Wireless Networks

Some Basic Observations

Wireless

- Free-space electromagnetic transmission
- Radio, optical, IR

Differs from wired at infrastructure layers

- Physical transmission / reception
- Medium access issues

Application programmer usually ignores infrastructure

- Generally sees OS-provided network API (sockets)
- Special case — telephone / PDA applications

Special issues in wireless infrastructures

- Mobility management
- Broadcast infrastructure
- Channel reliability

Wireless Personal Area Network (wPAN)

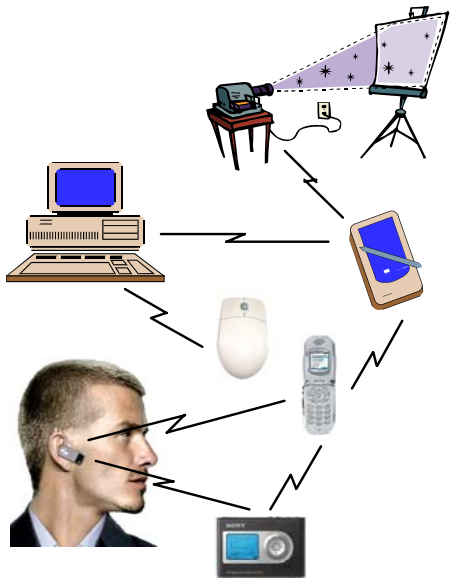
Short range broadcast transmission

Standard technologies

- Bluetooth
- Infrared Data Association (IrDA)
- Wireless USB

Applications

- Wireless computer peripherals
- Bluetooth earpiece
- Transfer interface for laptops, PDAs, cellphones
- Remote control



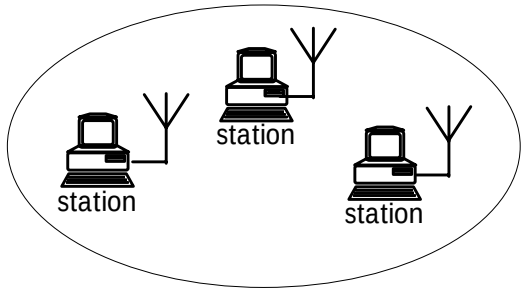
Wireless Local Area Networks

Wireless equivalent to local Ethernet

- Wireless network card
- Defines user authentication and encryption
- No external connection

Standard technologies

- IEEE 802.11 (WiFi)
- Bluetooth
- IrDA



Basic Wireless LAN

Wireless LAN with WAN Infrastructure

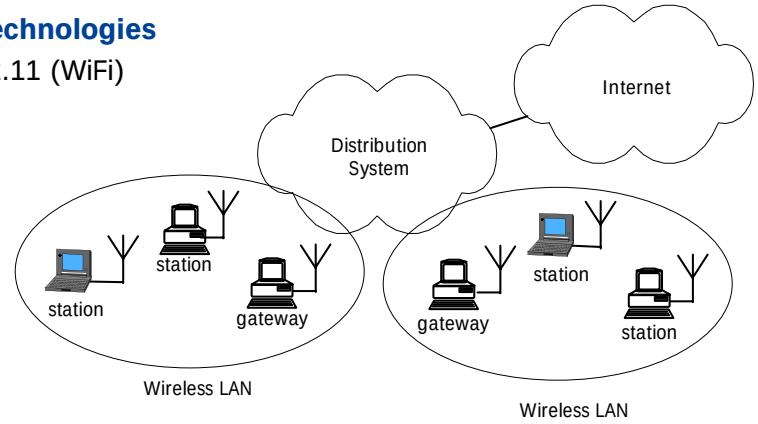
Extension of wireless LAN

Allows mobile access to external networks

Allows roaming between wLAN groups

Standard technologies

IEEE 802.11 (WiFi)



Wireless LAN Access to WAN

Cellular Telephony

Medium range broadcast with private channel assignment

Standard technologies

AMPS / TACS (1G)

GSM / d-AMPS (2G)

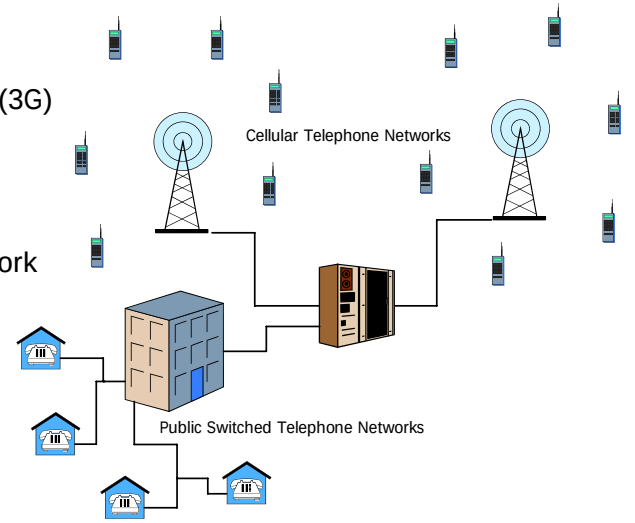
CDMA (2G)

UMTS / CDMA2000 (3G)

WCDMA (4G)

Application

Wireless voice network



Cellular Data Networks and Wireless IP

Wireless wide area data network (wWAN)

Data WAN over cellular telephone network

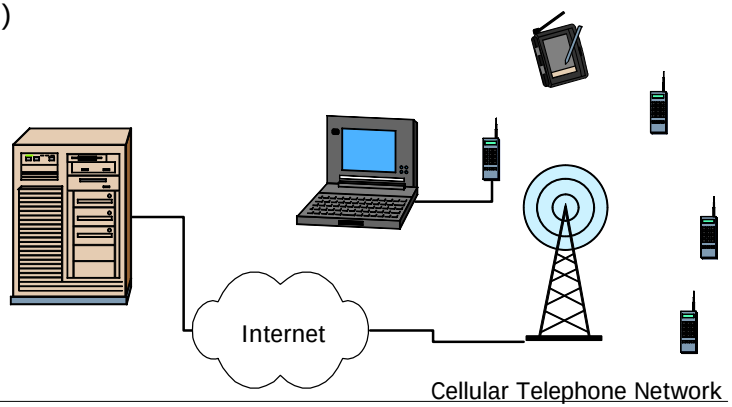
Standard technologies

CDPD (1.5G)

GPRS (2G)

EDGE (2.5G)

UMTS (3G)



Cellular Telephone Network

Wireless Application Protocol (WAP)

Protocol stack for mobile web interface

Adapts web for

- Phone screens
- PDA keypad

WML interactive scripting language



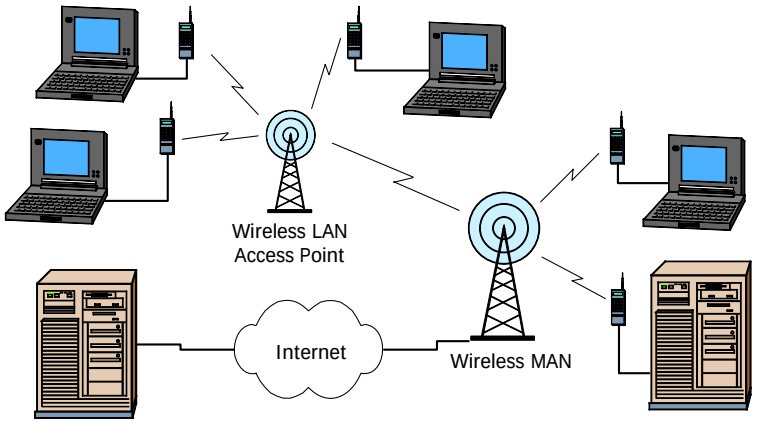
Wireless Metropolitan Area Network (wMAN)

Cellular broadband data access

WAN access via wireless network

Standard technologies

IEEE 802.16 (WiMAX)



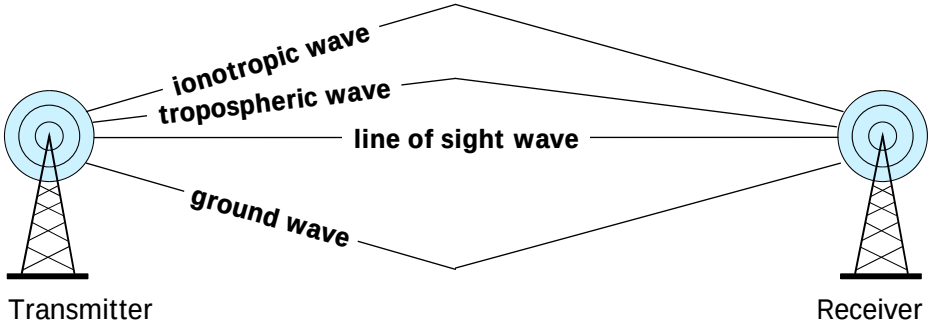
Radio Wave Propagation

Transmitter generates radio waves

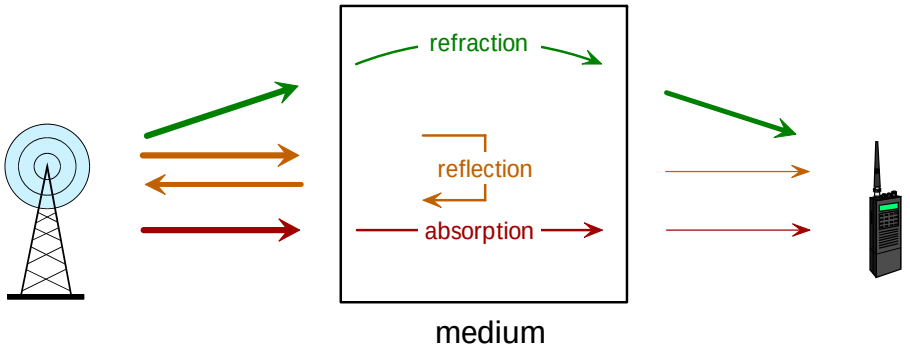
Waves propagate (spread out) through space

Part of radiated power may be obstructed

Part of radiated power is detected by receiver



Interference with Radio Signals



Multipath Fading

Obstacles reflect radio waves

Receiver gets signals from multiple paths

Time-to-arrive depends on path taken by signal

Receiver gets signals transmitted at different times

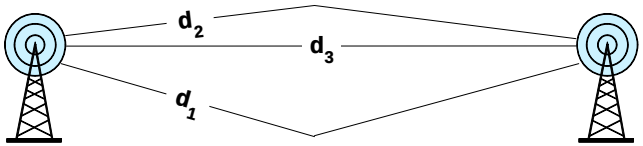
Example

Three signals sent at times $t_1 < t_2 < t_3$

Antenna receives all three signals at time t

- Signal 1 — sent first and followed longest path d_1
- Signal 2 — sent second and followed second longest path $d_2 < d_1$
- Signal 3 — sent last and followed shortest path $d_3 < d_2$

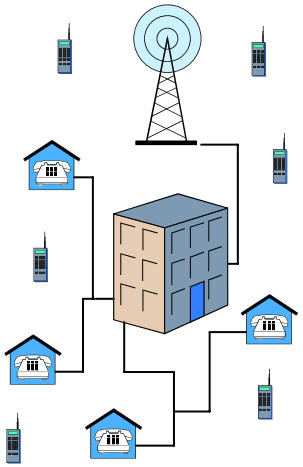
Sum of waves can cancel out signals



0G (1970) Mobile Phone System (MPS)

One central transceiver (transmitter/receiver)

- Mobile telephones communicate via central transceiver
- Transmit at high power for maximum distance
- System covers 65 to 80 km



Modulation is standard analog FM

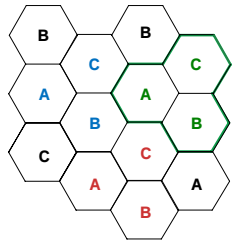
- Supports 12 simultaneous mobile phone calls
- If 12 channels busy, other calls are blocked

Requires 24 carrier frequencies

- 2 frequencies per phone:
  - Dedicated transmit frequency
  - Dedicated receive frequency

Cellular Concept

Divide coverage area into cells



In each cell

- Central cell transceiver serves all clients in cell
- Mobile Stations communicate via cell transceiver

Transmit at low power (just enough to cover a cell)

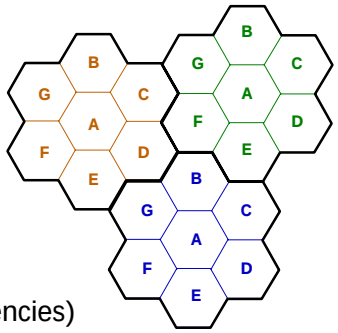
- Use same frequencies in many cells
- No interference between cells

Handoff

- Telephone can move from cell to cell during a call
- Requires cell-to-cell infrastructure and coordination

Cell Implementation

Divide region into clusters



Divide cluster into seven cells

- A, B, … , G

In each cell

- One central transceiver
- Many mobile stations (telephones)
- A frequency group (set of dedicated frequencies)

Each telephone has a private link with central transceiver

- Dedicated transmit frequency
- Dedicated receive frequency

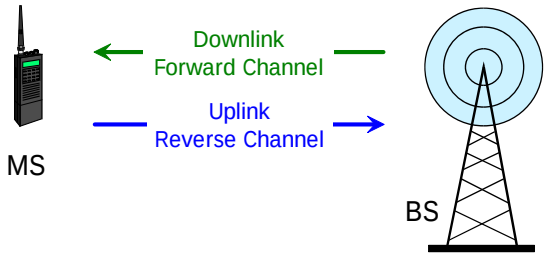
7 cell reuse

- Frequency group A assigned to every A cell
- Frequency group B to every B cell, ...
- At least two cells separate every pair of A cells, etc.

