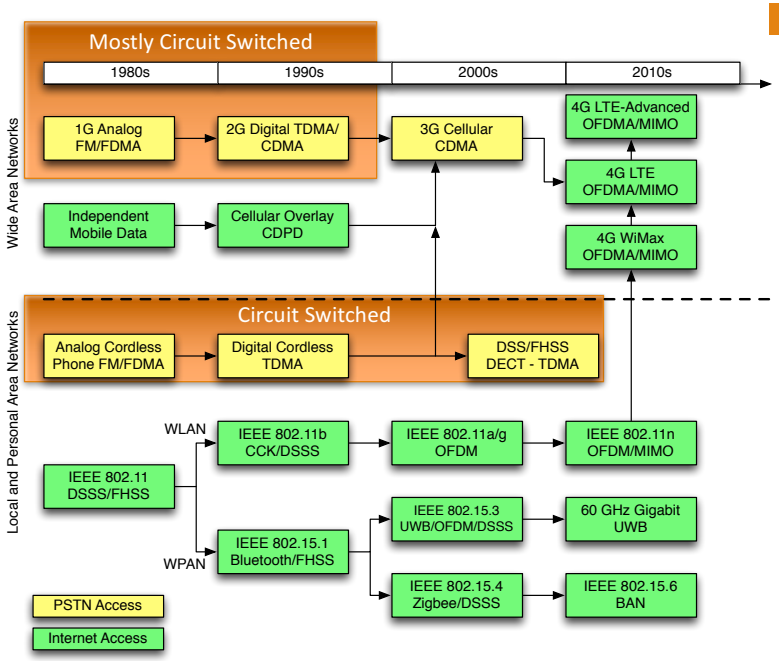
Lecture 3

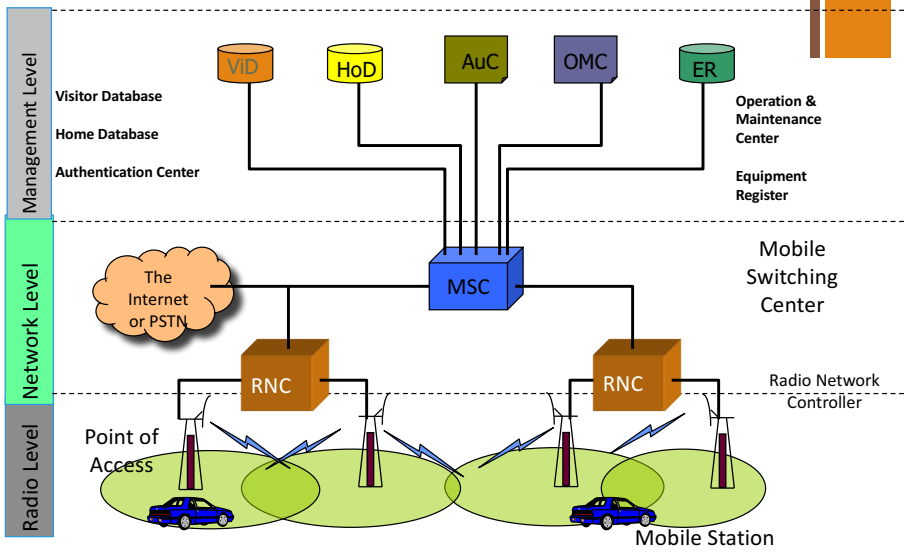
Overview of Wireless Systems (2)

Preview

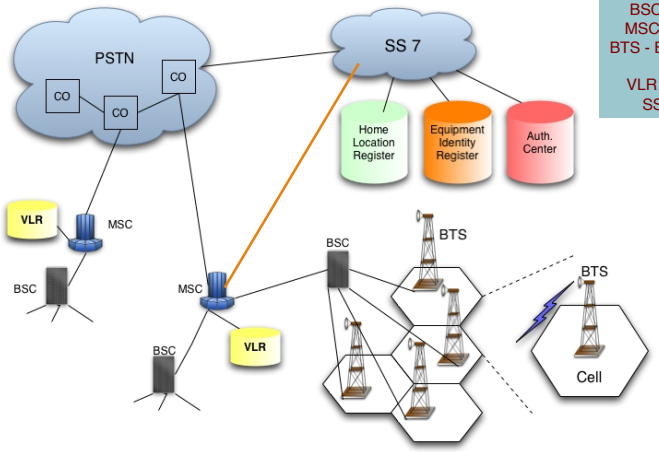
- Last week
  - Looked at air interface of 1G and 2G cellular networks
  - Both are primarily circuit switched
- In GSM, the control signaling uses packets and a "protocol stack"
  - We briefly consider this today
- 3G, 4G, WLANs and WPANs are more packet oriented
  - Brief overview today



Generic Architecture – 2G WWANs



2G Cellular Network Architecture



BTS- Base Transceiver Subsystem
BSC - Base Station Controller
MSC - Mobile Switching Center
BTS - Base Transceiver Subsystem
CO - Central Office
VLR - Visitor Location Register
SS 7 - Signaling System 7

Terms and terminology

- Mobile Station (MS)
  - Mobile Terminal – MT, Mobile End System – M-ES, Mobile Node – MN, Mobile Device, Handheld Device, Wireless Device, etc.
- Point of Access
  - Base Station (BS), Base Transceiver Subsystem (BTS), Mobile Data Base Station (MDBS), Access Point (AP), Node B, E-Node B
- Radio Controller
  - Base Station Controller – BSC, Radio Network Controller – RNC
- Mobile Control Center
  - Mobile Switching Center – MSC, Mobile Data Intermediate System – MD-IS, Gateway GPRS Support Node – GGSN
- Visiting Database
  - Visiting Location Register – VLR, Mobile Serving Function – MSF, Serving GPRS Support Node – SGSN, Foreign Agent – FA
- Home Database
  - Home Location Register – HLR, Mobile Home Function – MHF, GPRS Register – GR, Home Agent - HA

Not all elements from the generic architecture exist in all technologies & the exact functionality of the elements may be different

Mobile Station or Device

- We will call this Mobile Station or MS
  - Irrespective of what it is
- Form factor and capabilities
  - Has to be light weight, durable, have long battery life and yet be capable of performing complex tasks
  - Energy efficient design of software and protocols
- Usability
  - User characteristics (size, dexterity, knowledge, etc.)
  - Environment characteristics (temperature, degree of mobility, etc.)
  - Device Characteristics
    - Start up time
    - Data integrity and security
    - CPU speed and memory size
    - Power supply
    - User interface (keypad, finger, stylus, voice)

Mobile Devices

Pager
- Receive only
- Tiny displays
- Simple text messages
- Two way pagers

Smartphones
- Graphical displays and touchscreens
- Almost full WWW
- Apps!

