UTRAN Architecture and Protocols

UTRAN ARCHITECTURE AND PROTOCOLS

First published 2000 by
WRAY CASTLE LIMITED
AMBLESIDE CUMBRIA
LA22 0JB U.K.

Yours to have and to hold but not to copy

The manual you are reading is protected by copyright law. This means that Wray Castle Limited could take you and your employer to court and claim heavy legal damages.

Apart from fair dealing for the purposes of research or private study, as permitted under the Copyright, Designs and Patents Act 1988, this manual may only be reproduced or transmitted in any form or by any means with the prior permission in writing of Wray Castle Limited.

© wray castle limited

UTRAN ARCHITECTURE AND PROTOCOLS

CONTENTS

Section 1 Introduction to the UTRAN

Lesson 1 Introduction
Lesson 2 UMTS Channel Types and Functions
Lesson 3 Types of Identifier

Section 2 UTRAN Areas and Access

Lesson 1 System Areas and UE States
Lesson 2 UE Synchronization

Section 3 General UTRAN Protocol Structure

Lesson 1 Introduction to UTRAN Protocols
Lesson 2 ATM
Lesson 3 Radio Network Layer and Transport Network Layer Identifiers

Section 4 Protocols Common to UTRAN Interfaces

Lesson 1 ALCAP
Lesson 2 SS7
Lesson 3 MTP3-b and M3UA
Lesson 4 Signalling Connection Control Part (SCCP)
Annex A IP
Annex B TCP/UDP

© wray castle limited

© wray castle limited

UTRAN ARCHITECTURE AND PROTOCOLS

CONTENTS

Section 5 Radio Protocols

Lesson 1 Radio Resource Control (RRC)
Lesson 2 Radio Link Control (RLC)
Lesson 3 Medium Access Control (MAC)
Lesson 4 Packet Data Convergence Protocol (PDCP) and Broadcast/Multicast Control (BMC)

Section 6 Terrestrial Protocols

Lesson 1 Iub Protocols
Lesson 2 Iur Protocols
Lesson 3 Iub and Iur Framing Protocols
Lesson 4 Iu Protocols (Circuit-Switched Domain)
Lesson 5 Iu Protocols (Packet-Switched Domain)
Annex A UTRAN Protocol Specifications
Annex B Message Sets

Section 7 Protocol Synopsis

Lesson 1 Overview of UTRAN Protocols

Section 8 Signalling Sequences

Lesson 1 Signalling Sequences
Lesson 2 Security

Section 9 Synchronization

Lesson 1 Synchronization

© wray castle limited

© wray castle limited

SECTION 1

INTRODUCTION TO THE UTRAN

© wray castle limited

LESSON 1

INTRODUCTION

© wray castle limited

LESSON CONTENTS

1 Services Provided by UMTS **1.1.1**
1.1 Introduction 1.1.1
1.2 General Aims 1.1.1
1.3 Fixed and Mobile Differentiation 1.1.1
1.4 Service Capabilities 1.1.3
1.5 Efficient Use of the Resource 1.1.3
1.6 UMTS Bit Rates 1.1.5
1.7 Factors Limiting Bit Rate 1.1.5

2 UMTS Teleservices **1.1.7**
2.1 Standardized Teleservices 1.1.7
2.2 Speech 1.1.7
2.3 Internet Access 1.1.7
2.4 Air Interface Modes of Operation 1.1.9

3 UMTS Main Elements **1.1.11**
3.1 Core Network (CN) 1.1.11
3.2 UMTS Terrestrial Radio Access Network (UTRAN) 1.1.11
3.3 User Equipment (UE) 1.1.11

4 UMTS Core Network **1.1.13**
4.1 Conditions for Evolution 1.1.13
4.2 General CN Architecture 1.1.13

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- state what services are supported within the UMTS concept
- state the UMTS teleservices
- briefly describe the overall architecture of UMTS, and the UTRAN's role within it

© wray castle limited

1 SERVICES PROVIDED BY UMTS

1.1 Introduction

The key aim for UMTS is that its service profile should carry those services and features that are generally associated with fixed networks into the mobile and roaming environments.

UMTS should provide an integrated telecommunication system that is able to support a wide range of applications. The throughput should be variable to provide a range of capability from narrowband to wideband. The user should experience true personal communication, regardless of location.

1.2 General Aims

If UMTS is to be successful, then all aspects of service provision need to be considered, including the need for types of services to be applicable to probable applications, and the ease with which these services can be utilized by the user. 3GPP Specification TS 22.101 'UMTS Service Principles' details many of these considerations. In many cases they are not specified as requirements, but set out as design aims for manufacturers and operators.

The reason for the relaxation of rigid service specification is to enable more flexibility for operators to differentiate their services from those of their competitors. Despite this, services should be accessed in a uniform and easy-to-understand way; this impacts on the design of both the service and the User Equipment (UE). It is also intended that a user should experience a similar level of service irrespective of location. In particular, attention should be paid to the roaming environment.

1.3 Fixed and Mobile Differentiation

The user should be able to access a range of services in the mobile environment, and these should offer similar rates and reliability to those normally associated with fixed networks. The practical limitations of the radio resource and radio characteristics will probably mean that this will not be possible in all environments. However, in the localized business and residential environments, full emulation of Private Branch Exchange (PBX) and Local Area Network (LAN)-type services should be available.

© wray castle limited

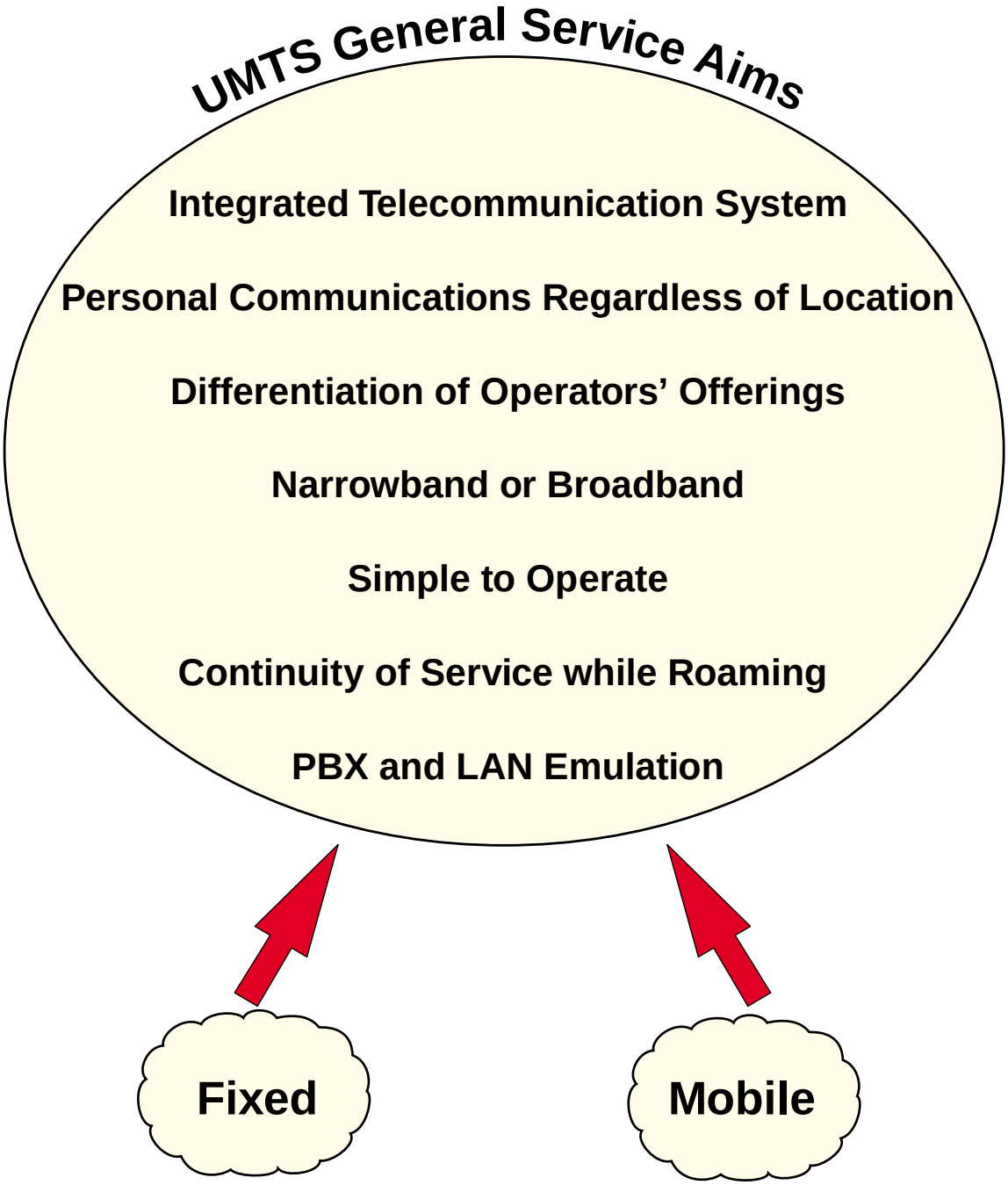


Figure 1
UMTS General Service Aims

© wray castle limited

1.4 Service Capabilities

For most telecommunications systems, including first- and second-generation mobile systems, it is common to define rigidly the bearer and teleservices that should be provided by an operator. However, it was felt that this approach would be too restrictive for third-generation systems. With this in mind, service capabilities have been defined for UMTS rather than a full set of teleservices. The teleservices that were defined for second-generation systems remain in place.

Service capabilities imply the definition of bearers, resource control mechanisms and QoS parameters. This allows operators to define more advanced teleservice types, based on the standard set of service capabilities. These non-standard services may include those used for alternative speech services: video, multimedia, messaging and other data applications.

1.5 Efficient Use of the Resource

Most applications, and in particular multimedia applications, exhibit some degree of asymmetry and are discontinuous. For example, applications involving Internet access would be both discontinuous and asymmetric; streaming video or audio would be completely asymmetric, but continuous. It is intended that UMTS, both in the Core Network (CN) and in the access network, will take full advantage of these characteristics to promote resource utilization efficiency.

© wray castle limited

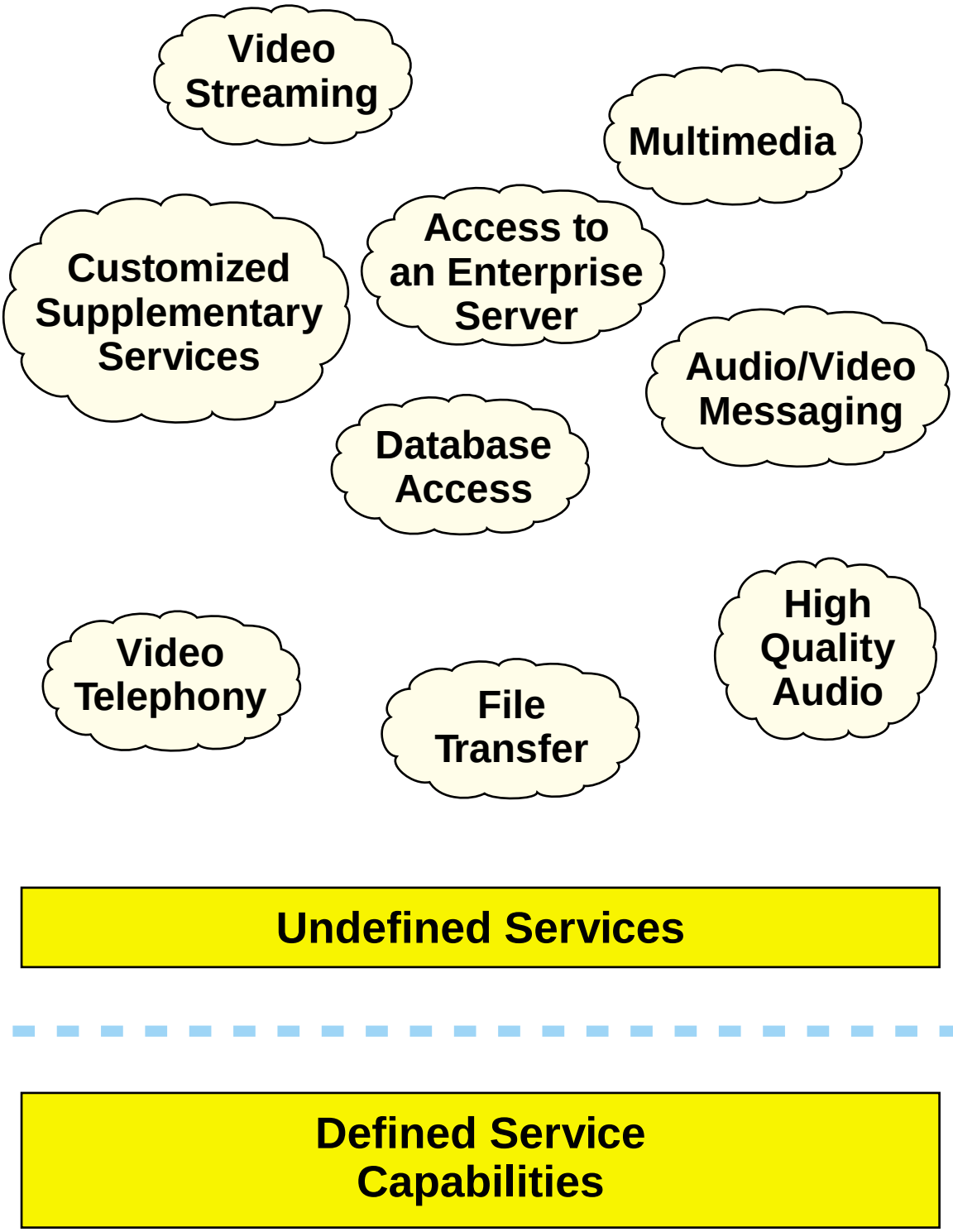


Figure 2
Service Capabilities

© wray castle limited

1.6 UMTS Bit Rates

An application requesting a bearer service will specify it in respect of the variables mentioned on the previous pages. It is possible for a single UE to have several active bearers in operation simultaneously: these may be a mixture of connection-oriented or connectionless services. The actual bit rate available for a particular application will depend on the radio environment and on operator-determined limitations.

In general, the aims for UMTS are summarized as:

- at least 144 kbit/s – rural outdoor
- at least 384 kbit/s – urban/suburban outdoor
- at least 2,048 kbit/s – indoor/low range outdoor

More detail is given in Figure 5.

1.7 Factors Limiting Bit Rate

There are two important factors that will limit the ultimate bit rate available to the user. The first will be related to the radio characteristics applicable to the user's physical location. This will include factors such as interference, Doppler shift and fading characteristics. These will affect the performance of the channel and, in general, more hostile radio conditions will limit the achievable throughput in the channel.

The second limiting factor relates to radio carrier capacity. The number of channels available on a UMTS radio carrier is inversely proportional to the bit rate provided in each channel. Thus the higher the bit rate allocated to a user, the fewer other users will have access to the cell. It is possible that one bearer at 2,048 kbit/s could represent the entire capacity of one radio carrier, which would represent a significant drain on network resources if allocated in a rural or suburban environment. However, it may be acceptable if allocated in the indoor picocell environment.

For Phase 1 of UMTS (Release 99), circuit-switched (CS) services are limited to 64 kbit/s due to Mobile Switching Centre (MSC) capability. Higher bit rates are only applicable to packet-switched (PS) services.

© wray castle limited

Operating Enviroment	Bit Rate	User Equipment Speed
Rural Outdoor	144 kbit/s	500 km/h
Urban/Suburban Outdoor	384 kbit/s	120 km/h
Indoor/Low Range Outdoor	2,048 kbit/s	10 km/h

Figure 3
Bearer Types for UMTS

© wray castle limited

2 UMTS TELESERVICES

Teleservices provide a description of the full end-to-end functionality of a specified service, including terminal, network and interworking functions. For UMTS there are some specified teleservices that provide compatibility with other network types as well as facilities for operators to introduce their own, more advanced teleservices.

2.1 Standardized Teleservices

The set of standardized teleservices reflects the need for interworking with other network types, in particular with GSM. They are mandatory for an operator, and they are:

- speech
- emergency calls
- Short Message Service (SMS)
- fax

2.2 Speech

The standard speech codec for UMTS will be the Adaptive Multi Rate (AMR) codec, as specified for GSM. The AMR codec really represents a collection of source coding capabilities, i.e. it incorporates a number of different operating modes which will be selected at call set-up according to geographical location and access conditions. These operating modes provide for efficient use of the air interface resource and compatibility with GSM, Japanese-specified networks and American National Standards Institute (ANSI)-specified networks. This can be summarized as follows:

- variable rate coding (eight rates)
- GSM Enhanced Full Rate (EFR) coding
- Packet Data Control (PDC) Enhanced Full Rate (EFR) coding
- ANSI-specified coding

2.3 Internet Access

The Internet is seen as the most important interworking requirement for UMTS. It is therefore intended that the specifications should provide for this. The aim is to facilitate optimized transmission of Internet Protocol (IP) traffic over the air interface, optimized use of encryption, and interoperation of QoS mechanisms.

© wray castle limited

Speech

Codec Mode	Source Codec Bit Rate
AMR_12.20	12.20 kbit/s (GSM EFR)
AMR_10.20	10.20 kbit/s
AMR_7.95	7.95 kbit/s
AMR_7.40	7.40 kbit/s (IS-641)
AMR_6.70	6.70 kbit/s (PDC-EFR)
AMR_5.90	5.90 kbit/s
AMR_5.15	5.15 kbit/s
AMR_4.75	4.75 kbit/s
AMR_SID	1.80 kbit/s

Emergency Call

Short Message Service (SMS)

Fax

Figure 4
Standardized UMTS Teleservices

© wray castle limited

2.4 Air Interface Modes of Operation

The UMTS specifications describe two different technology modes for the air interface. These are allocated to each of the two types of duplexed radio spectrum:

- Code Division Multiple Access (CDMA), used for the paired spectrum
- Time Division CDMA (TD-CDMA), used for the unpaired spectrum

The CDMA part of UMTS is used in the paired radio spectrum, i.e. Frequency Division Duplex (FDD). As such, it is referred to as FDD Mode 1. Mode 1 distinguishes it from the other technologies that are part of the 3GPP family of technologies. It may also be referred to as Direct Sequence (DS) Mode.

The TD-CDMA part of UMTS is used in the unpaired radio spectrum, i.e. Time Division Duplex (TDD). It is simply referred to as TDD Mode.

© wray castle limited

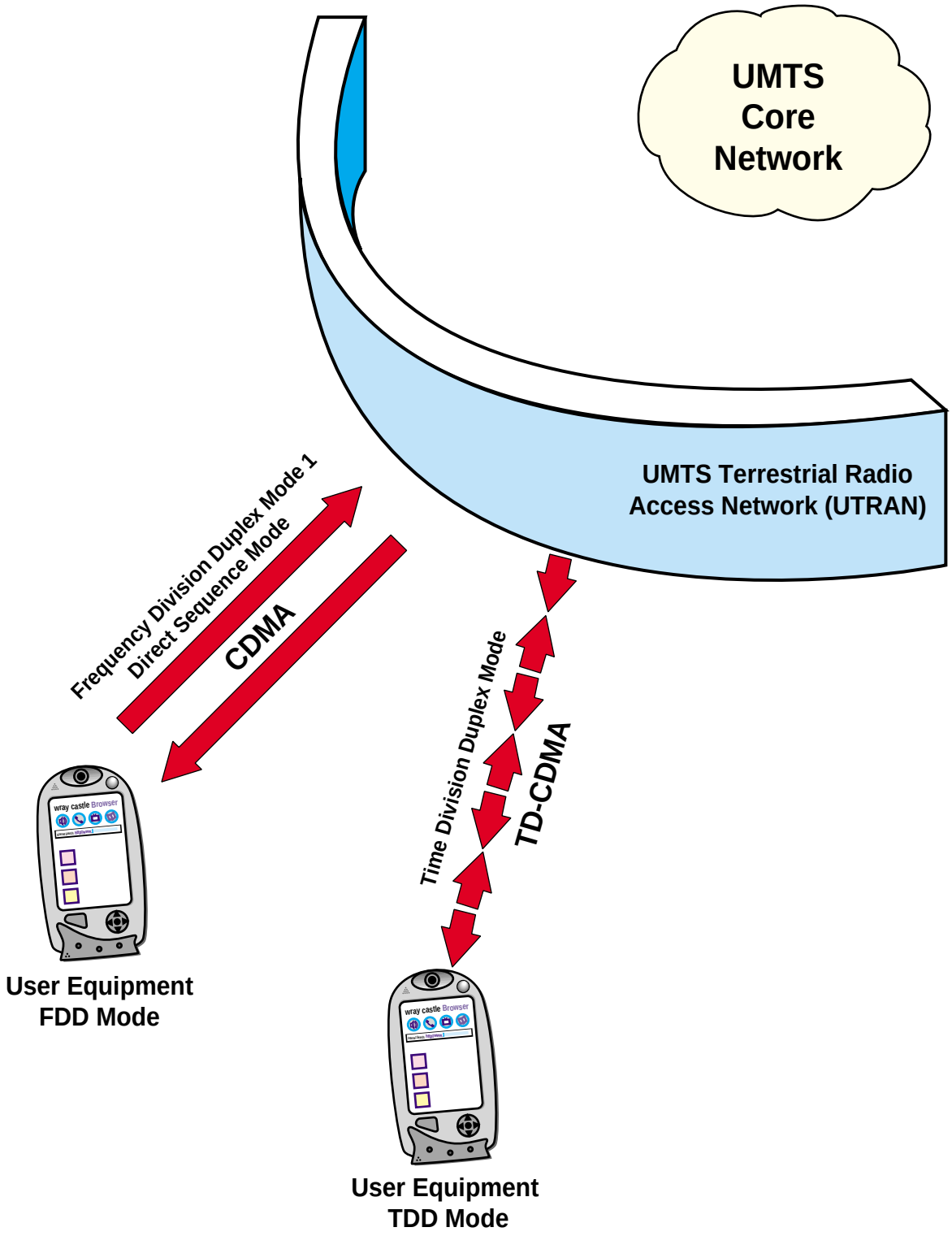


Figure 5
Air Interface Modes

© wray castle limited

3 UMTS MAIN ELEMENTS

A UMTS network can be considered as three interacting domains. These are the Core Network (CN), the UMTS Terrestrial Radio Access Network (UTRAN), and the User Equipment (UE). Interfaces are defined within and between these systems, providing standardization and, in many cases, inter-vendor compatibility.

3.1 Core Network (CN)

The main function of the CN is to provide switching, routing and transit for user traffic. There are many possible implementations for the CN, but a general requirement will be flexible high bandwidth capability, provided as real-time or non-real-time services. This may be provided by a combination of circuit switching and packet switching.

The CN will also contain the databases and network management functions.

3.2 UMTS Terrestrial Radio Access Network (UTRAN)

The UTRAN is concerned with the provision of radio coverage across the operating area and the provision of services across the air interface. Included in this is the handling of macro diversity through the provision of soft handover. Soft handover may take place within the UTRAN, or between UTRANs.

The UTRAN contains the base stations, referred to as Node Bs, and Radio Network Controllers (RNCs), which provide the control functionality for one or more Node Bs.

The description of Node B and RNC functions is logical rather than physical. Although there is a defined interface between Node B and RNC, the logical nature of their definition means that this does not necessarily correspond to a physical interface in a particular vendor’s equipment.

A single RNC and its associated Node Bs is known collectively as Radio Network Subsystem (RNS). An UTRAN may contain one or more RNS.

3.3 User Equipment (UE)

The UE encompasses the radio equipment, application platform and Man–Machine Interface (MMI) used by a subscriber to access services provided by the network. There are different classes of UE with differing levels of capability, and there are many different physical forms for the UE, depending on the intended function.

© wray castle limited

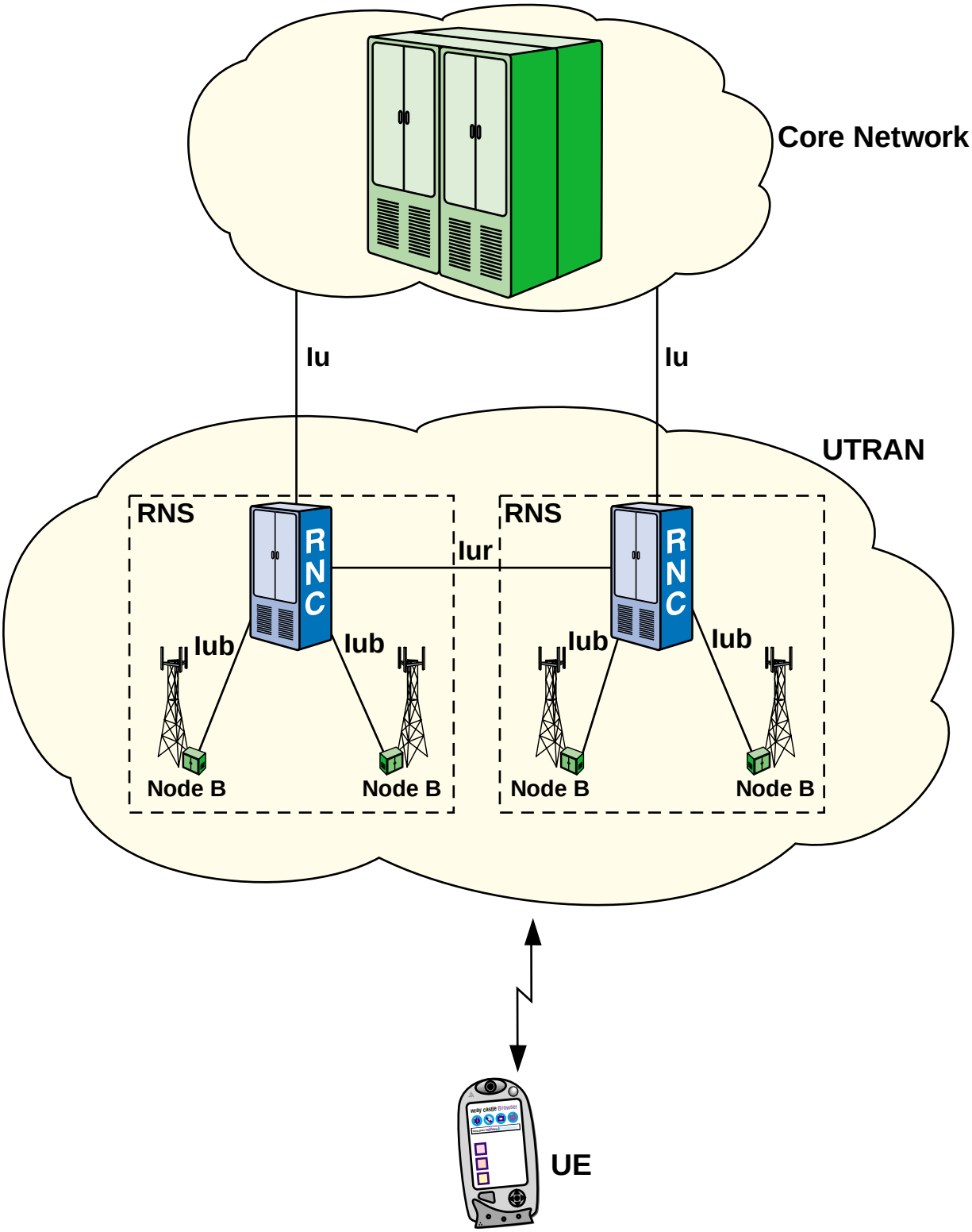


Figure 6
UMTS Main Elements

© wray castle limited

4 UMTS CORE NETWORK

4.1 Conditions for Evolution

The first third-generation systems are assumed to be built on an evolved GSM system. There are a number of preconditions that need to be in place to support the full functionality of Release 99. The main requirement is the provision of General Packet Radio Service (GPRS) within the GSM system.

Release 99 allows for separated or combined Mobile Switching Centre/Visitor Location Register (MSC/VLR) and Serving GPRS Support Node (SGSN) architectures.

4.2 General CN Architecture

The basic architecture for UMTS is based on that of GSM incorporating GPRS. Thus switching will be a combination of circuit switching provided by the MSC/VLR, and packet switching provided by the SGSN and the Gateway GPRS Support Node (GGSN).

These GSM elements are, however, modified for UMTS operation and service provision. A UMTS MSC will need to support a new interface in order to communicate and exchange traffic with the UTRAN. Similarly, a 3G-SGSN will also need to support the new interface. In both cases these elements will need to be able to supply the bearer types required to provide UMTS multimedia services.

The GSM databases VLR and Home Location Register (HLR) are present in UMTS. The VLR is a temporary distributed database assumed to be integrated into the MSC. The HLR is a permanent store for subscriber data within an operator’s system.

© wray castle limited

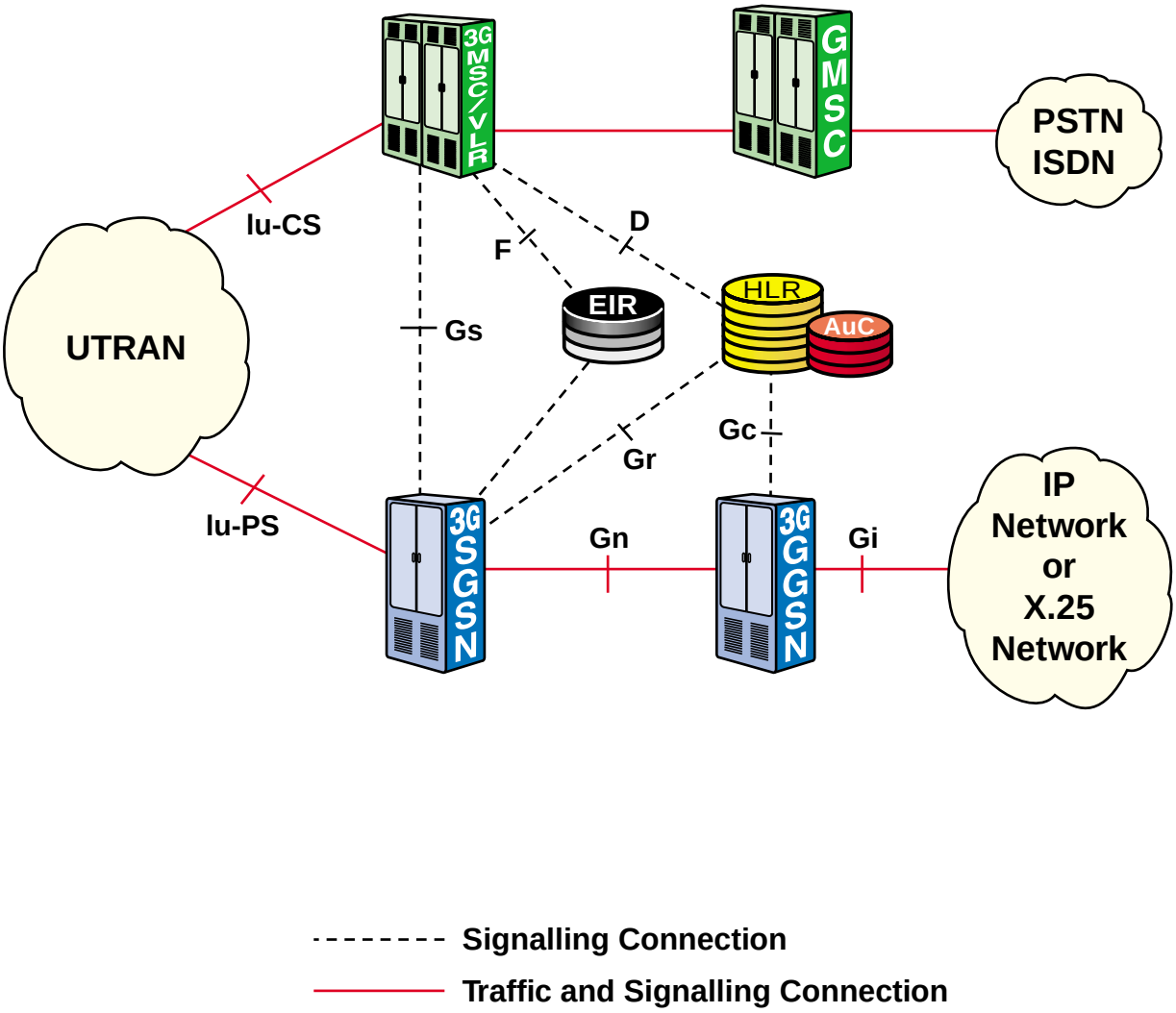


Figure 7
UMTS Core Network

© wray castle limited

© wray castle limited

LESSON 2

UMTS CHANNEL TYPES AND FUNCTIONS

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 UMTS Channel Types and Functions 1.2.1
1.1 Logical Channels 1.2.1
1.2 Transport Channels 1.2.5
1.3 Transport Formats 1.2.5
1.4 Transport Channel Types 1.2.7

2 FDD Access Mode – L1 to L2 Mapping 1.2.9
2.1 Logical to Transport Channel Mapping 1.2.9
2.2 Mapping for the Uu Interface 1.2.9

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe the different UMTS channel types and their functions

© wray castle limited

1 UMTS CHANNEL TYPES AND FUNCTIONS

1.1 Logical Channels

The MAC layer provides transfer services via a set of logical channels. A logical channel is defined for each different transfer requirement. Each logical channel relates to particular kinds of information that need to be transferred. Some relate to signalling information, some to traffic information.

Most of the logical channels are applicable to both FDD mode and TDD mode, but a few are applicable only to TDD mode, as indicated in Figure 1.

The following logical channels are used for the transfer of signalling information:

- Broadcast Control Channel (BCCH)
- Paging Control Channel (PCCH)
- Common Control Channel (CCCH)
- Dedicated Control Channel (DCCH)
- ODMA Common Control Channel (OCCCH)
- ODMA Dedicated Control Channel (ODCCH)

The following logical channels are used for the transfer of user information:

- Dedicated Traffic Channel (DTCH)
- ODMA Dedicated Traffic Channel (ODTCH)
- Common Traffic Channel (CTCH)

© wray castle limited

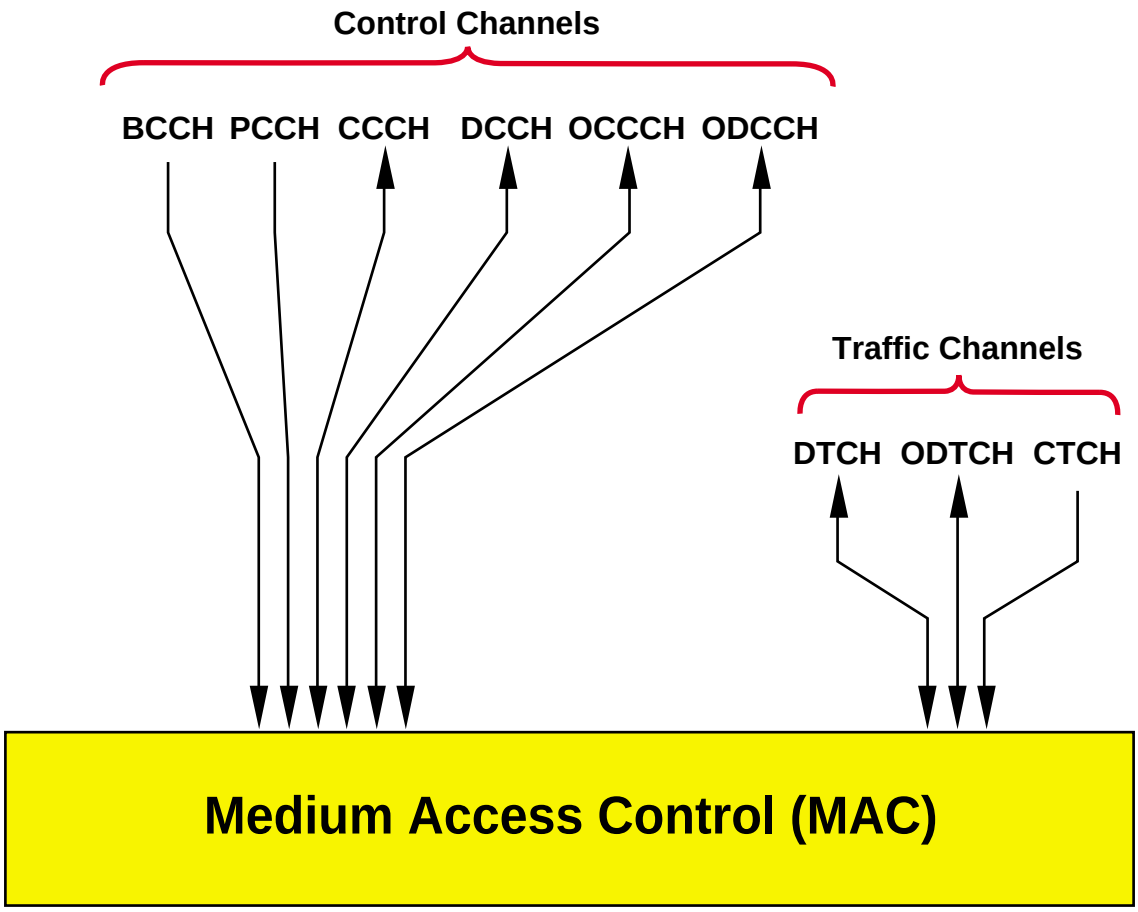


Figure 1
Logical Channel Types

© wray castle limited

1.1.1 Broadcast Control Channel (BCCH)

The BCCH is a downlink (DL) BCH carrying system information.

1.1.2 Paging Control Channel (PCCH)

The PCCH is a DL channel carrying paging messages. It is used when the network does not know the location cell of the UE, or when the UE is using sleep mode procedures.

1.1.3 Common Control Channel (CCCH)

The CCCH is a bidirectional channel carrying control information between the network and the UE. It is used when the UE has no Radio Resource Control (RRC) connection with the network.

1.1.4 Dedicated Control Channel (DCCH)

The DCCH is a point-to-point bidirectional channel carrying dedicated control information between the network and the UE. It is used when a dedicated connection has been established through RRC connection set-up procedures.

© wray castle limited

1.1.5 ODMA Common Control Channel (OCCCH)

The OCCCH is a bidirectional channel for transmitting control information directly between UEs. It is used when the UE has no RRC connection with the network.

1.1.6 ODMA Dedicated Control Channel (ODCCH)

The ODCCH is a point-to-point bidirectional channel carrying dedicated control information directly between UEs. It is used when a dedicated connection has been established through RRC connection set-up procedures.

1.1.7 Dedicated Traffic Channel (DTCH)

The DTCH is a dedicated point-to-point channel carrying user information between the network and the UE. It may be used in both the uplink (UL) and DL directions.

1.1.8 ODMA Dedicated Traffic Channel (ODTCH)

The ODTCH is a dedicated point-to-point channel carrying user information directly between UEs. It is used as a relay link.

1.1.9 Common Traffic Channel (CTCH)

The CTCH is a point-to-multipoint unidirectional channel carrying user information for a specified group of UEs.

© wray castle limited

1.2 Transport Channels

Information is transferred from the MAC layer and mapped into the physical channels via a set of transport channels. Transport channels can be classified into two groups: common channels and dedicated channels. Information in common channels will require inband identification of the UE. For dedicated channels, the UE's identity is associated with the channel allocation.

The common transport channels are:

- Random Access Channel (RACH)
- ODMA Random Access Channel (ORACH)
- Common Packet Channel (CPCH) (FDD mode only)
- Forward Access Channel (FACH)
- Downlink Shared Channel (DSCH)
- Uplink Shared Channel (USCH) (TDD mode only)
- Broadcast Channel (BCH)
- Paging Channel (PCH)

The dedicated transport channels are:

- Dedicated Channel (DCH)
- ODMA Dedicated Channel (ODCH)

1.3 Transport Formats

Each transport channel has an associated transport format. This is defined as a combination of encoding, interleaving, bit rate and mapping into physical channels. For some transport channels this may be variable within a set of transport formats.

© wray castle limited

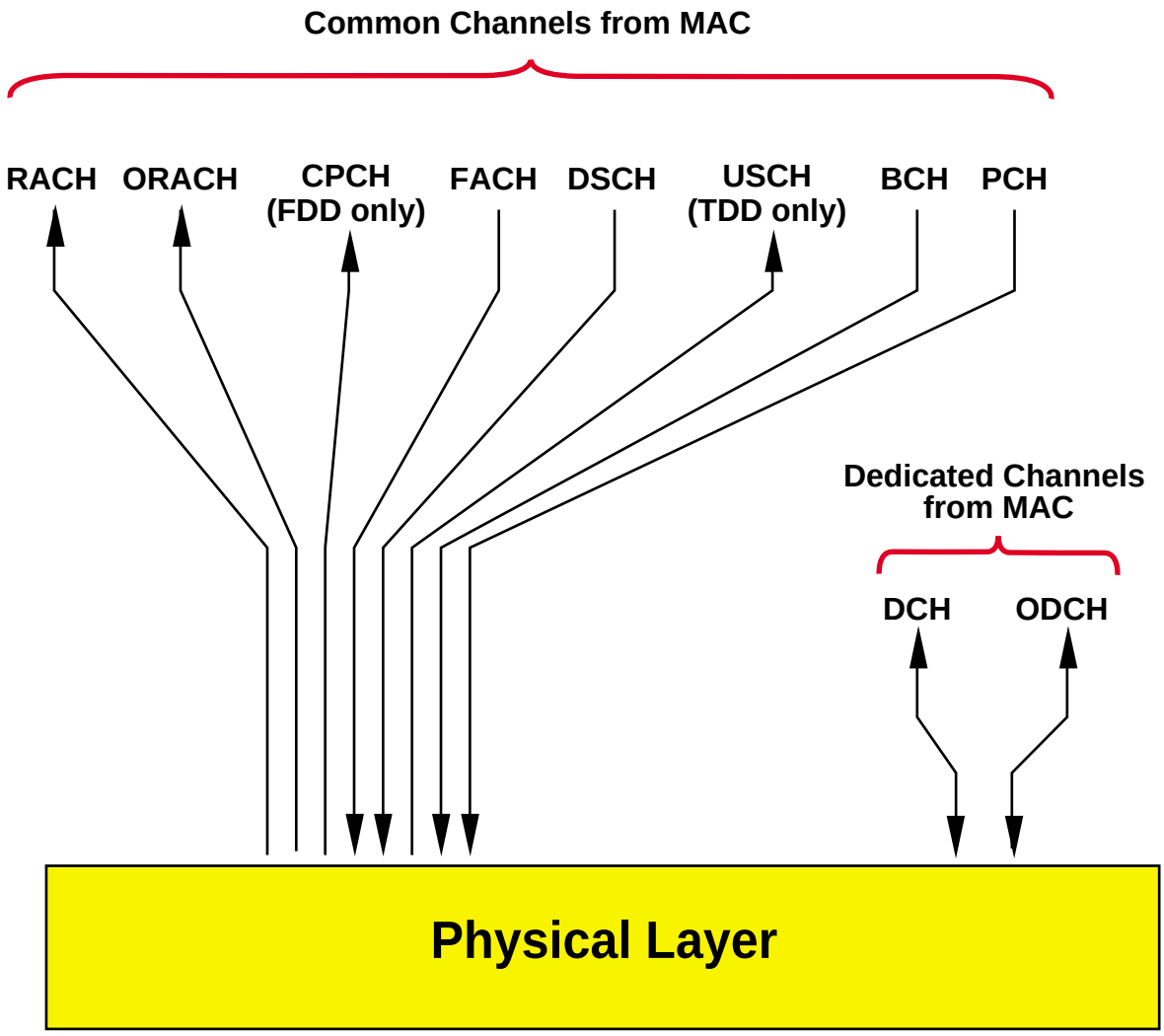


Figure 2
Transport Channel Types

© wray castle limited

1.4 Transport Channel Types

1.4.1 Random Access Channel (RACH)

The RACH is a contention-based channel in the UL direction. It is used for initial access or non-real-time dedicated control or traffic data.

1.4.2 ODMA Random Access Channel (ORACH)

The ORACH is similar to the RACH. It is used in the relay link.

1.4.3 Common Packet Channel (CPCH)

The CPCH is only used in FDD mode. It is a contention-based channel, used for the transmission of bursty traffic data in a shared mode. Fast power control is used.

1.4.4 Forward Access Channel (FACH)

The FACH is a common DL channel without power control. It is used for relatively small amounts of data.

1.4.5 Downlink Shared Channel (DSCH)

The DSCH is a DL channel used in shared mode by several UEs. It is used to carry control or traffic data.

1.4.6 Uplink Shared Channel (USCH)

The USCH is only used in TDD mode. It is an UL channel used in shared mode by several UEs. It is used to carry control or traffic data.

© wray castle limited

1.4.7 Broadcast Channel (BCH)

The BCH is a DL Channel used to carry system information across a whole cell.

1.4.8 Paging Channel (PCH)

The PCH is a DL BCH used to carry paging and notification messages across a whole cell.

1.4.9 Dedicated Channel (DCH)

The DCH is used in the UL or DL direction to carry user information to or from the UE.

1.4.10 ODMA Dedicated Channel (ODCH)

The ODCH is dedicated to one UE that is being used in the relay link.

© wray castle limited

2 FDD ACCESS MODE – L1 TO L2 MAPPING

2.1 Logical to Transport Channel Mapping

Before its transmission across the air interface, information presented in logical channels must be mapped into transport channels. This mapping process is very flexible, and for some logical channels there are several options, depending on the function and the type of information being transferred.

2.2 Mapping for the Uu Interface

The directions of arrows shown in Figure 3 reflect the mapping process as seen from the UTRAN side. For the channels carrying broadcast information, mapping is direct from BCCH to BCH and from PCCH to PCH.

For the other control and traffic-carrying channels, mapping is more flexible. For example, DL DCCH can be mapped either to FACH or to DSCH, depending on information requirements. In the UL direction, DCCH may take information from CPCH, RACH, USCH or DCH. The logical channel DTCH is similar, in that it has access to a range of transport channels. However, the CCCH is simple; it uses only RACH and FACH for bidirectional communication.

© wray castle limited

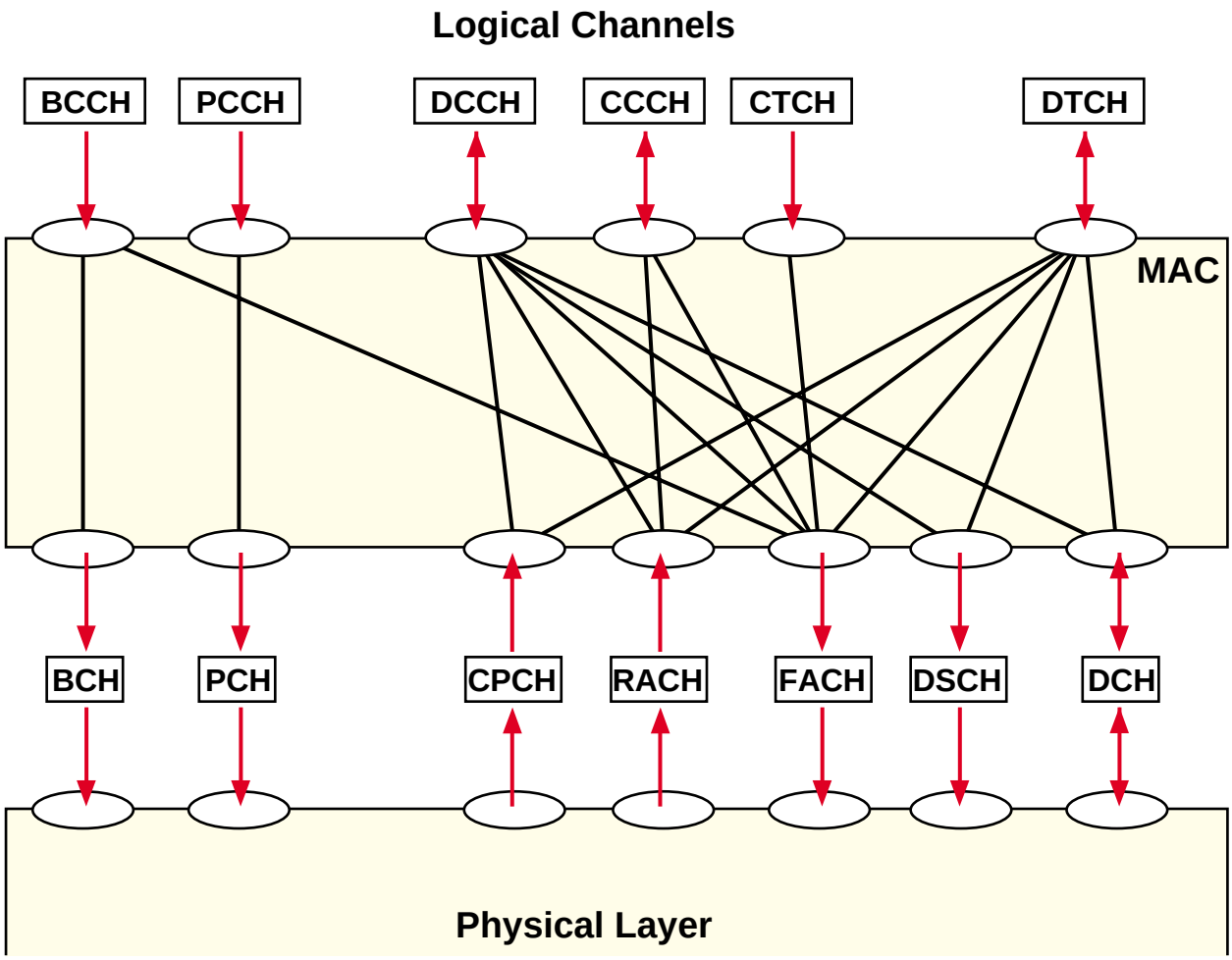


Figure 3

FDD Model Logical to Transport Channel Mapping

© wray castle limited

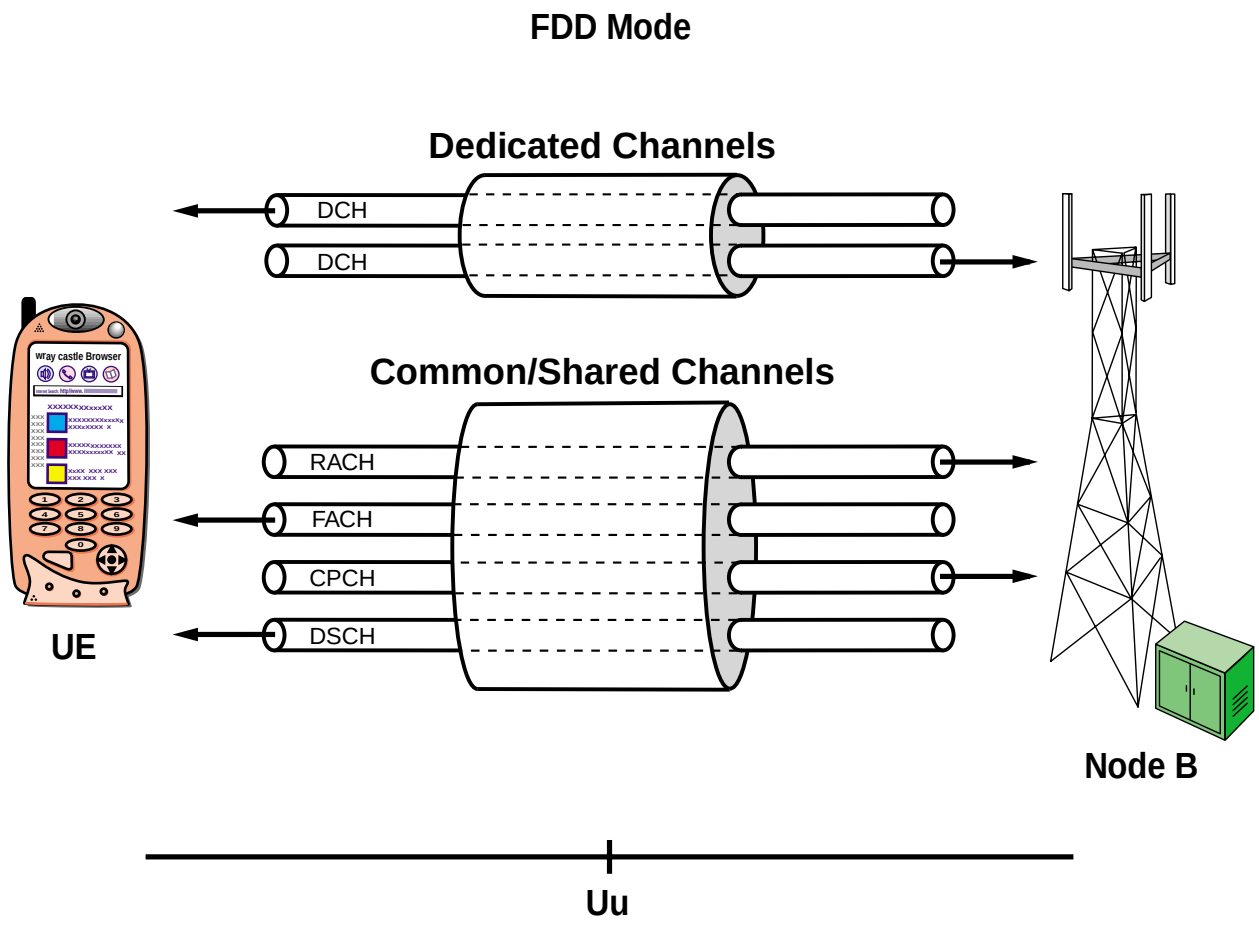


Figure 4
Summary of Transport Layer Pipes (FDD Mode)

© wray castle limited

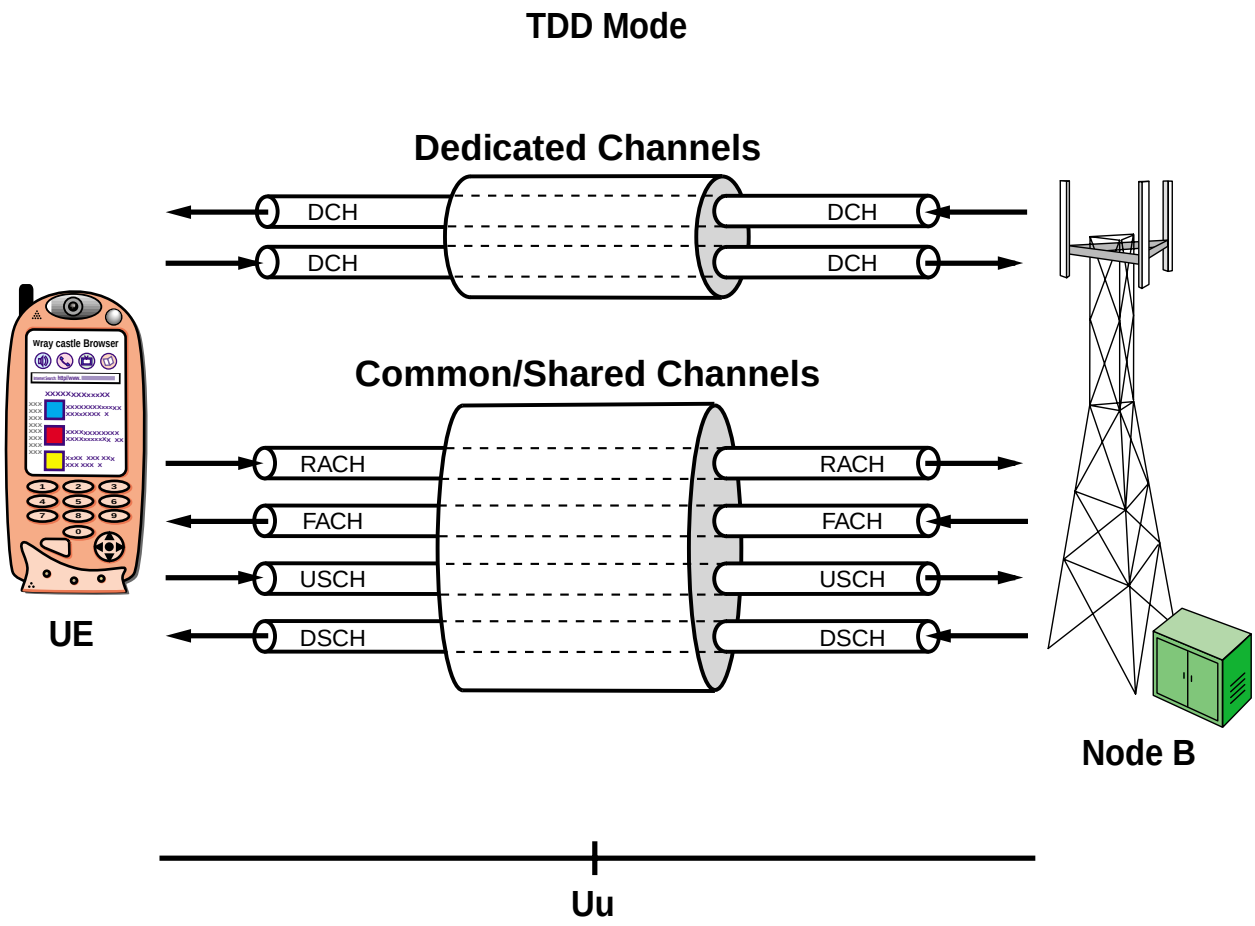


Figure 5
Summary of Transport Layer Pipes (TDD Mode)

© wray castle limited

© wray castle limited

LESSON 3

TYPES OF IDENTIFIER

© wray castle limited

© wray castle limited

LESSON CONTENTS

1	**The Radio Network Controller (RNC)**		**1.3.1**
2	**The Node B**		**1.3.3**
	2.1	Closed Loop Power Control	1.3.5
	2.2	Additional Functions of a Node B	1.3.7
3	**Types of RNC**		**1.3.9**
	3.1	Different RNCs	1.3.9
4	**Iu Interface**		**1.3.11**
	4.1	Location of the Iu Interface	1.3.11
5	**Identifiers used within the UTRAN**		**1.3.13**
	5.1	Introduction	1.3.13
	5.2	PLMN Identifier (PLMN-Id)	1.3.13
	5.3	Global RNC Identifier (RNC-Id)	1.3.13
	5.4	Service Area Identifier (SAI)	1.3.13
	5.5	Cell Identifier (C-Id)	1.3.13
	5.6	UE Identifiers	1.3.15
	5.7	UE Core Network Identifiers	1.3.17

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe in detail the architecture of the UTRAN, including the functions of the Serving Radio Network Controller (SRNC), the Drift Radio Network Controller (DRNC), the Radio Network Controller (RNC) and the Node B
- explain the structure of the UTRAN identifiers

© wray castle limited

1 THE RADIO NETWORK CONTROLLER (RNC)

The RNC controls many functions, which can be grouped into five main areas:

Overall Systems Access Control
This allows the UMTS user to access the UTRAN for UMTS services.

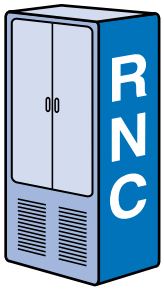
Radio Channel Ciphering and Deciphering
This protects the radio transmitted data from unauthorized third parties.

Functions Related to Mobility
These manage the mobility of users within the UTRAN.

Functions Related to Radio Resource Management
These look after main aspects of radio resources.

Functions Related to Broadcast and Multicast services
Only broadcast services are applicable to Release 99.

© wray castle limited



Radio Network Controller (RNC)

Functions include:

- **Overall System Access Control**
  - **Admission Control**
  - **System Broadcasting Signalling**
- **Radio Channel Ciphering and Deciphering**
- **Mobility**
  - **Handover Control**
- **Radio Resource Management**
  - **Radio Resource Control**
  - **Channel Allocation**
  - **Power Control Thresholds**
  - **Macro Diversity**
  - **Combining/Splitting**
  - **Open Loop Power Control**
- **Broadcast and Multicast**

Figure 1
The RNC

© wray castle limited

2 THE NODE B

Node B functional behaviour is specified exactly and completely, allowing the operator to interconnect different manufacturers' equipment.

The Node B maintains the radio link between the UE and the UTRAN. Its functions include:

Radio Transmission/Reception
This includes modulation and demodulation of the radio carrier.

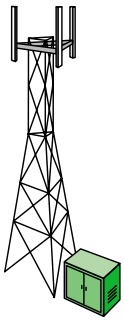
CDMA Physical Channel Coding
This is the application of CDMA spreading and scrambling codes to data streams.

Micro Diversity
This is the combining of different radio paths at the Node B.

Error Protection
Physical layer error protection using Forward Error Correction (FEC) techniques.

Closed Loop Power Control
Fast power control to an individual mobile.

© wray castle limited



Node B

Functions include:

- **Transmission/Reception**
- **CDMA Physical Channel Coding**
- **Micro Diversity**
- **Error Protection**
- **Closed Loop Power Control**

Figure 2
The Node B

© wray castle limited

2.1 Closed Loop Power Control

Closed loop power control can be divided into two processes:

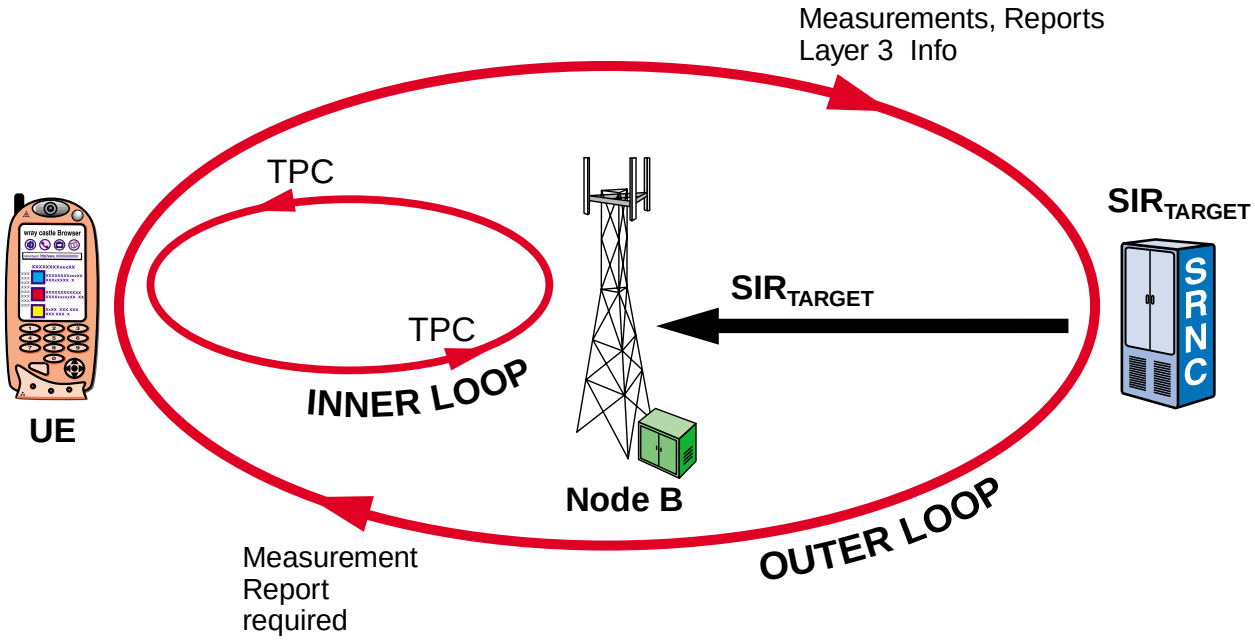
Outer Loop
Outer loop power control sets the Signal-to-Interference Ratio (SIR_{target}). This is carried out via RRC Layer 3 measurement reports sent from the UE to the SRNC.

Inner Loop
The inner loop power control in the physical layer (adjustment is done with Transmit Power Control (TPC) commands) adjusts the peer entity transmit power so that the measured SIR fulfils the SIR_{target} requirement.

The receiving entity (UE physical layer or Node B physical layer) measures the SIR and compares it to the SIR_{target}. If $SIR_{est} – SIR_{target}$ is larger than 0 then TPC bits = 00, therefore commanding its peer entity to reduce its transmit power. The TPC is transmitted once in every timeslot. There is no neutral command, it is either up or down.

Note, inner loop is performed entirely in the physical layer. It therefore makes the system very fast in the adjustment of power control demand.

© wray castle limited



Outer loop power control sets signal-to-interference ratio (SIR_{TARGET})

Inner loop power control in Layer 1 adjusts peer entity transmit power so that the measured SIR fulfils SIR_{TARGET} requirements

Figure 3

Transmit Power Control (TPC) Commands

© wray castle limited

2.2 Additional Functions of a Node B

2.2.1 Adaptive Antennas

UMTS will probably be the first network to exploit the use of adaptive antennas on a widespread basis. Interference is the major factor of WCDMA systems as this has a direct effect on the capacity of a cell, i.e. the number of users a cell can support. Adaptive antennas are particularly useful in WCDMA as they reduce the amount of intra-cell interference considerably.

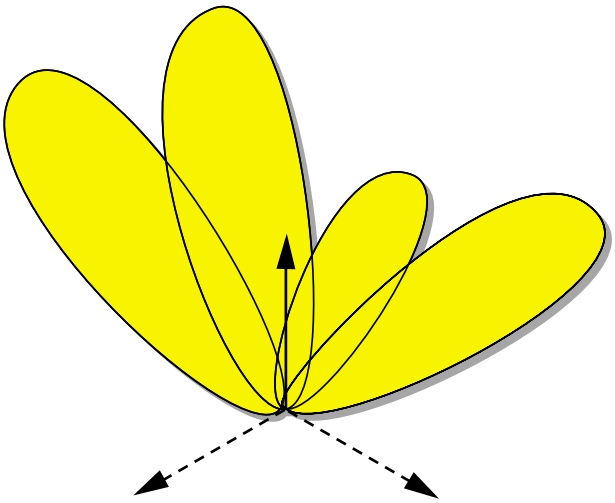
Adaptive antennas have multiple beams. Each beam may be dynamically ajdusted in gain and azimuth. Dynamic adjustment is used to optimize the cell's performance in terms of traffic capacity, interference rejection and coverage.

With adaptive antennas it is possible that frequency, time and codes could be reused on a single site.

In summary, the benefits of adaptive antennas include the reduction of co-channel interference; an increase in the range of a cell; and increased capacity.

Adaptive antennas are sometimes known as smart antennas.

© wray castle limited



Azimuth and radiated power of beam(s) may be dynamically adjusted to account for traffic distribution and interference sources

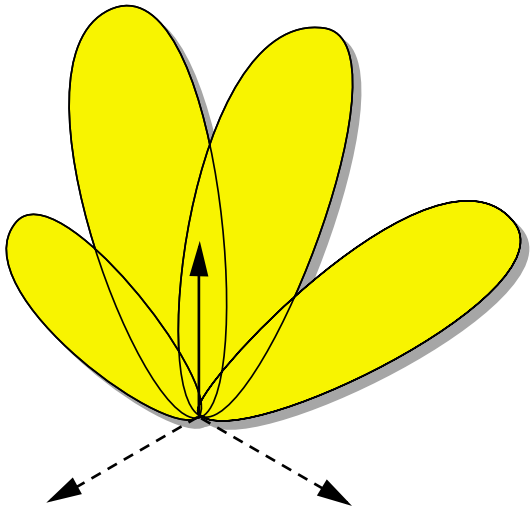


Figure 4
Adaptive Beamforming Antennas

© wray castle limited

3 TYPES OF RNC

3.1 Different RNCs

The RNC can be identified as a Controlling RNC (CRNC), Serving RNC (SRNC) or Drift RNC (DRNC).

3.1.1 Controlling RNC (CRNC)

The RNC controlling a Node B is identified as the CRNC. The CRNC has many functions including code allocation, admission control, scheduling of system information, cell configuration and radio link management.

3.1.2 Serving RNC (SRNC)

The SRNC is the RNC that terminates the Iu interface (data and signalling) for a specific mobile. The signalling between the UE and the UTRAN is Radio Resource Control (RRC), which is terminated at the SRNC. SRNC functions also include Radio Resource Management (RRM), outer loop power control and handovers. The UE can be connected to only one SRNC.

3.1.3 Drift RNC (DRNC)

It is possible that the UE is using a cell belonging to an RNC other than the SRNC. This RNC is called a Drift RNC (DRNC).

© wray castle limited

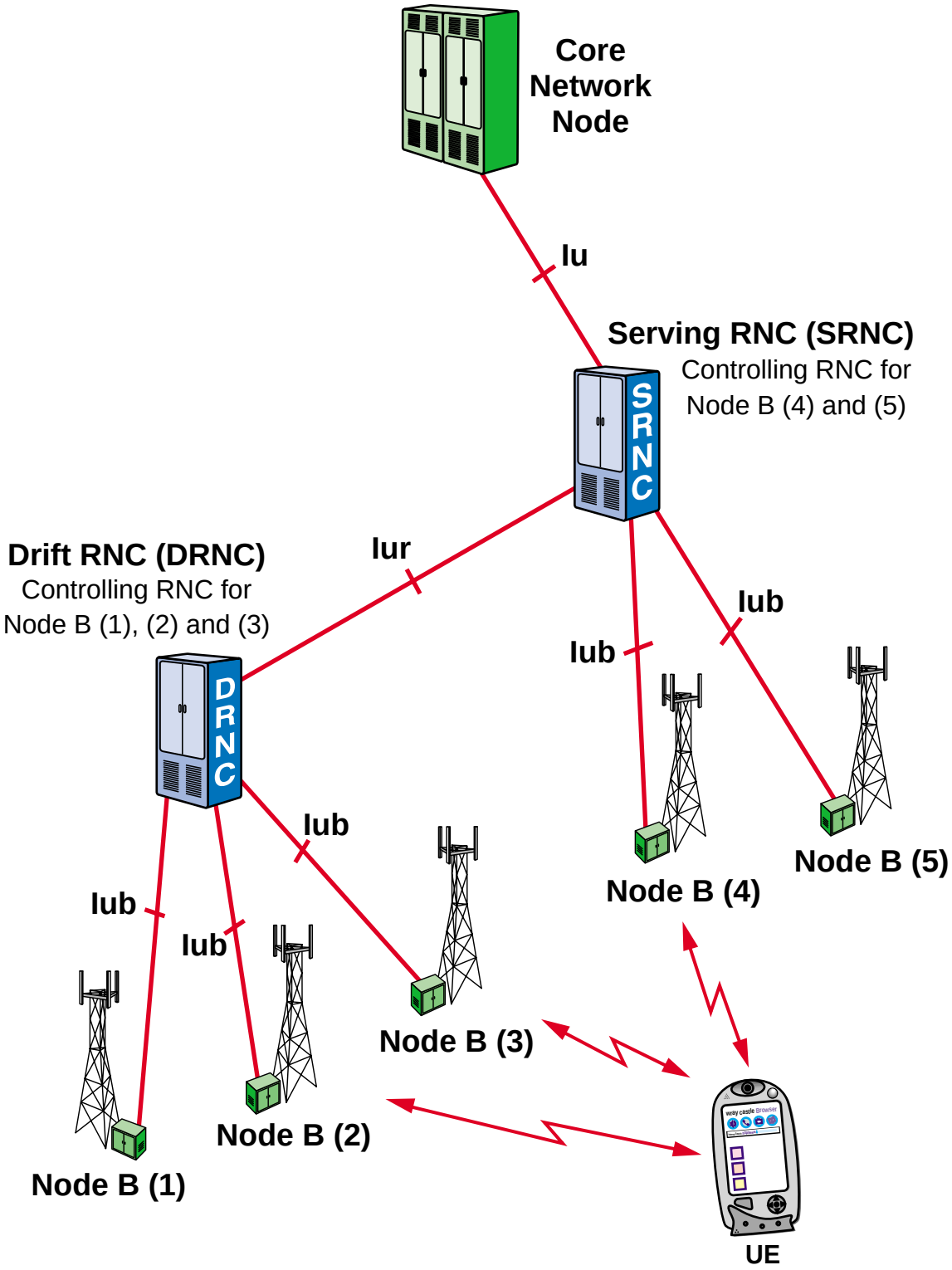


Figure 5
Serving and Drift RNC

© wray castle limited

4 Iu INTERFACE

4.1 Location of the Iu Interface

The Iu interface is used to carry signalling and traffic between the UTRAN and the CN. The access point within the UTRAN will be the RNC. This access point can be connected to no more than one CN domain of each type.

A 3G-CN may have either combined or separated packet-switched (PS) and circuit-switched (CS) domains. Each of these domains may be connected to one or more UTRAN access point, i.e. RNC. The interface between the CS domain and the RNC is called Iu-CS; the interface between the PS domain and the RNC is called the Iu-PS.

The access points within the CN will be a 3G-MSC for the Iu-CS interface, and the 3G-SGSN for the Iu-PS interface.

The Iu-BC is used for the forwarding of cell broadcast messages from the cell broadcast centre to the relevant service area. The information passed will contain the actual information to be broadcast to UEs in the service area, plus the scheduling information, e.g. repeat time.

© wray castle limited

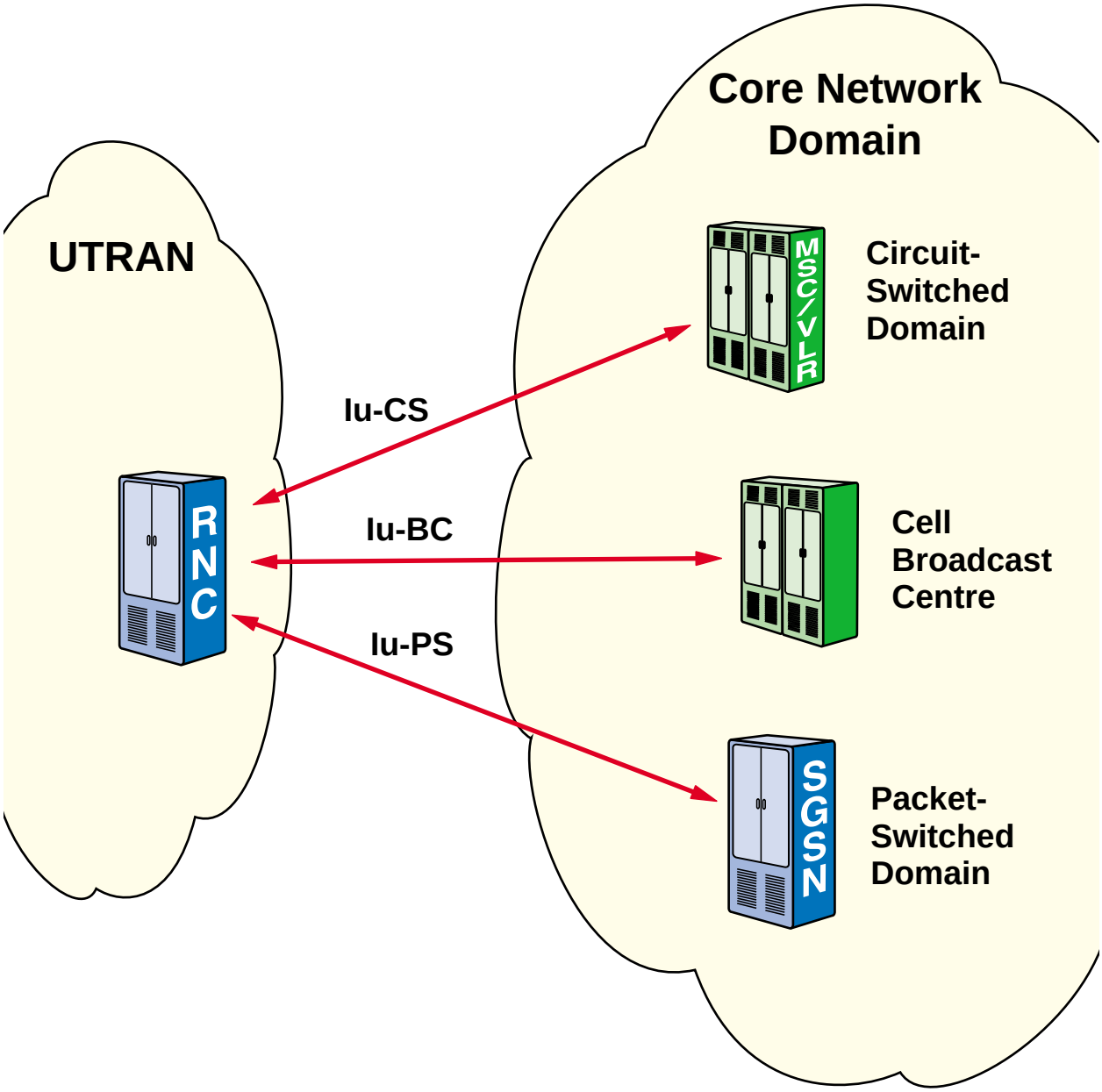


Figure 6
Iu Interface

© wray castle limited

5 IDENTIFIERS USED WITHIN THE UTRAN

5.1 Introduction

The UTRAN uses a number of different identifiers.

5.2 PLMN Identifier (PLMN-Id)

The PLMN-Id uniquely identifies a Public Land Mobile Network (PLMN). The UTRAN can identify the CN EDGE node by its CN Domain Identifier. There are two types of CN Domain identifiers:

CS = PLMN-Id + LAC

PS = PLMN-Id + LAC + RAC.

5.3 Global RNC Identifier (RNC-Id)

An RNC node is uniquely identified within UTRAN by its RNC-Id. The RNC-Id and the PLMN-Id together are used to globally identify the RNC.

5.4 Service Area Identifier (SAI)

The SAI uniquely identifies an area consisting of one or more cells. The Service Area can be used for indicating the location of a UE to the CN.

5.5 Cell Identifier (C-Id)

The C-Id uniquely identifies a cell within an RNS. The UTRAN Cell Identity (UC-Id) consists of the C-Id together with the RNC-Id.

© wray castle limited

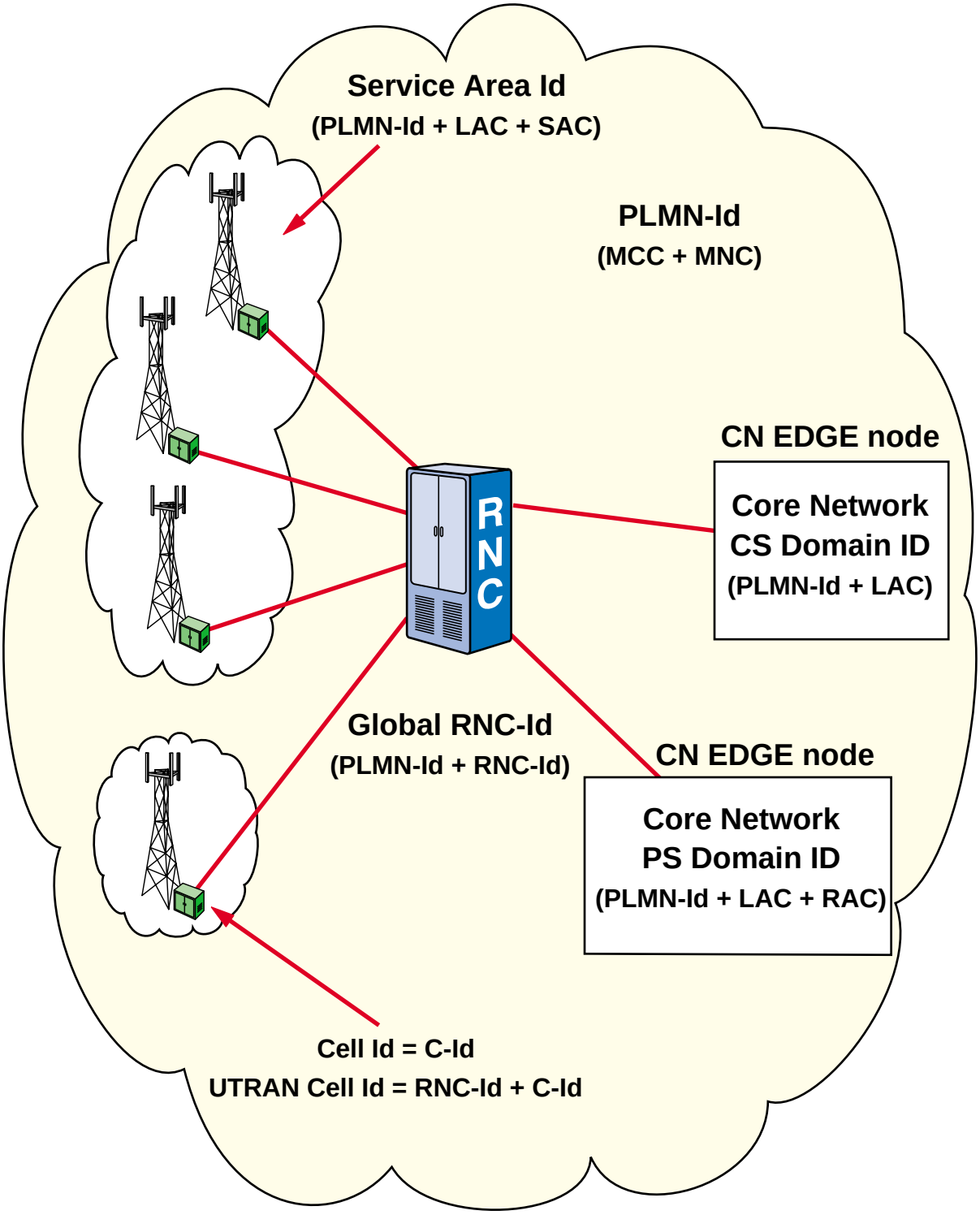


Figure 7
UTRAN Identifiers

© wray castle limited

5.6 UE Identifiers

The UTRAN uses Radio Network Temporary Identities (RNTI) as UE identifiers. Four types of RNTI exist, as follows.

5.6.1 Serving RNC RNTI (s-RNTI)

The s-RNTI is allocated by the SRNC for all UEs having an RRC connection.

5.6.2 Drift RNC RNTI (d-RNTI)

The d-RNTI is allocated by the DRNC and identifies the UE in the DRNC. An SRNC knows the mapping between the s-RNTI and the d-RNTIs for a UE. The DRNC stores the s-RNTI and SRNC-Id related to the d-RNTI.

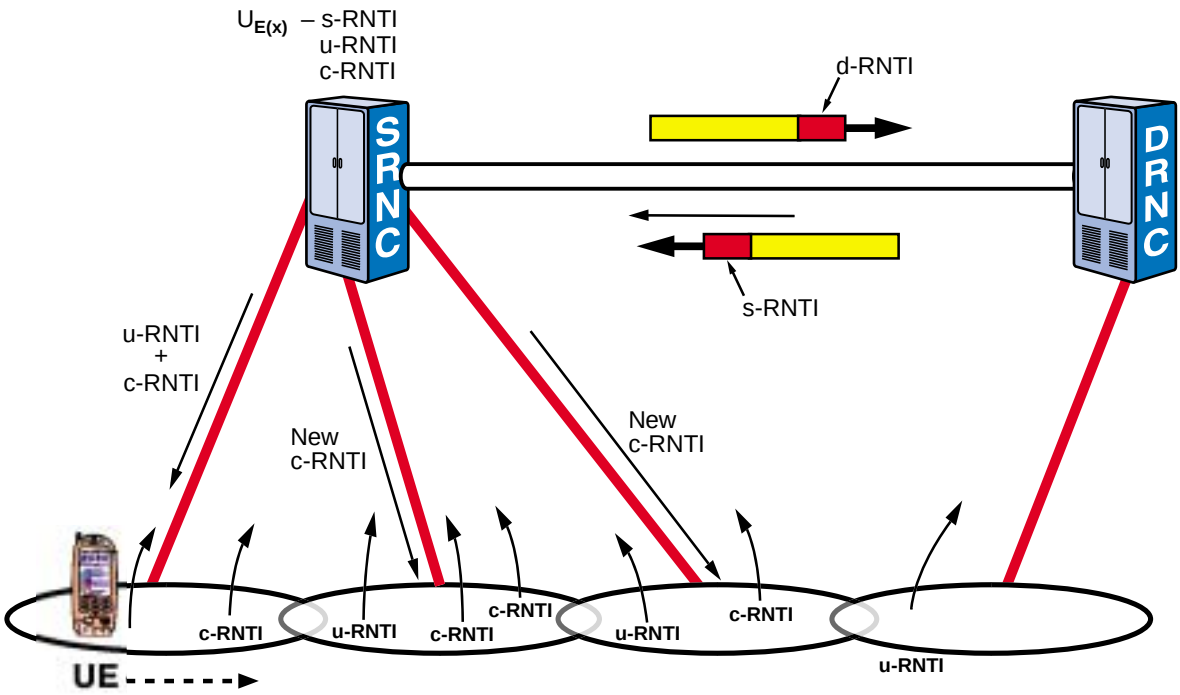
5.6.3 Cell RNTI (c-RNTI)

A UE accessing a new cell will be allocated a c-RNTI by the controlling RNC.

5.6.4 UTRAN RNTI (u-RNTI)

The u-RNTI is allocated to a UE with an RRC connection and uniquely identifies the UE within the UTRAN. The u-RNTI is made from a combination of RNC-Id and s-RNTI.

© wray castle limited



c-RNTI value only relevant within a cell
u-RNTI value relevant within the UTRAN – used for forwarding information to the SRNC

u-RNTI = SRNC-Id + s-RNTI

Figure 8
UE Identifiers

© wray castle limited

5.7 UE Core Network Identifiers

5.7.1 UE Core Network Permanent Identifier

The CN still recognizes the UE by its IMSI value, which is its permanent identifier. The make-up of the IMSI value has not changed, i.e.

MCC + MNC + MSID

5.7.2 UE Core Network Temporary Identifiers

The main provision for this type of security is the use of temporary identities. When attached to the CS domain of the CN, the user should be allocated a Temporary Mobile Subscriber Identity (TMSI). When attached to the PS domain of the CN, the user should be allocated a Packet Temporary Mobile Subscriber Identity (P-TMSI). It is possible for a user to possess TMSI and P-TMSI simultaneously.

To ensure an effective level of security for the use of temporary identities, they should be changed regularly.

In addition, it is recommended that any messages carried over the air interface are ciphered if they could compromise the user's permanent identity.

5.7.3 Allocation of TMSI/P-TMSI

Temporary identities are allocated by the CN entities VLR or SGSN and they are applicable within the areas controlled by those entities. Thus a TMSI/P-TMSI has local significance within an LA or an RA in which the user is registered. If the user moves into a new area, the TMSI/P-TMSI is presented to the CN along with the LA or RAI in which it was allocated. This enables the permanent identity of the user to be derived within the CN domain.

© wray castle limited

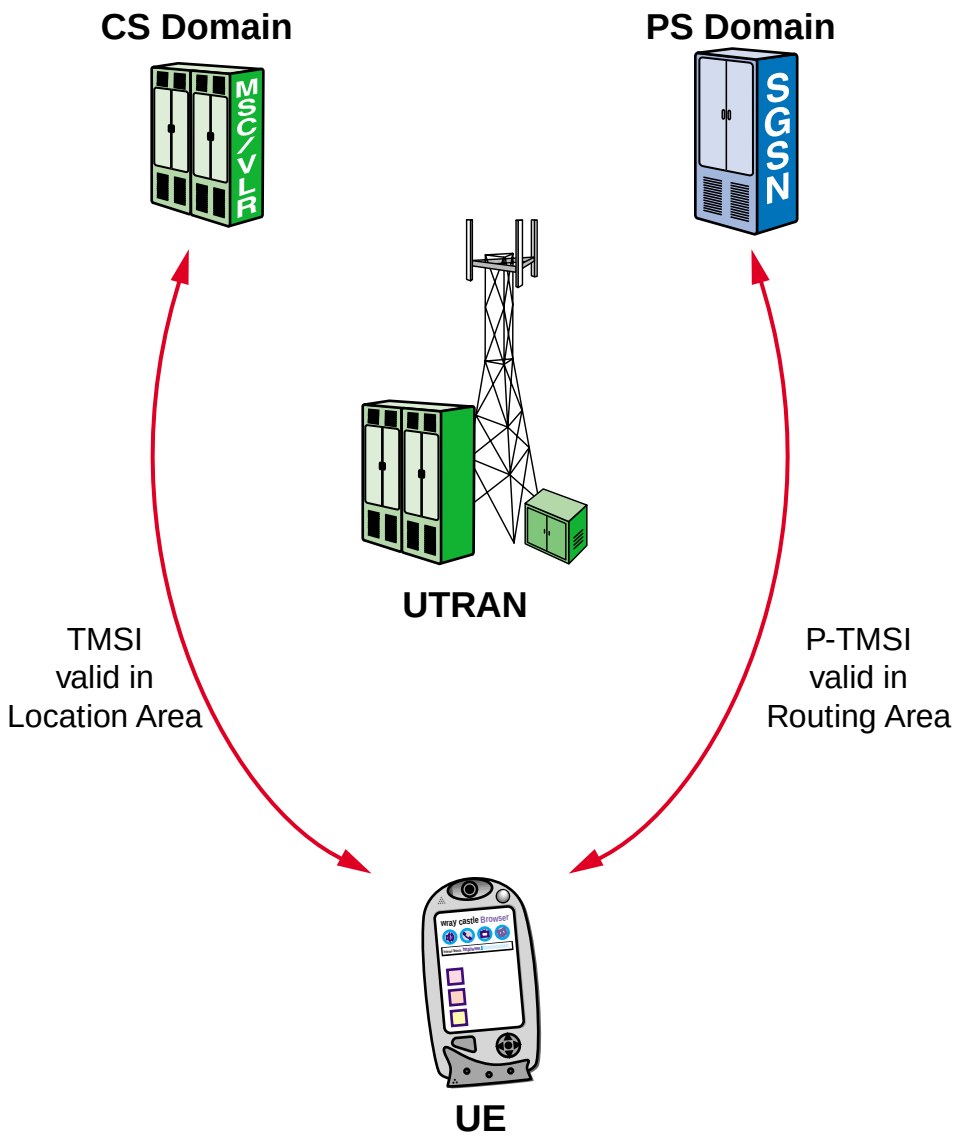


Figure 9
User Identity Confidentiality

© wray castle limited

© wray castle limited

SECTION 2

UTRAN AREAS AND ACCESS

© wray castle limited

LESSON 1

SYSTEM AREAS AND UE STATES

© wray castle limited

LESSON CONTENTS

1 UMTS System Areas **2.1.1**
1.1 Location Area (LA) 2.1.1
1.2 Routing Area (RA) 2.1.1
1.3 UTRAN Registration Area (URA) 2.1.1

2 UE Service States **2.1.3**
2.1 Introduction 2.1.3
2.2 Detached State 2.1.3
2.3 UTRAN Idle State 2.1.3
2.4 UTRAN Connected State 2.1.3

3 Idle Mode Procedures **2.1.5**
3.1 Aims for Idle Mode 2.1.5
3.2 General Idle Mode Activity 2.1.5
3.3 PLMN Types 2.1.7
3.4 PLMN Selection Considerations 2.1.7
3.5 Cell Selection 2.1.7

4 System Access Control **2.1.9**
4.1 Admission Control 2.1.9
4.2 Congestion Control 2.1.9
4.3 System Information Messages 2.1.9

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- define the following UMTS system areas:
  - Location Area (LA)
  - Routing Area (RA)
  - UTRAN Registration Area (URA)
- describe the three basic UE states:
  - detached state
  - UTRAN idle
  - UTRAN connected
- identify UE idle mode procedures
- describe the methods used to control access to the system

© wray castle limited

1 UMTS SYSTEM AREAS

In order that a UE may be paged, it is necessary for the CN to keep a record of the UE's approximate location. The location information available depends on the current service state of the UE and on the CN domain in which it is registered. This may be the CS domain, the PS domain, or both.

1.1 Location Area (LA)

A UE which has registered on the CS domain will report its position in terms of LA. There is no fixed size for an LA, but it would typically correspond to a fairly large number of cells. Location Area Identities (LAIs) are broadcast in each cell's system information. As the UE moves through the system in idle mode it will report changes in LA, which will be stored in the VLR.

1.2 Routing Area (RA)

A UE which is registered on the PS domain will report its position in terms of RA. This is operated in a similar way to the LA, but there is no requirement for RAs and LAs to correspond. UEs in both idle mode and connected mode will monitor Routing Area Identities (RAI) and report changes, which will be stored in the SGSN.

1.3 UTRAN Registration Area (URA)

This area within the network is only used when the UE has established a signalling and/or traffic connection with the UTRAN. A URA is always a subset of an RA and as such is only relevant to the PS mode of operation. The URA for the UE is tracked and used by the RNC; it is not associated with the CN.

© wray castle limited

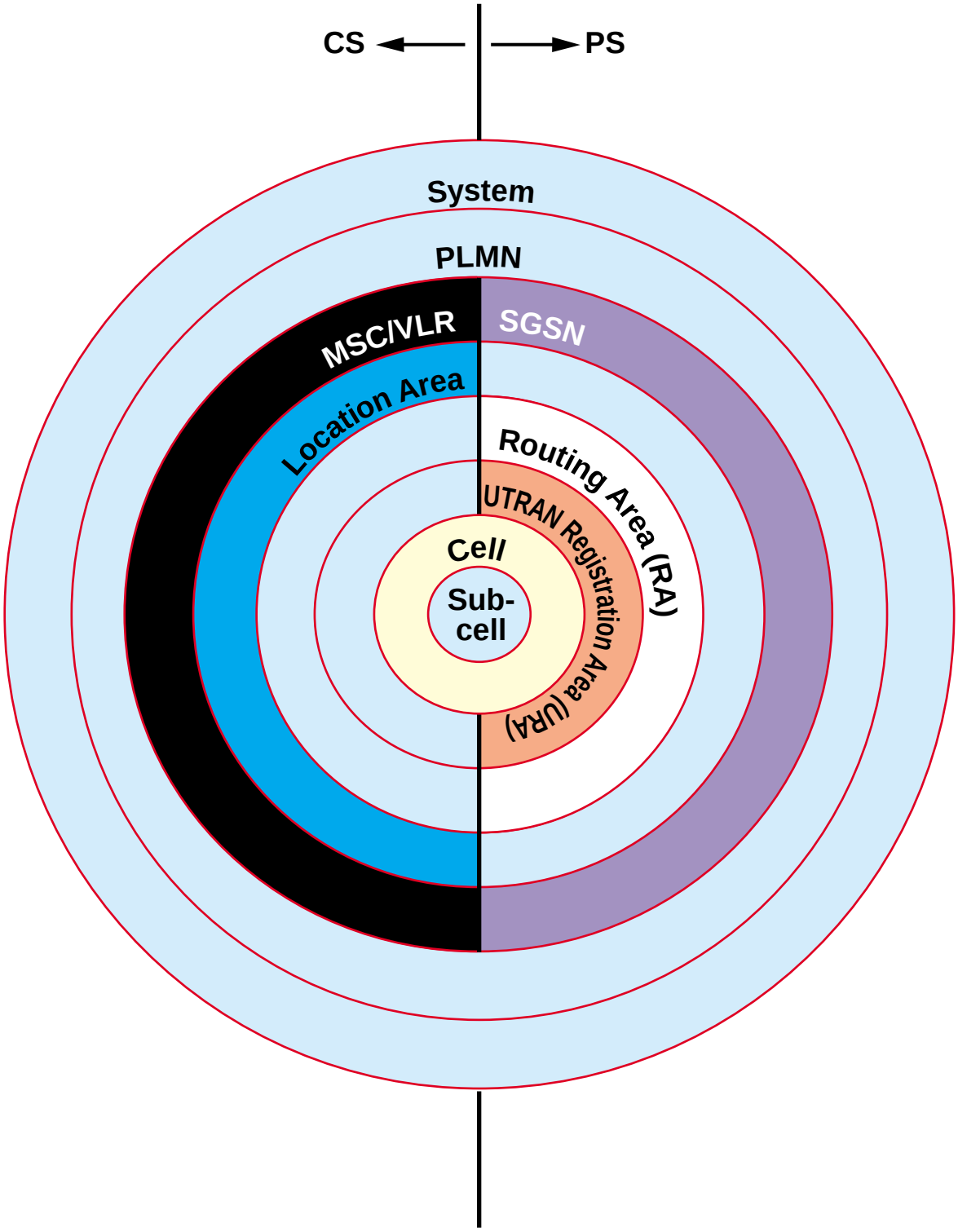


Figure 1
UMTS System Areas

© wray castle limited

2 UE SERVICE STATES

2.1 Introduction

The UE operates in one of three basic states:

- detached
- UTRAN idle
- UTRAN connected

These service states are applicable to both CS operation and PS operation. But for the connected state, UE activity varies slightly for the two types of service.

2.2 Detached State

In this state, the UE is not registered on the network; it is not performing LA updates or RA updates. The network cannot contact it for either CS- or PS-related services.

2.3 UTRAN Idle State

In this state, the UE is registered on the network; it will be performing both LA updates and RA updates. These updates will be triggered by boundary crossings and by the periodic timers. The UE can be paged for CS and PS services.

2.4 UTRAN Connected State

The behaviour of the UE in the connected state is different for the CS and PS domains. In both cases, ‘connected mode’ means that the UE has established a signalling link with the CN for either CS or PS services.

In the CELL_DCH state a UE has a UL and DL dedicated physical channel.

In the CELL_FACH state no dedicated physical channel is allocated. The UE continuously monitors a FACH in the DL.

In the CELL_PCH state no dedicated physical channel is allocated to the UE. The UE monitors the PCH.

In the URA_PCH state no dedicated channel is allocated to the UE. The location of the UE is known on the URA. The UE monitors the PCH.

© wray castle limited

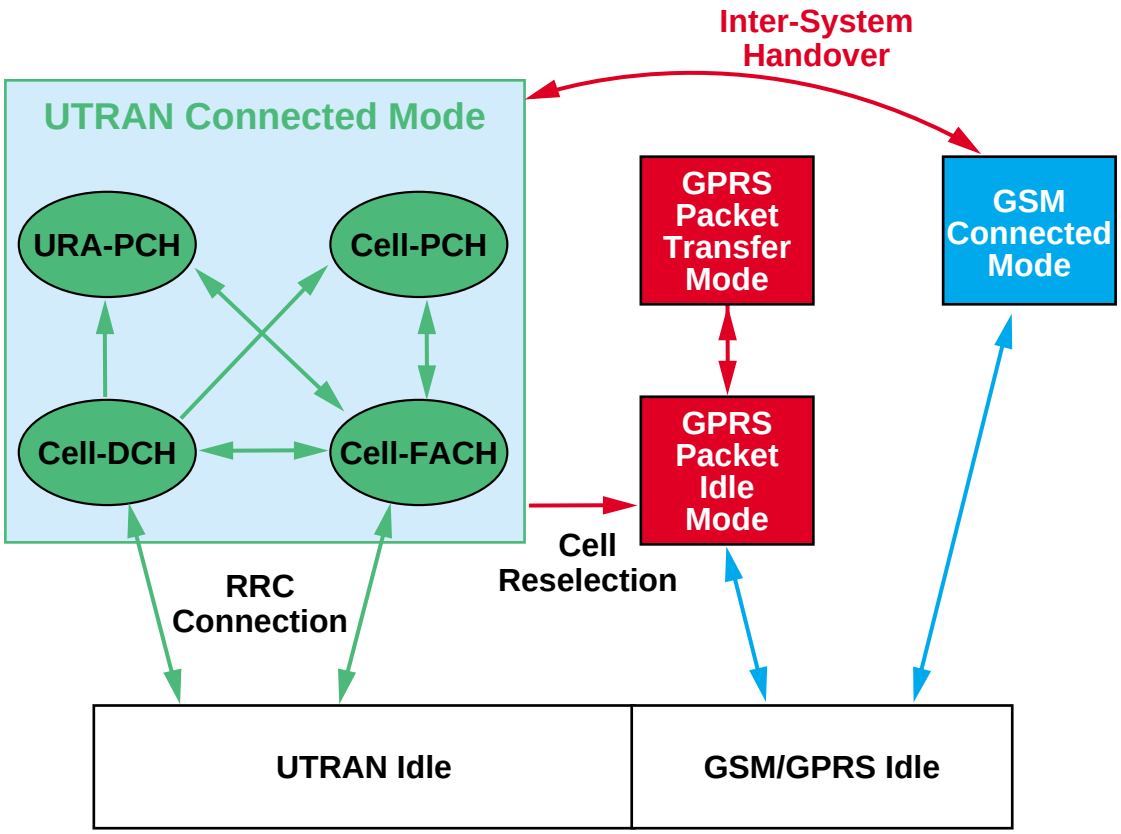


Figure 2
UE Service States

© wray castle limited

3 IDLE MODE PROCEDURES

3.1 Aims for Idle Mode

Idle mode represents a state of operation for the UE where it has successfully performed the following:

- PLMN selection
- cell selection
- location registration

Once in idle mode, the UE will continue to reassess the suitability of its serving cell and, in some circumstances, its serving network. In order to do this it will implement cell reselection procedures and PLMN reselection procedures.

3.2 General Idle Mode Activity

A UE in idle mode will be monitoring its current serving cell in terms of radio performance and signalling information. The radio performance measurements are done on the basis of a quality measure. This is an assessment of radio signal strength and interference level, and it will be made for both the serving cell and its neighbours. The aim will be to ensure that the UE is always served by the cell most likely to give the most reliable service should information transfer of any kind be required.

The UE will also be monitoring two key types of signalling from the serving cell: system information messages, and paging or notification messages. System information messages convey all the cell and system parameters. The UE will record changes in these parameters that may affect the service level provided by the cell, or access rights to the cell. Changes in these parameters could provoke a cell reselection, or a PLMN reselection. Paging or notification messages will result in connection establishment.

All of these procedures are performed through communication between the Access Stratum (AS) and the Non Access Stratum (NAS). In general, instructions are sent from the NAS to the AS; the AS then performs the requested procedure and returns a result to the NAS. This process is summarized in Figure 3.

© wray castle limited

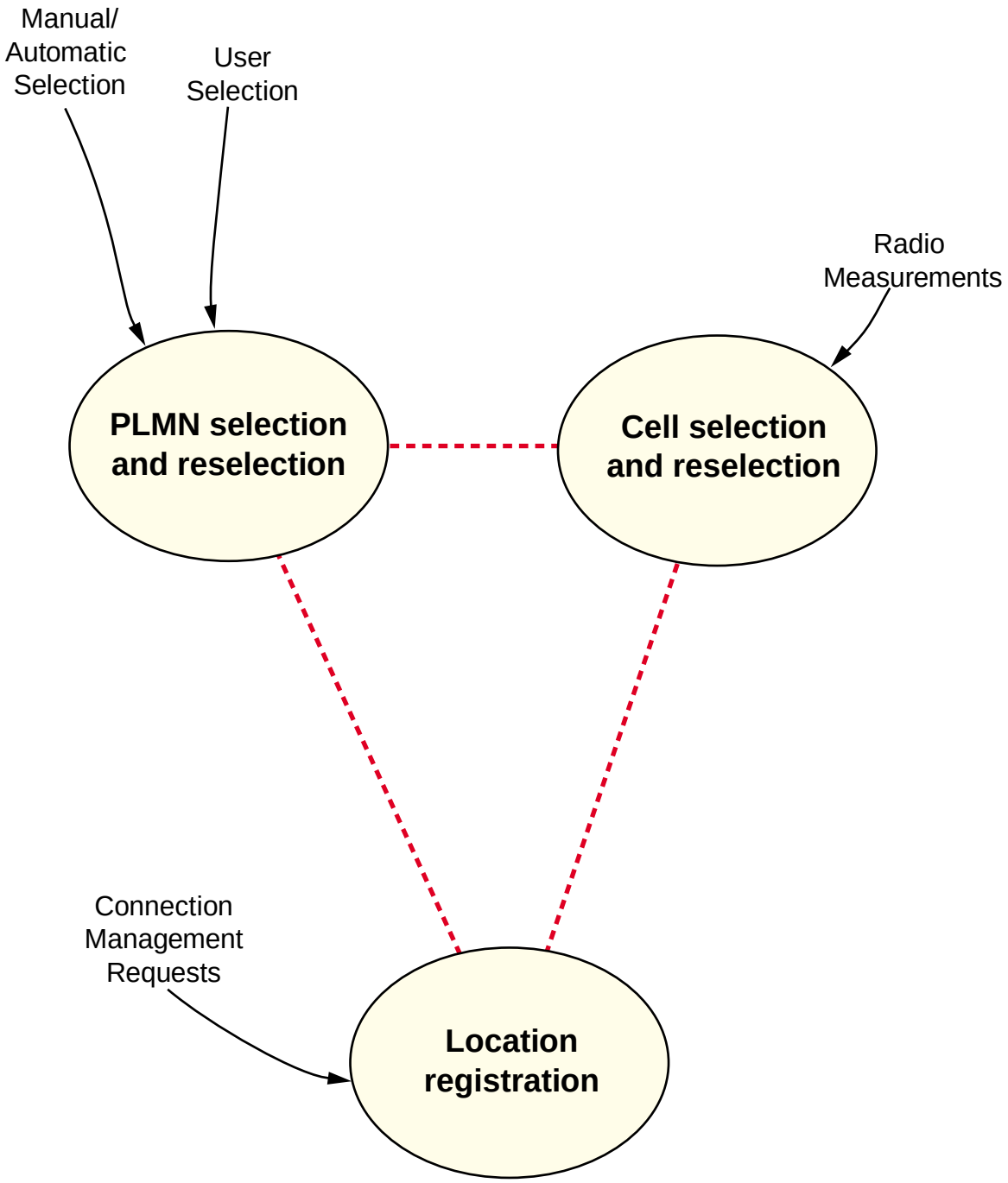


Figure 3
Summary of Idle Mode Process

© wray castle limited

3.3 PLMN Types

A UE may be capable of accessing more than one type of PLMN. This implies the ability to access both GSM-MAP-based CNs or ANSI-41-based CNs. These two types of CN use different identity formats and the NAS should be able to recognize both.