Transmission Directions

Downlink

- Base Station (BS) transmit frequency
- Mobile Station receive frequency
- Forward Channel



Uplink

- Mobile Station (MS) transmit frequency
- Base Station receive frequency
- Reverse Channel

Handoff

User moves between cells

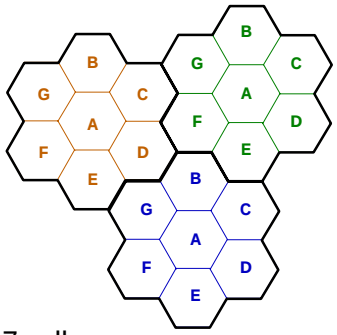
Hard Handoff

- Old cell transfers control to new cell
- Break-Before-Make sequence
  - Transceiver in old cell stops transmitting to user
  - Transceiver in new cell begins transmitting to user
- New BS assigns user frequency pair from its frequency group

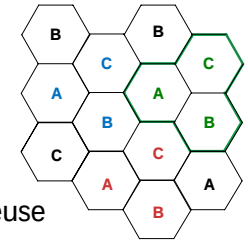
Soft Handoff

- Central transceiver coordinates with nearest cells
- Determines which transmitter is receiving strongest signal from user
- Make-Before-Break sequence
  - Transceiver in old cell transmitting to user
  - Transceiver in new cell begins transmitting to user
  - Transceiver in old cell stops transmitting to user

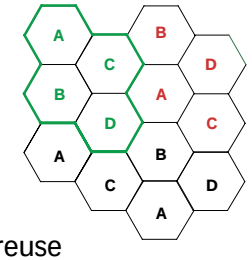
Reuse Patterns



7 cell reuse



3 cell reuse

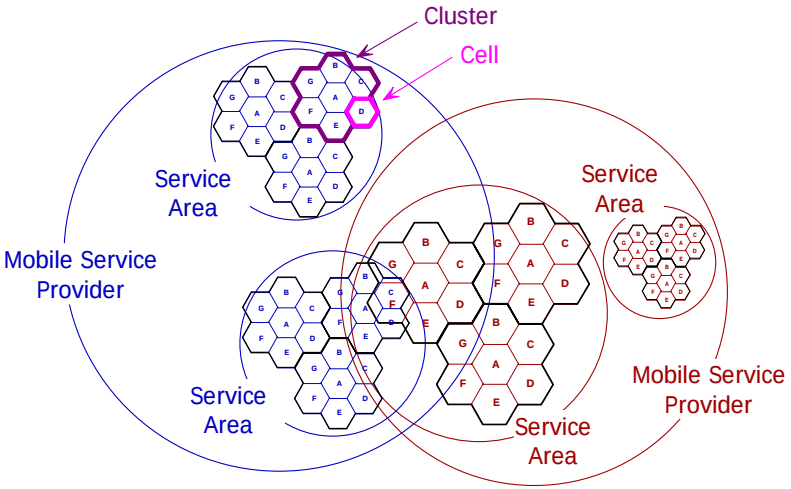


4 cell reuse

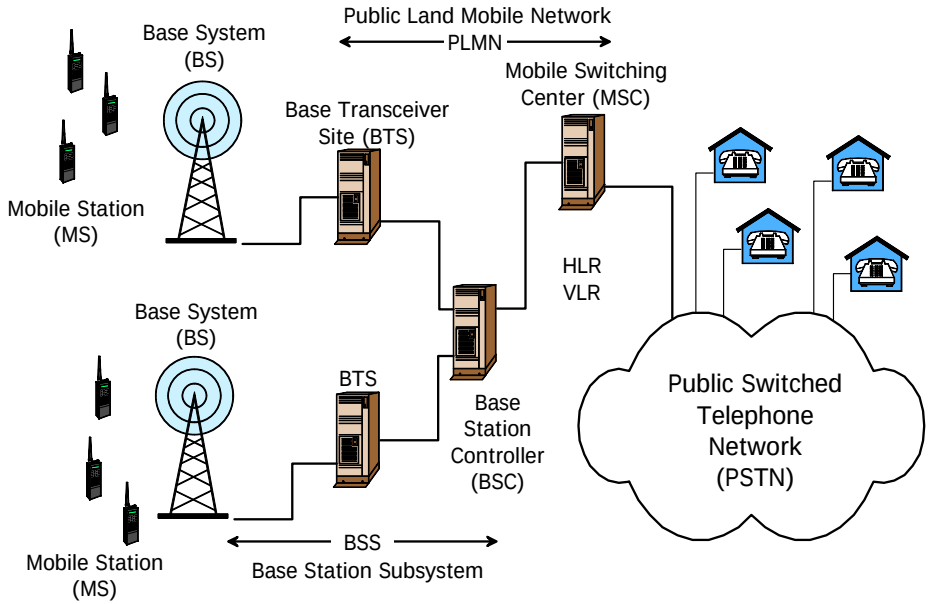
Mobile Network Switching Hierarchy

Mobile Service Provider

- Service Areas or Registration Areas
  - Clusters
    - Cells



The Cellular and Wired Telephone Network



Elements of GSM Mobile Network Hierarchy

Mobile Station (MS)

The telephone/terminal

Base Transceiver Site (BTS)

Fixed radio transmitter/receiver

Manages channels for with MSs in one cell

Base Station Controller (BSC)

Coordinates cluster of cells

Base Station Subsystem (BSS)

One BCS and all BTSs it controls

Mobile Switching Center (MSC)

Telephone Central Office for one Service Area

Handles local calls and Routes calls out of Service Area

Public Land Mobile Network (PLMN)

The wired portion of one Service Area (BTSs, BCSs, and MCS)

Mobility Service

Home Service Area

Service Area in which MS subscribes to cellular service

Home Subscriber

MS operating in its Home Service Area

Roamer

MS operating outside its Home Service Area

Handoff

Call control transfer when MS moves between cells in Service Area

Roaming

Call control transfer when MS moves between Service Areas

Problems of Mobility

MS must locate service provider access point

User must authenticate to service provider

Service provider must locate the MS

Provider must verify user's access rights

Home Location Register (HLR)

Located in MSC of Home Service Area

Maintains user's account information

Maintains location information for active MSs

Visitor Location Register (VLR)

Located in MSC for each Service Area

Cache of HLR data on active roamers

Registration Process

MS enters Service Area

Establishes low bit-rate control channel with service provider

MS requests service

BS allocates a frequency pair

MS reports to Mobile Switching Center (MSC)

Location, Status, and Identity

- Dedicated hardware ID code in phone
- Subscriber Identity Module (SIM) card identifies customer in GSM
- Mobile Station generates access code to network

Transmits code by public key encryption (PKE) algorithm

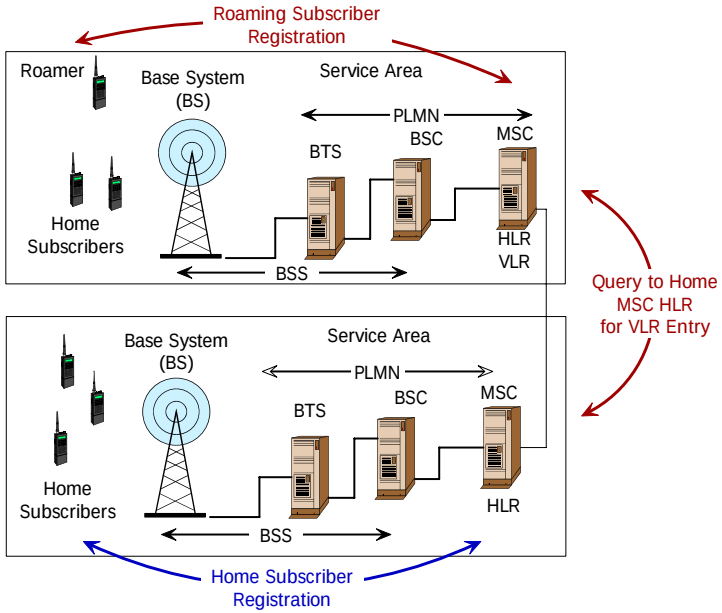
Mobile Switching Center (MSC)

Authenticates customer identity with HLR

For roaming subscriber, creates VLR entry

Updates Home Location Register (HLR) and billing database

Mobility Elements in the Cellular Network



1G — Advance Mobile Phone Systems (AMPS)

North American first generation analog system — IS-553

25 MHz transmission band per direction

Mobile Station (uplink): 825 - 849 MHz

Base Station (downlink): 870 - 895 MHz

Frequency Division Multiple Access (FDMA)

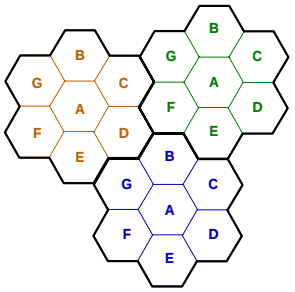
Divide band into 30 kHz RF voice channels

$$\frac{\text{25 MHz per cluster}}{\text{30 kHz per channel}} = 832 \text{ channels per cluster}$$

7 cell frequency reuse pattern (A, B, ..., G)

832 channels / 7 cells < 118 channels per cell

Typically 90 useful channels per cell



Second Generation Systems

2G Analog systems

Triple number of channels per cell

Motorola proprietary products

- Narrowband Advance Mobile Phone Systems (N-AMPS)
- Motorola Integrated Radio System (MIRS)

Time Division Multiple Access (TDMA)

Divide FDMA radio channel into time slots

MS transmits digitized voice in one time slot on one frequency

North American d-AMPS

European GSM

Code Division Multiplex Access (CDMA)

Create orthogonal binary digital transmission codes

MS transmits in one code on one frequency

GSM

Global System for Mobile Communications

European Union 2G digital cellular

Channelization

Divide band into 200 kHz RF channels

25 MHz per cluster / 200 kHz per channel = 125 channels per cluster

Digital transmission

Transmit 270.883 kbps in each 200 kHz radio channel

Voice and control modulation

- Gaussian minimum-shift keying (GMSK) — optimized FSK

Time Division Multiple Access (TDMA)

