P1 Security
Priority One Security

Attacking GRX

Attacking The GPRS Roaming eXchange (GRX)

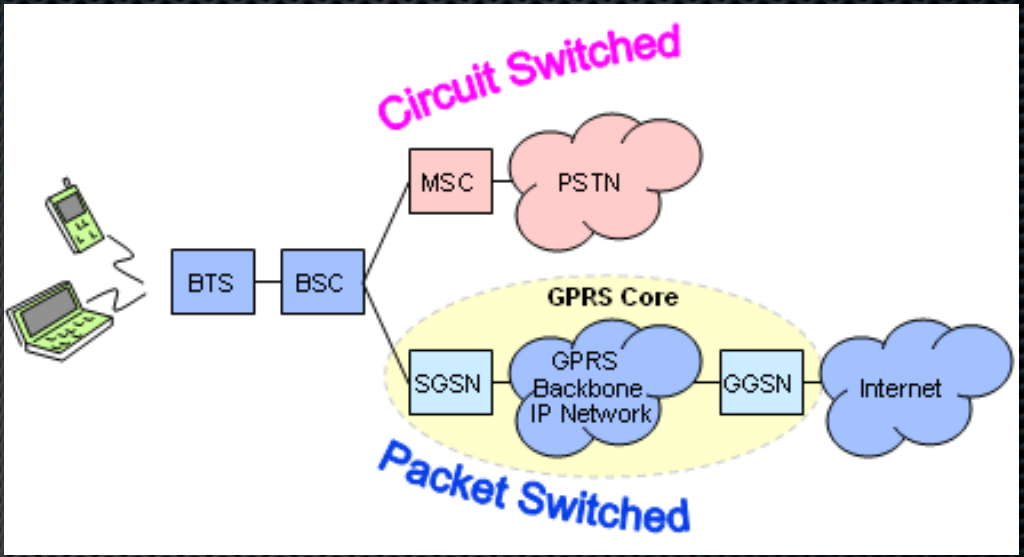
Philippe.Langlois@p1sec.com

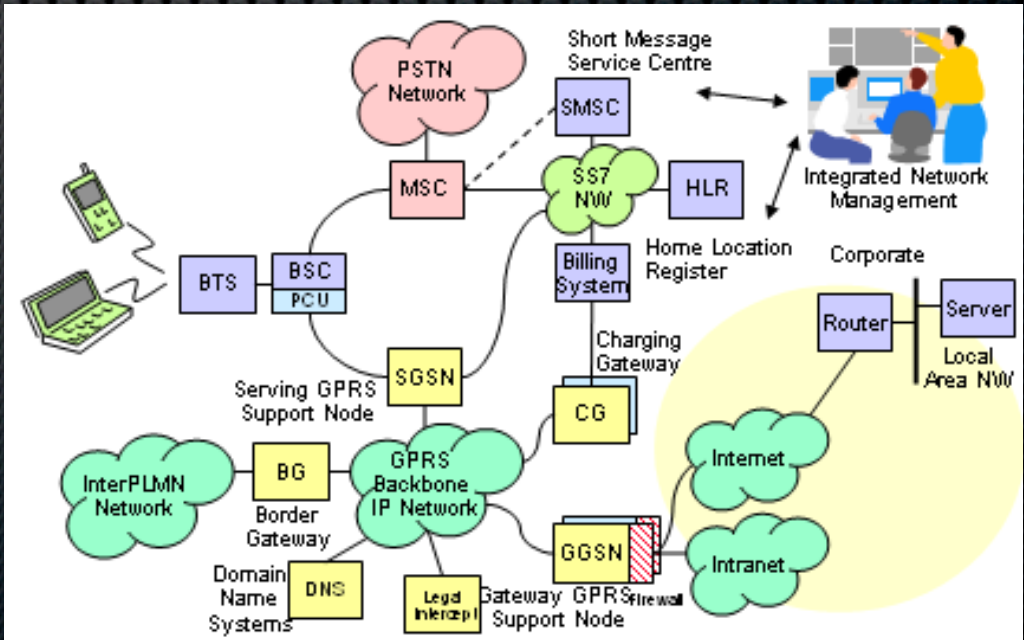
V1.5

GPRS architecture

P1 Security
Priority One Security

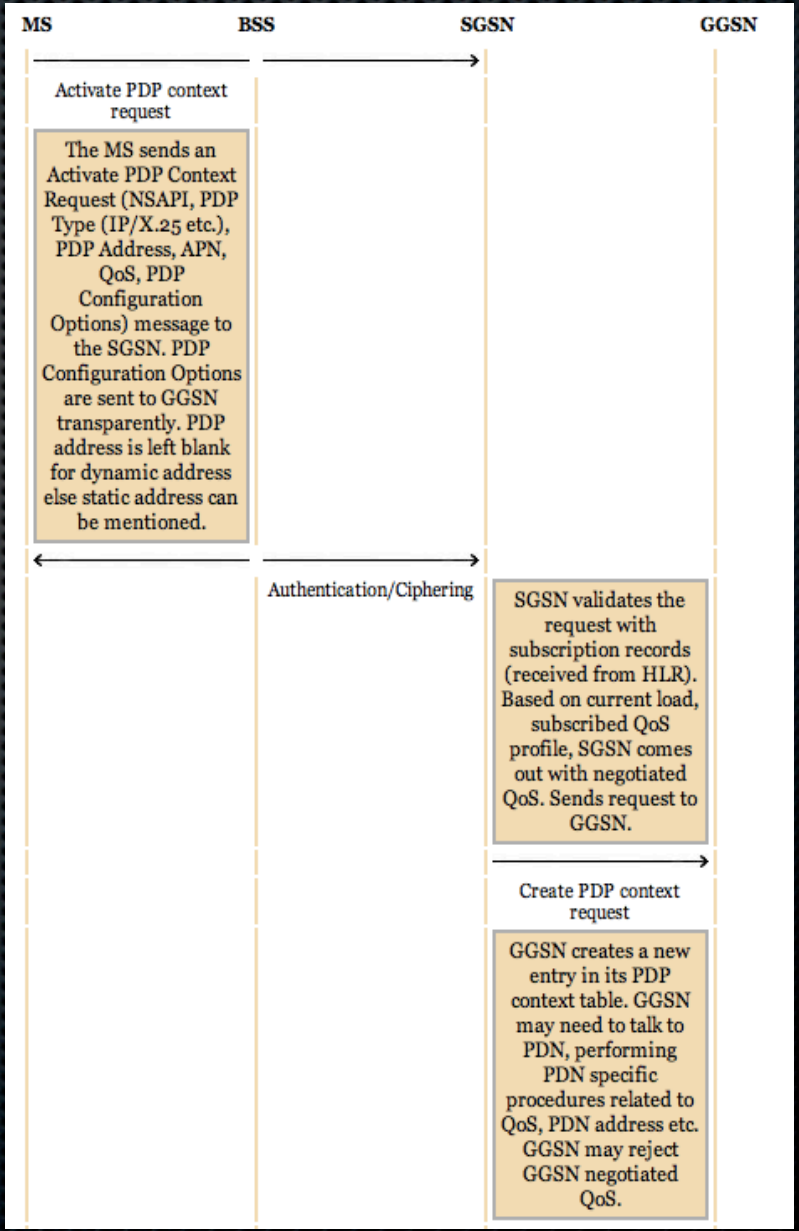
- "PS" Domain in context
- Successor to GSM 9600 baud modem (CSD or HSCSD)
- PDP context = GPRS session
- 2G/3G: SGSN, GGSN
- 4G: MGW, PDGW/PGW
- But also many more machines (LI, DNS, Billing…)
- GPRS backbone = GRX





