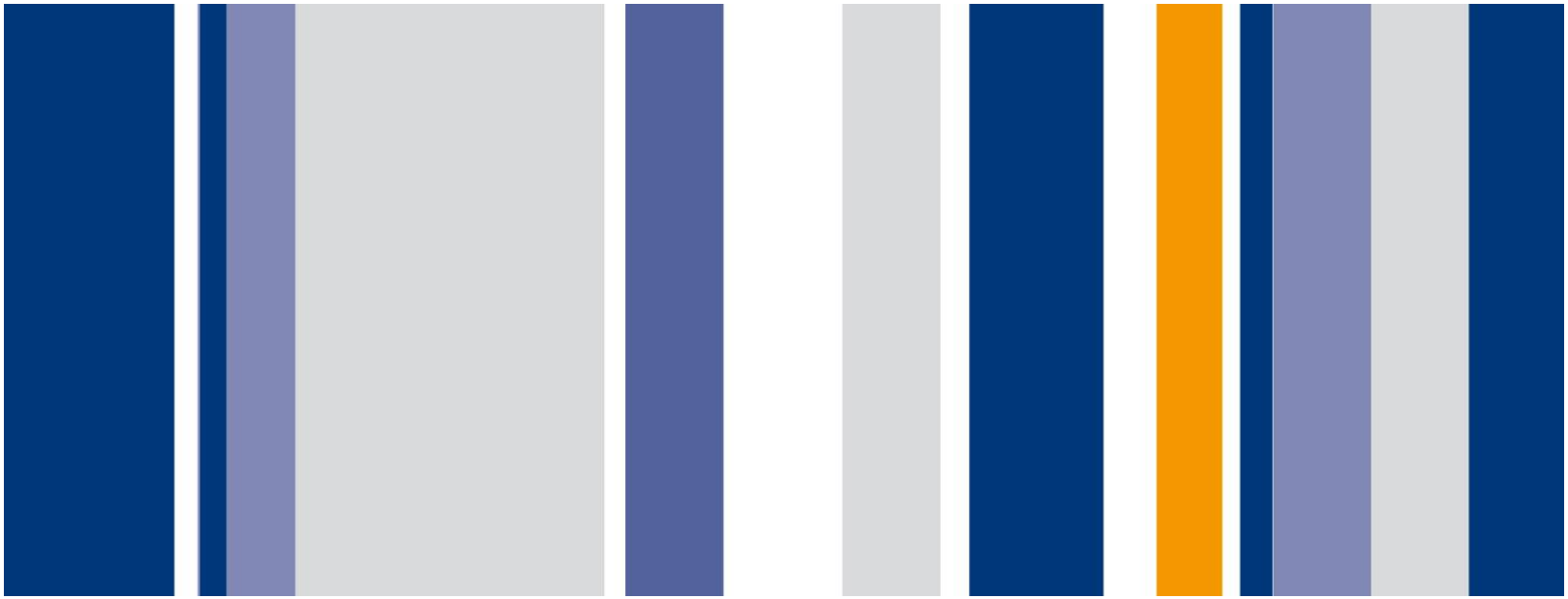
Practical Security Testing for LTE Networks

BlackHat Abu Dhabi
December 2012
Martyn Ruks & Nils



MWR INFOSECURITY

Today's Talk

- Intro to LTE Networks
- Technical Details
- Attacks and Testing
- Defences
- Conclusions

Intro to LTE Networks

Mobile Networks

A Brief History Lesson

- 1G – 1980s Analogue technology (AMPS, TACS)
- 2G – 1990s Move to digital (GSM,GPRS,EDGE)
- 3G – 2000s Improved data services (UMTS, HSPA)
- 4G – 2010s High bandwidth data (LTE Advanced)

Mobile Networks

Historic Vulnerabilities

- Older networks have been the subject of practical and theoretical attacks
- Examples include:
  - Ability to man in the middle
  - No perfect forward secrecy
  - No encryption on the back-end
- LTE Advanced addresses previous attacks

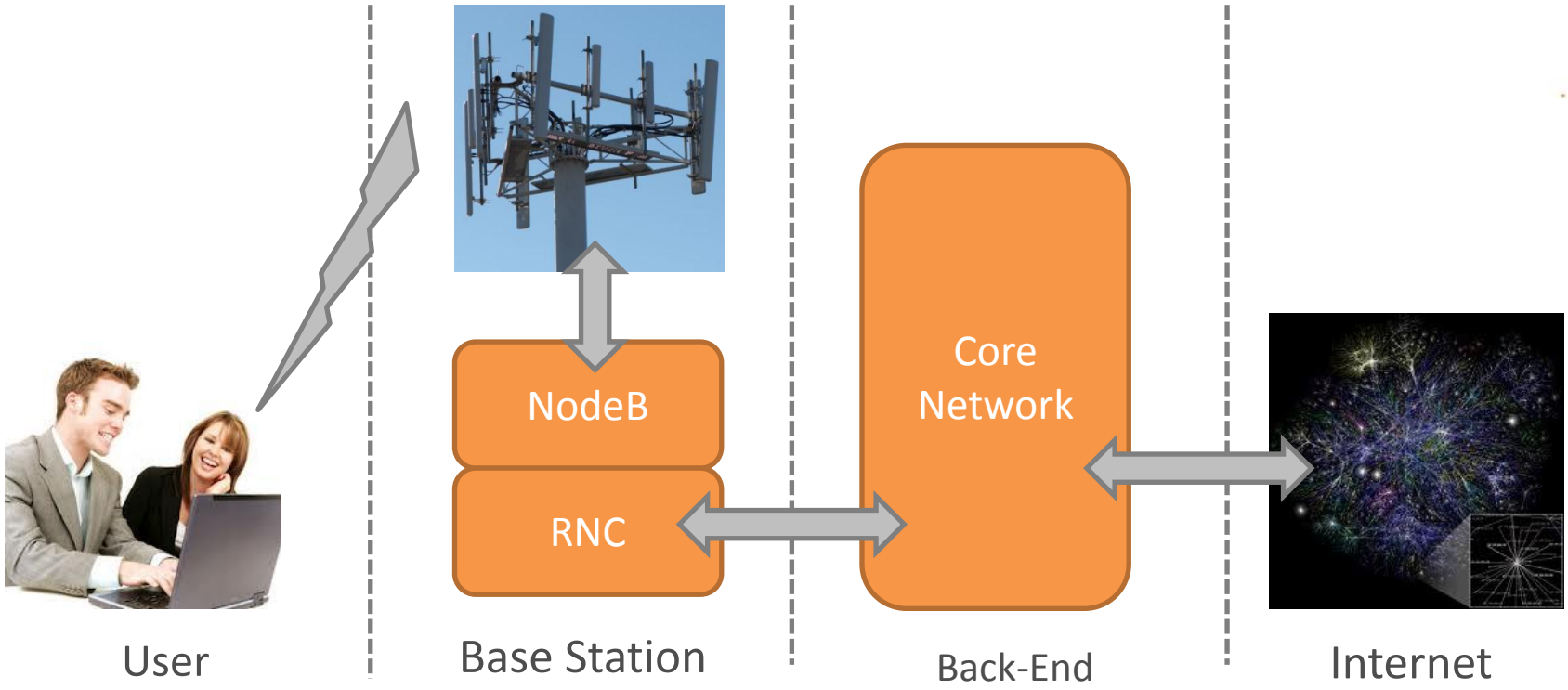
Mobile Networks

Why is LTE Important?

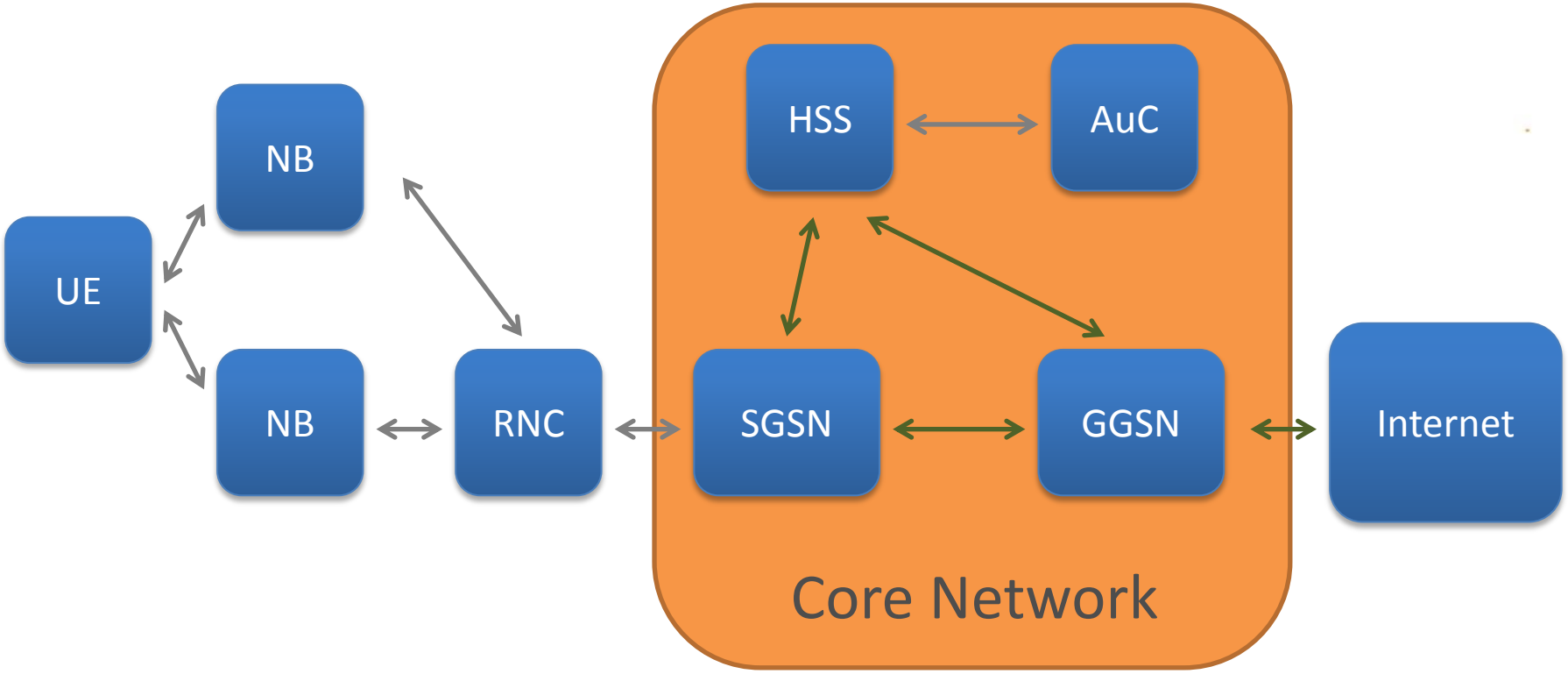
- We have lived with 3G for a long time
- 4G provides high speed mobile data services for customers
- High level of scalability on the back-end for operators

