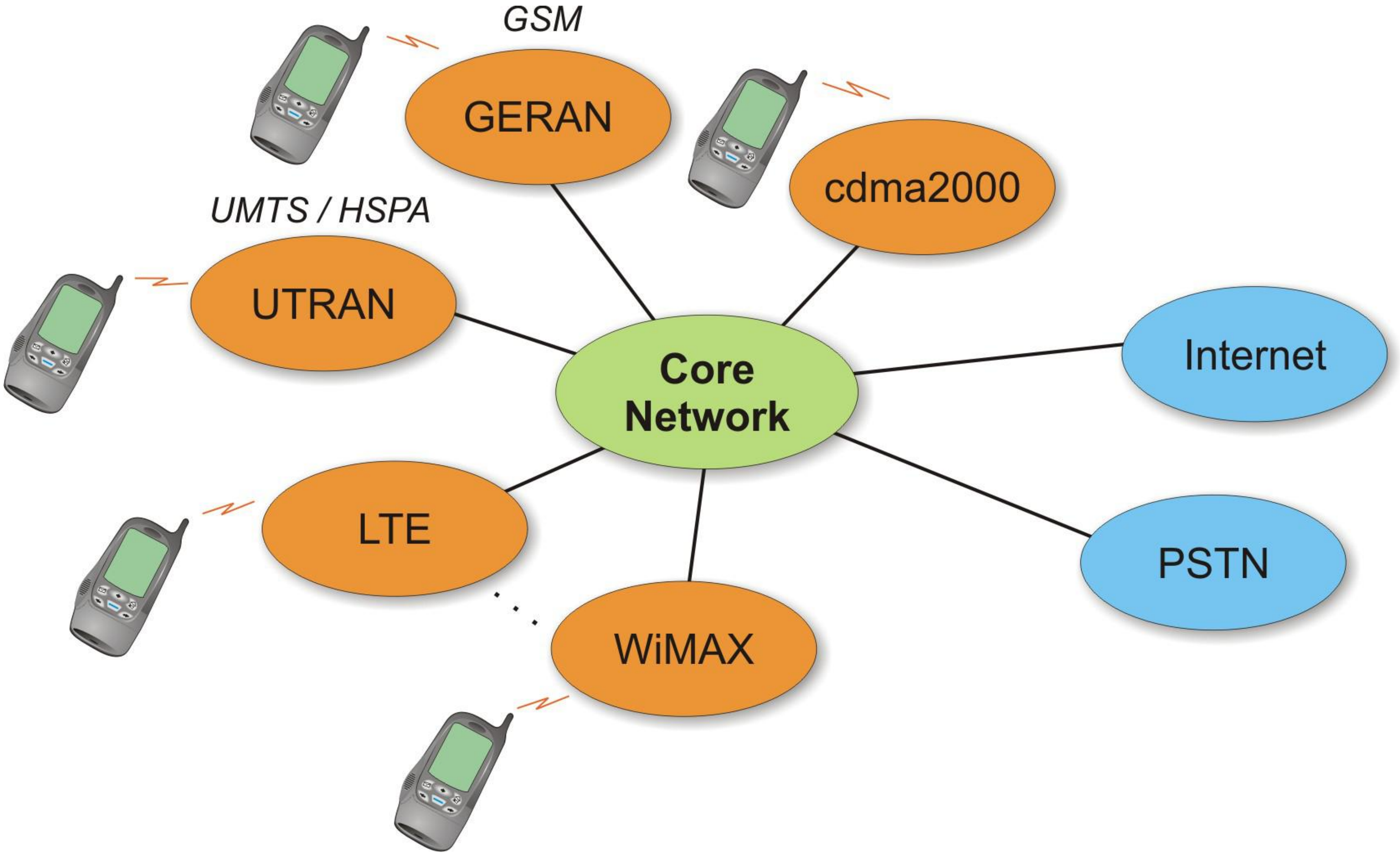
Wireless Network Optimization with Wireshark

Gunnar Heine / INACON
Sharkfest in Palo Alto
Tuesday June 16, 2009

The Wireless Environment



Some Details about the different Access Networks

- **GERAN (1991 - ..)**
  The GSM EDGE Radio Access Network is based on TDMA and was originally standardized by ETSI. It represents the most successful mobile standard to date with app. 2 billion subscribers worldwide. Its major application is voice traffic but through GPRS and EGPRS, GSM also provides packet-switched services.