GPRS uses cases

- APN
  - internet
  - mms
  - special APNs (OAM, billing, ...)
  - *.corp APNs
  - M2M APNs
  - Telco internal APNs !

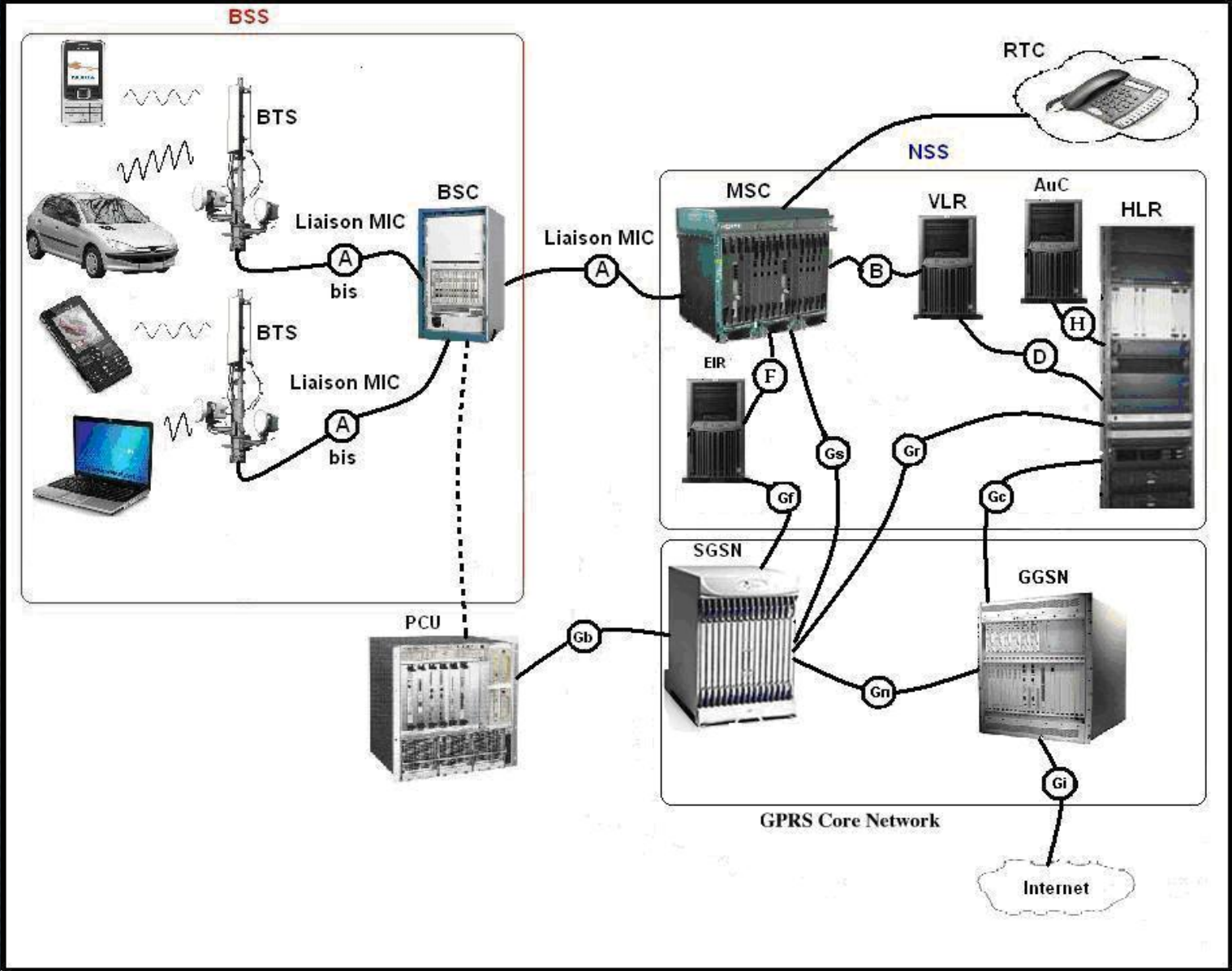


Example: UPS management

- M2M example: management of UPS
- Access the devices… and the management console too (Java, vulnerable)
- Usually on corporate network (IP bastion or router)

2G

- IP was new in telco
- Billing is a big issue in GPRS
- Many GGSNs
- SGSN & GGSN to CGF not shown
- Proxies, security filters not shown
- Typical of telco



