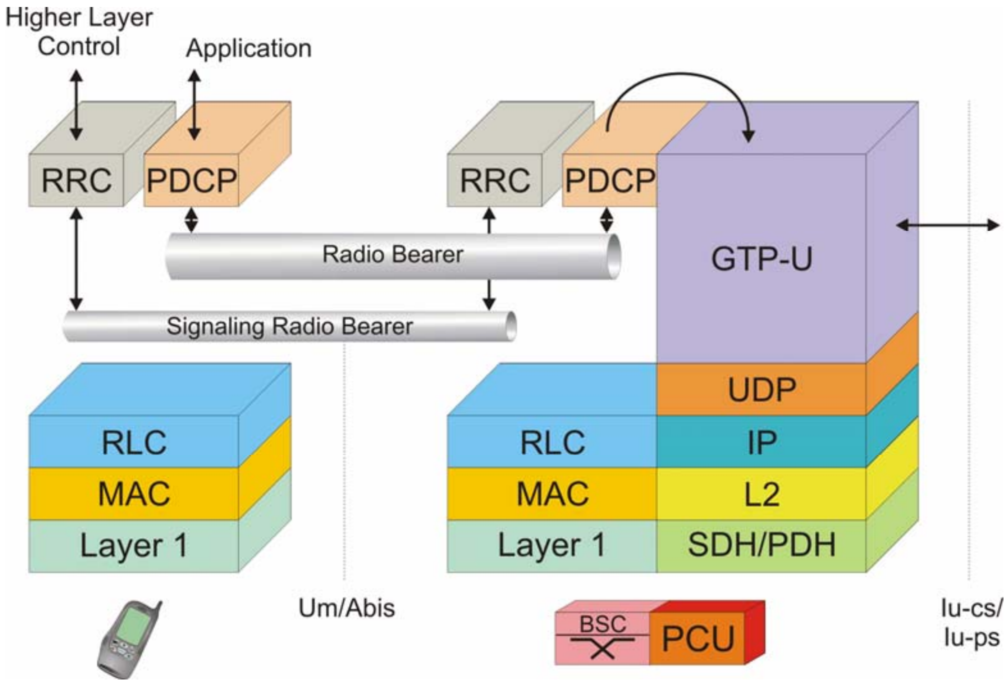
1

1.1 GERAN in A/Gb- or Iu-Mode



The objective of this section is to introduce the student into the principles of the Iu-mode of operation within GERAN [3GPP TS 43.051 (5.3)].

The key points of this section are:
1. If Iu-mode is used, then there are UMTS-like radio bearers and signaling radio bearers between the mobile station and the BSC/PCU.
2. RRC and PDCP represent the higher layers, just like in UMTS.
3. The BSC/PCU uses Iu-like signalling and protocols towards the SGSN and towards the MSC. This includes the use of GTP-U within the PCU.

1

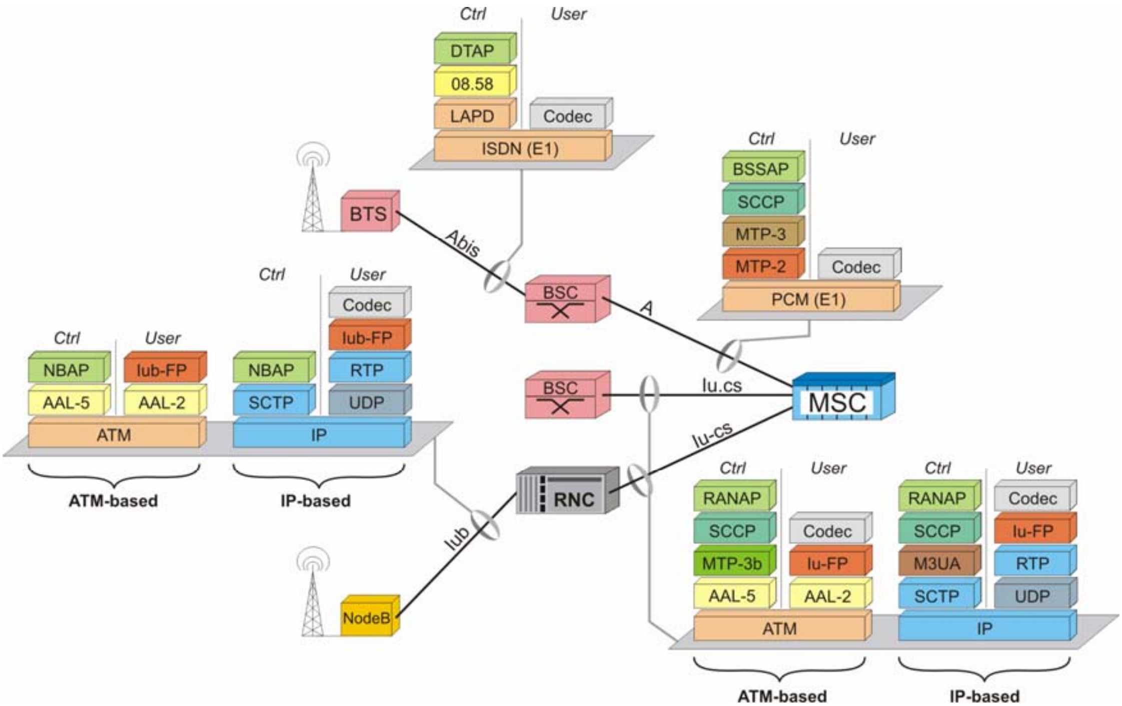
Room for your Notes

- **Abbreviations of this Section:**

GERAN	GSM EDGE Radio Access Network	**RRC**	Radio Resource Control (3GTS 25.331)
PDCP	Packet Data Convergence Protocol (3GTS 25.323)	**GTP-U**	GTP User Plane
RLC	Radio Link Control (UMTS 3GTS 25.322)	**MAC**	Medium Access Control ((E)GPRS 3GTS 04.60 / 3GTS 44.060)
UDP	User Datagram Protocol (RFC 768)	**IP**	Internet Protocol (RFC 791)
L2	Layer 2 (data link layer)	**SDH**	Synchronous Digital Hierarchy
PDH	Plesiochronous Digital Hierarchy	**BSC**	Base Station Controller
PCU	Packet Control Unit	**3GPP**	Third Generation Partnership Project (Collaboration between different standardization organizations (e.g. ARIB, ETSI) to define advanced mobile communications standards, responsible for UMTS)
TS	Timeslot	**UMTS**	Universal Mobile Telecommunication System
BSC	Base Station Controller	**PCU**	Packet Control Unit
SGSN	Serving GPRS Support Node	**MSC**	Mobile Services Switching Center

1

1.4 Iub- and Iu-cs-Interfaces IP-based



The objective of this section is to illustrate that the Iub- and the Iu-cs interfaces may with Rel. 5 alternatively be IP-based [3GTS 25.431, 3GTS 25.432, 3GTS 25.410, 3GTS 25.411] rather than mandatory ATM-based as with Rel. 99 and Rel. 4.

The key points of this section are:
1. The new feature is not mandating IP as transport plane instead of ATM, it is only giving the option of using IP.
2. The new feature is only applicable to Iub- and Iu-cs interface but not to A- or Abis-interface; those remain based on PCM. Still, because the Abis-interface is vendor-specific, it may well be IP-based.

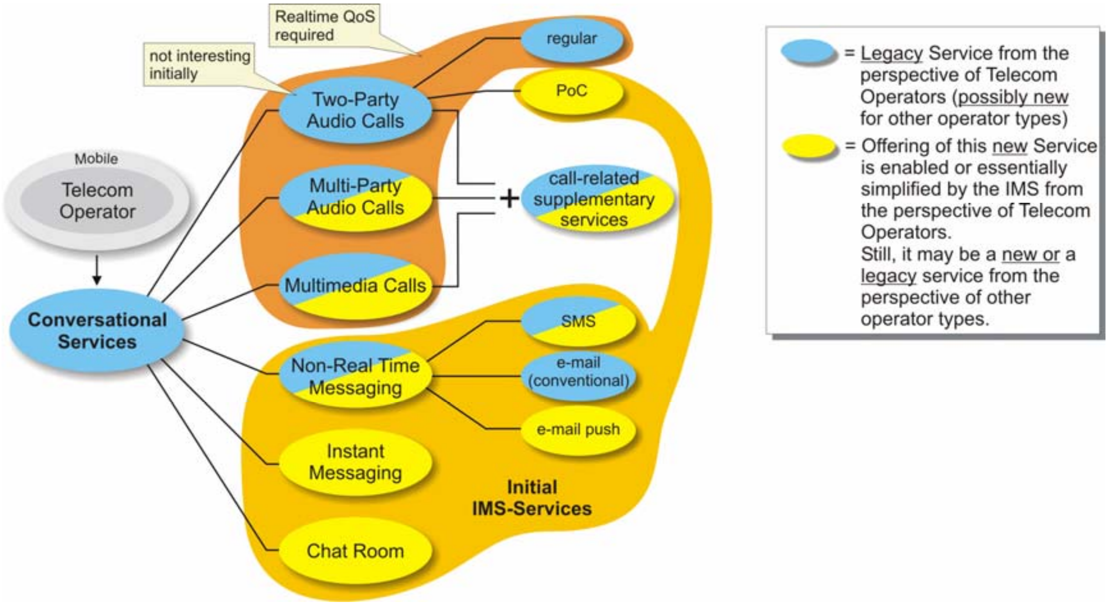
Room for your Notes

- **Abbreviations of this Section:**

3GTS	3rd Generation Test Specification	**RANAP**	Radio Access Network Application Part (3GTS 25.413)
IP	Internet Protocol (RFC 791)	**DTAP**	Direct Transfer Application Part
LAPD	Link Access Protocol for the ISDN D-Channel	**ISDN**	Integrated Services Digital Network
BTS	Base Transceiver Station	**BSC**	Base Station Controller
SCCP	Signaling Connection Control Part (ITU-T Q.711 – Q.714)	**MTP**	Message Transfer Part (ITU-T Q.701 – Q.709)
PCM	Pulse Code Modulation	**NBAP**	NodeB Application Part (3GTS 25.433)
FP	Frame Protocol	**AAL-5**	ATM-Adaptation Layer 5 (non-real time) (ITU-T I.363.5)
AAL-2	ATM Adaptation Layer 2 (for real-time services) (ITU-T I.363.2)	**ATM**	Asynchronous Transfer Mode (ITU-T I.361)
RTP	Real-time Transport Protocol (RFC 3550, RFC 3551)	**SCTP**	Stream Control Transmission Protocol (RFC 2960)
UDP	User Datagram Protocol (RFC 768)	**MSC**	Mobile Services Switching Center
RNC	Radio Network Controller		
M3UA	MTP-3 User Adaptation Layer (RFC 3332 / 3GPP 29.202 (Annex A))		

2

1.2.2 Conversational Services



The objective of this section is to depict the various different conversational services that may be offered through the IMS.

