Attacking BaseStations

Hendrik Schmidt <hschmidt@ernw.de>

Brian Butterly <bbutterly@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*

Motivation

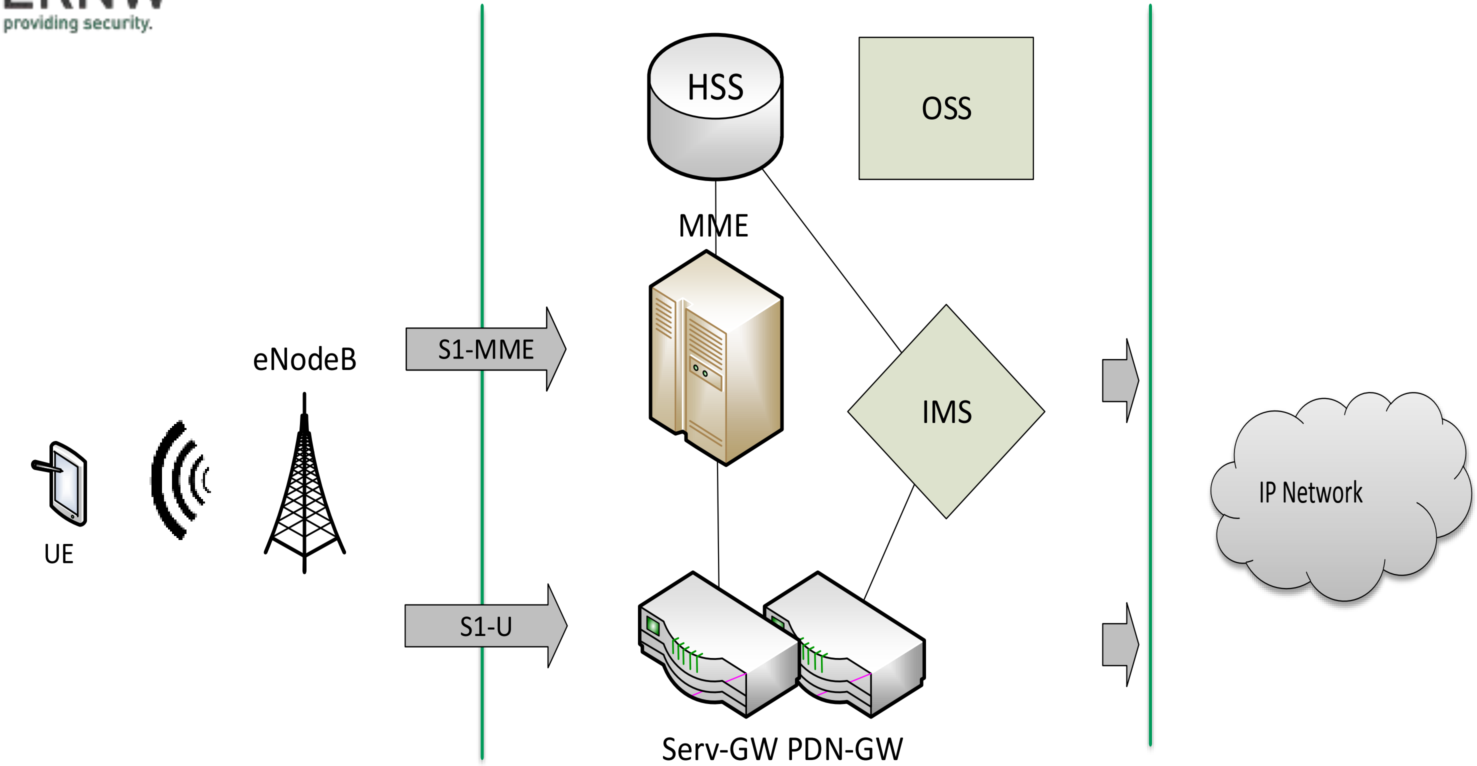
- The 4G standard introduces a lot of new technologies providing modern services to the customer.
  - This includes features as VoLTE, *SON*, ...Trust and optional controls

- BaseStations are the big (and small) antennas in the field

- With our research we want to bring visibility to
  - How the environment works
  - What providers do
  - What vendors do

Introduction

From 2G to 4G Telecommunication Networks



eUTRAN

4G Core

Typical Environment?

Source: worldlte.blogspot.com

Typical Environment?

BaseStation Physical Setup

- Usually a closed/outdoor rack
  - Baseband Unit (BBU) (or multiple)
  - Power Distribution Unit (PDU)
  - Power Supply Unit (PSU)
  - Ventialation
  - Temperatur/ Humidity Sensors
  - Alarm Sensors
- Extra box with power connections

The Idea

1. **Understand** BaseStation Setup
2. **Purchase** an old BaseStation out of the field
3. Get BS running in an **emulated environment**
4. Perform an evaluation of **configuration & security**

What we need: Basestation Physical Setup

- Base Band Unit (BBU)
  - Usually standing on the ground
- Remote Radio Head/Unit (RRH/RRU)
  - May be placed on the cell mast or on the ground
- Antenna
  - Come in various shapes and sizes
  - Nowadays often vector antennas

- All active parts are interconnected
  - BBU, RRU, sensors, power supply, vents

Power Supply

- Components run on -48V
  - Not +-48V (96V differential)
  - Basically just 48V connected the other way round

RRU

- Basically receives raw RF signals via Fiber and sends them out via Copper
  - Towards the antenna
- Usually capable of serving a specific frequency band

Most important Unit: the BBU

- Frame for holding power unit and **functional blades**
- Sometimes have a backplane for interconnection between components
  - Arbitrary PCB connectors
  - Multiple interfaces (LAN, UART, Arbitrary, CAN)

- Functional blades decide the network type
  - Ericsson: DUL/DUW/DUG -> Digitial Unit LTE/WCDMA/GSM
- Slots for multiple blades
  - Single BBU could serve GSM and WCDMA
  - Depends highly on specific BBU and blade combination
- Single blade can serve multiple cells
  - Using sector antennas a single mast could i.e. serve 4 cells in 4 different directions

ERNW
providing security.

Variants of an eNodeB

- 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

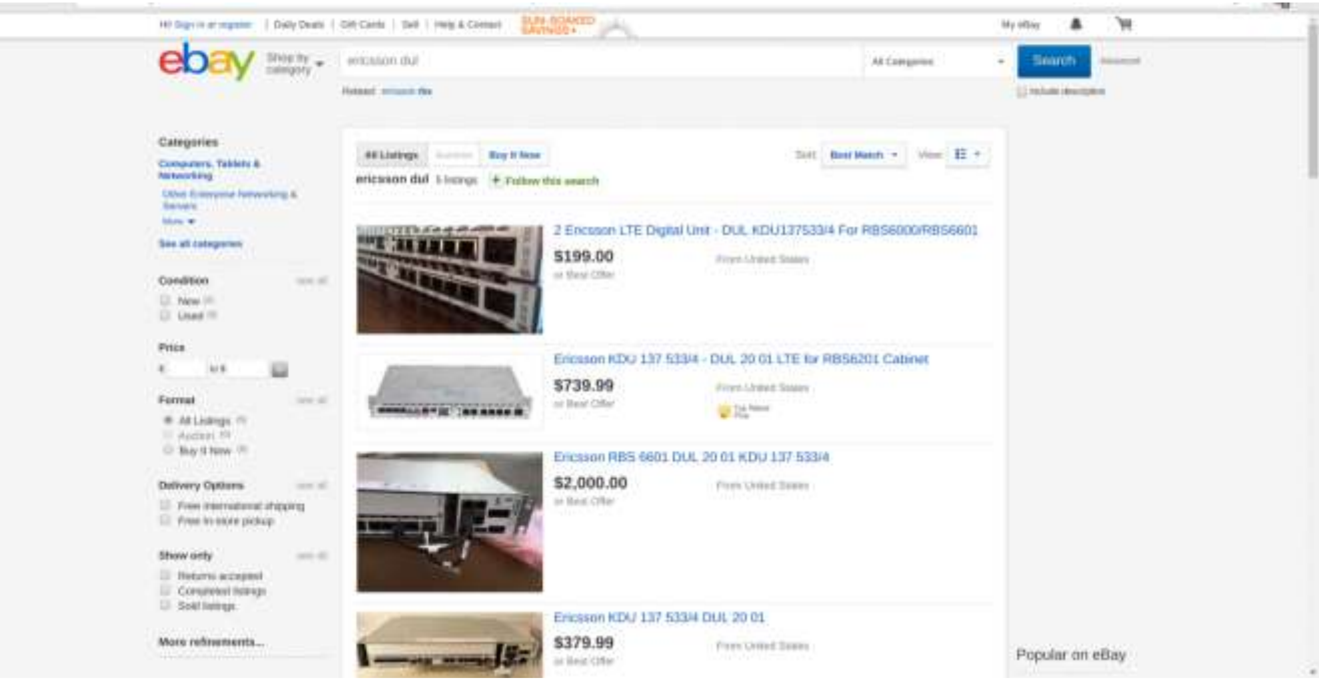
Implementing a Lab

Just a Quick HowTo

How to Start…

- Purchasing a BTS is not easy, you have to be aware of the architecture
- Searching for „eNodeB“ is not working very well because every vendor has its own architecture, boards, and naming
- Some helpful words:
  - Nokia - FlexiBTS
  - Huawei – BBU + LMPT/UMPT
  - Ericsson – RBS + DUL
  - ALU – MBS

Ebay ☺



ericsson dul

ericsson dul 5 listings

2 Ericsson LTE Digital Unit - DUL KDU137533/4 For RBS6000/RBS6601
$199.00
or Best Offer
From United States

Ericsson KDU 137 533/4 - DUL 20 01 LTE for RBS6201 Cabinet
$739.99
or Best Offer
From United States

Ericsson RBS 6601 DUL 20 01 KDU 137 533/4
$2,000.00
or Best Offer
From United States

Ericsson KDU 137 533/4 DUL 20 01
$379.99
or Best Offer
From United States

Lab Setup – What You Need

- A Basestation
  - The RRU is optional if you just want to play with the BTS itself
- Power Supply
  - -48V ~ 5A will be sufficient
- Power Connectors
  - Good luck ;-)
  - The devices sometimes have strange plugs, so you might need some time to find or make them

Lab Setup – What You Need

- Proper switch
  - Depending on the model and configuration the backhaul interface will be using multiple VLANs (signaling, configuration)
- Stack of network cables
- A Box/VM
  - Be prepared to set up multiple IP addresses
  - Virtual interfaces with VLANs
  - NTP server

