Wireless LANs: 802.11 and Mobile IP

Sridhar Iyer

Leena Chandran-Wadia

K R School of Information Technology

IIT Bombay

{sri, leena}@it.iitb.ac.in

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

Outline

- Overview of wireless networks
  - Single-hop wireless: Cellular, Wireless LANs (WLANs)
  - multiple wireless hops – Mobile ad hoc networks (MANETS)
- Challenges of wireless communications
- IEEE 802.11
  - spread spectrum and physical layer specification
  - MAC functional specification: DCF mode
    - role in WLANs – infrastructure networks
    - role in MANETs
  - MAC functional specification: PCF mode
- Mobile IPv4
- Mobile IPv6

References

- http://standards.ieee.org/getieee802/802.11.html IEEE Computer Society 1999, Wireless LAN MAC and PHY layer specification
- J. Schiller, “Mobile Communications”, Addison Wesley, 1999. – several figures
- Short tutorials on 802.11 and spread spectrum by J.Zyren, A.Petrick, C.Andren http://www.intersil.com
- Mobile IPv4 – RFC 3344 (main)
- IPv6 and Mobile IPv6
  - many RFCs, Internet drafts
  - http://www.iprg.nokia.com/~charliep/

Overview of wireless networks

Wireless networks

- Access computing/communication services, on the move

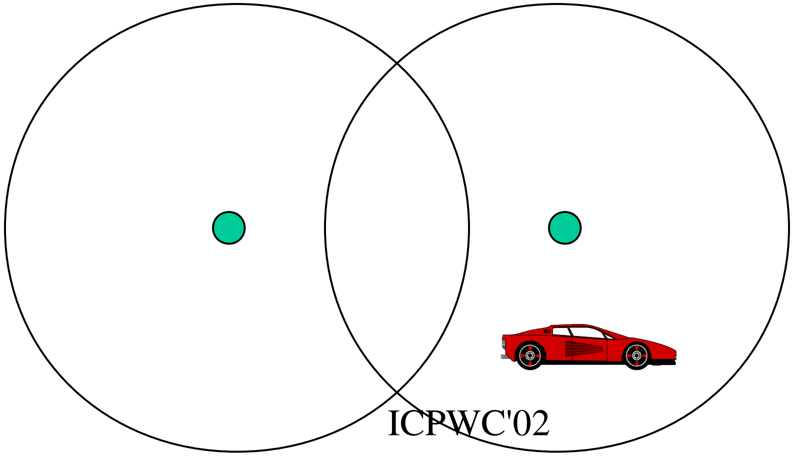
- Cellular Networks
  - traditional base station infrastructure systems

- 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)

- Multihop Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - military applications, rescue, home networking

Cellular Wireless

- Single hop wireless connectivity to the wired world
  - Space divided into cells, and hosts assigned to a cell
  - A base station is responsible for communicating with hosts/nodes in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station



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

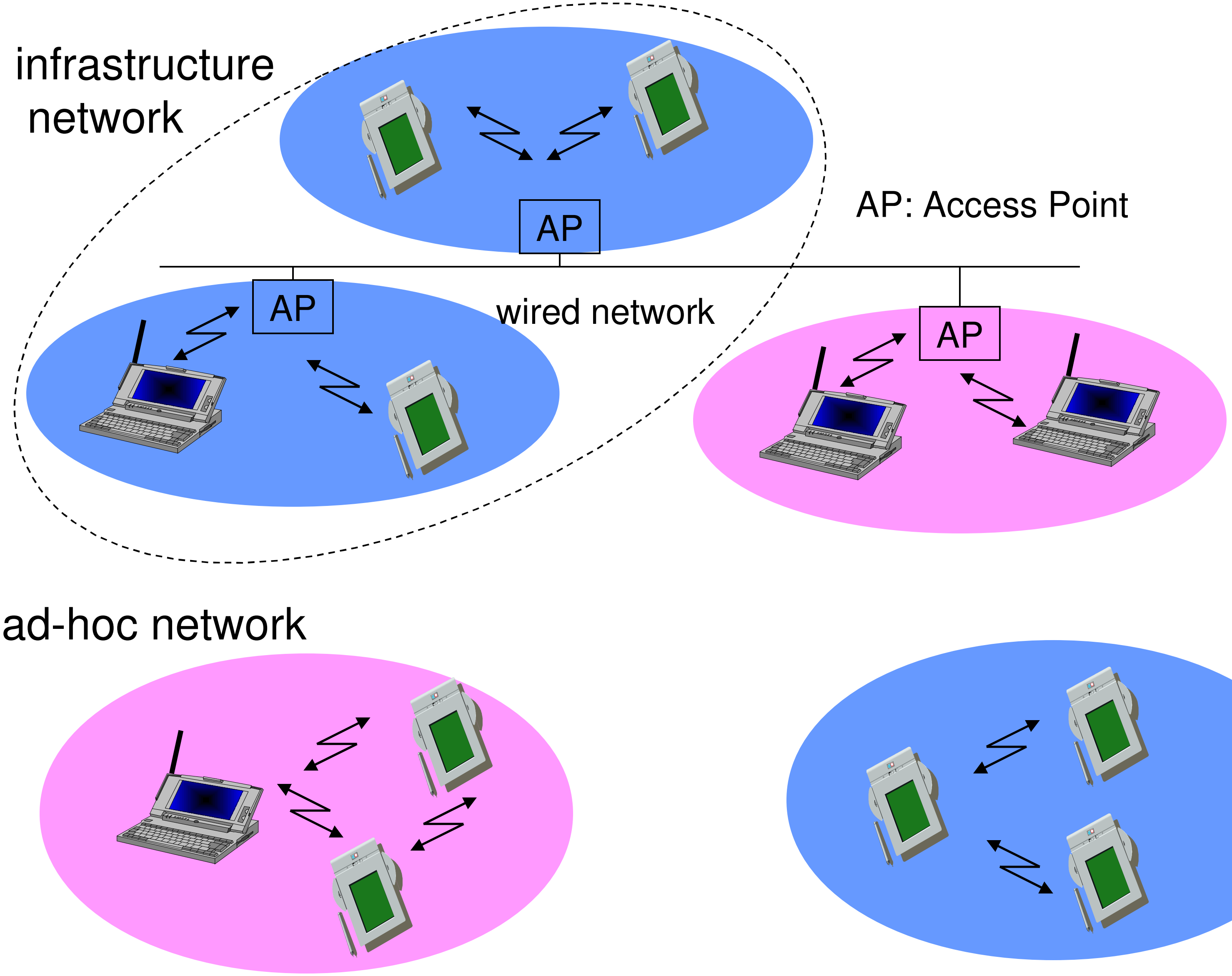
Wireless LANs

- 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
    - Bluetooth, HiperLAN and IEEE 802.11

