Wireless & Mobile Networks concepts and security

Prof. Amine Berqia
Email : berqia@gmail.com

Welcome to WMN

Course logistics

Office hours: by appointment

I’m very responsive with email

Grading :
Examination: 50%
Project & Practical exercises: 50%
Bonus : Class participation: 10% E.g. question you ask and how much you interact.

Topics

- ✓ WLAN: IEEE802.11 …
- ✓ WPAN: IEEE 802.15 …
- ✓ Mobile IP
- ✓ WMAN: IEEE 802.16 …
- ✓ WWAN: GSM, GPRS, EDGE, 3G…

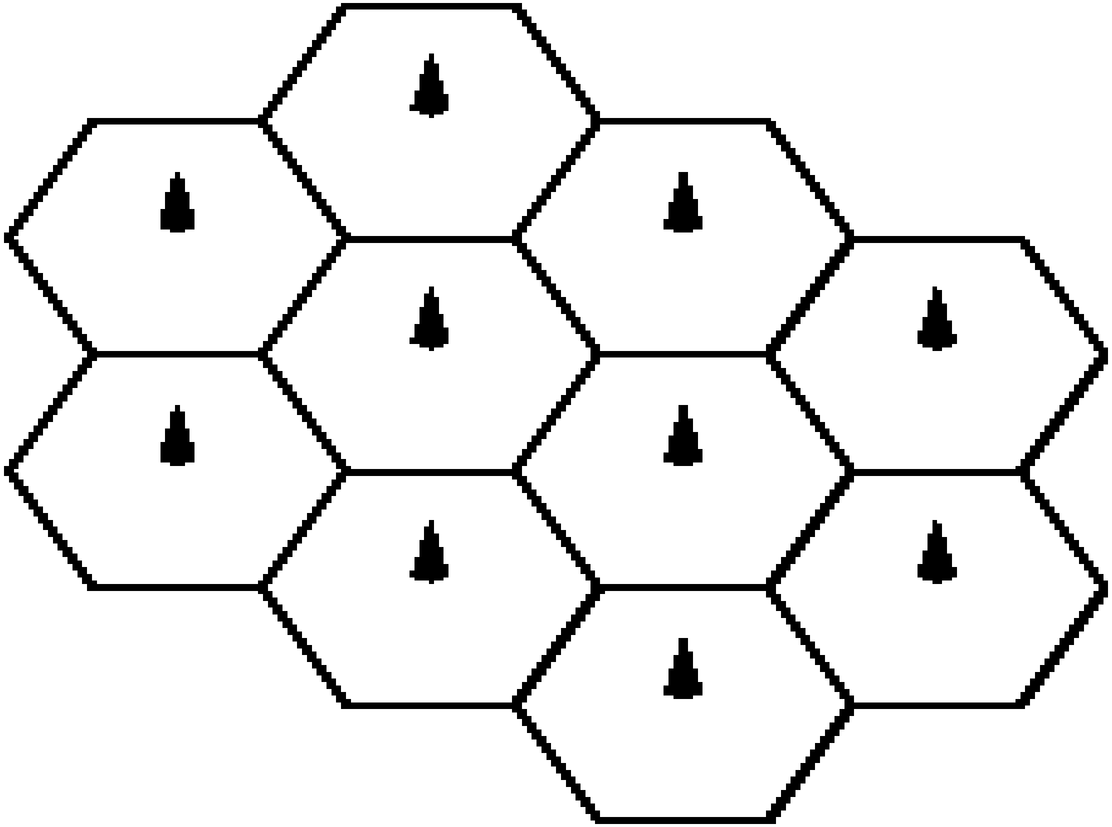
Mobile Networks
&
Wireless Networks

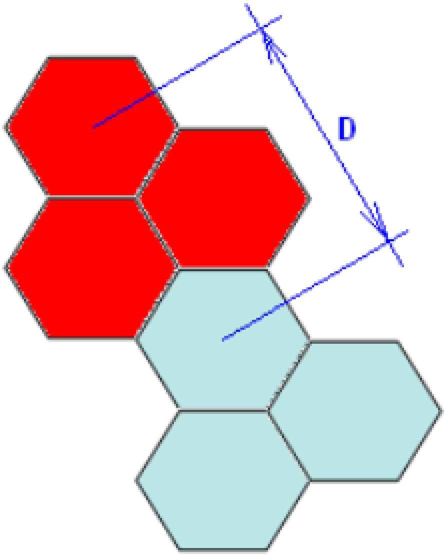
MN	WN
An user is defined as mobile user if he is capable to communicate outside of its net of signature conserving same address.	A system is called wireless if the system proposes a service of communication completely independent of sockets..

Examples of Mobile and/or Wireless Networks

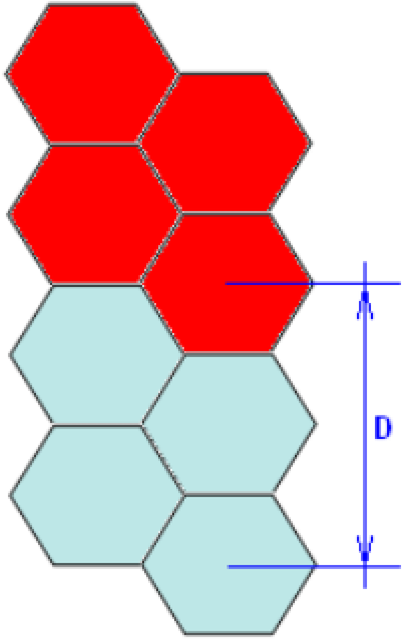
	WN	MN
GSM	✓	✓
UMTS	✓	✓
TCP/IP	x	x
IP Mobile	x	✓
ATM	x	x
DECT	✓	x

Cellular Concept



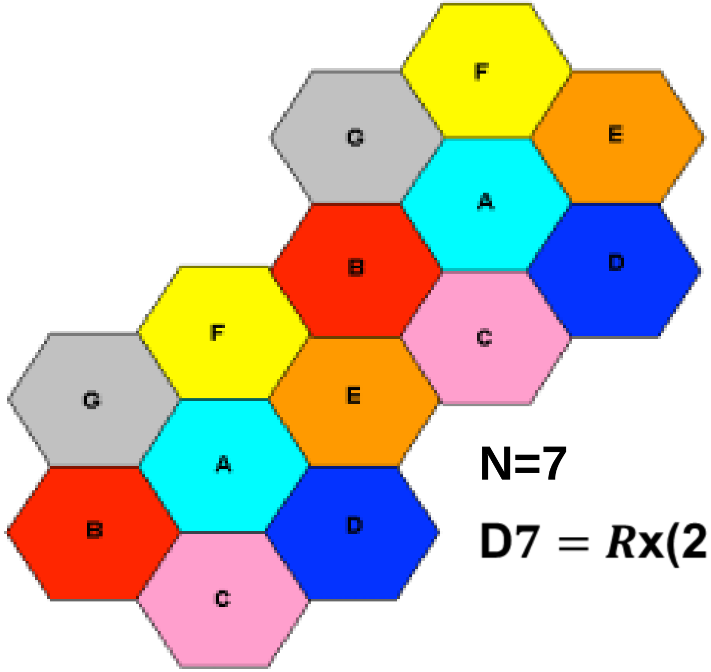


N = 3



N = 4

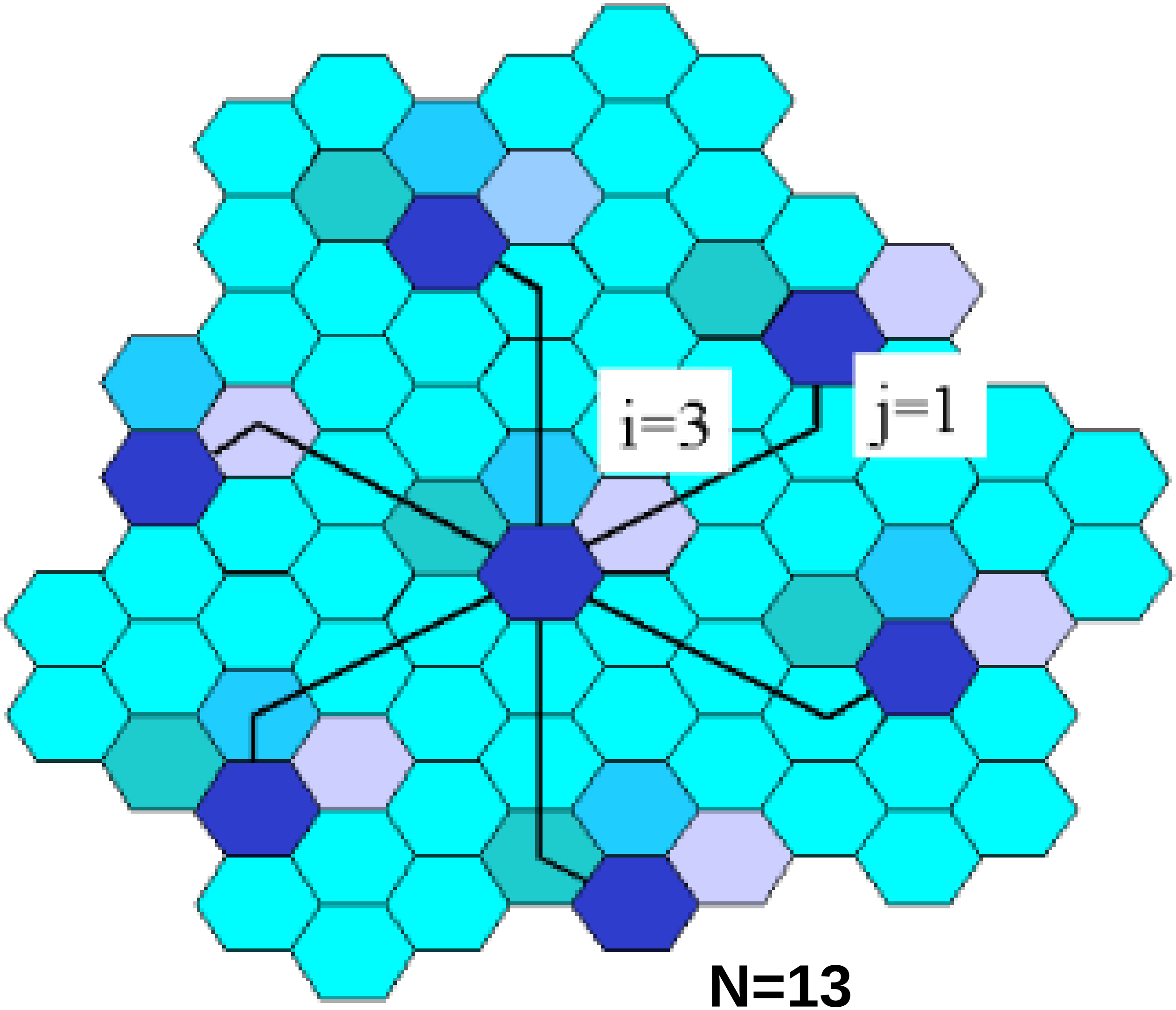
$$D_3 = 3R;$$
$$D_4 = 2R(3)^{1/2} ;$$



N=7

D7 $= R$x$(21)^{1/2}$;

$$D_N = R\text{x}(3N)^{1/2}$$



N=13

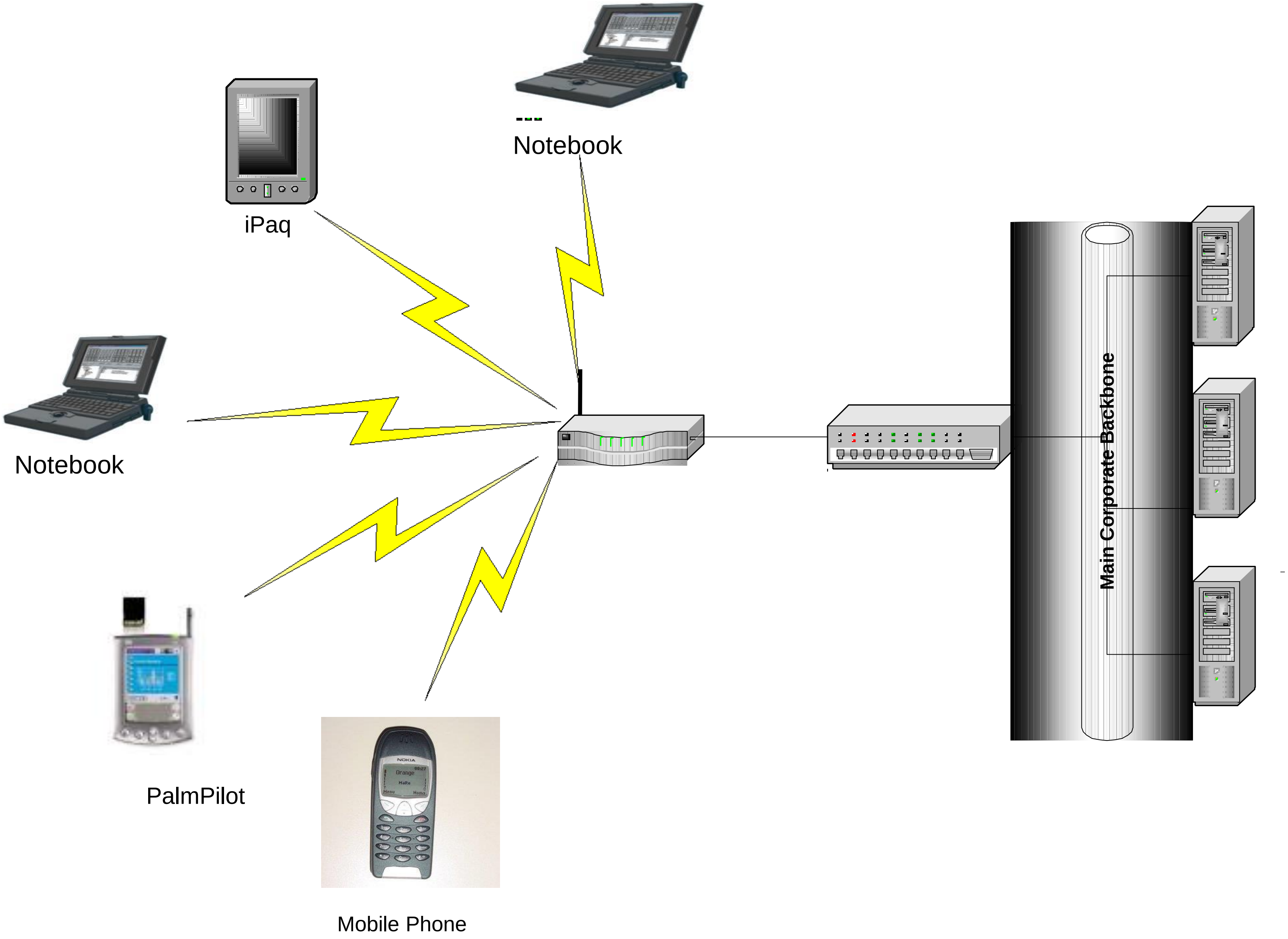
WLAN

- 1990 : WLAN project

- IEEE (Institute of Electrical and Electronics Engineers) :
  - IEEE 802.11
  - IEEE 802.15

- Hiperlan (High Performance Local Area Network)
  - HiperLAN

WLAN?