3.4 PLMN Selection Considerations

PLMN selection is initiated by the NAS, and there are several scenarios for this. It may provide an indication to search for a particular PLMN, or to perform a general search for any available PLMN. A specifically requested PLMN will be the one with the highest priority, which may be because it is the Home PLMN (HPLMN) or because it was the last one stored before the previous power-off. The AS will attempt to find a suitable cell belonging to the requested PLMN; if successful, it will report this to the NAS. If a suitable cell belonging to the requested PLMN cannot be found, then the AS will return a list of any other available PLMNs.

The most likely cause for a search of available PLMNs is in response to a user request. In this case, the AS will again return a list of available PLMNs. If a higher-priority PLMN to the one currently selected has been found, then the NAS may instruct the AS to reselect it. Prioritization may be based on service level provision or on PLMN identity; i.e. it may be the HPLMN.

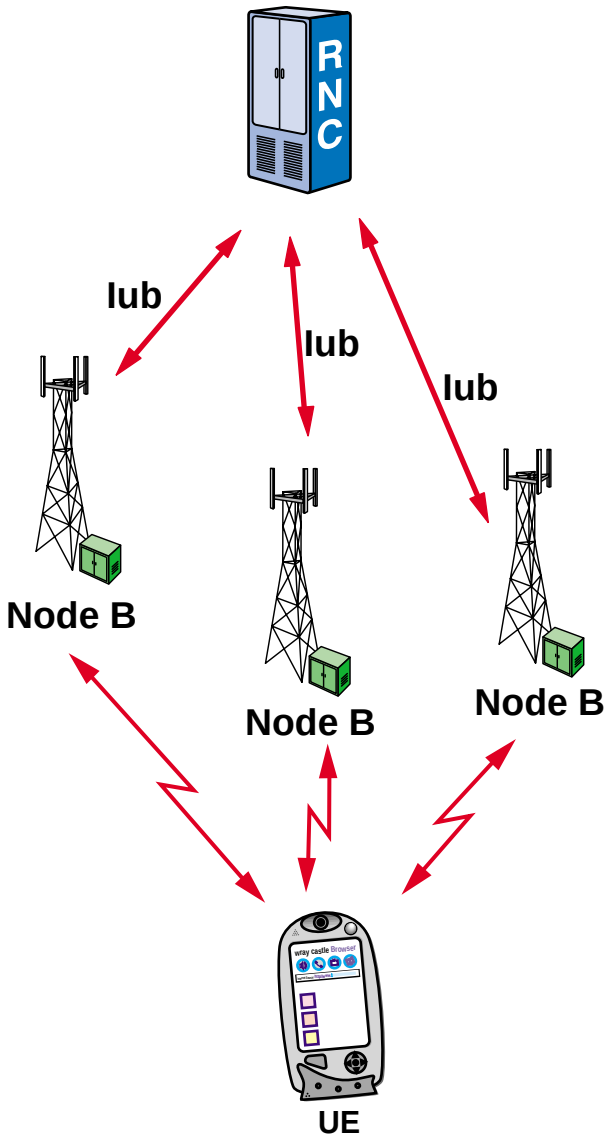
3.5 Cell Selection

When a required PLMN is indicated, the UE will attempt to find a suitable cell to camp on and through which it will be able to perform location registration. There are two possibilities for the selection procedure, either initial cell selection or stored information cell selection.

For initial cell selection, the UE has no prior knowledge of which radio channels the PLMN is using. The UE will therefore scan all the channels within the UMTS band. On each channel the UE will scan for available cells, looking for those that belong to the required PLMN. Once a radio carrier belonging to the required PLMN is found, the UE will use the cell selection quality criteria to choose the most suitable cell.

For stored information cell selection, the UE will use previously stored information on carrier frequencies used by the required PLMN. It may also have stored information on scrambling codes used.

© wray castle limited



- **Initial Cell Selection**
- **Stored Information Cell Selection**

Figure 4
Cell Selection

© wray castle limited

4 SYSTEM ACCESS CONTROL

System access control enables the user to connect to the UMTS network in order to use UMTS services. Access control can be broken down into three main parts: admission control, congestion control and system information messages.

4.1 Admission Control

The admission control function is located at the CRNC or SRNC, depending on whether the admission function is being performed on common channels or dedicated channels. New calls increase the interference level for all other calls. This affects the quality of all current calls. Admission control provides the ability to admit or deny communication links to new users either by changing parameters in system information messages or by its ability to differentiate user channels. The decisions are based on QoS requirements, interference, current load conditions and resource measurements.

4.2 Congestion Control

This will be a management element which gathers information concerning network load. When the network becomes congested, i.e. running out of resources, it is able to revert the system to a stable state.

4.3 System Information Messages

System information messages provide the UE with information about the cell configuration, network information and access power information. Therefore, this enables the system to control some UE operations/procedures.

© wray castle limited

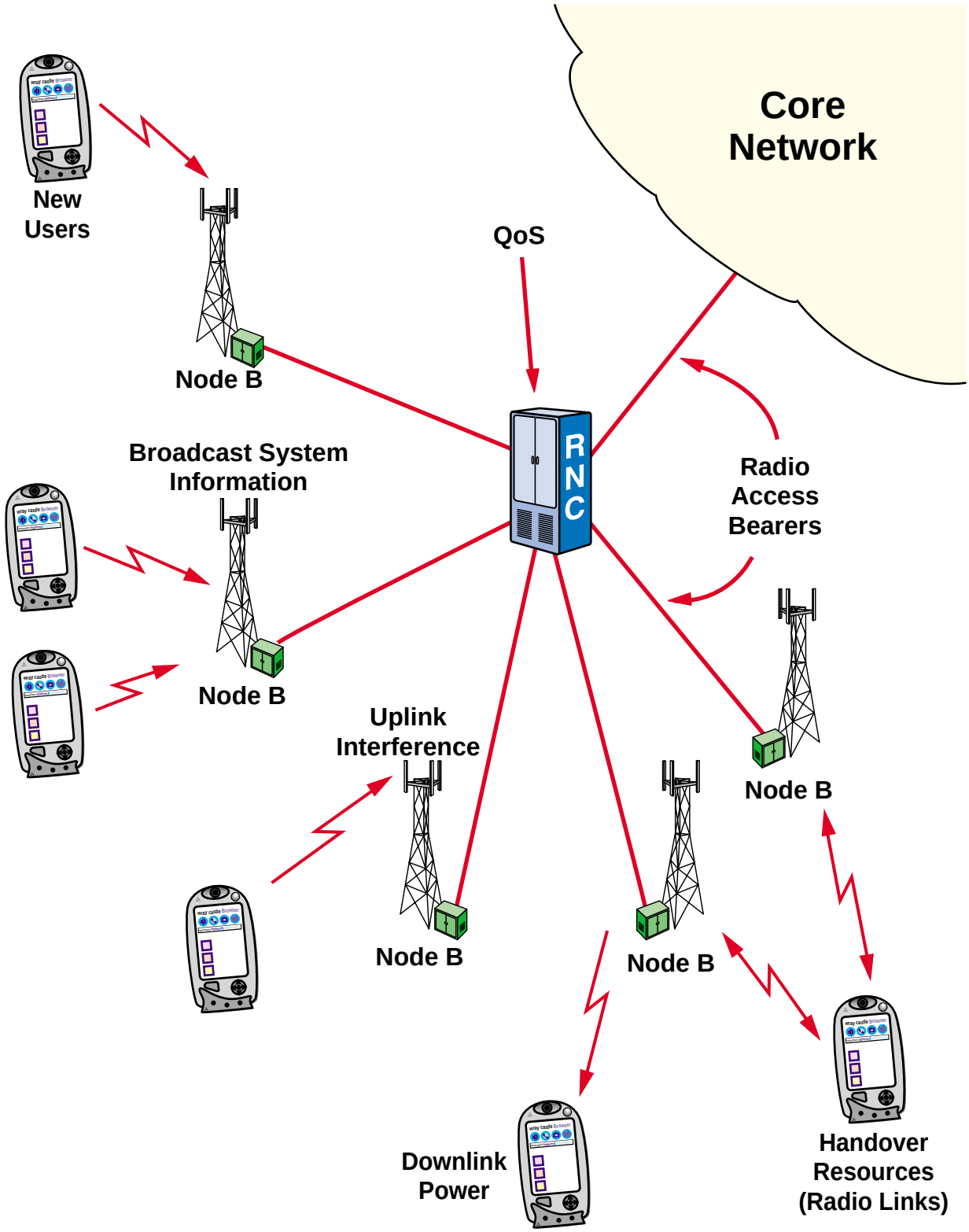


Figure 5
System Access Control

© wray castle limited

© wray castle limited

LESSON 2

UE SYNCHRONIZATION

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Initial Synchronization 2.2.1
1.1 Requirements for Synchronization 2.2.1
1.2 Synchronization Procedure 2.2.3
1.3 Synchronization Example 2.2.5
1.4 Broadcast of System Information 2.2.7
1.5 Overview of SIB Contents 2.2.9

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe how a UE initially synchronizes with the system
- identify the types of code employed during initial synchronization
- describe the organization and transmission of system information messages and the contents of System Information Blocks (SIBs)

1 INITIAL SYNCHRONIZATION

1.1 Requirements for Synchronization

Before the UE registers on the system, it must select a suitable PLMN, and within that PLMN, a suitable code. In order that these selections can be made, the UE must synchronize to and read information from potential candidate cells.

Once synchronized the UE will be in a position to read system information carried by the Broadcast Control Channel (BCCH) in the PCCPCH, and paging or resource allocations in the SCCPCH(s).

The SCH is used by the UE for initial cell synchronization. It enables the UE to determine a cell's scrambling code group and to gain slot and frame alignment. However, for this to be successful the UE must possess knowledge of the codes listed in Figure 1.

© wray castle limited

Code	Comment
Primary Synchronization Code (Hierarchical Golay)	**One code unique to the whole of UMTS of length 256 chips**
Secondary Synchronization Code (Hierarchical Golay)	**16 codes of length 256 chips**
Primary Cell Scrambling Code (Gold Codes)	**512 codes organized into 64 groups of 8**

Figure 1

Codes Known to the UE and Employed in Initial Synchronization

© wray castle limited

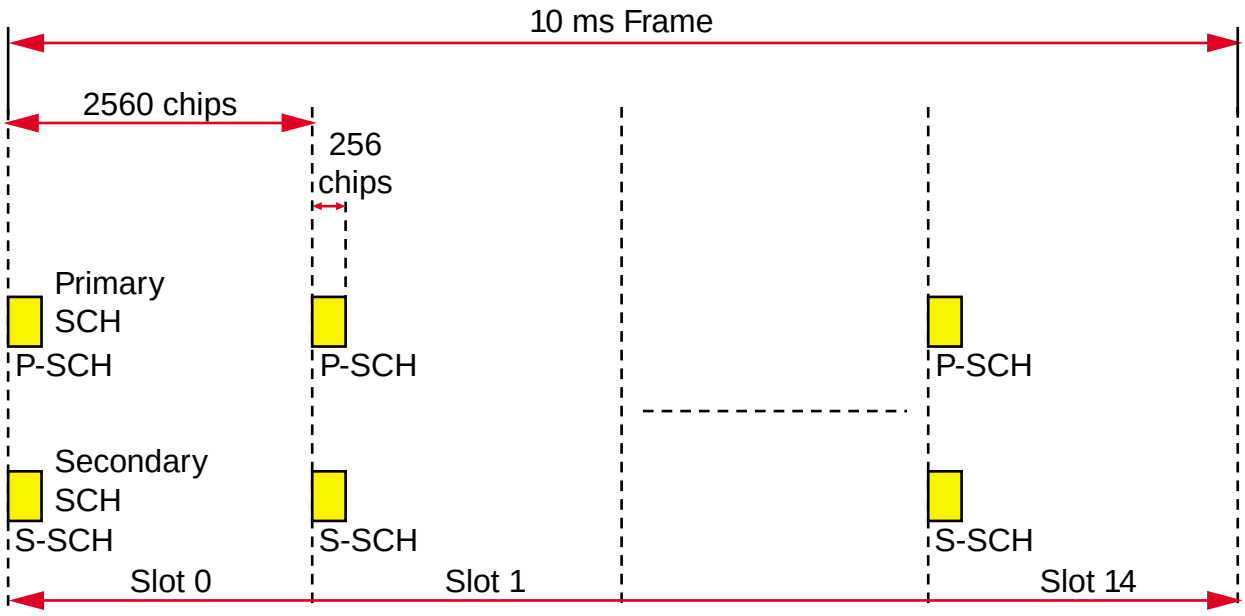
1.2 Synchronization Procedure

The primary part of the SCH consists of a hierarchical Golay code of length 256 chips. This primary synchronization code is the same for every cell in the system. It is transmitted at the system chip rate and time-aligned with the start of each slot (it will, therefore, occupy the first tenth of the slot period). This gives the mobile station slot alignment.

The secondary part of the SCH is transmitted over the top of the primary part and in each slot will be one of 16 different codes of length 256 chips. Each code is formed from the combination of Golay and Hadamard codes. Codes from the set of 16 are sent in one of 64 different predetermined sequences of length 15. This gives the mobile station the cell's scrambling code group. The sequences of Gold codes are time-aligned with the start of each frame, and the sequences are chosen so that they are unique in any cyclic shift. This gives the mobile station frame alignment.

Each cell scrambling code group identifies eight of the possible primary scrambling codes from the group of 64. The UE identifies the correct primary scrambling code by cross-correlating the received signal on the CPICH with all eight scrambling codes belonging to the group. Once the correct primary scrambling code has been detected it can be used to decode the BCCH information on the primary CCPCH. Any other codes required will be indicated in the BCCH.

© wray castle limited



P-SCH – Primary Synchronization Code

S-SCH – Secondary Synchronization Code, one of 16 codes in a 15-code sequence from a set of 64

Figure 2
Structure of the SCH

© wray castle limited

1.3 Synchronization Example

With reference to Figure 3 the UE has successfully obtained slot timing of the target cell correlating the received signal from the P-SCH. Thus, it now knows where a slot begins but not the slot number or radio frame boundary.

The UE correlates the signal received on the S-SCH in order to obtain the scrambling code group number for that particular cell, in this case code group number 12. Once the UE has successfully decoded 15 successive Secondary Synchronization Codes (SSCs) it becomes frame synchronized and in possession of the scrambling code group for that cell.

All eight possible primary scrambling codes are correlated with the received signal in order to identify the correct one for that target cell, in this case primary scrambling code 4.

© wray castle limited

Scrambling Code Group	slot number														
	#0	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14
Group 0	1	1	2	8	9	10	15	8	10	16	2	7	15	7	16
Group 1	1	1	5	16	7	3	14	16	3	10	5	12	14	12	10
Group 2	1	2	1	15	5	5	12	16	6	11	2	16	11	15	12
Group 3	1	2	3	1	8	6	5	2	5	8	4	4	6	3	7
Group 4	1	2	16	6	6	11	15	5	12	1	15	12	16	11	2
Group 5	1	3	4	7	4	1	5	5	3	6	2	8	7	6	8
Group 6	1	5	11	3	4	10	9	2	11	2	10	12	12	9	3
Group 7	1	6	6	6	14	9	10	2	13	9	2	5	14	1	13
Group 8	1	6	10	10	4	11	7	13	16	11	13	6	4	1	16
Group 9	1	6	13	2	14	2	6	5	5	13	10	9	1	14	10
Group 10	1	7	8	5	7	2	4	3	8	3	2	6	6	4	5
Group 11	1	7	10	9	16	7	9	15	1	8	16	8	15	2	2
Group 12	**1**	**8**	**12**	**10**	**9**	**4**	**13**	**16**	**5**	**1**	**13**	**5**	**12**	**4**	**8**
Group 13	1	8	14	15	14	1	15	15	8	5	11	4	10	5	4
Group 14	1	9	2	6	15	16	10	7	8	1	10	8	2	16	9
Group 15	1	9	15	11	16	2	13	14	10	11	7	4	5	12	3
Group 16	1	10	9	4	15	7	6	4	16	5	2	12	13	3	14
Group 62	9	11	12	15	12	9	13	13	11	14	10	16	15	14	16
Group 63	9	12	10	15	13	14	9	14	15	11	11	13	12	16	10

Figure 3
Synchronization Example

	Scrambling Code Group															
	#0	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
3	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144
4	193	194	195	196	197	198	199	200	201	202	203	204	**205**	206	207	208
5	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272
6	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336
7	385	366	387	388	389	390	391	392	393	394	395	396	397	398	399	400
8	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464

	Scrambling Code Group															
	#16	#17	#18	#19	#20	#21	#22	#23	#24	#25	#26	#27	#28	#29	#30	#31
1	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
3	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
4	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224
5	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288
6	337	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353
7	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416
8	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480

	Scrambling Code Group															
	#32	#33	#34	#35	#36	#37	#38	#39	#40	#41	#42	#43	#44	#45	#46	#47
1	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
2	97	98	99	100	101	102	103	104	105	106	107	109	110	111	112	113
3	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176
4	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
5	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304
6	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368
7	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432
8	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496

	Scrambling Code Group															
	#48	#49	#50	#51	#52	#53	#54	#55	#56	#57	#58	#59	#60	#61	#62	#63
1	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
2	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
3	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192
4	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256
5	305	306	307	308	309	310	311	311	312	313	314	315	316	317	318	319
6	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384
7	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	478
8	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512

© wray castle limited

1.4 Broadcast of System Information

This is a point-to-multipoint service which broadcasts a large number of system information parameters that must be broadcast to UEs in a cell. Some elements are static, some dynamic; others may need frequent retransmission, and some not.

In order to provide this flexibility, information elements are hierarchically organized into a Master Information Block (MIB), 18 System Information Blocks (SIBs) and up to two Scheduling Blocks (SB).

The MIB indicates the identity and schedule of a number of SIBs which contain the actual system information. The MIB may also indicate the scheduling of SBs, which give references and scheduling information for additional SIBs.

Once a UE has attained the scheduling information of the various SIBs it can conserve power by ‘waking up’ to receive only the SIBs it requires and omit reception of the rest.

© wray castle limited

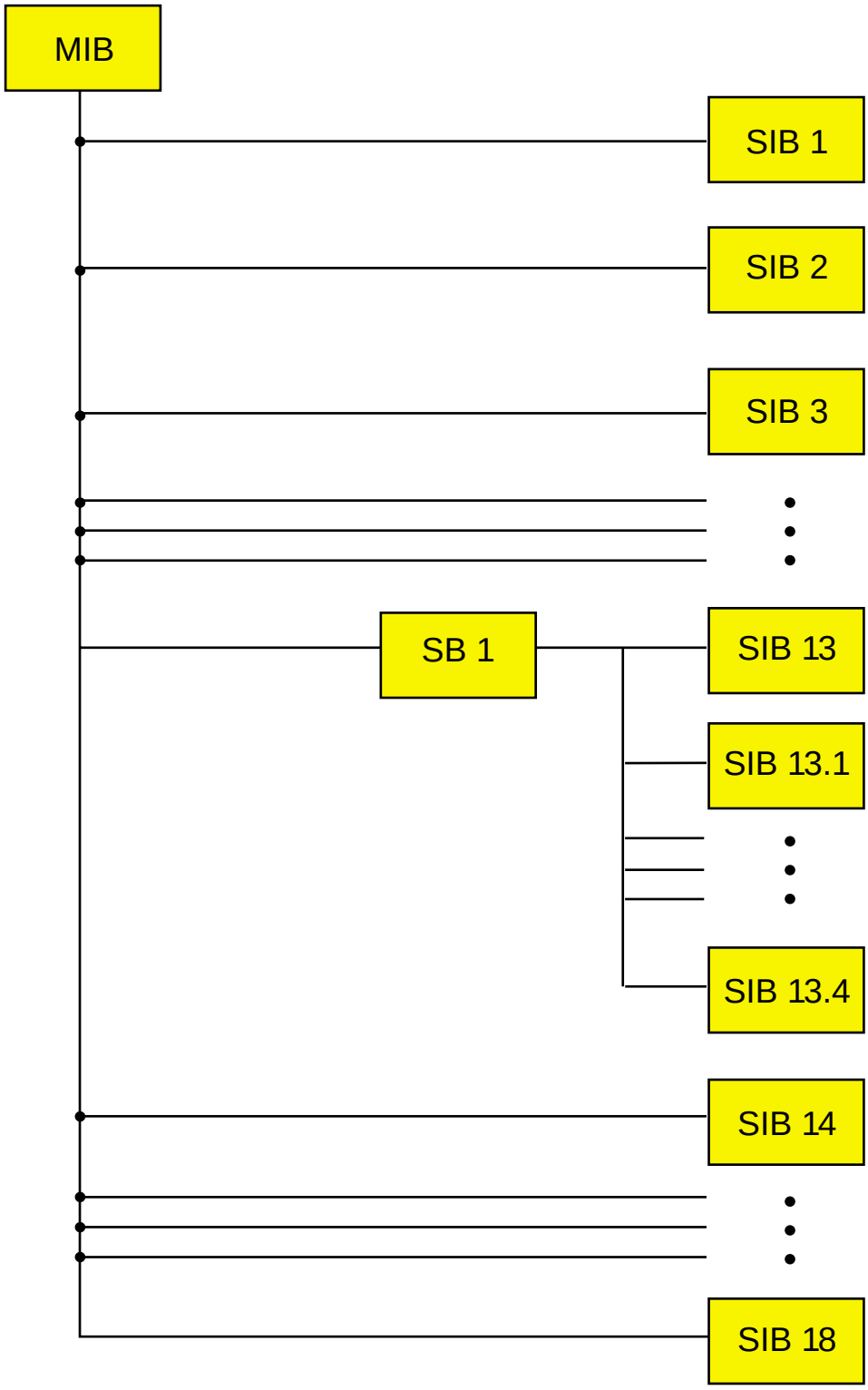


Figure 4
Example SIB Scheduling Tree

© wray castle limited

1.5 Overview of SIB Contents

The following is a brief description of the contents of the eighteen SIBs currently specified in Release 99 of UMTS.

For a more detailed description of each of the SIBs, consult the 3rd Generation Partnership Project (3GPP) TS 25.331 RRC Protocol Specification.

MIB : Contains PLMN identity and GSM or ANSI-41 Core Network and references to other SIBs.

SIB 1: Contains Core Network system information NAS and information pertaining to UE timers and counters to be used in idle mode and cell-DCH state only.

SIB 2: Contains the URA identity and information for periodic cell and URA update. It also includes the UE timers and counters to be used in connected mode.

SIB 3: Contains parameters for cell selection and reselection (to be used by cell selection and reselection algorithm) and optionally contains parameters about when to perform various measurements.

SIB 4: Contains further parameters for cell selection and reselection to be used in connected mode only.

SIB 5: Contains parameters for the configuration of the common physical channels in the cell which paging block to monitor for DRX. Also contains ASC for RACH access.

SIB 6: Contains parameters for the configuration of the common and shared physical channels to be used in connected mode only.

SIB 7: Contains the fast changing parameters such as UL interference level and dynamic persistence levels for RACHs.

SIB 8: Contains static CPCH information, FDD only, to be used in connected mode only.

SIB 9: Contains fast changing CPCH information such as dynamic persistence levels.

© wray castle limited

SIB 10: Contains information to be used by UEs having their DCH controlled by a Dynamic Resource Allocation Control (DRAC). FDD only.

SIB 11: Contains measurement control information and the neighbour cell list.

SIB 12: Measurement control information to be used in connected mode.

SIB 13: Contains ANSI-41 system information, to be used only when CN of the system is ANSI-41.

SIB 14: Contains parameters for common and dedicated physical channel uplink outer loop power control information to be used in both idle and connected mode for TDD only.

SIB 15: Contains information useful for LCS. In particular it allows the UE based method to perform localization without dedicated signalling.

SIB 16: Radio bearer, transport channel and physical channel parameters to be stored by UE in idle and connected mode for use during handover to the UTRAN.

SIB 17: Contains fast changing parameters for the configuration of the shared physical channels. Used in connected mode for TDD only.

SIB 18: Contains the PLMN identities of neighbour cells.

© wray castle limited

© wray castle limited

SECTION 3

GENERAL UTRAN PROTOCOL STRUCTURE

© wray castle limited

LESSON 1

INTRODUCTION TO UTRAN PROTOCOLS

© wray castle limited

LESSON CONTENTS

1	**General UTRAN Protocol Structure**		**3.1.1**
	1.1	Data Bearer	3.1.3
	1.2	Signalling Bearer	3.1.3
	1.3	Application Protocol	3.1.3
	1.4	Data Protocol	3.1.3
2	**Radio Bearer (RB) Control Procedures**		**3.1.5**
	2.1	Signalling Radio Bearers (SRB)	3.1.5
	2.2	Radio Access Bearers (RAB)	3.1.7
	2.3	The GSM/EDGE Radio Access Network (GERAN)	3.1.9
	2.4	General Protocol Architecture	3.1.11
	2.5	The User Plane	3.1.11
	2.6	The Control Plane	3.1.11
3	**The Non-Access Stratum (NAS)**		**3.1.13**
	3.1	Services Provided by the NAS	3.1.13
	3.2	NAS Control Plane	3.1.15
4	**The Access Stratum (AS)**		**3.1.17**
	4.1	Overall Aims	3.1.17
	4.2	AS Protocol Overview	3.1.19

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- state the principles of the general protocol architecture model for both the user plane and the control plane
- describe the general UTRAN protocol architecture

© wray castle limited

1 GENERAL UTRAN PROTOCOL STRUCTURE

The UTRAN protocols employ a common architecture on all three terrestrial interfaces Iub, Iur and Iu.

The protocol architecture is divided horizontally into two key layers. The upper part is referred to as the Radio Network Layer, and the lower part is referred to as the Transport Network Layer. The Radio Network Layer constitutes the source for data to be transferred across the interfaces, this data will be signalling or traffic. The Transport Network Layer provides the necessary transport mechanisms, based on Asynchronous Transfer Mode (ATM).

The protocol architecture is also divided vertically into three planes: the control plane, which handles control information pertaining to the radio interface protocols; the user plane, which handles user data; and a transport network control plane. A simplified diagram is shown in Figure 1b.

The control plane includes the application protocols, Radio Access Network Application Part (RANAP) on the Iu interface, Radio Network System Application Part (RNSAP) on the Iur interface and Node B Application Part (NBAP) on the Iub interface. Because this is external to the Transport Network Layer it is considered to be in the user plane of the Transport Network Layer.

The user plane includes the data stream(s) and the data bearer(s) for the data stream(s) which are characterized by one or more User Plane (UP) framing protocols specified for each interface. This is also external to the Transport Network Layer and is considered to be in the user plane of the transport network.

The Transport Network Control Plane includes Access Link Control Application Protocol (ALCAP) needed to establish, release and maintain point-to-point connections on the Iu-CS, Iub and Iur interfaces.

© wray castle limited

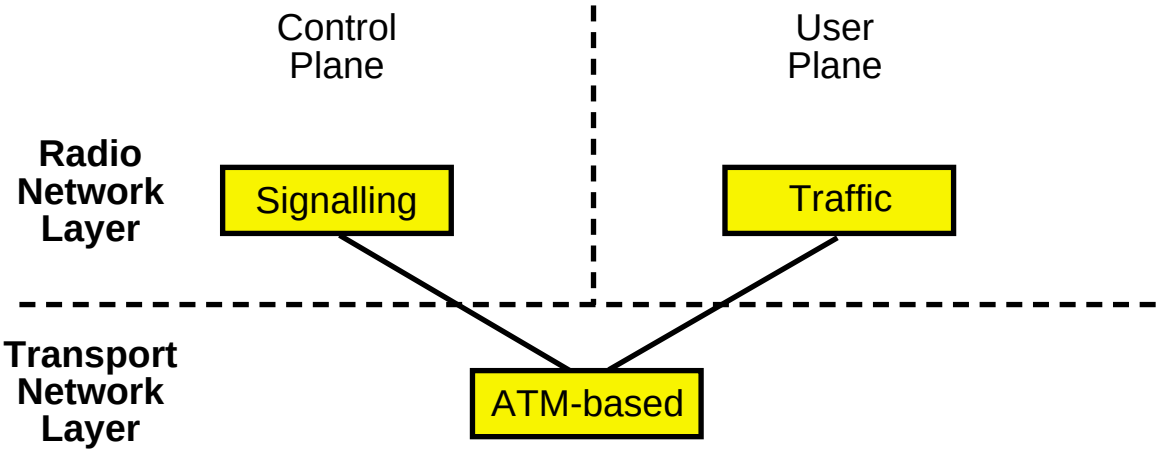


Figure 1a
Simplified UTRAN Protocol Structure

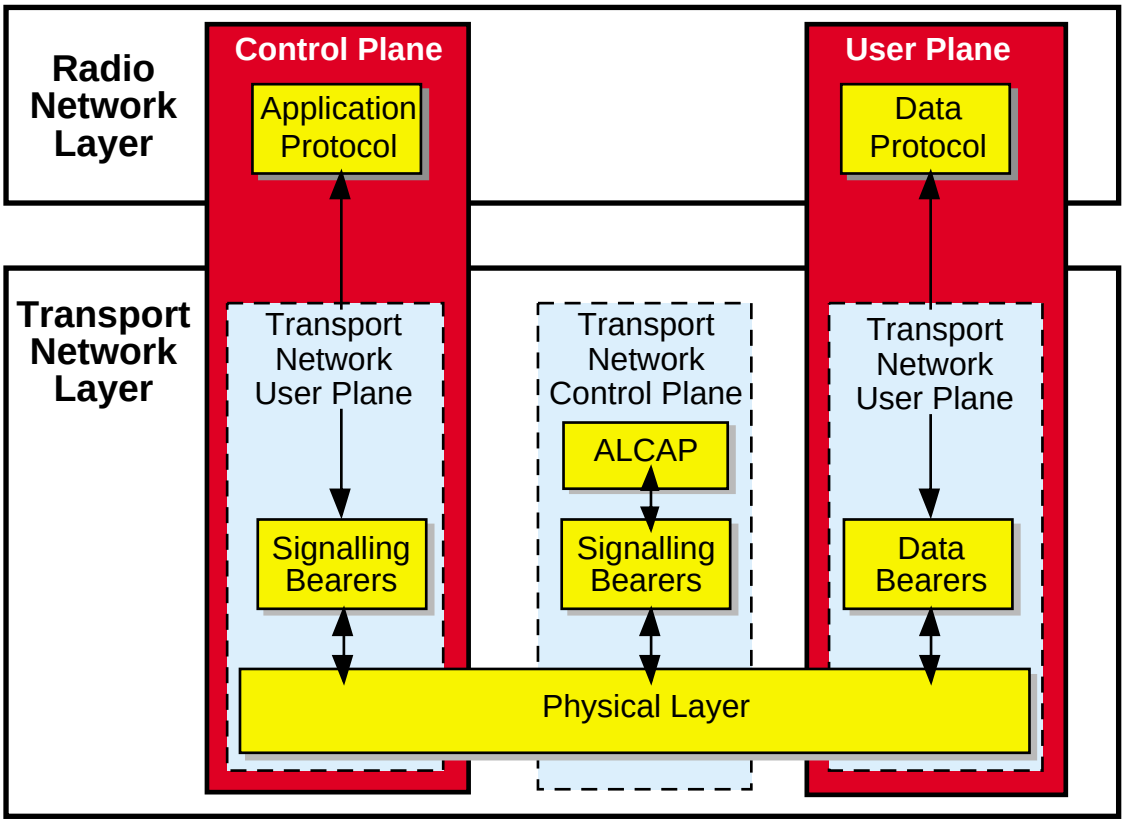


Figure 1b
UTRAN Protocol Structure

© wray castle limited

1.1 Data Bearer

This represents a pipe or connection used to carry user data from one node to another, user data being derived from the user plane in the UE in the form of voice, video, IP datagram etc. or from the user plane in the CN.

1.2 Signalling Bearer

This represents a pipe or connection dedicated to carry signalling information only from node to node. This can be used to carry user (UE) control/signalling information or nodal information, e.g. Node B to RNC from the control plane protocol.

1.3 Application Protocol

The application protocol will carry out specific services across the specific interface e.g. management of resources and nodal reconfiguration. It can also be used on certain interfaces to carry user (UE) control/signalling information, for example a RANAP message can carry information destined for a specific UE. RANAP is found on Iu-CS and Iu-PS.

1.4 Data Protocol

The data protocol can offer specific services of the user plane, dependent on the applications' QoS requirements (such as time, delay and bit rate) for voice, video, data and IP datagrams.

It can also indicate the rate of information flow when changed, for example different AMRs.

© wray castle limited

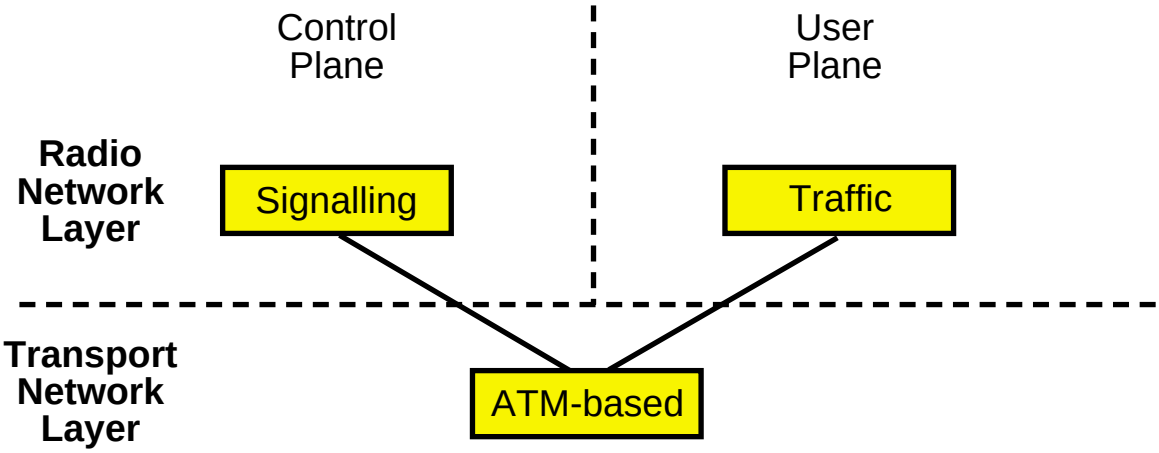


Figure 1a (repeated)
Simplified UTRAN Protocol Structure

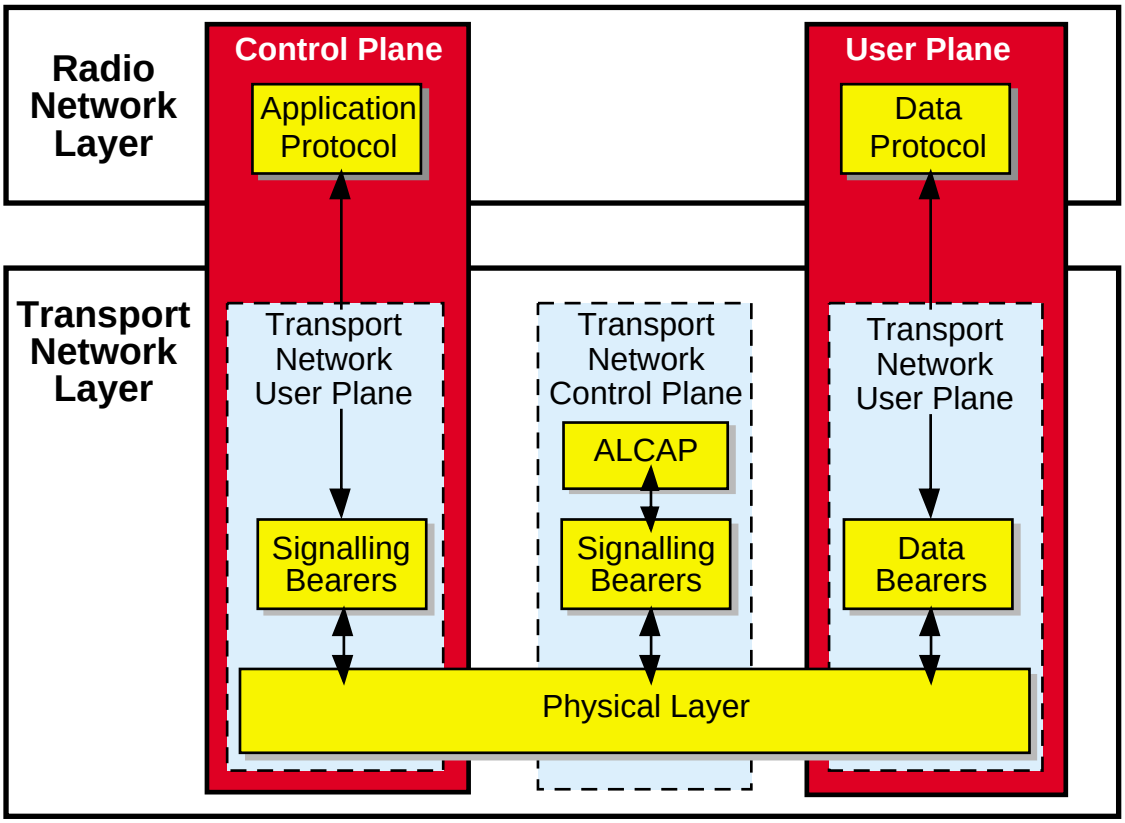


Figure 1b (repeated)
UTRAN Protocol Structure

© wray castle limited

2 RADIO BEARER (RB) CONTROL PROCEDURES

2.1 Signalling Radio Bearers (SRB)

Each connection to a UE requires the allocation of several Radio Bearers (RBs). Each RB represents the description of RLC and MAC functionality to be applied to information carried in that particular RB. RBs are required for both signalling and traffic transfer to and from a UE. The RBs used to carry signalling will be established as part of the RRC connection establishment procedure.

The RRC Connection Set-up message carries details of up to five RBs allocated for signalling between the UE and the UTRAN:

- RB0 – all messages using the CCCH
- RB1 – using the unacknowledged mode of RLC and DCCH
- RB2 – using the acknowledged mode of RLC and DCCH except direct transfer
- RB3 – used for direct transfer with the acknowledged mode of RLC and DCCH
- RB4 – optional, similar to RB3 but for lower-priority messages

© wray castle limited

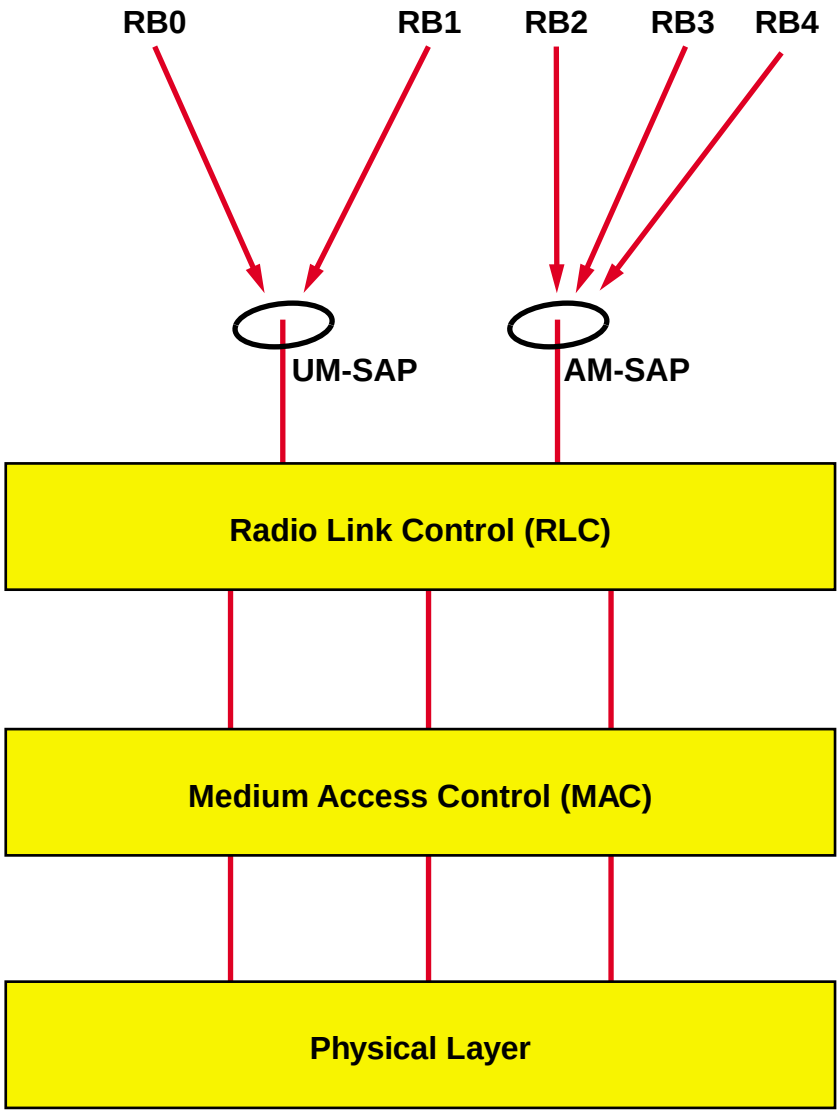


Figure 2
Signalling Radio Bearers (SRB)

© wray castle limited

2.2 Radio Access Bearers (RAB)

Radio Access Bearers (RABs) represent the service provided to higher layers in the user plane to transfer traffic data between the UE and the required CN domain. RLC MAC and the physical layer of the air interface handle the part of the RAB path between the UE and the UTRAN. Control of this resource and its provision in terms of RB is the responsibility of RRC.

Part of the measurement and reporting mechanism from the UE and the UTRAN lower layers informs RRC of traffic load. RRC will then assess traffic load and required QoS parameters to determine the required RB configuration.

2.2.1 Example Transport Channel Reallocation

Figure 3a shows a state in which signalling and traffic RBs are defined in terms of shared transport and physical channel resources. In this case, the uplink signalling and traffic-carrying RBs are implemented sharing the uplink transport channel Random Access Channel (RACH).

Figure 3b shows the state after RRC has determined a need to reallocate transport channel resources such that dedicated transport channels are now being used. In this case there will be a corresponding change in allocated physical resources.

© wray castle limited

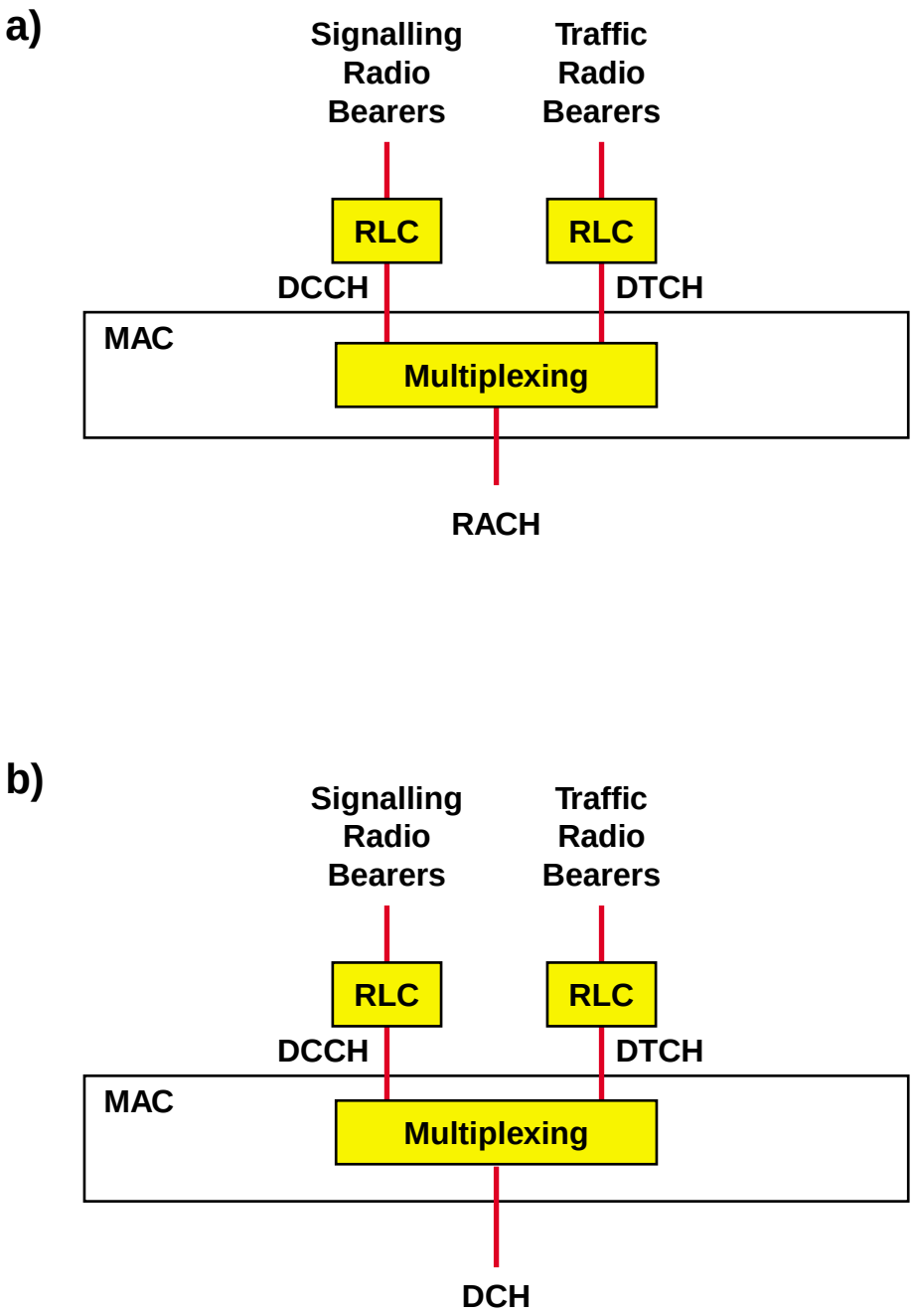


Figure 3
Transport Channel Reallocation

© wray castle limited

2.3 The GSM/EDGE Radio Access Network (GERAN)

The GERAN architecture looks similar to that of the GSM Base Station Subsystem (BSS). The main difference is the GSM/EDGE air interface. The GERAN needs to support a multitude of different interfaces, including the standard 'A' and Gb interfaces and the Iu-CS and Iu-PS interfaces. The GERAN requires similar functionality to that of the UTRAN. Since mobility is handled within the UTRAN, a GERAN must also support mobility. The Iur-g interface is included for this purpose.

The GERAN uses the combination of GSM and EDGE modulation schemes to produce reasonable data rates. The details of this are found in the 3GPP Recommendation TS 43.051 'GERAN Overall Description; Stage 2'.

The GERAN provides a platform to provide the four UMTS bearer classes:

- conversational
- streaming
- interactive
- background

This includes IP end-to-end voice and multimedia services and provides the possibility to connect the 200 kHz radio access to a 3G CN.

Multiple protocol stacks are required to interface with different CNs (GSM and UMTS). The GERAN specifications are not finalized at the time of writing. However, they utilize existing standards, which eases compatibility issues.

© wray castle limited

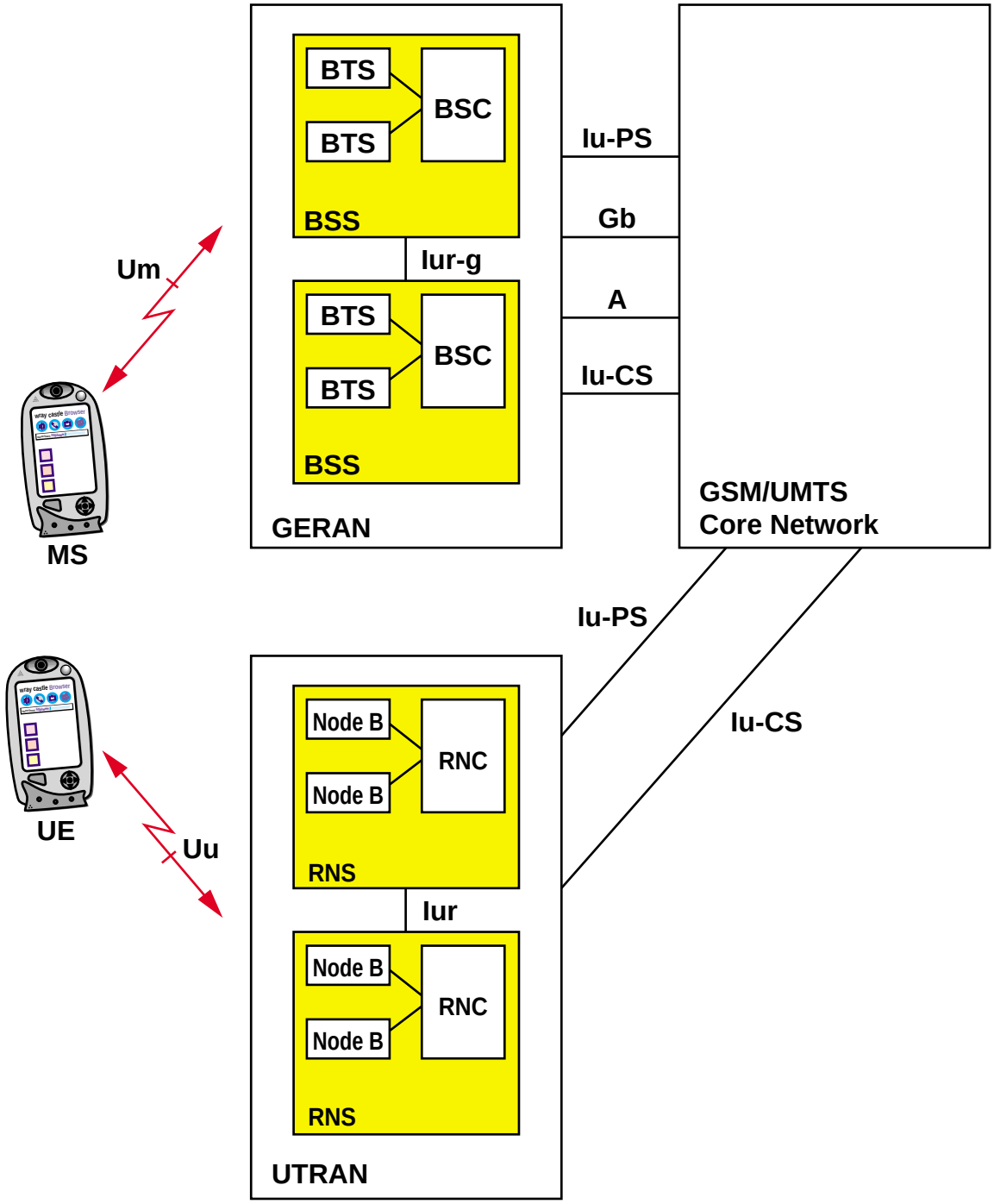


Figure 4
GERAN

© wray castle limited

2.4 General Protocol Architecture

Figure 5 illustrates the general protocol architecture for the UTRAN. The protocols are viewed on two planes, the User Plane and the Control Plane; and then each plane is split into two strata, the Non-Access Stratum (NAS) and Access Stratum (AS).

In each plane, it is the NAS that represents the service-related information (user data in the User Plane, and service-related signalling in the Control Plane).

2.5 The User Plane

The NAS uses the services of the AS to carry user data between the UE and CN. The name given to this service is the Radio Access Bearer (RAB) service. It effectively represents a *pipe* through which user data can be transferred. It is provided from Service Access Point (SAP) to Service Access Point (SAP-to-SAP) by the AS.

The UTRAN forms an integral part of the AS, and therefore the RAB, but it is transparent to the NAS user data.

2.6 The Control Plane

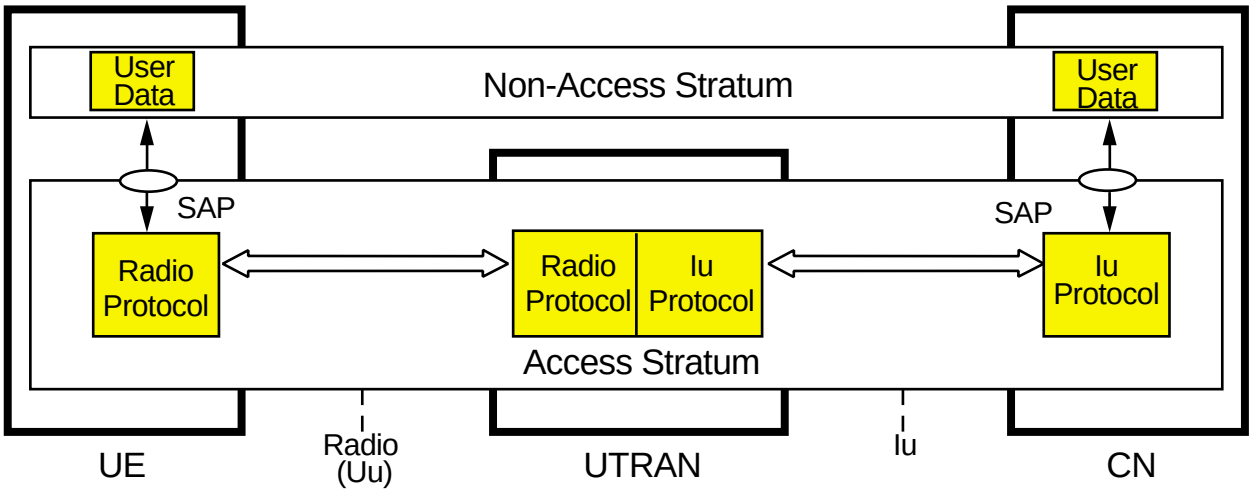
The Control Plane within the AS provides protocols used to control connections from the UE to CN, where the connection may be used for user data or service-related signalling, or for other control purposes (handover, control of transmission resources, requesting service, etc.).

In addition, as for the User Plane, the NAS uses the services of the AS to transfer information between the UE and CN transparently. However, this time, it is the service-related signalling, in the form of Connection Management (CM), Mobility Management (MM), GPRS Mobility Management (GMM), and Session Management (SM) protocols, which is being transferred.

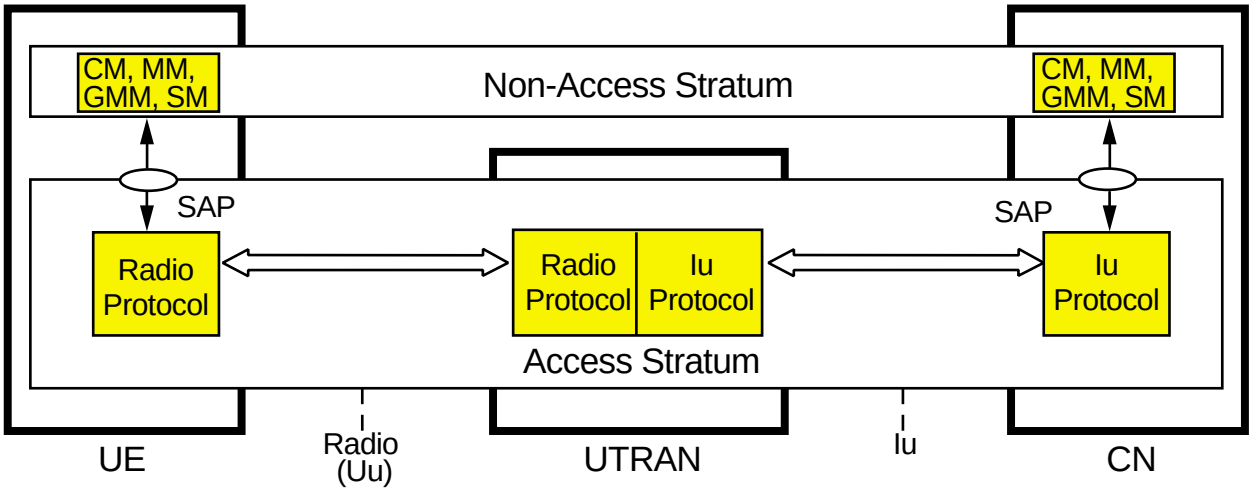
The UTRAN protocols form an integral part of the AS and are used to control the UE to CN connections. However, the UTRAN is transparent to NAS signalling.

© wray castle limited

a) Iu and Uu User Plane



b) Iu and Uu Control Plane



SAP↔SAP = Radio Access Bearer Service

Figure 5
General Protocol Architecture

© wray castle limited

3 THE NON-ACCESS STRATUM (NAS)

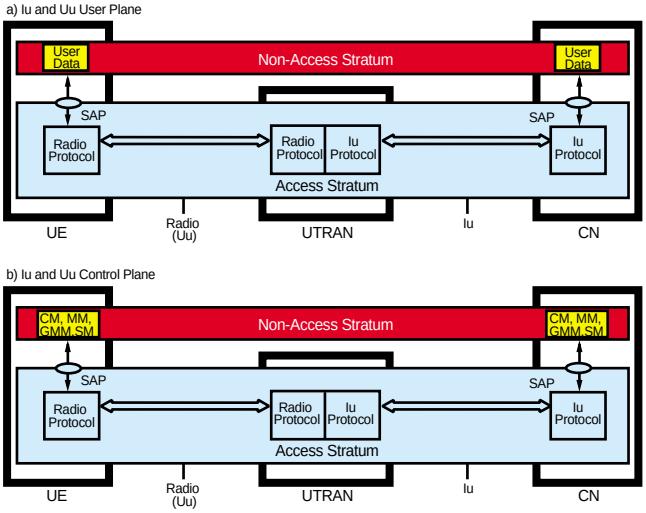
3.1 Services Provided by the NAS

The services provided by the NAS can be broken down into those provided in the User Plane and those provided in the Control Plane, as shown in Figure 6.

In the User Plane, the service provided by the NAS is the transfer of user data. The NAS actually uses the RAB service that is provided by the AS.

In the Control Plane, the services provided by the NAS include procedures related to the control of services: registration, location and routing area updates, connection control (including call control, supplementary services and SMS), session management and the control of logical links.

© wray castle limited



User Plane

- Transfer of user data

Control Plane

- Registration
- Call Control
- Short Message Service (SMS)
- Supplementary Services (Call Independent)
- Session Management
- Logical Link Control

Figure 6

Services Provided by the NAS

© wray castle limited

3.2 NAS Control Plane

The NAS Control Plane protocols provide support for procedures that are relevant end to end between the UE and CN.

The architecture in the NAS is composed of two layers: one providing MM functions (comprised of MM and GMM), and the other providing CM functions (comprised of Session Management (SM), GPRS SMS (GSMS), Call Control (CC) and Supplementary Services (SS)).

As is usual in a layered architecture, the CM layer uses the services of the MM layer below it. Note that MM uses the services of the Radio Resources (RR) layer below it. However, since RR terminates within the UTRAN rather than the CN, it is considered to be part of the AS and therefore not shown on Figure 7. Interaction between the two MM functional blocks is provided for co-ordination purposes.

In all cases, access to services is provided via SAPs and the appropriate identifiers: Protocol Discriminator (PD), Transaction identifiers (TI), and Packet Data Protocol (PDP) identifiers.

The MM layer is accessed directly from above the CM layer in the case of registration, and Logical Link Control (LLC) effectively bypasses both CM and MM layers.

An additional factor to consider is the termination point for NAS protocols in the CN. For CS operation, the termination point will be the MSC, while for PS operation, it will be the SGSN. (If this functionality is combined, there may be one physical termination point only). This necessitates two separate logical interfaces between the UTRAN and the CN, as illustrated in Figure 7.

These protocols are terminated by the UE and CN and are transported transparently through the UTRAN. Therefore, they do not contribute to UTRAN functionality.

© wray castle limited

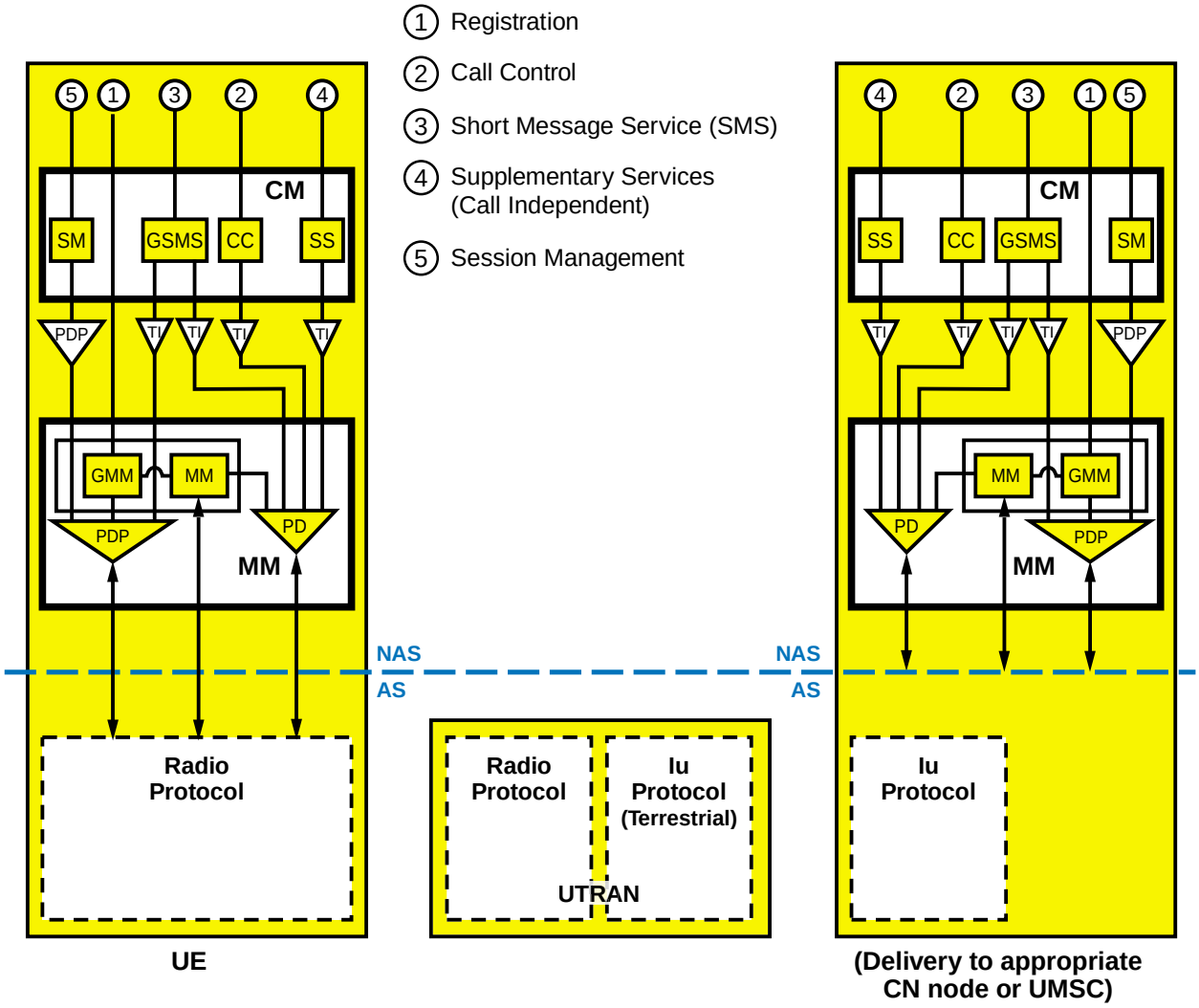


Figure 7
NAS Control Plane

© wray castle limited

4 THE ACCESS STRATUM (AS)

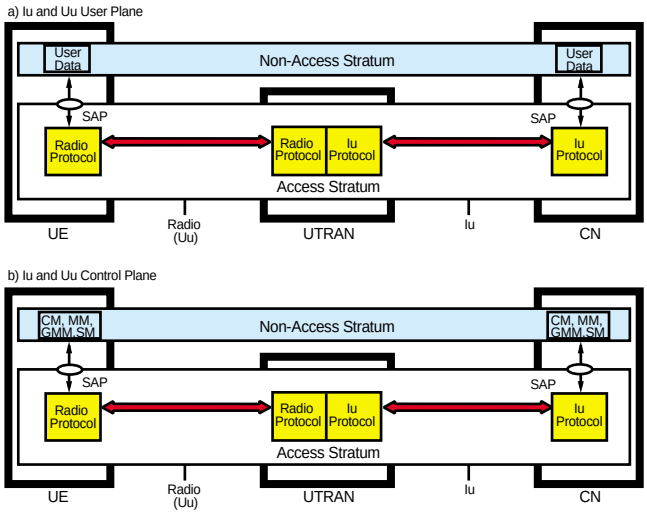
4.1 Overall Aims

The UTRAN forms an integral part of the AS. It is designed to provide for radio access to the CN. The NAS provides access to, and control of, user services; but the AS supports the transport of this information end to end from the UE, through the UTRAN, to the CN.

In order to provide this overall service to the NAS, the AS (and therefore the UTRAN) is designed to:

- provide transparent end-to-end delivery of NAS information (user and control) via the appropriate channels;
- allow control information to be passed between network elements in order to allocate the required resources and set up the appropriate channels;
- encompass suitable transport protocols – although the underlying transport mechanism is considered to be independent of the UTRAN.

© wray castle limited



Note: Drift RNC may not be present in any given connection

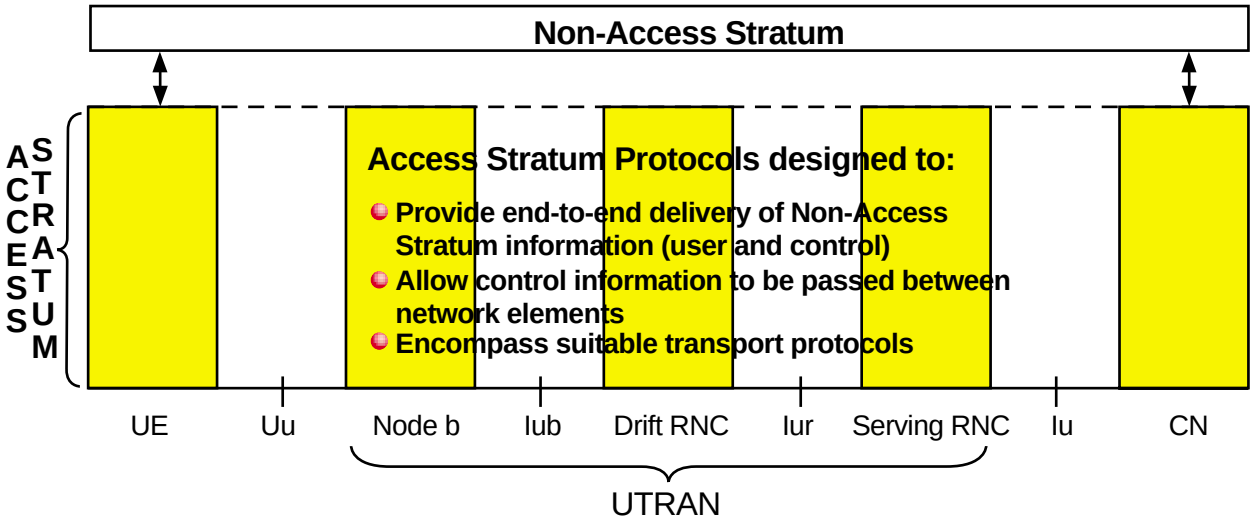


Figure 8

AS Overall Aims

© wray castle limited

4.2 AS Protocol Overview

Figure 9 illustrates the basic concepts of the AS.

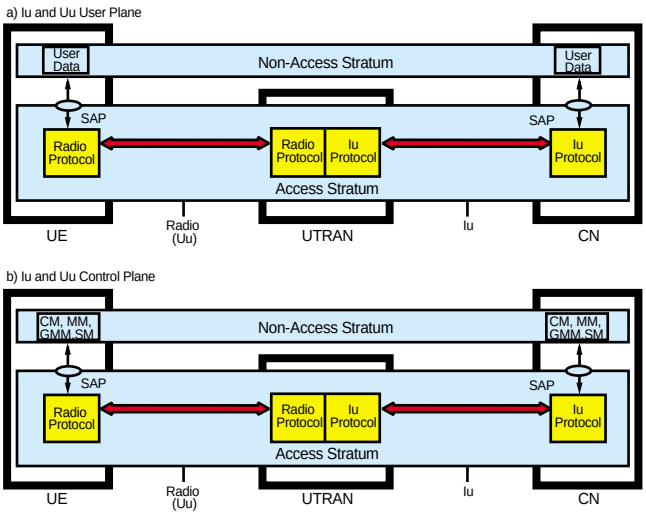
The UTRAN can initially be considered as a single functional entity which provides radio access to the CN. It interfaces to both the UE and the CN, and in each instance provides for transfer of both control information (RRC on the interface to the UE, and RANAP to the CN), and user data.

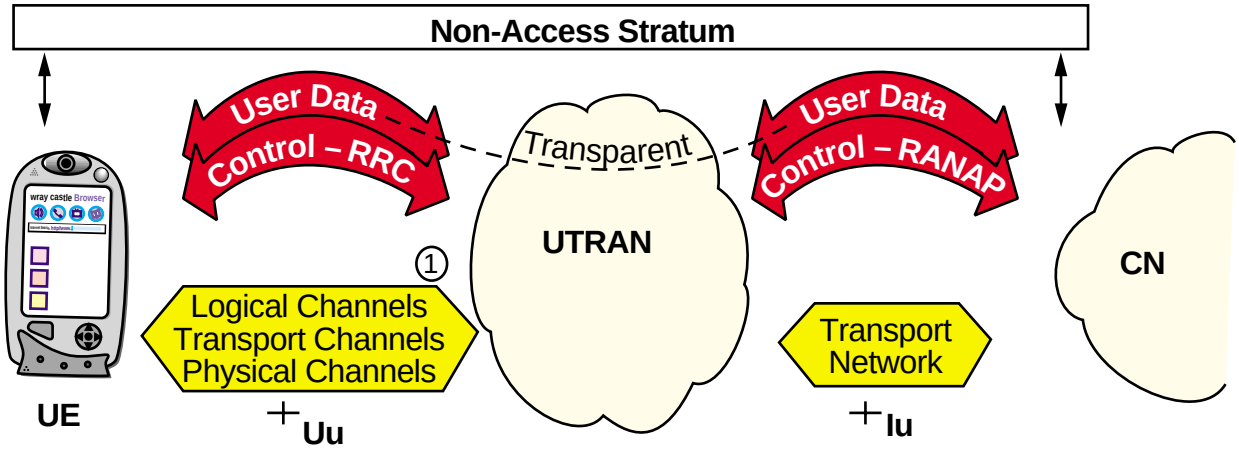
The user data is transferred over each of these, with the UTRAN providing a transparent mapping function between interfaces.

In the case of both user data and control information, logical, transport and physical channels are used to transfer information over the Uu interface, while the appropriate transport network is used for transfer over the Iu interface.

In the case of user data, the UTRAN performs a transparent relay function. However, control information on both interfaces is terminated and acted upon accordingly by the UTRAN.

© wray castle limited





Note: 1 Both user data and RRC information are carried within logical and transport channels, terminating (mainly) in the SRNC/CRNC within the UTRAN

Figure 9
AS Protocol Overview

© wray castle limited

© wray castle limited

LESSON 2

ATM

© wray castle limited

LESSON CONTENTS

1	**Asynchronous Transfer Mode (ATM)**		**3.2.1**
	1.1	ATM Operation	3.2.1
	1.2	ATM Layers	3.2.3
	1.3	ATM in the UTRAN	3.2.5
	1.4	The ATM Layer	3.2.7
	1.5	ATM Cell Headers	3.2.9
	1.6	Virtual Connections	3.2.11
	1.7	Permanent Virtual Connection and Switched Virtual Connection	3.2.13
	1.8	ATM Adaptation Layer 2 (AAL2)	3.2.15
	1.9	AAL Structure	3.2.17
	1.10	ATM Adaptation Layer 5 (AAL5)	3.2.19

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- briefly describe the operation of ATM as a transport protocol within the UTRAN

1 ASYNCHRONOUS TRANSFER MODE (ATM)

1.1 ATM Operation

ATM is defined for a UMTS network.

Figure 1 outlines a potential ATM network. In this diagram there are a number of ATM switches with their respective interconnections shown. The interconnections between switches would be Network–Network Interfaces (NNI), with User–Network Interfaces (UNI) between an ATM user and the ATM switch.

© wray castle limited

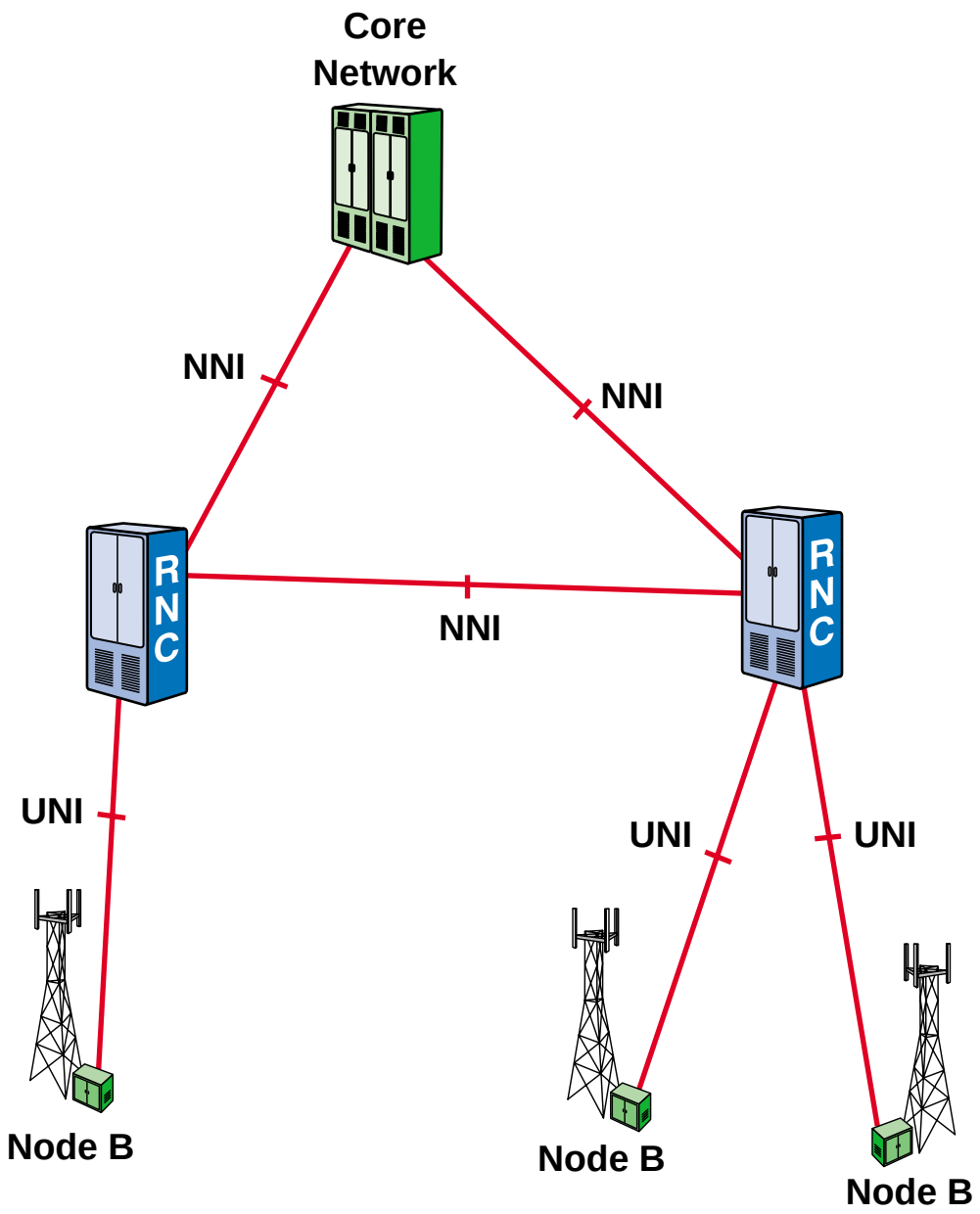


Figure 1
ATM Interfaces within the UTRAN

© wray castle limited

1.2 ATM Layers

The higher-layer protocols are identified as ATM Adaptation Layers (AALs), which provide the means by which user data is processed into the 48-octet cell payloads. Different AALs are needed to support the possible services supported by ATM equipment.

© wray castle limited

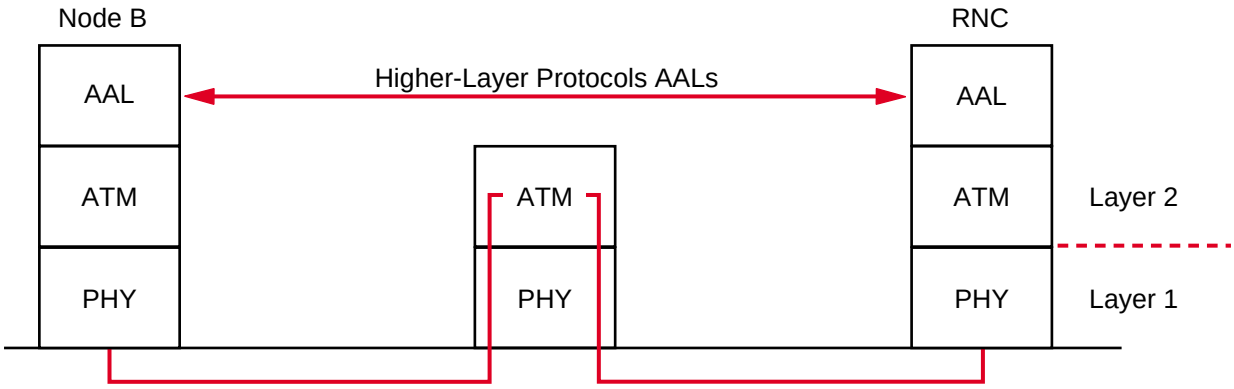


Figure 2
ATM Layers

© wray castle limited

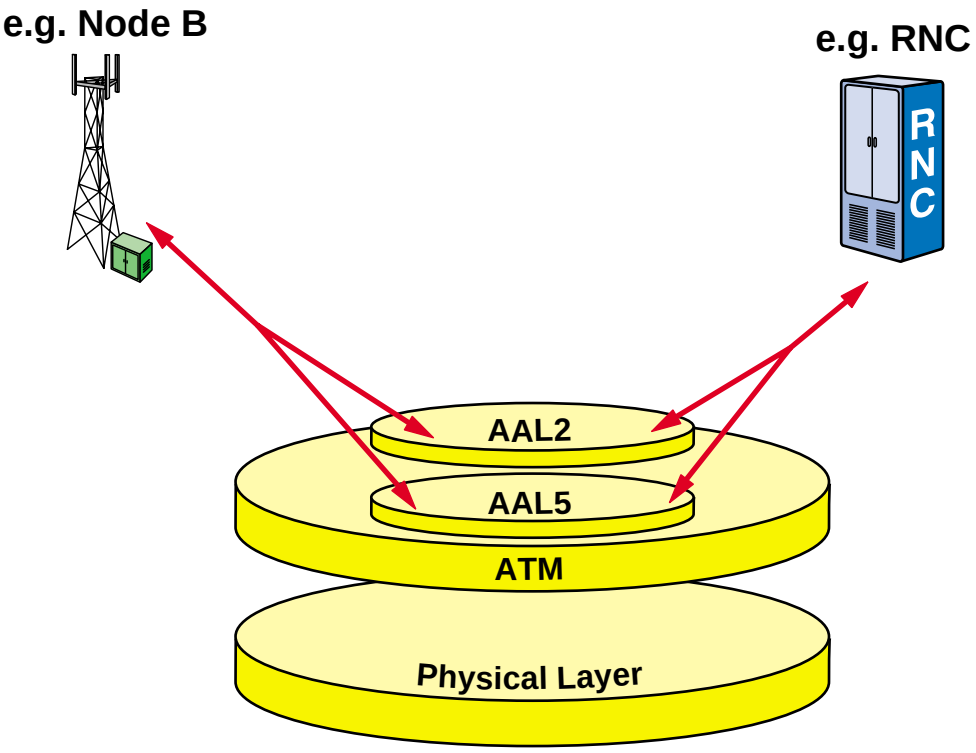
1.3 ATM in the UTRAN

ATM provides logical channels between entities. This allows efficient multiplexing of signalling functions and traffic onto a physical link. Each of these functions has different requirements, hence the need for the vertical partitioning of the protocol stacks. Vertical partitioning of the AAL is used to give the required services to the higher layers.

AAL2 is designed to deal with synchronous, variable-bit-rate, time-critical data flows.

AAL5 is designed to deal with asynchronous, connectionless or connection-oriented, non-time-critical variable-length frames. These characteristics are suited to packet transfer of either signalling or traffic. Thus AAL5 is used for the User and Control Plane.

© wray castle limited



AAL2

- Synchronous
- Variable bit rate
- Time-critical
- Connection-oriented

AAL5

- Asynchronous
- Variable length frames
- Non-time-critical
- Connectionless or connection-oriented

Figure 3
Use of ATM on UTRAN Interfaces

© wray castle limited

1.4 The ATM Layer

The ATM Layer operates on the cell headers and performs functions related to routing, cell multiplexing and demultiplexing, cell header generation/extraction, user flow control and Operations and Maintenance (O&M).

Within the ATM header, two fields are used for routing:

- Virtual Path Identifier (VPI)
- Virtual Channel Identifier (VCI)

© wray castle limited

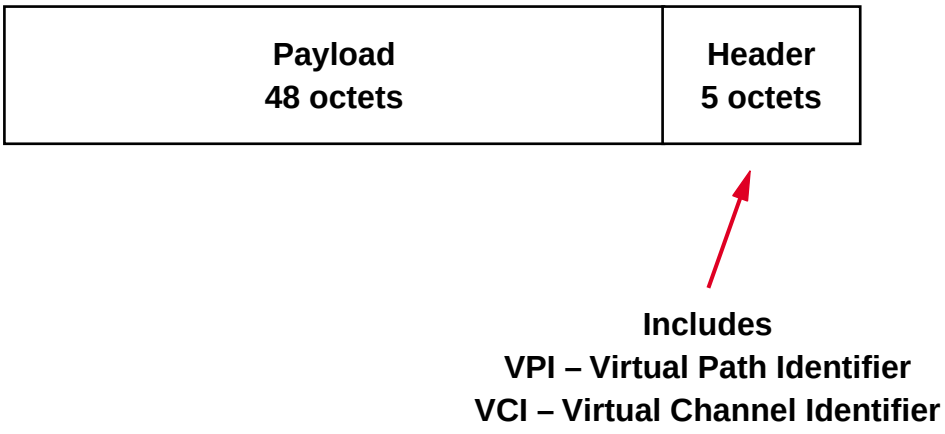


Figure 4
The ATM Layer

© wray castle limited

1.5 ATM Cell Headers

The relevant connection information is carried within the five-octet header, together with information to allow for header error control, payload type, for example user data or management information, and a means of prioritizing cells, indicating whether or not this particular cell may be discarded if required by the network. The header format is shown in Figure 5, where (a) shows the header as used on a user–network interface, and (b) shows the header on a network–node interface. The former has a field for Generic Flow Control (GFC), whilst the latter has a larger range of values for identifying the virtual path.

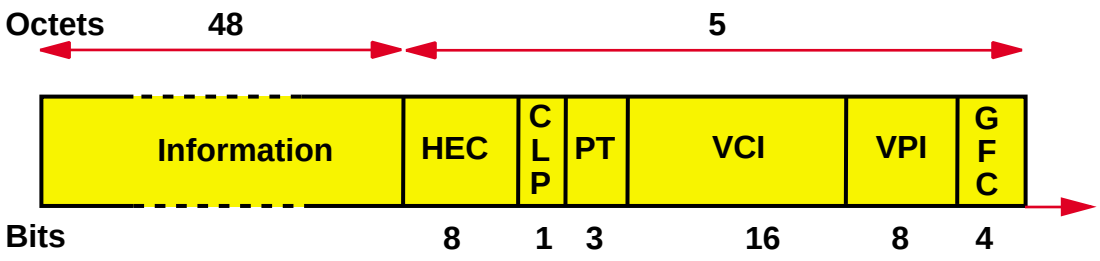
Identification is by use of the Virtual Channel Identifier (VCI) and Virtual Path Identifier (VPI).

VCI
A virtual channel is similar to a virtual circuit in X.25. The VCI allows the cells of different virtual channels to be multiplexed onto a single physical link. The VCI is unique only within that link.

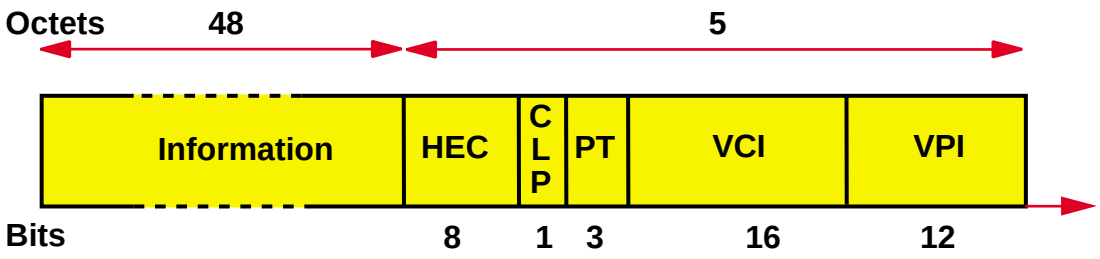
VPI
A virtual path is a group of virtual channels, allowing them to be routed through a network together.

© wray castle limited

a) User–Network Interface



b) Network–Node Interface



GFC – Generic Flow Control
VPI – Virtual Path Identifier
VCI – Virtual Channel Identifier
PT – Payload Type
CLP – Cell Loss Priority
HEC – Header Error Control

Figure 5
ATM Cell Headers

© wray castle limited

1.6 Virtual Connections

ATM is a connection-oriented technique. Connection identifiers are assigned to each link of a connection when required and released when no longer needed. This ensures that all cells relating to a specific connection follow the same route through the network, thus minimizing cell delay variation. The relevant connection information is carried within the 5-octet header, together with information relating to HEC, PT and CLP. The routing of cells is based on the VPI and VCI.

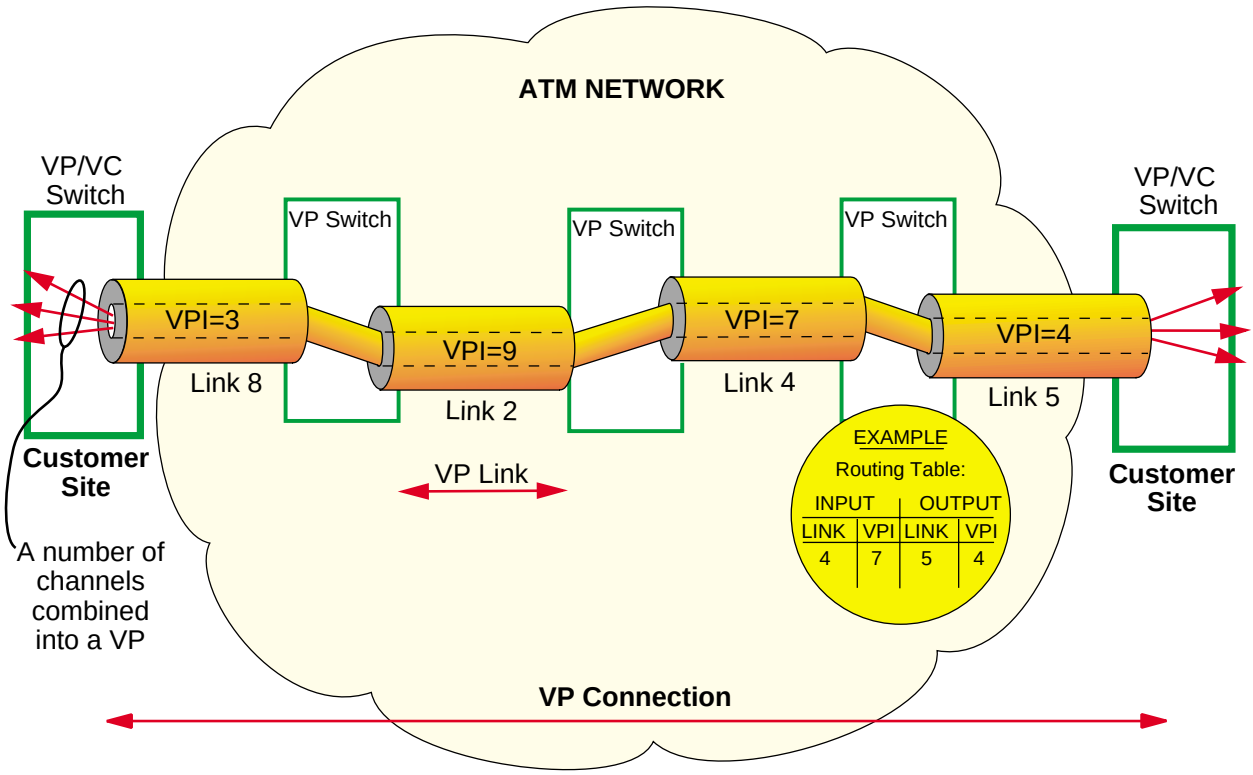
The VCI allows the cells of different Virtual Channels (VC) to be multiplexed onto a single physical link. A Virtual Path (VP) is a group of VCs. The VPI allows them to be routed through a network together. The VCI/VPI values are relevant only to a single ATM trunk and may change each time a cell traverses a switch. Two different VCs belonging to two different VPs at a given interface may have the same VCI value. Therefore, a VC is only fully identified at an interface by both its VPI and VCI values.

The use of VCI and VPI reference values means, in effect, that two levels of switching are in operation at the same time. VPs may be connected together across a network to form a Virtual Path Connection (VPC). A VPC can be seen to be a concatenation of VP links. This is shown in Figure 6. Alternatively, VCs may be switched across a network via a number of VPs to form Virtual Channel Connections (VCC). A VCC is a concatenation of VC links. This is shown in Figure 7. Routing can be based solely on the value of the VPI (a VP switch) or on the values of both VPI and VCI (a VC switch).

When only VPI is used in a VP switch, the value of VCI remains unaltered and the switch is sometimes referred to as an ATM cross-connect. From this it can be seen that a VC link spans a VPC. All ATM switches contain routing tables which map the VPI/VCI of an incoming cell from a given link to a new VPI/VCI value and an output link. When a switch receives a cell, it uses the table to modify the VPI/VCI field in the cell header, and then forwards the cell to the output port identified in the table.

Example routing tables are included in Figures 6 and 7.

© wray castle limited



VC – Virtual Channel
VP – Virtual Path
VPI – Virtual Path Identifier

Note: A single link can carry more than one VP.

Figure 6
VP Switching

© wray castle limited

1.7 Permanent Virtual Connection and Switched Virtual Connection

There are two types of virtual connection used in ATM: the Permanent Virtual Connection (PVC) and the Switched Virtual Connection (SVC).

1.7.1 Permanent Virtual Connection (PVC)

A PVC takes the form of a preconfigured connection where the VPI/VCI for each link through the network are preassigned using management procedures with Quality of Service (QoS) parameters determined. The benefit of PVCs is that there are no call set-up delays as no signalling procedures are needed.

1.7.2 Switched Virtual Connection (SVC)

An SVC is a dynamic connection configured during user-initiated signalling procedures. These procedures are performed over a reserved signalling VC predefined for point-to-point connections over an interface.

© wray castle limited

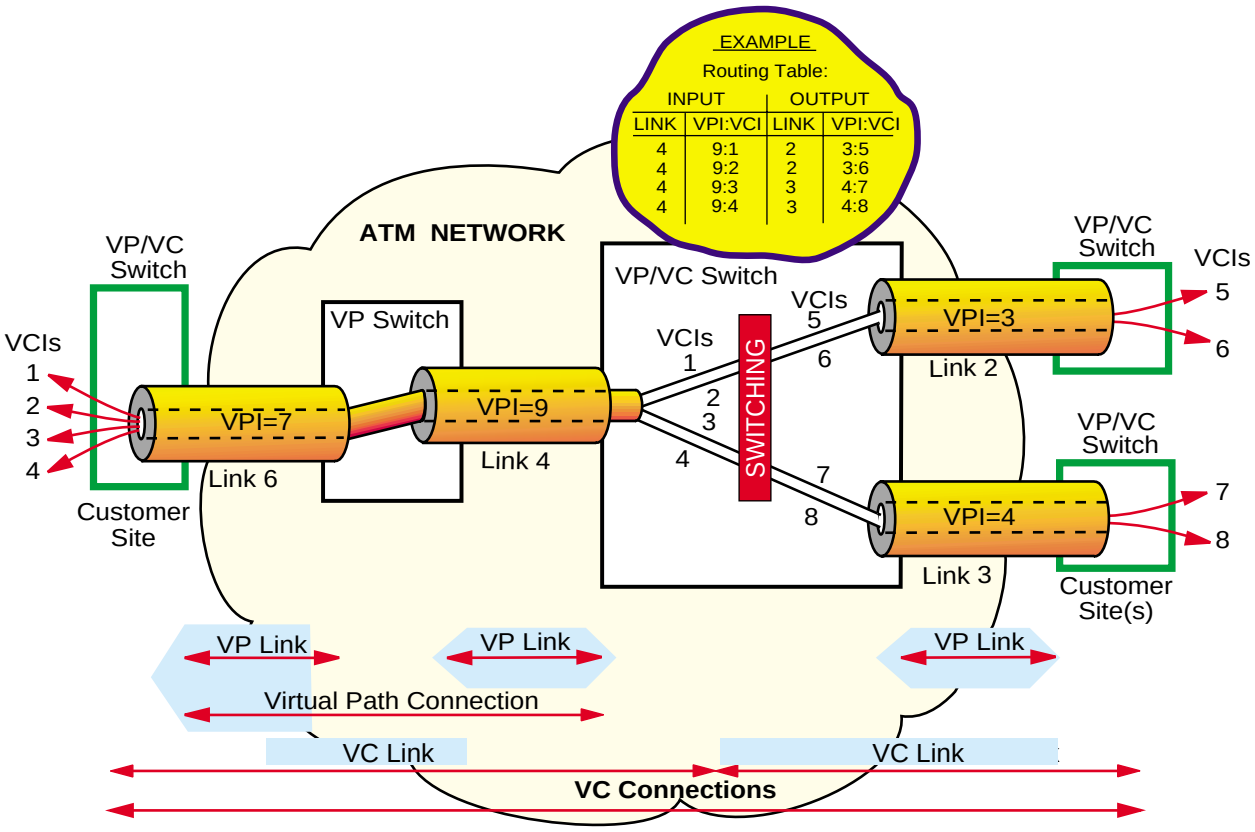


Figure 7
VC Switching

© wray castle limited

1.8 ATM Adaptation Layer 2 (AAL2)

AAL2 provides a bandwidth-efficient transmission of low-rate, short and variable-length packets in delay-sensitive applications. More than one AAL2 user information stream can be supported on a single ATM connection.

AAL2 consists of a Common Part Sublayer (CPS) and provides data transfer of user packets, up to 45 (default) or 64 octets, from one CPS user to another through an ATM network. A header (3 octets) that contains a Channel Identifier (CID), LI, User-to-User Indication (UUI) and HEC is added to the higher-layer user packet. The user data packet plus the header is referred to as a CPS-packet.

The CPS segments the CPS-PDUs (as shown in Figure 8) then adds a *Start Field* (STF) header (1 octet).

The STF contains:

- Offset Field (OSF) – 6 bits
- Sequence Number (SN) – 1 bit
- Parity (P) – 1 bit
- Possible padding, making sure PDU and header align to multiples of 48 octets.

The CPS-PDU is delivered to the ATM layer, where the ATM header is added.

© wray castle limited

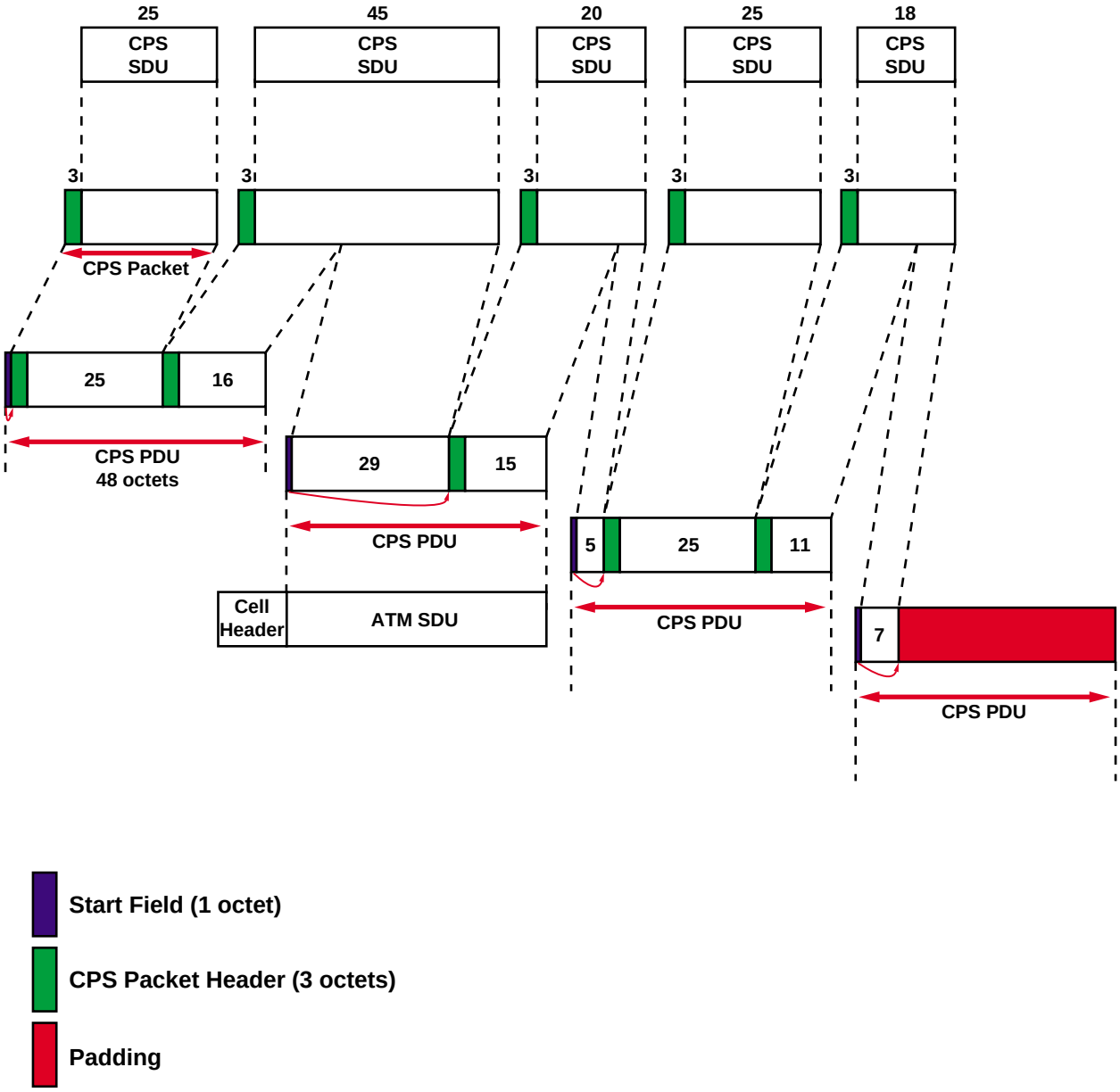


Figure 8
AAL2 CPS Packing

© wray castle limited

1.9 AAL Structure

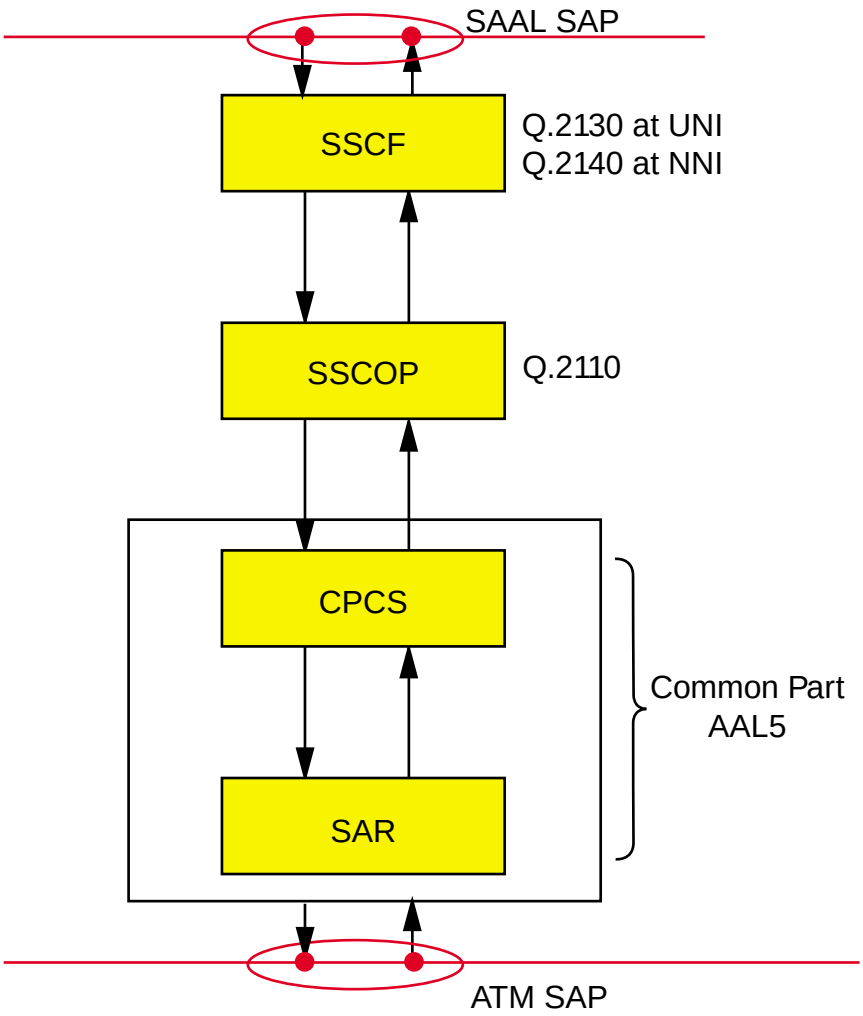
The AAL performs functions required by the control plane and supports mapping between the ATM layer and the next higher layer. The Signalling AAL (SAAL) is functionally divided into a Common Part (CP) and a Service Specific Part (SSP). The CP can be used with different SSPs; the SSP is specific to the needs of the service application (ITU-T Recommendation Q.2630.1).

The purpose of the SAAL is to provide reliable transport of Q.2630.1 signalling messages between peer ATM entities. These messages are transported over the ATM layer. The specification of the SAAL is given in Figure 9.

