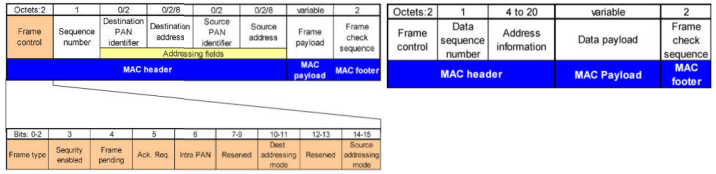
IEEE 802.15.4 Media Access Control (MAC) Layer

innovate achieve lead



- The MAC frame, i.e. the MPDU, is composed of **an MAC header (MHR**), **MAC service data unit (MSDU),** and **MAC footer (MFR).**
- **Frame control field (2 Bytes) :**
- It indicates the type of MAC frame being transmitted, specifies the format of the address field, and controls the acknowledgment.
- FC also specifies how the rest of the frame looks and what it contains.
- A Data Frame may contain both source and destination information with the size of the address field between 4 and 20 bytes.
- The payload field is variable in length. However, the maximum MAC data payload (that is the maximum size of the MSDU), aMaxMACFrameSize, is equal to aMaxPHYPacketSize (127 bytes) – aMaxFrameOverhead (25 bytes) = 102 bytes

IEEE 802.15.4 Media Access Control (MAC) Layer

innovate achieve lead

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Frame Type field

Table 2—Values of the Frame Type field

Frame type value $b_2\ b_1\ b_0$	Description
000	Beacon
001	Data
010	Acknowledgment
011	MAC command
100–111	Reserved

IEEE 802.15.4 Media Access Control (MAC) Layer

innovate achieve lead

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

- **Security Enabled field**
- The Security Enabled field shall be set to one if the frame is protected by the MAC sublayer and shall be set to zero otherwise.
- **Frame Pending field**
- The Frame Pending field shall be set to one if the device sending the frame has more data for the recipient. This field shall be set to zero otherwise.
- The Frame Pending field shall be used only in beacon frames or frames transmitted either during the CAP by devices operating on a beacon-enabled PAN or at any time by devices operating on a nonbeacon-enabled PAN.
- **Acknowledgment Request (AR) field**
- The AR field specifies whether an acknowledgment is required from the recipient device on receipt of a data or MAC command frame. If this field is set to one, the recipient device shall send an acknowledgment frame only if, upon reception

IEEE 802.15.4 Media Access Control (MAC) Layer

innovate achieve lead

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

PAN ID Compression field

The PAN ID Compression field specifies whether the MAC frame is to be sent containing only one of the PAN identifier fields when both source and destination addresses are present. If this field is set to one and both the source and destination addresses are present, the frame shall contain only the Destination PAN Identifier field, and the Source PAN Identifier field shall be assumed equal to that of the destination. If this field is set to zero, then the PAN Identifier field shall be present if and only if the corresponding address is present.

Destination Addressing Mode field

If this field is equal to zero and the Frame Type field does not specify that this frame is an acknowledgment or beacon frame, the Source Addressing Mode field shall be nonzero, implying that the frame is directed to the PAN coordinator with the PAN identifier as specified in the Source PAN Identifier field.

innovate achieve lead

IEEE 802.15.4 Media Access Control (MAC) Layer

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Destination Addressing Mode field

Table 3—Possible values of the Destination Addressing Mode and Source Addressing Mode fields

Addressing mode value b_1 b_0	Description
00	PAN identifier and address fields are not present.
01	Reserved.
10	Address field contains a short address (16 bit).
11	Address field contains an extended address (64 bit).

IEEE 802.15.4 Media Access Control (MAC) Layer

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Frame Version field

The Frame Version field specifies the version number corresponding to the frame. This field shall be set to 0x00 to indicate a frame compatible with IEEE Std 802.15.4-2003 and 0x01 to indicate an IEEE 802.15.4 frame.

Source Addressing Mode field

If this field is equal to zero and the Frame Type field does not specify that this frame is an acknowledgment frame, the Destination Addressing Mode field shall be nonzero, implying that the frame has originated from the PAN coordinator with the PAN identifier as specified in the Destination PAN Identifier field.

IEEE 802.15.4 Media Access Control (MAC) Layer

The IEEE 802.15.4 MAC has four different frame types. These are the beacon frame, data frame, acknowledgment frame and MAC command frame

Beacon Frame Format:

Beacon frames : Used by a Coordinator

Octets:2	1	4 or 10	2	variable	variable	variable	2
Frame control	Beacon sequence number	Source address information	Superframe specification	GTS fields	Pending address fields	Beacon payload	Frame check sequence
MAC header			MAC payload				MAC footer

Bits: 0-3	4-7	8-11	12	13	14	15
Beacon order	Superframe order	Final CAP slot	Battery life extension	Reserved	PAN coordinator	Association permit

https://www.sharetechnote.com/html/IoT/LR_WPAN_802_15_4.html

IEEE 802.15.4 Media Access Control (MAC) Layer

Data frames : Used for all transfer of data

Octets:2	1	4 to 20	variable	2
Frame control	Data sequence number	Address information	Data payload	Frame check sequence
MAC header			MAC Payload	MAC footer

Acknowledgement frames : Used for confirming successful frame reception

Octets:2	1	2
Frame control	Data sequence number	Frame check sequence
MAC header		MAC footer

https://www.sharetechnote.com/html/IoT/LR_WPAN_802_15_4.html

IEEE 802.15.4 Media Access Control (MAC) Layer

MAC command frames : Used for handling all MAC peer entity control transfer

Octets:2	1	4 to 20	1	variable	2
Frame control	Data sequence number	Address information	Command type	Command payload	Frame check sequence
MAC header			MAC payload		MAC footer

Command Frame Types

- Association request
- Association response
- Disassociation notification
- Data request
- PAN ID conflict notification

https://www.sharetechnote.com/html/IoT/LR_WPAN_802_15_4.html

IEEE 802.15.4 MAC sublayer operational modes

The IEEE 802.15.4 MAC sublayer has two operational modes. They are

- Beacon-enabled mode
- Nonbeacon –enabled mode

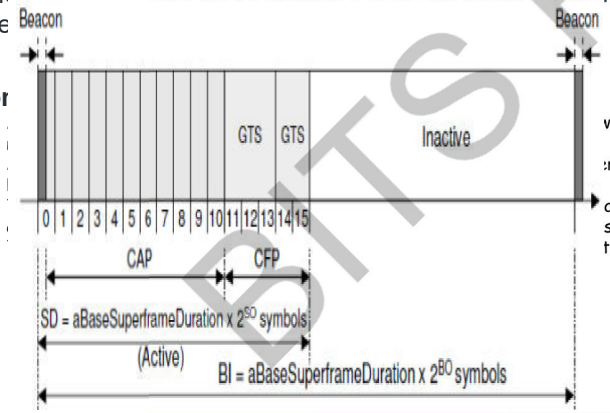
Beacon-enabled mode

- Beacon is a message with specific format that is used to synchronize the clocks of the nodes in the network.
- A coordinator has the option to transmit beacon signals to synchronize the devices attached to it.
- Beacons are periodically sent by the PAN or Coordinator to synchronize nodes that are associated with it, and to identify the PAN.
- Medium access is basically ruled by Slotted CSMA/CA.
- This mode also enables the allocation of contention free time slots, called Guaranteed Time Slots (GTSs) for nodes requiring guaranteed bandwidth.

IEEE 802.15.4 MAC sublayer operational modes

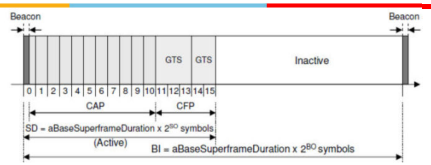
The IEEE 802.15.4 MAC sublayer has two operational modes.
The

Nor



vn as a
:riods
a beacon-
s often.
ts.

IEEE 802.15.4 MAC sublayer operational modes



Beacon:

The beacon frame is transmitted at the start of slot 0.
It contains the information on the addressing fields, the superframe specification, the GTS fields, the pending address fields and other PAN related.

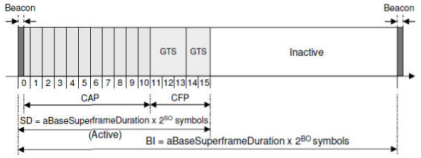
Contention Access Period (CAP):

The CAP starts immediately after the beacon frame and ends before the beginning of the CFP, if it exists. Otherwise, the CAP ends at the end of the active part of the superframe.

Contention Free Period (CFP):

In the contention-free method, the PAN coordinator dedicates a specific time slot to a particular device. This is called a guaranteed time slot (GTS)
A device with an allocated GTS will start transmitting during that GTS without using the CSMA-CA mechanism.