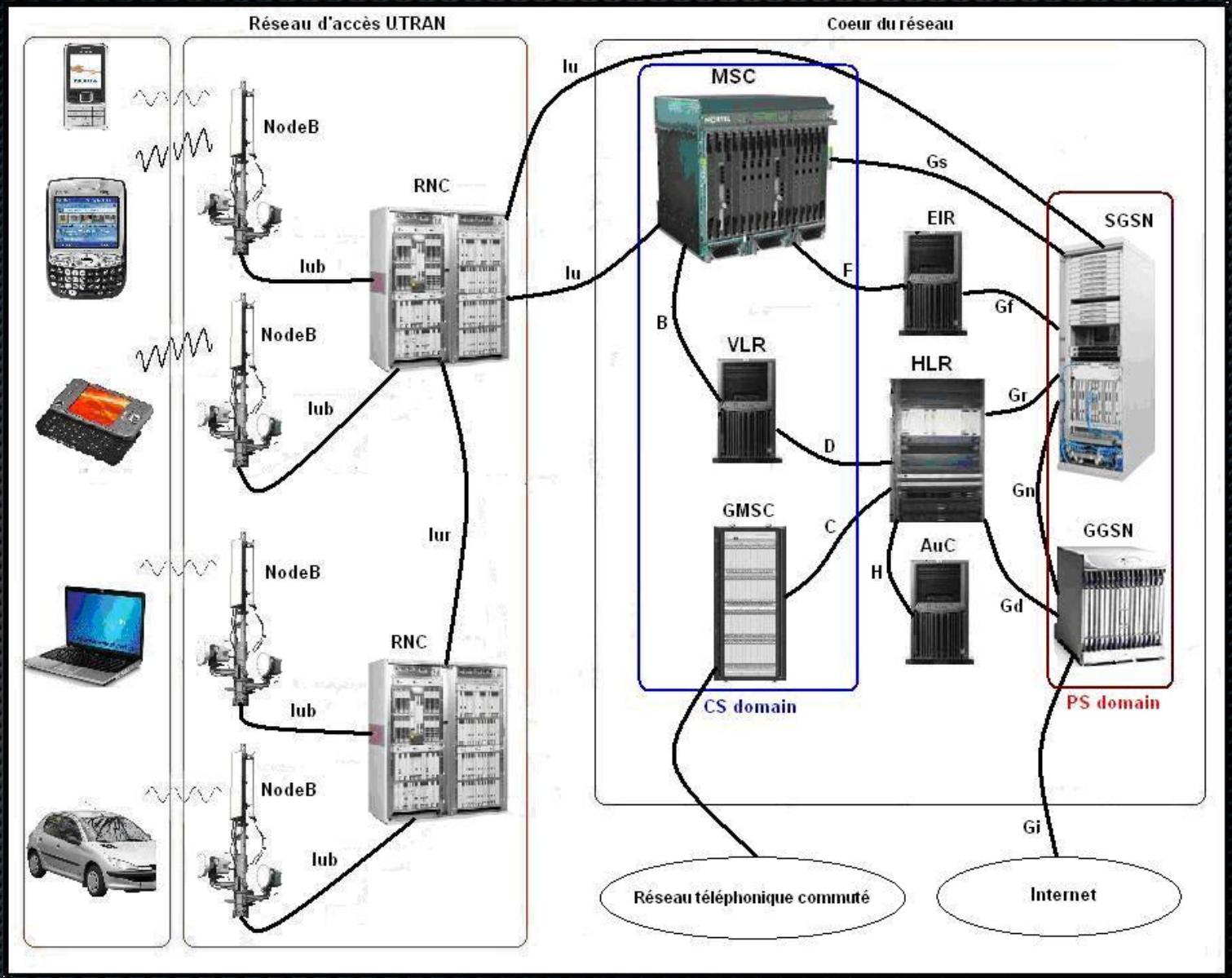
GPRS Radio security in 2G

P1 Security
Priority One Security

- Many GPRS implementations in clear text (Italy, Denmark) !
- OsmocomBB with 4 receptors (and HW mod) http://bb.osmocom.org
- Radio encryption algorithm GEA1 and GEA2 broken
  - By Karsten Nohl, Mate Soos, Sylvain Munaut
  - At CCC Camp 2011 (August)
- Big state (1500 byte MTU), many known point in the equation system
- Linearization, gaussian solving, not even SAT solving

3G

- UMTS
- No open source hw receptor for 3G
- Only “client” access through USB dongles or 3G phones.
- GEA3 (Kasumi KLEN=64 bits) and GEA4 (Kasumi KLEN=128 bits)



Getting access: The SIM card!

P1 Security
Priority One Security

- Obtaining an anonymous SIM card for GPRS hacking
- Varying level of ID checking depending on the country
  - Malaysia checks a lot
  - Thailand MNOs give them out for free at airport
  - France doesn't check well anymore
- MVNOs check less
- Some SIM cards are part of CUGs

Buy second-hand !

- Second hand hardware
- Guess what's still in it?
  - SIM card!
- Cheap PCMCIA cards
- Sometime in laptops
- Company gets rid of previous “mobility” fleet: CUG access to network
- 1 out of 3 equipment !

Typical GPRS hacking methods

P1 Security
Priority One Security

- APN bruteforcing
- “In GPRS network” attack of peers / other client devices
- X25 GPRS network hunting
- “In GPRS network” attack of server devices
  - GPS tracker M2M gives access to LEA management server !

GPRS hacking from the air

P1 Security
Priority One Security

- RFC1918 network, reach your peers
- Worm on Paris “Velib” M2M network
- Contaminated Velib stations over the air
- Enter GPRSdroid

Telco GPRS hacking

P1 Security
Priority One Security

- A tale from Indonesia
  - GPRS normal connection
  - Lack of network segmentation from “Internet”
  - Seize control of NSS / OAM and Routers (MPLS CE and PE)
- APN “mms” or “wap”
  - Access to MMSC and other Core Network infrastructure
  - Ports not firewalled
  - Telecom Operators (MNO) lack proper automated tools to check network segmentation

