

# LTE Network Security – Private Networks

Simon Lardner

Challenge Networks / Vocus

# Introduction to Challenge Networks

- One of the leaders in private LTE network design & build in Australia
- Have 20+ deployed LTE networks both in Australia and internationally
- Recently acquired by Vocus
- A number of 'first's in private LTE networks:
  - First underground LTE network in mining
  - First in Oil & Gas
  - First Gold mine
  - First in Peru
  - First in Copper mine
  - First using Nokia technology
  - First to use Band1 (2100 MHz) in Australia for LTE

The logo for Vocus, featuring the word 'VOCUS' in a bold, dark blue, sans-serif font. The letter 'O' is stylized as a cluster of six small, dark blue circles.The logo for Challenge Networks. It features the word 'challenge' in a lowercase, black, sans-serif font, with the word 'NETWORKS' in a smaller, orange, uppercase, sans-serif font below it. To the left of the text is a stylized graphic consisting of orange and black lines forming a shape that resembles a network or a stylized 'E'.

# Why talk about it ?

- Security is becoming more topical -> Some people are getting paid lots!
- Some (in)famous examples recently
- In the area of private networks – becoming a ‘hot topic’ as the industry becomes more mature
- More edge devices being connected -> More to go wrong
- Smarter edge devices -> More to go wrong
- Different types of edge devices -> More to go wrong

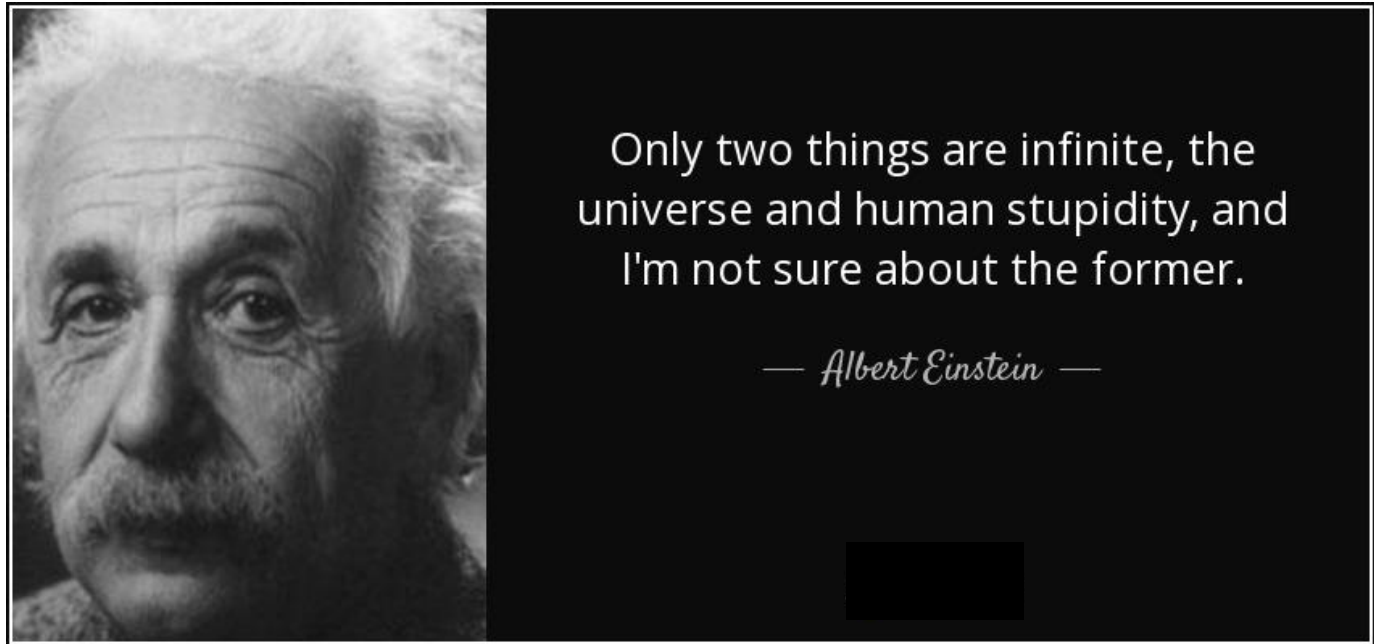
“DDos by Fridge”

# What are we talking about (and not) today ?

- A huge topic – just touching on a few items !!
- Focus on private industrial networks so NOT consumer networks or public safety networks (but there is some overlap)
- Just talk about 4G (but 5G is similar)
- What are key areas to not worry about
- What are key areas to worry about
- Four specific solutions – ‘easy wins’

