IEEE COMSOC TRAINING™ CONTINUING EDUCATION FOR COMMUNICATIONS PROFESSIONALS

4 Day Intensive Wireless Communications Course

12-15 September 2017

9:00am – 3:00pm EDT each day

Instructor: Alan Bensky

Presented by the IEEE Communications Society

Published September 2017; United States of America.

Instructor

Alan Bensky

MScEE, IEEE WCP, Electronics Engineering Consultant

Alan Bensky is an electronics engineering consultant with over 30 years of experience in analog and digital design, management, and marketing. Specializing in wireless circuits and systems, Alan has carried out projects for varied military and consumer applications and led the development of three patents on wireless distance measurement. Alan has taught electrical engineering courses and lectures on radio engineering topics and is the author of two books: Short-range Wireless Communication, Second Edition, published by Elsevier in 2004, and Wireless Positioning Technologies and Applications, Second Edition, Artech House, 2016. In addition, he is a contributing author to five other books dealing with wireless communication. Alan Bensky holds degrees of B.E.E and B.A. from Union College, Schenectady, New York, and M.Sc.E.E. from the Technion in Haifa, Israel. He is a senior member of IEEE and an IEEE certified Wireless Communications Professional.

4 Day Intensive Wireless Communications

12 – 15 September 2017

Instructor: Alan Bensky

IEEE ComSoc IEEE Communications Society

IEEE

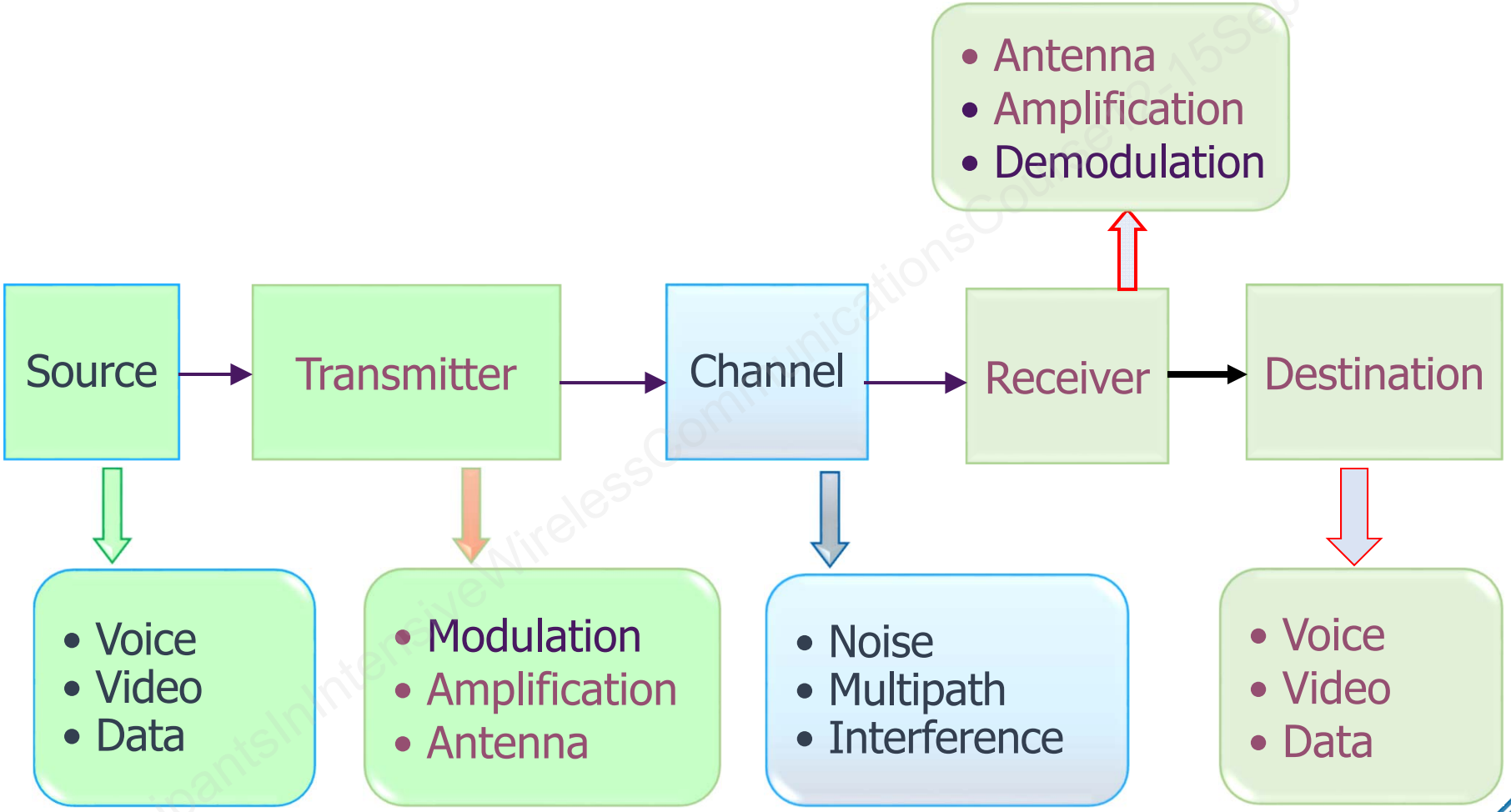
Course Content

- Part 1
  - Fundamentals Review
  - RF Engineering, Propagation and Antennas
  - Wireless Access Technologies
- Part 2
  - Network and Service Architectures
  - Network Management and Security
  - Infrastructure
  - Agreements

Fundamentals Review

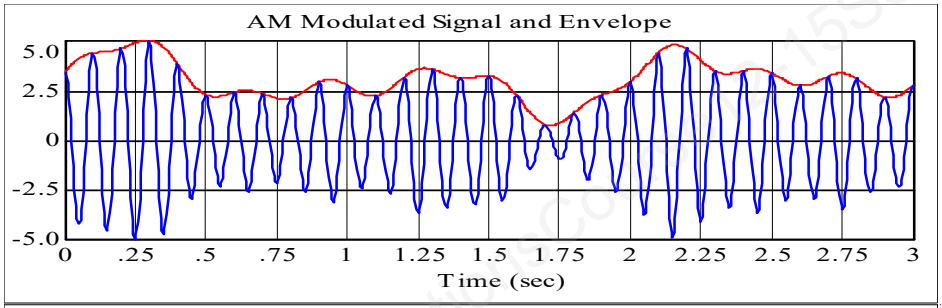
Basic concepts related to electrical engineering, communications systems, and general engineering management.

Wireless Communication System

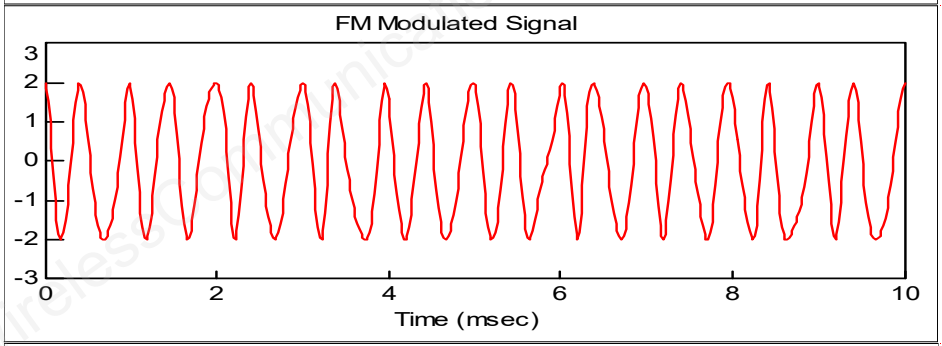


Modulation

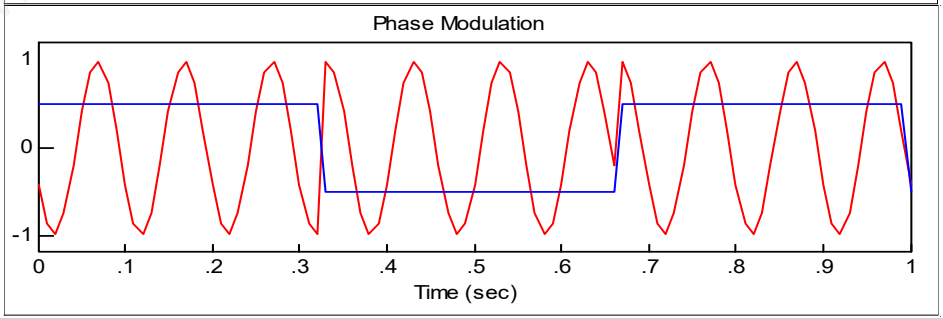
Analog amplitude modulation



Analog frequency modulation

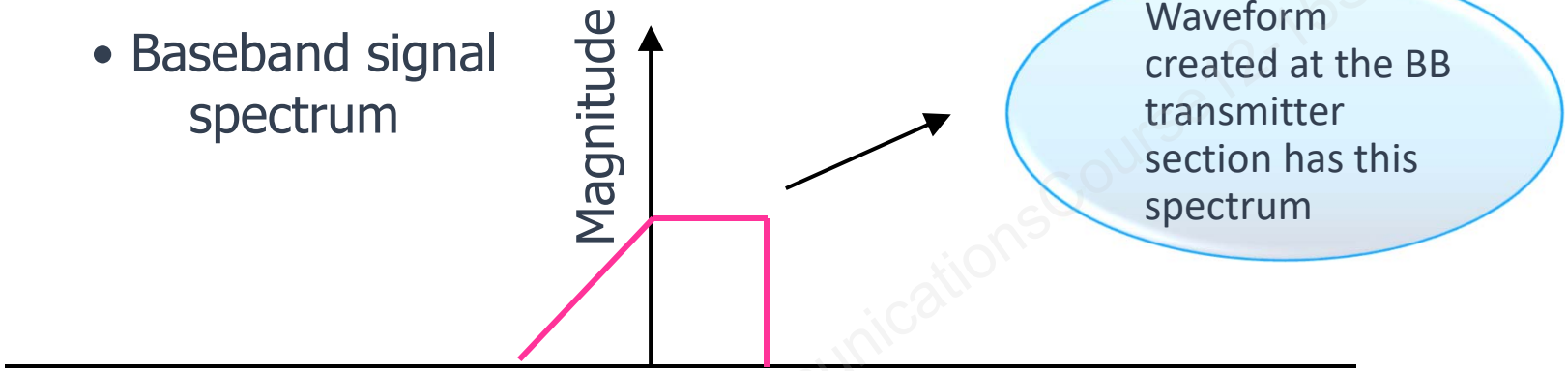


Digital phase modulation



Baseband & Passband

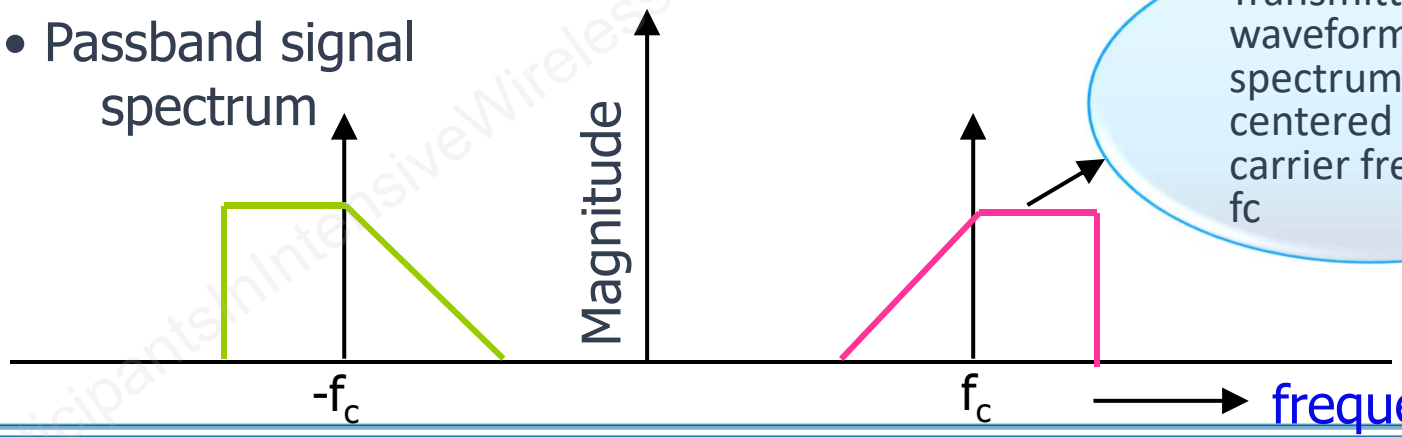
- Baseband signal spectrum



Waveform created at the BB transmitter section has this spectrum

$$s(t) = \mathrm{Re}\{[\, x(t) + jy(t)](\cos\ 2\pi f_c t + j \sin\ 2\pi f_c t)\}$$
$$s(t) = x(t)\cos\ 2\pi f_c t - y(t)\sin\ 2\pi f_c t$$

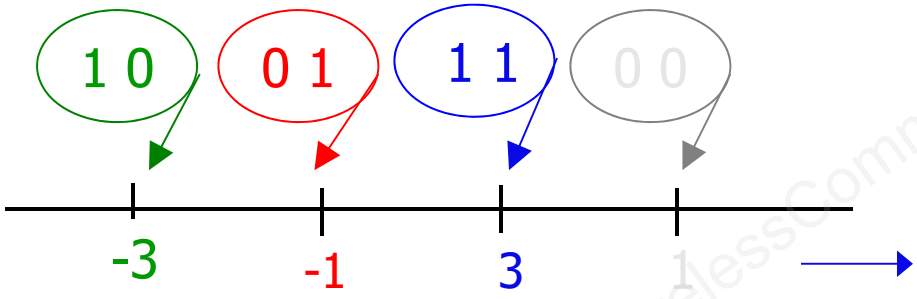
- Passband signal spectrum



Transmitted waveform has spectrum centered at carrier frequency fc

Symbols and Bits

- Can map more than 1 bit to 1 state of the carrier
- Creation of symbols by grouping 2 or more bits together
- Grouping of bits – Spectrally efficient



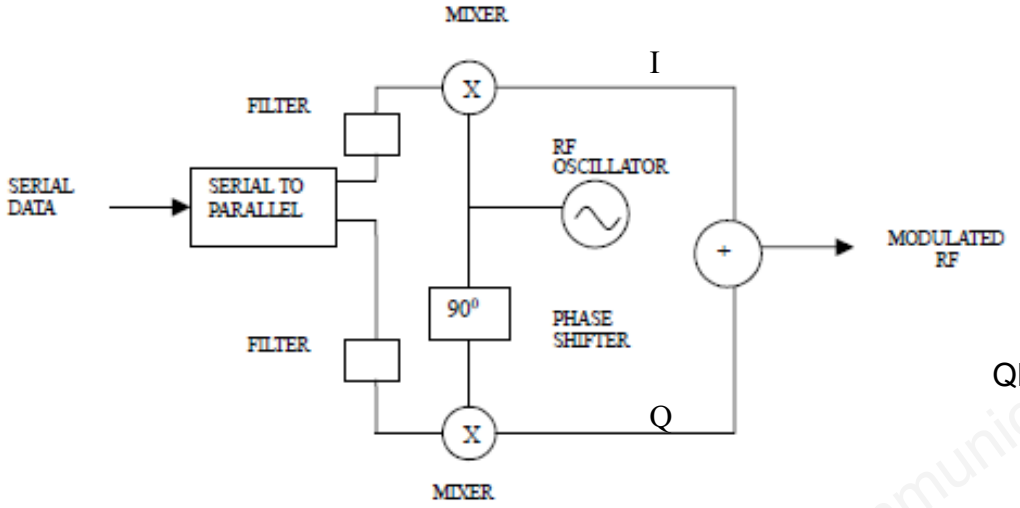
- 4 – Possible Amplitude states
- Carrier state can change every $2T_b$ seconds

$T_s = m*T_b$

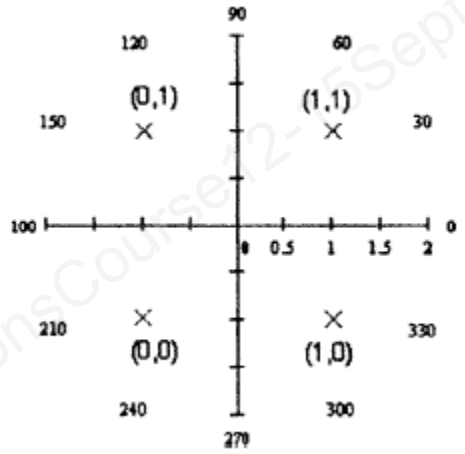
Number of states = 2^m

T_s - Symbol Duration
m - number of bits per symbol
T_b - Bit duration

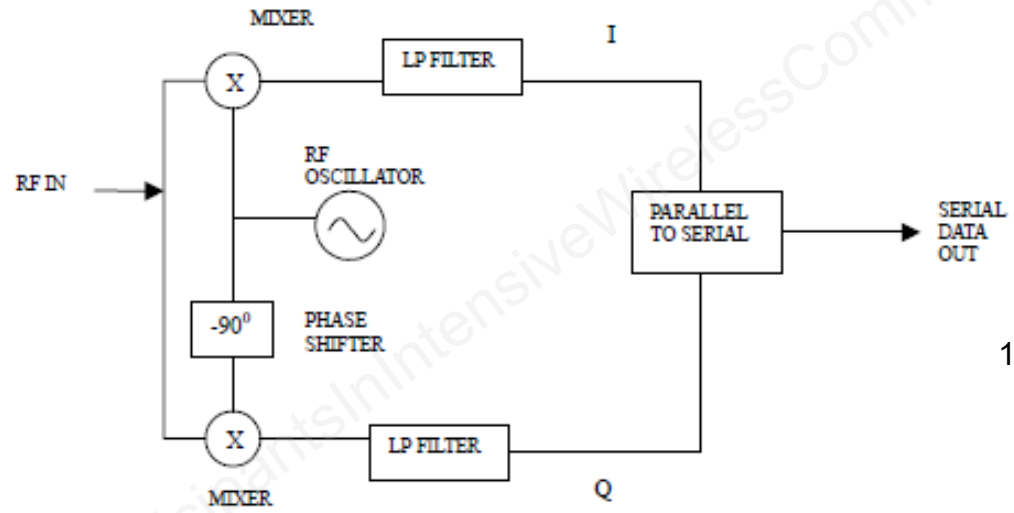
Quadrature Modulation/Demodulation

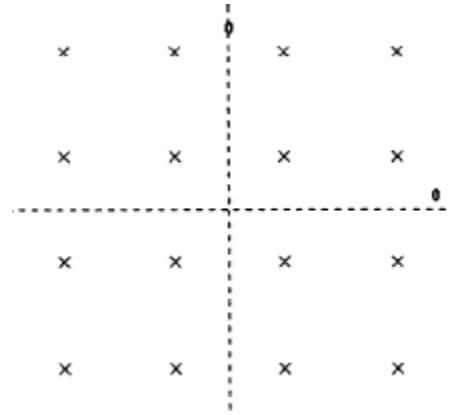


CONSTELLATION DIAGRAMS



QPSK





16-QAM

Understanding dBs

- Useful in representing voltage and power ratios; Gain and Loss are the typical parameters in a system
- dB is a ratio of two similar quantities expressed in logarithmic scale
- Relation between the linear values and dB value is given as

$$dB = 10\log_{10}(P_1/P_2)$$

- 3dB increase in dB corresponds to $P_1=2*P_2$

Understanding dBms

- dBm- used to measure absolute power with reference to 1 mW

$$P_{dBm} = 10 * \log_{10}(P / 1mW)$$

- 0dBm corresponds to 1 mW. Values between 0 mW and 1 mW takes negative dBms
- In wireless systems, transmit and receive powers are represented using dBm
- dBW, dBi and other variants of dB are used wherever appropriate

Information Theory – Capacity

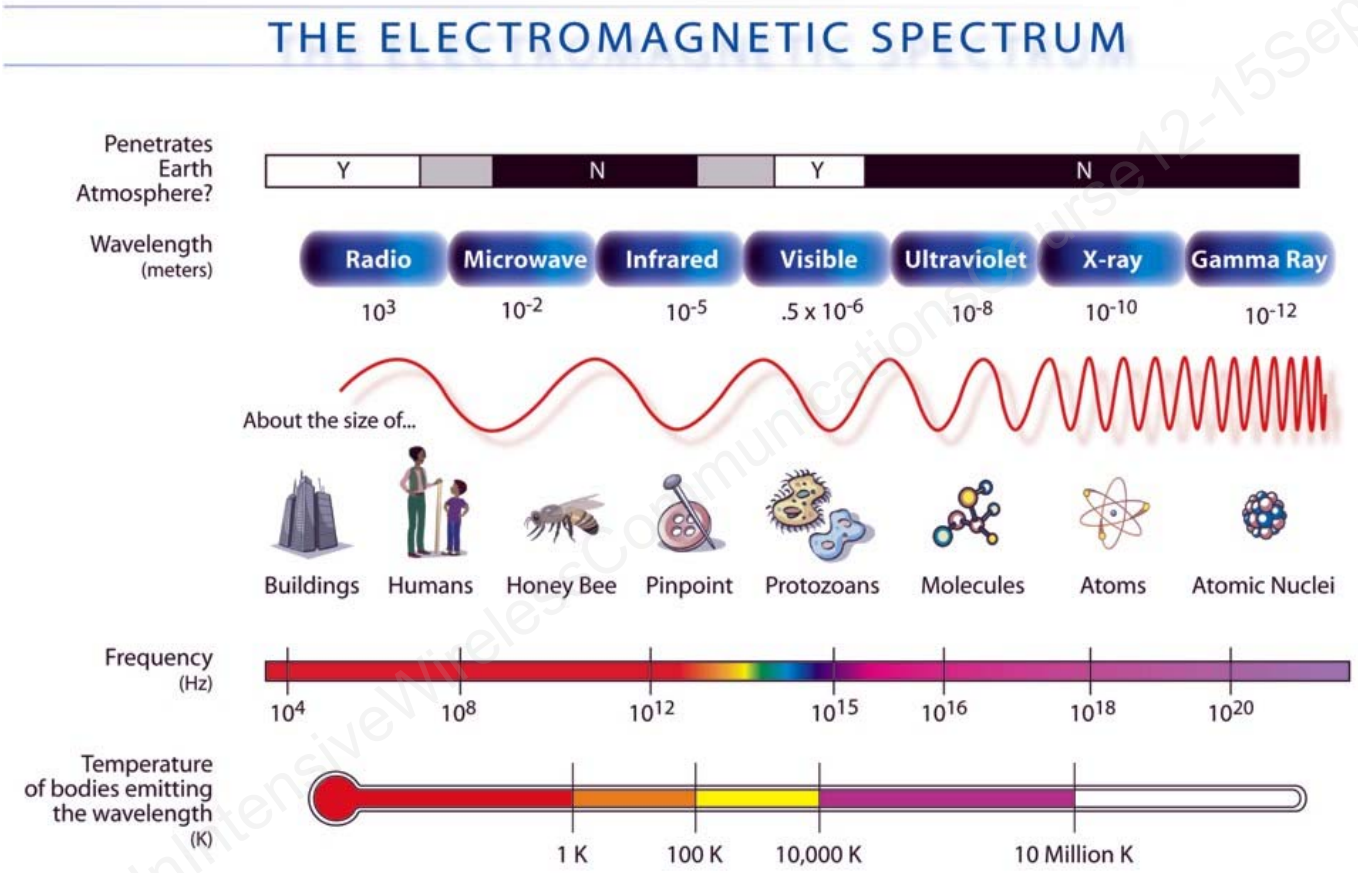
- Shannon's capacity of a channel perturbed by noise is a function of received signal power, noise power density, and bandwidth.
- Capacity:

$$C = B \cdot \log_2(1 + SNR) \qquad SNR = \frac{P}{B \cdot N_0}$$

$$\lim_{B \to \infty} (C) = \frac{1}{\ln(2)} \left(\frac{P}{N_0} \right)$$

- It is possible to transmit at rate R, { R <= C }, with sufficiently small probability of error, with complex coding.

Frequency Spectrum



Wavelength in meters is 300/*f*(MHz)

RF Engineering, Propagation and Antennas

Antenna properties and types, wave propagation, channel modeling, RF engineering.

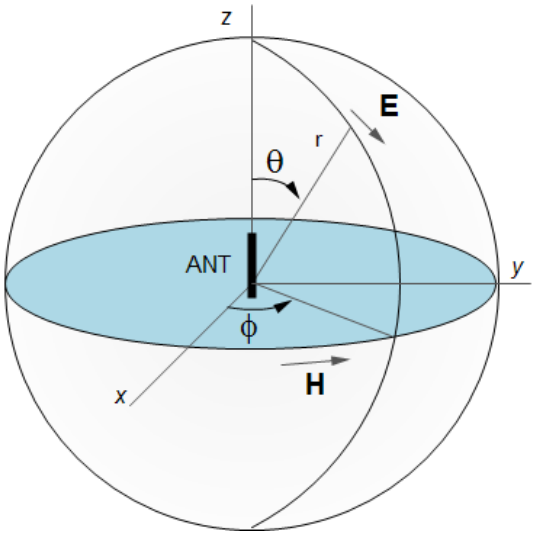
IEEE ComSoc IEEE Communications Society

IEEE

Antennas

- Antenna Properties
  - Directivity, gain, beamwidth
  - Effective Aperture
  - Radiation efficiency
  - Feed impedance
  - Bandwidth
  - Polarization
- Phased Arrays, beamforming
- Antenna Types

Radiation and Directivity



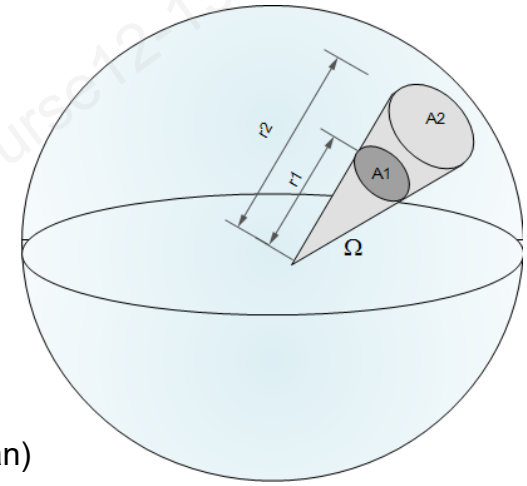
power density $S = \frac{1}{2} E \times H^*$

radiation intensity $U(\theta,\phi) = S(\theta,\phi) r^2$

radiated power $P = \iint_{S_{ff}} S \cdot ds$

$P = \iint U(\theta,\phi) d\Omega \quad d\Omega = \sin(\theta) \cdot d\theta \cdot d\phi$

$$U_{avg} = \frac{P}{4\pi} \quad W/sr$$ (sr=steradian)



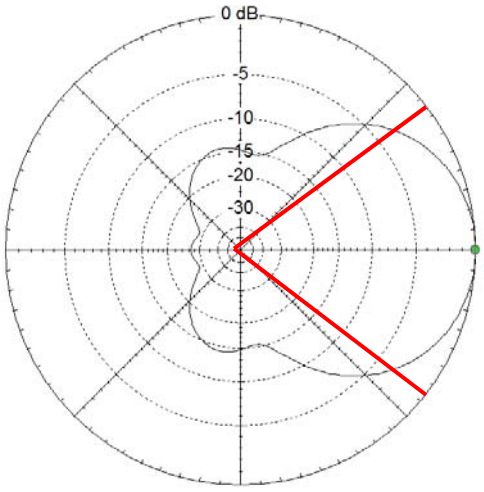
$$S_{avg} = \frac{P}{4\pi \cdot r^2} \quad W/m^2$$

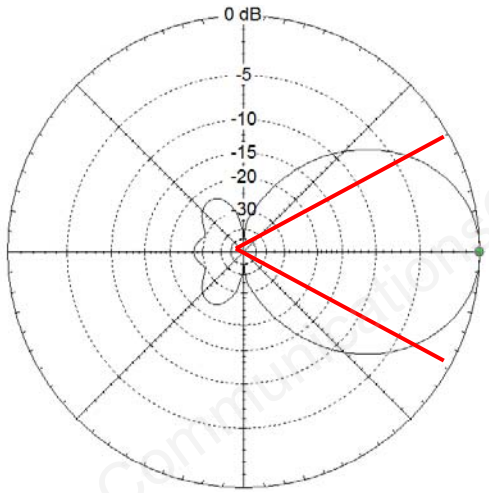
$S1 \cdot r1^2 = S2 \cdot r2^2$

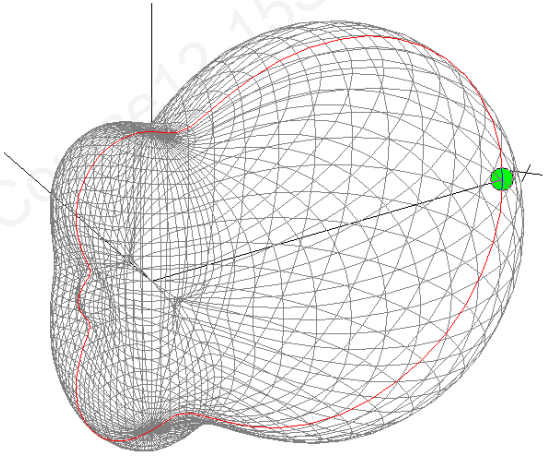
directive gain $D(\theta,\phi) = U(\theta,\phi) / U_{avg} = S(\theta,\phi) / S_{avg}$

directivity $D = U_{\max} / U_{avg} = S_{\max} / S_{avg}$

Directivity vs. Beam Width







Vbw=72.6 deg *Hbw=54.3 deg*

half power beam widths

$$D \approx \frac{4}{\pi}\frac{180 \cdot 180}{Hbw \cdot Vbw} \qquad D_{dB} = 10\log(D)$$

DdB~10.2dBi

DdB=9.84dBi

(true, calculated from pattern)

(no side lobes, low directivity antennas)

Directivity, Aperture, and Gain

D=Directivity
P_A=available power
S=power density
A_e=(max.) effective aperture
A_p=physical aperture
e_{ap}=aperture efficiency
e_r=radiation efficiency

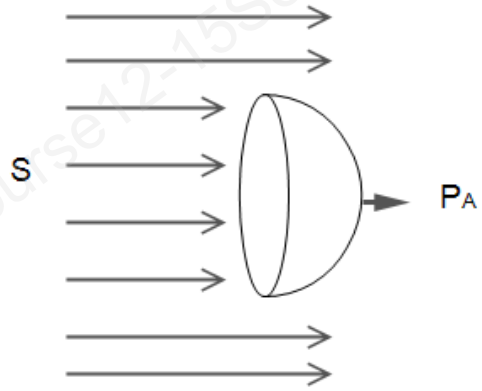
$$P_A = A_e \cdot S$$

$$\boxed{D = \frac{4\pi}{\lambda^2} A_e}$$

$$A_e = e_{ap} A_p$$

$$G = e_r \cdot D$$

$$G_{dB} = 10\log(G)$$



Gain is referred to a specific reference:

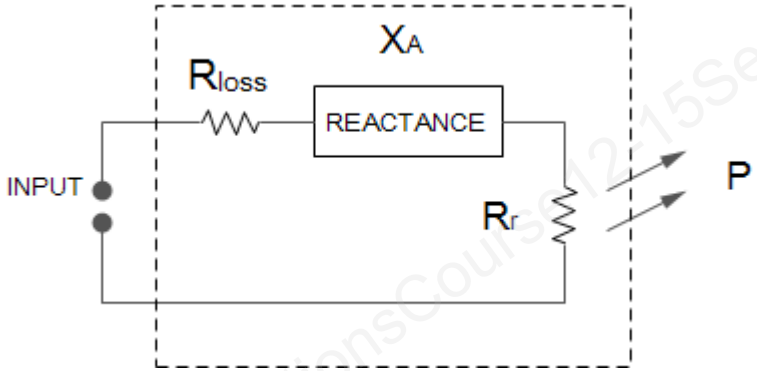
- dBi: relative to an isotropic antenna
- dBd: relative to a half-wave dipole antenna, 0dBd = 2.15dBi
- dBic: relative to a circularly polarized isotropic antenna

Antenna Impedance

$$Z_A = R_A + jX_A$$

$$R_A = R_r + R_{loss}$$

$$P_{in} = \tfrac{1}{2} R_A |I_A|^2$$



radiation resistance $R_r = \dfrac{2P}{|I_A|^2}$

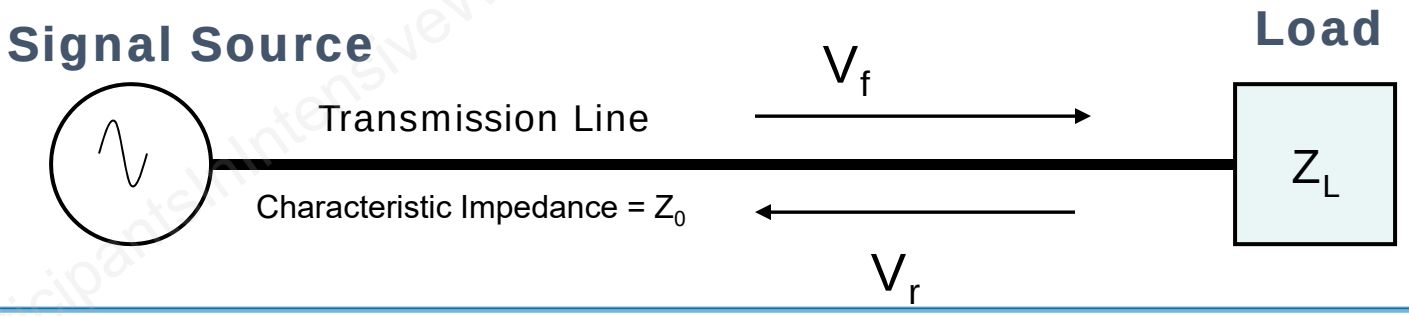
radiation efficiency $e_r = \dfrac{P}{P_{in}} = \dfrac{R_r}{R_A}$

reflection coefficient: $\rho = \dfrac{V_r}{V_f} = \dfrac{Z_L - Z_0}{Z_L + Z_0}$

$VSWR = \dfrac{1+|\rho|}{1-|\rho|}$

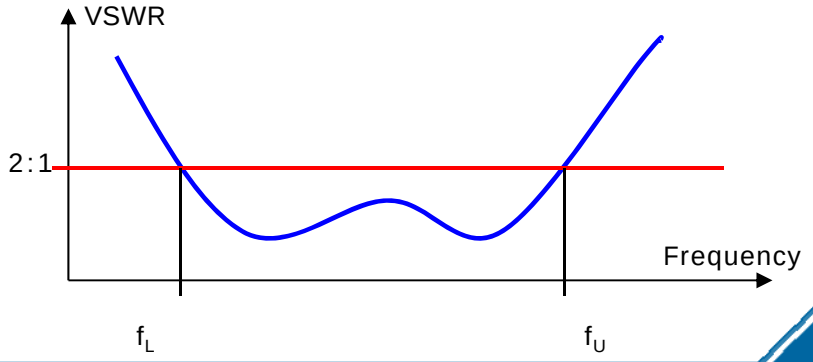
return loss: $RL = -20\log|\rho|$

matching loss: $ML = -10\log\left(1-|\rho|^2\right)$



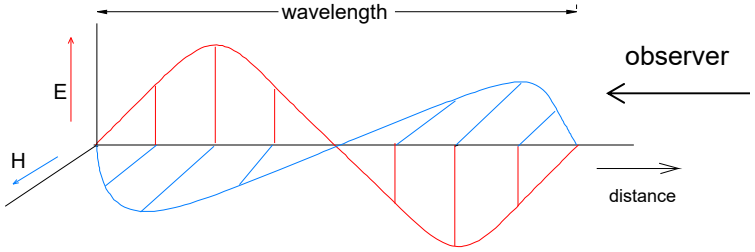
Antenna Bandwidth

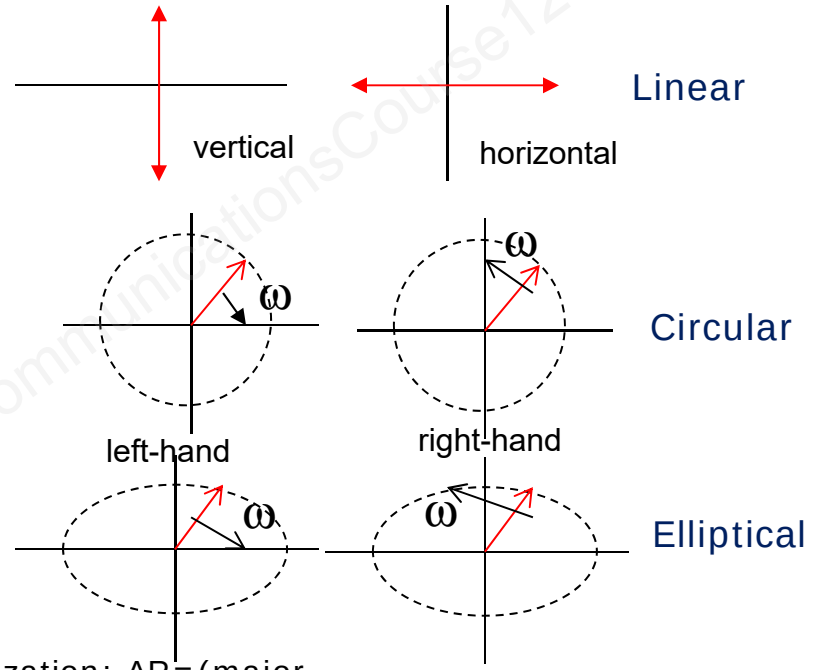
- Frequency range over which some parameter varies within a prescribed limit
- Types of bandwidth
  - Impedance (< 2:1 VSWR) ← most common
  - Gain (-3 dB)
  - Beamwidth
  - Axial Ratio (measure of circular polarization) (3 dB)
- Can be expressed in absolute frequency (KHz, MHz, GHz) or as a percentage bandwidth (referenced to center frequency)



Polarization

Polarization of an electromagnetic wave is defined as the orientation of the electric field vector as it travels through space





Axial Ratio (AR) is measure of circularity of polarization: AR=(major axis)/minor axis)

expressed in dB: 20log|AR|

0 dB, perfectly circular

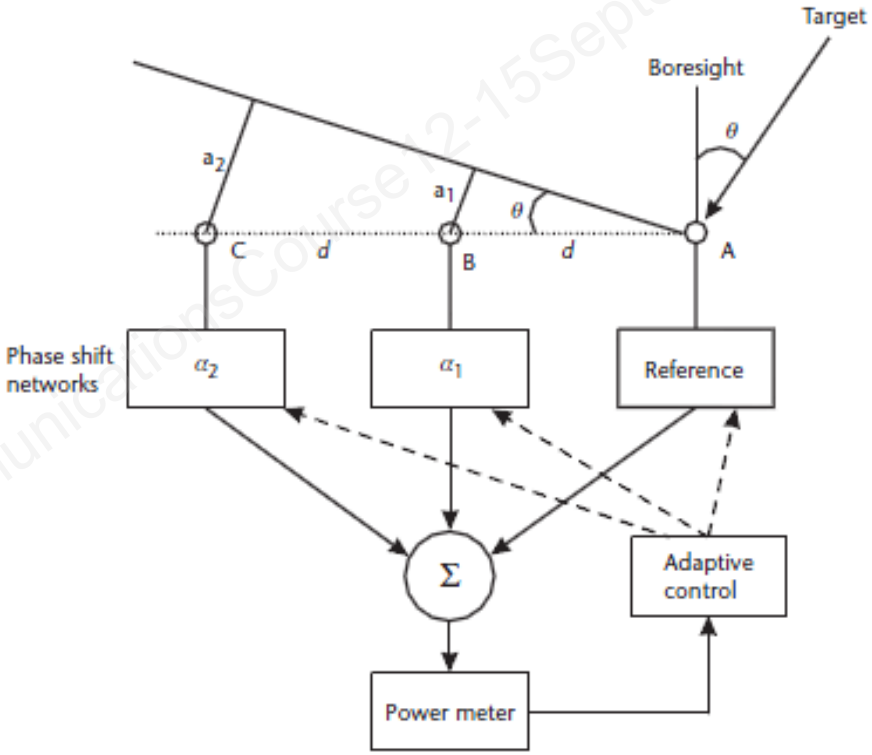
∞ dB, perfectly linear

Polarization Mismatch

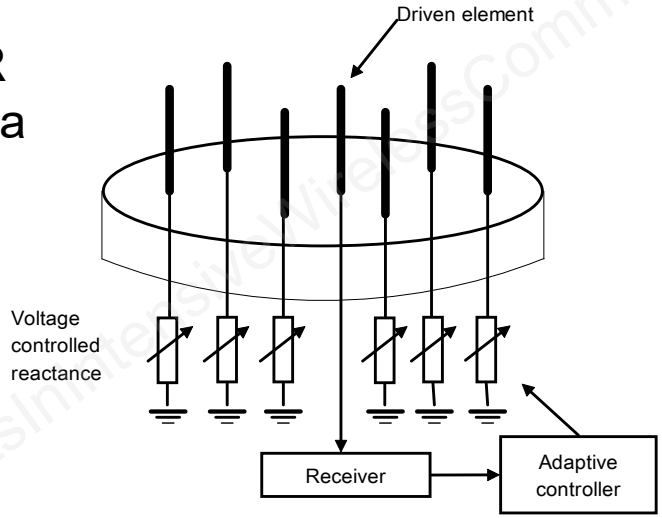
- Transmitting and receiving antennas must have polarization match to minimize power loss
- Polarization mismatch is a significant concern in wireless system design and operation
  - As example, a linearly polarized antenna can receive circularly polarized signal but with 3 dB loss
- In theory, an antenna designed for vertical polarization will not be able to receive a horizontally polarized signal. In practice there is a very small amount of HP signal present and this is called the cross-polarization (or cross-pol) term
- Polarization diversity

Smart Antennas

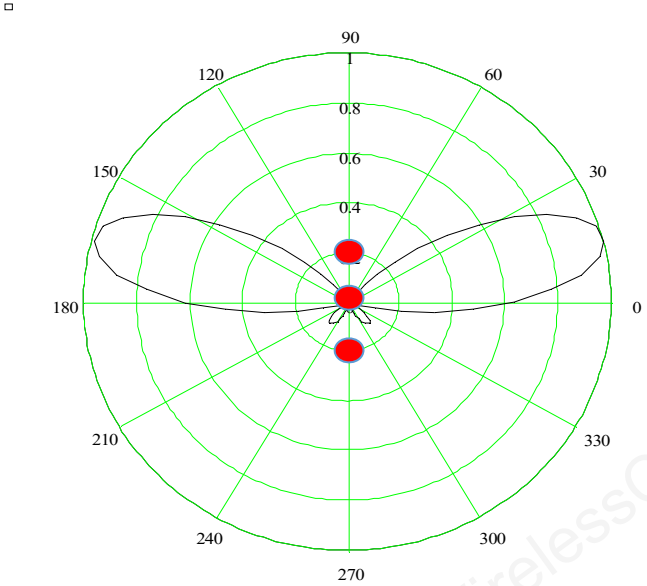
- Beam steered phased array, adaptive array
- Pattern shape depends on
  - element type
  - geometric configuration
  - element feed current vector
- Adjust for peak or null in desired directions



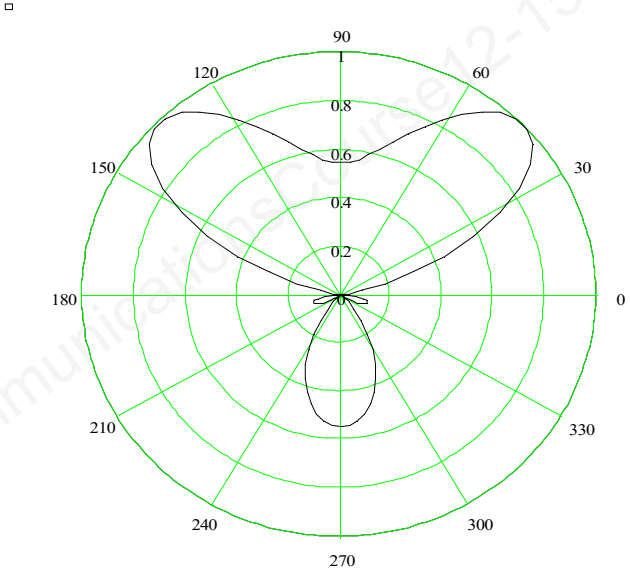
ESPAR Antenna



Beam Forming



15 deg



45 deg

Three isotropic elements

Antenna Types

Electrically Small

- low directivity
- low input resistance
- high input reactance
- low radiation efficiency

Resonant

- low to moderate gain
- real input impedance
- narrow bandwidth

Broadband

- low to moderate gain
- real input impedance
- wide bandwidth

Aperture

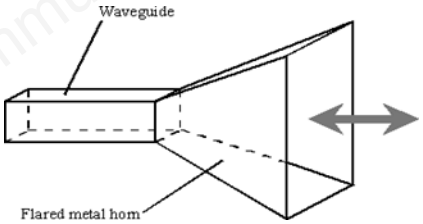
- high gain
- increased gain with frequency
- moderate bandwidth

Common Antennas by Frequency

- HF: f <= 30 MHz – wire antennas, rhombic, V
- VHF: 30 MHz < f < 300 MHz – Monopole, Yagi (parasitic element beam antenna)
- UHF: 300 MHz < f < 3 GHz – Monopole, Yagi, PC planar antenna (patch), Inverted F
- uWave: > 3 GHz – Horn, dish, helical (axial), lens

Yagi

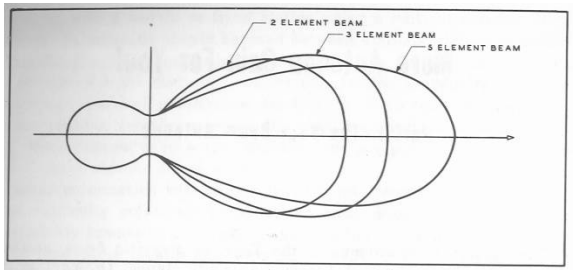
Parabolic Dish



Horn

Planar Array

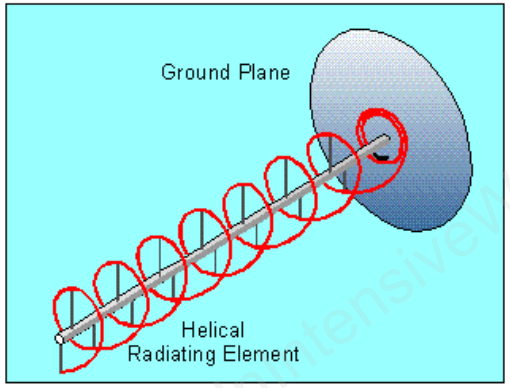
Yagi Antenna



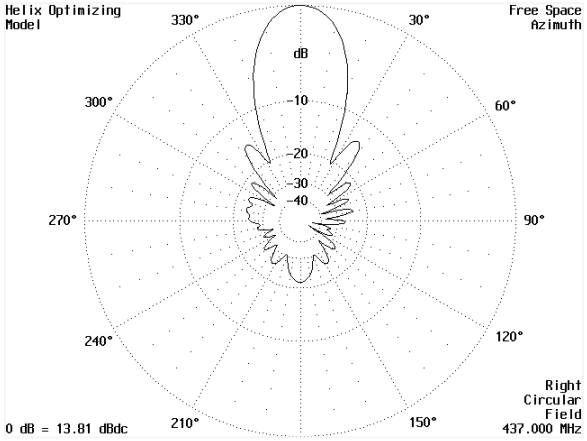
- Formal name Yagi-Uda antenna
- Consists of single driven element and one or more parasitic elements (reflectors and directors) to provide gain
- Elements can be half-wavelength dipoles, or full wavelength loops (quads)
- Crossed dipole yagis can be used to create circular polarization
- Moderate gain (6 – 20 dB)
- Relatively narrow impedance bandwidth (~ 2-5 % typically)
- Common Applications: VHF/UHF earth stations, WLAN

Helical Antennas

- Helically wound radiating element and reflecting ground plane
- Radiates endfire
- Moderate gain (typically 10-20 dB depending on axial length)
- Wide impedance and gain bandwidth (50%)
- Helix circumference approximately 1 λ, spacing between turns 0.25 λ
- Commonly used at VHF/UHF
- Circular polarization



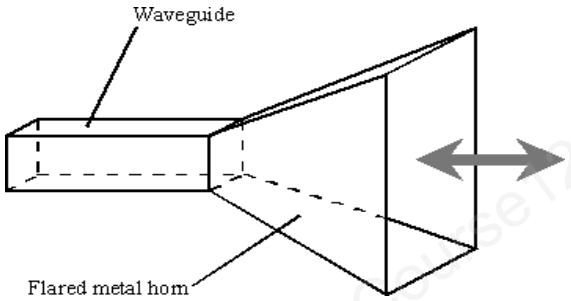
helical antenna

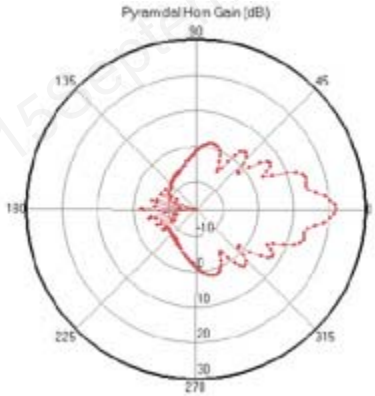


Dish Antennas

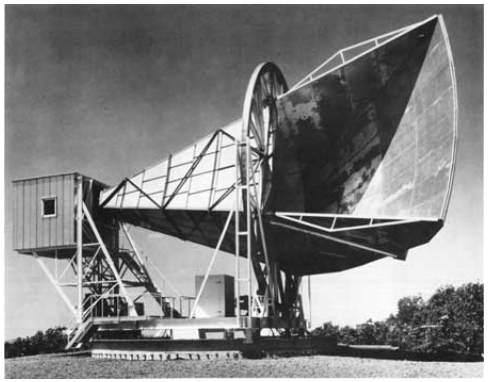
- Most common antenna associated with SATCOM
- Surface shape parabolic
- Energy from the feed is reflected by the dish and focused to a tight beam
- Surface smoothness and shape important
- Characteristics:
  - High gain (10 – 50 dB depending on size)
  - Narrow beamwidth (can be fractions of a degree)
  - Diameter large compared to wavelength (10’s – 1000’s)
- Common Applications
  - Satellite communications
  - Terrestrial microwave links

Horn Antennas





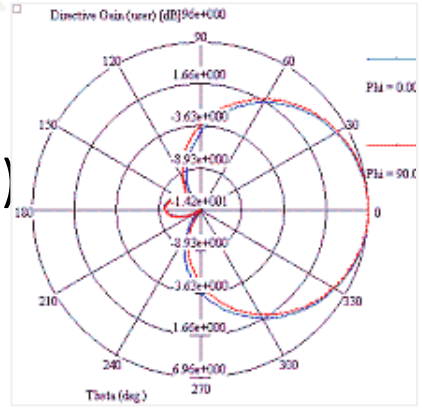
- Waveguide feeding flared metal horn
- Can be rectangular or conical
- Linear or circular polarization
- Wide bandwidth
  - determined by waveguide bandwidth
  - ridged horns can have multiple octave BW
- Well defined pattern and gain behavior
- Common applications
  - Dish feeds
  - Gain standards
  - Array elements

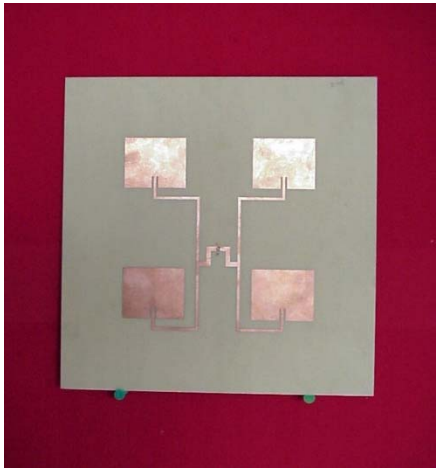


Patch Antenna

- Antennas formed by etching structures on PCB material (microstrip)
- Back of material is solid ground plane
- Rectangular patch dimensions ~ 0.5λ in PCB
- Impedance bandwidth usually narrow, 2-5%
  - Other designs have
  - wider bandwidths
- Pattern is broad,
- gain low (0-6 dBi or worse)
- Common applications
  - GPS receivers
  - Elements in arrays

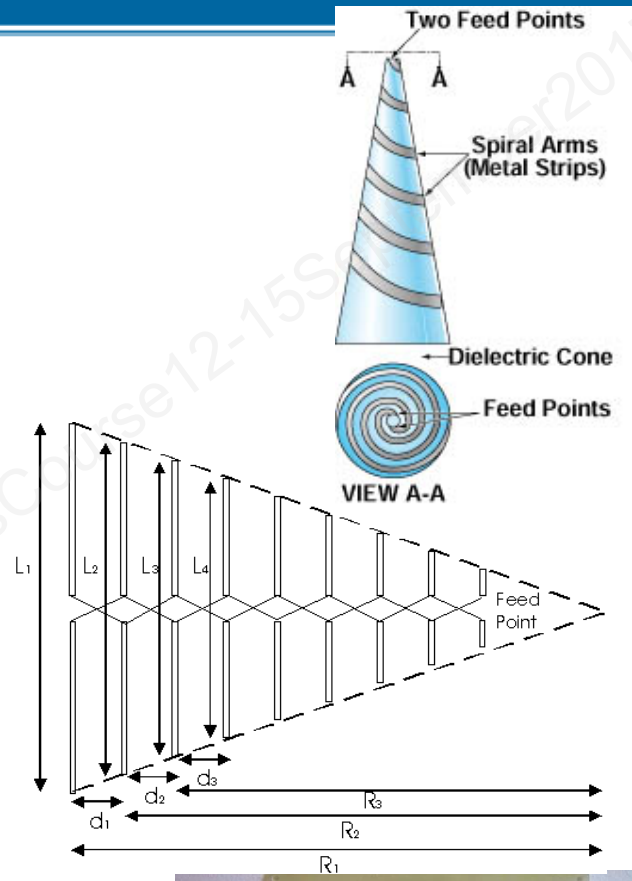
GPS antenna 25 mm x 25 mm x 4 mm



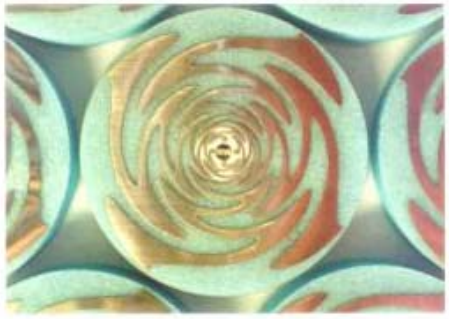


Wideband Antennas

- Class of frequency independent antennas
  - Very wide impedance bandwidths, 2:1 to 10:1 bandwidths
  - Geometries are defines by angles
  - Gain usually low (0 – 12 dBi)
  - Beamwidth usually large
- Common frequency independent antenna
  - Log periodic dipole array
  - Spiral
  - Conical spiral
  - Sinuous

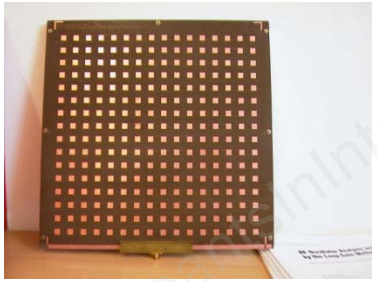


Planar Sinuous Antenna



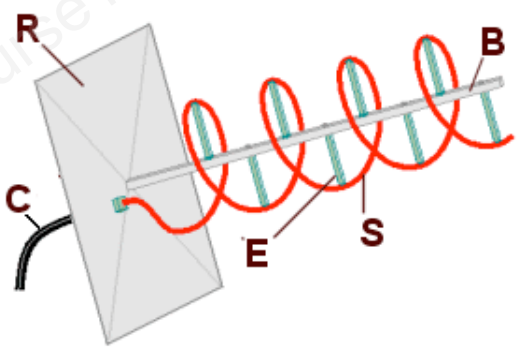
Phased Array Antennas

- An array consists of two or more antenna elements located and fed such that their fields add in certain directions and cancel in others
- Elements can be any type of antenna, from patches (small) to dishes (big)
- The spacing of the antennas, and the electrical phasing and amplitudes of the individual element feeds is critical to the array performance



Mobile Handset Antennas

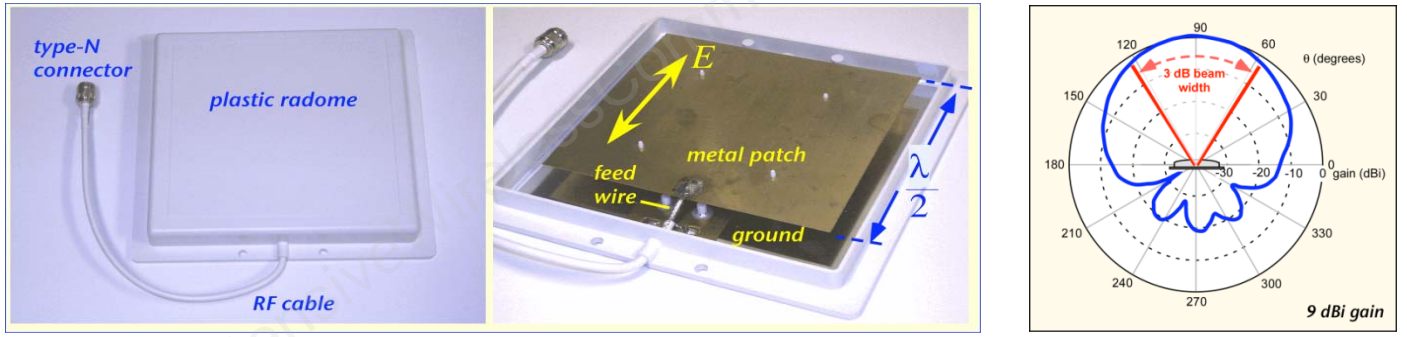
- Complicated design due to severe size constraints and overall system issues
- Typically low-gain and omnidirectional, and have to be small.
- A retractable monopole is a good (but not preferable) choice for a handset antenna.
- Other popular designs are based on a normal-mode helical antenna (NMHA) that can be easily printed on dielectric film and rolled into a round shape with a dielectric cover to form a short antenna stub for handsets.



B: Central Support,
C: Coaxial Cable,
E: Spacers/Supports for the Helix,
R: Reflector/Base,
S: Helical Aerial Element
Source: wikipedia.org

Mobile Handset Antennas (cont'd)

The planar inverted F antenna (PIFA) is another good design to enclose in handsets; it's a combination of wire- and patch-antenna structures and can also be designed for dual or tri-band use in global roaming handsets



A simple half-wavelength patch antenna and typical radiation pattern at 900MHz

.Source: wikipedia.org

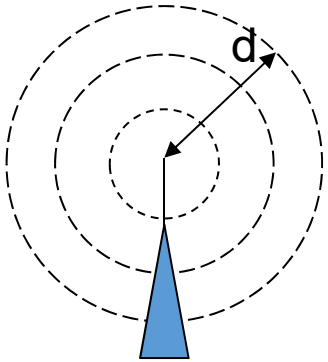
Practice Questions (1)

1. 64-QAM modulation improves spectral efficiency over 16-QAM by a) 4 times, b) 2 times, c) 50%, d) 25%
2. 13 dBm refers to a power of a) 10 mW, b) 20 mW, c) 50 mW, d) 100 mW
3. The gain of an efficient UHF antenna with vertical and horizontal beam widths, at 3 dB down, of 23 and 15 deg is approximately
   a) 94 dB
   b) 20 dB
   c) 6 dB
   d) 32 dB
4. An antenna and feed has a return loss of 10 dB. What is the approximate VSWR?
   a) 2
   b) 2.5
   c) 3
   d) 4

Radio Wave Propagation

- Path Loss
  - Line of Sight (LOS), Non Line of Sight (NLOS)
  - Reflection, Diffraction, Scattering
  - Multipath
  - Fading
- MIMO Technology
- Link Budget
- Propagation Models
- Software Modeling Tools

LOS (Free Space) Propagation



P_t=power to Tx antenna
G_t=Tx ant. gain
G_r=Rx ant. gain
A_e=Rx ant. effective area

Power density on surface of sphere:

$$S(r) = P_t G_t / (4\pi \cdot d^2)$$

Received power:

$$P_r = S(r) \cdot A_e \qquad A_e = \frac{G_r \lambda^2}{4\pi}$$

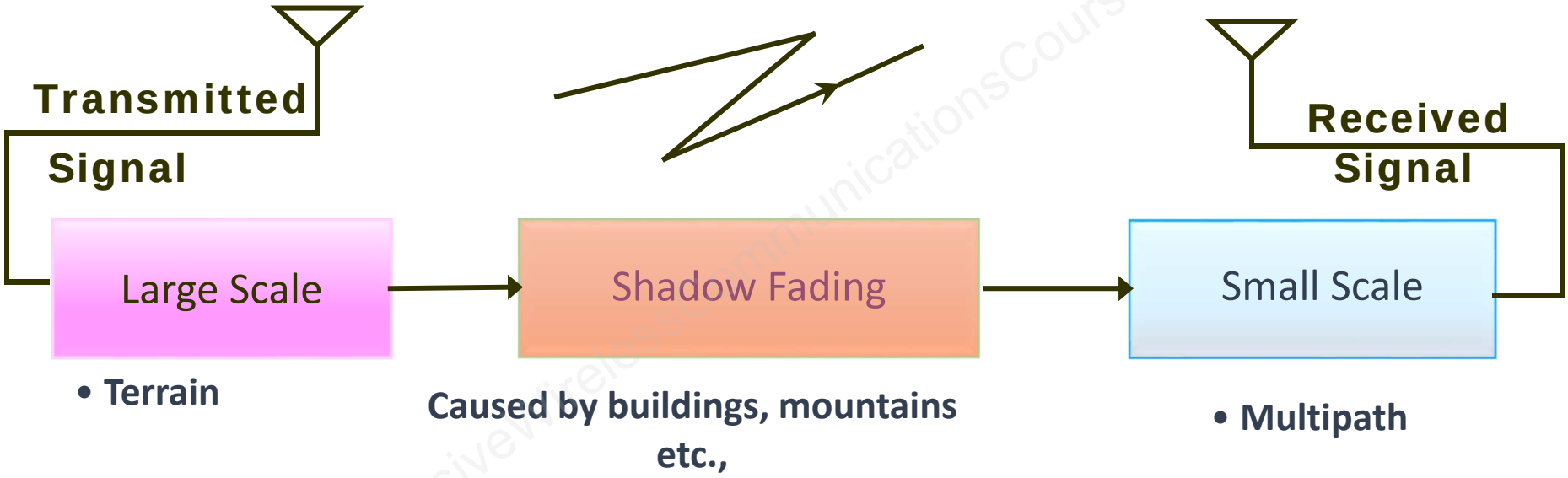
Friis Equation:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi \cdot d} \right)^2$$

Valid in far field $d > \frac{2D^2}{\lambda}$ D is largest ant. dimension

Non Line of Sight (NLOS)

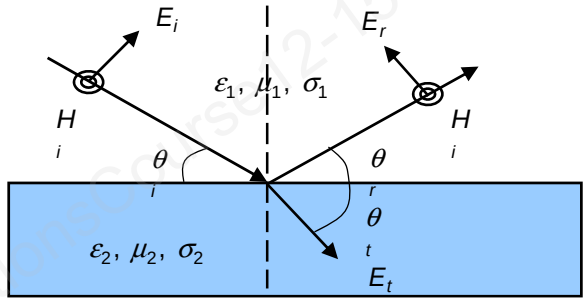
Path Loss Components



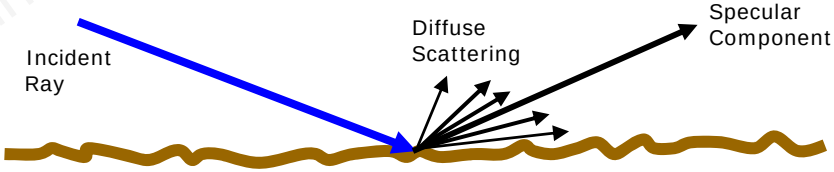
Propagation Mechanisms

Three basic mechanisms to impact propagation in communications system

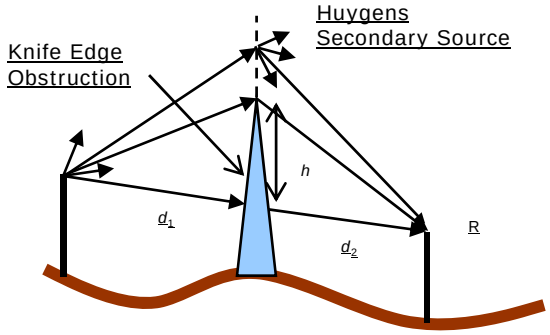
- **Reflection:** Electromagnetic wave impinges upon object with large dimension compared to λ, e.g. buildings and wall.



- **Scattering:** obstructing objects are numerous and having smaller dimensions than λ, e.g., foliage, street signs, lamp posts.

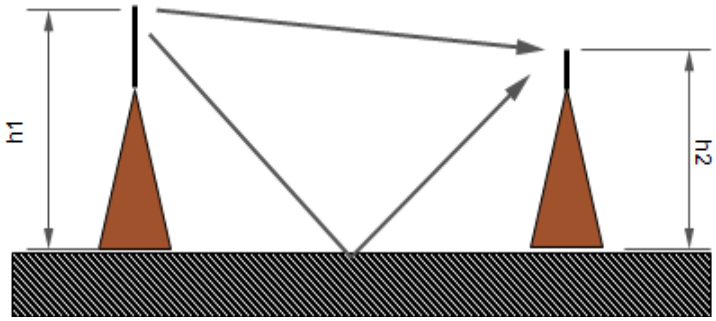


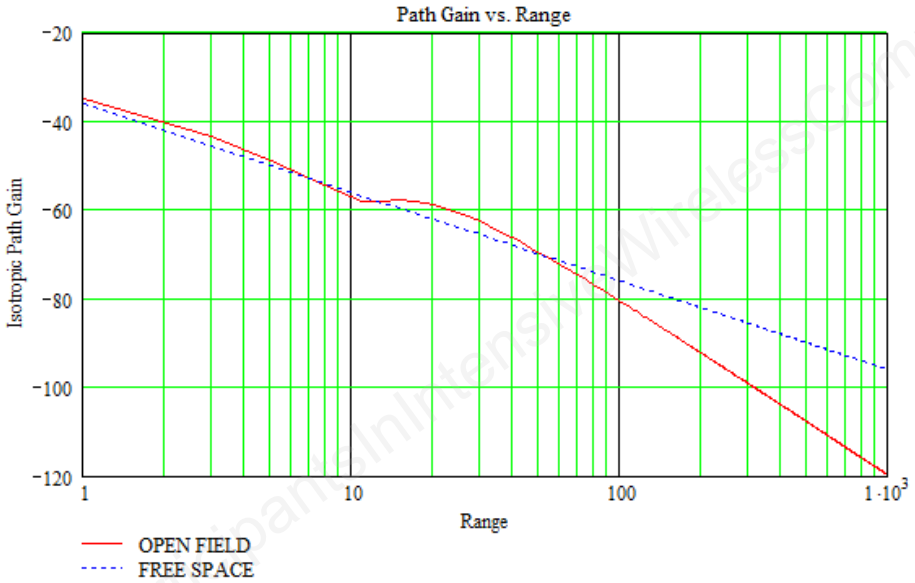
- **Diffraction**: path obstructed by surface having sharp irregularity causing "bending" of waves.



