Mobile Internet

Wireless Network Architectures and Applications

Sridhar Iyer

K R School of Information Technology

IIT Bombay

sri@it.iitb.ac.in

http://www.it.iitb.ac.in/~sri

Outline

- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- TCP over wireless
- GSM air interface
- GPRS network architecture
- Wireless application protocol
- Mobile agents
- Mobile ad hoc networks

References

- J. Schiller, "Mobile Communications", Addison Wesley, 2000
- 802.11 Wireless LAN, IEEE standards, www.ieee.org
- Mobile IP, RFC 2002, RFC 334, www.ietf.org
- TCP over wireless, RFC 3150, RFC 3155, RFC 3449
- A. Mehrotra, "GSM System Engineering", Artech House, 1997
- Bettstetter, Vogel and Eberspacher, "GPRS: Architecture, Protocols and Air Interface", IEEE Communications Survey 1999, 3(3).
- M.v.d. Heijden, M. Taylor. "Understanding WAP", Artech House, 2000
- Mobile Ad hoc networks, RFC 2501

- Others websites:
  - www.palowireless.com
  - www.gsmworld.com; www.wapforum.org
  - www.etsi.org; www.3gtoday.com

Wireless networks

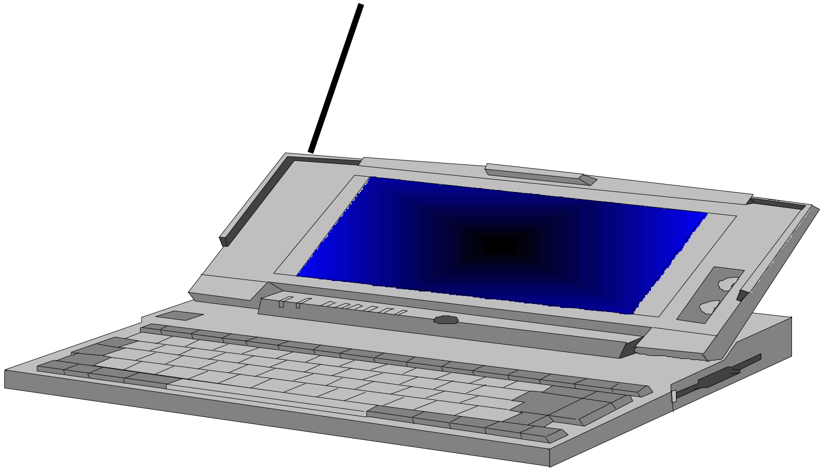
- Access computing/communication services, on the move
- Cellular Networks
  - traditional base station infrastructure systems
- Wireless LANs
  - infrastructure as well as ad-hoc networks possible
  - very flexible within the reception area
  - low bandwidth compared to wired networks (1-10 Mbit/s)
- Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - military applications, rescue, home networking

Some mobile devices

Palm-sized

Tablets

Clamshell handhelds



Laptop computers

Net-enabled mobile phones

Limitations of the mobile environment

- Limitations of the Wireless Network
  - limited communication bandwidth
  - frequent disconnections
  - heterogeneity of fragmented networks

- Limitations Imposed by Mobility
  - route breakages
  - lack of mobility awareness by system/applications

- Limitations of the Mobile Device
  - short battery lifetime
  - limited capacities

Wireless v/s Wired networks

- Regulations of frequencies
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- Bandwidth and delays
  - Low transmission rates
    - few Kbits/s to some Mbit/s.
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to interference, e.g., engines, lightning
- Always shared medium
  - Lower security, simpler active attacking
  - radio interface accessible for everyone
  - Fake base stations can attract calls from mobile phones
  - secure access mechanisms important

Cellular systems: Basic idea

- Single hop wireless connectivity
  - Space divided into cells
  - A base station is responsible to communicate with hosts in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station

- Factors for determining cell size
  - No. of users to be supported
  - Multiplexing and transmission technologies

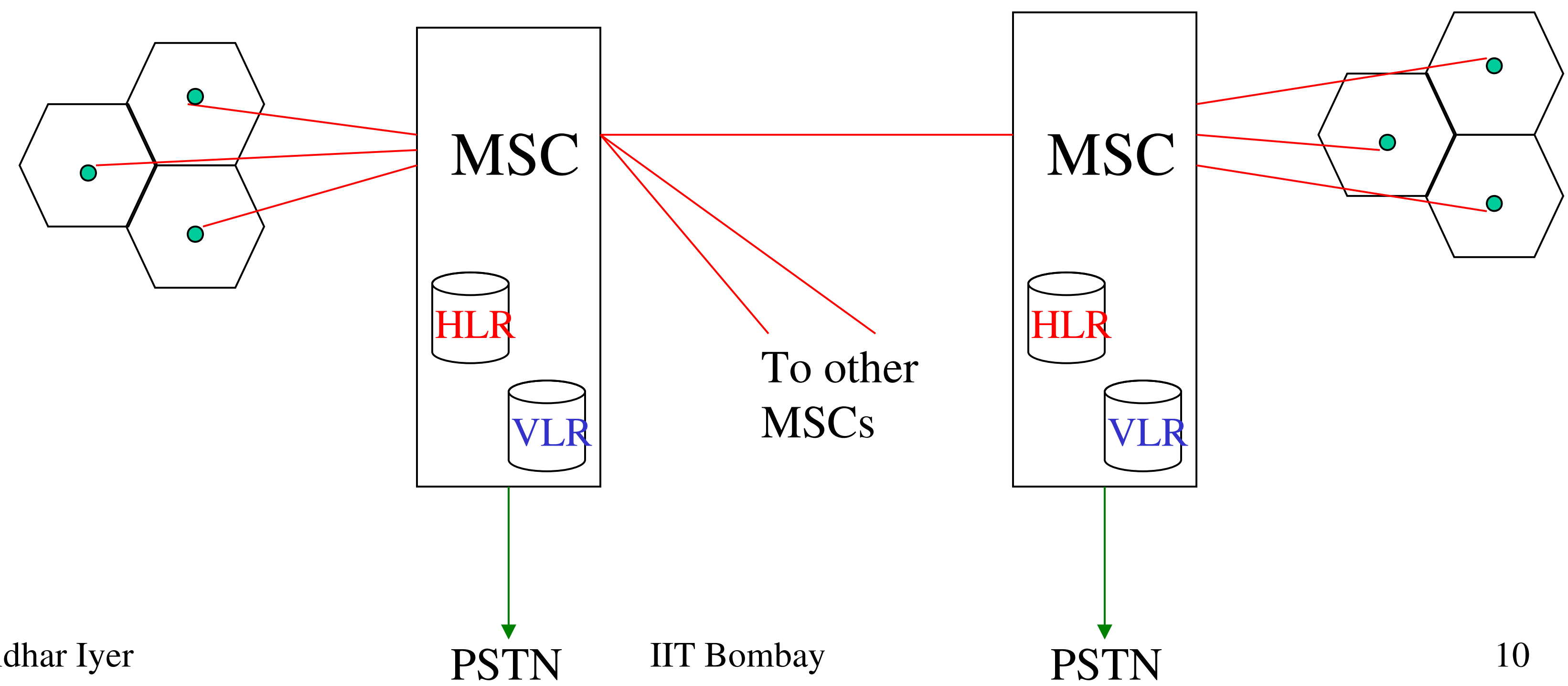
Cellular concept

- Limited number of frequencies => limited channels
- High power antenna => limited number of users
- Smaller cells => frequency reuse possible => more users

- Base stations (BS): implement space division multiplex
  - Cluster: group of nearby BSs that together use all available channels
- Mobile stations communicate only via the base station
  - FDMA, TDMA, CDMA may be used within a cell
- As demand increases (more channels are needed)
  - Number of base stations is increased
  - Transmitter power is decreased correspondingly to avoid interference

Cellular system architecture

- Each cell is served by a base station (BS)
- Each BSS is connected to a mobile switching center (MSC) through fixed links
- Each MSC is connected to other MSCs and PSTN



Outgoing call setup

- Outgoing call setup:
  - User keys in the number and presses send
  - Mobile transmits access request on uplink signaling channel
  - If network can process the call, BS sends a channel allocation message
  - Network proceeds to setup the connection
- Network activity:
  - MSC determines current location of target mobile using HLR, VLR and by communicating with other MSCs
  - Source MSC initiates a call setup message to MSC covering target area

Incoming call setup

- Incoming call setup:
  - Target MSC (covering current location of mobile) initiates a paging message
  - BSs forward the paging message on downlink channel in coverage area
  - If mobile is on (monitoring the signaling channel), it responds to BS
  - BS sends a channel allocation message and informs MSC
- Network activity:
  - Network completes the two halves of the connection

Hand-Offs

- BS initiated:
  - Handoff occurs if signal level of mobile falls below threshold
  - Increases load on BS
    - Monitor signal level of each mobile
    - Determine target BS for handoff
- Mobile assisted:
  - Each BS periodically transmits beacon
  - Mobile, on hearing stronger beacon from a new BS, initiates the handoff
- Intersystem:
  - Mobile moves across areas controlled by different MSC's
  - Handled similar to mobile assisted case with additional HLR/VLR effort

Effect of mobility on protocol stack

- Application
  - new applications and adaptations
- Transport
  - congestion and flow control
- Network
  - addressing and routing
- Link
  - media access and handoff
- Physical
  - transmission errors and interference

Mobile applications - 1

- Vehicles
  - transmission of news, road condition etc
  - ad-hoc network with near vehicles to prevent accidents
- Emergencies
  - early transmission of patient data to the hospital
  - ad-hoc network in case of earthquakes, cyclones
  - military ...

Mobile applications - 2

- Travelling salesmen
  - direct access to central customer files
  - consistent databases for all agents
- Web access
  - outdoor Internet access
  - intelligent travel guide with up-to-date location dependent information
- Location aware services
  - find services in the local environment

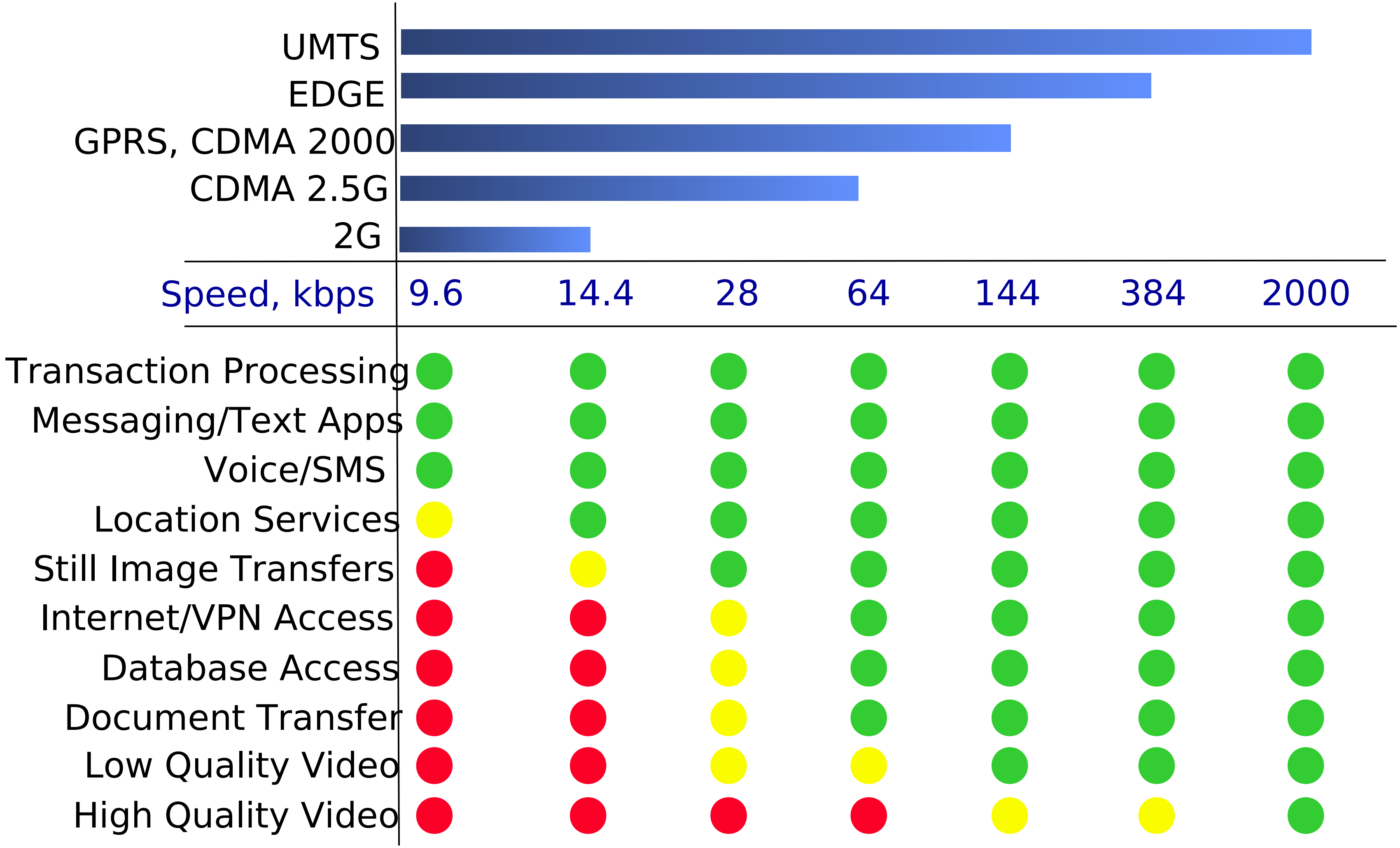
Mobile applications - 3

- Information services
  - push: e.g., stock quotes
  - pull: e.g., weather update
- Disconnected operations
  - mobile agents, e.g., shopping
- Entertainment
  - ad-hoc networks for multi user games
- Messaging

Mobile applications in the Industry

- Wireless access: (phone.com) openwave
- Alerting services: myalert.com
- Location services: (airflash) webraska.com
- Intranet applications: (imedeon) viryanet.com
- Banking services: macalla.com
- Mobile agents: tryllian.com
- ….

Bandwidth and applications



Evolution of cellular networks

- First-generation: Analog cellular systems (450-900 MHz)
  - Frequency shift keying; FDMA for spectrum sharing
  - NMT (Europe), AMPS (US)
- Second-generation: Digital cellular systems (900, 1800 MHz)
  - TDMA/CDMA for spectrum sharing; Circuit switching
  - GSM (Europe), IS-136 (US), PDC (Japan)
  - <9.6kbps data rates
- 2.5G: Packet switching extensions
  - Digital: GSM to GPRS; Analog: AMPS to CDPD
  - <115kbps data rates
- 3G: Full-fledged data services
  - High speed, data and Internet services
  - IMT-2000, UMTS
  - <2Mbps data rates

GSM to GPRS

- Radio resources are allocated for only one or a few packets at a time, so GPRS enables
  - many users to share radio resources, and allow efficient transport of packets
  - connectivity to external packet data networks
  - volume-based charging

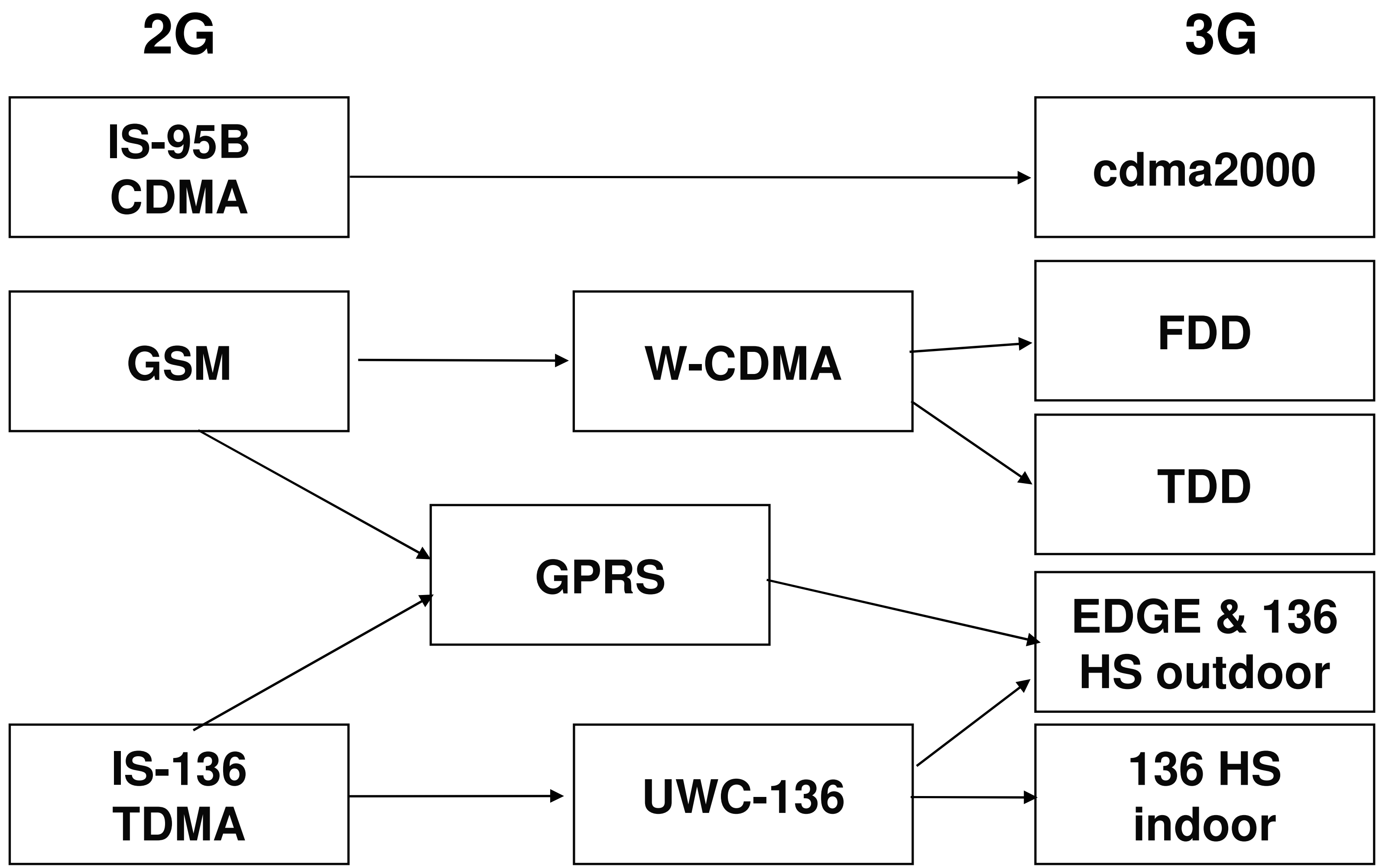
- High data rates (up to 171 kbps in ideal case)
- GPRS carries SMS in data channels rather than signaling channels as in GSM

UMTS: Universal Mobile Telecomm. Standard

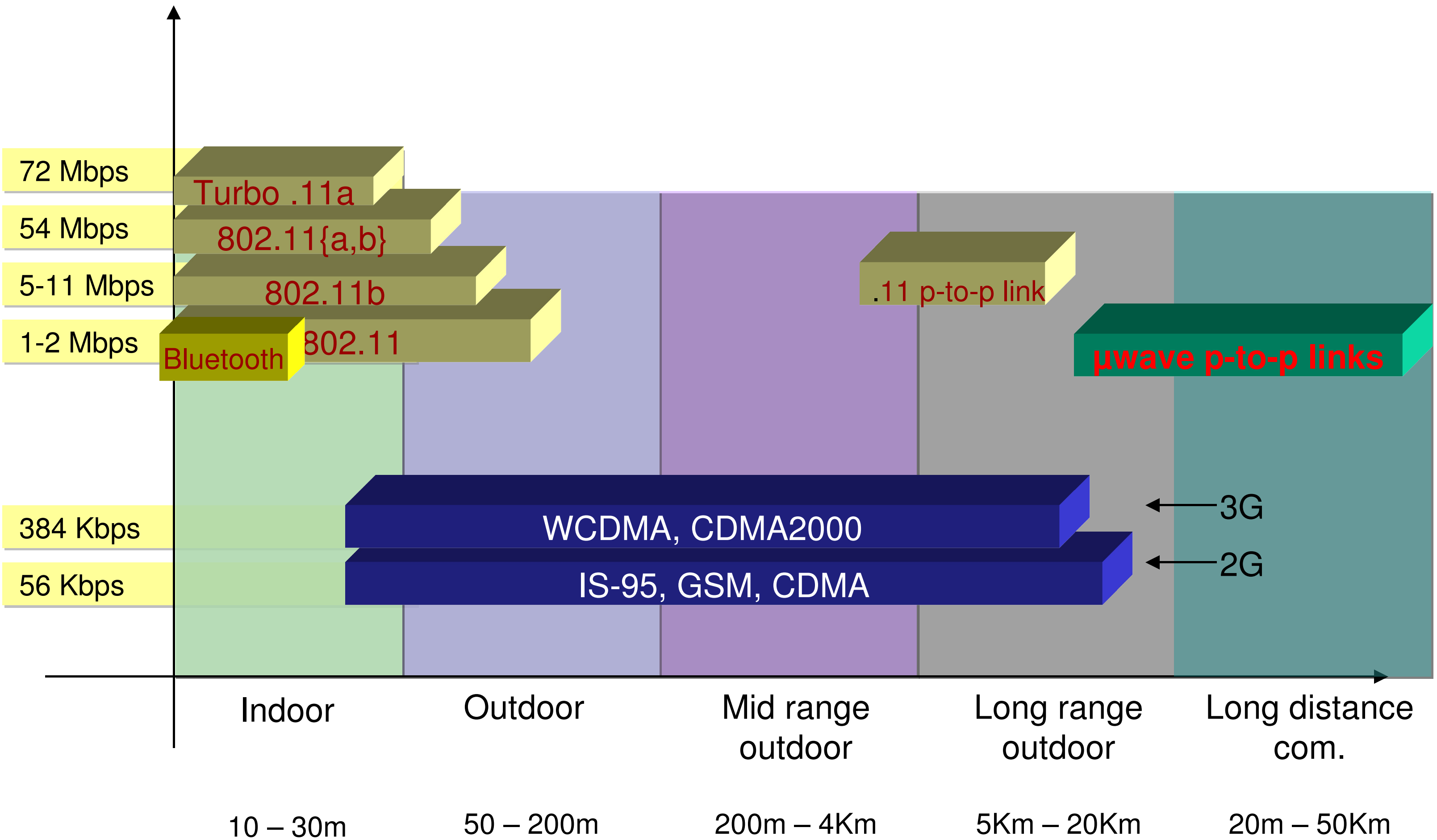
- Global seamless operation in multi-cell environment (SAT, macro, micro, pico)
- Global roaming: multi-mode, multi-band, low-cost terminal, portable services & QoS

- High data rates at different mobile speeds: 144kbps at vehicular speed (80km/h), 384 kbps at pedestrian speed, and 2Mbps indoor (office/home)
- Multimedia interface to the internet
- Based on core GSM, conforms to IMT-2000
- W-CDMA as the air-interface

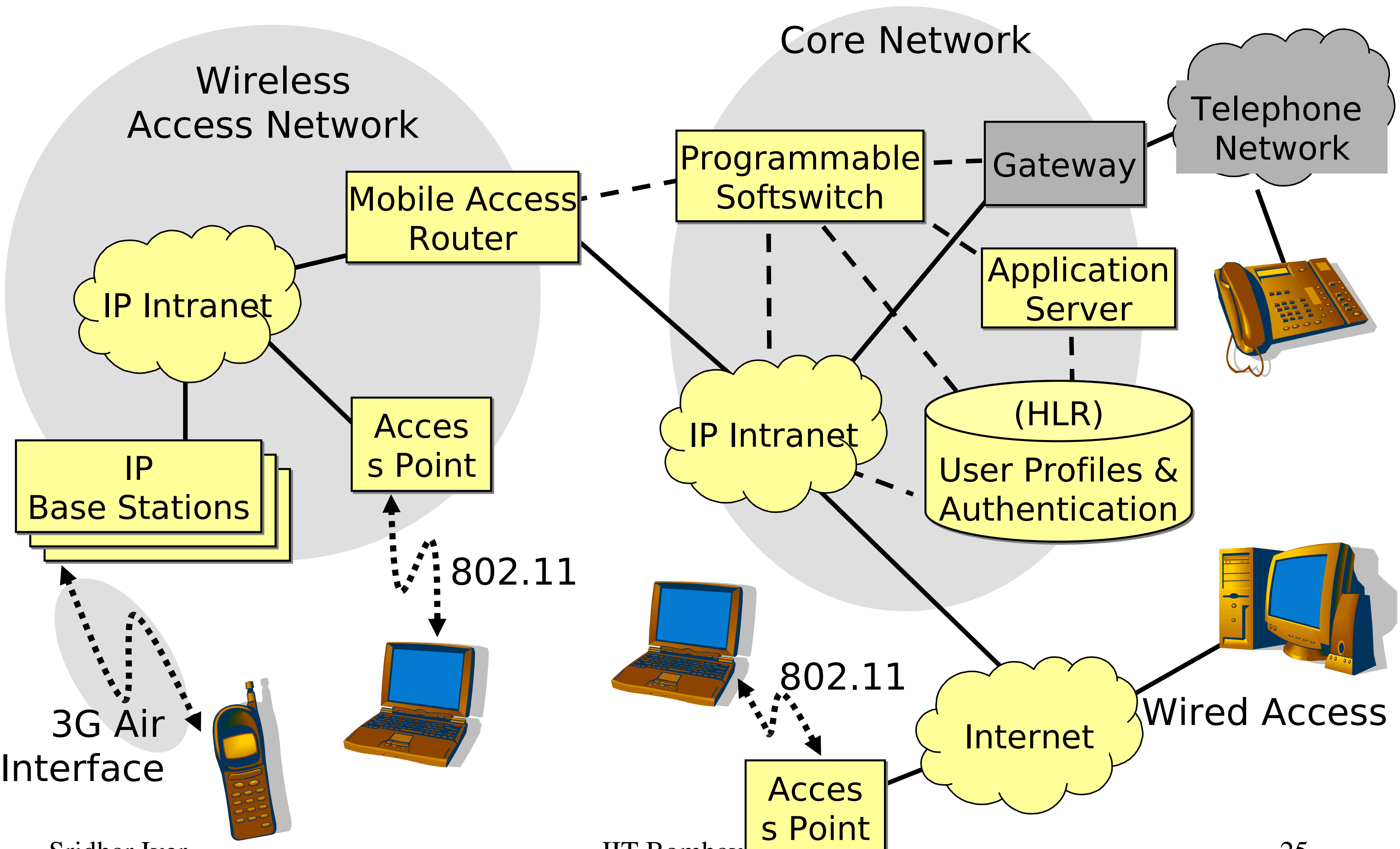
Evolution to 3G Technologies



Wireless Technology Landscape



3G Network Architecture

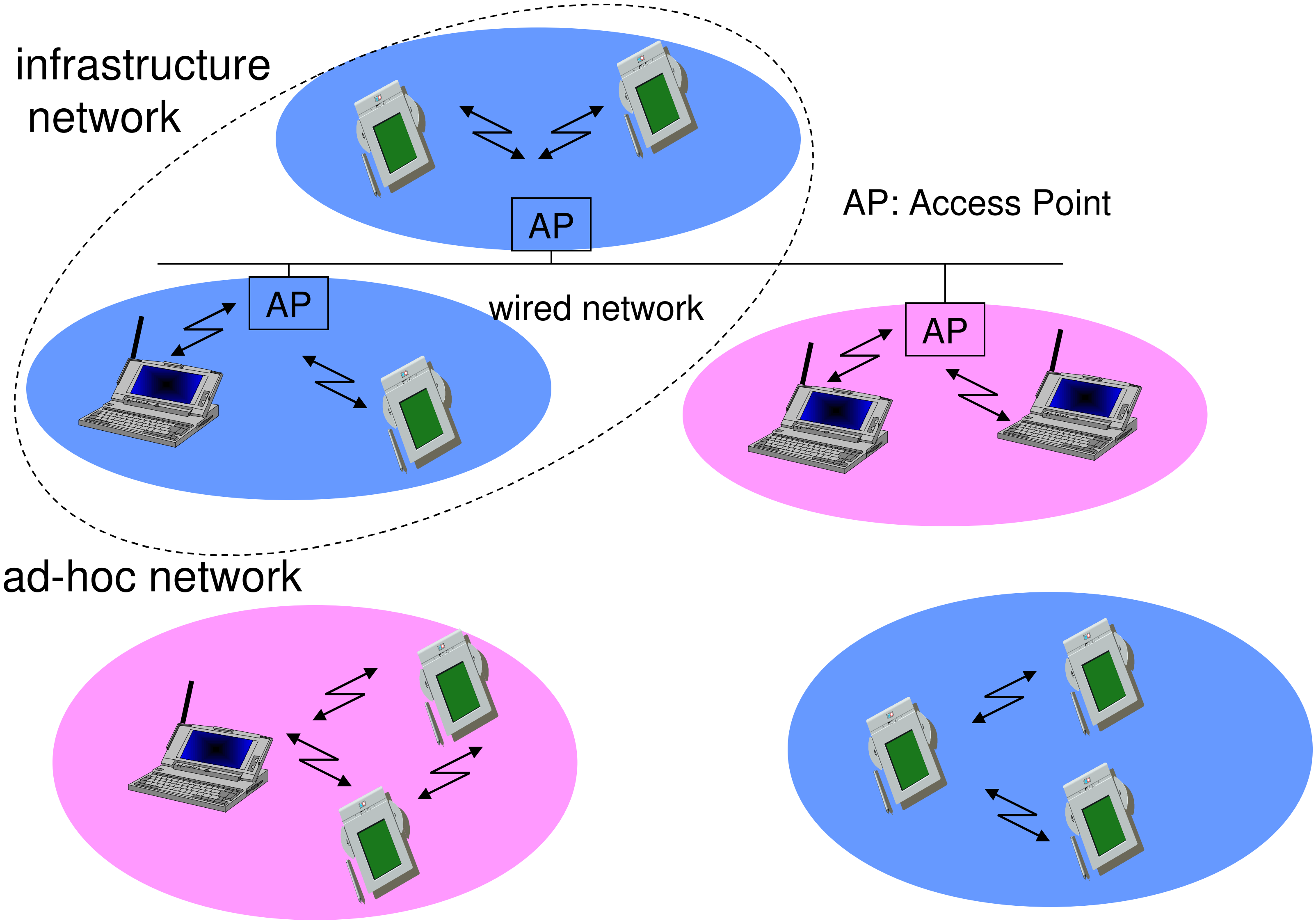


Wireless LANs

- Infrared (IrDA) or radio links (Wavelan)
- Advantages
  - very flexible within the reception area
  - Ad-hoc networks possible
  - (almost) no wiring difficulties
- Disadvantages
  - low bandwidth compared to wired networks
  - many proprietary solutions

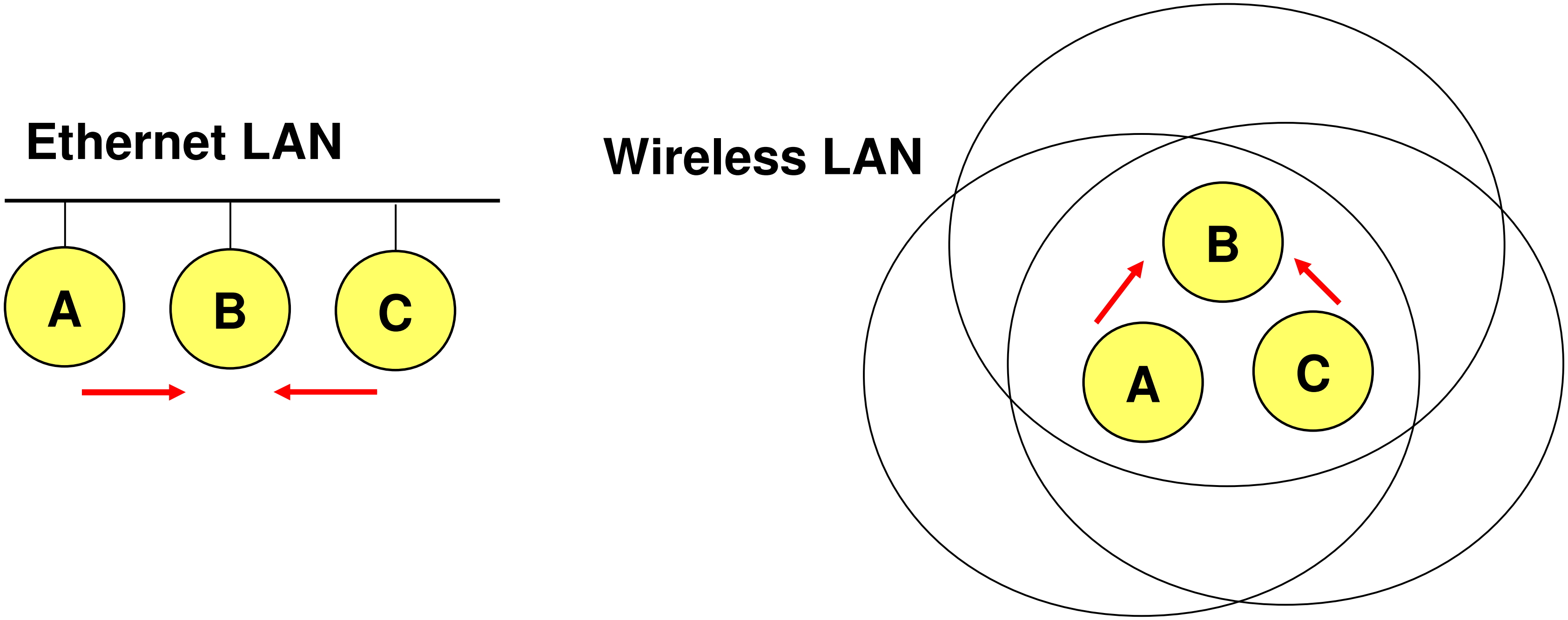
- Infrastructure v/s ad-hoc networks (802.11)

Infrastructure vs. Adhoc Networks



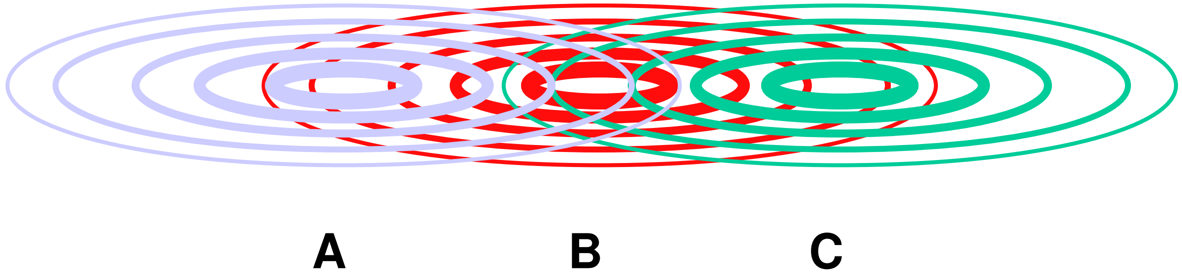
Source: Schiller

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



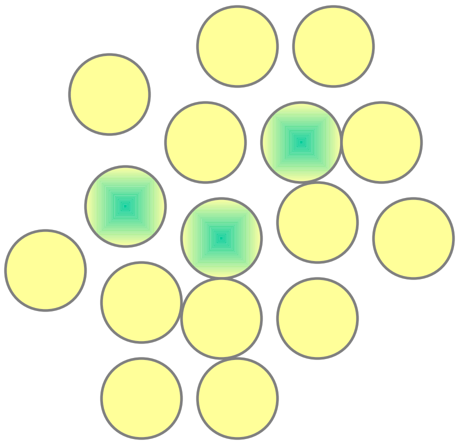
- A and C cannot hear each other.
- A sends to B, C cannot receive A.
- C wants to send to B, C senses a "free" medium (CS fails)
- Collision occurs at B.
- A cannot receive the collision (CD fails).
- A is "hidden" for C.

IEEE 802.11

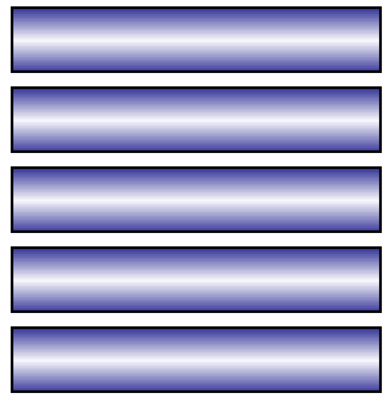
- Acknowledgements for reliability
- Signaling packets for collision avoidance
  - RTS (request to send)
  - CTS (clear to send)
- Signaling (RTS/CTS) packets contain
  - sender address
  - receiver address
  - duration (packet size + ACK)
- Power-save mode

Spectrum War: Status today

Enterprise 802.11 Network



Wireless Carrier



Public 802.11

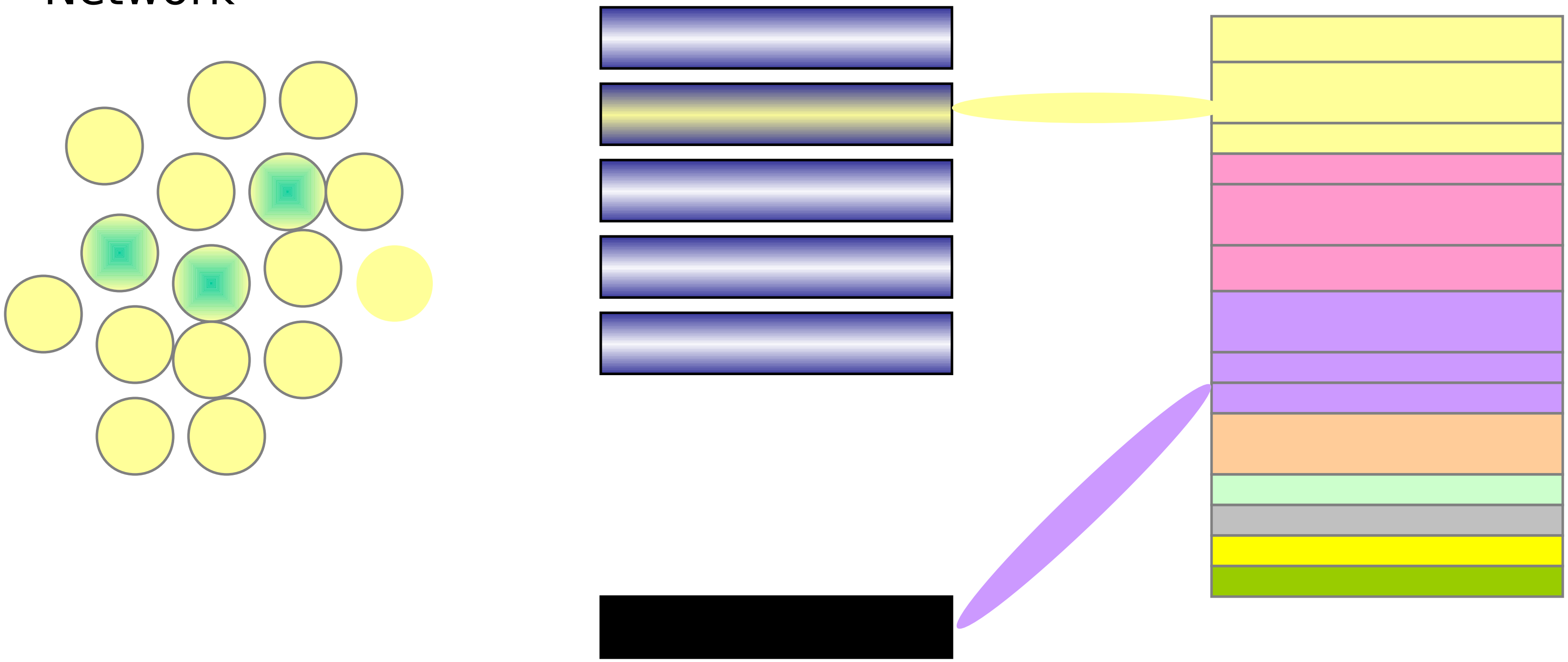
Source: Pravin Bhagwat

Spectrum War: Evolution

Enterprise 802.11 Network

Wireless Carrier

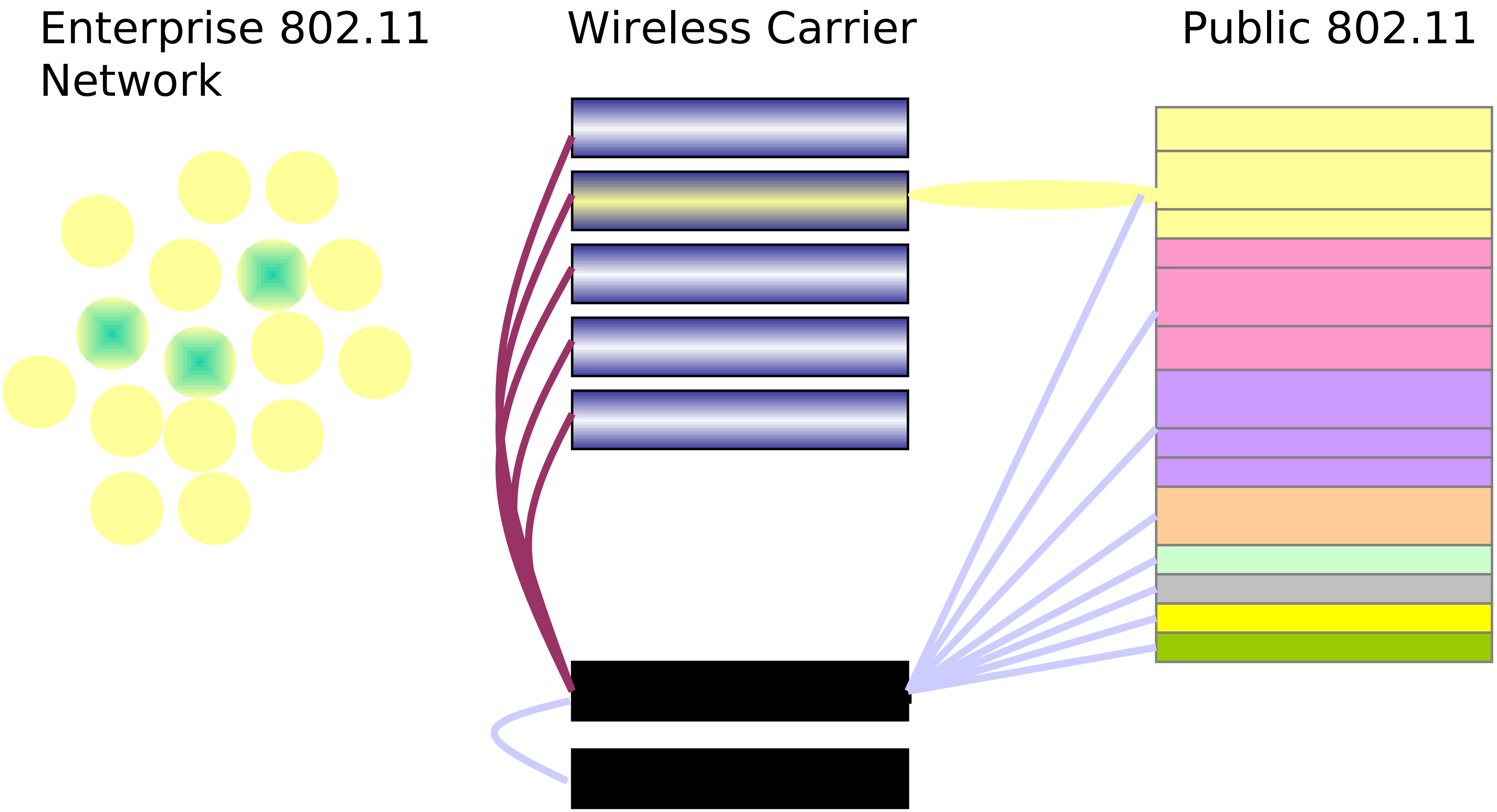
Public 802.11



- Market consolidation
- Entry of Wireless Carriers
- Entry of new players
- Footprint growth

Source: Pravin Bhagwat

Spectrum War: Steady State



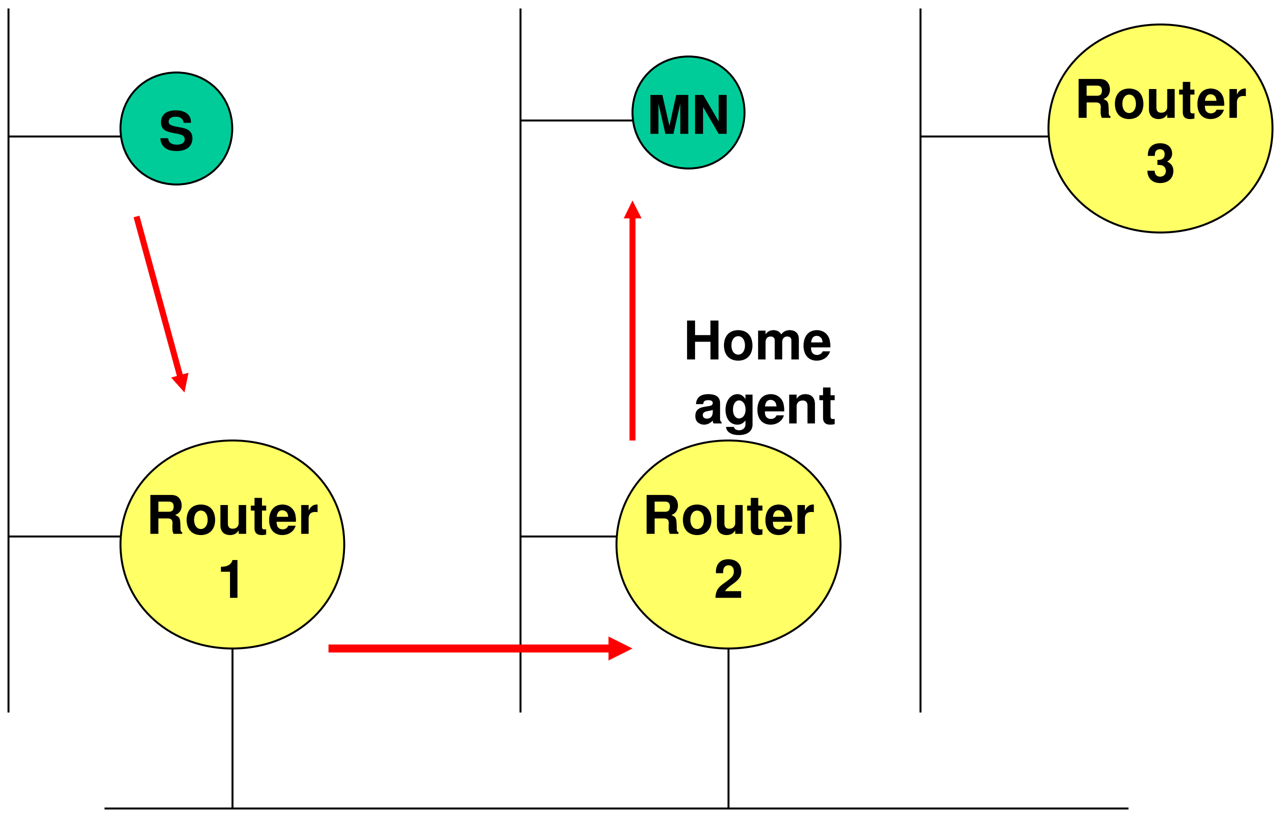
- Emergence of virtual carriers
- Roaming agreements

Source: Pravin Bhagwat

Routing and Mobility

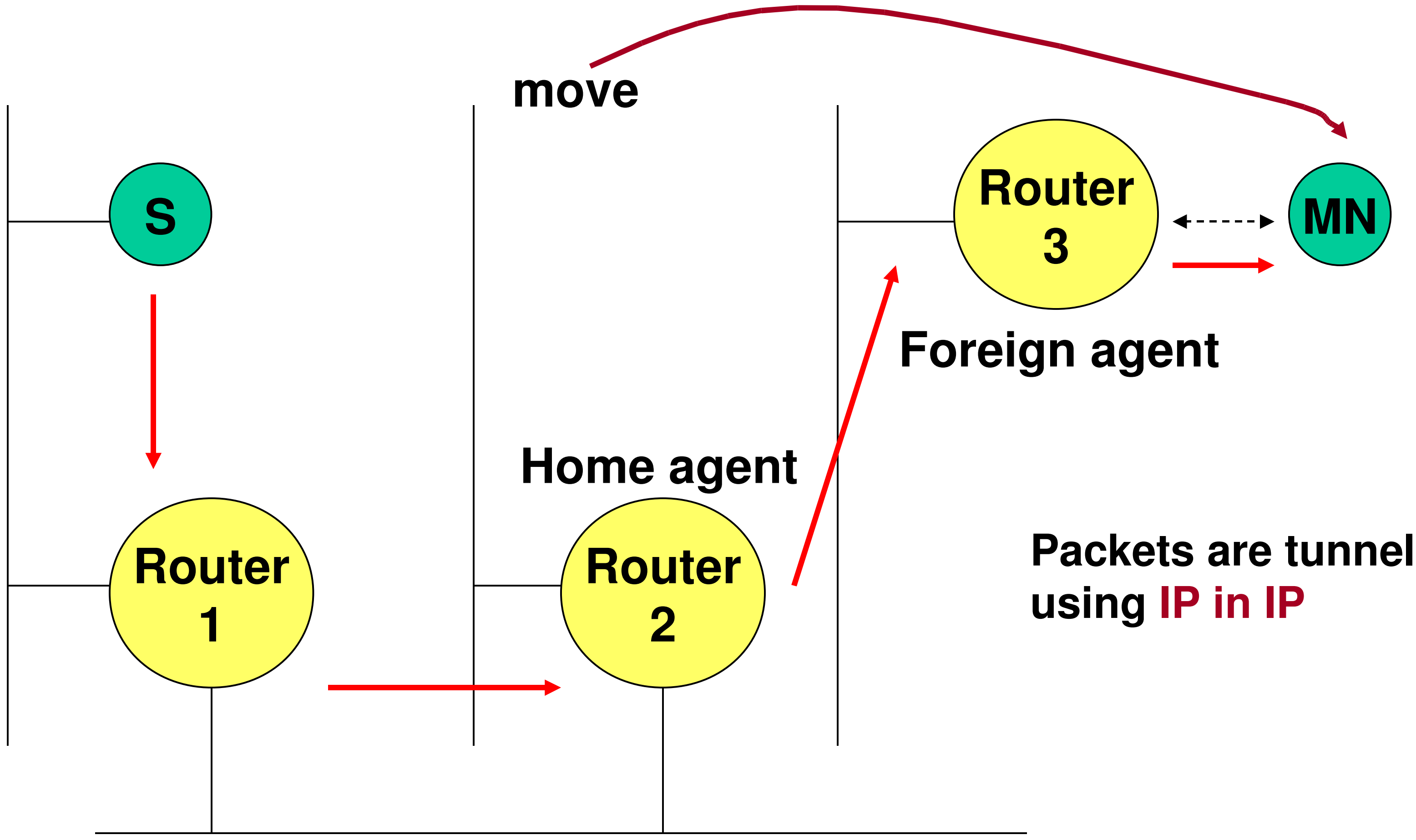
- Finding a path from a source to a destination
- Issues
  - Frequent route changes
  - Route changes may be related to host movement
  - Low bandwidth links
- Goal of routing protocols
  - decrease routing-related overhead
  - find short routes
  - find “stable” routes (despite mobility)

Mobile IP: Basic Idea



Source: Vaidya

Mobile IP: Basic Idea



Packets are tunneled using **IP in IP**

Source: Vaidya

TCP over wireless

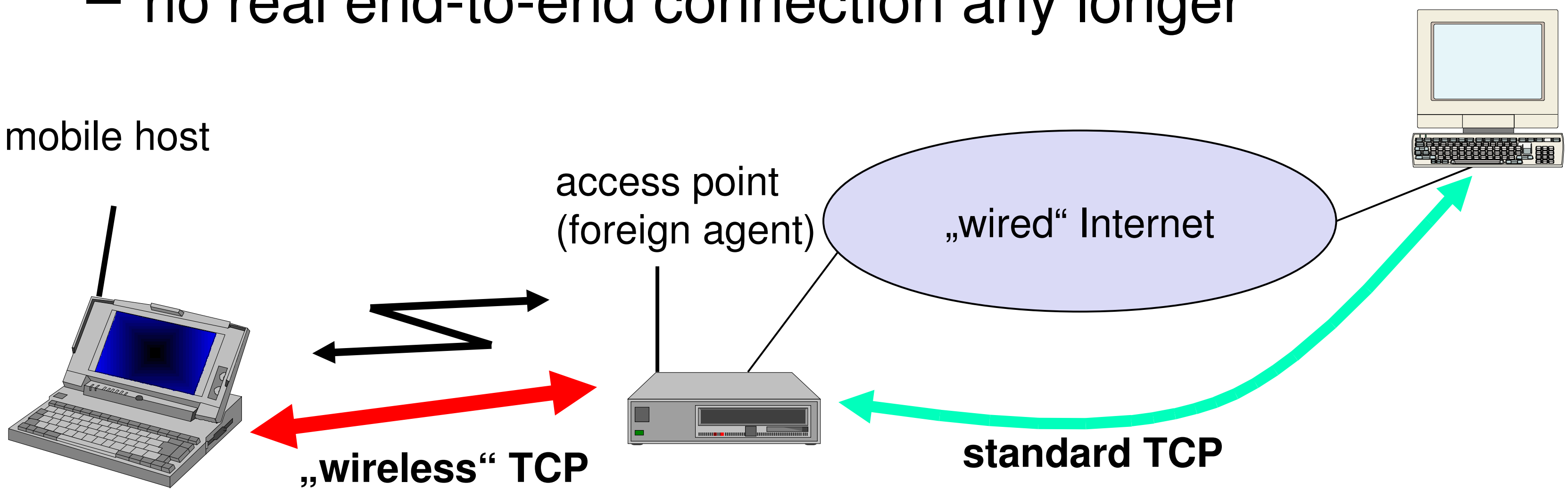
- TCP provides
  - reliable ordered delivery (uses retransmissions, if necessary)
  - cumulative ACKs (an ACK acknowledges all contiguously received data)
  - duplicate ACKs (whenever an out-of-order segment is received)
  - end-to-end semantics (receiver sends ACK after data has reached)
  - implements congestion avoidance and control using congestion window

TCP over wireless

- Factors affecting TCP over wireless:
  - Wireless transmission errors
    - may cause fast retransmit, which results in reduction in congestion window size
    - reducing congestion window in response to errors is unnecessary
  - Multi-hop routes on shared wireless medium
    - Longer connections are at a disadvantage compared to shorter ones, because they have to contend for wireless access at each hop
  - Route failures due to mobility

Indirect TCP (I-TCP)

- I-TCP splits the TCP connection
  - no changes to the TCP protocol for wired hosts
  - TCP connection is split at the foreign agent
  - hosts in wired network do not notice characteristics of wireless part
  - no real end-to-end connection any longer



Source: Schiller

Mobile TCP (M-TCP)

- Handling of lengthy or frequent disconnections
- M-TCP splits as I-TCP does
  - unmodified TCP for fixed network to foreign agent
  - optimized TCP for FA to MH
- Foreign Agent
  - monitors all packets, if disconnection detected
    - set sender window size to 0
    - sender automatically goes into persistent mode
  - no caching, no retransmission

Application Adaptations for Mobility

- Design Issues
  - System transparent v/s System aware
  - Application transparent v/s Application aware
- Models
  - conventional, "*unaware*" client/server model
  - client/proxy/server model
  - caching/pre-fetching model
  - mobile agent model