Key points of this section are:
1. The distinction between legacy conversational services (blue) and new conversational services (yellow) from the perspective of telecom operators.
2. The distinction between conversational services that do require real-time QoS and those that do not.

Conversational services are the domain of telecom operators. Please note that the telecom operator may be a regular one or a mobile network operator.

- **Two-Party Audio Calls**
  As illustrated, this service type also contains PoC, because PoC is no longer a proprietary service when offered through the IMS.
  Note that (mobile) telecom offer close to perfect two-party audio call services without the IMS. It needs to be emphasized that for them the focus of the IMS therefore should not be on the provision of this kind of services, esp. initially. At a later stage, audio calls etc. may be migrated to the IMS to use only one service delivery platform.

- **Multiparty Audio Calls**
  The bullet is colored partly yellow because the conduction of multiparty calls becomes much more common, inherent and easy to use with the IMS.

- **Call-Related Supplementary Services**
  Any IMS-solution has to continue offering the legacy call-related supplementary services like caller representation, call on hold or call forwarding. However, the IMS will add new call-related supplementary services like “black lists” for callers or simultaneous forking.

- **Multimedia Calls**
  Through the IMS, the setup and selection of video calls will be simplified (although video calls have been around for quite some time). In addition, the IMS offers the combination of more media types than just audio + video. For instance, a service offering may combine audio + whiteboard + instant messaging to provide for advanced audio conferencing. Yet another example for multimedia calls is a “see what I see” service.

- **Non-Real Time Messaging**
  This bullet is colored partly yellow because some form of non-real time messaging has been there also prior to the IMS. However, SMS is (usually) a new service type for wireline telecom operators and definitely the famous e-mail push service is new.

- **Instant Messaging**
  Instant messaging has become an important means to communicate but it is a new type of service for telecom operators (both fixed and mobile).

- **Chat Rooms**
  The same applies what was said for instant messaging.

Please note the remarks on the right hand side of the graphics page. The color for new and legacy services only applies for telecom operators but not necessarily for other operator types, offering triple play services. One example is instant messaging which is a new service for telecom operators but which definitely is a legacy service from the perspective of ISP’s.

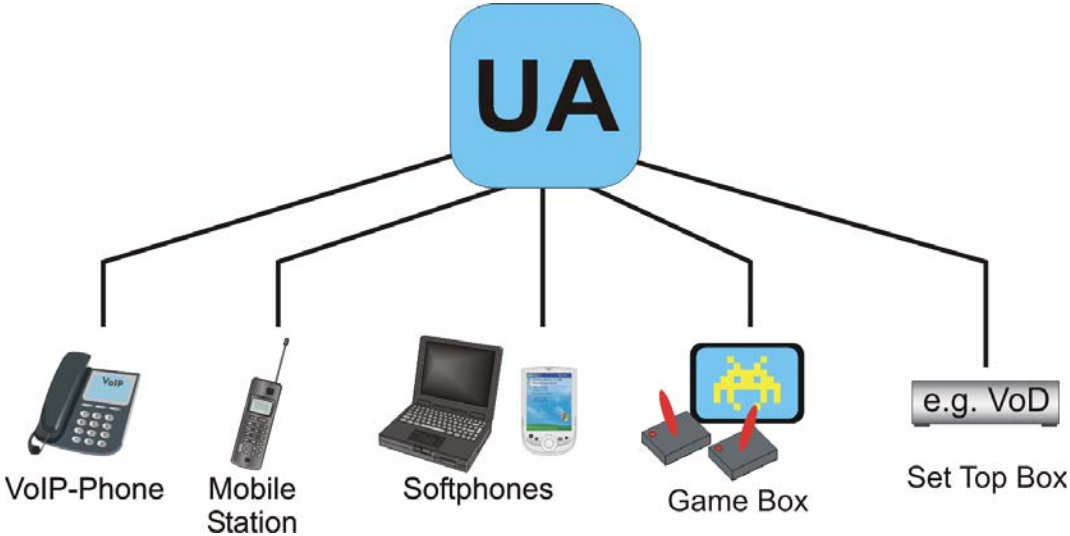
- **Abbreviations of this Section:**

QoS	Quality of Service	**PoC**	Push to talk over Cellular (3GTR 29.979 and various OMA-specifications)
SMS	Short Message Service (3GTS 24.011, 3GTS 23.040)	**IMS**	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)
ISP	Internet Service Provider		

2

1.4 The Perspective of the IMS User Agent

1.4.1 Typical User Agents of the IMS



The objective of this section is to surprise the student with the variety of possible SIP-user agents.

Key point of this section is to understand that SIP is only a session control protocol that remains independent from the actual session. This explains the variety of user device types.

- **Dedicated VoIP-Phones**
  With VoIP becoming more and more commonly used by corporations and residential customers, dedicated VoIP-phones are also becoming a typical SIP-user device. Although below the surface these dedicated VoIP-phones are nothing more but regular computers with a simple operating system and a SIP-softphone, we considered them as important enough to be listed separately.

- **Mobile Stations**
  Mobile stations with an integrated SIP-client will be the typical user devices of tomorrow's 3GPP-networks. This is obvious, since 3GPP bases its entire IMS session control on SIP. We list the dedicated mobile station separate.

- **Softphones**
  The best known and most widespread SIP user agent is certainly the softphone. These softphones are nowadays available for literally every operating system and every platform. Probably the best about them is that they usually come free-of-charge and that they can be downloaded from the internet.

In the figure we illustrate a PDA and a desktop PC as bearers for softphones. Note that the PDA with softphone is still a different type of user agent than the dedicated mobile station since the PDA will tendentiously allow much more software configuration and updating than the mobile station. That is, the mobile station and the dedicated VoIP-phone are rather telephones or communication devices while the PDA still represents a generic computer with add-on SIP capability.
In the long run, softphones will mutate to become generic devices supporting any potential SIP and IMS-controlled application.

- **Game Boxes**
  The flexibility and range of SIP user agents becomes obvious when comparing the previous devices with the game box which allows remote users to play games against each other or against application servers.

- **Set Top Boxes**
  Another type of SIP user agent is a set top box. Set top boxes are no telephones but they represent the other end of SIP user agents, dedicated for VoD or audio on demand.

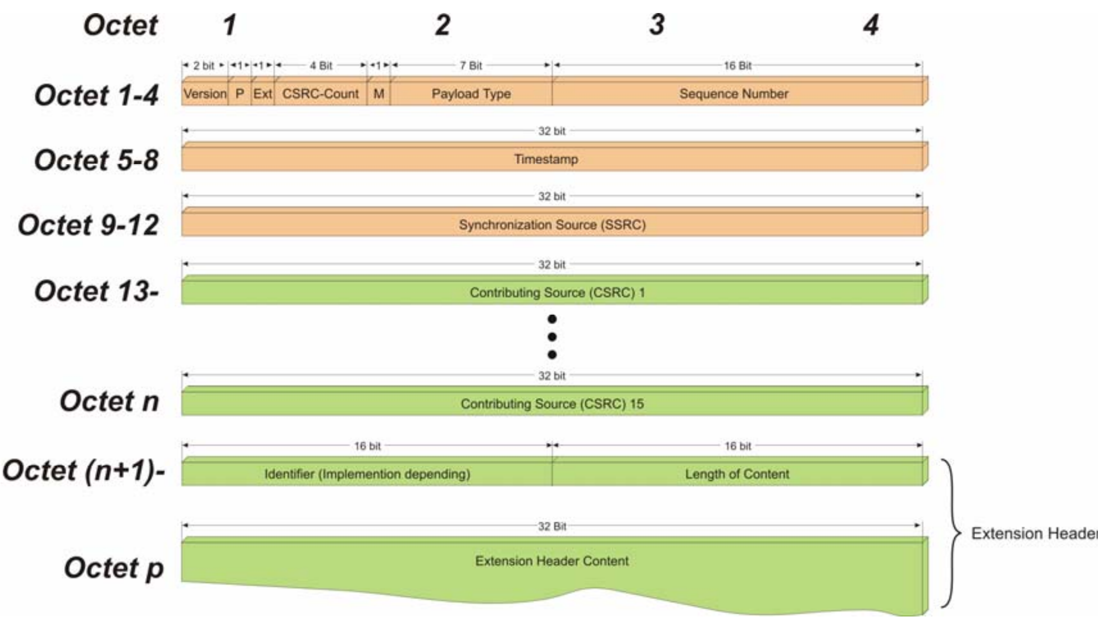
  Note that the support of both, UDP and TCP as transport layer protocols has been mandated for UA's with RFC 3261 (18).