Divide each channel into 8 time slots

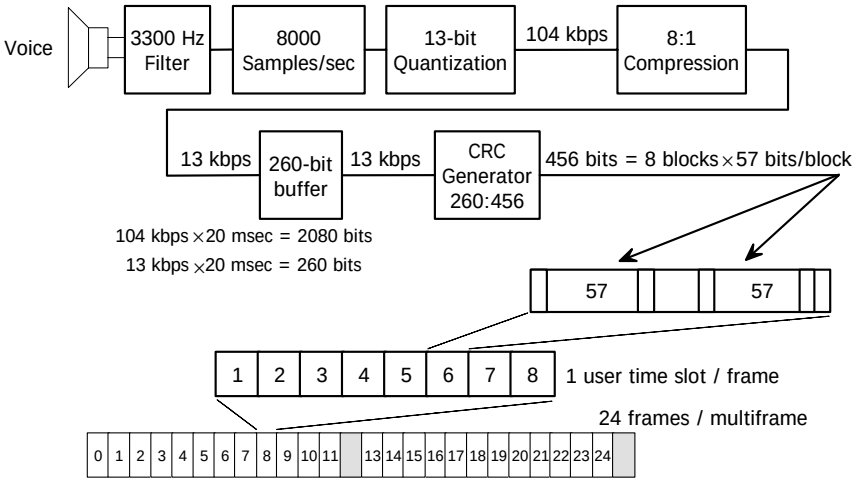
Allocate 1 time slot per user

- 270.883 kbps per channel / 8 users per channel = 33,086 bps per user

Standards

European Telecommunications Standards Institute (ETSI)

GSM Voice Transmission Summary



57 user bits per field × 2 fields per frame × 24 frames per multiframe = 2736 user bits per multiframe

2736 bits per multiframe / 120 ms per multiframe = 22.8 kbps

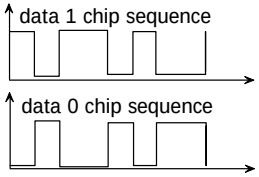
22.8 kbps / (456/260) = 13 kbps

Direct Sequence Spread Spectrum (DSSS)

Transmit data bit as chip sequence

- Chip
  - Shortest binary pulse on transmission channel
  - n-chip sequence is symbol for one data bit

Multiplies transmission rate



- User generates data at m bits per second
- Transmit n-chip sequence for every user bit
- Example
  - 1-sequence for data 1 = 10110100
  - 0-sequence for data 0 = 01001011
- Chip rate = m bps × n chips per bit = n × m chips per second (cps)

Receiver easily distinguishes 1-sequence from 0-sequence

- Bit error requires > n / 2 chip errors
- Works well in noisy environment

CDMA

Code Division Multiple Access

- Commercial system developed by Qualcomm
- Operates on AMPS frequencies

Channelization

- 25 MHz radio band per direction
- Divide band into 1.25 MHz RF channels
- 25 MHz per cluster / 1.25 MHz per channel = 20 channels per cluster

DSSS digital transmission

- Transmit 1.2288 Mcps in 1.25 MHz radio channel
- Voice and control modulation — QPSK

Code division

- Users transmit simultaneously using independent chip sequences
  - Orthogonal (Walsh) Codes / Pseudorandom noise (PN) codes
- Receiver separates channels by decoding chip sequences

Standards

- IS-95 — now called CDMAone

Orthogonal CDMA Codes

m-dimensional vector space with inner product

$$\mathbf{U} \cdot \mathbf{V} = \frac{1}{m} \sum_{i=1}^{m} U_i \times V_i$$

m orthonormal basis vectors

$S_i, i = 1, \ldots, m$

$\mathbf{T} = \sum_{i=1}^{m} t_i \times S_i$, with coefficient t_i for any vector $\mathbf{T}$

$$S_i \cdot S_j = m \times \delta_{ij} = \begin{cases} 0, i \neq j \\ m, i = j \end{cases}$$

$$t_i = S_i \cdot \mathbf{T} = S_i \cdot \frac{1}{m} \sum_{j=1}^{m} t_j \times S_j = \frac{1}{m} \sum_{j=1}^{m} t_j \times \left(S_i \cdot S_j \right) = \frac{1}{m} \sum_{j=1}^{m} t_j \times m\delta_{ij} = t_i$$

Code scheme

Basis vector S_i is code assigned to station i

Station i transmits $t_i \times S_i$ with coefficient

$$t_i = \begin{cases} -1, \text{data 0} \\ 0, \text{no transmission} \\ +1, \text{data 1} \end{cases}$$

Total transmission from all stations

$$\mathbf{T} = \sum_{i=1}^{m} t_i \times S_i$$

Example — 4-Chip CDMA

Code vectors for m = 4 stations

$$S_1 = \begin{bmatrix} -1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \quad S_2 = \begin{bmatrix} -1 \\ +1 \\ +1 \\ -1 \end{bmatrix} \quad S_3 = \begin{bmatrix} -1 \\ -1 \\ +1 \\ +1 \end{bmatrix} \quad S_4 = \begin{bmatrix} -1 \\ +1 \\ -1 \\ +1 \end{bmatrix}$$

4-bit transmission levels (chips)

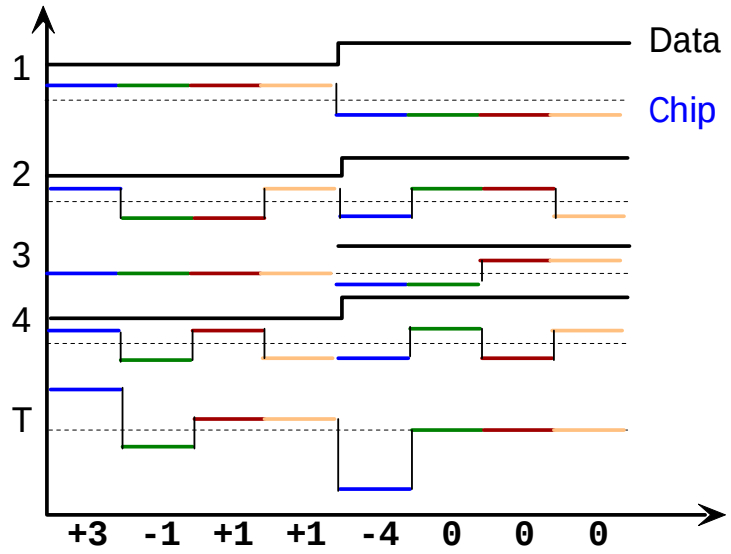
	Binary 1	Binary 0
Station 1	−1 −1 −1 −1	+1 +1 +1 +1
Station 2	−1 +1 +1 −1	+1 −1 −1 +1
Station 3	−1 −1 +1 +1	+1 +1 −1 −1
Station 4	−1 +1 −1 +1	+1 −1 +1 −1

Radio signal amplitudes added together

Example — 2-bit Transmission

Station 1	Data	0	1
	Signal	+1 +1 +1 +1	−1 −1 −1 −1
Station 2	Data	0	1
	Signal	+1 −1 −1 +1	−1 +1 +1 −1
Station 3	Data	no data	1
	Signal	0 0 0 0	−1 −1 +1 +1
Station 4	Data	0	1
	Signal	+1 −1 +1 −1	−1 +1 −1 +1
Total Transmission	Signal	+3 −1 +1 +1	−4 0 0 0

Example — 2-bit Transmission



Example — Decoding

Inner Product

$$\mathbf{U} \cdot \mathbf{V} = \frac{1}{4} \sum_{i=1}^{4} U_i V_i \qquad t_j = \mathrm{T} \cdot \mathrm{S}_j$$

First bit **T** = (+3, -1,+1,+1)	$t_1 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,-1,-1,-1) = \frac{1}{4}[-3+1-1-1] = -1 \Rightarrow 0$ $t_2 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,+1,+1,-1) = \frac{1}{4}[-3-1+1-1] = -1 \Rightarrow 0$ $t_3 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,-1,+1,+1) = \frac{1}{4}[-3+1+1+1] = 0 \Rightarrow$ no data $t_4 = \frac{1}{4}(3,-1,+1,+1)\cdot(-1,+1,-1,+1) = \frac{1}{4}[-3-1-1+1] = -1 \Rightarrow 0$
Second bit **T** = (-4,0,0,0)	$t_1 = \frac{1}{4}(-4,0,0,0)\cdot(-1,-1,-1,-1) = \frac{1}{4}[4] = +1 \Rightarrow 1$ $t_2 = \frac{1}{4}(-4,0,0,0)\cdot(-1,+1,+1,-1) = \frac{1}{4}[4] = +1 \Rightarrow 1$ $t_3 = \frac{1}{4}(-4,0,0,0)\cdot(-1,-1,+1,+1) = \frac{1}{4}[4] = +1 \Rightarrow 1$ $t_4 = \frac{1}{4}(-4,0,0,0)\cdot(-1,+1,-1,+1) = \frac{1}{4}[4] = +1 \Rightarrow 1$

Orthogonal Walsh Codes

Walsh 0

$W_0 = \boxed{1}$ $\quad W_0' = \boxed{-1}$

Walsh 1

$$W_1 = \begin{array}{|c|c|}\hline W_0 & W_0 \\ \hline W_0 & W_0' \\ \hline \end{array} = \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & -1 \\ \hline \end{array}$$

Walsh 2

$$W_2 = \begin{array}{|c|c|}\hline W_1 & W_1 \\ \hline W_1 & W_1' \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ \hline 1 & -1 & -1 & 1 \\ \hline \end{array} = \begin{array}{|c|}\hline S_1 \\ \hline S_4 \\ \hline S_3 \\ \hline S_2 \\ \hline \end{array}$$

Walsh 3

$$W_3 = \begin{array}{|c|c|}\hline W_2 & W_2 \\ \hline W_2 & W_2' \\ \hline \end{array}$$

Walsh N

$$W_N = \begin{array}{|c|c|}\hline W_{N-1} & W_{N-1} \\ \hline W_{N-1} & W_{N-1}' \\ \hline \end{array}$$

Walsh N is $2^N \times 2^N$ matrix

Pseudo-Noise (PN) Coding

Pseudorandom Bernoulli sequence of 1 or –1

Equivalent to sequence of m coin tosses

Nearly equal number of 1 and –1 in each code

By central limit theorem

$$P_{-1} = P(-1) = \frac{1}{2} + \delta \qquad P_{+1} = P(+1) = \frac{1}{2} - \delta \qquad |\delta| < \frac{1}{\sqrt{m}}$$

Codes are "nearly orthogonal"

For codes A and B with chip patterns $C_i^{(A)}$ and $C_i^{(B)}$

$$A = B \Rightarrow \frac{1}{m}\sum_{i=1}^{m} C_i^{(A)} \times C_i^{(B)} = \frac{1}{m}\sum_{i=1}^{m} [\pm 1]^2 = 1$$

$$A \neq B \Rightarrow \frac{1}{m}\sum_{i=1}^{m} C_i^{(A)} \times C_i^{(B)}$$

$$= \frac{1}{m}\sum_{i=1}^{m} \left[P_{+1} \times P_{+1} - P_{+1} \times P_{-1} - P_{-1} \times P_{+1} + P_{-1} \times P_{-1}\right] = 4\delta^2 < \frac{4}{m}$$

Channel Coding

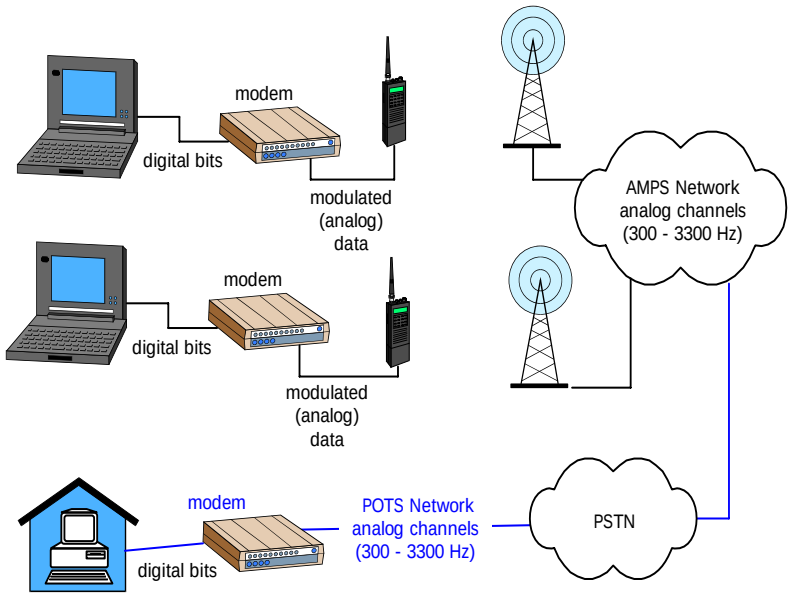
Forward channels

- 64 orthogonal Walsh codes to 64 users
  - Theoretically perfect separation between users
- All signals in same cell scrambled using PN sequence
  - Reduces interference between same Walsh code in neighboring cells
  - Short PN sequence uses cell ID as seed
  - Paging and traffic scrambled with long PN sequence before Walsh