Our Lab ☺

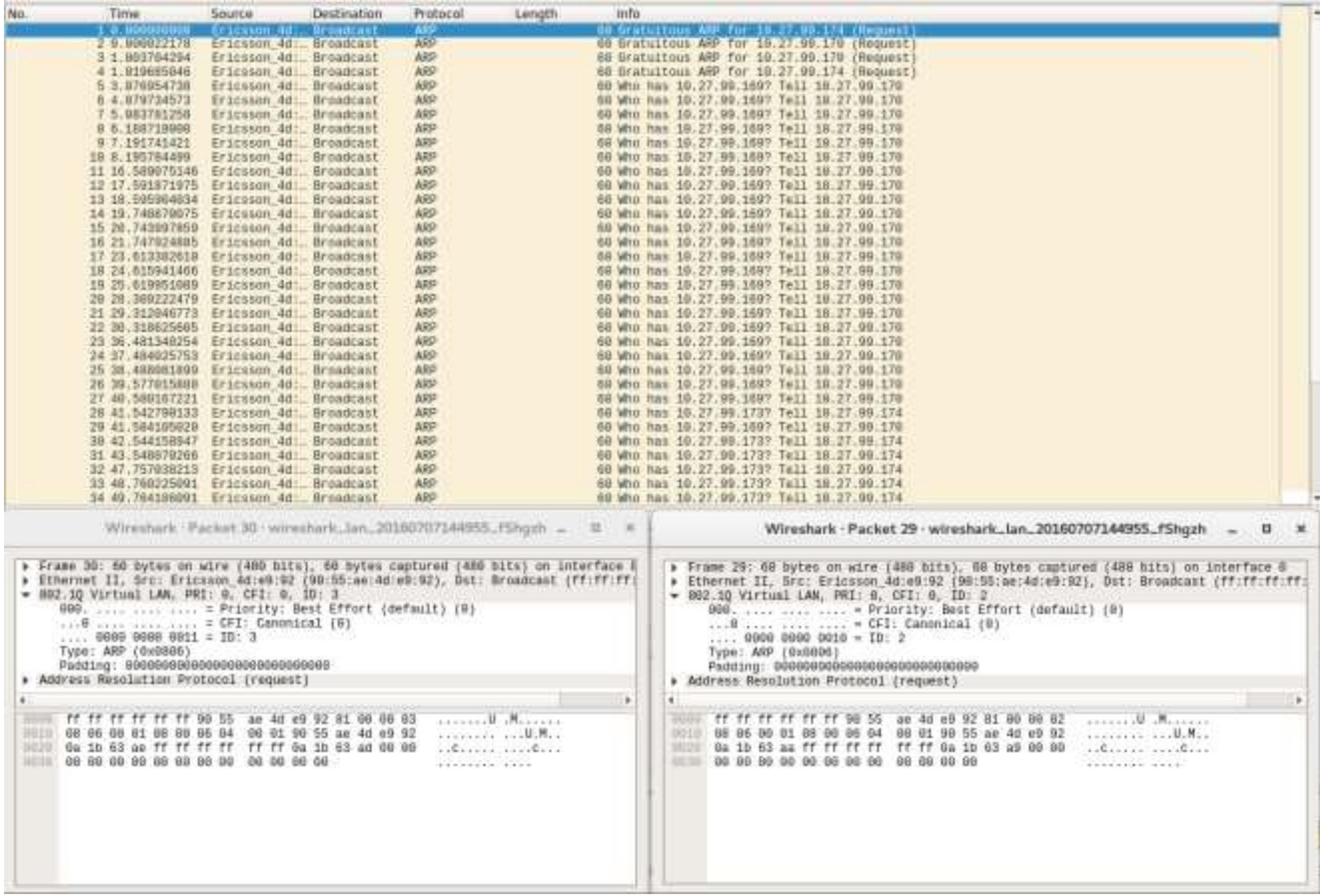
CAUTION
HIGH VOLTAGE TESTING IN PROGRESS
AUTHORIZED PERSONNEL ONLY

Ericsson RBS6601 - DUL RJ-45 & Gbic Interfaces

- GPS
  - For timing or positioning (during setup)
- EC
  - Connection to power unit
- AUX
  - For clustering multiple units
- LMT A
  - Local maintenance terminal A
- LMT B
  - Local maintenance terminal B
- TN A
  - Backhaul Access – S1

- IDL
  - Currently unknown
- TN B
  - Backhaul Access – S1
- A, B, C, D, E, F
  - Interfaces towards RRU

The First Sniff ☺



```
No.     Time            Source           Destination  Protocol  Length  Info
      1 0.000000000     Ericsson_4d:…    Broadcast    ARP               60 Gratuitous ARP for 10.27.99.174 (Request)
      2 0.000022178     Ericsson_4d:…    Broadcast    ARP               60 Gratuitous ARP for 10.27.99.170 (Request)
      3 1.003704294     Ericsson_4d:…    Broadcast    ARP               60 Gratuitous ARP for 10.27.99.170 (Request)
      4 1.019685046     Ericsson_4d:…    Broadcast    ARP               60 Gratuitous ARP for 10.27.99.174 (Request)
      5 3.076954738     Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
      6 4.079734573     Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
      7 5.083781258     Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
      8 6.188719000     Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
      9 7.191741421     Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     10 8.195784499     Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     11 16.589075146    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     12 17.591871975    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     13 18.595904034    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     14 19.748679075    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     15 20.743897059    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     16 21.747924885    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     17 23.613382618    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     18 24.615941466    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     19 25.619951089    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     20 28.309222479    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     21 29.312046773    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     22 30.318625605    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     23 36.481348254    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     24 37.484025753    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     25 38.488081899    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     26 39.577015808    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     27 40.580167221    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     28 41.542798133    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.173? Tell 10.27.99.174
     29 41.584105028    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.169? Tell 10.27.99.170
     30 42.544158947    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.173? Tell 10.27.99.174
     31 43.548079266    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.173? Tell 10.27.99.174
     32 47.757038213    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.173? Tell 10.27.99.174
     33 48.760225091    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.173? Tell 10.27.99.174
     34 49.764186091    Ericsson_4d:…    Broadcast    ARP               60 Who has 10.27.99.173? Tell 10.27.99.174
```

Wireshark · Packet 30 · wireshark_lan_20160707144955_fShgzh

```
▸ Frame 30: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Ericsson_4d:e9:92 (90:55:ae:4d:e9:92), Dst: Broadcast (ff:ff:ff:
▾ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 3
     000. .... .... .... = Priority: Best Effort (default) (0)
     ...0 .... .... .... = CFI: Canonical (0)
     .... 0000 0000 0011 = ID: 3
     Type: ARP (0x0806)
     Padding: 0000000000000000000000000000
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 90 55  ae 4d e9 92 81 00 00 03   .......U .M......
0010  08 06 00 01 08 00 06 04  00 01 90 55 ae 4d e9 92   ........ ...U.M..
0020  0a 1b 63 ae ff ff ff ff  ff ff 0a 1b 63 ad 00 00   ..c..... ....c...
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Wireshark · Packet 29 · wireshark_lan_20160707144955_fShgzh

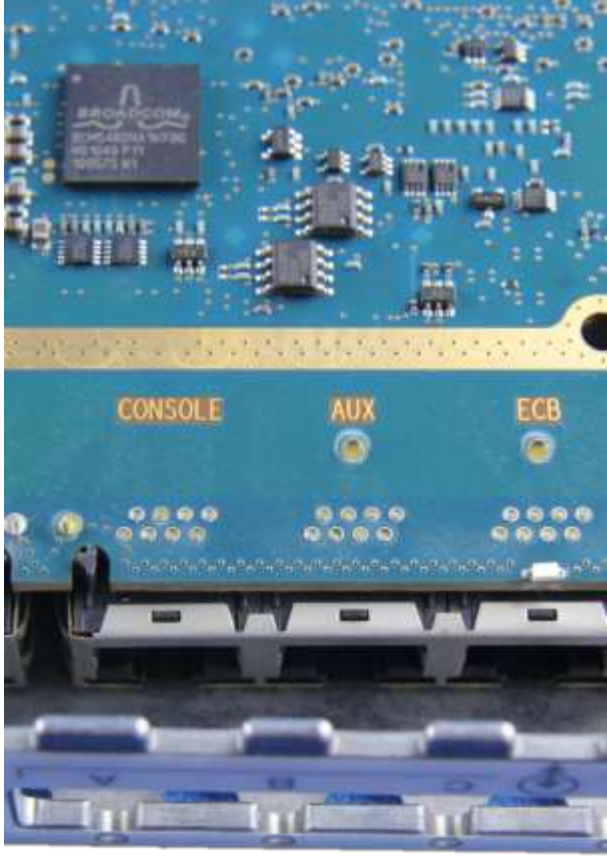
```
▸ Frame 29: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Ericsson_4d:e9:92 (90:55:ae:4d:e9:92), Dst: Broadcast (ff:ff:ff:ff:
▾ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
     000. .... .... .... = Priority: Best Effort (default) (0)
     ...0 .... .... .... = CFI: Canonical (0)
     .... 0000 0000 0010 = ID: 2
     Type: ARP (0x0806)
     Padding: 0000000000000000000000000000
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 90 55  ae 4d e9 92 81 00 00 02   .......U .M......
0010  08 06 00 01 08 00 06 04  00 01 90 55 ae 4d e9 92   ........ ...U.M..
0020  0a 1b 63 aa ff ff ff ff  ff ff 0a 1b 63 a9 00 00   ..c..... ....c...
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Let‘s get Started!