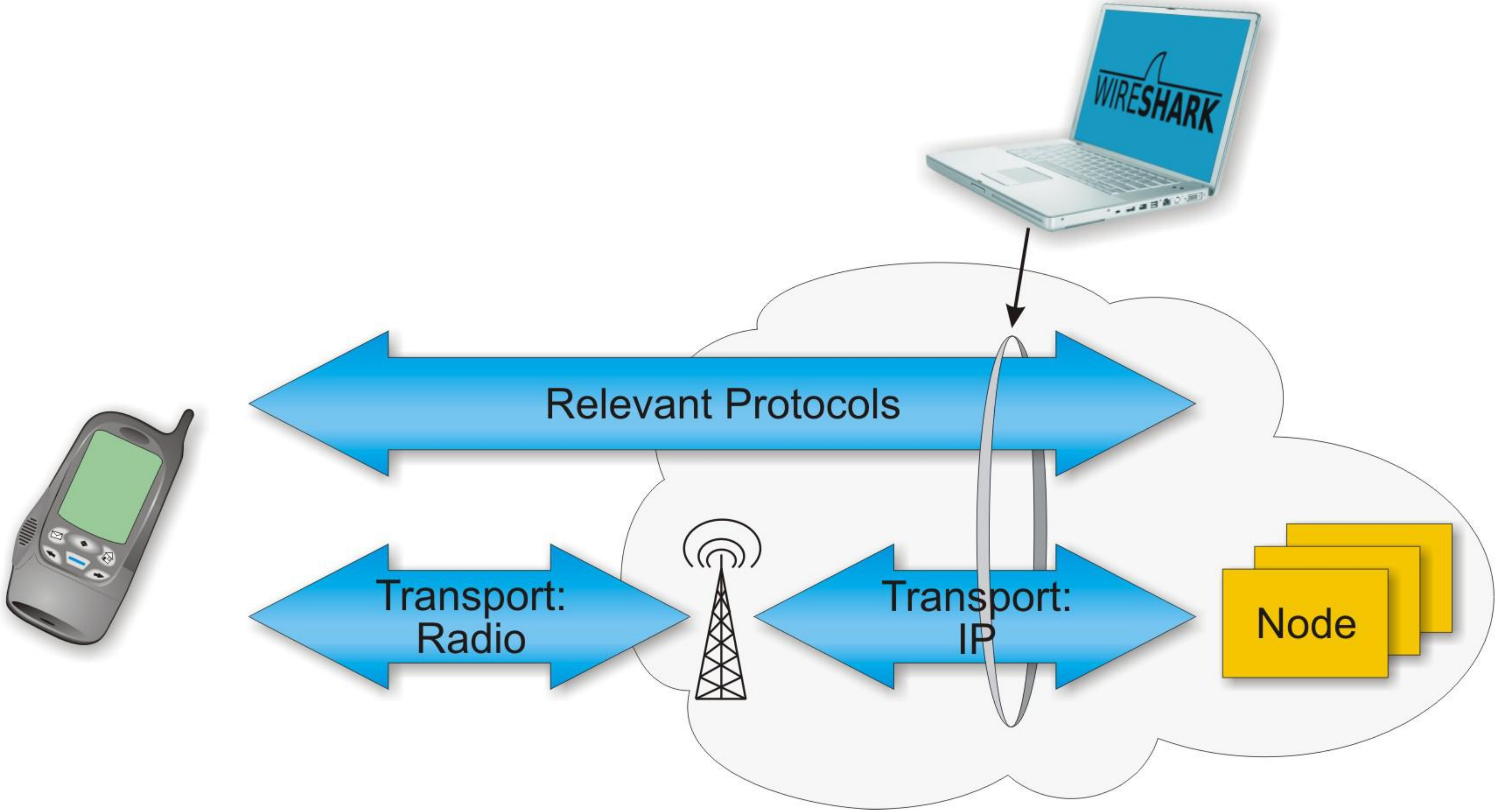
- **UTRAN (2001 - ..)**
  UMTS is based on W-CDMA and was the first project of 3GPP. The system was intended to replace the GSM but till today, UMTS and GSM usually coexist. UMTS was enhanced through HSDPA and HSUPA which improve its suitability for bursty IP-traffic.

- **LTE (2010? - ..)**
  Long Term Evolution was originally the answer of 3GPP to WiMAX. It is based on OFDMA and is the first 3GPP-network that does not offer circuit-switched voice services. It is fully IP-centric and offers multiple times the throughput rates of GSM/GPRS and UMTS.

- **WiMAX (2008 - ..)**
  WiMAX as mobile standard has its origins in an IEEE-based microwave standard that dates back to the year 2001. In its mobile variant it uses OFDMA. The commissioning of WiMAX-networks was frequently delayed and suffered from various technical teething diseases. In that respect, WiMAX lost a lot of its momentum and credibility.

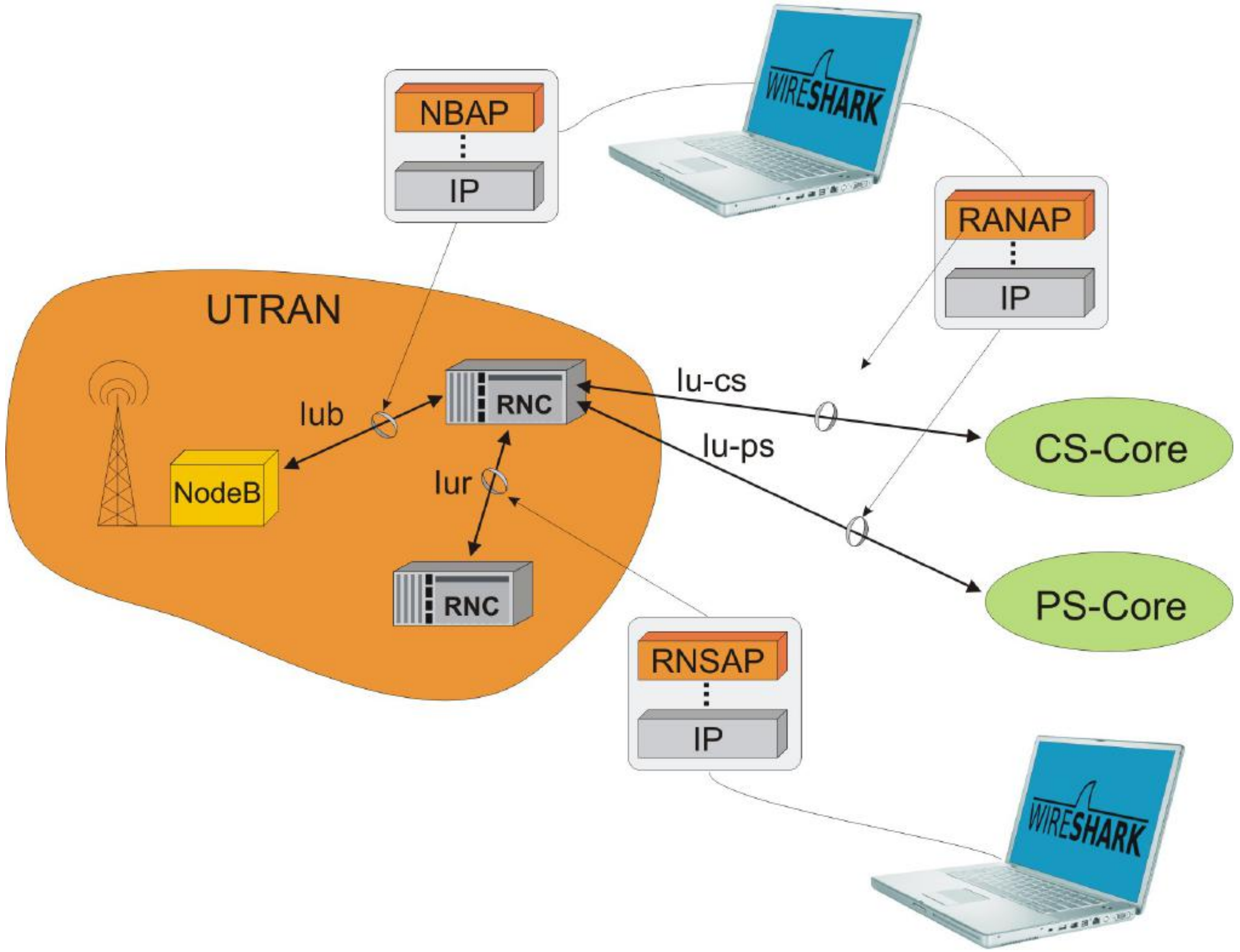
- **cdma2000 (2001 - ..)**
  Like UMTS, cdma2000 is based on W-CDMA. It is predominantly a US-based standard and has its origins in IS-95. Support for cdma2000 is declining with major operators migrating to UMTS and LTE.