The SAAL makes use of the service provided by the Common Part Convergence Sublayer (CPCS) and SAR, which form the CP of AAL5 and provide unassured information transfer. The Service Specific Convergence Sublayer (SSCS) part of AAL5 is performed by a combination of the Service Specific Connection-Oriented Protocol (SSCOP) and a Service Specific Coordination Function (SSCF) defined for the UNI or NNI. The SSCOP provides assured transfer of variable-length signalling messages, while the SSCF adapts the service provided by the SSCOP to the needs of the Q.2630.1 signalling layer.

The SSCOP function provides mechanisms for the establishment and release of connections and the reliable exchange of information between peer entities. The SSCOP, which is applicable to both the UNI and NNI, is detailed in ITU-T Recommendation Q.2110. The CPCS provides transparent transport of SDUs produced by the next higher layer, while the SAR segments SAR SDUs to fit into outgoing ATM cells and reassembles incoming cells into SAR SDUs. Both the CPCS and the SAR belong to the AAL5 specification found in ITU-T Recommendation I.363.5.

© wray castle limited



Service Specific Coordination Function (SSCF)

Service Specific Connection-Oriented Protocol (SSCOP)

Common Part Convergence Sublayer (CPCS)

Segmentation and Reassembly Sublayer (SAR)

Figure 9

Complete AAL Structure for Signalling Applications

© wray castle limited

1.10 ATM Adaptation Layer 5 (AAL5)

AAL5 allows variable-length frames (up to 65,535 octets) to be transported across the ATM network. AAL5 is subdivided into the Convergence Sublayer (CS) and the Segmentation and Reassembly (SAR) Sublayer.

The user data, PDU, is first passed to the CS, where eight octets of tail information are added, consisting of:

- 2 octets – control, used for alignment
- 2 octets – length information
- 4 octets – CRC
- possible padding, making sure the PDU and the header align to multiples of 48 octets

The SAR Sublayer takes the Convergence Sublayer PDU (CS-PDU) and performs segmentation into blocks of 48 octets (SAR-PDU). The SAR-PDU is delivered to the ATM layer, where the ATM header is added.

© wray castle limited

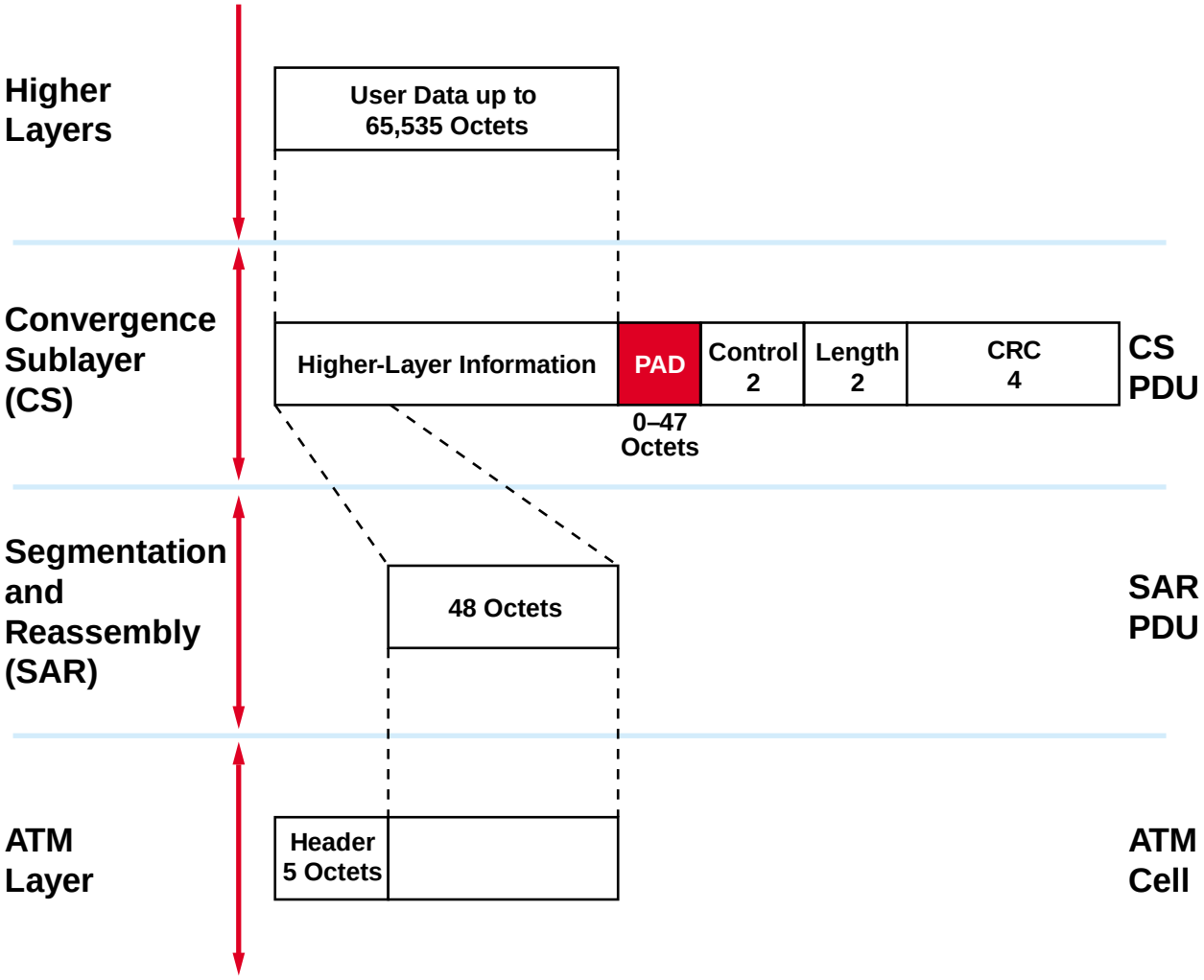


Figure 10
AAL5 Process

© wray castle limited

© wray castle limited

LESSON 3

RADIO NETWORK LAYER AND TRANSPORT NETWORK LAYER IDENTIFIERS

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Radio Network Control Plane Identifiers 3.3.1

2 Transport Network Control Plane Identifiers 3.3.3
2.1 ATM Adaptation Layer 2 (AAL2) Identifiers 3.3.3
2.2 GPRS Tunnelling Protocol (GTP) over Internet Protocol (IP) 3.3.3

3 Binding Identifier 3.3.5

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- identify the Radio Network Layer and Transport Network Layer Control Plane identifiers
- describe the use of binding identifiers

1 RADIO NETWORK CONTROL PLANE IDENTIFIERS

The Radio Network Control Plane identifiers are used by the application part when setting up and referencing Objects. Four Objects are defined and require identifiers:

- Radio Access Bearer (RAB-Id)
- Dedicated Transport Channel (DCH-Id)
- Downlink Shared Channel (DSCH-Id)
- TDD Uplink Shared Channel (USCH-Id).

Figure 1 shows which interfaces will use these Object identifiers.

© wray castle limited

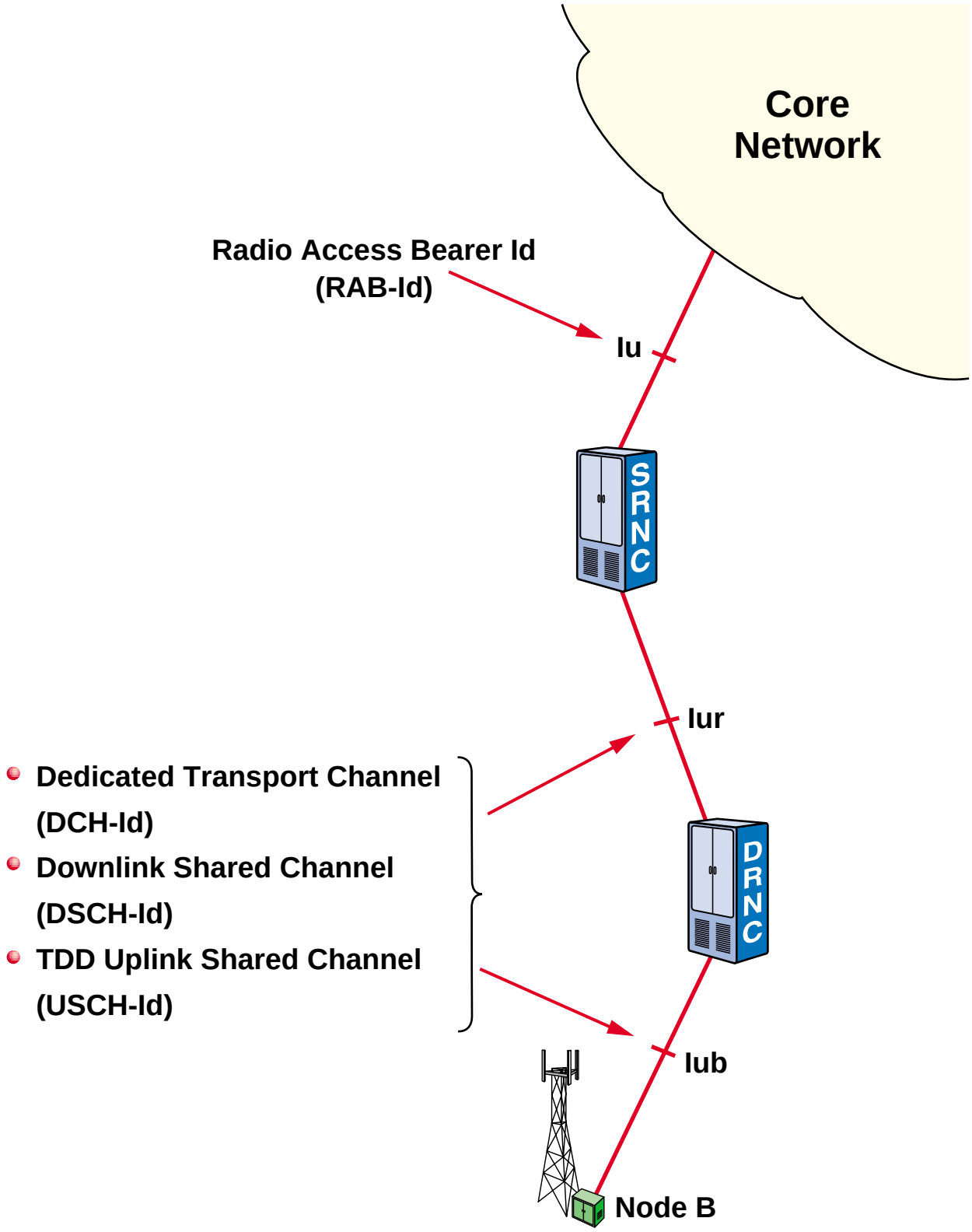


Figure 1
Radio Network Control Plane Identifiers

© wray castle limited

2 TRANSPORT NETWORK CONTROL PLANE IDENTIFIERS

The Access Link Control Application Part (ALCAP) identifier is used in the Transport Network Control Plane and possibly in the User Plane for data transmission. There are two identifiers specified; each can be binded to an Application Part identifier.

2.1 ATM Adaptation Layer 2 (AAL2) Identifiers

AAL2 exists on the Iu-CS, Iur and Iub interfaces. ALCAP establishes the AAL2 connection and specifies the ALCAP identifier, which consists of AAL2 Path ID and Channel ID (CID)

2.2 GPRS Tunnelling Protocol (GTP) over Internet Protocol (IP)

The Iu-PS interface uses GTP over Internet Protocol (IP) for data transfer.

© wray castle limited

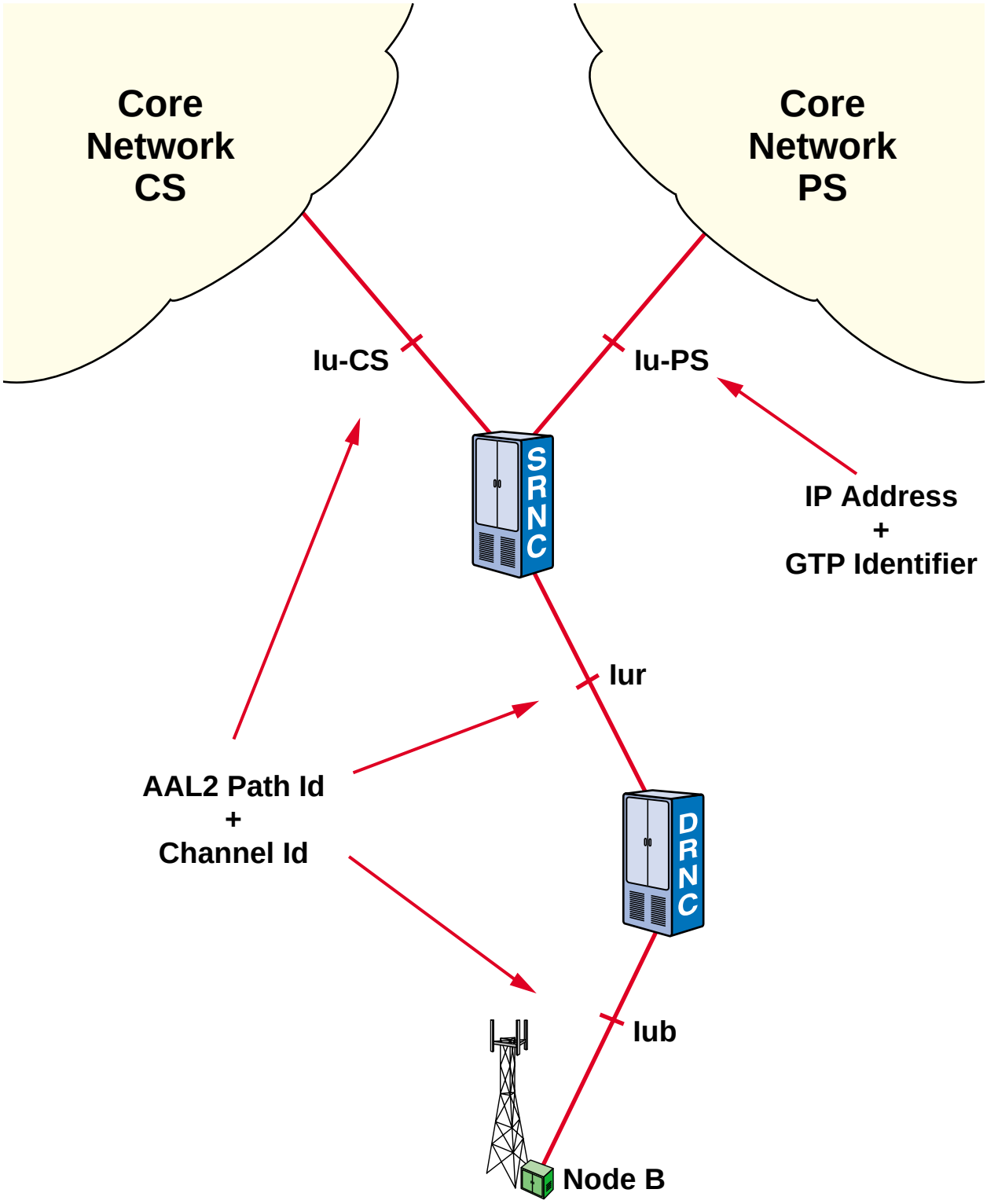


Figure 2
Transport Network Control Plane Identifiers

© wray castle limited

3 BINDING IDENTIFIER

The Binding identifier is used to link ALCAP and Application Part identifiers i.e. binding the Radio and Transport Network Control Plane identifiers together. Binding identifiers are used when new transmission links are established. The Application Part protocol sends the Binding identifier in one direction, it is returned in the other direction by the ALCAP protocol.

© wray castle limited

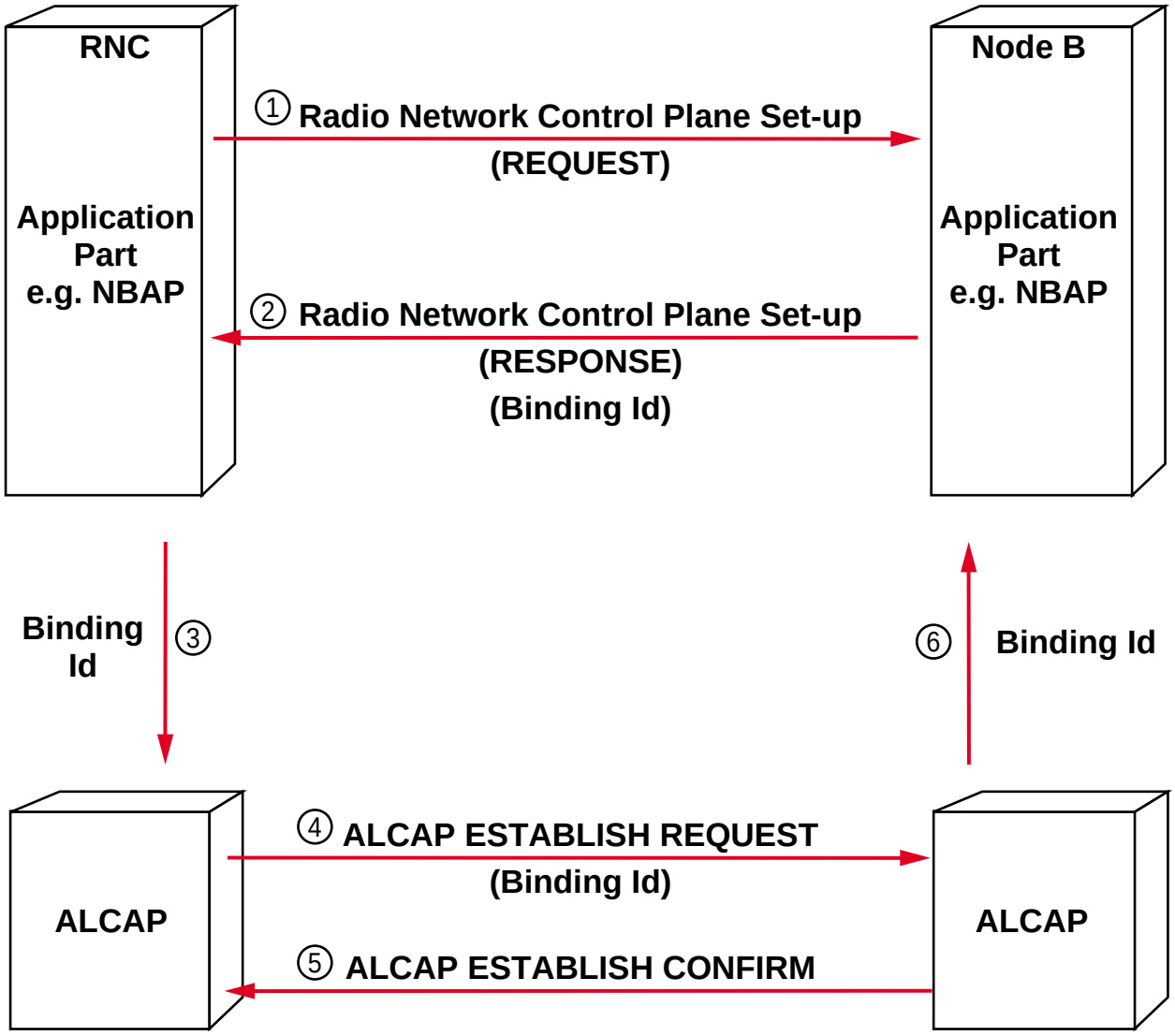


Figure 3
Binding Identifier

© wray castle limited

© wray castle limited

SECTION 4

PROTOCOLS COMMON TO UTRAN INTERFACES

© wray castle limited

LESSON 1

ALCAP

© wray castle limited

LESSON CONTENTS

1	**Access Link Control Application Part (ALCAP)**		**4.1.1**
	1.1	Services Provided by ALCAP	4.1.1
	1.2	Functions of ALCAP	4.1.3
	1.3	AAL Type 2 Signalling Protocol	4.1.5
	1.4	ALCAP Connection Set-up	4.1.7
	1.5	AAL Structure	4.1.9
	1.6	Service Specific Connection-Oriented Protocol (SSCOP)	4.1.11
	1.7	An Example of an AAL2 Signalling Message Delivery	4.1.15

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of Access Link Control Application Part (ALCAP)

© wray castle limited

1 ACCESS LINK CONTROL APPLICATION PART (ALCAP)

1.1 Services Provided by ALCAP

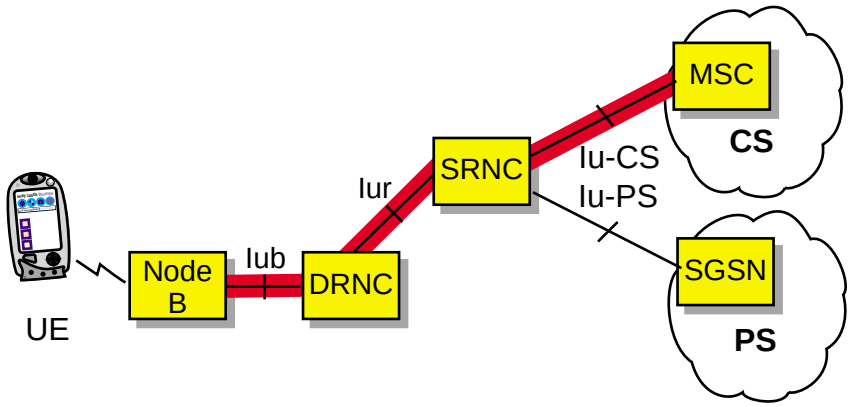
ALCAP is used on the Iu-CS, Iub and Iur interfaces to set up User Plane Transport Bearers.

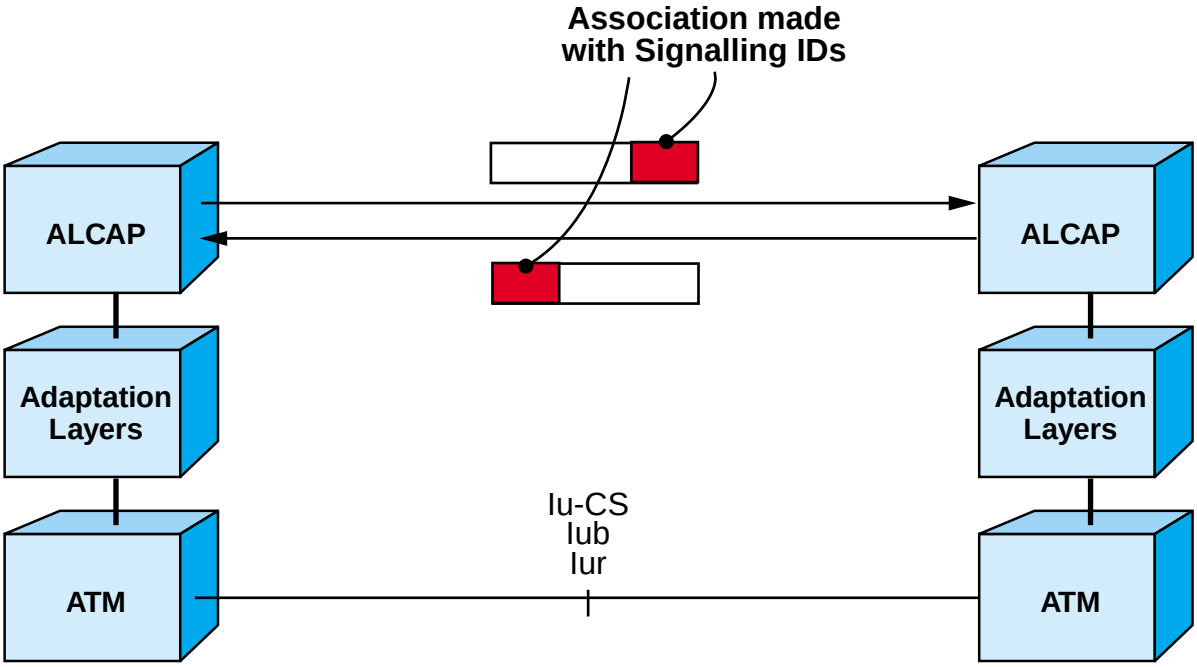
The set-up of the User Plane Transport Bearers is controlled by the:

- SRNC for the Iur interface
- CRNC for the Iub interface
- CN and RNC for the Iu interface

ALCAP is the AAL Type 2 signalling protocol, which provides the signalling capability to establish, release and maintain AAL Type 2 point-to-point connections across the UTRAN.

© wray castle limited





- Establishes/maintains and releases User Plane Transport Bearer

Figure 1

Services Provided by ALCAP

© wray castle limited

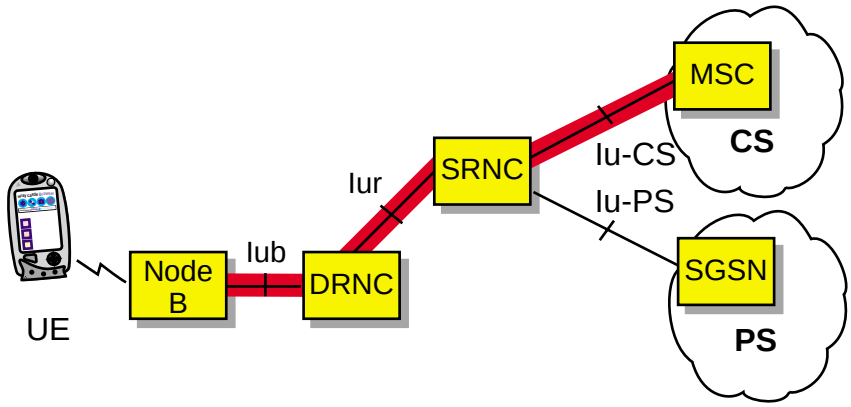
1.2 Functions of ALCAP

The functions of ALCAP are summarized in Figure 2.

The main functions are:

- specifying the Link Characteristics (QoS) when establishing the transport bearer;
- identifying the Path ID, which corresponds to the Virtual Channel Connection (VCC) for the User Plane Transport Bearer;
- transporting the Binding Id, to link ALCAP with the Application Part (RANAP, RNSAP and NBAP).

© wray castle limited



Functions of ALCAP:

- Specifying Link Characteristics (QoS)
- Identifying the Path Id
- Transporting the Binding Id

Figure 2
Functions of ALCAP

© wray castle limited

1.3 AAL Type 2 Signalling Protocol

Access Link Control Application Part (ALCAP) is the generic name for the AAL Type 2 signalling protocol specified in the ITU-T Recommendation Q.2630.1. This protocol supports the dynamic establishment and release of individual AAL Type 2 point-to-point connections. The ALCAP protocol is required on the Iu-CS, Iur, and Iub interfaces.

ALCAP messages are shown below:

BLC	Block confirm
BLO	Block request
CFN	Confusion
ECF	Establish confirm
ERQ	Establish request
RLC	Release confirm
REL	Release request
RSC	Reset confirm
RES	Reset request
UBC	Unblock confirm
UBL	Unblock request

Only the Establish and Release messages are shown in Figure 3.

© wray castle limited

Parameter	Description	ERQ	ECF	REL	RLC
Cause	Reason for Release	–	–	M	–
Connection Element Identifier	Path ID and Channel ID	M	–	–	–
Destination E.164 Service Endpoint Address		1)	–	–	–
Destination NSAP Service Endpoint Address		1)	–	–	–
Destination Signalling Association Identifier	Four-Octet Reference	–	M	M	M
Link Characteristics	Maximum and Average Bit Rate and SDU Size	O	–	–	–
Originating Signalling Association Identifier	Four-Octet Reference	M	M	–	–
Served User Generated Reference (SUGR)	Used to carry Binding ID	O	–	–	–
Served User Transport		O	–	–	–
Service Specific Information	Audio, Multimedia, SAR-assured or SAR-unassured information	2)	–	–	–
Test Connection Indicator	If present identifies test connection	O	–	–	–

1) One of these parameters must be present.

2) Contains information specific to audio, multirate, SAR-assured or SAR-unassured data transfer.

Figure 3

AAL Type 2 Signalling Protocol

© wray castle limited

1.4 ALCAP Connection Set-up

Upon receiving notification requesting a new connection, a free Signalling Association Identifier (SAID) is allocated for the outgoing protocol entity. Upon allocating a SAID, an ERQ message is sent to the adjacent AAL Type 2 node.

Upon receiving an indication from the peer protocol entity requesting a new connection, the receiving entity checks the availability of the CID value and other resources.

The receiving entity acknowledges the successful AAL Type 2 connection establishment towards the peer entity using an ECF message. This includes the Originating and Destination signalling association identifier.

© wray castle limited

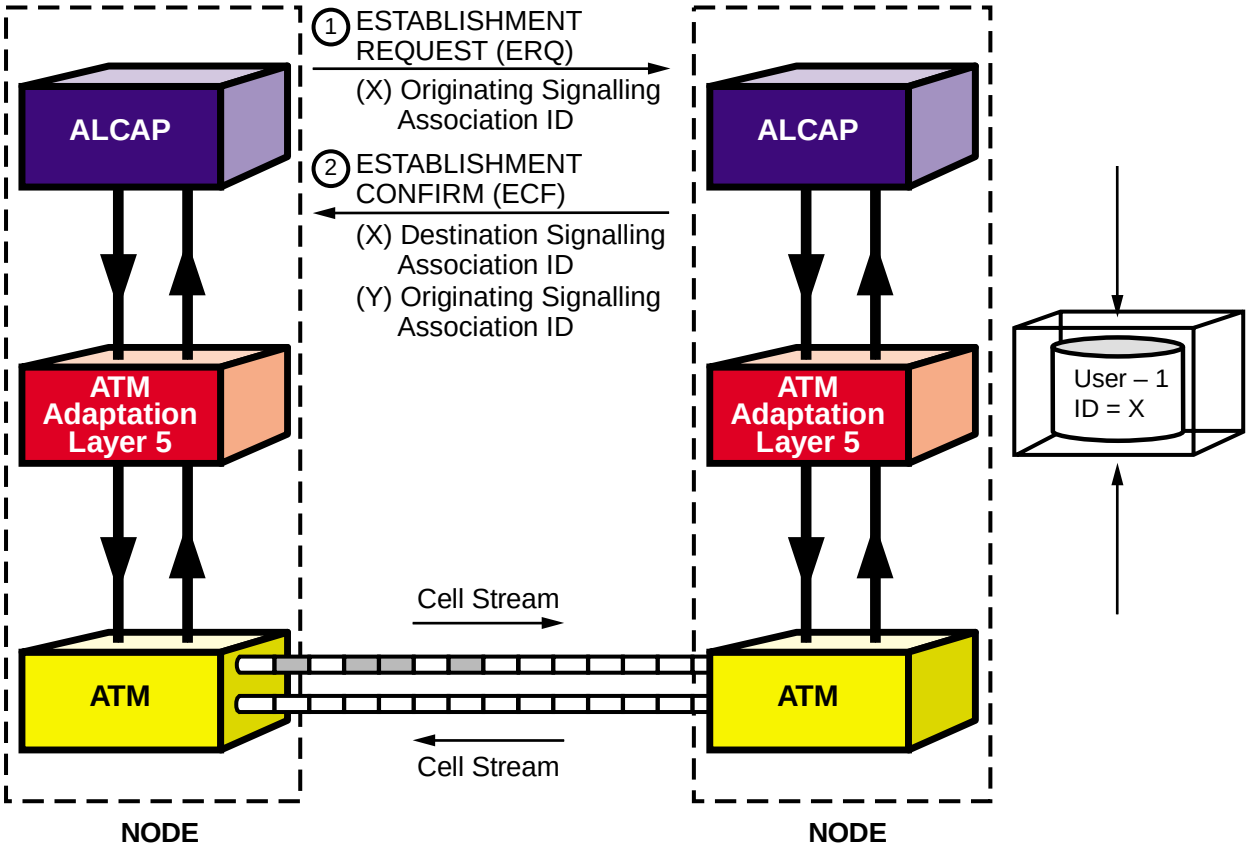


Figure 4
ALCAP Connection Set-up

© wray castle limited

1.5 AAL Structure

The AAL performs functions required by the Control Plane and supports mapping between the ATM layer and the next higher layer. The Signalling AAL (SAAL) is functionally divided into a Common Part (CP) and a Service Specific Part (SSP). The CP can be used with different SSPs; the SSP is specific to the needs of the service application (ITU-T Recommendation Q.2630.1).

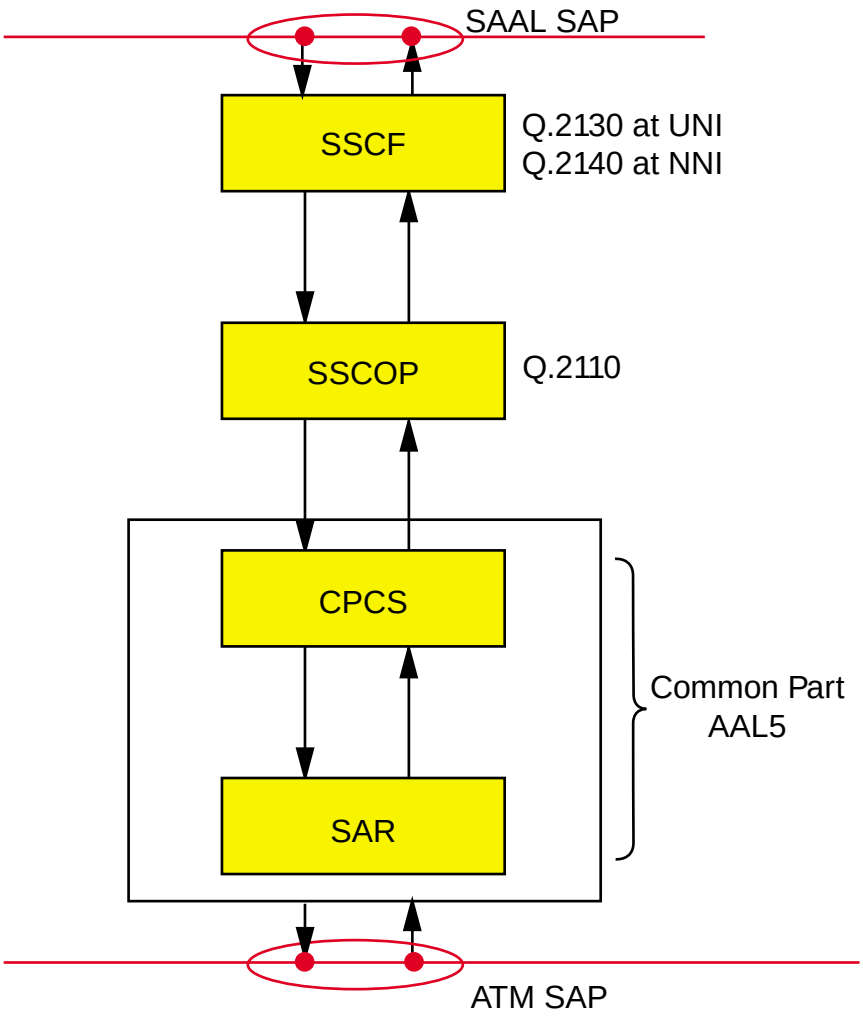
The purpose of the SAAL is to provide reliable transport of Q.2630.1 signalling messages between peer ATM entities. These messages are transported over the ATM layer. The specification of the SAAL is given in Figure 5.

The SAAL makes use of the service provided by the Common Part Convergence Sublayer (CPCS) and SAR, which form the CP of AAL5 and provide unassured information transfer. The Service Specific Convergence Sublayer (SSCS) part of AAL5 is performed by a combination of the Service Specific Connection-Oriented Protocol (SSCOP) and a Service Specific Coordination Function (SSCF) defined for the UNI or NNI. The SSCOP provides assured transfer of variable-length signalling messages, while the SSCF adapts the service provided by the SSCOP to the needs of the Q.2630.1 signalling layer.

The SSCOP function provides mechanisms for the establishment and release of connections and the reliable exchange of information between peer entities. The SSCOP, which is applicable to both the UNI and NNI, is detailed in ITU-T Recommendation Q.2110. The CPCS provides transparent transport of SDUs produced by the next higher layer, while the SAR segments SAR SDUs to fit into outgoing ATM cells and reassembles incoming cells into SAR SDUs. Both the CPCS and the SAR belong to the AAL5 specification found in ITU-T Recommendation I.363.5.

The SCCF-UNI or NNI has a null function or offers no services to the higher layer user, i.e. ALCAP. This is due to the primitives for SSCF being the same as for SSCOP, so that the SSCF maps the service of SSCOP to the needs of the AAL user.

© wray castle limited



Service Specific Coordination Function (SSCF)

Service Specific Connection-Oriented Protocol (SSCOP)

Common Part Convergence Sublayer (CPCS)

Segmentation and Reassembly Sublayer (SAR)

Figure 5

Complete AAL Structure for Signalling Applications

© wray castle limited

1.6 Service Specific Connection-Oriented Protocol (SSCOP)

The SSCOP is used to transfer variable-length SDUs between users of SSCOP. In terms of signalling, SSCOP receives SDUs from the signalling layer then forms PDUs and transfers them to the peer SSCOP. At the receiving end, SSCOP delivers the received SDU to the signalling layer. SSCOP uses the services provided by CPCS, which are an unassured information transfer and a mechanism for detecting corruption in SSCOP PDUs.

The functions provided by the SSCOP are detailed below.

Sequence Integrity
This preserves the order of SSCOP SDUs submitted for transfer by the signalling layer.

Error Correction
The receiving SSCOP detects missing SDUs, and sequence errors are corrected through retransmission.

Flow Control
This allows the receiver to control the rate at which the peer SSCOP transmitter may send information.

Error Reporting
This indicates to layer management errors that have occurred.

Keep Alive
This verifies that two peer SSCOP entities participating in a connection remain in a connected state even in a prolonged absence of data transfer.

Local Data Retrieval
This allows the local SSCOP user to retrieve in-sequence SDUs which have not yet been released by the SSCOP entity.

Connection Control
This performs the establishment, release and resynchronization of an SSCOP connection.

© wray castle limited

Functionality	PDU Name	Description
Establishment	BGN	Request Initialization
	BGAK	Request Acknowledgement
	BGREJ	Connection Reject
Release	END	Disconnect Command
	ENDAK	Disconnect Acknowledgement
Resynchronization	RS	Resynchronization Command
	RSAK	Resynchronization Acknowledgement
Recovery	ER	Recovery Command
	ERAK	Recovery Acknowledgement
Assured Data Transfer	SD	Sequenced Connection-mode-Data
	POLL	Transmitter State Information with request for Receiver State Information
	STAT	Solicited Receiver State Information
	USTAT	Unsolicited Receiver State Information
Unacknowledged Data Transfer	UD	Unnumbered User Data
Management Data Transfer	MD	Unnumbered Management Data

Figure 6
SSCOP PDU Names and Definitions

© wray castle limited

Transfer of User Data
This is used for the conveyance of user data between the users of SSCOP in both assured and unassured transfer modes.

Protocol Error Detection and Recovery
This detects and recovers from errors in the operation of the protocol.

Status Reporting
This allows the transmitter and receiver peer entities to exchange status information.

In order to perform these functions, different types of SSCOP PDUs are defined for peer-to-peer communications between two SSCOP entities. These are listed in Figure 6. The 15 defined PDU types all have different formats, which are given in ITU-T Recommendation Q.2110.

© wray castle limited

Functionality	PDU Name	Description
Establishment	BGN	Request Initialization
	BGAK	Request Acknowledgement
	BGREJ	Connection Reject
Release	END	Disconnect Command
	ENDAK	Disconnect Acknowledgement
Resynchronization	RS	Resynchronization Command
	RSAK	Resynchronization Acknowledgement
Recovery	ER	Recovery Command
	ERAK	Recovery Acknowledgement
Assured Data Transfer	SD	Sequenced Connection-mode-Data
	POLL	Transmitter State Information with request for Receiver State Information
	STAT	Solicited Receiver State Information
	USTAT	Unsolicited Receiver State Information
Unacknowledged Data Transfer	UD	Unnumbered User Data
Management Data Transfer	MD	Unnumbered Management Data

Figure 6 (repeated)
SSCOP PDU Names and Definitions

© wray castle limited

1.7 An Example of an AAL2 Signalling Message Delivery

Figure 7 shows the processing of an AAL2 signalling message being delivered and highlighting the lower layer functions before being fired across the ATM interface.

© wray castle limited

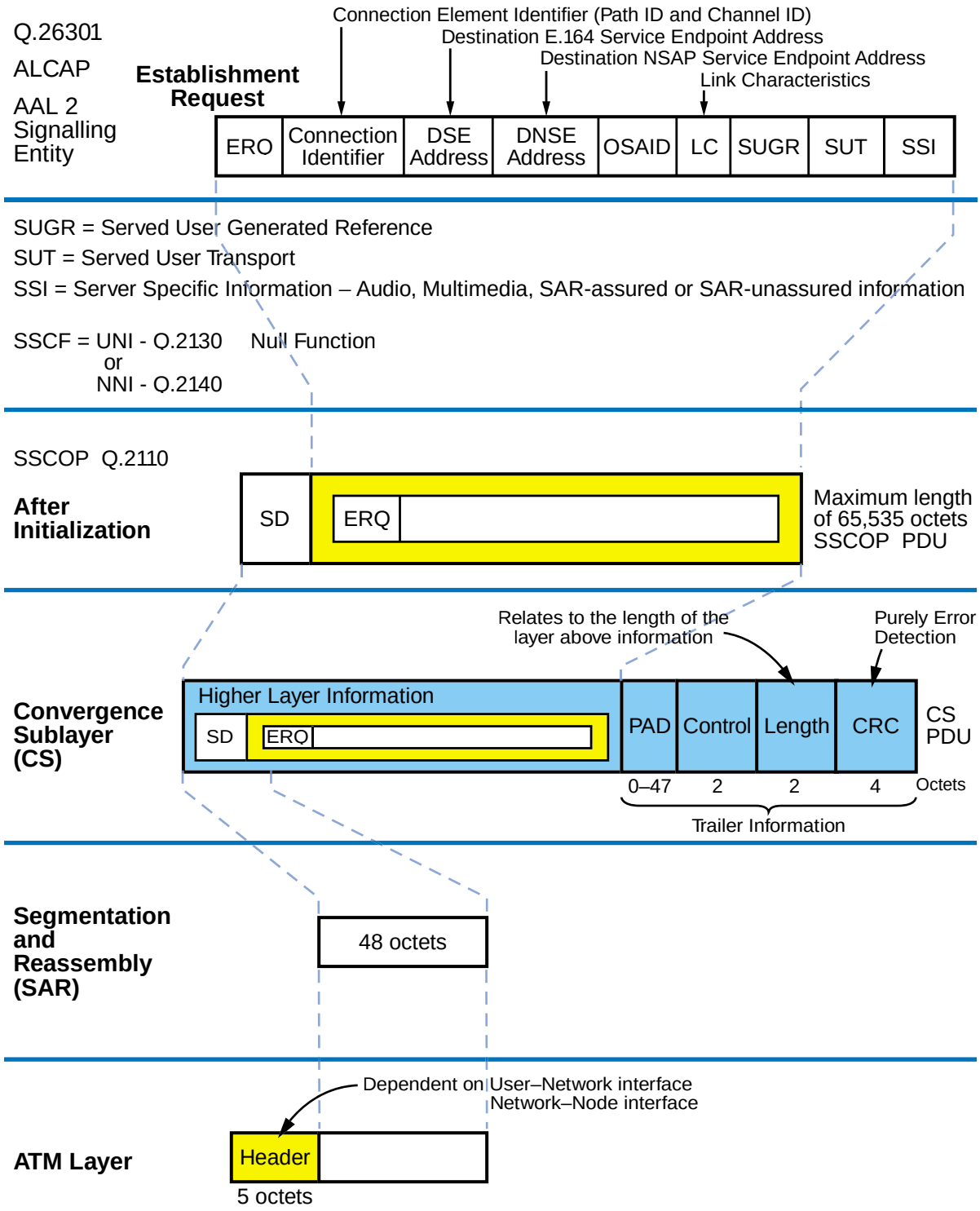


Figure 7

An Example of an AAL2 Signalling Message Delivery

© wray castle limited

© wray castle limited

LESSON 2

SS7

© wray castle limited

LESSON CONTENTS

1 Signalling System No. 7 (SS7) 4.2.1
1.1 Introduction 4.2.1
1.2 Structure of SS7 4.2.1
1.3 Overview of the Signalling Connection Control Part (SCCP) 4.2.3
1.4 Overview of the Message Transfer Part (MTP) 4.2.3

2 MTP Overview 4.2.5
2.1 Introduction 4.2.5
2.2 MTP Level 3 4.2.7

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe the basic structure of SS7
- describe the structure and function of the Message Transfer Part (MTP) levels 1, 2 and 3
- describe the functions of the Signalling Connection Control Part (SCCP)

1 SIGNALLING SYSTEM No. 7 (SS7)

1.1 Introduction

In SS7, signalling takes place between the Central Processing Units (CPUs) of different network elements via signalling terminals. Point codes are used to identify signalling terminals resident at different nodes (signalling points) in the network. In this way the signalling is effectively separated from the traffic circuits, and as long as the correct point codes are used, any signalling point in the network can communicate with any other.

1.2 Structure of SS7

The functions of the above two scenarios differ markedly from each other. It therefore makes sense to provide different higher-level message sets to deal with each, while retaining a common transport mechanism.

In practice, SS7 has a number of message sets specified for different applications, termed User Parts (UP) (provided for by level 4), and a common stable transport mechanism responsible for the routing of messages, called the Message Transfer Part (MTP), (provided for by levels 1–3).

So long as any message is passed from the UP to the MTP with the correct destination point code, user part identity and an indication of message routing requirements, MTP will provide the complete transport service. For non-circuit-related messages destined for outside the home network (where different signal point codes exist), an enhancement in the form of the Signalling Connection Control Part (SCCP) is required to generate the correct signalling points for MTP to route on.

© wray castle limited

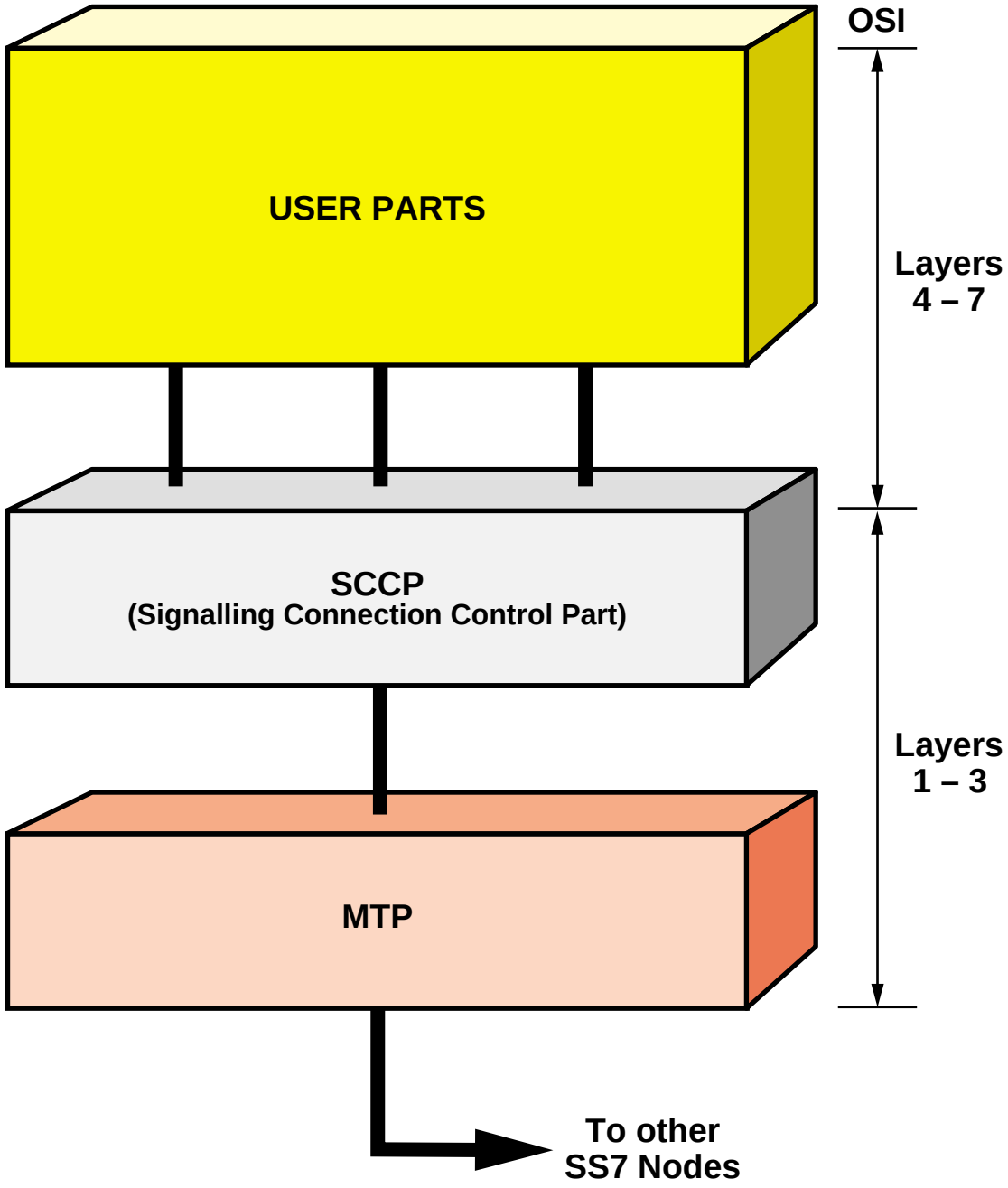


Figure 1
SS7 Structure

© wray castle limited

1.3 Overview of the Signalling Connection Control Part (SCCP)

The SCCP defines a means of transferring signalling data or management data without the need to establish a circuit. This *connectionless* mode of data transfer may be used in mobile networks, for example, for the updating of location registers. SCCP is really an addition to MTP, which results in a Network Service Part (NSP), which aligns correctly with layers 1–3 of the OSI Model.

Reference ITU-T Recommendations Q.711 – Q.714, 716
B-ISDN or Broadband SS7 Q.2200 – Q.2599

1.4 Overview of the Message Transfer Part (MTP)

MTP is split into two layers, MTP2 and MTP3. Each layer has specific functions or services.

MTP3 deals with delivery of the higher layer information to the correct signalling point, via the correct signalling link and to the correct user of MTP3.

MTP2's functions are to frame the higher layer information indicating the start and stop of the message; detect errors within the frame (via a CRC field); and delivery of the information sequence and without duplication.

Reference ITU-T Recommendations Q.701 – Q.704, 706, 707
Broadband MTP Q.2210

© wray castle limited

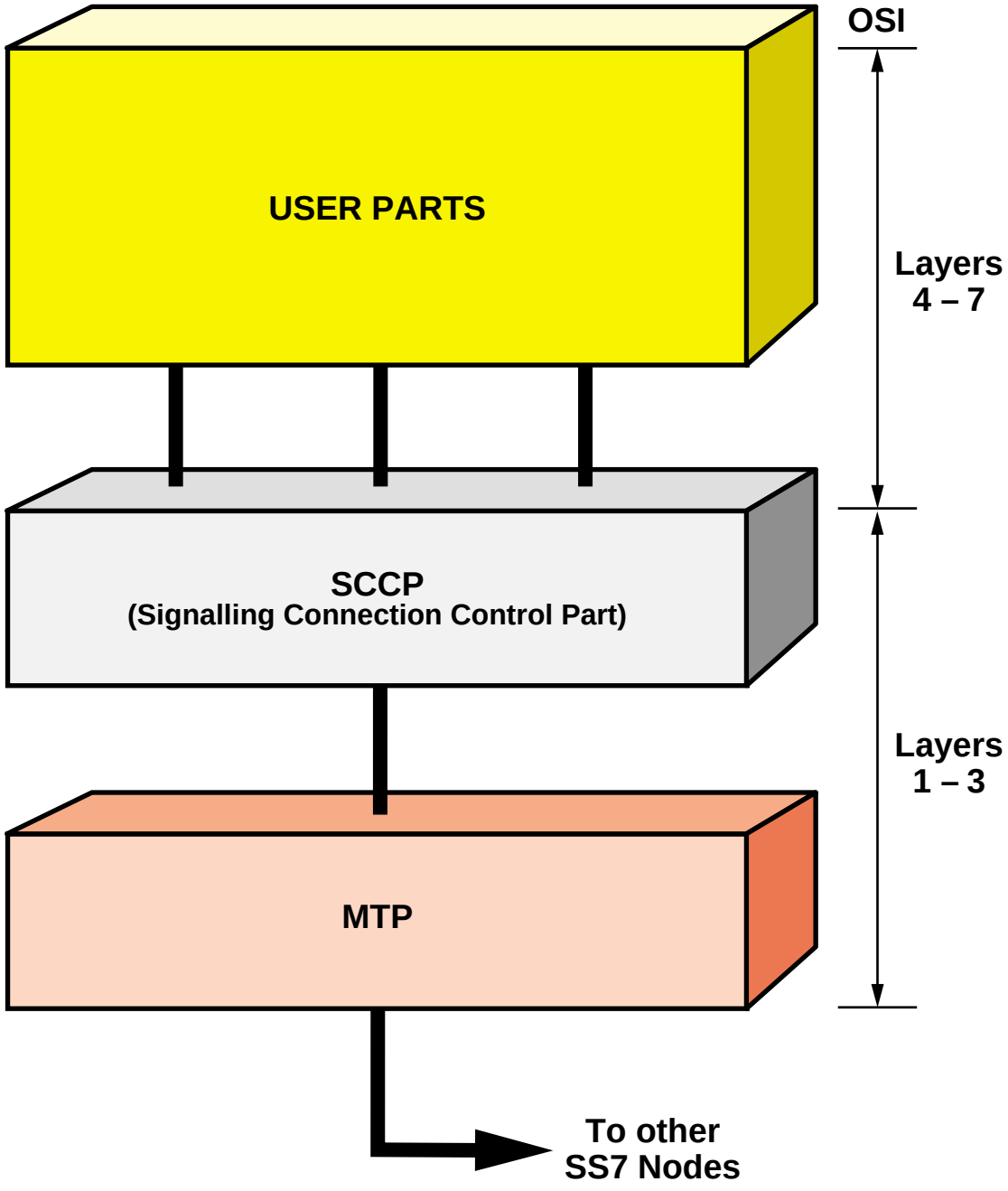


Figure 1 (repeated)
SS7 Structure

© wray castle limited

2 MTP OVERVIEW

2.1 Introduction

The lower levels of an SS7 signalling network consist of the MTP. The two main aims of MTP are:

1 To reliably transfer user part information across the SS7 network between signalling points, without error, in sequence and without duplication.

2 To manage network failures that would affect reliable transfer, in such a way that the transfer capability is maintained.

MTP consists of three functional levels:

Level 1 – Signalling Data Link
Level 2 – Signalling Link Functions
Level 3 – Signalling Network Functions

Level 3 of MTP consists of two main functions: Signalling Message Handling (SMH) and Signalling Network Management (SNM), which relate to the two aims identified above. Level 3 of MTP is the only level utilized in a broadband network as the lower layers are covered by ATM adaptation layers and ATM.

Figure 2 illustrates the structure of MTP.

© wray castle limited

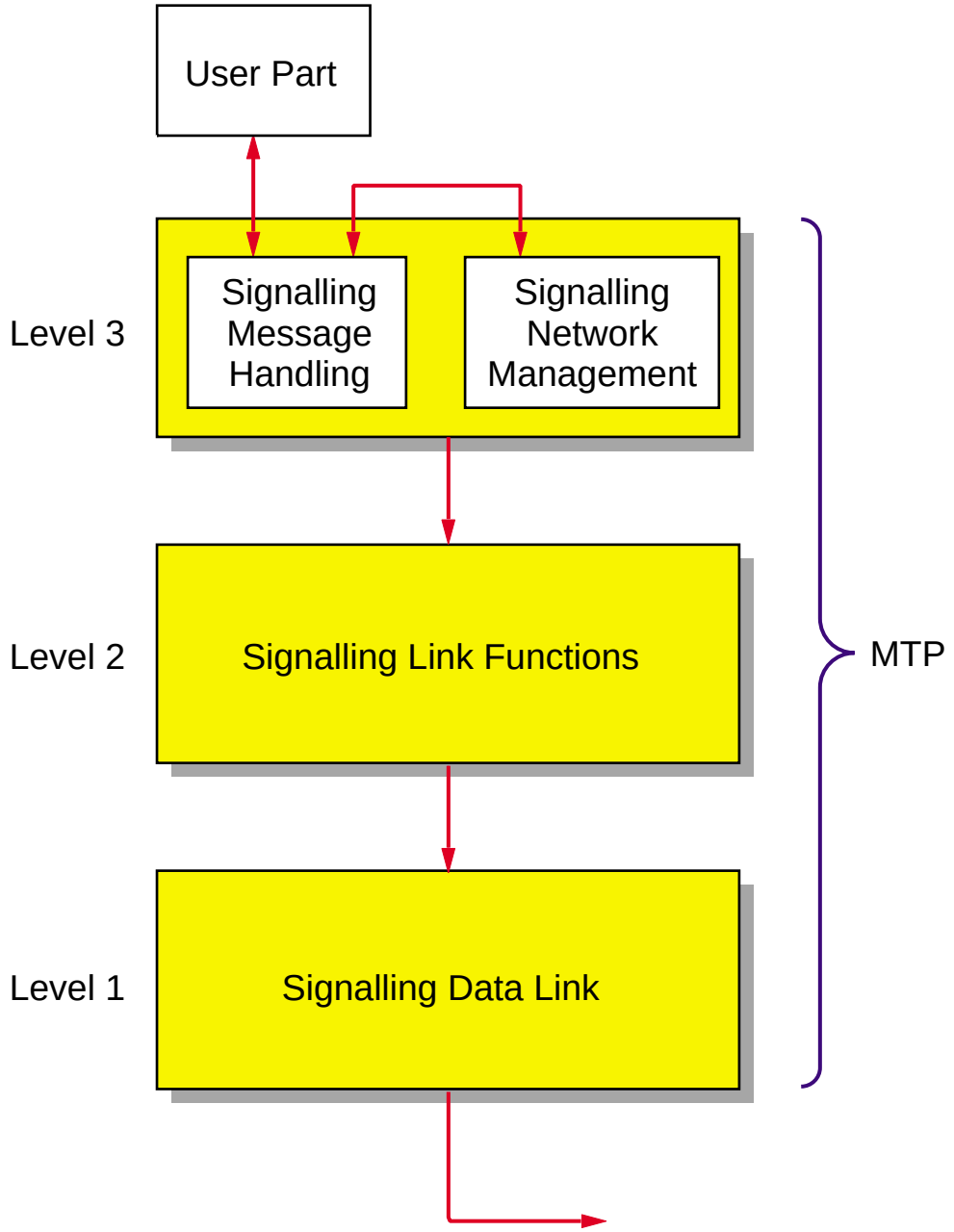


Figure 2
MTP Structure

© wray castle limited

2.2 MTP Level 3

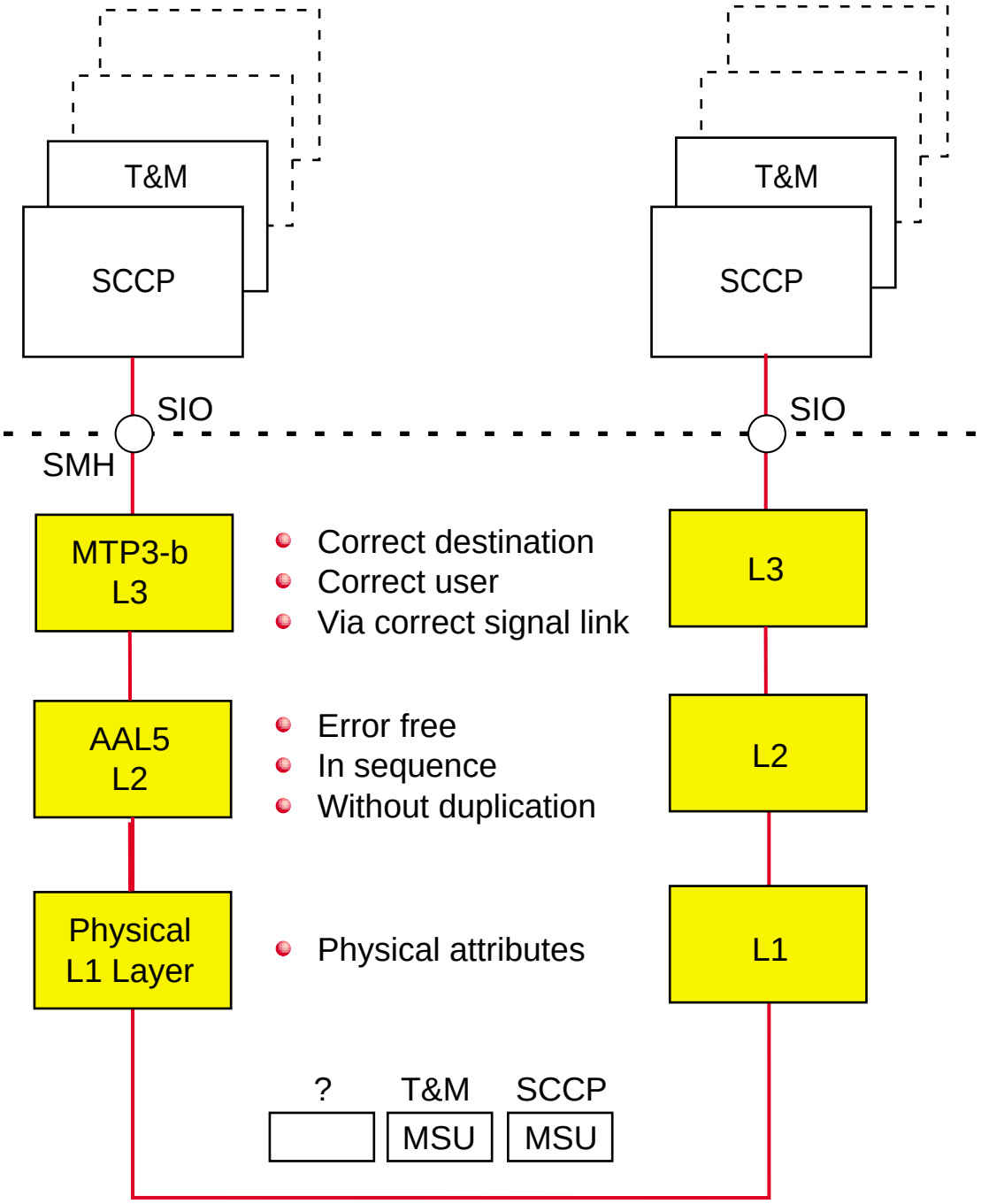
The primary function of MTP Level 3 is to transfer messages between user parts at different nodes by means of routing over appropriate links. As a secondary function Level 3 must monitor the status of a signalling network so that it can react to failures. Processes at Level 3 will then reconfigure or restore the signalling network so that normal transfer is either maintained or resumed.

MTP3, therefore, ensures the delivery of information:

- to the correct destination
- to the correct user
- via the correct signalling link

This is illustrated in Figure 3.

© wray castle limited



T&M – Test and Maintenance

Figure 3
Service Provided by MTP

© wray castle limited

© wray castle limited

LESSON 3

MTP3b AND M3UA

© wray castle limited

LESSON CONTENTS

1 Message Transfer Part Level 3 (MTP3) 4.3.1
1.1 Introduction 4.3.1
1.2 Signalling Message Handling (SMH) 4.3.3
1.3 Service Information Octet (SIO) 4.3.5

2 Message Transfer Part 3 Broadband (MTP3b) 4.3.7

3 Introduction to M3UA 4.3.9
3.1 Signalling Transport (SIGTRAN) Layer 4.3.9
3.2 Realization of Signalling Transport 4.3.11
3.3 Stream Control Transmission Protocol 4.3.15

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- identify how MTP Level 3 routes information to the correct point and user within a signalling network
- recognize the role of Signalling Message Handling (SMH) function within MTP Level 3
- examine the role of the SIGTRAN protocol stack in transferring signalling information across an IP network

© wray castle limited

1 MESSAGE TRANSFER PART LEVEL 3 (MTP3)

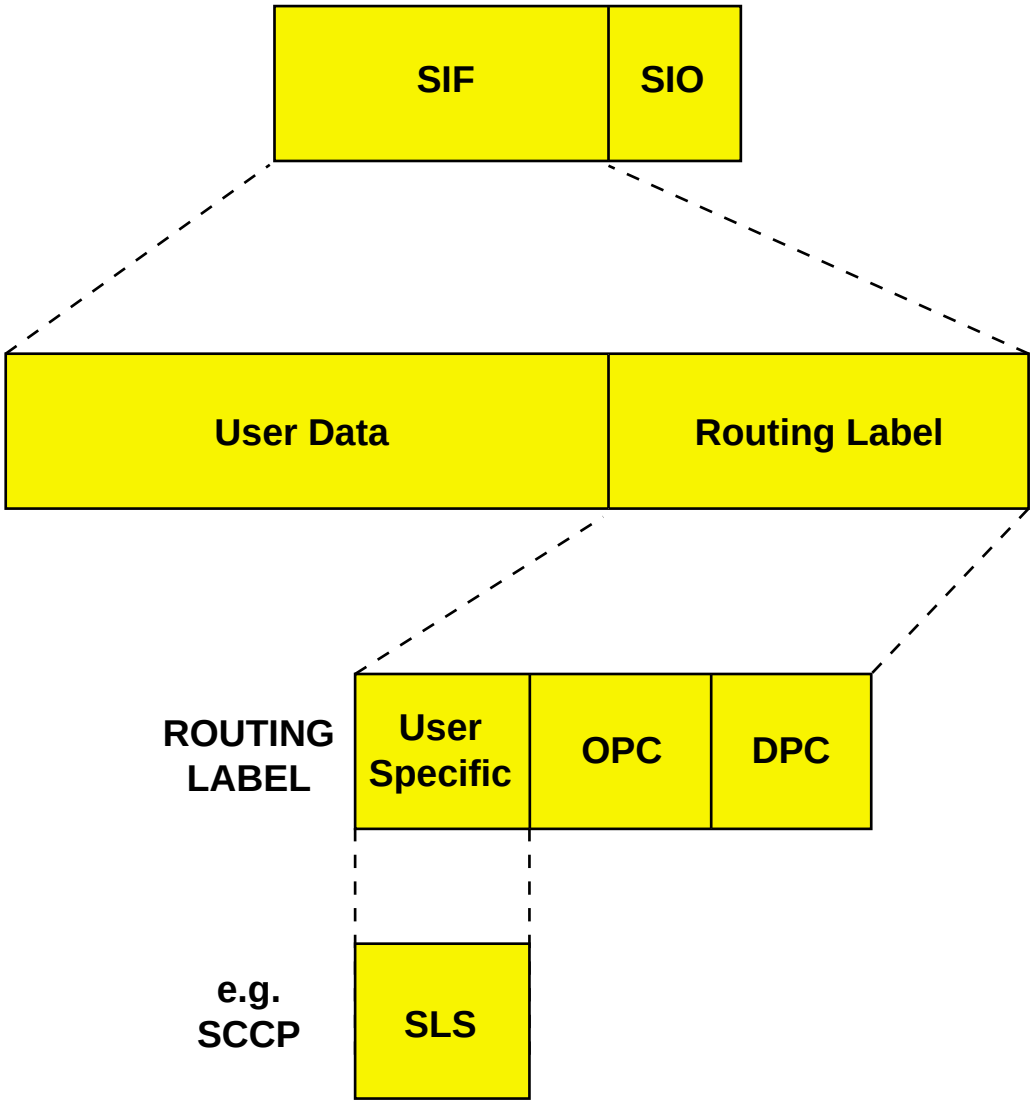
1.1 Introduction

Message Transfer Part Level 3 (MTP3) consists of two distinct functions, Signalling Message Handling (SMH) and Signalling Network Management (SNM).

SMH is responsible for delivering a message from a user part at an originating node, through the signalling network, to a user part at the destination node, via the correct signalling link(s).

This routing function is performed by using the Signalling Point Code (SPC) of both the origination and destination nodes. These codes are both contained in an element known as the label, which is a header in the message. Figure 1 shows the structure of this label.

© wray castle limited



DPC – Destination Point Code
OPC – Originating Point Code
SLS – Signalling Link Selection
SIO – Service Information Octet

Figure 1
MTP Routing Label

© wray castle limited

1.2 Signalling Message Handling (SMH)

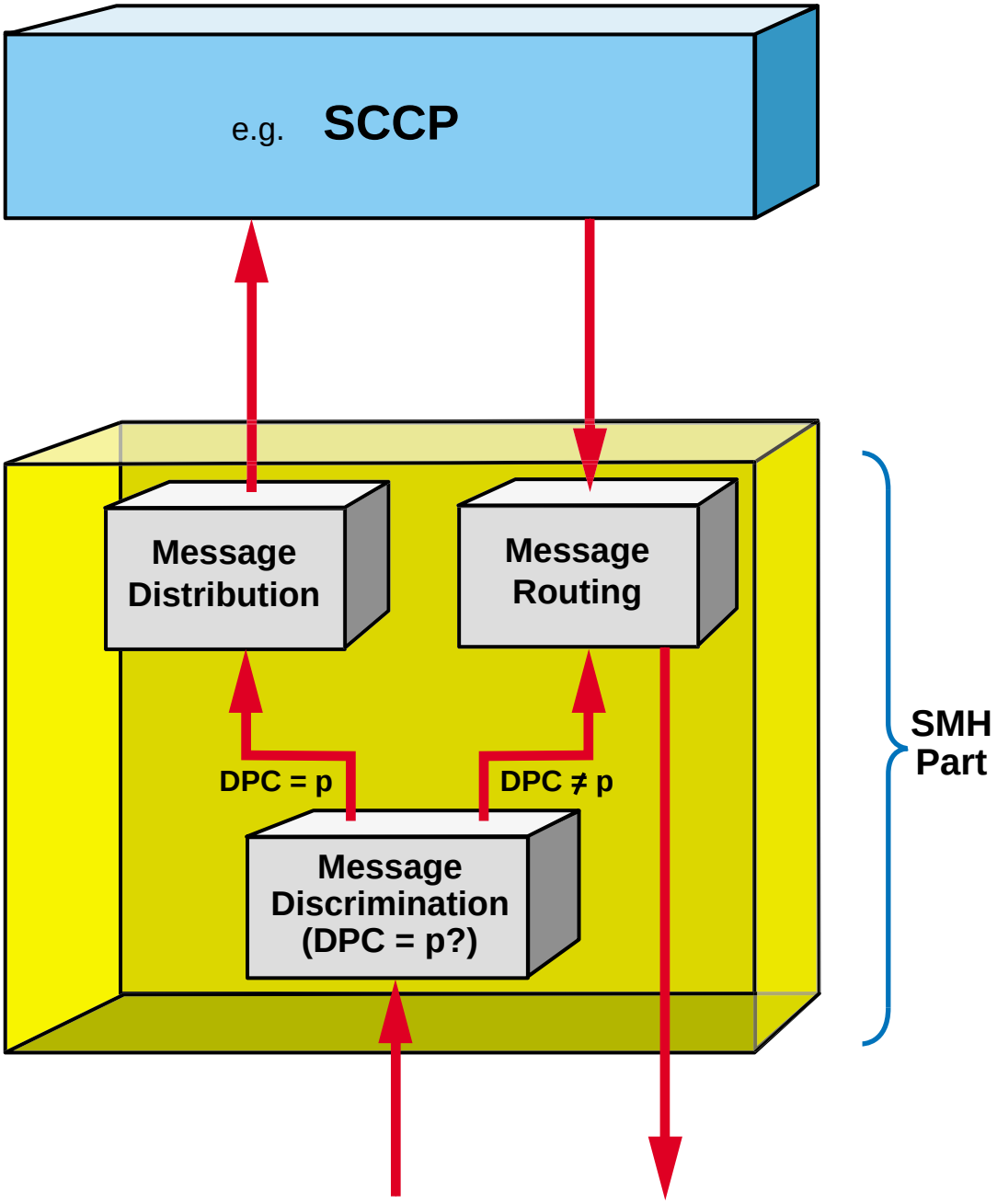
To achieve its functions, SMH consists of three elements:

- Message Routing
- Message Distribution
- Message Discrimination

The routing function at each node determines the signalling link to be used to route a message towards its intended destination. Distribution routes messages internally to the appropriate user parts. The discrimination elements look at the destination point code on each received message to determine whether this node is the destination (in which case the message is given to the distribution element), or if the message is to be forwarded on to another node (by means of the routing function).

Figure 2 illustrates the relationship between these three elements, the signalling links and the user parts.

© wray castle limited



Signalling Point Code for this node = p

Figure 2
Level 3 Signalling Message Handling (SMH)

© wray castle limited

1.3 Service Information Octet (SIO)

The message set (i.e. User Part) being carried by MTP is indicated by a parameter known as the Service Information Octet (SIO), specifically the Service Indicator Field of the SIO.

Figure 3 shows the codings of the Service Indicator Field (SIF) within the SIO. Within the Sub-Service Field (SSF), the most significant bit is used to distinguish between national and international networks.

© wray castle limited

Service Indicator				Allocation
A	B	C	D	
0	0	0	0	Signalling Network Management
0	0	0	1	Signalling Network Testing and Maintenance
0	0	1	0	Spare
0	0	1	1	SCCP
0	1	0	0	TUP/NUP
0	1	0	1	ISDN-UP
0	1	1	0	DUP (Call- and Circuit-Related)
0	1	1	1	DUP (Facility Registration and Cancellation)
1	0	0	0	Spare
1	0	0	1	Spare
1	0	1	0	Spare
1	0	1	1	Spare
1	1	0	0	Spare
1	1	0	1	Spare
1	1	1	0	Spare
1	1	1	1	Spare

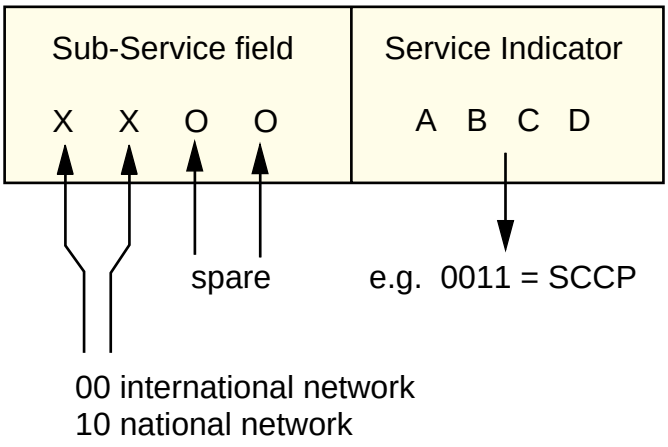


Figure 3
Service Information Octet (SIO)

© wray castle limited

2 MESSAGE TRANSFER PART 3 BROADBAND (MTP3b)

The maximum amount of user data supported by MTP level 3 for signalling links that provide the services of Recommendation Q.2140 is 4,091 octets. Note the maximum SDU size (including the SIO) supported by SSCF at NNI is 4,096 octets.

MTP3b also covers network management procedures such as traffic status (congestion), signalling link status (inhibit/uninhibit) and signalling route management (e.g. controlled/forced re-routing).

© wray castle limited

General Format and Coding Conventions of Messages Conveying Peer-to-Peer Information of User Parts

8	7	6	5	4	3	2	1	Bit / Octet
MSB	Sub-service Field		LSB	MSB	Service Indicator		LSB	1
DPC							LSB	2
OPC	LSB	MSB	DPC					3
OPC								4
MSB	SLS		LSB	MSB	OPC			5
User Data								6
User Data								...
User Data								n

General Format and Coding Conventions of Signalling Network Management Messages

8	7	6	5	4	3	2	1	Bit / Octet
MSB	Sub-service Field		LSB	MSB	Service Indicator		LSB	1
DPC							LSB	2
OPC	LSB	MSB	DPC					3
OPC								4
MSB	SLC		LSB	MSB	OPC		LSB	5
MSB	Heading Code H1		LSB	MSB	Heading Code H0		LSB	6
								(Note) 7
								(Note) ...
MSB								(Note) m

Note: The octets numbered from 7 to m may not be present or may consist of one or more than one octet, depending on the type of signalling network management message.

Figure 4

Message Code Formats

© wray castle limited

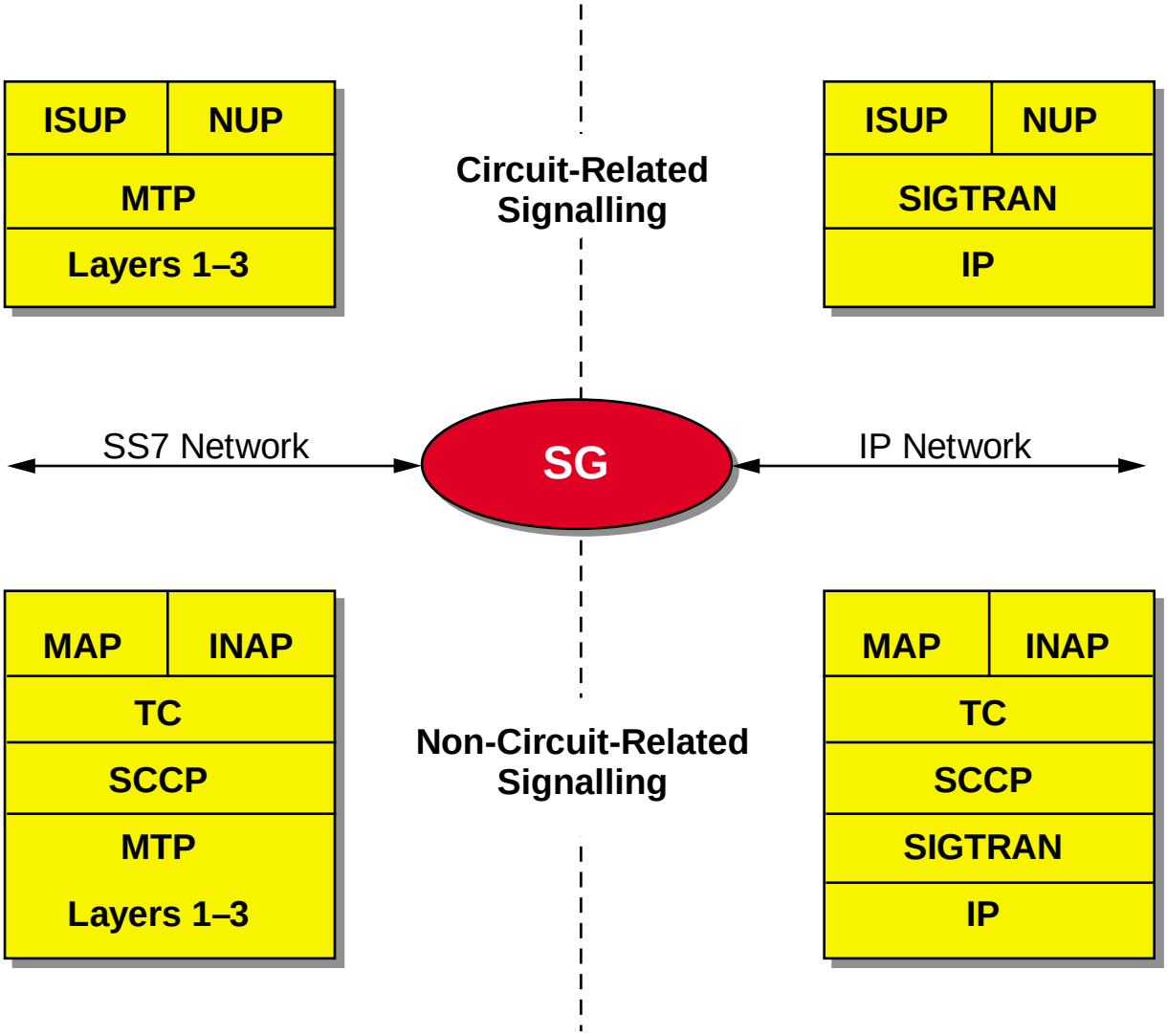
3 INTRODUCTION TO M3UA

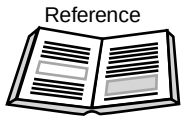
3.1 Signalling Transport (SIGTRAN) Layer

Signalling passed between the SS7 and IP networks will do so via the Signalling Gateway. Within the SS7 network, the underlying layers are realized through the use of MTP and offer services such as the in-sequenced delivery of SS7 messages, without error and without repetition.

The IP network was designed using its own layer protocols. As such, MTP and the services it offers within the SS7 network need to be provided by an alternative layer within the IP network. The layer providing these services therefore sits between the SS7 protocols being transferred and the IP layer protocol performing the transfer. The IETF have identified this layer as the Signalling Transport (SIGTRAN) layer.

© wray castle limited





draft-ietf-sigtran-m3ua

Figure 5
Signalling Transport (SIGTRAN)

© wray castle limited

3.2 Realization of Signalling Transport

In essence, the Signalling Transport Layer supports primitives from the higher SS7 layers, negating the need to modify these layers, and it supplements the IP network transport protocols to cater for the service requirements of the above SS7 layers.

Signalling Transport is itself realized through the use of two protocols, SS7 MTP3 User Adaptation (M3UA) and SCTP. The former provides the SS7 primitive support function, while the later provides both the reliable transport and IP interface functions.

It should be noted that M3UA is shown here carrying SS7 information normally seen within the user data field of an MTP layer 3 message. As such, M3UA deals with MTP layer 3 primitives. Alternative User Adaptation (UA) layers may therefore be seen if signalling systems other than SS7 are being supported.

M3UA bases its routing choice on a routing key. This key consists of parameters, example of which may be a DPC, DPC and OPC, DPC and CIC range. Within M3UA, the routing key is mapped to an address identifying the appropriate terminating node.

© wray castle limited

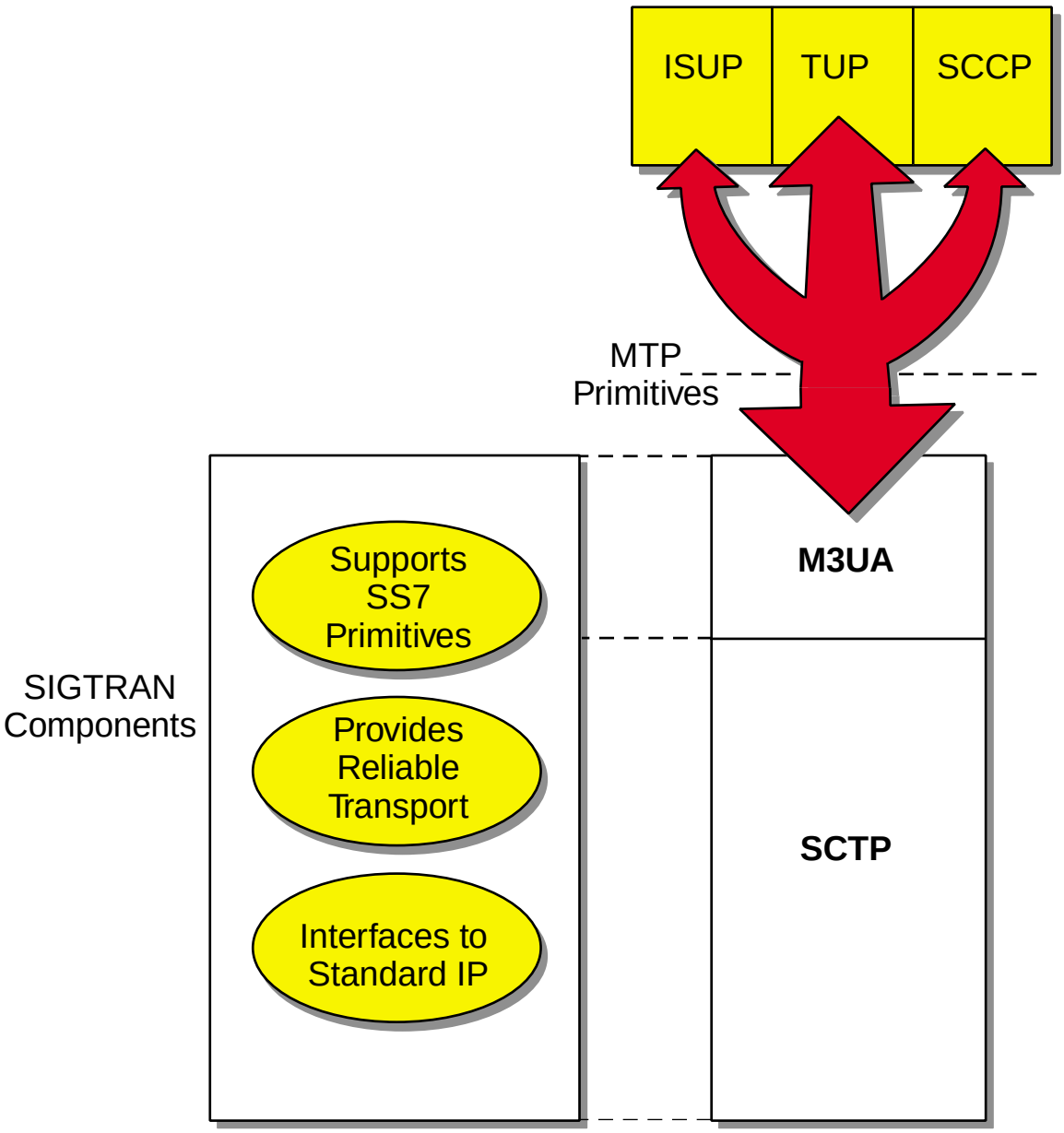


Figure 6
Realization of Signalling Transport

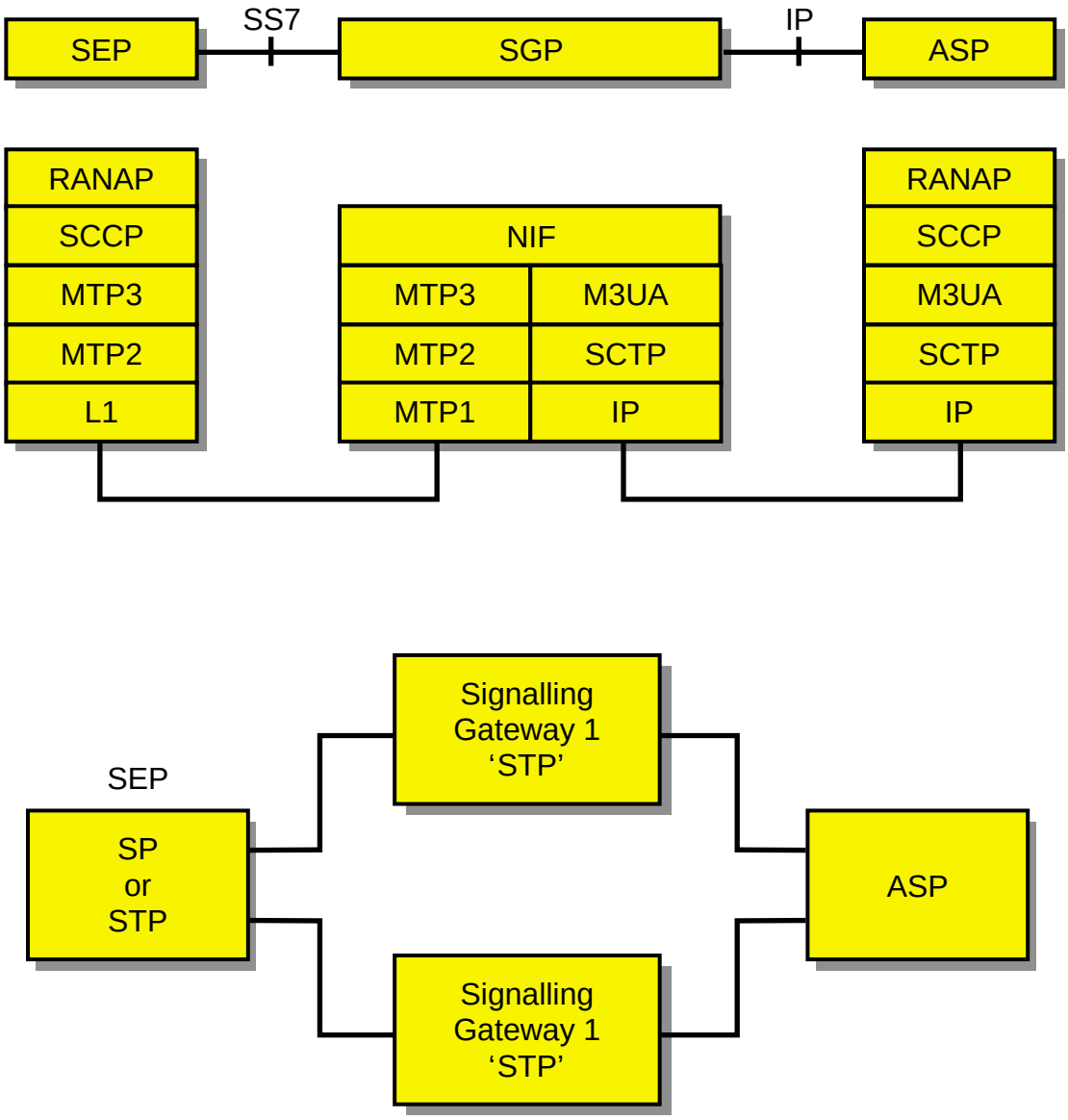
© wray castle limited

The transfer of SS7 or signalling messages across an IP network requires that the traditional protocol stack be split. The result is that the lower layers (MTP) appear only at the entry point of the IP network, within the signalling gateway point/unit, while the higher layer protocols, e.g. SCCP, are passed on and only require processing at some internal element such as an MGC. In other words, the two parts of the split SS7 stack reside remotely to one another.

Figure 7 shows an example of information being transported from an SS7 network to an IP network, which could go via another signalling gateway (similar in functionality to an STP) before reaching its destination point, such as an application server process.

The application server process is the termination point of the message where the information is processed, for example a virtual database that could handle HLR transactions.

© wray castle limited



SEP – Signalling End Point
SGP – Signalling Gateway Point
ASP – Application Server Process
NIF – Nodal Interworking Function

Figure 7

Information Transfer between SS7 and IP Networks

© wray castle limited

3.3 Stream Control Transmission Protocol

SCTP, like TCP, is connection-oriented in nature, and runs over the connectionless service of IP. However, unlike TCP, which allows only a single session between two hosted applications (described by an IP address and port number), SCTP is able to provide multiple sessions (described by Session Identifiers). These sessions are multiplexed over what is termed an 'association'.

Multiple sessions within an association allow signalling to be separated, perhaps sending time-critical information over one session and non-time-critical information over another. This has the advantage of overcoming head-of-line blocking and has the added benefit of conserving port numbers. Each session is described through a single graceful start-up in which an association between the two hosts is agreed, (security information, transport addresses and port addresses to be used) and torn down through a single graceful take-down process. Functionally, therefore, SCTP provides the following:

Sequenced Delivery within Streams
The term *stream* is used in SCTP to refer to a sequence of user messages referenced by Stream Sequence Numbers (SSN) that are to be delivered to the upper layer. This is in contrast to TCP, where it refers to a sequence of bytes. The multiplexed sessions allow delivery from one stream, while another stream may be blocked, waiting the next in-sequence user message. SCTP also has the ability to bypass sequential delivery if required.

User Data Fragmentation
When needed, SCTP fragments user messages to ensure that the SCTP packet passed to the lower layer conforms to the path Maximum Transmission Unit (MTU). On receipt, fragments are reassembled into complete messages before being passed to the SCTP user.

Acknowledgement
SCTP assigns a Transmission Sequence Number (TSN) to each user data fragment or message. The TSN is independent of any stream sequence number assigned at the stream level. In this way, reliable delivery is kept functionally separate from sequenced stream delivery.

Chunk Bundling
The SCTP packet as delivered to the IP layer consists of chunks. Each chunk may contain either user data or SCTP control information. SCTP may bundle more than one user message into a single SCTP packet if the MTU allows. The chunk bundling function of SCTP is responsible for assembly of the complete SCTP packet and its disassembly at the receiving end.

© wray castle limited

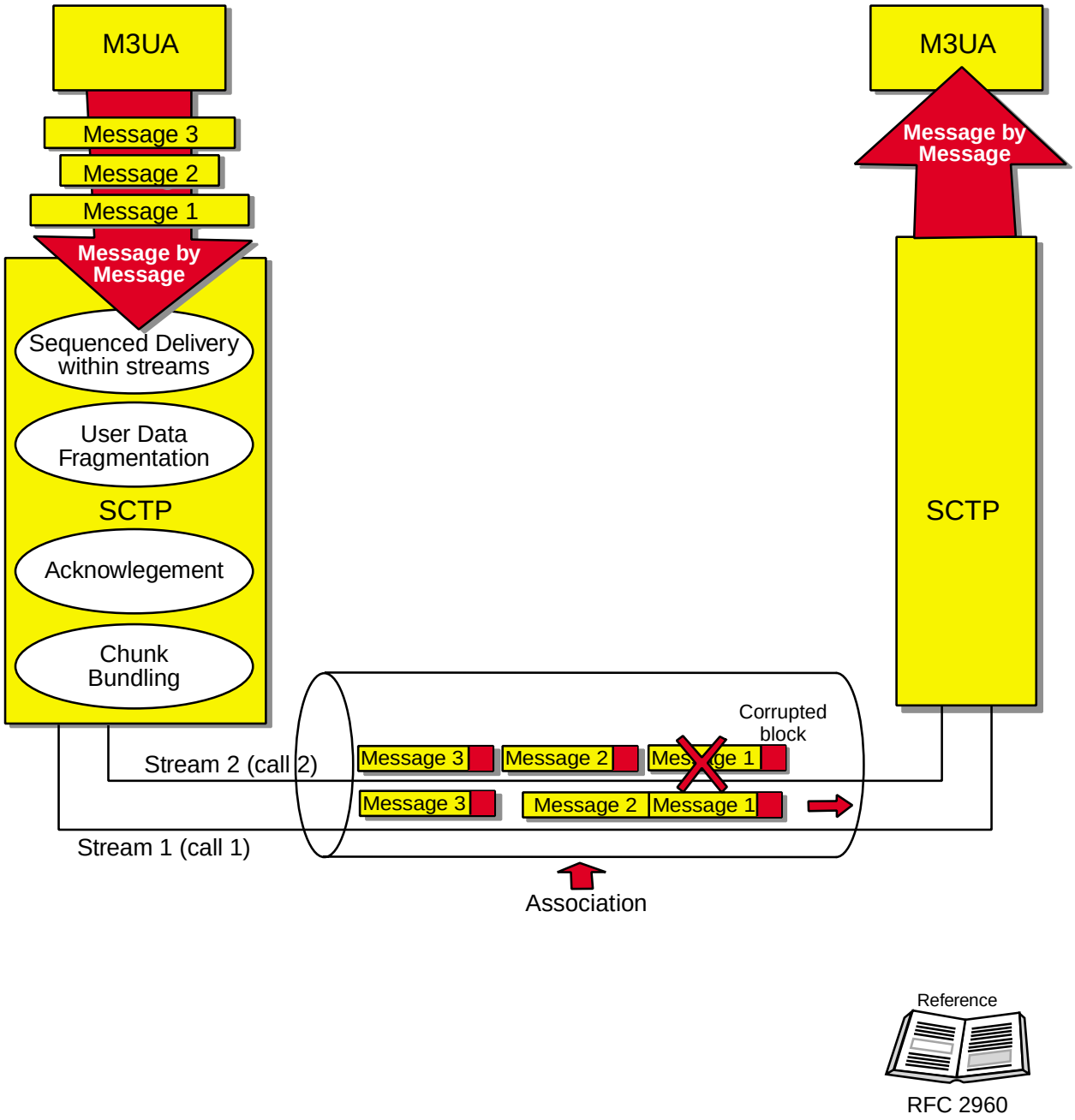


Figure 8

Functional View of SCTP

© wray castle limited

© wray castle limited

LESSON 4

SIGNALLING CONNECTION CONTROL PART (SCCP)

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Signalling Connection Control Part (SCCP) 4.4.1
1.1 Introduction 4.4.1
1.2 SCCP Structure 4.4.3
1.3 SCCP Services 4.4.3
1.4 SCCP Procedures in the UTRAN 4.4.9
1.5 Parameters for Routing 4.4.11
1.6 Global Titles (GT) 4.4.13
1.7 Subsystem Numbers (SSNs) 4.4.13
1.8 Translation 4.4.13
1.9 Called Party Address (CDA) 4.4.15
1.10 Identifying Users of SCCP 4.4.21

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe how SCCP supports signalling messages on the Iu and Iur interfaces

1 SIGNALLING CONNECTION CONTROL PART (SCCP)

1.1 Introduction

The SCCP is a functional block of SS7, which adds to the functionality of MTP3b. SCCP may also sit on M3UA.

The SCCP is used to support signalling messages on the Iu and Iur interfaces. RANAP and Radio Network Subsystem Application Part (RNSAP) messages use the services of SCCP. SCCP will establish one signalling connection for a UE per interface. Signalling messages may be transferred by means of logical connections, which may operate in a connectionless or connection-oriented mode.

Connectionless and connection-oriented procedures are used to support RANAP and RNSAP. 3GPP Specifications TS 25.413 ‘UTRAN Iu Interface RANAP Signalling’ and TS 25.423 ‘UTRAN Iur Interface RNSAP Signalling’ specify whether connection-oriented or connectionless services should be used for a layer 3 procedure.

© wray castle limited

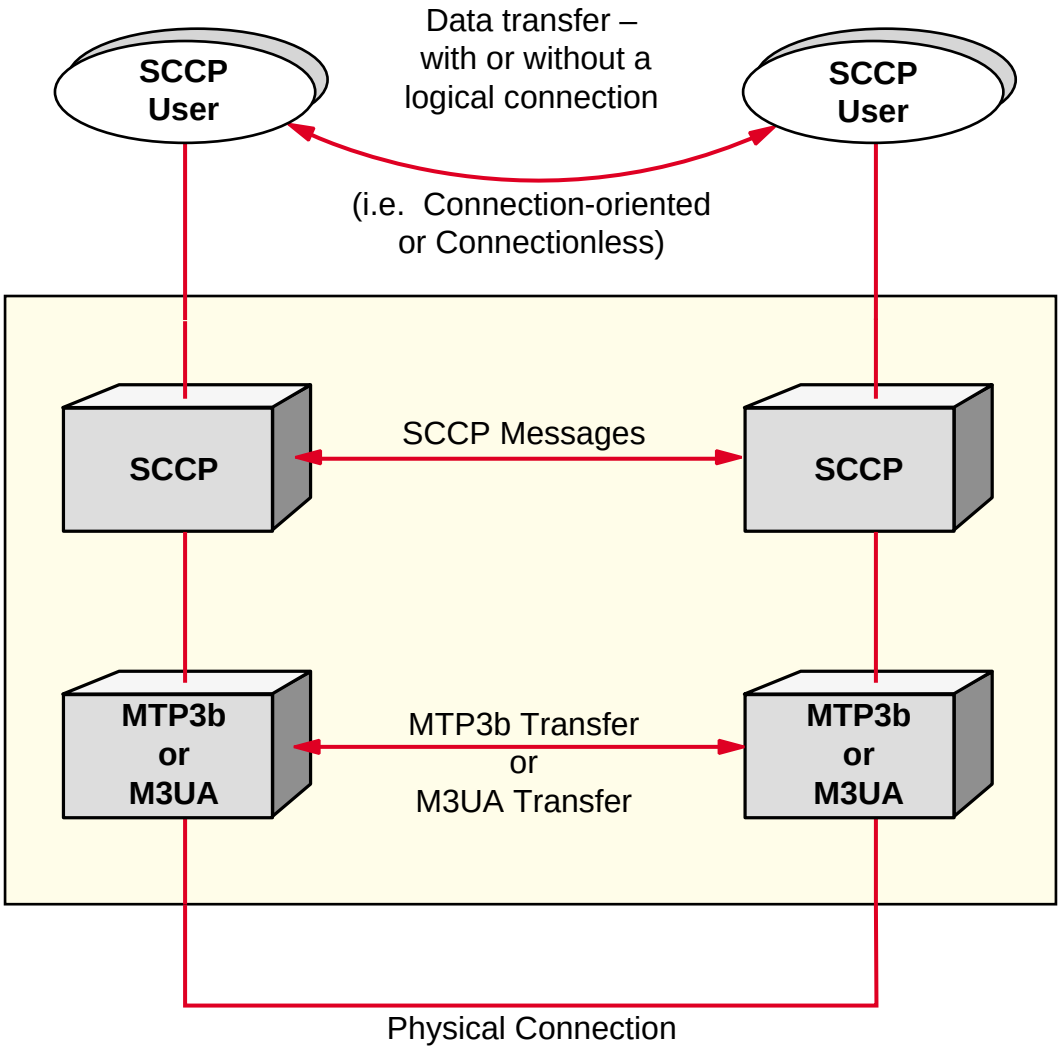


Figure 1
SCCP

© wray castle limited

1.2 SCCP Structure

Figure 2 shows the structure of SCCP. The four internal functions of SCCP deal with connection-oriented transfer, connectionless transfer, routing and SCCP management.

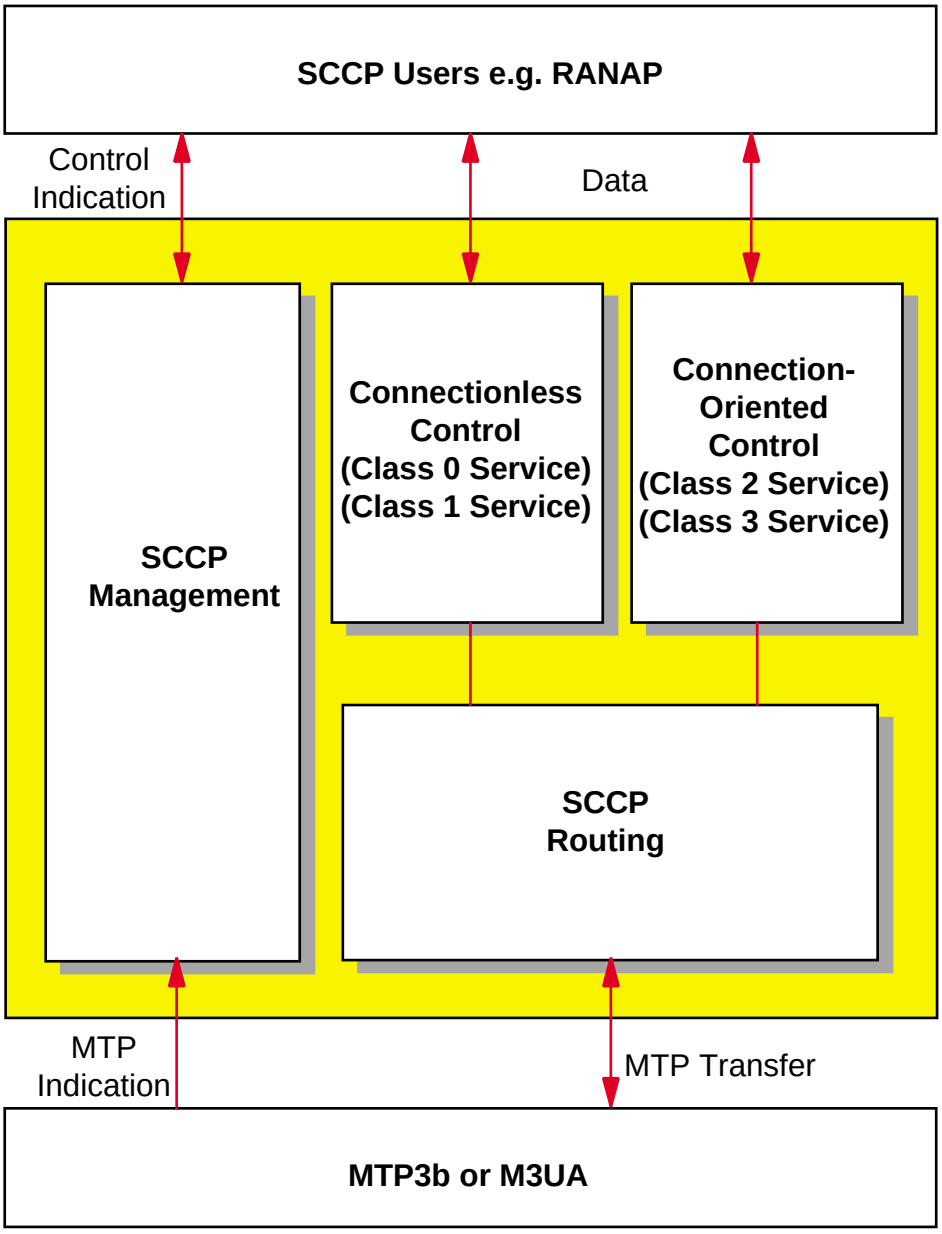
The transfer elements allow SCCP to interface to its users and offer either connection-oriented or connectionless service. The management element translates MTP indications (Pause, Resume and Status) to controls/indications from/to the user parts.