Technical Details

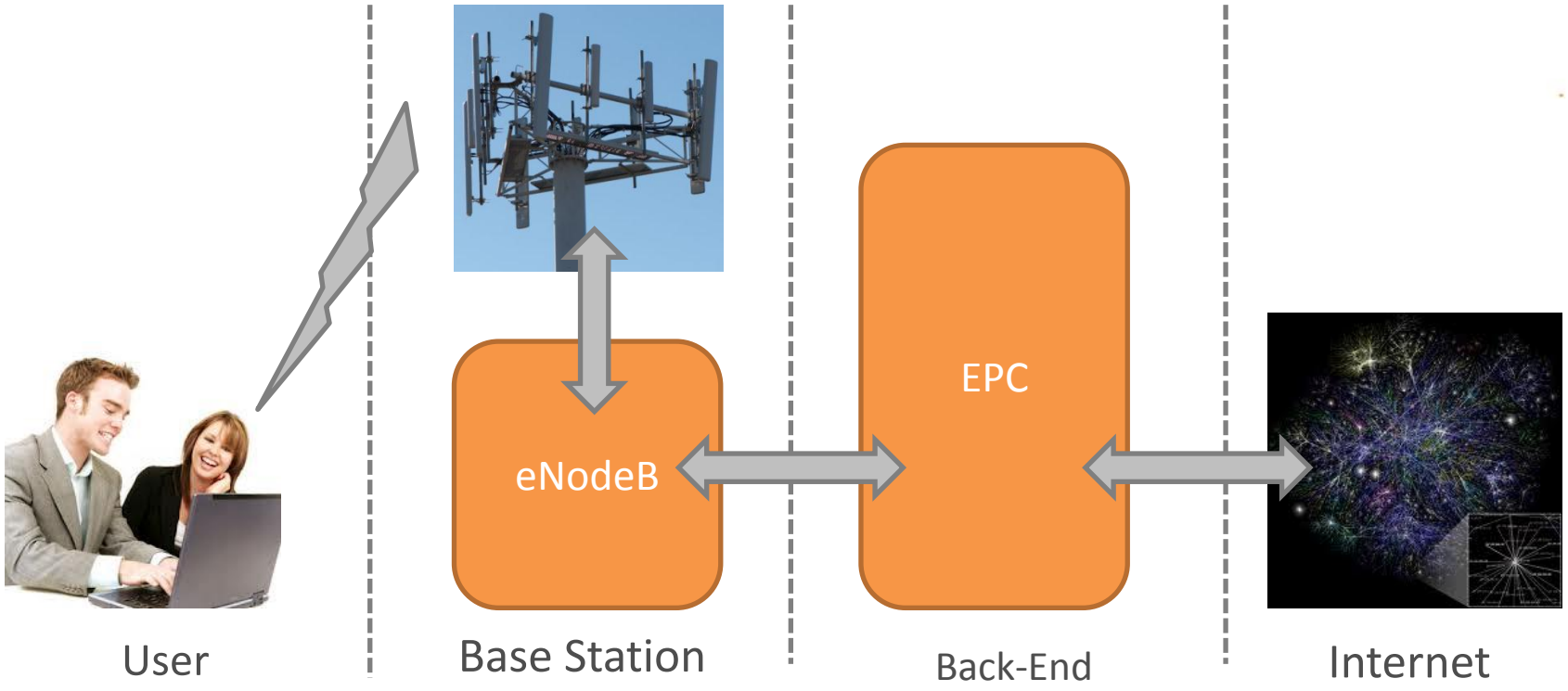
Conceptual View 3G



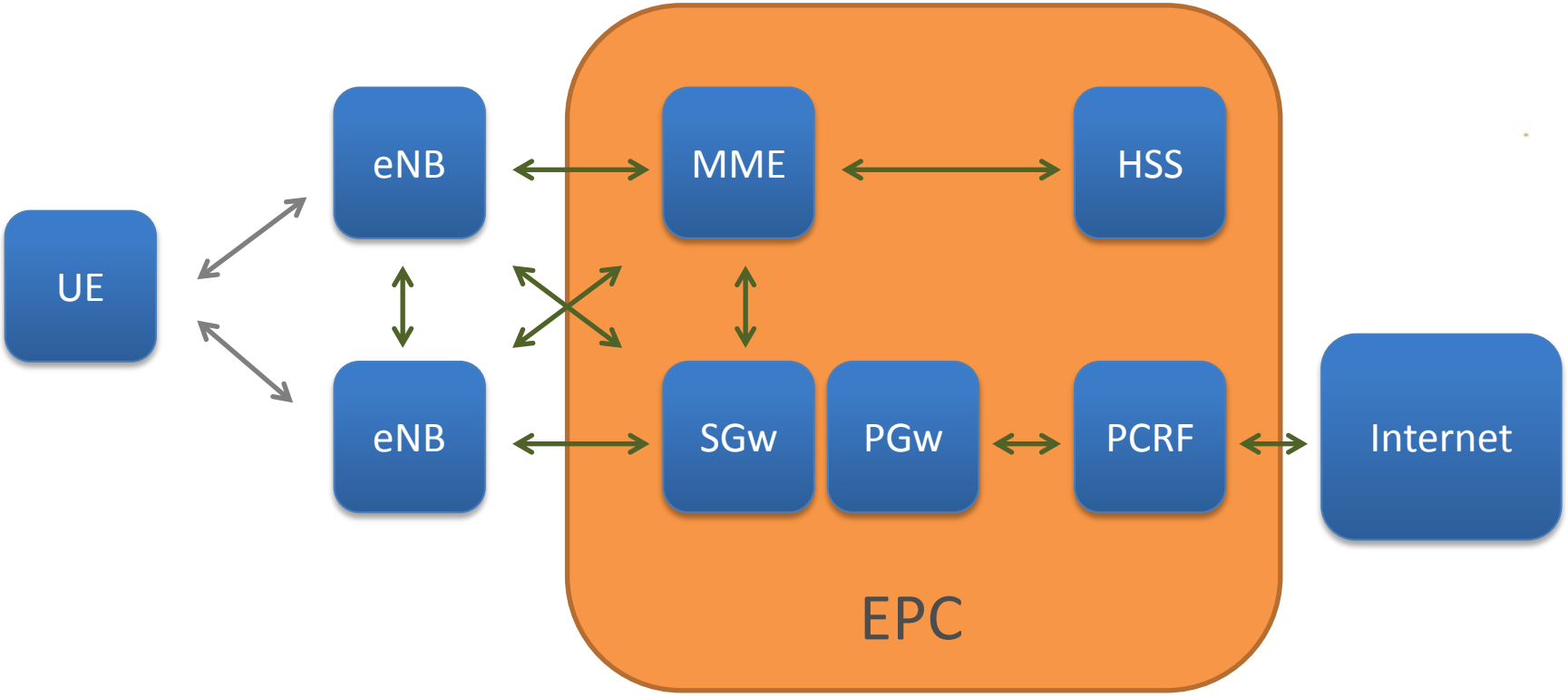
Network Overview 3G



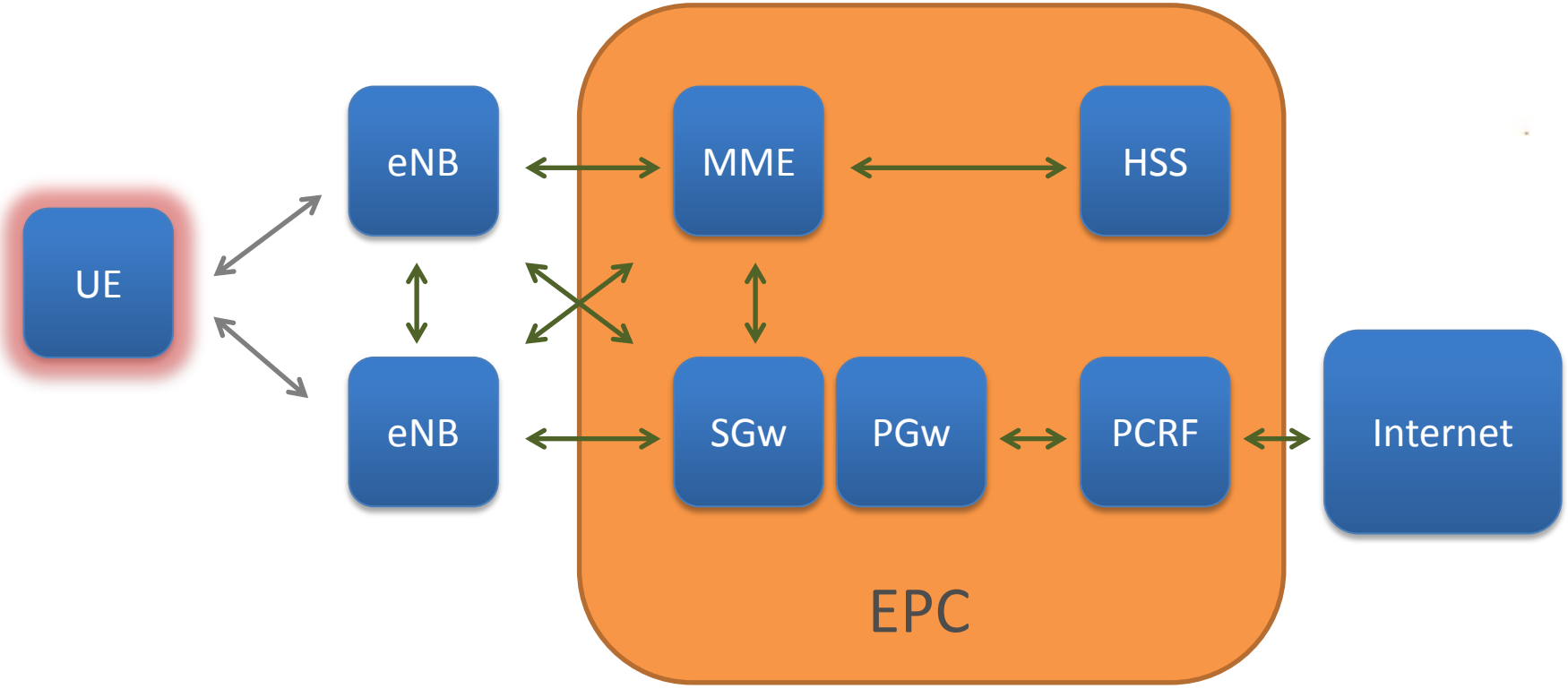
Conceptual View 4G



Network Overview 4G



The Components

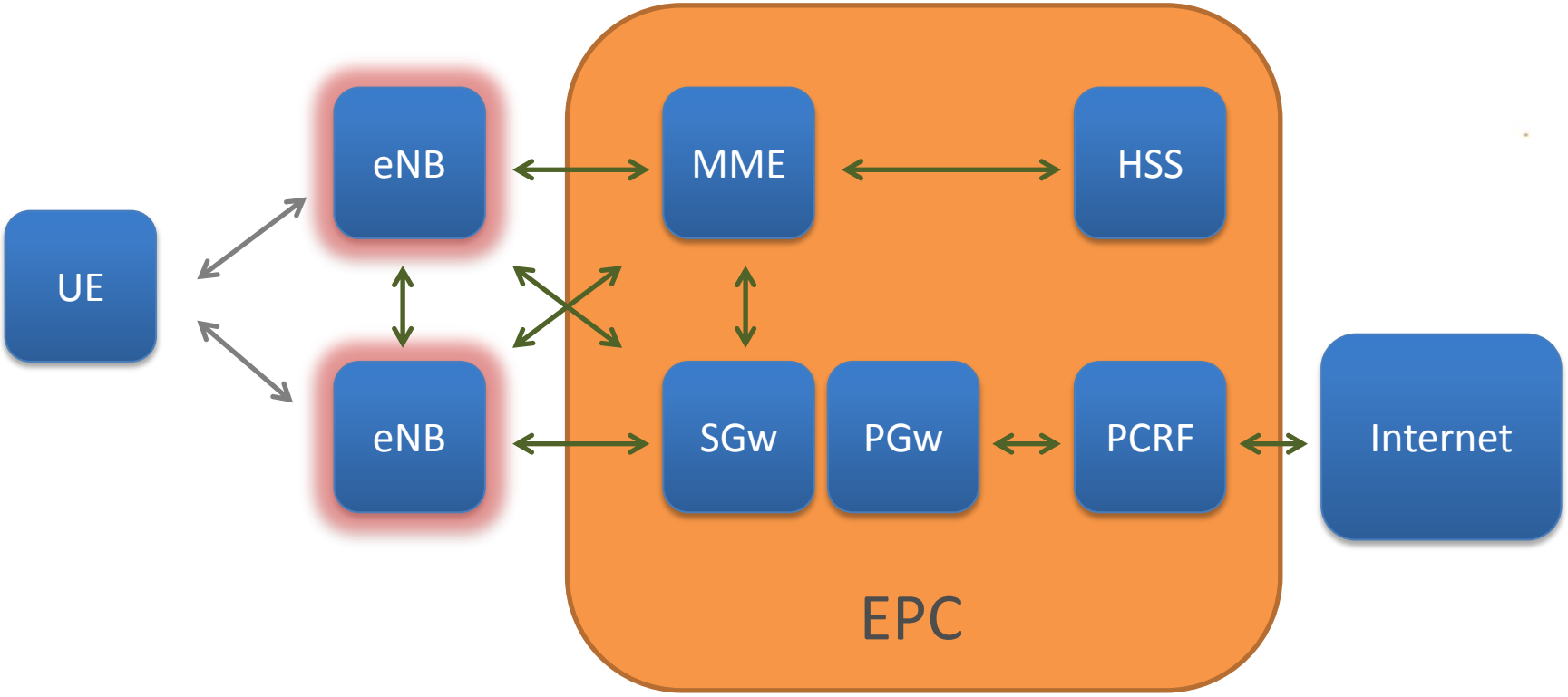


The Components

User Equipment (UE)

- What the customer uses to connect
- Mainly dongles and hubs at present
- Smartphones and tablets will follow (already lots in US)

