

Two approaches have been taken to improve GSM's data capability—High Speed Circuit Switched Data (HSCSD) •Achieved by Bundling TCH's •Time Slots are dedicated, whether sending or not—General Packet Radio Service (GPRS) •Packet oriented service rather than connection oriented•Dynamic Allocation of timeslots based on demand•This service is under development•Involves building a separate data network, requires infrastructure

**HSCSD** •MS requests one or more TCH's which corresponds to one or more timeslots•In theory each TDH corresponds to a TDM slot and there can be up to 8 assigned per call.—This would result in a data rate of up to 115.2 Kb/sec in each direction•The assignment can also be asymmetric, transmit and receive have different allocations•In practice there are limitations—MS is required to send and receive at the same time—Standard GSM does not require this—uplink and downlink slots are shifted in time by 3 slots—Therefore in HSCSD only 4 slots can be used

**Disadvantages of HSCSD** •This is a circuit switched service with all the limitation of this approach•Subscriber pays for allocation, i.e connect time, whether or not they are sending data •Computer traffic is bursty, therefore this leads to inefficient utilization •Once the slots/ channel has been allocated, even if idle, it cannot be used by other subscribers

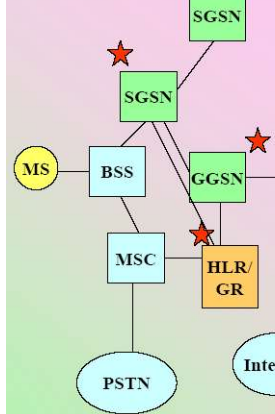
**GPRS**•GSM was designed to be a voice network, rather than a data network..circuit switched rather than packet switched •GSM has been enhanced to provide a service that provides transmission of packet data •GPRS is considered a 2.5 G technology•Gaining acceptance / deployment increasing•Idea is to make use of some frequency channels reserved exclusively for GPRS use, these channels can be dynamically assigned

**GPRS Operations** •Time slots are assigned on demand and can vary based on needs.—Analogous to Statistical Multiplexing Concepts•A number of MT's can use the same channels. •A transfer rate up to 170 Kbps per subscriber is theoretically possible. •Actual rate lower:—Depends on coding scheme—Coding scheme depends on error rate •GPRS can be used in parallel to other GSM services—In fact a parallel network is constructed•GPRS requires additional network elements for routing, address conversion,tunneling data, administering users of GPRS—Essentially a lot of new infrastructure is required to operate the service

**GPRS Quality of Service** •GPRS users can specify a QOS profile•QOS parameters —Precedence / Priority ( high, normal, low ) —Reliability—Delay Class —User Data Throughput •GRPS can act to provide minimal delay and jitter to packets within the radio network.—Low delay packets are processed before other packets to keep them from being delayed.

**GPRS Architecture** •GPRS coincides with components for GSM voice / early data services•New Elements—GPRS Support Nodes (GSN)—Serving GSN (SGSN)—Gateway GSN ( GGSN)—GPRS Register (GR)•Modifications—Changes to Mobility Management

**Architecture**



**GPRS New Components** •GPRS Support Node (GSN)—essentially a router—Provides Interworking between GPRS network and PDN ( Public Data Networks—to the GGCN—Requests user addresses from the GPRS register—Acts at the equivalent level of the MSC —Interfaces to BSS•GR —GPRS Register —Keeps track of individual SGSN—Collecting Billing Information—Access Control

**GPRS Data Transmission Reference Model** •Used Tunneling to transport data between SGSN and GGSN—Uses the GPRS Tunneling Protocol ( GTP ) •A Sub-network dependent convergence protocol is used between the SGSN and the MS•SGSN is connected via Frame Relay to the BSS

•Applications -Protocol Data Units of the application•SNDCP —Subnetwork Dependence Protocol —Adapts Application PDUs to lower level protocol •LLC •GTP —GPRS Tunneling Protocol •LLC —Link layer Control •MAC —Medium Access Layer •RLC —Radio Link Control •FR —Frame Relay •IP —internet Protocol•UDP/TCP —Data Gram and Transport Control Protocol

**GPRS service**—intermittent data transfers benefit from sharing the available bandwidth.—GPRS data is billed per kilobytes of informationtranscevedcontrast to circuit switched data connections, billed per second of connect time —Provides Authentication and Encryption Services •GPRS upgrades GSM data services providing:—Point-to-point (PTP) service: internetworking with the Internet (IP protocols) and X.25 networks. —Point-to-multipoint (PTM) service, point-to-multipoint multicast and—Short Message Service(SMS): bearer for SMS.

GPRS Today-2003•Telephone operators have priced GPRS relatively cheaply compared to HSCSD•Typical rates vary wildly, ranging from EUR1 per megabyte to over EUR 20 per megabyte. •In the US, T-mobile offers \$30 per month unlimited GPRS. Other carriers such as AT&T Wirelessalso offer flat-rate plans. •The maximum speed of a GPRS connection (as offered in 2003) about 4-5 Kbyte/sec •Latency is poor, a pingbeing about 600-700 ms and often about 1 second round trip time. •GPRS is typically prioritized lower than speech, and thus the quality of connection varies greatly. •GPRS could be made to work a lot faster, requires additional modifications to network

**3G** •The next generation of cell phone and other portable communication devices and services is broadly called 3G•Growth in Data is anticipated•3G Goal: Provide high data rates to end users > 150 Kb/sec•These services fall into the following categories—Inherent to the Network•Connectivity, addressing, location, supplementary services—Applications•Web Browsing, Games, E-mail•Next Generation of cell phones will have higher security in addition to Bandwidth and Functional Capability•Cell Phones /should remain a growth area

**3G Initiatives** •IMT-2000 ( International Mobile Telecommunications)—ITU made a request for proposals to establish a world wide communication systems that allowed for terminal and user mobility — Within this context ITU made a number of recommendations•IMT-2000 includes different environments—Indoor, vehicles, satellites—WRC ( World Radio Conference identified 1885 –2025 Mhz and 2110 – 2200 Mhz as frequency bands for IMT-2000 services •IMT-2000 evolved into a family of standards, as no consensus could be reached on the best way to proceed •The European proposal for IMT-2000 prepared by ETSI is called Universal Mobile Telecommunication System ( UMTS )—Part of UMTS is to provide a natural evolution form GSM into 3G

**UMTS** •Europe's approach for 3rd Generation -Universal Mobile Telecommunication System —A group of technologies and standards that will deliver broadband wireless at speeds up to 2 Mb/sec—Products include Voice, Data, audio, video—Packet Based Transport vs Circuit Based—Wireless access through various Terrestrial Cellular Systems and Satellites—Based on GSM standards and philosophy•Similar Subscriber Management Overlayer.