1.3 SCCP Services

SCCP offers users four classes of service, two of which are connectionless, the other two being connection-oriented.

- Class 0 SCCP = Basic Connectionless
- Class 1 SCCP = Sequenced (MTP) Connectionless
- Class 2 SCCP = Basic Connection-Oriented
- Class 3 SCCP = Flow Control Connection-Oriented

© wray castle limited



Class 0 SCCP – Basic Connectionless
Class 1 SCCP – Sequenced (MTP) Connectionless
Class 2 SCCP – Basic Connection-Oriented
Class 3 SCCP – Flow Control Connection-Oriented

Figure 2
SCCP Structure

© wray castle limited

1.3.1 Class 0

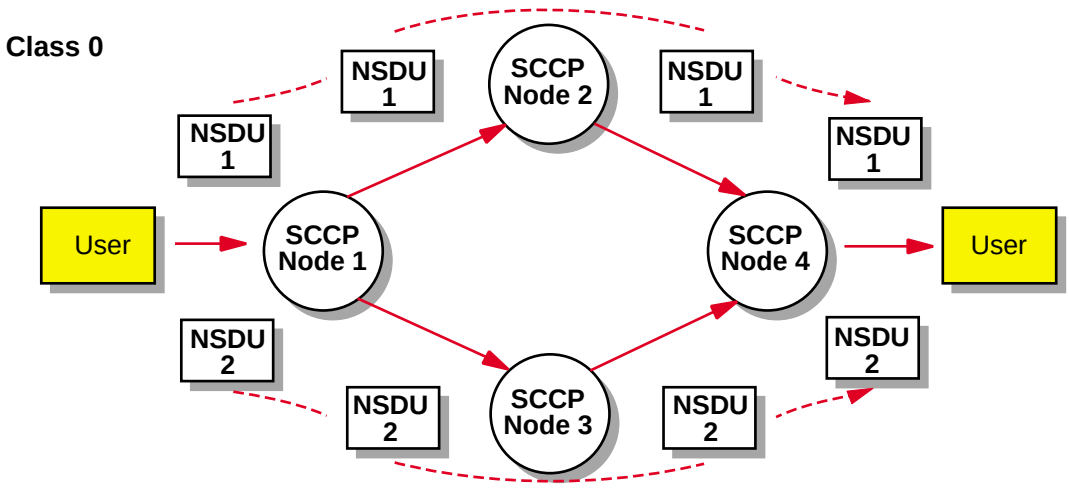
The connectionless protocol classes provide the capability to transfer one block of data between two SCCP users. This block of data is referred to as a Network Services Data Unit (NSDU). See Figure 3.

In the connectionless service, SCCP will transfer NSDUs between users without first establishing a connection between those users. Every message sent must contain an address for SCCP to route on.

With Class 0 operation, each NSDU that passes between users is dealt with separately for routing through the signalling network and therefore may be delivered non-sequentially.

SCCP connectionless services are used throughout the UTRAN.

© wray castle limited



Note NSDU 1 and 2 could arrive out of sequence. No logical connections are established

Figure 3
Connectionless Service

© wray castle limited

1.3.2 Class 2

Class 2 supports the transfer of NSDUs in connection-oriented mode. SCCP is responsible for setting up and clearing down the logical connections.

In Figure 4a, at the request of the SCCP User, SCCP Node 1 (N1) establishes a logical connection by sending a Connection Request (CR) message to SCCP Node 2 (N2) and assigns a Source Local Reference (SLR) to the request. The remote node confirms the connection by sending a Connection Confirm (CC) message and includes its own SLR and a Destination Local Reference (DLR) equal to the SLR of SCCP N1. Both nodes now have a reference for this connection.

The CR message must contain the address of the destination SCCP node and the user. Subsequent data messages associated with the connection need only send the SLR and/or DLR. The clear-down messages contain both SLR and DLR. If intermediate nodes are involved they make associations between pairs of SLR/DLRs to establish the logical connection (see Figure 4b).

The use of SLR and DLR allows SCCP nodes to establish multiple simultaneous logical connections, i.e. to multiplex logical connections onto a single physical connection. This function is particularly important over the A-interface, where many simultaneous SCCP connections are required to support dedicated signalling channels to mobile stations.

Class 2
Class 2 operation provides a SAR service for messages too long to fit in the MTP user data field 2^{12} (MTP3b) or 2^{32} (M3UA).

© wray castle limited

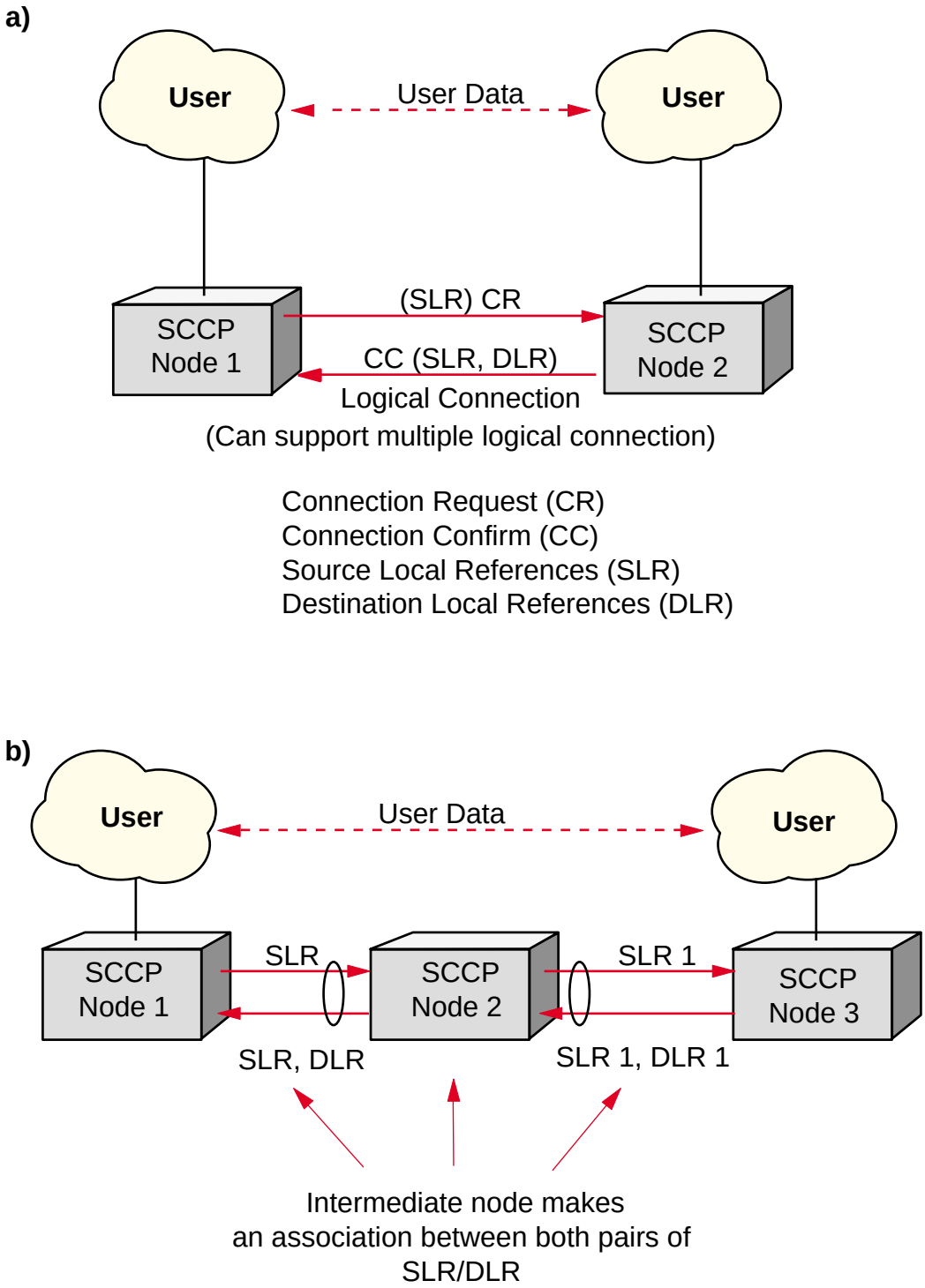


Figure 4
Connection-Oriented Data Transfer

© wray castle limited

1.4 SCCP Procedures in the UTRAN

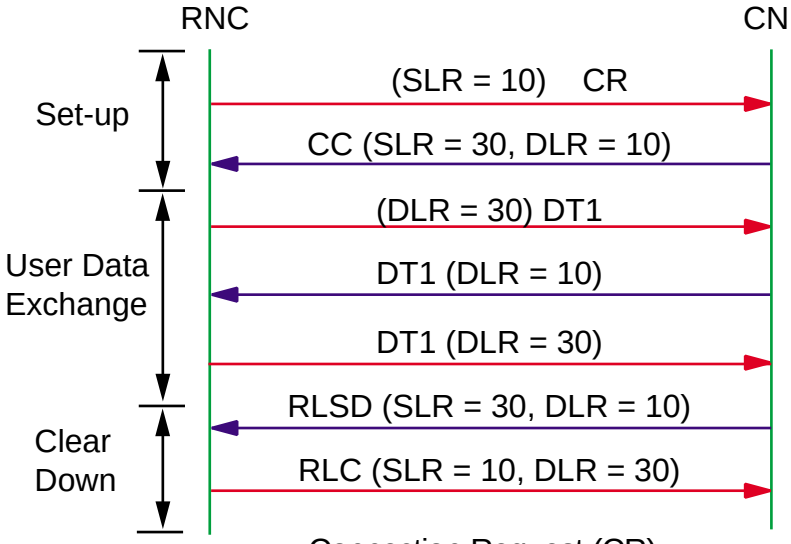
SCCP procedures may be considered on the Iu and Iur interfaces, in connection-oriented and connectionless modes. The UTRAN uses SCCP in modes 0 or 2.

A typical exchange of SCCP connection-oriented messages across the Iu interface is shown in Figure 5a. SCCP connection establishment may be initiated by the RNC or the CN. However, the the SCCP connection release procedure is always initiated at the CN.

Figure 5b shows RANAP messages being transferred across the Iu interface in SCCP connectionless mode. SCCP makes no association between UnitData (UDT) messages.

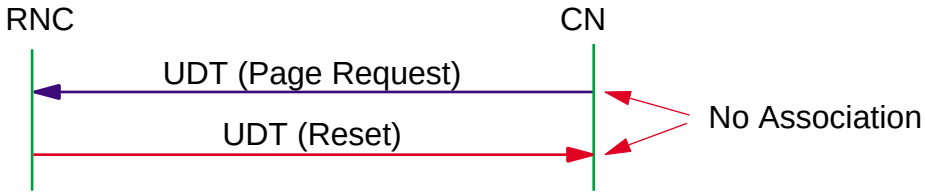
© wray castle limited

a) Iu Interface Connection-Oriented Procedures



Connection Request (CR)
Connection Confirmed (CC)
Dataform 1 (DT1)
Released (RLSD)
Release Complete (RLC)
Source Local Reference (SLR)
Destination Local Reference (DLR)

b) Iu Interface Connectionless Procedures



UnitData (UDT)

Figure 5
SCCP Procedures

© wray castle limited

1.5 Parameters for Routing

Routing in SS7 may be considered at two levels:

- MTP3b
- SCCP

1.5.1 MTP3b

An application is resident at a signalling point. In order to route to a given signalling point, MTP requires a Destination Point Code (DPC). It is the responsibility of SCCP to provide MTP with the correct DPC and Signalling Link Selection (SLS). The DPC passed to MTP may not correspond to the final destination point for the message. In this case it would represent the next SCCP node at which a further point code may be generated for onward routing.

1.5.2 SCCP

SCCP is capable of routing on either:

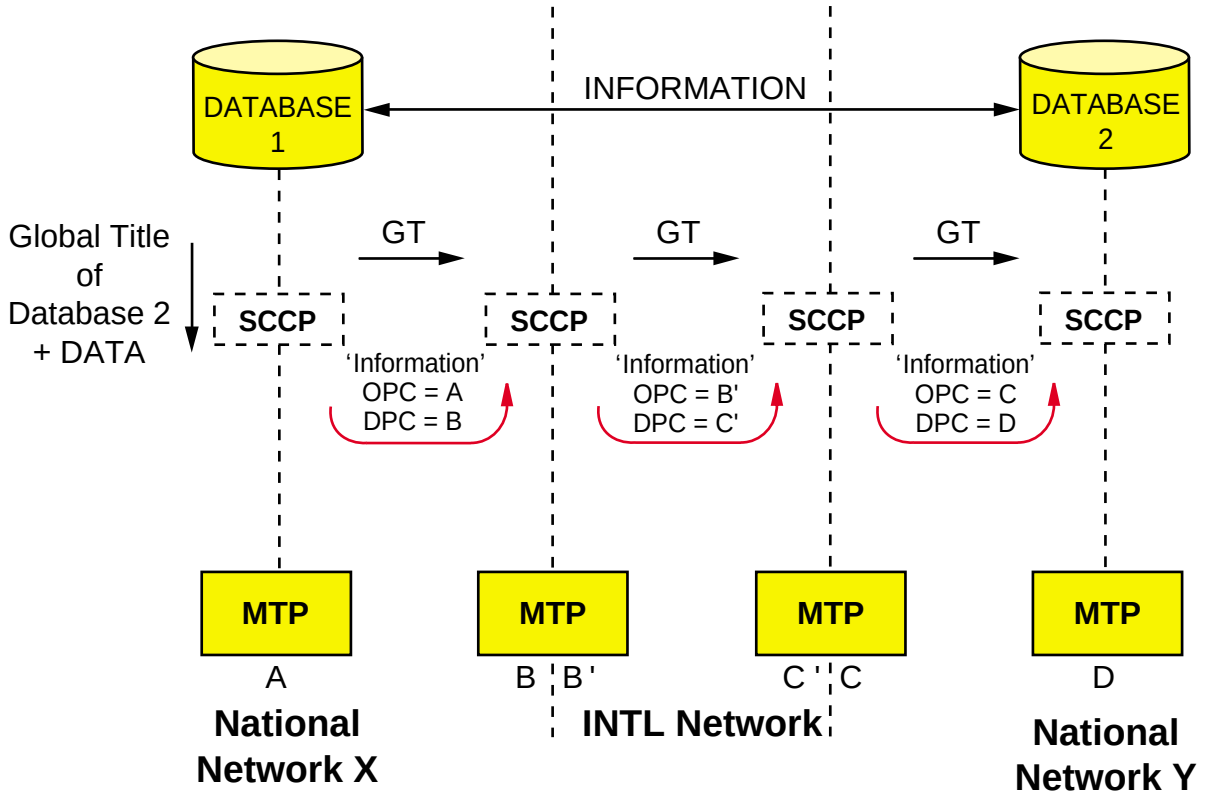
- Global Titles (GT), or
- Subsystem Number (SSN) and Point Codes

Intermediate SCCP nodes may route on a GT, while the destination node is more likely to route on the combination of SSN and Signalling Point Code.

In Figure 6, SCCP addressing information for legs A–B and B–C would most probably contain only the GT and SSN of Database 2, since the PC of D could not be generated at this stage.

At C, the PC of D could be generated (C and D in same network) and this is now inserted into the SCCP addressing information, as well as being passed to MTP in order to route towards SCCP at Node D. The routing indicator is changed at C to instruct SCCP at D to route on PC and SSN.

© wray castle limited



Since Node A cannot provide the point code of D (Network X has no knowledge of PCs in Network Y), the Global Title of Database 2 is translated at SCCP into the relevant point code for MTP to route on at each stage.

Figure 6

Database Communication – Enhanced Routing Required

© wray castle limited

1.6 Global Titles (GT)

In order to route messages, SCCP must know to which node, and to which application on that node, a message is destined. The application process generates the destination address and transfers it to SCCP. The user may supply address information to SCCP in the form of Point Codes (PC) or Global Titles (GT).

Most applications have no knowledge of point code addressing and will generally address a remote application using a GT. The GT identifies a particular application resident on a particular node in a particular network. Generally, then, the SCCP user will generate a GT for SCCP to route on. The GT may be one of the following formats:

E.163/4	ISDN/Telephony Numbering Plan
X.121	Data Numbering Plan
F.69	Telex Numbering Plan
E.210/1	Maritime Mobile Numbering Plan
E.212	Land Mobile Numbering Plan
E.214	ISDN/Mobile Numbering Plan

1.7 Subsystem Numbers (SSNs)

Any application that uses the services of SCCP is known to SCCP as a subsystem and is allocated a Subsystem Number (SSN).

1.8 Translation

The SCCP contains a number of translation tables and is able to translate GTs supplied by an application process (Figure 7).

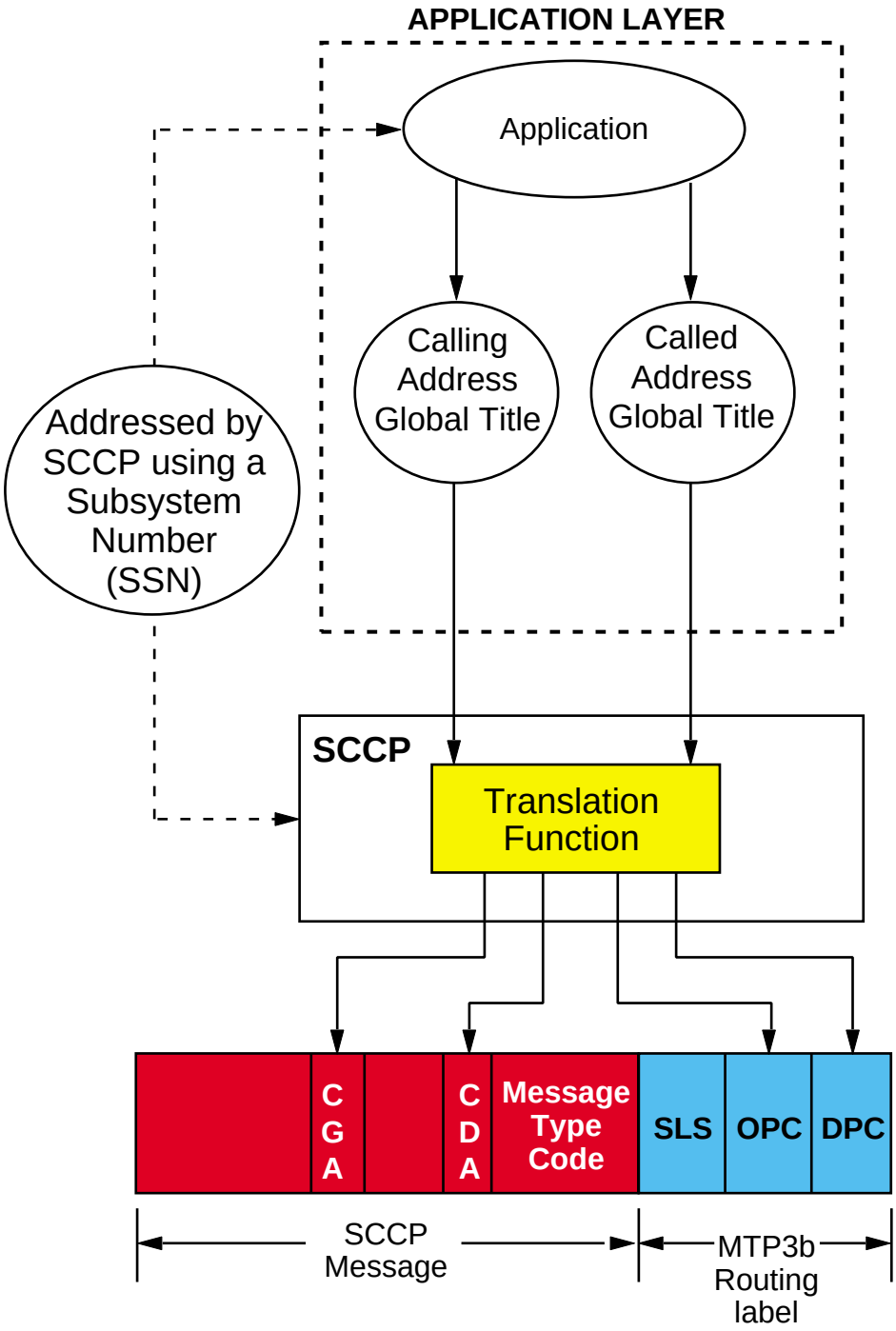
SCCP translates the called party GT to provide MTP3b with DPC and SLS.

These are then used to create the routing label. SCCP also supplies MTP3b with the Originating Point Code (OPC) for inclusion in the routing label.

In addition, SCCP generates a Called Party Address (CDA), which it inserts in the Called Party Address Field in the relevant SCCP message.

Optionally, SCCP may also include the Calling Party Address (CGA) in the SCCP message.

© wray castle limited



Note: The called and calling address global titles may be generated by users of SCCP other than TC user (e.g. ISUP)

Figure 7

SCCP Translation

© wray castle limited

1.9 Called Party Address (CDA)

The general format of the CDA Field, shown in Figure 8, is composed of an Address Indicator and an Address Information Field.

The format of the Address Indicator is shown in Figure 9.

The Point Code Indicator identifies whether or not a point code is present in the Address Information Field.

The SSN Indicator identifies whether or not an SSN is present in the Address Information Field.

The Global Title Field Format Indicator identifies whether or not a GT is present in the address information field and, if so, which one of four GT formats is used.

The Routing Indicator is an instruction informing a remote SCCP node whether to route on a GT or SSN/PC.

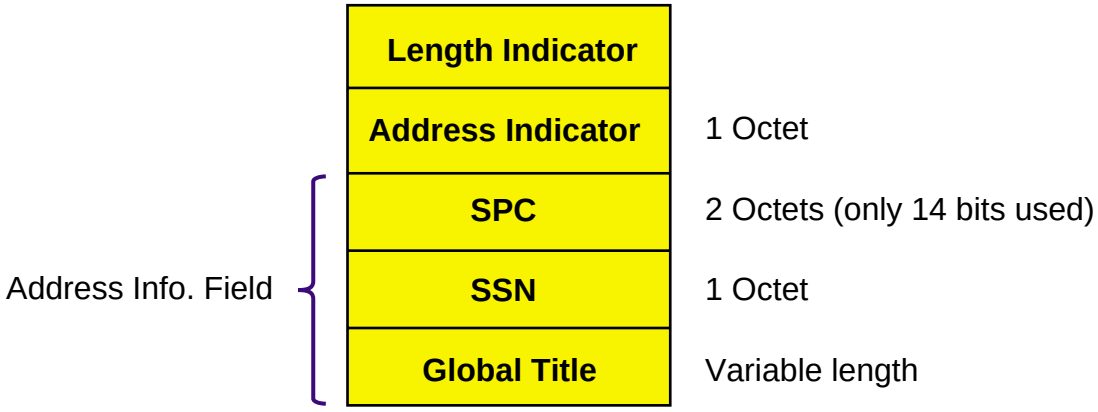
The address information field may contain three possible elements:

- Signalling Point Code (SPC)
- Subsystem Number (SSN)
- Global Title (GT)

One, two, or all three elements may be included and appear in the order shown in Figure 9.

© wray castle limited

a) CDA General Structure



b) Address Indicator

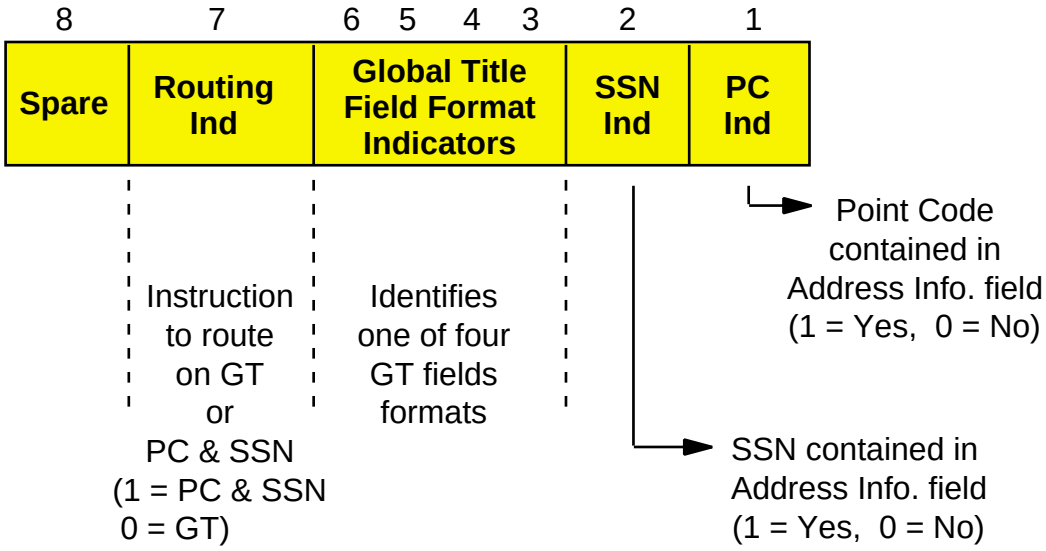


Figure 8

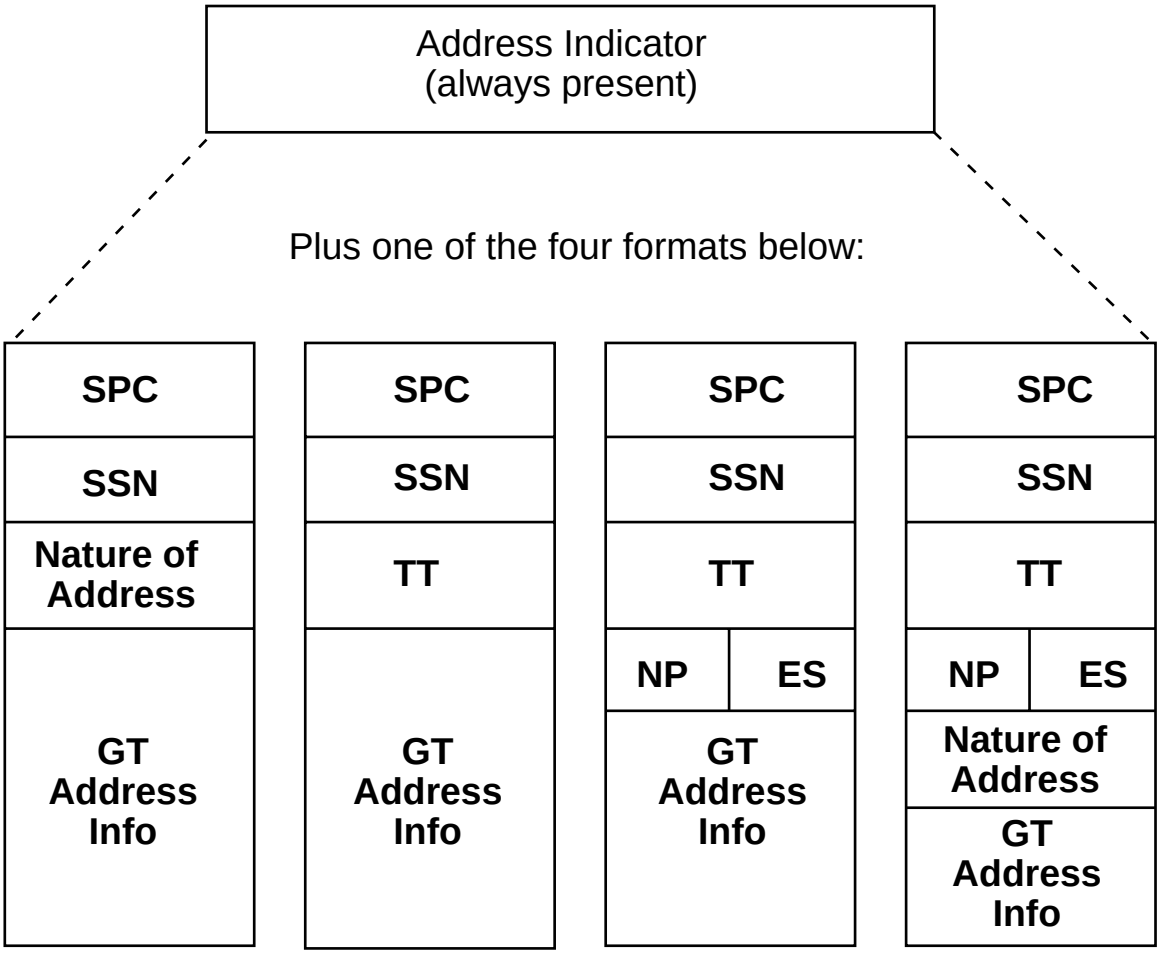
SCCP – Called Destination Address (CDA) Field

© wray castle limited

1.9.1 CDA Formats

Figure 9 illustrates the format of the called party address field when the SPC, SSN and GT are all present. The address indicator is always present and is followed by one of the four formats, as shown in Figure 9.

© wray castle limited



TT – Translation Type (may imply a specific service such as 'Freephone' No. translation-coded to 00hex when not used)
NP – Numbering Plan (E.163, E.164, X.121, F.69, etc.)
ES – Encoding Scheme used in Address Info
(For example: BCD odd number of digits
BCD even number of digits)

Nature of address indicates the type of number in the GT Address Field:

- Subs Number
- National Significant Number
- International Significant Number

Figure 9
SCCP CDA Formats

© wray castle limited

1.9.2 Subsystem Numbers

The Subsystem Numbering (SSN) plan specified by the ITU-T is shown in Figure 10.

© wray castle limited

The subsystem number is coded as follows:

00000000	SSN not known/not used
00000001	SCCP Management
00000010	Reserved for ITU-T allocation
00000011	ISDN User Part
00000100	OMAP (Operation, Maintenance & Administration Part)
00000101	MAP (Mobile Application Part)
00000110	HLR (Home Location Register)
00000111	VLR (Visitor Location Register)
00001000	MSC (Mobile Switching Centre)
00001001	EIC (Equipment Identifier Centre)
00001010	AUC (Authentication Centre)
00001011	ISDN Supplementary Services
00001100	Reserved
00001101	Broadband ISDN edge-to-edge applications
00001110	TC test responder
00001111 to 11111110	Reserved
11111111	Reserved for expansion of national/international SSN

Network specific subsystem numbers should be assigned in descending order starting with ‘11111110’. For example: BSSAP subsystem is allocated 11111110 (FE_H) over the A interface within GSM.

Figure 10

Subsystem Numbering

© wray castle limited

1.10 Identifying Users of SCCP

RANAP
The UE has one signalling connection for the transfer of Layer 3 messages. RANAP may use SSN, SPC and/or GT, any combination of them as addressing schemes for the SCCP which is an operator matter.

When GT is used:

SSN Indicator	=	1
GT Indicator	=	0100 format 4
Translation Type	=	0000 0000 (not used)
NP	=	0001 (E163/4)
Nature of Add Ind	=	000 0100 (international significant number)
ES	=	0001 or 0010 (odd or even BCD)
Routing Ind	=	0 or 1 (route on GT or PC/SSN)

National Network Subsystem Numbers

1111 1010	–	BSC (BSSAP-LE)
1111 1011	–	MSC (BSSAP-LE)
1111 1100	–	SMLC (BSSAP-LE)
1111 1101	–	BSS (A interface)
1111 1110	–	BSSAP (A interface)
1000 1110	–	RANAP
1000 1111	–	RNSAP
1001 0001	–	GMLC (MAP)
1001 0010	–	CAP
1001 0011	–	gsmSCF (MAP)
1001 0100	–	SIWF (MAP)
1001 0101	–	SGSN (MAP)
1001 0110	–	GGSN (MAP)

© wray castle limited

© wray castle limited

© wray castle limited

ANNEX A TO SECTION 4

IP

© wray castle limited

ANNEX CONTENTS

1 Internet Protocol (IP) 4A.1
1.1 The IP Datagram 4A.1
1.2 The IP Datagram Header 4A.3

2 Internet Protocol Version 6 (IPv6) 4A.5
2.1 Introduction 4A.5
2.2 IPv6 Base Header Format 4A.7

© wray castle limited

ANNEX OBJECTIVES

At the end of this annex you will be able to:

- identify the role of the Internet Protocol (IP) IPv4 and IPv6
- state the purpose of the various fields in the IP header

1 INTERNET PROTOCOL (IP)

The Internet Protocol (IP) provides a best-effort connectionless delivery system that is inherently unreliable in nature. It is responsible for the transfer of data (IP datagrams) from source hosts to destination hosts and as such will use the services of the Layer 2 transport mechanism. Thus, we can say that IP sits above the many different network technologies and provides a common interface to the Transport Layer. To achieve this routers will be used to convert between the different network technologies at Layer 2 and the Internet Protocols at Layer 3.

The datagrams being passed from source to destination may well be lost, duplicated, delayed, delivered out of sequence, or even fragmented. Therefore, it is the responsibility of the IP Layer to trigger error messages and to reassemble any fragmented datagrams before they are passed up to the higher-layer protocols.

1.1 The IP Datagram

The size of the data area within the IP datagram is not fixed, which allows it to be as flexible as possible. In fact the data area can contain as little as a single octet or as much as 65,535 octets of data (IPv4). The datagram header is similar to that of a frame header in that it contains information to route the datagram across the Internet. For example, the header contains the address of the computer that sent the datagram as well as the address of the computer to which the datagram is destined. However, it should be noted that the addresses that appear in the datagram header are IP addresses, whereas the addresses that appear in the frame header will contain hardware or MAC addresses.

Datagrams are said to traverse an internet by following a path from originating host to receiving host. Each router along the path receives the datagram, extracts the destination address from the header, and uses it to determine the next ‘hop’ in the path. The router will then send the datagram to either the receiving host or another router.

The format of the IP datagram (IPv4) can be seen in Figure 1.

© wray castle limited

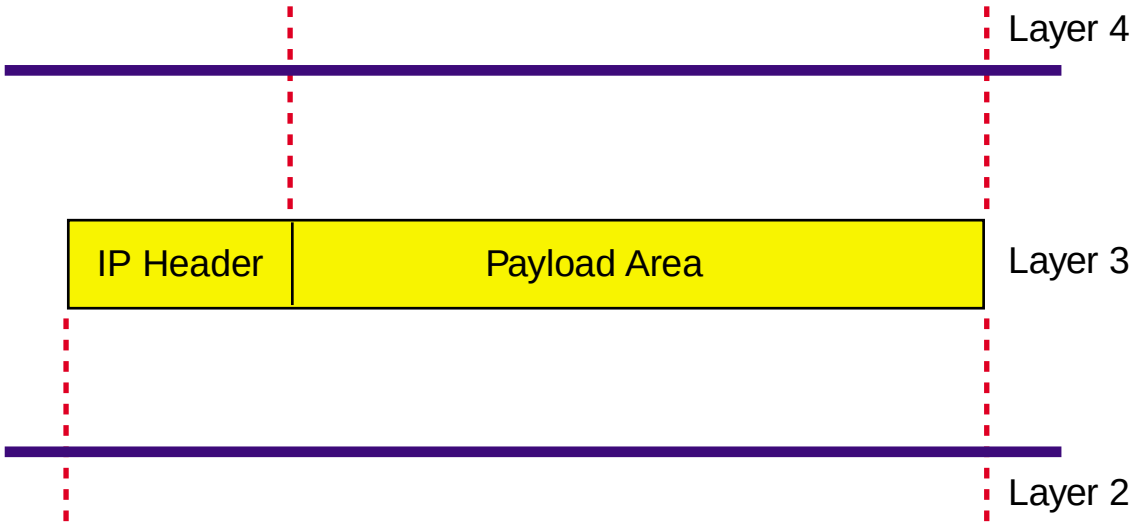


Figure 1
IP Datagram

© wray castle limited

1.2 The IP Datagram Header

The IP datagram header, which can be seen in Figure 2, is made up of the following fields.

1.2.1 Header Length

The Header Length field is used to specify the number of 32-bit (four-octet) groups that make up the IP Header. The header length is used to point to the beginning of the IP Payload Area and is usually set to 5 when the Options field is not used. This would indicate that the IP header is generally comprised of 20 octets. If the Options field does contain data, the Padding field will be used to ensure that the IP Header fills a complete 32-bit group.

1.2.2 Version

The Version field is used to specify the protocol version number that is being used in the datagram. For this IP datagram header format, the value will be set at 4 to signify IPv4. The inclusion of this field allows different versions of IP to operate on the same network. An experimental version of IP has been developed which has the version field set to 5, and the next-generation IP datagrams to be used publicly have the field set to 6. Hence the name IPv6. All other values in this field are either reserved or unassigned.

© wray castle limited

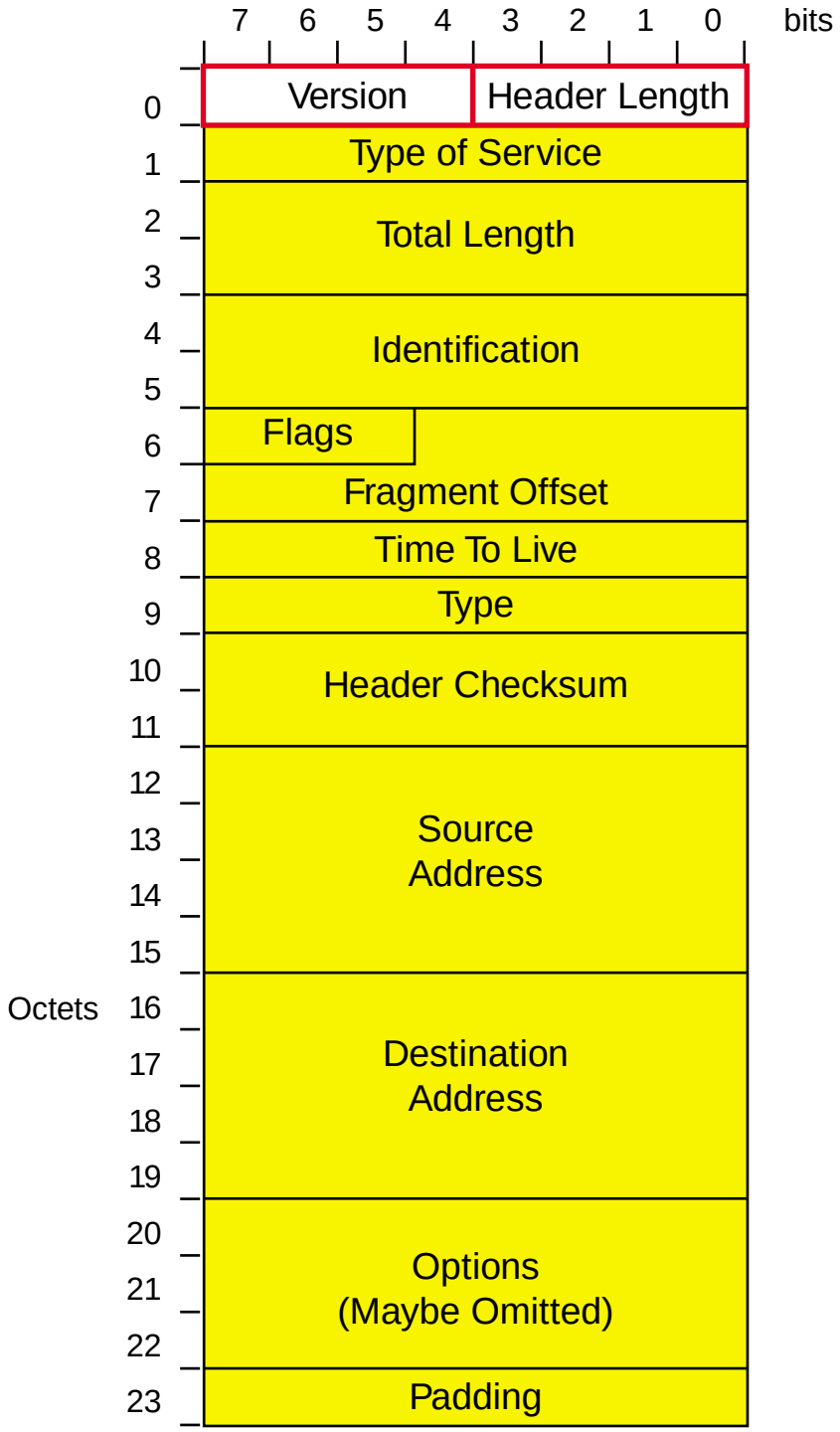


Figure 2
IP Datagram Header

© wray castle limited

2 INTERNET PROTOCOL VERSION 6 (IPv6)

2.1 Introduction

IPv6 retains many of the design features that have made IPv4 so successful. Like IPv4, IPv6 is connectionless with each datagram containing a destination address and being routed independently. There have, however, been changes in the new version of IP and these are as follows.

2.1.1 Address Size

The address size has been increased to 128 bits instead of the 32 bits currently used. This should accommodate continued growth of the World Wide Web for many years to come!

2.1.2 Header Format

The IPv6 datagram header is completely different from the IPv4 with almost every header either being modified or replaced.

2.1.3 Extension Headers

IPv6 is able to encode information into separate headers. The new datagram will now consist of a source header, followed by zero or more extension headers before the actual data begins (see Figure 3).

2.1.4 Support for Audio and Video

IPv6 includes a mechanism that will allow a sender and receiver to establish a ‘high quality’ path across the underlying networks that make up the Internet. Such paths will ensure quality levels through a priority scheme.

2.1.5 Extensible Protocol

The designers of IPv6 have provided a scheme that will allow a sender to add additional information to a datagram. This is intended to make IPv6 future-proof as new features can be added to the design when needed.

© wray castle limited

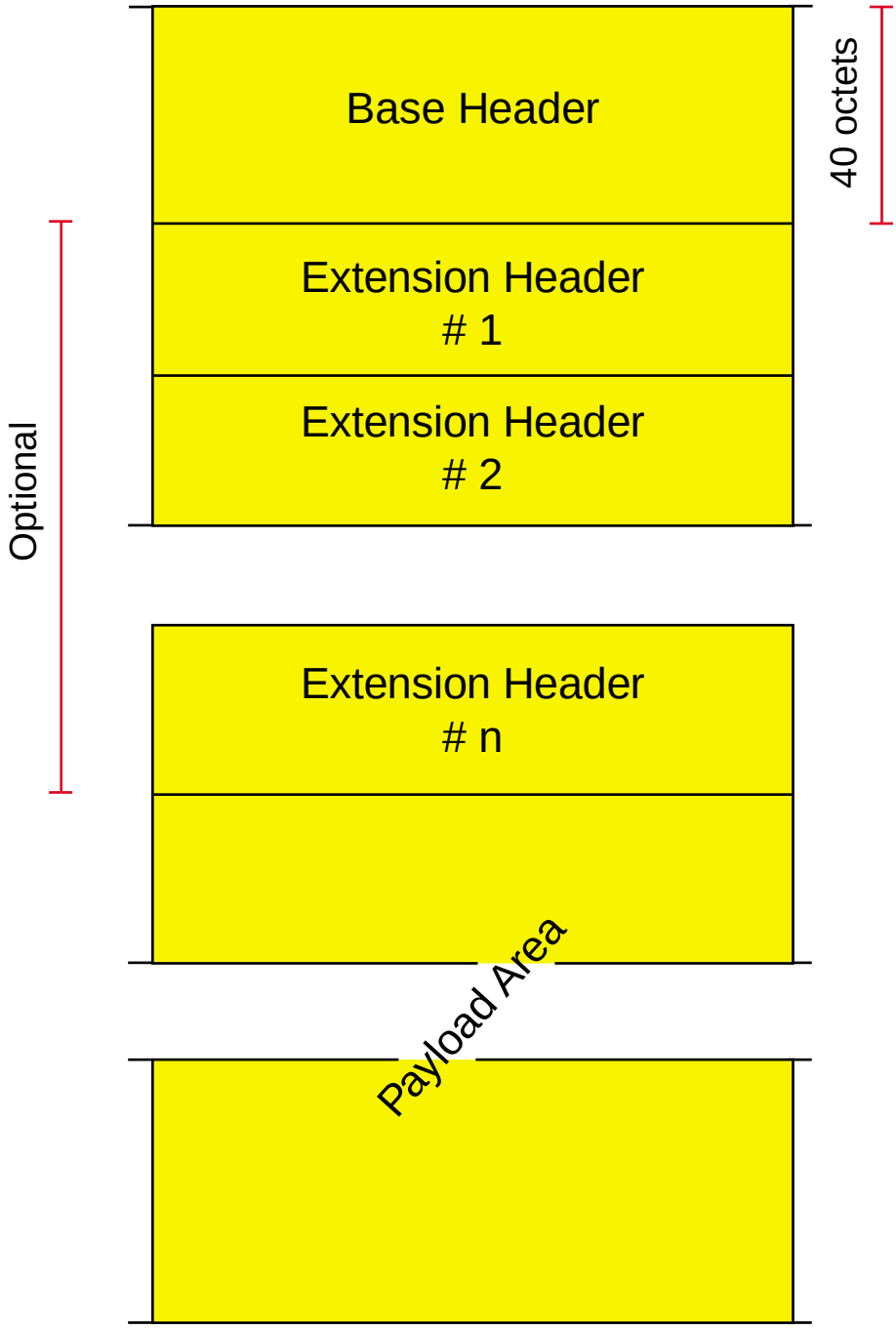


Figure 3
IPv6 Format

© wray castle limited

2.2 IPv6 Base Header Format

The IPv6 header is twice the size of the IPv4 header. It actually contains less information, however, since the majority of the bits are used for the larger Source Address and Destination Address fields. In addition to these, the Base Header will also contain six other fields:

2.2.1 Version

The Version field is used to specify that the current IP datagram is from version IPv6. This has the same function as the Version field in the IPv4 header.

2.2.2 Priority

The 4-bit Priority field allows a host to specify the delivery order of its datagrams. There are two categories of traffic, those that yield to congestion in a router and those that cannot yield because of the time-sensitive nature of the traffic.

2.2.3 Flow Label

The Flow Label is to be used when performance guarantees are required, for example video and Voice over IP (VoIP). This field is split into two further fields. These are Tclass and the Flow Identifier.

- The Tclass is a 4-bit field which specifies the traffic class of the datagram. Values 0 to 7 specify the time sensitivity of flow-controlled data. Values 8 to 15 are used to prioritize non-flow data.

- The remaining 24 bits contain the Flow Identifier (FI) which along with the source address ties a specific Quality of Service (QoS) with a specific host.

The format of the IPv6 header can be seen in Figure 4.

© wray castle limited

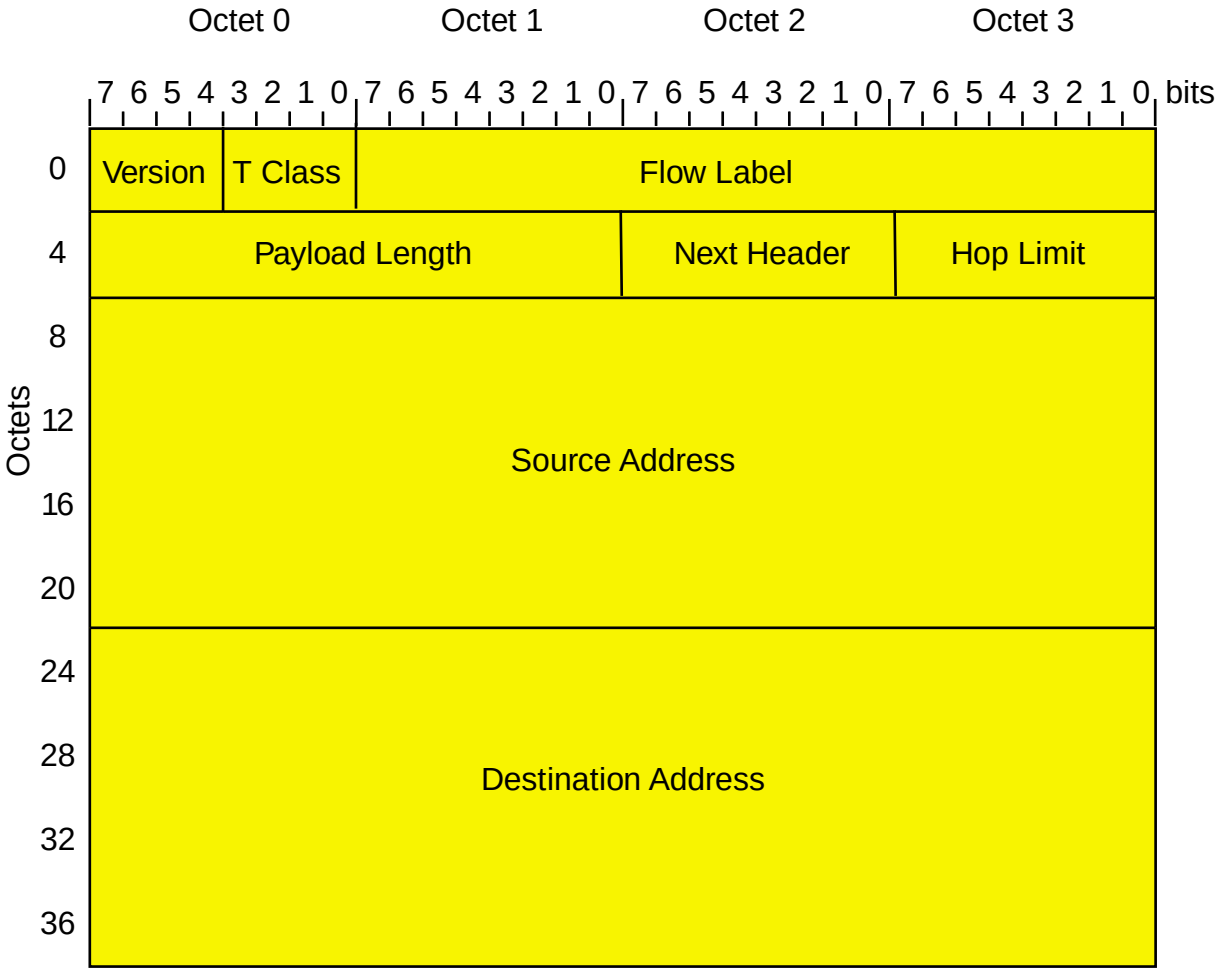


Figure 4
IPv6 Base Header Format

© wray castle limited

2.2.4 Payload Length

The 16-bit Payload Length field is used to signify the number of octets in the payload area immediately following the IPv6 header. The value can range from 1 to 65,535.

2.2.5 Next Header

The Next Header field consists one octet. In IPv6, the header size is minimized by eliminating fixed fields for features or options, whether they are used or not. For example, the Fragment Offset field is always present in an IPv4 header irrespective of whether the datagram was fragmented. In IPv6, these features are dealt with by the use of extension headers which are only present when needed. The extension headers are stacked in a prescribed way with the first header immediately following the Destination Address field. As such, the Next Header field is used to identify the presence of the first extension header.

2.2.6 Hop Limit

This is an 8-bit field which is decremented by 1 each time the datagram passes through a device. As with the Time To Live field in IPv4, once this value reaches 0, the datagram is discarded.

The format of the IPv6 header can be seen in Figure 4.

Note: in UMTS, IPv4 shall be supported, but the support of IPv6 is optional.

© wray castle limited

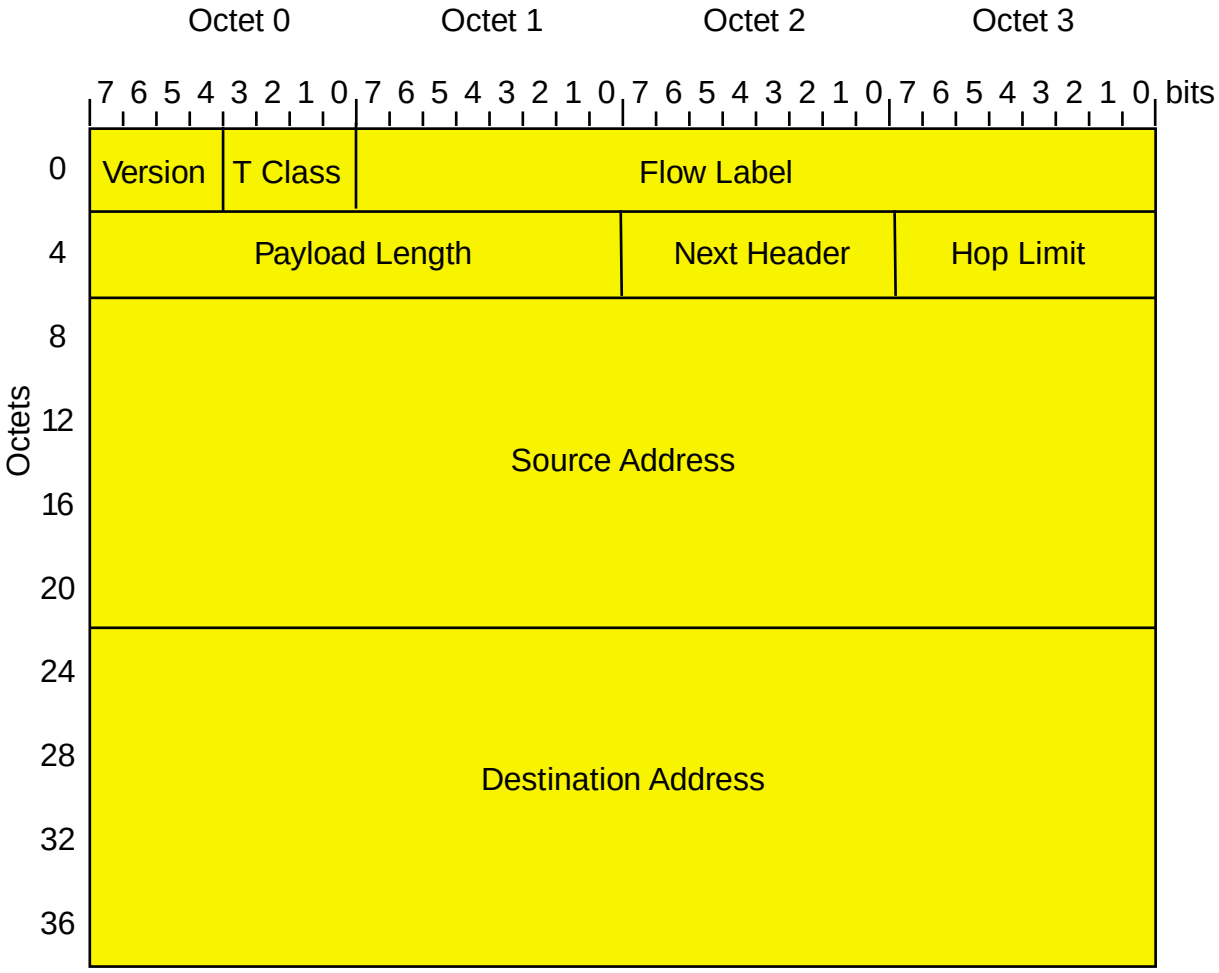


Figure 4 (repeated)
IPv6 Base Header Format

© wray castle limited

© wray castle limited

ANNEX B TO SECTION 4

TCP/UDP

© wray castle limited

ANNEX CONTENTS

1 The Transport Layer 4B.1
1.1 Introduction 4B.1

2 Transmission Control Protocol (TCP) 4B.3
2.1 Connection-Oriented 4B.3
2.2 Point-to-Point 4B.3
2.3 Complete Reliability 4B.3
2.4 Full Duplex Communication 4B.3
2.5 Stream Interface 4B.3
2.6 Reliable Connection Start-up 4B.3
2.7 Graceful Connection Shut Down 4B.3
2.8 Port Addressing 4B.5

3 User Datagram Protocol (UDP) 4B.9
3.1 Introduction 4B.9
3.2 UDP Header Format 4B.9
3.3 Data Offset 4B.11
3.4 Code Bits 4B.11
3.5 Options 4B.12
3.6 Padding 4B.12

© wray castle limited

© wray castle limited

ANNEX OBJECTIVES

At the end of this annex you will be able to:

- identify the role of the transport protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
- describe the support of packet switched services in UMTS

© wray castle limited

1 THE TRANSPORT LAYER

1.1 Introduction

We can see from Figure 1 that the Transport Layer of the TCP/IP Protocol Suite comprises two protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

In this section, we shall address both of these protocols and establish their mode of operation and the services offered. We can see from Figure 1 that both TCP and UDP use the services of IP in Layer 3 and thus are said to be encapsulated into the IP datagram payload area.

Fundamentally, the services offered by TCP are connection-oriented, whereas UDP provides a connectionless service.

© wray castle limited

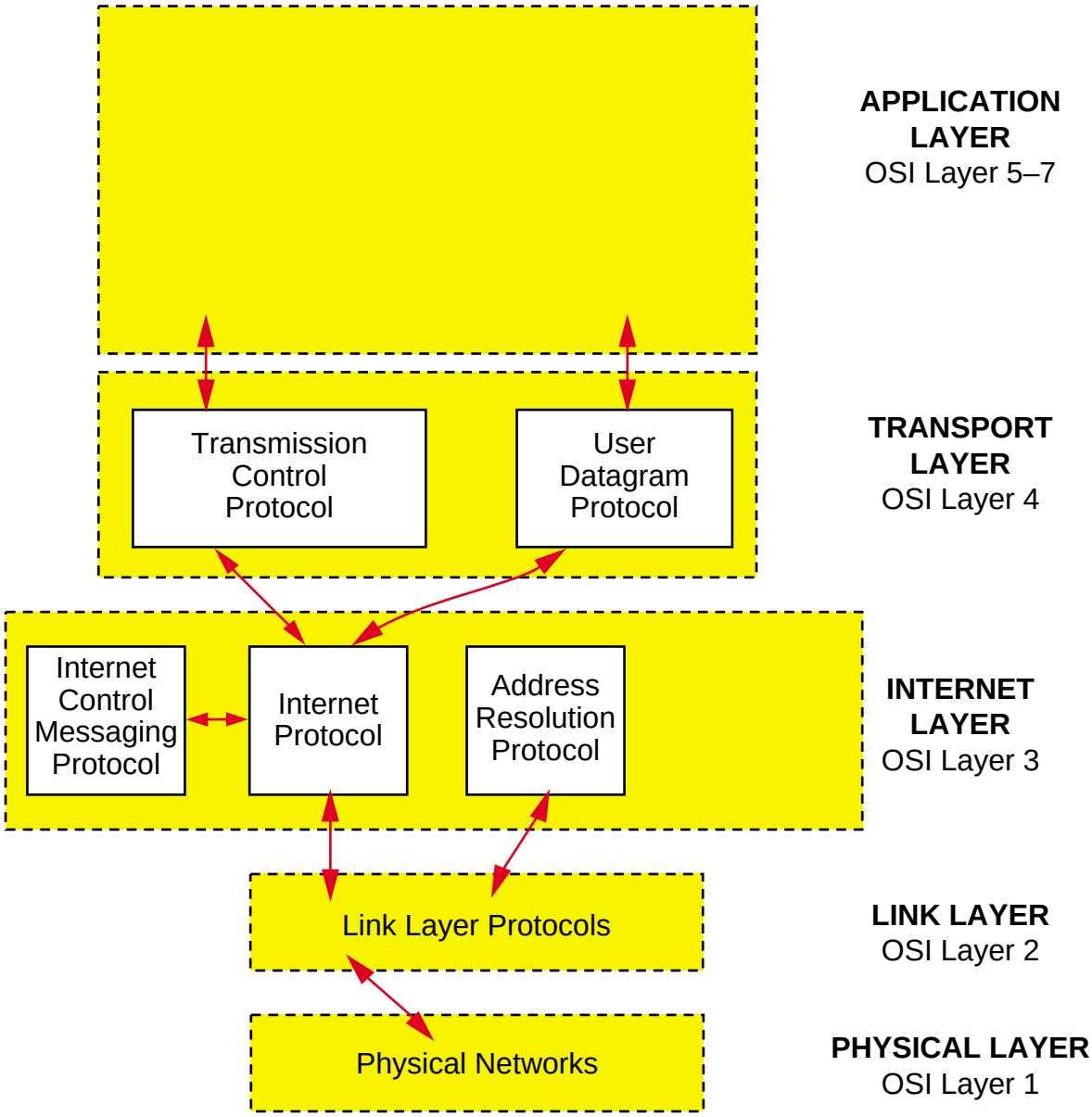


Figure 1
TCP/IP Suite

© wray castle limited

2 TRANSMISSION CONTROL PROTOCOL (TCP)

The Transmission Control Protocol (TCP) provides a highly reliable transport service which has proved to be so successful that most internet applications use the services of TCP to transport data between hosts. With regard to these applications, TCP is said to offer seven major features (Figure 2):

2.1 Connection-Oriented

Unlike UDP, TCP provides a connection-oriented service in which an application must first establish a connection to the destination before any data is transferred.

2.2 Point-to-Point

Each TCP connection has only two end points.

2.3 Complete Reliability

TCP ensures that data sent across a connection is error free and in the correct sequence.

2.4 Full Duplex Communication

When a connection is established using TCP, data is able to be transferred in either direction allowing either application program to send data when required. TCP software is also able to support buffering of data, which enables an application to send data and then continue processing whilst the data is being transferred.

2.5 Stream Interface

TCP provides a stream interface in which an application sends a continuous sequence of octets across a connection. Thus, TCP does not guarantee that transferred data will arrive at the destination host in the same size packets as it left the source host.

2.6 Reliable Connection Start-up

TCP requires that both applications creating a connection agree to the new connection. Thus duplicate packets used in previous connections will not be valid responses.

2.7 Graceful Connection Shut Down

If an application establishes a connection, it sends data across the link and then requests that the connection be terminated. TCP will ensure that all data is delivered reliably before closing the connection.

© wray castle limited

Connection-Oriented

Point-to-Point

Complete Reliability

Full Duplex Communication

Stream Interface

Reliable Connection Start-up

Graceful Connection Shut-down

Figure 2
TCP Features

© wray castle limited

2.8 Port Addressing

At the Internet Layer, data is routed according to its IP address, with no distinction made regarding the user or process on the destination host. The Transport Layer extends the TCP/IP protocol suit to distinguish between processes on a given host.

Operating systems typically run multiple processes simultaneously. Consequently, the final destination of data is a specific process on a specific host. Processes are created and destroyed dynamically and are replaced by a new process when hosts reboot, so instead of identifying the specific process to which data must be sent, an abstract port is considered to be the destination for data. These ports are known as ‘Protocol Ports’ and can be addressed using the 16 bits in the Source and Destination Port address fields. These 16 bits can describe 65,536 possible ports on the host. Ports 1 to 1,024 are known as the ‘well-known ports’ and are used to establish sessions between hosts. Some of the well-known ports are listed below.

File Transfer Protocol (control)	Port 20
File Transfer Protocol (Data)	Port 21
TELNET	Port 23
HTTP	Port 80
Simple Network Management Protocol	Port 161

2.8.1 Sequence Number

The sequence number occupies 32 bits and it is used to identify a portion of data which is sent between two application protocols. The entire data sent from one host to another is referred to as a *stream* and tends to be too great to send in one datagram. As such, the stream is broken down into segments. The first sequence number of the first sequence number of the first TCP segment will point to the first octet of the original stream.

2.8.2 Acknowledgement Number

This too is comprised of a 32-bit field and is used to indicate the data that is next expected.

© wray castle limited

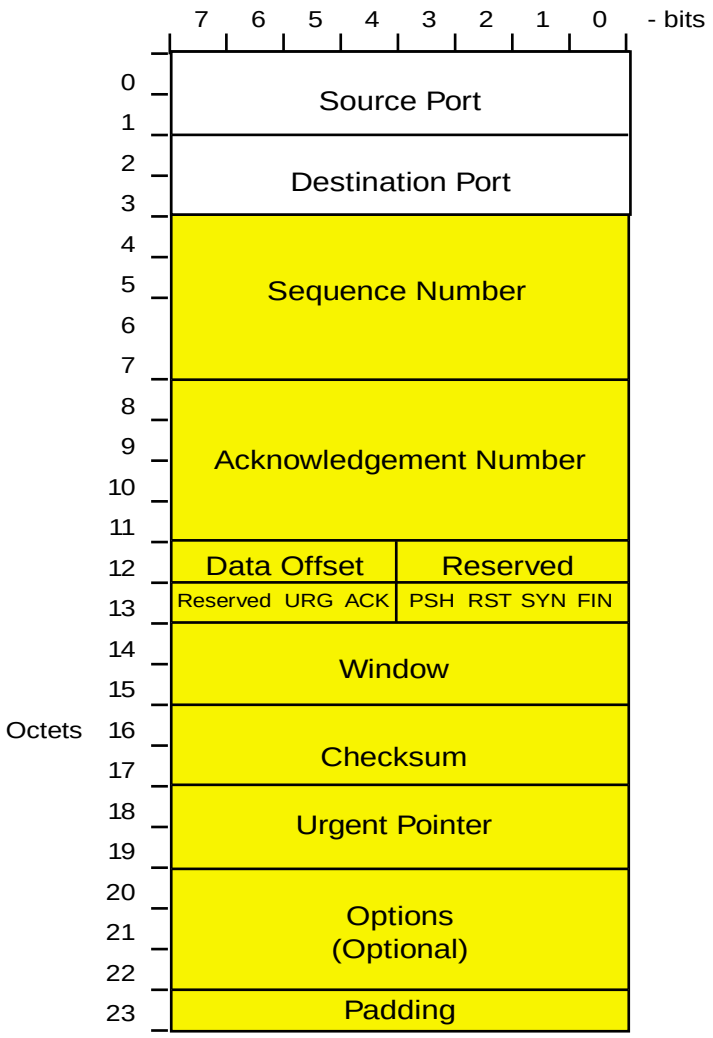


Figure 3
Port Addressing

© wray castle limited

Between the TCP layers a three-way handshake takes place in order to establish an association between the send and acknowledge sequence numbers. This enables the TCP layer to reassemble the information before passing all the information to the higher layer. The handshake also sets the maximum transmission unit size.

If any of the packets are lost on their way to the end host the TCP layer will be able to ask for a retransmission of the missing information from its peer entity.

The three-way handshake is shown in Figure 4.

© wray castle limited

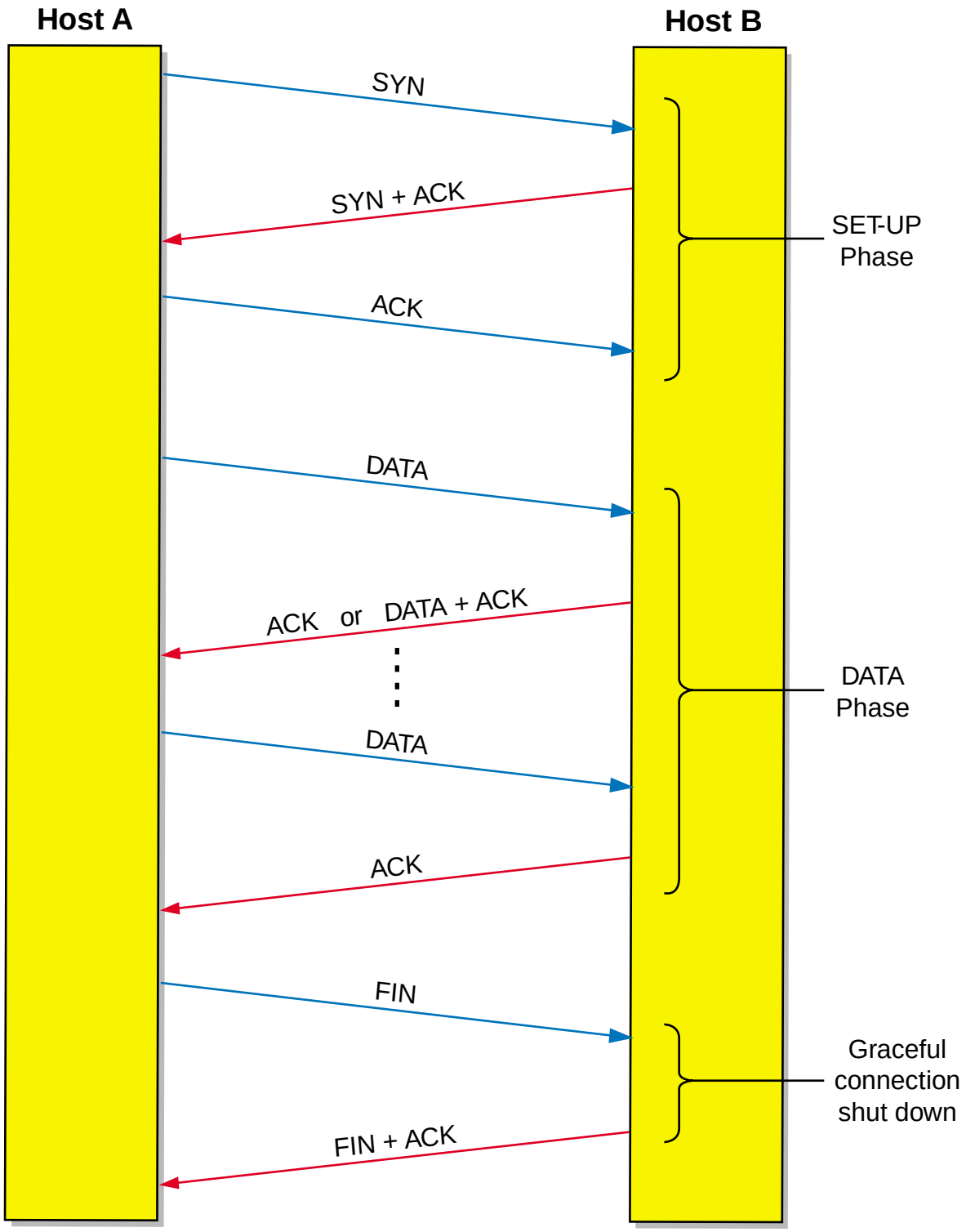


Figure 4
Three-Way Handshake

© wray castle limited

3 USER DATAGRAM PROTOCOL (UDP)

3.1 Introduction

User Datagram Protocol (UDP) provides Application Layer Services with a transaction-oriented, datagram-type service which, like IP, is connectionless and unreliable. It is a simple and efficient protocol in resource usage which makes it ideal for such applications as Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP) and Domain Name System (DNS).

As UDP operates in the Transport Layer, it is addressed by the Type field in the IP header, which is set to 17. This enables the Internet Layer (Layer 3) to pass its payload up to UDP. Once at UDP, the Destination Port address is used to direct the data from the IP datagram to the appropriate process queue.

3.2 UDP Header Format

The format of the UDP header can be seen in Figure 5. From this it is clear that UDP is a far simpler protocol than TCP. There are four fields within the header.

3.2.1 Source Port

As with the Source port in TCP, with the IP address this provides an association between the two end points at the Application Layer. However, UDP is connectionless and, as such, the Source port may be set to zero if no response is required or expected. In UMTS the source port number (between SGSN and RNC) shall be a locally allocated number at the sending SGSN/RNC.

3.2.2 Destination Port

This is also comprised of 16 bits and, as with TCP, it points to the Application Layer protocol which is to be the recipient of the UDP payload area. There are defined Port addresses, and for the protocols mentioned above these are:

Trivial File Transfer Protocol (TFTP)	=	69
Simple Network Management Protocol (SNMP)	=	161/162
Domain Name System (DNS)	=	53

In UMTS the UDP destination port number shall be 2,152 – registered port number for GTP-U at the SGSN/RNC.

3.2.3 Message Length

This 16-bit field contains a count of the total number of octets in both the UDP payload area and UDP header. The minimum value of the length field is eight, which is equal to the number of octets in the header.

© wray castle limited

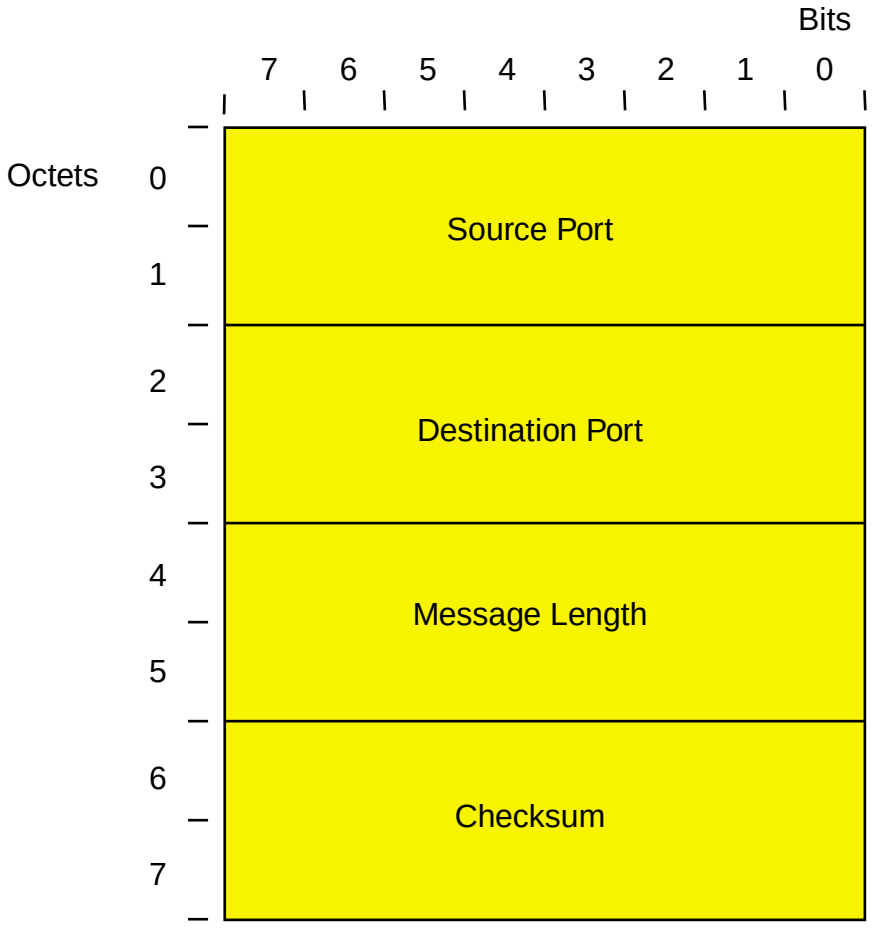


Figure 5
UDP Header

© wray castle limited

3.3 Data Offset

The Data Offset consists of four bits and is used to indicate the total number of four-octet groups (32 bits) in the TCP header. This value is typically equal to five unless the Options field is present. In that case, Padding will be added after the Options to ensure the total TCP header is comprised of multiples of four octets.

3.4 Code Bits

The Code Bits each occupy one bit and are summarized below:

URG
The URG bit is used to indicate whether the Urgent Pointer field in the TCP header is active (bit set to 1). If the bit is equal to 0, the Urgent Pointer is not active.

ACK
When the ACK bit is equal to 1, the Acknowledgement Number in the TCP header is said to be valid. This should always be the case after the connection is established.

PSH
Although a transmit buffer may not be full, the sender may force it to be delivered to the application. This is achieved by setting the bit to 1.

RST
If the RST bit is set in a segment, it causes the connection to be aborted and all buffers associated with the connection will be emptied.

SYN
The SYN bit is set during connection establishment in order to synchronize the Sequence Number in the TCP header.

FIN
This bit is set during the connection in order to close it.

© wray castle limited

3.5 Options

This field is optional and is used to permit the application program to negotiate various characteristics during connection establishment. These may include such things as the maximum TCP segment size that the application is allowed to receive.

The Option field is subdivided into three further fields: Option Type, which will be set to 2 for segment size negotiation; Option Length, which is set to 4 as there are four octets in the Option Field; and finally Value, which in this case indicates the maximum segment size.

3.6 Padding

This is only present if the Option field does not fill an entire 32-bit group.

© wray castle limited

© wray castle limited

SECTION 5

RADIO PROTOCOLS

© wray castle limited

LESSON 1

RADIO RESOURCE CONTROL (RRC)

© wray castle limited

LESSON CONTENTS

1 Protocol Termination within the UTRAN 5.1.1
1.1 Termination Nodes 5.1.1
1.2 Variations for Protocol Termination 5.1.1

2 Radio Resource Control (RRC) 5.1.3
2.1 Functions of RRC Messages 5.1.3
2.2 The RRC Model 5.1.5

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of the Radio Resource Control (RRC) protocol

© wray castle limited

1 PROTOCOL TERMINATION WITHIN THE UTRAN

1.1 Termination Nodes

The UTRAN contains two logical functions, the RNC and the Node B. The Non-Access Stratum (NAS) is transparent to both these node types, but the protocols of the Access Stratum (AS) will terminate at either the RNC or the Node B. In general the Node B is concerned only with physical layer functions, thus the layer 2 protocols Medium Access Control (MAC) and Radio Link Control (RLC) will terminate at the RNC. This is shown in Figure 1.

1.2 Variations for Protocol Termination

The precise arrangements for protocol termination are subject to some variation. One factor resulting in variation is the logical channel type in use. Figure 1 holds true for most logical and transport channel types, but for some types of system information being broadcast on the Broadcast Channel (BCH), rapid update may be required. This update period may be in the order of fractions of a second. Since it is considered unlikely that such a rapid update rate would be available from the RNC, it is permitted for the AS to terminate in the Node B. Basic system information is then transported transparently to the Node B and the rapidly updated system information is added locally for transmission.

© wray castle limited

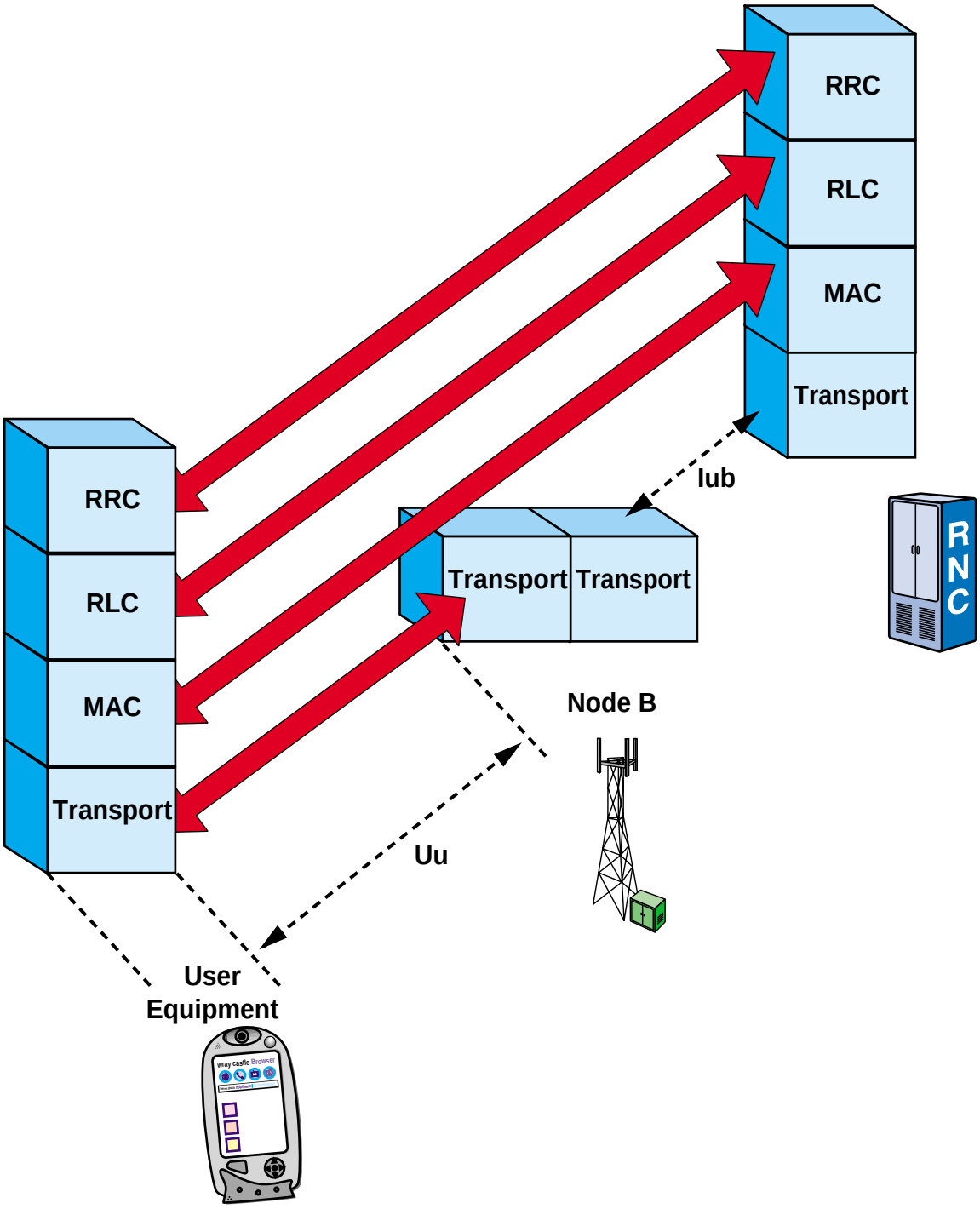


Figure 1
Protocol Termination

© wray castle limited

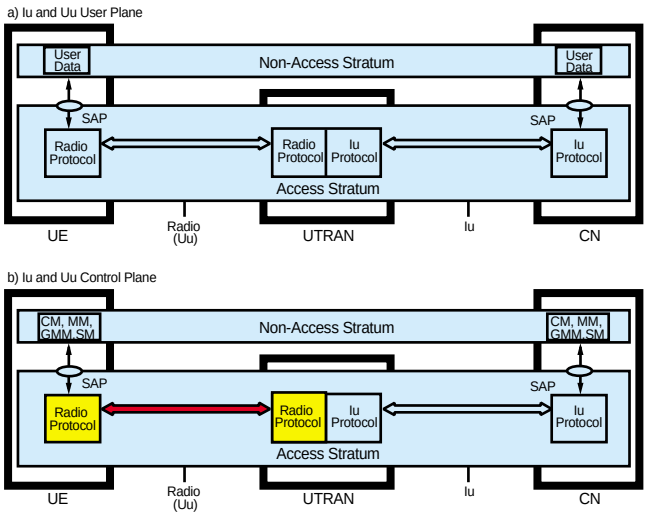
2 RADIO RESOURCE CONTROL (RRC)

2.1 Functions of RRC Messages

Most of the signalling between UE and the UTRAN constitutes RRC messages. These messages provide support for various functions, some of which are as follows.

- establishment, maintenance and release of RRC connections between the UE and the UTRAN, together with the establishment, reconfiguration and release of Radio Bearers (RB);
- assignment, reconfiguration and release of Radio Resources (RRs) for the RRC connection, and RRC connection mobility functions;
- transfer of higher-layer signalling messages and routing towards the correct CM/MM entity or CN domain;
- control of requested QoS;
- UE measurement reporting, outer loop power control;
- control of ciphering;
- paging/notification;
- initial cell selection and reselection in idle mode;
- broadcast of NAS (CN) information and AS information.

© wray castle limited



Function of RRC Messages:

- establishment, maintainance and release of RRC connections and radio bearers
- control of radio resources
- transfer and routing of MM and CM messages
- control of requested QoS
- functions related to power control
- initial cell selection, paging/notification and control of ciphering
- broadcast procedures

Figure 2

Functions of RRC Messages

© wray castle limited

2.2 The RRC Model

The RRC function is located in the control plane at the top of the AS. It provides SAPs through which higher-layer signalling entities can gain services in the form of signalling transfer from the AS.

There are three main forms of signalling transfer offered to these higher-layer entities:

- general control
- paging and notification
- dedicated control

In order that these services can be provided, RRC communicates with and controls the operation of all the lower layers of the AS. Thus RRC provides control to Radio Link Control (RLC), Medium Access Control (MAC) and the physical layer.

RRC needs to gain service from the lower layers, and in this respect it uses three SAP types from the RLC layer.

- Transparent Mode SAP (Tr-SAP)
- Unacknowledged Mode SAP (UM-SAP)
- Acknowledged Mode SAP (AM-SAP)

© wray castle limited

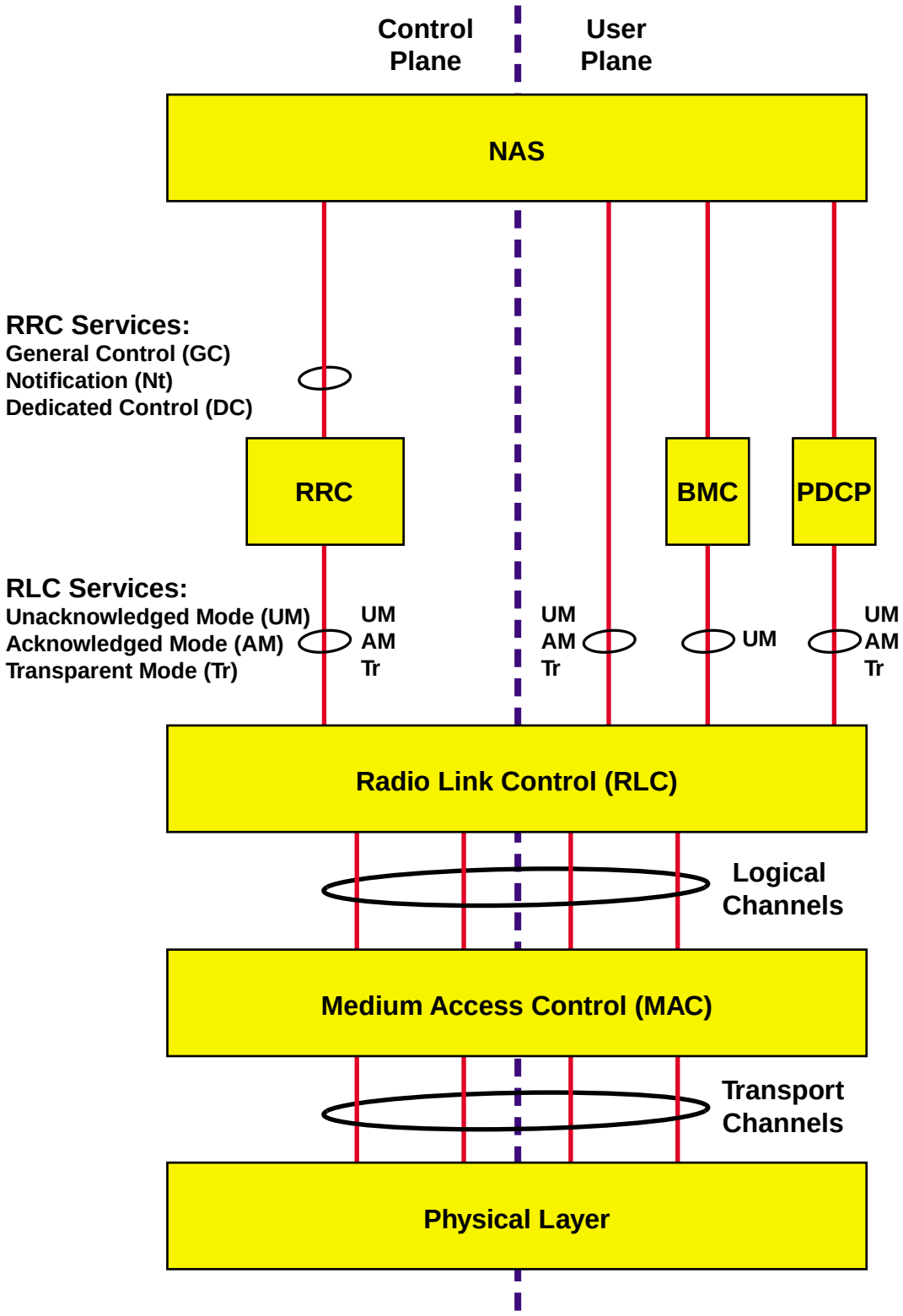


Figure 3
The RRC Model (UE Side)

© wray castle limited

© wray castle limited

LESSON 2

RADIO LINK CONTROL (RLC)

© wray castle limited

LESSON CONTENTS

1 Radio Link Control (RLC) Architecture 5.2.1
1.1 RLC Functional Entities (FEs) 5.2.1
1.2 RLC Transparent Mode (TrM) 5.2.3
1.3 RLC Unacknowledged Mode (UM) 5.2.5
1.4 RLC Acknowledged Mode (AM) 5.2.7

2 RLC Protocol Data Unit (PDU) Types 5.2.9
2.1 UMD PDU Structure 5.2.11
2.2 AMD PDU Structure 5.2.13

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe the use and scope of the Radio Link Control (RLC) protocol

© wray castle limited

1 RADIO LINK CONTROL (RLC) ARCHITECTURE

1.1 RLC Functional Entities (FEs)

Radio Link Control (RLC) can be considered as two complementary sides, the transmit side and the receive side. Both functions exist for control and user planes of the protocol stack. The services offered by RLC are referred to as Signalling Radio Bearers (SRBs) in the control plane and Radio Bearers (RBs) in the user plane.

There are three modes of operation for RLC, and each has a transmit and receive element.

Transparent Entity
The transparent entity provides the minimum level of service from RLC. There is no added header information.

Unacknowledged Entity
The unacknowledged entity offers some degree of reliability with internal RLC processing and RLC header information. As its name suggests, there is no acknowledgement of the successful reception of transferred data.

Acknowledged Entity
The acknowledged entity is shown in Figure 1 as bridging the transmit and receive sides of RLC. In this mode of operation RLC offers a full acknowledgement of successful delivery and retransmission for unsuccessful delivery.

© wray castle limited

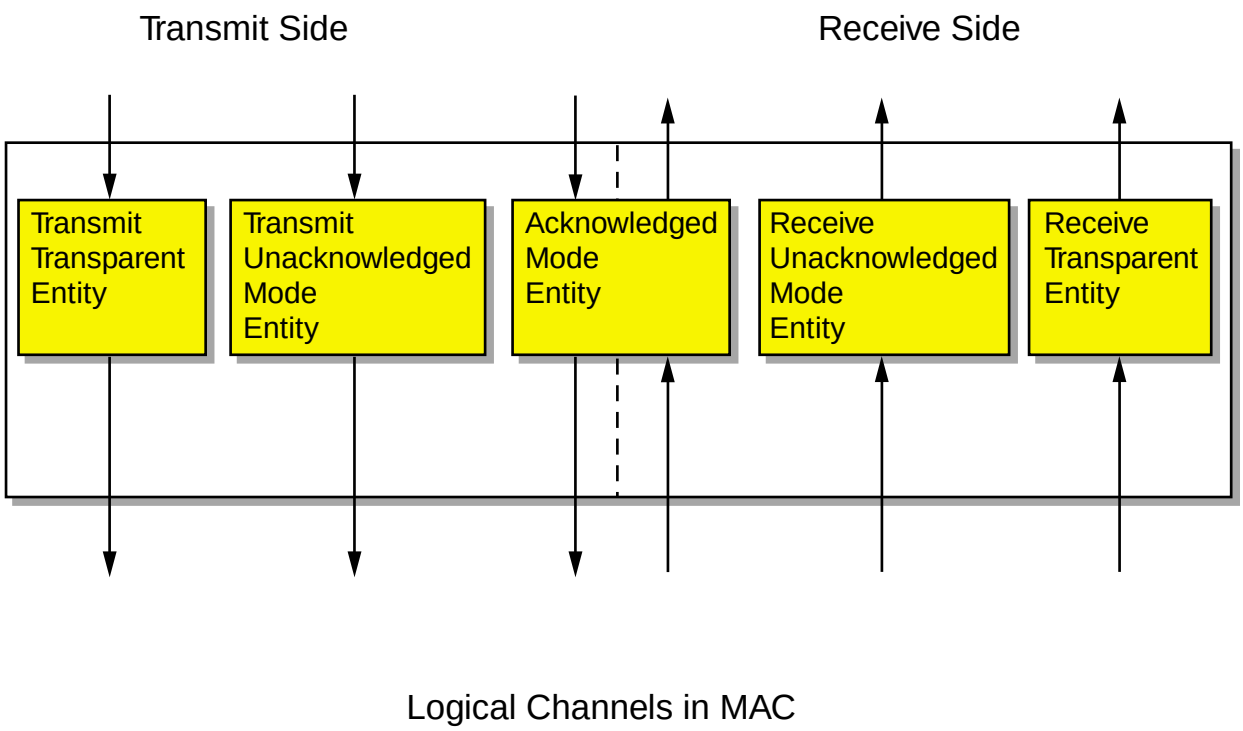


Figure 1
RLC Functional Entities

© wray castle limited

1.2 RLC Transparent Mode (TrM)

The Transparent Mode (TrM) service of RLC is accessed via the Transparent Mode Service Access Point (Tr-SAP). No RLC header information is added in this mode, but the RLC may perform segmentation and reassembly of higher-layer Service Data Units (SDUs). If this is to be done, it will be negotiated at RB set-up.

RLC PDUs are passed to and from the Medium Access Control (MAC) layer via any of the control plane logical channels:

- Broadcast Control Channel (BCCH)
- Common Control Channel (CCCH)
- Dedicated Control Channel (DCCH)
- Paging Control Channel (PCCH)
- Shared Channel Control Channel (SHCCH)

or the user plane logical channel Dedicated Traffic Channel (DTCH).

Although itself a bidirectional channel, the CCCH only makes use of TrM in the Uplink (UL) direction.

There is no interaction between the UL and Downlink (DL) operation of TrM.

© wray castle limited

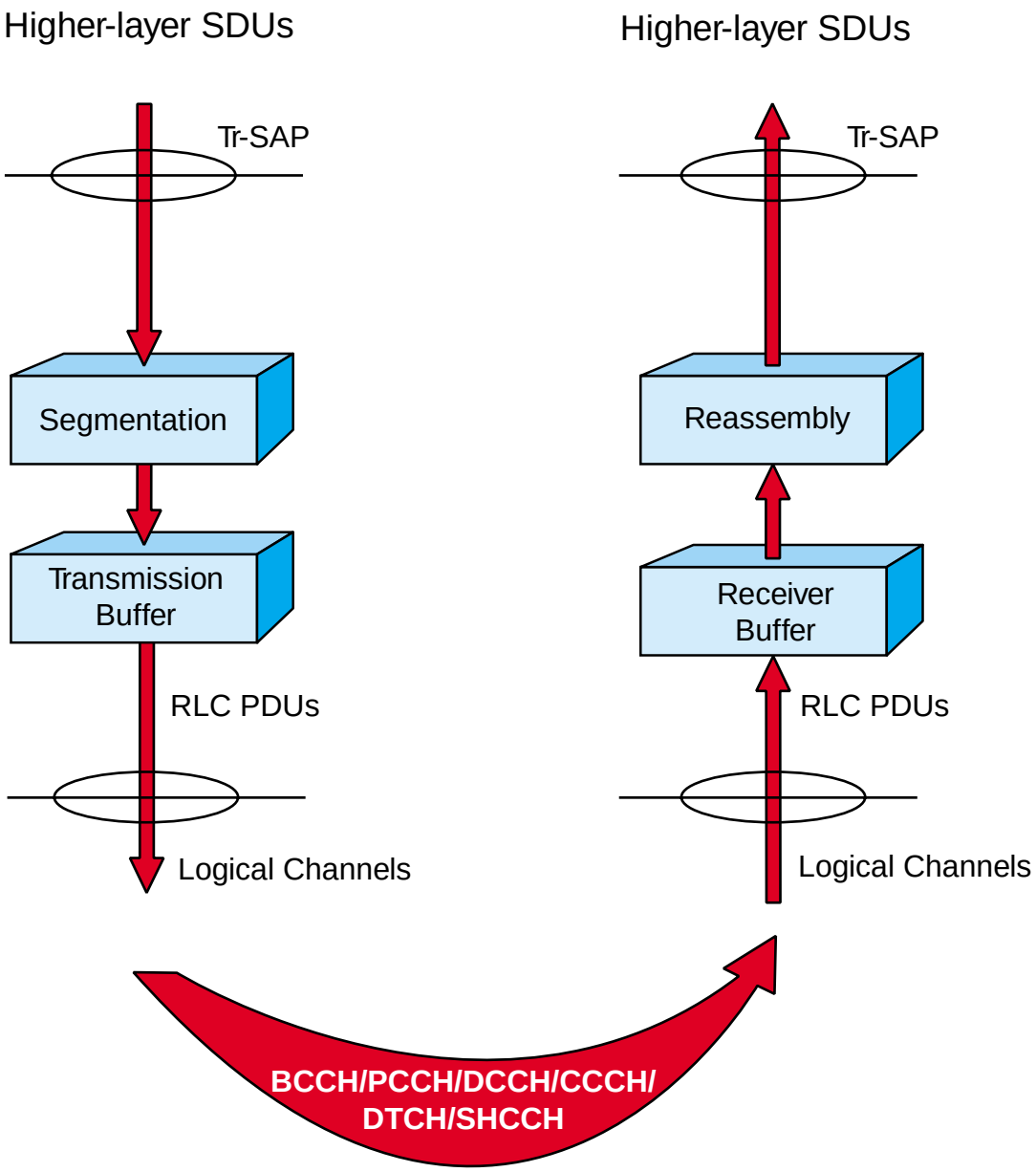


Figure 2
Transparent Mode Operation

© wray castle limited

1.3 RLC Unacknowledged Mode (UM)

The Unacknowledged Mode (UM) service of RLC is accessed via the Unacknowledged Mode Service Access Point (UM-SAP). Like the TrM, segmentation may be applied to higher-layer SDUs; however, in addition, the UM may apply concatenation. An indication of segmentation and concatenation is provided in the RLC header information. The RLC header also provides sequence numbers on RLC PDUs, enabling more reliable reassembly.

RLC PDUs are passed to and from the MAC layer via any of the control plane logical channels:

- CCCH
- DCCH
- SHCCH

or user plane logical channels:

- DTCH
- CTCH

Although itself a bidirectional channel, the CCCH makes use of UM in the DL direction only.

© wray castle limited

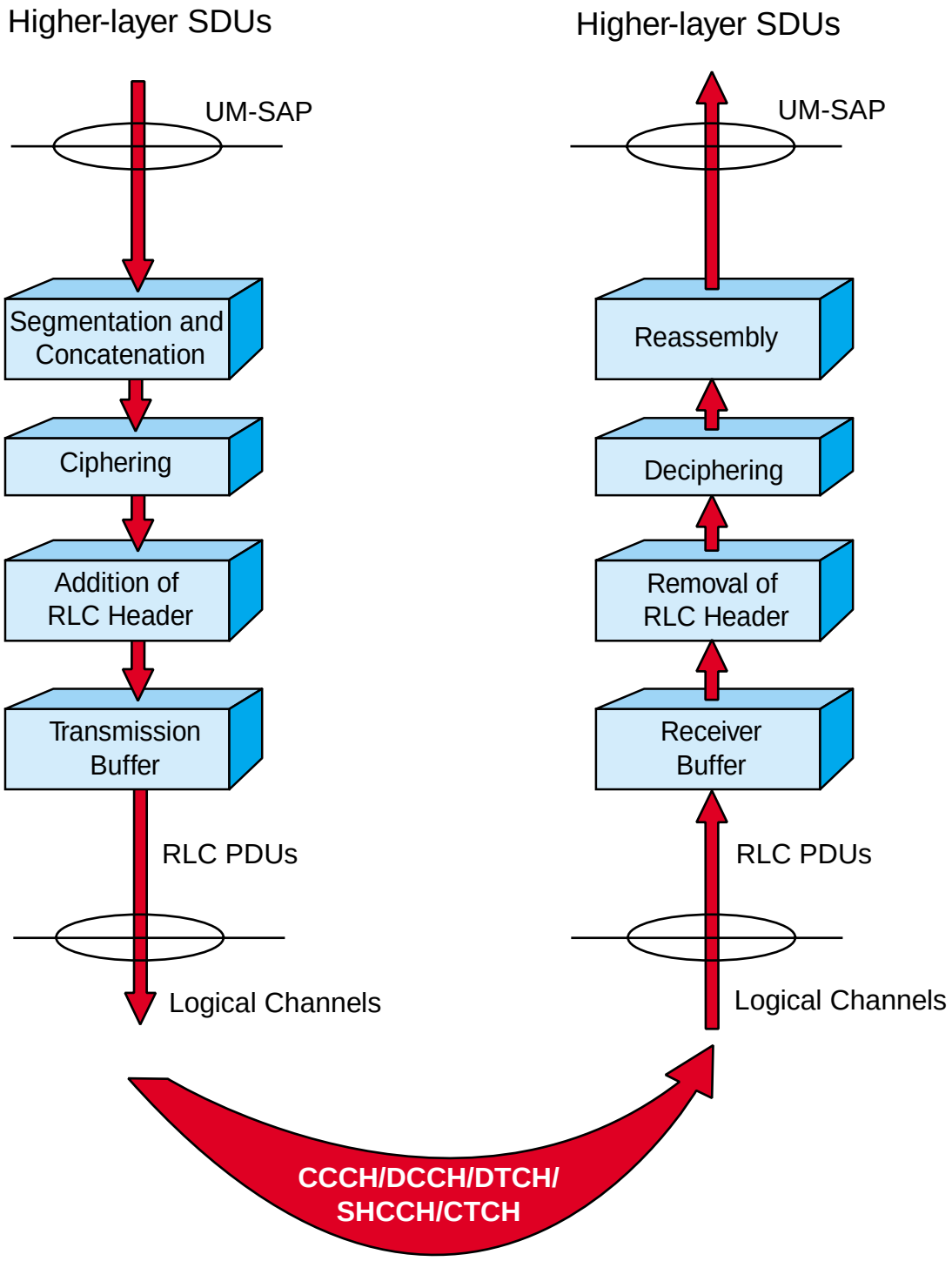


Figure 3
Unacknowledged Mode Operation

© wray castle limited

1.4 RLC Acknowledged Mode (AM)

As its name suggests the Acknowledged Mode (AM) of RLC provides for acknowledged transfer of higher-layer SDUs across the air interface. It will map these SDUs into logical channels and for AM there may be more than one logical channel for an RB. If more than one logical channel is used in the UL direction, then the RRC in the UTRAN may indicate that data will be passed through the first logical channel and control be passed through the second (shown in Figure 4 as a dotted line).

1.4.1 RLC AM Transmission

Higher-layer SDUs arrive through the RLC Acknowledged Mode Service Access Point (AM-SAP) and may be segmented or concatenated into Payload Units (PUs) of predetermined fixed length. The length of PUs for a particular RB is established by RRC in bearer set-up. It can only be changed as part of the RRC bearer reconfiguration procedure. This is followed by the addition of the RLC header information to form RLC PDUs.

PDUs are simultaneously passed to the retransmission buffer and the multiplexer (MUX). The MUX then decides which PDUs are delivered, and when they are delivered to the MAC layer.

As well as data-carrying PDUs, status PDUs also need to be exchanged. These may be transferred in their own right, or may be included as padding in data PDUs. This second option is known as *Piggybacking*.

Ciphering may be applied to PDUs, but it does not cover the RLC header. Following ciphering, PDUs are passed to the transmission buffer. Then finally, as they are passed to the MAC layer, they pass through a function that computes the fields in the RLC header.

1.4.2 RLC AM Reception

Incoming PDUs are retained in the receive buffer until a complete SDU has been received. Piggybacked-status PDUs are removed and retransmissions are triggered if required. Indications are passed to the retransmission buffer if positive acknowledgments of transmitted PDUs are received.

After RLC header removal, successfully recovered SDUs are passed back to higher layers.

