Fixed Network Architectures that Support Mobility

Irfan Ali

Objective of this lecture

- ***Understand the need of defining an architecture for wireless networks***
- ***Get an understanding of the process of how standards are written and from where to get standards documents***
- ***Understand the evolution of GSM family of standards***
  - Circuit Switch (CS) domain
  - Packet Switch (PS) domain
- ***Understand LTE architecture***
- ***Basic procedure of Attach (Registration) to illustrate how the entire architecture works***

LTE	Long Term Evolution

Overview of this lecture

- ***Process of Standards***
  - Why a cellular network architecture?
  - How is cellular network architecture defined?
  - Components of architecture (protocols, interfaces, etc)
  - From Lab to Standards to Products to Deployment
- ***GSM (3GPP) family of Standards***
  - GSM Architecture
  - UMTS Architecture
  - **LTE Architecture**

Why Standards?

- ***Cell phones from a large number of cellphone vendors (Nokia, Samsung, Motorola, Apple, etc.) need to work with infrastructure of a large number of infrastructure-vendors (Ericsson, Nokia, Huawei, Alcatel-Lucent, Samsung, etc).***
  - Need for an open and well specified interface between cellphones and the infrastructure.
- ***Operators would like to buy infrastructure from different vendors.***
  - Need for open and well specified interfaces in the infrastructure.
- ***Law of large numbers ➔ Lower-cost system***
  - Open and well specified systems ➔ attract a large number of vendors to build systems (networks and cell phones)

How?

- ***Operators and vendors form an open alliance to define specifications (standards) for systems***
  - Defining entire system
    - 3GPP Alliance (GSM [ETSI], UMTS, LTE)
    - 3GPP2 Alliance (CDMA)
    - WiMAX Forum (WiMAX)
    - ITU (Fixed telephony network, SS7, …)
    - IETF (Internet, e.g.: IP, TCP, UDP, PPP, …)
  - Defining limited-scope systems
    - IEEE (Ethernet, WiFi, 802.16m, RS 232, RS 485, etc)

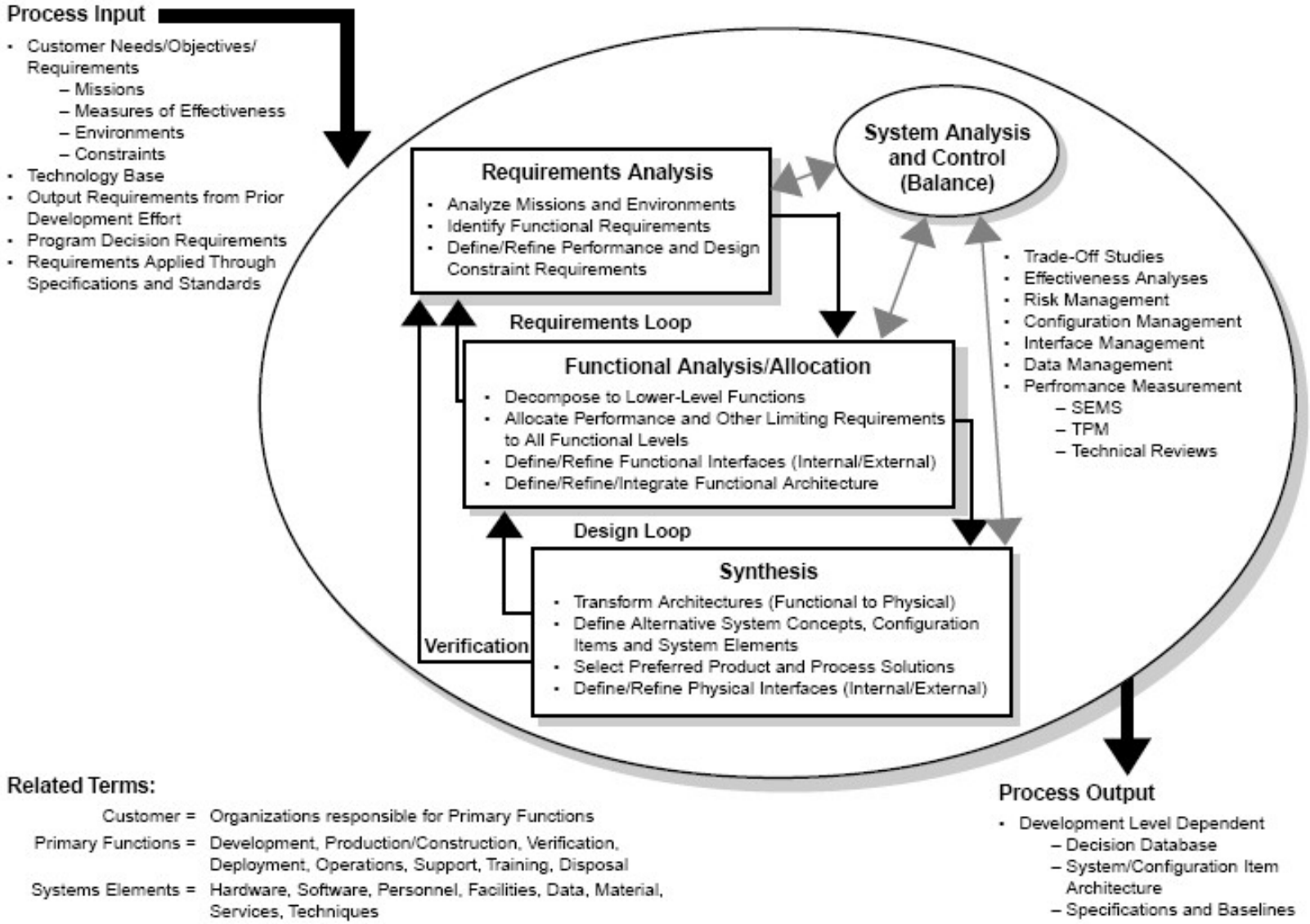
3GPP	3rd Generation Partnership Project
WiMAX	Worldwide Interoperability for Microwave Access
ETSI	European Telecommunication Standards Institue
UMTS	Universal Mobile Telecommunications System
CDMA	Code Division Multiple Access
ITU	International Telecommunications Union
IETF	Internet Engineering Task Force
SS7	Signalling System 7
IEEE	Institute of Electrical and Electronic Engineers

Systems Engineering and building blocks of system model

- ***Systems engineering is an interdisciplinary field of engineering that focuses on how complex engineering projects should be designed and managed over the life cycle of the project.***
  - In this course we will be focused on the design of cell phone systems
- ***System: There are many definitions of what a system is in the field of systems engineering. Below are a few authoritative definitions:***
  - ANSI/EIA-632-1999: "An aggregation of end products and enabling products to achieve a given purpose."
  - IEEE Std 1220-1998: "A set or arrangement of elements and processes that are related and whose behavior satisfies customer/operational needs and provides for life cycle sustainment of the products."
  - ISO/IEC 15288:2008: "A combination of interacting elements organized to achieve one or more stated purposes."

Source: Wikipedia

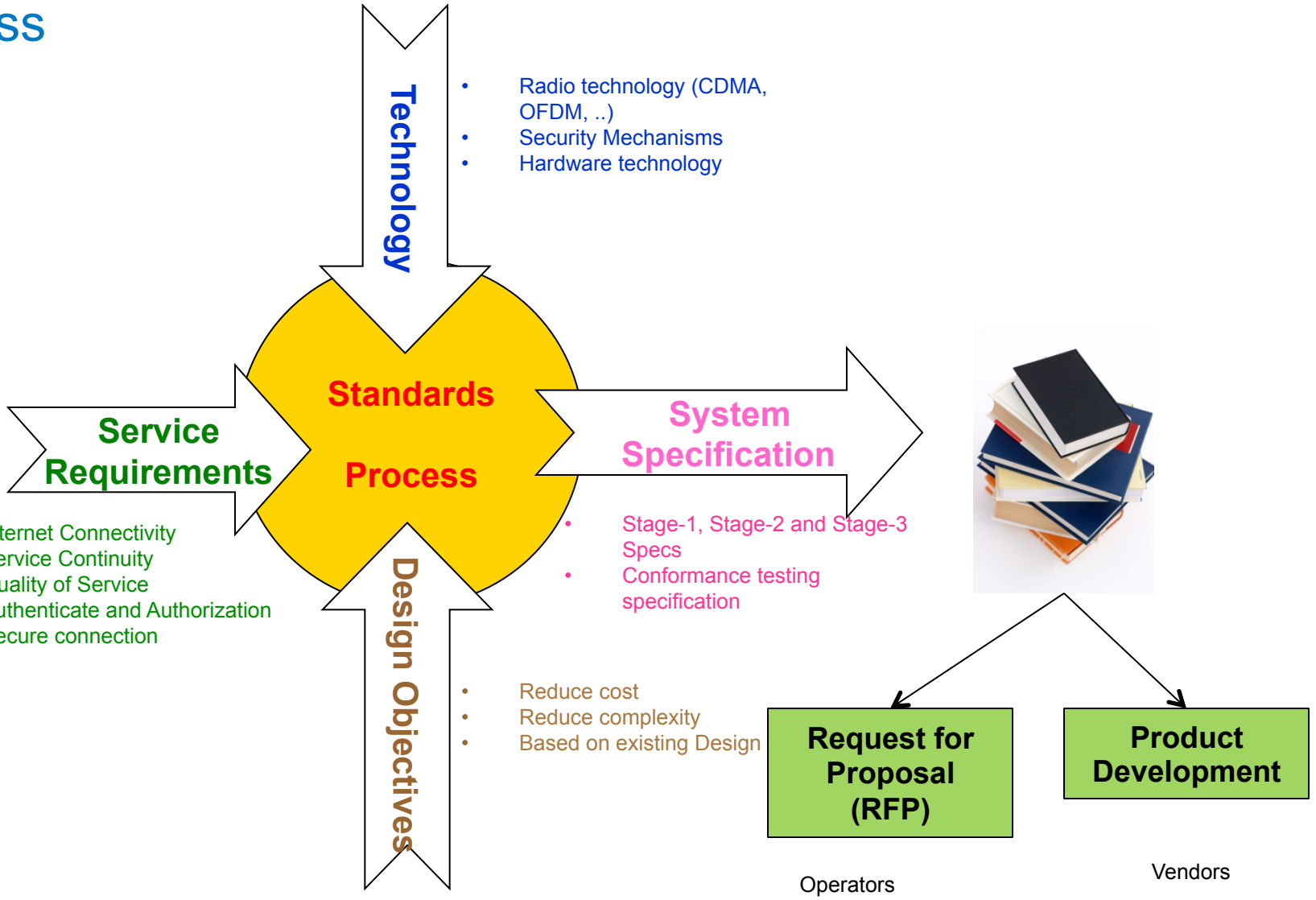
Systems Engineering Process



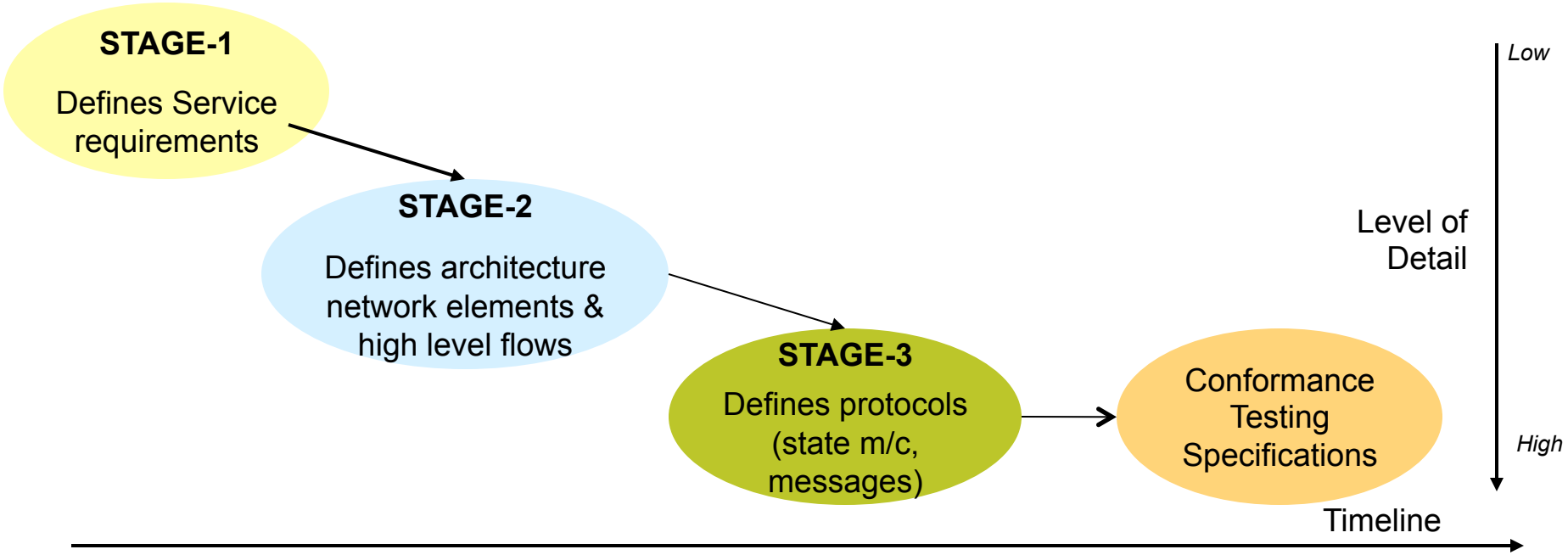
Related Terms:

Customer =	Organizations responsible for Primary Functions
Primary Functions =	Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal
Systems Elements =	Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques

Systems Engineering Process and Standards Process



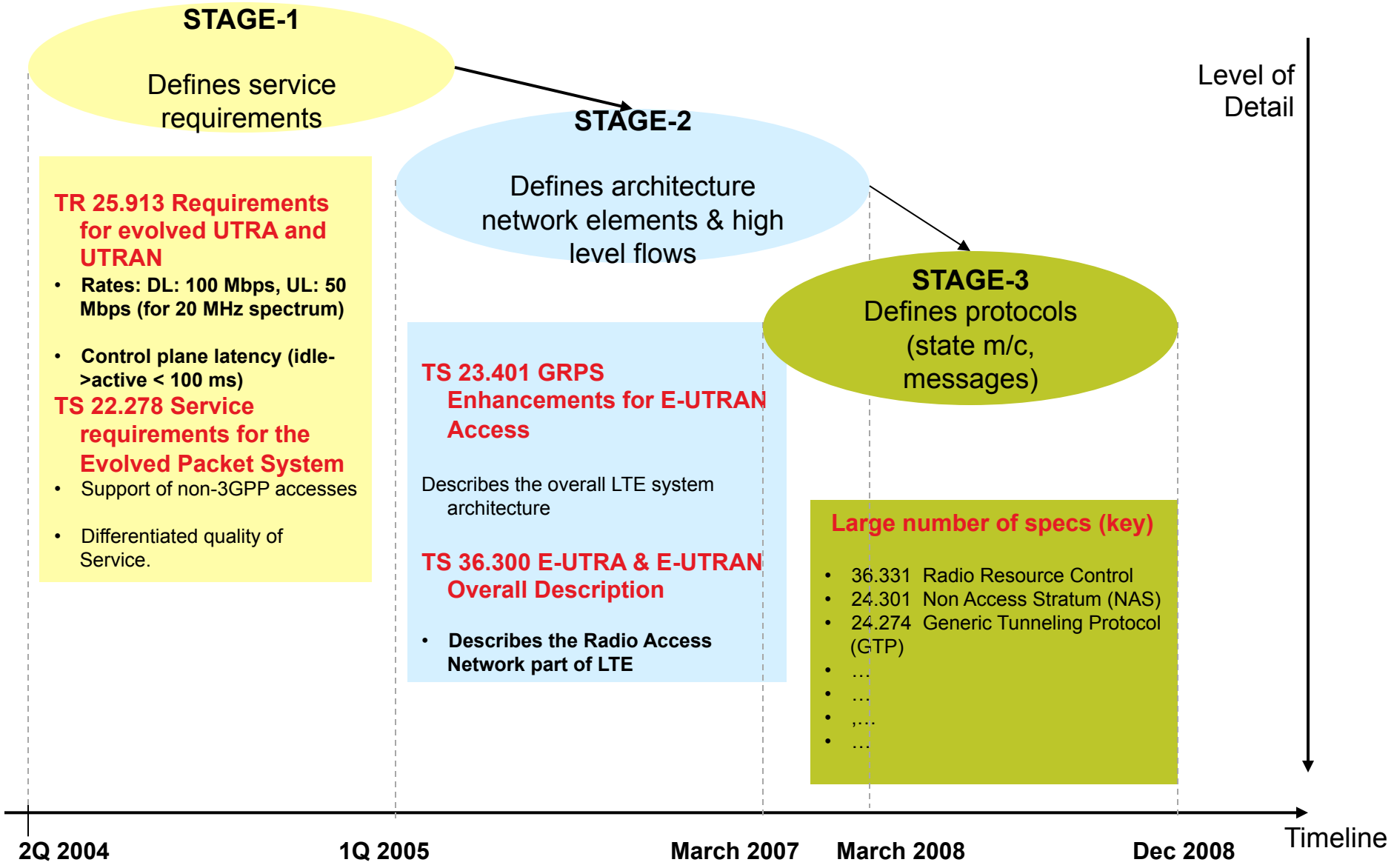
The 3GPP Process of Developing a New System/Feature/Service



- ***The process is applied to both "big features" e.g., LTE and to smaller features, e.g., Emergency-call support in LTE.***

Stages are defined in ITU-T Specification Recommendation I.130.
http://www.itu.int/rec/T-REC-I.130/en

The 3GPP Standards Process applied to LTE



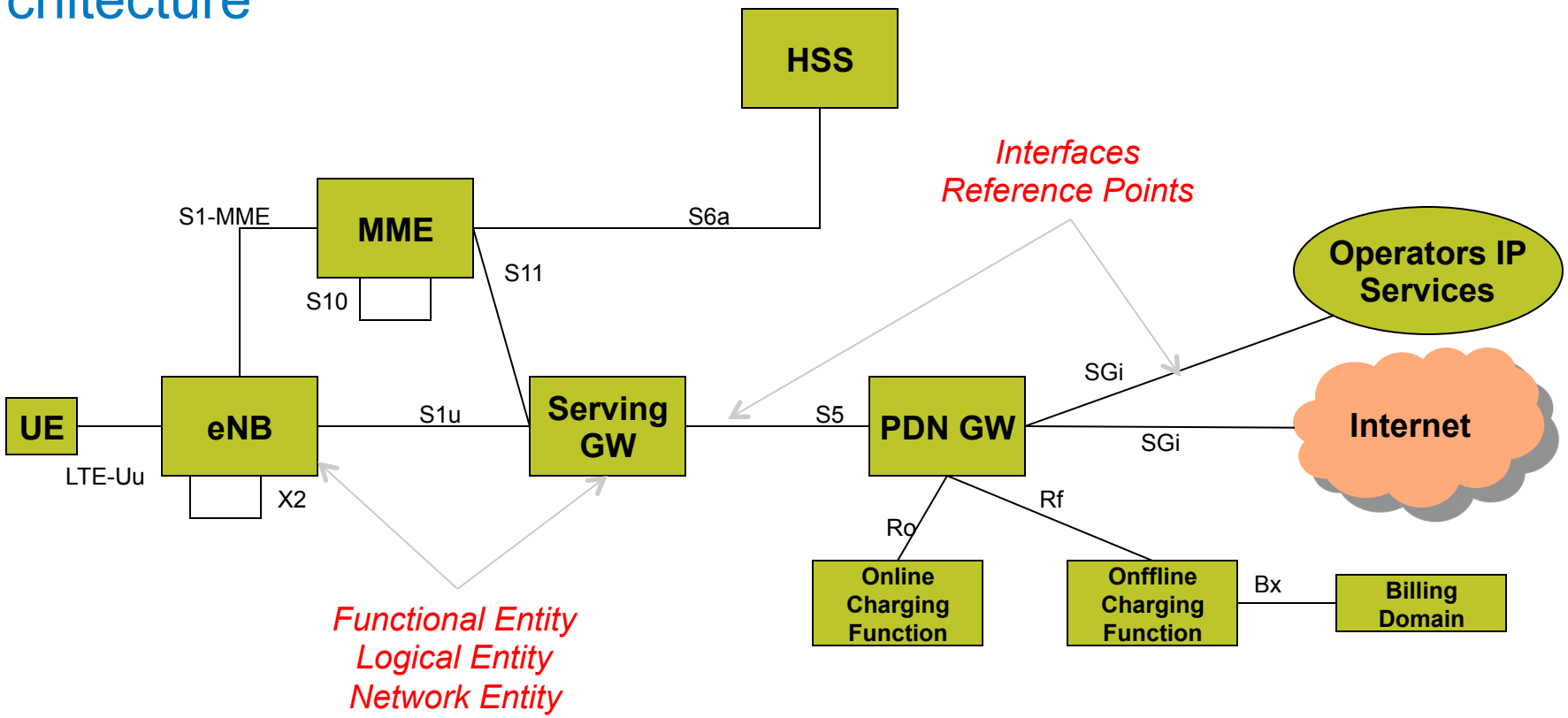
Stages are defined in ITU-T Specification Recommendation I.130.
http://www.itu.int/rec/T-REC-I.130/en

What are the components of Communication System Architecture Specification?