**UMTS Standards** •Radio Interface -UTRA —Universal Terrestrial Radio Access •UMTS leverages the infrastructure of GSM•Initial Enhancement include GSM EDGE that we covered previously as part of GPRS —Edge used in US but not in Europe •UMTS fits into an even larger framework developed in the mid 1990's called Global Multimedia mobility ( GMM)

**UMTS Today**•Introduced in many Countries —Release called R99•Radio Access Technologies —UTRA FDD ( Frequency Division and Code Spreading—very different than the TDM interface of GSM —UTRA TDD •Various Releases of specifications have occurred within

**UMTS System Architecture** •Simplified Reference Architecture •UE —user Equipment ( Mobile )•UTRAN -UMTS Terrestrial Radio Access Network—Comprised of a number of Radio Network Subsystems•CN-Core Network•Uu —User Equipment Radio Interface ( similar to Um Interface in GSM ) •Lu ( similar to A bis interface in GSM ) —Radio to Core

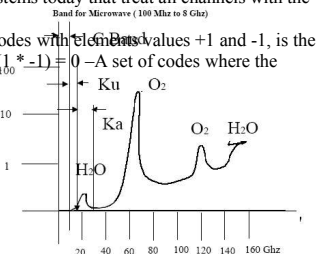
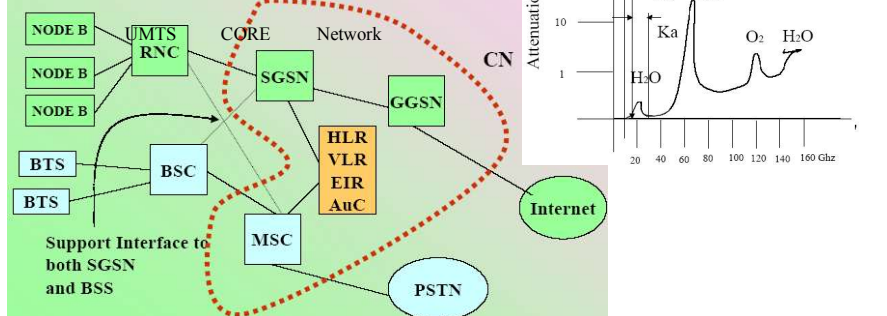
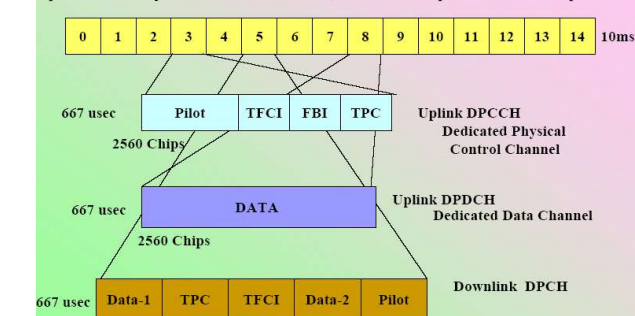
**UMTS Domains and Interfaces**•User Equipment —USIM ( user related-contains SIM ) + Mobile Equipment ( Physical radio system)•Access Network —Interface between Radio and Network•Serving Network comprises all functions currently used by user for accessing UMTS services•Home Network Domain-all functions related to the home network of user, data look-up etc

**UMTS Network** •UMTS is a network infrastructure is two main elements, connected over a standard interface, called Lu. These two elements are:—UTRAN(UMTS Terrestrial Radio Access Network)—Core Network •Similar to NSS. •UTRAN (UMTS Terrestrial Radio Access Network(RAN)—equivalent to the GSM BTS and the Radio Network Controller (RNC) which is equivalent to the GSM BSC. •UTRAN uses : Frequency Division Duplex (FDD) and W-CDMA. This mode offers the highest efficiency within a single system whatever the conditions—wide area, urban, indoor coverage from outdoor, indoor, and so on. One carrier use 5Mhz.

**UMTS Core Network** •The Core Network equivalent of the GSM NSS. •Implementation Options —ATM based architecture: in some cases the two-domain architecture of GSM/GPRS, with: Lu-PS (Packet Switched) interface instead of Gb on the packet domain. Lu-CS (Circuit Switched) interface instead of A on the circuit domain. —Transport Independent and multimedia architecture: this R'00 architecture is in line with the Next Generation Networks architecture and introduces separation of control and user planes. It also integrates multimedia capabilities.

**UMTS Radio Interface**•As stated, UMTS uses a very different modulation scheme than GSM•CDMA, orthogonal codes, 5 Mhz wide bands •Chipping rate of 3.84 Mchip/sec•To allow combinations of different data rates over the same spectrum, yet maintaining orthogonal behavior UMTS uses Orthogonal Variable Spreading Factor—In contrast to CDMA based systems today that treat all channels with the same rate.

Orthogonal Variable Spreading Factor-1 •As way of review—Two codes are said to be orthogonal when their inner products is zero. The inner product, in the case of codes with elements values +1 and -1, is the sum of all the terms we get by multiplying two codes element by element.—For example, (1, 1, 1, 1) and (1, 1, -1, -1) are orthogonal: (1 \* 1) + (1 \* 1) + (1 \* -1) + (1 \* -1) = 0 —A set of codes where the inner products of any two codes are all zero, with the exception of the inner product of the code with itself



Satellite in Low Earth Orbit—R = 1000 Km, compute period—Re = 6.37 x 103 Km—M = 5.98 x 1024 Kg—G = 6.67x 10-11 Nt-M2/Kg2—T = 6.26 SQRT(( 7.37)3 x 1018) / (6.67 x 5.98x1013) = 6.26 SQRT(10.03 x 105) = 6353 seconds = 105 minutes•Satellite in Geo-Synchronous Orbit—T = 24 hours, compute Radius —T = 86400 sec—Rearrange R and T equation, substitute for R—R = (75 x 1021)1/3 = 4.2 x 107 meters = 42,000 Km—Height above Earth = R —Re = 42,000 —6,370 Km = 35,630 Km

$$F_{gravity} = \frac{GMm}{R^2}$$

$$F_{centripetal} = \frac{mV^2}{R}$$

For Circular Motion :  $F_{gravity} = F_{centripetal}$

$$V = \frac{2\pi R}{T}$$

**Spectrum for Communication**

Satellites Band Frequency Downlink Uplink Comments

L, 2.1-6 GHz, 2-3 GHz, Mobile Globalstar  
 S, 1.6-1.7 GHz, 1.5-1.6 GHz, GPS  
 C, 3.7-4.2 GHz, 3.5-6.5 GHz, GEO  
 Ku, 11/14, 11.7-12.2GHz, 14.0-14.5 GHz  
 Ka, 20/30, 17.7-21.7 GHz, 27.5-30.5GHz Susceptible to Rain Fade

$$\sqrt{\frac{R^3}{GM}} = \text{or } R = \left(\frac{T^2 GM}{4\pi^2}\right)^{1/3}$$