The Components

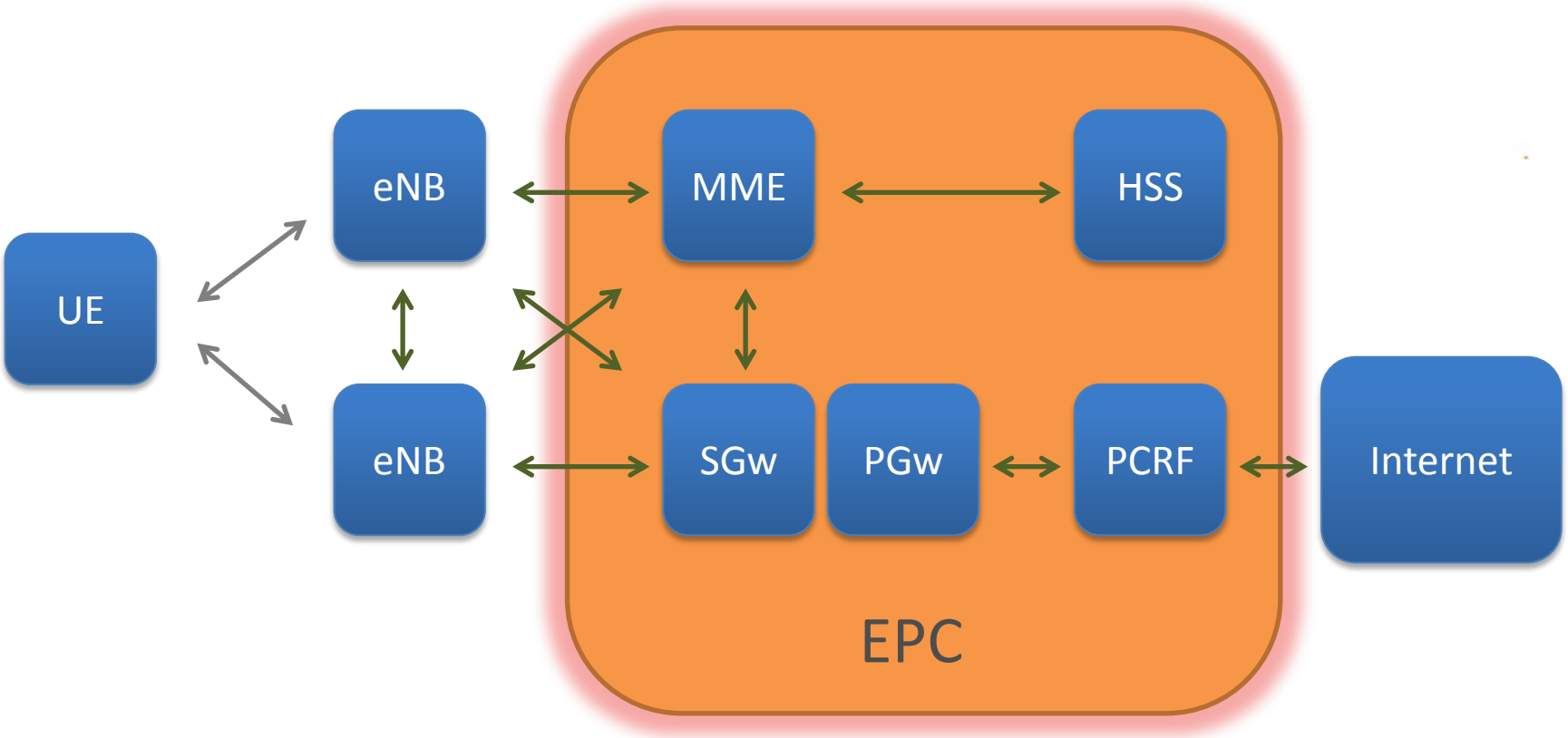


The Components

evolved Node B (eNB)

- The bridge between wired and wireless networks
- Forwards signalling traffic to the MME
- Passes data traffic to the PDN/Serving Gateway

The Components

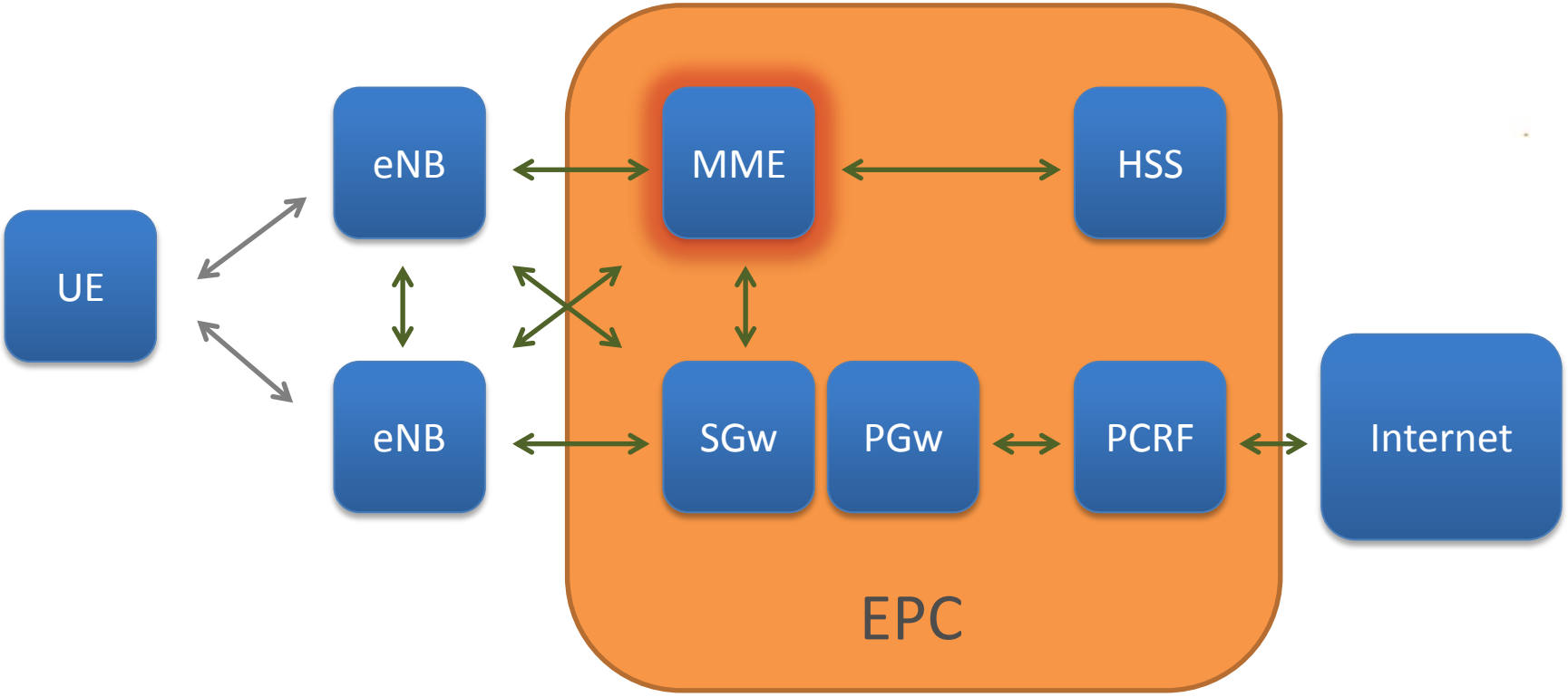


The Components

Evolved Packet Core (EPC)

- The back-end core network
- Manages access to data services
- Uses IP for **all** communications
- Divided into several components

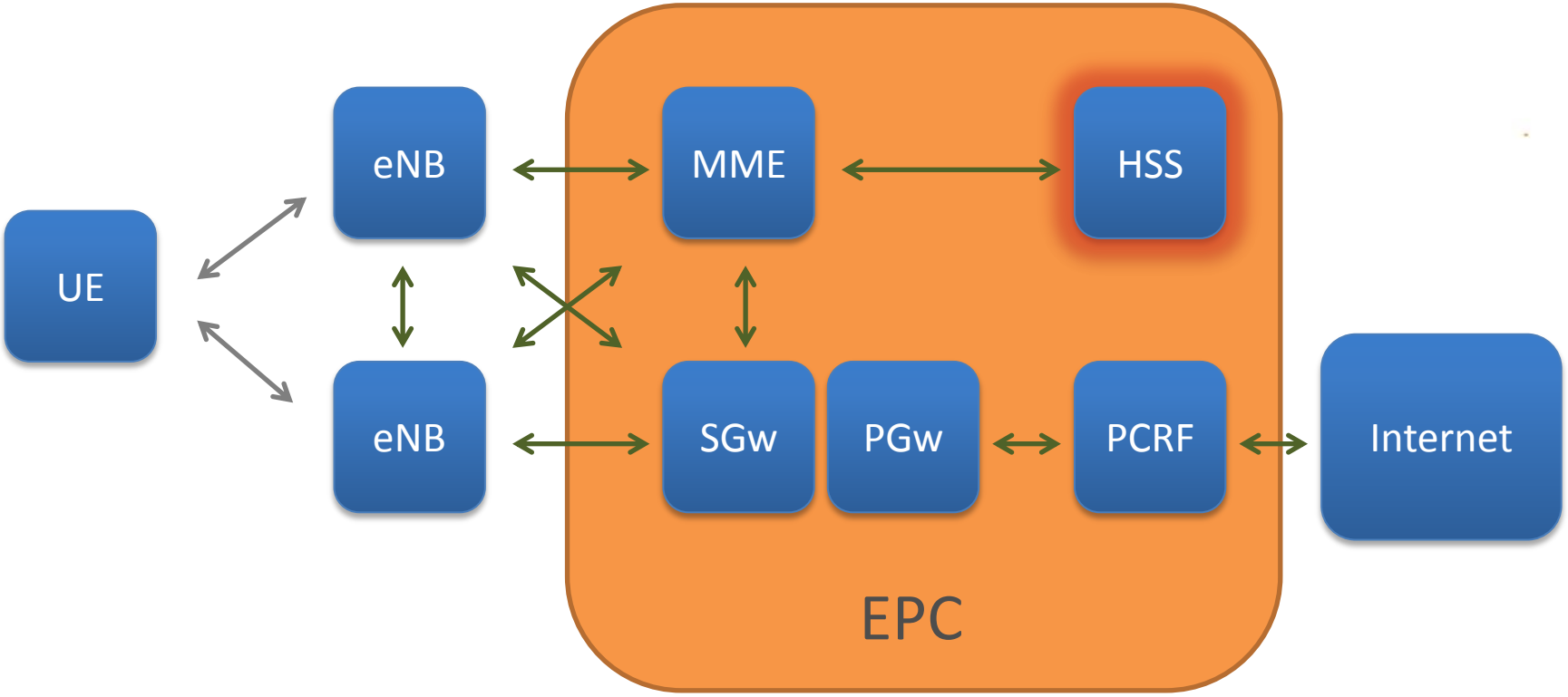
The Components



Mobile Management Entity (MME)

- Termination point for UE Signalling
- Handles authentication events
- Key component in back-end communications

The Components

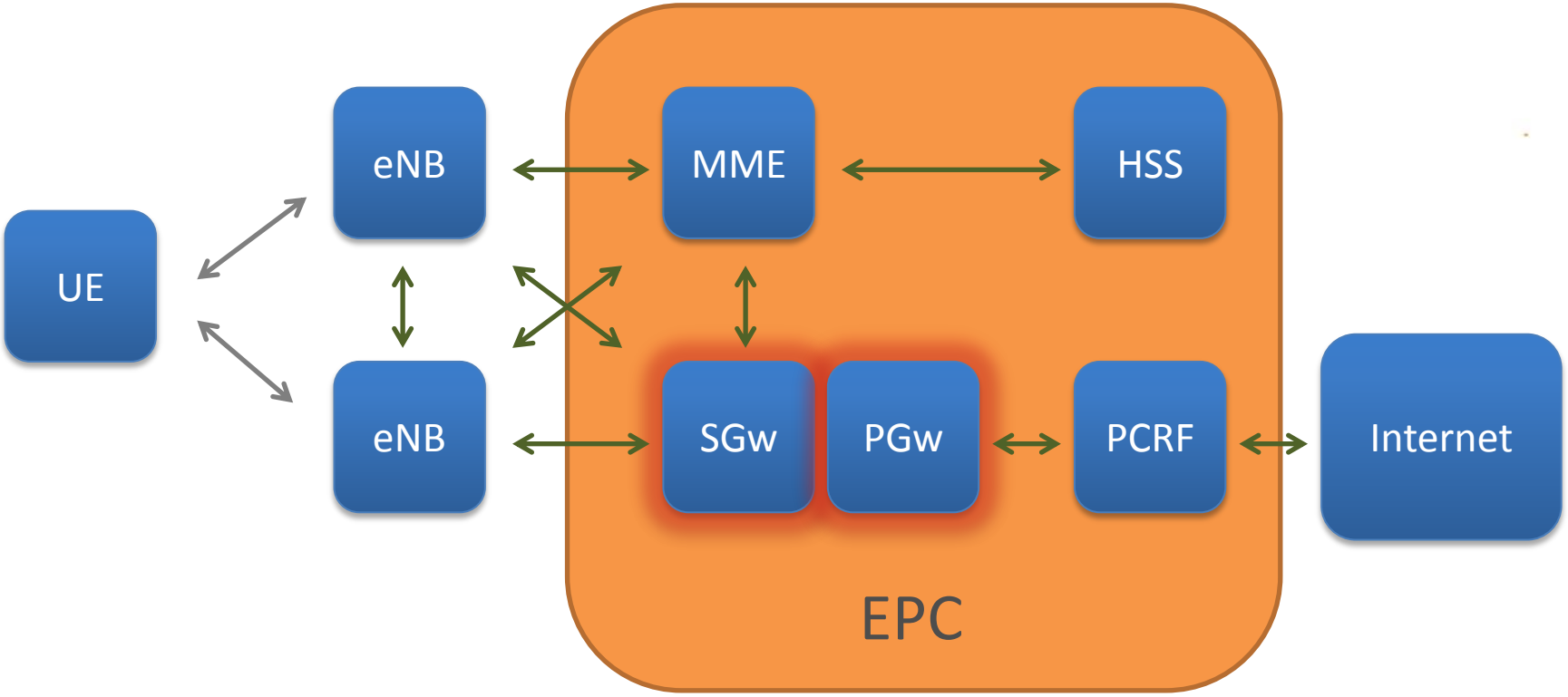


The Components

Home Subscriber Service (HSS)