# What are you trying to protect from ?

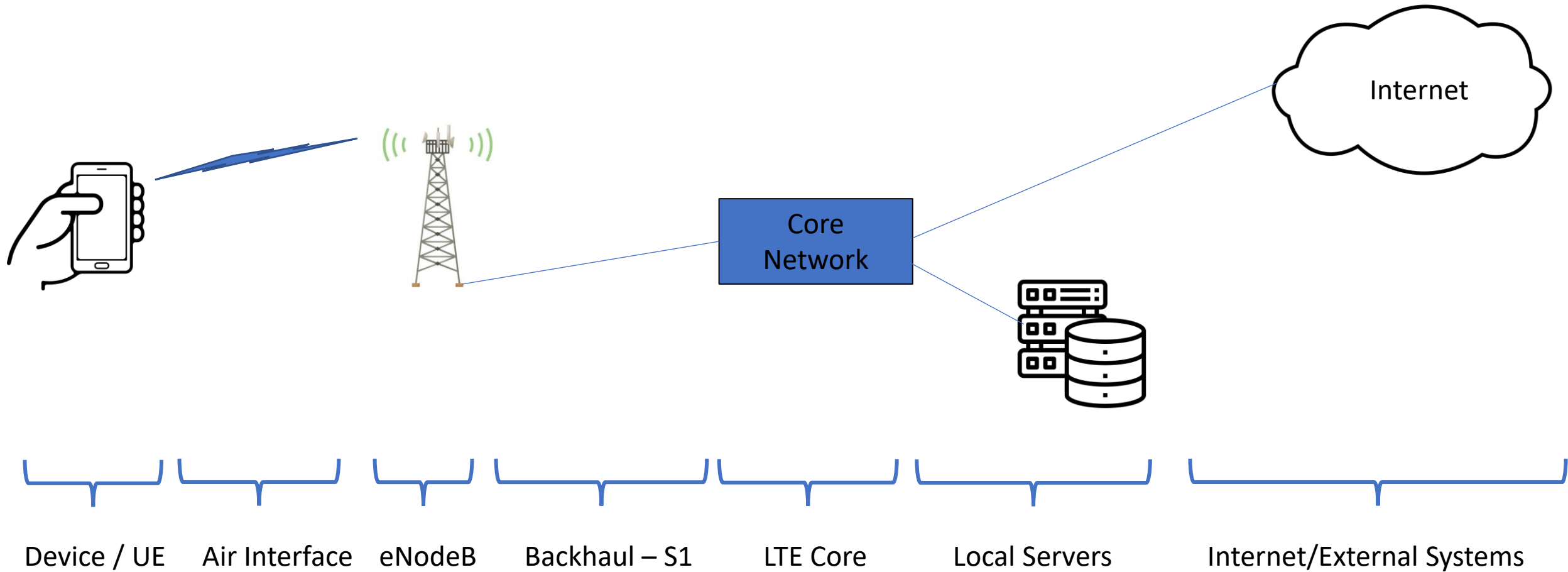
- Stupidity
- Ignorance
- Maliciousness
- Mistakes



# Opening statements

- By design, with regards to security, LTE is ‘pretty good’
- It’s better than Wi-Fi – so don’t confuse them
- LTE/4G (and now 5G) is a continually evolving protocol

# The basic network components



# Device (UE) Authentication

- User authentication
  - Device
  - SIM card
- Data confidentiality
- Data integrity protection
- User identity confidentiality
- Mutual Authentication