IEEE 802.15.4 MAC sublayer operational modes



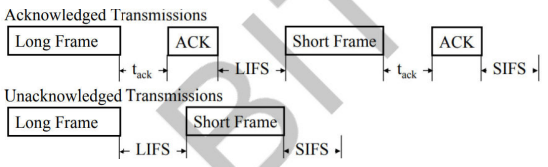
- The Beacon Interval (BI):
  - It defines the time between two consecutive beacon frames.
- The Superframe Duration (SD):
  - It defines the active portion in the BI, and is divided into 16 equally-sized time slots, during which frame transmissions are allowed

IEEE 802.15.4 CSMA-CA mechanism

- CSMA-CA mechanism for channel access Like most other protocols designed for wireless networks
- 802.15.4 uses CSMA-CA mechanism for channel access.
- Devices will use slotted or unslotted CSMA-CA depending whether the PAN is beacon-enabled or not, respectively.
- In slotted CSMA-CA channel access mechanism, the backoff period boundaries of every device in the PAN are aligned with the superframe slot boundaries of the PAN coordinator

IEEE 802.15.4 CSMA-CA mechanism

- **Beaconless Operation: Unslotted CSMA**
  - If coordinator does not send beacons, there are no slots
  - Acknowledgements if requested by the sender.
  - Short inter-frame spacing (SIFS) if previous transmission is shorter than a specified duration. Otherwise, Long inter-frame spacing (LIFS)



IEEE

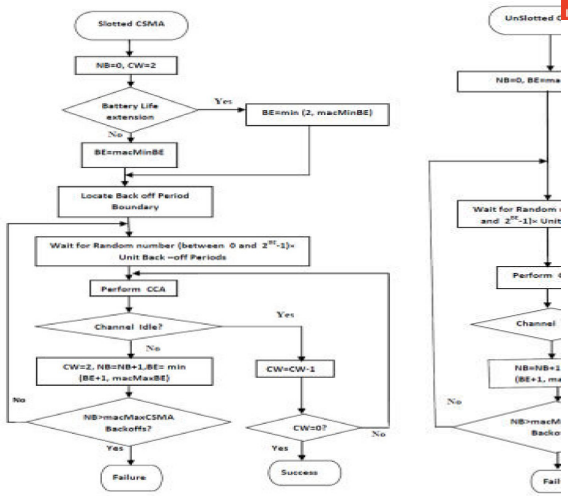


Figure 3.7: Slotted/Un-slotted CSMA-CA Algorithm [7]

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

Contact Session 3 and 4

innovate achieve lead

CH	List of Topics	Text
3-4	Wireless Personal Area Networks • Overview of Wireless Personal Area Network (WPAN) • WPAN Technologies and Protocols • 802.15.4 Network Architecture • 802.15.4 Network Components • Bluetooth Network Architecture • Bluetooth Network Components • WPAN Applications	Text-1

Wireless Personal Area Networks (WPAN) - Bluetooth

- Bluetooth is a wireless LAN technology.
- Designed to connect devices of different functions, such as telephones, Computers (desktop and laptop), cameras, printers when they are at a short distance from each other.
- A Bluetooth LAN is an ad hoc network
  - the network is formed spontaneously; the devices find each other and make a network called a piconet.
- Monitoring devices can communicate with sensor devices in a small health care center.
- Home security devices can use this technology to connect different sensors to the main security controller.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.

Wireless Personal Area Networks (WPAN) - Bluetooth

- Universal short-range wireless capability
- Uses 2.4-GHz band
- Available globally for unlicensed users
- Devices within 10 m can share up to 2.1 Mbps or 24 Mbps of capacity
- Supports open-ended list of applications
  - Data, audio, graphics, video
- Started as IEEE 802.15.1
  - New standards come from the Bluetooth Special Interest Group (Bluetooth SIG)
- Bluetooth 2.0, 2.1, 3.0, and 4.0

innovate achieve lead

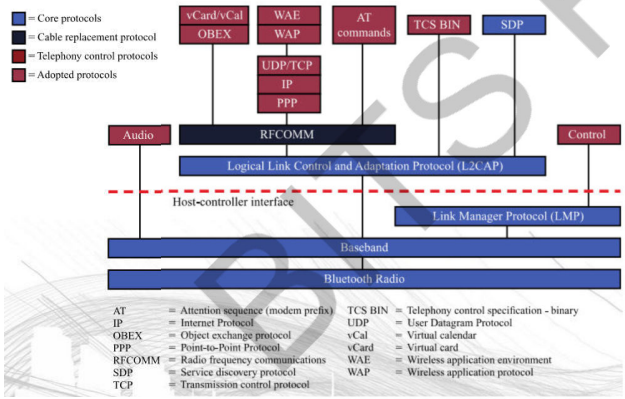
Bluetooth Application areas

- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range

USES OF BLUETOOTH

- Mobile handsets
- Voice handsets
- Stereo headsets and speakers
- PCs and tablets
- Human interface devices, such as mice and keyboards
- Wireless controllers for video game consoles
- Cars
- Machine-to-machine applications: credit-card readers, industrial automation, etc

BLUETOOTH PROTOCOL STACK



BLUETOOTH PROTOCOL STACK

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)
- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - WAE/WAP

innovate achieve lead

BLUETOOTH PROFILES

innovate achieve lead

- Over 40 different profiles are defined in Bluetooth documents
- – Only subsets of Bluetooth protocols are required
- – Reduces costs of specialized devices
- All Bluetooth nodes support the Generic Access Profile
- Profiles may depend on other profiles
- Example: File Transfer Profile
  - Transfer of directories, files, documents, images, and streaming media formats
  - Depends on the Generic Object File Exchange, Serial Port,and Generic Access Profiles.
  - Interfaces with L2CAP and RFCOMM protocols

BLUETOOTH Architecture

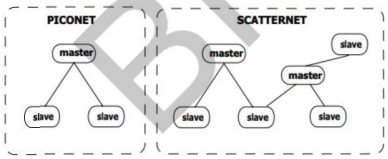
innovate achieve lead

- Over 40 different profiles are defined in Bluetooth documents
- – Only subsets of Bluetooth protocols are required
- – Reduces costs of specialized devices
- All Bluetooth nodes support the Generic Access Profile
- Profiles may depend on other profiles
- Example: File Transfer Profile
  - Transfer of directories, files, documents, images, and streaming media formats
  - Depends on the Generic Object File Exchange, Serial Port,and Generic Access Profiles.
  - Interfaces with L2CAP and RFCOMM protocols

BLUETOOTH Architecture

innovate achieve lead

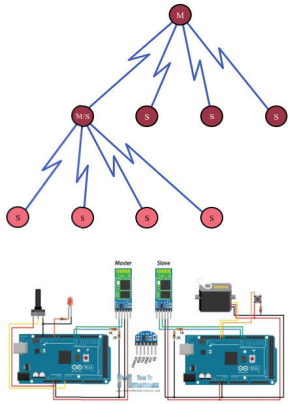
- PICONETS AND SCATTERNETS
- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
  - there can be more slaves in a parked state. Parked slaves are not active on the channel, but they are synchronized to the master of a piconet
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth



BLUETOOTH Architecture

innovate achieve lead

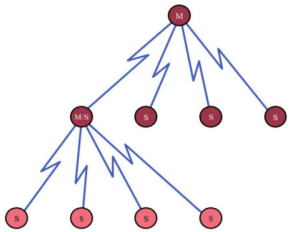
- Master/Slave relationship
- When Bluetooth devices connect to each other it's known as a master-slave relationship.
  - E.g. Connecting phone to wireless speaker
- One of the devices is the master and the other devices are slaves.
- The master transmits information to the slave and the slave listens for information from the master.
- The Bluetooth module working in slave mode can only be searched by the host.
- After the device is connected to the host, it can also send and receive data with the host device

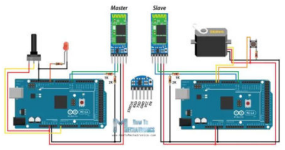


innovate achieve lead

BLUETOOTH Architecture

- Master/Slave relationship
- When Bluetooth devices connect to each other it's known as a master-slave relationship.
  - E.g. Connecting phone to wireless speaker
- One of the devices is the master and the other devices are slaves.
- The master transmits information to the slave and the slave listens for information from the master.
- The Bluetooth module working in slave mode can only be searched by the host.
- After the device is connected to the host, it can also send and receive data with the host device

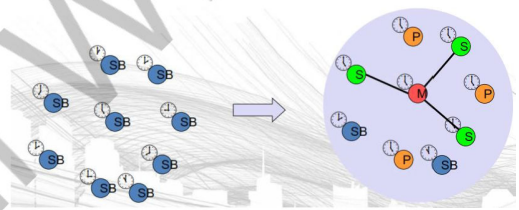




Bluetooth Architecture-Forming A Piconet

- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

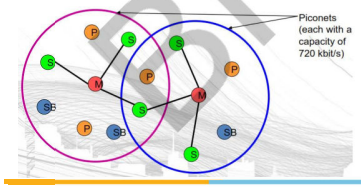
M=Master
S=Slave
P=Parked
SB=Standby



Bluetooth Architecture-Forming A Scatternet

- A scatter-net is formed when two or more piconets connect through a bridge node.
- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
  - Communication between piconets
- Devices jumping back and forth between the piconets