- **Abbreviations of this Section:**

IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**UA**	User Agent (SIP-Term / RFC 3261)
VoIP	Voice over IP	**VoD**	Video on Demand
SIP	Session Initiation Protocol (RFC 3261)	**3GPP**	Third Generation Partnership Project (Collaboration between different standardization organizations (e.g. ARIB, ETSI) to define advanced mobile communications standards, responsible for UMTS)
PDA	Personal Digital Assistant	**PC**	Personal Computer
UDP	User Datagram Protocol (RFC 768)	**TCP**	Transmission Control Protocol
RFC	Request for Comments (Internet Standards)		

1.5.3 Real-time Transport Protocol (RTP)

1.5.3.1 Format of the RTP-Header



The objective of this section is to illustrate the format of the RTP-header [RFC 3550].

Key point of this section is the fact that RTP-headers are usually 12 octets long because all the optional fields are typically not used.

Note that the major asset of using RTP/UDP instead of plain UDP is to allow the receiver to determine the jitter of the transmission line between sender and receiver.

- **Version**
  This 2 bit long field identifies the version of RTP. The current version is ‘2’. The value ‘1’ is used by the first draft version of RTP and the value’ 0’ is used by the protocol initially implemented in the VAT-audio tool.

- **P-Bit (Padding)**
  If the padding bit is set, the RTP-packet contains one or more additional padding octets at the end which are not part of the payload. The last octet of the padding actually identifies the number of padding octets (incl. this last octet). Padding may be needed by some encryption algorithms (e.g. IPsec) with fixed block sizes or for carrying several equally sized RTP packets in a lower-layer protocol data unit.

- **Ext-Bit (Header Extension)**
  This bit identifies whether the regular RTP-header is followed by a payload specific extension header.

- **CSRC-Count**
  This 4 bit long field identifies whether and how many CSRC's are included in the header. Between 0 and 15 CSRC's are possible.

- **M-Bit (Marker)**
  The M-bit may be used by an application to indicate certain events to the receiver like the end of a certain period or frame.

- **Payload Type**
  The payload type indicates the codec type. Some examples are illustrated in the following section. The end-to-end payload type values between users have to be negotiated through the SDP (Session Description Protocol). The respective SDP-elements are nested into SIP-messages.

- **Sequence Number**
  The 16 bit long sequence number increments by one for each RTP data packet sent and may be used by the receiver to detect packet loss and to restore packet sequence. The initial value of the sequence number is random (unpredictable) to make attacks on encryption more difficult.

- **Timestamp**
  The 32 bit long Timestamp represents the time of sampling of the first octet in the payload of the RTP-frame. The initial value of the Timestamp is random and shall consecutively be incremented to allow jitter calculation at the receiver side. The resolution of the underlying clock should be bigger or equal to the used sampling period. Example: GSM Fullrate works with a sampling rate of 13 kbit/s, hence the used clock to determine the Timestamp value should be app. 13 kHz.

  (To be continued)

- **Abbreviations of this Section:**

RTP	Real-time Transport Protocol (RFC 3550, RFC 3551)	**RFC**	Request for Comments (Internet Standards)
GSM	Global System for Mobile Communication	**CSRC**	Contributing Source
SDP	Session Description Protocol (RFC 2327, RFC 3266, RFC 3264)		

(Continued)

- **Synchronization Source (SSRC)**
  The 32 bit long Synchronization Source identifies the source of the information which is included in this RTP-frame. The SSRC is assigned by the sender and represents a random number. Examples for synchronization sources are a camera or a microphone.

- **Contributing Source (CSRC)**
  Optionally, the RTP-header may include up to 15 CSRC's of which each is 32 bit long. CSRC's are necessary, if a mixer is deployed that multiplexes streams from different sources of the same type together. Example: A mixer is used to merge the audio data streams during a telephone conference that stem from the same network before the only one RTP-stream is transmitted to destinations outside the network.
  In such a case, each CSRC represents the original SSRC which contributed to this data stream. The SSRC-field in such a frame will be that of the mixer.

- **Extension Header**
  The optional extension header is for future use.

[RFC 3550]

Room for your Notes

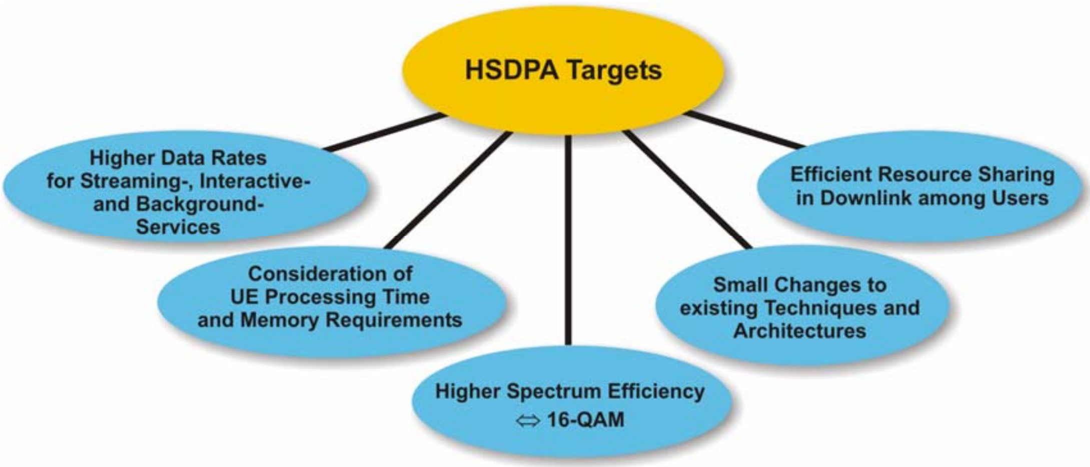
- **Abbreviations of this Section:**

RTP	Real-time Transport Protocol (RFC 3550, RFC 3551)	**RFC**	Request for Comments (Internet Standards)

2

4. HSDPA

4.1 Targets



Higher Data Rates for Streaming-, Interactive- and Background Services
HSDPA is a feature based on a downlink shared channel that allows user net-data rates of up to 10 Mbit/s. It is designed to support services that require instantaneous high rates in the downlink and lower rates on the uplink. This feature also decreases the level of retransmissions (at the radio link and hence higher layers), in turn allowing the reduction of delivery time. Examples of end-user services targeted by HSDPA are internet browsing and video on demand.

Consideration of UE Processing Time and Memory Requirements
HSDPA takes UE limitations like available physical memory for transmission and especially for combining with retransmission into account. Also the physical channel processing capability is considered. (Examples: Minimum inter-TTI interval, maximum number of transport channel bits per TTI)
The terminals can be grouped in categories from 1 to 12. The UE's can firstly be distinguished by the amount of physical channels they support, further distinction is possible by the maximum number of TB size and total number of soft channel bits available for soft combining.

Higher Spectrum Efficiency
With 16-QAM applied in downlink, throughput rates can be doubled compared to QPSK which is used for Rel. '99 and Rel. 4 physical channels. The amount of bits/Hz is increased with 16-QAM as one modulation symbol corresponds to 4 bits whereas in QPSK one modulation symbol represents 2 bits. Even when HSDPA uses QPSK modulation the spectrum efficiency increases as HSDPA exploits good downlink C/I conditions. This is achieved by reducing the amount of FEC (increasing the code rate) and thus having more capacity for the application data.

Small Changes to existing Techniques and Architectures
HSDPA minimizes the necessary upgrades and changes in UTRAN and UE. Nevertheless some protocol additions are necessary in NodeB and UE as well some enhancements of existing procedures and protocols. They are mentioned in the following pages and are explained in full detail in chapter 4.

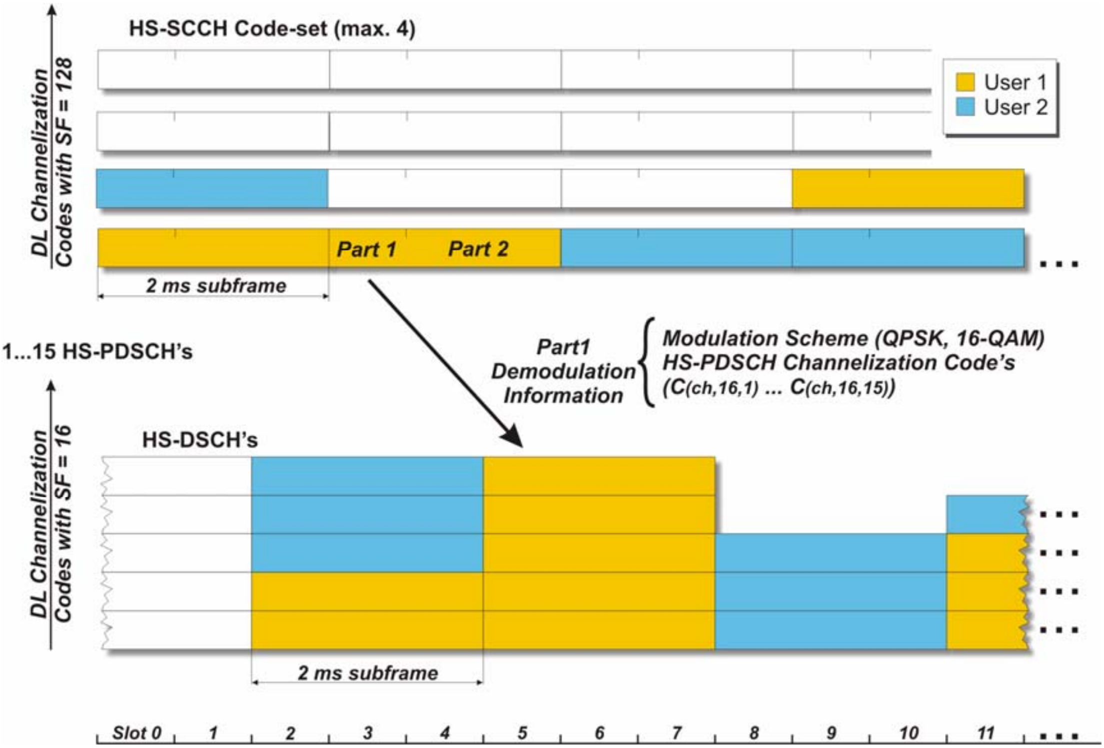
Efficient Resource Sharing in Downlink among Users
HSDPA introduces a new transport channel type that makes efficient use of valuable radio frequency resources. Beside this, it takes into account the bursty nature of packet switched data by sharing the channelization codes, transmission power and infrastructure hardware among users.
Statistical multiplex gain is obtained as HSDPA shares the physical resources in a time and/or code multiplex manner among the users. If a user requires a high peak throughput, all available physical resources can be allocated for a short time.