Path Loss -- Reflection

Reflection Environment – open field



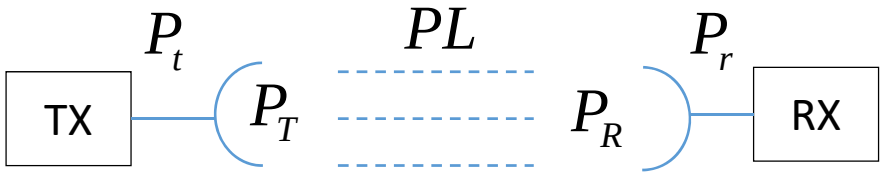


$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$$ free space

$$PL = \frac{P_T}{P_R} = \frac{P_t G_t}{P_r / G_r} \qquad PL = \left(\frac{4\pi d_0}{\lambda}\right)^2 \left(\frac{d}{d_0}\right)^n$$ open field: n=4

$$PL_{dB} = PL(d_0) + 10n \cdot \log\left(\frac{d}{d_0}\right) + X_\sigma \,|_{dB}$$

$$PG = \frac{1}{PL} = \frac{P_R}{P_T} \qquad PG_{dB} = -PL_{dB}$$



Path Loss -- Diffraction

- The diffraction loss can be computed by evaluating the Fresnel-Kirchoff diffraction parameter and the complex Fresnel integral

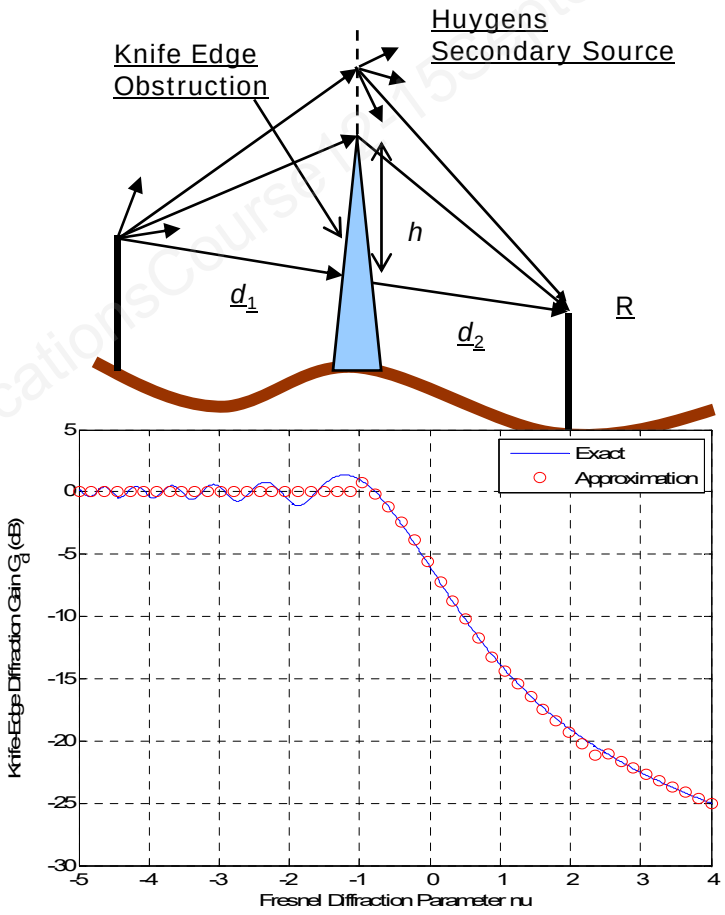
$$F(v) = \frac{E_d}{E_0} = \frac{1+j}{2}\int_v^{\infty} \exp\left(-j\pi t^2/2\right)dt$$

$$v = h\sqrt{\frac{2(d_1+d_2)}{\lambda d_1 d_2}}$$

1st Fresnel Zone

$$r = \sqrt{\frac{\lambda d_1 d_2}{d_1+d_2}}$$

- Multiple Knife-Edge Diffraction
  - Replace multiple obstacles by a single equivalent obstacle and apply signal knife edge diffraction model

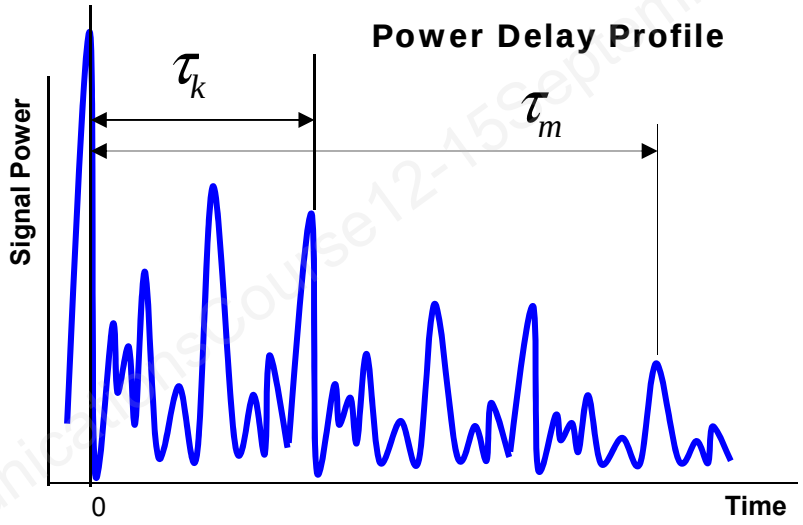


Numerical solution vs. Approximation

Multipath Effects

Impulse Response

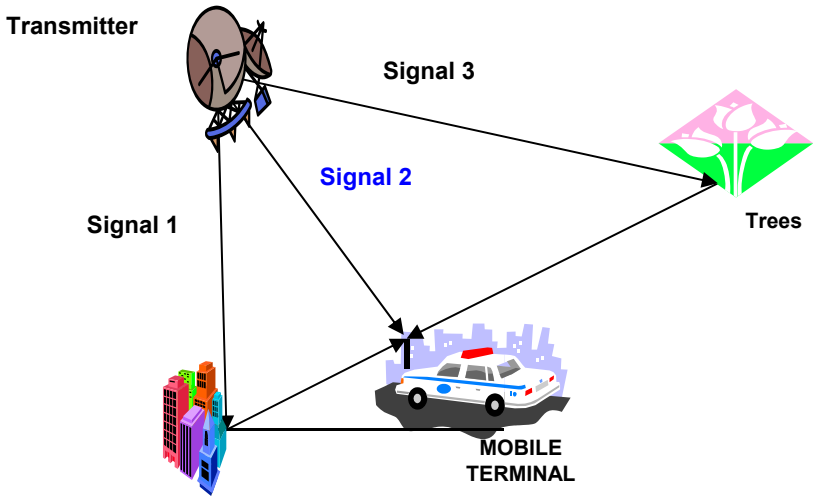
Short symbols relative to delay subject to intersymbol interference .



Single Frequency Response

$$S(f)=s_1e^{-2\pi f\tau_1}+s_2e^{-2\pi f\tau_2}+s_3e^{-2\pi f\tau_3}$$

Moving terminals or reflectors cause Doppler shift and motion fading.

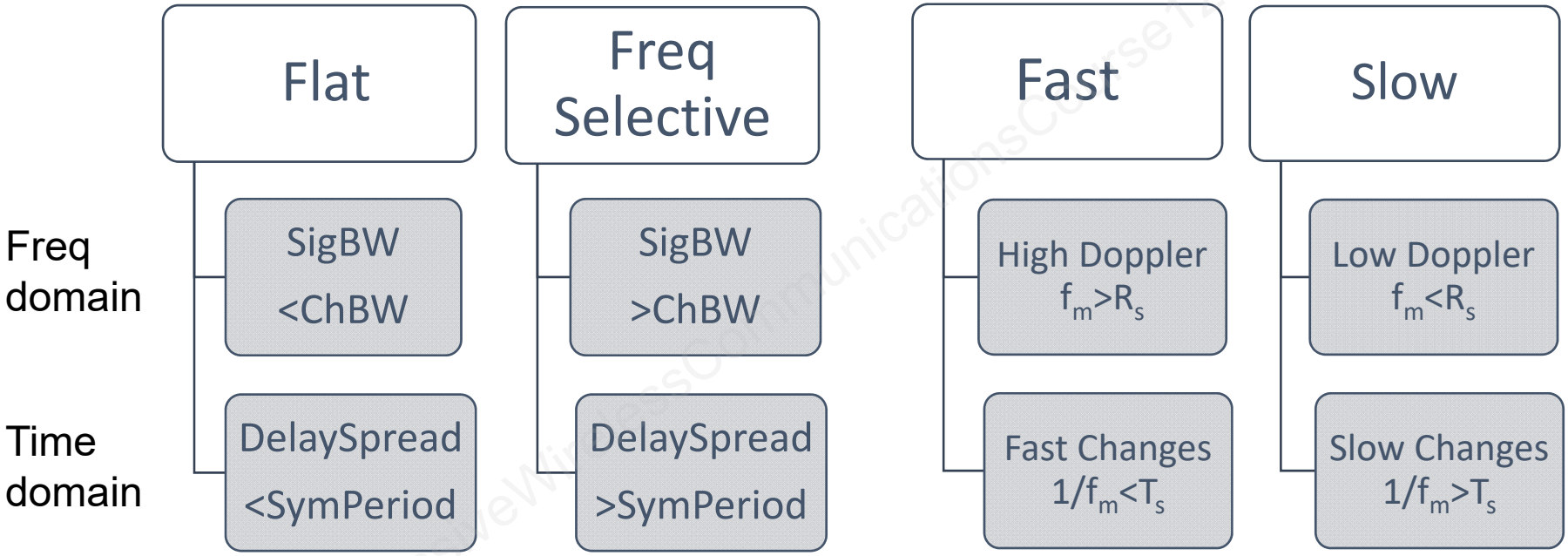


Small Scale Fading

Multipath

Motion

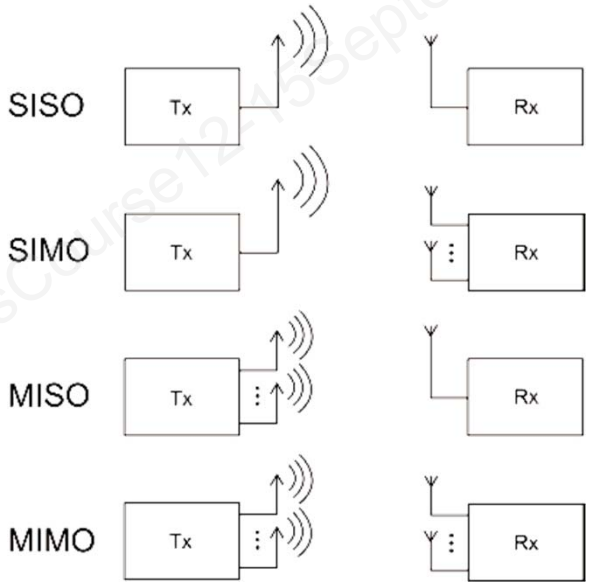
$$f_m = \frac{v}{\lambda} = \frac{v}{c} f$$



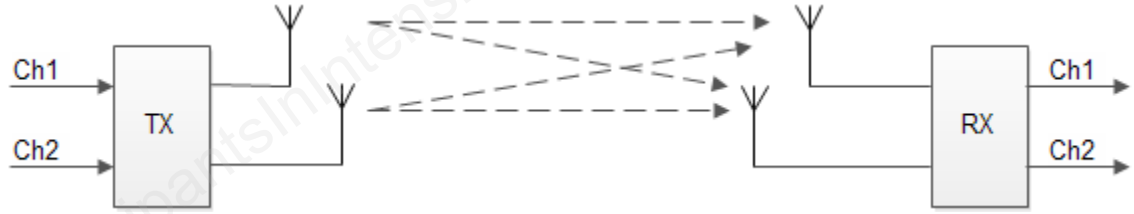
Antenna MIMO Technology

- Multiple input/Multiple output (MIMO) can improve range, data rate, reliability, and facilitate multiple channels
- Modes:
  - spatial multiplex
  - spatial diversity
  - beam forming
- Requires low correlation signal paths for maximum performance

$$N_{CH} = \min(N_{TX}, N_{RX})$$

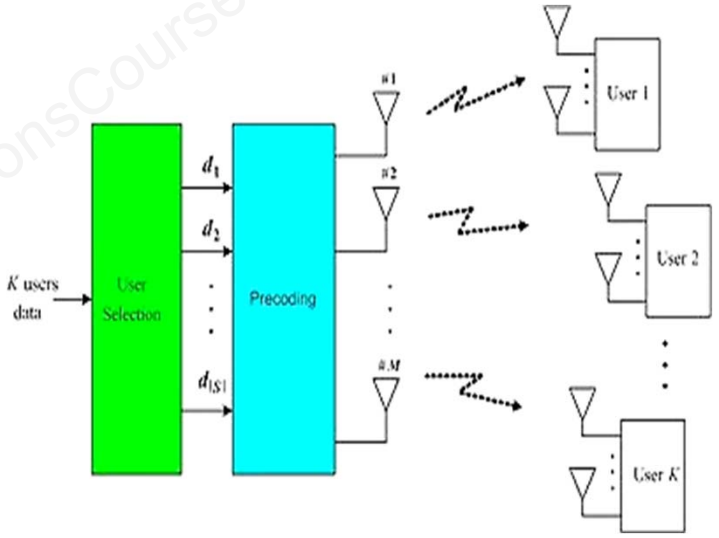


Differences between SISO, SIMO, MISO and MIMO
Source: wikipedia.org



Multi-User MIMO(MU-MIMO)

- Can handle multiple users as spatially distributed transmission resources
  - MIMO broadcast channels (MIMO BC) for downlink. The transmitter has to know the channel state information at the transmitter (CSIT). Uses interference aware precoding and SDMA (space division multiple access)-based downlink user scheduling
  - MIMO multiple access channels (MIMO MAC) for uplink case in the multiple sender to single receiver wireless network. The receiver has to know the channel state information at the receiver (CSIR)



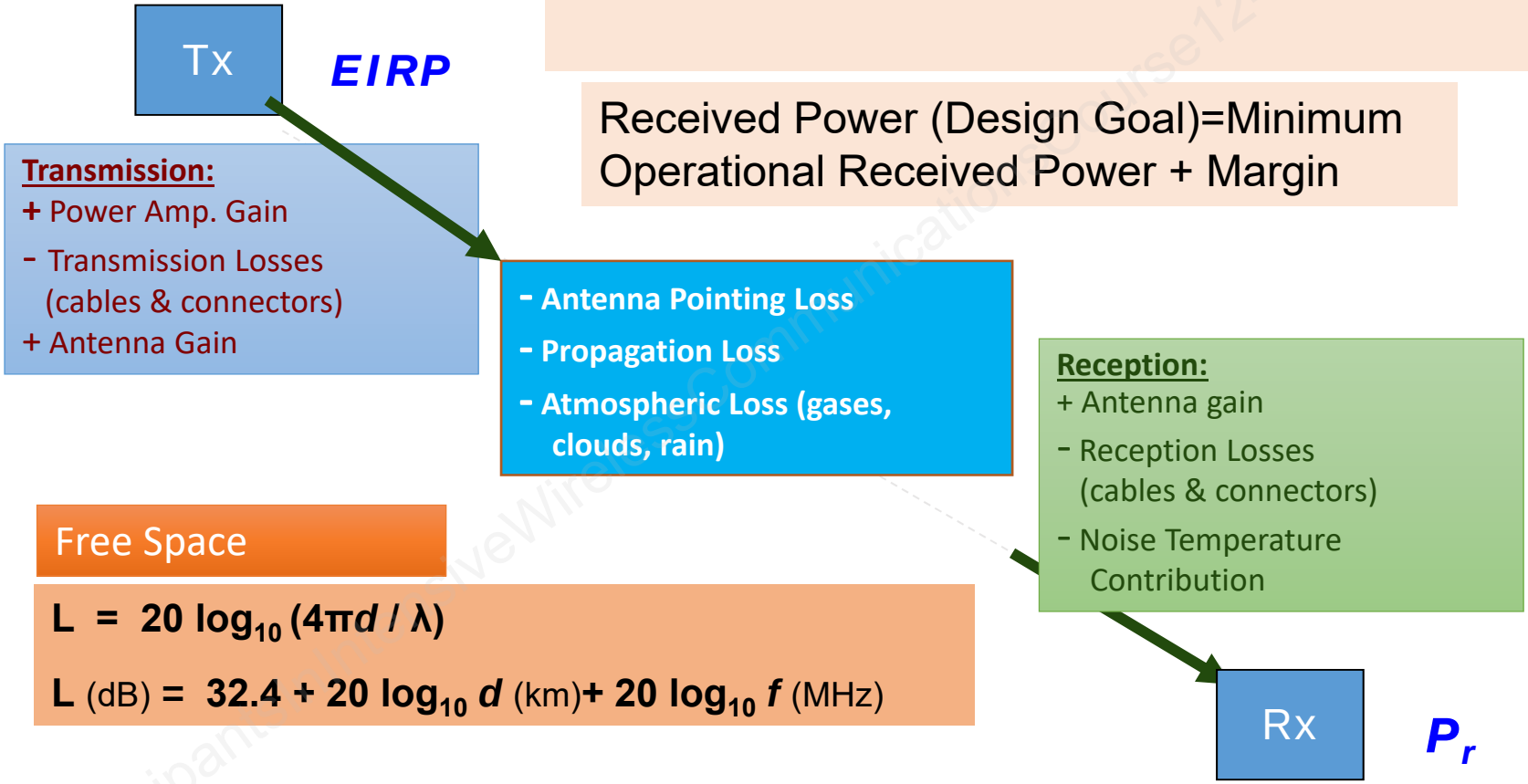
Multiuser MIMO System: MIMO BC case.

Source: wikipedia.org

The Link Budget

Received Power=Transmitted Power+Gains-Losses

Received Power (Design Goal)=Minimum Operational Received Power + Margin



Free Space

$L = 20 \log_{10}(4\pi d / \lambda)$

$L\ (\text{dB}) = 32.4 + 20 \log_{10} d\ (\text{km}) + 20 \log_{10} f\ (\text{MHz})$

The Link Budget Equation: Losses in the Link

- L_s = Propagation loss
- L_a = Due to atmospheric attenuation (e.g. rain)
- L_{ta} = Associated with transmitting antenna
- L_{ra} = Associated with receiving antenna
- L_{pol} = Due to polarization mismatch
- $L_{pointing}$ = Due to antenna pointing mismatch
- L_r = Losses at receiver (after receiving antenna)
- L_{other} = Any other known loss

$$P_r = \frac{P_t G_t G_r}{L_s L_a L_{ta} L_{ra} L_{pol} L_{pointing} L_r L_{other}} = \frac{P_t G_t G_r}{L_s L_0}$$

Link Margin

$$P_r = \frac{EIRP \cdot G_r}{L_s L_0} \qquad EIRP = P_t G_t$$

1 $$\frac{P_r}{N_0} = \frac{EIRP \cdot G_r / N_0}{L_s L_0}$$

2 $$\frac{P_r}{N_0} = \frac{EIRP \cdot G_r / T_S}{k L_s L_0} \qquad N_0 = kT_S$$

k=Boltzmann's constant
T_S = system temperature

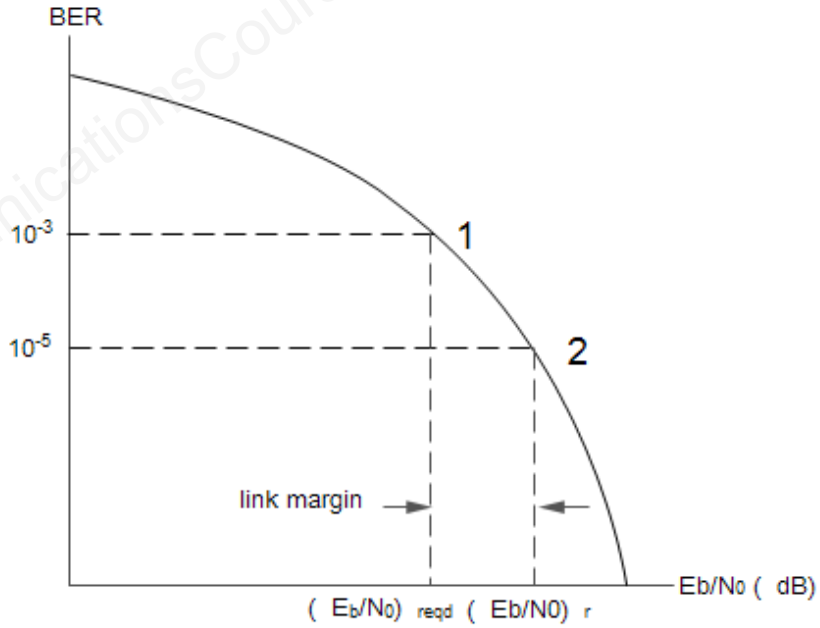
3 $$\left(\frac{E_b}{N_0}\right)_r = \frac{EIRP \cdot G_r / T_S}{R \cdot k L_s L_0} \qquad \frac{E_b}{N_0} = \frac{P_r}{N_0} \cdot \frac{1}{R} \qquad \frac{\text{Energy/bit}}{\text{Noise density}}$$

R=data rate

4 $$\left(\frac{E_b}{N_0}\right)_r = M \left(\frac{E_b}{N_0}\right)_{reqd}$$

M=link margin

5 $$M = \frac{EIRP \cdot G_r / T_S}{\left(\frac{E_b}{N_0}\right)_{reqd} R \cdot k L_s L_0}$$



Link Budget Example

Link Margin: $$M\ (dB) = EIRP + \left(\frac{G_r}{T_S}\right)_{dB} - \left(\frac{E_b}{N_0}\right)_{reqd} - R - k - L_s - L_0$$

EIRP=69.6 dBW

$(G_r/T_S)_{dB}$ =-1 dB/K

$$EIRP = (P_t)_{dB} + (G_t)_{dB}$$

$$T_S = T_A + (F-1)290^0$$

T_S=system temperature,
T_A=antenna temperature
F = noise factor

E_b/N_0=10 dB — Depends on modulation, coding, BER

R=63 dB bit/s — R_b=2 Mb/s

k=-228.6 dBW/K-Hz — Boltzman's constant

L_s=202.7 dB — Free space at 8GHz, 40,586 km

L_0=13.5 dB — Atmosphere, rain, pointing errors

Margin=8 dB

Outdoor Propagation Models

- A large number of models are available to predict path loss over irregular terrain.
  - In urban areas, the average height of the buildings plays a critical role in path-loss determination, while in rural areas shadowing, scattering and absorption by trees and other vegetation are dominant especially at higher frequencies.
- The prediction models differ in their applicability over different terrain and environmental conditions. However, no one model stands out as ideally suited to all environments
- Most models aim to predict the median path loss. Knowledge of the signal statistics then allows the variability of the signal to be estimated.
- Thus, the model must be chosen carefully.
- Examples are shown next

RF Environment

Category	Characteristics
Open Area	Very few structures, such as tall buildings and trees, are in the propagation path. The area is mostly farms, open fields, rice fields, etc.
Suburban Area	Residential, with small one or two-story houses, with some obstacles near the mobile radio, but not very congested
Urban	Heavily built-up areas with tall buildings and high-rise apartments
Indoor	Short reflection paths, non line of sight

The Egli Model

Egli's model for median path loss (path loss less than the predicted value at half the locations and half the time).

$$PL = 20\log\left(\frac{d^2 f_{MHz}}{40 h_t h_r}\right)$$

h_t, h_r = antenna heights
d = distance
heights and distance in same units

The Okumura Model

Frequency range: 150 < f <1920 MHz (but extrapolated to 3000 MHz).
Distance: 1 < d < 100 km.
Base station antenna height: 30 < 1000 m.

$$L_{50}(dB) = L_F + A_{mu}(f,d) - G(h_{te}) - G(h_{re}) - G_{AREA}$$

$$L_F = 32.4 + 20\log d(km) + 20\log f(MHz)$$

$$G(h_{te}) = 20\log_{10}\left(\frac{h_{te}}{200}\right) \quad 30m < h_{te} < 100m$$

$$G(h_{re}) = \begin{cases} 10\log_{10}\left(\frac{h_{re}}{3}\right) & h_{re} \le 3m \\ 20\log_{10}\left(\frac{h_{re}}{3}\right) & 3m < h_{re} < 10m \end{cases}$$

A_{mu}(f,d) example values:

f MHz	d km	A_{mu} dB
1000	1	19
1000	10	28
1000	50	45
400	10	26

G_{AREA} example corrections (dB):

f MHz	Suburban	Open Area
1000	10	28
400	7	24

The Hata Model

Median path loss in urban areas:

$$L_{50,urban} = 69.55 + 26.16 \log f_c - 13.82 \log h_{te} - a(h_{re}) + (44.9 - 6.55 \log h_{te}) \log d$$

f_c=frequency in MHz, 150 MHz < f_c < 1500 MHz
h_{te} = base station antenna height (m), 30 m < h_{te} <200 m
h_{re} = mobile antenna height (m), 1m < h_{re} < 10 m
d= transmitter-receiver separation (km), 1 km < d < 100 km
$a(h_{re})$ = mobile antenna height correction, function of coverage area

$$a(h_{re}) = (1.1 \log_{10} f_c - 0.7) h_{re} - (1.56 \log_{10} f_c - 0.8)$$

small to medium sized city

$$a(h_{re}) = \begin{cases} 8.29(\log 1.54 h_{re})^2 - 1.1 & f_c \le 300\,MHz \\ 3.2(\log 11.75 h_{re})^2 - 4.97 & f_c > 300\,MHz \end{cases}$$

large city

$$L_{50}(dB) = \begin{cases} L_{50,urban} - 2[\log(f_c / 28)]^2 - 5.4 & \text{Surburban area} \\ L_{50,urban} - 4.78[\log f_c]^2 + 18.33 \log f_c - 40.94 & \text{Open rural area} \end{cases}$$

The COST-231 Model

- EURO-COST: European Cooperative for Scientific and Technical research
- COST-231 aim: extend Hata's model to 2 GHz

$$L_{50,Urban} = 46.3 + 33.9 \log f_c - 13.82 \log h_{te} - a(h_{re}) + (44.9 - 6.55 \log h_{te}) \log d + C_M$$

1. $a(h_{re})$ defined in Hata model
   f_c, h_{te}, h_{re}, d defined in Hata model, with limits shown below
2. C_M = 0 dB for medium sized city and suburban areas
   C_M = 3 dB for metropolitan centers
3. $$1,500 \ MHz \leq f_c \leq 2,000 \ MHz$$
   $$30 \ m \leq h_{te} \leq 200 \ m$$
   $$1 \ m \leq h_{re} \leq 10 \ m$$
   $$1 \ km \leq d \leq 20 \ km$$

Propagation Modeling Software

- Based on specific site geometry and parameters
- Calculates path loss and delay profiles.
- Employs ray tracing to simulate propagation.
- 3D representations of buildings may be integrated with software that carries out reflection, diffraction, and scattering models.
- Works with AutoCAD files for indoor or outdoor environments.
- Uses transmitter and receiver antenna radiation patterns.
- Accounts for polarization in simulations.

Practice Questions (2)

- 1. The maximum number of spatial multiplex channels for MIMO with 2 TX antennas and 3 RX antennas is

  a) 3; b)2: c)5; d) 6

- 2. A GPS satellite transmits 25 watts on 1.575 GHz to its helical antenna which has a gain of 13 dBi.

  a) What is the EIRP?

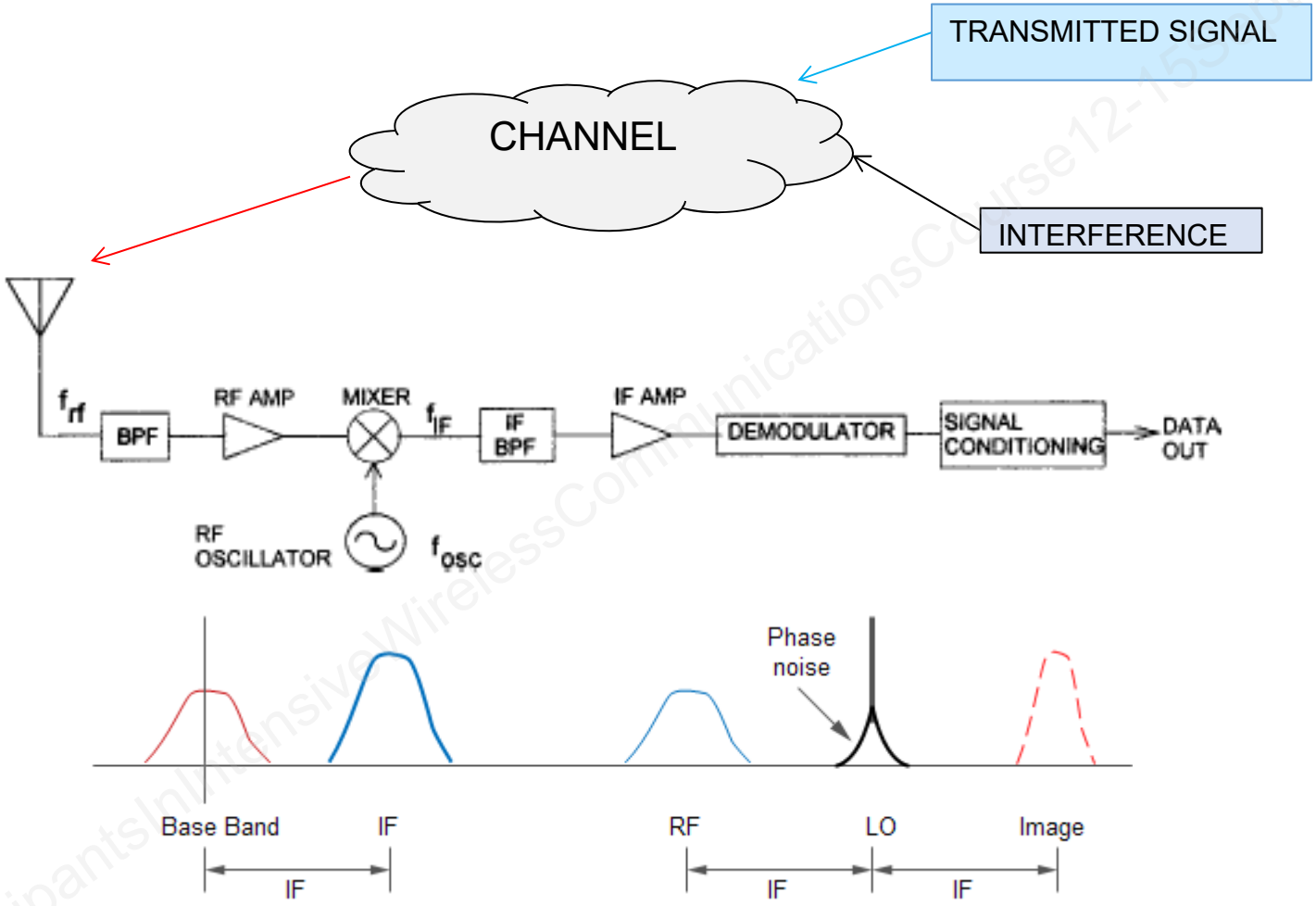
  b) How much isotropic power is received at a receiver on Earth 25,000 km away?

- 3. Compare Okumura and Egli path loss estimates at a range of 10 km in an open area on 400 MHz. The BS antenna is 50 meters high and the mobile height is 3 meters. Would results match better in a suburban area?

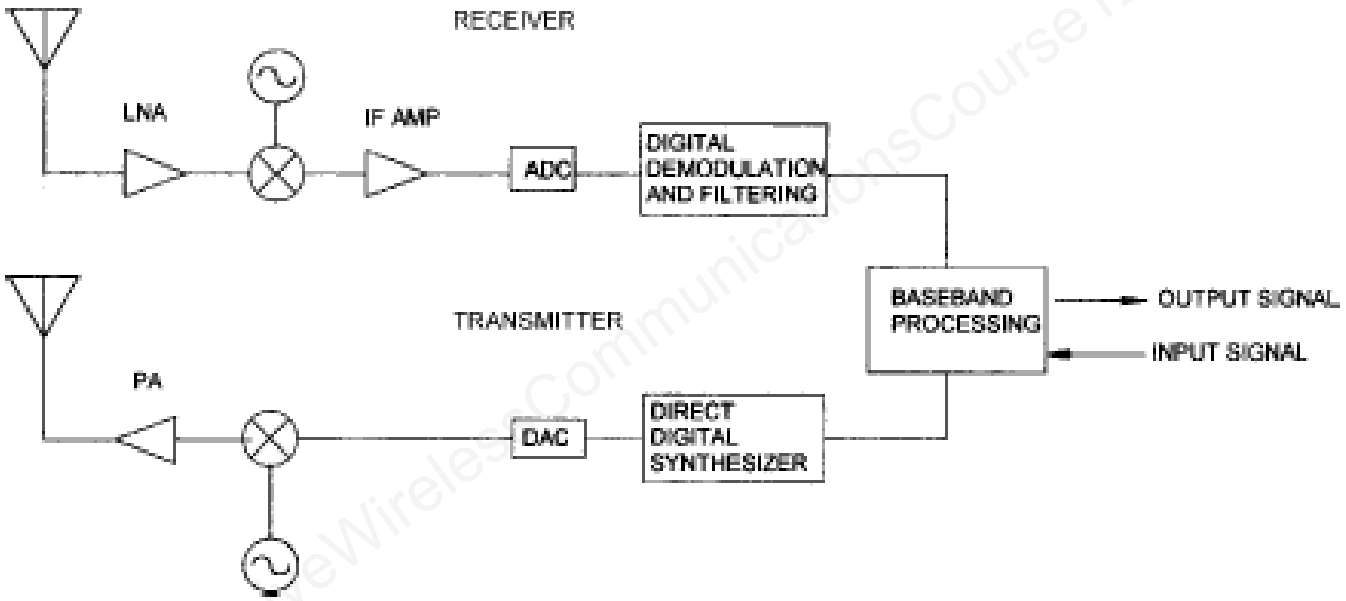
RF Engineering

- The Superheterodyne Receiver
- Receiver Phase Noise
- Filtering and Selectivity
- Direct Conversion
- Receiver Sensitivity
- Receiver Dynamic Range

Superheterodyne Receiver

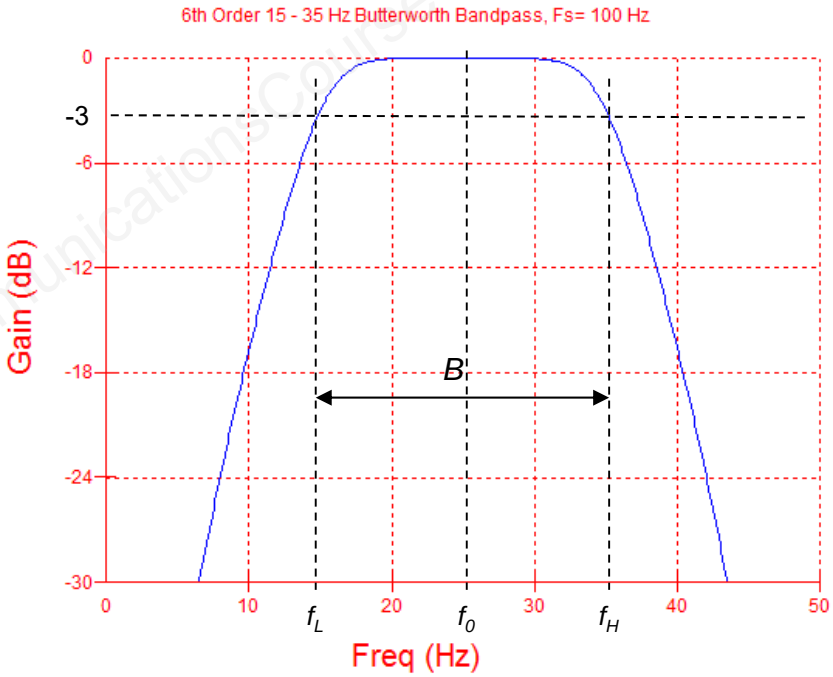


Digital Transceiver



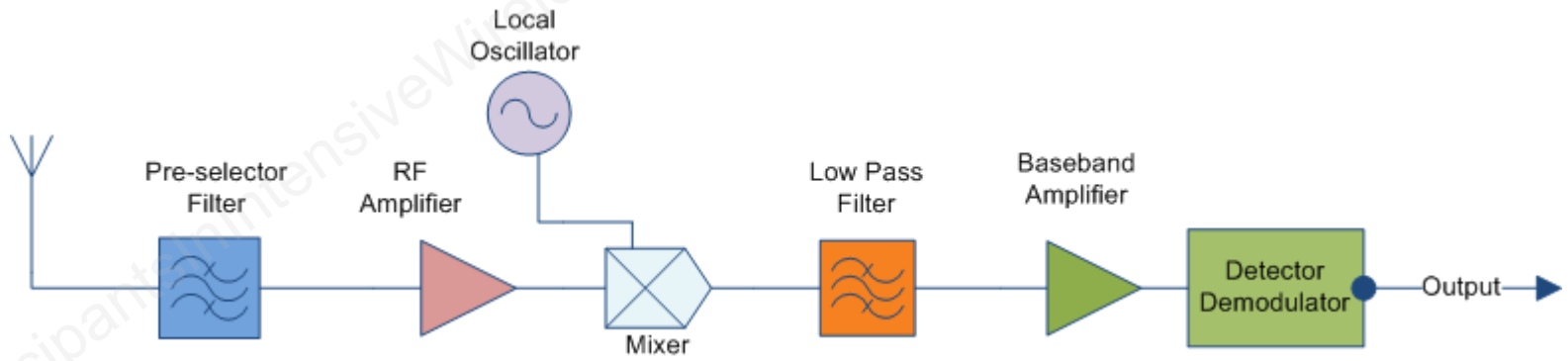
Filtering & Selectivity

- Filters play a key role in rejecting adjacent-channel signals, reducing the effect of the receiver's spurious responses such as the image, and reducing the effect of non-linear mixing products
- Complex filters have more attenuation in the stop band and can transition from pass band to stop band faster at the expense of waveform distortion in the time domain

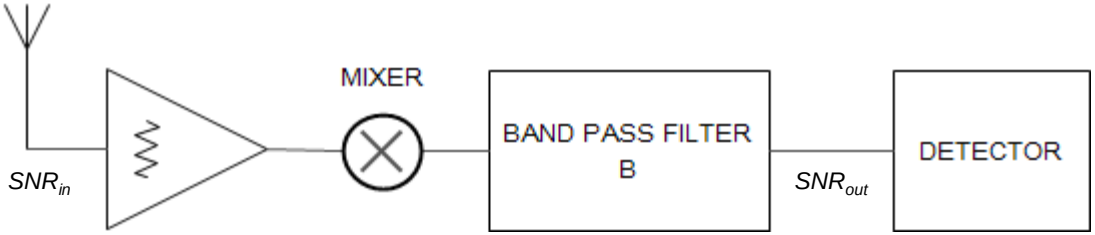


Direct Conversion Receiver

- Instead of producing IF, direction conversion Rx down-converts the RF input signal directly to baseband by tuning the LO to the frequency of the incoming signal.
- The mixer output is the sum and the difference of the signal and the LO frequencies. Because the signal and LO frequencies are equal, the difference is zero. The mixer output is then low pass filtered.
- The resulting output is the original information contained in modulation sidebands about the carrier frequency. This is called a direct-conversion (DC), homodyne, or zero-IF receiver.



Sensitivity



1. $$(P_{\min})_{dBm} = (N_0)_{dBm/Hz} + (NF)_{dB} + (10\log B)_{dBHz} + (SNR_{out})_{dB}$$

2. $$(NF)_{dB} = (SNR_{in})_{dB} - (SNR_{out})_{dB}$$

$$F = (SNR_{in})/(SNR_{out}) \qquad F = 10^{(NF)_{dB}/10}$$

$$F = (N_a + G_a N_i)/G_a N_i$$

3. $$F_{total} = F1 + (F2-1)/G1 + (F3-1)/(G1 \cdot G2)\ldots$$

4. Noise Temperature $N_0 = kT_0$ T_0=290K $k = 1.38 \cdot 10^{-23} J/K$

$T_e = T_0(F-1)$ T_e=effective noise temperature N_0=-174 dBm/Hz

$$(T_e)_{total} = T_1 + T_2/G_1 + T_3/G_1G_2\ldots$$

5. $T_S = T_A + T_e$ T_S=system temperature, T_A=antenna temperature

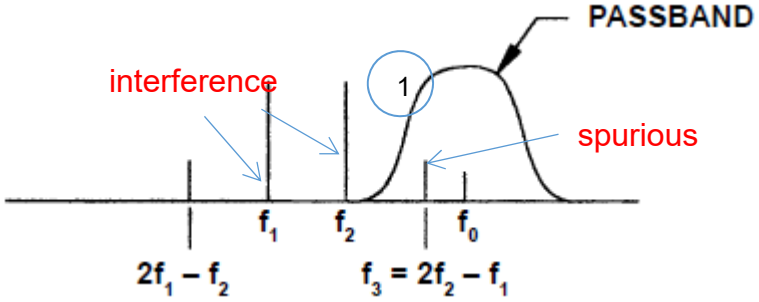
6. $F_e = 1 + \frac{T_0}{T_A}(F-1)$ F_e=effective noise factor

SNR=signal to noise ratio
NF=noise figure
F=noise factor
N_0=input noise power density
N_a=amplifier internal noise power
N_i=amplifier input noise power
G_a=stage gain
B=noise bandwidth
T_0=reference temperature
k=Boltzmann's constant
E_0 = energy/bit
R = bit rate

Digital Receiver:

$$\frac{S}{N} = \frac{E_0}{N_0} \cdot \frac{R}{B}$$

Intermodulation Distortion and Dynamic Range



3rd Order Intermodulation Distortion

6 $$P_{si} = 3 \cdot P_{ii} - 2 \cdot IIP3$$

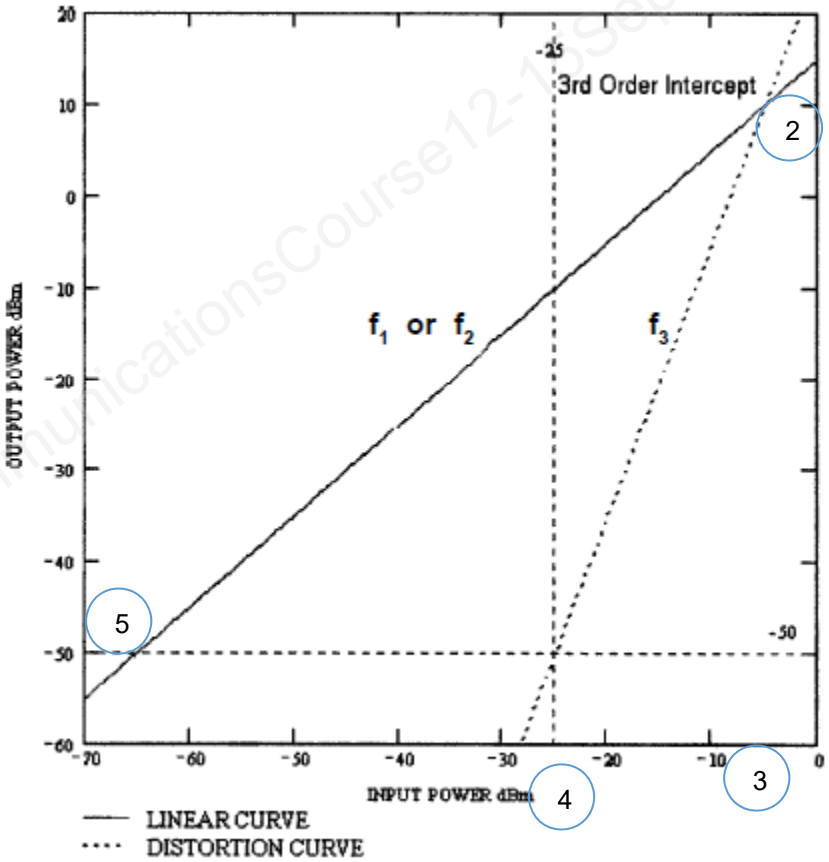
P_{si}=spurious input power
P_{ii}=interference input power
IIP3=input 3rd order intercept power

7 SFDR=Spurious Free Dynamic Range

$$SFDR = \tfrac{2}{3}(IIP3 - MDS)$$

8 $$MDS = (N_0)_{dBm/Hz} + (NF)dB + (10\log B)_{dBHz}$$

MDS=minimum discernible signal=noise floor



OIP3 Output 3rd order intercept=10dBm
Gain=15dB

Practice Questions (3)

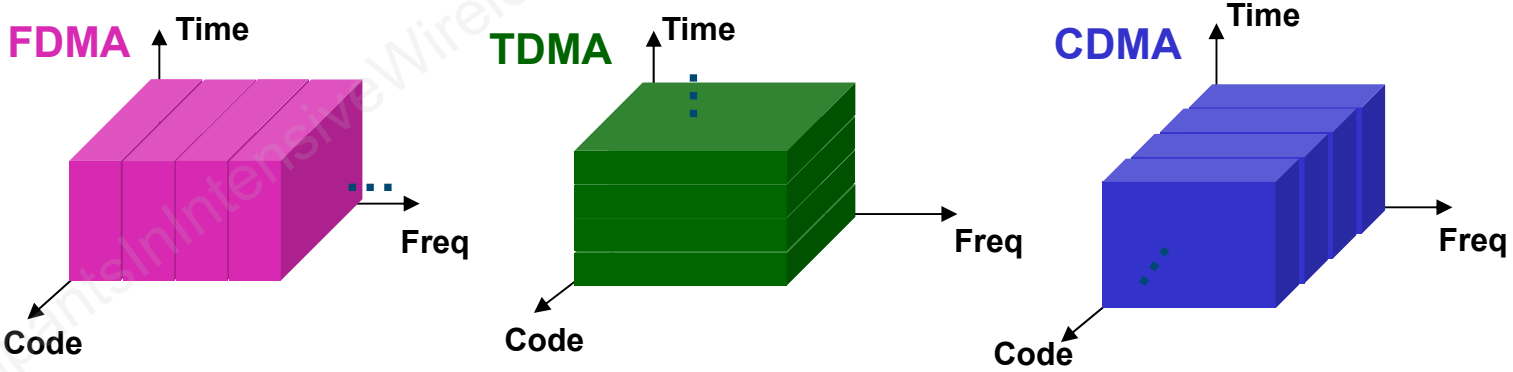
1. The noise figure of a receiver is 8 dB. How much can the NF be improved by using a 13 dB gain LNA (low noise amplifier) whose noise figure is 3 dB?
2. A superheterodyne receiver receives on 150 MHz. The IF frequency is 10.7 MHz. Assuming a high side local oscillator, what is the image frequency?
   a) 128.6 MHz
   b) 171.4 MHz
   c) 160.7 MHz
   d) 139.3 MHz
3. Find the dynamic range SFDR of a receiver with input 3rd order IM of 0 dBm, input noise density -174 dBm/Hz, NF 6 dB, and BW 100 kHz.

Wireless Access Technologies

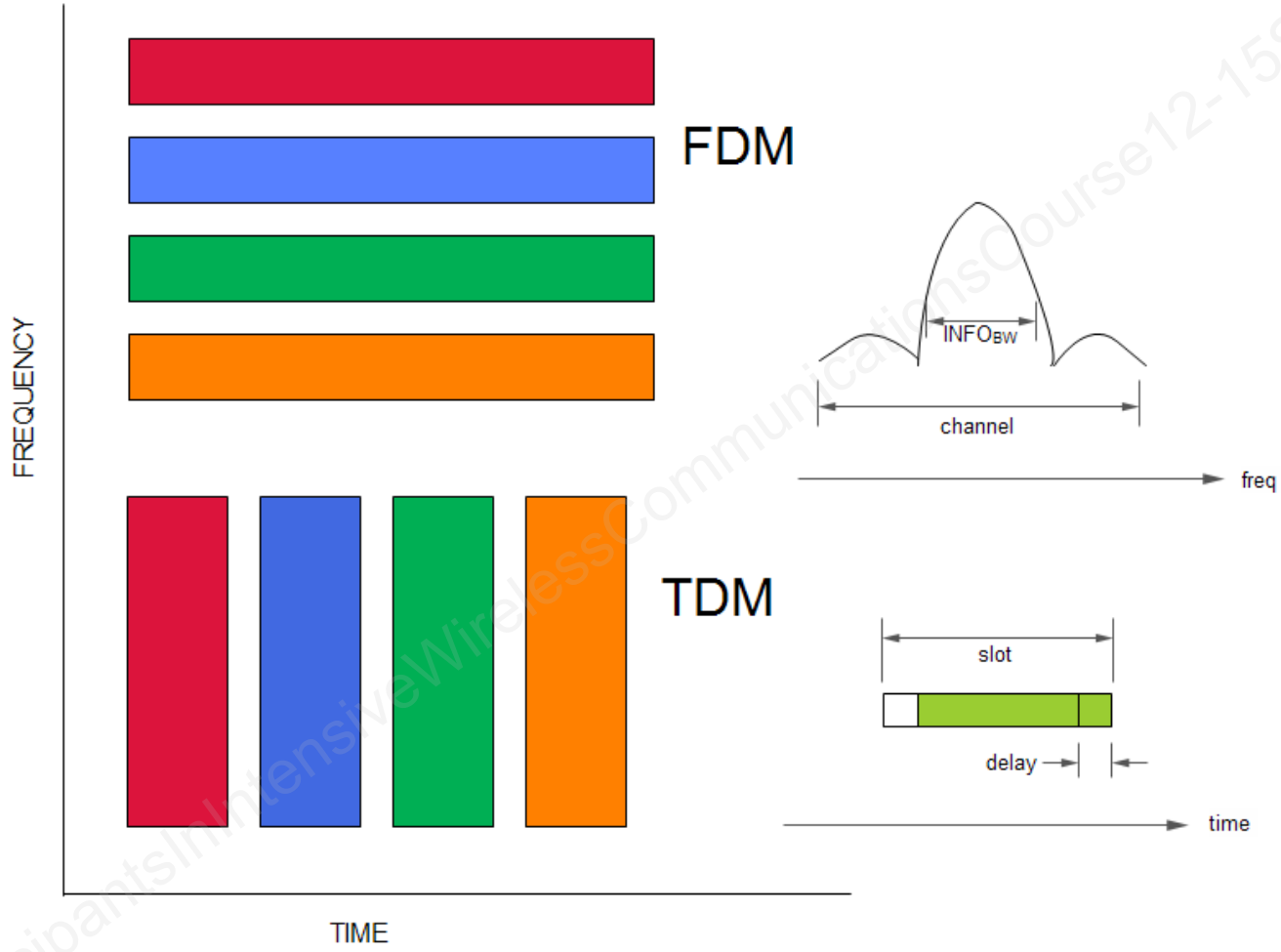
- Access Techniques
- Mobile Cellular Standards & Evolution
- IEEE Wireless Network Standards
- Other Wireless Systems
- Satellite Communications

Multiple Access Schemes

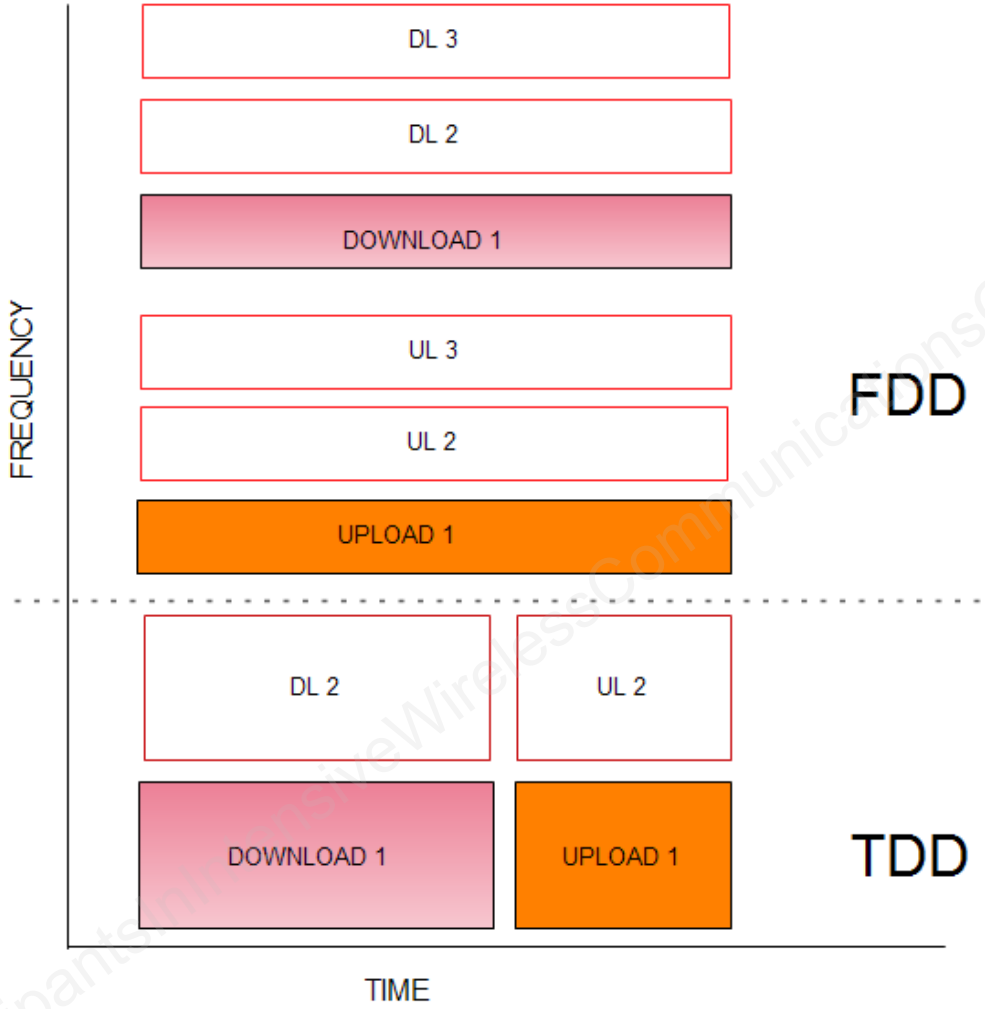
- Allow communication between large number of users in a geographical area within a given frequency range.
  - Maximize capacity at acceptable performance
- FDMA: Multiple narrow band channels (analog or digital) in given frequency range with non overlapping spectrums
- TDMA: Multiple channels (digital) with common carrier frequency transmit in bursts on non overlapping time slots
- CDMA: Spread spectrum scheme where all users occupy concurrently same frequency band and use (quasi) orthogonal spreading codes for interference rejection and correlation detection.



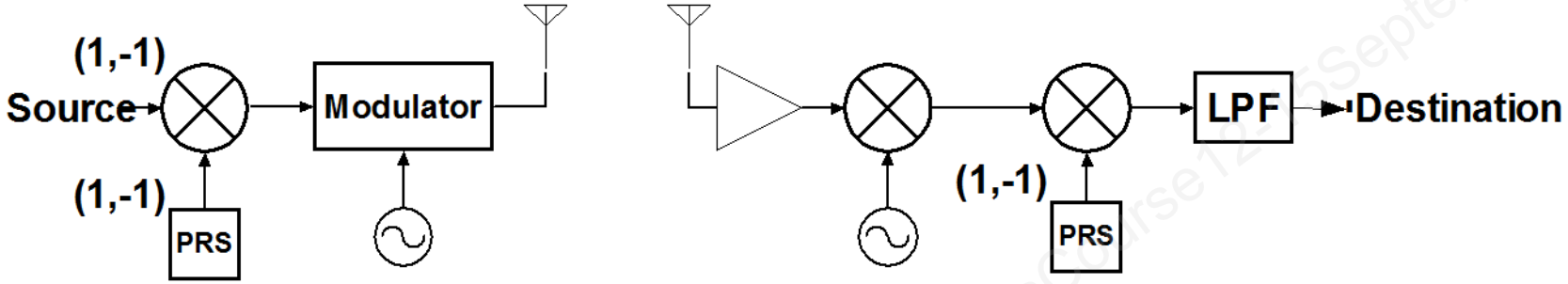
Multiple Access

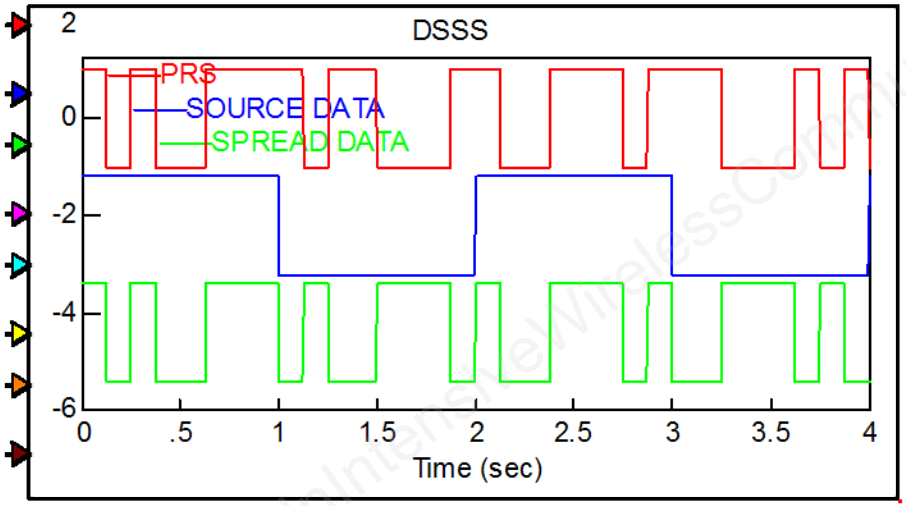


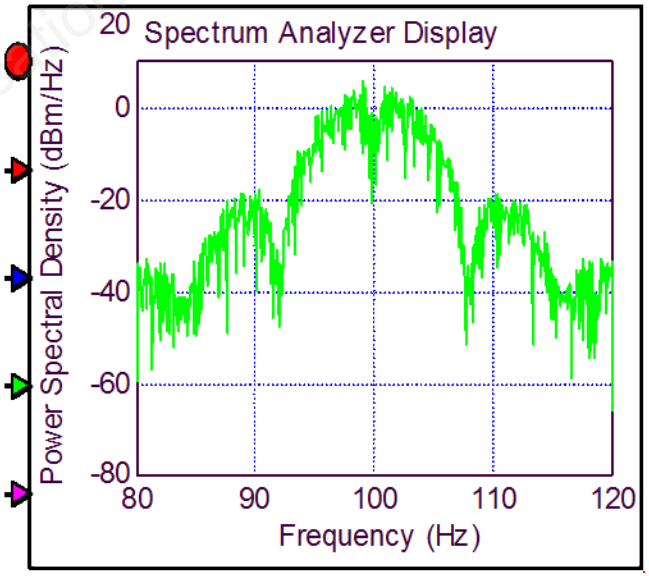
Duplex



CDMA: Direct Sequence Spread Spectrum

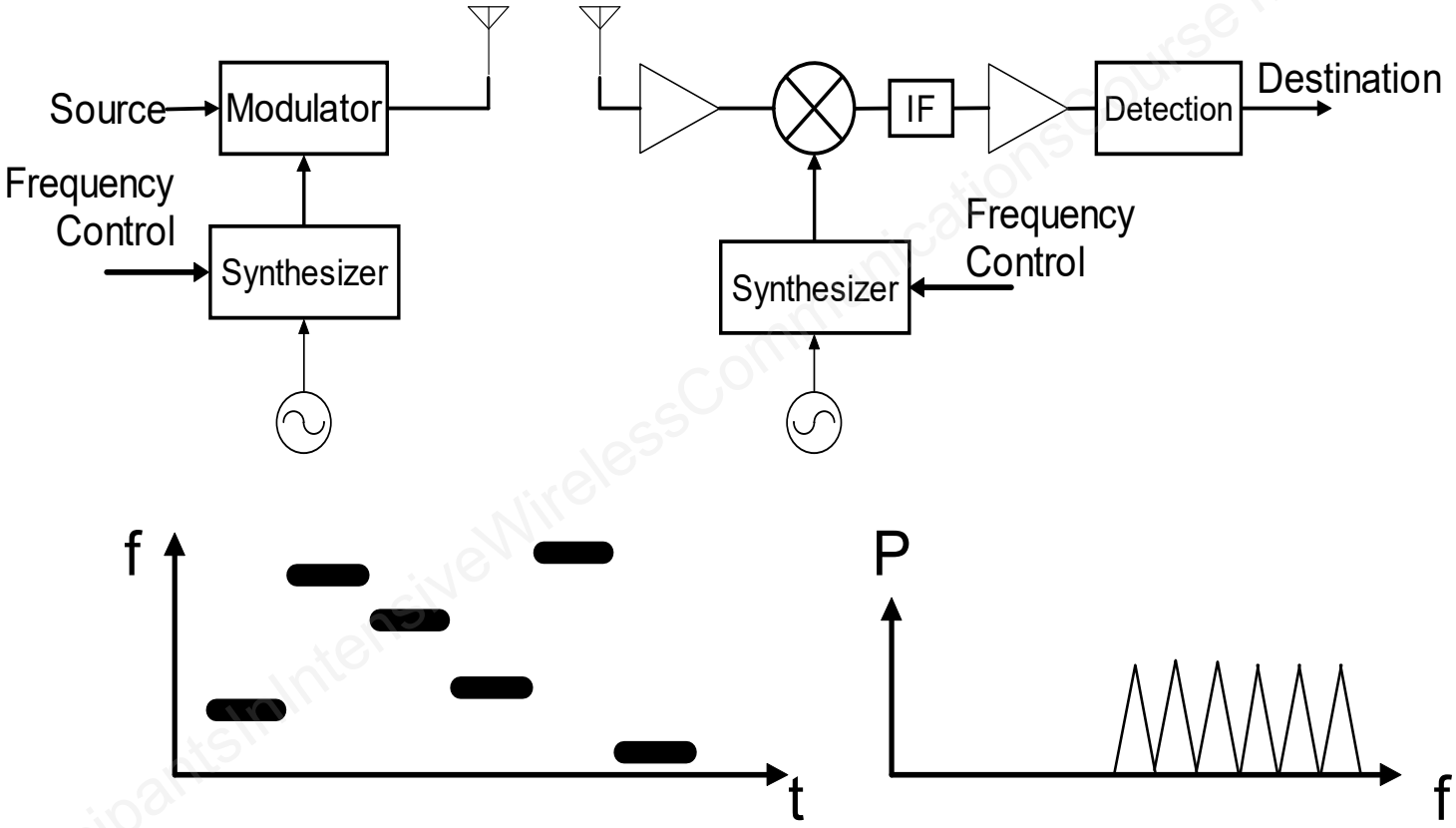






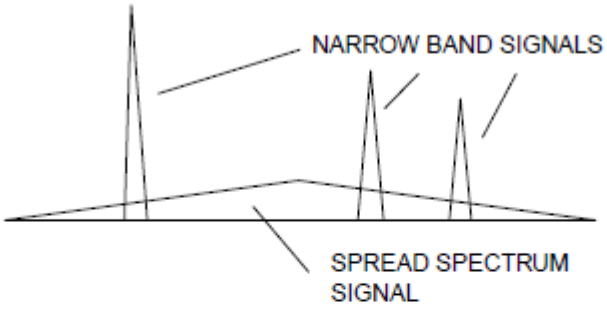
PRS – Pseudo Random Sequence

CDMA-Frequency Hopping Spread Spectrum

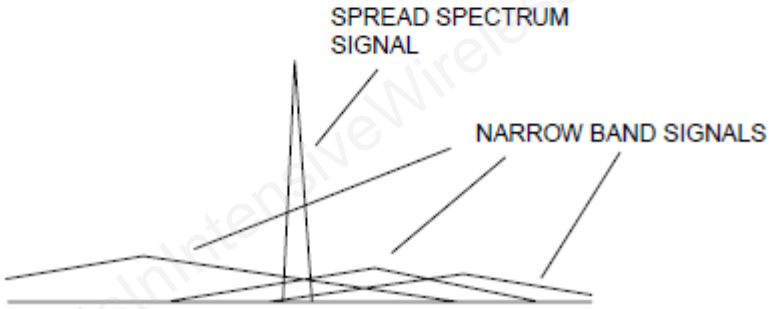


Processing Gain

a) Signals at receiver input



b) Signals after despreading



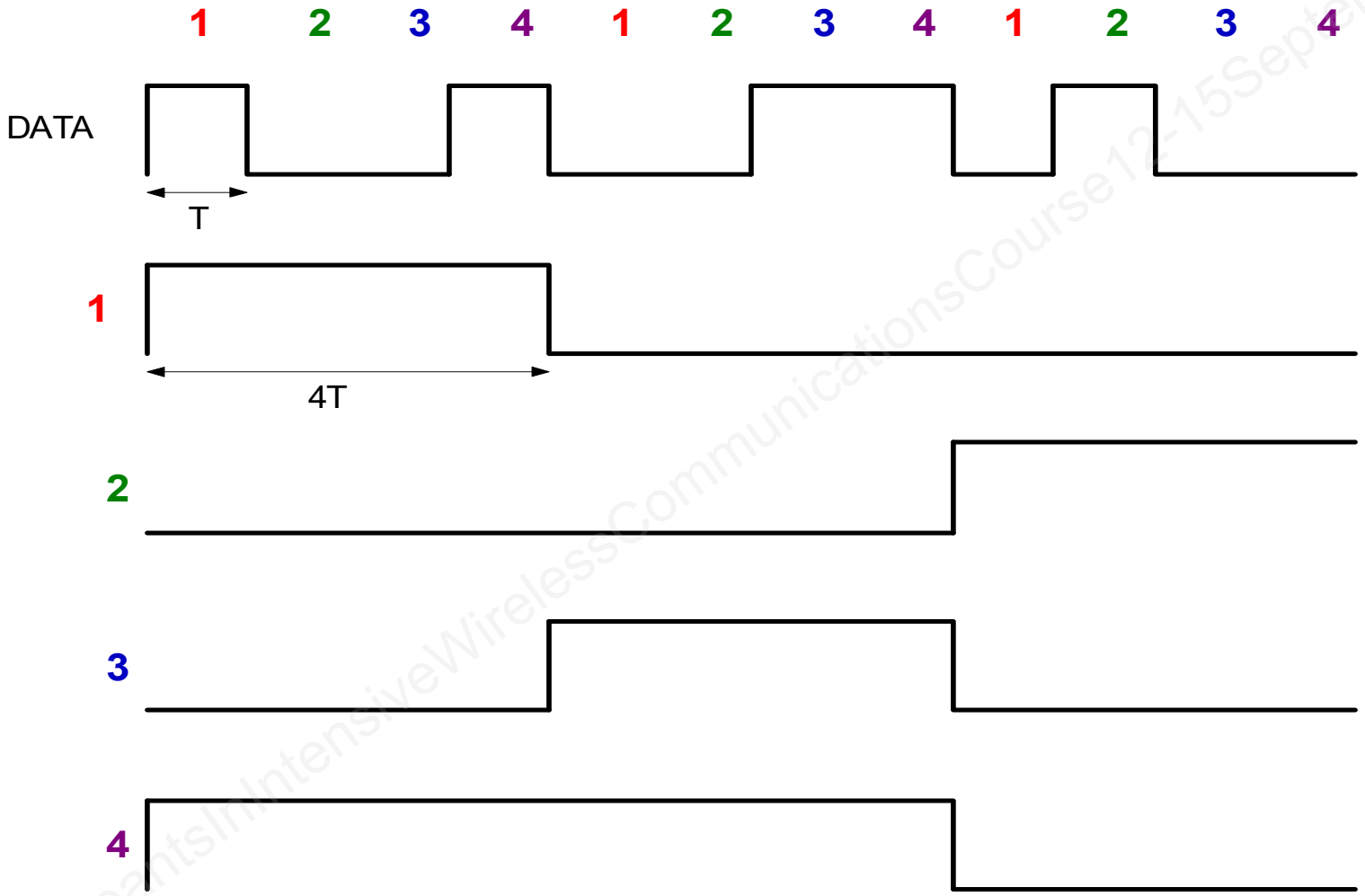
$$G_P = \frac{ChipRate}{SymbolRate}$$

Note:
ChipRate ≈ spread signal BW,
SymbolRate ≈ data BW

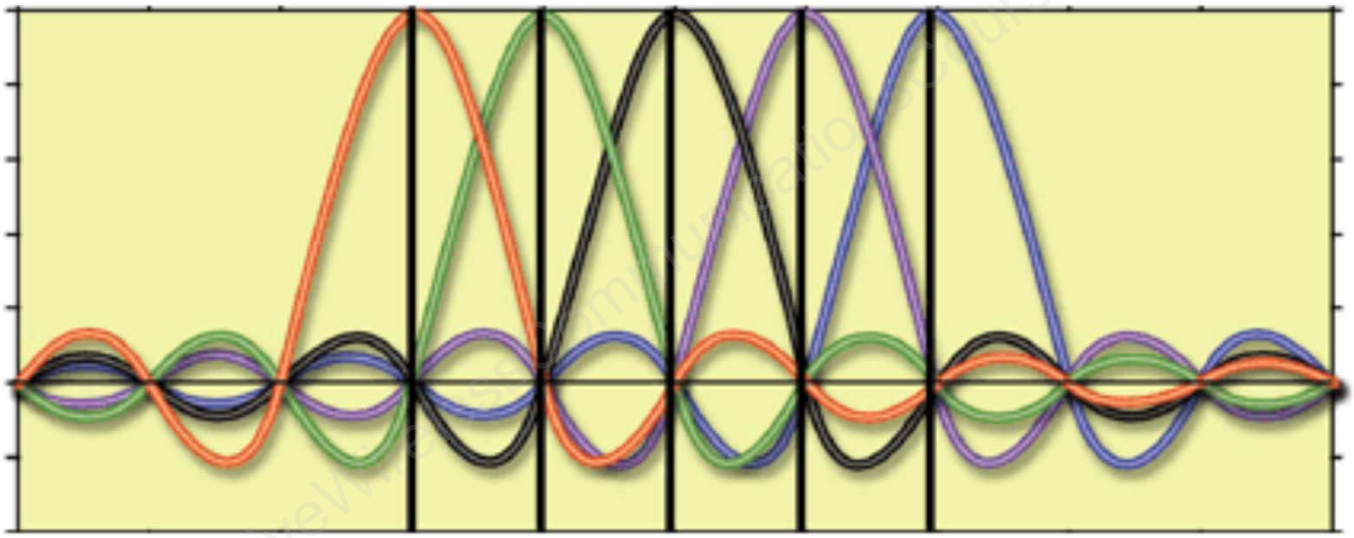
OFDM

- ADSL
- Digital Audio Broadcast DAB
- Digital Video Broadcasting-Terrestrial DVB-T
- IEEE 802.11a/g (Wi-Fi), 802.16 (WiMAX)
- 4G Cellular (LTE)
- Power Line Networking (Home Plug)

