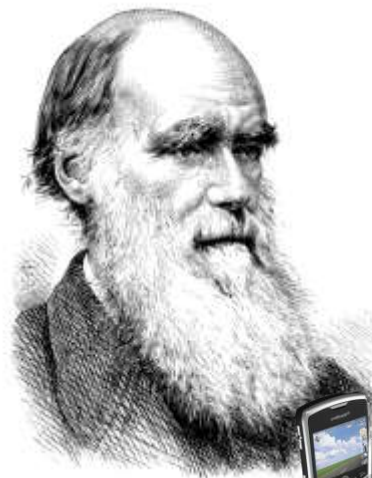


LTE vs. Darwin: Return of the SON

Hendrik Schmidt <hschmidt@ernw.de>

Brian Butterly <butterly@ernw.de>



Who we are



- Old-school network geeks, working as security researchers for
- Germany based ERNW GmbH
 - Independent
 - Deep technical knowledge
 - Structured (assessment) approach
 - Business reasonable recommendations
 - We understand corporate
- Blog: *www.insinuator.net*
- Conference: *www.troopers.de*
- Telco research project: *www.asmonia.de*

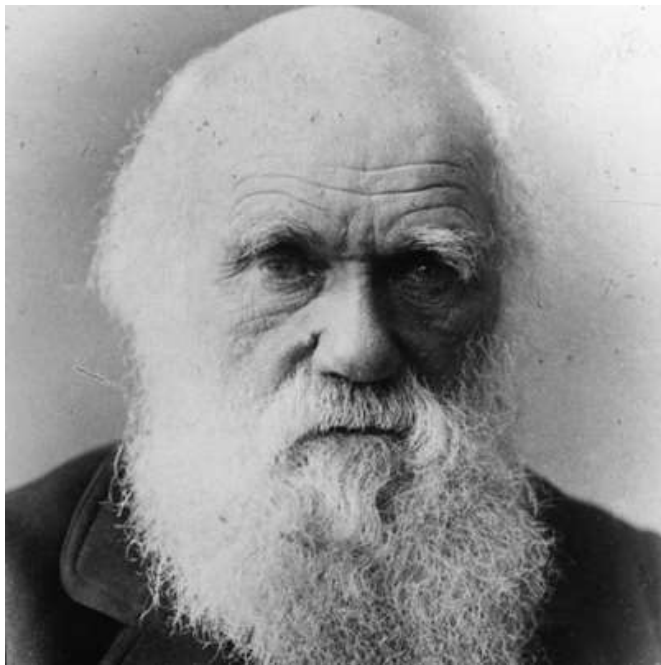
Motivation - Long Term Evolution (LTE)



- 4G wireless technology for mobile communication

- The 4G standard introduces a lot of new technologies providing modern services to the customer.
 - This includes features as *SON*,
.....Trust and optional controls

Charles Darwin and the Darwin Award



From: biography.com

- “Taking oneself out of the gene pool by their own (unnecessarily foolish) actions.”
- First on Usenet group discussions as early as 1985
- 1993 on a website and collection of books by University of California, Berkeley
- www.darwinawards.com

One Example



“(2003, Australia) Parents often warn that firecrackers can blow your hand off, but as a 26-year-old Australian learned, they can also remove your gonads from the gene pool. An ambulance rushed to an Illawarra park after receiving reports that a man was hemorrhaging from his behind. The mercifully unidentified man had placed a lit firecracker between the cheeks of his buttocks, stumbled, and fell upon it.”

<http://darwinawards.com/darwin/darwin2003-19.html>



Rly? 😊

From: youtube.com

We'll start with some basics...

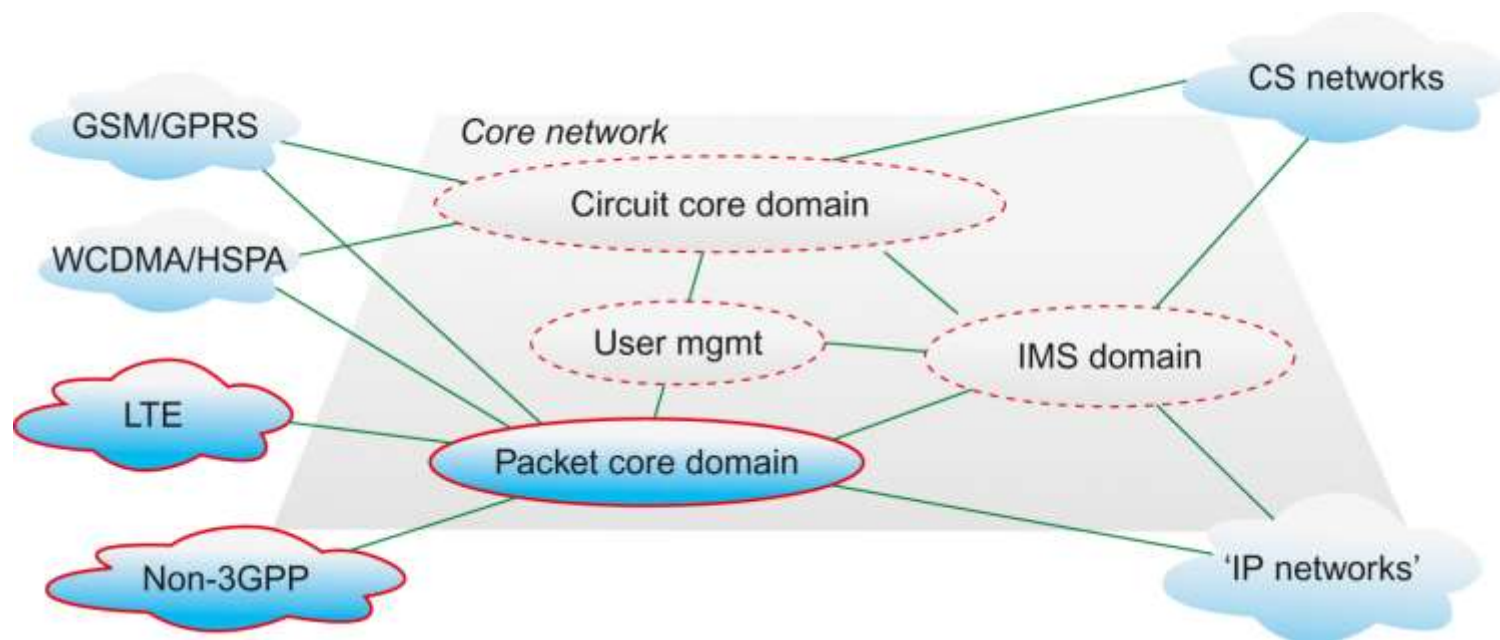


Standards - Overview

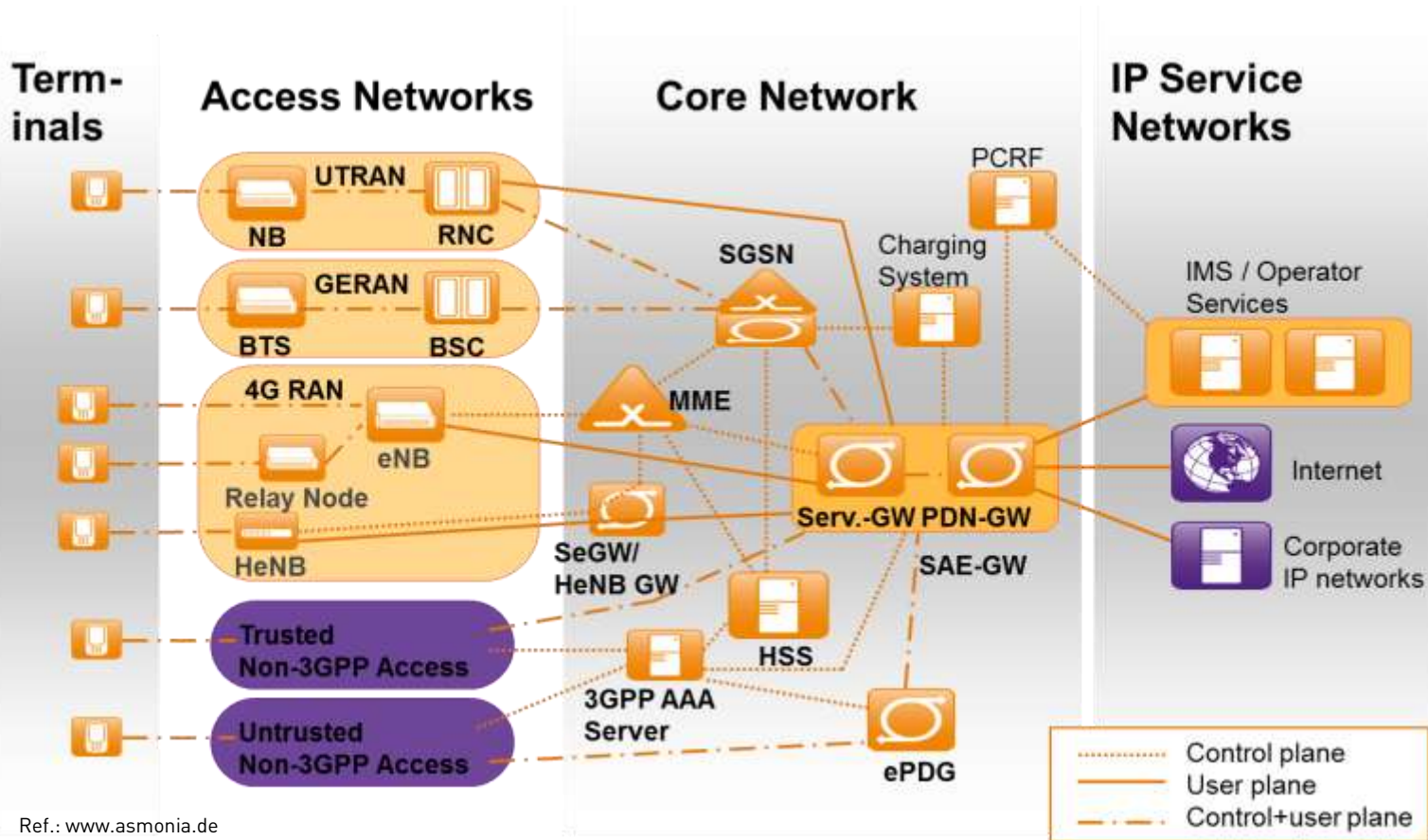


- International Telecommunication Union (ITU)
 - <http://www.itu.int/>
- 3rd Generation Partnership Project (3GPP)
 - www.3gpp.org
- Europäisches Institut für Telekommunikationsnormen (ETSI)

