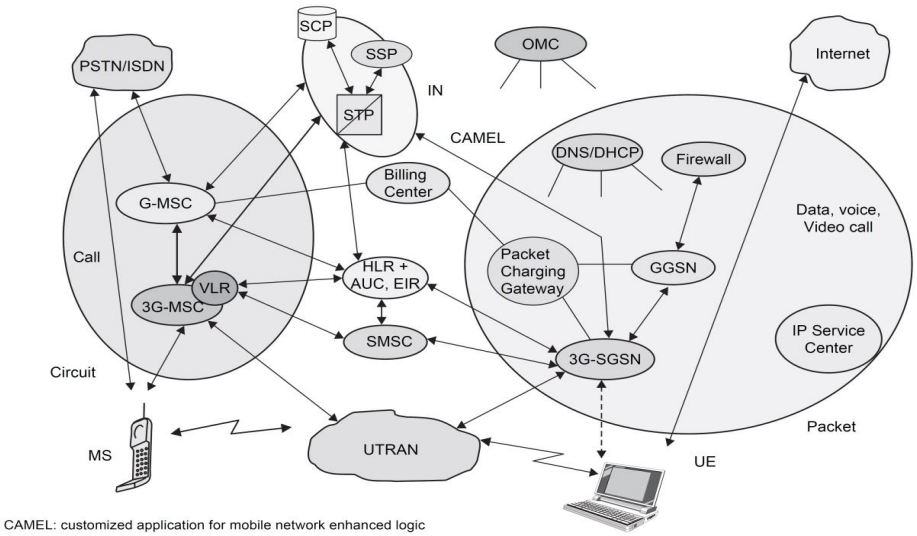
- ✓ Functional entities needed to support PS services (e.g. 3G-SGSN, 3G-GGSN)
- ✓ Functional entities needed to support CS services (e.g. 3G-MSC/VLR)
- ✓ Functional entities common to both types of services (e.g. 3G-HLR)

Other areas that can be considered part of the core network include:

- ✓ Network management systems (billing and provisioning, service management, element management, etc.)
- ✓ IN system (service control point (SCP), service signaling point (SSP), etc.)
- ✓ ATM/SDH/IP switch/transport infrastructure

51. Draw Logical architecture of the UMTS core network.

Logical architecture of the UMTS core network is shown



52. What is 3G-MSC?

- ➢ The 3G-MSC is the main CN element to provide CS services.
- ➢ The 3G-MSC also provides the necessary control and corresponding signaling interfaces including SS7, MAP, ISUP (ISDN user part), etc.
- ➢ The 3G MSC provides the interconnection to external networks like PSTN and ISDN.

53. What are the functions of 3G-MSC?

The following functionality is provided by the 3G-MSC:

- ✓ Mobility management
- ✓ Call management
- ✓ Supplementary services

- ✓ CS data services
- ✓ Vocoding
- ✓ SS7, MAP and RANAP interfaces
- ✓ ATM/AAL2
- ✓ Short message services (SMS)
- ✓ VLR functionality
- ✓ IN and CAMEL.
- ✓ OAM (Operation, Administration, and Maintenance) agent functionality.

54. What is 3G-SGSN?

- ➢ The 3G-SGSN is the main CN element for PS services.
- ➢ The 3G-SGSN provides the necessary control functionality both toward the UE and the 3G-GGSN.
- ➢ It also provides the appropriate signaling and data interfaces including connection to
  - ✓ an IP-based network toward the 3G-GGSN,
  - ✓ SS7 toward the HLR/EIR/AUC, and
  - ✓ TCP/IP or SS7 toward the UTRAN.

55. What are the functions of 3G-SGSN?

The 3G-SGSN provides the following functions:

- ✓ Session management
- ✓ I_u and G_n MAP interface
- ✓ ATM/AAL5
- ✓ SMS
- ✓ Mobility management
- ✓ Subscriber database functionality
- ✓ Charging
- ✓ OAM agent functionality.