- ***A model of the system is created.***
  - An abstraction of reality designed to answer specific questions about the real world
  - An imitation, analogue, or representation of a real world process or structure; or
  - A conceptual, mathematical, or physical tool to assist a decision maker.
- ***Key components of model description are:***
  - Block Diagrams: Block diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines, that show the relationships of the blocks. (a.k.a., NRM – Network Reference Model)
  - Message Sequence Charts/ Sequence Diagrams: A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. (a.k.a., call flows)
  - Protocol level State Diagram: State diagrams model the system as composed of a finite number of states and the events that lead to transition between these states. (a.k.a., state machine)

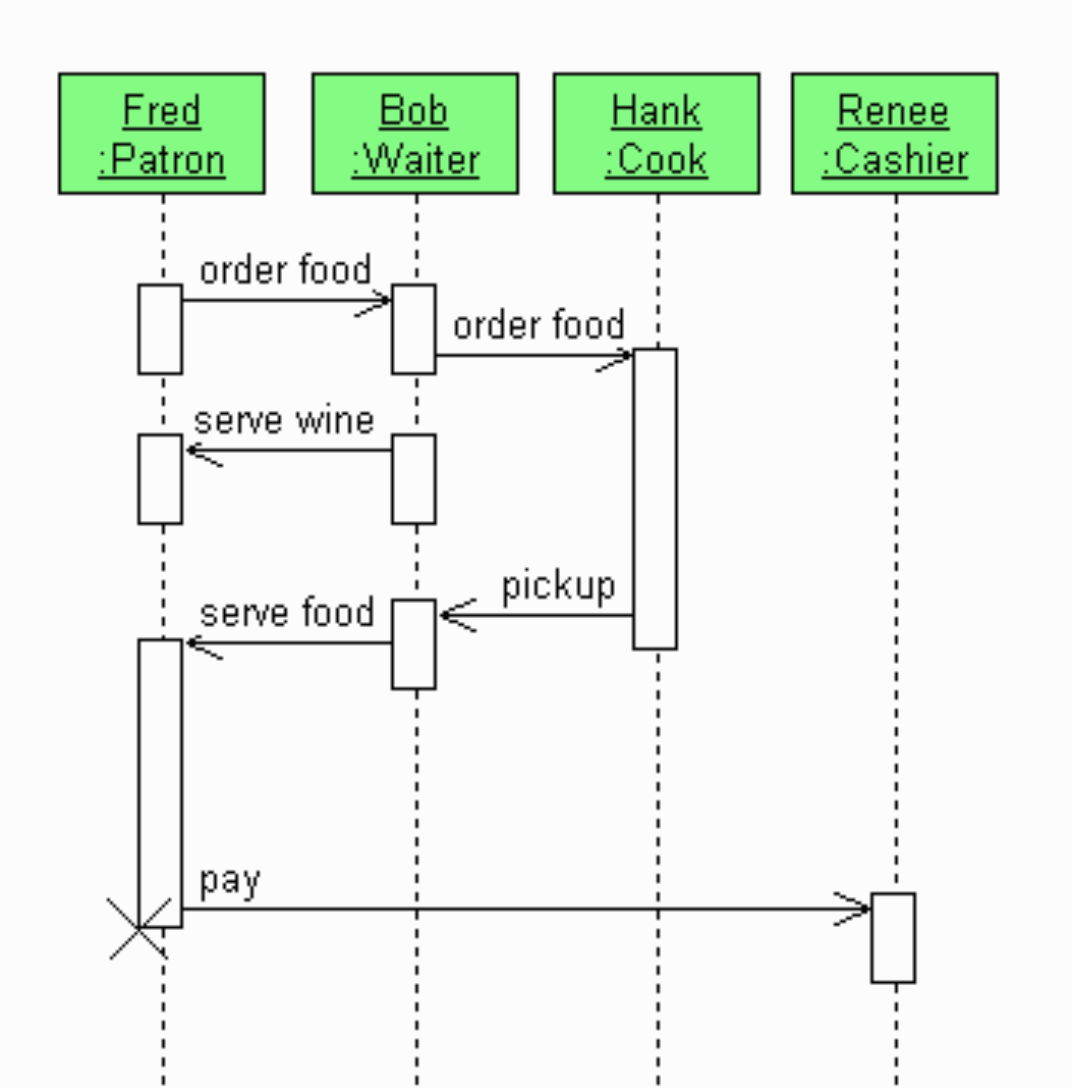
Source: Wikipedia

Block Diagram example: LTE Architecture

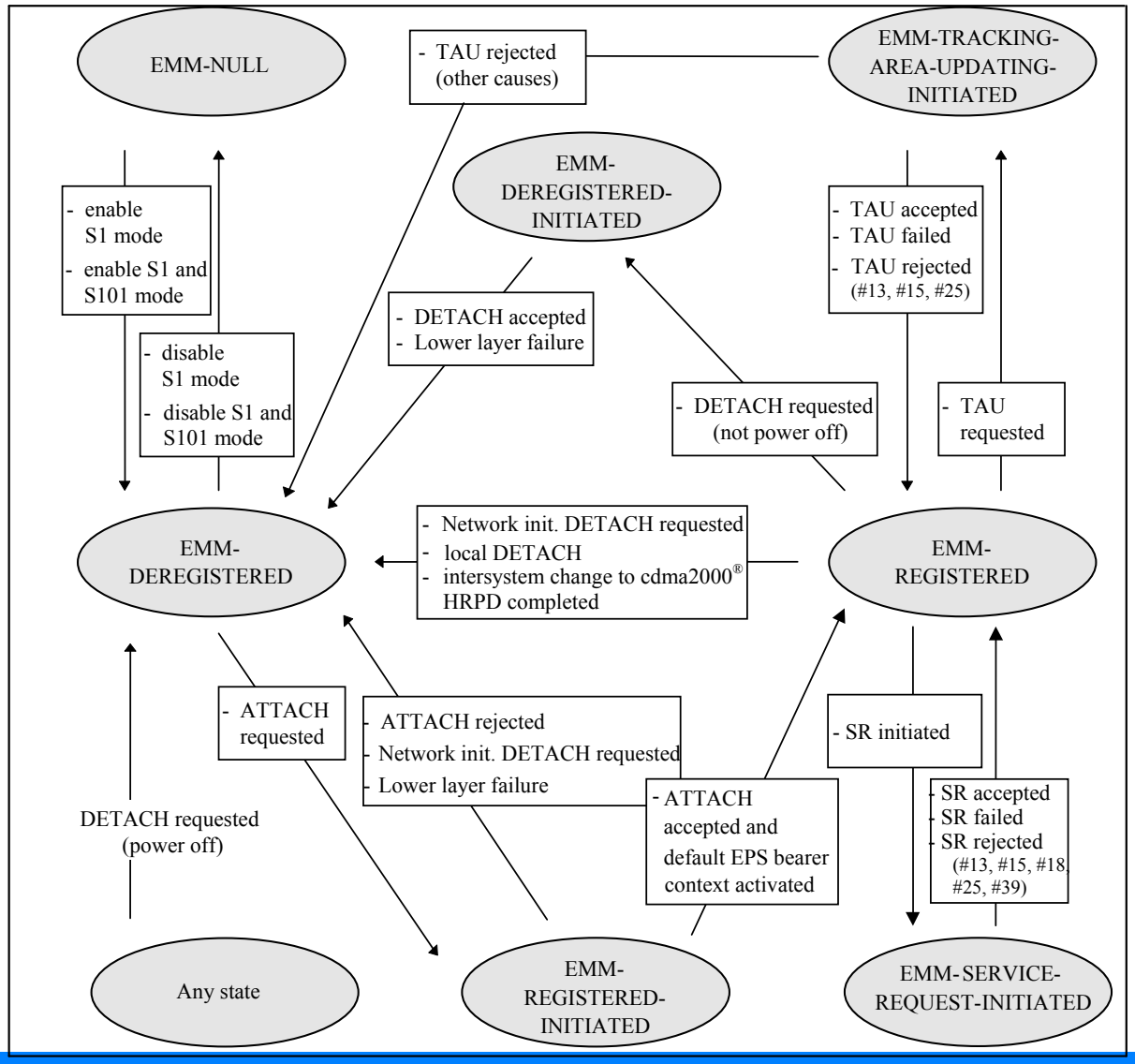


eNB	Enhanced Node B
MME	Mobility Management Entity
S-GW	Serving Gateway
PDN GW	Packet data network GW
HSS	Home Subscriber System

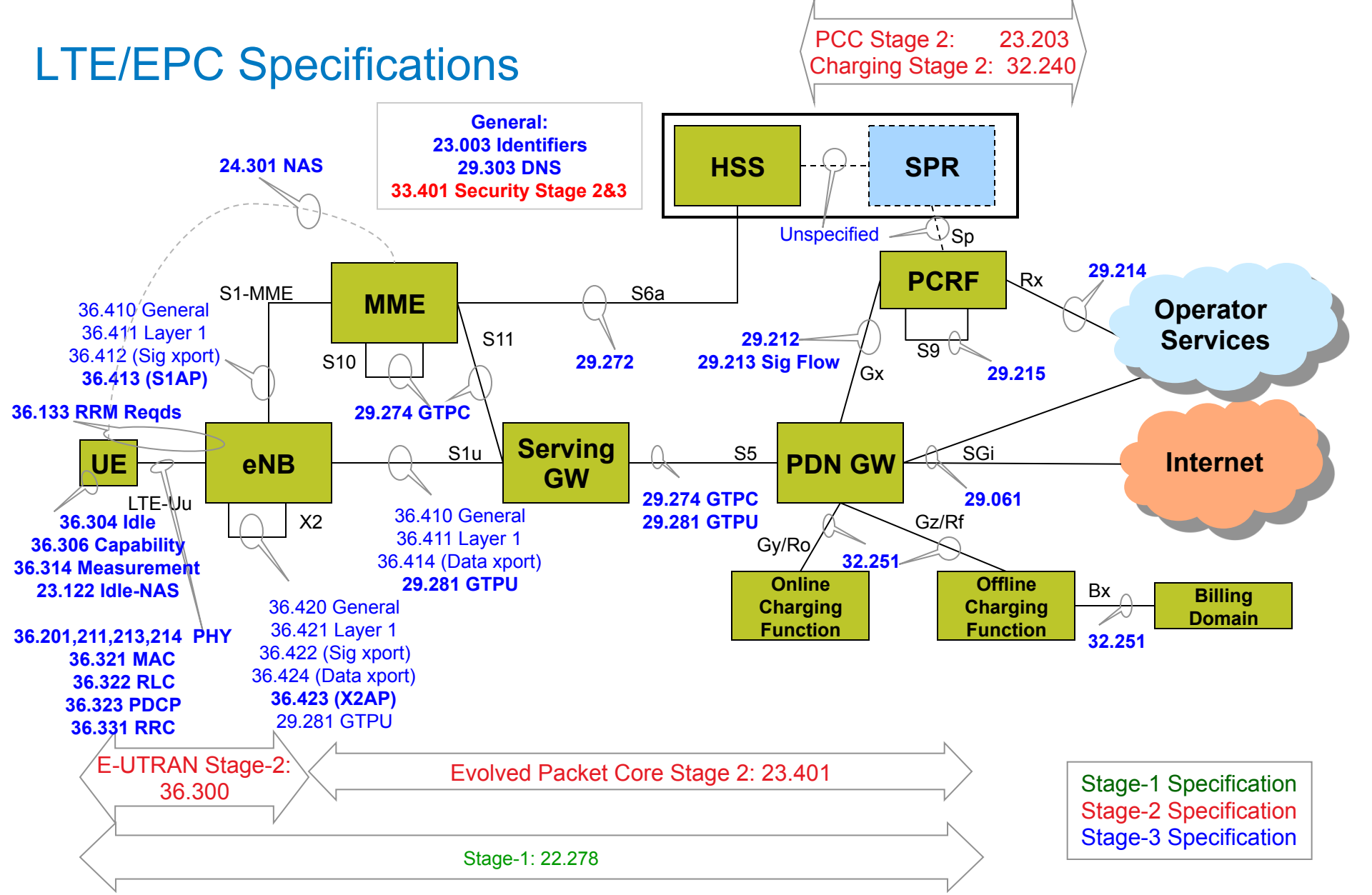
Message Sequence Chart Example: Restaurant



State Diagram Example: Enhanced Mobility Management (EMM) States in Mobile for LTE



LTE/EPC Specifications

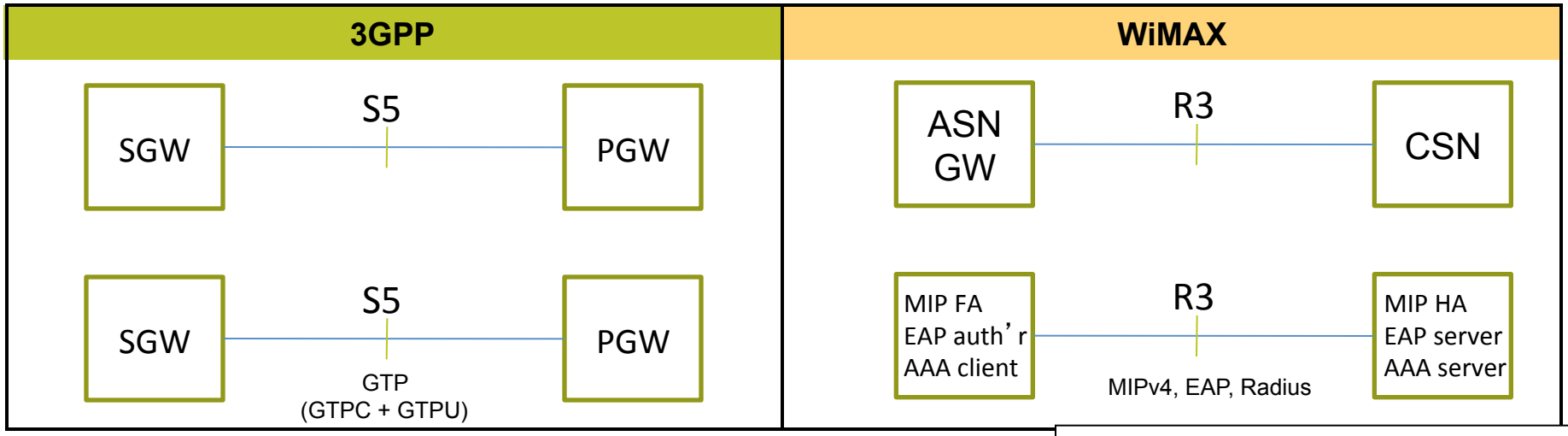


Protocols and Architecture

- *A communications protocol is a formal description of message formats and the rules for exchanging those messages (source: Wikipedia).*
- *Protocol: A formal set of procedures that are adopted to ensure communication between two or more functions within the same layer of a hierarchy of functions (source: ITU-T I.112).*
  - **Protocols are typically created for meeting a simple function and assume simple architecture, e.g.:**
    - **Point to Point Protocol (PPP) (RFC 1661): Setting up serial link between a PPP client and PPP Server**
    - **Mobile IPv6: IP-layer mobility support between an IPv6 client and a MIPv6 home agent.**
    - **IEEE 802.16e: Physical and MAC layer protocols between two modems using OFDM technology.**
- *Network architecture is the design of a communications network to meet a complex set of functionality.*
  - **It includes specifying functional elements, reference points between them, protocols running on those reference points, and the interactions.**
  - 3GPP LTE architecture
  - WiMAX architecture
  - 3GPP2 architecture

Reference point, Interface and Protocols

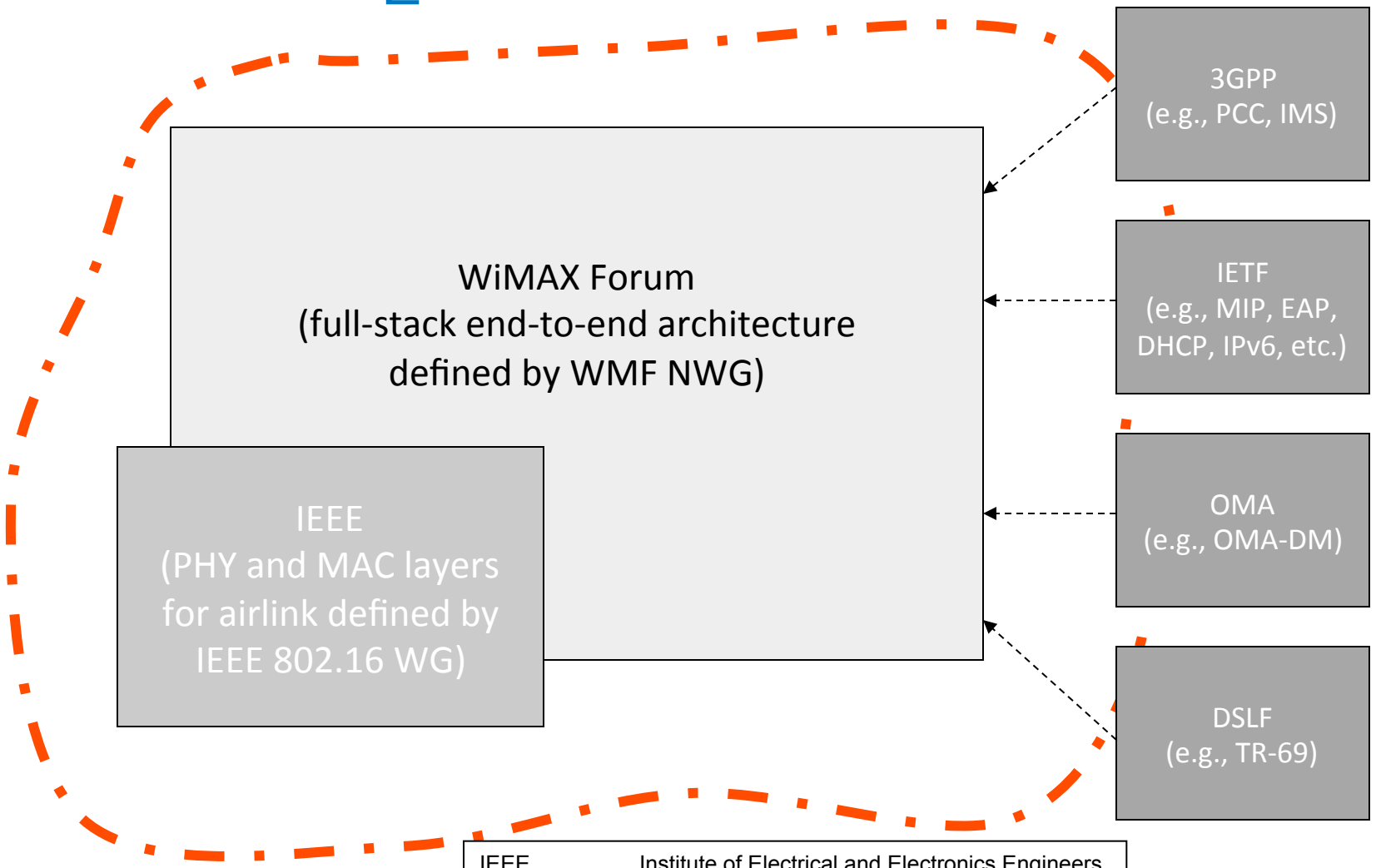
- ***Reference point: A conceptual point at the conjunction of two non-overlapping functional groups (source: ITU-T I.112).***
- ***Interface: The common boundary between two associated systems (source: ITU-T I.112).***
- ***Terms "reference point" and "interface" are used inter-changeably in standards***
- ***One or more protocols are used on a reference point.***
  - In case of 3GPP up-to a maximum of one user-plane and one control-plane protocol is used on an interface
  - For WiMAX, multiple protocols may exist on a reference point.