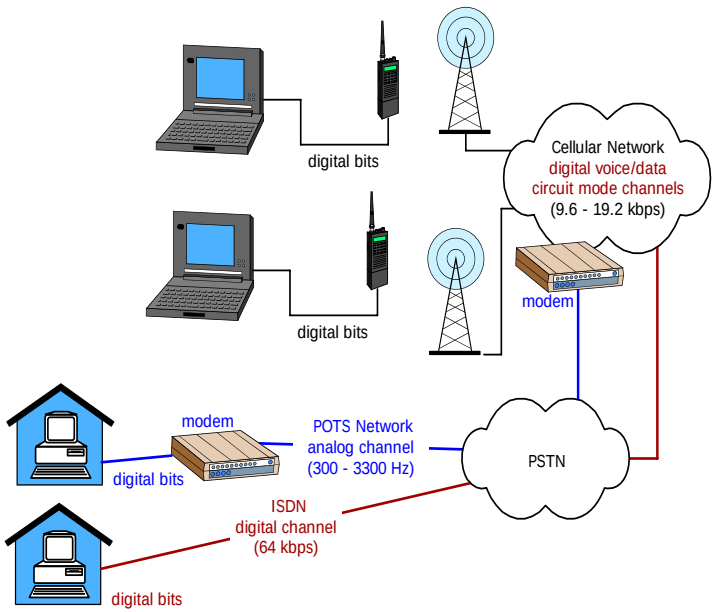
Reverse channels

- Orthogonal codes not applicable in uplink
  - Orthogonality requires time synchronization
  - MSs transmit asynchronously
- Long PN sequence
- Stream is scrambled using short PN sequence
- Carries cell ID

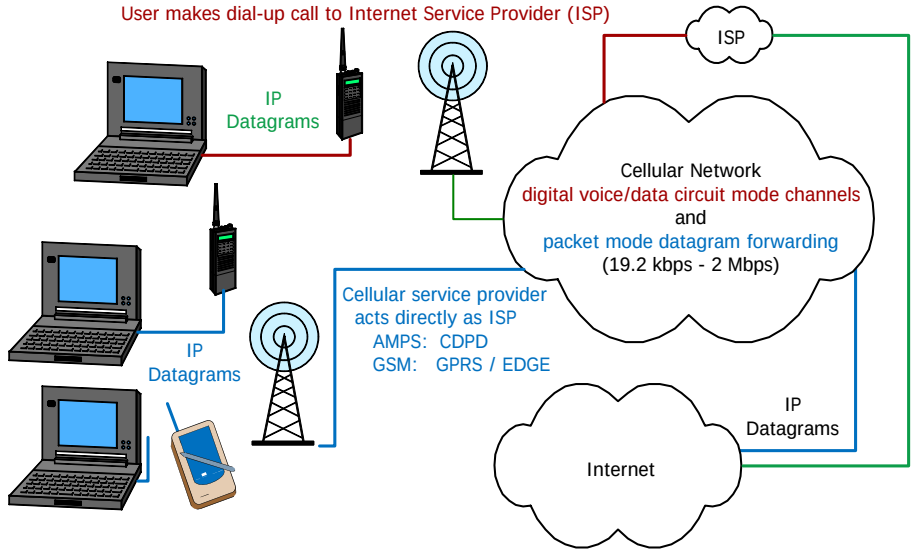
Data over AMPS



Cellular Circuit Mode Data Services



Cellular Packet Mode Data Services



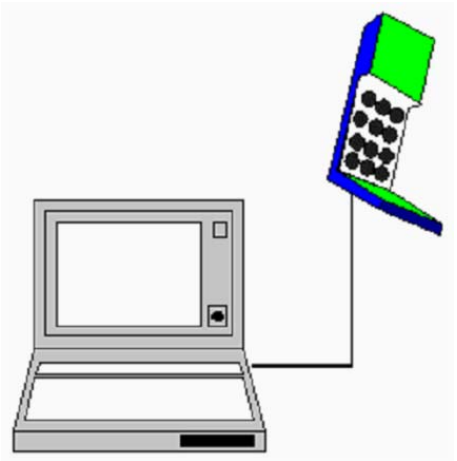
Cellular Data Terminals

Laptop with integrated cellular modem





Smartphone
with integrated cellular
modem



Laptop using cellular phone
as modem

General Packet Radio Service (GPRS)

Provides packet mode data access for GSM

- IP-based architecture
- Considered 2.5G enhancement

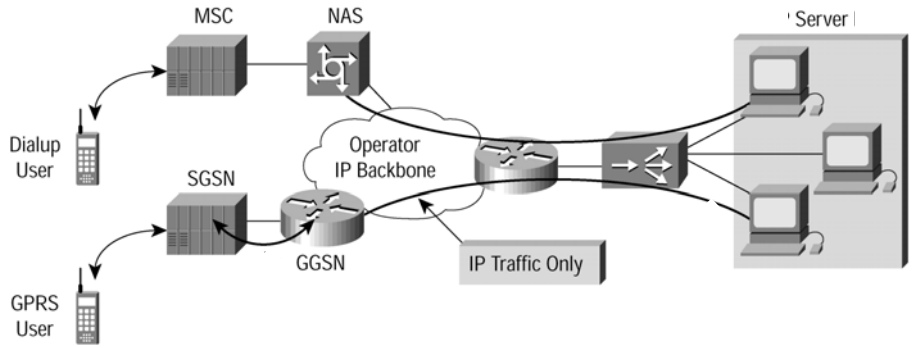
IP datagrams separated from circuit mode traffic at cluster

- Packet Control Unit (PCU)
  - Packet mode function in BSC to handle IP datagrams
- Circuit mode voice/data routed to MSC
  - Forwarded to other MSC or PSTN
- Packet mode data is routed to Serving GPRS Support Node (SGSN)
  - Forwarded to Internet or X.25 PSDN
  - PCU to SGSN runs IP over Frame Relay

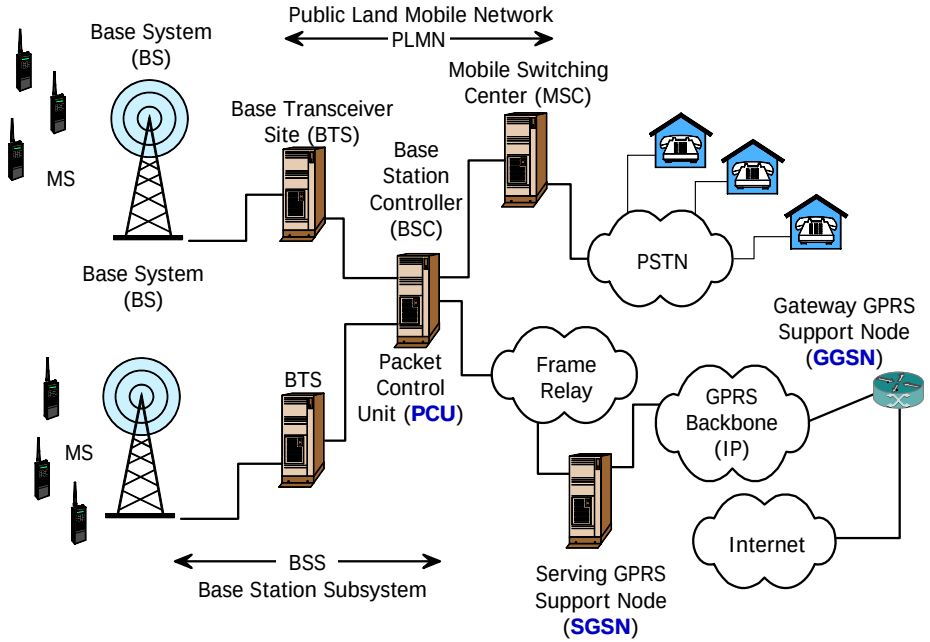
Mobility management

- Circuit mode traffic uses PSTN / PLMN routing
- Packet mode traffic uses IP routing

GSM Circuit Mode and GPRS Packet Mode Data



GPRS System Architecture



Short Message Service (SMS)

Transmission of short text messages

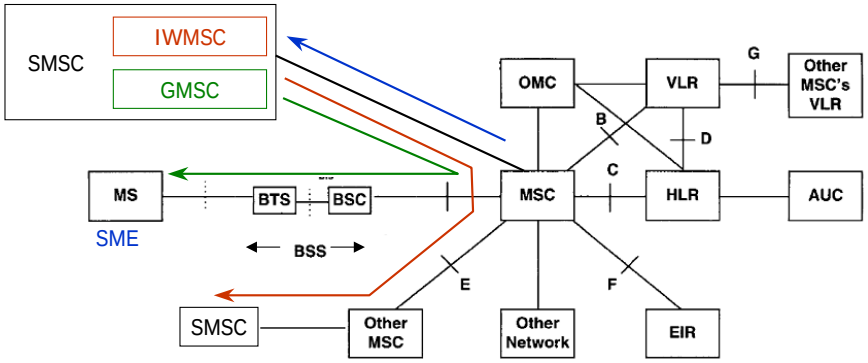
- Up to 160 bytes of alphanumeric data
  - 160 English ASCII characters
  - 16-bit unicode for non-English alphabets ⇒ 80 characters
- GSM permits message concatenation

Supported by GSM, d-AMPS, and CDMA

Out-of-band signaling

- SMS sent over signaling channel — not traffic channel
- SMS can be sent during a voice call
- Short messages do not create a heavy traffic load

SMS in GSM Architecture



SME: Short Messaging Entity

SMSC: Short Message Service Center

GMSC: Gateway Message Service Center

IWMSC: Interworking Message Service Center

SMS Nodes

Short Messaging Entity (SME)

- Any entity that can receive or send short messages
  - Fixed network element
  - Mobile Station
  - Another service center

Short Message Service Center (SMSC)

- Store and forwarding of SMS between SME and MS

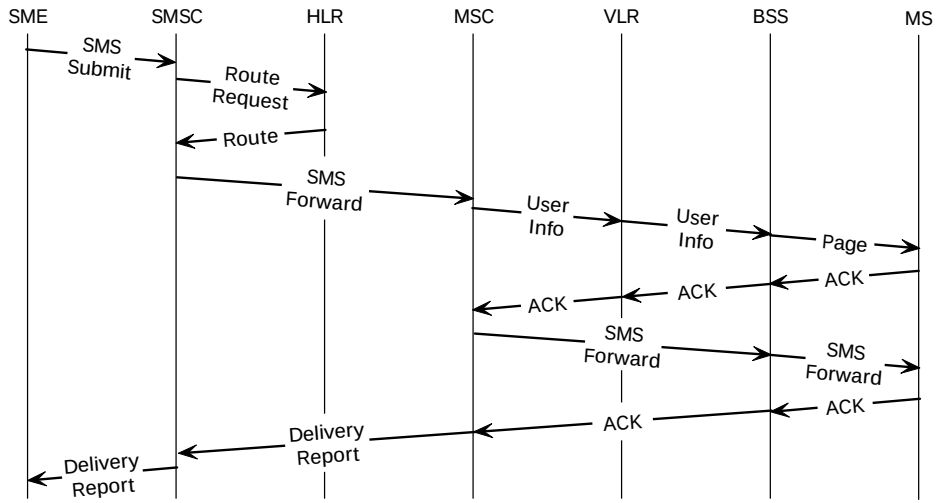
Gateway Message Service Center (GMSC)

