Introduction to Mobile Networks

Introduction to Cellular Mobile Networks

Dr. Shahriar Bijani

Shahed University
Faraconesh Co.

Main References

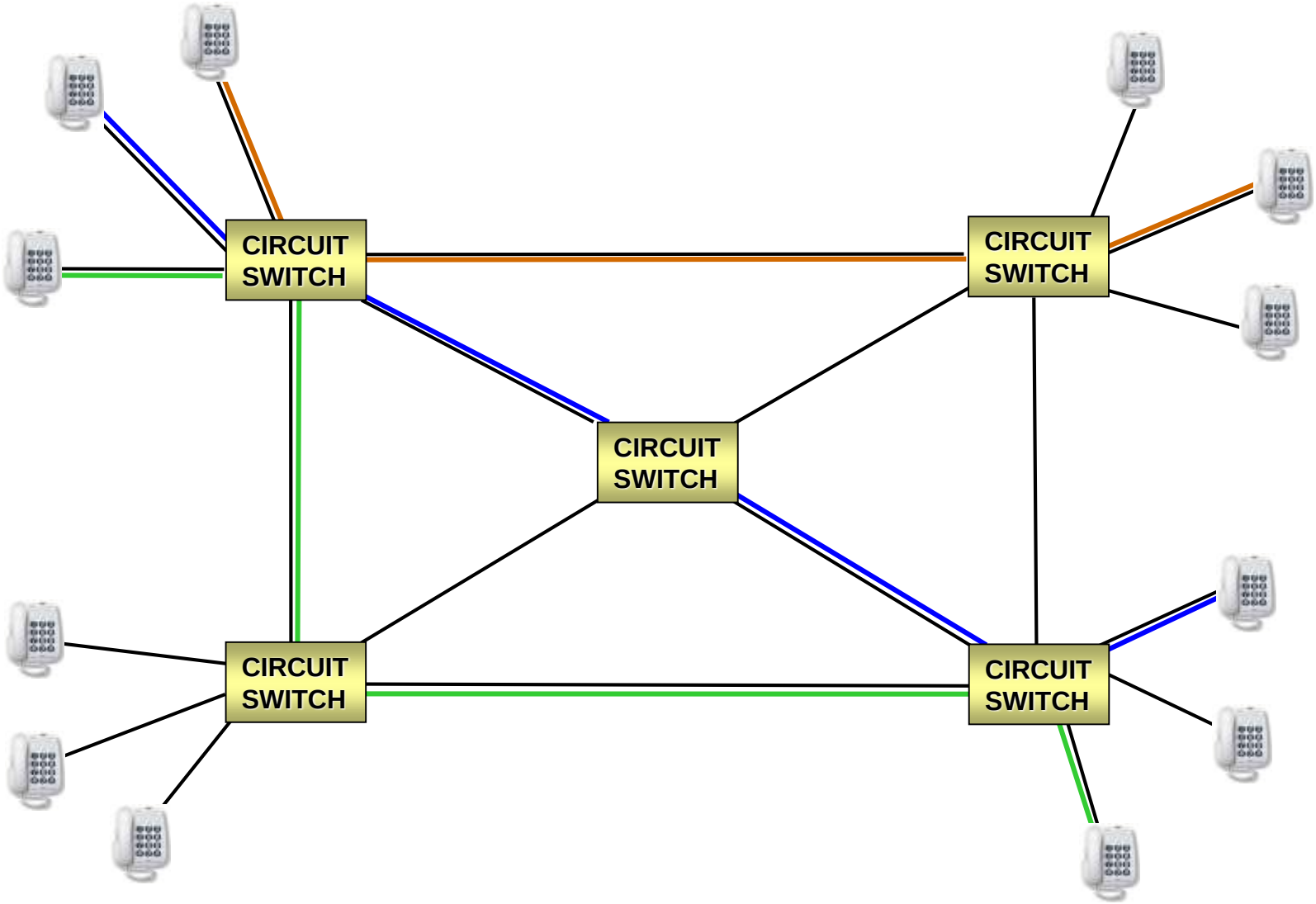
- A. S. Tanenbaum and D. J. Wetherall, **Computer Networks** (5th Edition), Pearson Education, 2011.
- Patrick Traynor, CS 8803 - **Cellular and Mobile Network Security**, Georgia Tech Information Security Center, 2012.
- **General Packet Radio Service (GPRS) For Engineers**, Aircom International.
- ICS 243E - Ch4. Wireless Telecomm. Sys.
- Justin Champion, **Mobile Computing Systems: UMTS**, Staffordshire University, UK.
- Tony Sung, **3rd Generation WCDMA / UMTS Wireless Network**, MC Lab, IE CUHK, 2003.
- Kari Aho,**Wideband Code Division Multiple Access** (WCDMA) for UMTS, Magister

Introduction

- Circuit vs. Packet Switching
- Multiplexing
- Mobile Phone Standards

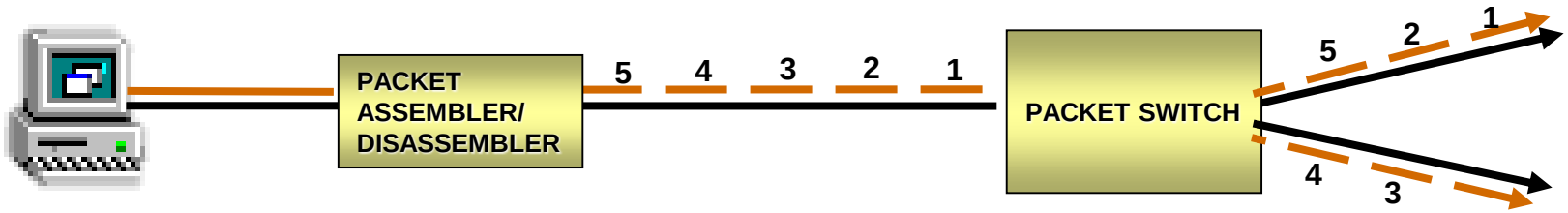
Dr Shahriar Bijani, www.faraconesh.com

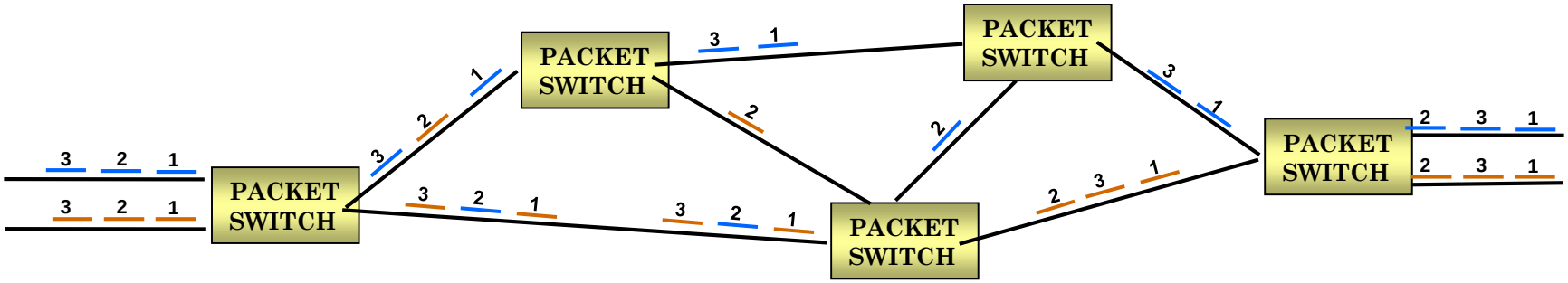
Circuit Switching



Dr Shahriar Bijani, www.faraconesh.com

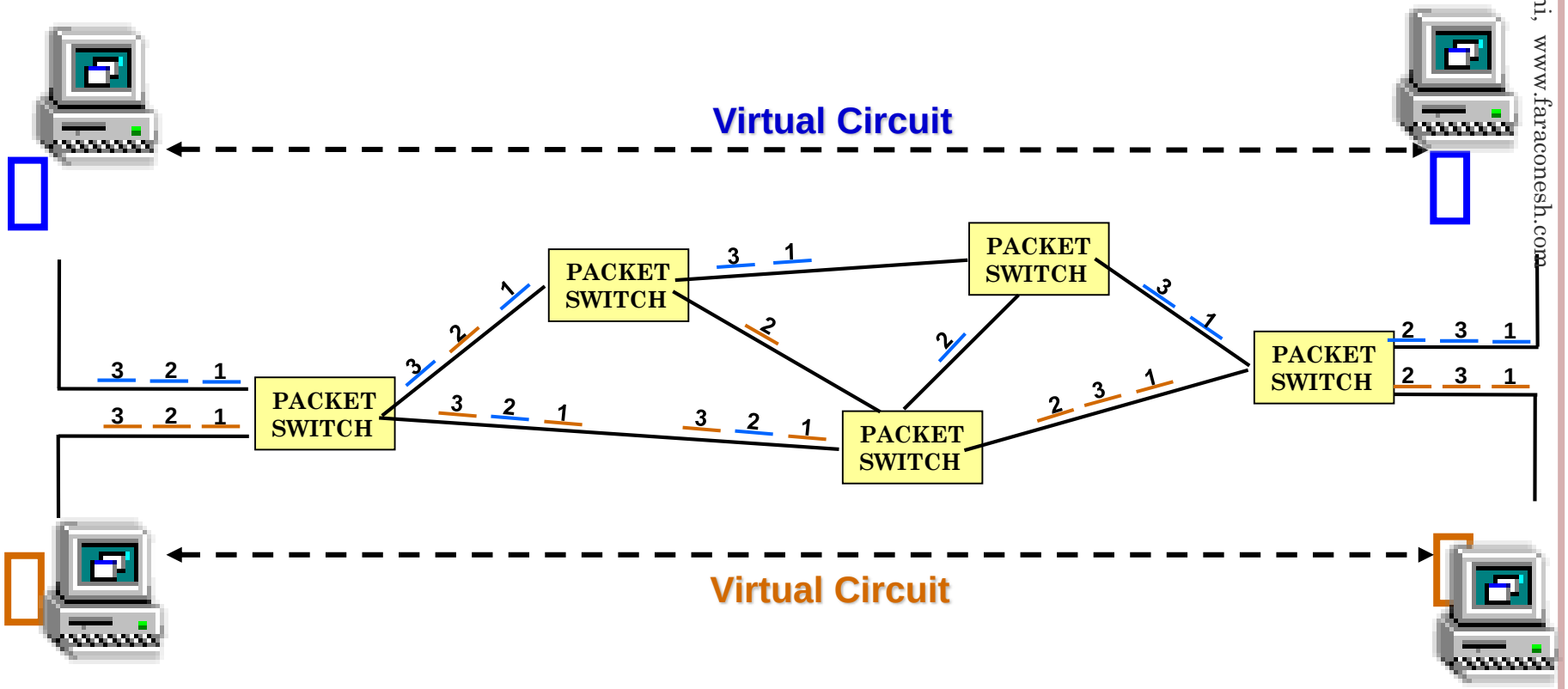
PACKET SWITCHING





Dr Shahriar Bijani, www.faraconesh.com

The Virtual Circuit (VC) Concept



Dr Shahriar Bijani, www.faraconesh.com

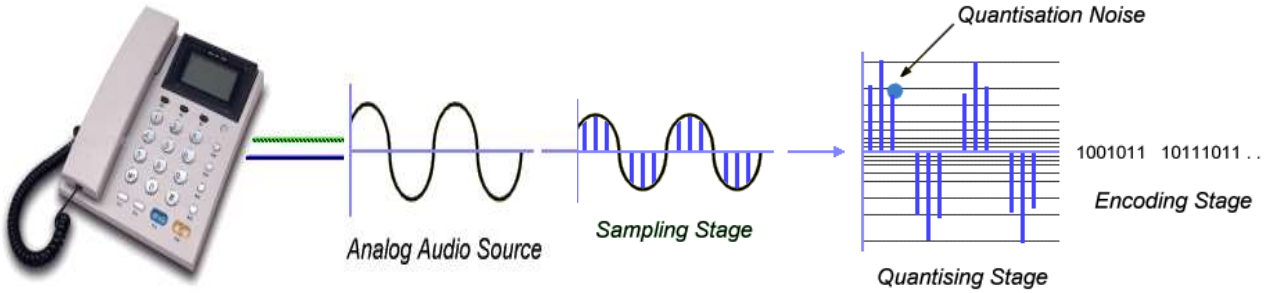
Virtual Circuit Connections

- Permanent Virtual Circuit (PVC):
  - Established by NMC
  - Dedicated resource for specific user
  - Connectionless
- Switched Virtual Circuit (SVC):
  - Setup on request
  - Temporary allocation of resources
  - Cleared on completion of session

Dr Shahriar Bijani, www.faraconesh.com

Modulation & Multiplexing

- **Modulation:** To send digital information, we must change analog signals to represent bits.
  - includes:
    - sampling
    - quantizing
    - Encoding



  - Example: PCM (**Pulse Code Modulation**)
    - the simplest form of *speech coding*
    - 2 standards: *A-law* in Europe (24-channels), and *μ-law* in the USA (30/32 channels).

- **Multiplexing:** sharing one channel by multiple signals
- Using a single channel (wire) to carry several signals is better than to allocate a channel (install a wire!) for every signal.

Dr Shahriar Bijani, www.faraconesh.com

Multiplexing

- Different multiplexing methods:
  - **Frequency Division Multiplexing (FDM)**
  - **Time Division Multiplexing (TDM)**
  - **Code Division Multiplexing (CDM)**
  - **Beam Division Multiplexing (BDM)**

Dr Shahriar Bijani, www.faraconesh.com

Frequency Division Multiplexing (FDM)

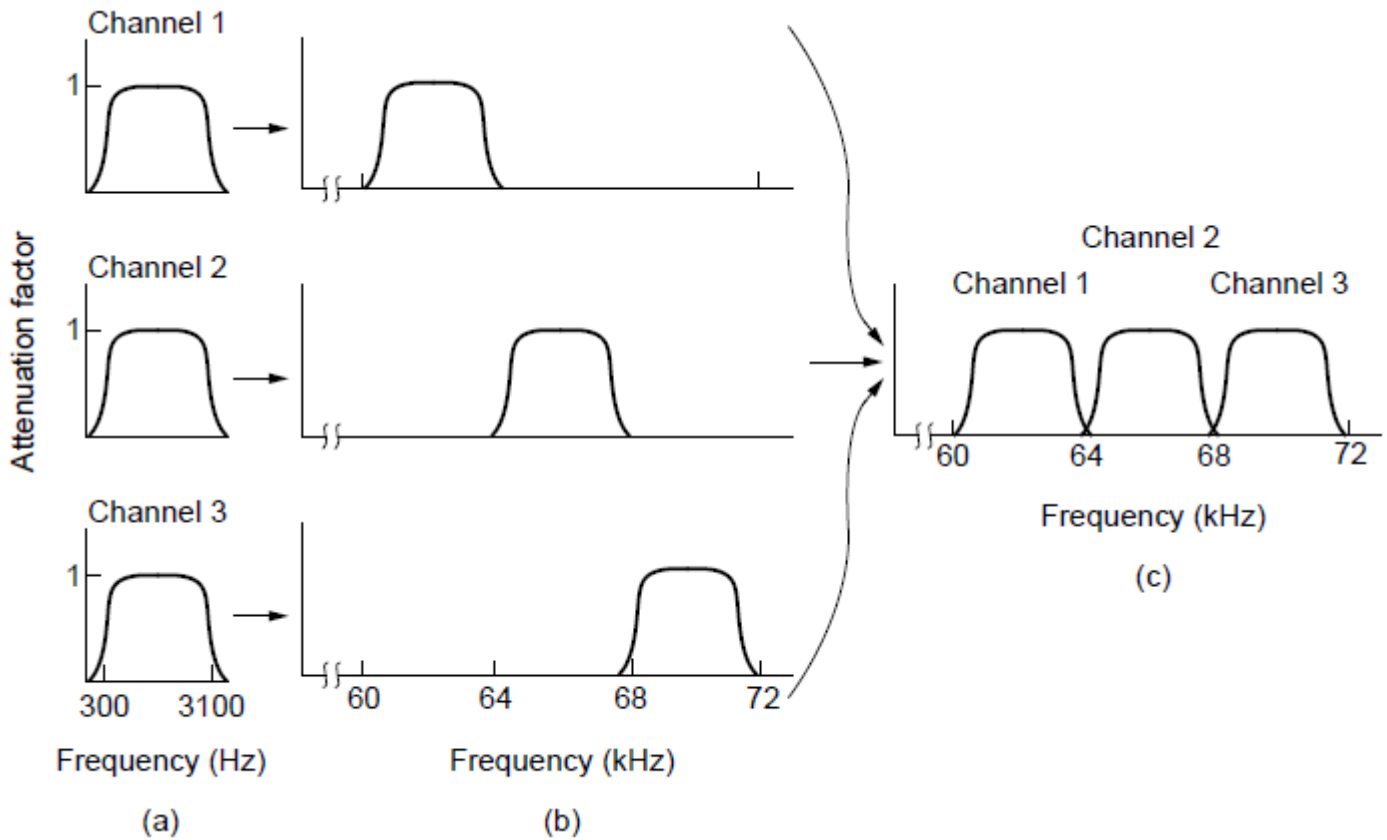
- AKA: **Frequency Division Multiple Access (FDMA)**

- FDM:
  - divides the spectrum into frequency bands
  - each user having exclusive ownership of some band to send their signal.

- **E.g.**: **AM radio**.
  - The allocated spectrum is about 1 MHz (~ 500 to ~1500 kHz)
  - Different frequencies are allocated to different logical channels (stations)

Dr Shahriar Bijani, www.faraconesh.com

Frequency Division Multiplexing (FDM)

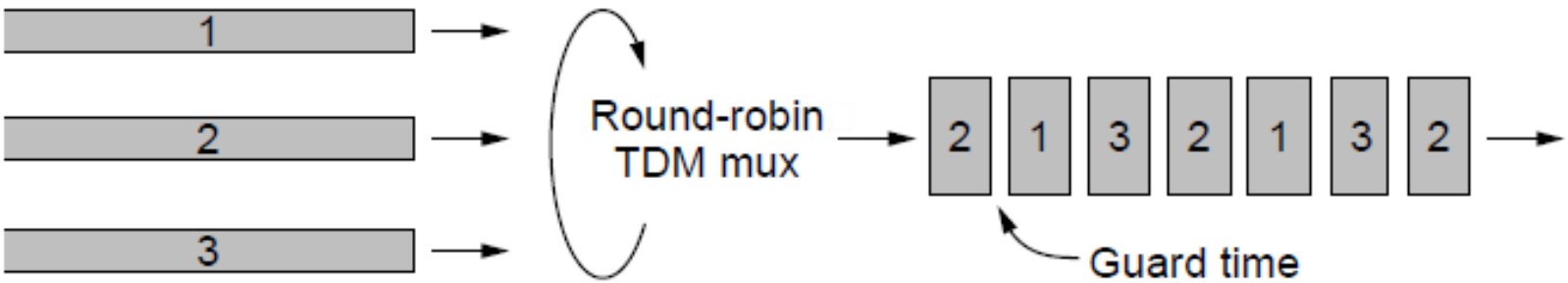


(a) The original bandwidths.
(b) The bandwidths raised in frequency.
(c) The multiplexed channel.

