Unit-3
WIRELESS NETWORKS

- Apart from transmitting the information over the air, wireless networks are very much like wired networks.
- A wireless network consists of several components that support communications using radio or light waves propagating through an air medium.

WLN and components

- **Wireless Networks Includes:--**

❖ Computer Devices,

❖ Base Stations

❖ Wireless Infrastructure

Computer devices

- Referred to as clients, operate on a wireless network.
- Specifically designed for users, whereas some computer devices are end systems.
- These devices generally have small screens, limited keyboards, and batteries.

- Some devices, such as a wireless bar code scanner, operate only on a wireless network.
- The operating system runs software needed to realize the wireless network application.
- ***NICs*** provides the interface between the computer device and the wireless

- Air also provides a medium for the propagation of wireless communications signals, which is the heart of wireless networking.
- The quality of transmission, however, depends on the air (Rain, snow and smoke etc.)

Wireless Network Infrastructures

- The infrastructure of a wireless network interconnects wireless users and end systems.
- The infrastructure might consist of ***base stations***, access controllers and a distribution system.
- These components enhance wireless communications and fulfill important functions necessary for specific applications.

Base Stations

- The base station is a common infrastructure component that interfaces the wireless communications signals traveling through the air medium to a wired network—often referred to as a **distribution system.**
- A base station often contains a wireless NIC that implements the same technology in operation by the user's wireless NIC.

- An ***access point***, for instance, represents a generic base station for a wireless LAN.
- **Residential gateways** and **routers** are more advanced forms of base stations that enable additional network functions.

- base station might support point-to-point or point-to-multipoint communications.
- Point-to-point systems enable communications signals to flow from one particular base station or computer device directly to another one.
- point-to-multipoint functionality enables a base station to communicate with more than one wireless computer device or base station.

Wireless Channels

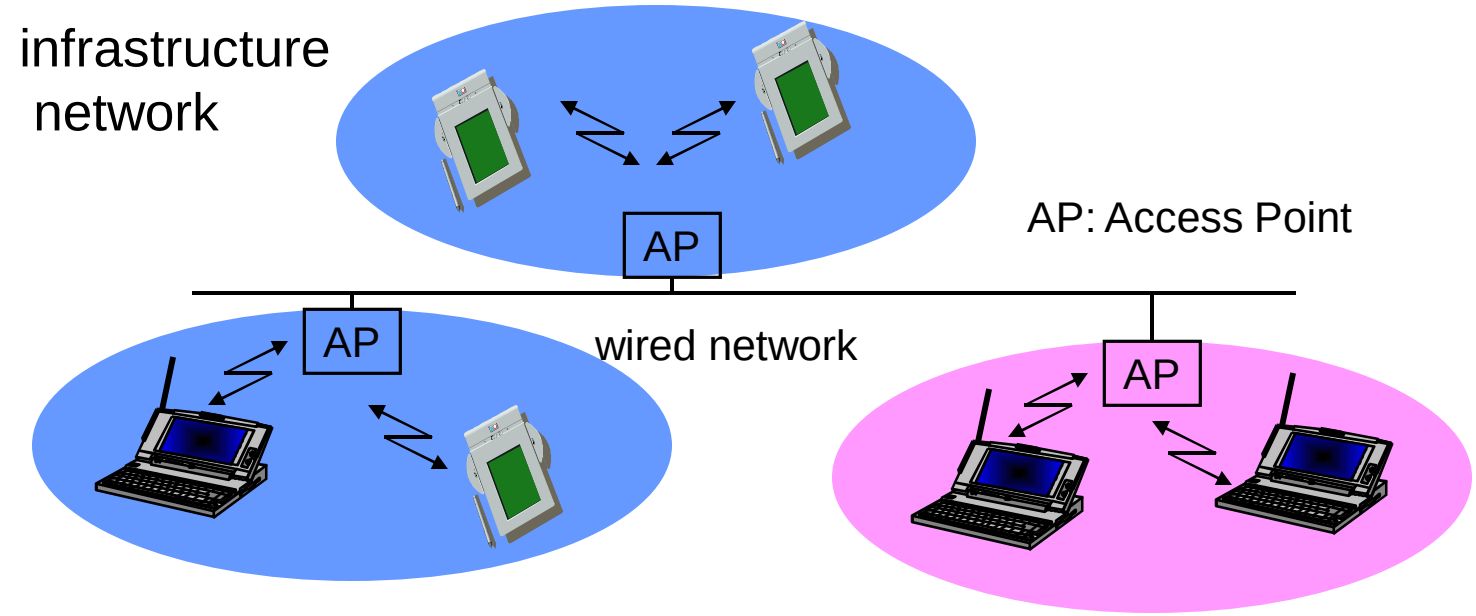
- Wired links →*electric signals*
- wireless links → *electromagnetic waves*
    - *Radio Transmission*
    - *Infrared Transmission*

Radio

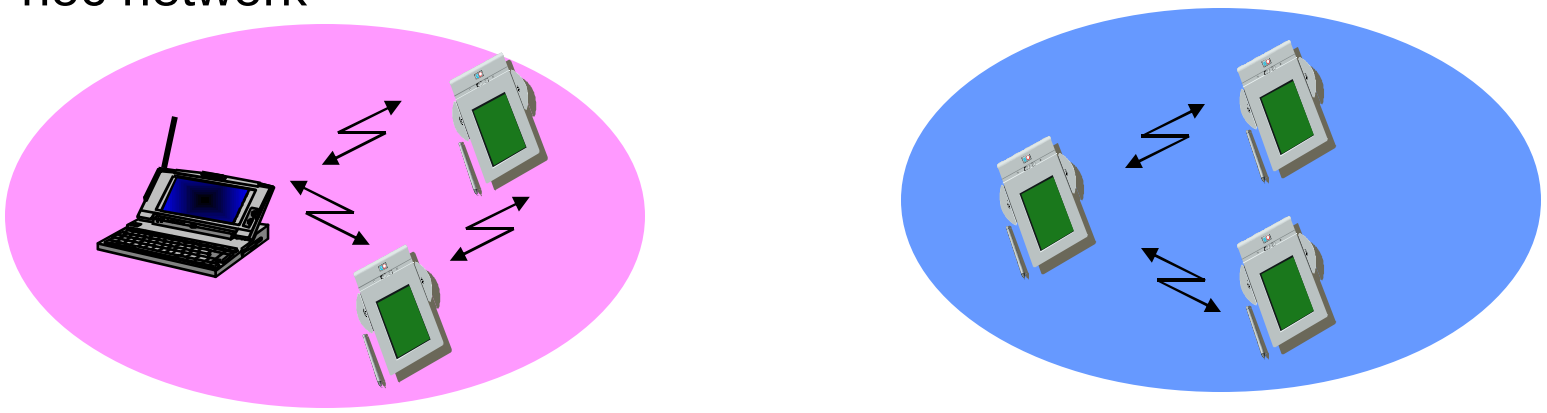
- Typically using the license free
- ISM band at 2.4 GHz
- Experience from wireless WAN
- Mobile phones can be used
- Coverage of larger areas possible
- Radio can penetrate walls, furniture etc.
- very limited license free frequency bands
- Shielding more difficult,
- Interference with other electrical devices

- Uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)
- Simple, cheap, available in many mobile devices
- No licenses needed
- Simple shielding possible
- Interference by sunlight, heat sources etc.
- Many things shield or absorb IR light
- low bandwidth
- Example: IrDA (Infrared Data Association) interface available everywhere

Infrastructure and Ad-hoc networks



ad-hoc network



IEEE 802.11
Wireless LAN

- A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier.
- The link with the users is wireless, to give a network connection to all users in a building or campus.

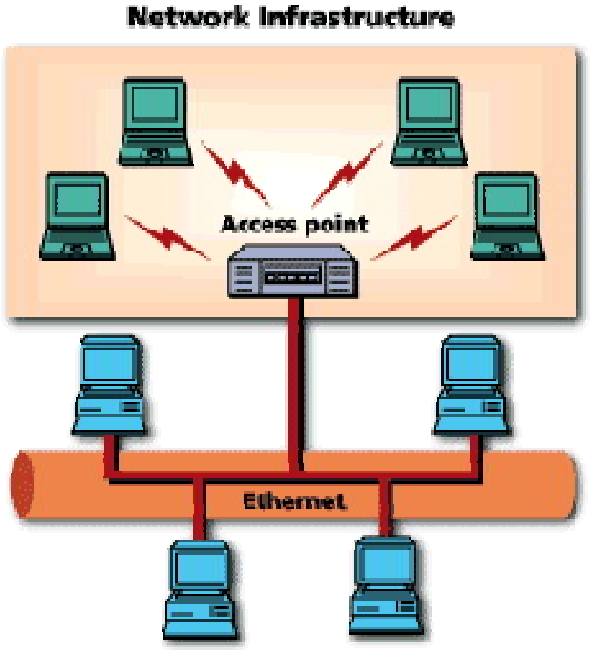
Wireless LANs: Characteristics

- **Types**
  - **Infrastructure based**
  - **Ad-hoc**
- **Advantages**
  - **Flexible deployment**
  - **Minimal wiring difficulties**
  - **More robust against disasters (earthquake etc)**
  - **Historic buildings, conferences, trade shows,...**
- **Disadvantages**
  - **Low bandwidth compared to wired networks (1-10 Mbit/s)**
  - **Proprietary solutions**
  - **Need to follow wireless spectrum regulations**

Common Topologies

The wireless LAN connects to a wired LAN

- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



Common Topologies

Complete Wireless Networks

- The physical size of the network is determined by the maximum reliable propagation range of the radio signals.
- Referred to as **ad hoc** networks
- Are self-organizing networks without any centralized control
- Suited for temporary situations such as meetings and conferences.

How do wireless LANs work?

Wireless LANs operate in almost the same way as wired LANs, using the same networking protocols and supporting the most of the same applications.

Components/Architecture

- Station (STA) - **Mobile node**
- Access Point (AP) - **Stations are connected to access points.**
- Basic Service Set (BSS) - **Stations and the AP with in the same radio coverage form a BSS**.
- Extended Service Set (ESS) - **Several BSSs connected through APs form an ESS.**

Design Goals

- Global, seamless operation
- Low power consumption for battery use
- No special permissions or licenses required
- Robust transmission technology
- Simplified spontaneous cooperation at meetings
- Easy to use for everyone, simple management
- Interoperable with wired networks
- Security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- Transparency concerning applications and higher layer protocols, but also location awareness if necessary

Characteristics

- Very flexible (economical to scale)
- Ad-hoc networks without planning possible
- (Almost) no wiring difficulties (e.g. historic buildings, firewalls)
- More robust against disasters or users pulling a plug
- Low bandwidth compared to wired networks (10 vs. 100 Mbit/s) - Many proprietary solutions, especially for higher bit-rates, standards take their time
- Products have to follow many national restrictions if working wireless, it takes a long time to establish global solutions
- Security
- Economy

Architecture of an infrastructure network

- STA-Terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS) - group of stations using the same radio frequency
- Access Point - station integrated into the wireless LAN and the distribution system
- Portal - bridge to other (wired) networks
- Distribution System - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

Directed communication within a limited range

- Station (STA): terminal with access mechanisms to the wireless medium
- Basic Service Set (BSS): group of stations using the same radio frequency
- You may use SDM or FDM to establish several BSS

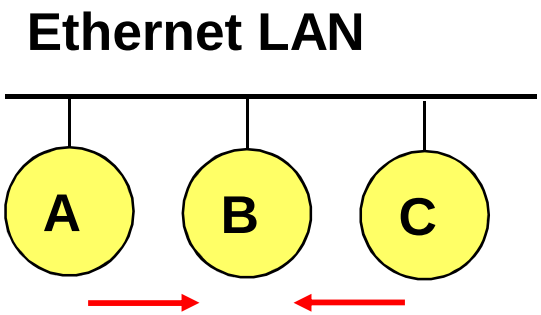
MACAW

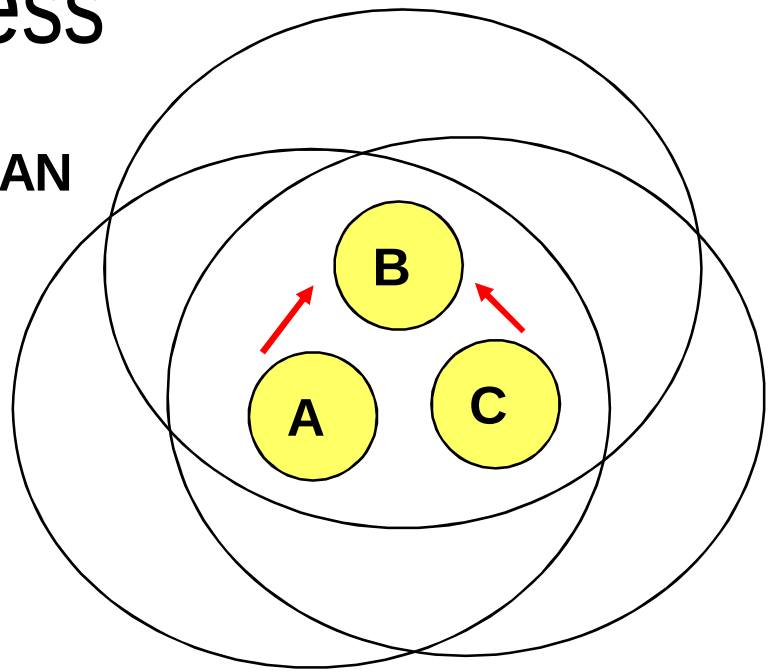
Multiple Access with Collision Avoidance for Wireless

Wireless MAC: Motivation

- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- Medium access problems in wireless networks
  - signal strength decreases proportional to the square of the distance
  - sender would apply CS and CD, but the collisions happen at the receiver
  - sender may not “hear” the collision, i.e., CD does not work
  - CS might not work, e.g. if a terminal is “hidden”

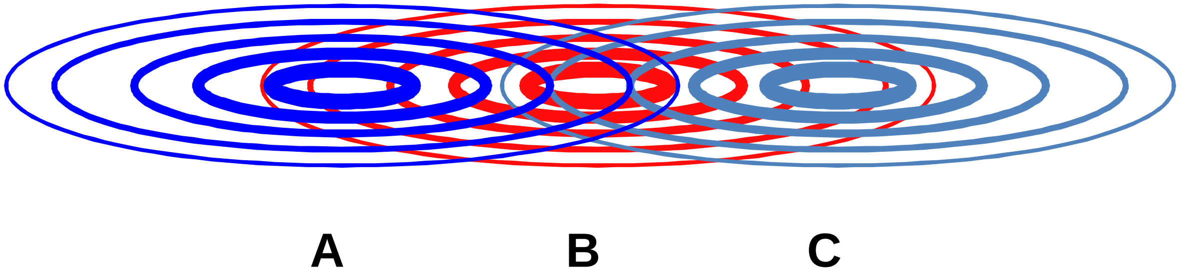
Difference Between Wired and Wireless





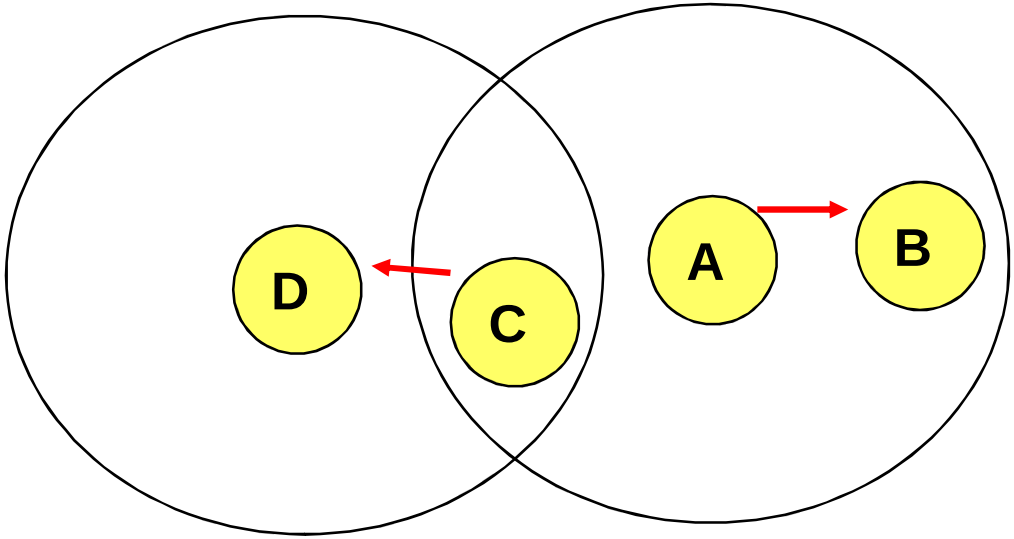
- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected at sender in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

Hidden Terminal Problem



- Hidden terminals
  - A and C cannot hear each other.
  - A sends to B, C cannot receive A.
  - C wants to send to B, C senses a “free” medium (CS fails)
  - Collision occurs at B.
  - A cannot receive the collision (CD fails).
  - A is “hidden” for C.
- Solution?
  - Hidden terminal is peculiar to wireless (not found in wired)
  - Need to sense carrier at receiver, not sender!
  - “virtual carrier sensing”: Sender “asks” receiver whether it can hear something. If so, behave as if channel busy.

Exposed Terminal Problem



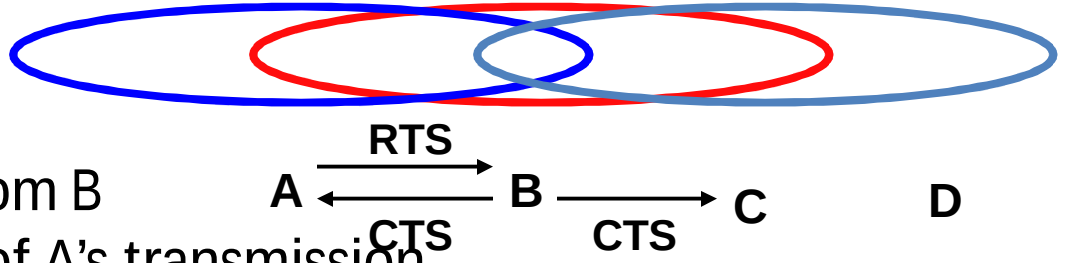
- Exposed terminals
  - A starts sending to B.
  - C senses carrier, finds medium in use and has to wait for A->B to end.
  - D is outside the range of A, therefore waiting is not necessary.
  - A and C are “exposed” terminals.
- A->B and C->D transmissions can be parallel; no collisions

MACA: Multiple Access with Collision Avoidance

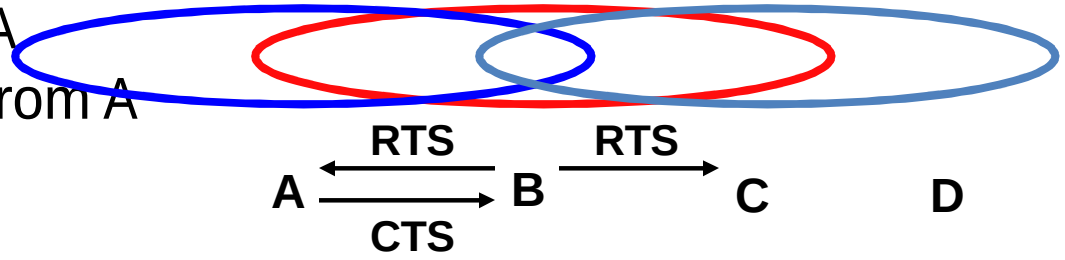
- MACA uses signaling packets for collision avoidance
  - RTS (request to send)
    - sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send)
    - receiver grants the right to send as soon as it is ready to receive
- Signaling (RTS/CTS) packets contain
  - sender address
  - receiver address
  - packet size
- Variants of this method are used in IEEE 802.11

MACA Solutions

- MACA avoids the problem of hidden terminals
  - A and C want to send to B
  - A sends RTS to B
  - B sends CTS to A
  - C "overhears" CTS from B
  - C waits for duration of A's transmission

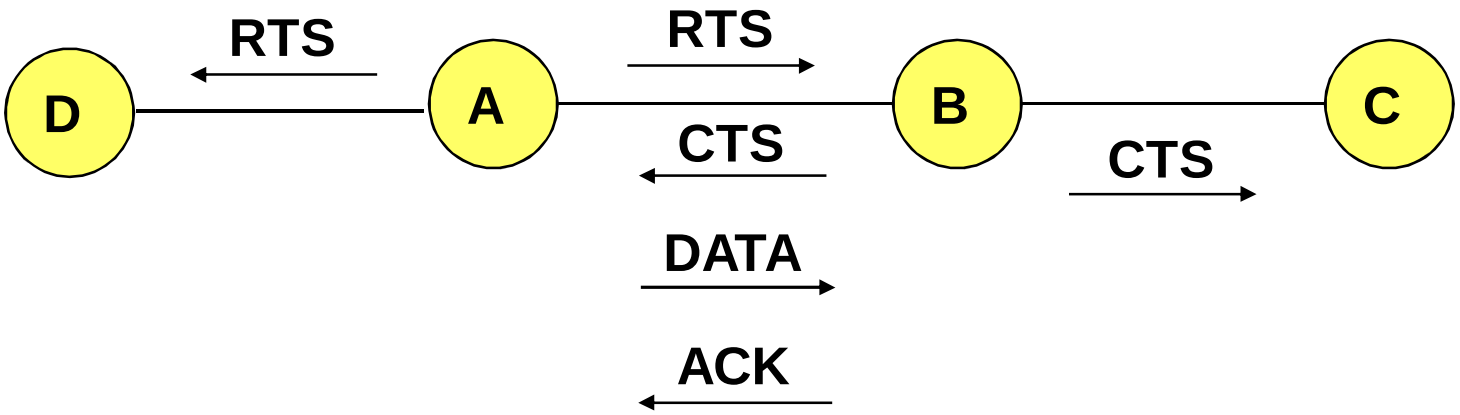


- MACA avoids the problem of exposed terminals
  - B wants to send to A, C to D
  - C hears RTS from B->A
  - C does not hear CTS from A
  - C sends RTS to D



MAC: Reliability

- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance.
- Solution: Use of acknowledgements
  - When B receives DATA from A, B sends an ACK.
  - If A fails to receive an ACK, A retransmits the DATA.
  - Both C and D remain quiet until ACK (to prevent collision of ACK).
  - Expected duration of transmission+ACK is included in RTS/CTS packets.
  - This approach adopted in many protocols [802.11].