(Evolved) Packet System - Architecture



Ref.: 3gpp.org



Ref.: www.asmonia.de

LTE in the Field

What we see



eNodeB



- The actual air interface.
- Come in different shapes and sizes.
 - Rack, “Small-Boxes“, Portable
- Different types for different size cells.
 - Macro (>100m), Micro (100m), Pico (20-50m), HeNB (10-20m)
 - (WiFi/WiMax)
- Termination Point for Encryption
 - RF channel encryption
 - Backend channel encryption

This results in.... Het-Nets

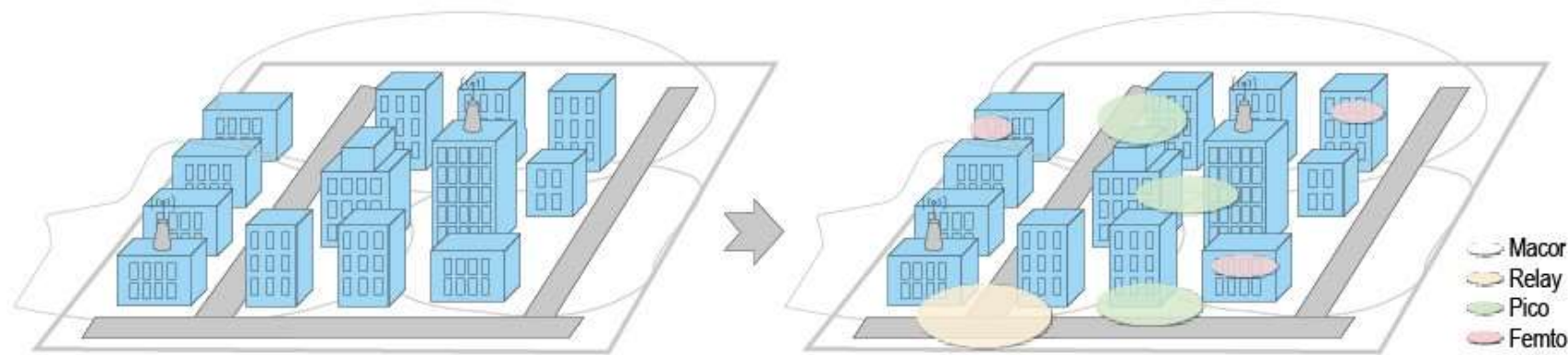


Figure 2. Evolution from homogeneous to heterogeneous networks.



An actual Runcom eNodeB

Source: runcom.com

eNodeB



- Ports for various amounts of “directional” antennas.
 - Single eNodeB, multiple Cells.
 - Cellmast “between” two cells
- Placed “close to antenna”
 - On the mast or down below.
 - Solutions with 5km fiber between eNB & “active antenna”
- Connected via LAN
 - “Self Configuring”
 - More on that later on





And now...? => Starting with the phone!

Part 1: UE Awareness

Phone means...



- Usually, it has to do phone calls ☺
 - or Internet; or some other stuff as we will see...
 - ...or everything merged together

- We've got
 - \$Tablets/Slates
 - \$USB-Sticks/-Modems
 - \$4G Cards
 - \$Mobile Hotspots
 - Relay Nodes ;-)

Our Scope



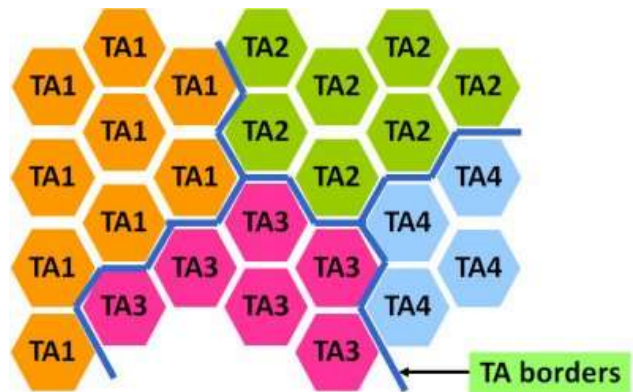
- When talking phone security you usually see the OS and its applications.
 - We'll check out some background functionality

UE: Look, Feel, Ask

- (Physical) Cell ID
- Tracking Area Code
- “Signal Strength”
- Position



PCI & TAC



- Physical Cell-ID
 - As known from “old” networks
 - Regionally unique identifier
 - 504 different IDs
 - Configured automatically
- Tracking Area Code
 - Contains multiple cells.
 - Paging area
 - UE’s current “location”

Source: <http://www.3gpp.org/technologies/keywords-acronyms/%6-nas>

Signal Strength & Location

Enhanced Serving Mobile Location Center (E-SMLC)

Backend part for positioning

Accepts requests from MME and organizes the actual process of positioning



- Signal Strength
 - Measured by device
 - Output in different formats
- Location
 - Positioning request
 - Use of OTDA (Observed Time Difference of Arrival)
 - Use differences in arrival times of packets from certain eNodeBs
 - GPS...GALILEO...GLONASS

Accessing Data

– Rather easy

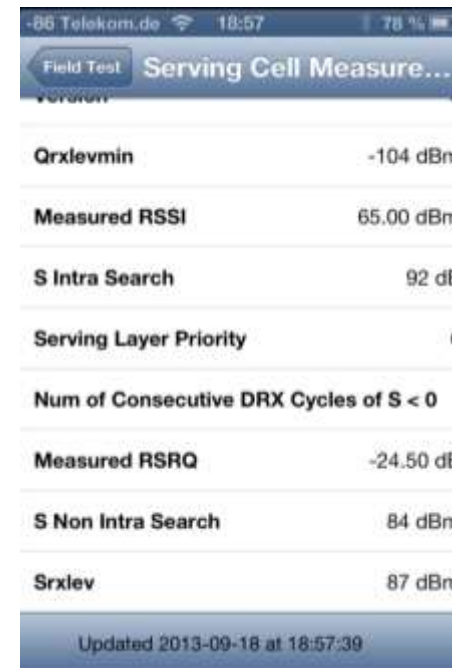
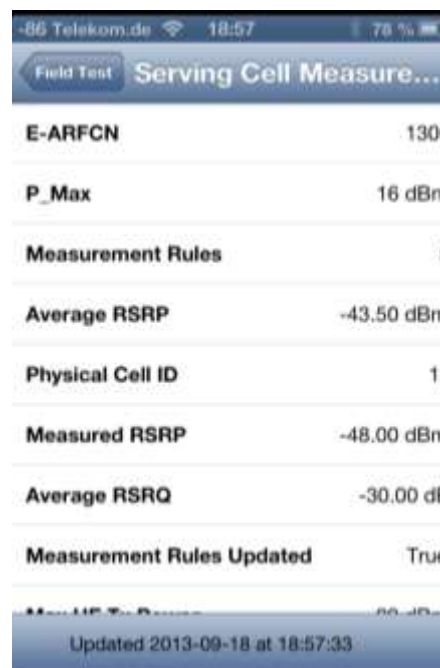
- Use of magic numbers
- Apps
- AT Commands



Hackers do „Information Gathering“

3001#12345#

– The magic number for iPhones



But why...?



From: youtube.com

- Knowledge! Understanding LTE!
- Collect and Log Data
- Answer a few questions
 - How large are Cells?
 - How large are Tracking Areas?