Why can Wireshark be used in Mobile / Wireless?

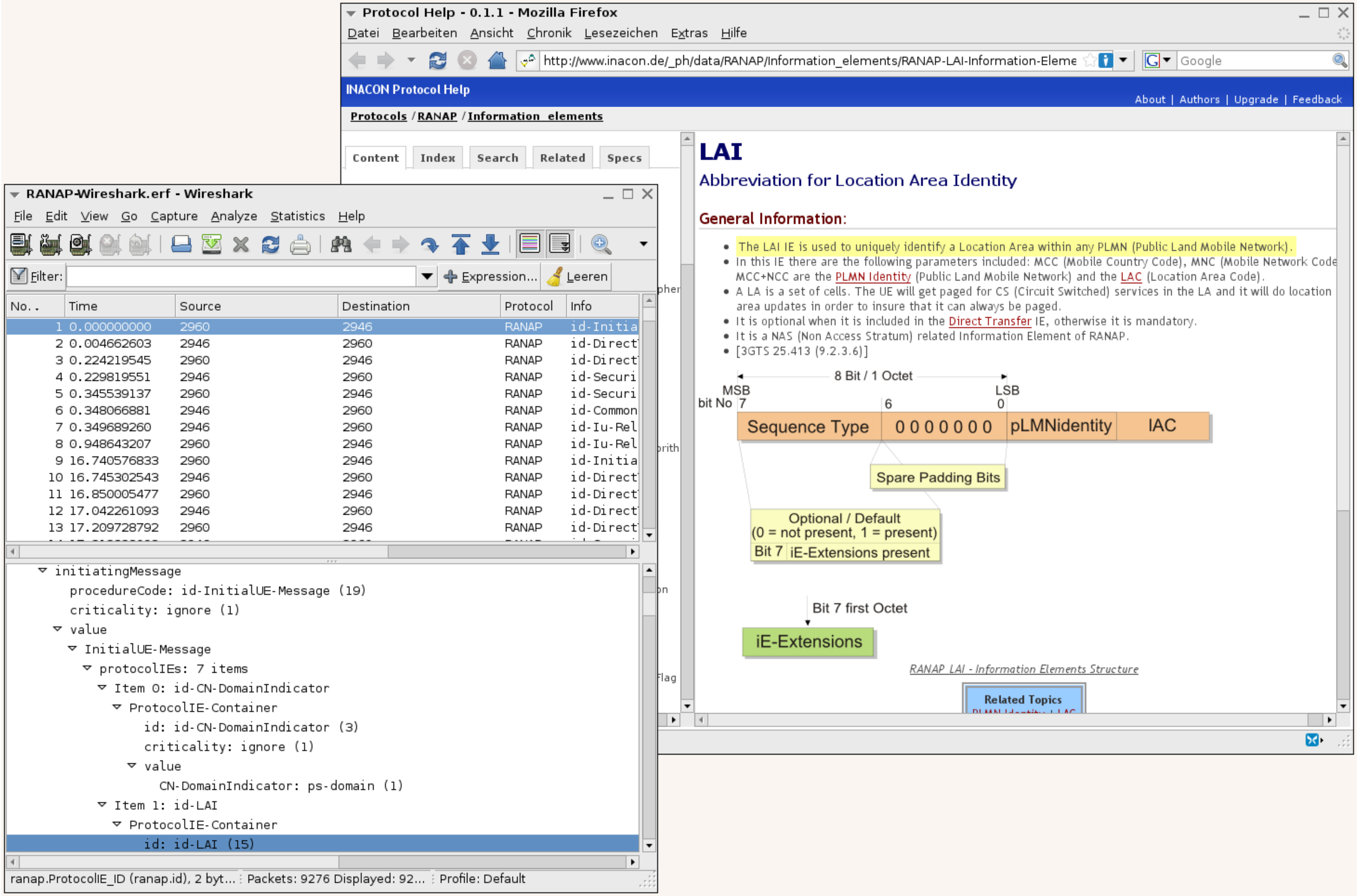


The Protocol Suite of the Mobile Environment

Example 1: UTRAN Protocols



Screenshot: Wireshark, RANAP & Protocol Help


Protocol Help - 0.1.1 - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.inacon.de/_ph/data/RANAP/Information_elements/RANAP-LAI-Information-Eleme
Google
INACON Protocol Help
About | Authors | Upgrade | Feedback
Protocols / RANAP / Information_elements
Content
Index
Search
Related
Specs
RANAP-Wireshark.erf - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Leeren