OFDM Subchannels



OFDM Subcarriers

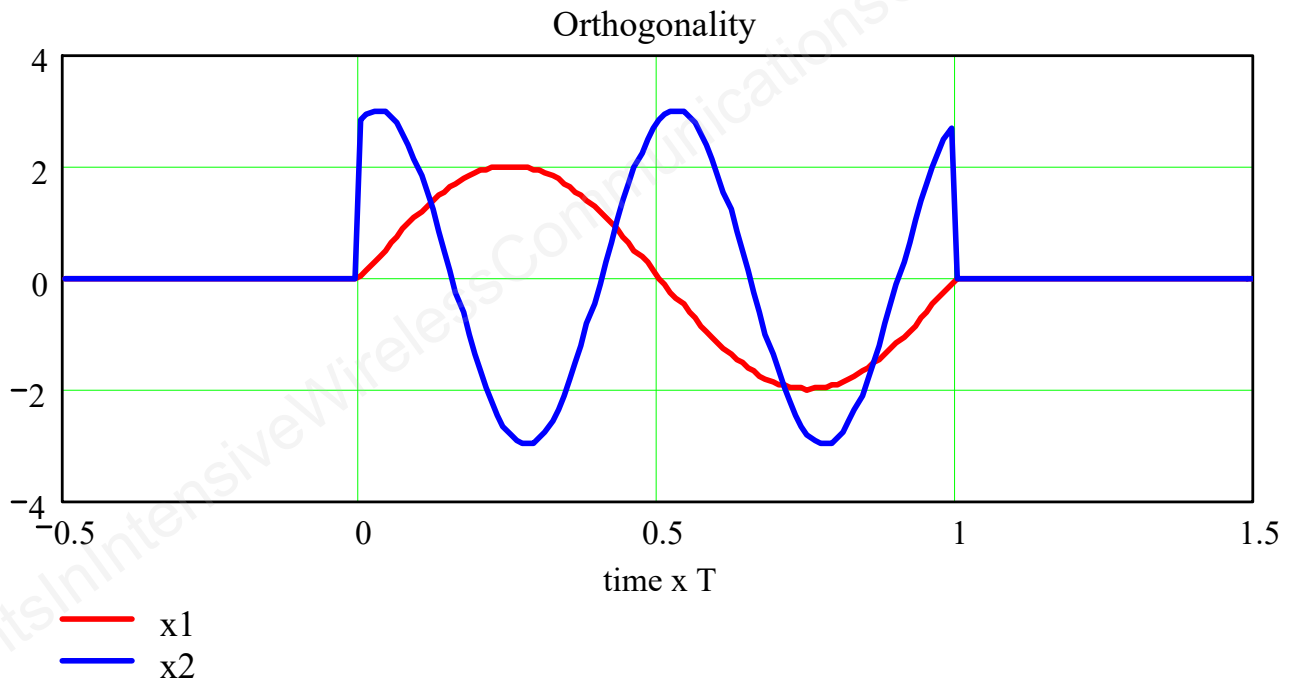


f_1 f_2 f_3 f_4 f_5

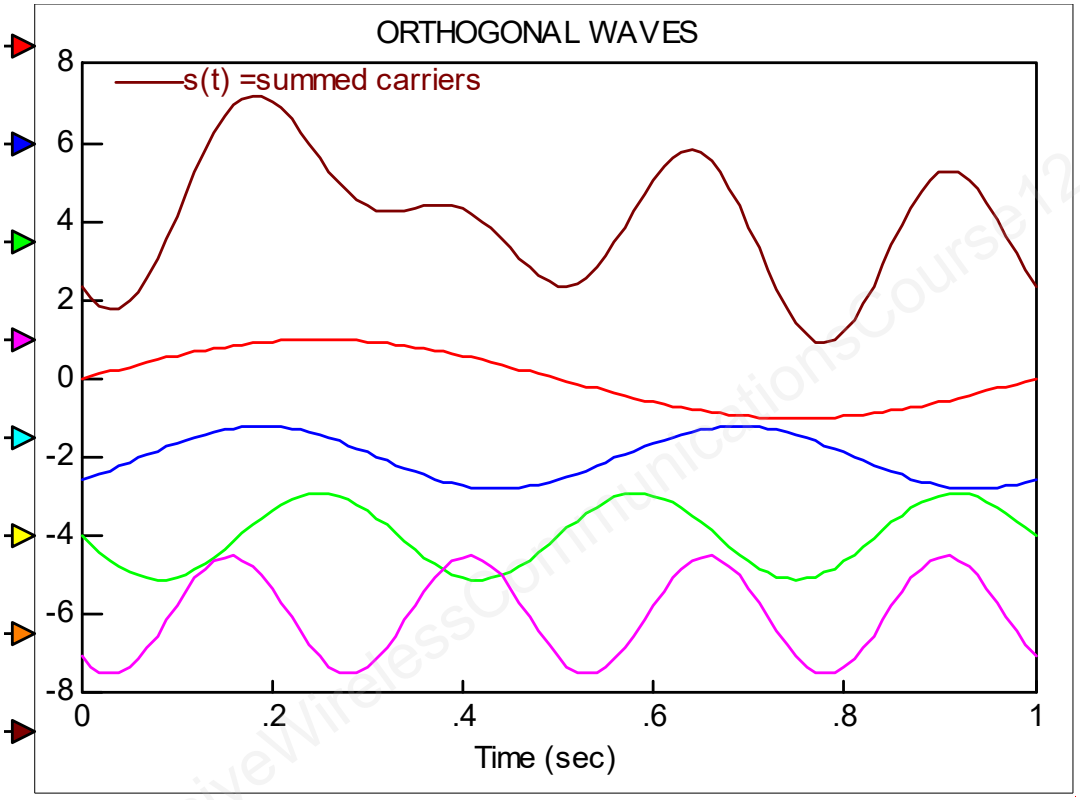
$$f_i - f_{i+1} = f_0 = 1/T$$

Orthogonality

$$\int_{-\infty}^{\infty} x_p(t) \cdot x_q(t) \cdot dt = 0 \qquad p \neq q$$

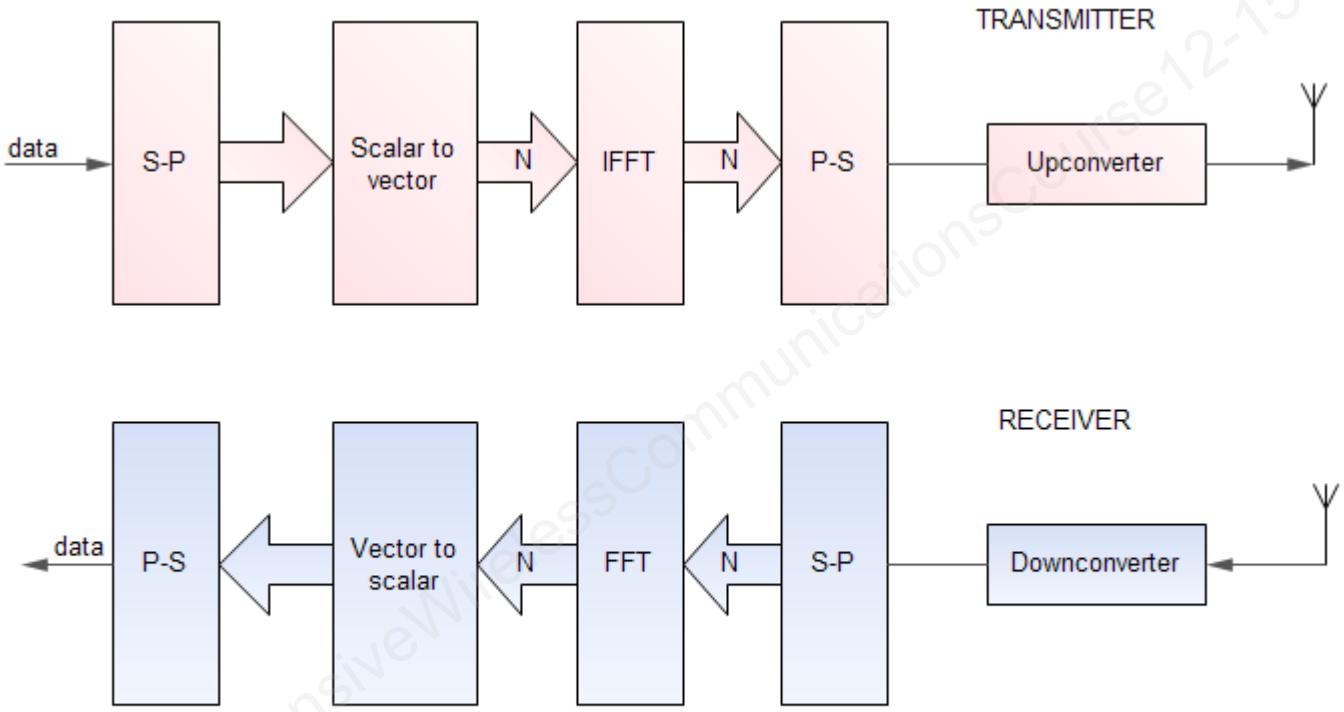


Orthogonal Carriers



$$s(t) = Re\left\{\sum_{k=1}^{N} x_k A_k e^{j2\pi \cdot k \cdot f_0 \cdot t}\right\} \qquad T = 1/f_0$$

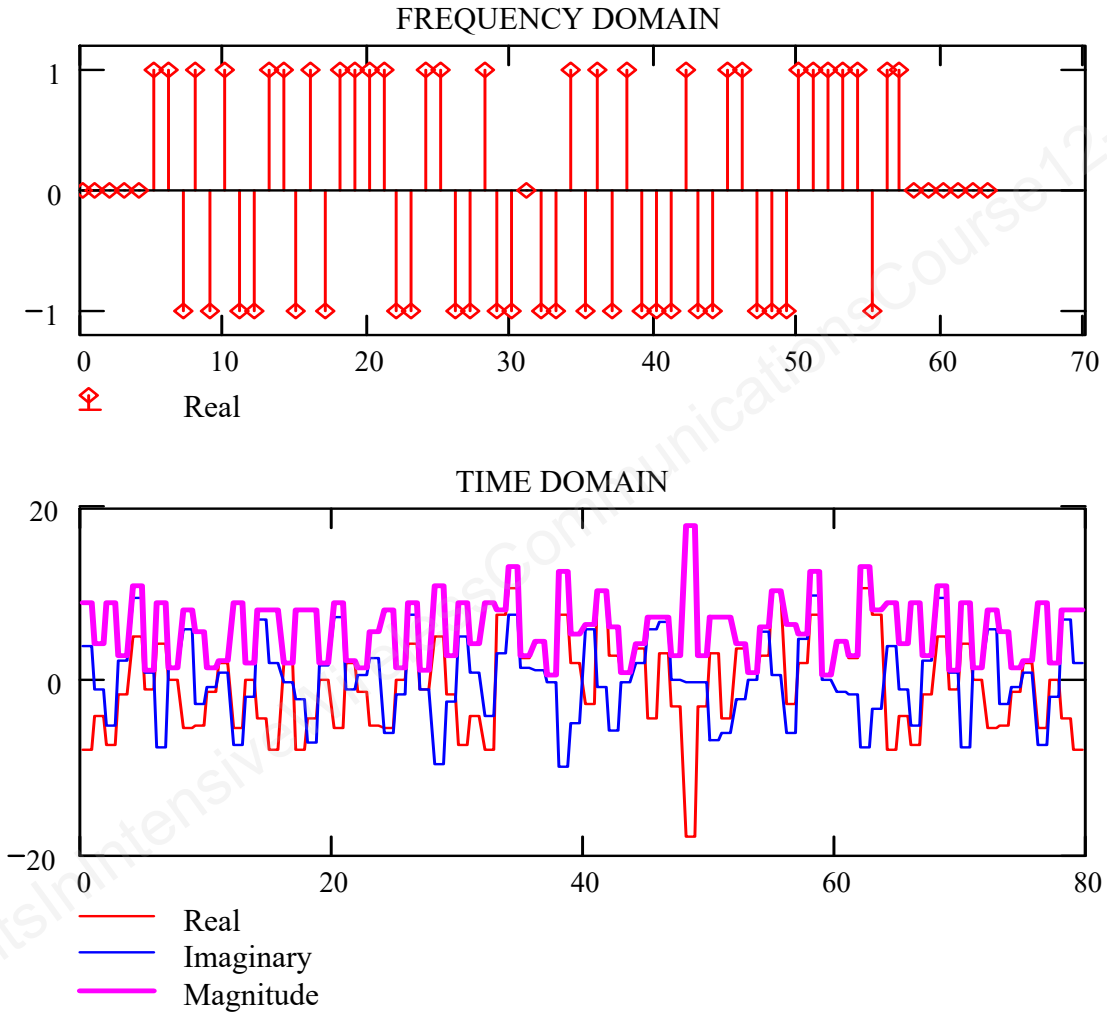
OFDM Basic Diagram



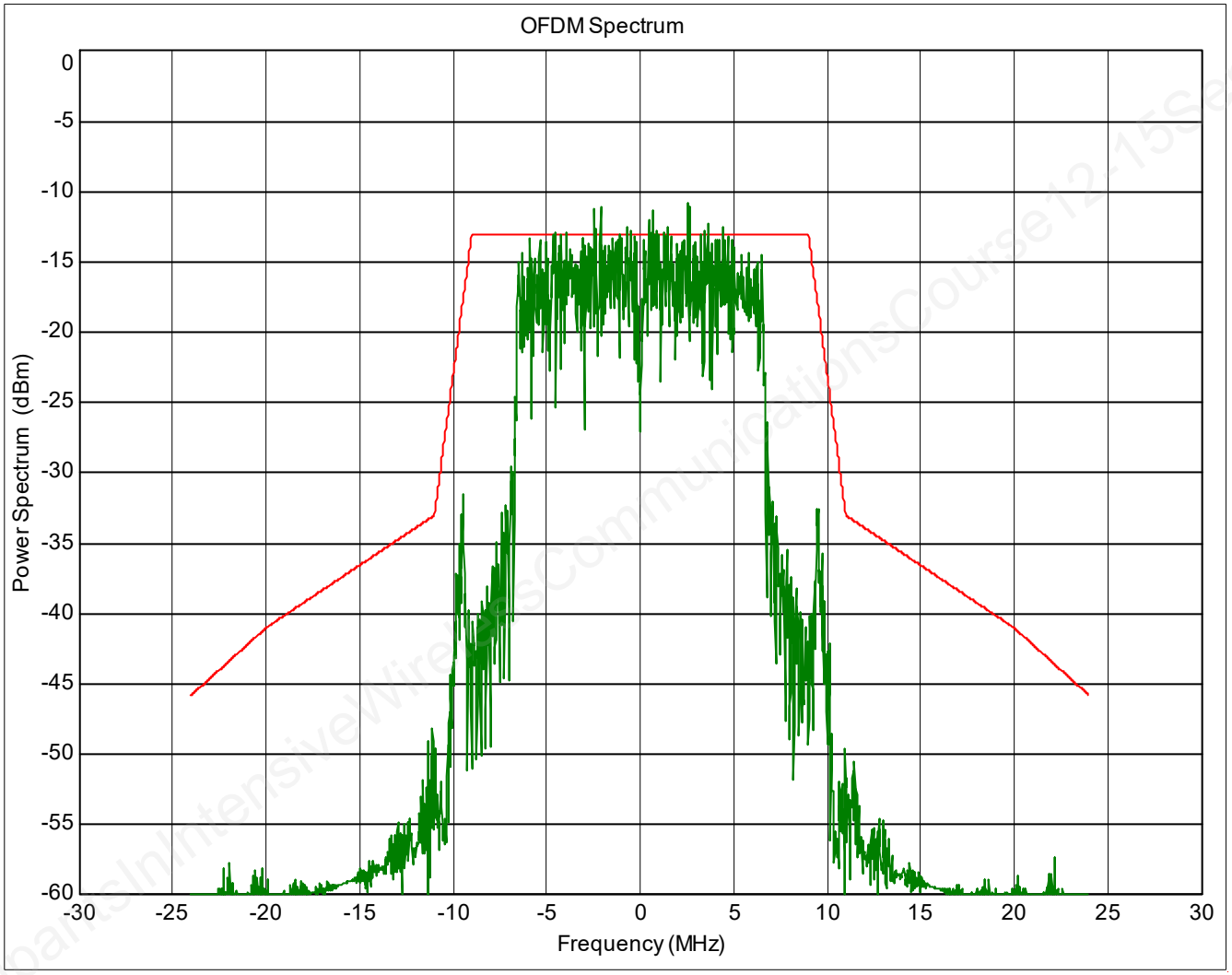
S-P Serial to Parallel
P-S Parallel to Serial
IFFT Inverse Fast Fourier Transform
FFT Fast Fourier Transform

$T=N/f_s$

OFDM Signals



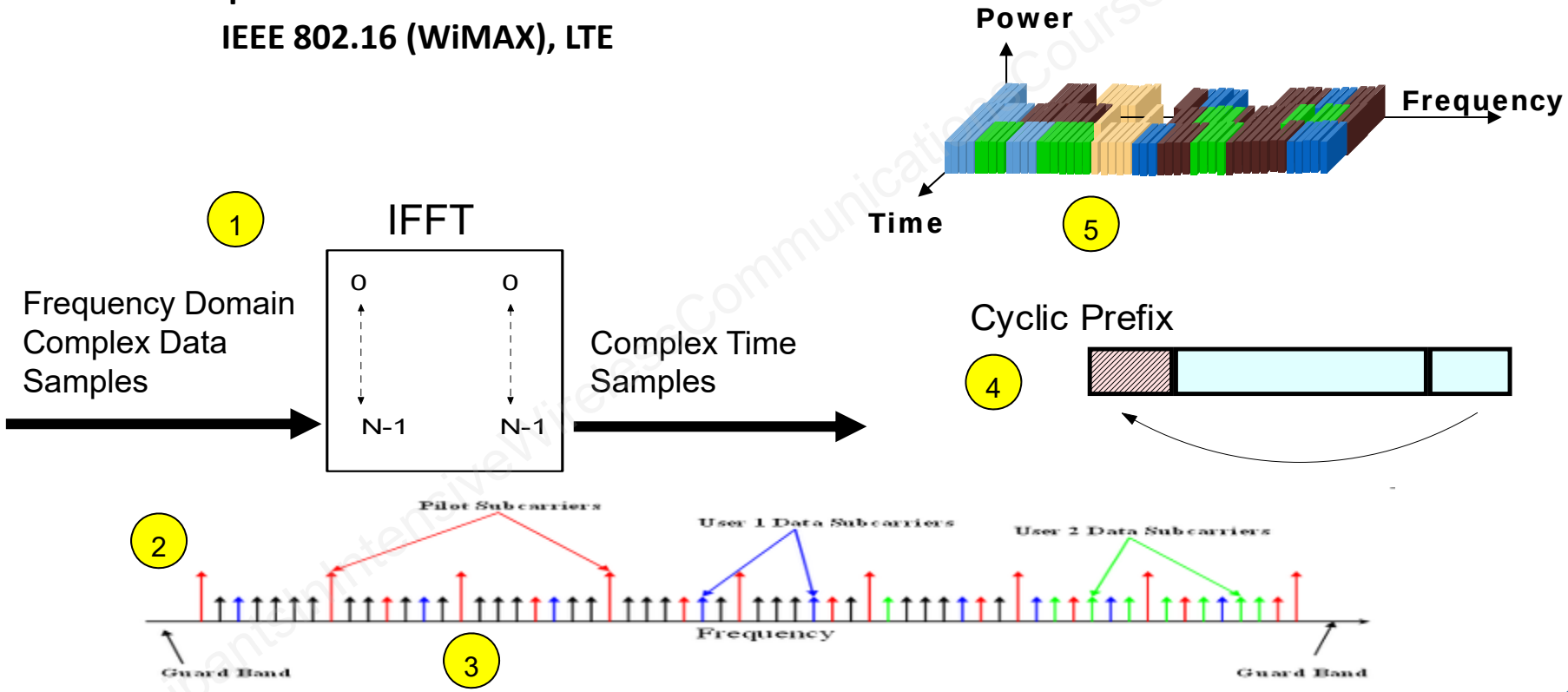
OFDM Spectrum



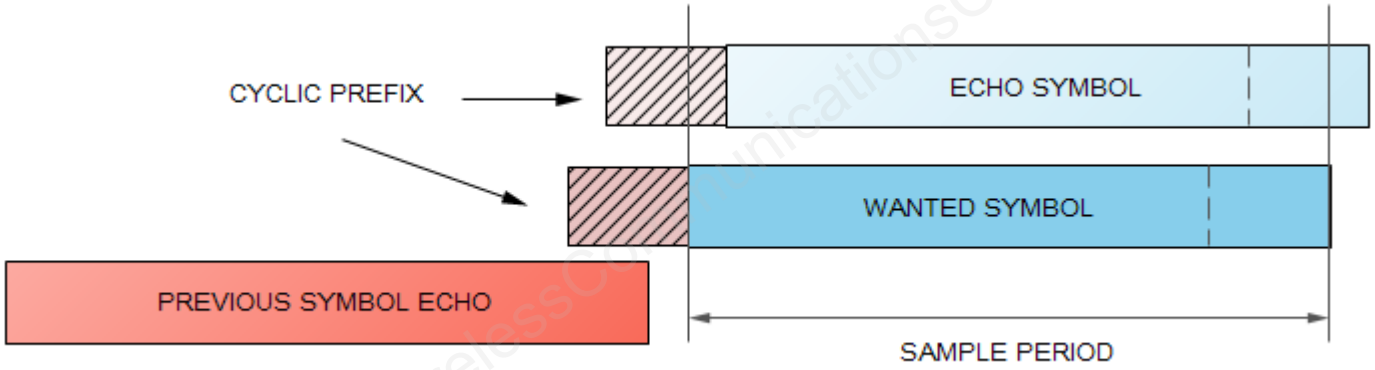
OFDMA

- **Based on Orthogonal Frequency Division Multiplexing (OFDM) technology**
- **Assign sub-sets of a large number of sub-carriers to different users**
- **Examples**

  IEEE 802.16 (WiMAX), LTE

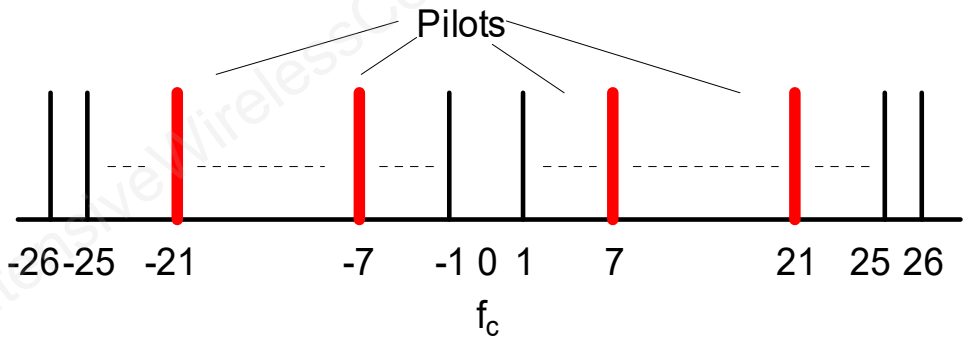


Cyclic Prefix



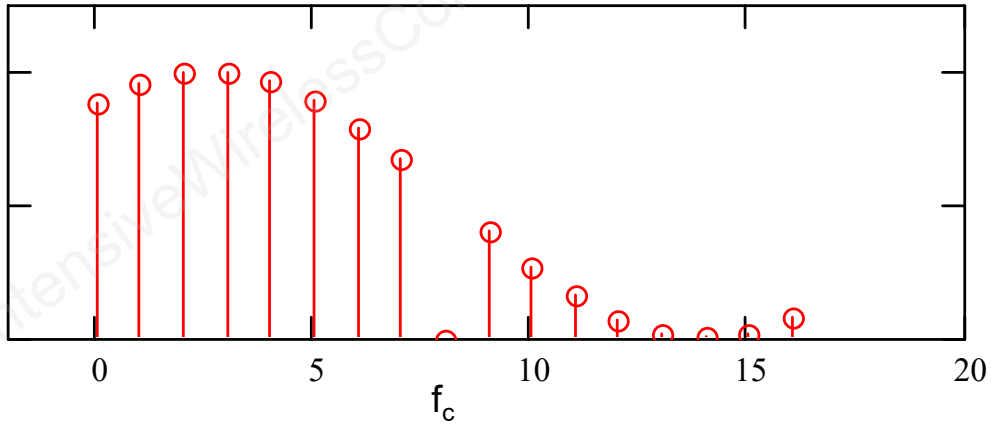
Pilot Subcarriers

- Synchronization ☺
- Phase adjustment ☺
- Increase Bandwidth ☹



Coding and Interleaving

- Reconstruct data lost on interfered with subcarriers
- Compensate for selective fading



Interleaving

ENCODED SOURCE

A						B						C						D						E						F					
A1	A2	A3	A4	A5	A6	B1	B2	B3	B4	B5	B6	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	D5	D6	E1	E2	E3	E4	E5	E6	F1	F2	F3	F4	F5	F6

INTERLEAVED

1						2						3						4						5						6					
A1	B1	C1	D1	E1	F1	A2	B2	C2	D2	E2	F2	A3	B3	C3	D3	E3	F3	A4	B4	C4	D4	E4	F4	A5	B5	C5	D5	E5	F5	A6	B6	C6	D6	E6	F6

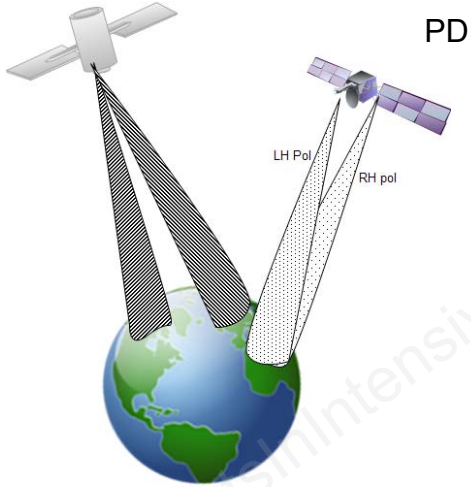
DE-INTERLEAVED BEFORE DECODING

A						B						C						D						E						F					
A1	A2	A3	A4	A5	A6	B1	B2	B3	B4	B5	B6	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	D5	D6	E1	E2	E3	E4	E5	E6	F1	F2	F3	F4	F5	F6

Other Multiple Access Schemes

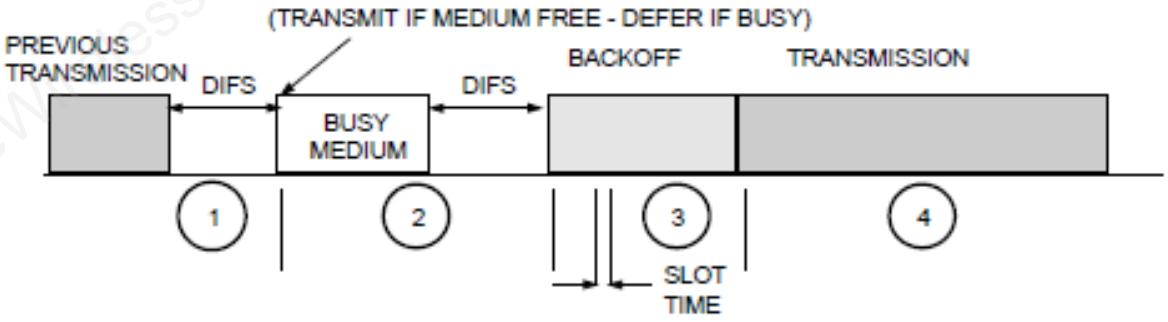
- Space Division Multiple Access (SDMA)
- Polarization Division Multiple Access (PDMA)
- Packet Radio
  - Pure ALOHA (random access)
  - Slotted ALOHA (equal time slots, synchronized clocks)
  - Carrier Sense Multiple Access with collision avoidance (CSMA/CA)
  - polling

SDMA

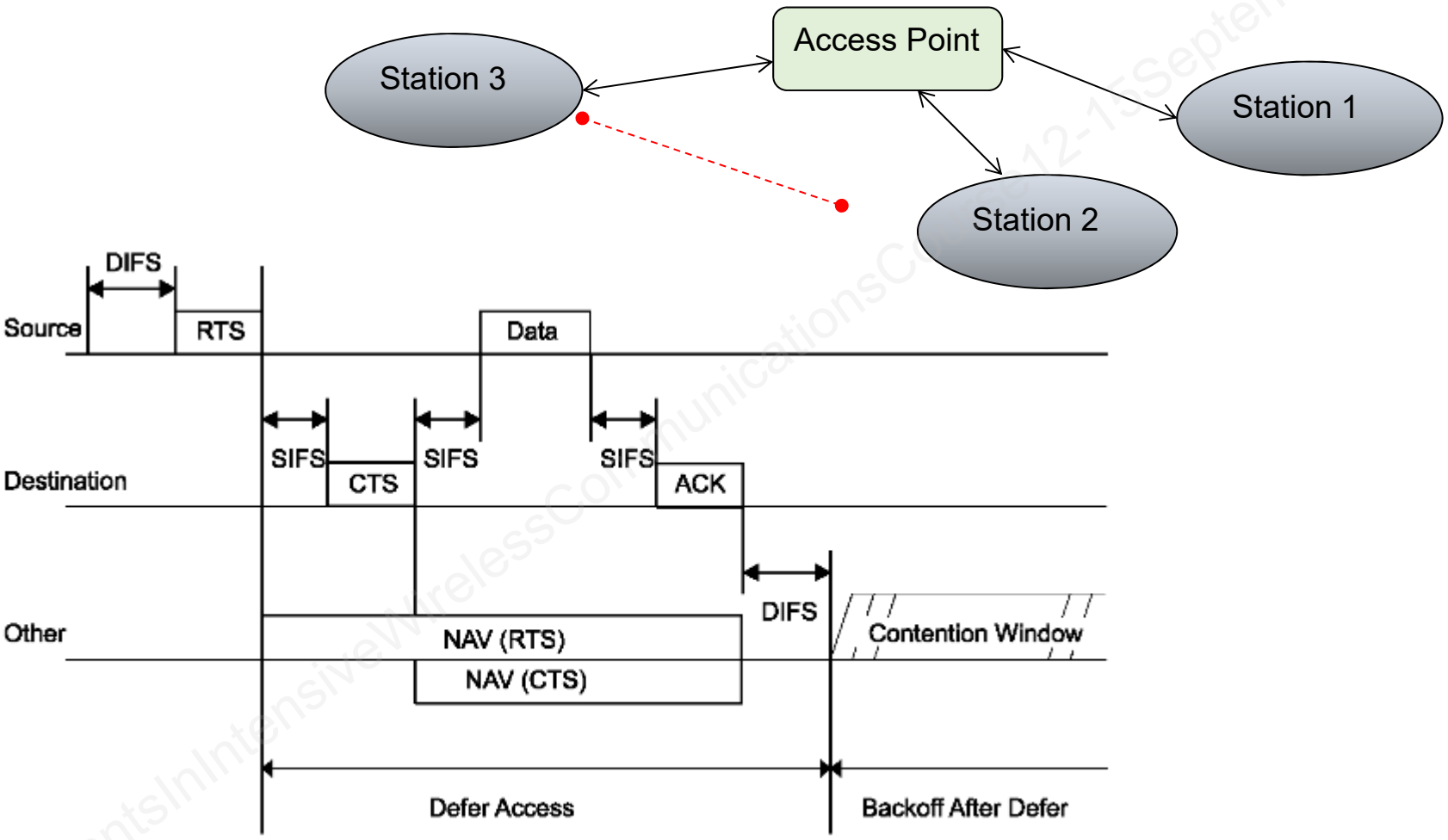


PDMA

CSMA/CA access method



RTS/CTS Medium Access



Source: IEEE Std. 802.11-2007

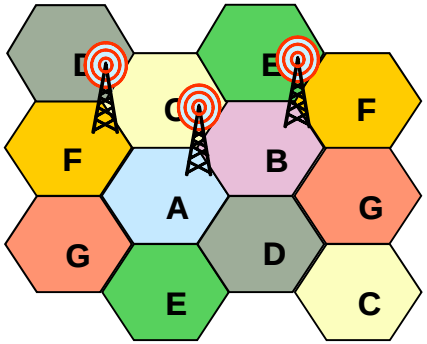
Practice Questions (4)

1. True or False: TDMA is better than FDMA because it multiples the number of users in a given bandwidth by the number of slots per frame.
2. One advantage of TDD over FDD is
   a) It has duplex filters to separate transmit and receive signals
   b) It doubles spectrum efficiency
   c) It facilitates channel estimation for link control
   d) It can be used for analog as well as digital signals
3. OFDM has better spectral efficiency than FDM because
   a) of the use of the cyclic prefix
   b) it can incorporate higher orders of phase modulation
   c) It eliminates intersymbol interference
   d) subcarrier separation is optimally small
4. A CDMA system occupies a bandwidth of 1.25 MHz. For a data rate of 64 kbps using QPSK modulation, the processing gain is approximately a) 13 dB, b) 16 dB, c)19 dB, d) 22 dB

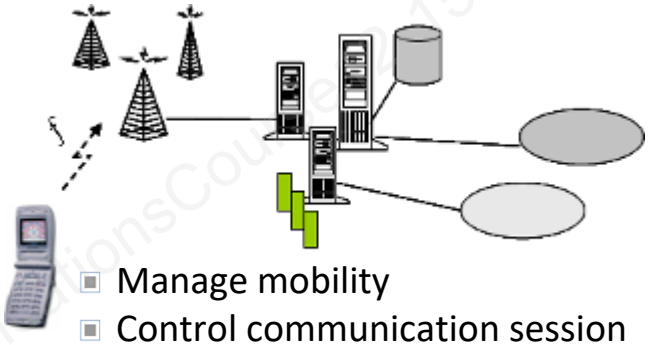
Cellular Communication

Cellular Concept

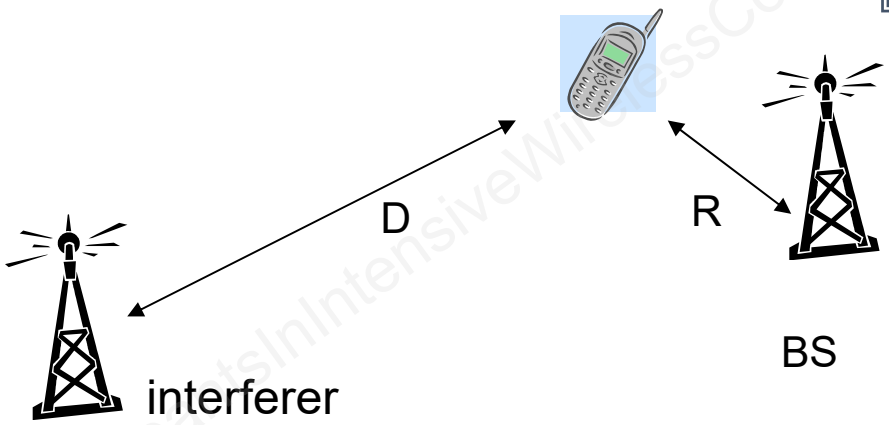
- Coverage
- Mobility & Handover
- Frequency re-use
- Sectors



Serving Mobile User



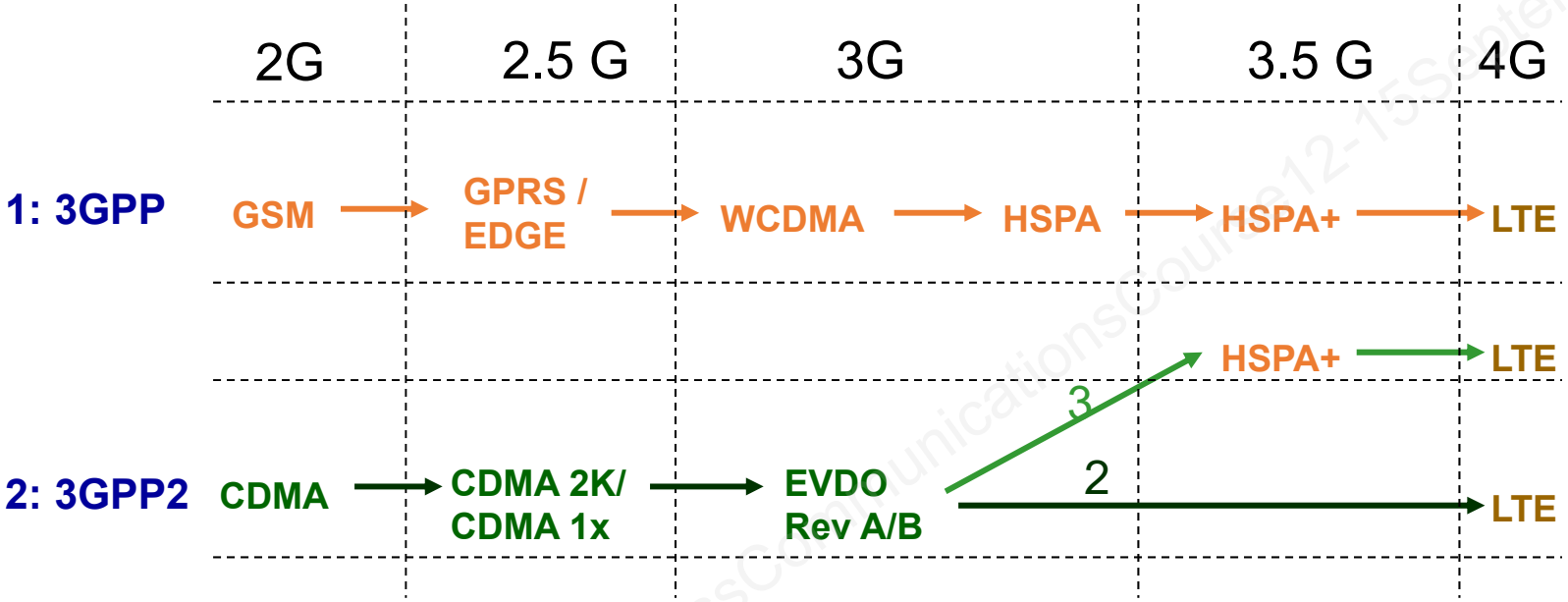
- Manage mobility
- Control communication session
- Allocate radio resources
  - Wireless Transmission & Access



$$\frac{S}{I} \approx \frac{(D/R)^n}{i_0} \approx \frac{\left(\sqrt{3N}\right)^n}{i_0}$$

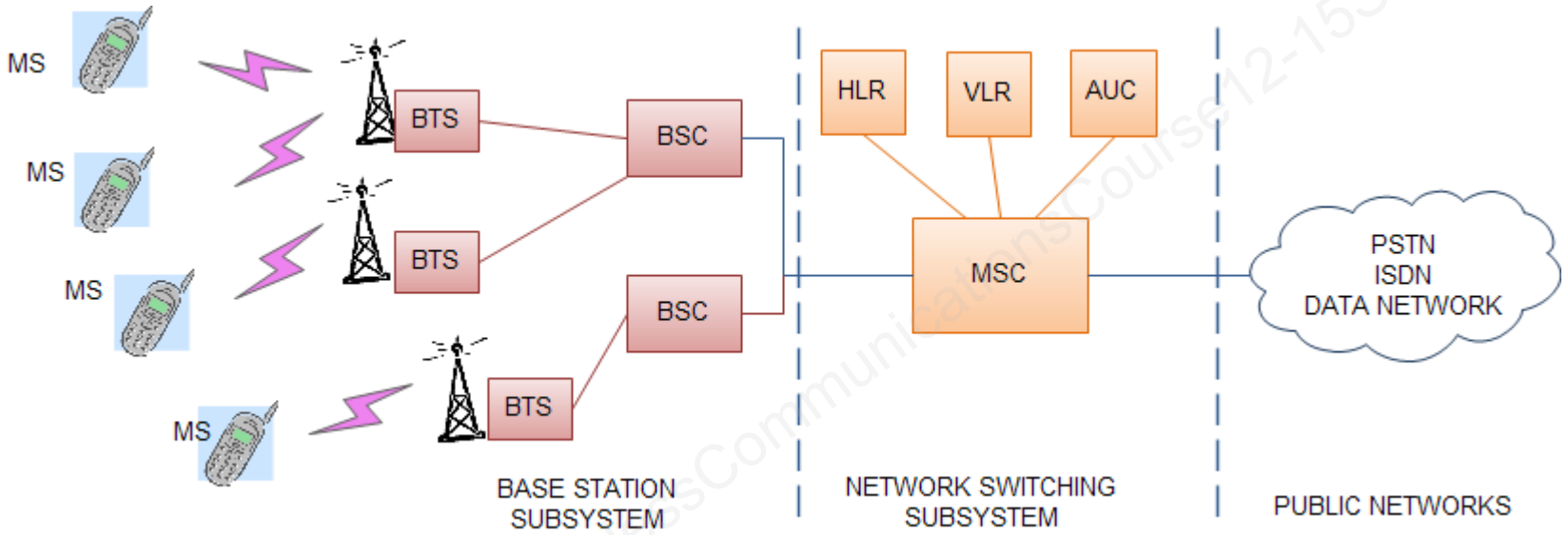
n=path loss exponent
N=cluster size
i_0=number of interfering cells
S/I=signal/interference (power ratio)

Cellular Network Evolution Tracks



3GPP: Third Generation Partnership Project
GSM: Global System Mobile
CDMA: Code Division Multiple Access
GPRS: General Packet Radio Service
EDGE: Enhanced Data Rates for GSM Evolution
WCDMA: Wide Code Division Multiple Access
HSPA: High Speed Packet Access
EVDO: 1xEVolution Data Optimized
LTE: Long Term Evolution

GSM Architecture



MS Mobile Station
BTS Base Transceiver Station
BSC Base Station Controller
MSC Mobile services Switching Center

HLR Home Location Register,
VLR Visitor Location Register,
AUC Authentication Center,

Packet Switching vs. Circuit Switching

- Circuit switching
  - Set up circuit, reserve resources
  - Tear down circuit at end
  - Data in circuit does not need to contain routing info
  - Resources (occupied channel) held even when no data to send
- Packet switching
  - Send packets with all routing info in header
  - Packets may be sent over different routes and arrive out of order
  - No resources used when there is nothing to send
- For bursty data, packet switching is more efficient
- Virtual circuit switching retains CS advantages

GSM, GPRS, EDGE

GSM

TDMA + Frequency hopping, FDD

200Khz channels, with 8 time slots

Circuit-switched voice channels

Gaussian Minimum Shift Keying Modulation

0.577 ms time slots

High speed Circuit Switched Data

GPRS

TDMA Based on GSM Allows Packet Data

Use of multiple timeslots and coding options to build throughput

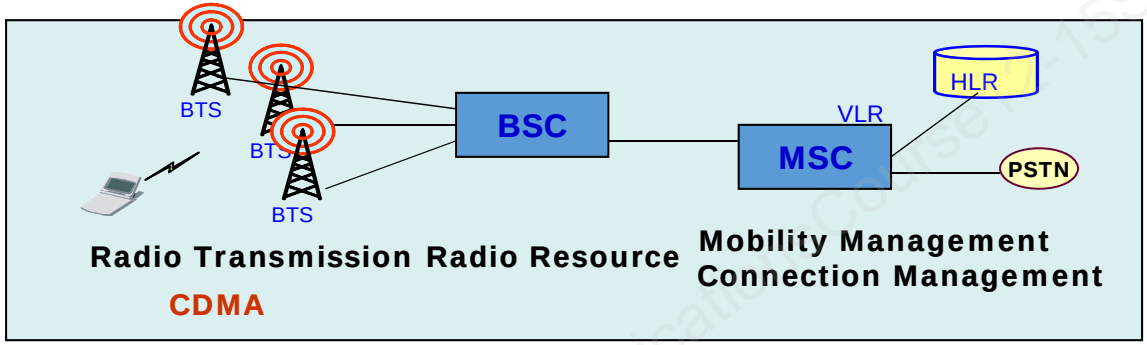
Two new functional entities or GPRS Support Nodes (GSN):

- Serving GSN (SGSN) – controls BSC
- Gateway GSN (GGSN) – interfaces packet networks

EDGE: 8 PSK modulation, max data rate 384 kb/s

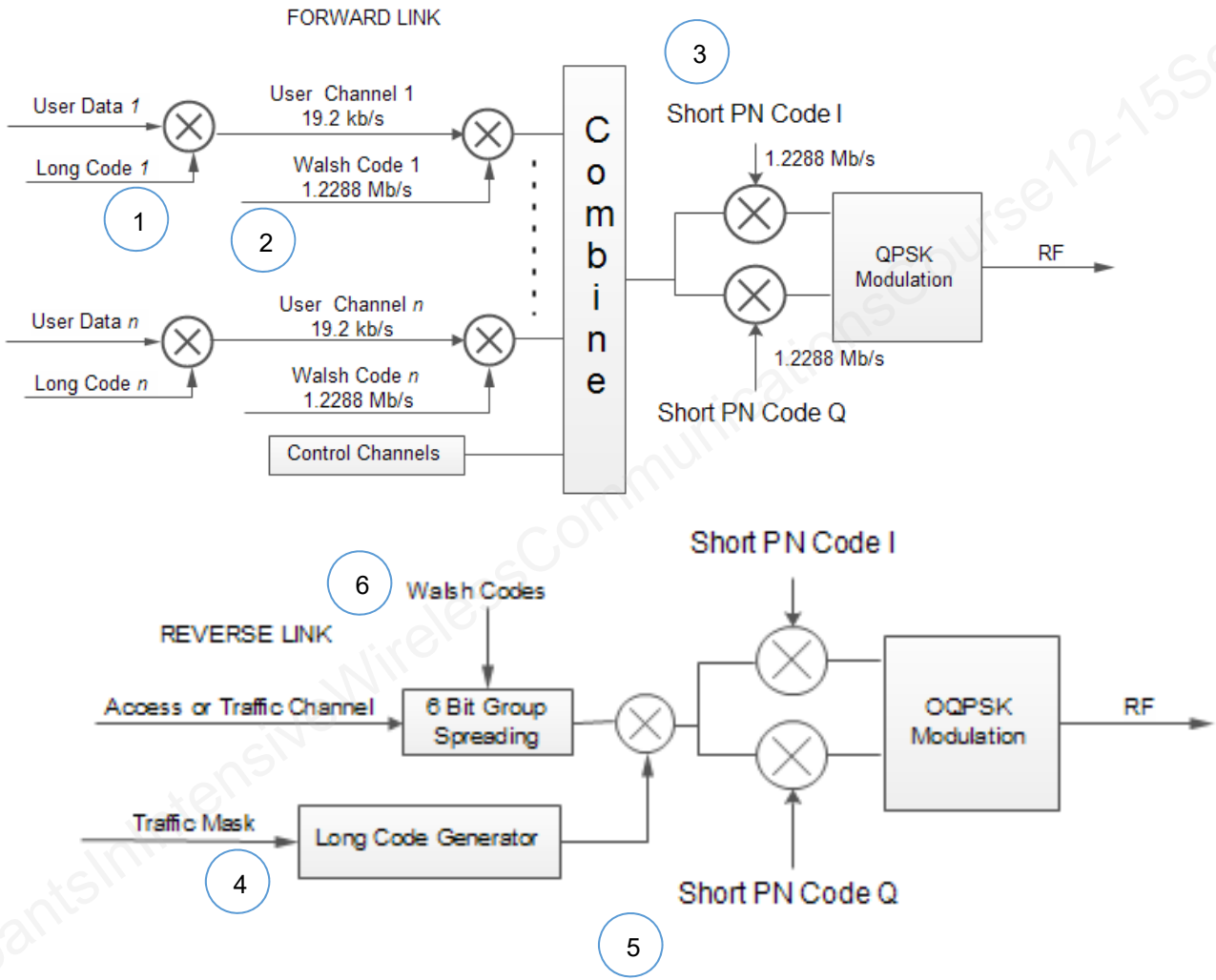
More advanced coding / modulation – Higher throughput

cdmaOne – 2G CDMA and its Enhancements (3GPP2)



- Complete wireless system based on (TIA/EIA IS-95) CDMA standards
  - IS-95A Revision
    - Basis for 2G CDMA systems (since mid-90s)
    - Wideband 1.25 MHz channel, and new handoff, power-control, call processing and other mechanisms
  - IS-95B Revision
- **Evolved to CDMA2000** (& other) systems

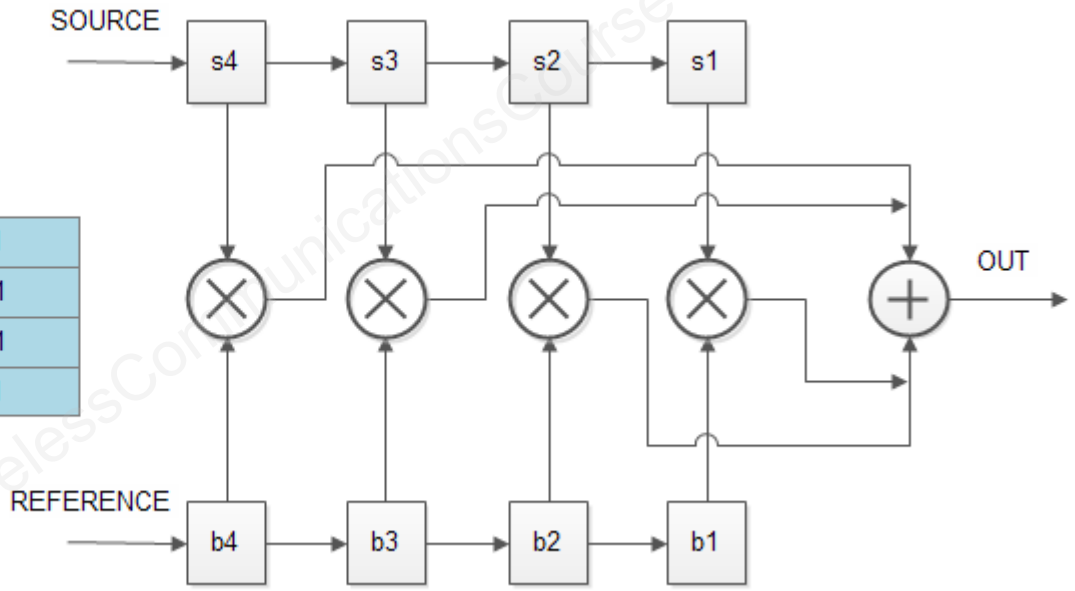
cdmaOne (IS-95) Modulation



Walsh Codes

WALSH CODES N=2

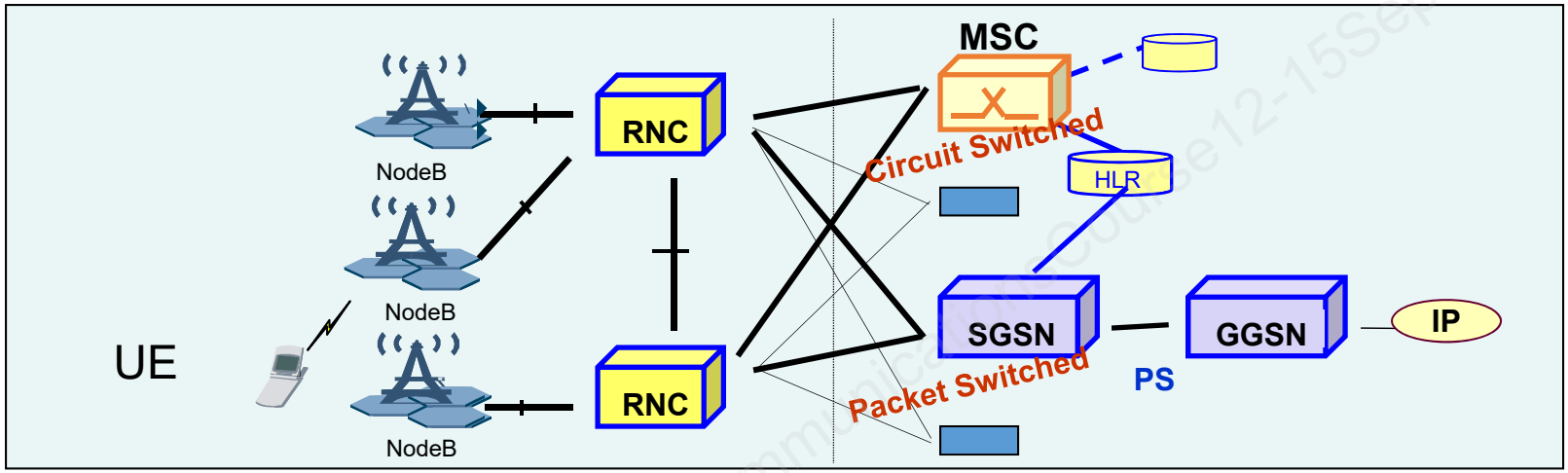
1	1	1	1
1	-1	1	-1
1	1	-1	-1
1	-1	-1	1



IMT-2000

- Used worldwide
- Used for all mobile applications
- Support both packet-switched (PS) and circuit-switched (CS) data transmission
- Offers high data rates up to 2 Mbps (depending on mobility/velocity)
- Offers high spectrum efficiency
- Original frequency bands
  - 1920 – 1980 MHz (UL) paired with 2110 – 2170 MHz (DL), FDD
  - 1900 – 1920 MHz and 2010 -2025 MHz unpaired, TDD

UMTS

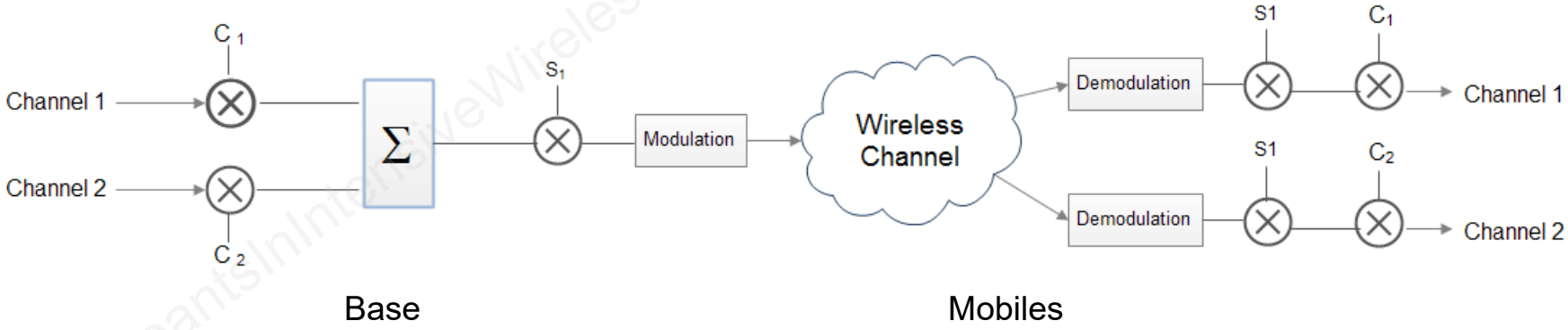


- Joint effort by organizations in 3G Partnership Project (3GPP)to meet goals of ITU IMT-2000
- Release 99 specified a new air interface using wideband CDMA (WCDMA) – maximizing re-use of GSM/GPRS network/service concepts
- HSPA-UMTS Evolution
  - **HSDPA (Rel 5)**
  - **HSUPA (Rel 6)**
  - **HSPA+ (Rel 7)**

UMTS – Universal Mobile Telecommunications System
HSDPA – High-Speed Downlink Packet Access
HSUPA – High-Speed Uplink Packet Access

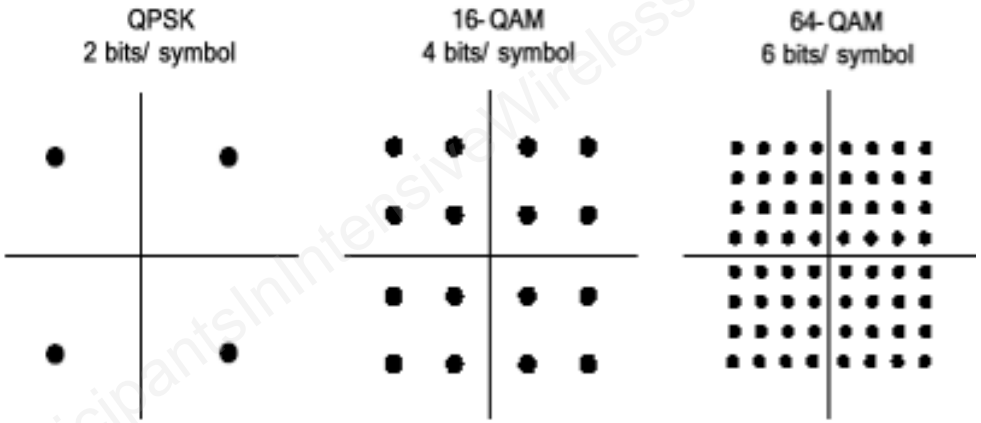
WCDMA

- Channel BW: 5MHz (x2 for FDD)
- FDD & TDD
- Chip rate 3.84 Mbps
- OVSF Orthogonal Variable Spreading Factor
- Maximum Data Rate 2 Mbps
- Closed Loop Power Control 1500 times/sec
- Soft and Softer Handover
- GSM Handover
- Supports MIMO



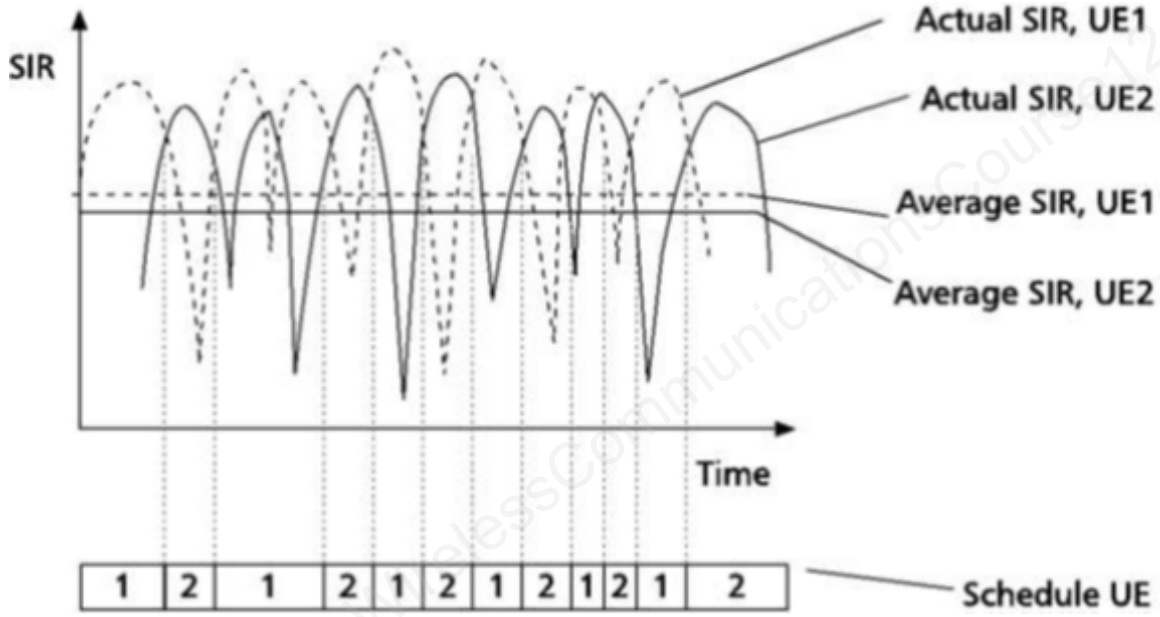
HSDPA

- 3GPP Release 5
- DL 14.4 Mbps (peak)
- New Data Channel:HS-PDSCH
  - 1 to 15 codes for concurrent channels
- Reduced frame time = 2 ms -- packet scheduling
- Hybrid ARQ (H-ARQ)
- Adaptive Modulation and Coding
  - QPSK or 16-QAM (64-QAM in later Release)



QPSK / QAM Signal Constellations

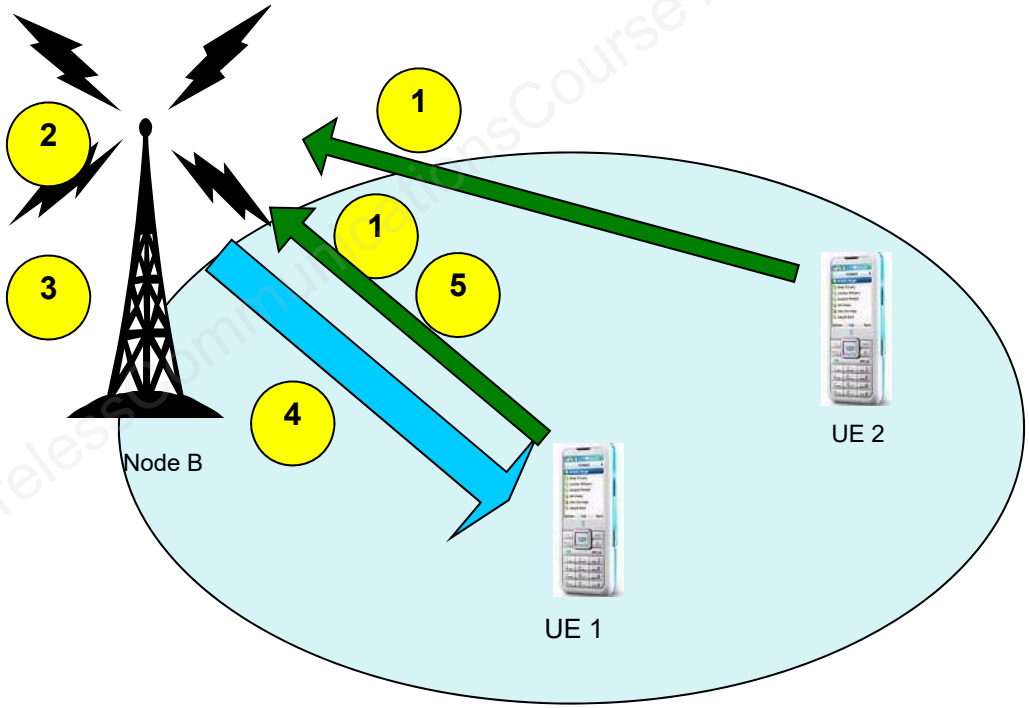
Downlink Packet Scheduling



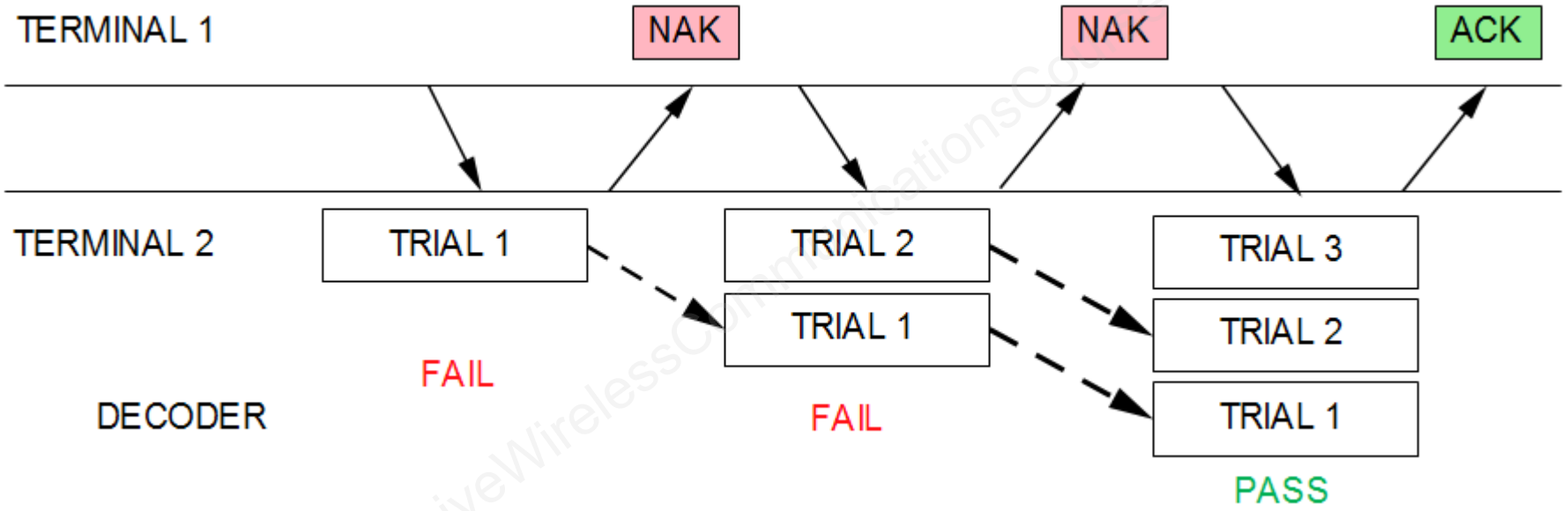
Multi-user spatial diversity

Adaptive Modulation and Coding

STEP 1: Channel quality feedback (CQI)
STEP 2: Scheduling – selection of the UE for transmission
STEP 3: Adaptive modulation order and coding redundancy
STEP 4: User data transmission
STEP 5: ACK/NACK feedback