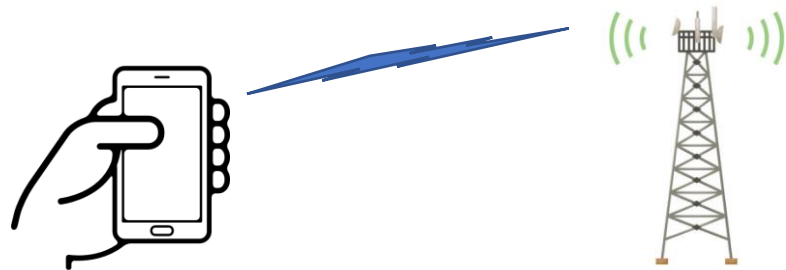


Device / UE





# Air Interface - Uu

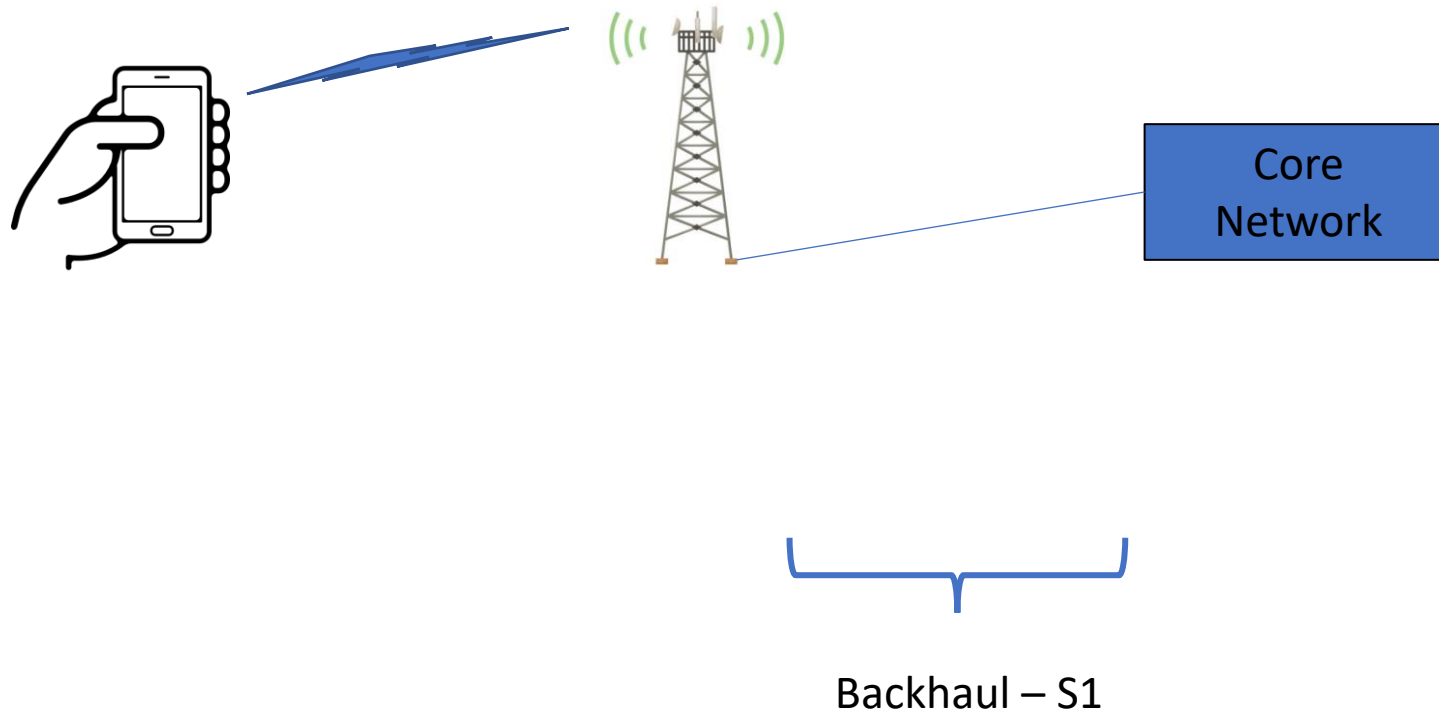


- Encryption of Control plane & User plane
- No collision domains or limitations in Broadcast Domains
- The above has lots of positive implications



Air Interface eNodeB

# eNodeB to Core interface – S1



- The ‘backhaul’ or transmission network
- NOT by default encrypted
- May (or may not) be a problem – depends on network

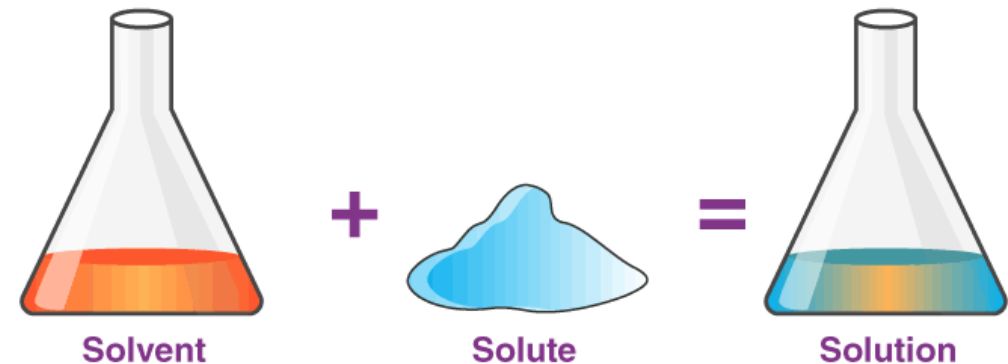
# A key problems / 'Opportunities' with private networks