GPRS	General Packet Radio System
GTP	GPRS Tunneling Protocol

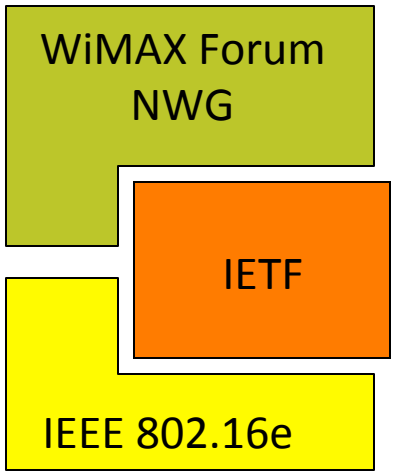
EAP	Extensible Authentication Protocol
AAA	Authentication Authorization and Accounting

WiMAX Standard = ∑ …

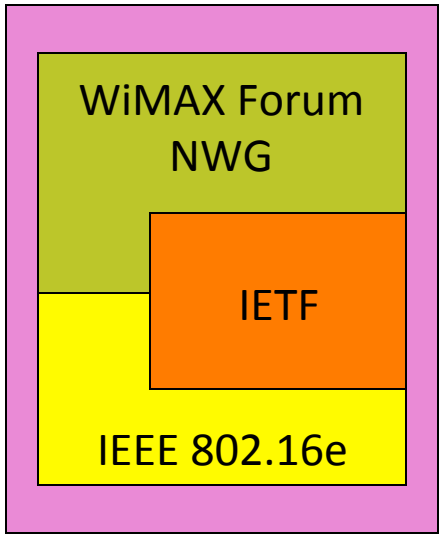


IEEE	Institute of Electrical and Electronics Engineers
WG	Working Group
PCC	Policy and Charging Control
IMS	Internet Multimedia System
IETF	Internet Engineering Task Force
MIP	Mobile IP
OMA	Open Mobile Alliance
DM	Device Management
DSLF	Digital Subscriber Line Forum

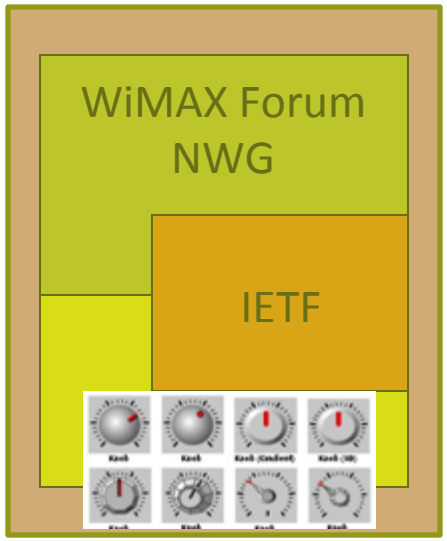
Packaging



WiMAX standards

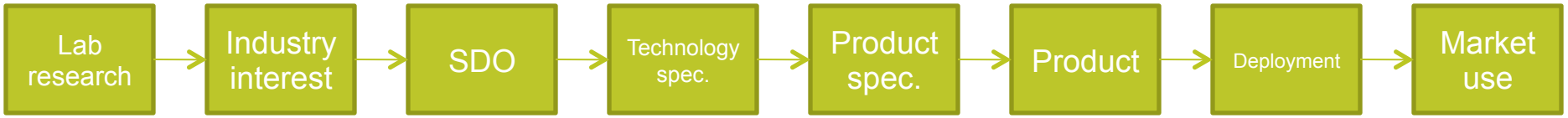


WiMAX product

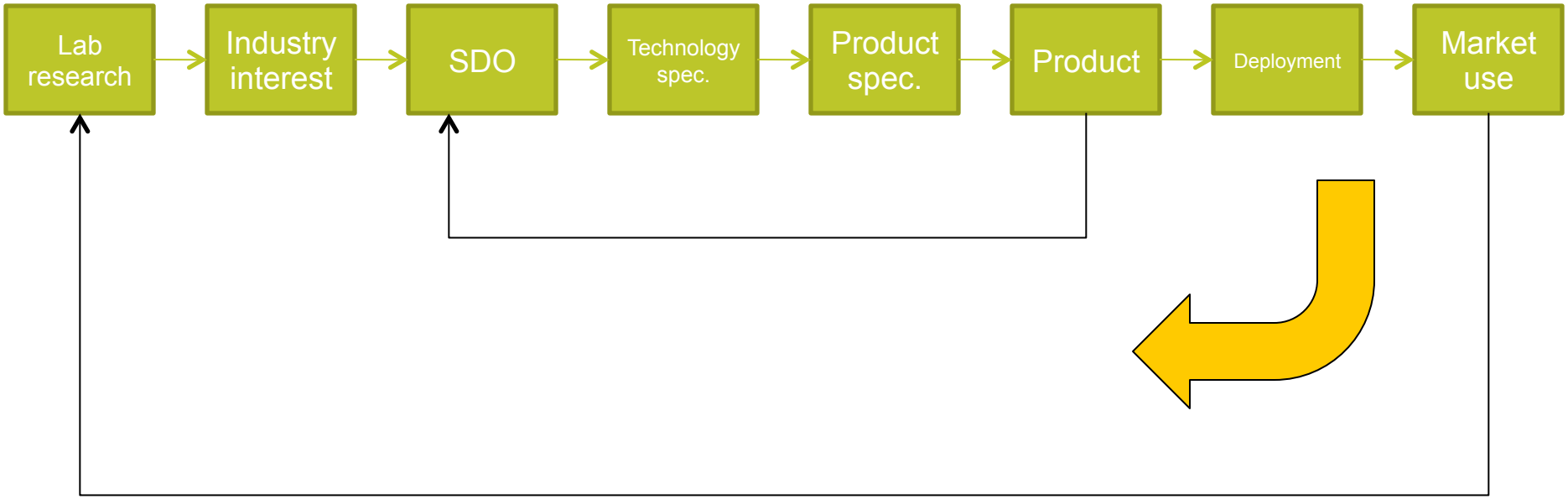


WiMAX deployment

Wireless Technology Lifecycle



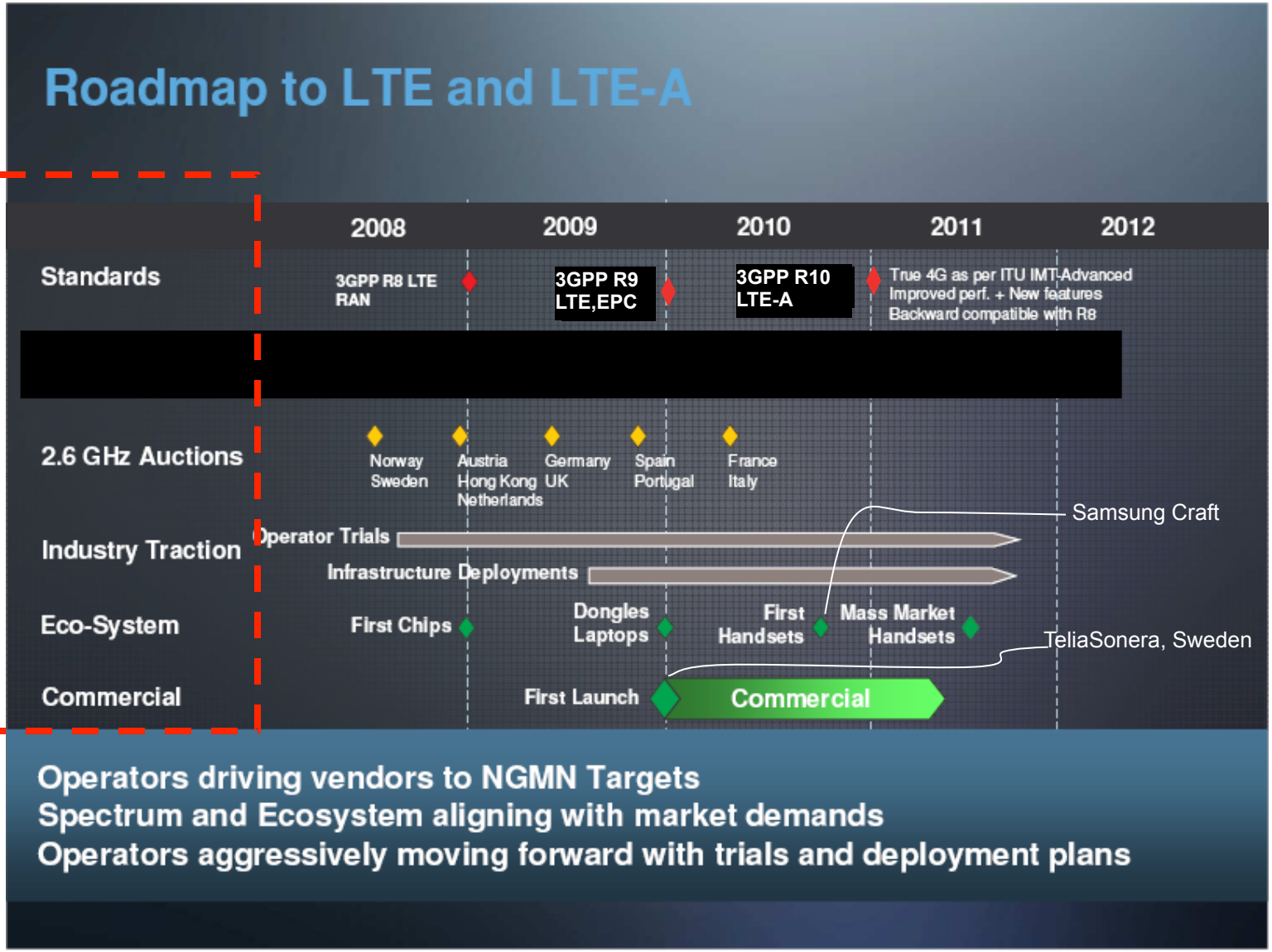
Iterations


Lab research
Industry interest
SDO
Technology spec.
Product spec.
Product
Deployment
Market use

Bumpy Ride


Lab research
Industry interest
SDO
Technology spec.
Product spec.
Product
Deployment
Market use

From Standards to Products

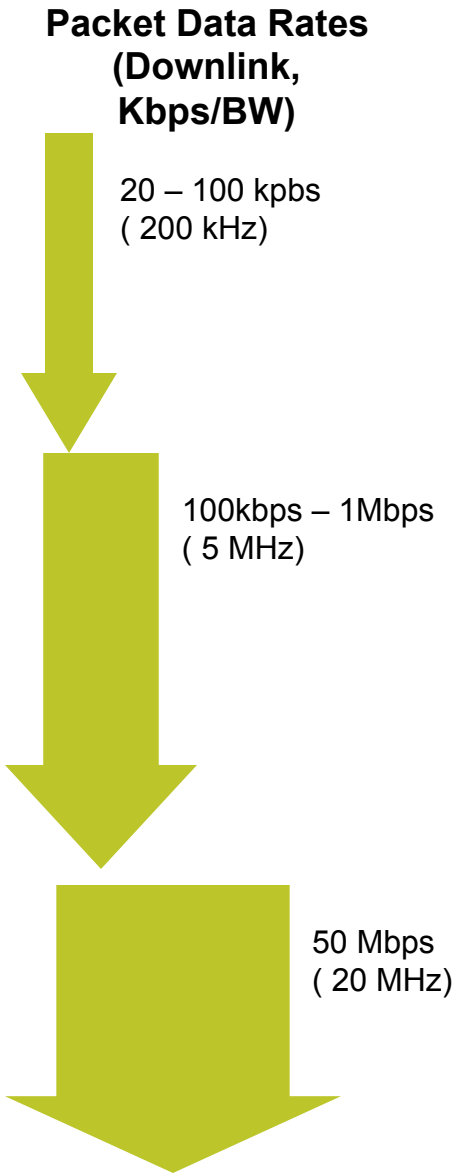


Source: Adapted from, Amitava Ghosh, "WiMAX or LTE or what else and beyond " IEEE Radio and Wireless Week, 18 – 22 Jan 2009

3GPP Family of Network Architectures

3GPP Radio Access Technology and Network Evolution

- ***2G: GSM – 1991 (Global System for Mobile communications)***
  - **Time Division Multiple Access Technology (TDMA)**
  - Primarily Circuit Switch (CS) Domain: Make and receive phone-calls
  - 1995: Packet Switch (PS) domain added. 20 -100 kbps. GPRS core-network added
- ***3G: UMTS – 2002 (Universal Mobile Telecommunications System)***
  - **Code Division Multiple Access Technology (CDMA)**
  - Both CS and PS Domain: 100s kbps – 1Mbps downlink data rates
  - PS Network architecture extended & re-used GPRS architecture
  - HSPA added in 2005-2009: Upto 14.4 and 28.8 Mbps downlink in 5MHz bandwidth
- ***4G: LTE – 2008 (Long Term Evolution)***
  - **Orthogonal Frequency Division Multiplexing (OFDM)**
  - Only PS domain: 100 Mbps DL, 50 Mbps UL in 20 MHz bands
  - PS architecture attempted to break from GPRS architecture.
    - PS architecture is further extension of GPRS architecture



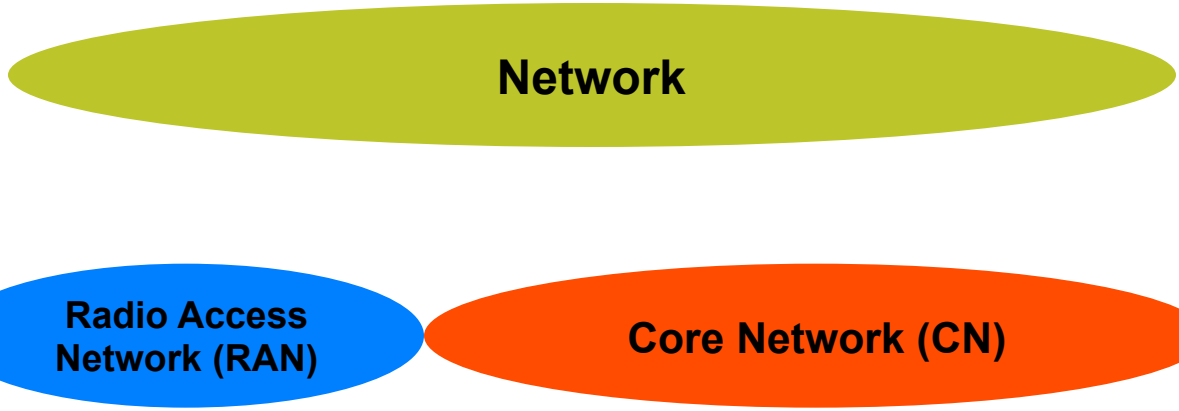
Dates are approximate and correspond to first large size commercial deployments

How of 3GPP (GSM family)

- ***3GPP is funded and attended by a large number of vendors and operators who have a financial stake in the GSM family of standards***
- ***3GPP is divided into a large number of groups, focused on different areas (eg Radio Access layer (L1, L2) vs higher layers (L3, L4)).***
- ***These groups meet several times a year (typically 6-8) and work together to create documents called "Technical Specifications (TS)" which defines how the system works.***
  - The technical specifications are "living documents" which are updated at the end of every meeting.
  - Discussion does occur via emails and conference calls, but most agreements are made in face-to-face meetings.
- ***The Technical Specifications are openly available to everyone (even non-members) via the Internet.***

3GPP Network Architecture

User Equipment (UE)



Base station Radio
+
Radio Resource Management

Upper Layers
(eg. Security, Mobility)

SIM	Subscriber Identity Module
USIM	Universal Subscriber identity Module

Some Key Architecture Requirements for EPC

IP Addressing/Mobility Related

- ***IP Address Continuity: IP address continuity shall be maintained as the user moves in the network.***
- ***Mobility between base-stations in visited-network will not be made visible to the home network.***

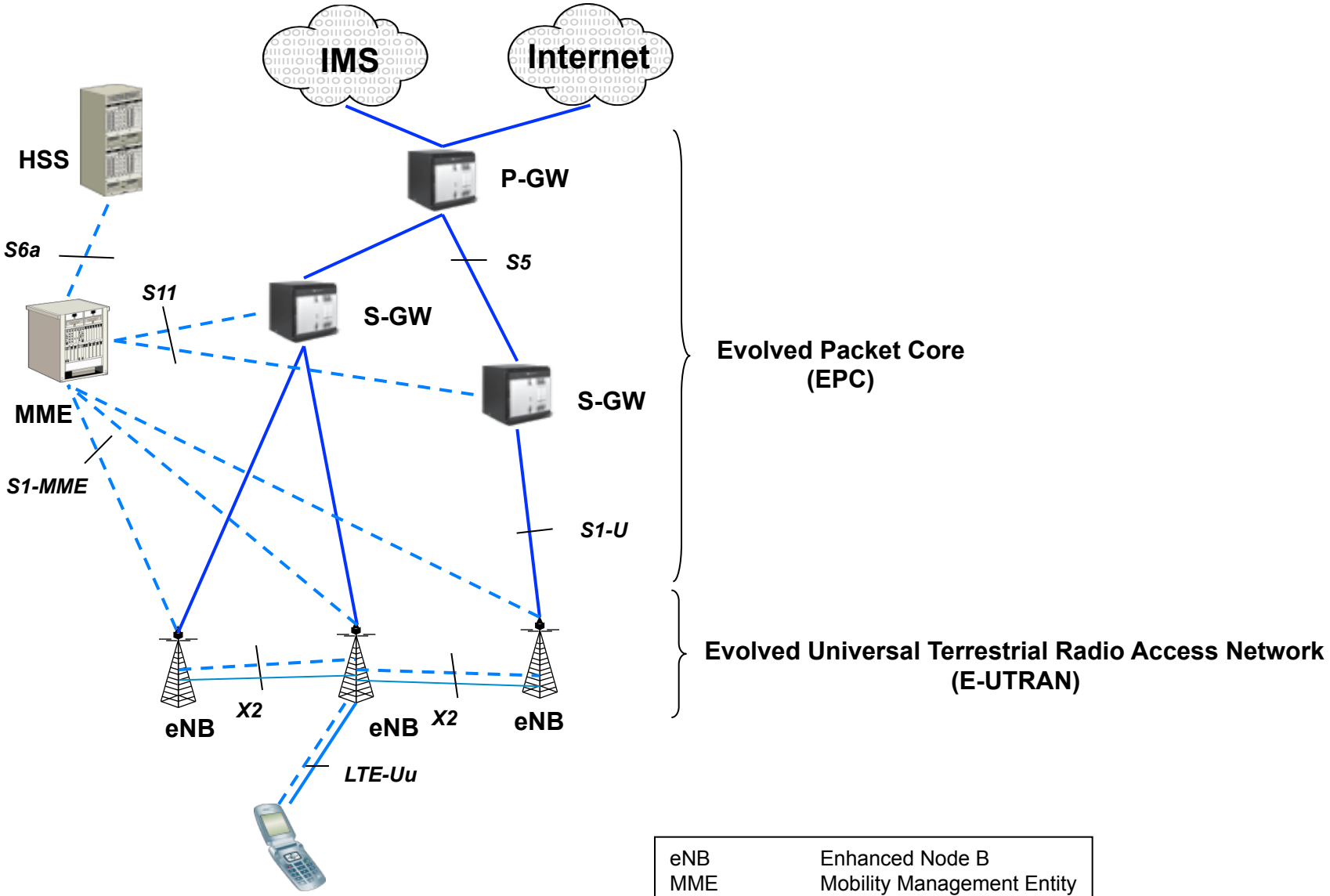
Security

- ***The radio-level signaling messages between the UE and the base-station will be secure (encrypted) and integrity-protected.***
- ***The network-level signaling between the UE and the core-network will be secure and integrity-protected. The eNB shall not be able to "look inside" or "tamper" the network-level signaling message.***

Access

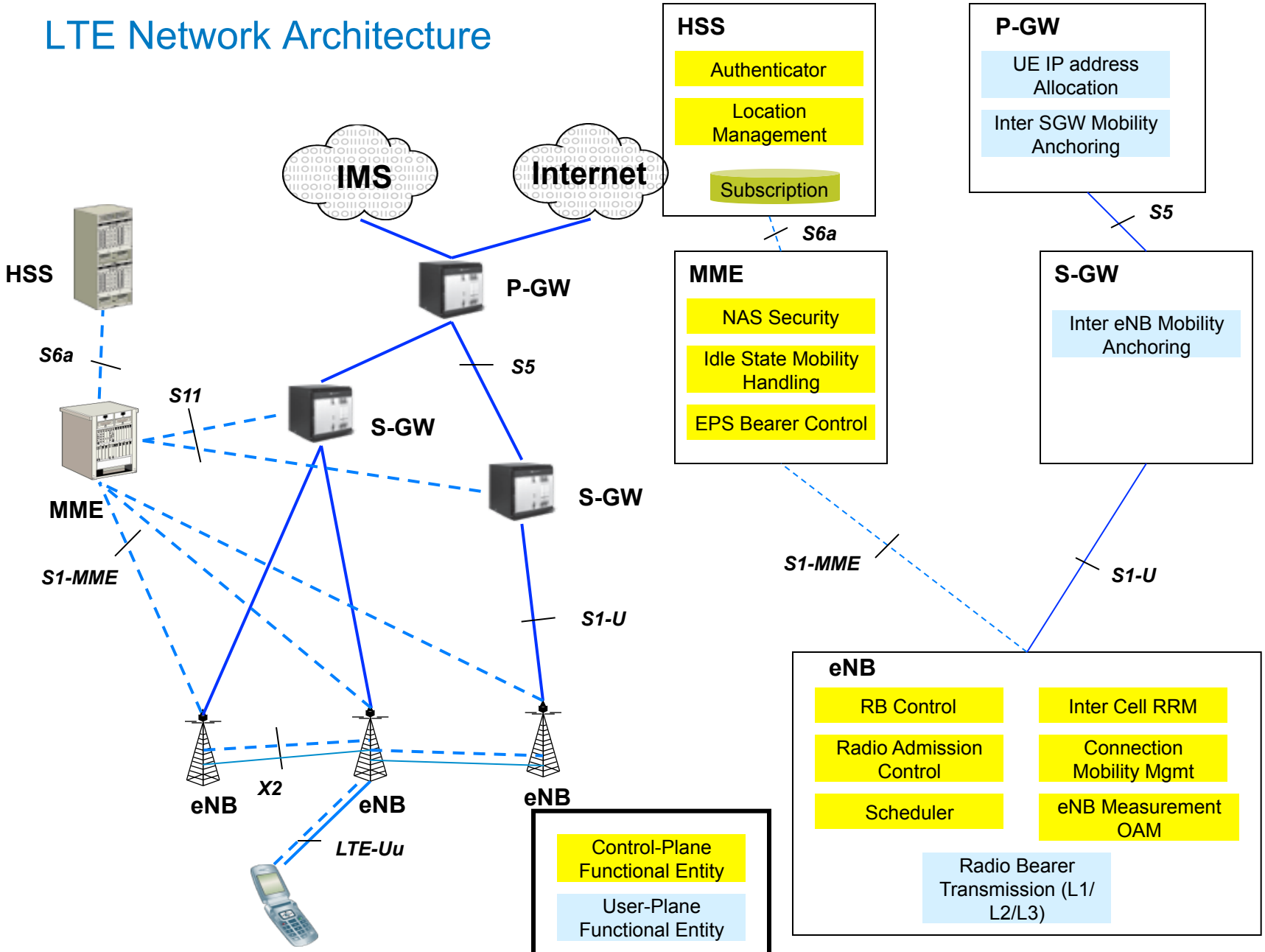
- ***Roaming will be supported whereby the user is allowed to access the network in a visited (foreign) network.***
- ***For roaming, the user will be authenticated and authorized by the home network.***