World Wide Web and Mobility

- HTTP characteristics
  - designed for large bandwidth, low delay
  - stateless, client/server, request/response communication
  - connection oriented, one connection per request
  - TCP 3-way handshake, DNS lookup overheads
- HTML characteristics
  - designed for computers with “high” performance, color high-resolution display, mouse, hard disk
  - typically, web pages optimized for design, not for communication; ignore end-system characteristics

System Support for Mobile WWW

- Enhanced browsers
  - client-aware support for mobility
- Proxies
  - Client proxy: pre-fetching, caching, off-line use
  - Network proxy: adaptive content transformation for connections
  - Client and network proxy
- Enhanced servers
  - server-aware support for mobility
  - serve the content in multiple ways, depending on client capabilities
- New protocols/languages
  - WAP/WML

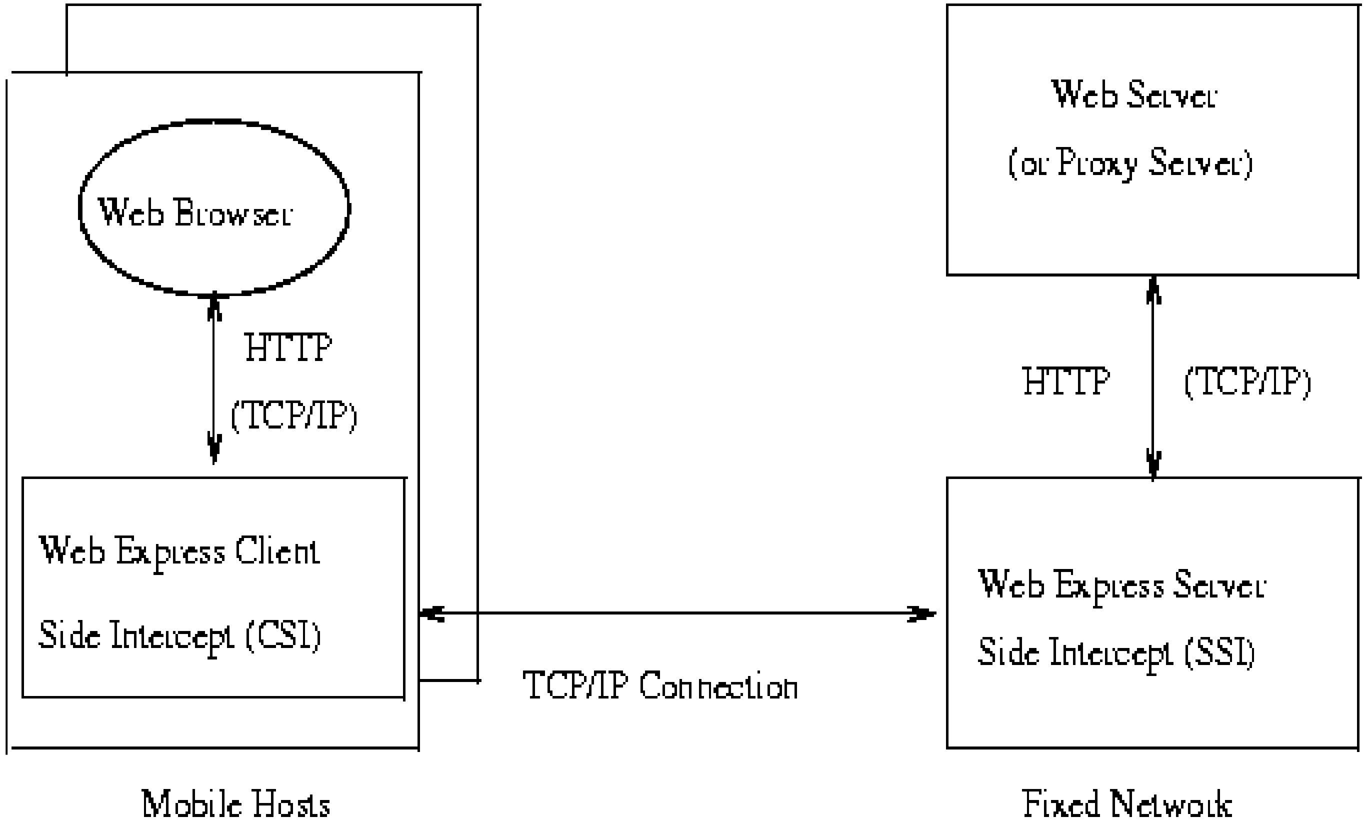
The Client/Proxy/Server Model

- Proxy functions as a client to the fixed network server
- Proxy functions as a mobility-aware server to mobile client

- Proxy may be placed in the mobile host (Coda), or the fixed network, or both (WebExpress)

- Enables thin client design for resource-poor mobile devices

Web Proxy in *WebExpress*



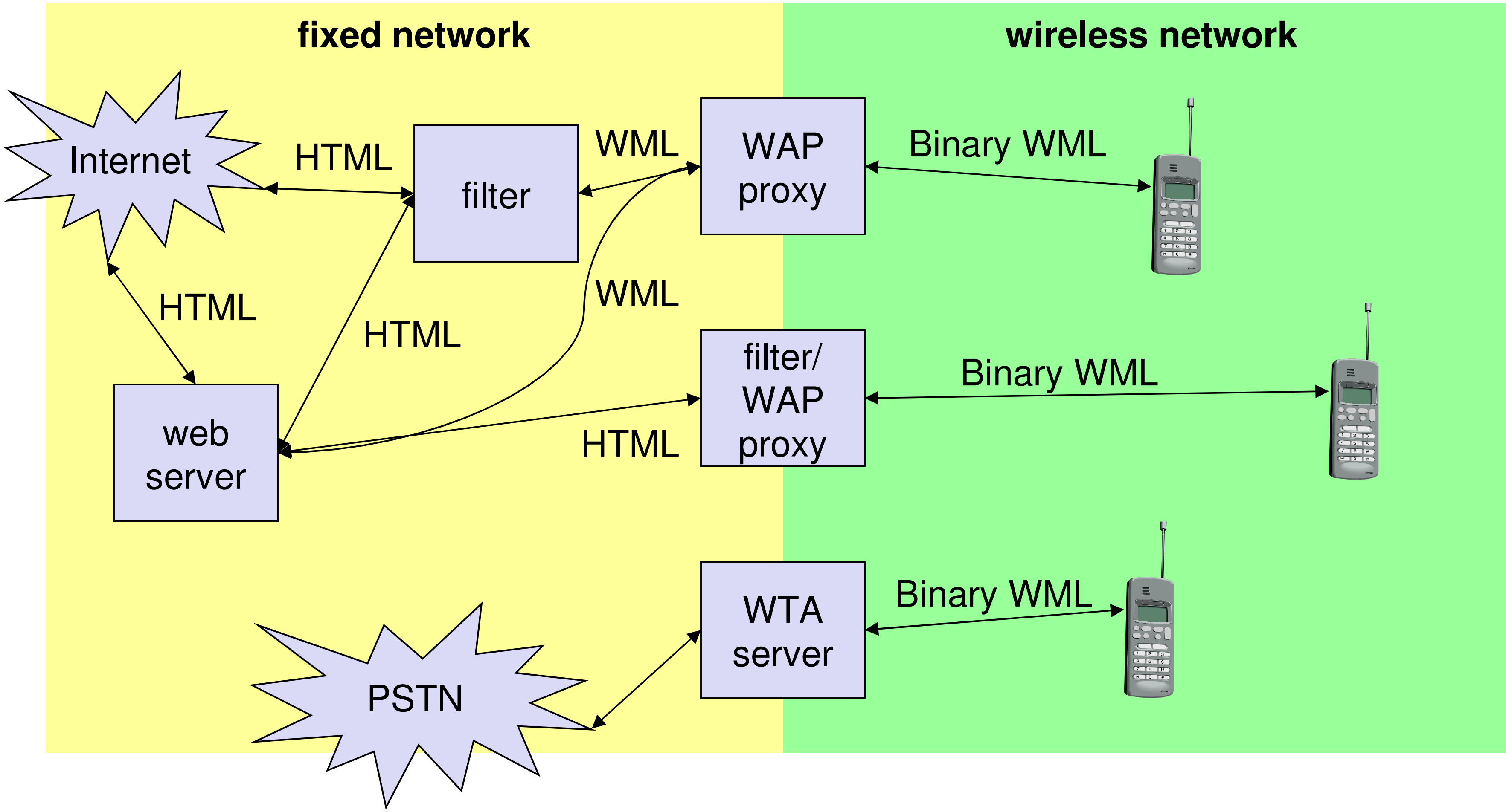
The WebExpress Intercept Model

Source: Helal

Wireless Application Protocol

- Browser
  - "Micro browser", similar to existing web browsers
- Script language
  - Similar to Javascript, adapted to mobile devices
- Gateway
  - Transition from wireless to wired world
- Server
  - "Wap/Origin server", similar to existing web servers
- Protocol layers
  - Transport layer, security layer, session layer etc.
- Telephony application interface
  - Access to telephony functions

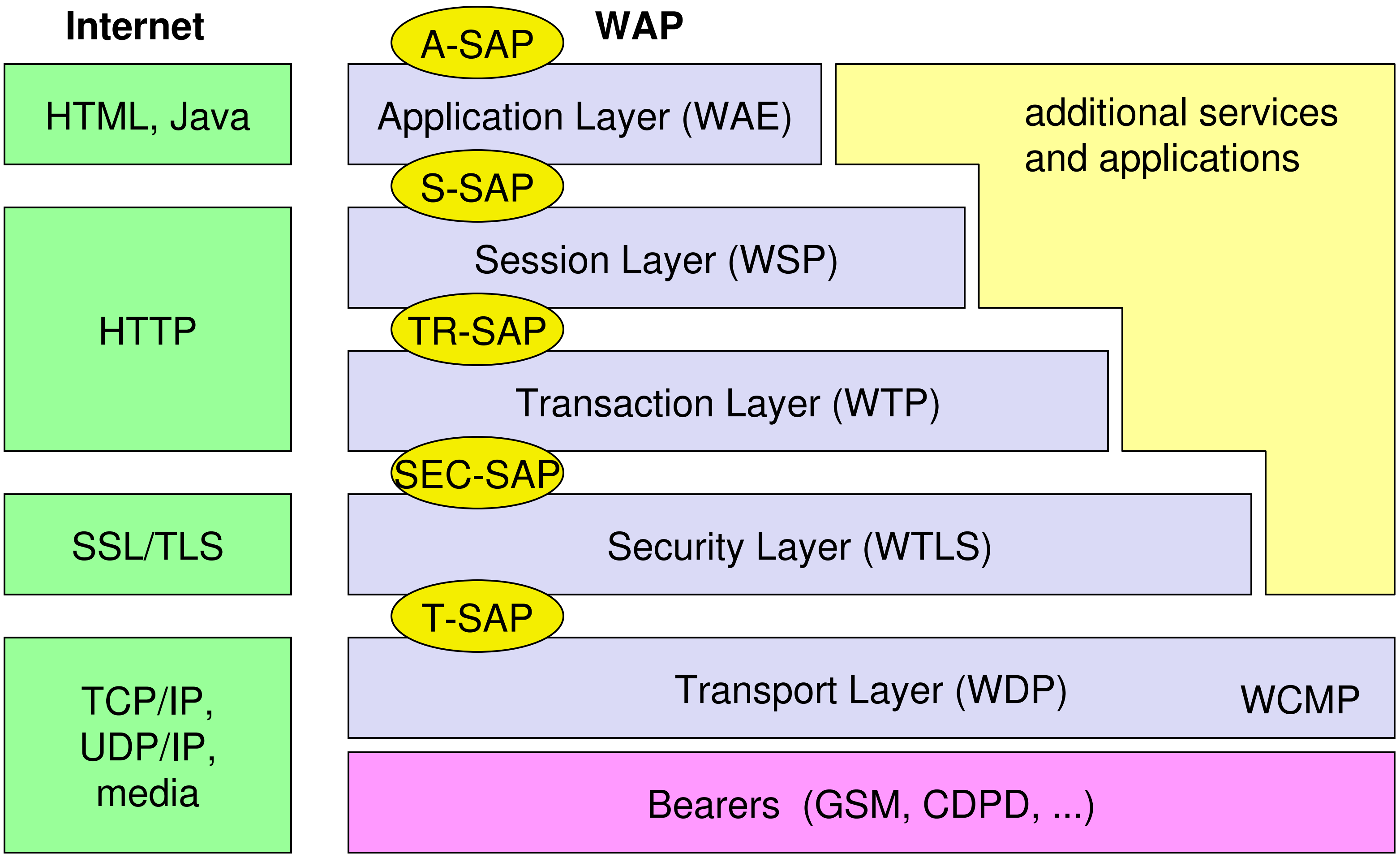
WAP: Network Elements



Binary WML: binary file format for clients

Source: Schiller

WAP: Reference Model



WAE comprises WML (Wireless Markup Language), WML Script, WTAI etc.

Source: Schiller

WAP Stack Overview

- WDP
  - functionality similar to UDP in IP networks
- WTLS
  - functionality similar to SSL/TLS (optimized for wireless)
- WTP
  - Class 0: analogous to UDP
  - Class 1: analogous to TCP (without connection setup overheads)
  - Class 2: analogous to RPC (optimized for wireless)
  - features of “user acknowledgement”, “hold on”
- WSP
  - WSP/B: analogous to http 1.1 (add features of suspend/resume)
  - method: analogous to RPC/RMI
  - features of asynchronous invocations, push (confirmed/unconfirmed)

The Mobile Agent Model

- Mobile agent receives client request and
- Mobile agent moves into fixed network

- Mobile agent acts as a client to the server
- Mobile agent performs transformations and filtering

- Mobile agent returns back to mobile platform, when the client is connected

Mobile Agents: Example

Outline

- Introduction and Overview
- **Wireless LANs: IEEE 802.11**
- Mobile IP routing
- TCP over wireless
- GSM air interface
- GPRS network architecture
- Wireless application protocol
- Mobile agents
- Mobile ad hoc networks

How Wireless LANs are different

- Destination address does not equal destination location
- The media impact the design
  - wireless LANs intended to cover reasonable geographic distances must be built from basic coverage blocks
- Impact of handling mobile (and portable) stations
  - Propagation effects
  - Mobility management
  - power management

Wireless Media

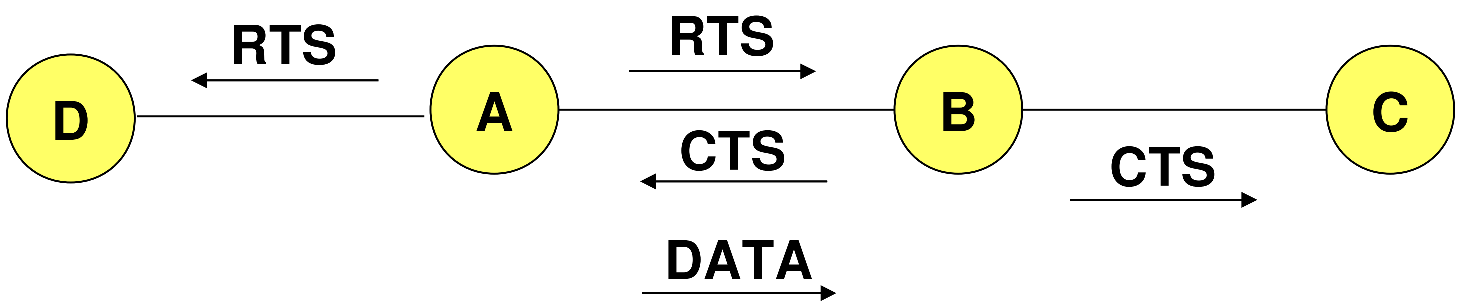
- Physical layers in wireless networks
  - Use a medium that has neither absolute nor readily observable boundaries outside which stations are unable to receive frames
  - Are unprotected from outside signals
  - Communicate over a medium significantly less reliable than wired PHYs
  - Have dynamic topologies
  - Lack full connectivity and therefore the assumption normally made that every station (STA) can hear every other STA in invalid (I.e., STAs may be "hidden" from each other)
  - Have time varying and asymmetric propagation properties

802.11: 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”
- Hidden and exposed terminals

Solution for Hidden/Exposed Terminals

- A first sends a *Request-to-Send (RTS)* to B
- On receiving RTS, B responds *Clear-to-Send (CTS)*
- Hidden node C overhears CTS and keeps quiet
  - Transfer duration is included in both RTS and CTS
- Exposed node overhears a RTS but not the CTS
  - D's transmission cannot interfere at B



IEEE 802.11

- Wireless LAN standard defined in the unlicensed spectrum (2.4 GHz and 5 GHz U-NII bands)

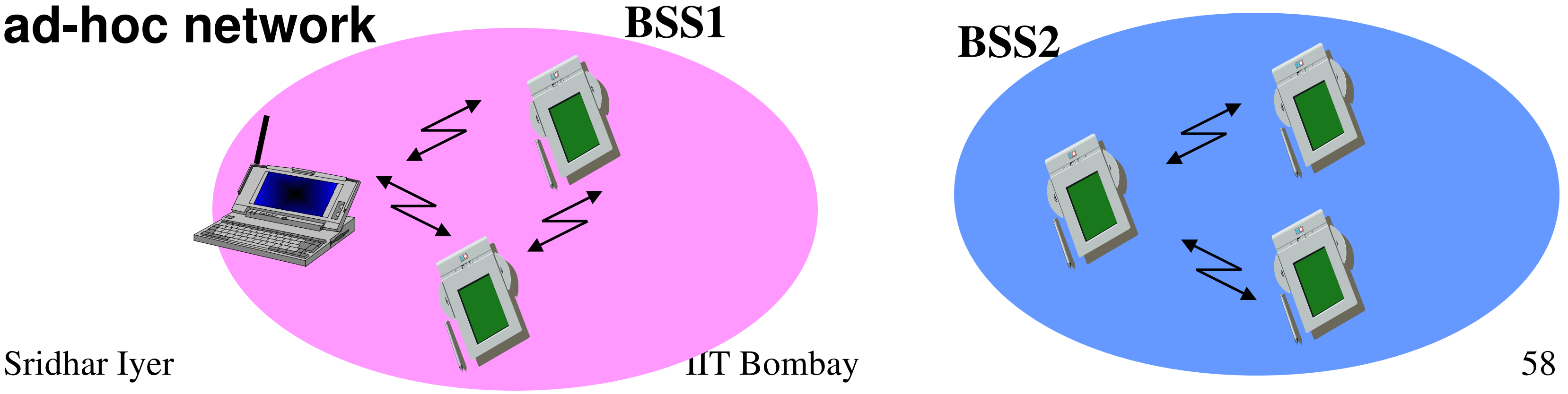
Region	Allocated Spectrum
US	2.4000 – 2.4835 GHz
Europe	2.4000 – 2.4835 GHz
Japan	2.471 - 2.497 GHz
France	2.4465 - 2.4835 GHz
Spain	2.445 - 2.475 GHz

Table 1 Global Spectrum Allocation at 2.4 GHz

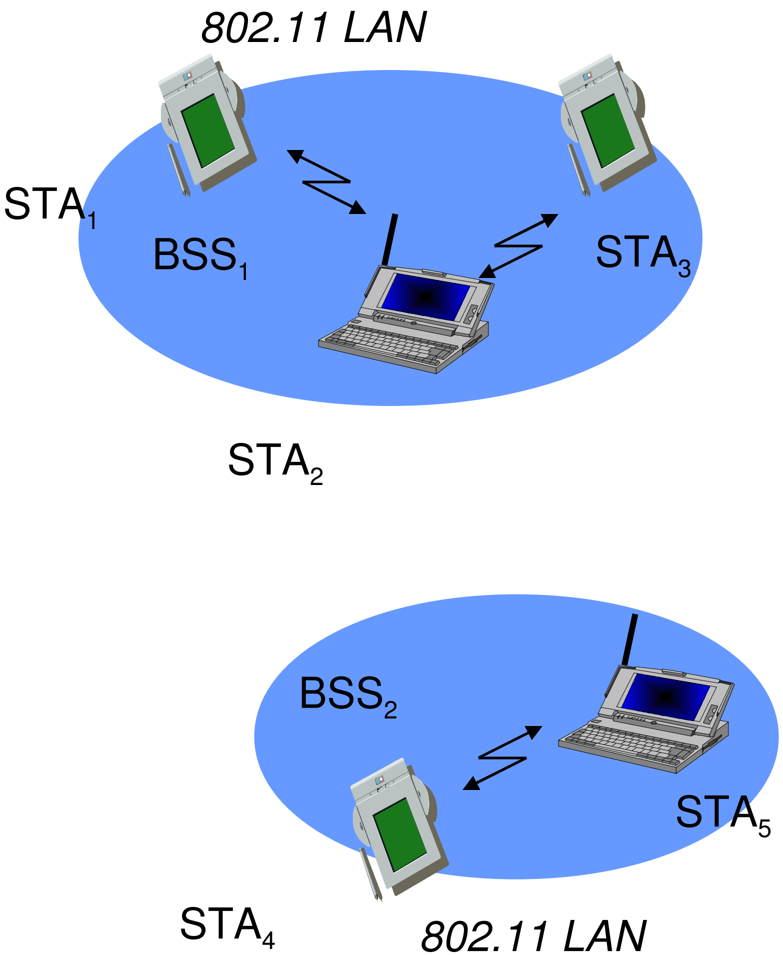
- Standards covers the MAC sublayer and PHY layers
- Three different physical layers in the 2.4 GHz band
  - FHSS, DSSS and IR
- OFDM based PHY layer in the 5 GHz band

Components of IEEE 802.11 architecture

- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



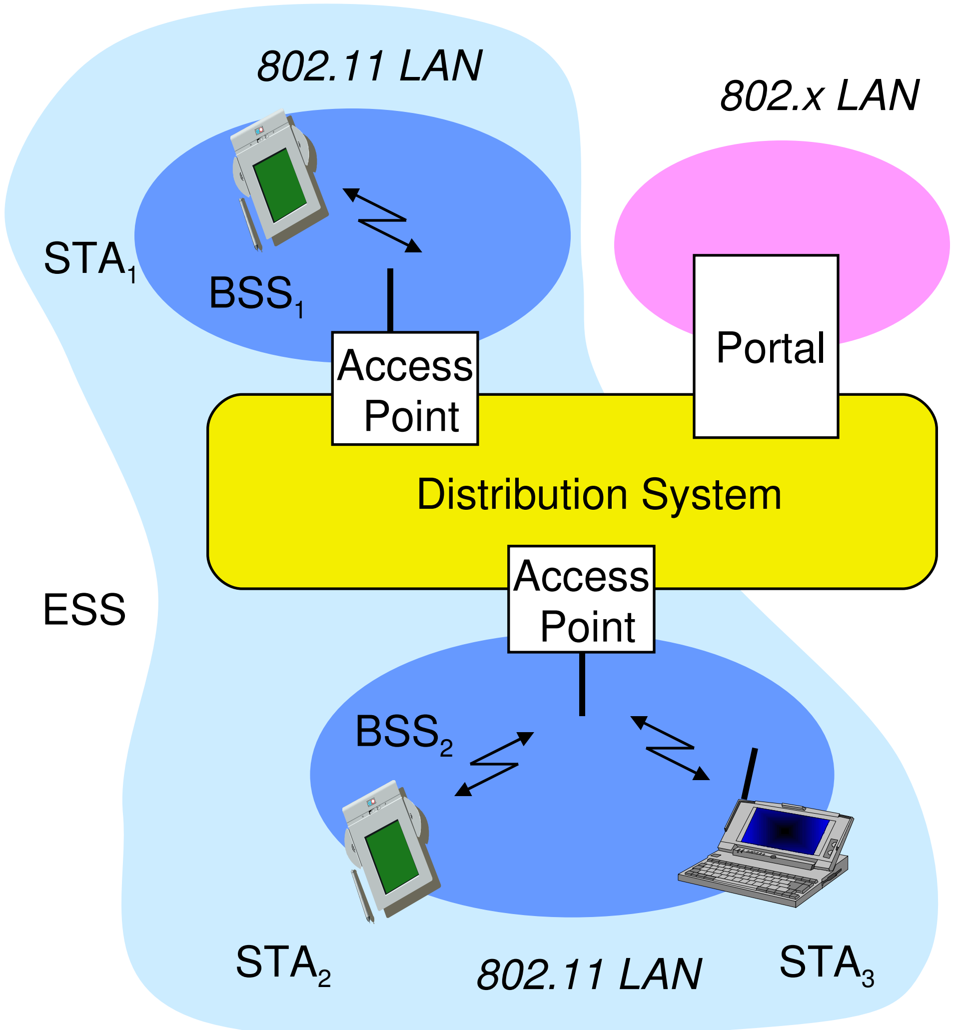
802.11 - ad-hoc network (DCF)



- Direct 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

Source: Schiller

802.11 - infrastructure network (PCF)



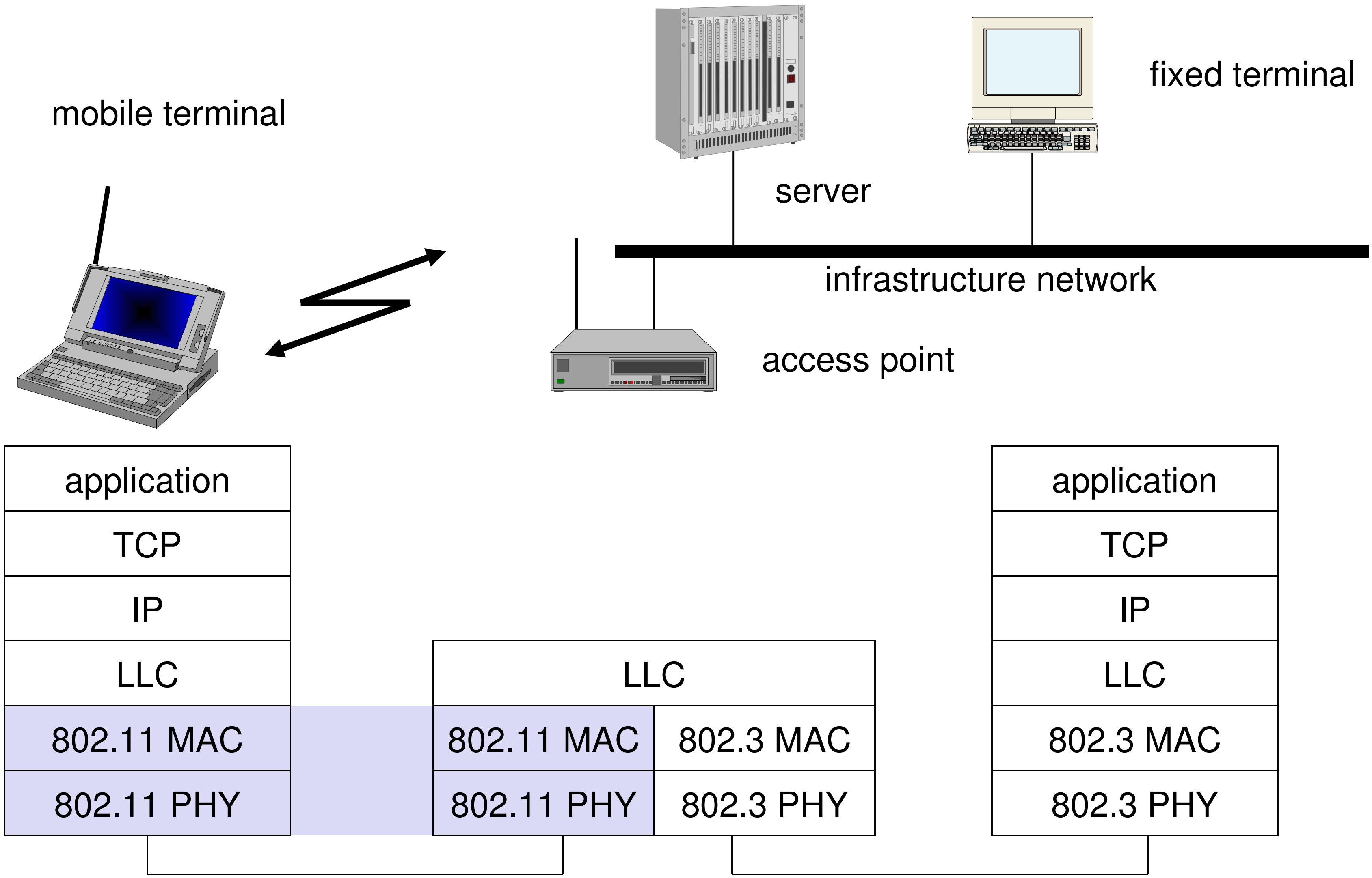
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to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

Source: Schiller

Distribution System (DS) concepts

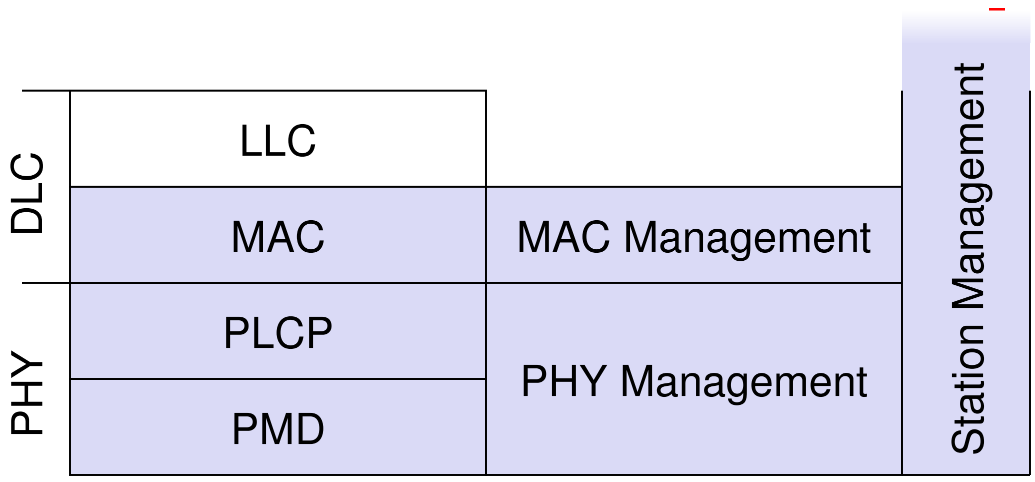
- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

802.11- in the TCP/IP stack



802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management



- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions

802.11 - Physical layer

- 3 versions: 2 radio (typically 2.4 GHz), 1 IR
  - data rates 1, 2, or 11 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typically 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum)
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbit/s
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- Infrared
  - 850-950 nm, diffuse light, typ. 10 m range
  - carrier detection, energy detection, synchonization

Spread-spectrum communications

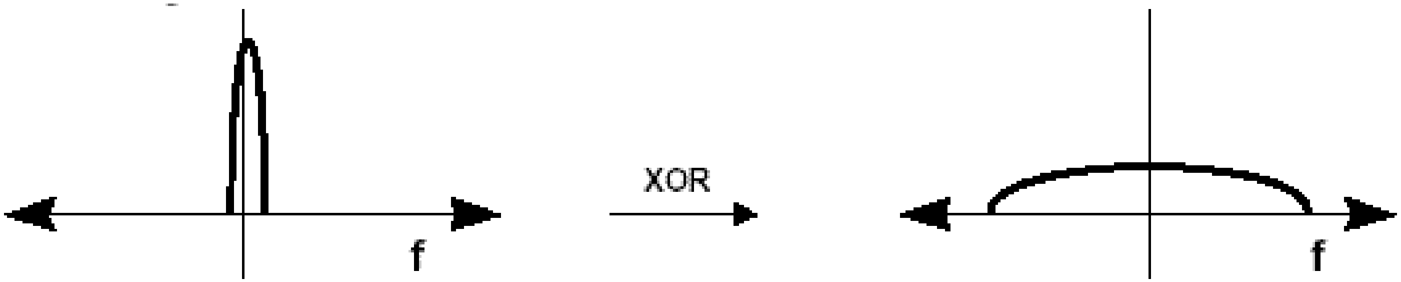


Figure 5a Effect of PN Sequence on Transmit Spectrum

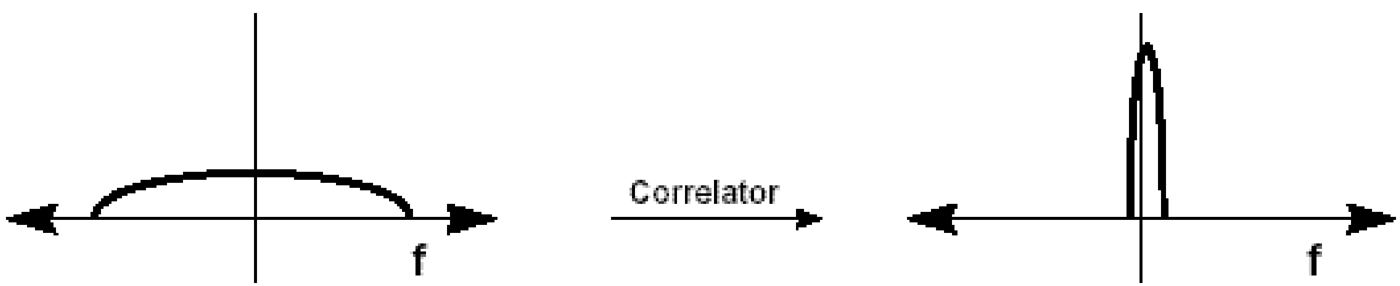
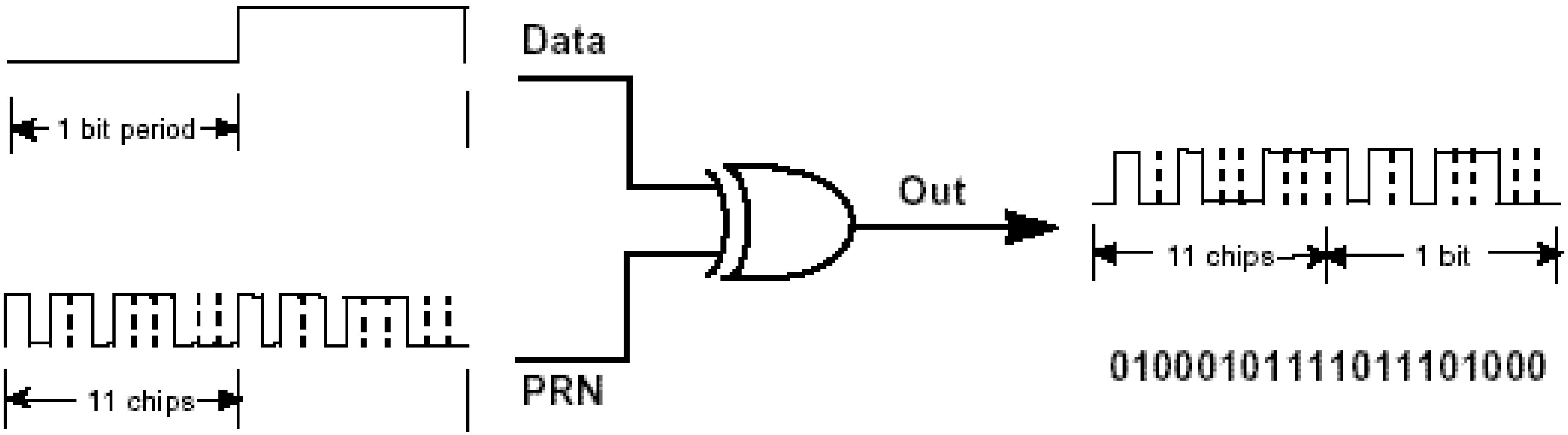


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

Source: Intersil

DSSS Barker Code modulation



11 Bit Barker Code (PRN):
1 0 1 1 1 0 1 0 0 0

Figure 3 Digital Modulation of Data with PRN Sequence

Source: Intersil

DSSS properties

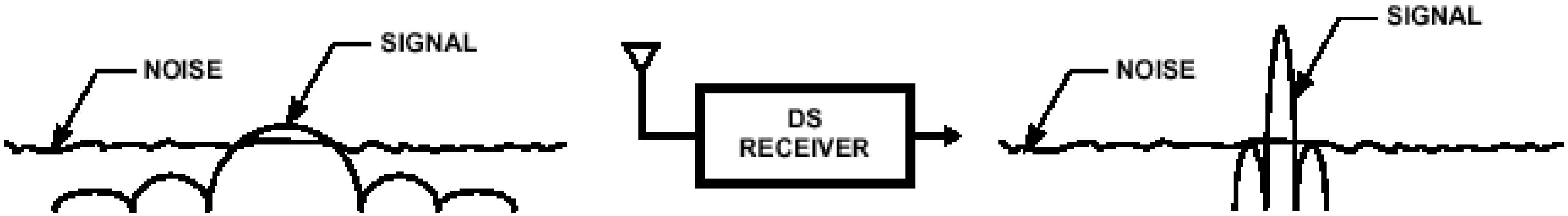


FIGURE 2A. LOW POWER DENSITY

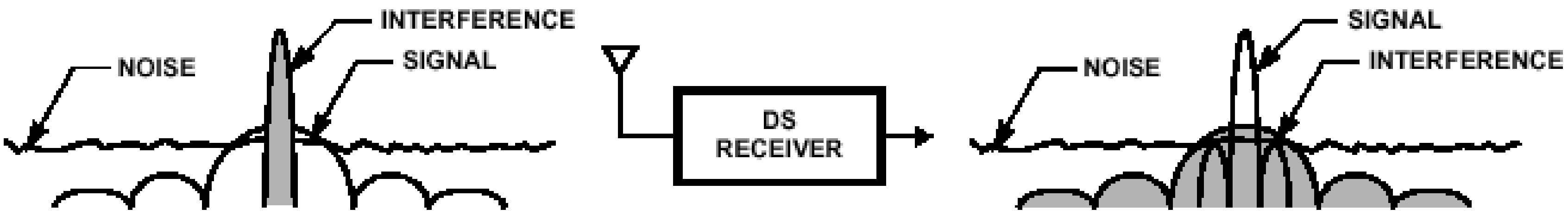


FIGURE 2B. INTERFERENCE REJECTION

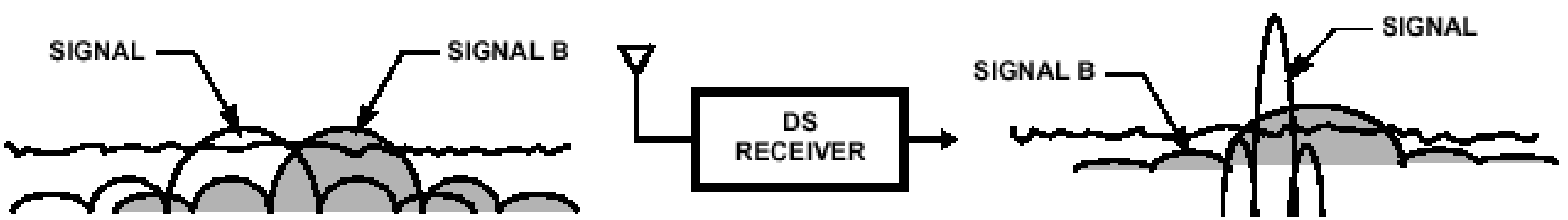


FIGURE 2C. MULTIPLE ACCESS

FIGURE 2. DIRECT SEQUENCE SPREAD SPECTRUM PROPERTIES

Source: Intersil

802.11 - MAC layer

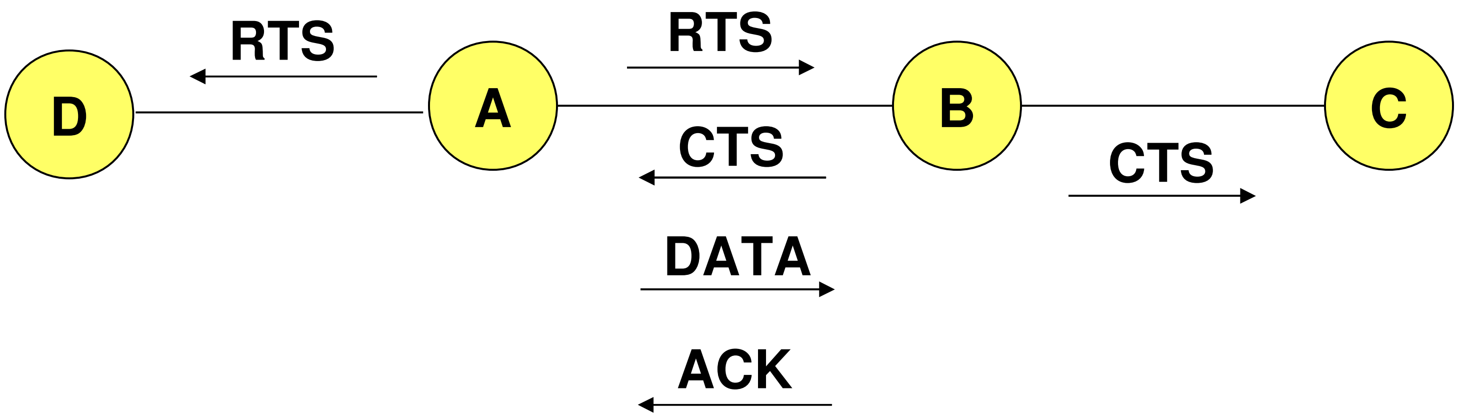
- Traffic services
  - Asynchronous Data Service (mandatory) – DCF
  - Time-Bounded Service (optional) - PCF
- Access methods
  - DCF CSMA/CA (mandatory)
    - collision avoidance via randomized back-off mechanism
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF w/ RTS/CTS (optional)
    - avoids hidden terminal problem
  - PCF (optional)
    - access point polls terminals according to a list

802.11 - Carrier Sensing

- **In IEEE 802.11, carrier sensing is performed**
  - at the air interface (*physical carrier sensing*), and
  - at the MAC layer (*virtual carrier sensing*)
- **Physical carrier sensing**
  - detects presence of other users by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources
- **Virtual carrier sensing** is done by sending MPDU duration information in the header of RTS/CTS and data frames
- Channel is busy if **either** mechanisms indicate it to be
  - Duration field indicates the amount of time (in microseconds) required to complete frame transmission
  - Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV)

802.11 - Reliability

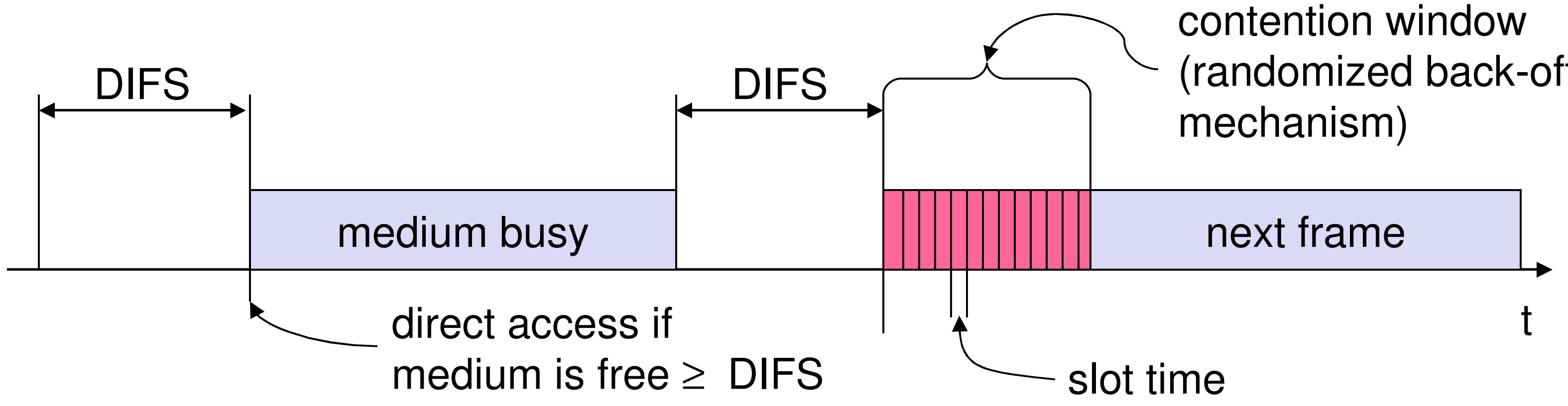
- Use of acknowledgements
  - When B receives DATA from A, B sends an ACK
  - If A fails to receive an ACK, A retransmits the DATA
  - Both C and D remain quiet until ACK (to prevent collision of ACK)
  - Expected duration of transmission+ACK is included in RTS/ CTS packets



802.11 - Priorities

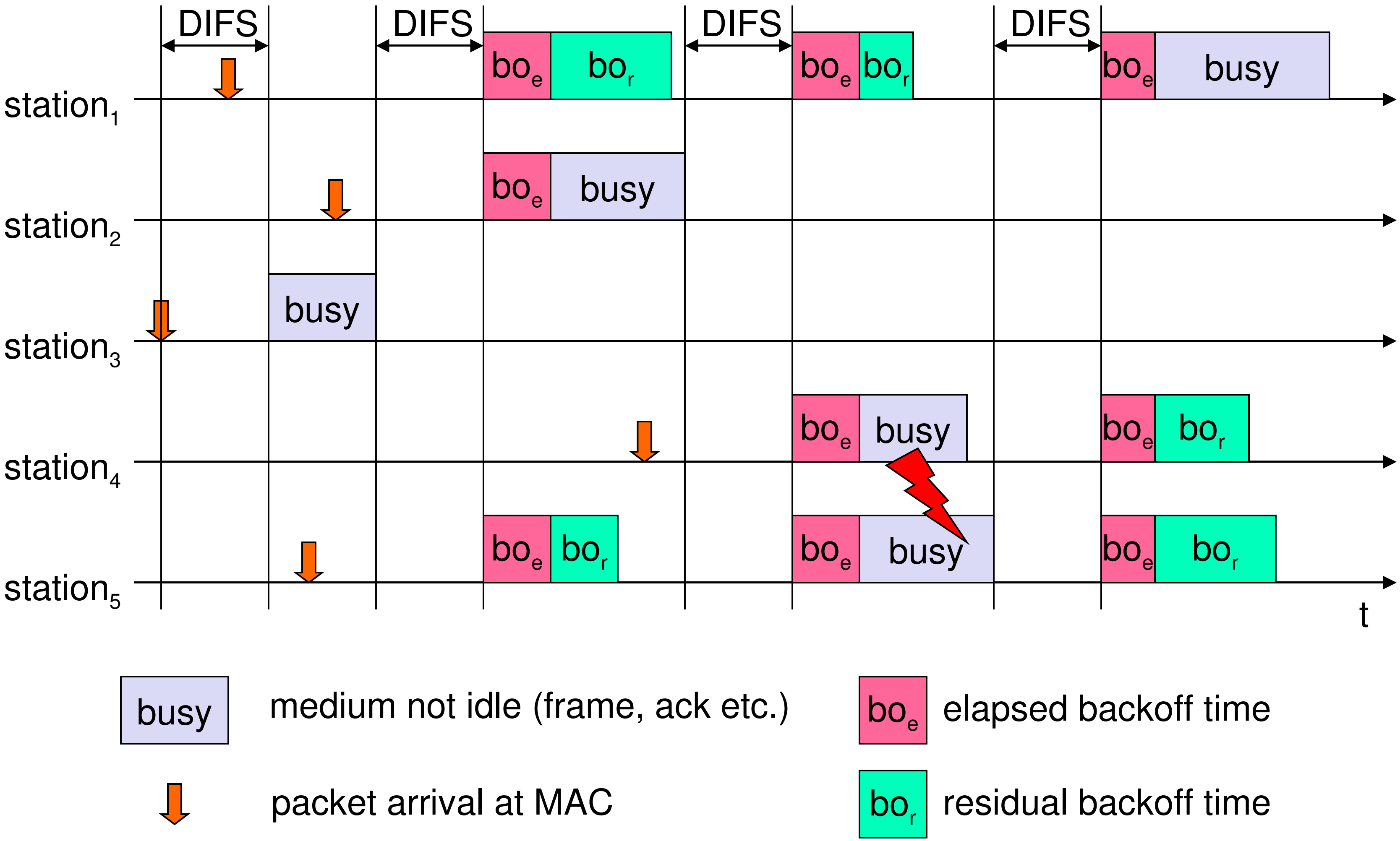
- defined through different inter frame spaces – mandatory idle time intervals between the transmission of frames
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
  - SIFSTime and SlotTime are fixed per PHY layer
  - (10 μ s and 20 μ s respectively in DSSS)
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
  - PIFSTime = SIFSTime + SlotTime
- DIFS (DCF IFS)
  - lowest priority, for asynchronous data service
  - DCF-IFS (DIFS): DIFSTime = SIFSTime + 2xSlotTime

802.11 - CSMA/CA



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

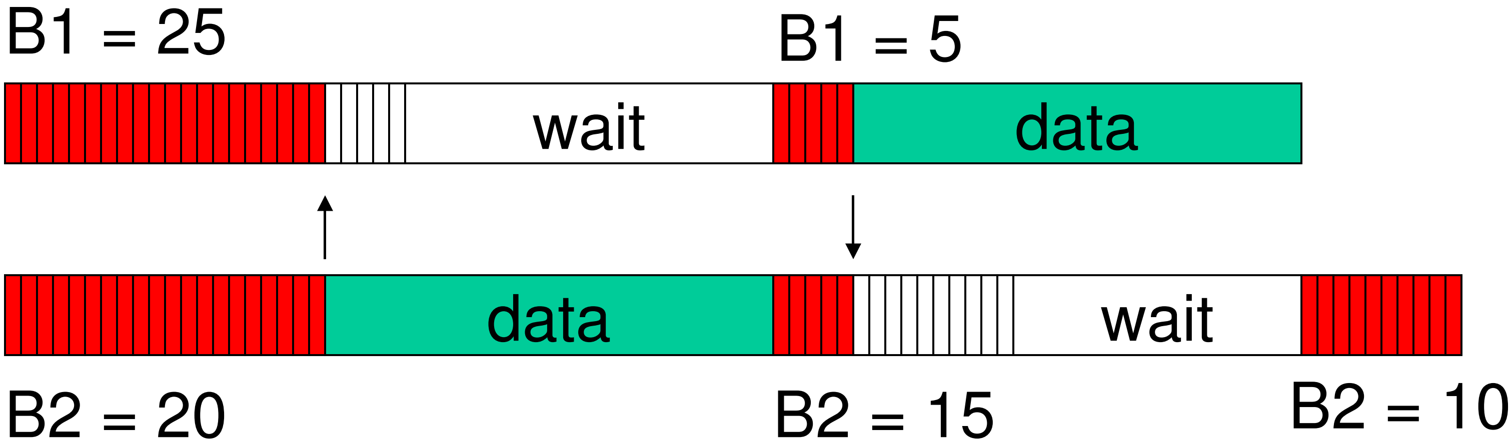
802.11 –CSMA/CA example



802.11 - Collision Avoidance

- Collision avoidance: Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit
- 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

DCF Example



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

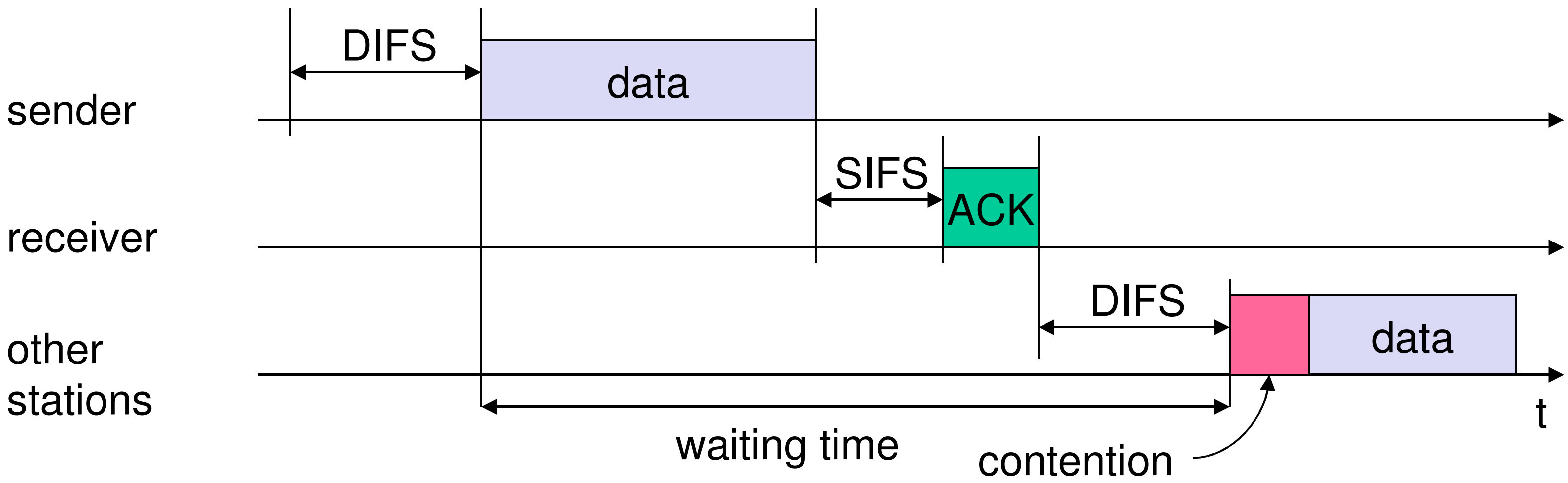
802.11 - Congestion Control

- Contention window (cw) in DCF: Congestion control achieved by dynamically choosing cw
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

- 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 CW_{max})
  - Upon successful completion data transfer, restore cw to CW_{min}