No.	Time	Source	Destination	Protocol	Info
1	0.000000000	2960	2946	RANAP	id-Initia
2	0.004662603	2946	2960	RANAP	id-Direct
3	0.224219545	2960	2946	RANAP	id-Direct
4	0.229819551	2946	2960	RANAP	id-Securi
5	0.345539137	2960	2946	RANAP	id-Securi
6	0.348066881	2946	2960	RANAP	id-Common
7	0.349689260	2946	2960	RANAP	id-Iu-Rel
8	0.948643207	2960	2946	RANAP	id-Iu-Rel
9	16.740576833	2960	2946	RANAP	id-Initia
10	16.745302543	2946	2960	RANAP	id-Direct
11	16.850005477	2960	2946	RANAP	id-Direct
12	17.042261093	2946	2960	RANAP	id-Direct
13	17.209728792	2960	2946	RANAP	id-Direct

```
▽ initiatingMessage
    procedureCode: id-InitialUE-Message (19)
    criticality: ignore (1)
  ▽ value
    ▽ InitialUE-Message
      ▽ protocolIEs: 7 items
        ▽ Item 0: id-CN-DomainIndicator
          ▽ ProtocolIE-Container
              id: id-CN-DomainIndicator (3)
              criticality: ignore (1)
            ▽ value
                CN-DomainIndicator: ps-domain (1)
        ▽ Item 1: id-LAI
          ▽ ProtocolIE-Container
              id: id-LAI (15)
```

ranap.ProtocolIE_ID (ranap.id), 2 byt... Packets: 9276 Displayed: 92... Profile: Default

LAI

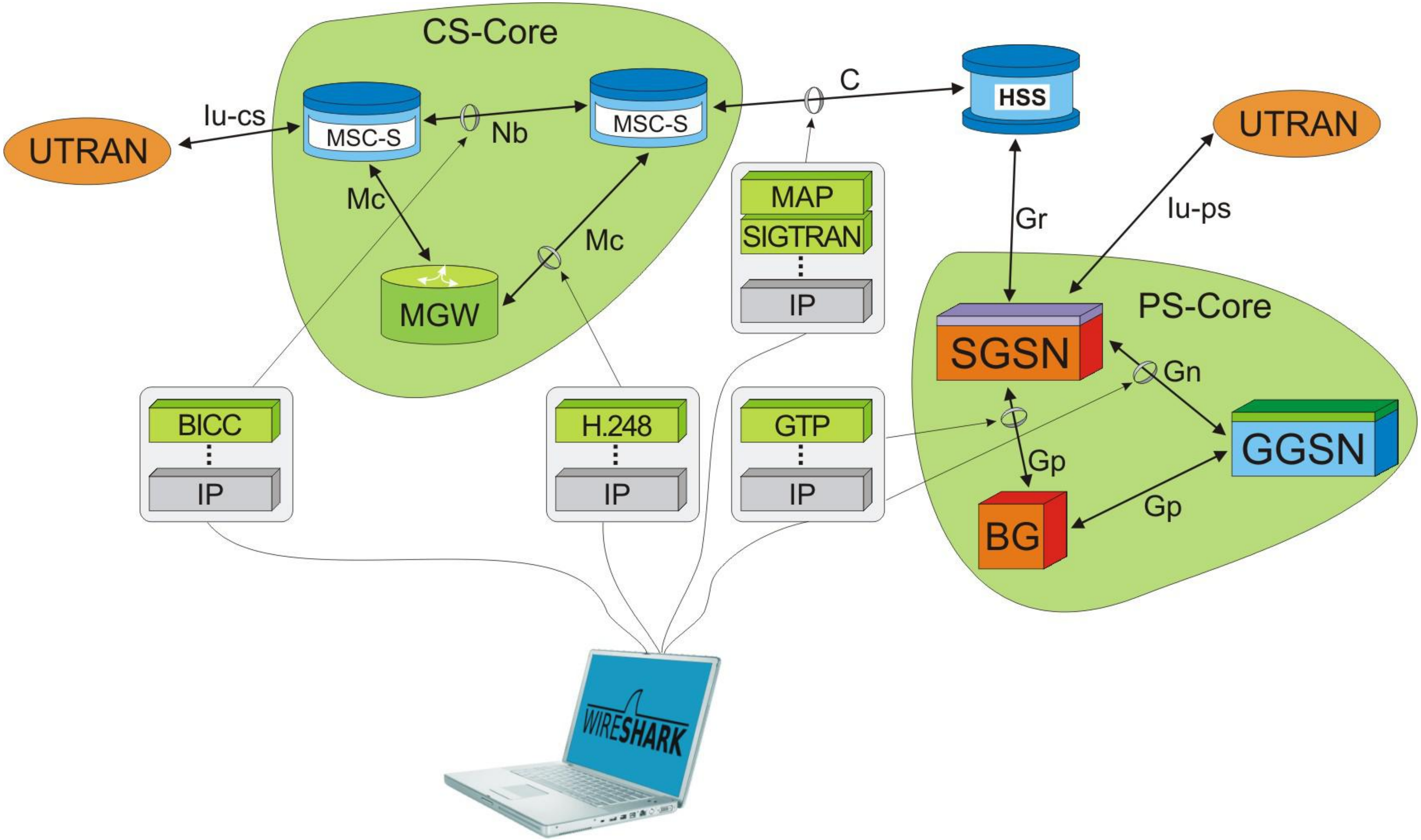
Abbreviation for Location Area Identity

General Information:

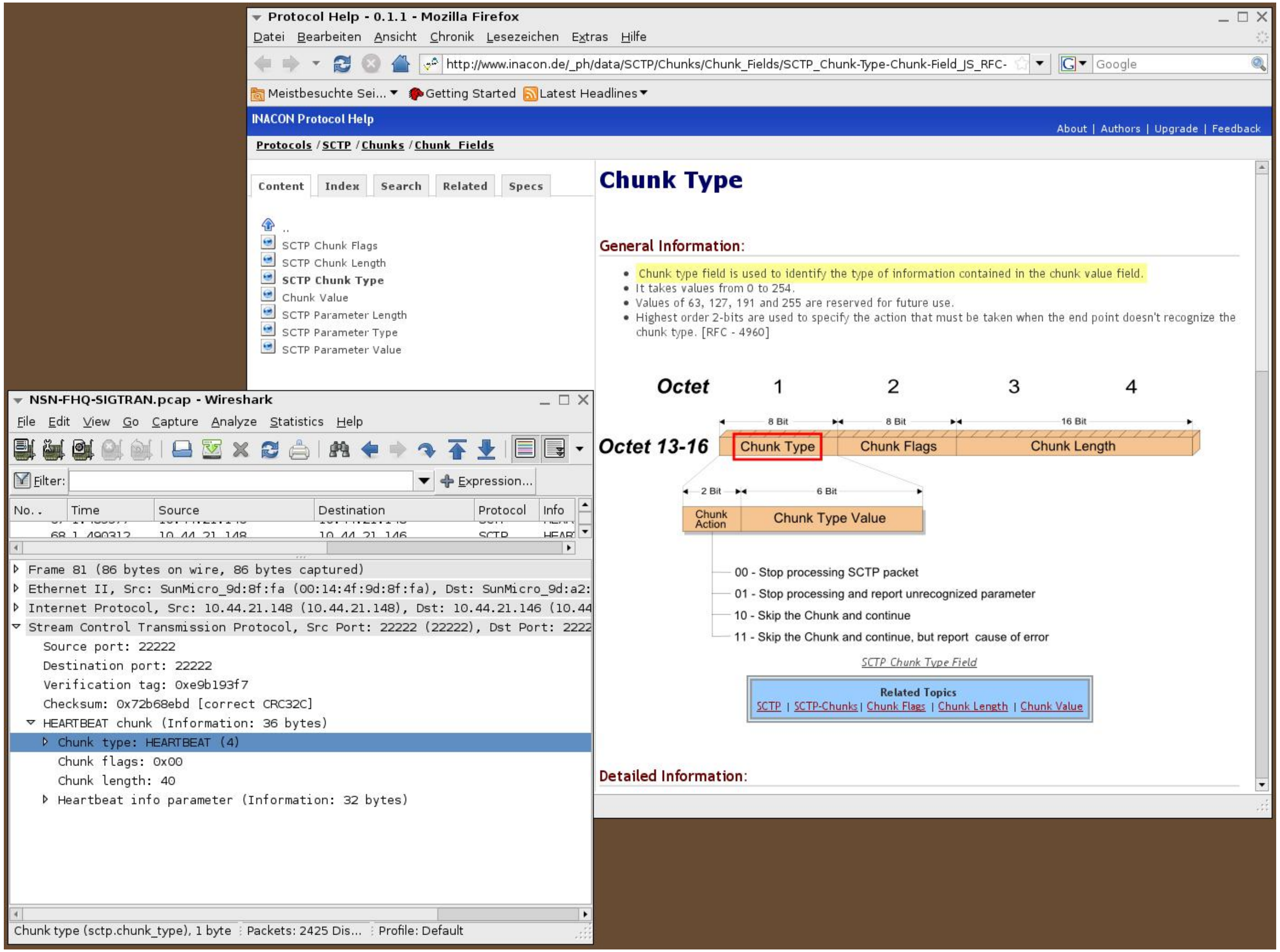
- The LAI IE is used to uniquely identify a Location Area within any PLMN (Public Land Mobile Network).
- In this IE there are the following parameters included: MCC (Mobile Country Code), MNC (Mobile Network Code MCC+NCC are the PLMN Identity (Public Land Mobile Network) and the LAC (Location Area Code).
- A LA is a set of cells. The UE will get paged for CS (Circuit Switched) services in the LA and it will do location area updates in order to insure that it can always be paged.
- It is optional when it is included in the Direct Transfer IE, otherwise it is mandatory.
- It is a NAS (Non Access Stratum) related Information Element of RANAP.
- [3GTS 25.413 (9.2.3.6)]

RANAP LAI - Information Elements Structure

Example 2: Core Network (circuit- and packet-switched)



Screenshot: Wireshark, SIGTRAN & Protocol Help



Protocol Help - 0.1.1 - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.inacon.de/_ph/data/SCTP/Chunks/Chunk_Fields/SCTP_Chunk-Type-Chunk-Field_JS_RFC-
Google
Meistbesuchte Sei... Getting Started Latest Headlines
INACON Protocol Help
About | Authors | Upgrade | Feedback
Protocols / SCTP / Chunks / Chunk_Fields
Content Index Search Related Specs
..
SCTP Chunk Flags
SCTP Chunk Length
SCTP Chunk Type
Chunk Value
SCTP Parameter Length
SCTP Parameter Type
SCTP Parameter Value

Chunk Type

General Information:

- Chunk type field is used to identify the type of information contained in the chunk value field.
- It takes values from 0 to 254.
- Values of 63, 127, 191 and 255 are reserved for future use.
- Highest order 2-bits are used to specify the action that must be taken when the end point doesn't recognize the chunk type. [RFC - 4960]

Octet
1
2
3
4
8 Bit
8 Bit
16 Bit
Octet 13-16
Chunk Type
Chunk Flags
Chunk Length
2 Bit
6 Bit
Chunk Action
Chunk Type Value