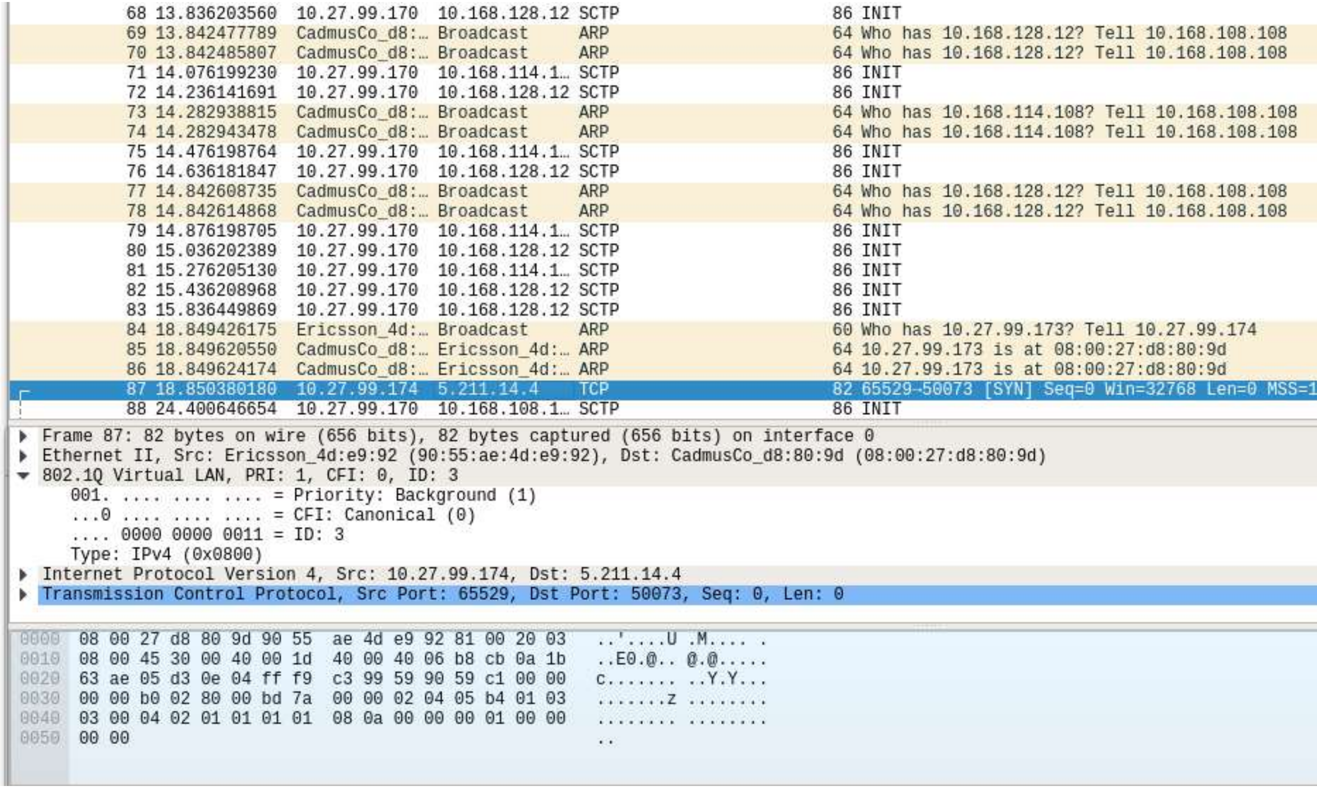
- We had to emulate Signalling and O&M Connection
  - Vlan 3: Signalling
  - Vlan 2: O&M

- You see a lot of traffic, the eNB is designed to operate almost as standalone

  → Not that many modifications needed



The Second Sniff



```
68 13.836203560  10.27.99.170  10.168.128.12 SCTP      86 INIT
69 13.842477789  CadmusCo_d8:… Broadcast     ARP       64 Who has 10.168.128.12? Tell 10.168.108.108
70 13.842485807  CadmusCo_d8:… Broadcast     ARP       64 Who has 10.168.128.12? Tell 10.168.108.108
71 14.076199230  10.27.99.170  10.168.114.1… SCTP      86 INIT
72 14.236141691  10.27.99.170  10.168.128.12 SCTP      86 INIT
73 14.282938815  CadmusCo_d8:… Broadcast     ARP       64 Who has 10.168.114.108? Tell 10.168.108.108
74 14.282943478  CadmusCo_d8:… Broadcast     ARP       64 Who has 10.168.114.108? Tell 10.168.108.108
75 14.476198764  10.27.99.170  10.168.114.1… SCTP      86 INIT
76 14.636181847  10.27.99.170  10.168.128.12 SCTP      86 INIT
77 14.842608735  CadmusCo_d8:… Broadcast     ARP       64 Who has 10.168.128.12? Tell 10.168.108.108
78 14.842614868  CadmusCo_d8:… Broadcast     ARP       64 Who has 10.168.128.12? Tell 10.168.108.108
79 14.876198705  10.27.99.170  10.168.114.1… SCTP      86 INIT
80 15.036202389  10.27.99.170  10.168.128.12 SCTP      86 INIT
81 15.276205130  10.27.99.170  10.168.114.1… SCTP      86 INIT
82 15.436208968  10.27.99.170  10.168.128.12 SCTP      86 INIT
83 15.836449869  10.27.99.170  10.168.128.12 SCTP      86 INIT
84 18.849426175  Ericsson_4d:… Broadcast     ARP       60 Who has 10.27.99.173? Tell 10.27.99.174
85 18.849620550  CadmusCo_d8:… Ericsson_4d:… ARP       64 10.27.99.173 is at 08:00:27:d8:80:9d
86 18.849624174  CadmusCo_d8:… Ericsson_4d:… ARP       64 10.27.99.173 is at 08:00:27:d8:80:9d
87 18.850380180  10.27.99.174  5.211.14.4    TCP       82 65529→50073 [SYN] Seq=0 Win=32768 Len=0 MSS=1
88 24.400646654  10.27.99.170  10.168.108.1… SCTP      86 INIT

▸ Frame 87: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▸ Ethernet II, Src: Ericsson_4d:e9:92 (90:55:ae:4d:e9:92), Dst: CadmusCo_d8:80:9d (08:00:27:d8:80:9d)
▾ 802.1Q Virtual LAN, PRI: 1, CFI: 0, ID: 3
    001. .... .... .... = Priority: Background (1)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0000 0011 = ID: 3
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.27.99.174, Dst: 5.211.14.4
▸ Transmission Control Protocol, Src Port: 65529, Dst Port: 50073, Seq: 0, Len: 0

0000  08 00 27 d8 80 9d 90 55  ae 4d e9 92 81 00 20 03   ..'....U .M.... .
0010  08 00 45 30 00 40 00 1d  40 00 40 06 b8 cb 0a 1b   ..E0.@.. @.@.....
0020  63 ae 05 d3 0e 04 ff f9  c3 99 59 90 59 c1 00 00   c....... ..Y.Y...
0030  00 00 b0 02 80 00 bd 7a  00 00 02 04 05 b4 01 03   .......z ........
0040  03 00 04 02 01 01 01 01  08 0a 00 00 00 01 00 00   ........ ........
0050  00 00                                              ..
```

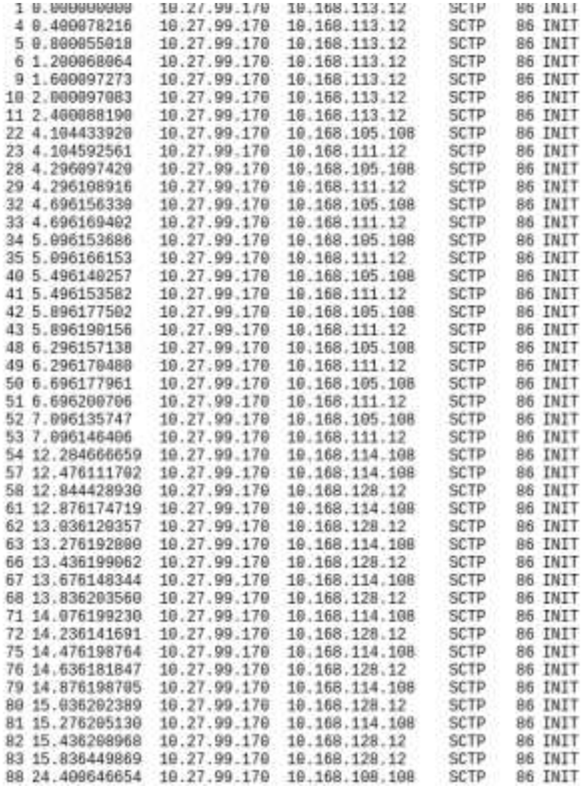
The Transport Interface

Build Your Own Provider Network

ERNW
providing security.

S1-Interface

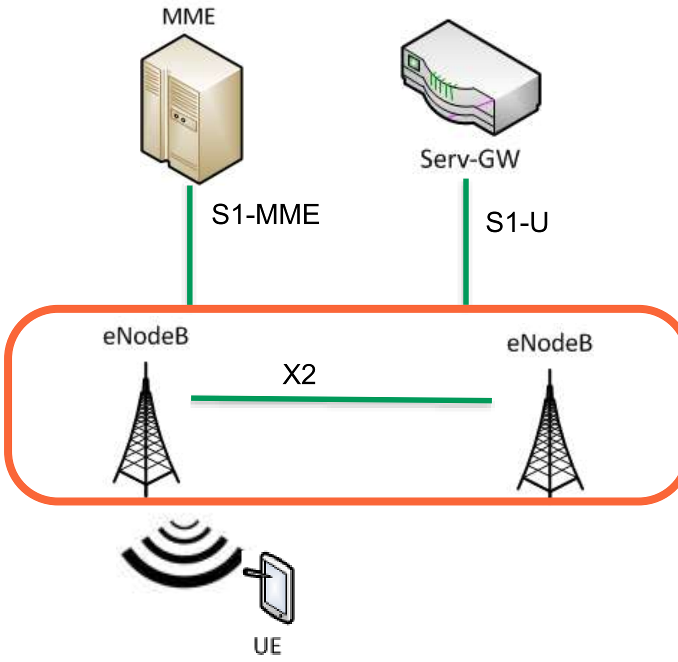
- After the host 10.27.99.169 on VLAN 2 becomes available the eNodeB activates communication over the S1-Interface
- Using SCTP it tried to reach 7 different hosts by SCTP INIT request to establish a connection



```
 1 0.000000000   10.27.99.170  10.168.113.12     SCTP   86 INIT
 4 0.400078216   10.27.99.170  10.168.113.12     SCTP   86 INIT
 5 0.800055018   10.27.99.170  10.168.113.12     SCTP   86 INIT
 6 1.200068064   10.27.99.170  10.168.113.12     SCTP   86 INIT
 9 1.600097273   10.27.99.170  10.168.113.12     SCTP   86 INIT
10 2.000097083   10.27.99.170  10.168.113.12     SCTP   86 INIT
11 2.400088190   10.27.99.170  10.168.113.12     SCTP   86 INIT
22 4.104433920   10.27.99.170  10.168.105.108    SCTP   86 INIT
23 4.104592561   10.27.99.170  10.168.111.12     SCTP   86 INIT
28 4.296097420   10.27.99.170  10.168.105.108    SCTP   86 INIT
29 4.296108916   10.27.99.170  10.168.111.12     SCTP   86 INIT
32 4.696156330   10.27.99.170  10.168.105.108    SCTP   86 INIT
33 4.696169402   10.27.99.170  10.168.111.12     SCTP   86 INIT
34 5.096153686   10.27.99.170  10.168.105.108    SCTP   86 INIT
35 5.096166153   10.27.99.170  10.168.111.12     SCTP   86 INIT
40 5.496140257   10.27.99.170  10.168.105.108    SCTP   86 INIT
41 5.496153582   10.27.99.170  10.168.111.12     SCTP   86 INIT
42 5.896177502   10.27.99.170  10.168.105.108    SCTP   86 INIT
43 5.896190156   10.27.99.170  10.168.111.12     SCTP   86 INIT
48 6.296157138   10.27.99.170  10.168.105.108    SCTP   86 INIT
49 6.296170488   10.27.99.170  10.168.111.12     SCTP   86 INIT
50 6.696177961   10.27.99.170  10.168.105.108    SCTP   86 INIT
51 6.696200706   10.27.99.170  10.168.111.12     SCTP   86 INIT
52 7.096135747   10.27.99.170  10.168.105.108    SCTP   86 INIT
53 7.096146406   10.27.99.170  10.168.111.12     SCTP   86 INIT
54 12.284666659  10.27.99.170  10.168.114.108    SCTP   86 INIT
57 12.476111702  10.27.99.170  10.168.114.108    SCTP   86 INIT
58 12.844428930  10.27.99.170  10.168.128.12     SCTP   86 INIT
61 12.876174719  10.27.99.170  10.168.114.108    SCTP   86 INIT
62 13.036120357  10.27.99.170  10.168.128.12     SCTP   86 INIT
63 13.276192080  10.27.99.170  10.168.114.108    SCTP   86 INIT
66 13.436199062  10.27.99.170  10.168.128.12     SCTP   86 INIT
67 13.676148344  10.27.99.170  10.168.114.108    SCTP   86 INIT
68 13.836203560  10.27.99.170  10.168.128.12     SCTP   86 INIT
71 14.076199230  10.27.99.170  10.168.114.108    SCTP   86 INIT
72 14.236141691  10.27.99.170  10.168.128.12     SCTP   86 INIT
75 14.476198764  10.27.99.170  10.168.114.108    SCTP   86 INIT
76 14.636181847  10.27.99.170  10.168.128.12     SCTP   86 INIT
79 14.876198705  10.27.99.170  10.168.114.108    SCTP   86 INIT
80 15.036202389  10.27.99.170  10.168.128.12     SCTP   86 INIT
81 15.276205130  10.27.99.170  10.168.114.108    SCTP   86 INIT
82 15.436208968  10.27.99.170  10.168.128.12     SCTP   86 INIT
83 15.836449869  10.27.99.170  10.168.128.12     SCTP   86 INIT
88 24.400646654  10.27.99.170  10.168.100.108    SCTP   86 INIT
```