- **Abbreviations of this Section:**

HSDPA	High Speed Downlink Packet Access (3GTS 25.301, 25.308, 25.401, 3GTR 25.848)	**UE**	User Equipment
QAM	Quadrature Amplitude Modulation	**TTI**	Transmission Time Interval
TB	Transport Block	**QPSK**	Quadrature Phase Shift Keying (3GTS 25.213)
FEC	Forward Error Correction	**UTRAN**	UMTS Terrestrial Radio Access Network

2

4.5 Fast Resource Scheduling in HSDPA



The objective of this section is to illustrate how the NodeB tags the UE wto receiving data on HS-PDSCH using the scheduling channel HS-SCCH.

Key point of this section is that the UE in HSDPA-mode has to continuously monitor the allocated HS-SCCH's to detect allocations to itself. Such an allocation is identified by the UE's H-RNTI and contains the channelization codes and the used modulation scheme.

HS-SCCH-set Decoding
The graphic demonstrates that both UE's have to decode their assigned HS-SCCH-set first, before they can attempt to decode the HS-PDSCH's. For simplicity reasons, both UE's have the same HS-SCCH-set assigned. A HS-SCCH-set consists of up to a maximum of four HS-SCCH channelization out of a possible range from codes C(ch,128,1) … C(ch,128,127) under e.g. the primary scrambling code. As depicted, only one of the four HS-SCCH's contains valid information per UE per TTI. This is indicated by the appropriate color coding for each UE. All the information necessary for demodulating the related HS-DSCH subframe which follows always 2 slots later after HS-SCCH, is transmitted to the UE's within part 1. It can be seen that every HS-SCCH is (logically) divided into two parts.

The second part contains the necessary information on how to decode the HS-DSCH. So part 1 and part 2 serve different purposes. Part 1 allows the demodulation of the HS-PDSCH subframe and part 2 is responsible for layer 2 decoding of the HS-DSCH.

The HS-SCCH is intended for the very UE once it recognizes its UE-id inside part 1 of the HS-SCCH subframe. If the UE detected consistent control information intended for it in the immediately preceding subframe, it is sufficient to only monitor the same HS-SCCH used in the immediate succeeding subframe. In the graph this is indicated by e.g. user 1 in slot 0 to slot 6 where user 1 gets two consecutive valid HS-SCCH's. Therefore UE 1 only needs to decode the same HS-SCCH from slot 3 onwards. From slot 8 onwards the complete HS-SCCH code-set has to be monitored again by UE 1 (only part 1).

HS-DSCH Demodulation
If a UE detects that one of the monitored HS-SCCH's contains its encoded UE-id (implicitly included) and consistent control information intended for this UE, the UE prepares to receive the HS-PDSCH's. Consistent control information hereby means that modulation scheme and HS-PDSCH channelization code-set info are valid according to the UE's capability. The UE has about one slot duration time after receiving part 1 to prepare for HS-PDSCH's reception. As already mentioned, the UE indicates via the category parameter if it supports up to 5, 10 or 15 HS-PDSCH channelization codes in parallel. The color coding used in the figure for the HS-SCCH and their related HS-DSCH shows that HSDPA allows for time multiplexing and code multiplexing of the HS-PDSCH's. Time multiplexing means that user 1 and user 2 get the HS-PDSCH's assigned one after the other in different subframes. Code multiplexing or multicode operation means that several user, here user 1 and user 2, use different HS-PDSCH's within the same subframe. The various HS-PDSCH's are separated by different channelization codes.

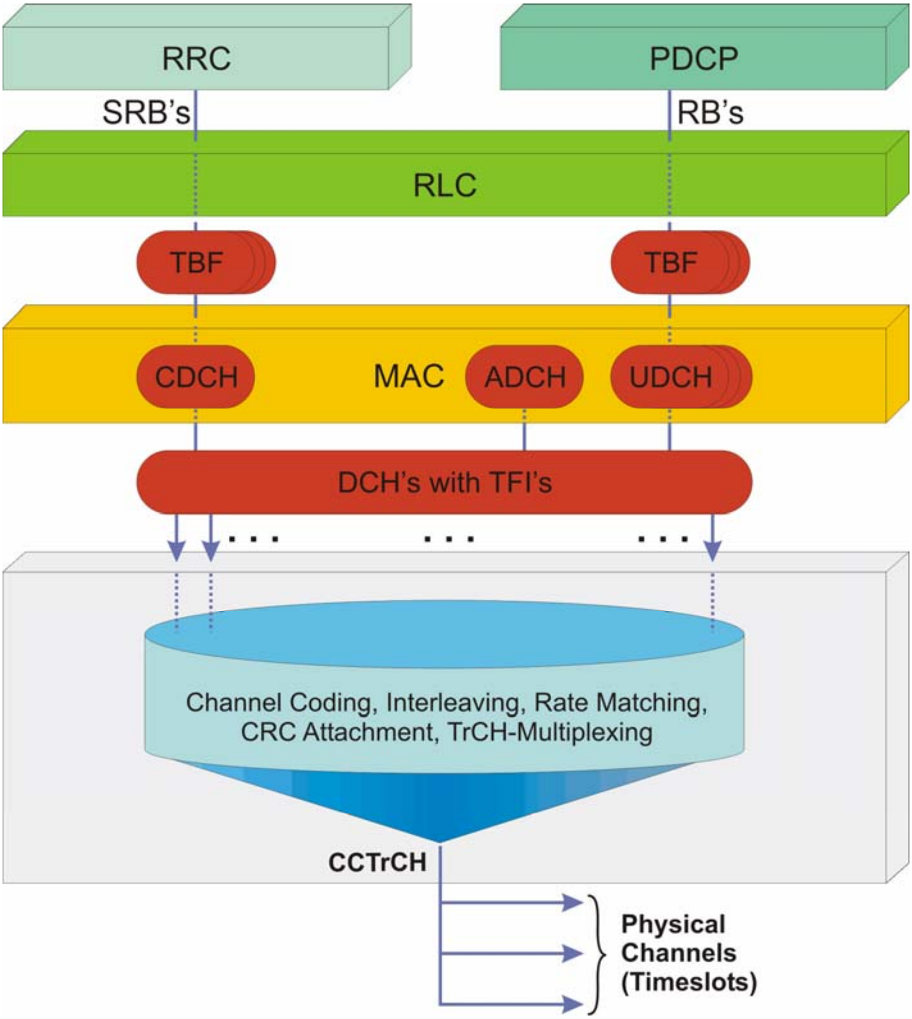
[3GTS 25.212 (4.6.2), 3GTS 25.213 (5.2.1)]

- **Abbreviations of this Section:**

HSDPA	High Speed Downlink Packet Access (3GTS 25.301, 25.308, 25.401, 3GTR 25.848)	**DL**	Downlink
SF	Spreading Factor	**HS-SCCH**	High Speed Shared Control Channel (3GTS 25.211, 25.214)
HS-PDSCH	High Speed Physical Downlink Shared Channel (3GTS 25.211)	**HS-DSCH**	High Speed Downlink Shared Transport Channel (3GTS 25.211, 25.212, 25.308)
QPSK	Quadrature Phase Shift Keying (3GTS 25.213)	**UE**	User Equipment
H-RNTI	HS-DSCH Radio Network Transaction Identifier (3GTS 25.331, 25.433)	**TTI**	Transmission Time Interval
3GTS	3rd Generation Test Specification		

3

3.3 Flexible Layer One (FLO)



The objective of this section is to illustrate how a GERAN-base station or mobile station operating in Iu-mode is interconnected to a physical layer which applies FLO.

Key points of this section are that:
1. FLO takes over the physical layer processing rules and definitions from UTRA like transport blocks and transport formats.
2. FLO is driven by the IMS with its high demand on the performance off packet-switched radio bearers.
3. FLO is only used on dedicated channels that use 26-/52-Multiframe structure, not on 51-multiframe.

Note that FLO shall operate in both Iu-mode and A-/Gb-mode, but right now is only defined for Iu-mode as stage 2 description.