H-ARQ



HSPA Evolution

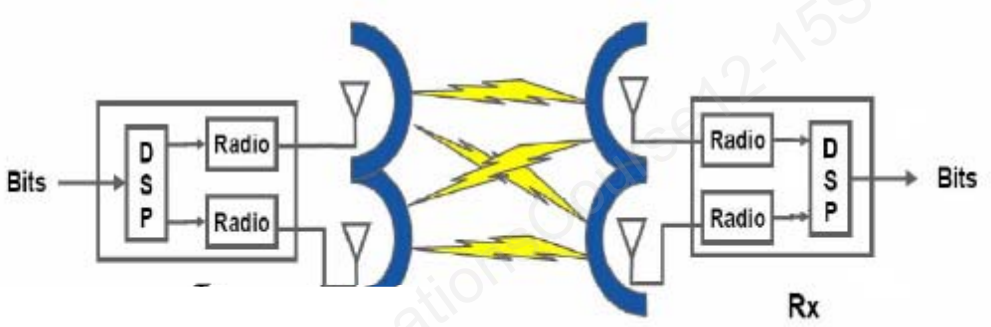
- **HSUPA - 3GPP Release 6**
  - **Enhancement of uplink's throughput: 5.76 Mbps (peak)**
  - **Uplink enhanced dedicated channel (E-DCH)**
  - **Short transmission time interval (2ms) – fast response to changing radio conditions**
  - **Fast Node B based scheduling – efficient allocation of radio resources – reduced latency**
  - **Fast Hybrid ARQ**

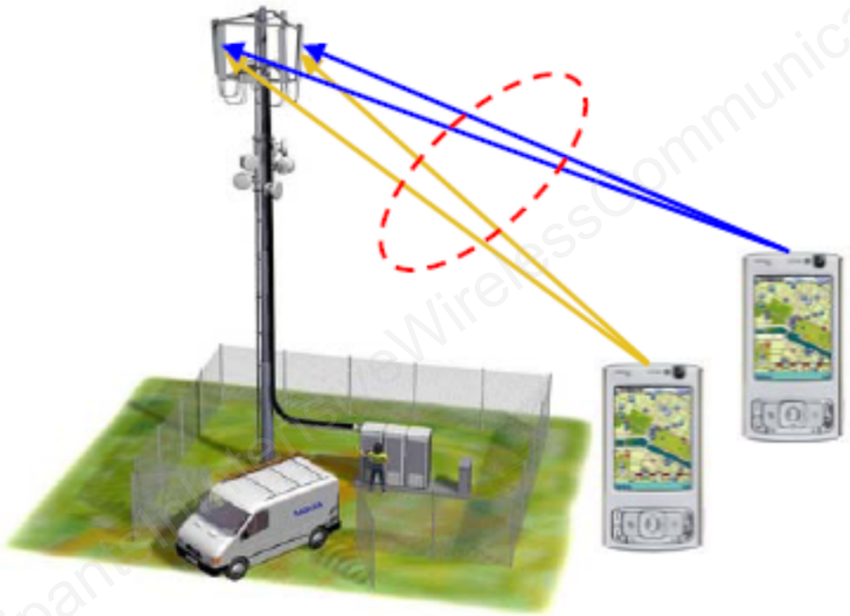
- **HSPA+ , 3GPP Release 7 & beyond**
  - **Enhancements to evolve HSPA family**
    - **Adaptive use of 64 QAM, in addition to QPSK and 16 QAM**
    - **Use of multi-user MIMO antenna technology**
    - **Use of multiple concatenated carriers**

Multiple-Input Multiple-Output (MIMO)

Example

- **2x2 MIMO System**





Example

- **Uplink Multi-user MIMO**

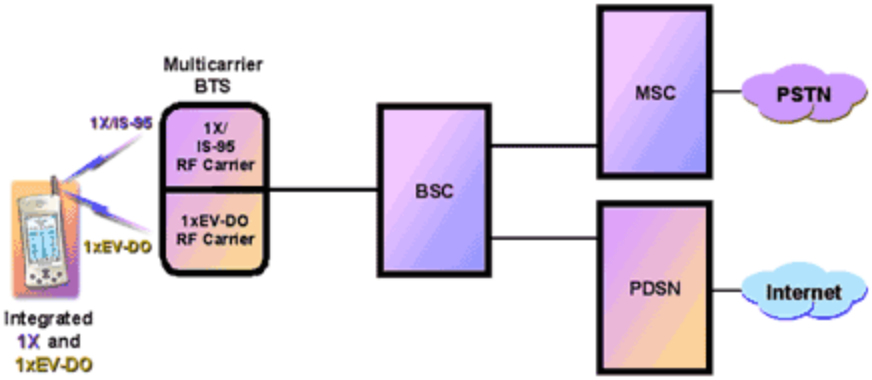
CDMA2000 – 3G Evolution

CDMA2000 1X

- Peak data rates of 307 Kbps downlink & 153 Kbps uplink, in a 1.25 MHz FDD channel

CDMA2000 1xEV-DO (Evolution-Data Optimized)

- **Release 0**
  - Peak data rates of 2.4 Mbps downlink & 153 Kbps uplink, in a single 1.25 MHz FDD channel
  - High-speed downlink packet channel
  - Advanced techniques as discussed earlier for HSPDA
    - Fast & adaptive modulation, coding, and scheduling
    - Fast re-transmission based on H-ARQ
    - Short Transmission Time Interval (TTI)
- **Rev A**
  - 3.1 Mbps DL, 1.8Mbps UL
- **Rev B**
  - Aggregation of up to 15 1.25MHz channels for 20 MHz BW
  - Modulation 64QAM DL, 16QAM UL
  - 73.5 Mbps peak



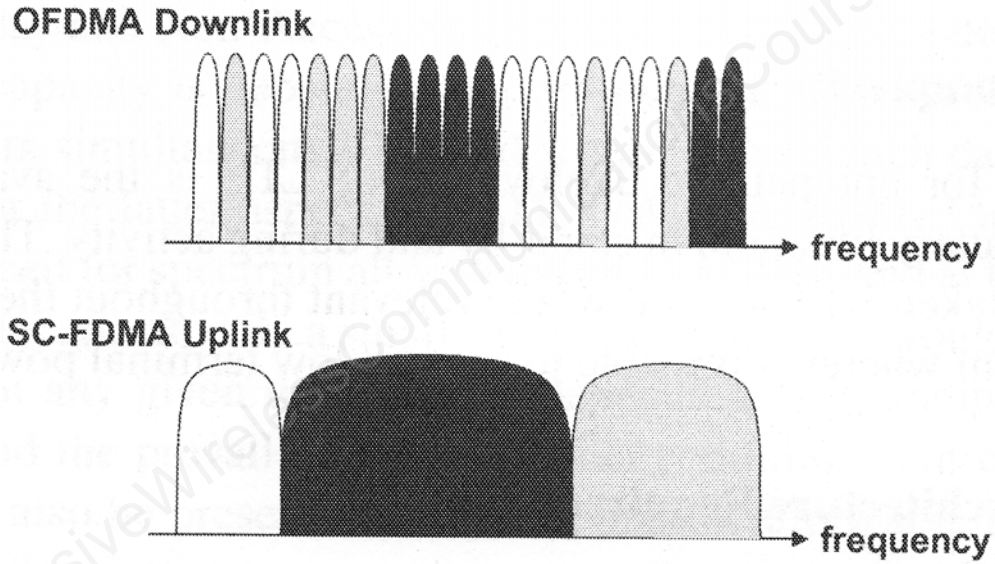
LTE Requirements

- Reduced connection establishment delay and transmission latency
- Increased user data rates
- Increased cell edge bit rate
- Reduced cost per bit – better spectral efficiency
- Spectrum usage flexibility – new and existing bands
- Simplified network architecture
- Seamless mobility, also between different radio access technologies
- Reasonable power consumption for mobile terminal

LTE Performance Targets

	Requirement	Value	Condition
DL	Peak rate	>100Mb/s	20MHz FDD MIMO 2x2
	Spectral efficiency	>5bps/Hz	
	Broadcast spectral efficiency	>1bps/Hz	Dedicated carrier
UL	Peak rate	>50Mbps	20MHz FDD Single ant. Tx
	Spectral efficiency	>2.5bps/Hz	
System	User plane latency	<10ms	2 way radio delay
	Connection setup	<100ms	Idle to active
	Operating bandwidth	1.4-20MHz	

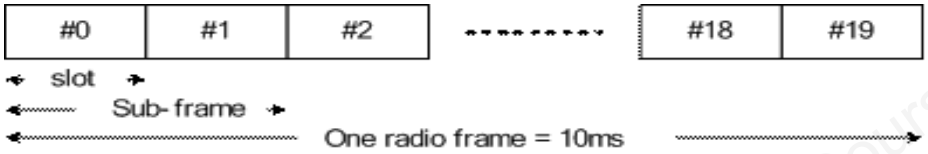
LTE Multicarrier Spectrum



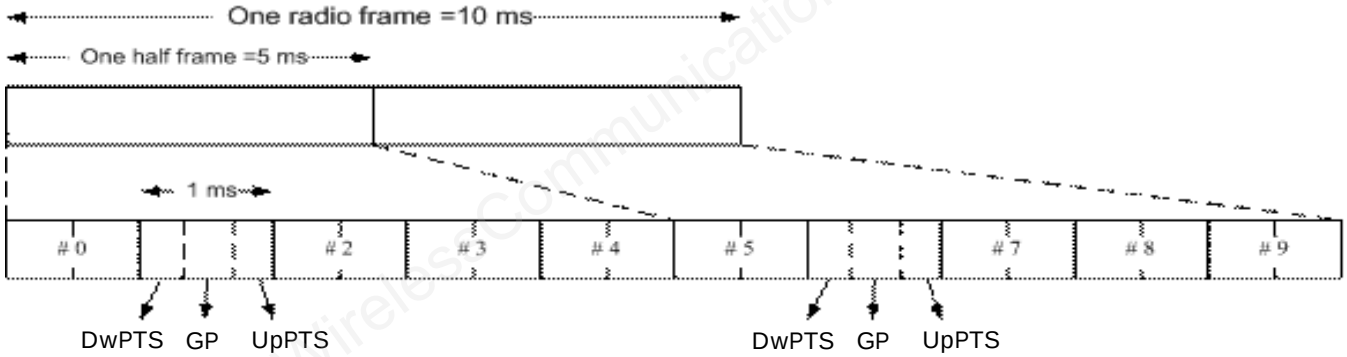
Reference: Sesia, Toufik, Baker, “LTE The UMTS Long Term Evolution”, Wiley, 2009, p. 14.

LTE Frame Structure

Type 1 - FDD

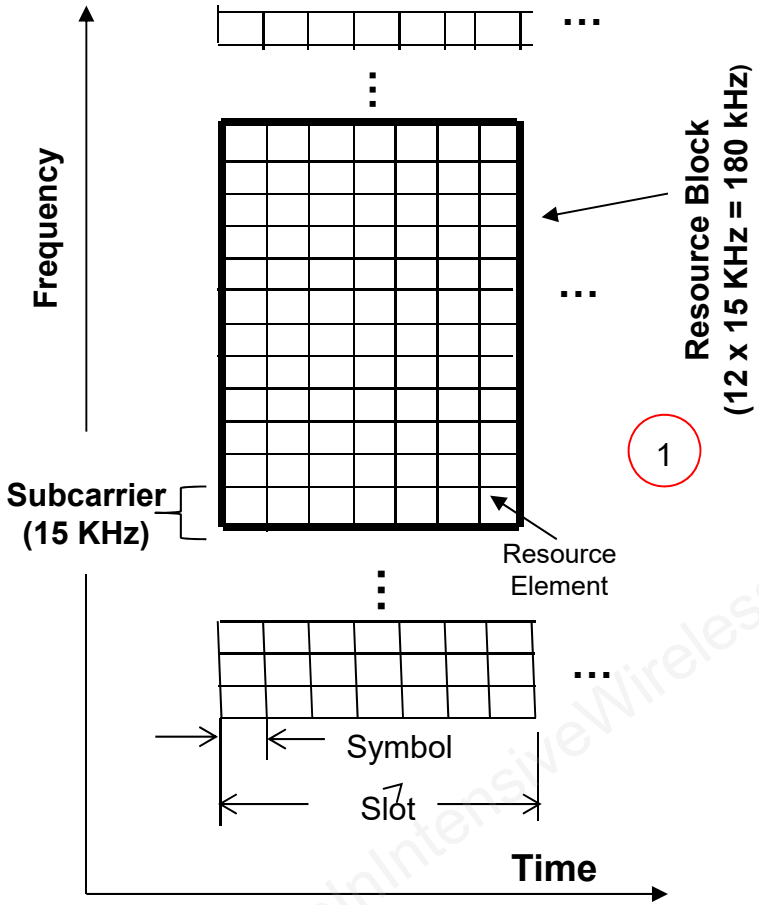


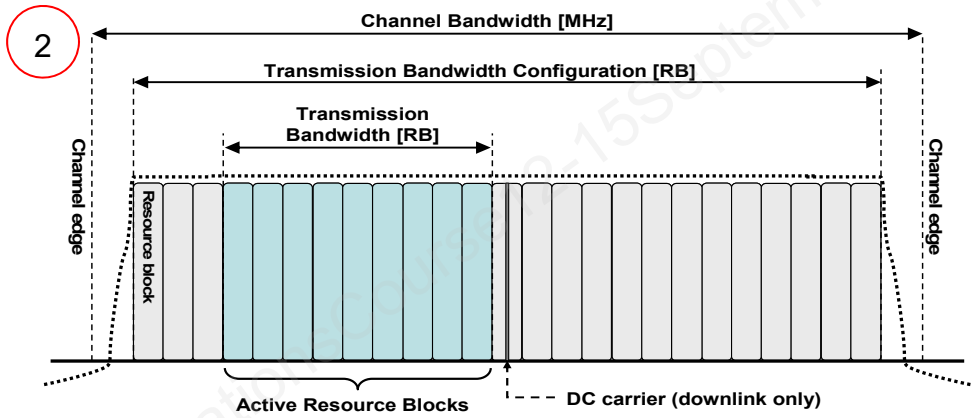
Type 2 - TDD



- One radio frame = 10 ms 10 sub-frames of 1 ms
- Each sub-frame includes 2 slots of 0.5 ms each (except sub-frames 1 & 6 in TDD as shown)
- In FDD, all 10 sub-frames can transmit in both downlink and uplink – separated in frequency
- In TDD, uplink and downlink transmission are separated in time – one half-frame is 5ms as shown

LTE Physical Layer Transmission





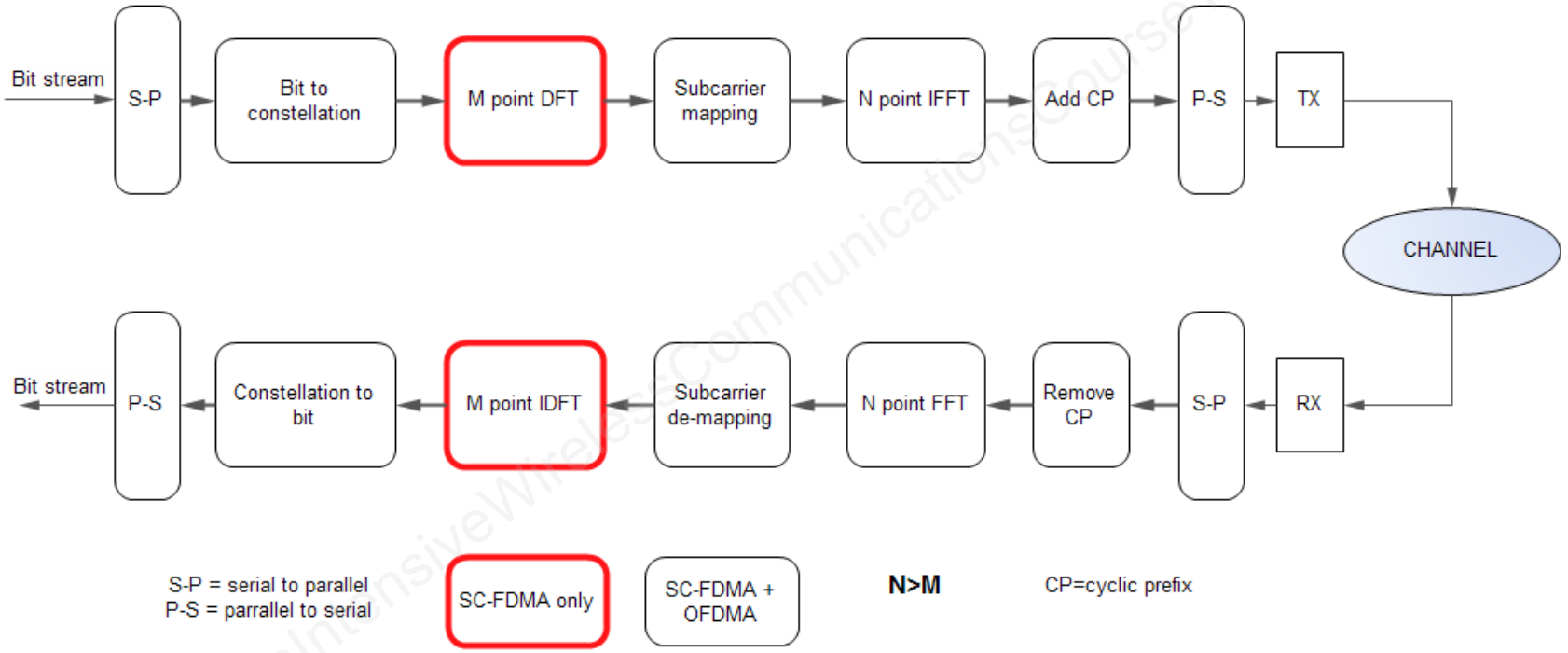
3

Channel BW, MHz	1.4	3	5	10	15	20
Resource Blocks	6	15	25	50	75	100
Resourced Subcarriers	72	180	300	600	900	1200
IDFT / DFT Size	128	256	512	1024	1536	2048

(I)DFT – (Inverse) Discrete Fourier Transform

- **Bandwidth agnostic based on resource blocks**
  - **Flexible spectrum / resource allocation**

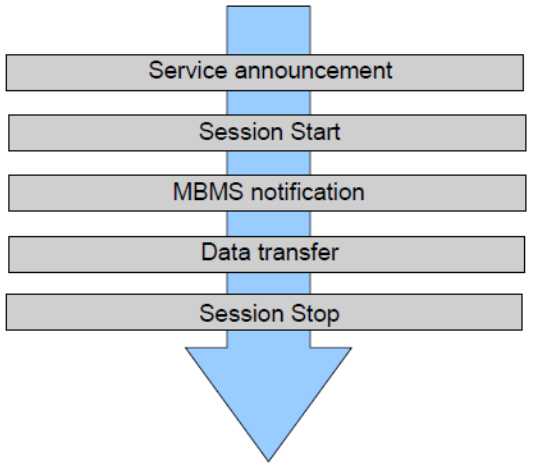
LTE Transmission and Reception



SC-FDMA : Single Carrier - Frequency Division Multiple Access

Evolved Multimedia Broadcast Multicast Service (eMBMS)

- Broadcast/multicast mechanism to deliver shared content to multiple user terminals
- Single frequency network (SFN)
- Basic transmission characteristics similar to unicast channel
- Mixed eMBMS and unicast carrier possible (part
- Standardization
  - Release 8 – Physical layer
  - Release 9 workable definition
  - Further enhancements in Rel 10



LTE Frequency Bands

E-UTRA Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6[1]	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
...			
24	1626.5 MHz – 1660.5 MHz	1525 MHz – 1559 MHz	FDD
...			
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD
41	2496 MHz 2690 MHz	2496 MHz 2690 MHz	TDD
42	3400 MHz – 3600 MHz	3400 MHz – 3600 MHz	TDD
43	3600 MHz – 3800 MHz	3600 MHz – 3800 MHz	TDD

Note 1: Band 6 is not applicable

From 3GPP TS 36.101 V10.1.0 (2010-12)

LTE-Advanced

- Antenna technology evolution (8x8 MIMO)
- Higher channel bandwidth
- Carrier (bandwidth) aggregation
  - Contiguous
  - Non Contiguous
- Self-Organizing Networks (SON)
  - Reduce effort needed to add new nodes to network
  - Load balancing between cells
- Improved cell edge interference coordination

5G: Performance Targets

Data Rate

- Aggregate data rate: x 1000 from 4G
- Edge rate: 100 Mbps to 1 GHz
- Peak rate: tens of GHz

Latency

- 1 ms (15 ms LTE) round trip

Energy and Cost

- No increase per link

Support High Diversity of Devices

5G: Key Technologies

Extreme densification and offloading

- Smaller cells: pico cells, femto cells
- More active nodes per unit area and Hz
- Mobility support across multiple radio access technologies (RAT) – heterogeneous networks
- Device to device (D2D) communication

Increased bandwidth

- mmWave spectrum – 20 to 100 GHz
- Use WiFi 5 GHz spectrum

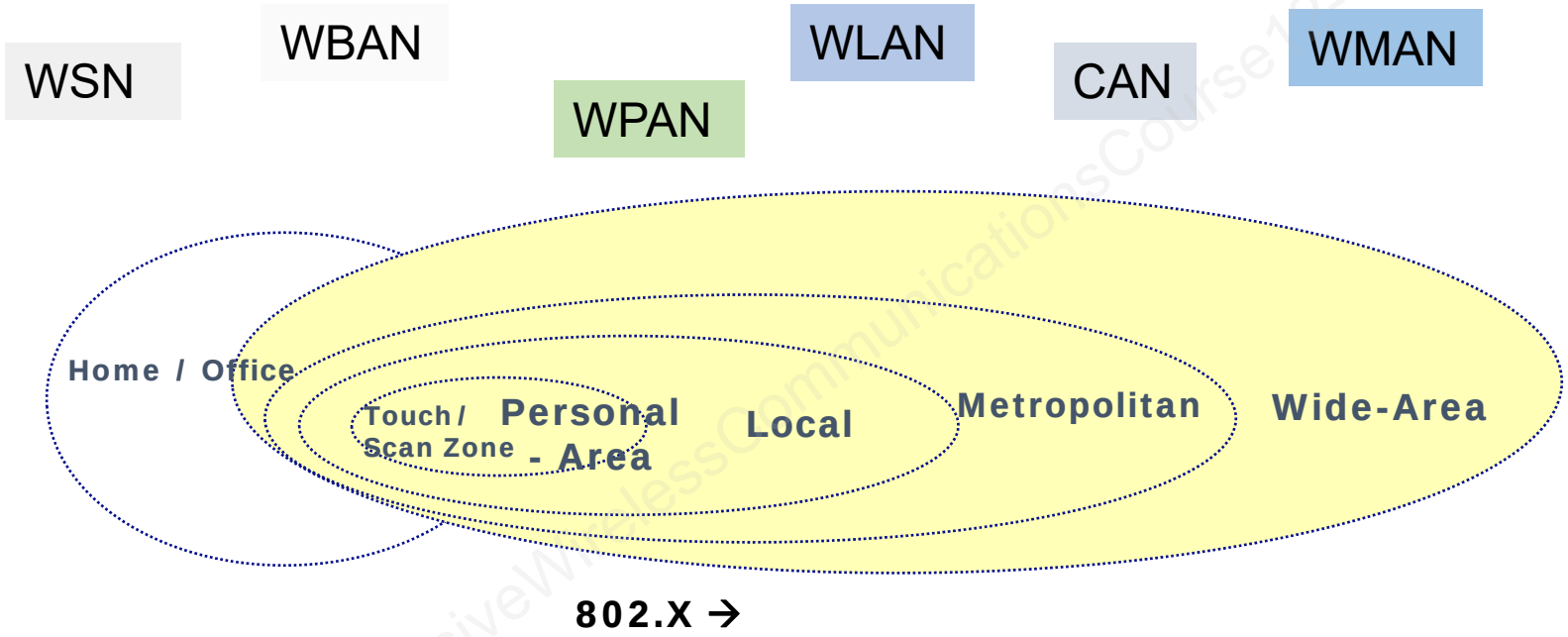
Increased Spectral Efficiency

- Massive MIMO
- Coordinated multipoint (CoMP) transmission/reception
- Beam alignment

Practice Questions (5)

1. The principle reason for power control in CDMA networks is
   a) to increase battery life
   b) to increase cell capacity
   c) to increase data rate
   d) to improve signal to noise ratio
2. Which is not true about IMT-2000:
   a) applies world wide
   b) applies to CDMA2000 as well as UMTS
   c) Specifies data rates up to 2 Mbps
   d) only supports packet switched connections
3. Which one of the following is not true in regard to HSPA:
   a) HSPA uses H-ARQ
   b) HSPA uses AMC (Adaptive Modulation and Coding)
   c) HSPA+ can use MIMO technology
   d) HSPA is based on OFDMA
4. The number of subcarriers in a LTE resource block is
   a) 7 b) 10 c)12 d) 25

Wireless Area Networks



IEEE 802.11 (Wi-Fi)(1)

- **Family of wireless local area network standards – specified protocols for data link layer & physical layer**
- **Broadly used globally for wireless broadband local access**

802.11 WLAN Technology	Ratified	Key (Physical-Layer) Attributes
802.11	1997	2.4 GHz band. Spread spectrum: DSSS, FHSS 1,2 Mbps
802.11a	1999	Operates at 5 GHz unlicensed band OFDM Up to 54 Mbps
802.11b	1999	Operates at 2.4 GHz unlicensed band Direct Sequence Spread Spectrum Up to 11 Mbps
802.11g	2003	Extends 802.11b speeds up to 54 Mbps (as in .11a) At 2.4 GHz Interoperable with .11b (device) OFDM
802.11n	2009	Next-Gen WLAN – Defined MIMO Up to 100s of Mbps – Greater Reach 2.4 & 5 GHz

IEEE 802.11 (Wi-Fi) (2)

802.11 Amendment	Ratified or estimate (e)	Description
802.11e	2005	Quality of service enhancements
802.11i	2004	Enhanced security (WPA2 Wi-Fi Protected Access)
802.11p	2010	WAVE—Wireless Access for the Vehicular Environment
802.11s	2011	Mesh Networking
802.11ac	2013	Very high throughput (VHT) for <6 GHz band
802.11ad	2012	Very high throughput (VHT) for 60 GHz band
802.11ah	2016	Sub 1 GHz License-Exempt operation
802.11ax	2018(e)	High efficiency 2.4/5 GHz
802.11az	2021(e)	Next Generation Positioning

IEEE 802.16 (WiMAX)

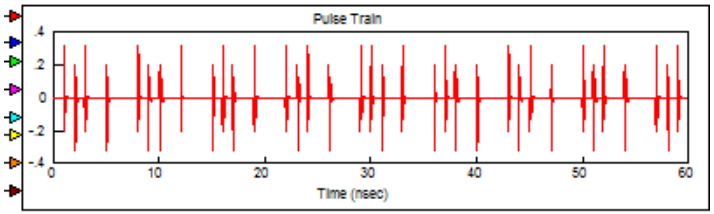
- Family of broadband Wireless Technologies based on IEEE 802.16 standards
- AS in 802.11 (WLAN), IEEE 802.16e standards focuses on the Physical & MAC layers

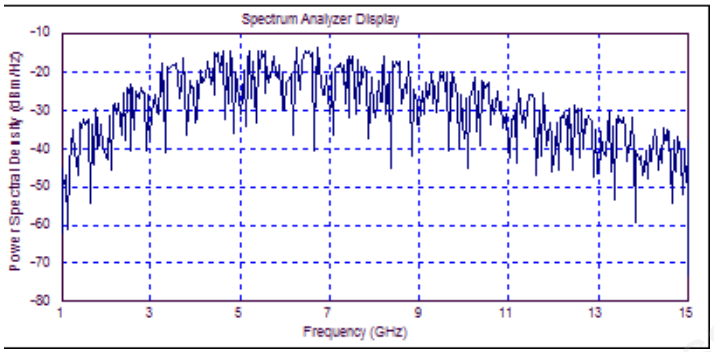
Mobile WiMAX (802.16e) Technology

- **Target peak data rate 63 Mbps downlink and 28 Mbps uplink in a 10 MHz channel**
- **Scalable OFDMA** – channel bandwidth **1.25 to 20 MHz**, up to 2048 sub-carriers
- **Adaptive modulation and coding** based on channel conditions – similar to HSPA & cdma2000
  - **BPSK, QPSK, 16QAM**, **64 QAM**
- **MIMO** antenna technology & Adaptive Antenna Systems
- Advanced re-transmits (**H-ARQ**) & error correction
- **Advanced QoS for various service flows**
- **Mobility Management & Scheduling**

Other Wireless Access Technologies

UWB - Ultra Wideband





- Wireless Personal Area Network (**WPAN**) – Up to several meters
- **NFC & RFID** – Within centimetres

IEEE 802.15 WPAN Task Group	Scope
802.15.1	WPAN / Bluetooth
802.15.2	Co-existence
802.15.3	High-Rate WPAN
802.15.4	Low-Rate WPAN
802.15.5	Mesh Networking
802.15.6 802.15.7	Body Area Networks (BAN) Visible Light Communication

Bluetooth

- Frequency Hopping Spread Spectrum
- 2.4 GHz band: 1, 3 Mbps raw
- Ad hoc in piconets
- Ver 4 : Smart/Smart ready
  - classic
  - high speed (24 Mbps, 802.11)
  - low energy (BLE)
- Bluetooth 5

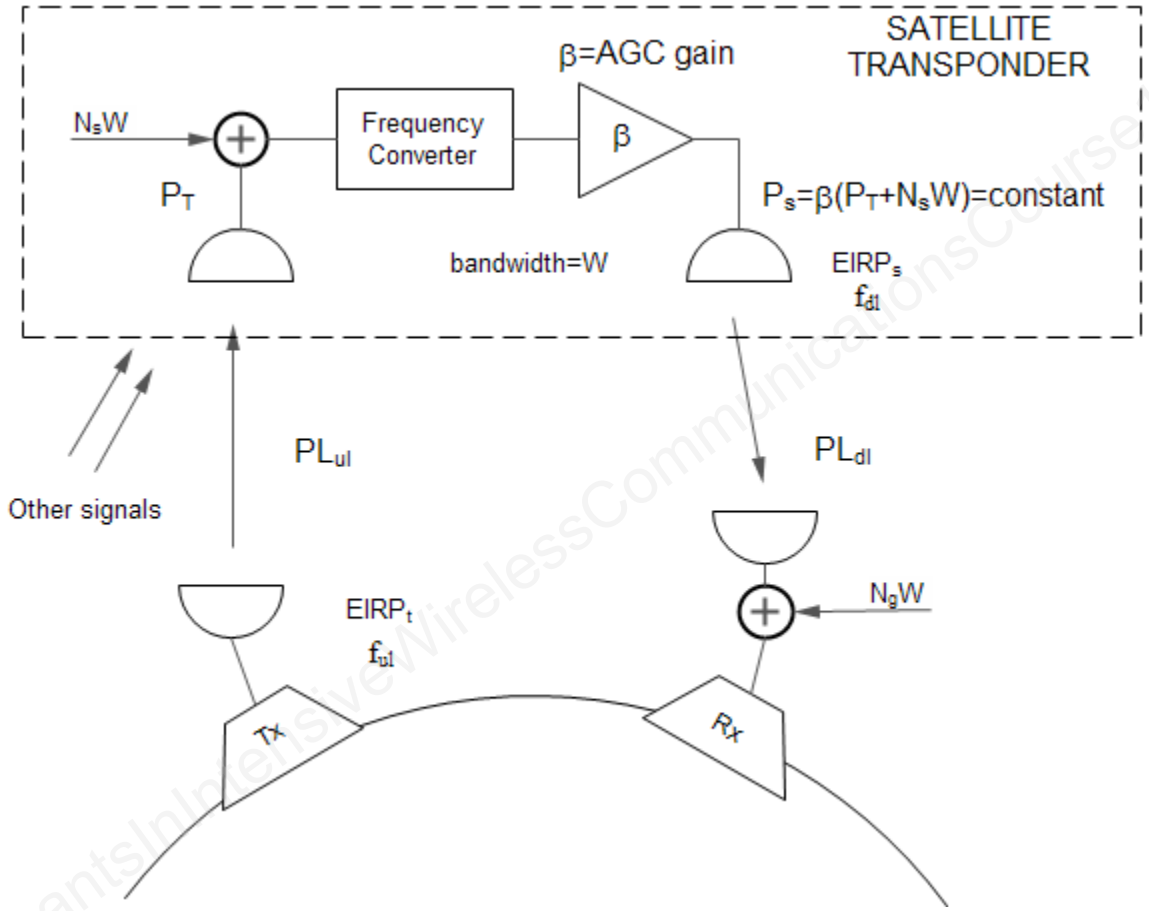
ZigBee

- Home automation, industrial control, WSN
- IEEE 802.15.4
- Direct Sequence Spread Spectrum
- 2.4GHz, 915MHz, 868MHz
- 250kbps, 40kbps, 20kbps

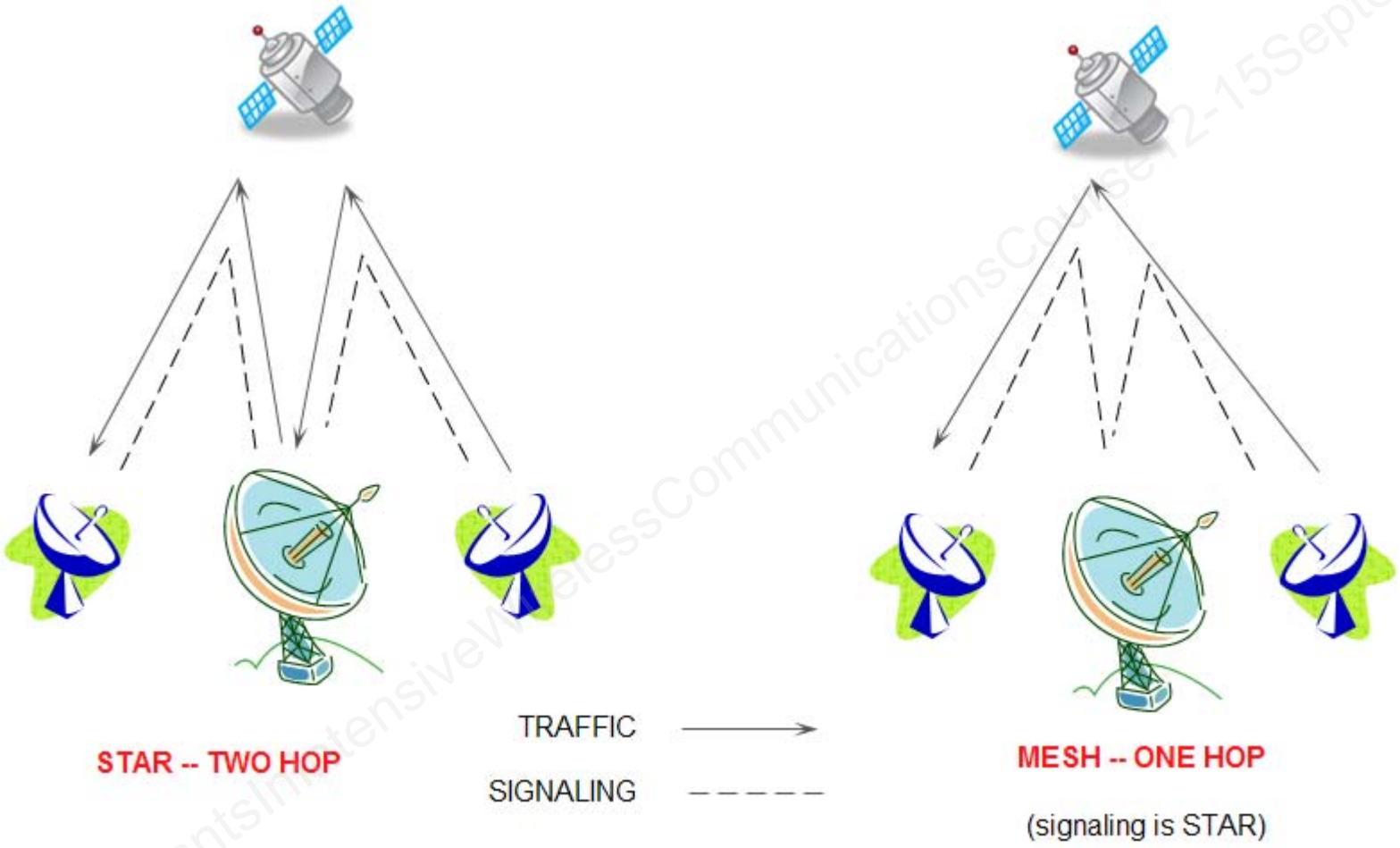
Satellite Communications

- Orbit
  - Low Earth Orbit (LEO): 200-1400 km
  - Medium Earth Orbit (MEO): 8000-18000 km
  - Geostationary Earth Orbit (GEO): 35,800 km
  - Highly elliptical
- Services
  - Fixed service satellite (FSS)
  - Broadcast Service Satellite (BSS)
  - Mobile Service Satellite (MBS)
- Characteristics
  - Large path loss – affected by precipitation and atmosphere
  - High latency
  - Bandwidth limited
  - Initial deployment very costly
- Technology
  - Regenerative repeater
  - Nonregenerative repeater
  - Multiple access techniques

Nonregenerative Repeater



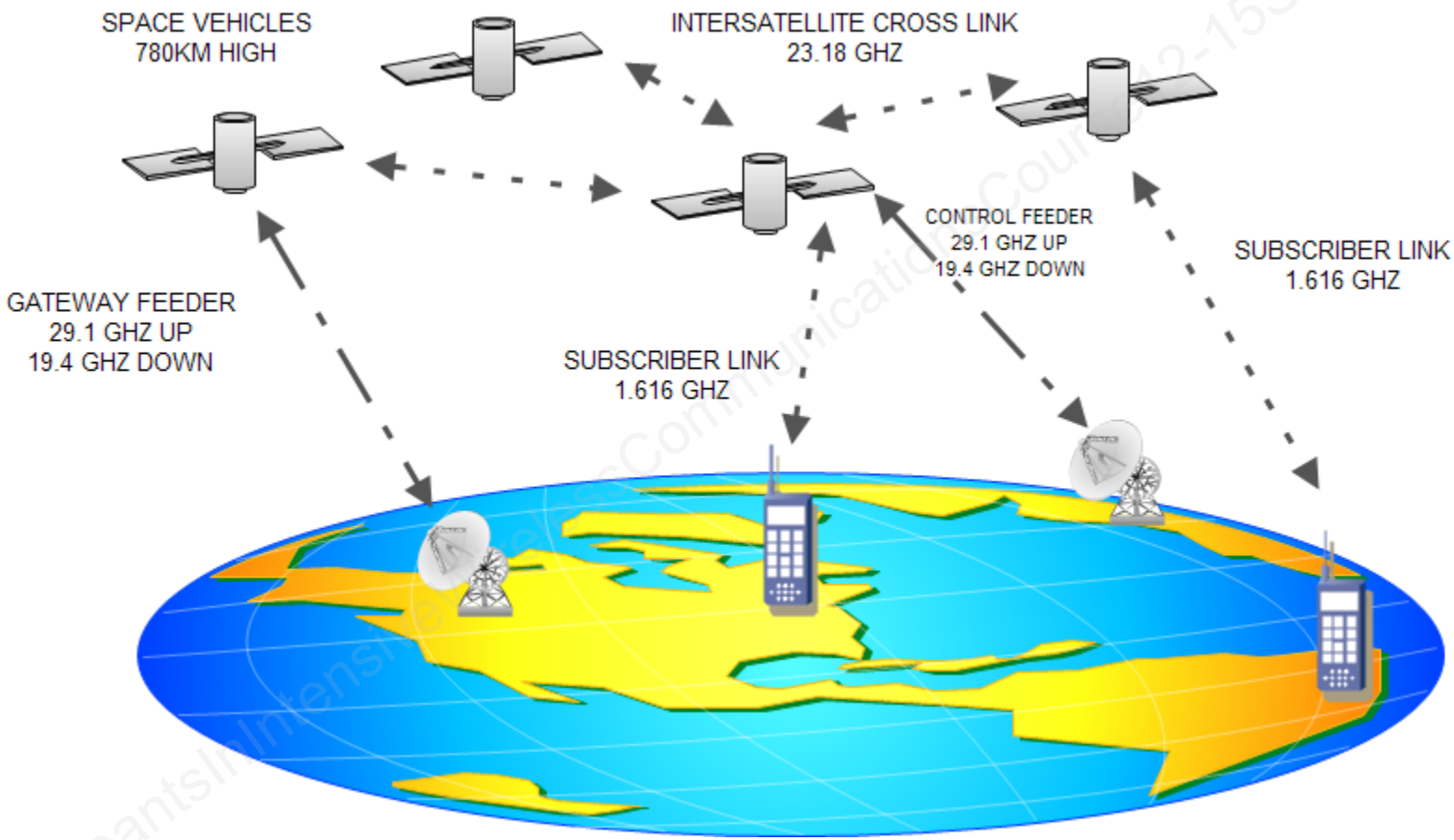
VSAT



Iridium Characteristics

Parameter	Description
Orbit	LEO: h=780 km, 86.4 deg inclination
Use	voice and data
Constellation size	66 active satellites, 6 planes
Relative velocity	26.8 km/hr
User frequency band	1616 -1626.5 MHz, L band
Gateway to satellite	29.1 – 29.3 GHz
Satellite to gateway	19.4 – 19.6 GHz
Inter-satellite link	23.18 – 23.38 GHz
Satellite view time	7 – 10 minutes
Access scheme	Hybrid FDMA/TDMA

Iridium Mesh Network



Frequency Band Designations

IEEE Letter Bands	Ranges in GHz	Satellite Services
L	1 – 2	MSS
S	2 – 4	MSS
C	4 – 8	FSS
X	8 – 12	FSS
Ku	12 – 18	FSS, BSS (DBS)
K	18 – 27	FSS, BSS
Ka	27 – 40	FSS
V	40 – 75	---
U	75 – 110	---

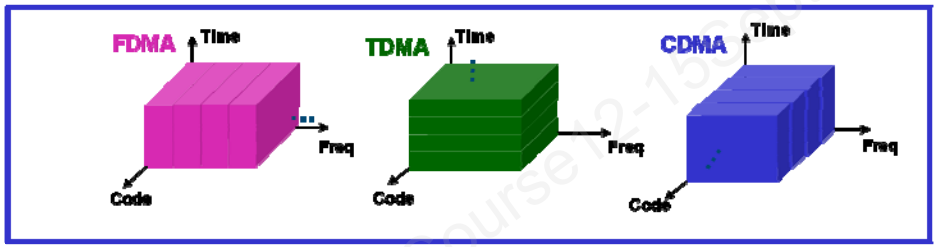
MSS Mobile Service Satellite
FSS Fixed Service Satellite
BSS Broadcast Service Satellite
DBS Direct Broadcast Service

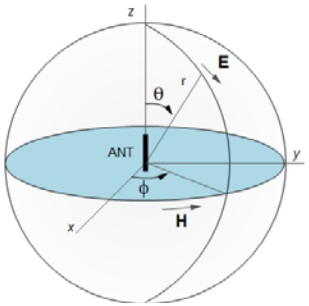
Future Trends

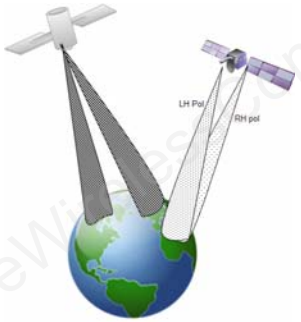
- Additional bands for mobile broadband
  - auctions for broadcast TV spectrum 572-698 MHz
  - more bandwidth for 4G/IMT-Advanced
  - public safety broadband
- Cognitive radio
  - Super Wi-Fi
  - Wireless regional area network—IEEE 802.22
  - use of unlicensed white spaces 54 – 862 MHz
- IEEE 802.11ac
  - high rate Wi-Fi
- UWB
- Metamaterial antennas
- 5G Mobile Networks

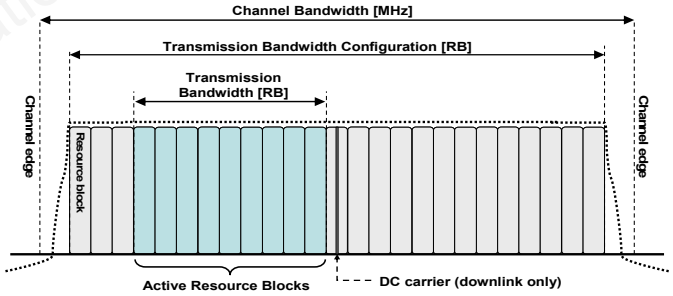
Summary of Part 1

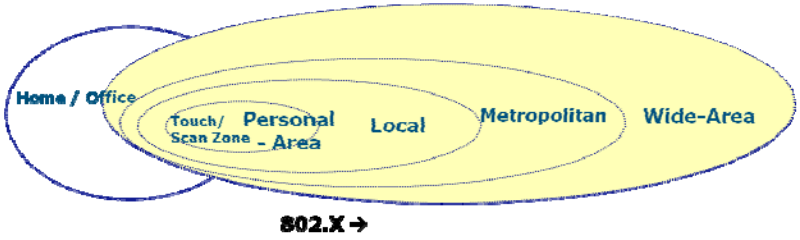
- Antennas
- Propagation
- Radio Receiver
- Multiple Access
- Cellular Networks
- Other Wireless Networks and Technology
- Satellite Communication

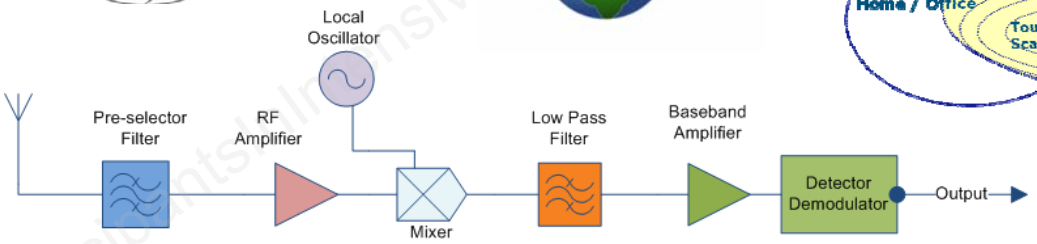












Principle Sources

- Bensky, A., *Short-range Wireless Communications 2nd Ed.*, Elsevier, 2004
- Rappaport, T. S., *Wireless Communications Principles and Practice, 2nd Ed.*, Prentice Hall PTR, 2002
- Sesia, S., Toufik, I., and Baker, M., *LTE--The UMTS Long Term Evolution*, Wiley, 2009
- Sklar, B., *Digital Communications Fundamentals and Applications, 2nd Ed.*, Prentice Hall PTR, 2001
- Stutzman, W. L. and Thiele, G. A., *Antenna Theory and Design, 2nd Ed.*, Wiley, 1998

Part 2 Highlights

- Network Architecture
  - Protocol layers
  - IP Addressing
  - Packet Routing
- Mobility in Cellular Networks
- Traffic Analysis
- Evolution of Cellular Core Networks through LTE
- IP Multimedia Subsystem and Open Service Access
- Network Management and Security
- Facilities Infrastructure
- Agreements, Standards, Policies, Regulations

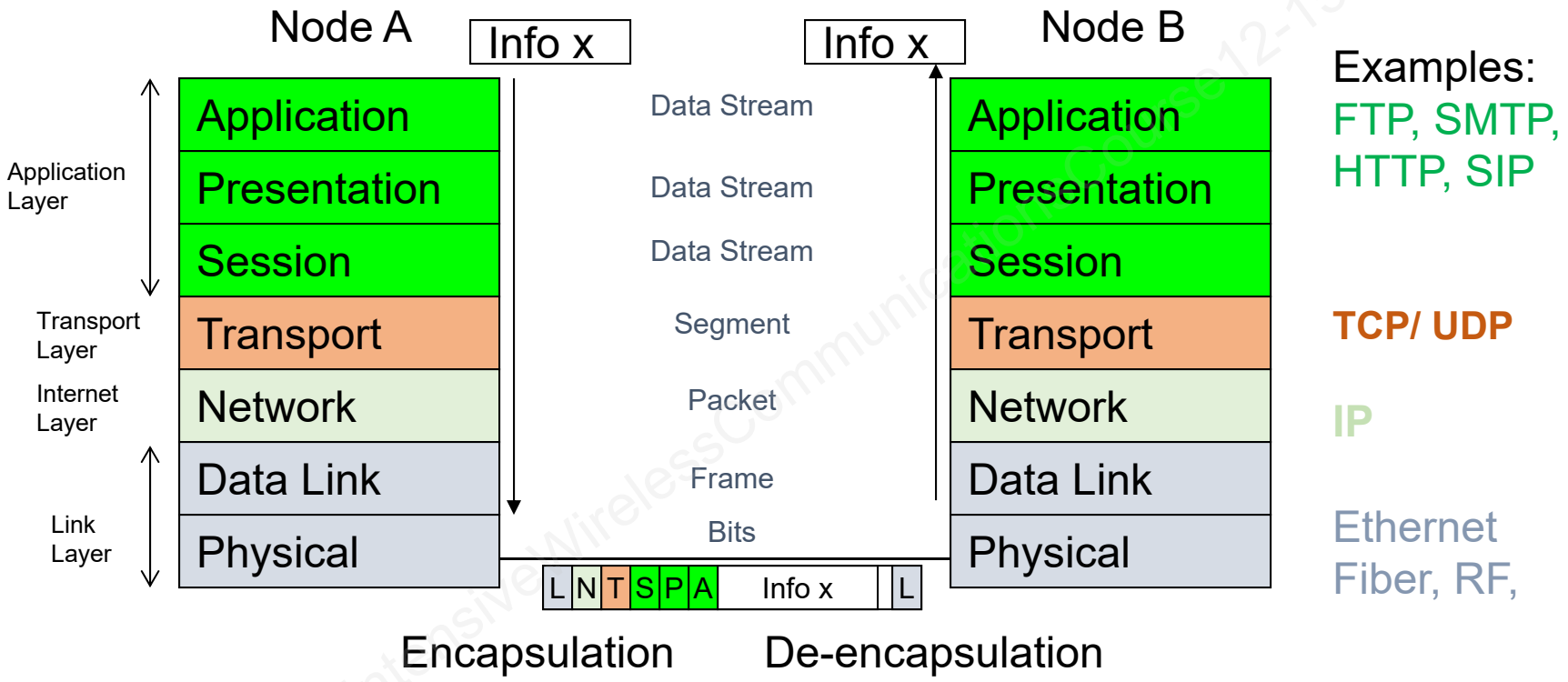
Network and Service Architectures

- *IP Fundamentals*
- *Cellular Architectures*
- *All IP Core Network*
- *Service and Alternative Architectures*
- *Location and Positioning Techniques*

IP Fundamentals

- Features
  - Can be used over many link technologies
  - Packet-switching
- Downside characteristics
  - Best-effort only
  - Hierarchical addressing/routing does not immediately support mobility

Protocol Layering: OSI and TCP/IP



The TCP/IP 4 layer reference model bundles the 3 upper layers into one layer called Application Layer and the two lower layers into the Link Layer.

IPv4 Addressing

- 32 bits
- Dotted Decimal Notation

01010100 01110101 ------

84.229.36.103

NetID HostID

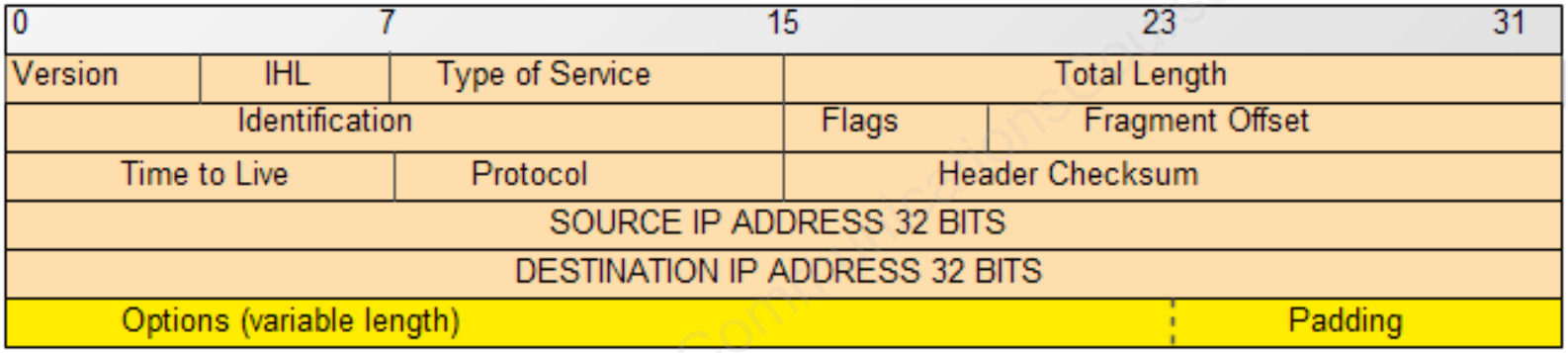
84.229.36.103/16

255.255.0.0 Mask

Classes (obsolete)
A: 8 NetID bits 0---
B: 16 NetID bits 10--
C: 24 NetID bits 110-
D multicast, E reserved
Classless addressing

•Dynamic Host Configuration Protocol (DHCP): host gets dynamic IP address
•Address Resolution Protocol (ARP) maps IP address to physical (MAC) address
•Network Address Translation (NAT)

IPv4 Header

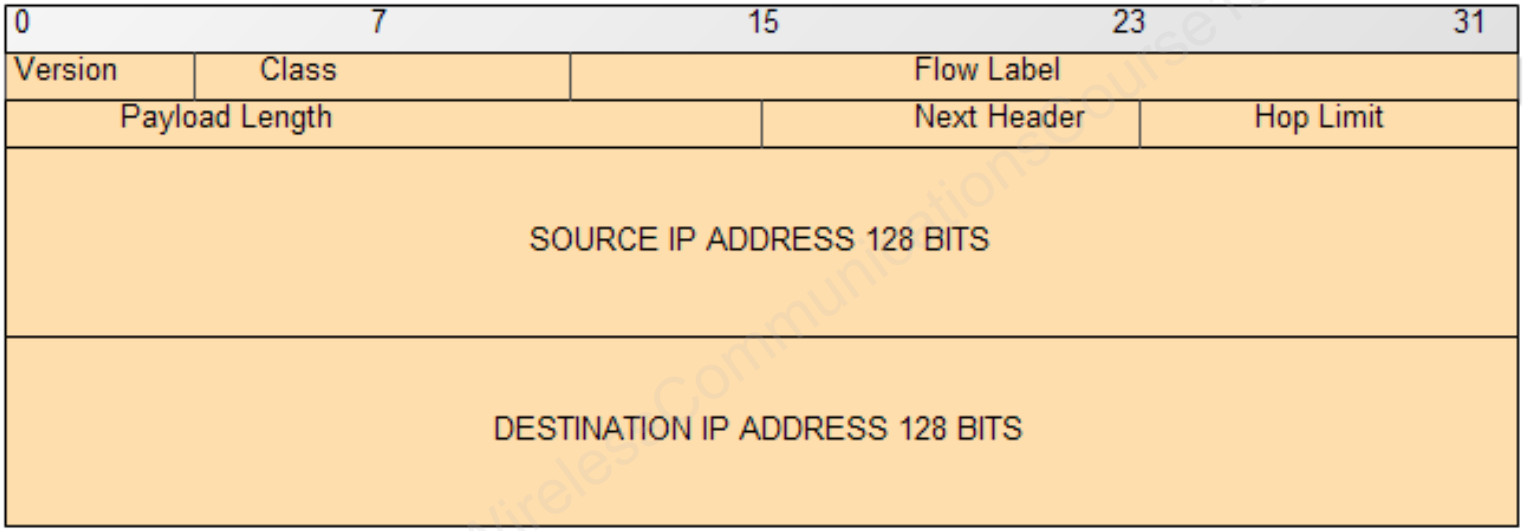


Total IPv4 Header Length (without options) = 20 Bytes

IPv6

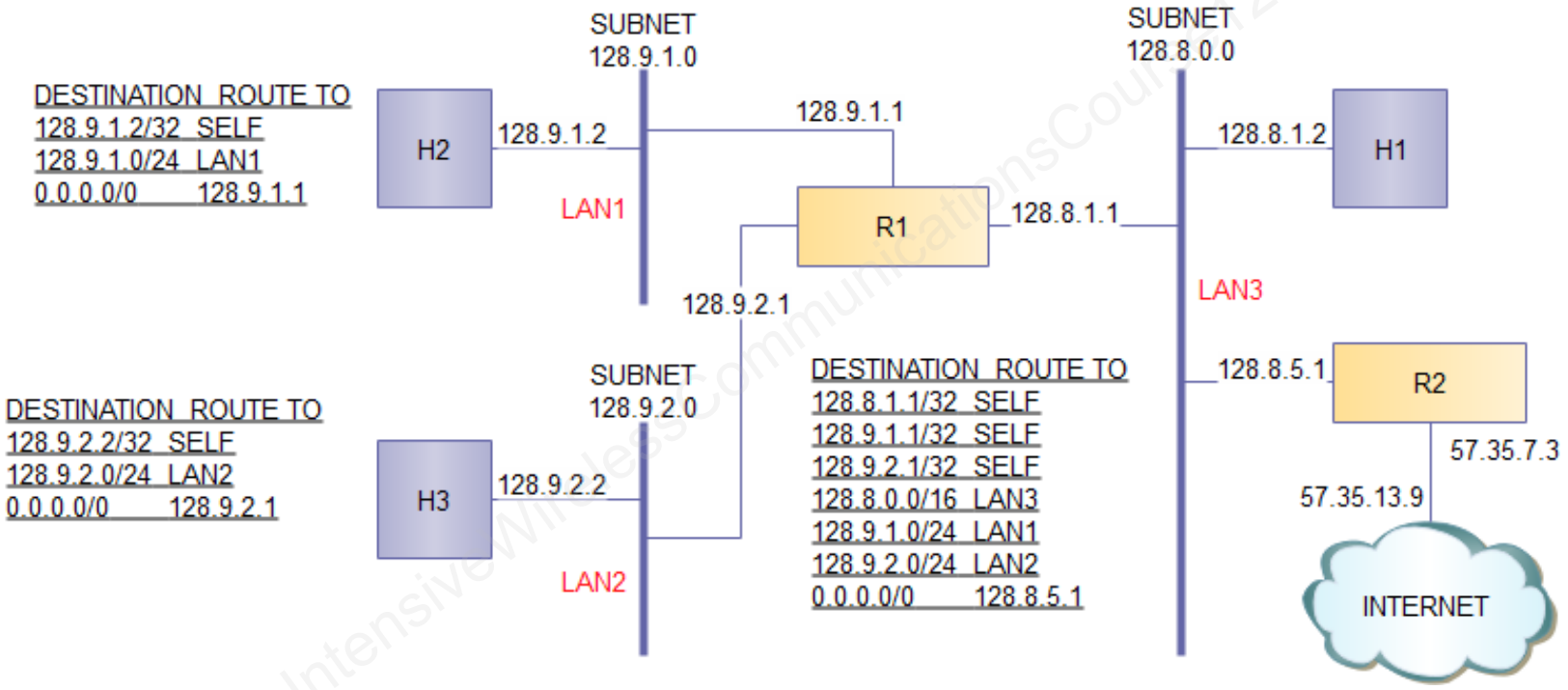
- 128-bit address space (32-bit in IPv4)
  - fe80::249b:19a9:f5ff:fffd/128
- Network auto-configuration
- Enhanced security support
- Enhanced QoS support
- Enhanced Mobility support
- Revamped IP header
  - More efficient IP header processing
    - New header extensions design

IPv6 Header



Total IPv6 Header Length = 40 Bytes

IP Routing

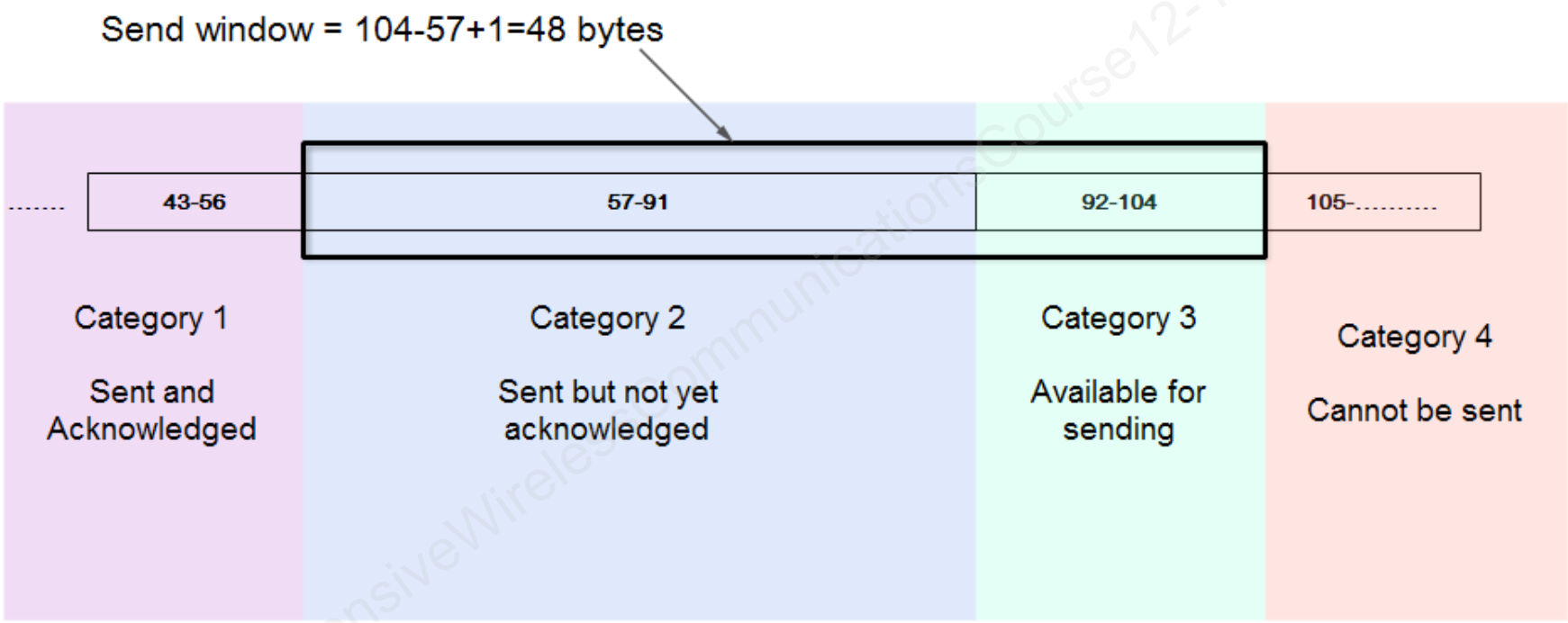


IP Upper Layers: TCP vs. UDP

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Features		TCP	UDP
Reliability		Yes ACK, retransmissions	No
Ordering		Sequence number	None
Timeliness	Guaranteed Delay	No	No
	Jitter Control	No	No
Integrity		Checksum	Checksum (optional)
Efficiency		Low efficiency	More efficient: less processing, stateless

TCP Sliding Window



TCP Over Wireless: Issues

- Wireless links
  - Lost packets
  - Delays
  - Result in poor throughput
- TCP congestion control mechanisms
  - Lost packets, delays, interpreted as congestion
  - Reduce data rate in response
- Various solutions
  - Split TCP, etc.