Laptops
- Fully functional
- Standard applications






RF-ID tags, Sensors, embedded controllers

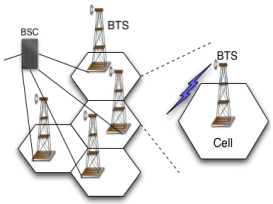
Regular cellphones
- Voice, data
- Simple text displays
- Simplified WWW

Tablets and netbooks
- Tiny or virtual keyboard
- CPU weak
- Long battery life

Performance and Cost?

Functionality of Elements (I)

- Point of access
  - The physical radio transceiver
  - Creates the air interface
    - Transmits signals to MSs
    - Receives signals from MSs
    - Involved in multiplexing on the link
      - Medium access



- Radio Network Controller
  - Again link level
  - Manages the air interface
    - Which RF carrier should I tune to?
    - What transmit power level should I use?
    - Is the frequency carrier I want to use capable of providing acceptable quality?
    - When should I make a handoff?

Base Stations (BS)

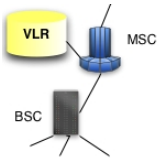
- Provides radio channels between mobile units and network
- Pico-cells : (indoor – 0-.5 Km) support 8-20 channels
- Micro-cells: (outdoor – 0-1 Km), Macro-cells: (1-30 Km)

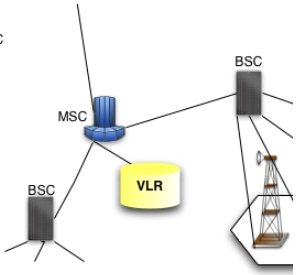
Base Stations and Radio Network Controllers

- Base Transceiver Subsystem (BTS)
  - Houses radio units
- Base Station Controller (BSC)
  - Manages a cluster of BS, channel assignment, handoff, power control, some switching, etc

Mobile Switching Center

- Mobile Switching Center (MSC)
  - Provides switching functions , coordinates location tracking, call delivery, handoff, interfaces to HLR,VLR, AUC, etc.
  - Size of central office switch



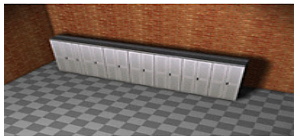


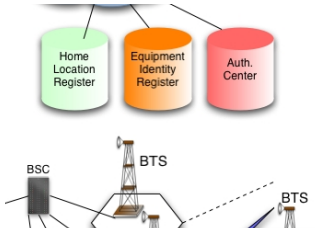
Functionality (II)

- Mobile Switching Center
  - Manages mobility of devices
    - Routes voice calls or packets to and from MSs
  - Keeps track of the location of the MSs
    - Location means "in which cell or group of cells" the MS may be located i.e., which points of access may be probable candidates for pinging the MS
    - How does it do this? Using the home database and visiting database
  - Ensures security
    - Uses the authentication center and equipment registers to authenticate the MS and to prevent fraudulent/stolen devices from using the network
  - Accounting and Billing
    - Operations and maintenance center

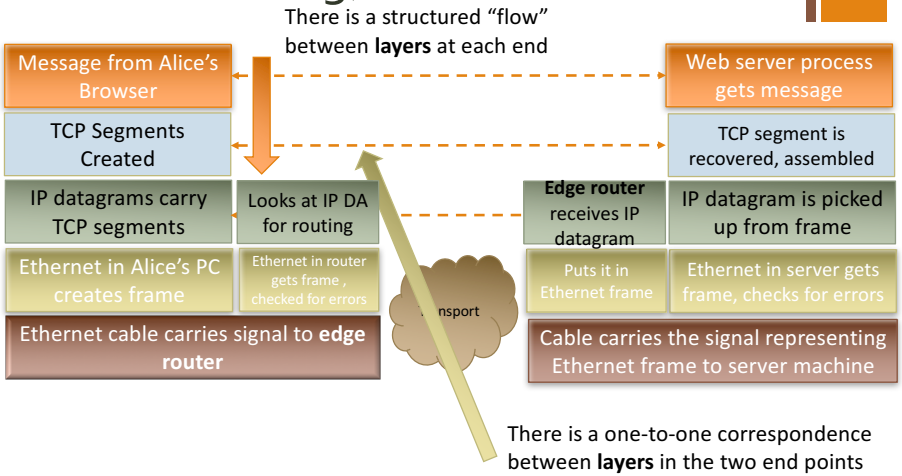
Home and Visitor Databases

- Home Location Register (HLR)
  - Specialized database server contains billing info, service profile and general location of a mobile user
- Visitor Location Register (VLR)
  - Similar to HLR contains location of users and their service profile of all users in a metro type area





Protocol Stack – TCP/IP (Simplified Web Browsing)