“Simple” Approach

- Writing an App on Android
- Use of onboard functionality & dump data into text

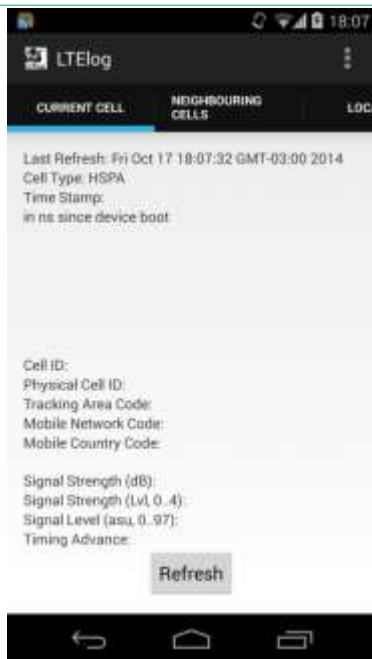


“LTElog”



- OpenSource wardriving tool
- Will be published in the next few weeks
- Logs available LTE cells, and current location
- Transmission of collected data mail
- Currently implementation of Google Maps API for plotting

LTElog output



```
27678209,347,3030,27678209,1,262,-
104,3,36,nA,52.24545494,8.98425866
nA,180,nA,nA,nA,nA,-112,2,28,nA,52.24545494,8.98425866
nA,97,nA,nA,nA,nA,-113,2,27,nA,52.24545494,8.98425866
nA,5,nA,nA,nA,nA,-105,3,35,nA,52.24545494,8.98425866
nA,311,nA,nA,nA,nA,-125,1,15,nA,52.24545494,8.98425866
nA,323,nA,nA,nA,nA,-126,1,14,nA,52.24545494,8.98425866
27678209,347,3030,27678209,1,262,-
104,3,36,nA,52.24545494,8.98425866
nA,180,nA,nA,nA,nA,-112,2,28,nA,52.24545494,8.98425866
nA,97,nA,nA,nA,nA,-114,2,26,nA,52.24545494,8.98425866
nA,5,nA,nA,nA,nA,-105,3,35,nA,52.24545494,8.98425866
nA,54,nA,nA,nA,nA,-118,1,22,nA,52.24545494,8.98425866
nA,311,nA,nA,nA,nA,-129,1,11,nA,52.24545494,8.98425866
nA,323,nA,nA,nA,nA,-128,1,12,nA,52.24545494,8.98425866
```

3rd Party Awareness

Am I being watched?



Can you see me??



- LTE is an IP Network
 - Scanning can be possible
- Exemplary Data
 - Attach Process
 - Paging Process

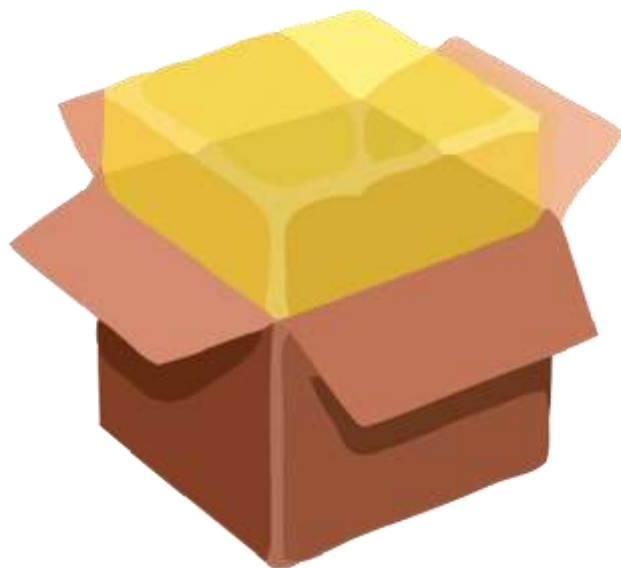


The Attach Procedure

Initial Bearer Setup



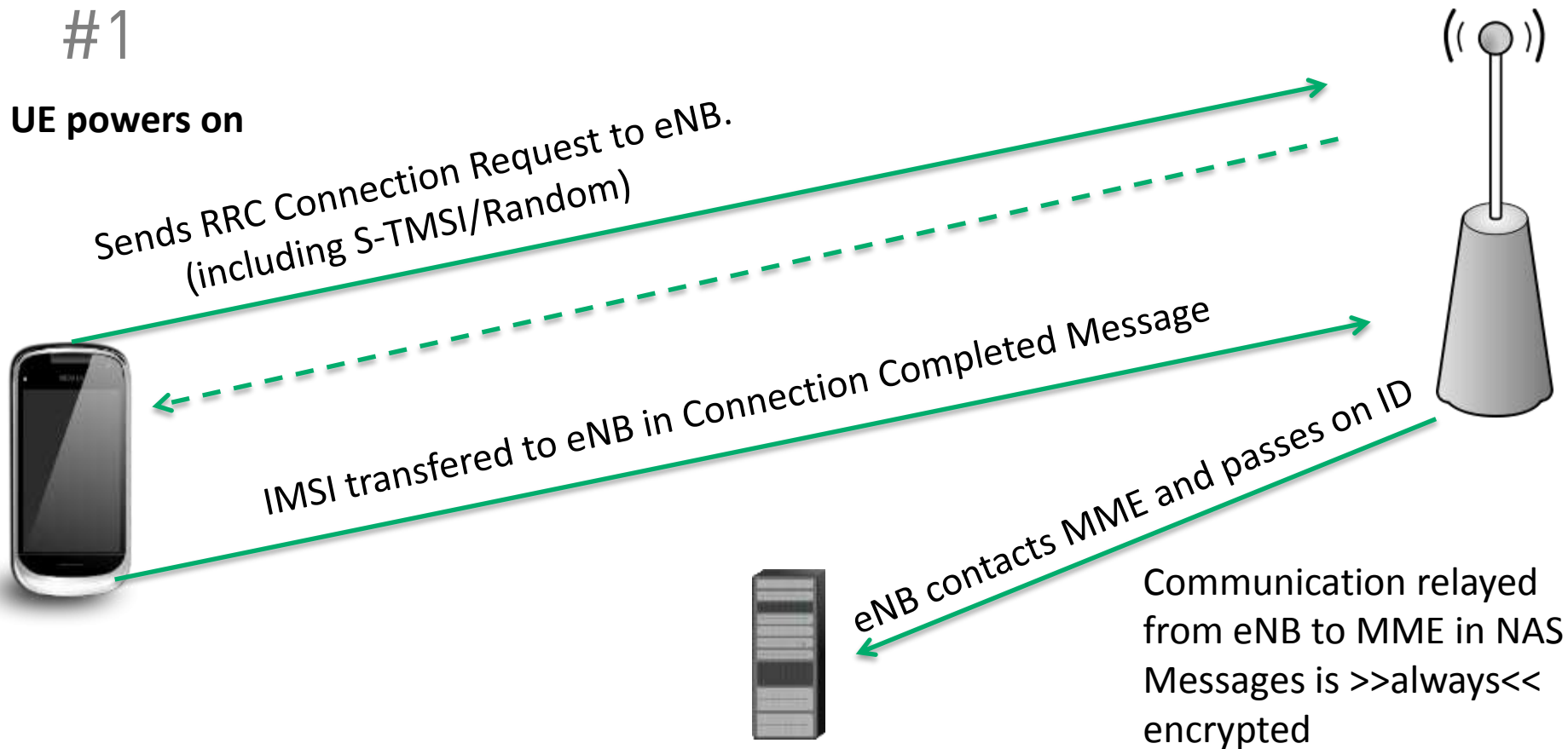
Involved components



- SIM Card
- UE
- eNB
- MME – Mobility Management Entity
- SGW – Serving Gateway
- PGW – PDN (Packet Data Network) Gateway
- HSS – Home Subscriber Server