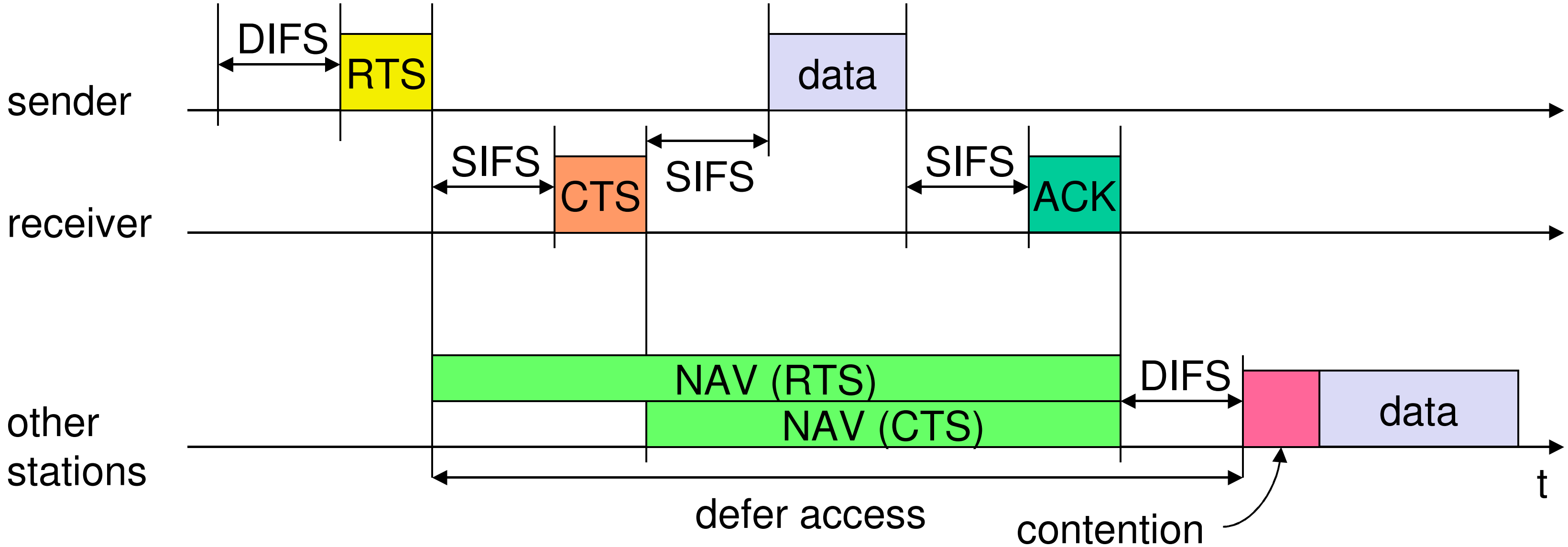
802.11 - CSMA/CA II

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors

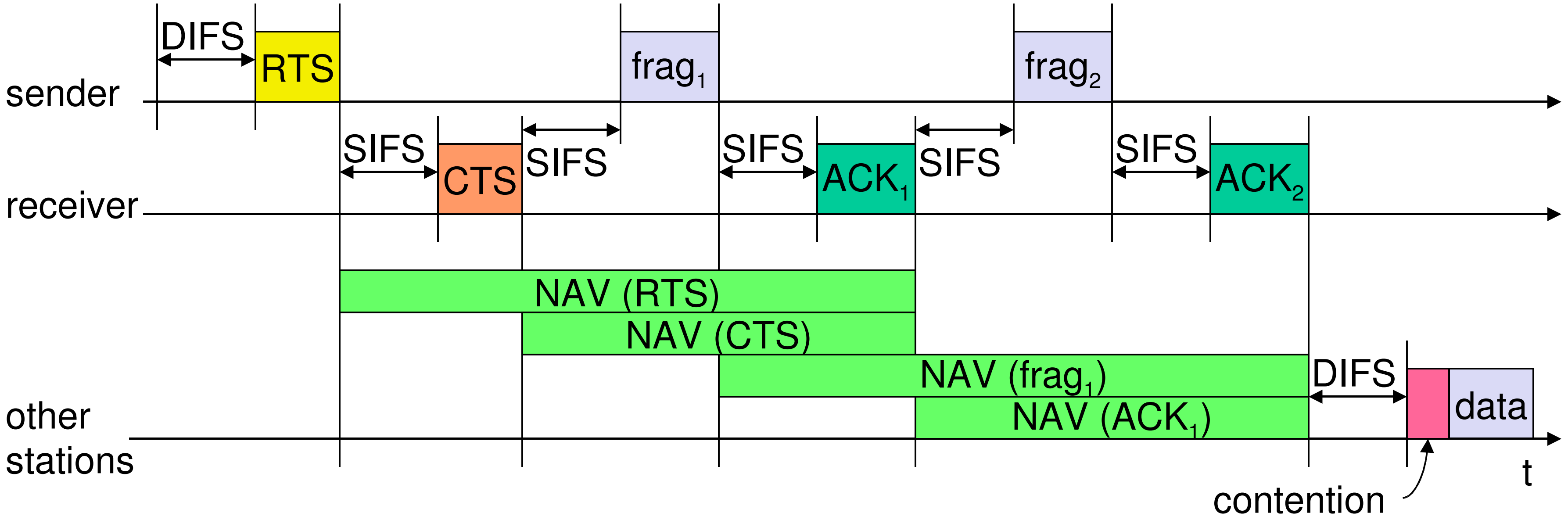


802.11 –RTS/CTS

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



Fragmentation



802.11 - Point Coordination Function

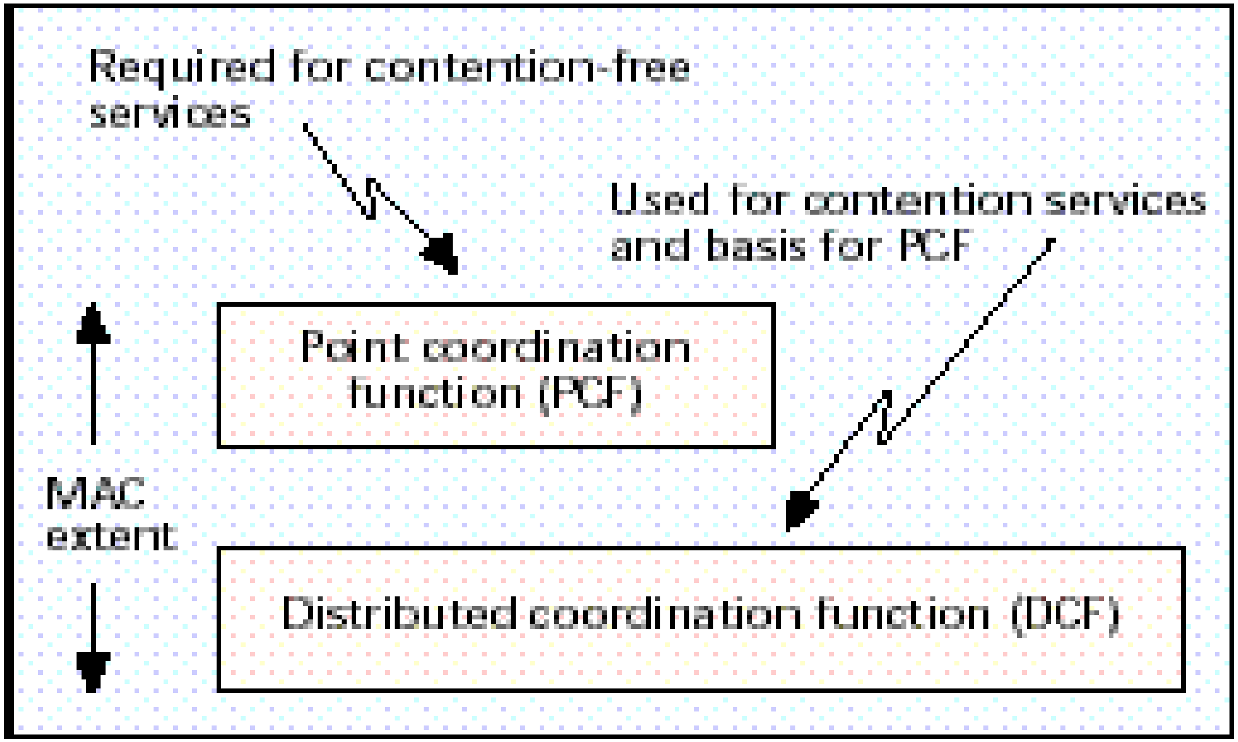
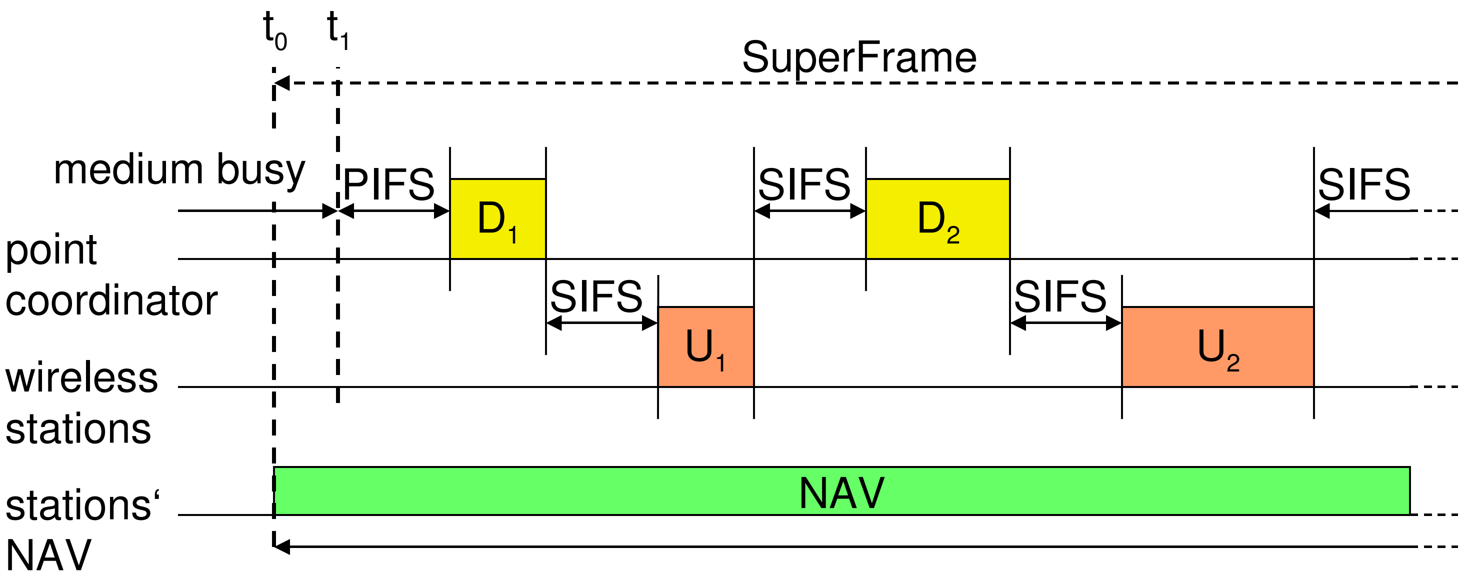


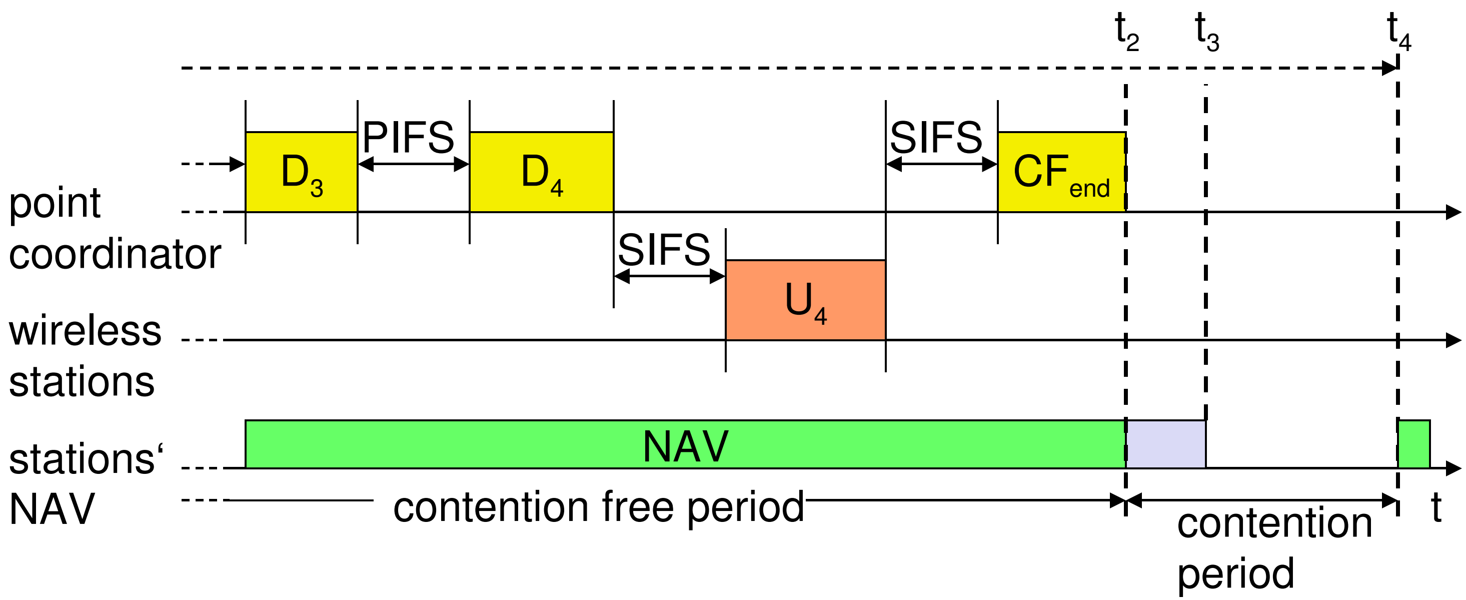
Figure 4. *MAC architecture.*

802.11 - PCF I



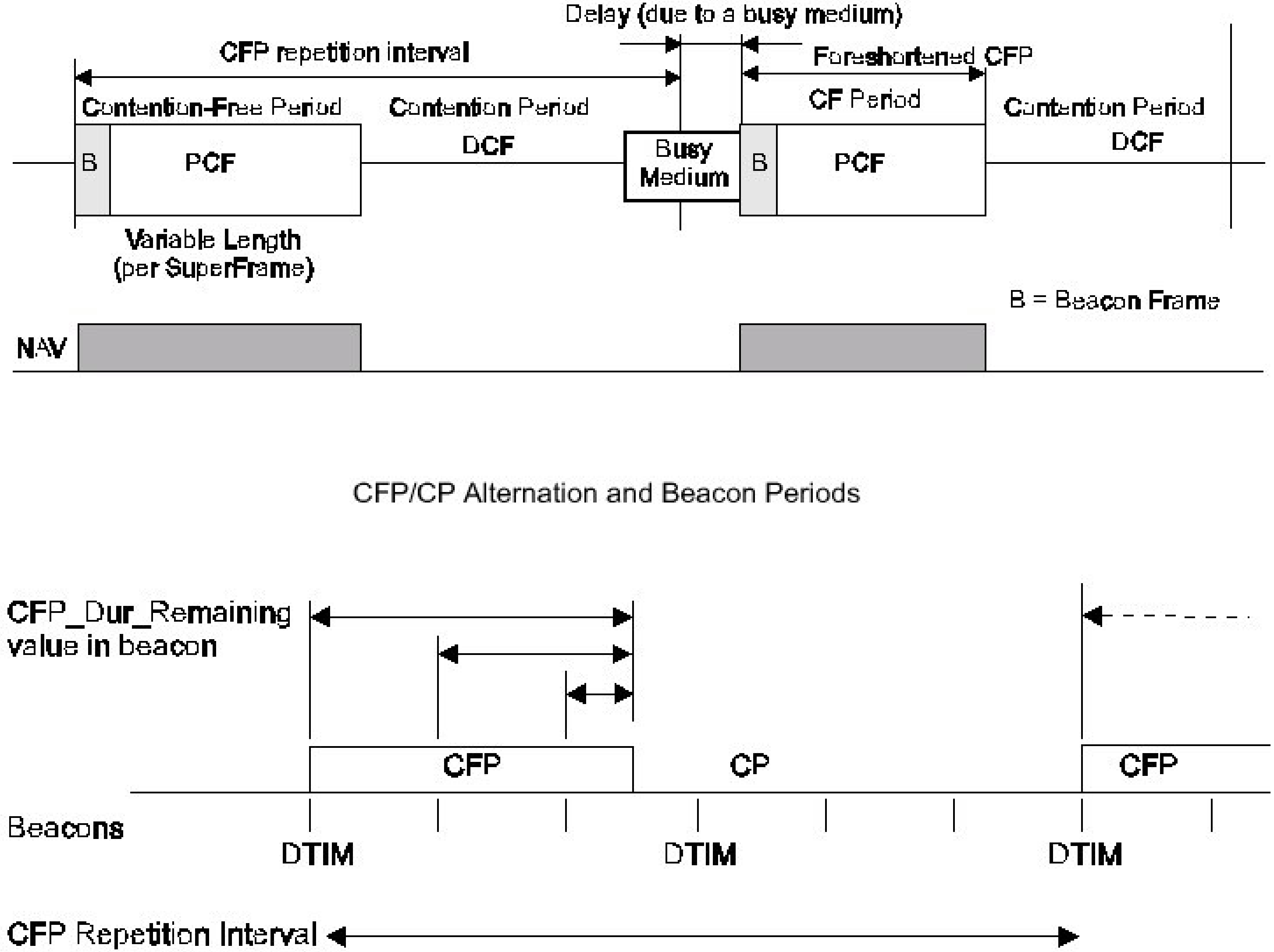
t_0
t_1
SuperFrame
medium busy
PIFS
D_1
SIFS
D_2
SIFS
point coordinator
SIFS
U_1
SIFS
U_2
wireless stations
stations' NAV
NAV

802.11 - PCF II



t2
t3
t4
PIFS
SIFS
D3
D4
CFend
point
coordinator
SIFS
U4
wireless
stations
stations'
NAV
NAV
contention free period
contention
period
t

CFP structure and Timing



PCF- Data transmission

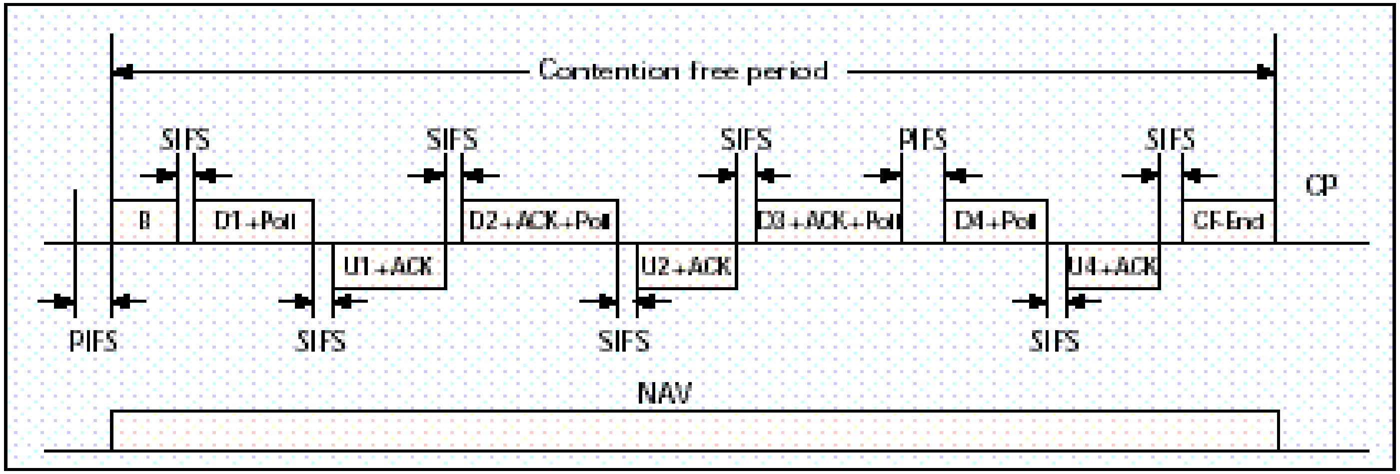


Figure 9. *PC-to-station transmission.*

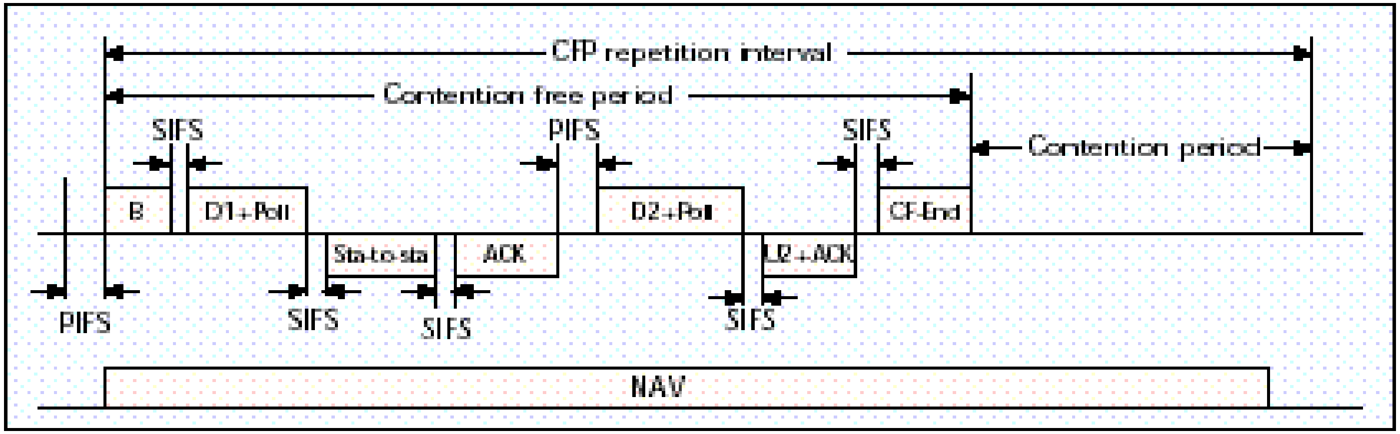


Figure 10. *Station-to-station transmissions.*

Polling Mechanisms

- With DCF, there is no mechanism to guarantee minimum delay for time-bound services
- PCF wastes bandwidth (control overhead) when network load is light, but delays are bounded
- With Round Robin (RR) polling, 11% of time was used for polling
- This values drops to 4 % when optimized polling is used
- Implicit signaling mechanism for STAs to indicate when they have data to send improves performance

Coexistence of PCF and DCF

- PC controls frame transfers during a Contention Free Period (CFP).
  - CF-Poll control frame is used by the PC to invite a station to send data
  - CF-End is used to signal the end of the CFP
- The CFP alternates with a CP, when DCF controls frame transfers
  - The CP must be large enough to send at least one maximum-sized MPDU including RTS/CTS/ACK
- CFPs are generated at the CFP repetition rate and each CFP begins with a beacon frame

802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

Frame Control: version, type, fragmentation, security, ...

Frame Control Field

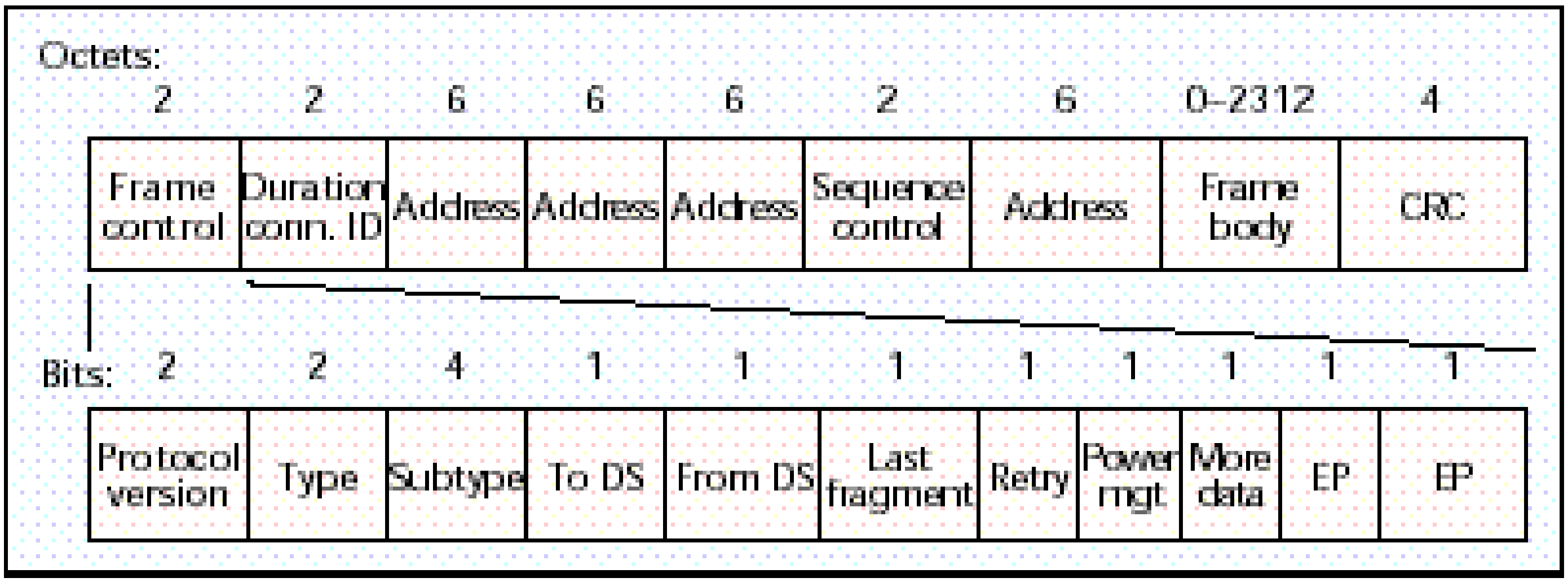


Figure 3. *Standard IEEE 802.11 frame format.*

Types of Frames

- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
- Management Frames
  - Beacons
  - Probe Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
  - Authentication/Deauthentication
  - ATIM
- Data Frames

MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

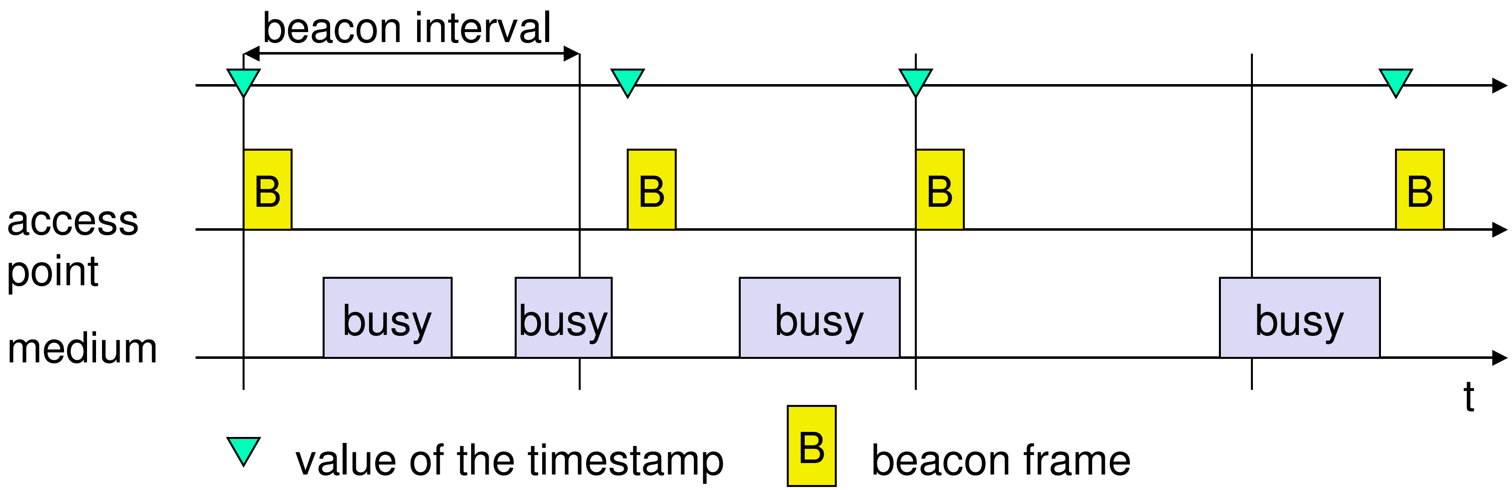
802.11 - MAC management

- Synchronization
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

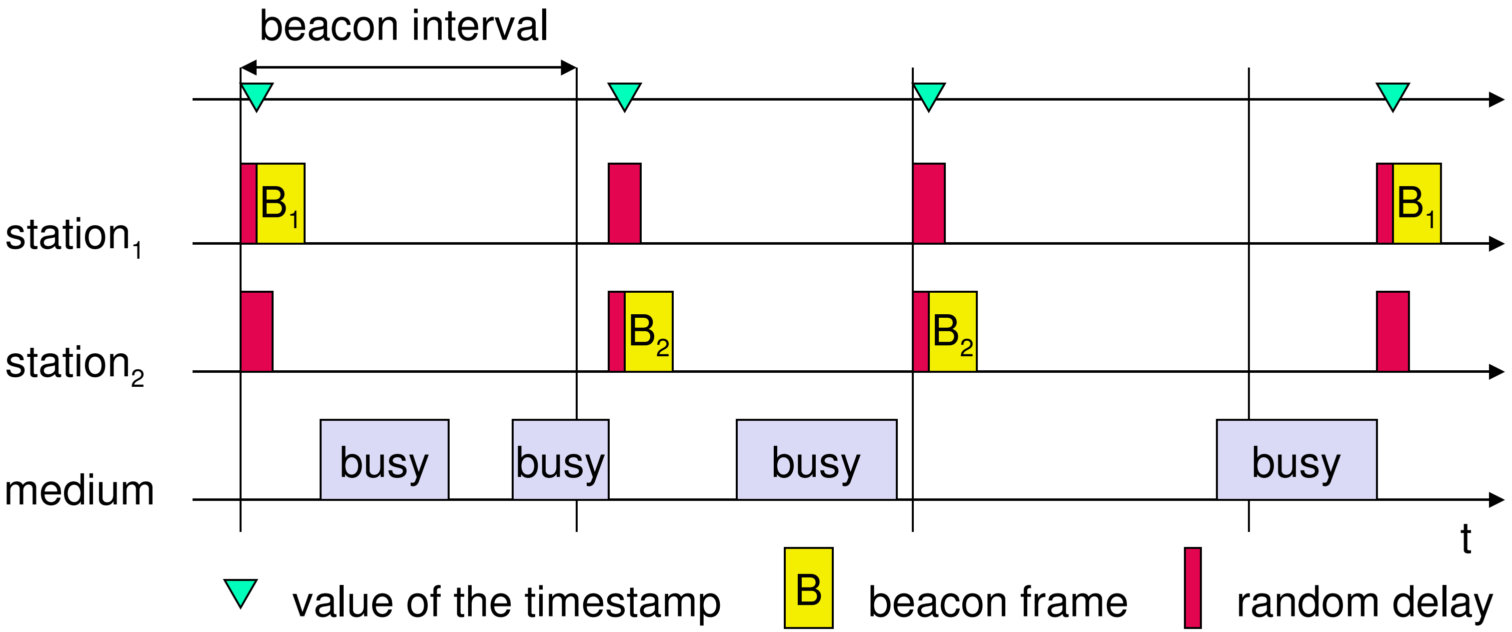
802.11 - Synchronization

- All STAs within a BSS are synchronized to a common clock
  - PCF mode: AP is the timing master
    - periodically transmits Beacon frames containing Timing Synchronization function (TSF)
    - Receiving stations accepts the timestamp value in TSF
  - DCF mode: TSF implements a distributed algorithm
    - Each station adopts the timing received from any beacon that has TSF value later than its own TSF timer
- This mechanism keeps the synchronization of the TSF timers in a BSS to within 4 μ s plus the maximum propagation delay of the PHY layer

Synchronization using a Beacon (infrastructure)



Synchronization using a Beacon (ad-hoc)



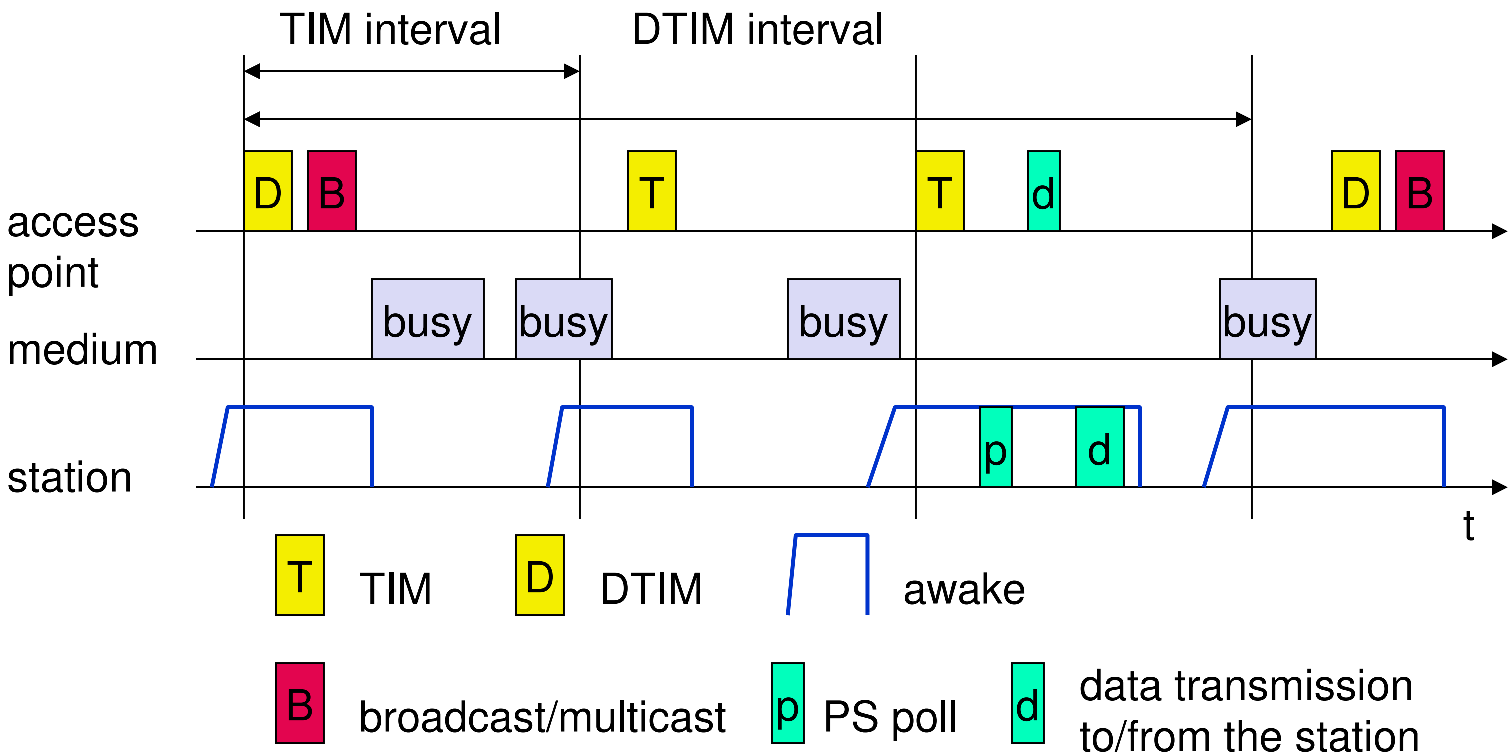
802.11 - Power management

- Idea: switch the transceiver off if not needed
  - States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)

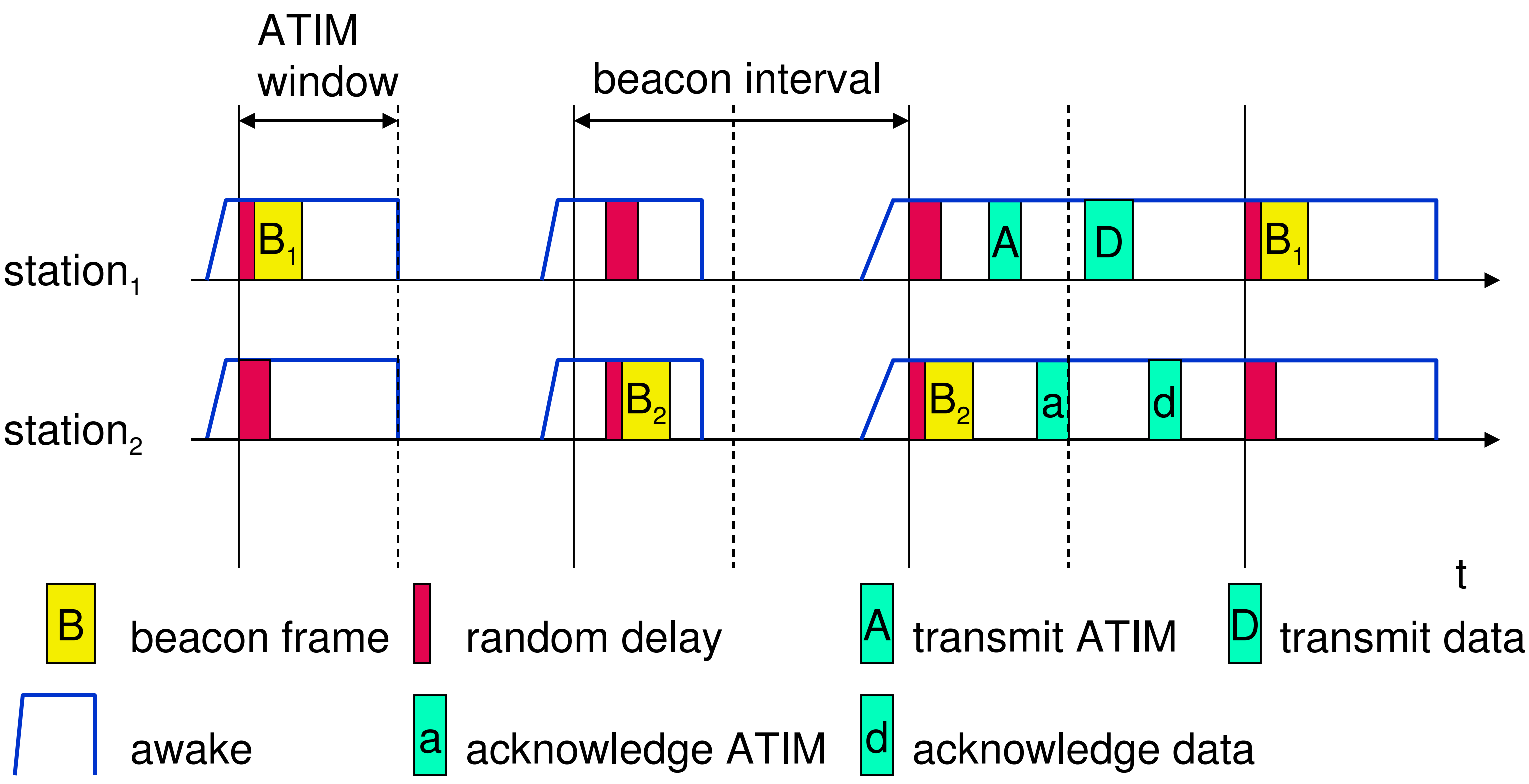
802.11 - Energy conservation

- Power Saving 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

Power saving with wake-up patterns (infrastructure)



Power saving with wake-up patterns (ad-hoc)



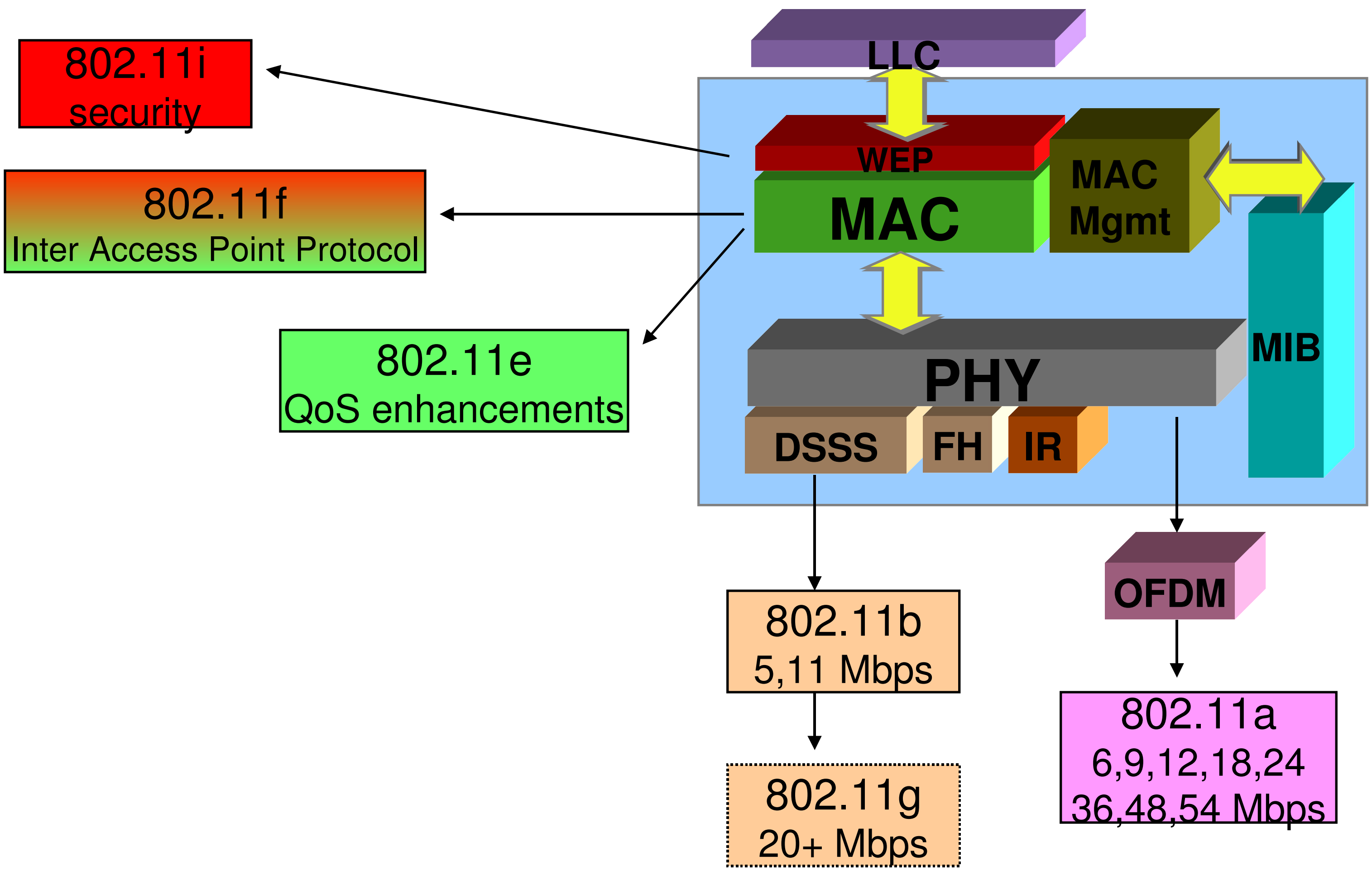
802.11 - Roaming

- No or bad connection in PCF mode? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

Hardware

- Original WaveLAN card (NCR)
  - 914 MHz Radio Frequency
  - Transmit power 281.8 mW
  - Transmission Range ~250 m (outdoors) at 2Mbps
  - SNRT 10 dB (capture)
- WaveLAN II (Lucent)
  - 2.4 GHz radio frequency range
  - Transmit Power 30mW
  - Transmission range 376 m (outdoors) at 2 Mbps (60m indoors)
  - Receive Threshold = –81dBm
  - Carrier Sense Threshold = -111dBm

802.11 current status



IEEE 802.11 Summary

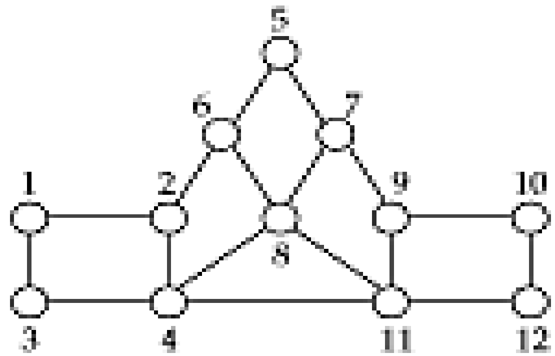
- Infrastructure (PCF) and adhoc (DCF) modes
- Signaling packets for collision avoidance
  - Medium is reserved for the duration of the transmission
  - Beacons in PCF
  - RTS-CTS in DCF
- Acknowledgements for reliability
- Binary exponential backoff for congestion control
- Power save mode for energy conservation

Outline

- Introduction and Overview
- Wireless LANs: IEEE 802.11
- **Mobile IP routing**
- TCP over wireless
- GSM air interface
- GPRS network architecture
- Wireless application protocol
- Mobile agents
- Mobile ad hoc networks

Traditional Routing

- A *routing protocol* sets up a *routing table* in *routers*



ROUTING TABLE AT 1

Destination	Next hop	Destination	Next hop
1	—	7	2
2	2□	8□	2□
3	3□	9□	2□
4	3□	10□	2□
5	2□	11□	3□
6	2	12	3

- Routing protocol is typically based on Distance-Vector or Link-State algorithms

Routing and Mobility

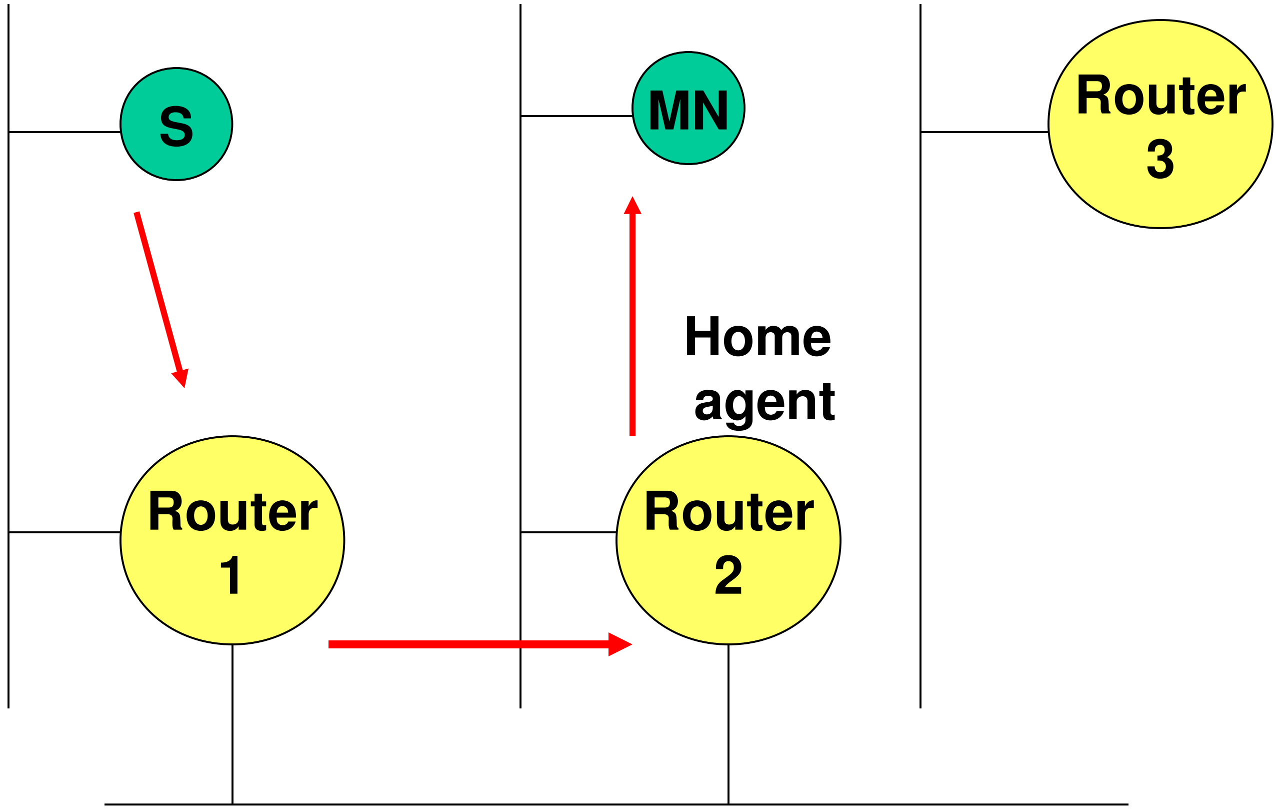
- Finding a path from a source to a destination
- Issues
  - Frequent route changes
    - amount of data transferred between route changes may be much smaller than traditional networks
  - Route changes may be related to host movement
  - Low bandwidth links

- Goal of routing protocols
  - decrease routing-related overhead
  - find short routes
  - find “stable” routes (despite mobility)

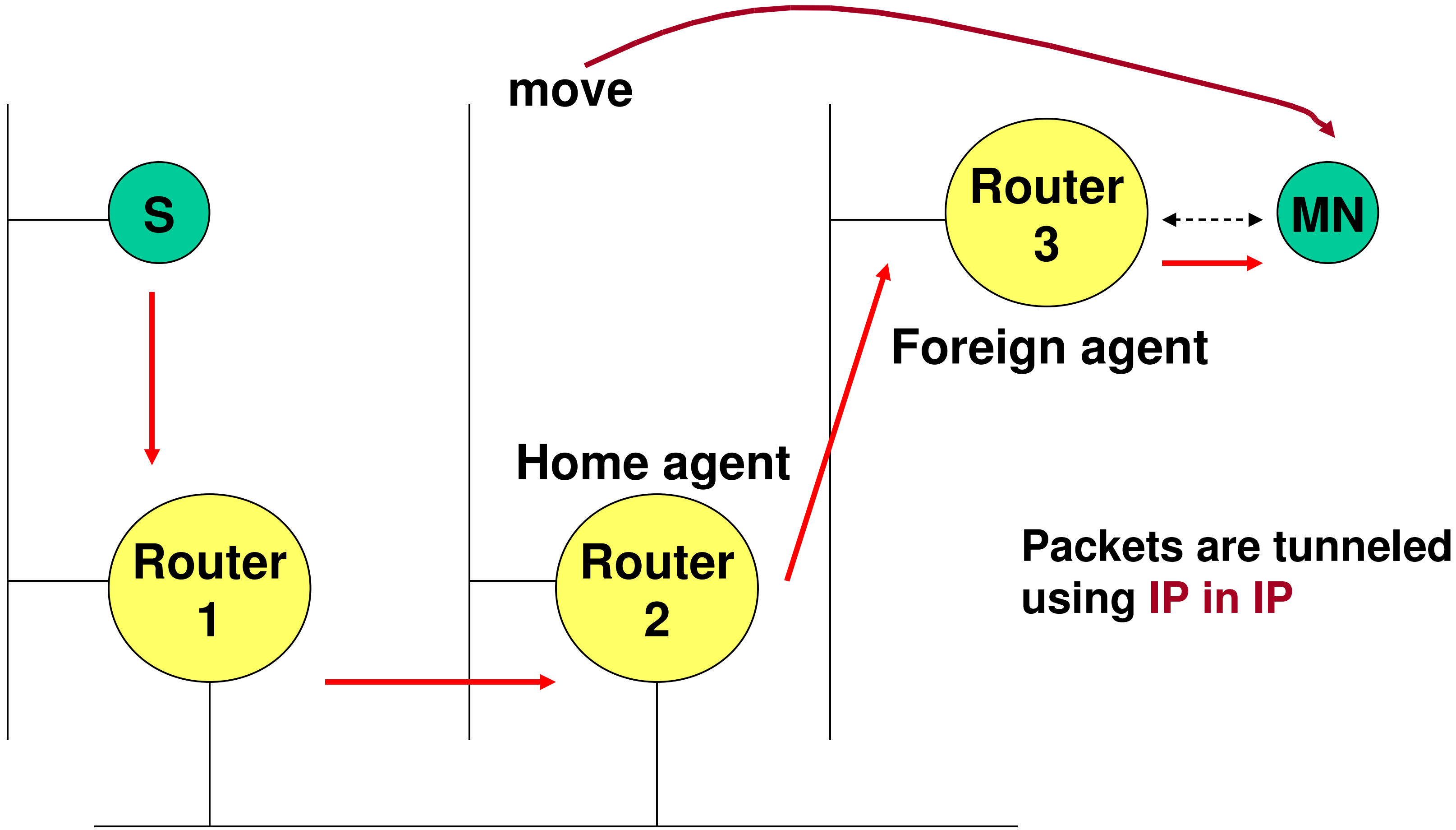
Mobile IP (RFC 3220): Motivation

- Traditional routing
  - based on IP address; network prefix determines the 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, …

Mobile IP: Basic Idea



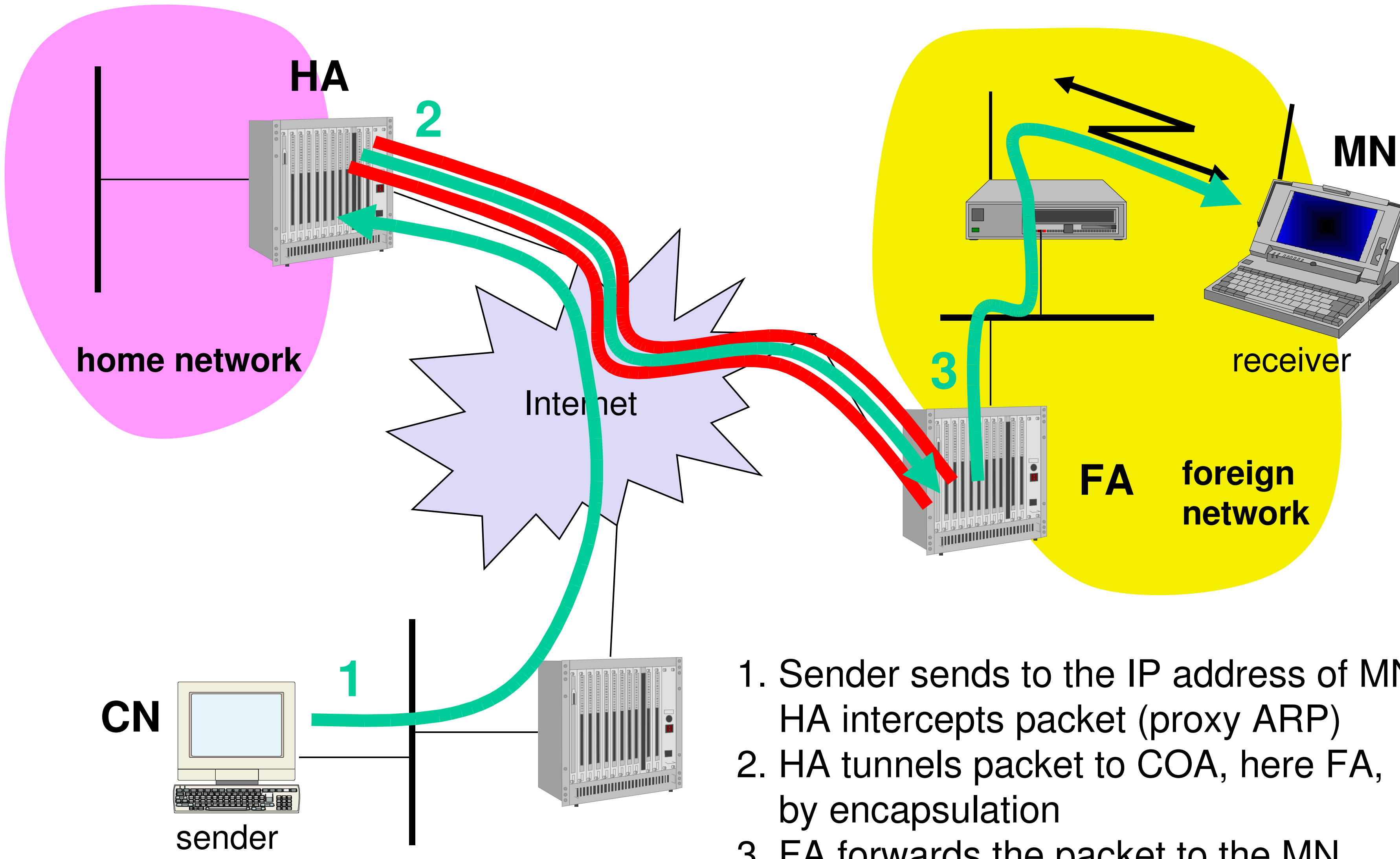
Mobile IP: Basic Idea



Mobile IP: Terminology

- Mobile Node (MN)
  - node that moves across networks without changing its IP address
- Home Agent (HA)
  - host in the home network of the MN, typically a router
  - registers the location of the MN, tunnels IP packets to the COA
- Foreign Agent (FA)
  - host in the current foreign network of the MN, typically a router
  - forwards tunneled packets to the MN, typically the default router for MN
- Care-of Address (COA)
  - address of the current tunnel end-point for the MN (at FA or MN)
  - actual location of the MN from an IP point of view
- Correspondent Node (CN)
  - host with which MN is “corresponding” (TCP connection)

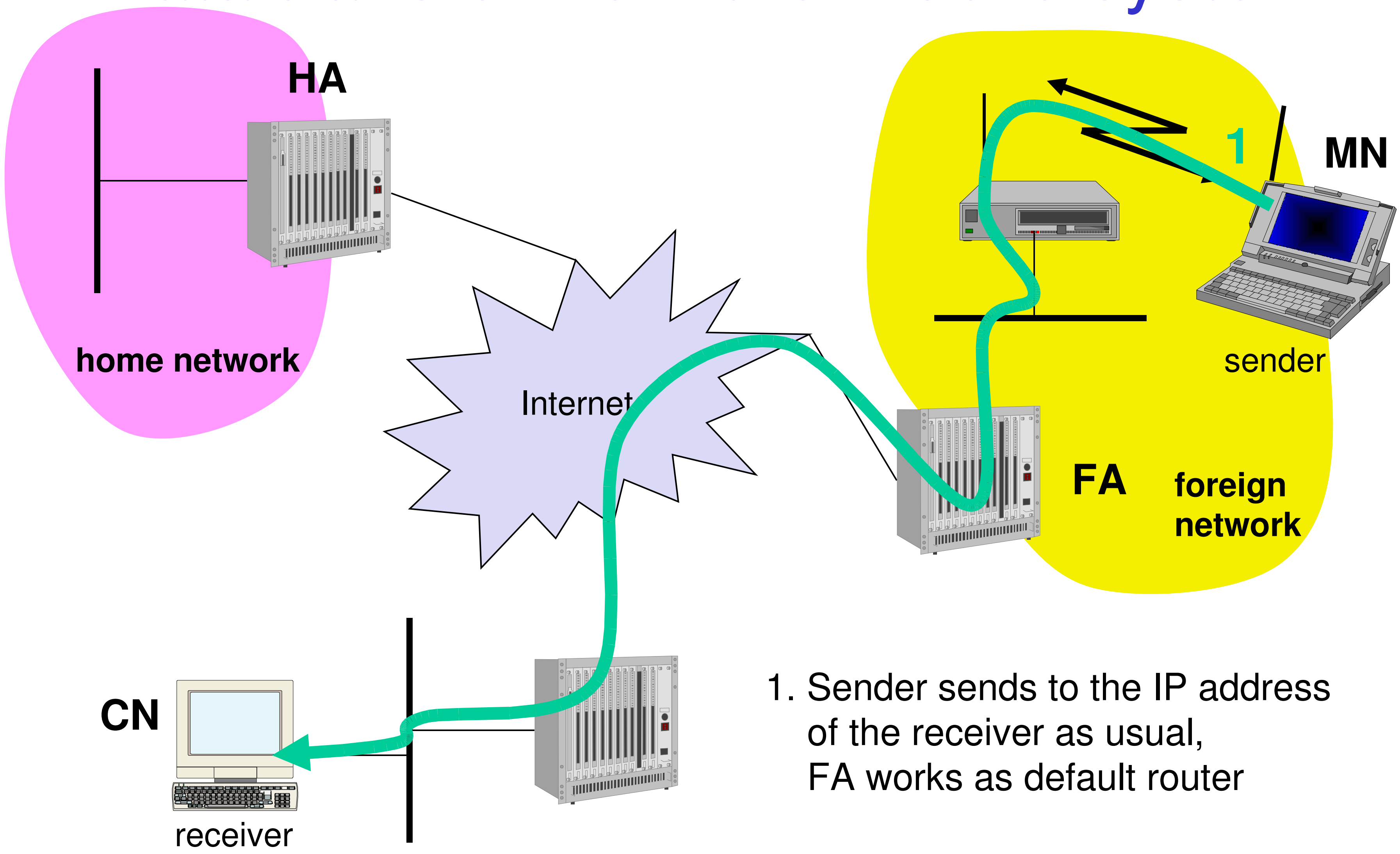
Data transfer to the mobile system



1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Source: Schiller

Data transfer from the mobile system



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

Source: Schiller

Mobile IP: Basic Operation

- Agent Advertisement
  - HA/FA periodically send advertisement messages into their physical subnets
  - MN listens to these messages and detects, if it is in home/foreign network
  - MN reads a COA from the FA advertisement messages
- MN Registration
  - MN signals COA to the HA via the FA
  - HA acknowledges via FA to MN
  - limited lifetime, need to be secured by authentication
- HA Proxy
  - HA advertises the IP address of the MN (as for fixed systems)
  - packets to the MN are sent to the HA
  - independent of changes in COA/FA
- Packet Tunneling
  - HA to MN via FA

Agent advertisement

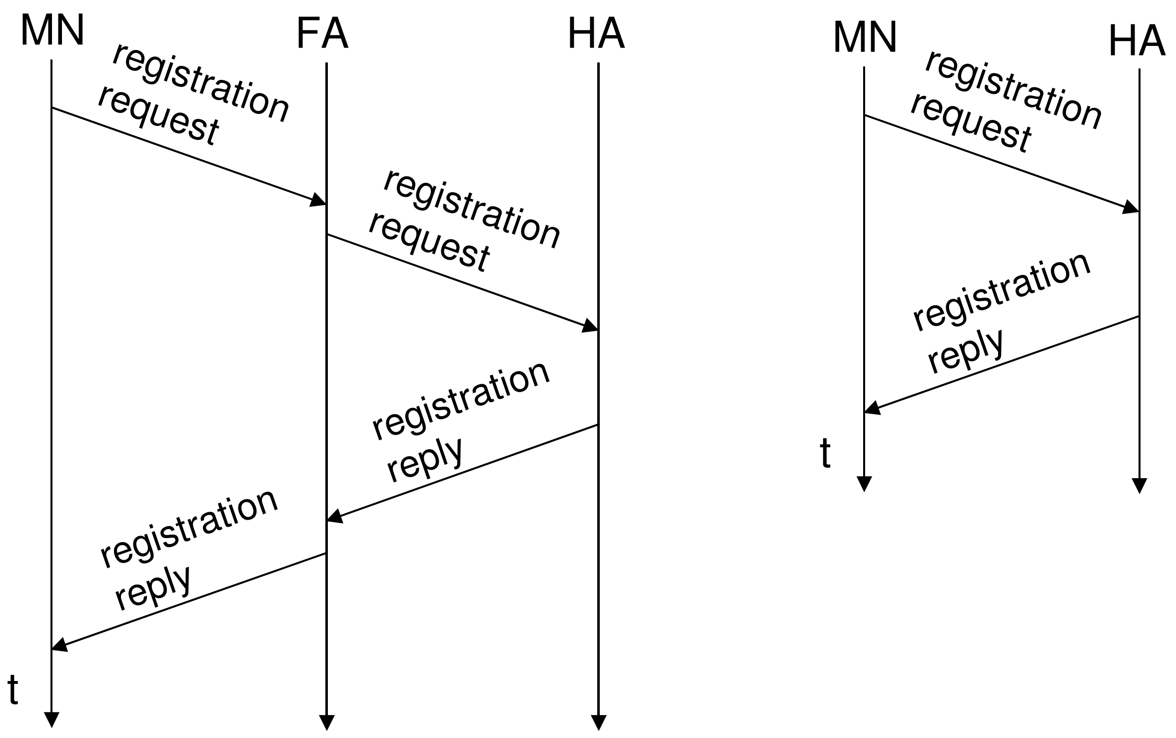
0 … 7	8 … 15	16 … 23	24 … 31
type	code	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			

. . .

type	length	sequence number								
registration lifetime		R	B	H	F	M	G	V	reserved	
COA 1										
COA 2										

. . .