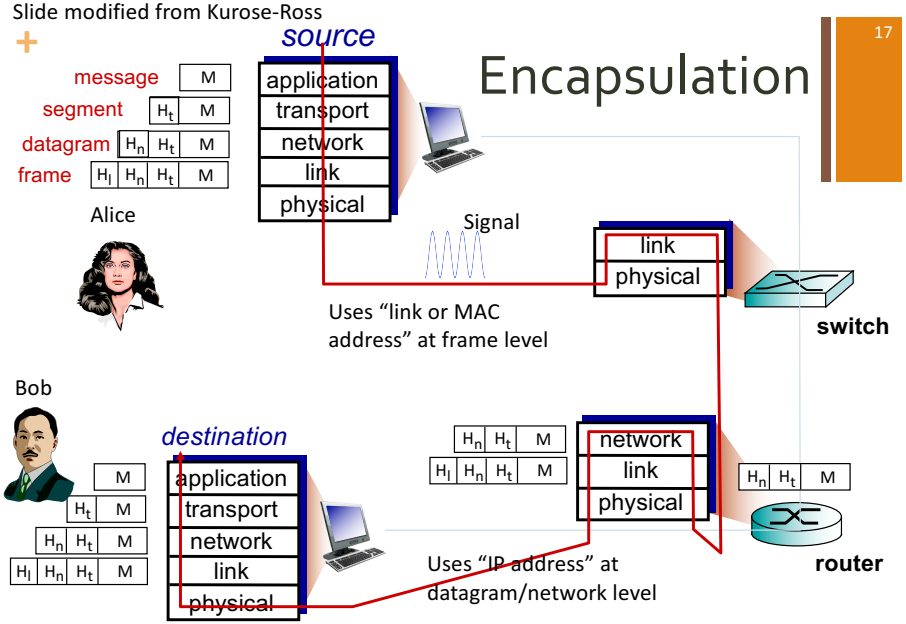
Slide modified from Agrawal

Layer names and tasks

Layer number	Layer name	Networking task	Header information
5	**Application**	Specify user needs, creates "message"	User commands
4	**Transport**	Segmentation and reassembly of data "segments", sometimes reliable transfer & speed matching	Sequence numbers
3	**Network**	Identifying and locating destination, best effort delivery of "datagrams"	Address
2	**Data-link**	Reliable delivery of "frames" over a link, Error control	Error check
1	**Physical**	Signaling, moving individual bits based on medium	Usually none, but in WiFi there is a header

Slide modified from Kurose-Ross

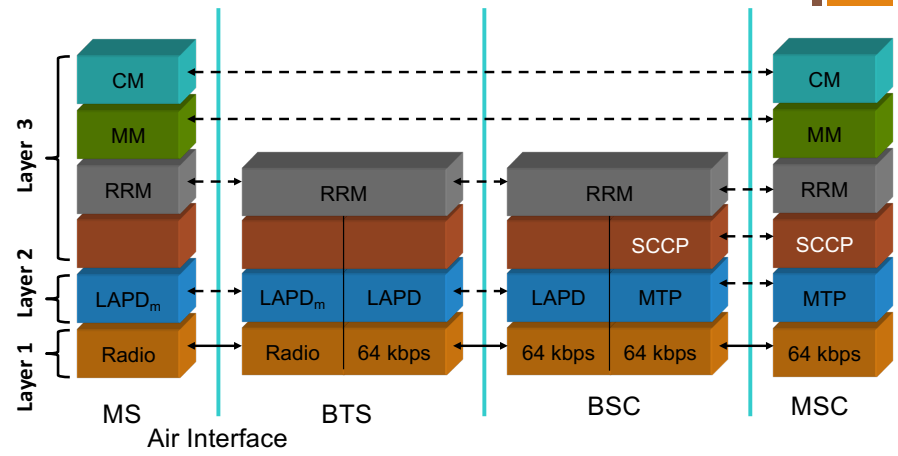
Encapsulation



Control Signaling and User Data (Voice) in 2G Systems

- Control Signaling
  - Messages for setting up the voice call
  - Messages for mobility management
  - Messages for radio resources management
  - Other signaling (SMS is carried on signaling channels)
- User data is primarily "voice" in 2G
  - Sometimes called "voice traffic"
  - Digitized and carried in circuits set up by the control signals

Control Signaling Protocol Stack – 2G GSM



CM: Connection Management; MM: Mobility Management; SCCP: Signal Connection Control Part
RRM: Radio Resource Management; MTP: Message Transfer Part; LAPD: Link Access Protocol-D

Example: Mobile Initiated Call in 2G GSM

Message Name	Category
1. Channel Request	RRM
2. Immediate Assignment	RRM
3. Call Establishment Request	CM
4. Authentication Request	MM
5. Authentication Response	MM
6. Ciphering Command	RRM
7. Ciphering Ready	RRM
8. Send Destination Address	CM
9. Routing Response	CM
10. Assign **Traffic Channel**	RRM
11. **Traffic Channel** Established	RRM
12. Available/Busy Signal	CM
13. Call Accepted	CM
14. Connection Established	CM
15. Information Exchange	voice bits