Dr Shahriar Bijani, www.faraconesh.com

Time Division Multiplexing (TDM)

- AKA: **Time Division Multiple Access (TDMA)**
- TDM is used widely as part of the telephone and cellular networks.



- **TDM** is different from STDM.
- **STDM (Statistical Time Division Multiplexing):**
  - Channel is allocated according to the statistics of each stream's demand
  - *STDM is packet switching*.

Dr Shahriar Bijani, www.faraconesh.com

Code Division Multiple Access (CDM)

- AKA: **Code Division Multiple Access (CDMA)**

- Narrowband signal is spread over a wider frequency band.

- Advantages:
  - More tolerant of interference,
  - Allowing multiple signals from different users to share the same frequency band.

Dr Shahriar Bijani, www.faraconesh.com

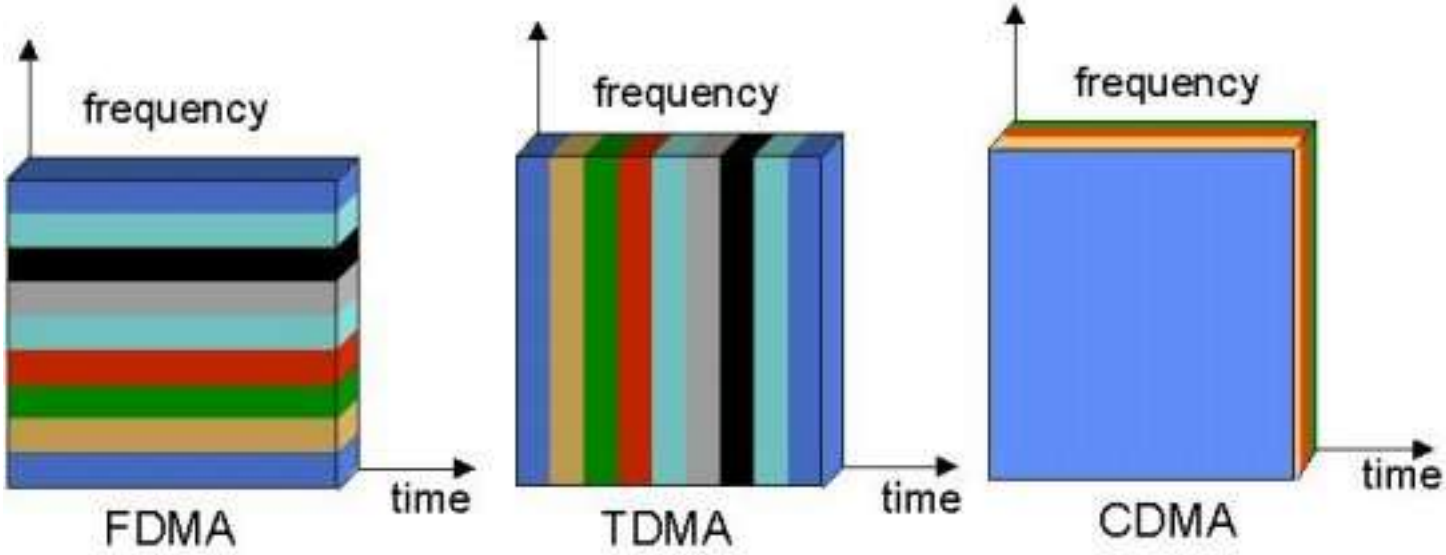
Beam Division Multiple Access (BDM)

- AKA: **Beam Division Multiple Access (BDMA)**

- New access technique for 5th generation of mobile wireless communication.
- The base station allocates separate antenna beams to each of the mobile devices.
- Based on **position** and moving **speed**, base station will calculate both width and direction of the beam for all the mobile stations.
- BDMA helps in achieving higher system capacity.

Dr Shahriar Bijani, www.faraconesh.com

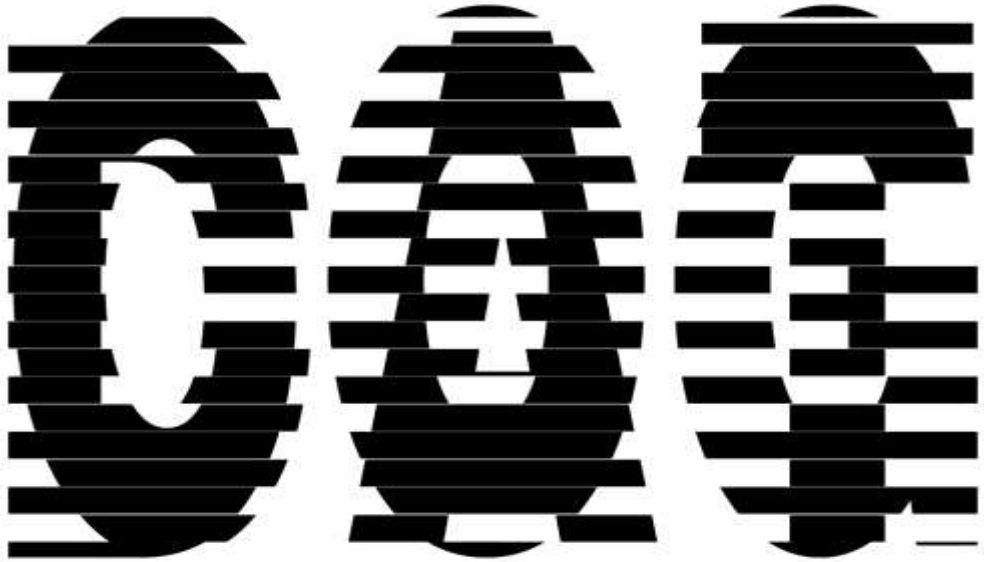
Multiple-Access Radio Techniques

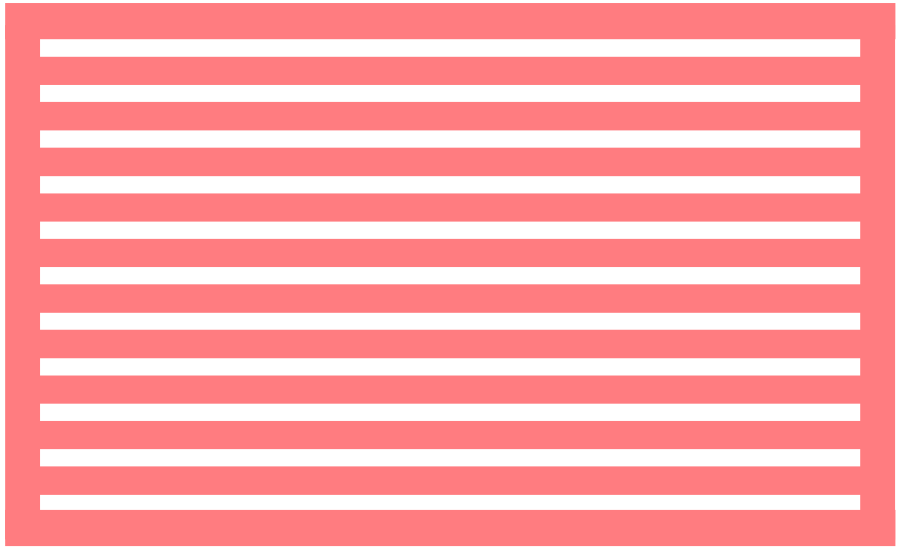


Courtesy of Petri Possi, UMTS World

Dr Shahriar Bijani, www.faraconesh.com

CDMA

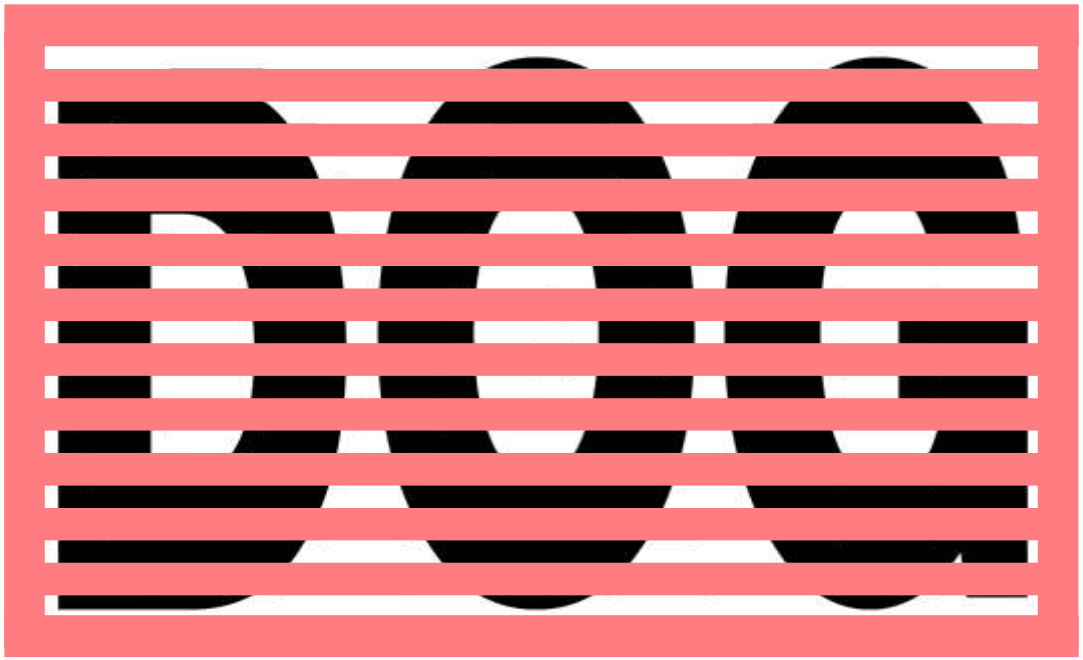




Courtesy of Suresh Goyal & Rich Howard

Dr Shahriar Bijani, www.faraconesh.com

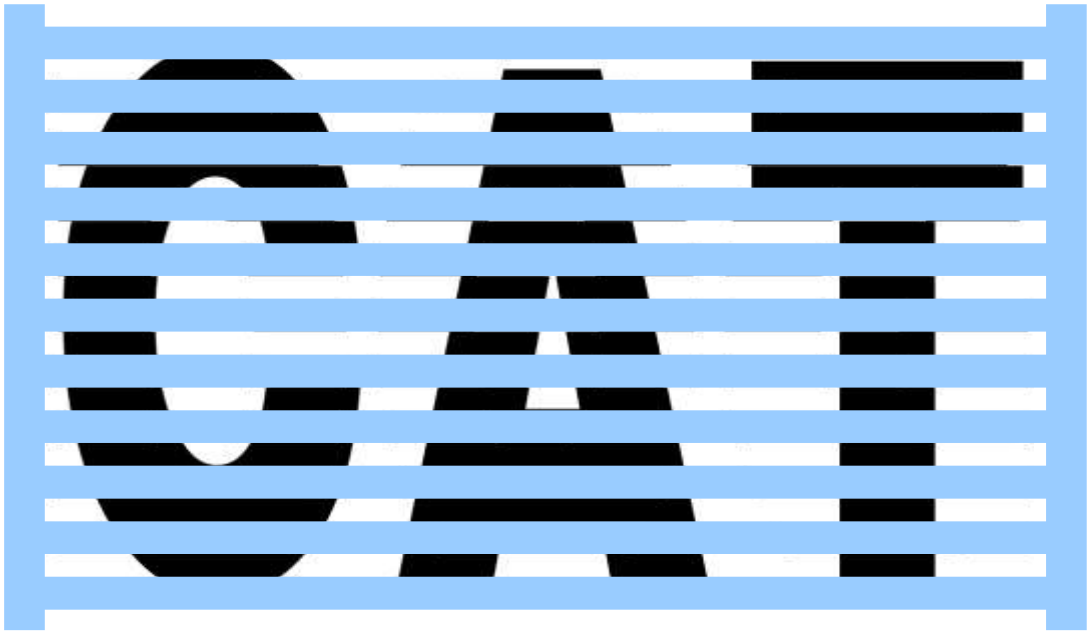
CDMA

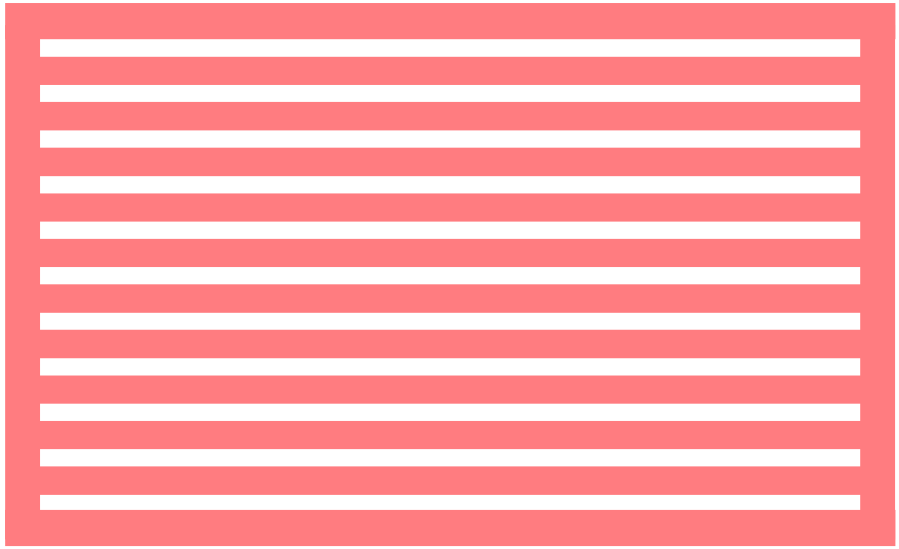


Courtesy of Suresh Goyal & Rich Howard

Dr Shahriar Bijani, www.faraconesh.com

CDMA

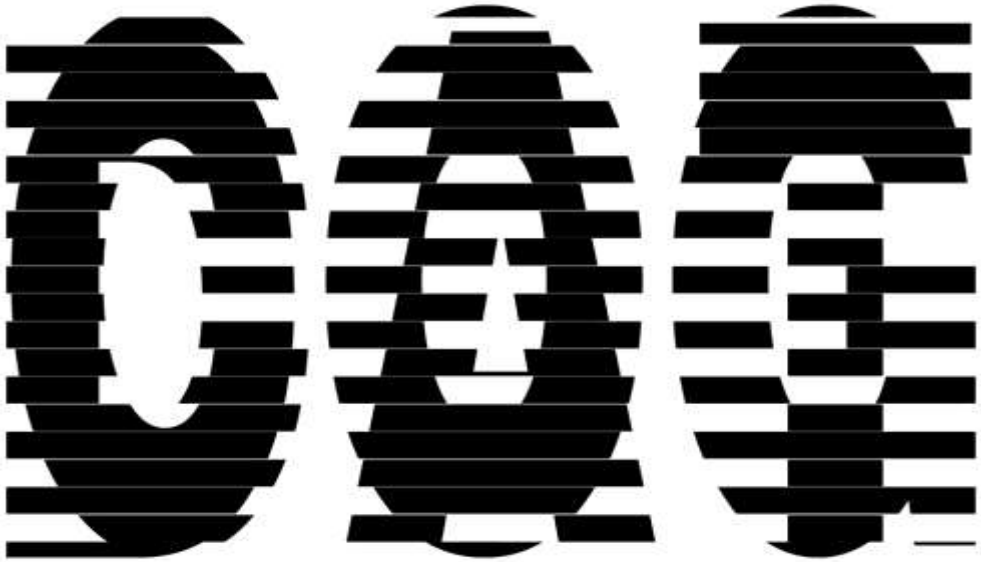




Courtesy of Suresh Goyal & Rich Howard

Dr Shahriar Bijani, www.faraconesh.com

CDMA

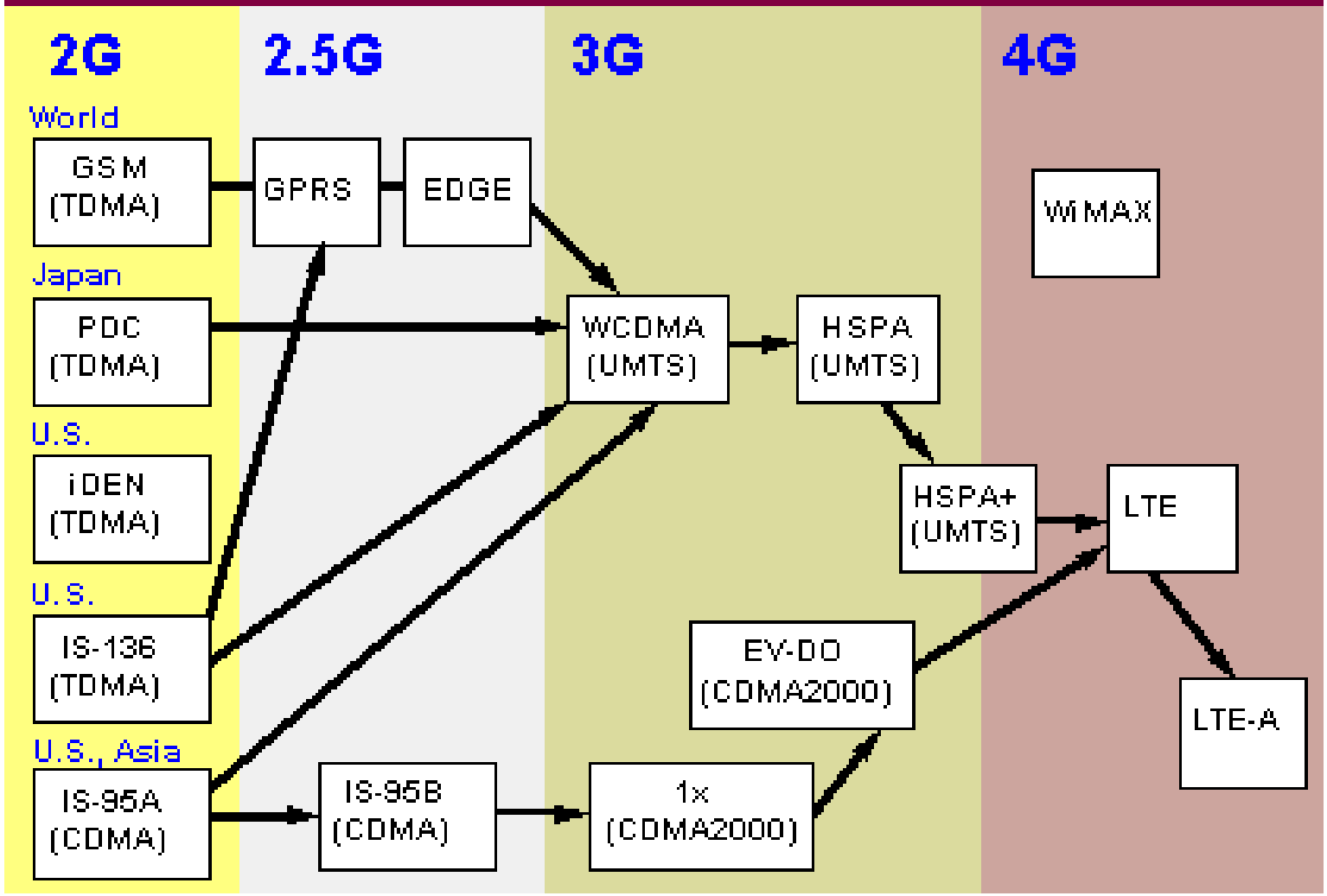


Courtesy of Suresh Goyal & Rich Howard

Dr Shahriar Bijani, www.faraconesh.com

From Computer Desktop Encyclopedia
© 2011 The Computer Language Co. Inc.