Notebook
iPaq
Notebook
Main Corporate Backbone
PalmPilot
Mobile Phone

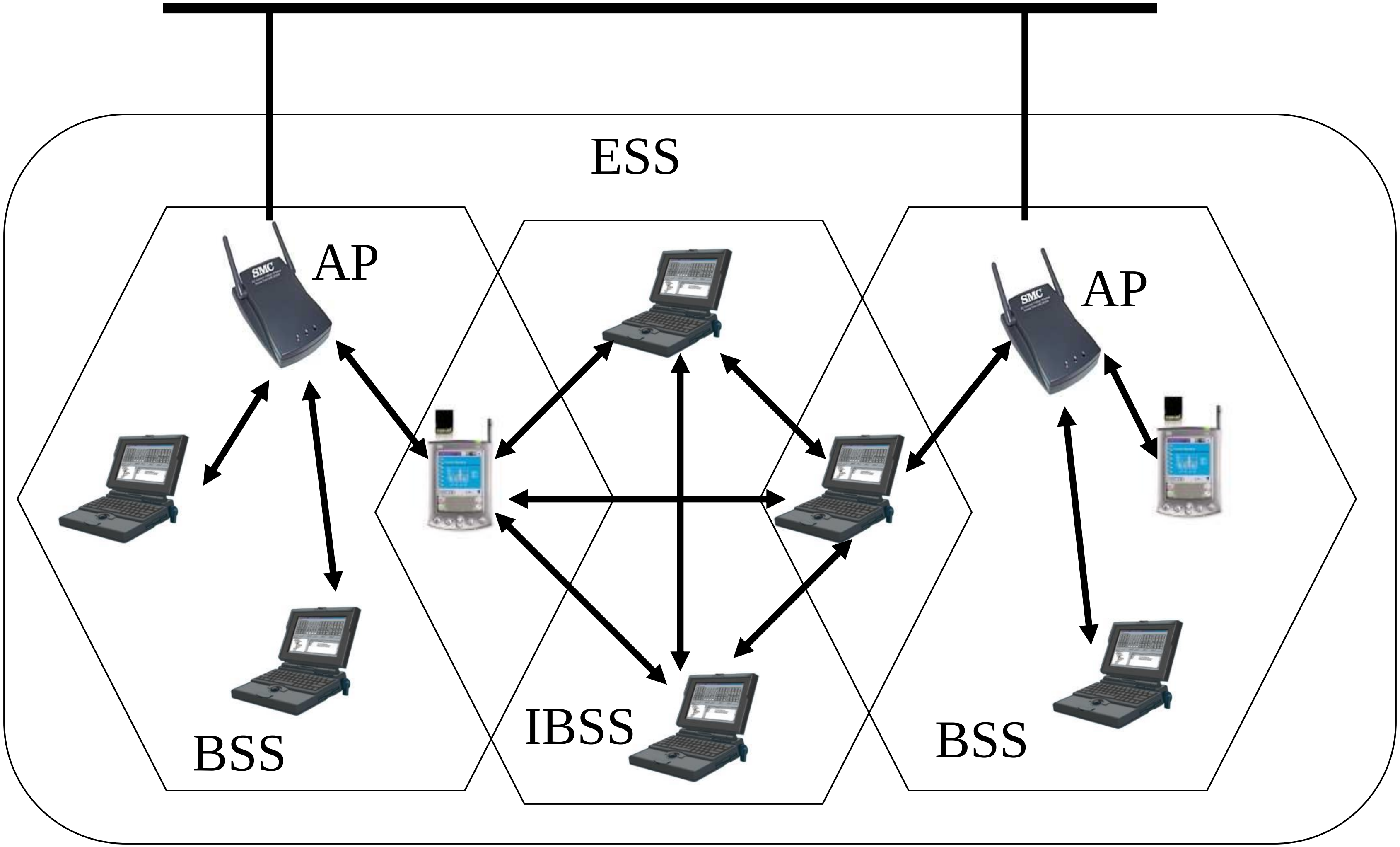
IEEE 802.11

<table>
<tr><td rowspan="3">MAC Layer</td><td colspan="4">LLC 802.2</td></tr>
<tr><td colspan="4">802.11f</td></tr>
<tr><td colspan="4">802.11 – 802.11e – 802.11i</td></tr>
<tr><td>Physical Layer</td><td>802.11
DSSS
FHSS
IR</td><td>802.11b</td><td>802.11g</td><td>802.11a</td></tr>
</table>

IEEE 802.11

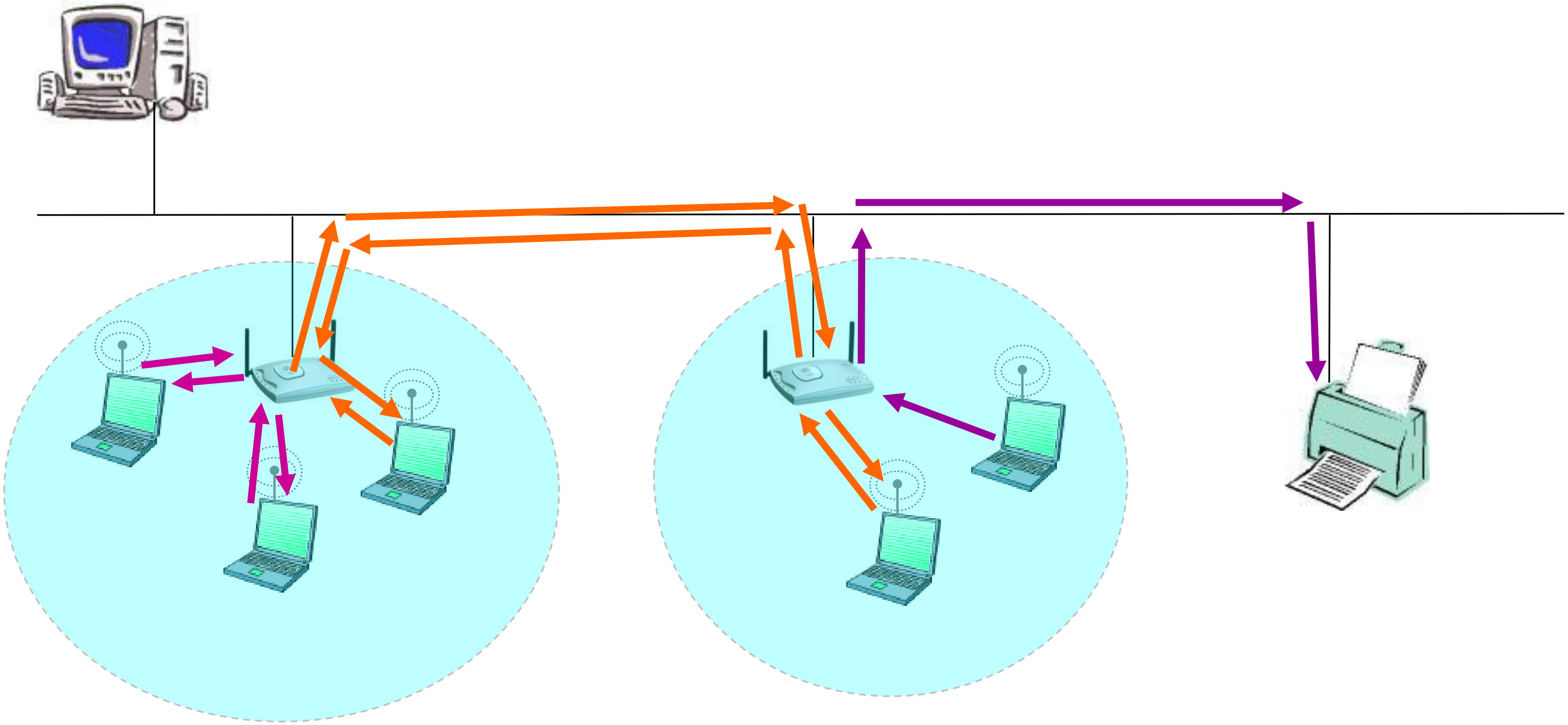
- Frequency : band 2,4 GHz;
- Infrastructue or Ad-hoc
- IEEE 802.11 is Cellular

IEEE 802.11 Architecture

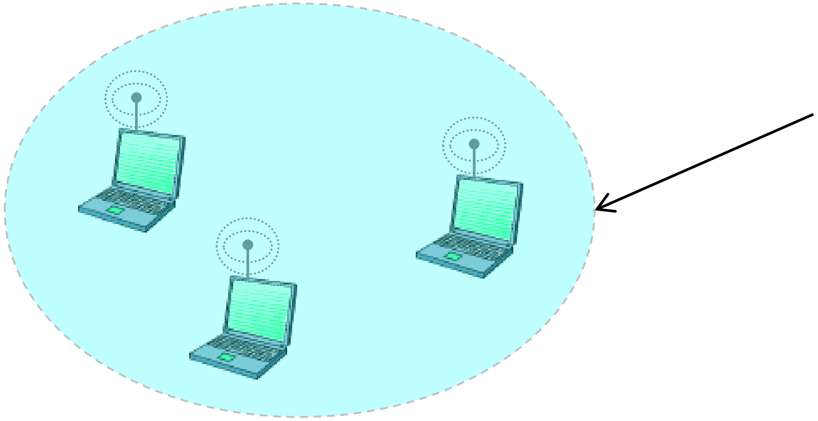


AP: Access point, BSS : Basic Set service, ESS : Extented Set Service, IBSS Independent BSS.

infrastructure



ad-hoc



IBSS (*Independent Basic Service Set*)

Method Access

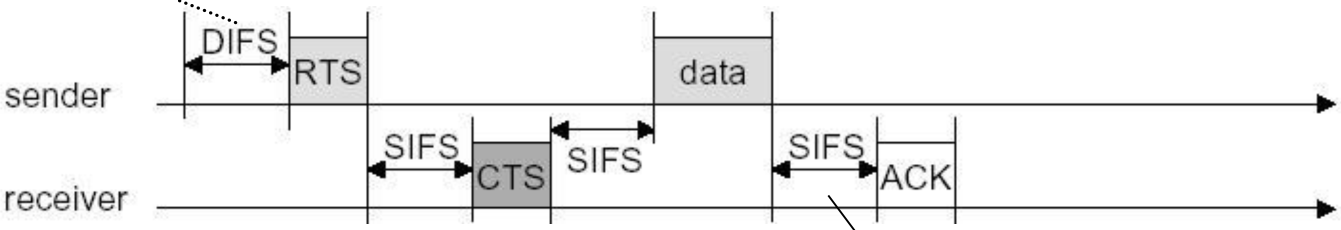
MAC layer:

- DCF (Distributed Coordination Function) :
  - based on CSMA/CA

- PCF (Point Coordination Function) :
  - Baseado on *polling*

DCF

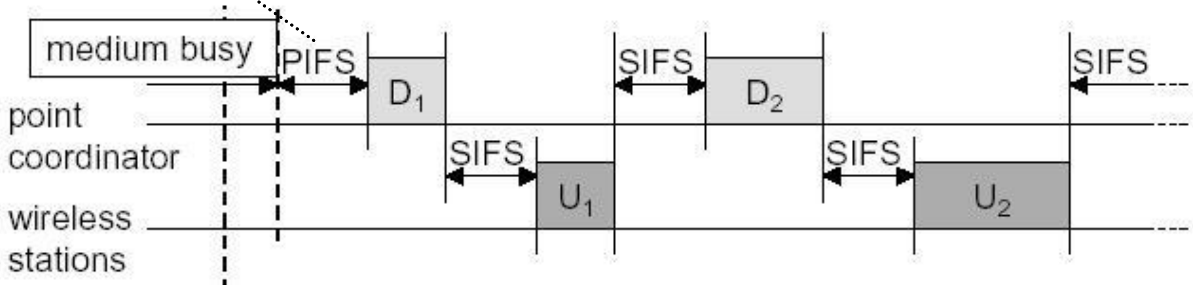
DIFS (Distributed Inter Frame Space)



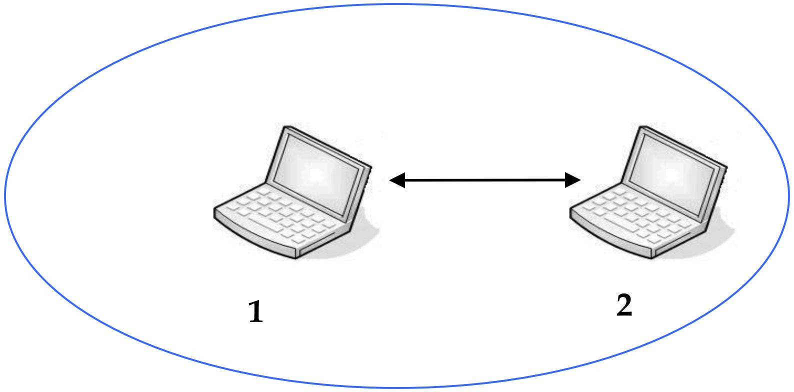
SIFS (Short Inter Frame Space)

PCF

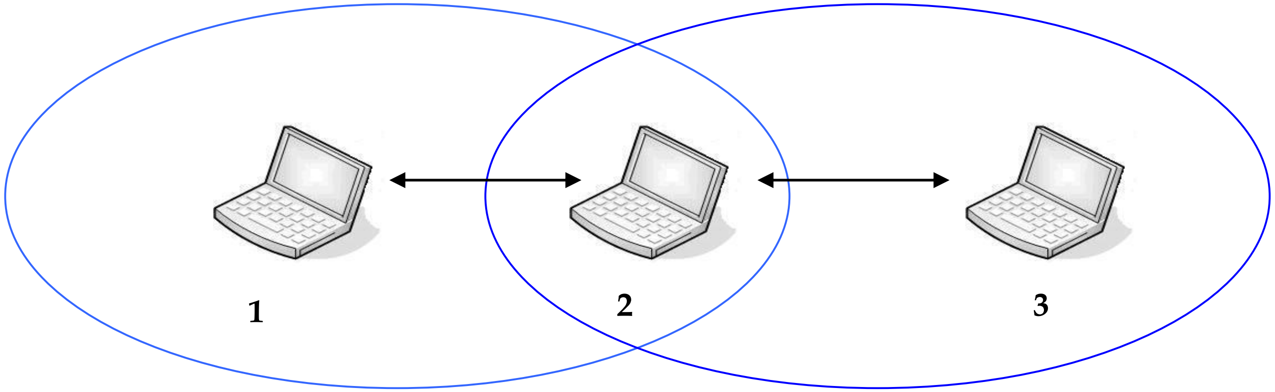
PIFS (Point Coordenation Inter Frame Space)



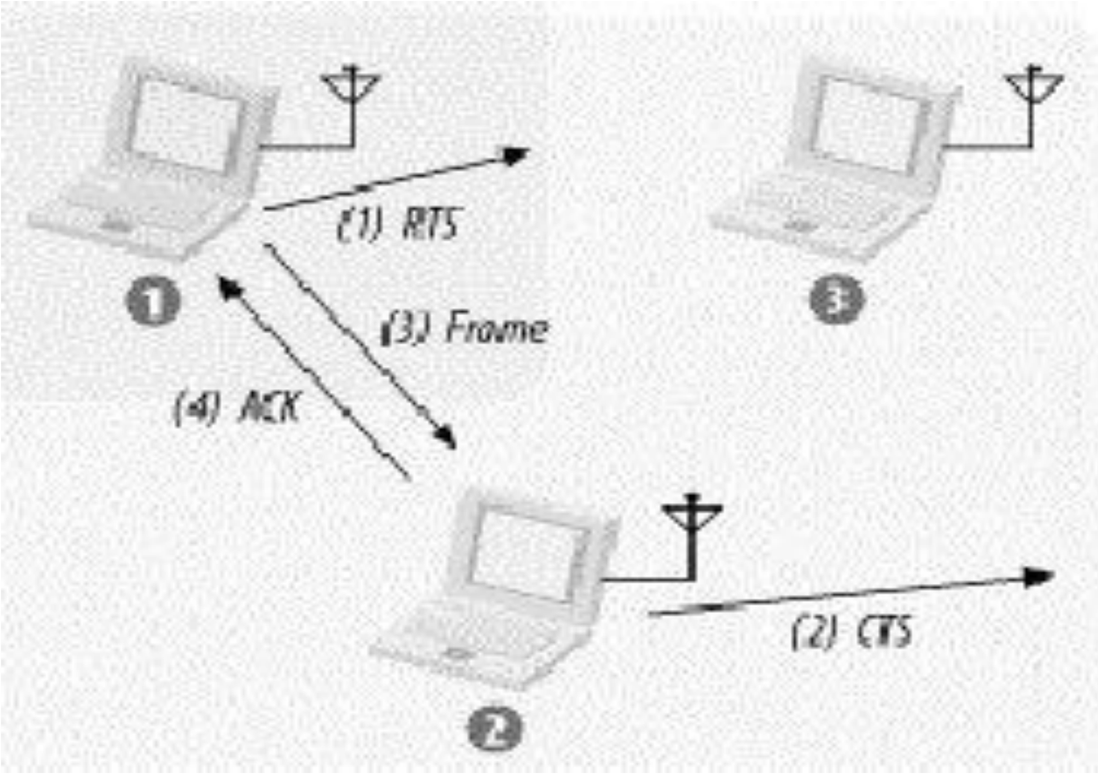
Hidden Node Problem



Hidden Node Problem



RTS/CTS



Bluetooth™

Bluetooth

King Viking, *Harald Blåtand* (english *Blåtand* = *Bluetooth*).