S1-Interface

- 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

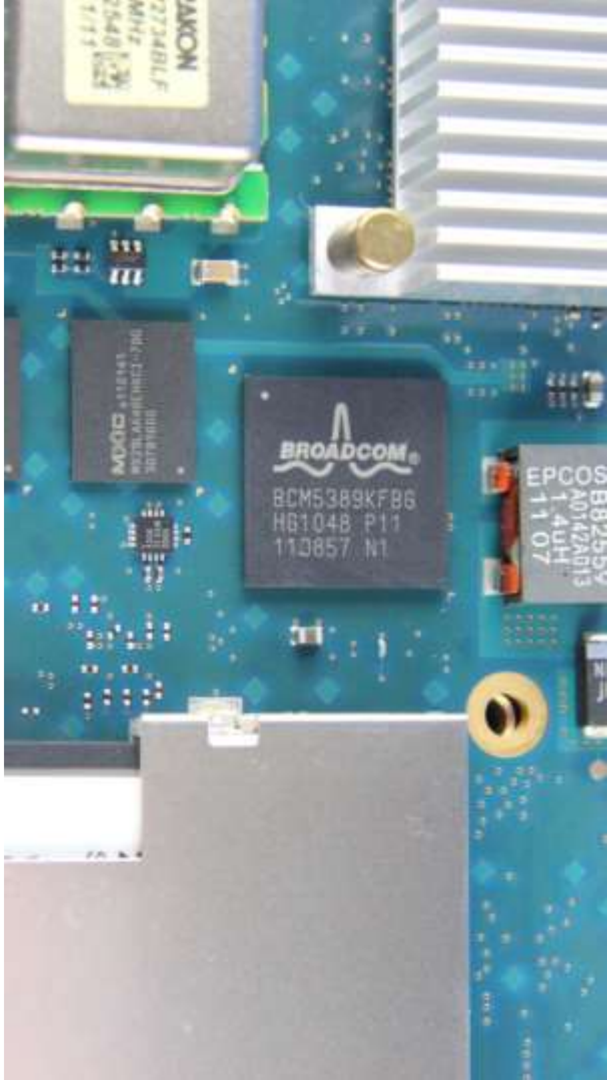


From 3GPP TS 33.401

- "In order to protect **the S1 and X2 control plane** as required by clause 5.3.4a, it is **required to implement IPsec** ESP according to RFC 4303 [7] as specified by TS 33.210 [5]. For both **S1-MME and X2-C**, IKEv2 certificates based authentication according to TS 33.310 [6] shall be implemented"
  - "NOTE 1: In case control plane **interfaces are trusted** (e.g. physically protected), there is **no need to use protection** according to TS 33.210 [5] and TS 33.310 [6]."

- "In order to protect the **S1 and X2 user plane** as required by clause 5.3.4, it is **required to implement IPsec** ESP according to RFC 4303 [7] as profiled by TS 33.210 [5], with confidentiality, integrity and replay 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**."

- "In order to achieve such protection, IPsec ESP according to RFC 4303 [7] as profiled by TS 33.210 [5] **shall be implemented for all O&M related traffic**, i.e. the management plane, with confidentiality, integrity and replay protection."
  - "NOTE 2: In case the S1 management plane **interfaces are trusted** (e.g. physically protected), the use of protection based on IPsec/IKEv2 or equivalent mechanisms is **not needed**."

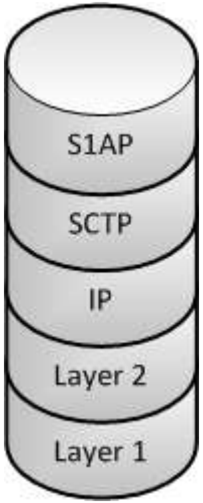


S1-AP

- S1 Application Protocol (S1AP), designed by 3GPP for the S1 interface
- Specified in 3GPP TS36.413

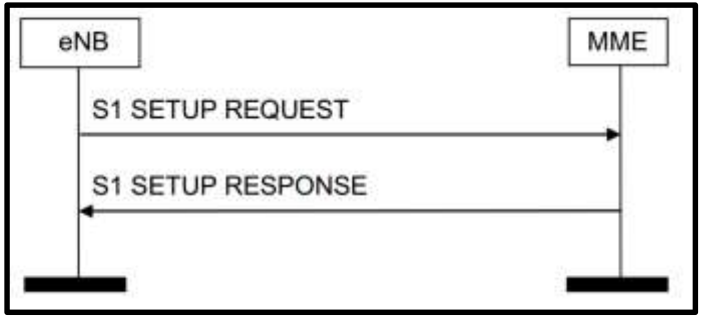
- Necessary for several procedures between MME and eNodeB
- Also supports transparent transport procedures from MME to the user equipment

- SCTP Destination Port 36412



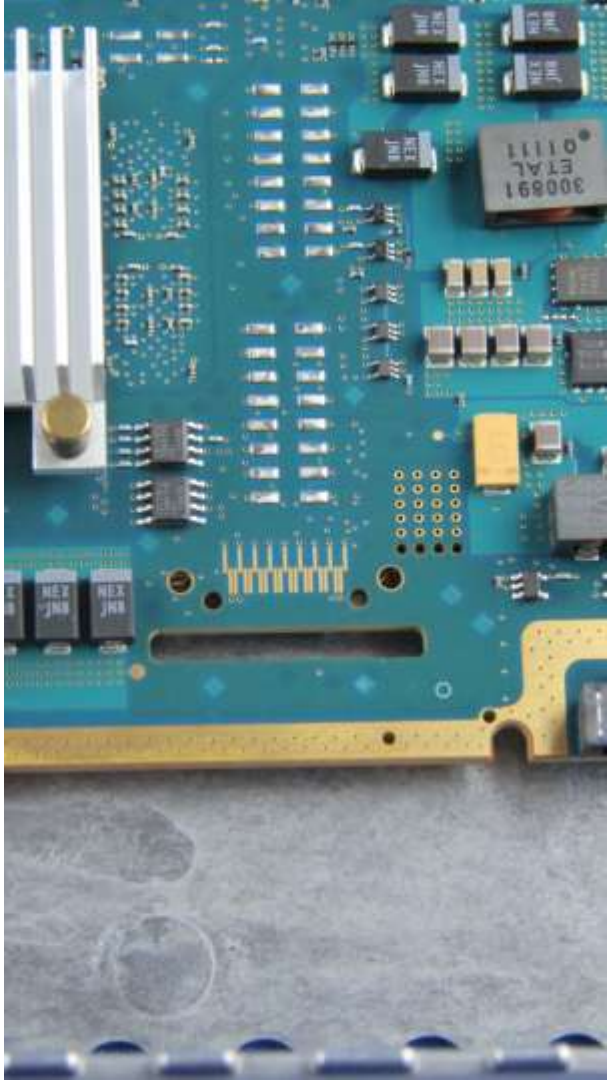
Let‘s get Started!

- S1-MME: Basically, only the S1 Setup Request is needed.
  - fake_mme.py



Working with S1AP

- After S1 Setup Request, a couple of messages can be sent.
- S1AP Scanner published in the past
  - S1AP_enum (www.insinuator.net)
- New scripts: sctp_mitm.py



ERNW
providing security.