- Contains a user's subscription data (profile)
- Typically includes the Authentication Centre (AuC)
- Where key material is stored

The Components

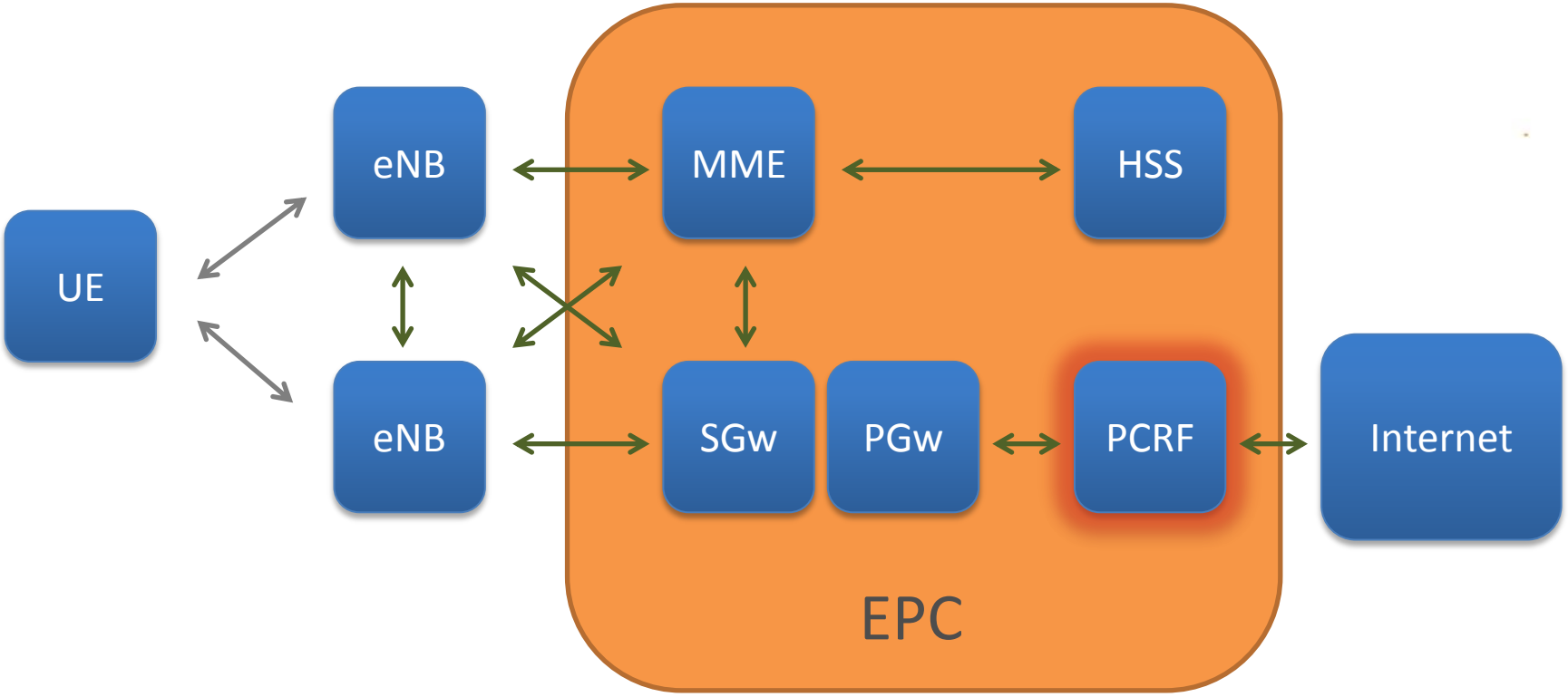


The Components

PDN and Serving Gateways (PGw and SGw)

- Handles data traffic from UE
- Can be consolidated into a single device
- Responsible for traffic routing within the back-end
- Implements important filtering controls

The Components

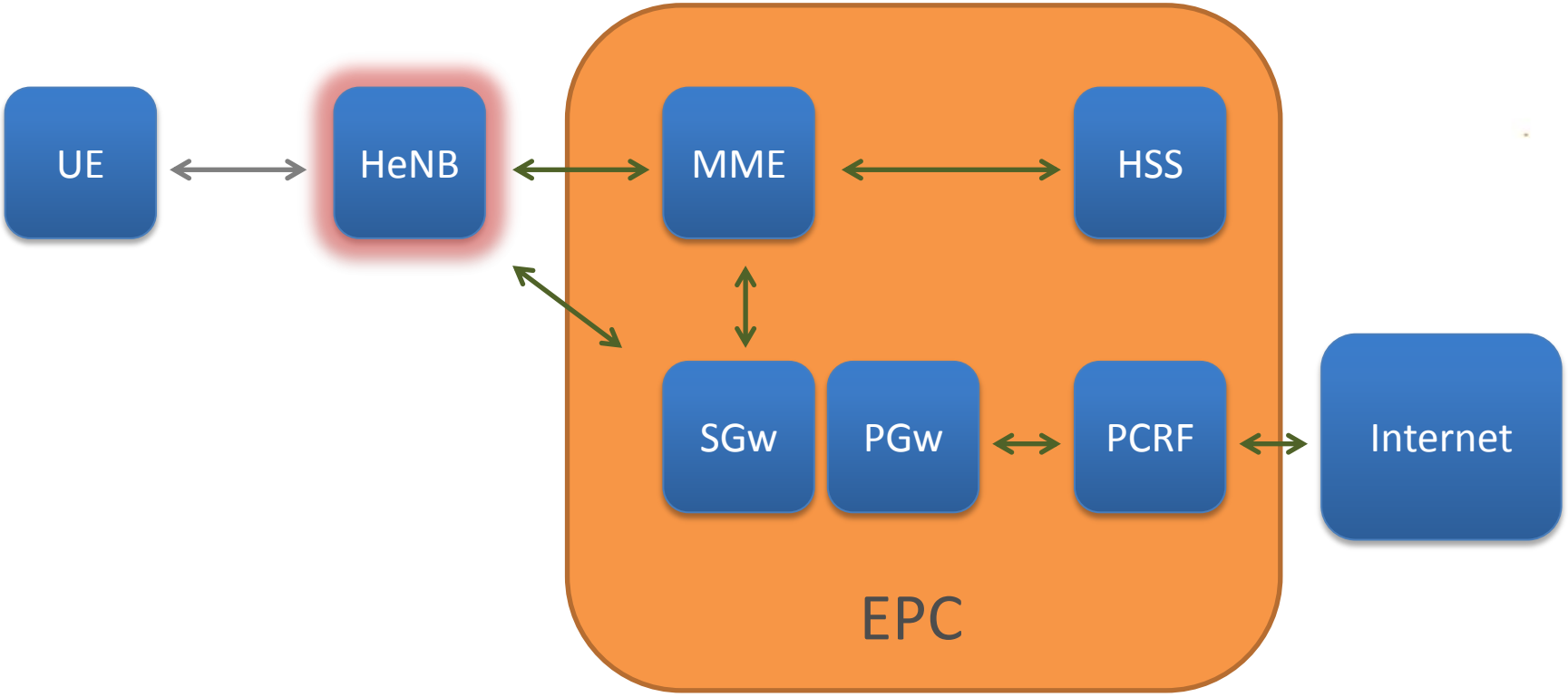


The Components

Policy Charging and Rules Function (PCRF)

- Does what it says on the tin
- Integrated into the network core
- Allows operator to perform bandwidth shaping

The Components



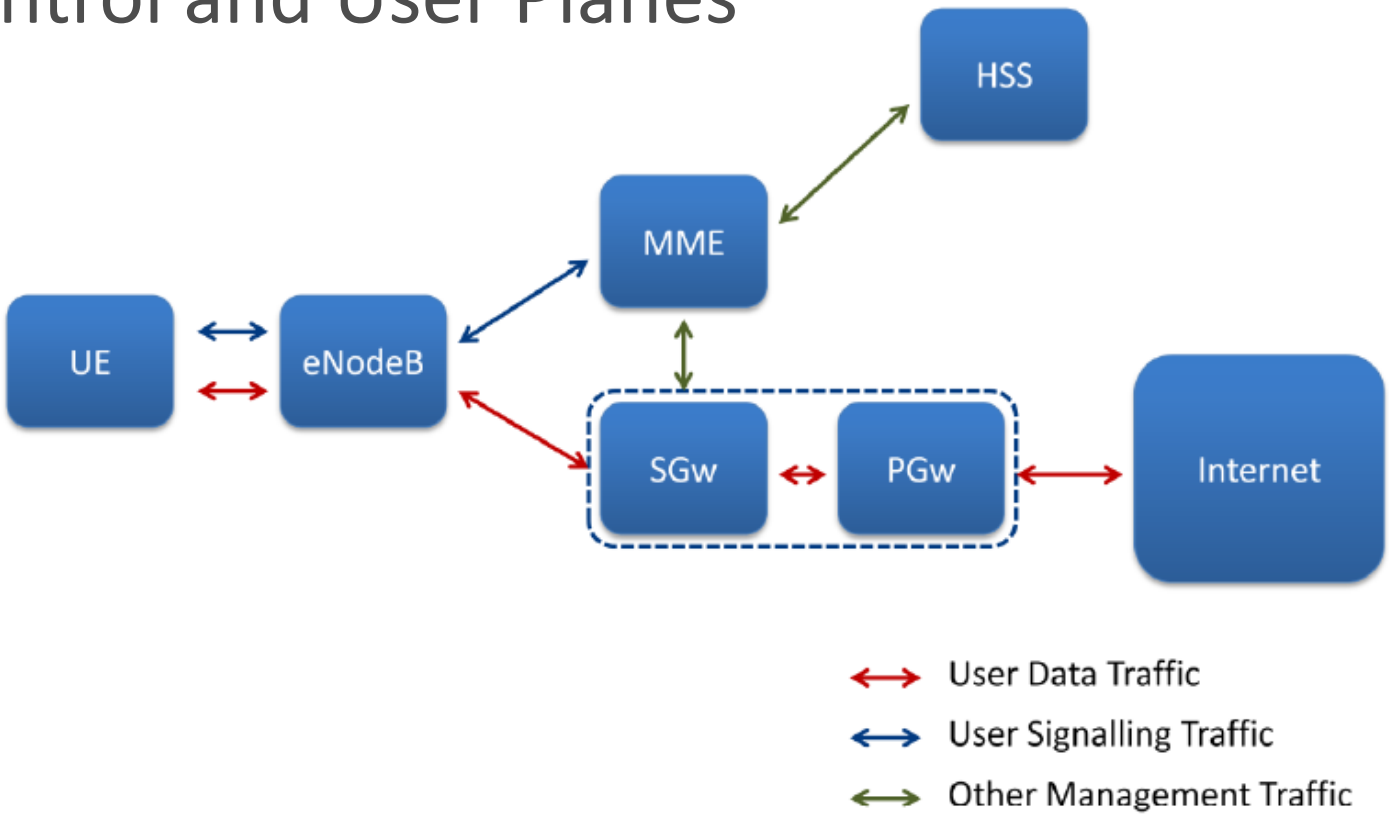
The Components

Home eNB (HeNB)