Wireless LANs vs. Wired LANs

- 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

Infrastructure vs. Ad hoc WLANs



infrastructure network

AP

AP

wired network

AP

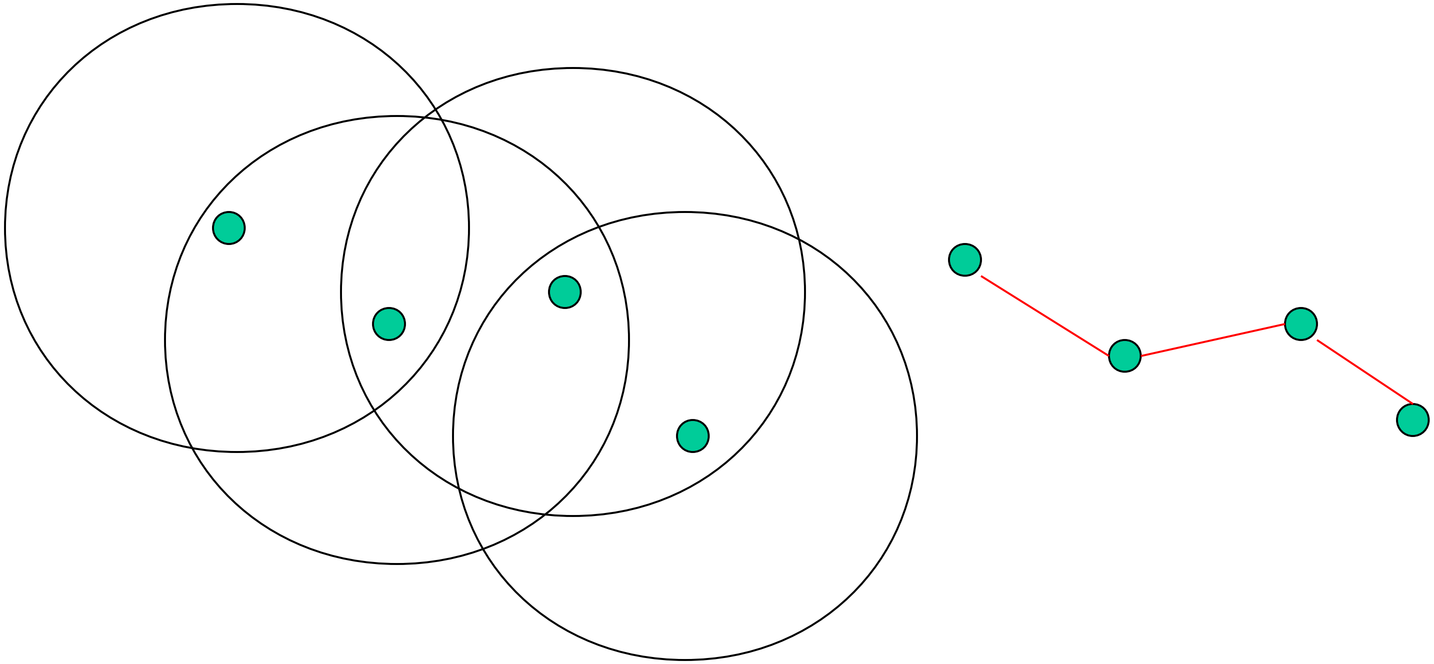
AP: Access Point

ad-hoc network

Source: Schiller

Multi-Hop Wireless

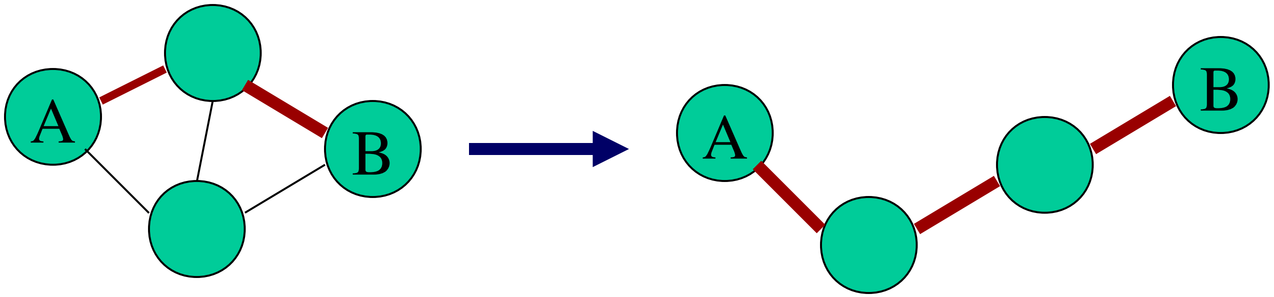
- May need to traverse multiple links to reach destination



- Mobility causes route changes

Mobile Ad Hoc Networks (MANET)

- Do not need backbone infrastructure support
- Host movement frequent
- Topology change frequent

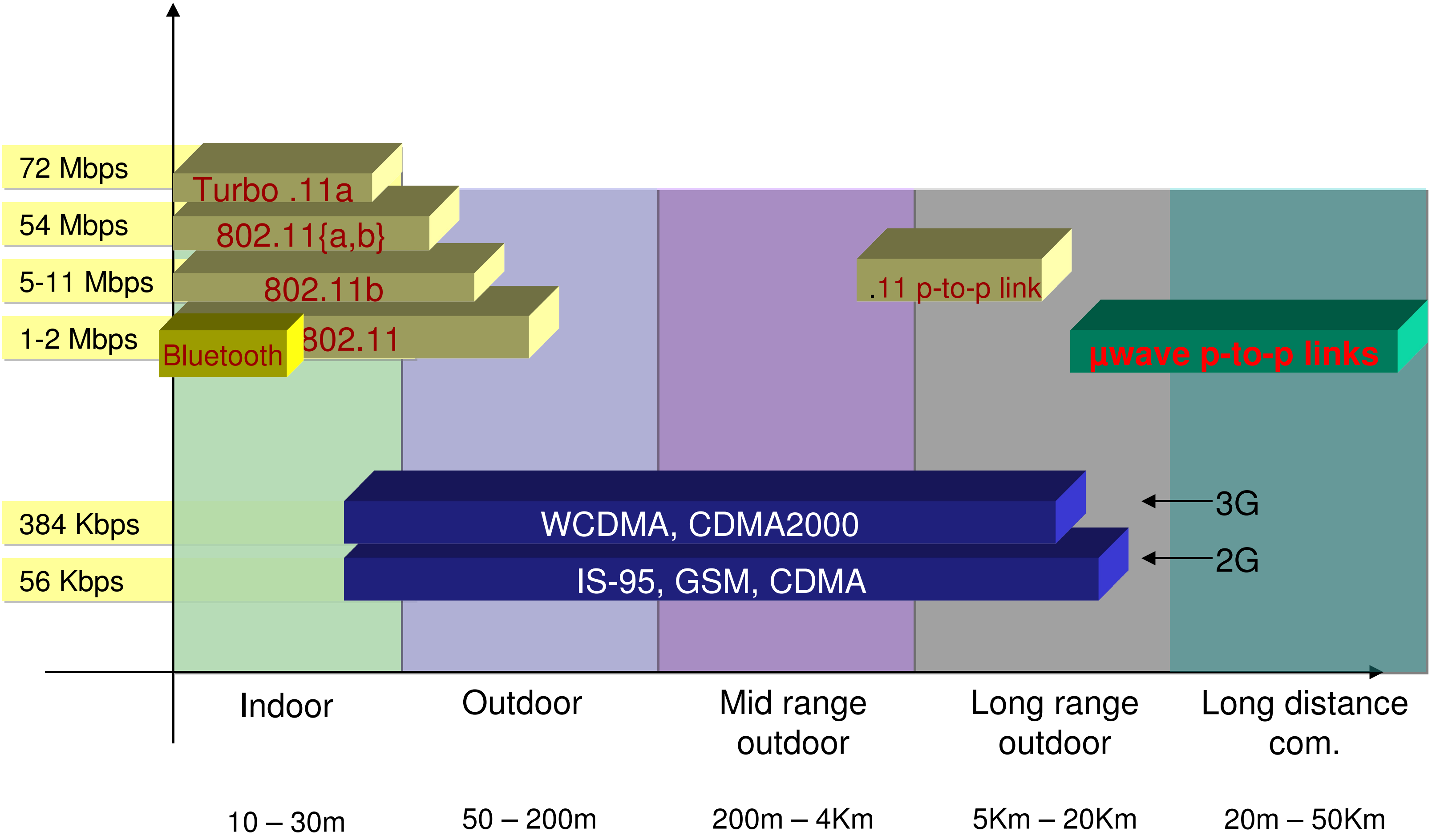


- Multi-hop wireless links
- Data must be routed via intermediate nodes

Applications of MANETS

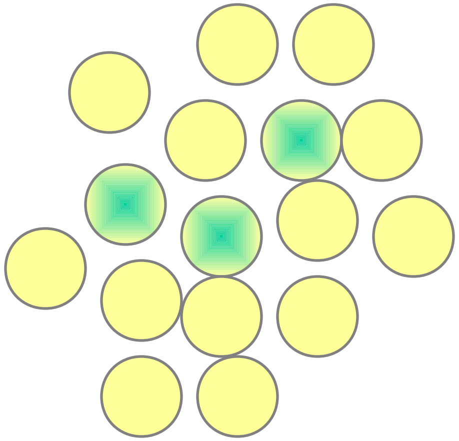
- Military - soldiers at Kargil, tanks, planes
- Disaster Management – Orissa, Gujarat
- Emergency operations – search-and-rescue, police and firefighters
- Sensor networks
- Taxicabs and other closed communities
- airports, sports stadiums etc. where two or more people meet and want to exchange documents
- Presently MANET applications use 802.11 hardware
- Personal area networks - Bluetooth