Evolution of Digital Cellular Standards



Dr Shahriar Bijani, www.faraconesh.com

A Comparison of All Mobile Generations

Technology / Features	1G	2G	3G	4G	5G
Start/ Deployment	1970 / 1984	1980 / 1999	1990 / 2002	2000/ 2010	2020
Data Bandwidth	2kbps	64kbps	2Mbps	200Mbs/ 1 Gbps	1 Gbps +
Standard	TACS, AMPS (Analog Cellular Technology)	TDMA, CDMA, GSM, GPRS, EDGE (Digital)	WCDMA, CDMA-2000, HSPA	WiMax , LTE, Wi-Fi	Unified IP & seamless combination of broadband , LAN, WAN, PAN,WLAN & www
Service	Mobile Telephony (Voice)	**Digital** voice, **SMS**, Higher capacity packetized data	Integrated **high quality** audio, video and **data**	Dynamic Information access, Wearable devices	Dynamic Information access, Wearable devices with **AI capabilities**
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA	CDMA, BDMA
Switching	Circuit	Circuit, Packet	(Circuit,) Packet	All Packet	
Core Network	PSTN	PSTN	Packet Network	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal and Vertical	Horizontal and Vertical

Dr Shahriar Bijani, www.farhconesh.com

GSM / 3GPP Releases

GSM Phases

GSM Release	Start Date
GSM Phase 1	1992
GSM Phase 2	1994
GSM Phase 2+	1997
GSM Phase 2+ Release 97	1998
GSM Phase 2+ Release 98	1999
GSM Phase 2+ Release 99 (3GPP UMTS Release 99)	2000

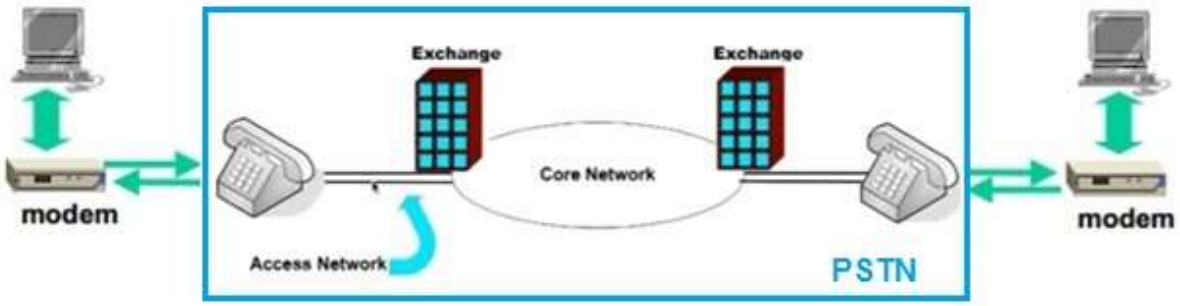
3GPP Releases

Release	Start Date
Release 4 (all IP)	2001
…	
Release 7	2007-8
Release 8 (LTE)	2008-9
Release 8 (LTE Advanced)	
Release 13	2016
Release 14	2017

Dr Shahriar Bijani, www.faraconesh.com

PSTN vs PSDN vs ISDN

- **PSTN: Public Switched Telephone Network**



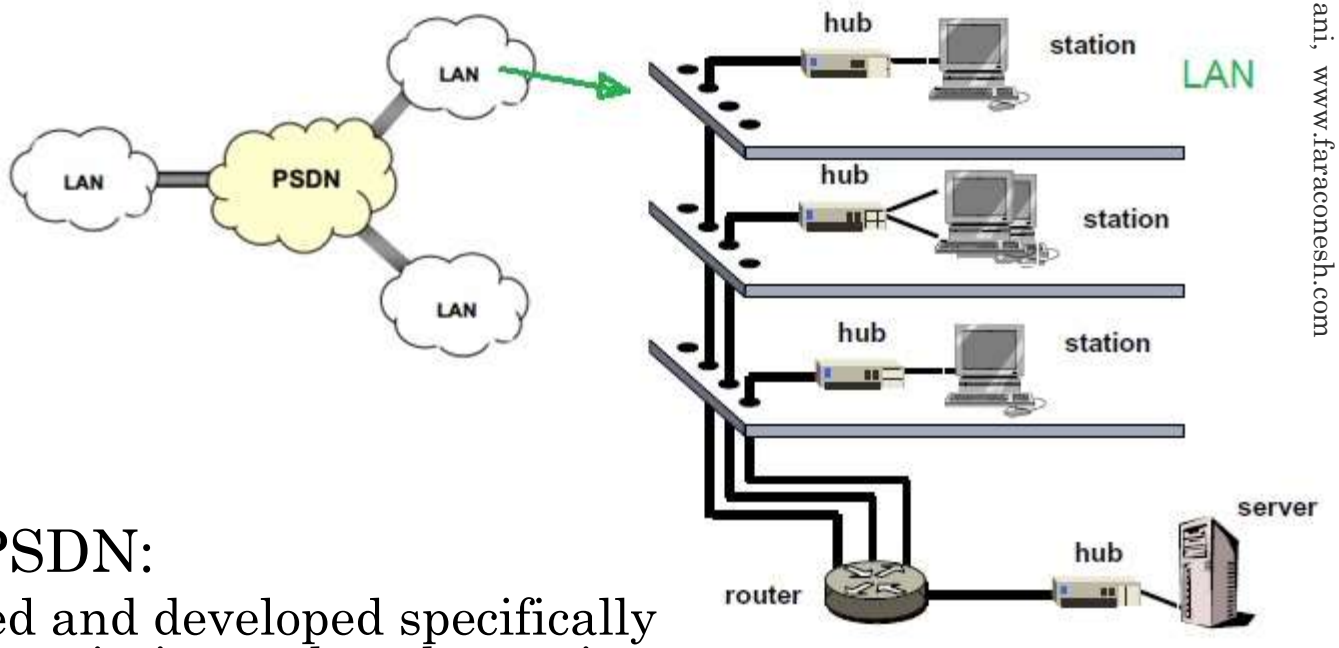
PSTN for Data

- Features of PSTN:
  - It uses circuit switching.
  - Bandwidth is reserved in advance.
  - Dedicated path is established between calling party and called party.
  - cost is based on distance and call duration or time.

Dr Shahriar Bijani, www.faraconesh.com

PSTN vs PSDN vs ISDN

- **PSDN: Public Switched Data Network**



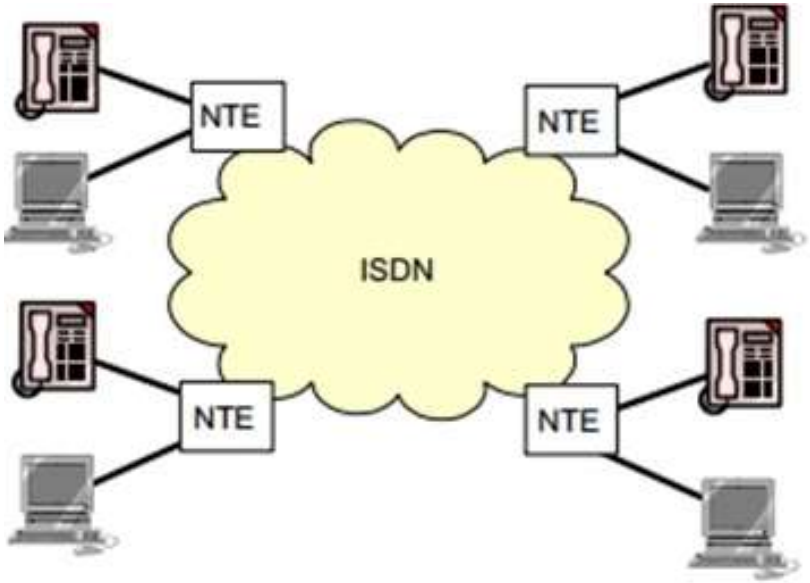
- Features of PSDN:
  - It is designed and developed specifically for data transmission rather than voice.
  - Communication is shared i.e. many companies share switching network.
  - It uses packet switching. It acquires and releases bandwidth as needed.
  - No dedicated path exists between sender and receiver.
  - Cost is not based on distance and time. It depends on usage of the data. Cost of service is normally lower than leased line.
  - Examples: X.25 Frame Relay ATM

Dr Shahriar Bijani, www.faraconesh.com

PSTN vs PSDN vs ISDN

- **ISDN: Integrated Services Digital Network**

It is a dial-up service designed for transmission of voice, data and video over digital line.



DSL

- "always on" connections. there is only a single route for carrying voice, data and video.
- Two types of DSL connections: Symmetric DSL (SDSL) and Asymmetric DSL (ADSL).
- For more downloading, ADSL is a better choice.

- ISDN and DSL are both distance sensitive: should not be more than 5.5 km away from the central office.

Dr Shahriar Bijani, www.faraconesh.com

GSM Network

Dr Shahriar Bijani, www.faraconesh.com

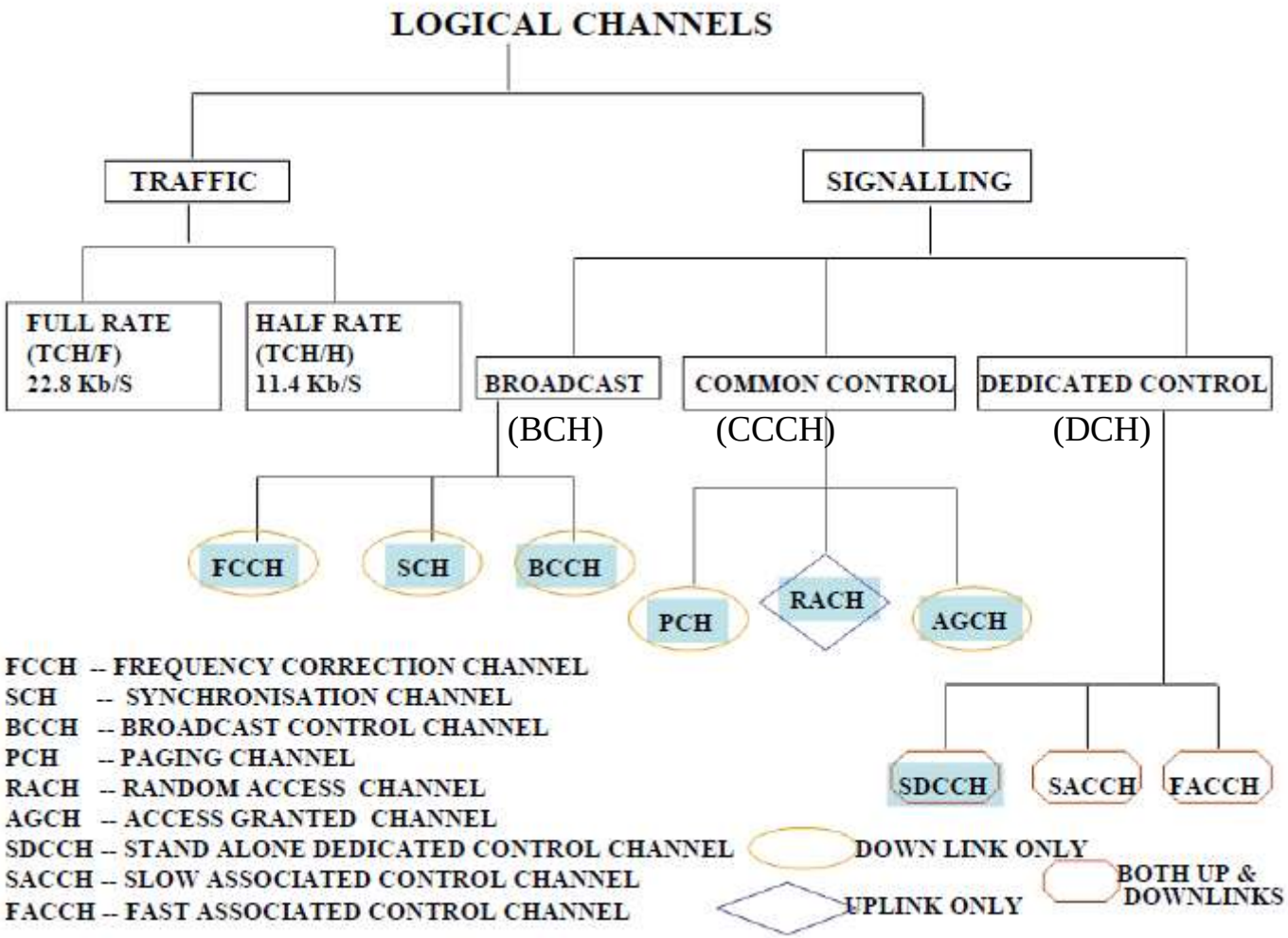
GSM

- GSM: Global System for Mobile Communication
- Pan-European standard (ETSI, European Telecommunications Standardisation Institute)

- simultaneous introduction of essential digital cellular services in 3 phases (1991, 1994, 1996) by the European

Dr Shahriar Bijani, www.faraconesh.com

GSM: PHYSICAL & LOGICAL CHANNELS

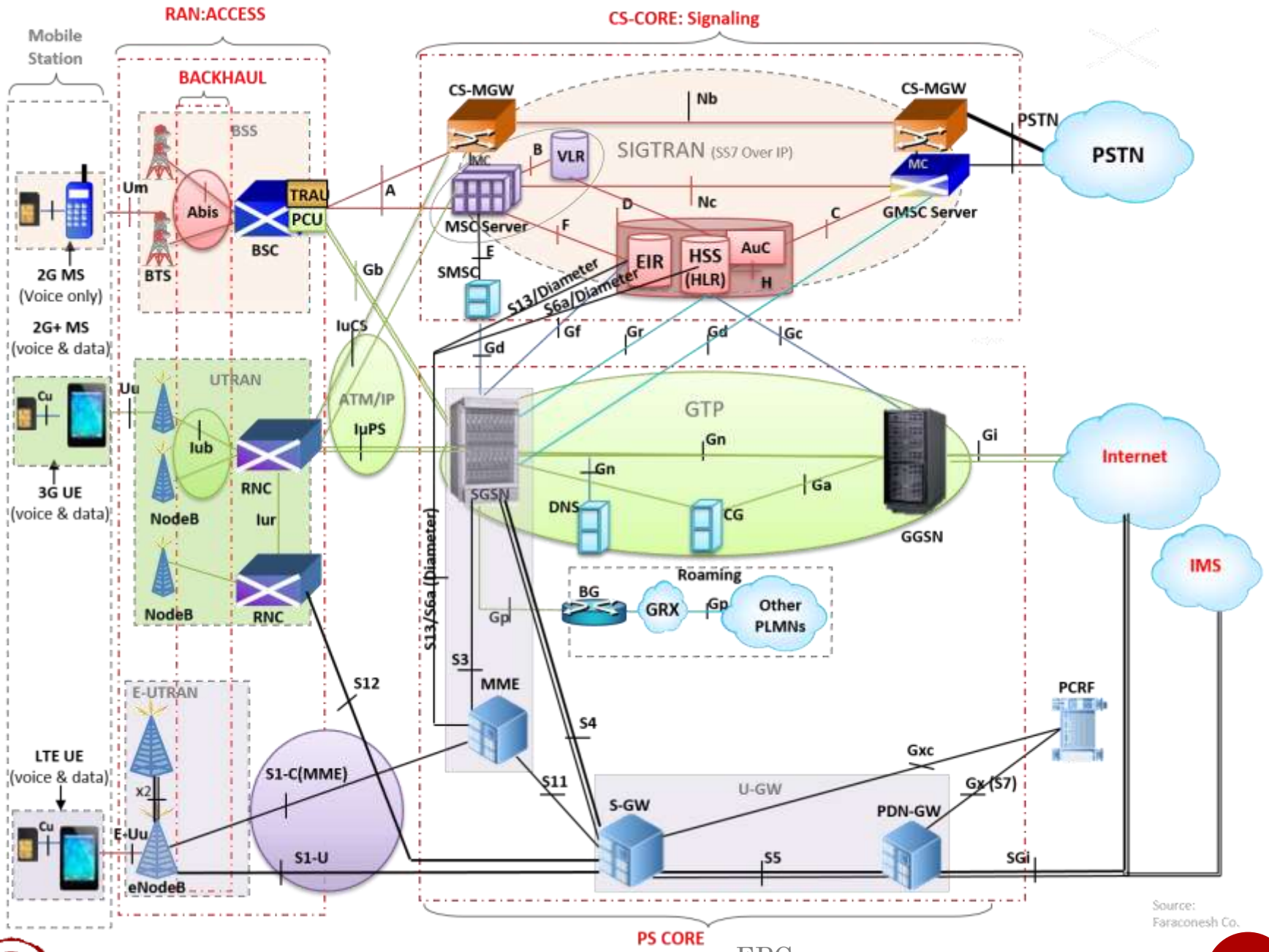


Dr Shahriar Bijani, www.faraconesh.com

Architecture of the GSM system

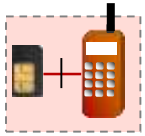
- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - BSS (Base Station Subsystem) or RSS (Radio SubSystem): covers all radio aspects
    - NSS (Network and Switching Subsystem): call forwarding, handover, switching
    - OSS (Operation SubSystem): management of the network