Security Related

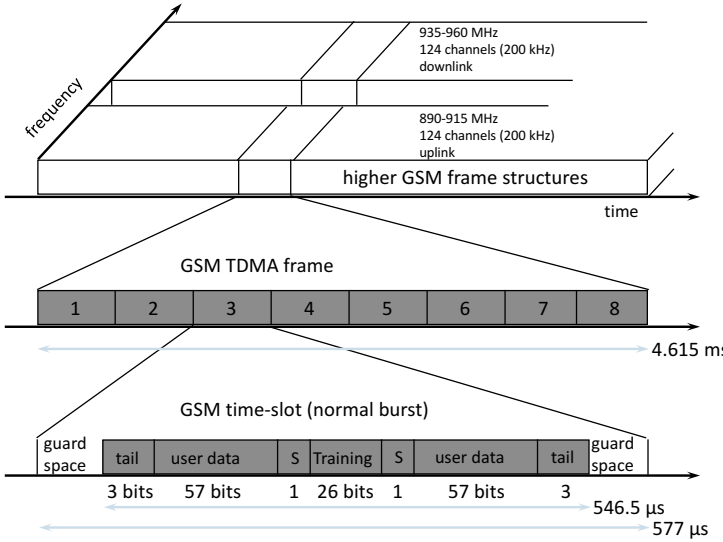
Traffic Channel = Circuit

This is all control signaling

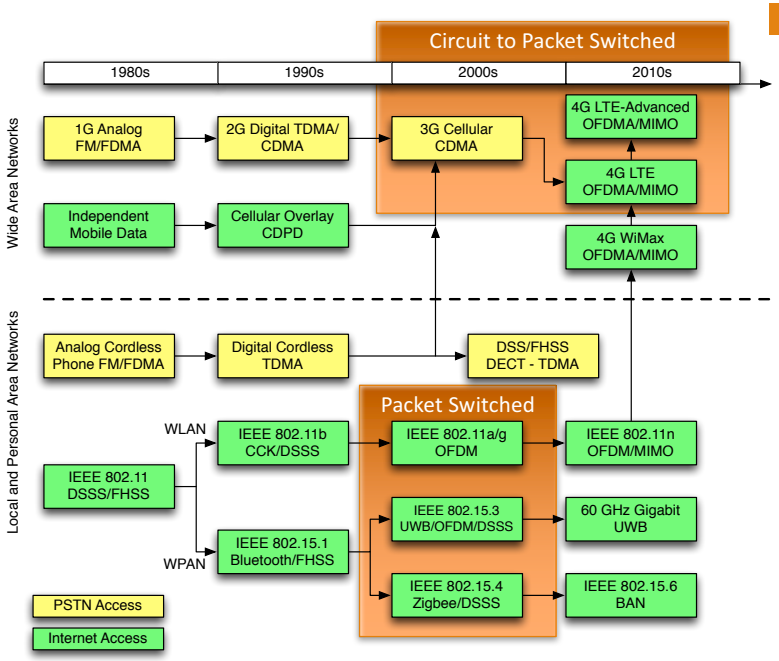
Physical Vs Logical "Channels"

- A 200 kHz frequency carrier is a "physical channel"
- A time slot used for "voice traffic" is a logical channel
- There are several "control channels" that are logical channels in GSM
  - They are used for call set up, managing mobility, handling radio resources, etc.

2G GSM - TDMA/FDMA/FDD



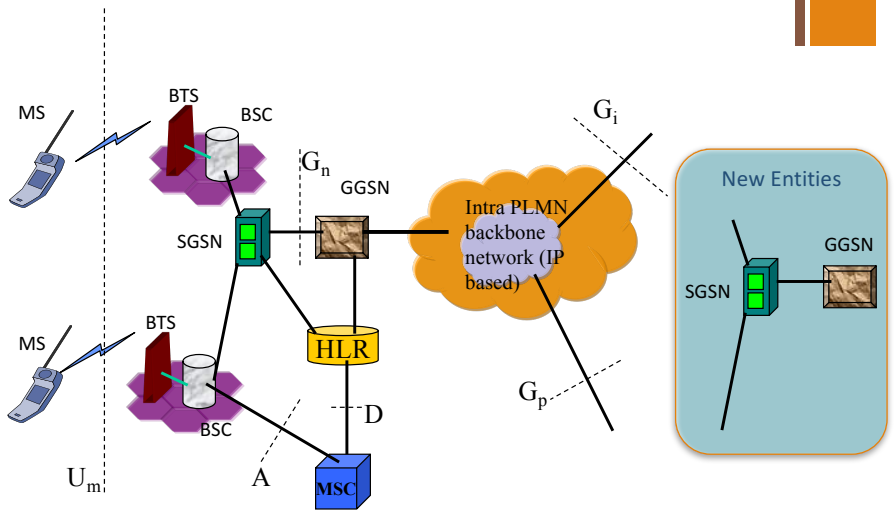
Show physical and logical channels



2.5 G Systems and Data

- 2G Systems provide slow speed data service
  - 9.6 Kbps – 14.4 Kbps
- 2.5G
  - Attempt to improve data services from 2G and build customer base for wireless data service
  - GPRS, HSCSD, cdma2000-1x -> Mislabeled as 3G
  - Basically overlay network of data service on 2G networks
    - Max data rate 57 Kbps – 150 Kbps, typical data rates 33-56 Kbps – similar to dialup modem service
- Mobile Data
  - Cellular Digital Packet Data (CDPD) -> Overlay on AMPS
  - **General Packet Radio Service (GPRS) -> Overlay on GSM**

GPRS System Architecture



Serving GPRS Support Node (SGSN)

- It controls access to MSs that may be attached to a group of BSCs
  - This is called a routing area (RA) or service area of the SGSN
- It is responsible for delivery of packets to the MS in its service area and from the MS to the Internet
- It also performs the logical link management, authentication, and charging functions

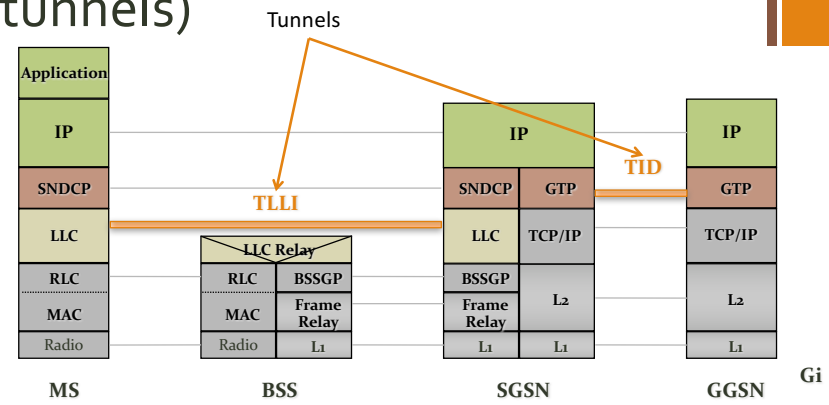
Gateway GPRS Support Node (GGSN)

- It acts as a logical interface to the Internet
- Maintains routing information related to a MS, so that it can route packets to the SGSN servicing the MS
- It analyses the packet data network (IP) address of the MS and converts it to the corresponding International Mobile Subscriber Identity (IMSI) number