History

- ✓ 1994 –*Ericsson*
- ✓ 1998 –Bluetooth SIG (*Special Interest Group*):
  - ✓ *Ericsson*
  - ✓ *IBM*
  - ✓ *Intel*
  - ✓ *Nokia*
  - ✓ *Toshiba*

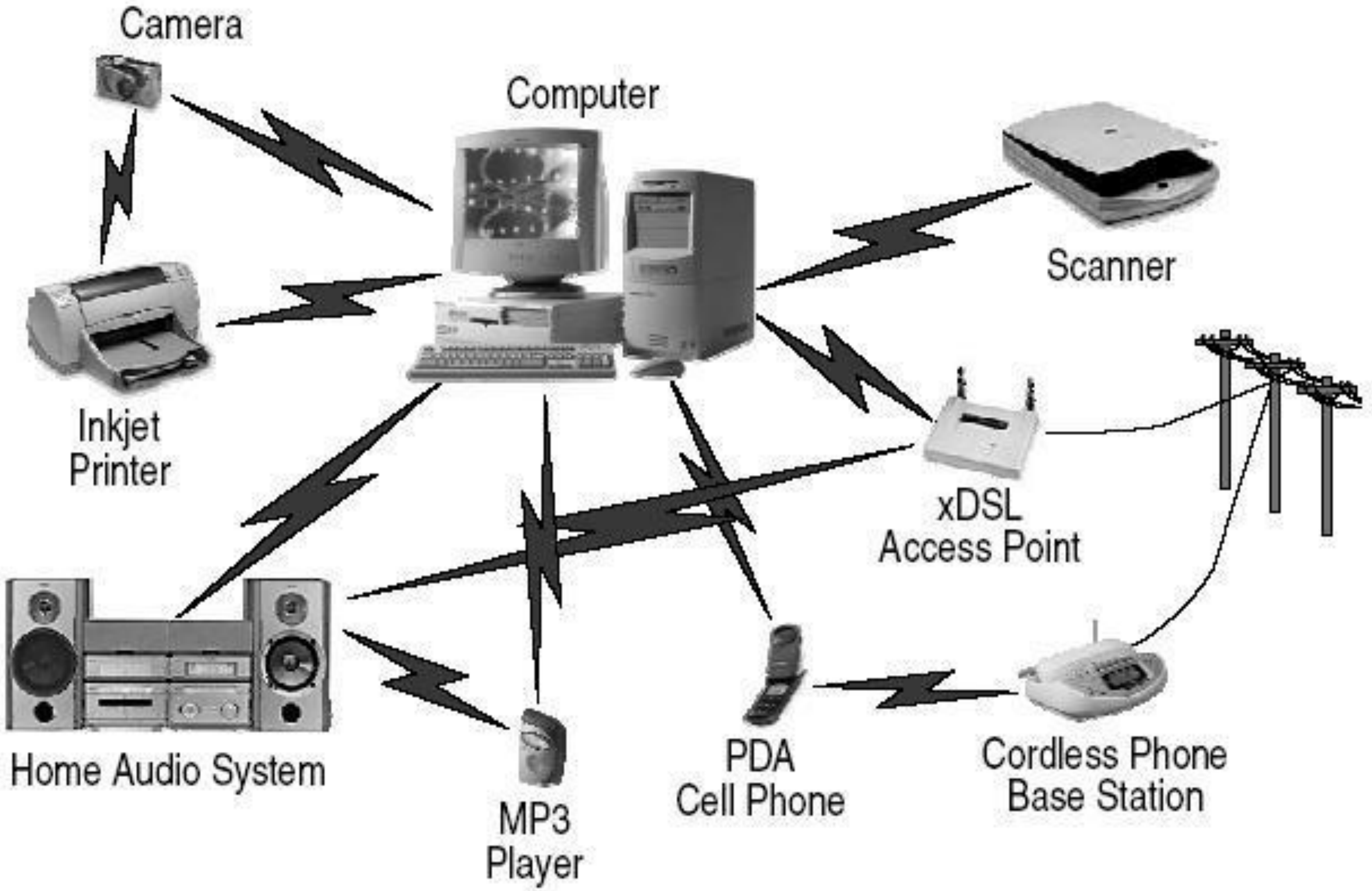
History

- ✓ 1999 –B-SIG : *Microsoft, Lucent Motorola* e&*3Com*
- ✓ 1999 – Version1.0
- ✓ 2001 – First devices
- ✓ More than 2500 companies in B-SIG

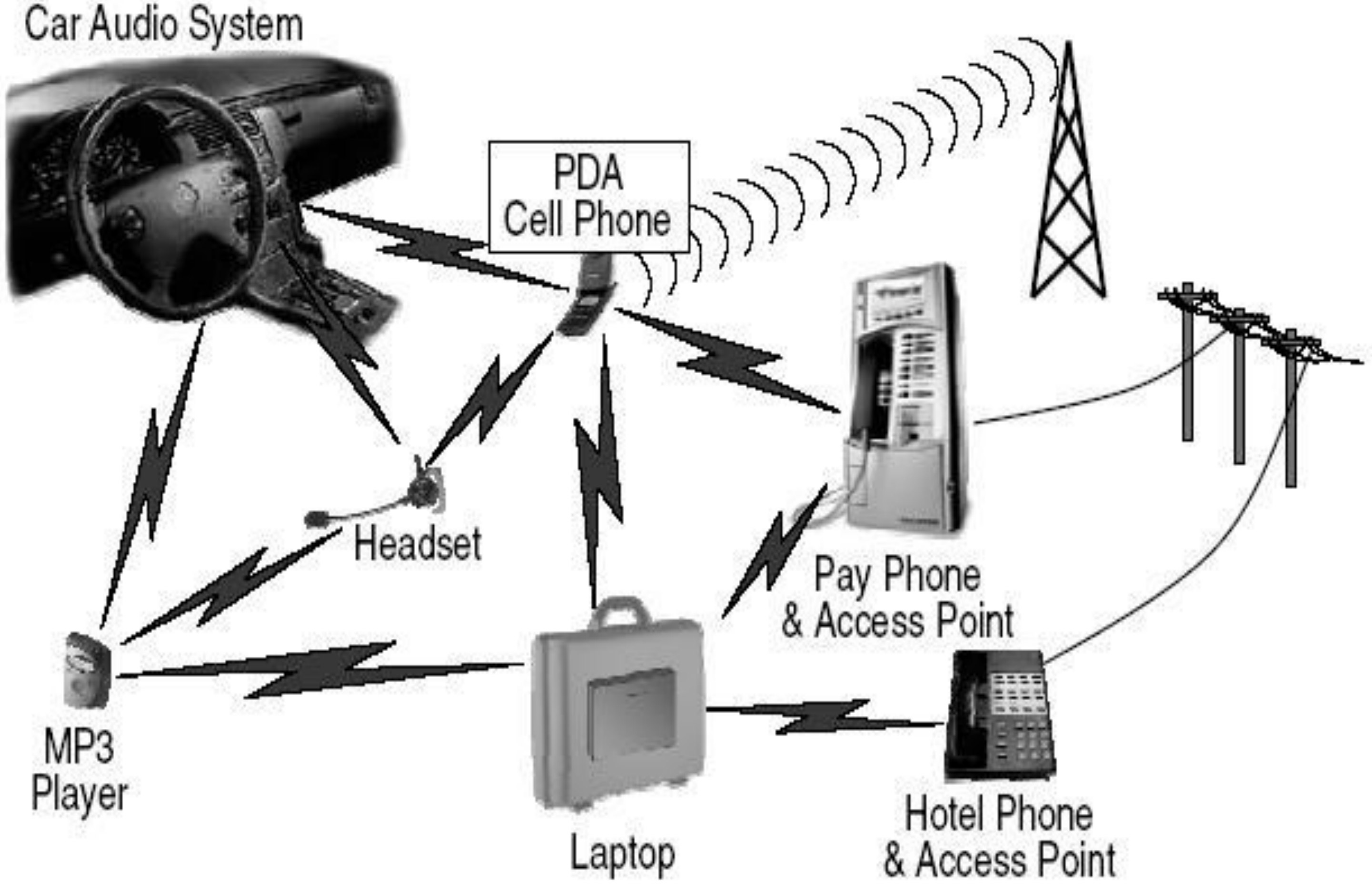
Characteristics

- ✓ WPAN Technology
- ✓ ad-hoc
- ✓ 10m till 100m
- ✓ Low cost
- ✓ 2,4 GHz
- ✓ Max – 1 Mbps
- ✓ Modulation GFSK (Gaussian Frequency Shift Keying)

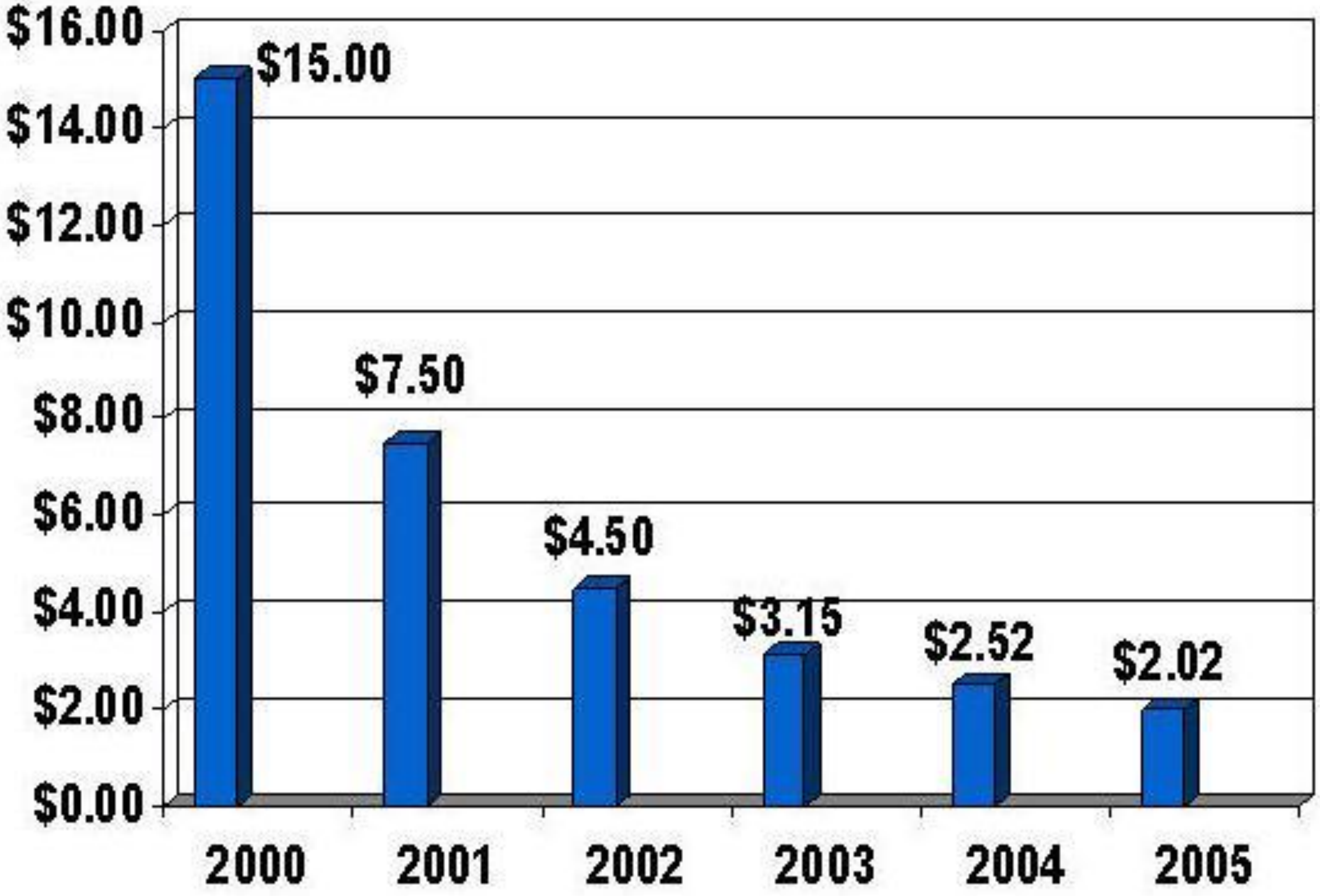
Bluetooth (1)


Camera
Computer
Scanner
Inkjet Printer
xDSL Access Point
Home Audio System
MP3 Player
PDA Cell Phone
Cordless Phone Base Station

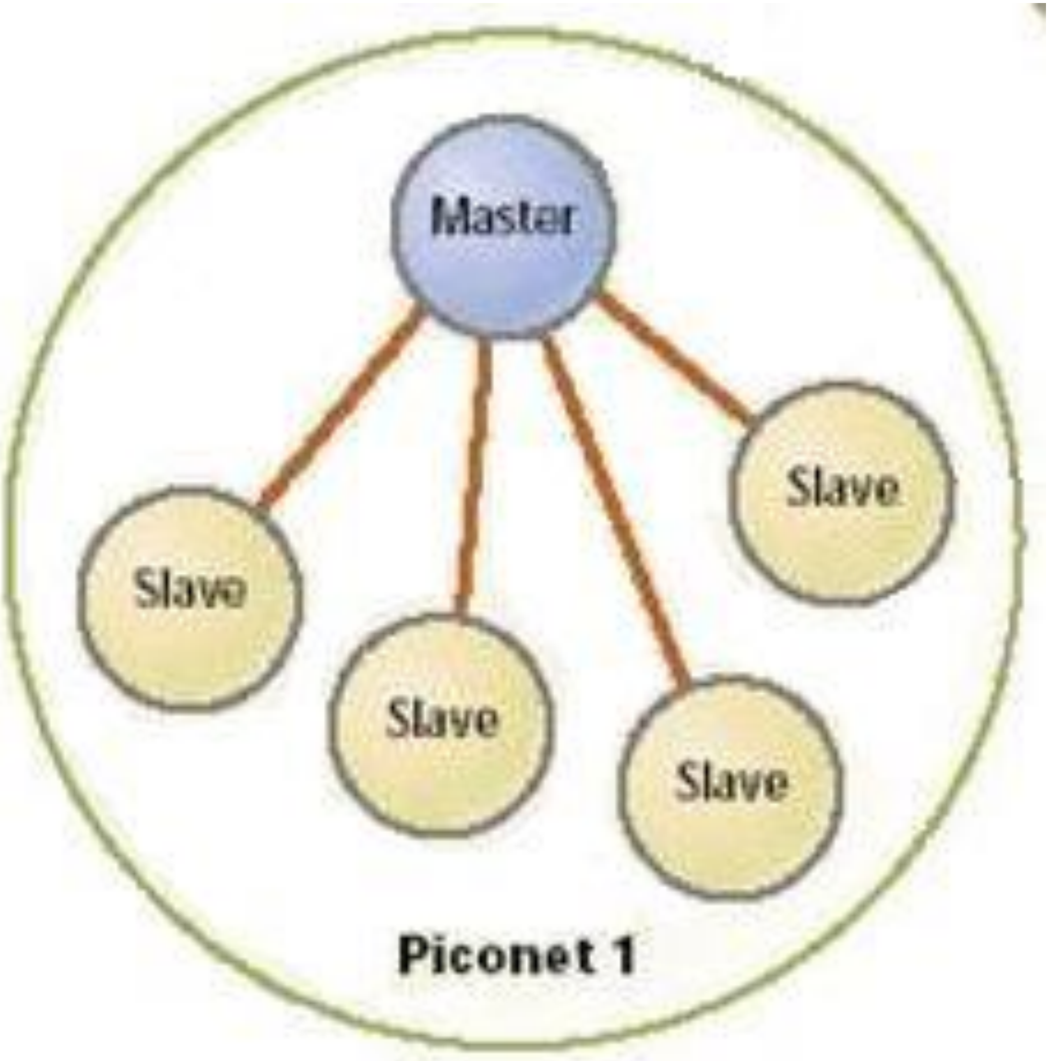
Bluetooth (2)


Car Audio System
PDA
Cell Phone
Headset
Pay Phone
& Access Point
MP3
Player
Laptop
Hotel Phone
& Access Point