Registration



Registration request

0 – 7	8 – 15	16 – 23	24 – 31
type	S B D M G V rsv	lifetime	
home address			
home agent			
COA			
identification			
extensions . . .			

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-in-IP*	IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	TOS	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ... payload				

Mobile IP: Other Issues

- Reverse Tunneling
  - firewalls permit only “topological correct“ addresses
  - a packet from the MN encapsulated by the FA is now topological correct
- Optimizations
  - Triangular Routing
    - HA informs sender the current location of MN
  - Change of FA
    - new FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA

Mobile IP Summary

- Mobile node moves to new location
- Agent Advertisement by foreign agent
- Registration of mobile node with home agent
- Proxying by home agent for mobile node
- Encapsulation of packets
- Tunneling by home agent to mobile node via foreign agent

- Reverse tunneling
- Optimizations for triangular routing

Outline

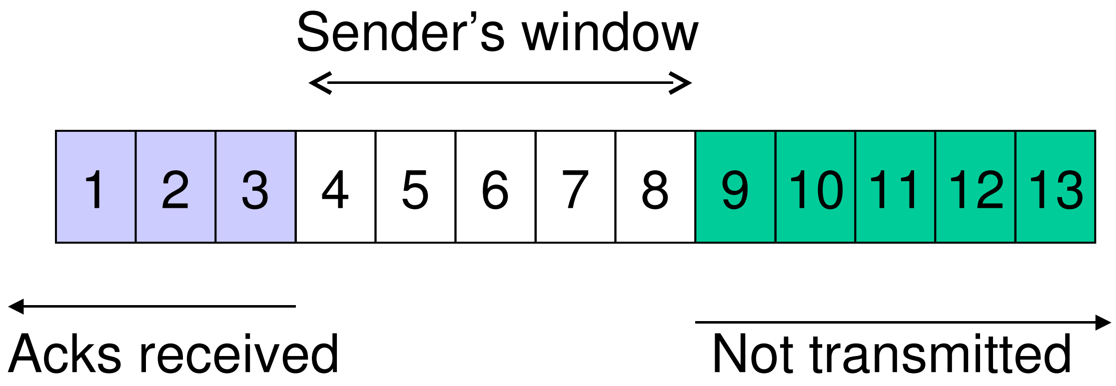
- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- **TCP over wireless**
- GSM air interface
- GPRS network architecture
- Wireless application protocol
- Mobile agents
- Mobile ad hoc networks

Transmission Control Protocol (TCP)

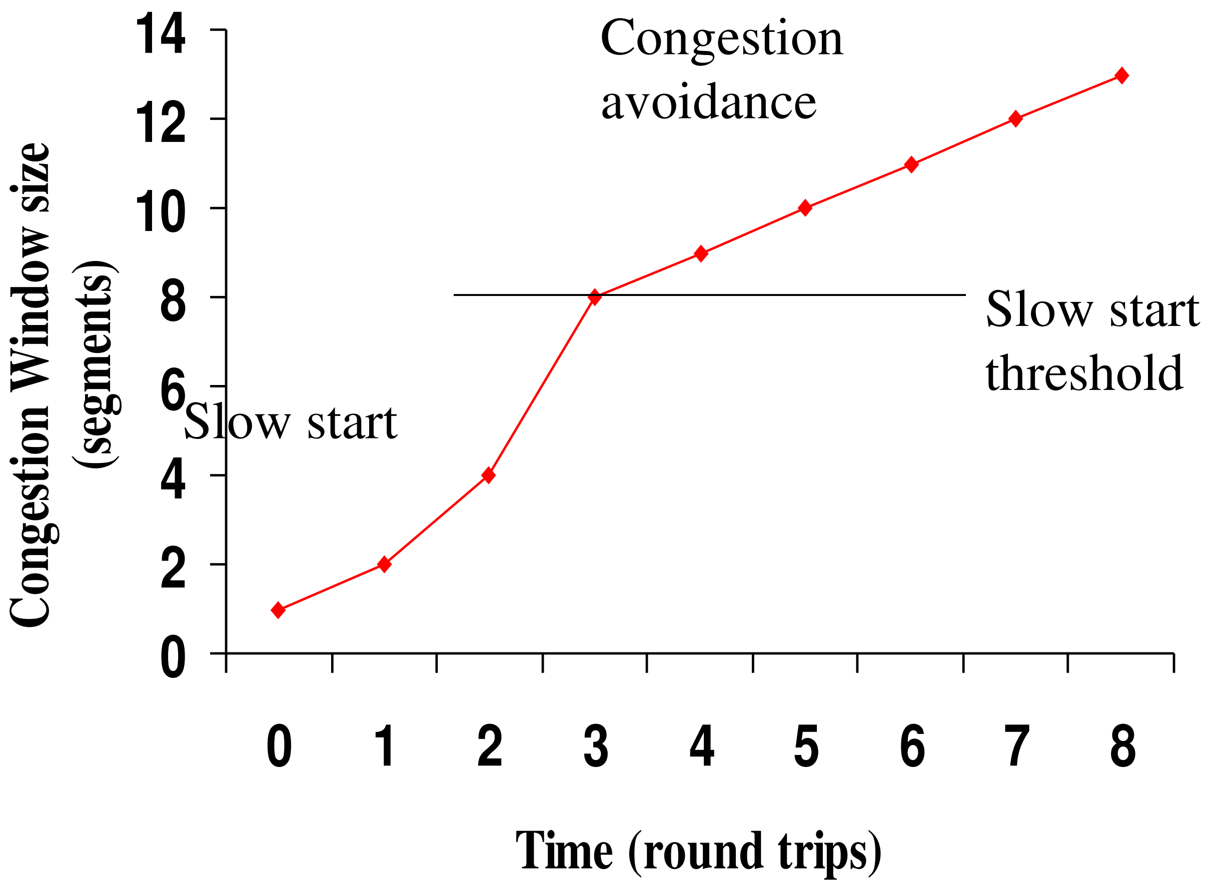
- Reliable ordered delivery
  - Acknowledgements and Retransmissions
- End-to-end semantics
  - Acknowledgements sent to TCP sender confirm delivery of data received by TCP receiver
  - Ack for data sent only **after** data has reached receiver
  - Cumulative Ack
- Implements congestion avoidance and control

Window Based Flow Control

- Sliding window protocol
- Window size minimum of
  - receiver's advertised window - determined by available buffer space at the receiver
  - congestion window - determined by the sender, based on feedback from the network



Basic TCP Behaviour

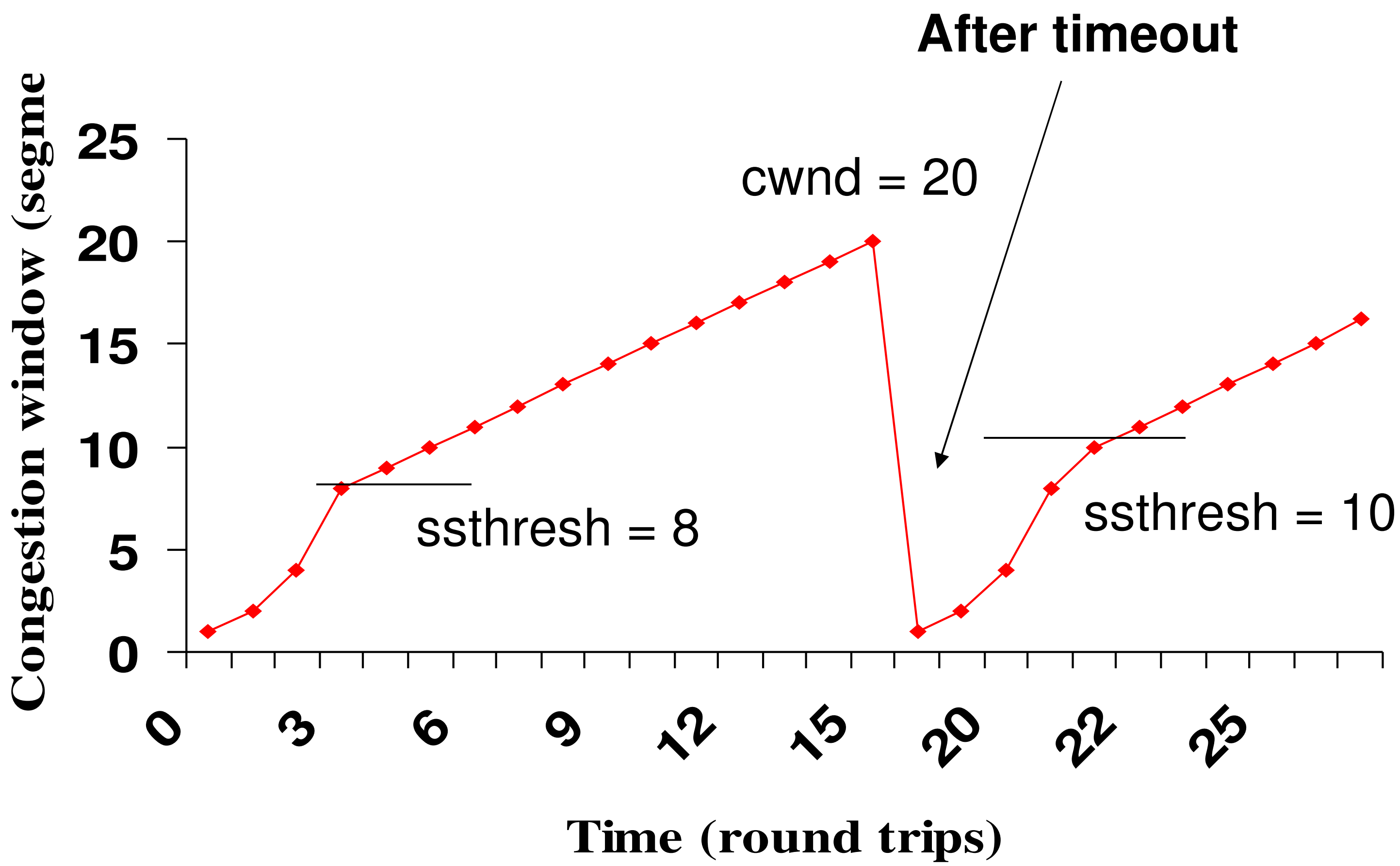


Example assumes that acks are not delayed

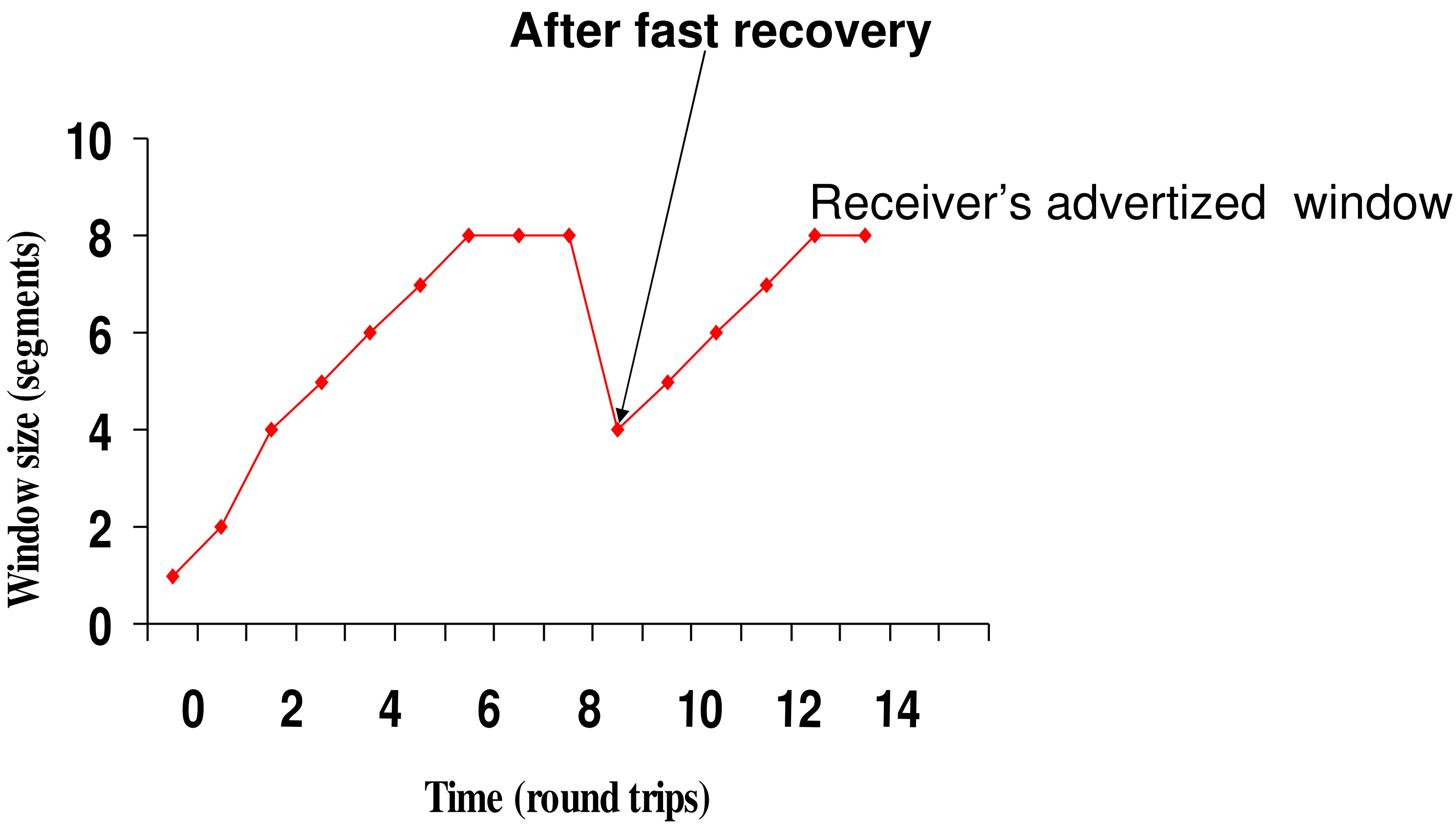
TCP: Detecting Packet Loss

- Retransmission timeout
  - Initiate Slow Start
- Duplicate acknowledgements
  - Initiate Fast Retransmit
- Assumes that ALL packet losses are due to congestion

TCP after Timeout



TCP after Fast Retransmit



After fast retransmit and fast recovery window size is
reduced in half.

Impact of Transmission Errors

- Wireless channel may have bursty random errors

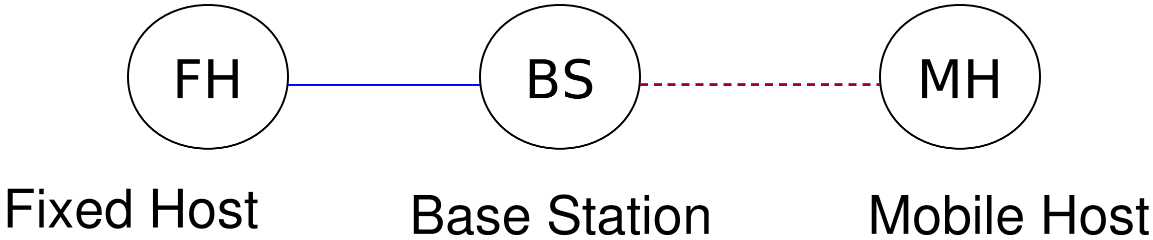
- Burst errors may cause timeout
- Random errors may cause fast retransmit
- TCP cannot distinguish between packet losses due to congestion and transmission errors

- Unnecessarily reduces congestion window
- Throughput suffers

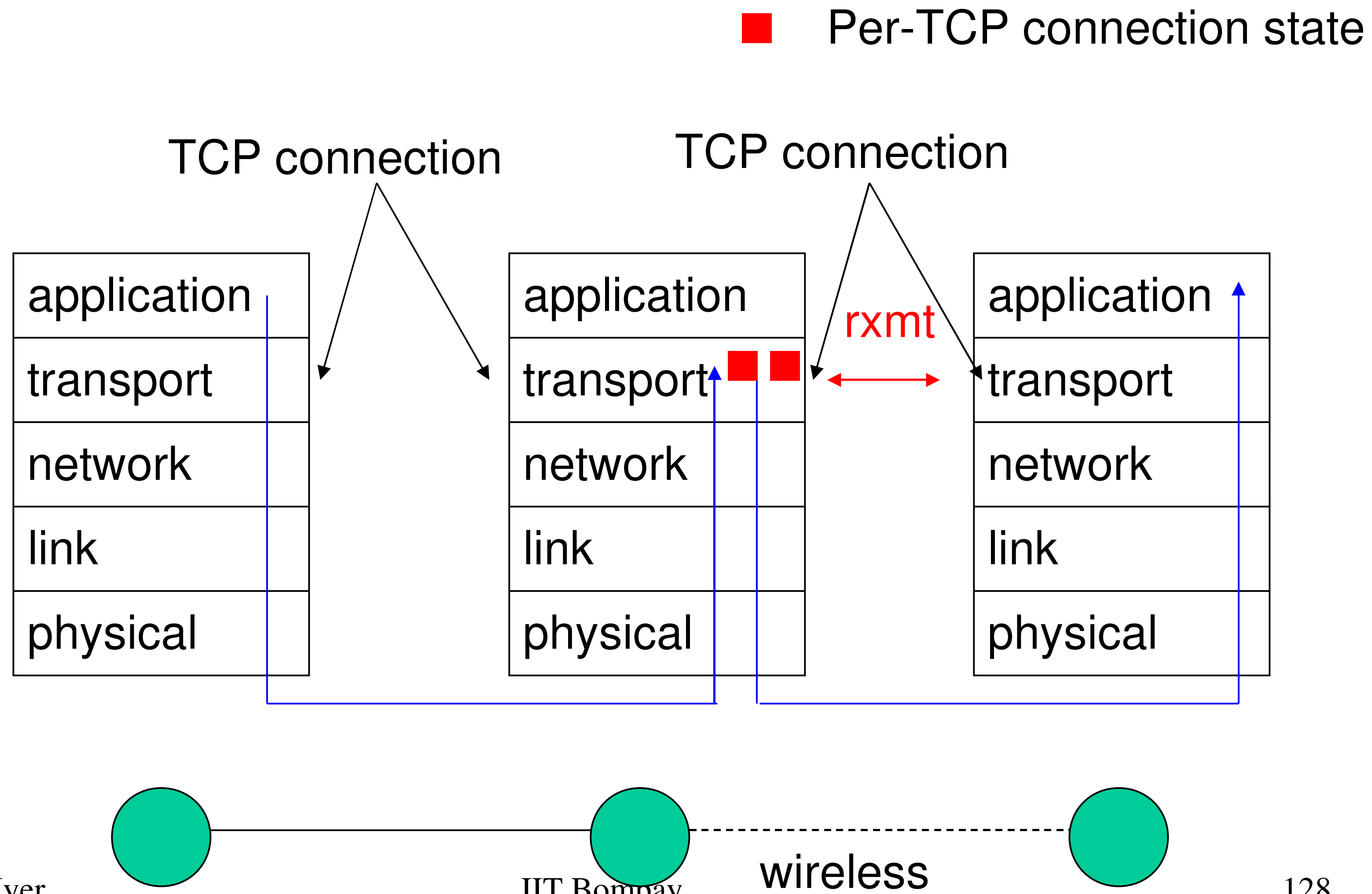
Split Connection Approach

- End-to-end TCP connection is broken into one connection on the wired part of route and one over wireless part of the route

- Connection between wireless host MH and fixed host FH goes through base station BS
- FH-MH = FH-BS + BS-MH

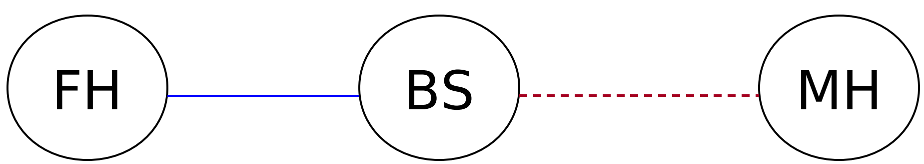


I-TCP: Split Connection Approach

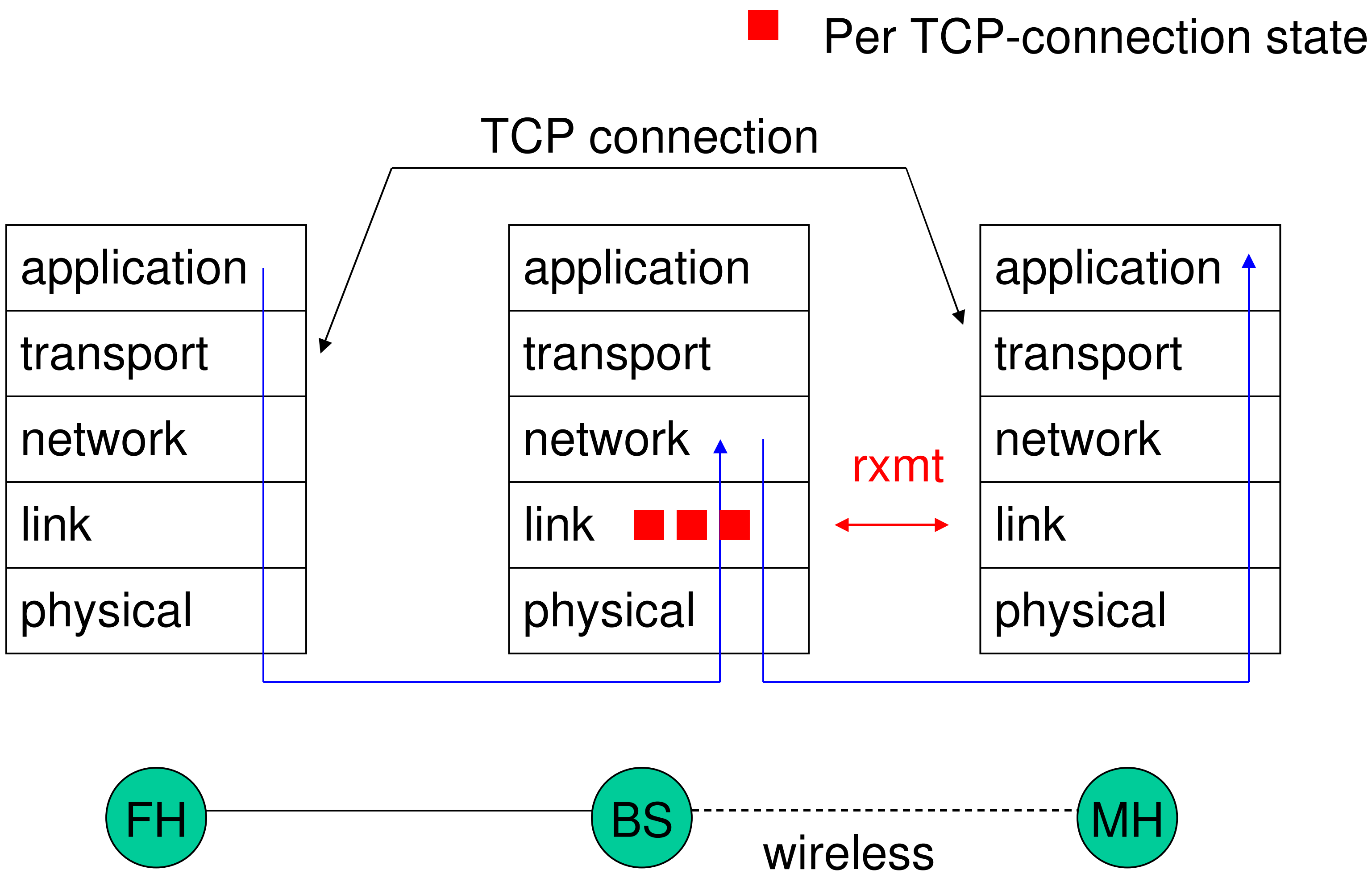


Snoop Protocol

- Buffers data packets at the base station BS
  - to allow link layer retransmission
- When dupacks received by BS from MH
  - retransmit on wireless link, if packet present in buffer
  - drop dupack
- Prevents fast retransmit at TCP sender FH



Snoop Protocol

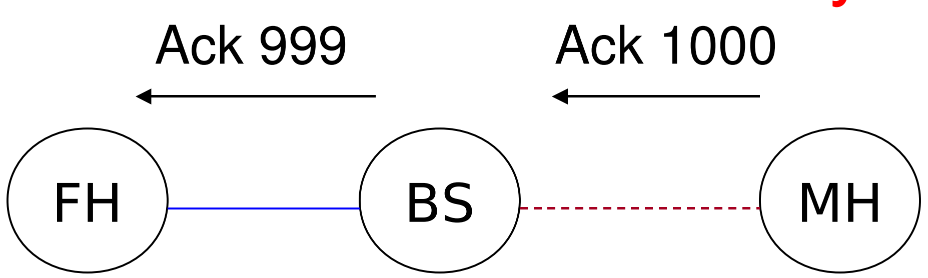


Impact of Handoffs

- Split connection approach
  - hard state at base station must be moved to new base station
- Snoop protocol
  - soft state need not be moved
  - while the new base station builds new state, packet losses may not be recovered locally
- Frequent handoffs a problem for schemes that rely on significant amount of hard/soft state at base stations
  - hard state should not be lost
  - soft state needs to be recreated to benefit performance

M-TCP

- Similar to the split connection approach, M-TCP splits one TCP connection into two logical parts
  - the two parts have independent flow control as in I-TCP
- The BS does not send an ack to MH, unless BS has received an ack from MH
  - maintains end-to-end semantics
- BS withholds ack for the last byte ack'd by MH



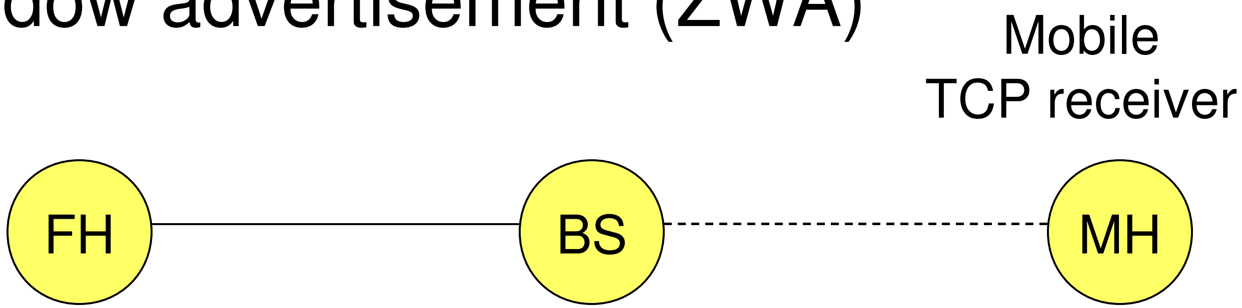
M-TCP

- When a new ack is received with receiver's advertised window = 0, the sender enters persist mode
- Sender does not send any data in persist mode
  - except when persist timer goes off

- When a positive window advertisement is received, sender exits persist mode
- On exiting persist mode, RTO and cwnd are same as before the persist mode

FreezeTCP

- M-TCP needs help from base station
  - Base station withholds ack for one byte
  - The base station uses this ack to send a zero window advertisement when a mobile host moves to another cell
- **FreezeTCP** requires the receiver to send zero window advertisement (ZWA)



TCP over wireless summary

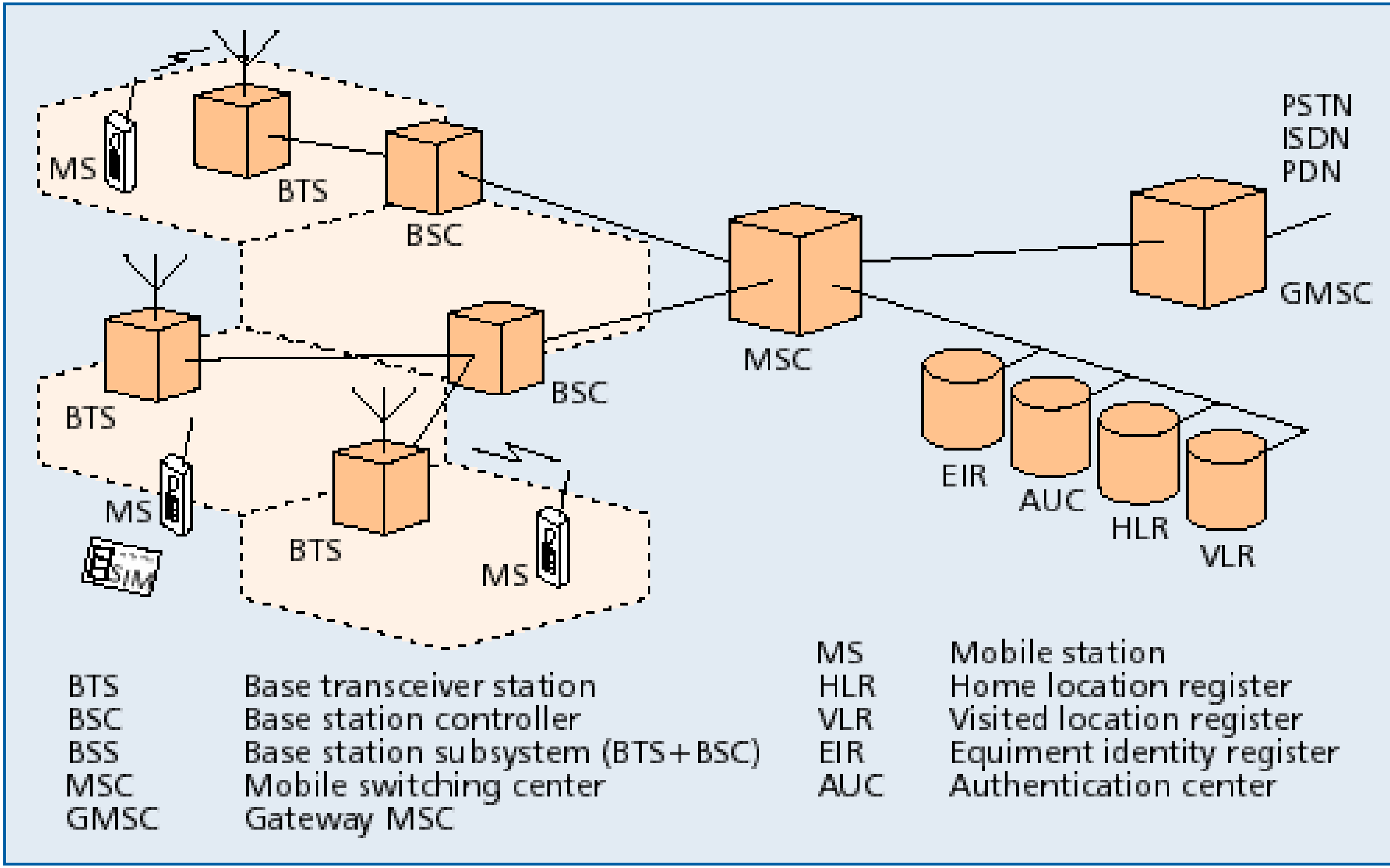
- Assuming that packet loss implies congestion is invalid in wireless mobile environments
- Invoking congestion control in response to packet loss is in appropriate

- Several proposals to adapt TCP to wireless environments
- Modifications at
  – Fixed Host
  – Base Station
  – Mobile Host

Outline

- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- TCP over wireless
- **GSM air interface**
- GPRS network architecture
- Wireless application protocol
- Mobile agents
- Mobile ad hoc networks

GSM: System Architecture



Base Transceiver Station (BTS)

- One per cell
- Consists of high speed transmitter and receiver
- Function of BTS
  - Provides two channel
    - Signalling and Data Channel
    - Message scheduling
    - Random access detection
  - Performs error protection coding for the radio channel
    - Rate adaptation
- Identified by BTS Identity Code (BSIC)

Base Station Controller (BSC)

- Controls multiple BTS
- Consists of essential control and protocol intelligence entities
- Functions of BSC
  - Performs radio resource management
    - Assigns and releases frequencies and time slots for all the MSs in its area
    - Reallocation of frequencies among cells
    - Hand over protocol is executed here
  - Time and frequency synchronization signals to BTSs
  - Time Delay Measurement and notification of an MS to BTS
  - Power Management of BTS and MS

Mobile Switching Center (MSC)

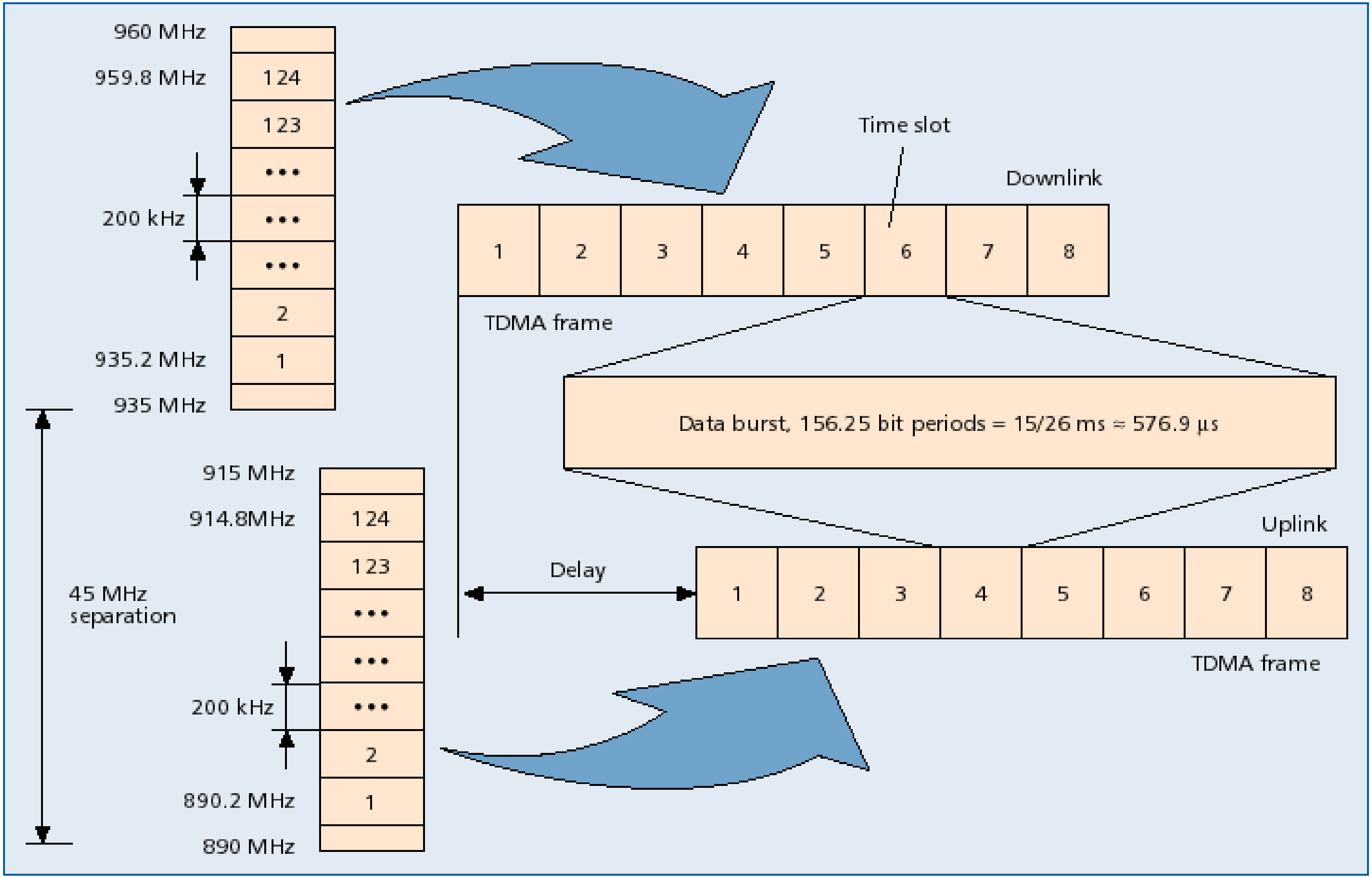
- Switching node of a PLMN
- Allocation of radio resource (RR)
  - Handover
- Mobility of subscribers
  - Location registration of subscriber
- There can be several MSC in a PLMN

Gateway MSC (GMSC)

- Connects mobile network to a fixed network
  - Entry point to a PLMN
- Usually one per PLMN
- Request routing information from the HLR and routes the connection to the local MSC

Air Interface: Physical Channel

- Uplink/Downlink of 25MHz
  - 890 -915 MHz for Up link
  - 935 - 960 MHz for Down link
- Combination of frequency division and time division multiplexing
  - FDMA
    - 124 channels of 200 kHz
    - 200 kHz guard band
  - TDMA
    - Burst
- Modulation used
  - Gaussian Minimum Shift Keying (GMSK)

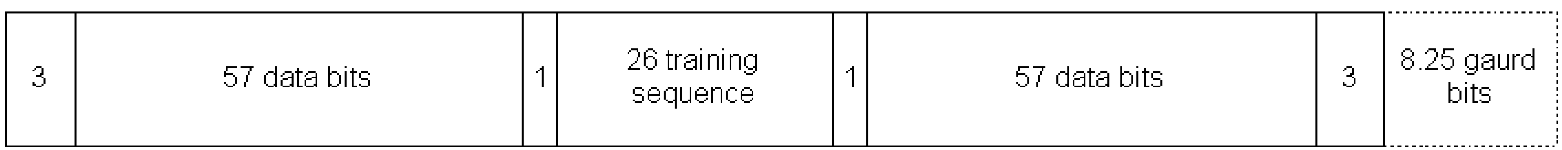

960 MHz
959.8 MHz
124
123
•••
200 kHz
•••
•••
2
935.2 MHz
1
935 MHz
Time slot
Downlink
1
2
3
4
5
6
7
8
TDMA frame
Data burst, 156.25 bit periods = 15/26 ms ≈ 576.9 µs
45 MHz
separation
915 MHz
914.8MHz
124
123
•••
•••
200 kHz
•••
2
890.2 MHz
1
890 MHz
Uplink
Delay
1
2
3
4
5
6
7
8
TDMA frame

Bursts

- Building unit of physical channel
- Types of bursts
  - Normal
  - Synchronization
  - Frequency Correction
  - Dummy
  - Access

Normal Burst

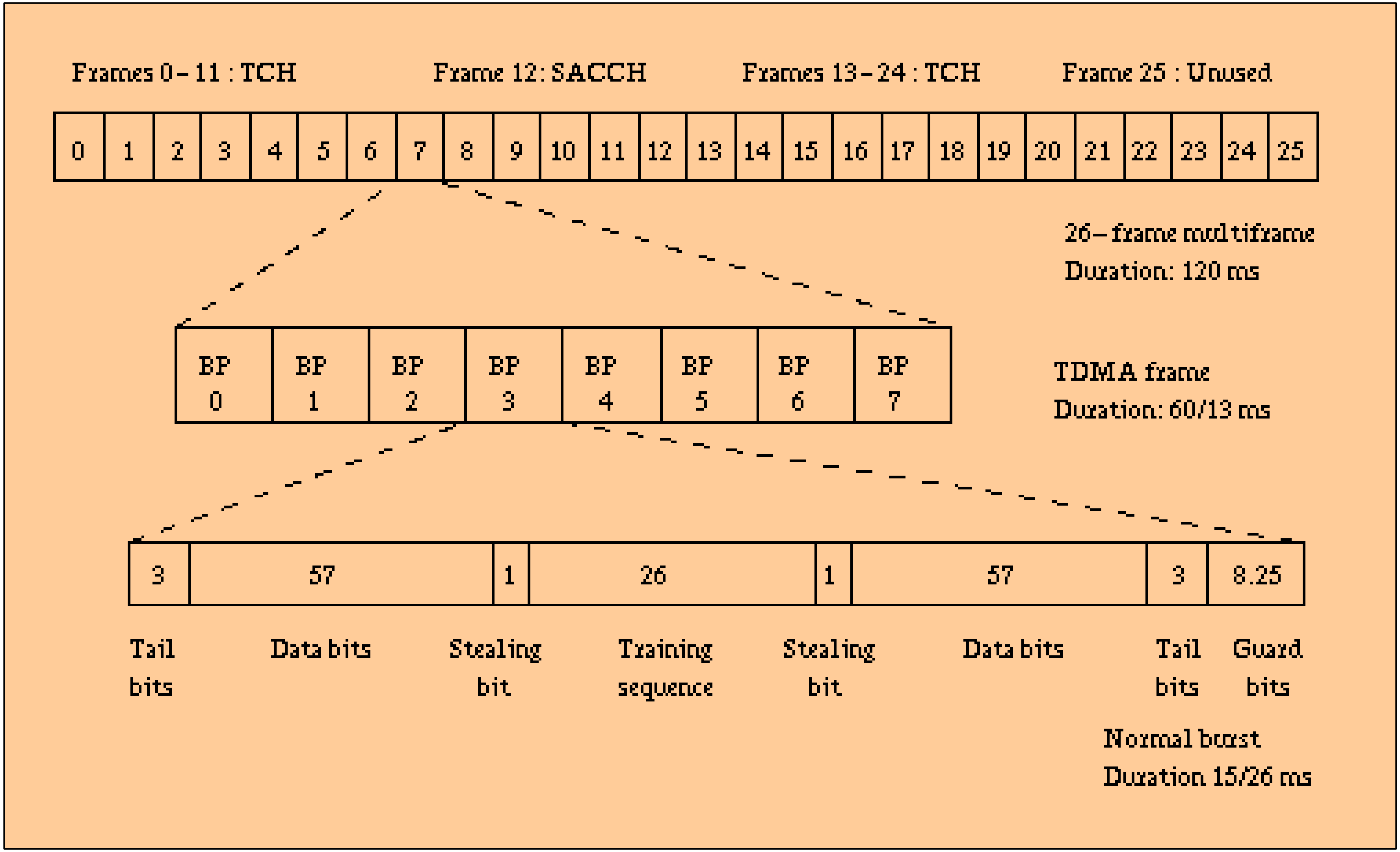
- Normal Burst
  - 2*(3 head bit + 57 data bits + 1 signaling bit) + 26 training sequence bit + 8.25 guard bit
  - Used for all except RACH, FSCH & SCH



Air Interface: Logical Channel

- Traffic Channel (TCH)

- Signaling Channel
  - Broadcast Channel (BCH)
  - Common Control Channel (CCH)
  - Dedicated/Associated Control Channel (DCCH/ACCH)


Frames 0 - 11 : TCH
Frame 12: SACCH
Frames 13 - 24 : TCH
Frame 25 : Unused
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26– frame multiframe
Duration: 120 ms
BP 0
BP 1
BP 2
BP 3
BP 4
BP 5
BP 6
BP 7
TDMA frame
Duration: 60/13 ms
3
57
1
26
1
57
3
8.25
Tail bits
Data bits
Stealing bit
Training sequence
Stealing bit
Data bits
Tail bits
Guard bits
Normal burst
Duration 15/26 ms

Traffic Channel

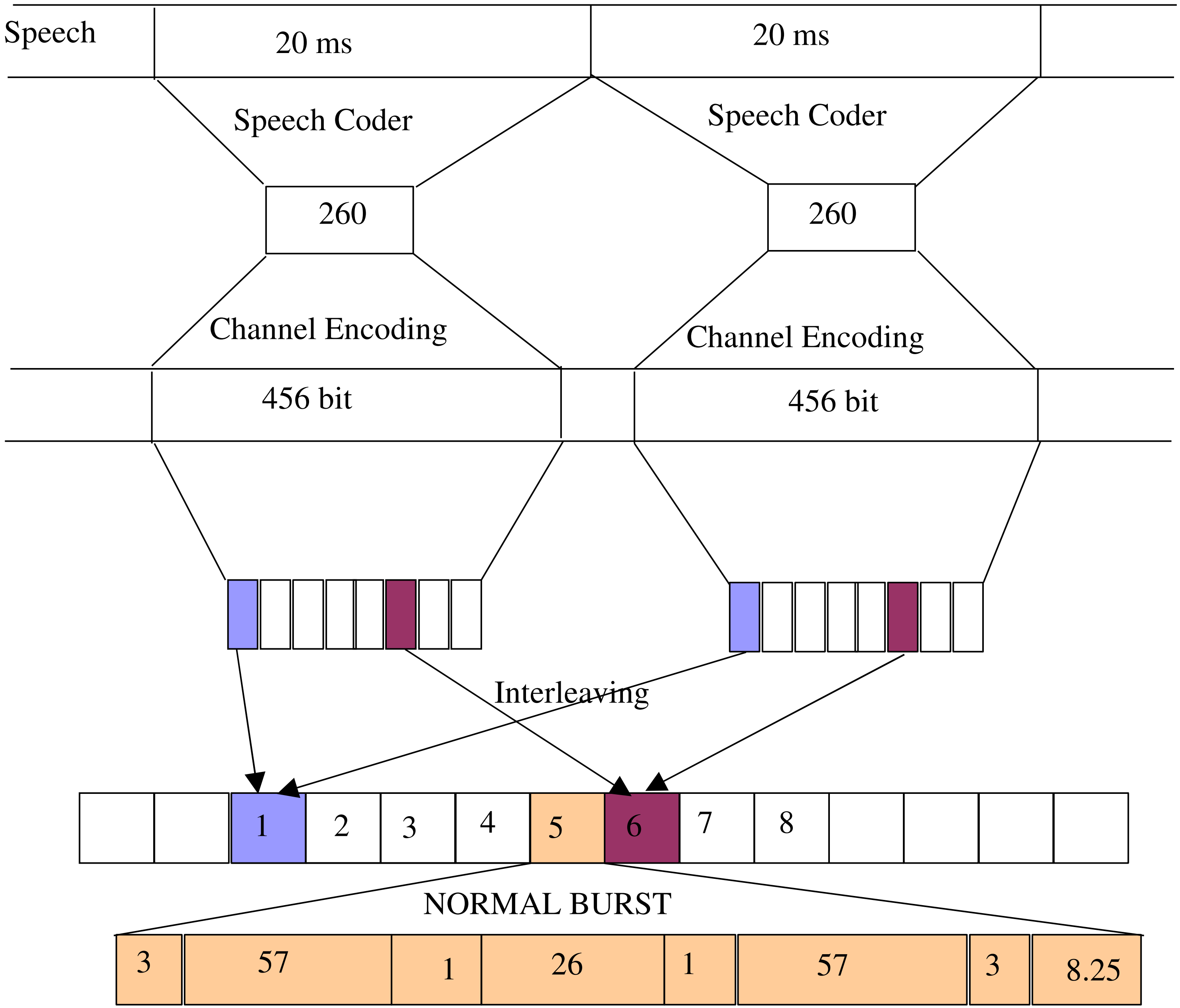
- Transfer either encoded speech or user data
- Bidirectional

- Full Rate TCH
  - Rate 22.4kbps
  - Bm interface

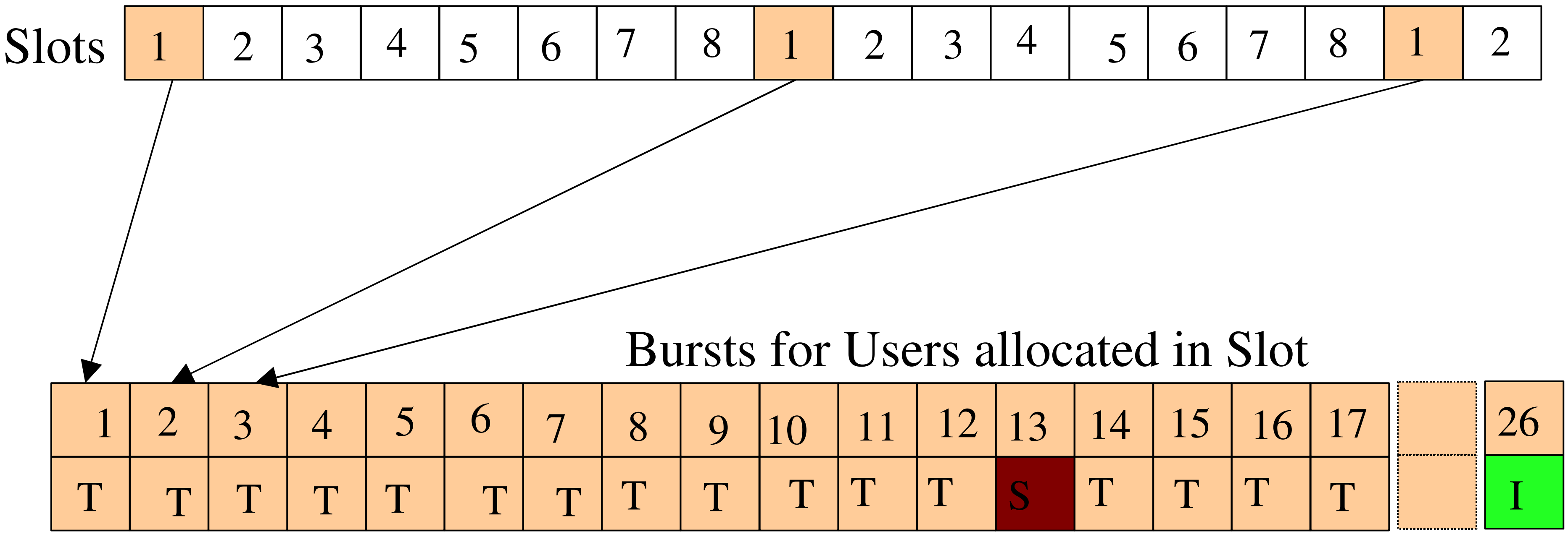
- Half Rate TCH
  - Rate 11.2 kbps
  - Lm interface