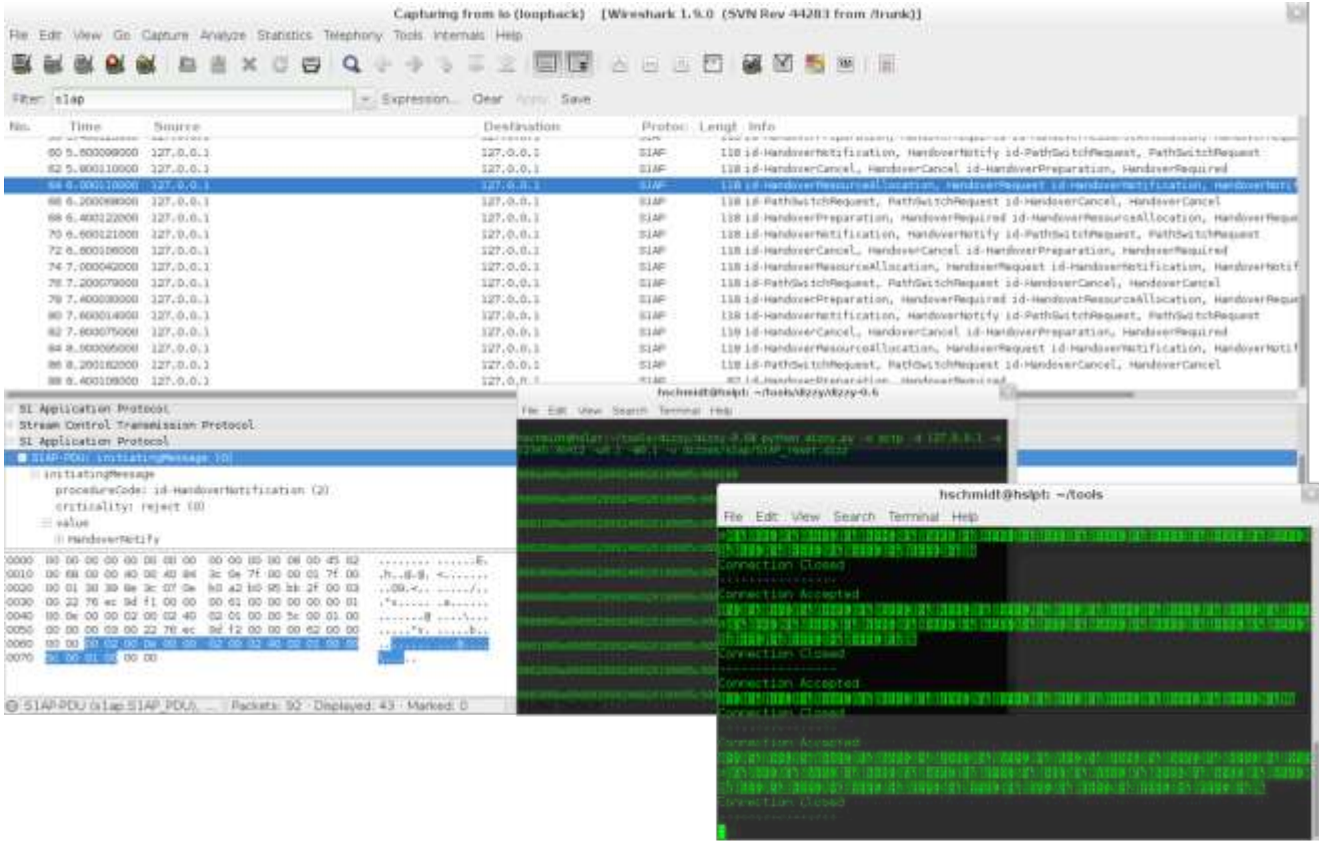
S1AP and X2AP Functions Overview

- 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

S1AP with Dizzy

www.insinuator.net

www.c0decafe.de



Capturing from lo (loopback) [Wireshark 1.9.0 (SVN Rev 44283 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: s1ap
Expression... Clear Apply Save

```
No.  Time          Source      Destination  Protoc Lengt Info
  60 5.800098000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverNotification, HandoverNotify id-PathSwitchRequest, PathSwitchRequest
  62 5.800110000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverCancel, HandoverCancel id-HandoverPreparation, HandoverRequired
  64 6.000110000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverResourceAllocation, HandoverRequest id-HandoverNotification, HandoverNotif
  66 6.200098000   127.0.0.1   127.0.0.1    S1AP   118 id-PathSwitchRequest, PathSwitchRequest id-HandoverCancel, HandoverCancel
  68 6.400122000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverPreparation, HandoverRequired id-HandoverResourceAllocation, HandoverReque
  70 6.600121000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverNotification, HandoverNotify id-PathSwitchRequest, PathSwitchRequest
  72 6.800108000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverCancel, HandoverCancel id-HandoverPreparation, HandoverRequired
  74 7.000042000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverResourceAllocation, HandoverRequest id-HandoverNotification, HandoverNotif
  76 7.200079000   127.0.0.1   127.0.0.1    S1AP   118 id-PathSwitchRequest, PathSwitchRequest id-HandoverCancel, HandoverCancel
  78 7.400030000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverPreparation, HandoverRequired id-HandovatResourceAllocation, HandoverReque
  80 7.600014000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverNotification, HandoverNotify id-PathSwitchRequest, PathSwitchRequest
  82 7.800075000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverCancel, HandoverCancel id-HandoverPreparation, HandoverRequired
  84 8.000095000   127.0.0.1   127.0.0.1    S1AP   118 id-HandoverResourceAllocation, HandoverRequest id-HandoverNotification, HandoverNotif
  86 8.200182000   127.0.0.1   127.0.0.1    S1AP   118 id-PathSwitchRequest, PathSwitchRequest id-HandoverCancel, HandoverCancel
  88 8.400108000   127.0.0.1   127.0.0.1    S1AP    87 id-HandoverPreparation, HandoverRequired
```

```
S1 Application Protocol
Stream Control Transmission Protocol
S1 Application Protocol
  S1AP-PDU: initiatingMessage (0)
    initiatingMessage
      procedureCode: id-HandoverNotification (2)
      criticality: reject (0)
      value
        HandoverNotify
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 02   ..............E.
0010  00 68 00 00 40 00 40 84  3c 0e 7f 00 00 01 7f 00   .h..@.@.<.......
0020  00 01 38 39 0e 3c 07 0e  b0 a2 b0 95 bb 2f 00 03   ..89.<......./..
0030  00 22 76 ec 9d f1 00 00  00 61 00 00 00 00 00 01   ."v......a......
0040  00 0e 00 00 02 00 02 40  02 01 00 00 5c 00 01 00   .......@....\...
0050  00 00 00 00 00 22 76 ec  9d f2 00 00 00 62 00 00   ....."v......b..
0060  00 00 00 02 00 0e 00 00  02 00 02 40 00 01 00 00   ...........@....
0070  00 00 01 00 00 00                                  ......
```

S1AP-PDU (s1ap.S1AP_PDU), ... Packets: 92 · Displayed: 43 · Marked: 0

hschmidt@hslpt: ~/tools/dizzy/dizzy-0.6

```
hschmidt@hslpt:~/tools/dizzy/dizzy-0.6$ python dizzy.py -o sctp -d 127.0.0.1 -e
[illegible] dizzes/s1ap/S1AP_reset.dizz
```

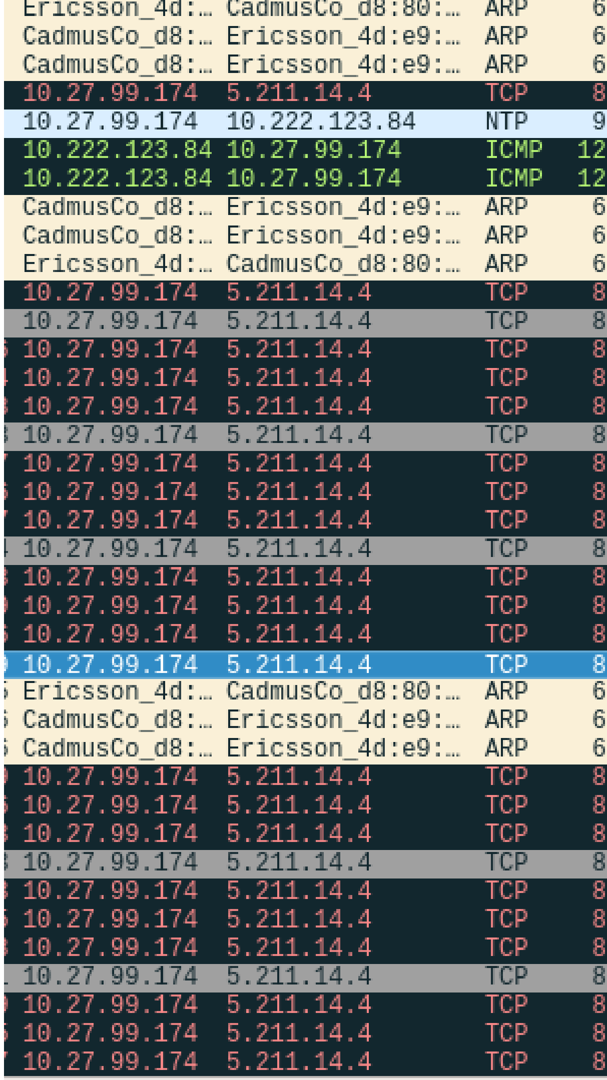
hschmidt@hslpt: ~/tools

```
Connection Closed
-----------------
Connection Accepted
Connection Closed
-----------------
Connection Accepted
Connection Closed
-----------------
Connection Accepted
Connection Closed
-----------------
```

Operations & Maintenance Network

OAM Network

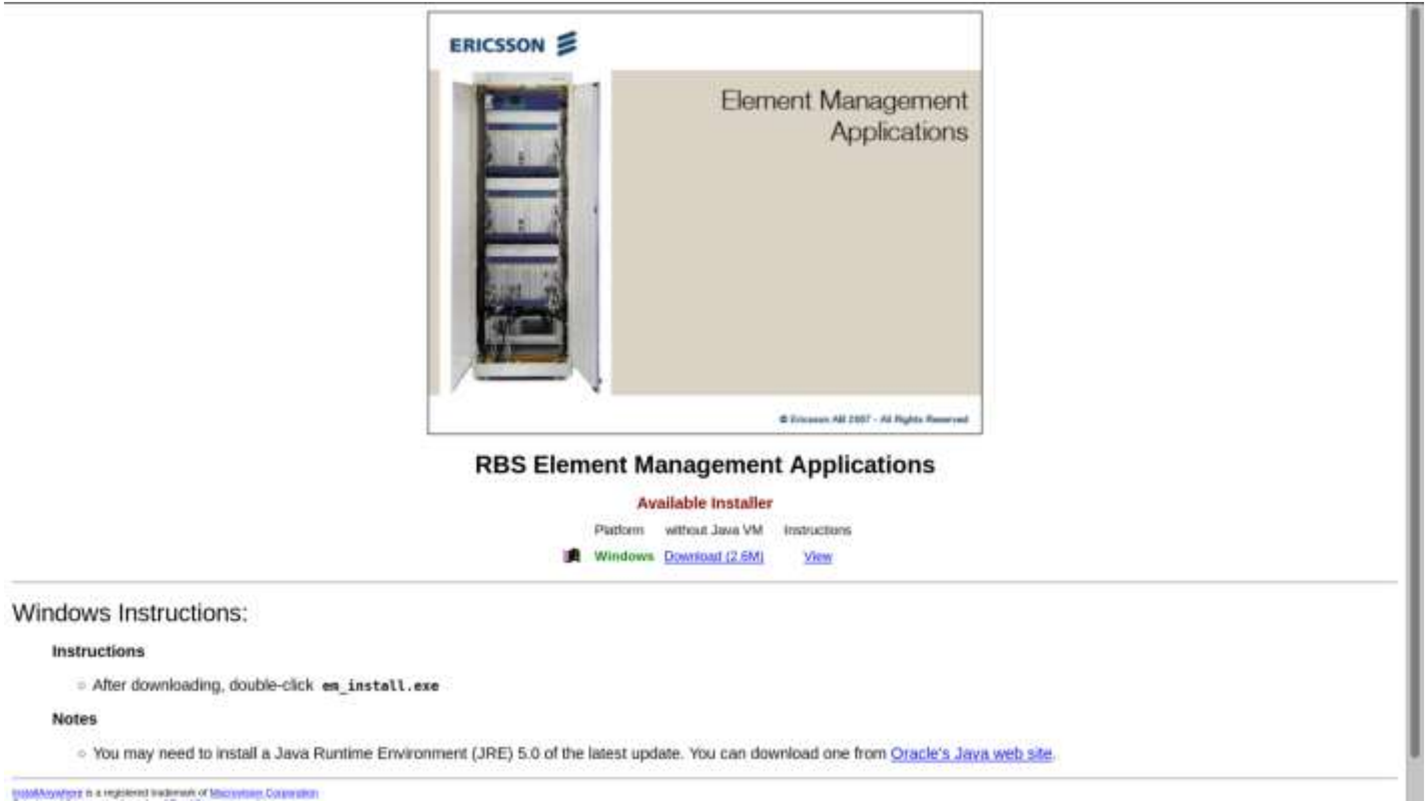
- After the host 10.27.99.173 on VLAN 3 becomes available the eNodeB starts searching for an NTP
- It also tries to establish a TCP session to some management system



```
Ericsson_4d:… CadmusCo_d8:80:…  ARP   6
CadmusCo_d8:… Ericsson_4d:e9:…  ARP   6
CadmusCo_d8:… Ericsson_4d:e9:…  ARP   6
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  10.222.123.84     NTP   9
10.222.123.84 10.27.99.174      ICMP 12
10.222.123.84 10.27.99.174      ICMP 12
CadmusCo_d8:… Ericsson_4d:e9:…  ARP   6
CadmusCo_d8:… Ericsson_4d:e9:…  ARP   6
Ericsson_4d:… CadmusCo_d8:80:…  ARP   6
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
Ericsson_4d:… CadmusCo_d8:80:…  ARP   6
CadmusCo_d8:… Ericsson_4d:e9:…  ARP   6
CadmusCo_d8:… Ericsson_4d:e9:…  ARP   6
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
10.27.99.174  5.211.14.4        TCP   8
```