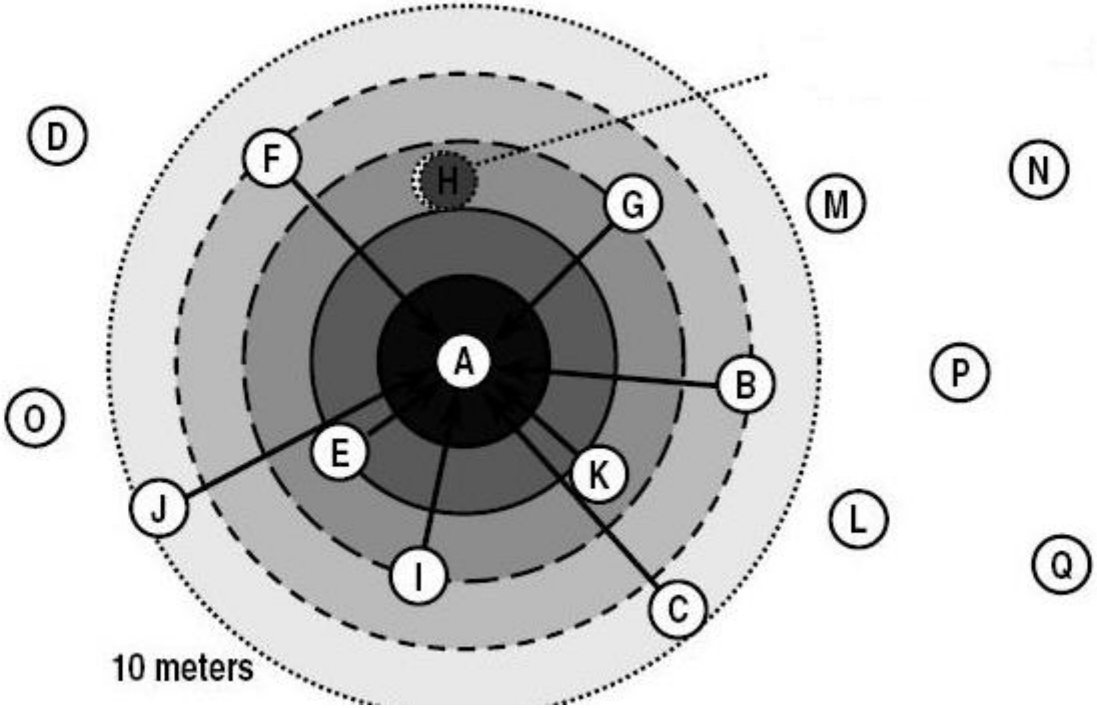
Cost USA



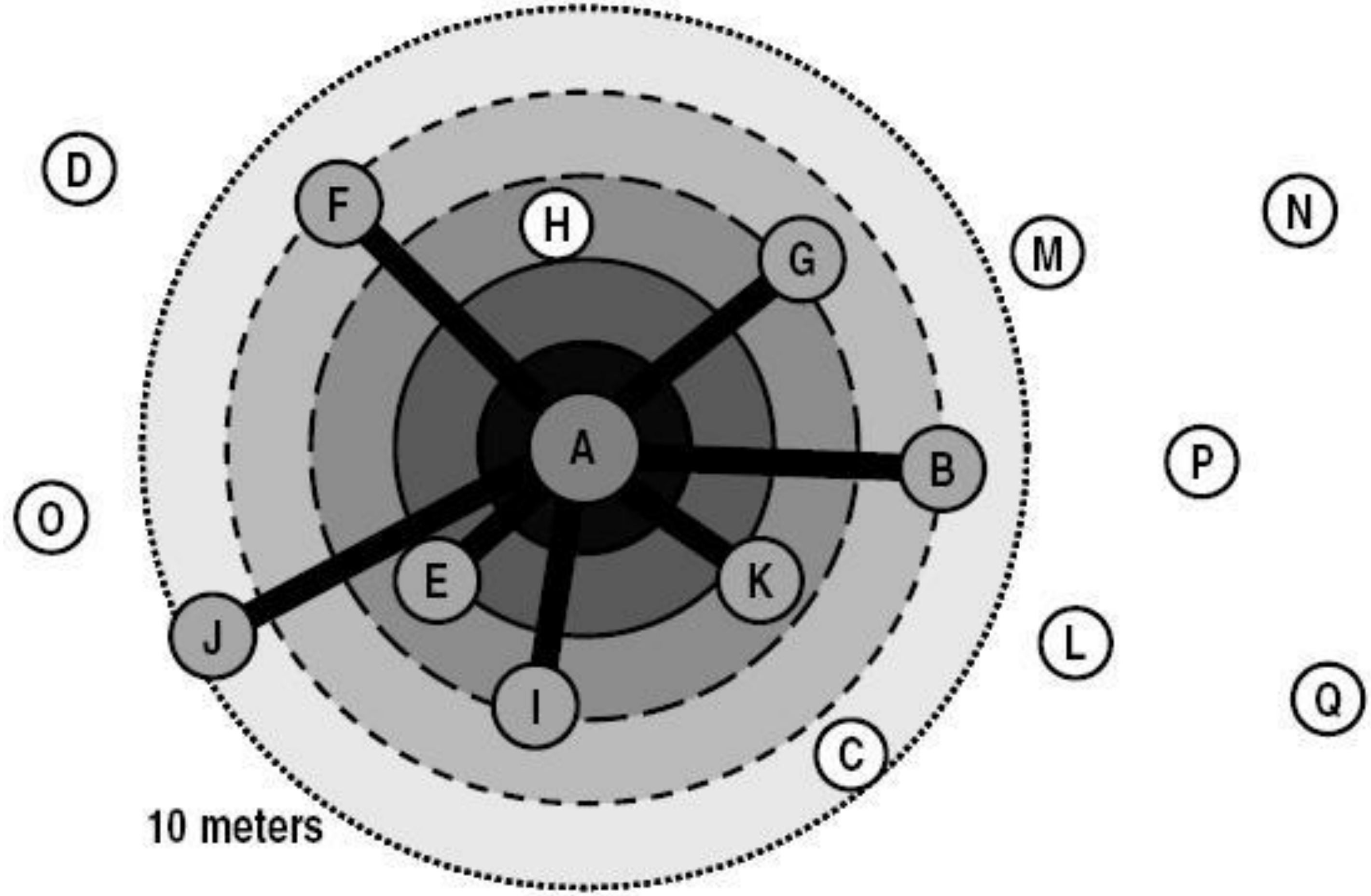
$16.00
$14.00
$12.00
$10.00
$8.00
$6.00
$4.00
$2.00
$0.00
$15.00
$7.50
$4.50
$3.15
$2.52
$2.02
2000
2001
2002
2003
2004
2005