Full Rate Speech Coding

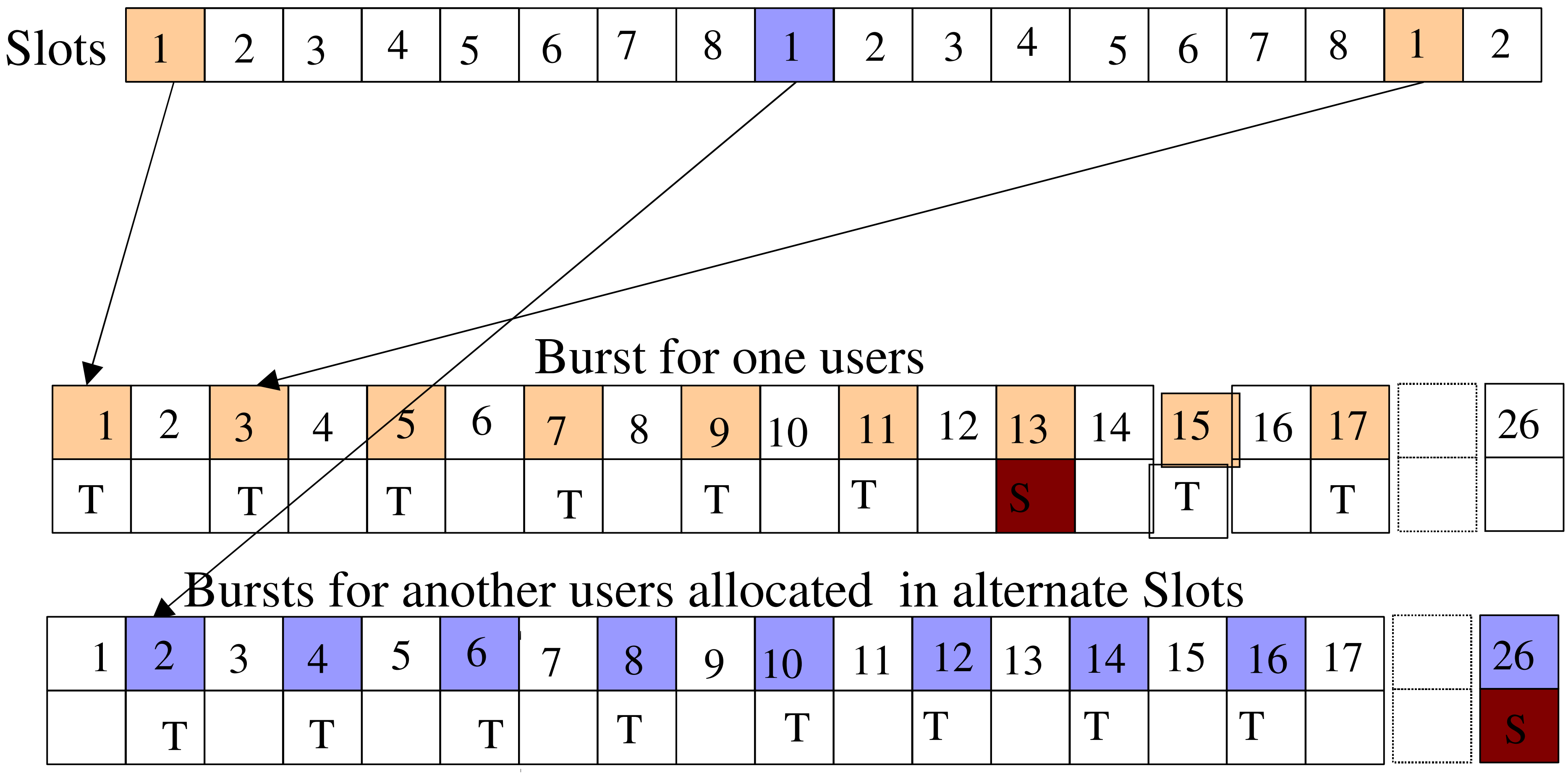
- Speech Coding for 20ms segments
  - 260 bits at the output
  - Effective data rate 13kbps
- Unequal error protection
  - 182 bits are protected
    - 50 + 132 bits = 182 bits
  - 78 bits unprotected
- Channel Encoding
  - Codes 260 bits into (8 x 57 bit blocks) 456 bits
- Interleaving
  - 2 blocks of different set interleaved on a normal burst (save damages by error bursts)


Speech
20 ms
20 ms
Speech Coder
Speech Coder
260
260
Channel Encoding
Channel Encoding
456 bit
456 bit
Interleaving
1
2
3
4
5
6
7
8
NORMAL BURST
3
57
1
26
1
57
3
8.25
Out of first 20 ms
Out of second 20ms

Traffic Channel Structure for Full Rate Coding



T = Traffic
S = Signal(contains information about the signal strength in neighboring cells)



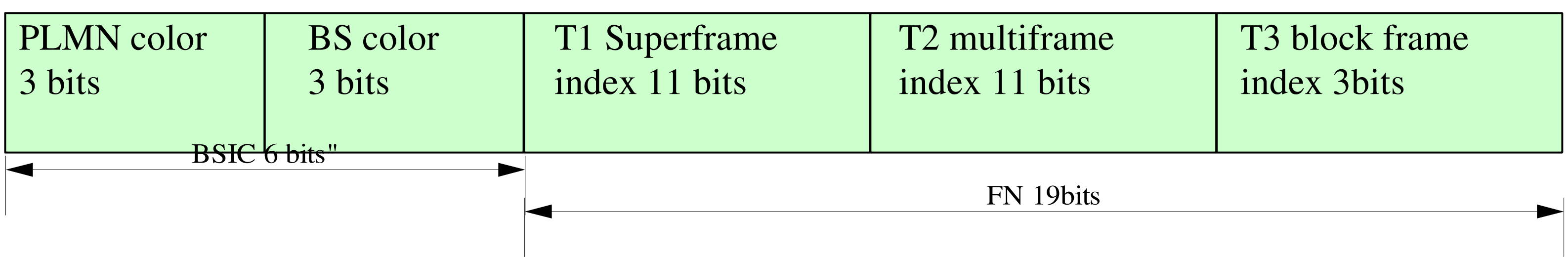
Traffic Channel Structure for Half Rate Coding

BCCH

- Broadcast Control Channel (BCCH)↓
  - BTS to MS
  - Radio channel configuration
    - Current cell + Neighbouring cells
  - Synchronizing information
    - Frequencies + frame numbering
  - Registration Identifiers
    - LA + Cell Identification (CI) + Base Station Identity Code (BSIC)

FCCH & SCH

- Frequency Correction Channel
  - Repeated broadcast of FB
- Synchronization Channel
  - Repeated broadcast of SB
  - Message format of SCH



RACH & SDCCH

- Random Access Channel (RACH)
  - MS to BTS
  - Slotted Aloha
  - Request for dedicated SDCCH

- Standalone Dedicated Control Channel (SDCCH)
  - MS ↔ BTS
  - Standalone; Independent of TCH

AGCH & PCH

- Access Grant Channel (AGCH)
  - BTS to MS
  - Assign an SDCCH/TCH to MS

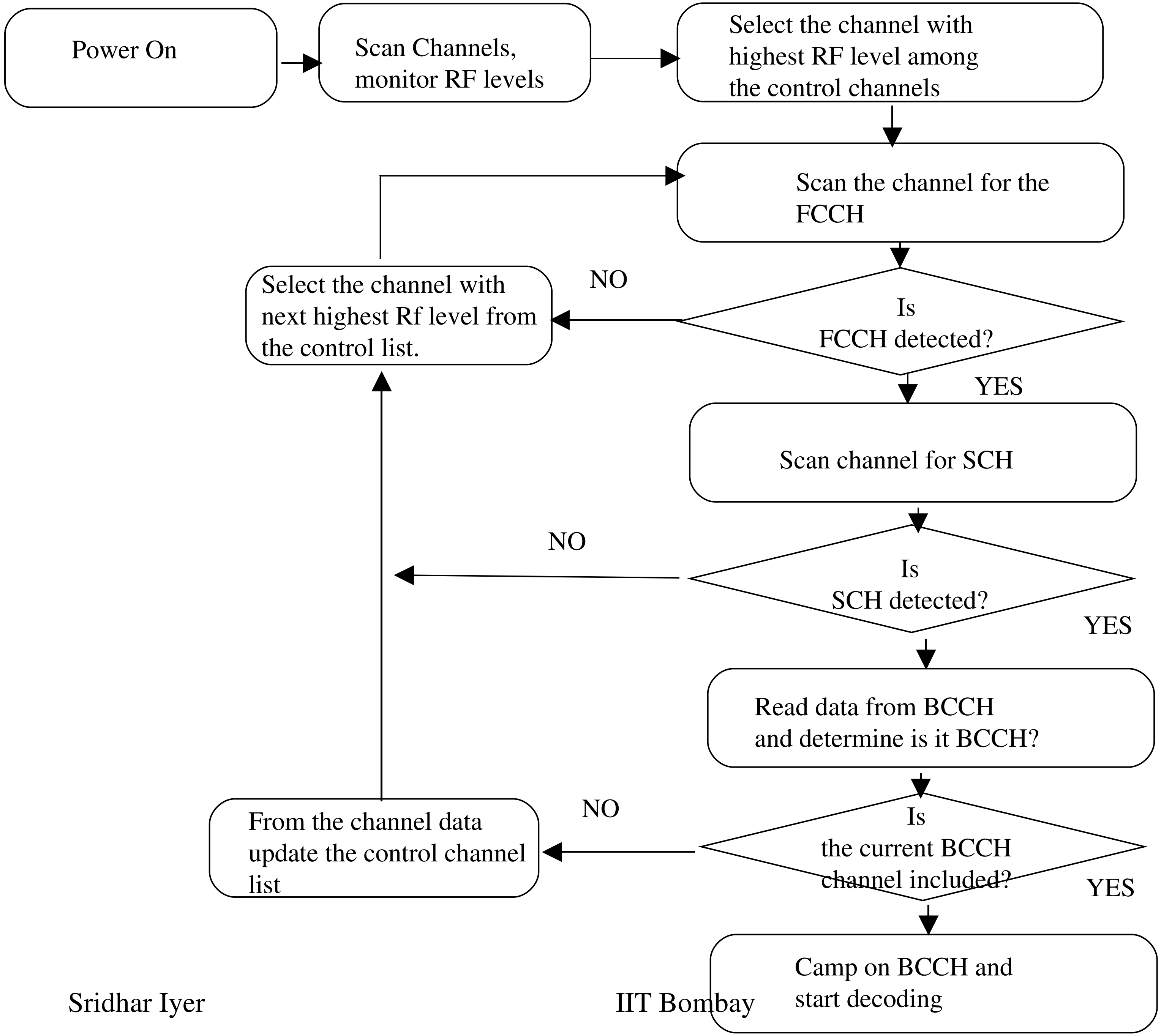
- Paging Channel (PCH)
  - BTS to MS
  - Page MS

SACCH & FACCH

- Slow Associated Control Channel (SACCH)
  - MS ↔ BTS
  - Always associated with either TCH or SDCCH
  - Information
    - Optimal radio operation; Commands for synchronization
    - Transmitter power control; Channel measurement
  - Should always be active; as proof of existence of physical radio connection
- Fast Associated Control Channel (FACCH)
  - MS ↔ BTS
    - Handover
    - Pre-emptive multiplexing on a TCH, Stealing Flag (SF)

Example: Incoming Call Setup

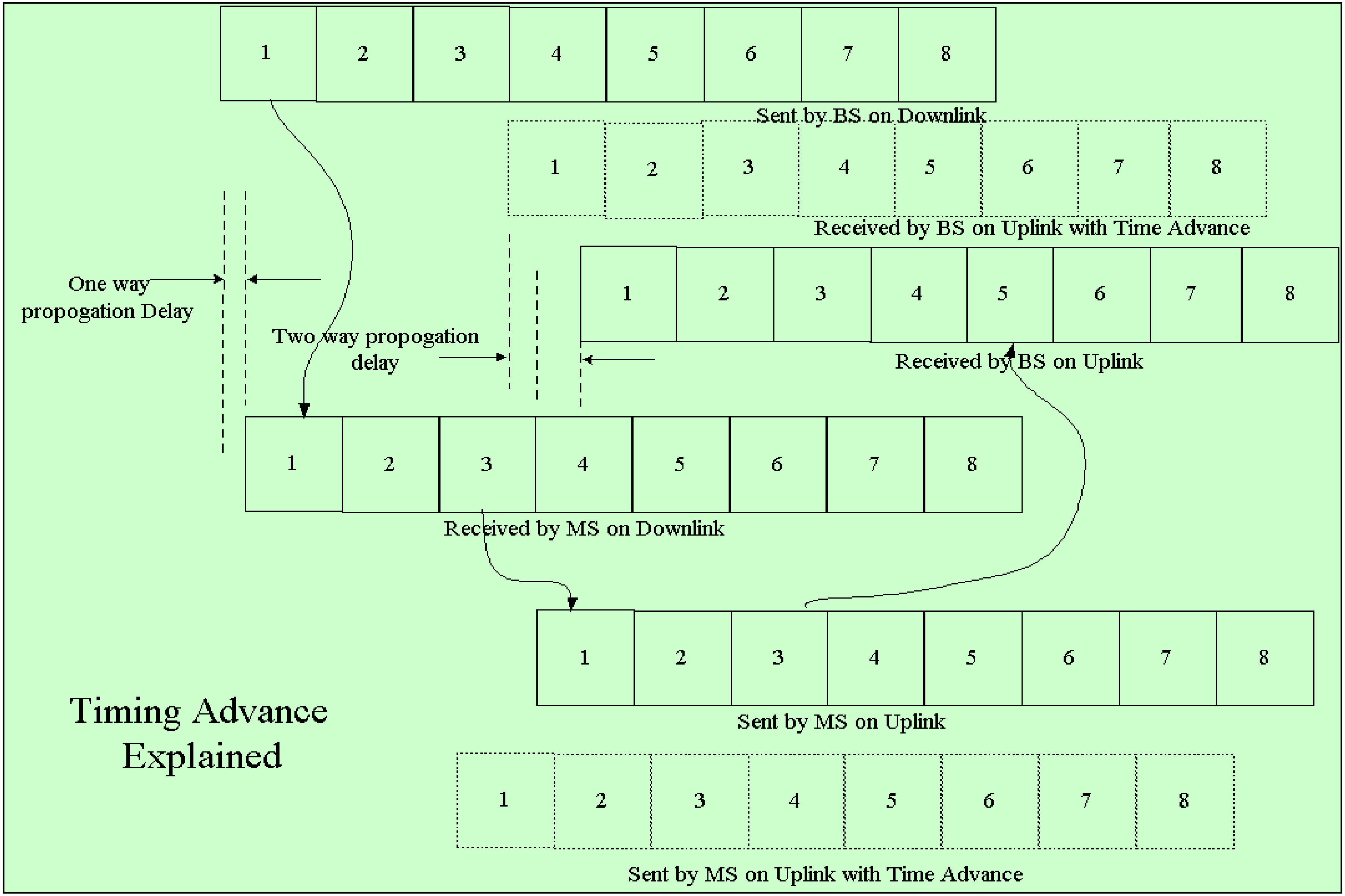
MS ↓BSS/MSC	------	Paging request	(PCH)
MS ↑BSS/MSC	------	Channel request	(RACH)
MS ↓BSS/MSC	------	Immediate Assignment	(AGCH)
MS ↑BSS/MSC	------	Paging Response	(SDCCH)
MS ↓BSS/MSC	------	Authentication Request	(SDCCH)
MS ↑BSS/MSC	------	Authentication Response	(SDCCH)
MS ↓BSS/MSC	------	Cipher Mode Command	(SDCCH)
MS ↑BSS/MSC	------	Cipher Mode Compl.	(SDCCH)
MS ↓BSS/MSC	------	Setup	(SDCCH)
MS ↑BSS/MSC	------	Call Confirmation	(SDCCH)
MS ↓BSS/MSC	------	Assignment Command	(SDCCH)
MS ↑BSS/MSC	------	Assignment Compl.	(FACCH)
MS ↑BSS/MSC	------	Alert	(FACCH)
MS ↑BSS/MSC	------	Connect	(FACCH)
MS ↓BSS/MSC	------	Connect Acknowledge	(FACCH)
MS ↔BSS/MSC	------	Data	(TCH)


Power On
Scan Channels, monitor RF levels
Select the channel with highest RF level among the control channels
Scan the channel for the FCCH
Is FCCH detected?
NO
Select the channel with next highest Rf level from the control list.
YES
Scan channel for SCH
Is SCH detected?
NO
YES
Read data from BCCH and determine is it BCCH?
Is the current BCCH channel included?
NO
From the channel data update the control channel list
YES
Camp on BCCH and start decoding

Adaptive Frame Synchronization

- Timing Advance
- Advance in Tx time corresponding to propagation delay

- 6 bit number used; hence 63 steps
- 63 bit period = 233 micro seconds (round trip time)
  - 35 Kms

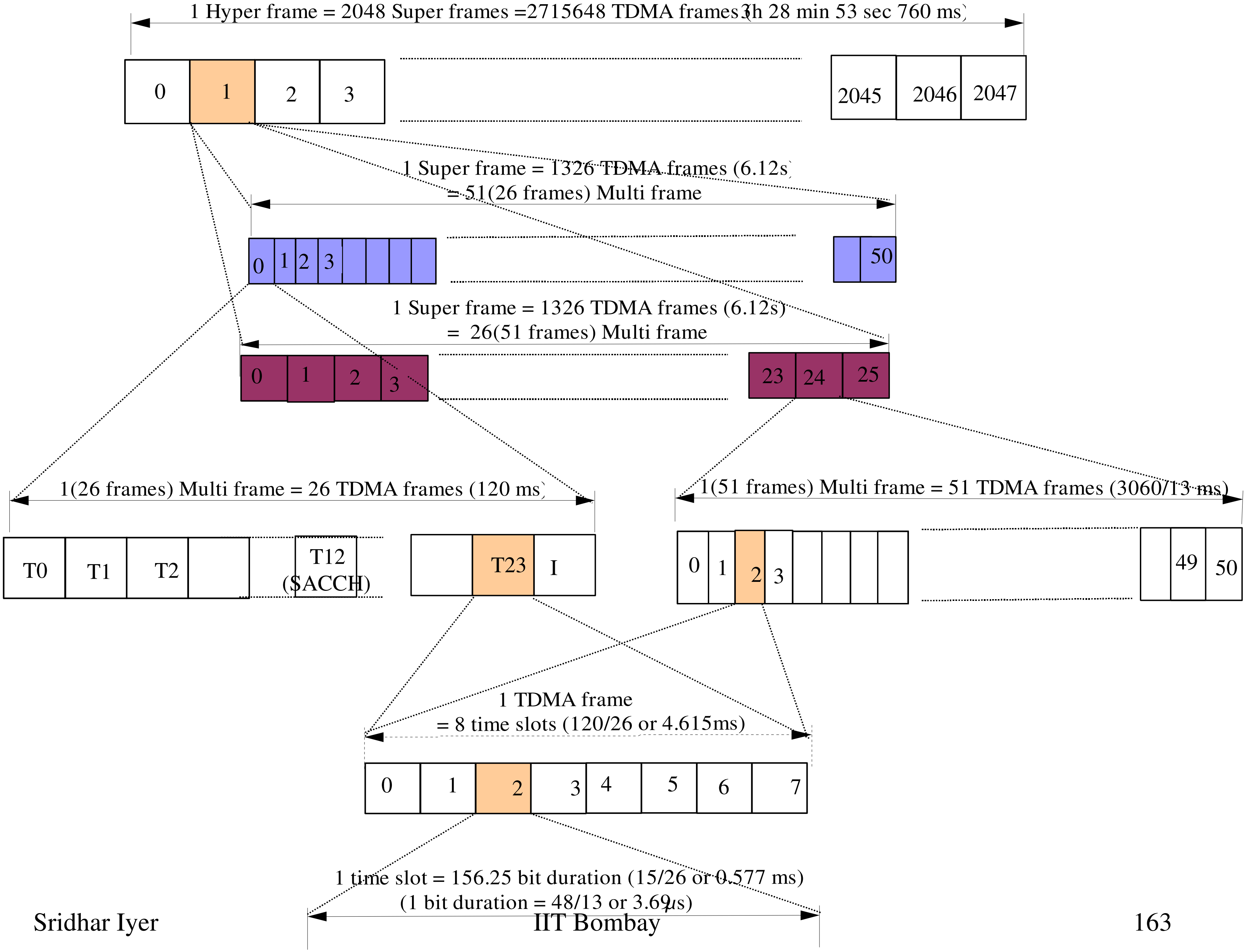


Timing Advance Explained

GSM: Channel Mapping Summary

- Logical channels
  - Traffic Channels; Control Channels
- Physical Channel
  - Time Slot Number; TDMA frame; RF Channel Sequence

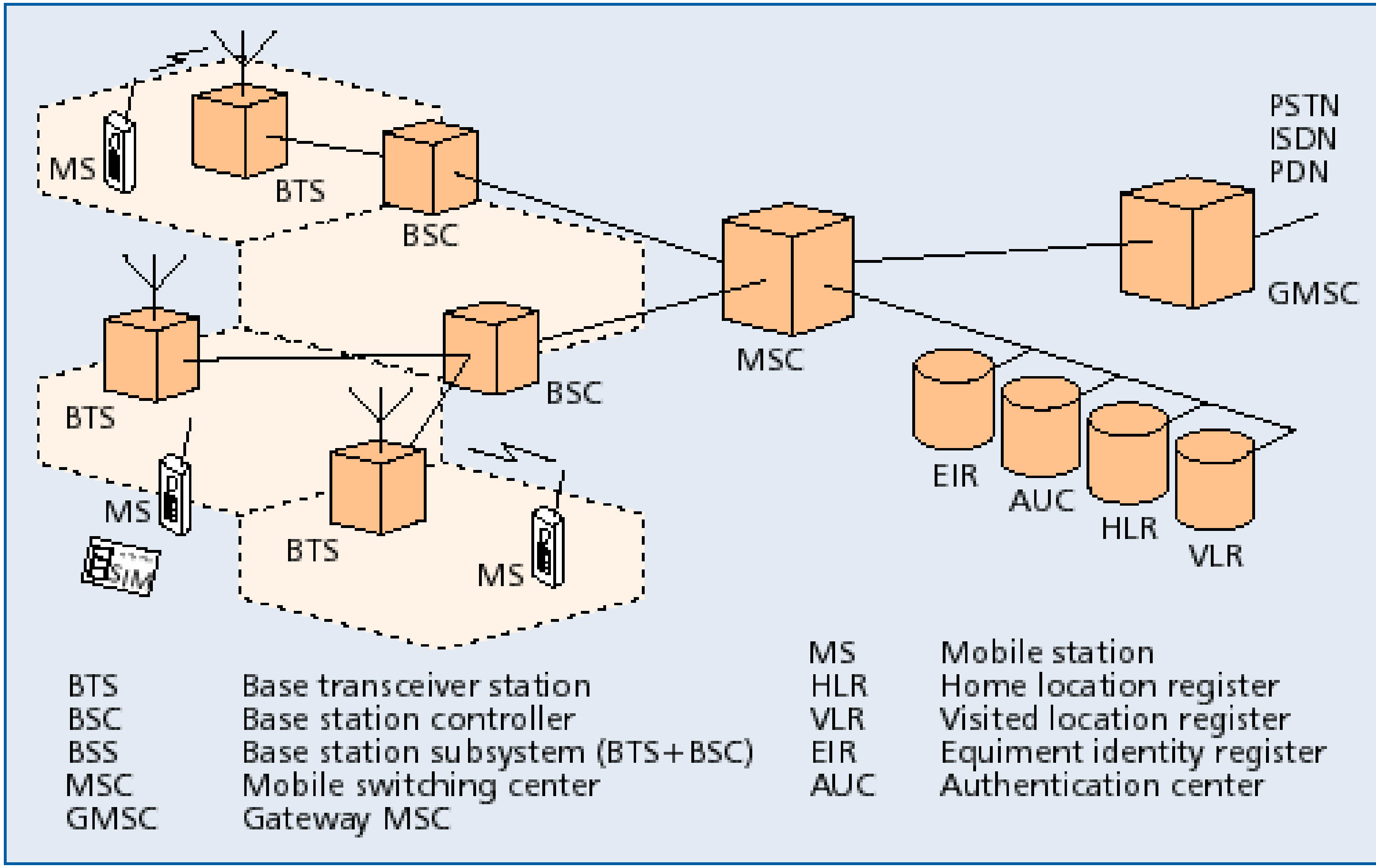
- Mapping in frequency
  - 124 channels, 200KHz spacing
- Mapping in time
  - TDMA Frame, Multi Frame, Super Frame, Channel
  - Two kinds of multiframe:
    - 26-frame multiframe; usage -Speech and Data
    - 51-frame multiframe; usage -Signalling


1 Hyper frame = 2048 Super frames =2715648 TDMA frames (3h 28 min 53 sec 760 ms)
0
1
2
3
2045
2046
2047
1 Super frame = 1326 TDMA frames (6.12s)
= 51(26 frames) Multi frame
0
1
2
3
50
1 Super frame = 1326 TDMA frames (6.12s)
= 26(51 frames) Multi frame
0
1
2
3
23
24
25
1(26 frames) Multi frame = 26 TDMA frames (120 ms)
T0
T1
T2
T12
(SACCH)
T23
I
1(51 frames) Multi frame = 51 TDMA frames (3060/13 ms)
0
1
2
3
49
50
1 TDMA frame
= 8 time slots (120/26 or 4.615ms)
0
1
2
3
4
5
6
7
1 time slot = 156.25 bit duration (15/26 or 0.577 ms)
(1 bit duration = 48/13 or 3.69μs)

Outline

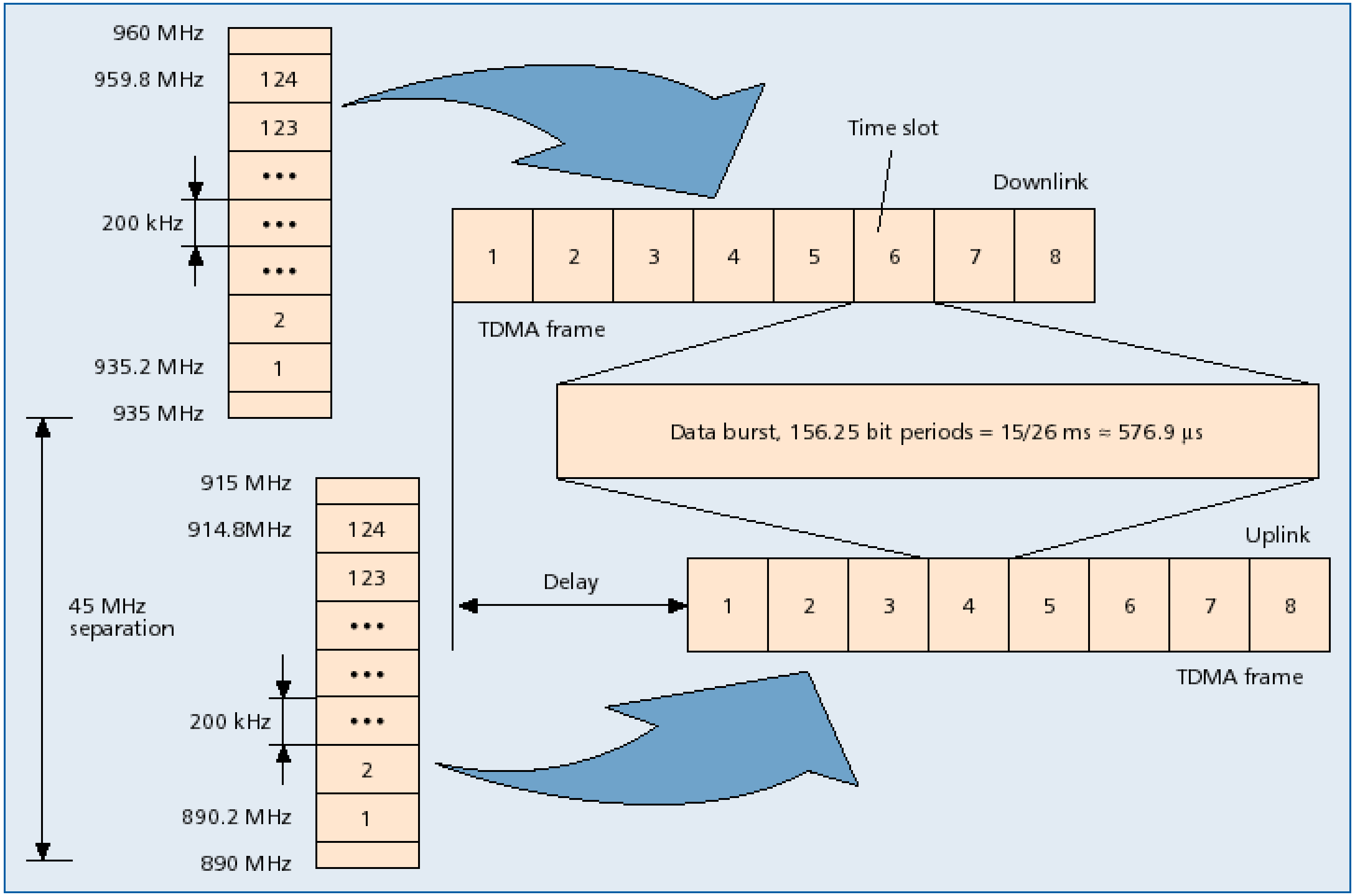
- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- TCP over wireless
- GSM air interface
- **GPRS network architecture**
- Wireless application protocol
- Mobile agents
- Mobile ad hoc networks

GSM architecture

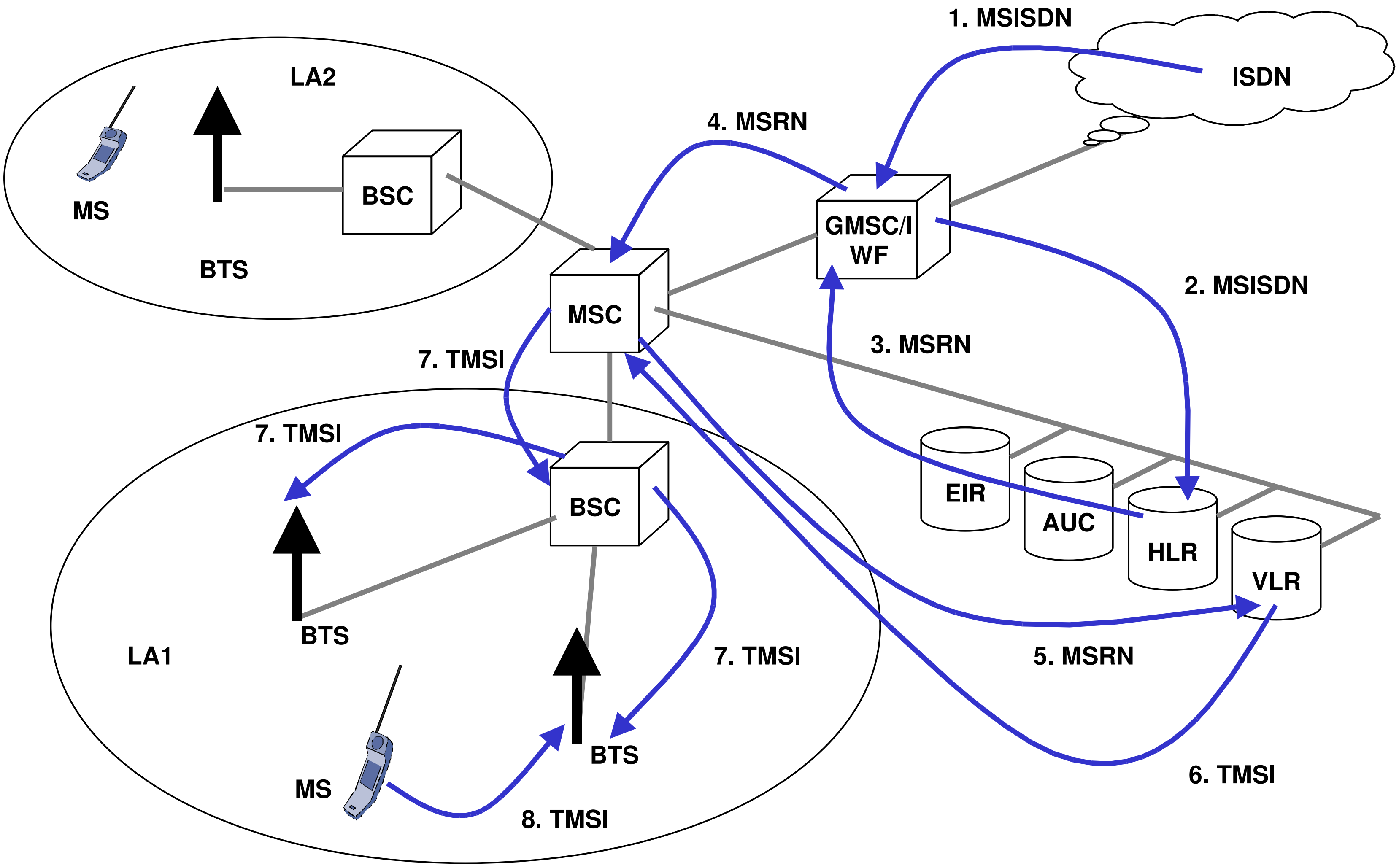


Source: Bettstetter et. al.

GSM multiple access



GSM call routing



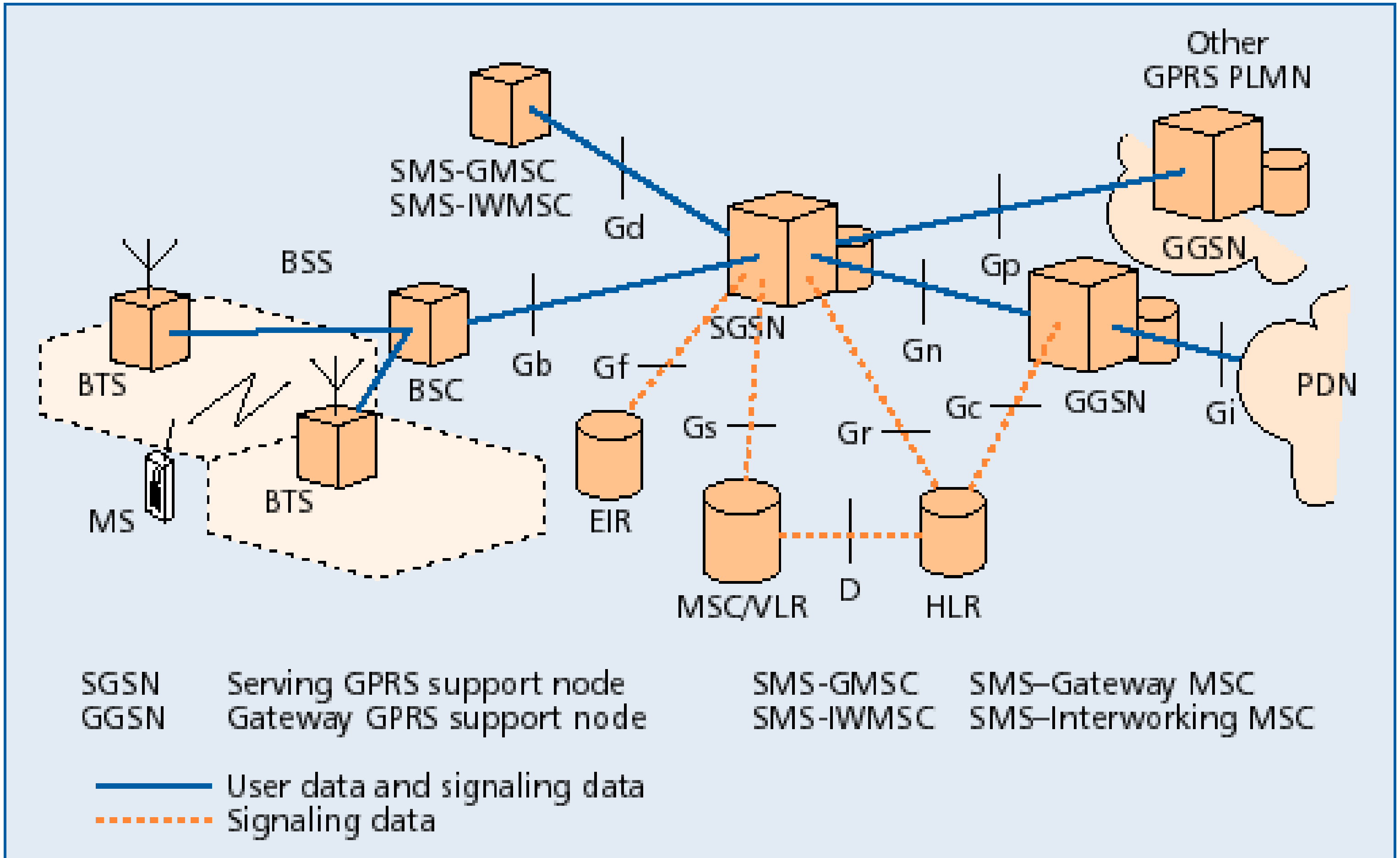
Options for data transfer

- Two enhancements to GSM for data
  - HSCSD - High Speed Circuit Switched Data
  - GPRS - General Packet Radio Service
- Both have capacity to use new coding schemes and to make multislot allocation
- GPRS, being a packet switched service, is known to be more efficient and flexible for data transfer purposes
- It delivers circuit and packet-switched services in one mobile radio network

GPRS features

- Radio resources are allocated for only one or a few packets at a time, so GPRS enables
  - many users to share radio resources, and allow efficient transport of packets
  - fast setup/access times
  - connectivity to external packet data n/w
  - volume-based charging
- GPRS also carries SMS in data channels rather than signaling channels as in GSM

GPRS Architecture



GPRS Architecture

- Requires addition of a new class of nodes called GSNs (GPRS Support Nodes)
  – SGSN: Serving GPRS Support Node,
  – GGSN: Gateway GPRS Support Node
- BSC requires a PCU (Packet Control Unit) and various other elements of the GSM n/w require software upgrades
- All GSNs are connected via an IP-based backbone. Protocol data units (PDUs) are encapsulated and tunneled between GSNs

GGSN

- Serves as the interface to external IP networks which see the GGSN as an IP router serving all IP addresses of the MSs
- GGSN stores current SGSN address and profile of the user in its location register
- It tunnels protocol data packets to and from the SGSN currently serving the MS
- It also performs authentication and charging
- GGSN can also include firewall and packet-filtering mechanisms

SGSN

- Analog of the MSC in GSM
- Routes incoming and outgoing packets addressed to and from any GPRS subscriber located within the geographical area served by the SGSN
- Location Register of the SGSN stores information (e.g. current cell and VLR) and user profiles (e.g. IMSI, addresses) of all GPRS users registered with this SGSN

BSC and others

- BSC must get a Packet Control Unit to
  - set up, supervise and disconnect packet-switched calls
  - also support cell change, radio resource configuration and channel assignment
- MSC/VLR, HLR and SMS Center must be enhanced for interworking with GPRS
- MS must be equipped with the GPRS protocol stack

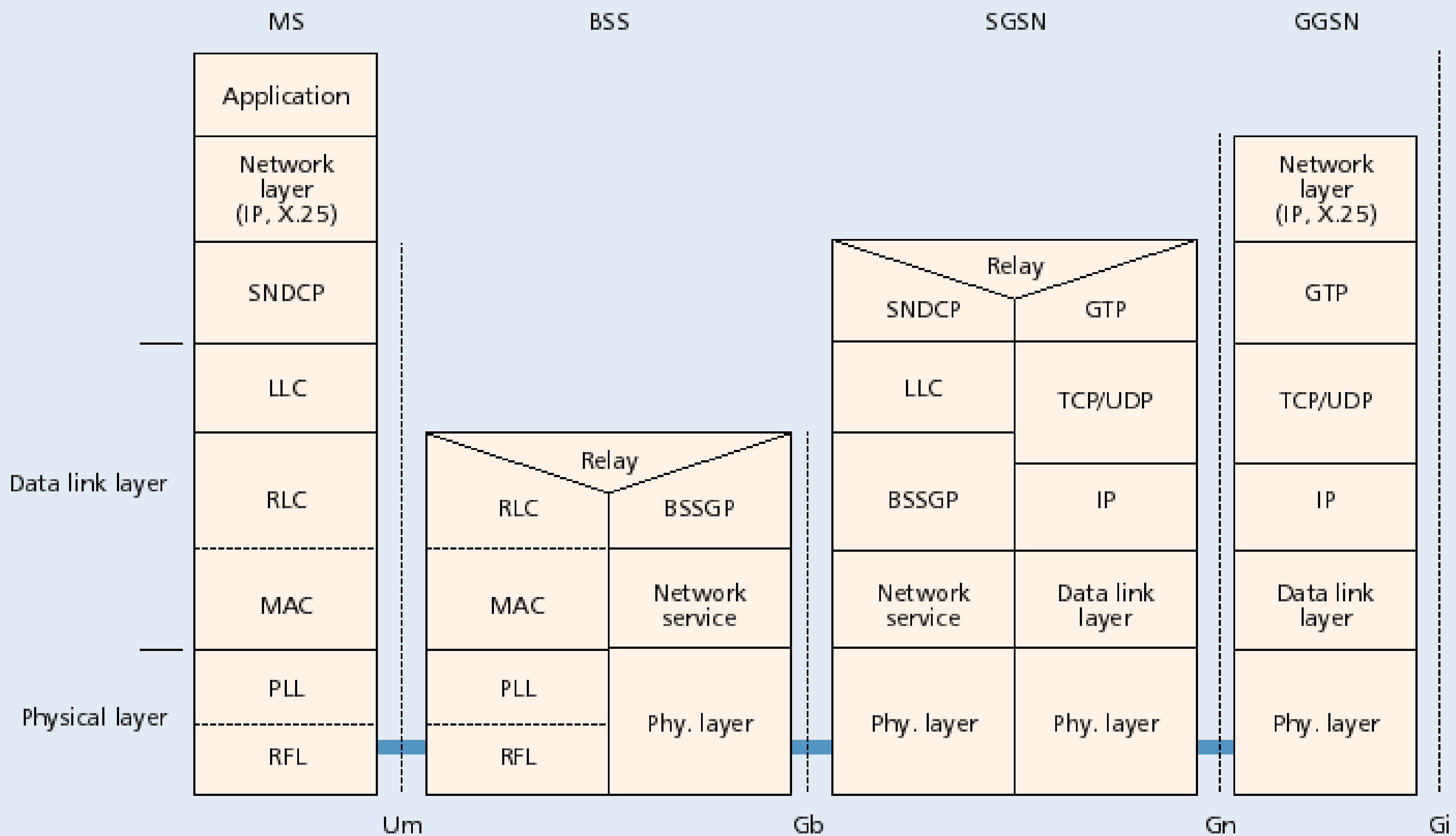
HLR - Home Location Register

- Shared database, with GSM
- Is enhanced with GPRS subscriber data and routing information
- For all users registered with the network, HLR keeps user profile, current SGSN and Packet Data Protocol (PDP) address(es) information
- SGSN exchanges information with HLR e.g., informs HLR of the current location of the MS
- When MS registers with a new SGSN, the HLR sends the user profile to the new SGSN

MSC/VLR-Visitor Location Register

- VLR is responsible for a group of location areas. It stores data of only those users in its area of responsibility
- MSC/VLR can be enhanced with functions and register entries that allow efficient coordination between GPRS and GSM services
  - combined location updates
  - combined attachment procedures

GPRS Transmission Plane



SNDCP	Subnetwork dependent convergence protocol
LLC	Logical link control
RLC	Radio link control
MAC	Medium access control
PLL	Physical link layer
RFL	Physical RF layer
BSSGP	BSS GPRS application protocol
GTP	GPRS tunneling protocol
TCP	Transmission control protocol
UDP	User datagram protocol
IP	Internet protocol

Air Interface U_m

- Is one of the central aspects of GPRS
  - Concerned with communication between MS and BSS at the physical, MAC and RLC layers
  - Physical channel dedicated to packet data traffic is called a packet data channel (PDCH)
- Capacity on Demand:
  - Allocation/Deallocation of PDCH to GPRS traffic is dynamic
  - BSC controls resources in both directions
  - No conflicts on downlink
  - Conflicts in uplink are resolved using slotted ALOHA

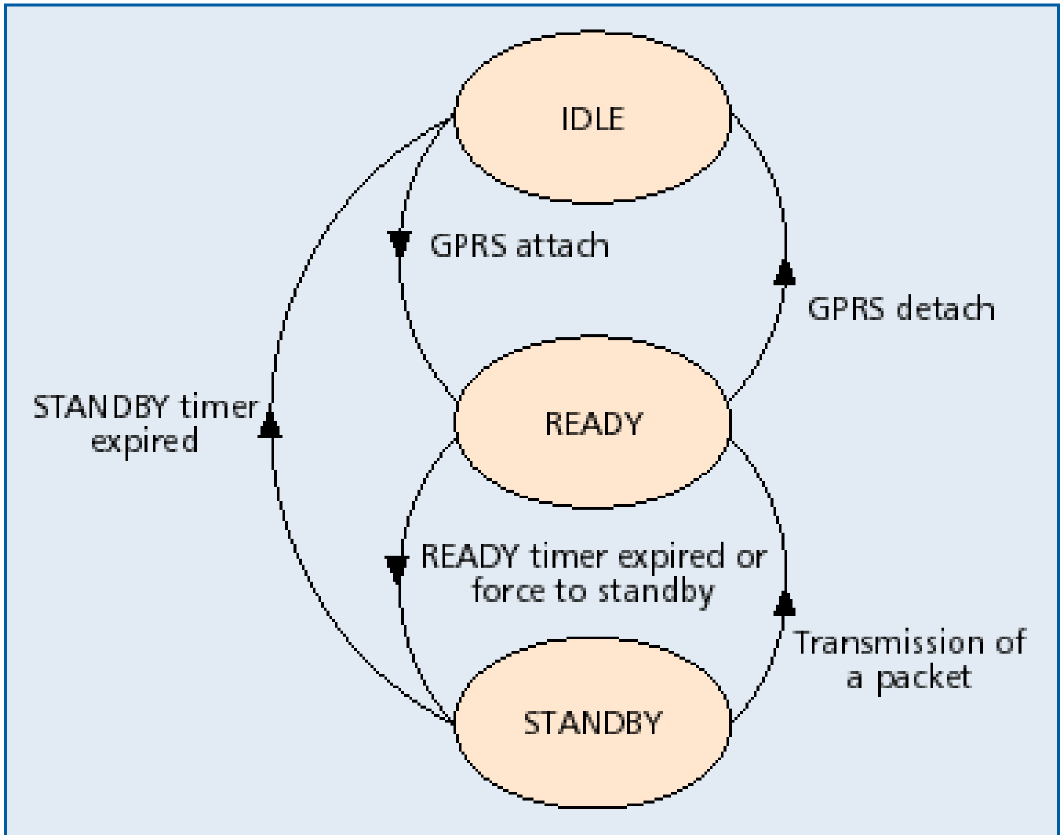
Data transfer between MS and SGSN

- SNDCP transforms IP/X.25 packets into LLC frames, after optional header/data compression, segmentation and encryption
- Maximum LLC frame size is 1600 bytes
- An LLC frame is segmented into RLC data blocks which are coded into radio blocks
- Each radio block comprises four normal bursts (114 bits) in consecutive TDMA frames
- RLC is responsible for transmission of data across air-interface, including error correction
- MAC layer performs medium allocation to requests, including multi-slot allocation
- PHY layer is identical to GSM

Data transfer between GSNs

- Although the GPRS network consists of several different nodes, it represents only one IP hop
- GTP enables tunneling of PDUs between GSNs, by adding routing information
- Below GTP, TCP/IP and IP are used as the GPRS backbone protocols

MS - state model

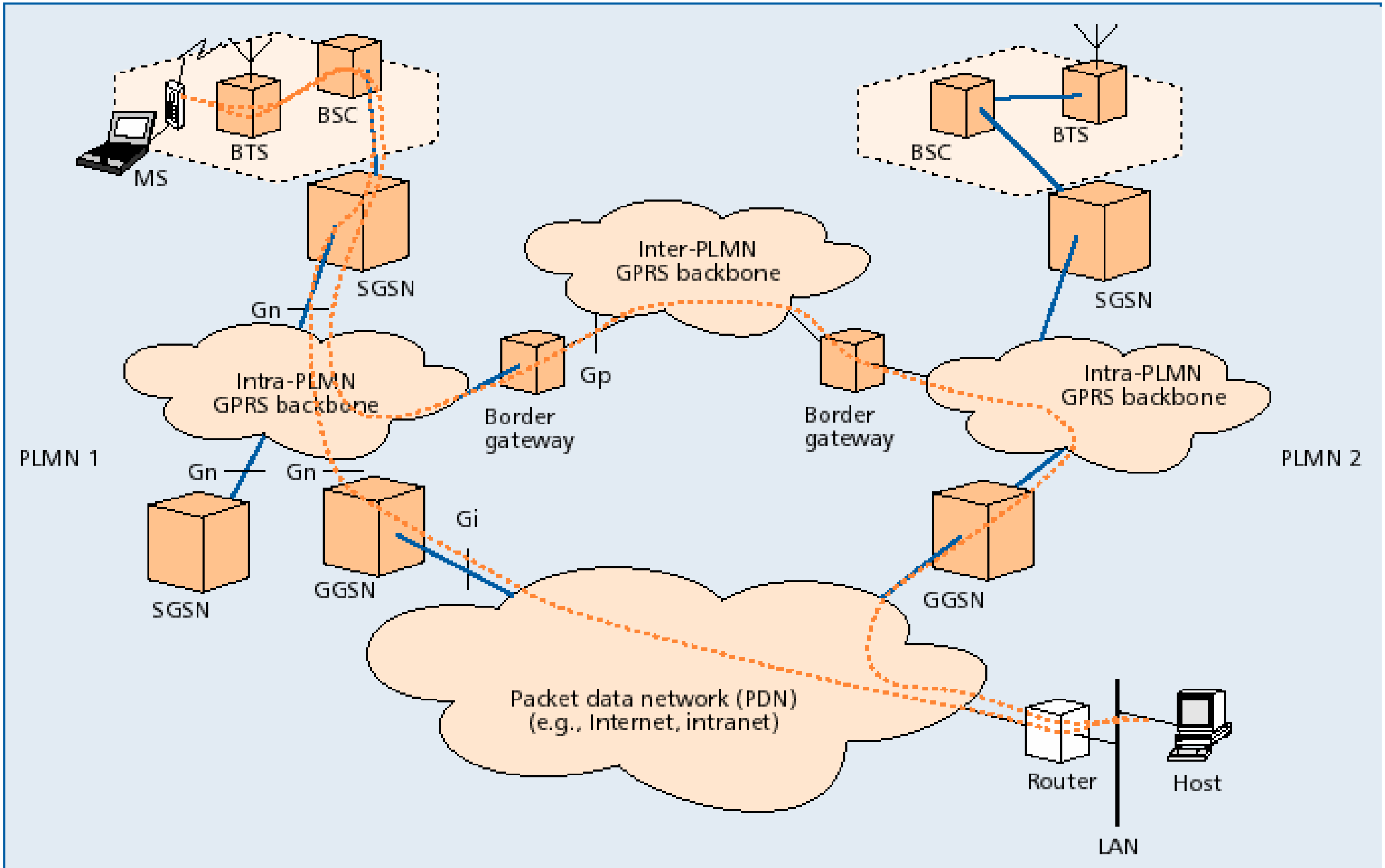


- In Idle State MS is not reachable
- With GPRS Attach MS moves into ready state
- With Detach, it returns to Idle state: all PDP contexts are deleted
- Standby state is reached when MS does not send data for a long period and ready timer expires

GPRS – PDP context

- MS gets a packet temporary mobile subscriber identity (p-TMSI) during Attach
- MS requests for one or more addresses used in the packet data network, e.g. IP address
- GGSN creates a PDP context for each session
  - PDP type (IPV4), PDP address (IP) of MS,
  - requested quality of service (QoS) and address of GGSN
- PDP context is stored in MS, SGSN and GGSN
- Mapping between the two addresses, enables GGSN to transfer packets between MS and the PDN

GPRS - Routing



GPRS - Routing

- MS from PLMN-2 is visiting PLMN-1.
- IP address prefix of MS is the same as GGSN-2
- Incoming packets to MS are routed to GGSN-2
- GGSN-2 queries HLR and finds that MS is currently in PLMN-1
- It encapsulates the IP packets and tunnels them through the GPRS backbone to the appropriate SGSN of PLMN-1
- SGSN decapsulates and delivers to the MS

GPRS Summary

- Enables many users to share radio resources by dynamic, on-demand, multi-slot allocation
- Provides connectivity to external packet data networks
- Modification to the GSM air-interface
- Addition of new GPRS Support Nodes
- Assignment of PDP context to MS
- Enables volume-based charging as well as duration based charging

Outline

- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- TCP over wireless
- GSM air interface
- GPRS network architecture
- **Wireless application protocol**
- Mobile agents
- Mobile ad hoc networks

Variability of the mobile environment

Mobility
- stationary
- nomadic (pedestrian speed)
- mobile (vehicular speed)
- roaming (mobile across networks)

Connectivity
- connected
- semi-connected (asymmetric)
- disconnected

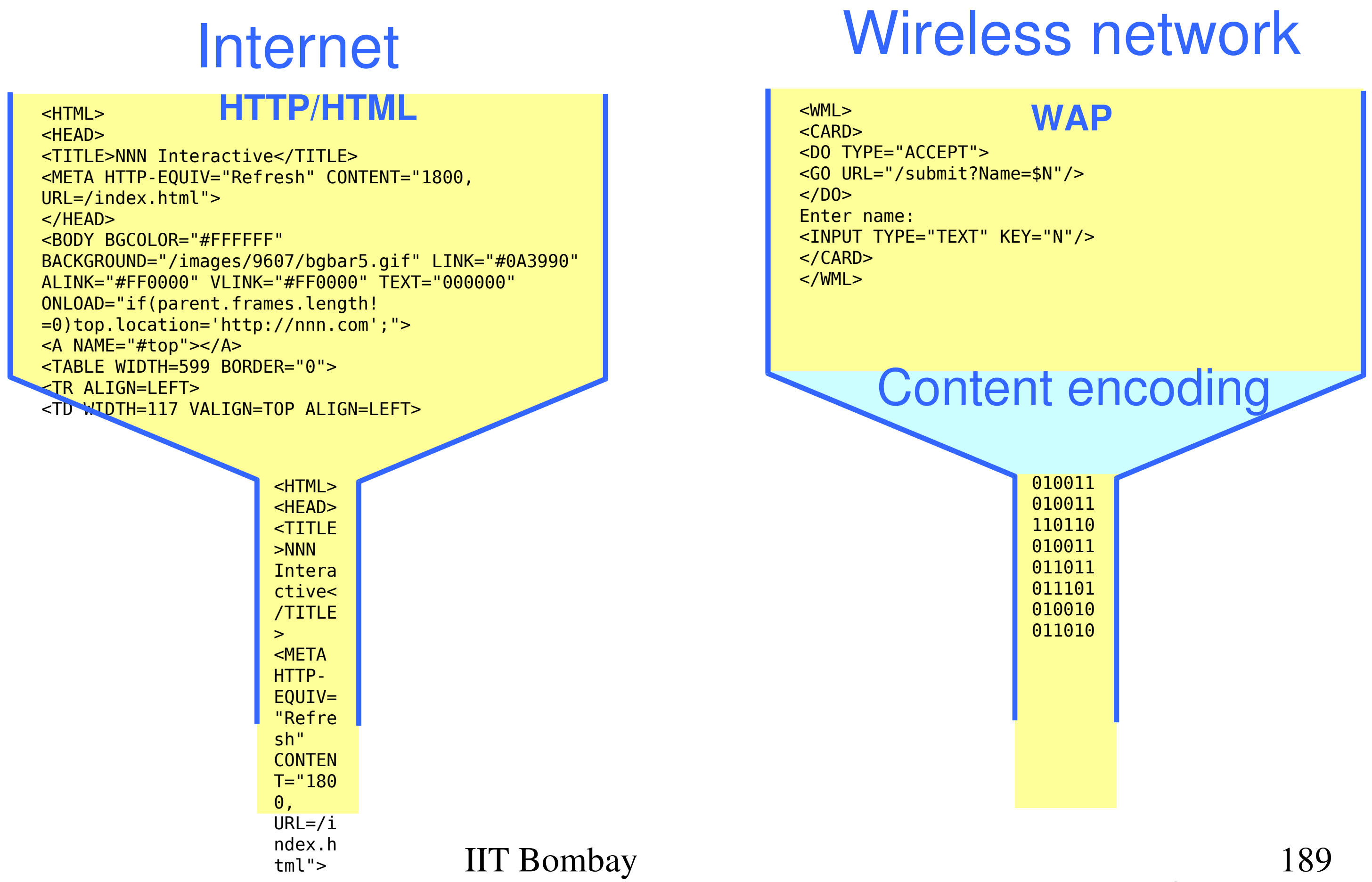
Mobile Device Capability
- form factor
- GUI
- multimedia
- real-time multimedia

Wireless Application Protocol (WAP)

- HTTP/HTML have not been designed for mobile devices and applications
- WAP empowers mobile users with wireless devices to easily access and interact with information and services.
- A “standard” created by wireless and Internet companies to enable Internet access from a cellular phone

Why is HTTP/HTML not enough?