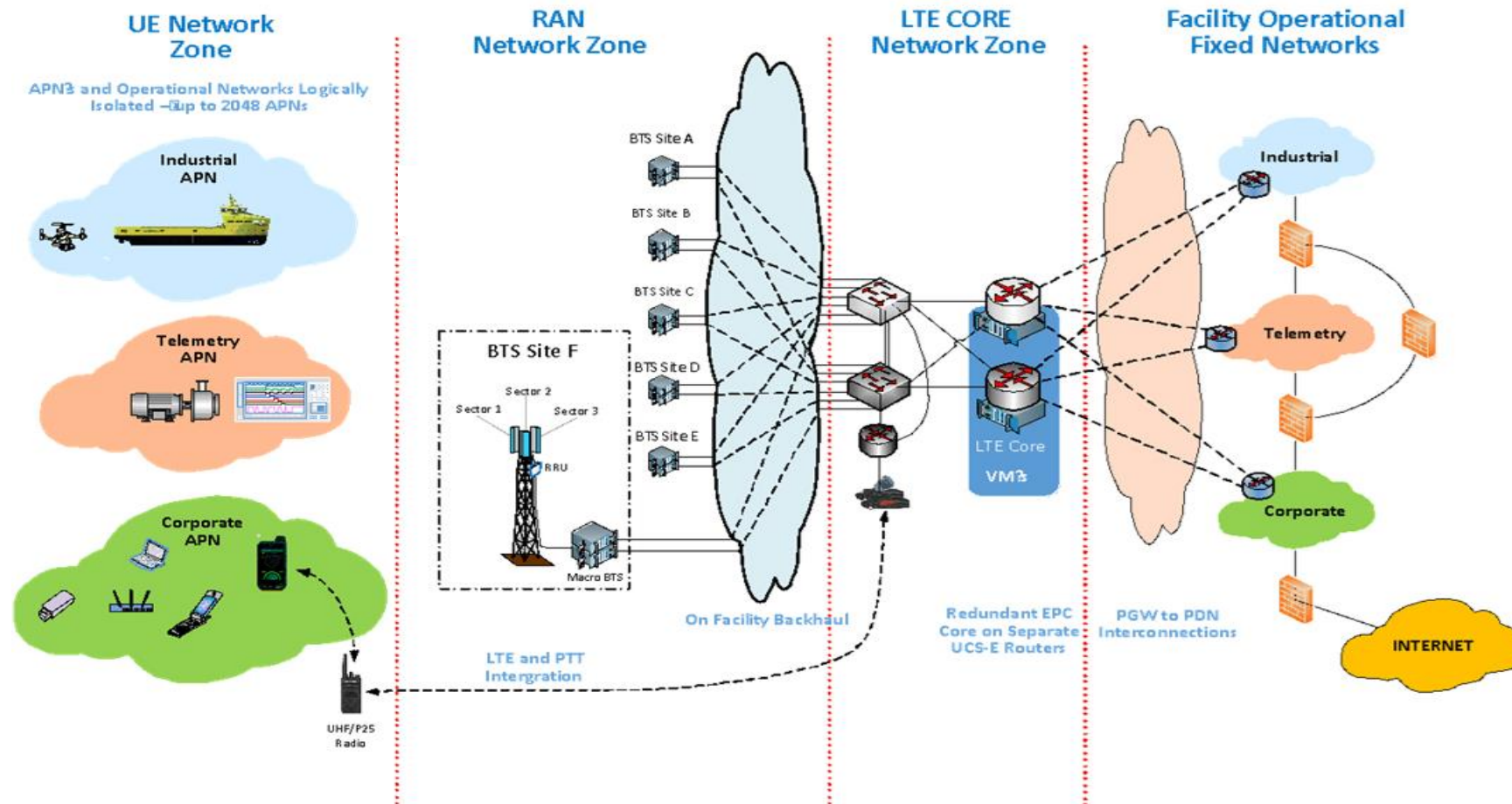
- Different users with different security profiles:
  - 'IT users'
  - 'OT users'
- Different user requirements:
  - QoS
  - Access control
- User devices have different 'abilities'
- Users sometimes 'play' with stuff
- Very specialised traffic flows

