LTE is pretty fragile

Goals and Objectives

-*Quickly* demystify the mobile network and the Evolved Packet Core (EPC) elements just enough

-EPC network elements' fragility

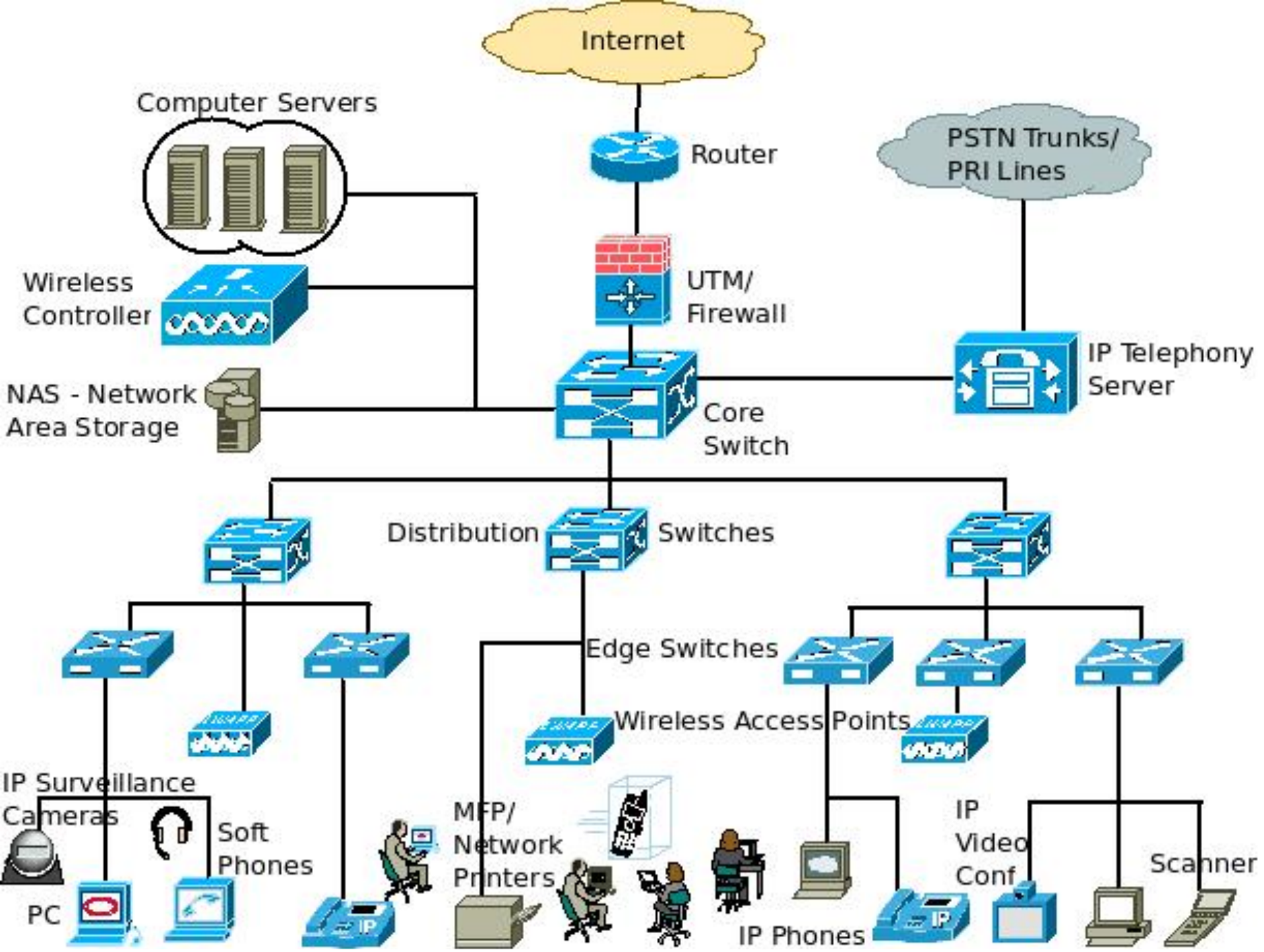
-Mobile security elements

Mobile Network vs. Generic Enterprise Network

A typical user's view of how the Internet works

INTERNET MAGIC!

How most people think the mobile network works


Internet
Computer Servers
Router
PSTN Trunks/
PRI Lines
Wireless
Controller
UTM/
Firewall
NAS - Network
Area Storage
Core
Switch
IP Telephony
Server
Distribution
Switches
Edge Switches
Wireless Access Points
IP Surveillance
Cameras
Soft
Phones
PC
MFP/
Network
Printers
IP Phones
IP
Video
Conf
Scanner

LTE Network Reference

PROTOCOLS and their SPECIFICATIONS		
Diameter	Diameter	RFC 3588, RFC 3589, RFC 4006, RFC 4740
EMM	EMM	EPS Mobility Management, 24.301, Section 5
ESM	ESM	EPS Session Management, 24.301, Section 6
GRE	GRE	Generic Routing Encapsulation, RFC 2784, RFC 2890
GTPv2-C	GTPv2-C	GPRS Tunneling Protocol ver. 2 Control Plane, 29.274
GTP-U	GTP-U	GPRS Tunneling Protocol User Plane, 29.281
IKEv2	IKEv2	Internet Key Exchange ver. 2, RFC 4306
IP	IP	Internet Protocol, RFC 791
MAC	MAC	Medium Access Control, 36.321
PDCP	PDCP	Packet Data Convergence Protocol, 36.323
PHY	PHY	Physical Layer for the Radio Link, 36.302
PMIPv6	PMIPv6	Proxy Mobile IP version 6, 23.402, 29.275
RLC	RLC	Radio Link Control, 36.322
RRC	RRC	Radio Resource Control, 36.331
RTP	RTP	Real-Time Protocol Transport Protocol, RFC 3550
S1AP	S1AP	S1 Application Part, 36.413
S101-AP	S101-AP	S101 Application Part, 29.276, 29.274
SCTP	SCTP	Streaming Control Transmission Protocol, RFC 3708
S1AP	SIP	Session Initiation Protocol, RFC 3261
TCP	TCP	Transmission Control Protocol, RFC 793
UDP	UDP	User Datagram Protocol, RFC 768
X2AP	X2AP	X2 Application Part, 36.423
not specified	Not Specified (proprietary)	

H-PLMN

V-PLMN

P-GW (PCEF)

H-PCRF

IMS

PSTN

P-CSCF

CPE

Internet

HSS

3GPP AAA server

3GPP AAA proxy

SPR

V-PCRF

MME

MME

Rel. 8 SGSN

UTRAN

RNC

S-GW

P-GW (PCEF)

ePDG

UE

OFDMA

LTE-Uu

SC-FDMA

eNB

eNB

X2

E-UTRAN

RNC

Trusted non-3GPP 1xEV-DO

HSGW

Untrusted non-3GPP (Wi-Fi)

Bearer 1

Bearer 2

Bearer 3

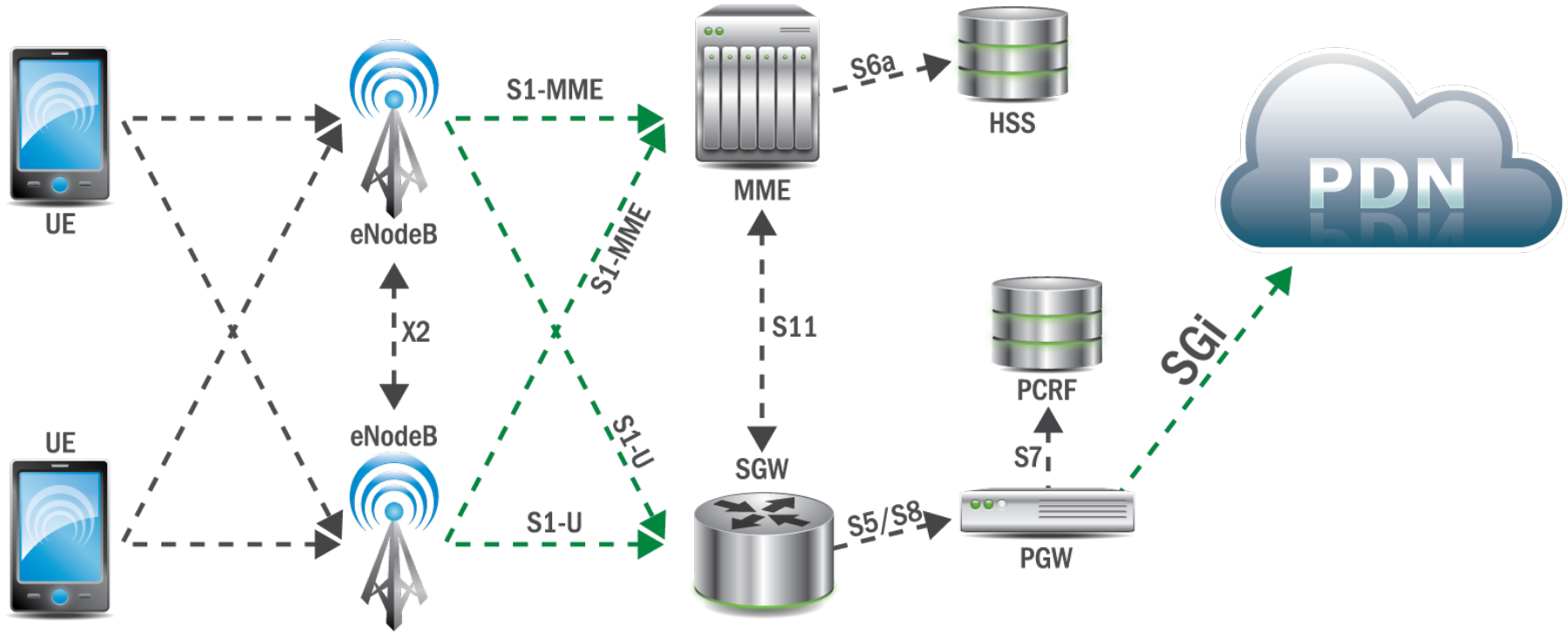
3GPP ACRONYMS and NODES	
3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
CPE	Customer Premise Equipment
eHRPD	Evolved High Rate Packet Data
eNB	Evolved Node B
eNodeB	Evolved Node B
ePDG	Evolved Packet Data Gateway
EV-DO RNC	Evolved Data Optimized RNC (eHRPD Access)
E-UTRAN	Evolved UTRAN
GERAN	GSM-EDGE Radio Access Network
H-PLMN	Home PLMN
HSGW	HRPD Serving Gateway
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
MME	Mobility Management Entity
NAS	Non-Access Stratum
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
P-GW	PDN Gateway
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RAT	Radio Access Technology
RNC	Radio Network Controller
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SPR	Subscription Profile Repository
UE	User Equipment
UTRAN	Universal Terrestrial Radio Access Network
V-PLMN	Visited PLMN

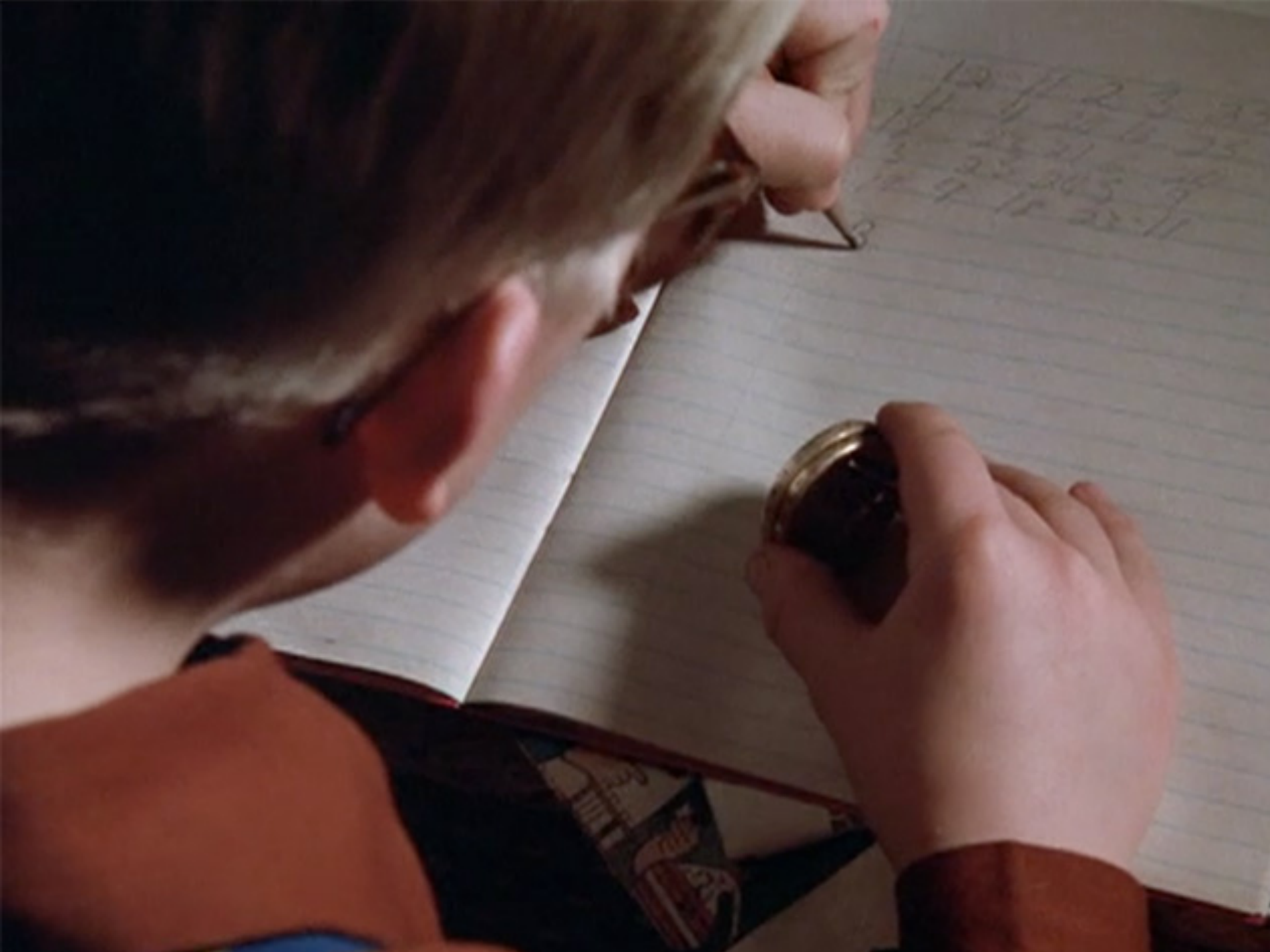
3GPP INTERFACES and TECHNICAL SPECIFICATIONS			
Interface	Nodes		Technical Specification
S1-MME	eNB	MME	36.413
S1-U	eNB	S-GW	36.414
S2a	HSGW	P-GW	23.402, 29.275
S2b	P-GW	ePDG	23.402, 29.275
S3	MME	Rel. 8 SGSN	29.274
S4	S-GW	Rel. 8 SGSN	29.274
S5/S8	S-GW	P-GW	29.274 (control plane)
			29.281 (user plane)
S6a	HSS	MME	29.272
S6b	3GPP AAA	P-GW	29.273
S9	PCRF	PCRF	29.215
S10	MME	MME	29.274
S11	MME	S-GW	29.274
S12	RNC	S-GW	29.281
S16	SGSN	SGSN	29.274
S101	MME	EV-DO RNC	29.276, 29.274
S103	S-GW	HSGW	29.276
X2	eNB	eNB	36.423 (control plane)
			36.424 (user plane)
LTE-Uu	UE	eNB	36.331 et. al.
Gx	PCRF	PCEF (P-GW)	29.212
Rx	AF	PCRF	29.214
SGi	P-GW	Internet	29.061
Sh	HSS	PCRF	29.328
Sp	PCRF	SPR	29.203
SWa	AAA	Untrusted Access	29.234
SWd	AAA	3GPP AAA	29.234
SWm	3GPP AAA	ePDG	29.234
SWn	ePDG	Untrusted Access	29.234
SWx	HSS	3GPP AAA	29.273