GPRS Signaling Plane

- GPRS employs out of band signaling in support of actual data transmission
- Signaling between SGSN, HLR, VLR, EIR is similar to GSM and extends only the GPRS related functionality
  - Based on Signaling System 7
- Between the MS and SGSN, a GPRS mobility management and session management (GMM/SM) protocol is used for signaling purposes

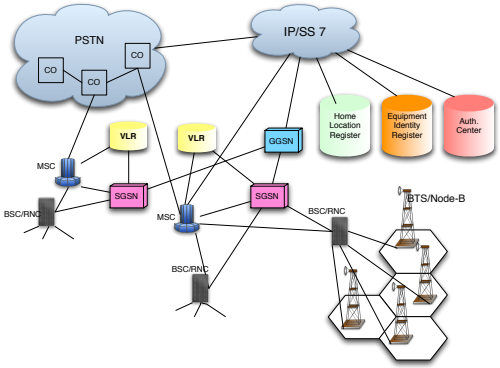
GPRS Transport Plane (two tunnels)



SNDCP: Subnetwork Dependent Convergence Protocol
BSSGP: BSS Gateway Protocol
GTP: GPRS Tunneling Protocol

3G (UMTS)

- Network architecture adds to the 2G architecture
- Similar core network as 2G systems
- WCDMA based air interface
  - True QPSK modulation
- Wider carrier bandwidths
  - 5 MHz
  - 3.84 Mcps
- SGSN and GGSN – Data!



What is UMTS?

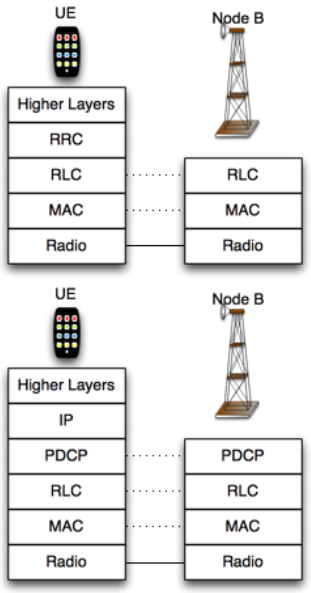
- UMTS stands for Universal Mobile Telecommunications System
  - 3G cellular standard in Europe & Japan
- Outcome of several research activities in Europe
  - Generated trial systems and basic understanding of WCDMA
  - Assisted the standardization efforts
- Most of the standardization work was focused in 3GPP
  - 3GPP refers to the physical layer as UTRA – UMTS Terrestrial Radio Access
  - There are two modes – FDD and TDD
- UMTS can support both GSM-MAP and IS-41 core networks
  - An all-IP third alternative is available now

Summary of WCDMA

- WCDMA is somewhat different compared to IS-95
- It is a “wideband” direct sequence spread spectrum system
  - Supports up to 2 Mbps using
    - Variable spreading
    - Multicode connections
- The chip rate is 3.84 Mcps
  - Approximate bandwidth is 5 MHz
  - Carrier spacing is **on a raster of 200 kHz**
  - Supports higher data rates/capacity
  - Increased multipath diversity (proportional to chip duration)

UMTS Protocol Stack (simplified)

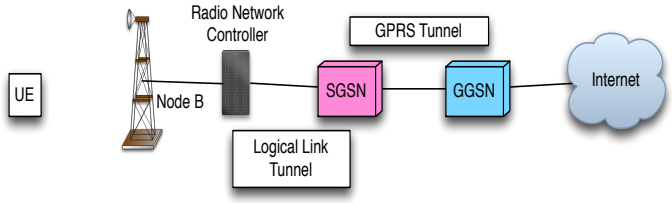
- Shown only for "radio access" part
- Top
  - Control signaling
- Bottom
  - User "Data"
- Voice is handled using circuit switching
  - Intricate – maybe later



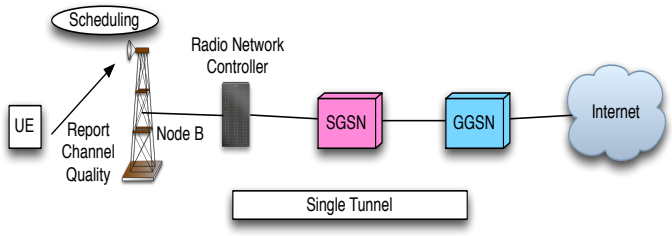
High Speed Packet Access (HSPA)

- HSUPA – uplink and HSDPA – downlink
  - Packet data only
  - More efficient (less tunneling, local scheduling)
- Makes use of
  - Hybrid ARQ
    - Combines erroneous frames with retransmitted frames to achieve diversity
  - Fast scheduling
    - Instead of signaling from the RNC, a node B is allowed to make decisions on the maximum data rates that a MS can use to transmit packet data
    - Vendors implement proprietary algorithms

Packet Data in UMTS Vs HSPA



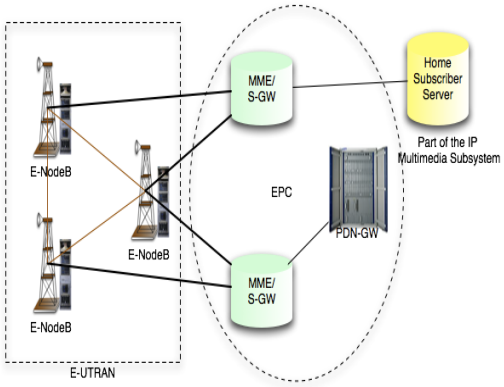
(a) Packet data in UMTS



(a) Packet data in HSPA

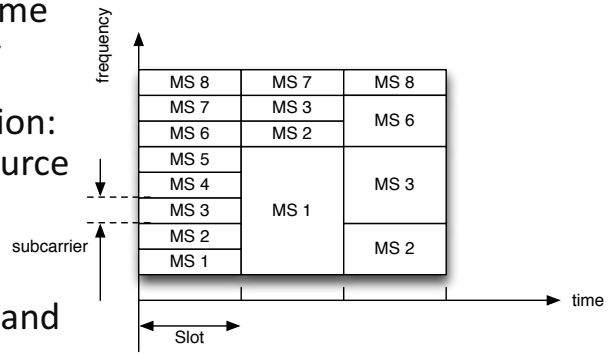
4G (LTE)