00 - Stop processing SCTP packet

01 - Stop processing and report unrecognized parameter

10 - Skip the Chunk and continue

11 - Skip the Chunk and continue, but report cause of error

SCTP Chunk Type Field

Related Topics
SCTP | SCTP-Chunks | Chunk Flags | Chunk Length | Chunk Value

Detailed Information:

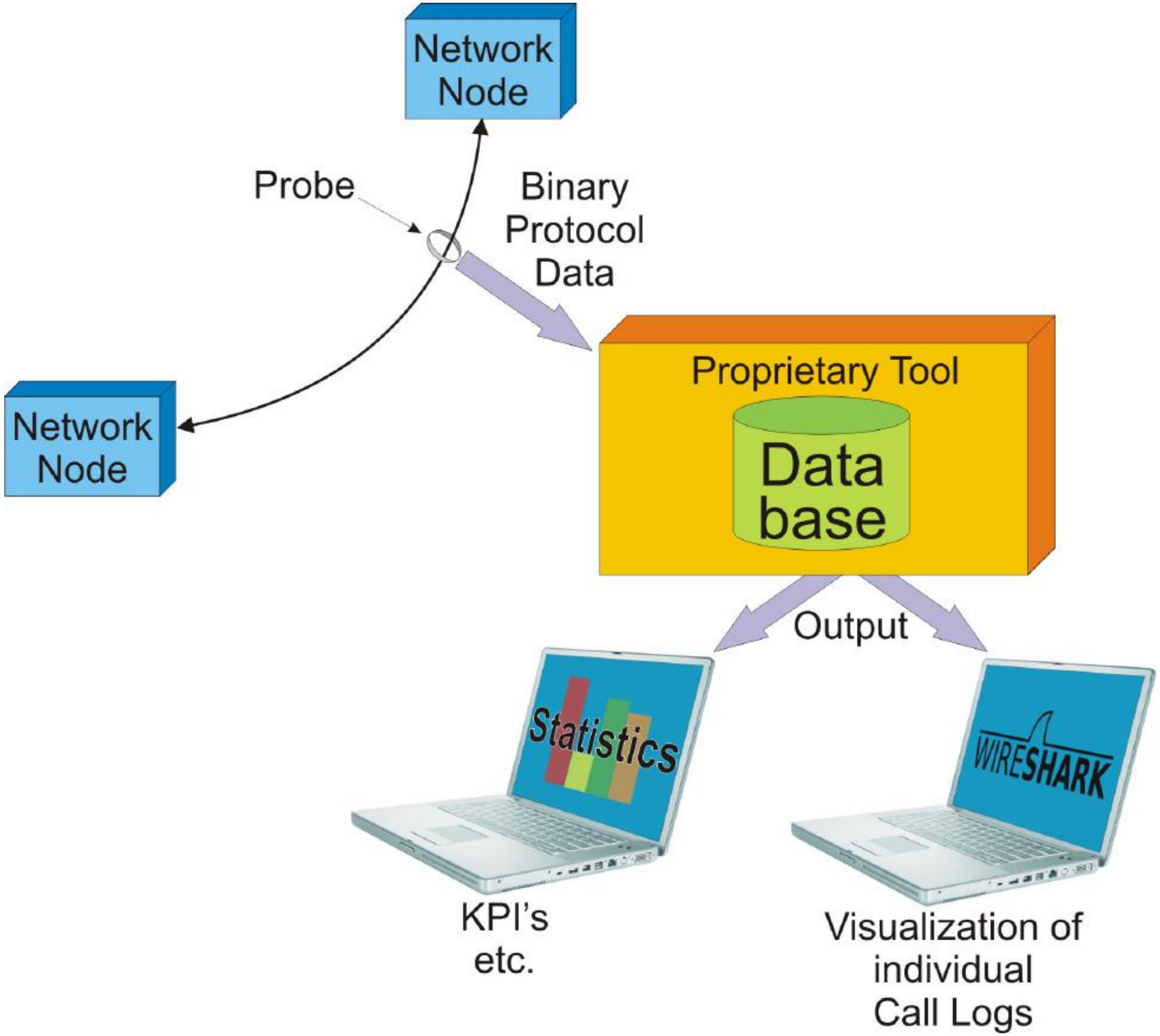
NSN-FHQ-SIGTRAN.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
No. . Time Source Destination Protocol Info

```
68 1.490312   10.44.21.148   10.44.21.146   SCTP   HEAR
```

```
▷ Frame 81 (86 bytes on wire, 86 bytes captured)
▷ Ethernet II, Src: SunMicro_9d:8f:fa (00:14:4f:9d:8f:fa), Dst: SunMicro_9d:a2:
▷ Internet Protocol, Src: 10.44.21.148 (10.44.21.148), Dst: 10.44.21.146 (10.44
▽ Stream Control Transmission Protocol, Src Port: 22222 (22222), Dst Port: 2222
    Source port: 22222
    Destination port: 22222
    Verification tag: 0xe9b193f7
    Checksum: 0x72b68ebd [correct CRC32C]
  ▽ HEARTBEAT chunk (Information: 36 bytes)
    ▷ Chunk type: HEARTBEAT (4)
      Chunk flags: 0x00
      Chunk length: 40
    ▷ Heartbeat info parameter (Information: 32 bytes)
```