Interface LEGEND

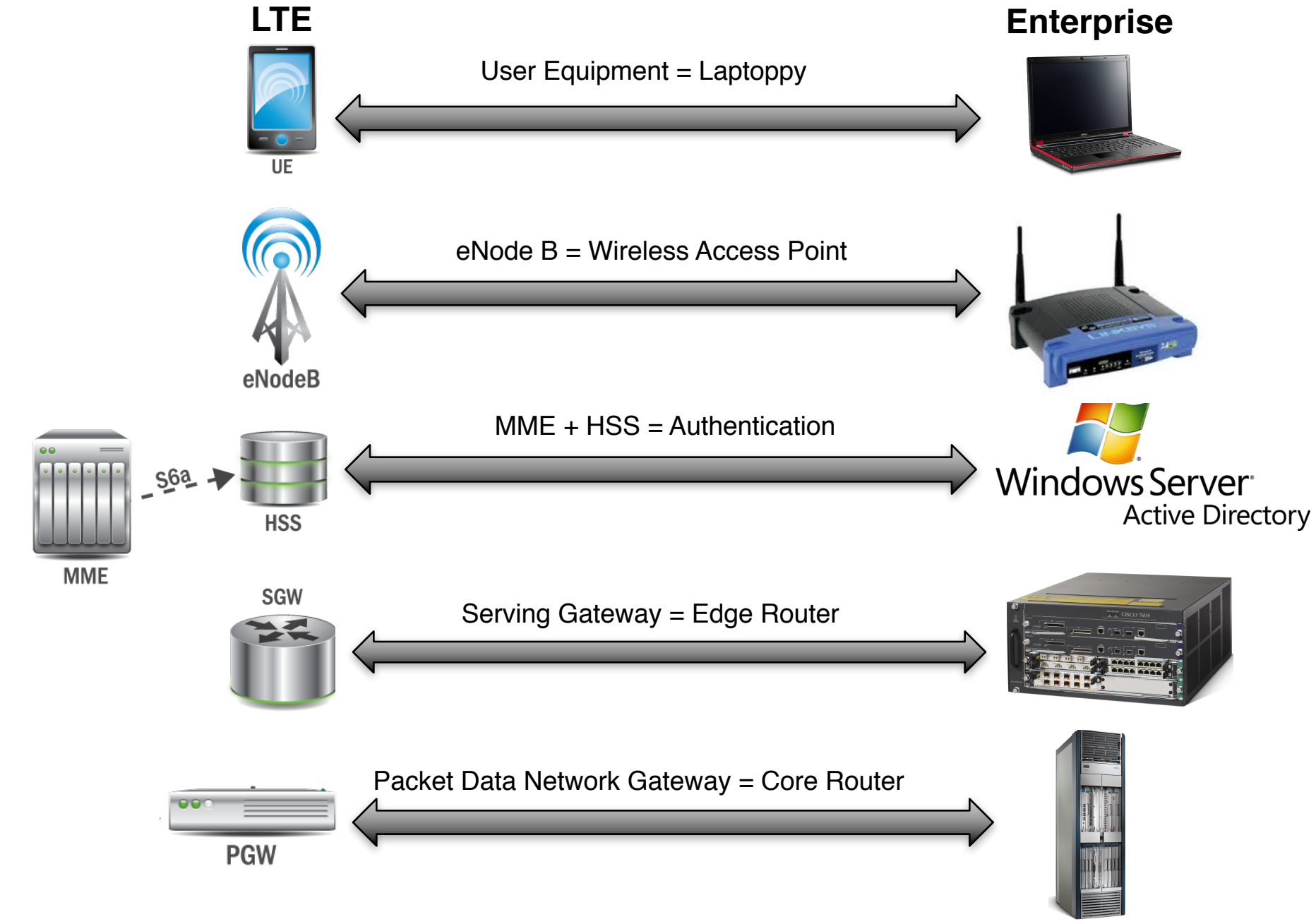
- Traffic
- Traffic and Signaling
- Signaling Only
- Service Control Plane
- Inter-RAT
- Radio
- NAS