Master
Slave
Slave
Slave
Slave
Piconet 1

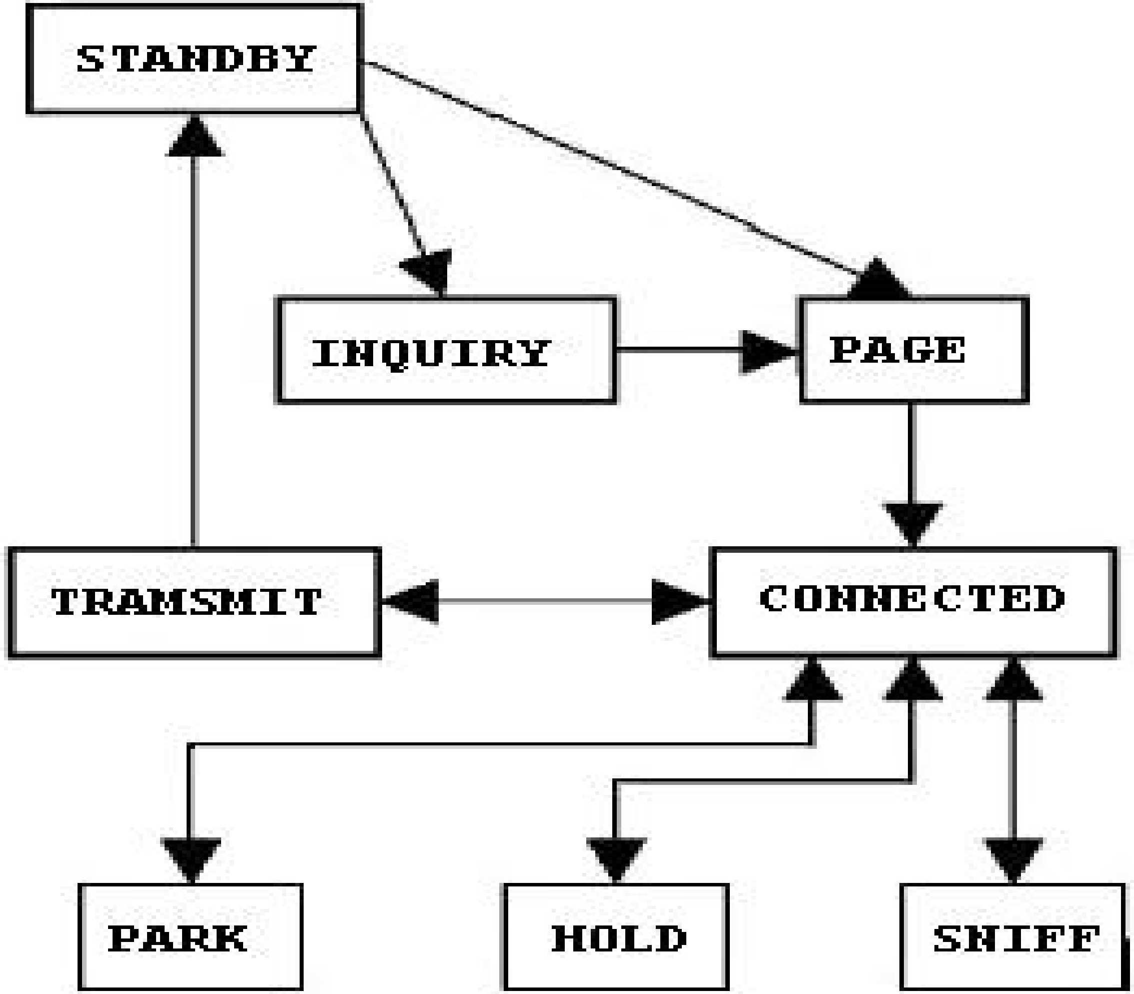
Inquiry



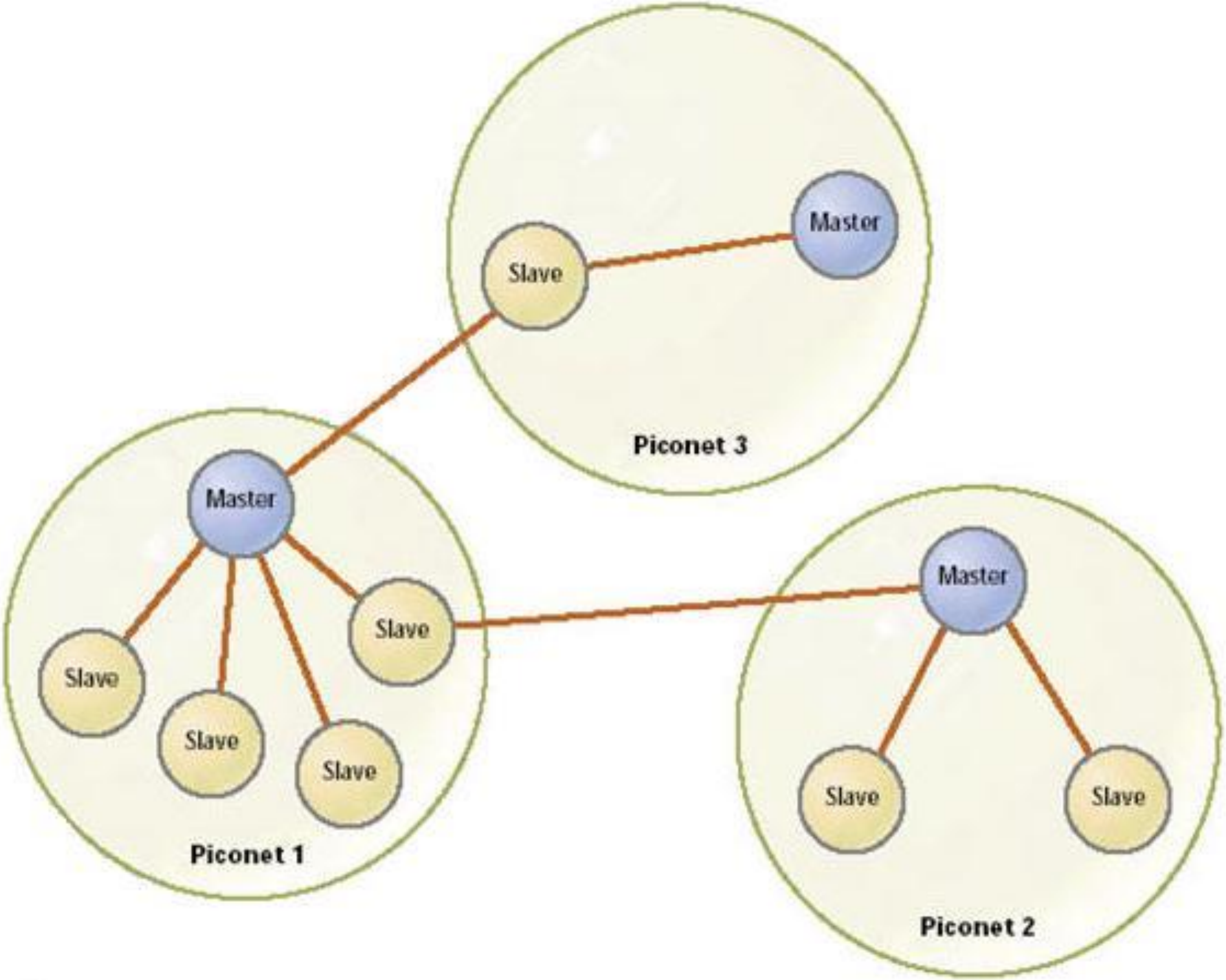
Paging



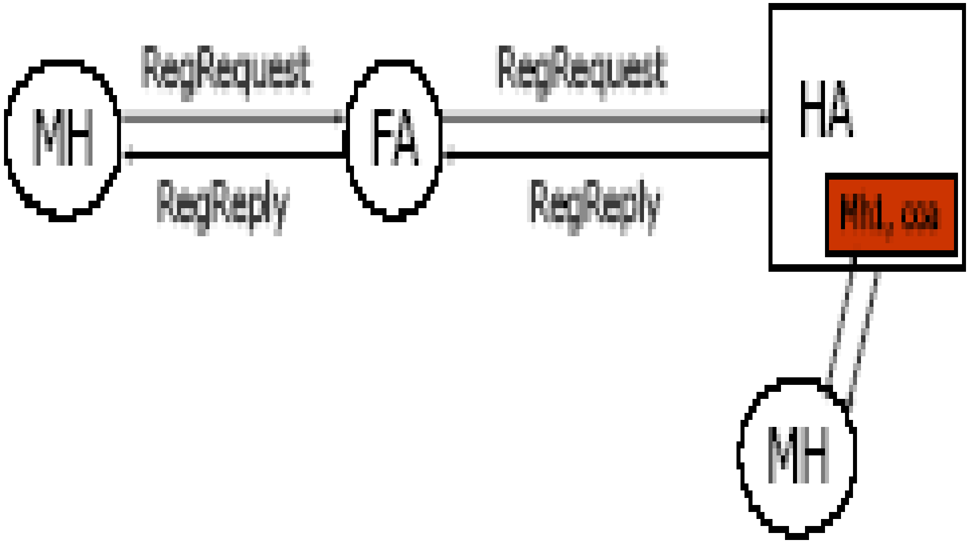
States

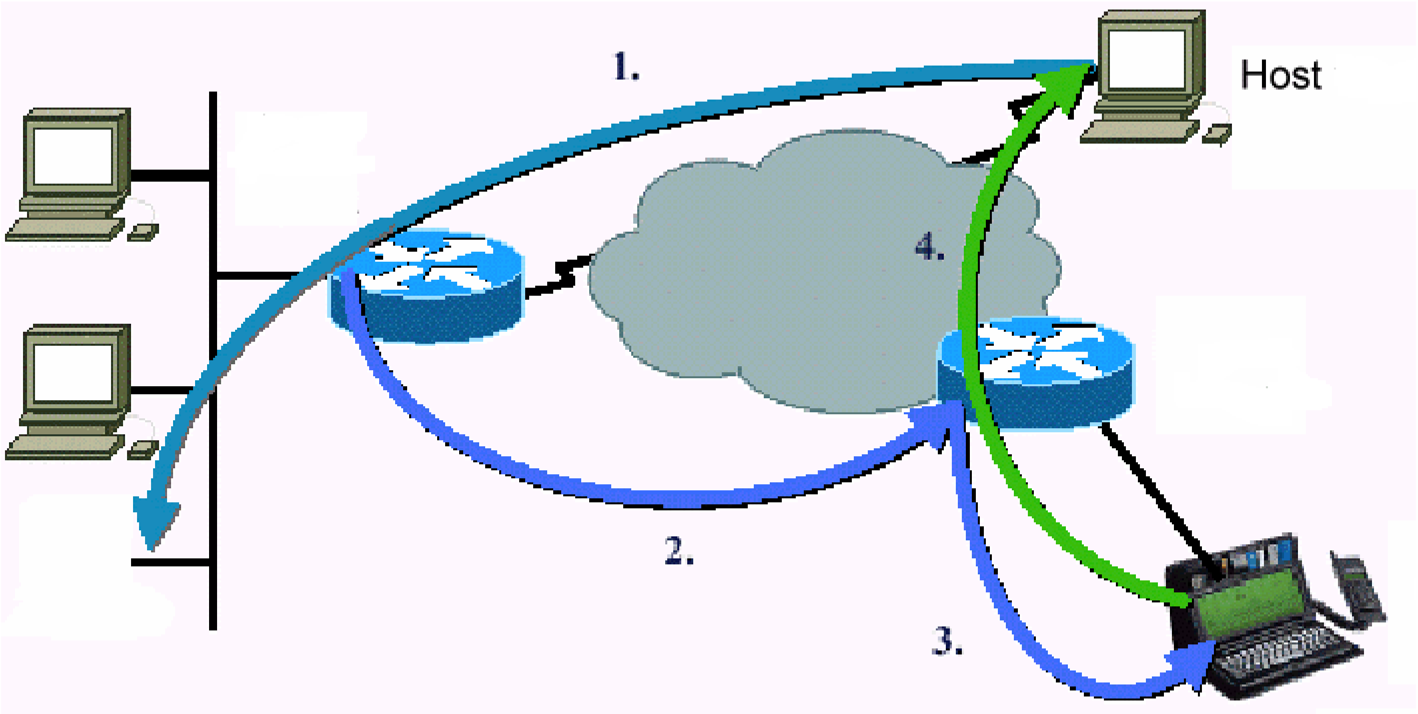


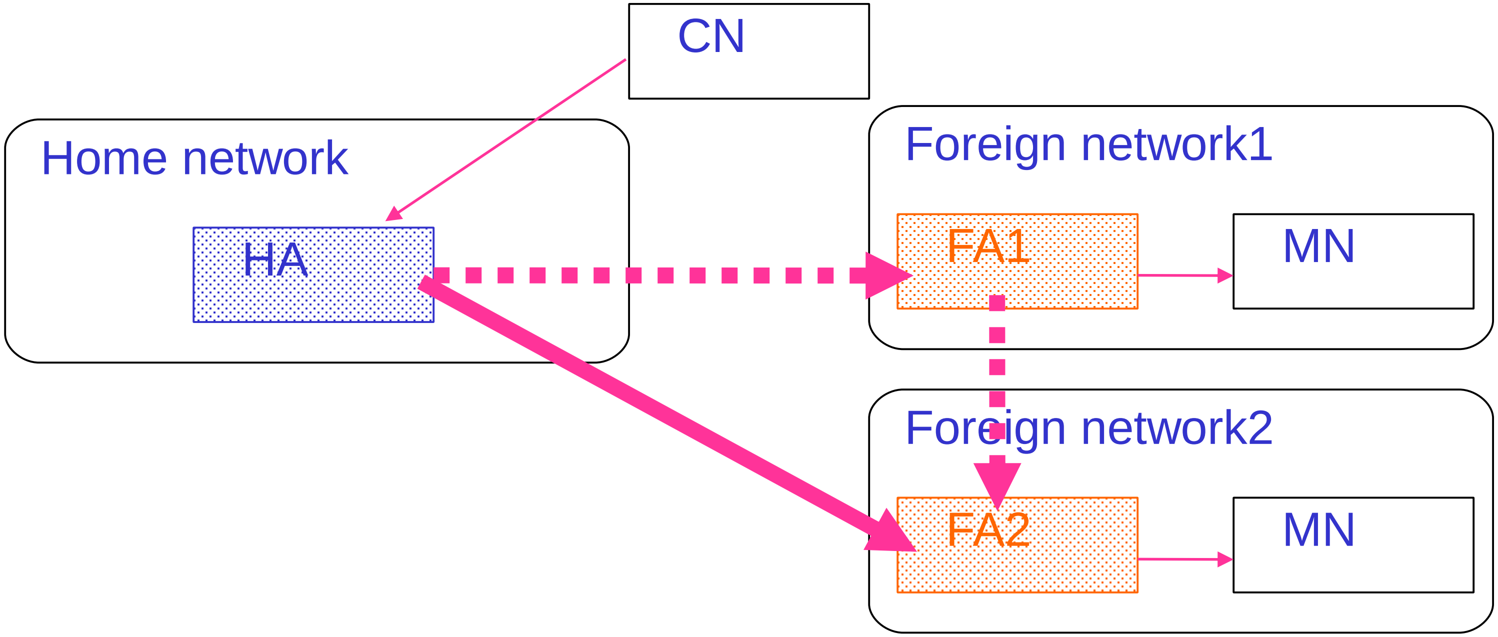
Scatternet


Master
Slave
Piconet 3
Master
Slave
Slave
Slave
Slave
Piconet 1
Master
Slave
Slave
Piconet 2

Mobile IP

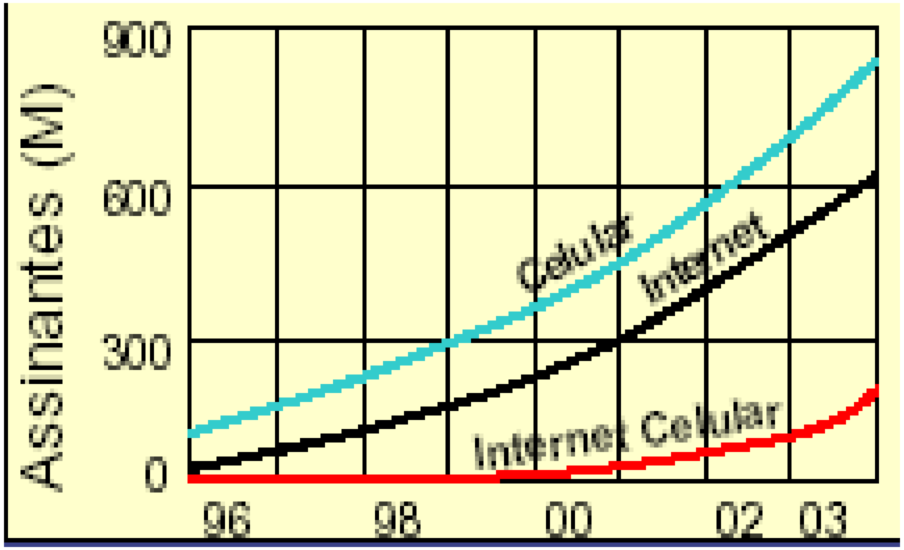

MH
RegRequest
FA
RegRequest
HA
RegReply
RegReply
Mh1, coa
MH


1.
Host
4.
2.
3.


CN
Home network
HA
Foreign network1
FA1
MN
Foreign network2
FA2
MN

GSM++ Technologies

- GSM
- HSCSD
- GPRS
- EDGE



Web site Ericsson

GSM - HSCSD – GPRS - EDGE

- **GSM - G**lobal **S**ystem for **M**obile communications

- **HSCSD** - **H**igh **S**peed **C**ircuit **S**witched **D**ata

- **GPRS** - **G**eneral **P**acket **R**adio **S**ervice

- **EDGE** = **E**nhanced **D**ata rates for **GSM E**volution

GSM

- 1979: reservation of the band of the 900 MHz for mobile communications in Europe (IUT);
- 1980: creation of GSM (Groupe Spécial Mobile) working group
- 1992: real commercialization of first systems GSM

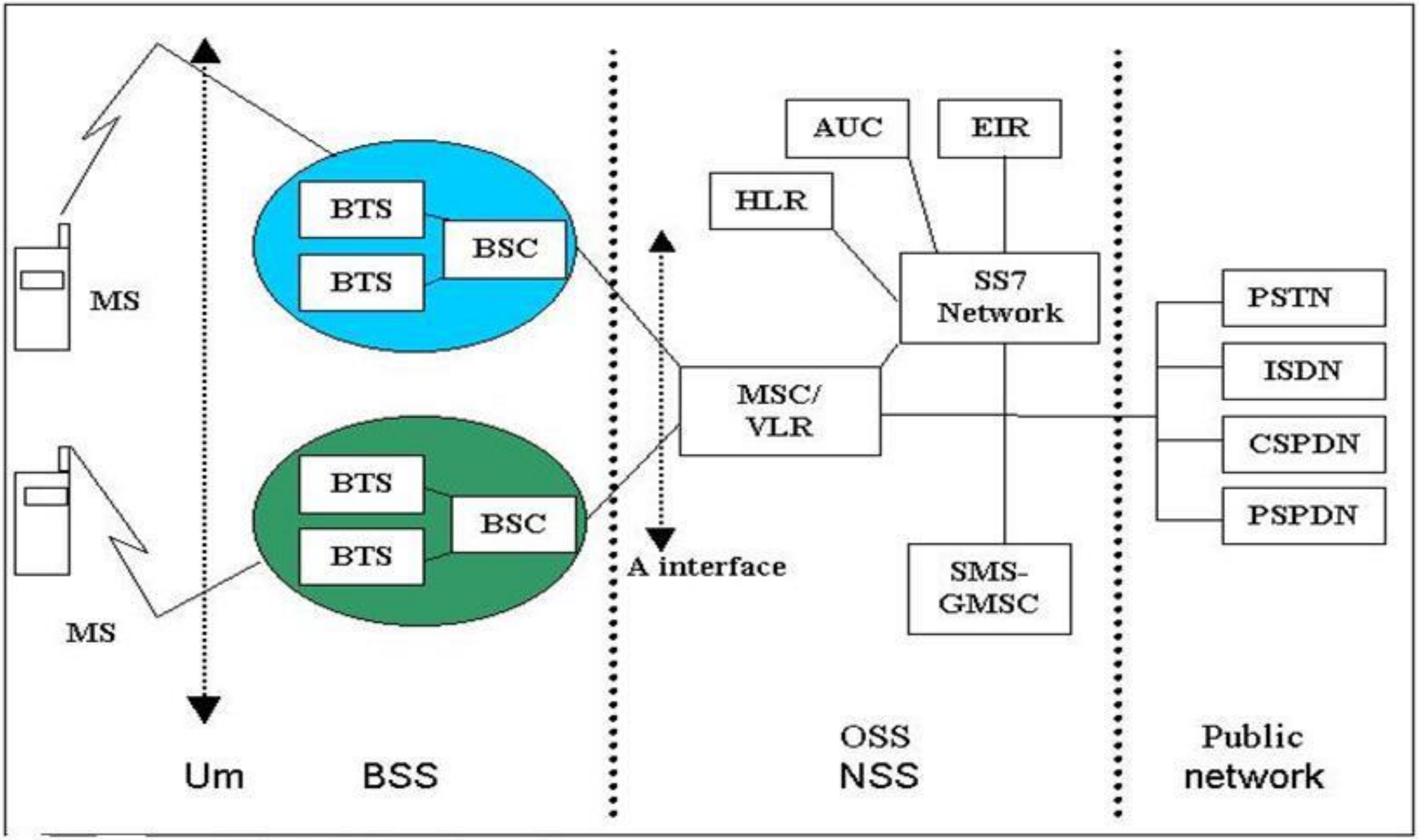
Since, the GSM communications left its French acronym for the one of Global System for Mobile communications and supplanted the analogical systems.

frequency:

- band 890-915 Mhz for the uplink (TM for BTS)

- band 935-960 Mhz for the downlink (BTS for TM)

General Architecture



BSS : Base Station Subsystem

- MS (Mobile Station) : visible part of the system mobile radio.

- BTS (Base Transceiver Station) : points of access net GSM. The BTSs are materialized under the form of antennas on the the buildings in the city or on the edge of the road.

- BSC (Base Station Controller) : a BSC generates the canals radios and the BTS applies the decisions taken by the BSC (as the control of admission of the calls and the management of handovers).

NSS : Network SubSystem

- MSC (Mobile-services Switching Center) : The MSC is a numerical switch that manages all the communications under its covering area;

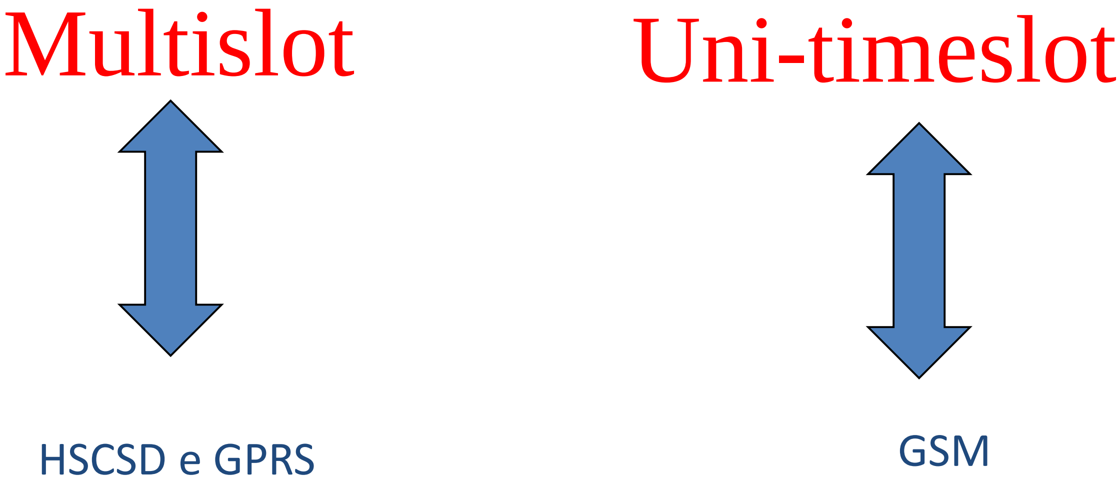
- HLR (Home Location Register) : database of nominal localization in which the relative information to the subscribers of a mobile net are stored;

- VLR (Visitor Location Register) : database of Local localization in which the relative information to the users of a specific region are stored .

GSM Services

- Voice
- Data
- Short Message Services (SMS)
- Sec.
- QoS!!!