Chunk type (sctp.chunk_type), 1 byte | Packets: 2425 Dis... | Profile: Default

WIRESHARK as Part of Complex Network Monitoring Tools



Network Node

Probe

Binary Protocol Data

Network Node

Proprietary Tool

Data base

Output

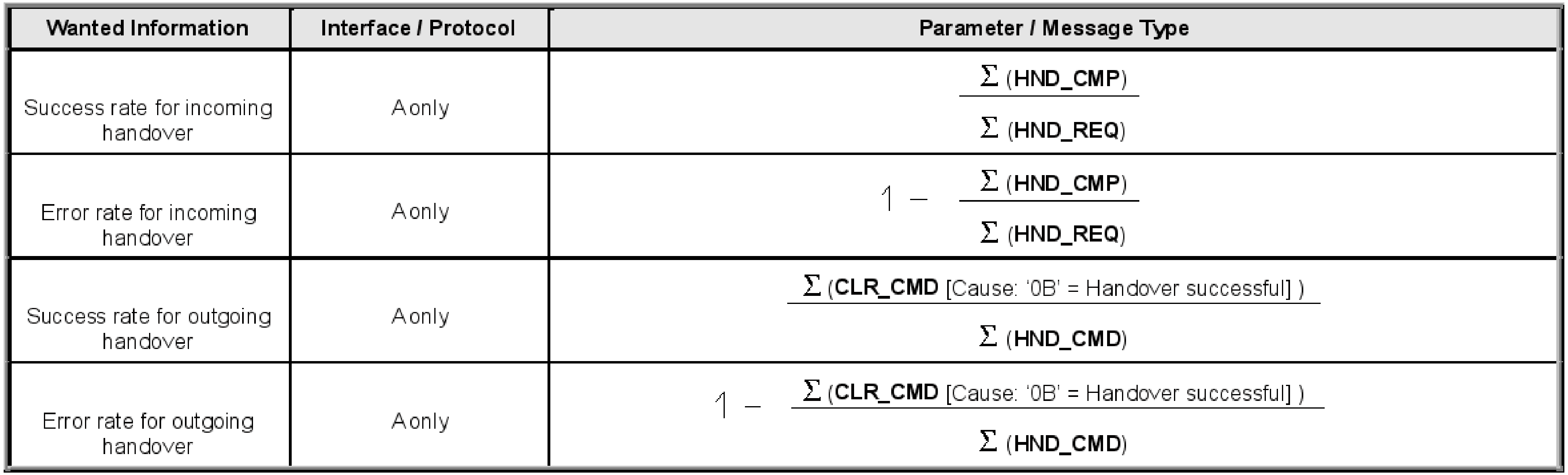
KPI's etc.

Visualization of individual Call Logs

(1) Important KPI's in the Mobile Environment

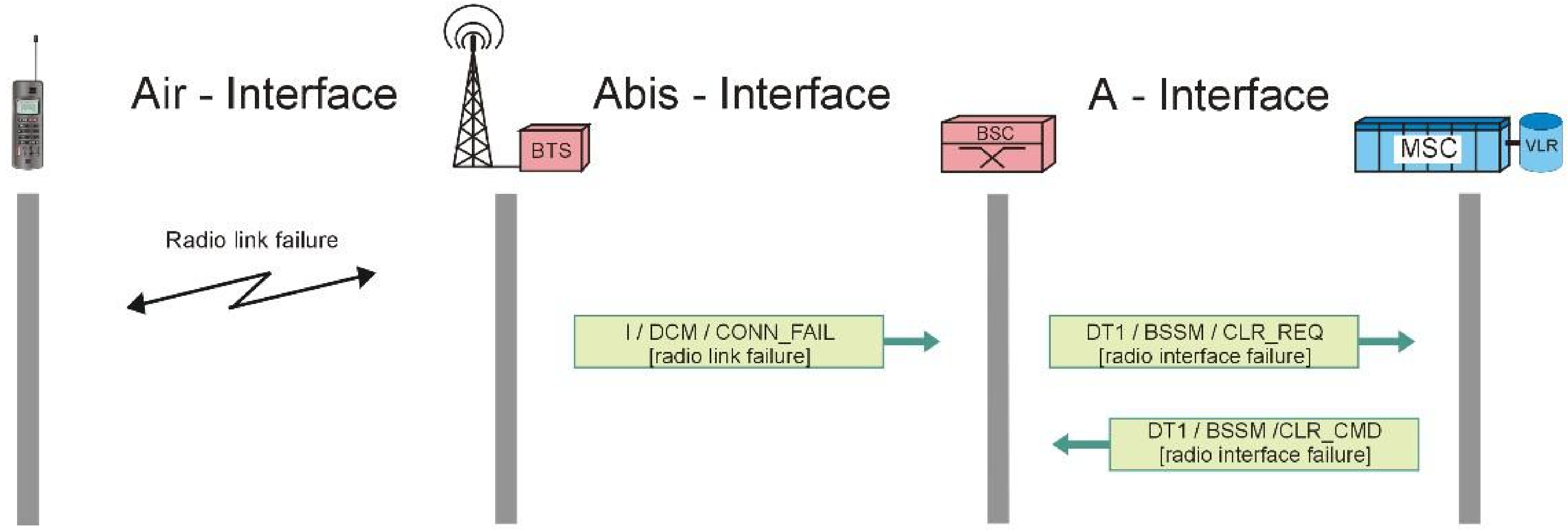
Wanted information	Interface / Protocol	Parameter / Message Type
Total of all MOC attempts (BTS / BSC)	Abis / A	$\sum(\textbf{CM\_SERV\_REQ})$
Total of all MTC attempts (BTS / BSC)	A / Abis	$\sum(\textbf{PAG\_RSP})$
Total of the successful incoming handover	A only	$\sum(\textbf{HND\_CMP})$
Total of the outgoing handover	A only	$\sum(\textbf{CLR\_CMD}\ [\text{Cause: '0B' = Handover successful}])$
Success rate for MOC's (BSS / BTS)	A / Abis	$\dfrac{\sum(\textbf{ALERT}\ [\text{from MSC} \rightarrow \text{MS}]) + \sum(\textbf{PROGRESS})}{\sum(\textbf{CM\_SERV\_REQ}\ [\text{Establishm. Cause = MOC}])}$
Error rate for MOC's (BSS / BTS)	A / Abis	$1 - \dfrac{\sum(\textbf{ALERT}\ [\text{from MSC} \rightarrow \text{MS}]) + \sum(\textbf{PROGRESS})}{\sum(\textbf{CM\_SERV\_REQ}\ [\text{Establishm. Cause = MOC}])}$
Success rate for MTC's (BSS / BTS)	A / Abis	$\dfrac{\sum(\textbf{ALERT}\ [\text{from MS} \rightarrow \text{MSC}])}{\sum(\textbf{PAG\_RSP})}$
Error rate for MTC's (BSS / BTS)	A / Abis	$1 - \dfrac{\sum(\textbf{ALERT}\ [\text{from MS} \rightarrow \text{MSC}])}{\sum(\textbf{PAG\_RSP})}$