- Collision of RTS/CTS packets can happen (hidden terminal).
  - If no CTS, retransmit RTS after backoff.

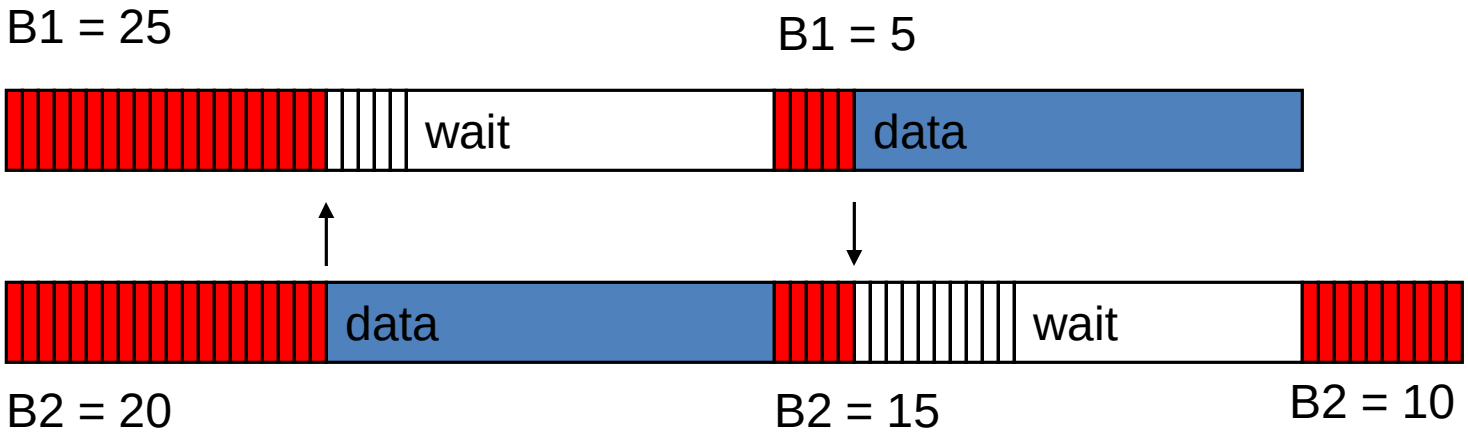
MAC: Collision Avoidance

- With half-duplex radios, collision detection is not possible
- Collision avoidance: Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit

- IEEE 802.11 DCF
  - When transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS

- Time spent counting down backoff intervals is part of MAC overhead
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

DCF Example



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

MAC: Congestion Control

- Number of nodes attempting to transmit simultaneously may change with time; some mechanism to manage congestion is needed.
- IEEE 802.11 DCF: Congestion control achieved by dynamically choosing the contention window cw

- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - cw is doubled (up to a bound CWmax)
  - Upon successful completion data transfer, restore cw to CWmin

- Optimization: MACAW
  - 802.11: cw reduces much faster than it increases
  - Backoff: multiply cw by 1.5 (instead of doubling)
  - Restore: Reduce cw by 1 (instead of CWmin)
  - cw reduces slower than it increases. Exponential increase linear decrease
  - Avoids wild oscillations of cw when congestion is high.

MAC: Energy Conservation

- Wireless nodes need to conserve power ("resource poor").
- Typical solution: Turning the radio off when not needed

- Power Saving Mode in IEEE 802.11 (Infrastructure Mode)
  - An Access Point periodically transmits a beacon indicating which nodes have packets waiting for them
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a node has a packet waiting, then it sends a PS-Poll
    - After waiting for a backoff interval in $[0, CW_{min}]$
  - Access Point sends the data in response to PS-poll

MAC Protocols: Summary

- Wireless medium is prone to hidden and exposed terminal problems

- Protocols are typically based on CSMA/CA
- RTS/CTS based signaling
- Acks for reliability

- Contention window is used for congestion control
- IEEE 802.11 wireless LAN standard
- Fairness issues are still unclear

Routing and Mobility

- Finding a path from a source to a destination
- Issues
  - Frequent route changes
    - amount of data transferred between route changes may be much smaller than traditional networks
  - Route changes may be related to host movement
  - Low bandwidth links
- Goal of routing protocols
  - decrease routing-related overhead
  - find short routes
  - find “stable” routes (despite mobility)

Mobile IP (RFC 2002): Motivation

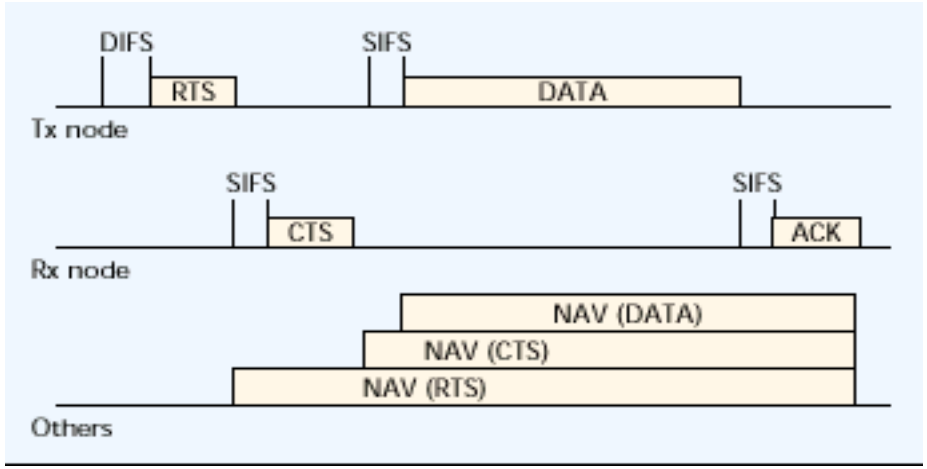
- Traditional routing
  - based on IP destination address
  - network prefix determines physical subnet
  - change of physical subnet implies
    - change of IP address (conform to new subnet), or
    - special routing table entries to forward packets to new subnet
- Changing of IP address
  - DNS updates take to long time
  - TCP connections break
  - security problems
- Changing entries in routing tables
  - does not scale with the number of mobile hosts and frequent changes in the location
  - security problems
- Solution requirements
  - retain same IP address, use same layer 2 protocols
  - authentication of registration messages, ...

Distributed MAC Protocols

- Collision Avoidance Mechanisms
  - With Out-of-Band Signaling : BTMA,RI-BTMA
  - With Control Handshaking : MACA, MACAW
- Distributed Random Access Protocols
  - Distributed Foundation Wireless MAC(DFWMAC)
  - Elimination Yield-Non-Preemptive Priority Multiple Access(EY-NPMA)

[Distributed MAC Protocols]

- Distributed Foundation Wireless MAC(DFWMAC)



Before making an RTS : Distributed Inter-Frame Space(DIFS)

Before sending an ACK : Short Inter-Frame Space(SIFS)

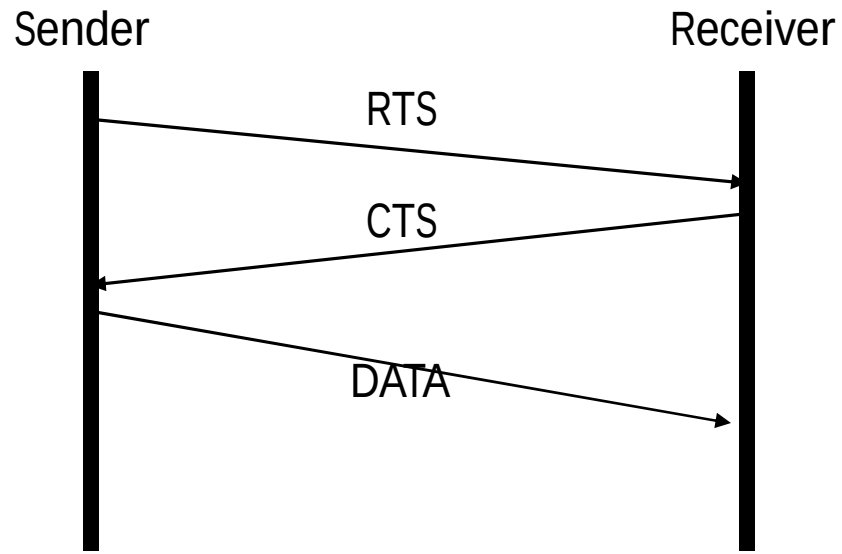
Network Allocation Vector(NAV)

; virtual carrier sensing

- SIFS interval is smaller than DIFS, station sending ACK takes priority to station attempting to send data

MACA

- Using short, fixed size signaling packets
  - Request-to-Send(RTS) , Clear-to-Send(CTS)
  - Include the length of the proposed data transmission



MACA

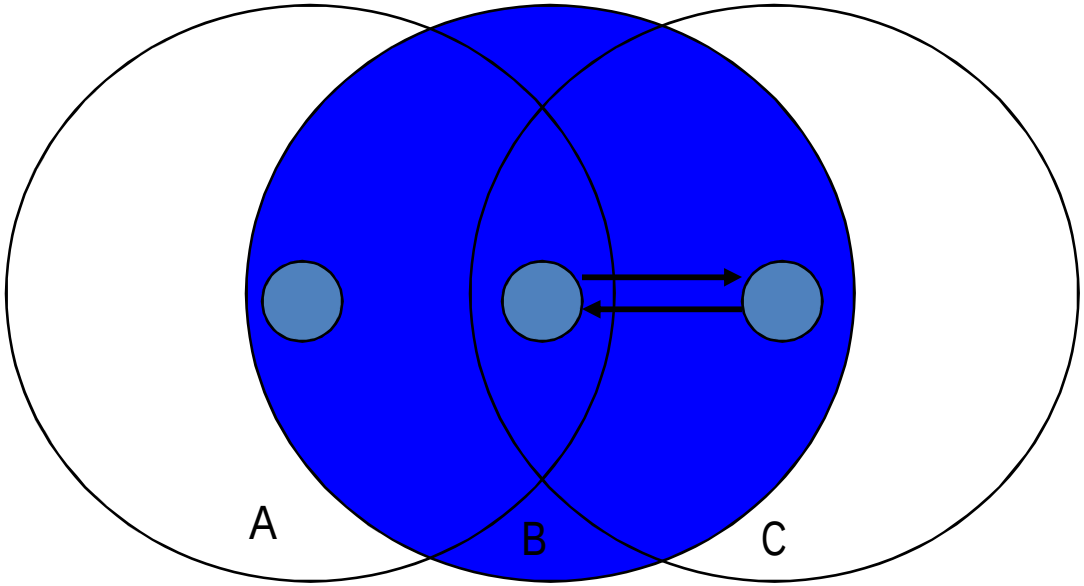
- When a station hears RTS/CTS, but isn't its destination
  - RTS : defer its transmission for CTS time
  - CTS : defer its transmission for data time
- When a station hears RTS but doesn't hear CTS
  - within sender's transmission area, out of receiver's transmission area
  - can start its transmission

MACA
[Hidden terminal scenario]

1.C send RTS

2.B hear RTS, send CTS

3.A hear CTS, defer transmission



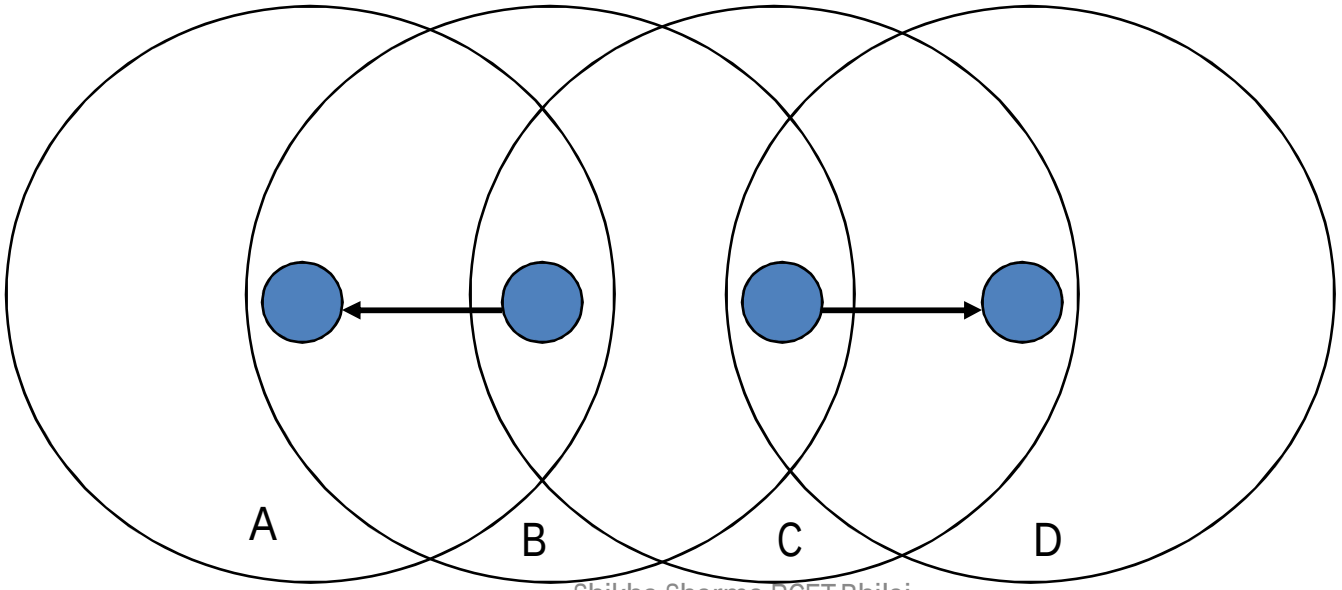
MACA
[Exposed terminal scenario]

1.B send RTS to A

2.A hear RTS, send CTS to B

3.C hear RTS,but can’t hear CTS, so send RTS to D

* Due to capture effect, it makes better, but Not completely solved



[Collisions in MACA]

- Collisions between RTSs may occur
  - only reduce collisions involving data packets
  - but not guarantee data packet collision never occur
  - because a CTS packet requires a certain minimum signal-to-noise ratio
- Use binary exponential backoff algorithm(BEB)
  - RTS -> collision -> wait random chosen interval -> try again -> doubling the average interval

MACA
[Bypassing the MACA Dialogue]

- If RTS and CTS are not significantly smaller than data packet

  $\Rightarrow$ overhead

- Bypassing RTS/CTS
  - efficient
  - risk of a collision
  - may be acceptable trade-off
  - ex) TCP ACK

MACAW

- New protocol : MACAW
  - MACA + several modifications
  - Enhanced performance
- 4 key observations for MACAW
  - Relevant contention is at the receiver, not the sender
  - Congestion is location dependent
  - For fair media access, learning about congestion levels must be collective
  - Synchronization info. about contention periods is needed

    $\Rightarrow$ all devices can contend effectively

MACAW

- BEB (binary exponential back-off)
  - Winner has small back-off counter
  - Loser are completely backed-off
  - Monopoly may occur : fairness problem
  - Different stations have widely varying views of the level of congestion
- Back off algorithm in MACAW : a crucial role for high overall throughput and fair allocation

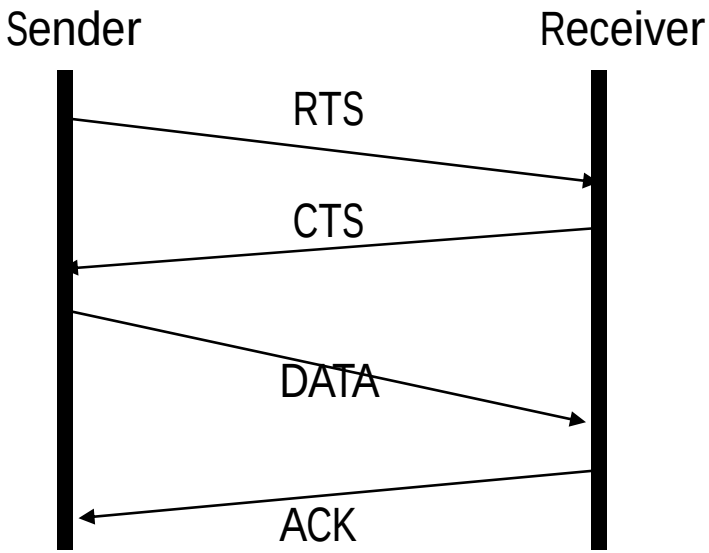
MACAW

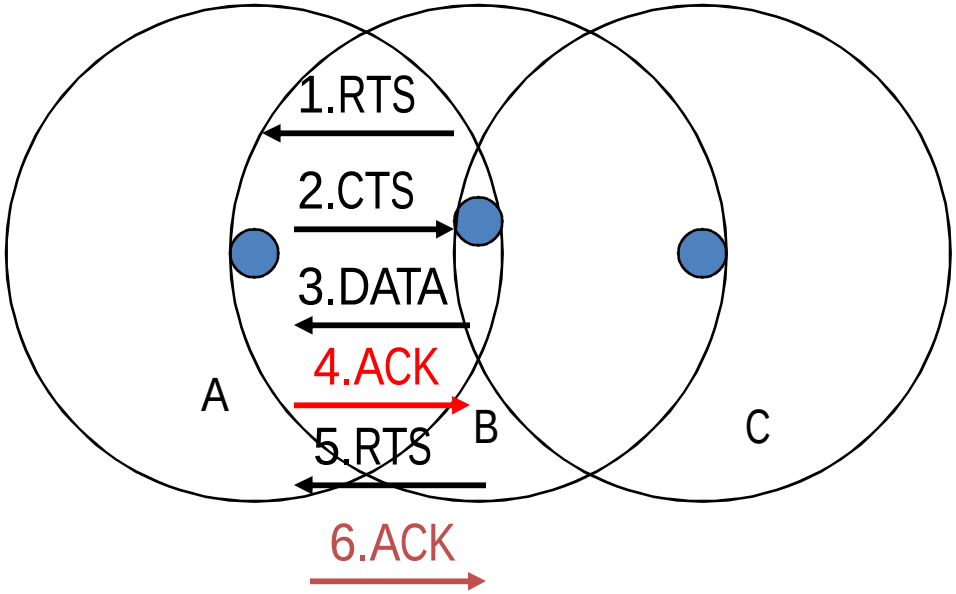
- Modified back-off algorithm
  - Packet header has current value of back-off counter
  - A station hears a packet $\Rightarrow$ copies into its own counter
  - Successful transmission => all have same backoff counter
  - BEB backoff calculation adjusts extremely rapidly;
    - Collision => back off quickly
    - Success => reduce immediately
- MILD(multiplicative increase and linear decrease)
  - fail: new back-off interval = old back-off interval * 1.5
  - success: new back-off interval = old back-off interval - 1

MACAW
[MACA + ACK]

- MACA
  - error $\Rightarrow$ error control in Transport layer
  - TCP minimum time out is 0.5 sec
    $\Rightarrow$ slow recovery
  - link-layer much faster
- Reliable data transmission
- ACK control packet
  - no ACK or CTS $\Rightarrow$ back-off increase
  - ACK $\Rightarrow$ back-off decrease

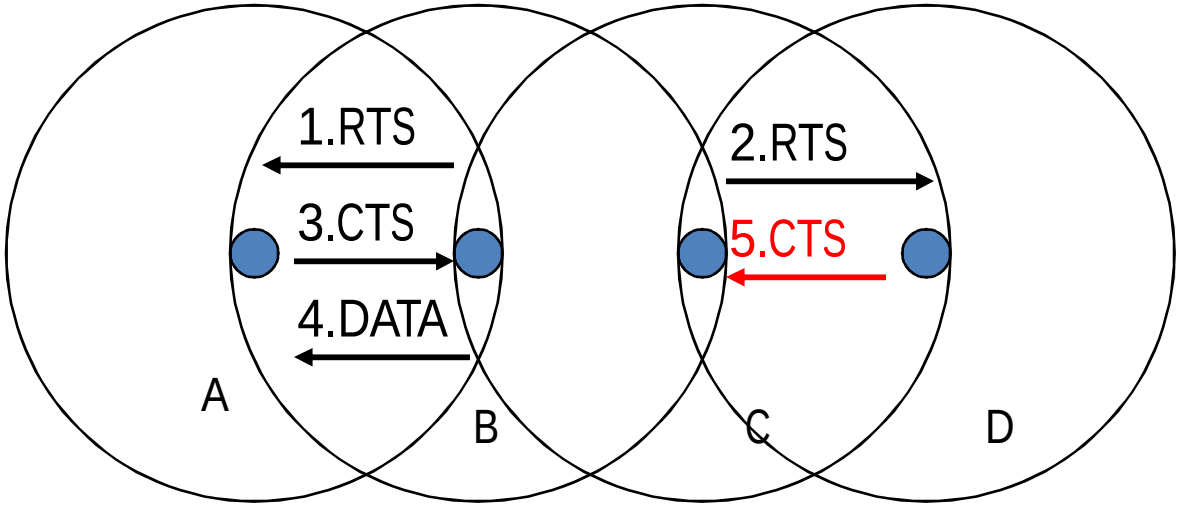
MACAW
[MACA + ACK]