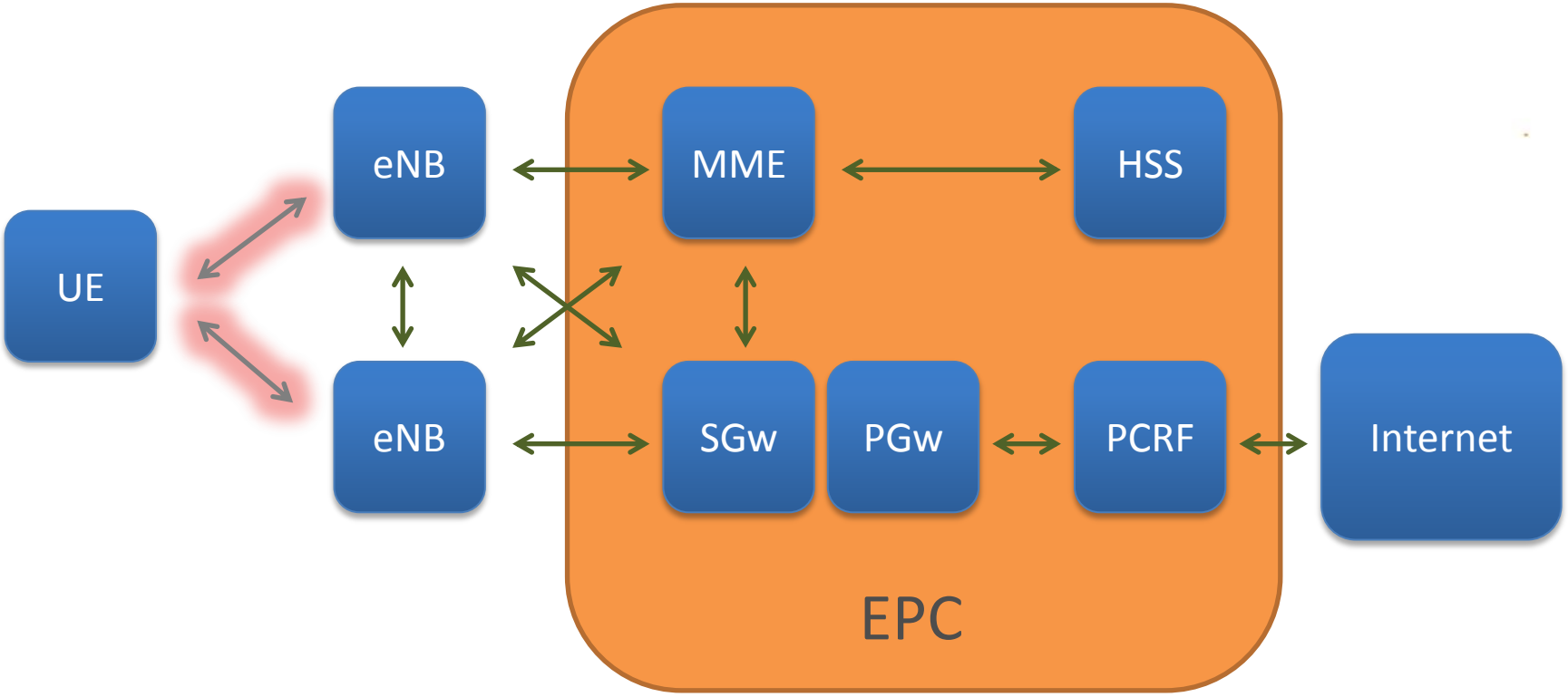
- The “FemtoCell” of LTE
- An eNodeB within your home
- Talks to the MME and PDN/Serving Gateway
- Expected to arrive much later in 4G rollout

Network Overview

Control and User Planes



The Protocols

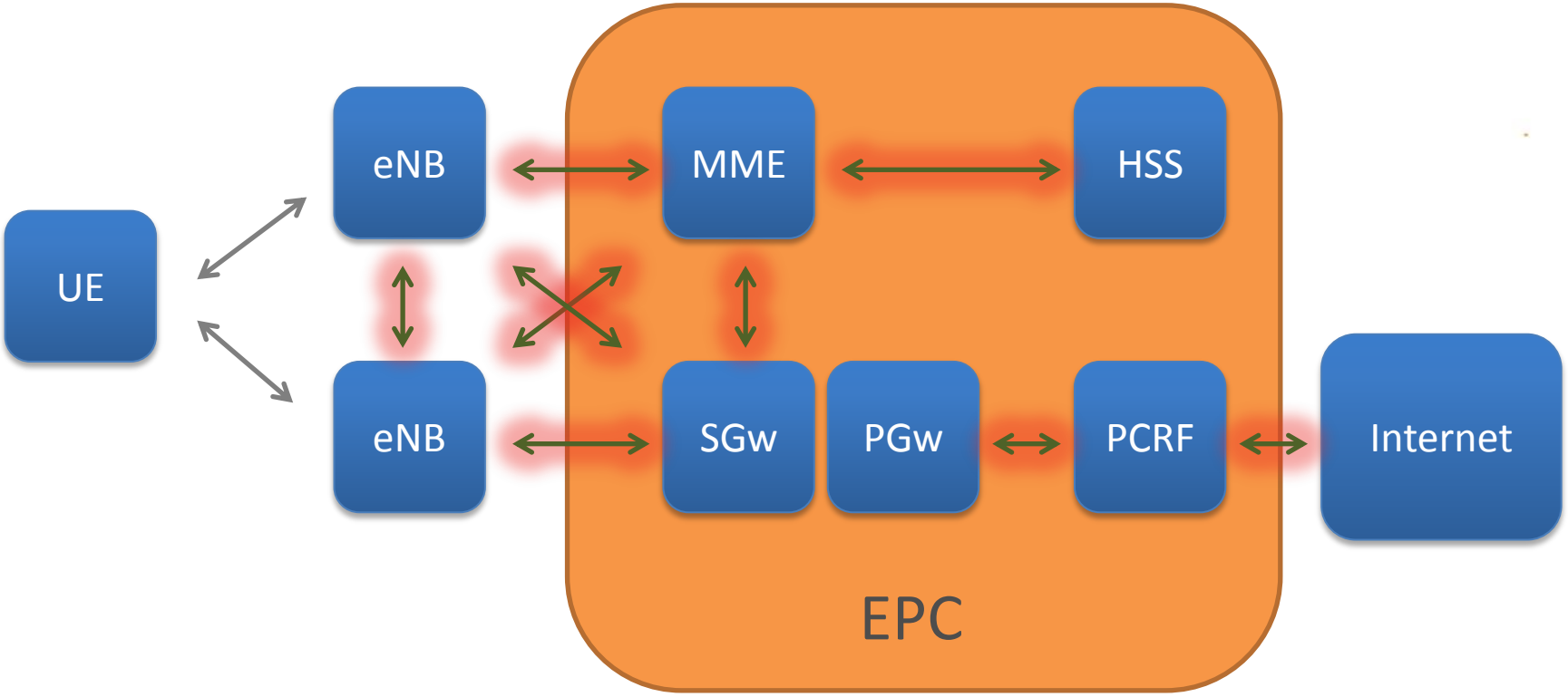


The Protocols

Radio Protocols (RRC, PDCP, RLC)

- These all terminate at the eNodeB
- RRC is only used on the control plane
- Wireless user and control data is encrypted (some exceptions)
- Signalling data can also be encrypted end-to-end

The Protocols

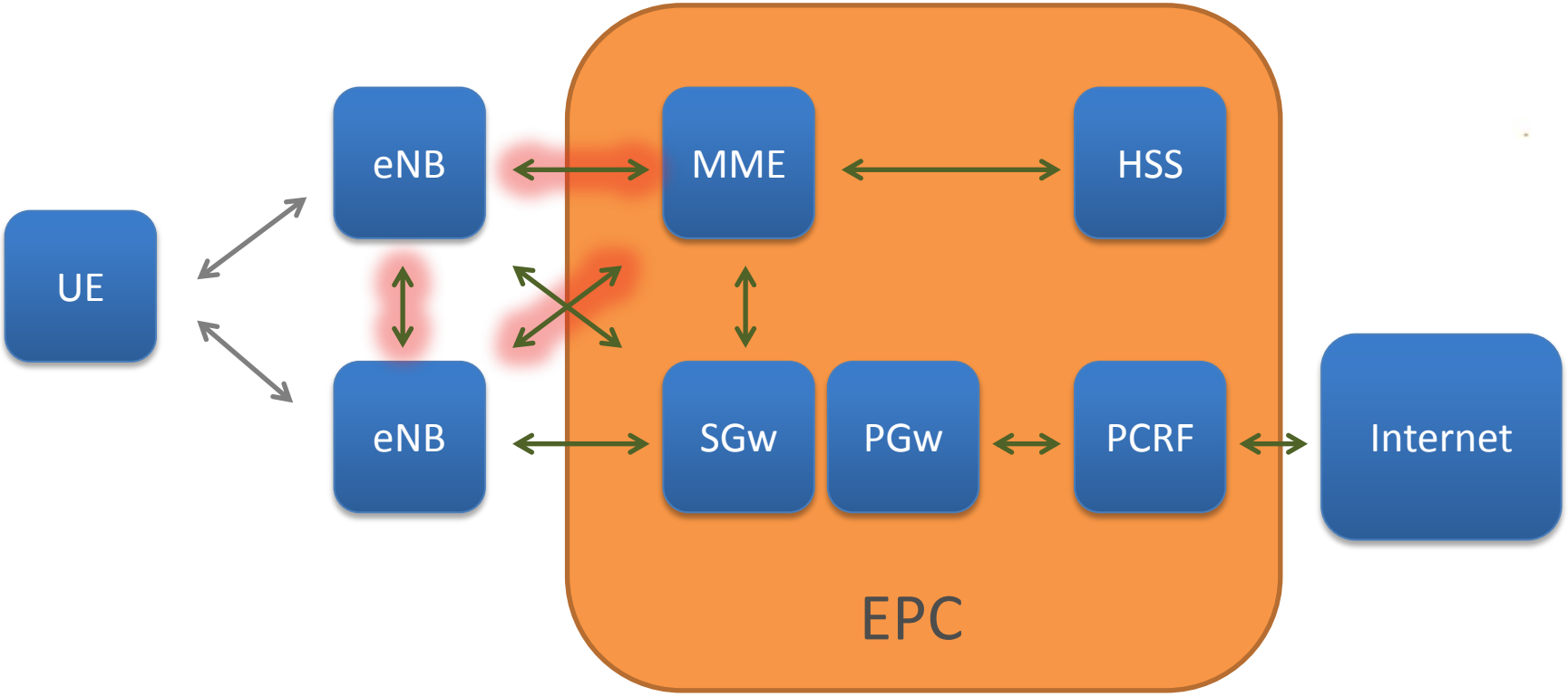


The Protocols

Internet Protocol (IP)

- Used by all back-end comms
- All user data uses it
- Supports both IPv4 and IPv6
- Important to get routing and filtering correct
- Common UDP and TCP services in use

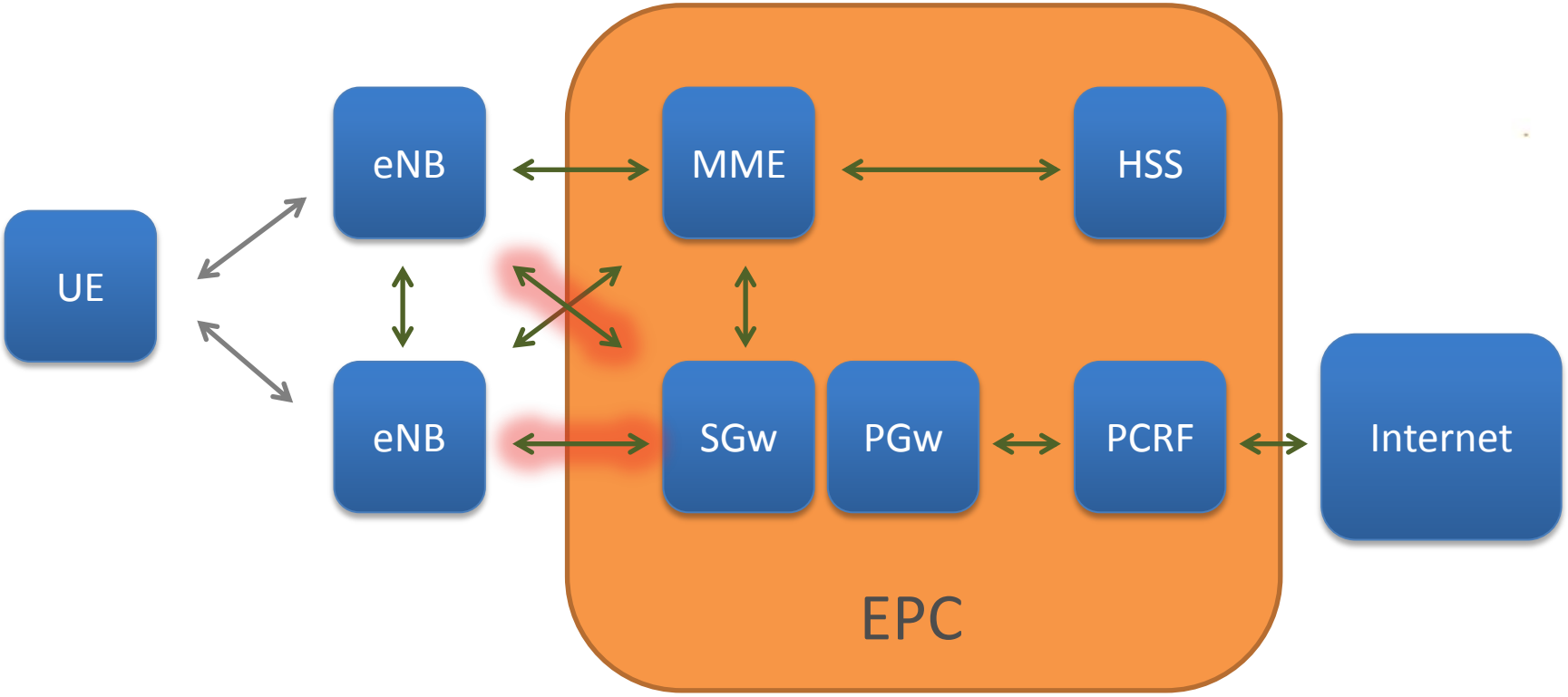
The Protocols



The Protocols - SCTP

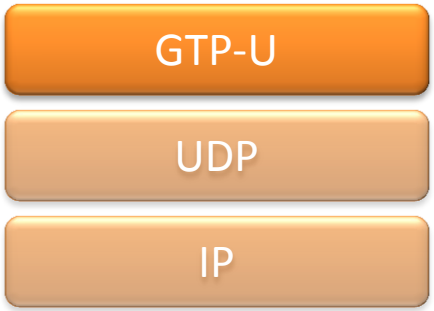
- Another protocol on top of IP
- Robust session handling
- Bi-directional sessions
- Sequence numbers very important