Nmap Results

```
Increasing send delay for 10.27.99.174 from 0 to 5 due to 45 out of 149 dropped probes since last increase.
Nmap scan report for 10.27.99.174
Host is up, received arp-response (0.00042s latency).
Scanned at 2015-12-28 19:16:02 CET for 842s
Not shown: 65529 closed ports
Reason: 65529 resets
PORT      STATE SERVICE    REASON        VERSION
21/tcp    open  ftp        syn-ack ttl 64
22/tcp    open  ssh        syn-ack ttl 64 (protocol 2.0)
| ssh-hostkey:
|   1024 39:6b:50:b5:68:ea:cf:f9:1b:85:48:dc:cb:5f:9c:dc (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAKjBoRJD3xs/PDF7i8Zh6VVNlnykkT0aZ/OJoZM0Qb/2Zm1SruM5bYkwAczqstUWXygtgSTmP4
Dv5VHNkmR5Gb5KIe2e5GXNp4HACdAVjThkpBzK27ai+Pj+CXIHQxHcZIMgJyQDA29oCg5KFk9lbtdDkiocabW/KyuAQmxB0
mIVAAAAFQCPdjPIB+E7/0QKPKXG0pcRglibLQAAAIBLD689UE2fmlufS53dHWsgxm9SsGD4GgP4bnRfV+G494PNfimiVv0W
oqAeDFtVqQLIxZHU2pJ275kgRyDHcp4fTaPssxZpljyVNiZkjLjDVeZb8D562E4PnG3BVFy2VcMrq4klbO02wKwE5zQrLQfGf7O
o1rv81+1OdpZzU3N48wAAAIEAhj3FTj4i2s8vKEVXzUtdK081YHhyvOJO77niYmJ+jG2IOtt4tJpuNfvdc19ab2wtrqerQ1R6KTA9
2InhktEZvS2e4peeVho0htYoDlDQTybpw5v/LaX8c0/7vtcKJt7On+A0rZwCAd2ScQxNKpcyJAqNf9J+esFJXo9KONWkpms=
|   1024 e8:c6:48:a5:f8:7b:ed:c3:6b:30:86:a6:42:c6:04:a6 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAz4L21u3pCegfIuLO+iz8te/XmrNhNSeCFf9SCwd8GYL7D1yktvdhn3kFPb+4gwM2B+sIn
hs0TM6+bt7HfW7AU0cPTMy3kgLxvOKU9V+Sm8QzvZSJkkKmbfnwRHY7IVvFSHNZPghWupcDUb7h7z+h3Q3BlcZP7ZQIFPd
3zXEyxIM=
23/tcp    open  telnet     syn-ack ttl 64
80/tcp    open  http       syn-ack ttl 64 WEBS - OSE web server
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: WEBS - OSE web server
|_http-title: 404 URL Not Found
8443/tcp  open  tcpwrapped syn-ack ttl 64
|_xmlrpc-methods: ERROR: Script execution failed (use -d to debug)
56834/tcp open  unknown    syn-ack ttl 64
```



ERICSSON

Element Management
Applications

© Ericsson AB 2007 - All Rights Reserved

RBS Element Management Applications

Available Installer

Platform	without Java VM	Instructions
Windows	Download (2.6M)	View

Windows Instructions:

Instructions

- After downloading, double-click `em_install.exe`

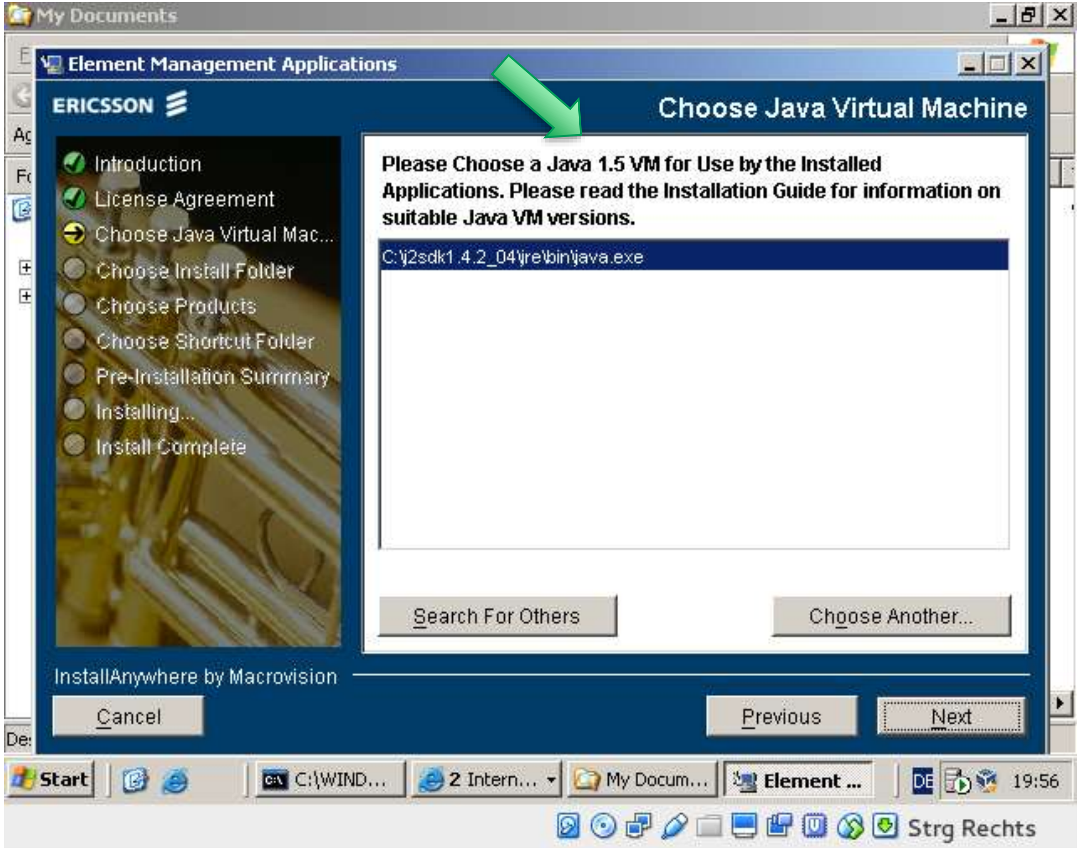
Notes

- You may need to install a Java Runtime Environment (JRE) 5.0 of the latest update. You can download one from Oracle's Java web site.

InstallAnywhere is a registered trademark of Macrovision Corporation.

LMT Software Installation

... and Windows XP ...



Please Choose a Java 1.5 VM for Use by the Installed Applications. Please read the Installation Guide for information on suitable Java VM versions.

C:\j2sdk1.4.2_04\jre\bin\java.exe

Local Maintenance Terminal

- The workflow
  1. Fault-State of BaseStation (NoService)
  2. Engineer moves on-site
  3. Engineer connects to BTS with $tool
  4. Engineer accesses debug information
  5. Engineer adjusts configuration

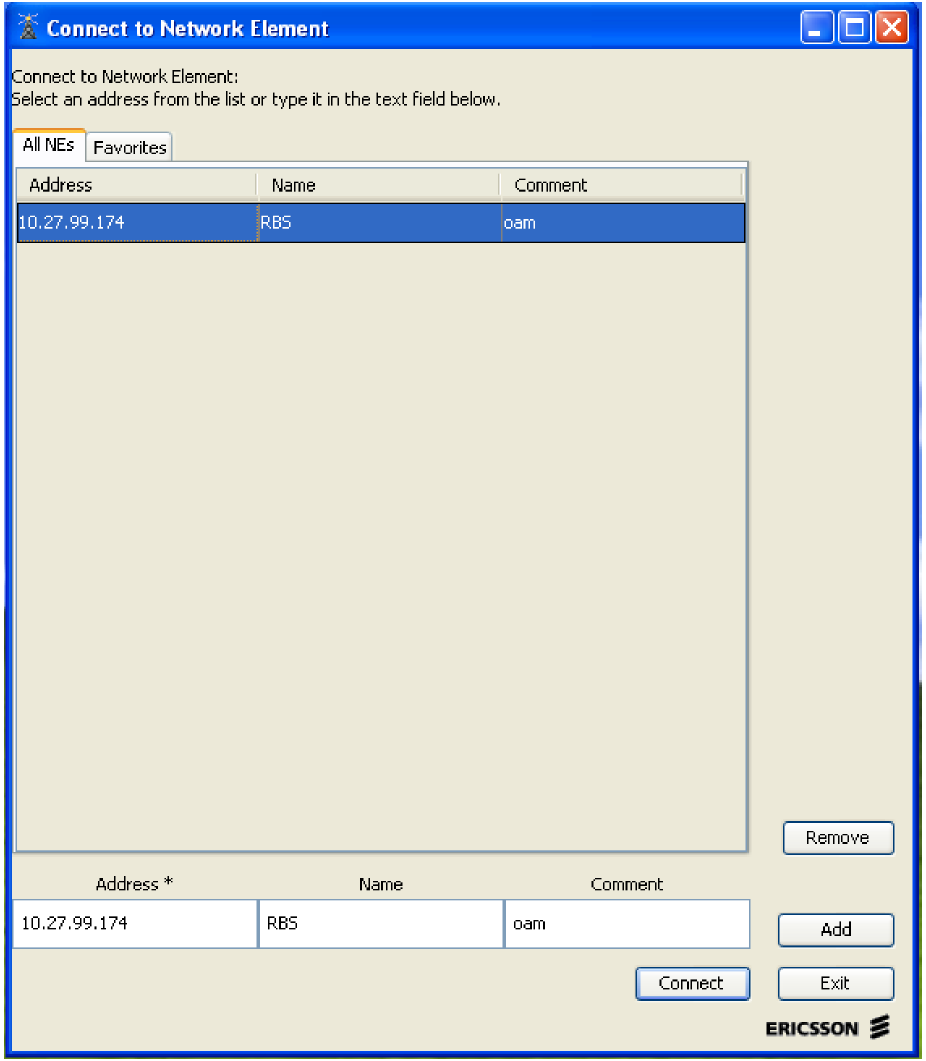
More on eNB Security

> “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. ”

- But, anyhow: 4G BaseStations are *yet another Network Device with IP connection*.