# Some solution options to consider

- Core network configuration – Network slicing
- EIR – Equipment Identity Register
- Monitoring – end to end network
- MDN – Mobile Device Manager



# Security 'zones' of a private LTE network – networks within a network



# End to End – Quality of Service (QoS)



FMS – Vehicle command and control

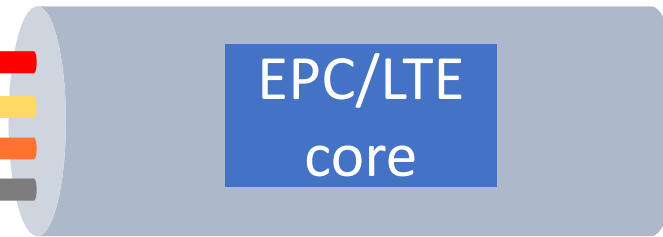
Video

PTT - voice

Telemetry

- ‘Tunnels’ of data, each with own priority and guaranteed bit-rate
- End to end QOS – from UE to application servers

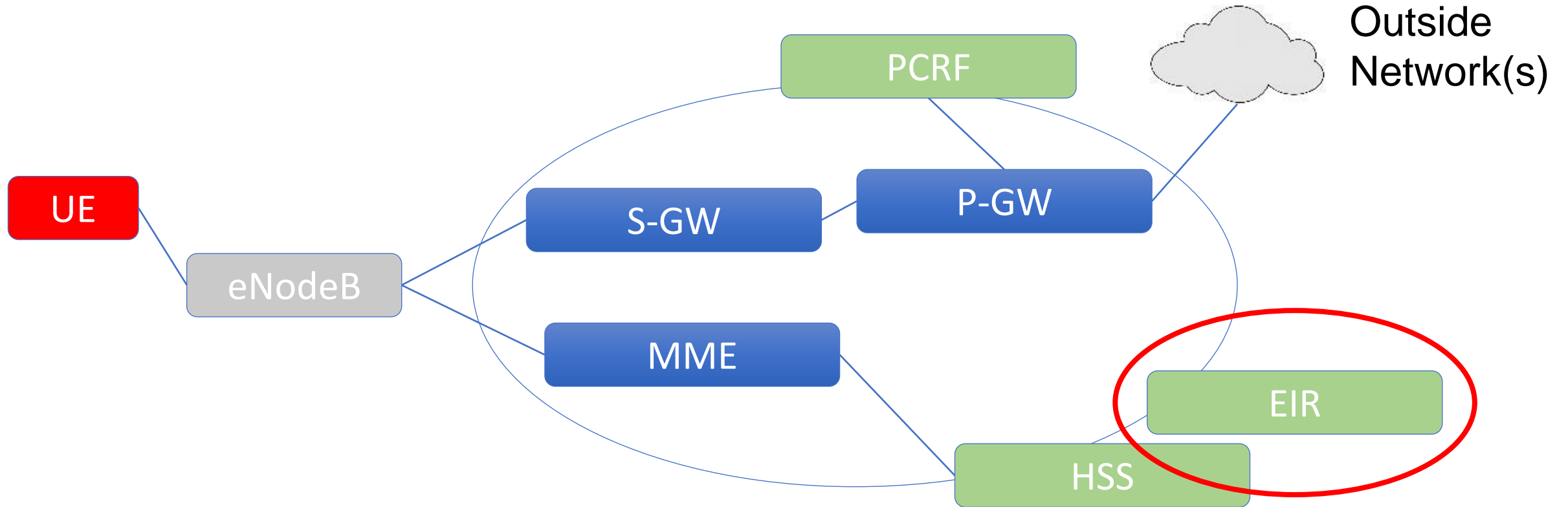
LTE router



Network Router



# Components of the network (a bit technical)



# EIR – Equipment identity Register

- Standard LTE function/system
- Used completely differently to consumer networks
- ‘Locks’ a SIM card (IMSI) to a specific Device (IMEI) or device type
- Requires some maturity from the end user and/or network owner
- Critical to implement if you multiple security domains in network