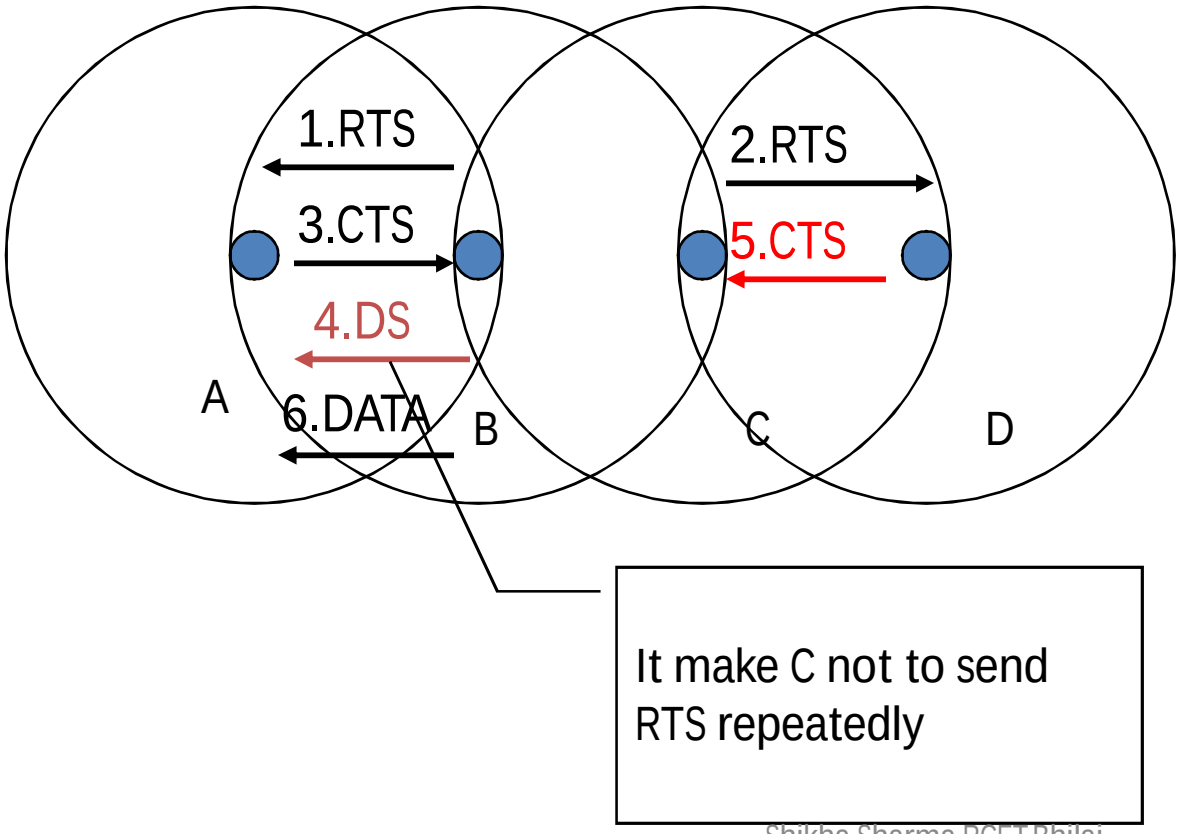


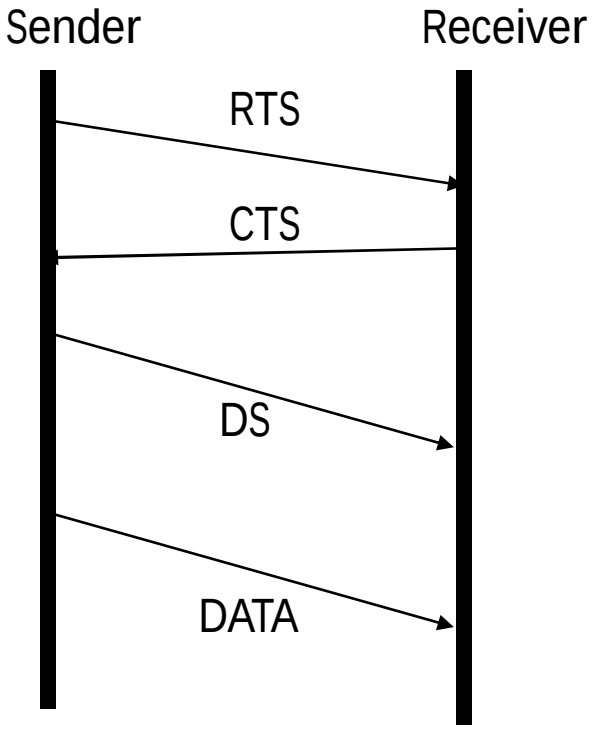
MACAW
MACA + DS

- C can't receive CTS $\Rightarrow$ can't start transmission
- C send RTS repeatedly $\Rightarrow$ Back-off counter increase



MACAW
MACA + DS



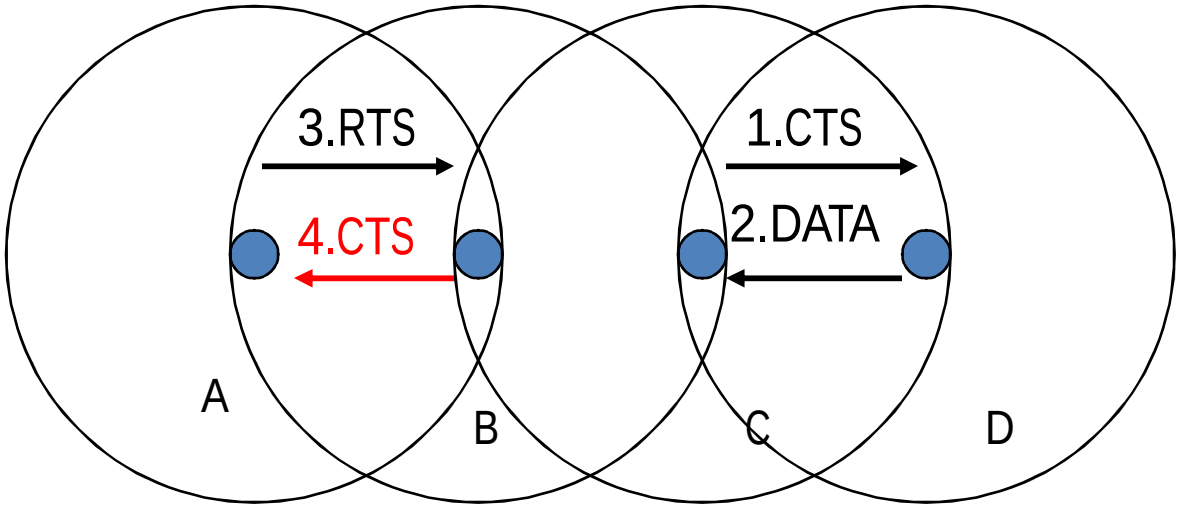


MACAW
MACA + DS

- DS(Data Sending) control packet
  - Announces successful RTS/CTS exchange
  - Informs the other stations about the existence and length of the following DATA packet
  - By DS, stations can know when they try their transmission
    - synchronization info.

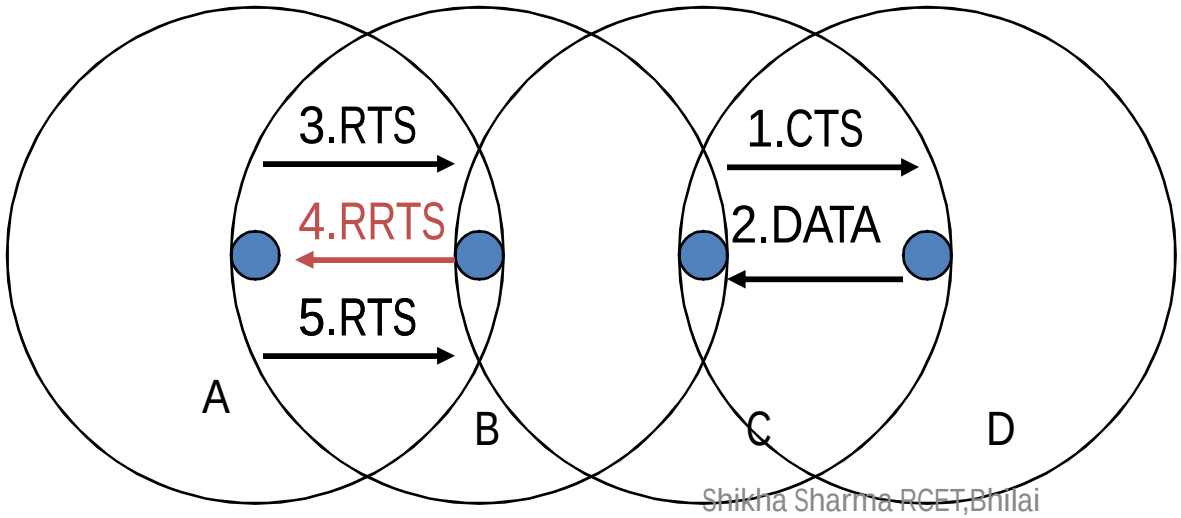
MACAW
MACA + RRTS

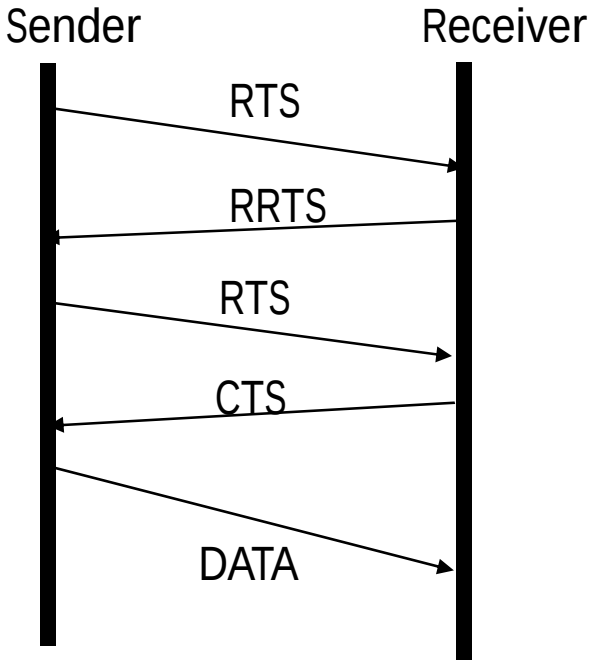
- D is sending to C
- A send RTS but B can't send CTS by C's CTS
  - Synchronization problem occurs
  - repeated time-out and maximum back-off
  - finding good time for sending is too difficult



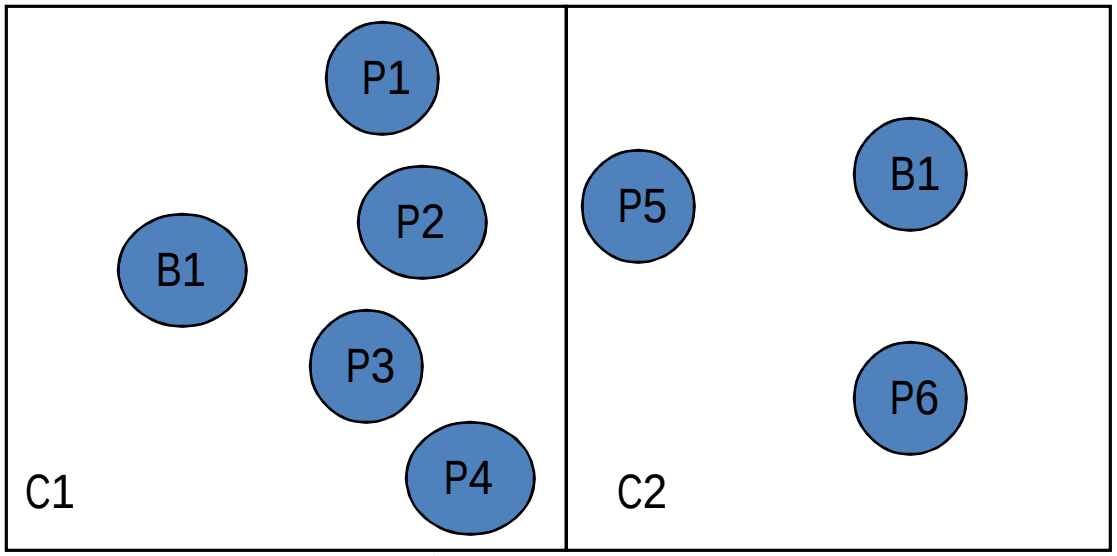
MACAW
MACA + RRTS

- on contention time
  - B send RRTS(request-for-request-to-send)
- on receiving RRTS,
  - A send RTS immediately
  - other stations deter for 2 slot time

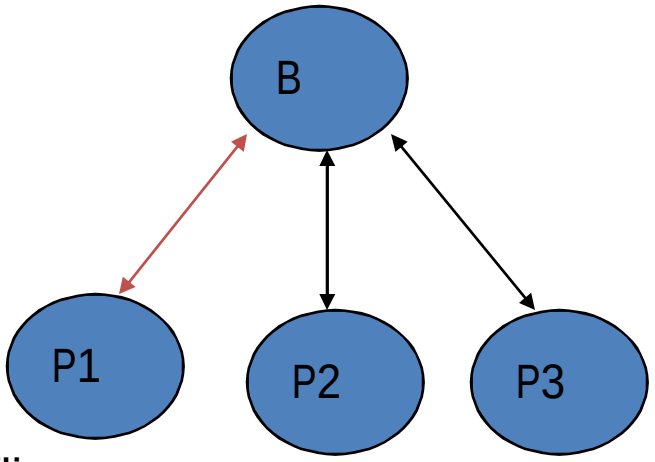




MACAW



Backoff value can be copied from one region to another



offline

MACAW

- By Copy Algorithm,
  - Multicell wireless LAN
    - congestion is typically not uniform
  - Noise next to the sender or receiver

    => Max backoff counter
  - A terminal is offline => Max backoff counter
- Solution
  - separate back-off counter for each stream
  - Per-destination backoff copying algorithm

- Multiple Access with Collision Avoidance for Wireless (MACAW) is a slotted MAC protocol widely used in Ad-hoc networks.
- It uses *RTS-CTS-DS-DATA-ACK* frame sequence for transferring data

Principles of operation

- Assume that node A has data to transfer to node B.

1. “Request To send” frame (RTS) from A to B
2. “Clear To Send” frame (CTS) from B to A
3. “Data Sending” frame (DS) from A to B
4. DATA fragment frame from A to B, and
5. Acknowledgement frame (ACK) from B to A.

RRTS:

To summarize, a transfer may in this case consist of the following sequence of frames between node D and C:

1. “Request To send” frame (RTS) from D to C
2. “Request for Request to send” frame (RRTS) from C to D (after a short delay)
3. “Request To send” frame (RTS) from D to C
4. “Clear To Send” frame (CTS) from C to D
5. “Data Sending” frame (DS) from D to C
6. DATA fragment frame from D to C,
7. Acknowledgement frame (ACK) from C to D.

- MACAW does not solve the exposed terminal problem.

BLUETOOTH

What is Bluetooth

- It is an low power, short ranged radio link for communication between mobile devices
- Developed in 1994 by the Swedish company Ericsson to enable laptops make calls over mobile phones
- Also known as 802.15
- Unlicensed band, Provides data rates of up to 720 Kbps

Bluetooth Applications

- Major use in consumer electronics
- Embedded in a whole slew of electronic products
- ranging from on PDAs, cellphones and printers, to automobiles

Bluetooth Characteristics

- Allows up to 8 devices to communicate in a local network called a Piconet , also known as a Personal Area Network or PAN
- Because of its low power consumption, its range is limited to 10 m.
- However, range can be increased to 100 m by employing a scatternet topology or a higher powered antenna
- Three classes of Bluetooth devices
- • Class 1 – 100 m
- • Class 2 – 10m
- • Class 3 – 1m

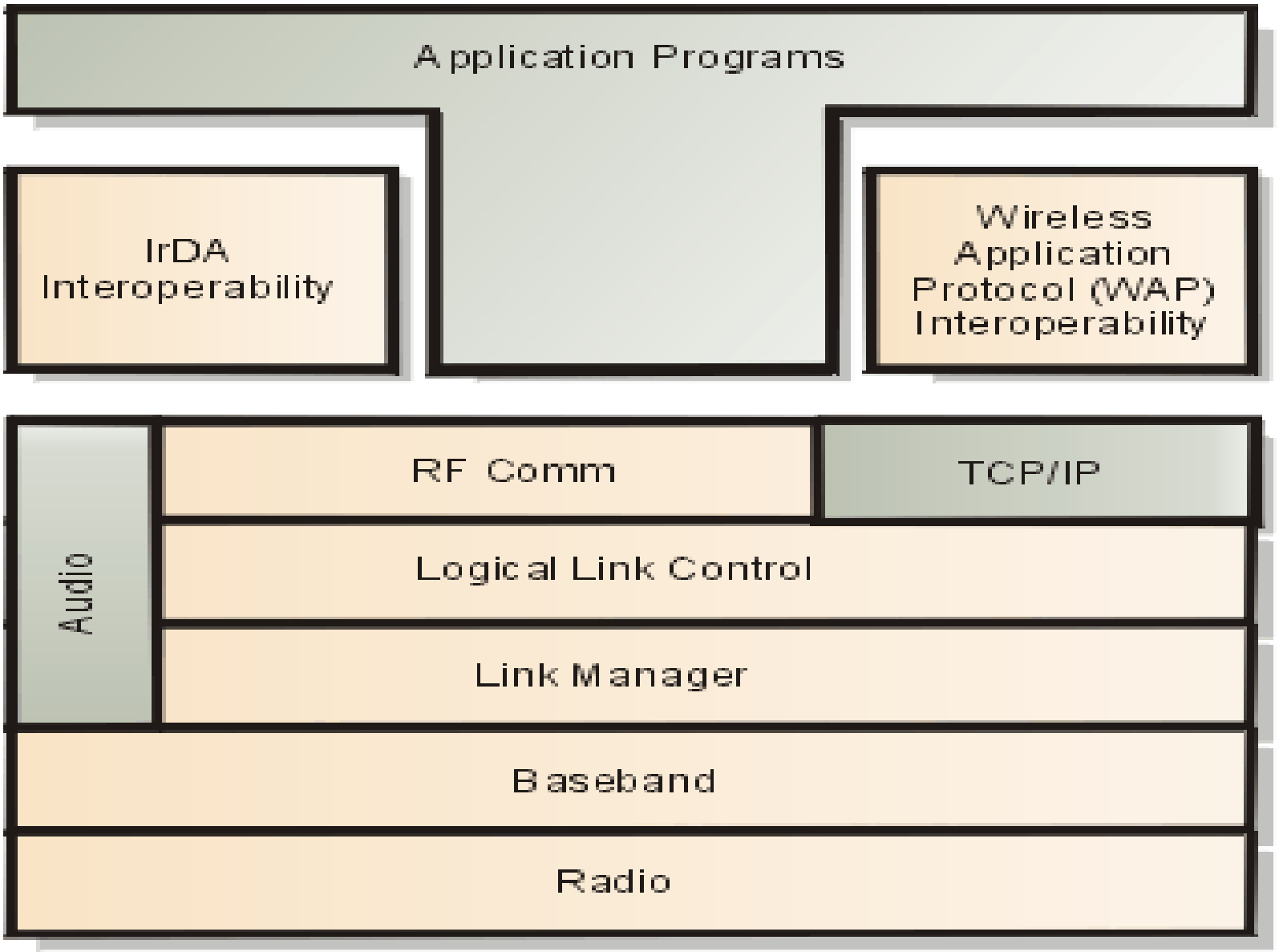
The Bluetooth Standard

- The Bluetooth standard is maintained and published by the Bluetooth Special Interest Group (SIG)
- Includes thousands of member companies Covers topics such as interoperability, testing and qualification of bluetooth devices
- Most important, outlines the specifications for:
- Bluetooth Radio
- Baseband
- LMP – Link Manager Protocol
- HCI – Host Controller Interface
- L2CAP – Logical Link Control & Adaptation Protocol
- RFCOMM
- Profiles

- Bluetooth communication occurs between a master radio and a slave radio.
- Bluetooth radios are symmetric in that the same device may operate as a master and also the slave.
- Each radio has a 48-bit unique device address that is fixed.
- Two or more radio devices together form ad-hoc networks called piconets.
- All units within a piconet share the same channel.
- Each piconet has one master device and one or more slaves.
- There may be up to seven active slaves at a time within a piconet.
- Thus, each active device within a piconet is identifiable by a 3-bit active device address.
- Inactive slaves in unconnected modes may continue to reside within the piconet.

- A master is the only one that may initiate a Bluetooth communication link.
- However, once a link is established, the slave may request a master/slave switch to become the master.
- Slaves are not allowed to talk to each other directly.
- All communication occurs within the slave and the master.
- Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master.
- Each piconet uses a different frequency hopping sequence.
- Radio devices used Time Division Multiplexing (TDM).
- A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

- Multiple piconets with overlapping coverage areas form a scatternet.
- Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis.
- A device may be a master in one piconet and a slave in another or a slave in more than one piconet.