56. What is 3G-GGSN?

- ➢ The GGSN provides interworking with the external PS network.
- ➢ It is connected with SGSN via an IP-based network.
- ➢ The GGSN may optionally support an SS7 interface with the HLR to handle mobile terminated packet sessions.

57. Mention the functions of 3G-GGSN.

The 3G-GGSN provides the following functions:

- ✓ Maintain information locations at SGSN level (macro-mobility)
- ✓ Gateway between UMTS packet network and external data networks (e.g. IP, X.25)
- ✓ Gateway-specific access methods to intranet (e.g. PPP termination)
- ✓ Initiate mobile terminate Route Mobile Terminated packets
- ✓ User data screening/security can include subscription based, user controlled, or network controlled screening.
- ✓ User level address allocation
- ✓ Charging
- ✓ OAM functionality

58. What is SMS-GMSC/SMS-IWMSC?

- The overall requirement for these two nodes is to handle the SMS from point to point. The functionality required can be split into two parts.
- The SMS-GMSC is an MSC capable of
  - ✓ Receiving a terminated short message from a service center,
  - ✓ Interrogating an HLR for routing information and SMS information, and
  - ✓ Delivering the short message to the SGSN of the recipient UE.
- The SMS-IWMSC is an MSC capable of receiving an originating short message from within the PLMN and submitting it to the recipient service center.

59. Mention the functions of SMS-GMSC.

The SMS-GMSC provides the following functions:

- ✓ Reception of short message packet data unit (PDU)
- ✓ Interrogation of HLR for routing information
- ✓ Forwarding of the short message PDU to the MSC or SGSN using the routing information

60. Mention the functions of SMS-IWMSC.

The SMS-IWMSC provides the following functions:

- ✓ Reception of the short message PDU from either the 3G-SGSN or 3G-MSC
- ✓ Establishing a link with the addressed service center
- ✓ Transferring the short message PDU to the service center

61. What is Firewall? (Nov 2017) (or)

What is the purpose of firewall used in UMTS network? (April 2017)

- This entity is used to protect the service providers' backbone data networks from attack from external packet data networks.
- The security of the backbone data network can be ensured by applying packet filtering mechanisms based on access control lists or any other methods deemed suitable.

62. What is DNS/DHCP?

- The DNS server is used, as in any IP network, to translate host names into IP addresses, i.e., logical names are handled instead of raw IP addresses.
- Also, the DNS server is used to translate the access point name (APN) into the GGSN IP address.
- It may optionally be used to allow the UE to use logical names instead of physical IP addresses.
- A dynamic host configuration protocol server is used to manage the allocation of IP configuration information by automatically assigning IP addresses to systems configured to use DHCP.

High-Speed Downlink Packet Access (HSDPA)

63. What is HSDPA?

HSDPA is based on the same set of technologies as high data rate (HDR) to improve spectral efficiency for data services such as

- Shared downlink packet data channel and high peak data rates — *using high-order modulation and adaptive modulation and coding,*

- Hybrid ARQ (HARQ) retransmission schemes,
- Fast scheduling, and
- Shorter frame sizes.

HSDPA marks a similar boost for WCDMA that EDGE does for GSM.