	Altitude (Km)	Delay	Global Coverage	Uses	Orbital Period
GEO	36,000	0.25 sec	3	Direct Broadcast TV, Net Back Bones	24 hrs
MEO	5,000 to 15000 Km	.035 to .085 sec	Around 10	Point to Point GPS-Global Positioning System	About 6 hours
LEO	700 to 1500 Km	.01-.05sec	Around 50	Point to Point Voice and Data, Remote Telemetry	About 1 to 2 hours

**Satellite Ground Terminals**•Satellite Terminals consist of Antenna for transmission and/ or reception, plus the electronics to encode/decode the modulated signal into a digital stream•For GEO's the Antennas are parabolic in shape, High Gain Antennas fixed in position•GPS receiver antennas are small( less than 6"), but enough to pick up the signals from 3 or more MEO satellites•LEO satellites can use less focused antennas—Satellites closer to earth surface than GEO, needed power scales roughly as (1/r)\*\*2—Form for Sat-phones are "cigar" sized.

**General Advantages and Disadvantages of Satcom vs Terrestrial**•Advantages—Global coverage from one platform—Safety from attack, sabotage, terrorism—Always available •Disadvantages —Capital Intensive / expensive / risky—Signal Limitations •Delay•Doppler Shift can be large for certain applications •Large distances —low / demanding power margins( link budgets)•Susceptible to solar activity•In some bands, mainly Ka, subject to rain fading •Despite the risks, costs, and limitations these systems are economically viable

**Satellites Networks and Services**•Satellite networks can consist of one satellite up to hundreds, and can consist of thousands of ground terminals•Ground Terminals requires coordination in using uplinks and downlinks...involved in managing the media access layer—Covered ALOHA Protocol •Frequency Division Multiplexing or Time Domain Multiplexing is required to make efficient use of satellite channels•Satellites often augment other networks and are the networks of last resort —because of their cost and other limitations( delay )

**LEO Satellite Systems**•LEO—Low Earth Orbit•Foot Print much smaller than GEO—Foot Print Diameter on the order of 1500 Km •Because of size and power limitations these systems tend to provide low data rate service.—Voice / Data on the order of 10 Kbs or less. •Advantage: —Low delay as compared to a GEO —Since satellites are lower altitude less power required by transmitter•Allows hand held devices to reach satellites•Disadvantage:—An orbital period of one hour corresponds to moving across the path—from horizon to directly overhead back to horizon of about 15 minutes—This requires that the ground stations have tracking antenna, that follow the path of a satellite, adding more complexity—Since these are low power and operate at certain frequencies, signals cannot penetrate buildings

**GPS—How it works**•GPS Satellite continuously sends a data stream that contains its orbit information, equipment status, and the exact time. •All of the satellites broadcast their messages on the same frequency, but they each include a unique identification code. The receiver determines which message is from which satellite by matching the identification code with the codes stored in its memory. •GPS receivers compute the difference between the time a satellite sends a signal and the time it is received. •Distance between the GPS receiver and the satellite (TIME x SPEED = DISTANCE), location in space. •With readings from three satellites, at the same time can determine with great precision the absolute position.

**DAB What is it**•The (Direct Audio Broadcasting)DAB system is a novel broadcasting system intended to supersede AM, FM systems. •DAB is spectrum and power efficient, designed for terrestrial and satellite as well as for hybrid and mixed delivery. •Provides CD-quality sound, noticeably better than an FM analog broadcast. —Immune from interference and fading (egprograms are not suddenly lost when the car passes through a tunnel or under power lines).•DAB allows broadcasters to transmit text or data relating to the program, so listeners could read on a small LCD screen related information and even a succession of images like a slide show, with images changing every few seconds. •DAB uses a single frequency (called a "Multiplex") can carry up to six stereo or 12 mono services or any combination in between. •Examples of DAB receiving equipment: car radios, sets for the home, PC plug-in receiver cards, etc.

**Digital Audio Broadcasting**•Systems are starting to be introduced in the US and Europe•DAB systems using single frequency networks—All senders transmitting the same radio program use the same frequency—Can also include side channels that provide data •A Single Frequency Network (SFN) is efficient—Radio station needs one frequency throughout the country DAB power per broadcasts are small ( orders of magnitude less than Traditional FM stations)—Can use Satellite as a distribution mechanism

**Advantage of WLANs**•Flexibility: Within Radio range nodes can communicate—No wiring —Works through walls•Planning—No wiring plant needed —Can put in old buildings•Design—Allow for design of small unwired devices—Many new services•Robustness —Can be quickly configured, used in emergencies etc•Cost—Low cost, wiring is expensive •Disadvantages •Quality of Service—Variable service—Range dependent data rates—Subject to interference•Restrictions—Wireless devices need to comply with regulations •Safety and Security—Interference with other equipment •Hospitals/ pacemakers etc —Open Radio Interface makes eavesdropping easy •Example War Driving •Power—As with any unwired device, power consumption is often limited to battery capacity

**Design / Implementation Considerations**•Global Operations•National and International consideration have to be considered by equipment vendors —varying requirements•Power Considerations•Often Devices are battery powered. •Amount of electrical power budgeted to communications is limited•License Free operations•LAN operators( you in your house) do not want to apply to the FCC for permission to transmit. Therefore must use ISM bands. for example 2.4 Ghz ISM in US •Robust Transmission Technologies•Subject to RF interference•Omni Directional Antennas•Subject to High BER•Simplified Spontaneous Operations—Should not require a complicated set up procedure, should be on line at boot up , no need for operator/ user intervention Protection of Investment—Interoperable with existing networks—Simple bridging between LANS—Simple standard interfaces to WANS•Safety / Security—Safe to operate in hospitals other sensitive RF—Users cannot be hared by antennas—Wireless LAN links need to be encrypted•Transparency of Applications—Applications that work over wireless LANS should work over wiredLANS even though subject to higher delay, higher BER, and higher noise