LTE Network Architecture: PS Domain only

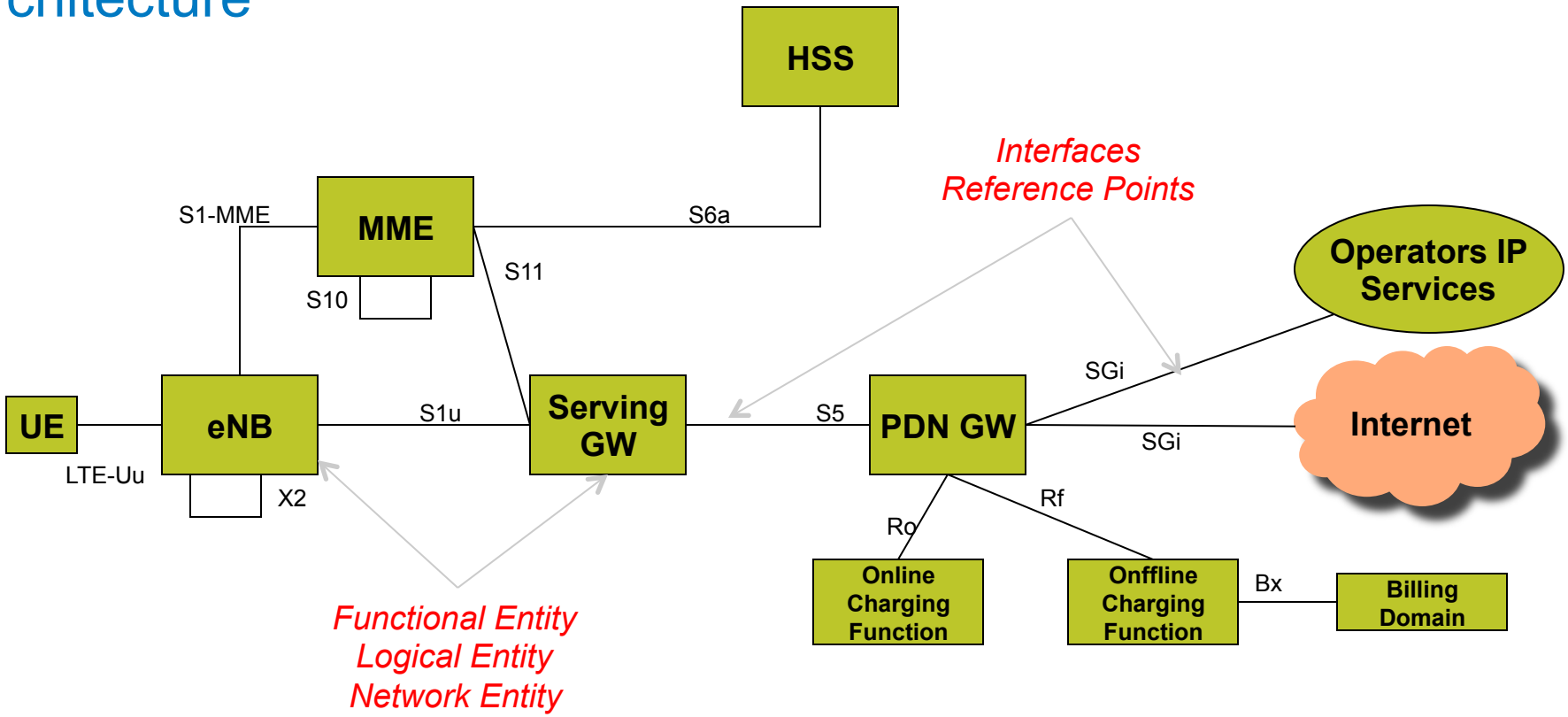


eNB	Enhanced Node B
MME	Mobility Management Entity
S-GW	Serving Gateway
P-GW	Packet data network GW
HSS	Home Subscriber System

LTE Network Architecture



Block Diagram example: LTE Architecture

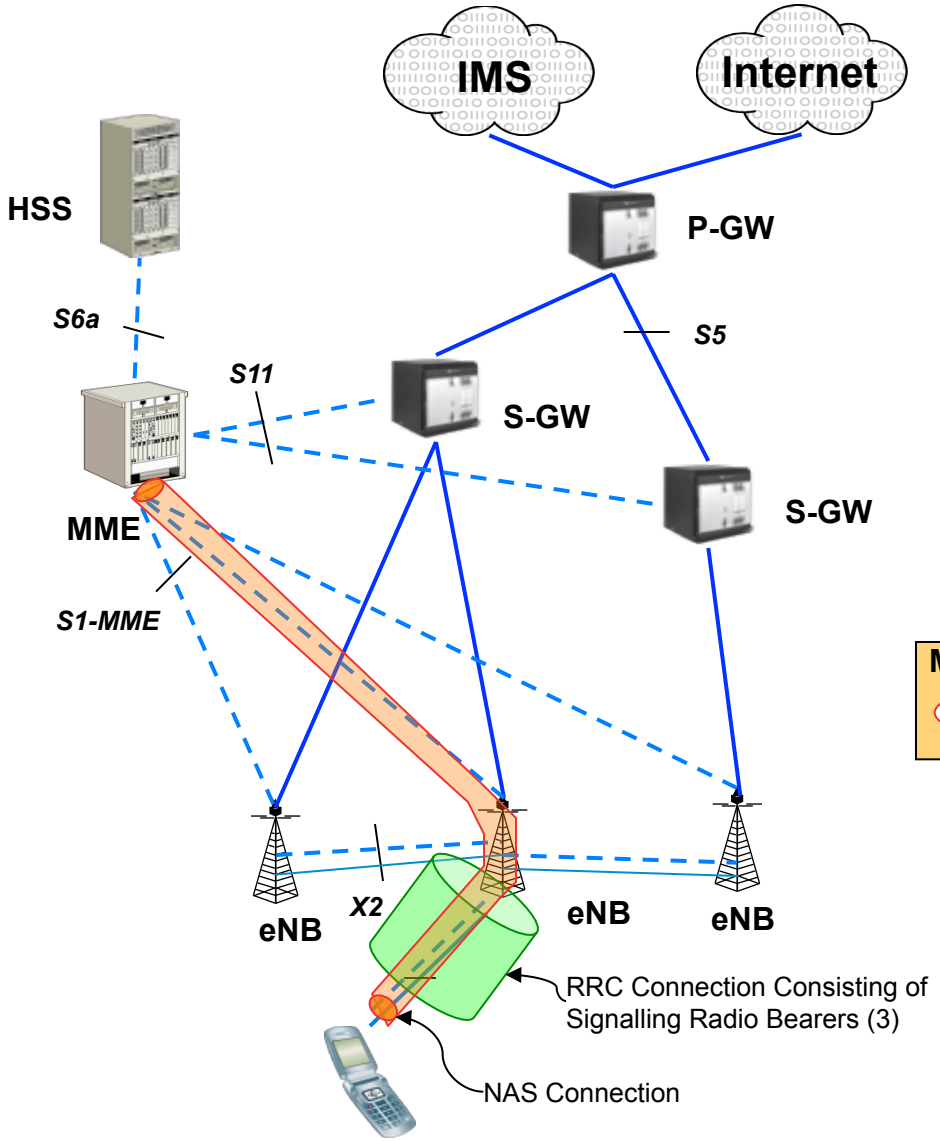


eNB	Enhanced Node B
MME	Mobility Management Entity
S-GW	Serving Gateway
PDN GW	Packet data network GW
HSS	Home Subscriber System

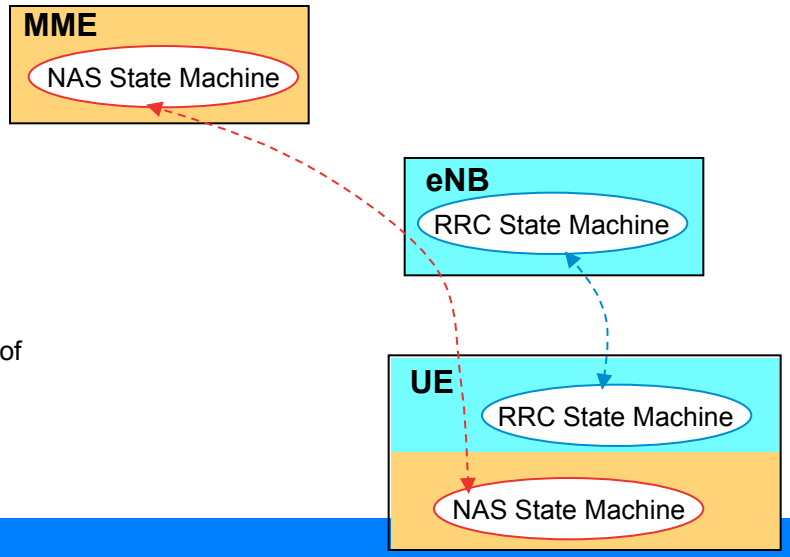
LTE Architecture Key Concepts

- ***All radio related functions are pushed down to the eNB***
  - There is no centralized radio resource management element like the RNC.
- ***In the core network, there is control-plane and user-plane separation***
  - MME is the control-plane entity.
  - SGW and PGW are the user-plane entity
  - To allow independent scaling of the control-plane and the user-plane.

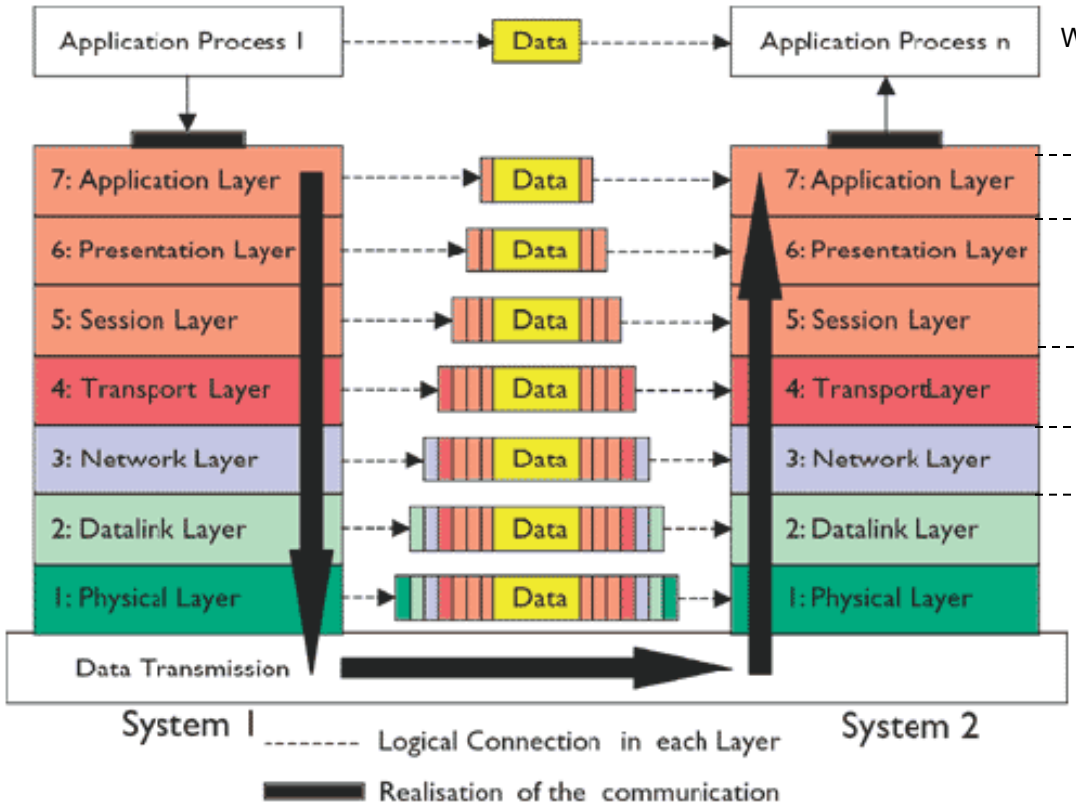
UE's Signalling with the network: Access Stratum (AS) and Non-Access Stratum (NAS)

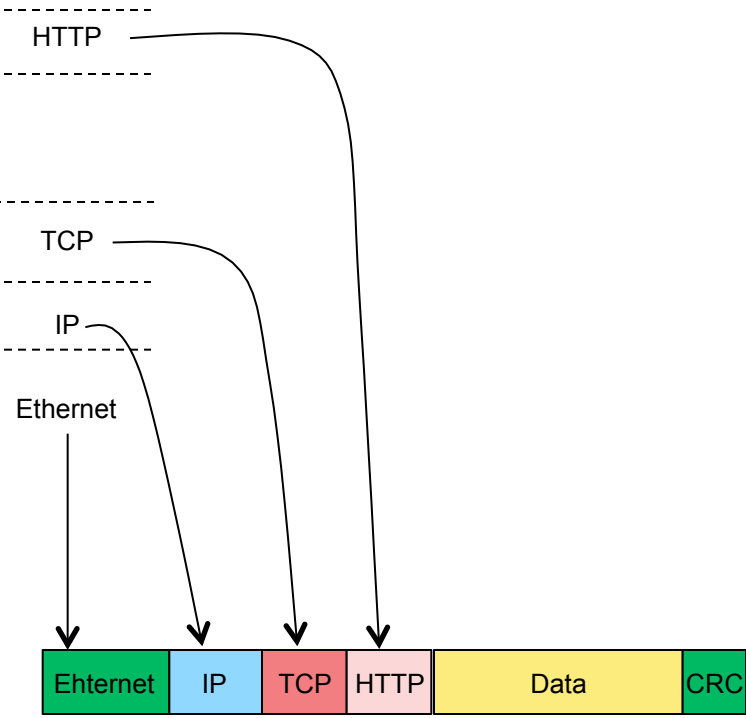


- ***The UE performs control communication (signalling) with two nodes in the network:***
  - **eNB** via the Radio Resource Control (RRC) protocol. This is called the access-stratum
  - **MME** via the Non-access-stratum protocol.
- ***The NAS messages are carried inside RRC messages.***

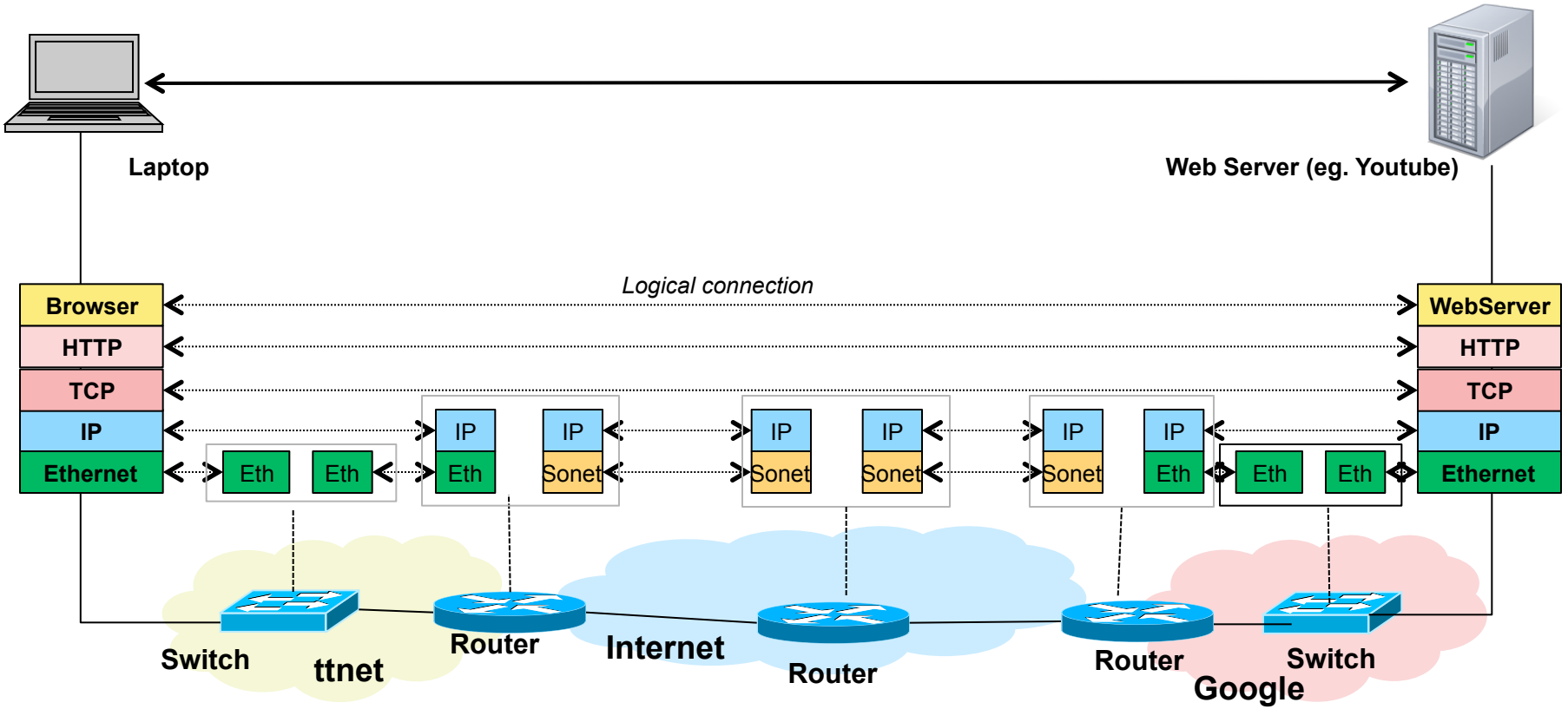


Protocol Stack and Bits on the Wire



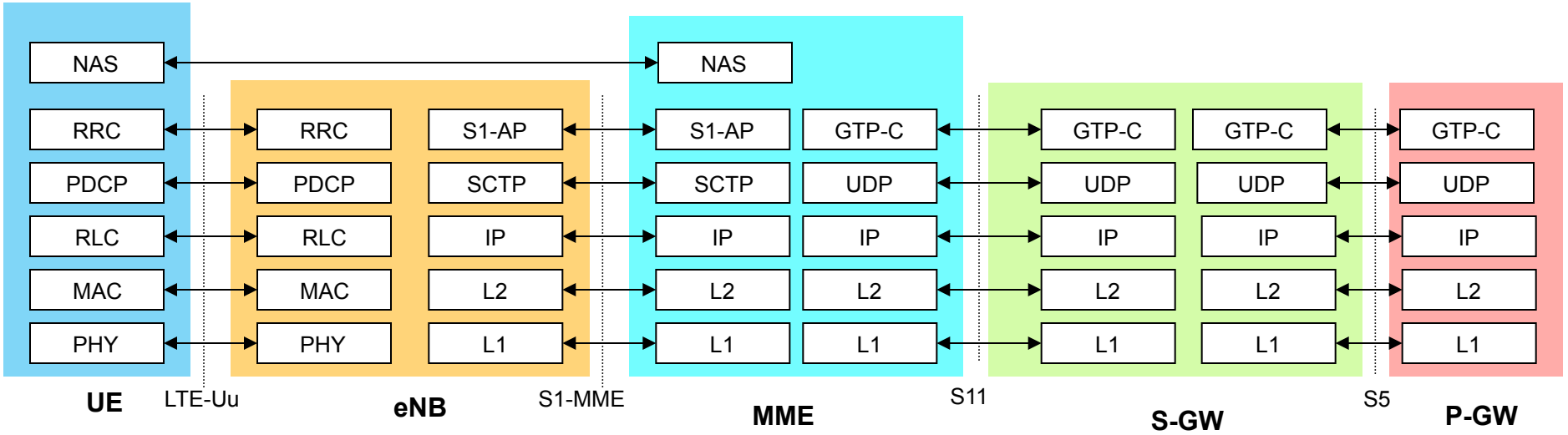


Protocol Stack and Processing on the Path



- *Protocol Stacks are at interfaces*
- *Layer 4 and above are end-to-end logical connections*
- *Layer 3 is processed by routers on the path. So this is a hop-by-hop logical connection*
- *Layer 2 and Layer 1 are link-by-link logical connections.*