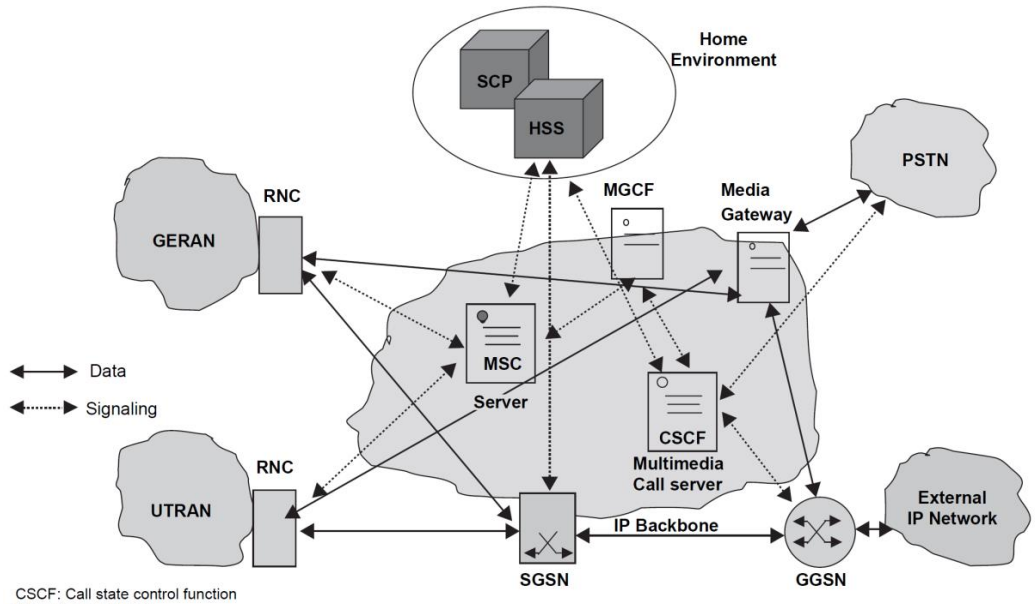
64. List the performance improvements in HSDPA.

The improvements in performance are achieved by:

- ✓ Bringing some key functions, such as
  - scheduling of data packet transmission and processing of retransmissions (in case of transmission errors) into the base station — that is, closer to the air interface.
- ✓ Using a short frame length to further accelerate packet scheduling for transmission.
- ✓ Employing incremental redundancy for minimizing the air-interface load caused by retransmissions.
- ✓ Adopting a new transport channel type, known as High-Speed Downlink Shared Channel (HSDSCH), to facilitate air interface channel sharing between several users.
- ✓ Adapting the modulation and coding scheme according to the quality of the radio link

65. Draw a simplified all-IP UMTS architecture.

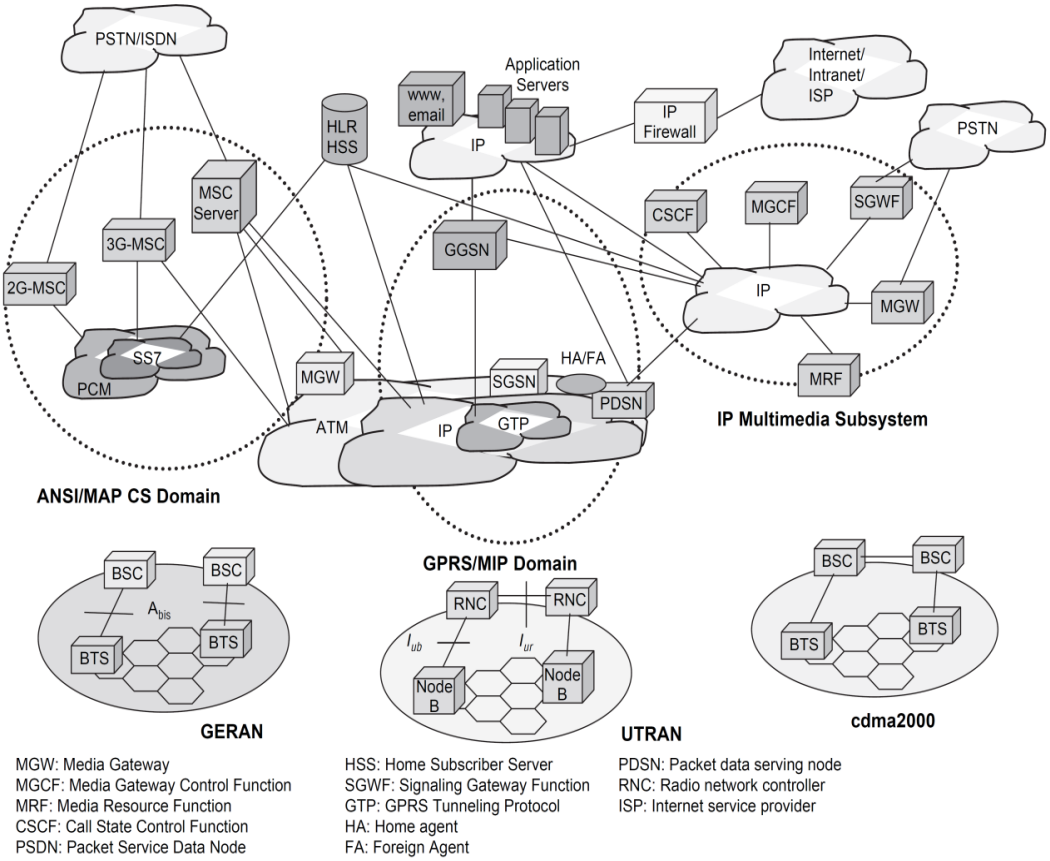
A simplified all-IP UMTS architecture is shown,