From 3GPP TS 33.401

Element Manager



Connect to Network Element

Connect to Network Element:
Select an address from the list or type it in the text field below.

Address	Name	Comment
10.27.99.174	RBS	oam

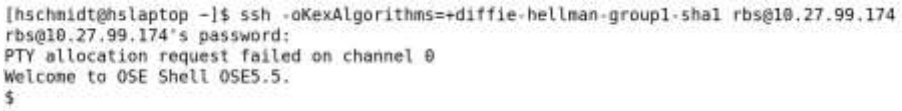
Address *: 10.27.99.174
Name: RBS
Comment: oam

What we see

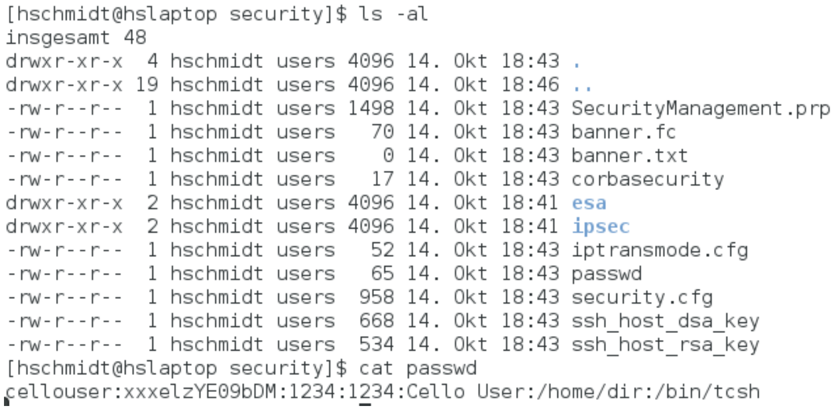
- Totally outdated Java
- EM is not asking for a password
- EM is based on HTTP and GIOP
  - Transmits current configuration data of the BTS
  - Configuration changes can be made

Well...

- Username: rbs / cellouser
  - Password: rbs



```
[hschmidt@hslaptop ~]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 rbs@10.27.99.174
rbs@10.27.99.174's password:
PTY allocation request failed on channel 0
Welcome to OSE Shell OSE5.5.
$
```

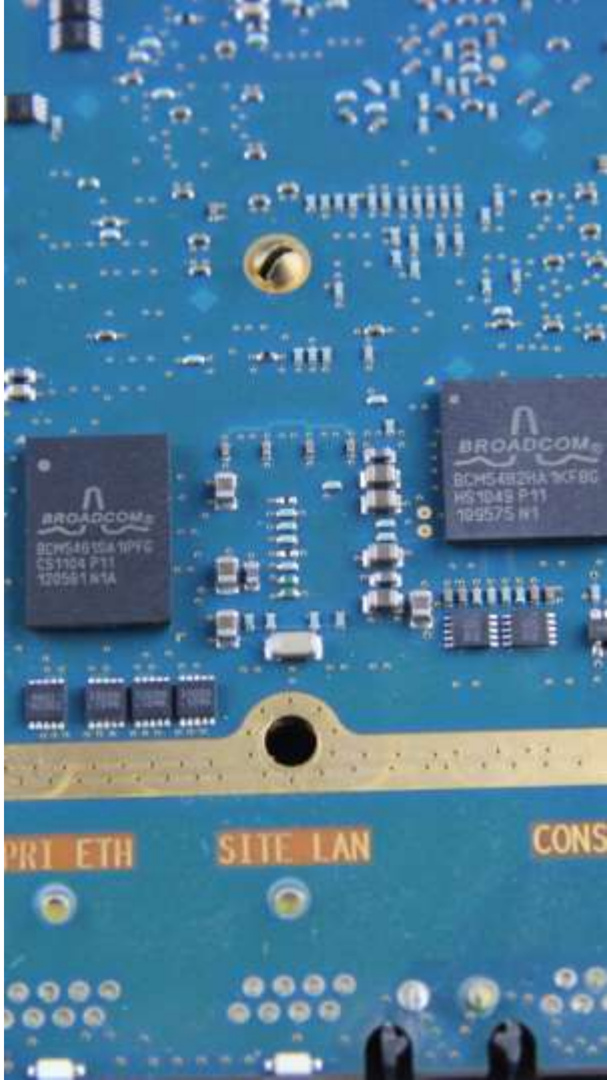


```
[hschmidt@hslaptop security]$ ls -al
insgesamt 48
drwxr-xr-x  4 hschmidt users 4096 14. Okt 18:43 .
drwxr-xr-x 19 hschmidt users 4096 14. Okt 18:46 ..
-rw-r--r--  1 hschmidt users 1498 14. Okt 18:43 SecurityManagement.prp
-rw-r--r--  1 hschmidt users   70 14. Okt 18:43 banner.fc
-rw-r--r--  1 hschmidt users    0 14. Okt 18:43 banner.txt
-rw-r--r--  1 hschmidt users   17 14. Okt 18:43 corbasecurity
drwxr-xr-x  2 hschmidt users 4096 14. Okt 18:41 esa
drwxr-xr-x  2 hschmidt users 4096 14. Okt 18:41 ipsec
-rw-r--r--  1 hschmidt users   52 14. Okt 18:43 iptransmode.cfg
-rw-r--r--  1 hschmidt users   65 14. Okt 18:43 passwd
-rw-r--r--  1 hschmidt users  958 14. Okt 18:43 security.cfg
-rw-r--r--  1 hschmidt users  668 14. Okt 18:43 ssh_host_dsa_key
-rw-r--r--  1 hschmidt users  534 14. Okt 18:43 ssh_host_rsa_key
[hschmidt@hslaptop security]$ cat passwd
cellouser:xxxelzYE09bDM:1234:1234:Cello User:/home/dir:/bin/tcsh
```

ERNW
providing security.

Webserver

- Running *WEBS - OSE web server*
  - EM Download
  - XML Configuration
- Java JDK (1.1.6, 1.2.1, 1.3.1, 1.4.2, 1.5.0, 1.6.0)
- Somehow, not very load resistant
  → Leading to a DoS of the whole machine



Insights

ERNW
providing security.

What We've Seen so far

- The device was obviously not wiped
- No IPSEC on S1 interface
- Hardcoded & default credentials
  - rbs – rbs
  - cellouser - rbs
- Telnet in use
- Unencrypted maintenance interface

And the BS belongs to…?

- Looks like a BaseStation from the US ☺

```
c/logfiles/alarm_event/ALARM_LOG.xml:1f1;x4;x4;EUtranCellFDD;SubNetwork=ONRM_
ROOT_MO_R,SubNetwork=PHL-
ENB,MeContext=PHLe0760889,ManagedElement=1,ENodeBFunction=1,EUtranCellFDD=P
HLe07608893;417;1355883768353300000;SubNetwork=ONRM_ROOT_MO_R,SubNetwork=
PHL-ENB,MeContext=PHLe0760889;356;6;ServiceUnavailable;0;S1 Connection failure for
PLMN mcc:311 mnc:660;SubNetwork=ONRM_ROOT_MO_R,SubNetwork=PHL-
ENB,MeContext=PHLe0760889_415;;0;2;0;0;
```

Using passwd

- We have the users cellouser and rbs
  - By the way, rbs is not in the passwd file

- While checking for use of hardcoded passwords in the management tool, we changed the user for rbs using passwd

- Afterwards cellouser's password was also change to the password

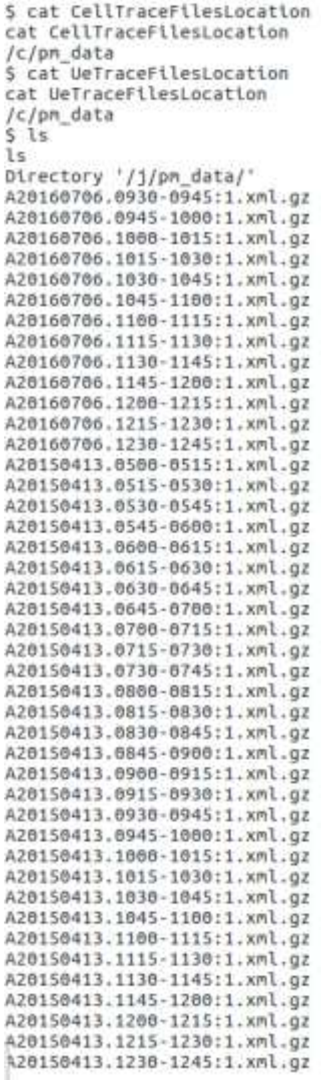
SSH

- SSH access to the device is enabled
- Sadly the only supported key exchange algorithm is disabled by default in current ssh clients
  - ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 rbs@10.27.99.174

Cell & UE Traces

- The eNodeB is able to create both traces for cells and UEs
- We found a set of traces on the device

- Sadly the traces seem to be purely cell traces
  - Containing data on packet loss etc.
  - No “interesting” information