- Receives SMS from SMSC
- Interrogates HLR for routing information
- Delivers SMS to MSC for destination SME

Interworking Message Service Center (IWMSC)

- Receives SMS from MSC
- Delivers SMS to appropriate SMSC for forwarding

SMS Delivery to MS



High Speed Circuit Switched Data (HSCSD)

Circuit Switched Data (CSD)

- 14.4 kbps circuit mode data connection in 2G GSM
- User data replaces digitized voice in 1 time slot

High Speed Circuit Switched Data (HSCSD)

- 2.5G enhancement
- Up to 8 slots (full user frame) allocated to one data channel
- Up to 115.2 kbps

Transparent data transmission

- User data stream can contain signaling to network
  - Allows dynamic reconfiguration of data connection (data rate, QoS)
- HSCSD data frames carry data sub-stream numbers
  - Maintains order of transmission over GSM

Non-transparent data transmission

- Only user data in data stream
  - No signaling or reconfiguration
- LLC functions performed by GSM protocols

Telecommunication Market Evolution — 1

Late 20th century

- Voice traffic >> data traffic
- Data traffic over analog / digital voice infrastructure
  - Access
    - V.35 / ADSL modem over telephone local loop
  - Backbone
    - Routers / switches on leased telco trunk lines
- Separate PSTN and cellular networks
  - Cellular backhaul
    - PLMN infrastructure on leased telco trunk lines
- Most profitable market sectors
  - PSTN
    - Long distance voice calls
  - Cellular
    - Air time

Telecommunication Market Evolution — 2

Early 21st century

Voice traffic < data traffic

Integrated networks — voice / data + fixed / mobile

IP over voice infrastructure → Voice over IP (VoIP)

Most profitable market sectors

PSTN

Leasing lines for data infrastructure

Cellular

Messaging, ring tones, multimedia services

Implications for Third Generation

System goals

Global mobility

Wide range of services

Voice telephony

Messaging + paging

Internet (WWW + email) access

Broadband data transport

Gateways among incompatible radio systems

More flexible PLMN routing infrastructure

Migration paths

TDMA d-AMPS → retirement

GSM → UMTS

More efficient radio spectrum utilization (CDMA replaces TDMA)

CDMA → cdma2000

More efficient radio spectrum utilization (higher capacity CDMA)

3G Standardization

Internal Mobile Telecommunications (IMT-2000)

International Telecommunications Union (ITU) standards for 3G

Defines multiple competing (incompatible) systems

Universal Mobile Telecommunications System (UMTS)

GSM/GPRS replacement using CDMA radio interface

Third Generation Partnership Project (3GPP)

Consortium of manufacturers (www.3gpp.com)

CDMA 2000

CDMA replacement using cdma2000 radio interface

Third Generation Partnership Project 2 (3GPP2)

Consortium of manufacturers (www.3gpp2.org)

WiMAX

Broadband wireless data access using cellular technology

WiMAX Forum

Consortium of manufacturers (www.wimaxforum.org)

UMTS

Physical layer

User access: GSM TDMA → W-CDMA or TD-CDMA

Similar to cdmaOne and cdma2000 but not compatible

Different frequency bands

Different pseudorandom noise (PN) coding scheme

Circuit mode data rates up to 1.92 Mbps

144 kbps and 384 kbps on high-utilization systems

New PLMN node definitions

BSS (base station subsystem) → RNS (radio network system)

BSC (base station controller) → RNC (radio network controller)

BTS (base transceiver system) → Node B

Protocols

New internal network operations

Frame Relay in backbone infrastructure → ATM

High Speed Downlink Packet Access (HSDPA)

Higher data rates for packet data

- Downlink speeds of 1.8, 3.6, 7.2, 14.0 Mbps

HS-DSCH simplified for fast packet data

- Power control and variable chip rate eliminated

Hybrid automatic repeat-request (HARQ)

- LLC layer added between PHY and MAC (not in RLC)
- Incremental redundancy
  - Corrupted packets not discarded
  - Retransmitted packets combined until error-free packet assembled
  - Faster than waiting for uncorrupted retransmitted packet

Fast packet scheduling

- 2 ms scheduling granularity (instead of 10 ms)
- Transmission scheduled to UEs reporting highest power levels

Adaptive Modulation and Coding (AMC)

- Modulation scheme and code rate depend on channel quality

cdma2000

Replacement for IS-95 CDMA (now called cdmaOne)

- Same radio frequencies
- Non-compatible pseudorandom noise (PN) coding scheme
- Higher data rates using improved modulation techniques
- Packet mode data — Mobile IP on voice network (like CDPD)

Evolutionary change from cmdaOne

- Multiple upgrade paths
- Operates in same radio frequencies
  - No new licensing costs for additional radio spectrum
- Backward compatible with cmdaOne
- Minimum risk to existing operators

Third Generation Partnership Project 2 (3GPP2)

- Consortium of manufacturers (www.3gpp2.org)

Standard

- IS-2000

IS-2000 Spreading Rates

1xRTT

- Same 1.25 MHz radio channel as IS-95
- Double IS-95 chip rate → 128 chips per bit
- Double users → 128 users per channel
- RF compatible with IS-95 in same cell
  - Uses codes orthogonal to IS-95 codes

1xEV-DO (data only)

- Physical layer different from 1xRTT
- Higher data rates (3.1 Mbps forward / 1.8 Mbps reverse)
- No increase in voice capacity

3x (3xRTT)

- Uses 3.75-MHz radio channels
- Direct Spread (DS) — one 3.75-MHz RF carrier
- Multicarrier (MC) — spreads data among 3 IS-95 1.25 MHz channels

Next Generation Networks (NGN)

ITU initiative for long-term network planning

- Standardizes current view of technology convergence

NGN definition

- Packet-based network
- Provide telecommunication services
- Use multiple broadband QoS-enabled transport technologies
- Service functions independent of transport technology
- Enables unfettered user choice of access to
  - Networks
  - Competing service providers and/or services
- Supports generalized **MOBILITY**
- Allow consistent and ubiquitous provision of services to users

From ITU-T Recommendation Y.2001 (12/2004)

NGN in the Marketplace

Mobility

- Basic feature of contemporary workflow
- Important source of profit for telecommunications industry

Convergence

- Workflow ⇒ universal access to services through any networks
- Multiple incompatible networks ⇒ market share + profits

Where do technologies converge?

- Most systems can interface service to infrastructure with TCP/IP
- Inherently digital services → internet
- Inherently analog services → A/D + compression → internet

NGN generally means all-IP network

- All services defined to work over IP
- All infrastructures defined to work below IP
- Problem — QoS, reliability, mobility not natural in IP

NGN Visions

Migration of all existing voice networks

- Most voice infrastructure is still hierarchical
  - DS-0 circuit switching
  - High speed trunk lines organized in tree topology among ESSs
  - Isochronous circuit mode operation natural for voice traffic
- NGN requires transforming voice networks to VoIP

Migration of local access from voice to DSL

- Single fast digital interface to doorstep
- Fiber to the door an expensive dream

Migration to flexible metropolitan area networks (MAN)

- "Carrier Ethernet" and cellular broadband (WiMAX) in urban areas

Improvement of QoS in IP networks

- Multiprotocol Label Switching (MPLS)
- Session Initiation Protocol (SIP)

4G Cellular

Initial planning for 4th generation cellular systems

- ITU working group planning IMT-2000 → IMT-Advanced
- Conceived as network supporting mobility — not telephones + data
- Convergence with NGN

4G objectives

- Higher network capacity than 3G
- Spectral efficiency (high bps / Hz and bps / Hz /site)
- 100 Mbps for moving client and 1 Gbps for stationary client
- 100 Mbps between any two points in world
- Smooth handoff across heterogeneous networks
- Global roaming across multiple networks
- QoS for multimedia support — audio, HDTV, etc
- Interoperability with existing wireless standards
- All IPv6 packet switched network — eliminate circuit mode entirely

Long Term Evolution (LTE)

3G standard

- Upgrade of 3G UMTS
  - Improved radio interface
  - Downlink < 300 Mbps
  - Uplink < 75 Mbit/s
- Marketed as 4G
  - Does not conform to 4G standards
  - Upgrade path while waiting for 4G

Flat IP-based network

- Evolved Packet Core (EPC) replaces GPRS
- Voice calls handled Voice over LTE (VoLTE)
  - Form of Voice over IP (VoIP)
  - Routed over EPC packet switched network
  - No separate circuit switched network for voice

IEEE 802.11

Specified by IEEE 802 Committee for LAN/MAN

Standards for Infrastructure Layers (OSI 1 and 2)

Extends Ethernet for wireless physical layer

Data rates

802.11 (1997) specified 1 or 2 Mbps (legacy)
802.11a (1999) specifies 6 to 54 Mbps
802.11b (1999) 5.5 Mbps and 11 Mbps (WiFi)
802.11g (2003) 54 Mbps (WiFi)
802.11n (2009) specifies up to 300 Mbps

Wireless Issues in LANs

Mobility

Addressable unit is a mobile station (STA)
Dynamic topologies
Medium boundaries are neither absolute nor visible
Lack full connectivity — STAs may be "hidden"

Reliability

Medium less reliable than wired PHY
Time-varying and asymmetric propagation

Power management

IEEE 802.11 wLAN Architectures

Ad Hoc Mode

Simple Peer-To-Peer Mode (STA-to-STA)
Limited to local communication
- No WAN access or hand-off

Authentication and Registration
- Permitted but not required

Infrastructure Mode

Basic topology
- Permits forwarding to wired LANs and WANs
- All communication via central Access Point (AP)
- Permits Authentication
- Requires Registration

Extended topology
- Permits hand-off among WLAN segments

Ad Hoc Mode (Peer-To-Peer Mode)

Independent Basic Service Set (IBSS)

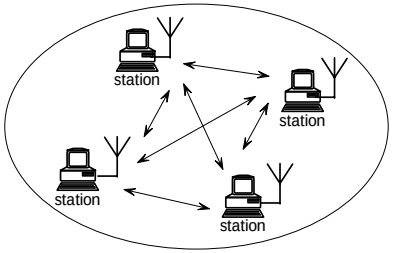
Any set of 802.11 STAs (wireless stations)
No connection to a wired network

Simple unmediated communication

STAs communicate directly with one another
Useful for quick set up
Authentication or Registration not required

Multiple IBSSs are independent

No bridging
No hand-off



Independent Basic Service Set

Infrastructure Mode

Basic Service Set (BSS)

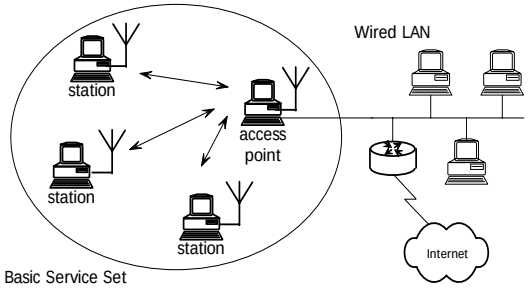
A set of wireless end stations (STA)

An Access Point (AP)

- Connected to the wired network infrastructure
- Acts as base station for the wireless network
- All traffic flows through AP by Contention or Polling (CFP)

Stations must Associate with AP

- Authentication
- Registration



Infrastructure Mode

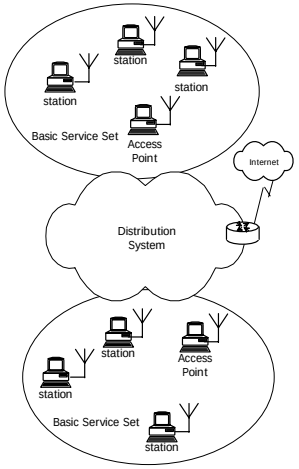
Extended Service Set (ESS)

Two or more BSSs

- Form single subnetwork (broadcast domain)
- Looks like one large BSS to LLC layer
- One Access Point (AP) in each BSS

BSSs connected via Distribution System (DS)

- DS is backbone network
- DS performs MAC-level transport of MAC SDUs
- DS implementation not specified in 802.11