© wray castle limited

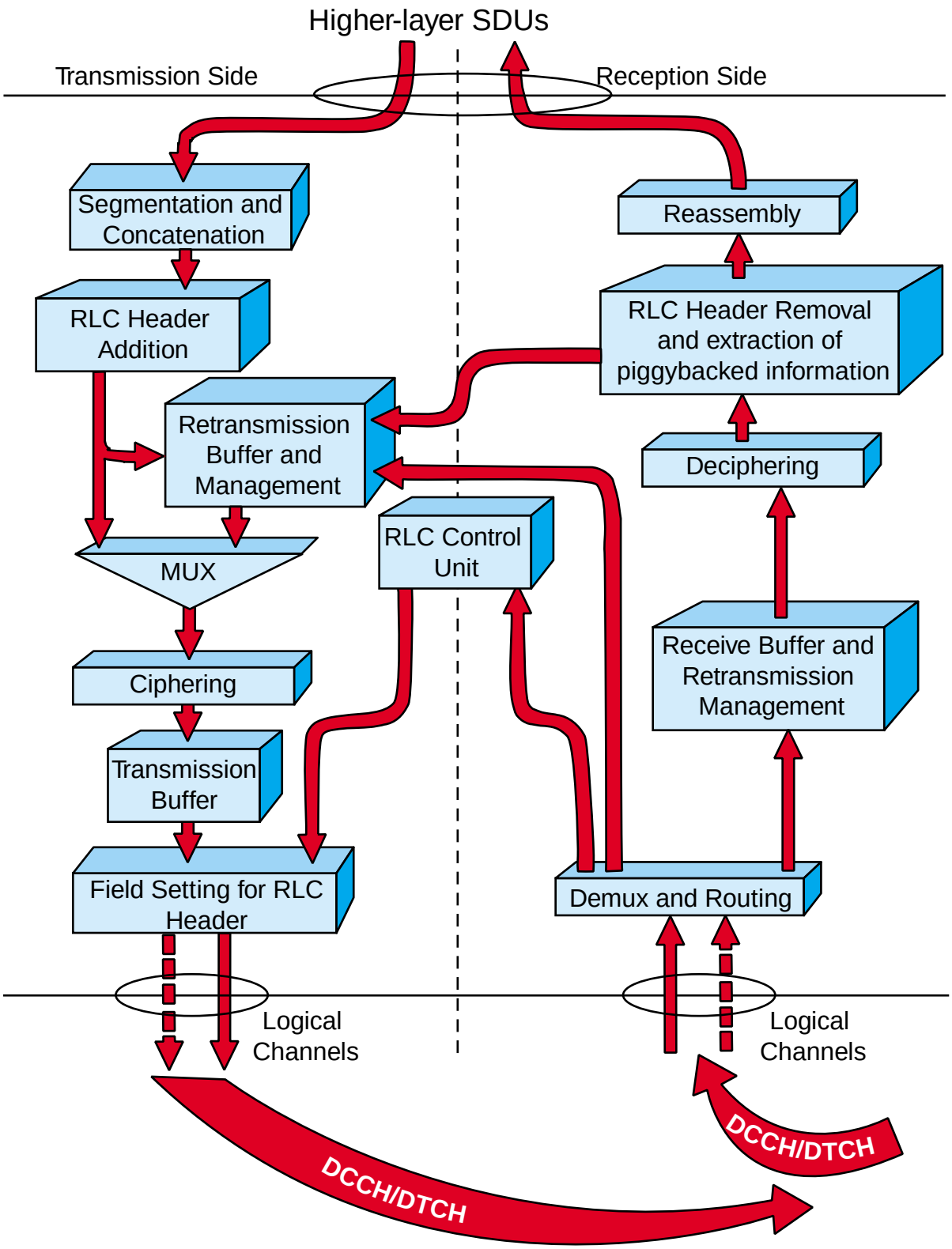


Figure 4
Acknowledged Mode Operation

© wray castle limited

2 RLC PROTOCOL DATA UNIT (PDU) TYPES

The range of PDU types defined for RLC is shown in Figure 5. Both the transparent mode and UM of RLC operation use only one type of PDU, but AM has five types available.

There is no RLC header to be added when the TrM is being used, thus the PDU simply consists of a block of higher-layer data. The data will be an SDU or a fragment of an SDU. This type of PDU is known as Transparent mode Data (TrD).

When UM is used, the PDU will contain higher-layer data and an RLC header. The higher-layer data will be an SDU, a fragment of an SDU, or, since concatenation may be used, more than one SDU. This type of PDU is known as Unacknowledged Mode Data (UMD).

For AM there is one type of PDU which is used to transfer a higher-layer SDU, and four which are used for peer-to-peer communication and control of RLC itself. The PDU that is used to carry higher-layer data is similar in structure to that used in UM, but it may also carry piggybacked STATUS information. This type of PDU is known as Acknowledged Mode Data (AMD).

Of the four control-related PDUs used in AM, there are two types used to carry status reports. The first, known as STATUS, is a stand-alone PDU; the second, known as Piggybacked STATUS, is included in the padding of an AMD. The remaining control related PDUs are RESET and RESET ACK; these are used to reset all protocol states, timers and variables in order to synchronize two peer entities.

© wray castle limited

RLC Mode	PDU Name	Description
Transparent	TrD	Transparent mode Data
Unacknowledged	UMD	Sequenced Unacknowledged Mode Data
Acknowledged	AMD	Sequenced Acknowledged Mode Data
	STATUS	Solicited or unsolicited status report
	Piggybacked STATUS	Piggybacked solicited or unsolicited status report
	RESET	Reset Command
	RESET ACK	Reset acknowledgement

Figure 5
RLC PDU Types

© wray castle limited

2.1 UMD PDU Structure

The UMD consists of two main parts, the RLC header and the PU. The RLC header itself can be divided into two elements, the first of which is the sequence number. In the UMD the sequence number is 7 bits long and is used for reassembly only. This may optionally contain one or more length indicators. Each length indicator may be either 7 or 15 bits long. The length indicators are used to identify the position of boundaries between SDUs concatenated within the PU. If there is more than one length indicator, they will appear in the same order as the SDUs to which they point. The length to the indicated boundary is in octets.

The PU consists of higher-layer SDUs and will be a whole number of octets. If the PU does not fill the whole of the PDU, then padding will be used to fill to the end.

© wray castle limited

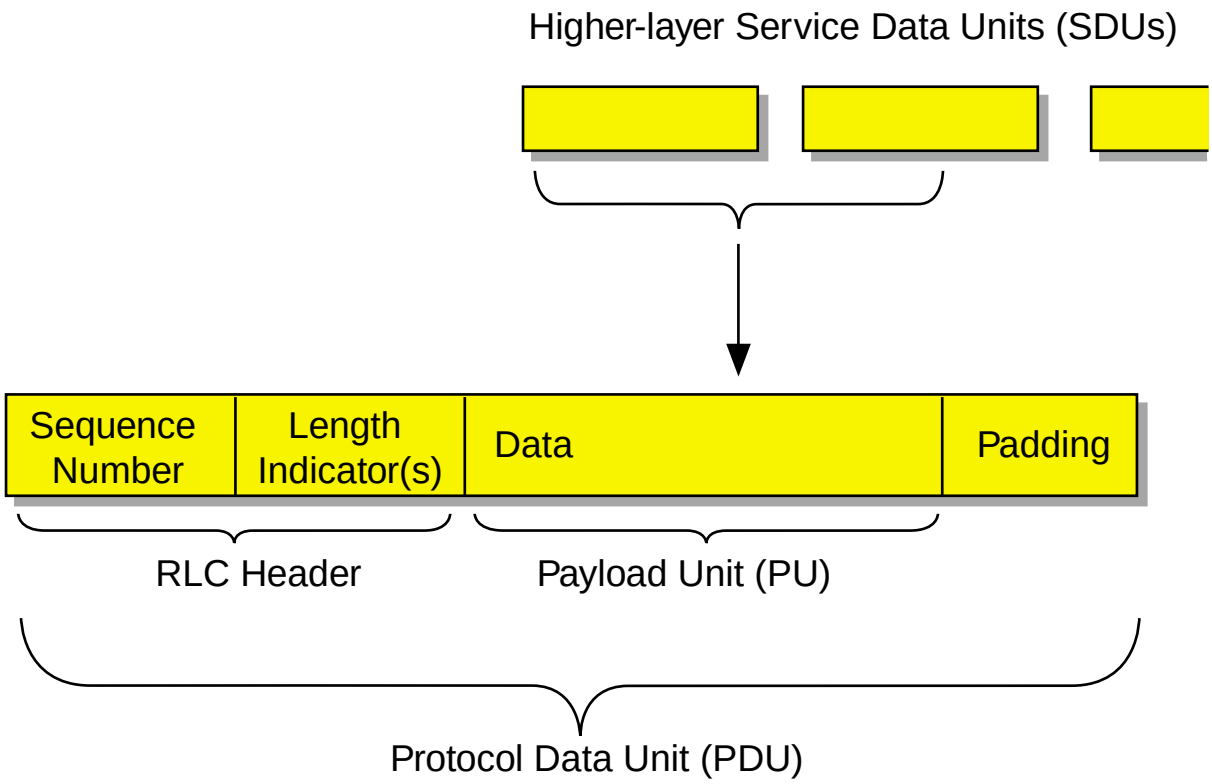


Figure 6
UMD PDU Structure

© wray castle limited

2.2 AMD PDU Structure

The RLC header for the AMD starts with the Data/Control (D/C) field. This is a single bit used to indicate whether it is a control or a data PDU; for the AMD, this will be set to indicate data. This is followed by the sequence number; for the AMD, the sequence number is 12 bits long and is used for both reassembly and retransmission.

The polling bit is used to request a status report from a peer entity. The 2-bit header extension field is used to indicate if there are any length indicators present. If there are length indicators present, then their function and structure is as for the UMD PDU.

The PU consists of higher-layer SDUs and will be a whole number of octets. If the PU does not fill the PDU, then padding will be used. If padding is present it may be replaced by a piggybacked STATUS PDU. The ability to include status reports within data PDUs in this way provides an efficiency gain.

© wray castle limited

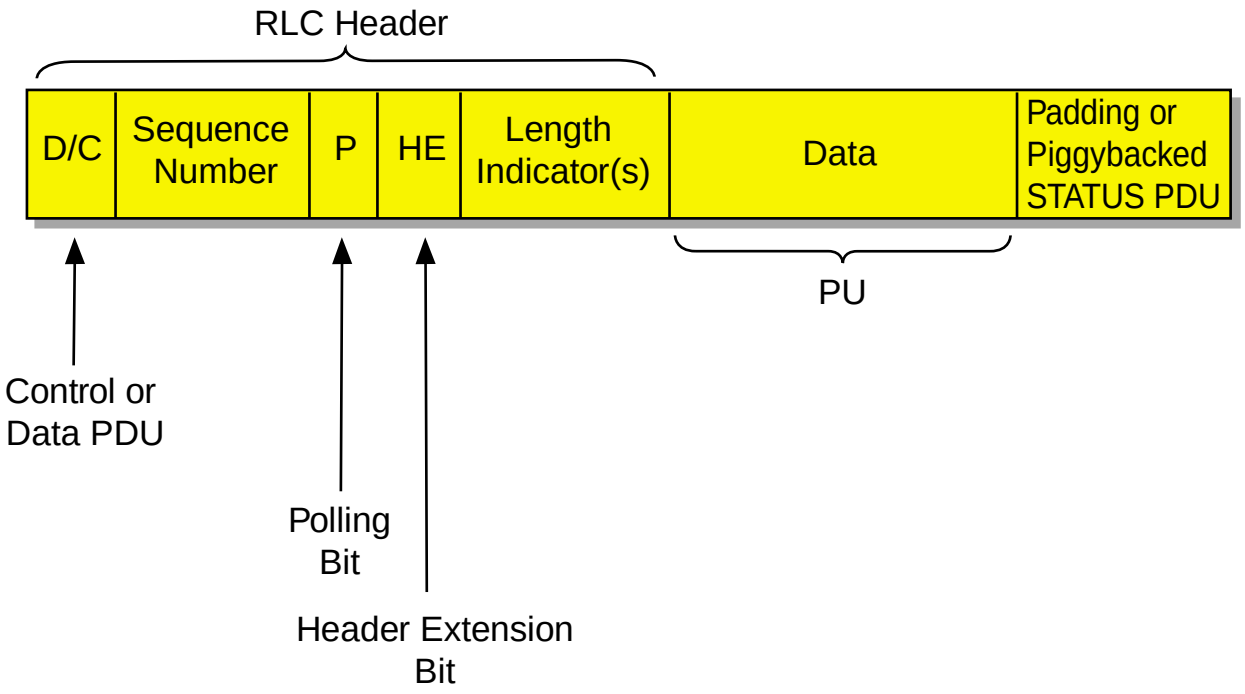


Figure 7
AMD PDU Structure

© wray castle limited

© wray castle limited

LESSON 3

MEDIUM ACCESS CONTROL (MAC)

© wray castle limited

LESSON CONTENTS

1 The Medium Access Control (MAC) Function 5.3.1

2 MAC Architecture 5.3.3
2.1 MAC Functional Entities (FEs) 5.3.3
2.2 MAC Functions 5.3.5

3 MAC Transmission Mechanisms 5.3.7
3.1 The MAC Header Information 5.3.7
3.2 Application of MAC Header Elements 5.3.9

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of the Medium Access Control (MAC) protocol

© wray castle limited

1 THE MEDIUM ACCESS CONTROL (MAC) FUNCTION

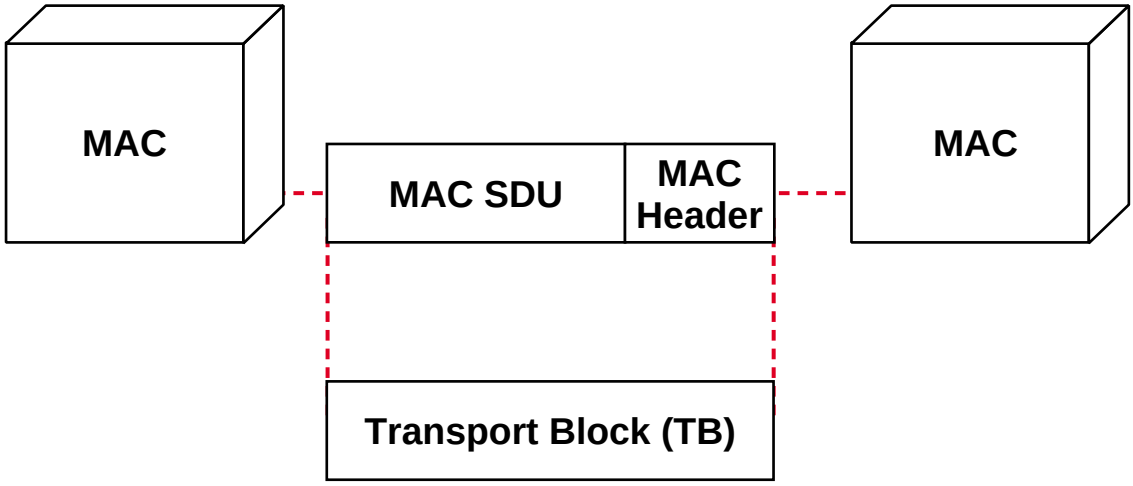
Medium Access Control (MAC) formats information into Service Data Units (SDUs), then adds a MAC header. The combination of MAC header and SDU is identified using the term *Transport Block* (TB). TBs are sent in a transport channel (e.g. RACH, DCH). Data frames on the Iub/Iur interface will contain these TBs.

The MAC function can be split into three entities:

- MAC-b – Broadcast Transport Channel
- MAC-c/sh – Common and Shared Transport Channels
- MAC-d – Dedicated Transport Channels

The MAC entity can terminate at the Node B, the Serving Radio Network Controller (SRNC) or the Drift RNC (DRNC).

© wray castle limited



- MAC-b is the MAC entity that handles the:
  - Broadcast Channel (BCH)

- MAC-c/sh is the MAC entity that handles the:
  - Paging Channel (PCH)
  - Forward Access Channel (FACH)
  - Random Access Channel (RACH)
  - Common Packet Channel (CPCH)
  - Downlink Shared Channel (DSCH)
  - Uplink Shared Channel (USCH) TDD Mode

- MAC-d is the MAC entity that handles the:
  - Dedicated Transport Channel (DCH)

Figure 1
MAC

© wray castle limited

2 MAC ARCHITECTURE

2.1 MAC Functional Entities (FEs)

There are three FEs within the MAC sublayer, these are the MAC-b, MAC-c/sh and MAC-d. Each of these entities is accessed using logical channels from the RLC sublayer, and each exchanges data with the physical layer using transport channels. The MAC sublayer is also connected directly to RRC via the MAC control Service Access Point (SAP). This is used by RRC to configure the MAC for information transfer and for the measurement processes.

The exact structure of MAC and the functions of the MAC entities are slightly different for the UE and the UTRAN.

2.1.1 MAC for the Broadcast Channel (MAC-b)

The MAC-b function maps information directly from the BCCH logical channel to the BCH transport channel. There is no addition of MAC header information associated with the use of MAC-b. In the UTRAN there will be one instance of MAC-b for each cell. In the UE there will be only one instance of MAC-b.

2.1.2 MAC for the Common and Shared Channels (MAC-c/sh)

The MAC-c/sh handles the mapping of all information associated with common transport channels. This includes signalling and traffic information. The mapping process for MAC-c/sh entails multiplexing and the addition of MAC header information. In the UTRAN there will be one instance of MAC-c/sh for each cell. In the UE there will be only one instance of MAC-c/sh.

2.1.3 MAC for the Dedicated Channels (MAC-d)

The MAC-d handles the mapping of information between the dedicated logical channels DCCH and DTCH to the transport channel DCH. This mapping process entails multiplexing and the addition of MAC header information. The MAC-d may also be used to map information into the common transport channels; in this case, the information is passed from MAC-d to MAC-c/sh. There is only one instance of MAC-d in a UE, and one in the UTRAN for each UE.

© wray castle limited

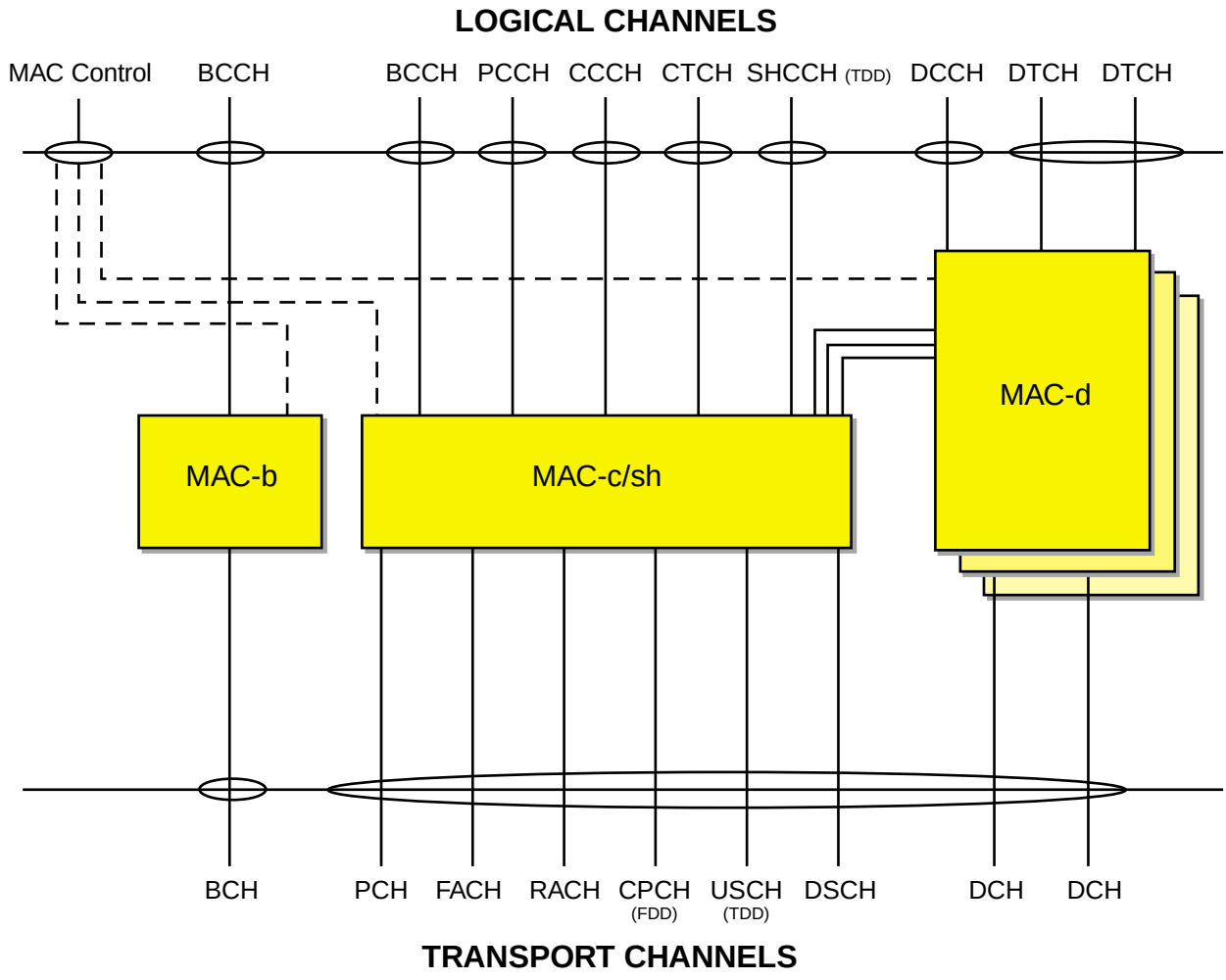


Figure 2
General MAC Entities

© wray castle limited

2.2 MAC Functions

The main functions of the MAC sublayer are summarized in Figure 3. These functions could be divided into two areas: those that deal directly with the formatting of data as it passes through the MAC sublayer, and those that relate to MAC processes and procedures.

Regarding the formatting of data, MAC accepts data through one of the logical channels as RLC PDUs. The MAC sublayer is then responsible for the mapping and multiplexing of PDUs into the appropriate transport channels. There may be other functions relating to the transfer of this data, including the identification of the communicating UE and priority handling. For data flows that are using the TrM of RLC, the MAC-d entity will apply ciphering and deciphering. Once data is correctly formatted, the MAC sublayer is responsible for the selection of an appropriate transport format for its transmission in a transport channel. Data is passed from the MAC layer to the physical layer as transport blocks.

Another function performed by the MAC sublayer is the selection of Access Service Class (ASC) for the use of the RACH and the CPCH.There are eight different access classes ranging from 0–7, 0 being the highest priority, 7 the lowest. An example of an access class of 0 is an emergency call or a service of the same priority level. In addition, MAC controls the access functions required for the use of RACH and CPCH, and is responsible for the reporting of traffic volume and physical layer measurements.

© wray castle limited

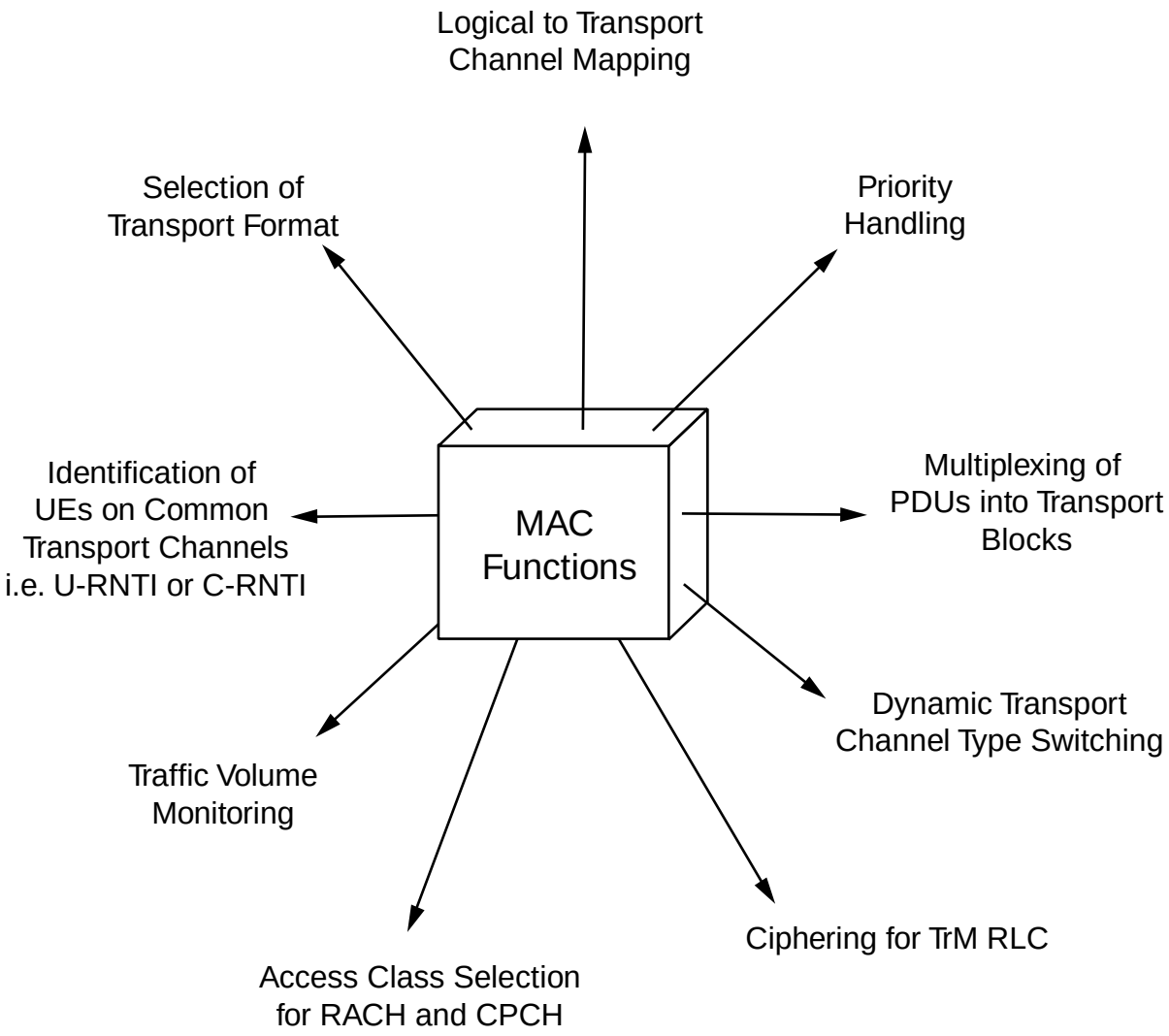


Figure 3
Functions of MAC

© wray castle limited

3 MAC TRANSMISSION MECHANISMS

3.1 The MAC Header Information

The MAC sublayer accepts higher-layer PDUs; these can be considered to be bit strings of any length. The higher-layer PDU then becomes the payload in a MAC PDU and is, as such, referred to as a MAC Service Data Unit (SDU). The size and contents of the MAC header will vary, depending on the services being offered by MAC. The MAC SDU and the MAC header are collectively referred to as a MAC PDU. These must be passed to the physical layer via the transport channels in such a way that they may be mapped at the correct rate into physical channels. This is achieved through the use of transport blocks.

Each transport block contains one MAC PDU. Transport blocks may then be grouped into a transport block set, which will be passed to the physical layer. When a transport channel is established, a Transmission Time Interval (TTI) is set, which corresponds to the interleaving period for the channel. One transport block set is passed through the transport channel for each TTI.

There may be up to four elements in the MAC header. Those that are present and their contents will depend on the logical/transport channel combinations in use.

3.1.1 Target Channel Type Field (TCTF)

This field is present only when the RACH/FACH transport channels are being used. For TDD mode it is also used for the Uplink Shared Channel/Downlink Shared Channel (USCH/DSCH). It indicates which logical channels are being mapped to the RACH/FACH. There are currently five values defined for FDD mode: BCCH, CCCH, CTCH, or DCCH. For TDD mode there are three additional values, SHCCH over RACH/FACH, SHCCH over USCH/DSCH and DTCH/DCCH over USCH/DSCH.

3.1.2 Channel Type (C/T)

This field is used to identify a particular logical channel for instances where multiple logical channels are multiplexed into one transport channel. It is a 4-bit field providing logical channel numbering from 1 to 15.

3.1.3 User Equipment Identity (UE-Id)

The UE-Id field is included in the header when a dedicated logical channel is being carried on a common transport channel. The UE-Id itself will be either a UTRAN Radio Network Temporary Identifier (u-RNTI) or a Cell Radio Network Temporary Identifier (c-RNTI). The UE-Id type field is used to indicate which is being carried. For a DCCH, the UE-Id used will be the u-RNTI, and for DTCH and DSCH it will be the c-RNTI.

© wray castle limited

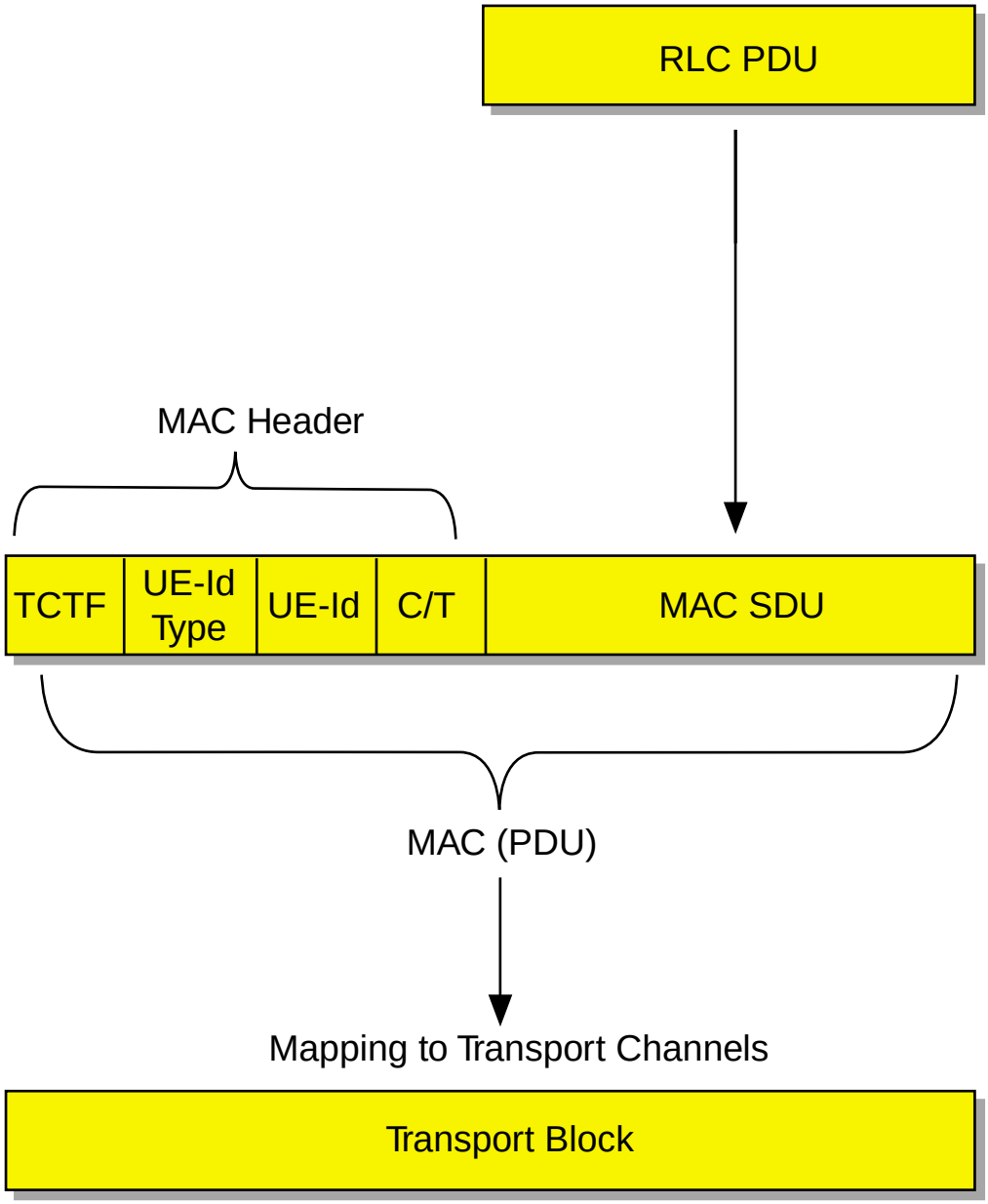


Figure 4
Addition of the MAC Header

© wray castle limited

3.2 Application of MAC Header Elements

Figure 5 summarizes the applicability of MAC header elements for various logical and transport channel combinations. It can be seen that there is some variation between elements used in FDD mode and TDD mode.

For the BCCH, when carried on the BCH and the PCCH there is no requirement for the MAC header because for these channels there are no variables in terms of MAC routing to higher layers. This is also true of the DTCH and the DCCH when they are carried on a dedicated transport channel.

For other combinations of logical and transport channel, the TCTF and/or the T/C fields may be present where there are different possibilities for logical to transport channel mapping. For shared transport channels, the UE-Id is present so that the intended UE can be correctly addressed at the receiving end.

© wray castle limited

Logical	Transport	MAC Header Elements
DTCH/DCCH	DCH (no multiplexing)	None
	DCH (with multiplexing)	C/T
DTCH/DCCH	RACH/FACH	TCTF C/T UE-Id Type UE-Id
DTCH/DCCH	DSCH/USCH (no multiplexing)	TCTF (TDD) UE-Id Type (FDD) UE-Id (FDD)
	DSCH/USCH (with multiplexing)	TCTF C/T UE-Id Type (FDD) UE-Id (FDD)
BCCH	BCH	None
BCCH	FACH	TCTF
PCCH	PCH	None
CCCH	RACH/FACH	TCTF
CTCH	FACH	TCTF

Figure 5
Application of MAC Header

© wray castle limited

© wray castle limited

LESSON 4

PACKET DATA CONVERGENCE PROTOCOL (PDCP) AND BROADCAST/MULTICAST CONTROL (BMC)

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Packet Data Convergence Protocol (PDCP) 5.4.1
1.1 General Functions of the PDCP 5.4.1
1.2 PDCP Architecture 5.4.1
1.3 Acknowledged PDCP Transfer 5.4.3
1.4 The PDCP Header 5.4.5

2 Broadcast/Multicast Control (BMC) 5.4.7
2.1 Location of BMC 5.4.7
2.2 General Functions of BMC 5.4.9

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe the use and scope of the following products:
  - Packet Data Convergence Protocol (PDCP)
  - Broadcast/Multicast Control (BMC)

© wray castle limited

1 PACKET DATA CONVERGENCE PROTOCOL (PDCP)

1.1 General Functions of the PDCP

The Packet Data Convergence Protocol (PDCP) exists in the user plane only. It is located just above the RLC, but is still considered part of layer 2. Its main function is to provide compression of packet headers for efficiency in the radio channel. This can be done because there is likely to be a large percentage of redundant header information in IP datagrams (e.g. TCP/IP. Several compression algorithms are available to PDCP, thus it can provide transparency through the UTRAN for a range of network layer protocols without the need for modification to lower-layer protocols.

In addition, the PDCP may maintain sequence numbers within the RBs for support of loss-less SRNC relocation.

1.2 PDCP Architecture

The PDCP has access to all three modes of RLC, i.e. Acknowledged Mode Service Access Point (AM-SAP), Unacknowledged Mode Service Access Point (UM-SAP) and Transparent Mode Service Access Point (Tr-SAP). For Release 1999 there is a one-to-one relationship between a PDCP-SAP, a PDCP entity and an RLC SAP, as shown in Figure 1. For Release 2000 it is expected that multiplexing will be included.

It can be seen that for AM PDCP entities there is the inclusion of PDCP sequence numbering.

© wray castle limited

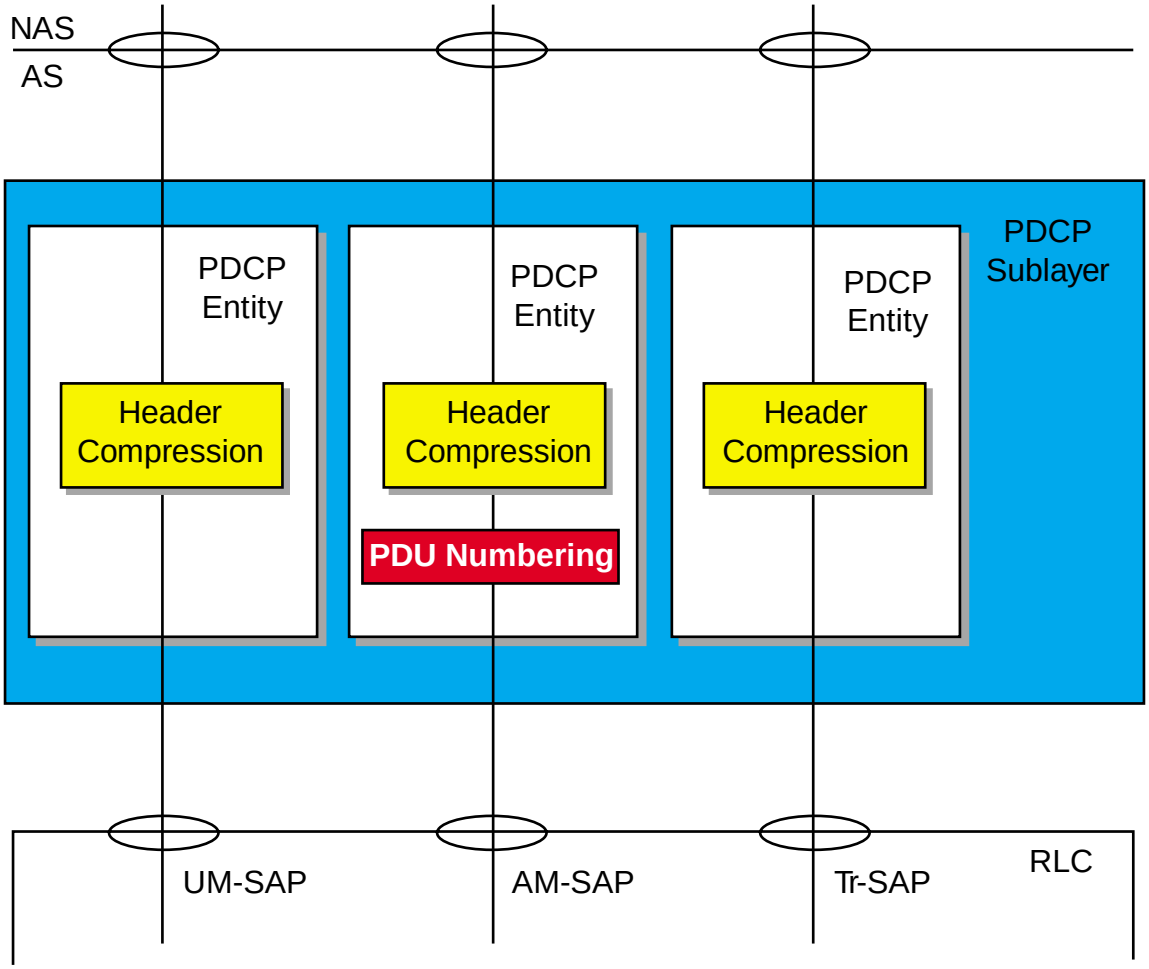


Figure 1
PDCP Architecture

© wray castle limited

1.3 Acknowledged PDCP Transfer

Figure 2 shows an IP datagram being transferred using PDCP and the Acknowledged Mode (AM) of RLC. The services provided by PDCP and RLC will have been established in the RRC connection establishment procedure.

1 The IP datagram is passed to PDCP using the primitive PDCP-DATA.req. The PDCP sublayer will perform the header compression as negotiated. The PDCP header information will be added, which will contain information about the type of compression applied and perhaps a sequence number.

2 The PDCP sublayer passes the PDCP PDU to RLC via the AM-SAP in the primitive RLC-AM-DATA.req. The RLC sublayer treats the arriving data as an RLC SDU.

3 RLC applies the AM of data transfer, including segmentation of the RLC SDU into multiple RLC PDUs and, if required, retransmission.

4 RLC reassembles the RLC SDU and passes it to PDCP in the primitive RLC-AM-DATA.ind.

5 PDCP removes the header information and passes the IP datagram to the higher-layer protocols using the primitive PDCP-DATA.ind.

6 The RLC sublayer will indicate the successful transfer of the RLC SDU to its peer entity with the primitive RLC-AM-DATA.cnf.

© wray castle limited

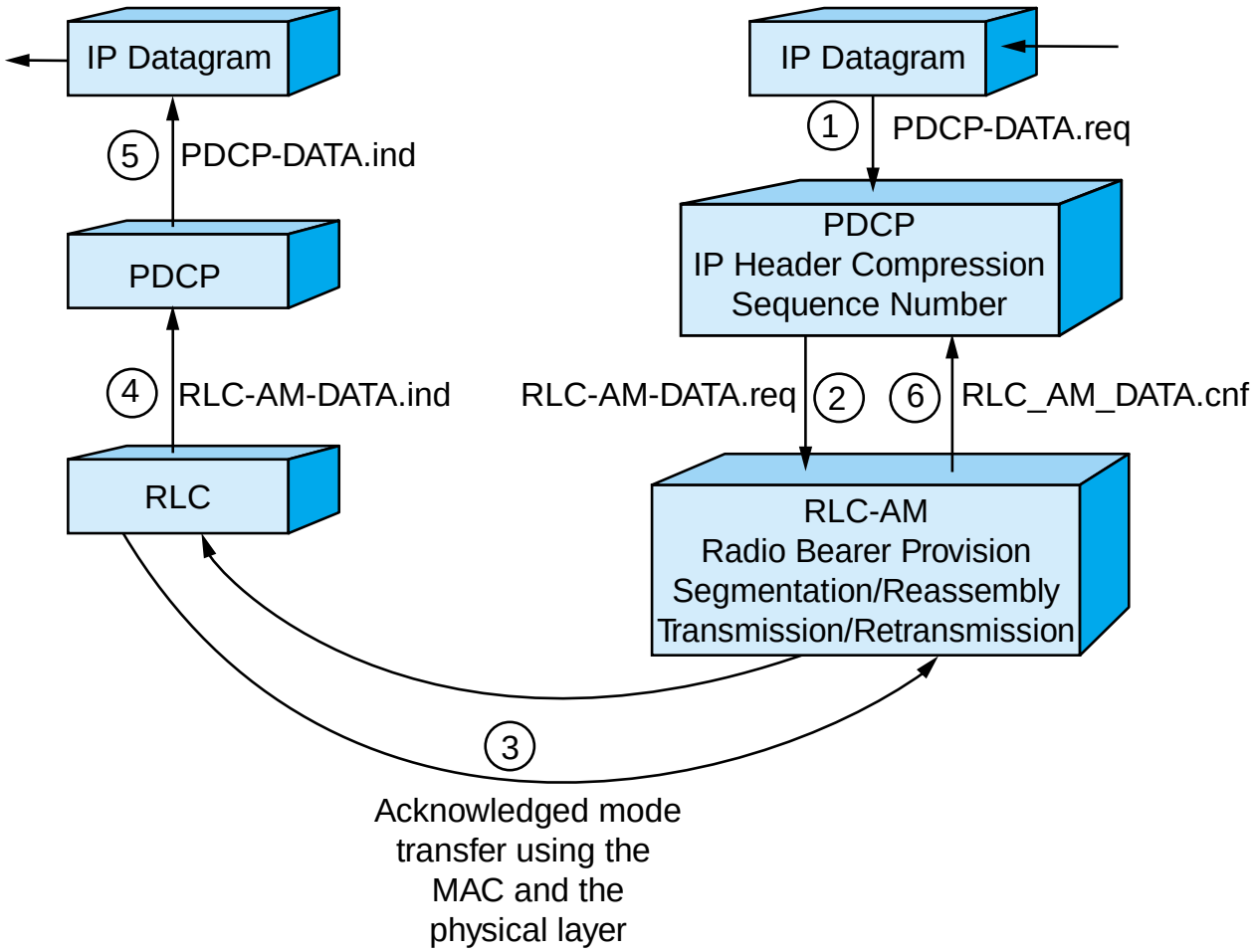


Figure 2

PDCP Acknowledged Transfer

© wray castle limited

1.4 The PDCP Header

There may be between zero and three elements in the PDCP header, depending on the services being applied by PDCP. Figure 3 shows a PDCP PDU with all three elements in place.

The PDU type field has two possible values, one that indicates the presence of the Packet Identifier (PID), and one that indicates the presence of the PID field and the sequence number.

The PID field is used to indicate the type of header compression that has been applied.

The sequence number is used to maintain loss-less PDCP transfer during an SRNC relocation.

© wray castle limited

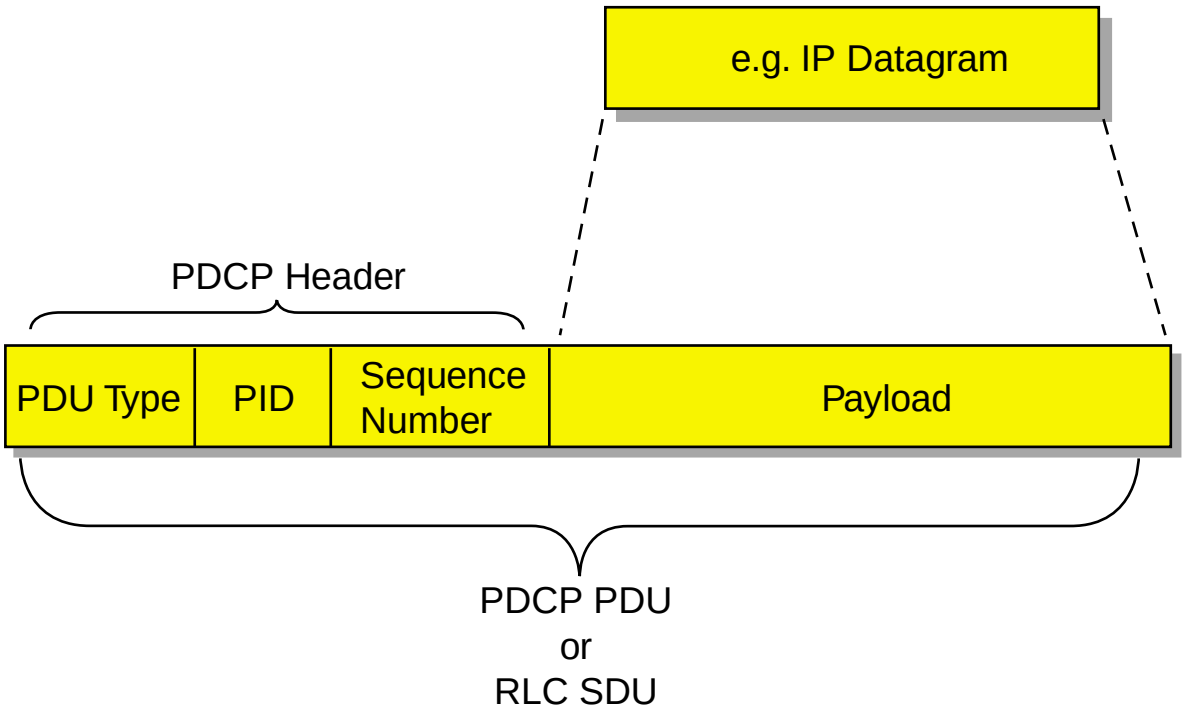


Figure 3
The PDCP Header

© wray castle limited

2 BROADCAST/MULTICAST CONTROL (BMC)

2.1 Location of BMC

The Broadcast/Multicast Control (BMC) exists only in the user plane. It is located above the RLC sublayer but is considered part of layer 2. The BMC makes use of the unacknowledged service of RLC for the transfer of Cell Broadcast (CB) messages. From RLC, these messages will be transferred using a CTCH/FACH logical and transport channel combination.

For Release 1999 the only user protocol using BMC will be the Short Message Service – Cell Broadcast (SMS-CB) protocol defined for GSM. In future releases, more use may be made of BMC capabilities.

The BMC sublayer exchanges control information with RRC in order to provide for the most efficient scheduling for the transmission of CB messages.

There is one BMC entity in the UE and one in the RNC for each cell. This enables separate scheduling of CB messages for each cell.

© wray castle limited

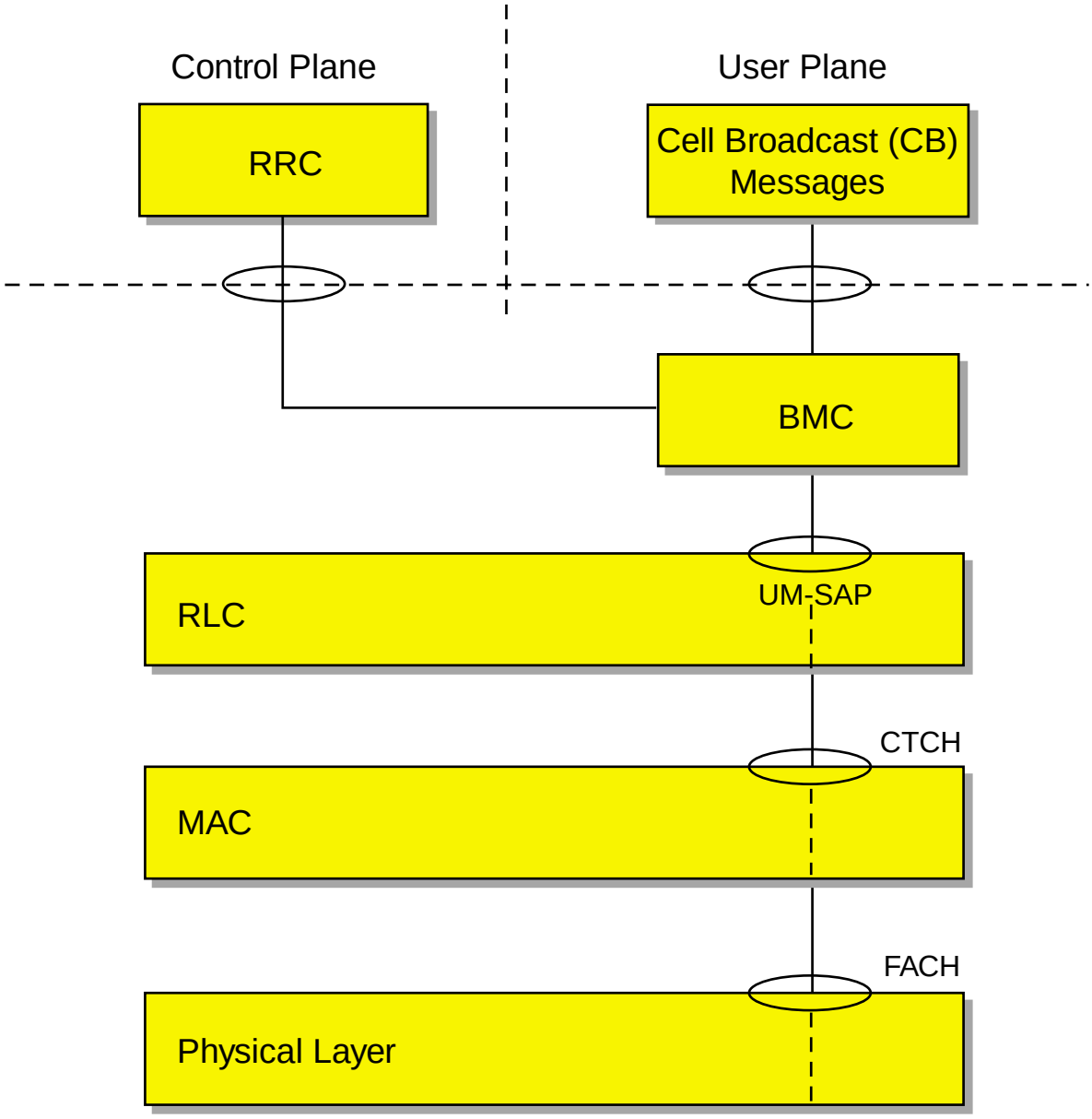


Figure 4
BMC Location

© wray castle limited

2.2 General Functions of BMC

1 CB messages are passed to the RNC from the CN entity, which may be either evolved GSM or ANSI IS-41. They are then passed to the BMC sublayers for each cell in which each message should be broadcast. The BMC sublayer is responsible for scheduling messages according to the information supplied with each message, i.e. the number of repetitions and repetition period.

2 The BMC assesses the required rate for cell broadcast transfer in each transmission cycle and indicates this to RRC. RRC responds with an appropriate configuration for CTCH.

3 The BMC generates a scheduling message and passes this on along with the CB messages for transmission over the air interface.

4 The BMC sublayer in the UE uses the scheduling message to indicate to RRC messages that should be received. Received CB messages are then passed on to the higher-layer entities.

© wray castle limited

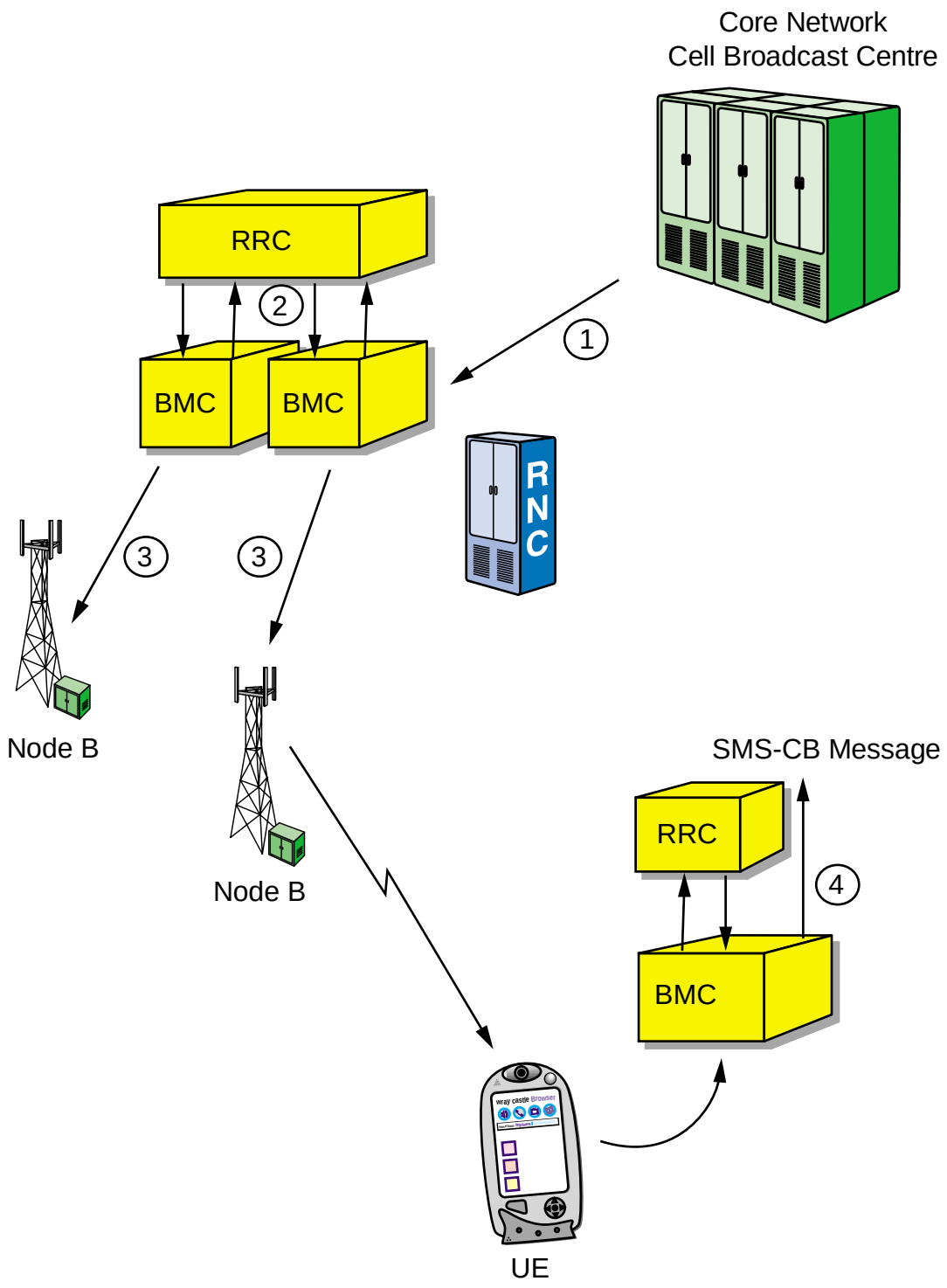


Figure 5
BMC Transfer Mechanism

© wray castle limited

© wray castle limited

SECTION 6

TERRESTRIAL PROTOCOLS

© wray castle limited

LESSON 1

Iub PROTOCOLS

© wray castle limited

LESSON CONTENTS

1	**Protocol Structures for the UTRAN Interfaces**		**6.1.1**
	1.1	General Interface Protocol Model	6.1.1
	1.2	Iub Interface Protocol Structure	6.1.3
2	**Protocol Structures**		**6.1.5**
	2.1	Iub Transport Protocol Structure	6.1.5
3	**Node B Application Part (NBAP)**		**6.1.7**
	3.1	Services Provided by NBAP	6.1.7
	3.2	NBAP Support for Logical O&M	6.1.9
	3.3	Functions of NBAP	6.1.11
	3.4	NBAP Data Transfer	6.1.13
	3.5	Cell Set-up	6.1.15
	3.6	Common Transport Channel Set-up	6.1.15

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of the protocols found in the user plane and control plane on the Iub interface

© wray castle limited

1 PROTOCOL STRUCTURES FOR THE UTRAN INTERFACES

1.1 General Interface Protocol Model

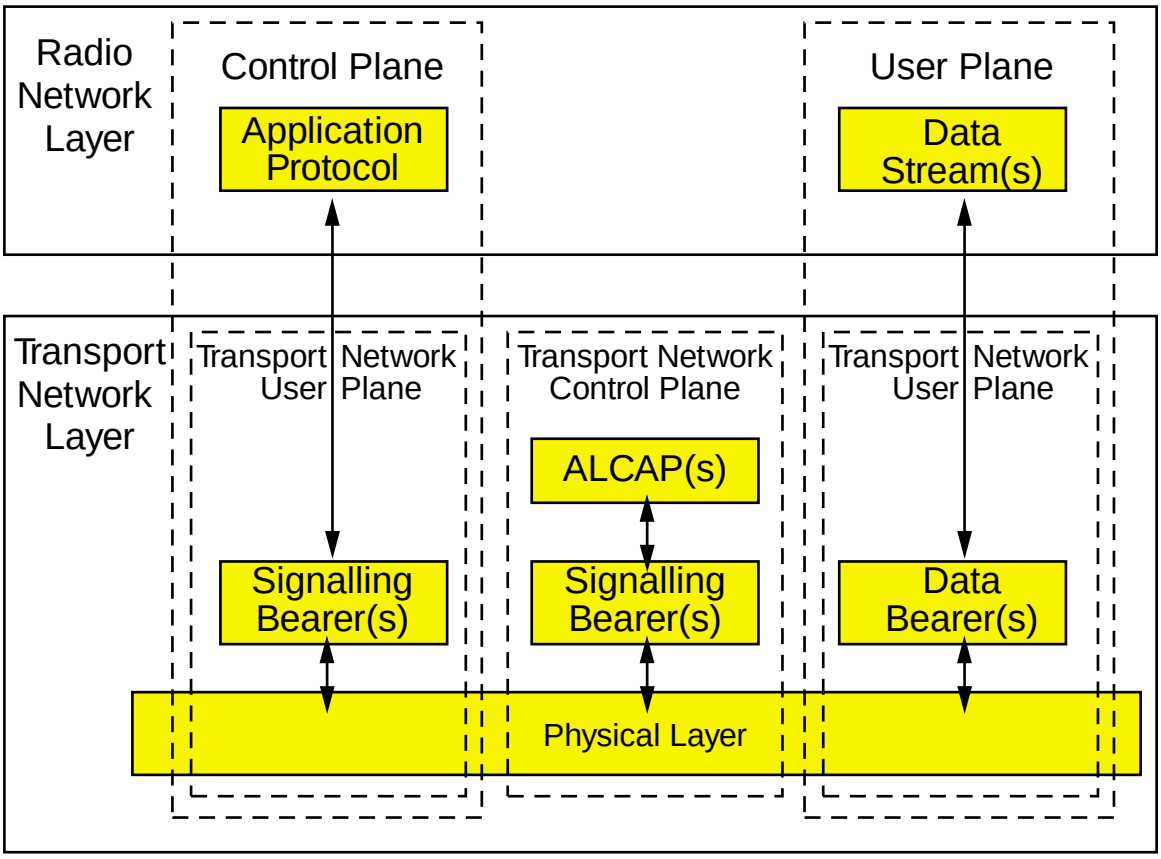
The general protocol model for individual UTRAN interfaces is split into two distinct layers – the Radio Network Layer and the Transport Network Layer. The UTRAN procedures and issues are contained solely in the Radio Network Layer.

The Radio Network Layer is divided into the Control Plane and the User Plane, which follows the general protocol architecture for the UTRAN. However, it must be remembered that on any specific interface, the User Plane simply describes the structure of data on that particular interface. Therefore RRC, which in the overall UTRAN general protocol architecture is considered to be control information, is carried transparently over the Iub interface and is therefore regarded as part of the User Plane on that particular interface.

The Transport Network Layer provides the means to transfer both Radio Network Layer Control Plane information and User Plane information, providing signalling bearer(s) and data bearer(s) respectively. Both these cases are considered to be part of the Transport Network Layer User Plane, with only the actual signalling (ALCAP) required to set up the bearer(s) being considered part of the Transport Network Layer Control Plane. Further to this, the signalling bearers (for both the application protocol and ALCAP) are set up by Operations and Maintenance (O&M) action, hence the Transport Network Control Plane is present solely to set up the required data bearers.

Although the signalling bearers are set up by O&M action, connection establishment, by way of exchanging identifiers, may still be required on the Iu and Iur interfaces at SCCP level in order to allow different RANAP and RNSAP procedures to be identified.

© wray castle limited



All UTRAN-related issues are visible
only in the Radio Network Layer

Figure 1

General Protocol Model for UTRAN Interfaces

© wray castle limited

1.2 Iub Interface Protocol Structure

On the Iub interface, the Radio Network Layer User Plane is made up of data carried within the relevant logical and transport channels. Framing protocols are used to frame each of the transport channels. The channels themselves carry either user data or RRC information. In all cases, though, the data is contained in the appropriate transport channel, which in turn is carried transparently over the Iub interface (in the framing protocol), and is therefore considered to be User Plane information on this interface. This is shown in Figure 2.

In the Control Plane, NBAP provides the mechanism to control the transparent transfer of User Plane information, as well as to provide all other UTRAN control functionality that is relevant in the Radio Network Layer on this interface.

Since User Plane information, in the form of transport channels within appropriate framing protocols, is carried in switched virtual circuits in the Transport Layer, the Transport Network Control Plane is comprised of the signalling protocols (ALCAP) required to set these up. Note that the Iub interface exists between a Node B and the Controlling RNC only, hence a point-to-point link exists for both ALCAP signalling and NBAP signalling. This is reflected in the protocol structure of the signalling bearers. On the Iur interface, a further layer is introduced, the Message Transfer Part (MTP) of Signalling System No. 7 (SS7), to allow for the routing of signalling messages between different RNCs as required.

The signalling bearers used to carry both this ALCAP information and NBAP signalling are predefined.

© wray castle limited

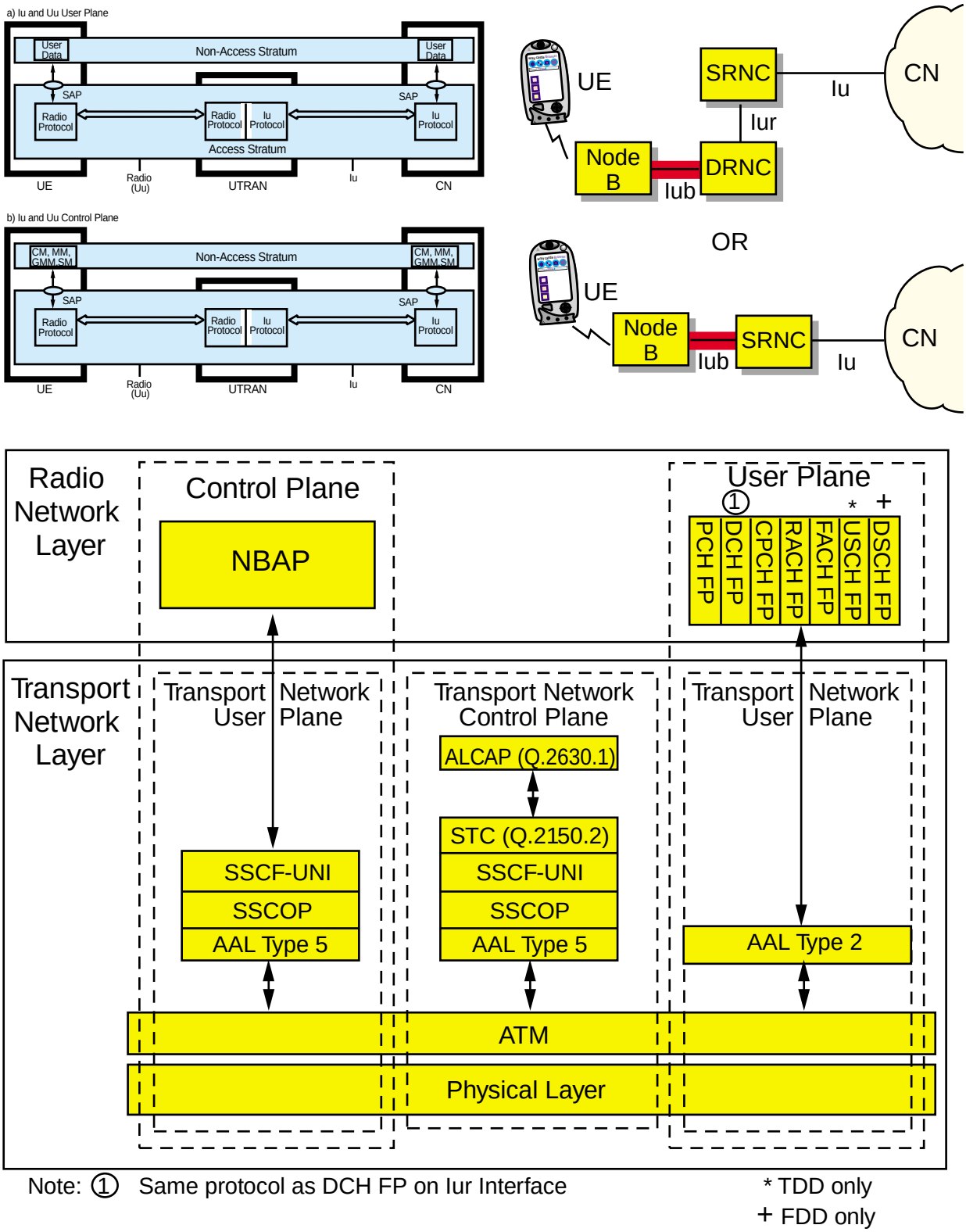


Figure 2

Iub Interface Protocol Structure

© wray castle limited

2 PROTOCOL STRUCTURES

2.1 Iub Transport Protocol Structure

The Iub interface uses the transport protocol structure shown in Figure 3. The AAL Type 2 signalling function resides on top of the Signalling Transport Converter (STC) (ITU-T Recommendation Q.2150.2).

This STC provides:

- independence from the underlying transmission media
- transparency of the information transferred
- connection establishment and release

In addition, the following SSCOP services are utilized:

- Sequence Integrity of STC-SDUs
- Error Correction of STC-SDUs
- Flow Control of STC-SDUs
- Keep Alive

AAL Type 2 STC resides on top of the SSCS. It deploys the services provided by SSCOP. SSCOP needs to have a connection established; the STC establishes and maintains this connection on behalf of its user, and the user is informed about the availability of the assured data transfer service.

In the SSCS, the SSCF is *Null*, in the sense that primitives arriving from STC are mapped directly into primitives for SSCOP.

SSCOP uses the service of the CPCS and SAR protocols, which provide an unassured information transfer and a mechanism for detecting corruption of SSCOP PDUs.

© wray castle limited

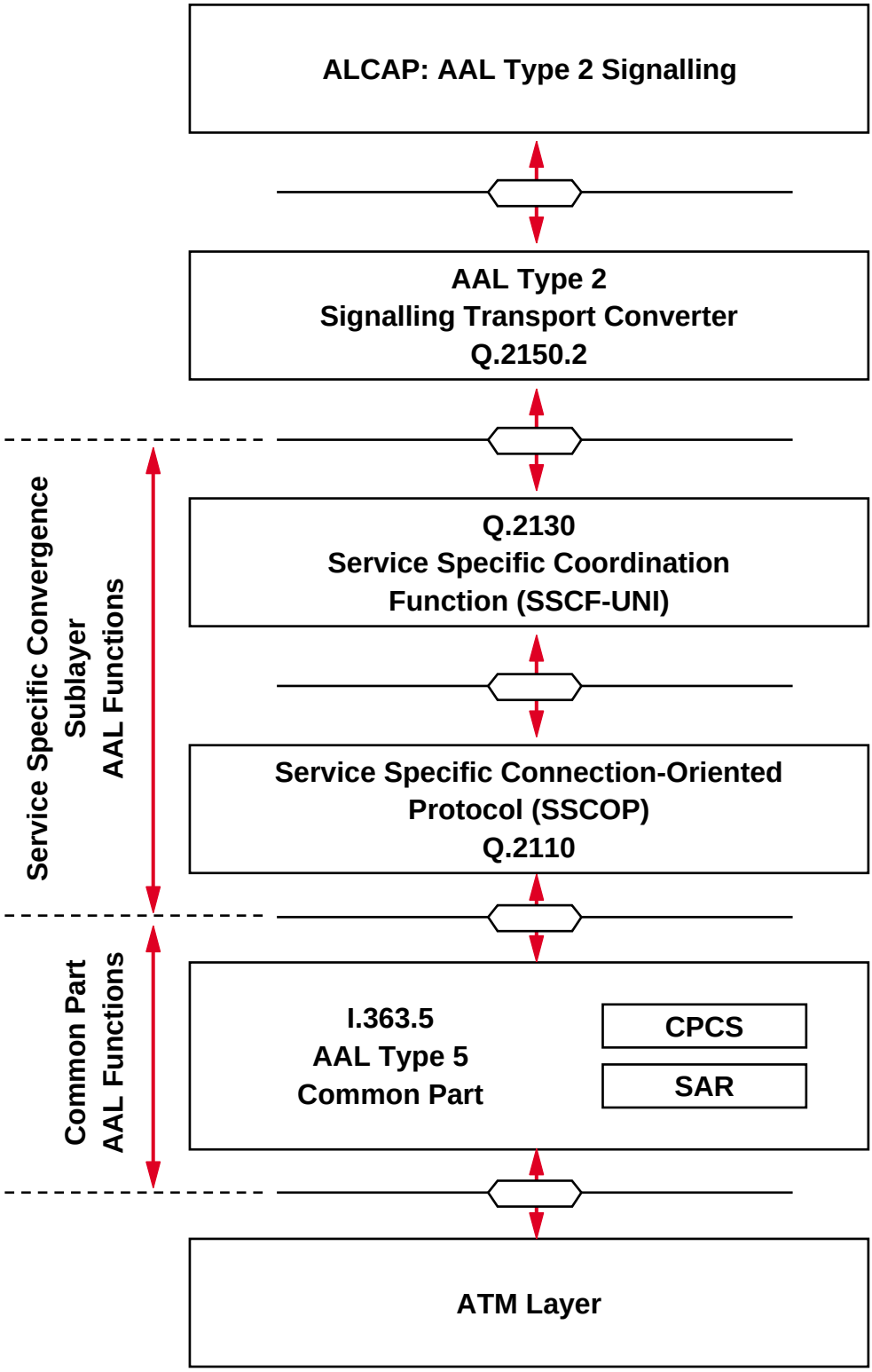


Figure 3
Iub Protocol Structure

© wray castle limited

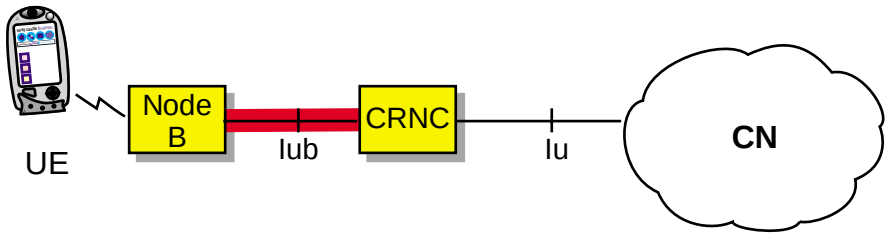
3 NODE B APPLICATION PART (NBAP)

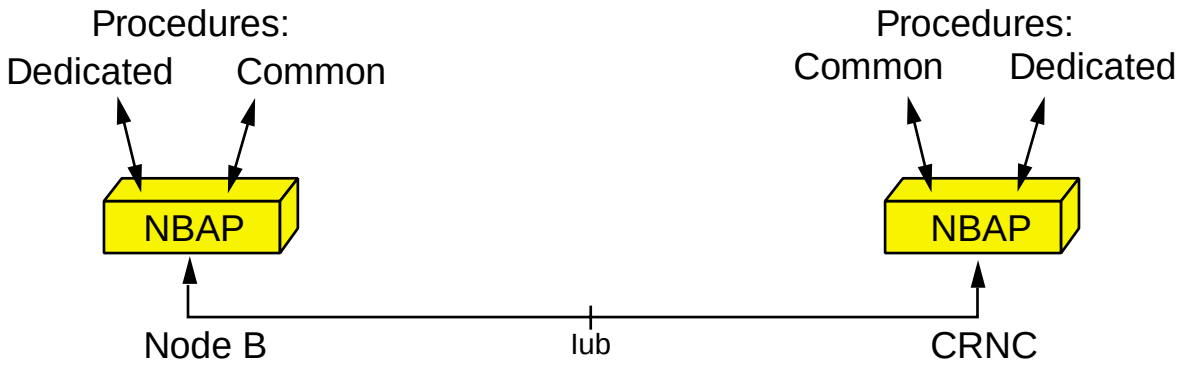
3.1 Services Provided by NBAP

The NBAP procedures are identified as common or dedicated. Common procedures are either request initiation for a UE context, or procedures not related to a specific UE. Dedicated procedures are related to a specific UE context.

Examples of the procedures that NBAP covers are paging distribution, broadcast system information, request/complete/release of dedicated resources, and management of logical resources.

© wray castle limited





NBAP:

- Includes common and dedicated procedures
- Covers:
  - Paging distribution
  - Broadcast system information
  - Request/Complete/Release of dedicated resources
  - Management of logical resources (logical O&M)

Note: Implementation-specific O&M is not supported by NBAP signalling, but logical O&M (i.e. RNC control of Node B resources) is supported.

Figure 4

Services Provided by NBAP

© wray castle limited

3.2 NBAP Support for Logical O&M

The O&M function at the Node B is split into two parts:

Implementation-Specific O&M
This consists of the O&M linked to the Node B. The Node B hardware and software components depend on the implementation of the Node B. It therefore needs to be implementation-dependent.

Logical O&M
This is the control of logical resources owned by the RNC but physically implemented at the Node B. NBAP controls the information transfer between the RNC and the Node B.

© wray castle limited

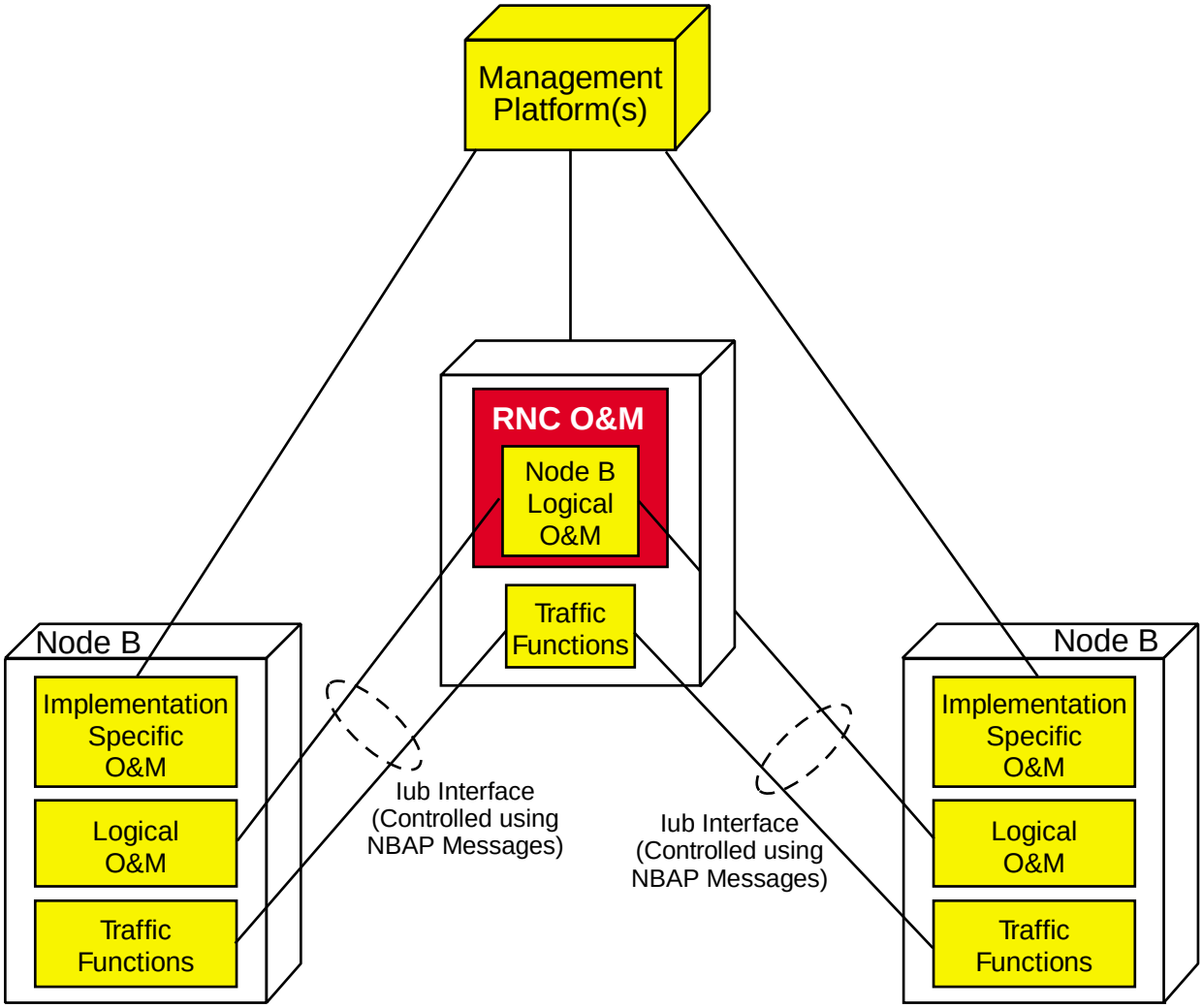


Figure 5

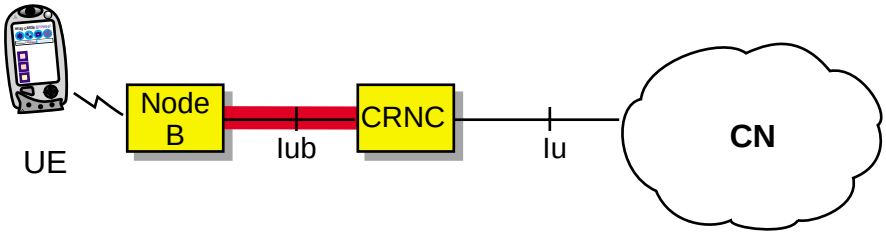
NBAP Support for Logical O&M

© wray castle limited

3.3 Functions of NBAP

NBAP functions are shown in Figure 6.

© wray castle limited



Common NBAP and logical O&M functions

- Common transport channel set-up, reconfiguration and deletion
- Control of Node B resources
- Common measurement handling
- Radio link set-up for new Node B communication contexts

Dedicated NBAP functions

- Radio link reconfiguration, failure and restoration
- Downlink power control
- Dedicated measurement handling (radio link)
- Control of compressed mode operation

Figure 6

Functions of NBAP

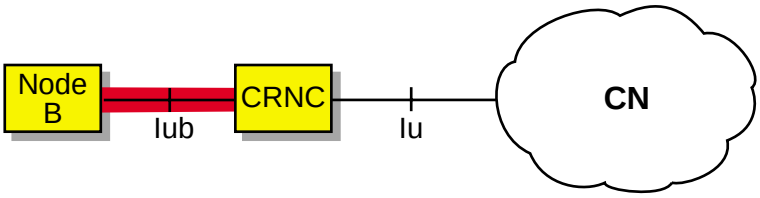
© wray castle limited

3.4 NBAP Data Transfer

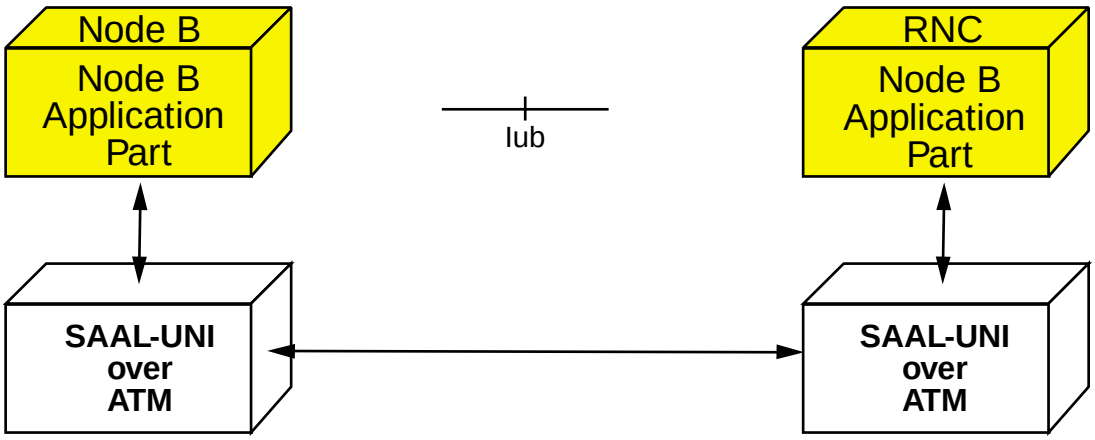
The NBAP transport service is a point-to-point signalling bearer. There may be multiple point-to-point links between an RNC and a Node B.

The signalling bearer in the control plane is Signalling ATM Adaptation Layer – User-Network Interface (SAAL-UNI) over ATM.

© wray castle limited



Transport Service for NBAP



- Signalling bearer for NBAP is a point-to-point protocol
- There may be multiple point-to-point links between an RNC and a Node B
- The two types of NBAP procedure (Common and Dedicated) may be carried on separate signalling links

Figure 7

NBAP Data Transfer

© wray castle limited

3.5 Cell Set-up

This procedure is used to set up a cell in a Node B. The CRNC takes the cell, identified via the cell-id, into service and uses the resources in the Node B. The cell within the Node B is identified via the local cell-id.

Successful cell set-up results in the configuration of resources such as CPICH(s), Primary SCH, Secondary SCH, Primary CCPCH and BCH.

3.6 Common Transport Channel Set-up

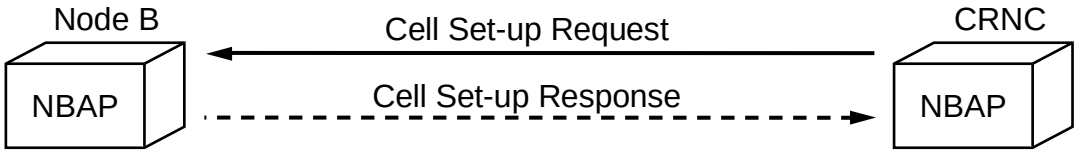
This procedure is used for establishing the necessary resources in the Node B regarding the following common transport channels.

Physical Layer (Uu interface)	Transport Channel
Secondary Common Control Physical Channel (CCPCH)	FACH or PCH
Present only at physical layer: Paging Indicator Channel (indicates to UE to look at the paging channel	–
Acquisition Indicator Channel (acknowledgement of random access probes)	–
PRACH	RACH
PCPCH	CPCH
PDSCH	DSCH

Note: there will be more than one of this type of message initiated at the CRNC to the Node B as one message can only configure a few of the above transport channels.

© wray castle limited

Example 1



Example 2

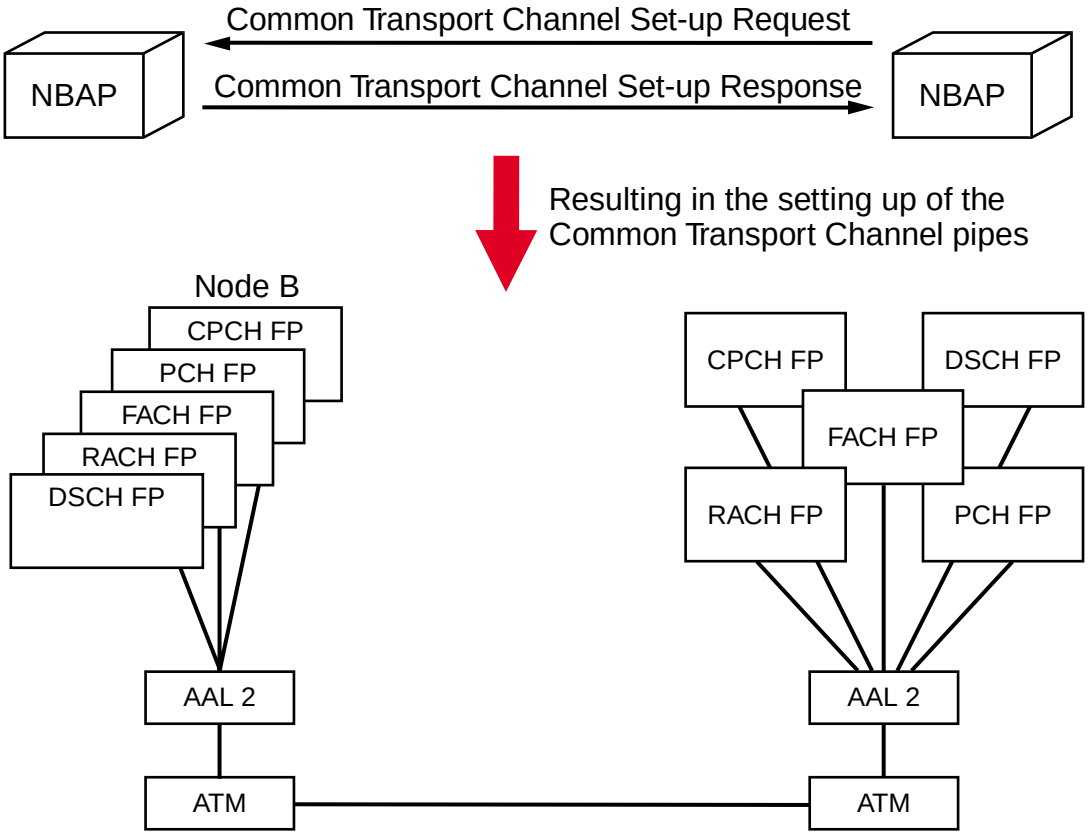


Figure 8
Examples of NBAP Procedures

© wray castle limited

As a result of common transport channel set-up between the CRNC and the Node B, the pipes for communication, notification and general information across the Iub and Uu interfaces are in place. This will ultimately allow UEs to access the system via this point and communicate with the RNC.

The purpose of the framing protocols, which extend the transport channels from the Uu interface across the Iub interface, will be explained later.

© wray castle limited

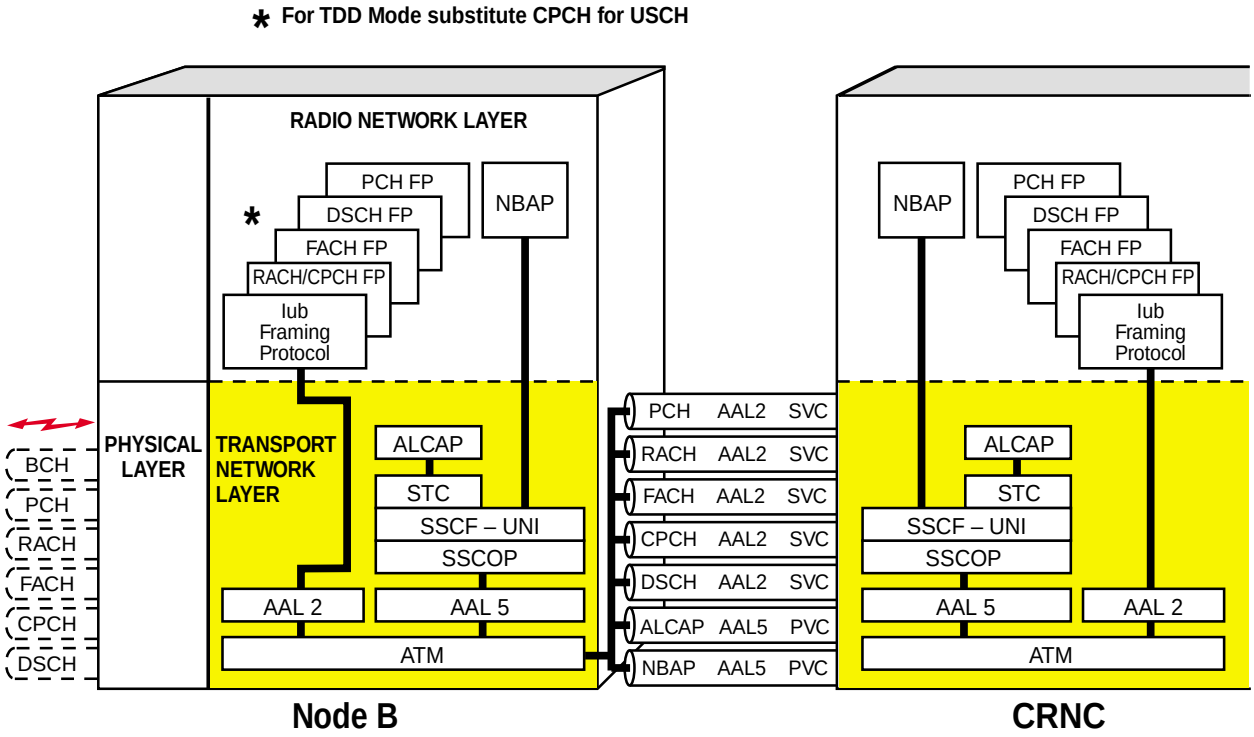


Figure 9

Common Transport Channel Set-up

© wray castle limited

© wray castle limited

LESSON 2

Iur PROTOCOLS

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Iur Interface Protocol Structure 6.2.1

2 Radio Network Subsystem Application Part (RNSAP) 6.2.3
2.1 Services Provided by RNSAP 6.2.3
2.2 Functions of RNSAP 6.2.5
2.3 RNSAP Connectionless SCCP Data Transfer Service 6.2.7
2.4 RNSAP Connection-Oriented SCCP Data Transfer Service 6.2.9

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of the protocols found in the user plane and control plane on the Iur interface

© wray castle limited

1 Iur INTERFACE PROTOCOL STRUCTURE

The structure of this interface, shown in Figure 1, is similar to that of the Iub interface, in that transport channels are framed and passed over the interface as part of the User Plane, and indeed the DCH Framing Protocol is identical to the DCH Framing Protocol on the Iub interface.

RNSAP provides the control within the Radio Network Layer for transferring the transport channels, in addition to providing other control functionality for the interface.

In the Transport Network Layer, switched virtual circuits are specified for the data bearers, while the signalling bearers for ALCAP and RNSAP are preconfigured (for each Iur interface). However, SS7 entities are introduced into the signalling bearer protocol stack. This allows different signalling bearers to different RNCs to be accessed when required (using MTP), and also, in the case of RNSAP, for different RNSAP procedures to be multiplexed onto a single signalling bearer (using SCCP).

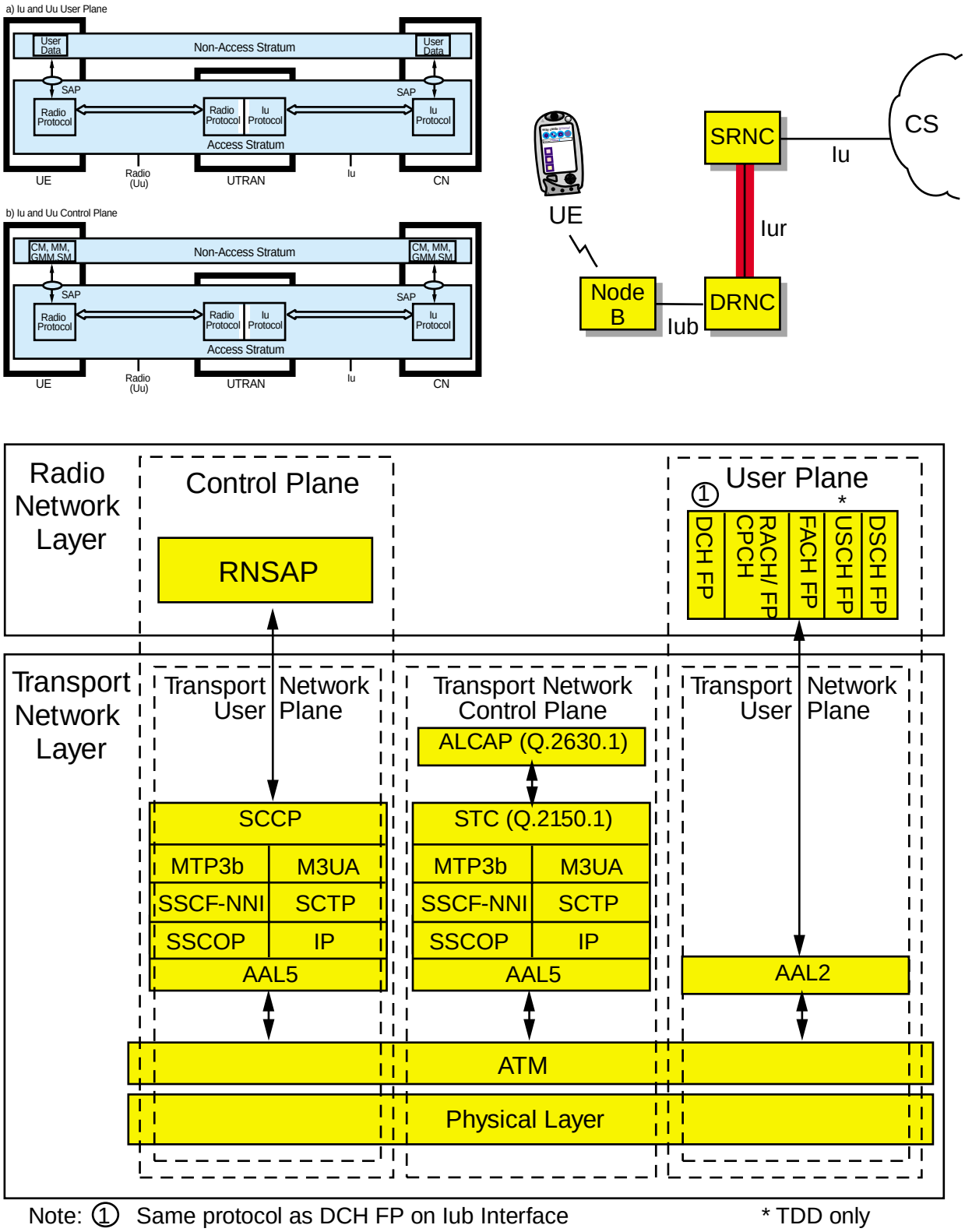
Figure 1 shows the Iur interface structure. This interface has two options for the Transport Layer.

Option 1
The MTP3b protocol is used for the control of signalling links. This protocol (Recommendation Q.2210) uses the services of SSCF and SSCOP.

Option 2
The MTP3 User Adaptation Layer (M3UA) protocol is used for supporting the transport of any SS7 MTP3-User signalling (e.g. SCCP messages) over IP using the services of the Stream Control Transmission Protocol (SCTP).

The Iu-PS interface uses the same options.

© wray castle limited



Note: ① Same protocol as DCH FP on Iub Interface * TDD only

Figure 1

Iur Interface Protocol Structure

© wray castle limited

2 RADIO NETWORK SUBSYSTEM APPLICATION PART (RNSAP)

2.1 Services Provided by RNSAP

The RNSAP procedures on the Iur interface are divided into four modules.

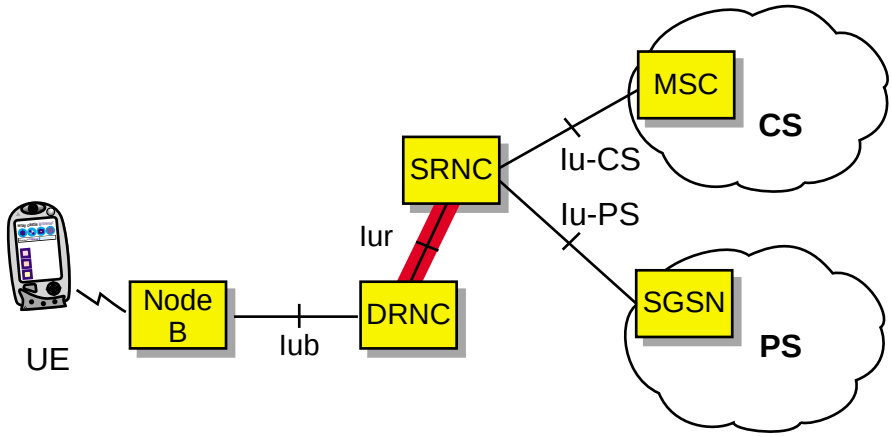
1 RNSAP Basic Mobility procedures are used to handle mobility within the UTRAN. (Inter-RNC Mobility)

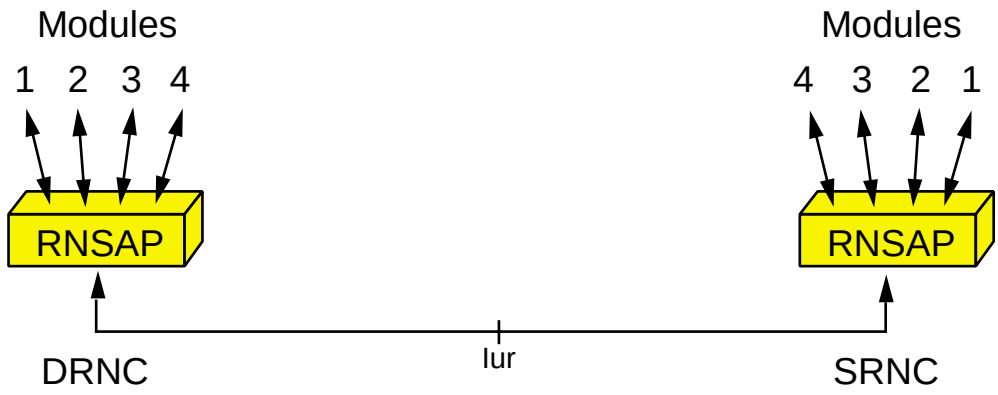
2 RNSAP DCH procedures are used to handle the dedicated channels (DCHs) between two RNSs. (Dedicated Channel Traffic)

3 RNSAP Common Transport Channel procedures are used to control common transport channel data streams. (Common Channel Traffic)

4 RNSAP Global procedures are used for functions not related to a specific UE. (Global Resource Management)

© wray castle limited





RNSAP Modules:

1 → Basic Mobility Procedures

2 → DCH Procedures

3 → Common Transport Channel Procedures

4 → Global Procedures

Figure 2

Services Provided by RNSAP

© wray castle limited

2.2 Functions of RNSAP

The functions of RNSAP include:

Radio Link Management
This enables the SRNC to manage radio links using dedicated resources in a DRNS.

Physical Channel Reconfiguration
This enables the DRNC to reallocate the physical channel resources for a Radio Link.

Radio Link Supervision
This enables the DRNC to report failures and restorations of a Radio Link.

Compressed Mode Control (FDD)
This enables the SRNC to control the usage of compressed mode within a DRNS.

Measurements on Dedicated Resources
This enables the SRNC to initiate measurements on dedicated resources in the DRNS. The function also allows the DRNC to report the result of the measurements.

Downlink (DL) Power Drifting Correction (FDD)
This enables the SRNC to adjust the DL power level of one or more radio links in order to avoid DL power drifting between the Radio Links

Common Control Channel (CCCH) Signalling Transfer
This enables the SRNC and DRNC to pass information between the UE and the SRNC on a CCCH controlled by the DRNS.

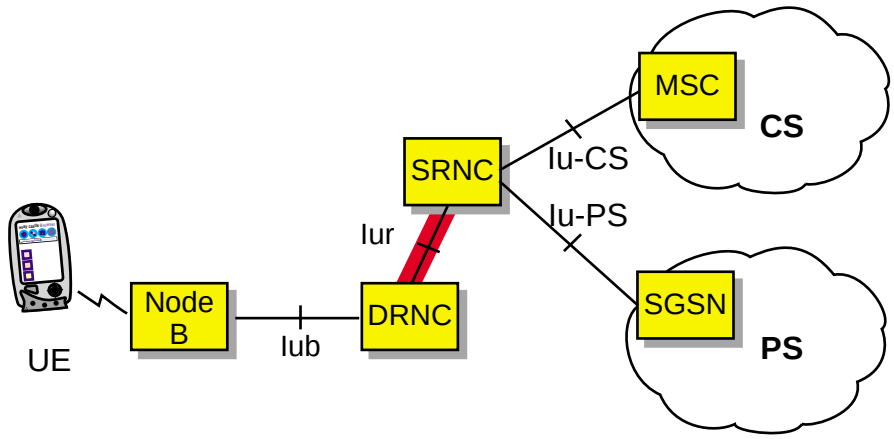
Paging
This enables the SRNC to page a UE in a UTRAN Registration Area (URA) or a cell in the DRNS.

Common Transport Channel (CTCH) Resources Management
This enables the SRNC to utilize Common Transport Channel Resources within the DRNS.

Relocation Execution
This enables the SRNC to finalize a relocation previously prepared via other interfaces.

Reporting of General Error Situations
This enables reporting of general error situations, for which function specific error messages have not been defined.

© wray castle limited



Basic Mobility Procedures:

- Uplink signalling transfer
- Downlink signalling transfer
- Relocation commit
- Paging

Common Transport Channel Procedure:

- Initialization and release of common transport channels

DCH Procedures:

- Radio link handling
- Physical channel reconfiguration
- Measurement reporting
- Downlink power control
- Control of compressed mode

Global Procedures:

- Error handling

Figure 3

Functions of RNSAP

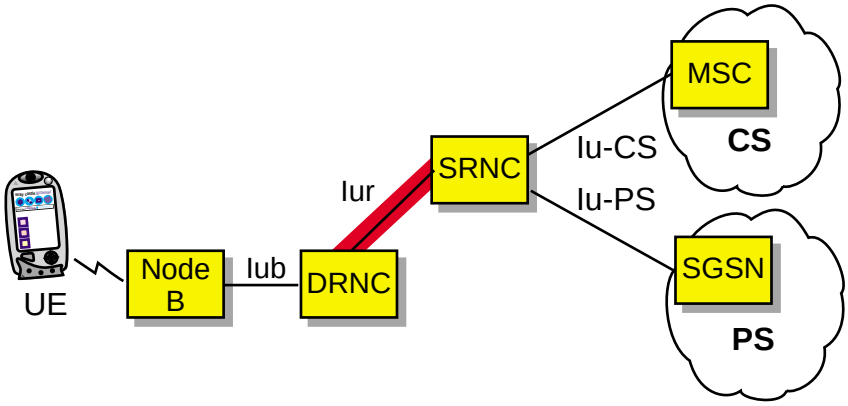
© wray castle limited

2.3 RNSAP Connectionless SCCP Data Transfer Service

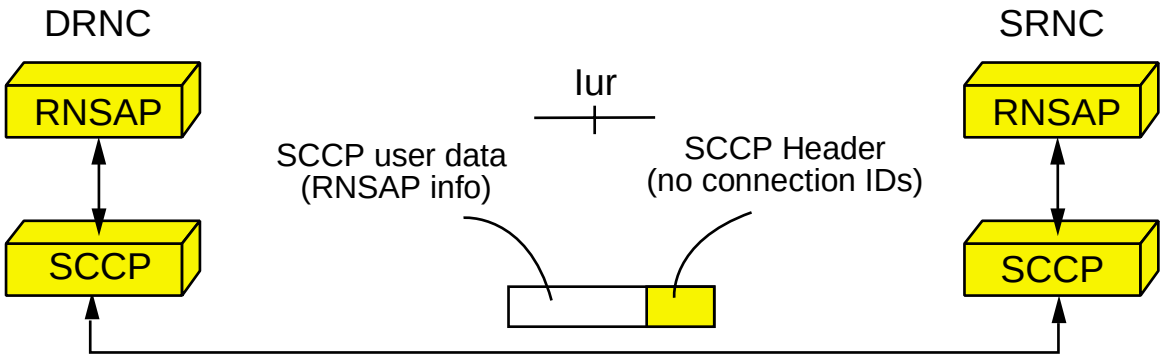
The signalling transport will provide a connection-oriented and connectionless data transfer service mode for the RNSAP.