- Different network architecture to support packet based access
  - Flatter!
- All IP core network that can interface better with technologies such as WiFi and WiMax
- Use of OFDMA as the medium access/modulation scheme
  - Underneath – QPSK, QAM
- Flexibility to deploy it in as little spectrum as 1.4 MHz and as much as 20 MHz of spectrum
- Support for true "broadband"



OFDMA

- Flexible resource allocation in time and frequency
- Unit of allocation: "Physical Resource Blocks"
- LTE Downlink, WiMax uplink and downlink



Channel Bandwidths

Check actual BW!

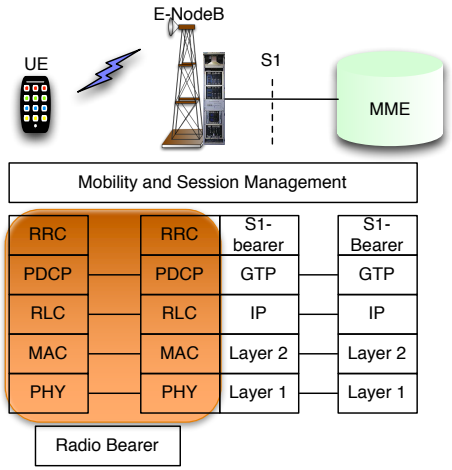
- Compare with AMPS, GSM, IS-95, UMTS and WiMax
- Can vary from 1.4 MHz to 20 MHz
- Resource Block (RB)
  - 180 kHz wide and 0.5ms long
  - 12 subcarriers spaced at 15 kHz (24 at 7.5 kHz possible later)
- Data rate limited by User Equipment (UE) categories

Channel BW (MHz)	1.4	3.0	5	10	15	20
Resource Blocks	6	15	25	50	75	100

Functional Changes

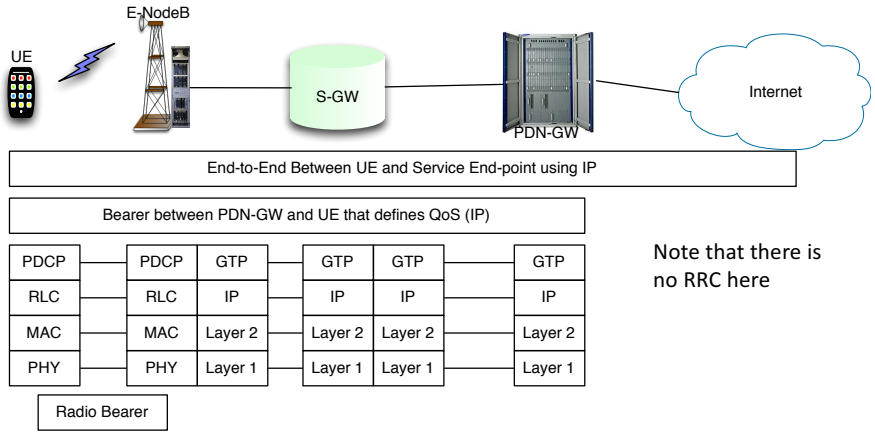
- E-NodeB
  - Does a lot more now! (no RNC or BSC)
  - Selection of MME, RRM functions, Handling Mobility
- MME
  - Sends pages to e-NodeBs
  - Handles security
  - Idle state mobility
- S-GW
  - Termination of user plane
  - Switching of user plane (mobility)

LTE Simplified Protocol Stack (Control Information)



- Shaded stack is called the "access stratum" - AS, upper layers are called "non-access stratum" – NAS
- RRC = Radio Resource Control
  - Includes measurements on signals
- PDCP = Packet Data Convergence Protocol
- RLC = Radio Link Control

LTE Simplified Protocol Stack ("Our Data")



Note that there is no RRC here

Wireless Local Area Networks

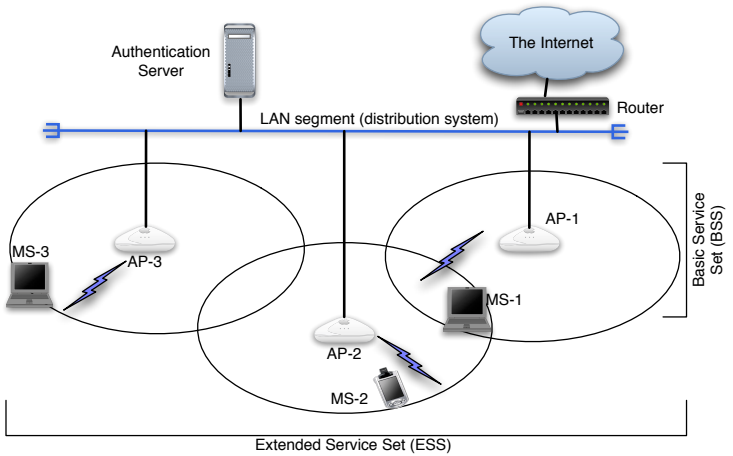
- Used primarily in smaller areas
  - Homes, campuses, coffee shops, businesses
  - Support communication to mobile data users via wireless channel
- Standards
  - IEEE 802.11 a, b, g, n, ac, ad, standard (wireless Ethernet)
  - The project was initiated in 1990, the first complete standard was released in 1997
    - 1Mbps, 2Mbps, 11Mbps, 54 Mbps, >100 Mbps rates
      - Use Barker codes (spread spectrum), CCK, OFDM, MIMO
    - Infrastructure based and Ad-Hoc based networks
  - HIPERLAN 1 and 2
- Typically use unlicensed spectrum