**Advantages/ Disadvantages of Infrared**•Advantages :-Simple and inexpensive to build emitters and sensors—Widespread use today in portable devices—Close Range, does not interfere—Data rates on the order of 115 Kb/sec to Mb/sec—Does not interfere with electrical devices and vice versa•Disadvantages:—Low bandwidth compared to other LAN technologies—Does not penetrate walls or scatter around obstacles, much more of a LOS type technology—For the remainder of Module we will focus on Radio Based LANS—Susceptible to Sunlight

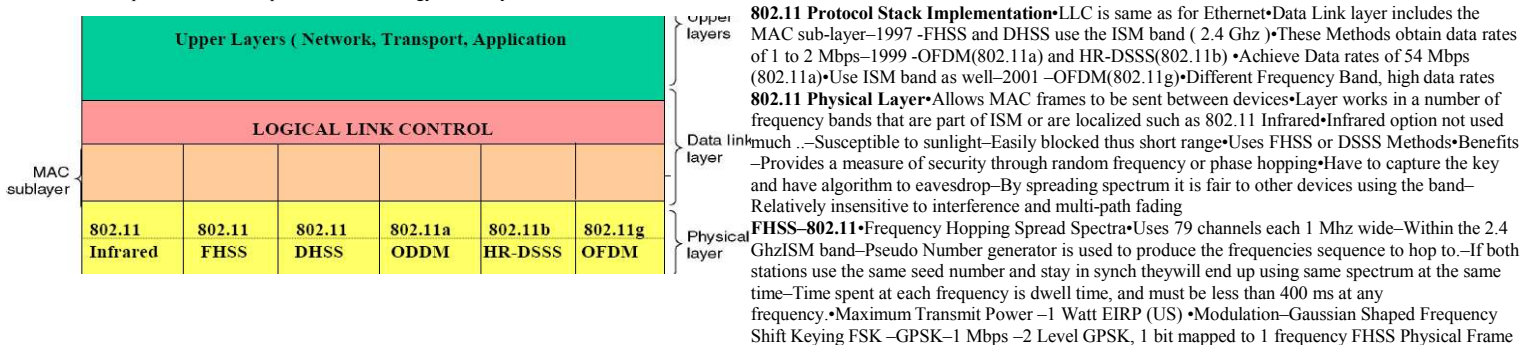
**Ad Hoc Networks**•Wireless Nodes communicate among themselves without the need for a central access or coordination point •Nodes using Ad hoc Networking can only work if they are within range of other nodes•Networks can be set up to route via intermediate nodes •Complexity in these networks are high—Hidden and Exposed Station problem •Advantage —Provides great flexibility and survivability•Some networks / systems can operate with a mix of adhoc and infrastructure

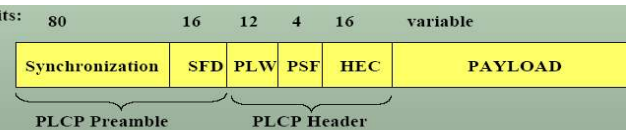
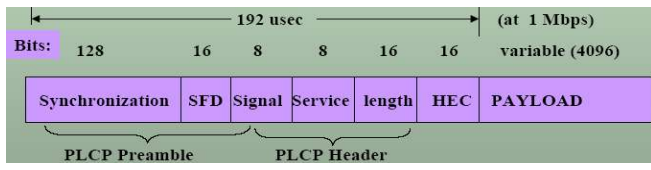
**IEEE 802.11** •The most well known set of wireless protocols •Part of the IEEE 802 family of standards —Each standard specifies the physical and media access but offers the same interface to higher layers ( link and layer 3 ) •Uses Spread Spectrum Radio Techniques •Operates at the 2.4, 5.4 Ghz ISM Bands •Data Rates supported in the Mb/sec and above range —802.11a ( up to 54 Mb/s at 5.4 Ghz)—802.11 b (up to 11 Mb/s at 2.4)—802.11g ( > 20 Mbps )

**Architecture of 802.11** —Infrastructure based •BSS—Basic Service Set —Station with range of Access Point •ESS —Extended Service Set—LAN extended bridging 2 access point •ESSID is the name of the network Nodes are called stations(STA) and connected to Access Points (AP) •STA's and AP's within a certain range form a basic service set ( BSS1, BSS2)•Extended Service Set is obtained through the connection of server Access Points•For a station to have access must have ESSID of Network•Stations can select an AP and associate with it. AP's support roaming between different AP's•AP's provide synchronization within a BSS , support power management, and control medium access to support time bounded services

**802.11 —Ad Hoc** 802.11 supports ad hoc networking between stations•Peer to Peer Networking •Forms one or more independent BSS's ( IBSS)•Each IBSS uses its own radio frequency—Thus stations in IBSS 1 even in physical range cannot communicate with stations in IBSS 2 •802.11 in Ad hoc mode does not support any special nodes that support routing, forwarding or data exchange

**Details of 802.11 lower levels** PMD = Physical medium Dependent Sub-Layer —Handles modulation, encoding decoding, •PLCP = Physical Layer Convergence Protocol —Provides carrier sense—And common service point to PMD independent of technology•MAC layer is described in detail later —uses MACA•DLC —Data Link Control





•Frame Consists of 2 basic parts –PLCP Part ( Preamble and Header )–Payload Part •Payload Part is scrambled using a polynomial– $s(z) = Z^7 + Z^4 + 1$ –Avoids DC blocking and whitening of spectrum .. Long strings of 0's and 1's are bad \

**FHSS Frame-2**•Fields of the FHSS frame –physical level frame •Synchronization–80 bit pattern of 010101...01–Pattern used by potential receivers for synchronization•Start Frame Delimiter (SFD)–16 bits indicate the start of the frame and provides frame synchronization–Pattern 0000110010111101 PCLP-PDU Length Word –Length of the Payload in Bytes including a 32 bit CRC included at end of payload –PLW can range up to 4096 •PLCP Signaling ( PSF )–This indicates the data rate of the payload–All bits 0(0000) indicates lowest data rate 1 Mb/sec–(0100) corresponds to 2 Mb/sec–(1111) corresponds to 8.5 Mb /sec•HEC –PLCP uses 16 bit HEC –Generator polynomial  $G(x) = X^{16} + x^{12} + x^5 + 1$