The connectionless data transfer service is between two RNCs. There is no establishment of a signalling connection. RNSAP will be notified in case an RNSAP message did not reach the intended peer RNSAP entity.

© wray castle limited



Signalling Transport Service for RNSAP – Connectionless Mode



- No signalling connection established
- Message returned on non-delivery to RNSAP
- Consult TS 25.423 to identify which RNSAP procedures use connectionless mode

Figure 4

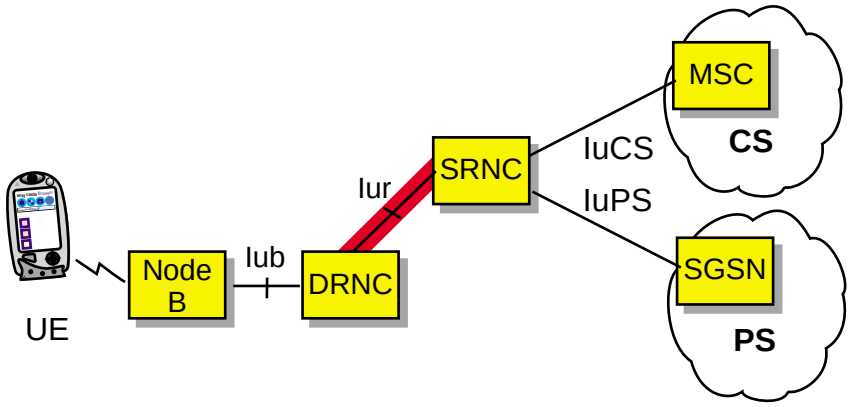
RNSAP Connectionless SCCP Data Transfer Service

© wray castle limited

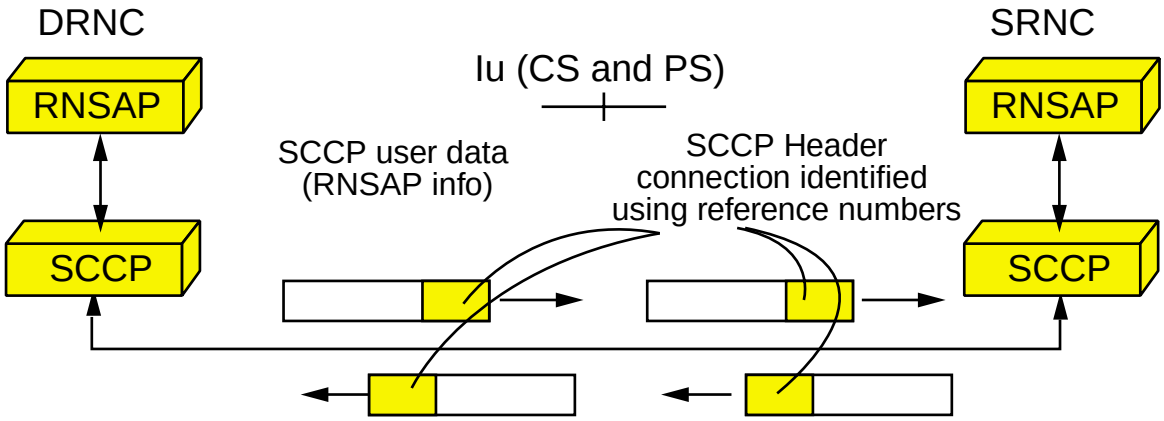
2.4 RNSAP Connection-Oriented SCCP Data Transfer Service

The connection-oriented data transfer service is between two RNCs. It dynamically establishes and releases signalling connections. An active UE will have its own signalling connection. The signalling connection will provide in-sequence delivery of RNSAP messages. RNSAP will be notified if the signalling connection breaks.

© wray castle limited



Signalling Transport Service for RNSAP – Connection-Oriented Mode



- Signalling connections dynamically established and released
- Connection identified using reference numbers
- Each active UE has its own signalling connection
- One signalling per DRNC is provided
- Provides in-sequence delivery of RANAP messages
- RNSAP notified if connection broken
- Consult TS 25.423 for which RNSAP procedures use connection-oriented mode

Figure 5

RNSAP Connection-Oriented SCCP Data Transfer Service

© wray castle limited

© wray castle limited

LESSON 3

Iub AND Iur FRAMING PROTOCOLS

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Framing Protocols (FP) 6.3.1
1.1 Introduction 6.3.1
1.2 Frame Types (FT) 6.3.3
1.3 Iub/Iur Frame Structures 6.3.5

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- identify the need and usage of framing protocols on the Iub and Iur interface

© wray castle limited

1 FRAMING PROTOCOLS (FP)

1.1 Introduction

The user plane of the Radio Network Layer on the Iur and Iub consists of data and control Framing Protocols (FPs). Data FPs can be further split into dedicated and common channel streams. Most common data streams are constantly available. Dedicated data streams are dynamically established/released when required.

The FP uses AAL2/ATM to transport frames across the Iub and Iur interface, so that the information does not incur unnecessary delays across the Iub and Iur interfaces.

© wray castle limited

Frame Types

- **Data Frames** → **Common Channels**, **Dedicated Channels**
- **Control Frames**

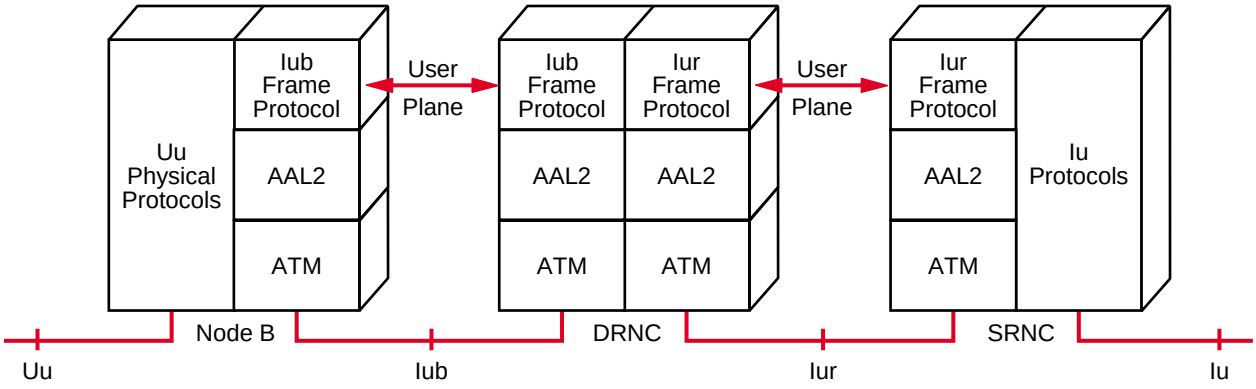


Figure 1
Iub/Iur FPs

© wray castle limited

1.2 Frame Types (FT)

The Iub and Iur interfaces use the same DCH transport frames. However, common transport frames are different. The Iub/Iur interfaces are split into data frames and control frames.

Figure 2 details the different FTs used on dedicated and common transport channels.

© wray castle limited

Iub/Iur DCH Transport Channels – User Plane	
Data Frame Types	**Control Frame Types**
Uplink (UL) Data Frame Downlink (DL) Data Frame	Outer Loop Power Control Timing Adjustment DL Synchronization UL Synchronization DL Signalling for DSCH DL Node Synchronization UL Node Synchronization RX Timing Deviation Radio Interface Parameter Update Timing Advance

Iub Common Transport Channels – User Plane	
Data Frame Types	**Control Frame Types**
RACH CPCH FACH PCH DSCH USCH	Timing Adjustment DL Synchronization UL Synchronization DL Node Synchronization UL Node Synchronization Dynamic PUSCH Assignment Timing Advance

Iur Common Transport Channels – User Plane	
Data Frame Types	**Control Frame Types**
RACH/CPCH FACH DSCH USCH	FACH Flow Control DSCH Capacity Request DSCH Capacity Allocation

Figure 2

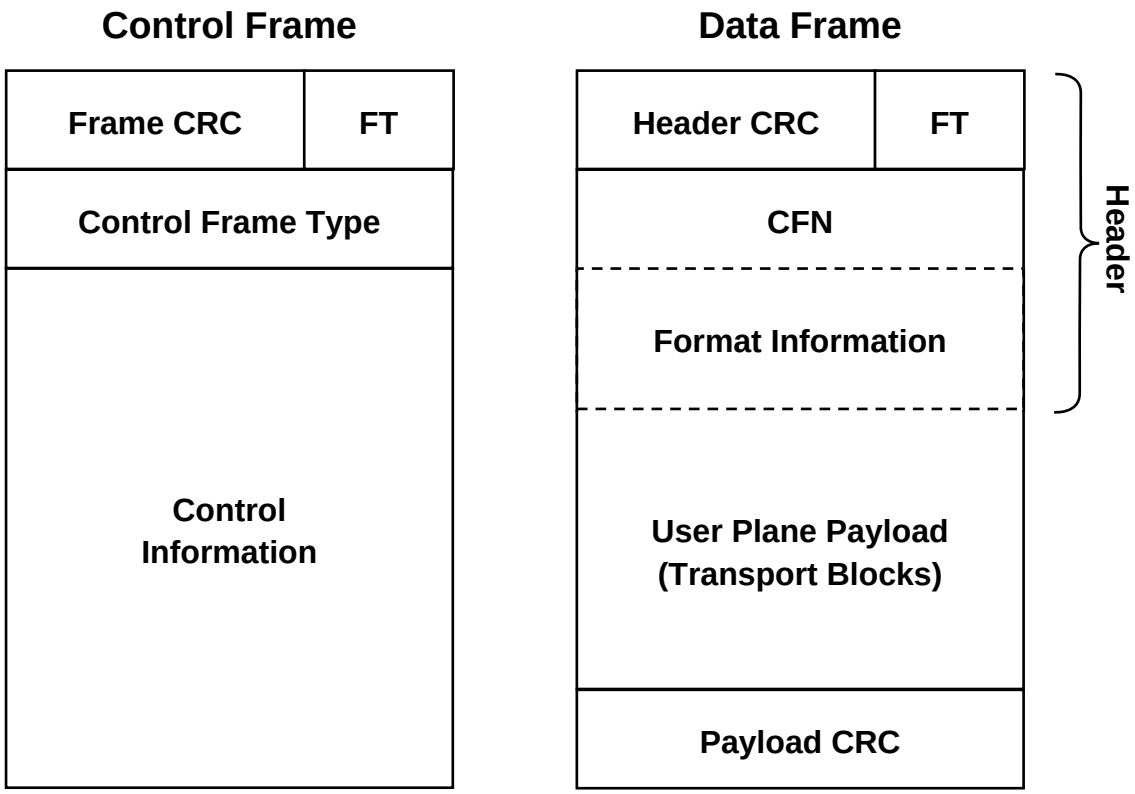
Frame Types

© wray castle limited

1.3 Iub/Iur Frame Structures

The Iub and Iur interfaces have two basic frame structures, data or control, indicated by the FT bit. The control frame structure is the same for the Iub and Iur interfaces. The format of data frames varies, depending on the transport channel and interface (Iur/Iub) used.

© wray castle limited



FT – Frame Type (0=data, 1=control)
CFN – Connection Frame Number

Figure 3
Iub/Iur Frame Structures

© wray castle limited

© wray castle limited

LESSON 4

Iu PROTOCOLS
(CIRCUIT-SWITCHED DOMAIN)

© wray castle limited

© wray castle limited

LESSON CONTENTS

1	**Iu Interface Protocol Structure Towards the CS Domain**		**6.4.1**
	1.1	Iur and Iu-CS Transport Protocol Structure	6.4.3
	1.2	Iu-PS Interface Protocol Structure	6.4.5
2	**Radio Access Network Application Part (RANAP)**		**6.4.7**
	2.1	Services Provided by RANAP	6.4.7
	2.2	Functions of RANAP	6.4.9
	2.3	RANAP Connectionless SCCP Data Transfer Service	6.4.11
	2.4	RANAP Connection-Oriented SCCP Data Transfer Service	6.4.13
3	**The Iu UP Protocol**		**6.4.15**
	3.1	Iu UP Protocol Modes of Operation	6.4.15
	3.2	Transparent Mode (TrM)	6.4.15
	3.3	Support Mode for predefined SDU size (SMpSDU)	6.4.17
	3.4	Iu Protocol Procedures	6.4.23
	3.5	SMpSDU Data Frames	6.4.31
	3.6	Summary of the Iu Interface	6.4.33

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of the Iu protocols involved in a circuit-switched connection

© wray castle limited

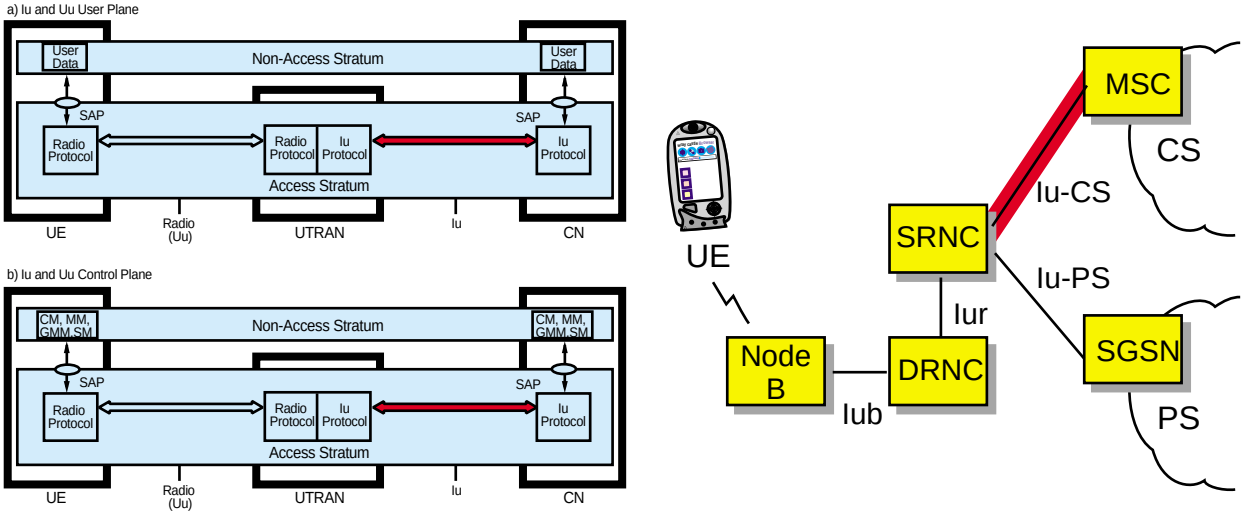
1 Iu INTERFACE PROTOCOL STRUCTURE TOWARDS THE CS DOMAIN

On the Iu interface towards the CS domain, the Radio Network Layer Control Plane application protocol is RANAP, carrying control data, including higher-layer messages (CM and MM) between the CN and the UTRAN. The User Plane within the Radio Network Layer consists solely of user data (no higher-layer AS or NAS control protocols are transferred over the interface outside of the RANAP protocol). Of course, application data such as WAP may be carried transparently as user data.

The standard Transport Network Layer, shown in Figure 1, is ATM-based, hence the Transport Network Control Plane ALCAP comprises the signalling protocols required to set up, maintain and release the data bearer (in the form of a switched virtual circuit). The signalling connection (signalling bearer), used to transfer the ALCAP information itself, is predefined, as is the signalling bearer used to carry RANAP signalling (although SCCP is used to establish different logical signalling connections at that level).

The Transport Network Layer protocols are not described any further in this section.

© wray castle limited



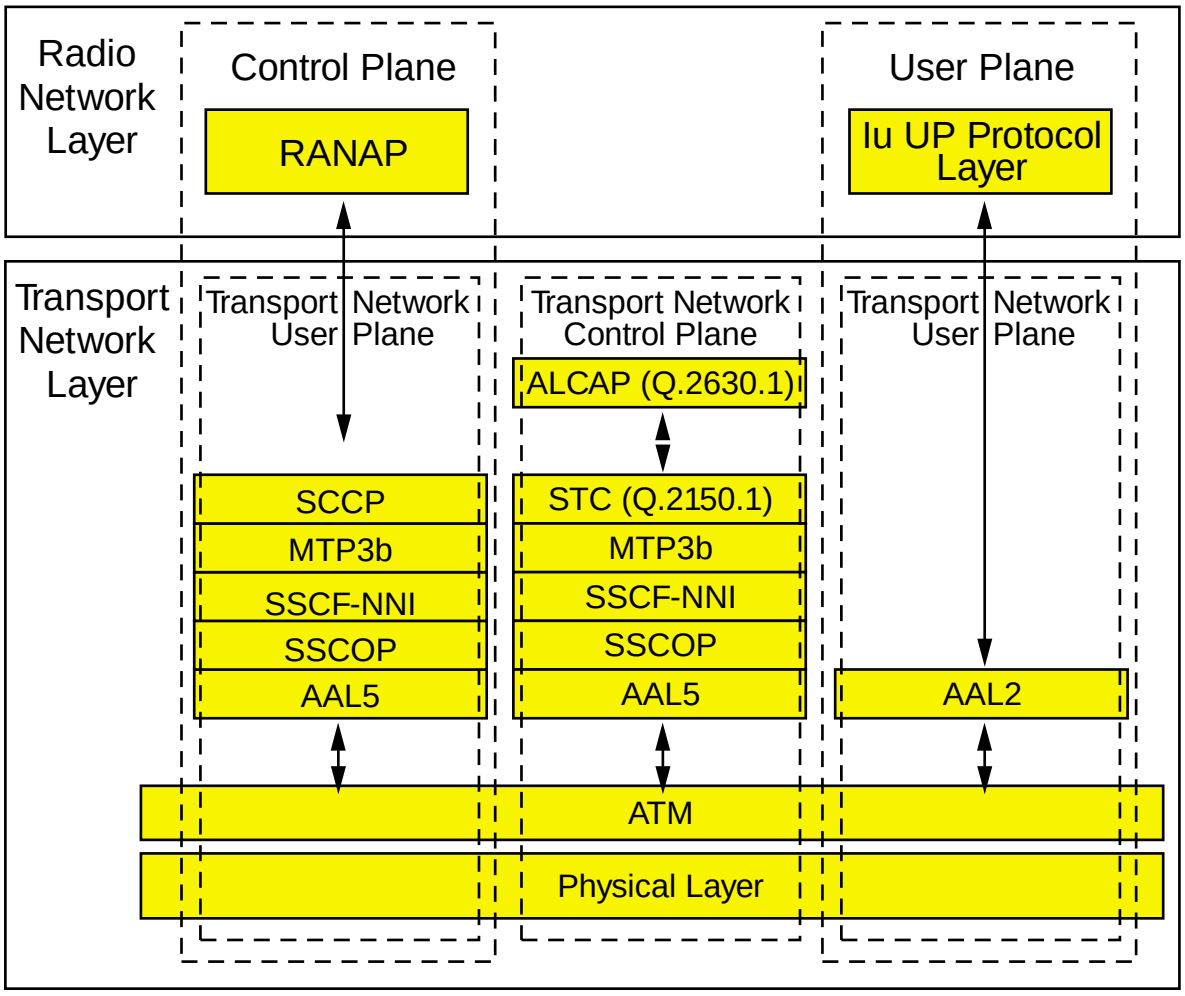


Figure 1

Iu Interface Protocol Structure Towards the CS Domain

© wray castle limited

1.1 Iur and Iu-CS Transport Protocol Structure

The interfaces Iur and Iu-CS may use the transport protocol structure shown in Figure 2. The AAL Type 2 signalling function resides on top of the STC. This STC is defined for use on Message Transfer Part level 3 broadband (MTP3b).

STC provides:

- independence from the underlying transmission media
- transparency of the information transferred
- service availability reporting to the STC user
- congestion reporting to the STC user

MTP3b specifies the peer-to-peer protocol for the transfer of information and control between any pair of MTP entities.

© wray castle limited

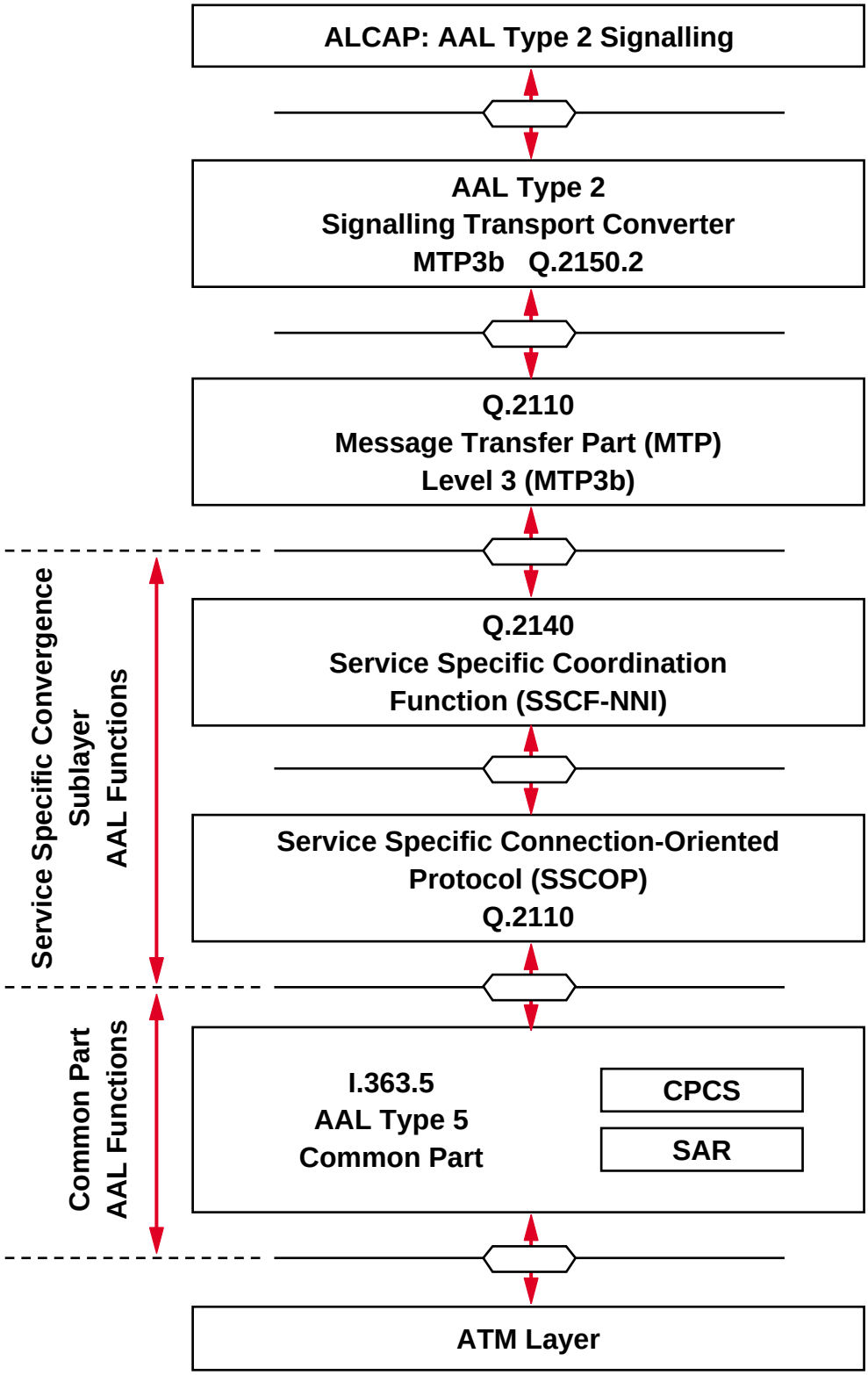


Figure 2

Iur and Iu-CS Transport Protocol Structure

© wray castle limited

1.2 Iu-PS Interface Protocol Structure

The Iu-PS interface has no requirement for a Transport Network Control Plane, since the Radio Network User Plane uses AAL5. The interface structure for the RNC Plane is the same as for the Iur interface, with two options available.

The Radio Network User Plane information is transferred using the GPRS Tunnelling Protocol (GTP). GTP uses the services of UDP and IP to address the peer entity. These IP datagrams are then transported in AAL5/ATM connections.

© wray castle limited

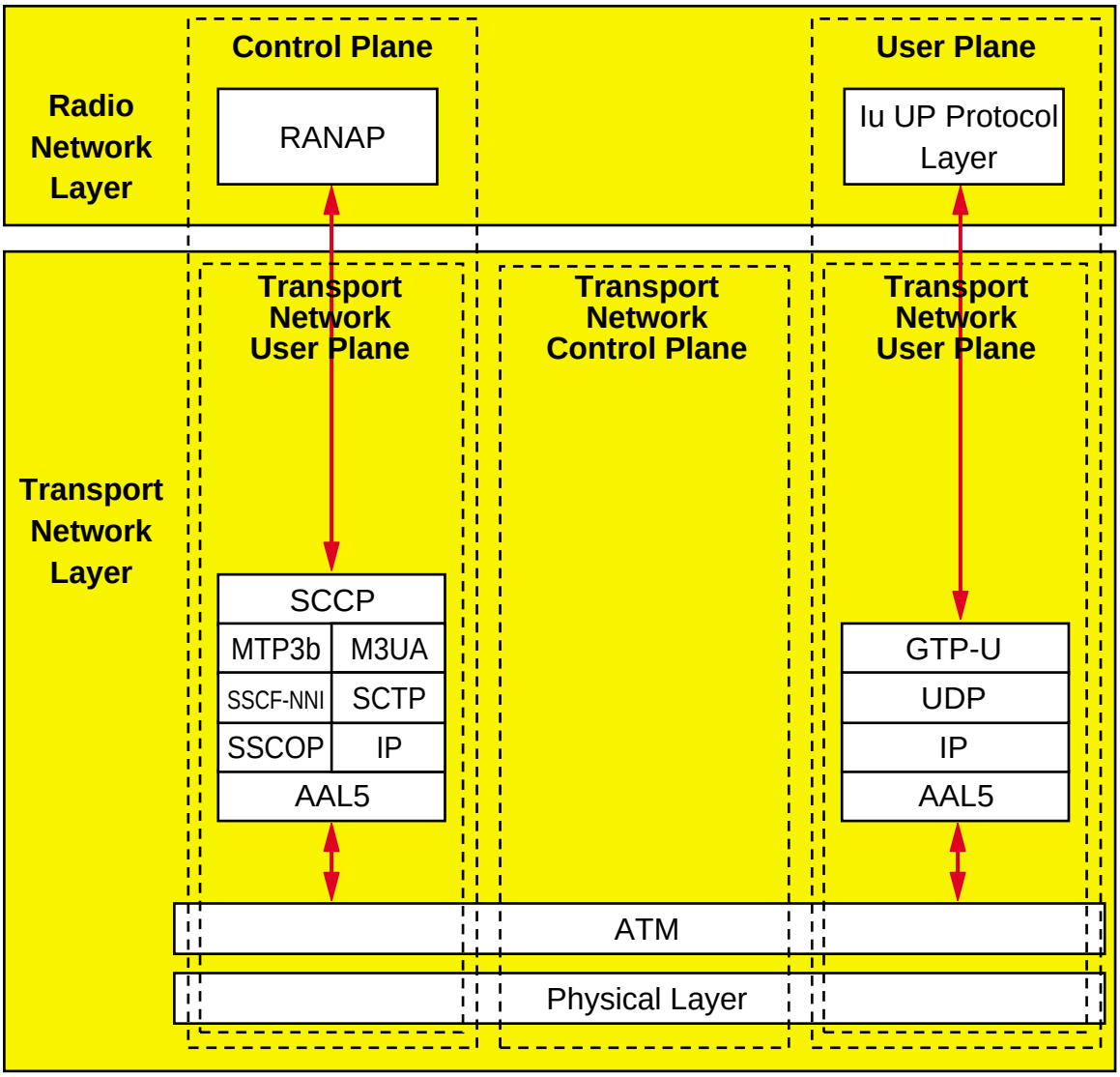


Figure 3

Iu-PS Interface Protocol Structure

© wray castle limited

2 RADIO ACCESS NETWORK APPLICATION PART (RANAP)

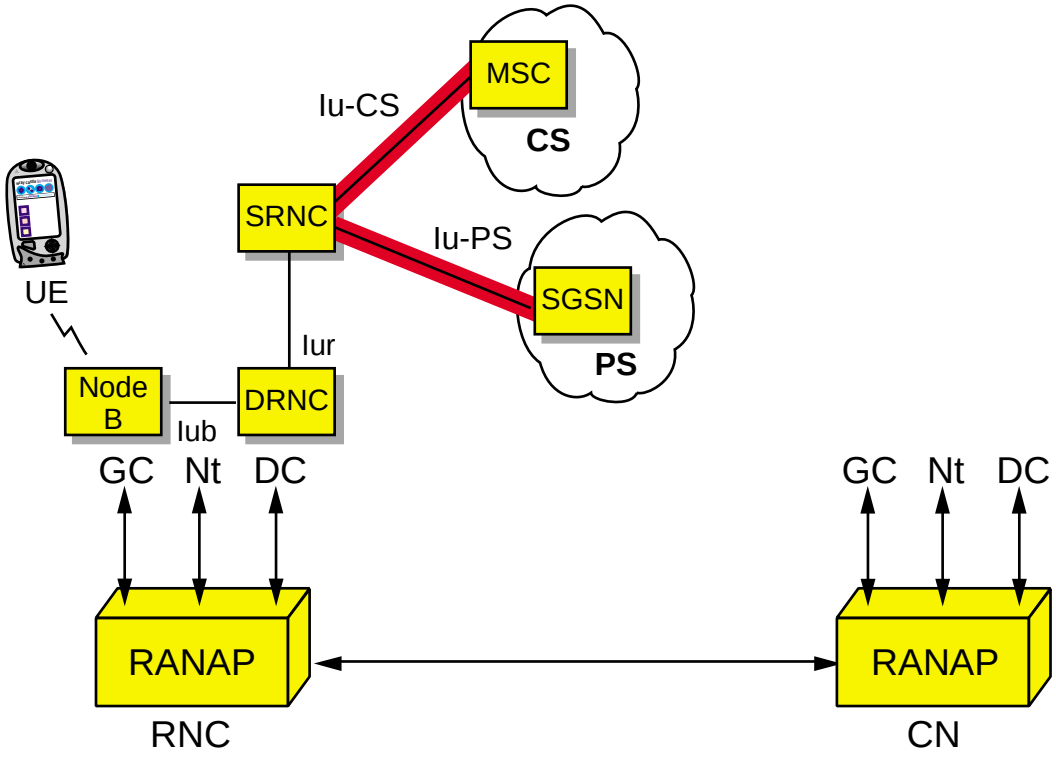
2.1 Services Provided by RANAP

Through the relevant SAPs, RANAP provides services to the NAS at the CN, as shown in Figure 4. These services are divided into three categories:

- General Control (GC) services
- Notification (Nt) services
- Dedicated Control (DC) services

Information related to these services is mapped to/from the RRC at the SRNC, and the RRC itself provides the corresponding services to the NAS through the appropriate SAPs at the UE.

© wray castle limited



RANAP provides:

- General Control (GC) services
- Notification (Nt) services
- Dedicated Control (DC) services

Note: This service architecture is the same as that provided to the NAS by RRC at the mobile. RRC and RANAP together provide the overall access service to NAS protocols CM (CC, SS, GSMS, SM) and MM (MM, GMM)

Figure 4
Services Provided by RANAP

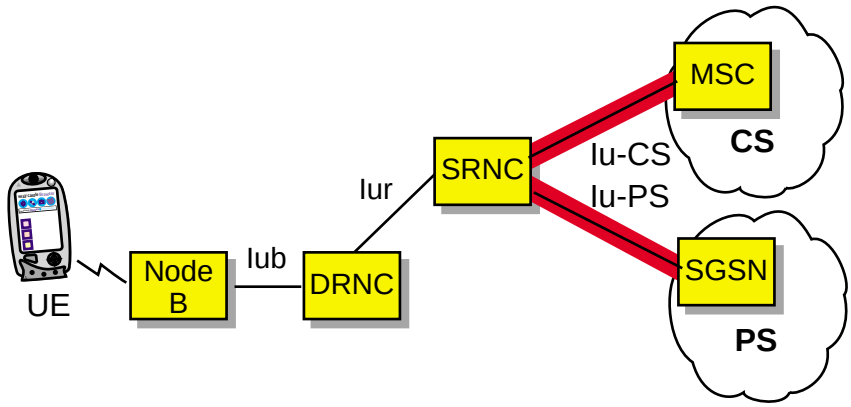
© wray castle limited

2.2 Functions of RANAP

The functions of RANAP are summarized in Figure 5. They include procedures for the management of resources, access to the network, mobility, provision of services, security, interface management and error handling.

RANAP is used on the Iu interface towards both the circuit-switched domain (Iu-CS) and the packet-switched domain (Iu-PS). Hence some procedures, and therefore messages, are only relevant on one or other of these interfaces.

© wray castle limited



Functions of RANAP:

- RAB management
- Transport of NAS information
- Relocating SRNC
- Security
- Location reporting
- Data volume reports
- General error reporting
- Tracing UE activity
- Paging
- Iu interface management
- SRNS context handling (forwarding)

Figure 5
Functions of RANAP

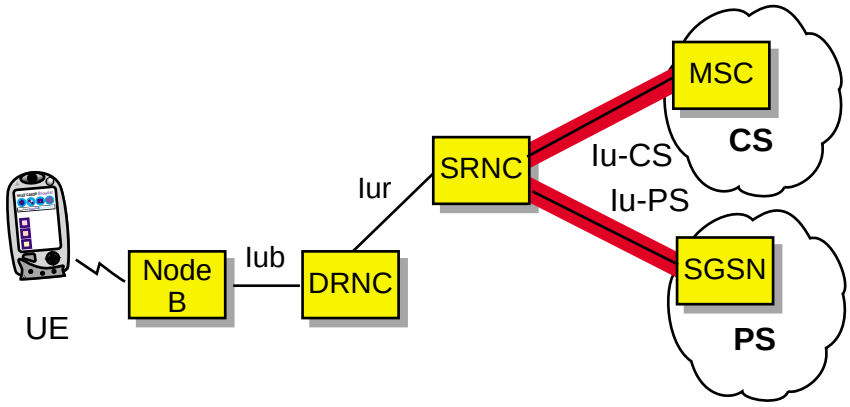
© wray castle limited

2.3 RANAP Connectionless SCCP Data Transfer Service

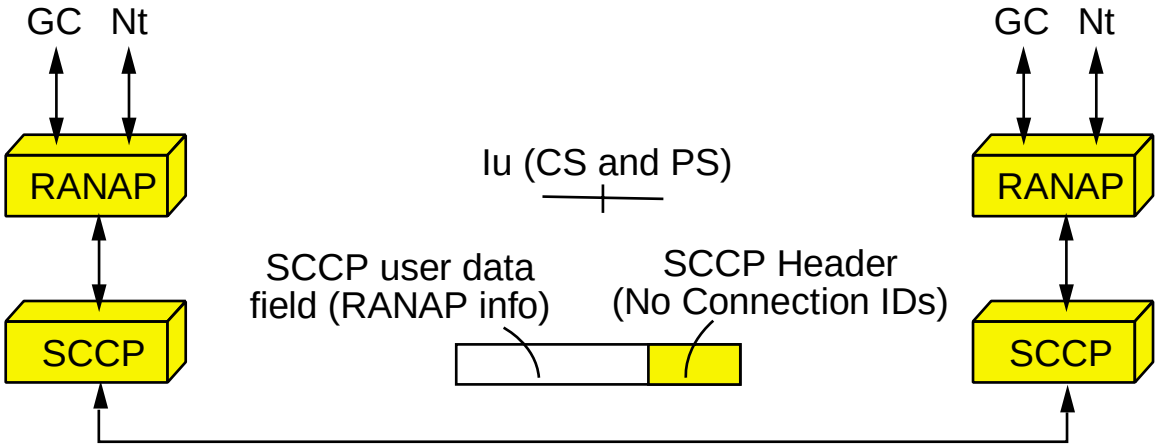
For both General Control services and Notification services procedures, the Transport Network Layer (signalling bearer) provides a connectionless service. This is because procedures relating to these services generally involve short exchanges of information (or single messages) and do not warrant the extra processing and signalling required to set up a logical signalling connection.

It is the SCCP of SS7 that provides this connectionless service when requested by RANAP, as shown in Figure 6.

© wray castle limited



Signalling Transport Service for RANAP – Connectionless Mode



- No signalling connection established
- Message returned on non-delivery to RANAP
- Used for General Control Services
- Used for Notification Services

Figure 6
RANAP Connectionless SCCP Data Transfer Service

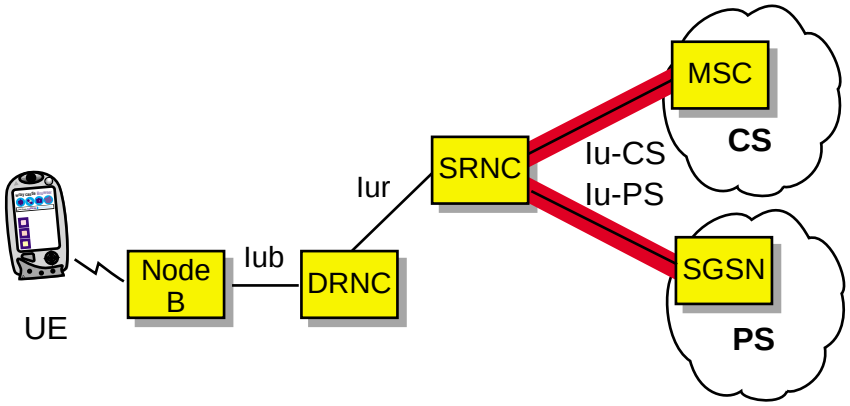
© wray castle limited

2.4 RANAP Connection-Oriented SCCP Data Transfer Service

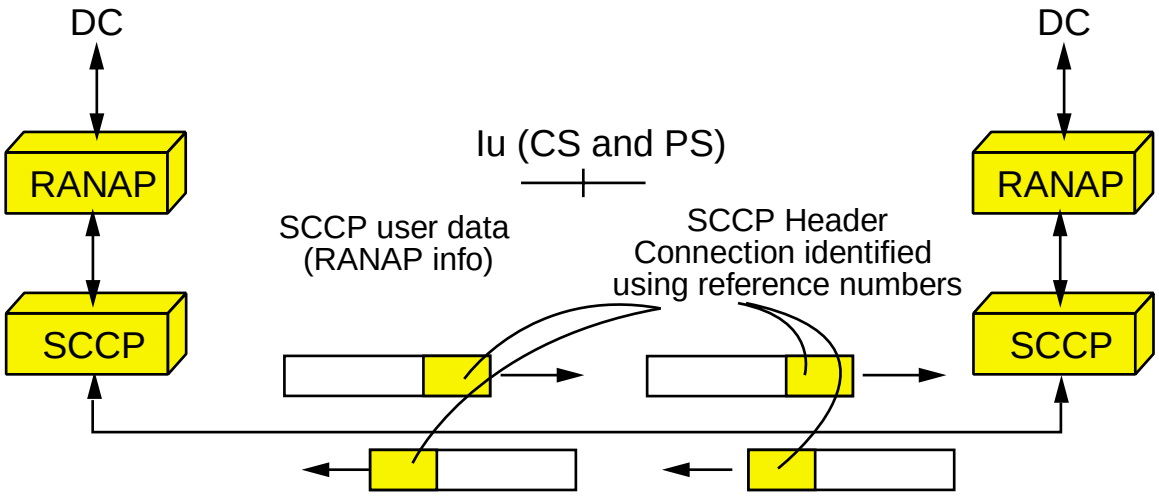
For Dedicated Control Services, SCCP of SS7 provides a connection-oriented service when requested by RANAP, as shown in Figure 7.

This takes the form of a logical signalling connection, which is established by SCCP by way of exchanging connection identifiers.

© wray castle limited



Signalling Transport Service for RANAP – Connection-Oriented Mode



- Signalling connections dynamically established and released
- Connection identified using reference numbers
- Each active UE has its own signalling connection
- Provides in-sequence delivery of RANAP messages
- RANAP notified if connection broken
- Used for Dedicated Control services

Figure 7

RANAP Connection-Oriented SCCP Data Transfer Service

© wray castle limited

3 THE Iu UP PROTOCOL

3.1 Iu UP Protocol Modes of Operation

The Iu UP protocol operates in one of two modes, Transparent Mode (TrM) or Support Mode for predefined SDU size (SMpSDU).

Determination of the Iu UP protocol instance mode of operation is a CN decision taken at RAB establishment based on the RAB characteristics. It is signalled in the Radio Network Layer Control Plane at RAB assignment and relocation for each RAB. It is internally indicated to the Iu UP protocol layer at User Plane establishment.

The choice of a mode is bound to the nature of the associated RAB and cannot be changed unless the RAB is changed.

Version 1 of the Iu protocol is currently supported.

3.2 Transparent Mode (TrM)

TrM is intended for those RABs that do not require any particular feature from the Iu UP protocol other than transfer of user data.

In this mode, no Iu frame structure exists.

© wray castle limited

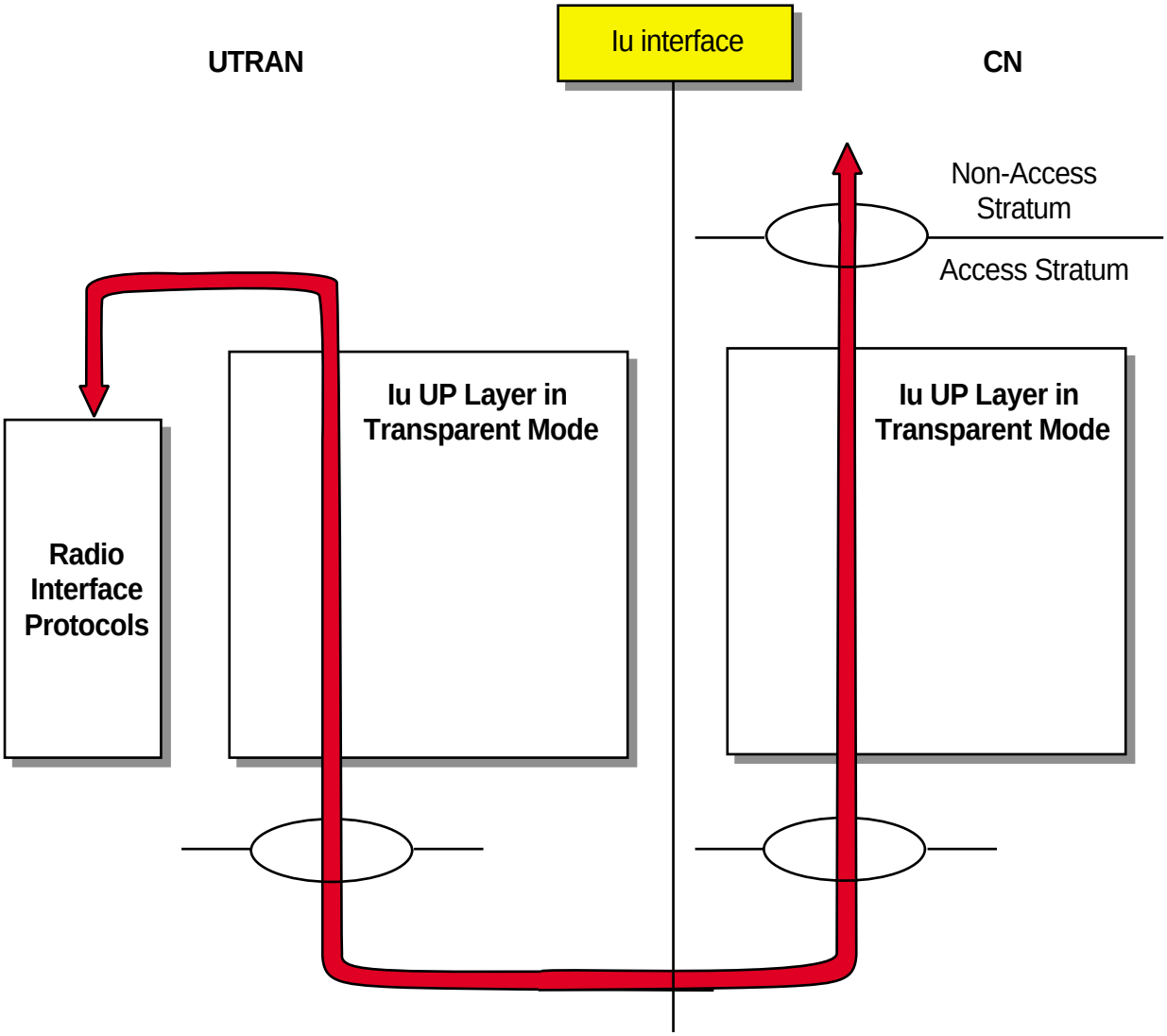


Figure 8
Transparent Mode (TrM)

© wray castle limited

3.3 Support Mode for predefined SDU size (SMpSDU)

The support modes are intended for those RABs that require particular features from the Iu UP protocol in addition to transfer of user data. When operating in a support mode, Iu UP frames are exchanges, whereas in transparent mode, no Iu UP frames are generated.

When requesting Iu UP protocol support, some RABs constrain the Iu UP protocol and possibly the radio interface protocols in specific ways. For instance, certain RABs can have variable predefined rates. e.g. AMR speech. The Iu UP support mode is prepared to support these variations.

© wray castle limited

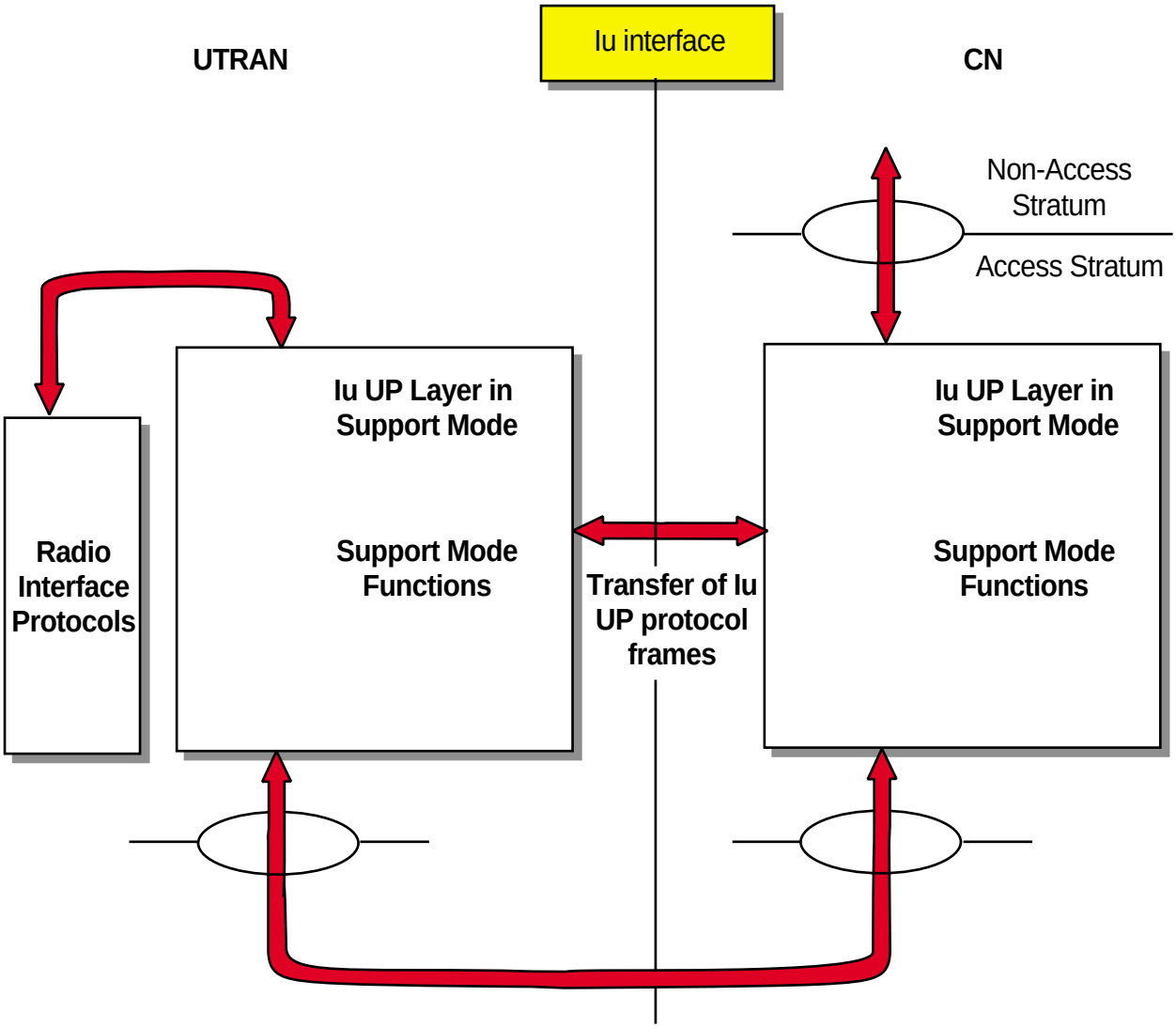


Figure 9
Support Mode for predefined SDU size (SMpSDU)

© wray castle limited

3.3.1 Functions of SMpSDU

The Iu UP protocol layer in Support mode is made up of three sets of functions.

Frame Handler
The Frame Handler function is responsible for framing and de-framing the different parts of an Iu UP protocol frame.

Procedure Control
The Procedure Control functions offer the control of a number of procedures handled at the Iu UP protocol level. The procedures defined are:

- Initialization
- Rate Control
- Time Alignment
- Handling of Error Event

Non Access Stratum (NAS) Data Streams
The Non Access Stratum (NAS) Data Streams' specific functions consist of functions related to consistency checking of the frame number, the CRC checking, and Frame Quality Classification handling.

© wray castle limited

Frame Handler function

- Transport of user data

Procedure Control functions

- Initialization
- Rate Control
- Time Alignment
- Handling of Error Event

Non Access Stratum Data Stream specific functions

- Frame Quality Classification

Figure 10
Functions of SMpSDU

© wray castle limited

3.3.2 RAB Sub-flows

A RAB is realized by the UTRAN through one or several sub-flows. Each sub-flow corresponds to the NAS service data streams that have QoS characteristics that differ in a predefined manner within a RAB, e.g. different reliability classes.

The sub-flows of a RAB are established and released together. RAB sub-flows are numbered from 1 to N (N is the number of sub-flows). RAB sub-flow number 1 corresponds to the highest reliability class and the RAB sub-flow number N corresponds to the lowest reliability class.

The RAB sub-Flow Combination (RFC) is the combination of the RAB sub-flows' variable attributes (e.g. SDU size) and is given by the CN to the SRNC. The different RAB sub-Flow Combinations are identified by a RAB sub-Flow Combination Indicator (RFCI).

© wray castle limited

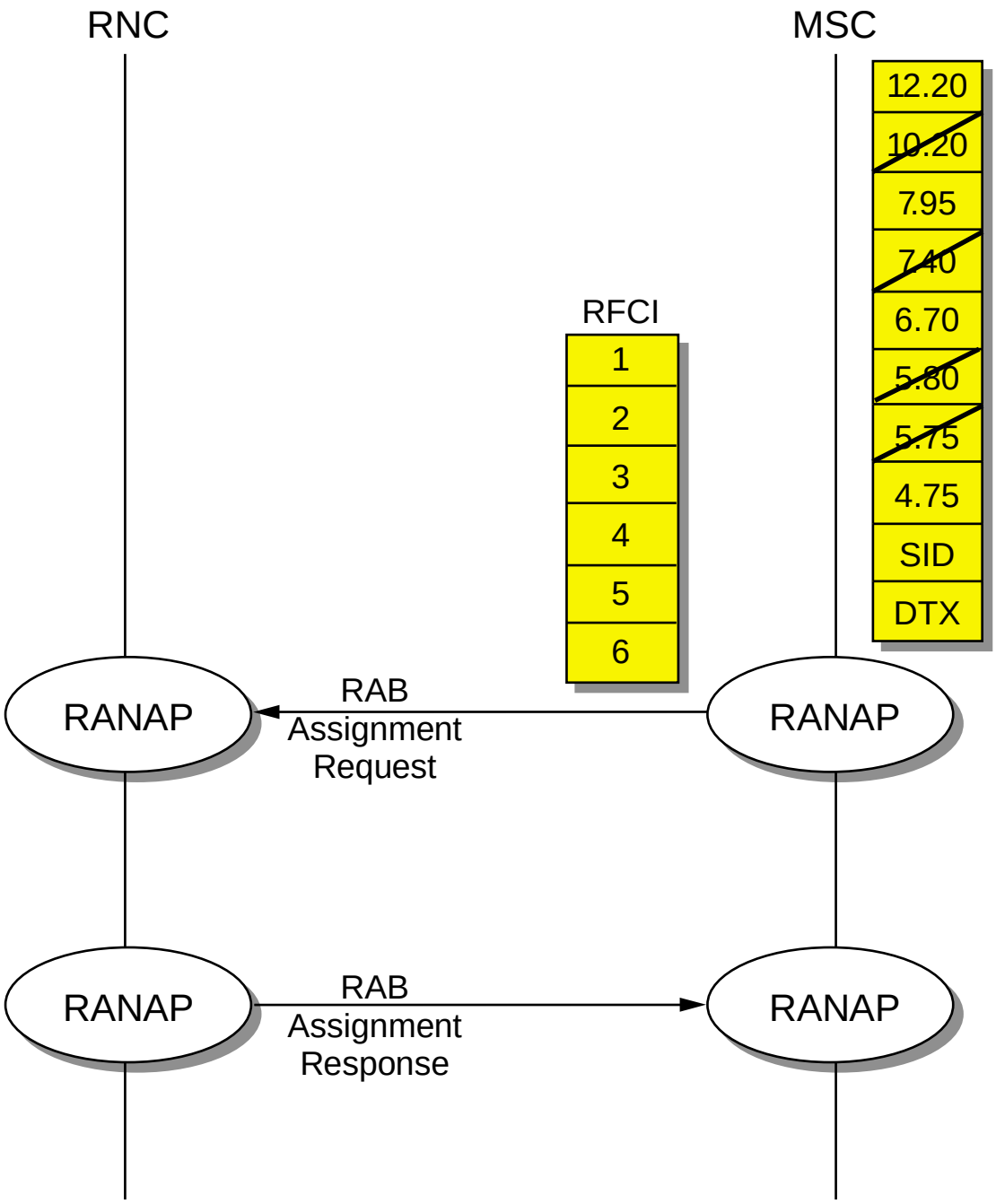


Figure 11
Speech RAB Establishment

© wray castle limited

3.4 Iu Protocol Procedures

Once ALCAP has established the AAL type 2 path, based on the RAB Assignment Request message, the Iu protocol is ready to use the path. There are a number of procedural control functions associated with the use of the path, and these are controlled by the Iu procedural control function. These are as follows.

3.4.1 Initialization of the Iu Path

This is required for RABs that have been specified to use SMdPSU. The purpose of the initialization is to configure both termination end points, namely the SRNC and the CN node with the RFCIs and SDU sizes associated with the RFCIs.

The procedure can be invoked either by the SRNC or the CN node through the Procedural Control Function. The node invoking the initialization formulates Iu type 14 frames in which the RFCIs and the SDU sizes associated with each RFCI are included in the order in which the node wishes to use them. ie RFCI 1 to RFCI n. The initialization message may extend over a number of frame, however each frame in the initialization process must be acknowledged by the peer entity before the next can be transmitted.

The first frame is sent across the interface and a timer is set. (If the frame is not acknowledged the invoking entity will retransmit the frame up to a maximum, typically three times). On receipt of the initializing frame the receiving entity stores the details of the RFCIs and SDU size associated with this RAB. The peers entities can now start to send data.

The message flow and frame are shown in Figure 12.

© wray castle limited

Bits								Number of Octets	
7	6	5	4	3	2	1	0		
PDU Type (=14)				Ack/Nack (=0. i.e. Procedure)		PDU Type 14 Frame Number		1	Frame Control Part
Iu UP Mode version				Procedure Indicator (=0) 0 = initialization procedure				1	
Header CRC						Payload CRC		2	Frame Checksum Part
Payload CRC									
Spare			TI 0=IPTS not present	Number of subflows per RFCI (N)			Chain Ind 0=last 1=more	1	Frame Payload Part
LRI 0	LI	1st RFCI						1	
Length of subflow 1								1 or 2 (dep. LI)	
Length of subflow 2 to N								(N–1)x (1or 2)	
LRI 1	LI	Nth RFCI						1	
Length of subflow 1								1 or 2 (dep. LI)	
Length of subflow 2 to N								(N–1)x (1or 2)	
…									
IPTI of 1st RFCI				IPTI of 2nd RFCI				0 or M/2 (M: Number of RFCIs in frame)	
IPTI of 3rd RFCI				Inter PDU timing interval					
Iu UP Mode Versions supported (bitmap)								2	
Data PDU type type 0 or type 1				Spare				1	
Spare extension								0–32	

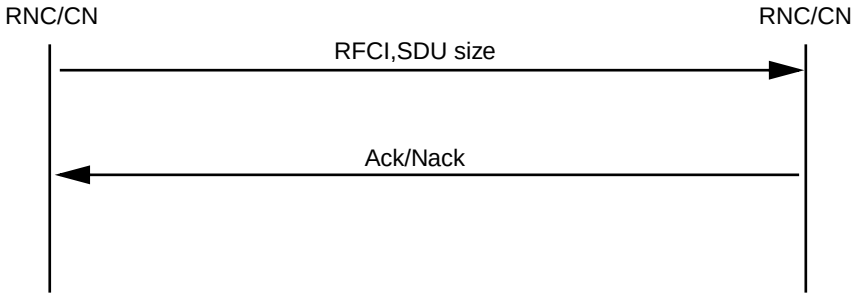


Figure 12
Initialization

© wray castle limited

3.4.2 Rate Control

At times in the flow it may be necessary for the SRNC to reduce the maximum rate permitted downlink from the CN to the SRNC. In order to do this the procedural function within the SRNC formulates a Type 14 rate control frame. In this frame it indicates the permissible RFCIs defined at initialization that are now valid downstream from the CN to the SRNC. This is passed in the same manner to the Initialization message. The message flow and frame are shown in the diagram opposite.

© wray castle limited

Bits								Number of Octets	
7	6	5	4	3	2	1	0		
PDU Type (=14)				Ack/Nack (=0. i.e. Procedure)		PDU Type 14 Frame Number		1	Frame Control Part
Iu UP Mode version				Procedure Indicator (=1) (rate control)				1	
Header CRC						Payload CRC		1	Frame Checksum Part
Payload CRC								1	
Spare		Number of RFCI Indicators (M)						1	Frame Payload Part
RFCI 0 Ind.	RFCI 1 Ind.	…	RFCI M–1 Ind	Padding				0–n	
Spare extension								0–32	

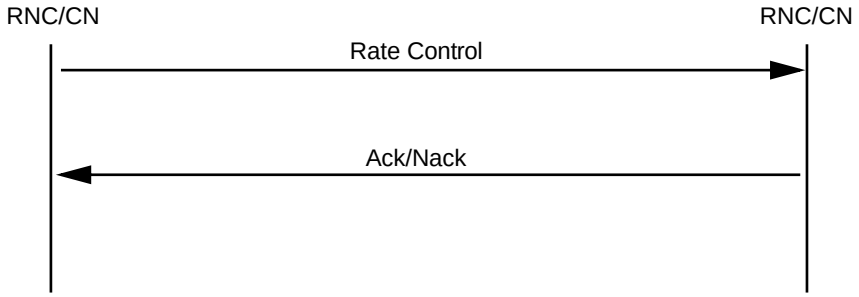


Figure 13
Rate Control

© wray castle limited

3.4.3 Time Alignment

The flow of data from the CN to the SRNC and from the SRNC across the UTRAN requires time alignment in order to reduce the buffering required at the RNC. If the CN is sending Iu data frames at a rate higher than that across the UTRAN the SRNC can use the Type 14 time alignment frame in order to slow down the flow of data frames. The delay/advance in the flow can be changed in 500 µs steps. The message is sent using the procedure described above. The message flow and frame are shown in the diagram opposite.

© wray castle limited

Bits								Number of Octets	
7	6	5	4	3	2	1	0		
PDU Type (=14)				Ack/Nack (=0)		PDU Type 14 Frame Number		1	Frame Control Part
Iu UP Mode version				Procedure Indicator (=2) (time alignment)				1	
Header CRC						Payload CRC		1	Frame Checksum Part
Payload CRC								1	
Time alignment 0–80 retard by n*500 µs 129–208 advance by n*500 µs								1	Frame Payload Part
Spare extension								0–32	

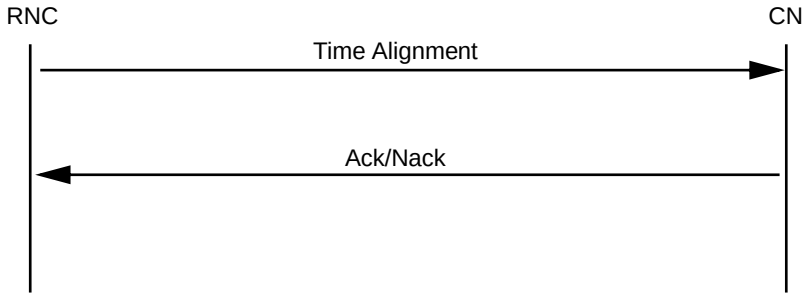


Figure 14
Time Alignment

© wray castle limited

3.4.4 Handling of Error Events

When the receiving peer receives a corrupt or unknown frame, this may be detected by the Iu function or a higher layer. It will report this back to the originating peer by use of the Type 14 Error Event frame. In this frame will be a cause value indicating the reason of the error report and which entity, Iu or a higher function, reported the error.

The message flow and frame are shown in Figure 15.

© wray castle limited

Bits								Number of Octets	
7	6	5	4	3	2	1	0		
PDU Type (=14)				Ack/Nack (=0)		PDU Type 14 Frame Number		1	Frame Control Part
Iu UP Mode version				Procedure Indicator (=3) (error event)				1	
Header CRC						Payload CRC		1	Frame Checksum Part
Payload CRC								1	
Error distance 0 = local error 1 = 1st fwding 2 = 2nd fwding		Error Cause Value						1	Frame Payload Part
Spare extension								0–32	

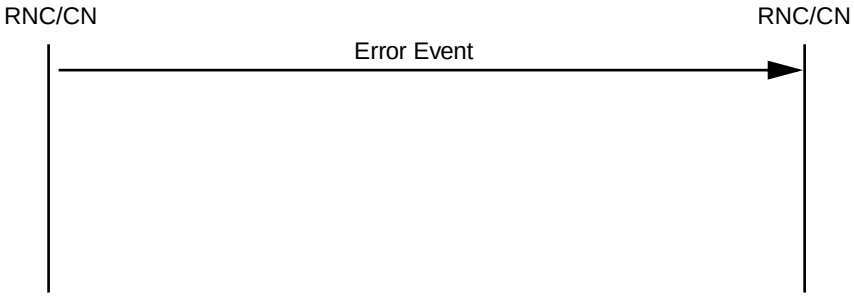


Figure 15
Error Event

© wray castle limited

3.5 SMpSDU Data Frames

Currently, SMpSDU data can be transported across the Iu interface either with error detection, in the form of a CRC, applied to the payload or not. If the RAB parameters indicate that error detection is required then a PDU Type 0 frame is used; otherwise a PDU Type 1 frame is used. PDU type 2-13 and PDU type 15 frame have not yet been defined. The message flow and frames are shown in the diagram opposite.

3.5.1 Frame Quality Classification

In the RAB Assignment message the RAB properties were used to indicate the QoS profile required. This included the element defining whether corrupt SDUs should be transmitted. If so the Frame Quality Classification address space is used to indicate this. 0 indicates a good frame, 1 indicates a bad frame and 2 indicates a bad frame due to the radio interface.

© wray castle limited

a) PDU Type 0

Bits								Number of Octets	
7	6	5	4	3	2	1	0		
PDU Type (=0)				Frame Number				1	Frame Control Part
FQC 0 = good, 1 = bad, 2 bad due to radio				RFCI				1	
Header CRC						Payload CRC		2	Frame Checksum Part
Payload CRC									
Payload Fields								0–n	Frame Payload Part
Payload Fields				Padding					
Spare extension								0–4	

b) PDU Type 1

Bits								Number of Octets	
7	6	5	4	3	2	1	0		
PDU Type (=1)				Frame Number				1	Frame Control Part
FQC 0 = good, 1 = bad, 2 bad due to radio				RFCI				1	
Header CRC						Spare		1	Frame Checksum Part
Payload Fields								0–n	Frame Payload Part
Payload Fields				Padding					
Spare extension								0–4	

Figure 16
PDU Type 0 and PDU Type 1

© wray castle limited

3.6 Summary of the Iu Interface

The Iu-CS interface will consist of a number of AAL5 connections for the signalling of ALCAP and RANAP messages. The RANAP messages are used to transport the NAS signalling between the CN and the UTRAN.

RANAP and ALCAP are both required to establish RABs at the Radio Network and Transport Network Layers respectively.

Depending on the UMTS bearer service in use, the Iu protocol will be required to interface to a number of functions.

© wray castle limited

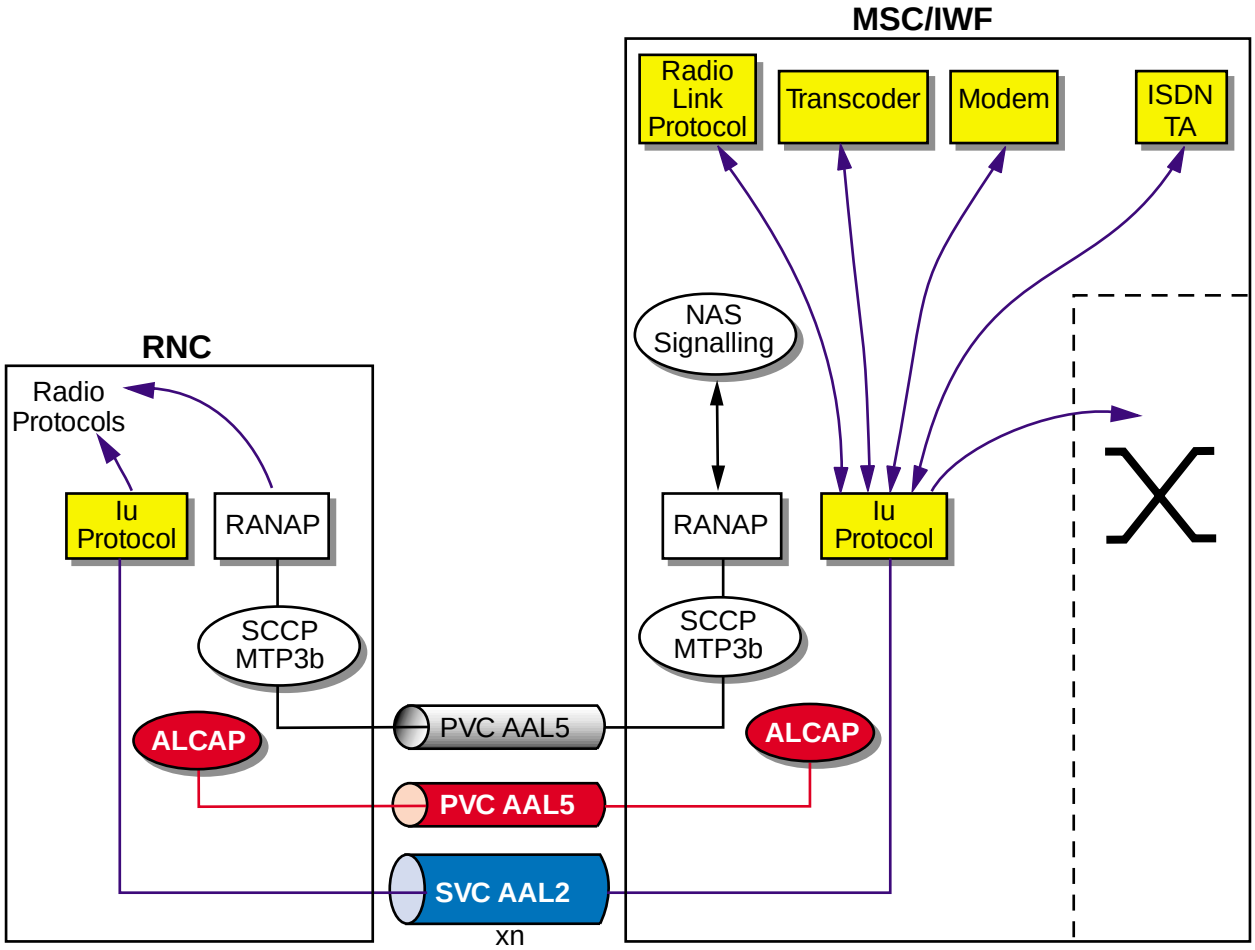


Figure 17
Iu-CS Summary

© wray castle limited

© wray castle limited

LESSON 5

Iu PROTOCOLS
(PACKET-SWITCHED DOMAIN)

© wray castle limited

© wray castle limited

LESSON CONTENTS

1 Iu Interface Protocol Structure Towards the PS Domain 6.5.1
1.1 GPRS Tunnelling Protocol – User Plane (GTP-U) 6.5.1
1.2 Iu Architecture – Options 6.5.3
1.3 Iu Interface Protocol Structure Towards the Broadcast Domain 6.5.5

2 Service Area Broadcast Protocol (SABP) 6.5.7
2.1 Services Provided by SABP 6.5.7
2.2 Functions of SABP 6.5.9
2.3 SABP Data Transfer 6.5.11

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- explain the use and scope of the Iu protocols involved in a packet-switched connection

© wray castle limited

1 Iu INTERFACE PROTOCOL STRUCTURE TOWARDS THE PS DOMAIN

RANAP is used on the Iu interface towards the PS domain to carry all control data including higher-layer (CM and MM) messages, as shown in Figure 1.

The User Plane is comprised of packet user data only (although higher-layer application protocols such as WAP information may be carried as user data).

Since switched virtual circuits in the Transport Network User Plane (for transport of the packet user data) are not required, there is no need for the use of signalling to set-up virtual circuits. Hence, the Transport Network Control Plane is empty/null.

1.1 GPRS Tunnelling Protocol – User Plane (GTP-U)

The GTP-U protocol is used to transmit and receive Traffic Packet Data Units (T-PDUs) between an SGSN and an RNC, encapsulated in GTP Packet Data Units (G-PDUs). A G-PDU is a packet including a GTP-U header and a T-PDU. The path protocol (IP) defines the path and the GTP-U header defines the tunnel. Several tunnels may be multiplexed on a single path.

© wray castle limited

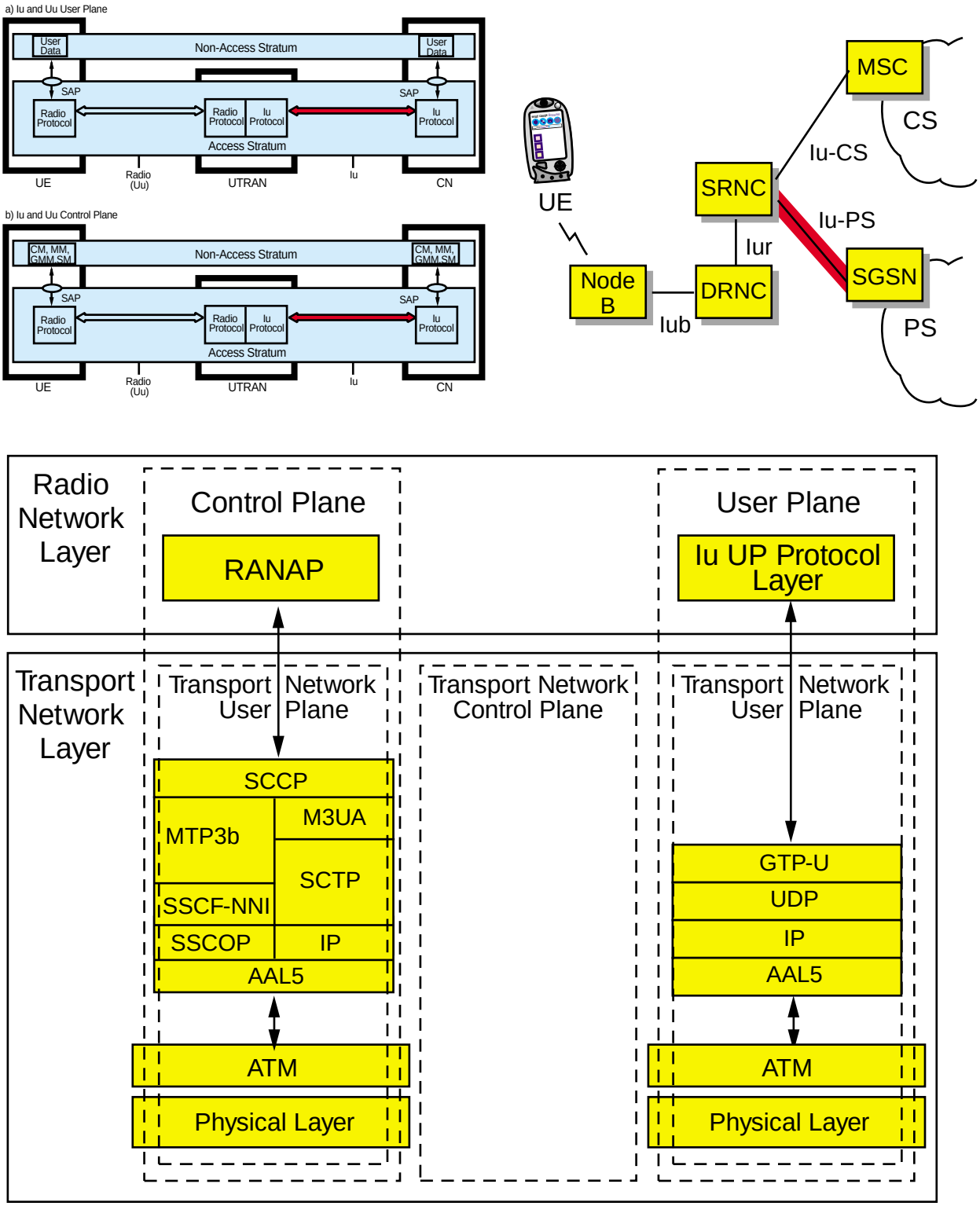


Figure 1

Iu Interface Protocol Structure Towards Packet-Switched (PS) Domain

© wray castle limited

1.2 Iu Architecture – Options

As shown in Figure 2, the options available on the Iu interface are either a physically separated MSC and SGSN, or a combined MSC/SGSN.

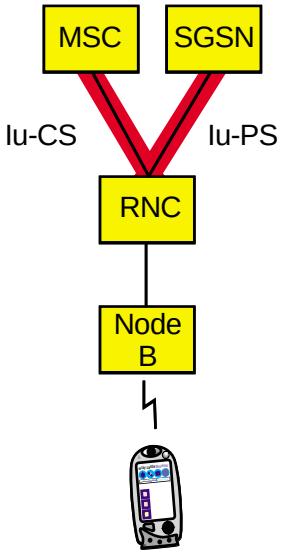
In each case, it is important to note that separate User Plane connections are provided to the CS and PS domains in both Transport and Radio Network Layers. In the case of a separate MSC and SGSN, the CN termination points for the two domains are, naturally, also physically separate.

Where the MSC and the SGSN are separate, individual links are provided for Control Plane information (RANAP signalling), with physically different connections at the CN. For the combined MSC and SGSN, however, different SSCP connections to the relevant domain(s) are set up as required.

The signalling links themselves may be shared, but identifiers exchanged at SCCP level ensure that signalling is handled by the required entity (MSC or SGSN) in the required domain.

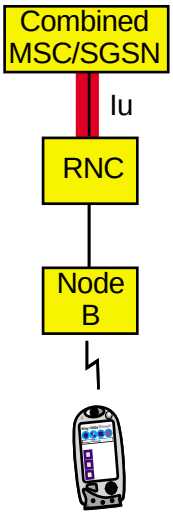
© wray castle limited

Separated CN Architecture



- Separate Control Plane (signalling) and User Plane connections towards CS and PS Domains
- Applies to both Transport and Radio Network Layers

Combined CN Architecture



- Separate User Plane connections to CS and PS domains (in both Transport and Radio Link Network)
- Separate SCCP connections in Control Plane to CS and PS domains

Figure 2

Iu Architecture – Options

© wray castle limited

1.3 Iu Interface Protocol Structure Towards the Broadcast Domain

Towards the broadcast domain, the User Plane and Control Planes are replaced with a single Service Area (SA) Broadcast Plane (see Figure 3).

In the Radio Network Layer, the Service Area Broadcast Protocol (SABP) provides the (CN-generated) broadcast functionality. In the Transport Network Layer, TCP/IP over ATM is used to transfer the SABP information to and from the UTRAN. A predefined ATM connection is used for this purpose, hence no Transport Network Layer Control Plane protocols are required.

© wray castle limited

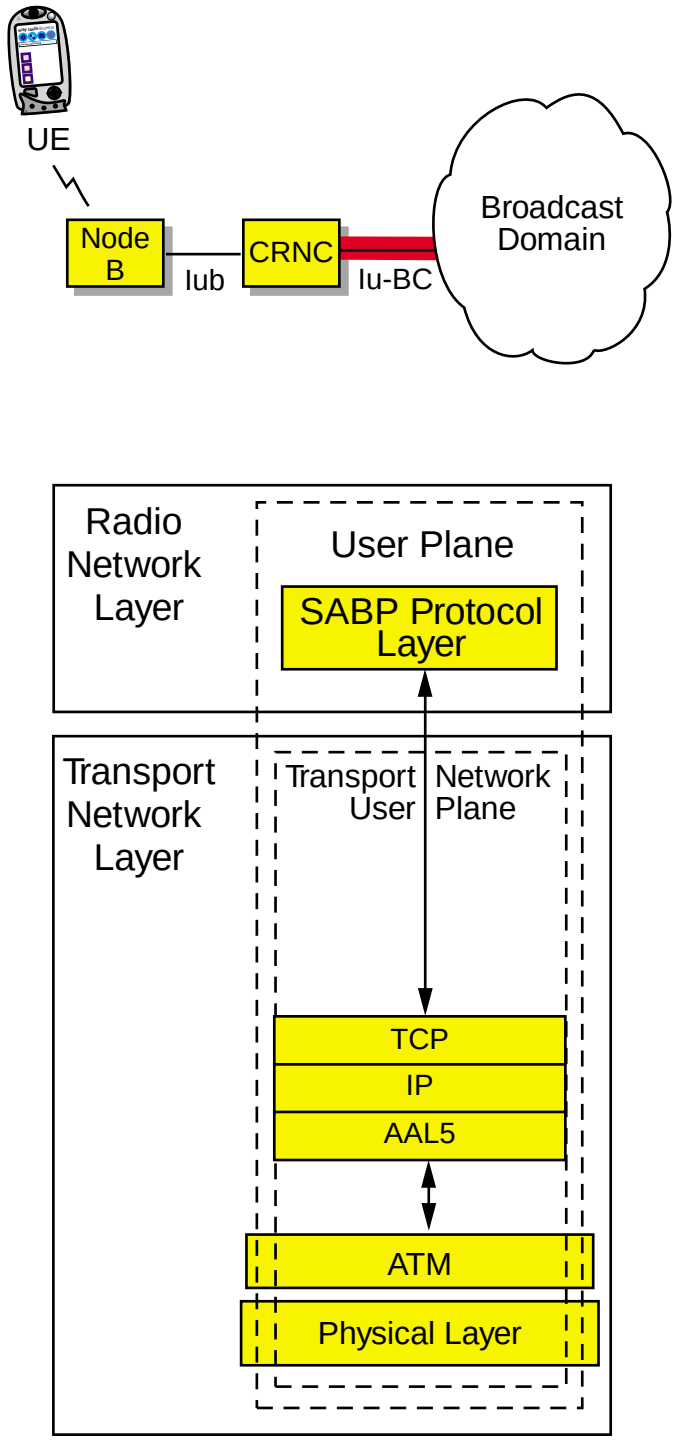


Figure 3

Iu Interface Protocol Structure Towards the Broadcast Domain

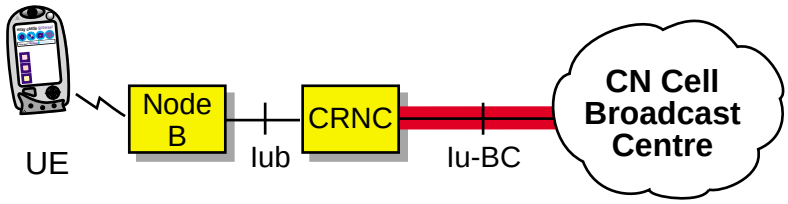
© wray castle limited

2 SERVICE AREA BROADCAST PROTOCOL (SABP)

2.1 Services Provided by SABP

The SABP provides message transfer from the CN (Cell Broadcast Centre (CBC)) to the RNC over the Iu-BC interface. SABP also allows for error and recovery procedures to be sent from the RNC to the CN.

© wray castle limited



SABP Provides:

- Cell Broadcast Message transfer

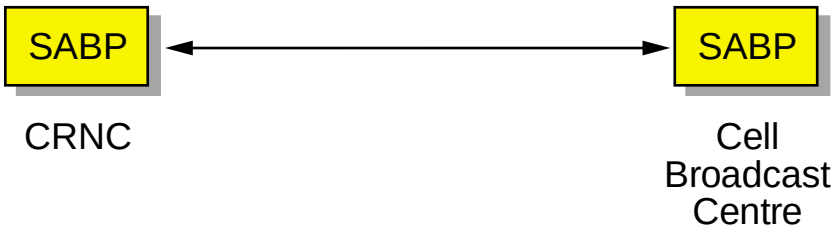


Figure 4

Services Provided by SABP

© wray castle limited

2.2 Functions of SABP

The functions of SABP are summarized in Figure 5.

They include procedures for the following:

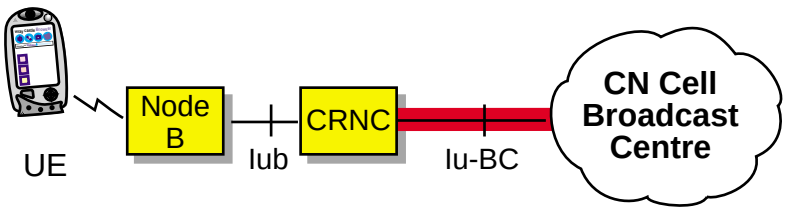
Message Handling
Message Handling is responsible for the broadcast of new messages and the amending/stopping of existing messages in one or more SA.

Load Handling
Load Handling is responsible for identifying that loading is a certain SA.

Reset
The Reset function allows the CBC to end broadcasting in one or more SA.

Error Handling
The Error Handling function allows error indications to be sent from the RNC to the CN (CBC).

© wray castle limited



Functions of SABP:

- Cell broadcast message handling
- Load handling
- Reset
- Error handling

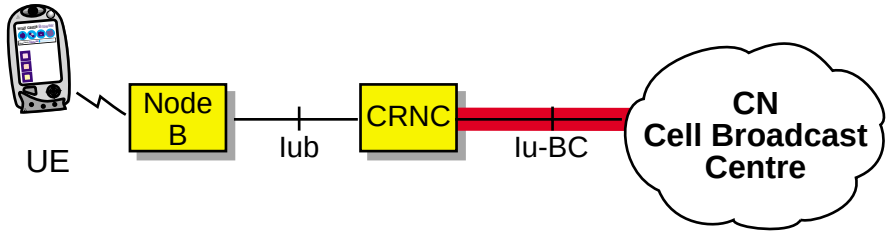
Figure 5
Functions of SABP

© wray castle limited

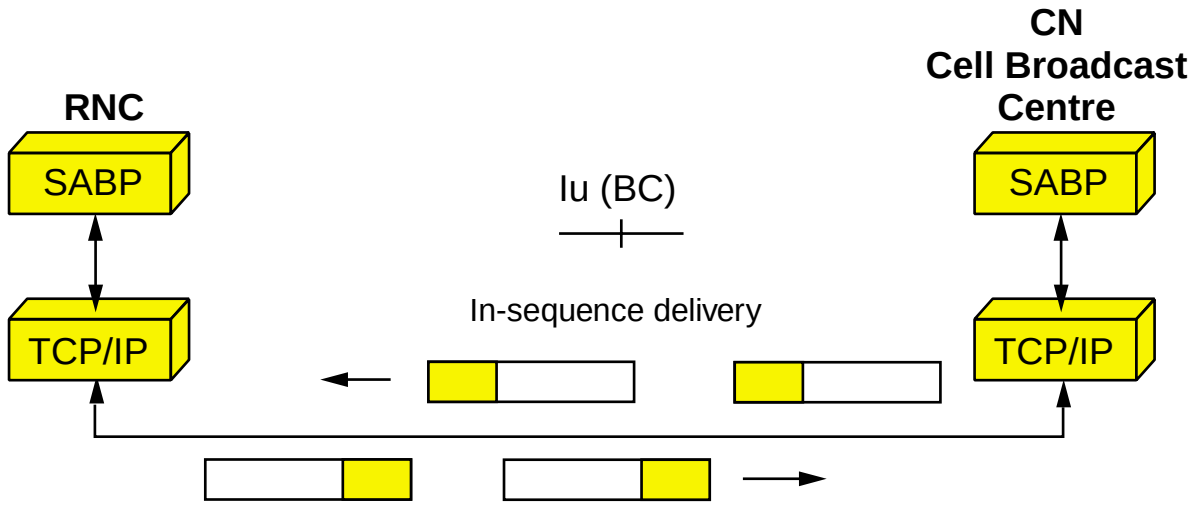
2.3 SABP Data Transfer

The SABP expects in-sequence delivery from the Transport Layer. The Transport Layer service for SABP is TCP/IP. Standard TCP/IP establishment procedures are used over the Iu-BC interface. The establishment of the connection for message transfer is done by the CN; RNC establishment is carried out when error and recovery procedures need to be initiated. The TCP/IP connection is always released by the node that initiated the connection.

© wray castle limited



Transport Service for SABP



- TCP/IP is used as a bearer
- Usually established by CN

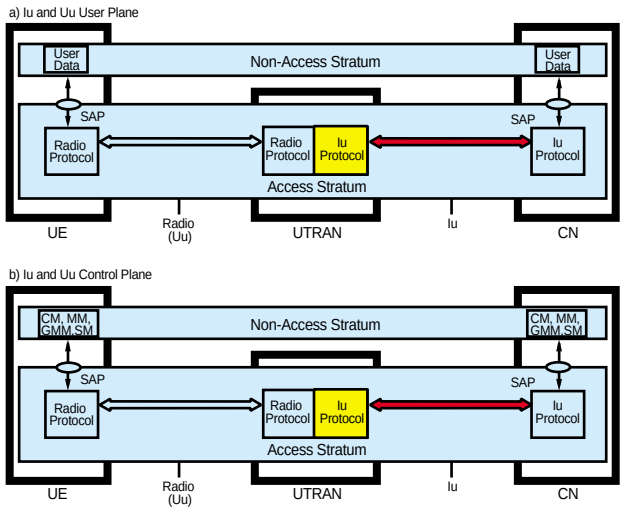
Figure 6
SABP Data Transfer

© wray castle limited

© wray castle limited

ANNEX A TO SECTION 6

UTRAN PROTOCOL SPECIFICATIONS



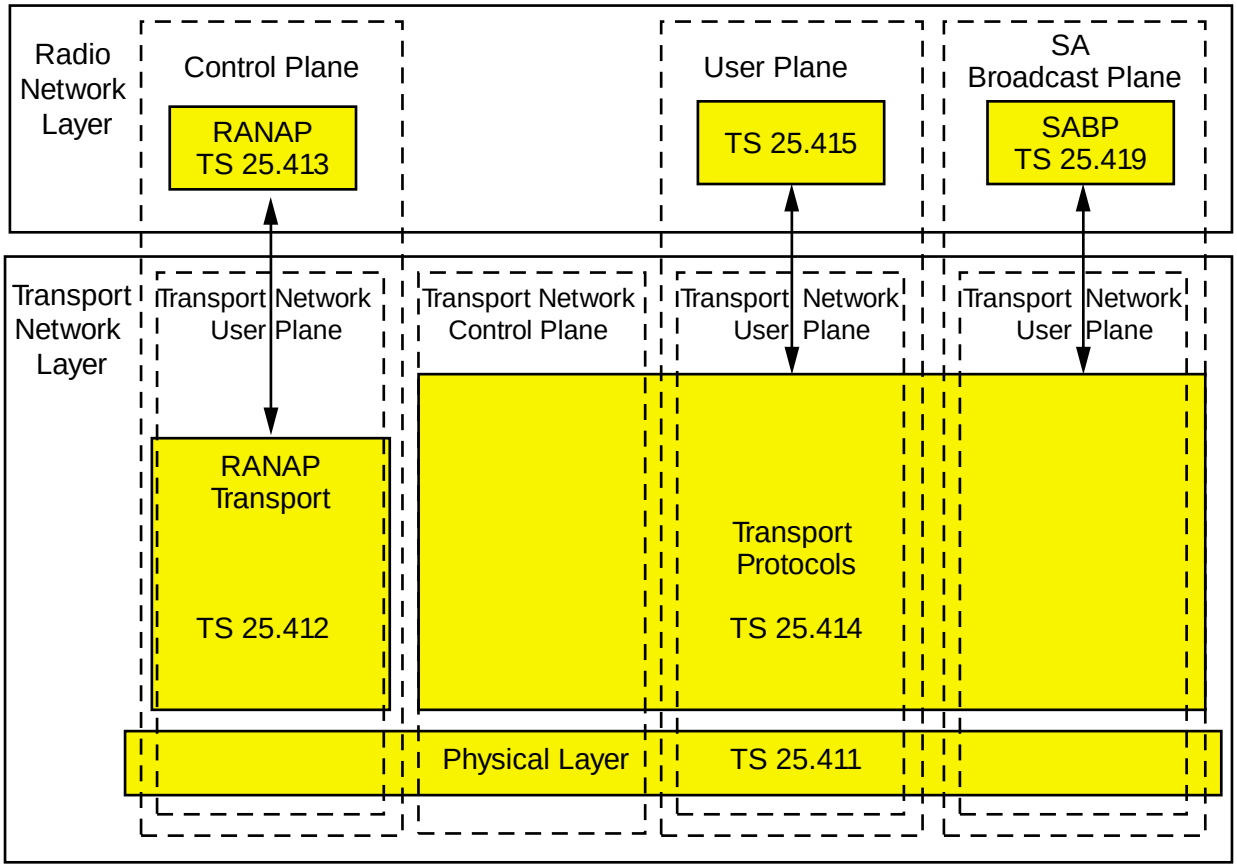
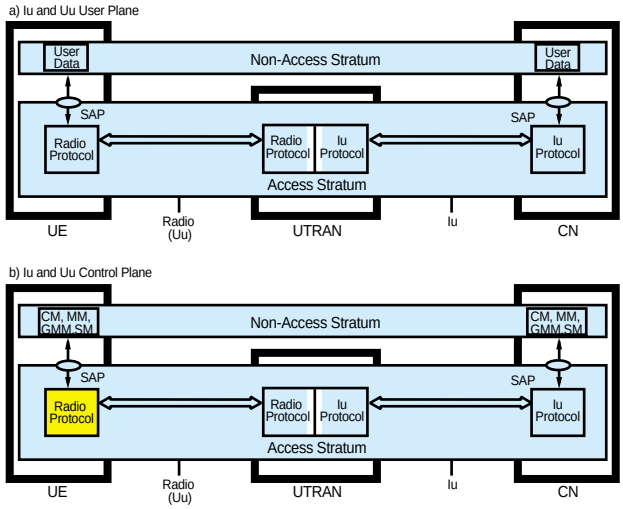


Figure 1

Summary of Iu Interface Specification Structure

© wray castle limited



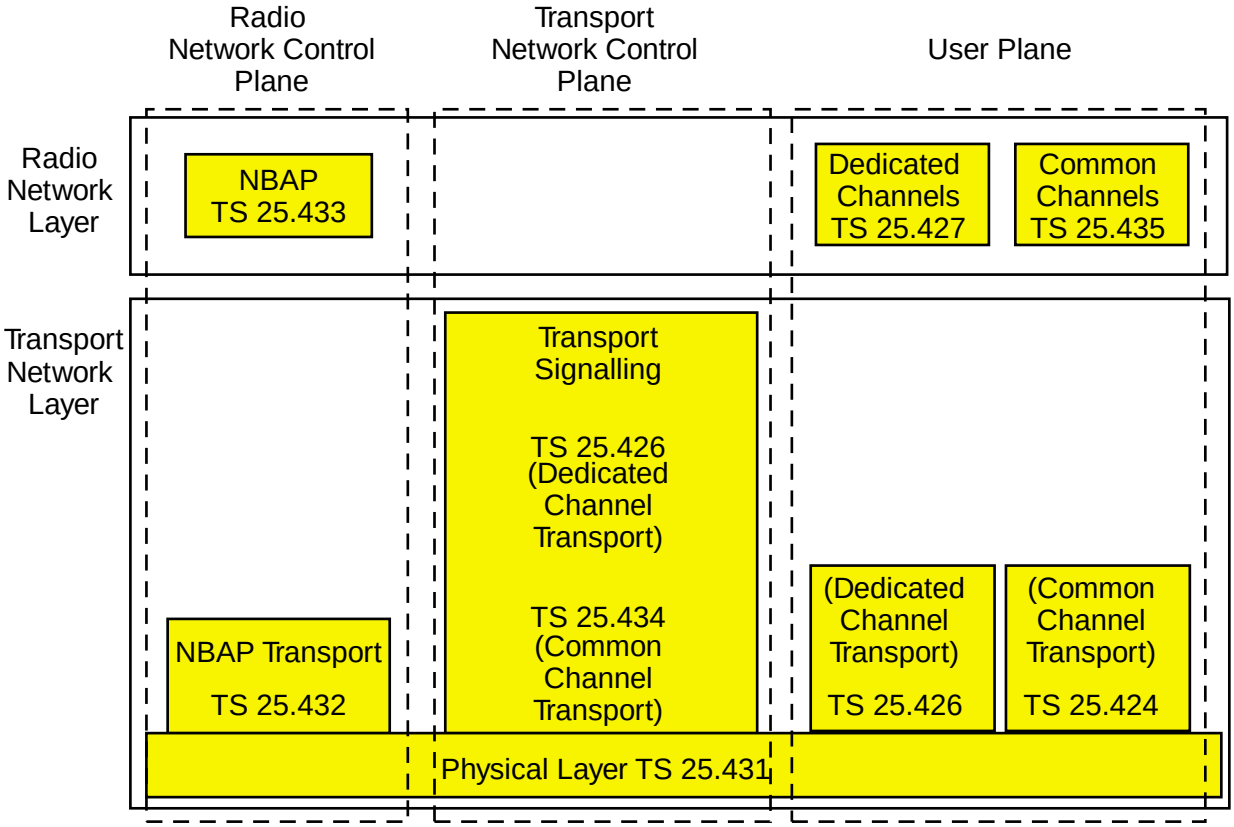
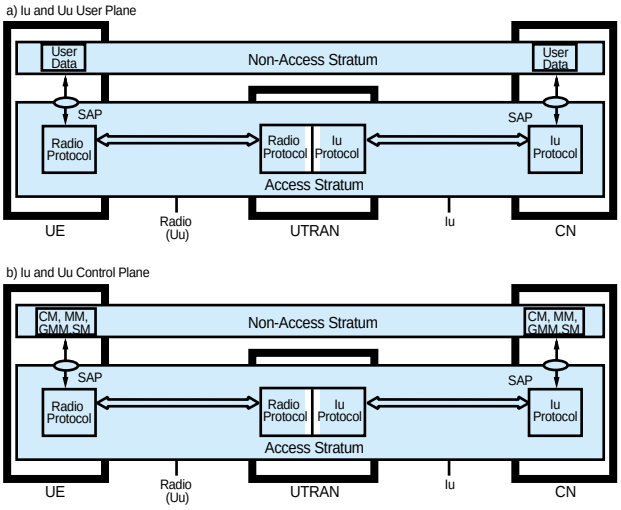


Figure 2

Iub Interface Technical Specifications

© wray castle limited



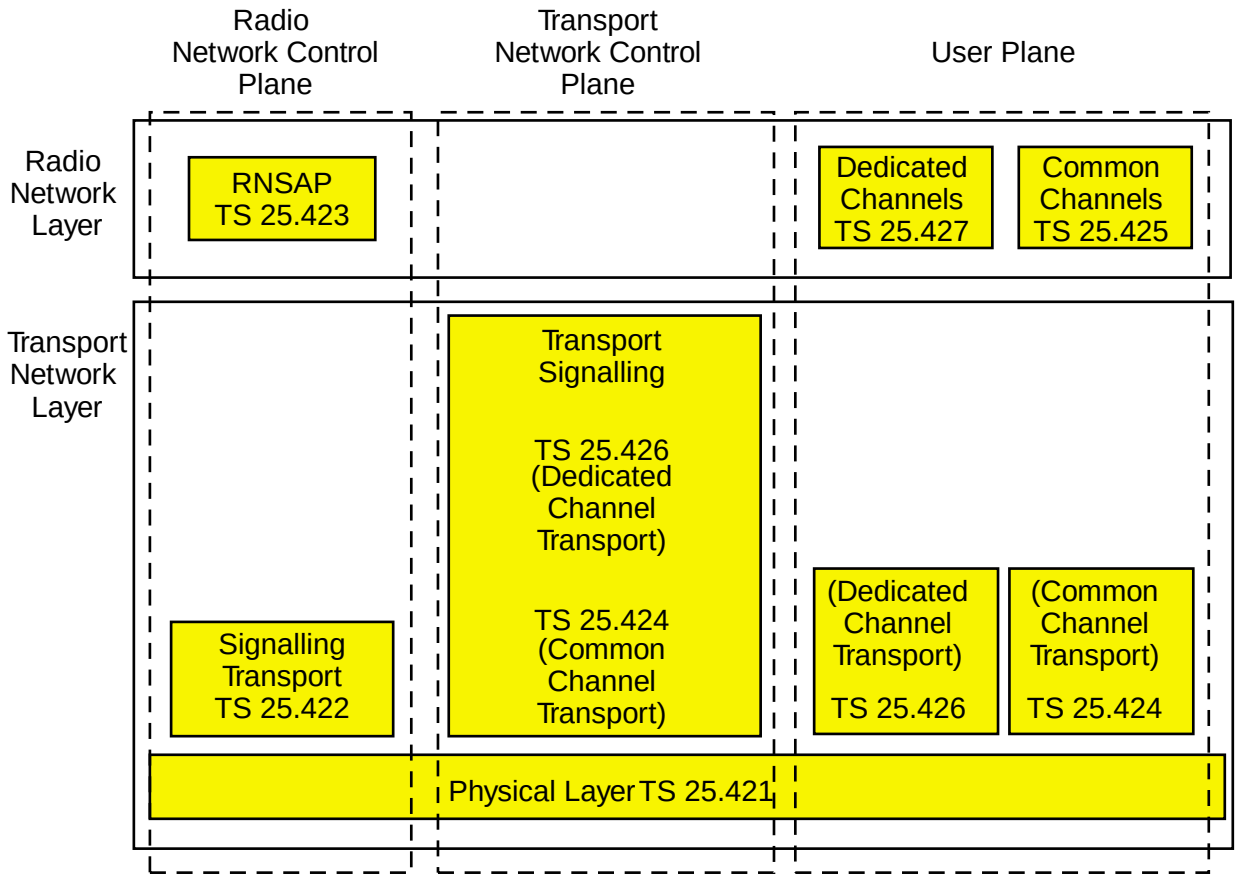


Figure 3

Iur Interface Technical Specifications

© wray castle limited

ANNEX B TO SECTION 6

MESSAGE SETS

RANAP Messages

RNC CN	Message	Response Message
←	RAB Assignment Request	RAB Assignment Response (xN)
→	RAB Release Request	–
→	Iu Release Request	–
←	Iu Release Command	Iu Release Complete
→	Relocation Required	Relocation Command (s) Relocation Preparation Failure (u)
←	Relocation Request	Relocation Request Ack (s) Relocation Failure (u)
→	Relocation Detect	–
→	Relocation Complete	–
→	Relocation Cancel	Relocation Cancel Ack
←	SRNS Context Request	SRNS Context Response
←	SRNS Data Forward Command	SRNS Data Forward Command
→	Forward SRNS Context	–
←	Paging	–
←	Common Id.	–
←	CN Invoke Trace	–
←	Security Mode Command	Security Mode Complete (s) Security Mode Reject (u)
←	Location Reporting Control	–
→	Location Report	–
←	Data Volume Report Request	Data Volume Report
→	Initial UE Message	–
↔	Direct Transfer	–
←	CN Information Broadcast Req	CN Information Broadcast Conf (s) CN Information Broadcast Rej (u)
↔	Overload	–
↔	Reset	Reset Acknowledge
↔	Error Indication	–
←	CN Deactivate Trace	–
↔	Reset Resource	Reset Resource Ack
↔	RNC RANAP Relocation Information	

Notes
1) RAB Assignment Request is Class 3 procedure (multiple responses allowed)
2) Where response messages are listed, these procedures are Class 1
3) Other procedures are Class 2

Figure 1
RANAP Messages

© wray castle limited

SABP Messages

RNC	CN (CBC)	Message	Response Message
	←	Write Replace	Write Replace Complete (s) Write Replace Failure (u)
	→	Kill	Kill complete Kill Failure (u)
	→	Load Query	Load Query Complete Load Query Failure (u)
	←	Message Status Query	Message Status Query Complete (s) Message Status Query Failure (u)
	→	Reset	Reset Complete Reset Failure
	←	Restart	–
	→	Failure	–
	→	Error Indication	–

Notes
1) Where response mesages are listed, these procedures are Class 1
2) Other procedures are Class 2

Figure 2
SABP Messages

© wray castle limited

NBAP Common Procedure Messages			
Node B — RNC	Message	Successful Outcome	Unsuccessful Outcome
		Response Message	Response Message
←	Cell Set-up Request	Cell Set-up Response	Cell Set-up Failure
←	Cell Reconfiguration Request	Cell Reconfiguration Response	Cell Reconfiguration
←	Common Transport Channel Set-up Request	Common Transport Channel Set-up Response	Common Transport Channel Set-up Failure
←	Common Transport Channel Reconfiguration Request	Common Transport Channel Reconfiguration Response	Common Transport Channel Reconfiguration Failure
←	Common Transport Channel Deletion Request	Common Transport Channel Deletion Response	
←	Audit Request	Audit Response	
→	Block Resource Request	Block Resource Response	Block Resource Failure
←	Radio Link Set-up Request	Radio Link Set-up Response	Radio Link Set-up Failure
←	System Information Update Request	System Information Update Response	System Information Update Failure
←	Common Measurement Initiation Request	Common Measurement Initiation Response	Common Measurement Initiation Failure
↔	Physical Shared Channel Reconfiguration Request (TDD)	Physical Shared Channel Reconfiguration Response	Physical Shared Channel Reconfiguration Failure

	Message
→	Resource Status Indication
→	Audit Required Indication
→	Common Measurement Report
←	Common Measurement Termination Request
→	Common Measurement Failure Indication
→	Unblock Resource Indication

Note:
Class 1 = Message and Response
Class 2 = Message with No Response (Assumed Successful)

Figure 3

NBAP Messages for Common Procedures

© wray castle limited

NBAP Dedicated Procedure Messages:			
Node B RNC	Message	Successful Outcome Response Message	Unsuccessful Outcome Response Message
←	Radio Link Addition Request	Radio Link Addition Response	Radio Link Addition Failure
←	Radio Link Deletion Request	Radio Link Deletion Response	
←	Radio Link Reconfiguration Prepare	Radio Link Reconfiguration Ready	Radio Link Reconfiguration Failure
←	Radio Link Reconfiguration Request	Radio Link Reconfiguration Response	Radio Link Reconfiguration Failure
←	Dedicated Measurement Initiation Request	Dedicated Measurement Initiation Response	Dedicated Measurement Initiation Failure
←	Compressed Mode Prepare	Compressed Mode Ready	Compressed Mode Failure

	Message
←	Radio Link Configuration Commit
←	Radio Link Reconfiguration Cancellation
→	Radio Link Failure Indication
→	Radio Link Restore Indication
→	Dedicated Measurement Report
←	Dedicated Measurement Termination Request
→	Dedicated Measurement Failure Indication
←	DL Power Control Request
←	Compressed Mode Commit
←	Compressed Mode Cancel
⇄	Error Indication

Note:
Class 1 = Message and Response
Class 2 = Message with No Response
(Assumed Successful)

Figure 4

NBAP Messages for Dedicated Procedures

© wray castle limited

RNSAP Basic Mobility Procedure Messages

DRNC		SRNC	Initiating Message
	→		Uplink Signalling Transfer Indication
	←		Downlink Signalling Transfer Request
Target RNC	←	Source RNC	SRNS Relocation Commit
CRNC	←	SRNC	Paging Request

RNSAP Common Transport Channel Procedure Messages

RNSAP Basic Mobility Procedure Messages:				
DRNC	SRNC	Initiating Message	Successful Outcome	Unsuccessful Outcome
			Response Message	Response Message
←		Common Transport Channel Resources Request	Common Transport Channel Resources Response	Common Transport Channel Resources Response
←				

	Message
←	Common Transport Channel Resources Release Request

RNSAP Global Procedure Messages

RNC 1	RNC 2	Message
←		Error Indication

Figure 5
RNSAP Messages for Basic Mobility, Common Transport Channel and Global Procedures

© wray castle limited

RNSAP DCH Procedure Messages:			
DRNC SRNC	Initiating Message	Successful Outcome Response Message	Unsuccessful Outcome Response Message
←	Radio Link Set-up Request	Radio Link Response	Radio Link Failure
←	Radio Link Addition Request	Radio Link Addition Response	Radio Link Addition Failure
←	Radio Link Deletion Request	Radio Link Deletion Response	
←	Radio Link Reconfiguration Prepare	Radio Link Reconfiguration Ready	Radio Link Reconfiguration Failure
←	Radio Link Reconfiguration Request	Radio Link Reconfiguration Response	Radio Link Reconfiguration Failure
→	Physical Channel Reconfiguration Request	Physical Channel Reconfiguration Command	Physical Channel Reconfiguration Failure
←	Dedicated Measurement Initiation Request	Dedicated Measurement Initiation Response	Dedicated Measurement Initiation Failure
←	Compressed Mode Prepare	Compressed Mode Ready	Compressed Mode Failure

	Message
←	Radio Link Reconfiguration Commit
←	Radio Link Reconfiguration Cancel
→	Radio Link Failure Indication
→	Radio Link Restore Indication
→	Dedicated Measurement Report
←	Dedicated Measurement Termination Request
→	Dedicated Measurement Failure Indication
←	DL Power Control Request
←	Compressed Mode Commit
←	Compressed Mode Cancel

Figure 6

RNSAP Messages for DCH Procedures

© wray castle limited

© wray castle limited

SECTION 7

PROTOCOL SYNOPSIS

© wray castle limited

LESSON 1

OVERVIEW OF UTRAN PROTOCOLS

© wray castle limited

LESSON CONTENTS

1 The UTRAN Protocols – Overall View 7.1.1
1.1 UTRAN and UE Control Plane Architecture (Idle Mode) 7.1.1
1.2 The Relationship Between RRC and UTRAN Interfaces 7.1.3
1.3 UTRAN and UE Control Plane Architecture (Connected Mode) 7.1.5
1.4 Common Channel Transport 7.1.7
1.5 Dedicated Channel Transport 7.1.9
1.6 Protocol Synopsis 7.1.11

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe the general operation of the UTRAN protocols

© wray castle limited

1 THE UTRAN PROTOCOLS – OVERALL VIEW

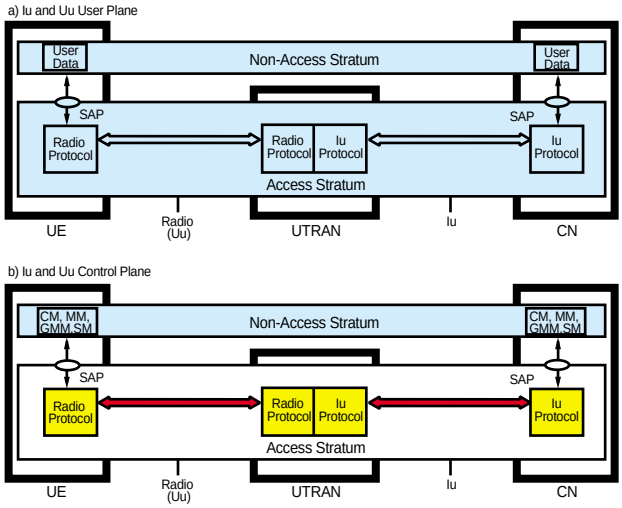
1.1 UTRAN and UE Control Plane Architecture (Idle Mode)

In idle mode, any information passed over any of the interfaces shown in Figure 1 will be transferred within the protocols shown. Note that RRC is carried within relevant logical and transport channels and terminates at the Node B in this case.