CSCF: Call state control function
MG: Media gateway
MGCF: Media gateway control function
HSS: Home subscriber server
SCP: Signal Control Point
RNC: Radio Network Controller
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
GERAN: GPRS/EDGE Radio Access Network
UTRAN: UMTS Radio Access Network

66. Draw all-IP core network architecture for UMTS.

All-IP core network architecture for UMTS is shown,



MGW: Media Gateway
MGCF: Media Gateway Control Function
MRF: Media Resource Function
CSCF: Call State Control Function
PSDN: Packet Service Data Node

HSS: Home Subscriber Server
SGWF: Signaling Gateway Function
GTP: GPRS Tunneling Protocol
HA: Home agent
FA: Foreign Agent

PDSN: Packet data serving node
RNC: Radio network controller
ISP: Internet service provider

67. Give the basic operational principles behind HSDPA.

Basic operational principles behind HSDPA

- Principles are relatively simple.
- RNC
- Node B
- UE
- Bandwidth
- Data Rate

68. Tabulate HSDPA data rates.

Chip rate = 3.84 Mcps, frame size = 3 slots				
Modulation	**Coding rate**	**Throughput with 5 codes**	**Throughput with 10 codes**	**Throughput with 15 codes**
16-QAM	1/2	2.4 Mbps	4.8 Mbps	7.2 Mbps
16-QAM	3/4	3.6 Mbps	7.2 Mbps	10.8 Mbps
16-QAM	4/4	4.8 Mbps	9.6 Mbps	14.4 Mbps
QPSK	1/4	600 kbps	1.2 Mbps	1.8 Mbps
QPSK	1/2	1.2 Mbps	2.4 Mbps	3.6 Mbps
QPSK	3/4	1.8 Mbps	3.6 Mbps	5.4 Mbps

69. Mention the issues of implementation in HSDPA.

Implementation Issues:

- ✓ Architectural issues
- ✓ Network deployment

- ✓ Core processing chassis

70. List the new channels introduced in HSDPA.

Three New channels introduced in HSDPA:

- ✓ High-speed downlink shared channel (HS-DSCH)
- ✓ High-speed shared control channel (HS-SCCH), and
- ✓ High speed dedicated physical control channel (HS-DPCCH).

71. What is HS-DSCH?

- ✓ The HS-DSCH is the primary radio bearer.
- ✓ Its resources can be shared among all users in a particular sector.
- ✓ The primary channel multiplexing occurs in a time domain, where each TTI consists of three time slots (each 2 ms).
- ✓ TTI is also referred to as a sub-frame.
- ✓ Within each 2 ms TTI, a constant spreading factor (SF) of 16 is used for code multiplexing, with a maximum of 15 parallel codes allocated to HS-DSCH.
- ✓ Codes may all be assigned to one user, or may be split across several users.
- ✓ The number of codes allocated to each user depends on cell loading, QoS requirements, and UE code capabilities (5, 10, or 15 codes).