Wireless Technology Landscape

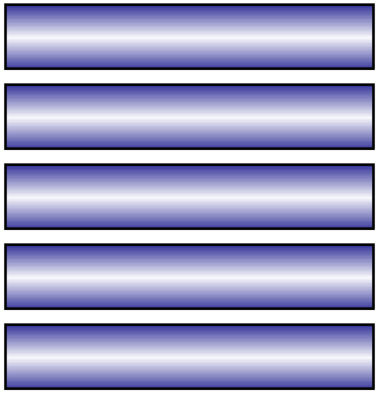


Spectrum War: Status today

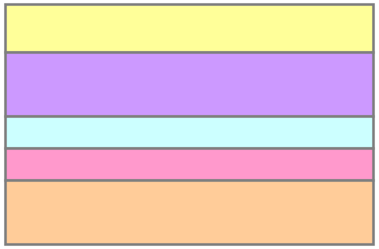
Enterprise 802.11 Network



Wireless Carrier



Public 802.11



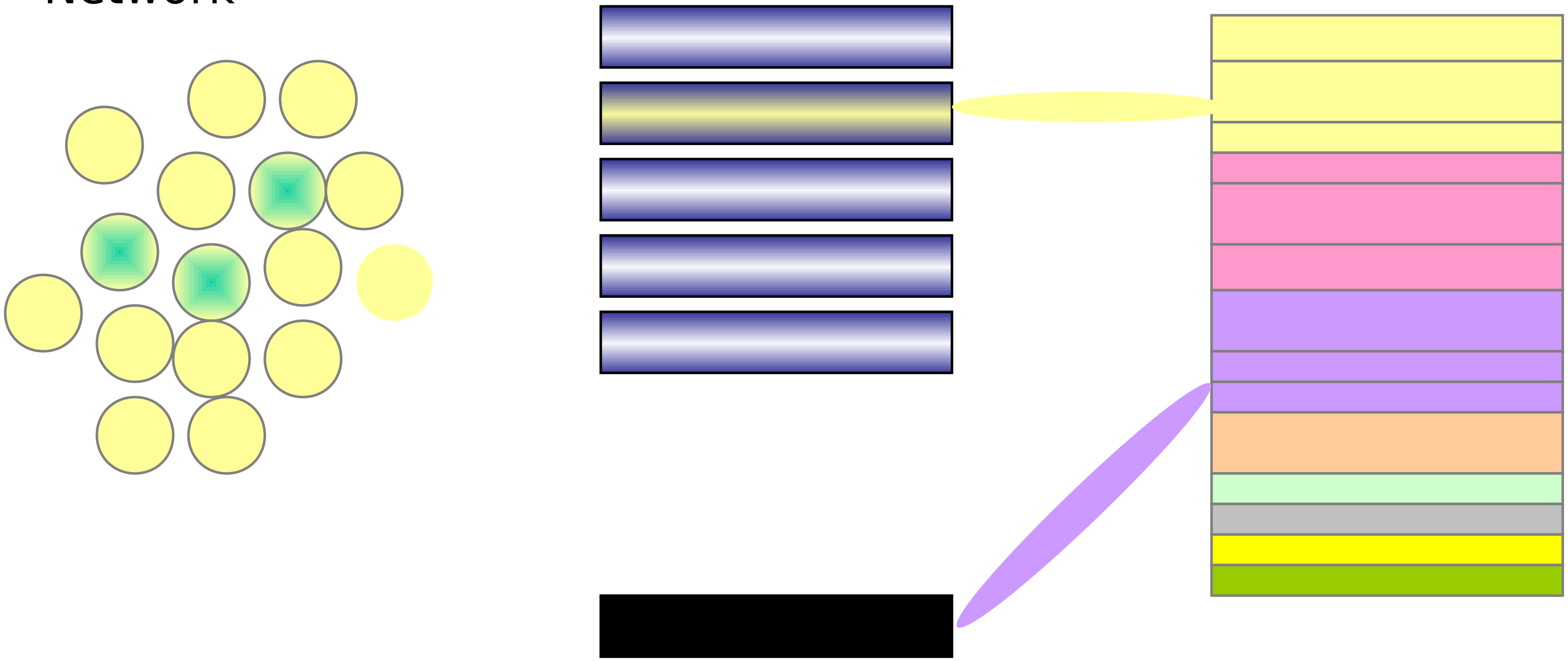
Source: Pravin Bhagwat

Spectrum War: Evolution

Enterprise 802.11 Network

Wireless Carrier

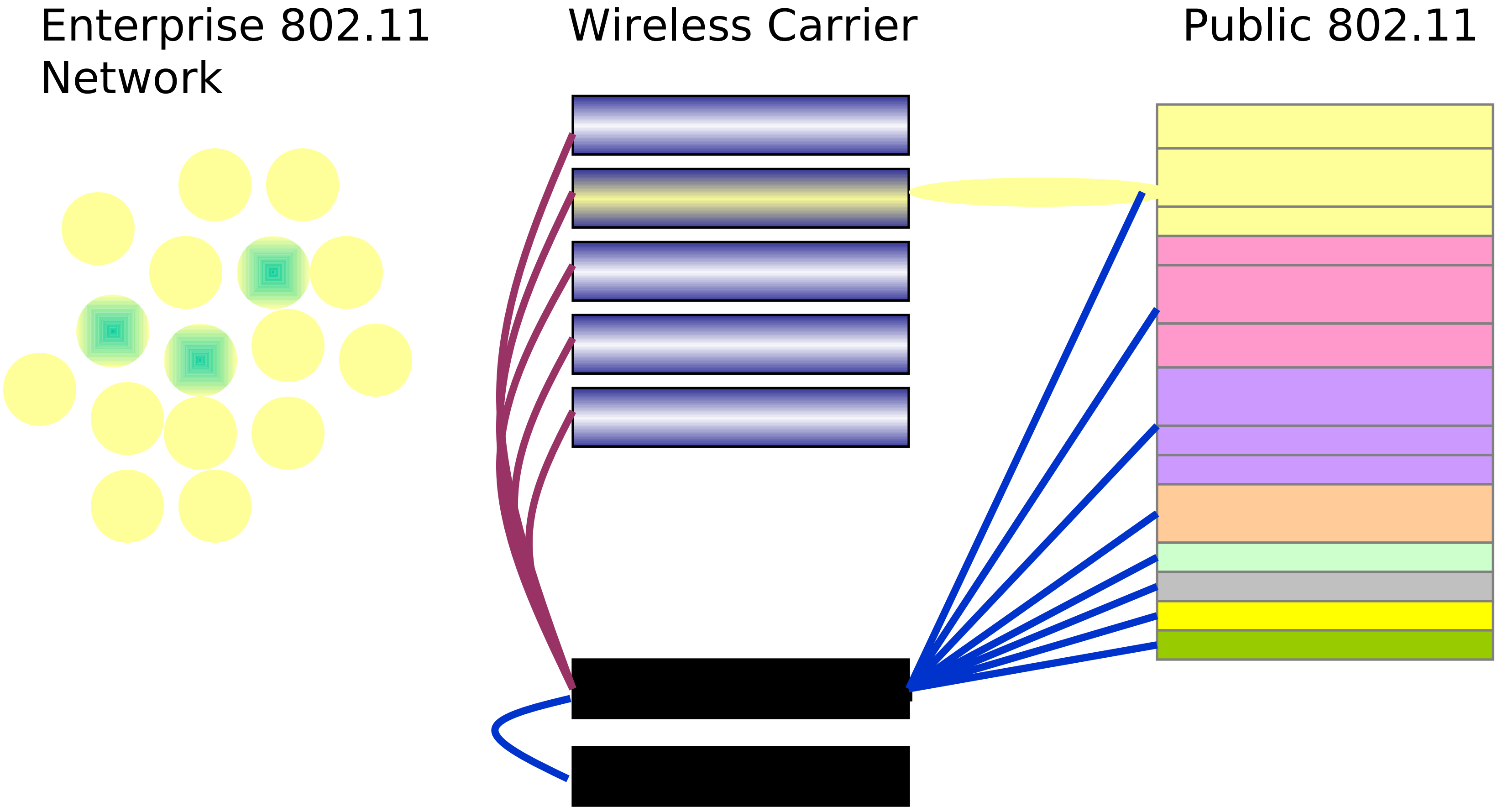
Public 802.11



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

Source: Pravin Bhagwat

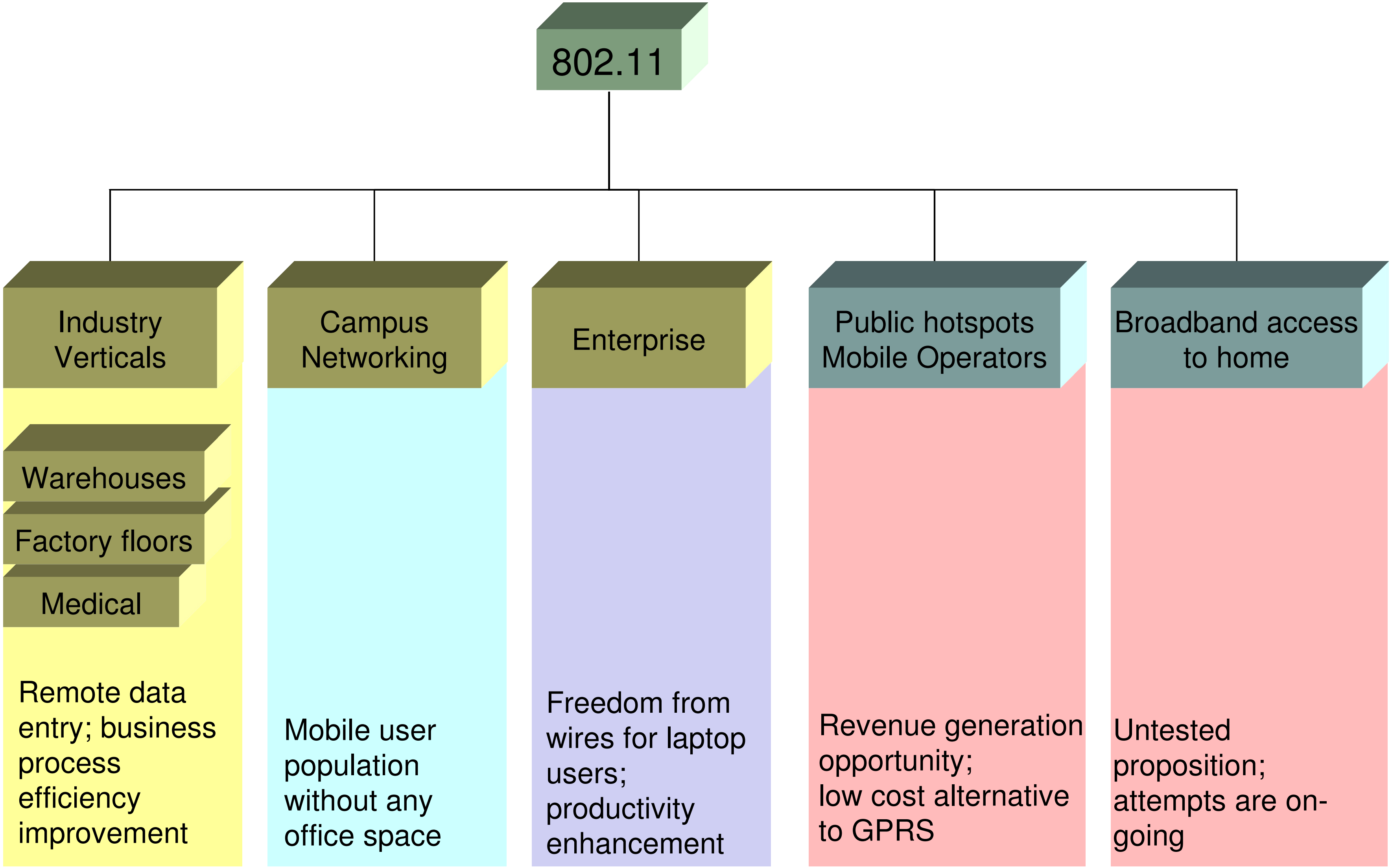
Spectrum War: Steady State



- Emergence of virtual carriers
- Roaming agreements

Source: Pravin Bhagwat

802.11 Market Evolution



802.11

Industry Verticals

Warehouses

Factory floors

Medical

Remote data entry; business process efficiency improvement

Campus Networking

Mobile user population without any office space

Enterprise

Freedom from wires for laptop users; productivity enhancement

Public hotspots Mobile Operators

Revenue generation opportunity; low cost alternative to GPRS

Broadband access to home

Untested proposition; attempts are on-going

Source: Pravin Bhagwat

Challenges of Wireless Communications

Wireless Media

- Physical layers used in wireless networks
  - have 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 the cable of a wired network
  - have dynamic topologies
