White Paper: Protocol Analysis in UMTS Networks

Tektronix, Inc.

Introduction

As of today, there are still very few UMTS networks offering commercial service. However, since third-generation (3G) handset functionality is improving and a wider range of handsets is becoming available, the number of 3G UMTS subscribers is increasing. By March 2003 there were more than 350,000 UMTS users and more than 6,000,000 cdma2000 users in Japan, and the rollout of UMTS throughout Europe is underway. Even some GSM operators in the US are already testing or are about to test UMTS. Therefore, there is an urgent need to provide hands-on practical examples of protocol testing in the first UMTS “islands“ of this world. Call tracing and similar tasks haven’t vanished with the advent of UMTS; in fact, tasks such as these have become even more complex. This is also valid for engineers with many years of protocol testing experience in GSM-networks. This document is intended to ease troubleshooting and protocol testing tasks in today and tomorrow’s UMTS-networks.

Standards

The International Telecommunication Union (ITU) solicited several international organizations for descriptions of their ideas for a 3G mobile network:

CWTS China Wireless Telecommunication Standard group
ARIB Association of Radio Industries and Businesses, Japan
T1 Standards Committee T1 Telecommunications, USA
TTA Telecommunications Technology Association, Korea
TTC Telecommunication Technology Committee, Japan
ETSI European Telecommunications Standards Institute

As a result, ITU combined different technologies for IMT-2000 standards at 2000 MHz. The main advantage of IMT-2000 is that it specifies international standards and also the interworking with existing PLMN standards, such as GSM.

In general the quality of transmission is improved. The data transfer rate is increased dramatically. Transfer rates of 144 kbit/s or 384 kbit/s is available in a short time; however, 2Mbit/s will only be available in certain small areas or will remain a theoretical value for a long time. New service offerings will help UMTS to become financially successful for operators and attractive to users. For example, users will have worldwide access with a mobile phone, and the look and feel of services will be the same wherever he or she may be.

There is a migration path from second-generation (2G) to 3G systems that may include an intermediate step - the so-called 2.5G network. Packet switches, the GPRS support nodes (GGSN/SGSN), are implemented in the already existing core network while the radio access network is not changed significantly. In the case of a migration from GSM to UMTS a new radio access technology (W-CDMA instead of TDMA) is introduced. This means the networks are equipped with completely new radio access networks that replace the 2G network elements in the RAN. EDGE is a different way to offer high-speed IP services to GSM subscribers without introducing W-CDMA. The already existing CDMA cellular networks, which are especially popular in Asia and North America, will undergo an evolution to become cdma2000 networks with larger bandwidth and higher data transmission rates.

UMTS

For the purpose of this paper, we are focusing on UMTS, the clear 3G successor to GSM and GPRS. As we discuss the most important UMTS procedures and with consideration of transaction-tracing possibilities, the experienced reader will frequently recognize the “spirit” of GSM, because much of the so-called Non-Access-Stratum or NAS-messaging in UMTS is actually adopted from GSM. However, in the lower layers within the UTRAN, UMTS introduces a set of new protocols, which deserve close understanding and attention for protocol

testing. Even more important, the UMTS control plane and user plane (figure 1) are essentially based on ATM and on AAL-2 and AAL-5 within the transport plane. While the generic objectives of a mobile network, and therefore the NAS-messaging, didn't significantly change from GSM and GPRS, the underlying access network signaling fully supports the new, and by far, more flexible requirements of a 3G- and W-CDMA-based standard.

The philosophy of UMTS is therefore continuously targeted at the separation of user plane and control plane, of radio and transport network, of access network and core network and of access stratum and non-access stratum. The User Plane is again separated into two traffic-dependent domains. The circuit switched domain (CS Domain) and the packet switched domain (PS Domain). Both traffic-dependent domains use the functions of the remaining entities – the Home Location Register (HLR) together with the Authentication Center (AC), or the Equipment Identity Register (EIR) - for subscriber management, mobile station roaming and identification, and handle different services. Thus, the HLR contains GSM, GPRS, and UMTS subscriber information. The two domains handle their traffic types at the same time for both the GSM and the UMTS access networks. The CS domain handles all circuit switched type of traffic for the GSM as well as for the UMTS access network; similarly, the PS domain takes care of all packet switched traffic in both access networks.

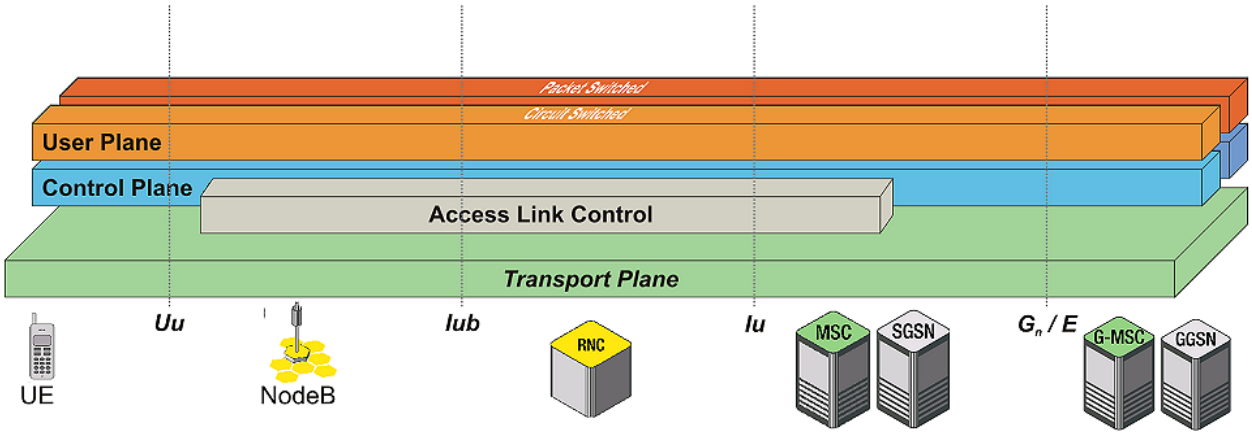

Figure 1: An Abstract View at the UMTS Protocol Stack

Protocol Analysis in UMTS Networks

The analysis of protocol recordings in UMTS is much more complex than in GSM-/GPRS-networks for a number of reasons:

1. No Pre-configured Timeslots or Channels for Signaling Messages and User Data

First of all, UMTS networks use the packet-switched ATM protocol to provide for the highest possible flexibility in resource allocation. Using so called cells on a serial link with a payload of just 48 octets, ATM is capable to share an E1, T1 or STM-1 link among a literally unlimited number of users or, at the other extreme, to provide all resources to only a single user.

With respect to ATM, the term "user" refers to virtual paths and channels, which in turn, are only bearers for the higher UMTS-layers. This and other advantages of using ATM are good for UMTS but unfortunately, ATM does not come with pre-configured timeslots or dedicated channels. This issue appears to be trivial, but finding signaling messages on the Iub- or Iu-interfaces in a UMTS-network without knowing where to look for them is impossible.

As a matter of fact, ATM is not providing dedicated timeslots or channels for neither signaling messages nor user data. Rather, ATM is providing virtual channels and virtual paths that need to be configured by the higher protocol layers of UMTS upon putting an interface and a network node (e.g. RNC, NodeB or cell) into service.

Figure 2 illustrates an example: In this case, the new cell No 5 is put into service at a given NodeB. Among other things, the common control channels need to be configured. Figure 2 highlights part of the configuration of a PCH on channel 11 of the ATM-path and circuit with VPI = 6 and VCI = 58. Note that VPI/VCI = 6/58 is only an example. The respective values are dynamic and need to be pre-configured in the protocol tester

You can also see that a few rows underneath this highlighted part on channel 12 (⇔ same VPI/VCI), a FACH is opened and on channel 13 (⇔ same VPI/VCI) a RACH is opened. Without tracking these configuration messages, protocol tracing on the respective channels becomes an almost impossible undertaking.