72. What is HS-SCCH?

- ✓ The HS-SCCH (a fixed rate 960 kbps, SF = 128).
- ✓ It is used to carry downlink signaling between Node B and UE before the beginning of each scheduled TTI.
- ✓ It includes UE identity, HARQ-related information and the parameters of the HS-DSCH transport format selected by the link-adaptation mechanism.
- ✓ Multiple HS-SCCHs can be configured in each sector to support parallel HS-DSCH transmissions.
- ✓ A UE can be allocated a set of up to four HS-SCCHs, which need to be monitored continuously.

73. What is HS-DPCCH?

- ✓ The HS-DPCCH (SF = 256) carries ACK/NACK signaling to indicate whether the corresponding downlink transmission was successfully decoded, as well as a channel quality indicator (CQI) to be used for the purpose of link adaptation.
- ✓ The CQI is based on a common pilot channel (CPICH)
  - It is used to estimate the transport block size, modulation type, and number of channelization codes
  - The codes support for reliability level in downlink transmission.
- ✓ The feedback cycle of CQI can be set as a network parameter in predefined steps of 2 ms.

74. List out UE capabilities.

- ➢ UE capabilities include
  - ✓ The maximum number of HS-DSCHs supported simultaneously (5, 10, or 15)

- ✓ Minimum TTI time (minimum time between the beginning of two consecutive transmissions to the UE),
- ✓ The maximum number of HS-DSCH transport block (TB) bits received within an HS-DSCH TTI
- ✓ The maximum number of soft channel bits over all HARQ and supported modulations (QPSK only or both QPSK and 16-QAM).

75. Tabulate UE categories in HSDPA.

Category	Codes	Inter-TTI	TB size (bits)	Total soft bits	Modulation	Data rate (Mbps)
1	5	3	7300	19,200	QPSK/QAM	1.2
2	5	3	7300	28,800	QPSK/QAM	1.2
3	5	2	7300	28,800	QPSK/QAM	1.8
4	5	2	7300	38,400	QPSK/QAM	1.8
5	5	1	7300	57,600	QPSK/QAM	3.6
6	5	1	7300	67,200	QPSK/QAM	3.6
7	10	1	14,600	115,200	QPSK/QAM	7.2
8	10	1	14,600	134,400	QPSK/QAM	7.2
9	15	1	20,432	172,800	QPSK/QAM	10.2
10	15	1	28,776	172,800	QPSK/QAM	14.4
11	5	2	3650	14,400	QPSK	0.9
12	5	1	3650		QPSK	1.8

LTE Network Architecture

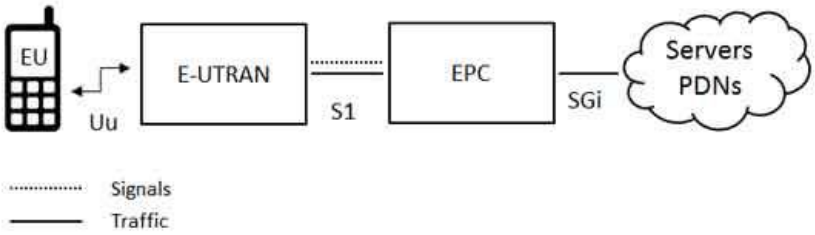
76. What are the main components of LTE network architecture?

The high-level network architecture of LTE is comprised of following three main components:

- The User Equipment *UE*
- The Evolved UMTS Terrestrial Radio Access Network *E−UTRAN*
- The Evolved Packet Core *EPC*

77. Draw the interfaces between the different parts of the system.

The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below:



78. What are the modules of mobile equipment?

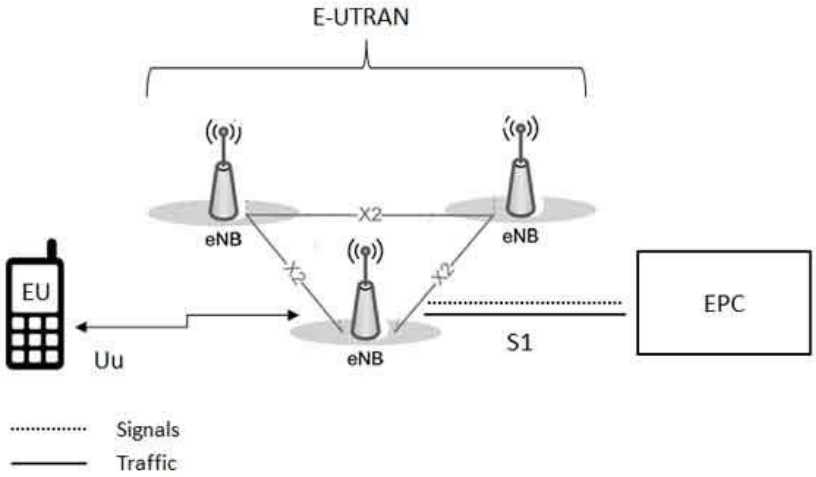
The mobile equipment comprised of the following important modules:

- ✓ Mobile Termination *MT*
- ✓ Terminal Equipment *TE*

- ✓ Universal Integrated Circuit Card *UICC*

79. Draw the architecture of E-UTRAN.

The architecture of *E−UTRAN* has been illustrated below.



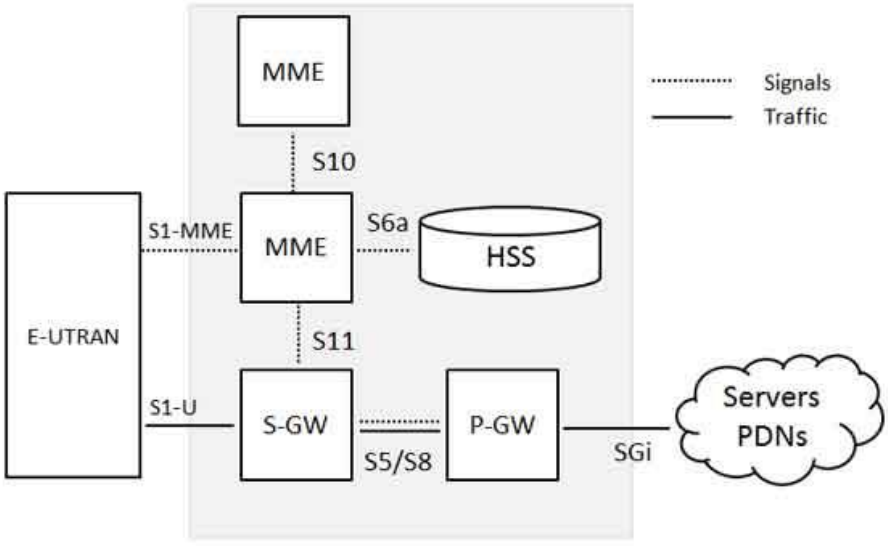
80. Mention the functions of LTE.

- The eNB sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
- The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

The Evolved Packet Core *EPC*

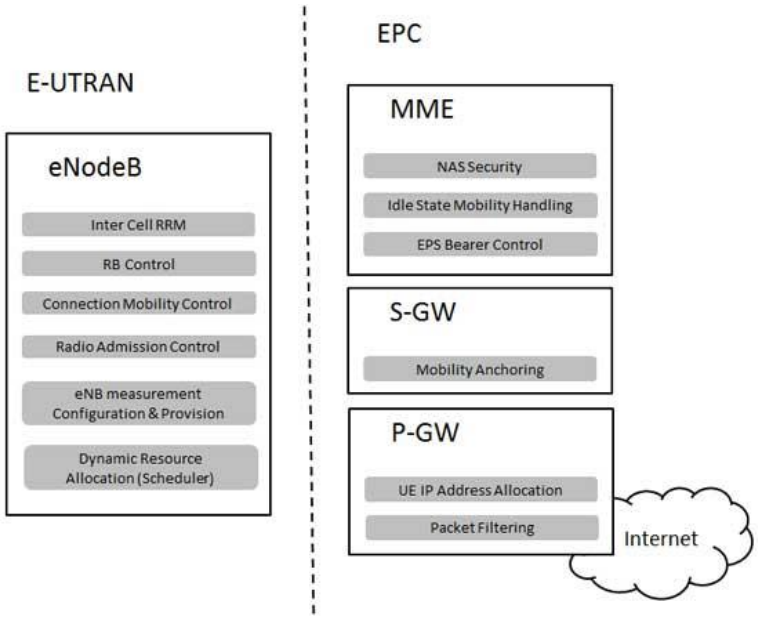
81. Draw the architecture of Evolved Packet Core *EPC.*