Protocol Stacks: Control Plane



Non-Access Stratum (NAS): The key control interface between MME and UE

Radio Resource Control (RRC): The main control interface between eNB and UE

Packet Data Convergence Protocol (PDCP): Duplicate detection, ROHC

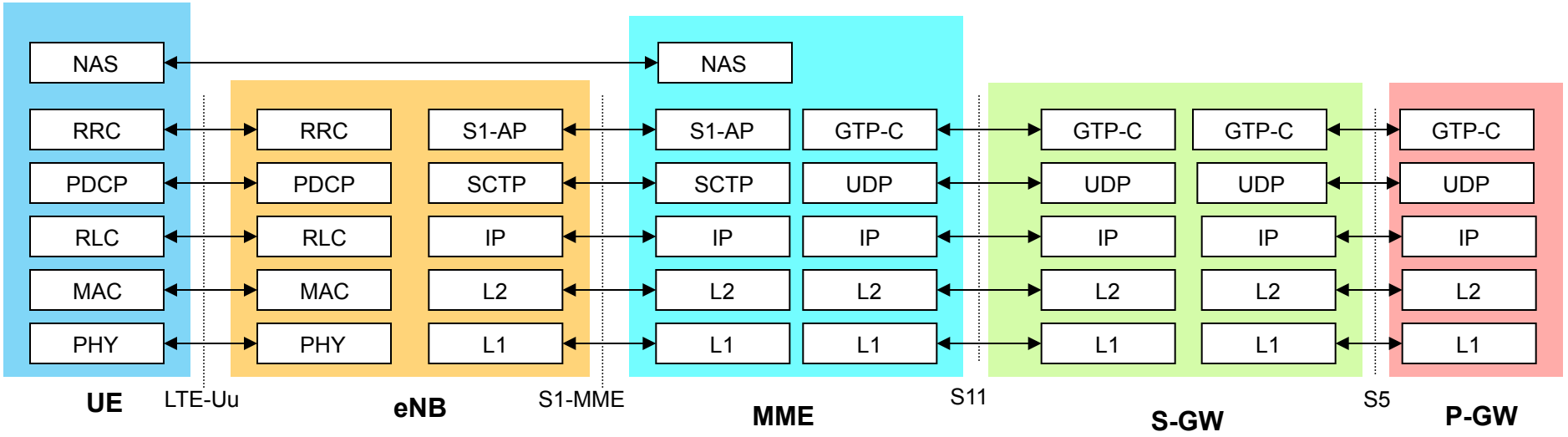
Radio Link Control (RLC): Segmentation/re-assmebly, ARQ, acknowledge mode (AM)/ un-acknowledged mode (UAM), etc

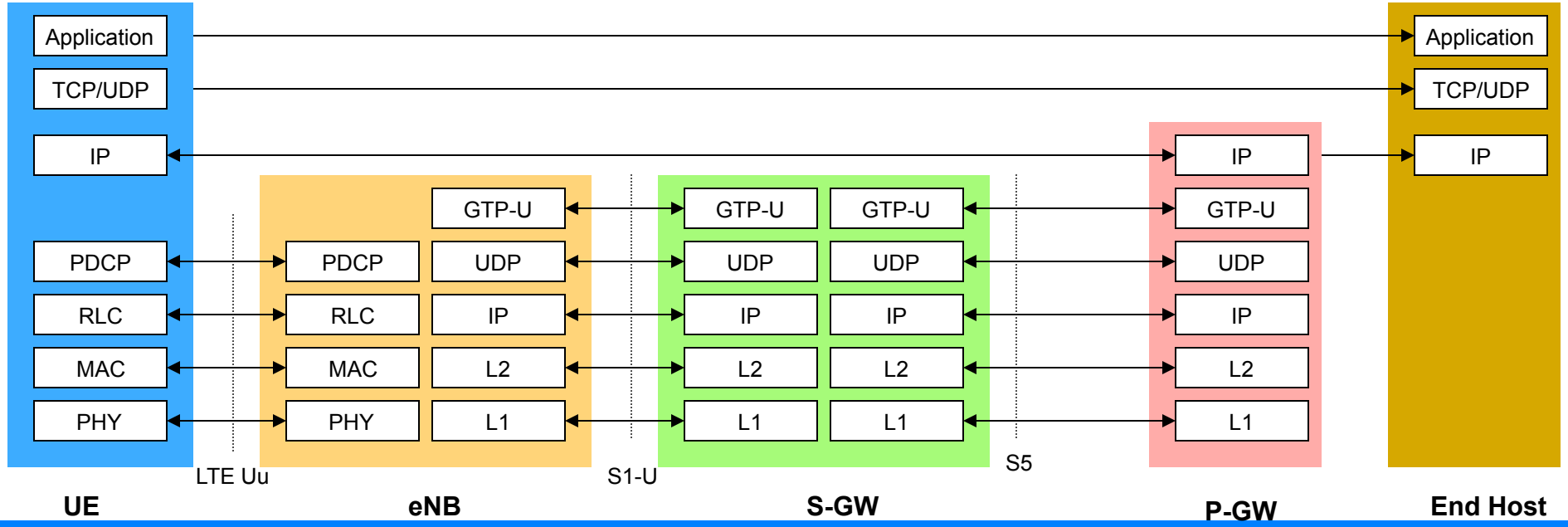
Medium Access Control (MAC): Access the channel

Physical Layer (PHY): Radio layer, eg modulation etc.

S1-AP	S1 Application protocol
SCTP	Stream Control Transport Protocol
GTP-C	GPRS Tunneling Protocol-Control Plane
GTP-U	GPRS Tunneling protocol- User Plane

Protocol Stacks: Control Plane & User Plane

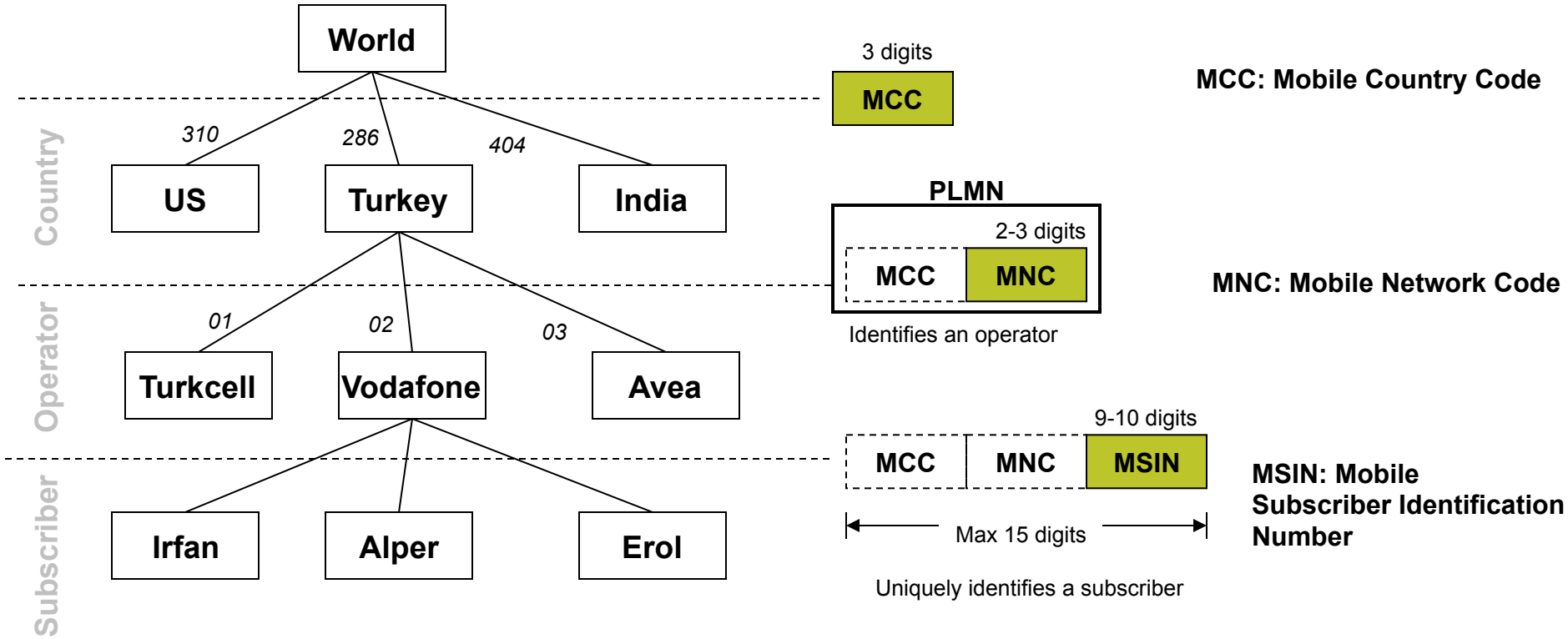




Making/Receiving calls – Call identifiers

- ***Two important identifiers***
  - International Mobile Subscriber Identifier (IMSI)
    - Embedded in SIM card
    - Stored in subscription data of HLR
    - Used to index UE's information in most network nodes
    - Format on next page
  - Mobile Station Integrated Services Digital Network Number (MSISDN)
    - Your phone number
    - Number used to identify a subscriber when making a call or sending an SMS
- ***The mapping between IMSI and MSISDN is stored in HLR***
  - MSISDN is not required to be stored in the SIM.
    - It is often stored in SIM.

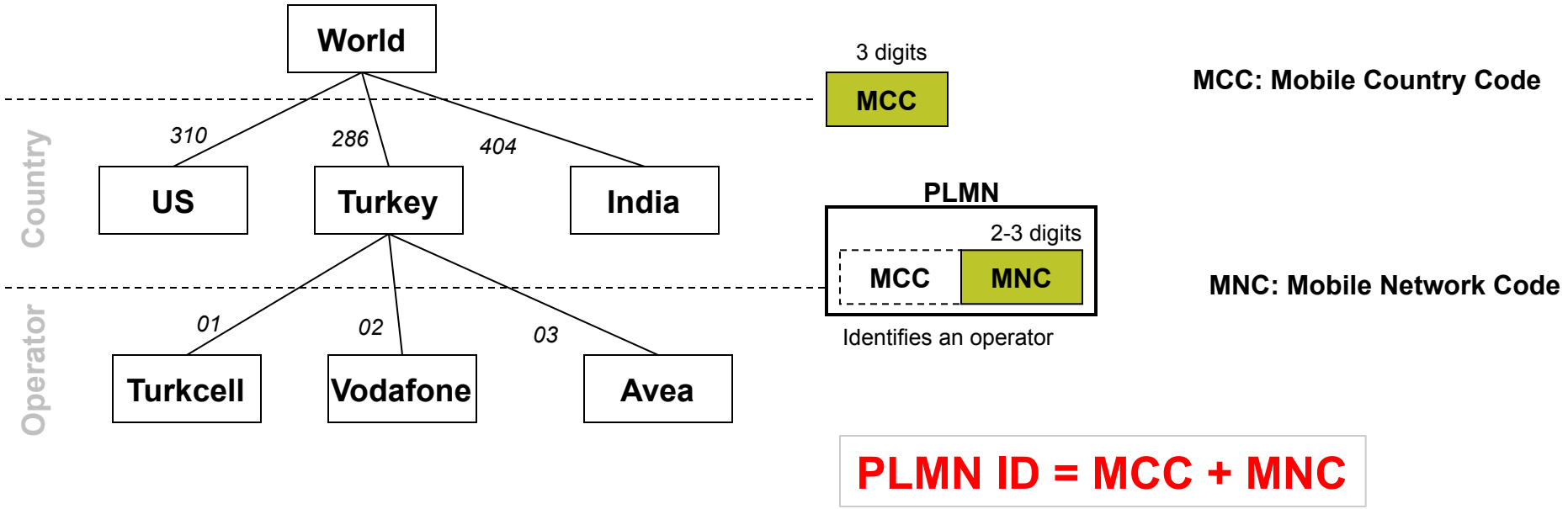
(International Mobile Subscriber Identifier) IMSI - Structure



Source for MCC and MNC codes:
http://en.wikipedia.org/wiki/Mobile_Network_Code
http://en.wikipedia.org/wiki/Mobile_Country_Code

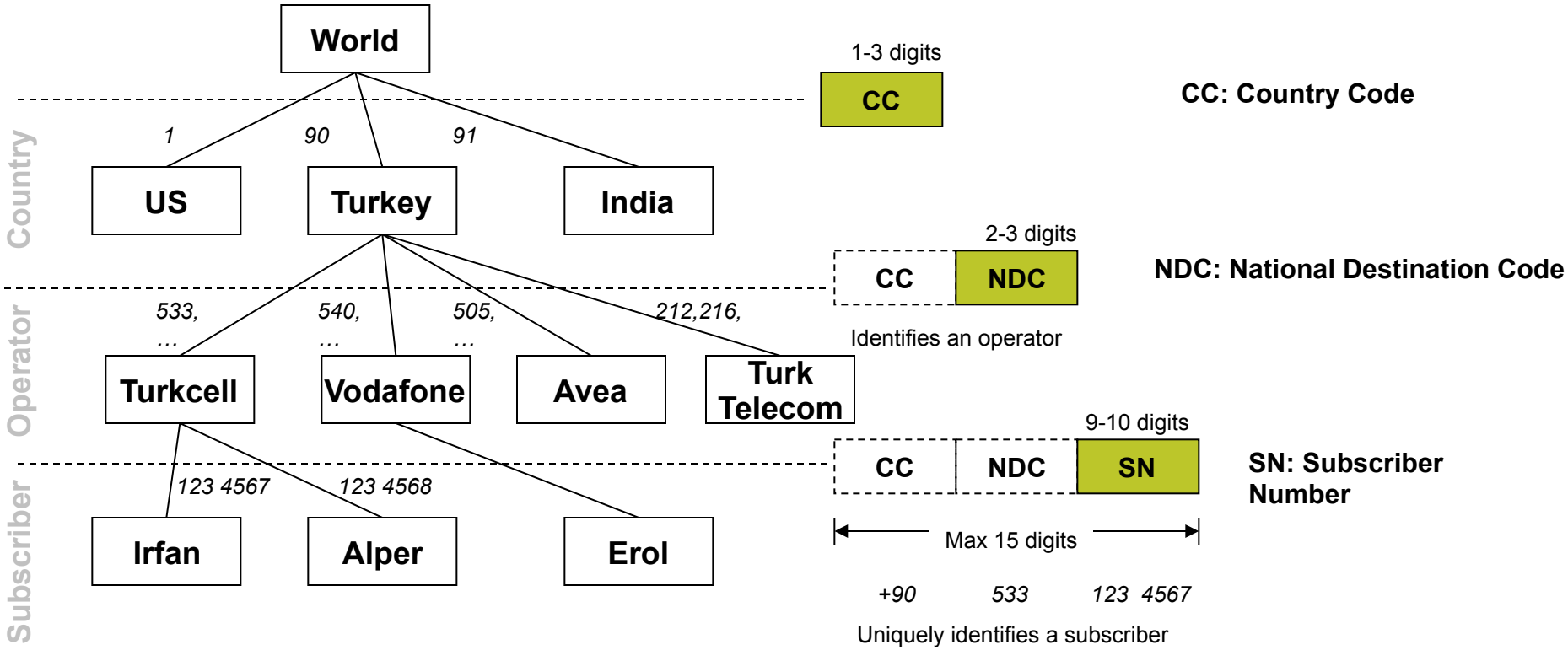
Operator Identity

- ***A mobile operator's network is also known as a Public Land Mobile Network (PLMN).***
- ***The identity used for an operator's network is called the PLMN-Identity (PLMN-ID) and consists of the Mobile Country Code and the Mobile Network Code.***
- ***An operator may be identified by more than one PLMN-ID***



PLMN ID = MCC + MNC

MSISDN – Structure

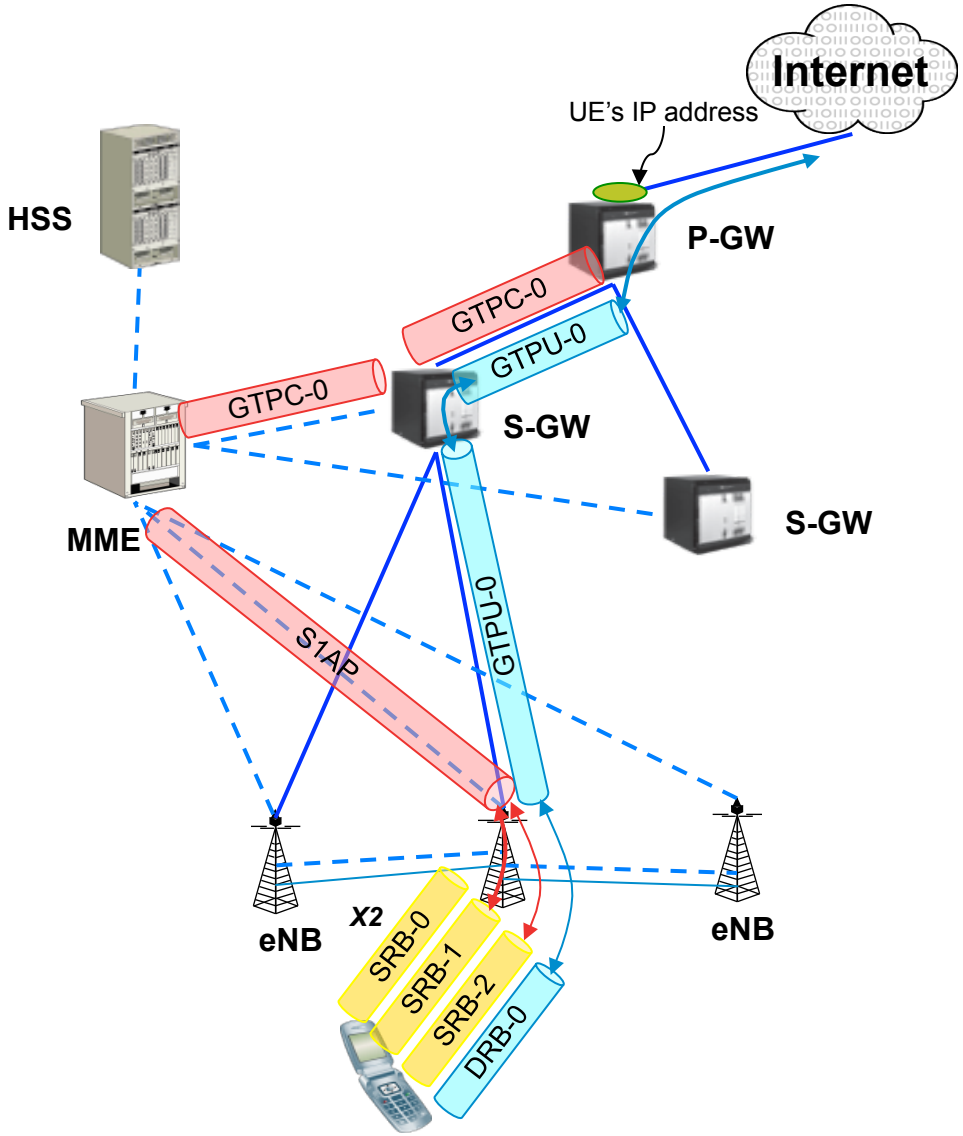


List of country calling codes:
http://en.wikipedia.org/wiki/List_of_country_calling_codes