#1

UE powers on

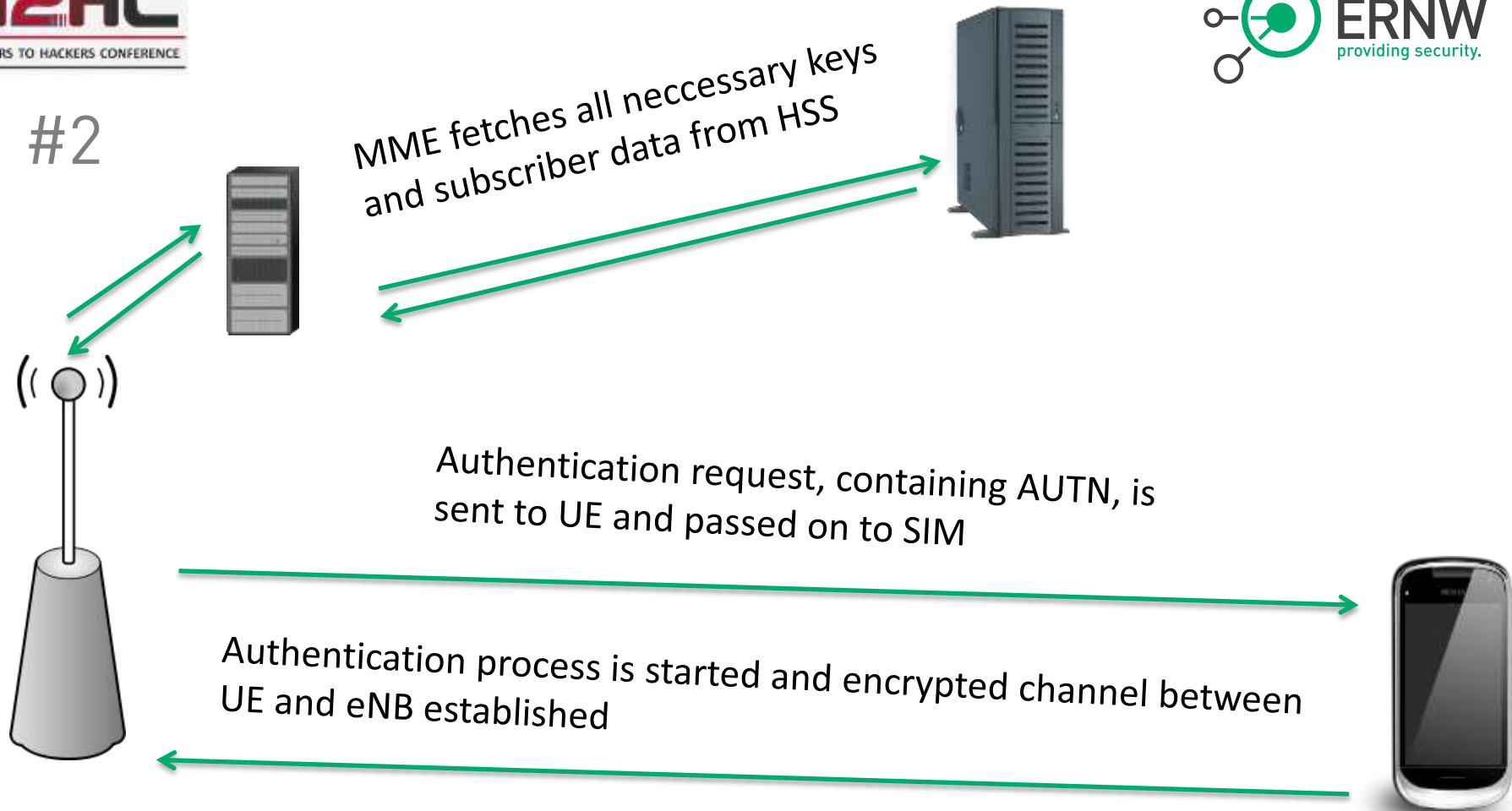


Always Encrypted?



- Yes!
- You may choose from three ciphering algorithms
 - EEA2 - AES
 - EEA1 - SNOW 3g
 - EEA0 - Null ciphering algorithm

#2



#3



- Final steps of attach procedure are processed
 - Establishment of IP connection etc.
- ...But, the connection is encrypted and we as a third party can't see it anymore....

Paging

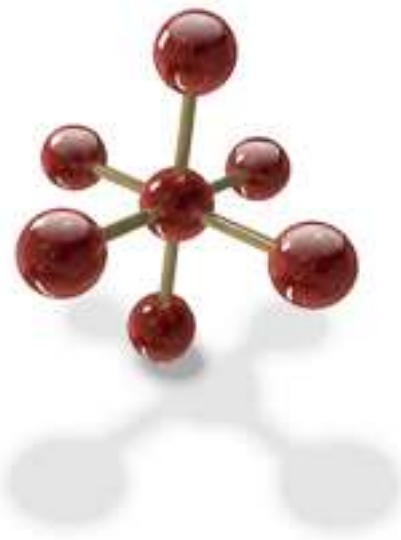


What is Paging



- “Wake up call”
 - UE is usually in a connected standby mode to save energy
- Paging wakes the UE and informs it of incoming messages and calls
- UE checks for Paging Messages periodically on certain channel

How to reach a certain UE ?



- Paging frames are sent out in a certain tracking area periodically
- Certain “ flags” can be set in these frames
 - Actually in certain sub-frames
- UE knows which “flag” to react to

After doing some
maths...



- We've got 8160 possible paging frames
- And 4 possible paging locations
- So we can page up to 32640 different devices
- Or...well...page a few different ones at the same time



Impact?



- You might loose some extra battery power
- Rather hard to actually track a mobile phone, due to different constansts on different eNBs

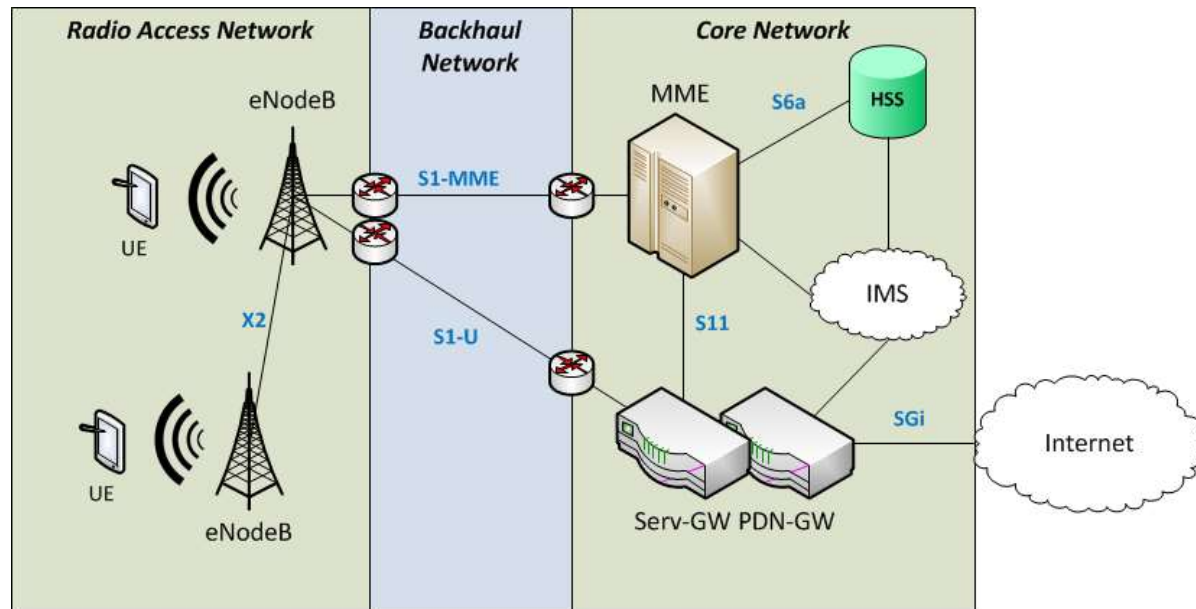
Btw:
Fallback!

- Voice and SMS over LTE not yet implemented
 - Depends on carrier
- When a call/message comes in, phone drops from 4g down to 3g/2g
- Triggered by paging
 - → Fallback, and call cancelation even before the phone rings
 - And it's free ;-)

The other side...

Backend Structure





Remember...?

The 4G LTE Basic



Access to Components and its Network?

Source: worldlte.blogspot.com



Some quotes from 3GPP TS 33.403

- “Setting up and configuring eNBs **shall be authenticated and authorized** so that attackers shall not be able to modify the eNB settings and software configurations via local or remote access.”



Access to Telco Network??

- Ever scanned your providers IP address range?

```

hschmidt@hslpt:~$ telnet [redacted]
Trying [redacted] .
Connected to [redacted].
Escape character is '^]'.
-----Welcome to ATP Cli-----
Login: █

hschmidt@hslpt:~/tools/nmap$ ./nmap -sP [redacted]
Starting Nmap 6.40 ( http://nmap.org ) at 2014-01-07 15:05 CET
Note: Host seems down. If it is really up, but with the wrong host name,
Nmap done: 1 IP address (0 hosts up) scanned

hschmidt@hslpt:~/ERNW/temp$ nmap -sP [redacted]
Starting Nmap 6.41SVN ( http://nmap.org ) at 2014-01-07 15:05 CET
Nmap scan report for [redacted] (100.70)
Host is up (0.032s latency).
Nmap done: 1 IP address (1 host up) scanned in 2.57 seconds
  
```



HSS!

```
[hschmidt@hslaptop ~]$ rsh -l root [REDACTED] /bin/sh  
[hschmidt@hslaptop ~]$ id  
uid=0(root) gid=0(root)
```



Access Point Names (APN)

- Access List often depends on the chosen APN.
- APNs are well-known, or?
- Ever heard of APNBF?
 - www.c0decafe.de



Specs about IPSec

- But this doesn't matter, 4G security is mostly based on Security-Gateways
- 3GPP TS 33.401
 - “In order to protect the S1 and X2 control plane [...], it is *required to* implement IPsec [...]. For both S1-MME and X2-C, IKEv2 certificates based authentication [...] *shall be* implemented.”
 - “In order to protect the S1 and X2 user [...], it is *required to* implement IPsec [...] with confidentiality, integrity and replay protection.”
 - “... transport mode IPsec is *optional* for implementation”

Specs about IPSec...

“NOTE 1: In case control plane interfaces are trusted (e.g. physically protected), there is no need to use protection [...].”

“NOTE 2: In case S1 and X2 user plane interfaces are trusted (e.g. physically protected), the use of IPsec/IKEv2 based protection is not needed.”



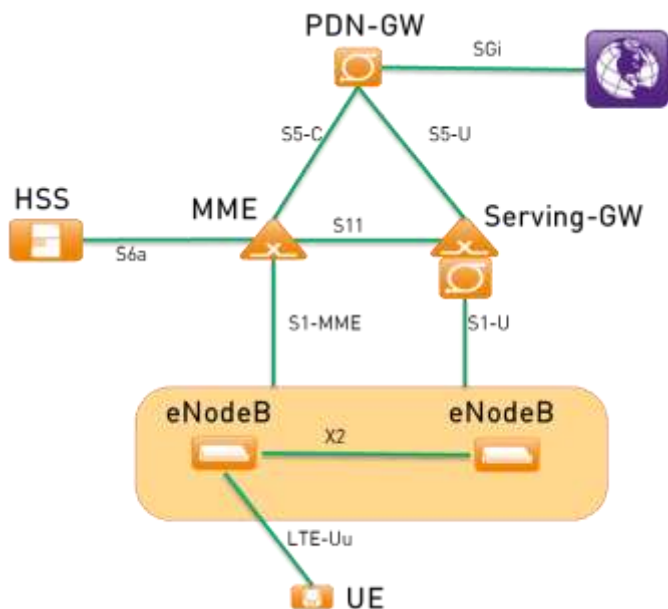


Physical protection??