Application Programs
IrDA Interoperability
Wireless Application Protocol (WAP) Interoperability
Audio
RF Comm
TCP/IP
Logical Link Control
Link Manager
Baseband
Radio
Bluetooth Stack

Bluetooth Radio

- Bluetooth uses a 74 MHz slice of the 2.4 GHz radio band.
- Bluetooth employs a Frequency Hopping strategy
- Specification of air interface
- Modulation

Baseband – Physical Link

- Baseband is the physical link of the Bluetooth protocol.
- Designed to support multimedia applications that mix voice (circuit-switched) and data (packet switched)
- It handles two types of links:
- SCO – Synchronous Connection Oriented
- ACL – Asynchronous Connectionless

Baseband - SCO

- SCO is a symmetric point-to-point link between a master and a single slave in the piconet
- The SCO link is maintained by the master by its use of time slots at regular intervals
- A SCO link can be considered as a circuit-switched connection

Baseband - ACL

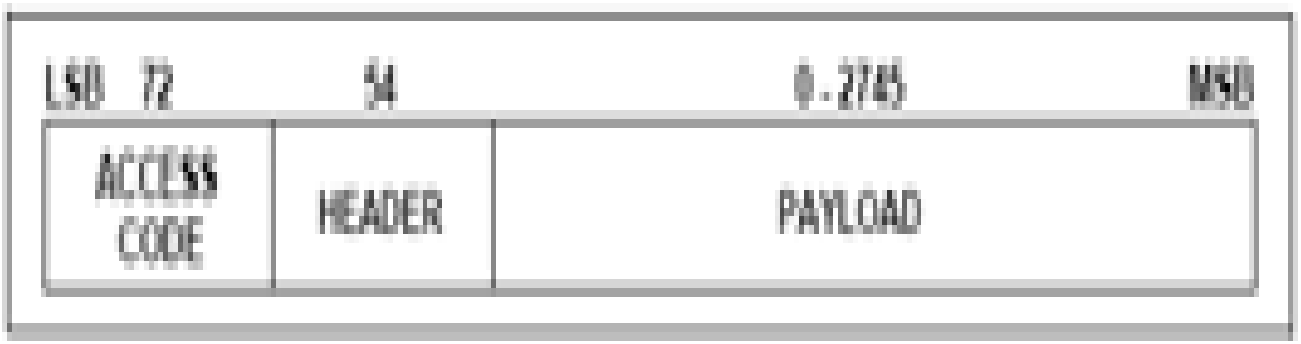
- Point-to-multipoint link between master and all slaves in the piconet
- ACL link can be established on per slot basis
- In the slots which are not reserved for SCO transmission, the master can establish an ACL link with any slave, including the slaves which are already engaged in SCO communication
- Unlike SCO where multiple SCO links can be established, only one ACL Link can be established between two nodes
- ACL packets which are lost are always retransmitted

Baseband - Packets

- The Bluetooth general packet format is comprised of three parts:
- Access Code, Header, and Payload
- Access Code: Can be 72 bits wide, depending on whether a packet header follows or not

The 6 fields are as follows:

- **ADDR**-- is a 3-bit active member address used to distinguish between the active members of a piconet
- **Type** --is a 4-bit type code used to distinguish between one of 16 different packet types, such as ID Packet, POLL packet, or NULL Packet.
- **Flow--** is a bit used for flow control over ACL. When the receiver buffer is full, a STOP indication is returned by means of FLOW = 0 to prevent further transmission
- **ARQN** -- is the acknowledgement bit for CRCed packets
- **SEQN**-- provided sequencing for multiple data packets
- **HEC**-- is the Header Error Check used to verify header integrity


LSB 72
54
0-2745
MSB
ACCESS CODE
HEADER
PAYLOAD

Link controller

- It is responsible for device discoverability, as well as establishing and maintaining connections with other devices Handling corrupted data
- Authentication, pairing and encryption
- Synchronization
- Capability negotiation
- Quality of service negotiation
- Power control

- Link supervision
- State and transmission mode change
- Further more it controls the power modes and duty cycles of the Bluetooth radio device, and the connection states of a Bluetooth unit in a piconet.

Logical Link Control and Adaptation Protocol (L2CAP)

- L2CAPs function is to take data from a higher level application and to pass it down to the lower stack
- L2CAP supports both connection oriented and connectionless data services to upper protocols
- It allows higher level protocols to transmit and receive data of up to 64 Kbytes.

- Multiplexing between different higher level protocols
- Segmentation and Reassembly to allow transfer of larger packets than lower levels can support
- Group management, provides one-way transmission to a group of BT devices
- QoS management for higher protocols

TCS Binary or TCS BIN

- Telephony Control protocol –
- A bit oriented protocol, defines the call control signaling for the establishment of speech and data calls between Bluetooth devices.

Mobile IP

- Mobile IP is an IETF standard communication protocol that is designed to allow mobile device users to move from one network to another while maintaining their permanent IP address.

Mobile IP: Protocol Overview

- Mobile IP is a network layer solution for homogenous and heterogeneous mobility on the global Internet which is scalable, robust, secure and which allows nodes to maintain all ongoing communications while moving.

Mobile IP

- Mobile IP was developed as a means for transparently dealing with problems of mobile users
  - Enables hosts to stay connected to the Internet regardless of their location
  - Enables hosts to be tracked without needing to change their IP address
  - Requires addition of some infrastructure
  - Has no geographical limitations
  - Requires no modifications to IP addresses or IP address format
  - Supports security
    - Could be even more important than physically connected routing

Mobile IP Entities

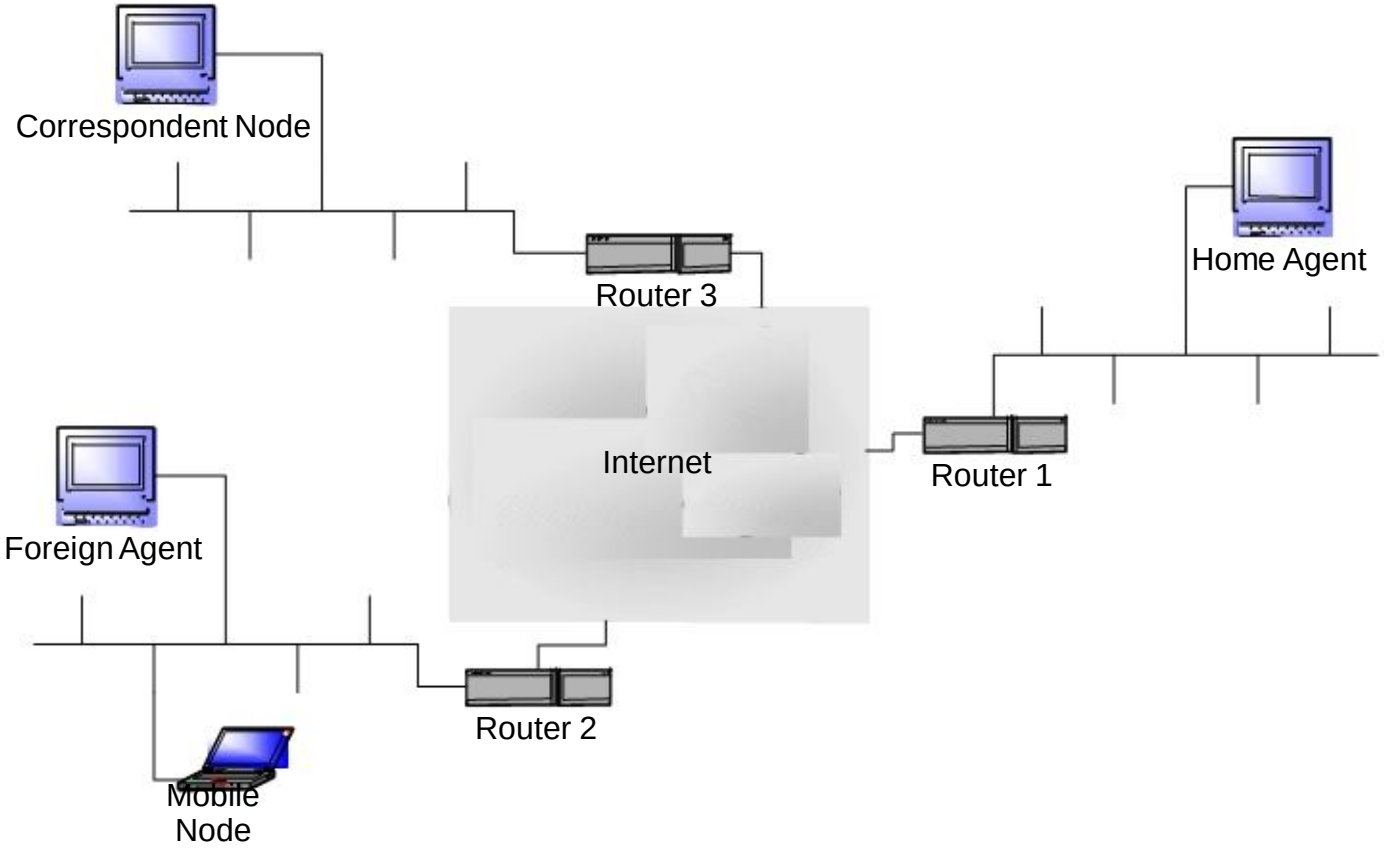
- Mobile Node (MN)
  - The entity that may change its point of attachment from network to network in the Internet
  - Assigned a permanent IP called its *home address* to which other hosts send packets regardless of MN's location
- Home Agent (HA)
  - This is router with additional functionality
  - Located on home network of MN
  - Does mobility binding of MN's IP with its COA
  - Forwards packets to appropriate network when MN is away
    - Does this through encapsulation

Mobile IP Entities contd.

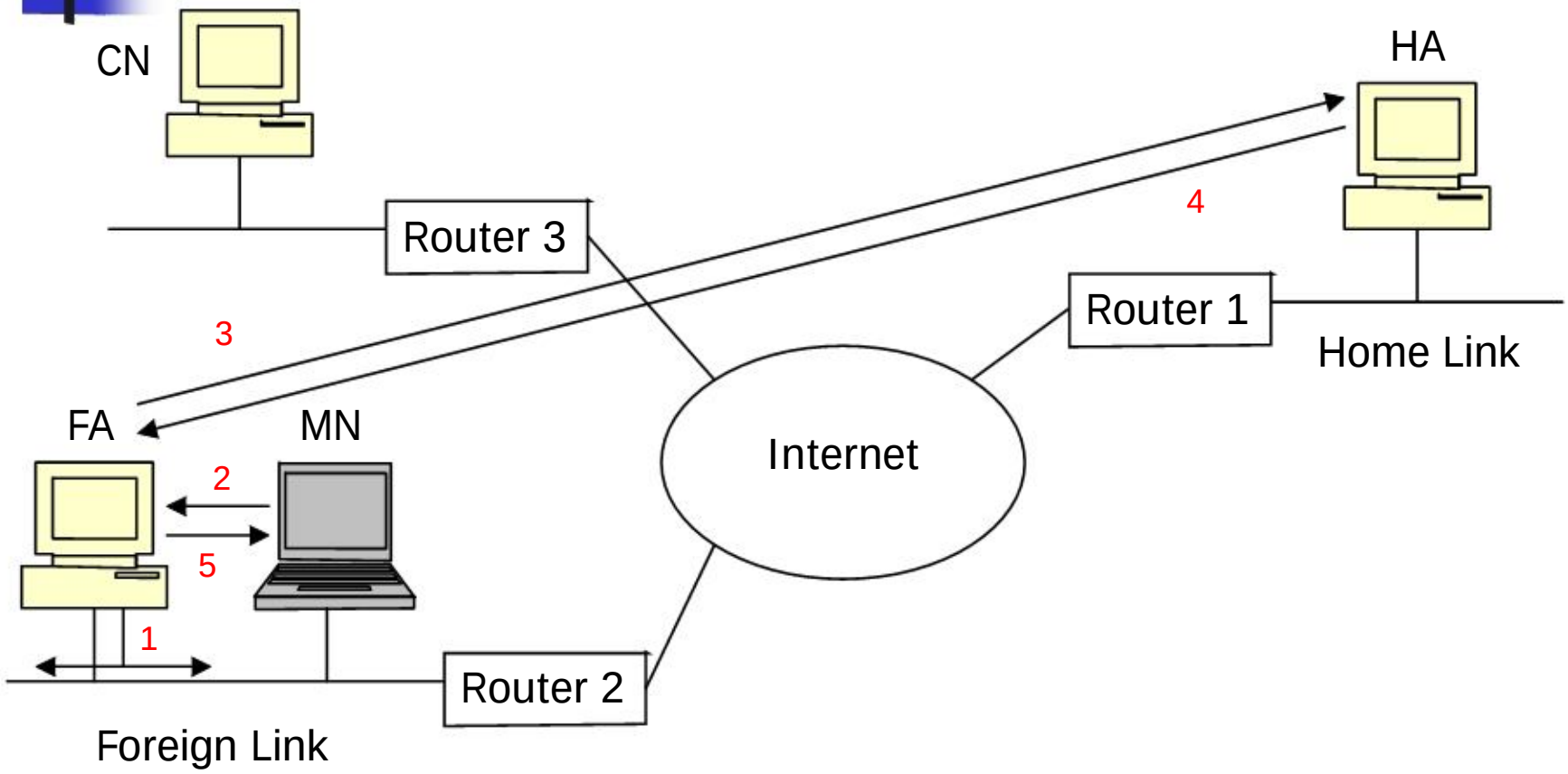
- Foreign Agent (FA)
  - Another router with enhanced functionality
  - If MN is away from HA the it uses an FA to send/receive data to/from HA
  - Forward's MN's registration request
  - Decapsulates messages for delivery to MN
- Care-of-address (COA)
  - Address which identifies MN's current location
  - Usually the IP address of the FA

- Correspondent Node (CN)
  - End host to which MN is corresponding
  - May be fixed device or mobile device

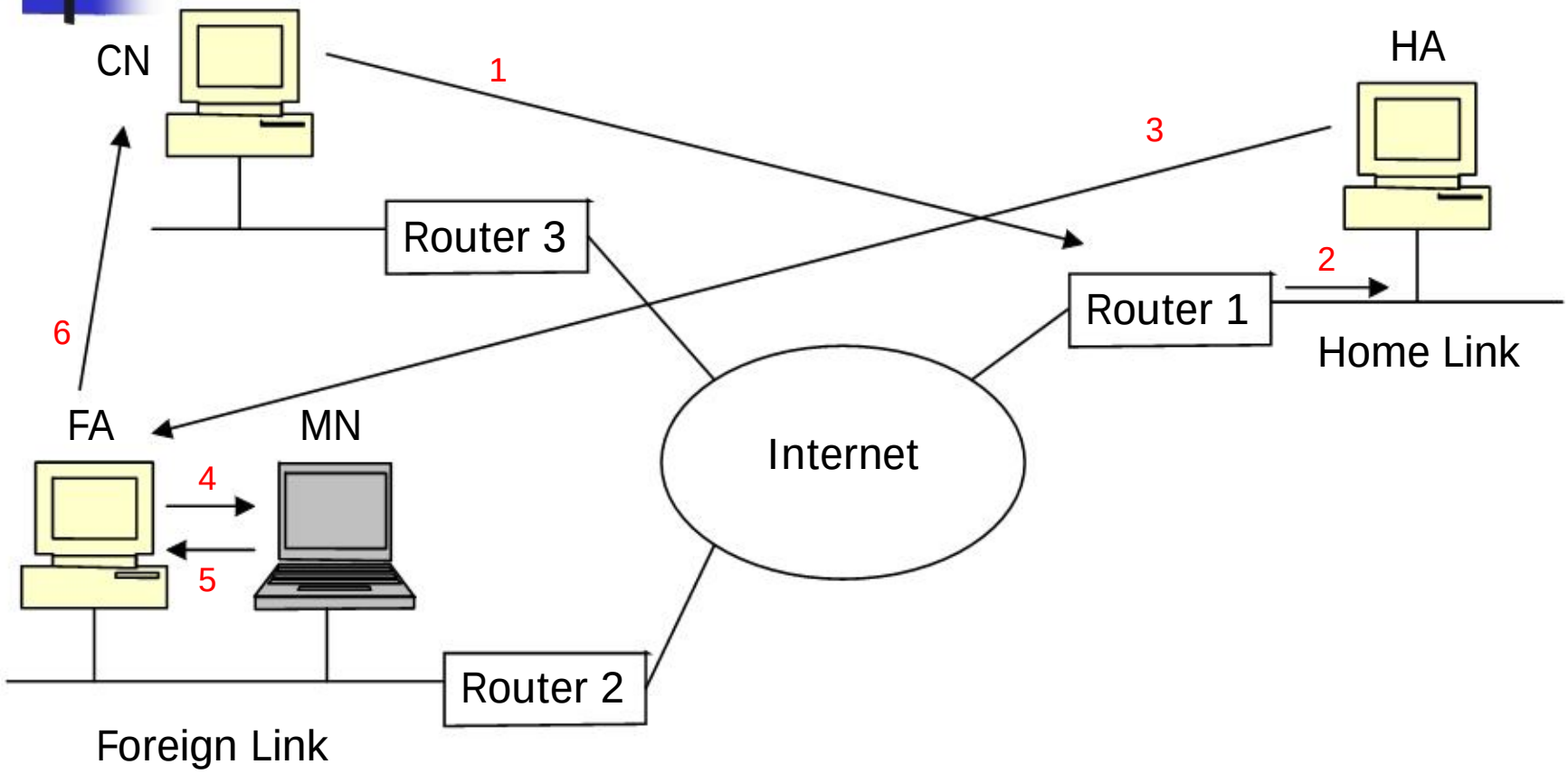
How Mobile IP Works? (Packet Delivery)


Correspondent Node
Router 3
Home Agent
Internet
Router 1
Foreign Agent
Router 2
Mobile Node

Common Scenario (2)



Common Scenario (1)



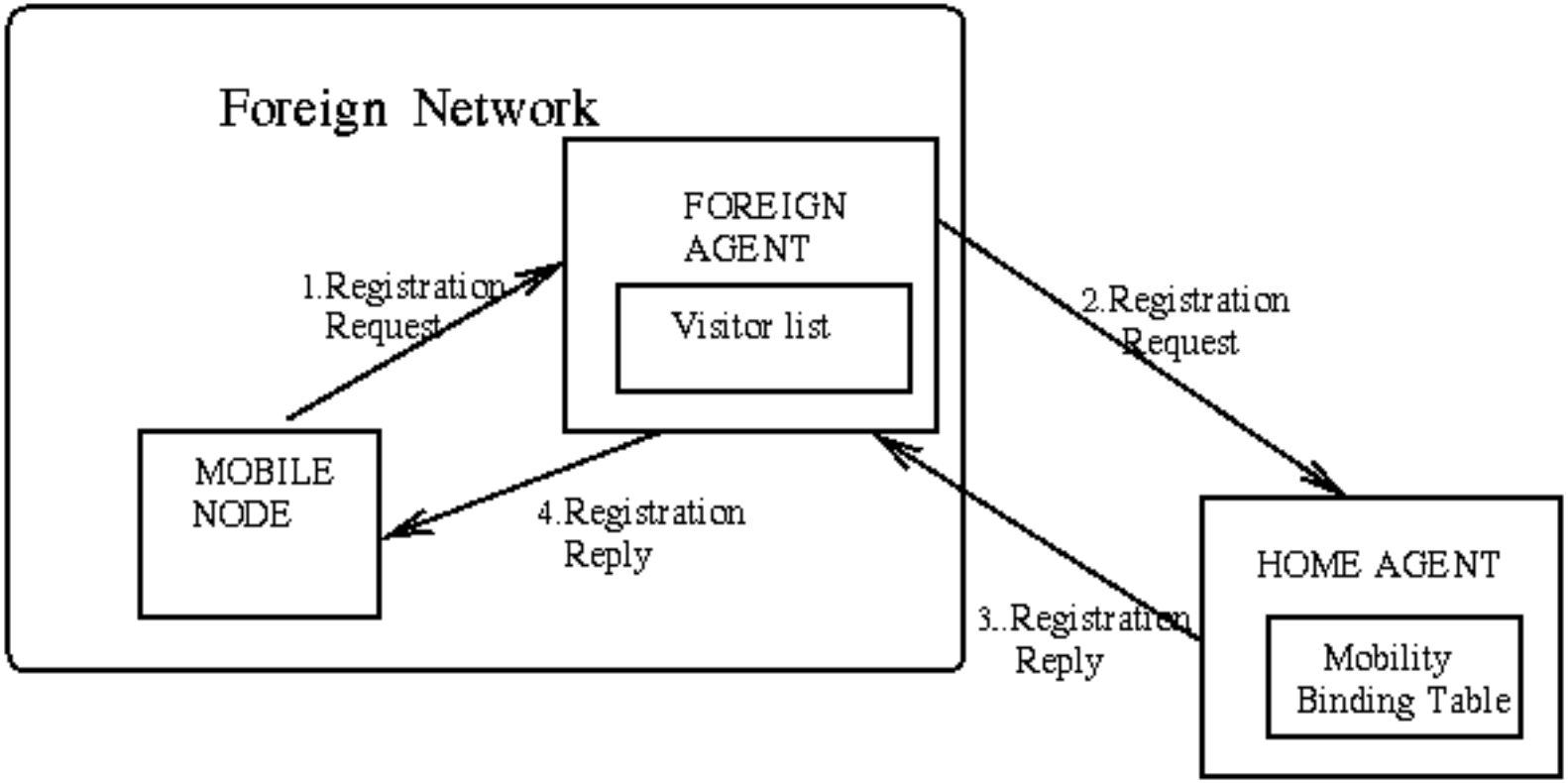
What is registration

- Mobile IP registration is the process by which a mobile node:
  - requests routing services from a foreign agent or foreign link
  - informs its home agent of its current care-of-address.
  - Renews a registration due to expire
  - deregisters when it returns to its home link

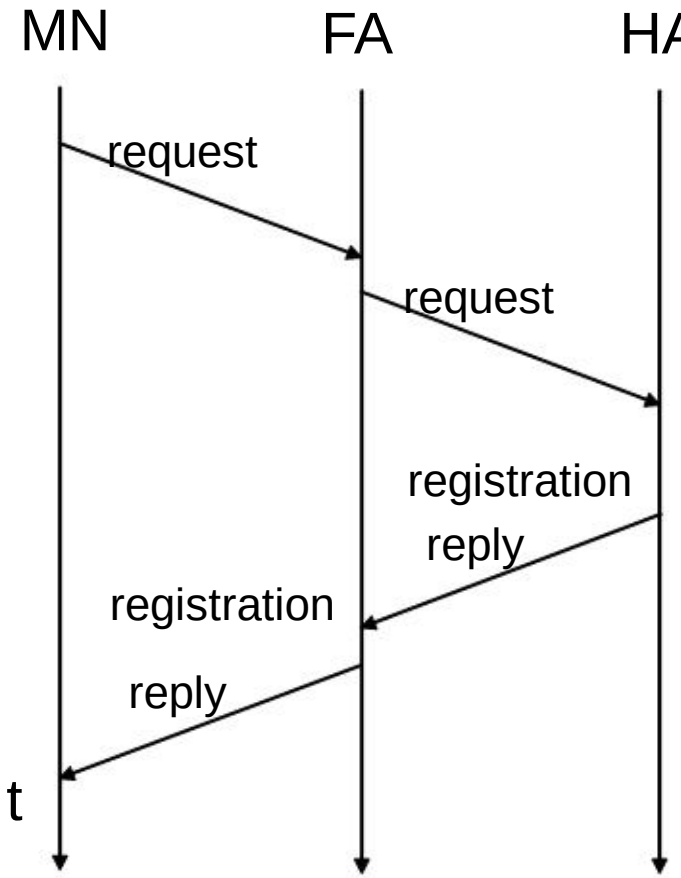
Registration scenarios

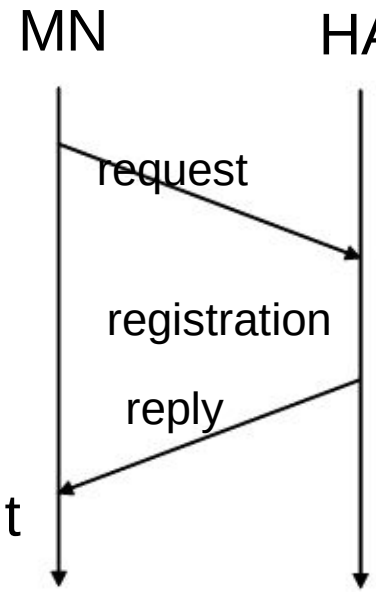
- A registration consists of an exchange of a Registration request and a Registration Reply between a mobile node and its home agent.
- Three common scenarios:
  - Using foreign agent c/o
  - Using co-located c/o
  - deregisters upon returning home