The architecture of Evolved Packet Core *EPC* has been illustrated below.



82. List the functional split between the E-UTRAN and the EPC.

Following diagram shows the functional split between the E-UTRAN and the EPC for an LTE network:

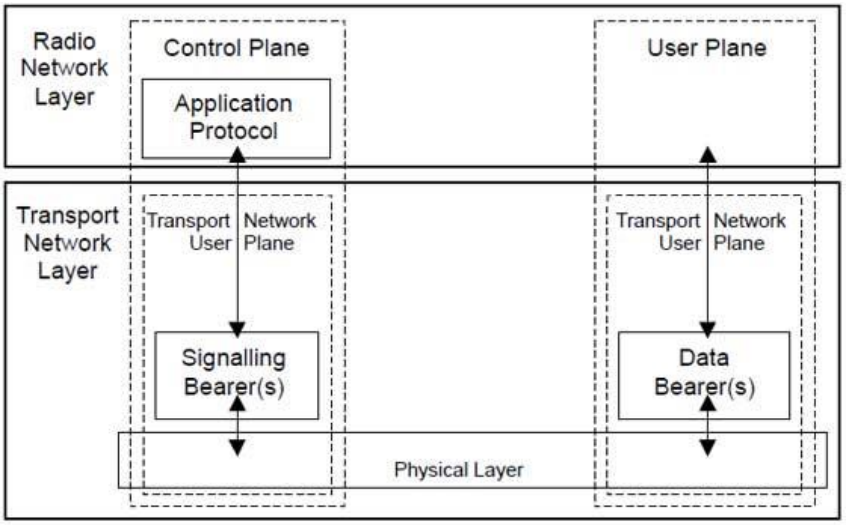


83. Distinguish between 2G/3G and LTE.

2G/3G	**LTE**
GERAN and UTRAN	E-UTRAN
SGSN/PDSN-FA	S-GW
GGSN/PDSN-HA	PDN-GW
HLR/AAA	HSS
VLR	MME
SS7-MAP/ANSI-41/RADIUS	Diameter
DiameterGTPc-v0 and v1	GTPc-v2
MIP	PMIP

84. Draw LTE Radio Protocol Architecture.

The radio protocol architecture for LTE can be separated into **control plane** architecture and **user plane** architecture as shown below:



85. What are the sub layers of User Plane in LTE?

The user plane protocol stack between the e-Node B and UE consists of the following sub-layers:

- PDCP (Packet Data Convergence Protocol)
- RLC (radio Link Control)
- Medium Access Control (MAC)

86. What is control plane in LTE?

- The control plane includes additionally the Radio Resource Control layer (RRC) which is responsible for configuring the lower layers.
- The Control Plane handles radio-specific functionality which depends on the state of the user equipment which includes two states: idle or connected.