Although the UE is in idle mode, information on an interface may be mapped over to the next interface in cases where procedures (such as paging) require more than one interface to be involved.

The relevant transport protocols are used on each interface.

© wray castle limited



Note: (1) RRC, NBAP and RANAP are used to transfer control information

(2) A paging request from the CN may invoke RRC at the RNC

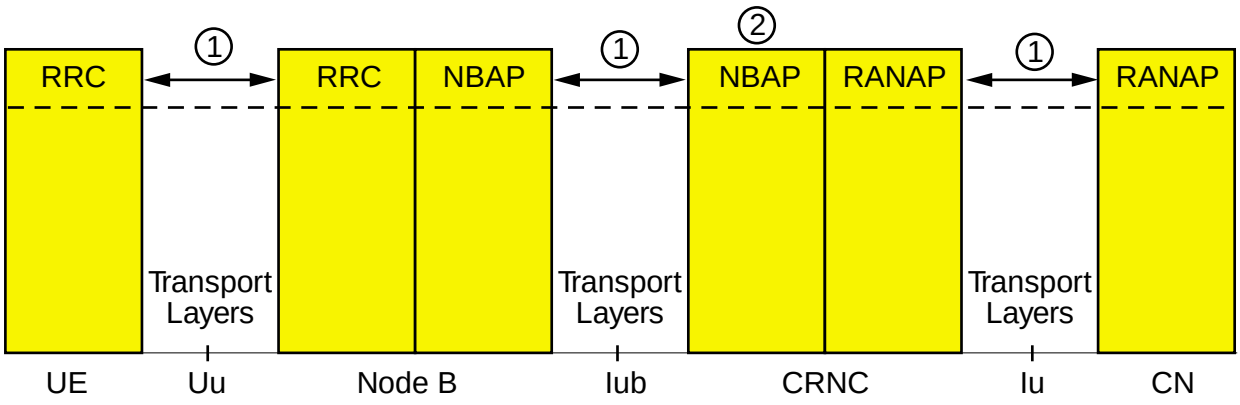


Figure 1

UTRAN and UE Control Plane Architecture (Idle Mode)

© wray castle limited

1.2 The Relationship Between RRC and UTRAN Interfaces

The relationship between the RRC and the UTRAN interfaces is shown in Figure 2.

An important point to note is that the RRC in idle mode is located at the Node B, while in dedicated mode it is located at the Serving RNC (SRNC). In both cases, the information is carried over the air interface in the appropriate logical and transport channels. Also in both cases, the logical and transport channels are carried over the air interface in physical channels, but in dedicated mode, the logical and transport channels are passed transparently through the UTRAN to the SRNC.

Since the RRC information is passed transparently over the Iub and Iur interfaces (within the appropriate channels), it is considered on each interface to be part of the User Plane and is simply carried within the appropriate framing protocols. However, control information is required on each interface to set up the appropriate pipes. This control information is provided in the form of the Node B Application Part (NBAP) on the Iub interface, and the Radio Network Subsystem Application Part (RNSAP) on the Iur interface. On both interfaces, the appropriate transport protocols are used.

Note that both NBAP and RNSAP functionalities are much wider than this (they are designed to carry all control information between the appropriate network entities).

RRC is designed to carry radio-related information (terminated at the UE and either the Node B or SRNC), and higher-layer messages (CM and MM), which terminate at the UE and CN and are therefore transferred over the Iu interface. RANAP provides the mechanism for the transfer of these higher-layer messages. The SRNC provides the mapping function.

Although it is not carried within the RRC, user data is shown in the diagram to illustrate its place in the channel/protocol organization. User data is simply carried between the UE and the SRNC within the appropriate logical and transport channels. It is therefore carried over the Iub and Iur within the appropriate framing and transport protocols.

© wray castle limited

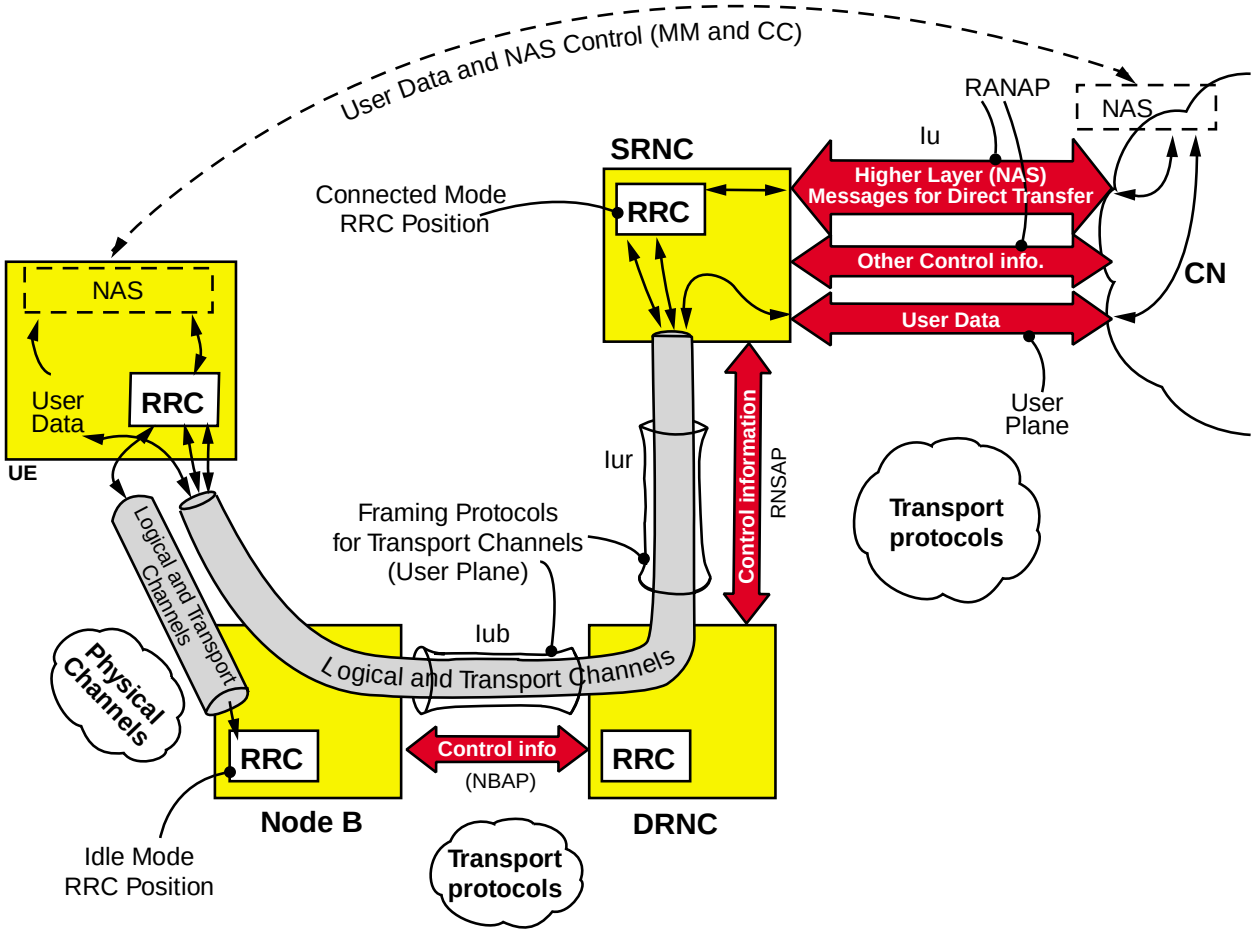


Figure 2

Relationship Between RRC and UTRAN Interfaces

© wray castle limited

1.3 UTRAN and UE Control Plane Architecture (Connected Mode)

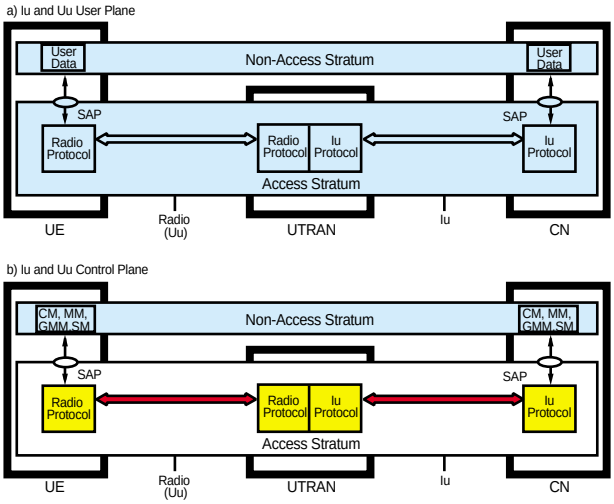
In the case of connected mode, the RRC connection is extended from the UE to the SRNC. RRC messages are carried over the Iub interface and, when present, the Iur interface, within transport channels in the User Plane of those interfaces.

At the SRNC, the RRC connection is terminated and relevant signalling is mapped to/from the RANAP connection for direct-transfer-type messages (higher-layer CM and MM messages). For other RRC messages, the SRNC interprets and acts on the information, or generates the message, depending on the direction of transfer.

NBAP and RNSAP are used to exchange relevant Iub and Iur interface control information, and also to control the transfer of User Plane information within the transport channels.

On all interfaces, the relevant transport protocols are used.

© wray castle limited



Note: (1) NBAP and RNSAP are used to control the transfer of RRC information in relevant transport channels (in User Plane).

(2) RRC and RANAP used to piggy back non-access stratum information and for additional control information.

(3) RRC information is organized into logical and transport channels' for delivery to UE and SRNC.

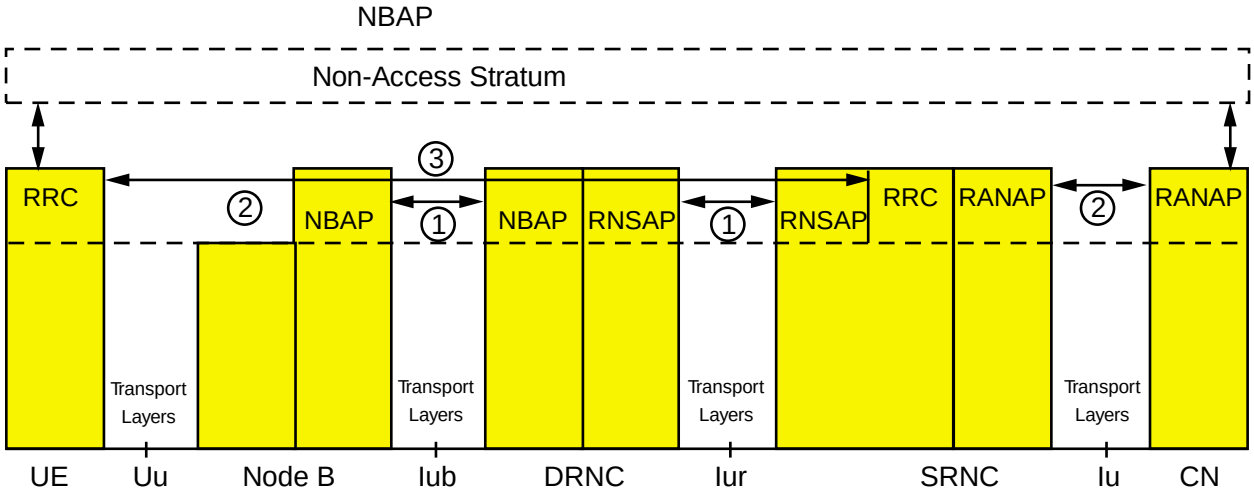


Figure 3

UTRAN and UE Control Plane Architecture (Connected Mode)

© wray castle limited

1.4 Common Channel Transport

Logical channels can use the services of MAC. The DCCH and DTCH map into MAC-d, which then uses the services of MAC-c/sh. The CCCHs map straight into MAC-c/sh.

The MAC header for CCCH consists of the Target Channel Type Field (TCTF). This is coded to indicate the type of channel, e.g. CCCH, BCCH, etc.

The MAC header for DCCH or DTCH consists of:

- TCTF
- UE-Id type – UTRAN Radio Network Temporary Identifier (u-RNTI) or Call RNTI (c-RNTI)
- UE-Id
- C/T – Channel Type (Logical)

The MAC SDU with the MAC header is passed down to the Physical Layer as a TB. Once over the air interface, the Node B interworks the TBs received into the Iub FP. The Iub FP entity adds header information to form an Iub FP PDU, which is transported to the RNC over an AAL2 connection.

The Iub FP header consists of:

- Header Cyclic Redundancy Check (CRC)
- Connection Frame Number (CFN)
- Transport Format Indicator (TFI)
- Propagation Delay (PD)

In this example, the Iur FP is used to interwork MAC-c/sh at the CRNC with MAC-d at the SRNC.

The CRNC adds the Iur FP header:

- Header CRC
- Serving RNC RNTI (s-RNTI)
- PD
- Length Indicator (LI)
- Number of MAC SDUs

© wray castle limited

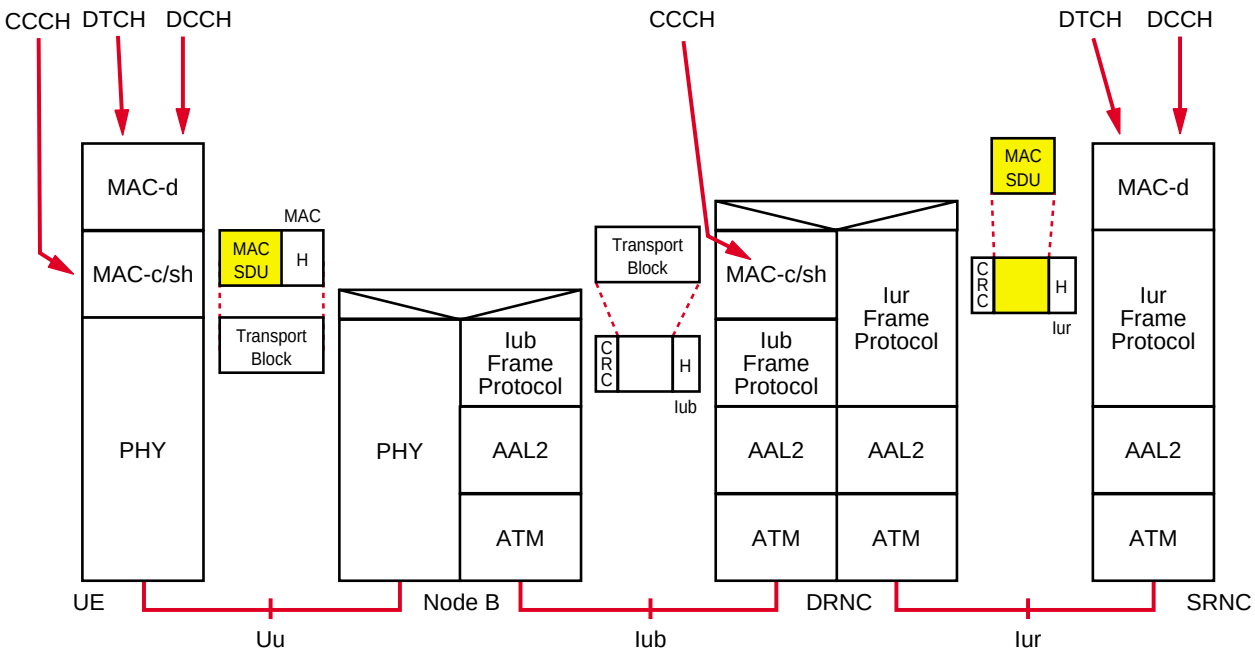


Figure 4
Common Channel Transport

© wray castle limited

1.5 Dedicated Channel Transport

Figure 5 shows the protocol model for the DCH transport channel. The DCH transport channel introduces the concept of distributed Physical Layer (PHY).

The MAC SDU will have a MAC header if it is multiplexing DCHs. This consists of a C/T field (Logical Channel Type).

The Node B interworks the TBs to the Iub/Iur DCH FP.

The Iub/Iur DCH FP header consists of:

- Header CRC
- CFN
- TFI x n

© wray castle limited

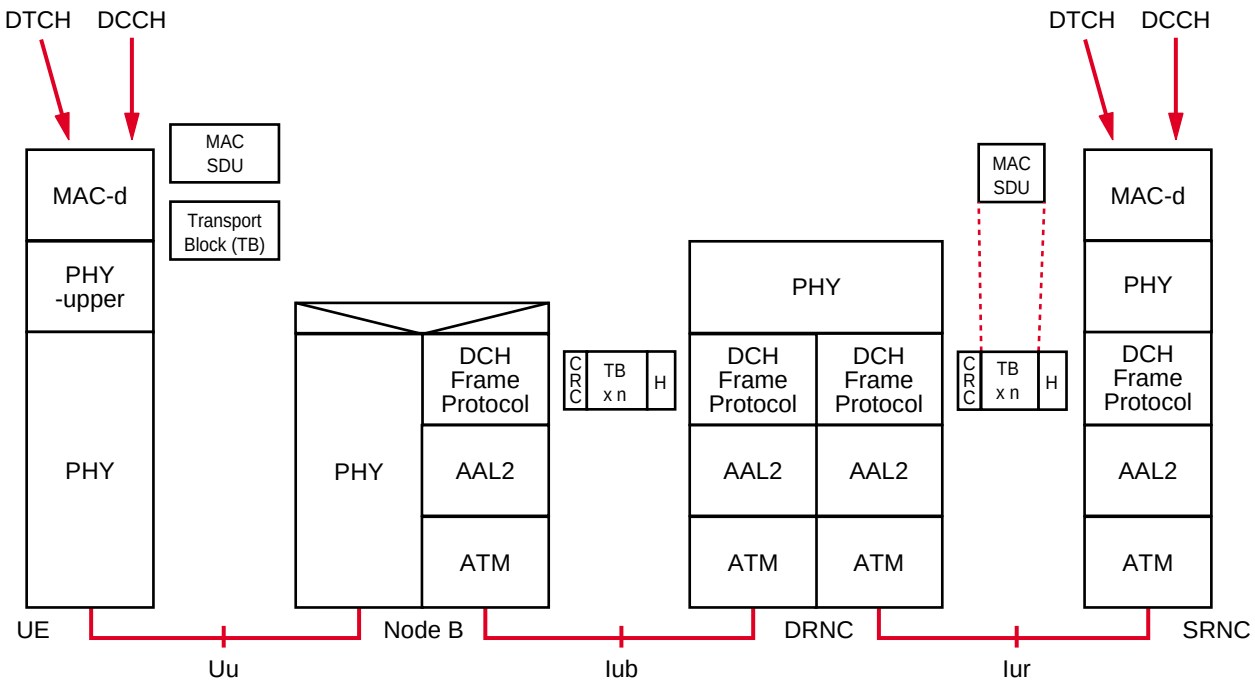


Figure 5
DCH Transport

© wray castle limited

1.6 Protocol Synopsis

The following diagrams simplify the delivery of NAS information from both the control and user planes of the UE using common, shared and dedicated resources, via the UTRAN to the CN.

© wray castle limited

An example of delivery of NAS in the Control Plane between UE and CN
Utilizing Common Transport Channels

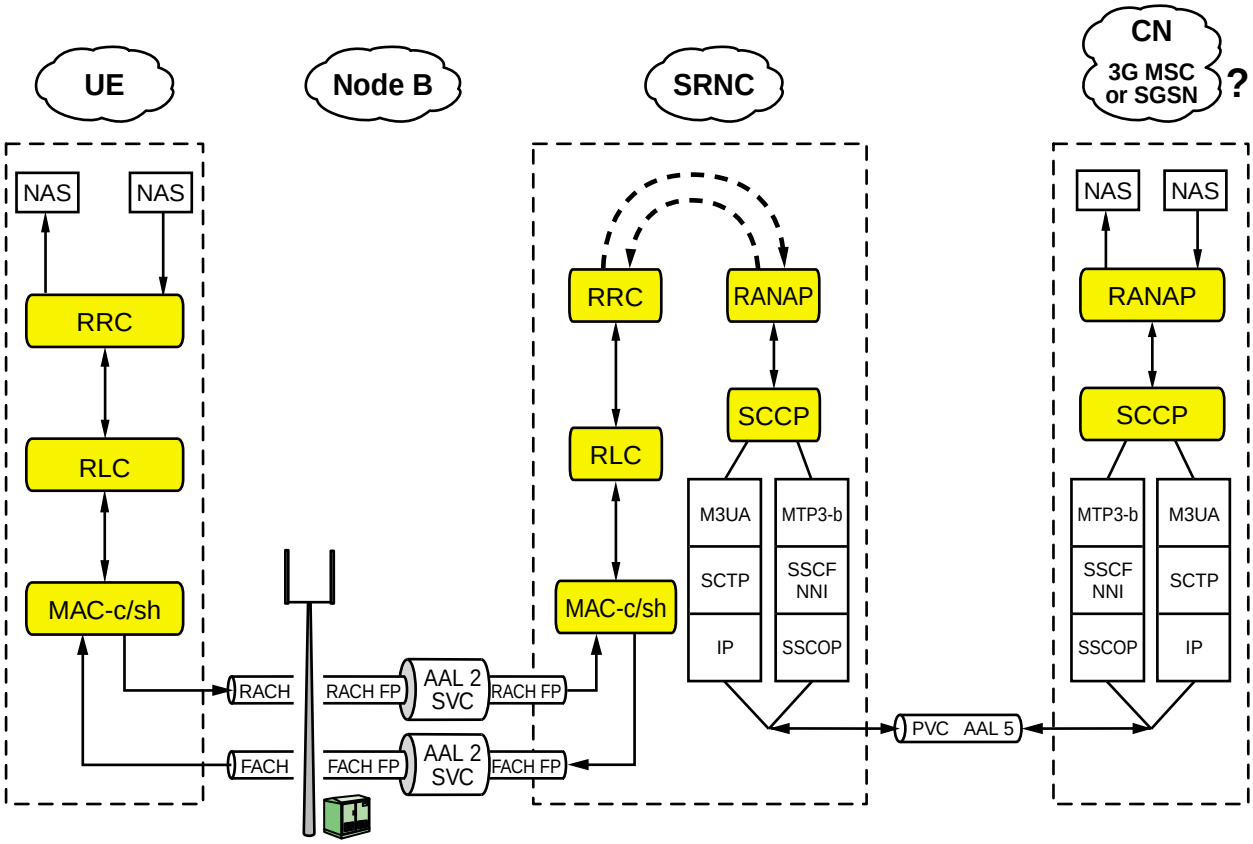


Figure 6

Utilizing Common Transport Channels

© wray castle limited

An example of delivery of NAS information in the User Plane between UE and CN
Utilizing Shared Transport Channels

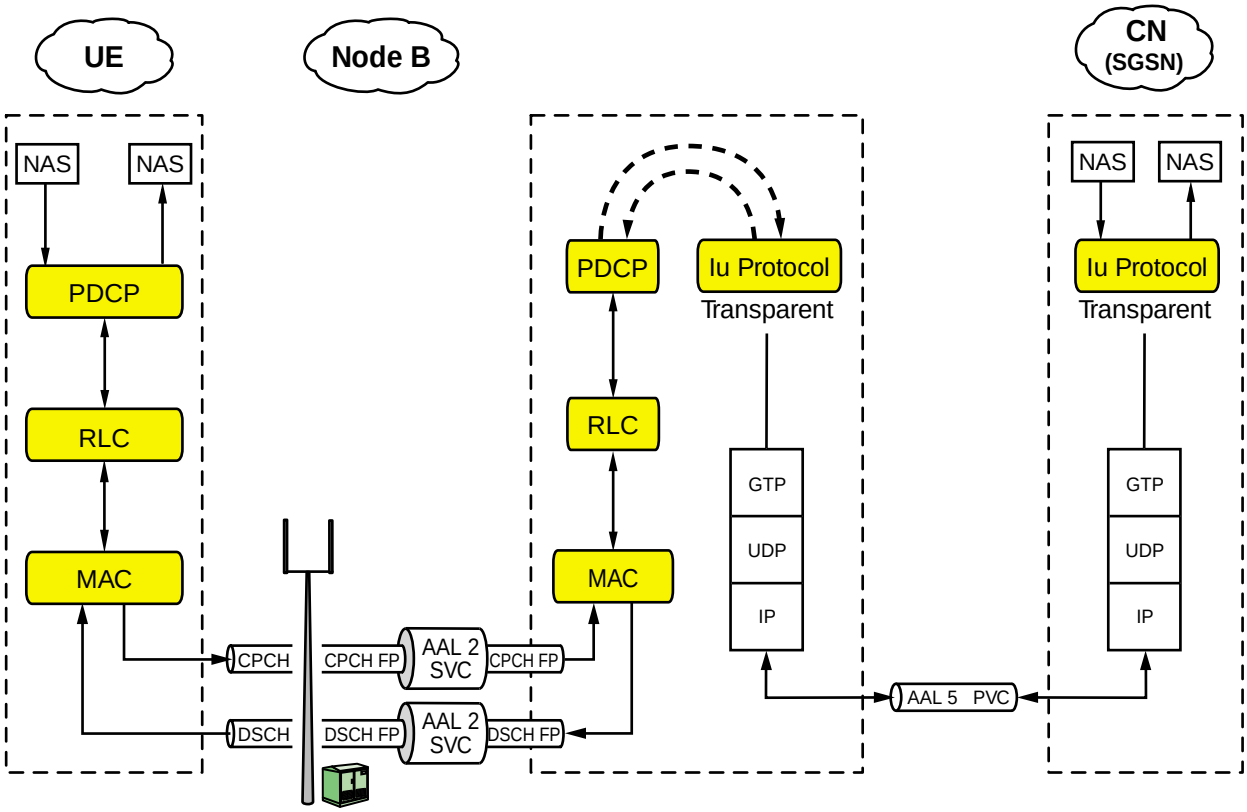


Figure 7
Utilizing Shared Transport Channels

© wray castle limited

An example of delivery of NAS information in the Control Plane between UE and CN
Utilizing Dedicated Transport Channels

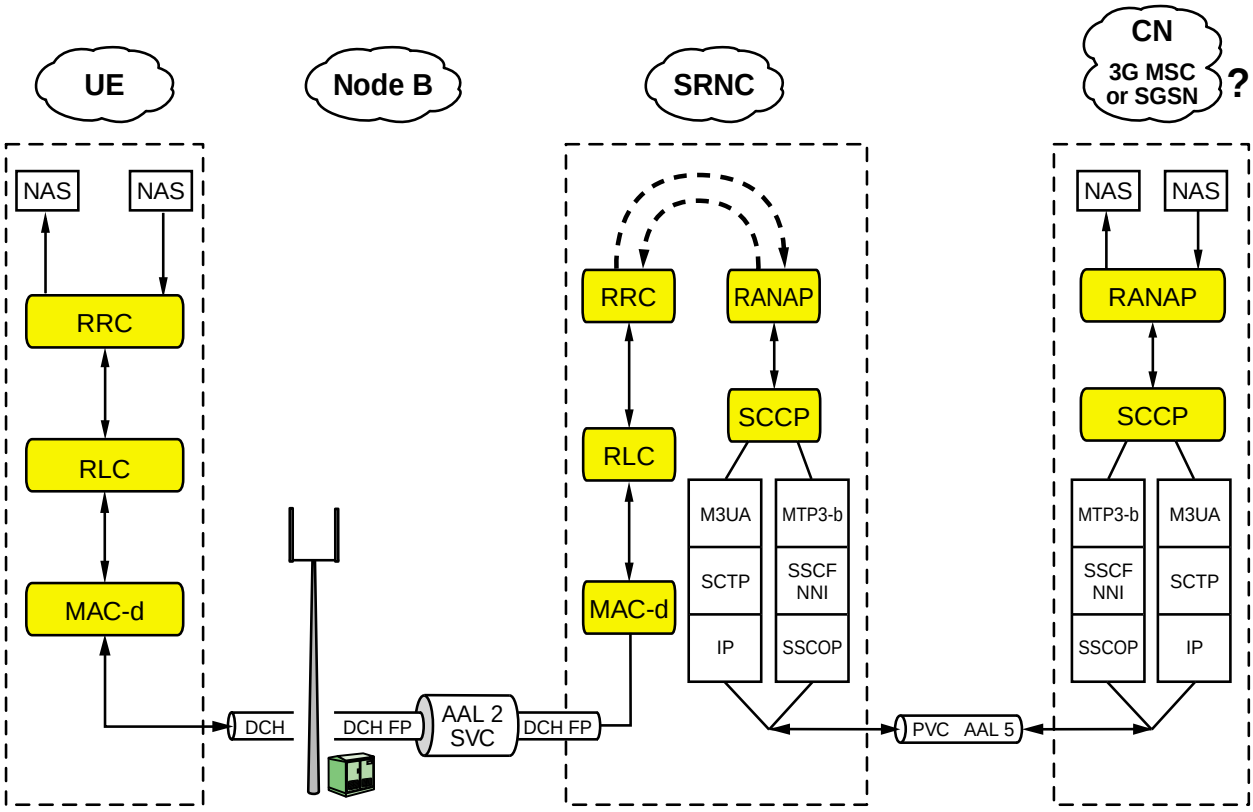


Figure 8
Utilizing Dedicated Transport Channels

© wray castle limited

© wray castle limited

SECTION 8

SIGNALLING SEQUENCES

© wray castle limited

LESSON 1

SIGNALLING SEQUENCES

© wray castle limited

LESSON CONTENTS

1	**Global Procedures**		**8.1.1**
	1.1	Introduction	8.1.1
	1.2	System Information Messages	8.1.1
	1.3	Service Area Broadcast	8.1.3
	1.4	Paging	8.1.5
2	**Connected Mode Procedures**		**8.1.7**
	2.1	General Concepts	8.1.7
	2.2	Communication between UE and the CN	8.1.7
	2.3	Radio Bearer Provision	8.1.7
	2.4	RRC Connection	8.1.9
	2.5	NAS Signalling Transfer	8.1.13
	2.6	RAB Establishment	8.1.15
	2.7	Radio Access Bearer (RAB) Release	8.1.17
	2.8	RRC Connection Release	8.1.19
3	**Handovers**		**8.1.21**
	3.1	Introduction	8.1.21
	3.2	Controlling Elements	8.1.21
	3.3	Soft Handover	8.1.23
	3.4	Macro and Micro Diversity	8.1.23
	3.5	Example of a Soft Handover	8.1.25
	3.6	Soft Handover – Radio Link Addition	8.1.27
	3.7	Soft Handover – Radio Link Deletion	8.1.29
	3.8	RNC Relocation	8.1.31
	3.9	Hard Handover	8.1.33
	3.10	UTRAN to GSM/BSS Handover	8.1.35
	3.11	Cell Update	8.1.39
	3.12	URA Update	8.1.41

© wray castle limited

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe the main signalling sequences used within the UTRAN

© wray castle limited

1 GLOBAL PROCEDURES

1.1 Introduction

The term *global* is used to identify procedures where the messages are not related to a specific UE. These procedures require the mobile to be listening at the right time to intercept the messages.

1.2 System Information Messages

System Information messages convey considerable information to the UEs.

The System Information transfer is shown in Figure 1, and detailed below.

1 The RNC sends an ‘NBAP: System Information Update Request’ to the appropriate Node B(s), including:
- System information to be broadcasted
- Broadcast Control Channel (BCCH) modification time
- Cell Identifier
- Transaction Identifier

2 The Node B returns an ‘NBAP: System Information Update Response’ message confirming its ability to broadcast.
- Transaction Identifier

3,4 The Node B broadcasts over the air interface using the ‘RRC: System Information’ message.

© wray castle limited

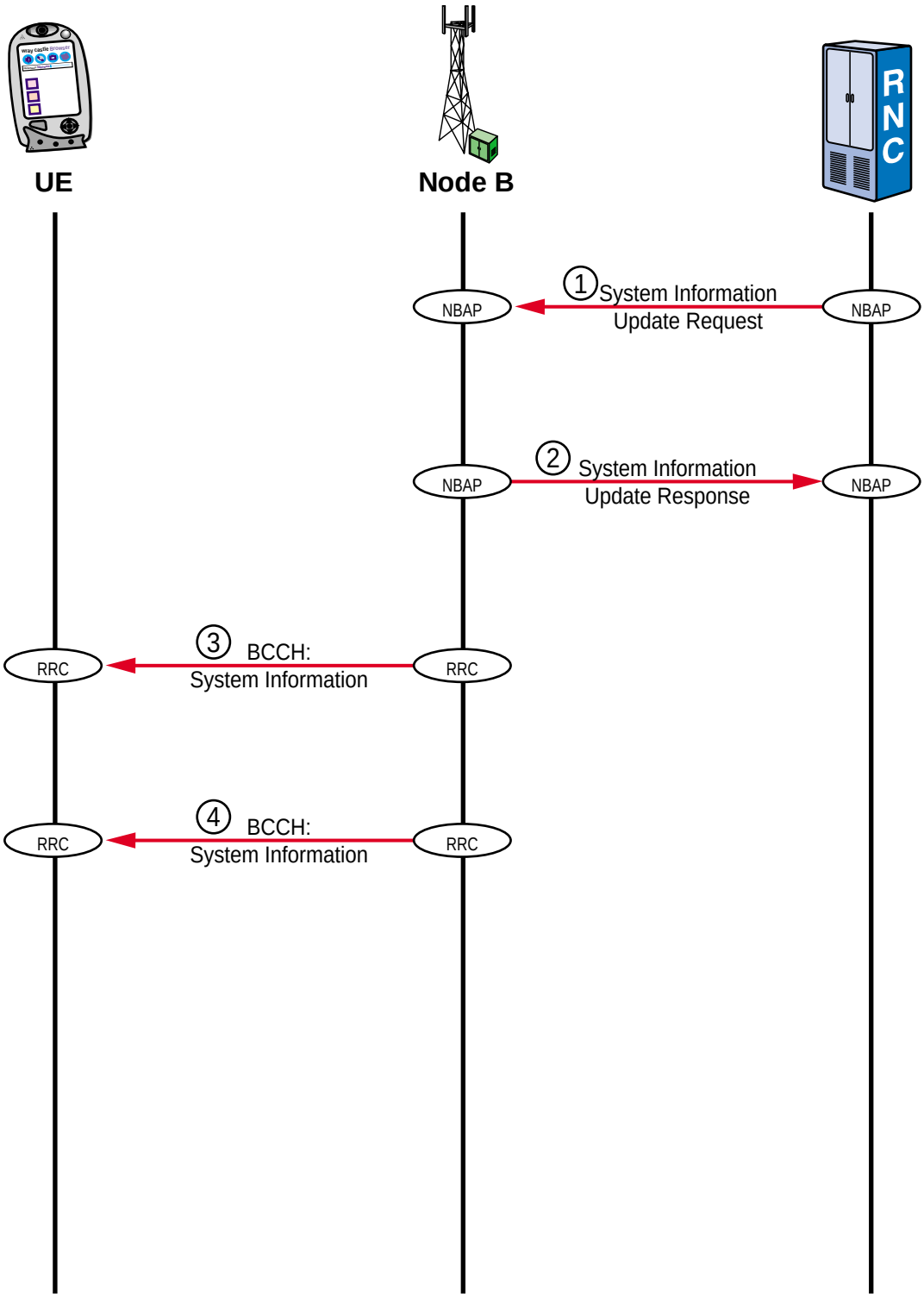


Figure 1
System Information Broadcasting

© wray castle limited

1.3 Service Area Broadcast

This procedure is used to broadcast cell information (Cell Broadcast messages) across a defined service area. The Cell Broadcast messages arriving from the CN are passed transparently through the UTRAN.

The cell broadcast procedure is shown in Figure 2, and detailed below:

1 The CN sends an ‘SABP: Write-replace’ message to the RNC. This contains:
- Cell Broadcast Message content
- Service Area (SA) list

2 The RNC positively responds to the CN with an ‘SABP: Write-replace Complete’ message.

3,4 The RNC sends a ‘BMC: CBS’ message over the air interface using the Common Traffic Channel (CTCH).This contains:
- Message Id
- Cell broadcast data

© wray castle limited

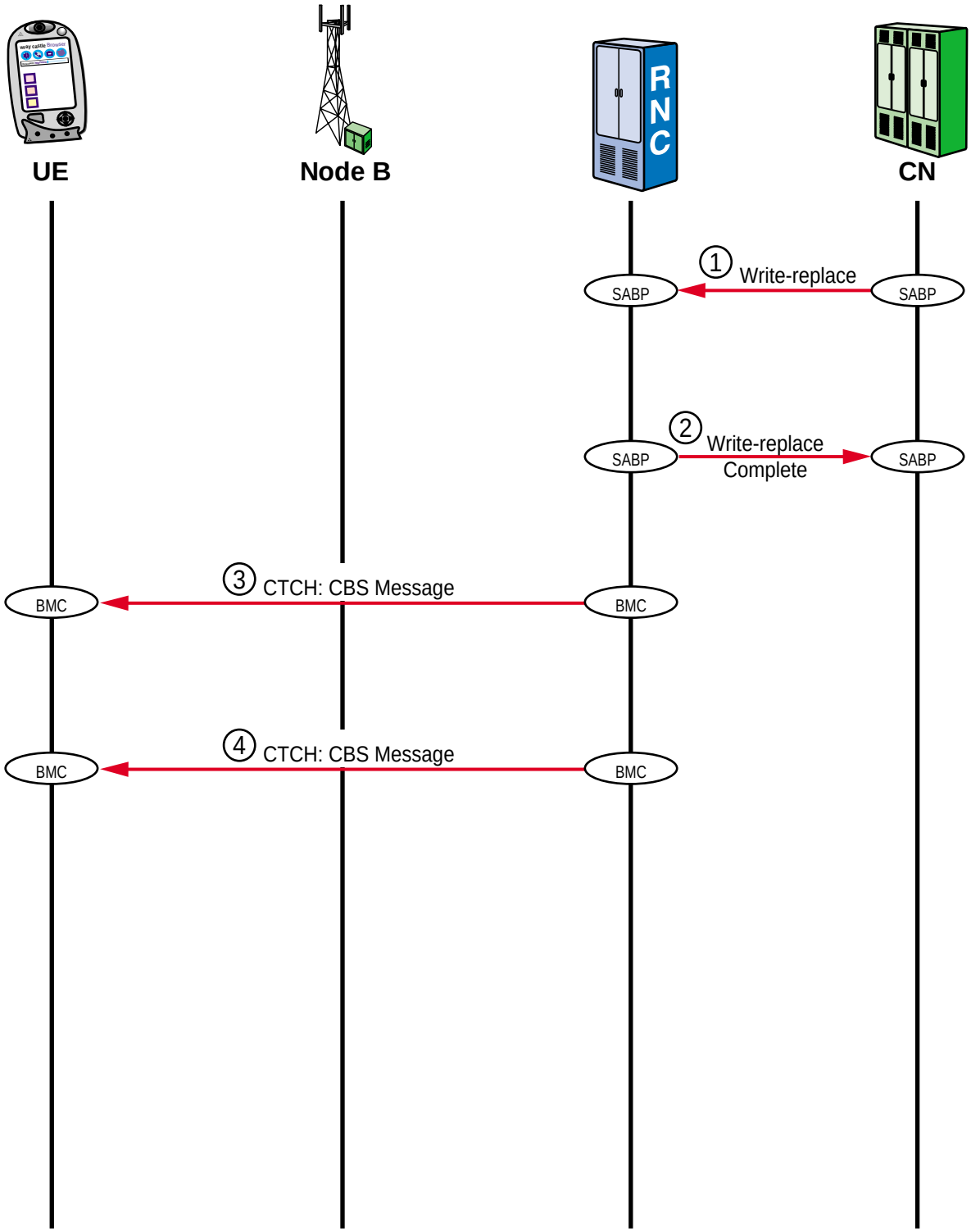


Figure 2
Service Area Broadcast

© wray castle limited

1.4 Paging

This paging procedure is used when the CN or UTRAN wants the UE to connect to the system. The UE could be in Cell-PCH or URA-PCH state.

An example of the paging procedure is shown in Figure 3, and detailed below:

1 The CN sends a ‘RANAP: Paging’ message to the UTRAN. This contains:
- CN Domain Identifier
- Permanent NAS UE Identity
- Temporary UE Identity
- Paging cause

2 The RNC forwards the ‘RRC: Paging Type 1’ message to all cells concerned.

Upon receiving the paging message from the UTRAN, the UE will respond.

© wray castle limited

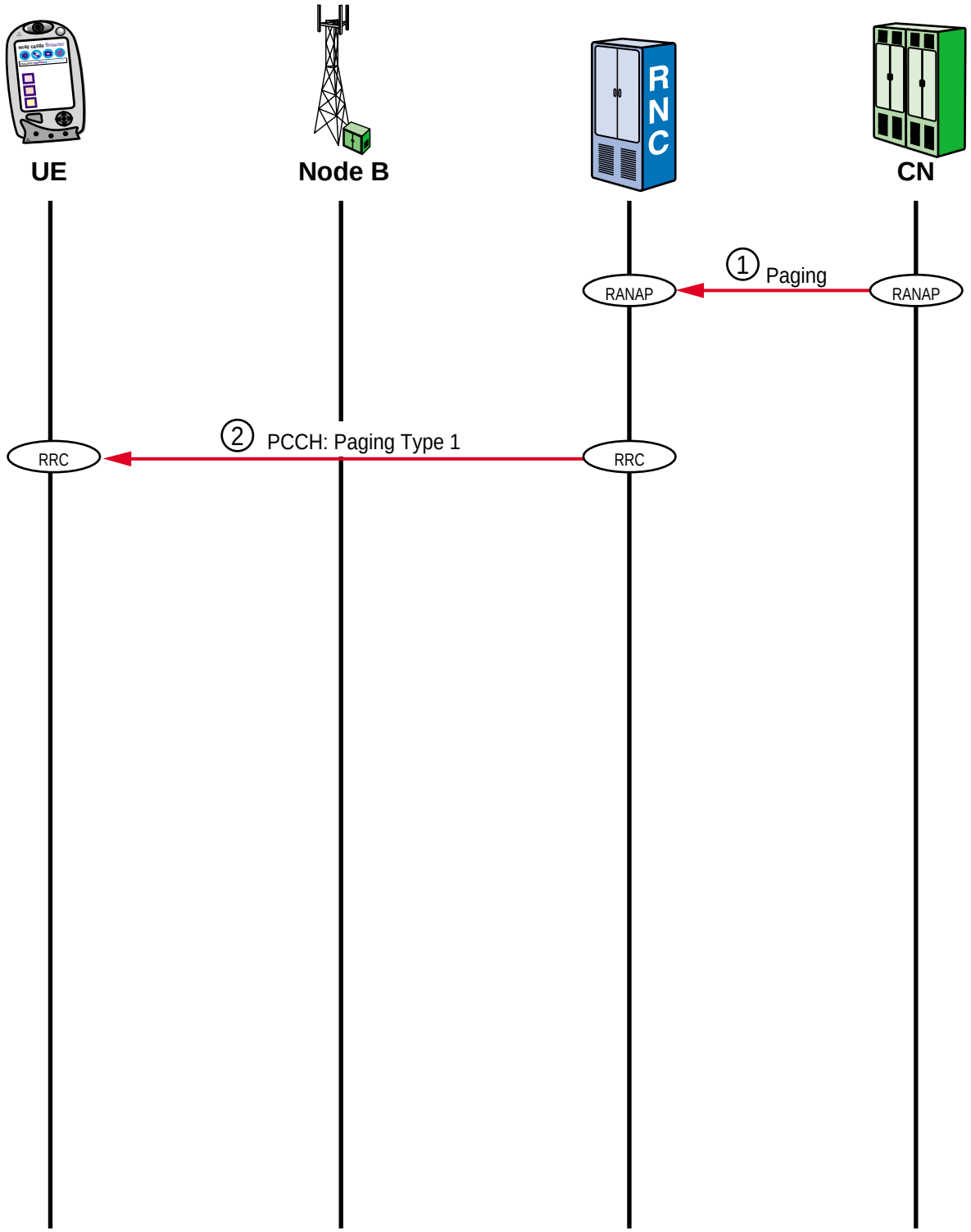


Figure 3
Paging for a UE in RRC Idle Mode

© wray castle limited

2 CONNECTED MODE PROCEDURES

2.1 General Concepts

Connected mode is entered when an RRC connection is established. This will need to be achieved for any prolonged exchange of information, signalling or traffic, with the system. The establishment of an RRC connection will involve the allocation of a Radio Network Temporary Identifier (RNTI), which facilitates the exchange of signalling messages between UE and the system.

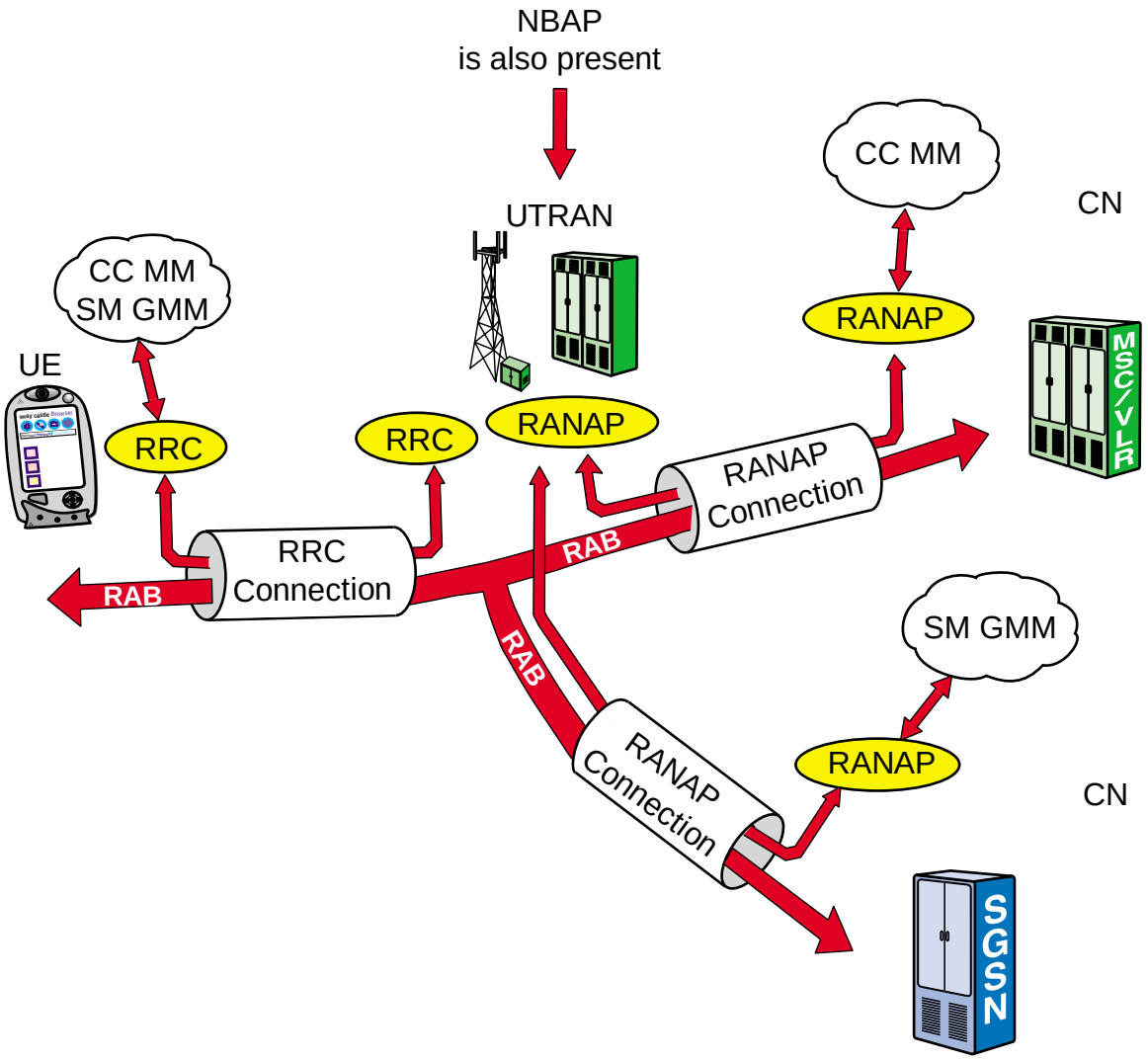
2.2 Communication between UE and the CN

The RRC connection is established to carry signalling between the UE and the RNC. Higher-layer signalling to or from the UE carried in this RRC connection will also need to be transported between the RNC and the appropriate CN node. This connection is implemented by the RANAP protocol that exists on the Iu interface. Separate RANAP connections are required for the CS and PS domains in the CN. However, PS- and CS-related signalling can share a single RRC connection. Refer to Figure 4.

2.3 Radio Bearer Provision

In order that user traffic can be transferred, a RAB must be established between the UE and the CN. The requirements of the RAB will vary, i.e. CS or PS, QoS, data rate. In all cases it must be able to transfer user data through the UTRAN. The establishment of the RAB is also handled by RRC and RANAP, as shown in Figure 4.

© wray castle limited



CC – Call Control
MM – Mobility Management
SM – Session Management

Figure 4
Linking the UE and the CN

© wray castle limited

2.4 RRC Connection

The RRC Establishment procedure moves the UE into the RRC connected state. This procedure can also be used to allocate a dedicated channel if required. Figure 5 shows an example of an RRC Connection Establishment. This example procedure includes the setting up of a dedicated channel.

1 The ‘RRC: RRC Connection Request’ message is transported to the RNC in a Common Control Channel (CCCH). This message includes:
- Initial UE identity
- Establishment cause
- Initial UE capability

2 The SRNC allocates a RNTI and decides if a DCH is required. If so, the ‘NBAP: Radio Link Set-up Request’ is sent to the required Node Bs.
- Transaction identity
- UL and DL physical channel information
- DCH information
- Radio link information
- CRNC context identifier

3 The Node B allocates resources, starts receiving over the air interface, and responds to the RNC with a ‘NBAP: Radio Link Set-up Response’.
- Transaction identity
- CRNC and Node B context identifier
- Radio link response information

4,5 The RNC initiates the set-up of the transport bearer using the ‘ALCAP: Establishment Request’ message. This contains an AAL2 address, Binding ID, AAL2 Path ID, Signalling ID and Channel Identifier to be set up. The Node B sends an ‘ALCAP: Establishment Confirm’ message as an acknowledgement.

6,7 The Node B and the RNC get synchronized using the Dedicated Channel Frame Protocol (DCH-FP). DCH-FP uses ‘DL Synchronization’ and ‘UL Synchronization’ frames to establish synchronization. The Node B starts DL transmission.

© wray castle limited

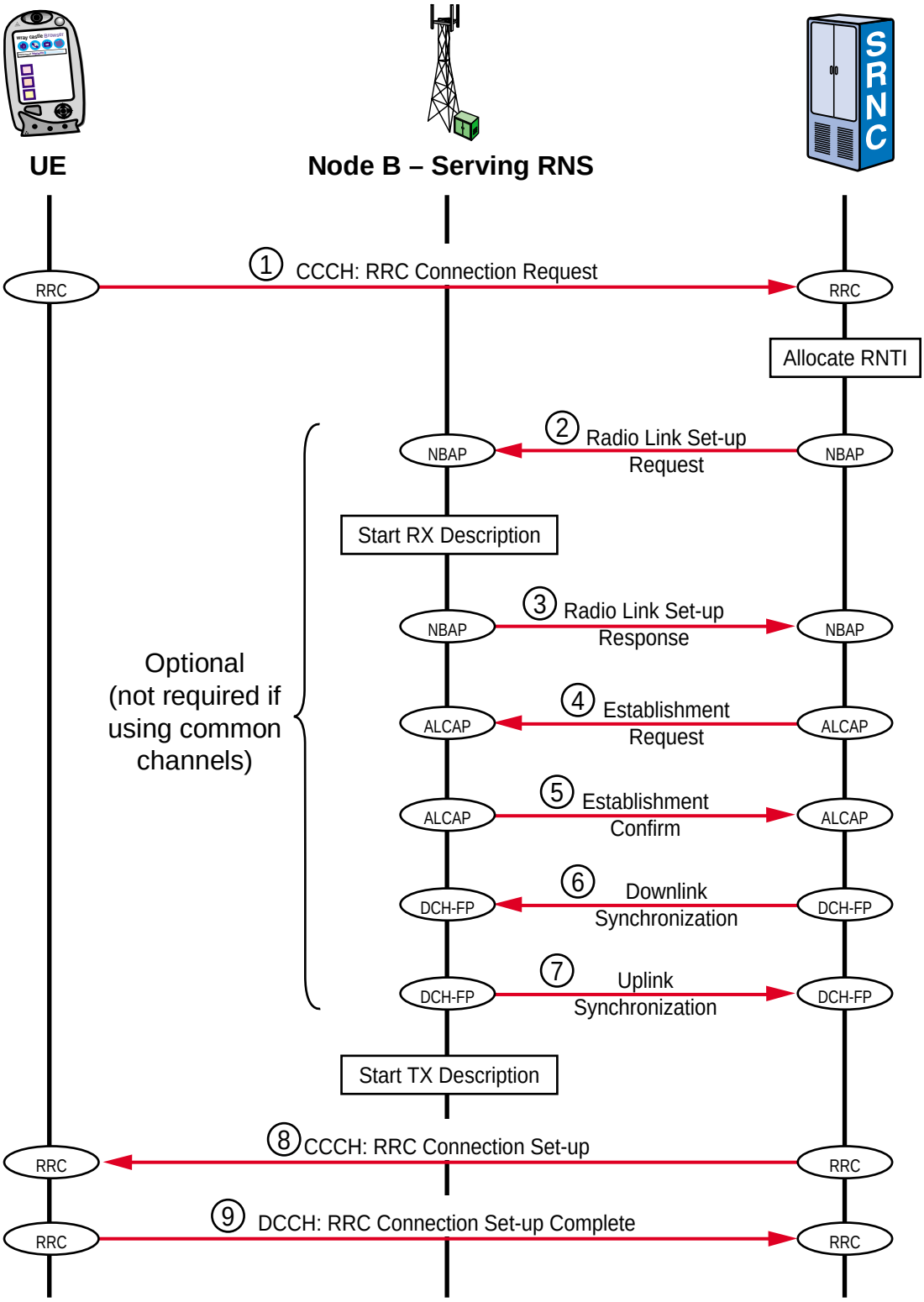


Figure 5

RRC Connection Establishment – DCH Establishment

© wray castle limited

8 The RNC sends the ‘RRC: RRC Connection Set-up’ on the CCCH to the mobile.
- Initial UE Identity
- UTRAN RNTI (u-RNTI). Optionally includes Cell RNTI (c-RNTI)
- Capability update required
- Radio bearer information
- UL and DL transport channel information
- UL and DL physical channel information

9 The message ‘RRC: RRC Connection Set-up Complete’ is sent on the Dedicated Control Channel (DCCH) from the UE to the RNC.
- CN domain identity
- UE radio access capability (o)
- UE system specific capability (o)

© wray castle limited

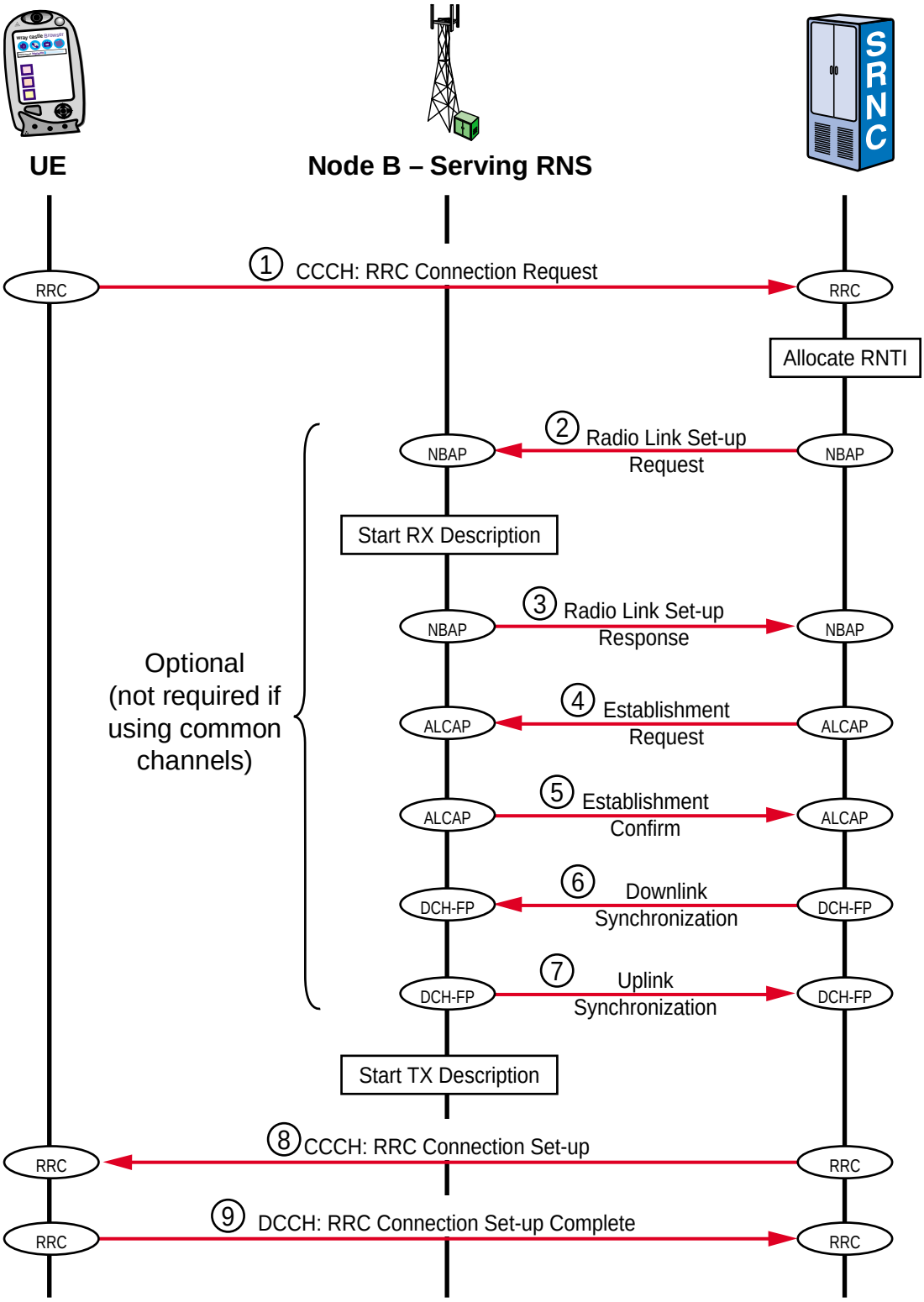


Figure 5 (repeated)
RRC Connection Establishment – DCH Establishment

© wray castle limited

2.5 NAS Signalling Transfer

An RRC connection must be established before NAS signalling can be transferred across the UTRAN.

1 An RRC connection is established (see RRC establishment procedure).

2 The first NAS signalling message from the UE will be transported in an ‘RRC: Initial Direct Transfer’ message. This contains:
- Initial NAS message
- CN Domain identifier
- Service descriptor
- Flow identifier

3 The SRNC initiates a connection-oriented signalling procedure towards the CN. The ‘RANAP: Initial UE Message’ transports the NAS message to the correct CN node.
- Initial NAS message
- CN Domain identifier
- Signalling connection identifier
- RNC Id

4 ‘RANAP: Direct Transfer’ message is used for subsequent transfer of NAS messages across the Iu interface.
- NAS message

5 ‘RRC: DL Direct Transfer’ message is sent on the DCCH to the UE.
- CN Domain identifier
- NAS message

6 ‘RRC: UL Direct Transfer’ message is sent on the DCCH to the SRNC.
- NAS message

7 ‘RANAP: Direct Transfer’ message is used for subsequent transfer of NAS messages across the Iu interface.
- NAS message

© wray castle limited

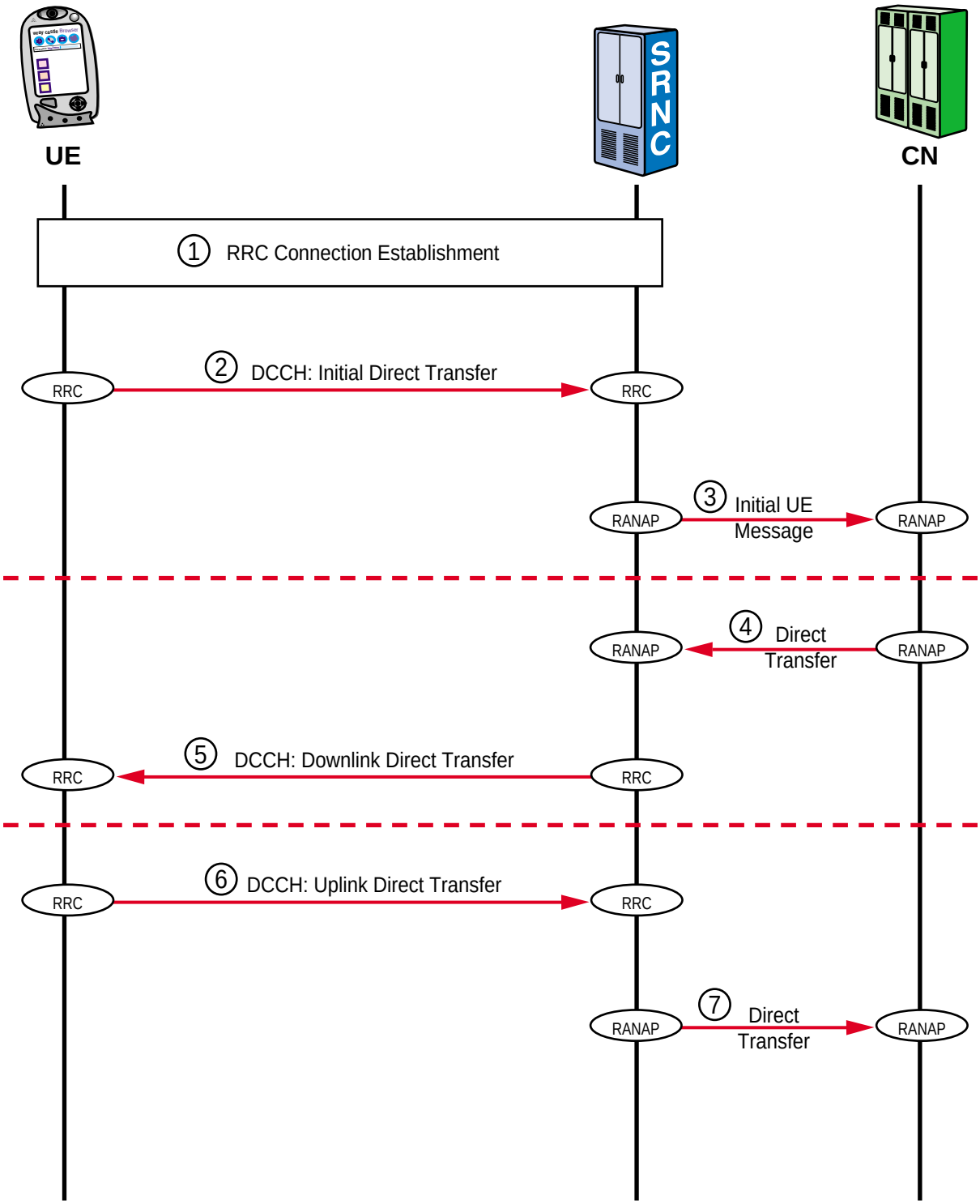


Figure 6
NAS Signalling Connection Establishment

© wray castle limited

2.6 RAB Establishment

If there is a requirement to transfer user data, a RAB needs to be set up. This procedure sets up the transport bearer on the required interfaces.

1 The CN initiates the procedure by sending ‘RANAP: RAB Assignment Request’ message to the SRNC.
   - RAB parameters (including RAB identifiers)
   - User Plane information

2 ‘NBAP: Radio Link Set-up Request’ enables SRNC to request the Node B to establish a new DCH in the existing radio link.
   - Transaction identity
   - UL and DL physical channel information
   - DCH information
   - Radio link information
   - CRNC context identifier

3 ‘NBAP: Radio Link Set-up Response’ informs the SRNC that the Node B has allocated resources.
   - Transaction identity
   - CRNC and Node B context identifier
   - Radio link response information

4 ALCAP establishes the Iub Data Transport Bearer

5 ALCAP establishes the Iu Data Transport Bearer

6 The SRNC sends an ‘RRC: Radio Bearer Set-up’ message to the UE. This identifies the bearer details.
   - New u-RNTI/c-RNTI (o)
   - CN information
   - UTRAN mobility information
   - Radio bearer information
   - UL and DL transport channel information
   - UL and DL physical channel information

7 The UE sends ‘RRC: Radio Bearer Set-up Complete’ message to the SRNC.
   - Integrity information
   - ciphering information

8 ‘RANAP: RAB Assignment Response’ message is sent from the SRNC to the CN.
   - RAB parameters (RAB identifier)

© wray castle limited

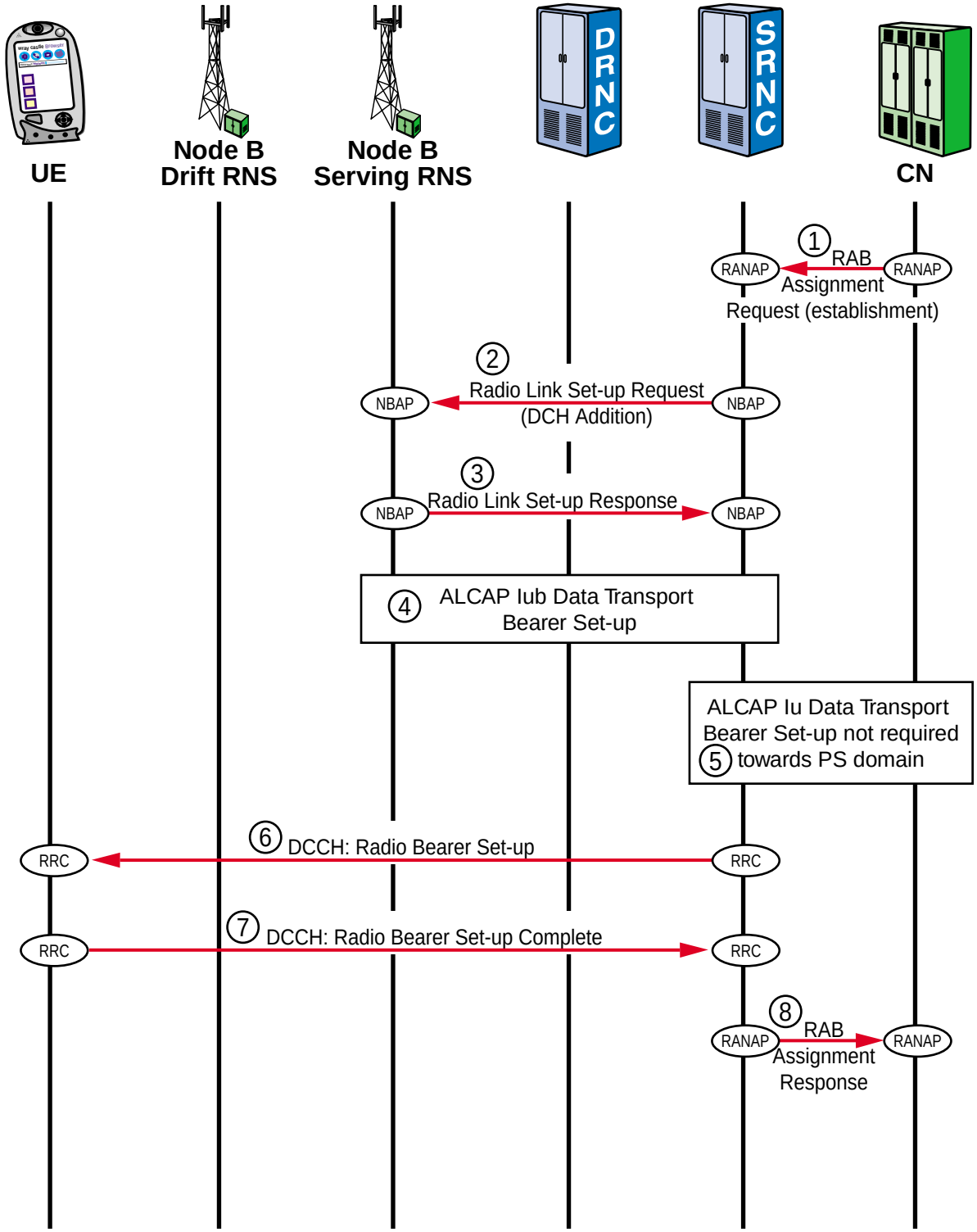


Figure 7

RAB Establishment – RACH/FACH – DCH Establishment – Unsynchronized

© wray castle limited

2.7 Radio Access Bearer (RAB) Release

The CN is able to release the RAB without releasing the RRC connection.

1 The CN sends ‘RANAP: RAB Assignment Request’ message to the SRNC indicating the release of a RAB.
   - RAB ID
   - Cause

2 Upon receiving the ‘RRC: Radio Bearer Release’ message, the UE releases the RAB.
   - RAB to be released

3 ‘RRC: Radio Bearer Release Complete’ is received by the SRNC. The SRNC can now release the resources on the Iub and Iur (if applicable).

4 The SRNC sends ‘RANAP: RAB Assignment Response’ message to the CN.
   - RAB ID

5 The Iu Data Transport Bearer can now be released by ALCAP. This uses the ‘ALCAP Release Request’ and ‘Release Confirm’ messages.
   - Cause
   - Signalling ID

6 In this example, the radio link on the Iub interface needs to be released. To do this the SRNC sends ‘NBAP: RL Reconfiguration Request’ to the Node B.
   - Transaction identifier
   - Node B context identifier
   - Radio link information (including RAB identifier)
   - DCH information

7 The Node B will respond with ‘NBAP: RL Reconfiguration Response’.
   - Transaction identifier
   - CRNC context identifier
   - Radio link information

8 Finally, to complete the procedure, ALCAP will release the Iub Data Transport Bearer. This uses the ‘ALCAP Release Request’ and ‘Release Confirm’ messages.
   - Cause
   - Signalling ID

© wray castle limited

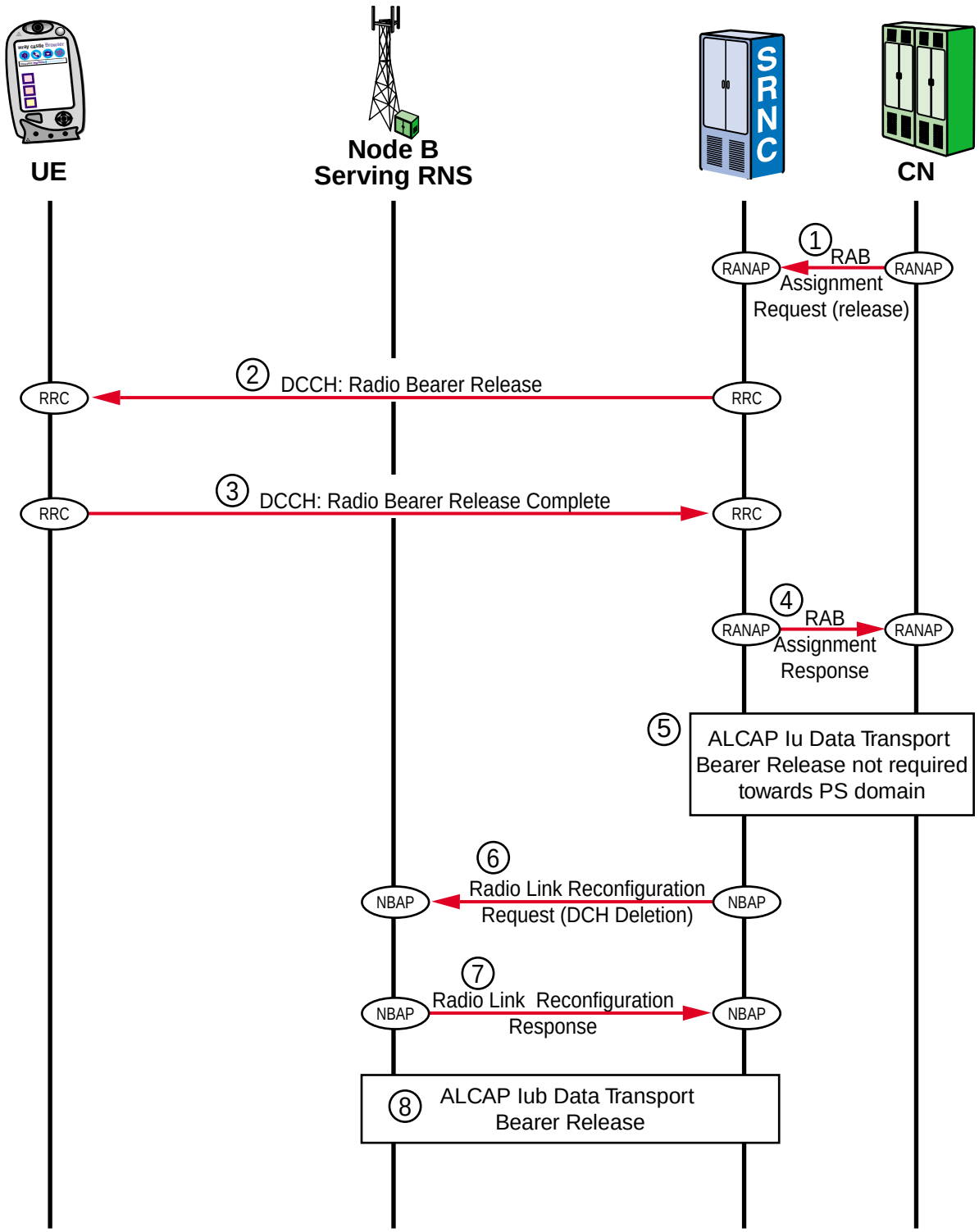


Figure 8

RAB Release – DCH – DCH Release – Unsynchronized

© wray castle limited

2.8 RRC Connection Release

The CN is able to release dedicated channels which may trigger the release of the RRC connection.

1 The ‘RANAP: Iu Release Command’ message is sent to the SRNC.
   - Cause

2 The SRNC acknowledges the CN by sending a ‘RANAP: Iu Release Complete’ message.
   - RAB data volume report
   - RABs released

3 The ALCAP protocol is used to release the Iu Data Transport bearer.

4 The ‘RRC: Connection Release’ message is sent from the SRNC to the UE. This initiates the RRC connection release.
   - Cause
   - u-RNTI (CCCH)

5 The UE responds with a ‘RRC Connection Release Complete’ message to confirm the RRC connection release.
   - u-RNTI (CCCH)

6 The SRNC sends the ‘NBAP: Radio Link Deletion’ to initiate the release of the link.
   - Radio link information
   - Transaction ID
   - Node B context identifier

7 The ‘NBAP: Radio Link Deletion Response’ confirms the release of the link.
   - Transaction ID
   - CRNC context identifier

8 ALCAP releases the Iub Data Transport bearer.

© wray castle limited

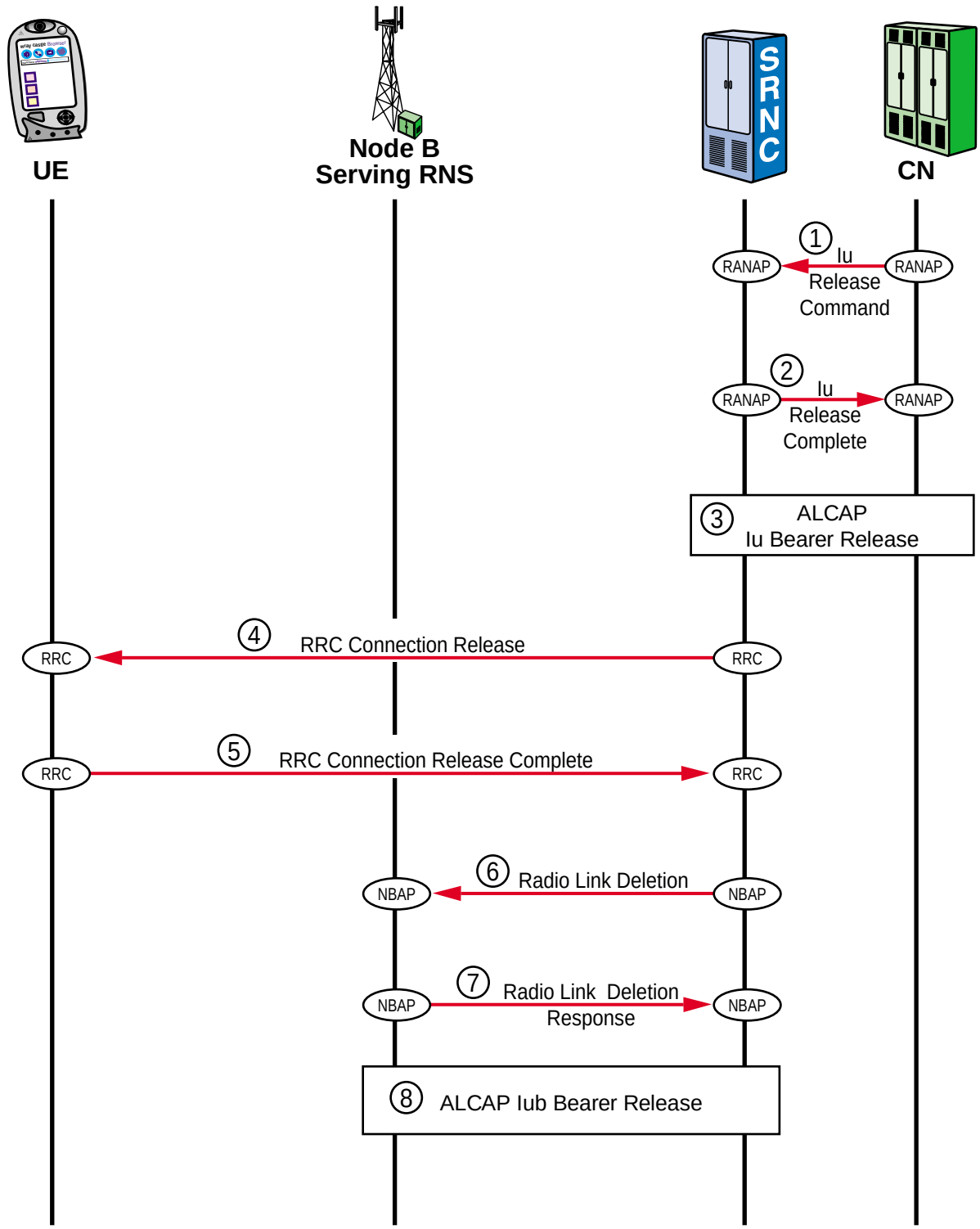


Figure 9

RRC Connection Release of a Dedicated Channel

© wray castle limited

3 HANDOVERS

3.1 Introduction

As with any cellular system, calls must be maintained while the UE travels from one cell area to another. This mobility is provided for by the inclusion of handover procedures. There are three broad categories for handover types specified for UMTS:

- intra-frequency, soft handover
- inter-frequency, hard handover
- inter-system, hard handover

The process of soft handover is related to the need for power control, itself related to interference control. It will occur when the UE enters a new cell and, as it does so, remains on the same cell layer. In this case it will use the same frequency with different DL codes on the new cell.

Hard handovers will generally occur when a UE is handed from one cell layer to another within UMTS. Hard handovers are also used when handing a UE from a UMTS cell to another technology, probably GSM, and vice versa.

3.2 Controlling Elements

UMTS handovers of all types are managed by the RNC within the UTRAN. UMTS uses the principle of Mobile Assisted Handovers (MAHO), i.e. the UE provides measurement information about the serving cell and potential target cells, which is used by the RNC in the handover decision. Essentially there are two elements to this decision, the requirement for a handover, and the type of handover.

The measurements taken will consist of quality measurements of the neighbour cells indicated for measurement to the UE by the RNC. These may be intra-frequency or inter-frequency with respect to UMTS neighbour cells. However, the neighbour cell list may include GSM cells; these measurements will be for signal strength and will need mapping functions similar to those used in cell reselection for the RNC to make a balanced quality judgement.

As well as the measurement process, handovers may be linked to service level. Thus the UE could be handed over as a result of a higher service requirement than can be provided on the current serving cell. The most likely result of this would be a handover between UMTS cell layers. It is also possible that a handover could take place for a particular UE in order to facilitate a service requirement for another UE, possibly even another UE in another cell. Again it will fall to the RNC handover algorithms to make decisions resulting in such a resource reallocation.

© wray castle limited

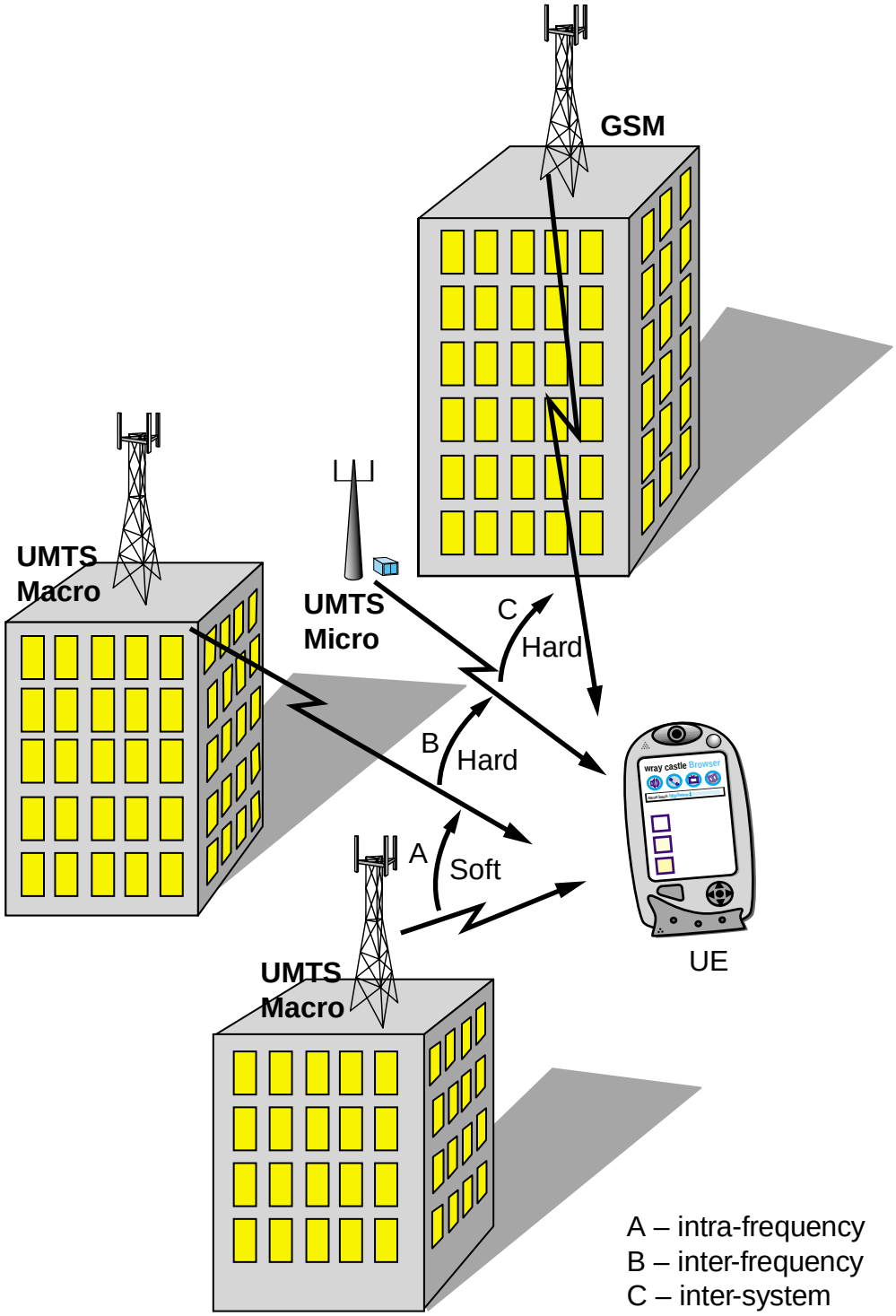


Figure 10
UMTS Handover Types

© wray castle limited

3.3 Soft Handover

A soft handover occurs when the UE is handed to a new cell on the same radio carrier as the current cell. When this happens, the new cell is added to a list of active cells before the current cell is removed. Thus during the soft handover the UE is communicating in both UL and DL directions with more than one cell. Any cell with which the UE is communicating is considered part of the active set. This active set could consist of one, two or more cells, and the state of soft handover could be maintained for long periods of time.

The soft handover could be considered in three phases:

- start of the soft handover
- maintenance of the soft handover
- end of the soft handover

3.4 Macro and Micro Diversity

As with any cellular system, sectorization will be used at base station sites. It is therefore the case that most Node Bs will contain more than one cell. If a soft handover takes place between two cells belonging to the same Node B, i.e. cells on the same site, it is considered to represent micro diversity. The UL and DL can be split and combined within the Node B. This is often referred to as a ‘softer handover’.

If the soft handover takes place between cells belonging to different Node Bs, then it is considered to represent macro diversity. In this case, UL and DL splitting and recombination will occur at the SRNC. If the cells are from Node Bs which themselves belong to different RNCs, then one RNC assumes the role of SRNC and one assumes the role of Drift RNC (DRNC). The DRNC will relay the UL and DL traffic and signalling between the UE and the SRNC via the Iur interface.

© wray castle limited

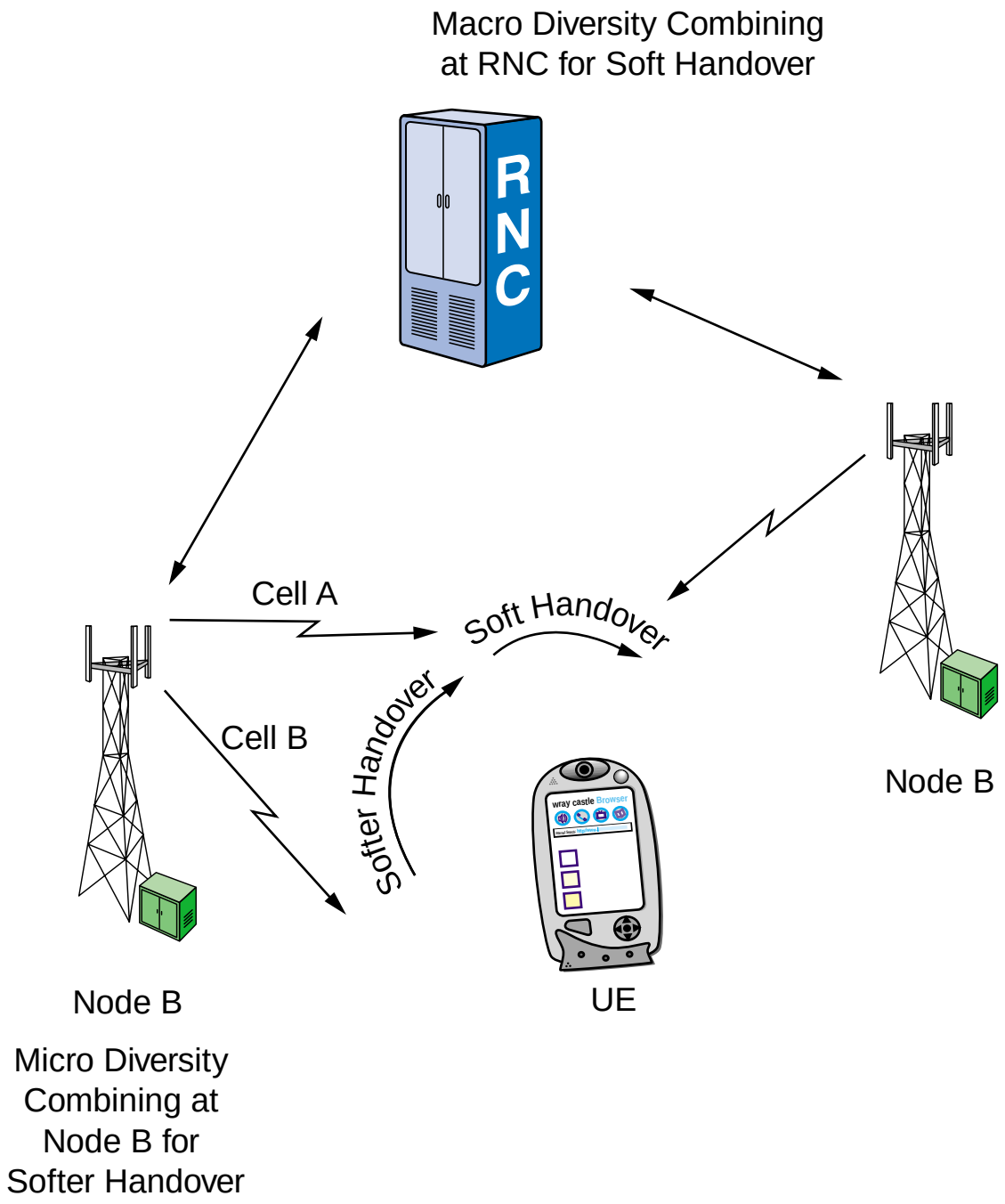


Figure 11
Macro and Micro Diversity

© wray castle limited

3.5 Example of a Soft Handover

Refer to Figure 12.

The example is simplified for clarity and involves a UE monitoring three Node Bs. The diagram shows the relative quality levels of the Node Bs' Common Pilot Channels (CPICHs) as the UE moves through the system.

Over the period of time shown on the diagram, the UE starts with an active set containing only cell A. In this case it is assumed that the active set is limited to two cells.

1 At this point, the quality measurement for cell B has reached the additional threshold for macro diversity. This is reported to the RNC and, subject to the requirements of access control and the expiry of a wait timer, the UE is sent a handover command. This message instructs the UE to add cell B to the active list and includes the required code and timing information.

2 At this point, the difference between the quality of cell A and cell C has fallen below the replacement hysteresis threshold. This is reported to the RNC and, subject to the requirements of access control and the expiry of a wait timer, the UE is sent a handover command. This time the handover command instructs the UE to remove cell A from the active list and replace it with cell C.

3 At this point, the quality measurement for cell C has fallen below the removal threshold for macro diversity. This is reported to the RNC and if this situation is maintained beyond the expiry of the appropriate timer, a handover command is sent to the UE. This message instructs the UE to remove cell C from the active set, leaving only cell B.

© wray castle limited

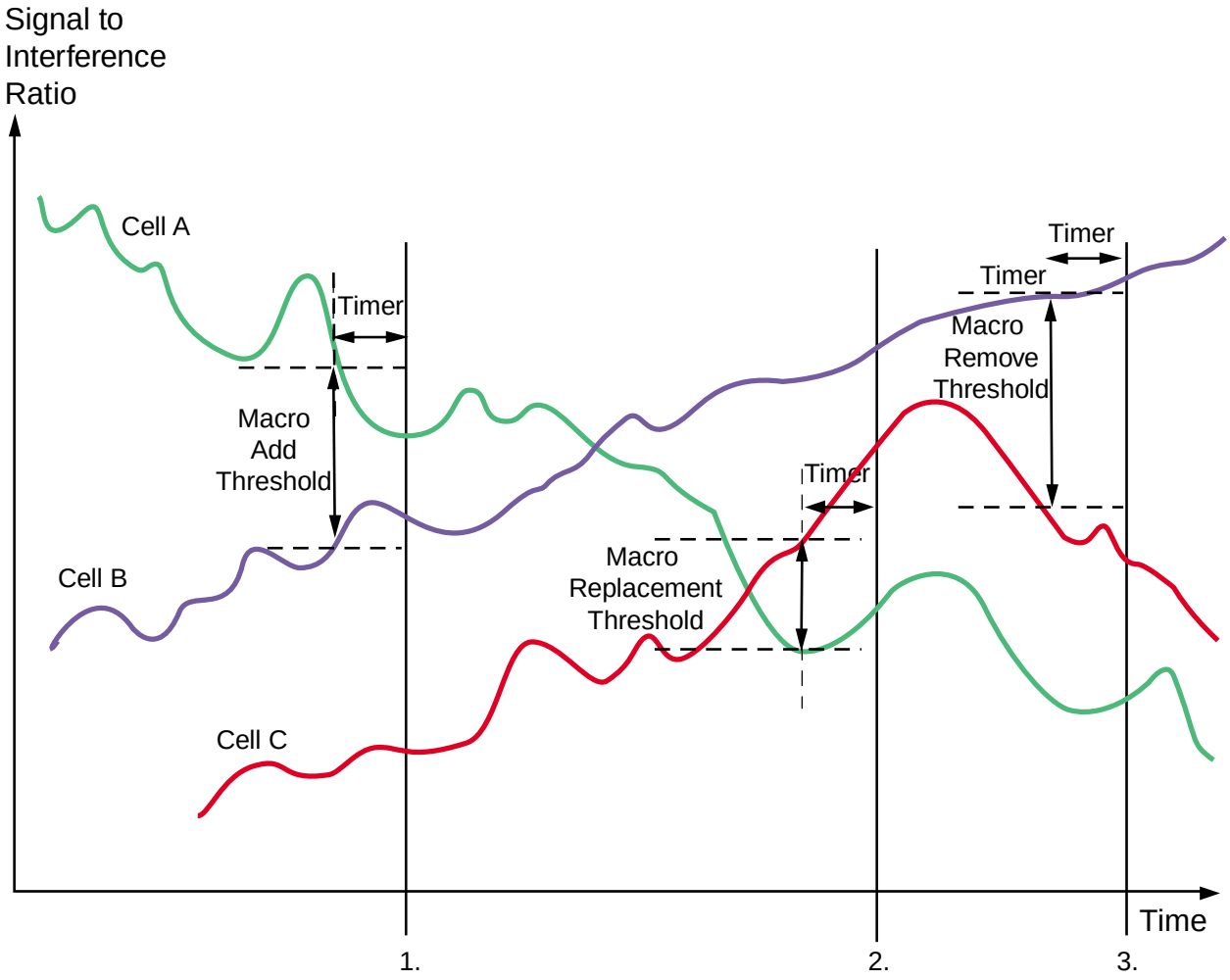


Figure 12
Example of a Soft Handover

© wray castle limited

3.6 Soft Handover – Radio Link Addition

This example details the establishment of a new radio link to a Node B controlled by another RNC (DRNC). The procedure is triggered by the SRNC deciding that a new radio link is required.

1 The SRNC requests the DRNC for resources. ‘RNSAP: Radio Link Addition Request’ is sent across the Iur interface. Since there are no existing radio links, a new signalling connection is required. All RNSAP messages for this UE will use this newly-established Iur signalling connection.
- Radio link information
- Transaction identifier

2 The ‘NBAP: Radio Link Set-up Request’ message is sent to the Node B if resources are available.

3 ‘NBAP: Radio Link Set-up Response’ informs the DRNC that the Node B has allocated resources. The Node B can now start receiving.

4 ‘RNSAP: Radio Link Addition Response’ is sent back to the SRNC.
- Radio link information

5 ALCAP bearers are established on the Iur and Iub interface.

6,7 The Node B and SRNC synchronize using the Dedicated Channel Frame Protocol (DCH-FP). DCH-FP uses ‘DL Synchronization’ and ‘UL Synchronization’ frames to establish synchronization. The Node B starts DL transmission.

8 ‘RRC: Active Set Update’ is sent from the SRNC to the UE.
- Primary CPICH information
- DL DPCH information for each RL

9 The UE acknowledges with ‘RRC: Active Set Update Complete’.

© wray castle limited

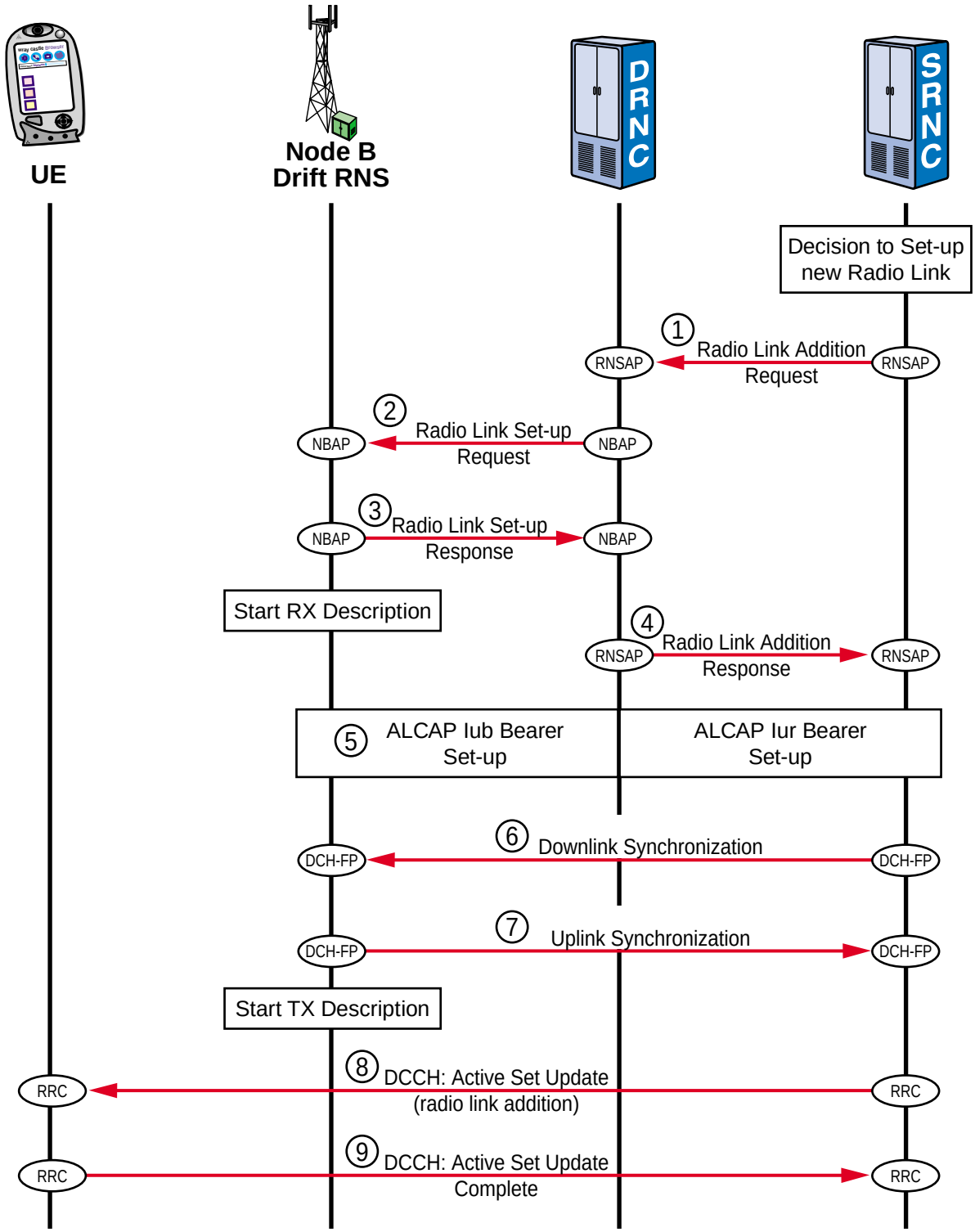


Figure 13

Soft Handover – Radio Link Addition (Branch Addition)

© wray castle limited

3.7 Soft Handover – Radio Link Deletion

This procedure shows the SRNC deciding to delete a radio link on a Node B belonging to a DRNC.