M=Master
S=Slave
P=Parked
SB=Standby

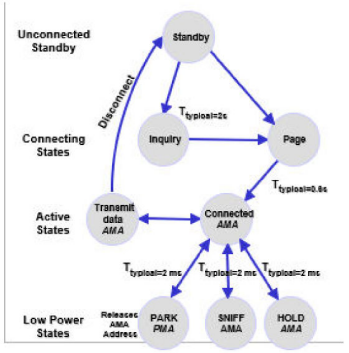


Bluetooth RF Specifications

- Specified for low cost, single chip implementation
- Noise floor margin for substrate noise and low current Low Noise Amplifier (LNA)
- Linearity set by near-far problem
- In-band image allows low-cost low IF
- TX-RX turn around time enables single synthesizer
- 2.4 ISM band chosen for global use and process capabilities

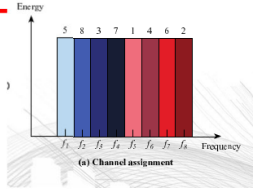
Functional Overview

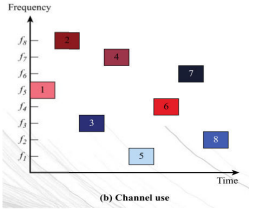
- Standby
  - Waiting to join a piconet
- Inquire
  - Ask about radios to connect to
- Page
  - Connect to a specific radio
- Connected
  - Actively on a piconet (master or slave)
- Park/Hold/Sniff
  - Low Power connected states

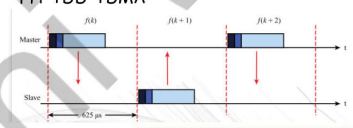


Frequency hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets.
- Total bandwidth divided into 1MHz physical channels.
- FH occurs by jumping from one channel to another in pseudorandom sequence.
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA

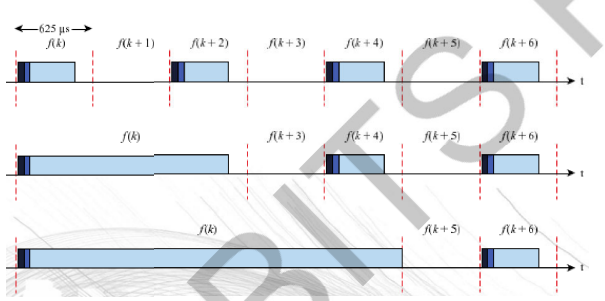






FREQUENCY-HOP TIME-DIVISION DUPLEX

Frequency hopping in Bluetooth



EXAMPLES OF MULTISLOT PACKET

Bluetooth Security Features

- Fast Frequency Hopping (79 channels)
- Low Transmit Power (range <= 10m)
- Authentication of remote device
  - Based on link key (128 Bit)
  - May be performed in both directions
- Encryption of payload data
  - Stream cipher algorithm (128 Bit)
  - Affects all traffic on a link
- Initialization
  - PIN entry by user

Bluetooth Protocol Stack

- The Bluetooth protocol stack defines the software layers that are used for communication on the top of the radio link.
- The top layer is the application layer.
- The middle layer comprises of the industry standard protocols.
- The lower layer consists the Bluetooth specific components.

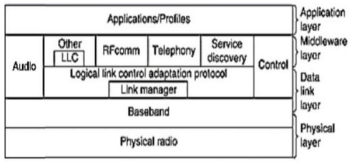


Fig. Bluetooth Protocol Stack

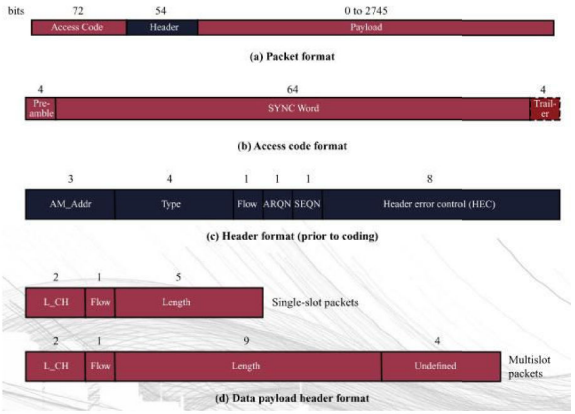
Bluetooth Protocol Stack

- It **transfers the data bits from the slave to the master** and vice-versa
- With range of **10m, it is a low per system.**
- **FHSS and Gaussian frequency shift keying (GFSK)** modulation are used in the Bluetooth transceivers.
- The Bluetooth networks can **support speech and data channels.**
- **Packet switching** allows the Bluetooth devices to send multiple data packets on the same path.

Physical links between Master and Slave

- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist
- Extended Synchronous connection oriented (eSCO)
  - Reserves slots just like SCO
  - But these can be asymmetric
  - Retransmissions are supported

Physical links between Master and Slave



innovate achieve lead

Bluetooth Packet Fields

innovate achieve lead

- Access code – used for timing synchronization, offset compensation, paging, and inquiry.
- Header – used to identify packet type and carry protocol control information.
- Payload – contains user voice or data and payload header, if present

(a) Packet format

Types of Access Codes

innovate achieve lead

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes.

Packet Header Fields

innovate achieve lead

- AM_ADDR – contains "active mode" address of one of the slaves.
- Type – identifies type of packet
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

(c) Header format (prior to coding)

Packet Header Fields

innovate achieve lead

- AM_ADDR: temporary address assigned to active members of the piconet, used on all packets in both directions sent between the master and the addressed slave
- TYPE: type of packet. There are 12 types of packets for each SCO and ACL physical links, and four types of common control packets for both
- FLOW: It is used for flow control. It is asserted by slave when its buffer is full and cannot receive any more data.
- ARQN: It is used to piggy back an acknowledgement onto a frame.
- SEQN: It contains sequence number for packet ordering.
- HEC: header error check for header integrity.

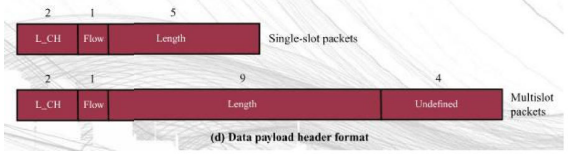
(c) Header format (prior to coding)

innovate achieve lead

Payload Format

innovate achieve lead

- Payload header
  - L_CH field – identifies logical channel
  - Flow field – used to control flow at L2CAP level
  - Length field – number of bytes of data
- Payload body – contains user data
- CRC – 16-bit CRC code



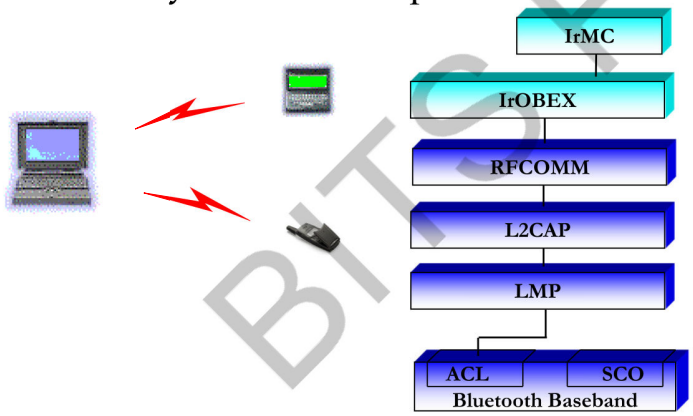
Synchronization

User benefits

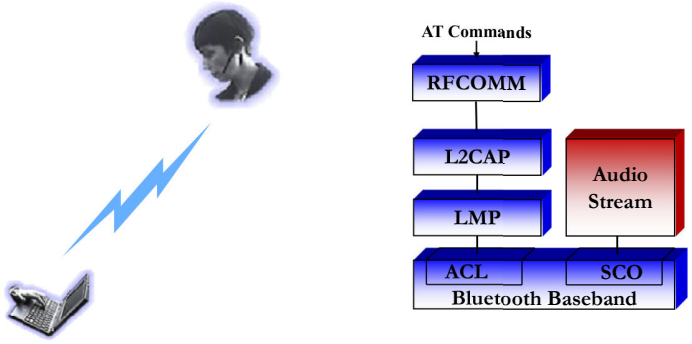
- **Proximity synchronization**
- **Easily maintained database**
- **Common information database**

Sharing Common Data…

Synchronization profile

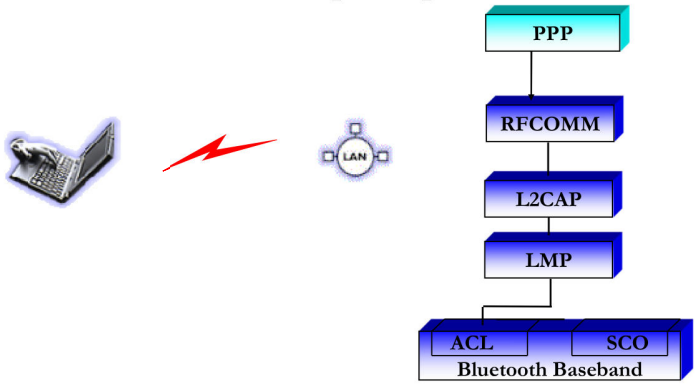


Headset profile



doc.: IEEE 802.15-99/069r0{802.11-99/220}

LAN access point profile



Advantages of Bluetooth

- Inexpensive: The technology of Bluetooth is cheap for companies to implement.
- Automatic: Bluetooth doesn't have you set up a connection or push any buttons.
- Low interference: Bluetooth devices almost always avoid interference from other wireless devices.
- Low energy consumption: As a result of Bluetooth using low power signals, the technology requires very little energy and will use less battery or electrical power as a result.
- Sharing voice and data: The standard for Bluetooth will allow compatible devices to share data and voice communications.