Dr Shahriar Bijani, www.faraconesh.com


RAN:ACCESS
CS-CORE: Signaling
Mobile Station
BACKHAUL
BSS
CS-MGW
Nb
CS-MGW
PSTN
PSTN
SIGTRAN (SS7 Over IP)
VLR
B
MC
MC
Um
Abis
TRAU
PCU
A
D
Nc
C
GMSC Server
MSC Server
F
BSC
BTS
E
SMSC
EIR
HSS (HLR)
AuC
H
S13/Diameter
S6a/Diameter
2G MS (Voice only)
2G+ MS (voice & data)
Gb
IuCS
Gd
Gf
Gr
Gd
Gc
Cu
Uu
UTRAN
ATM/IP
IuPS
GTP
Gn
Gi
Internet
Iub
RNC
Gn
Ga
3G UE (voice & data)
NodeB
Iur
SGSN
DNS
CG
GGSN
IMS
NodeB
RNC
Roaming
BG
GRX
Gp
Other PLMNs
S13/S6a (Diameter)
Gp
S3
S12
MME
E-UTRAN
PCRF
S4
LTE UE (voice & data)
S1-C(MME)
Gxc
x2
S11
U-GW
Gx (S7)
S-GW
PDN-GW
Cu
E-Uu
S1-U
S5
SGi
eNodeB
Source: Faraconesh Co.
PS CORE

EPC

Mobile Station (MS)



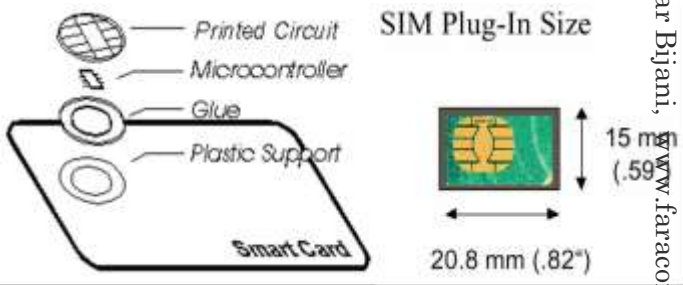
- MS is the user's handset and has two parts:

1. Mobile Equipment (ME)
   - Radio equipment
   - User interface
   - Processing capability and memory required for various tasks
     - Call signalling
     - Encryption
     - SMS
   - Equipment IMEI number

2. Subscriber Identity Module (SIM)

Dr Shahriar Bijani, www.faraconesh.com

Subscriber Identity Module (SIM)

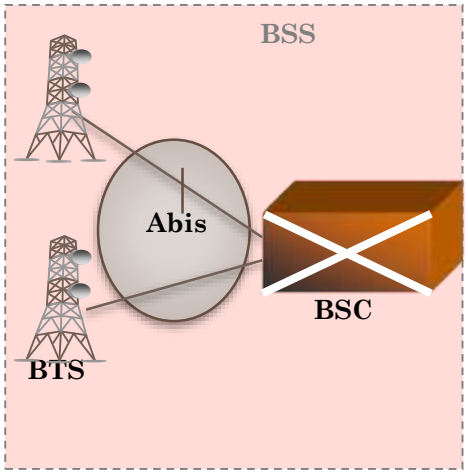


- A small smart card
- Main task: data storage
- Includes:
  - Encryption codes needed to identify the subscriber (Ki, Kc, …)
  - IMSI: International Mobile Subscriber Identify
    - For identification
  - Subscriber's own information (telephone directory)
  - Third party applications (banking etc.)
- Advantage: independence from the ME
- Can also be used in other systems besides GSM,
  - e.g., some WLAN access points accept SIM based user authentication

Dr Shahriar Bijani, www.faraconesh.com

Base Station Subsystem (BSS)

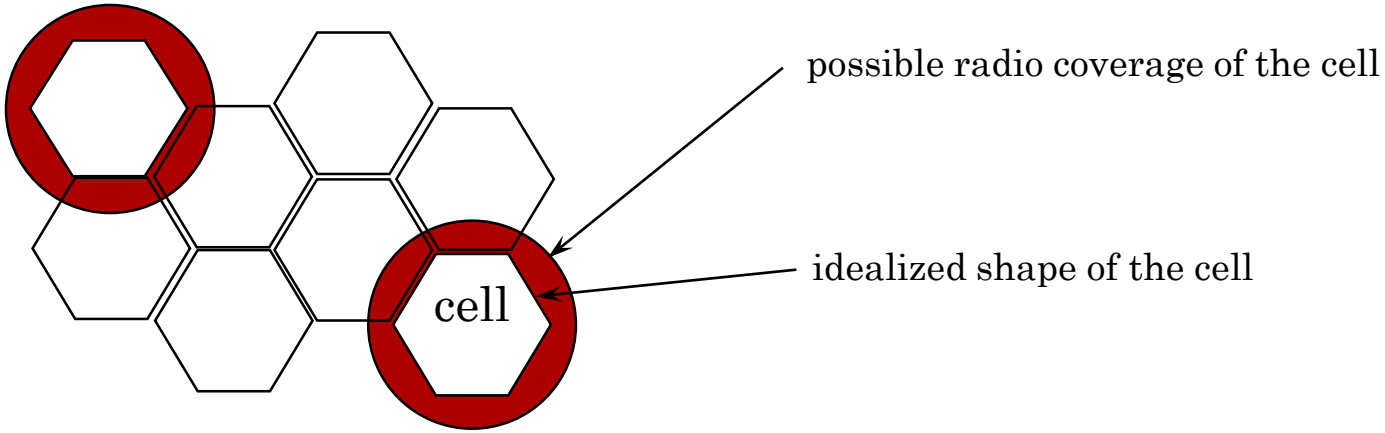
- The **Base Station Subsystem (BSS)** performs :
  - All functions necessary to maintain Radio connection to the MS
  - Coding/Decoding of Voice
  - Rate Adaptation to/from the Wireless Network part



Dr Shahriar Bijani, www.faraconesh.com

GSM is a Cellular Network

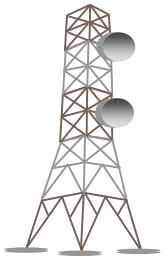
segmentation of the area into cells



- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells
  - ➪ handover of the connection to the neighbor cell

Dr Shahriar Bijani, www.faraconesh.com

Base Station Subsystem



- **Base Transceiver System (BTS)**
  - Controls several transmitters
  - Each transmitter has 8 time slots, some used for signaling, on a specific frequency
- **Transcoding Rate and Adaptation Unit (TRAU)**
  - Tasks:
    - compress and de-compress the speech data (main task)
    - the rate adaptation for data
  - The BTS contains TRAU.
  - In certain situations the TRAU is located at the MSC
    - more compressed transmission between the BTS and the MSC.
- **Base Station Controller (BSC)**
  - Controls the channel (time slot) allocation implemented by the BTSes
  - Manages the handovers within BSS area
  - Knows which mobile stations are in the cell and informs the MSC/VLR about this

Dr Shahriar Bijani, www.faraconesh.com

Functions of BTS and BSC

- Tasks of a BSS are distributed over BSC and BTS
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

Dr Shahriar Bijani, www.faraconesh.com

Network SubSystem (NSS)

- **The Network SubSystem (Network and Switching Subsystem)**
  - connects the wireless network with standard PSTN
  - performs handovers between different BSSs
  - supports charging and accounting
  - supports roaming of users between different providers in different networks/countries

Dr Shahriar Bijani, www.faraconesh.com

Network and Switching Subsystem

- The backbone of a GSM network is a telephone network with additional cellular network capabilities

- **Mobile Switching Center (MSC)**
  - An typical telephony exchange (ISDN exchange) which supports mobile communications
  - **Visitor Location Register (VLR)**
    - A database, part of the MSC
    - Contains the location of the active Mobile Stations
- **Gateway Mobile Switching Center (GMSC)**
  - Links the system to PSTN and other operators
- **Home Location Register (HLR)**
  - Contain subscriber information, including authentication information in **Authentication Center (AuC)**
- **Equipment Identity Register (EIR)**
  - International Mobile Station Equipment Identity (IMEI) codes for e.g., blacklisting stolen phones

Dr Shahriar Bijani, www.faraconesh.com

VLR (Visitor Location Register)

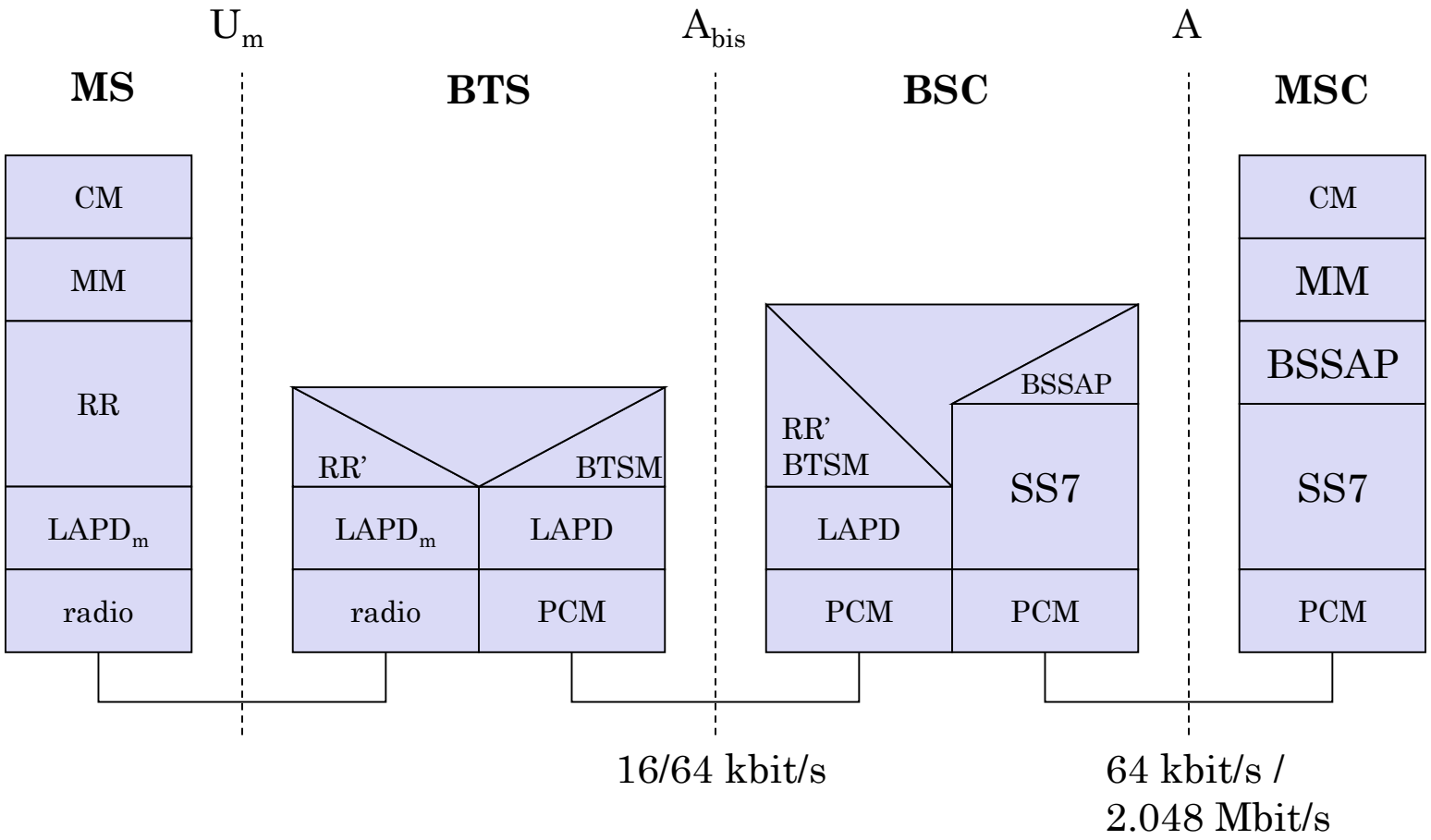
- VLR represents a temporary, very dynamic, database and usually used for roamer.
- Usually there is one VLR per MSC
- The register contains information about the MS who are currently in the service area covered by the MSC/VLR
- Once the visited system detects a mobile, its VLR queries the assigned HLR.
- The VLR makes sure that the mobile is a valid subscriber, then retrieves just enough information from the HLR to manage the call
- The temporary subscriber information in a VLR includes:
  - Features currently activated (special services its subscribed to)
  - Temporary mobile station identity (TMSI)
  - Last known location information about the MS (e.g., location area and cell identities)
  - the power the mobile uses

The Authentication Center (AuC)

- AuC is a protected database that stores a copy of the secret key stored in each subscriber's SIM card and the algorithm used for **authentication** and **encryption** over the radio channel
- AuC is used to <u>authenticate a subscriber</u> before allowing a *call to* or *from* the subscriber and in initial location registration,
- AuC is normally co-located with the HLR

Dr Shahriar Bijani, www.faraconesh.com

GSM PROTOCOL LAYERS FOR SIGNALING



Dr Shahriar Bijani, www.faraconesh.com

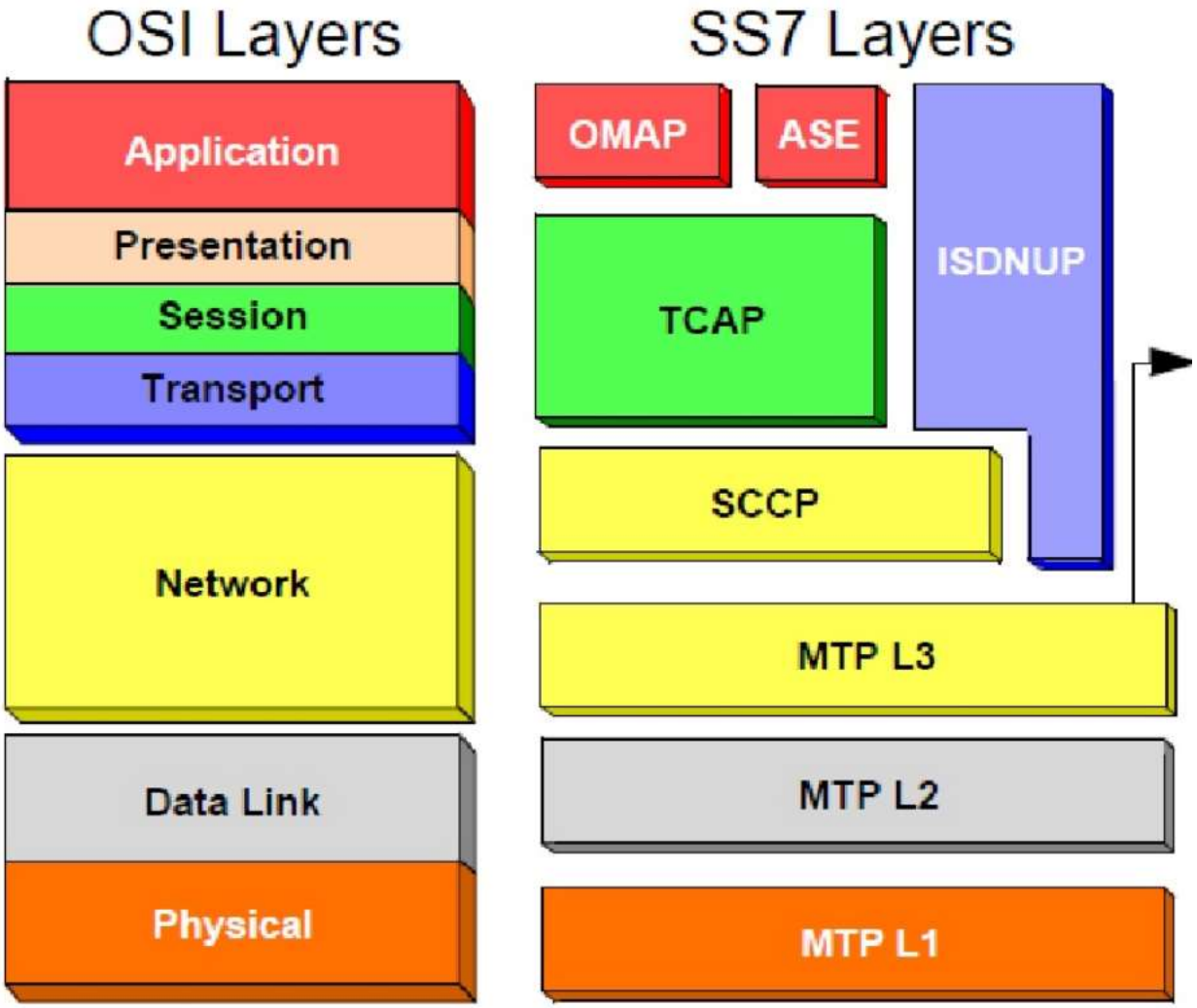
SS7

- Signaling System No. 7
  Signaling Support 7
  Common Channel Signalling (CCS)
- An architecture for performing out-of-band signaling in support of the functions of the PSTN

- PSTN functions
  - Call-establishment
  - Routing
  - Billing
  - Information exchange

Dr Shahriar Bijani, www.faraconesh.com

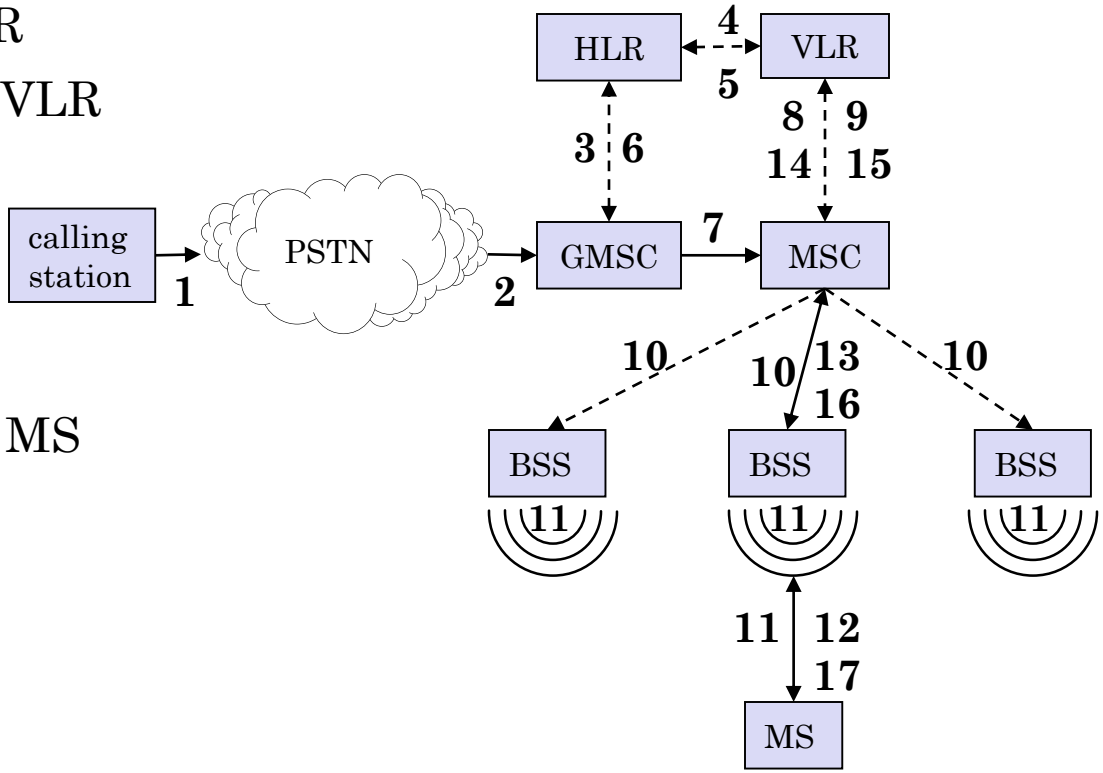
SS7 PROTOCOL STACK



Dr Shahriar Bijani, www.faraconesh.com

Mobile Terminated Call

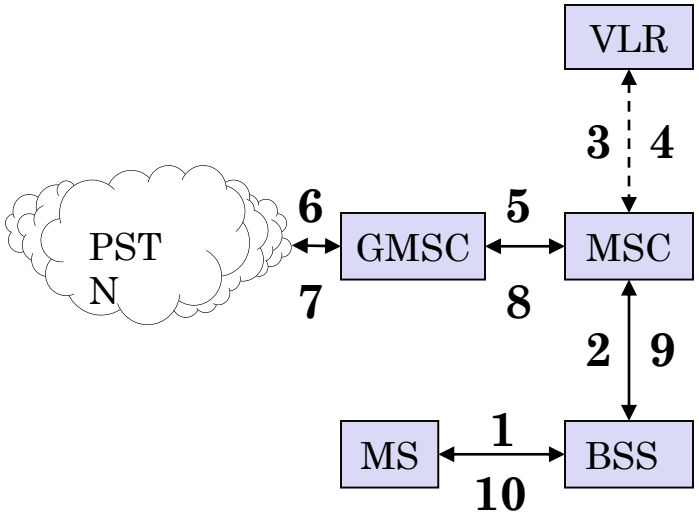
- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: request MSRN from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: set up connection