1 SRNC sends ‘RRC: Active Set Update’ message indicating radio link deletion to the UE.
   - Cell ID

2 The UE deactivates DL reception via the old Node B, and acknowledges with an ‘RRC: Active Set Update Complete’ message.

3 SRNC requests the DRNC to deallocate the radio link by sending the ‘RNSAP: Radio Link Deletion Request’ message.
   - RL ID
   - Transaction ID
   - Node B Communication Context ID

4 ‘NBAP: Radio Link Deletion Request’ message is send to Node B from the DRNC.
   - RL ID
   - Transaction ID

5 ‘NBAP: Radio Link Deletion Response’ message will be sent back to the DRNC.
   - Transaction ID

6 DRNC sends ‘RNSAP: Radio Link Deletion Response’ message to SRNC.
   - CRNC Communication Context ID
   - Transaction ID

7 SRNC initiates release of Iur/Iub Data Transport Bearer using the ALCAP protocol.

© wray castle limited

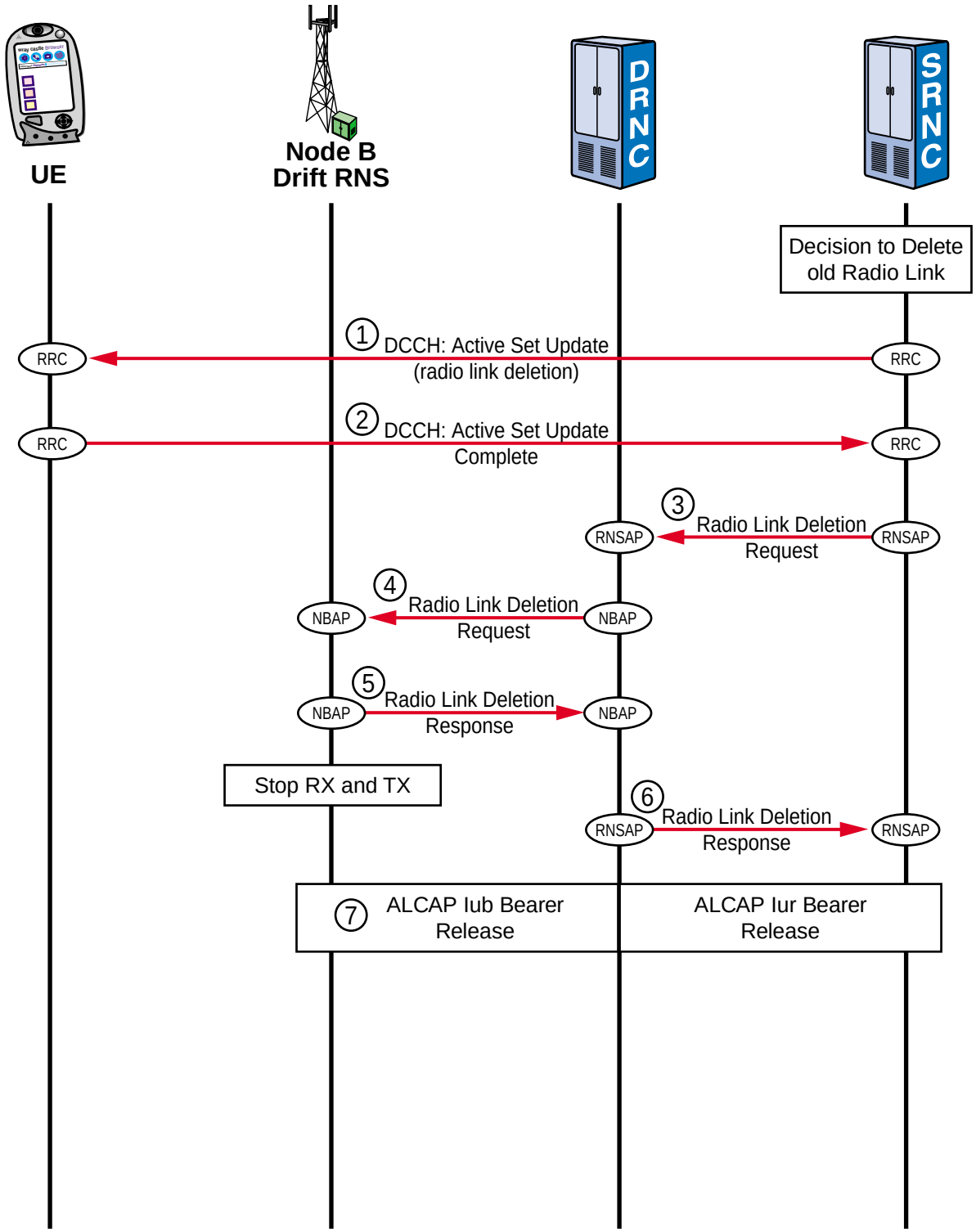


Figure 14

Soft Handover – Radio Link Deletion (Branch Deletion)

© wray castle limited

3.8 RNC Relocation

As the UE moves through the system while maintaining a current connection, it will be passed from cell to cell. The links to the CN are maintained through the SRNC. Relocation takes place when the UE begins to access only via Node Bs belonging to a DRNC.

1 The source RNC sends ‘RANAP: Relocation Required’ messages to the CN. The CN prepares itself for switching and may also suspend traffic and/or signalling.
   - Cause
   - Source/Target ID
   - Transparent Container (source to target) including UE Id

2 The CN sends the ‘RANAP: Relocation Request’ message. This contains information required to build the same RAB configuration as previously existed for the UE before relocation.
   - Cause
   - CN ID
   - Transparent Container (source to target) including UE Id
   - RAB information

3 The target RNC establishes the new ALCAP Iu transport bearers (if CS).

4 When the target RNC has completed its tasks, ‘RANAP: Relocation Request Acknowledge’ message is sent to CN.
   - Transparent Container (target to source)
   - RAB Information

5 The CN sends the ‘RANAP: Relocation Command’ message.
   - Transparent Container (target to source)
   - RABs to be released

6 The source RNC sends a ‘RNSAP: Relocation Commit’ message to target RNC.
   - Transaction Id
   - D-RNTI (optional)

7 The target RNC (which is now the SRNC) sends ‘RANAP: Relocation Complete’ messages to the CN.

8 ‘RANAP: Iu Release Command’ is sent by the CN.
   - Cause

9 ALCAP releases the Iu bearer (if CS)

10 ‘RANAP: Iu Release Complete’ indicates the end of the procedure.

© wray castle limited

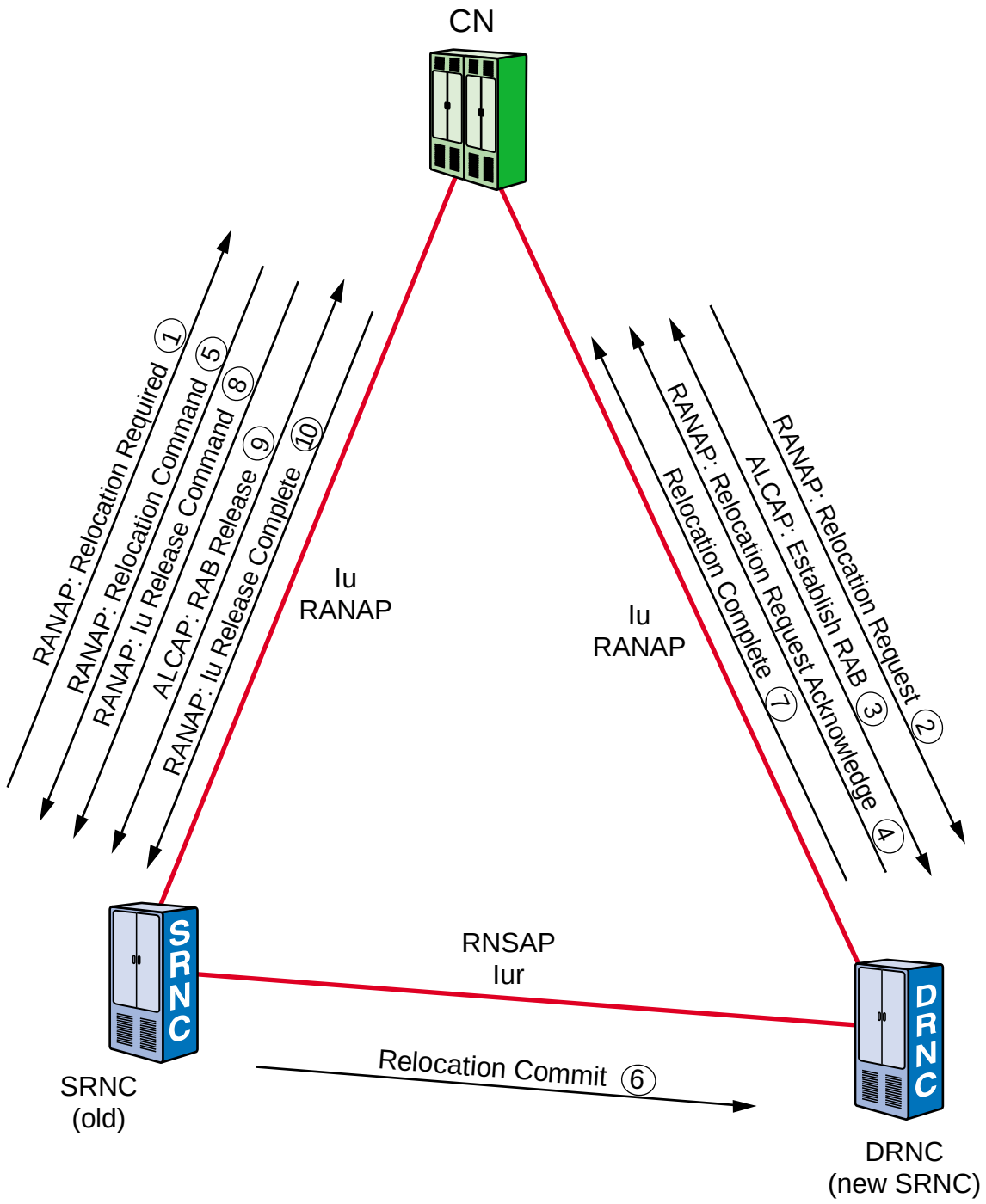


Figure 15
RNC Relocation

© wray castle limited

3.9 Hard Handover

Hard handover initiated by the SRNC is normally performed by the procedure Physical Channel Reconfiguration, but may also be performed by the procedures Radio Bearer Establishment, Radio Bearer Reconfiguration, Radio Bearer Release or Transport Channel Reconfiguration.

1 The RNC sends the ‘NBAP: Radio Link Set-up Request’ message to the target Node B.
   - Cell Id
   - Transport format information
   - Frequency
   - UL scrambling code (FDD only)
   - Timeslots (TDD only), user codes (TDD only)
   - Power control information

2 The Node B allocates resources, starts receiving over the air interface, and responds to the RNC with an ‘NBAP: Radio Link Set-up Response’.
   - Signalling link termination
   - Transport Layer information (AAL2 address, Binding ID)

3 ALCAP bearers are established on the Iub interface.

4 SRNC sends an ‘RRC: Physical Channel Reconfiguration’ message to the UE. This causes the UE to switch to the new radio link.
   - UL and DL information

5 ‘NBAP: Radio Link Failure Indication’ message is sent to the RNC. This indicates that the source Node B has detected a failure.
   - RL ID

6 The UE sends an ‘RRC: Physical Channel Reconfiguration Complete’ message to the SRNC. This indicates that the physical reconfiguration has been done.

7 ‘NBAP: Radio Link Deletion Request’ message is send to the Node B from the RNC.
   - RL ID

8 ‘NBAP: Radio Link Deletion Response’ message will be sent once the Node B has deallocated resources.
   - Transaction ID

9 SRNC initiates release of the Iub Data Transport Bearer using the ALCAP protocol.

© wray castle limited

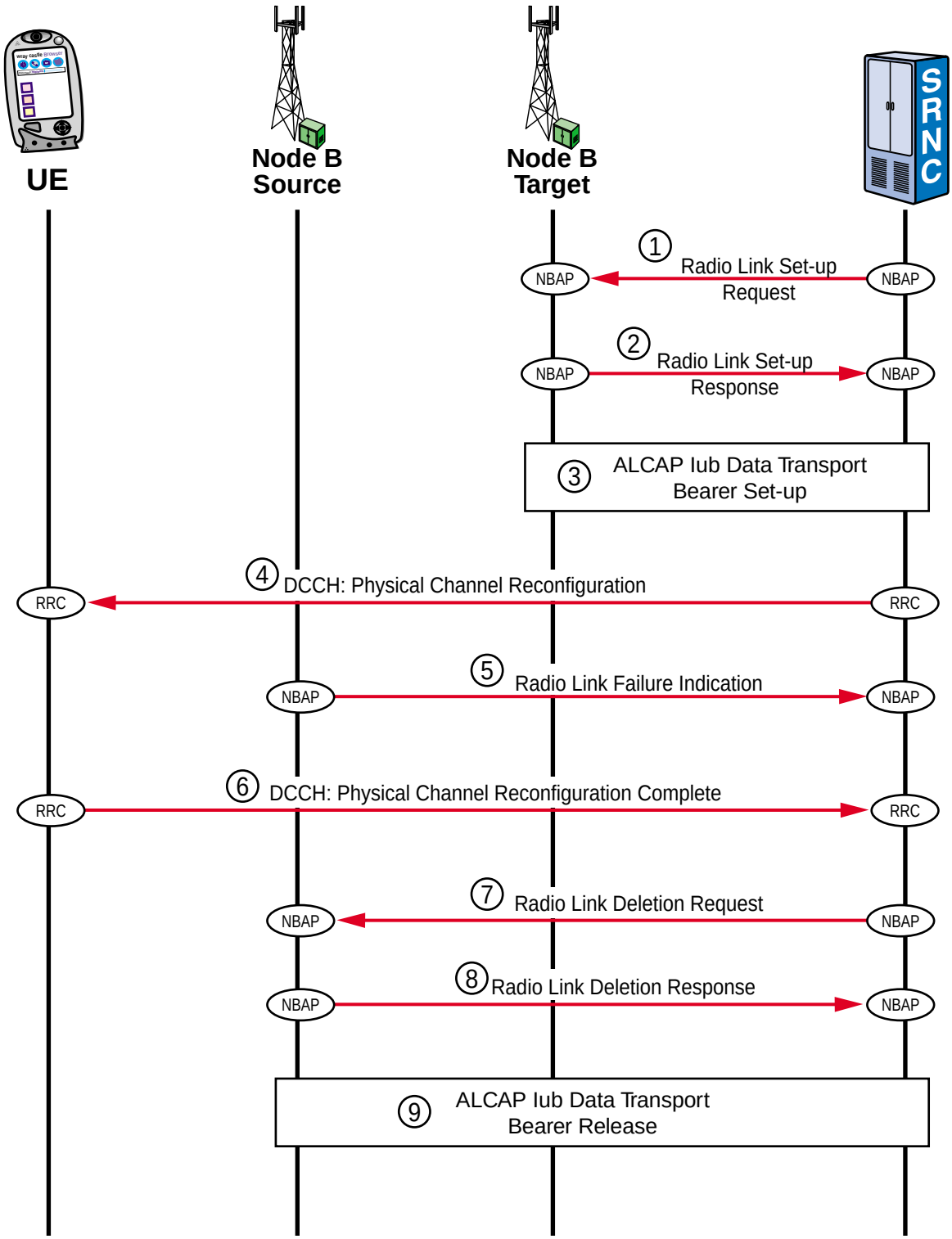


Figure 16
Hard Handover

© wray castle limited

3.10 UTRAN to GSM/BSS Handover

This procedure is used when an UTRAN wants to handover a UE to a GSM network. This procedure deals with a CS connection.

1 The SRNC sends ‘RANAP: Relocation Required’ message to the CN.
- Cause
- Source/Target ID
- Old BSS to new BSS information

2 The UMTS CN Sends the ‘MAP: Prepare Handover’ message to the GSM MSC.
- Target cell
- Old BSS to new BSS information

3 The ‘BSSMAP: Handover Request’ message.
- Serving/Target Cell ID
- Old BSS to new BSS information

4 The ‘BSSMAP: Handover Request Acknowledge’ message.
- Channel type
- Handover command information

5 The GSM/MSC sends the ‘MAP: Prepare Handover Response’.
- Handover command information

6 CN responds to the SRNC by sending ‘RANAP: Relocation Command’ message.
- Handover command information

7 SRNC sends ‘RRC: Inter-System Handover Command’ message to the UE. This causes the UE to change its mode of operation, and access the GSM cell.
- System Type (CDMA2000™, GSM 900, etc.)
- Handover command information

© wray castle limited

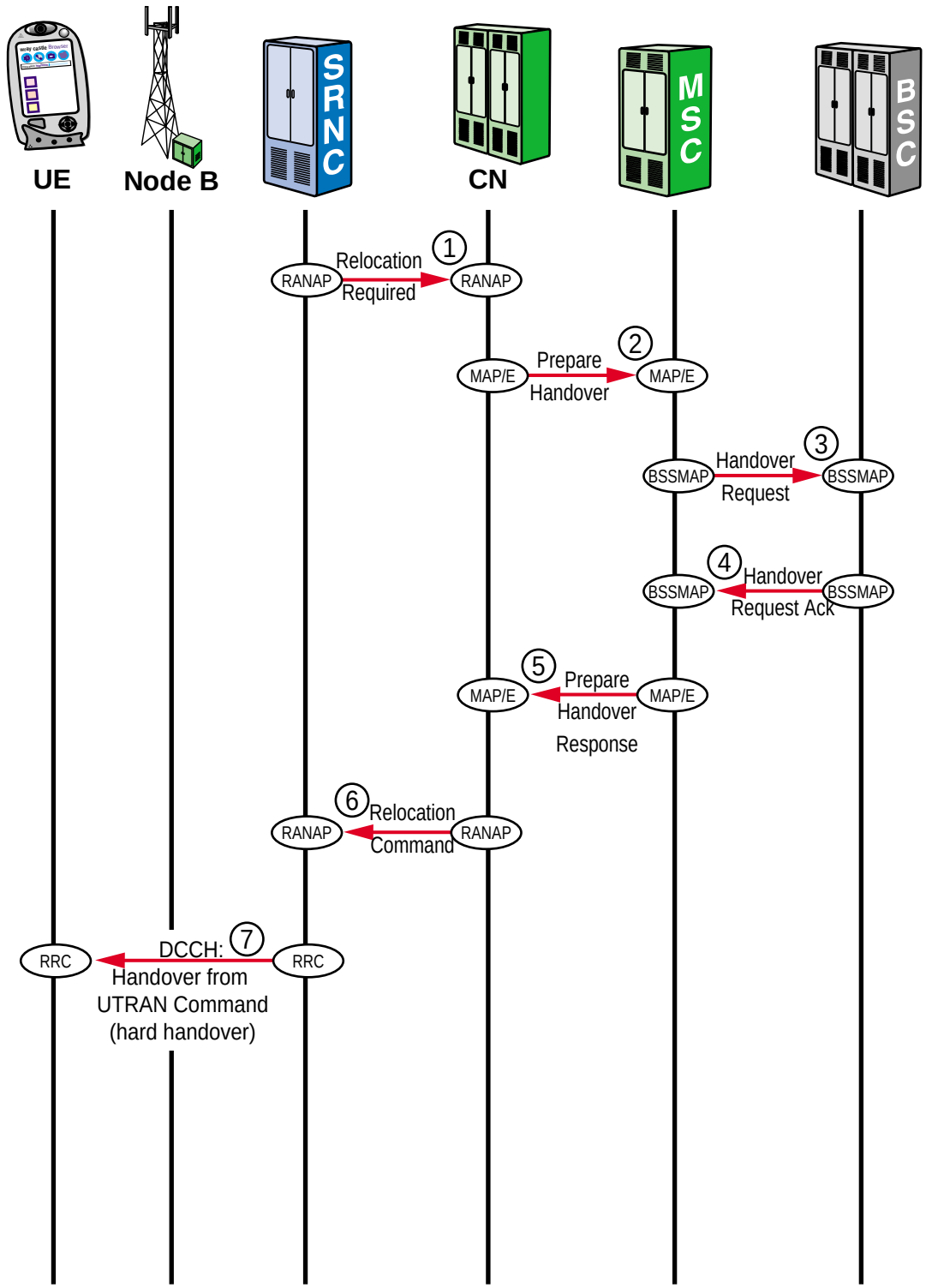


Figure 17
UTRAN to GSM/BSS Handover

© wray castle limited

UE changes mode of operation and accesses the new system.

8 The BSC sends the ‘BSSMAP: Handover Detect’ message when it detects the UE accessing.

9 The ‘RR: Handover Complete’ message is sent when the mobile has established itself on the GSM system.

10 The ‘BSSMAP: Handover Complete’ message is then sent to the GSM/MSC.

11 The GSM system sends the ‘MAP: Send End Signal Request’ message to the UMTS CN.

12 ‘RANAP: Iu Release Command’ is send by the CN. This triggers ALCAP to release the Iu bearer.
- Cause

13 ‘RANAP: Iu Release Complete’ indicates the end of the procedure.

The UMTS CN will maintain control until the call is cleared.

14 The CN sends ‘MAP: Send End Signal Response’ message to conclude this procedure.

© wray castle limited

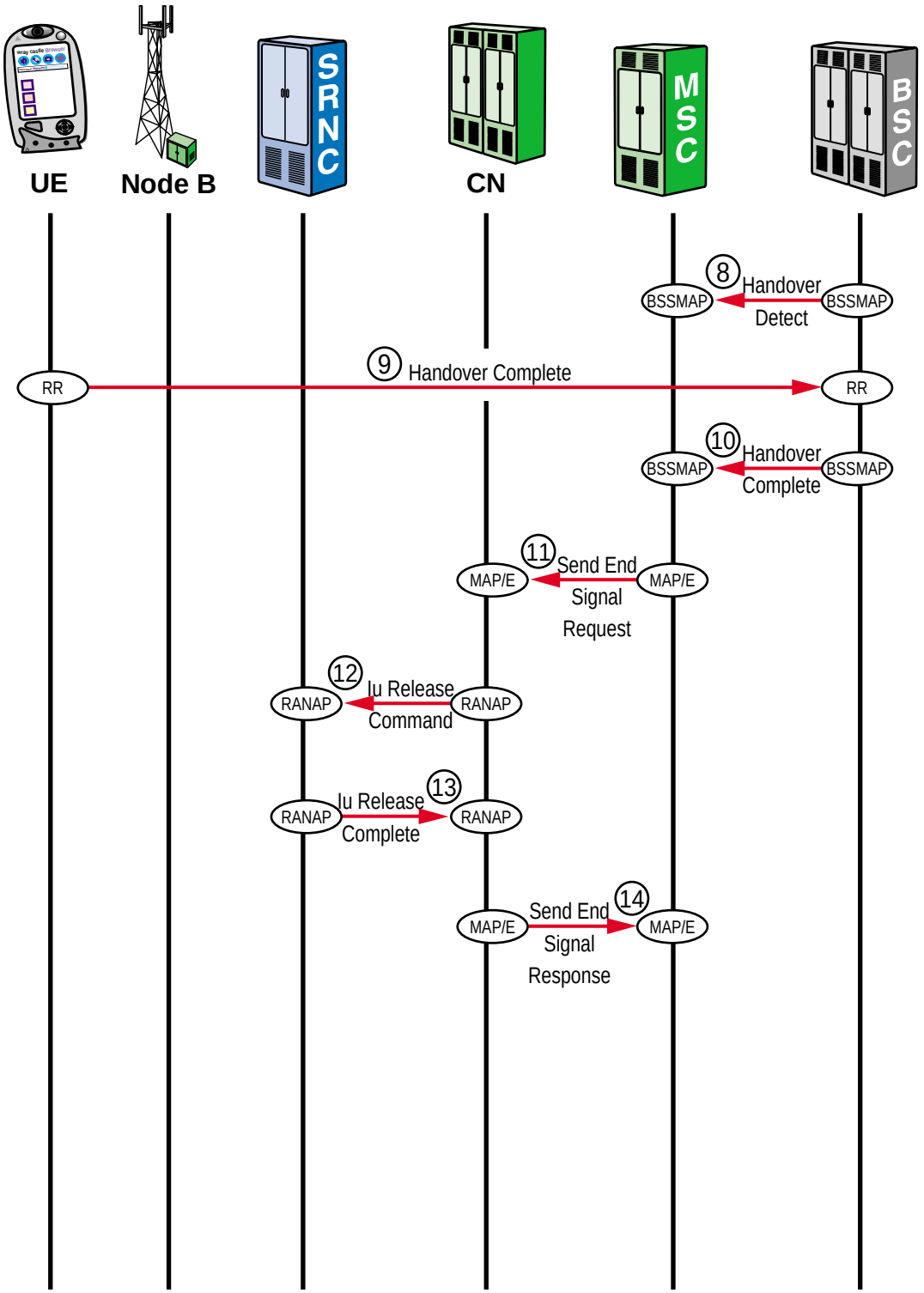


Figure 17 (continued)
UTRAN to GSM/BSS Handover

© wray castle limited

3.11 Cell Update

The purpose of this procedure is to update the UTRAN with the current cell of the UE. This procedure occurs:

- after cell reselection in CELL_FACH or CELL_PCH states
- when transition to the CELL_FACH state prior to transmitting UL data
- for supervision of the RRC connection

The procedure in Figure 18 occurs after cell reselection.

1 After cell reselection, the UE sends an ‘RRC: Cell Update’ message to the UTRAN.
   - u-RNTI
   - Cell update cause

2 The RNC decodes the u-RNTI. In this example, the UE is not registered in the DRNC. This triggers the ‘RNSAP: UL Signalling Transfer Indication’ message to the SRNC.
   - Cell-ID
   - DRNC ID
   - c-RNTI and s-RNTI (optionally d-RNTI)
   - Transaction ID

3 SRNC decides not to perform the relocation procedure. The ‘RNSAP Common Transport Channel Resources Initialization Request’ message is used to initialize the Common Transport Channel User Plane towards the DRNC.
   - d-RNTI
   - Cell-ID

4 The target DRNC sends ‘RNSAP: Common Transport Channel Resources Response’ message.
   - s-RNTI
   - Transport Layer address
   - Binding ID

5 ALCAP establishes the Iur bearer if required.

6 The ‘RRC: Cell Update Confirm’ message is sent to the UE. This is sent over the Iur interface in the User Plane.
   - u-RNTI

7 The ‘RRC: UTRAN Mobility Update Confirm’ message acknowledges the new RNTI.

© wray castle limited

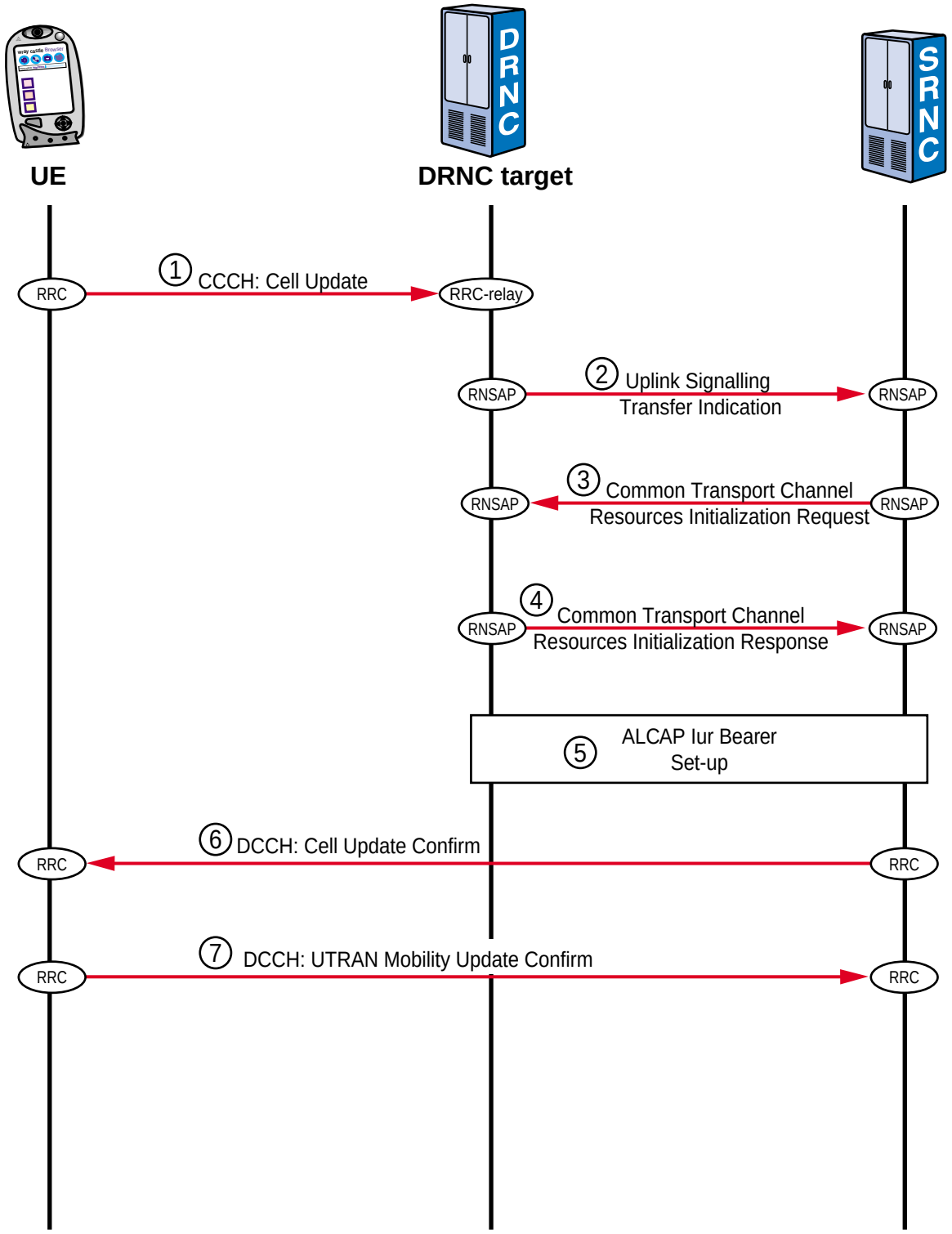


Figure 18

Cell Update via Iur without SRNC Relocation

© wray castle limited

3.12 URA Update

After URA reselection in the URA_PCH state, the URA update procedure sends the UE's current URA to the UTRAN.

1 After cell reselection, the UE sends an 'RRC: URA Update' message to the UTRAN.
   - u-RNTI
   - Cause

2 Target RNC decodes the u-RNTI and forwards the 'RNSAP: UL Signalling Transfer Indication' message to the SRNC.
   - Cell-ID
   - DRNC ID
   - c-RNTI and d-RNTI
   - Transaction ID

3 The SRNC decides not to perform an SRNS relocation procedure. SRNC sends 'RNSAP: DL Signalling Transfer Request'.
   - Transaction ID
   - C-Id
   - d-RNTI
   - L3 information
   - D-RNTI Release Indication

4 The 'RRC: URA Update Confirm' is send to the UE.
   - u-RNTI

© wray castle limited

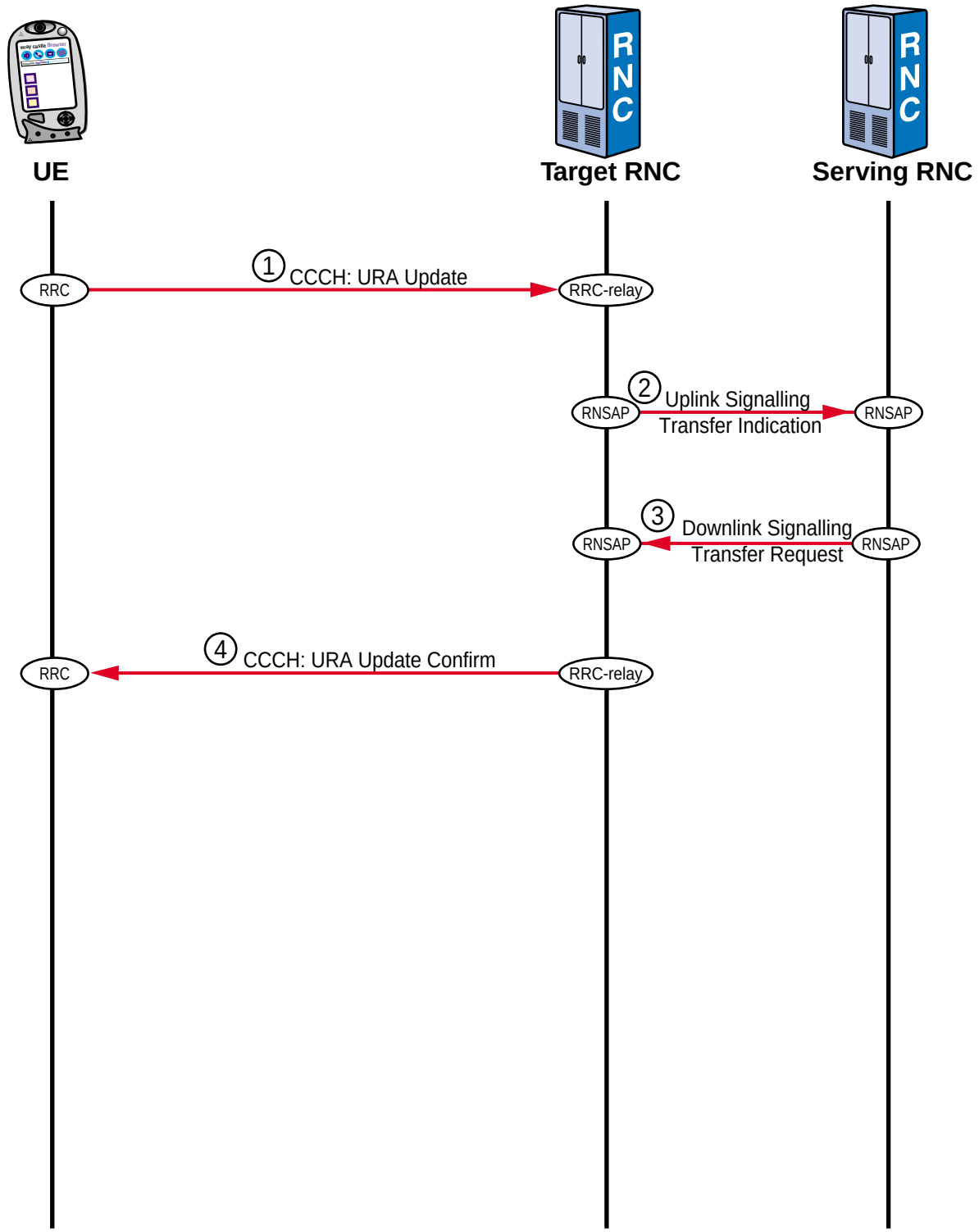


Figure 19
URA Update

© wray castle limited

© wray castle limited

LESSON 2

SECURITY

© wray castle limited

LESSON CONTENTS

1 Security Functions **8.2.1**
1.1 Provision for Security 8.2.1
1.2 User Identity Confidentiality 8.2.3
1.3 Authentication 8.2.5
1.4 Confidentiality 8.2.7
1.5 Data Integrity 8.2.13

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- describe how security procedures are implemented in the UTRAN

1 SECURITY FUNCTIONS

1.1 Provision for Security

Security features have proved to be a critical part of second-generation systems. If the more ambitious services promised for third-generation systems are to be a success, then security for users and for information flows must be provided for.

Network access security is defined for UMTS in terms of five key areas:

- user identity confidentiality
- entity authentication
- confidentiality
- data integrity
- mobile equipment identification

© wray castle limited

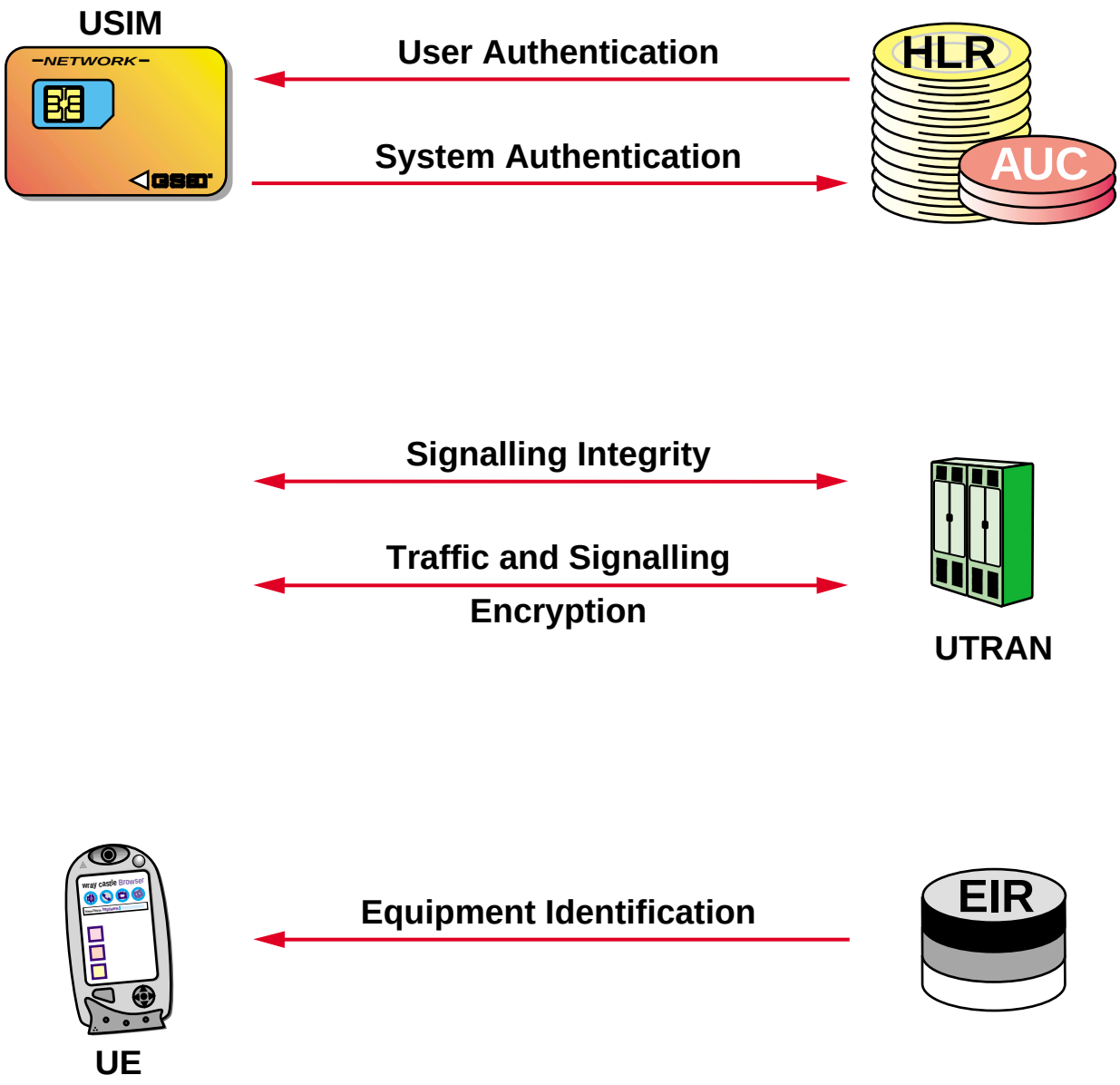


Figure 1
Network Access Security

© wray castle limited

1.2 User Identity Confidentiality

This area of security functions aims to protect a user's identity as they access and use services provided by the system. It should not be possible for an eavesdropper to either capture a user's permanent identity from the air interface, detect the presence or the arrival of a user in a particular area, or deduce whether different services are being delivered to the same user.

The main provision for this type of security is the use of temporary identities. When attached to the CS domain of the CN, the user should be allocated a Temporary Mobile Subscriber Identity (TMSI). When attached to the PS domain of the CN, the user should be allocated a Packet Temporary Mobile Subscriber Identity (P-TMSI). It is possible for a user to possess both TMSI and P-TMSI simultaneously.

To ensure an effective level of security for the use of temporary identities, they should be changed regularly.

In addition, it is recommended that any messages carried over the air interface that could compromise the user's permanent identity are ciphered.

1.2.1 Allocation of TMSI/P-TMSI

Temporary identities are allocated by the CN entities VLR or SGSN and they are applicable within the areas controlled by those entities. Thus a TMSI/P-TMSI has local significance within an LA or an RA in which the user is registered. If the user moves into a new area, the TMSI/P-TMSI is presented to the CN along with the LA or RAI in which it was allocated. This enables the permanent identity of the user to be derived within the CN domain.

© wray castle limited

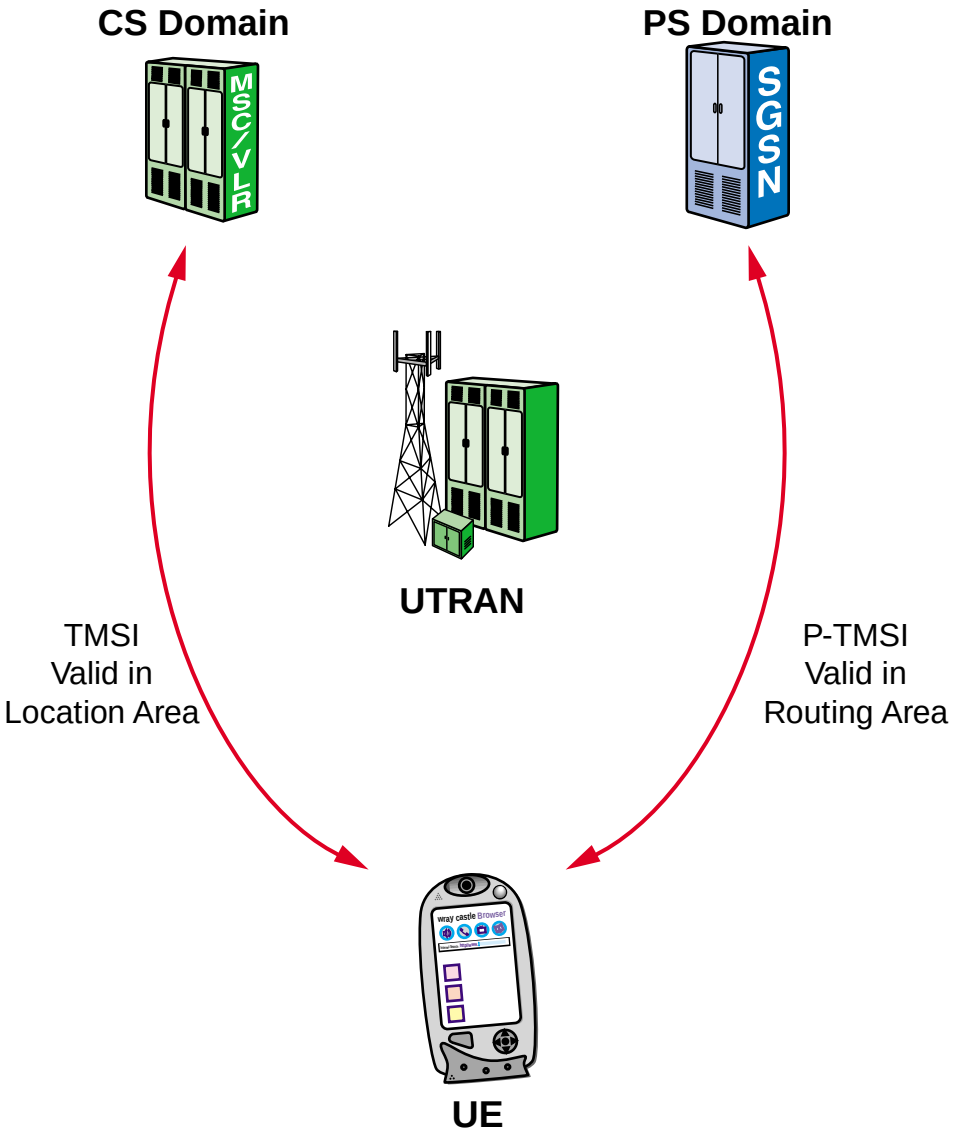


Figure 2
User Identity Confidentiality

© wray castle limited

1.3 Authentication

Authentication has been widely used in second-generation systems, where it has been very successful in the detection and blocking of attack by false users. This is continued in UMTS, but the basic authentication process is supplemented to provide for mutual authentication. Thus potential attack from false base stations is also prevented.

Authentication of users is provided by shared knowledge of secret keys (K) stored on the UMTS Subscriber Identity Module (USIM) and in the Authentication Centre (AUC). The key is verified through the use of authentication algorithms, ensuring that the key is never exposed to an eavesdropper.

Mutual authentication is achieved by the inclusion of sequence counters in the UE and the network. Successful authentication will keep these counters in synchronization. A false base station would not be aware of the correct sequence number.

1.3.1 Authentication Process

The process should be considered in two stages, the distribution to local CN nodes of the Authentication Vectors (AV), and the authentication process itself.

The distribution is initiated by a CN node when it requires AV information for a particular user. The Authentication Data Request message is directed to the AUC in the user's home network. The AUC generates one or more AV. Each AV consists of five authentication-related elements; hence they may be referred to as *Quintets*. The AVs are then passed to the requesting CN node in the Authentication Data Response message, where they are stored until required.

When an authentication is required, the CN node selects one of the stored AVs. Two of the authentication elements, the Random Challenge (RAND) and the Authentication Token (AUTN) are passed over the air interface to the UE. These elements are processed in the USIM: the RAND relates to the generation of the UE's Response (RES) and the AUTN relates to the UE's verification of the network.

If the UE verifies AUTN, then it will compute and return RES. The CN node then compares RES with the Expected Response (XRES), which was supplied as one of the elements in the AV. If the two values are the same, then the authentication is considered successful.

The computations relating to authentication are also used to provide a Cipher Key (CK) and an Integrity Key (IK). These will be computed by the UE and selected from the AV by the CN node as required. The CK and IK values will be passed to the RNC for use, since ciphering and integrity are functions of the UTRAN.

© wray castle limited

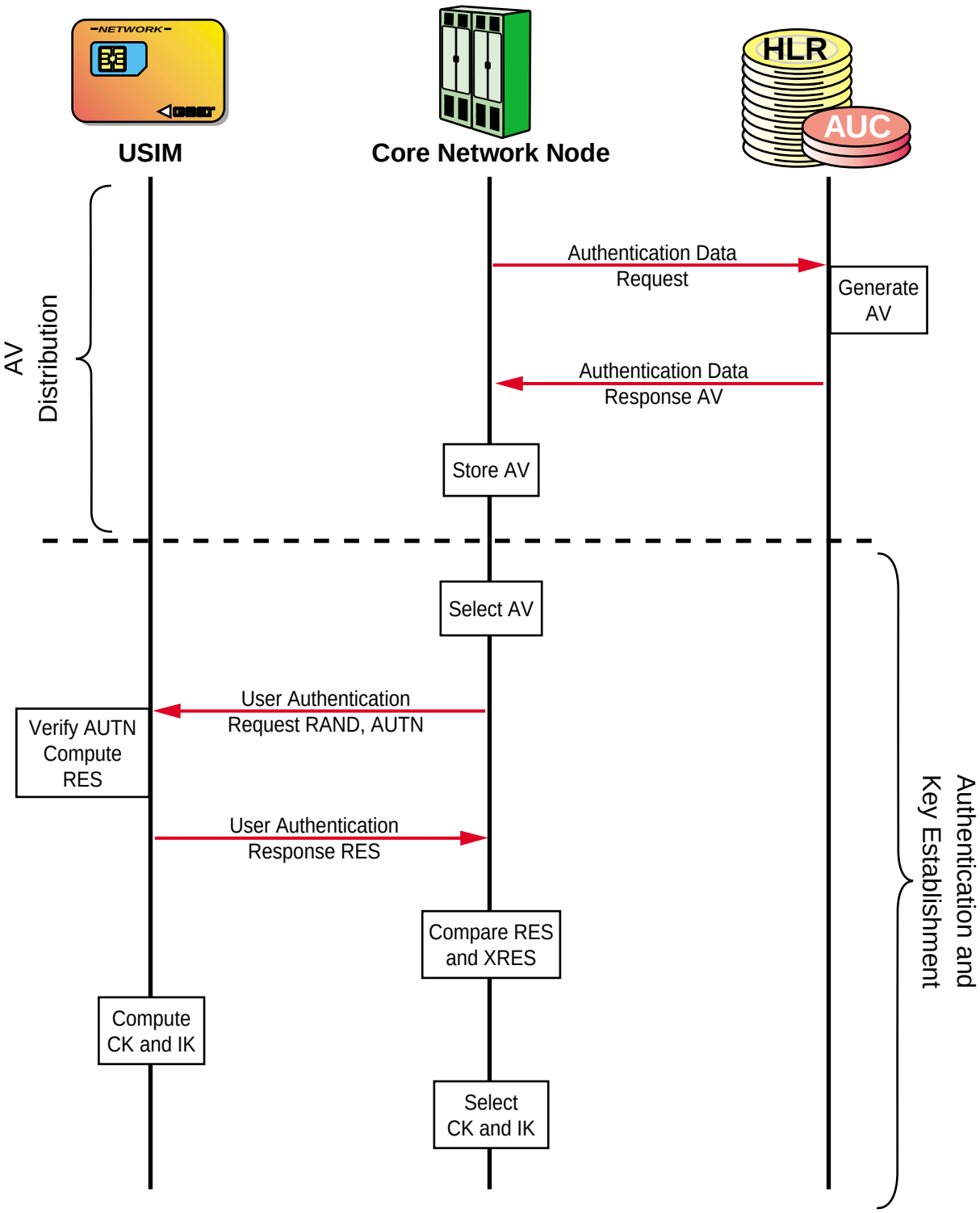


Figure 3
Authentication Process

© wray castle limited

1.4 Confidentiality

The term *confidentiality* refers to the ciphering of signalling and user traffic across the air interface when the UE is in RRC connected mode. The process of ciphering is a function of layer 2 in the air interface protocol stack. Since layer 2 resides in the RNC for all connected mode procedures, ciphering can be considered to protect data between the UE and the RNC, i.e. it includes the Iub interface within the UTRAN.

1.4.1 Implementation of Ciphering

Ciphering is applied independently to each Radio Bearer (RB) that a UE has in place; this includes both signalling and traffic RBs. Ciphering is applied at layer 2, but is dependent on the service provided for a particular RB. It may be implemented in RLC or in MAC.

Ciphering will be applied in the RLC sublayer if the logical channel used by the RB is mapped into a common transport channel, or if the logical channel is using one of the RLC non-transparent modes, Acknowledged Mode (AM) or Unacknowledged Mode (UM).

Ciphering will be applied at the MAC sublayer (MAC-d) if the transparent mode of RLC is being used.

1.4.2 The Keystream Block

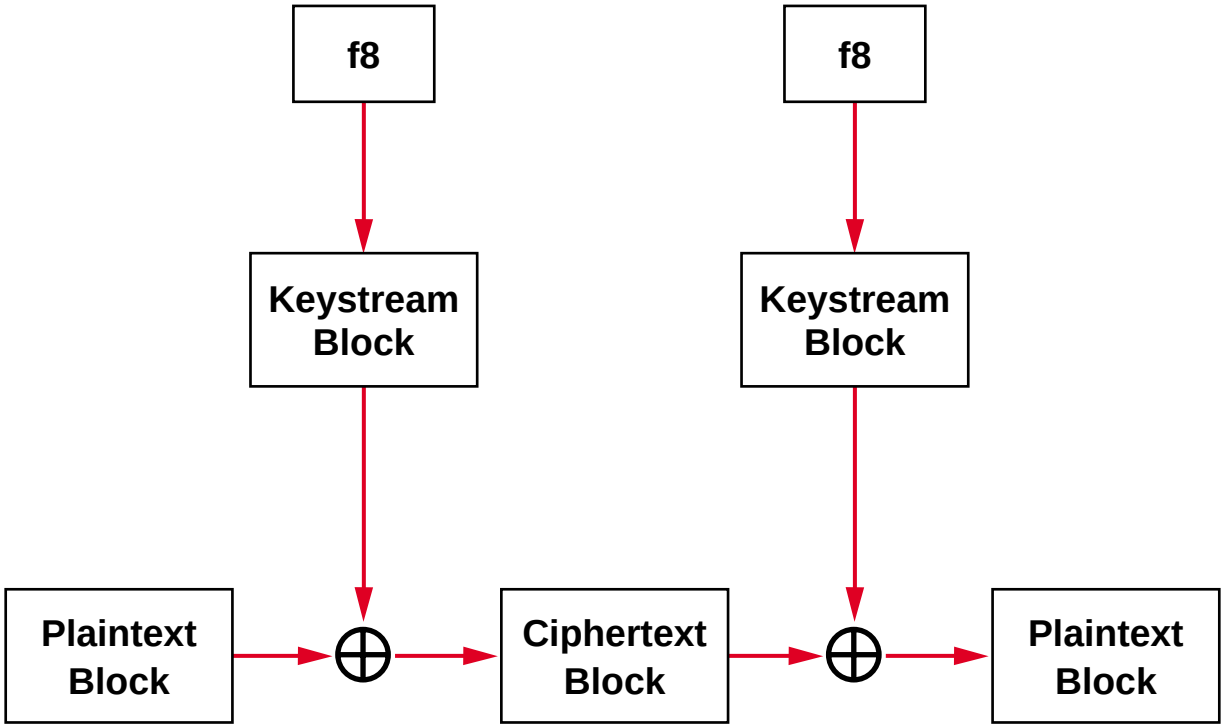
Data streams to be ciphered are divided into blocks known as *plaintext* blocks and each one is ciphered by binary addition to a correspondingly-sized *keystream* block. The keystream block is generated by the ciphering algorithm f8, and a new keystream block is generated for each consecutive plaintext block.

The size of the plaintext block will depend on the type and rate of the RB being ciphered. The length will correspond to the payload of RLC Packet Data Units (PDUs) or MAC Service Data Units (SDUs) to be carried in one 10 ms radio frame. The inputs to the f8 ciphering algorithm are such that they can be adjusted to ensure that keystream blocks are produced at a rate and length corresponding to the plaintext blocks.

The sum of a plaintext block and a keystream block is known as a *ciphertext* block; it is the ciphertext block that is carried between the UE and the RNC.

At the receiving end, the f8 algorithm is again used to produce a corresponding keystream block, which is combined with the incoming ciphertext block by binary addition. Thus the plaintext block is recovered.

© wray castle limited



RLC PDUs or MAC SDUs mapped to 10 ms radio frame.

Figure 4
The Keystream Block

© wray castle limited

1.4.3 Inputs to the Ciphering Algorithm f8

The f8 algorithm is implemented in the UE and the RNC. There are five input values to the f8 algorithm:

Cipher Key (CK) (128 bits)
The CK is generated as part of the authentication process; it will be passed to the RNC by the CN node and passed to the UE from the USIM.

COUNT-C (32 bits)
The value COUNT-C is time-dependent and will be incremented simultaneously in the UE and the RNC. When ciphering is being performed in the MAC sublayer, COUNT-C is incremented with the Frame Number (FN). When ciphering is being performed in the RLC sublayer, COUNT-C is incremented with the RLC Sequence Number (SN).

BEARER (5 bits)
The value BEARER indicates the RB number that is being ciphered. This means that independent RBs being used by one UE will have different ciphering applied even though they all use the same CK.

DIRECTION (1 bit)
The value DIRECTION is a single bit used to differentiate between the ciphering applied in the UL and DL.

LENGTH (16)
The value LENGTH is used to set the length of the keystream block to match that of the plaintext block. It does not get included in the f8 computation; it only determines the length of the keystream block, not its content.

© wray castle limited

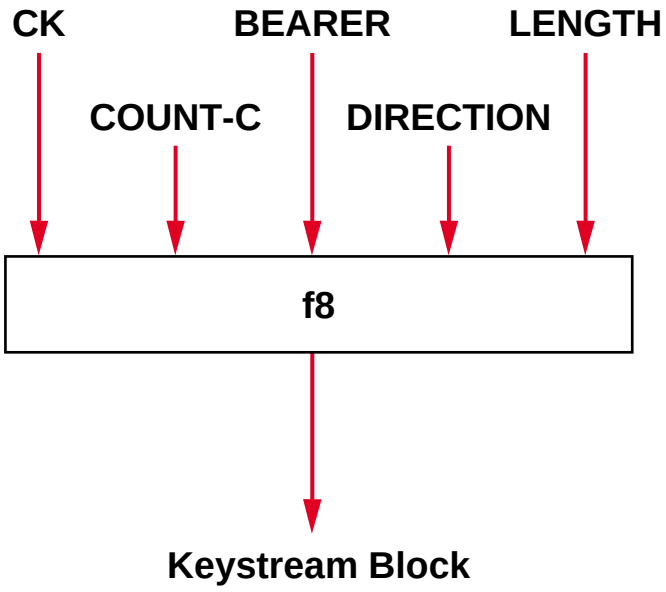


Figure 5
Inputs to f8 Algorithm

© wray castle limited

1.4.4 Starting Ciphering

In order that ciphering is successful, it is necessary for the RNC and the UE to use the same f8 input values at the same time. This requires some negotiation between the UE and the RNC before ciphering can be started. Figure 6 outlines this process.

1 At RRC connection establishment, the UE will indicate its security capabilities and start values for COUNT-C initialization (and COUNT-I for data integrity). The security capabilities inform the system which encryption and integrity algorithms it can support; i.e. there will be more than one version of f8 available. The 32-bit COUNT-C parameter is divided into a short and a long section, the long section being the UE's RLC or MAC HyperFrame Number (HFN). The short part is either the MAC Cipher Frame Number (CFN) or the RLC Sequence Number (SN). At the start of ciphering, initial values for CFN or SN will be set at zero, but the UE must supply starting values for the HFN. It is this that is supplied at RRC connection establishment.

2 When the UE transfers the initial layer 3 message (CM Service Request, Location Update, etc.), it will contain the user identity and the last Key Set Identifier (KSI). The KSI indicates a set of CK and IK that may already be stored in the CN node from a previous authentication. It is likely that the next operation will be authentication, and if this is the case a new set of keys will be generated and a new KSI allocated.

3 The CN node initiates the ciphering process by sending the 'Security Mode Command' message to the SRNC. This message contains the allowed set of algorithms for ciphering and for data integrity. It also contains CK and IK to be used by the SRNC.

4 The SRNC stores the CK and IK to be used and initiates ciphering with the UE by sending the 'RRC Security Mode Command' message to the UE. This message informs the UE about the CN domain and the key set and ciphering algorithm to use. This and subsequent messages will be protected by data integrity, so it also contains parameters that relate to the starting of data integrity.

5 The UE implements ciphering and data integrity using the indicated parameters and responds with the 'RRC Security Mode Complete' message. The SRNC checks this message for integrity and then indicates a successful start to both integrity and ciphering with the 'Security Mode Complete' message.

© wray castle limited

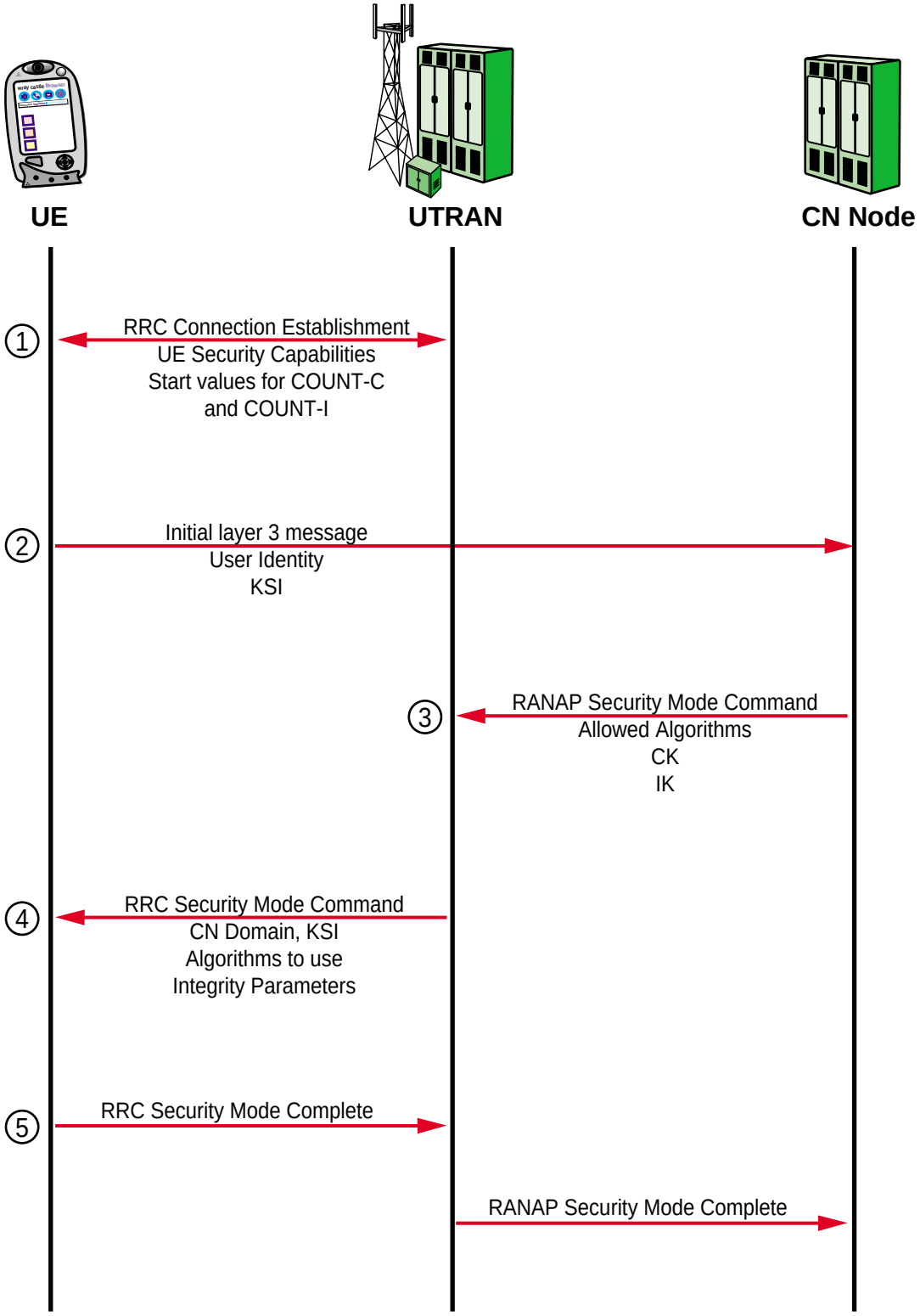


Figure 6
Initializing for Ciphering

© wray castle limited

1.5 Data Integrity

This process appends each outgoing message, UL or DL, with a check sum that can be used to verify the origin of the message. A fresh check sum, known as Message Authentication Code for Integrity (MAC-I), is computed for each message in the f9 algorithm.

There are five input parameters for f9:

Integrity Key (IK)
The value IK is a product of the authentication process and will be stored until needed for integrity by the UE and the CN node.

COUNT-I
COUNT-I is a time-dependent value consisting of the RRC HFN and the RRC SN. It will increment independently for each logical channel used for signalling according to the RRC HFN.

DIRECTION
The value DIRECTION is a single bit used to differentiate between integrity used in the UL and DL directions.

FRESH
FRESH is a random number generated by the RNC at the initiation of data integrity for a particular connection.

MESSAGE
On reception of an integrity-protected message, the receiving terminal uses f9 on the received message and appropriate stored parameters to generate an Expected MAC-I (XMAC-I). The values of MAC-I and XMAC-I are compared; if they do not match, the message is ignored.

© wray castle limited

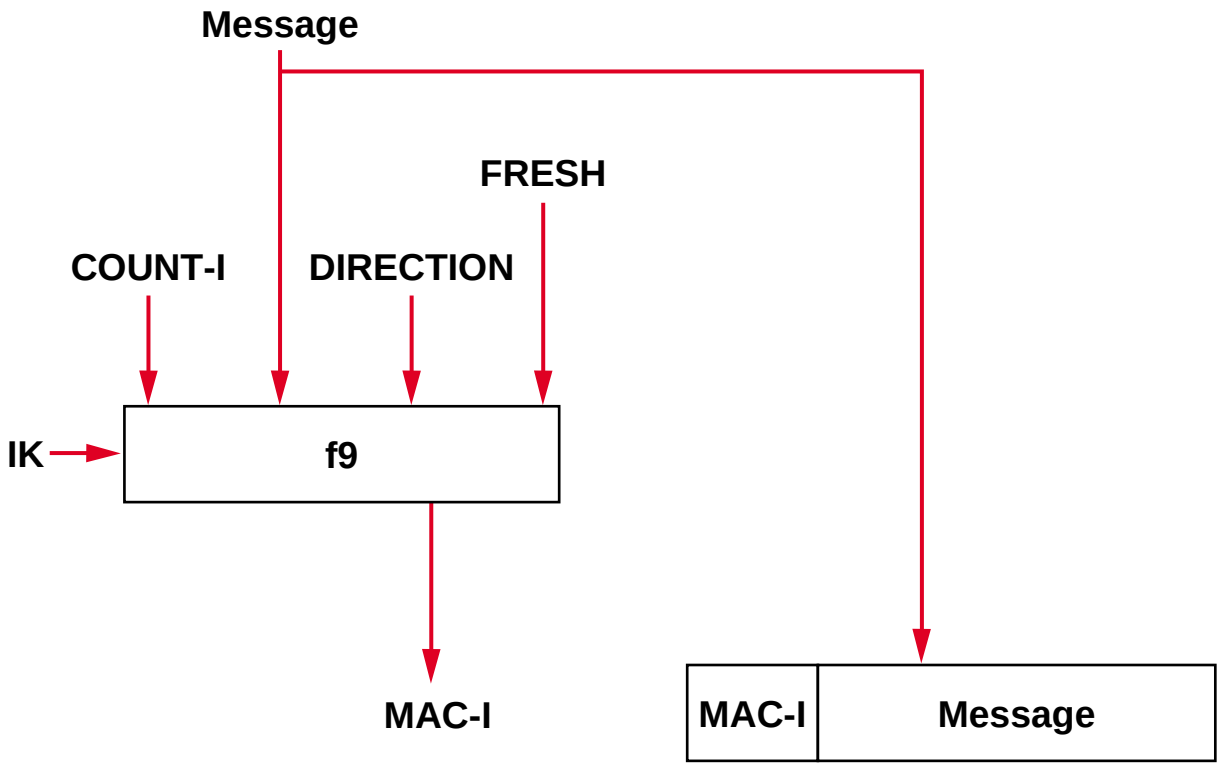


Figure 7
Data Integrity

© wray castle limited

© wray castle limited

SECTION 9

SYNCHRONIZATION

© wray castle limited

LESSON 1

SYNCHRONIZATION

© wray castle limited

LESSON CONTENTS

1	**Node Synchronization**		**9.1.1**
	1.1	Introduction	9.1.1
	1.2	UTRAN Synchronization	9.1.3
2	**Transport Synchronization**		**9.1.5**
	2.1	Introduction	9.1.5
	2.2	Cell System Frame Number (SFN)	9.1.5
	2.2	Connection Frame Number (CFN)	9.1.7
	2.3	Transport Channel Synchronization	9.1.9
	2.4	Node B Timing	9.1.11
	2.5	Timing Adjustment	9.1.13
	2.6	Monitoring Synchronization	9.1.15

© wray castle limited

LESSON OBJECTIVES

At the end of this lesson you will be able to:

- appreciate the general synchronization issues which need consideration when implementing the UTRAN
- state what synchronization counters and parameters are available within the UTRAN
- explain how synchronization is achieved at the RNC and the Node B, and within the transport channel
- appreciate what calculations are used within the UTRAN and UE in support of synchronization

© wray castle limited

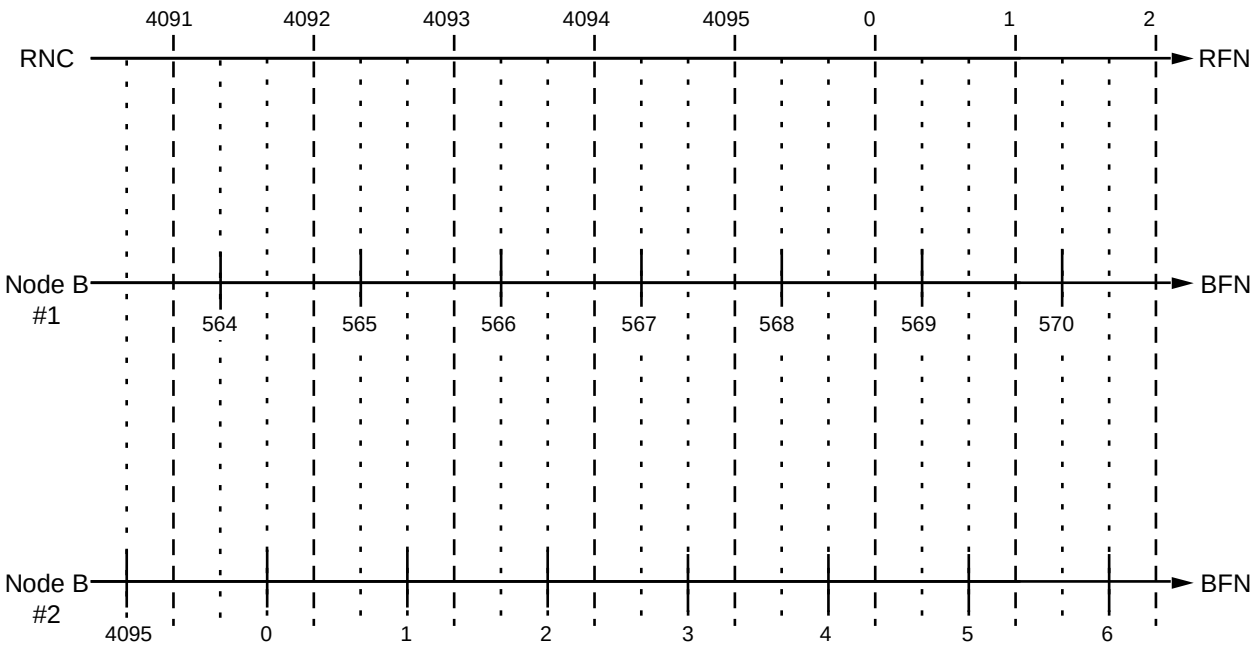
1 NODE SYNCHRONIZATION

1.1 Introduction

The term *Node Synchronization* generally means a common timing reference among different nodes. Using a common timing reference among all the nodes is useful, but not mandatory. RNCs must therefore have a mechanism to compensate for timing differences within the UTRAN.

The RNCs and Node Bs run independent frame counters. The RNC uses a RNC Frame Number (RFN) and the Node B uses a Node B Frame Number (BFN). These frame numbers range from 0 to 4,095, and increment every 10 ms.

© wray castle limited



RFN – RNC Frame Number
Range: 0–4095

BFN – Node B Frame Number
Range: 0–4095

Figure 1
UTRAN Counters

© wray castle limited

1.2 UTRAN Synchronization

The node synchronization procedure allows the RNC to identify the transmission delay. This optimizes buffering time for downlink (DL) transmission the Uu interface.

The DL node synchronization control frame is sent from the RNC. This includes the time (t1) when the frame was transmitted. Upon receiving the DL synchronization control frame, the Node B identifies t2. The Node B shall respond with uplink (UL) synchronization control frame, indicating t1, t2 and t3.

© wray castle limited

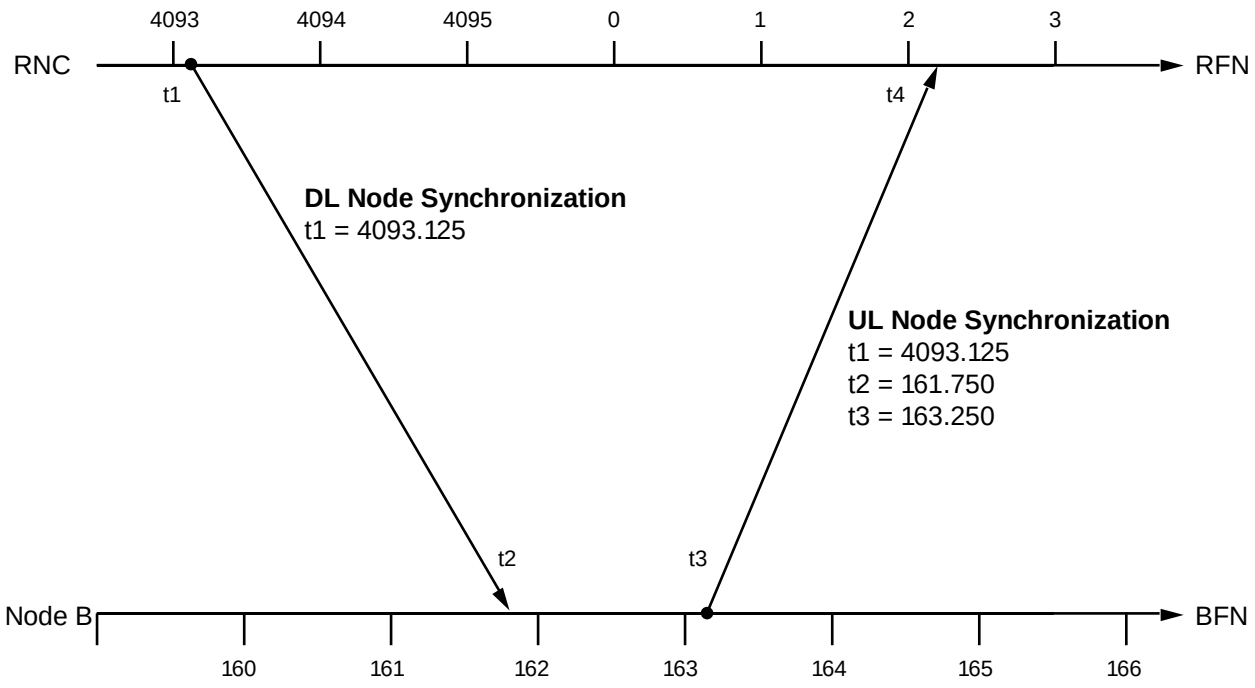


Figure 2

RNC Node B – Node Synchronization

© wray castle limited

2 TRANSPORT SYNCHRONIZATION

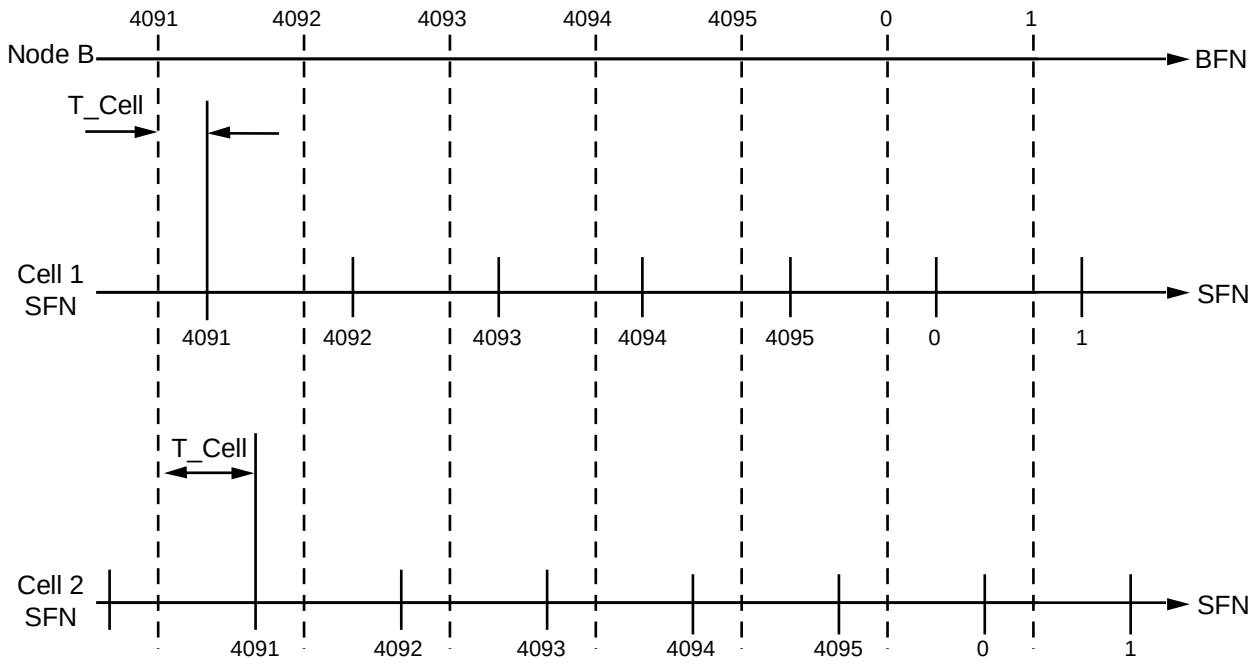
2.1 Introduction

Transport synchronization is the synchronization of the frame transport between the RNC and the Node B.

2.2 Cell System Frame Number (SFN)

The Node B may consist of a number of cells. Using the same timing on all cells would result in interference on the air interface. This interference is due to the transmission of multiple Synchronization Channels (SCH) at the same time. Cells (with the same frequency) belonging to a Node B must have different frame numbers. UTRAN cells use Cell SFN for timing. The SFN is identified by an offset from the BFN, which is referred to as T_Cell.

© wray castle limited



Cell System Frame Number (SFN) = BFN + T_Cell

Where T_Cell = 0 → 9 x 256 chips (0 → 9 x 1/10 of Frame)

Figure 3

Cell SFN

© wray castle limited

2.2 Connection Frame Number (CFN)

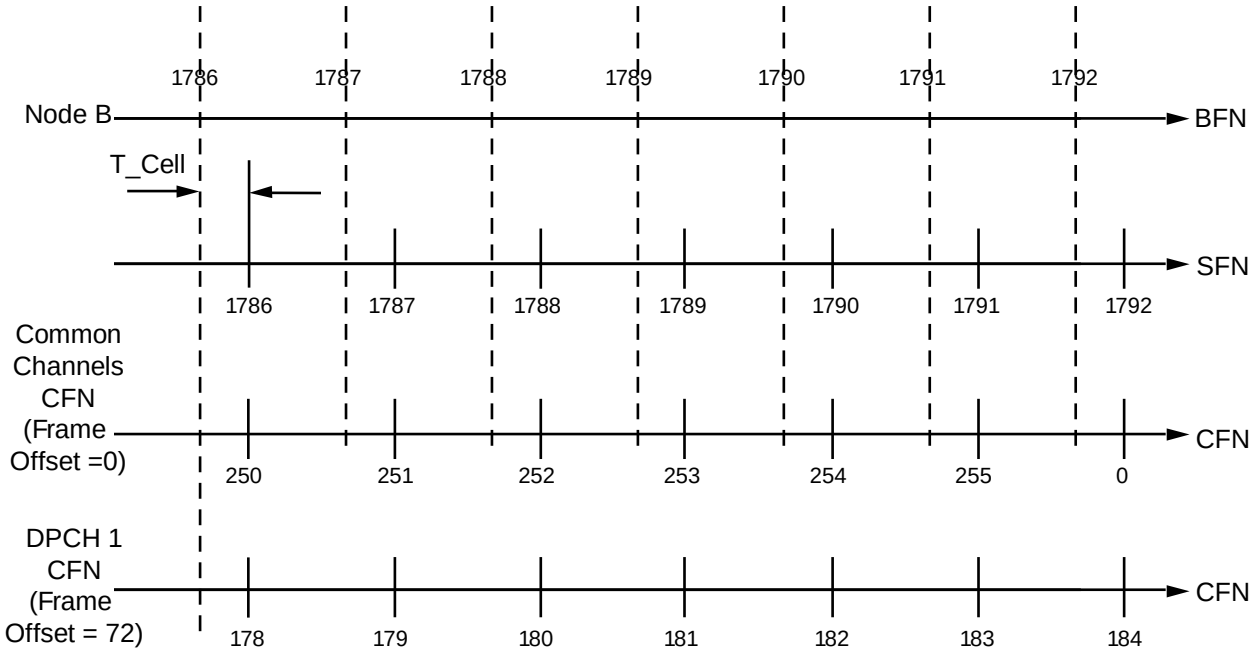
The CFN is used to synchronize the transport of frames between RNCs and Node Bs.

The CFN range is from zero to 255 and is calculated by:

CFN = (SFN – Frame Offset) mod 256

When establishing a dedicated channel, an SRNC informs the Node B of the frame offset required. The frame offset for common channels is set to zero (CFN = SFN mod 256).

© wray castle limited



Connection Frame Number (CFN) = (SFN – Frame Offset) mod 256

e.g. CFN = (1786 – 72) mod 256
= 178

Figure 4
CFN

© wray castle limited

2.3 Transport Channel Synchronization

The RNC configures a receiving window in the Node B for each channel. DL transmissions are adjusted to fit into a receiving window by adjusting the DL timing in the RNC. The UL transmission is adjusted by moving the reception window timing internally in the RNC.

© wray castle limited

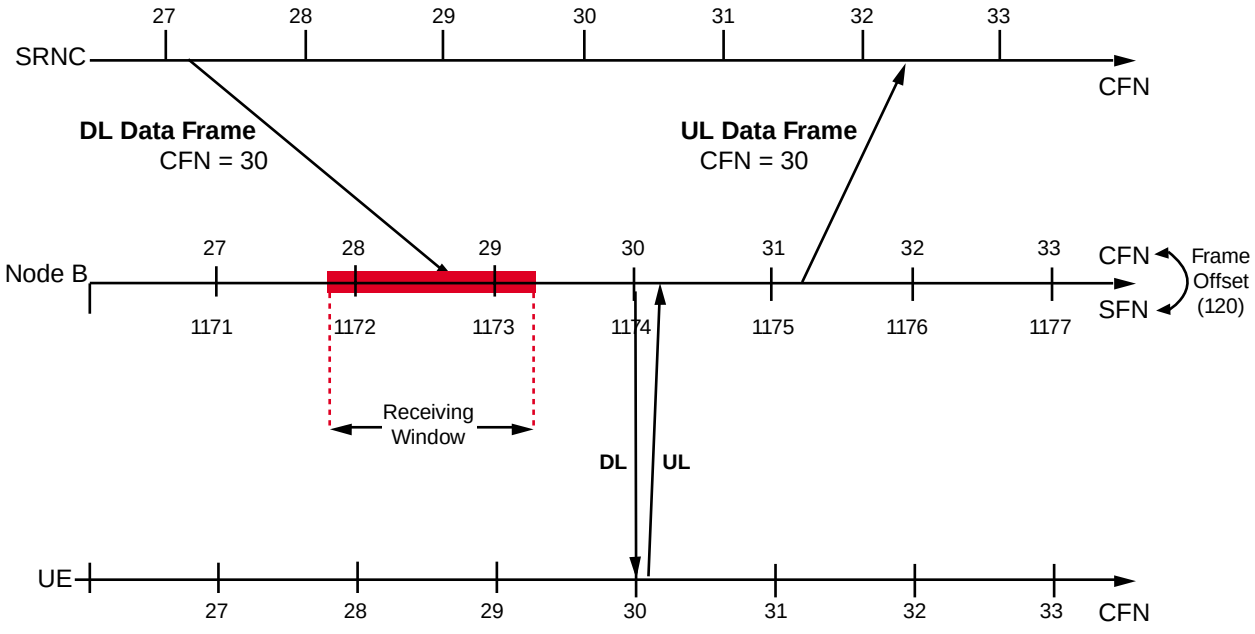


Figure 5

Transport Channel Synchronization

© wray castle limited

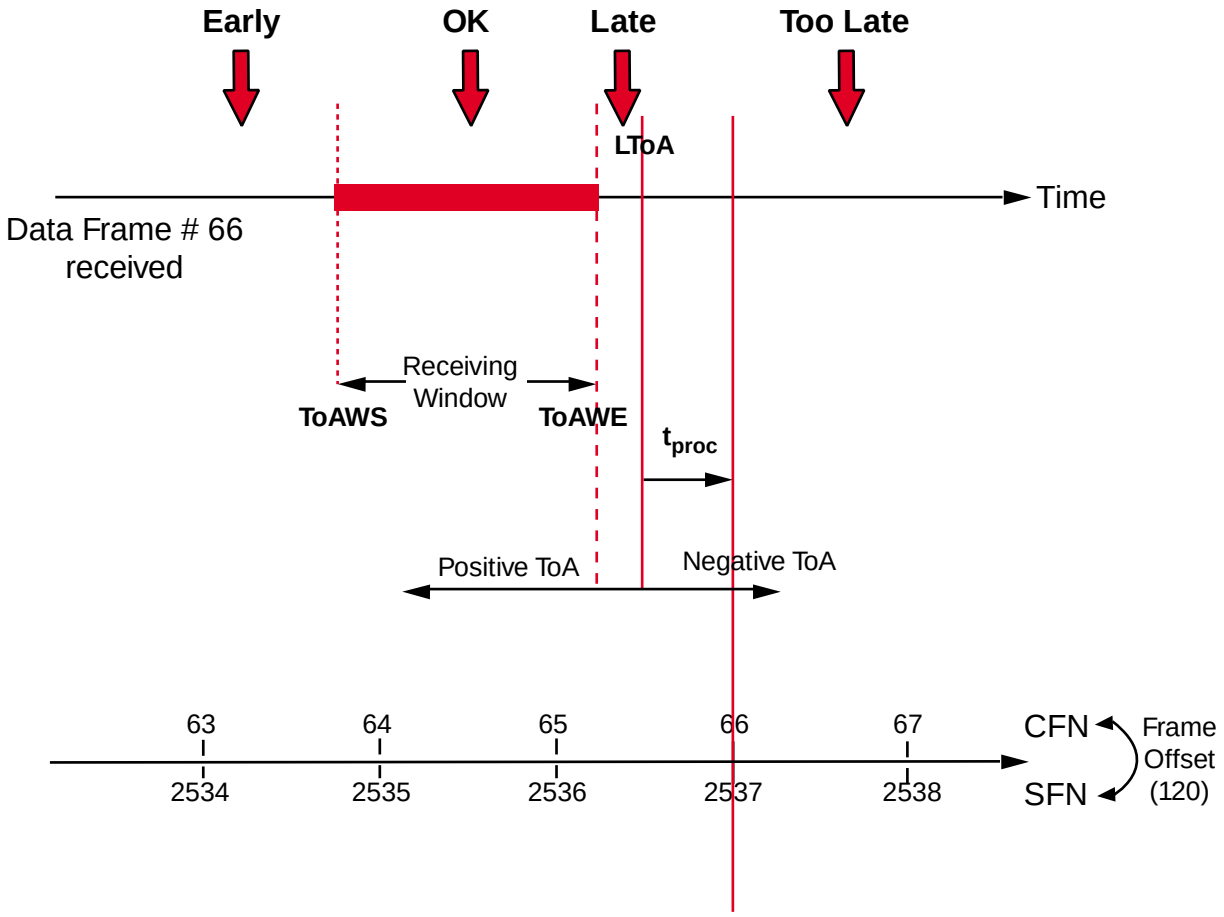
2.4 Node B Timing

The RNC sends information to the Node B that defines the receiving window for the channel. The two parameters that specify the receiving window are:

- Time of Arrival Window Startpoint (ToAWS)
- Time of Arrival Window Endpoint (ToAWE)

The Node B specifies a Latest Time of Arrival (LToA). This gives the Node B processing time (t_{proc}) before transmitting the frame.

© wray castle limited



ToA	**Time of Arrival**
ToAWS	**ToA Window Startpoint**
ToAWE	**ToA Window Endpoint**
LToA	**Latest Tme of Arrival**
t_{proc}	**Processing time before transmission**

Figure 6
Timing in Node B

© wray castle limited

2.5 Timing Adjustment

A DL data frame arriving with a negative ToA will trigger the sending of a Timing Adjustment frame. This frame will contain the ToA, allowing the RNC to correct the transmission timing.

© wray castle limited

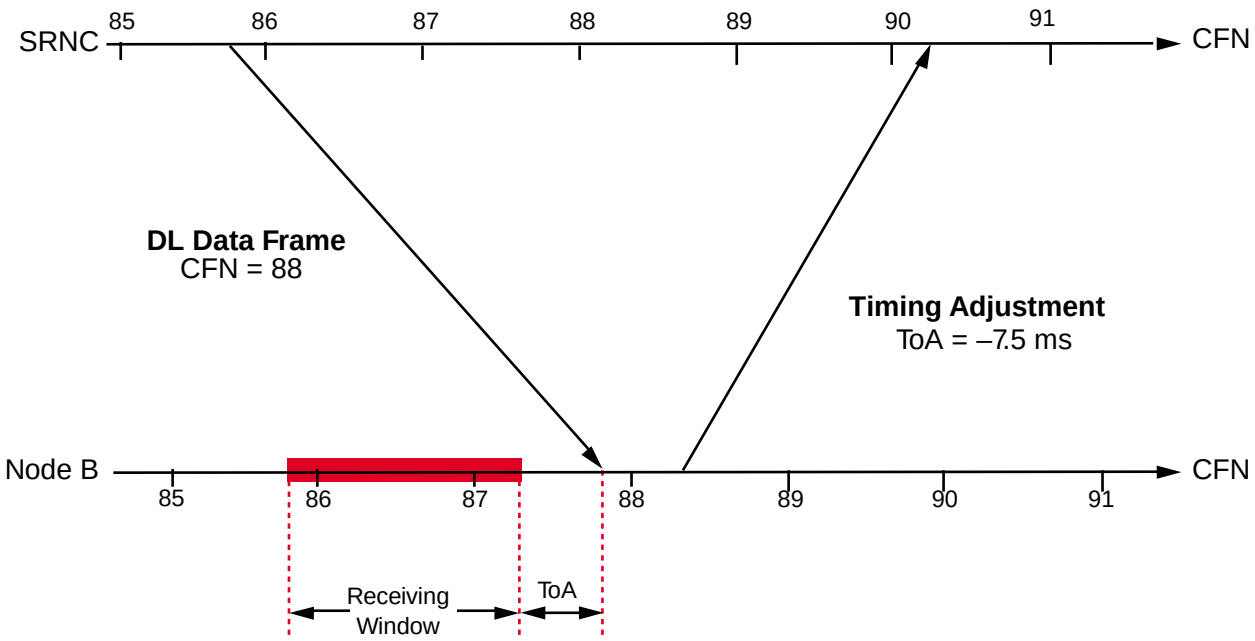


Figure 7
Timing Adjustment

© wray castle limited

2.6 Monitoring Synchronization

If there are no data frames to be sent, the RNC sends a DL synchronization frame. This will trigger the sending of a UL synchronization frame to the RNC. The UL synchronization frame will contain the ToA.

© wray castle limited

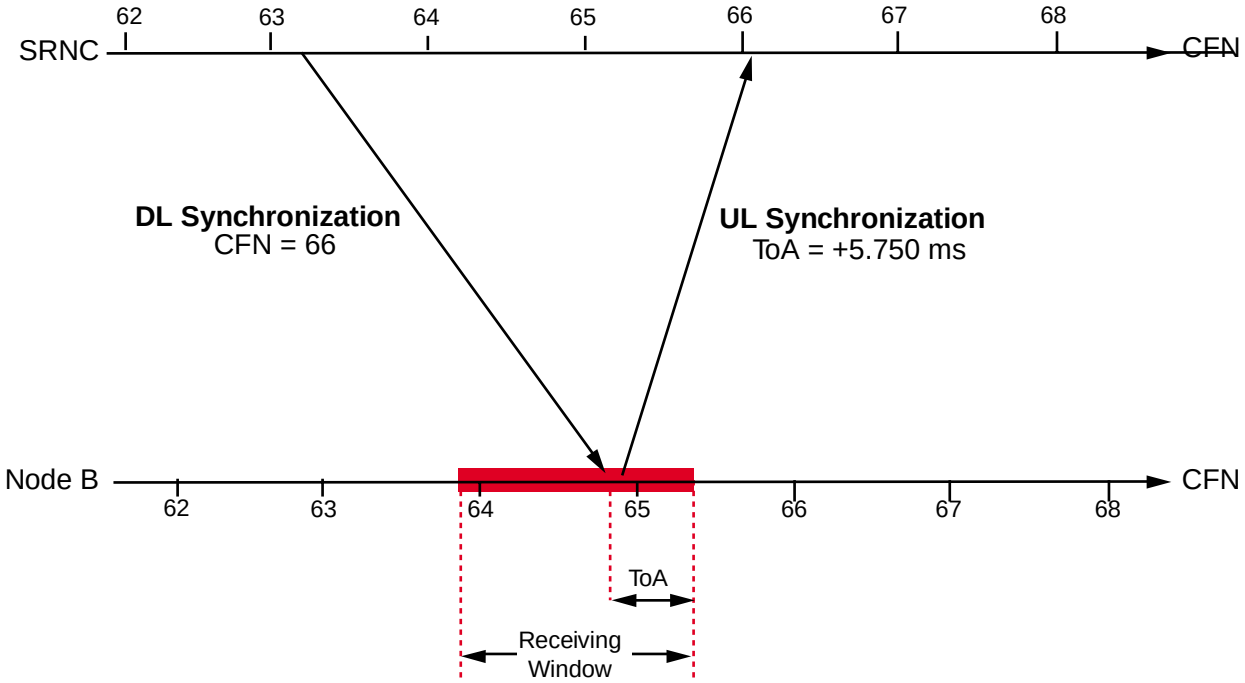


Figure 8
Monitoring Synchronization

© wray castle limited

© wray castle limited

UTRAN ARCHITECTURE AND PROTOCOLS

GLOSSARY OF TERMS

© wray castle limited

© wray castle limited

2G	Second Generation
3G	Third Generation
3GPP	3rd Generation Partnership Project
AAL	ATM Adaptation Layer
AAL2	ATM Adaptation Layer 2
AAL5	ATM Adaptation Layer 5
ACK/Ack	Acknowledgement
ALCAP	Access Link Control Application Part
AM	Acknowledged Mode
AMPS	Advanced Mobile Phone System
AMR	Adaptive Multi Rate
ANSI	American National Standards Institute
ARIB	Association of Radio Industries and Businesses
AS	Access Stratum
ATM	Asynchronous Transfer Mode
AUC	Authentication Centre
AUTN	Authentication Token
AV	Authentication Vector
BCCH	Broadcast Control Channel
BCFE	Broadcast Control Functional Entity
BCH	Broadcast Channel
BGAK	Begin Acknowledgement
BGN	Begin
BGREJ	Begin Reject
BLC	Block Confirm
BLK	Block Request
BRAN	Broadband Radio Access Network
BSN	Node B Frame Number
BSS	Base Station Subsystem
C/T	Channel Type
CBC	Cell Broadcast Centre
CC	Call Control
CC	Connection Confirm
CCCH	Common Control Channel
CDMA	Code Division Multiple Access
CFN	Cipher Frame Number
CFN	Confusion
CFN	Connection Frame Number

© wray castle limited

CID	Channel ID
C-Id	Cell Identifier
CK	Cipher Key
CLP	Cell Loss Priority
CM	Connection Management
CN	Core Network
CP	Common Part
CPCH	Common Packet Channel
CPCS	Common Part Convergence Sublayer
CPICH	Common Pilot Channel
CPS	Common Part Sublayer
CR	Connection Request
CRC	Cyclic Redundancy Check
CRNC	Controlling RNC
c-RNTI	Cell RNTI
CS	Circuit-Switched
CS	Convergence Sublayer
CS-PDU	Convergence Sublayer - Packet Data Unit
CTCH	Common Traffic Channel
D-AMPS	Digital Advanced Mobile Phone System
DC	Dedicated Control (SAP)
DCCH	Dedicated Control Channel
DCFE	Dedicated Control Functional Entity
DCH	Dedicated Channel
DCH-FP	Dedicated Channel Frame Protocol
DCH-Id	Dedicated Transport Channel Id
DECT	Digital Enhanced Cordless Telephony
DL	Downlink
DLR	Destination Local Reference
DRNC	Drift Remote Network Controller
d-RNTI	Drift RNC RNTI
DSCH	Downlink Shared Channel
DSCH-FP	Downlink Shared Channel Frame Protocol
DSCH-Id	Downlink Shared Channel Id
DT1	Dataform 1
DTCH	Dedicated Traffic Channel
ECF	Establish Confirm
EDGE	Enhanced Data-rates for Global Evolution
EFR	Enhanced Full Rate
END	End
ENDAK	End Acknowledgement
ER	Error

© wray castle limited

ERAK	Error Acknowledgement
ERQ	Establish Request
ETSI	European Telecommunications Standards Institute
FACH	Forward Access Channel
FACH FP	Forward Access Channel Frame Protocol
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FN	Frame Number
FP	Frame Protocol
FT	Frame Type
GC	General Control (SAP)
GERAN	GSM/EDGE Radio Access Network
GFC	Generic Flow Control
GGSN	Gateway GPRS Support Node
GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMS	GPRS Short Message Service
GTP	GPRS Tunnelling Protocol
GTP-U	GPRS Tunnelling Protocol for User Plane
HEC	Header Error Control
HFN	HyperFrame Number
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
IK	Integrity Key
IMT-2000	International Mobile Telecommunications 2000
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
Iu	RNC - CN interface
Iub	RNC - Node B interface
Iu-CS	RNC - CN interface Circuit-Switched
Iu-PS	RNC - CN interface Packet Switched
Iur	RNC - RNC interface
K	Secret Key
KSI	Key Set Identifier

© wray castle limited

L1	Layer 1 - Physical Layer
LAC	Link Access Control
LAI	Local Area Identity
LAN	Local Area Network
LI	Length Indicator
LLC	Logical Link Control
LtoA	Latest Time of Arrival
M3UA	MTP3 User Adaptation Layer
MAC	Medium Access Control
MAC-b	MAC sublayer - Broadcast Transport Channel
MAC-c/sh	MAC sublayer - common and Shared Transport Channel
MAC-d	MAC sublayer
MAC-I	Message Authentication Code for Identity
MAHO	Mobile Assisted Handover
MD	Unnumbered Management Data
MM	Mobility Management
MMI	Man-Machine Interface
MS	Mobile Station
MSC	Mobile Switching Centre
MTP	Message Transfer Part
MTP3b	Message Transfer Part level 3 broadband
N1	SCCP Node 1
N2	SCCP Node 2
NAS	Non-Access Stratum
NBAP	Node B Application Part
NMT	Nordic Mobile Telephone
NNI	Network-Node Interface
NSDU	Network Services Data Unit
Nt	Notification (SAP)
O&M	Operations and Maintenance
OCCCH	ODMA Common Control Channel
ODCCH	ODMA Dedicated Control Channel
ODCH	ODMA Dedicated Channel
ODTCH	ODMA Dedicated Traffic Channel
ORACH	ODMA Random Access Channel
OSF	Offset Field
OSI	Open Systems Interconnect

© wray castle limited

P	Parity
PBX	Private Branch Exchange
PCCH	Paging Control Channel
PCH	Paging Channel
PD	Protocol Discriminator
PD	Propagation Delay
PDC	Personal Digital Communications
PDU	Packet Data Unit
PHY	Physical Layer
PLMN	Public Land Mobile Network
PLMN-Id	Public Land Mobile Network Identifier
PNCFE	Paging and Notification Control Functional Entity
POLL	Transmitter State Information with request for Receiver State Information
PS	Packet Switched
PSTN	Public Switched Telephone Network
PT	Payload Type
P-TMSI	Packet Temporary Mobile Subscriber Identity
PUSCH	Physical Uplink Shared Channel
PVC	Permanent Virtual Connection
QoS	Quality of Service
RA	Routing Area
RAB	Radio Access Bearer
RAB-Id	Radio Access Bearer Id
RAC	Routing Area Code
RACH	Random Access Channel
RACH/SPCH-F	Random Access Channel/Shared Physical Channel Frame Protocol
RAI	Routing Area Identity
RAND	Random Challenge
RAT	Radio Access Technology
RB	Radio Bearer
REL	Release Request
RES	Response
RES	Reset Request
RFE	Routing Functional Entity
RFN	RNC Frame Number
RLC	Radio Link Control
RLC	Release Confirm
RLC	Release Complete
RLSD	Released

© wray castle limited

RNC	Radio Network Controller
RNC-Id	Global Remote Network Controller Identifier
RNS	Radio Network Subsystem
RNSAP	Radio Network Subsystem Application Part
RNTI	Radio Network Temporary Identifier/Identity
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
RS	Resynchronization Command
RSAK	Resynchronization Acknowledgement
RSC	Reset Confirm
RX	Receive
SA	Service Area
SAAL	Signalling AAL
SAAL-UNI	Signalling ATM Adaptation Layer
SABP	Service Area Broadcast Protocol
SAC	Service Area Code
SAI	Service Area Identifier
SAID	Signalling Association Identifier
SAP	Service Access Point
SAR-PDU	Segmentation and Reassembly - Packet Data Unit
SCCP	Signalling Connection Control Part
SCFE	Shared Control Functional Entity
SCH	Synchronization Channel
SCTP	Stream Control Transmission Protocol
SD	Sequenced Connection-mode-Data
SDU	Service Data Unit
SFN	System Frame Number
SGSN	Serving GPRS Support Node
SLR	Source Local Reference
SLS	Signalling Link Set
SM	Session Management
SMS	Short Message Service
SN	Sequence Number
SPCH	Shared Physical Channel
SRNC	Serving Remote Network Controller
s-RNTI	Serving RNC RNTI
SS	Supplementary Service
SS7	Signalling System No. 7
SSCF	Service-Specific Coordination Function
SSCF-NNI	Service-Specific Control Function - Network-Node Interface
SSCOP	Service-Specific Connection-Oriented Protocol

© wray castle limited

SSCS	Service Specific Co-ordination Function
SSP	Service Specific Part
STAT	Solicited Receiver State Information
STC	Signalling Transport Converter
SUGR	Served User Generated Reference
SVC	Switched Virtual Connection
TACS	Total Access Communication System
TB	Transport Block
TCP/IP	Transmission Control Protocol/Internet Protocol
TCTF	Target Channel Type Field
TD-CDMA	Time Division - Code Division Multiple Access
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TFI	Transport Frame Indicator
TI	Transaction Identifier
TIA	Telecommunications Industry Association
TME	Transfer Mode Entity
TMSI	Temporary Mobile Subscriber Identity
ToAWE	Time of Arrival Window Endpoint
ToAWS	Time of Arrival Window Startpoint
tproc	Node B Processing Time
TX	Transmit
UBC	Unblock Confirm
UBL	Unblock Request
UC-Id	UTRAN Cell Identifier
UD	Unnumbered User Data
UDP	User Datagram Protocol
UDT	UnitData
UE	User Equipment
UL	Uplink
UM	Unacknowledged Mode
UMTS	Universal Mobile Telecommunications System
UNI	User-Network Interface
URA	UTRAN Registration Area
u-RNTI	UTRAN RNTI
USCH	Uplink Shared Channel
USCH-FP	Uplink Shared Channel Frame Protocol
USCH-Id	Uplink Shared Channel Id
USIM	UMTS Subscriber Identity Module
USTAT	Unsolicited Receiver State Information

© wray castle limited

UTRAN	UMTS Terrestrial Radio Access Network
Uu	Node B - UE interface
UUI	User-to-User Indication
VC	Virtual Channel
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VLR	Visitor Location Register
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
XMAC-I	Expected Message Authentication Code for Identity
XRES	Expected Response

© wray castle limited