Advantages of Bluetooth

- Instant PAN (Personal Area Network): Can connect up to seven Bluetooth devices to each other within a range of up to 30 feet, forming a piconet or PAN
- Upgradeable: Upgradeable is the standard for Bluetooth. There are newer versions of Bluetooth in the works, which offer many new advantages and backward compatible with older versions.

Disadvantages of Bluetooth

- Disadvantages:
- The only real downsides are the data rate and security.
- Infrared can have data rates of up to 4 MBps, which provides very fast rates for data transfer, while Bluetooth only offers 1 MBps.

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

Wireless and Mobile Networks

innovate achieve lead

Background:

wireless (mobile) phone subscribers now exceeds # wired phone subscribers!

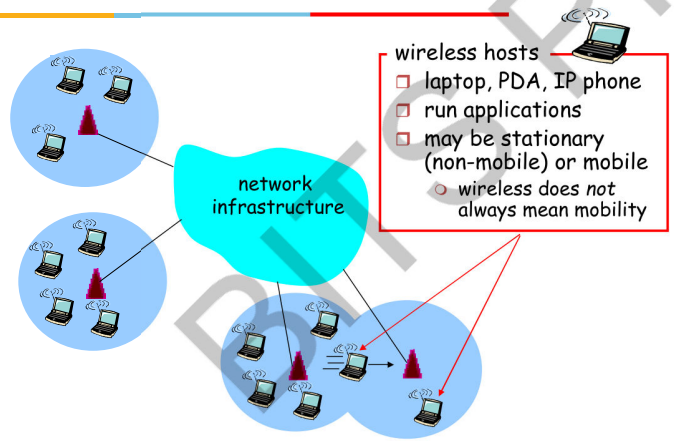
computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access

two important (but different) challenges

- *wireless:* communication over wireless link
- *mobility:* handling the mobile user who changes point of attachment to network

Elements of a wireless network

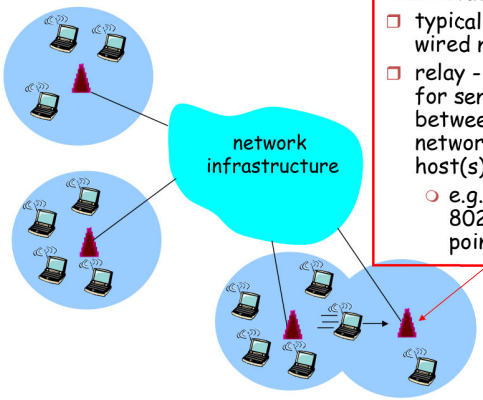
innovate achieve lead



wireless hosts
- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

Elements of a wireless network

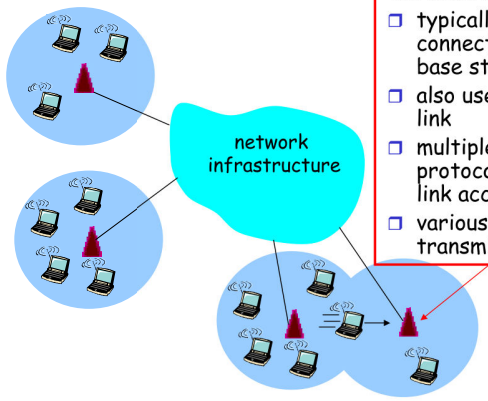
innovate achieve lead



base station
- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

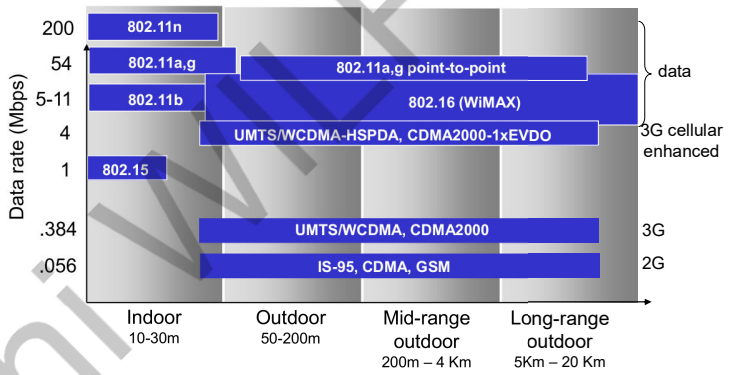
innovate achieve lead

Elements of a wireless network

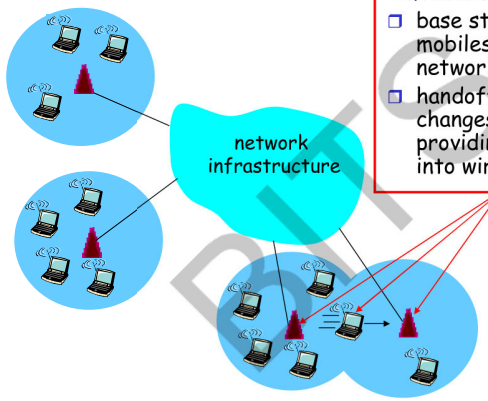


wireless link
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless link standards

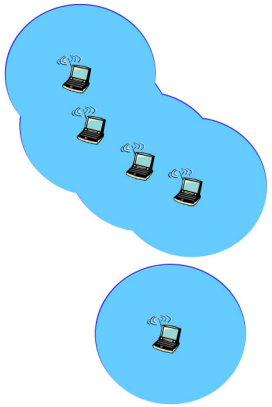


Elements of a wireless network



infrastructure mode
- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode
- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless Link Characteristics (1)

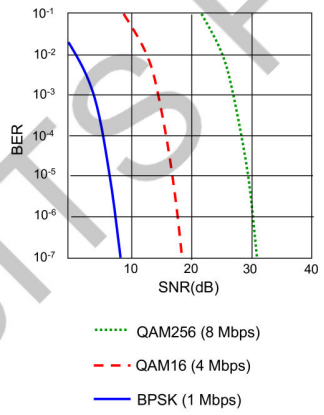
Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

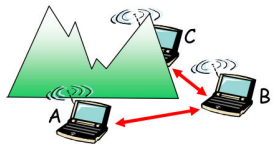
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



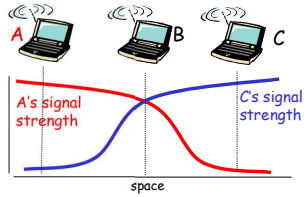
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem
- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B



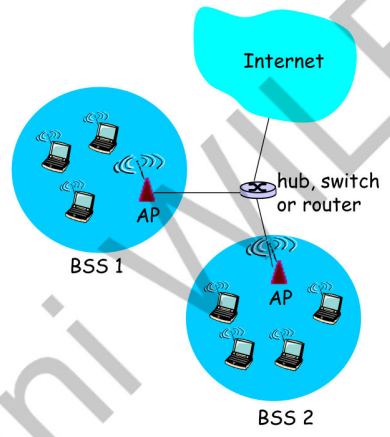
Signal attenuation:
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

802.11 LAN architecture

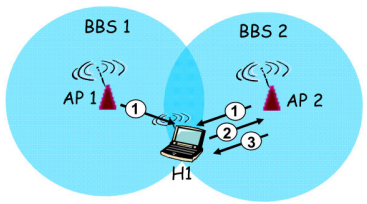


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

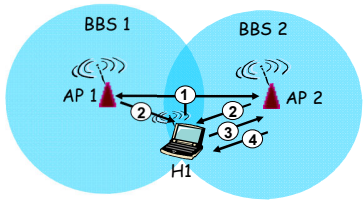
802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication [Chapter 8]
  - will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning



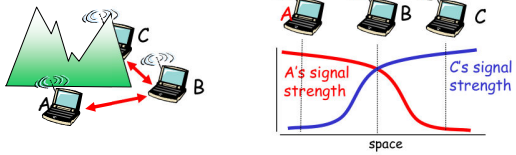
Passive Scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: H1 to selected AP



Active Scanning:
(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: H1 to selected AP

IEEE 802.11: multiple access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)