Portal

Software gateway function in AP

Bridges BSS to any non-802.11 DS protocol

DS services permit handoff

Station moving from one BSS to another

Requires coordination between APs

802.11 Protocol Layers

PHY Dependent Sublayer

Transmission type

Modulation scheme

Data transmission rates

Physical Layer Convergence Sublayer

PHY medium dependent

Specifies header for PHY Dependent Sublayer

MAC layer

Medium access

Addressing

Procedures

Data Link Layer	LLC	802.2	LLC frame for SEQ/ACK/Control
	Bridging		Exchange of 802.2 PDUs
	MAC	802.11	CSMA/CA, MACA, CFP
Physical Layer	Convergence		PHY-Dependent Convergence Sublayer
	PHY		FHSS, DSSS, IR, Data rates

MAC Layer Issues

Channel Allocation Method

Contention (distributed control)

Round Robin (deterministic)

Polling (centralized control)

Collision Detection and Error Detection

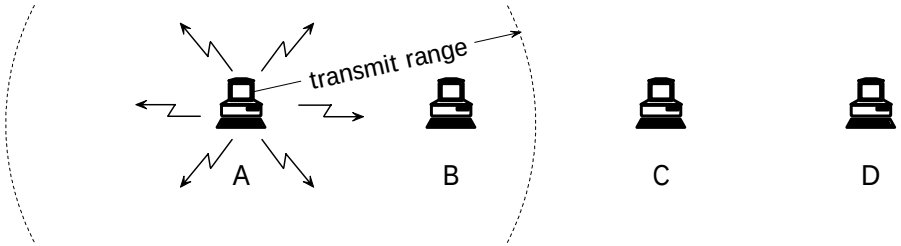
Fragmentation

Addressing

Control and Management Frames

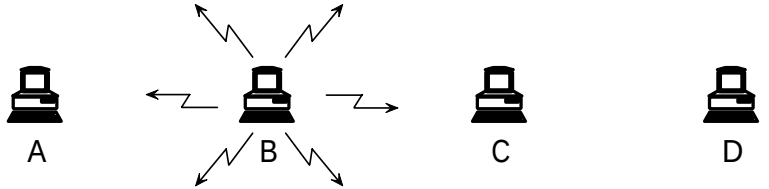
Hidden Node Problem

A transmits to B
C cannot receive from A — out of range
C is may interfere with A's transmission



Exposed Node Problem

B transmits to A
C receives B's transmission and is not free to start
C delays its transmission to D unnecessarily



CSMA with Collision Avoidance (CSMA/CA)

Carrier Sense Multiple Access (CSMA)

- Stations listen for transmissions
- Do not transmit if carrier is detected
- Collision detection not possible
  - Hidden node problem
  - Antenna cannot receive while transmitter active

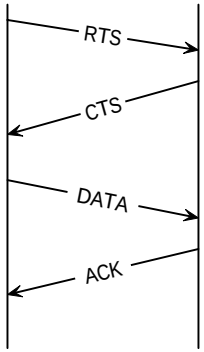
Collision Avoidance (CA)

- Non-persistent access
- Random backoff

Multiple Access with Collision Avoidance (MACA)

Channel set-up before data transmission

- RTS — Request To Send
- CTS — Clear To Send
- ACK — Acknowledgment of error-free transmission



Net Allocation Vector (NAV)

- Transmitted in RTS
- Predicted data transmission time

Improves behavior of Hidden Nodes and Exposed Nodes

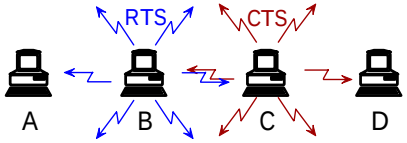
Multiple Access with Collision Avoidance (MACA)

B sends 30-byte RTS (request to send) packet to C

- Includes a NAV for the data to be sent
- All stations in B's range hear RTS

C responds with CTS (clear to send) packet to B

- Echoes NAV
- All stations in C's range hear CTS



B in range of A but not D

- A receives RTS but not CTS
- A can transmit without interfering with B's destination

C in range of B but not A

- D receives CTS but not RTS
- D waits data transmit time before transmitting

Station Services (SS) — 1

Privacy in wired LAN

- Design assumes physical closure
- Illegal access requires physical connection

Privacy in wLAN

- Any 802.11 receiver in range can receive all frames
- Wired Equivalent Privacy (WEP) algorithm
  - Shared key encryption
  - Not secure
  - No worse than wire

Station Services (SS) — 2

Authentication

- Station provides proof of identity to AP or STA
- Method not specified in 802.11
- Required before Association

Deauthentication

- Terminate authentication of another station
- Deauthentication invokes Disassociation

MAC Service Data Unit (MSDU) Delivery

- End-to-end delivery of LLC packets
- LLC packets (PDUs) are the SDUs of the MAC

Distribution System Services (DSS) — 1

Association

- Station associates with one AP
- Association provides STA/AP mapping to the DS
- DS forwards to STA via unique AP association

Reassociation

- Station moves from BSS to New BSS
- Station associates with New AP in New BSS

Disassociation

- New AP informs Old AP of Reassociation
- Old AP terminates old association
- APs may also disassociate all STAs (for maintenance)

Distribution System Services (DSS) — 2

Distribution

Delivery of packets to stations through DS

STA sends to source AP

Logically invokes DSS Distribution Service

DS passes frame to Destination AP

Destination AP passes frame to Destination STA

Integration

Portal services provided by DS

Source AP sends frame to Portal

Portal forwards to foreign (not 802.11) network

MAC Layer Address Fields

4 Address Fields

5 possible MAC entities:

BSS Identification Number (BSSID)

Source Address (SA)

Station which initiated the message

Destination Address (DA)

Final destination for the message

Transmitting Station Address (TA)

Station sending the message on this hop

Receiving Station Address (RA)

Destination for the message on this hop

Address Field Definitions

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	—
0	1	DA	BSSID	SA	—
1	0	BSSID	SA	DA	—
1	1	RA	TA	DA	SA

Address 1	Immediate destination address
Address 2	Immediate source address
Address 3	Final destination or source when DS performs distribution
Address 4	Source address for DS to DS messages (802.11 is also DS)

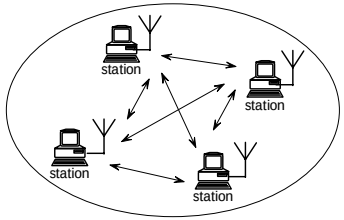
Addressing in an IBSS

To DS	From DS	Address 1	Address 2	Address 3
0	0	DA	SA	BSSID

Independent Basic Service Set (IBSS)

No Access Point (AP) and no DS

Fields To DS and From DS are 0



Independent Basic Service Set

Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	BSSID Identifies Ad Hoc network Prevents message from reaching outside IBSS

Data Addressing in a BSS

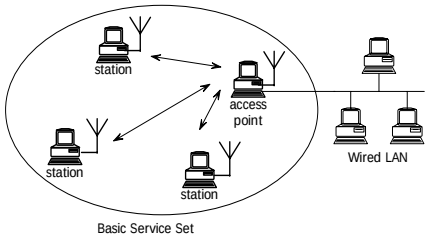
To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Basic Service Set (BSS)

All transmissions are sent To/From Access Point

To/From DS actually means To/From AP

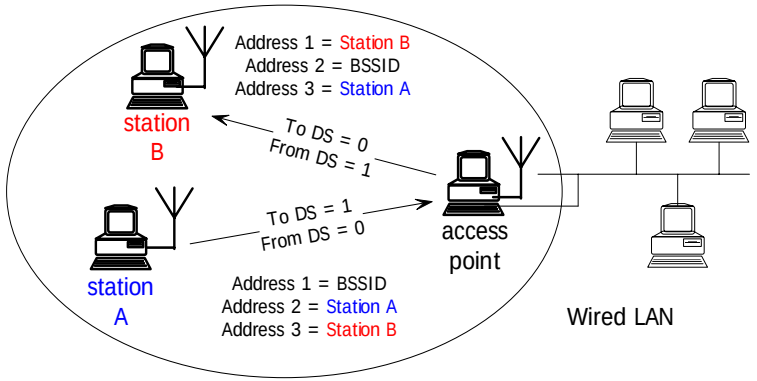
Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	Final Destination or Source



BSS Addressing Example

To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Station A sends message to Station B via AP (BSSID)



Control and Management Addressing in a BSS

To DS	From DS	Address 1	Address 2	Address 3
0	0	DA	SA	BSSID

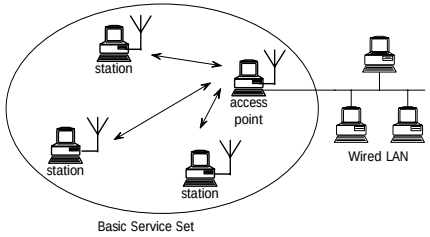
Control and Management messages in a BSS:

Only involve stations in the BSS and the AP

Are sent with To DS = From DS = 0

Either the Source or the Destination will be the AP (BSSID)

Address 3 in included as an error check



Addressing in an ESS

To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

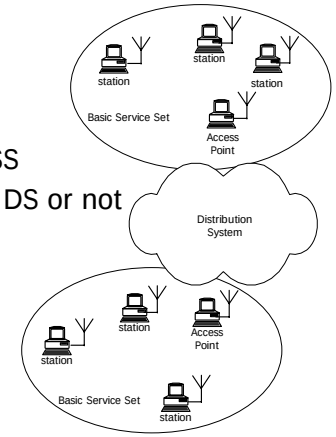
Extended Service Set (ESS)

All transmissions are sent via an AP

To the stations, entire ESS looks like one BSS

Stations do not know if message passes via DS or not

Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	Final Destination or Source



ESS Addressing Example

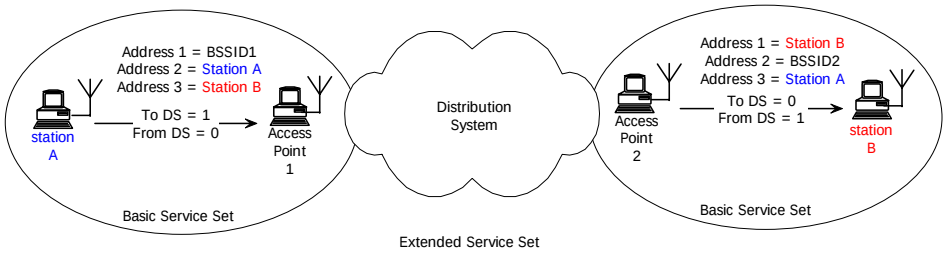
To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Station A sends message to Station B via

AP1 (BSSID1) → DS → AP2 (BSSID2)

DS must forward Data, Sequence, SA, and DA

By some legal means



WEP Encryption/Decryption Procedure

Plaintext

MAC Layer PDU (MPDU)

CRC-32 Frame Check Sequence (FCS) on MPDU

Key Sequence

Generated from Secret Key and Initialization Vector (IV)

Key length is MPDU length + 4

Transmission

Encrypted Plaintext

Unencrypted Initialization Vector (IV)

Receiver

Generates Key Sequence from Secret Key and IV

Deciphers Plaintext and checks FCS for errors

WEP Encryption Algorithm

Secret Key distributed by some background process

Initialization Vector (IV) 24-bit suffix generated by transmitter

IV may be changed as frequently as every MPDU

IV transmitted unencrypted with message to receiver

Receiver needs IV to decrypt

IV provides no information about secret key

Seed

64-bit concatenation: Secret Key ## IV

Seed input to Pseudo-Random Number Generator (PRNG)

Key Sequence k

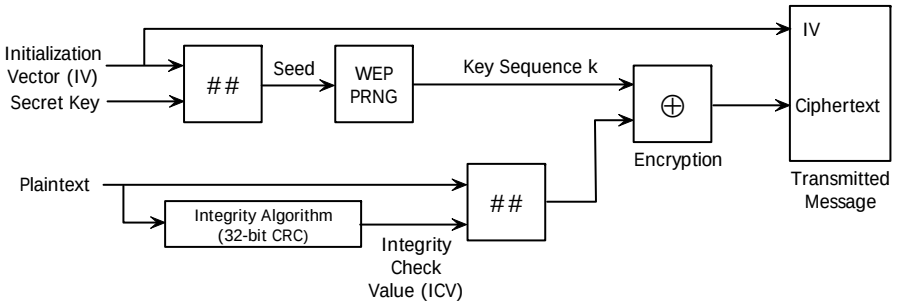
Pseudo-Random Number generated by PRNG using seed