ICMP (Internet error and Control Messages Protocol)

Error Messages

- Destination unreachable
- Time exceeded
- Invalid Parameters
- Source quench
- Redirect

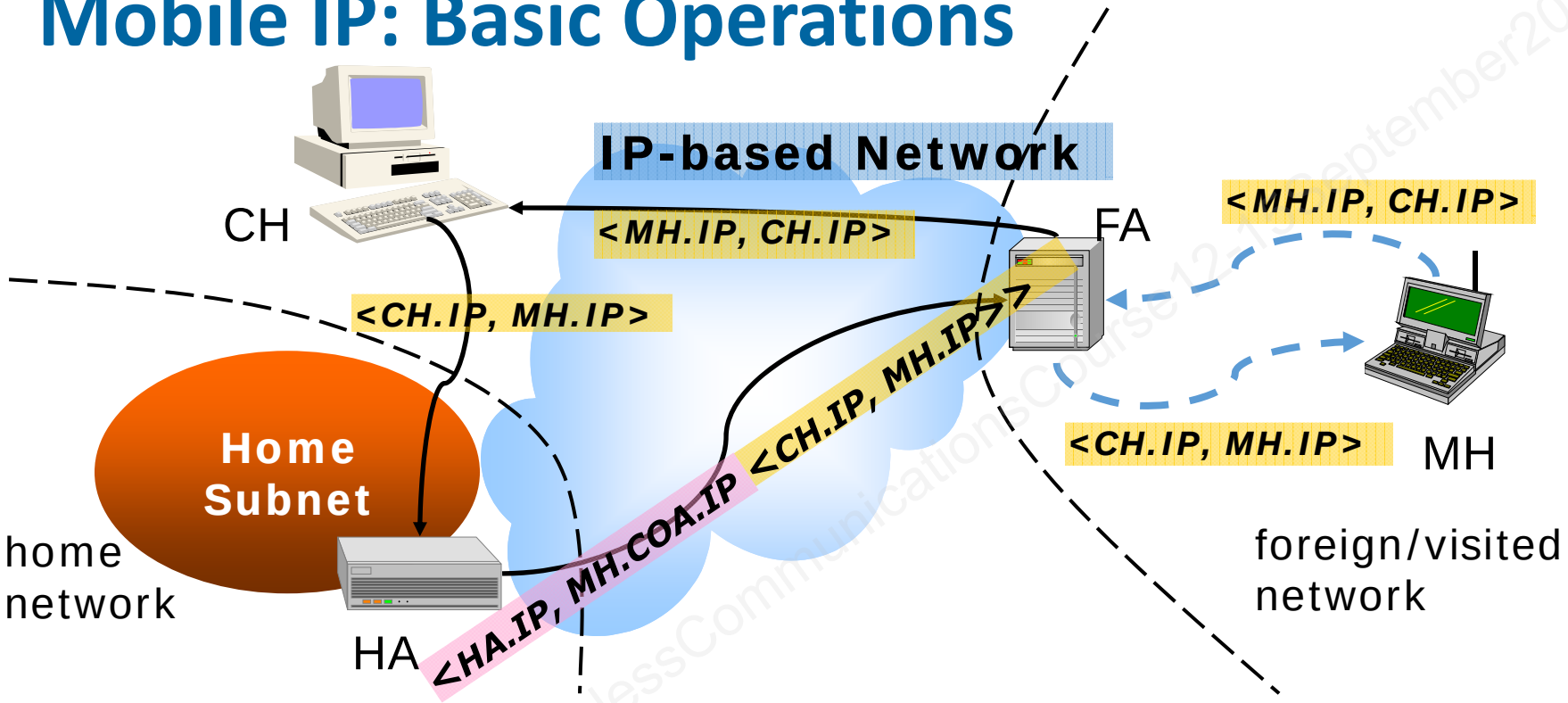
Query messages

- Echo request and reply messages
- Time-stamp request and reply messages
- Subnet mask request and reply messages

Mobile IP

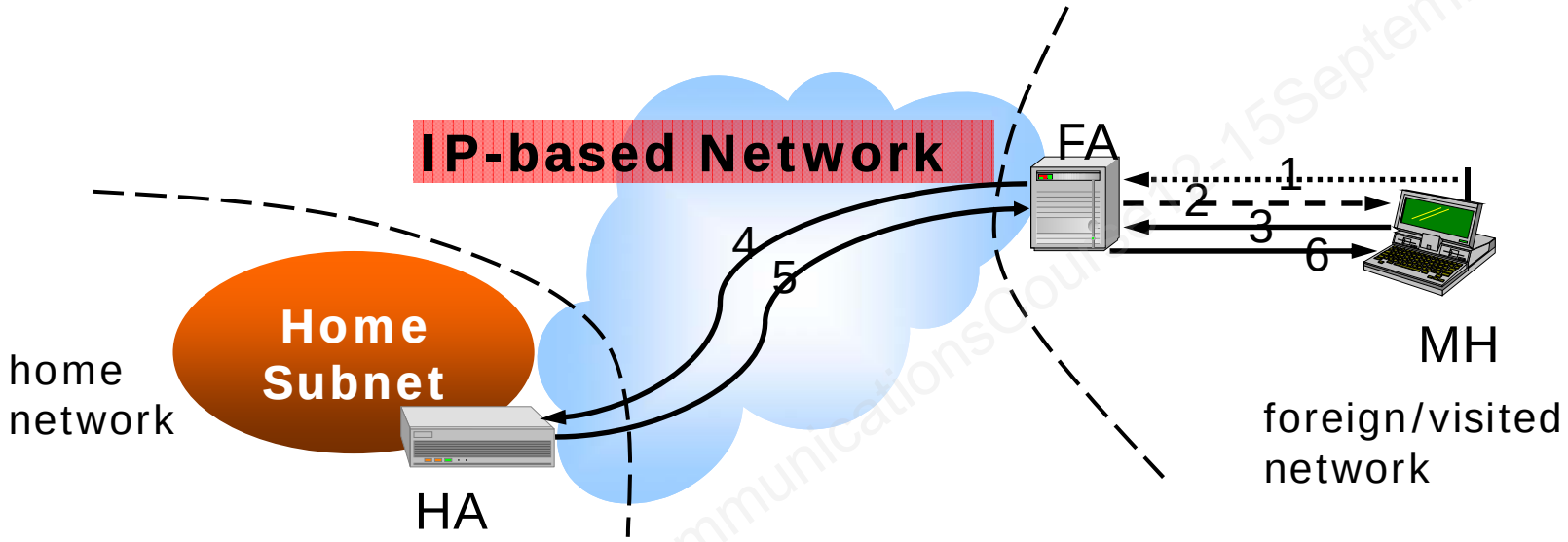
- IP originally designed without mobility support in mind
  - Hierarchical routing assumes geographically static addresses
- Mobile IP
  - One IP address for identity, one for location
  - “home agent” to forward packets from old location to new
- Operations: advertisement, registration, tunneling

Mobile IP: Basic Operations



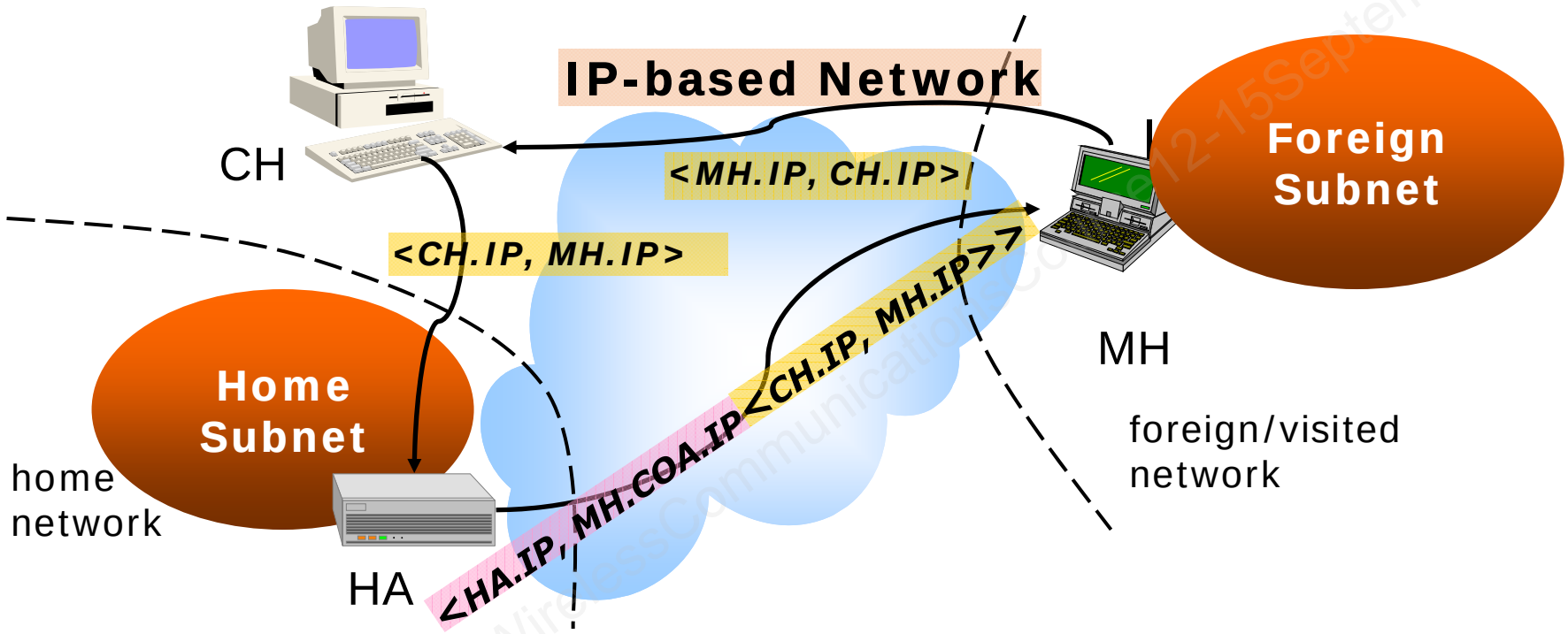
- CH to MH
  - CH sends packet to MH home address as usual
  - HA in home subnet intercepts packet, tunnels it to FA
  - FA un-encapsulates packet, forwards to MH
- MH to CH
  - Normal IP routing from foreign network

Mobile IP: Registration



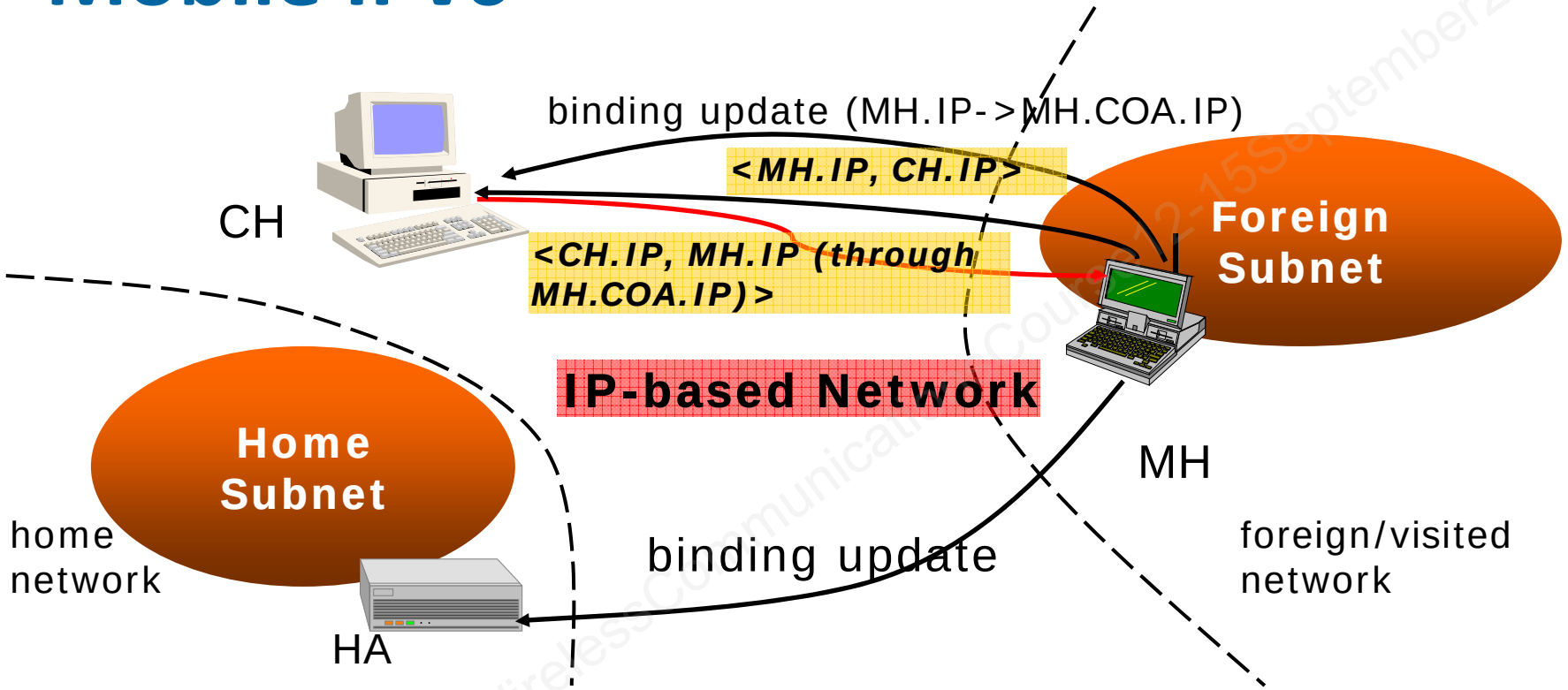
1. (optional) agent solicitation
2. Agent advertisement
3. MIP registration request
4. MIP registration request
5. MIP registration reply
6. MIP registration reply

Mobile IP: co-located COA



- CH to MH
  - CH sends packet to MH home address as usual
  - HA in home subnet intercepts packet, tunnels it to COA of MH
  - MH un-encapsulates packet, processes it
- MH to CH
  - Normal IP routing from foreign network

Mobile IPv6

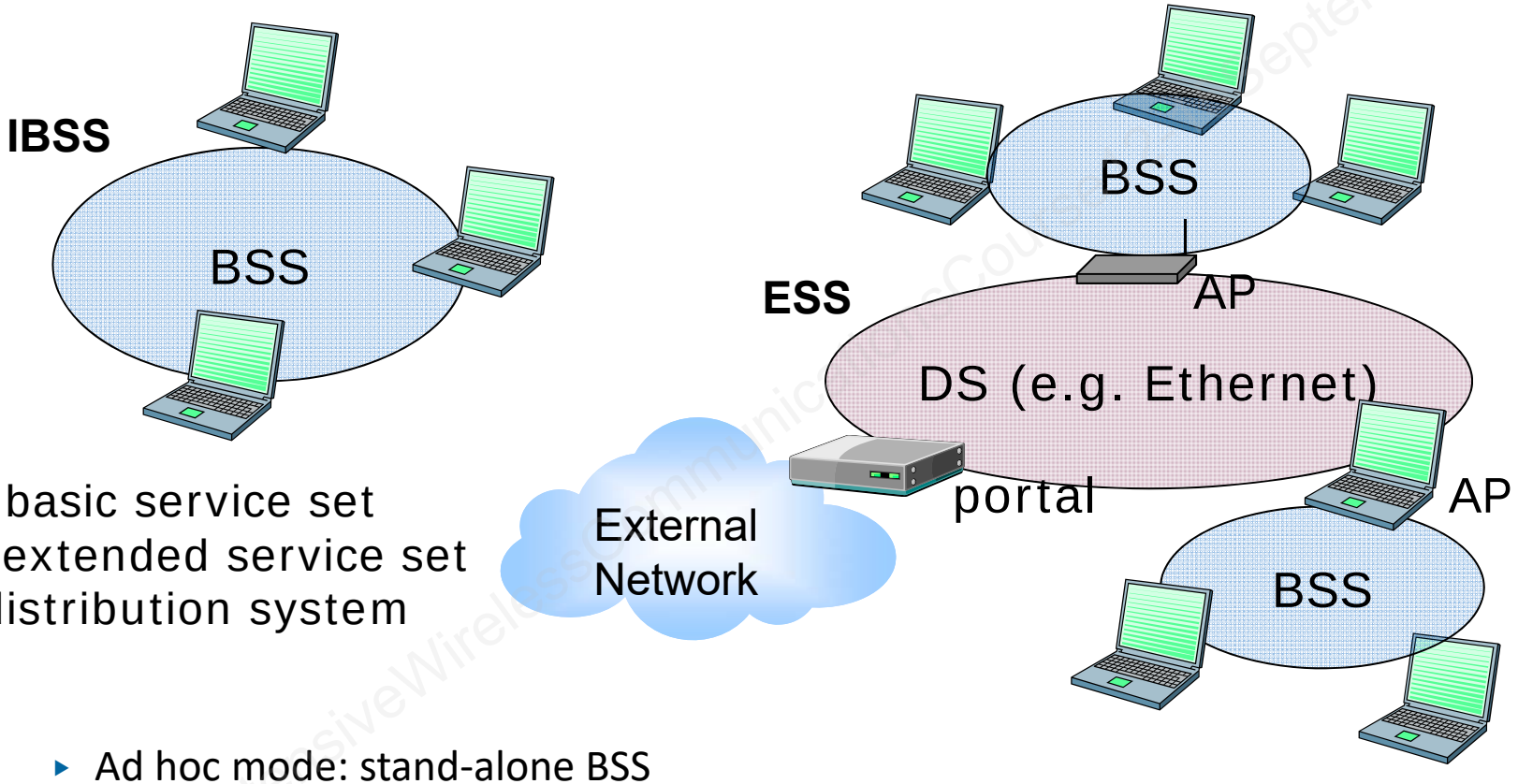


- Address auto-configuration is inherent in IPv6
- No FA, no triangular routing
- Use of source routing through MH.COA.IP, avoids/reduces encapsulation overhead
  - But if any packets go through HA, would still be tunneled to MH
- Binding update can be piggybacked on data packets

Practice Questions (1)

1. The protocol layer responsible for routing datagrams is
   a) internet layer
   b) transport layer
   c) link layer
   d) any layer may perform routing
2. Which characteristic does not apply to UDP?
   a) Connectionless
   b) Delivery not guaranteed
   c) Commonly used for video streaming
   d) Does packet sequencing and reordering
3. The number of bits in an IPv6 address is
   a) 32
   b) 64
   c) 128
   d) 256
4. True or False: A foreign agent is essential for both IPv4 and IPv6 in order to give a roaming host a Care-of-Address.

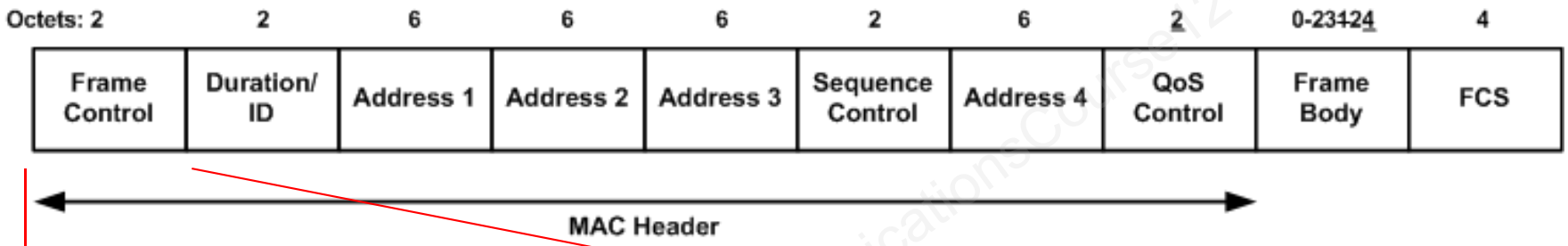
802.11 Network Architecture Basics



- BSS: basic service set
- ESS: extended service set
- DS: distribution system

- Ad hoc mode: stand-alone BSS
- Infrastructure mode: multiple BSS's can be linked by a DS into an ESS; looks like one big LAN – one IP subnet

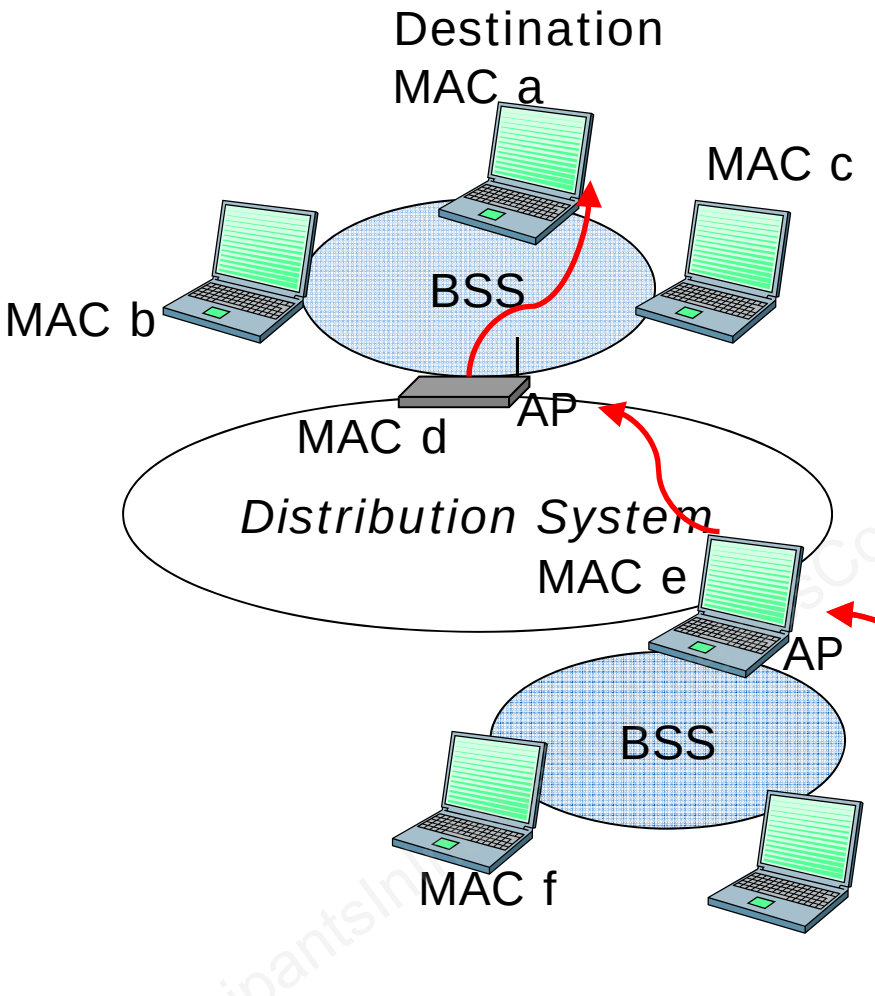
802.11 General Frame Format



Control Field

B0	B1	B2	B3	B4	B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version		Type		Subtype		To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	Protected Frame	Order
Bits : 2		2		4		1	1	1	1	1	1	1	1

802.11: Up to 4 MAC Addresses



To DS	From DS	Addr1	Addr2	Addr3	Addr4
0	1	MAC a	MAC d	MAC g	N/A

To DS	From DS				
1	1	MAC d	MAC e	MAC a	MAC g

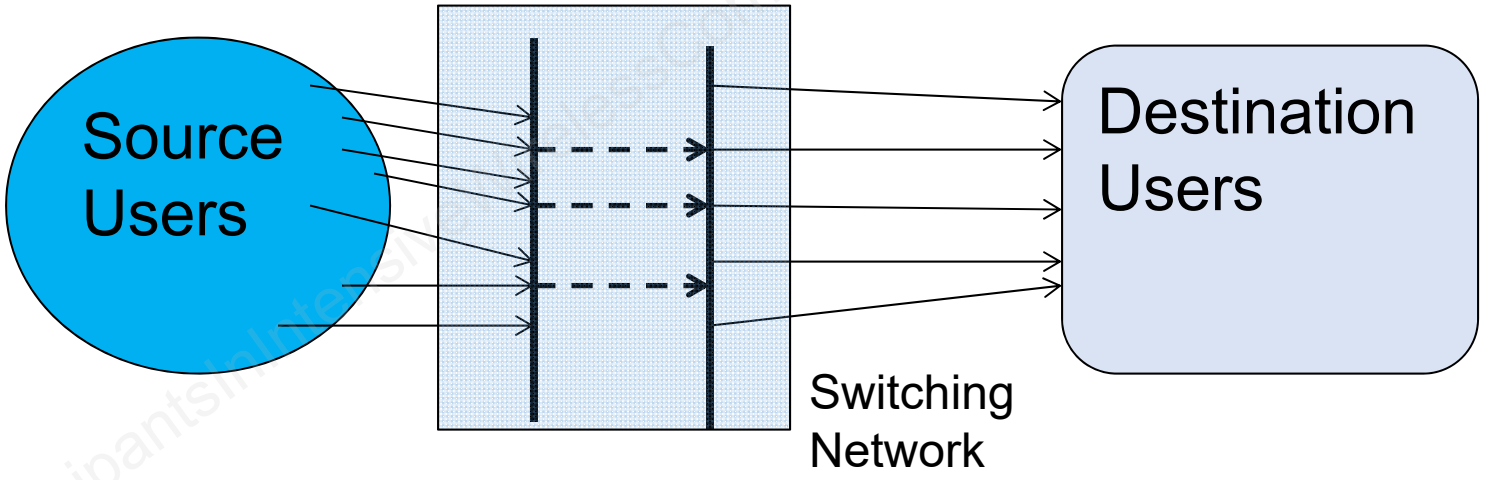
To DS	From DS				
1	0	MAC e	MAC g	MAC a	N/A

WLAN vs. Cellular

- Unlicensed bands (WLAN) vs. licensed (Cellular)
- Range
- Scope
  - Cellular: whole network
  - 802.11: just link and MAC, access (physical) network

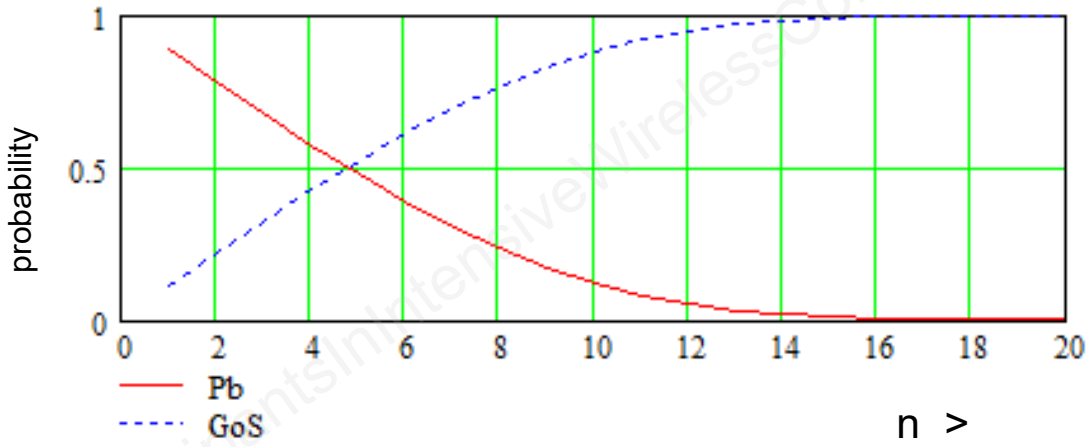
Teletraffic Analysis: Introduction

- Definition
- Traffic intensity/Load in units of Erlang
- Blocked Call
- Holding Time
- Quality of Service (QoS)/Grade of Service (GOS)



Traffic Analysis: Erlang B

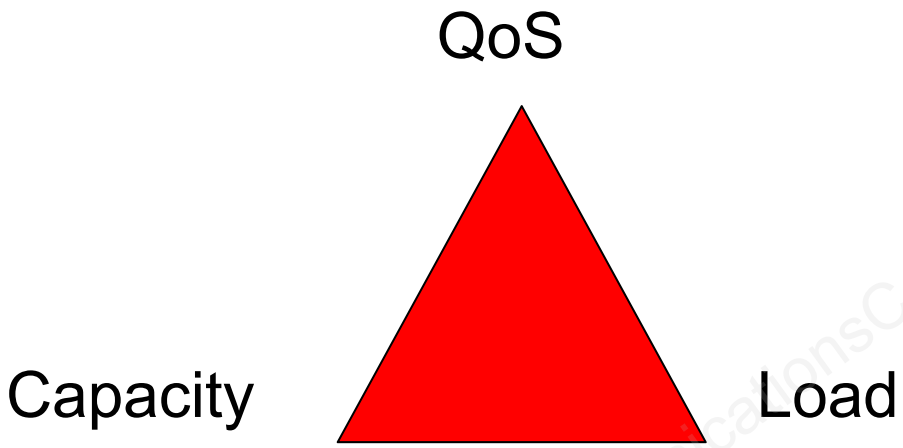
- Capacity: *n*=total number of channels
- call arrival rate=λ, calls/unit time
- mean holding time=*h*
- Traffic load: *a*=offered traffic intensity=λh, *erlangs (erl)*
- Calls arrive according to Poisson process
- Holding times are independently and identically distributed.
- P_b=blocking probability (GoS=1-P_b)

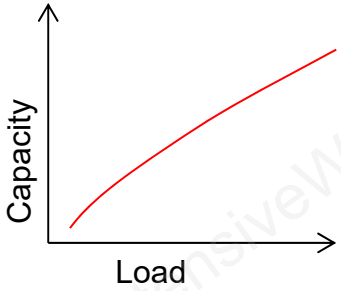


a=8

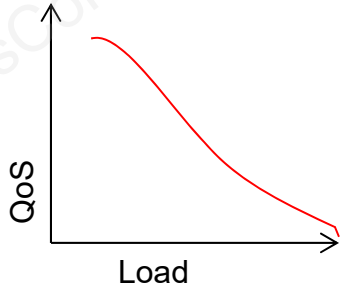
$$P_b = \frac{\frac{a^n}{n!}}{\sum_{i=0}^{n} \frac{a^i}{i!}}$$

Teletraffic Tradeoffs

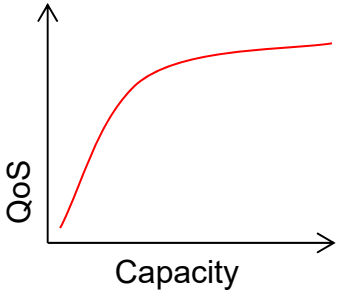




Given QoS



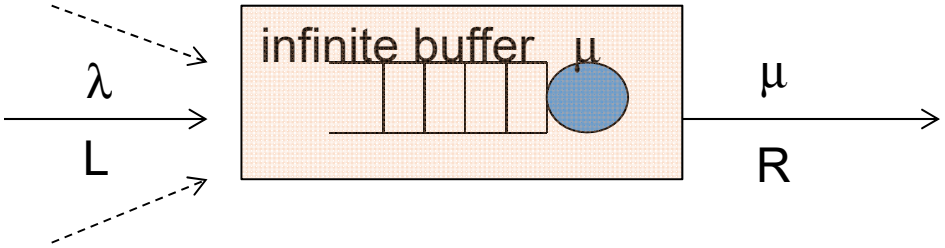
Given Capacity



Given Load

QoS=*1-P*$_b$

Traffic Analysis: packet switching



λ=average packet arrival rate, packets/s
L=av. packet length, bits
R=link speed b/s (capacity)
μ=service rate, packets/s
ρ=traffic load

$$P_z = \frac{\lambda L}{R} e^{-\left(\frac{R}{L}-\lambda\right)z} = \rho \cdot e^{-\mu(1-\rho)z}, \text{ if } \rho < 1$$

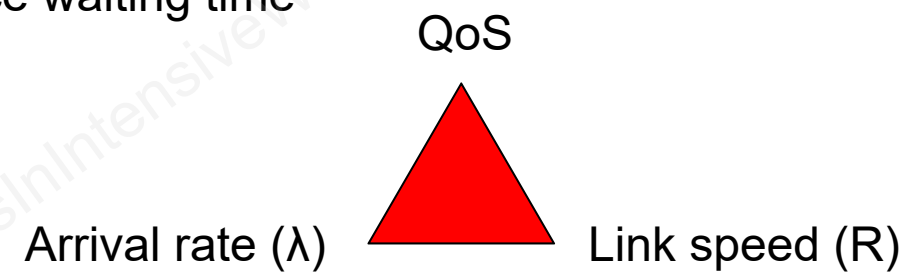
$$\rho = \frac{\lambda}{\mu} \qquad \mu = R/L$$

$$P_z = 1, \text{if } \rho \geq 1 \text{ (unstable)}$$

P_z= probability (packet delay > time *z*)

z=reference waiting time

$$P_z \uparrow \Rightarrow QoS \downarrow$$



Traffic Analysis: wireless

- Dropped calls and handoffs
- Dropping probability
- Reserved channels for handoffs
- Channel borrowing
- Modeling wireless systems

Cellular Network Architectures

- Functional requirements
  - Voice services
  - Data services
- Network elements and functions
- Network protocols
- Examples of signaling for call delivery, roaming, etc.
- Packet data services in 2.5 G and higher cellular systems

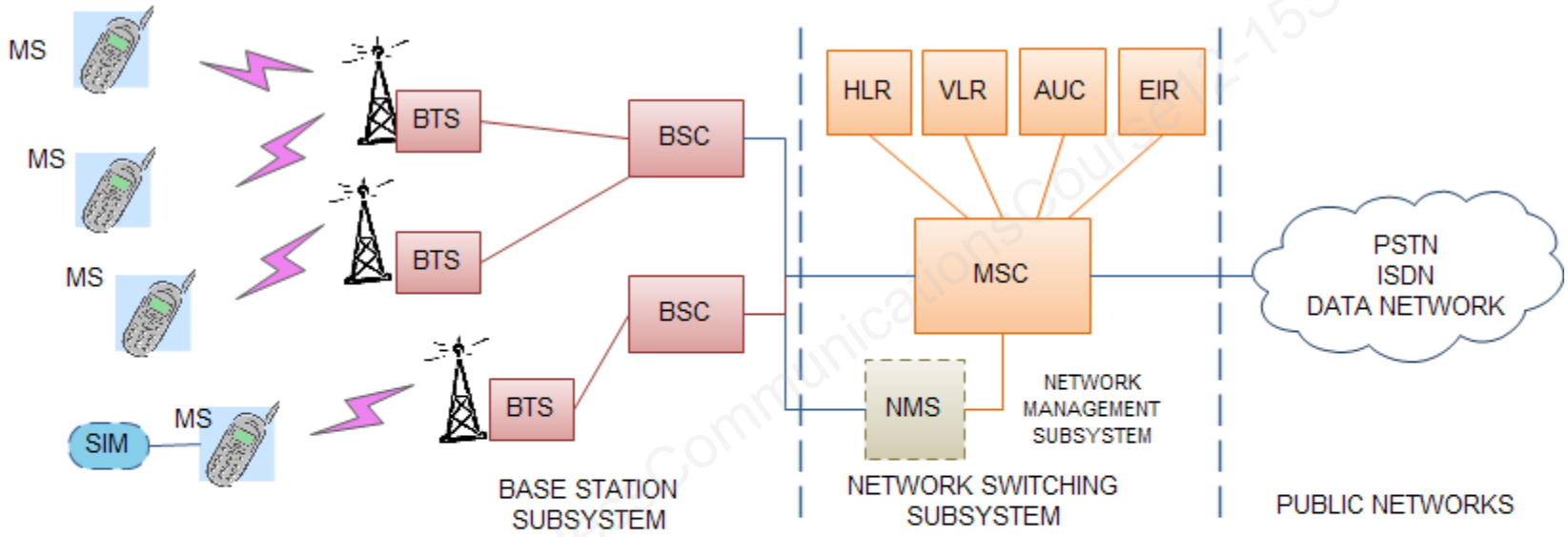
Original GSM Services

- Teleservices
  - Speech (telephony and emergency calls)
  - SMS (Point-to-Point and Cell Broadcast)
  - Facsimile
- Bearer Services
  - 13 kb/s bearer for voice
  - Unrestricted digital information (UDI) at rates up to 9,600 bps
- Supplementary Services
  - e.g. Calling Line Identification Presentation, various Call Forwarding, Call Waiting, Advice of Charging, barring of various incoming or outgoing calls

Cellular Network Functional Requirements for Voice

- The goal is to support:
  - Call initiation (out-going calls)
  - Call delivery (in-coming calls)
  - Handoffs/handovers (between base stations)
  - Roaming
  - Privacy, security for authorized users
  - Good coverage, low drop rates, low blocking

GSM Architecture



MS Mobile Station
BTS Base Transceiver Station
BSC Base Station Controller
MSC Mobile Switching Center
SIM Subscriber Identity Module

HLR Home Location Register
VLR Visitor Location Register
AUC Authentication Center
EIR Equipment Identity Register

PSTN Public Switched Telephone Network
ISDN Integrated Services Digital Network

Text Messaging

- SMS (short message service)
  - Hugely popular
  - Up to 160 characters per message
  - Estimated 80 billion-dollar industry
  - SMS-PP (point-to-point) and SMS-CB (cell broadcast)
- SMSC (Short Message Service Center)
  - Handles messages
  - Queues messages for retry

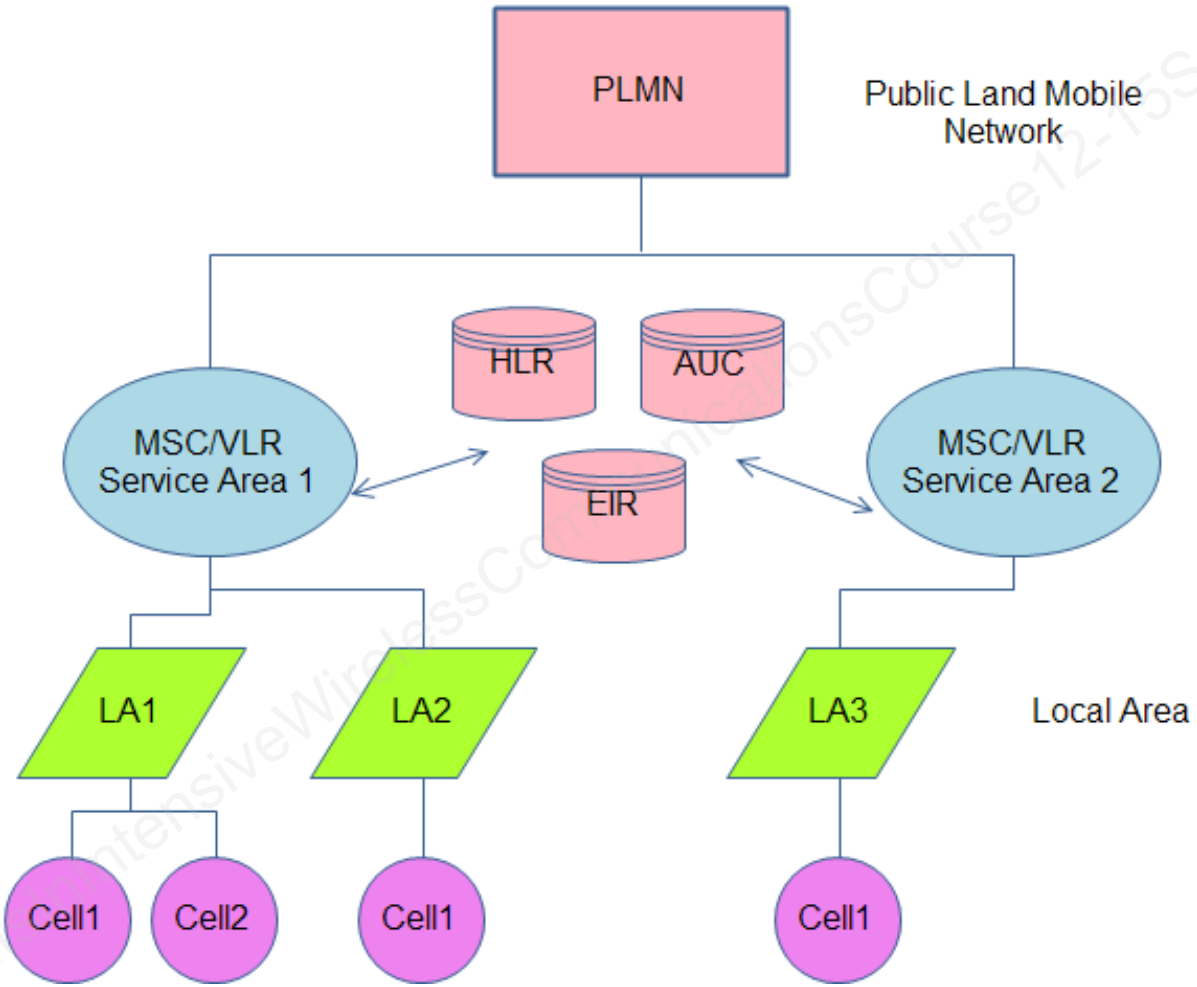
Roaming

- Roaming
  - Service through other networks with different location area and/or area numbering code
- Assuming
  - roaming agreement in place
  - air interface is compatible
- Need
  - Some user profile information
    - For authentication, authorization, etc.
- Additional requirements for incoming call delivery

Roaming: Location Area & Paging Concepts

- To support roaming call delivery
- The challenge
  - Keeping track of mobile equipment
  - Waste of resources while idle?
- The tradeoff
  - Location areas
- Paging

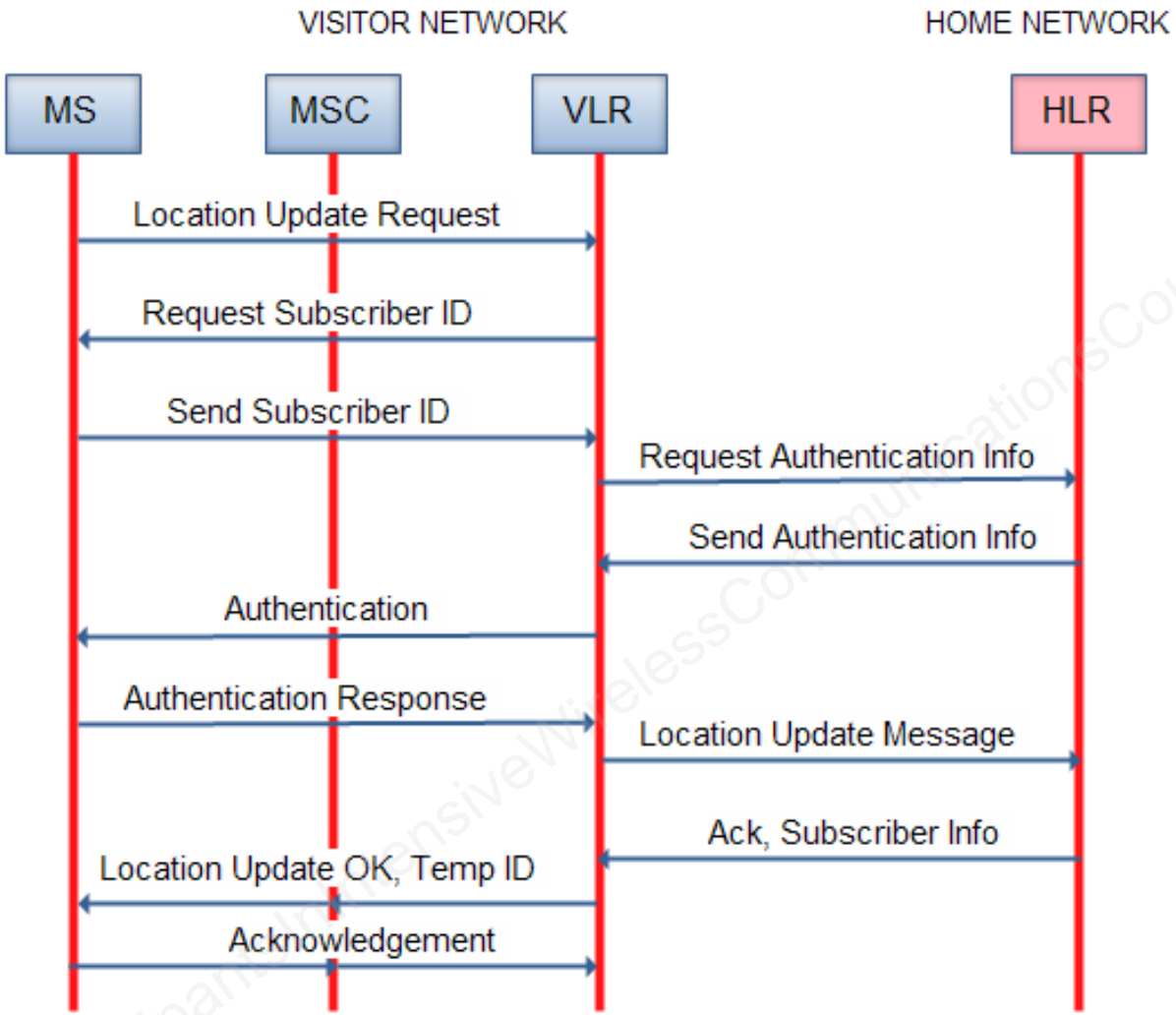
GSM Location Area Hierarchy



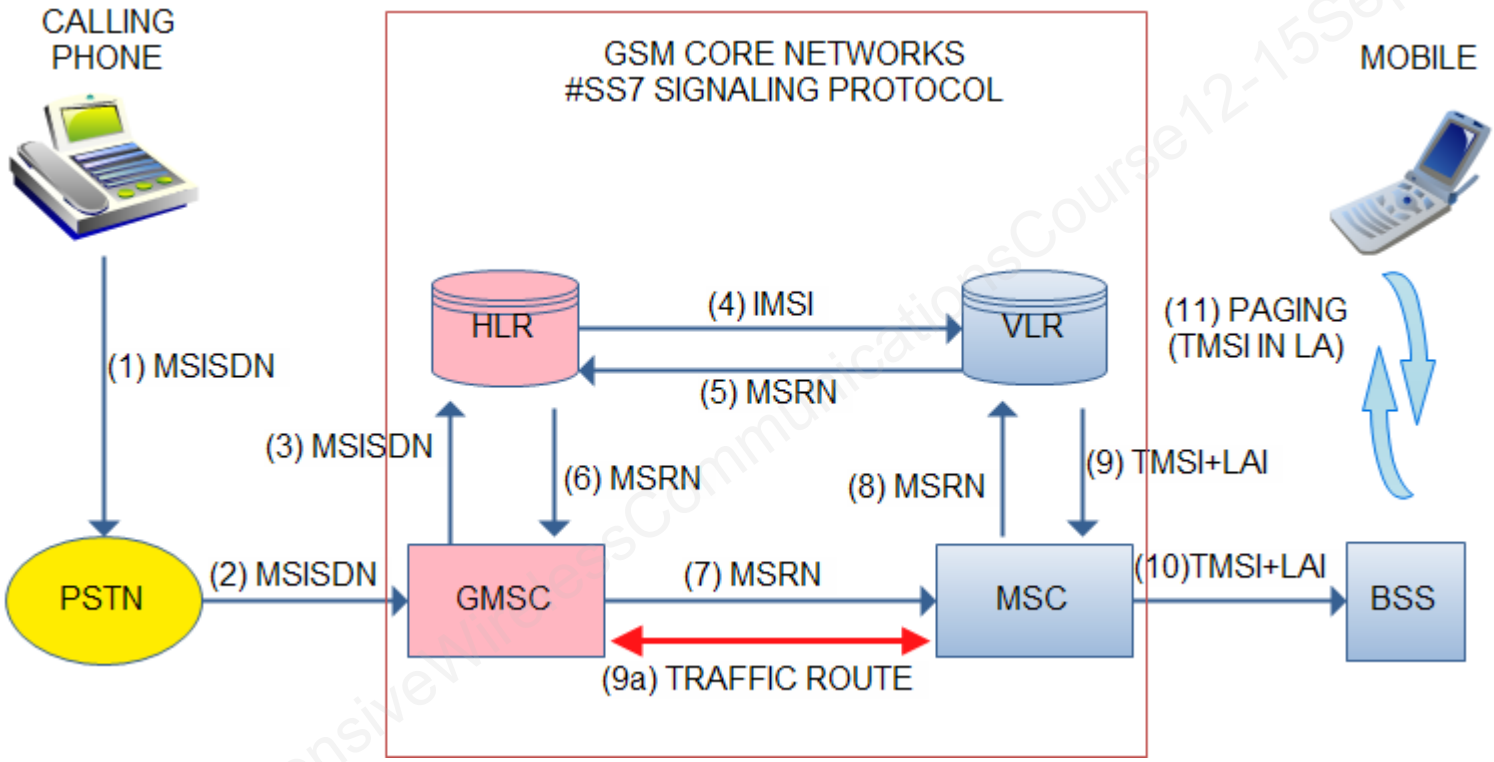
Identification Numbers

- MSISDN Mobile Subscriber International ISDN Number=Country Code+National Destination Code+Serial Number=CC+NDC+SN
- IMSI International Mobile Subscriber Identity=Mobile Country Code+Mobile Network Code+Mobile Subscriber Identification Number=MCC+MNC+MSI
- MSRN Temporary Mobile Station Roaming Number=CC+NDC+SN
- TMSI Temporary Mobile Subscriber Identity: 32 bits – unique to location area.
- LAI Location Area Identity=MCC+MNC+Location Area Code
- CID Cell IDentifier: 2x8 bits – defines cell within location area.
- HON HandOver Number (format of MSRN)
- IMEI International Mobile Equipment Identity. (Device SN)

Registration and Location Update



PSTN to Mobile Call Flow



PSTN Public Switched Telephone Network

MSISDN Mobile Subscriber International ISDN

IMSI International Mobile Subscriber Identity

MSRN Temporary Mobile Station Roaming Number

TMSI Temporary Mobile Subscriber Identity

LAI Location Area Identity

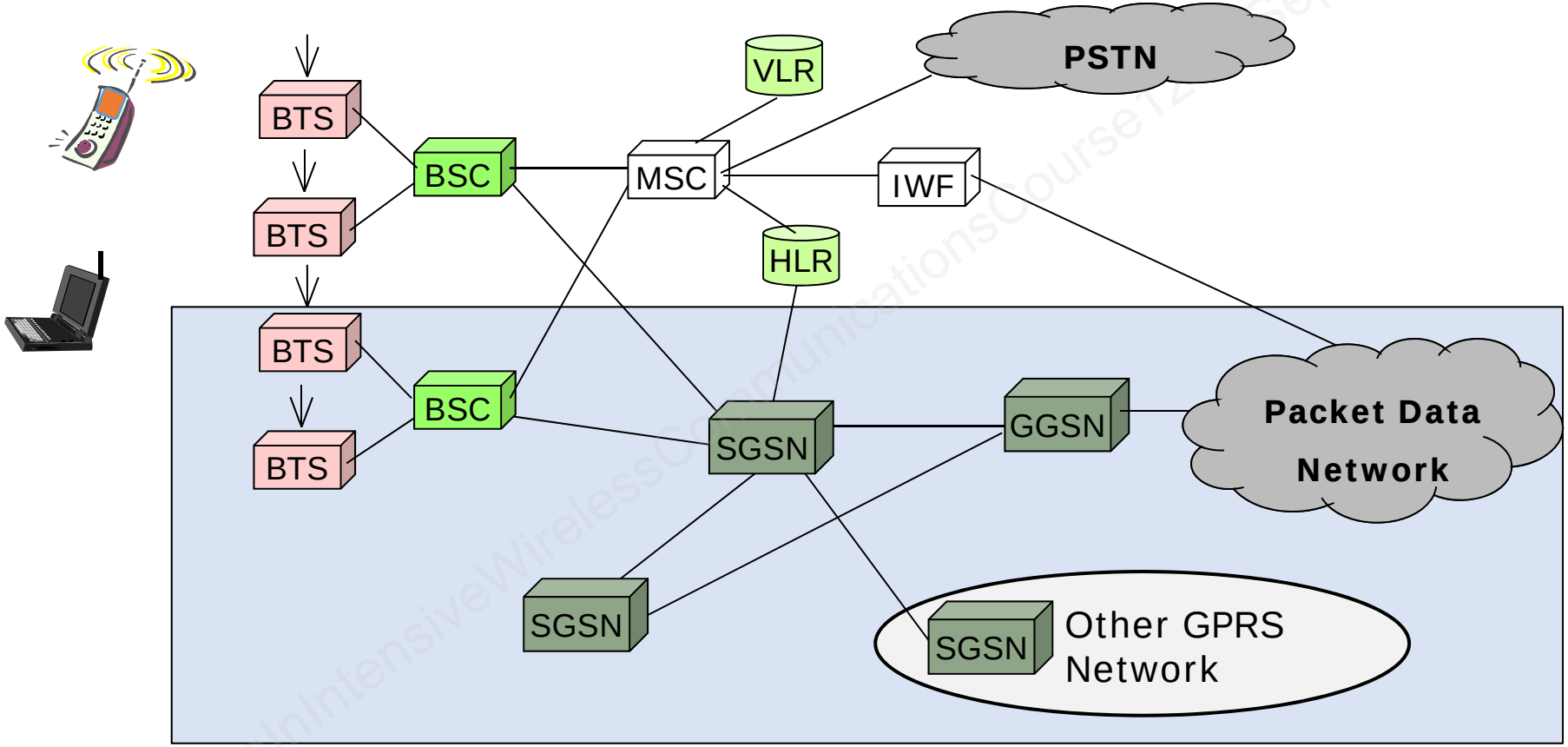
GPRS: Introduction

- General packet radio service
  - Packet data service in GSM to access packet data networks (PDN)
  - Consists of packet wireless access network and IP-based backbone
  - Radio resources shared dynamically between speech and data services
- Benefits
  - Users – charging based on traffic volume, not hold time
  - Operators – efficient use of spectrum

What is GPRS?

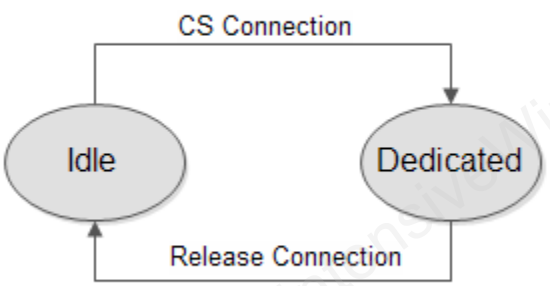
- Cost effective and efficient use of network resources for intermittent, frequent transmission of small volumes of data
- PTP and PTM bearer services
- Applications
  - Web surfing, messaging, telnet,
  - News, weather, traffic reports, dispatch services
  - (later) bearer for IMS
- Three classes of GPRS equipment
  - Class A: voice and data simultaneously
  - Class B: voice and data one at a time
  - Class C: disconnect from one mode to use other

GPRS Architecture

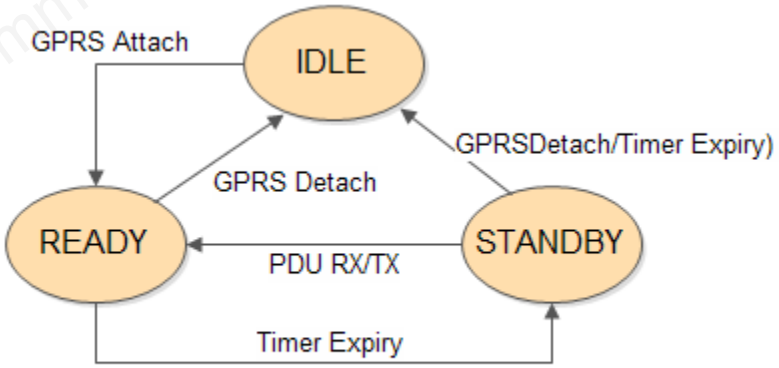


GPRS State Models

- Idle state: not traceable
- Ready state: data sent or received
- Standby state: reduced tracking – data sent/received triggers Ready state

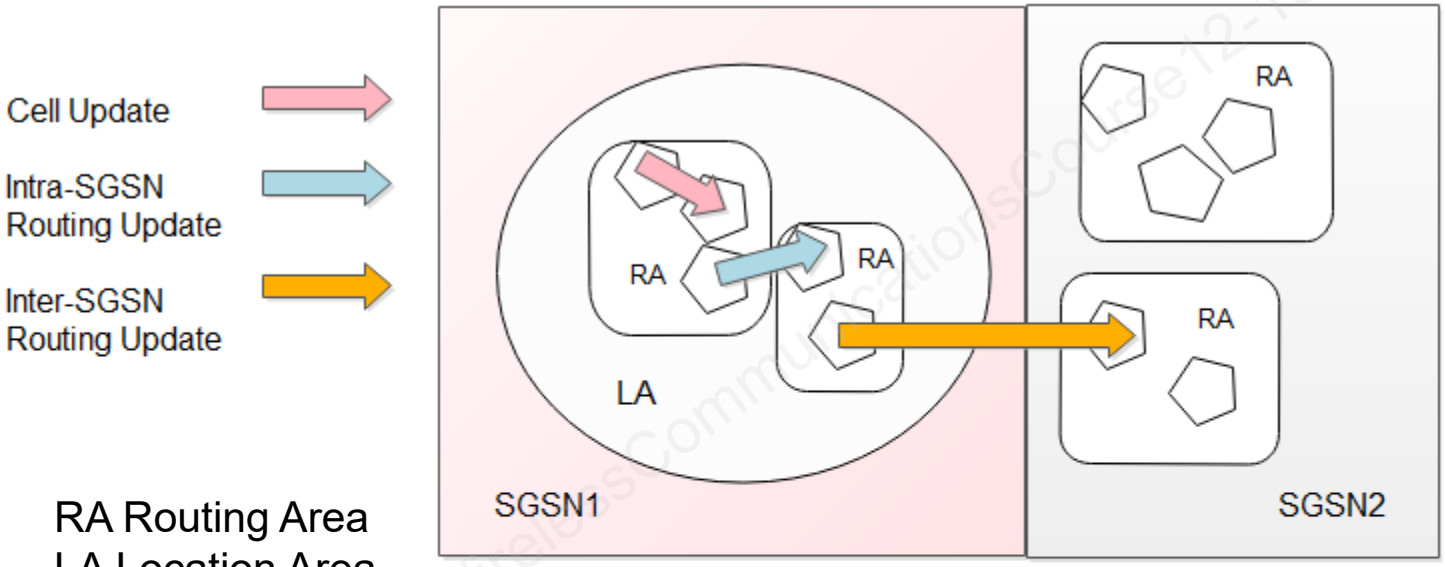


GSM States



GPRS States

GPRS Location Management

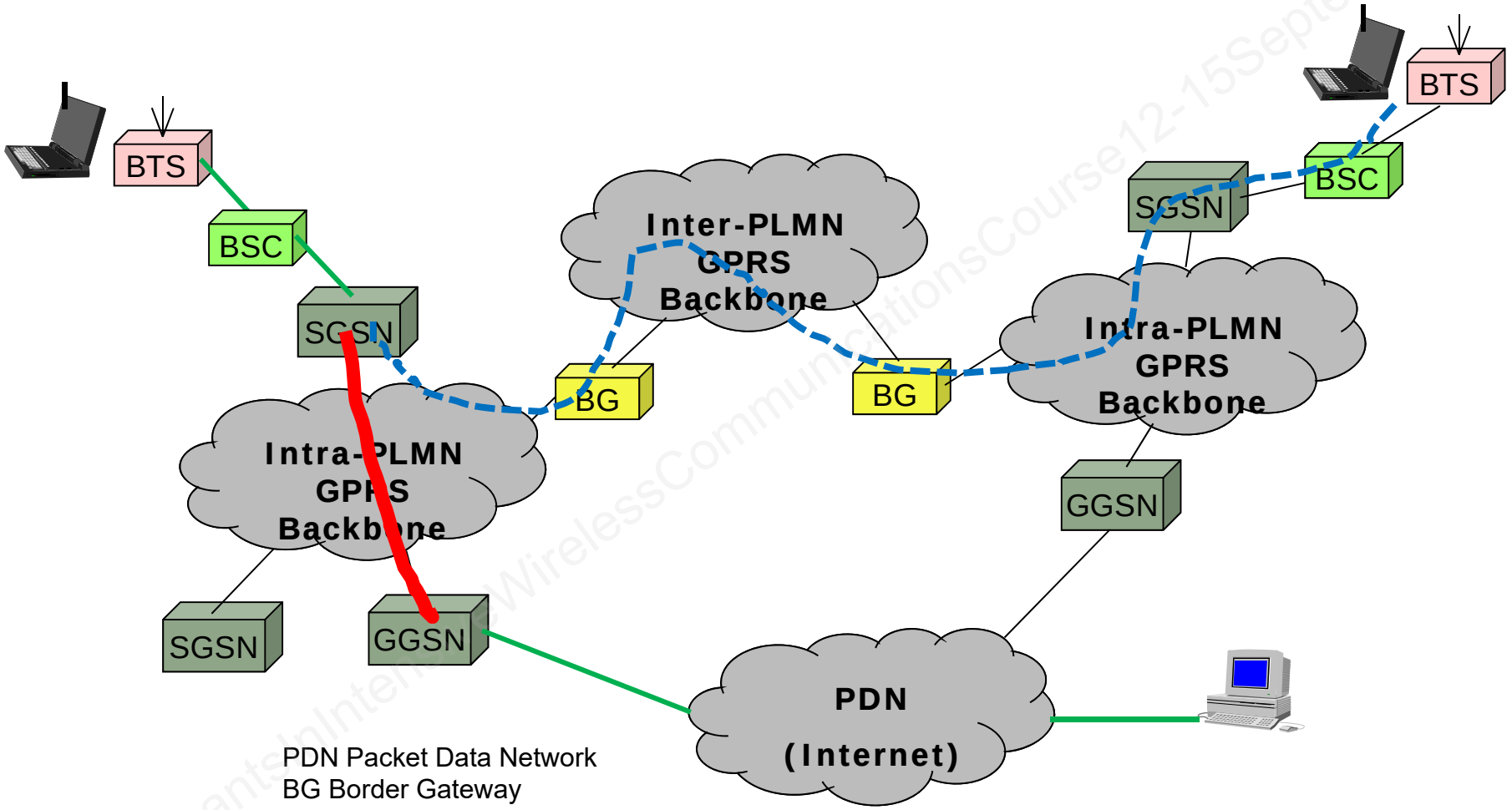


RA Routing Area
LA Location Area

Cell

Idle	No	No	No
Standby	No	Yes	Yes
Ready	Yes	Yes	Yes

GPRS Routing Example



Practice Questions (2)

1. Maximum number of MAC addresses in 802.11 frame:
   a) 2
   b) 3
   c) 4
   d) 5
2. A call center gets an average of 1800 new calls per hour. Each call lasts on the average 3 minutes. The traffic intensity is
   a) 600 lines
   b) 5400 erlangs
   c) 300 erlangs
   d) 90 erlangs
3. In GSM, mobile units are paged using
   a) IMSI
   b) MSRN
   c) MSISDN
   d) TMSI
4. True or False: Authentication is not required for registration when mobile is in home network.

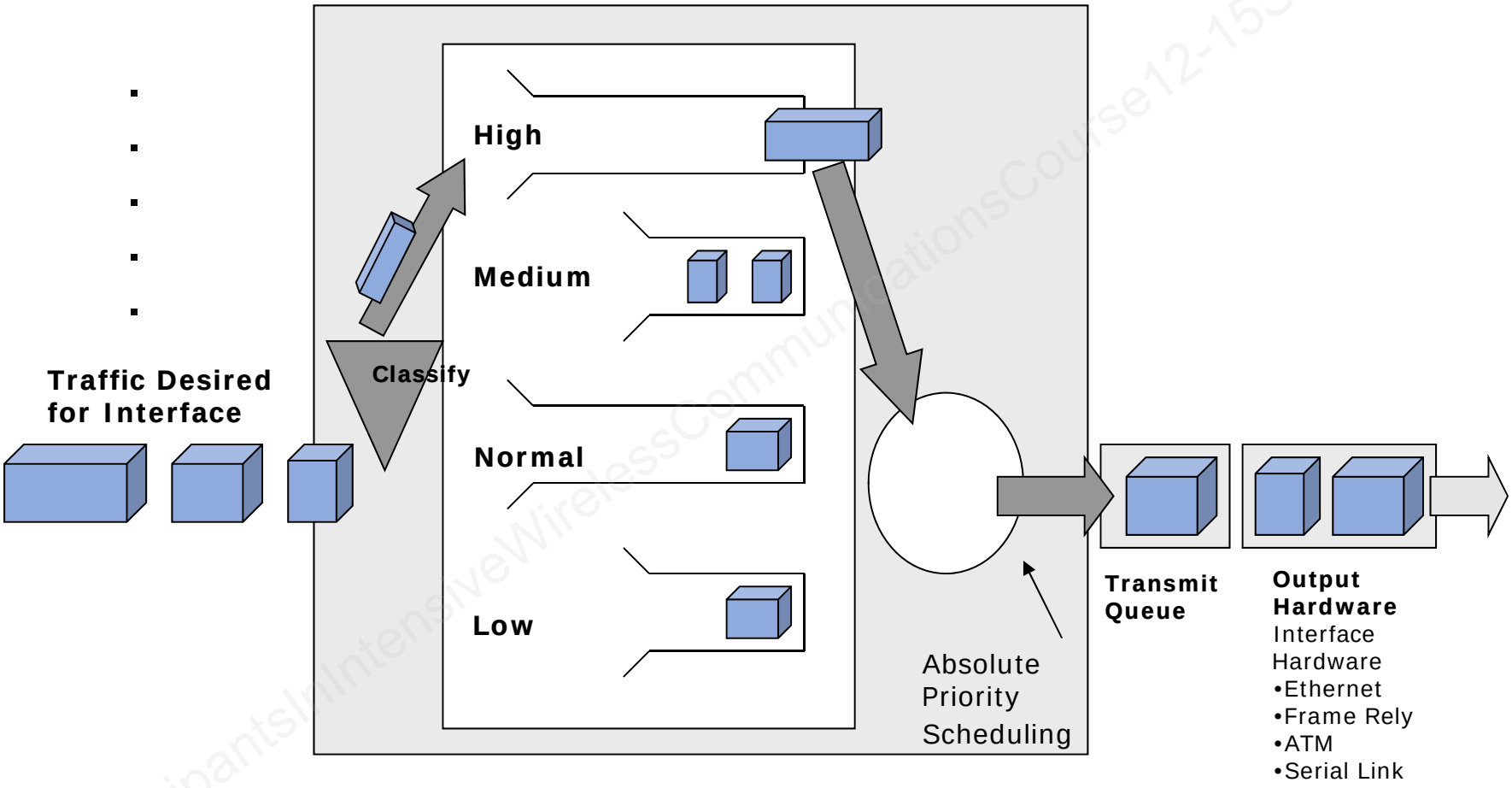
All IP Core Network

- Technologies for QoS support
- Technologies for VoIP transport
- Cellular network evolution to all-IP core network architectures
- LTE's EPC (Evolved Packet Core)
- Fixed-Mobile Convergence

The Need for QOS

IntServ Category	Sub – Category	Examples	Constant Rate Necessary	Low Delay Necessary	Low Jitter Necessary	Low Delay Preferred
Tolerant Real - Time		Audio/Video Streaming	√			
Intolerant Real – Time		IP Telephony, teleconferencing	√	√	√	
Elastic (Non-Real -Time)	Interactive Burst	Telnet, HTTP				√
	Interactive Bulk Transfer	FTP				√
	Asynchronous Bulk Transfer	SMTP				

QOS: Queuing



QOS: MPLS

- Between layer 2 and layer 3
- How it works:
  - Ingress LSR (Label Switching Router) adds the label to IP packet according to the destination
  - Core LSR forwards the packet based on the label only
- LDP (Label Distribution Protocol)
  - distributes the labels among the LSRs, i.e., establishes LSPs (label switched paths)
  - Can be control-driven (such as routing updates) or data-driven (such as flow request)
  - Can be used by a source LSR to specify explicit routes

VoIP and All-IP Networks

- 2 parallel networks through 3G
  - Packet switching good for data
  - Circuit switching good for voice
  - Ideal: IP-based data network together with PSTN
- Convergence, compromise
  - Treat voice as just another kind of data
  - Voice over packets, e.g., VoIP
  - Same IP network as for IP video
  - Converged network carrying voice/video and data

VoIP: Requirements

- Delay (latency) and jitter
  - 100-200 ms one-way delay
  - People can tolerate up to 400 ms one-way delay in some situations
  - Jitter should be kept small – reduced by buffering
- Other requirements
  - Timing reconstruction, loss detection, and content identification
  - Conferencing: source ID, synchronization
  - Security – encryption, authentication
  - Packet loss rate < 1%

VoIP: QoS

- Traffic classification
  - Conversational, streaming, interactive, background
- QoS mechanisms
  - Marking, shaping, admission control …
- QoS implemented in core network
  - DiffServ for differentiated services
  - MPLS for bandwidth allocation and service guarantees (virtual circuits)
- Challenge: multiple provider networks

VoIP: Meeting the Requirements

- QoS in network
- Buffering
  - Protection against jitter
- Transport protocol
  - TCP: unhelpful features (retransmission)
  - UDP: provides too few features
  - RTP/UDP, plus RTCP for source ID, etc.
- Small packets for reduced delay
  - Header overhead becomes substantial
  - Header compression!