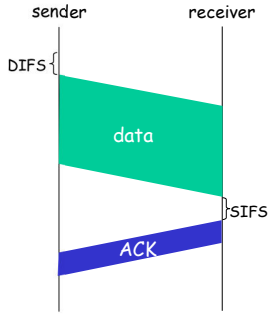
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
  transmit entire frame (no CD)
2 if sense channel busy then
  start random backoff time
  timer counts down while channel idle
  transmit when timer expires
  if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)



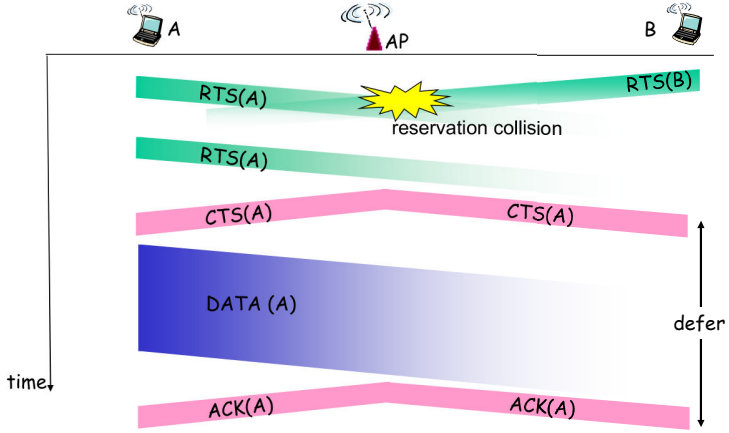
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

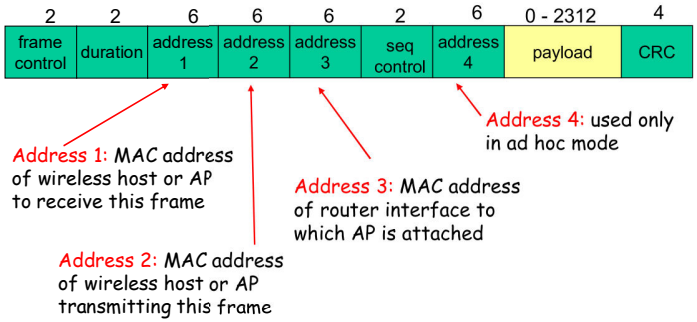
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

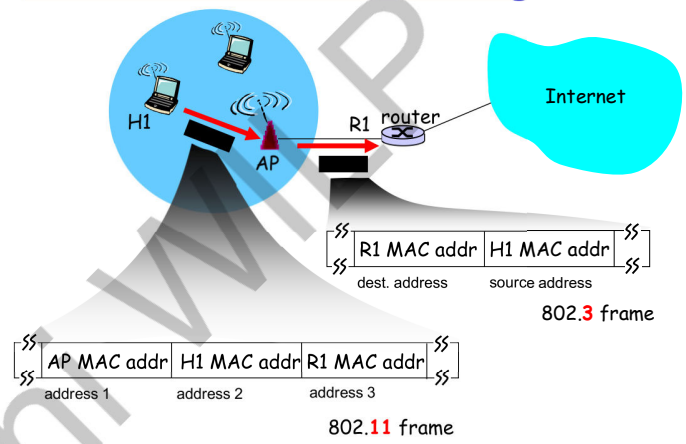
Collision Avoidance: RTS-CTS exchange



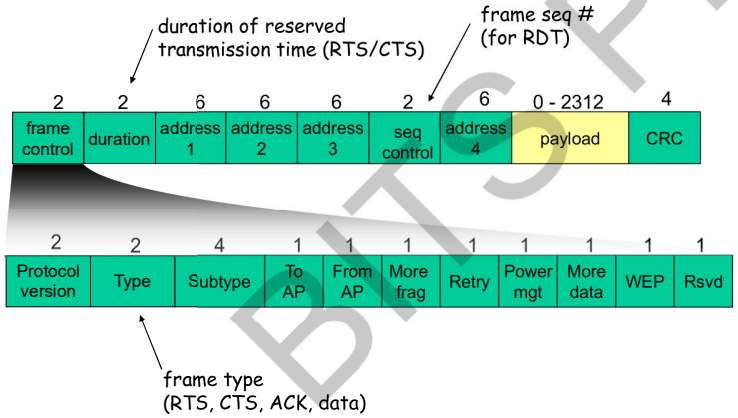
802.11 frame: addressing



802.11 frame: addressing

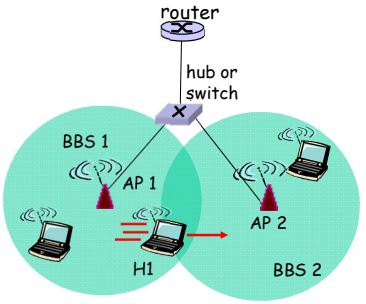


802.11 frame: more



802.11: mobility within same subnet

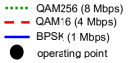
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1

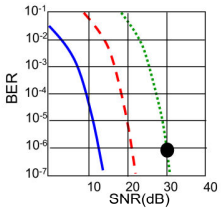


802.11: advanced capabilities

Rate Adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies





1. SNR decreases, BER increase as node moves away from base station

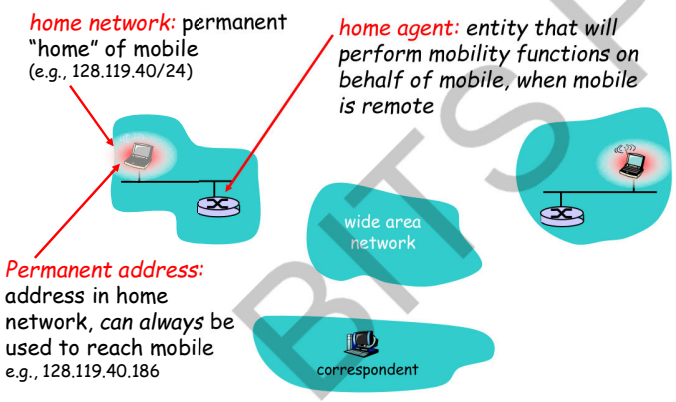
2. When BER becomes too high, switch to lower transmission rate but with lower BER

802.11: advanced capabilities

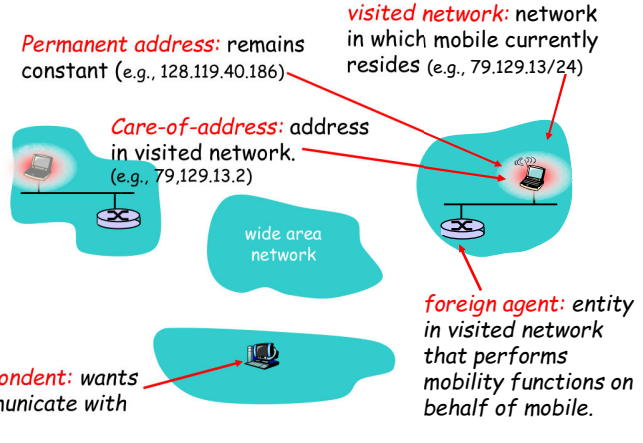
Power Management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

Mobility: Vocabulary



Mobility: more vocabulary



Mobility: approaches

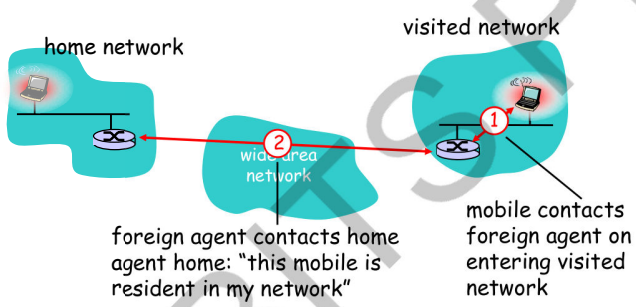
- *Let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *Let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: approaches

- *Let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

not scalable to millions of mobiles

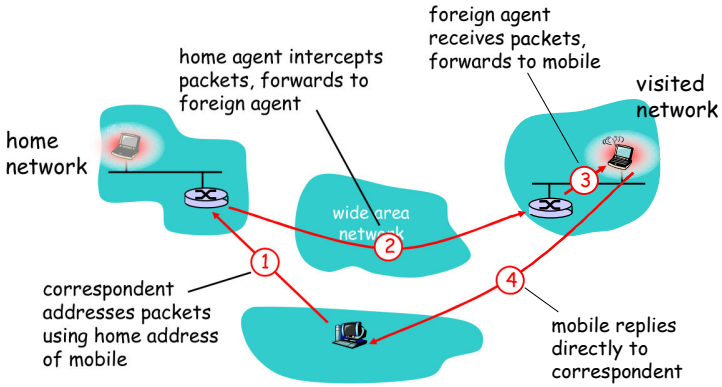
Mobility: registration



End result:

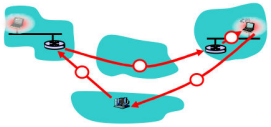
- Foreign agent knows about mobile
- Home agent knows location of mobile