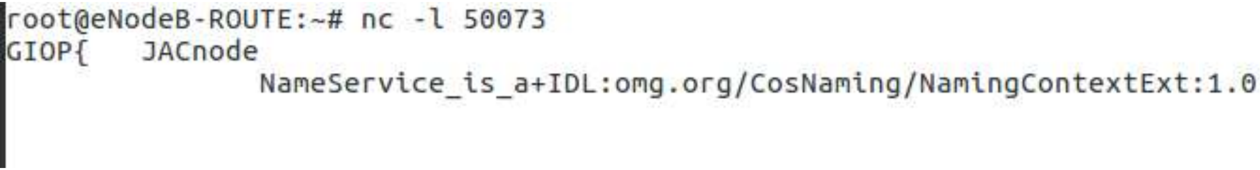


```
$ cat CellTraceFilesLocation
cat CellTraceFilesLocation
/c/pm_data
$ cat UeTraceFilesLocation
cat UeTraceFilesLocation
/c/pm_data
$ ls
ls
Directory '/j/pm_data/'
A20160706.0930-0945:1.xml.gz
A20160706.0945-1000:1.xml.gz
A20160706.1000-1015:1.xml.gz
A20160706.1015-1030:1.xml.gz
A20160706.1030-1045:1.xml.gz
A20160706.1045-1100:1.xml.gz
A20160706.1100-1115:1.xml.gz
A20160706.1115-1130:1.xml.gz
A20160706.1130-1145:1.xml.gz
A20160706.1145-1200:1.xml.gz
A20160706.1200-1215:1.xml.gz
A20160706.1215-1230:1.xml.gz
A20160706.1230-1245:1.xml.gz
A20150413.0500-0515:1.xml.gz
A20150413.0515-0530:1.xml.gz
A20150413.0530-0545:1.xml.gz
A20150413.0545-0600:1.xml.gz
A20150413.0600-0615:1.xml.gz
A20150413.0615-0630:1.xml.gz
A20150413.0630-0645:1.xml.gz
A20150413.0645-0700:1.xml.gz
A20150413.0700-0715:1.xml.gz
A20150413.0715-0730:1.xml.gz
A20150413.0730-0745:1.xml.gz
A20150413.0800-0815:1.xml.gz
A20150413.0815-0830:1.xml.gz
A20150413.0830-0845:1.xml.gz
A20150413.0845-0900:1.xml.gz
A20150413.0900-0915:1.xml.gz
A20150413.0915-0930:1.xml.gz
A20150413.0930-0945:1.xml.gz
A20150413.0945-1000:1.xml.gz
A20150413.1000-1015:1.xml.gz
A20150413.1015-1030:1.xml.gz
A20150413.1030-1045:1.xml.gz
A20150413.1045-1100:1.xml.gz
A20150413.1100-1115:1.xml.gz
A20150413.1115-1130:1.xml.gz
A20150413.1130-1145:1.xml.gz
A20150413.1145-1200:1.xml.gz
A20150413.1200-1215:1.xml.gz
A20150413.1215-1230:1.xml.gz
A20150413.1230-1245:1.xml.gz
```

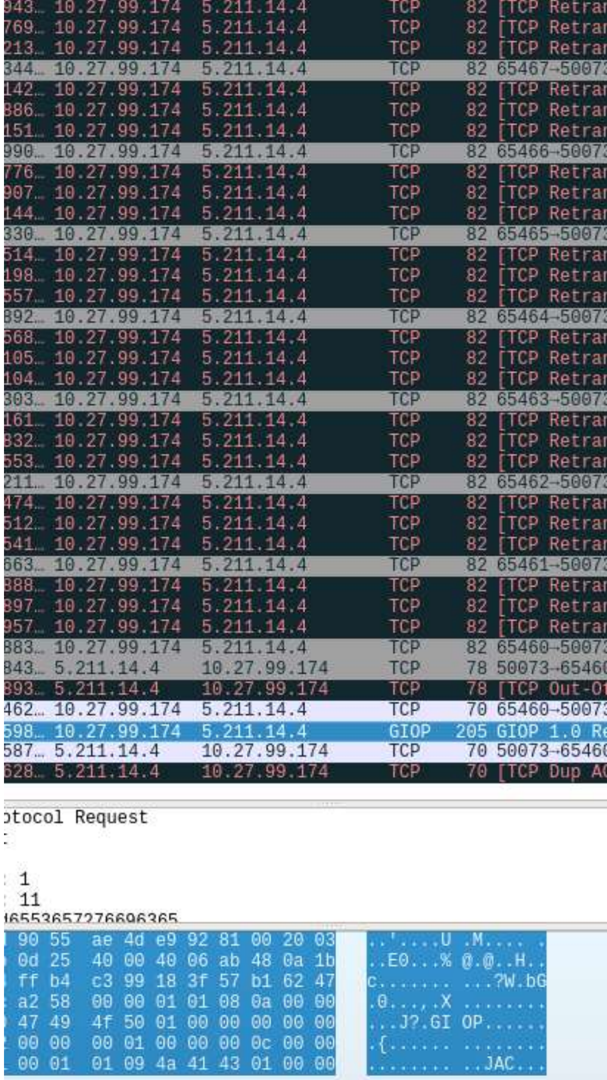
ERNW
providing security.

GIOP Remote Session

- The eNodeB ties to establish a TCP session with 5.211.14.4
- When connected it sends a simple GIOP request
- Seems to be: Java IDL: Interoperable Naming Service (INS)



```
root@eNodeB-ROUTE:~# nc -l 50073
GIOP{    JACnode
                NameService_is_a+IDL:omg.org/CosNaming/NamingContextExt:1.0
```



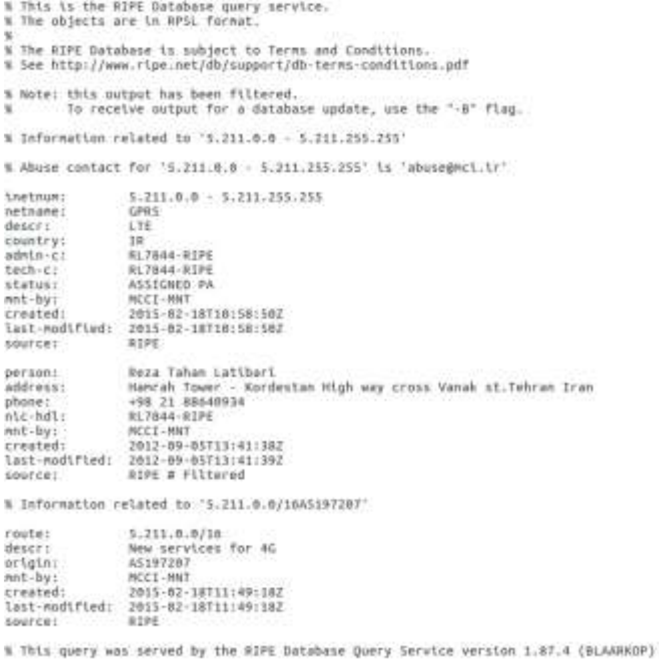
```
943… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
769… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
213… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
344… 10.27.99.174  5.211.14.4     TCP   82 65467→5007
142… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
886… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
151… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
990… 10.27.99.174  5.211.14.4     TCP   82 65466→5007
776… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
907… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
144… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
330… 10.27.99.174  5.211.14.4     TCP   82 65465→5007
514… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
198… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
557… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
892… 10.27.99.174  5.211.14.4     TCP   82 65464→5007
568… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
105… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
104… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
303… 10.27.99.174  5.211.14.4     TCP   82 65463→5007
161… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
832… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
553… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
211… 10.27.99.174  5.211.14.4     TCP   82 65462→5007
474… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
512… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
541… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
663… 10.27.99.174  5.211.14.4     TCP   82 65461→5007
888… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
897… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
957… 10.27.99.174  5.211.14.4     TCP   82 [TCP Retran
883… 10.27.99.174  5.211.14.4     TCP   82 65460→5007
843… 5.211.14.4    10.27.99.174   TCP   78 50073→6546
893… 5.211.14.4    10.27.99.174   TCP   78 [TCP Out-Of
462… 10.27.99.174  5.211.14.4     TCP   70 65460→5007
598… 10.27.99.174  5.211.14.4     GIOP 205 GIOP 1.0 Re
587… 5.211.14.4    10.27.99.174   TCP   70 50073→6546
628… 5.211.14.4    10.27.99.174   TCP   70 [TCP Dup AC
```

```
otocol Request
:

: 1
: 11
46553657276696365
```

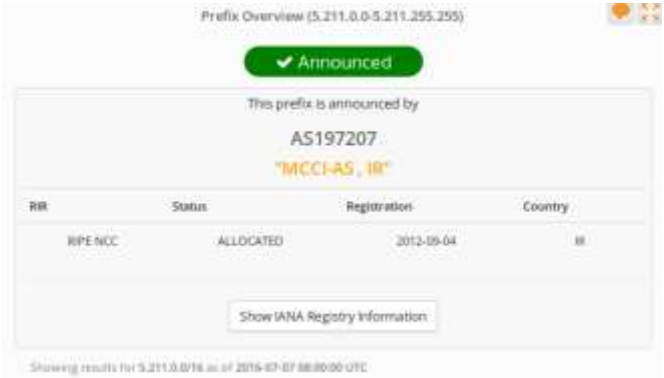
```
 90 55  ae 4d e9 92 81 00 20 03    ..'....U .M.....
 0d 25  40 00 40 06 ab 48 0a 1b    ..E0...% @.@..H..
 ff b4  c3 99 18 3f 57 b1 62 47    c....... ...?W.bG
 a2 58  00 00 01 01 08 0a 00 00    .0...,.X ........
 47 49  4f 50 01 00 00 00 00 00    ...J?.GI OP......
 00 00  00 01 00 00 00 0c 00 00    .{...... ........
 00 01  01 09 4a 41 43 01 00 00    ........ ...JAC...
```

IP Address: 5.211.14.4

- This is the only public IP address the device talks to
- Strangely (reminder of the operator: MetroPCS, USA) the IP address is located in Iran
- From the dates we've seen the eNodeB was initially provisioned and setup in 2013
  - The IP address range was registered in 2012 for an Iranian telco



```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '5.211.0.0 - 5.211.255.255'

% Abuse contact for '5.211.0.0 - 5.211.255.255' is 'abuse@mci.ir'

inetnum:        5.211.0.0 - 5.211.255.255
netname:        GPRS
descr:          LTE
country:        IR
admin-c:        RL7844-RIPE
tech-c:         RL7844-RIPE
status:         ASSIGNED PA
mnt-by:         MCCI-MNT
created:        2015-02-18T10:58:50Z
last-modified:  2015-02-18T10:58:50Z
source:         RIPE

person:         Reza Tahan Latibari
address:        Hamrah Tower - Kordestan High way cross Vanak st.Tehran Iran
phone:          +98 21 88640934
nic-hdl:        RL7844-RIPE
mnt-by:         MCCI-MNT
created:        2012-09-05T13:41:38Z
last-modified:  2012-09-05T13:41:39Z
source:         RIPE # Filtered

% Information related to '5.211.0.0/16AS197207'

route:          5.211.0.0/16
descr:          New services for 4G
origin:         AS197207
mnt-by:         MCCI-MNT
created:        2015-02-18T11:49:18Z
last-modified:  2015-02-18T11:49:18Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.87.4 (BLAARKOP)
```



Prefix Overview (5.211.0.0-5.211.255.255)

This prefix is announced by

AS197207

"MCCI-AS , IR"

RIR	Status	Registration	Country
RIPE NCC	ALLOCATED	2012-09-04	IR

Showing results for 5.211.0.0/16 as of 2016-07-07 08:00:00 UTC

IP Address: 5.211.14.4

- Looks strange?
- Well, we can not disprove:
  - The IP address range might have been shared/let/lent
  - The operator might have misused public IPs privately
- The port seems to be down

Thank you for your Attention!

✉ hschmidt@ernw.de
bbutterly@ernw.de

@hendrks_
@BadgeWizard

www.ernw.de

www.insinuator.net