The Mobile Network

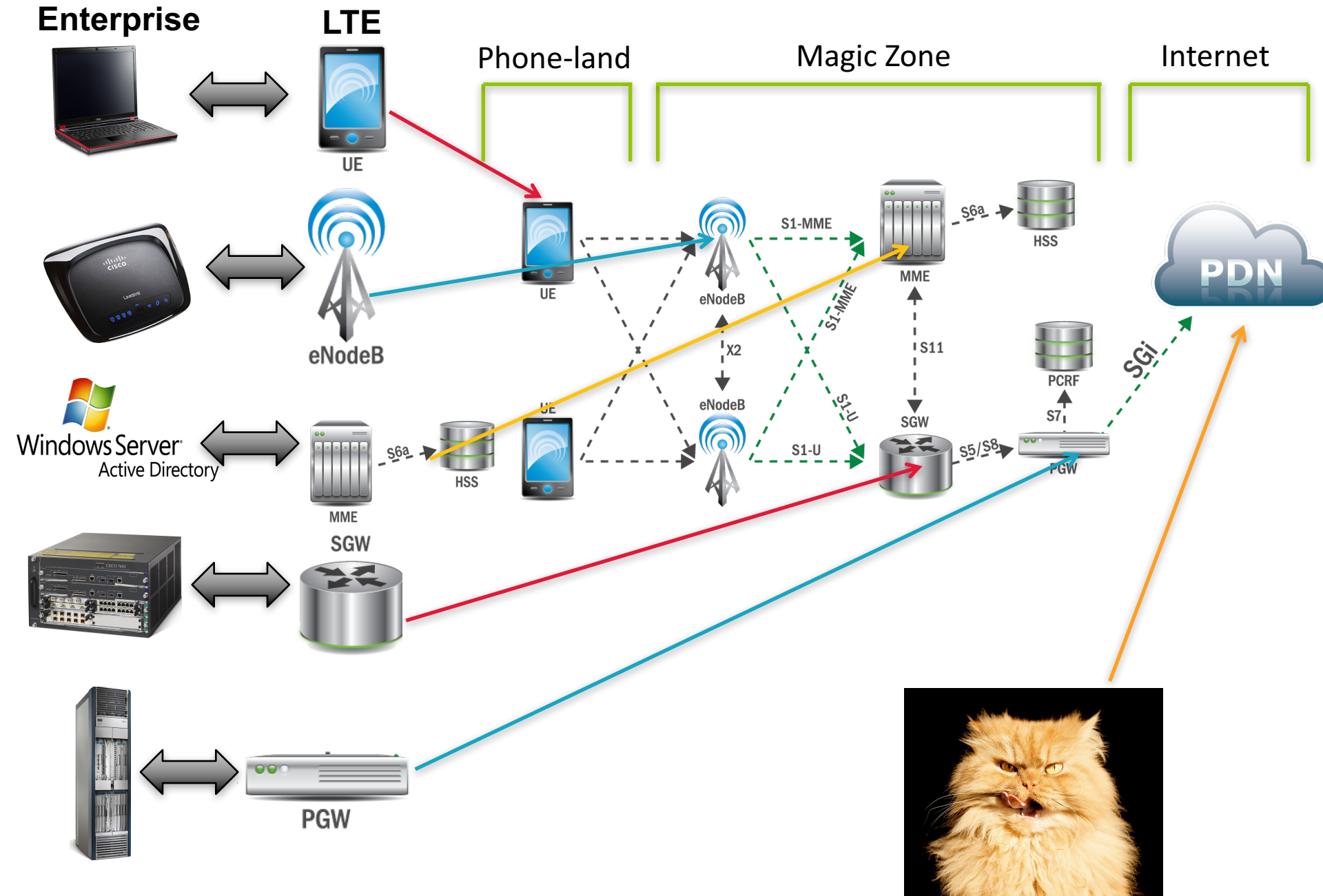




Decoder Ring: Long Term Evolution (LTE) to Enterprise



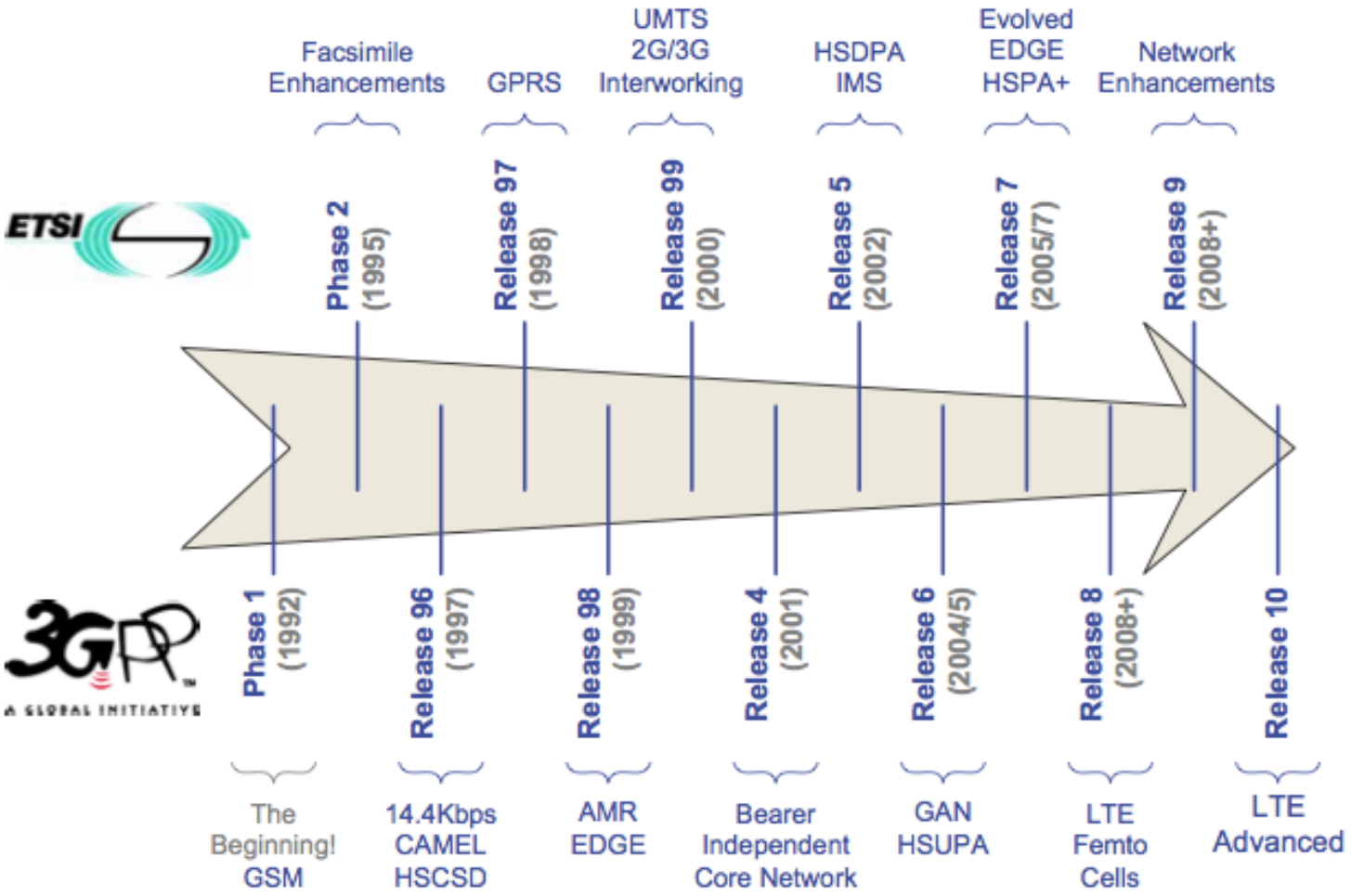
Decoder Ring: LTE to Enterprise



The State of LTE

LTE is Immature

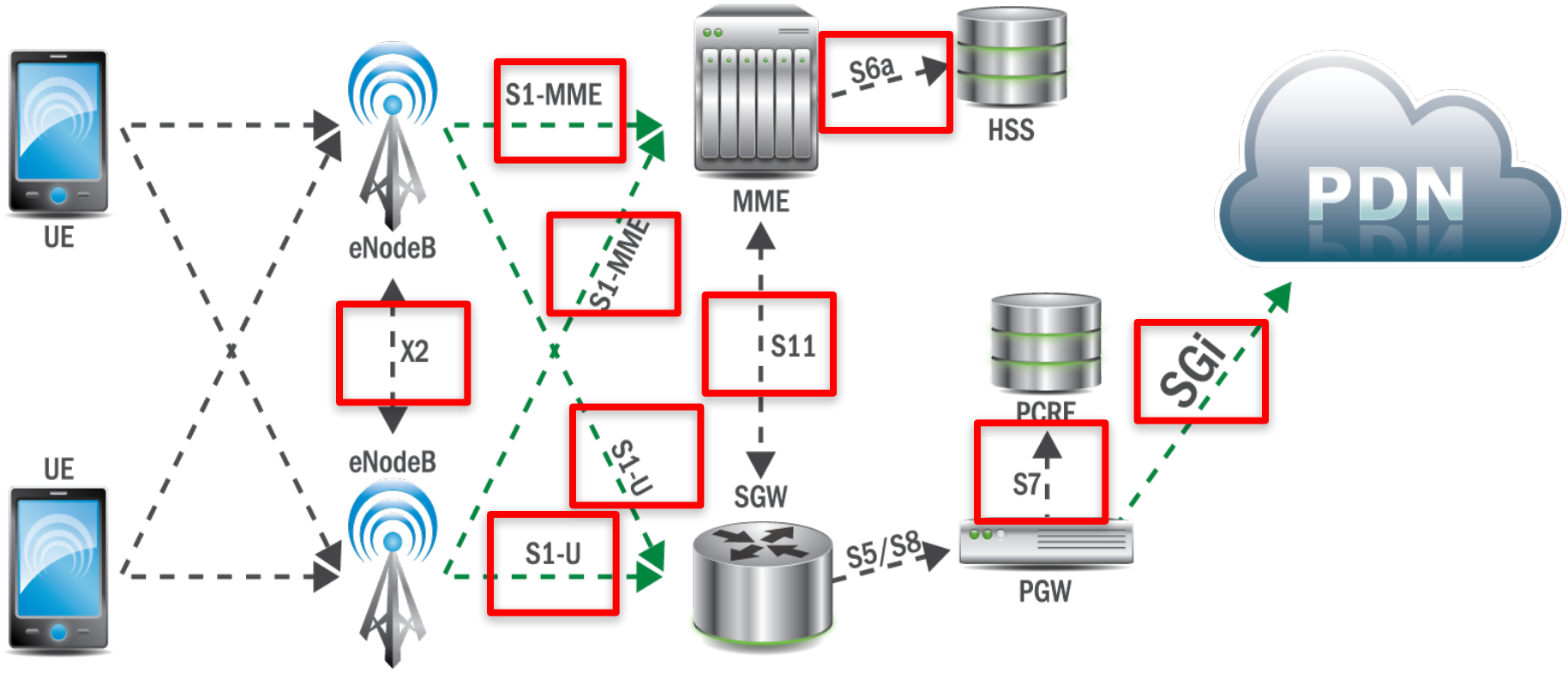
- 2G/3G have been around for 14+ years
- 4G (LTE, specifically) specifications have been “frozen” for 5 years, while the initial spec was proposed 9 years ago
- There will continue to be growing pains



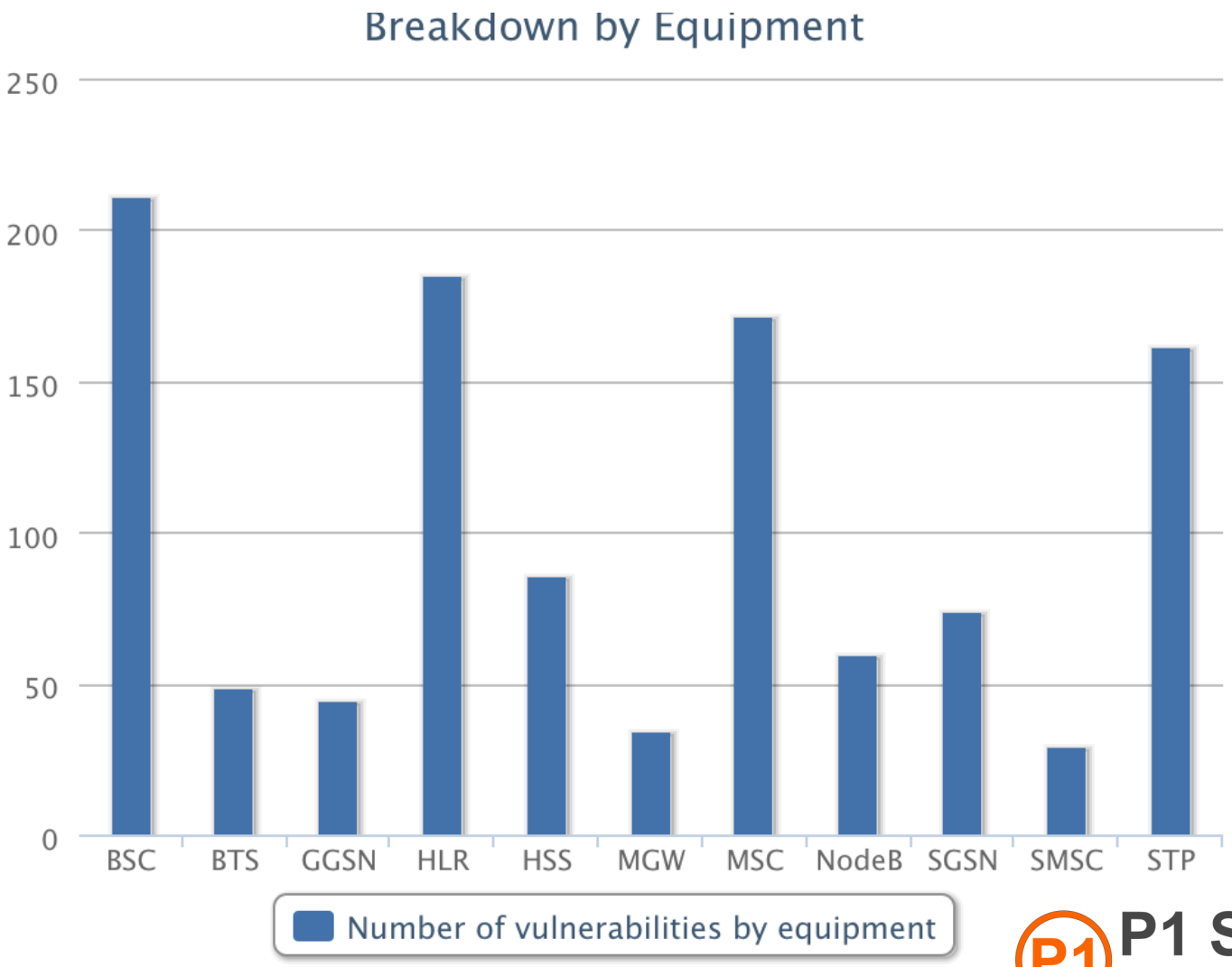
Limited Vendor Competition

Alcatel·Lucent

Large number of interfaces



LTE Network Equipment Vulnerabilities



P1 Security
Priority One Security

The Lack of Security Elements

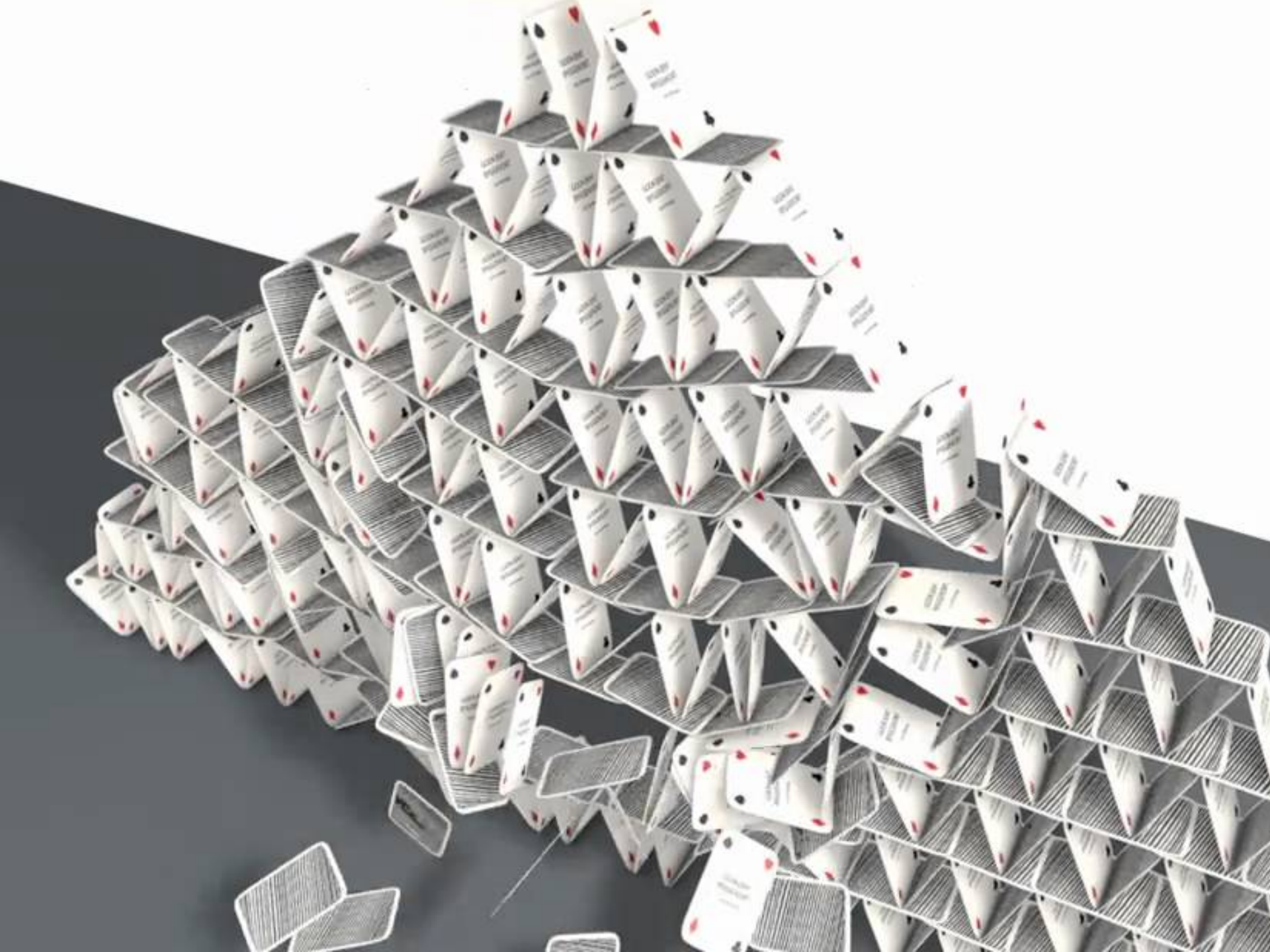
"It's a protected network (managed by others) that users cannot reach."

"Yes, but no one would ever do that."

"Why would you do that?"

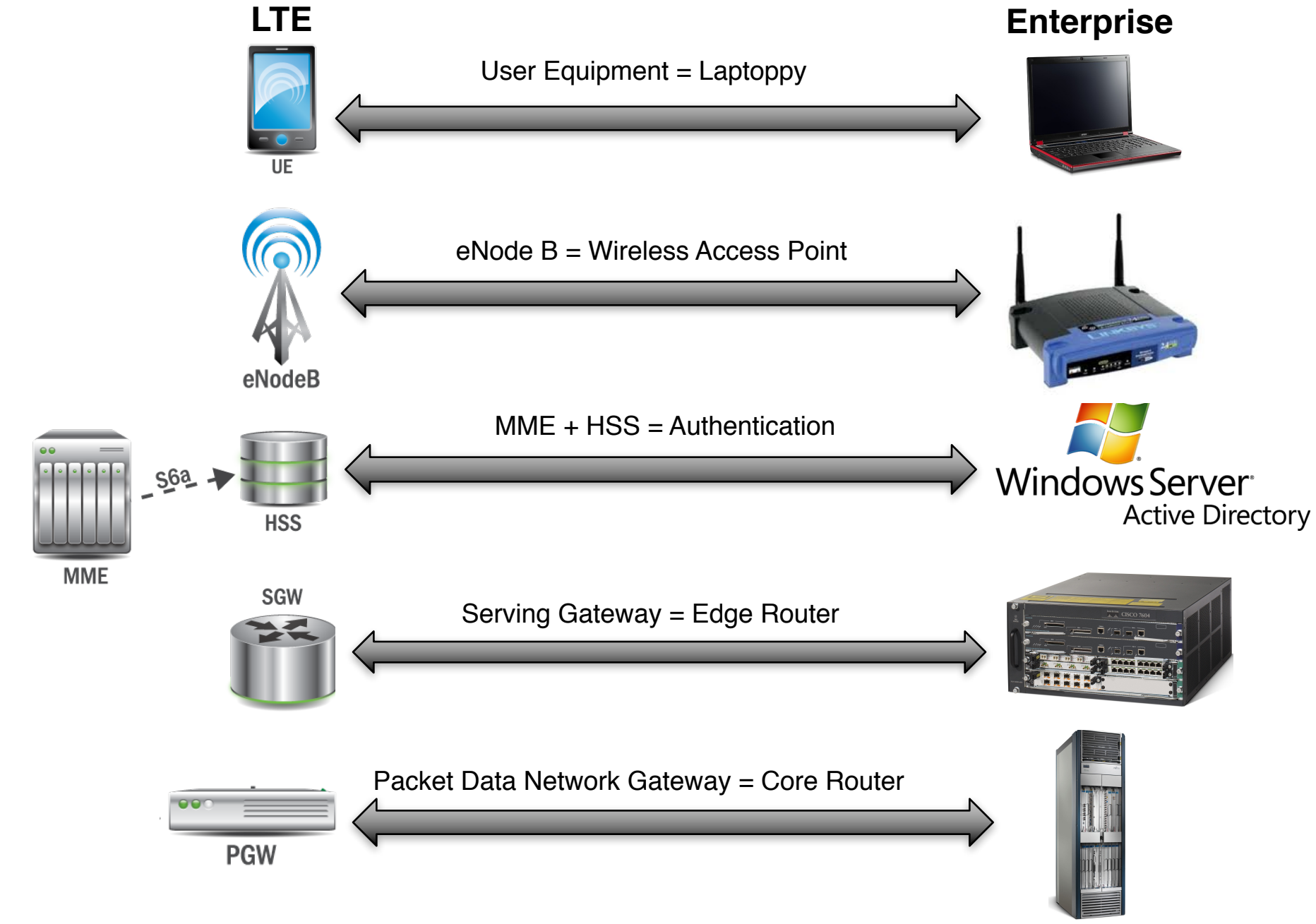
"The economics of consumer subscriber networks do not incent providers to implement security until a problem occurs."