Mobility via Indirect Routing



Indirect Routing: comments

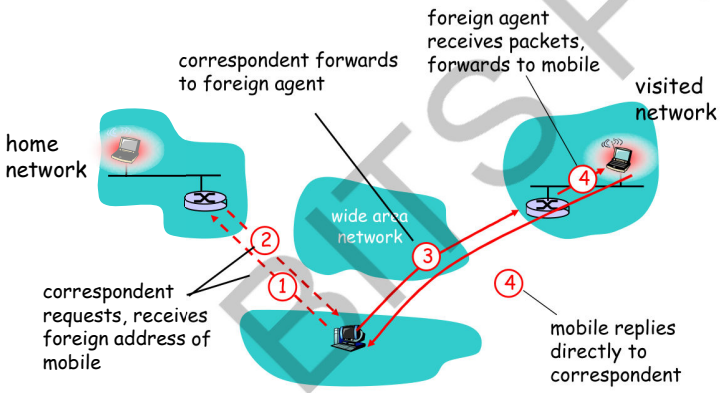
- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



Indirect Routing: moving between networks

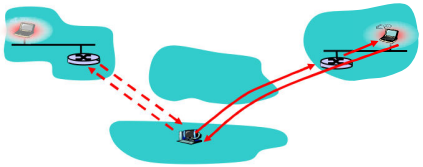
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*

Mobility via Direct Routing



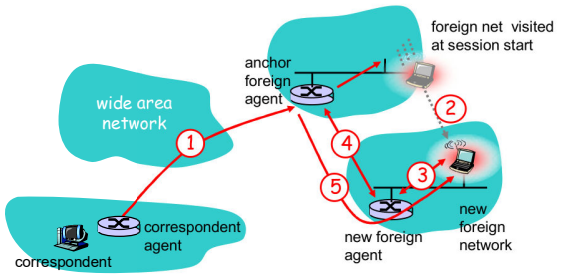
Mobility via Direct Routing: comments

- overcome triangle routing problem
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Wireless and Mobile Networks

innovate achieve lead

Background:

wireless (mobile) phone subscribers now exceeds # wired phone subscribers!

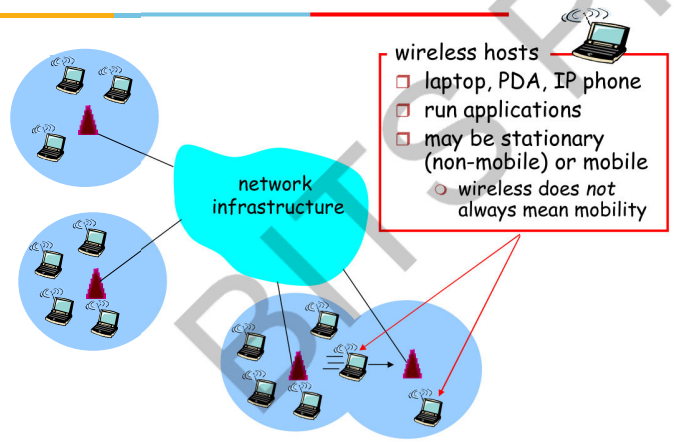
computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access

two important (but different) challenges

- *wireless:* communication over wireless link
- *mobility:* handling the mobile user who changes point of attachment to network

Elements of a wireless network

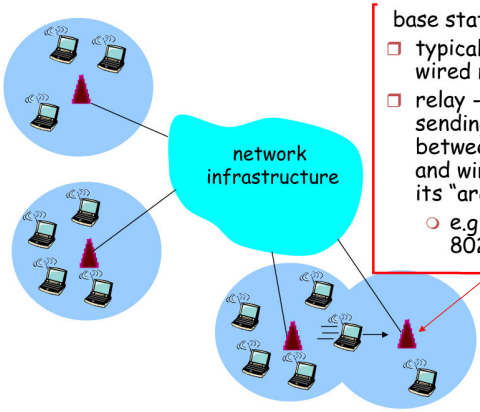
innovate achieve lead



wireless hosts
- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

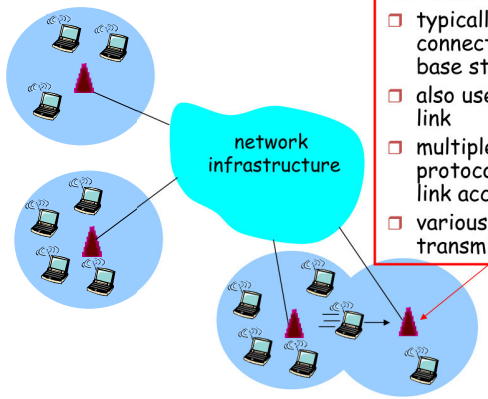
Elements of a wireless network

innovate achieve lead



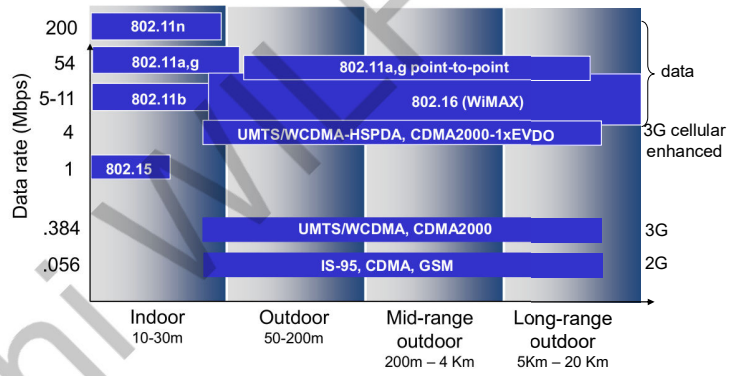
base station
- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

Elements of a wireless network

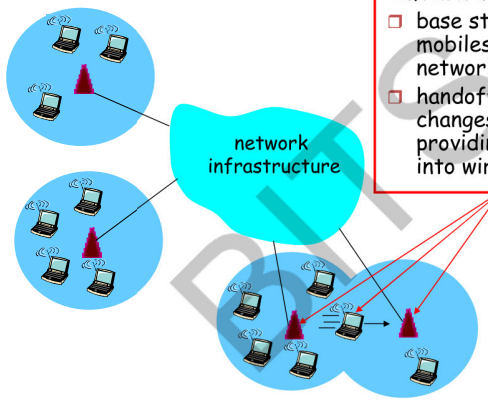


wireless link
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless link standards

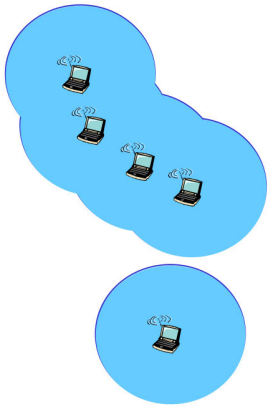


Elements of a wireless network



infrastructure mode
- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode
- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

innovate achieve lead

Wireless network taxonomy

innovate achieve lead

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless Link Characteristics (1)

innovate achieve lead

Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

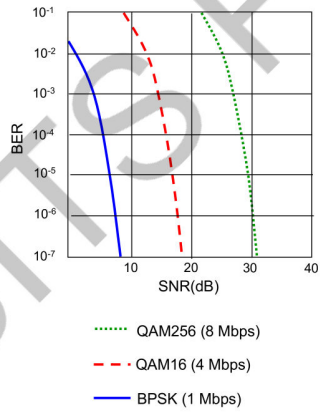
…. make communication across (even a point to point) wireless link much more "difficult"

Wireless Link Characteristics (2)

innovate achieve lead

SNR: signal-to-noise ratio
- –larger SNR – easier to extract signal from noise (a "good thing")

SNR versus BER tradeoffs
- –*given physical layer:* increase power -> increase SNR->decrease BER
- –*given SNR:* choose physical layer that meets BER requirement, giving highest thruput
  - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



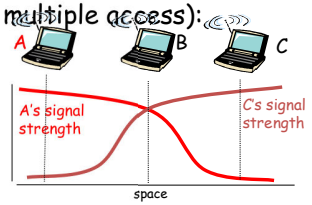
Wireless network characteristics

innovate achieve lead

Multiple wireless senders and receivers create additional problems (beyond multiple access):

Hidden terminal problem
- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B



Signal attenuation:
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

innovate achieve lead

IEEE 802.11 Wireless LAN

innovate achieve lead

802.11b
- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

802.11a
- 5-6 GHz range
- up to 54 Mbps

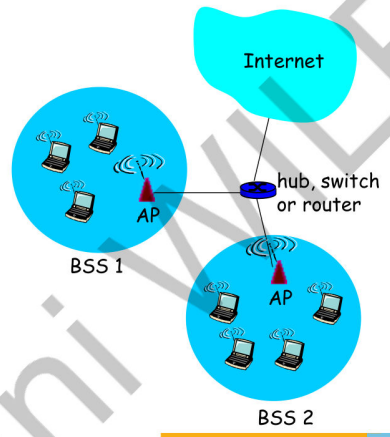
802.11g
- 2.4-5 GHz range
- up to 54 Mbps