Source: worldlte.blogspot.com



Control Structure



– GTP Interfaces

- ShmooCon 2011: Attacking 3G and 4G mobile telecommunications networks.

– S1 Interface

- S1-MME: control interface between eNB and MME
- S1-U: user plane
- *IPSec Encryption*



Attack Vectors



- In reality you will find...
 - Clients with process controls, DHCP, certificates, auto-connection/configuration
 - Servers with DHCP, CMDB, CA, Gateway, QoS
 - Certificate Problems

- And you know how this works, or?
 - Management Interfaces?
 - Complexity?
 - Common (IP) network problems/vulns?

3GPP Security Assurance Methodology (SECAM)

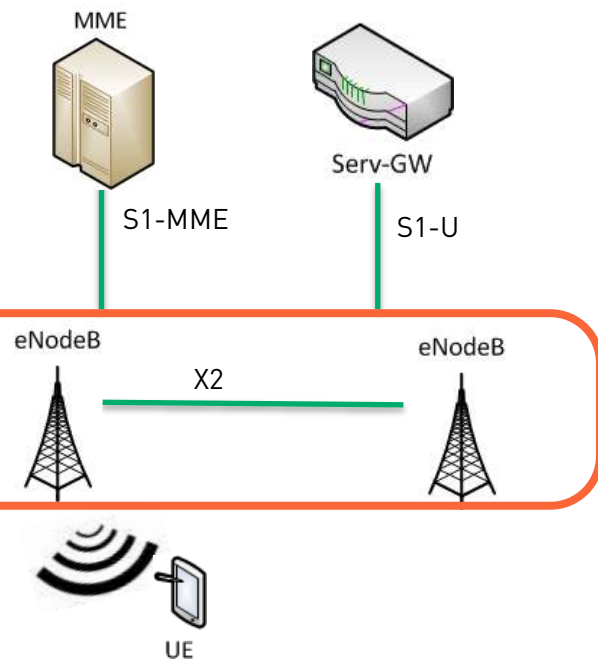
- Defined in 3GPP TR 33.805 (year 2013)
 - “Each 3GPP network product class [...] can have vulnerabilities which, if exploited, can damage the MNO and/or end-users.”

SECAM evaluation will cover the following four tasks:

- Vendor network product development and network product lifecycle management process assurance compliance (assessing if the method used to develop the products is compliant with the Security Assurance Process)
- Security Compliance Testing (assessing if requested security requirements are correctly implemented in a network product)
- Basic Vulnerability Testing (running of a set of FOSS/COTS tools on external interfaces of the Network product)
- Enhanced Vulnerability Analysis (holistic approach to analyse risk and impact of Vulnerabilities found in the Network Product)

S1-Interface

Control and User Plane

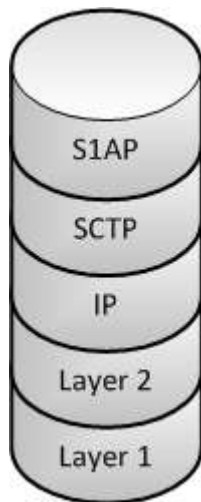


– S1 interface is divided into two parts

- S1-MME (Control Plane)
 - Carries signalling messages between base station and MME
- S1-U (User Plane)
 - Carries user data between base station and Serving GW

S1-AP

Protocol Stack



- S1 Application Protocol (S1AP), designed by 3GPP for the S1 interface
- Specified in 3GPP TS36.413
- Necessary for several procedures between MME and eNodeB
- Also supports transparent transport procedures from MME to the user equipment
- SCTP Destination Port 36412



S1AP with Dizzy

www.c0decafe.de



Technology in Perfection?



From: youtube.com

Self Organizing Networks

SON



Random Quote

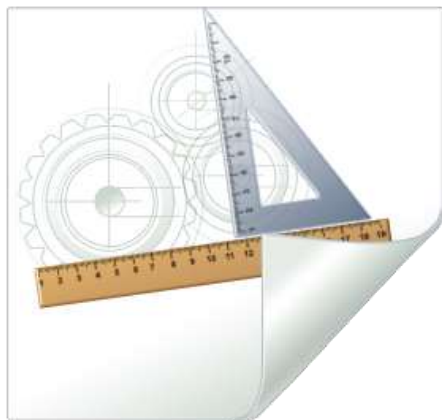
- It is likely that only a subset of SON functions can be standardised within the timeframe of the first release of the EPS. For that reason a step-by-step roll out of SON functions should be provided.
- From: 3GPP TS 32.500 V11.1.0 (2011-12)

Self Configuration

Big style “ Plug & Play”



Why?

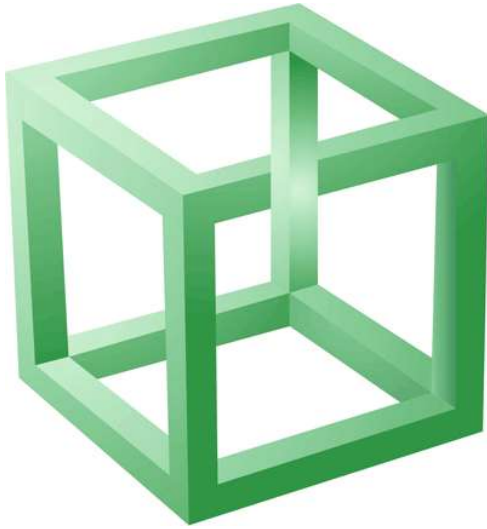


- Reduce on-site activities by installer
 - Reduce work to:
 - Connect to Antenna
 - Connect to LAN-Cable
 - Connect to Power
- Reduce installation costs
- Increase flexibility



How?

Base firmware is installed in factory



- eNB gets IP via DHCP
- Config gets pushed depending on HW-ID
- Installer configures positioning data or device uses internal GPS receiver
- (Work out PID and maybe new PID for surrounding cells)

Relay Nodes

Selective repeaters

Repeat data for certain eNodeBs



- Install and switch on
- Relay Node acts as UE
 - Connects to “Configurator eNB”
 - Fetches config from backend
- Relay Node relays data from “Donor eNB”

Self-Optimization





Optimized!

From: youtube.com

Self-Optimization



- “Automatically avoiding overlap”
- eNBs are aware of neighboring eNBs/cells
- Automated communication between adjacent eNBs
 - Band sharing both in time and frequency domains
 - Adapting of signal strength

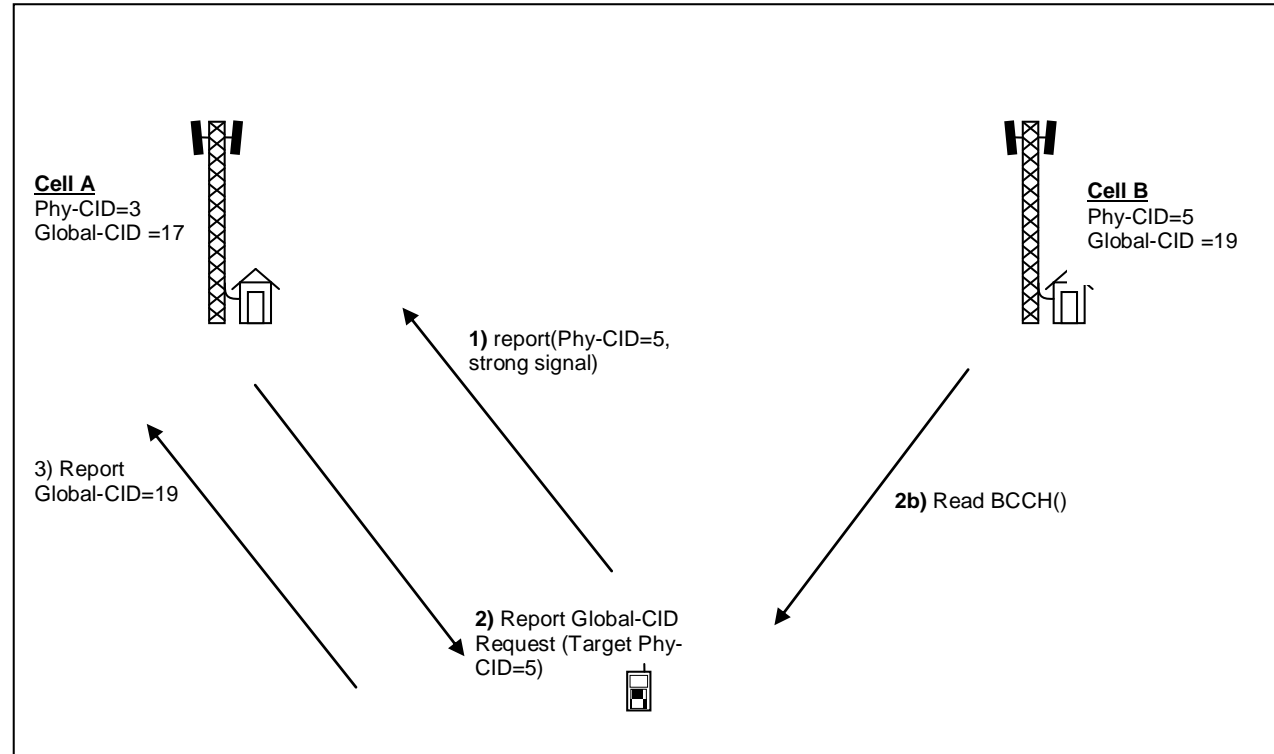
ANR

Automatic Neighbour Relation



- eNB checks for other cells in it's range.
 - Either itself or by asking an UE for the cells it can see
- If a cell is found, a channel is established via backend.
- Communication via X2 channel
 - Both eNBs communicate directly