[3GTS 45.902]

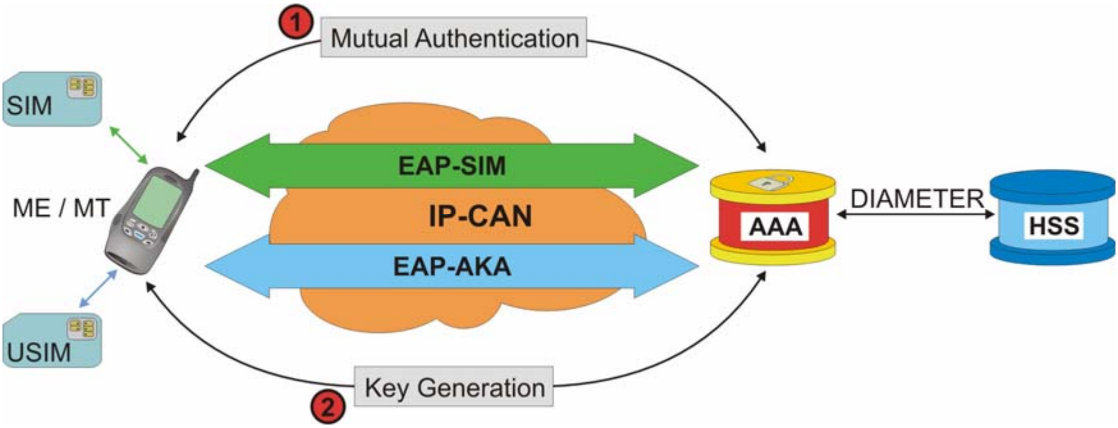
Room for your Notes

- **Abbreviations of this Section:**

FLO	Flexible Layer 1 (3GTS 45.902)	**RRC**	Radio Resource Control (3GTS 25.331)
PDCP	Packet Data Convergence Protocol (3GTS 25.323)	**SRB**	Signaling Radio Bearer
RB	Receive Block Bitmap (EGPRS)	**RLC**	Radio Link Control ((E)GPRS / 3GTS 04.60 / 3GTS 44.060)
TBF	Temporary Block Flow	**CDCH**	Control-plane Dedicated Channel (3GTS 45.902)
MAC	Medium Access Control ((E)GPRS 3GTS 04.60 / 3GTS 44.060)	**ADCH**	Associated Dedicated Channel (3GTS 45.902)
UDCH	User-plane Dedicated Channel (3GTS 45.902)	**DCH**	Dedicated Channel (Transport)
TFI	Temporary Flow Identity ((E)GPRS)	**CRC**	Cycle Redunancy Check
TrCH	Transport Channel (UMTS)	**CCTrCH**	Coded Composite Transport Channel (UMTS)
GERAN	GSM EDGE Radio Access Network	**UTRA**	UMTS Terrestrial Radio Access

3

4.5 EAP-SIM and EAP-AKA



The objective of this section is to introduce the ideas of EAP-SIM and EAP-AKA based authentication and key derivation techniques.

The key point of this section is that EAP-SIM is tailored to operate with legacy GSM-SIM-cards while EAP-AKA has been designed to operate with USIM-cards. Still, although SIM-cards never provided for network to mobile station authentication, EAP-SIM does!

1 In a first step, EAP-SIM and EAP-AKA provide for mutual authentication between a mobile device and an AAA-server through some IP-CAN (e.g. WLAN-home network).

2 In a second step and as consequence of the authentication procedure, but still as part of EAP-SIM and EAP-AKA, keying material is derived by both parties which can be used for message integrity protection and payload encryption for the upcoming data transfers.

- **Abbreviations of this Section:**

EAP-SIM	Extensible Authentication Protocol method for gsm Subscriber Identity Module (RFC 4186)	**EAP-AKA**	Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement (RFC 4187)
SIM	Subscriber Identity Module	**ME**	Mobile Equipment (ME + SIM = MS)
MT	Mobile Terminal or Mobile Terminating	**USIM**	Universal Subscriber Identity Module (3GTS 31.102)
IP-CAN	Internet Protocol - Connectivity Access Network (e.g. DSL, TV-Cable, WIMAX, UMTS)	**HSS**	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5
AAA	Authentication, Authorization and Accounting	**GSM**	Global System for Mobile Communication
WLAN	Wireless Local Area Network (IEEE 802.11)		

Chapter 4:

Detailed Consideration of Selected Release 6 Enhancements and Features

Objectives

After this lesson the student is able to…

- **Describe how Multimedia Broadcast Multicast Messaging Service (MBMS) operates** 3GTS 23.846

- **Describe the concepts and processes of High Speed Uplink Packet Access (HSUPA)** 3GTS 25.309 3GTR 25.896
  We like to provide information about the operational principles of HSUPA which means that we won't go into full detail. Note that 3GPP terms this feature "FDD Enhanced Uplink" rather than HSUPA.

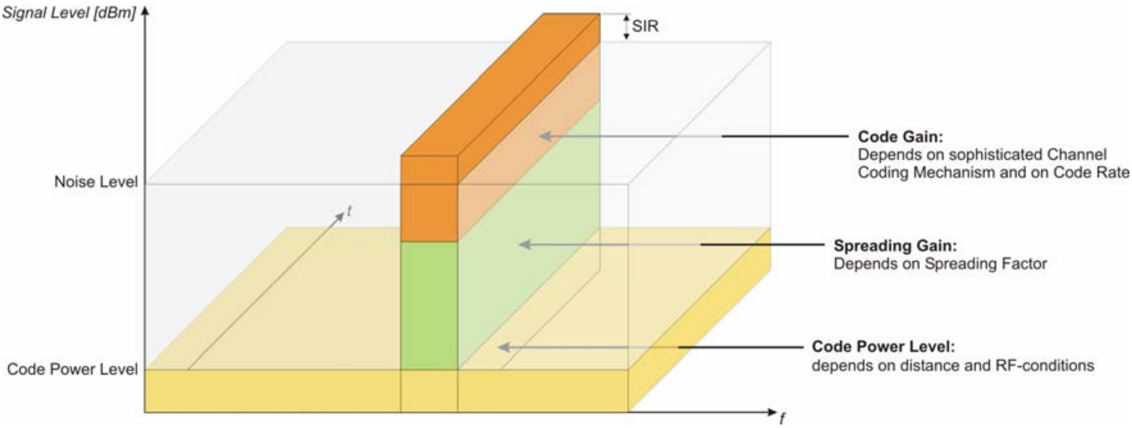
- **Describe how non-3GPP radio access technologies (RAT) like WLAN or WIMAX can be integrated into the 3GPP network environment using UMA-like procedures or alternatives** 3GTS 22.234 3GTS 23.234 3GTS 24.234 3GTS 33.234
  With Release 6, WLAN, Bluetooth or WIMAX represent alternative RAT's with entry on the (U)SIM-card that may be used instead of GERAN or UTRAN.

4

4

2.4 Operation of HSUPA

2.4.1 Review: SIR Considerations in a CDMA-system



The objective of this section is to illustrate how any CDMA-system achieves a given SIR.

Key points of this section are that:
1. A CDMA-system can usually transmit at a very low output power level because of the inherent spreading gain. Tendency: The higher the spreading factor the lower the output power can be.
2. Of course, this rule works both ways: In HSUPA with a spreading factor of only 2, almost no more spreading gain is left which ultimately requires an increase of the output power level on the UE-side.
3. Ultimately, this increases the noise level for all other users which means that simultaneous operation of multiple HSUPA-users with full throughput rate is not possible.

- **More Information**
  - ⇒ One of the most critical issues in every CDMA-system is power control, because each user is an interferer for each other user. The power control mechanism needs to be fast enough to cope with the rapidly changing RF-conditions and it needs to provide for the absolute minimum output power that provides for the ordered SIR (Signal to Interference Ratio).
  - ⇒ As the figure illustrates, the signal level of one user does not only depend on the RSCP (Received Signal Code Power). CDMA allows to hide a signal underneath the noise level, because it is particularly the spreading gain and the channel coding gain which allows to recover a user data signal from the spread signal.

⇒ At any given time, the overall signal level depends on the code power (□ transmit power), on the spreading gain and on the channel coding gain. In UTRA, the spreading gain varies between 6 dB and 27 dB. The channel coding gain is app. 6 dB (1/2-rate convolutional coding) – 9.5 dB (1/3-rate turbo coding).

- **The Consequences are:**

⇒ The required output power can be reduced by the same amount of dB which is added to the overall signal level through the channel coding gain and the spreading gain.

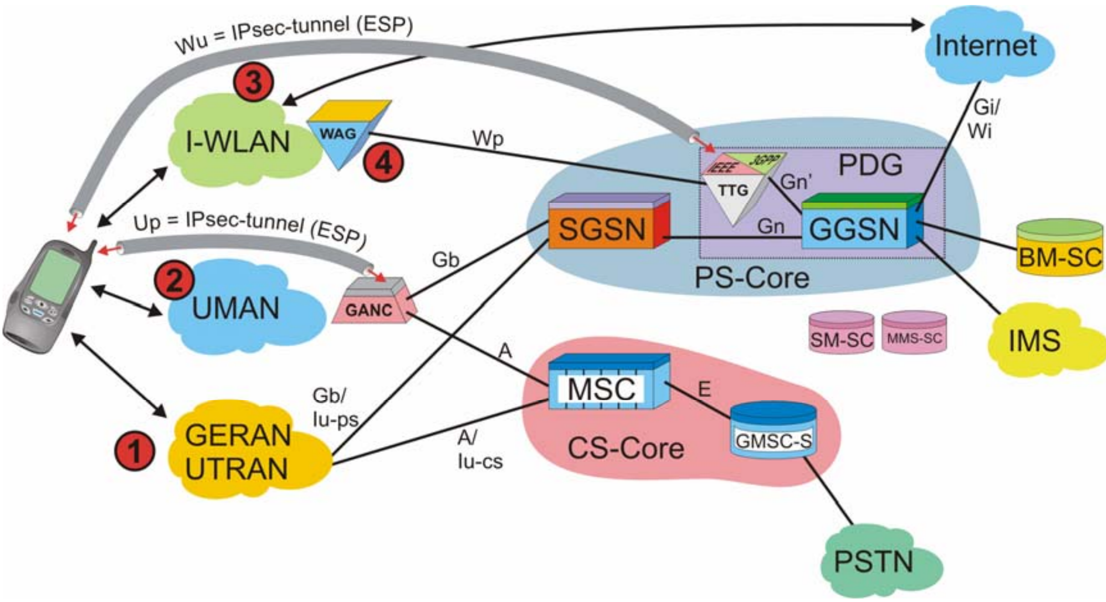
⇒ Vice versa, if high throughput rates and therefore low spreading factors (□ small spreading gain) are requested, the necessary output power needs to be increased accordingly.