Dr Shahriar Bijani, www.faraconesh.com

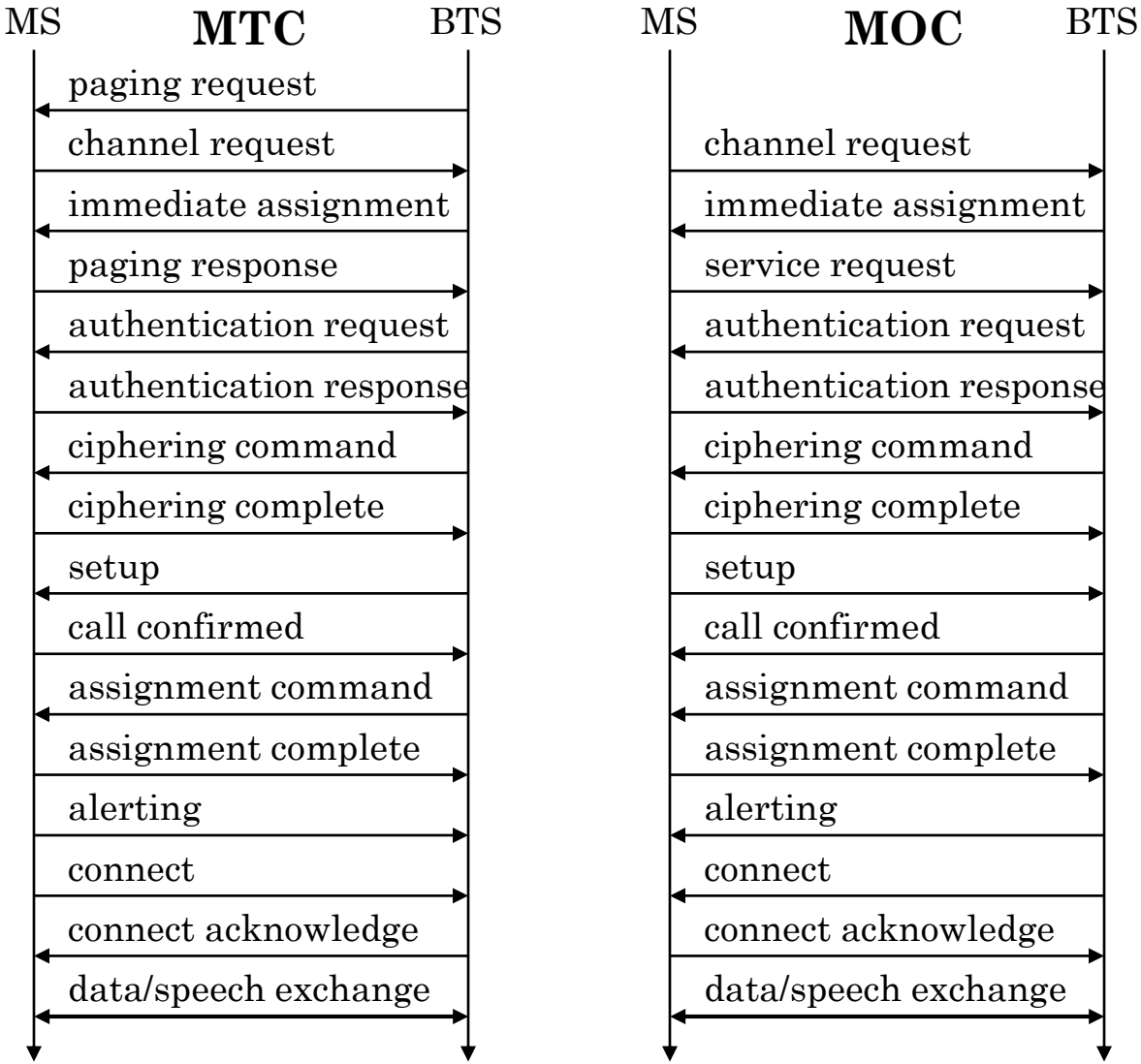
Mobile Originated Call

- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



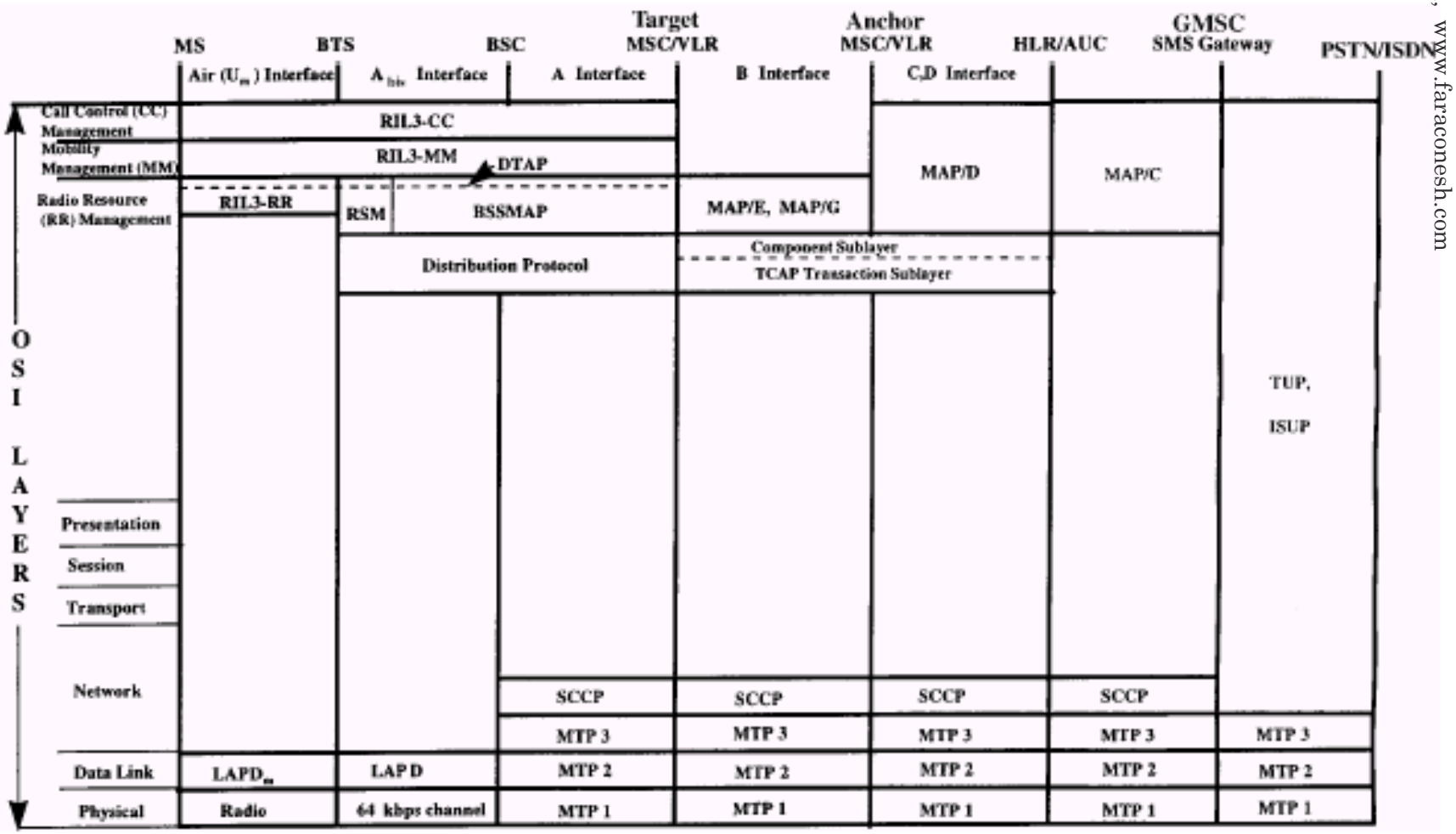
Dr Shahriar Bijani, www.faraconesh.com

MTC/MOC



Dr Shahriar Bijani, www.faraconesh.com

GSM PROTOCOL STACK



Dr Shahriar Bijani, www.faraconesh.com

GPRS

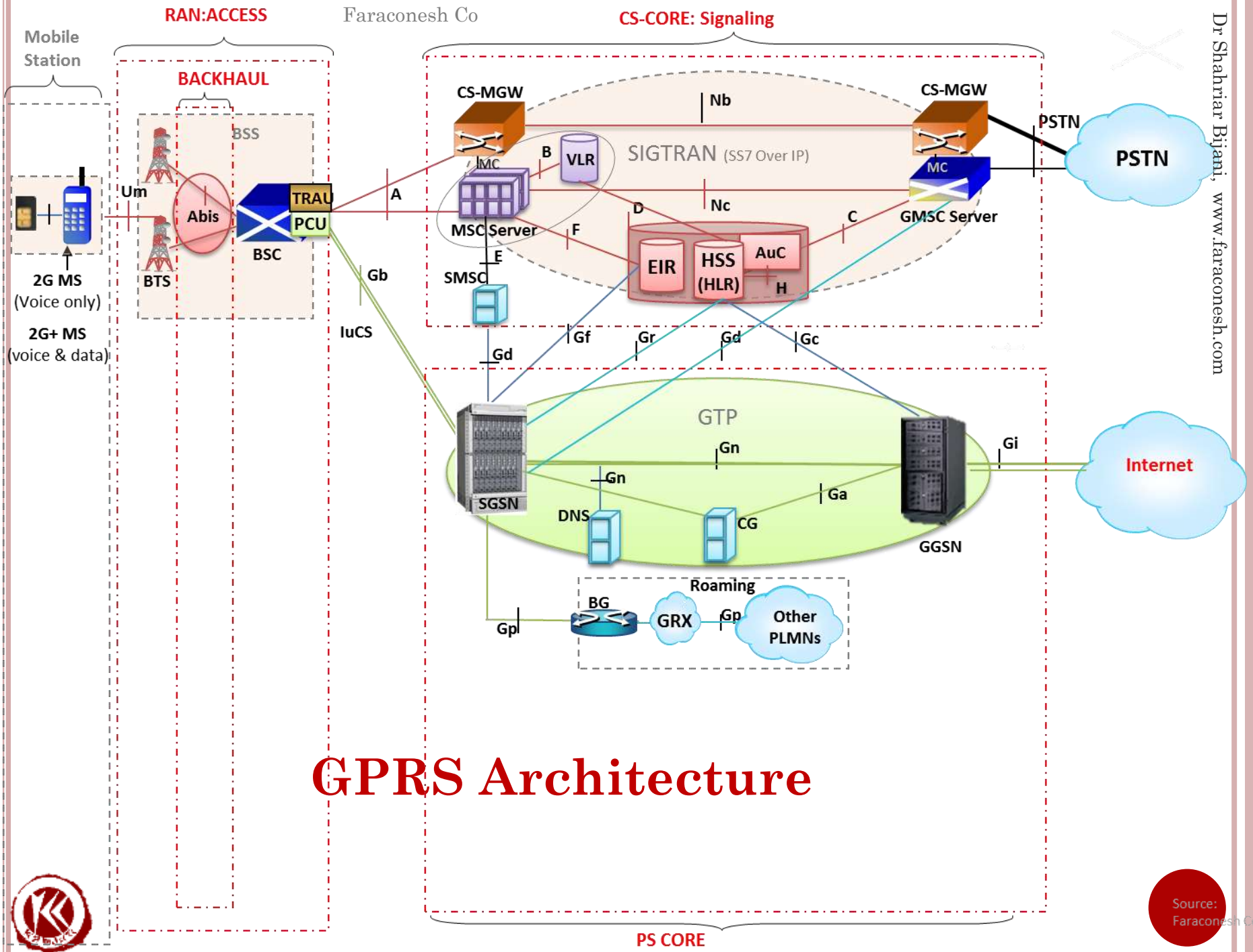
- Packet-switching technology
- Transparent end-to-end data transport of data packets over a modified GSM network
- Shares Radio Resources with GSM
- New GPRS core network different from GSM

Dr Shahriar Bijani, www.faraconesh.com

GPRS Features

- Introduces new air interface coding schemes
- Introduces Quality of Service (QoS) profiles
- Supports low and high speed (9.6-171.2kbps) data
- Supports multiple Packet Data Protocols (PDPs)
- Supports SMS over GPRS
- Allows for shared usage of GSM control functions

Dr Shahriar Bijani, www.faraconesh.com



GPRS Architecture

Dr Shahriar Bijani, www.faraconesh.com

Source: Faraconesh Co.

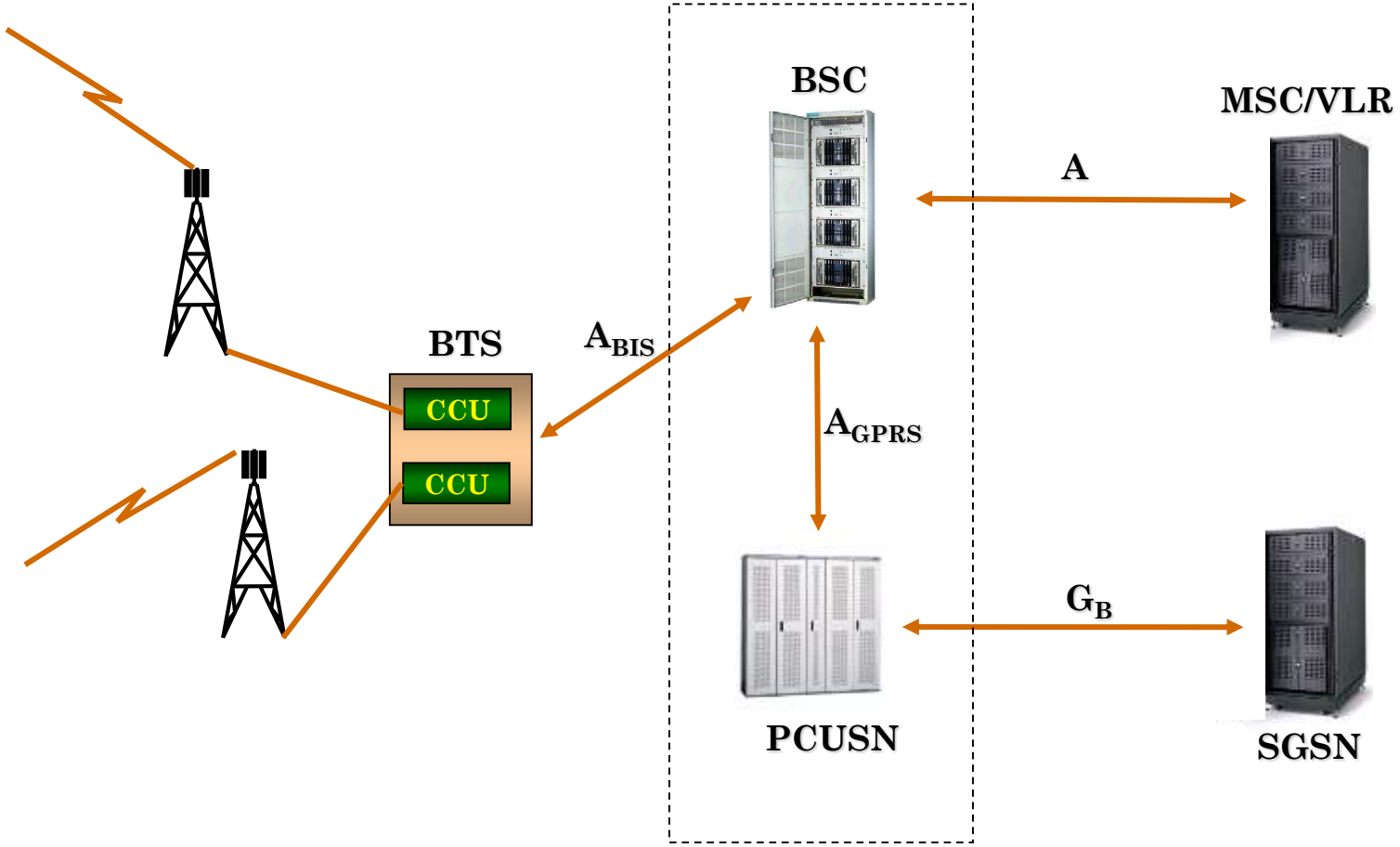
Base Station Subsytem (BSS) Modifications

- BTS Requires software upgrade
- Inclusion of a CCU in the BTS
- BSC requires software upgrade and addition of PCUSN
- PCUSN can contain multiple PCUs

Siemens BSC

Dr Shahriar Bijani, www.faraconesh.com

Packet Control Unit Support Node (PCUSN)



Physical Connectivity

GPRS Core Network Elements

The following GSM network changes are required:

- New GPRS entities:
  - Serving GPRS Support Node (SGSN)
  - Gateway GPRS Support Node (GGSN)
- Modified GSM entities:
  - HLR
  - MSC/VLR
  - SMS-GMSC