Integrity Check Value (ICV)

32-bit CRC on MPDU

Plaintext (MPDU ## ICV) encrypted with Key Sequence

WEP Encryption Algorithm



WEP Decryption Algorithm

Key Sequence generated from IV and Secret Key

Decryption

- Key Sequence applied to Ciphertext
- Plaintext includes MPDU and ICV

Integrity check performed on Plaintext

- On error in received MPDU
  - Error indication is sent to MAC management
  - Data not passed to LLC

Problems with WEP Algorithm

XOR encryption is not very strong

Secret Key is too easy to deduce

- Part of MPDU may be easy to guess
  - Example: IP header fields
  - Can find k from P and C

Encryption strength

- Depends on lifetime of Initialization Vector (IV)
- Best privacy when IV is changed for every MPDU

More Problems with WEP

AP beacons

- Announce service availability
- Can be found by unauthorized listeners

WEP not always implemented

Weak encryption

- 40-bit secret key
- Simple XOR of key with plaintext

Weak authentication

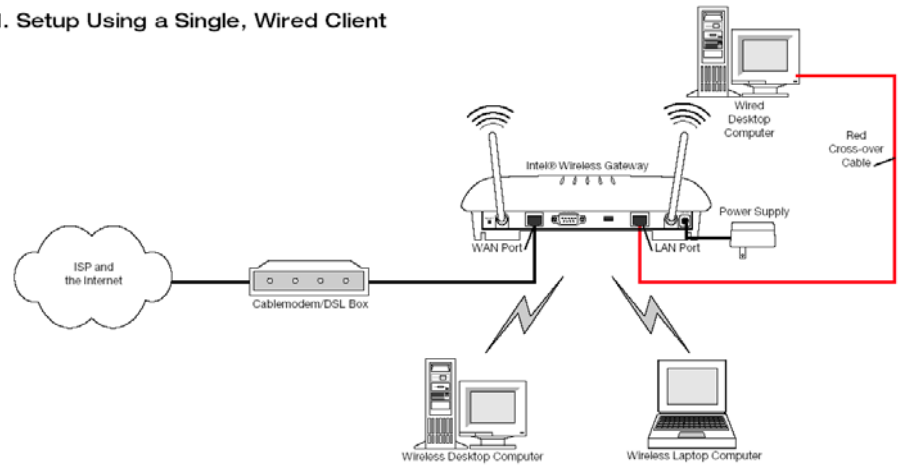
- STA requests service
- AP sends random number
- STA returns number encrypted with key (password)

Authentication password is used as encryption key

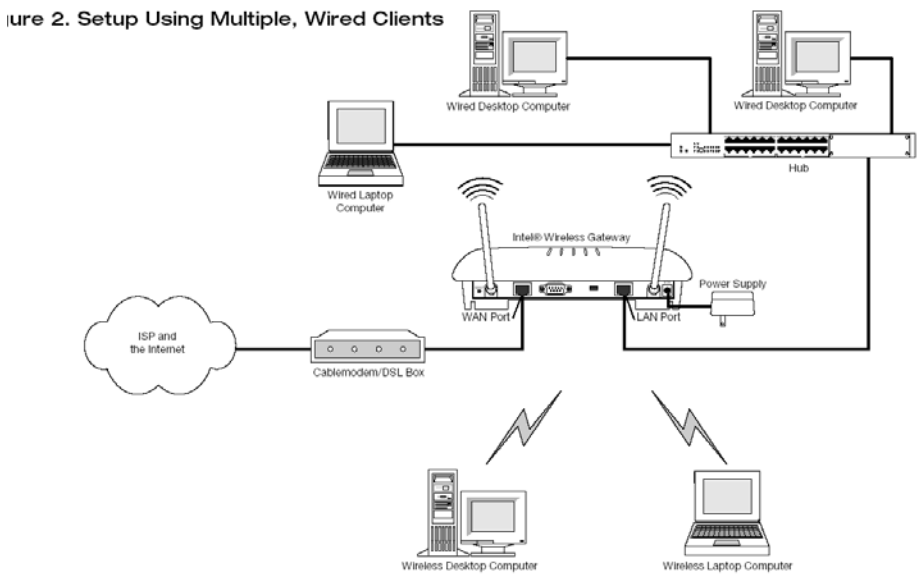
- Eavesdropper can learn key from plaintext and encrypted number

Infrastructure Network Configurations — 1

1. Setup Using a Single, Wired Client



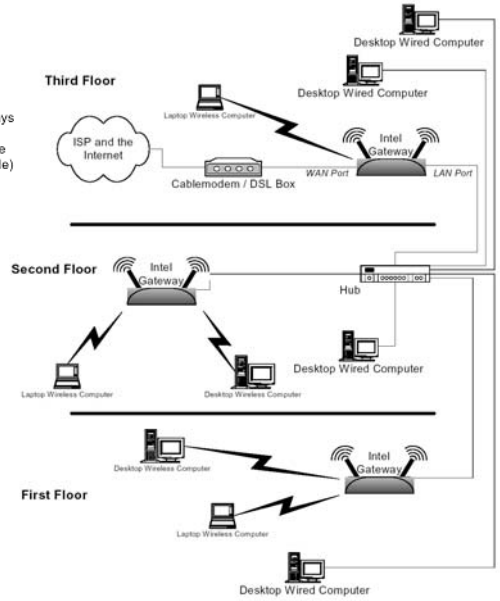
Infrastructure Network Configurations — 2



Infrastructure Network Configurations — 3

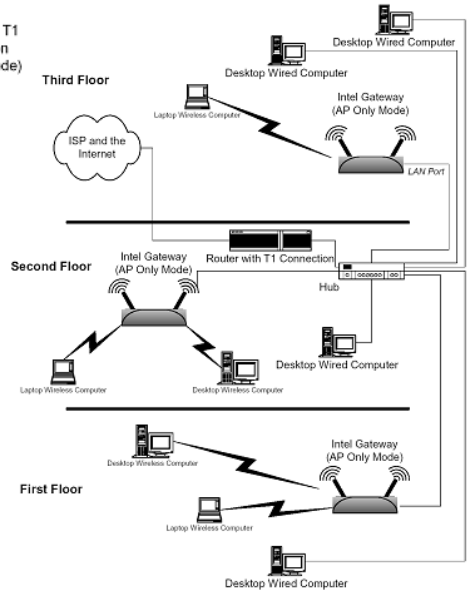
Installation example with multiple gateways

(one Intel Gateway in gateway/AP mode and other Intel Gateways in AP only mode)



Infrastructure Network Configurations — 4

Installation example with multiple Intel Gateways and T1 or other Internet connection (all Gateway's in AP only mode)



The Bluetooth Vision

Universal wireless connectivity

- Replace existing cables with radio
- Connect systems that have been separate

Ubiquitous computing environment

- Intelligent devices performing distributed services
- Redesign hardware as object-oriented

Unconscious connectivity paradigm

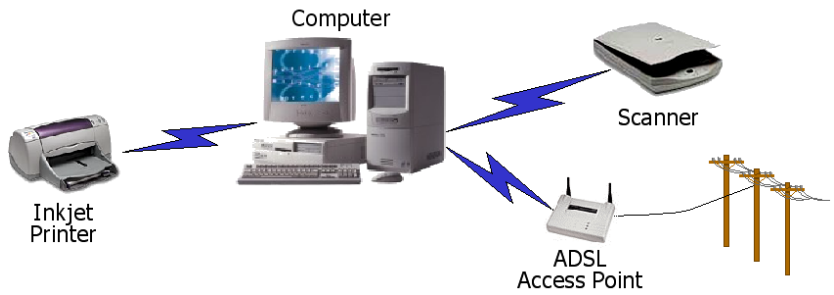
- Devices interconnect automatically
- Minimal user intervention

Wireless Personal Area Network (wPAN)

- Small networks formed dynamically
- Wireless internetworking among wPANs

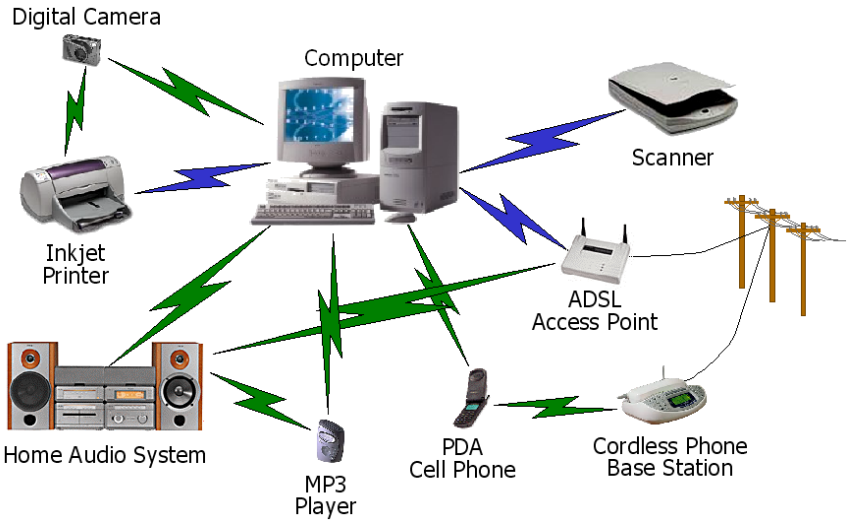
Universal Wireless Connectivity

Replace existing cables with radio



Universal Wireless Connectivity

Connect systems that have been separate



Ubiquitous Computing Environment

Intelligence is local and communication is universal

Bluetooth devices

- Search for other compatible devices
- Share information about services they provide
- Exchange commonly defined data objects

Service provision is distributed over wPAN

Integrated automation of

- Central servers
- Information repositories
- Sensors
- Actuators

Unconscious Connectivity Paradigm

Connectivity is a problem for the user

- Inconvenient to establish connections manually
- Available devices change frequently
- Users may not remember how to connect

Devices connect automatically and dynamically

- Devices discover one another
- Devices determine when and why to connect
- Users do not need to remember how to connect

Example of The Vision

User

Enters hotel lobby

PDA in user's pocket

Connects to hotel reservations system for check in

Receives key code for door

Displays room number

Alerts laptop in suitcase to log onto hotel email server

User's Laptop

Downloads messages while user waits for elevator

User's PDA

Unlocks door of hotel room

User's laptop

Uploads music to audio system

User's PDA

Orders room service from menu user prepared on airplane

Example of a Real Product

Three-in-One Telephone

Automatic network selection by environment:

Intercom at home or in office

PSTN phone when a PSTN access point is available

Cellular mobile phone otherwise

How is Bluetooth Different?