ANR Process



Source: 3GPP TS 36.300 V12.1.0 (2014-03)

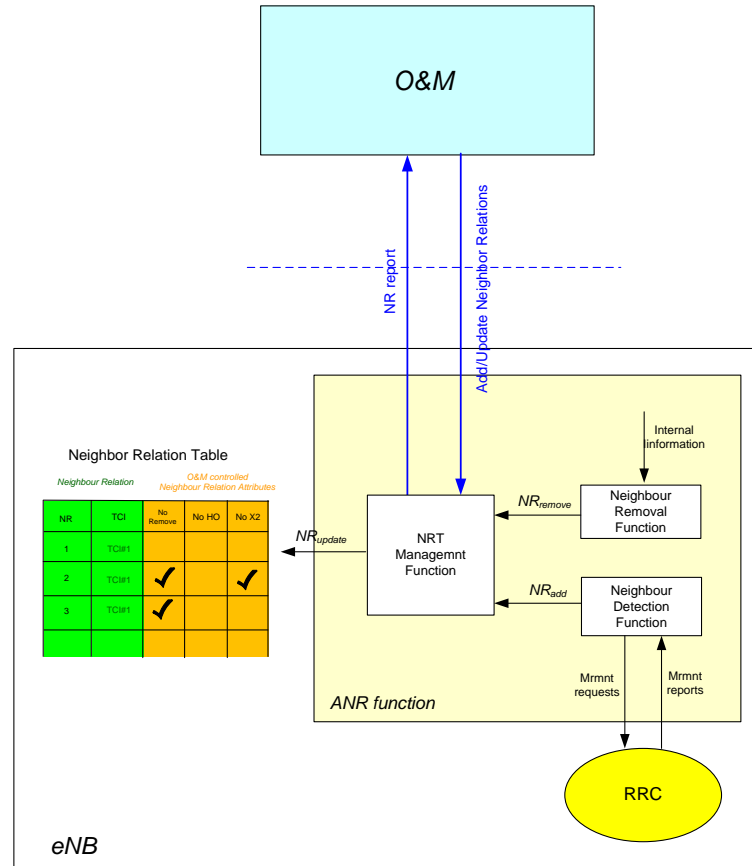
ANR@eNB

Neighbor Relation Table

Neighbour Relation *O&M controlled
Neighbour Relation Attributes*

NR	TCI	No Remove	No HO	No X2
1	TCI#1			
2	TCI#1	✓		✓
3	TCI#1	✓		

- Local table for known neighbours
 - No Remove: eNB may not remove constraint
 - No HO: Relation not to be used for hand overs
 - No X2: Do not use X2 for com with device
- Neighbour defined as adjacent cell



ANR@eNB

Source: 3GPP TS 36.300 V12.1.0
(2014-03)

HeNBs



- Home-eNodeBs are able to take part in SON process
 - The ones you might have at home
 - The ones you might have hacked and rooted
- Protocol was adapted to support communication with HeNBs
 - Addition of extra security gateway
 - “HeNB Gateway”

The Real Thing Hitachi ER5000



- LTE Femto-Cell
 - Or Home-eNodeB
- Comes in residential and in enterprise version
- Also comes with “Femto-Cell-Gateway”
 - Reduce load on backend, produced by multiple HeNBs

Source: <http://www.hitachi.com/>

Hitachi ER5000 Quotes I

Alas! A scientific man ought to have no wishes, no affections — a mere heart of stone.

Charles Darwin

- Autonomous Inter-cell Interference Control
 - Hitachi ER5000 LTE Femtocell (HeNB) autonomously mitigates inter-cell interference that deteriorates data rate and causes service outage at cell boundary.
- Femto-GW Minimizing Impacts on EPC
 - Reduction of signaling load on MME and S-GW, with 3GPP compliant techniques and our proprietary enhancement such as C-plane messaging reduction and intra-Femto-GW mobility control.

Hitachi ER5000 Quotes II

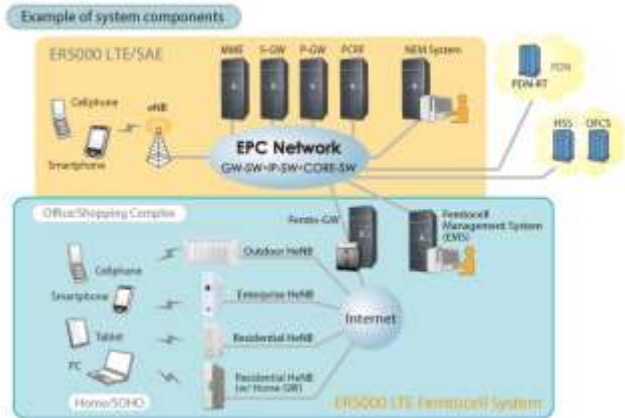
I love fools' experiments. I am always making them.

Charles Darwin

- Mobile Traffic Offloading
 - The ER5000 LTE Femtocell (HeNB) and Femto-GW enable traffic offloading from macrocell-eNBs and operator's EPC network.
- Integrated OAM & P Solution
 - The ER5000 LTE Femtocell system's 'Plug and Play', 'Self Planning', 'Self Recovery', 'Self Healing' and 'Self Optimization' - the EMS helps management of a large number of HeNBs with enabling easy installation and maintenance as well as optimizing the system.

Hitachi ER5000

Summary



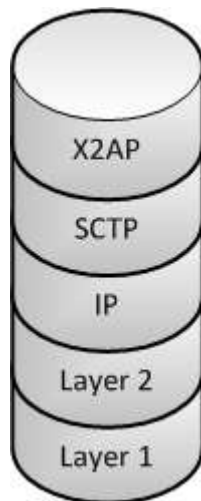
- Autonomous Inter-cell Interference Control
 - So it ought to be using SON/ANR features and the X2 channel
- Femto-GW Minimizing Impacts on EPC
 - Just as the specs recommend
- Mobile Traffic Offloading
 - Will only I be able to use my HeNB or might you be connected to it, too?
- Integrated OAM & P Solution
 - So it'll get an IP, should be forwarded some configuration Server and fetch it's config over my line?

Source: <http://www.hitachi.com/>

Quick reminder

- The specs also talk about WiFi
- When Voice via LTE works, your mobile might roam into certain WiFi networks
 - i.e. in malls or office buildings
- Yet again: SON
 - → In future even some WiFi Routers/Hotspots might have certain SON functionality

Another interesting Interface: X2



- Similar to S1AP ☺
- X2 Application Protocol (X2AP) is defined in 3GPP TS 36.423
- Interconnecting two eNodeBs within E-UTRAN architecture
 - Providing signaling information across the X2 interface
- SCTP Destination port 36422

X2AP

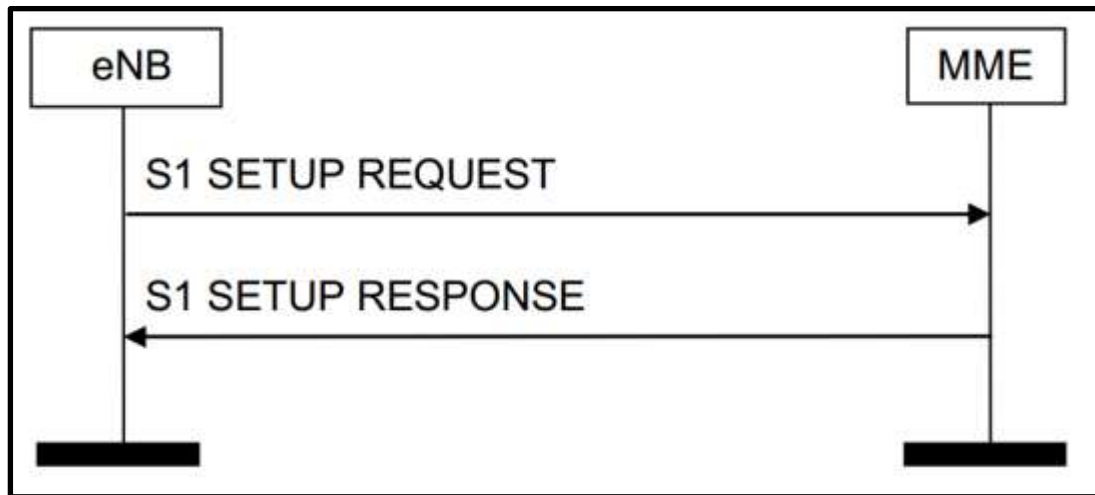


- Basic procedure: X2 Setup
- Some more interesting
 - eNB Configuration Update
 - Handover Preparation/Initiation
 - Cell Activation
 - Load Information Exchange
 - ...
- But also: Relaying of NAS