Registration Process

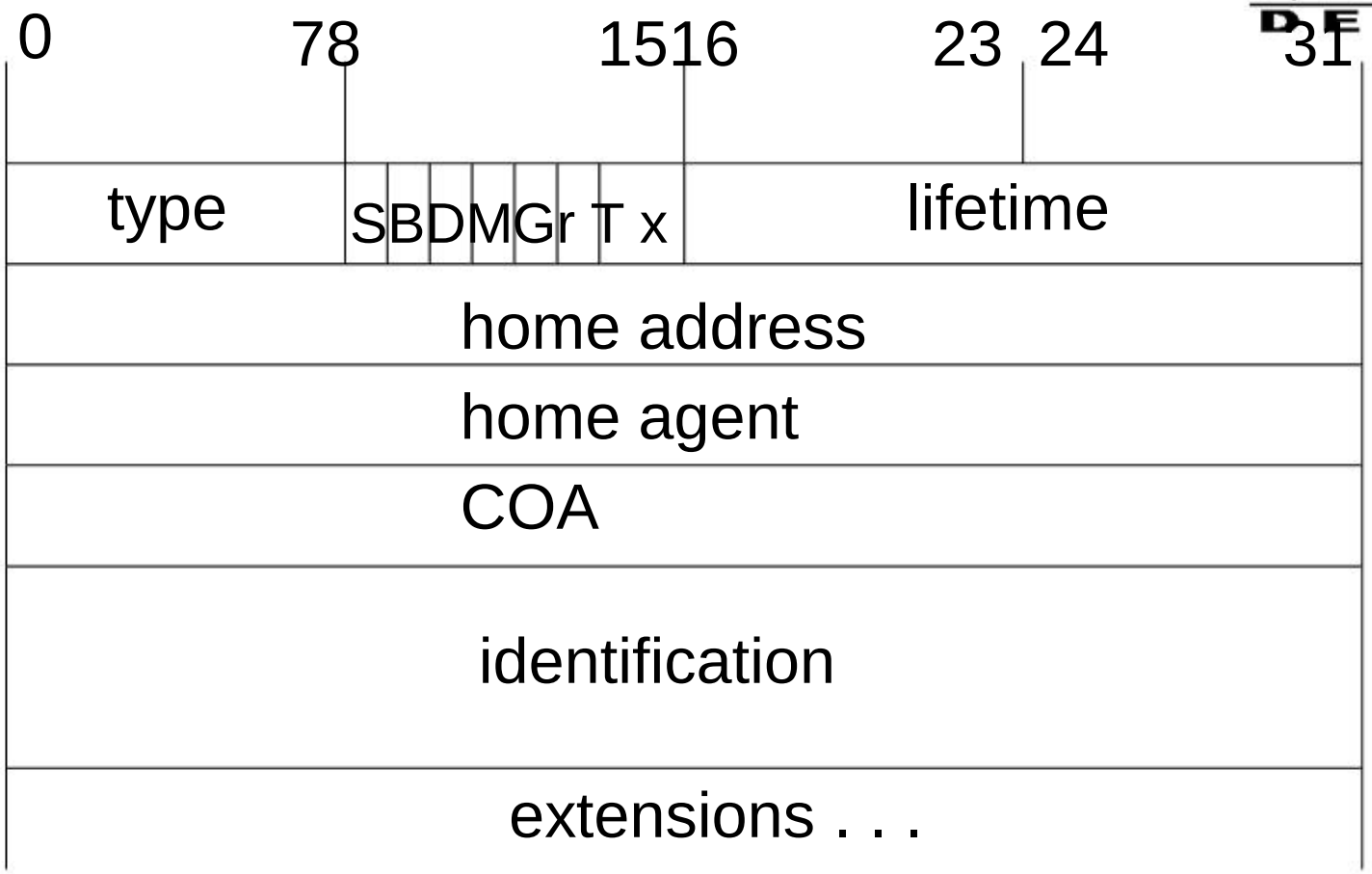


Registration

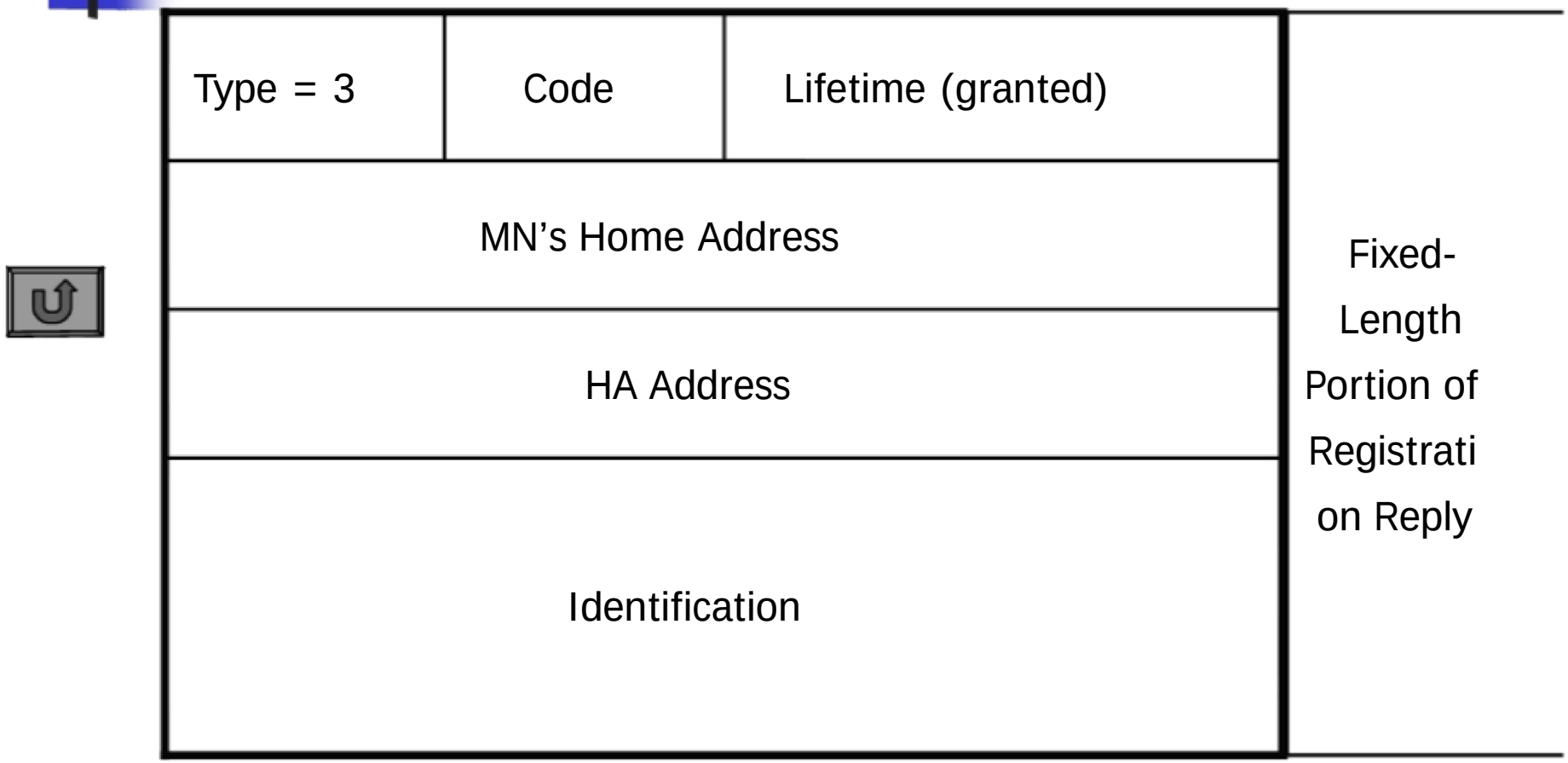




Registration request



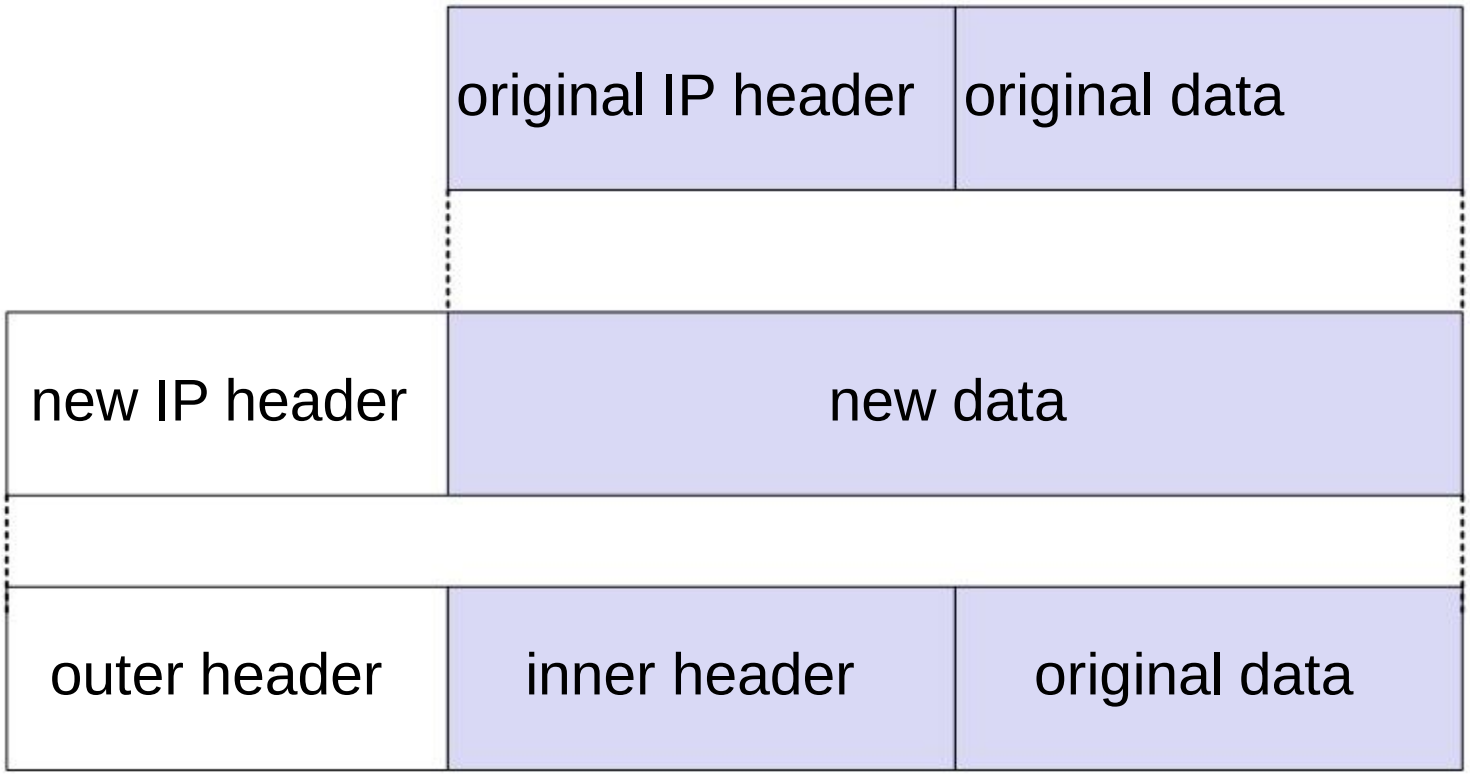
Registration Reply Message (Fixed Portion Only)



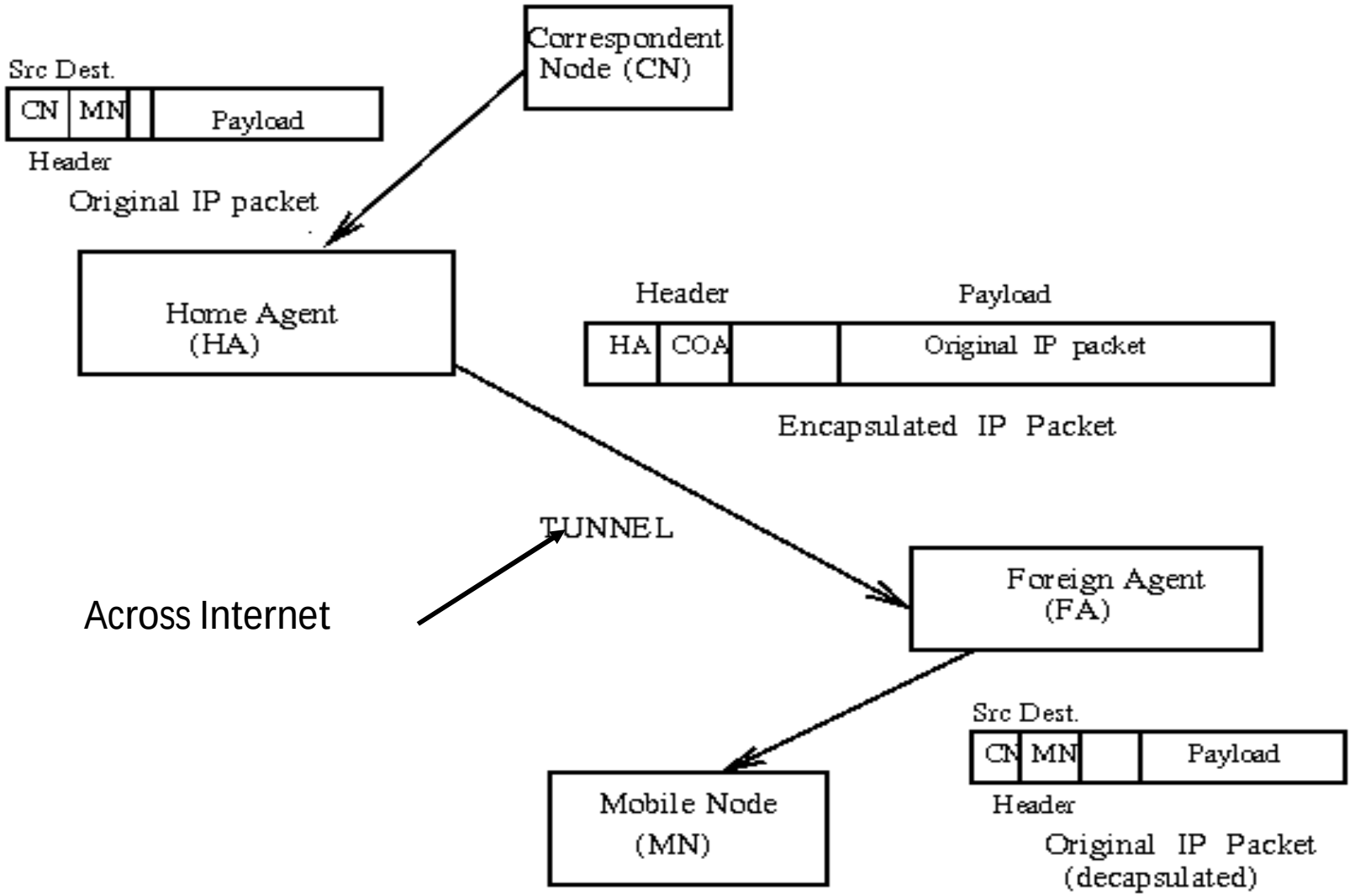
Tunneling and Encapsulation

- A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoints.
- Sending a packet through a tunnel is achieved by using encapsulation.
- Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it in to the data part of a new packet.
- Encapsulation – just like standard IP only with COA
- Decapsulation – again, just like standard IP

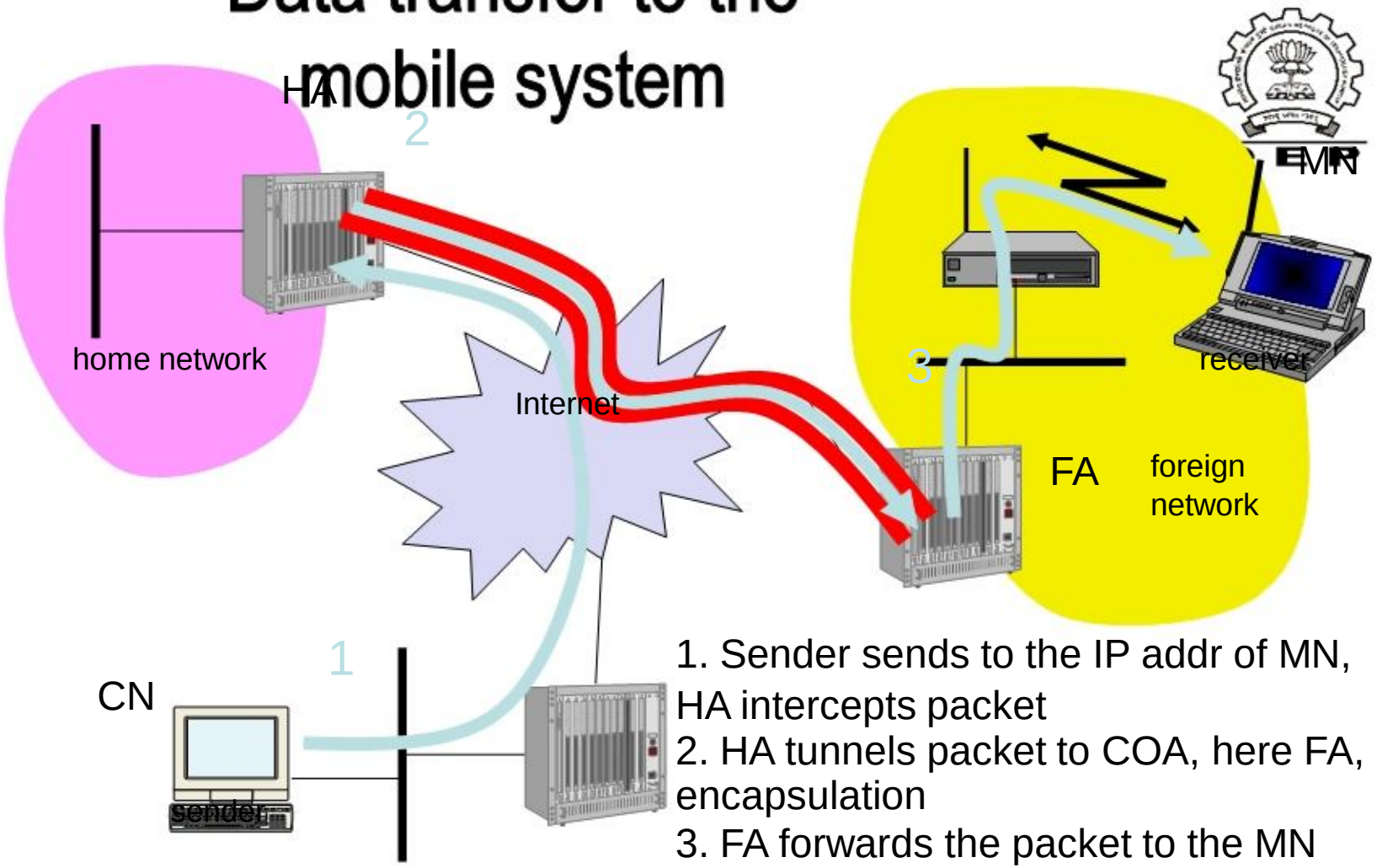
Encapsulation



Mobile IP Tunneling

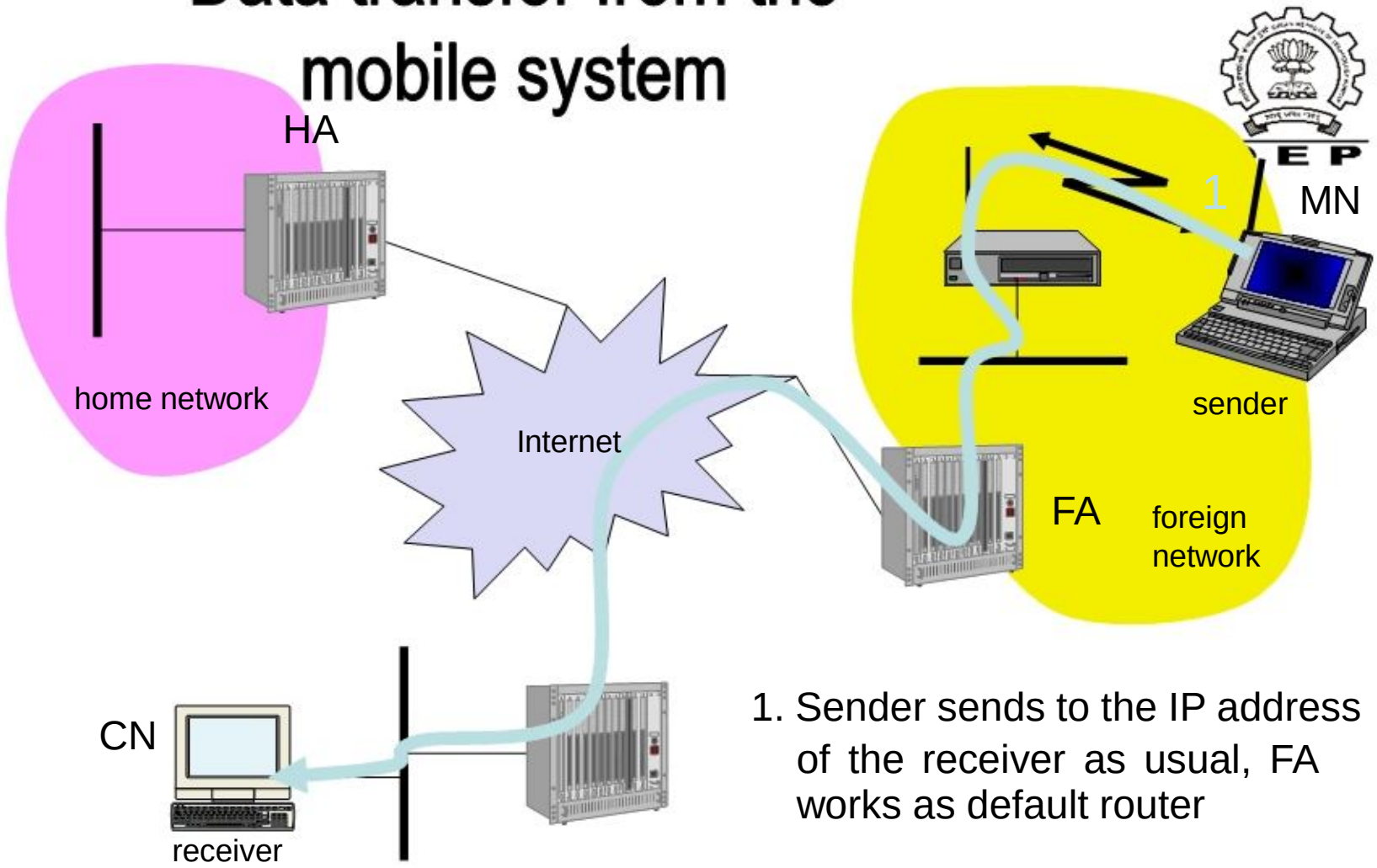


Data transfer to the mobile system



1. Sender sends to the IP addr of MN, HA intercepts packet
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



1. Sender sends to the IP address of the receiver as usual, FA works as default router

IP-in-IP encapsulation

- IP-in-IP-encapsulation (mandatory in RFC 2003)
  - tunnel between HA and COA

ver.	IHL	TOS	length	
IP identification			flags	fragment offset
TTL			IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	TOS	length	
IP identification			flags	fragment offset
TTL			IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ... payload				