802.11n: multiple antennae
- 2.4-5 GHz range
- up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

802.11 LAN architecture

innovate achieve lead



- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

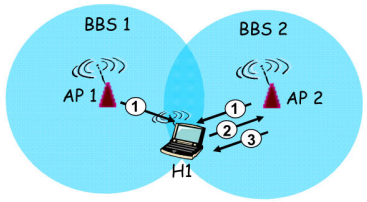
innovate achieve lead

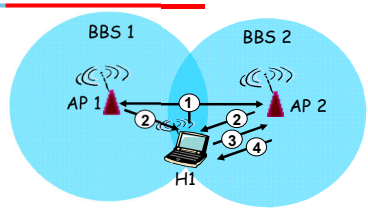
802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
- AP admin chooses frequency for AP
- interference possible: channel can be same as that chosen by neighboring AP!

host: must *associate* with an AP
- scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
- selects AP to associate with
- may perform authentication [Chapter 8]
- will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning

innovate achieve lead





Passive Scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: H1 to selected AP

Active Scanning:
(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: H1 to selected AP

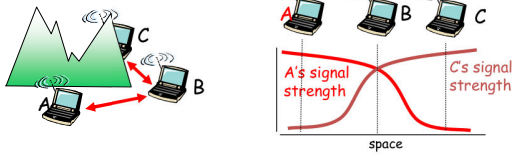
innovate achieve lead

IEEE 802.11: multiple access

avoid collisions: 2+ nodes transmitting at same time

802.11: CSMA - sense before transmitting
- don't collide with ongoing transmission by other node

802.11: *no* collision detection!
- difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
- can't sense all collisions in any case: hidden terminal, fading
- goal: *avoid collisions:* CSMA/C(ollision)A(voidance)



IEEE 802.11 MAC Protocol: CSMA/CA

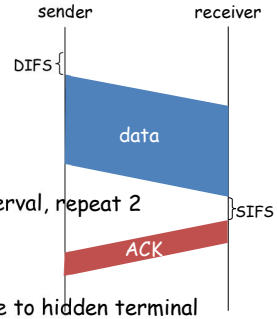
802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)



Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

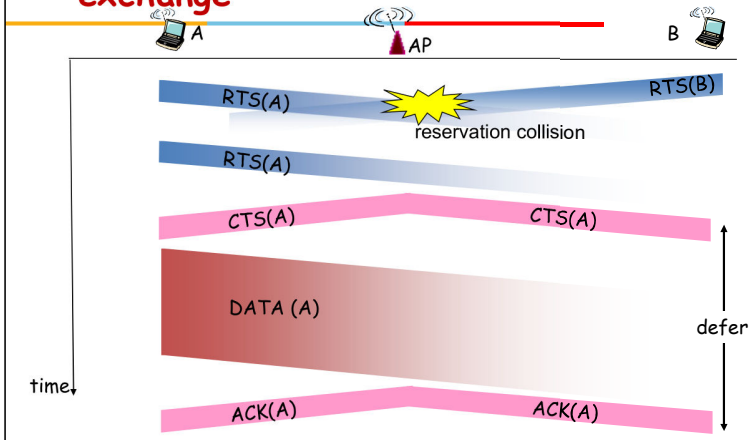
sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
- RTSs may still collide with each other (but they're short)

BS broadcasts clear-to-send CTS in response to RTS

CTS heard by all nodes
- sender transmits data frame
- other stations defer transmissions

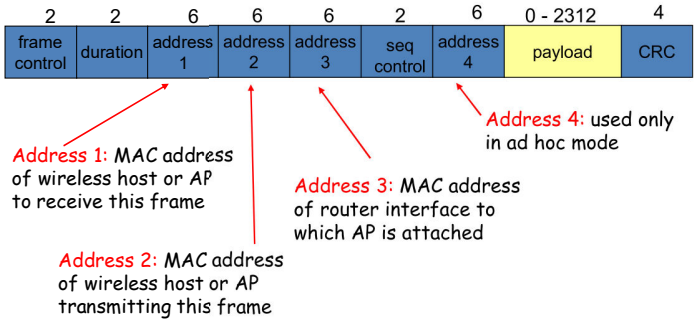
avoid data frame collisions completely using small reservation packets!

Collision Avoidance: RTS-CTS exchange

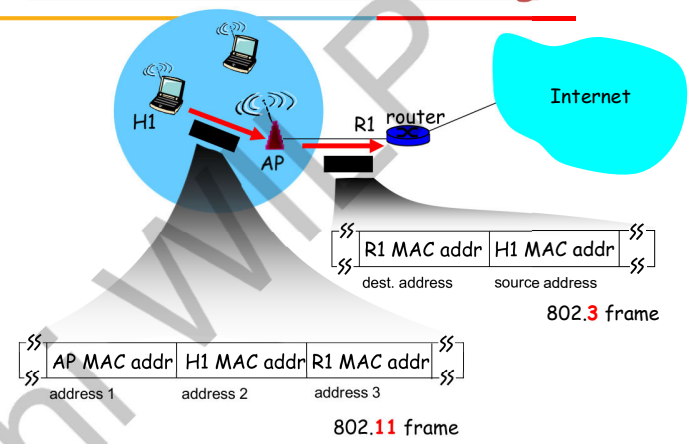


innovate achieve lead

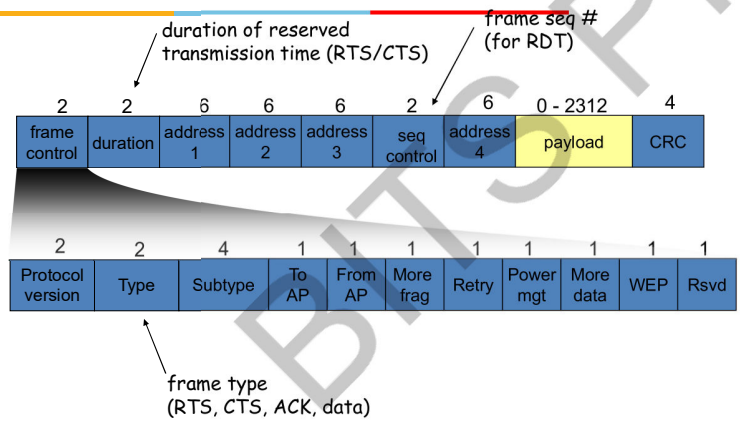
802.11 frame: addressing



802.11 frame: addressing



802.11 frame: more

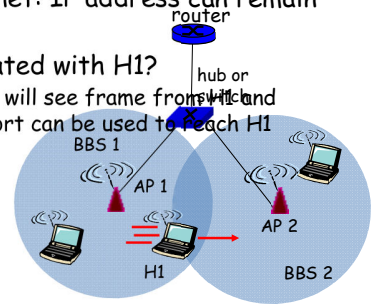


802.11: mobility within same subnet

H1 remains in same IP subnet: IP address can remain same

switch: which AP is associated with H1?

- self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1

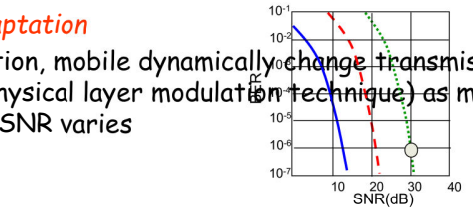


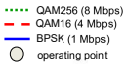
innovate achieve lead

802.11: advanced capabilities

Rate Adaptation

base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies





1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

802.11: advanced capabilities

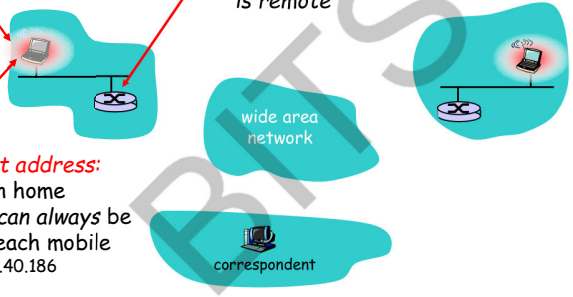
Power Management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

Mobility: Vocabulary

home network: permanent "home" of mobile (e.g., 128.119.40/24)

home agent: *entity that will perform mobility functions on behalf of mobile, when mobile is remote*



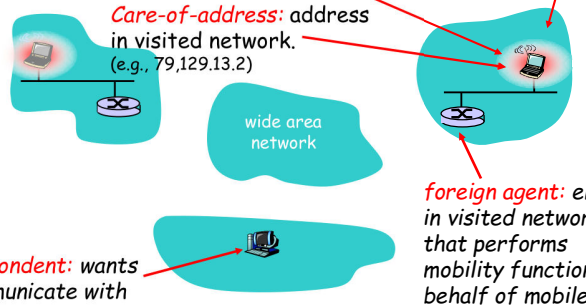
Permanent address: address in home network, *can always* be used to reach mobile e.g., 128.119.40.186

Mobility: more vocabulary

Permanent address: remains constant (e.g., 128.119.40.186)

visited network: network in which mobile currently resides (e.g., 79.129.13/24)

Care-of-address: address in visited network. (e.g., 79,129.13.2)



foreign agent: *entity in visited network that performs mobility functions on behalf of mobile.*

correspondent: *wants to communicate with mobile*

innovate achieve lead

Mobility: approaches

Let routing handle it: routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.