  - lack full connectivity and therefore the assumption normally made that every station can hear every other station in a LAN is invalid (i.e., STAs may be "hidden" from each other)
  - have time varying and asymmetric propagation properties

Limitations of the mobile environment

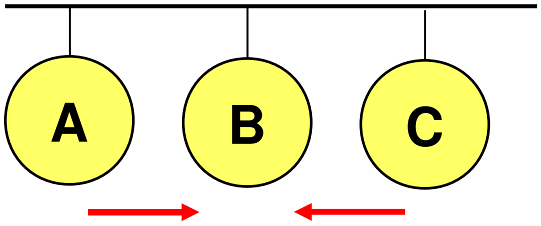
- Limitations of the Wireless Network
  - limited communication bandwidth
  - frequent disconnections
  - heterogeneity of fragmented networks
- Limitations Imposed by Mobility
  - route breakages
  - lack of mobility awareness by system/applications
- Limitations of the Mobile Device
  - short battery lifetime
  - limited capacities

Wireless v/s Wired networks

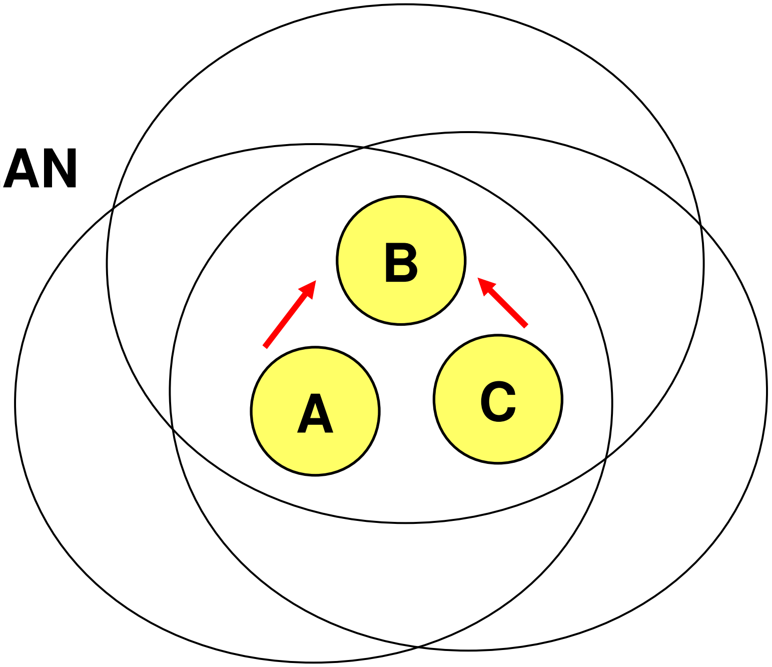
- Regulations of frequencies
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- Bandwidth and delays
  - Low transmission rates
    - few Kbps to some Mbps.
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to 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

Difference Between Wired and Wireless

Ethernet LAN

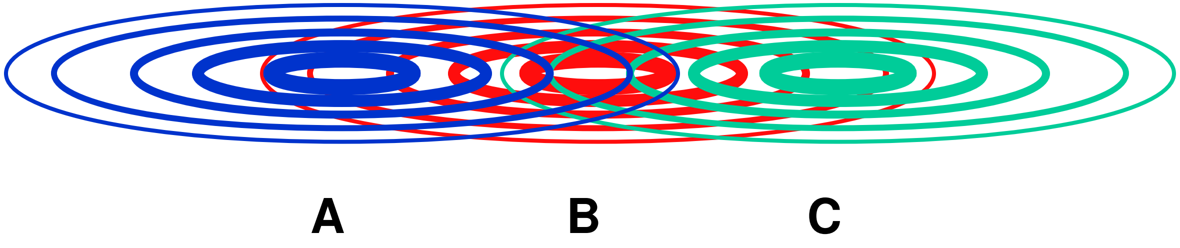


Wireless LAN



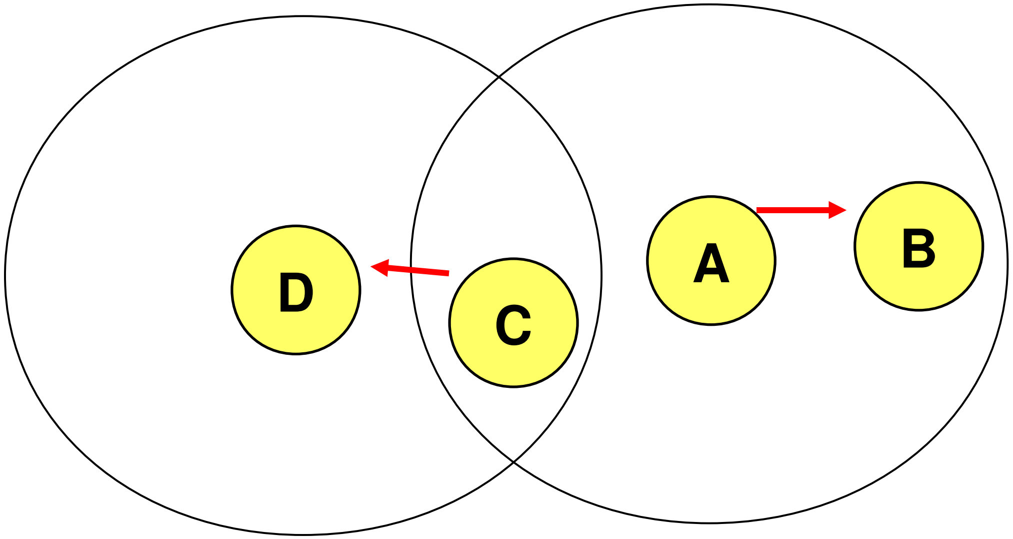
- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected at sender in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

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.