Some WiFi Standards

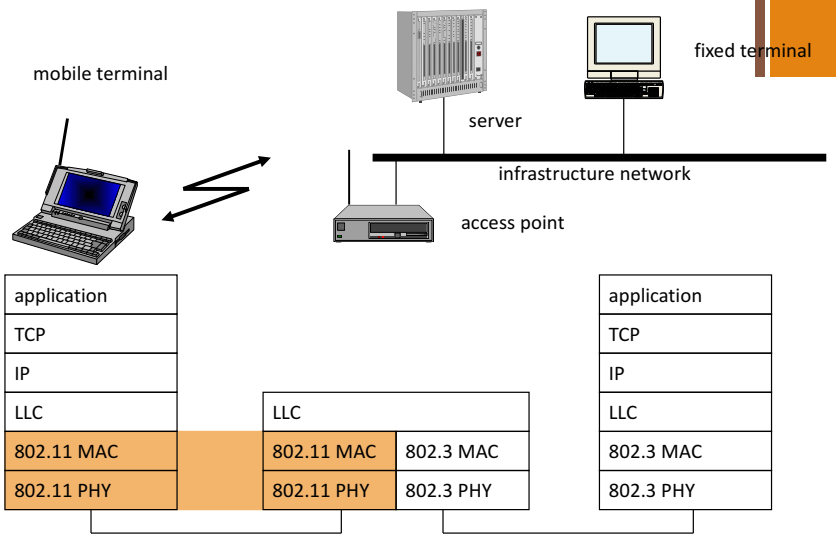
How about channels?

Standard	*Spectrum – US (GHz)*	*Data Rates*	*Transmission Scheme*
Base IEEE 802.11	2.402-2.479	1, 2 Mbps	GFSK, FHSS
	2.402-2.479	1, 2 Mbps	B/QPSK, DSSS
	850-950 nm	1, 2 Mbps	PPM, IR
802.11a	5.15-5.35, 5.725-5.825	6-54 Mbps	OFDM
802.11b	2.402-2.479	1, 2, 5.5, 11 Mbps	CCK
802.11g	2.402-2.479	1-54 Mbps	OFDM, CCK
802.11n	2.4 and 5 GHz	Up to 600 Mbps	MIMO/OFDM
802.11ac	2.4 and 5 GHz	> 1 Gbps	MIMO/OFDM and multi-user MIMO

Generic Architecture - WLANs



Protocol position of IEEE 802.11

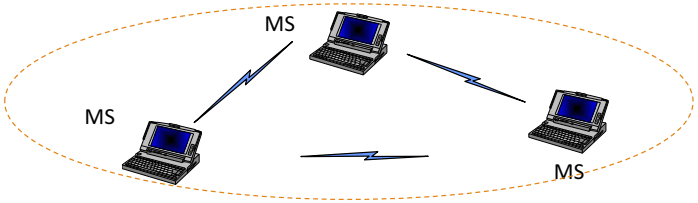


Ad hoc network topology

- Distributed topology
  - Devices communicate between each other directly (like walkie-talkies)
- Characteristics
  - Reconfigurable networks
  - No need for a wired infrastructure
  - Suitable for rapid deployment
- Need to "discover" communicating parties, services, methods of routing data, and so on

Ad Hoc WLANs

- MSs communicate in a peer-to-peer manner
  - Single-hop: They have to be in range of one another
    - Most vendors support only this option
  - Multi-hop: MSs can act as "relay nodes"
    - HIPERLAN/1 supports this, but there are no real products



Independent Basic Service Set (IBSS) in 802.11 WLANs

What is a personal area network?

- Origins in the BodyLAN project initiated by BBN in the early 1990s
- Networking "personal" devices – sensors, cameras, handheld computers, audio devices, etc.
  - Range of around 5 feet around a soldier
- Today: Networking digital cameras to cell phones to cameras to laptops to printers to …

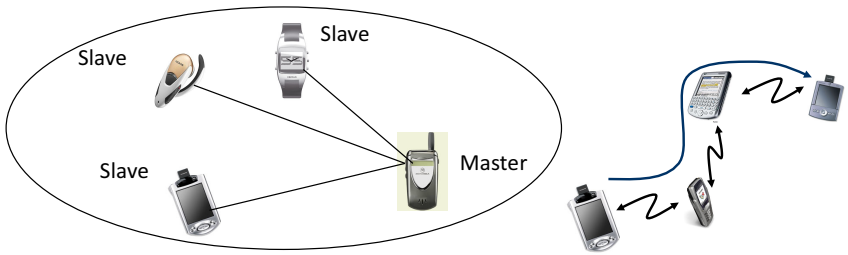
IEEE 802.15

- Started in 1997 as a sub-group of IEEE 802.11
- Initial functional requirements
  - Low power devices
  - Range of 0-10m
  - Low data rates (19.2-100 kbps)
  - Small sizes (0.5 cubic inches)
  - Low cost
  - Multiple networks in the same area
  - Up to 16 separate devices

Some WPAN Standards

Technology/ Feature	802.15.1 (Bluetooth)	802.15.4
Frequency	2.4GHz	2.4GHz - 868/915MHz
Modulation	FHSS/BPSK	DSSS/QPSK
MAC	TDMA/TDD	CSMA/CA
Max. data rate	1Mbps	20/40/250Kbps
Device types	One	Full/Reduced Function
No. of channels	79 (hopped)	26
Max. No. of devices	8	Up to 65535
Battery life	Weeks	Months
Coverage	10 m	10/50m
Topologies	Star, peer-peer	Star and cluster-tree
Connection time	3-5s	30ms