One way to quickly gather information on which VPI/VCI values are used by the NBAP and ALCAP and on what VPI/VCI/CID values are used by the Common Control Channel is to simply re-start the Node B and look at the content of the initialization messages. However, it interrupts service to subscribers—the one thing no network can afford to do unnecessarily.

Another way is to use an Iub Automatic Configuration application; the configuration task becomes completely automated. Expert software can automatically configure all the logical links required to monitor NBAP, ALCAP for each Node B under observation and RACH, FACH, PCH for each cell under observation. The ability to perform automatic analysis on the Iub-interface will give users a large advantage. It will automatically track the configured channels and display the configuration of each channel in plain text. The protocol tester locks to these channels and allows tracing of the upcoming signaling messages.

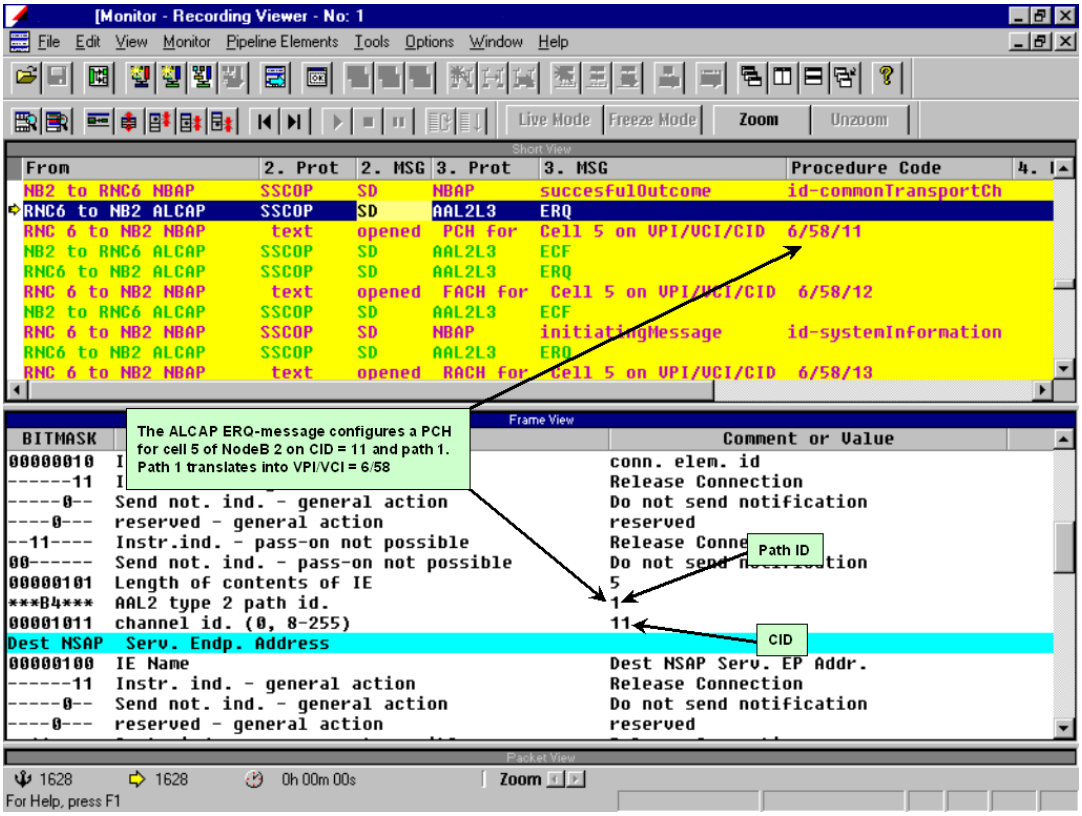

Figure 2: Extract of a Cell Configuration, recorded on an Iub-interface

2. Limited Possibility of HEX-Trace Analysis

Another challenge for the experienced GSM-protocol expert is the fact that some higher layer UMTS-protocols like RANAP, NBAP or RRC do not only use ASN.1 encoding rules but for optimization, apply the so called Packed Encoding Rules (PER).

Figure 3 illustrates the basic parameter encoding rules of ASN.1: Each parameter is encoded using a unique tag, followed by a length indication and finally the parameter value. Of course, ASN.1 provides many more capabilities, but what is important to consider is the fact this type of encoding is a waste of radio resources.

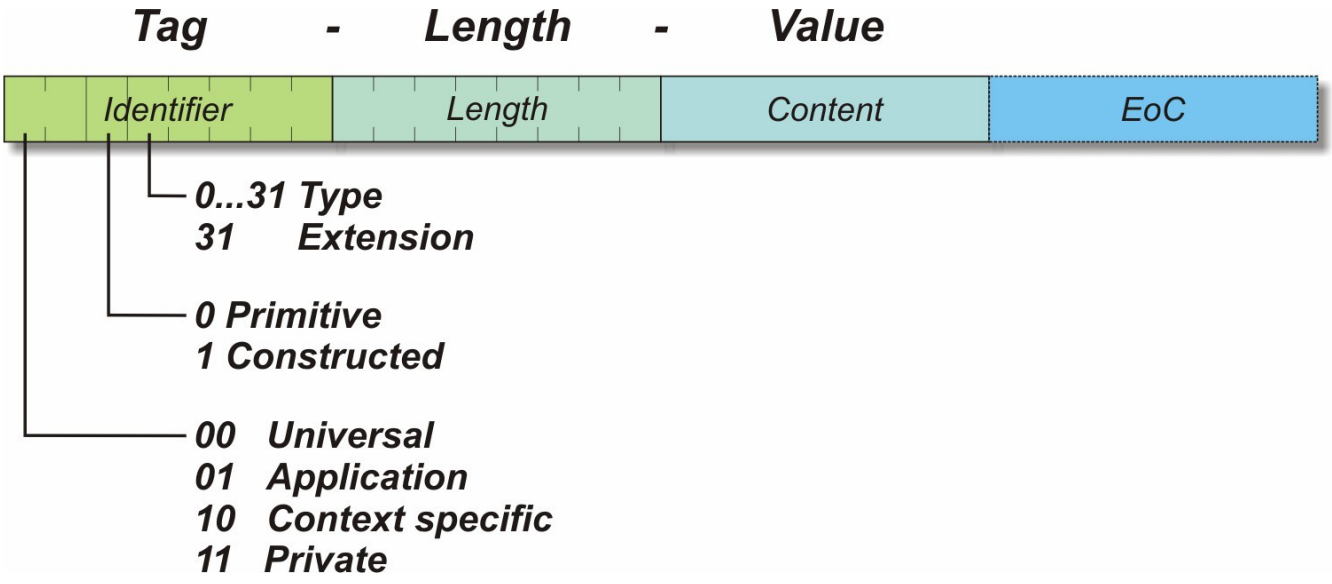

Figure 3: Parameter Encoding in ASN.1

Figure 4 clearly highlights this problem, using the example parameter "MyInteger." This parameter can take on only two values: '0' and '1.' Besides, the presence of the parameter "MyInteger" shall be mandatory in the message to be encoded. Just applying ASN.1 basic encoding leaves us with three octets to be transmitted. But after applying PER, only a single bit (⇔ '0' or '1') needs be sent. The benefits of PER are obvious; however, one may still miss the possibility to easily match hexadecimal values to protocol tester mnemonics.

In UMTS, it is therefore no longer trivial to translate hexadecimal recordings into mnemonics just by using the respective specifications. One needs a PER decoding and therefore, a protocol tester for almost any kind of protocol analysis. The hexadecimal debugging alternative is cumbersome for all protocols that apply the PER.