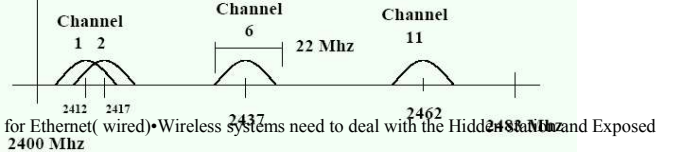
**DHSS –802.11**•Direct Sequence Spread Spectrum is an alternate to FSS–Robust against interference and multipath propagation ( delay time spread ) •Characteristics –Uses 2.4 Ghzband, data rates up to 2 Mbps–Maximum Transmit Power 1 W US ( EIRP), 100 mW in Europe and 10 mW in Japan–Uses phase shift Modulation–Has similarities to CDMA( Code Division Multiple Access )–802.11

DSSS uses 11-code Barker Code •Strong Autocorrelation Properties •Code ( +1 -1 +1 +1 -1 +1 +1 -1 -1 -1 ) •Chipping rate is 11 Mhz•Implementation more complex than FSSS **DHSS Level-1 Frame** •Synchronization:Used for Synchronization as well as gain setting, energy detection, frequency offset compensation•Synchronization fieldconsists of scrambled bits •Start Frame Delimited–used for synchronization at the beginning of a frame consists of the pattern 1111001110100000•Signal–used to indicate data rate of the payload–1 Mbps 0x0A, DBPSK–2 Mbps 0x14, DQPSK–Other values reserved for higher use Service –Field reserved for future use–0x00 indicates IEEE802.11 compliant frame •Length –16 bits used for length indication of the payload, units in microseconds•Header Error Check (HEC) –uses CRC-16 type polynomial

**HR-DSSS 802.11b**•High Rate Direct Sequence Spread Spectrum•Achieves 11 Mbps in the 2.4 Ghz band•This is the dominant standard in use today•Uses Walsh Type Codes assigned to different connection•Has a good range ( 7 times greater than 802.11a )•Enhanced version of 802.11b is called 802.11g•Uses modulation scheme of 802.11a but operated in 2.4Ghz band

**802.11b Channel Plan** •US/ Canada Channels–14 channels –Bandwidth 22 Mhz–Separation 5 Mhz

**The 802.11 MAC Layer** •The MAC layer has a number of important functions –Firs it needs to deal with the Medium Access challenge of radios –Also offers support for roaming , authentication, and power management•The MAC layer supports 2 basic services –Asynchronous services –Adhoc–Time-bounded service: Adhocand Infrastructure •Asynchronous Service–Adhocmode, best effort delivery model•Time bounded service–Guarantees a delay less than a maximum, only available in infrastructure mode



**802.11 MAC Sub-layer**•As we have discussed the 802.11 MAC sublayer is very different to the 802.3 Sub-layer for Ethernet (wired) •Wireless systems need to deal with the Hidden/Exposed Station problem

**802.11 Sub Layer Operation**•To deal with Hidden/ Exposed Station 802.11 supports 2 Classes of Access mechanisms–DCF = Distributed Coordination Function:Does not use any type of Central Control ( like Ethernet)•Support Async Services•CSMA/CA with RTS/CTS exchange–PCF = Point Coordination Function:Base Station Control activities in its area ( cell)•Support Time-bounded Services •Polling from AP –\* All implementations of 802.11 must support both types of operating modes simultaneously

**802.11 Event Intervals** •Interval spacings is system dependent/variable•SIFS:Allows 2 communicating parties in a dialog to send again. They have highest priority. After frame sent ACK issued again •PIFS:Base station can send a beacon or poll frame, if nothing happened in SIFS time•DIFS:(DCF Inter-frame Spacing) If nothing happened in SIFS or PIFS, any station can attempt to acquire the channel to send a new frame•EIFS:(Extended Inter-frame Spacing) : Stations can report bad or unknown frames •This allows DCF and PCF to coexist in a given cell

**DCF (Distributed Coordination Function)**•DCF uses CSMA/CA•Uses Physical Channel Sensing or Virtual Channel Sensing ( MACA)•Physical Channel Sensing( very much like Ethernet)–Station wants to transmit and senses channel–If channel idle start transmitting, sends entire frame–If busy the sender defers a random time and tries sensing again–If a collision occurs, stations wait random time again using the binary exponential back off Algorithm,and try again later–Problem of Hidden and Exposed Stations! •Virtual Channel –Uses RTS, CTS, ACK, and NAV( Network Allocation Vector )

**MACAW process** •NAV = Network Allocation Vector:An Internal timer that creates a “virtual channel busy”. Station will not attempt to transmit when it has a NAV enabled–NAV signals are not sent, they are just internal reminders •RTS and CTSframe include information on expected transmission including ACK, therefore other stations compute their NAV based on that information–In this example both C and D have a NAV and do not attempt to transmit in that time frame until the time of the ACK CSMA/CA: explicit channel reservation–sender: send RTS (20 bytes)–receiver: reply with CTS (14 bytes)•CTS reserves channel for sender, notifying (possibly hidden) terminals

**PCF-Point Coordination Function**•In PCF the base stations polls other stations asking if they have frames to send. it acts as a coordinator•No collisions ever occur because of central coordination.....No need for MACA/MACAW•Mechanism–Base Station Broadcasts a Beacon Frame on a semi-periodic basis–Beacon Frame contains, Hopping frequencies, Dwell Times, Clock Synchronization–Asks new stations to sign up for polling service•Power management important. Base station can put a station into sleep mode–Awakened by base station or user–Base station needs to buffer sent frames while station wakes up and is ready PCF and DCF may coexist within a cell

**802.11 MAC Frame Structure**•Standard Defines three different classes of frames–Data–Control(these include RTS, CTS ) –Management•MAC frames are transmitted between Mobile Nodes, Nodes and Access points , and between access points•802.11 Data Frame