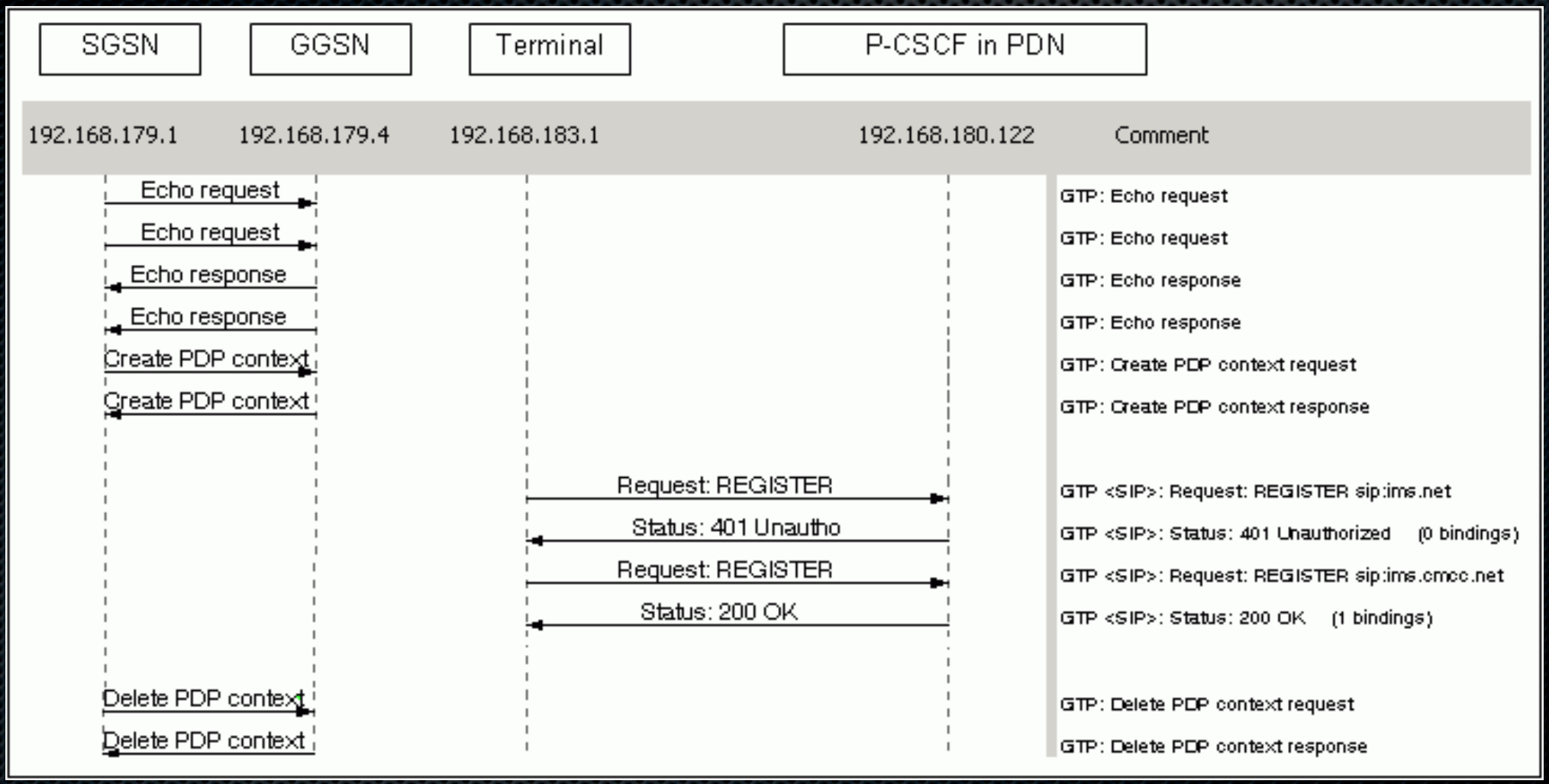
GPRS current (recognized) major issue is...

P1 Security
Priority One Security

- iodine !
- Bills (CDR) generated on proxy
- Traffic possibly not billed (SGSN or GGSN CDR?)
- Why Telecom operators (MNO) are lagging so bad?
  - Telecom Culture
  - If it does not create costs, it’s not detected by Fraud Management Systems