Big pipe - small pipe syndrome



Source: WAP Forum

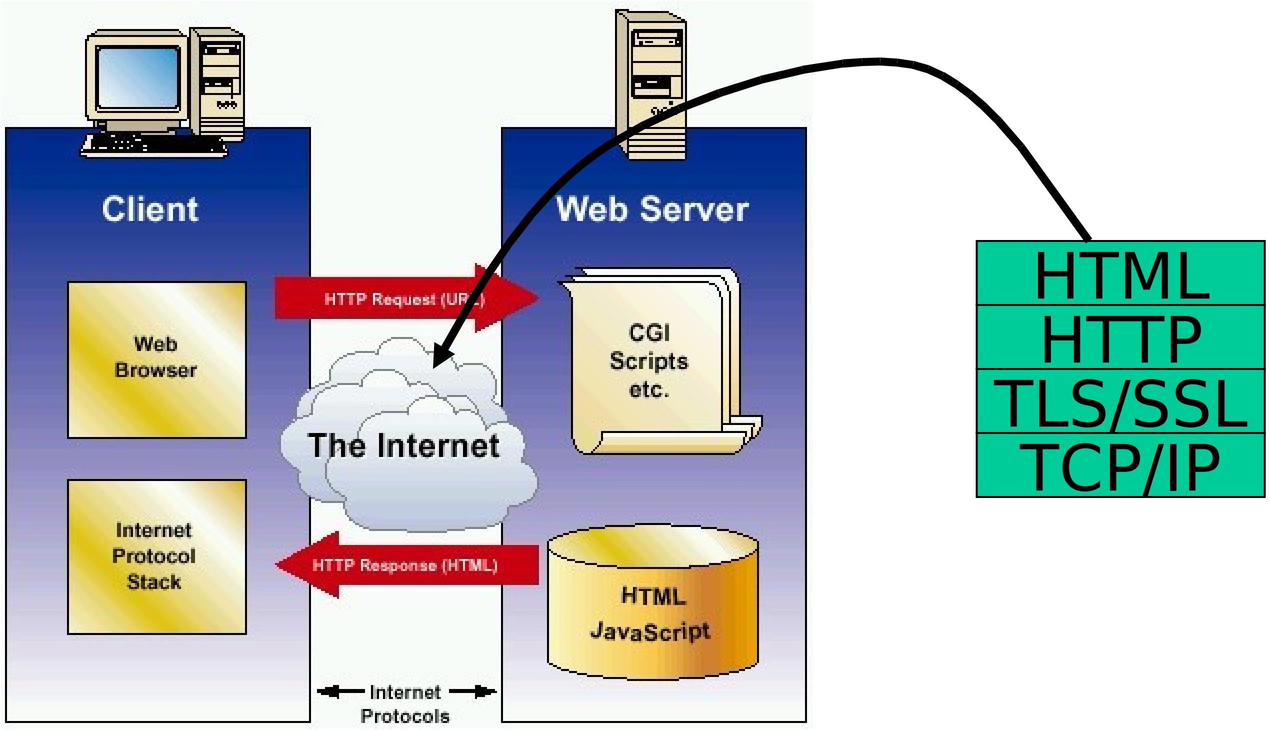
WHY WAP?

- Wireless networks and phones
  - have specific needs and requirements
  - not addressed by existing Internet technologies
- WAP
  - Enables any data transport
    - TCP/IP, UDP/IP, GUTS (IS-135/6), SMS, or USSD.
  - Optimizes the content and air-link protocols
  - Utilizes plain Web HTTP 1.1 servers
    - utilizes standard Internet markup language technology (XML)
    - all WML content is accessed via HTTP 1.1 requests
  - WML UI components map well onto existing mobile phone UI
    - no re-education of the end-users
    - leveraging market penetration of mobile devices

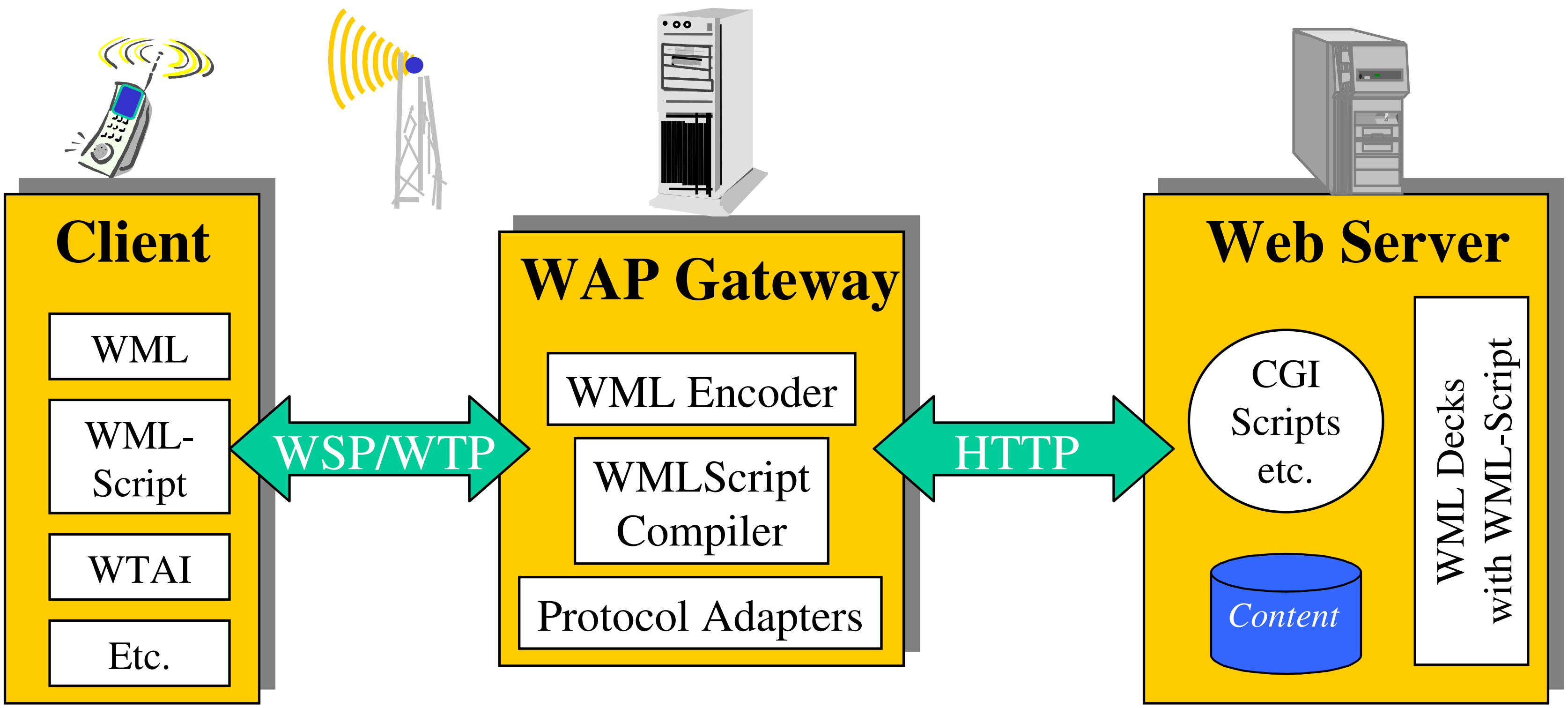
WAP: main features

- Browser
  - "Micro browser", similar to existing web browsers
- Markup language
  - Similar to HTML, adapted to mobile devices
- Script language
  - Similar to Javascript, adapted to mobile devices
- Gateway
  - Transition from wireless to wired world
- Server
  - "Wap/Origin server", similar to existing web servers
- Protocol layers
  - Transport layer, security layer, session layer etc.
- Telephony application interface
  - Access to telephony functions

Internet model

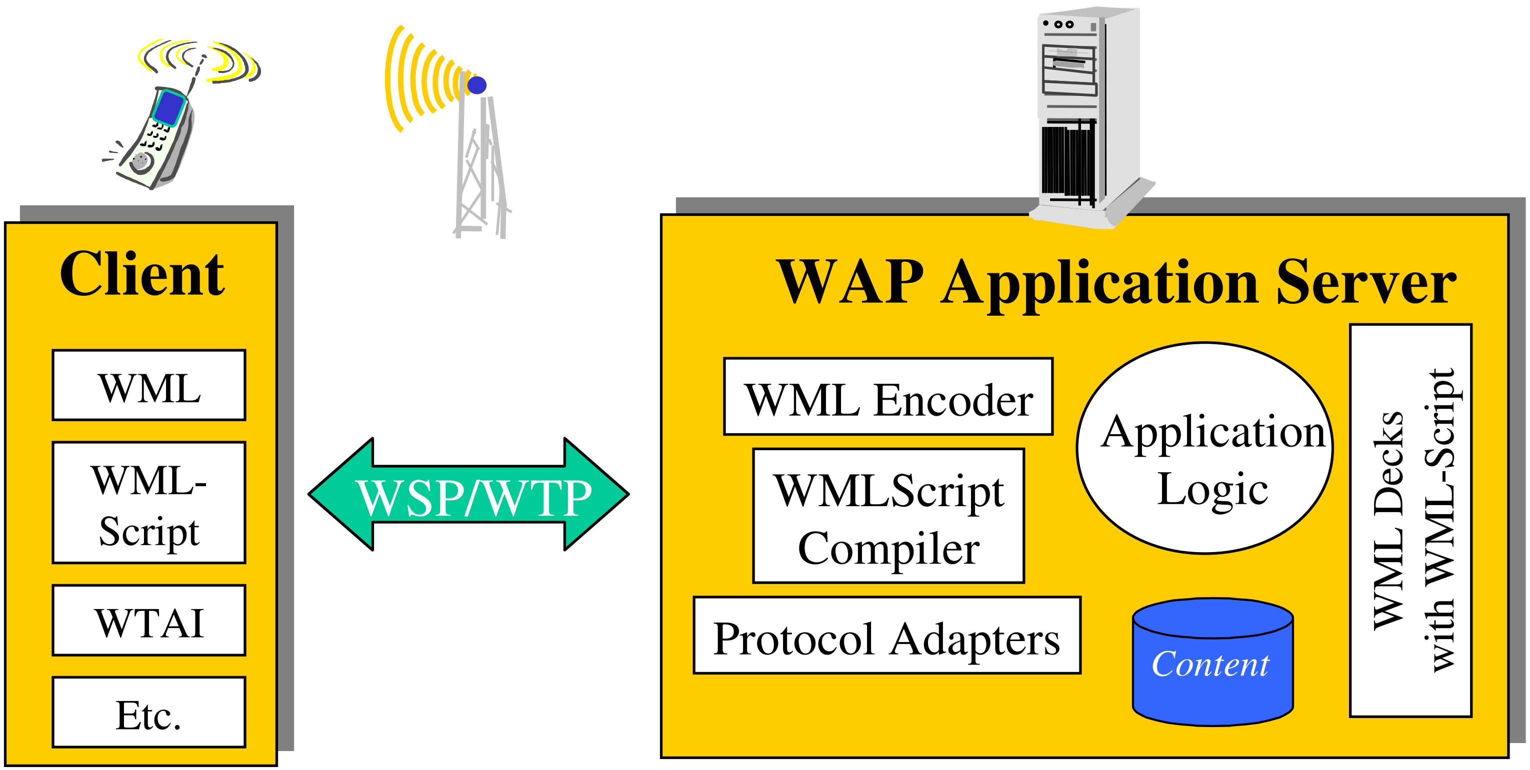


WAP architecture



Source: WAP Forum

WAP application server



Source: WAP Forum

WAP specifies

- Wireless Application Environment
  - WML Microbrowser
  - WMLScript Virtual Machine
  - WMLScript Standard Library
  - Wireless Telephony Application Interface (WTAI)
  - WAP content types
- Wireless Protocol Stack
  - Wireless Session Protocol (WSP)
  - Wireless Transport Layer Security (WTLS)
  - Wireless Transaction Protocol (WTP)
  - Wireless Datagram Protocol (WDP)
  - Wireless network interface definitions

WAP stack

- WAE (Wireless Application Environment):
  - Architecture: application model, browser, gateway, server
  - WML: XML-Syntax, based on card stacks, variables, ...
  - WTA: telephone services, such as call control, phone book etc.
- WSP (Wireless Session Protocol):
  - Provides HTTP 1.1 functionality
  - Supports session management, security, etc.

WAP stack (contd.)

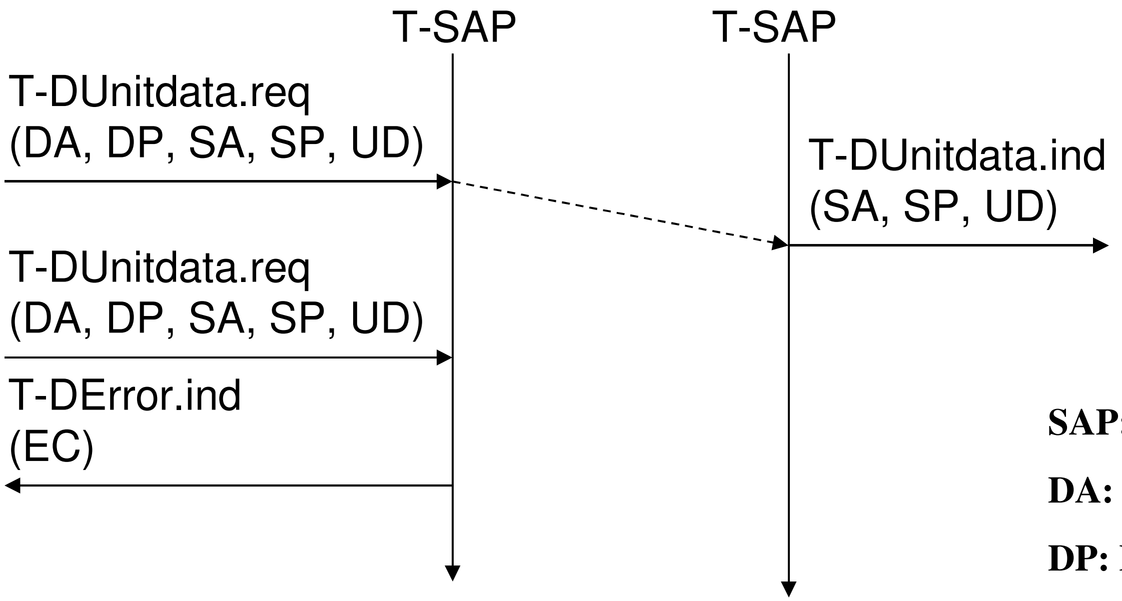
- WTP (Wireless Transaction Protocol):
  - Provides reliable message transfer mechanisms
  - Based on ideas from TCP/RPC
- WTLS (Wireless Transport Layer Security):
  - Provides data integrity, privacy, authentication functions
  - Based on ideas from TLS/SSL
- WDP (Wireless Datagram Protocol):
  - Provides transport layer functions
  - Based on ideas from UDP

Content encoding, optimized for low-bandwidth channels, simple devices

WDP: Wireless Datagram Protocol

- Goals
  - create a worldwide interoperable transport system by adapting WDP to the different underlying technologies
  - transmission services, such as SMS in GSM might change, new services can replace the old ones
- WDP
  - Transport layer protocol within the WAP architecture
  - uses the Service Primitive
    - T-UnitData.req .ind
  - uses transport mechanisms of different bearer technologies
  - offers a common interface for higher layer protocols
  - allows for transparent communication despite different technologies
  - addressing uses port numbers
  - WDP over IP is UDP/IP

WDP: service primitives



SAP: Service Access Point

DA: Destination Address

DP: Destination Port

SA: Source Address

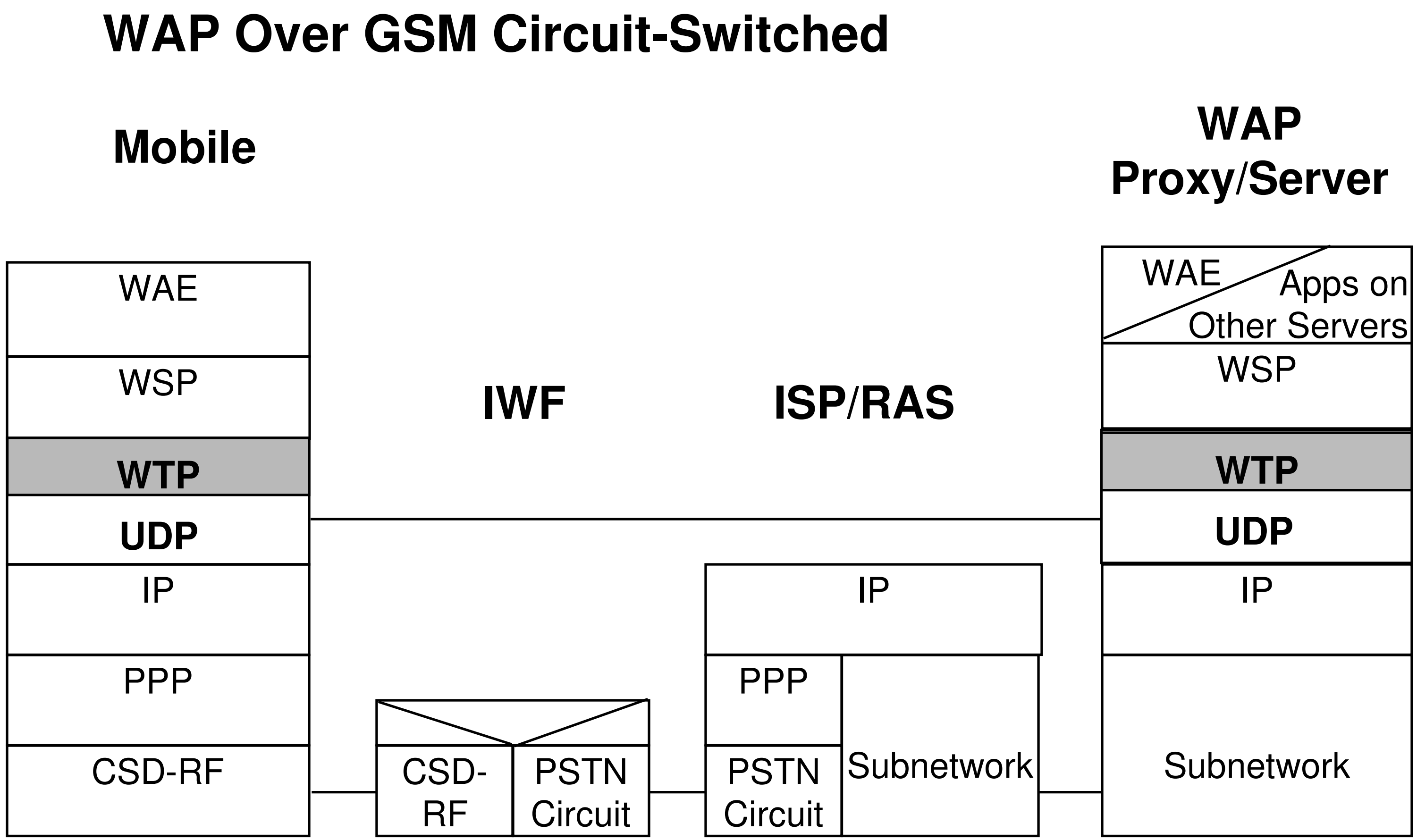
SP: Source Port

UD: User Data

EC: Error Code

Source: Schiller

Service, Protocol, Bearer: Example

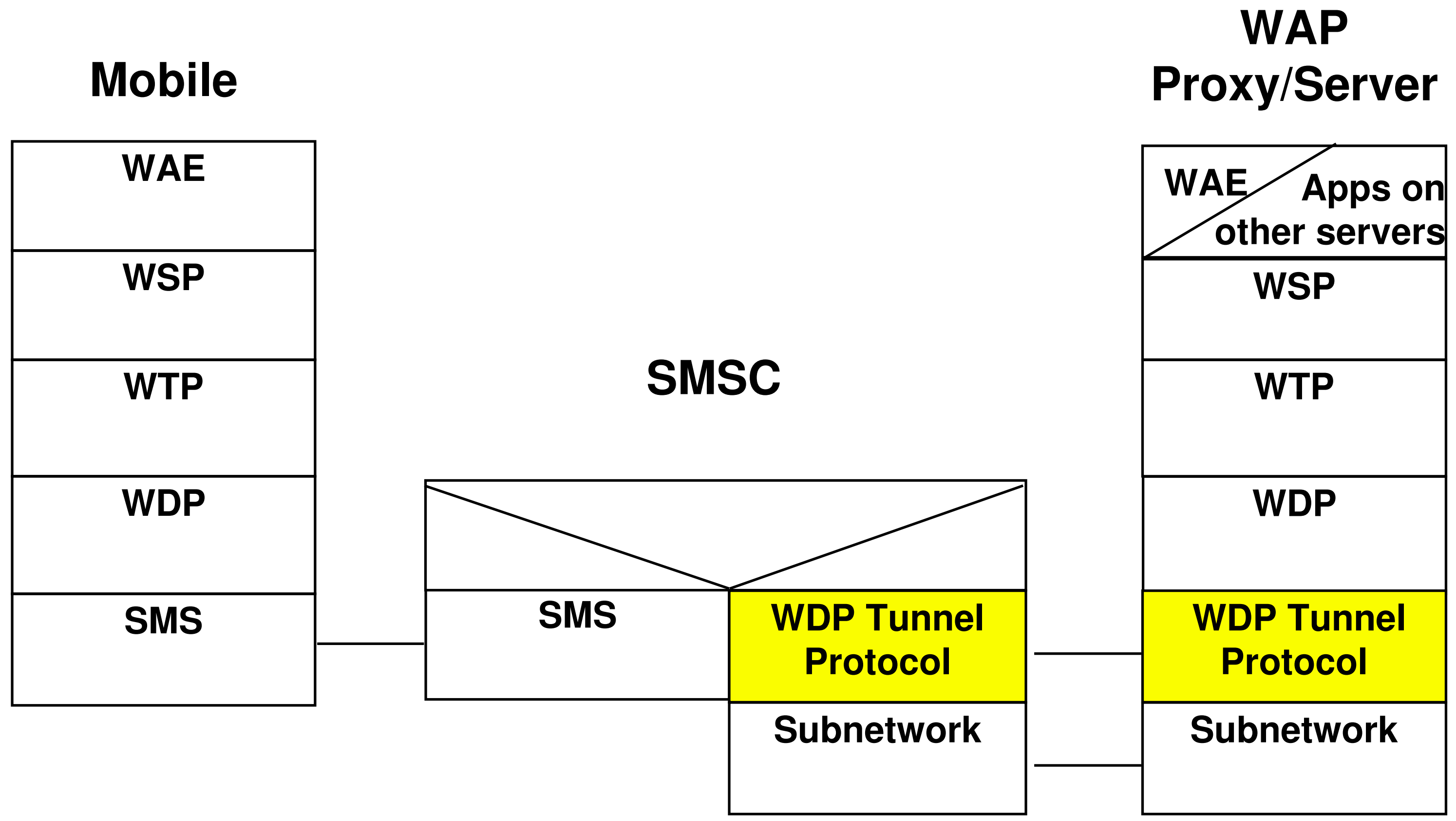


RAS - Remote Access Server
IWF - InterWorking Function

Source: WAP Forum

Service, Protocol, Bearer: Example

WAP Over GSM Short Message Service

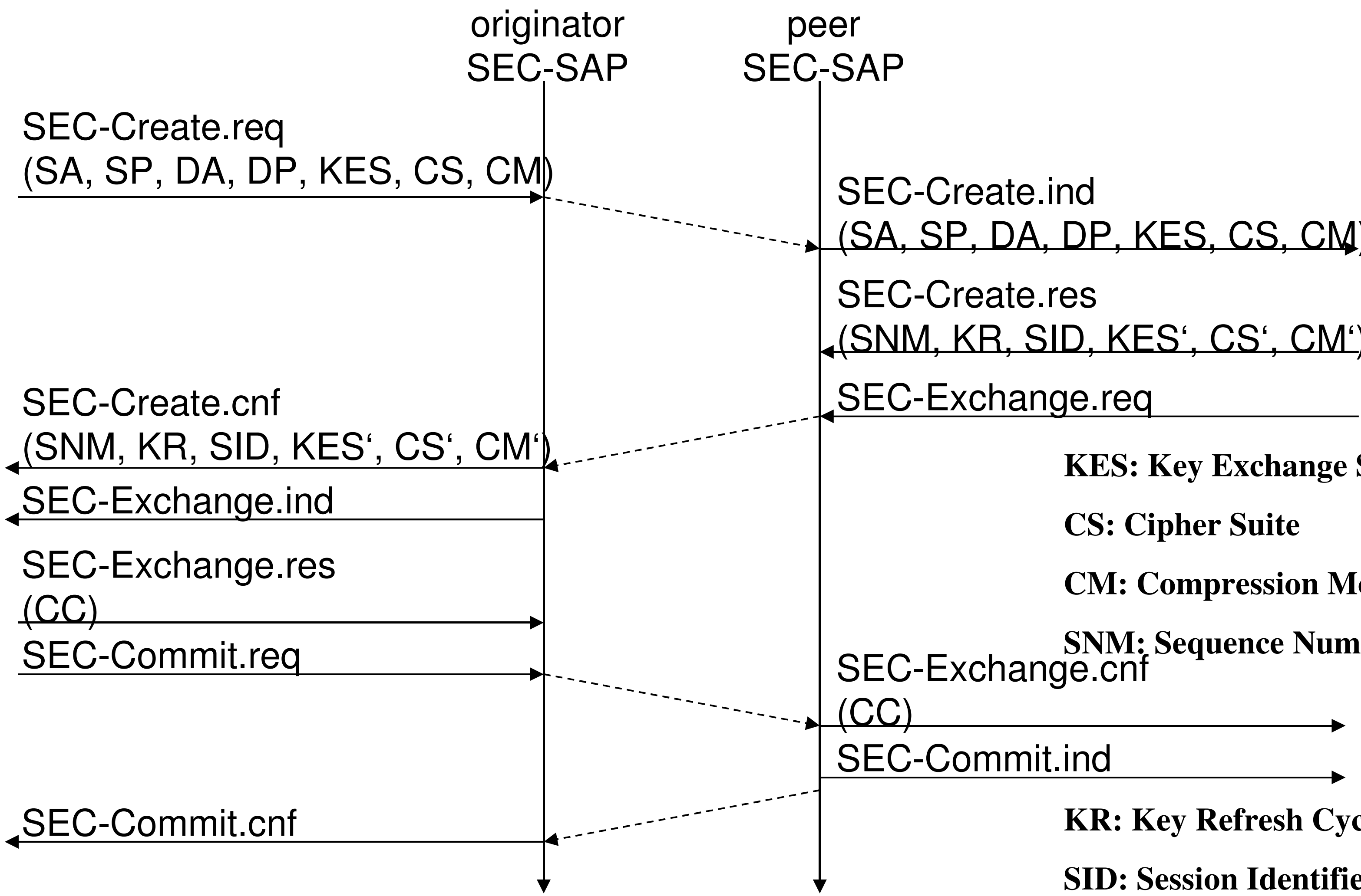


Source: WAP Forum

WTLS:Wireless Transport Layer Security

- Goals
  - Provide mechanisms for secure transfer of content, for applications needing privacy, identification, message integrity and non-repudiation
- WTLS
  - is based on the TLS/SSL (Transport Layer Security) protocol
  - optimized for low-bandwidth communication channels
  - provides
    - privacy (encryption)
    - data integrity (MACs)
    - authentication (public-key and symmetric)
  - Employs special adapted mechanisms for wireless usage
    - Long lived secure sessions
    - Optimised handshake procedures
    - Provides simple data reliability for operation over datagram bearers

WTLS: secure session, full handshake



KES: Key Exchange Suite

CS: Cipher Suite

CM: Compression Mode

SNM: Sequence Number Mode

KR: Key Refresh Cycle

SID: Session Identifier

CC: Client Certificate

Source: Schiller

WTP: Wireless Transaction Protocol

- Goals
  - different transaction services that enable applications to select reliability, efficiency levels
  - low memory requirements, suited to simple devices (< 10kbyte)
  - efficiency for wireless transmission
- WTP
  - supports peer-to-peer, client/server and multicast applications
  - efficient for wireless transmission
  - support for different communication scenarios

WTP transactions

- class 0: unreliable message transfer
  - unconfirmed Invoke message with no Result message
  - a datagram that can be sent within the context of an existing Session
- class 1: reliable message transfer without result message
  - confirmed Invoke message with no Result message
  - used for data push, where no response from the destination is expected
- class 2: reliable message transfer with exactly one reliable result message
  - confirmed Invoke message with one confirmed Result message
  - a single request produces a single reply

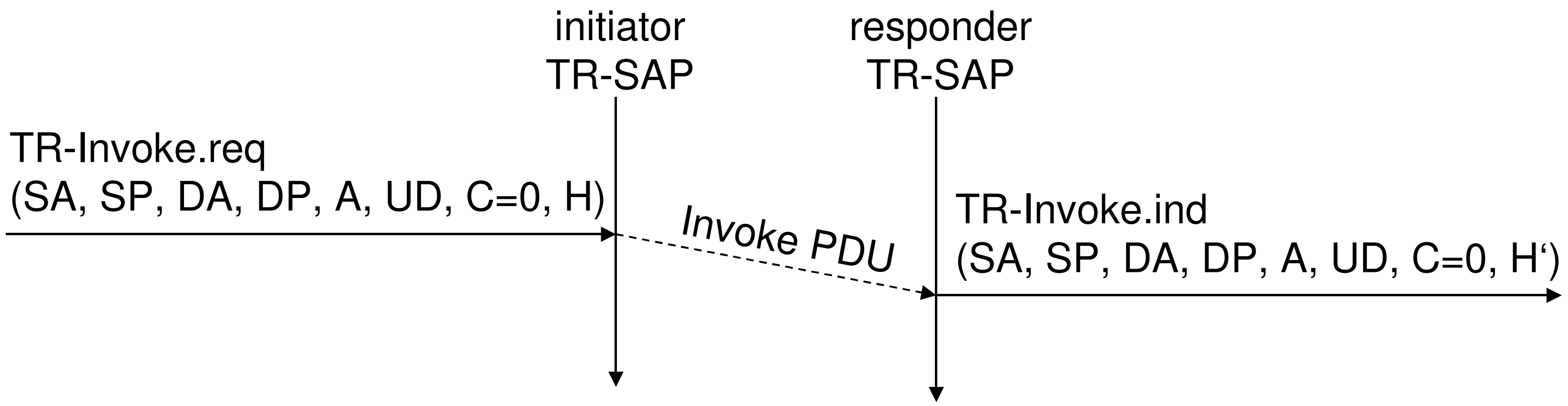
WTP: services and protocols

- WTP (Transaction)
  - provides reliable data transfer based on request/reply paradigm
    - no explicit connection setup or tear down
    - optimized setup (data carried in first packet of protocol exchange)
    - seeks to reduce 3-way handshake on initial request
  - supports
    - header compression
    - segmentation /re-assembly
    - retransmission of lost packets
    - selective-retransmission
    - port number addressing (UDP ports numbers)
    - flow control

WTP services

- message oriented (not stream)
- supports an Abort function for outstanding requests
- supports concatenation of PDUs
- supports two acknowledgement options
  - User acknowledgement
  - acks may be forced from the WTP user (upper layer)
  - Stack acknowledgement: default

WTP Class 0 Transaction



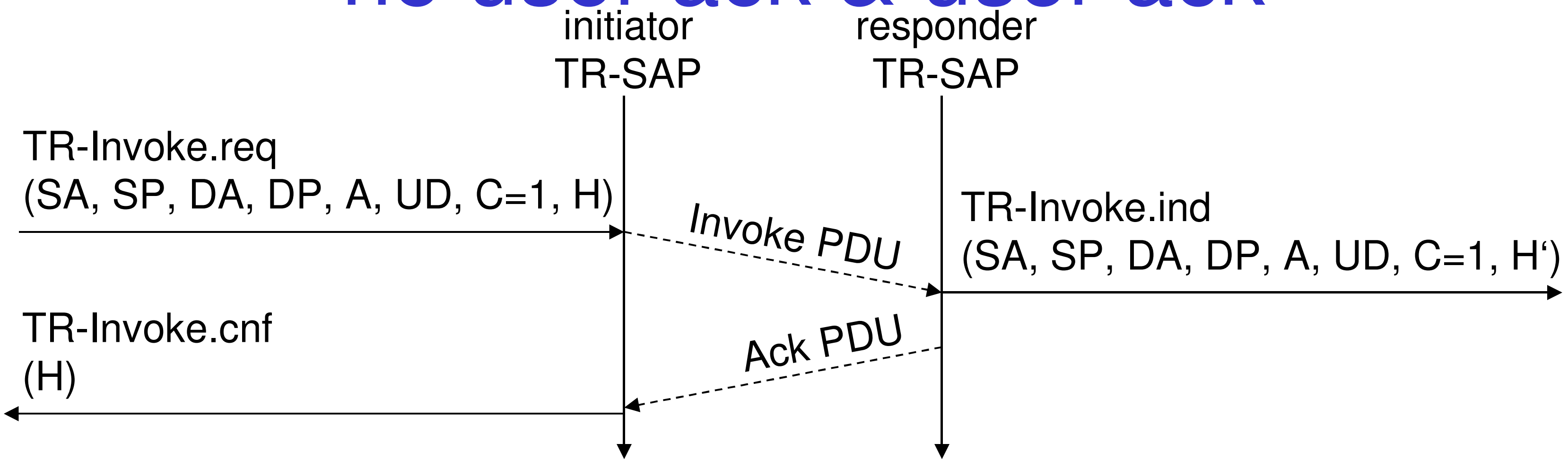
A: Acknowledgement Type (WTP/User)

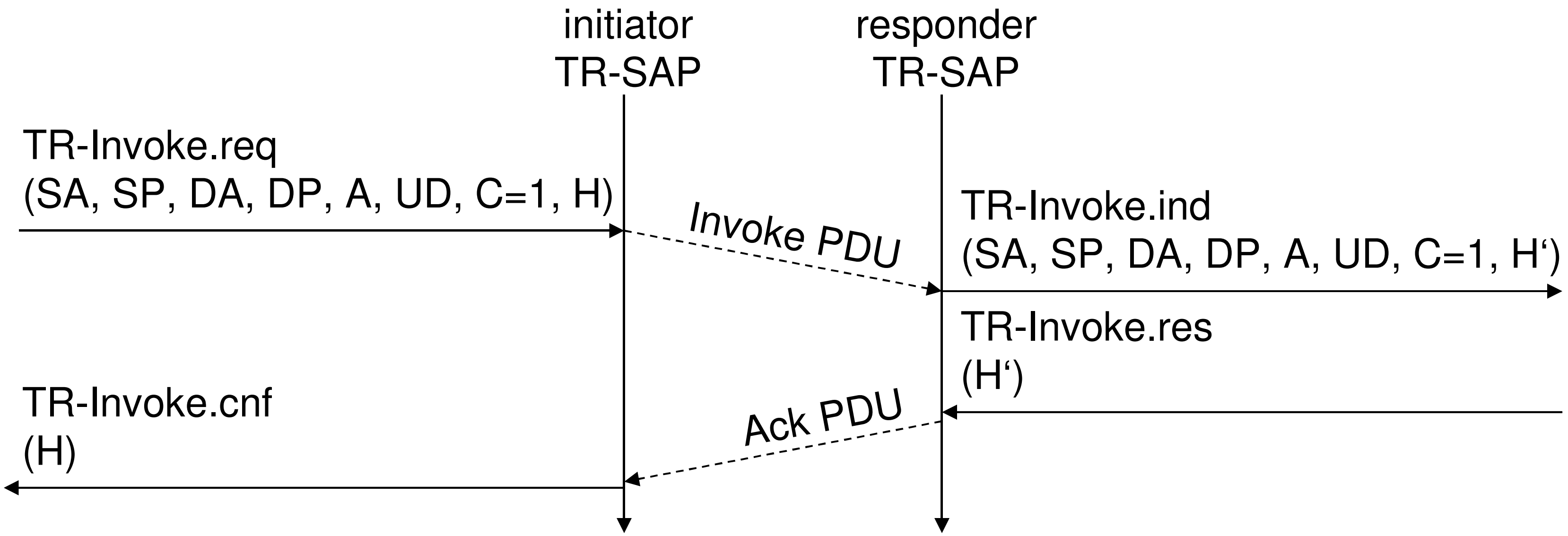
C: Class (0,1,2)

H: Handle (socket alias)

Source: Schiller

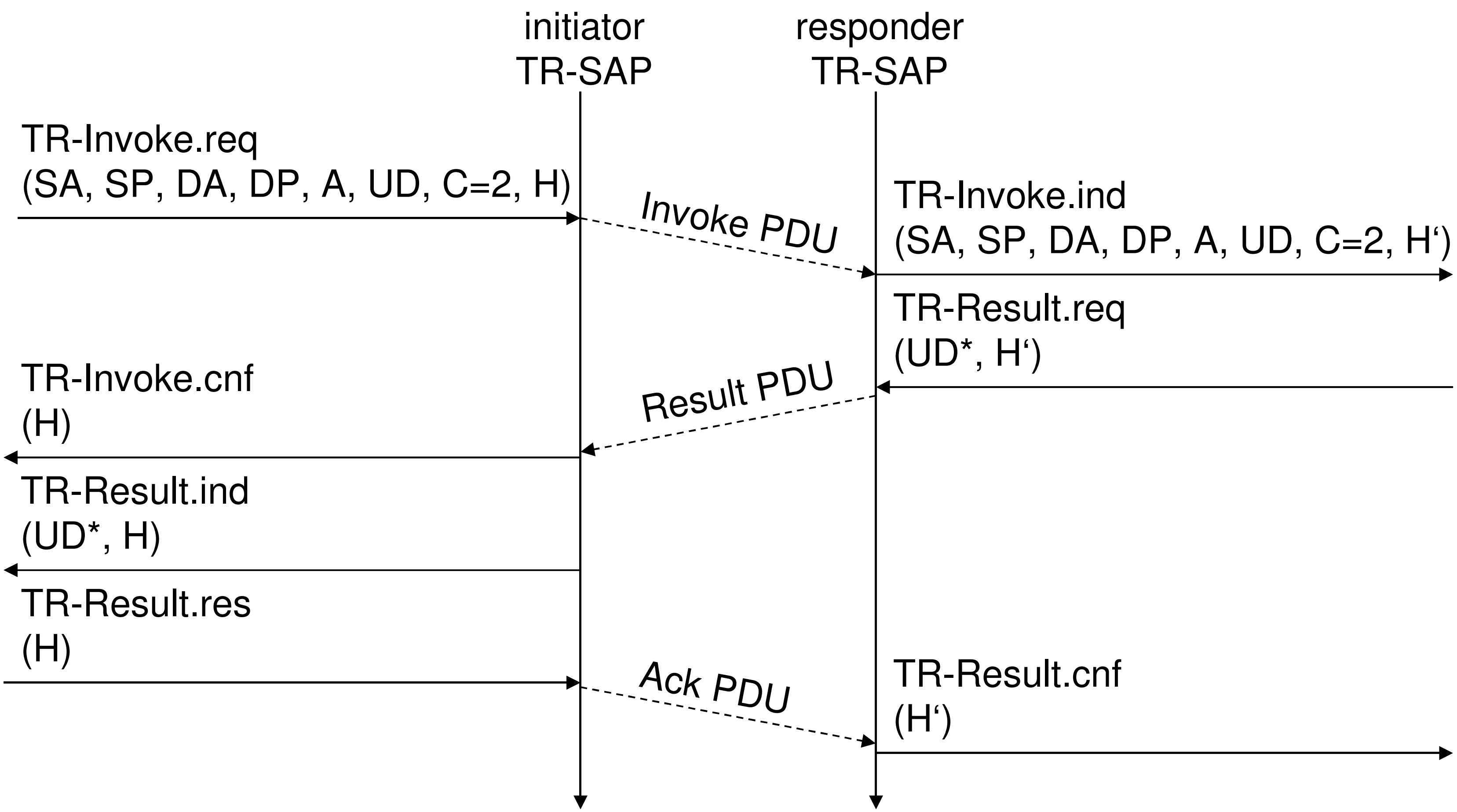
WTP Class 1 Transaction, no user ack & user ack





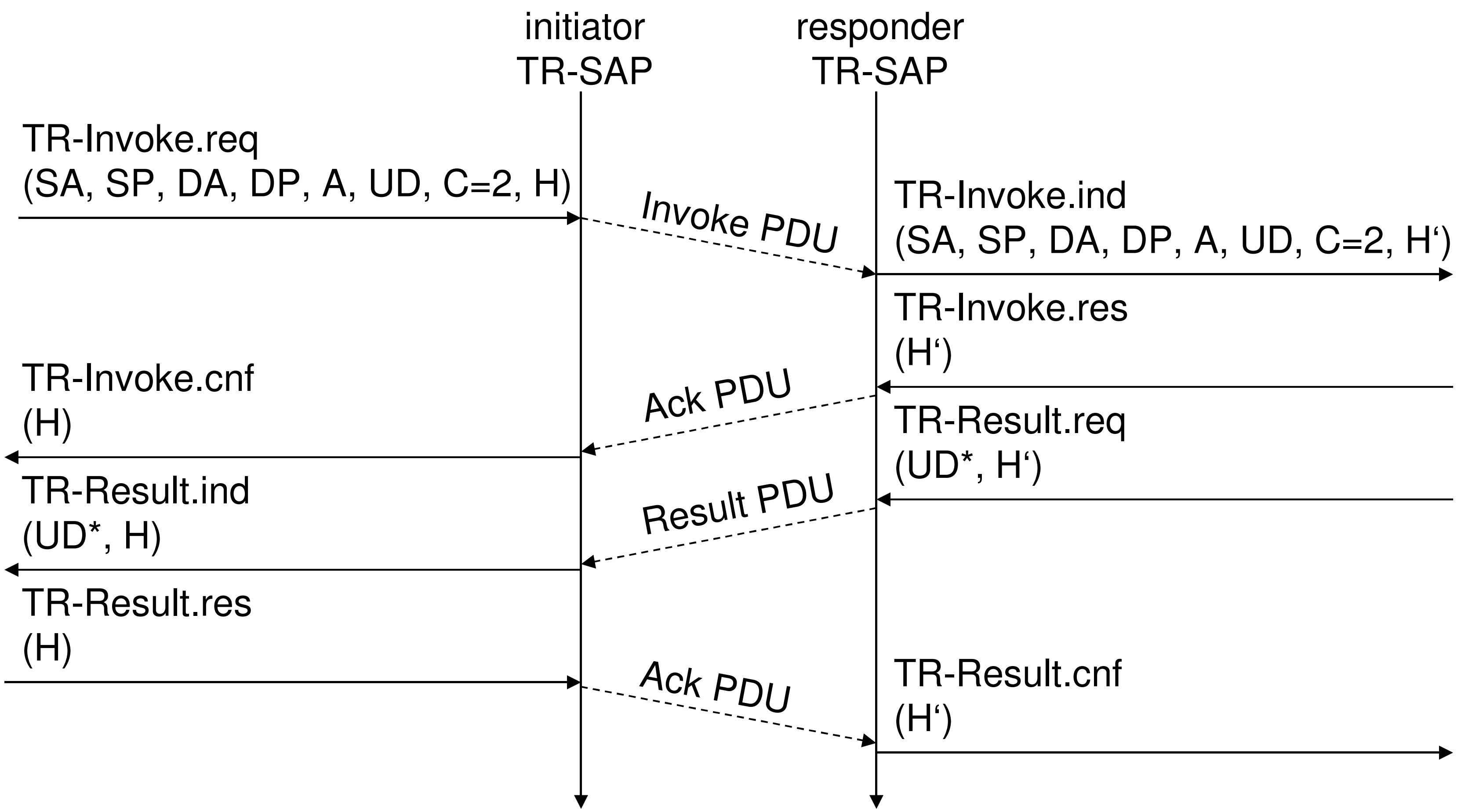
Source: Schiller

WTP Class 2 Transaction, no user ack, no hold on



Source: Schiller

WTP Class 2 Transaction, user ack



Source: Schiller

WSP - Wireless Session Protocol

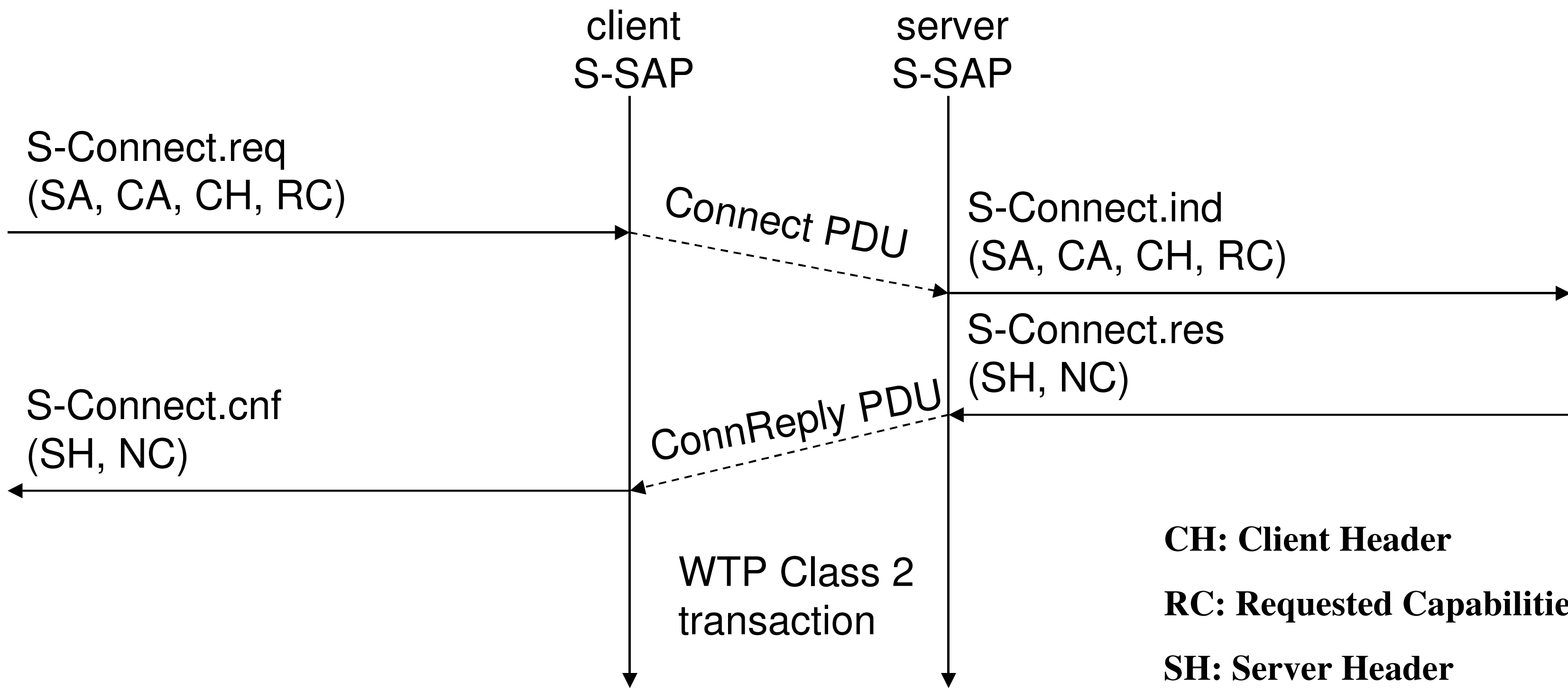
- Goals
  - HTTP 1.1 functionality
    - Request/reply, content type negotiation, ...
  - support of client/server transactions, push technology
  - key management, authentication, Internet security services

- WSP Services
  - provides shared state between client and server, optimizes content transfer
  - session management (establish, release, suspend, resume)
  - efficient capability negotiation
  - content encoding
  - Push

WSP overview

- Header Encoding
  - compact binary encoding of headers, content type identifiers and other well-known textual or structured values
  - reduces the data actually sent over the network
- Capabilities (are defined for):
  - message size, client and server
  - protocol options: Confirmed Push Facility, Push Facility, Session Suspend Facility, Acknowledgement headers
  - maximum outstanding requests
  - extended methods
- Suspend and Resume
  - server knows when client can accept a push
  - multi-bearer devices
  - dynamic addressing
  - allows the release of underlying bearer resources