**802.11 Frame Control**•Contains 11 subfields–Protocol Version:2 bit field indicates current protocol version , set to 0 –Type( type of frame : data(=10) , control(=01) , or management(=00))–Subtype :For Management( RTS(1011), CTS(1100), beacon(1000)–TO DS / From DS: Indicate frame going or coming from other Cell/ Network–MF :Frame Fragments will follow this frame is set to 0 –Retry :if this is a Retransmission(=1)–PWR:put station into sleep( powersave=1 ) or take it out of sleep, or remain on –More:Sender has additional frames for receiver–W:Whether frame body has been encrypted–O:Tells receiver whether frames need to be in order(=1) or not (=0)to deliver to higher layer **802.11 MAC Frame –Duration, Addresses**•Duration Field :Tells how long the frame and acknowledgment will occupy channel: used for NAV•Four addresses in frame ( in IEEE-802 format ) –48 bits–Address 1:Address of intended receiver –Address 2:Address of sender ( within cell ) –received ACKS–Address 3:Source base station for inter-cell traffic–Address 4:Destination base station for inter-cell traffic

**MAC Management** •The MAC layer conducts a number of management functions needed for the system to operate•Some of the primary functions are–Synchronization•Synchronization of clocks, hopping frequencies, generation of beacon signals –Power Management•Functions needed for power conservation such as sleeping–Roaming•Function for joining a network•Changing access point–System Management Interface•Management Information Base for the MAC layer.... Data is stored for retrieval and control by a network management station

**Synchronization**•Timing synchronization is essential for operation of the LAN•Clocks used for –Power management –PCF coordination functions–Coordination of hopping sequences in FHSS•Beacon Frame –Timing is conveyed using a periodic( not always ) transmission of a Beacon Frame. •Contains a time-stamp and other information related to roaming and power management–Nodes adjust their clocks based on beacon signals information –Beacon frames can be suppressedif the medium is busy sending data for example–The time between successive beacons is called the beacon interval

**Beacon Frames** •Infrastructure networks–The access point send out a beacon frame–Nodes in the network read the timestamp in the frame to adjust their clocks •Ad hoc networks more complicated–All nodes can send a beacon frame –Each node maintains it's own synchronization times and starts the transmission of a beacon frame after the beacon intervals–Multiple stations will attempt to send a beacon frame but they must contend for the channel and are controlled by the a random back-off algorithm, so one station wins.–All stations now adjust their clocks to the beacon signal that was sent by the winner–The process will start again after the beacon interval has expired

**Power Management in 802.11**•Basic idea is to turn off the transceiver when the station is not in use, it enters a sleep mode•If a sender wants to send data to a node that is asleep it must buffer the data until the station awakens•Stations sleep and awaken periodically•If all stations wake up at the same time, all senders can announce their destinations and the stations that need to receive a message or send a message stay awake. •The others stations can go back to sleep •Since the stations are synchronized with beacon frames it becomes possible for all of them to awaken and go back to sleep at the same time

**Power Management in an Infrastructure Network** •The access point buffers all frames destined for stations in power saving mode ( sleep on and off)•With every beacon sent by the access point, a traffic information map(TIM) is transmitted. –TIM contains list of stations for which buffered frames exist •The power saving mode stations wake up periodically to receive the beacon **802.11 Services**•802.11 specification requires 9 services–5 Distribution Services : relate to interacting with stations outside a cell and with cell membership –4 station services : relate to activity within a cell

•Distribution Services–Association–Disassociation–Re-association–Distribution –Integration•Station Services–Authentication–De-authentication–Privacy –Data Delivery **802.11 Distribution Services**•Association–Allows mobile station to connect to a base station( used when mobile moves within area )–Includes identity information and capabilities–Capabilities include data rates, PCF requirements, Power Management Requirements–Base station may accept or reject station•Disassociation–The termination of an association–A station should use this service before shutting down or leaving–Base station can also send out disassociation when it is going off air. Reassociation–Station may change it's preferred base station using this service –Useful for stations moving from one cell to another•Distribution–Service determines how frames are routed. If destination is local to base station frames sent thorough radio channels. If destination is out of cell base station needs to route this over a network–Base stations use services when going down for maintenancepurposes. •Integration–This service handles the translation from 802.11 format to the format required by the destination network

**802.11 Station (Intra-cell ) Services**•Authentication–After association the base station sends a special challenge frame to mobile. Mobile encrypts the challenge frame and sends it back to base station. If base station can decrypt message then mobile has proper key and can be admitted to the group•De-authentication–When a mobile leaves a cell needs to Authenticate again to get services•Privacy–Encryption Algorithm for data •Data Delivery–The services associated with sending and receiving data between 2 stations in a cell

**Basic Security Goals and Mechanisms**•Security Goals–Confidentiality: Prevent casual Eavesdropping–Access Control: Protect access to a network. Discard all packets that are not properly encrypted using WEP–Data Integrity: Prevent Tampering with transmitted messages•Mechanisms •Network Access Control based on SSID –not very secure( contained in beacon frame) •MAC Address Filtering•Wired Equivalent Privacy (WEP)•Shared Key Authentication •Data Encryption

**WEP -Encryption Mechanism**•WEP uses a stream cipher called RC4•The key has a public part and a secret part. •For each frame a public key is added to the unencrypted part of the frame. •The secret part is kept by each station and is the same among a group of stations•To decrypt the receiver needs to add the public and private part of the key–Total length of the private key is 40 bits–EnhancedVersion 128 bit key. Station and AP share a 40-bit secret key–semi-permanent•Station appends a 24-bit initialization vector(IV) to create a 64-bit key( this is the public part)•The 64-bit key is used to generate a key sequence, kiIV–kiIVis used to encrypt the i-thdata bit,di:ci= diXORkiIV–IV and encrypted bits, ciare sent. WEP provides a good level of privacy but cannot meet goals against a strong attack

**Broadband Wireless -WiMax**•Apply wireless technologies over larger physical areas( Radius of 25 miles) ...more than 802.11a,b, g( 100's meters ) •WiMaxapplicable to last mile connectivity needs, replacement for wired local loop(DSL) or cable •Services envisioned include voice as well as advanced data services •Competes –with 3G Services / Cellular telephones–Cable Operator Services–DSL

providers – A disruptive technology – with barriers to overcome • Service envisioned to stationary devices • Standard developed to address this area is 802.16 – Referred to as wireless local loop – Wireless Metropolitan Area Network (MAN)

**Comparison of 802.11 to 802.16** • 802.16 envisioned for fixed stations opposed to 802.11 that supports mobility • 802.16 is used in large scale environments, one station can connect to many wired assets (e.g. a LAN in a building, village) .. Uses full duplex communication whereas 802.11 is half duplex • 802.16 uses more spectrum and operates in a much higher frequency band 10 to 66 GHz vs 2.4 and 5 GHz ISM bands. High freq has different propagation characteristics • Meant for outdoor antenna, physical layer very different characteristics than 802.11 • 802.16 is connection oriented, 802.11 is not