In cellular and wLAN systems:

Base Stations and Mobile Stations are clearly distinct

Base Stations handle services

Channel access

Channel allocation

Traffic control

Interference problems

Mobile Stations are relatively simple clients

In Ad Hoc Bluetooth networks:

Communication is peer to peer

No central controller

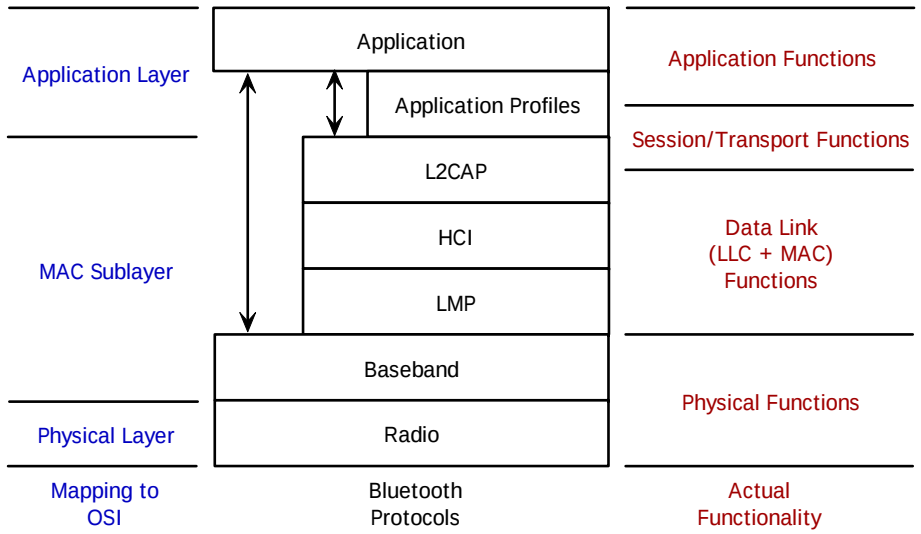
Devices in area self-organize in a shared channel

May be many Bluetooth devices in region

Only a few need to communicate

Mutual coordination is complex

Protocol Layers



Protocol Overview

Application Layer	User application programs
Application Profiles	User application support protocols: FTP, TCP, WAP, PPP, telephony, USB, Serial Port, etc
Logical Link Control and Adaptation Protocol (L2CAP)	Channel management (socket-type interface), Segmentation and Reassembly, QoS (speed, reliability, delay)
Host Controller Interface (HCI)	Supports standard I/O hardware standards (when Bluetooth device is external to PC)
Link Manager Protocol (LMP)	Manages Piconet membership and link activity
Baseband Layer	Manages point-to-point links, handles security, and interfaces user data to the radio links
Radio Layer	Physical data transmission (FHSS in ISM band, at 10 or 100 meter broadcast range)

Frequency Hopping

Bluetooth transmits using Frequency Hopping (FHSS)

Group of RF frequencies = 2401 + k MHz,
for k = 0, 1, ... , 78

Specific Hop Sequence depends on

Bluetooth Service

Bluetooth Clock

Bluetooth Device

Data transmission

Pseudorandom hop sequence

Connection control

Deterministic hop sequences

Frequency Hop Sequence

Train = sequence of integers $\{k_0, k_1, k_2, ..., k_N\}$

$0 \le k_i \le 78$, for i = 0, 1, ..., N

N = 16 or 32

Time Slots

Bluetooth Clock is a 28-bit counter

Upper 27 bits define Bluetooth Time Slot

2 Clock Cycles per Time Slot

Counter creates 2^{27} = 134,271,728 numbered Time Slots

Counts from 0 to $2^{27} - 1$ (then returns to 0)

Each Time Slot is 625 µs in length (1600 slots/second)

Time slot number returns to 0 every 23.3 hours

Frequency Hopping

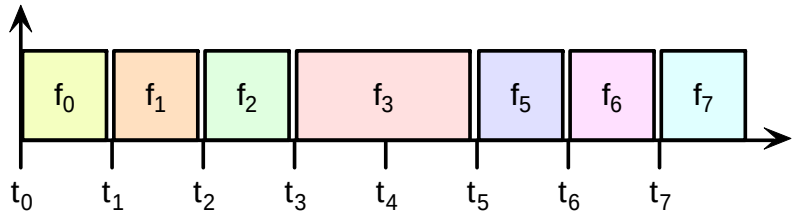
Packet transmission begins on a Time Slot boundary

Packets may be up to 5 Time Slots in length

Frequency hop on each Time Slot

Unless packet is longer than 1 Slot

No frequency hop during a multi-slot packet



Piconet Topologies

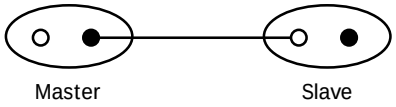
Piconets (from pico = 10^{-12})

Physical Channel

Specific Frequency Hop Sequence

Point-to-Point Piconet

Two devices on a common Physical Channel
FHS is unique to a given Piconet
Master device acts as client
Slave device acts as server



Synchronous Connection Oriented (SCO) Links

Point-to-Point link between Master and Slave

Circuit-mode connection based on reserved slots

Symmetric transmission rate
Supports isochronous information like voice

Master can support

1 to 3 SCO links to one or more Slaves

Slave can support

1 to 3 SCO links with one Master
1 or 2 SCO links from different Masters

Asynchronous Connectionless Link (ACL)

Point-to-Multipoint link

Connects Master and all active Slaves in Piconet

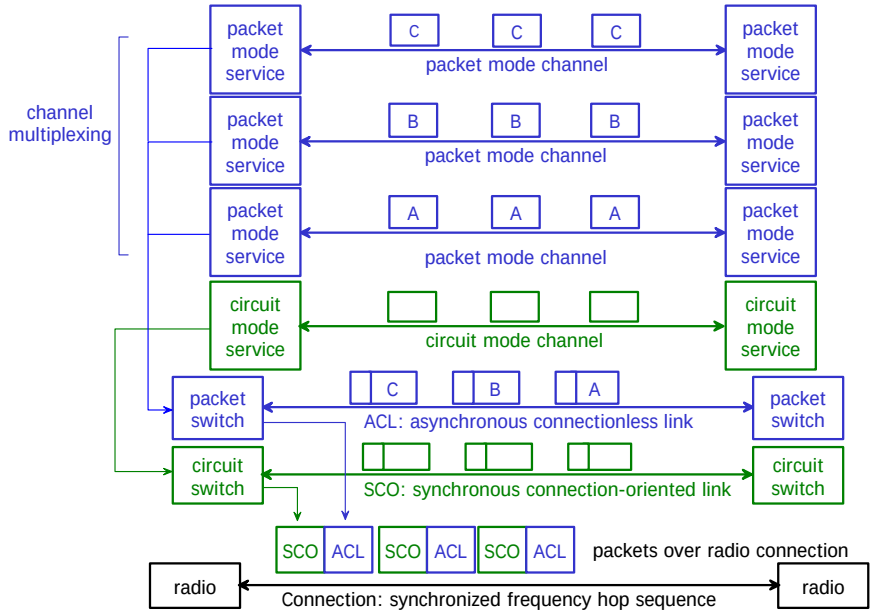
Packet-mode connection

Based on statistical multiplexing
Uses available slots not reserved for SCO links

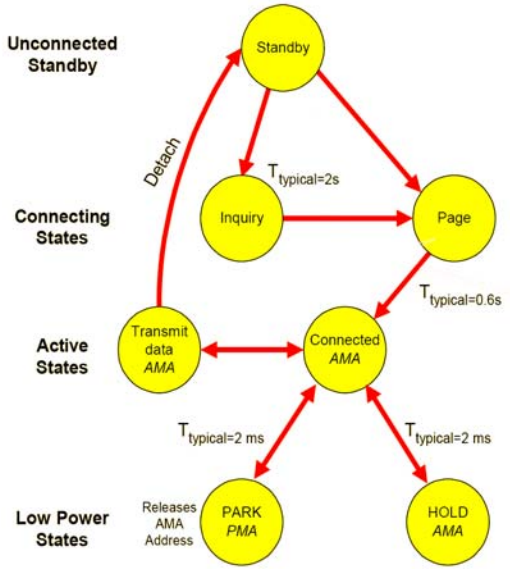
Asynchronous and Isochronous services supported

Only one ACL link between a Master and a Slave

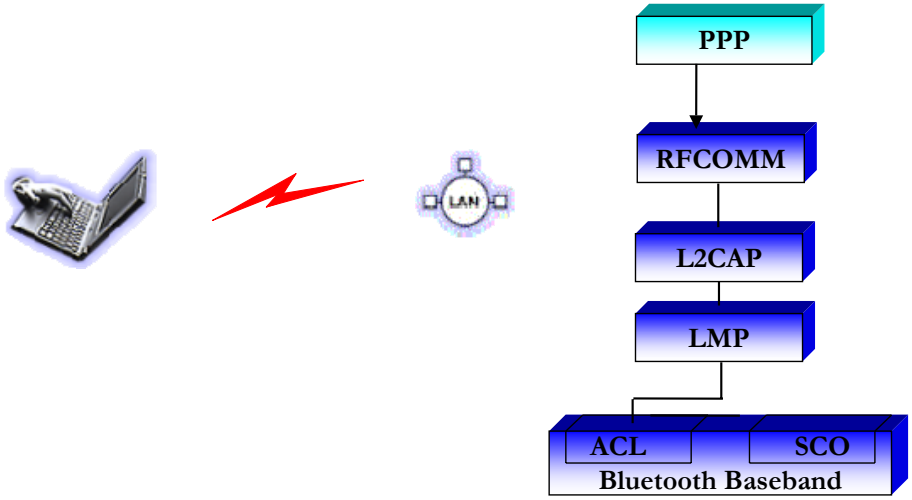
Bluetooth Connection Layers



State Relationships



LAN Access Point Profile



Bluetooth Earpiece

Philips Semiconductor VWS26003

3 Integrated Circuits

Baseband processor (VWS26002)
Ceramic Multi-chip RF module (PBA 31301)
External Flash memory

NiMh or Lithium ion battery

Talk time ~4 hours

Size weight 75g, 15cc



Philips Semiconductor VWS26003

VWS26002 Baseband processor

ARM7 TDMI 32-bit embedded RISC processor
- 72 kbytes internal SRAM
- 4 kbytes internal ROM
- 4 kbytes internal SRAM instruction cache
- Timers and watchdog.
- 8 general purpose PIO pins.
- Voice Codec

PBA 31301 Radio Frequency Module

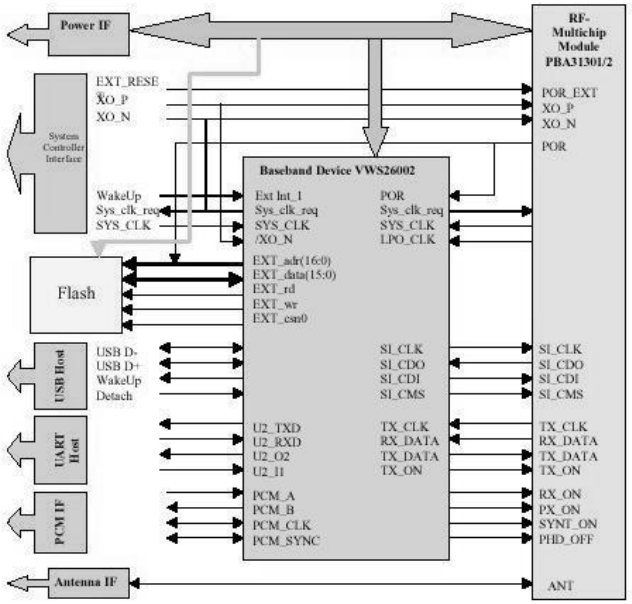
Software

Point to Point Protocol stack

Systems

or NiMh or Li Ion battery

Philips Semiconductor VWS26003



Single Chip Bluetooth Device Controller

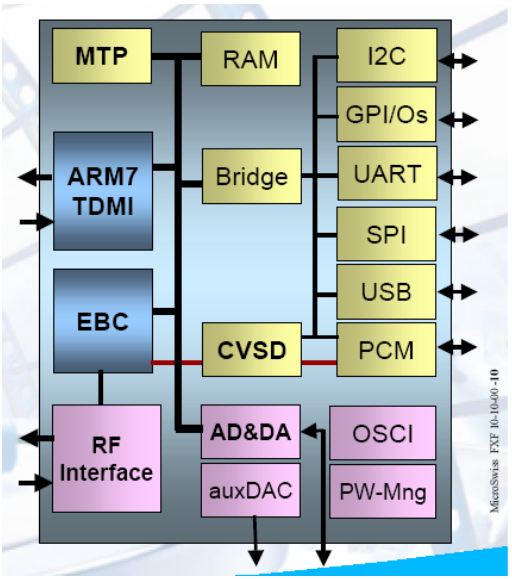
Philips PCD87750E

MTP = Multiple Time Programmable ROM

EBC = Ericsson Bluetooth Core

CVSD = Continuously Variable Slope Delta modulation

SPI = Security Parameter Index



Typical Earpiece Organization