- **Abbreviations of this Section:**

HSUPA	High Speed Uplink Packet Access (3GTS 25.301, 25.309, 25.401, 3GTR 25.896)	**SIR**	Signal to Interference Ratio
CDMA	Code Division Multiple Access	**dBm**	The unit dBm measures a power. The conversion of a power value from Watt [W] to dBm is done in the following way: X [dBm] = 10 x log10(X [W] / 0.001 [W])
UE	User Equipment	**RF**	Radio Frequency
RSCP	Received Signal Code Power (3GTS 25.215)	**UTRA**	UMTS (Universal Mobile Telecommunication System)Terrestrial Radio Access

4

3.1 Interconnection Options for Alternative RAT's



The objective of this section is to illustrate the different routes through which the mobile station can gain access to PLMN-based services and to the internet.

The key points of this section are that:
1. 3GPP uses IPsec-tunnels between mobile station and GANC or TTG to ensure a safe communication.
2. Through GAN/UMA, the mobile station may gain access to both, circuit-switched and packet-switched PLMN-services.
3. In case of I-WLAN, it is the choice of the mobile subscriber to access the internet directly or through the PLMN.

1

- **Access through GERAN/UTRAN**
  Through GERAN/UTRAN the mobile station gets access to all circuit-switched and packet-switched services that the PLMN offers, namely to the PSTN, to the internet (incl. IP-address allocation), to MBMS (□ BM-SC), SMS and MMS and to the IMS.

2

- **Access through GAN/UMAN**
  GAN/UMAN offers the same access service to the mobile station. The GANC interconnects to both, the circuit-switched and the packet-switched core network domain and therefore to all services that these offer.

- **I-WLAN Direct IP-Access**
  In this case, the mobile station only uses the PLMN for access authentication and authorization. The access to internet based services is done directly without involvement of the PLMN. However, the mobile station can access PLMN-based packet-switched services like MBMS or SMS only through GERAN/UTRAN.

3

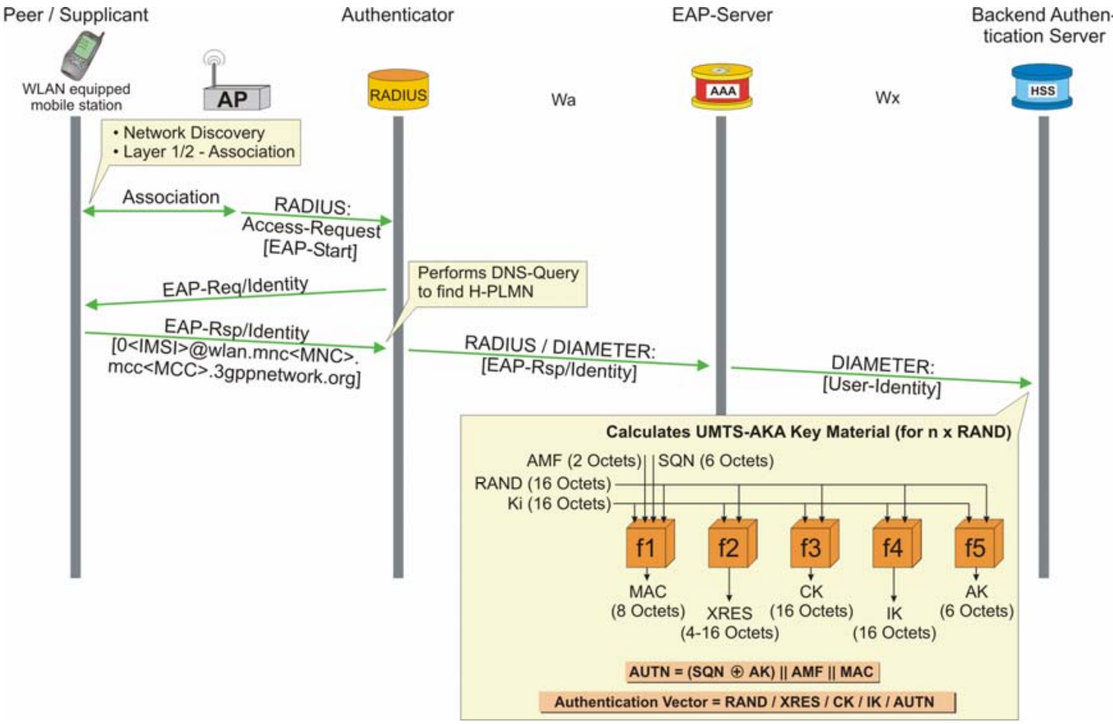
- **I-WLAN 3GPP IP-Access**
  In this case, the mobile station and the packet-switched core network domain establish an IPsec-tunnel between themselves and the mobile station gets access to all PLMN-based packet-switched services, namely IMS, MBMS, MMS and SMS. It is a configuration issue whether direct internet traffic is routed through the PLMN or is handled as in case of "I-WLAN Direct IP-Access".

4

- **Abbreviations of this Section:**

3GPP	Third Generation Partnership Project (Collaboration between different standardization organizations (e.g. ARIB, ETSI) to define advanced mobile communications standards, responsible for UMTS)	**UMA**	Unlicensed Mobile Access (3GTS 43.318)
ESP	Encapsulating Security Payload (RFC 4303)	**SGSN**	Serving GPRS Support Node
GANC	Generic Access Network Controller (3GTS 43.318)	**WLAN**	Wireless Local Area Network
GERAN	GSM EDGE Radio Access Network	**PDG**	Packet Data Gateway
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**PSTN**	Public Switched Telephone Network
IPsec	Internet Protocol / secure (RFC 2401)	**PS**	Puncturing Scheme
MBMS	Multimedia Broadcast / Multicast Service (3GTS 23.246, 3GTS 43.846)	**SMS**	Short Message Service (3GTS 24.011, 3GTS 23.040)
MMS	Multimedia Messaging Service (3GTS 22.140, 3GTS 23.140]	**IMS**	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)
MMS-SC	Multimedia Message Service Center	**BM-SC**	Broadcast Multicast Service Center
PLMN	Public Land Mobile Network		
RAT	Radio Access Technology (e.g. GERAN, UTRAN, ...)	**CS**	Coding Scheme
SM-SC	Short Message Service Center		
UMAN	Unlicensed Mobile Access Network	**GGSN**	Gateway GPRS Support Node
UTRAN	UMTS Terrestrial Radio Access Network	**GMSC-S**	Gateway MSC Server
WAG	WLAN Access Gateway	**TTG**	Tunnel Termination Gateway

3.2.2 The EAP-AKA Procedure



The objective of this section is to illustrate how EAP-AKA-based mutual authentication and key generation [RFC 4187] are performed between a mobile station with USIM-card and a 3GPP-AAA server that is termed EAP-server.

The key points of this section are:
1. The mobile station selects EAP-AKA authentication by prefixing a ‘0’ in front of its user identity (□ “0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org).
2. The 3GPP-AAA-server obviously requires the HSS for calculating the UMTS-AKA-specific quintuplet RAND, XRES, CK, IK and AUTN.

- **Initial Conditions**
  - ⇒ The mobile station contains a WLAN-enabled client and a USIM-card (no SIM).
  - ⇒ The mobile station has just selected the illustrated WLAN as access network. Simultaneous association with e.g. GERAN/UTRAN is possible.
  - ⇒ The selected WLAN access point and its backbone network (the AAA-server) support EAP-based authentication.