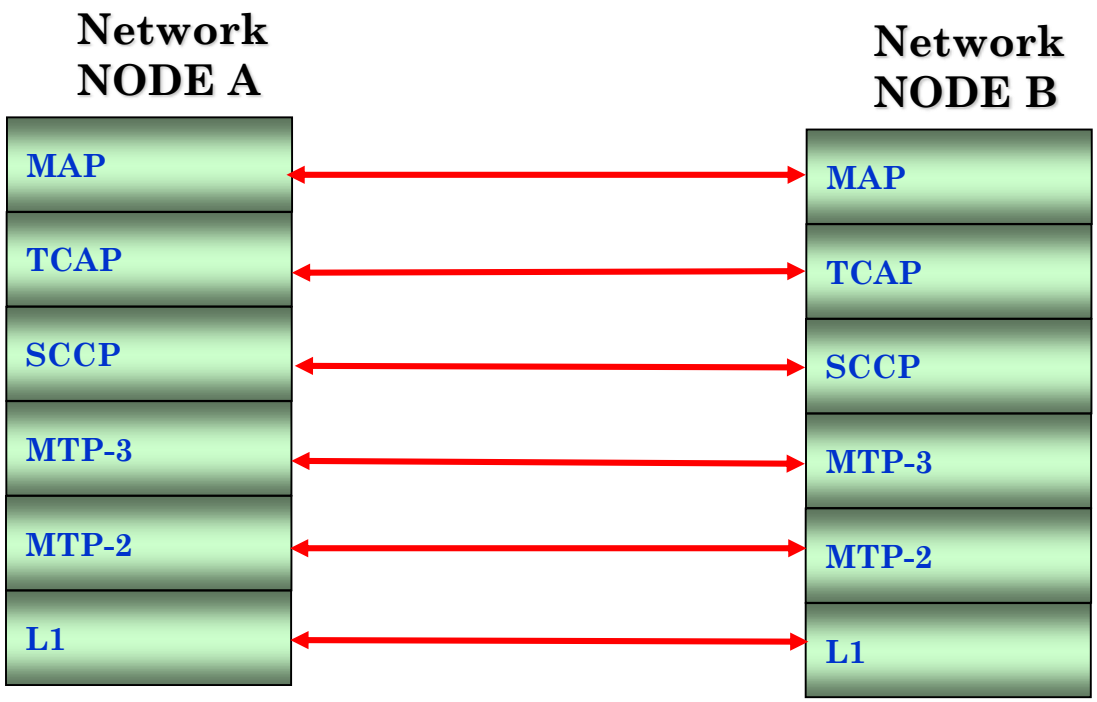
Dr Shahriar Bijani, www.faraconesh.com

ISO 7-Layer OSI Model

7	APPLICATION	File transfer, access management
6	PRESENTATION	Syntax and data representation management
5	SESSION	Application entity dialogue and synchronisation
4	TRANSPORT	End-to-end message transfer
3	NETWORK	Network routing, addressing, call management
2	DATA LINK	Data link control (framing, error control)
1	PHYSICAL	Mechanical and electrical interfacing

Dr Shahriar Bijani, www.faraconesh.com

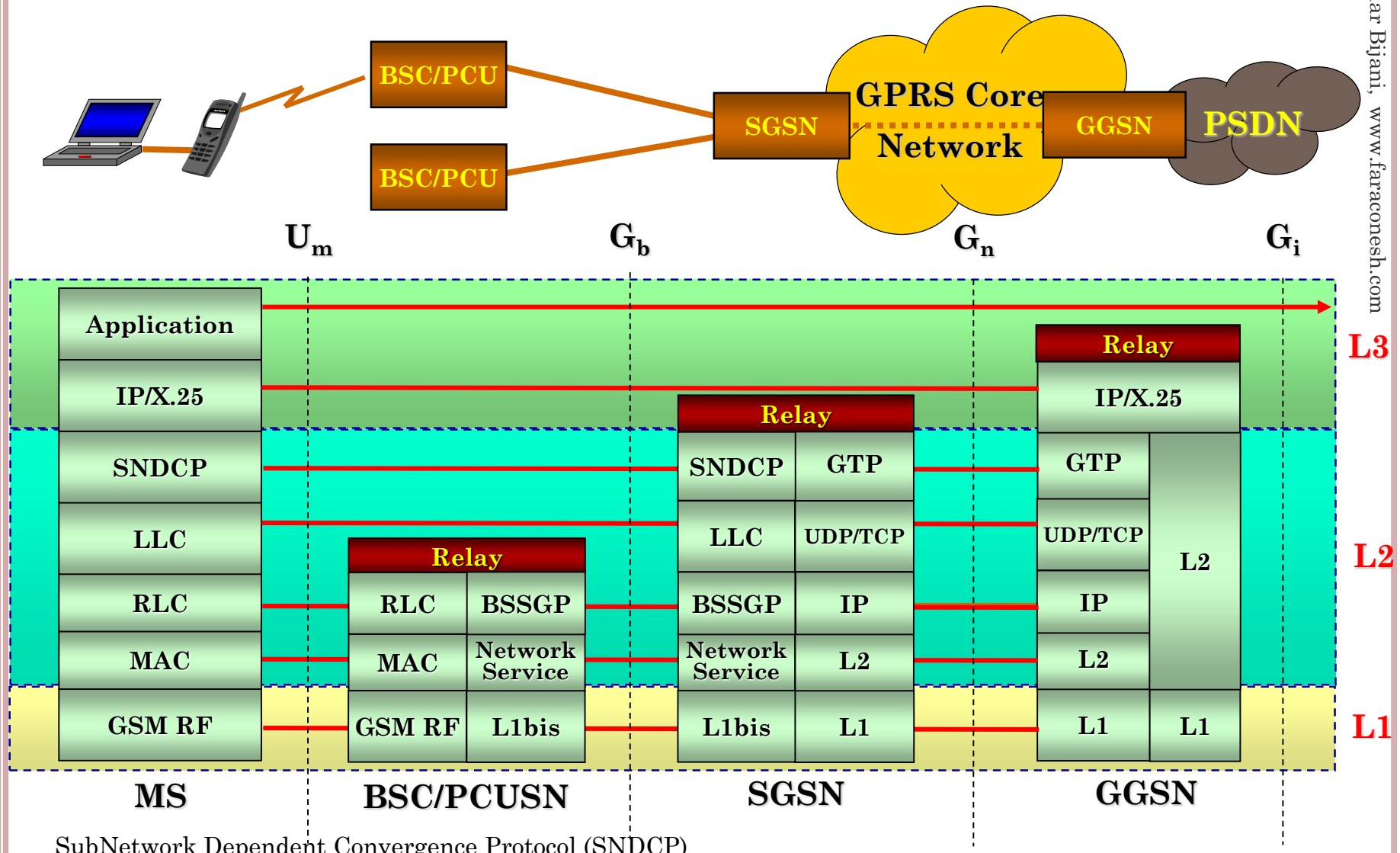
GPRS Core Network Signalling Protocols



MAP – Mobile Application Part
TCAP – Transaction Capabilities Application Part
SCCP – Signalling Connection Control Part
MTP – Message Transfer Part

Dr Shahriar Bijani, www.faraconesh.com

The GPRS Protocol Stack



SubNetwork Dependent Convergence Protocol (SNDCP)
Logical Link Control (LLC)
RLC (Radio Link Control)
Base Station System GPRS Protocol (BSSGP)

Dr Shahriar Bijani, www.faraconesh.com

The GPRS Protocol Stack

- Layer 3 (L3):
  - Session management (establishes data calls and negotiates QoS)
  - Mobility management (Registration, Authentication, Location management, Encryption management ,…)

- Layer 2 (L2)
  - SNDCP: compression, storage and segmentation, …
  - LLC: encryption, Protection and framing, storage
  - RLC: segmentation
  - MAC: logical/physical channels scheduling, control and management.

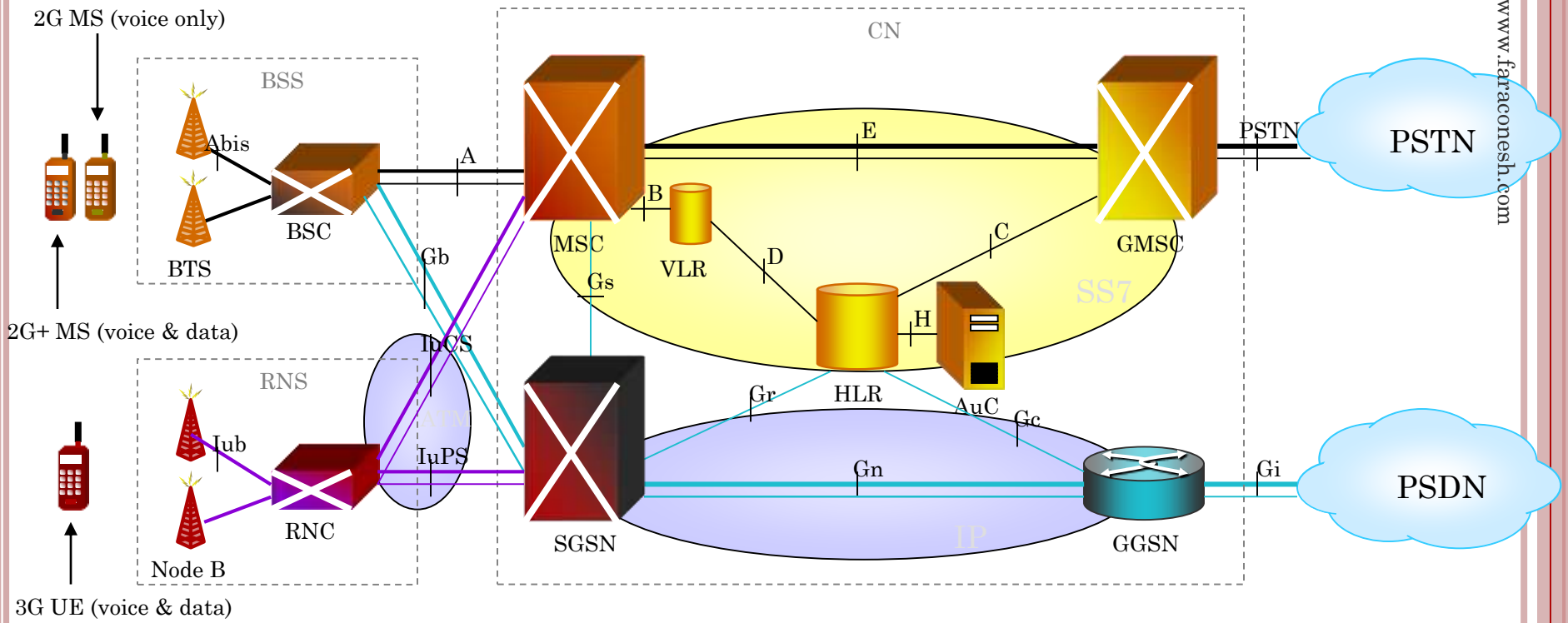
Dr Shahriar Bijani, www.faraconesh.com

3G: UMTS (WCDMA)

Dr Shahriar Bijani, www.faraconesh.com

3G REL99 ARCHITECTURE (UMTS) — *3G RADIOS*

Dr Shahriar Bijani, www.faraconesh.com



BSS — Base Station System
BTS — Base Transceiver Station
BSC — Base Station Controller

RNS — Radio Network System
RNC — Radio Network Controller

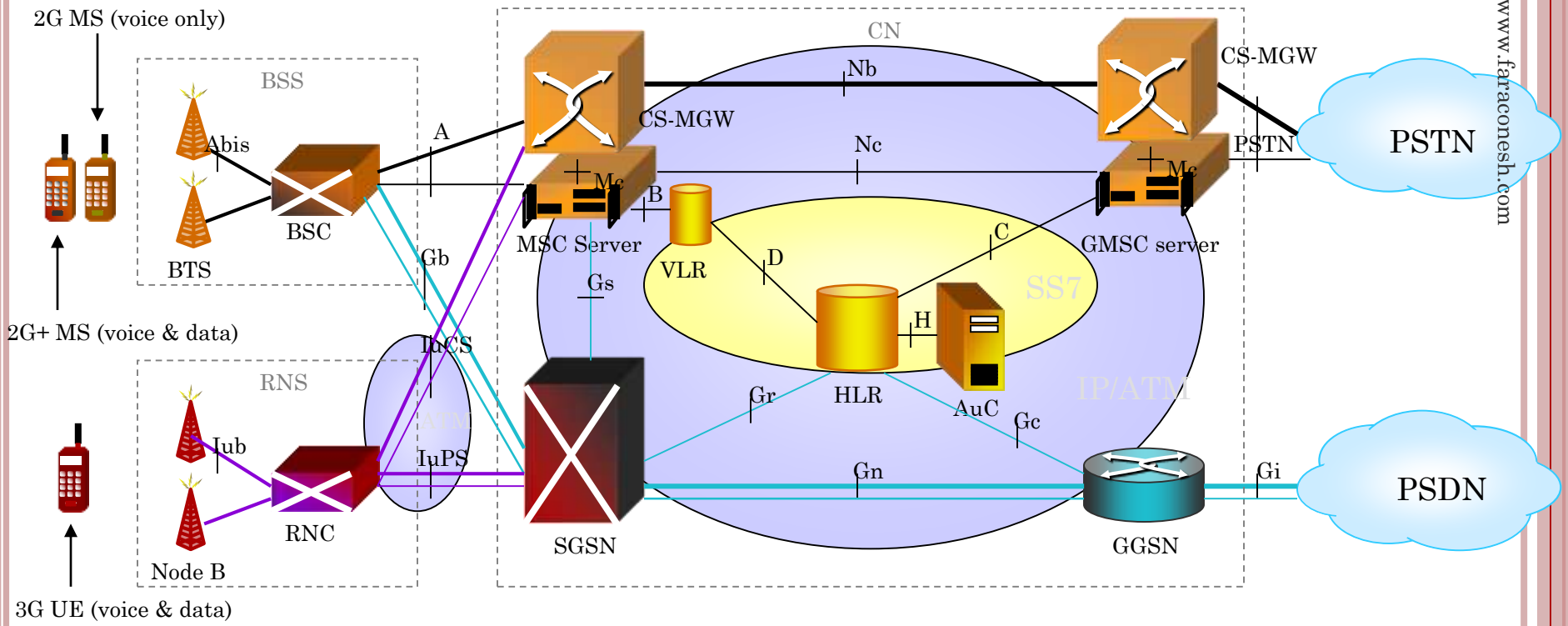
CN — Core Network
MSC — Mobile-service Switching Controller
VLR — Visitor Location Register
HLR — Home Location Register
AuC — Authentication Server
GMSC — Gateway MSC

SGSN — Serving GPRS Support Node
GGSN — Gateway GPRS Support Node

UMTS — Universal Mobile Telecommunication System

3G REL4 ARCHITECTURE (UMTS) — *SOFT SWITCHING*

Dr Shahriar Bijani, www.faraconesh.com



BSS — Base Station System
BTS — Base Transceiver Station
BSC — Base Station Controller

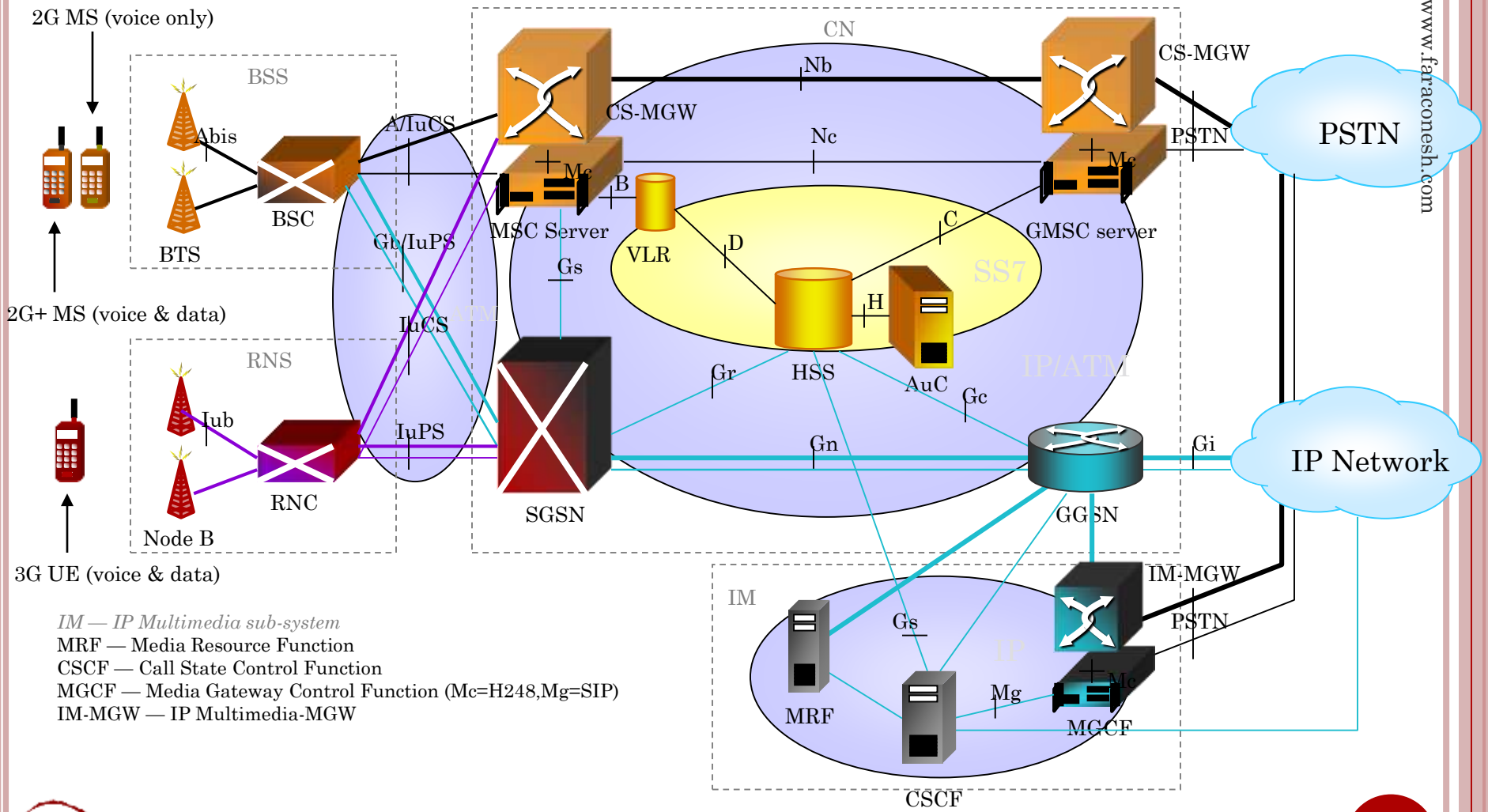
RNS — Radio Network System
RNC — Radio Network Controller

CN — Core Network
MSC — Mobile-service Switching Controller
VLR — Visitor Location Register
HLR — Home Location Register
AuC — Authentication Server
GMSC — Gateway MSC

SGSN — Serving GPRS Support Node
GGSN — Gateway GPRS Support Node

3G REL5 ARCHITECTURE (UMTS) — *IP MULTIMEDIA*

Dr Shahriar Bijani, www.faraconesh.com



IM — IP Multimedia sub-system
MRF — Media Resource Function
CSCF — Call State Control Function
MGCF — Media Gateway Control Function (Mc=H248,Mg=SIP)
IM-MGW — IP Multimedia-MGW

3RD GENERATION: UMTS

- **UMTS**: Universal Mobile Technology System
- FDMA and TDMA are not very efficient
  - TDMA wastes time resources
  - FDMA wastes frequency resource
  - CDMA can use the whole bandwidth constantly
- WCDMA (Wideband Code Division Multiple Access)
  - WCDMA was selected for a radio access system for UMTS (1997)

Dr Shahriar Bijani, www.faraconesh.com

3G Standardization

- At end of 1998 different standardization organization got together and created 3GPP, 3rd Generation Partnership Project.
  - ETSI (Europ),
  - ARIB+TTC (Japan),
  - TTA (Korea),
  - T1P1 (USA)

  - CWTS (China) joined later.