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

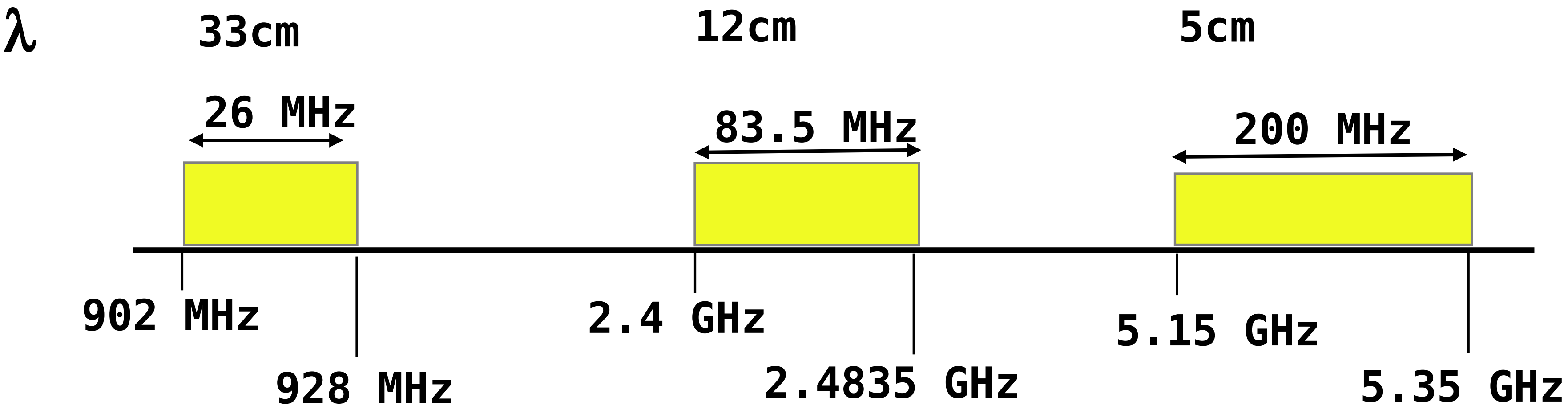
Effect of mobility on protocol stack

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

802.11-based Wireless LANs
Architecture and Physical Layer

IEEE 802.11

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



λ

33cm

12cm

5cm

26 MHz

83.5 MHz

200 MHz

902 MHz

928 MHz

2.4 GHz

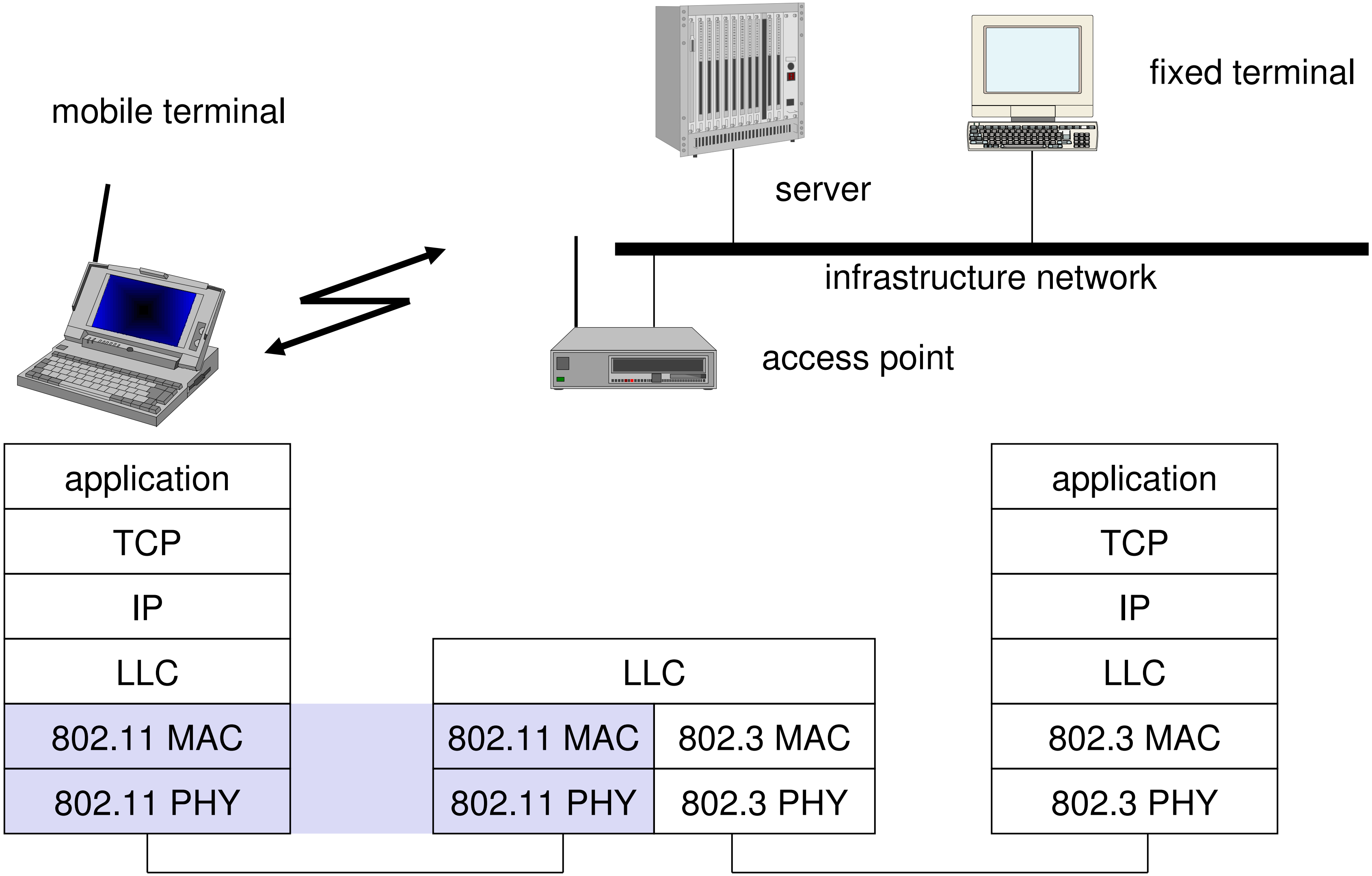
2.4835 GHz

5.15 GHz

5.35 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 Phys layer in the 5 GHz band (802.11a)

802.11- in the TCP/IP stack



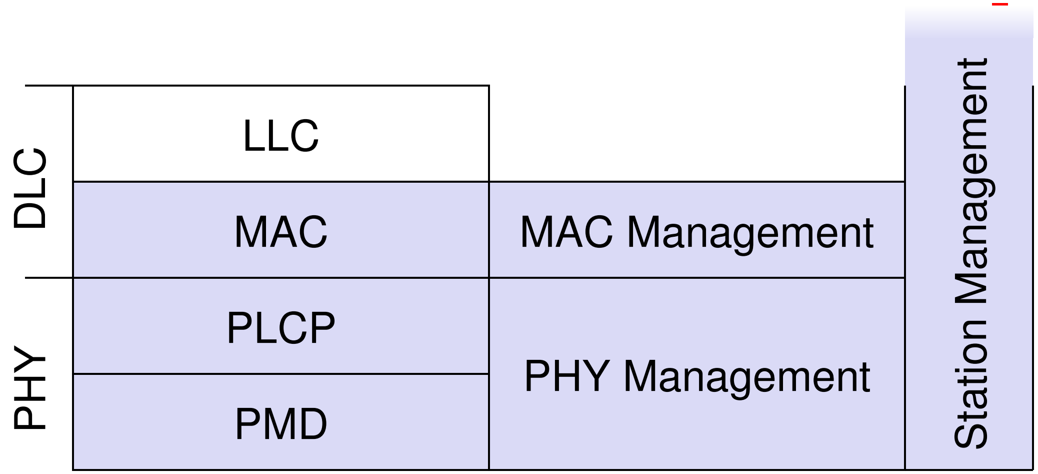
application			application
TCP			TCP
IP			IP
LLC	LLC		LLC
802.11 MAC	802.11 MAC	802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY	802.3 PHY	802.3 PHY