S1AP and X2AP Functions Overview

- E-RAB management functions (setup, management, modifying)
- An "Initial Context transfer" function to establish a S1UE context in the eNodeB to setup E-RABs, IP connectivity and NAS signaling.
- UE Capability Info Indication function: providing UE capability information.
- Mobility functions for UE, active in LTE network in case of change of the eNodeB or RAN (e.g. location change).
- Paging: provides the capability for the MME to page the UE.
- NAS signaling transport
- S1 UE context release/modification functions: modify and release UE context information
- Status transfer: transferring Packet Data Convergence Protocol (PDCP) SN, defined at [31], status information between two eNodeBs.
- Trace functions
- Location Reporting functions
- LPPa (LTE Positioning Protocol Annex) signaling transport: providing the transfer of LPPa messages between eNodeB and E-SMLC.
- S1 CDMA2000 tunneling functions: carrying CDMA2000 signaling messages between the UE and the CDMA2000 RAT.
- Warning message transmission
- RAN Information Management (RIM) functions: transferring RAN system information between two RAN nodes.
- Configuration Transfer functions: requesting and transferring RAN configuration information





The S1 Setup Procedure

Source: 3GPP TS 36.413

8.7.3.3 Unsuccessful Operation

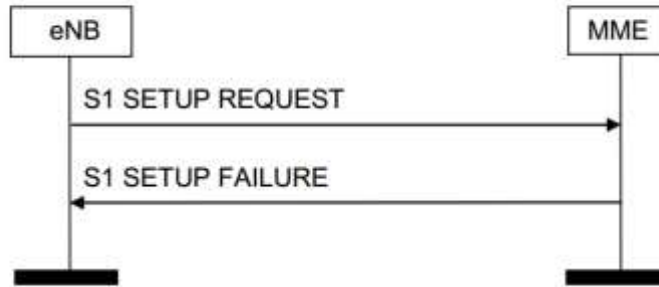


Figure 8.7.3.3-1: S1 Setup procedure: Unsuccessful Operation.

If the MME cannot accept the setup, it should respond with a S1 SETUP FAILURE and appropriate cause value.



On Failure...

Source: 3GPP TS 36.413

```

Item 2: id-CriticalityDiagnostics
  ProtocolIE-Field
    id: id-CriticalityDiagnostics (58)
    criticality: ignore (1)
  value
    CriticalityDiagnostics
      procedureCode: id-S1Setup (17)
      triggeringMessage: initiating-message (0)
      procedureCriticality: ignore (1)
      iEsCriticalityDiagnostics: 3 items
      Item 0: id-Global-ENB-ID
        CriticalityDiagnostics-IE-Item
          iECriticality: reject (0)
          iE-ID: id-Global-ENB-ID (59)
          typeOfError: missing (1)
      Item 1: id-SupportedTAs
        CriticalityDiagnostics-IE-Item
          iECriticality: reject (0)
          iE-ID: id-SupportedTAs (64)
          typeOfError: missing (1)
      Item 2: id-DefaultPagingDRX
        CriticalityDiagnostics-IE-Item
          iECriticality: ignore (1)
          iE-ID: id-DefaultPagingDRX (137)
          typeOfError: missing (1)

```

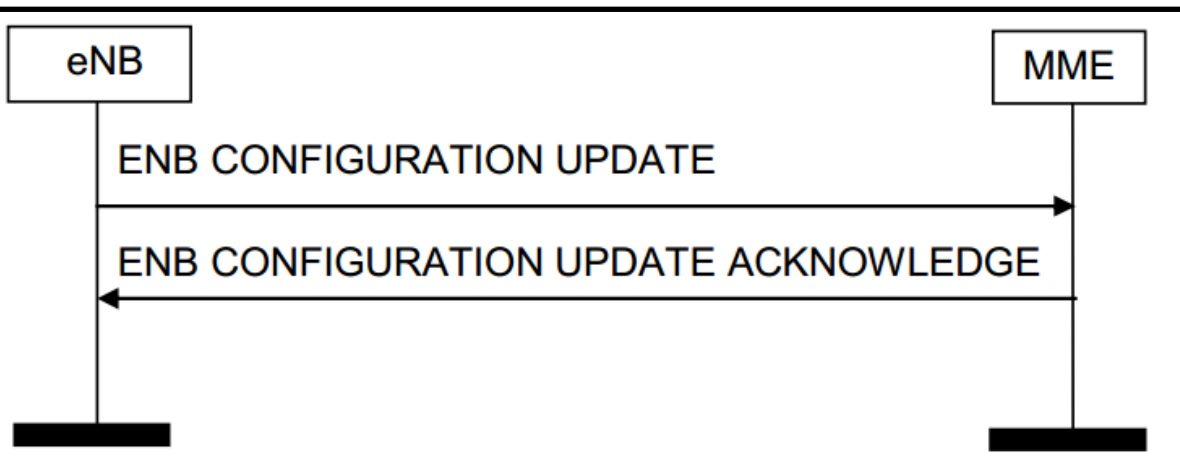


Very informative for
Hackers 😊



Participating in the Network

Source: 3GPP TS 36.413



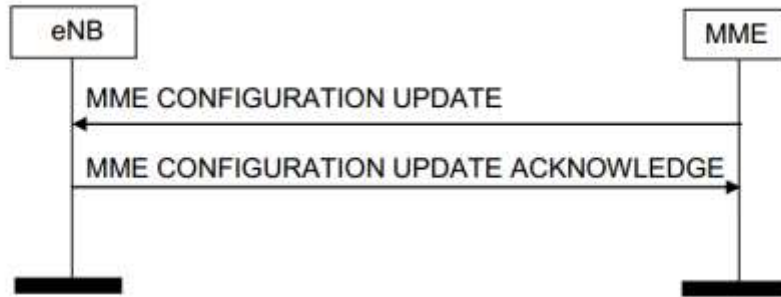


Figure 8.7.5.2-1: MME Configuration Update procedure: Successful Operation.

The MME initiates the procedure by sending an MME CONFIGURATION UPDATE message including the appropriate updated configuration data to the eNB. The eNB responds with an MME CONFIGURATION UPDATE ACKNOWLEDGE message to acknowledge that it successfully updated the configuration data. If information element(s) is/are not included in the MME CONFIGURATION UPDATE message, the eNB shall interpret that the corresponding configuration data is not changed and shall continue to operate the S1 with the existing related configuration data.



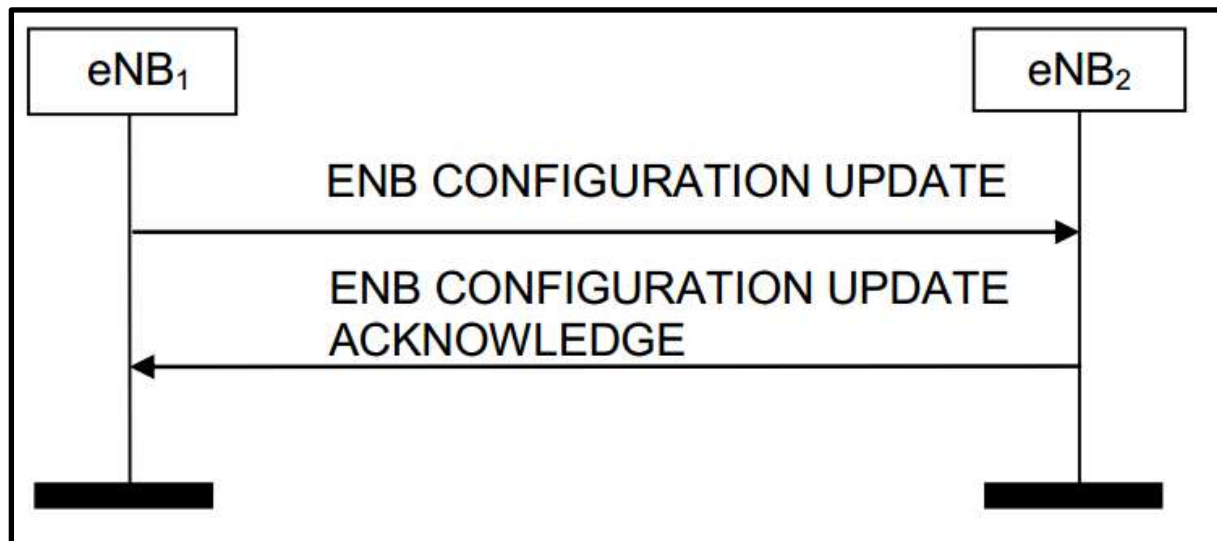
From MME 😊

Source: 3GPP TS 36.413



Or more interesting in
X2AP ☺

Source: 3GPP TS 36.423



Participating in the Network



- Once having access, enables possibility to inject control messages:
 - Load Indication
 - Configuration
 - Handover
 - Triggering of any SON procedures (tracing, tracking)

- Think on roaming access to other providers!

Masscan supports SCTP

Besides the well-known transport protocols of TCP and UDP, there is also one called SCTP. It's been included in Windows, Linux, Mac OS X for 10 years. Almost nobody uses it. I know little more about this protocol than you do.

But I can now scan for it in [masscan](#). Scanning the entire Internet for an SCTP service would look something like this:

```
masscan 0.0.0.0/0 -pS:36422,36412 --rate 100000
```

Like *nmap*, you can prefix ports with the letter of the transport protocol, where *T*: is for TCP, *U*: is for UDP, and *S*: is for SCTP.