HSCSD & GPRS vs GSM



Multislot

HSCSD e GPRS

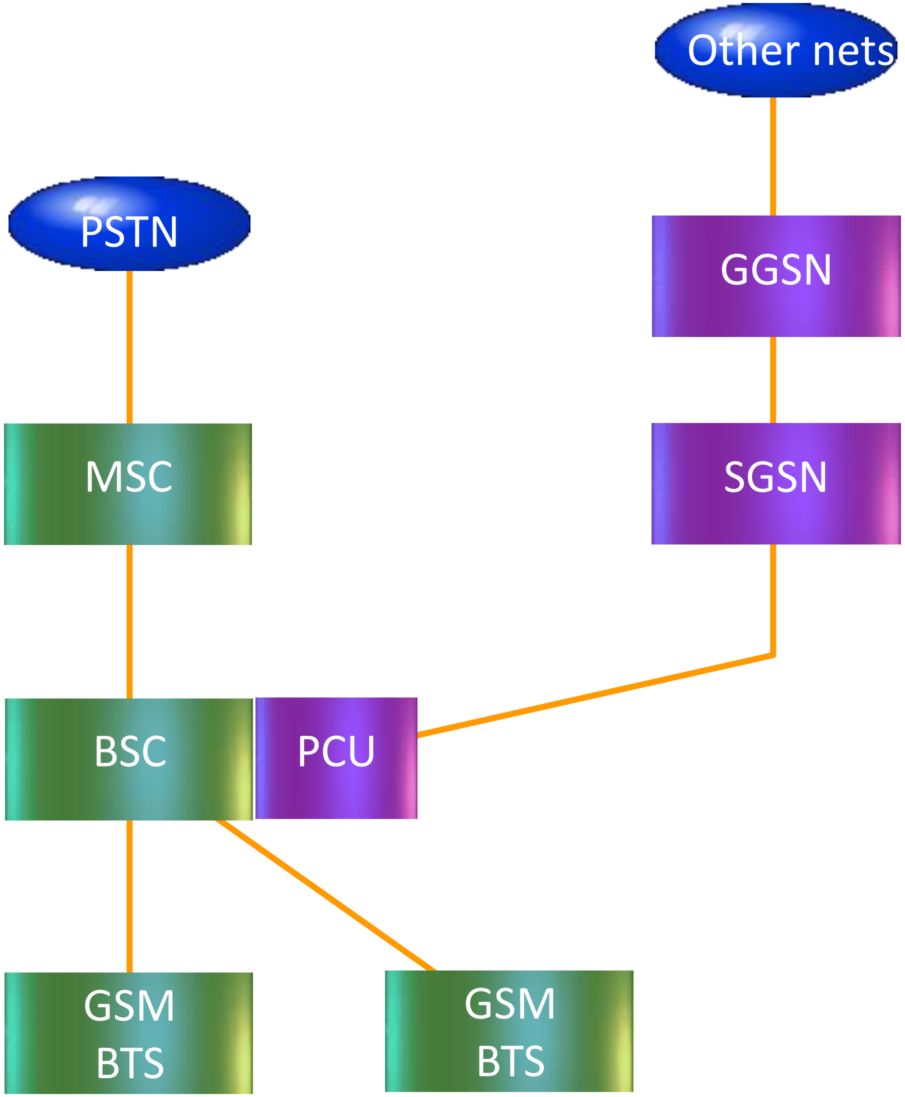
Uni-timeslot

GSM

GSM + GPRS

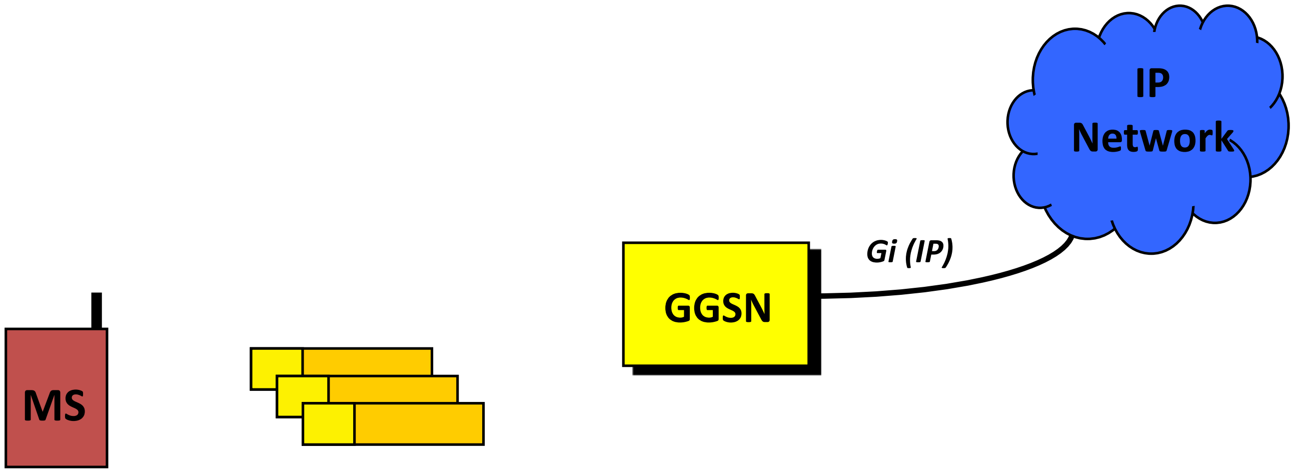
1. BSS : software upgrade
   hardware upgrade

2. New components
   (SGSN – GGSN)



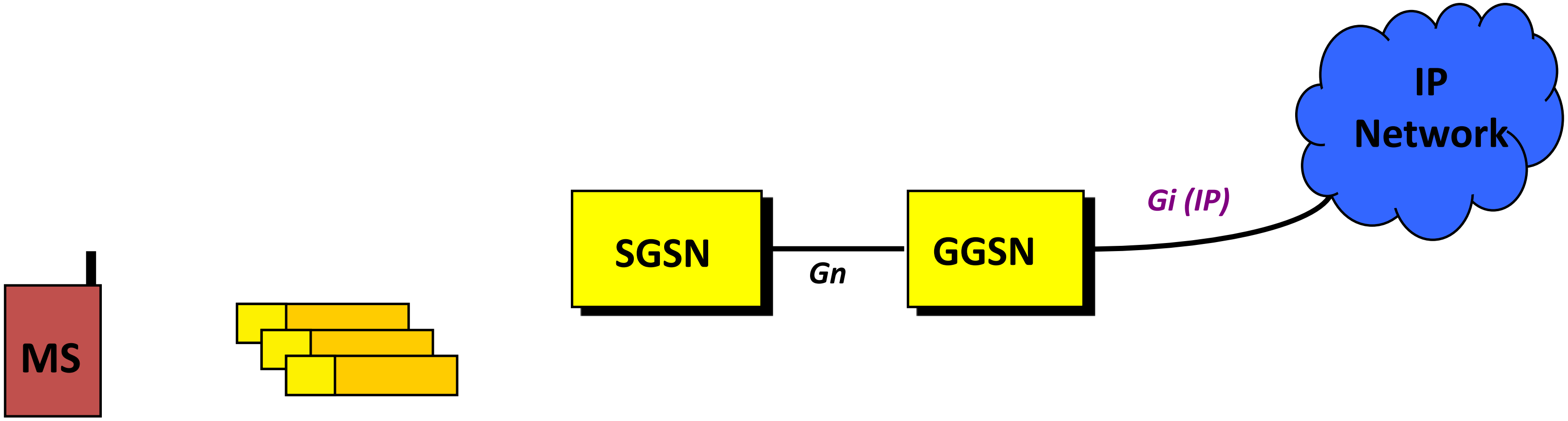
Gateway GPRS Support Node GGSN

- Interface for external Nets
- Like traditional Gateway
- Routing
- …



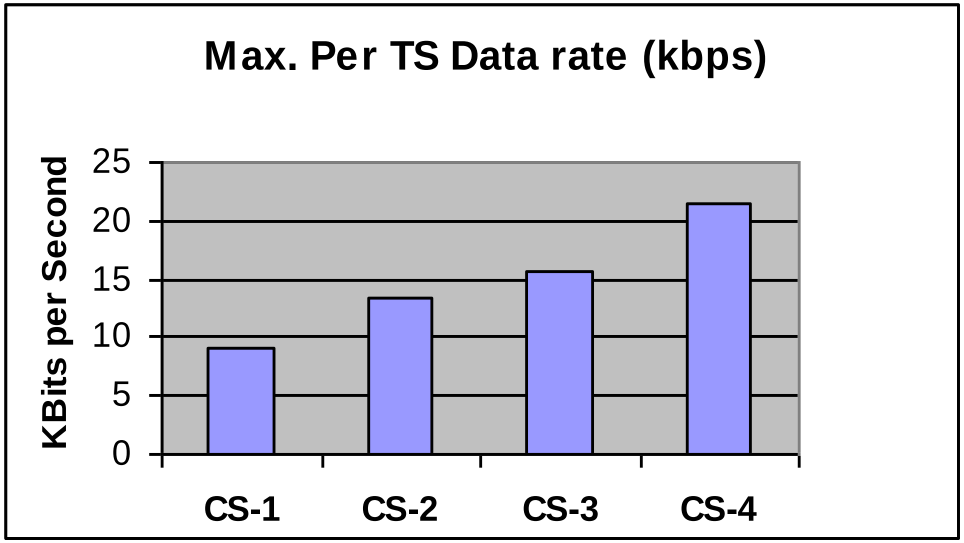
Serving GPRS Support Node - SGSN

- In same level like MSC
- Packets transfer between MS & GGSN.
- …

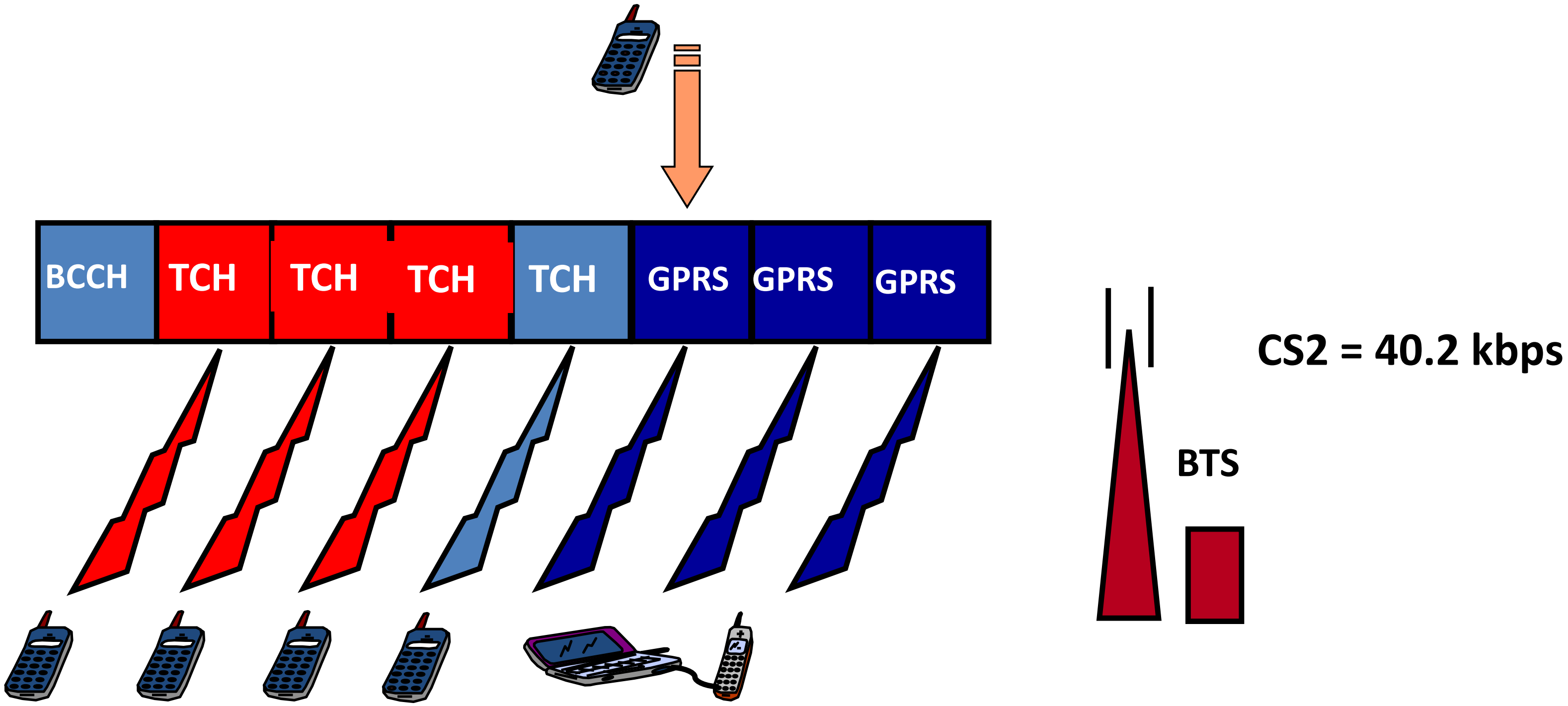


Coding Scheme

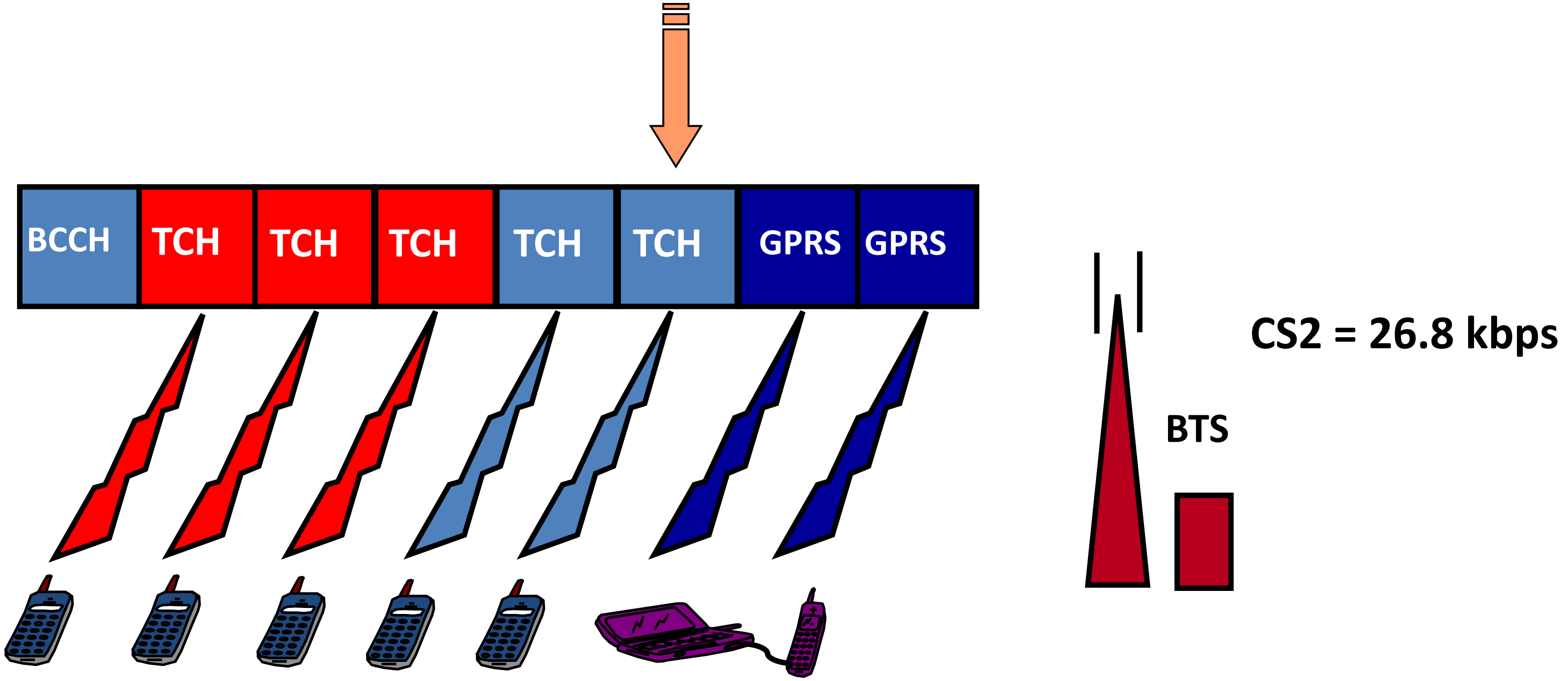
Coding Scheme	Coded bits	Punctured bits	Data Rate (kbps)	Multiple Slot Max. Data Rate (kbps)
CS-1	456	0	9,05	72,4
CS-2	588	132	13,4	107,2
CS-3	676	220	15,6	124,8
CS-4	456	0	21,4	171,2