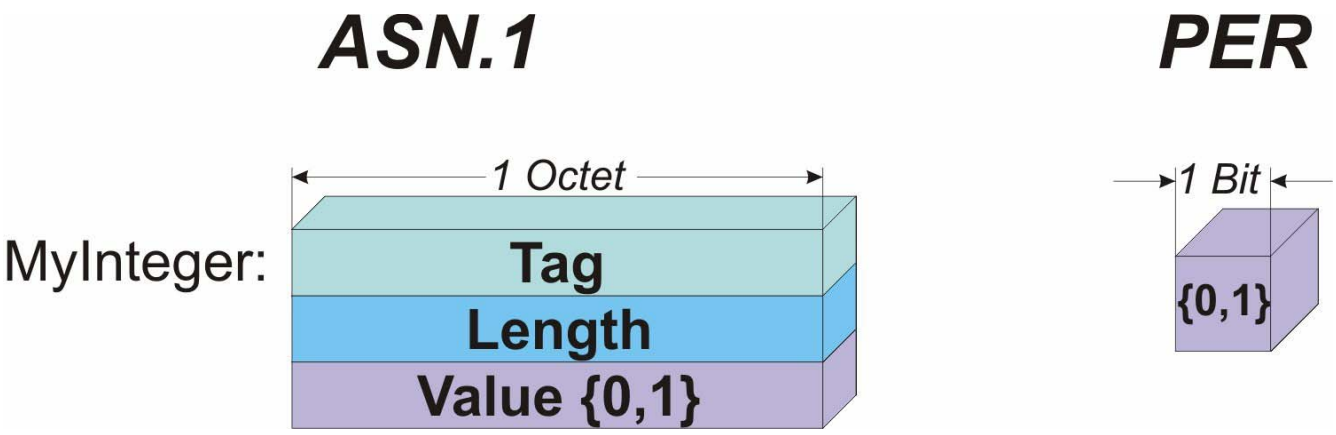

Figure 4: The Impact of Applying PER on Mandatory Parameter "MyInteger"

3. Following a Single Call Flow

Protocol analysis in UMTS, compared to GSM, has an essential impact on the very basic task to follow a single call setup or registration or PDP context activation. To recall some of the very basic questions:

⇒ Which parameters tie the various messages to each other?
⇒ Which call was successful and which one wasn't?
⇒ Did this transaction fail because of errors in the previous parameterization?

Now, let's clearly line out how you can follow a single transaction in your recording.

Selected UMTS-Procedures

Registration / Location Updating

Upon power-on, the UE will register to the network. The following pages illustrate the respective message flow on the terrestrial interfaces Iub (⇐ NodeB ⇔ RNC) and Iu-Cs (⇐ RNC ⇔ MSC). Please note the additional information to reflect how the parameters relate the messages of a single call flow to each other.

Example: The NBAP: successful Outcome-message [Procedure Code: id-radioLinkSetup] being sent from the Node-B to the RNC can be linked to the related ALCAP: ERQ-message by means of the parameter 'Binding ID' which value is repeated in the ERQ-message in the 'Served User Generator Reference' parameter. To continue, one may use the parameter 'Originating Signaling Association ID' in the ALCAP: ERQ-message to relate it to the respective ALCAP: ECF-message (the parameter 'Originating Signaling Association ID' is mirrored in the ALCAP: ECF-message as 'Destination Signaling Association ID').

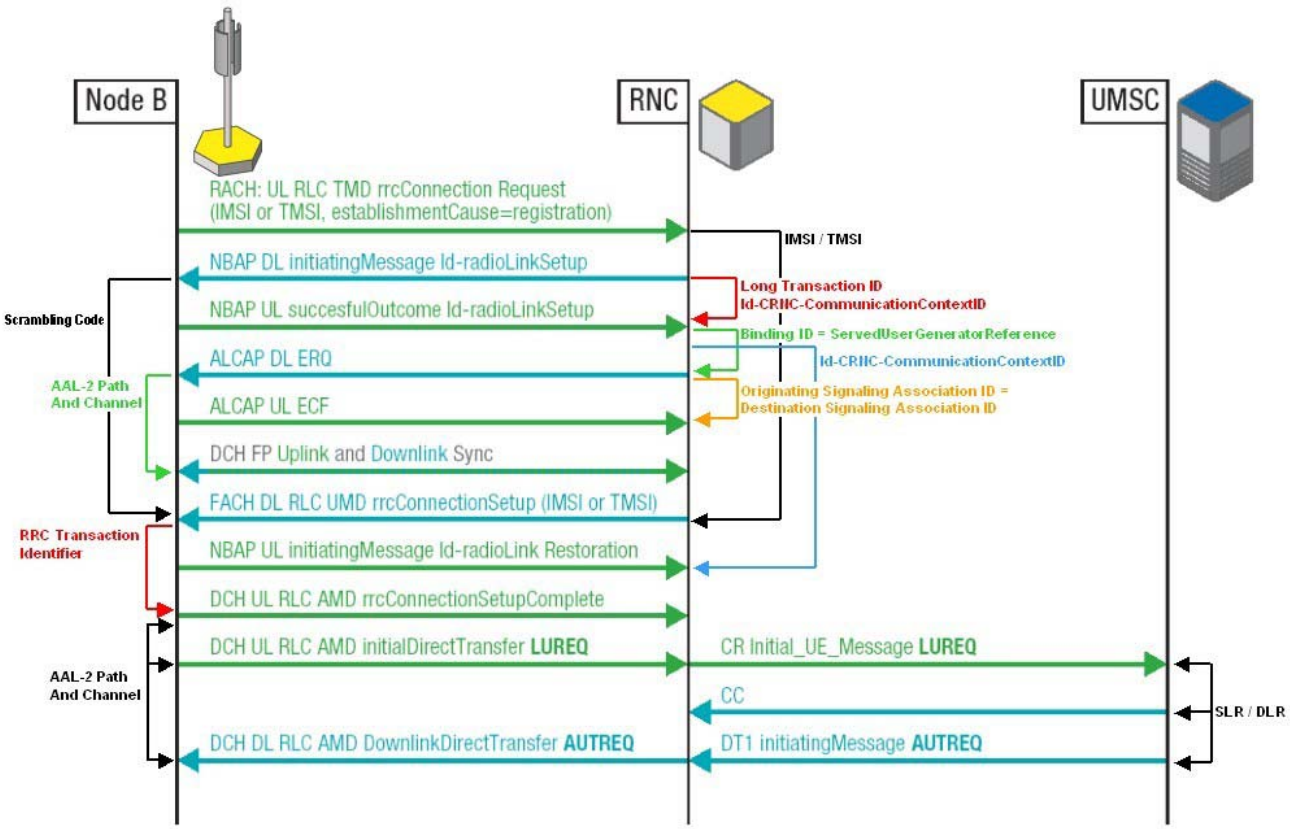

Figure 5: Registration of a UMTS UE (circuit-switched)