**The 802.16 Protocol Stack** • More sub layering than 802.11 or 802.3 • More a reflection on personalities of spec writers than physical necessity • Physical Layer: Narrow band radio is used with conventional modulation schemes

**802.16 Physical Layer** • 10 to 66 GHz is one of the few unused areas of spectrum – Susceptible to rain fade – At 30 GHz, the wavelength is  $3 \times 10^8 / 30 \times 10^9 = .01$  meters! • **802.16 Physical Propagation** – These small wavelength signals propagate in straight lines • Base station can have multiple steerable antennas • Because of sharp drop off, uses different modulation scheme based on distance from base station – Closest : 64 QAM – Middle : 16 QAM – Far : QPSK • Typical BW allocated per channel about 25 MHz. – For QPSK corresponds to best case 50 Mbps (Nyquist estimate) • Works best with a high Antenna and a flat geography – Hills are bad! – they cast long shadows • 802.16 provides flexible BW allocation to support asymmetric data transmission rates.

**Physical Layer Design** • Each TDM Frame is comprised of a series of timeslots • The ratio or down stream to upstream can be changed to meet the traffic demand • The system uses Hamming Codes in physical layer to carry out Forward Error Correction but also uses checksums in some of the higher layers (FEC can only correct 1 bit errors) • Design allows ability to burst frames in a single transmission reducing the number of preambles and headers

**802.16 Data Link Layer** • Comprised of 3 layers – Service Specific Convergence Layer – MAC sub-layer common part – Security Sub-layer • Security Sub-layer – Provide security service, authentication, encryption, key management – Same challenges that 802.11 faces • MAC sub-layer – Completely connection oriented • Provide a QOS guarantee – Base Station has strong control over system • Schedules base station to station and help coordinate station to base station communications – System does not have an Ad-Hoc mode.

**802.16 MAC Sub-layer Protocol-Channel Allocation** • MAC frames occupy an integral number of physical layer timeslots • A Upstream and Downstream MAP is created that keeps track of which MAC frames are occupying time slots and what timeslots are free • Downstream Channel (base Station to subscriber station) has easy mapping – Base Station decides which MAC frames to allocate to slots • Upstream channel (subscriber to base station) more complicated – Competing uncoordinated resources need access to it

**Connection Oriented Service** • Four classes of service are defined – Constant Bit Rate service – Real-Time Variable Bit Rate service – Non-real Time variable bit rate service – Best Effort Service • 802.16 is connection oriented, any connection is assigned one of these services • 802.16 defines 2 forms of bandwidth allocation – By station – By Connection • By Station: Subscriber station aggregates needs of all users and makes collective request for them. Station then allocates BW across users • By connection: Base station Manages each connection directly. • **802.16 Data Services** – Constant Bit Rate Service: Intended for transmitting uncompressed voice. Dedicated channels are allocated for this service. Used to carry multiplexed voice channels for example T1 • Real time variable bit rate service: Compressed Multi media and soft real time applications in which BW can vary. Accommodated by the Base station polling the subscriber to see how much BW is needed per instant • Non Real Time : Large File Transfers, less requirements on maintaining a minimum BW • Best Efforts: No Polling, subscriber contends with other stations. Request for BW by channels are done in time slots marked for contention in the upstream MAP

**Blue Tooth Introduction** • Whereas 802.16 covers MANs, BLUETOOTH is a set of standards and technology that addresses “pico-nets” – Piconet = Scales of 30 feet rather than 20 miles (802.16) – Consortium of five companies initiated effort in mid 90’s: Ericsson, NOKIA, IBM, TOSHIBA, INTEL • Goal is to develop a short range standard for connecting computing/ electronic devices – Get rid of cables – Devices automatically find out about each other and then configure themselves • Grew into a possible LAN technology that competes with 802.11 • Standard adopted by IEEE 802.15, working group covering wireless personal area networks • 2001 many products hit the market .... Many applications, met with some success. Interest into 2004 remains strong

**Blue Tooth Architecture** • Basic Unit is a Pico Net, one master node and up to 7 active slave nodes and 255 parked nodes – Size up to 10 meters from master • Multiple PICO-NETS form a SCATTER NET – bridged by a node • Data Rate up to 1 Mbps

**BlueTooth Architecture Considerations** • Power Management is important in small wireless devices • Master can switch nodes into low power, ie parked state • In parked state nodes can only respond to activation from Master • Master / Slave relationship : put smarts in Master, slave is a \$5 chip (easy to embed in consumer devices) • All communication is between Master and Slave, there is no direct slave to slave communication

**Blue Tooth Applications** • Specification to such precision and breath a good idea? – time will tell but it could be a bad way to go, but overall this appears to be a trend in the industry • Profiles are used to produce end user Applications • All Blue Tooth devices are expected to implement the Generic Access and Service Discovery profiles • Serial Port Profile: Support of legacy applications that require a serial port • Generic Object Profile : Client Server relationship . A slave can either be a client or a server. Supports peer to peer • In addition to the required profiles they can support application specific profiles. Networking Profiles – LAN access allows a BLUETOOTH device to connect to a fixed network – Dial Up Networking: allows a mobile computer to access the network via a mobile phone – Fax Profile: Allows Faxes to connect to mobile phones • Telephony Profiles – Cordless Telephony, Intercom, Head set • Data Exchange Profiles – Object Push – File Transfer – Synchronization

**Blue Tooth Protocol Stack** • From Physical to Application Level • BaseBand is analogous to the MAC layer in 802.11, 3 • Physical Layer: similar to 802.11, uses ISM bands

**Blue Tooth Physical Layer** • Designed to operate on Battery Power – Small low power chips • Low power system, range up to 100 meters • Three classes of power – Power class 1: Maximum Power is 100 mW, Minimum 1 mW – Power class 2: Max Power is 2.5 mW, nominal power is 1 mW – Power class 3: Out put Power 1 Milliwatt (mW) • Compared these powers to a cell phone that can transmit up to 600 mW, 802.11b device (1000 mW Operates in 2.4GHz ISM band – Potential for interference with 802.11 LAN stations • Band divided into 79 channels of 1MHz bandwidth each (like 802.11 FHSS)