(2) Important KPI's in the Mobile Environment

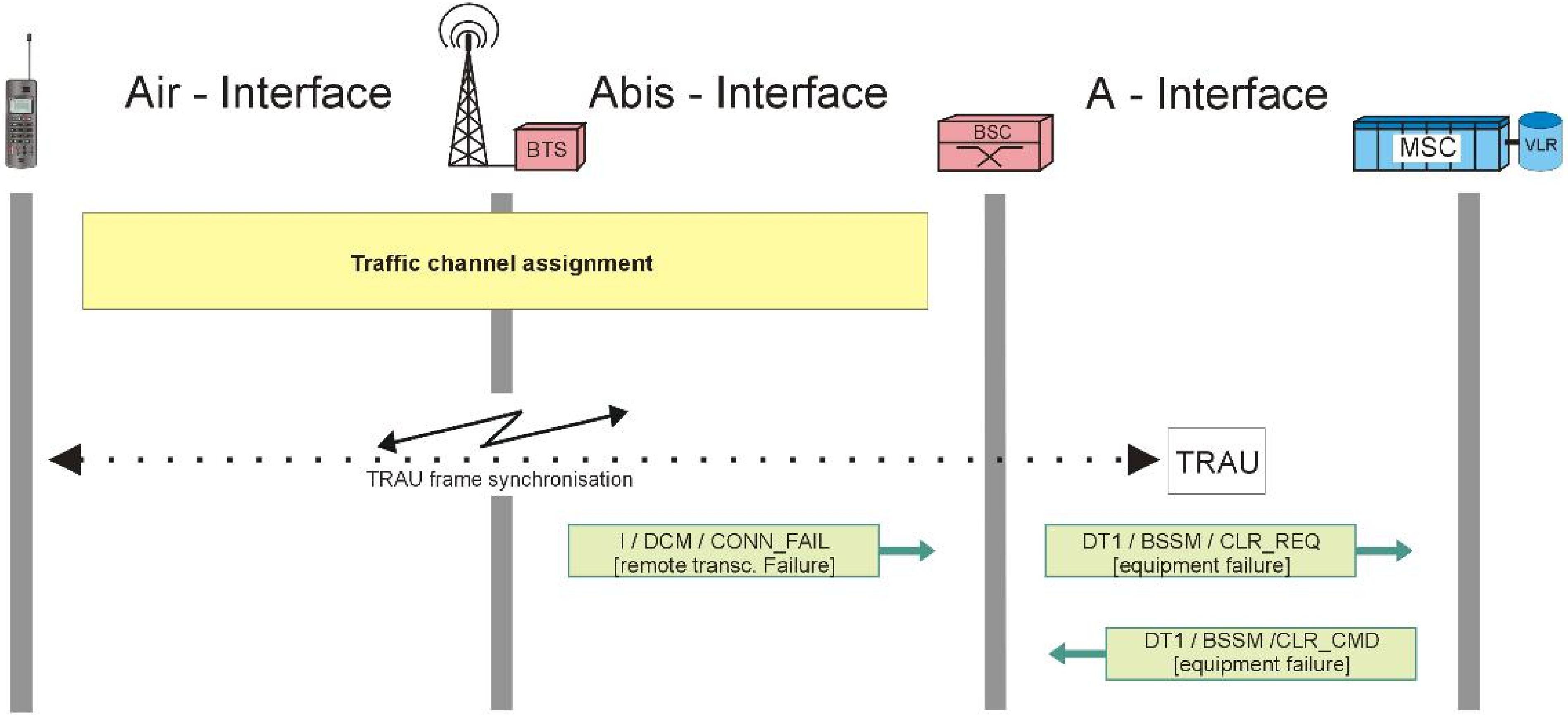


Wanted Information	Interface / Protocol	Parameter / Message Type
Success rate for incoming handover	A only	$\dfrac{\Sigma\,(\textbf{HND\_CMP})}{\Sigma\,(\textbf{HND\_REQ})}$
Error rate for incoming handover	A only	$1 - \dfrac{\Sigma\,(\textbf{HND\_CMP})}{\Sigma\,(\textbf{HND\_REQ})}$
Success rate for outgoing handover	A only	$\dfrac{\Sigma\,(\textbf{CLR\_CMD}\text{ [Cause: `0B' = Handover successful] })}{\Sigma\,(\textbf{HND\_CMD})}$
Error rate for outgoing handover	A only	$1 - \dfrac{\Sigma\,(\textbf{CLR\_CMD}\text{ [Cause: `0B' = Handover successful] })}{\Sigma\,(\textbf{HND\_CMD})}$

(1) Typical Issues in the Mobile Environment


Air - Interface
BTS
Abis - Interface
BSC
A - Interface
MSC
VLR
Radio link failure
I / DCM / CONN_FAIL [radio link failure]
DT1 / BSSM / CLR_REQ [radio interface failure]
DT1 / BSSM /CLR_CMD [radio interface failure]

(2) Typical Issues in the Mobile Environment



Future Update Ideas for Wireshark

- **Semi-automatic interpretation of mobile log files**
  similar to existing TCP-traffic evaluation tools
  could be used to ease logfile interpretation

- **Fast integration of latest mobile standards (e.g. LTE-protocols)**

- **Integration of INACON's protocol help**
  to ease logfile interpretation in any protocol environment

Thank You!