WSP/B session establishment



CH: Client Header

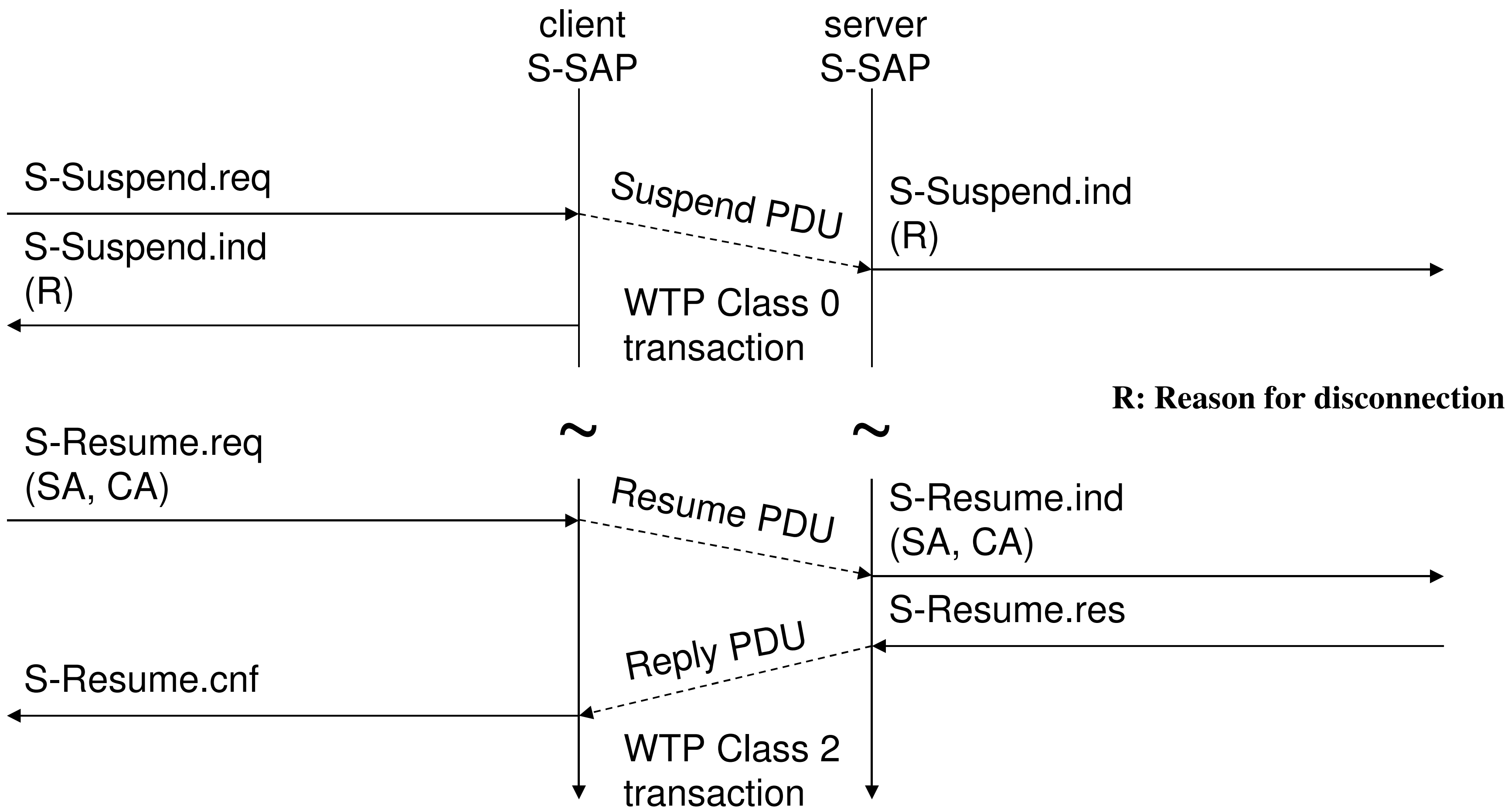
RC: Requested Capabilities

SH: Server Header

NC: Negotiated Capabilities

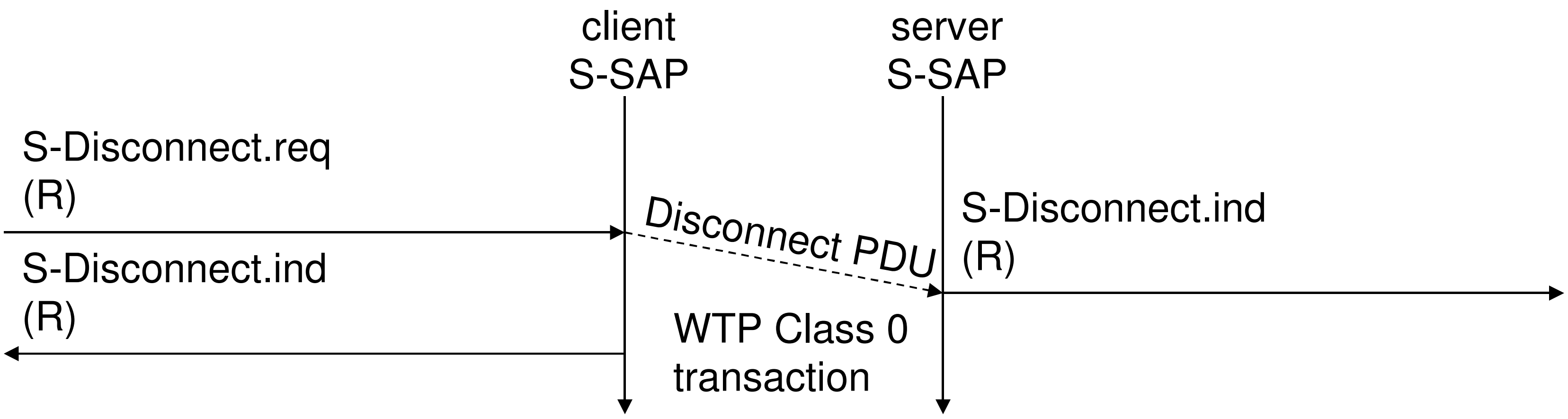
Source: Schiller

WSP/B session suspend/resume



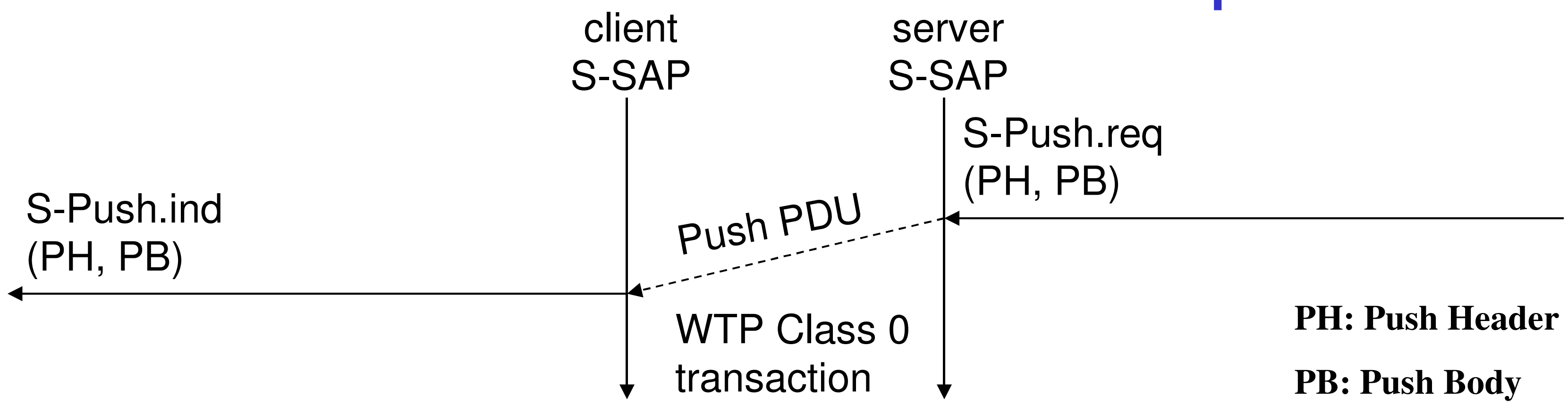
Source: Schiller

WSP/B session termination



Source: Schiller

confirmed/non-confirmed push

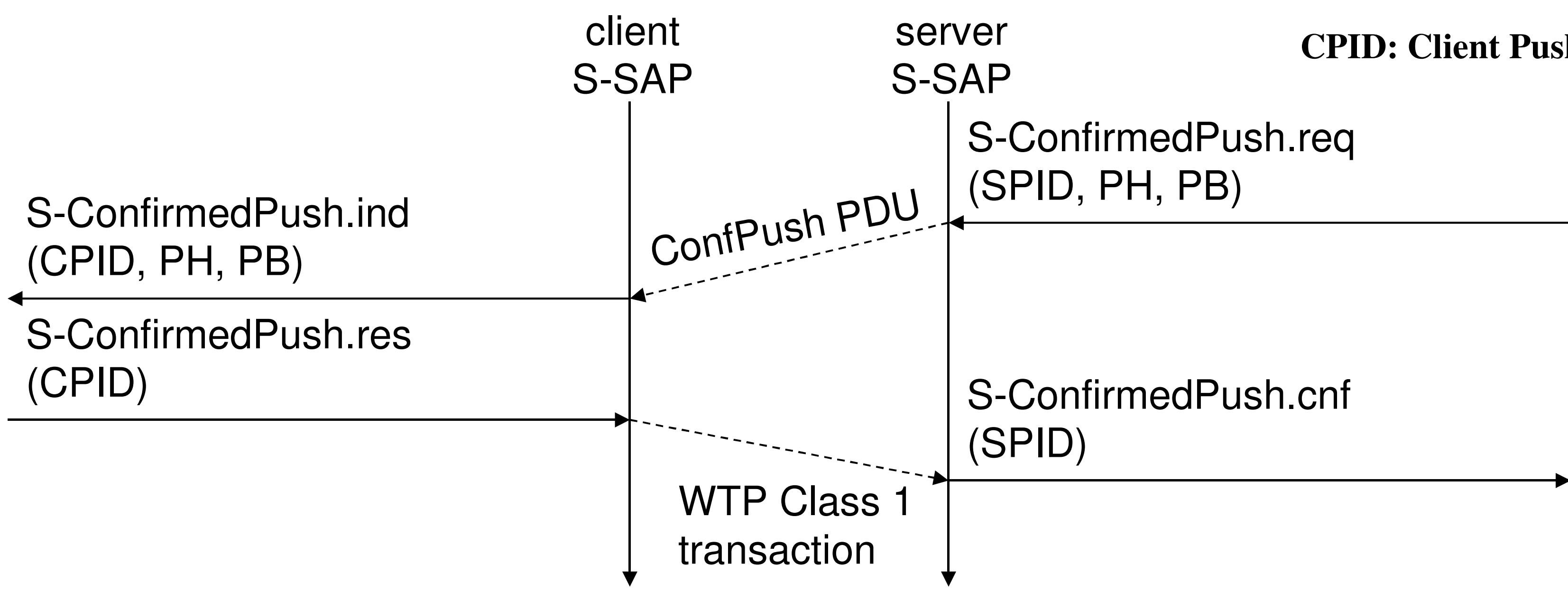


PH: Push Header

PB: Push Body

SPID: Server Push ID

CPID: Client Push ID



Source: Schiller

WAP Stack Summary

- WDP
  - functionality similar to UDP in IP networks
- WTLS
  - functionality similar to SSL/TLS (optimized for wireless)
- WTP
  - Class 0: analogous to UDP
  - Class 1: analogous to TCP (without connection setup overheads)
  - Class 2: analogous to RPC (optimized for wireless)
  - features of “user acknowledgement”, “hold on”
- WSP
  - WSP/B: analogous to http 1.1 (add features of suspend/resume)
  - method: analogous to RPC/RMI
  - features of asynchronous invocations, push (confirmed/unconfirmed)

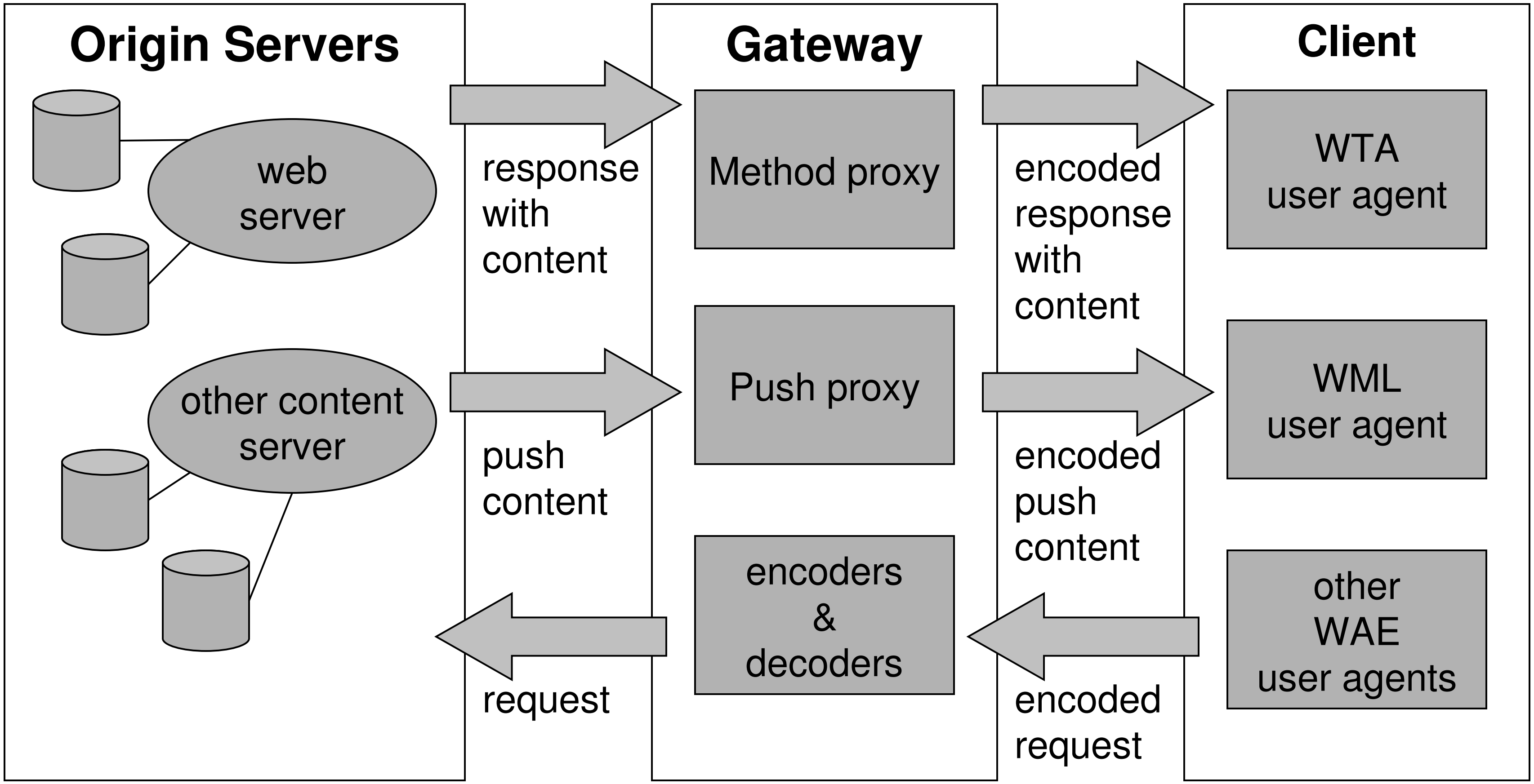
Wireless Application Environment (WAE)

- Goals
  - device and network independent application environment
  - for low-bandwidth, wireless devices
  - considerations of slow links, limited memory, low computing power, small display, simple user interface (compared to desktops)
  - integrated Internet/WWW programming model
  - high interoperability

WAE components

- Architecture
  - Application model, Microbrowser, Gateway, Server
- User Agents
  - WML/WTA/Others
  - content formats: vCard, vCalendar, Wireless Bitmap, WML..
- WML
  - XML-Syntax, based on card stacks, variables, ...
- WMLScript
  - procedural, loops, conditions, ... (similar to JavaScript)
- WTA
  - telephone services, such as call control, text messages, phone book, ... (accessible from WML/WMLScript)
- Proxy (Method/Push)

WAE: logical model

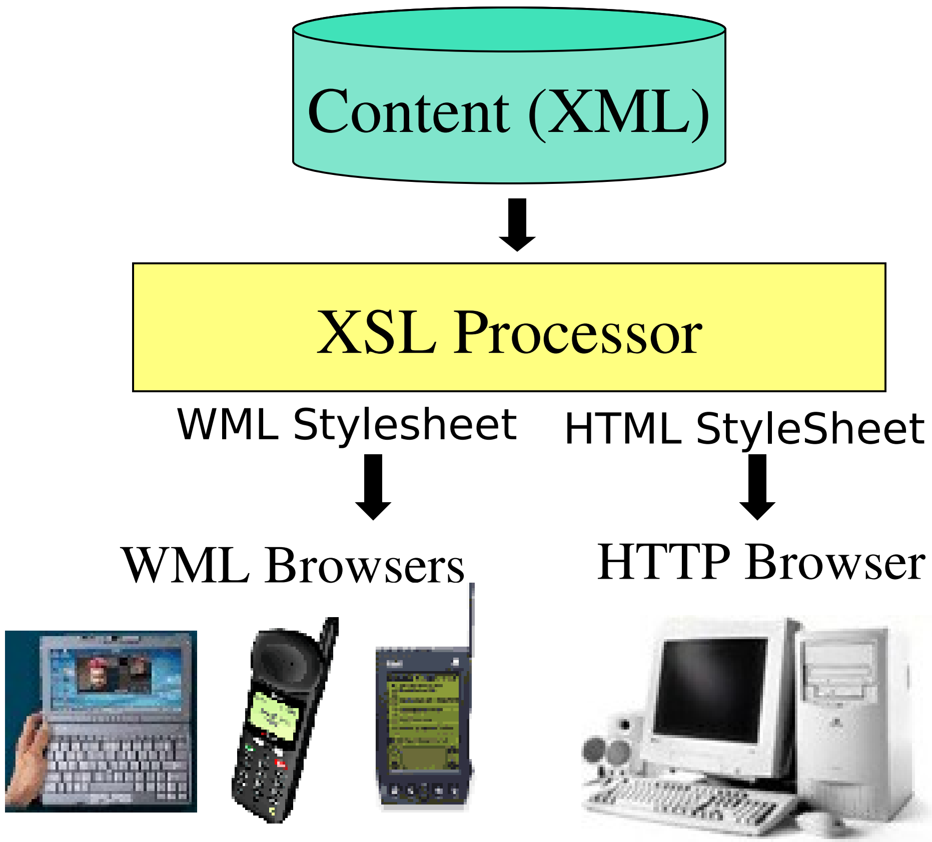


WAP microbrowser

- Optimized for wireless devices
- Minimal RAM, ROM, Display, CPU and keys
- Provides consistent service UI across devices
- Provides Internet compatibility
- Enables wide array of available content and applications

WML: Wireless Markup Language

- Tag-based browsing language:
  - Screen management (text, images)
  - Data input (text, selection lists, etc.)
  - Hyperlinks & navigation support
- Takes into account limited display, navigation capabilities of devices

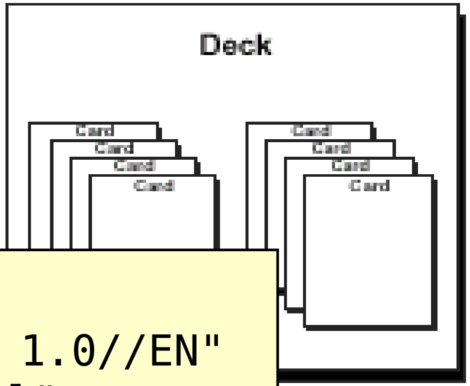


WML

- XML-based language
  - describes only intent of interaction in an abstract manner
  - presentation depends upon device capabilities
- Cards and Decks
  - document consists of many cards
  - User interactions are split into cards
  - Explicit navigation between cards
  - cards are grouped to decks
  - deck is similar to HTML page, unit of content transmission
- Events, variables and state mgmt

WML

- The basic unit is a **card**. Cards are grouped together into **Decks** Document ~ Deck (unit of transfer)
- All decks must contain
  - Document prologue
    - XML & document type declaration
  - <WML> element
    - Must contain one or more cards



WML File Structure

```
<?xml version="1.0"?>
<!DOCTYPE WML PUBLIC "-//WAPFORUM//DTD WML 1.0//EN"
        "http://www.wapforum.org/DTD/wml.xml">

<WML>
    ...
</WML>
```

WML cards

```
<WML>
  <CARD>
    <DO TYPE="ACCEPT">
      <GO URL="#eCard"/>
    </DO
    Welcome!
  </CARD>
  <CARD NAME="eCard">
    <DO TYPE="ACCEPT">
         <GO URL="/submit?N=$(N)&S=$(S)"/
>
    </DO>
    Enter name: <INPUT KEY="N"/>
    Choose speed:
    <SELECT KEY="S">
      <OPTION VALUE="0">Fast</OPTION>
      <OPTION VALUE="1">Slow</OPTION>
    <SELECT>
  </CARD>
</WML>
```

Navigation

Variables

Input Elements

Card

Deck

Wireless Telephony Application (WTA)

- Collection of telephony specific extensions
  - designed primarily for network operators
- Example
  - calling a number (WML)
    `wtai://wp/mc;07216086415`
  - calling a number (WMLScript)
    `WTAPublic.makeCall("07216086415");`
- Implementation
  - Extension of basic WAE application model
  - Extensions added to standard WML/WMLScript browser
  - Exposes additional API (WTAI)

WTA features

- Extension of basic WAE application model
  - network model for interaction
    - client requests to server
    - event signaling: server can push content to the client
  - event handling
    - table indicating how to react on certain events from the network
    - client may now be able to handle unknown events
  - telephony functions
    - some application on the client may access telephony functions

WTA Interface

- generic, high-level interface to mobile's telephony functions
  - setting up calls, reading and writing entries in phonebook
- WTA API includes
  - Call control
  - Network text messaging
  - Phone book interface
  - Event processing
- Security model: segregation
  - Separate WTA browser
  - Separate WTA port

WTA Example (WML)

Placing an outgoing call with WTAI:

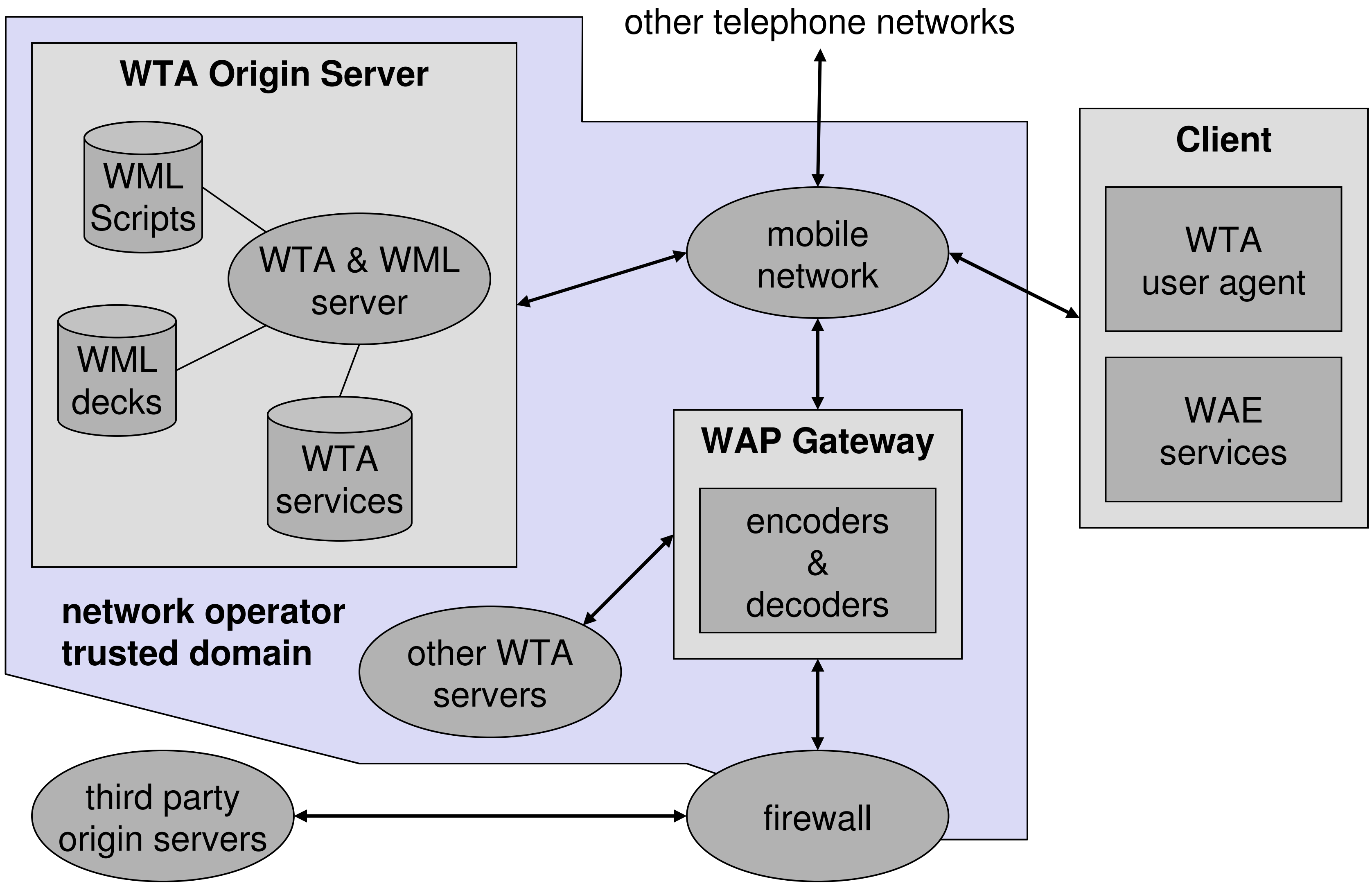
WTAI Call

Input Element

```
<WML>
<CARD>
  <DO TYPE=“ACCEPT”>
    <GO URL=“wtai:cc/mc;$(N)”/>
  </DO>
    Enter phone number:
    <INPUT TYPE=“TEXT” KEY=“N”/>
</CARD>
</WML>
```

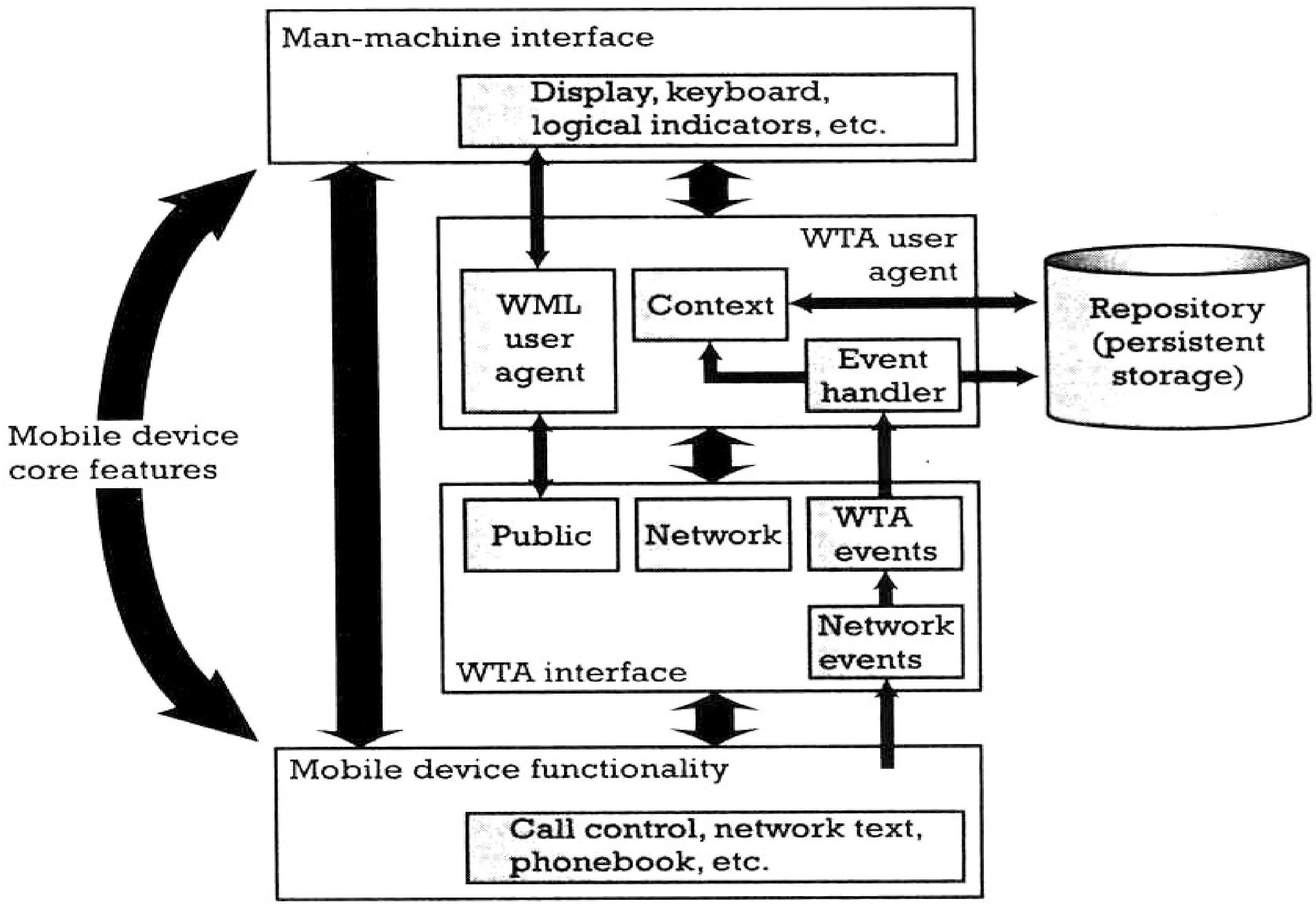

Source: WAP Forum

WTA Logical Architecture



Source: Schiller

WTA Framework Components



Source: Heijden

WTA User Agent

- WTA User Agent
  - WML User agent with extended functionality
  - can access mobile device's telephony functions through WTAI
  - can store WTA service content persistently in a repository
  - handles events originating in the mobile network

WTA User Agent Context

- Abstraction of execution space
- Holds current parameters, navigation history, state of user agent
- Similar to activation record in a process address space

- Uses connection-mode and connectionless services offered by WSP
- Specific, secure WDP ports on the WAP gateway

WTA Events

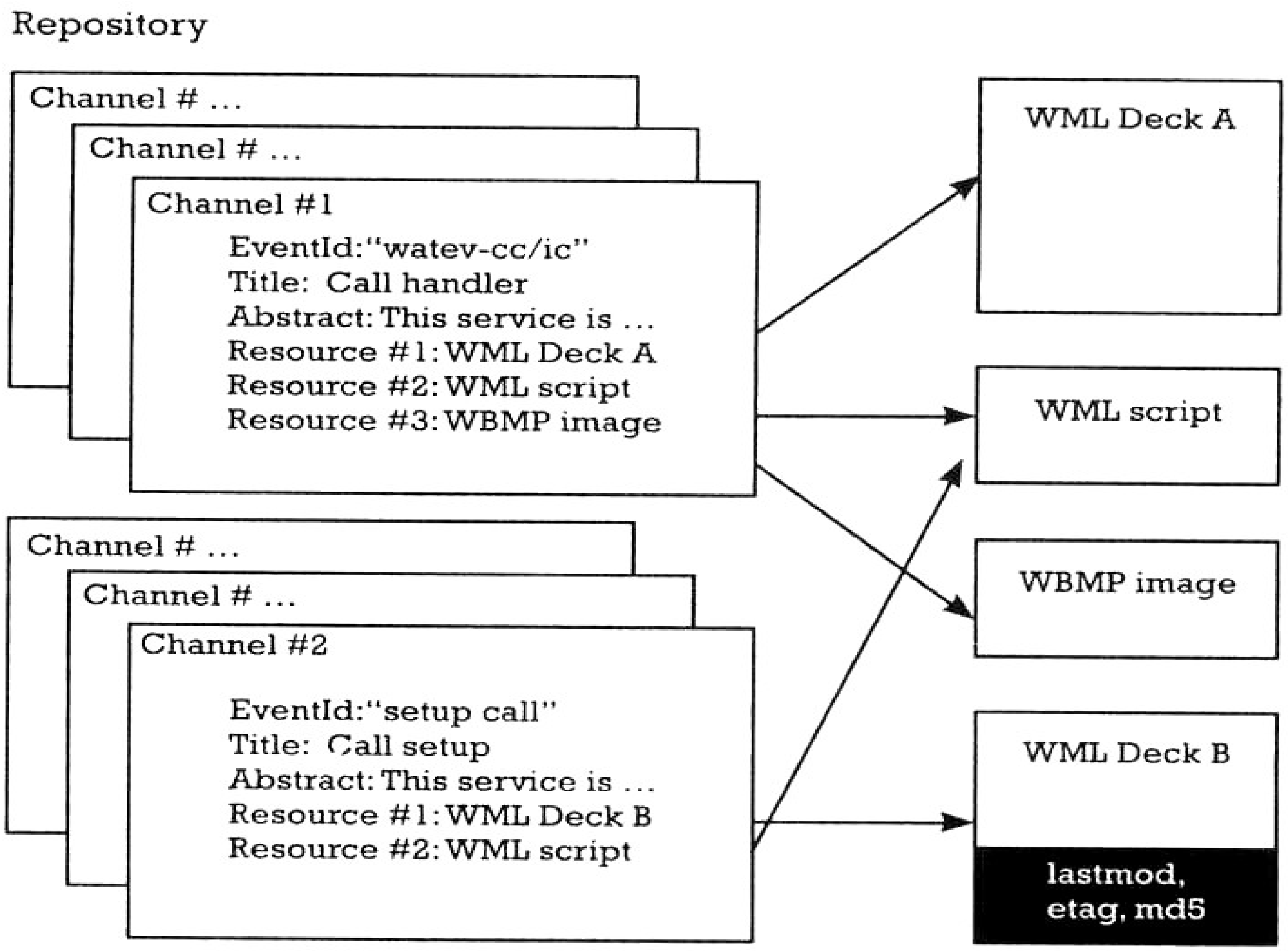
- Network notifies device of event (such as incoming call)
- WTA events map to device's native events
- WTA services are aware of and able to act on these events

- example: incoming call indication, call cleared, call connected

WTA Repository

- local store for content related to WTA services (minimize network traffic)
- Channels: define the service
  - content format defining a WTA service stored in repository
  - XML document specifying eventid, title, abstract, and resources that implement a service
- Resources: execution scripts for a service
  - could be WML decks, WML Scripts, WBMP images..
  - downloaded from WTA server and stored in repository before service is referenced
- Server can also initiate download of a channel

WTA Channels and Resources



Source: Heijden

WTA Interface (public)

- for third party WML content providers
- restricted set of telephony functions available to any WAE User Agent
  - library functions
    - make call: allows application to setup call to a valid tel number
    - send DTMF tones: send DTMF tones through the setup call
- user notified to grant permission for service execution
  - cannot be triggered by network events
  - example: Yellow pages service with “make call” feature

WTA Interface (network)

- Network Common WTAI
  - WTA service provider is in operator's domain
  - all WTAI features are accessible, including the interface to WTA events
  - library functions
    - Voice-call control: setup call, accept, release, send DTMF tones
    - Network text: send text, read text, remove text (SMS)
    - Phonebook: write, read, remove phonebook entry
    - Call logs: last dialed numbers, missed calls, received calls
    - Miscellaneous: terminate WTA user agent, protect context
  - user can give blanket permission to invoke a function
  - example: Voice mail service

WTAI (network)

- Network Specific WTAI
  - specific to type of bearer network
  - example: GSM: call reject, call hold, call transfer, join multiparty, send USSD

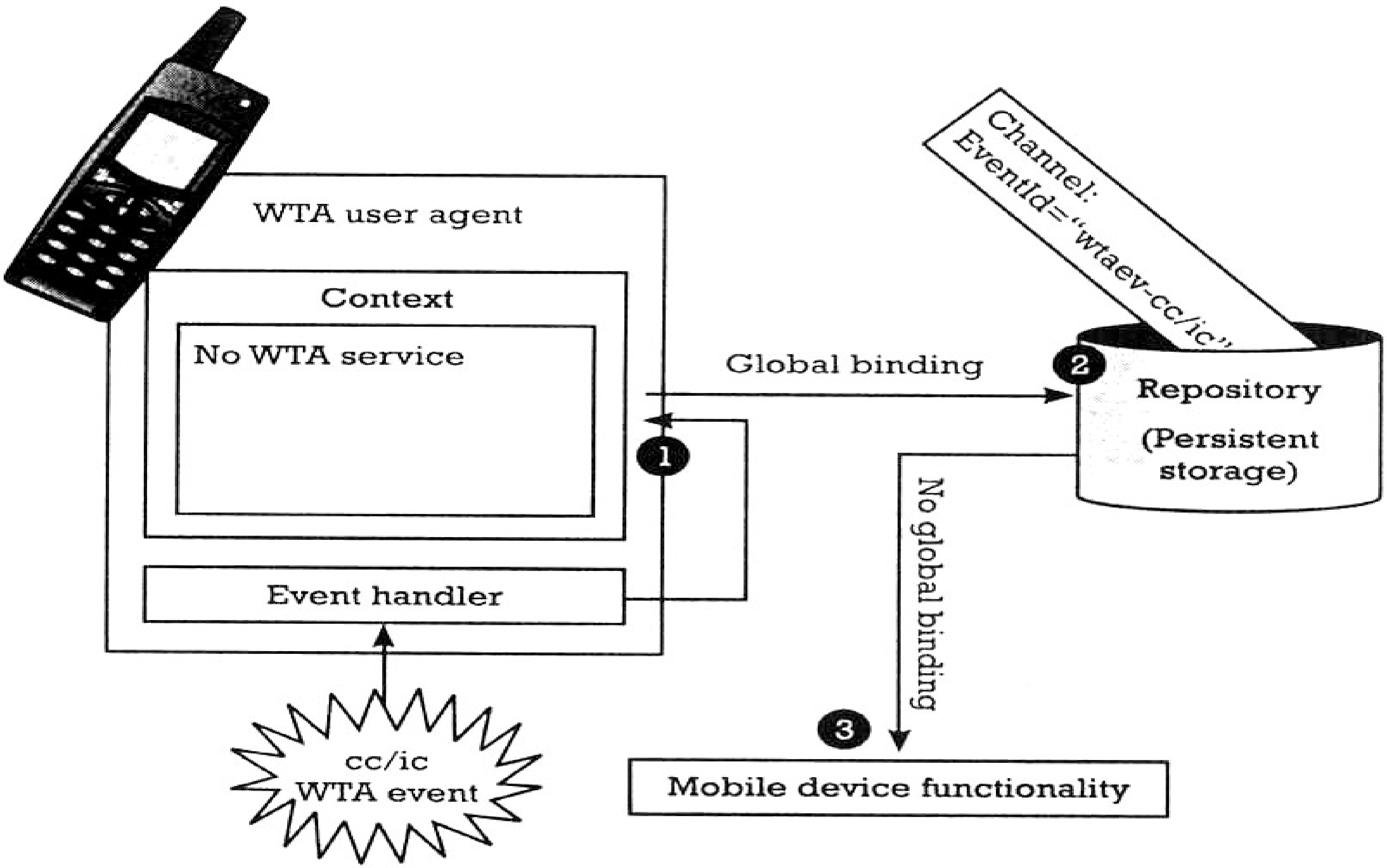
WTA: event handling

- Event occurrence
  - WTA user agent could be executing and expecting the event
  - WTA user agent could be executing and a different event occurs
  - No service is executing
- Event handling
  - channel for each event defines the content to be processed upon reception of that event

WTA: event binding

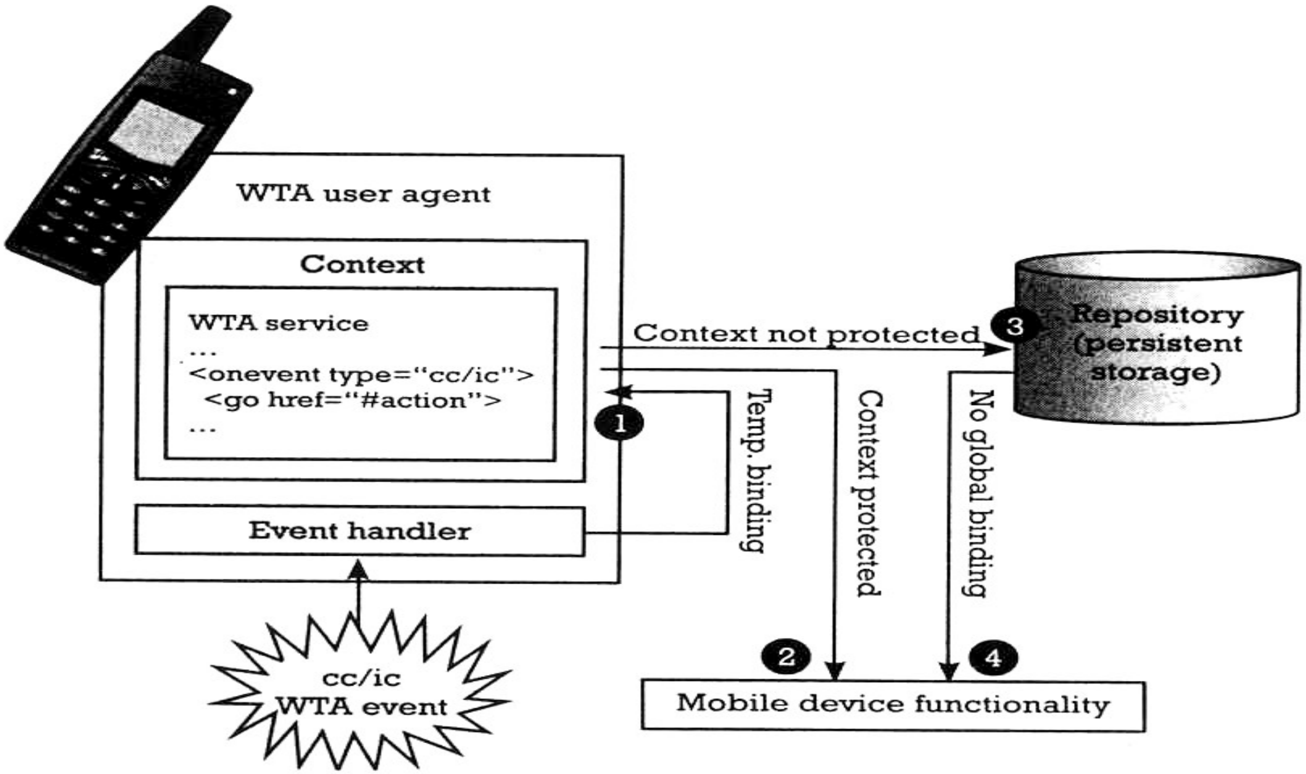
- association of an event with the corresponding handler (channel)
- Global binding:
  - channel corresponding to the event is stored in the repository
  - event causes execution of resources defined by the channel
  - example: voice mail service
- Temporary binding:
  - resources to be executed are defined by the already executing service
  - example: yellow pages lookup and call establishment

Event Handling (no service in execution)



Source: Heijden

Event Handling (service already execution)



1: Temporary binding exists

2. No temporary binding and context is protected

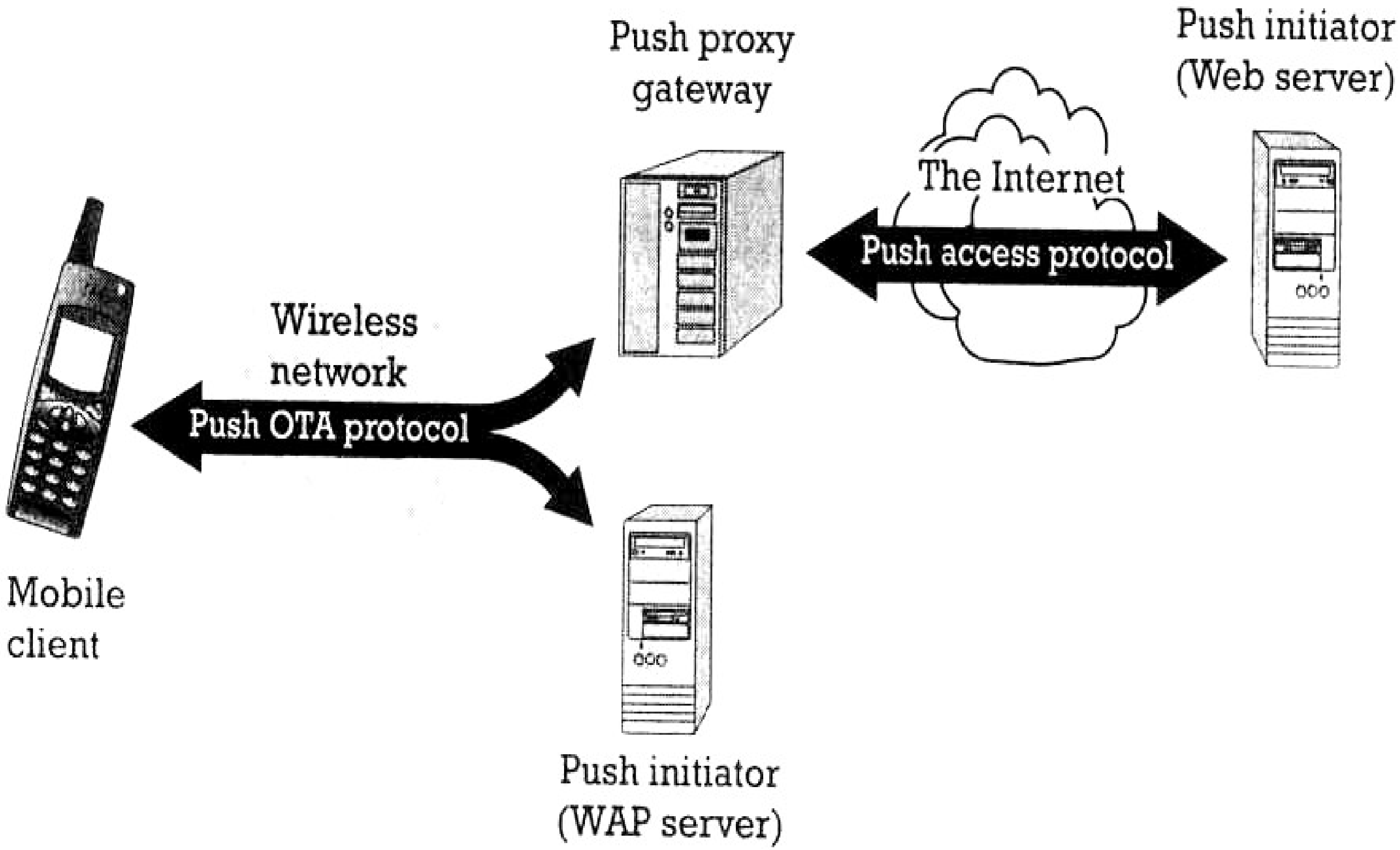
3: No temporary binding and context is not protected

Source: Heijden

WAP Push Services

- Web push
  - Scheduled pull by client (browser)
    - example: Active Channels
  - no real-time alerting/response
    - example: stock quotes
- Wireless push
  - accomplished by using the network itself
    - example: SMS
  - limited to simple text, cannot be used as starting point for service
    - example: if SMS contains news, user cannot request specific news item
- WAP push
  - Network supported push of WML content
    - example: Alerts or service indications
  - Pre-caching of data (channels/resources)

WAP push framework



Source: Heijden

Push Access Protocol

- Based on request/response model
- Push initiator is the client
- Push proxy is the server
- Initiator uses HTTP POST to send push message to proxy
- Initiator sends control information as an XML document, and content for mobile (as WML)
- Proxy sends XML entity in response indicating submission status
- Initiator can
  - cancel previous push
  - query status of push
  - query status/capabilities of device

Push Proxy Gateway

- WAP stack (communication with mobile device)
- TCP/IP stack (communication with Internet push initiator)
- Proxy layer does
  - control information parsing
  - content transformation
  - session management
  - client capabilities
  - store and forward
  - prioritization
  - address resolution
  - management function

Over the Air (OTA) Protocol

- Extends WSP with push-specific functionality
- Application ID uniquely identifies a particular application in the client (referenced as a URI)
- Connection-oriented mode
  – client informs proxy of application IDs in a session
- Connectionless mode
  – well known ports, one for secure and other for non-secure push
- Session Initiation Application (SIA)
  – unconfirmed push from proxy to client
  – request to create a session for a specific user agent and bearer

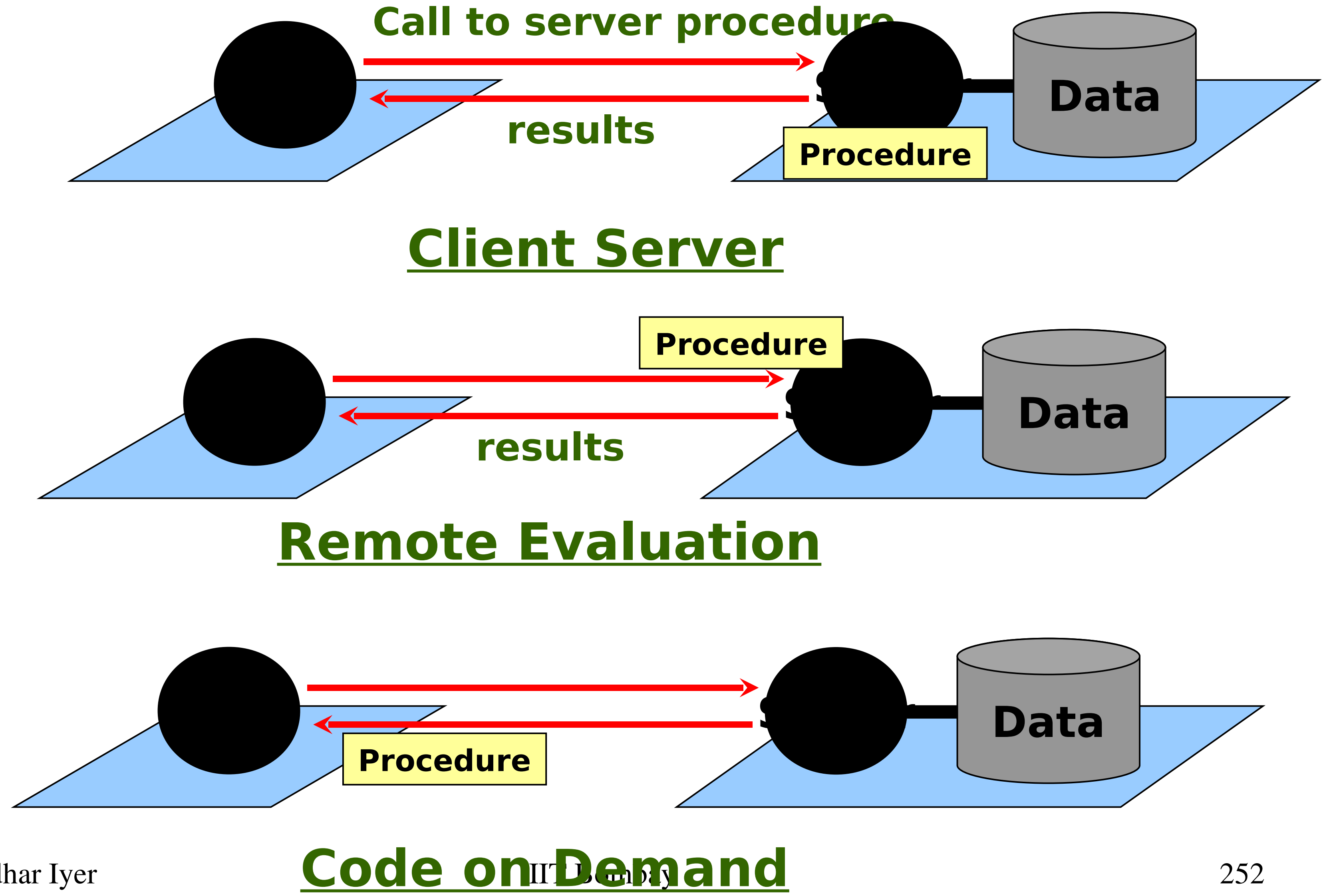
WAE Summary

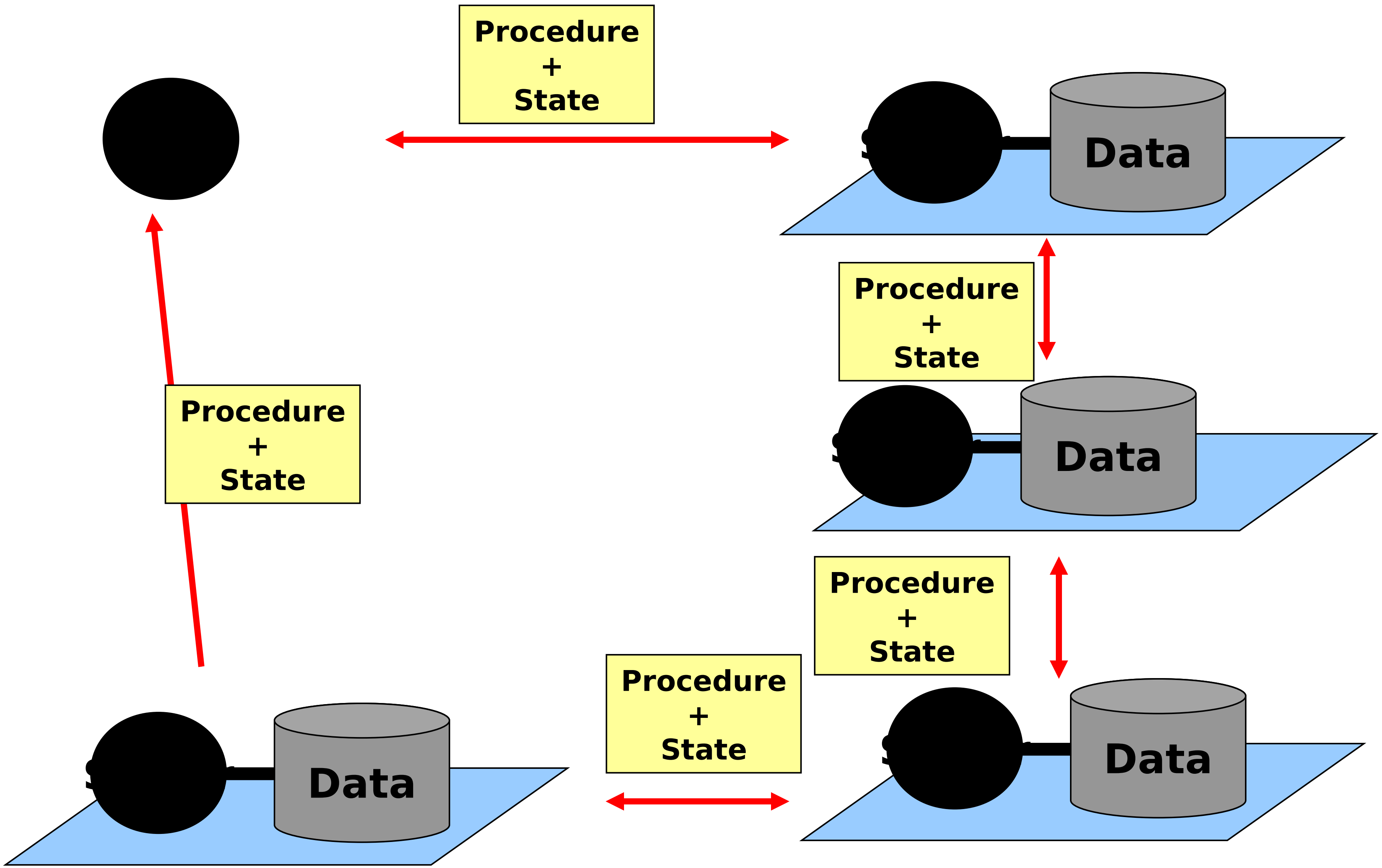
- WML and WML Script
  - analogous to HTML and JavaScript (optimized for wireless)
  - microbrowser user agent; compiler in the network
- WTA
  - WTAI: different access rights for different applications/agents
  - WTA User Agent (analogy with operating systems)
    - Context – Activation Record
    - Channel – Interrupt Handler
    - Resource – Shared routines invoked by interrupt handlers
    - Repository – Library of interrupt handlers
  - feature of dynamically pushing the interrupt handler before the event
- Push
  - no analogy in Internet

Outline

- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- TCP over wireless
- GSM air interface
- GPRS network architecture
- Wireless application protocol
- **Mobile agents**
- Mobile ad hoc networks

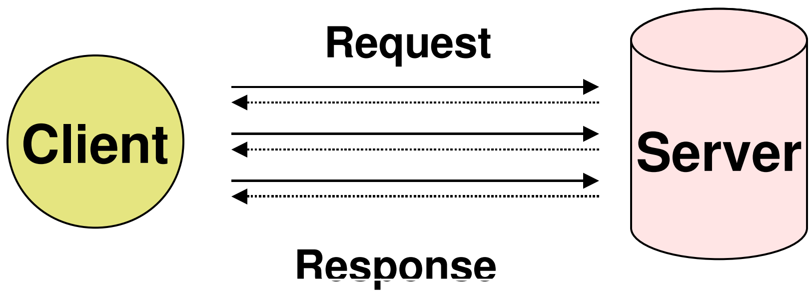
Structuring Distributed Applications



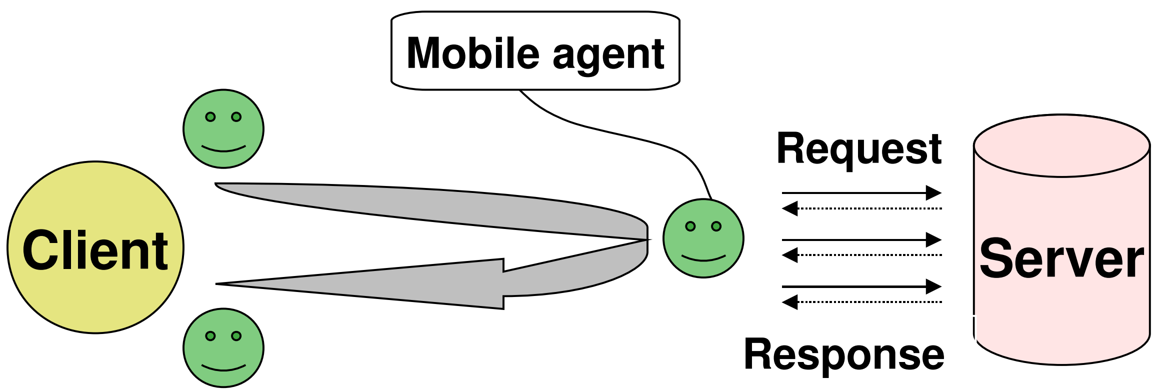


Mobile Agents

Interaction Model



Client/server communication



Mobile agent communication

A generic Mobile Agent Framework

- Event notification
- Agent collaboration support

Event Manager

Mobile Agent

- Execution environment
- Communication (agent dispatching)
- Agent life cycle (creation, destruction)