4

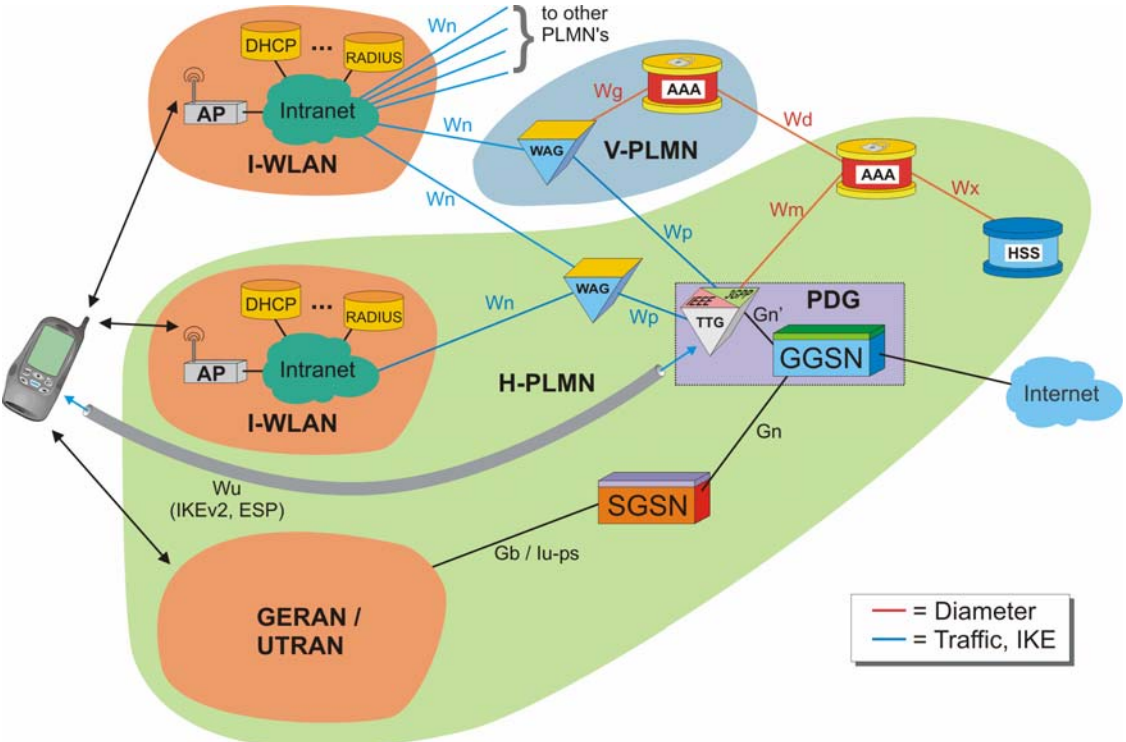
- **Applicability of this Procedure**
  The presented EAP-AKA-procedure applies in different cases; independent from other procedures or as part of IKEv2. The presented procedure is related to "I-WLAN Direct IP-Access".
  However, in those other cases the mobile station would indicate another user identity, indicating its desire to access a GANC or a PDG. In the presented case, the RAT is based on WLAN (IEEE 802.11) but the procedure works almost unchanged for WIMAX (IEEE 802.16).

EAP-AKA	Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement (RFC 4187)	**WLAN**	Wireless Local Area Network (IEEE 802.11)
AP	Access Point (IEEE 802.11, 802.16)	**RADIUS**	Remote Authentication Dial In User Service (RFC 2865)
EAP	Extensible Authentication Protocol (RFC 3748)	**AAA**	Authentication, Authorization and Accounting
HSS	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5	**DNS**	Domain Name System
H-PLMN	Home PLMN	**UMTS**	Universal Mobile Telecommunication System
AKA	Authentication and key agreement (3GTS 33.102)	**RAND**	Random Number
AMF	Authentication management field (3GTS 33.102)	**SQN**	Sequence number (used in UMTS-security architecture / 3GTS 33.102)
Ki	Subscriber Key	**MAC**	Medium Access Control ((E)GPRS 3GTS 04.60 / 3GTS 44.060)
CK	Ciphering Key (3GTS 33.102)	**AK**	Authentication Key (IEEE 802.16)
AUTN	Authentication Token (3GTS 33.102)	**XRES**	Expected Response (3GTS 33.102)
IK	Integrity Key (3GTS 33.102)	**RFC**	Request for Comments (Internet Standards)
USIM	Universal Subscriber Identity Module (3GTS 31.102)	**GERAN**	GSM EDGE Radio Access Network
UTRAN	UMTS Terrestrial Radio Access Network	**IKEv2**	Internet Key Exchange protocol / version 2 (RFC 4306)
GANC	Generic Access Network Controller (3GTS 43.318)	**PDG**	Packet Data Gateway
RAT	Radio Access Technology (e.g. GERAN, UTRAN, ...)	**IEEE**	Institute of Electrical and Electronics Engineers
WIMAX	Worldwide Interoperability for Microwave Access (IEEE 802.16)	**NAI**	Network Access Identifier (RFC 2486)
3GTS	3rd Generation Technical Specification	**3G...**	3rd Generation ...

4

3.5 Details of I-WLAN 3GPP IP-Access

3.5.1 Network Architecture



The objective of this section is to illustrate how operator-owned or arbitrary WLAN's can be used to provide "I-WLAN 3GPP IP-Access" services.

The key points of this section are:
1. So called Wireless Access Gateways (WAG) are used between I-WLAN and TTG to assure charging data record generation and to allow for traffic filtering.
2. The GGSN may be expanded by a TTG to perform the tasks of a PDG.
3. The upper I-WLAN may belong to a third party operator (e.g. hotel) and support interworking towards various different PLMN's.

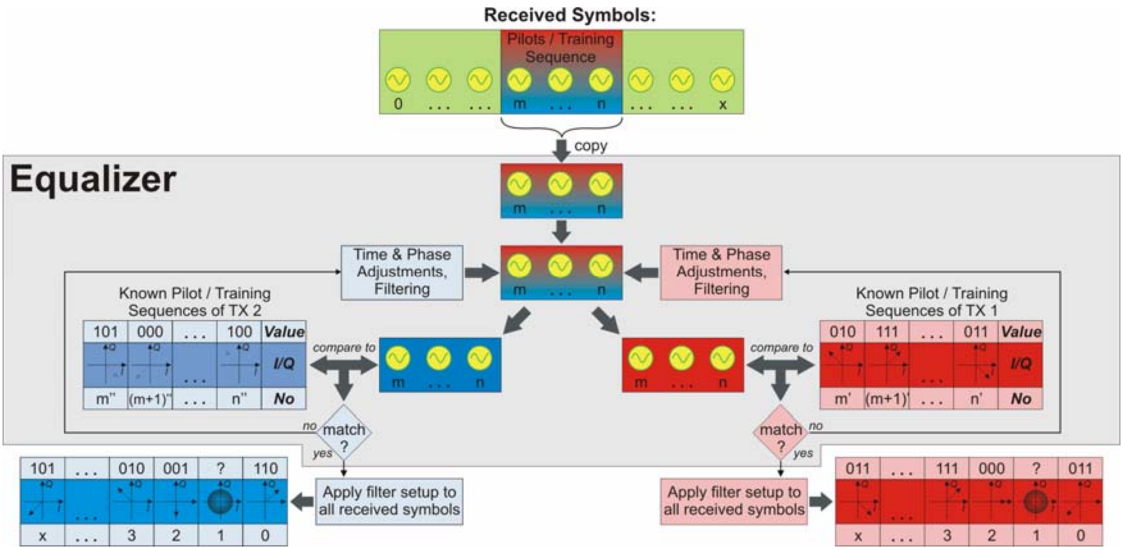
Room for your Notes

- **Abbreviations of this Section:**

AP	Access Point (IEEE 802.11, 802.16)	**WAG**	WLAN (Wireless Local Area Network) Access Gateway
DHCP	Dynamic Host Configuration Protocol (RFC 2131)	**H-PLMN**	Home PLMN
W-LAN	Wireless Local Area Network (IEEE 802.11)	**V-PLMN**	Visited PLMN
RADIUS	Remote Authentication Dial In User Service (RFC 2865)	**PLMN**	Public Land Mobile Network
AAA	Authentication, Authorization and Accounting	**HSS**	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5
TTG	Tunnel Termination Gateway	**3GPP**	Third Generation Partnership Project (Collaboration between different standardization organizations (e.g. ARIB, ETSI) to define advanced mobile communications standards, responsible for UMTS)
GGSN	Gateway GPRS Support Node	**IEEE**	Institute of Electrical and Electronics Engineers
PDG	Packet Data Gateway	**SGSN**	Serving GPRS Support Node
GERAN	GSM EDGE Radio Access Network	**UTRAN**	UMTS (Universal Mobile Telecommunication System)Terrestrial Radio Access Network
IKEv2	Internet Key Exchange protocol / version 2 (RFC 4306)	**ESP**	Encapsulating Security Payload (RFC 4303)
IP	Internet Protocol (RFC 791)		

5

2.3.2 Equalization – Distinction of Tx1 and Tx2



⇒ Equalizers operate based on known bit sequences like pilots of training sequences. A well known example for a training sequence is the midamble of a normal GSM-burst.

⇒ During the demodulation process the symbols (m … n) representing this training sequence / these pilot bits are copied into the equalizer.

⇒ This step is followed by the most important step for the understanding of equalization: The equalizer compares the result of its filtering on symbol (m … n) with the known pilot bits / training sequence. This process to remodel the current multipath situation is iterative and consists of various time and phase filter adjustments.

⇒ When a matching filter setup is found, this filter setup is also applied on the symbols that carry the data. Matching means that the detected symbols match those of the predefined pilot or training sequence bits.

⇒ Obviously, this approach is based on the assumption that the multipath does not change at least for the duration of a single burst / frame. In case of GSM this is true considering the burst duration of 577 µs and a maximum speed of 250 km/h:

⇒ 577 µs x 250 km/h = 0,04 m which is about 1/10 of the wavelength. That is: We can assume that the channel remains static for the duration of one burst even if the mobile station moves with a centrifugal speed of 250 km/h towards or away from the base station.