Source for MCC and MNC codes: www.wikipedia.org

LTE Attach Procedure

Objective of UE Attach Procedure

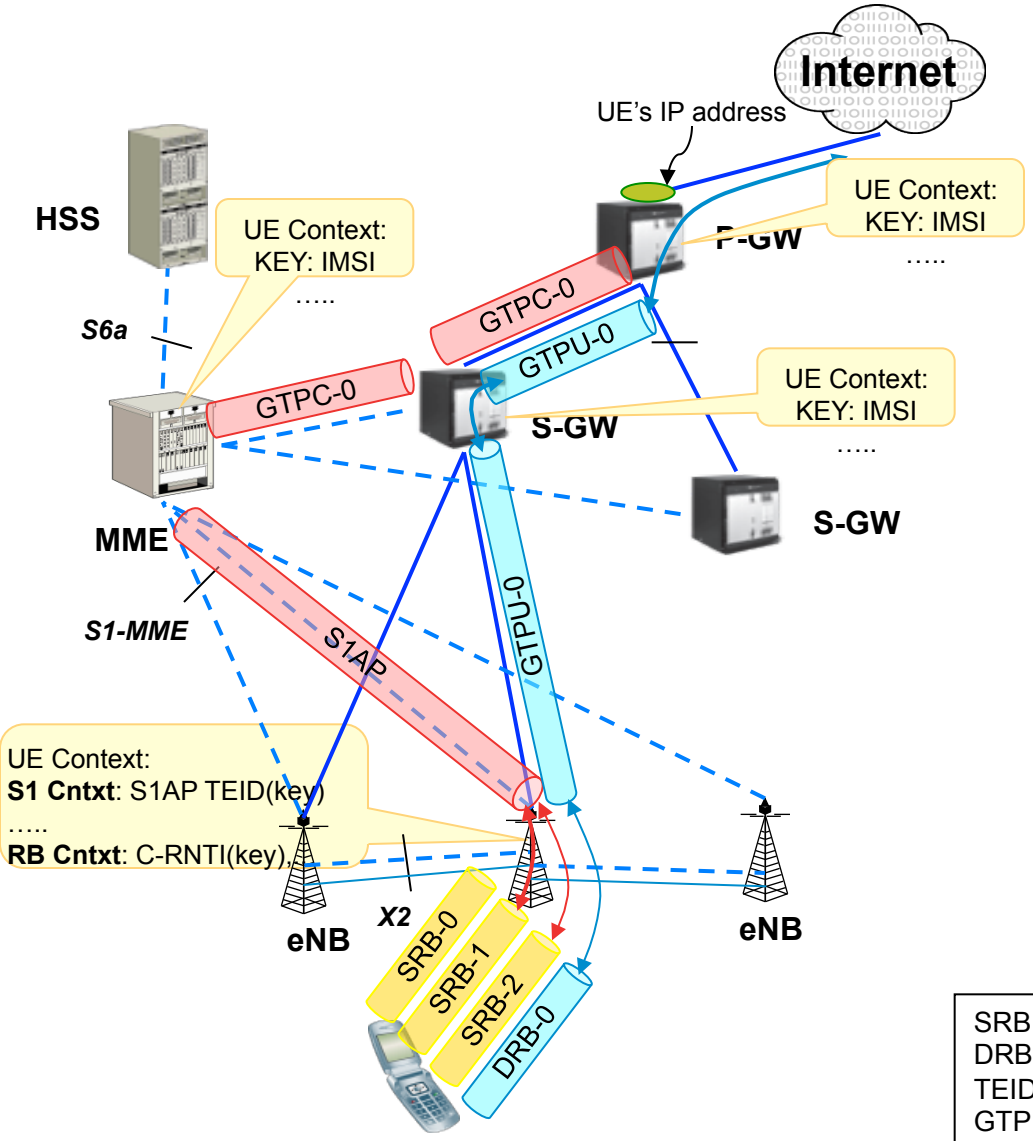


Bearer Setup at end of the Attach Procedure

- ***The goal of "attaching" to the network is to obtain an IP address to communicate with outside world.***
- ***During the process of "attach"***
  - The UE is authenticated and authorized to use send/receive data.
  - Data path created between UE<->eNB<->S-GW<->PGW
  - UE Context created in all the nodes in the network
  - UE is provided an IP address

SRB	Signalling Radio Bearer
DRB	Data Radio Beaer
TEID	Tunnel Endpoint Identifier
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity

Objective of UE Attach Procedure

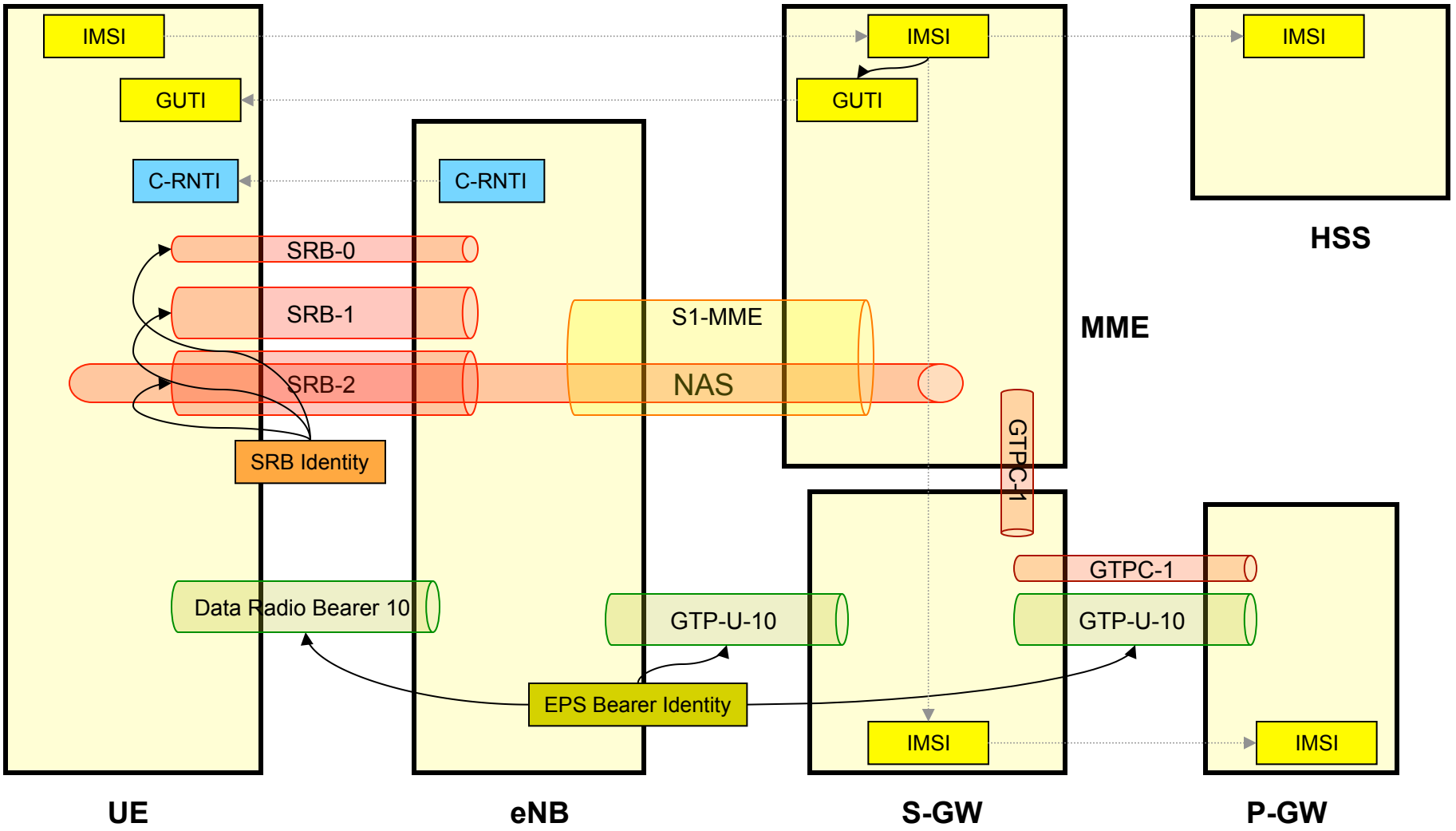


Bearer Setup at end of the Attach Procedure

- ***The goal of "attaching" to the network is to obtain an IP address to communicate with outside world.***
- ***During the process of "attach"***
  - The UE is authenticated and authorized to use send/receive data.
  - Data path created beteween UE<->eNB<->S-GW<->PGW
  - UE Context created in all the nodes in the network
  - UE is provided an IP address

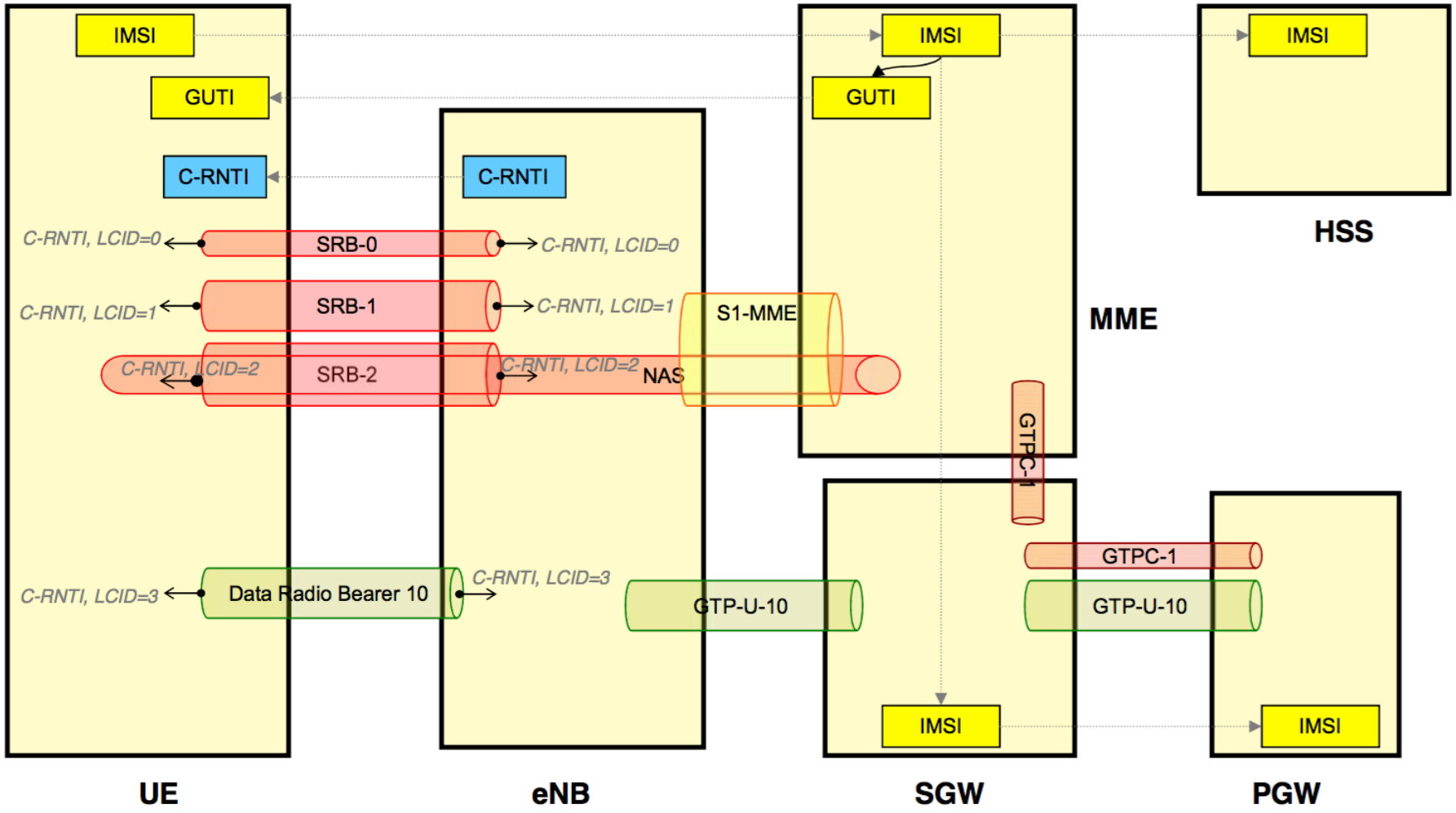
SRB	Signalling Radio Bearer
DRB	Data Radio Beaer
TEID	Tunnel Endpoint Identifier
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity

Identities and Plumbing for LTE



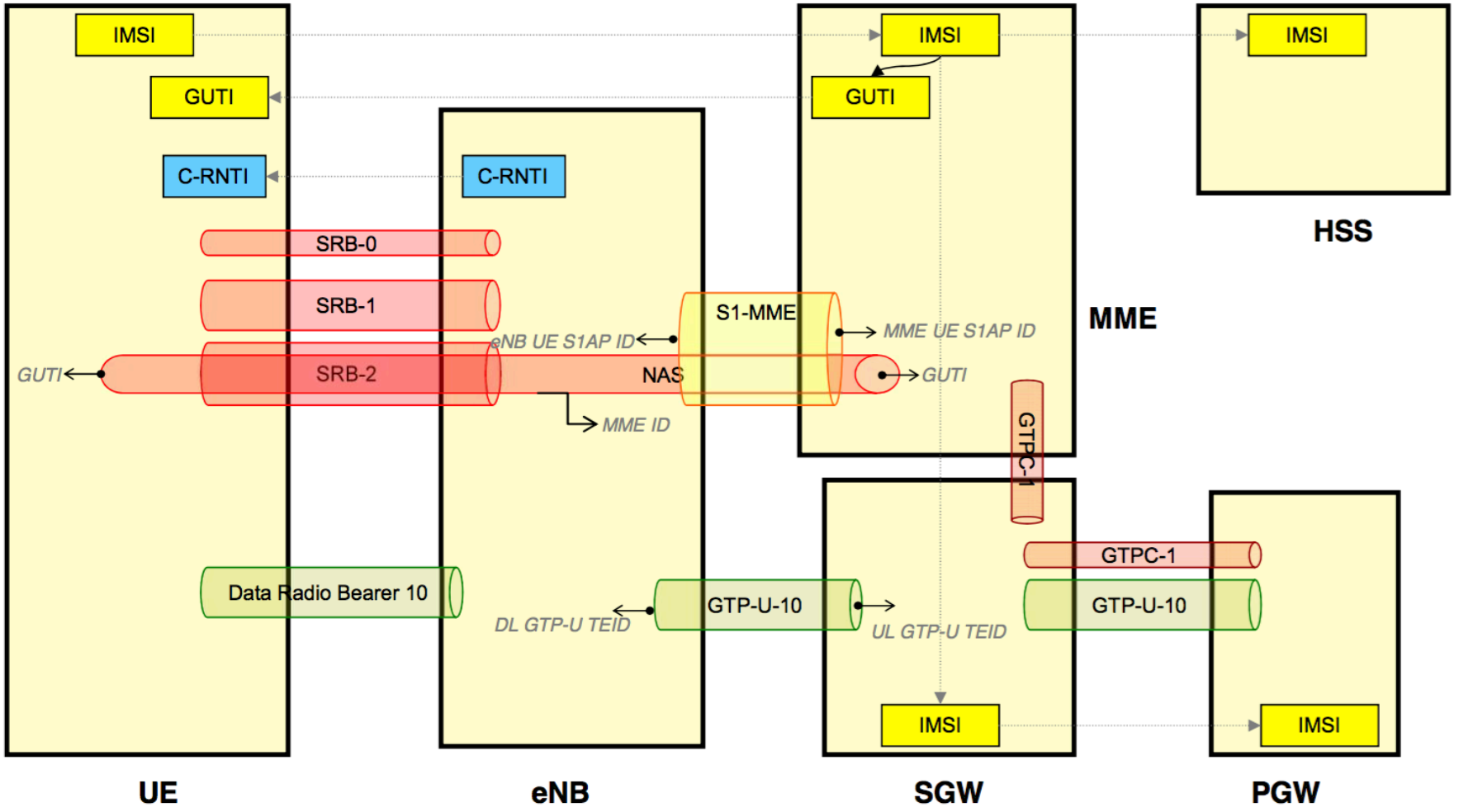
SRB	Signalling Radio Bearer
DRB	Data Radio Beaer
TEID	Tunnel Endpoint Identifier
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity
GUTI	Globally Unique Temporary Identity

Identities on the Radio-interface



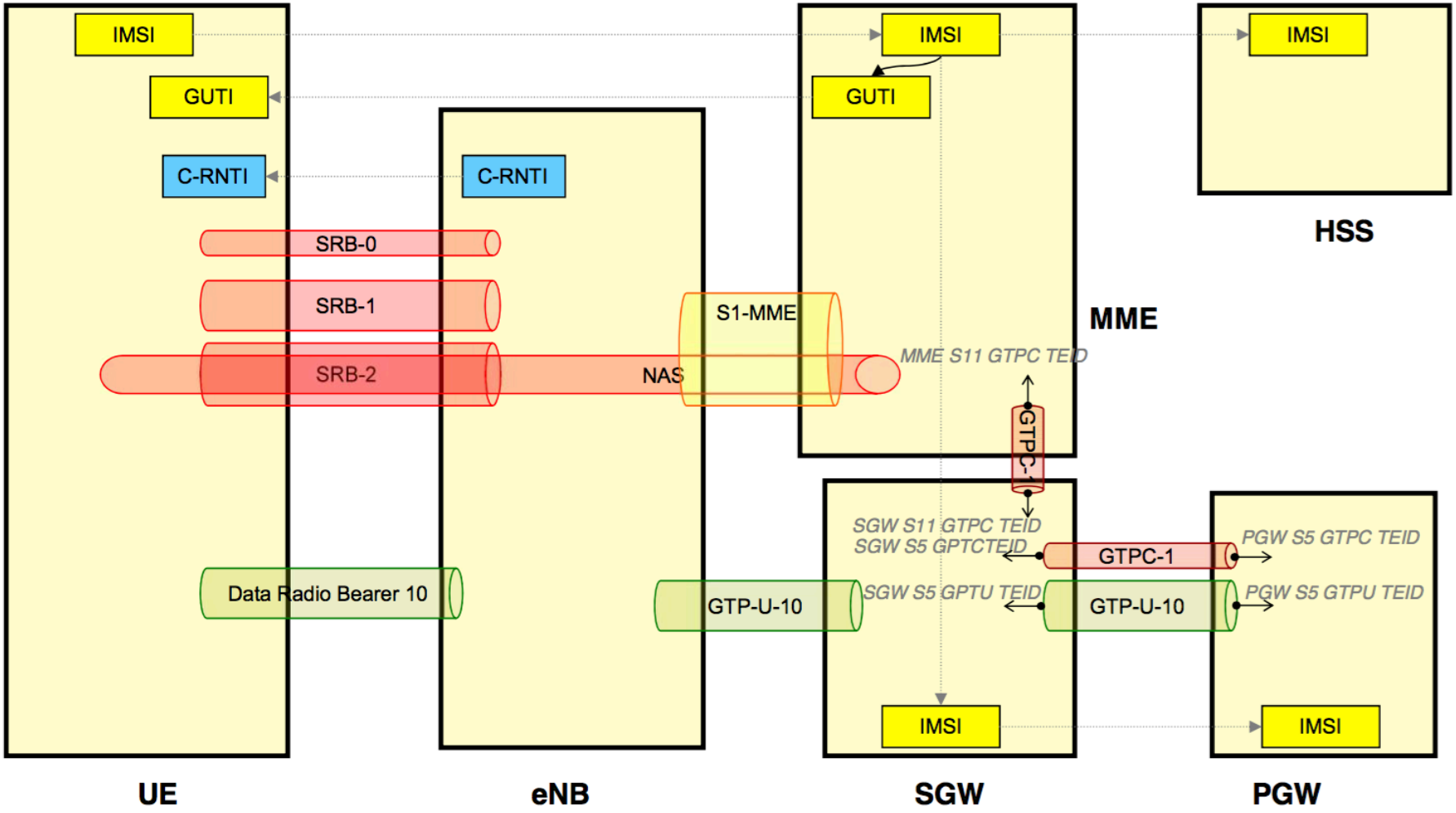
SRB	Signalling Radio Bearer
DRB	Data Radio Beaer
TEID	Tunnel Endpoint Identifier
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity
GUTI	Globally Unique Temporary Identity

Identities for the Backhaul (S1AP and S1U)



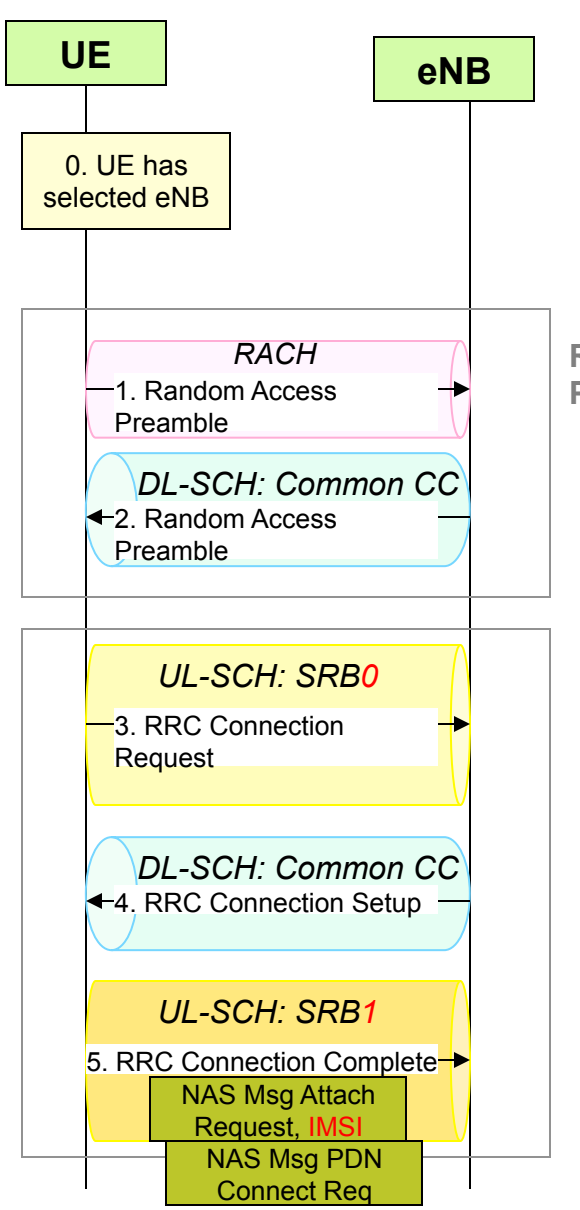
SRB	Signalling Radio Bearer
DRB	Data Radio Beaer
TEID	Tunnel Endpoint Identifier
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity
GUTI	Globally Unique Temporary Identity