Agent Manager

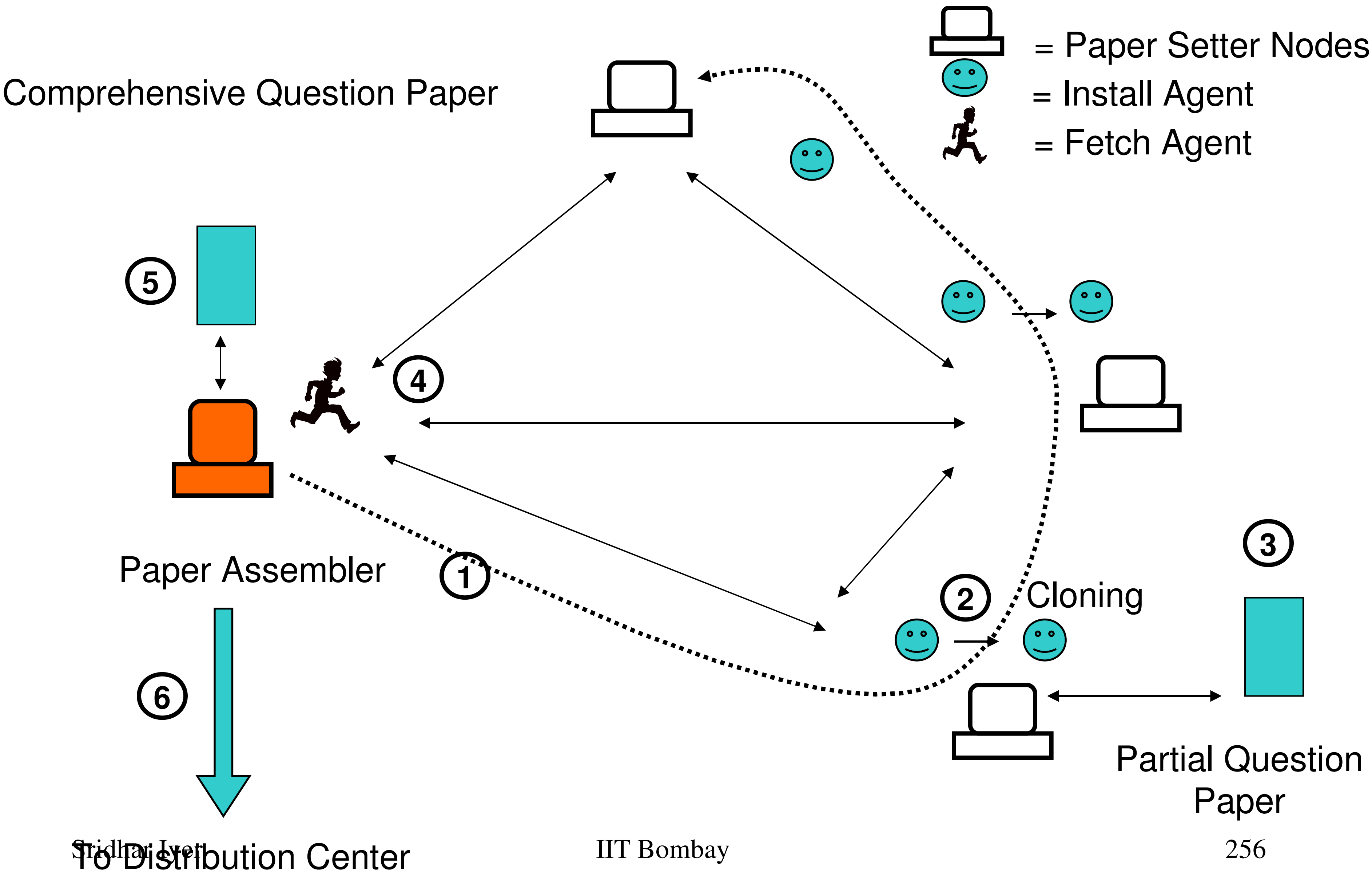
- User identification
- Protection (agent, server)
- Authentication

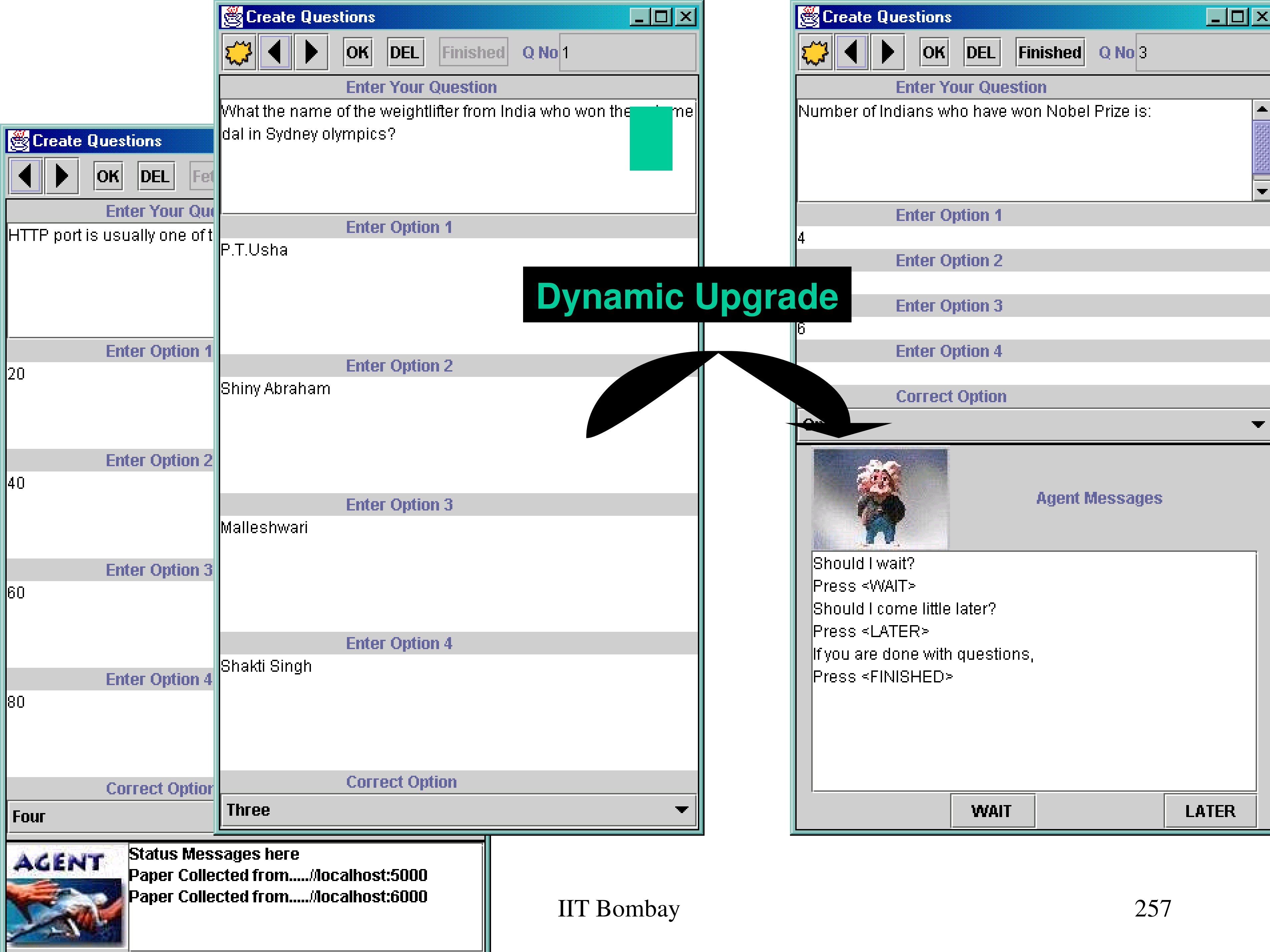
Security Manager

- Agent state
- Agent checkpoint (fault tolerance)

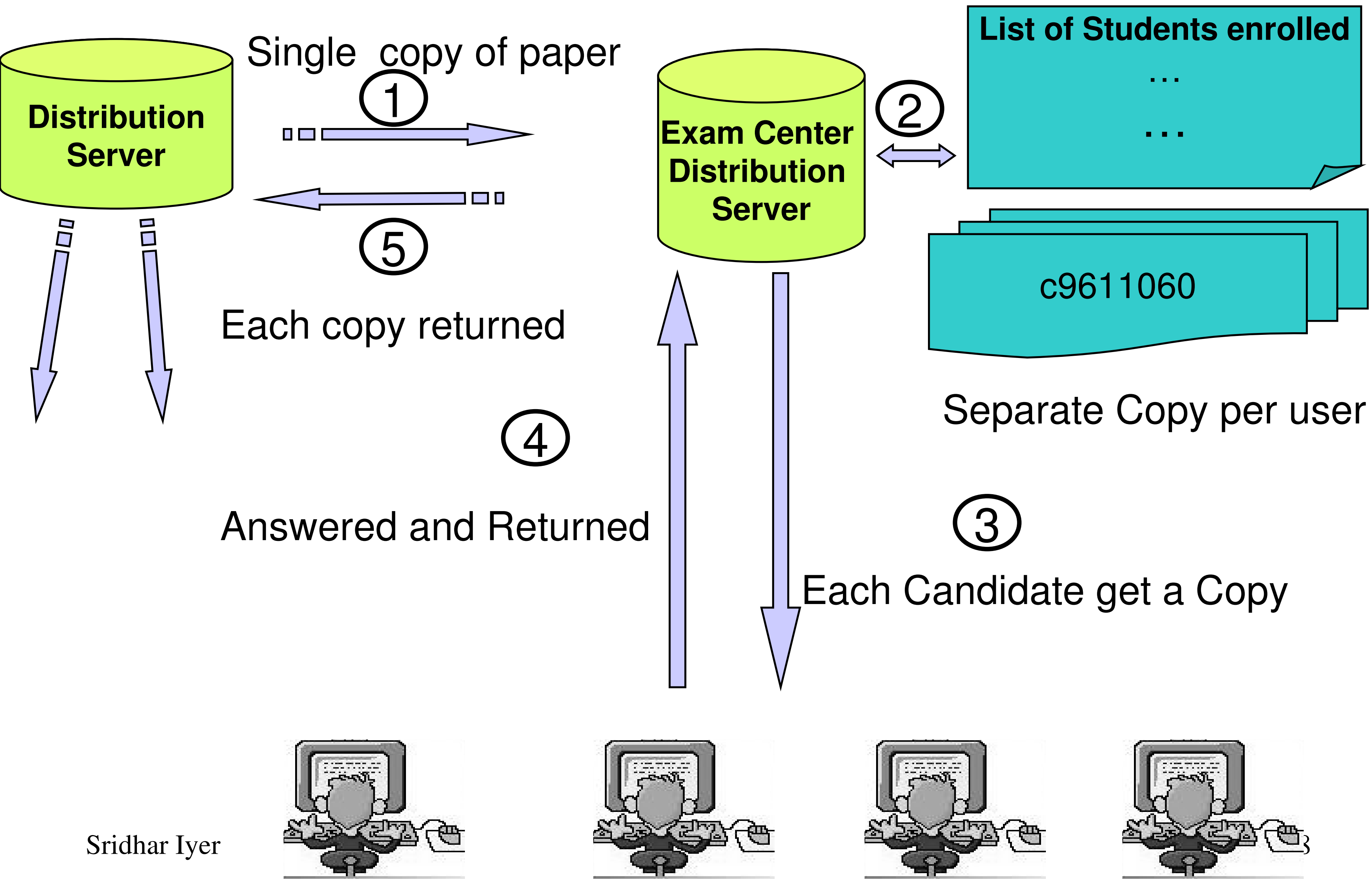
Persistent

Example: Student Examination Scenario

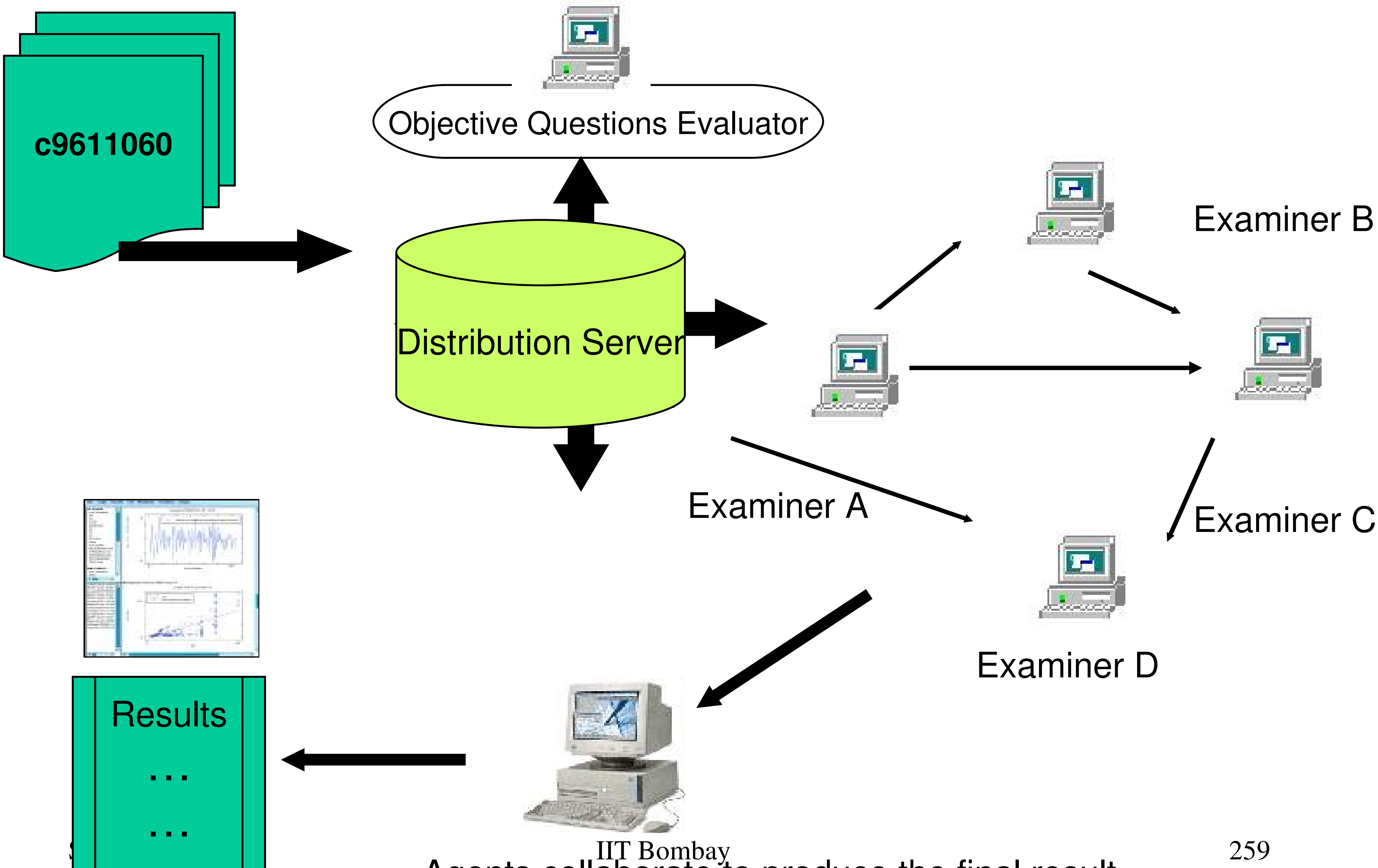



Create Questions
OK
DEL
Enter Your Qu
HTTP port is usually one of t
Enter Option 1
20
Enter Option 2
40
Enter Option 3
60
Enter Option 4
80
Correct Option
Four
Create Questions
OK
DEL
Finished
Q No 1
Enter Your Question
What the name of the weightlifter from India who won the me
dal in Sydney olympics?
Enter Option 1
P.T.Usha
Enter Option 2
Shiny Abraham
Enter Option 3
Malleshwari
Enter Option 4
Shakti Singh
Correct Option
Three
Dynamic Upgrade
Create Questions
OK
DEL
Finished
Q No 3
Enter Your Question
Number of Indians who have won Nobel Prize is:
Enter Option 1
4
Enter Option 2
Enter Option 3
6
Enter Option 4
Correct Option
Agent Messages
Should I wait?
Press <WAIT>
Should I come little later?
Press <LATER>
If you are done with questions,
Press <FINISHED>
WAIT
LATER
AGENT
Status Messages here
Paper Collected from...../localhost:5000
Paper Collected from...../localhost:6000

Example: Distribution and Testing



Example: Evaluation and Results



Agents collaborate to produce the final result

Mobile Agents Summary

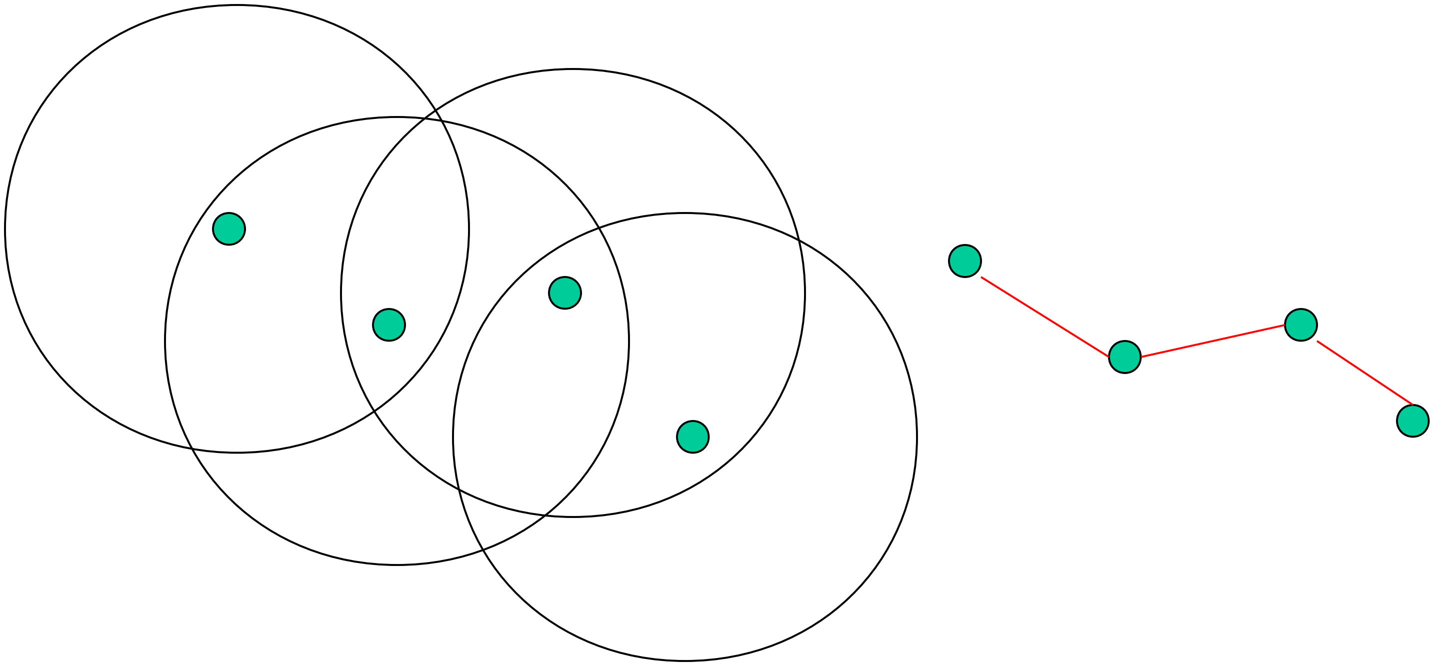
- Appears to be a useful mechanism for applications on mobile and wireless devices
  - Reduce the network load
  - Help in overcoming latency
  - Execute asynchronously and autonomously
- Several issues yet to be addressed
  - Heavy frameworks
  - Interoperability
  - Security concerns

Outline

- Introduction and Overview
- Wireless LANs: IEEE 802.11
- Mobile IP routing
- TCP over wireless
- GSM air interface
- GPRS network architecture
- Wireless application protocol
- Mobile agents
- **Mobile ad hoc networks**

Multi-Hop Wireless

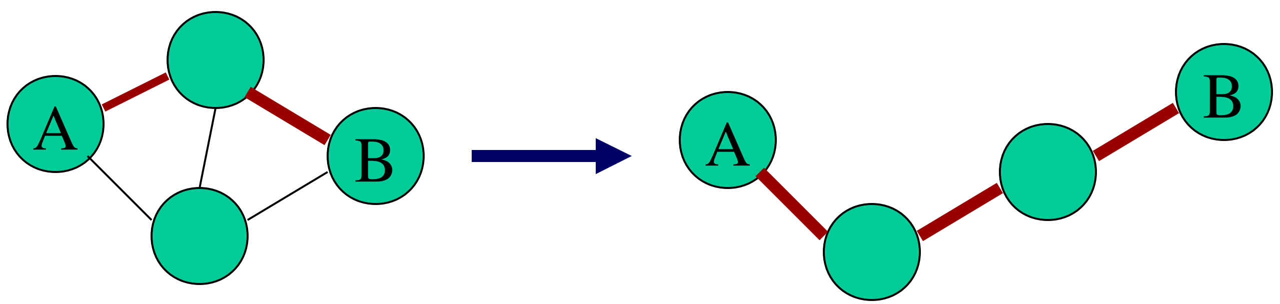
- May need to traverse multiple links to reach destination



- Mobility causes route changes

Mobile Ad Hoc Networks (MANET)

- Host movement frequent
- Topology change frequent



- No cellular infrastructure. Multi-hop wireless links.
- Data must be routed via intermediate nodes.

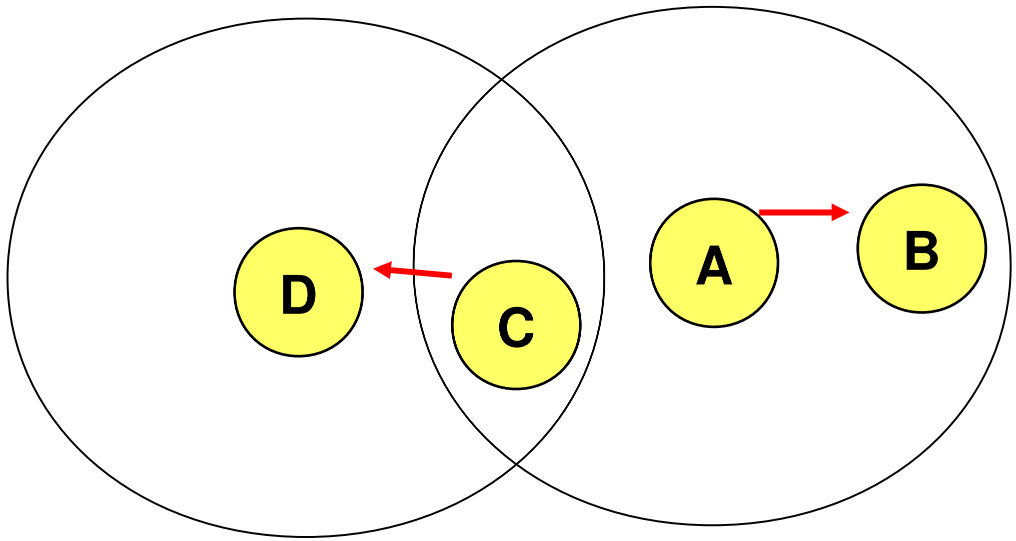
Many Applications

- Ad hoc networks:
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Useful when infrastructure is absent, destroyed or impractical
  - Infrastructure may not be present in a disaster area or war zone
- Applications:
  - Military environments
  - Emergency operations
  - Civilian environments
    - taxi cab network
    - meeting rooms
    - sports stadiums

MAC in Ad hoc Networks

- IEEE 802.11 DCF is most popular
  - Easy availability
- 802.11 DCF:
  - Uses RTS-CTS to avoid hidden terminal problem
  - Uses ACK to achieve reliability
- 802.11 was designed for single-hop wireless
  - Does not do well for multi-hop ad hoc scenarios
  - Reduced throughput
  - Exposed terminal problem

Exposed Terminal Problem



- 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

Routing Protocols

- Proactive protocols
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; High routing overhead
  - Example: DSDV (destination sequenced distance vector)

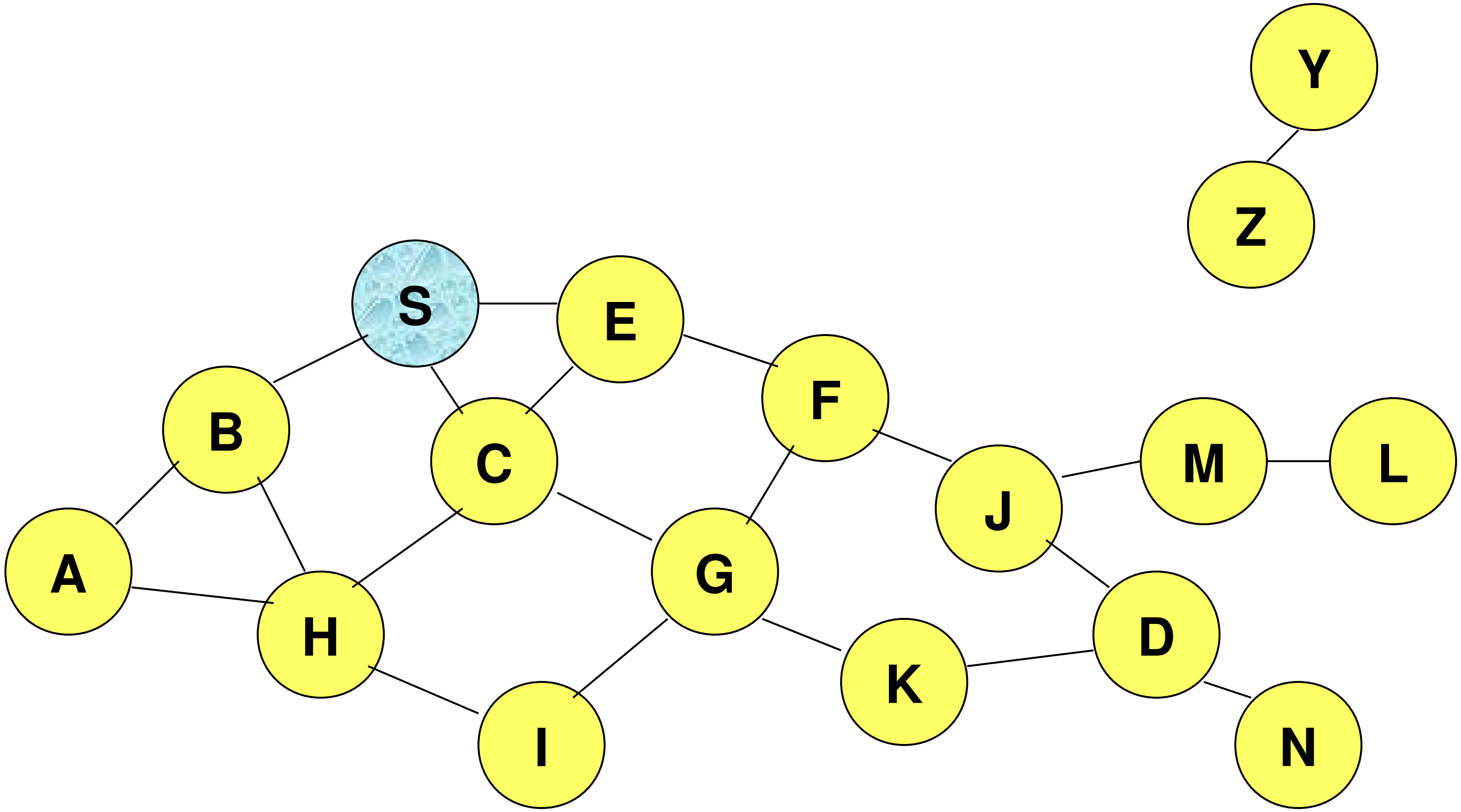
- Reactive protocols
  - Determine route if and when needed
  - Source initiates route discovery
  - Example: DSR (dynamic source routing)

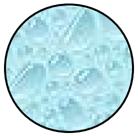
- Hybrid protocols
  - Adaptive; Combination of proactive and reactive
  - Example : ZRP (zone routing protocol)

Dynamic Source Routing (DSR)

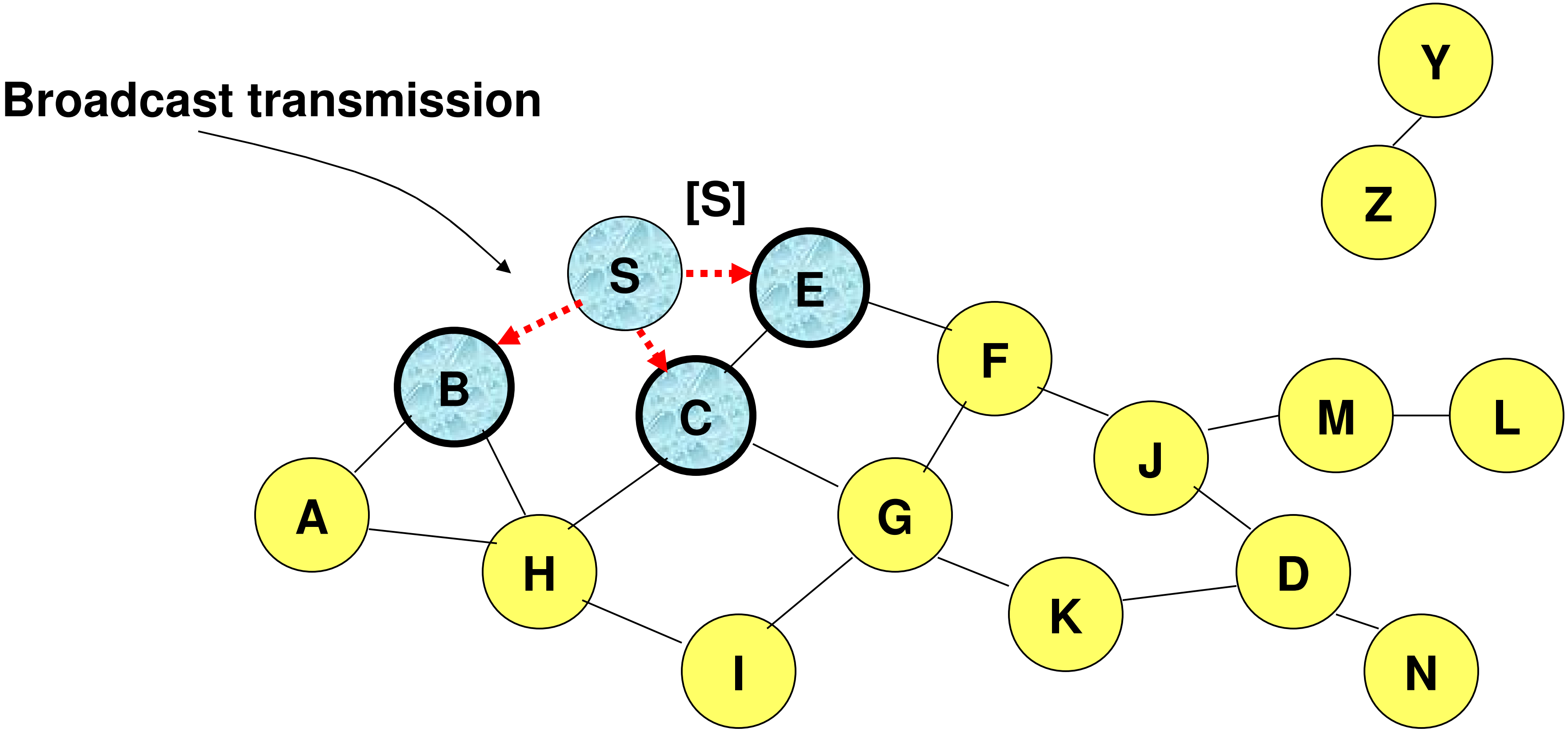
- Route Discovery Phase:
  - Initiated by source node S that wants to send packet to destination node D
  - Route Request (RREQ) floods through the network
  - Each node *appends own identifier* when forwarding RREQ
- Route Reply Phase:
  - D on receiving the first RREQ, sends a Route Reply (RREP)
  - RREP is sent on a route obtained by reversing the route appended to received RREQ
  - RREP includes the route from S to D on which RREQ was received by node D
- Data Forwarding Phase:
  - S sends data to D by source routing through intermediate nodes

Route Discovery in DSR




Represents a node that has received RREQ for D from S

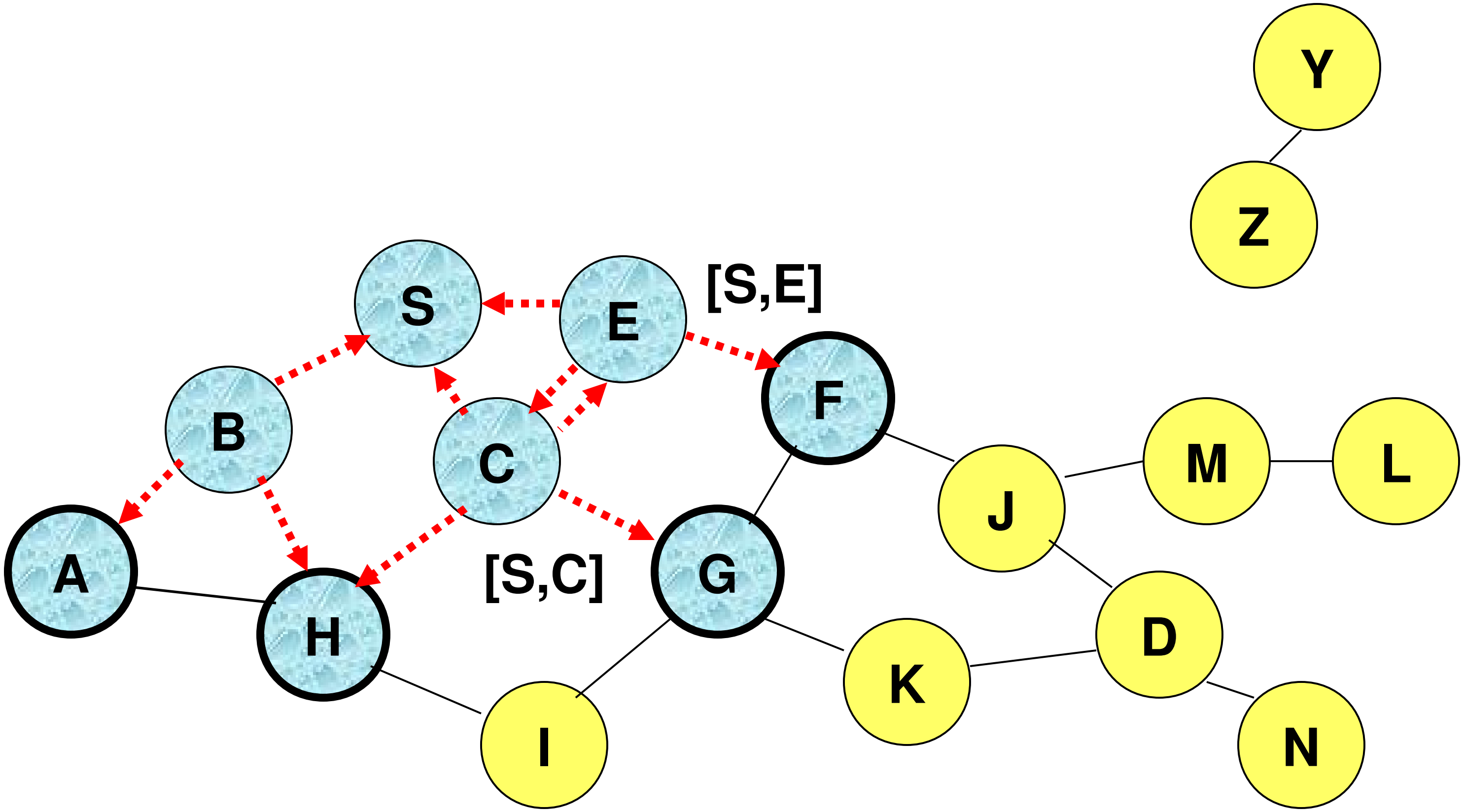
Route Discovery in DSR



Represents transmission of RREQ

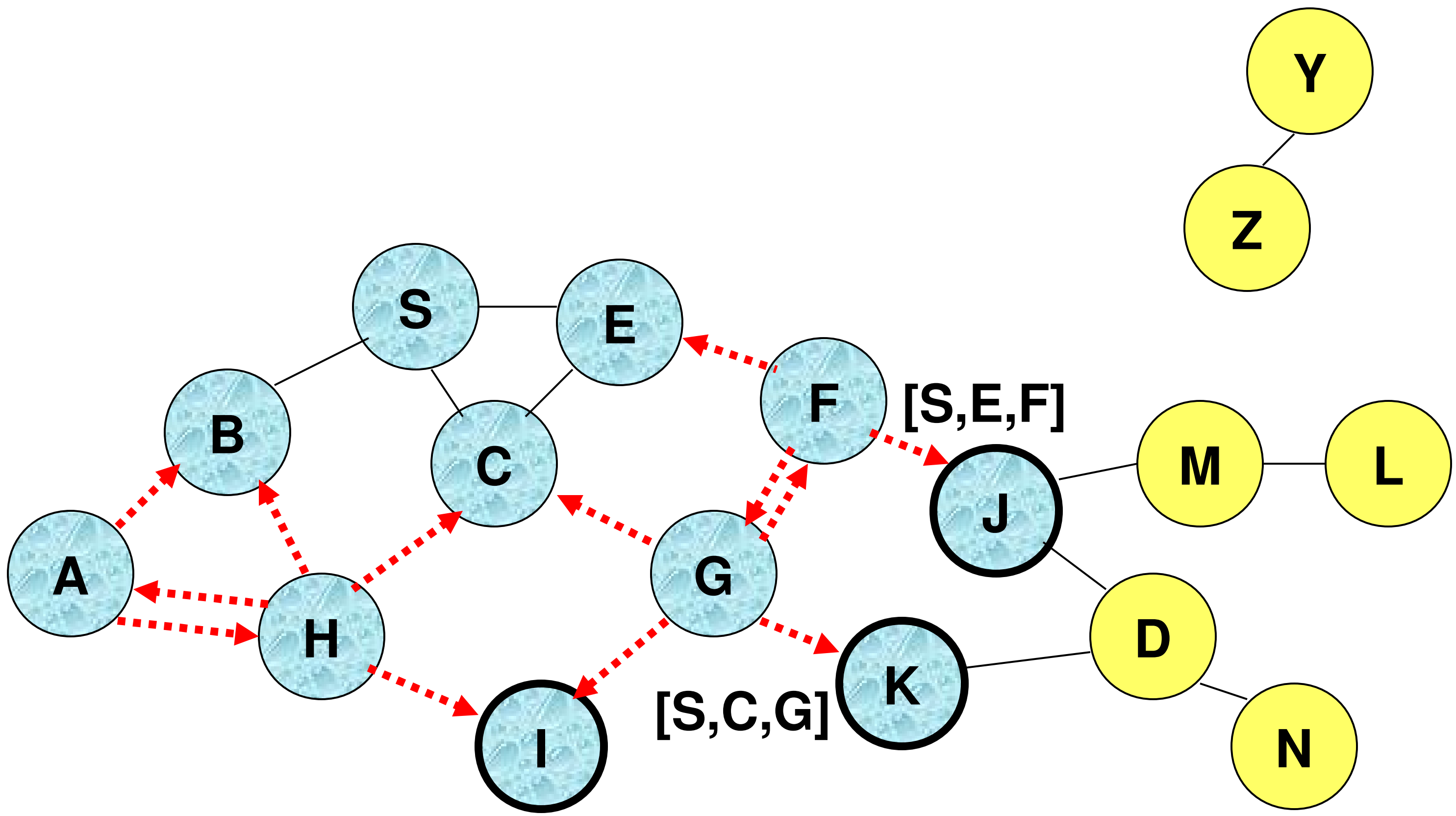
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



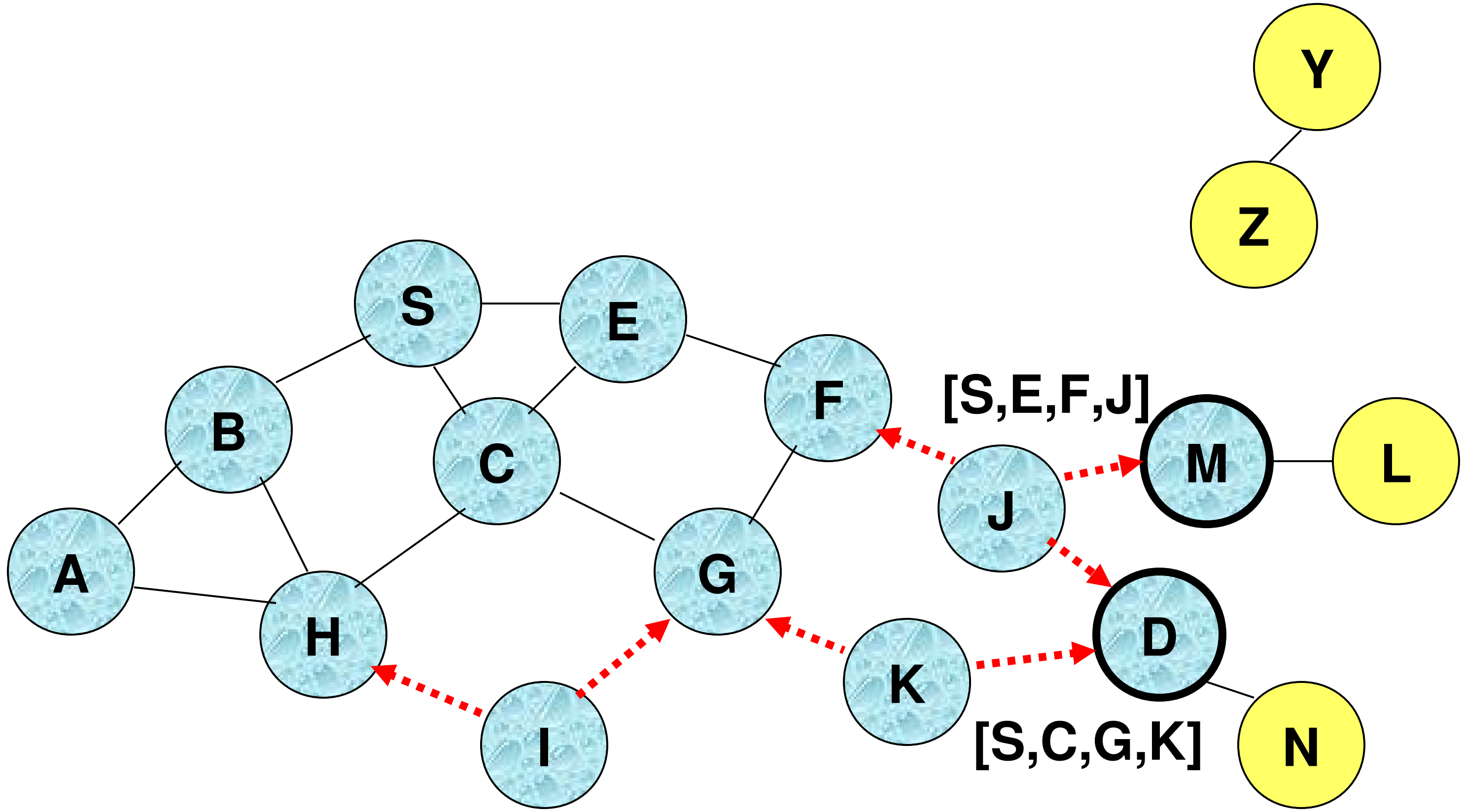
- **Node H receives packet RREQ from two neighbors: potential for collision**

Route Discovery in DSR



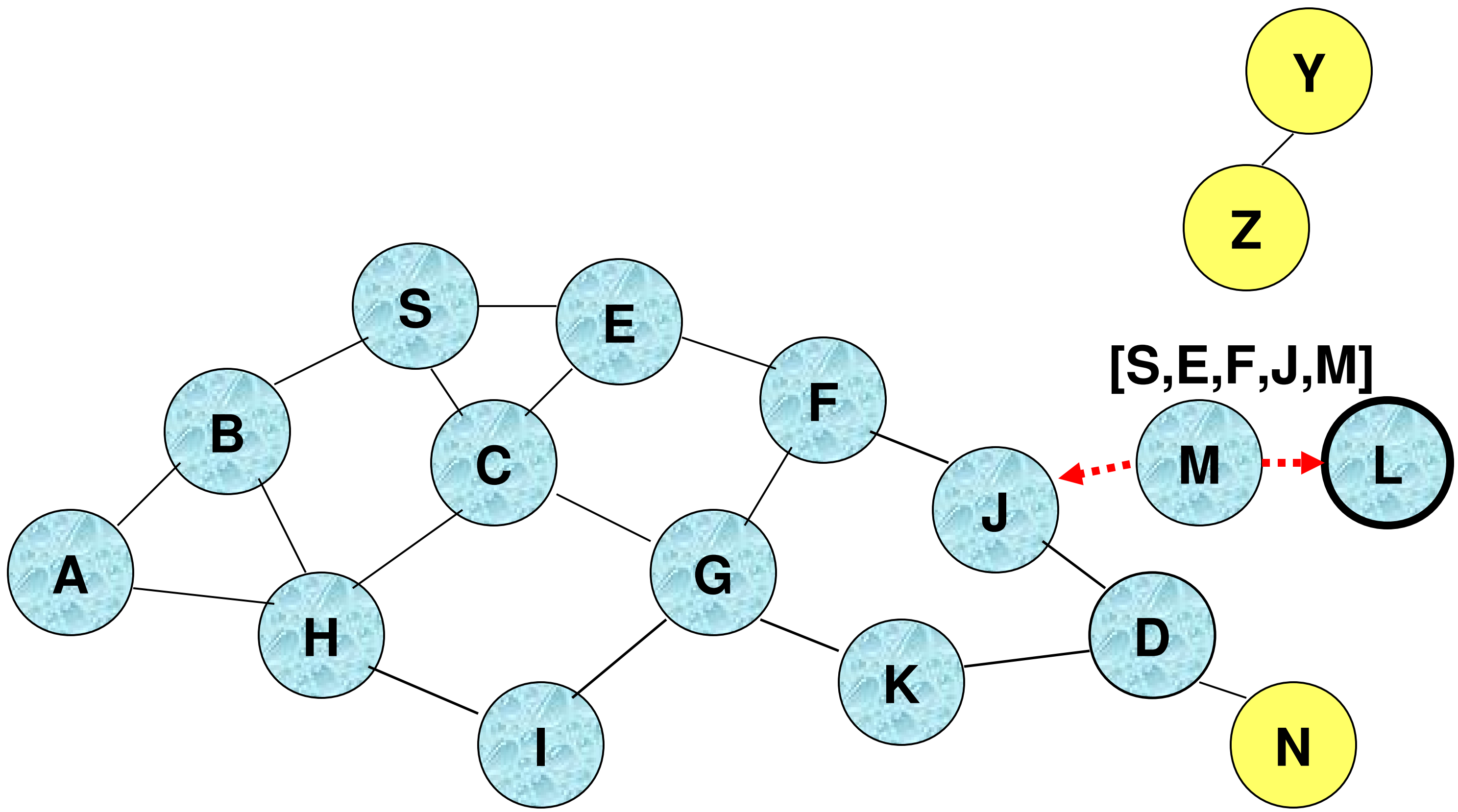
- Node C receives RREQ from G and H, but does not forward it again, because node C has **already forwarded RREQ** once

Route Discovery in DSR



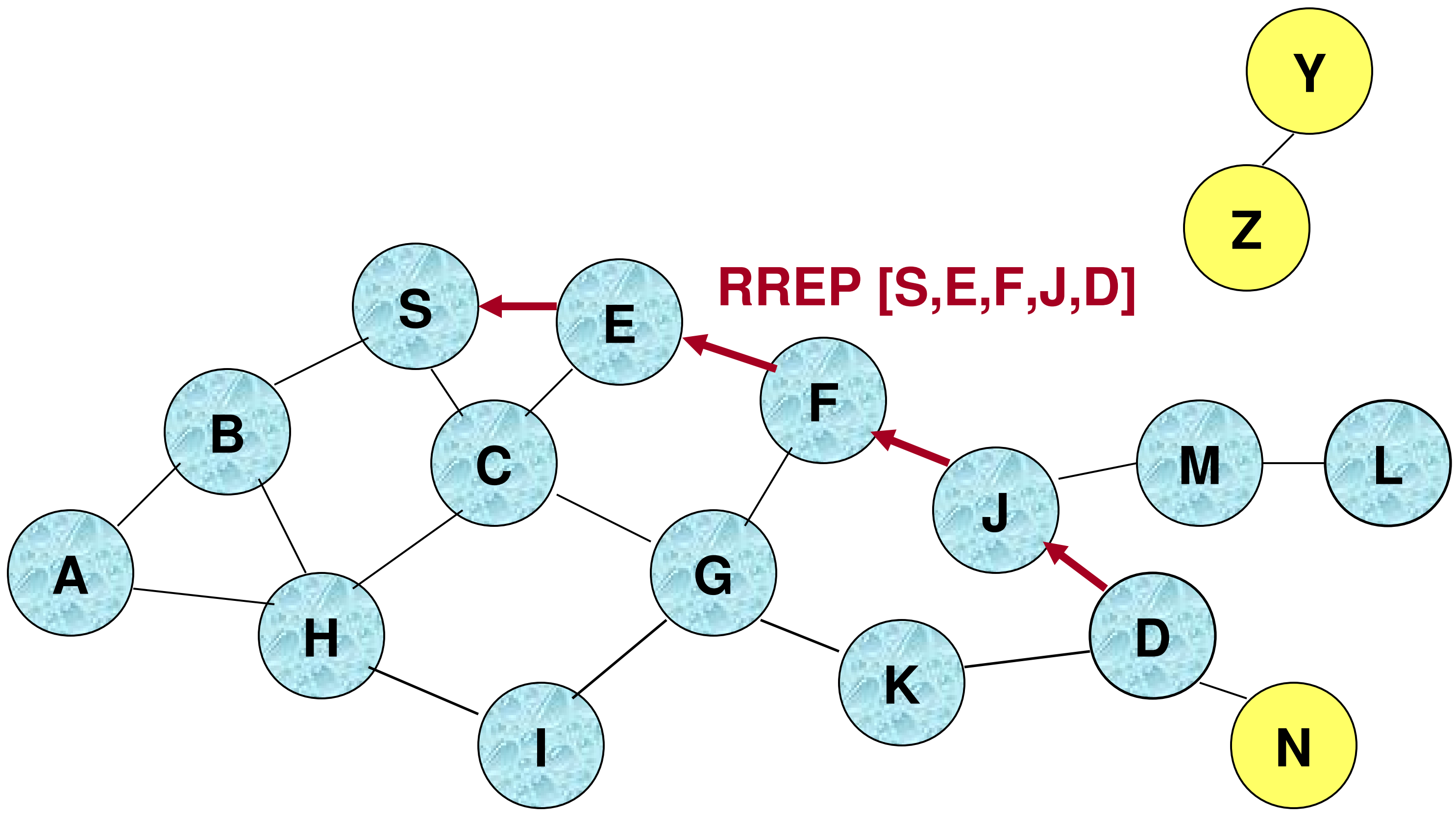
- **Nodes J and K both broadcast RREQ to node D**
- **Since nodes J and K are hidden from each other, their transmissions may collide**

Route Discovery in DSR



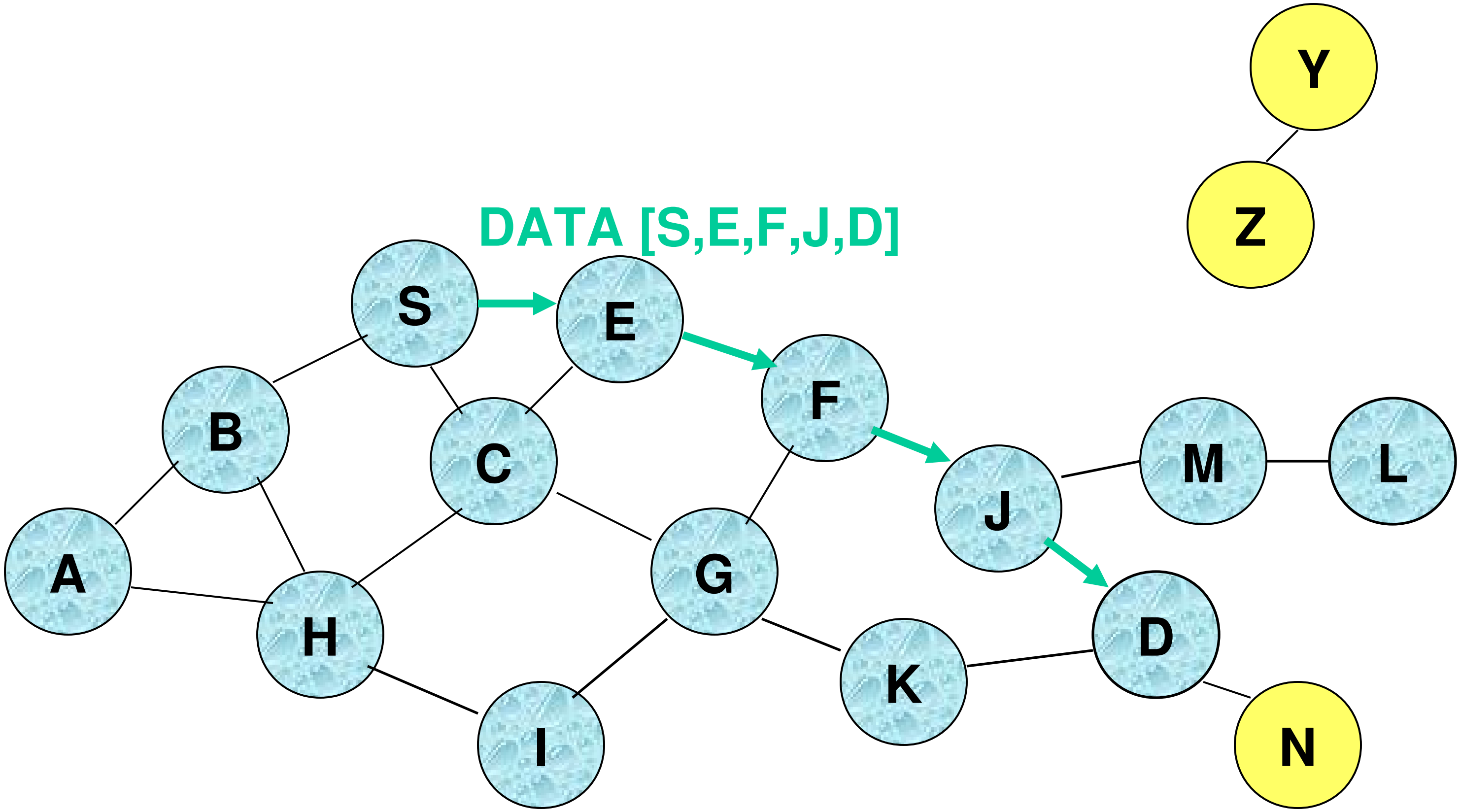
- **Node D does not forward RREQ, because node D is the intended target of the route discovery**

Route Reply in DSR



← **Represents RREP control message**

Data Delivery in DSR



Packet header size grows with route length

TCP in MANET

Several factors affect TCP in MANET:

- Wireless transmission errors
  - reducing congestion window in response to errors is unnecessary
- Multi-hop routes on shared wireless medium
  - Longer connections are at a disadvantage compared to shorter connections, because they have to contend for wireless access at each hop
- Route failures due to mobility

MANET Summary

- Routing is the most studied problem
- Interplay of layers is being researched

- Large number of simulation based expts
- Small number of field trials
- Very few reported deployments

- Fertile area for imaginative applications
  - Standardizing protocols does not seem to be a very good idea
  - Scope for proprietary solutions with limited interop

References

- J. Schiller, “Mobile Communications”, Addison Wesley, 2000
- 802.11 Wireless LAN, IEEE standards, www.ieee.org
- Mobile IP, RFC 2002, RFC 334, www.ietf.org
- TCP over wireless, RFC 3150, RFC 3155, RFC 3449
- A. Mehrotra, “GSM system engineering”, Artech House, 1997
- Bettstetter, Vogel and Eberspacher, “GPRS: Architecture, Protocols and Air Interface”, IEEE Communications Survey 1999, 3(3).
- M.v.d. Heijden, M. Taylor. “Understanding WAP”, Artech House, 2000
- Mobile Ad hoc networks, RFC 2501

- Others websites:
  - www.palowireless.com
  - www.gsmworld.com; www.wapforum.org
  - www.etsi.org; www.3gtoday.com

Thank You

Other Tutorials at: www.it.iitb.ac.in/~sri

Contact Details:

Sridhar Iyer
School of Information Technology
IIT Bombay, Powai, Mumbai 400 076
Phone: +91-22-2576-7901
Email: sri@it.iitb.ac.in