Generic Architecture - WPANs

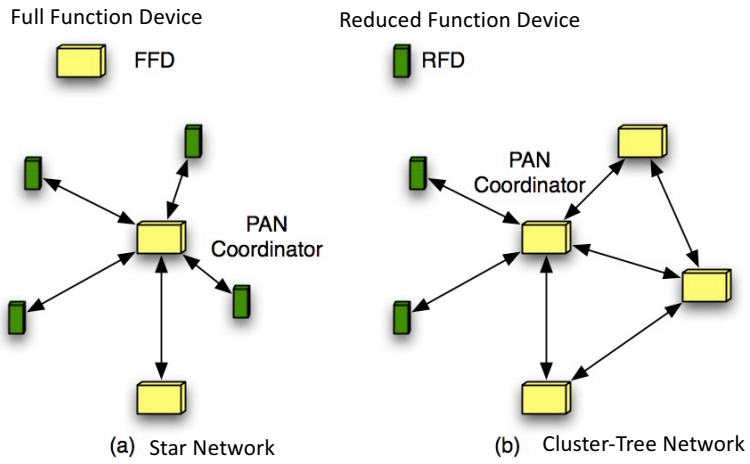


- Ad-hoc topology
- Bluetooth: A "cell" or "piconet" is defined by a Master device
  - The master controls the frequency hopping sequence
  - The master also controls the transmission within its piconet
- Others
  - Sensor networks (802.15.4), RF-IDs, mobile ad hoc networks

IEEE 802.15.1 or Bluetooth

- Operates in the same 2.4 GHz bands as IEEE 802.11b
- It employs frequency hopping spread spectrum
  - Channels are 1 MHz wide
  - The modulation scheme is GFSK for a raw data rate of 1 Mbps on the air
  - A basic time slot is defined as 625 microseconds
- A Bluetooth packet can occupy one, three or five slots
  - Sometimes a transmission is half a slot
- The frequency is changed every packet

802.15.4 and Zigbee



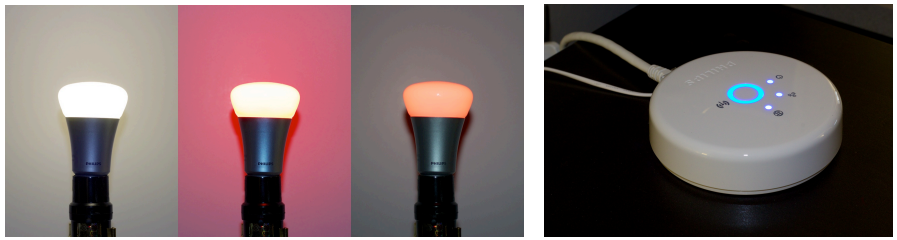
General Idea in 802.15.4/Zigbee

- Full function device (FFD)
  - Serves as a PAN coordinator (like a master)
  - Can route packets (relay)
- Reduced function device (RFD)
  - Mostly in sleep mode and communicate mostly with an FFD
- Star network similar to Bluetooth
- Cluster-tree provides ability to have a mesh network with different topologies

Example of 802.15.4/Zigbee

- Philips Hue
- Mesh networked
- Accessible through the Internet

Source: http://arstechnica.com/gadgets/2012/11/in-living-color-ars-reviews-the-hacker-approved-philips-hue-leds/2/



Ultrawideband (UWB)

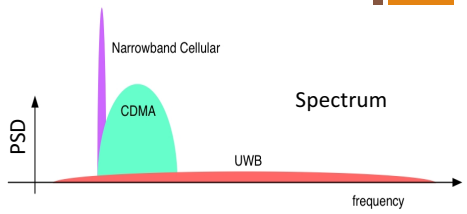
- Two definitions by the FCC
  - A radio signal that has an instantaneous bandwidth greater than or equal to 500 MHz
  - A radio signal with a fractional bandwidth ≥ 0.2 where

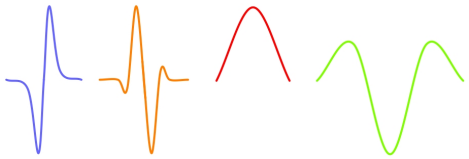
$$\text{Fractional Bandwidth} = \frac{2(f_H - f_L)}{f_H + f_L}$$

- Example: What is the fractional bandwidth of a UWB device operating between 3.1 and 4.8 GHz?
  - Answer: $2 \times 1.7/(7.9) = 3.4/7.9 = 0.4304 > 0.2$
- You can think of this as also being W/f_c where f_c is the center frequency and W is the bandwidth occupied
  - The bandwidth definition here is the frequency range beyond which the PSD is 10 dB below the maximum

More on UWB

- Typically transmit very short pulses of different shapes
  - Pulse width may be as small as a tenth of a nanosecond
  - Bandwidth associated with such pulses is huge (GHz)
  - Pulses are transmitted with a low duty cycle
- The PSD is very low
  - Looks like noise to most other signals

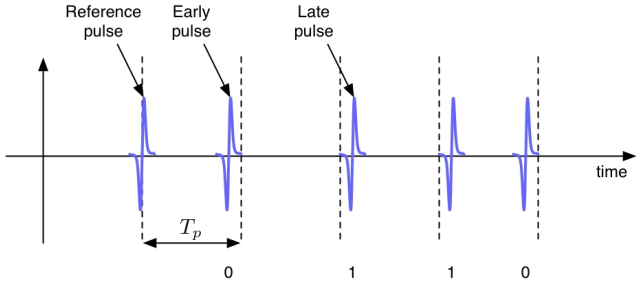




Pulse Shapes

UWB - Time Hopping PPM

- Idea
  - Use a reference pulse to indicate start of a period
  - A pulse transmitted earlier than the period represents a 0
  - A pulse transmitted later than the period represents a 1
- Different Tx-Rx pairs use different times to transmit pulses



Where can we use UWB?

- FCC regulations limit the PSD to a specific "spectral mask"
  - Suitable for short range applications
  - Very high data rates for a few meters
- Standards activities
  - Wireless Personal Area Networks using UWB
    - 802.15.3a - 110-480 Mbps

Next Week

- We start with dB and antennas
- Introduction to Radio Propagation