A GLOBAL INITIATIVE

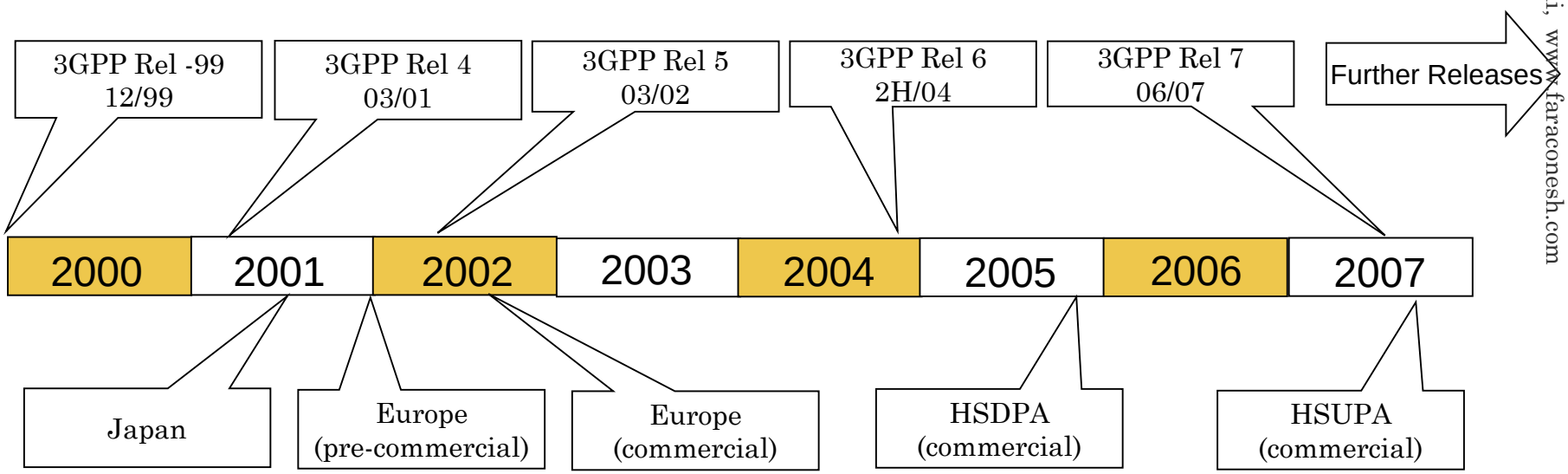
Dr Shahriar Bijani, www.faraconesh.com

3G Evolution

- **Release -99** (12/1999)
  - Targeted mainly on access part of the network
- **Release 4** (2003/01)
  - Core network was extended
- **Release 5** (2003/02) (All IP)
  - High Speed Downlink Packet Access (HSDPA)
  - First IP Multimedia Services (IMS)
- **Release 6**, end of 04/beginning of 05
  - High Speed Uplink Packet Access (HSUPA)
  - "All IP" network
- **Release 7** (2006/07)
  - Continuous Packet connectivity (improvement for e.g. VoIP), MIMO, Higher order modulation

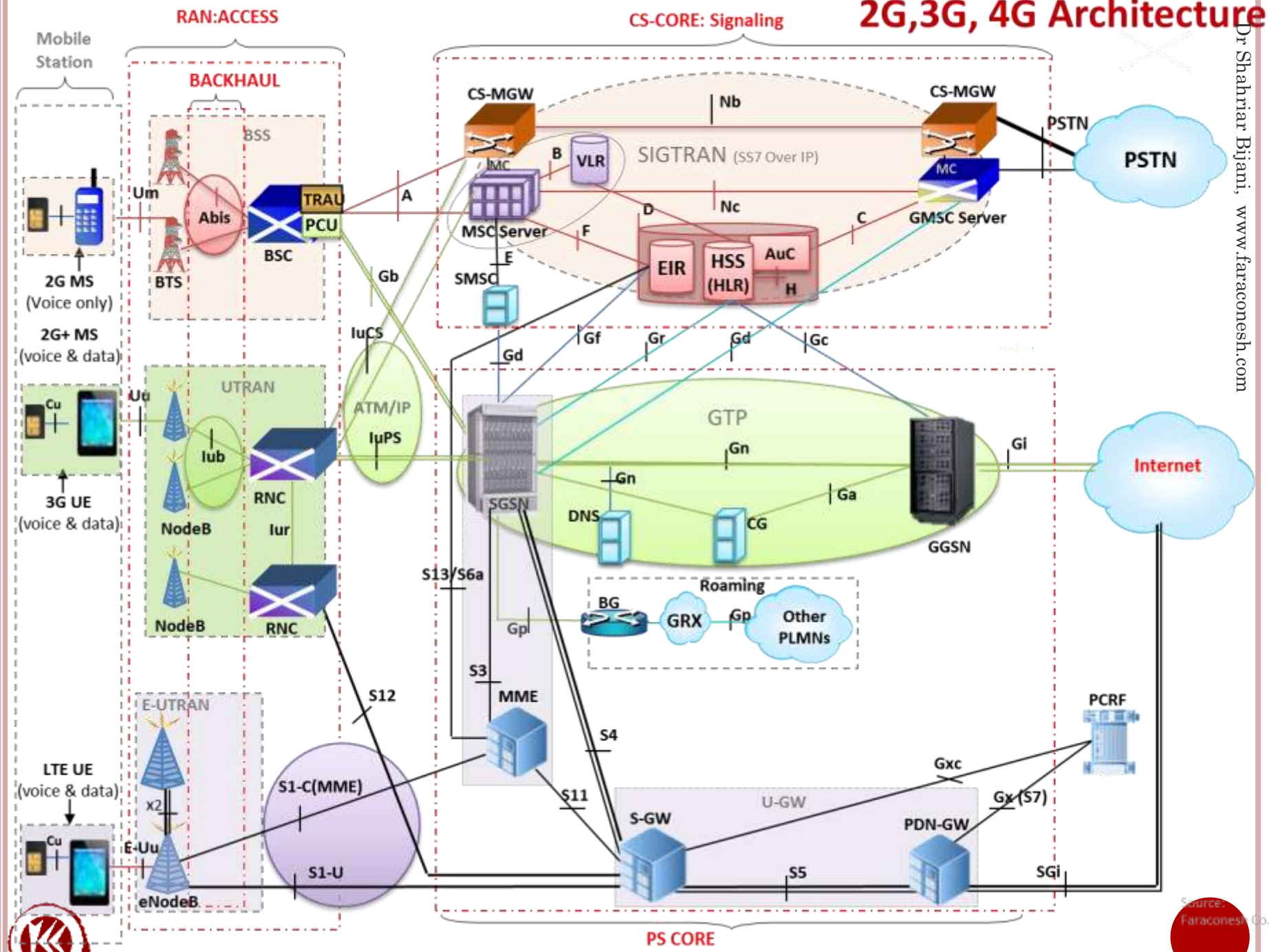
Dr Shahriar Bijani, www.faraconesh.com

3G Evolution



Dr Shahriar Bijani, www.faraconesh.com

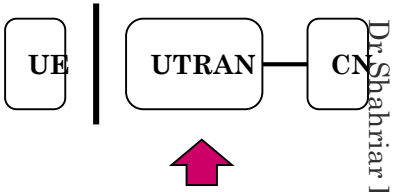
2G,3G, 4G Architecture



Dr Shahriar Bijani, www.faraconesh.com

Source: Faraconesh Co.

UTRAN



Dr. Shahriar Bijani, www.faraconesh.com

UMTS Terrestrial Radio Access Network, Overview

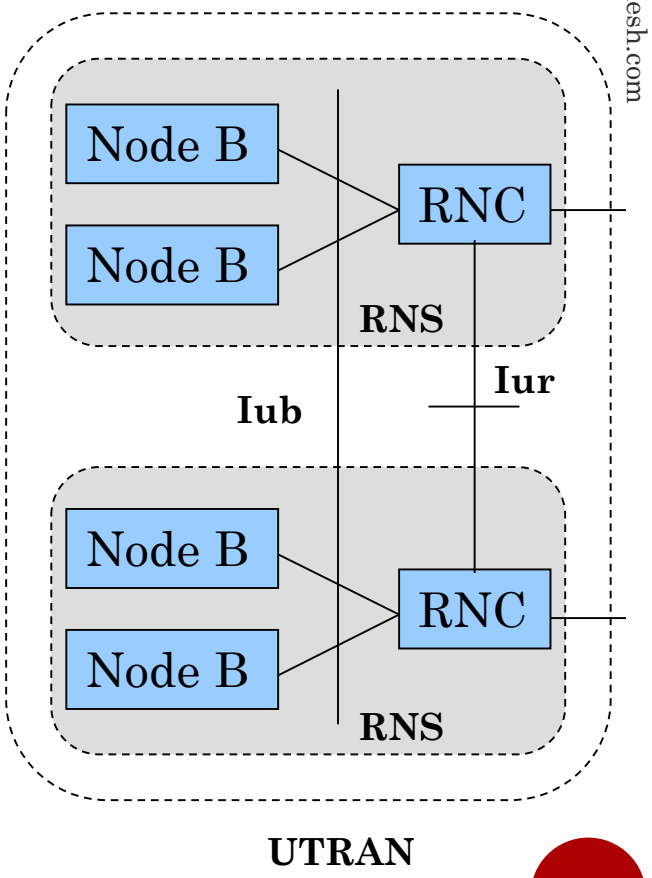
- Two Distinct Elements :

  Base Stations (Node B)
  Radio Network Controllers (RNC)

- 1 RNC and 1+ Node Bs are group together to form a Radio Network Sub-system (RNS)

- Handles all Radio-Related Functionality
  - Soft Handover
  - Radio Resources Management Algorithms

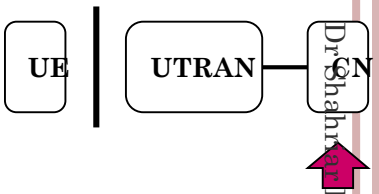
- Maximization of the unities of the PS and CS data handling



Functions of Node B (Base Station)

- Air Interface L1 Processing (Channel Coding, Interleaving, Rate Adaptation, Spreading, etc.)

Core Network

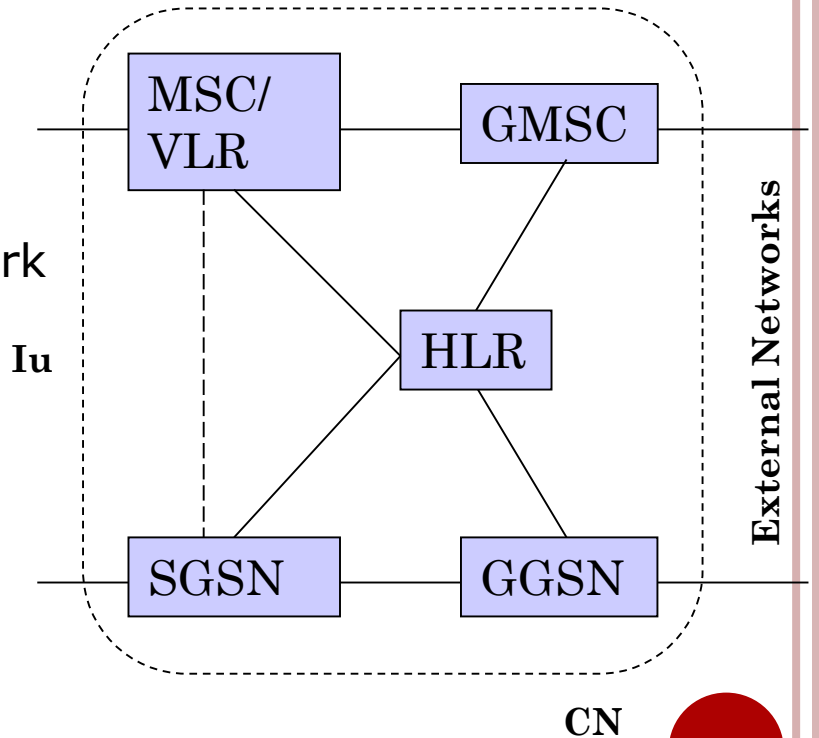


Dr. Shahriar Bijani, www.faraconesh.com

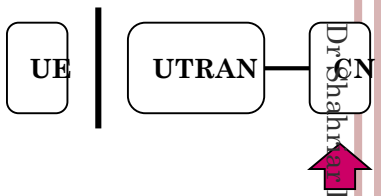
Core Network, Overview

- Changes From Release '99 to Release 5
- A Seamless Transition from GSM to All-IP 3G Core Network
- Responsible for Switching and Routing Calls and Data Connections within, and to the External Networks

  (e.g. PSTN, ISDN and Internet)
- Divided into CS Network and PS Network

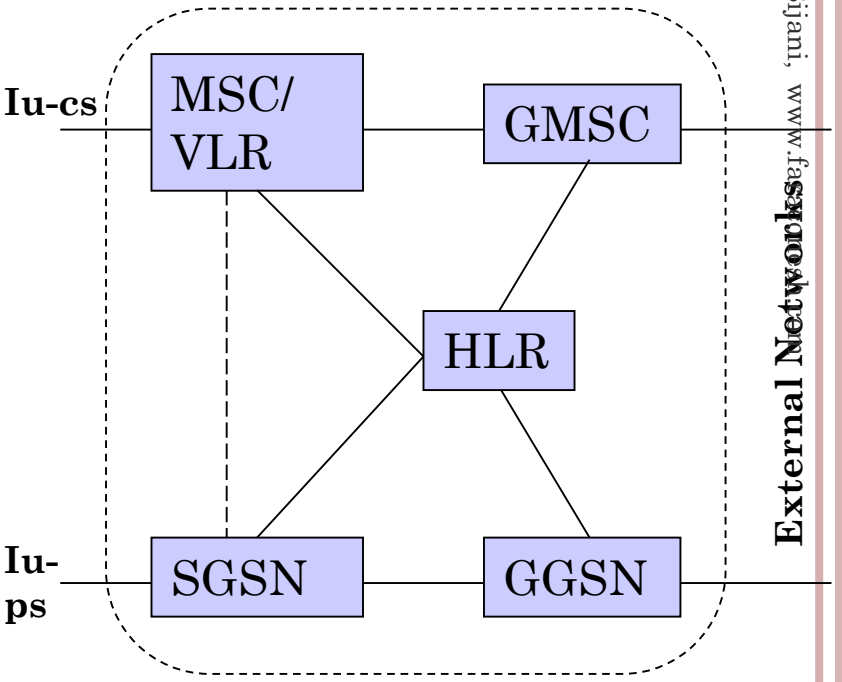


Core Network



Dr. Shahnaz Bijani, www.fastcourses.com

Core Network, Release '99



- CS Domain :
  - Mobile Switching Centre (MSC)
    - Switching CS transactions
  - Visitor Location Register (VLR)
    - Holds a copy of the visiting user's service profile, and the precise info of the UE's location
  - Gateway MSC (GMSC)
    - The switch that connects to external networks

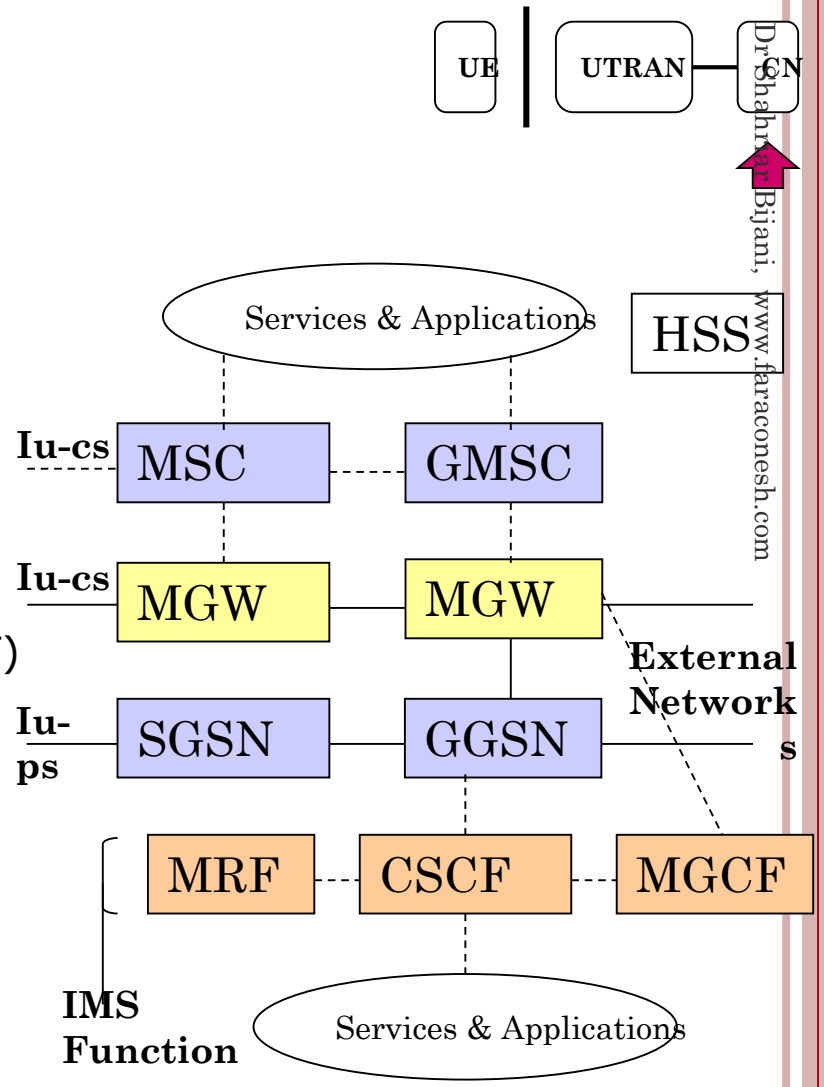
- PS Domain :
  - Serving GPRS Support Node (SGSN)
    - Similar function as MSC/VLR
  - Gateway GPRS Support Node (GGSN)
    - Similar function as GMSC