IP header fields

Source and Destination addresses are those of the tunnel end points

- Internet header length :
  - Length of outer header in 32 bit words
- Total length :
  - Measures length of entire encapsulated IP datagram
- Don't fragment bit :
  - Copied from inner header if set
- Time to live TTL:
  - Appr time to deliver to tunnel exit

ICMP messages from the tunnel

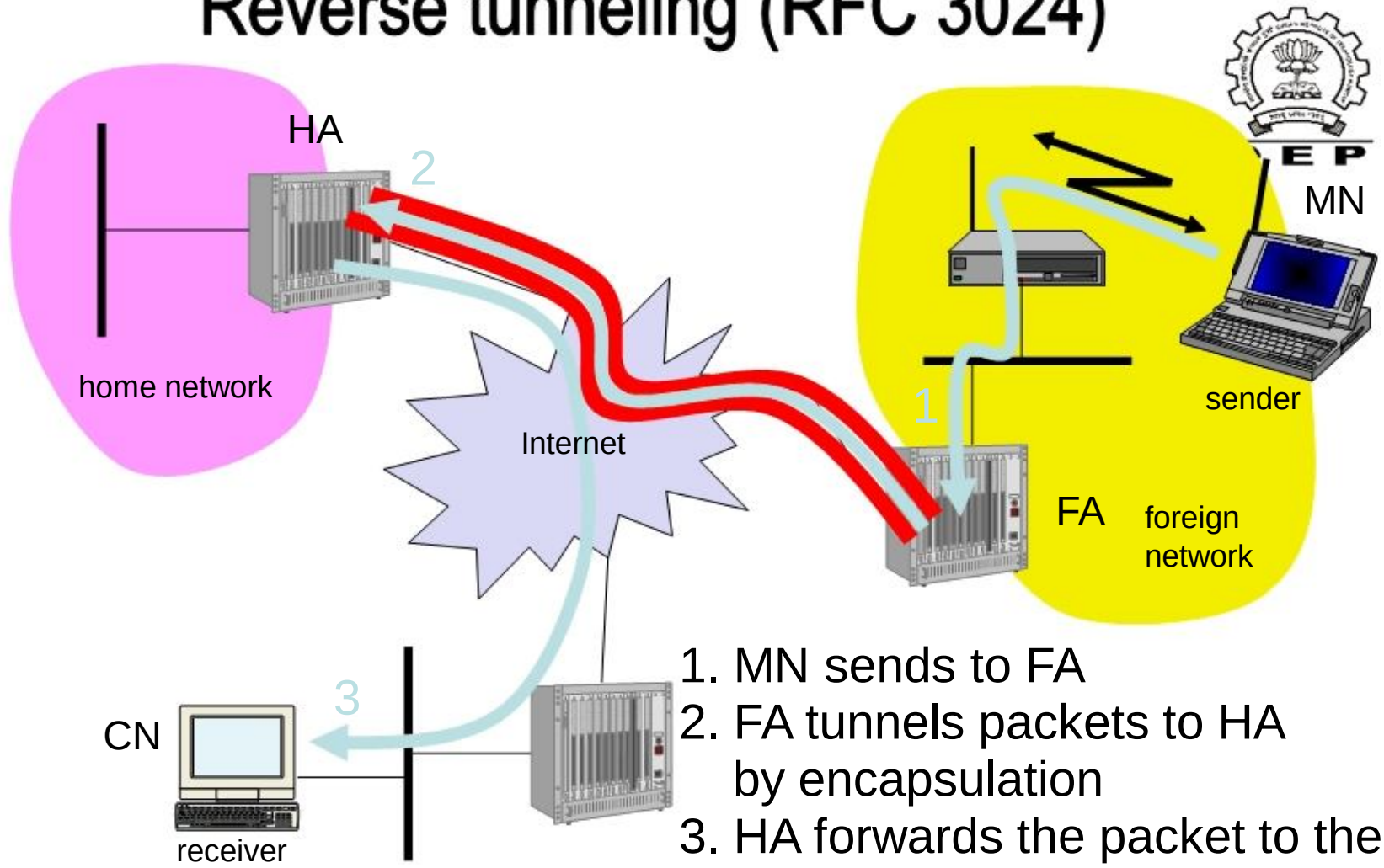
Encapsulator may receive ICMP messages from any intermediate router in the tunnel other than exit

- Network unreachable:
  - Return dest unreachable message to org sender
- Host unreachable:
  - Return host unreachable message
- Datagram too big:
  - Relay ICMP datagram too big to org sender

ICMP error messages (contd.)

- Source route failed:
  - Handled by encapsulator itself and MUST NOT relay message to orginal sender
- Source quench:
  - SHOULD NOT relay message to original sender , SHOULD activate congestion control mechanism
- Time exceeded:
  - MUST be reported to original sender as host unreachable message

Reverse tunneling (RFC 3024)



1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)

Mobile IP: Reverse tunneling

- Router accept often only “topological correct“ addresses (firewall!)
  - a packet from the MN encapsulated by the FA is now topological correct
  - furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is too far away from the receiver)

Reverse tunneling

- Reverse tunneling does not solve
  - problems with *firewalls*, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
  - optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)

Agent Discovery

- Agent Discovery
  - Determines whether it is currently connected to its home link or a foreign link.
  - Detects whether it has moved from one link to another
  - obtains a care-of adress when connected to a foreign link
- Agent discovery consists of 2 messages:

Agent Advertisement
Agent Solicitation

- Home agents and foreign agents advertise their presence by periodically multicasting (broadcasting)
  - Agent advertisements
- Mobile node's listens to Agent advertisements (I am a home or away)
- A mobile node connected to a foreign link acquires a c/o adress
- Mobile node registers its c/o address with its home agent

- Home agent adverties reachibility to the netwrok-prefix of the mobile node's home link (Attracting packets sent to the mobiles home adress.
  - Intercept these messages and tunnels them to the C/O
- At C/O, the original packet is extracted from the tunnel and then delivered to the mobile node
- In reverse direction, packets sent from the mobile node are routed directly to thier destination, without need for tunneling (FA only router)

Mobile IP Support Services

- Agent Discovery
  - HA's and FA's broadcast their presence on each network to which they are attached
    - Beacon messages via ICMP Router Discovery Protocol (IRDP)
  - MN's listen for advertisement and then initiate registration
- Registration
  - When MN is away, it registers its COA with its HA
    - Typically through the FA with strongest signal
  - Registration control messages are sent via UDP to well known port
- Encapsulation – just like standard IP only with COA
- Decapsulation – again, just like standard IP

Mobile IP Operation

- A MN listens for agent advertisement and then initiates registration
  - If responding agent is the HA, then mobile IP is not necessary
- After receiving the registration request from a MN, the HA acknowledges and registration is complete
  - Registration happens as often as MN changes networks
- HA intercepts all packets destined for MN
  - This is simple unless sending application is on or near the same network as the MN
  - HA masquerades as MN
  - There is a specific lifetime for service before a MN must re-register
  - There is also a de-registration process with HA if an MN returns home

Tables maintained on routers

- Mobility Binding Table
  - Maintained on HA of MN
  - Maps MN's home address with its current COA

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

- Visitor List
  - Maintained on FA serving an MN
  - Maps MN's home address to its MAC address and HA address

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Security in Mobile IP

- Authentication can be performed by all parties
  - Only authentication between MN and HA is required
  - Keyed MD5 is the default
- Replay protection
  - Timestamps are mandatory
  - Random numbers on request reply packets are optional
- HA and FA do not have to share any security information.

Problems with Mobile IP

- Suboptimal “triangle” routing
  - What if MN is in same subnetwork as the node to which it is communicating and HA is on the other side of the world?
    - It would be nice if we could directly route packets
  - Solution: Let the CN know the COA of MN
    - Then the CN can create its own tunnel to MN
    - CN must be equipped with software to enable it to learn the COA
    - Initiated by HA who notifies CN via “binding update”
    - Binding table can become stale

Other Mobile IP Problems

- Single HA model is fragile
  - Possible solution – have multiple HA
- Frequent reports to HA if MN is moving
  - Possible solution – support of FA clustering
- Security
  - Connection hijacking, snooping…
- Many open research questions

Mobility in IPv6

- Route Optimization is a fundamental part of Mobile IPv6
  - Mobile IPv4 it is an optional set of extensions that may not be supported by all nodes
- Foreign Agents are not needed in Mobile IPv6
  - MNs can function in any location without the services of any special router in that location
- Security
  - Nodes are expected to employ strong authentication and encryption
- Other details...

Wireless Local Loop (WLL)

Wireless Local Loop (WLL)

- WLL is a new communications access method that uses radio waves for transmission of information between customers and service provider sites, rather than traditional fixed methods such as copper or fiber optic delivery.
- WLL is a system that connects subscribers to the local telephone station wirelessly.
- WLL can be used to provide voice, fax, and data connections.

WLL

- Wireless local loop provides two-way communication services to stationary or near-stationary users within a small service area.
- This technology is intended to replace the wire line local loop.

WLL

- Other names
  - Radio In The Loop (RITL)
  - Fixed-Radio Access (FRA)
  - Fixed wire less Access (FWA)

Advantages of WLL

- Wireless local loop offers following advantages over wireline local loop:
- **Cost:** Wireless systems are less expensive than wired systems with the cost of installing cables, either underground or on poles, and avoided the cost of maintaining the wired infrastructure.
- **Ease of Installation and deployment** – WLL systems can be installed and deployed easily.

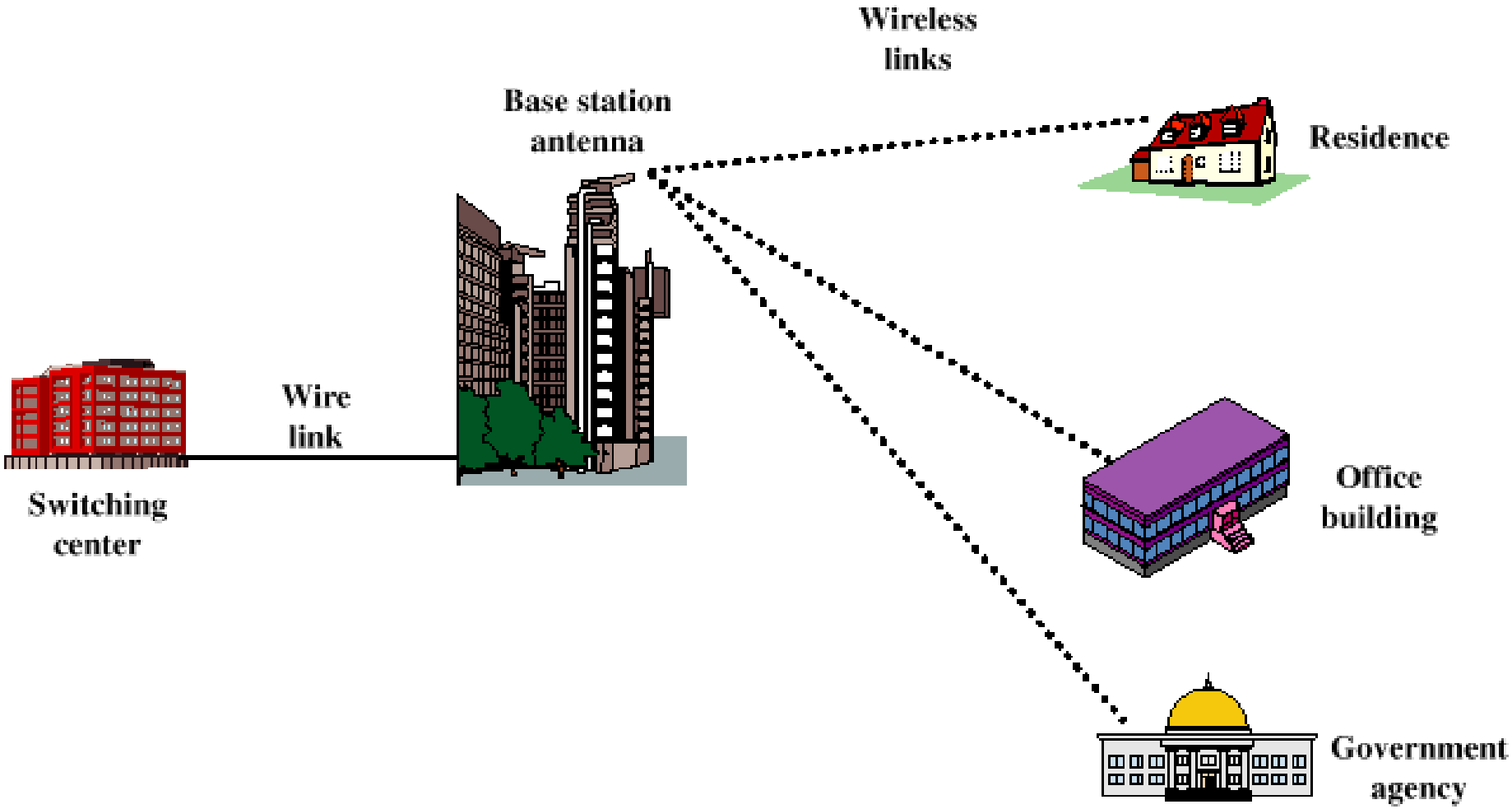
Advantages of WLL

- **Installation time**: WLL systems can be installed in a small fraction of the time required for a new wired system. WLL eliminates the wires, poles, and ducts essential for a wire line network; in other words the WLL approach significantly speeds the installation process.

- **WLL Applications**: WLL systems find applications in competitive telecommunications markets, in developing telecommunications markets, and in rural and remote markets that would not be economically served by conventional wireline access technologies.

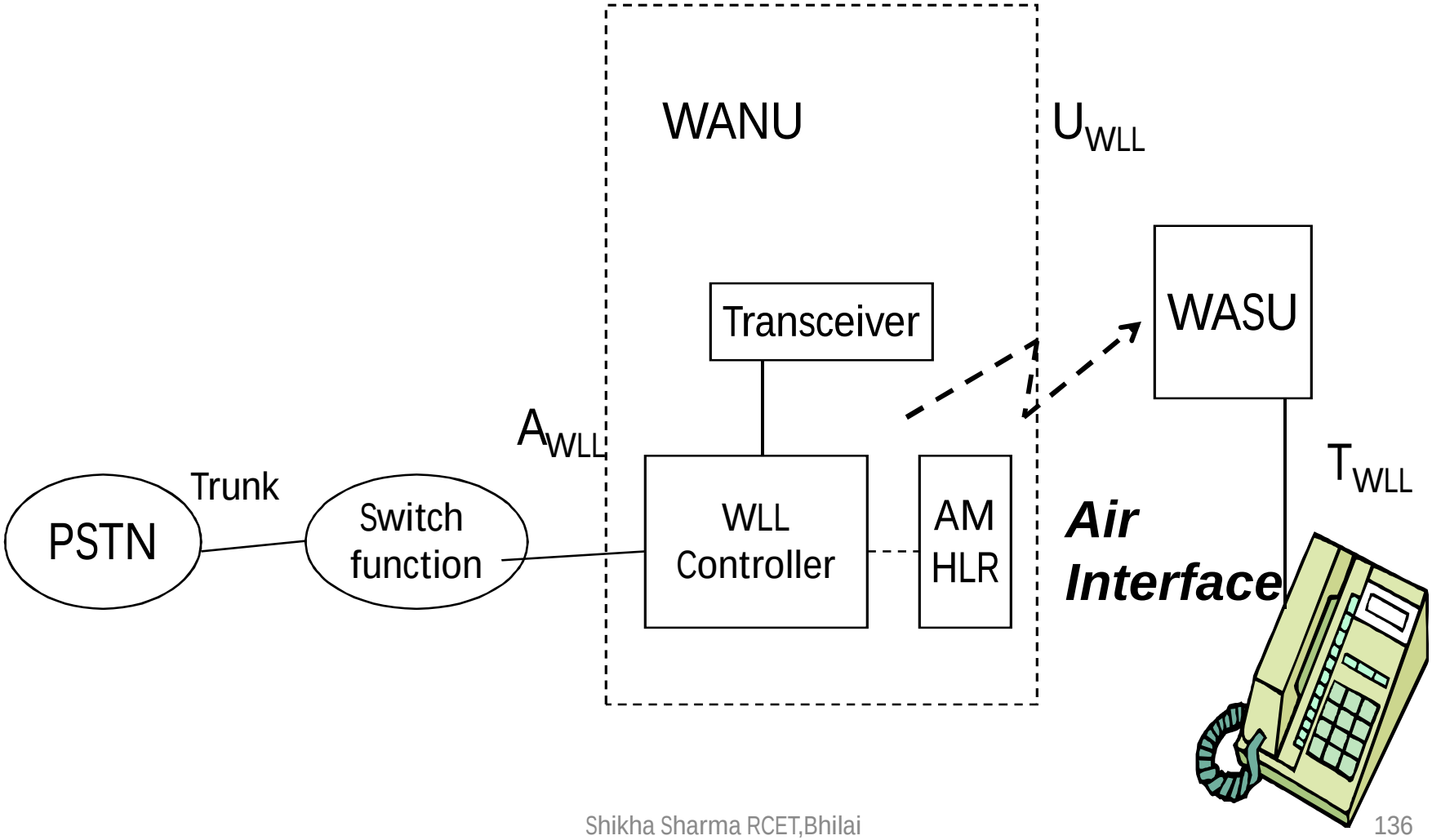
How wireless local loop works

- Wireless local loop phones in homes, offices connect with a wireless system in a manner similar to that of CDMA cell phones. The difference is that WLL phones usually stay in a relatively fixed location.
- WLL phones often connect to AC current rather than using batteries.
- The telephone company will install a small antenna on the customer's building, the size and shape of which will not require planning permission to be obtained.
- Direct line of sight is required between the customer antenna and the nearest base station antenna.