The Protocols

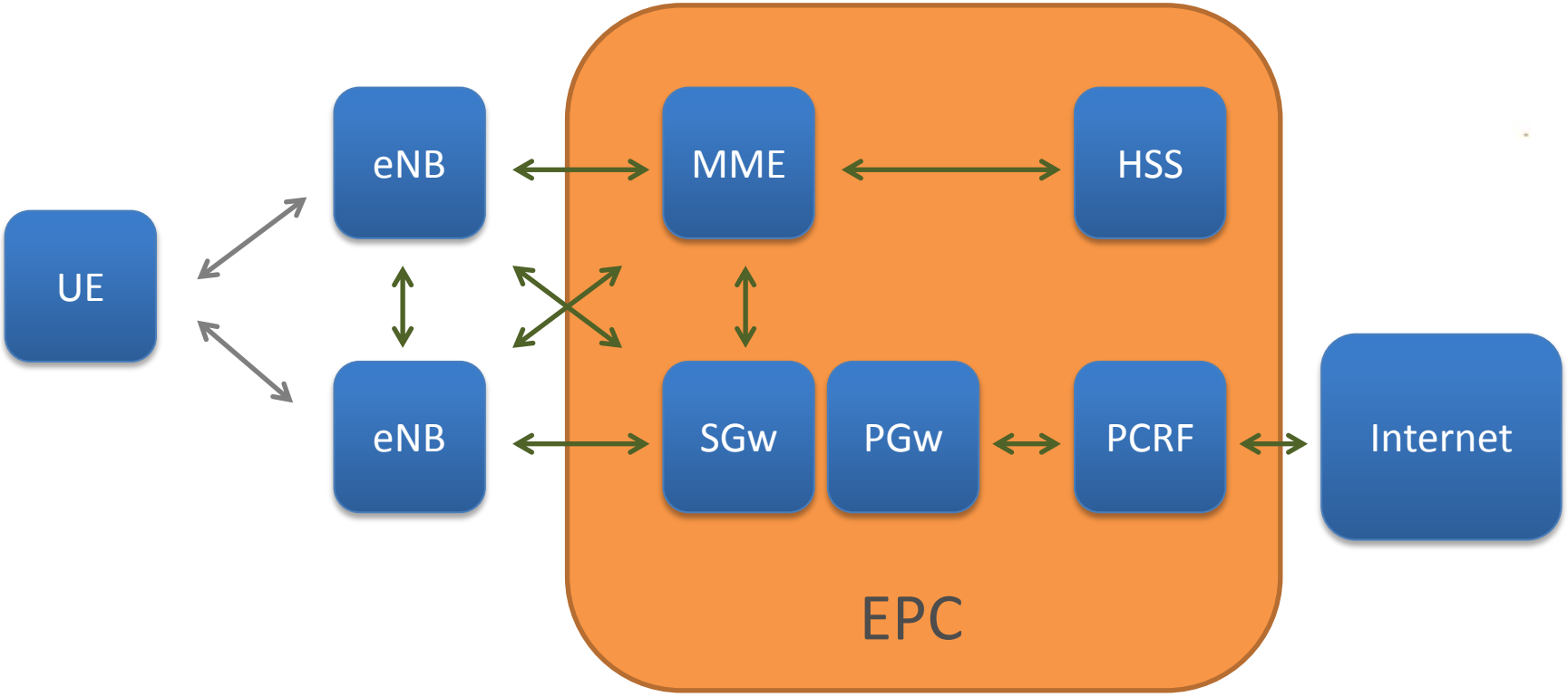


The Protocols – GTP-U

- Runs on top of UDP and IP
- One of two variants of GTP used in LTE
- This transports user IP data
- Pair of sessions are used identified by Tunnel-ID

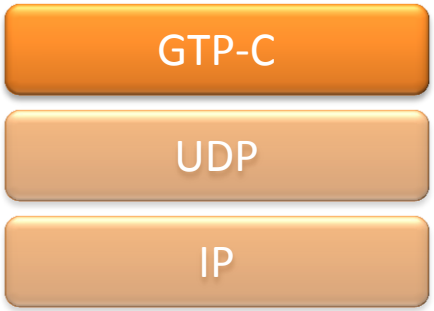


The Protocols

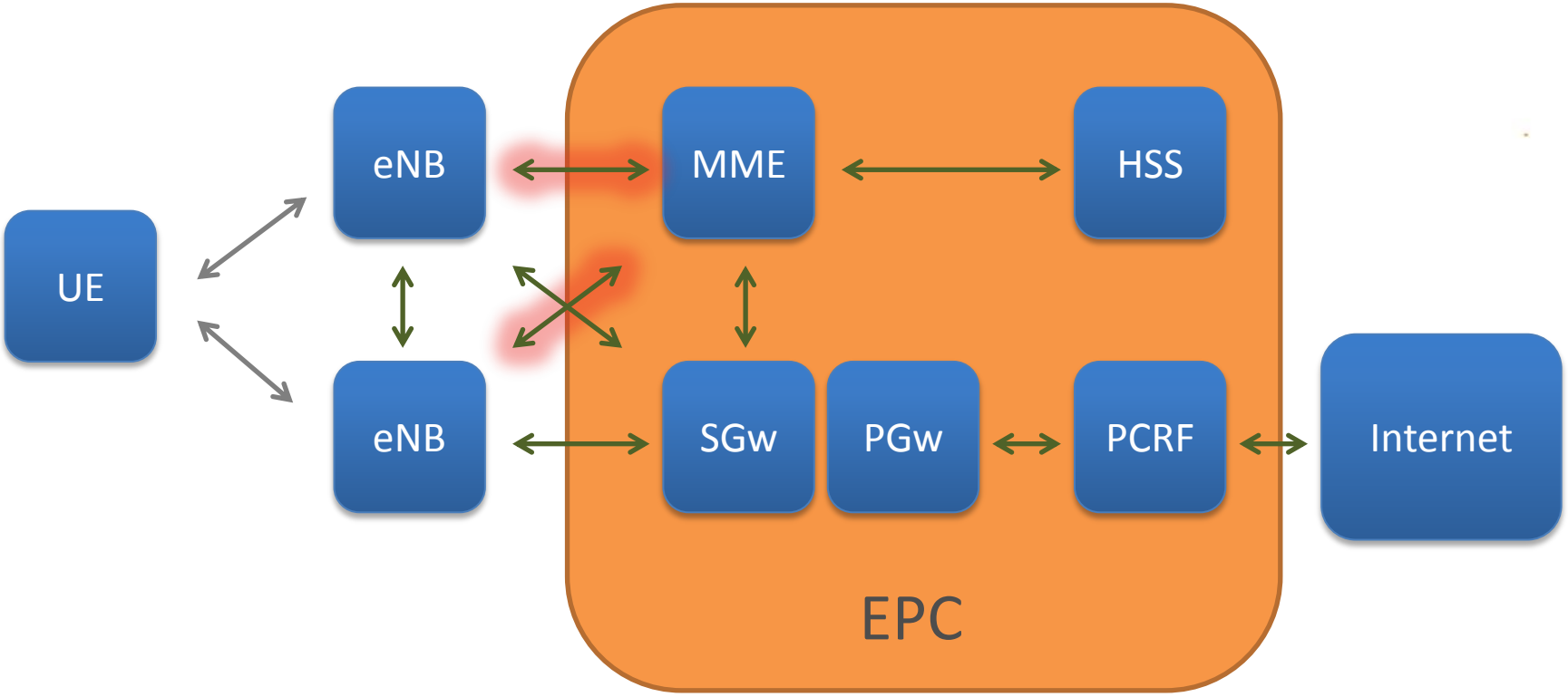


The Protocols – GTP-C

- Runs on top of UDP and IP
- The other variant of GTP used in LTE
- Used for back-end data
- Should not be used by the MME in pure 4G



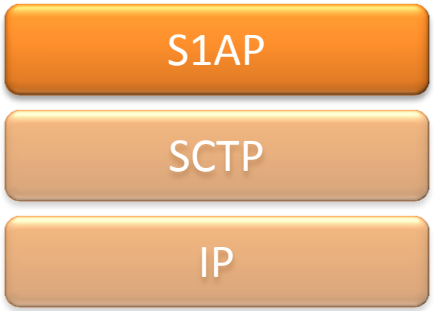
The Protocols



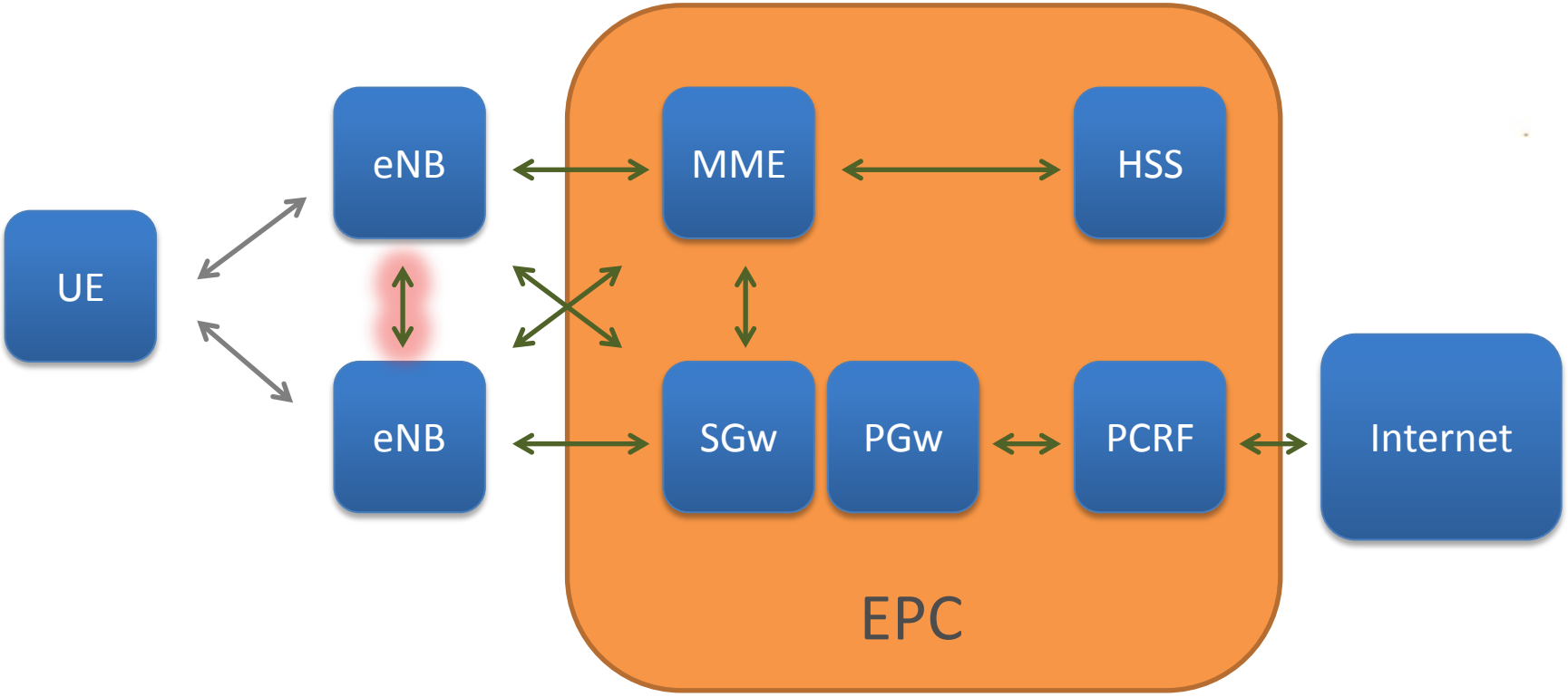
The Protocols

S1AP

- Runs on top of SCTP and IP
- An ASN.1 protocol
- Transports UE signalling
- UE sessions distinguished by a pair of IDs