• Modulation is QPSK, leading to a maximum rate of 1 Mbps per channel • Channel allocation is carried out using frequency hopping of 1600 hops/sec, dwell time is 625 usec • All nodes impico-net hop simultaneously to same frequency and controlled by Master Station • **Blue Tooth Physical Framing** • Blue Tooth data frame consists of 3 parts – Access Code: Identifies Master, so slaves within radio range of multiple masters can route to right one – Header includes checksum – Up to a 5 slot data transmission is allowed, yielding a maximum packet size of 2744 bits – Uses Stop and Wait Protocol

**Blue-Tooth Framing -Access Code** - Used for timing synchronization and piconet Identification • The 64 bit synch field contains addressing information

**Blue-Tooth Framing-Header** • Address Identifies destination station (1 of 8) • Type identifies the frame type ACL or SCO, slot length, and type of error correction used • F is flow bit , set to 1 when buffer is full and cannot receive any more data • A is a Piggyback ACK , set to 1 to verify previous frame • S = sequence Bit, 0 or 1 since this is a stop and wait protocol • 8 bit checksum • Entire header is repeated 3 times to form a 54 total bit header

**Link Manager Protocol** • The LMP manages various aspects of the radio link between the master and slave • The following functions fall within the LMP – Authentication, Pairing, and Encryption – Synchronization – Capability Negotiation – Quality of Service Negotiation – Power Control – Link Supervision – State and Transmission Mode Change

**BlueTooth BaseBand** • Layer analogous to the MAC layer • Master in each Piconet defines 625 usec time slots – Master slots in even – Slave slots in odd – \* Any node has the physical ability to be a master of a slave. • Frames can be 1, 3 or 5 slots long • There are up to 1600 hops/sec or 625 usec between hops, and there can be 625 bits in a slot. Frequency settling time takes 250 usec leaving only 375 bits remaining in a slot for useful transmission • OF the 375 remaining bits, 126 bits used for overhead, including header, leaving only 249 bits remaining. (249/625 = 40% efficiency) • If for example 5 slots are strung together, then there is only one frequency hop required. • Frames are transmitted over logical channels, called a link between the master and the slave • Two types of links are used – Asynchronous Connectionless (ACL) – Synchronous Connection Oriented (SCO) • ACL – Used for packet data – bursty and irregular in nature – ACL delivers on a best effort basis, if frames lost need to be re transmitted – Only one ACL link allowed between Master and Slave • SCO – For a dedicated fixed BW channel – Uses FEC ( forward error correction) – A fixed slot(s) are allocated in each direction – Up to 3 SCO links between the Master and Slave

**Robustness of Blue Tooth Links** • Bluetooth considering the low power manages to transmit data successfully up to 1 Mbps. • The technologies that make this possible are – FHSS – Error Correction • Blue Tooth 1/3 FEC simply sends three copies of each bit. A voting process is used to select the right bit. This will correct all single bit errors across these three bits • Blue Tooth 2/3 FEC detects all double errors and can correct all single bit errors and codewords – ACK links are protected using ACK scheme and check sums

**LMP -1** • Authentication, Pairing, Security – Manages the exchange of random numbers and signed responses for basic authentication – Pairing Service is a process to establish initial trust level between 2 devices, when this is established there is a pair link key – Set the encryption mode ( no encryption, point to point, broadcast) • Synchronization – Synchronization is always important in these systems – Clock offset updates each time a packet is received from the master – Devices can exchange timing information related to time differences between 2 adjacent piconets, so as to make corrections for slot boundaries • **LMP -2** • Capability Negotiation – As Different Bluetooth devices support different application profiles devices need to exchange information on supported features – Even some basic features may not be the same across devices related to voice encoding, SCO links, Encryption, etc, so this information needs to be exchanged • Quality of Service Negotiation – Different parameters control the QOS of a Bluetooth device at lower layers. Master set poll intervals and transfer rates, and type of packets to be used (for example Full , partial or no FEC) • Power Control: – Bluetooth device can measure the received signal strength. Depending on the signal level the device can direct the sender the measured signal to increase or decrease transmit power • State and Transmission Mode Change: – Devices may switch roles from Master to Slave, detach from a connection, or change state. The state changes are covered next slide

**State of a Blue tooth Device** • Standby defines the state of all devices not participating in piconet but are powered on – Node is running a clock • From Standby a device can enter Inquiry mode • Inquiry Mode – A device scans for other devices in the vicinity – Start inquiry procedure by sending out a Inquiry access code (IAC) – The IAC is broadcast – A device may periodically listen for other IAC messages – As soon as a device detects an inquiry it returns a packet containing its address and timing information required by Master to initiate connection – Device is now in SLAVE MODE • If Inquiry is successful the device enters page mode • In page mode the master set up connections to devices and calculates hopping sequences to contact each device individually. • The slave then answers and synchronizes with the Master’s clock • Once device enters the hopping sequence defined by the master it now is in the connected state • The Connected state involves 4 different states – Active State – Park – (Low power) – Sniff – (Low power) – Hold – (Low power) • In active state the slave can send, listen and transmit • All active devices have a 3-bit active member address (1 master & 2 slaves at any moment) • A device can return to standby mode via a detach procedure • Low Power Connected States – Park – (Lowest energy usage of the Low power) – Sniff – (Highest energy usage of the Low power) – Hold – (Low power) • Sniff State – Device listens to the piconet at a reduced rate – not every slot. The listening interval and rest time are programmable into the device – Can still receive messages SCO and ACL – Device holds AMA • Hold State – Device Holds AMA – Stops ACL transmissions – May still exchange SCO packets • Park State – Device release its AMA, freeing it up for other slaves – Receives a PMA – Device still member of piconet, FH synchronized, and wakes up at certain beacon intervals to maintain synchronization.

**Blue Tooth Security** • Main Features – Challenge Response process for Authentication – A cipher stream for Encryption – Key Generation Mechanism – Stronger than WEP used for 802.11b • The algorithms are implemented in silicon • Rely on higher layers for strong encryption • Security mechanism is used to set up a local domain of trust between devices • The security algorithms use – Public Identity of a Device – Secret/ Private user Key – Internally generated random key • For each transaction a new random number is generated and a new key generated • Key Management such as generation of the private key left to higher layers

**Blue Tooth Security Strength** • Stronger than WEP used in 802.11b • Quality of security depends on implementation • Often the PINS which are the start of the process are set to all 0’s, to insure interoperability without security management overhead • If Blue Tooth Devices are on they can be detected, this is a form of security but can be set into a non – discoverable mode – No answers to inquiry requests