- routing tables indicate where each mobile located
- no changes to end-systems

Let end-systems handle it:

- *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
- *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: approaches

Let routing handle it: routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.

- routing tables indicate where each mobile located
- no changes to end-systems

not scalable to millions of mobiles

let end-systems handle it:

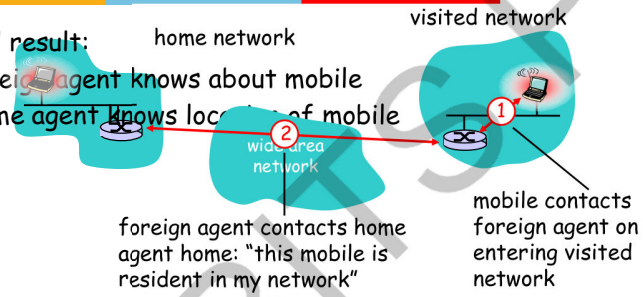
- *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
- *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: registration

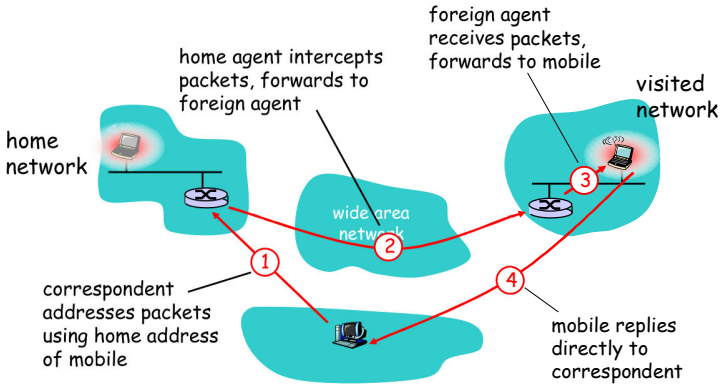
End result:

Foreign agent knows about mobile

Home agent knows location of mobile



Mobility via Indirect Routing



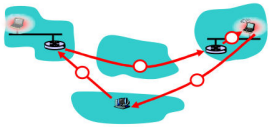
innovate achieve lead

Indirect Routing: comments

Mobile uses two addresses:
- permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
- care-of-address: used by home agent to forward datagrams to mobile

foreign agent functions may be done by mobile itself

triangle routing: correspondent-home-network-mobile
- inefficient when correspondent, mobile are in same network

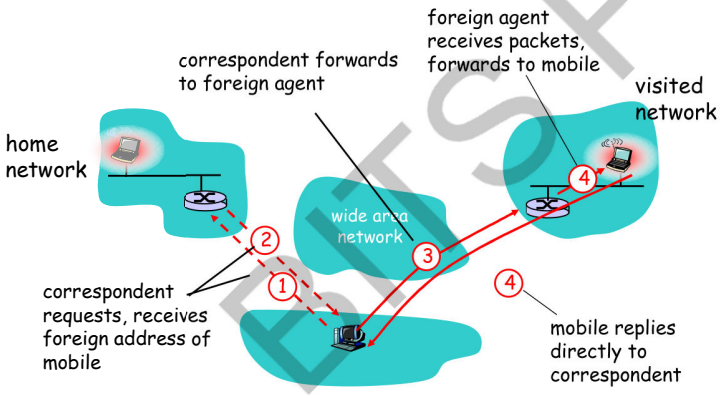


Indirect Routing: moving between networks

suppose mobile user moves to another network
- registers with new foreign agent
- new foreign agent registers with home agent
- home agent update care-of-address for mobile
- packets continue to be forwarded to mobile (but with new care-of-address)

mobility, changing foreign networks transparent: *on going connections can be maintained!*

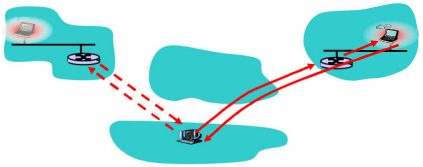
Mobility via Direct Routing



Mobility via Direct Routing: comments

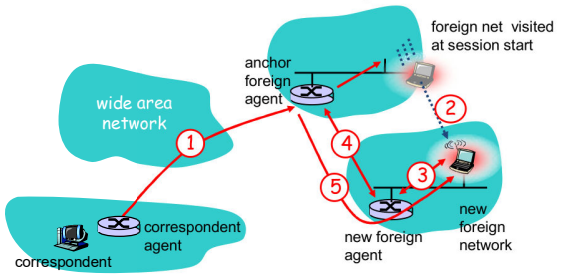
overcome triangle routing problem

non-transparent to correspondent: correspondent must get care-of-address from home agent
- what if mobile changes visited network?



Accommodating mobility with direct routing

anchor foreign agent: FA in first visited network
data always routed first to anchor FA
when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

WIRELESS CELLULAR and LTE 4G BROADBAND (17EC81)

Module - 3

Overview and Channel Structure of LTE

Module - 3

- **Overview and Channel Structure of LTE:**
- Introduction to LTE, Channel Structure of LTE, Downlink OFDMA Radio Resource, Uplink SC-FDMA Radio Resource (Sec 6.1 – 6.4 of Text).
- **Downlink Transport Channel Processing:**
- Overview, Downlink shared channels, Downlink Control Channels, Broadcast channels, Multicast channels, Downlink physical channels, H-ARQ on Downlink (Sec 7.1 – 7.7 of Text).

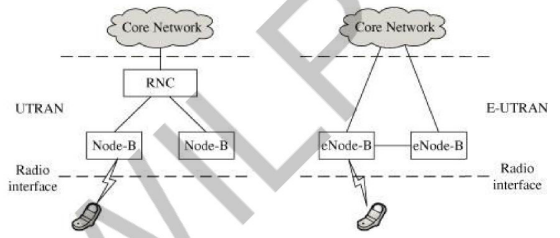
Introduction to LTE (4G)

- MT- Mobile Terminal
- BS-Base Station
- 3GPP-3rd Generation Partnership Project
- RAN- Radio Access Network
- CN-Core Network
- LTE-Long-Term Evolution
- UTRA-UMTS Terrestrial Radio Access
- EPC-Evolved Packet Core
- E-UTRA-Evolved UMTS Terrestrial Radio Access
- E-UTRAN-Evolved UMTS Terrestrial Radio Access Network
- eNode-B - evolved Node-B
- HSUPA-High-Speed Uplink Packet Access
- HSDPA-High-Speed Downlink Packet Access

Introduction to LTE (4G)

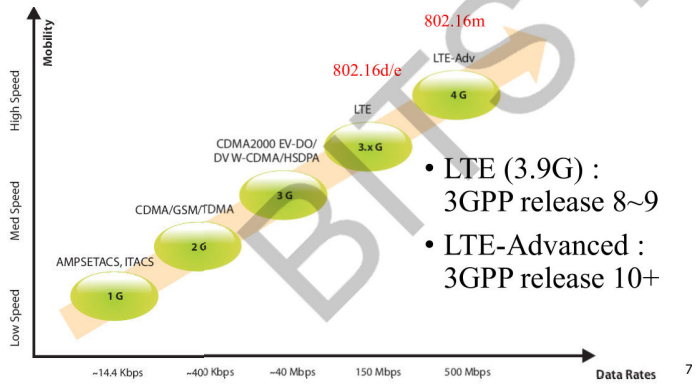
- LTE stands for **Long Term Evolution,** started as a project in 2004 by telecommunication body 3GPP (Third Generation Partnership Project)
- Successor of UMTS (3G) and GSM (2G)
- The main goal of LTE is to provide a high data rate, low latency and packet optimized radio access technology.
- Network architecture has been designed with the goal to support **packet-switched traffic** with seamless **mobility** and great QoS.

Introduction to LTE (4G)



Radio interface architectures of UTRAN and E-UTRAN

Evolution of Radio Access Technologies



- LTE (3.9G) : 3GPP release 8~9
- LTE-Advanced : 3GPP release 10+

Introduction to LTE (4G)

- **Facts about LTE**
  - LTE is the **successor technology** not only of UMTS but also of CDMA 2000.
  - It will bring up to 50 times performance improvement and better spectral efficiency
  - It was introduced to get higher data rates, 300Mbps peak downlink and 75 Mbps peak uplink
  - Ideal technology to support **high date rates** for the services such as VOIP, streaming multimedia, videoconferencing or even a high-speed cellular modem.
  - All LTE devices have to support (MIMO) Multiple Input Multiple Output transmissions.
  - Quality of Service (QoS) mechanism have been standardized on all interfaces.
  - Works with GSM/EDGE/UMTS systems utilizing existing 2G and 3G spectrum and new spectrum