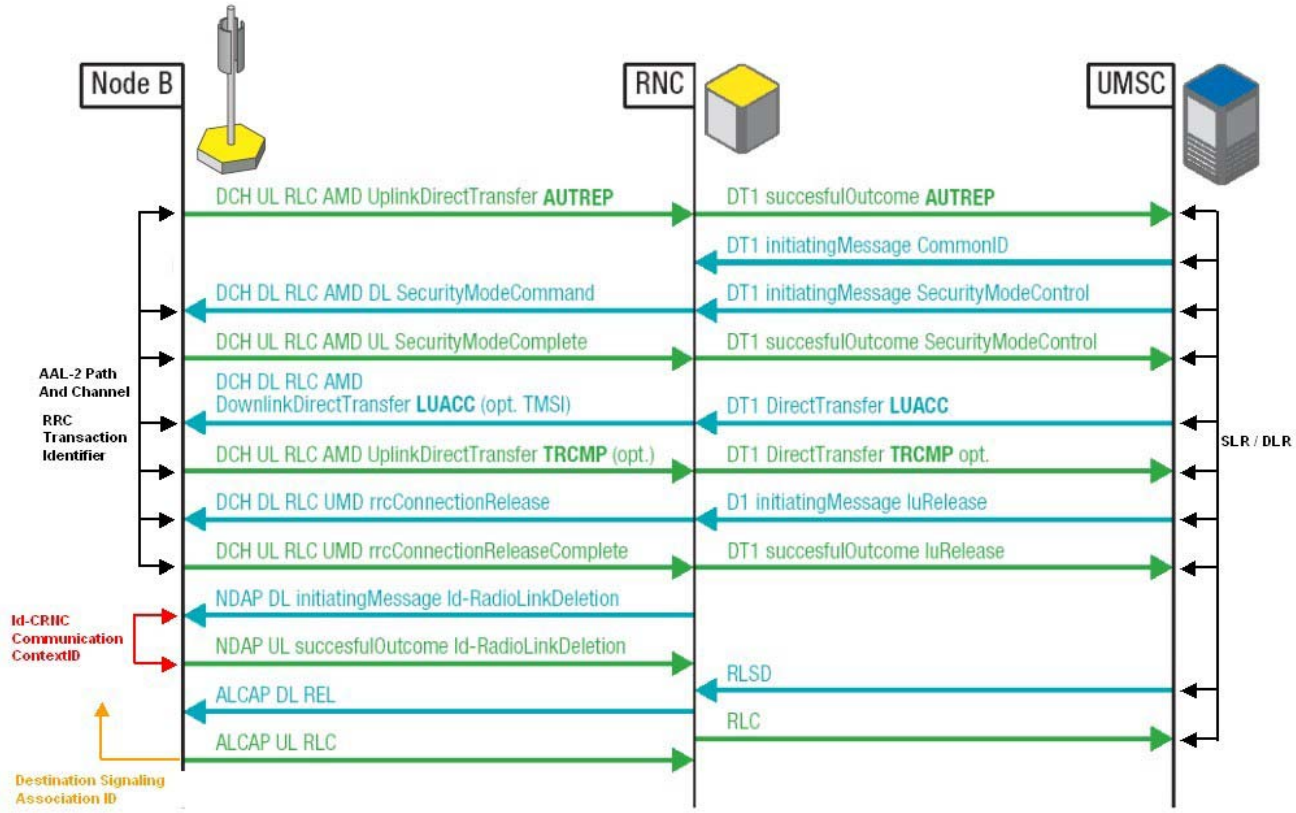

Figure 6: Registration of a UMTS UE (circuit-switched)

Please note that on the Iu-interface the well-known SCCP is used to establish virtual signaling connections between the RNC and the MSC. Also, one should recall SCCP is using SLR / DLR (Source Local Reference and Destination Local Reference) to identify SCCP-messages that belong to the same connection. In this scenario, “registration” and the following scenarios will be the SLR and the DLR. These are almost always used on the Iu-interface to relate the very RANAP-messages to each other. Following a successful registration, the bearer channels in the transport network are released. Note how the RANAP is initiating this release through an initiating Message (Procedure Code: ‘Id-Iu-Release’). On the Iub-interface, ALCAP will release the respective bearer channel by sending an ALCAP: ERQ-message.

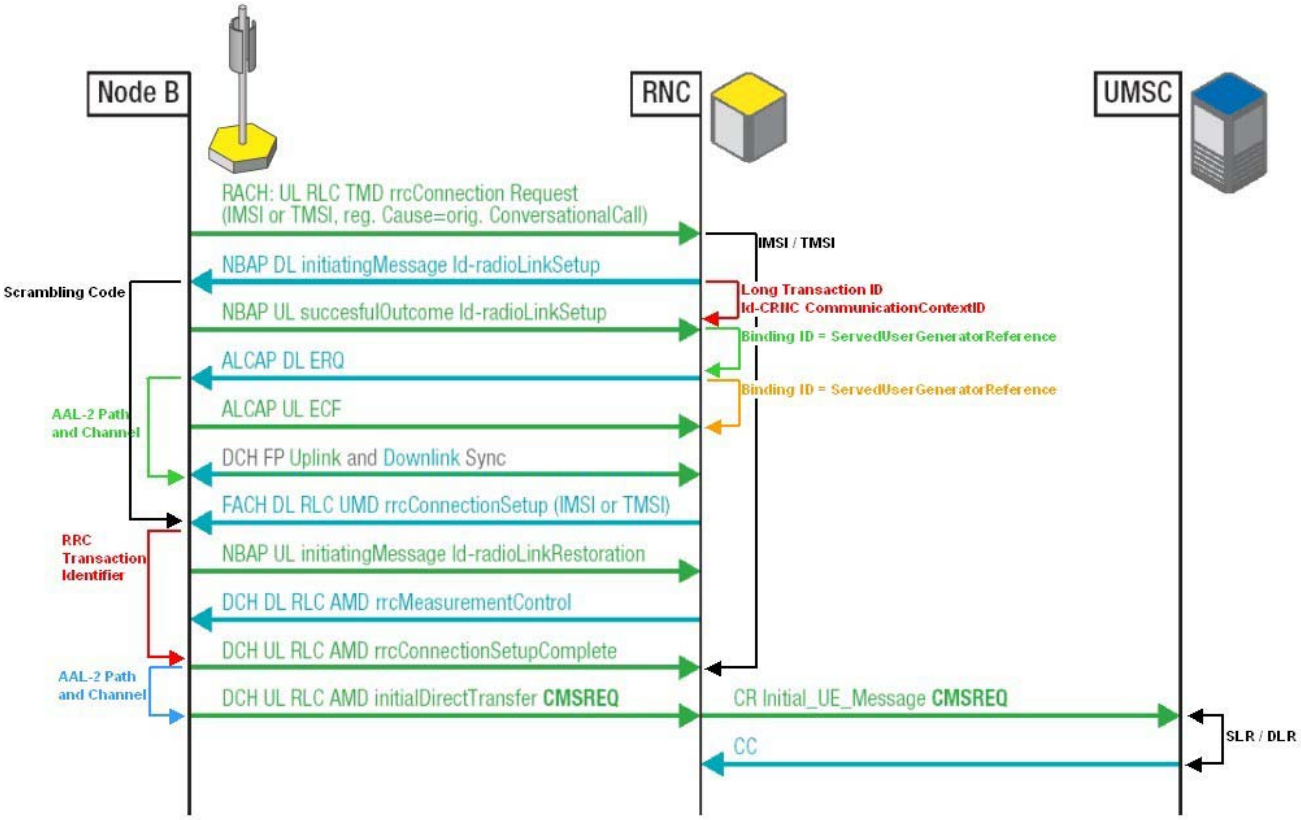

Figure 7: Mobile Oriented Call

Mobile Oriented Call

The following scenario illustrates a more complex transaction: A mobile oriented call that includes the allocation and release of a radio access bearer. Please note that in case of conversational calls in UMTS opposed to GSM there is no CC: DISC-message sent when the network side releases the call.

As seen in the previous registration scenario, the SCCP SLR/DLR is used on the Iu-interface for identification purposes. The situation on the Iub-interface is more complicated, at least during the initial setup phase and for the setup of the radio link (⇔ figure 7). For example, to link an NBAP-initiating message (Id-radioLinkSetup) to the respective rrcConnectionSetup-message, only the scrambling code can be used.

The only difference during the radio link setup phase between the illustrated scenario and the previously presented scenario registration is the measurement initiation through the RNC. It is important to emphasize that this measurement initiation is optional, and that most likely, the RNC will invoke it.

For the relation of this rrcConnectionSetup-message and all the RRC-messages that follow in Figure 8, the RRC-transaction identifier is used. Please note that these RRC-messages are really transparent bearers for the respective NAS-messages. Please compare these NAS-messages to the ones that are used in GSM.