Toward IMS / 4G: Full IP

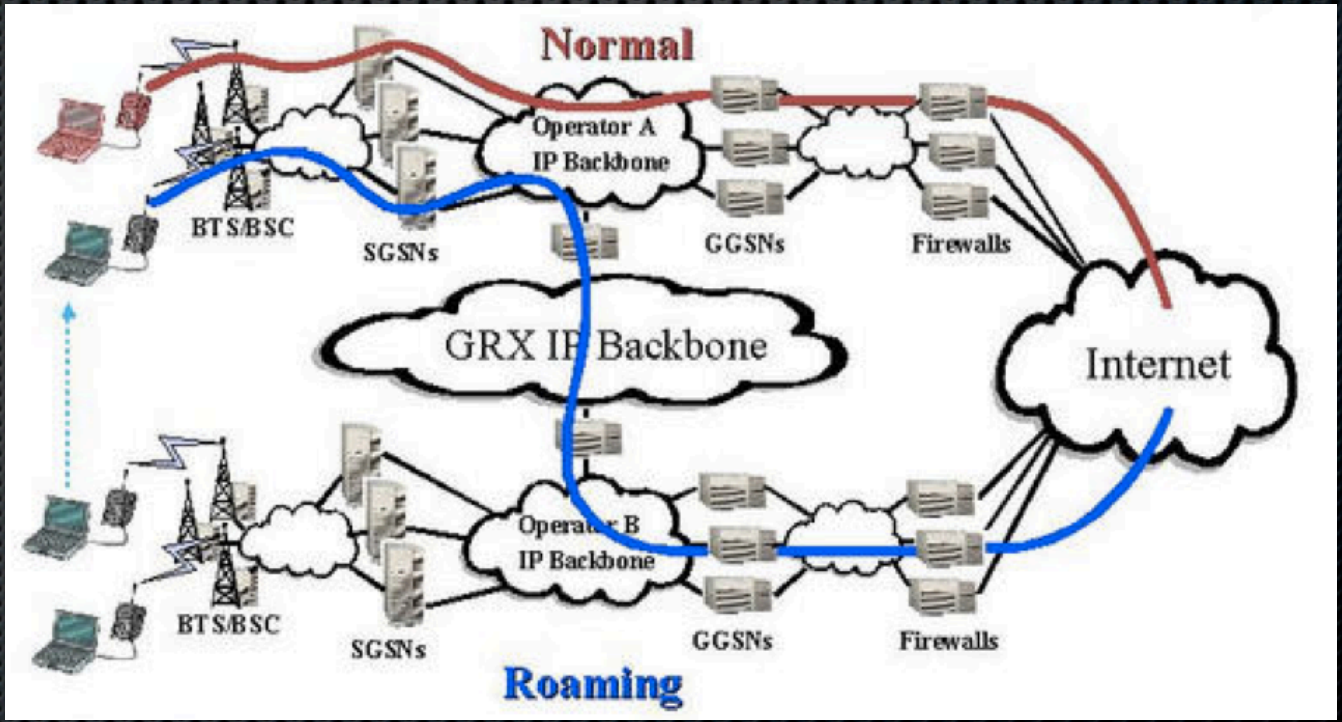
P1 Security
Priority One Security



Hint: a) SBC is not far away b) RTP is rarely inspected

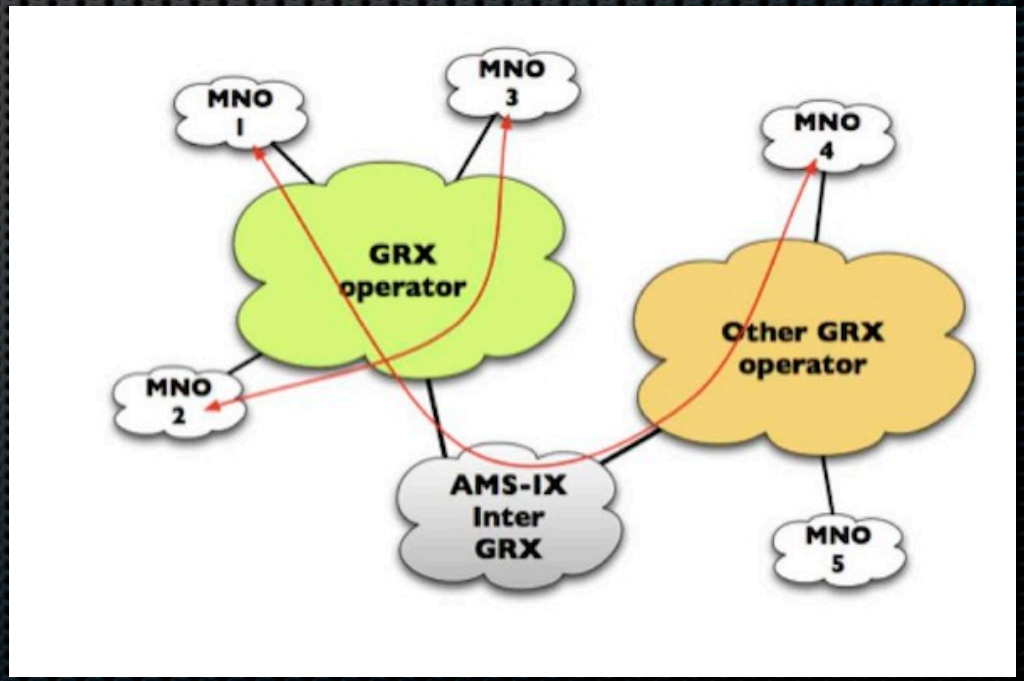
Here comes GRX

- Your national network, from abroad.
- GPRS roaming
- Tunnels (GTP)
- One to one vs. one to many
- From GGSNs to SGSNs



What do Amsterdam and Singapore share?

- NOPE! Not what you're thinking!
- Inter GRX exchanges
- AMS-IX & Singapore Equinix
- No need to go there to access GRX