WLL Configuration

WLL Architecture



WLL Architecture

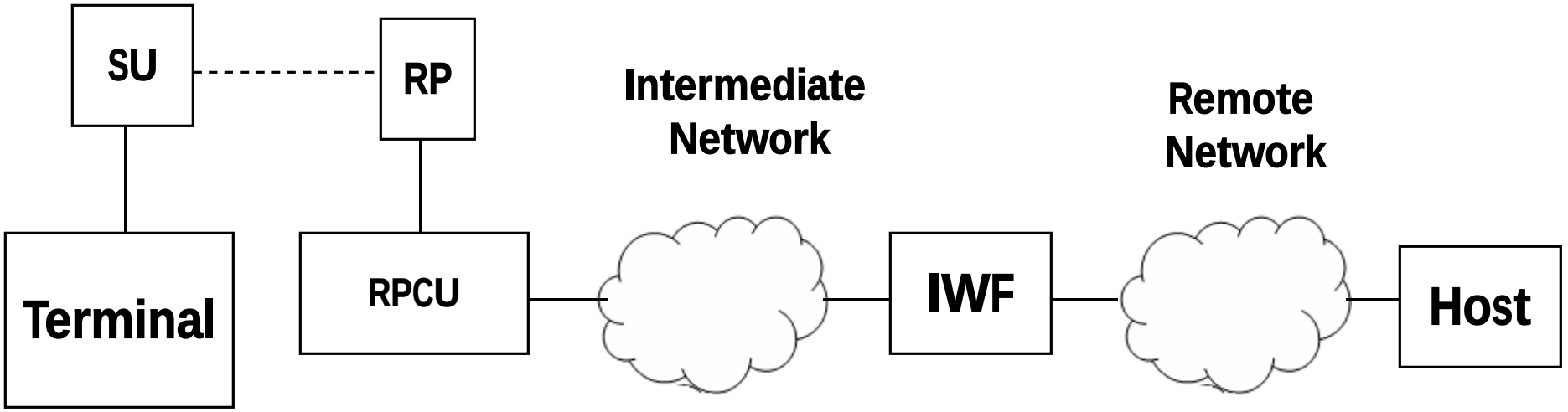
- The architecture consists of three major components:
  - Wireless Access Network Unit (WANU)
  - Wireless Access Subscriber Unit (WASU)
  - Switching Function (SF)

WLL Architecture

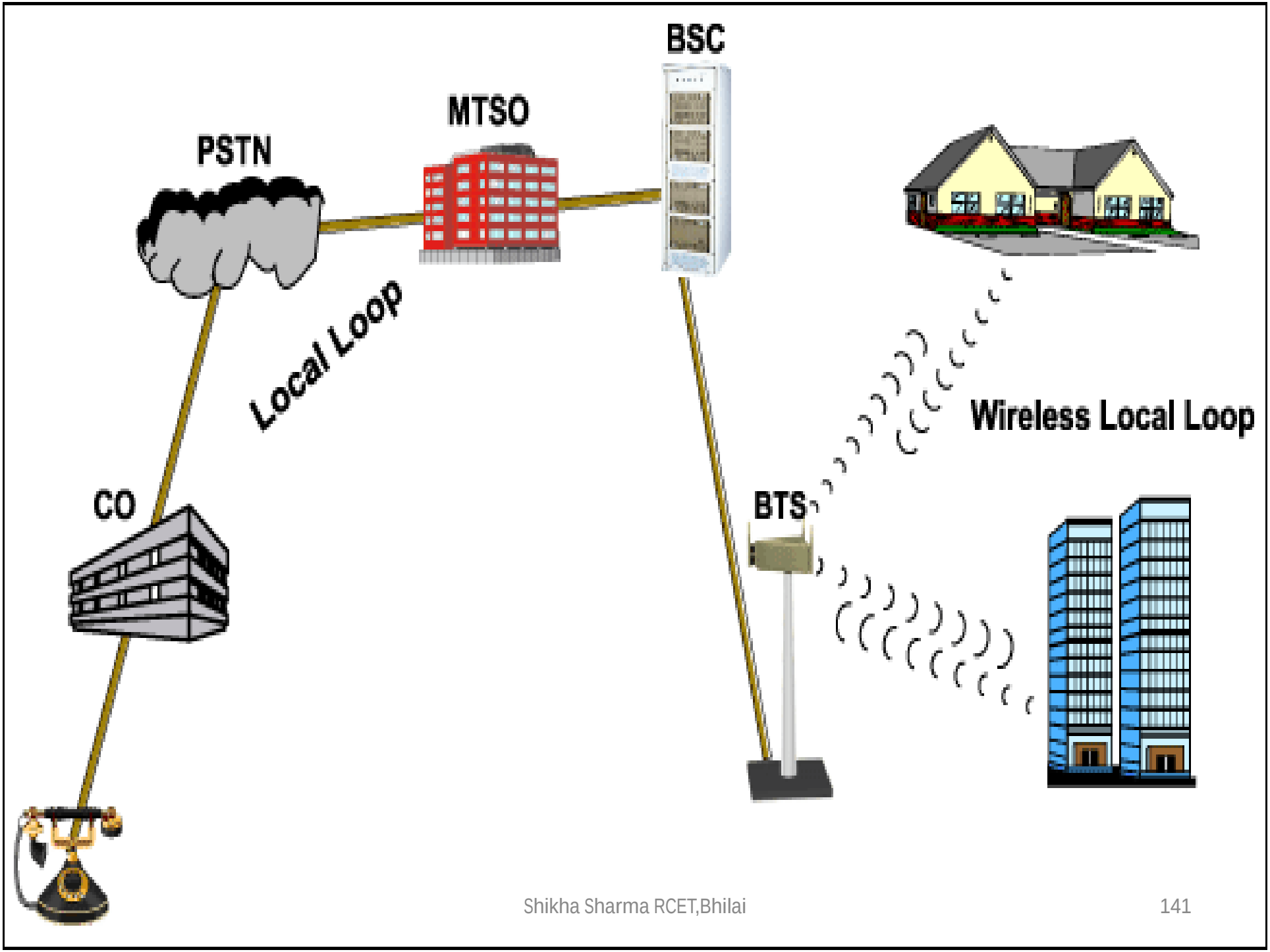
- **Wireless Access Network Unit (WANU)**
  - Interface between underlying telephone network and wireless link
  - consists of
    - Base Station Transceivers (BTS)
    - Radio Ports (RP)
    - Radio Port Controller Unit (RPCU)
    - Access Manager (AM)
    - Home Location Register (HLR)
- **Wireless Access Subscriber Unit (WASU)**
  - located at the subscriber
  - translates wireless link into a traditional telephone connection

- Wireless local loop (WLL)
  - Narrowband – offers a replacement for existing telephony services
  - Broadband – provides high-speed two-way voice and data service

WLL Architecture



Generalized network architecture for wireless-to-wireline data interworking


BSC
MTSO
PSTN
Local Loop
Wireless Local Loop
CO
BTS

Services delivered over WLL

- Wireless Local Loop, offers a range of services up to a maximum of 6Mbs
  - IP Line - always-on Internet access.
  - Leased line to connect 2 sites for example for LAN Interconnect and Video Conferencing.
  - Frame Relay - for data networks between multiple sites.
  - ISDN (PRI) - 30 digital channels which can be used for voice, Internet or voice conferencing.

Wireless Local Loop Technologies

- Systems WLL is based on:
  - Satellite-Based Systems
  - Cellular-Based Systems

WLL OAM Management Functions

- WLL-OAM describe the WLL Operation, Administration and Maintenance functions.
- Written in 35,000 lines of C++ code, WLL-OAM provides the OAM services necessary to control and monitor the equipment in a DECT WLL system.
- The network elements managed by WLL-OAM are:
  - WANU, including the base station controller (BSC) and radio base station (RBS)
  - WASU, called radio network termination (RNT)
  - Customer premise equipment (CPE; e.g., a telephone set) connected to the RNT.

Transmission Mechanism on Air Interface

- WLL standard specifies two modes of operation, one targeted to support a continuous transmission stream (mode A), such as audio or video, and one targeted to support a burst transmission stream (mode B), such as IP-base traffic.

Bursty Data Transmission - Upstream and Downstream

- In upstream and downstream direction, data (burst data) transmission uses a DAMA-TDMA (**demand assignment multiple access – time division multiple access**) technique.

Voice and Video Transmission - Downstream and Upstream

- For voice and video transmission FAMA-FDMA **(fixed assignment multiple access—frequency division multiple access)** scheme is used.
- This is equivalent to a FDD (frequency division duplex).
- FDD simply means that a different frequency band is used for transmission in each direction.
- FDD implies that all subscribers can transmit and receive simultaneously, each on their own assigned frequencies.

Voice and Video Transmission - Downstream and Upstream

- There are also some other methods that can be used:
- **Time Division Duplexing (TDD):** A TDMA frame is used, with part of the time allocated for upstream transmission and part for downstream transmission.
- **FDD with adaptive modulation:** This is the same FDD, but with a dynamic capability to change the modulation and error correction schemes.

Propagation Considerations for WLL

- For most high speed WLL schemes, frequencies in what is referred to as the millimeter wave region are used.

- Frequencies above 10 GHz up to about 300 GHz, are considered to be in the millimeter wave region.

Atmospheric Absorption

- Radio waves at frequencies above 10 GHz are subject to molecular absorption
  - Peak of water vapor absorption at 22 GHz
  - Peak of oxygen absorption near 60 GHz
- Favorable windows for communication:
  - From 28 GHz to 42 GHz
  - From 75 GHz to 95 GHz

Effect of Rain

- Attenuation due to rain
  - Presence of raindrops can severely degrade the reliability and performance of communication links
  - The effect of rain depends on drop shape, drop size, rain rate, and frequency
- Estimated attenuation due to rain:

$$A = aR^b$$

  - A = attenuation (dB/km)
  - R = rain rate (mm/hr)
  - a and b depend on drop sizes and frequency

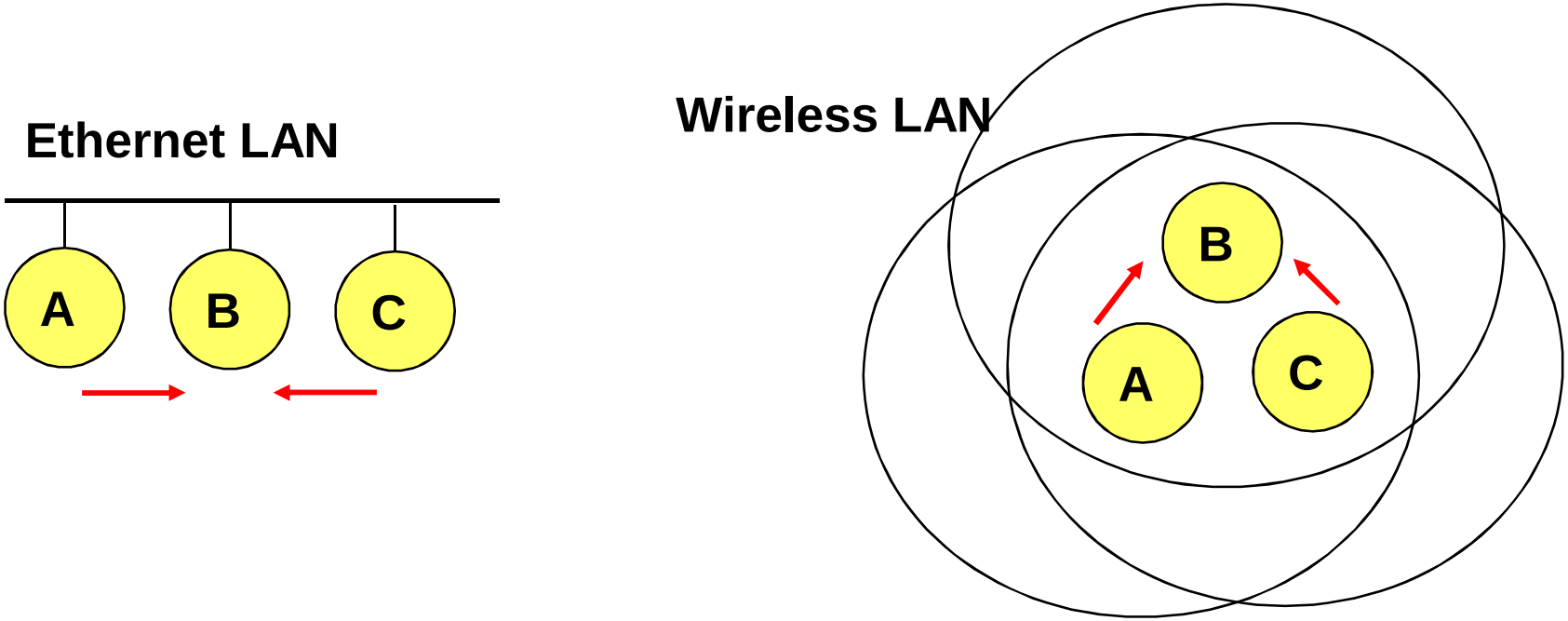
Comparison

WLL	Mobile Wireless	Wireline Local Loop
Narrow beam directed antennas	Omni directional antennas	Expensive wires
High Channel reuse	Less Channel reuse	Reuse Limited by wiring
Simple design	Expensive to design, build, power control	Expensive to build and maintain
Low in-premises mobility, easy access	High mobility allowed, easy access	Low in-premises mobility, wiring of distant areas cumbersome
Weather conditions effects, not very reliable	Weather conditions effects, Not very reliable	Very reliable

MACAW

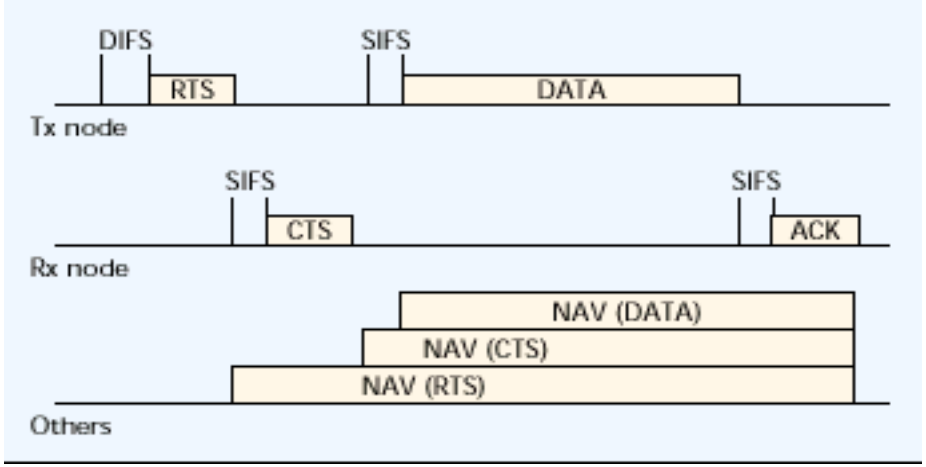
Multiple Access with Collision Avoidance for Wireless

Difference Between Wired and Wireless



- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected at sender in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

CSMA/CA Protocol



Before making an RTS : Distributed Inter-Frame Space(DIFS)

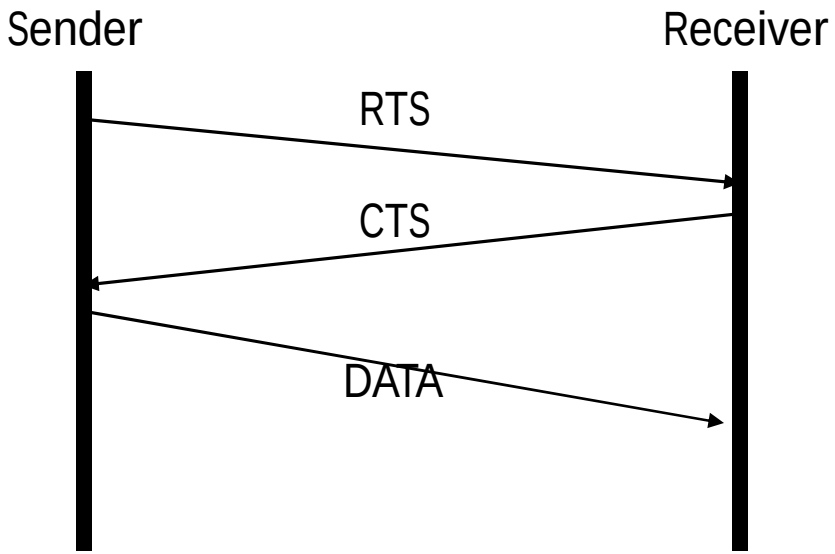
Before sending an ACK : Short Inter-Frame Space(SIFS)

Network Allocation Vector(NAV)

; virtual carrier sensing

CSMA/CA

- Using short, fixed size signaling packets
  - Request-to-Send(RTS) , Clear-to-Send(CTS)
  - Include the length of the proposed data transmission



MACAW

- New protocol : MACAW
  - MACA + several modifications
  - Enhanced performance
- 4 key observations for MACAW
  - Relevant contention is at the receiver, not the sender
  - Congestion is location dependent
  - For fair media access, learning about congestion levels must be collective
  - Synchronization info. about contention periods is needed

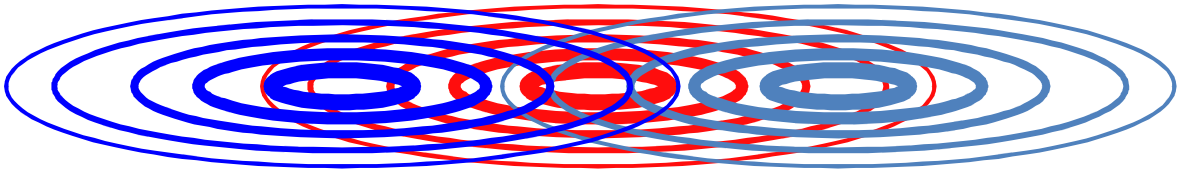
    $\Rightarrow$ all devices can contend effectively

- Multiple Access with Collision Avoidance for Wireless (MACAW) is a slotted MAC protocol widely used in Ad-hoc networks.
- It uses *RTS-CTS-DS-DATA-ACK* frame sequence for transferring data

CSMA/CA

- When a station hears RTS/CTS, but isn't its destination
  - RTS : defer its transmission for CTS time
  - CTS : defer its transmission for data time
- When a station hears RTS but doesn't hear CTS
  - within sender's transmission area, out of receiver's transmission area
  - can start its transmission

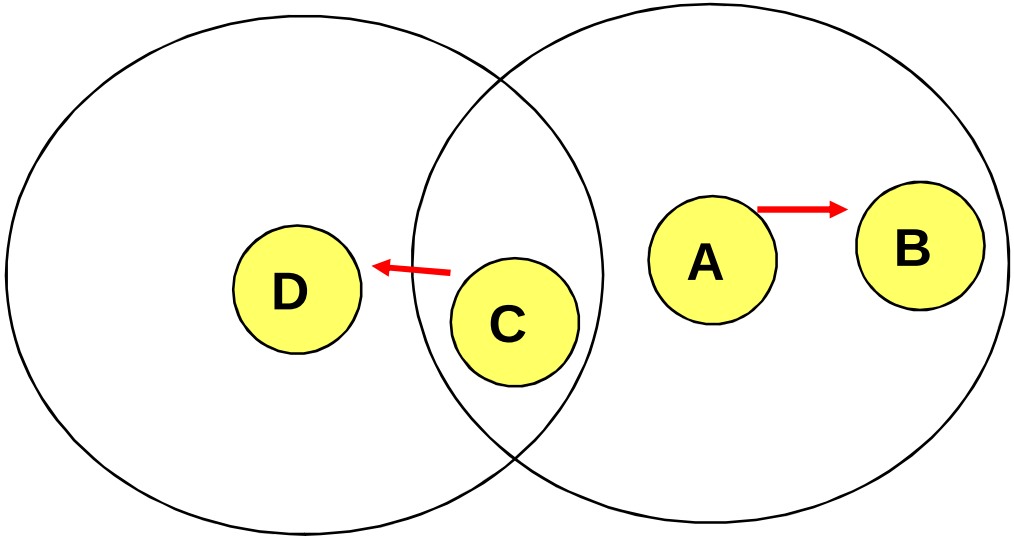
Hidden Terminal Problem



A **B** **C**

- Hidden terminals
  - A and C cannot hear each other.
  - A sends to B, C cannot receive A.
  - C wants to send to B, C senses a “free” medium (CS fails)
  - Collision occurs at B.
  - A cannot receive the collision (CD fails).
  - A is “hidden” for C.
- Solution?
  - Hidden terminal is peculiar to wireless (not found in wired)
  - Need to sense carrier at receiver, not sender!
  - “virtual carrier sensing”: Sender “asks” receiver whether it can hear something. If so, behave as if channel busy.

Exposed Terminal Problem



- Exposed terminals
  - A starts sending to B.
  - C senses carrier, finds medium in use and has to wait for A->B to end.
  - D is outside the range of A, therefore waiting is not necessary.
  - A and C are “exposed” terminals.
- A->B and C->D transmissions can be parallel; no collisions

Principles of operation

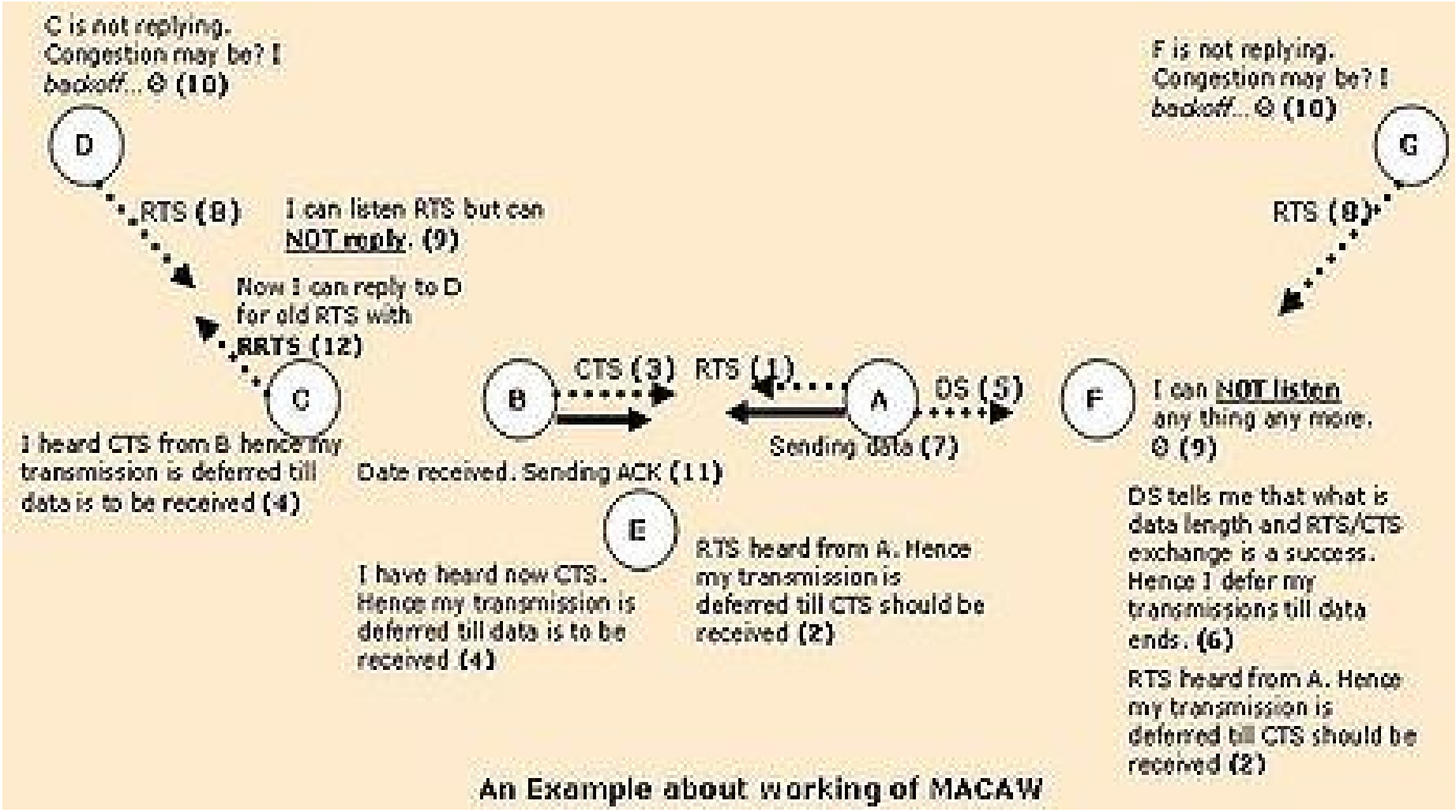
Assume that node A has data to transfer to node B.