# UE – MDM (mobile device Manager)

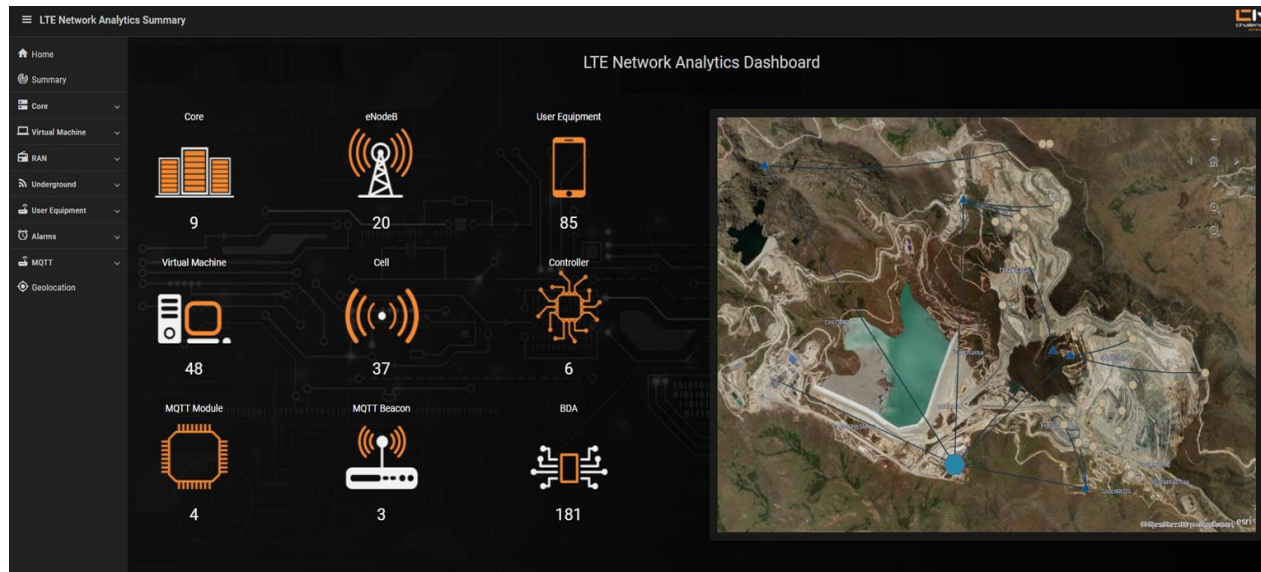
- Essentially ‘controls’ the phone.
- Really important if you have critical applications on device.



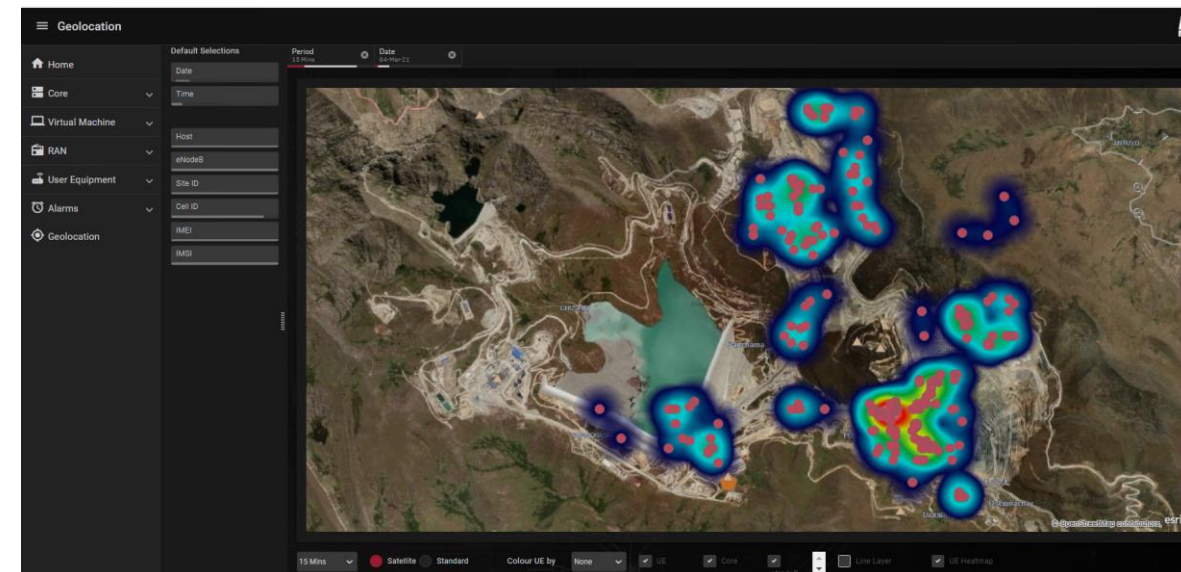
# Network monitoring

- Only one thing worse than having a problem...
- Not knowing you have a problem.
- Needs to be at 'whole of network' & 'UE level'

Whole of Network



UE 'Heat map'



# Questions ?