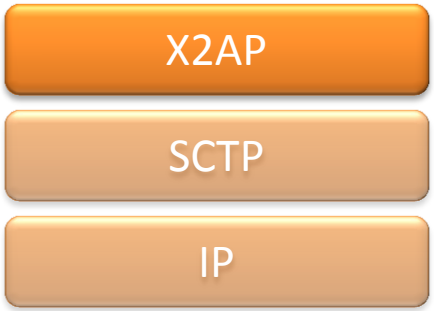
The Protocols



The Protocols

X2AP

- Very similar to S1AP
- Used between eNodeBs for signalling and handovers
- Runs over of SCTP and IP and is also an ASN.1 protocol



Potential Attacks

Targets for Testing

What Attacks are Possible

- Wireless attacks and the baseband
- Attacking the EPC from UE
- Attacking other UE
- Plugging into the Back-end
- Physical attacks (HeNB)

Targets for Testing

Wireless Attacks and the Baseband

- A DIY kit for attacking wireless protocols is now closer (USRP based)
- Best chance is using commercial kit to get a head-start
- Not the easiest thing to attack

Targets for Testing

Attacking the EPC from UE

- Everything in the back-end is IP
- You pay someone to give you IP access to the environment ☺
- Easiest place to start

Targets for Testing

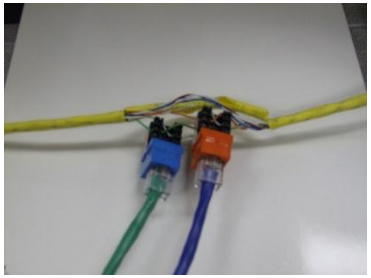
Attacking other UE

- Other wirelessly connected devices are close
- May be less protection if seen as a local network
- The gateway may enforce segregation between UE

Targets for Testing

Wired network attacks

- eNodeBs will be in public locations
- They need visibility of components in the EPC
- Very easy to communicate with an IP network
- Everything is potentially in scope



Targets for Testing

Physical Attacks (eNB)

- Plugging into management interfaces is most likely attack, except …
- A Home eNodeB is a different story
- Hopefully we have learned from the Vodafone Femto-Cell Attack

What you can Test

Tests to Run

As a Wirelessly Connected User

- Visibility of the back-end from UE
- Visibility of other UEs
- Testing controls enforced by Gateway
  - Spoofed source addresses
  - GTP Encapsulation (Control and User)

Tests to Run

From the Back-End

- Ability to attack MME (signalling)
- Robustness of stacks (eg SCTP)
  - Fuzzing
  - Sequence number generation
- Testing management interfaces
  - Web consoles
  - SSH
  - Proprietary protocols

Tests to Run

Challenges

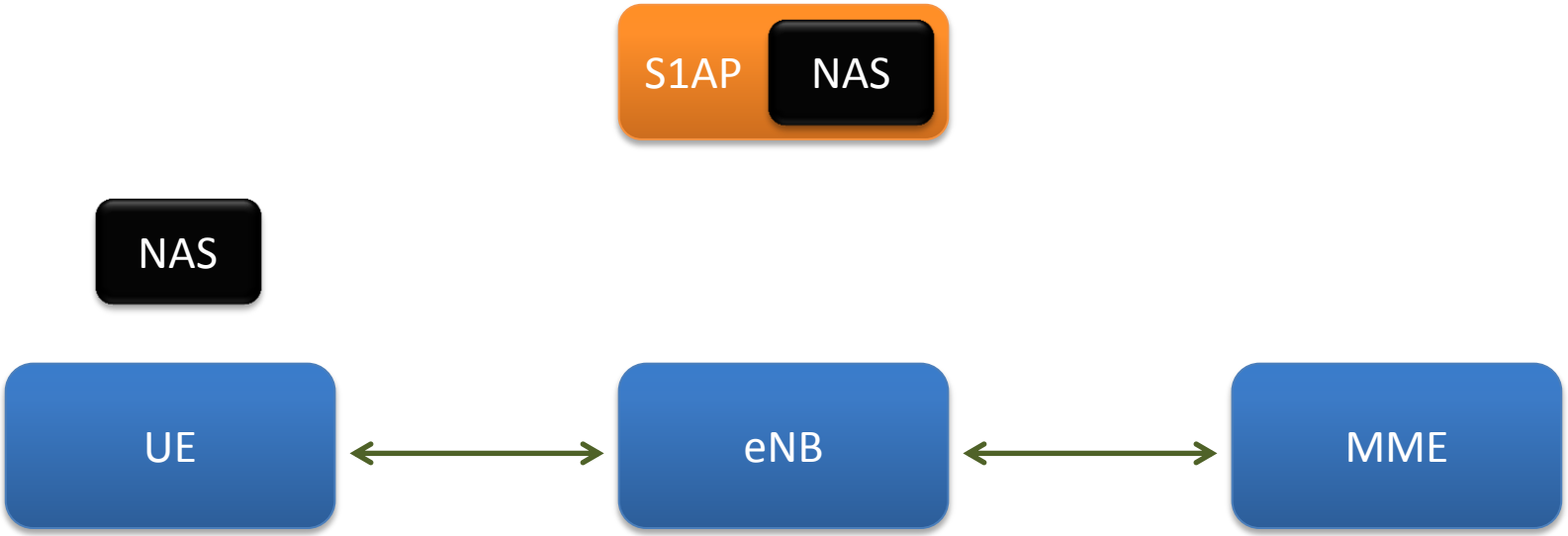
- Spoofing UE authentication is difficult
- Messing with radio layers is hard
- ASN.1 protocols are a pain
- Injecting into SCTP is tough
- Easy to break back-end communications

Tests to Run

S1AP Protocol

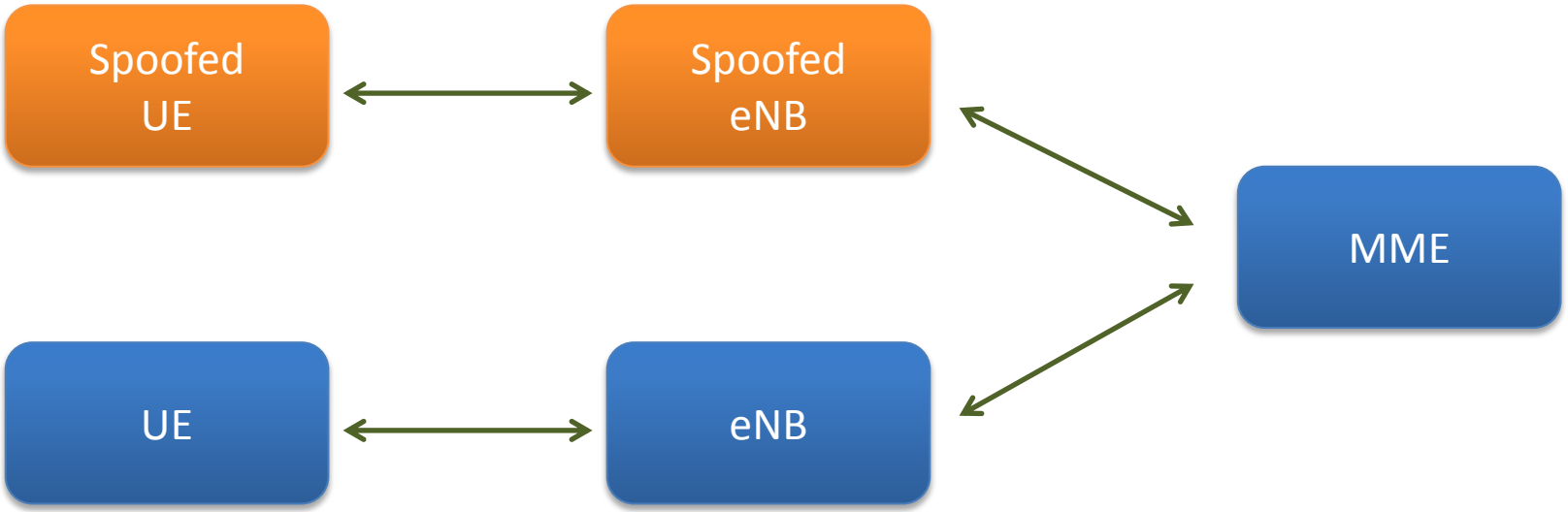
- By default no authentication to the service
- Contains eNodeB data and UE Signalling
- UE Signalling can make use of encryption and integrity checking
- If no UE encryption is used attacks against connected handsets become possible