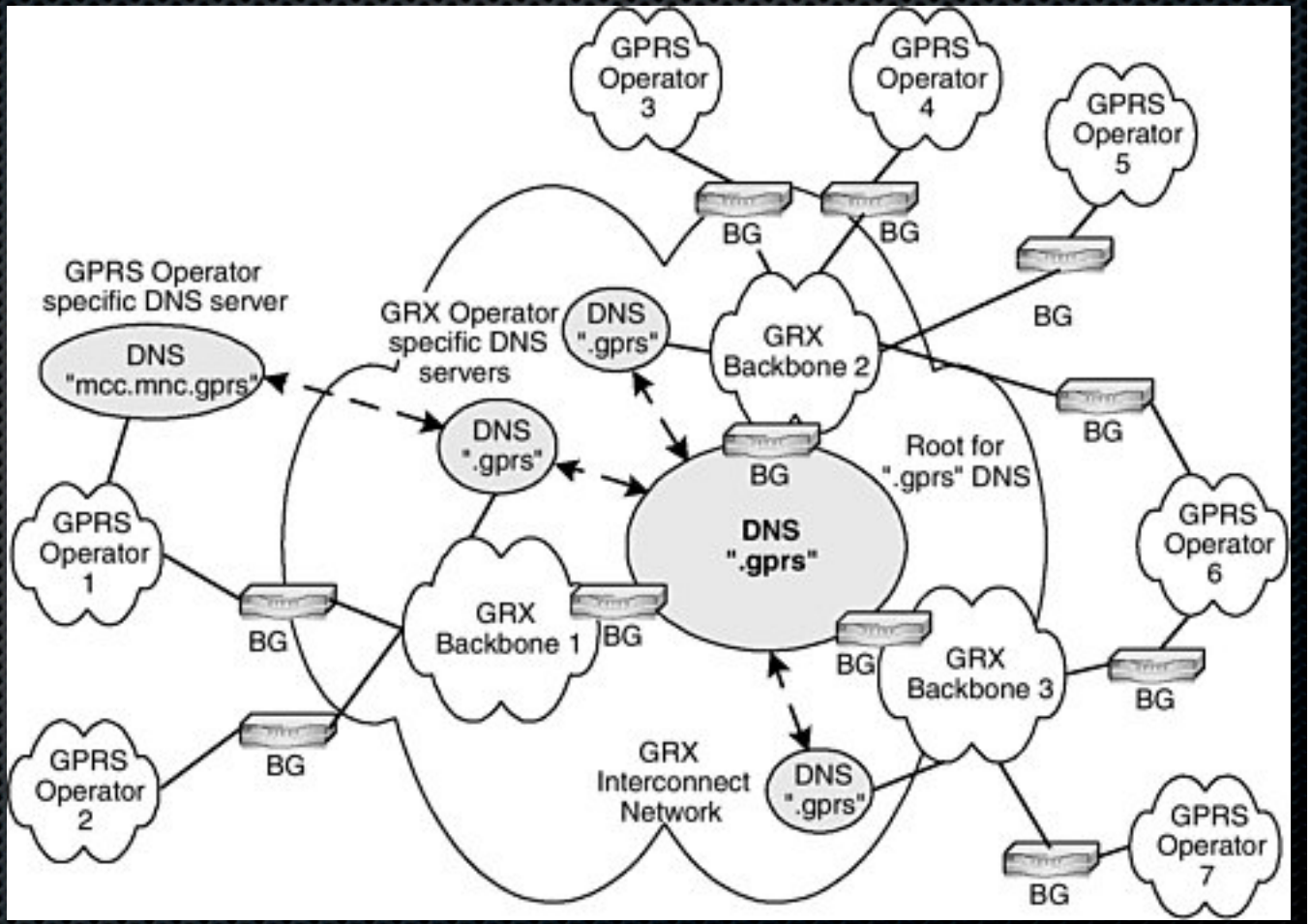
GRX technologies

P1 Security
Priority One Security

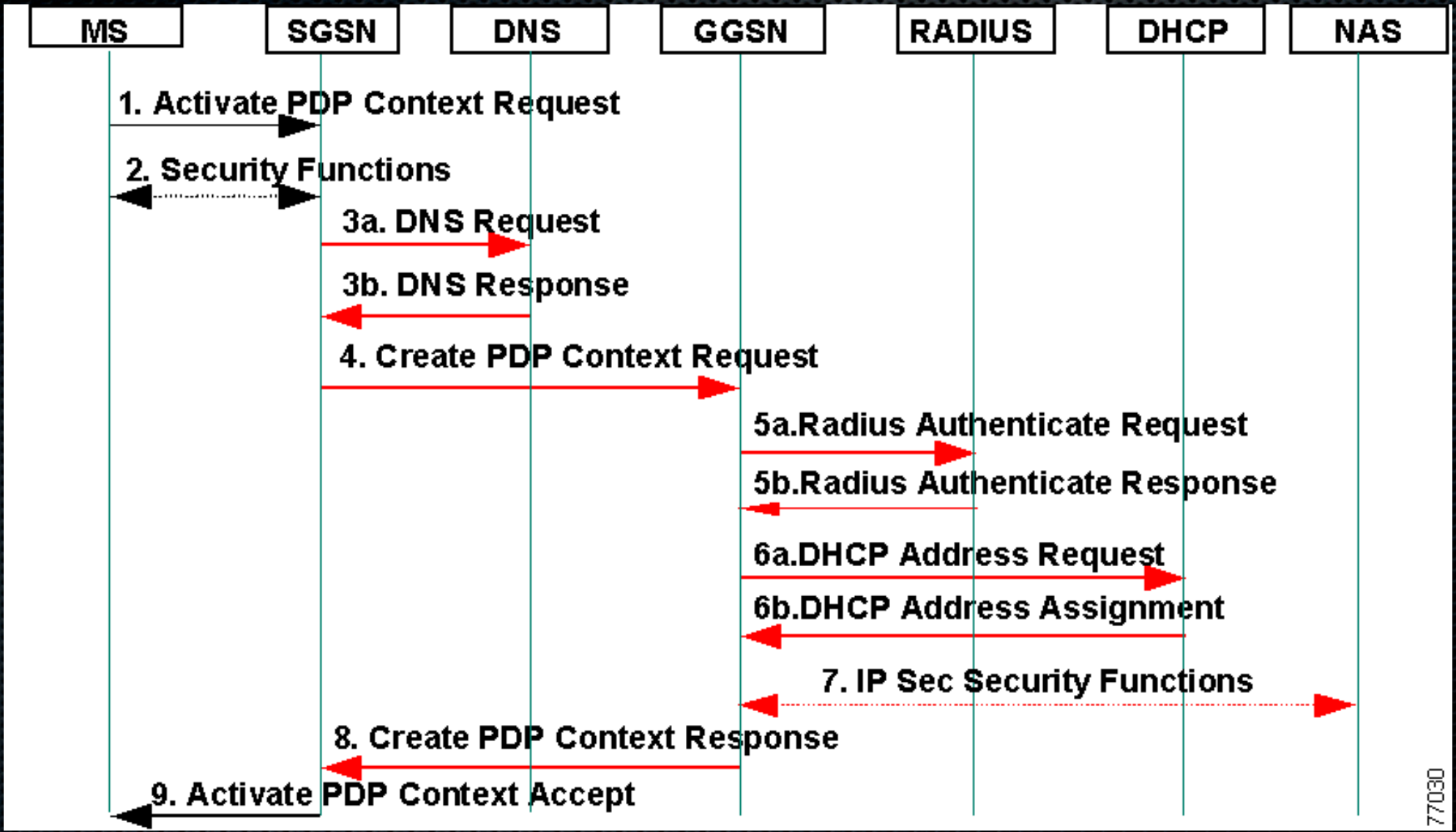
- GTP – GPRS Tunnelling Protocol
- DNS
  - `<APN>.mncYYY.mccZZZ.gprs`
  - SFR in France : `internet.010.208.gprs`
  - “Segmented” from the internet… right.

DNS - Do Not Share?

- Internet technology MADE FOR sharing
- Hard to split



GPRS Dialogue



A story of split DNS

P1 Security
Priority One Security

- Of course it's not a valid IANA TLD

```
$ host -t ANY gprs.
Host gprs. not found: 3(NXDOMAIN)
```

- ".gprs" is considered crown jewel, to be protected
  - Direct connectivity to all SGSN and GGSN
  - Big machines, one crash == thousands of disconnected
- Well… let's try from inside a GPRS session?

And from inside?

- From a GPRS session, most of the time, same thing:

```
$ host -t ANY gprs.
Host gprs. not found: 3(NXDOMAIN)
```

- Some problem happens sometime

```
$ host -t ANY gprs.
gprs has SOA record dns1.GRXOPERATOR.com. info.GRXOPERATOR.com
gprs has address 10.XX.20.1
gprs name server dns5.GRXOPERATOR.com.
```

- W00t!
- Then the whole hierarchy is accessible
- Because you're a SGSN!

Enter GRXdroid

- Soon on the Android market
- Bruteforce resolving of GPRS DNS (and more)
- Horrible UI for now, wanna help? :-)
- But does the Job
- Send me an email, I'll send you the APK

P1 Security
Priority One Security

Triple play, four way

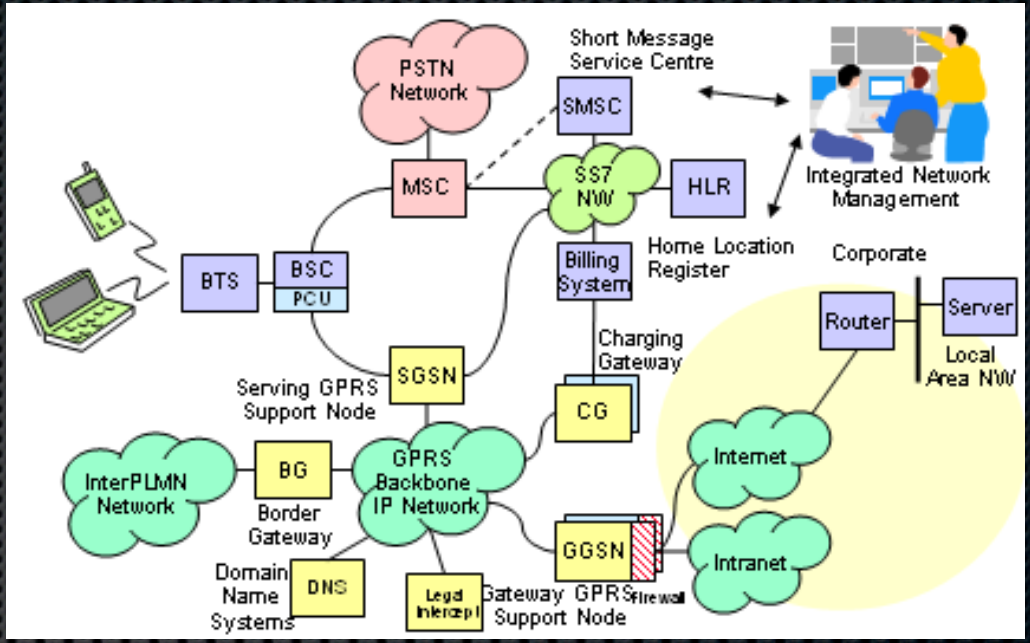
P1 Security
Priority One Security

- GPRS APNs
- WLAN
- VoIP network (VLAN and MPLS plane)
- ADSL / FTTH network / IPTV
- Customer traffic VLANs / MPLS planes everywhere, connecting to so many services
- Everything for the application,
- Network is considered "necessary evil, make it just work”
- Management cares only about new services roll out