802.11 - Layers and functions

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

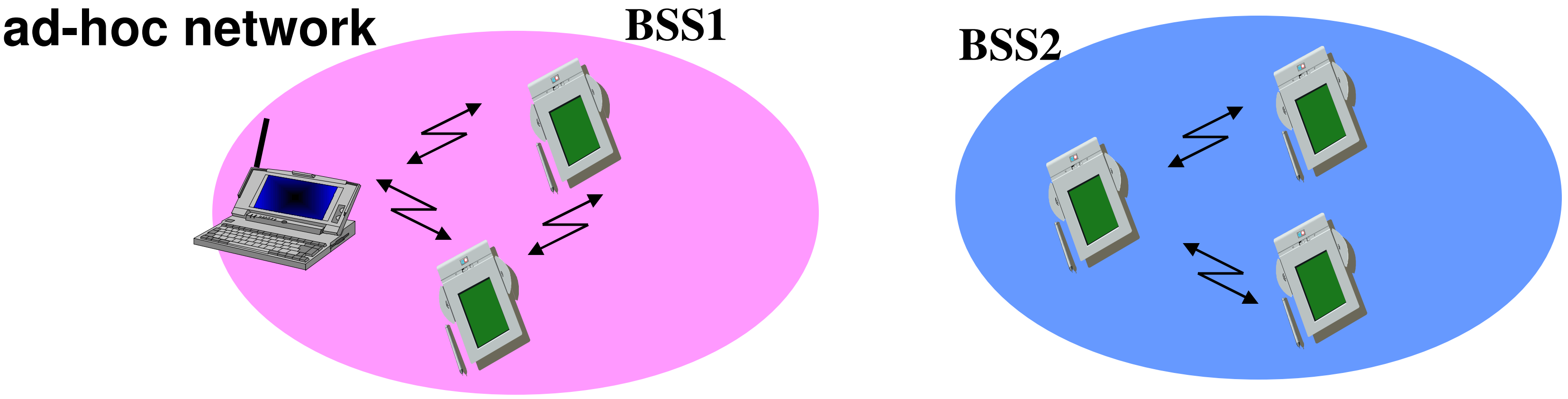
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB

Station Management
  - coordination of all management functions

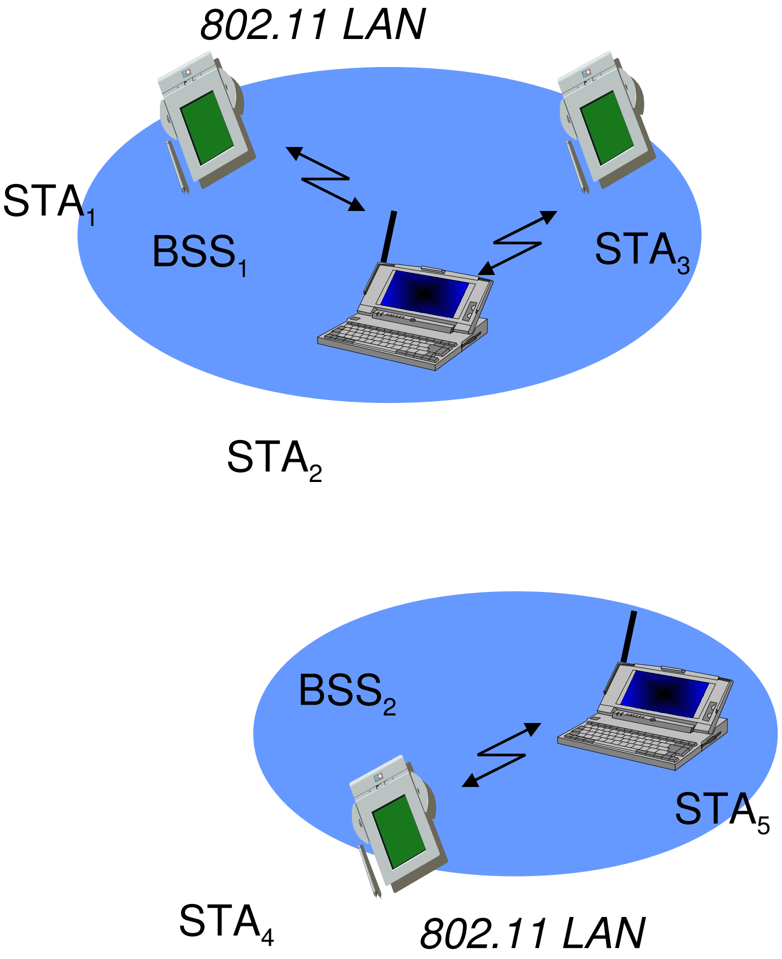


Components of IEEE 802.11 architecture

- 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



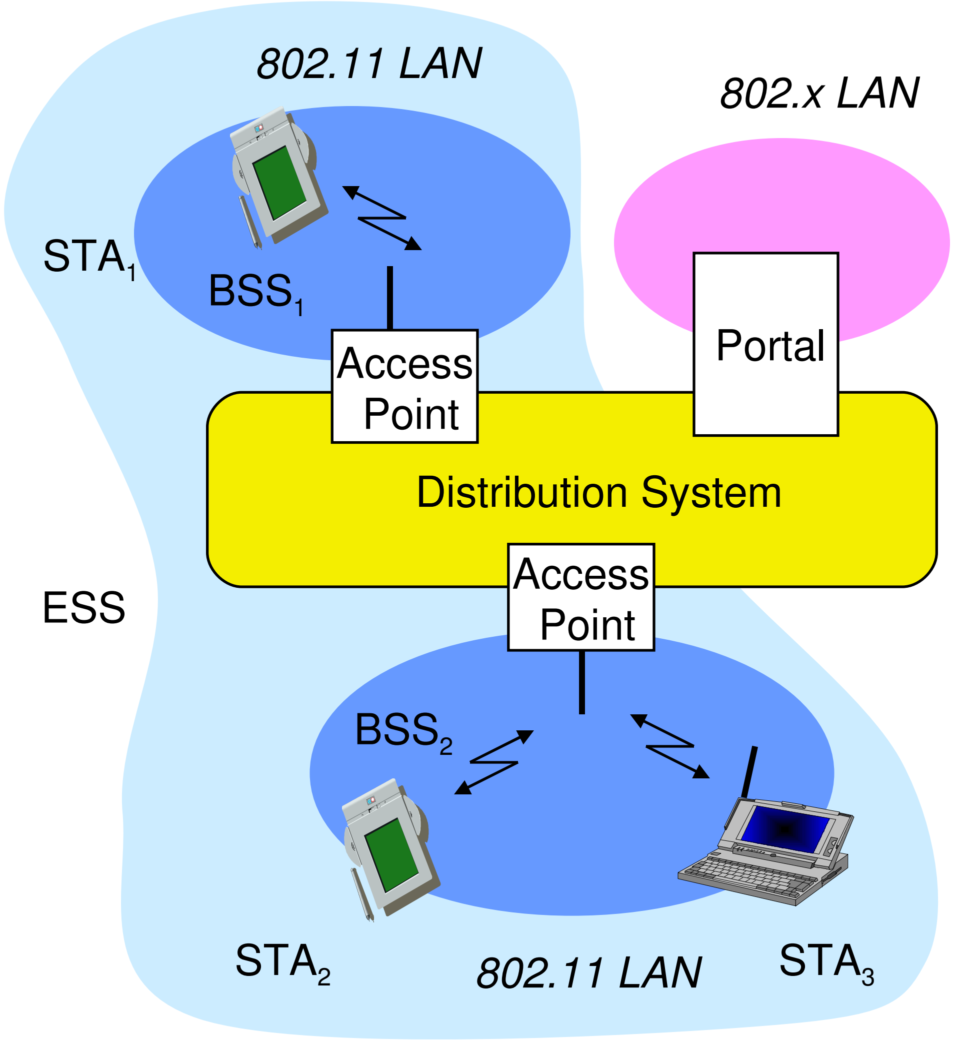
802.11 - ad-hoc network



- 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



- 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)