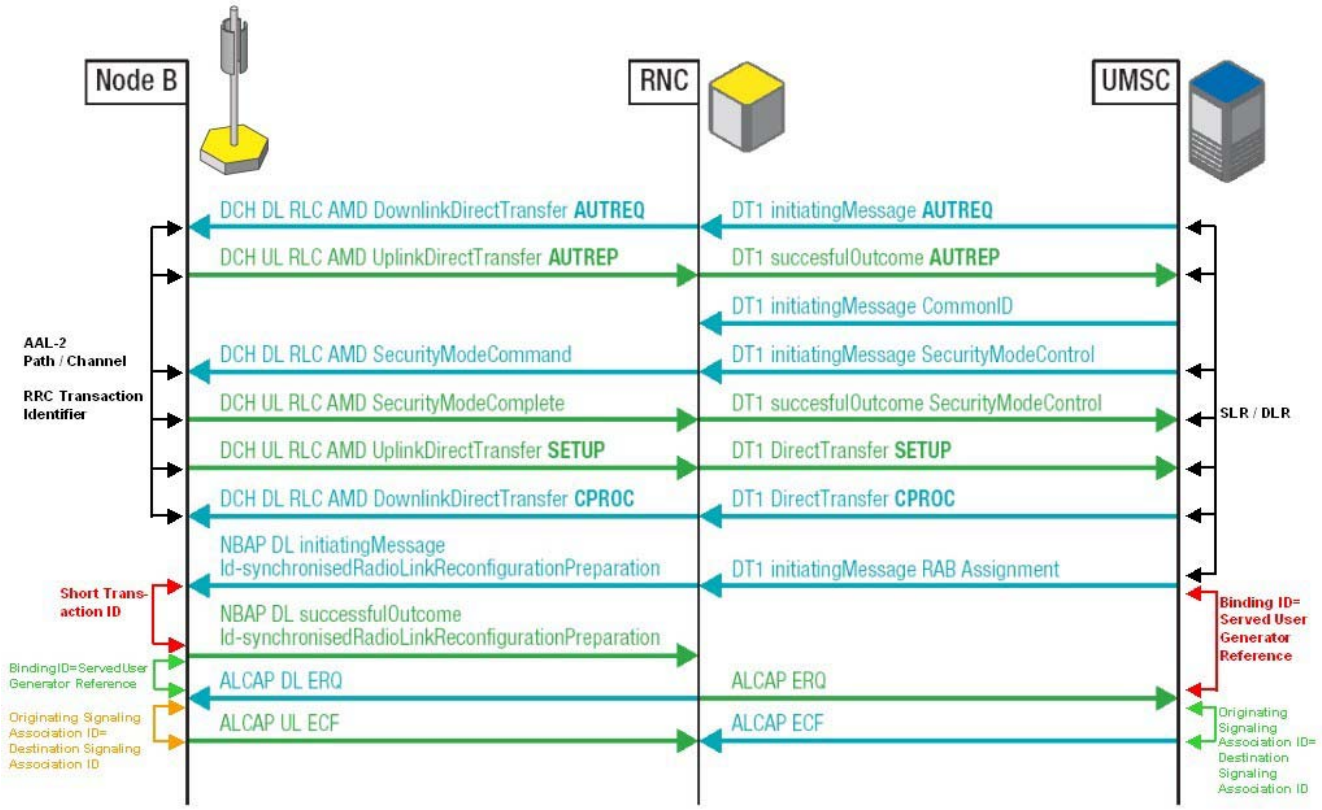

Figure 8: Mobile Oriented Call

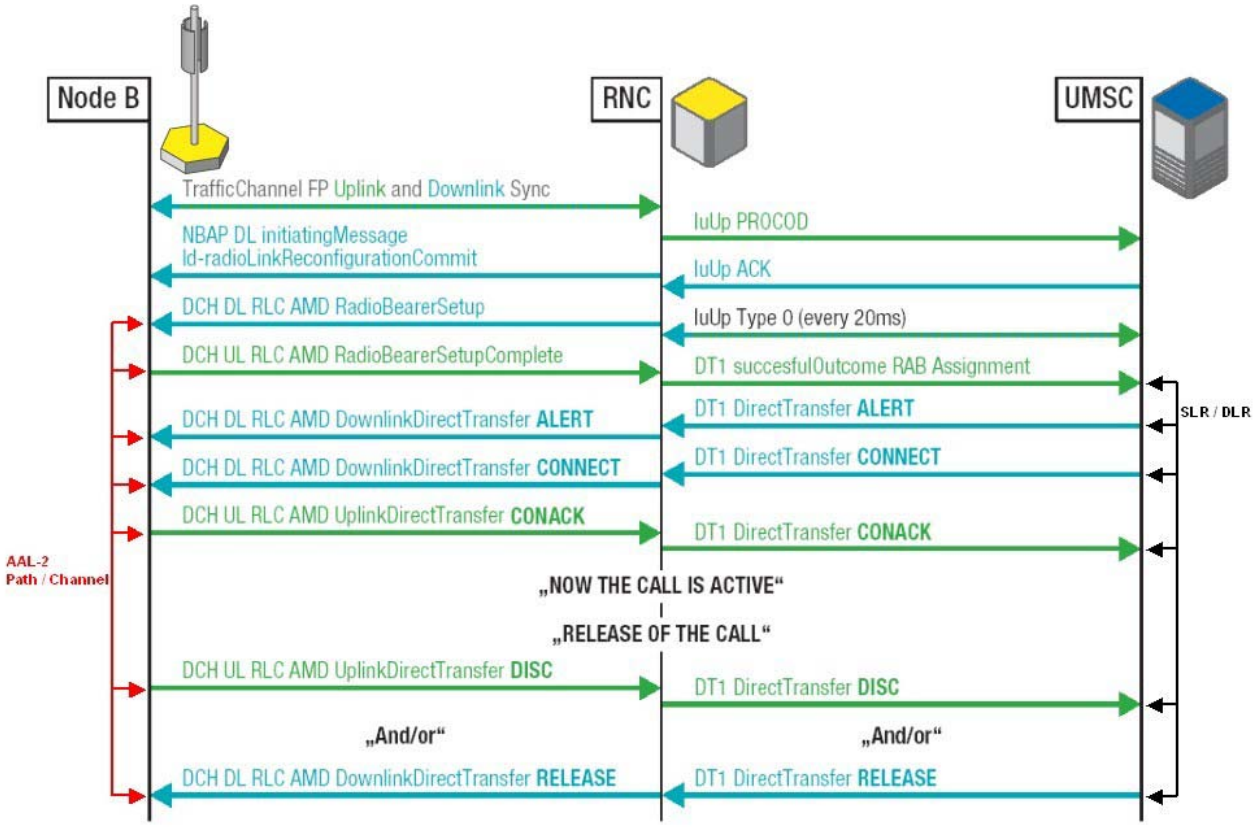

Figure 9: Mobile Oriented Call

Figure 9 illustrates in detail the establishment of the radio access bearer channel, which is required for the actual conversation. This configuration is required as well on the Iu-interface as on the Iub-interface and is the responsibility of the ALCAP. Please note the use of the AAL-2 path and channel to relate the following RRC-messages to each other. Of course, you may still want to use the RRC-transaction identifier for the same purpose.

Again, it is worth emphasizing that there would be no DISC-message if the call release would have been initiated by the network. In this case, the network would have sent just the REL-message. This way, the release procedure is simplified. Note how the RANAP initiating Message (Procedure Code: ‘id-Iu-Release’) invokes the upcoming release of the allocated bearer channels on the Iu- and Iub-interfaces.