When, not if

- Wait, wait, wait, win!
- Here comes the sentinel, a tale of an old finger trick
  - Pentest from the 90s in Thailand
- DNSsentinel
  - Keep trying till it succeeds
- Many tubes to be using
  - GPRS APN, username + password, Dial number
  - IN profile + USSD setup (for example *136# on Maxis)

Inside the GRX



- From DNS leaks to route/packets leaks
- Firewalling issues
- You're a SGSN ! GTP to all GGSNs
- SGSN should contact GGSN… filter? Anyone?
- Way too many services exposed
  - From Solaris RPC down to SIGTRAN services (SS7! Wow!)
- MNO says: “Protect? Well, it’s restricted to operators right?”

Evolution of GRX: 3gppnetwork.org

P1 Security
Priority One Security

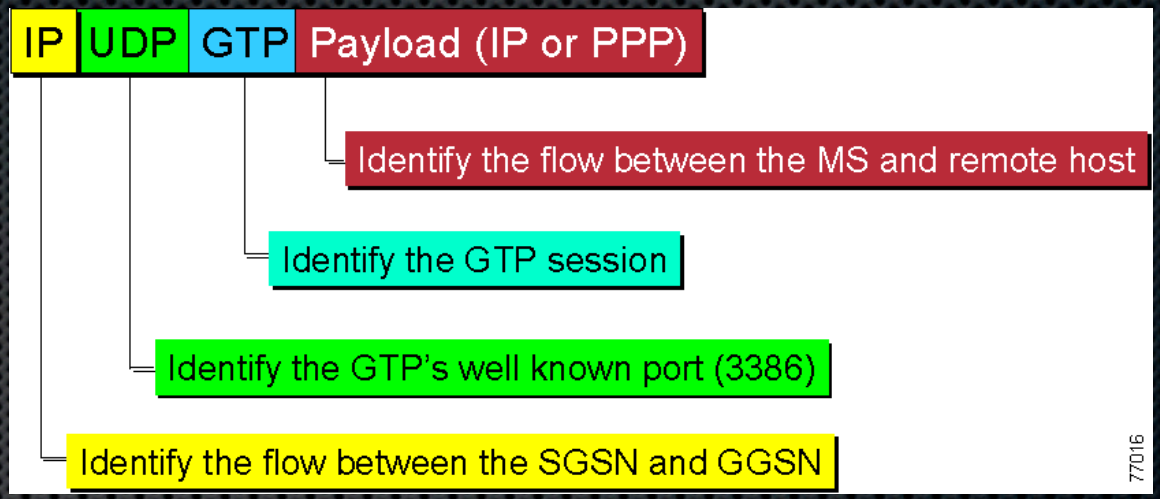
- A bit like ENUM (cf. e164.arpa zone) but for Core Network
- Many different subdomains
  - APN `<APN name>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.`
  - IMS `ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org.`
  - SGSN `sgsnXXXX.mnc<MNC>.mcc<MCC>.3gppnetwork.org.`
  - LTE EPC `epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.`
  - LTE MME `mmegiXXX.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.`
- Used for identities, many RAN / RAT

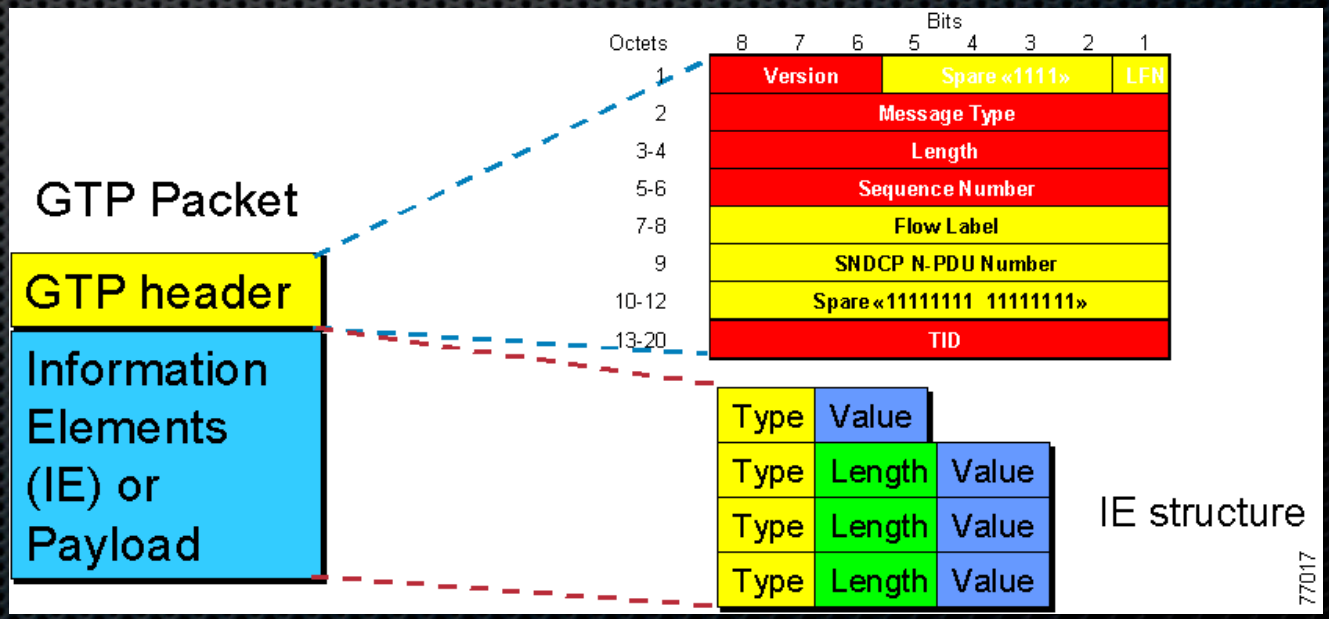
```
User-Name = "1208012000584533@wlan.mnc001.mcc208.3gppnetwork.org"
```

  - Diameter enabled servers (scan for port 3868)

GTP basics

- From SGSN (client)
- To GGSN (server)
- Many “commands” possible in Message Type





GTP scanning in GRX

P1 Security
Priority One Security

Table 6.1-1: Messages in GTP-U

Message Type value (Decimal)	Message	Reference	GTP-C	GTP-U	GTP'
1	Echo Request		X	X	x
2	Echo Response		X	X	x

- Daniel Mende did it on the Internet, here is
- Way too many open GTP service on the Internet
- Higher ratio on GRX of course
- Easily scanned with GTP Echo Request
- UDP ports 2123, 2152, 3386, Super fast positive scanning

GTP in GTP attack

P1 Security
Priority One Security

GRX	MNO
✓	✓

- Free Internet surfing
- Access directly the GGSN from another GGSN
- Not supposed to happen… but happens!
- Just use sgsnemu / OpenGGSN to create new interface and route your traffic through it
- Sometime, GTP in GTP is not supported by GGSN… at all
  - Crash and unavailability
- Super fast scanning on GRX: covers the whole planet!