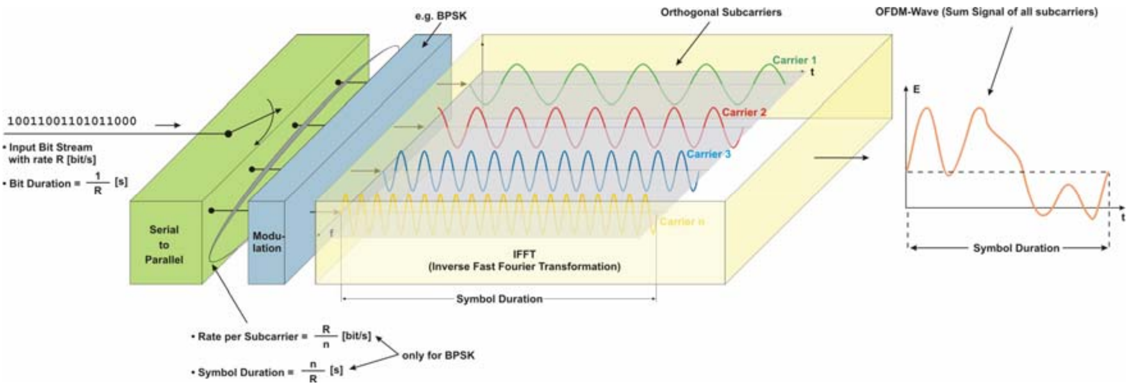
⇒ As the figure illustrates, a MIMO system "knows" the training sequence / pilot bits for each Tx-antenna beforehand (in the figure there have been two Tx's). Joint detection becomes possible. Joint detection means that the unique multipath pattern of each Tx Rx relationship can be used to receive from more than one transmit antenna on a single Rx-antenna at the same time, although the Tx-antennas use the same physical resources time, frequency and space.

Room for your Notes

- **Abbreviations of this Section:**

GSM	Global System for Mobile Communication	**MIMO**	Multiple In, Multiple Out

3.3.2.1 What is OFDM?



5

The objective of this section is to illustrate the principles of OFDM.

Key points of this section are:
1. By using any FDM-system, the rate of the input bit stream is reduced whereas the reduction rate depends on the number of carriers.
2. The more subcarriers with the same bandwidth are used, the more frequency demand the system has altogether. Of course, OFDM therefore is well suited for scalable frequency use.

⇒ The figure illustrates that OFDM firstly divides a high speed data stream of rate R into n substreams. If BPSK is used on all substreams, then the symbol rate on each substream becomes R/n.

⇒ Another very important consequence of OFDM is that the duration of one symbol (□ in case of BPSK of one bit, too) is extended from 1/R [s] before the S/P-conversion into n/R [s] behind the S/P-conversion.

⇒ In any case, the various substreams are input to independent modulators (e.g. BPSK with 1 bit/symbol, QPSK with 2 bit/symbol or 16-QAM with 4 bit/symbol) which modulate the symbols accordingly. Which modulation scheme is actually used per subcarrier is variable and there is no need that all subcarriers use the same modulation scheme.

⇒ Important for the OFDM is the fact that the different RF-carriers upon which the substreams are modulated are all orthogonal to each other (□ they don't interfere with each other).

⇒ All subcarriers are then added to each other and create a waveform like the one illustrated in the right part of the figure.

- **Some important remarks:**

  ⇒ As mentioned earlier: The modulation scheme which is actually used per subcarrier is variable and there is no need that all subcarriers use the same modulation scheme. If the different subcarriers use different modulation schemes then the input bit rate R depends on the number of bits per symbol which in turn depends on the modulation scheme.

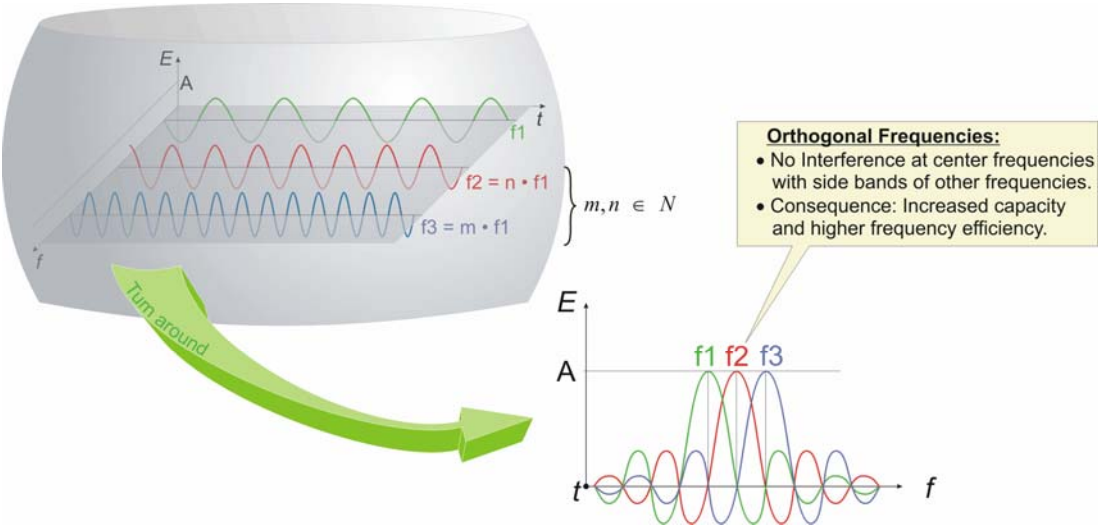
⇒ Each modulated subcarrier remains constant during one symbol duration (□ n/R), that is, there is no modulation change occurring during the symbol time. Please take a look at the figure; there are neither phase changes nor frequency or amplitude changes during one symbol duration.

⇒ Another important aspect is that in any case the amplitude of the OFDM-wave at the start of a symbol equals the amplitude at the end of that symbol because all contributing carriers provide a multiple of one period (□ n x 2π). The reason for this will be explained on the following slides.

- **Abbreviations of this Section:**

OFDM	Orthogonal Frequency Division Multiplexing	**FDM**	Frequency Division Multiplexing
QPSK	Quadrature Phase Shift Keying (⇔ 3GTS 25.213)	**BPSK**	Bipolar Phase Shift Keying
QAM	Quadrature Amplitude Modulation		

3.3.2.3.3 Step 3: Modulated Orthogonal Sine Waves



The objective of this section is to depict the consequence of using orthogonal carriers in an FDM-system.

Key point of this section is that orthogonal subcarriers avoid interference among each other only at the center frequencies because the amplitude of all other carriers is zero at these center frequencies.

Sampling
With OFDM, the receiver samples the received information only at the center carrier frequency. As the figure illustrates, no interference with adjacent carriers is possible.

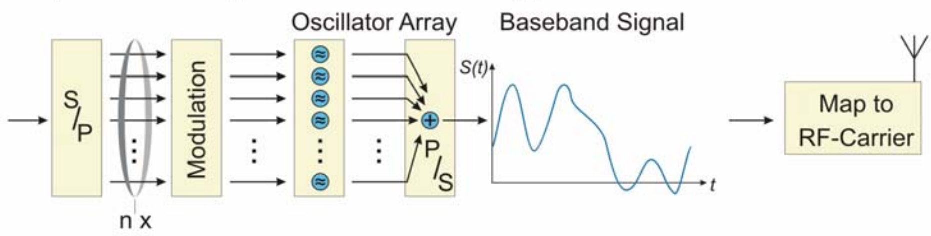
Room for your Notes

- **Abbreviations of this Section:**

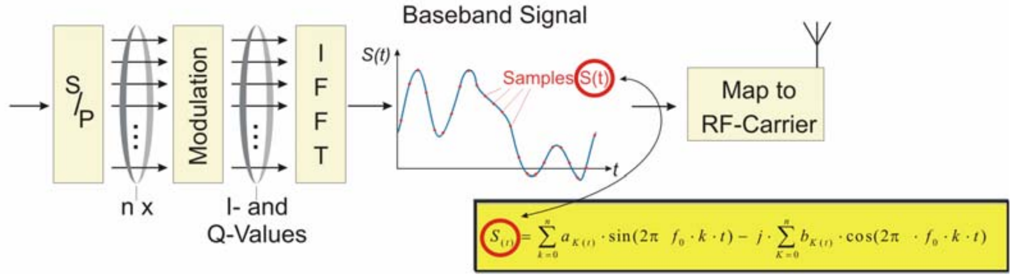
OFDM	Orthogonal Frequency Division Multiplexing	**FDM**	Frequency Division Multiplexing

3.3.2.4 And finally: Why do we need IFFT for OFDM?

1. Implementation Option: Discrete Technology



2. Implementation Option: Inverse FFT



The objective of this section is to illustrate how OFDM-systems are implemented in real-life applications.

Key points of this section are:
1. IFFT is used because the implementation of an oscillator array with possibly thousands of very accurate hardware oscillators is not feasible.
2. IFFT emulates the behaviour of orthogonal frequencies by calculating the sum function of definitely orthogonal frequencies. The orthogonality is then inherent because of the coefficient “k” which is used to multiply with the base frequency f(0).
3. The coefficients a(k(t)) and b(k(t)) represent the I/Q-coefficients of the related modulation schemes, e.g. QPSK or 16-QAM.

Additional Information
Please note that in both cases, the resulting S(t) is a baseband signal that needs to be mapped to the respective RF-carrier frequency.
The number of samples S(t) over one symbol duration T depends on the highest OFDM frequency which is k x f(0).
According to Nyquist, we therefore need 2 x k x f(0) different samples S(t) per symbol period T to provide for an error-free signal processing.
Obviously, for each sample S(t), all different k-values need to be applied.
We provided the aforementioned details to illustrate the enormous processing power that is required for OFDM.

Room for your Notes

- **Abbreviations of this Section:**

IFFT	Inverse Fast Fourier Transformation	**OFDM**	Orthogonal Frequency Division Multiplexing
RF	Radio Frequency	**QPSK**	Quadrature Phase Shift Keying (⇔ 3GTS 25.213)
16-QAM	16 symbols Quadrature Amplitude Modulation (⇔ 3GTS 25.213)		