-Arbor Network 2012 Security Report

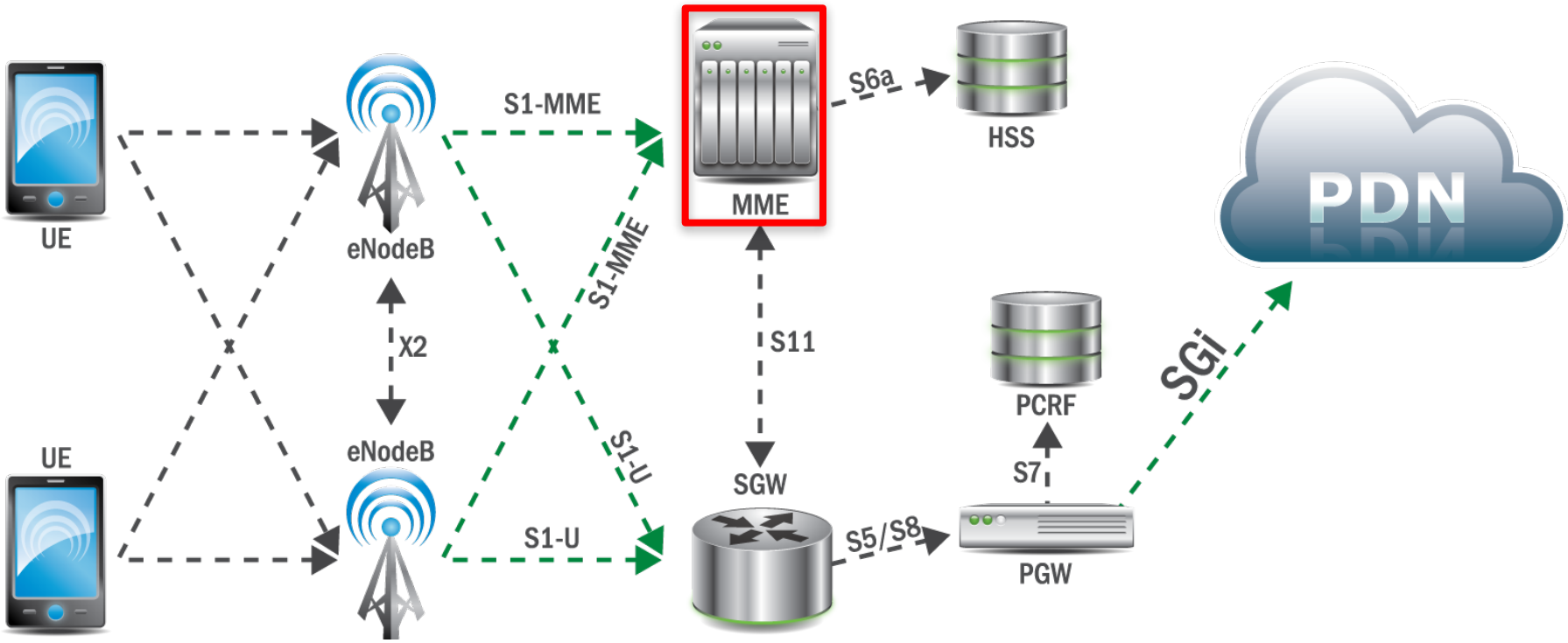


EPC Network Elements

Decoder Ring: Long Term Evolution (LTE) to Enterprise

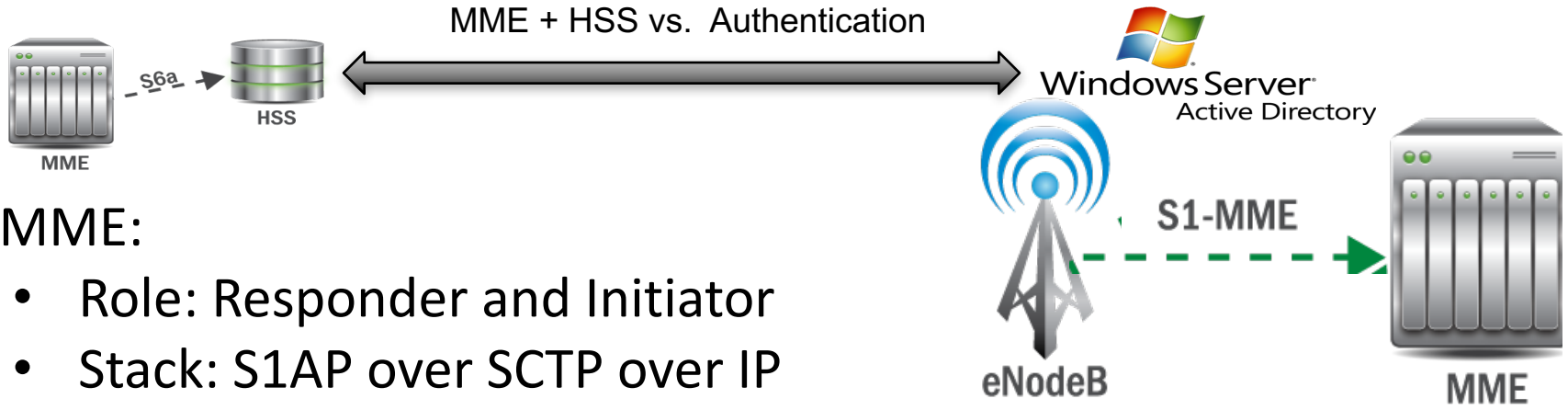


MME


UE
UE
eNodeB
eNodeB
X2
S1-MME
S1-MME
S1-U
S1-U
MME
S6a
HSS
S11
SGW
S5/S8
PGW
S7
PCRF
SGi
PDN


MME = Unicorn
You’re probably never going to see one.

MME: S1-MME Interface



S1-MME:

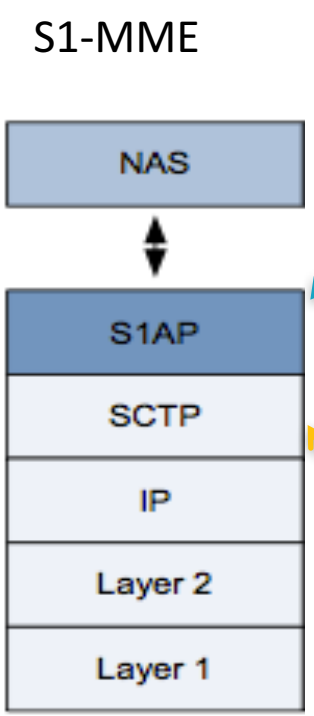
- Role: Responder and Initiator
- Stack: S1AP over SCTP over IP
- Usually uses IPSec (“Carrier Grade”)
- Used for control-plane communication between the eNodeB and the MME (AAA)
- Listens on SCTP port 36412 – set port scanners to stun

Generic Potential Vectors / Methods of Attack:

- Compromised eNodeB
- No safety mechanisms in place for DDoS mitigation
  - Can flood the MME with “UE Attach” messages
- No cryptographic authentication on S1AP
  - Any host can connect to an MME as long as ACLs allow it

MME: S1-MME Interface

Potential Vectors / Methods of Attack:



- S1AP is an open attack surface
  - Fuzz it—there are millions of fields available for fuzzing with random data
  - Send S1AP control plane registration messages out of order to "confuse" the state machine
  - Send S1AP control plane registration messages that do not include mandatory fields
  - Send multiple requests/responses for the same UE ID (IMEID) at the same time
  - Send requests/responses for a different IMEID after one was already established
- SCTP stack is not as well tested as TCP
  - Fuzz it
  - Create crazy scenarios with the stream ID
  - Send Fragments / Jumbo packets
    - 4/27/2013: MME reset bug related to fragmentation processing

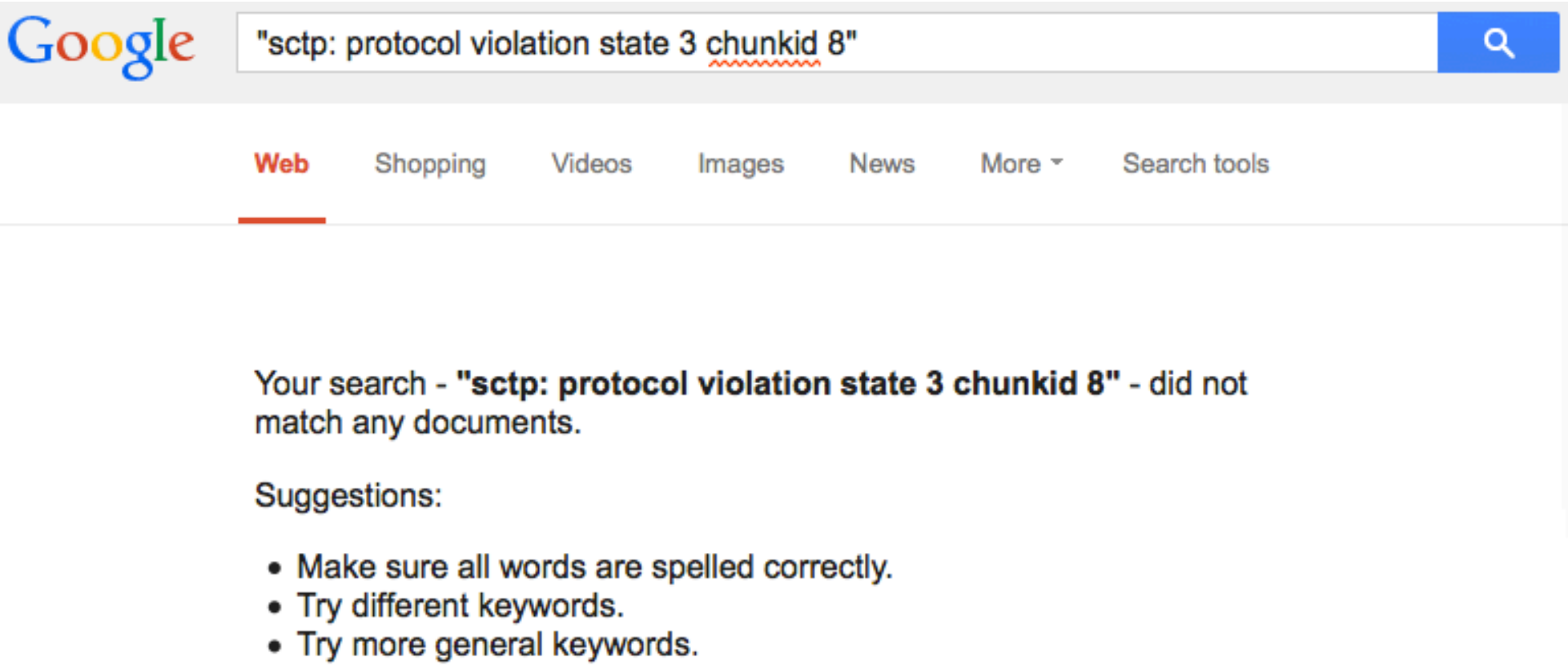
SCTP – A digression – RFC 4960

- SCTP was developed to support SIGTRAN/SS7
  - Long distance, IP-based transition, phone call system
  - Ties into PSTN (aka “the phone network”)
  - Developed by phone companies
- SCTP is a TCP “replacement”
  - Stream-based
  - Has “advanced features” to “protect” against attacks that affect TCP
  - According to wikipedia it has a “simpler, basic structure”
- However, run a quick fuzzer for a few seconds and get one of these:

```
[691801.142074] sctp: protocol violation state 3 chunkid 8
[691801.869213] sctp: protocol violation state 3 chunkid 8
[691803.079132] sctp: protocol violation state 3 chunkid 8
[691895.137059] sctp: protocol violation state 3 chunkid 8
[692036.171734] sctp: protocol violation state 3 chunkid 8
[692036.264610] sctp: protocol violation state 3 chunkid 8
```

```
nobletrout@freakazoid:~$ sctp_darn -H 192.168.5.100 -l -P 1338
sctp_darn: can not bind to 192.168.5.100:1338: Address already in use.
```

Google is no help



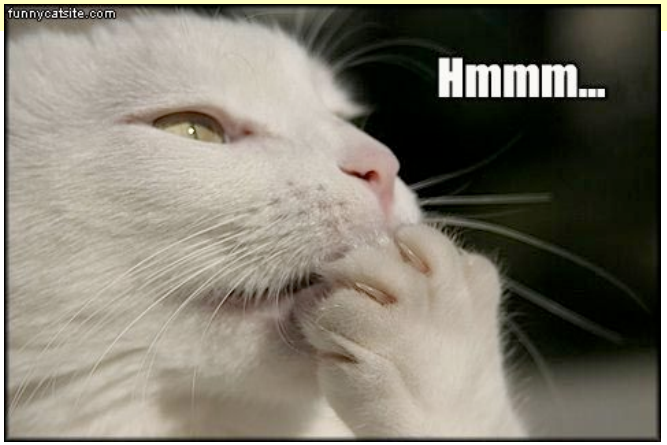
Even more SCTP digression

Also, go look at RFC 2960 (written back in 2000), which is a specification for SCTP. Section 3.3.5 is particularly revealing since it describes a part of the SCTP protocol that involves... you guessed it, heartbeats. And what does the SCTP heartbeat request look like? It's strangely familiar:

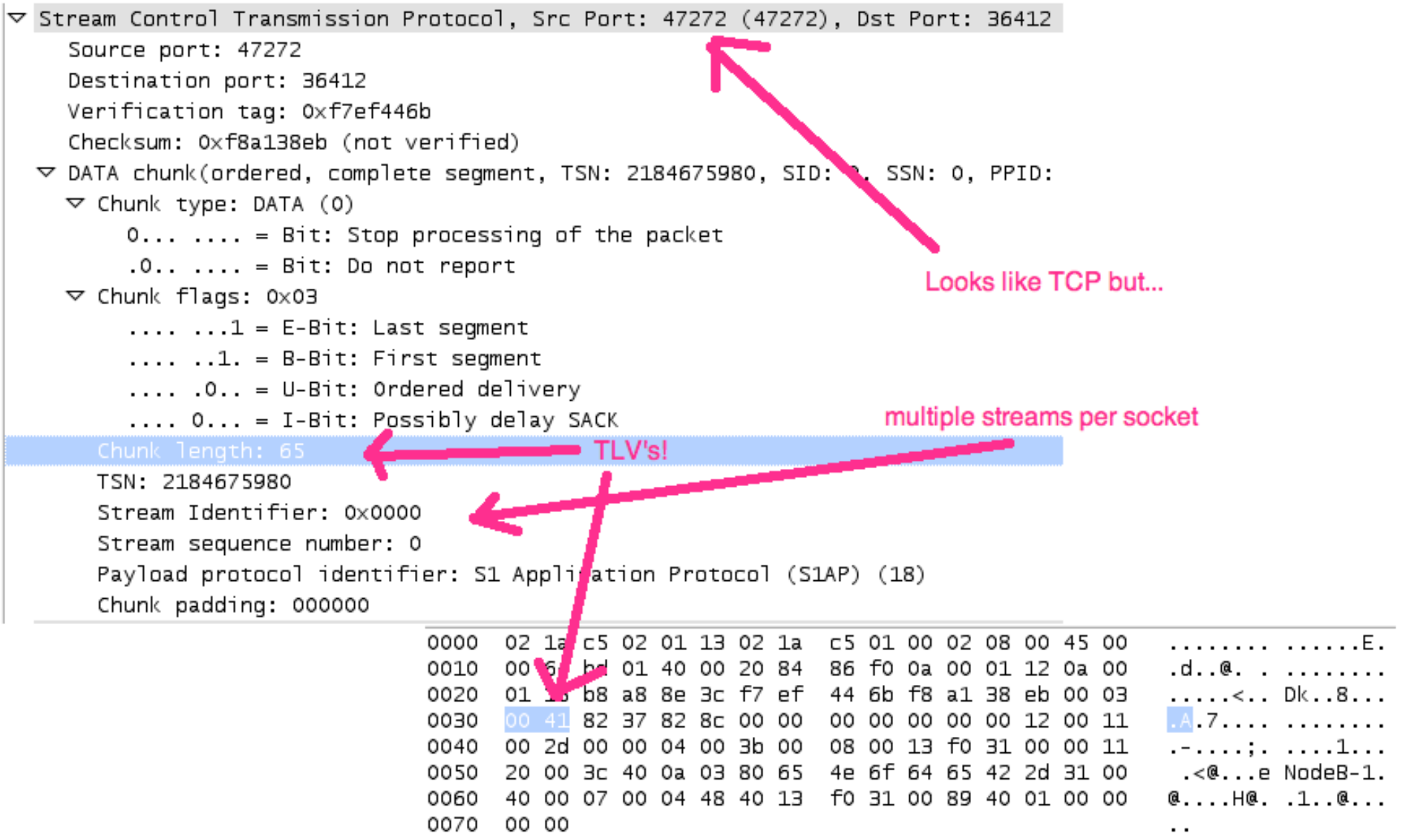
```
3.3.5 Heartbeat Request (HEARTBEAT) (4):

   An endpoint should send this chunk to its peer endpoint to probe the
   reachability of a particular destination transport address defined in
   the present association.

   The parameter field contains the Heartbeat Information which is a
   variable length opaque data structure understood only by the sender.

    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Type = 4    | Chunk  Flags  |      Heartbeat Length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /            Heartbeat Information TLV (Variable-Length)        /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Essentially, this all appears to have been done to support SCTP. That would certainly provide the motivation for doing this.

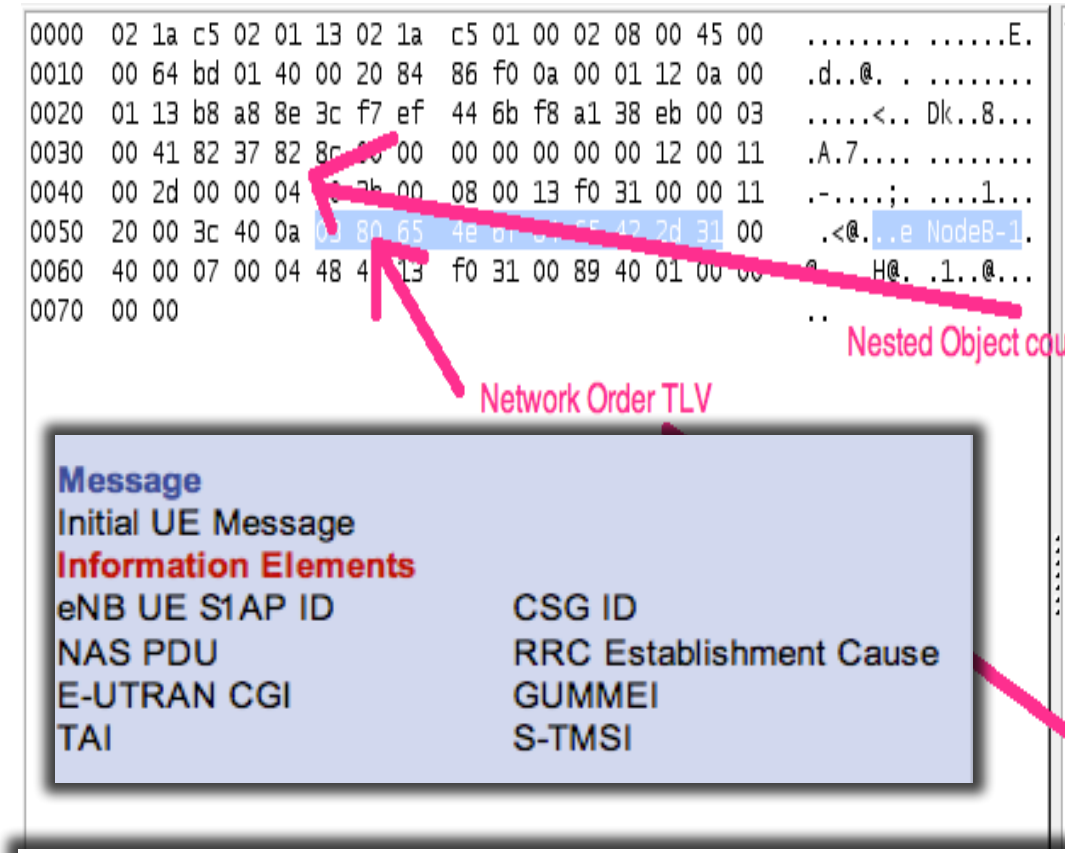
Robin Seggelman might've based heart beat code for SSL off of SCTP protocol/code
http://tinyurl.com/o5xdrot <--- goes to reddit

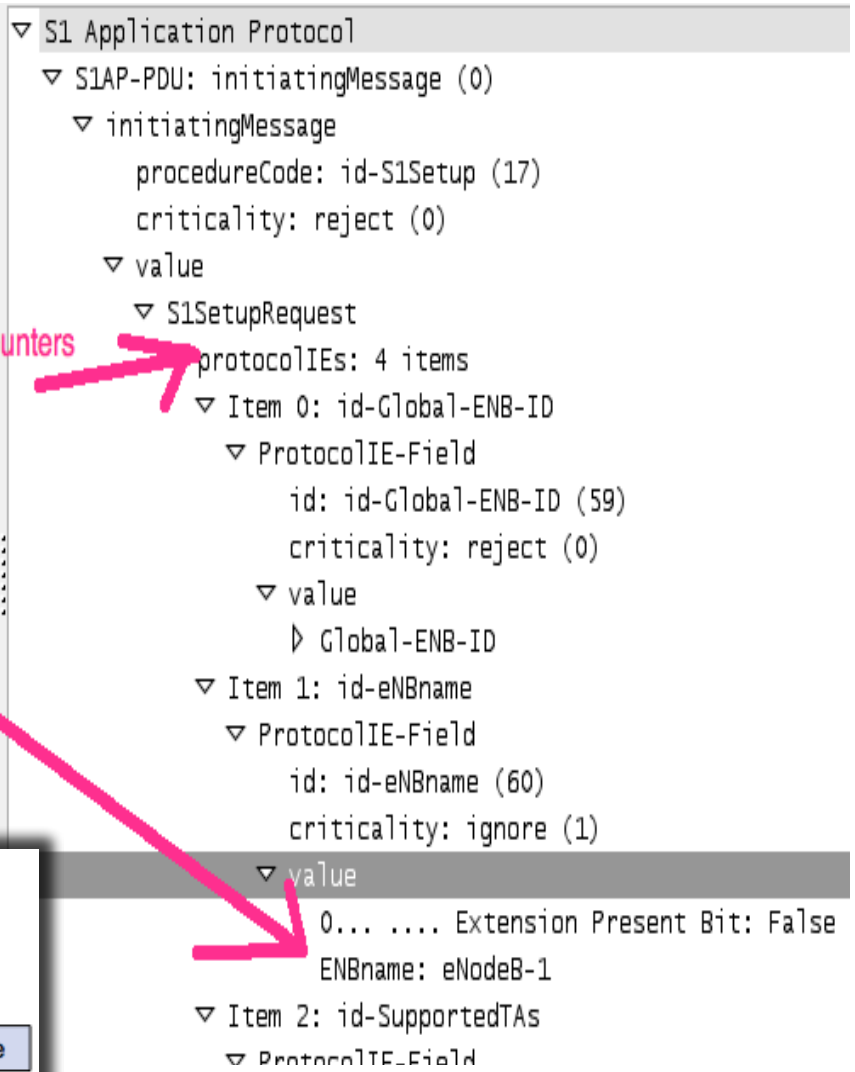


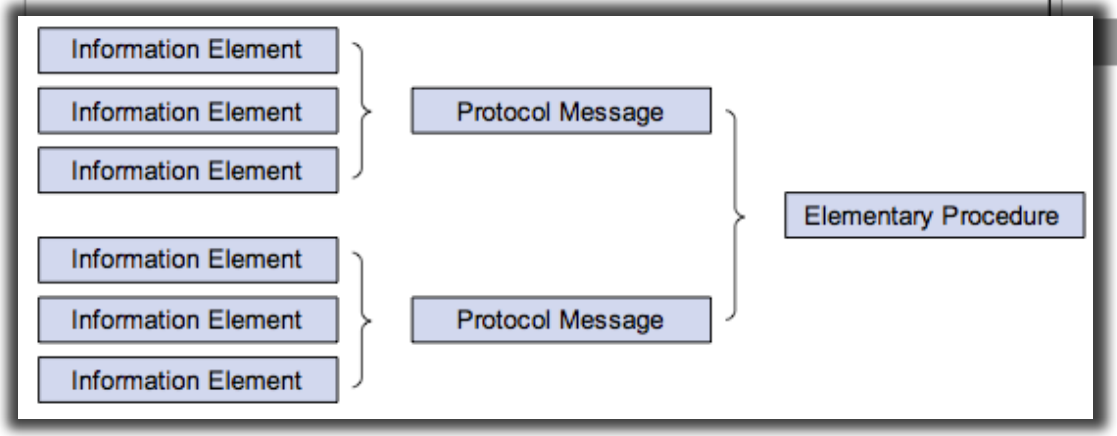
SCTP Points of interest



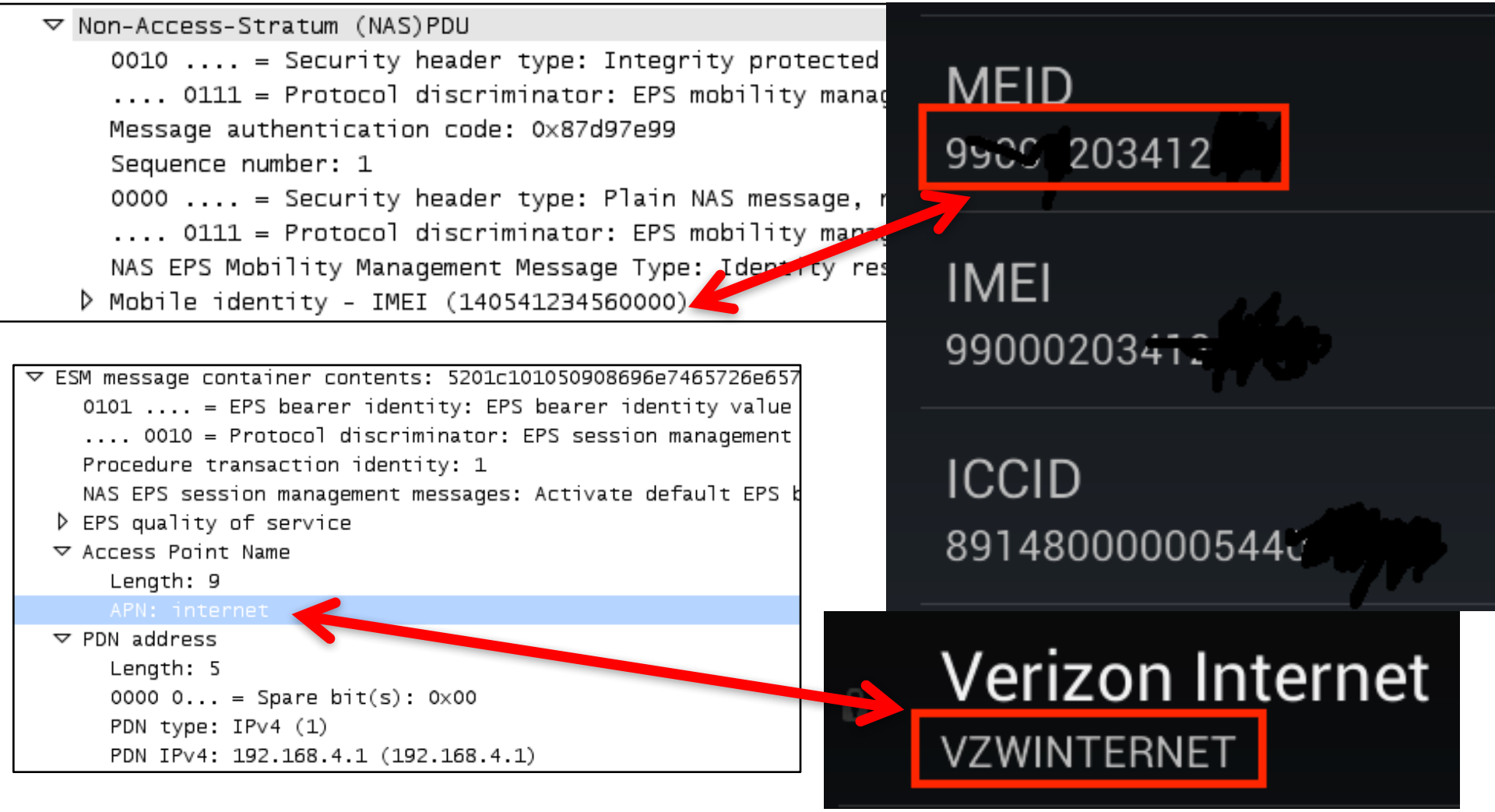
S1AP Points of Interest



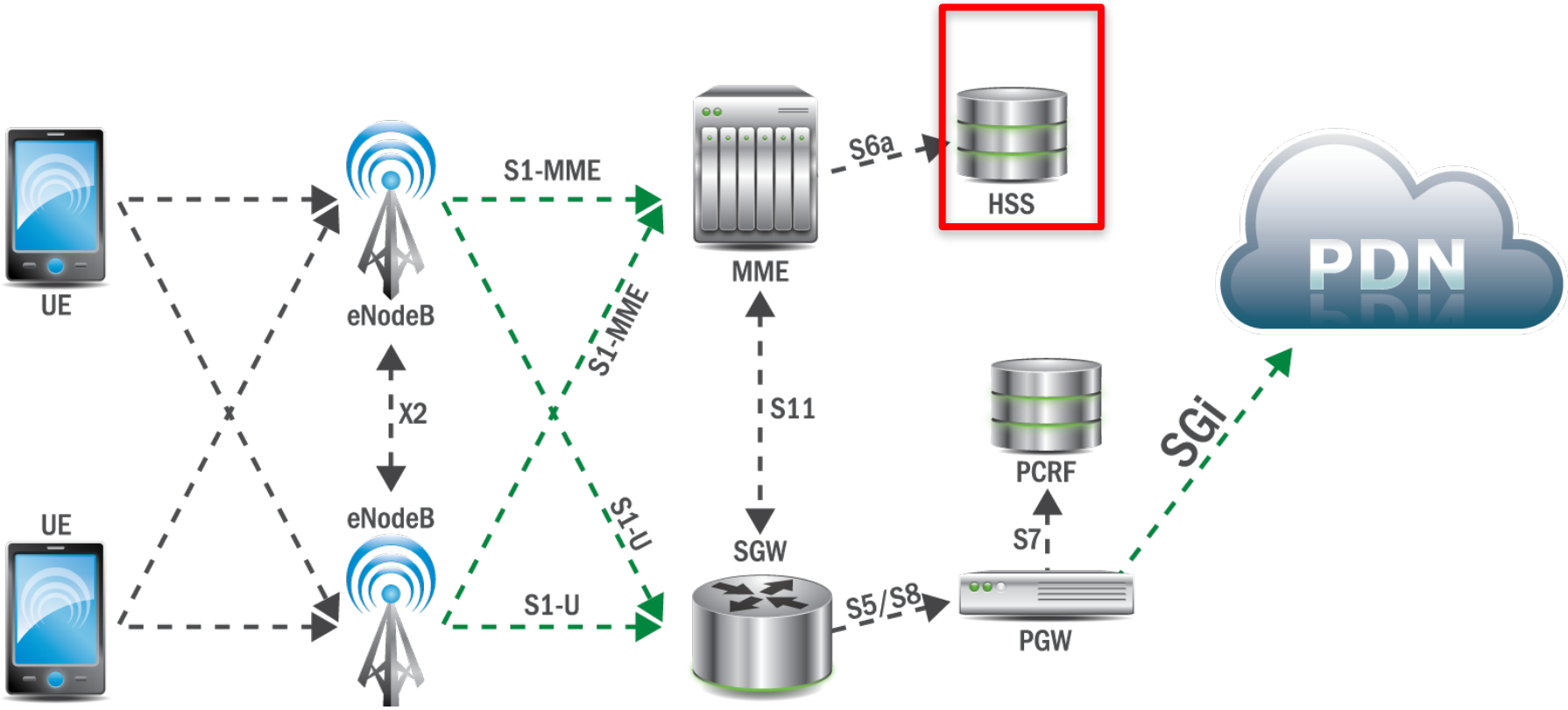




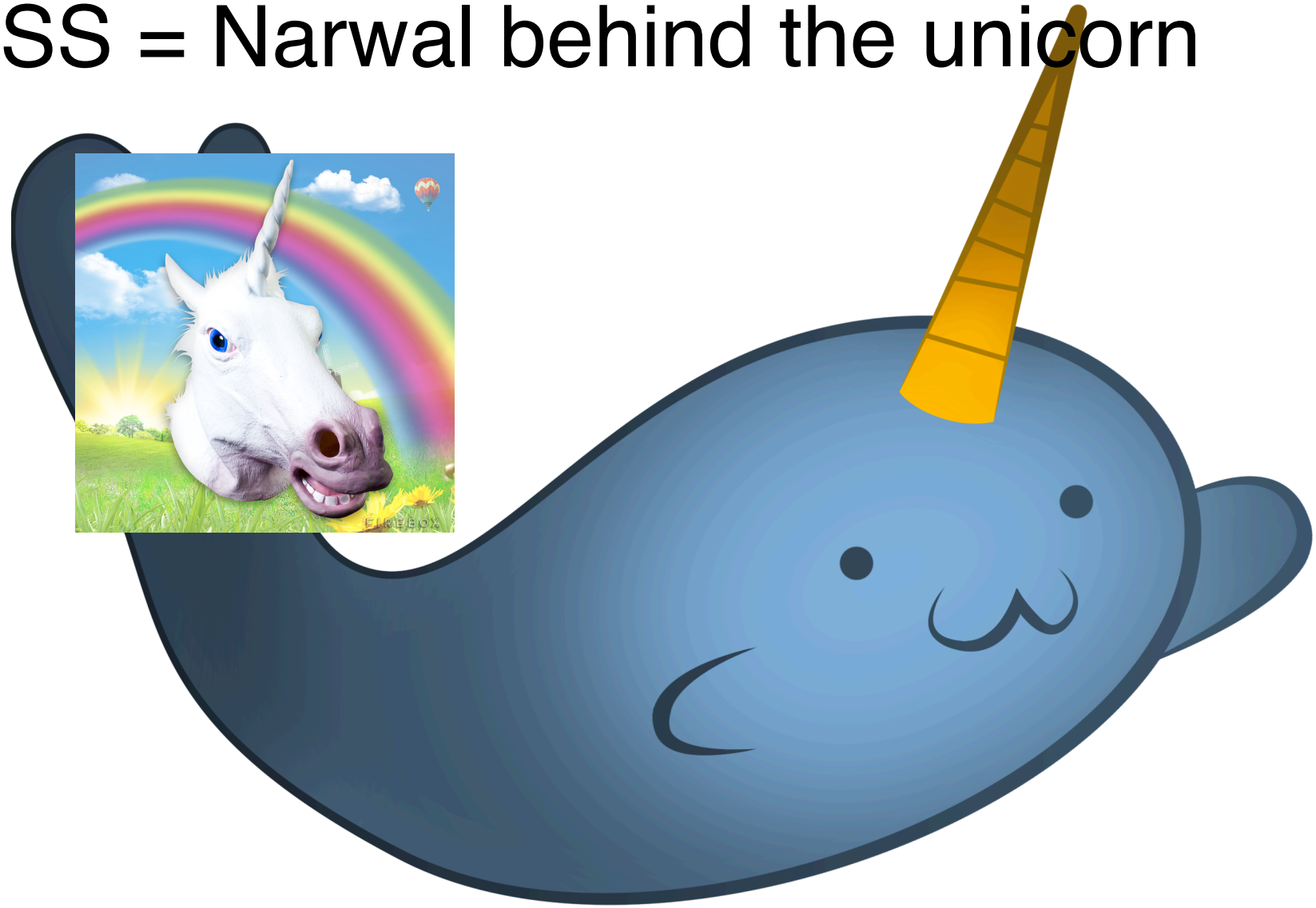
Mapping S1AP Messages to Phone Information



HSS


UE
UE
eNodeB
eNodeB
X2
S1-MME
S1-MME
S1-U
S1-U
MME
S6a
HSS
S11
SGW
S5/S8
PGW
S7
PCRF
SGi
PDN

HSS = Narwal behind the unicorn

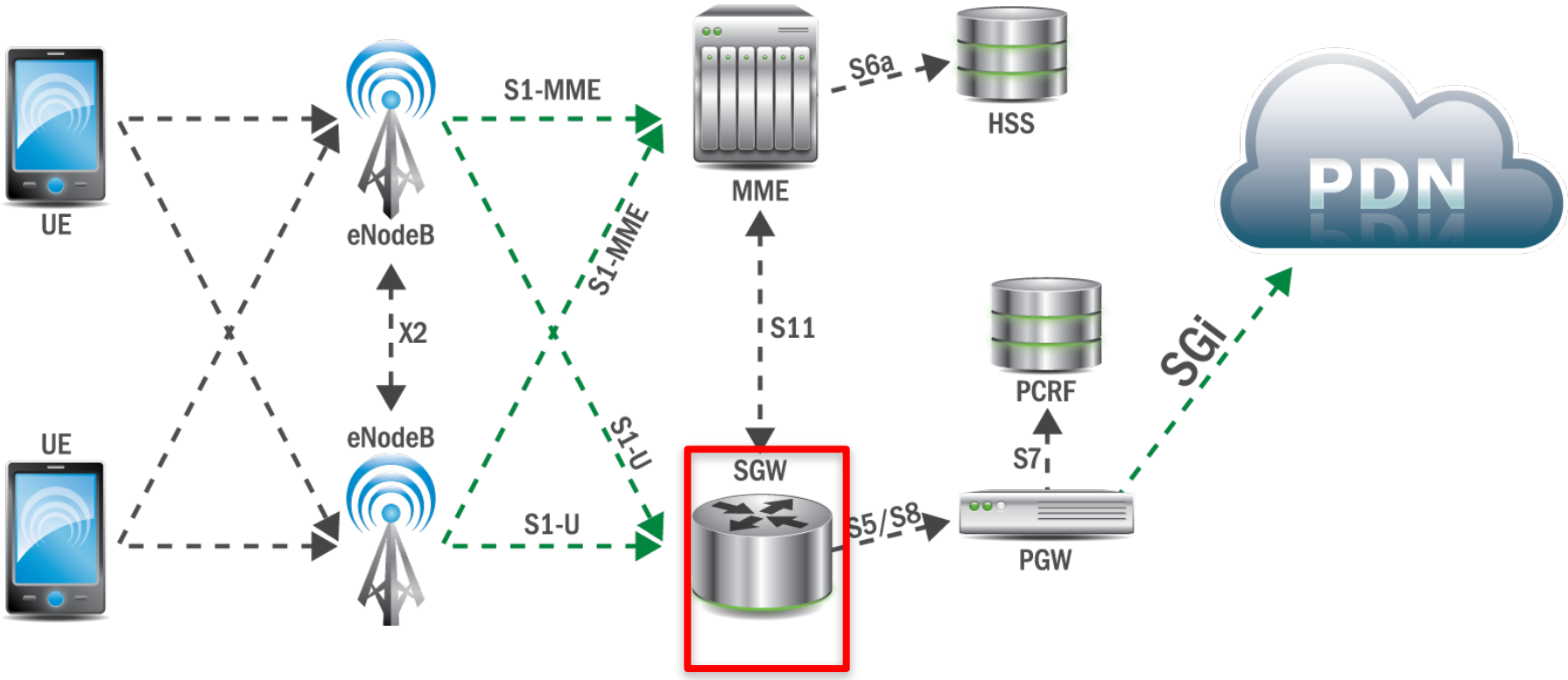


It exists, but you'll probably never get to see it either.

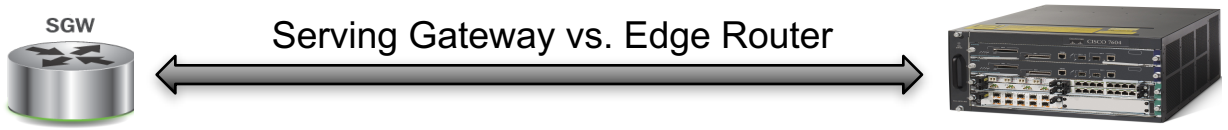
HSS

- Home Subscriber Server
- Diameter server
- SCTP port 3868
- Typically, an appliance-ized Linux or BSD box
- MME authenticates phone IMEID against HSS

SGW


UE
UE
eNodeB
eNodeB
X2
S1-MME
S1-MME
S1-U
S1-U
MME
S6a
HSS
S11
SGW
S5/S8
PGW
S7
PCRF
SGi
PDN

SGW: S11 Interface

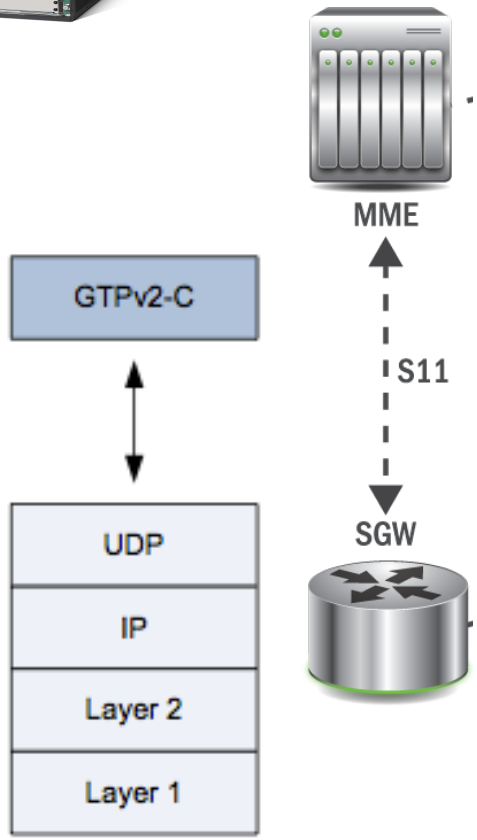


S11: GTPv2-C

- Role: Responder
- Used for bringing up GTP “Contexts”-- otherwise known as tunnels
- TLV-based protocol that runs over UDP
- UDP port 2123

Potential Attacks:

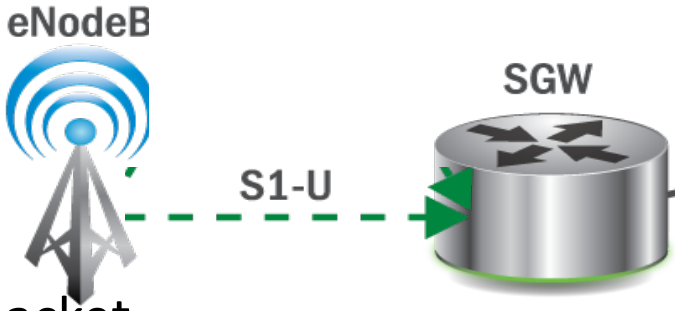
- Send random fuzzed traffic at GTP-C port—with or without the GTP headers. This has been successful and caused repeated reboots of SGWs



SGW: S1-U Interface

S1-U: GTPv1-U

- Role: Responder
- Tunnels IP packets inside of IP
- Similar function to VPN
- TLV fields followed by encapsulated IP packet
- Contains all of the users' data traffic



Potential Attacks:

- This is the easiest point of entry for an attacker as this is an IP address that the UE knows and uses
- Toll fraud, using wrong data channel for data
- Tunnel data traffic over DNS
- Sending malformed IP PDUs over GTP-U has caused many crashes on SGWs as it "unwraps" the packet
- DDoS or "performance test" with a standard application protocol mix

HTTP
TCP
IP
GTP-U
UDP port 2125
IP
Layer 2
Layer 1

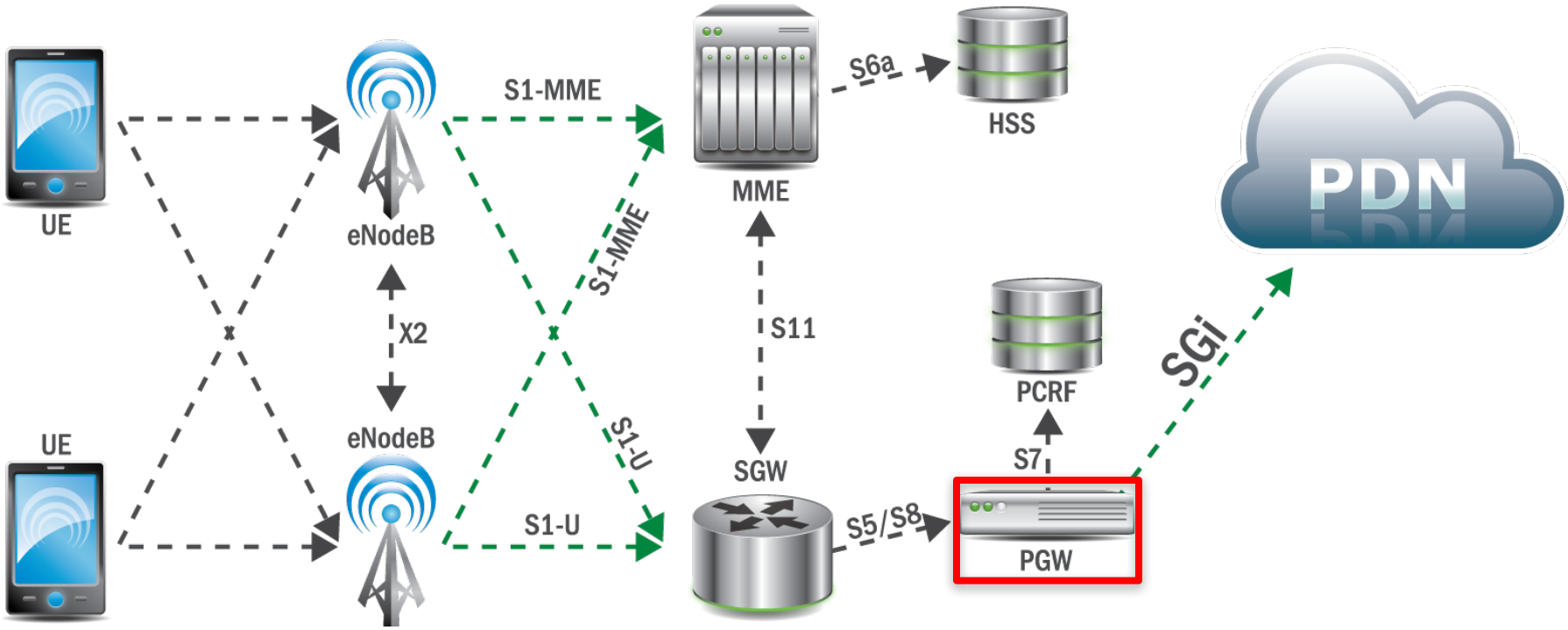
Case Study: Toll Fraud “Exploitation”

- LTE allows the use of “bearer” channels
- Designed to allow data limits for different applications
- The UE decides which bearer channel to send for each type of traffic
- Should be trivial to send different traffic over different bearer channel

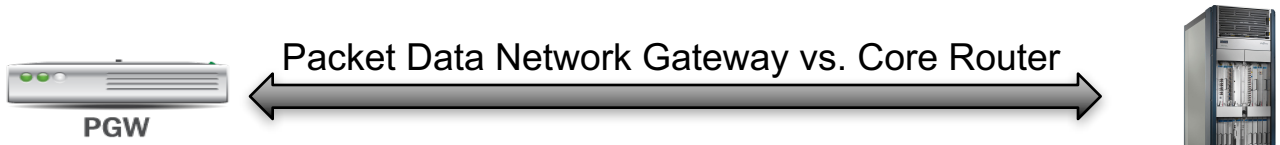
OR

- DNS-tunnel is allowed through most carriers networks
  - Set VPN to port 53
  - Free data
- ICMP-tunneling can also work

PGW

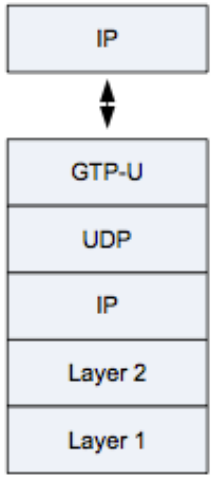

UE
UE
eNodeB
eNodeB
X2
S1-MME
S1-MME
S1-U
S1-U
MME
S11
SGW
S6a
HSS
PCRF
S7
S5/S8
PGW
SGi
PDN

PGW : S5/8 Interface



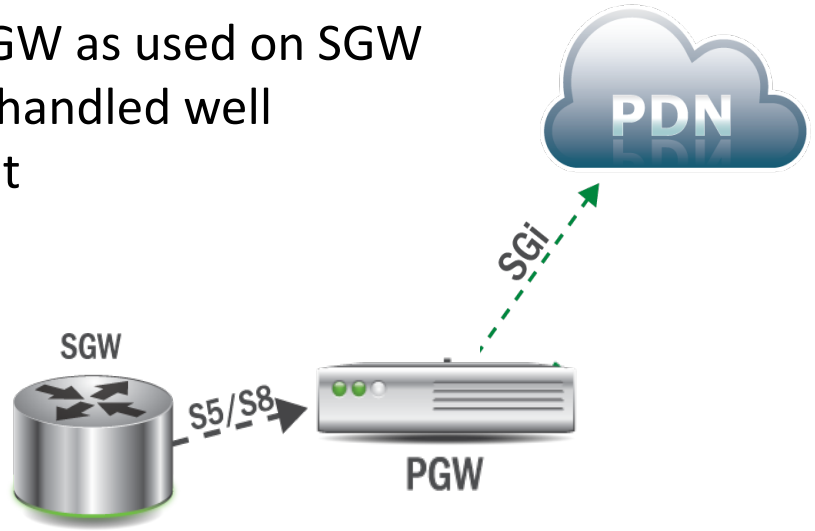
S5/8 Interface:

- PGW acts as “core router” for all traffic exiting the mobile network to the PDN
- Multiple SGWs are typically connected to one PGW
- In smaller environments the SGW and PGW are integrated into one unit
- PGW uses GTPv2-C and GTP-U, in a similar fashion to SGW
  - Packet headers are the same, but data changes

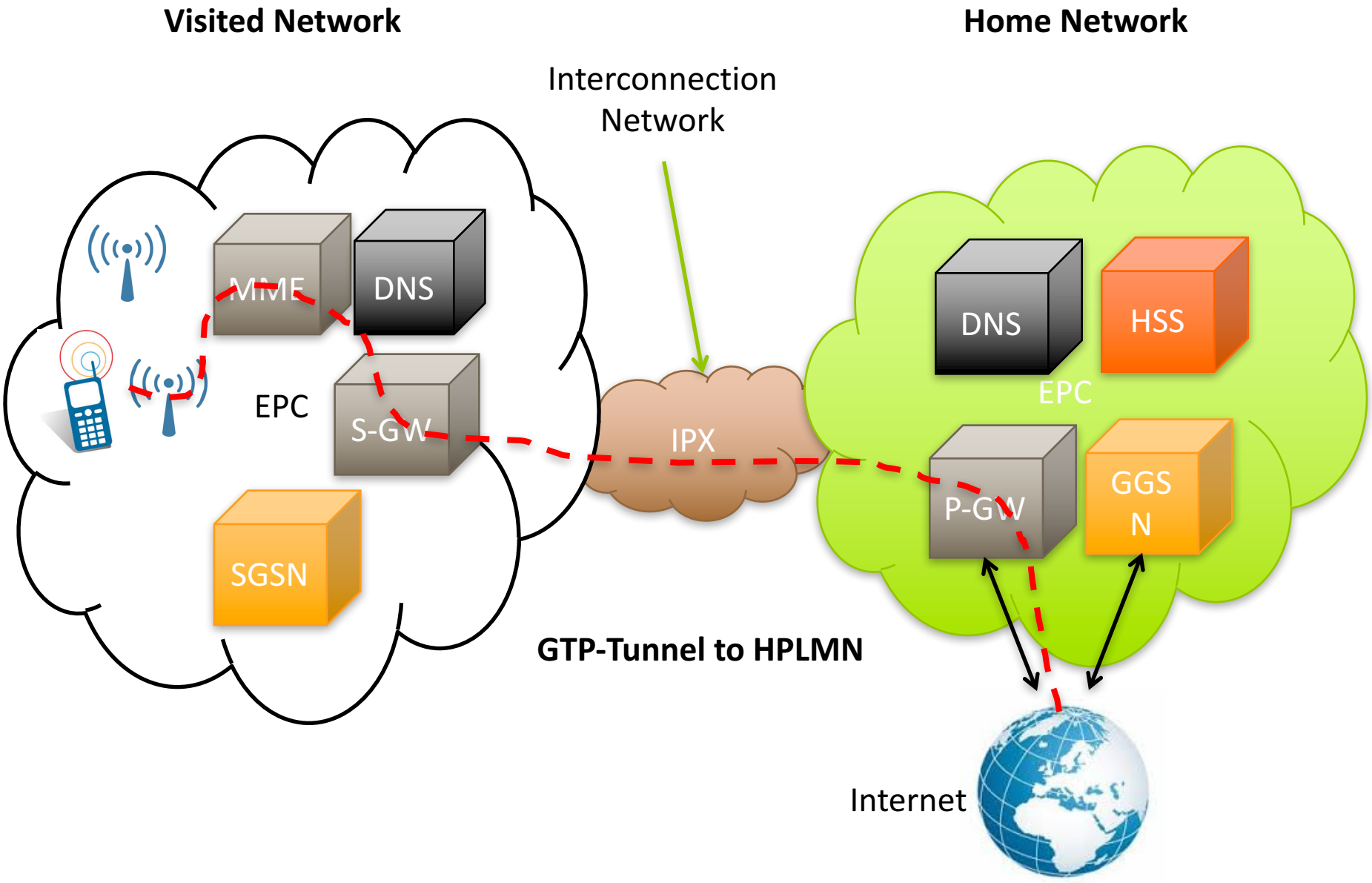


Potential Attacks:

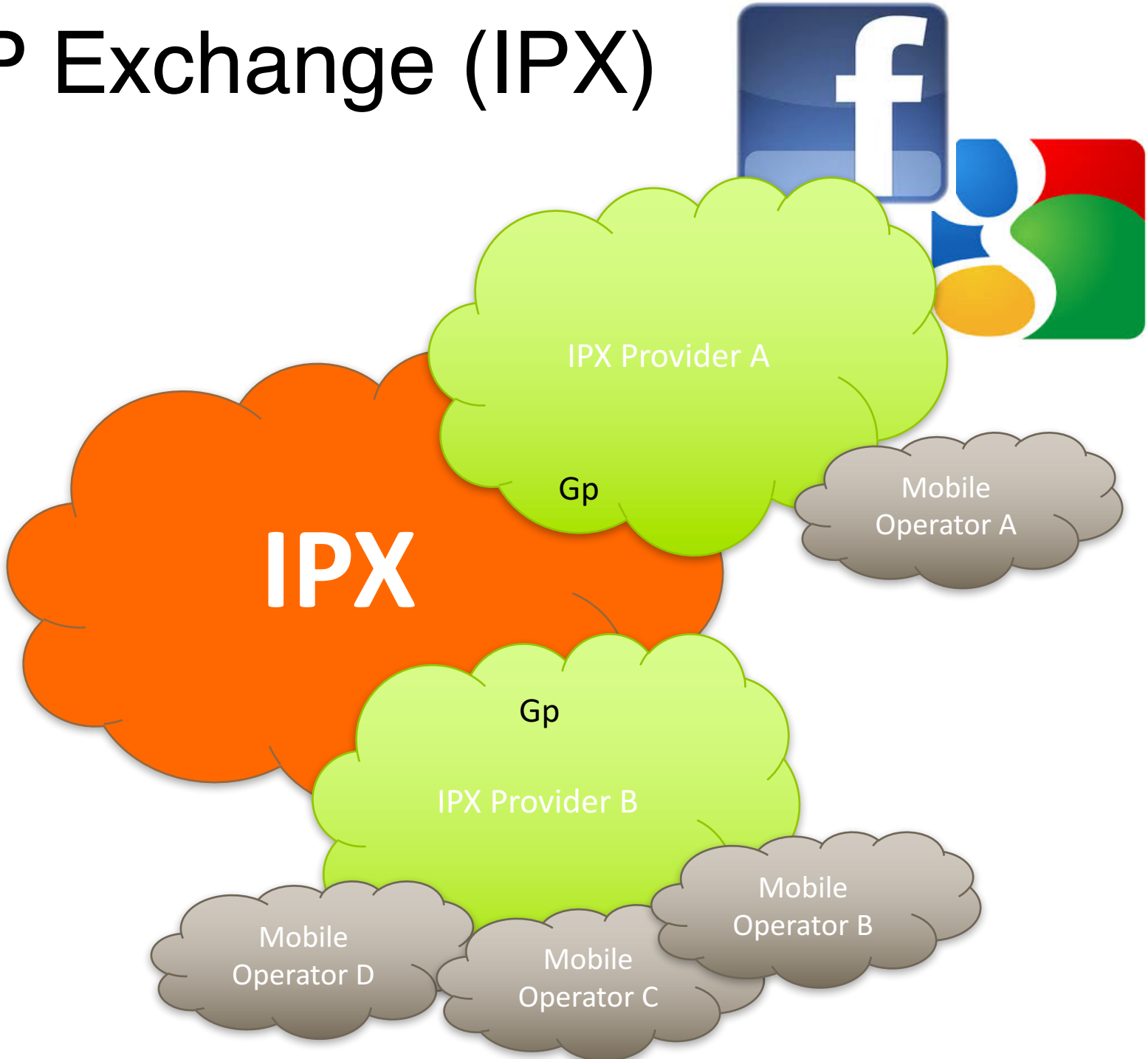
- Utilize the same techniques to break PGW as used on SGW
- Malformed IP packets are not typically handled well
- GTP-C flood to setup contexts that don’t



**Roaming?


Visited Network
Home Network
Interconnection Network
MME
DNS
EPC
S-GW
SGSN
IPX
DNS
HSS
EPC
P-GW
GGS N
GTP-Tunnel to HPLMN
Internet

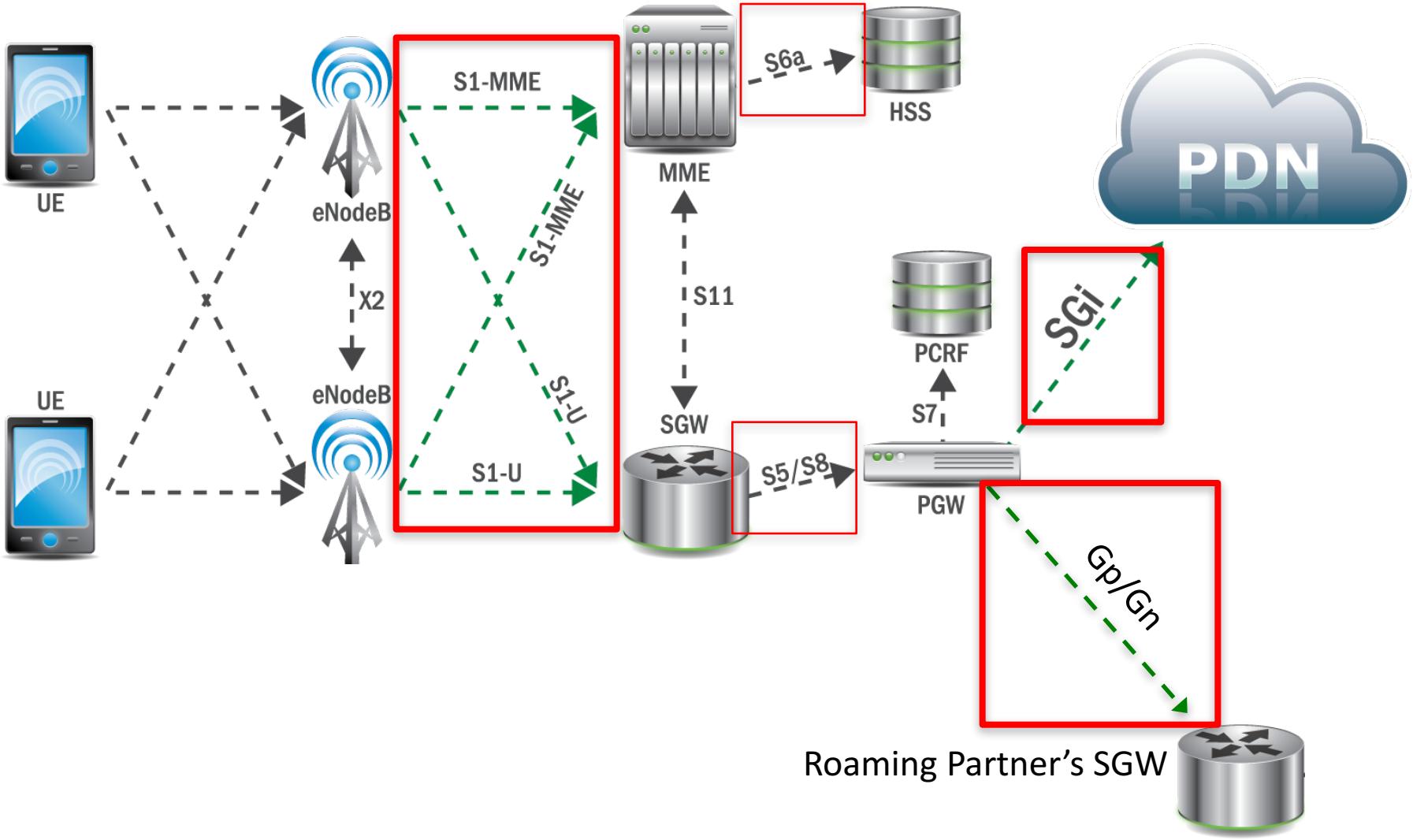
IP Exchange (IPX)



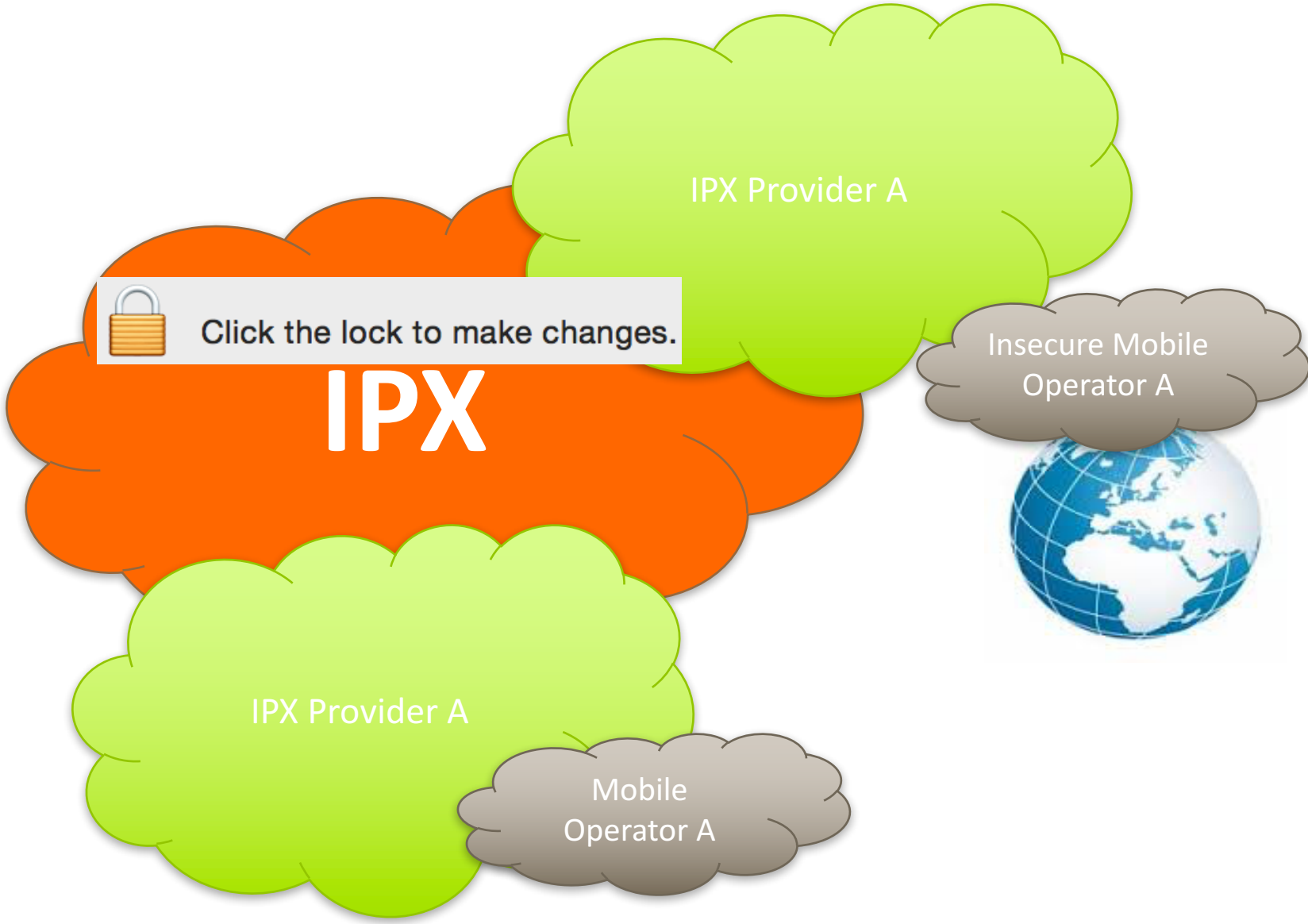
Security Elements

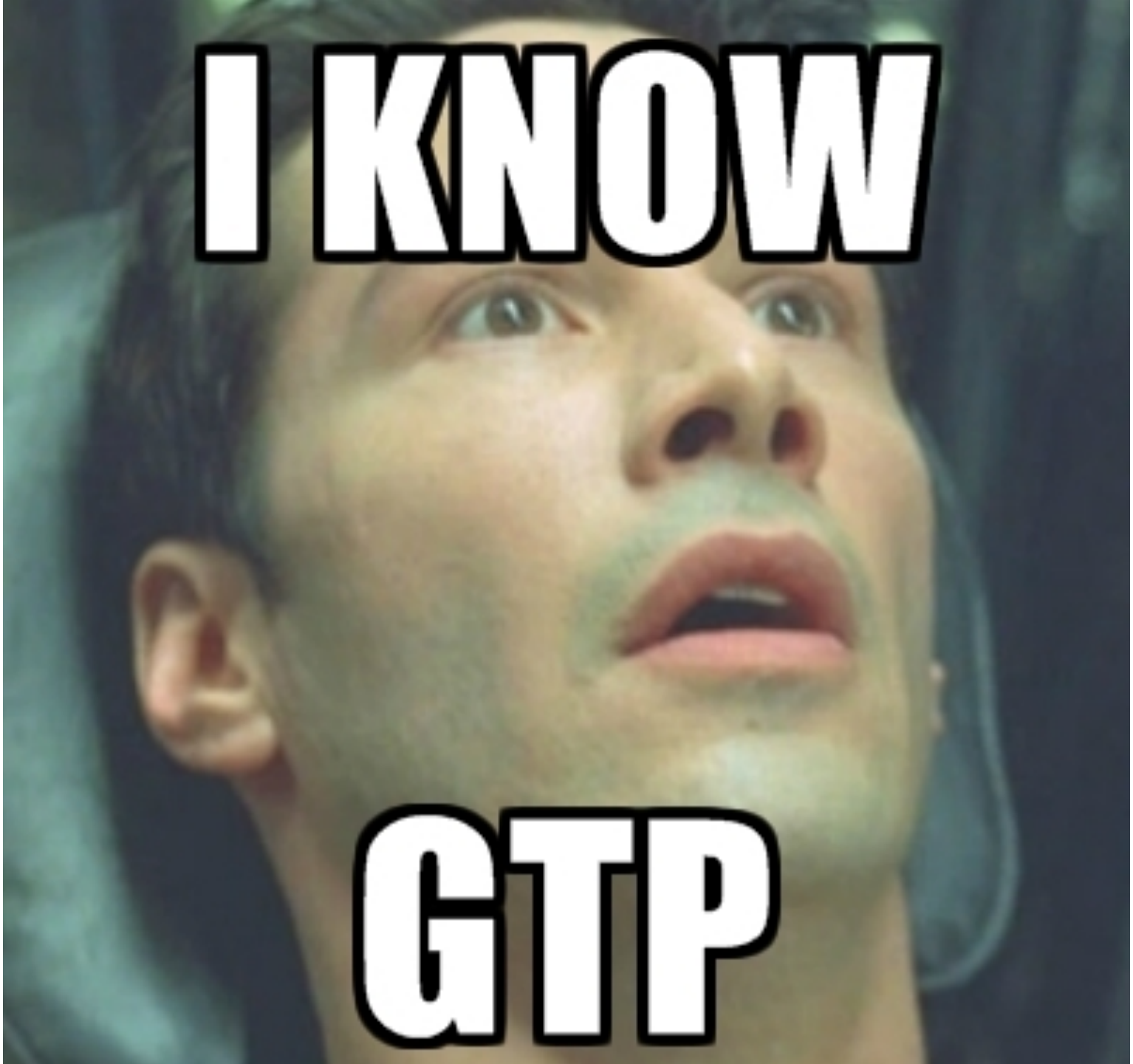
Some Dedicated Elements

Firewall Insertion Points



Is the IPX a protected network?




I KNOW
GTP

IPX Exposed Protocols

More (Internet standard) protocols usually means more tools….

OpenSource tools to poke cellular nodes available (e.g. **openss7, openggsn, metasploit**)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	149.254.	193.254.	GTPv2	301	Create Session Reque
2	0.350189290	193.254.	149.254.	GTPv2	193	Create Session Respo