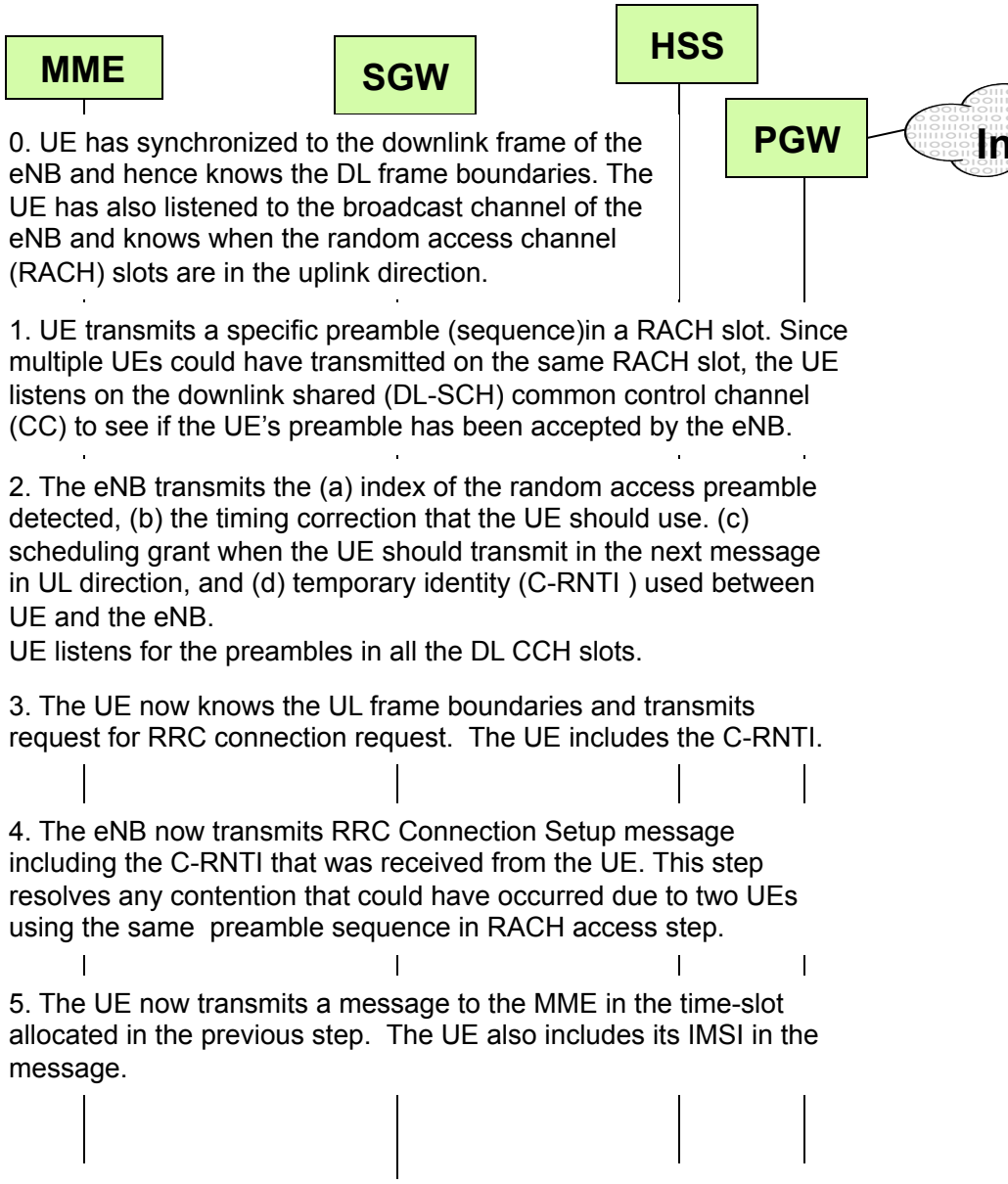
Identities in the Core Network (S11 and S5)



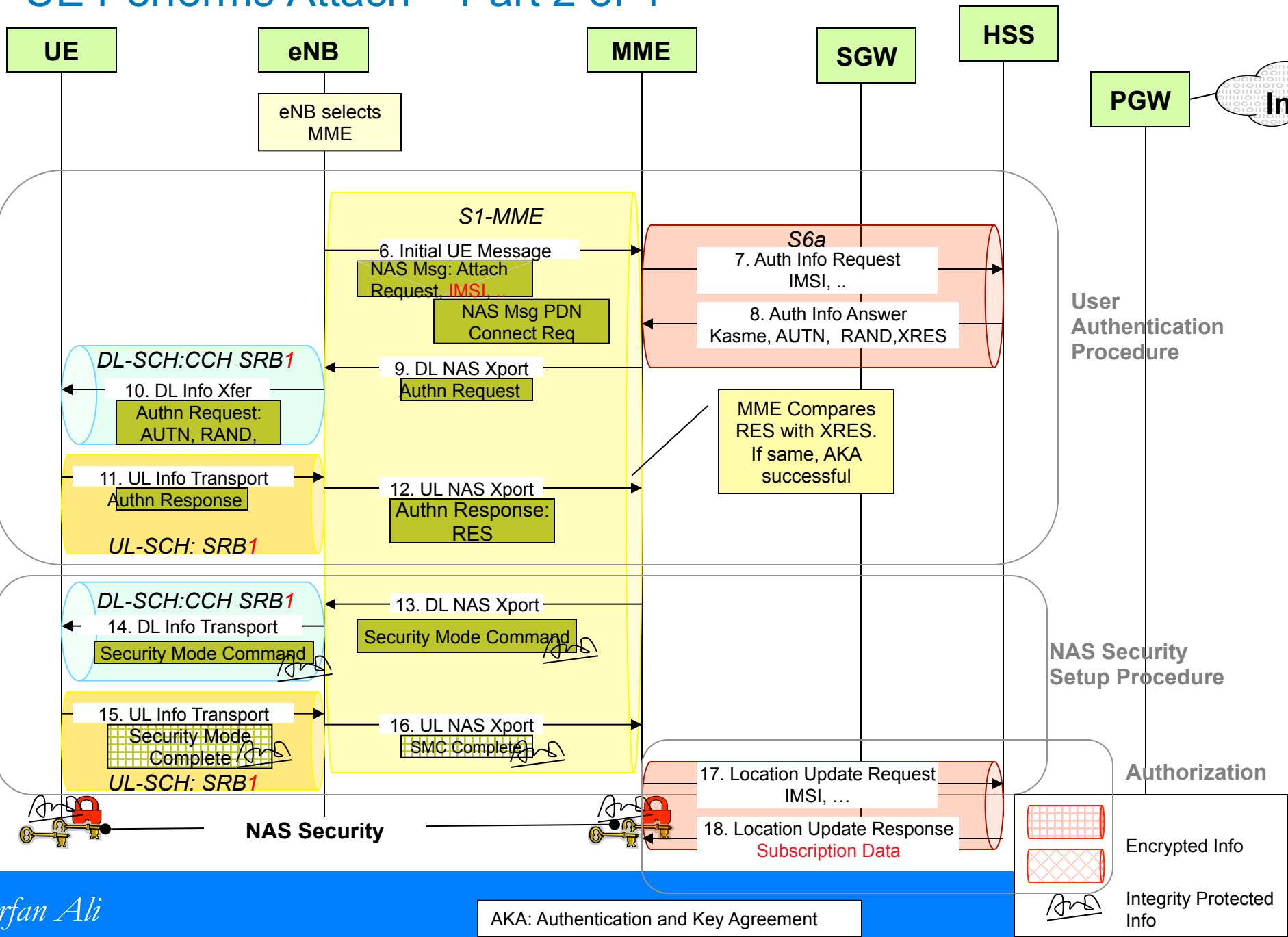
SRB	Signalling Radio Bearer
DRB	Data Radio Beaer
TEID	Tunnel Endpoint Identifier
GTP	GPRS Tunneling Protocol
C-RNTI	Cell- Radio Network Temporary Identity
GUTI	Globally Unique Temporary Identity

UE Performs attach – Part 1 of 4

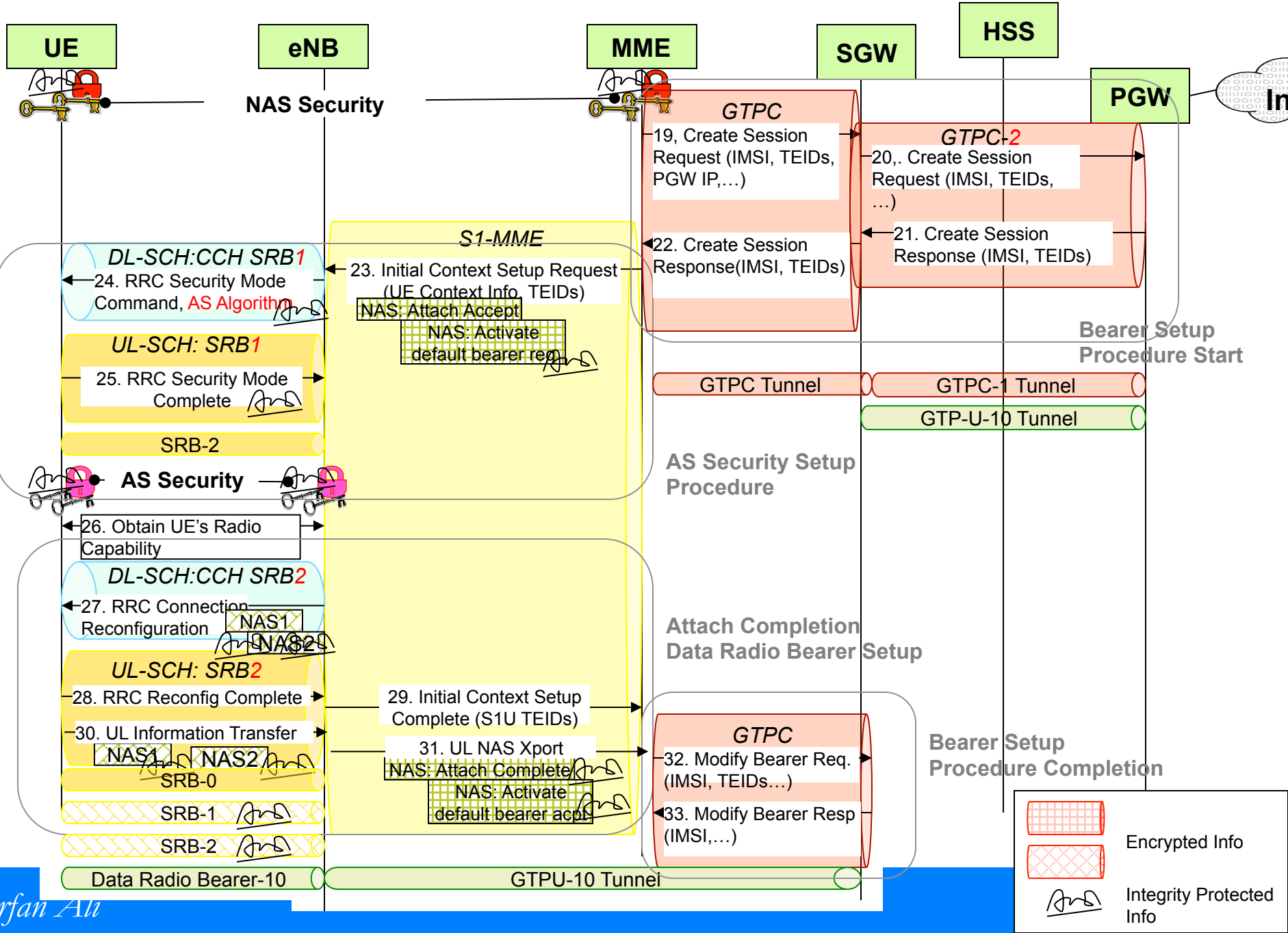




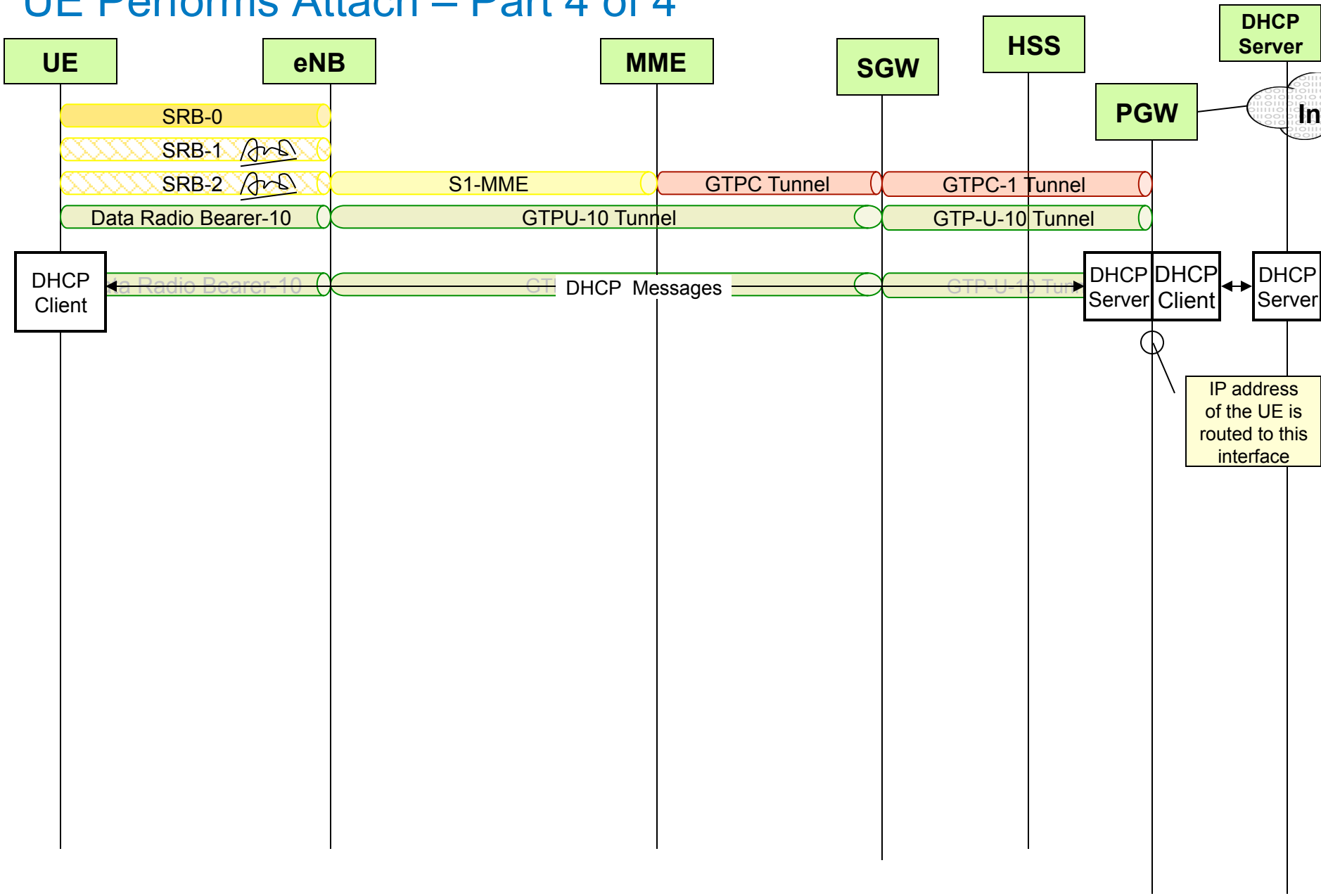
UE Performs Attach – Part 2 of 4



UE Performs Attach – Part 3 of 4



UE Performs Attach – Part 4 of 4

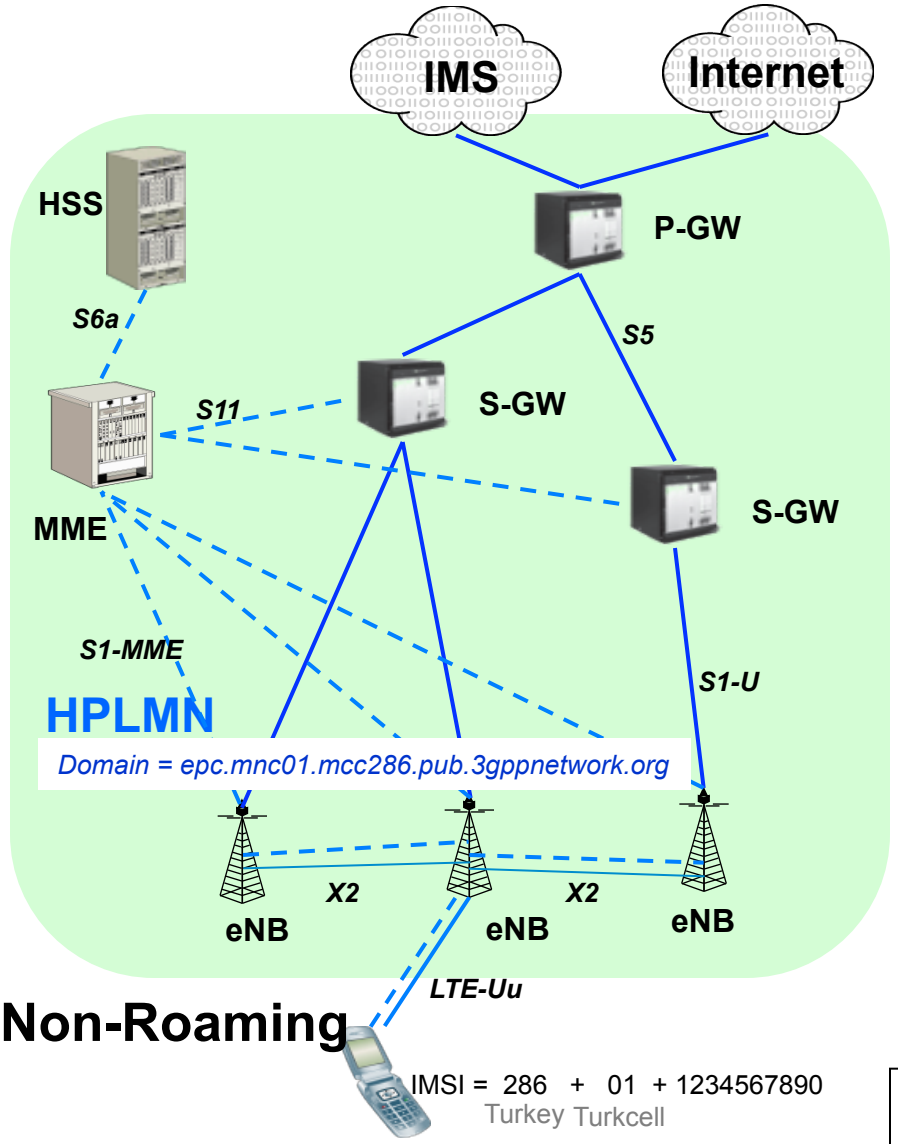


Architecture key Concept: Roaming

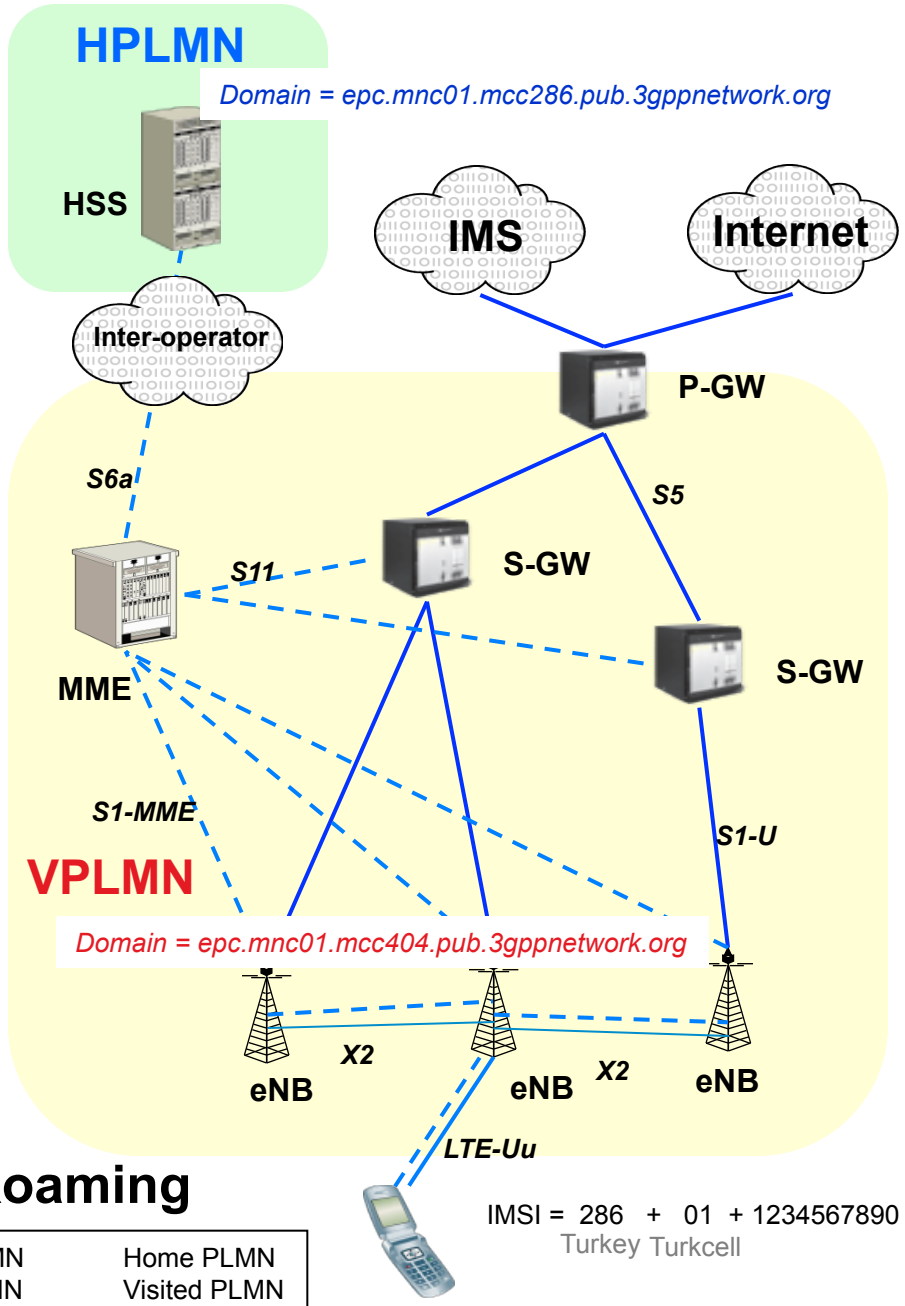
- ***3GPP architecture from early days has supported a subscriber going to a foreign network and still getting service***
  - Home PLMN: Subscriber's home network (eg. Turkcell)
  - Visited PLMN: Foreign/Roamed-to network (eg. Orange)
- ***What does roaming require:***
  - Ability from VPLMN to identify the HPLMN of the subscriber
  - Ability to authenticate the subscriber from VPLMN
  - Sharing of revenue between VPLMN and HPLMN (roaming charges)