Extended Service Set network

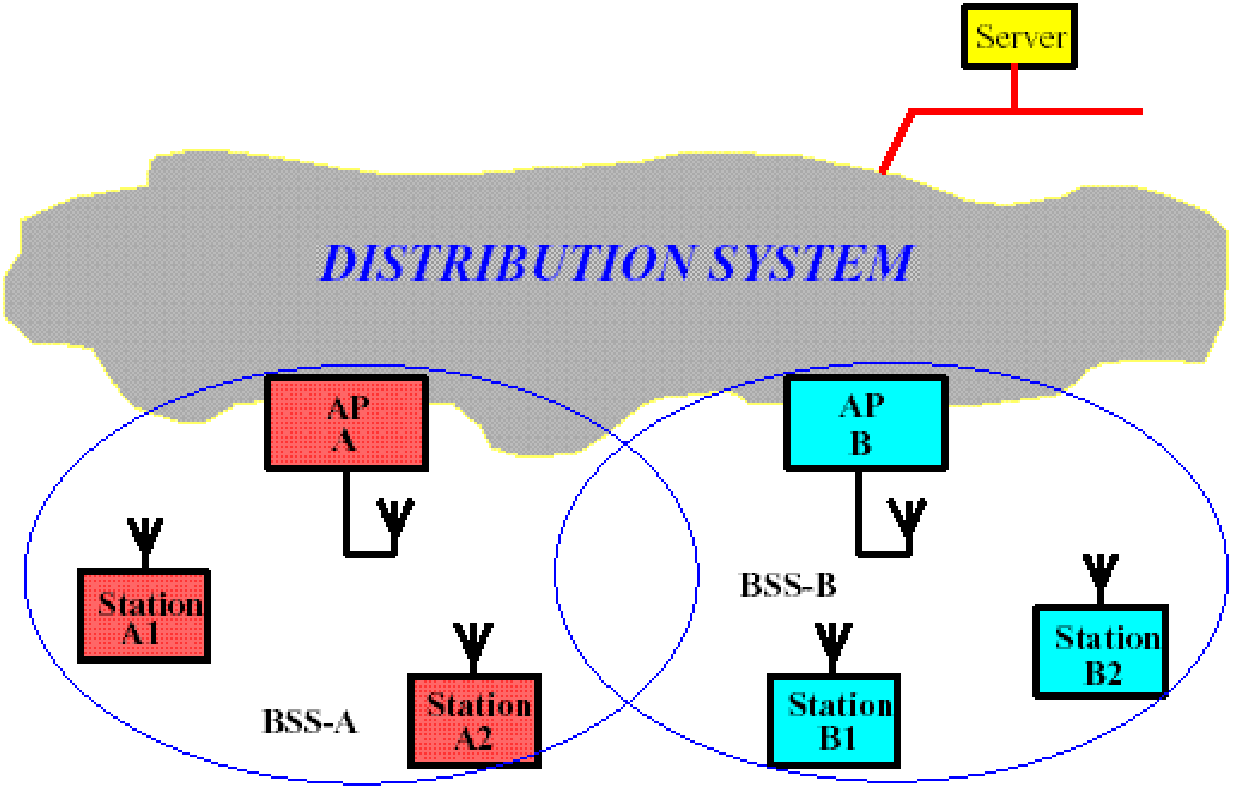


Figure 2 ESS Provides Campus-Wide Coverage

Source: Intersil

802.11 - Physical layer

- 3 versions of spread spectrum: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbps
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typically 1 Mbps
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum)
  - DBPSK modulation for 1 Mbps (Differential Binary Phase Shift Keying), DQPSK for 2 Mbps (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbps, rest of transmission 1 or 2 Mbps
  - 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, synchronization

Spread-spectrum communications

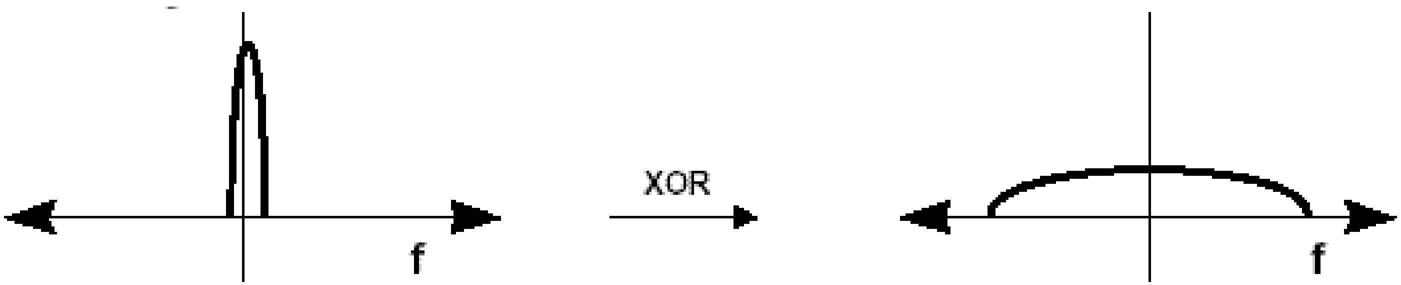


Figure 5a Effect of PN Sequence on Transmit Spectrum

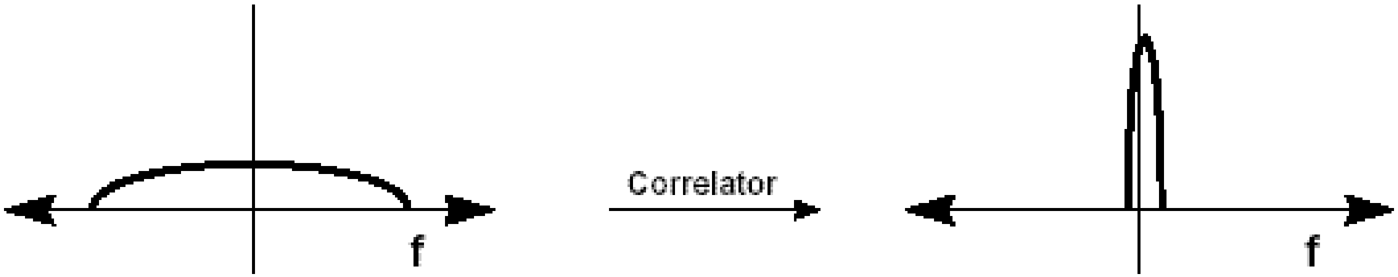
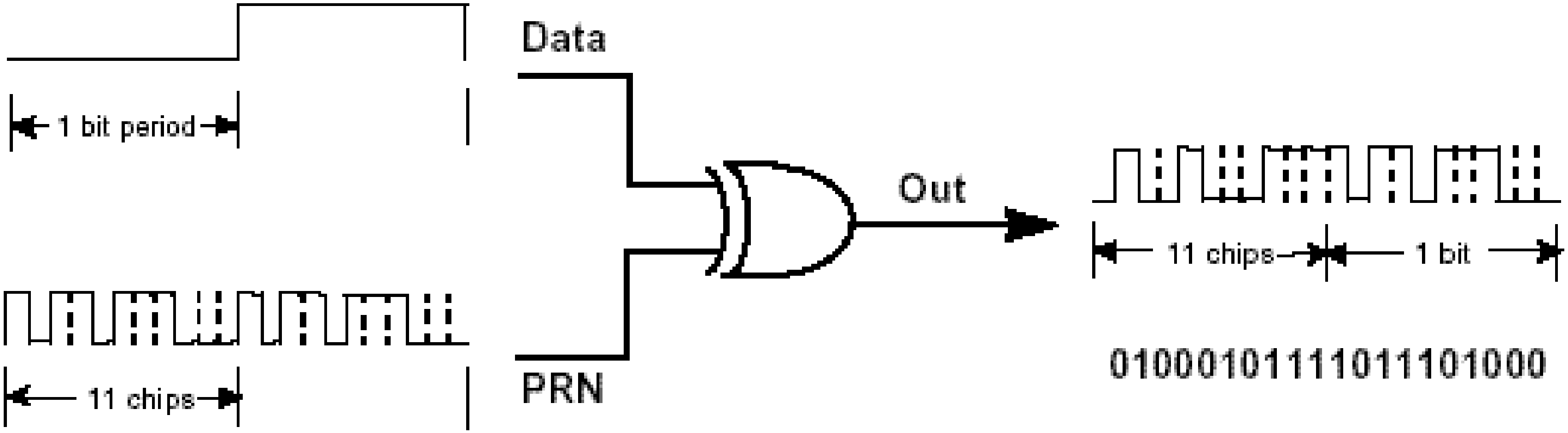