The ports above are for protocols in the LTE/4G protocol suite. Running this scan, I got the following results:

```
Discovered open port 36412/sctp on 31.204.128.247
Discovered open port 36412/sctp on 41.213.0.147
Discovered open port 36412/sctp on 41.213.0.163
Discovered open port 36412/sctp on 61.252.41.113
Discovered open port 36412/sctp on 64.71.135.220
Discovered open port 36412/sctp on 115.12.152.194
Discovered open port 36422/sctp on 115.12.152.194
Discovered open port 36412/sctp on 119.194.139.93
Discovered open port 36412/sctp on 119.39.227.186
Discovered open port 36422/sctp on 120.199.33.154
Discovered open port 36422/sctp on 120.199.63.234
Discovered open port 36412/sctp on 173.228.61.6
Discovered open port 36412/sctp on 182.98.163.217
Discovered open port 36422/sctp on 183.247.170.18
Discovered open port 36422/sctp on 197.243.0.89
Discovered open port 36422/sctp on 197.243.0.90
Discovered open port 36422/sctp on 197.243.0.91
Discovered open port 36422/sctp on 197.243.0.92
Discovered open port 36422/sctp on 197.243.0.93
Discovered open port 36422/sctp on 197.243.0.94
Discovered open port 36422/sctp on 211.72.48.37
Discovered open port 36422/sctp on 221.112.39.244
```



„Nobody would use
this in the Internet“

<http://blog.erratasec.com/2014/01/masscan-supports-sctp.html#.U1gQ4R9vK0x>

Just a few thoughts



- Can I set up a connection with \$device in \$network?
- Can I get my phone to actually make 2 eNBs think that they're closer than the actually are?
- Can I use my HeNB and tell a macro cell eNB, that I'm actually covering all it's area and that I'm so much better in doing so?

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **s1ap** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
97	4.22283200	192.168.1.82		SIAP	374	COOKIE_ECHO id-S1Setup, S1Se
124	4.60800500		192.168.1.82	SIAP	90	id-S1Setup, S1SetupResponse

Stream Control Transmission Protocol, Src Port: s1-control (36412), Dst Port: 36411 (36411)

S1 Application Protocol

- SIAP-PDU: successfulOutcome (1)
 - successfulOutcome
 - procedureCode: id-S1Setup (17)
 - criticality: reject (0)
 - value
 - S1SetupResponse
 - protocolIEs: 2 items
 - Item 0: id-ServedGUMMEIs
 - ProtocolIE-Field
 - id: id-ServedGUMMEIs (105)
 - criticality: reject (0)
 - value
 - Item 1: id-RelativeMMECapacity
 - ProtocolIE-Field
 - id: id-RelativeMMECapacity (87)
 - criticality: ignore (1)
 - value
 - RelativeMMECapacity: 50



S1 Setup, how it would look like ;-)



Tool: S1AP_ENUM



- Thanks to Daniel@ERNW
 - www.c0decafe.de
- Enumerator for S1AP Interfaces
- Collects information and bruteforces PLMN

```
..Trying PLMN-ID: {eNBid,[55,240],[80],[50,18],[101,78,66,49]}
Got bad answer: {unsuccessfulOutcome,{unsuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'unknown-PLMN'}}]}}}}!
... Trying PLMN-ID: {eNBid,[55,240],[144],[50,18],[101,78,66,49]}
Got bad answer: {unsuccessfulOutcome,{unsuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'unknown-PLMN'}}]}}}}!
... Trying PLMN-ID: {eNBid,[55,240],[1],[50,18],[101,78,66,49]}
Got bad answer: {unsuccessfulOutcome,{unsuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'unknown-PLMN'}}]}}}}!
... Trying PLMN-ID: {eNBid,[55,240],[153],[50,18],[101,78,66,49]}
Got bad answer: {unsuccessfulOutcome,{unsuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'unknown-PLMN'}}]}}}}!
..Trying PLMN-ID: {eNBid,[100,240],[0],[50,18],[101,78,66,49]}
Got bad answer: {unsuccessfulOutcome,{unsuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'unknown-PLMN'}}]}}}}!
..Trying PLMN-ID: {eNBid,[100,240],[16],[50,18],[101,78,66,49]}
Got good answer for Mcc 460, Mnc 1
{successfulOutcome,{ 'SuccessfulOutcome',17,reject,{ 'S1SetupResponse',[{ 'ProtocolIE-Field',105,reject,{ 'ServedGUMMEISItem',[[100,240,16]],[[128,1]],[[1]],asn1_NULLVALUE}}]},{ 'ProtocolIE-Field',87,ignore,50}}}}
Network: [67,104,105,110,97,32,85,110,105,99,111,109,32], Name []
```

So we were able to establish a S1 session with this one, someone wants to (de-)reg some UE? xD

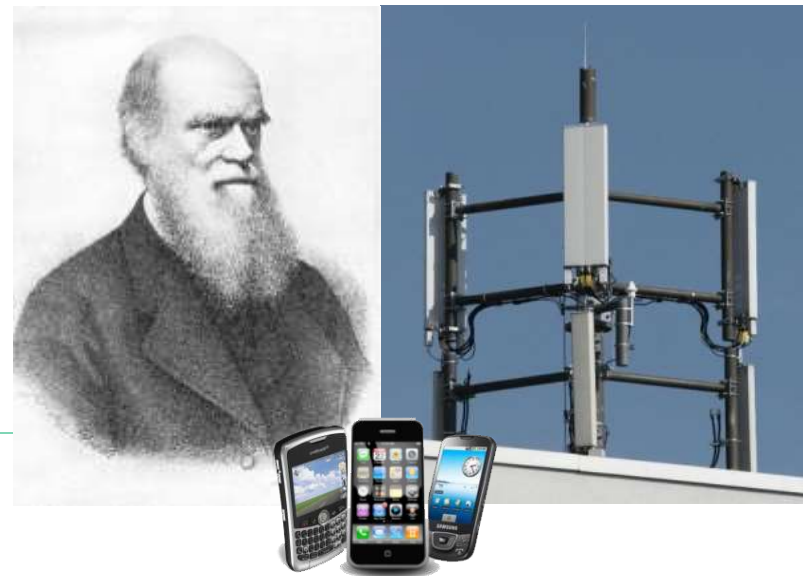
Others are not so nice, like this one here:

```
... Trying PLMN-ID: {eNBid,[55,248],[16],[50,18],[101,78,66,49]}
Got bad answerfor Mcc 738, Mnc 1
{unsuccessfulOutcome,{ 'SuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'om-intervention'}}]},{ 'ProtocolIE-Field',65,ignore,v60s}}}}
... Trying PLMN-ID: {eNBid,[55,248],[32],[50,18],[101,78,66,49]}
Got bad answerfor Mcc 738, Mnc 2
{unsuccessfulOutcome,{ 'SuccessfulOutcome',17,reject,{ 'S1SetupFailure',[{ 'ProtocolIE-Field',2,ignore,{misc,'om-intervention'}}]},{ 'ProtocolIE-Field',65,ignore,v60s}}}}
..
```

www.insinuator.net

S1AP_enum

Will Darwin strike again?



Conclusions



- Overall, it is a good concept, but there is high complexity!
- Some things are a bit shocking...
- Do not trust roaming partners 😊
- But you see: they have learned!



Random Darwin Award

(5 Feb 2013, São Paulo, Brazil)

<http://darwinawards.com/darwin/darwin2013-01.html>

- Mechanic Sérgio A. Rosa, 49, was welding a gas tanker that, curiously, exploded, sending his remains flying 400 meters through the air.



There's never enough time...

THANK YOU...




...for yours!

Blog:  **INSINUATOR.NET** Conference: **TROOPERS.de**

Stay in touch



- Visit our blog and join the discussion:  **INSINUATOR.NET**
- Join us at **TROOPERS.de** conference!
- Ping us at Twitter: [@WEareTROOPERS](#)
[@Insinuator](#)
- Drop us a mail.

Random Darwin Award

(July 2011, New York)

<http://darwinawards.com/darwin/darwin2011-03.html>

- Protesting motorcycle helmet laws, an Onondaga, NY man was participating in a bare-noggin protest ride when he was killed via flipping over the handlebars.

Random Darwin Award

[10 January 2007, Germany]

<http://darwinawards.com/darwin/darwin2007-01.html>

- A 63-year-old man's extraordinary effort to eradicate moles from his property resulted in a victory for the moles. The man pounded several metal rods into the ground and connected them [...] to a high-voltage power line, intending to render the subterranean realm uninhabitable. Incidentally, the maneuver electrified the very ground on which he stood.

Random Darwin Award

[1995]

<http://darwinawards.com/darwin/darwin1996-07.html>

- Azninski, 30, had been drinking with friends when it was suggested they strip naked and play some "men's games". Initially they hit each other over the head with frozen turnips, but then one man upped the ante by seizing a chainsaw and cutting off the end of his foot. Not to be outdone, Azninski grabbed the saw and, shouting "Watch this then," he swung at his own head and chopped it off.

Random Darwin Award

[27 February 2012, North Carolina]

<http://darwinawards.com/darwin/darwin2012-03.html>

- Gary was at a friend's apartment when he spotted a salsa jar containing a mystery fluid. Thinking that it was an alcoholic beverage, he helped himself to a sizeable swig of gasoline! Naturally enough, he immediately spit out the offending liquid onto his clothes. Then, to recover from the shock, Gary lit a cigarette.

Random Darwin Award

(5 Feb 2013, São Paulo, Brazil)

<http://darwinawards.com/darwin/darwin2013-01.html>

- Mechanic Sérgio A. Rosa, 49, was welding a gas tanker that, curiously, exploded, sending his remains flying 400 meters through the air.