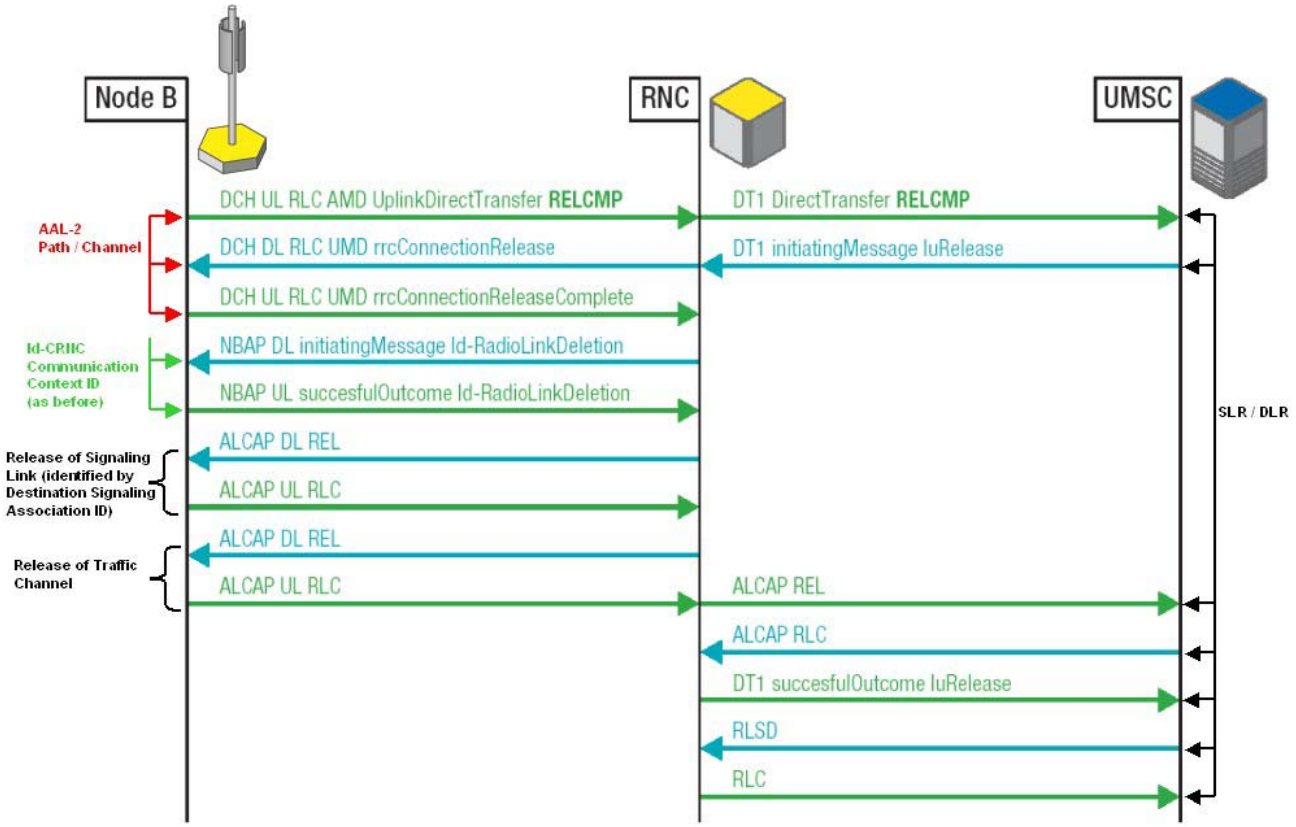

Figure 10: Mobile Oriented Call

Finally, ALCAP will de-allocate the bearer channels on Iu- and Iub-interface. Opposed to the scenario registration, this de-allocation is also required on the Iu-interface. For registration this was obviously not required.

PDP-Context Activation and Deactivation (Mobile Originating)

The last scenario is the packet-switched PDP-context activation, which is usually originated by the user equipment. Please note the differences, and in particular, the similarities between circuit-switched call establishment and packet-switched PDP-context activation. Whether the mobile station intends to perform either procedure is identified already in the rrcConnection Request-message through the access reason (in this case 'originating background call').

The message flow in Figure 11 is quite similar to what is already known from the registration and mobile oriented call scenario. Obviously, the peer of the mobile station will be in this case the SGSN rather than the MSC. Therefore the mobile station will identify itself through the P-TMSI (if available) or the IMSI.
The packet data transfer itself is not illustrated when focused on the control plane.