```
Frame 1: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits)
Ethernet II, Src: Cisco_59:1e:80 (c8:f9:f9:59:1e:80), Dst: Cisco_e5:e0:c0 (00:1b:0d:e5:e0:c0)
802.1Q Virtual LAN, PRI: 3, CFI: 0, ID: 2360
Internet Protocol Version 4, Src: 149.254.[redacted] (149.254.[redacted]), Dst: 193.254.143.130 (193.254.[redacted])
User Datagram Protocol, Src Port: 12778 (12778), Dst Port: 2123 (2123)
GPRS Tunneling Protocol V2
Create Session Request
  Flags: 0x48
  Message Type: Create Session Request (32)
  Message Length: 247
  Tunnel Endpoint Identifier: 0
  Sequence Number: 2671872
  Spare: 0
  International Mobile Subscriber Identity (IMSI) : 26201[redacted]88
  MSISDN : 4915165[redacted]67
  Mobile Equipment Identity (MEI) : 3544[redacted]3801
  User Location Info (ULI) : TAI ECGI
  Serving Network : MCC 234 United Kingdom of Great Britain and Northern Ireland, MNC 30 Jersey Airtel
  RAT Type : EUTRAN (6)
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 SGW GTP-C interface, TEID/GRE Key: 0xc2fbd499, IPv4
  Access Point Name (APN) : internet.telekom.mnc001.mcc262.gprs
```