1. “Request To send” frame (RTS) from A to B
2. “Clear To Send” frame (CTS) from B to A
3. “Data Sending” frame (DS) from A to B
4. DATA fragment frame from A to B, and
5. Acknowledgement frame (ACK) from B to A.

RRTS:

To summarize, a transfer may in this case consist of the following sequence of frames between node D and C:

1. “Request To send” frame (RTS) from D to C
2. “Request for Request to send” frame (RRTS) from C to D (after a short delay)
3. “Request To send” frame (RTS) from D to C
4. “Clear To Send” frame (CTS) from C to D
5. “Data Sending” frame (DS) from D to C
6. DATA fragment frame from D to C,
7. Acknowledgement frame (ACK) from C to D.



An Example about working of MACAW

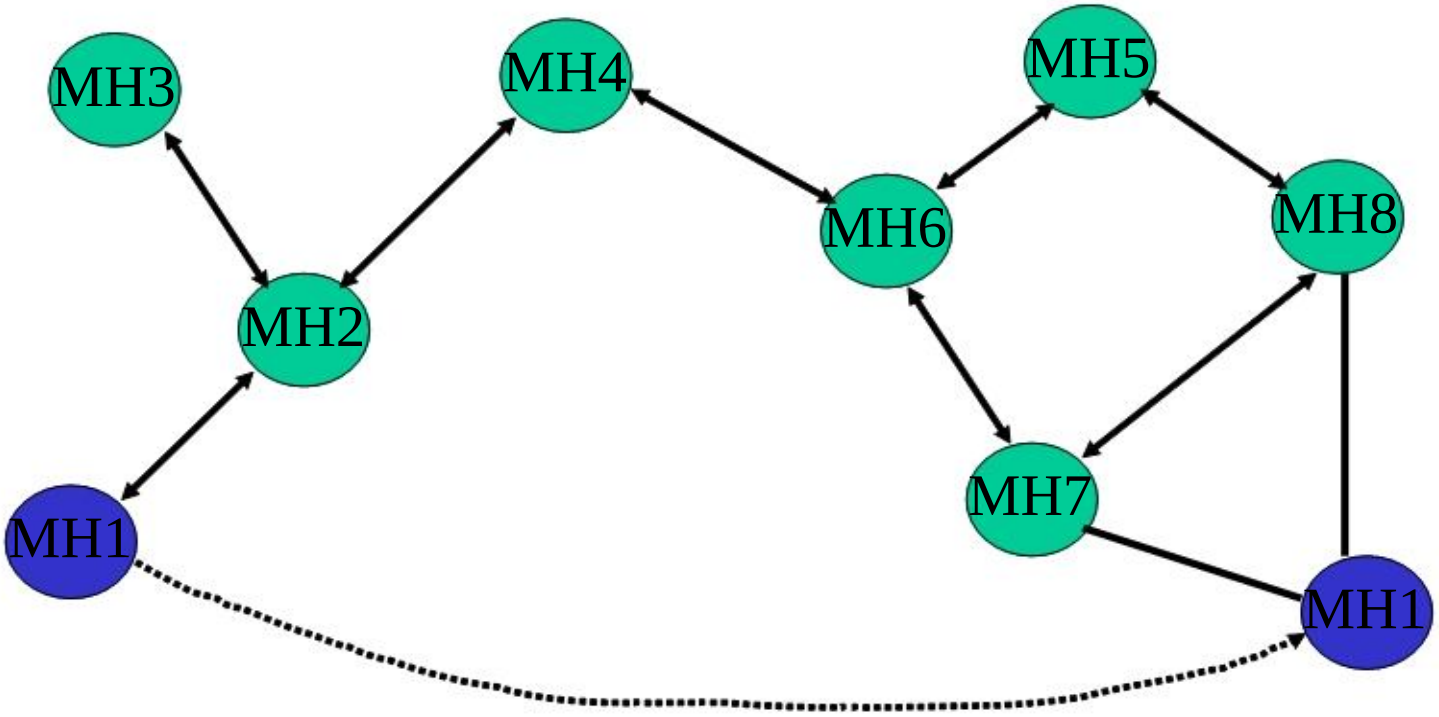
Ad Hoc Networking

1

What is an ad hoc network?

- A short lived network just for the communication needs of the moment.
- Infrastructureless network.

Model of operation



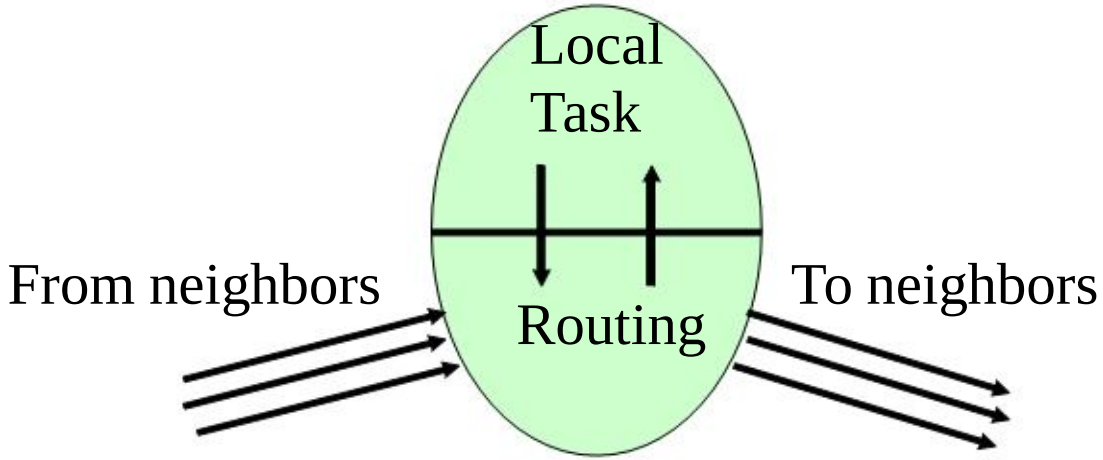
3

Commercial Applications

- Emergency services
  - Damaged infrastructure
  - Difficult to set up infrastructure
- Sensor network

A node in an ad hoc network

Two main components of a node



5

Routing methods

- Idea
  - Each node maintains a table of routing information.
  - Table entry: destination X preferred neighbor.
  - Data packet contains a destination ID in header.
  - Packet received: forward packet to the preferred neighbor.
  Use table entry for the destination.

Routing method

- Manner in which route tables are constructed, maintained and updated.

6

Routing methods

- Two routing algorithms on fixed networks
  - Distance-Vector (DV)
  - Link state
- Destination-Sequenced Distance Vector (DSDV)
- Dynamic Source Routing
- Location Aided Routing

Two routing algorithms for fixed networks

Distance Vector (RIP: Routing Info. Protocol)
Link State (OSPF: Open Shortest Path First)

8

Distance Vector

- Distributed Bellman-Ford algorithm
  - Node i maintains, for each dest x, a set of distances $\{d_{ij}(x)\}$, where j is a neighbor of i.
  - Node i treats neighbor k as a next hop for a packet for x if $d_{ik}(x) = \min_j\{d_{ij}(x)\}$.
  - To keep $\{d_{ij}(x)\}$ up to date,
    - Node i monitors the cost of its outgoing links. - Periodically broadcast your estimate of the shortest distance to every other node.

Distance Vector (contd.)

- Advantages: efficient, easier to implement, less storage.
- Drawback: short/long-lived loops. ☹ dist, stale info

- Ad hoc networks ☹ rapid topological changes ☹loops.

10

Link State

- Each node has a view of the net topology, link cost.
- For consistent view

- Each node periodically broadcasts outgoing link costs. -

Based on received info, nodes update their view of net. •
Apply shortest-path algorithm to choose its next hop for each destination.

DSDV Routing Algorithm

(Enhancement of DV routing)

DSDV Protocol Overview

- Each node constructs and maintains a route table.
- Route table entry:

Destination (available)	Next hop	# of hops	Sequence #

Sequence #: originated by the destination node.

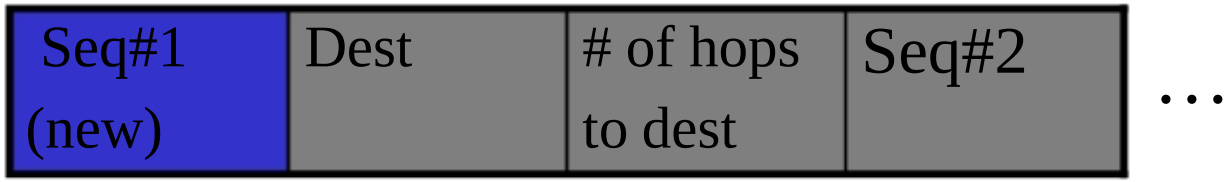
13

Overview (contd.)

- To maintain consistency of route tables, each node
  - Periodically transmits updates.
  - Transmits immediately when significant new info is available.
- Update information consists of
  - Which nodes are accessible from the node. -
  Number of hops necessary to reach them. -
  (Sequence #)

Route Advertisement

- For consistency, each node periodically transmits updates to its current neighbors.
- An update packet indicates which nodes are accessible from the sender and the number of hops to reach them.
- Structure of a packet broadcast by each node



15

Route selection criteria

- When a node receives info. about a new route to a node

  -Compare it to existing info. of a route to the same node. - A route with a more recent sequence number is used. - A route with an identical sequence number is used if it has a better metric. (The existing route is discarded or saved as a less preferable route.)

  - The metrics for routes chosen from the newly received broadcast info are each incremented by one hop.

Responding to topology change

- What is a topology change?

  - Discover a new node. ∅ from a received advertisement - Broken link with a neighbor.

    » No communication from neighbor for a long time.

- What to do immediately: Update route table

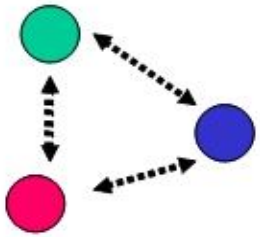
  - Assign an infinity metric to that destination. - Assign a new sequence number. (last seq # received from that node + 1)

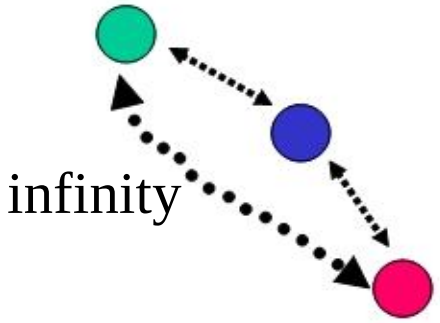
- What to do next because of this substantial change:

  - Disclose this new info in a broadcast packet.

Responding to topology change

- When a node receives an infinity metric and it has a "=" or ">" sequence # with a finite metric
  - Trigger a route update broadcast.





18

Responding to topology change

- To reduce amount of info in broadcast packets, two types of broadcasts:

  - Full dump: All available routing info., periodic - Incremental: Info changed since last full dump

Route selection criteria (contd.)

- Should you make an advt. after every change?
- Yes ৷ Continuing burst of new transmittals. • Solution
  - Delay the advertisement activity -
    Maintain two tables
    - » One for routing »
      One for advertising
- Note: Don’t delay advt. of infinity metric.

Dynamic Source Routing

It is the responsibility of the source to find and maintain routes.

Source Routing

• The source of a packet determines the complete sequence of nodes (i.e. the route) for the packet.

• The route is put in the packet's header.

• There is no periodic route advertisement.

• When a node needs one, it dynamically determines one based on

- Cached information
- Results of a route discovery protocol

Basic Operation

- To send a packet, construct a source route in the packet header.
- The sender transmits the packet to the first node on the route.
- When a node receives a packet, if it is not the final destination, it simply transmits the packet to the next node on the route.
- When a source wants to send a packet to another node, it first checks its route cache.
  - If a route is found, use the route.
  - If no route is found, attempt to discover one.
- Each node maintains a route cache in which it caches source routes that it has learned.

Route Discovery (find a route)

- A host initiating a route discovery broadcasts a route request (RR) packet (to all its neighbors).
  - RR header = Sequence#, source, destination.

• A node receiving an RR packet further broadcasts it if it is NOT the destination, after inserting its ID in the RR header. ☜ Incrementally construct a route. • If the destination receives an RR, it sends a route reply packet containing the route (sequence of nodes from the source to the destination).

Route Discovery (efficiency)

• Each node maintains a list of

<source address, RRseq. #> for all sources • When a node receives a route request, it does this:

- If the pair <source ad. RRseq. #> from the RR is already on the above list, discard the packet.
- If the node's address is already in the route record in the request, discard the packet.
- If the target of the request matches this node's address, send a route reply.
- Else, insert this node's own address in the route record, and rebroadcast the packet.

Route Maintenance

- While a route is in use, a route maintenance procedure monitors the operation of the route and informs the sender of any routing error.
  - Wireless networks generally utilize hop-by-hop ACK. If the data-link layer in a node on a route reports a problem, the node sends a route error packet to the original sender. - When a route error packet is received, the hop in error is removed from this node's route cache, and all routes which contain this hop must be truncated at this point. - If link-level error detection is not available, you may use the idea of passive ACK (i.e. being able to hear that node transmitting the packet again.)
  - Worst case: Ask for an explicit ACK.

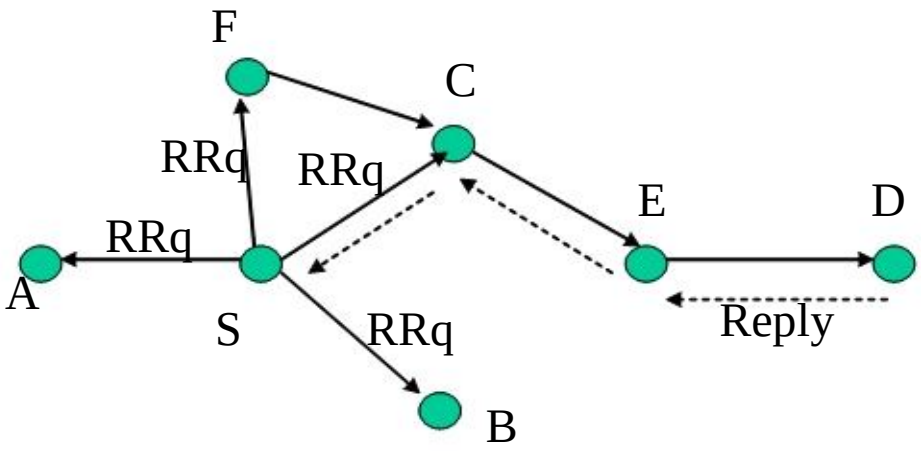
Location Aided Routing (LAR)

1. Obtain location information from a GPS receiver
2. Utilize location information to improve the performance of routing protocols

Basic Idea

- Host mobility causes topology change
  - Task of DISCOVERING and maintaining routes is non-trivial
- Flooding is a brute force way of discovering routes.
- LAR: Reduces the full impact of flooding by forwarding route discovery messages in a selective manner by using location information.

Route discovery using flooding



S: Source
D: Destination

29

Route discovery using flooding

- A sender broadcasts a route request (RRq) to all its neighbors
- If a node is not the destination of an RRq, it broadcasts the RRq. (Subsequent copies of an RRq are not broadcast again. Thus, save recent <Sender, sequence #> pairs).
- The destination sends a reply back to the sender.

The reply takes the reverse path taken by the RRq. • If the sender does not receive a reply within a certain timeout period, it reinitiates the process.

LAR: Preliminaries

- Assumptions

  - Node S needs to find a route to D.
  - S knows D's location "L" at time t0. - Current time is t1.

- Expected Zone of D from the viewpoint of S at t1

  - This is the region that S expects to contain D at time t1.

    - Initially, the entire network area is the expected zone. - Having more information regarding mobility of a destination node can result in a smaller expected zone.

LAR: Preliminaries

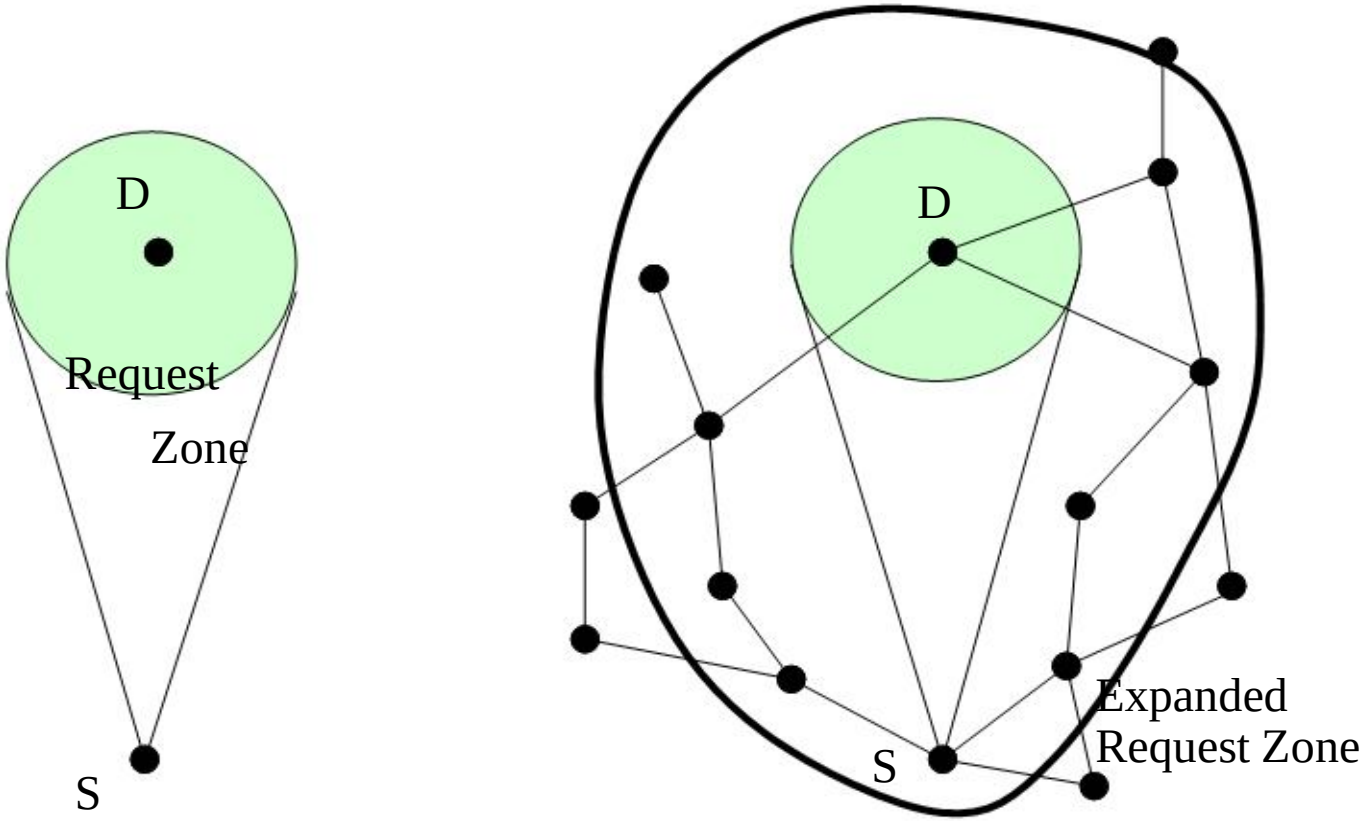
- Request Zone

  - Node S (sender) defines a request zone for the route req. - A node forwards a route request only if it lies in the request zone.

  - To increase the probability that the route request will reach node D, the request zone includes the expected zone. - Additional regions must be included in the request zone so that S and D belong to the request zone.

  - If a route is not discovered within a suitable time period, S reinitiates route discovery with an EXPANDED request zone.

Request Zone



Tradeoff between probability of finding a route and discovery overhead.

The LAR Algorithm

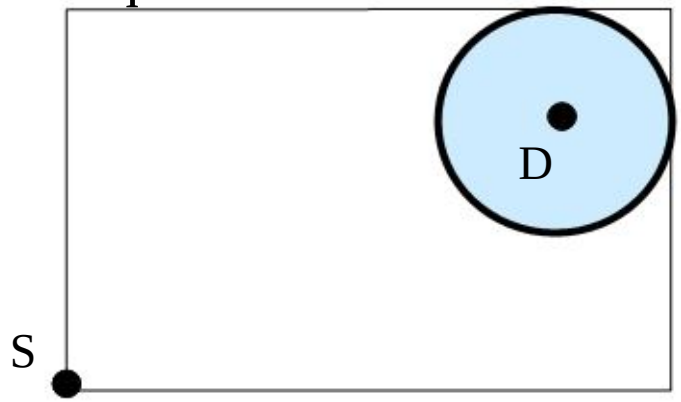
- It is the FLOODING algorithm.
- A node that is NOT in the request zone does not forward a route request to its neighbors.

Two ways of computing a Request Zone

- LAR Scheme 1
- LAR Scheme 2

LAR Scheme 1

- A request zone is the smallest rectangle that includes the current location of S and the expected zone of D, such that the sides of the rectangle are parallel to the X- and Y-axis.
- The source explicitly specifies the request zone in its route request.



When D receives a Route request, it sends a route reply which includes its current location and the current time.

LAR Scheme 2

- Sender S includes these info with a route request.
  - DISTS : Distance of S from D
  -(Xd, Yd): Coordinates of D
- When a node I receives the route request from S, I calculates its distance DISTI from D and acts as follows:

- If DISTS + ™>= DISTI I forwards the request to its neighbors after replacing DISTS with DISTI . - If DISTS + δ< DISTI I discards the request. • Idea: A node (I) forwards a request forwarded by another node (S), if I is “at most δ farther”.