RTP: Real Time Protocol
RTCP: Real Time Control Protocol

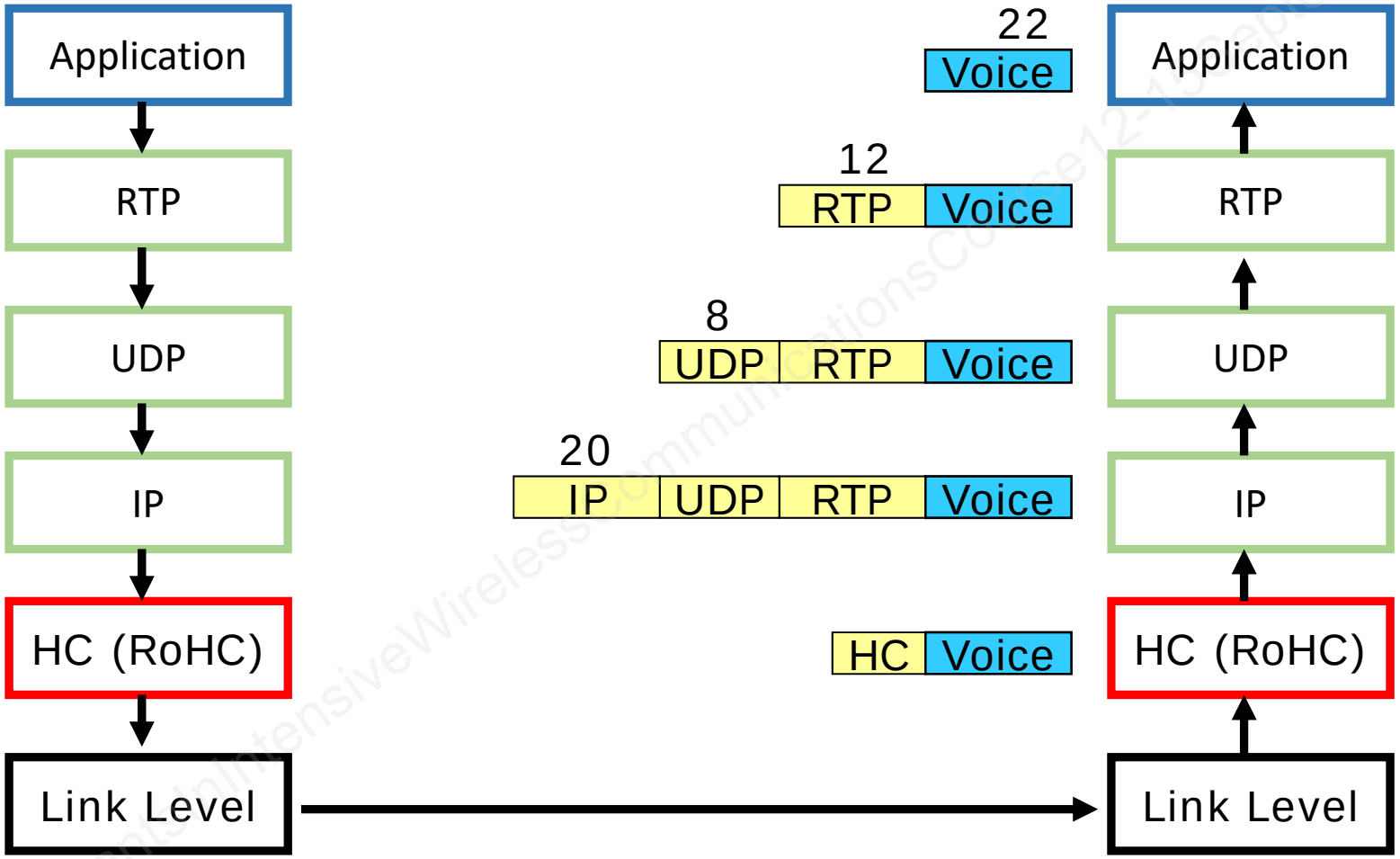
VoIP: Robust Header Compression (RoHC)

- The problem
  - RTP/UDP/IP has high bandwidth overhead
  - E.g., 10 ms of speech
    - 20 ms, 30 ms also possible, but higher delay
  - With 16 Kbit/s codec, e.g., G.728
    - 100 packets/s
    - 20 bytes codec data per packet
  - 40 byte RTP/UDP/IP header
  - 40 out of 60 bytes per packet are in header!

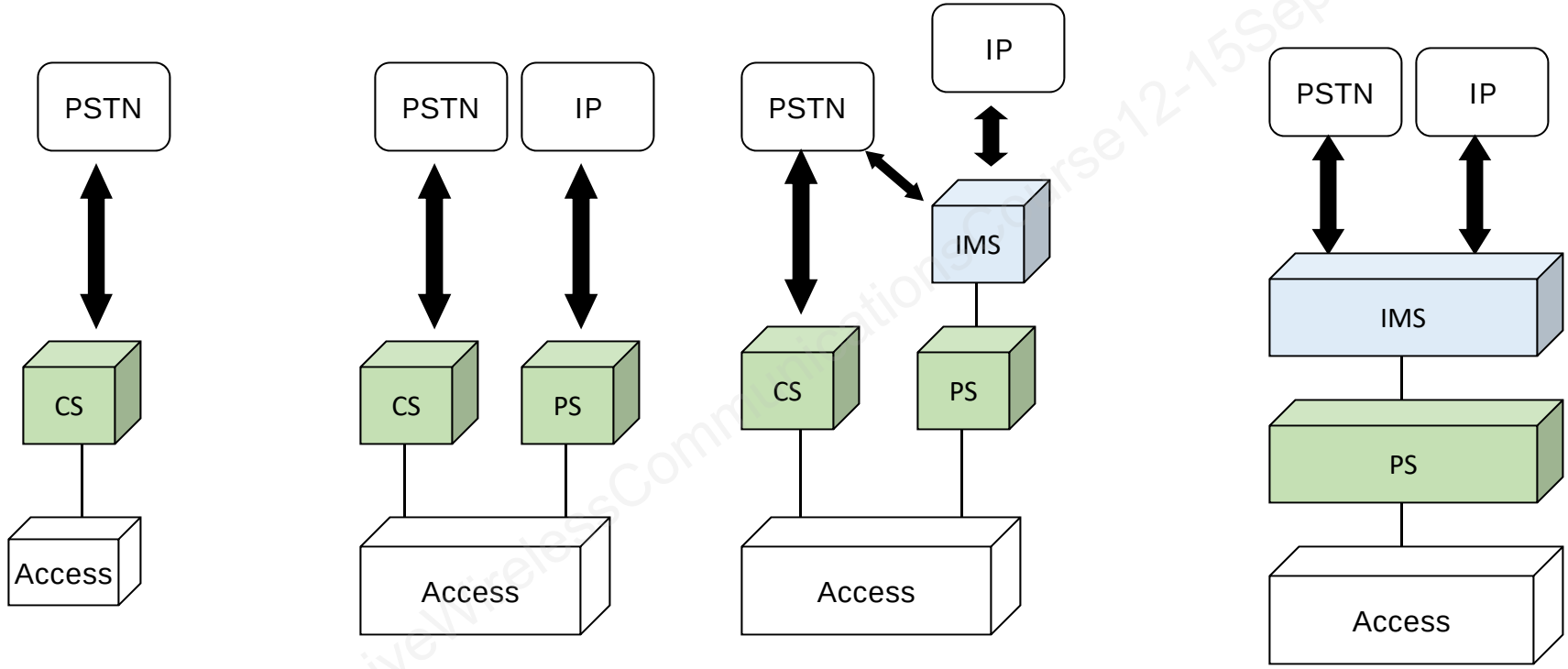
VoIP:RoHC

- A lot of redundant information in headers
  - Same source and destination IP addresses
  - Same source and destination UDP ports
  - Same payload type in RTP header
  - Send once at start of media stream
- Incremental differences in consecutive packets
  - Time stamp increments fixed amount within each talk spurt
  - Send only at beginning of talk spurt

VoIP: RoHC Protocol Stack



Evolution From GSM to EPC (Evolved Packet Core)



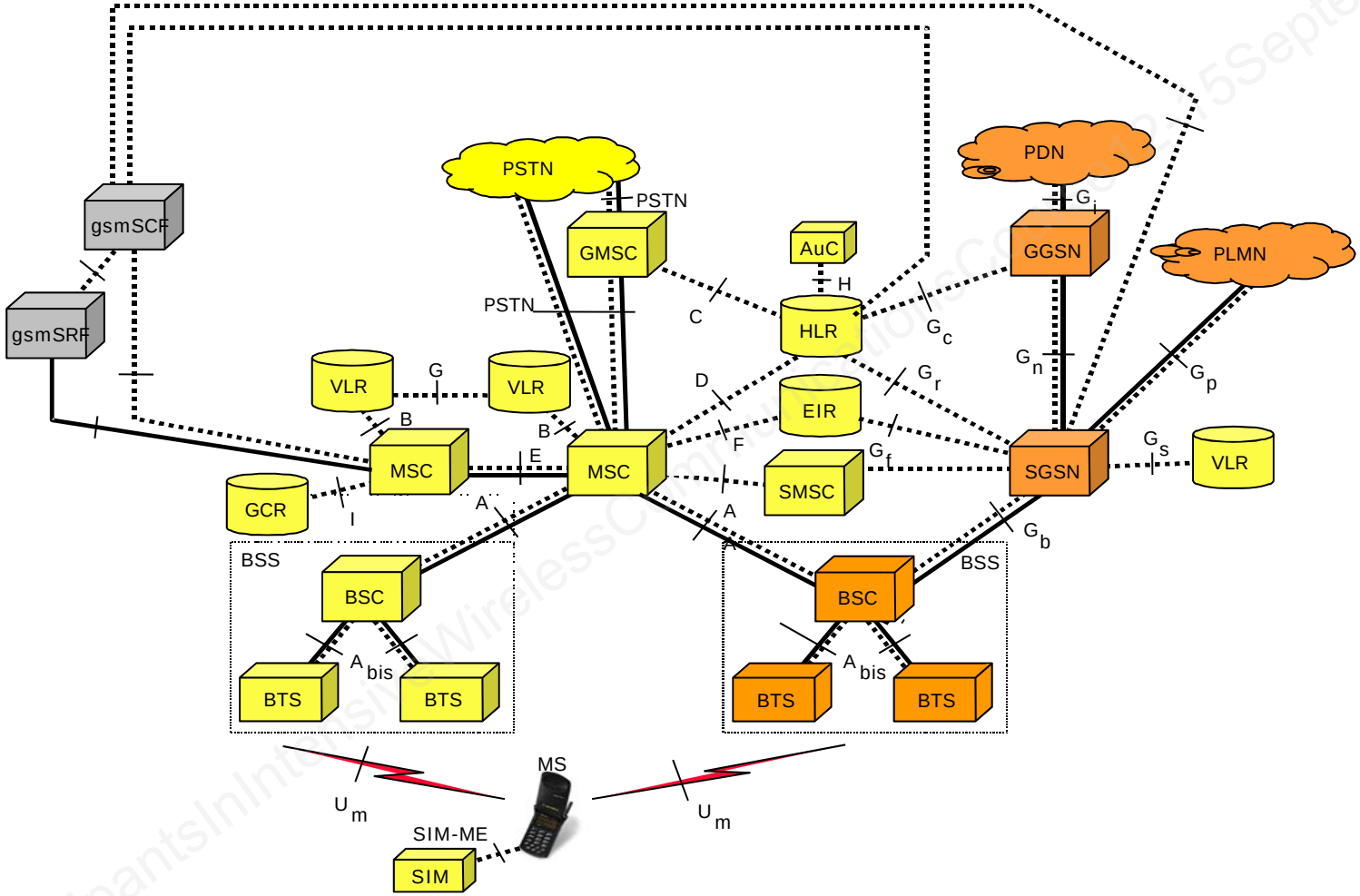
2G initial architecture (GSM)

2G packet evolution (GPRS/EDGE)

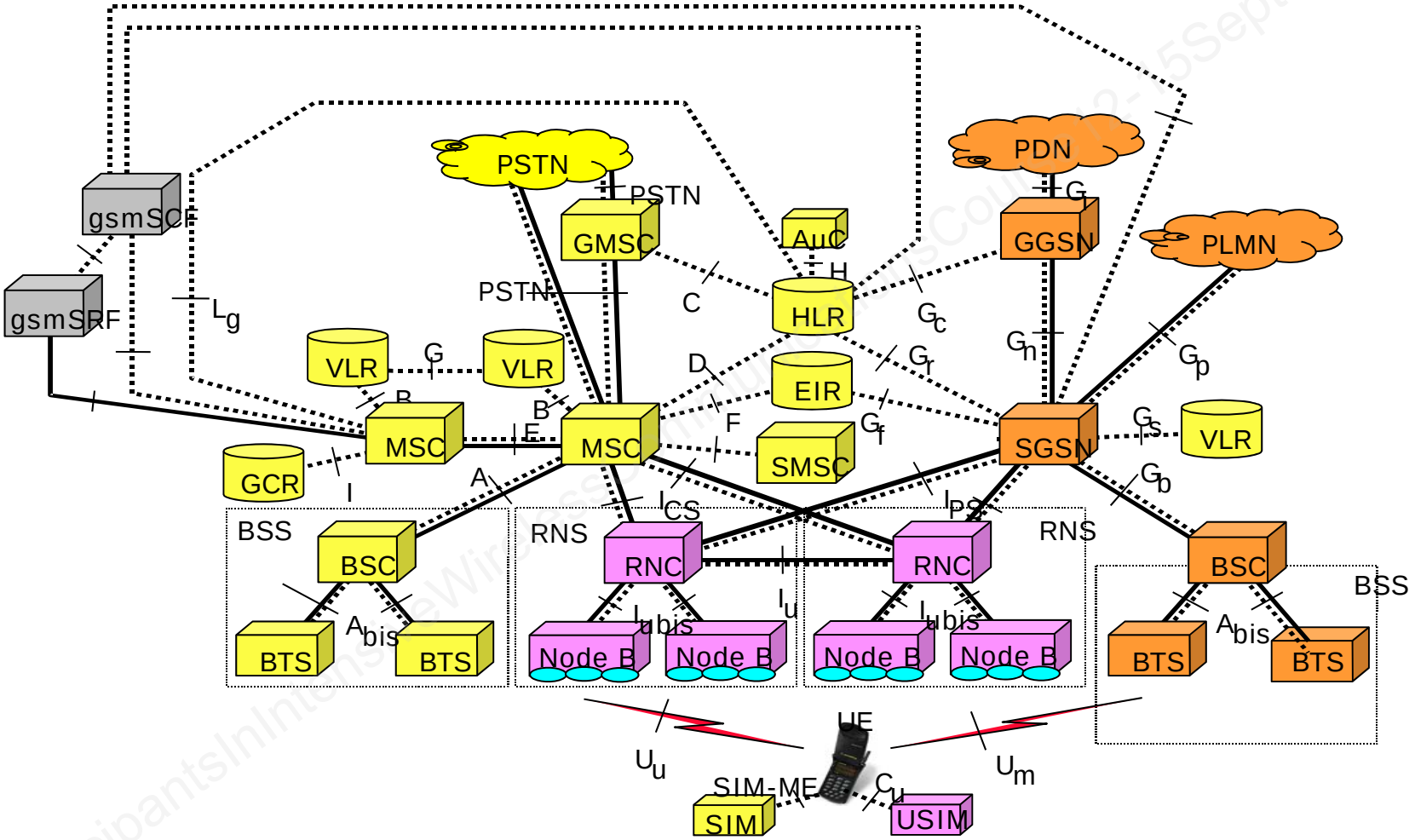
3G IMS evolution

EPC Architecture

Evolution from 2G to GSM 2.5G

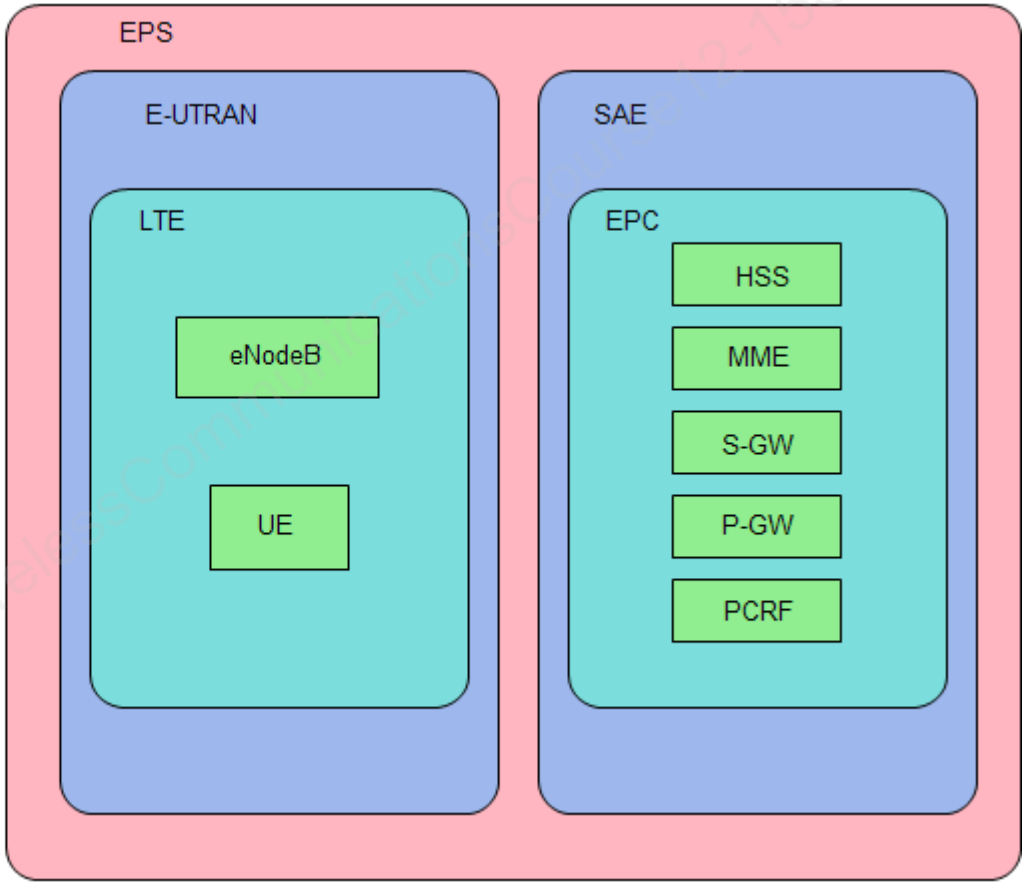


Evolution from 2.5G to UMTS Release 99

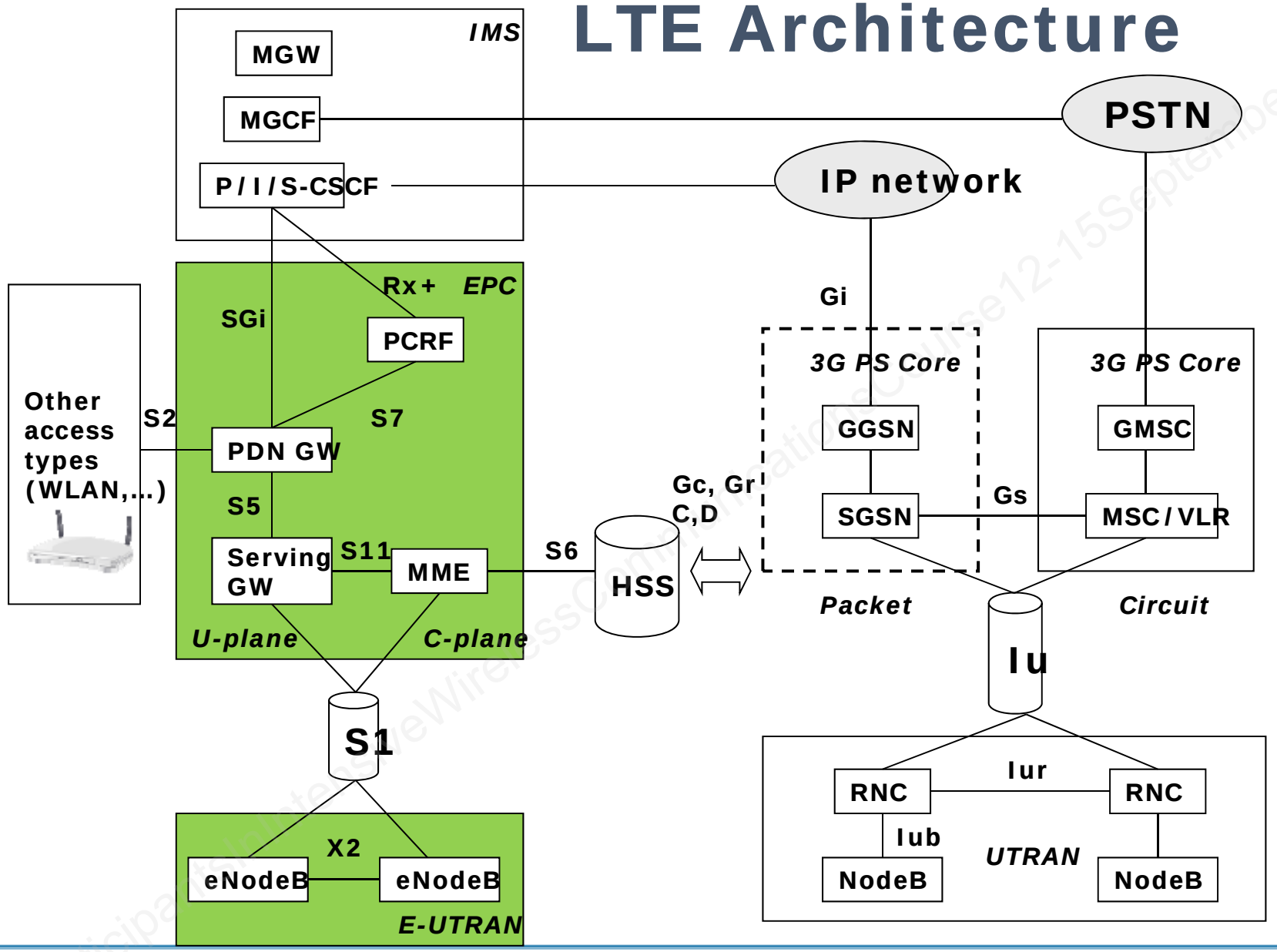


LTE Terminology

EPS- Evolved Packet System
E-UTRAN- Evolved UTRAN
UTRAN- Universal Terrestrial Radio Access Network
SAE- System Architecture Evolution
LTE- Long Term Evolution
EPC- Evolved Packet Core
eNodeB- Evolved NodeB
UE- User Equipment
HSS- Home Subscriber Server
MME- Mobility Management Entity
S-GW- Serving Gateway
P-GW- PDN Gateway
PDN- Packet Data Network
PCRF- Policy Control and Charging Rules Function



LTE Architecture



MME Mobile Management Entity

- Overall functionality is to provide the control for mobility and session management (Control Plane)
- Communicates with eNB for access control
- Communicates with S-GW for bearer control and mobility management
- Communicates with HSS for authentication and to obtain subscriber information
- Communicates with UE for mobility, registration, user identity, etc. (NAS (Non-Access-Stratum) layer)
- Communicates with 3GPP SGSN for handover to/from 3GPP networks

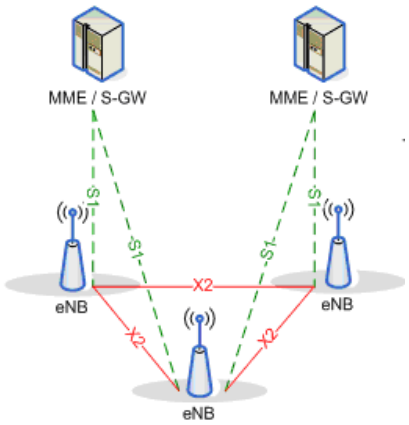
Serving Gateway Node

- Terminates the media interface with the LTE radio network
- Communicates with PDN-GW for access to external IP networks
- Communicates to MME for bearer management and mobility control
- Anchors LTE handovers between LTE and 3GPP networks (HSPA, GPRS)

PDN-Gateway node

- Access to external IP networks
- Enforces PCRF policies
- Anchors LTE handovers with non-3GPP networks
  - Trusted
    - Trusted EVDO, trusted Wi-Fi
  - Non-Trusted
    - Untrusted Wi-Fi, other untrusted access networks
- Access with IMS

LTE Evolved Radio Network (E-UTRAN)

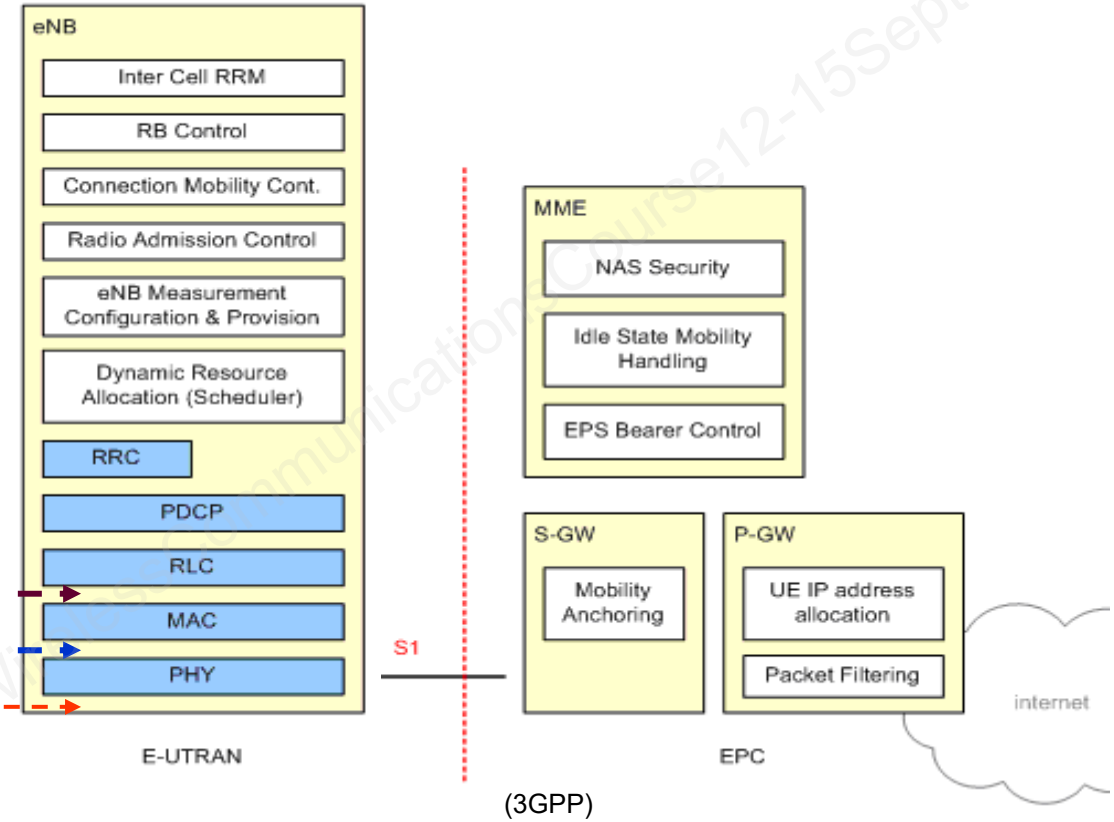


Radio Resource Control (Layer 3)

Radio Link Control (Layer 2)

Medium Access Control (Layer 2)

Physical Layer (Layer 1)



Logical Channels

Transport Channels

Physical Channels

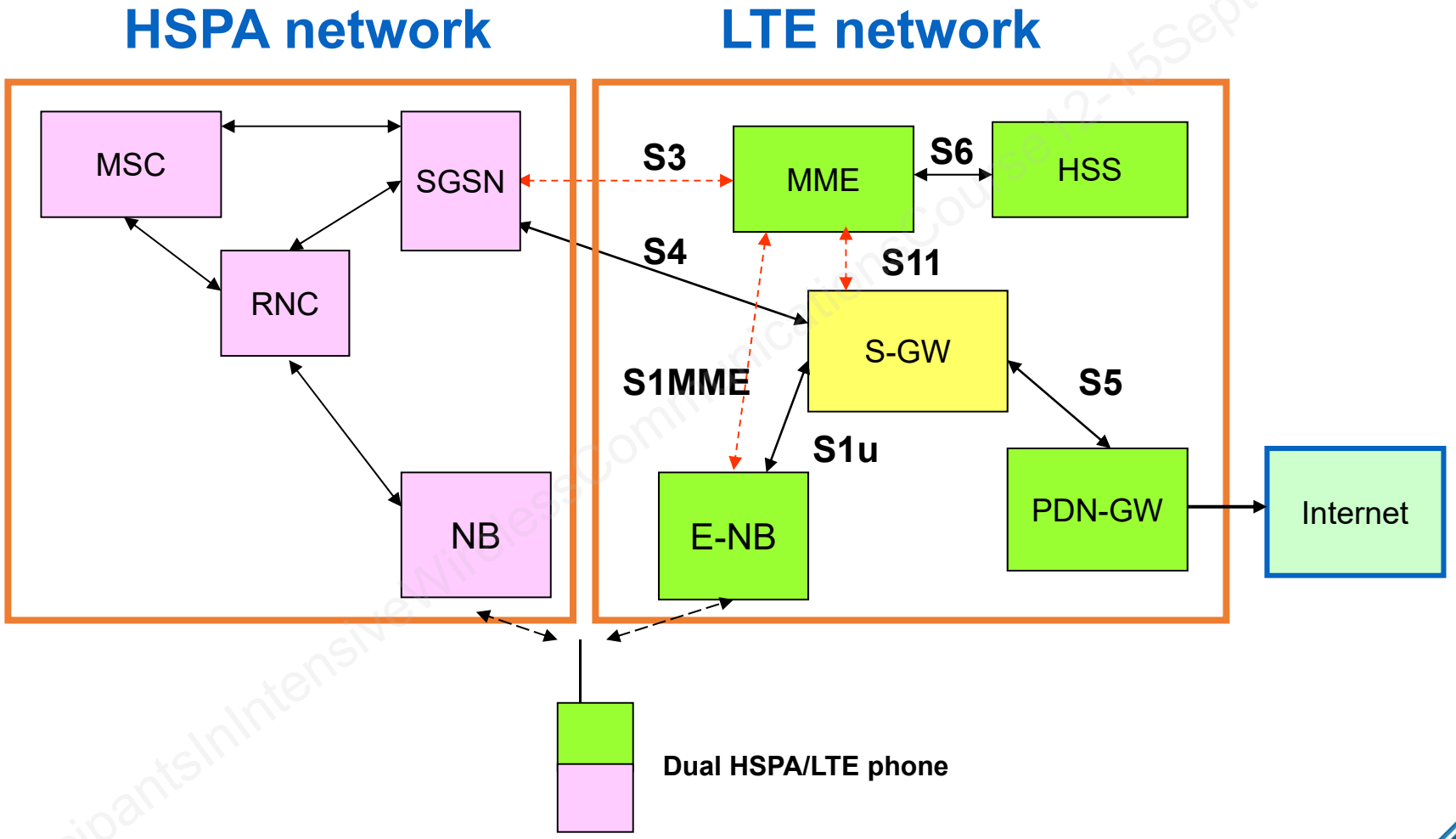
- **Mapping of control and traffic channels between (sub-)layers**

LTE Internetworking

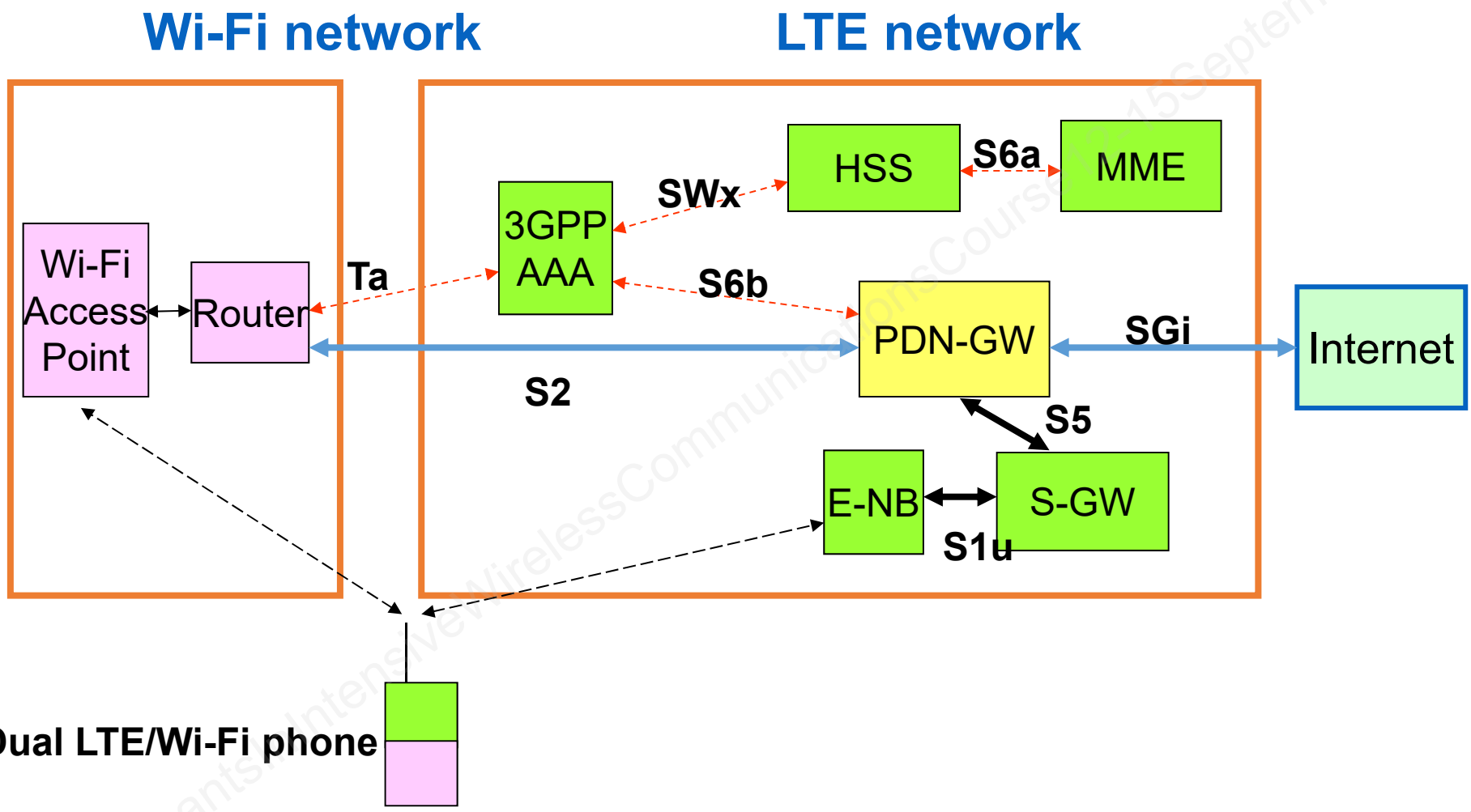
- Trusted networks
  - LTE with HSPA internetworking
    - S-GW is the anchor for handover
    - SGSN interfaces both the MME and S-GW
  - Trusted Wi-Fi
    - PDN-GW is the anchor for handover
- Untrusted network
  - untrusted Wi-Fi or other untrusted access networks
    - PDN-GW is the anchor for handover
    - ePDG node introduced

ePDG: Enhanced Packet Data Gateway

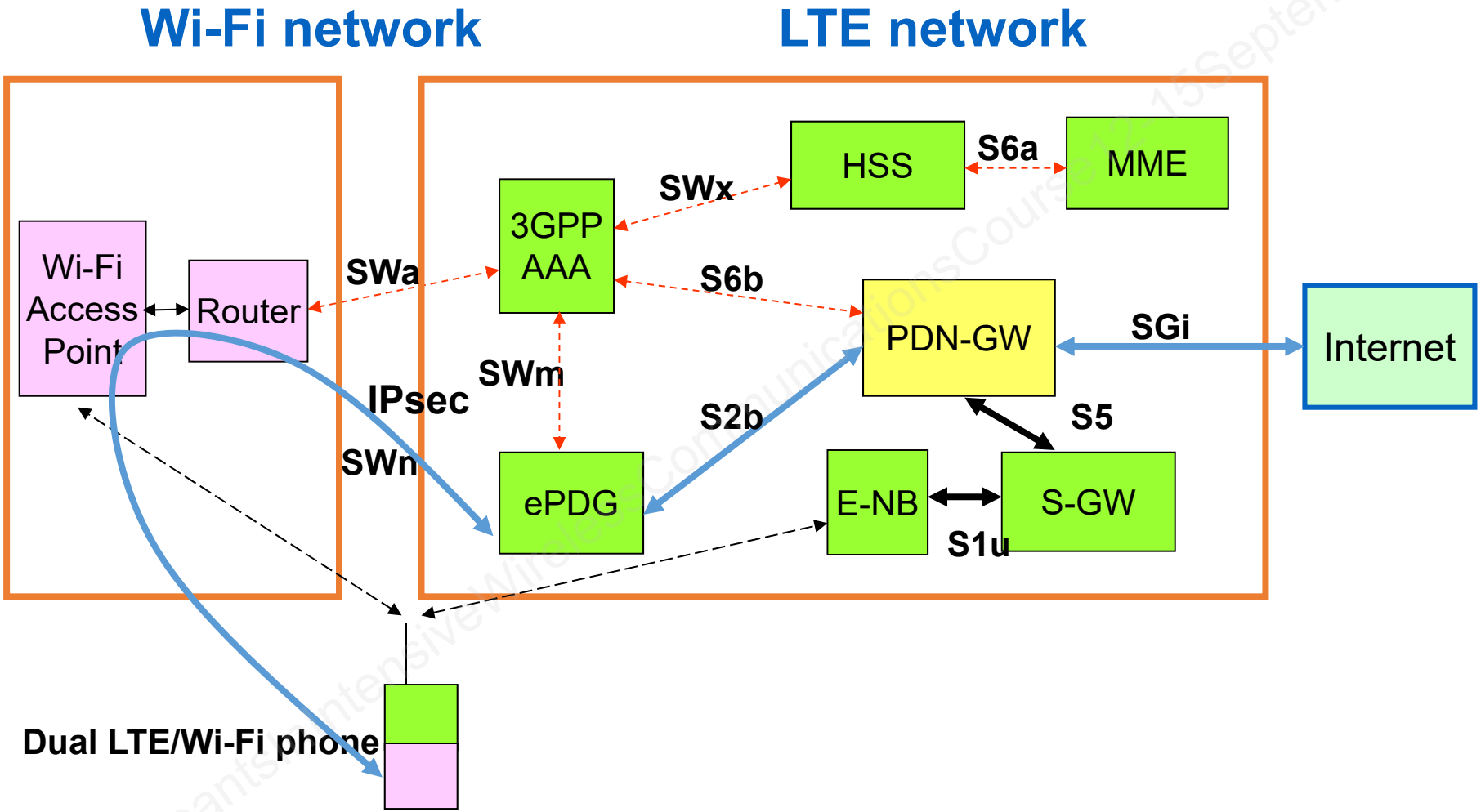
LTE and HSPA Data Internetworking Architecture



LTE to Trusted Wi-Fi Interworking Architecture



LTE to Untrusted Wi-Fi Interworking Architecture



LTE Bearers and QoS

- LTE bearer enables different traffic treatments
- E2E LTE bearer QOS adds:
  - Access QOS (terminal to eNB)
  - Backhaul QOS (eNB to S-GW)
  - Core QOS (S-GW to PDN-GW)
- E2E service includes from terminal to terminal
  - E2E LTE QOS
  - External QOS (outside operator networks)

EPS Bearers

Minimum Guaranteed Bit Rate (GBR)

- VoIP
- Permanently allocated dedicated transmission resources

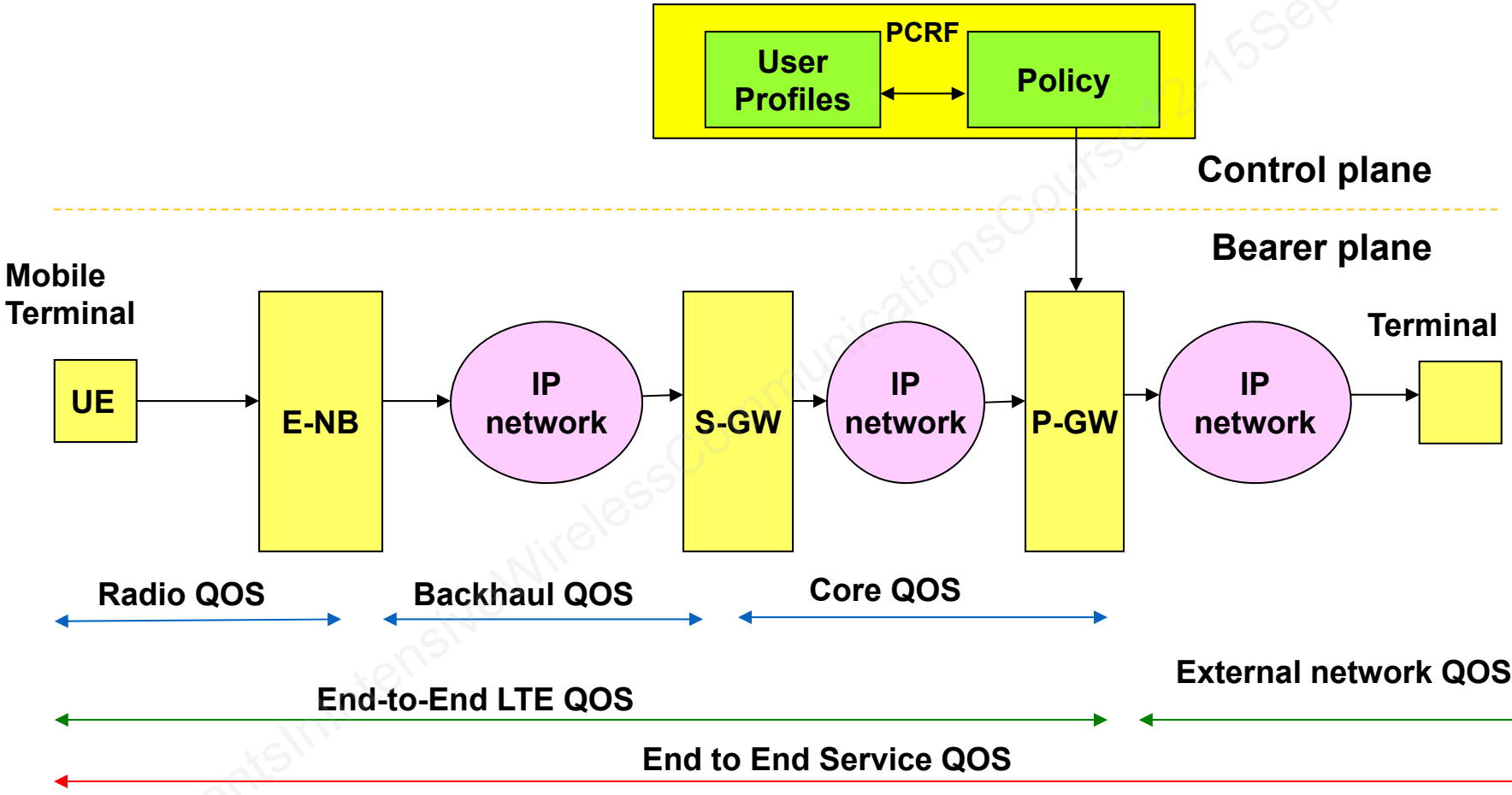
Non-GBR

- Web browsing
- FTP transfer
- No permanently allocated resources

Quality of Service Class Identifiers

QCI	Resource Type	Priority	Packet Delay (ms)	Packet Loss	Example
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real time gaming
5	Non-GBR	1	100	10^{-6}	IMS signaling
6	Non-GBR	7	100	10^{-3}	Live streaming, interactive gaming
7	Non-GBR	6	300	10^{-6}	Video (buffered streaming)
8	Non-GBR	8	300	10^{-6}	TCP-based (WWW,e-mail, chat, FTP, p2p file sharing)
9	Non-GBR	9	300	10^{-6}	(same as QCI 8)

LTE End-to-End QOS Bearers



Transport QOS Techniques

- Backhaul and core QOS
  - Diffserv
    - Classifies and marks packets
    - DSCP IP header field (6 bits)
    - Routers check DSCP field for routing
- External network QOS
  - MPLS
    - Label is added to IP header
    - Core LSR checks label value for routing
- Traffic shaping (packet delay)

DSCP: Differentiated Services Code Point
MPLS: Multi Protocol Label Switching
LSR: Label Switching Routers

LTE QoS Example: VoIP

- Voice service requires:
  - Constant bit rate
  - Low latency
  - Low jitter
- LTE Bearer:
  - QCI = 1
  - Priority = 2
  - GBR = yes
- Diffserv DSCP
  - Expedited Forwarding service (low loss, low delay, low jitter; maximum priority). DSCP code= 101110

LTE Voice Services Options

- All IP network for all services including voice
  - Voice standardized as VOLTE
  - Based on IMS
  - First commercial launch on 7 August 2012
- Interim/transition with limited LTE/IMS
  - SR-VCC for handoff between IMS/CS(legacy)
- Interim/transition when IMS not deployed
  - SVLTE
  - Circuit switched fallback (CSFB)
- VOLGA as alternative to VOLTE
  - Fallen out of favor

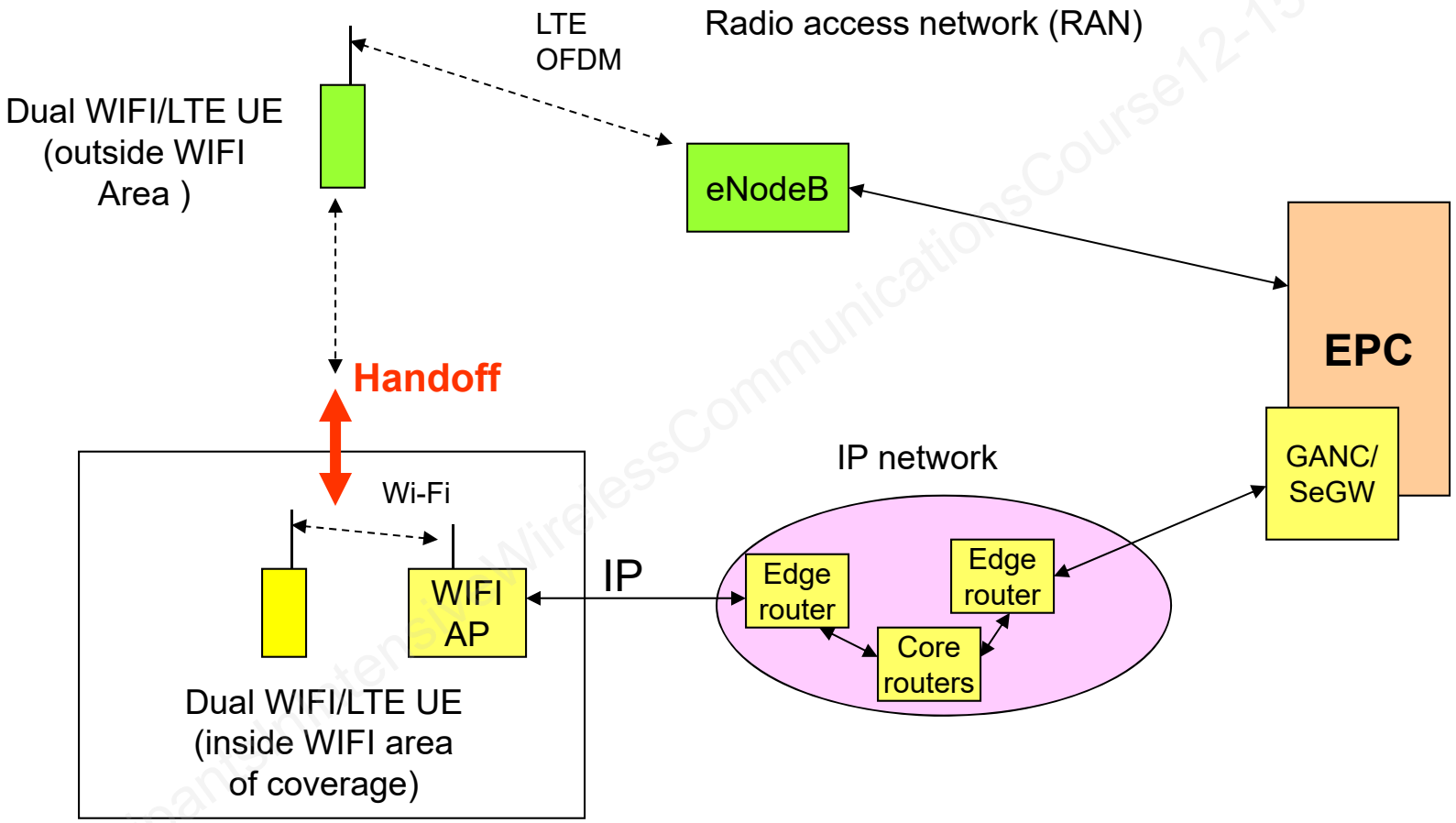
VOLTE: voice over LTE
SR-VCC: single radio voice call continuity
SVLTE: simultaneous voice & LTE
CSFB: circuit switched fallback
VOLGA: voice over LTE via Generic Access

Fixed-Mobile Convergence

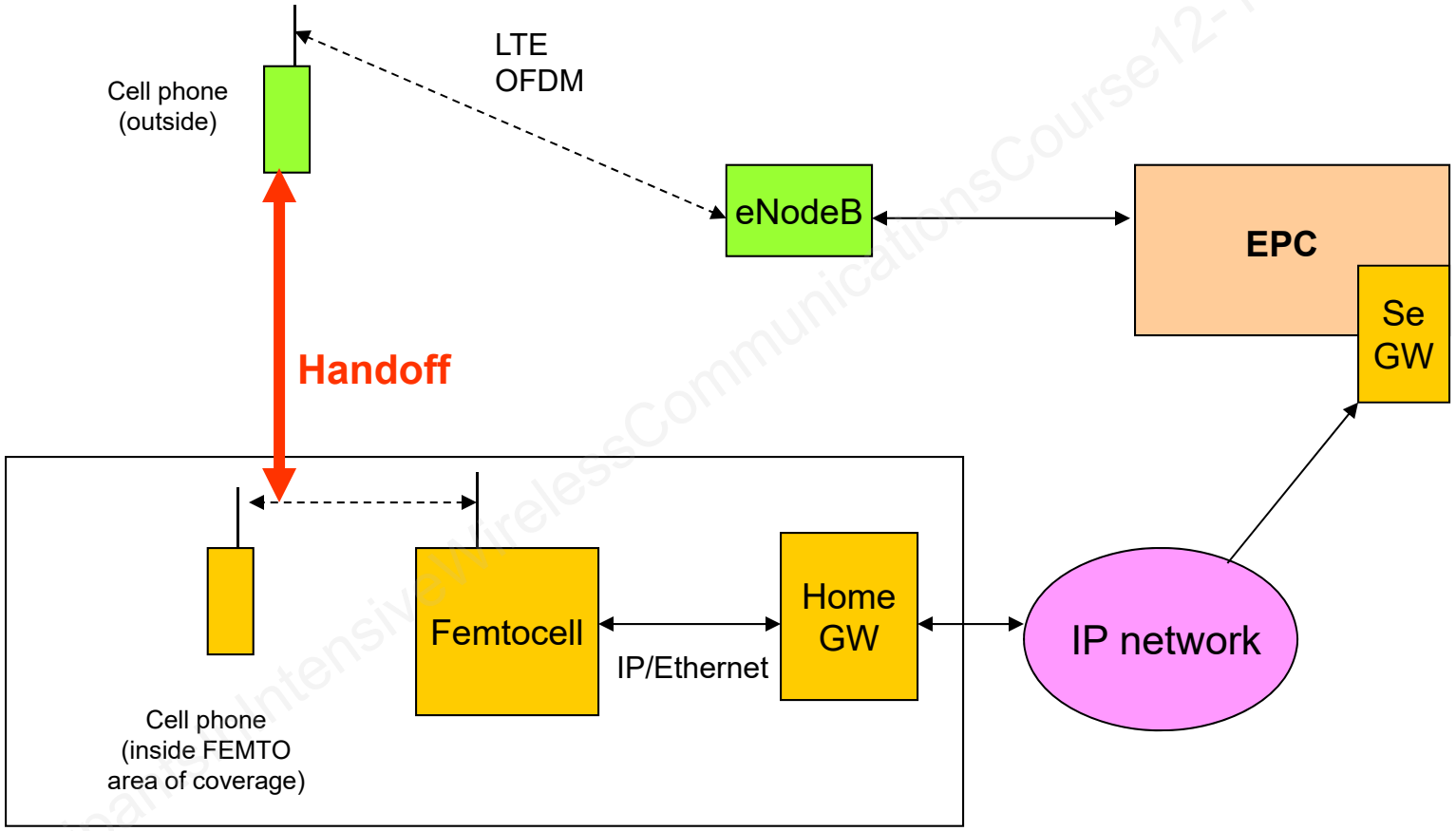
- GAN(previously called UMA)
  - Dual WIFI/LTE phone required
- Femto
  - Regular LTE phone
  - Smaller base stations connected via IP to core LTE
- IMS service integration

GAN: Generic Access Network
UMA: Unlicensed Mobile Access

GAN Diagram



Femtocell Diagram



Practice Questions (3)

1) True or False: Voice service in LTE is provided using IMS.
2) The dominant change in evolution from GSM 2G to 3G is
   a. incorporation of packet switching
   b. major update of core network
   c. adoption of TDMA radio interface
   d. adoption of WCDMA radio interface
3) The purpose of the Generic Access Network (GAN) is uninterrupted handoffs between
   a. cellular and Wi-Fi networks
   b. microcells and femtocells
   c. 2G and 3G networks
   d. GSM and LTE

Service and Alternative Architectures

- IMS: IP Multimedia Subsystem
- SIP: Session Initiation Protocol
- Service creation and architectures, including Parlay/OSA concepts
- Ad hoc networks
- Mesh networks
- Location and Positioning

IP Multimedia Subsystem (IMS)

- Provides session interaction among multiple services reusing common resources
- Based on existing standards (SIP, diameter, etc.)
- Main functionalities
  - Call session control
  - Subscriber management
  - Open interface to multiple application servers
  - Interconnection with IP, Public Switched Telephony Network (PSTN) and Public Land Mobile Network (PLMN) networks
  - Charging and policy interfaces
- VOIP is one example of IMS-based services

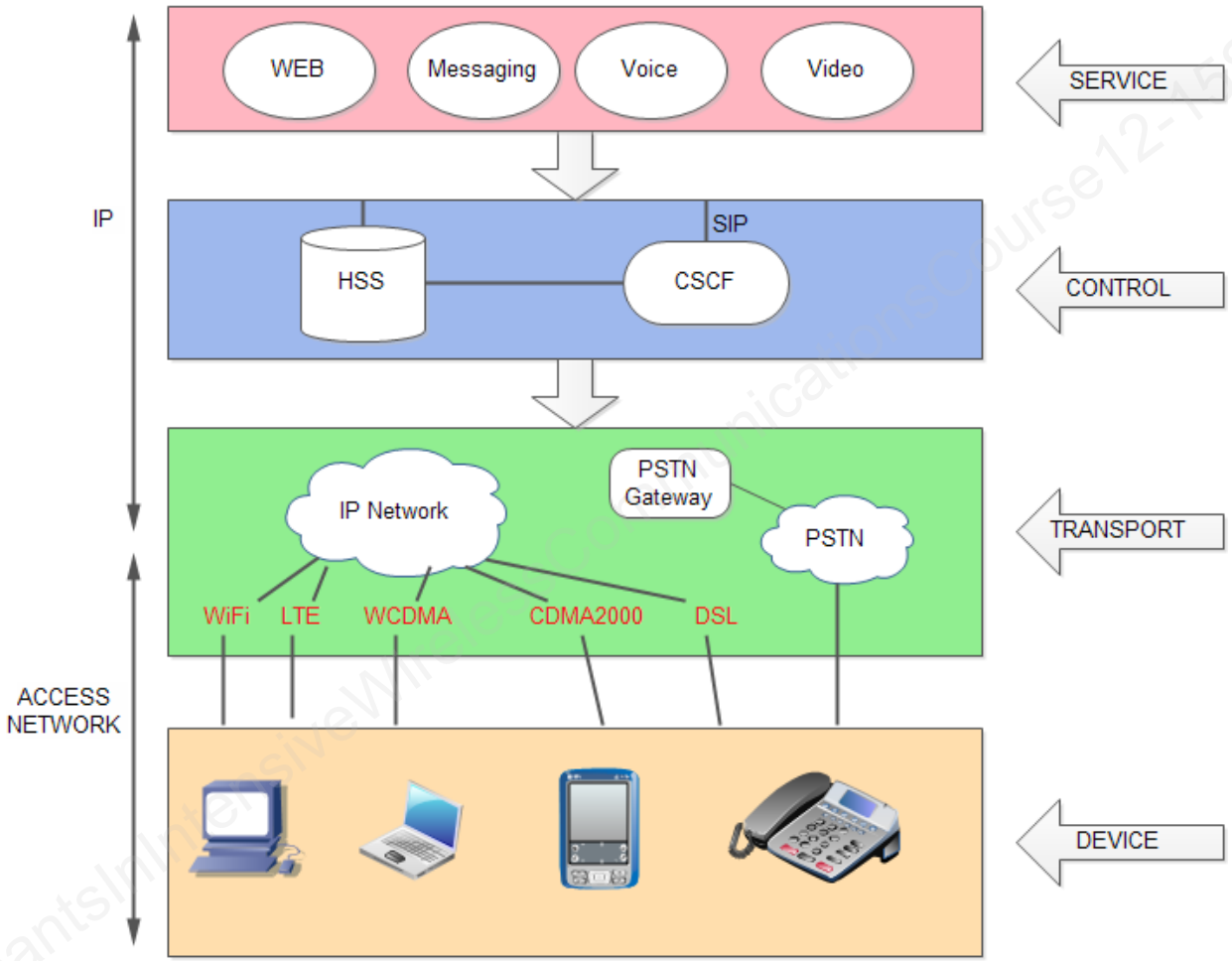
IMS: Introduction

- **Goals**
  - –Enable operators to offer multimedia services built upon Internet applications, services and protocols
    - Voice, video, messaging, data, web-based services
  - –Enable the convergence of wireless and wireline communications
  - –Support 3rd party development of IP-based services
  - –Based on IETF-approved standards

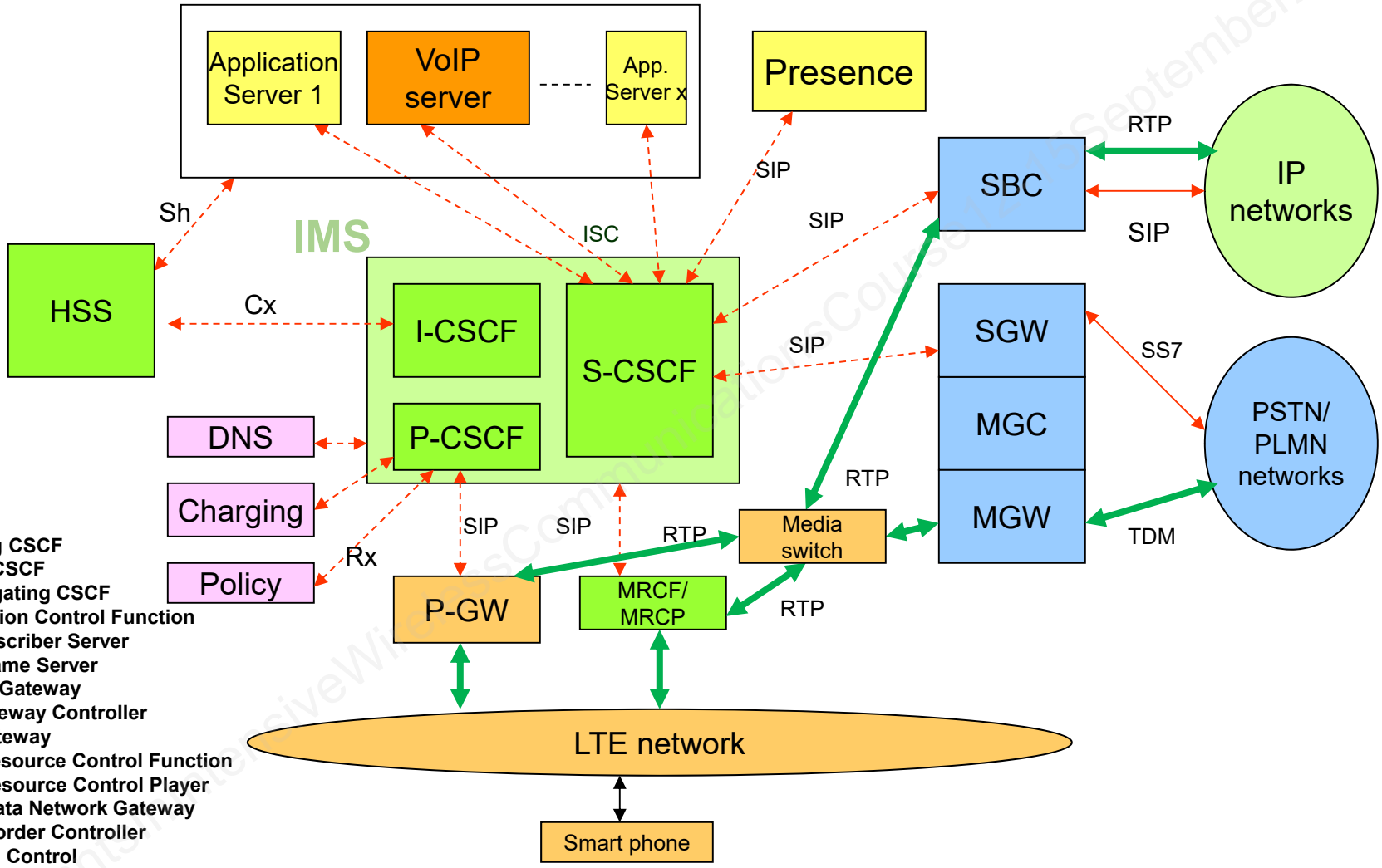
IMS: Requirements

- Utilize PS domain to transport multimedia signaling and bearer traffic
- End-to-end QoS for voice as good as CS
- Roaming support
- Same level of privacy and security as PS and CS services
- Support interworking with PS and CS services
- Support interworking with Internet
- Access independence

IP Multimedia Subsystem (IMS)



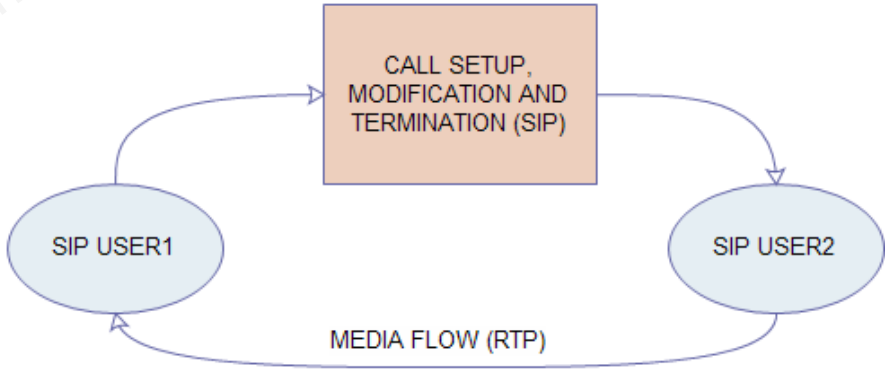
VoIP using IMS architecture



S-CSCF: Serving CSCF
P-CSCF: Proxy CSCF
I- CSCF: Interrogating CSCF
CSCF: Call Session Control Function
HSS: Home Subscriber Server
DNS: Domain Name Server
SGW: Signaling Gateway
MGC: Media Gateway Controller
MGW: Media Gateway
MRCF: Media Resource Control Function
MRCP: Media Resource Control Player
P-GW: Packet Data Network Gateway
SBC: Session Border Controller
ISC: IMS Service Control
RTP: Real Time Protocol
SIP: Session Initiation Protocol