PLMN	Public Land Mobile Network
VPLMN	Visited PLMN
HPLMN	Home PLMN

Roaming Architecture



Non-Roaming

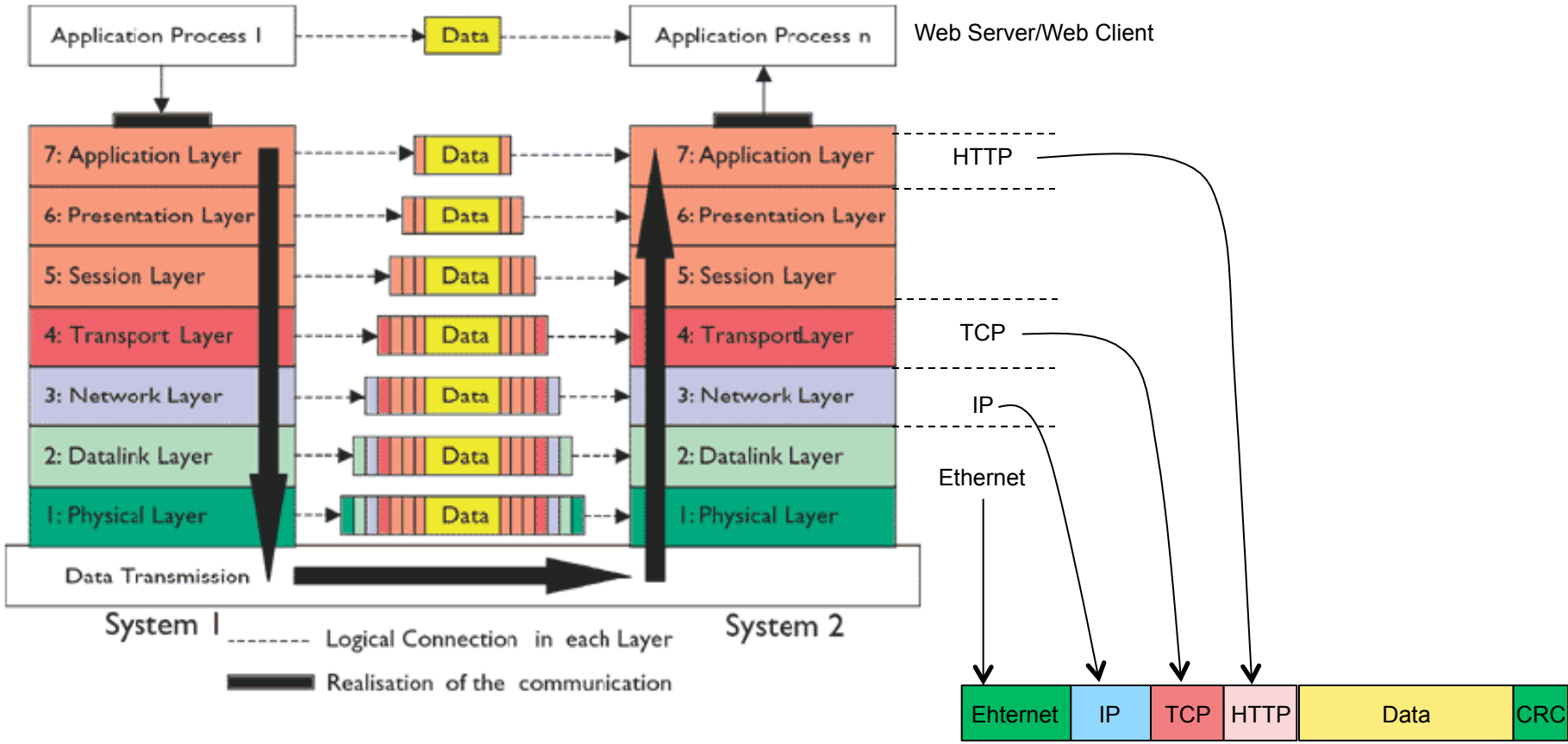


Roaming

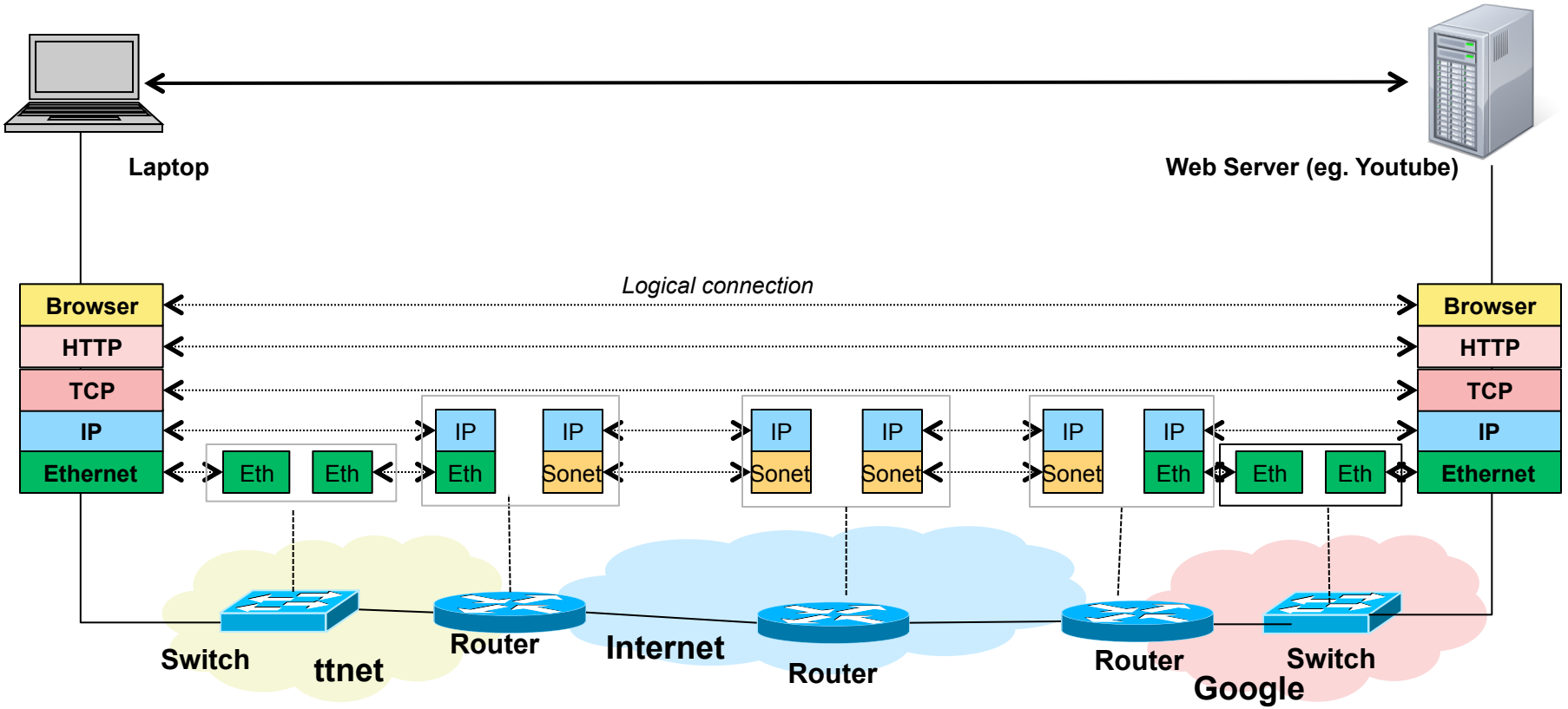
HPLMN	Home PLMN
VPLMN	Visited PLMN

IP ADDRESSING AND ADDRESS SUMMARIZATION

Protocol Stack and Bits on the Wire



Protocol Stack and Processing on the Path

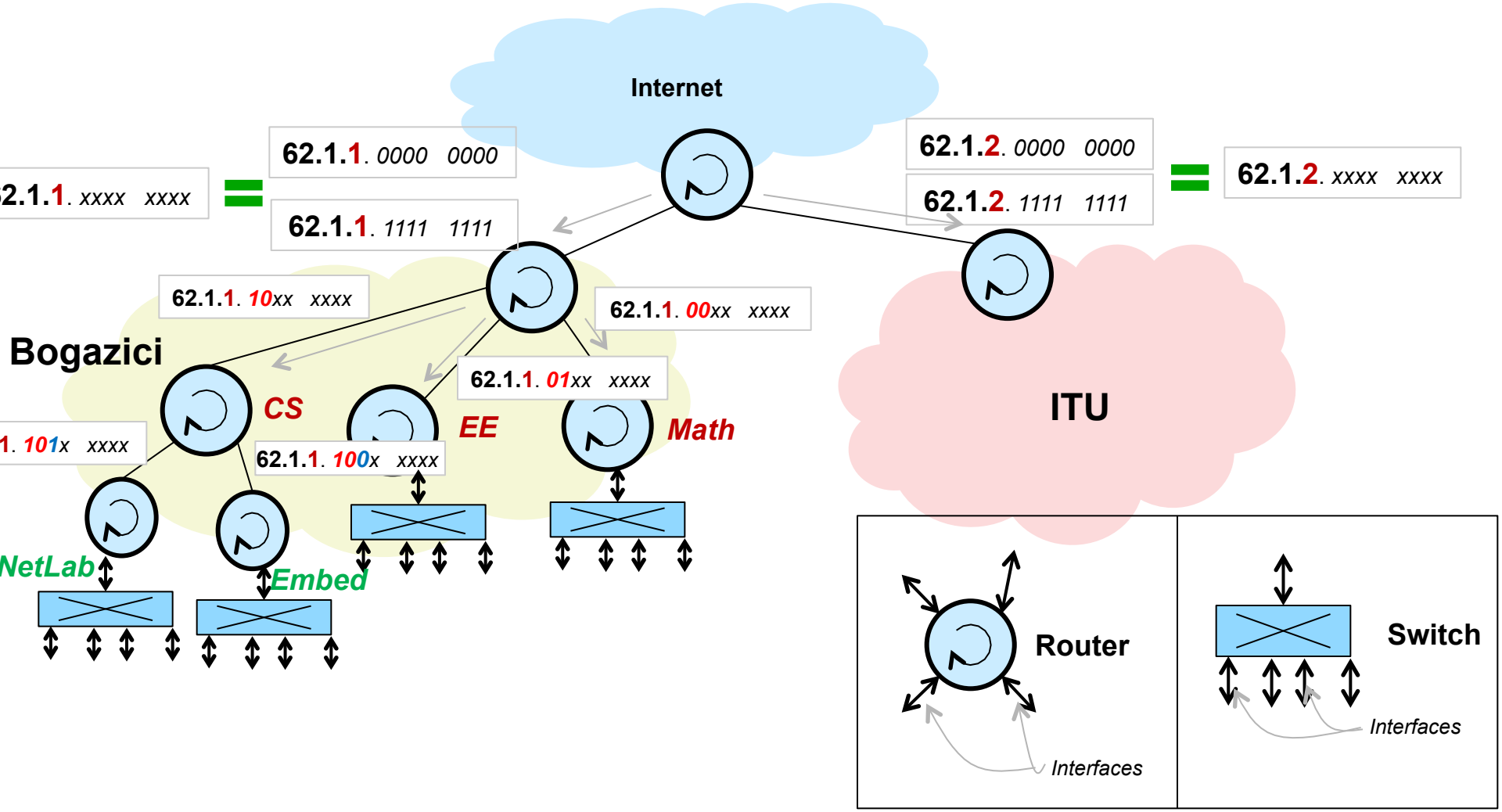


- *Protocol Stacks are at interfaces*
- *Layer 4 and above are end-to-end logical connections*
- *Layer 3 is processed by routers on the path. So this is a hop-by-hop logical connection*
- *Layer 2 and Layer 1 are link-by-link logical connections.*

IP Address

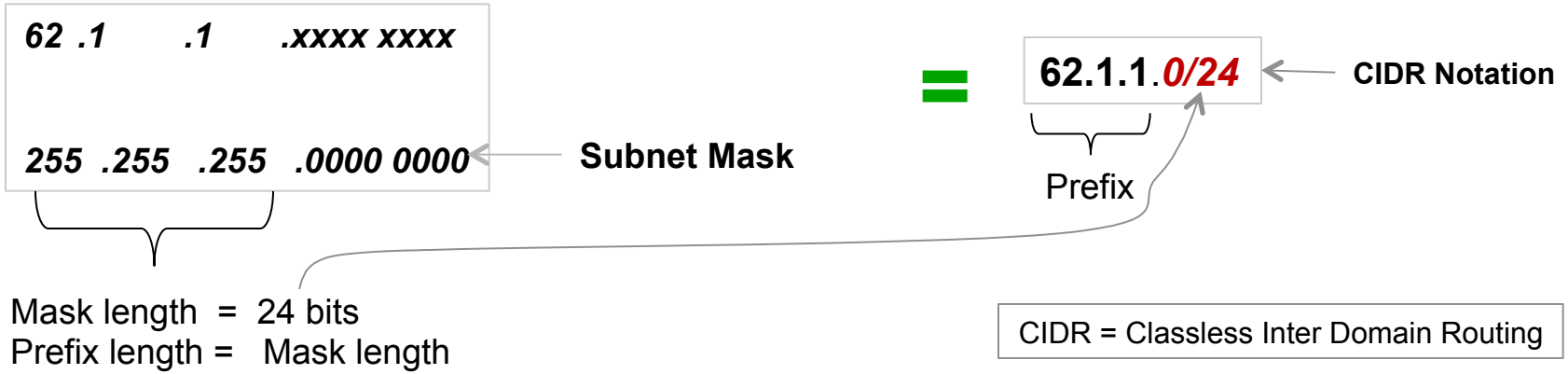
- ***IP Address is a 32 bit number***
  - 2^32 addresses = ~ 4 billion (9 zeros) address
  - Typically represented as in the following form “192.168.2.5”, each digit representing eight bits (0-255).
- ***Routing in the Internet is based on IP addresses***
  - Each IP packet has an IP address.
  - Actually, two: Source IP address and Destination IP address
- ***Routing on your campus address is also based on IP addresses***
  - The principles of routing are the same, though the routing protocols used differ.
- ***IP routing depends on good IP address summarization.***
- ***We will consider a campus address to explain IP address summarization***
- ***IP address summarization and concept of subnets will be used when studying mechanisms to support IP mobility***

IP Address Summarization Goal



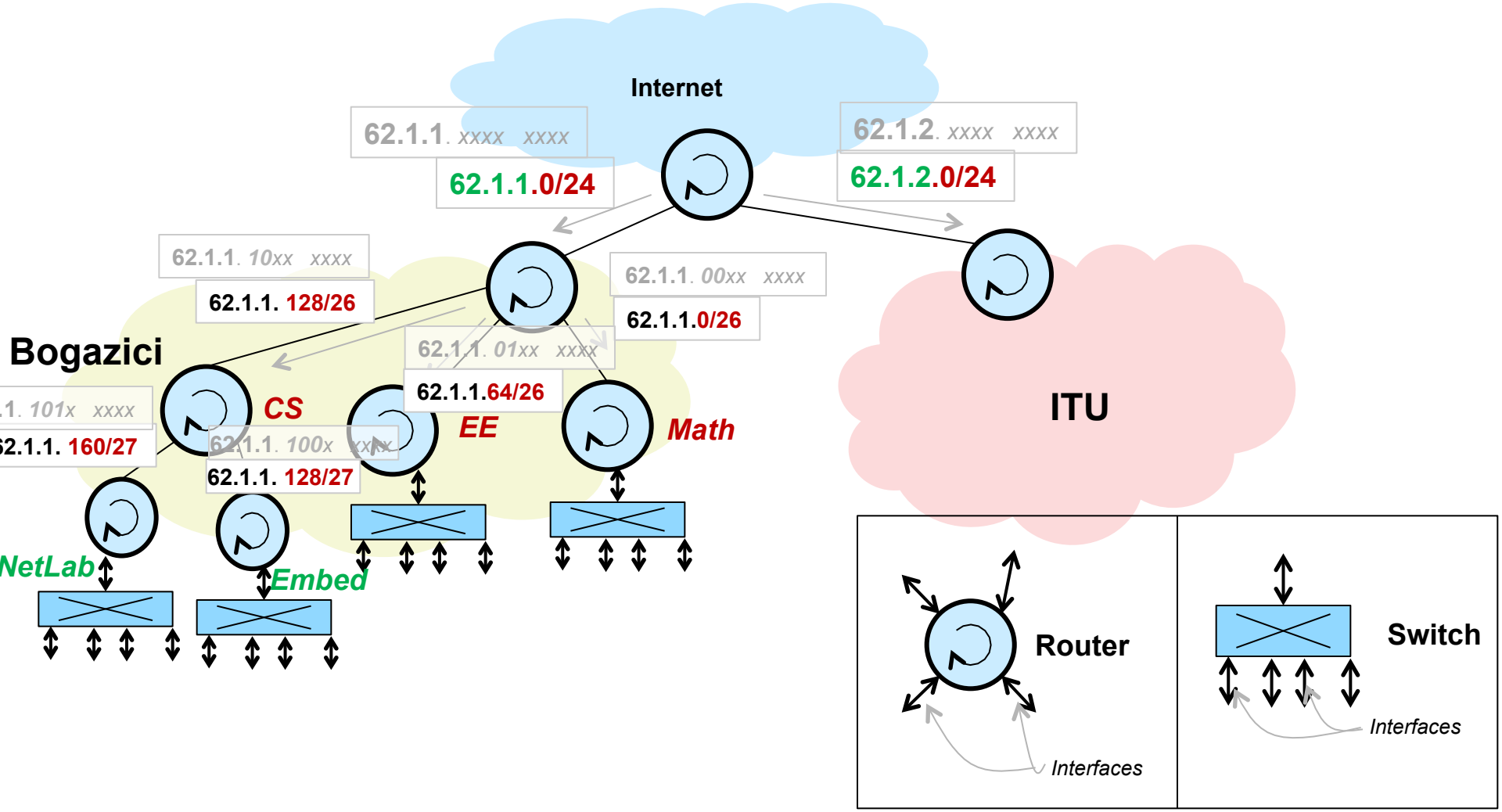
- *IP Address Summarization makes routing decisions easier for a router*
- *It converts your IP address into a hierarchical map: internet -> bogazici -> cs -> netlab -> Emre*

IP Address Summarization: Subnet mask and Address/ Prefix notation



- *The "all zeros" address (62.1.1.0) of a subnet is not provided to any host. It is called the subnet ID.*
- *The "all ones" address (62.1.1.255) of a subnet is not provided to any host. It is the broadcast address in the subnet.*
- *Hence, a subnet with n bits of addresses contain (2^n – 2) host addresses.*
- *If you take an IP address and AND it with the subnet mask, you get the prefix (subnet ID) of the subnet*

IP Address Allocation using CIDR notation



- ***CIDR notation makes it easier to show subnets in an IP network***
- ***The subnet mask become bigger as you go lower down in the network hierarchy.***