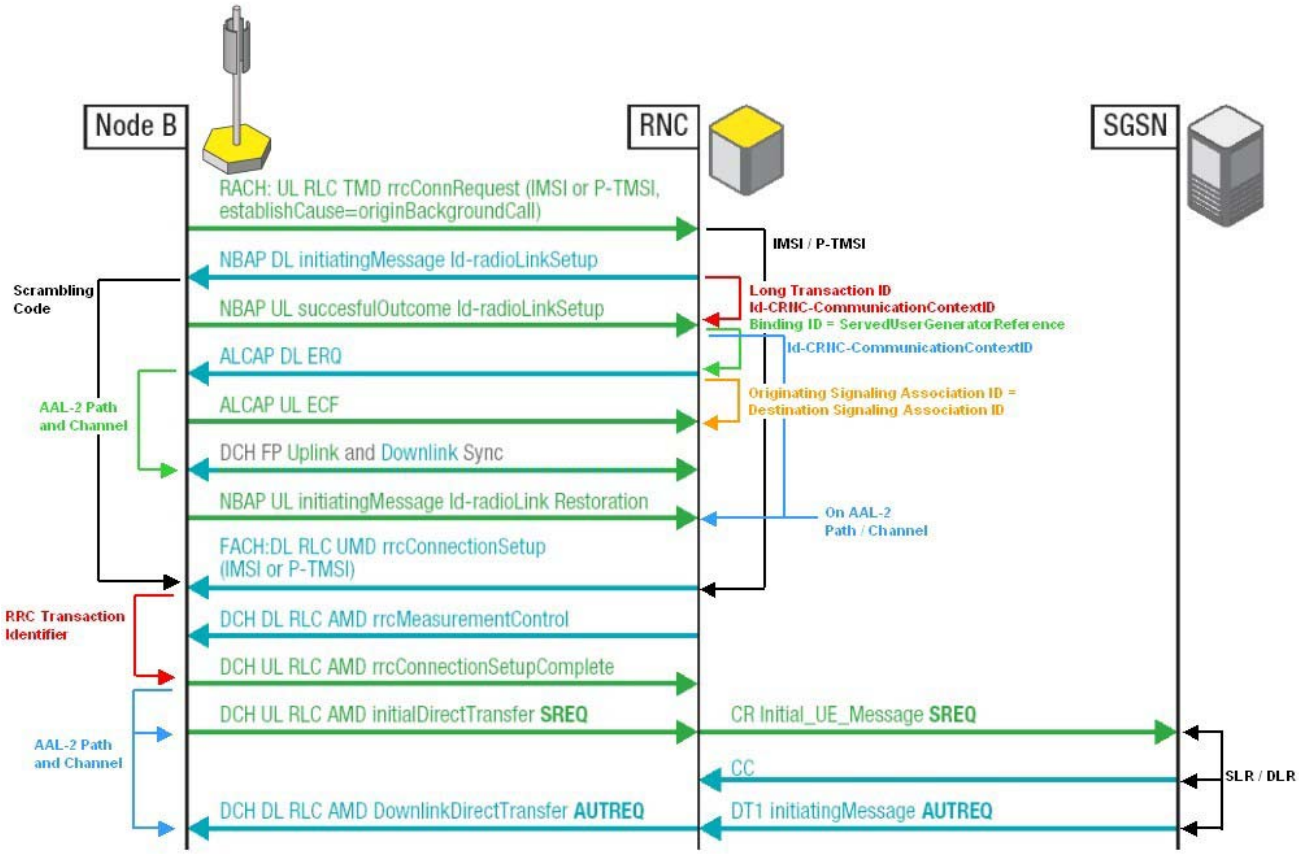

Figure 11: Mobile Originating PDP-Context Activation and Deactivation

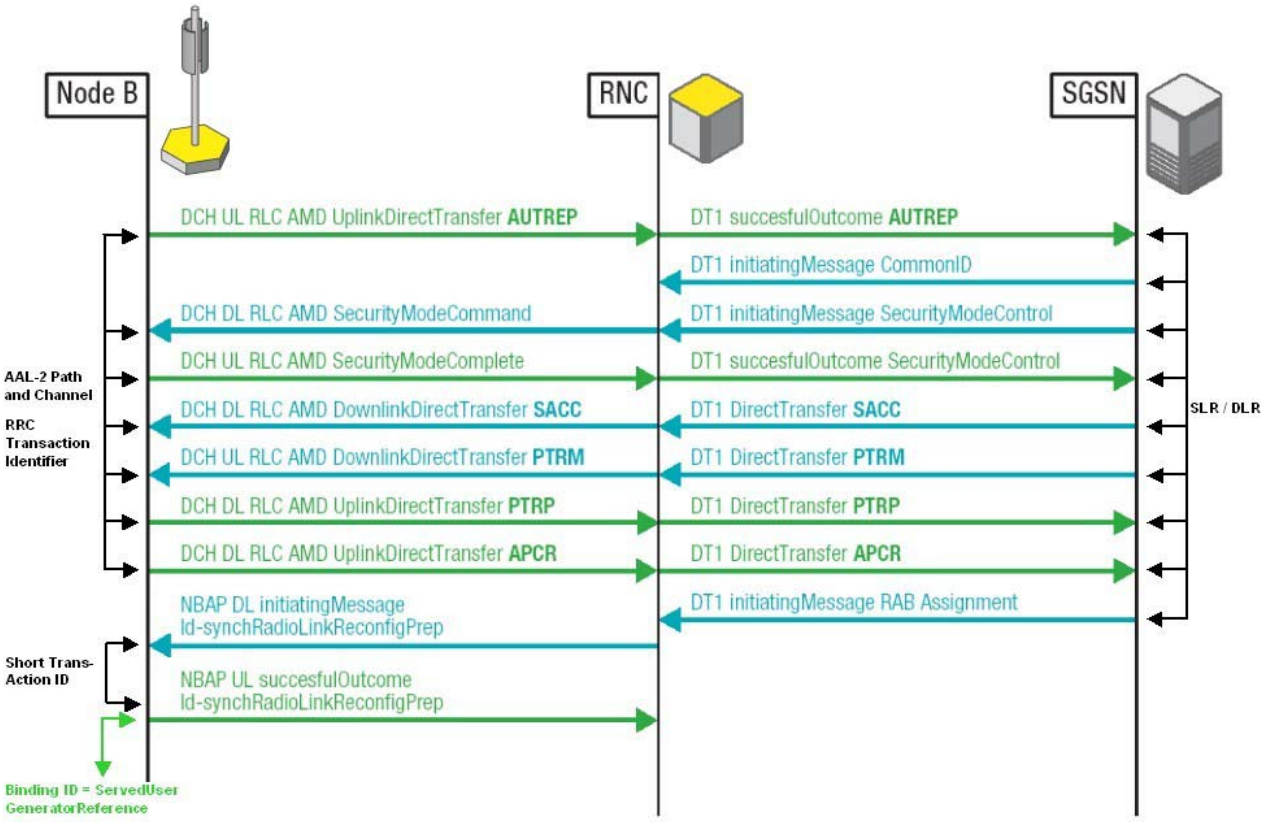

Figure 12: Mobile Originating PDP-Context Activation and Deactivation

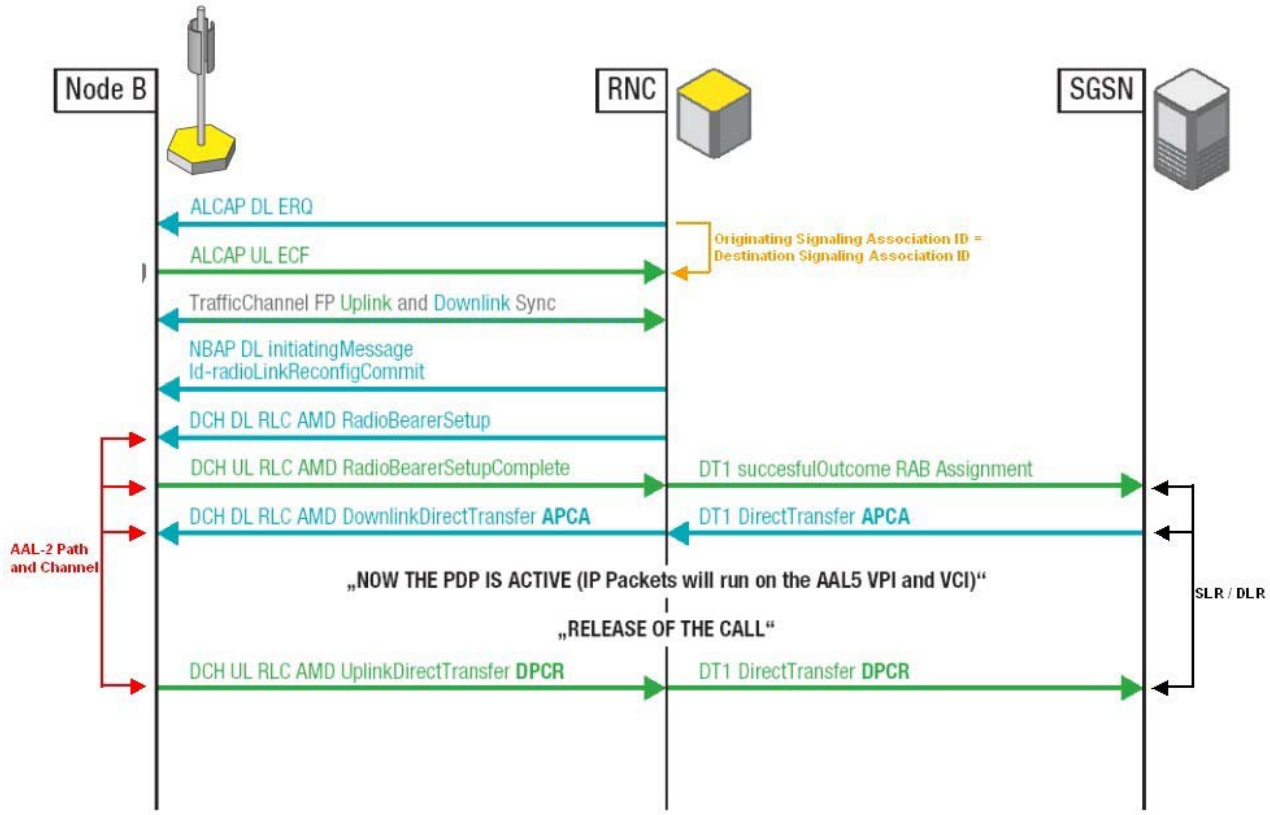

Figure 13: Mobile Originating PDP-Context Activation and Deactivation

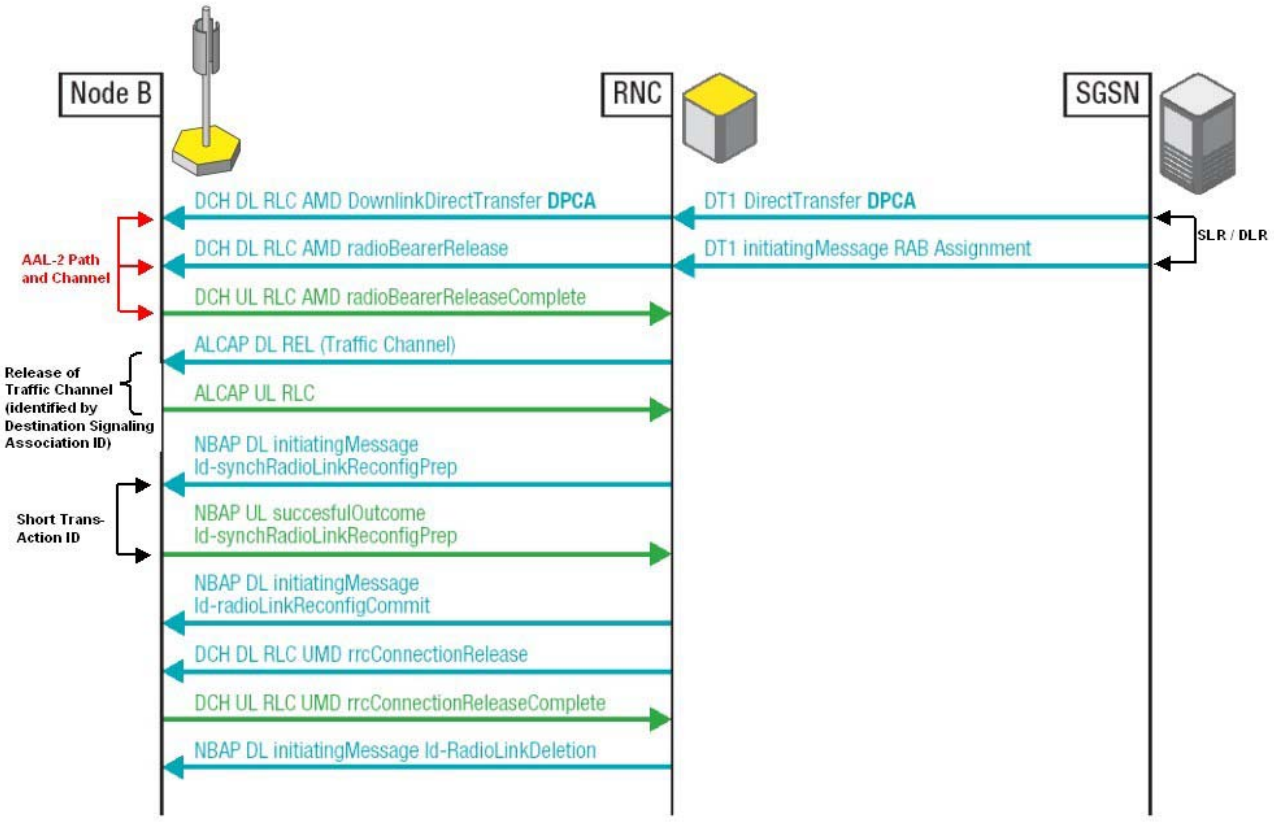

Figure 14: Mobile Originating PDP-Context Activation and Deactivation

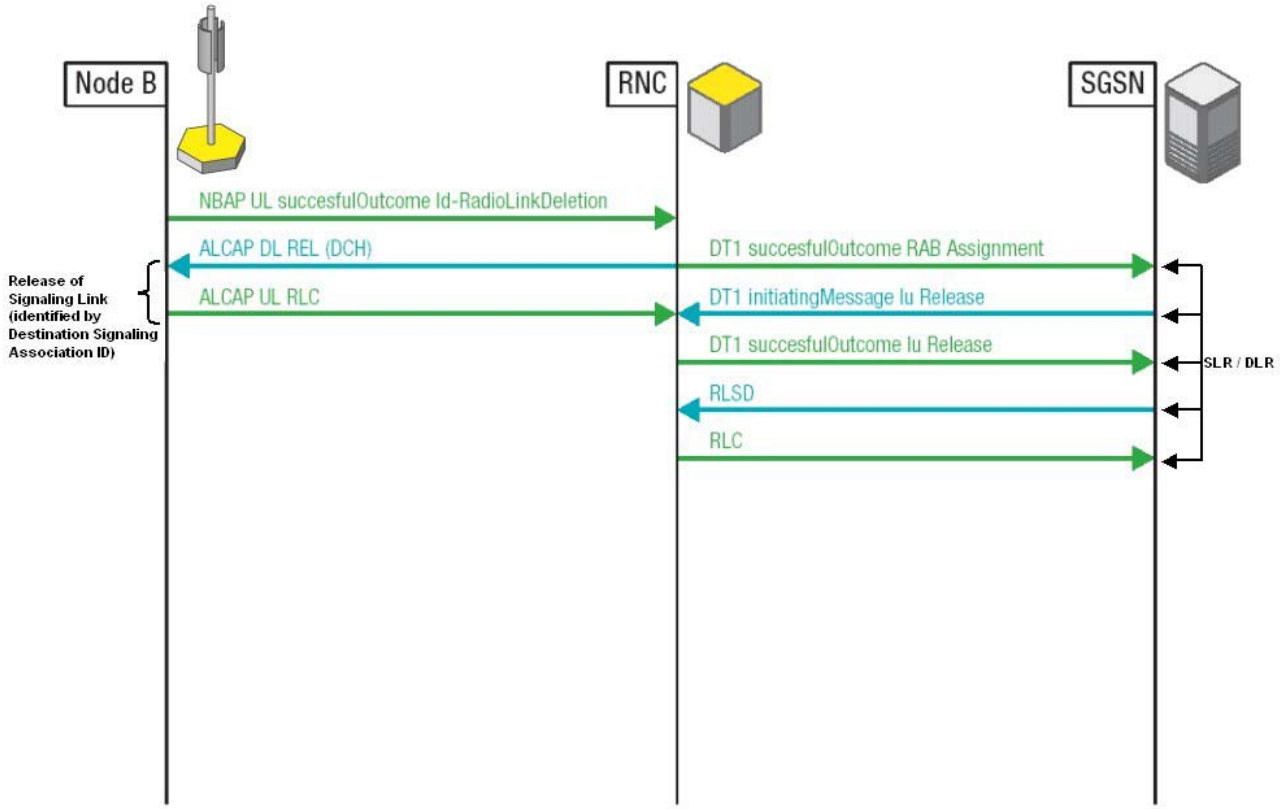

Figure 15: Mobile Originating PDP-Context Activation and Deactivation

Abbreviation List

AAL-2	ATM Adaptation Layer 2
AAL2L3	See ALCAP
AAL-5	ATM Adaptation Layer 5
ALCAP	Access Link Control Application Protocol (ITU-T Q.2630.1; Q.2630.2 (also referred to as AAL2L3)
REL	Release Request (⇔ ALCAP)
RLC	Release Confirm (⇔ SCCP / ALCAP)
RLSD	Released (SCCP)
CRNC	Controlling Radio Network Controller
AS	Access Stratum
CID	Channel Identifier
ASN.1	Abstract Syntax Notation 1 (ITU-T X.690)
ATM	Asynchronous Transfer Mode
DRNC	Drift Radio Network Controller
EDGE	Enhanced Data Rates for GSM Evolution
ERQ	ALCAP: Establishment Request
FACH	Forward Link Access Channel
GGSN	Gateway GPRS Support Node
PROCOD	Procedure Coding (3GTS 25.415)
GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GSM	Global Systems for Mobile Communications