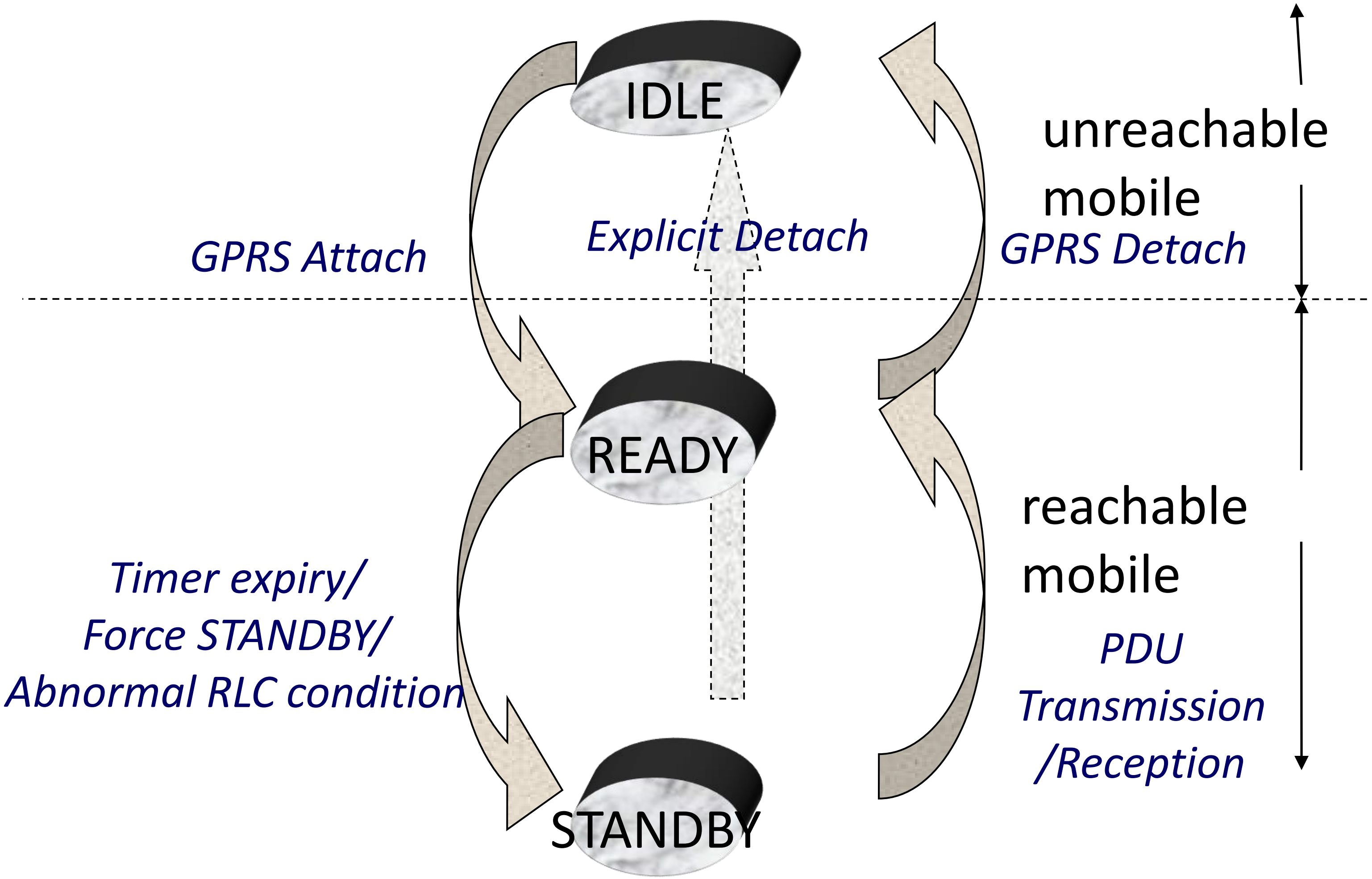
Timeslot sharing



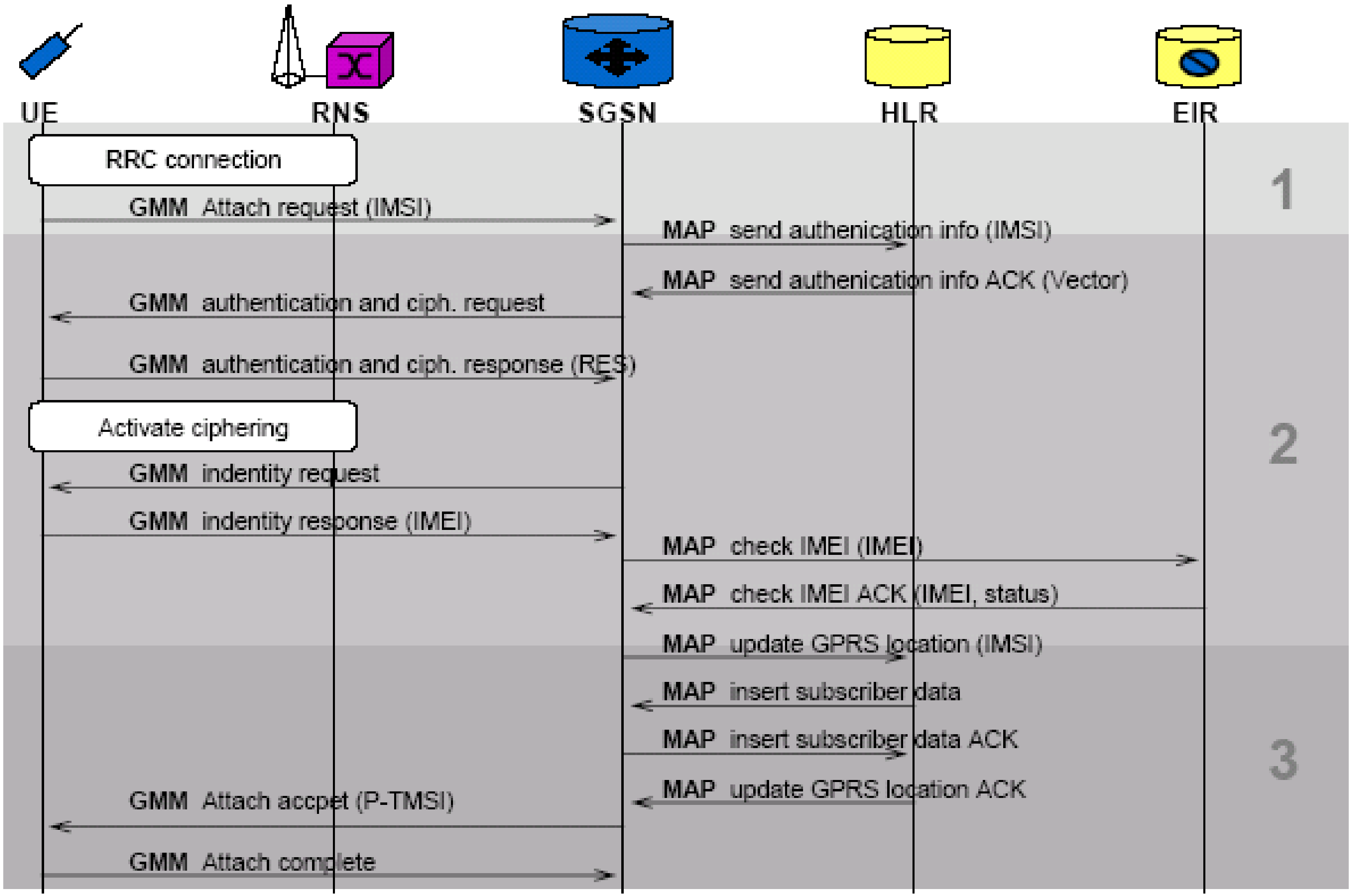
Timeslot sharing



MS States


IDLE
unreachable
mobile
Explicit Detach
GPRS Attach
GPRS Detach
READY
reachable
mobile
Timer expiry/
Force STANDBY/
Abnormal RLC condition
PDU
Transmission
/Reception
STANDBY

Attach



UE

RNS

SGSN

HLR

EIR

RRC connection

GMM Attach request (IMSI)

MAP send authenication info (IMSI)

MAP send authenication info ACK (Vector)

GMM authentication and ciph. request

GMM authentication and ciph. response (RES)

Activate ciphering

GMM indentity request

GMM indentity response (IMEI)

MAP check IMEI (IMEI)

MAP check IMEI ACK (IMEI, status)

MAP update GPRS location (IMSI)

MAP insert subscriber data

MAP insert subscriber data ACK

MAP update GPRS location ACK

GMM Attach accpet (P-TMSI)

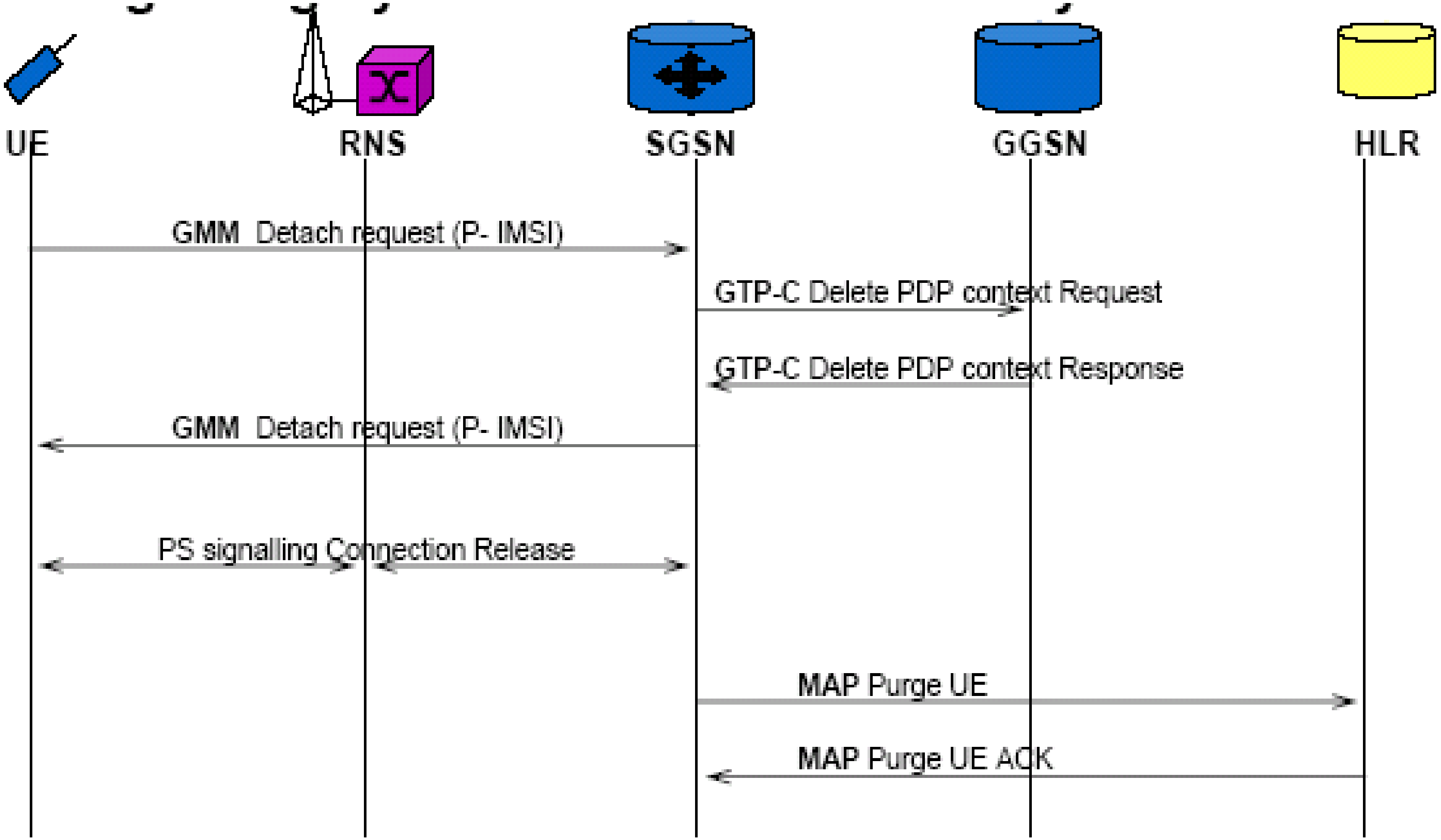
GMM Attach complete

1

2

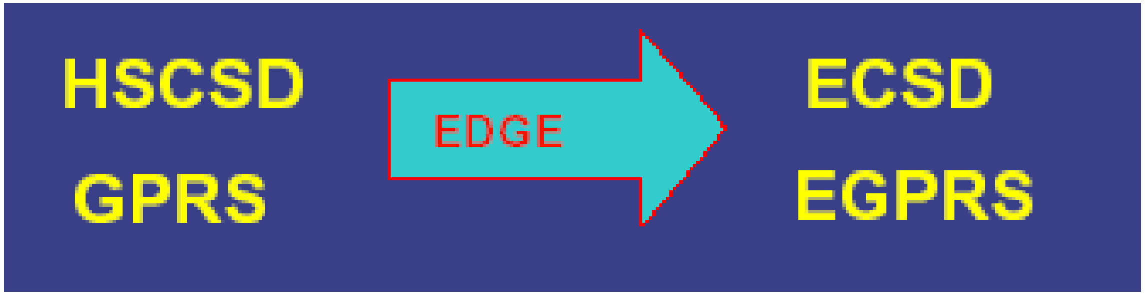
3

Detach

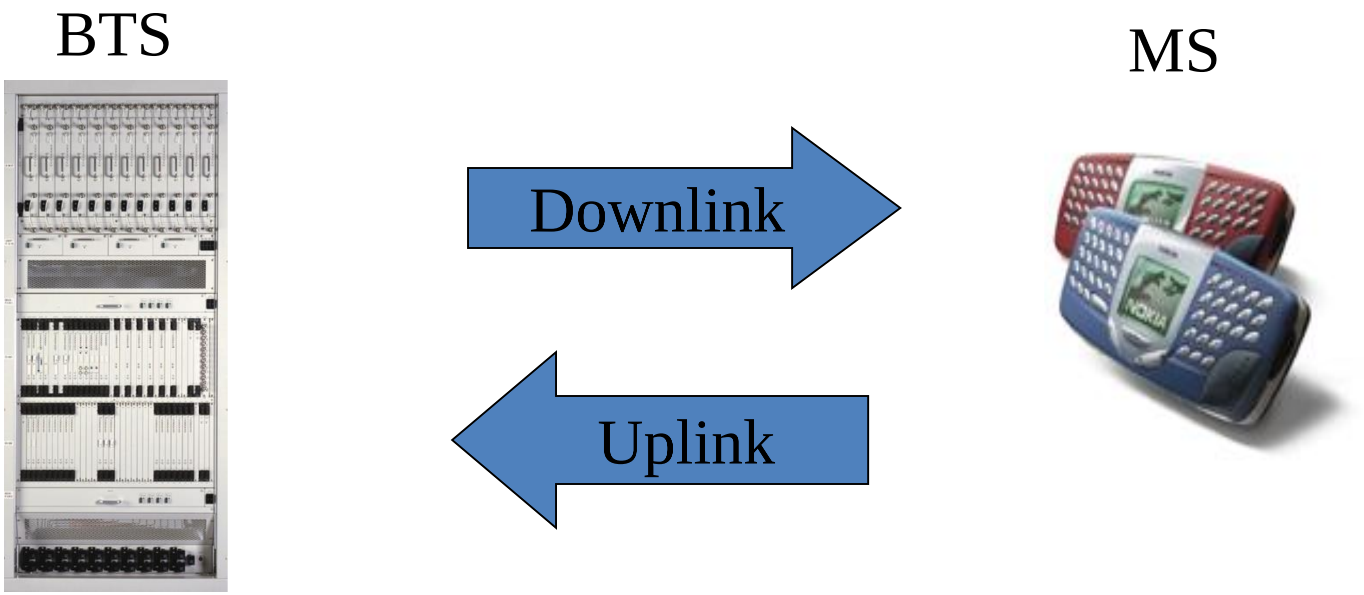

UE
RNS
SGSN
GGSN
HLR
GMM Detach request (P- IMSI)
GTP-C Delete PDP context Request
GTP-C Delete PDP context Response
GMM Detach request (P- IMSI)
PS signalling Connection Release
MAP Purge UE
MAP Purge UE ACK