S1AP and Signalling



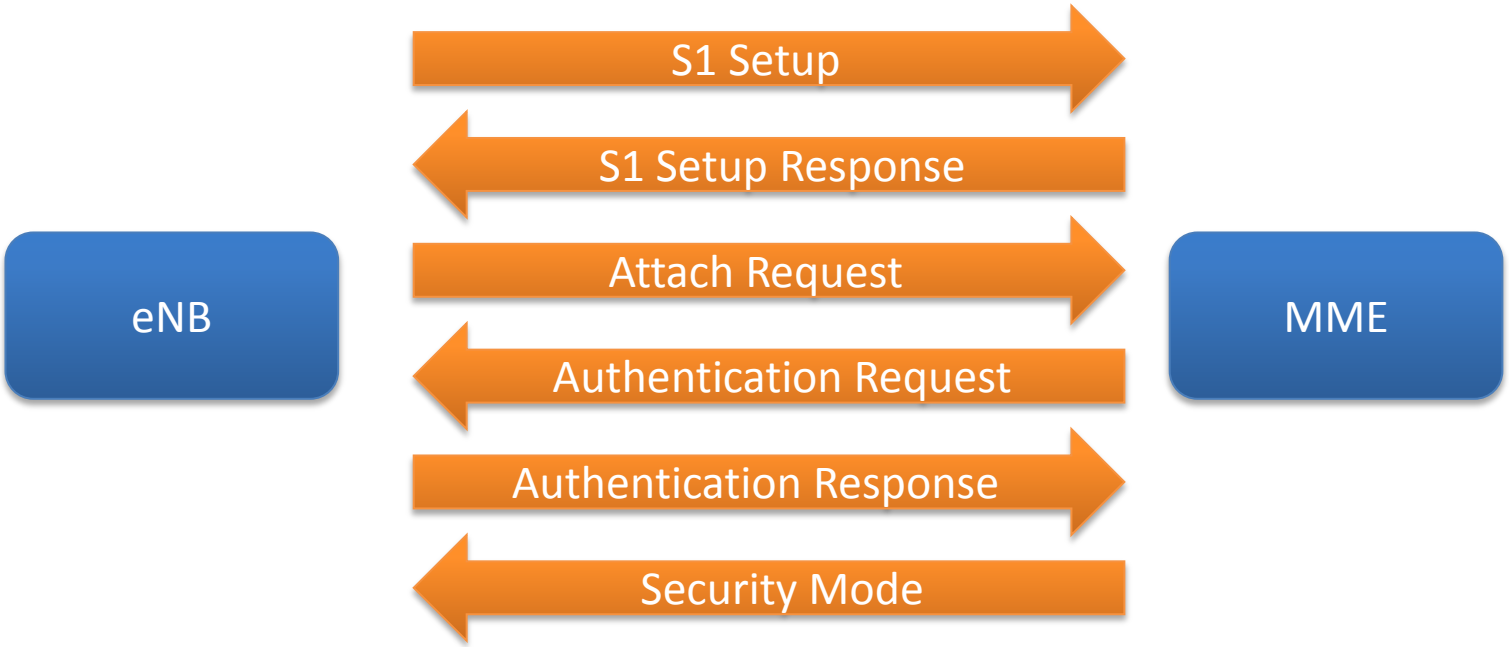
Tests to Run

S1AP and Signalling



Tests to Run

S1AP and Signalling

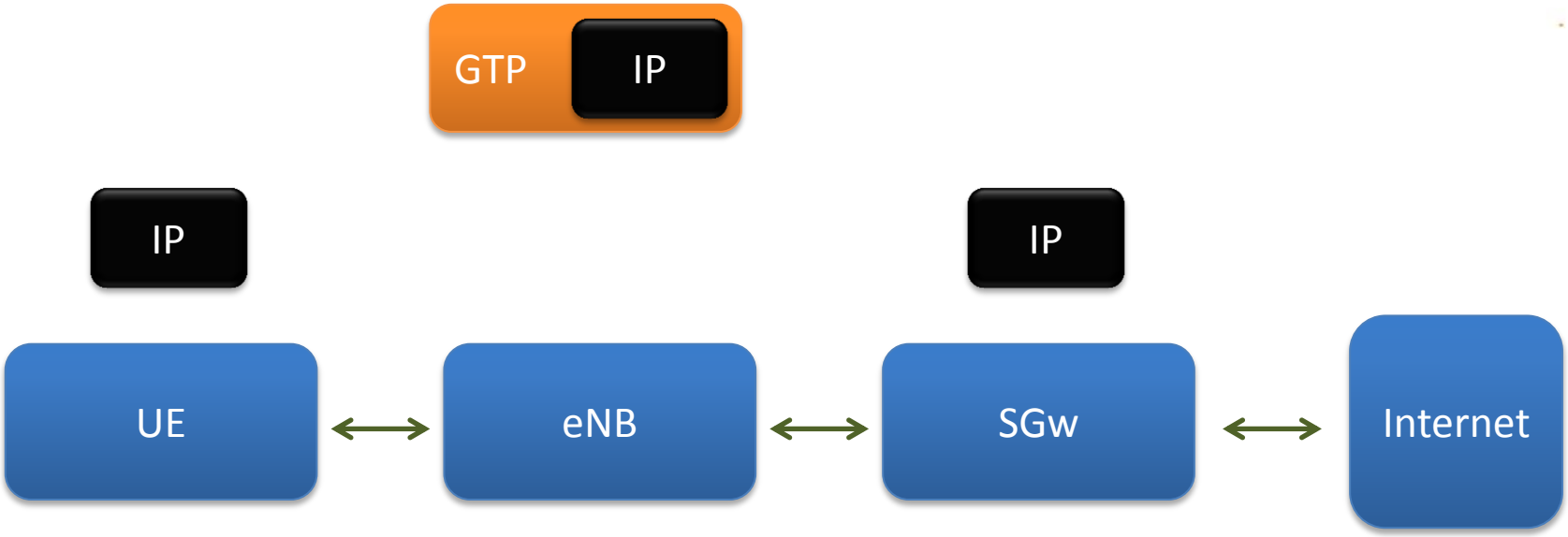


Tests to Run

GTP Protocol

- Gateway can handle multiple encapsulations
- It uses UDP so easy to have fun with
- The gateway needs to enforce a number of controls that stop attacks

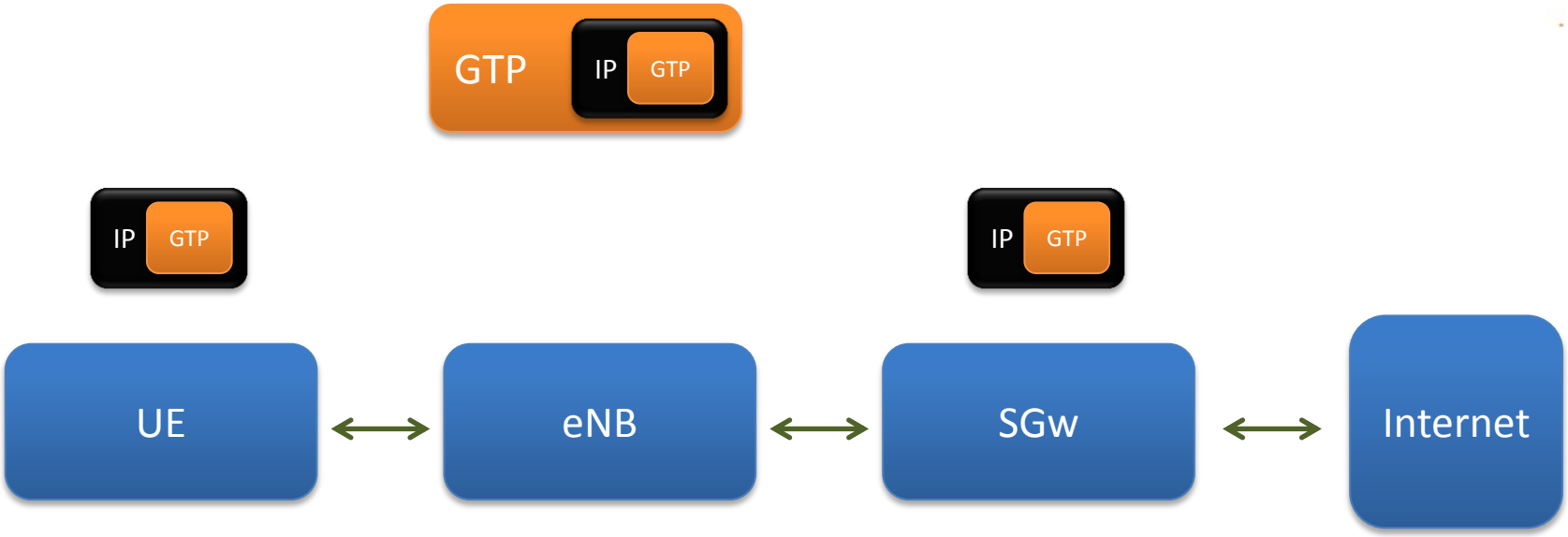
GTP and User Data



Tests to Run

GTP and User Data

GTP and User Data



Tests to Run

GTP and User Data

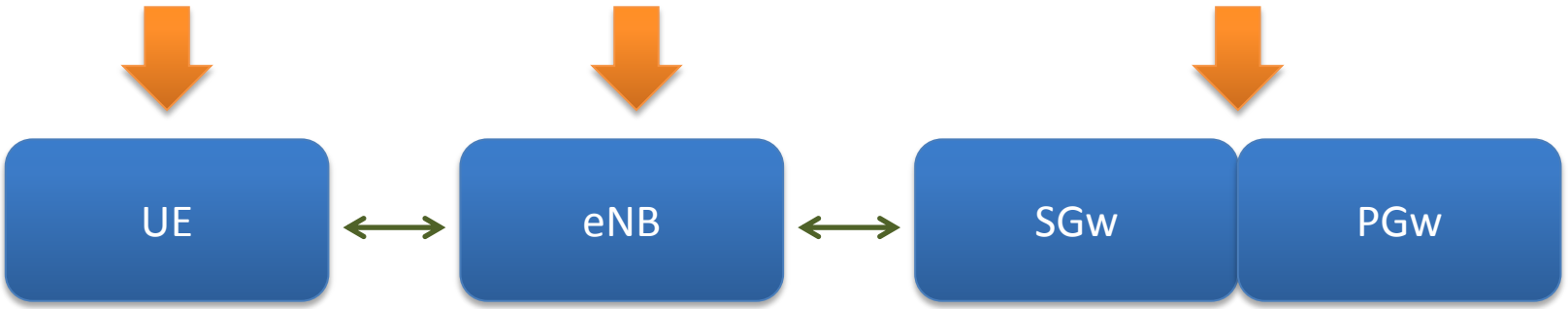
Destination IP Address (IP)

GTP Tunnel ID (GTP)

Source IP Address (GTP)

Source IP Address (IP)

Invalid IP Protocols (IP)



Tests to Run

Old Skool

- Everything you already know can be applied to testing the back-end
- Its an IP network and has routers and switches
- There are management services running

Defences

Defences

The Multi-Layered Approach

- Get the IP network design right
- Protect the IP traffic in transit
- Enforce controls in the Gateway
- Ensure UE and HeNBs are secure
- Monitoring and Response
- Testing

Defences

Unified/Consolidated Gateway

- The “Gateway” enforces some very important controls:
  - Anti-spoofing
  - Encapsulation protection
  - Device to device Routing
  - Billing and charging of users

Defences

IP Routing

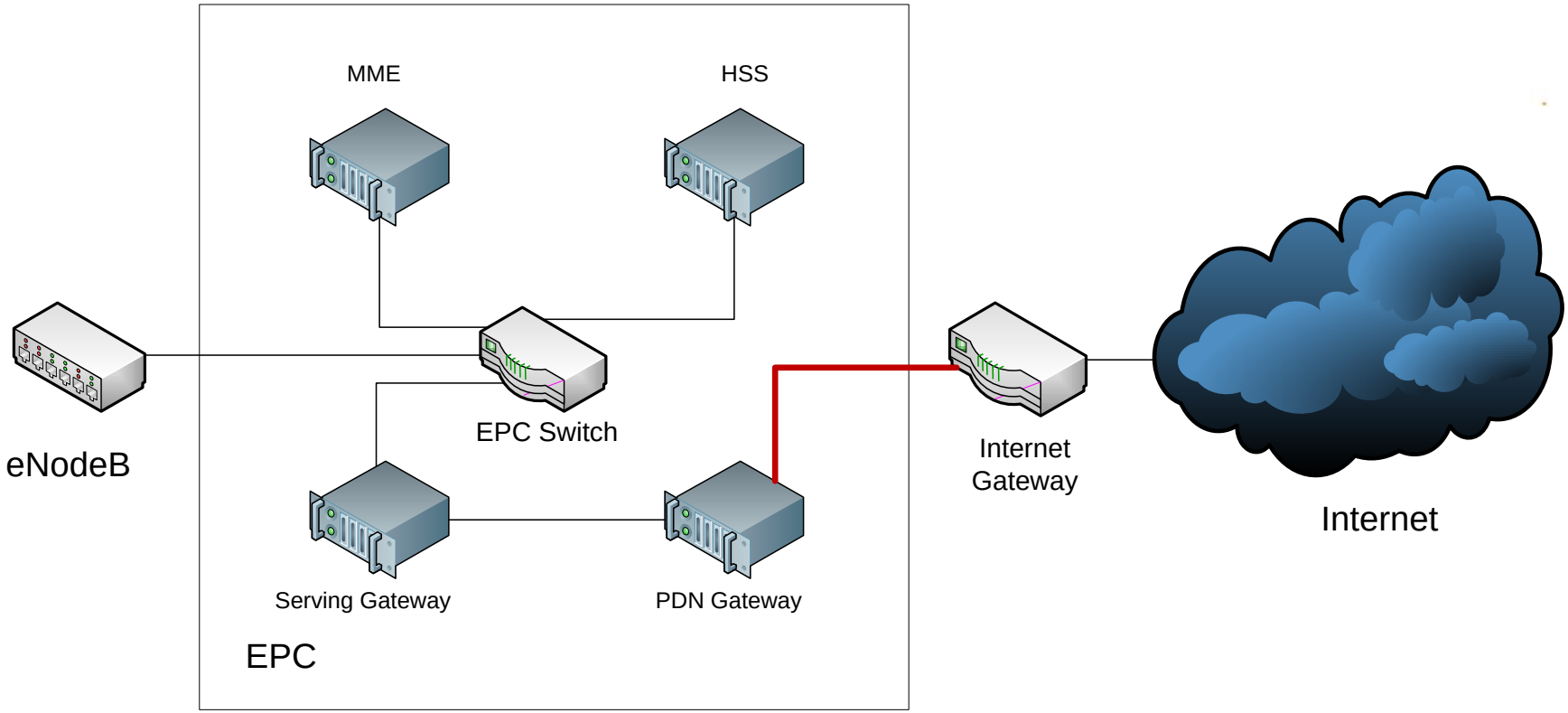
- Architecture design and routing in the core is complex
- Getting it right is critical to security
- We have seen issues with this
- This must be tested before an environment is deployed

Defences

IPSec

- If correctly implemented will provide Confidentiality and Integrity protection
- Can also provide authentication between components
- Keeping the keys secure is not trivial and not tested

Architecture Consideration



Conclusions

Conclusion 1

- There are 3 key protective controls that should be tested within LTE environments
  - Policies and rules in the Unified/Consolidated Gateway
  - The implementation of IPSec between all back-end components
  - A back-end IP network with well-designed routing and filtering

Conclusion 2

- Despite fears from the use of IP in 4G, LTE will improve security if implemented correctly
  - The 3 key controls must be correctly implemented
  - Testing must be completed for validation
  - Continued scrutiny is required
  - Legacy systems may be the weakest link

Conclusion 3

- Protecting key material used for IPSec is not trivial
  - The security model for IPSec needs careful consideration
  - Operational security processes are also important
  - Home eNodeB security is a challenge

Conclusion 4

- More air interface testing is needed
  - Will need co-operation from vendors/operators
  - “Open” testing tools will need significant development effort
  - Still lower hanging fruit if support for legacy wireless standards remain

Questions

@mwrinfosecurity
@mwrlabs