```
0020  c6 a0 c1 fe 8f 82 31 ea  08 4b 01 03 00 00 48 20   ......1. .K....H
0030  00 f7 00 00 00 00 28 c5  00 00 01 00 08 00 62 02   ......(. ......b.
0040  41 07 30 57 89 f8 4c 00  07 00 94 51 61 95 60 60   A.0W..L. ...Qa.``
0050  f7 4b 00 08 00 53 44 63  50 94 71 83 10 56 00 0d   .K...SDc P.q..V..
0060  00 18 32 f4 03 2c 89 32  f4 03 00 27 3f 00 53 00   ..2..,.2 ...'?.S.
```

Message Type (gtpv2.messa... | Pa... | Profile: Default

Protocol	Type	Port
BGP	TCP	179
DNS	UDP	53
GTPv0	UDP	3386
GTPv1-C	UDP	2023
GTPv2-C	UDP	2023
GTPv1-U	UDP	2052
SMTP/MMS-IW	TCP	23
Diameter	SCTP	3868
Sigtran (IP)	SCTP	

EPC Element Kills

SGW:

S1-U Interface:

1. Fragmented IP traffic —> GTP-U manager crash
2. High rate of 64B TCP —> GTP-U manager crash
3. Fuzz GTP-U (<20Mbps) + application traffic ->GTP-U manager crash

S11 Interface:

1. Malformed “Idle Control” Command Message + application traffic -> GTP-U manager crash
2. Fuzz just TCP/IP headers, not even the GTP-C + application traffic ->NPU-manager crash
3. Fuzz GTP-C traffic -> GTP-U manager crash

MME:

S1-MME interface:

1. DDoS with attach request floods, SCTP connection flood and other general mayhem on S1AP

DRA:

S6a Interface:

1. 1x SCTP connection, simulating 1x MME, 4000 messages/s (authentications, then location updates) -> Crash

HSS:

S6a Interface:

1. X000 messages/s -> Crash

Questions / Arguments ?