EDGE

- **EDGE** = **E**nhanced **D**ata rates for **G**SM **E**volution



EDGE Classes



BTS

Downlink

Uplink

MS

Classe	Downlink	Uplink
A	8PSK	GMSK
B	8PSK	8PSK

EDGE Coding Schemes

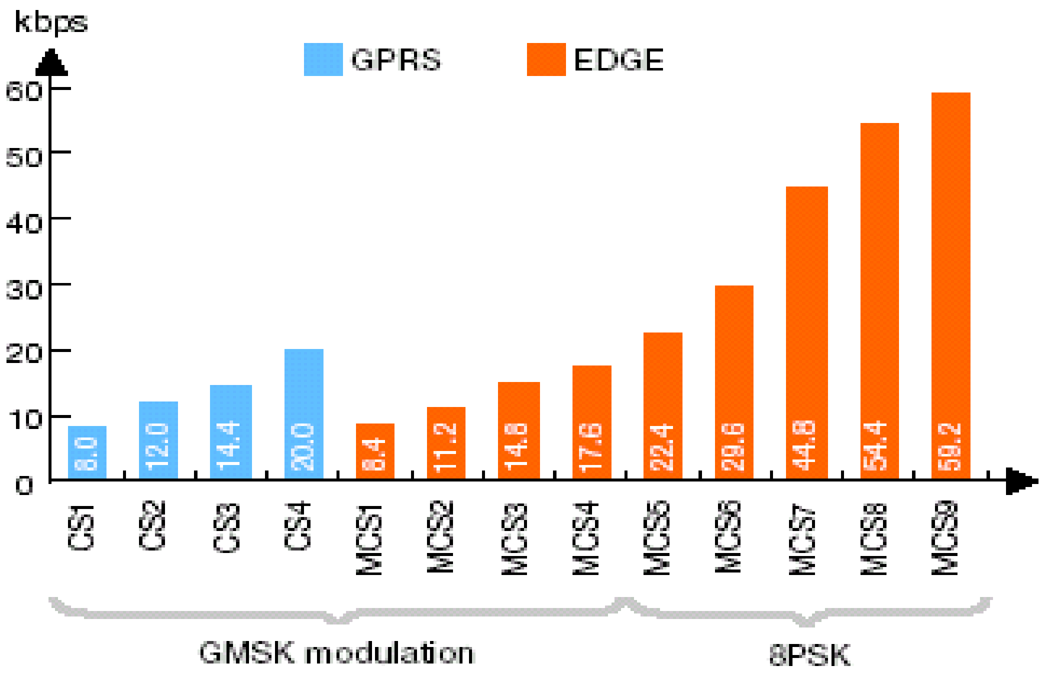
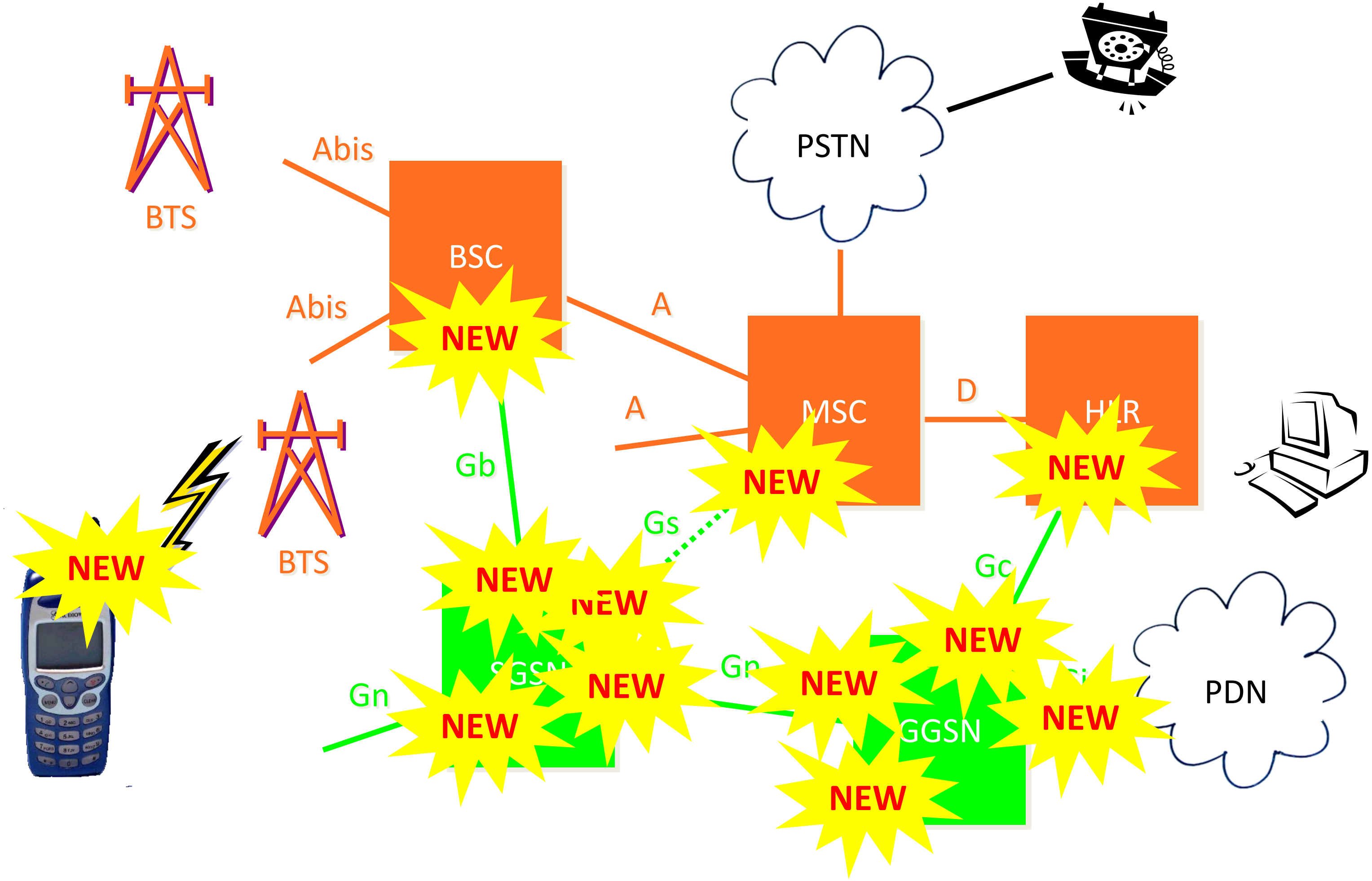


Figure 4. Coding schemes for GPRS and EGPRS (user data rate). (Key: 8PSK, 8-phase shift keying; CS, Coding scheme; EGPRS, Enhanced GPRS; GMSK, Gaussian minimum shift keying; MCS, Modulation coding scheme)

EDGE Impact

- Hardware upgrade in BSS
- Software upgrade for BS and BSC
- New Terminals
  - Terminal : 8PSK uplink e downlink
  - Terminal : GMSK uplink e 8PSK downlink

GSM + GPRS + EDGE



Wireless Networks Security

Prof. Amine Berqia
berqia@gmail.com

IEEE 802.11 Basic Security Mechanisms

- Service Set Identifier (SSID)
- MAC Address filtering

- Wired Equivalent Privacy (WEP) protocol

802.11 products are shipped by the vendors with all security mechanisms disabled !!

Service Set Identifier (SSID) and their limits!

- Limits access by identifying the service area covered by the access points.
- AP periodically broadcasts SSID in a beacon.
- End station listens to these broadcasts and chooses an AP to associate with based upon its SSID.
- Use of SSID – weak form of security as beacon management frames on 802.11 WLAN are always sent in the clear.
- A hacker can use analysis tools (eg. AirMagnet, Netstumbler, AiroPeek) to identify SSID.
- Some vendors use default SSIDs which are pretty well known (eg. CISCO uses tsunami)

MAC Address Filtering

The system administrator can specify a list of MAC addresses that can communicate through an access point.

Advantage :

- Provides a little stronger security than SSID

Disadvantages :

- Increases Administrative overhead
- Reduces Scalability
- Determined hackers can still break it

Wired Equivalent Privacy (WEP)

- Designed to provide confidentiality to a wireless network similar to that of standard LANs.
- WEP is essentially the RC4 symmetric key cryptographic algorithm (same key for encrypting and decrypting).
- Transmitting station concatenates 40 bit key with a 24 bit Initialization Vector (IV) to produce pseudorandom key stream.
- Plaintext is XORed with the pseudorandom key stream to produce ciphertext.
- Ciphertext is concatenated with IV and transmitted over the Wireless Medium.
- Receiving station reads the IV, concatenates it with the secret key to produce local copy of the pseudorandom key stream.
- Received ciphertext is XORed with the key stream generated to get back the plaintext.

WEP – vulnerability to attack

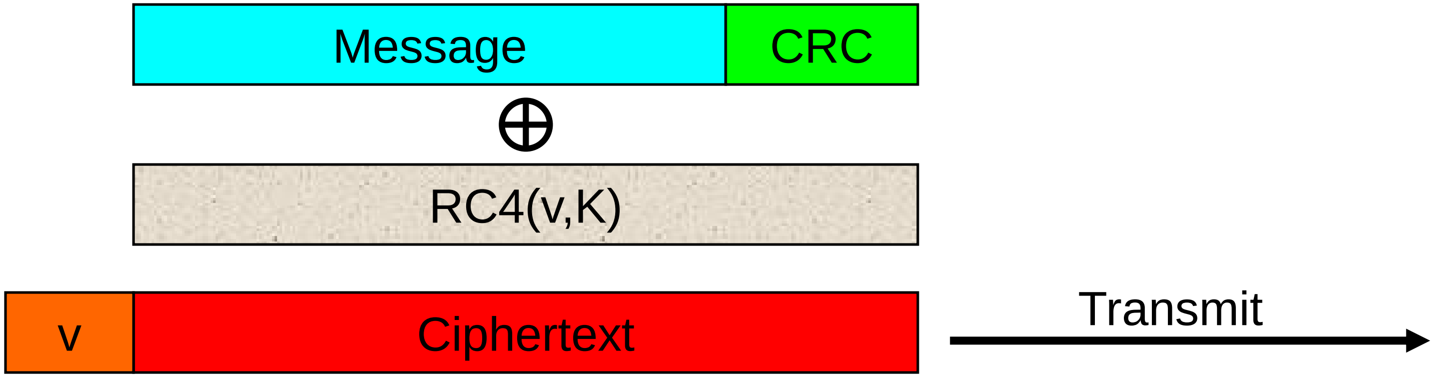
- WEP has been broken! Walker (Oct 2000), Borisov et. al. (Jan 2001), Fluhrer-Mantin -Shamir (Aug 2001).
- Unsafe at any key size : Testing reveals WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size.
- More about this at: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

WEP Overview

- WEP relies on a shared key K between communicating parties

1. **Checksum:** For a message M, we calculate c(M). The plaintext is P={M,c(M)}
2. **Encryption:** The plaintext is encrypted using RC4. RC4 requires an initialization vector (IV) v, and the key K. Output is a stream of bits called the keystream. Encryption is XOR with P.
3. **Transmission:** The IV and the ciphertext C are transmitted.

$$C = P \oplus RC4(v, K)$$



WEP Security Goals

- WEP had three main security goals:
  - Confidentiality: Prevent eavesdropping
  - Access Control: Prevent inappropriate use of 802.11 network, such as facilitate dropping of not-authorized packets
  - Data Integrity: Ensure that messages are not altered or tampered with in transit
- The basic WEP standard uses a 40-bit key (with 24bit IV)
- Additionally, many implementations allow for 104-bit key (with 24bit IV)
- None of the three goals are provided in WEP due to serious security design flaws and the fact that it is easy to eavesdrop on WLAN

128 bit WEP

- Vendors have extended WEP to 128 bit keys.
  - 104 bit secret key.
  - 24 bit IV.
- Brute force takes 10^19 years for 104-bit key.
- Effectively safeguards against brute force attacks.

Key Scheduling Weakness

- Paper from Fluhrer, Mantin, Shamir, 2001.
- Two weaknesses:
  - Certain keys leak into key stream.
    - Invariance weakness.
  - If portion of PRNG input is exposed,
    - Analysis of initial key stream allows key to be determined.
    - IV weakness.

IV weakness

- WEP exposes part of PRNG input.
  - IV is transmitted with message.
  - Every wireless frame has reliable first byte
    - Sub-network Access Protocol header (SNAP) used in logical link control layer, upper sub-layer of data link layer.
    - First byte is 0xAA
  - Attack is:
    - Capture packets with weak IV
    - First byte ciphertext XOR 0xAA = First byte key stream
    - Can determine key from initial key stream
- Practical for 40 bit and 104 bit keys
- Passive attack.
  - Non-intrusive.
  - No warning.

Wepcrack

- First tool to demonstrate attack using IV weakness.
  - Open source, Anton Rager.
- Three components
  - Weaker IV generator.
  - Search sniffer output for weaker IVs & record 1st byte.
  - Cracker to combine weaker IVs and selected 1st bytes.
- Cumbersome.

Airsnort

- Automated tool
  - Cypher42, Minnesota, USA.
  - Does it all!
  - Sniffs
  - Searches for weaker IVs
  - Records encrypted data
  - Until key is derived.
- 100 Mb to 1 Gb of transmitted data.
- 3 to 4 hours on a very busy WLAN.

Avoid the weak IVs

- FMS described a simple method to find weak IVs
  - Many manufacturers avoid those IVs after 2002
  - Therefore Airsnort and others may not work on recent hardware
- However David Hulton aka h1kari
  - Properly implemented FMS attack which shows many more weak IVs
  - Identified IVs that leak into second byte of key stream.
  - Second byte of SNAP header is also 0xAA
  - So attack still works on recent hardware
  - And is faster on older hardware
  - Dwepcrack, weplab, aircrack

Generating WEP traffic

- Not capturing enough traffic?
  - Capture encrypted ARP request packets
  - Anecdotally lengths of 68, 118 and 368 bytes appear appropriate
  - Replay encrypted ARP packets to generate encrypted ARP replies
  - Aireplay implements this.

802.11 safeguards

- Security Policy & Architecture Design
- Treat as untrusted LAN
- Discover unauthorised use
- Access point audits
- Station protection
- Access point location
- Antenna design

Security Policy & Architecture

- Define use of wireless network
  - What is allowed
  - What is not allowed
- Holistic architecture and implementation
  - Consider all threats.
  - Design entire architecture
    - To minimise risk.

Wireless as untrusted LAN

- Treat wireless as untrusted.
  - Similar to Internet.
- Firewall between WLAN and Backbone.
- Extra authentication required.
- Intrusion Detection
  - at WLAN / Backbone junction.
- Vulnerability assessments

Discover unauthorised use

- Search for unauthorised access points, ad-hoc networks or clients.
- Port scanning
  - For unknown SNMP agents.
  - For unknown web or telnet interfaces.
- Warwalking!
  - Sniff 802.11 packets
  - Identify IP addresses
  - Detect signal strength
  - But may sniff your neighbours…
- Wireless Intrusion Detection
  - AirMagnet, AirDefense, Trapeze, Aruba,…

Access point audits

- Review security of access points.
- Are passwords and community strings secure?
- Use Firewalls & router ACLs
  - Limit use of access point administration interfaces.
- Standard access point config:
  - SSID
  - WEP keys
  - Community string & password policy

Station protection

- Personal firewalls
  - Protect the station from attackers.
- VPN from station into Intranet
  - End-to-end encryption into the trusted network.
  - But consider roaming issues.
- Host intrusion detection
  - Provide early warning of intrusions onto a station.
- Configuration scanning
  - Check that stations are securely configured.

Location of Access Points

- Ideally locate access points
  - In centre of buildings.
- Try to avoid access points
  - By windows
  - On external walls
  - Line of sight to outside
- Use directional antenna to “point” radio signal.

WPA

- Wi-Fi Protected Access
  - Works with 802.11b, a and g
- “Fixes” WEP’s problems
- Existing hardware can be used
- 802.1x user-level authentication
- TKIP
  - RC4 session-based dynamic encryption keys
  - Per-packet key derivation
  - Unicast and broadcast key management
  - New 48 bit IV with new sequencing method
  - Michael 8 byte message integrity code (MIC)
- Optional AES support to replace RC4

WPA and 802.1x

- 802.1x is a general purpose network access control mechanism
- WPA has two modes
  - Pre-shared mode, uses pre-shared keys
  - Enterprise mode, uses Extensible Authentication Protocol (EAP) with a RADIUS server making the authentication decision
  - EAP is a transport for authentication, not authentication itself
  - EAP allows arbitrary authentication methods
  - For example, Windows supports
    - EAP-TLS requiring client and server certificates
    - PEAP-MS-CHAPv2

Practical WPA attacks

- Dictionary attack on pre-shared key mode
  - CoWPAtty, Joshua Wright
- Denial of service attack
  - If WPA equipment sees two packets with invalid MICs in 1 second
    - All clients are disassociated
    - All activity stopped for one minute
    - Two malicious packets a minute enough to stop a wireless network

802.11i

- Robust Security Network extends WPA
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - Based on a mode of AES, with 128 bits keys and 48 bit IV.
  - Also adds dynamic negotiation of authentication and encryption algorithms
  - Allows for future change
- Does require new hardware
- www.drizzle.com/~aboba/IEEE/

Relevant RFCs

- Radius Extensions: RFC 2869
- EAP: RFC 2284
- EAP-TLS: RFC 2716