GPRS CUG accesses attacks

GRX	MNO
✓	✓

- CUG = Closed User Group
- At GTP level, you're either a SGSN or GGSN
- Since you are a SGSN (client), you control
  - APN you're going to use for the tunnel and
  - MSISDN / IMSI you are impersonating.
- CUG are based on these parameters
- Bank networks, Operator networks, Administration, etc…
- Straight from the Net or from an existing PDP with unfiltered GGSN GTP ports.

GTP Tunnel disconnection DoS attack

P1 Security
Priority One Security

GRX	MNO
✓	✓

- TEID bruteforce
- Disconnect Message Type (Delete Session Request. Delete PDP, …) + spoof SGSN (really?)
- 2^32 would be a problem… if TEID were not sequential :-)

```
[...]
00 00 17 04    Delete PDP Context: Request Accepted
00 00 17 44    Delete PDP Context: Request Accepted
00 00 17 A1    Delete PDP Context: Request Accepted
00 00 17 BF    Delete PDP Context: Request Accepted
00 00 17 D8    Delete PDP Context: Request Accepted
00 00 17 E8    Delete PDP Context: Request Accepted
[...]
```

Fake charging attacks

94	Charging ID	Extendable / 8.29
95	Charging Characteristics	Extendable / 8.30

GRX	MNO
✓	✓

- Normal GTP 2 traffic
- But with Charging ID and Charging GW (CGF) address specified
- Creates fake CDRs (Call Detail Records or Charging Data Records) for any customer
- Not necessary to get free connection anyway :-)

GRX Subscriber Information Leak

P1 Security
Priority One Security

GRX	MNO
✓	✓

- SGSN and GGSN need to communicate with many Network Elements in 3G and 4G networks
- GTP v2 enables many requests to these equipment directly over GTP.
- Think “HLR Request” over UDP
  - No authentication
  - Much more available than an SS7 interconnection :-)
- And you’re GLOBAL ! Thanks GRX. That is, any operator in the world that is connected to any GRX.

Relocation Cancel attack

P1 Security
Priority One Security

- Basically tell one SGSN that the user it is serving should come back to you
- User is effectively disconnected (or hangs), no more packets.
- Targer user by IMSI
  - But you already got that by the Info leak of previous attack

Table 32: Information Elements in a Relocation Cancel Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Private Extension	Optional	7.7.46

GRX	MNO
✓	✓

  - Shoule be Intra-operator, but does work over GRX!

GGSN DoS attack

P1 Security
Priority One Security

GRX	MNO
✓	✓

- Another magic packet
- “Oh, I’m a bit congested and about to crash, it would be good for you to relocate to another GGSN to continue your service”
- Result: GGSN deserted, users don’t get any other GGSN, users loose service.
- Per APN impact (i.e. “internet” or “*.corp”)
- Exercise to the ****er

SGSN DoS attack - Ouch

P1 Security
Priority One Security

GRX	MNO
✓	✓

- More rare because by their nature (client), SGSN are rarely reachable through IP
- Same attack as previous (Hey, you should really switch to another node, this one is going down)
- Much more impact:
  - Targets a region rather than a network,
  - Repeat on GRX == Disconnect many countries
- Both these are caused by “evolved GTP” i.e. GTP on LTE Advanced networks.

A tube in a tube in a tube

P1 Security
Priority One Security

GRX	MNO
✓	✓

- Air -> GTP -> SIGTRAN M3UA SCTP -> SS7
- Oh My Goat, SS7 from the GPRS network
- Script:

  1) Connect to APN

  2) Scan for SCTP M3UA (port 2905)

  3) Establish M3UA connection to say 10.27.1.30

  4) Send SS7 over GPRS ;-) for example, SSP (SubSystem Prohibited) or MSC Reset !!! (disconnect all users from MSC)
- It's Core Network access from GRX !

As an operator: Protecting your GRX connection

P1 Security
Priority One Security

- Filter smartly your GGSN
- Beware of spaghetti tunnel (i.e. tunnel in a tunnel, tunnel chainings, ...)
- Hard, even impossible to predict routing and filtering results (GTP + GRE + MPLS + VLAN + Filtering + Routing + Load Balancing + HA + Multihoming)
  - You need to TEST !
- You are responsible of all entries on GRX through your GRX interconnection!

Go massive

P1 Security
Priority One Security

- “A tube in a tube in a tube”
- With many access network technologies
- Very difficult to get right in order to protect
- Automation is key!

M2M: In the end, the customer

P1 Security
Priority One Security

- Banks, Transportation, Smart grid, smart meters
- Worm on the CUG?
- Bills of the other side of the planet
- GTP, DNS and M2M for profit
- GRX: Nice little global network
- Globally accessible with the right APN

Here comes India

P1 Security
Priority One Security

- Admitedly some "problems" with "importations", Backdoors, Remote accesses, Clueless operators about their Provider contracts
- Telecom CIP: now serious about Critical Infrastructure Protection
- Leading the way in telecom regulation: $11M fine, license kill
- Law export: DMCA in the US exported to Europe?
- Indian Telecom Law exported to US & Europe, worldwide soon

A glimpse on the future

P1 Security
Priority One Security

- IMS and 4G
- All in DNS paradigm
- From HLR to ...
- Diameter and HSS?
- or
- DNS and ENUM?
- Compatible options, who will win?

Questions?

P1 Security
Priority One Security

- Now!
- Or join us for the workshop !
- Send email for the APKs
- SVC global pass – ask us!
- Hackito Ergo Sum, Paris, 12-14 April 2012.

P1 Security
Priority One Security

THANK YOU!

Philippe.Langlois@p1sec.com