SIP: Session Initiation Protocol

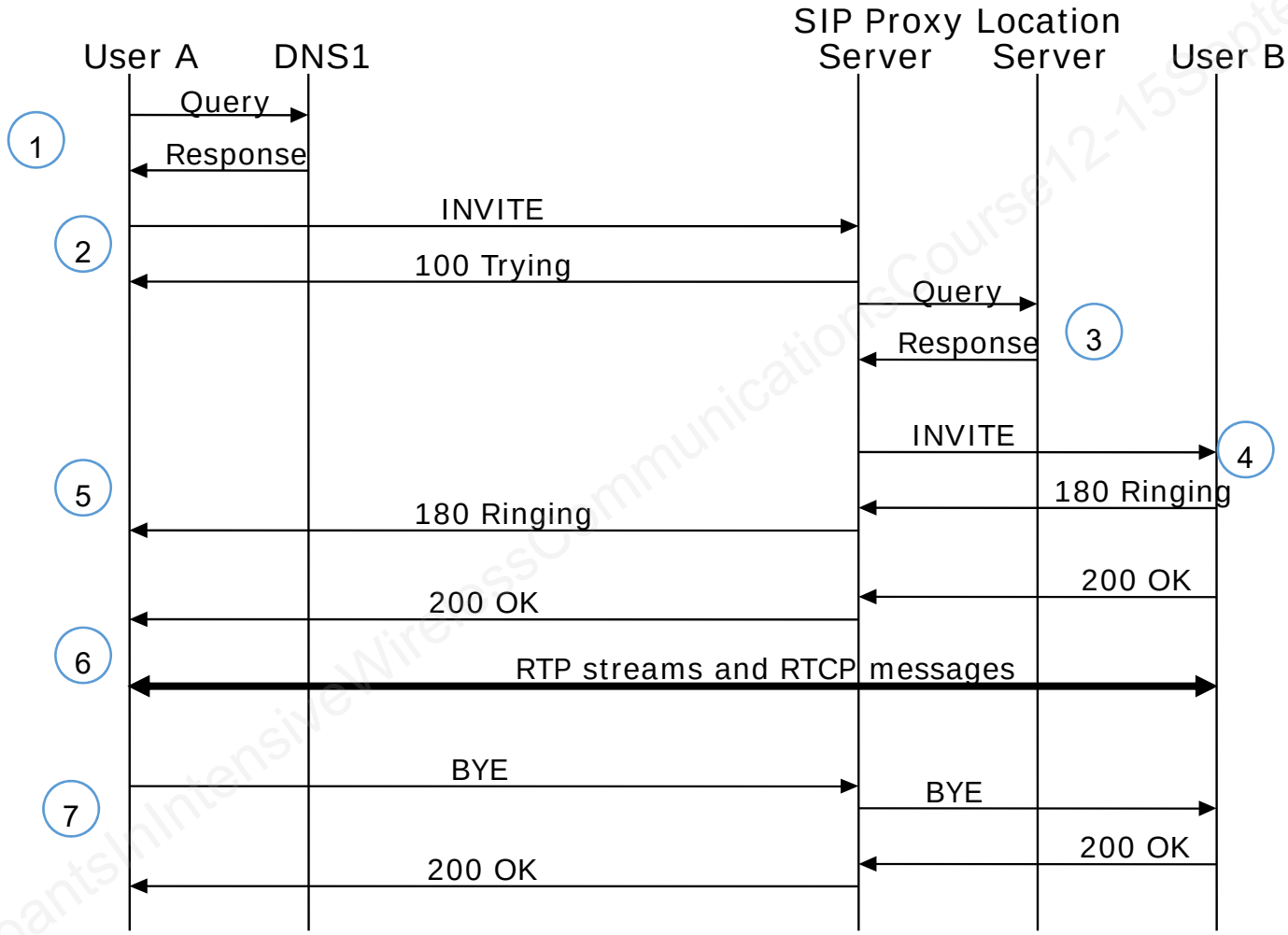
- Control signaling for sessions
  - Internet telephone, multimedia distribution, conferences
- Functions
  - Establishment of user location
  - Session establishment
  - Feature negotiation
  - Call management
- Associated protocols
  - RTP Real-time Transport Protocol
  - SDP Session Description Protocol



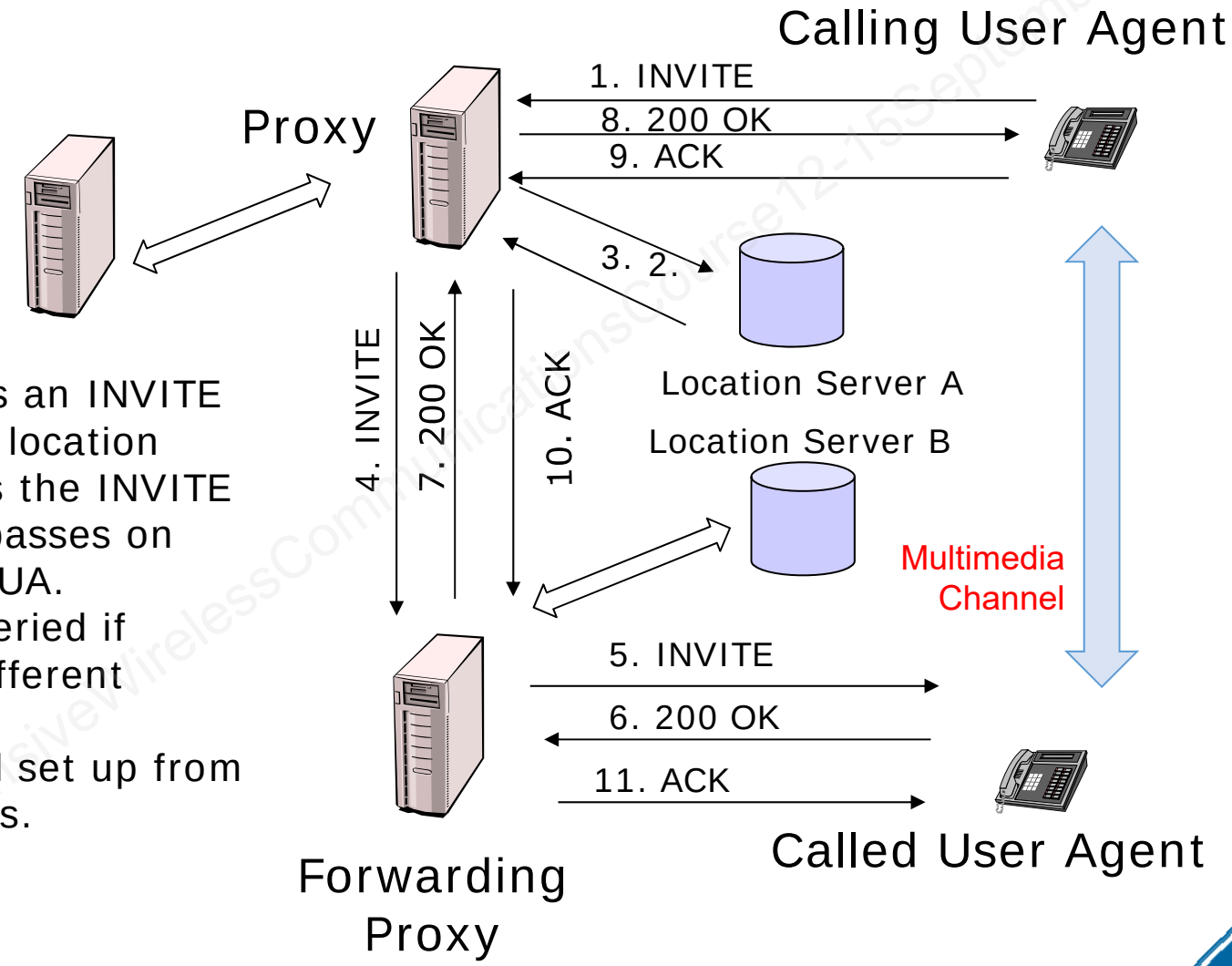
SIP Methods

- Basic Methods
  - INVITE initiates sessions
  - ACK confirms session establishment
  - BYE terminates sessions
  - REGISTER binds permanent address to current location
  - OPTIONS – query user agent/proxy for functionality
  - CANCEL – abort earlier message, if it has not completed
- Extensions
  - INFO – transfer of mid-session information between endpoints
  - SUBSCRIBE – request notification of events
  - NOTIFY – inform subscriber of event occurrence
  - PRACK – Provisional reliable responses
  - COMET – Resource reservation confirmation

SIP Call Flow

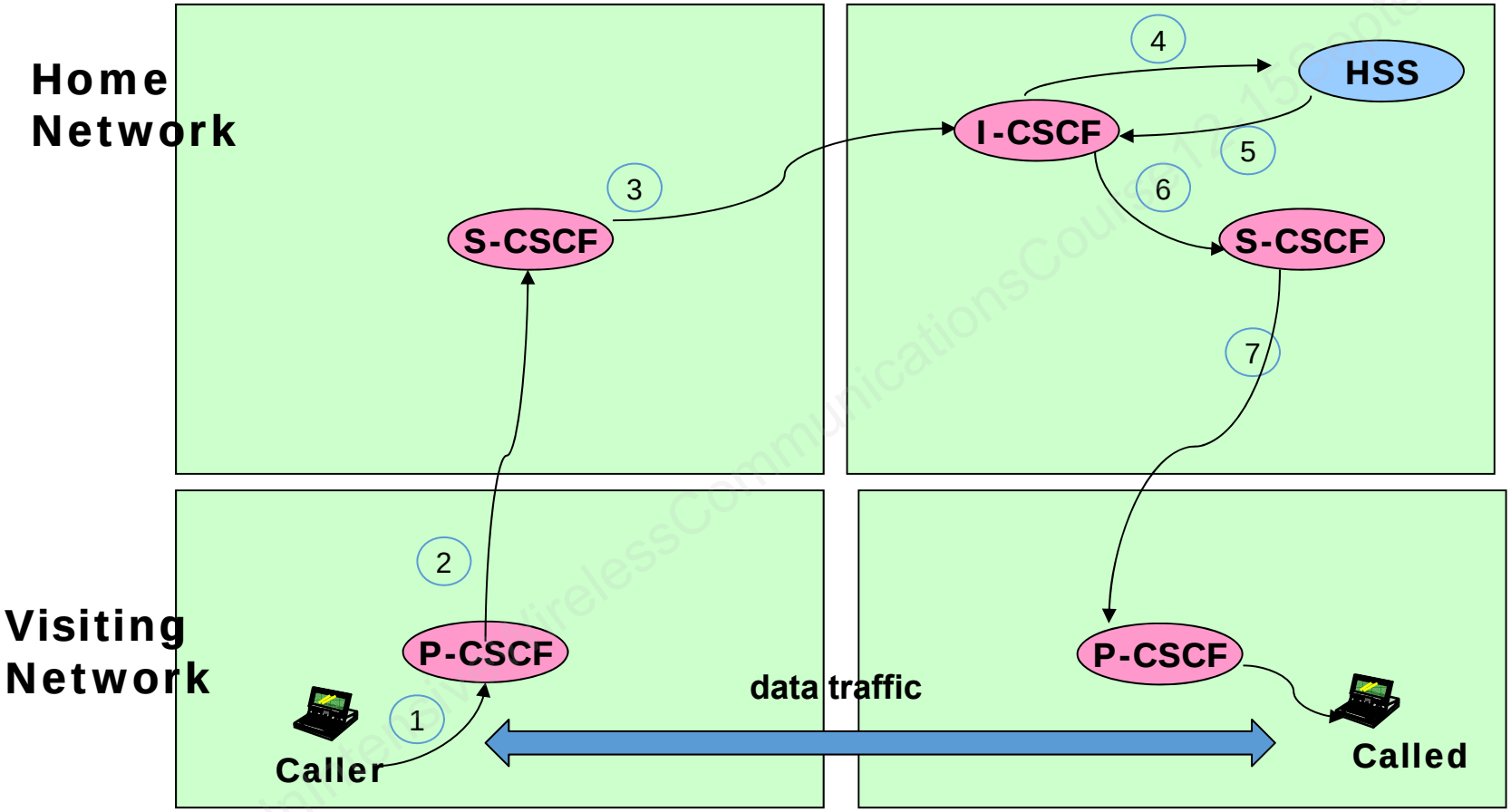


SIP Operation



- A User Agent sends an INVITE
- The Proxy consults location server and forwards the INVITE
- Forwarding Proxy passes on messages to called UA.
- Redirect Server queried if destination UA in different domain
- Multimedia channel set up from info in SIP messages.

IMS Signaling Example

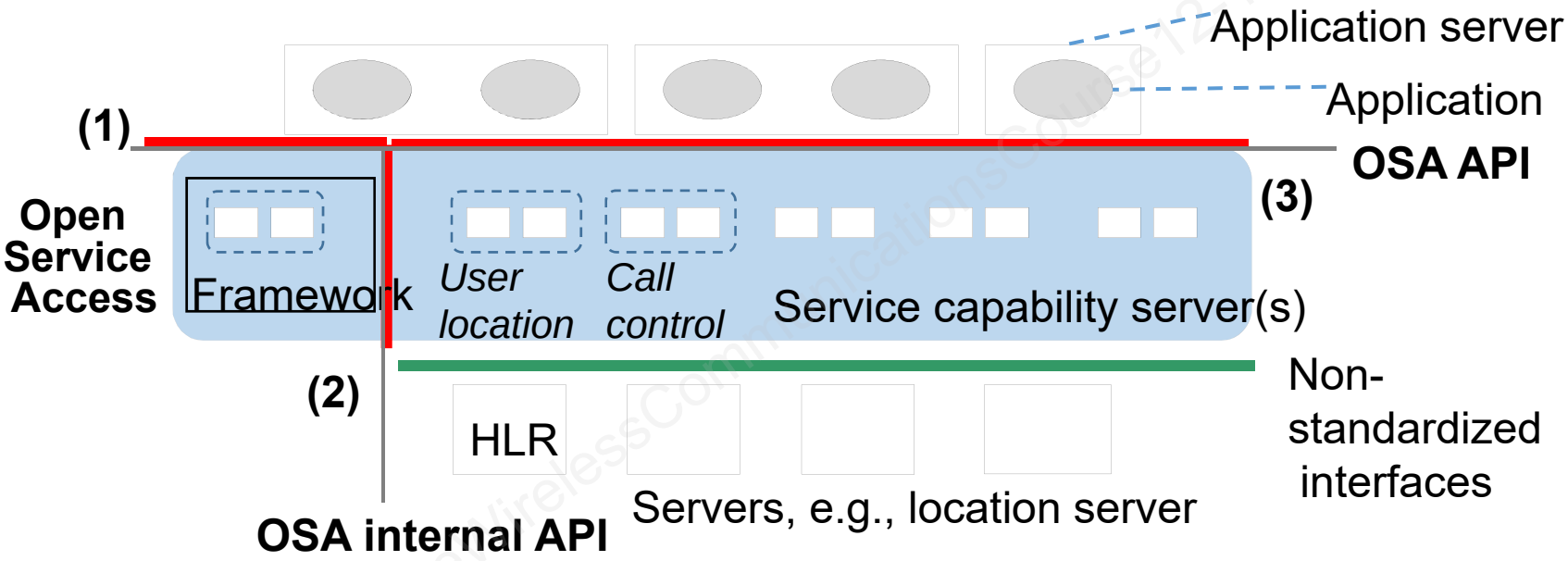


P-CSCF Proxy Call Session Control Function, Serving-CSCF, Interrogating-CSCF

OSA (Open Service Access)

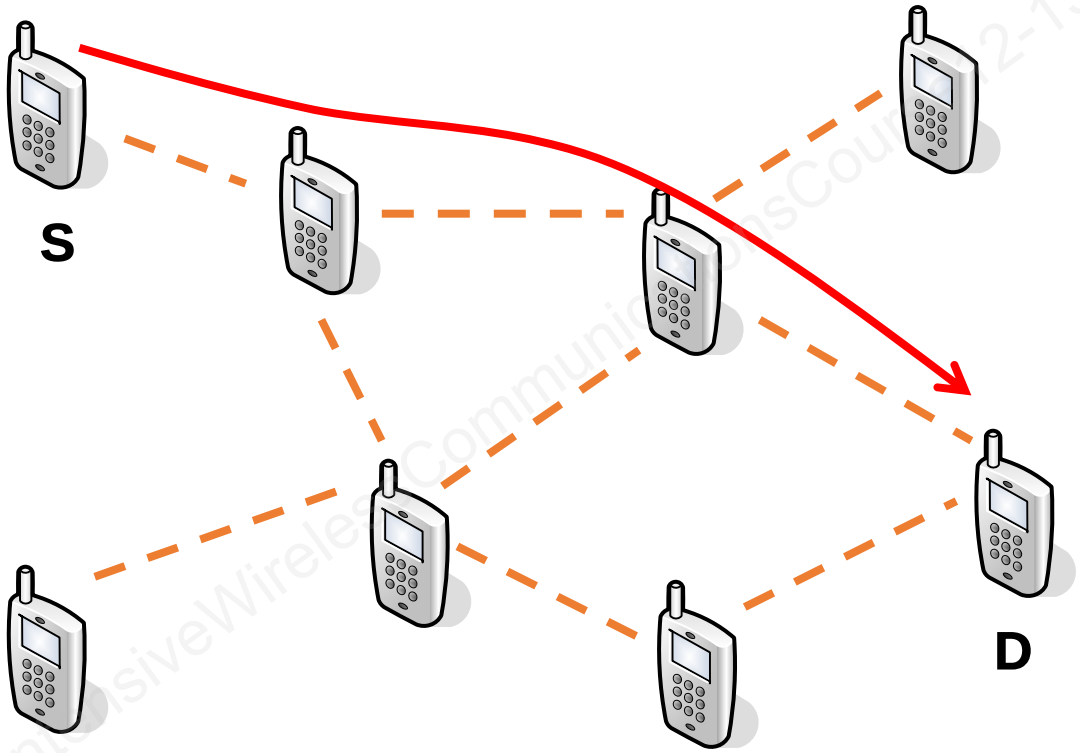
- OSA/Parlay is an open Application Programming Interface (API) for application access to telecoms network resources,
- Integrates telecom network capabilities with IT applications.
- Network independent.
- **Parlay X** (superceded by OneAPI) is a simplified web services interface to telecom network functionality.
- Includes comprehensive set of APIs for communications applications.

OSA Architecture: Overview



- Based on Parlay work
- Abstracts underlying network into service capabilities
- Framework SCS controls access and usage

Ad Hoc Networks: Finding a Path from Source to Destination



- Every node is a router

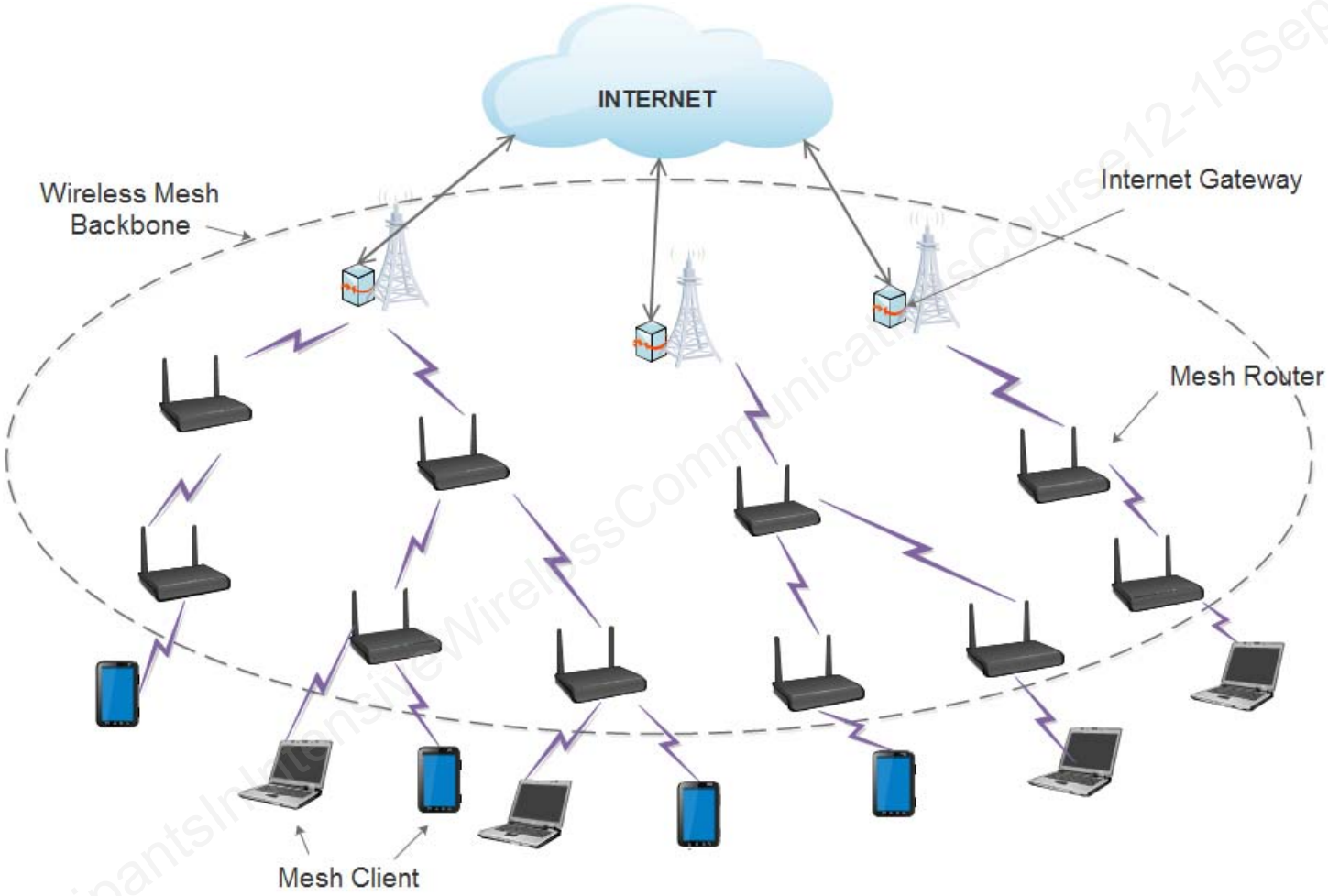
Ad Hoc Networks: Routing

- How to do routing?
  - Frequent movement, topology changes
    - "best" path from source to destination would keep changing
  - Power consumption considerations
    - Devices running on batteries
    - Minimize broadcasts, messages
- Pro-active vs. re-active routing protocols
  - Pro-active: maintain current routing table
  - Re-active: find paths on-demand
  - Hybrid: somewhere in between

Mesh Networks (1)

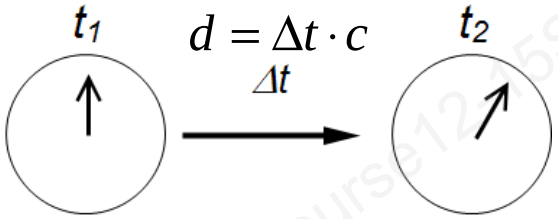
- Like ad hoc networks but for access network
  - Multi-hop
  - Not mobile, no power constraint
- Architecture
  - IGWs (Internet Gateways)
  - MRs (Mesh Routers): on top of tall buildings
  - MCs (Mesh Clients)
- “fully managed” vs. “community based”
- Deployment issues
  - Placement of IGWs, MRs

Mesh Networks (2)

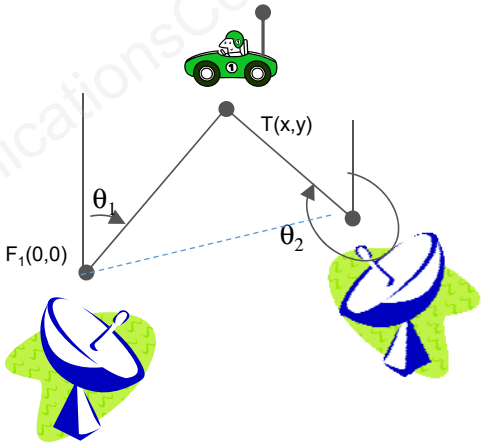


Location and Positioning Techniques

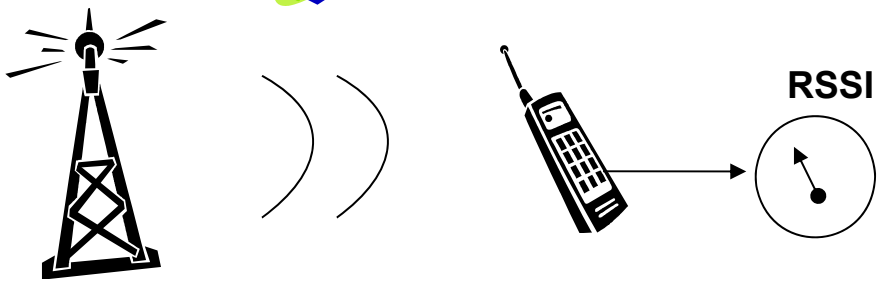
- Time of Flight (TOF)
  - Time of Arrival (TOA)
  - Time Difference of Arrival (TDOA



- Angle of Arrival (AOA)

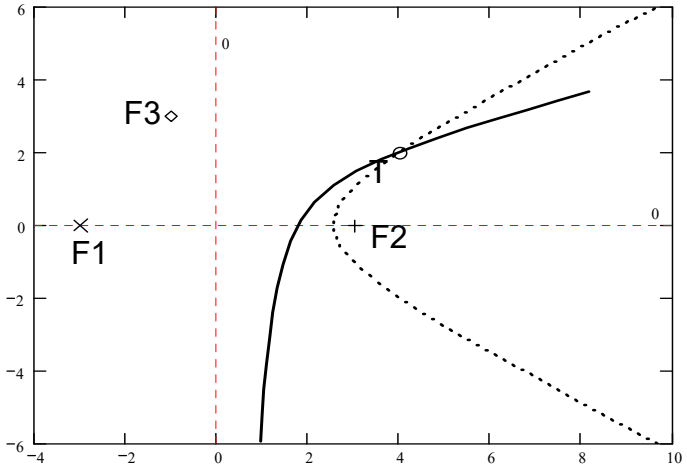


- Received Signal Strength (RSS)
  - Proximity
  - Pattern recognition (fingerprinting)



Cellular Network Location Methods

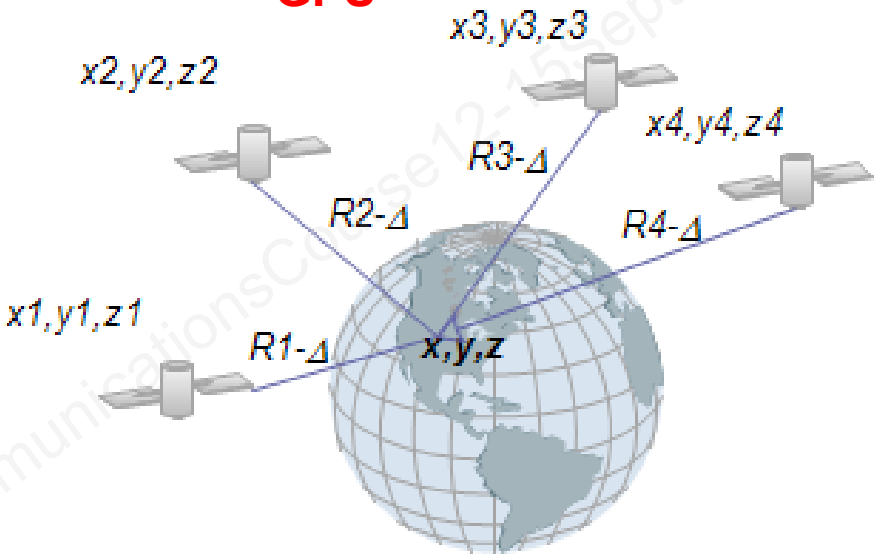
TDOA



$$\Delta_{1,2} = \sqrt{(y_1 - y)^2 + (x_1 - x)^2} - \sqrt{(y_2 - y)^2 + (x_2 - x)^2}$$

$$\Delta_{2,3} = \sqrt{(y_2 - y)^2 + (x_2 - x)^2} - \sqrt{(y_3 - y)^2 + (x_3 - x)^2}$$

GPS



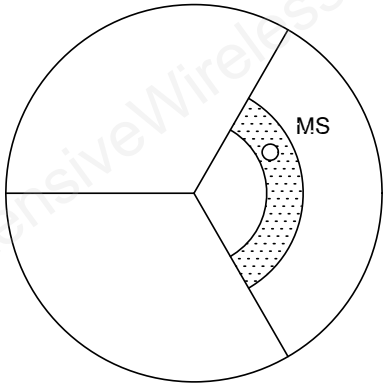
$$(R_1 - \Delta)^2 = (x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2$$

$$(R_2 - \Delta)^2 = (x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2$$

$$(R_3 - \Delta)^2 = (x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2$$

$$(R_4 - \Delta)^2 = (x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2$$

Enhanced Cell ID



Assisted GPS

Remote server provides

- Satellite selection, range, and range-rate
- Initial position and time estimate
- Precise satellite orbit and clock information
- Position computation

A-GPS results in

- Lower required device processing power
- Longer battery life
- Acquisition in poor environmental conditions
- Faster location acquisition

GPS vs. Terrestrial Cellular Location

GPS	Terrestrial
Very weak signals	Strong signals
Similar power from all satellites	Strong signal from serving BS, weaker from neighboring BS's
Close timing of all satellites	Base station timing sync not guaranteed
LOS required	NLOS – works in urban/indoor areas
3 dimensional	Usually 2 dimensional

LTE/LTE-A Positioning

Method	UE-based	UE-assisted	eNB- assisted	3GPP Release
A-GNSS	Yes	Yes	No	Rel 9
Downlink (OTDOA)	No	Yes	No	Rel 9
Enhanced Cell ID	No	Yes	Yes	Rel 9
Uplink (UTDOA)	No	No	Yes	Rel 11
Barametric, WLAN, Bluetooth, TBS	No	Yes	No	Rel 13

TBS Terrestrial Beacon System

Practice Questions (4)

1. True or False: IMS provides defined user services to the LTE packet switched cellular network.
2. True or False: SIP is responsible for voice stream transport.
3. Which of the following is **not** an ad hoc network
   a) MANET
   b) WMN
   c) WSN
   d) Wi-Fi hot spot
4. True or False: A dynamic routing table is not required in a fixed ad hoc network with static nodes.

Network Management & Security

Knowledge related to fault, configuration, account, performance, maintenance, security management, management availability, and operation support systems.

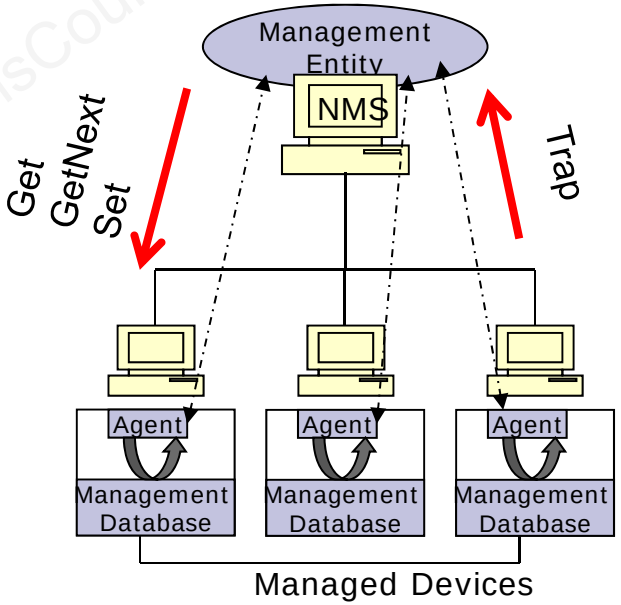
Network Management

- Simple Network Management Protocol
- Remote Monitoring
- Network Management Attributes
- FCAPS Framework
- Fault Management
- Configuration and Inventory
- Accounting
- Performance
- Self Organizing Network

SNMP

Basic Components
- Managed device
- Agent
- Network-managed system (NMS)

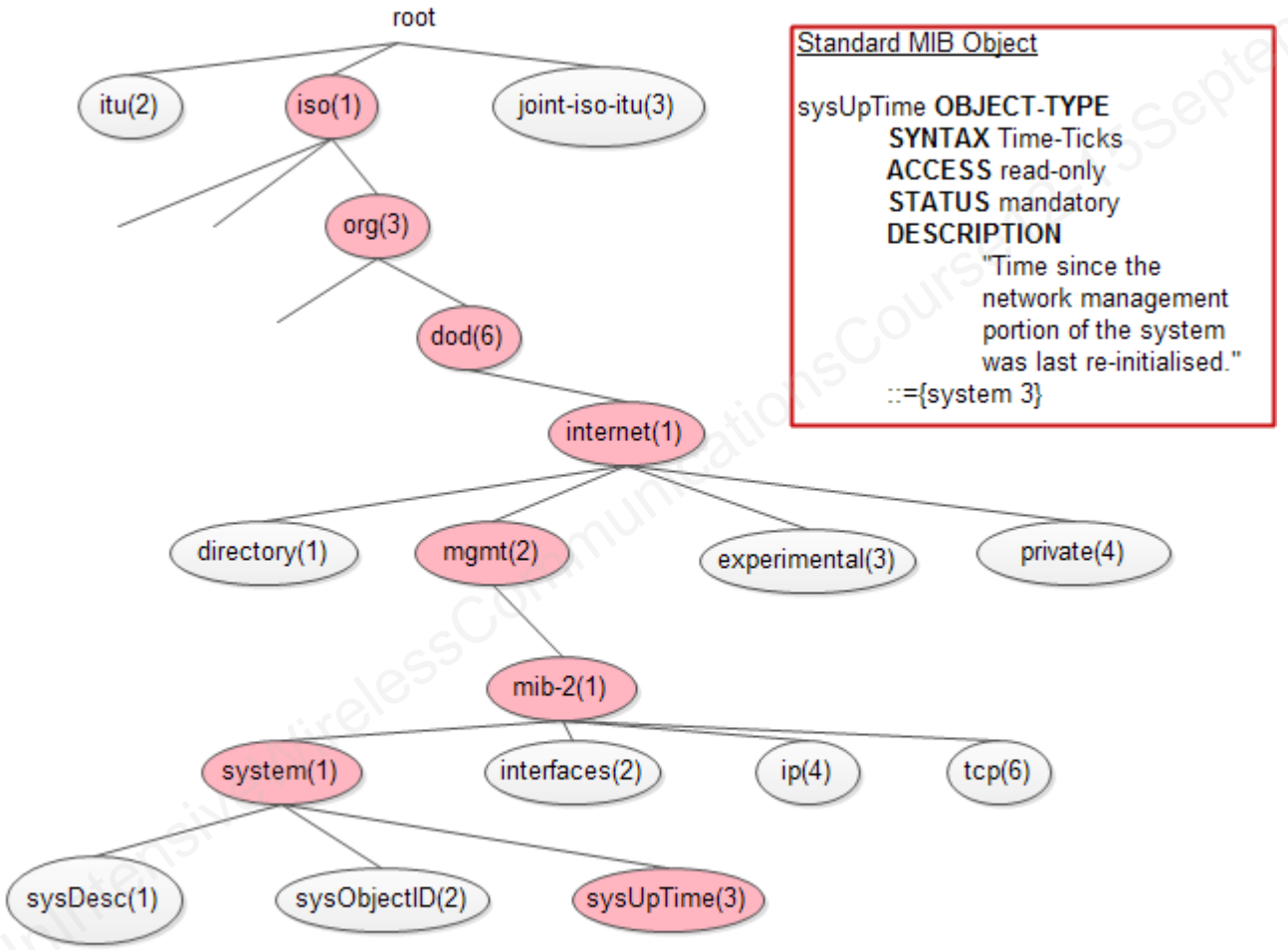
Protocol Operations
- Get: *retrieve value*
- GetNext*: retrieve next value*
- Set*: set value*
- GetResponse*: agent's response*
- Trap*: change of state or alarm*
- GetBulk*: retrieve large data blocks (v2)*



(Source: Cisco)

SNMP-Simple Network Management Protocol

Management Information Base



Standard MIB Object

sysUpTime **OBJECT-TYPE**
SYNTAX Time-Ticks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Time since the network management portion of the system was last re-initialised."
::={system 3}

Object IDentifier (OID) 1.3.6.1.2.1.1.3

RMON

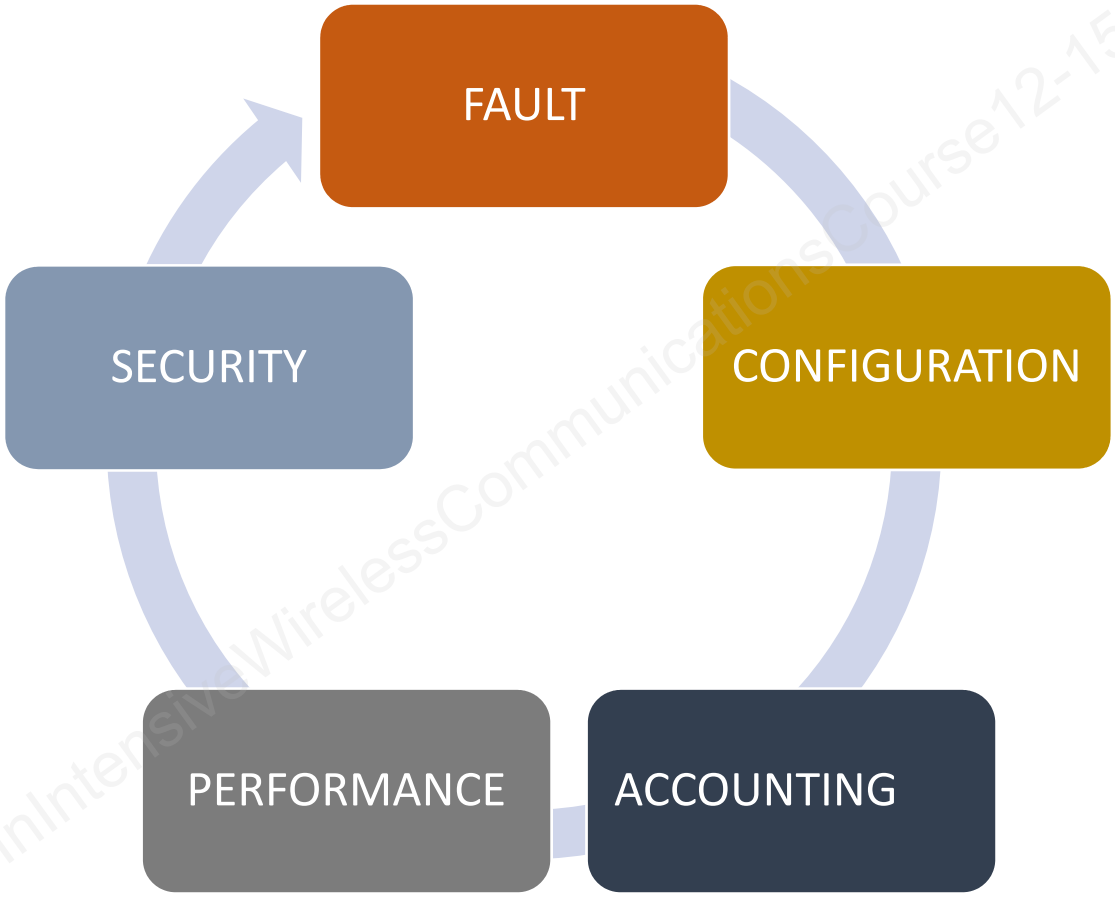
- Statistics about LAN traffic
  - MIB for individual devices
    - Traffic to and from individual devices
  - What about LAN as a whole?
  - Network monitors, network analyzers
- RMONv1: RFC 2819
  - Packet level statistics about LAN/WAN
- RMONv2: RFC 2021
  - Network-level, app-level statistics

ITU Telecommunications Management Network (TMN)

An operational framework to manage networks

- **Management Layers** – levels of abstraction (M.3010)
  - Functional
  - Physical
  - Informational
  - Logical
    - -Business Management (BML)
    - -Service Management (SML)
    - -Network Management (NML)
    - -Element Management (EML)
- **Management Functions** (M.3400): FCAPS
  - Fault Management (FM)
  - Configuration Management (CM)
  - Accounting Management (AM)
  - Performance Management (PM)
  - Security Management (SM)

Network Management - FCAPS



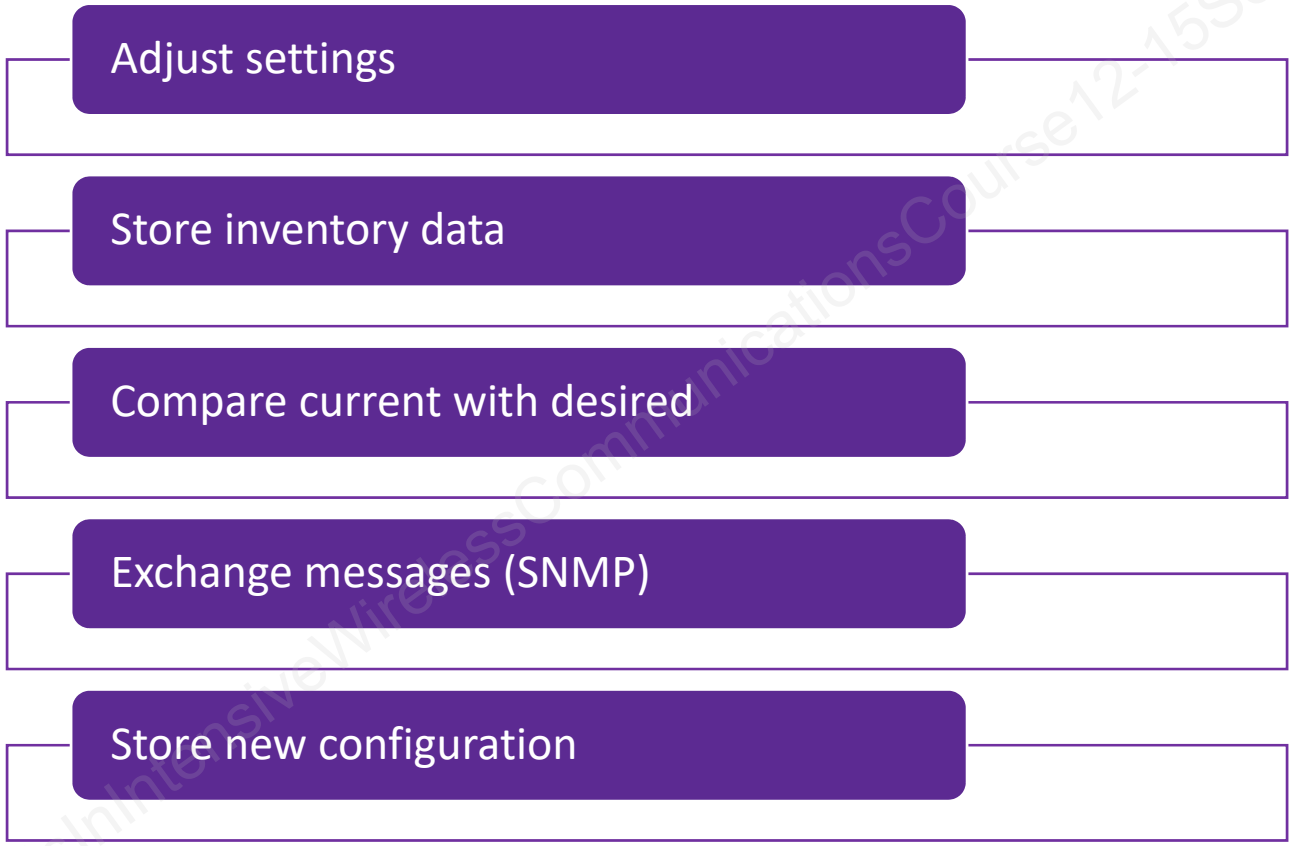
Fault Management (FM)

- Identify, locate, correct
- Inform management of problem
- Alarm and initiate troubleshooting
- Communicate with other functions
- Take immediate measures

FM Key Metrics

- Number of failures (quantity)
- Severity of the failure (critical, medium, etc.)
- Service impact (how the failure affects the customer)
- Downtime (time to fix the problem)
  - Of the network element
  - Of the service (if any)
- MTBF (mean time between failures)

Configuration and Inventory Management

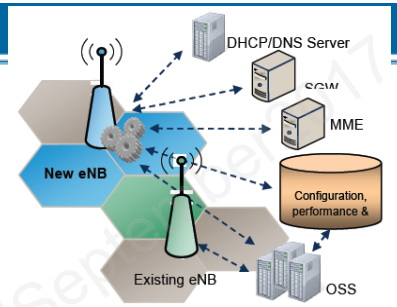


Self Organizing Network (SON)

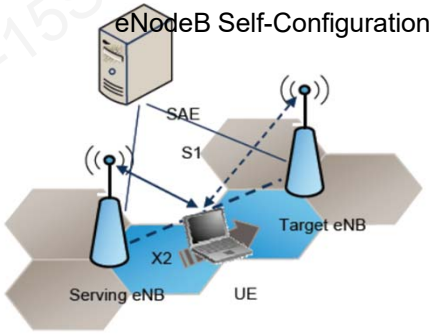
Self Configuration	• Plug and Play installation of new nodes • Automatic connectivity establishment • Self test
Self Optimization	• Handover parameter optimization • Load balancing
Self Healing	• Automated fault management • Outage detection

Operational Efficiency & SON in LTE

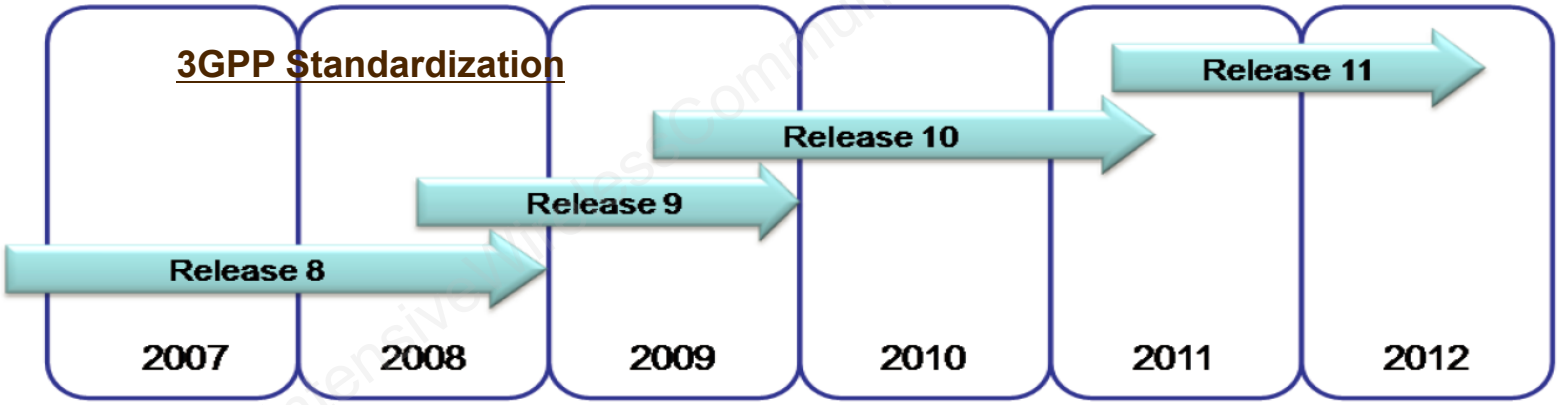
Self-Organizing Networks (SON) - New environment with Operational Efficiency paradigms – Automation, standardization, simplification & unification of functions, plus real-time use of abundant network knowledge



eNodeB Self-Configuration



Automatic Neighbour Relation



Self-Configuration Initial Phase, e.g. Automatic inventory, automatic S/W download, automatic neighbour relation (ANR), automatic physical cell ID assignment

Self optimization: Load balancing, Mobility robustness/handover optimization, inter-cell interference coordination (ICIC)

Adv Self-Configuration, (Real-time) Self-Optimization, Capacity and Coverage Optimizations, Self-Healing, Energy Savings, Test Drive Minimization, Cell Outage Detection and Compensation, enhanced ICIC

Accounting Management

- Collect and send security information
- Track user services and used resources

Performance Management (PM)

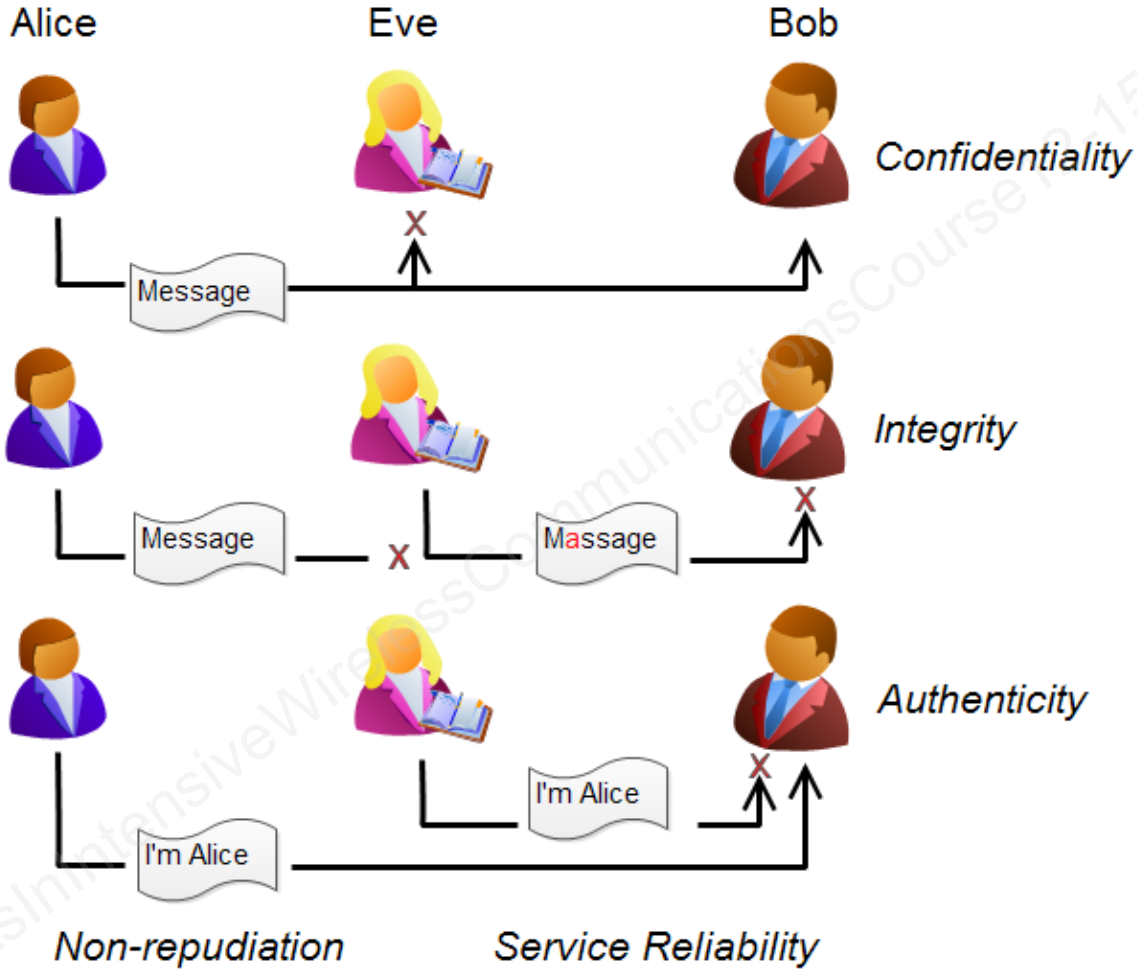
Security Management

- Identify information source to be protected
- Monitor access points
- Define attack impact
- Identify current attacks
- Log and report

Security

- Basic concepts
- Wireless security
- Wi-Fi security
- Cellular security
  - GSM, UMTS, LTE

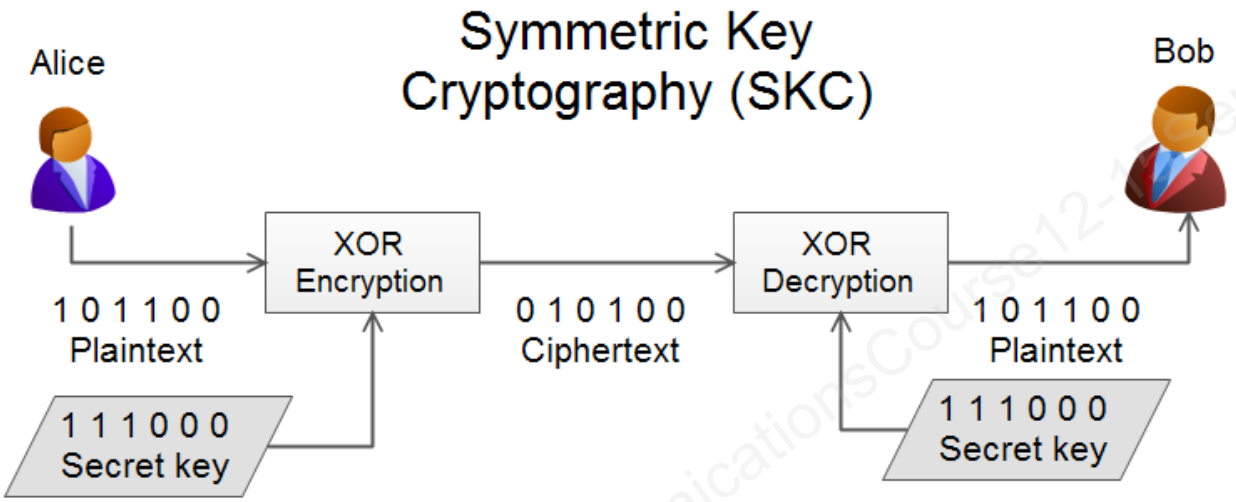
Security Concepts

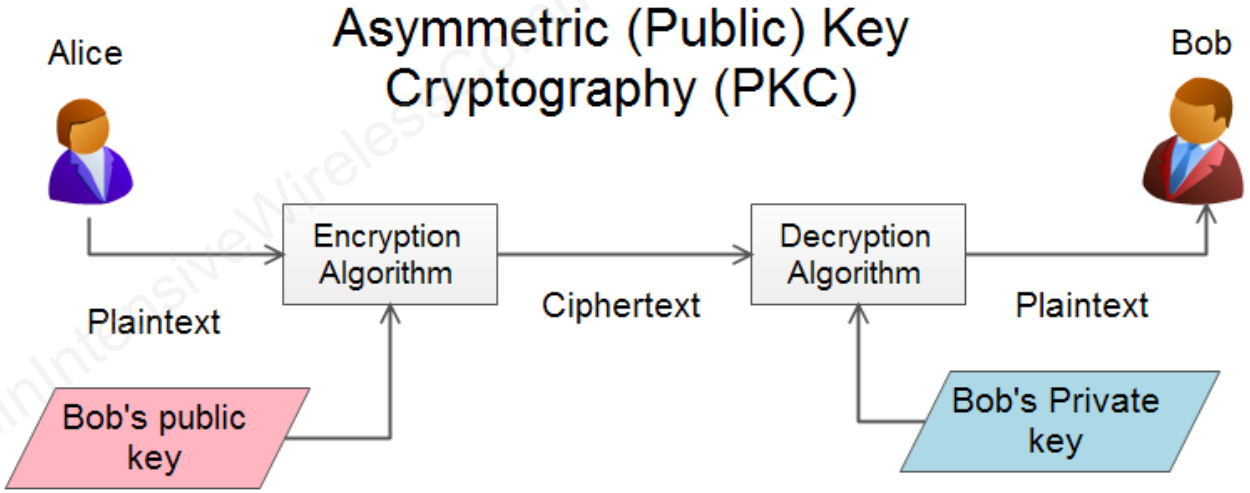


Security Threats and Protection

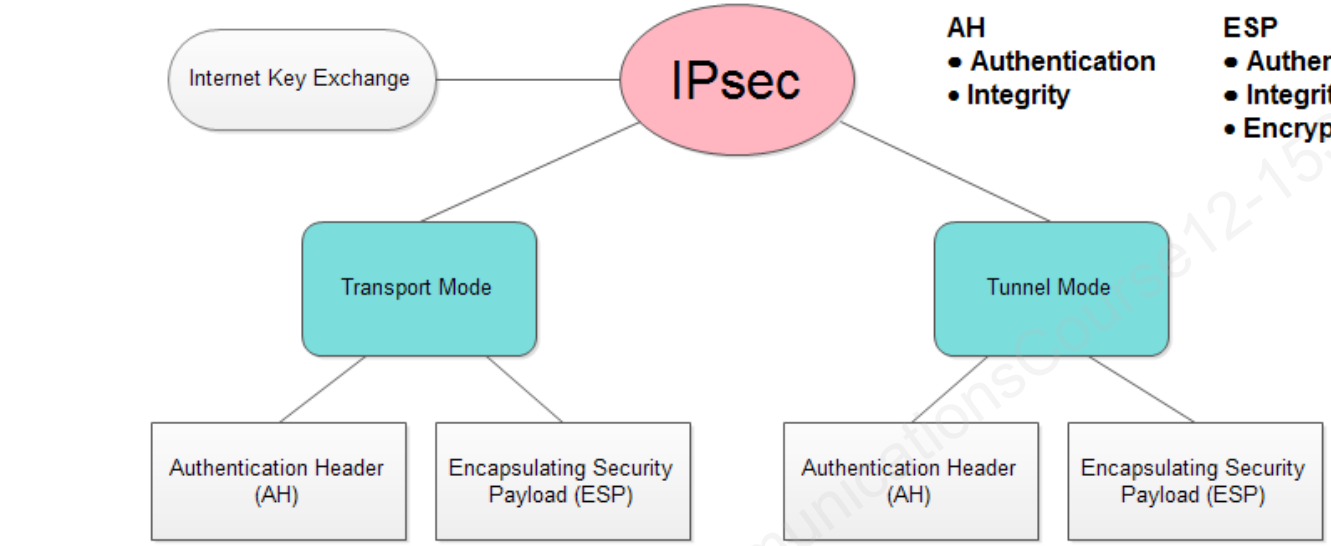
Threat	Category	Countermeasure
Denial of service	Service Reliability	Multiple resources, source tracing
Eavesdropping	Confidentiality	Encryption
Man-in-the-middle	Authentication, confidentiality	Authentication, encryption
Masquerading	Authentication	Authentication
Message modification	Integrity	Hash function
Message replay	Authentication	Time stamp, session numbering
Traffic analysis	Confidentiality	Steganography

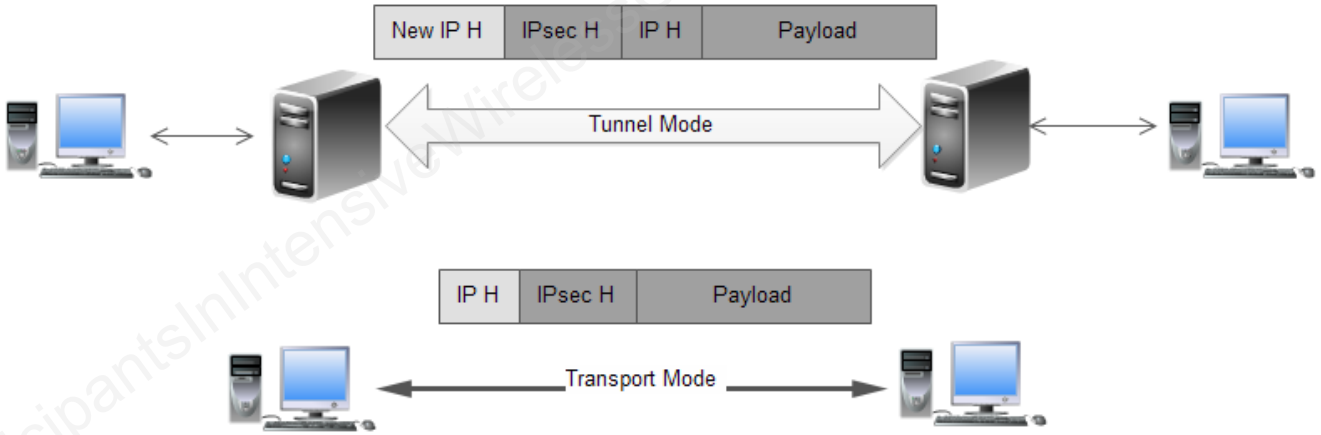
Symmetric and Asymmetric Keys



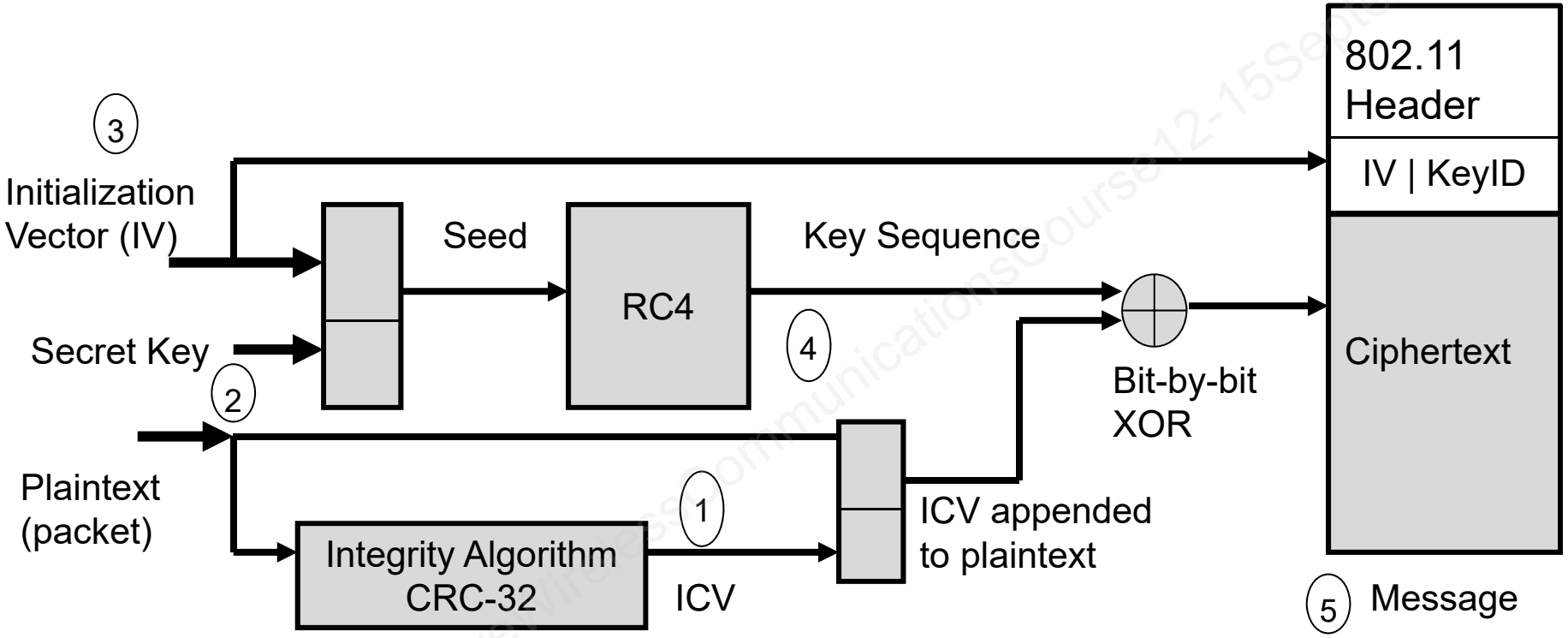


IP Security





Wi-Fi Security: WEP



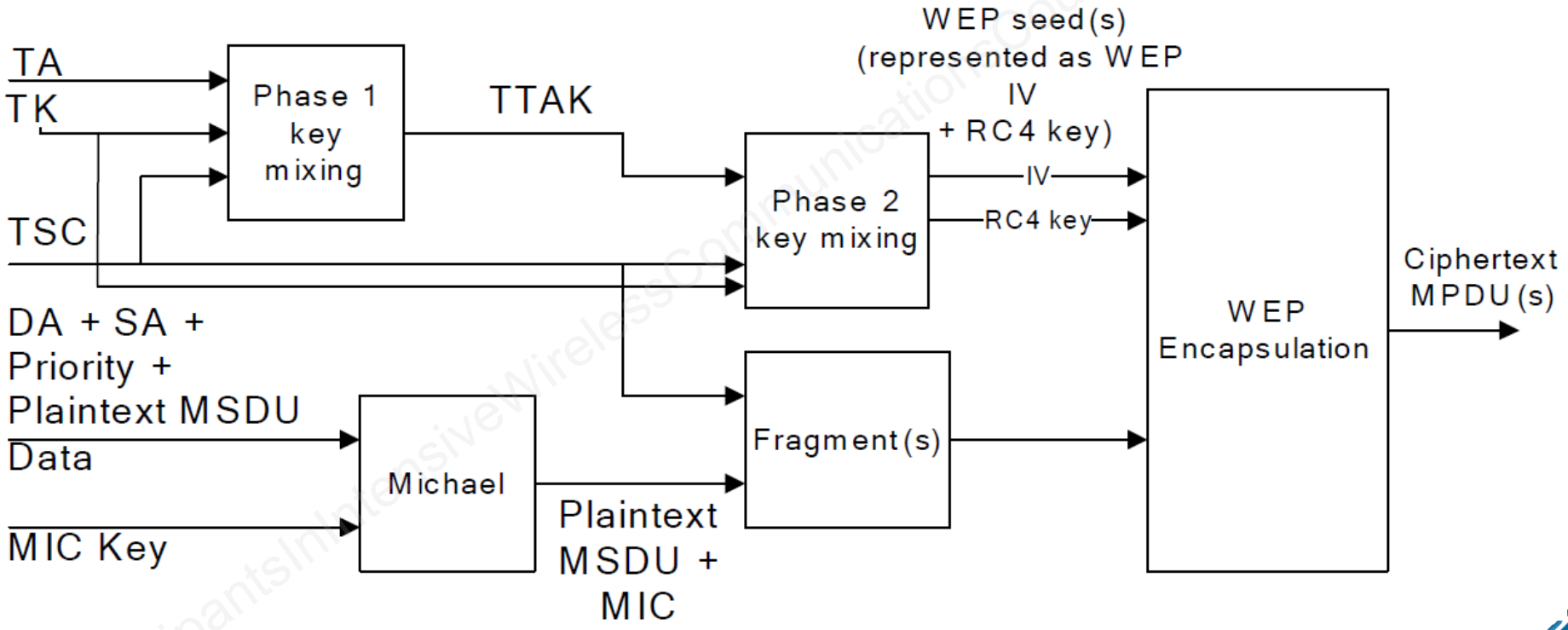
RC4 Stream cipher generator
ICV Integrity Check Value
CRC Cyclic Redundancy Check

Wi-Fi Security: WPA1

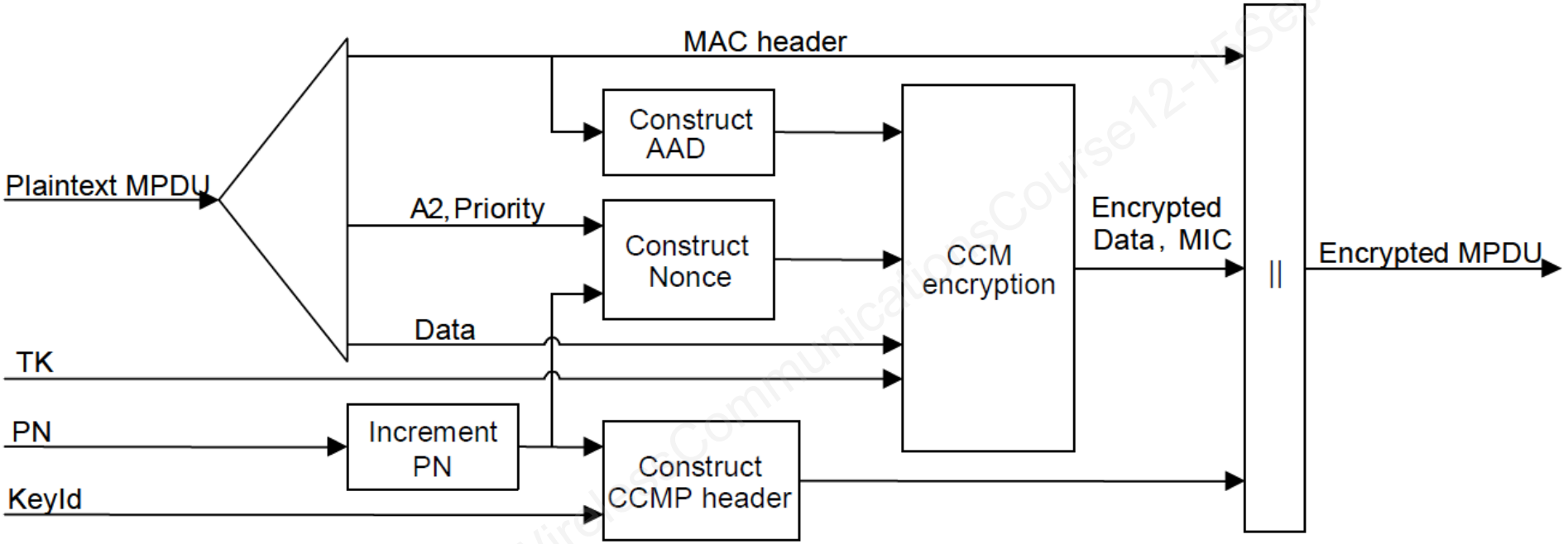
TA: transmitter address
TK: transient key
TSC: TKIP sequence counter (IV)