87. Give a note on idle mode and connected mode.

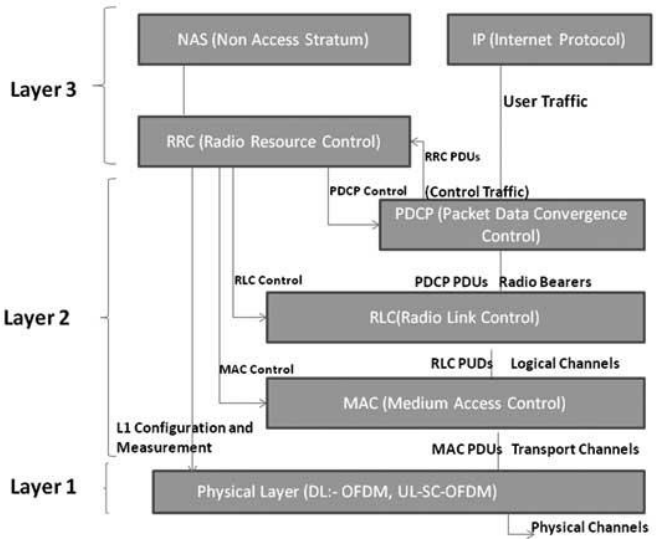
Mode	Description
Idle	The user equipment camps on a cell after a cell selection or reselection process where factors like radio link quality, cell status and radio access technology are considered. The UE also monitors a paging channel to detect incoming calls and acquire system information. In this mode, control plane protocols include cell selection and reselection procedures.
Connected	The UE supplies the E-UTRAN with downlink channel quality and neighbor cell information to enable the E-UTRAN to select the most suitable cell for the UE. In this case, control plane

	protocol includes the Radio Link Control (RRC) protocol.

LTE Protocol Stack Layers

88. Draw the E-UTRAN Protocol Stack.

Diagram of E-UTRAN Protocol Stack



89. Mention the responsibility of Physical Layer (Layer 1).

- Physical Layer carries all information from the MAC transport channels over the air interface.
- Takes care of the link adaptation (AMC), power control, cell search (for initial synchronization and handover purposes) and other measurements (inside the LTE system and between systems) for the RRC layer.

90. Mention the responsibility of Medium Access Layer (MAC).

MAC layer is responsible for

- Mapping between logical channels and transport channels,
- Multiplexing of MAC SDUs from one or different logical channels onto transport blocks (TB) to be delivered to the physical layer on transport channels,
- Demultiplexing of MAC SDUs from one or different logical channels from transport blocks (TB) delivered from the physical layer on transport channels,

91. Mention the modes of Radio Link Control (RLC).

RLC operates in 3 modes of operation:

- Transparent Mode (TM)
- Unacknowledged Mode (UM)

- Acknowledged Mode (AM)

92. Mention the responsibility of RLC.

RLC is also responsible for

- re-segmentation of RLC data PDUs (Only for AM data transfer),
- reordering of RLC data PDUs (Only for UM and AM data transfer),
- duplicate detection (Only for UM and AM data transfer),
- RLC SDU discard (Only for UM and AM data transfer),
- RLC re-establishment, and
- Protocol error detection (Only for AM data transfer).

93. What are the services and functions of Radio Resource Control (RRC)?

The main services and functions of the RRC sublayer include

- broadcast of System Information related to the non-access stratum (NAS),
- broadcast of System Information related to the access stratum (AS),
- Paging, establishment, maintenance and release of an RRC connection between the UE and E-UTRAN.

94. Name the 3G radio access schemes identified to support different spectrum scenario. (April 2017)

- OFDM Orthogonal Frequency Division Multiplexing
- WCDMA Wavelength Code Division Multiple Access
- GSM Global System for Mobile communication
- GPRS General Packet Radio Services
- EDGE Enhanced Data rates for GSM Evolution
- EGPRS Enhanced GPRS

95. How is isolation between users in the downlink accomplished in a WCDMA? (Nov 2017)

In a WCDMA system, isolation between users in the downlink is accomplished through the combination of user-specific channelization codes and cell-specific scrambling codes.

96. What are the nonexclusive options hold by GSM operators for evolving their networks to 3G wideband multimedia operation?

GSM operators have two nonexclusive options for evolving their networks to 3G wideband multimedia operation:

(1) using GPRS and EDGE in the existing radio spectrum, and in small amounts of the new spectrum; or

(2) using WCDMA in the new 2 GHz bands, or in large amounts of the existing spectrum.

****