- Register :
  - Home Location Register (HLR)
    - Stores master copies of users service profiles
    - Stores UE location on the level of MSC/VLR/SGSN

Core Network

Core Network, R5

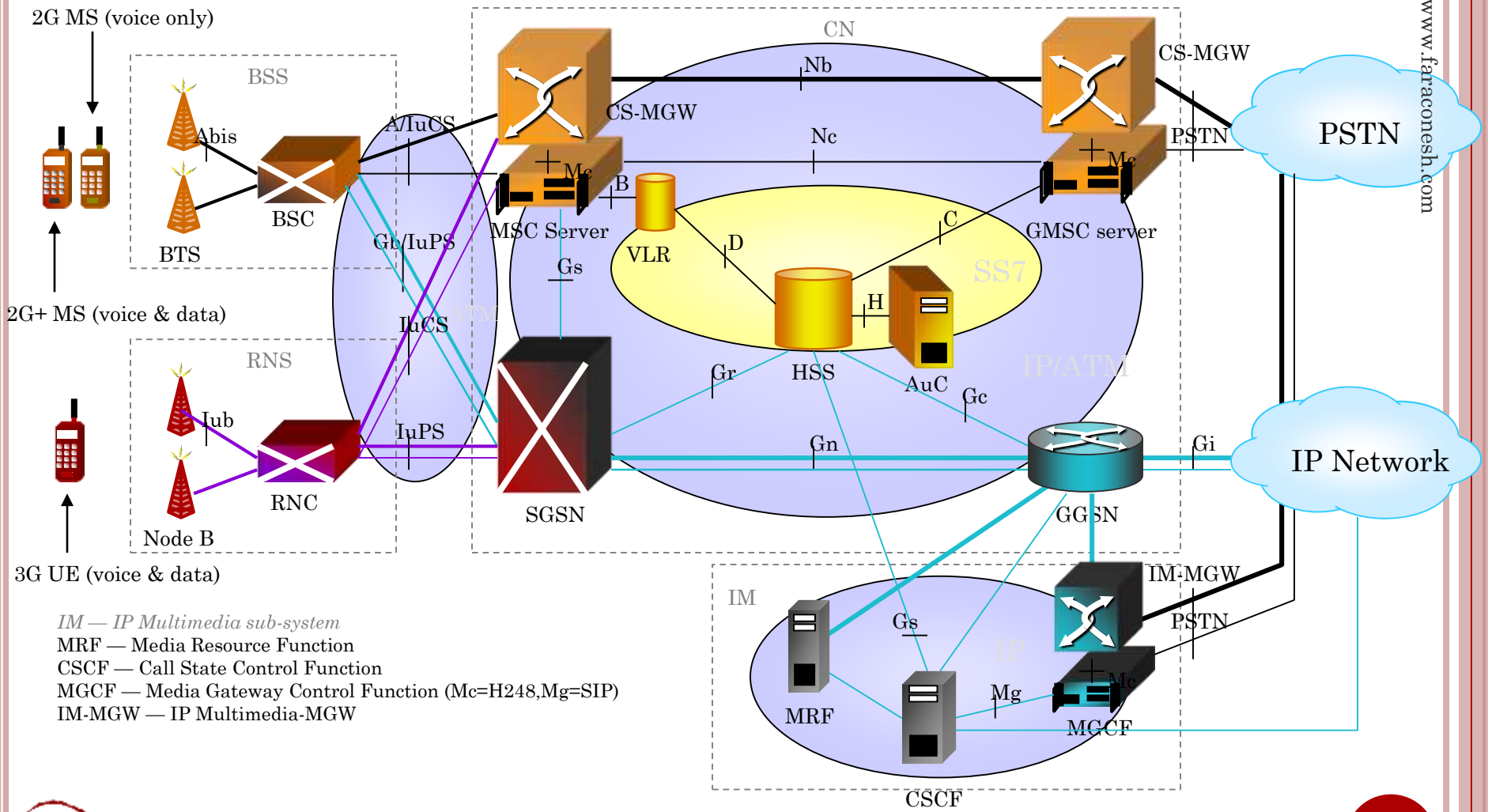
- 1st Phase of the IP Multimedia Subsystem (IMS)
  - Enable standardized approach for IP based service provision
  - Media Resource Function (MRF)
  - Call Session Control Function (CSCF)
  - Media Gateway Control Function (MGCF)
- CS Domain :
  - MSC and GMSC
    - Control Function, can control multiple MGW, hence scalable
  - MSG
    - Replaces MSC for the actual switching and routing
- PS Domain :
  - Very similar to R'99 with some enhancements



Dr. Shahram Bijani, www.faraconesh.com

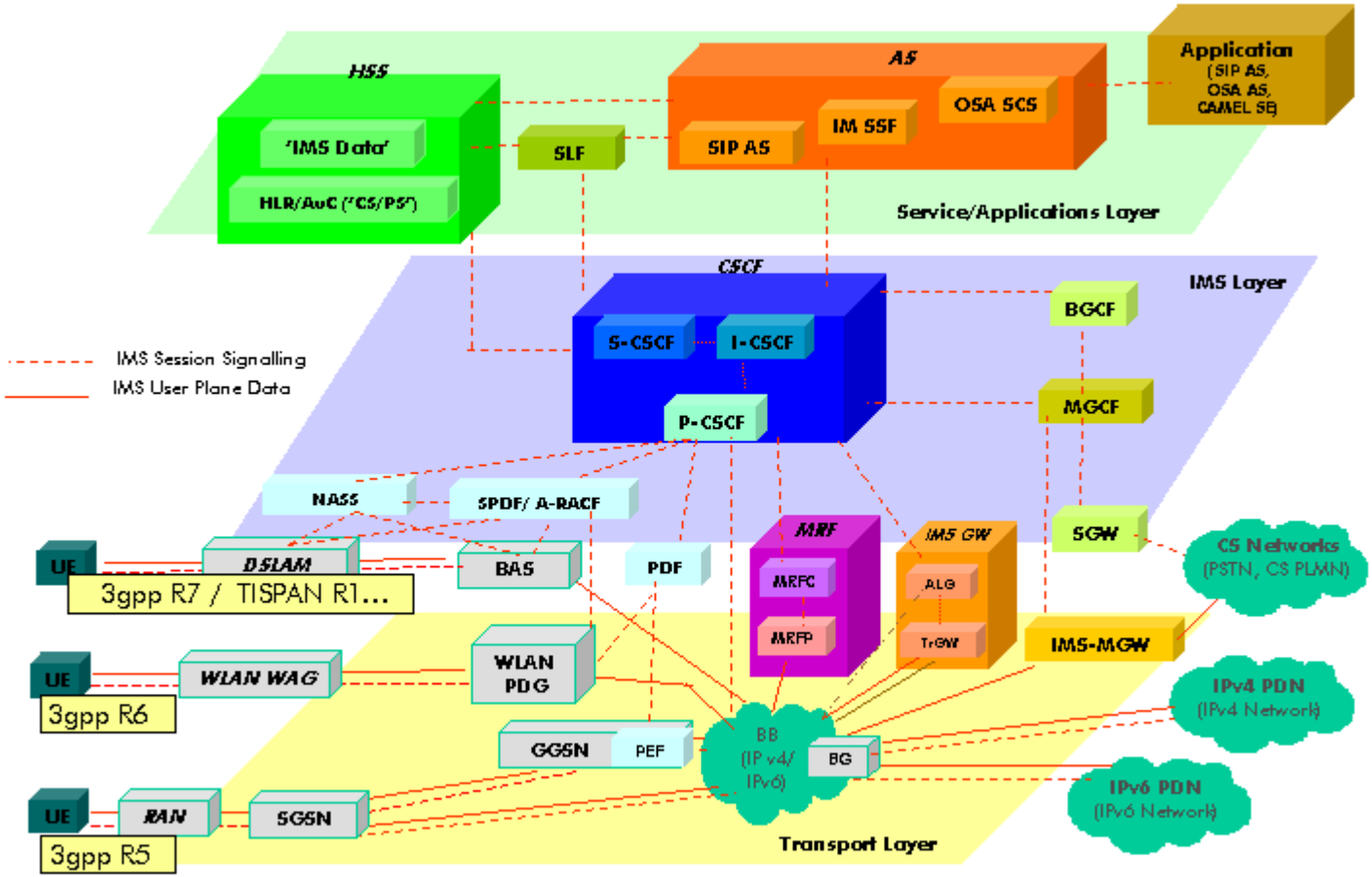
3G REL5 ARCHITECTURE (UMTS) — *IP MULTIMEDIA*

Dr Shahriar Bijani, www.faraconesh.com



IM — IP Multimedia sub-system
MRF — Media Resource Function
CSCF — Call State Control Function
MGCF — Media Gateway Control Function (Mc=H248,Mg=SIP)
IM-MGW — IP Multimedia-MGW

2. IMS Architecture 2



Dr Shahriar Bijani, www.faraconesh.com

2. IMS Protocols

Signalling Plane - Session Control Protocol - SIP (Session Initiation Protocol, RFC 3261 by IETF):

- Protocol to establish and manage Multimedia sessions over IP networks.
- Follows client-server model
- Design borrowed from SMTP and HTTP
- Text-based

(CS analogy – ISUP + IN protocols)

Authentication, Authorization, Accounting – Diameter (Radius based)

Media Plane:

- H.248 (signaling nodes to control nodes)
- RTP (RealTime Transport Protocol) – RT Media transport – A&V

Dr Shahriar Bijani, www.faraconesh.com

Diameter Protocol Background

- Diameter is a Attribute-Value Pairs (AVP) protocol for authentication, authorization, and accounting (AAA)
- Diameter is a improvement over RADIUS
  - RADIUS cannot deal effectively with remote access, IP mobility and policy control.
- Runs over reliable TCP or SCTP based transport protocol
- Relies on Transport Level for congestion management
- TCP and SCTP based network congestion procedures
- Drops IP packets during congestion

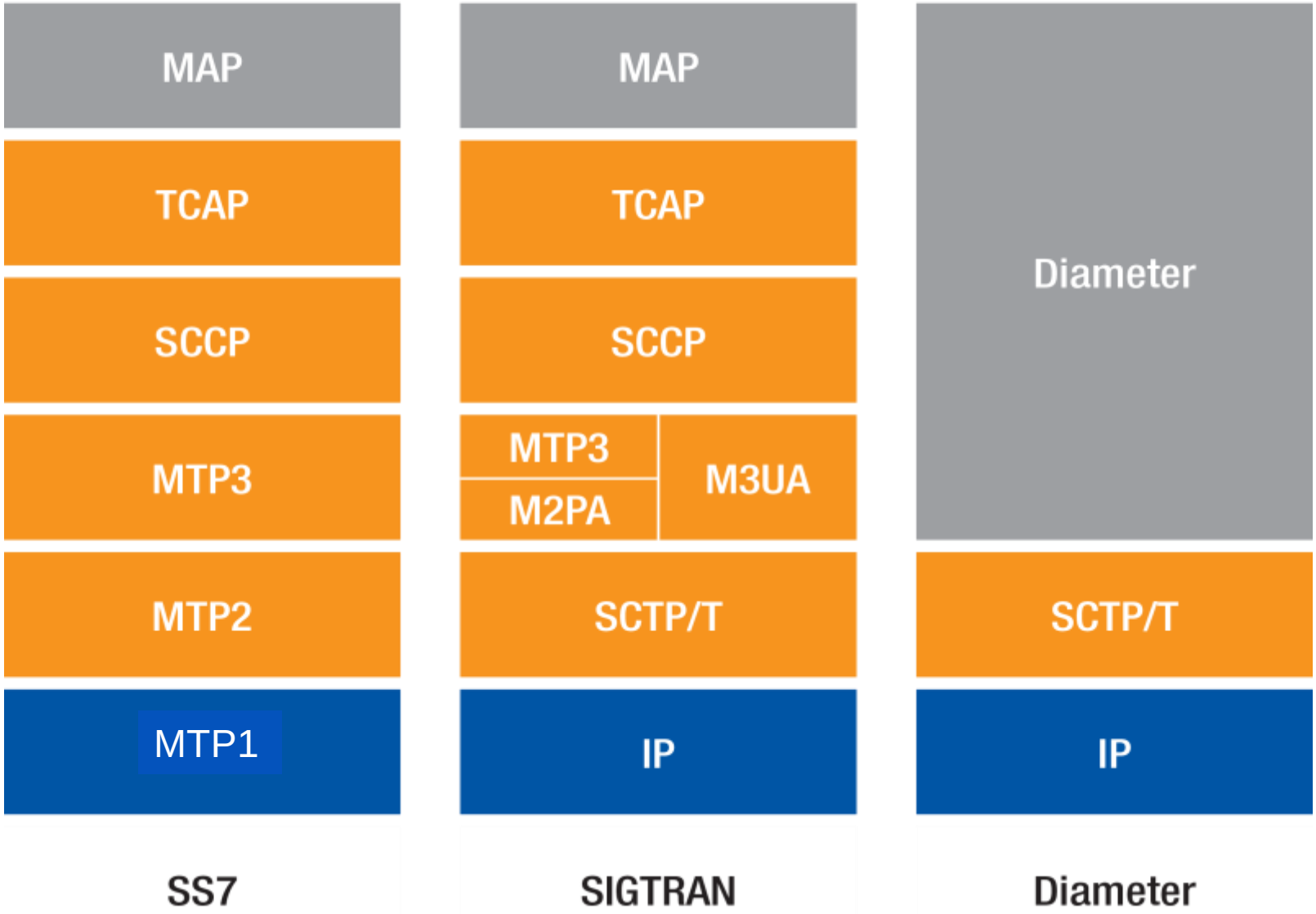
Dr Shahriar Bijani, www.faraconesh.com

Diameter Protocol Background

- Diameter is an IETF defined protocol originally designed for Authentication, Authorization and Accounting (AAA) supporting:
  - Improved failure handling
  - More reliable message delivery
  - Bigger information elements
  - Improved security
  - Extensibility
  - More flexible discovery of other nodes

Dr Shahriar Bijani, www.faraconesh.com

Legacy to LTE



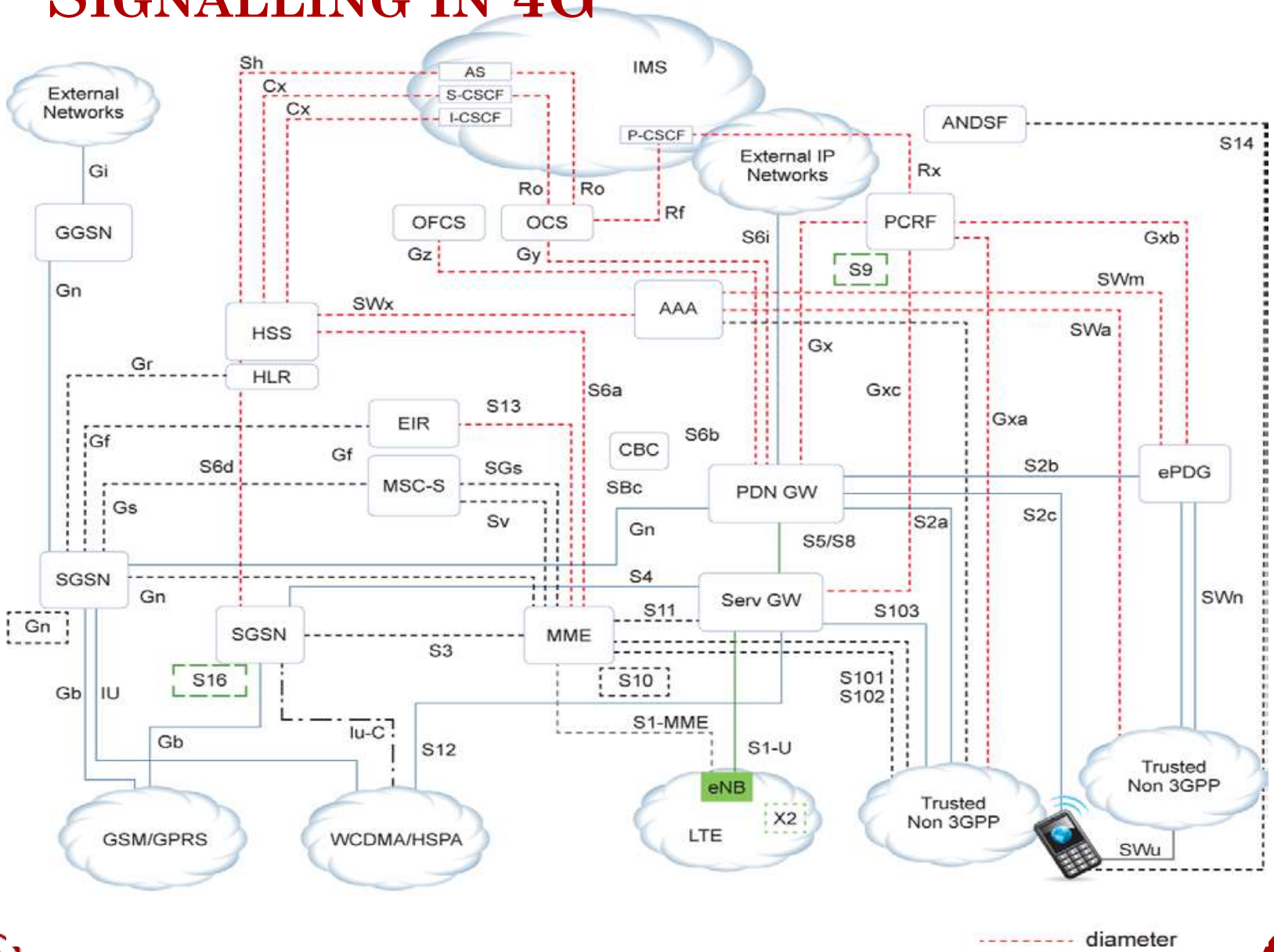
Dr Shahriar Bijani, www.faraconesh.com

Diameter in LTE Network

- 3GPP mandated DIAMETER for Signaling Interface in LTE
  - Replaces Legacy SS7 protocol using TCAP-Query Responses
- Diameter used in the following signaling interfaces
  - MME – Mobile Management Entity (S6a)
  - HSS – Home Subscriber Servers (S6a)
  - EIR – Equipment Identity Register(S13)
  - PCRF – Policy Control Resource Functions (Sy, Gx)
  - Mobility Gateways – SGW/PGW (Gx)
  - IMS – IP Based Multimedia Systems (Cx, Dh, Rf, Ro and Sh)

Dr Shahriar Bijani, www.faraconesh.com

SIGNALLING IN 4G



Dr Shahriar Bijani, www.faraconesh.com