TTAK: TKIP-mixed transmit address and key
MIC: message integrity code
DA: Destination Address

SA: Source Address
MSDU: MAC Service Data Unit
MPDU: MAC Protocol Data Unit



Wi-Fi Security: WPA2 or 802.11i

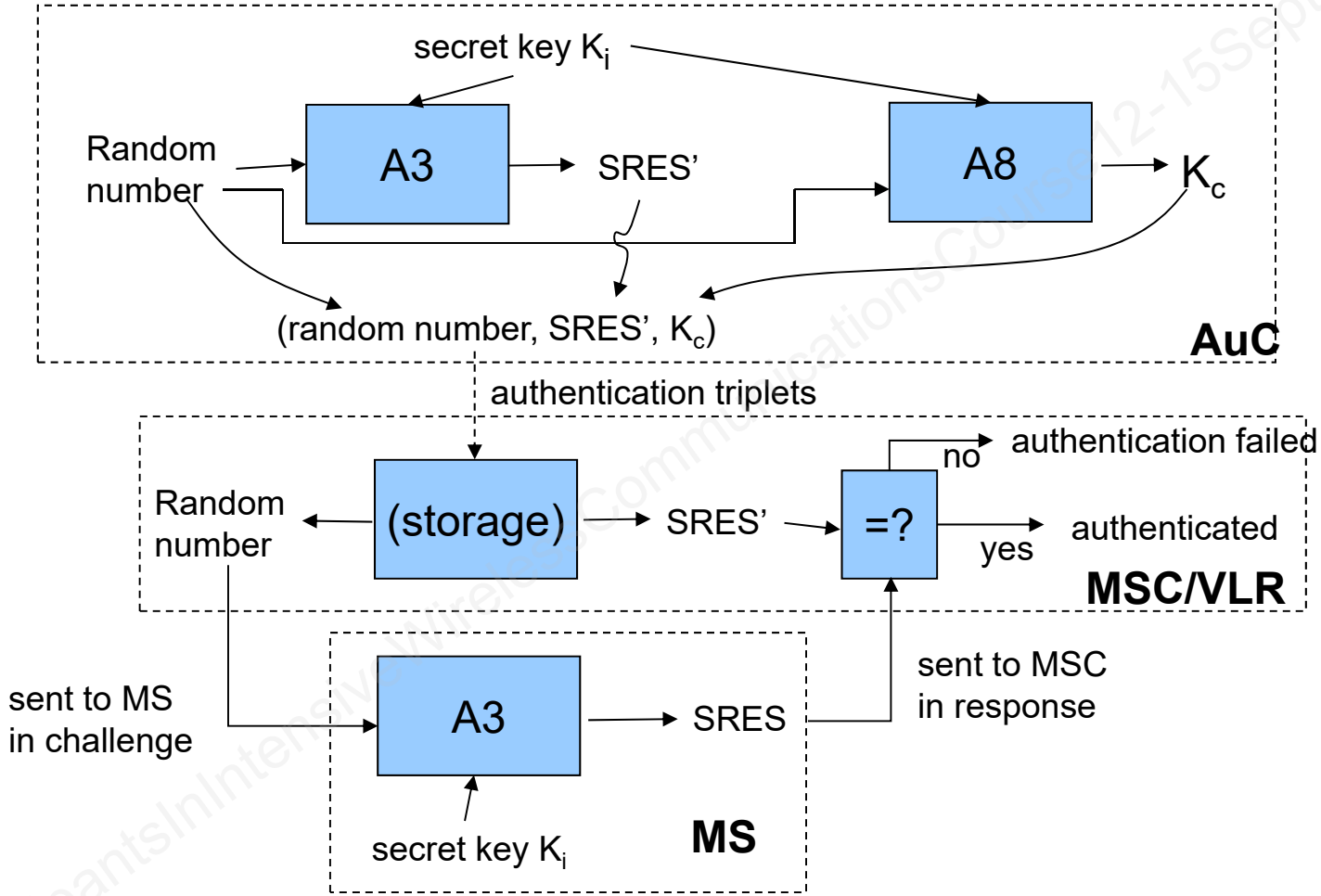


AES-CCMP : Advanced Encryption Standard Counter-mode CBC-MAC Protocol

TK=Transit key
PN=Packet Number
KeyId= Key ID
AAD=Additional Authentication Data
A2=Source Address

Priority (reserved field)
CCM=Counter with CBC-MAC (Cipher Block Chaining with Message Authentication Code)
MIC=Message Integrity Code

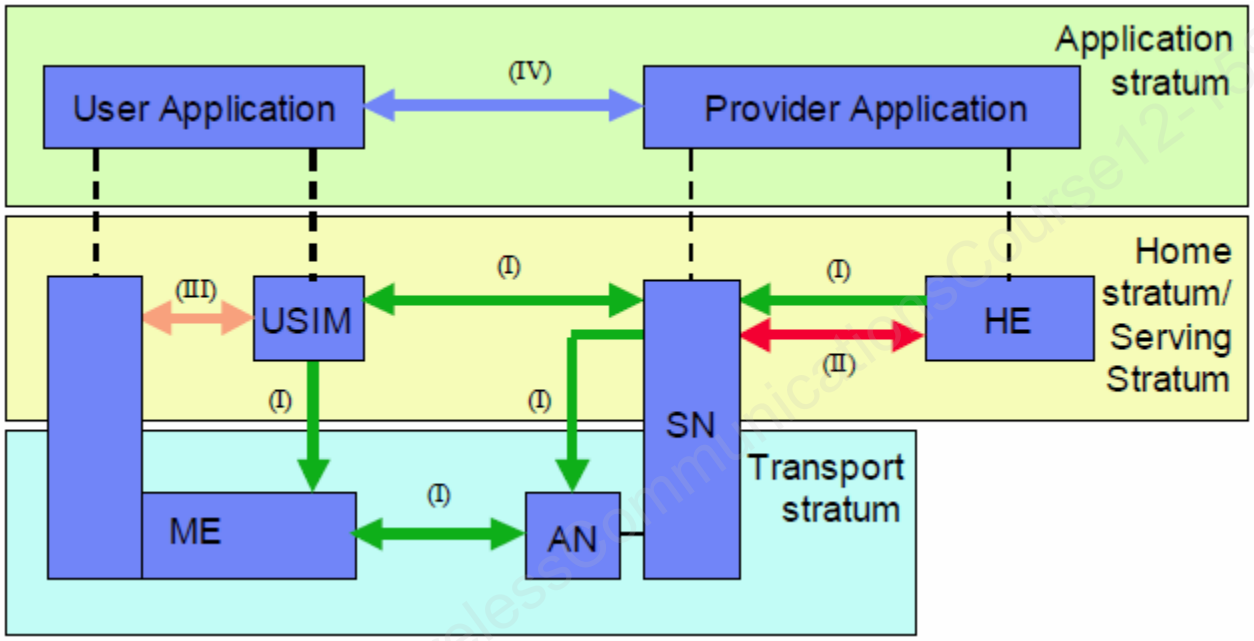
GSM Authentication



GSM Security Problems

- Lack of integrity protection of data or messages
- Limited encryption scope: MS-BTS only
- Session key K_c is small, effectively 54 bits
- One way authentication: network verifies subscriber but not the opposite
- Possibility of SIM cloning

UMTS Security Architecture

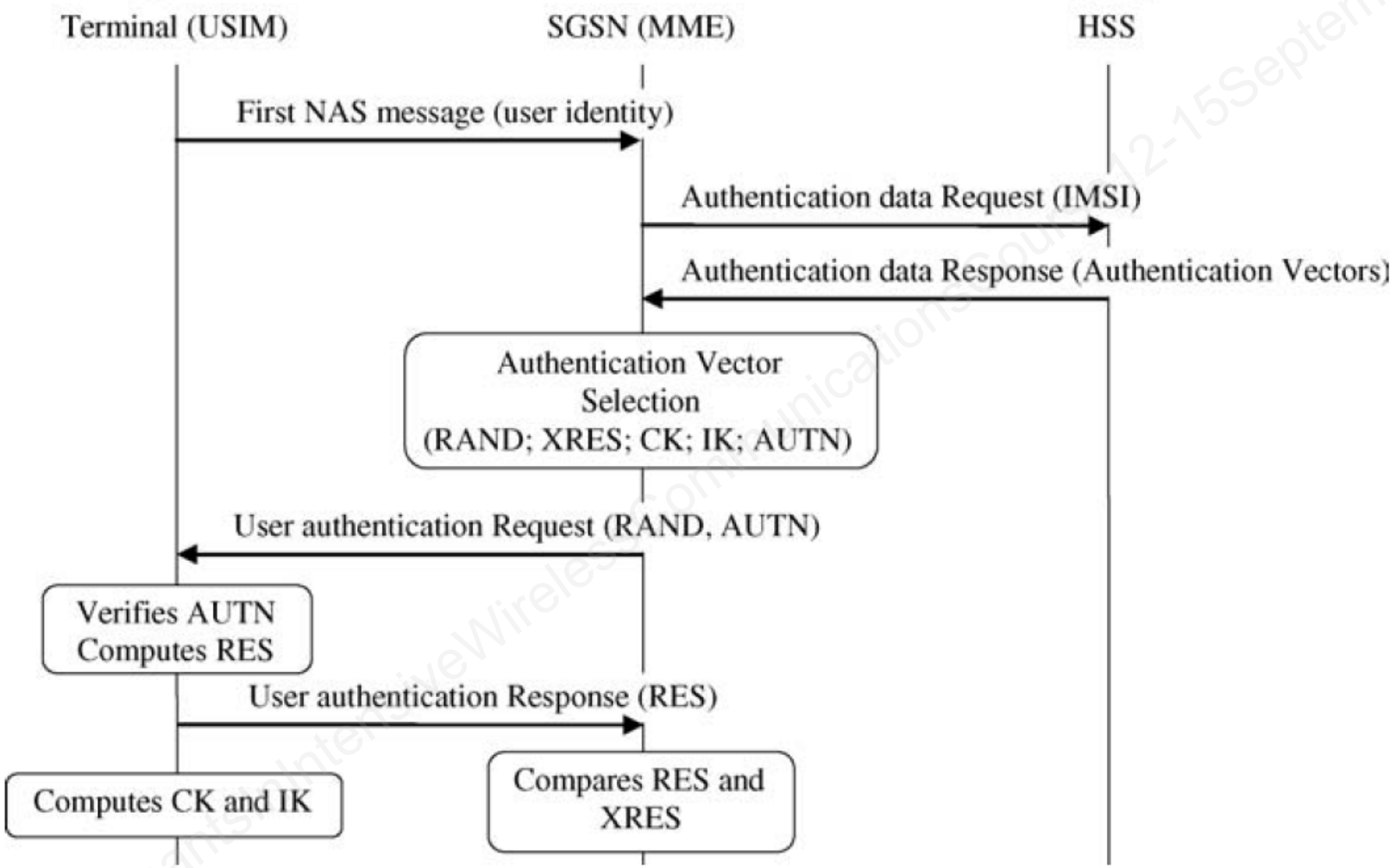


USIM universal subscriber identity module
ME mobile environment
HE home environment
AN access network
SN serving network

UMTS Network Access Security

- Adapts GSM security features to insure interoperability
- Provides mutual MS-network authentication
- Reduces MS identity and location exposure
- Extends encryption to RNC (Radio Network Controller)
- Integrity protection for signaling data
- Cipher (and integrity) key length 128 bits (GSM 54)
- Improved protection against fraud

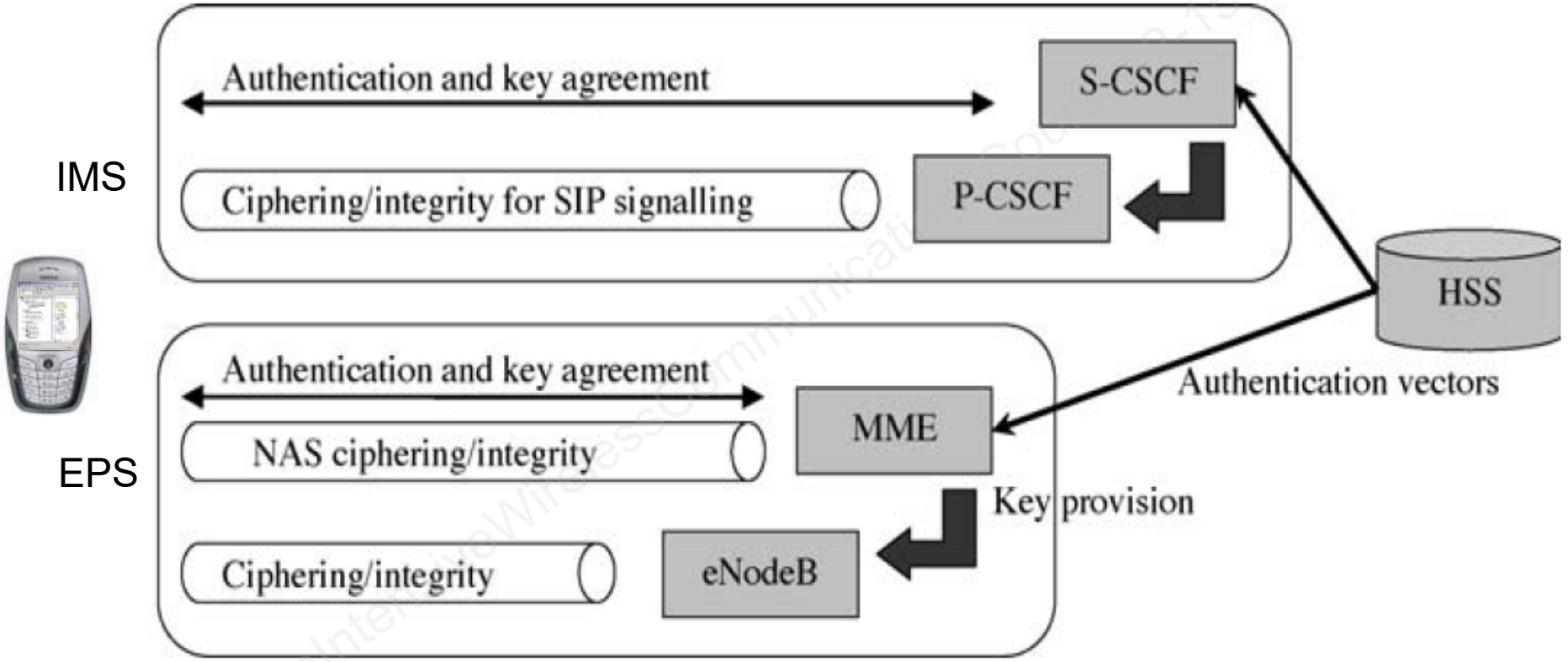
UMTS/LTE Authentication



LTE Security Changes

- Hierarchal key system
- Separation of security functions for NAS (Non-Access Stratum) and AS (Access Stratum)
- Forward Security concept
- Additional security functions for 3G< >LTE

LTE Security



Practice Questions (5)

1. True or False: Encrypting a message automatically assures its integrity.
2. True or False? The AH header of IPsec does not prevent eavesdropping.
3. Real time alarm monitoring in SNMP is accomplished through which protocol command:
   a) Get
   b) Set
   c) Get response
   d) Trap
4. Which feature is new in WPA2?
   a) one-time key sequence
   b) no repetition of Initiation Vector
   c) Michael integrity check instead of CRC-32
   d) AES encryption.

Infrastructure and Wireless Communication

Specification, design, implementation, and operation of facilities and sites.

IEEE ComSoc IEEE Communications Society

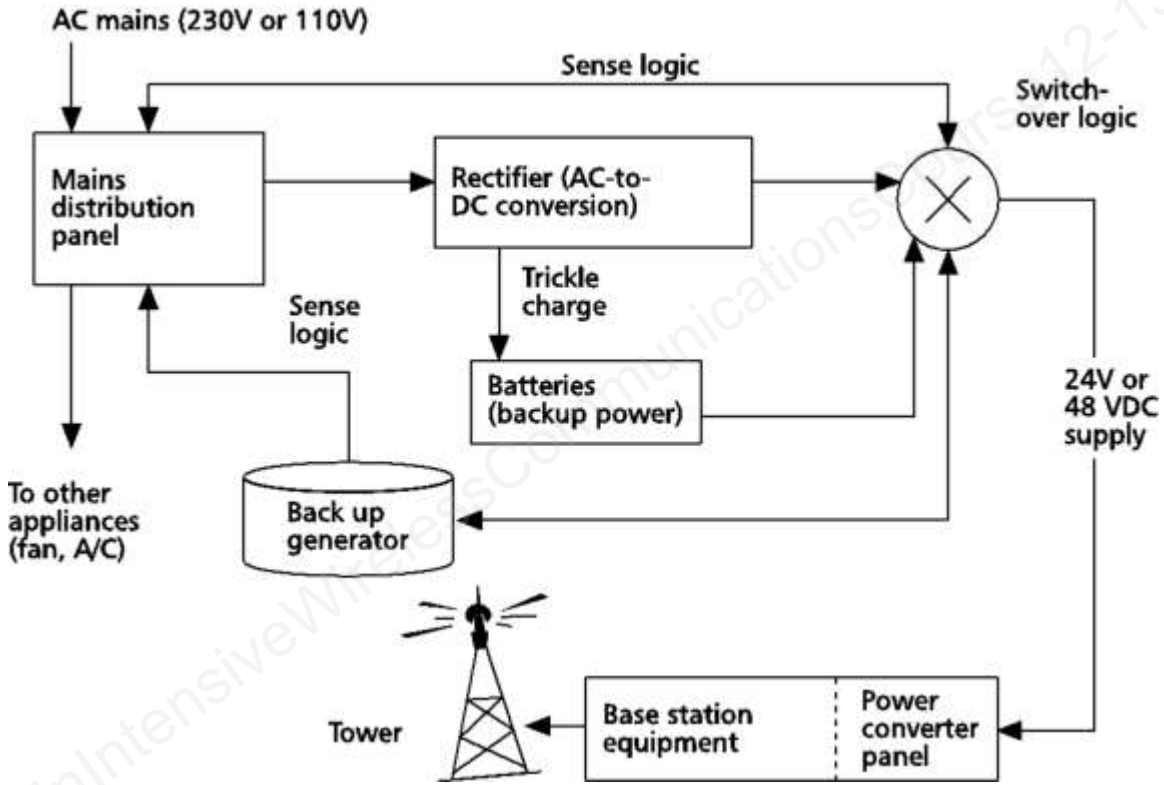
IEEE

Facilities Infrastructure

- Power supplies
- Electrical Protection
- Heating, ventilation and air-conditioning (HVAC)
- Equipment racks
- Waveguides and cables
- Tower requirements
- In-building wireless
- Physical security

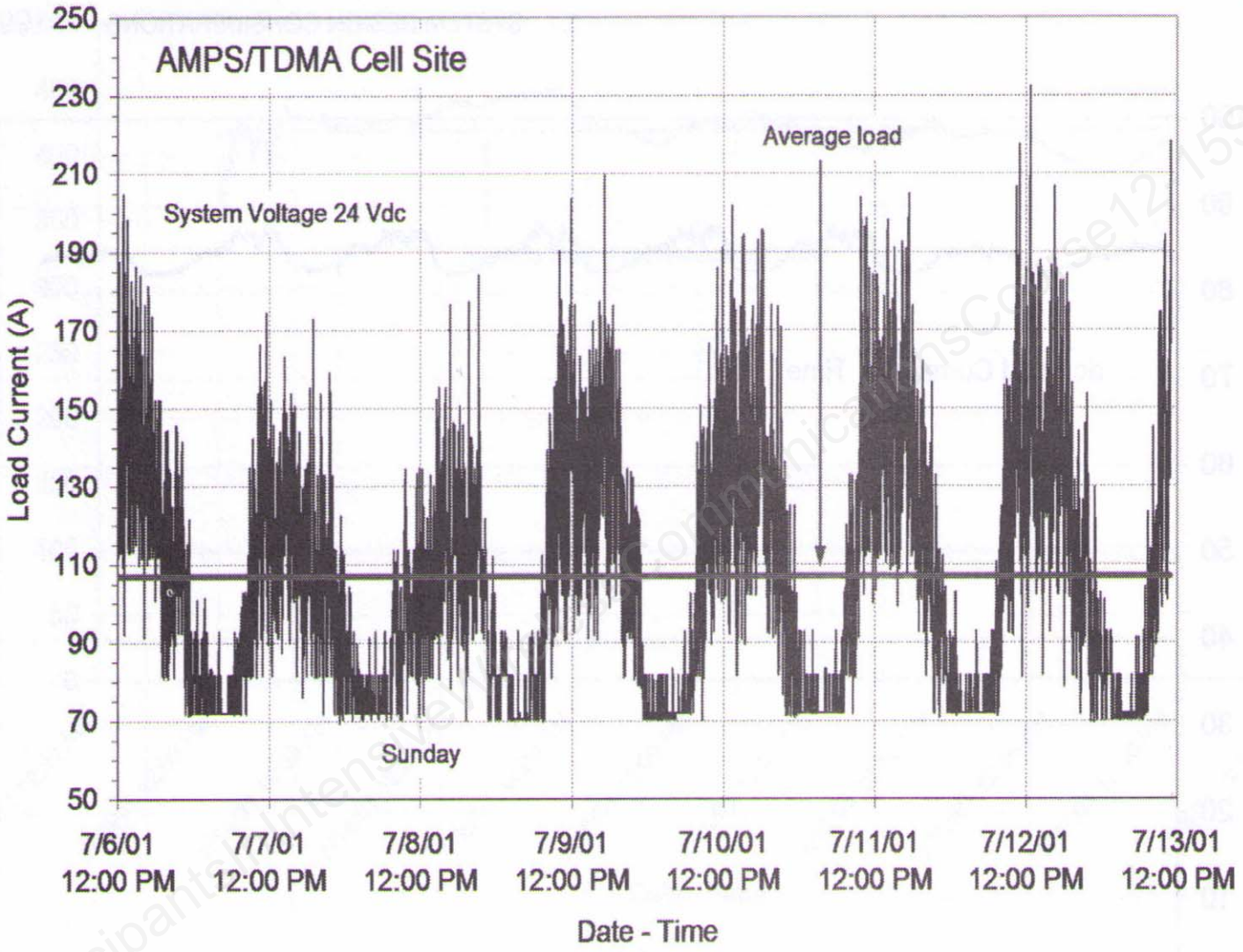
Power Supplies

Base station power system with backup

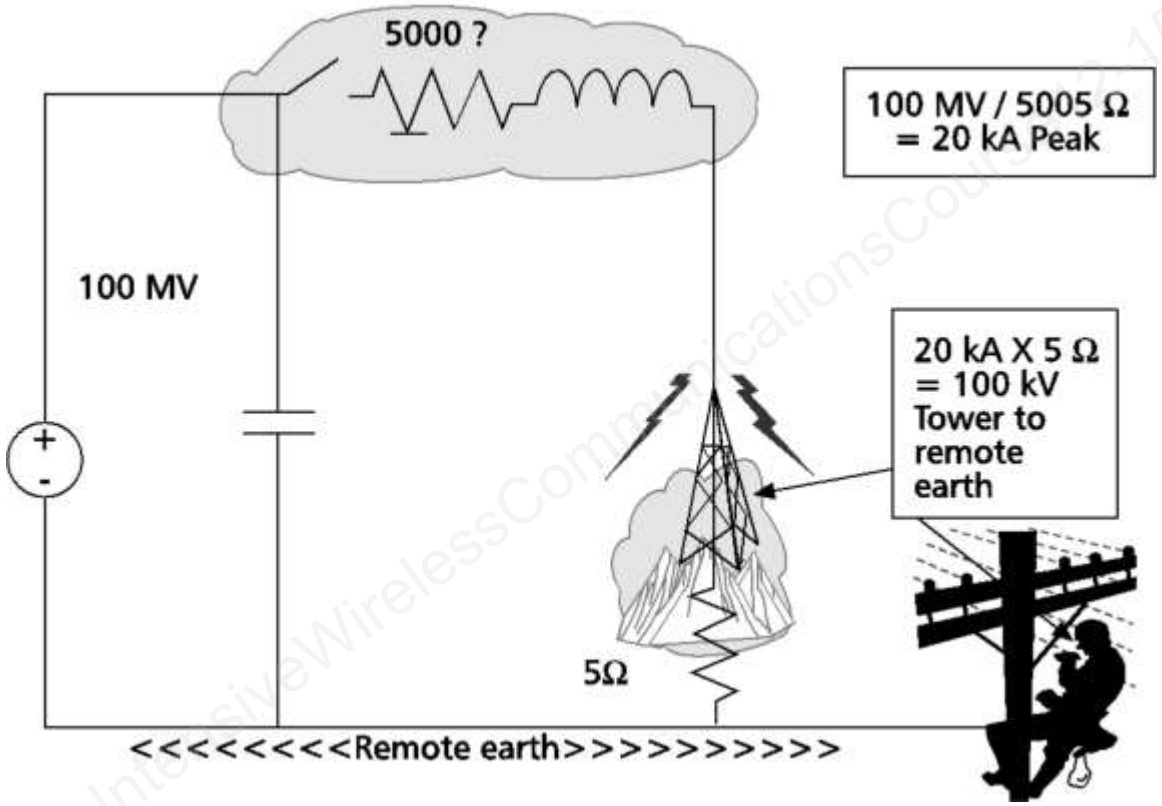


from IEEE ComSoc "A Guide to the Wireless Engineering Body of Knowledge (WEBOK)

AC & DC Power Systems: BS Example

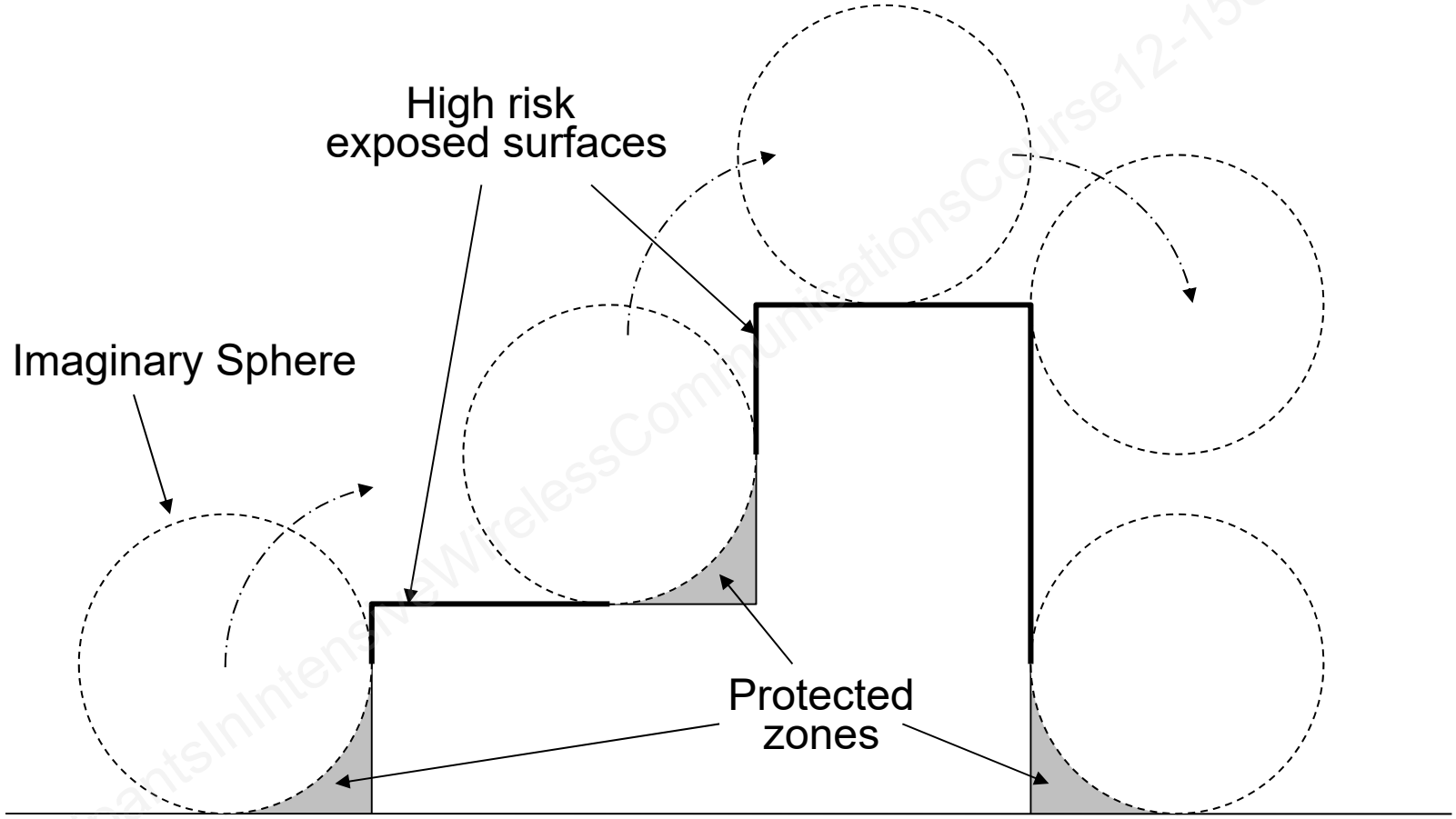


Electrical Protection

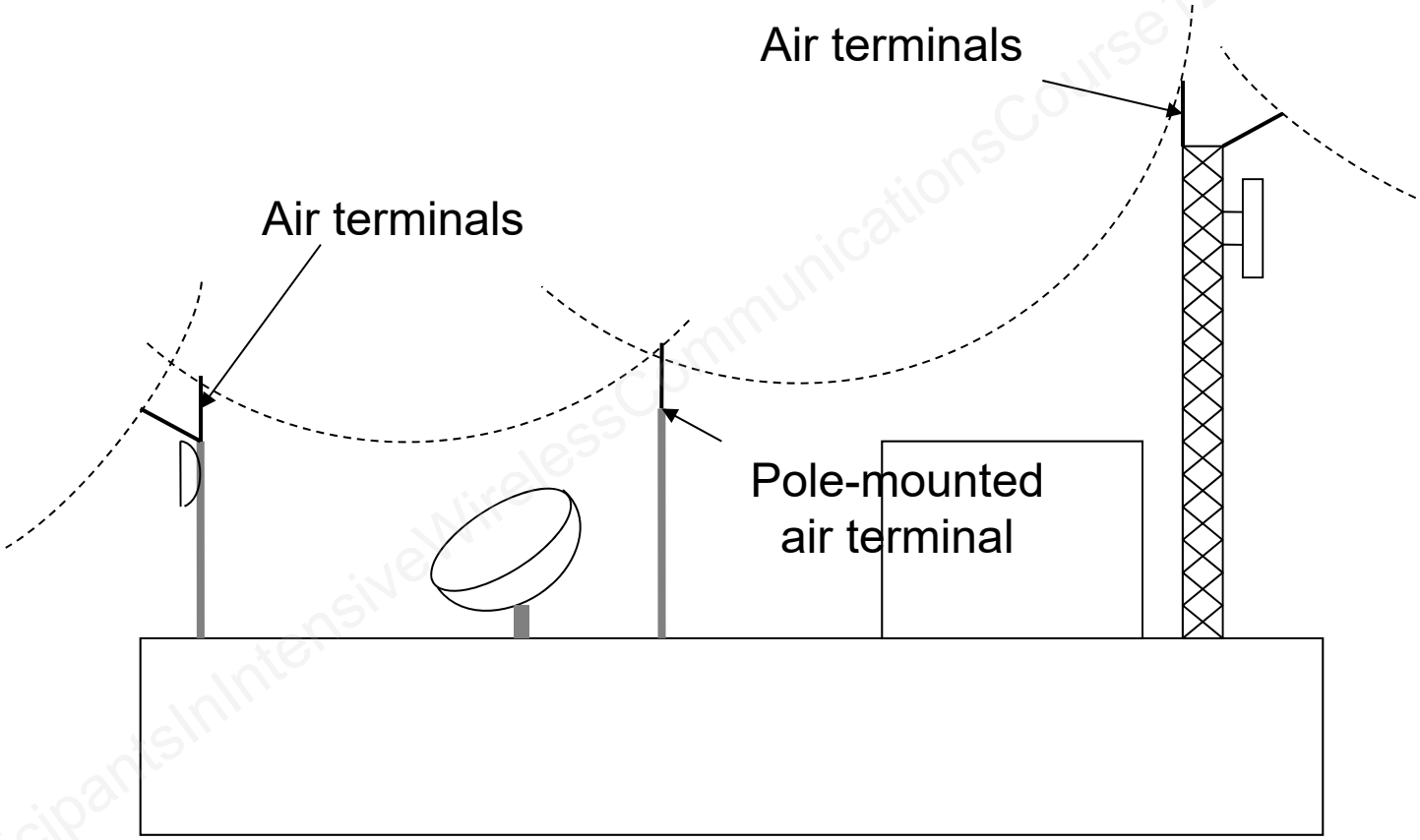


from IEEE ComSoc "A Guide to the Wireless Engineering Body of Knowledge (WEBOK)

Electrical Protection: Lightning Rods and the Rolling Spheres Method



Electrical Protection: Lightning Rods and the Rolling Spheres Method



Facilities Infrastructure Topics(1)

Heating, Ventilation, Air-conditioning (HVAC)

- maintain equipment internal temperature
- battery temperature
- storage battery ventilation

Equipment Racks

- standards for 19”, 23” panels, mounting hardware
- earthquake risk may require special design
- design for adequate space for maintenance, connection and cable access

Facilities Infrastructure Topics (2)

Waveguides and Transmission Lines

- WG minimum bend radius
- transmission loss: WG best
- support: at least every meter
- ground bonding at housing entrance

Tower Requirements

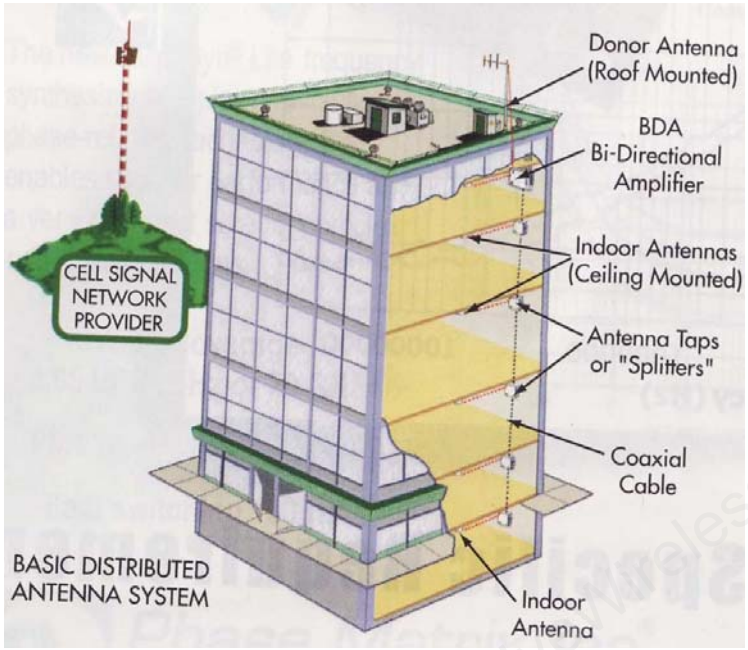
- environmental considerations
- loading, including snow and ice
- corrosion
- flexing from uneven solar radiation
- foundation—adequacy of ground/soil composition

Tower Types

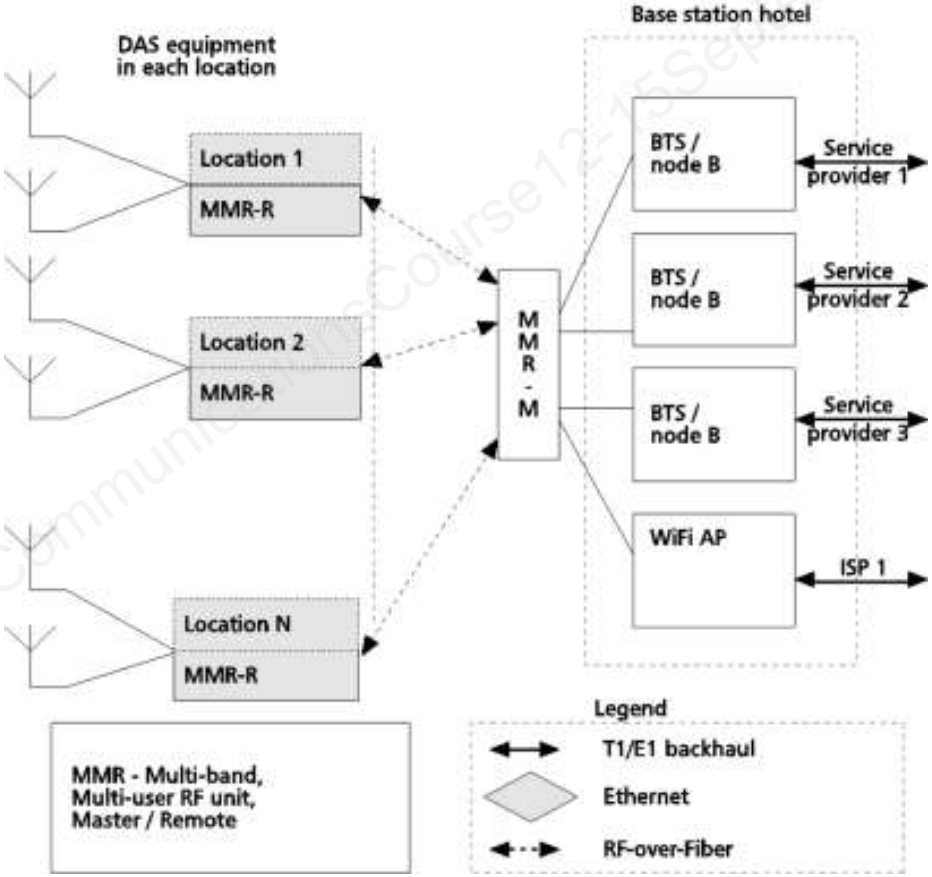
Towers: FAA Regulations

- Federal Aviation Administration (FAA) regulates objects that project into or use navigable airspace
  - FCC is enforcer for FAA for tower issues
- 7460 forms
  - applicability
    - For towers higher than 200 feet
    - for towers in glide path of any airport
  - contents
    - Site's polar coordinates
    - Base elevation about mean sea level
    - Overall height of the tower and antennas
    - Start and end times of tower construction
- Rules for
  - Tower marking – alternating red and white sections
  - Lighting – red incandescent lights, white strobe lights, or a combination, a.k.a dual lighting

Distributed Antenna Systems



from Microwaves & RF magazine, April 2014



from IEEE ComSoc "A Guide to the Wireless Engineering Body of Knowledge (WEBOK)

Physical Security

Considerations

- flood, earthquake, fire
- vandalism
- wildlife damage
- terrorism

Alarm and surveillance systems

- equipment status report
- temperature, humidity, fire
- unauthorized entry

Electronic access

- entry access authorization
- battery backup
- secure access backup in case of electronics failure

Agreements, Standards, Policies, & Regulations

Voluntary and externally imposed compliance requirements and conformance testing, including interoperability.

ASPR

Agreements

- Mutually accepted terms defining expectations
- Non-governmental: commercial legal frameworks
- Implementation relatively fast
- Consumer-Supplier agreements involve Price, Features, Service, Quality
- Examples:
  - service provider/consumer
  - mutual aid in emergency, between telecoms operators
  - product quality management, between network operator and equipment supplier

Standards

- Some aspects of standards:
  - an emphasis on quality
  - voluntary compliance
  - can enable interoperation of networks, equipment
  - set performance levels
- Standard development organizations for telecommunications:
  - European Telecommunications Standards Institute (ETSI)
  - International Telecommunication Union (ITU)
  - International Standards Organization (ISO)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Internet Engineering Task Force (IETF)
  - Telecommunications Industry Association (TIA)
  - The 3rd Generation Partnership Project (3GPP)
- Examples:
  - ETSI EN 300 220-1 technical characteristics of short-range devices
  - IEEE 802.11 wireless local area networks
  - ITU-T X 805 Security architecture for networks

Standards Example: 3G Partnership Project (3GPP)

- 3GPP is a partnership project of national and regional standard bodies ETSI, ARIB, T1, CWTS, TTA, and TTC
- 3GPP was founded towards the end of 1998
- 3GPP aims to produce Technical Specifications for a 3rd Generation Mobile System based on the evolved GSM core network and the radio access technologies that the project partners support (i.e. UTRA both FDD and TDD modes)
- The architectures are also known as UMTS from historical roots

Policies

- Public non-mandatory set of best practices, procedures, etc. adopted by consensus by a group of companies to facilitate implementation of different services.
- Can include compliance with mandatory standards or agreements.
- Examples:
  - Emergency procedures
  - Deployment and maintenance procedures
  - Color coding for alarm, cables, etc.
  - Industry best practices to promote reliability and security

Regulations

- Mandatory set of compliance specifications established by various levels of government authorities with the goal to serve the best interest of the people they govern.
- Slow to develop, hard to change
- Examples of areas covered by regulations:
  - Spectrum management
  - Emergency requirements (E911, etc.)
  - Lawful Intercept
  - Competition rules
- Examples of Regulatory Bodies:
  - FCC, USA (Federal Communication Commission)
  - CRTC, Canada (Canadian Radio-Television Telecommunications Commission)

Safety & Cellular Power Limitations

- ICNIRP standard limit is 450 µW/cm2 at 900 MHz, and 950 µW/cm2 at 1,900 MHz.
- FCC limit is 580 µW/cm2 over any 30-minute period for the 869 MHz, and 1mW/cm2 (1,000 µW/cm2) for PCS frequencies (1850-1990 MHz).

ICNIRP: International Commission on Non-Ionized Radiation Protection

Type Approvals

- Equipment to be sold in a specific country needs to be certified by a national body dedicated to homologation and type approvals.
- In order to get the certification through type approval, the vendor's equipment needs to pass a set of tests defined by the specific country for that type of equipment.
- Factory audits and equipment trials may be included in the procedure for type approval.

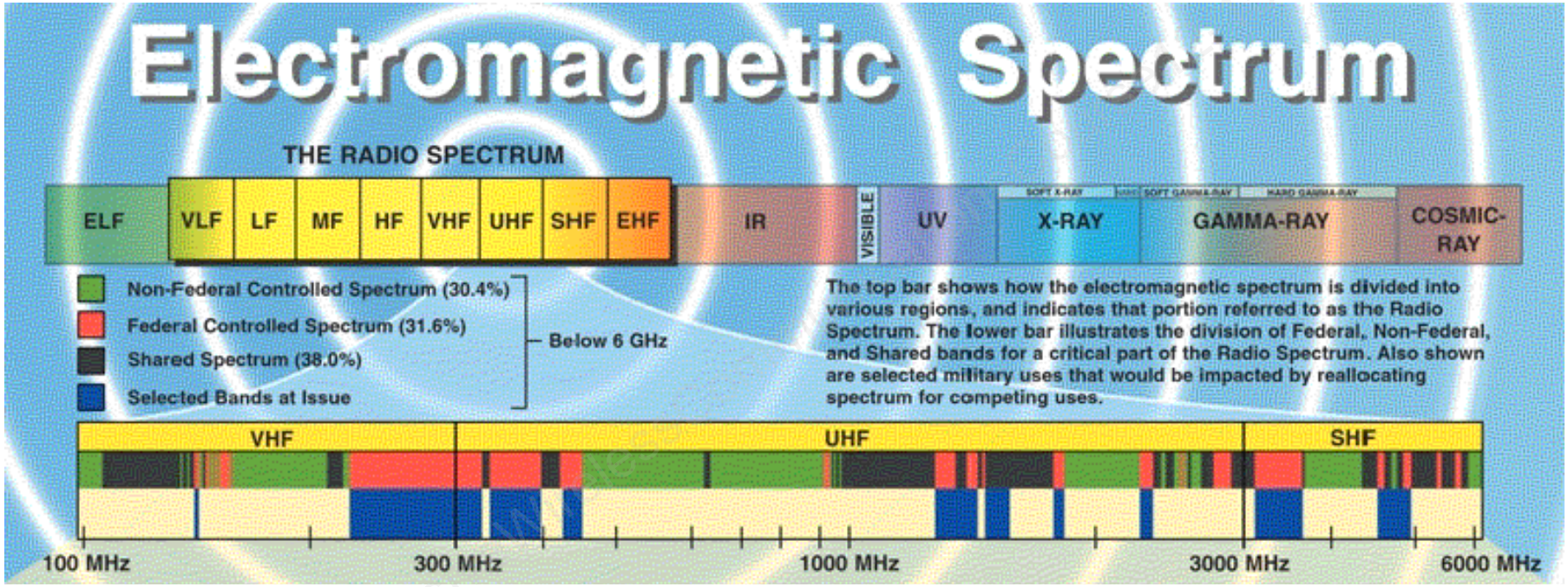
International Telecommunication Union (ITU)

- The ITU, headquartered in Geneva, Switzerland is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services.
- ITU-T (Telecommunications) mission is to ensure an efficient and on-time production of high quality standards (recommendations) covering all fields of telecommunications.
- ITU-D (Development Bureau) has well-established programs of activities to facilitate connectivity and access, foster policy, regulatory and network readiness, expand human capacity through training programs, formulate financing strategies and enable enterprises in developing countries (the Digital Divide).

ITU-R & the WRC

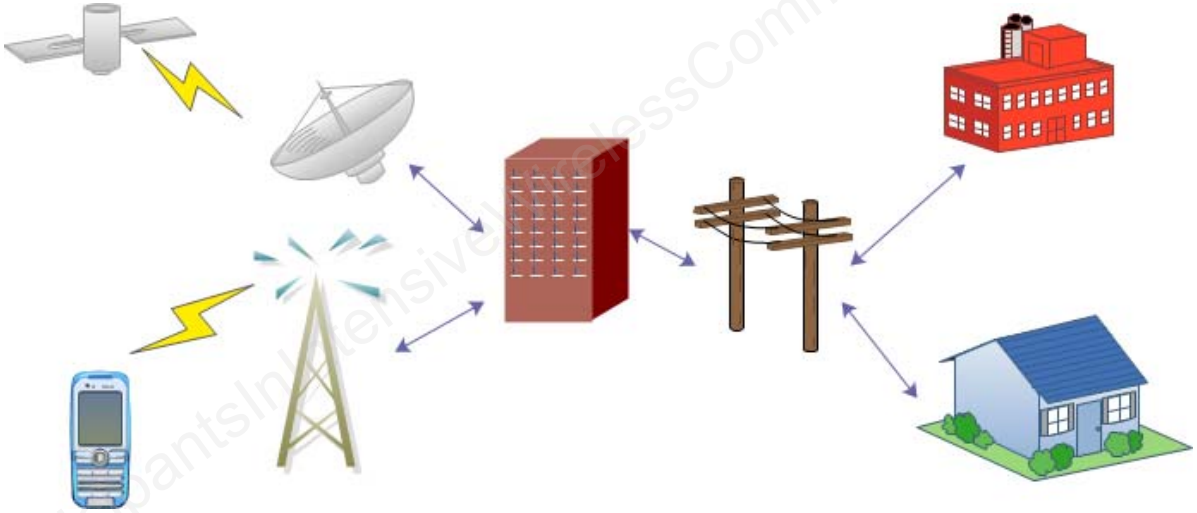
- WRC (World Radio Communication Conference) is held every two to three years.
- It is the job of WRC to review, and, if necessary, revise the Radio Regulations, the international treaty governing the use of the radio frequency spectrum and the geo-stationary satellite and non-geo-stationary satellite orbits.
  - Revise the Radio Regulations and any associated frequency assignment & allotment plans,
  - Address any radio communication matter of worldwide character,
  - Instruct the Radio Regulations Board and the Radio Communication Bureau, and review their activities,
  - Determine questions for study by the Radio Communication Assembly and its study groups in preparation for future radio communication conferences.

Frequency Spectrum



Summary of Part 2

- Principles of internet protocols
- From circuit to packet switching
- Multimedia service fundamentals
- Management, security and infrastructure
- Telecommunication systems documentation



Abbreviations and Acronyms

Term = Description

3G = third generation

3GPP = third generation partnership project

3GPP = 3rd Generation Partnership Project

3GPP2 = 3rd Generation Partnership Project 2

5G NR = 5G New Radio

A = availability

A5 = encryption algorithm

AAA= authentication authorization accounting

AAD = additional authentication data

AAH = asterisk at home (server)

ABS = almost blank subframes

ACK = acknowledgement

ACM = address complete message

ADC = analog to digital converter

AES = advanced encryption standard

AF = Diffserv Assured Forwarding

AFD = average fade distortion

AGC = automatic gain control

AM = amplitude modulation

AMC = adaptive modulation and coding

AMPS = advanced mobile phone service (system)

ANM = answer message

ANSI = American National Standards Institute

AODR = Ad hoc on demand routing

AP = access point

APCO - Association of Public safety Communication Officials

AR = axial ratio for elliptical polarization

ARIB = Association of Radio Industries and Business

ARQ = automatic repeat-request

AS = application server

ASCII = American Standard code for information interchange

ASK = amplitude shift keying

ASN = access service network

ASN.1 = abstract syntax notion one

ASP = application service provider

ATIS = Association Telecommunications Industries Standards

ATM = asynchronous transfer mode

ATPC = automatic transmit power control

AS = autonomous system

AuC = authentication center

AUT = antenna under test

AUTN = network authentication token

AUTS = Token used in resynchronization

AWGN = additive white Gaussian noise

AWS = advanced wireless services

BCMCS = broadcast and multicast services

BE = best effort

BER = bit error rate

BGP = border gateway protocol

BPSK= binary phase shift

BS = base station

BSC = base station controller

BSS = basic service set

BTS = base transceiver station

CA = Carrier Aggregation

CB = certification body

CB = Coordinated Beamforming

CBC = cipher block chaining message

CBC-MAC = cipher block chaining message authentication code

CBQ = class based queuing

CC = call control

CCCH/BCCH = common control channel broadcast control channel

CCI = co-channel interface

CCM = CTR mode with CBC-MAC

CCMP = counter mode with cipher block chaining message authentication code protocol

CCSA = China Communications Standard Association

CDMA = code division multiple access

CGM = conjugate gradient method

CID = connection ID

CIR = carrier to interference ratio

CM = connection management

CMA = constant modulus algorithm

CNR = carrier-to-noise ratio

COFDM = coded orthogonal frequency division multiplexing

CoMP = Coordinated MultiPoint

COMP128 = algorithm

CP = circular polarization

CP = cyclic prefix

CPC = cyclic prefix code

CQI = channel quality indicator

CRC = cyclic redundancy check (cyclic redundancy code)

CRC-32 = cyclic redundancy check 32 bits

CRS = Cell-specific Reference Signal

CS = circuit switched

CS = coding scheme

CS = Coordinated Scheduling

CSA = Canadian Standard Association

CSCF = call session control function

CSFB = Circuit Switched FallBack

CSG = closed subscriber group

CSI-IM = Channel State Information Interference Measurement

CSI-RS = Channel State Information-Reference Signals

CSMA/CA = carrier-sense multiple access with collision avoidance

CSMA/CD = carrier sense multiple access with collision detection

CSN = connectivity service network

CST = computer simulation technology

CTIA =International Association for the Wireless Telecommunications Industry

CTS = clear to send

D2D = Device to Device

DARPA = Defense Advanced Research Projects Agency

dBi = decibel isotropic

dBm = decibel milliwatt

dBr = decibel relative

DCF = distributed coordination function

DCH = dedicated channel

DDoS = distributed denial-of-service

DECT = digital enhanced cordless telephony

DeNB = Donor eNodeB

DES= data encryption standard

DFS = Dynamic Frequency Selection

DFT = Discrete Fourier Transform

DHCP = Dynamic Host Configuration Protocol

DIFS = Distributed Inter-Frame Space

DL = down link

DL-SCH = Downlink Shared CHannel

DMB = digital multimedia broadcasting

DM-RS = DeModulation Reference Signal

DNS = domain name system

DoS = denial-of-service

DPCCH = dedicated physical control channel

DPS = Dynamic Point Selection

DPSK = differential phase shift keying

DQPSK = differential quadrature (or quaternary) phase shift keying

DRA = dielectric resonator antenna

DRC = data rate control

DS0 = Digital Signal 0 (zero)

DS-CDMA = direct sequence code division multiple access

DSL = digital subscriber line

DSR = dynamic source routing

DSS1 = digital subscriber signaling system 1

DSSS = direct sequence spread spectrum

DVB-H = digital video broadcast handheld

DWDM = dense wavelength division multiplexing

DwPTS = Downlink Pilot Time Slot

E_b / N_0 = energy per bit to white noise power spectral density ratio

EAP = extensible authentication protocol

EAP-FAST = EAP flexible authentication via secure tunneling

EAPoL = EAP over LAN

EAP-TLS = EAP transport layer security

EAP-TTLS = EAP tunneled TLS

ECGI = EUTRAN Cell Global ID (EUTRAN is Universal Terrestrial Radio Access Network – same as eNB)

E-DCH = enhanced dedicated channel

EDGE = enhanced data rates for GSM evolution

EF = diffserv expedited forwarding

EGC = equal gain combining

EGPRS = enhanced GPRS

EIA = Electronics Industries Alliance

EIR = equipment identity register

EIRP = effective isotropic radiated power

EM = electromagnetic

eMBB = enhanced Mobile BroadBan

eNB = Evolved Node B – The LTE Radio Access Network

EP = elliptical polarization

EPC = Evolved Packet Core

ERP = effective radiated power

ESS = extended service set

eTOM = enhanced telecom operations map

ET = error tracking

ETSI - European Telecommunication Standards Institute

FA = foreign agent

FACA = US Federal Advisory Committee Act

FBSS = fast base station switching

FCAPS = Fault Configuration Accounting Performance and Security

FCC = Federal Communications Commission

FDD = frequency division duplexing

FDMA = frequency division multiple access

FDTD = finite difference time domain

FEM = finite element method

FFT = fast fourier transform

FHSS = frequency hop spread spectrum

FSK = frequency shift keying

FSO = free space optics

FSS = frequency selective surfaces

FSTD = Frequency Switched Transmit Diversity

G.711 = encoder

GEO = geostationary earth orbit

GGSN = gateway GPRS support node

GKH = group key hierarchy

GMSC = gateway mobile switching center

GMSK = Gaussian minimum shift keying

GPRS = general packet radio service

GPS = global positioning system

GSA = GSM Suppliers Association

GSM = Global System for Mobile-communications

GTC = generic token card

GW = gateway

H.263 = video codec low-bit rate

H.264 = video codec MPEG-4 advanced video codec

HA = home agent

HARQ = hybrid automatic repeat request

HDLC = high-level data link control

HE = home environment

HeNB = Home eNodeB

HetNet = Heterogeneous Network

HFSS = high frequency structure simulator

HHO = hard handoff

Hi-Cap = high capacity

HLR = home location register

HLR/AUC = home location register / authentication center

HN = home network

HO = handoff

HPLMN = home public land mobile network

HSDPA = high speed downlink packet access

HS-DSCH = high speed downlink shared channel

HSPA = high speed packet access

HSS = home subscriber server

HSUPA = high-speed uplink packet access

HTTP = hypertext transfer protocol

IBSS = independent basic service set

ICIC = Inter-Cell Interference Coordination

ICMP = internet control message protocol

I-CSCF = interrogating CSCF

ICV = integrity check value

ID= Identification

IDEN = integrated digital enhanced network

IDU = indoor unit

IEC = International Electro Technical Commission

IECEE = International Electrotechnical Committee for Conformity Testing to Standards for Electrical Equipment

IETF = Internet Engineering Task Force

IF = intermediate frequency

IFFT = inverse fast fourier transform

IK = integrity key

IKE = internet key exchange

IMS = IP multimedia subsystem

IMSI = international mobile subscriber identity

IMP-2000 = International Mobile Telecommunications 2000 ITU Standard

IP = internet protocol

IPv4 = internet protocol version 4

IPv6 = internet protocol version 6

IP-CAN = IP connectivity access networks

IPSec = internet protocol security

IRP = Integration Reference Point

IS-136 = Interim Standard 136

IS-95 = Interim Standard 95

ISAKMP = Internet Security Association and Key Management Protocol

ISI = inter-symbol interference

IS-IS = intermediate system to intermediate system

ISM = industrial, scientific, and medical (band)

ISO = International Standard Organization

ISUP = ISDN user part

ISUP IAM = ISUP initial address message

I-TCP = indirect transmission control protocol

ltf-N = “Northbound Interface” – Interface between Network Management System and Element Management System

ltf-P2P = “Peer-To-Peer Interface” – Interface between two element management systems

ltf-S = “Southbound Interface” – Interface between Element Management System and the Elements

ITIL = Information Technology Infrastructure Library

ITU = International Telecommunication Union

ITU-R = ITU-Radiocommunication (radio communication sector)

ITU-T = ITU-Telecommunication (standards sector)

KA = knowledge area

KC = ciphering key

KCI = EAPoL key communication key

KEK = EAPoL key encryption key

LAA = License Assisted Access

LAN = local area network

LEO = low earth orbit

LH = left hand circular polarization

LMS = least mean square

LO = local oscillator

Lo-Cap = low capacity

LOS = line of sight

LP = linear polarization

LR-WPAN = low rate wireless personal area network

LS-CMA = least squares constant modulus algorithm

LTE = long term evolution

LTE-A = LTE-Advanced

LTE-M = LTE Cat-M1

MAC = media access protocol

MAC = message authentication code

MAC-S = authentication token used in resynchronization

MAN = metropolitan area network

MAP = mobile application part

MBMS = multimedia broadcast / multicast service

MBSFN = Multicast-broadcast single-frequency network

MCPTT = Mission critical push-to-talk over LTE

MCW = multi codeword

MD5 = message digest (algorithm) 5

MDHO = macro diversity handover

MDS = minimum discernible signal

MDT = Minimization of Drive Tests

MEdiaFLO = forward link only technology

MEO = medium earth orbit

MGCF = media gateway control function

MGW = media gateway

MIB = management information base

MIC = message integrity check

MIMO = multiple-input multiple-output

MIP = mobile IP

MISO = multiple input single output

MM = mobility management

MME = mobility management entity

MMUSIC = multiparty multimedia session control

MoM = method of moments

MOS = mean opinion score

MPDU = MAC protocol data unit

MPEG = moving picture expert group

MPLS = multiprotocol label switching

MR = mesh router

MRC = maximum ratio combining

MRF = media resource function

MS = mobile station

MSC / VLR = mobile switching center / visitor location register

MSC = mobile switching center

MSISDN = mobile station integrated services digital network

MSK = minimum-shift keying

MSRN= mobile station roaming number

MSS = maximum segment size

MTBF = mean time between failures

MTC = Machine Type Communications

MTTR = mean time to repair

MU-MIMO = multiple user MIMO

NACK = negative acknowledgement

NAS = network access server

NAV = network allocation vector

NBAP= node B application part

NB-IOT = NarrowBand Internet of Things

NCRP = National Council on Radiation Protection

NEBS = Network Equipment Building Systems Standard

NEC = numerical electromagnetics code

NFV = Network Functions Virtualization

NF = noise figure

NFC = near field communication

NGMC = next generation mobile committee

NGMN = next generation mobile networks

NGN = next generation network(s)

NIC= network interface card

NIST = National Institute of Standards and Technology

NLOS = non-line-of-sight

NMHA = normal mode helical antenna

NMS = network management system

Node B = base station designation in UMTS

NPA = nonlinear power amplifier

NRSC = network reliability steering committee

NRZ = non-return to zero

NSP = network service provider

NSS = network subsystem

NSTAC = National Security Telecommunications Advisory Committee (US)

OAM = Operation, Administration and Maintenance – Management System

OATS = open area test site

OCC = Orthogonal Cover Code

ODU = outdoor unit

OFDM = orthogonal frequency division multiplexing

OFDMA = orthogonal frequency division multiple access

OGC = Office of Government Commerce

OLSR = optimized link state routing

OSA = opportunistic spectrum address

OSG = Open Subscriber Group

OSS/BSS = operational and business support systems

OSPF = open shortest path first

OSI = open systems interconnection

OTA = over the air programming

OTP = one time password

OVS = open virtual switch

PA = power amplifier

PAN = personal area network

PAPR = high peak to average power ratio

PBCCH = Packet Broadcast Control Channel

PCFR = policy and charging rules function

PCI = Physical Cell ID

PCM = pulse code modulation

P-CSCF = proxy CSCF

PDC = personal digital cellular

PDSN = packet data serving node

PDU = protocol data unit

PEAP = protected EAP

PFDM = orthogonal frequency division multiplex

P-GW = variant of PDN-GW, packet data network gateway

PHY = physical (layer)

PIFA = planar inverted F antenna

PIN = personal identification number

PKH = pairwise key hierarchy

PL = path loss

PLMN = Public Land-Mobile Network

PN = pseudo-noise

PO = physical optics

PPP = point to point protocol

PS = packet switched

PSK = phase shift keying

PSTN = public switched telephone network

PUCCH = Physical Uplink Control CHannel

PUSCH = Physical Uplink Shared CHannel

QAM = quadrature amplitude modulation

QoS = quality of service

QPSK = quadrature (quaternary) phase shift keying

RAB = radio access bearer

RACH = random access channel

RADIUS = remote access dial in user server

RAN = radio access network

RAND = random

RC4 = RC4 cipher algorithm

RET = remote electrical tilt

RF = radio frequency

RFC = request for change

RFC = request for comment

RFID = radio frequency identification

RHCP = right hand circular polarization

RIP = routing information protocol

RLC = radio link control

RLS = recursive least squares

RMON = Remote network Monitoring

RN = Relay Node

RNC = radio network control

ROAMOPS = IETF roaming operations

ROHC = robust header compression

R-PDCCG = Relay Physical Downlink Control Channel

RR = radio resource

RRC = radio resource control

RSA = Rivest, Shamir, Alderman

RSN = robust security networks

RSNA = robust security network associations

RSRP = Reference Signal Received Power

RSSI = received signal strength indicator

RTP = real time protocol

RTS = request to send

RTT = round trip time

RZ = return to zero

S/N = signal to noise ratio

SA = Security Association

SAR = specific absorption rate

SCCP = signaling connection control protocol

SC-FDMA = Single Carrier FDMA

SCH = Shared CHannel

SCP = ETSI smart card platform

S-CSCF = serving CSCF

SCTP = stream control transmission protocol

SCW = single codeword

SDCCH = stand alone dedicated channel

SDH = synchronous digital hierarchy

SDMA = space division multiple access

SDP= session description protocol

SDR = software defined radio

SEGF = security gateway function

SET = secure electronic transaction

SF = spreading factor

SFBC = Space-Frequency Block Codes

SFDR = spurious free dynamic range

SFID = service flow ID

SG/MGC = signaling gateway/media gateway controller

SGSN = serving GPRS support node

S-GW = serving gateway

SGW = signaling gateway

SHA = secure hash algorithm

SID = system identification number

SIFS = short inter-frame space

SIG = special interest group of WWRF

SIGTRAN = signal transport

SIM= subscriber identity module

SIMO = single input multiple output

SINR = signal-to-interference-plus-noise ratio

SIP = session initiation protocol

SIR = signal to interference ratio

SISO = single input single output

SLF = subscriber location function

SMI = structure of management information

SMS = short message service

SM-SC = short message service center

SMTP = simple message transfer protocol

SNMP = simple network management protocol

SNR = signal-to-noise ratio

SON = Self Organizing Network

SPC = single parity check

SQN = sequence number

SRES = signed response

SRS = Sounding Reference Signal

SRTP = secure RTP

SS7 = signaling system number 7

SSB = single sideband

SSID = service site identifier

SSPA = solid state power amplifier

STA = stations

STM = synchronous transfer mode

SVLTE = simultaneous voice and LTE

SYN = synchronization

T2P = traffic to pilot

TCAP = transaction capabilities application part

TCH / FS = traffic channel full rate speech

TCH / HS = traffic channel half rate speech

TCH = traffic channel

TCP / IP = suite of protocols

TCP = transmission control protocol

TD-CDMA = time division CDMA

TDD = time division duplex

TDM = time-division multiplexing

TDMA = time division multiple access

TDOA = time difference of arrival

TD-SCDMA = time division synchronous CDMA

TIA = Telecommunications Industry Association

TIMSI = temporary international mobile subscriber identity

TK = temporal key

TKIP = temporal key integrity protocol

TMF = TM Forum

TRAP = TDMA-based randomly addressed polling

Triple DES = encryption standard

TS = time slot

TSC = TKIP sequence counter

TSG CT = TSG core network & terminals

TSG GERAN = TSG GSM EDGE radio access network

TSG RA = ETG services and system aspects

TSG RAN = TSG radio access network

TTA = Telecommunications Technology Association of Korea

TTC = Telecommunications Technology Committee

TTI = Transmit Time Interval

UDP = user datagram protocol

UE = user equipment

UL = Underwriters Laboratories

UL = Uplink

UL-SCH = Uplink Shared CHannel

UMB = ultra mobile broadband

UMTS = universal mobile telecommunications system

UMTS AKA = protocol used in 3G

UpPTS = Uplink Pilot Time Slot

UPS = uninterruptible power supply

USGS = United States Geological Survey

USIM= universal subscriber identity module

UTRA = universal terrestrial radio access

UTRA TDD-HCR = TD-CDMA UTRA mode

UTRA TDD-LCR = TD-SCDMA UTRA mode

UTRAN = UMTS terrestrial radio access network

UWB = ultra-wideband

VLR = visitor location register

VN = visited network

VoIP = Voice over Internet Protocol

VOLTE = voice over LTE

VOLGA = voice over LTE via Generic Access

VPLMN = visited public land mobile network

VSAT = very small aperture terminal

VSWR = voltage standing-wave ratio

WAN = wide area network

W-CDMA = wideband code division multiple access

WCET = wireless communications engineering technologies

WCP = wireless communication professional

WEP = wired equivalent privacy

WERT = wireless emergency response team

WFQ = weighted fair queuing

WG = working group of WWRF

Wi-Fi = Wireless Fidelity

WiMAX = worldwide interoperability for microwave access

WINNER = wireless world initiative new radio

WLAN = wireless local area network

WMAN = wireless metropolitan area network

WMN = wireless mesh network

WPA = Wi-Fi Protected Access

WPAN = wireless personal area network

WRC = World Radiocommunication Conference

WWRF = wireless world research forum

XG = next generation

XKMS = XML Key Management Services

XMAC (PG 26) = cryptographic primitive in the 3GSM key generation process

XOR = exclusive or

ZRP = zone routing protocol