GSMS	Short Message Services through GPRS (⇔ packet-switched transmission)
HLR	Home Location Register
IP	Internet Protocol
MAC	Medium Access Control (3GTS 25.321)
NAS	Non-Access Stratum
NBAP	Node B Application Protocol (3GTS 25.433)
PCH	Paging Channel
PCU	Packet Control Unit
PDCP	Packet Data Convergence Protocol (3GTS 25.323)
PDP	Packet Data Protocol
PER	Packed Encoding Rules (ITU-T X.691)
QoS	Quality of Service
RACH	Random Access Channel
RANAP	Radio Access Network Application Part (3GTS 25.413)
RLC	Radio Link Control (3GTS 25.322)

RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control (3GTS 25.331)
SGSN	Serving GPRS Support Node
SLR	Source Local Reference (SCCP)
DLR	Destination Local Reference (SCCP)
SCCP	Signaling Connection Control Part (ITU-T Q.710 – Q714)
SM	Session Management
SMS	Short Message Service
SRNC	Serving Radio Network Controller
SSCOP	Service Specific Connection Oriented Protocol (ITU-T Q.2110)
TBF	Temporary Block Flow
TCP	Transmission Control Protocol
TLLI	Temporary Logical Link Identifier
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System for the time beyond the year 2000
UTRAN	UMTS Terrestrial Radio Access Network
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
W-CDMA	Wideband Code Division Multiple Access