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

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

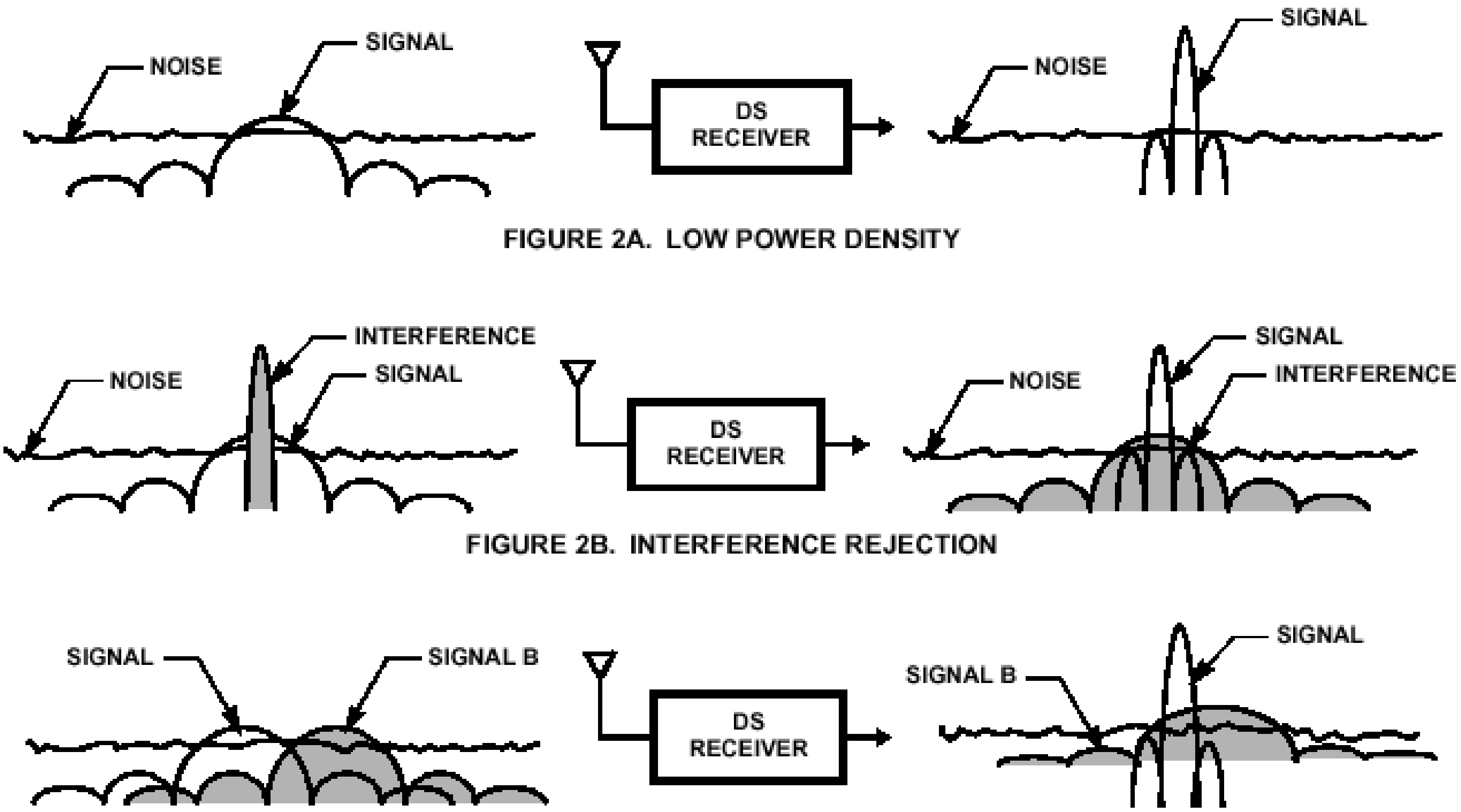


FIGURE 2A. LOW POWER DENSITY

FIGURE 2B. INTERFERENCE REJECTION

FIGURE 2C. MULTIPLE ACCESS

FIGURE 2. DIRECT SEQUENCE SPREAD SPECTRUM PROPERTIES

Source: Intersil

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
- Many others….Agere, Cisco,………

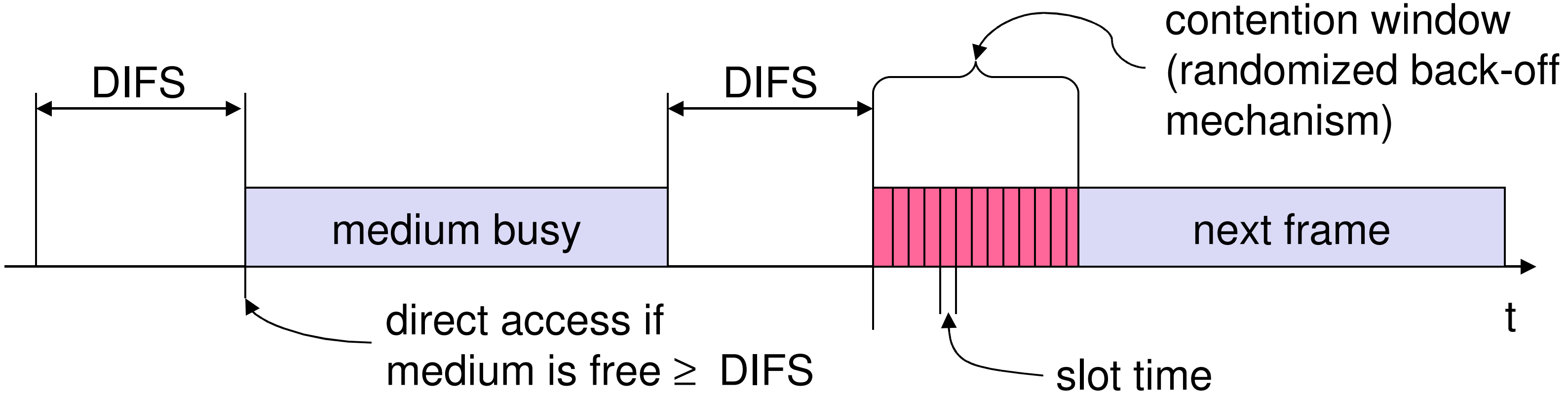
802.11-based Wireless LANs
MAC functional spec - DCF

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/exposed terminal problem, provides reliability
  - PCF (optional)
    - access point polls terminals according to a list

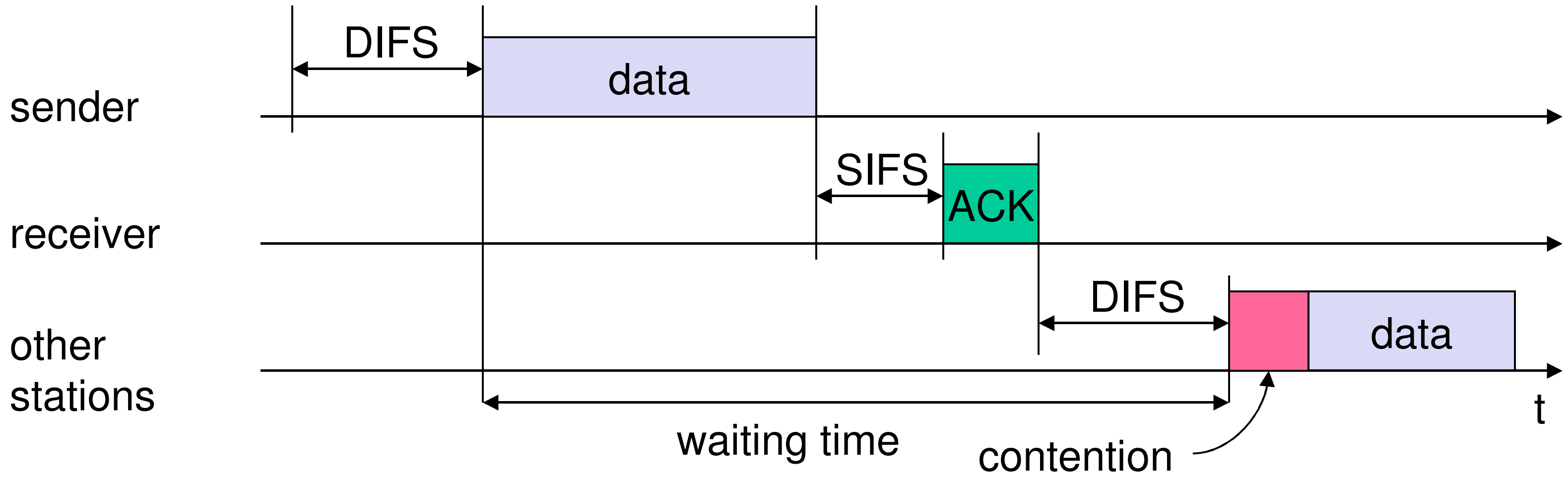
802.11 - CSMA/CA



- station which has data 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 plus an additional random back-off time (multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

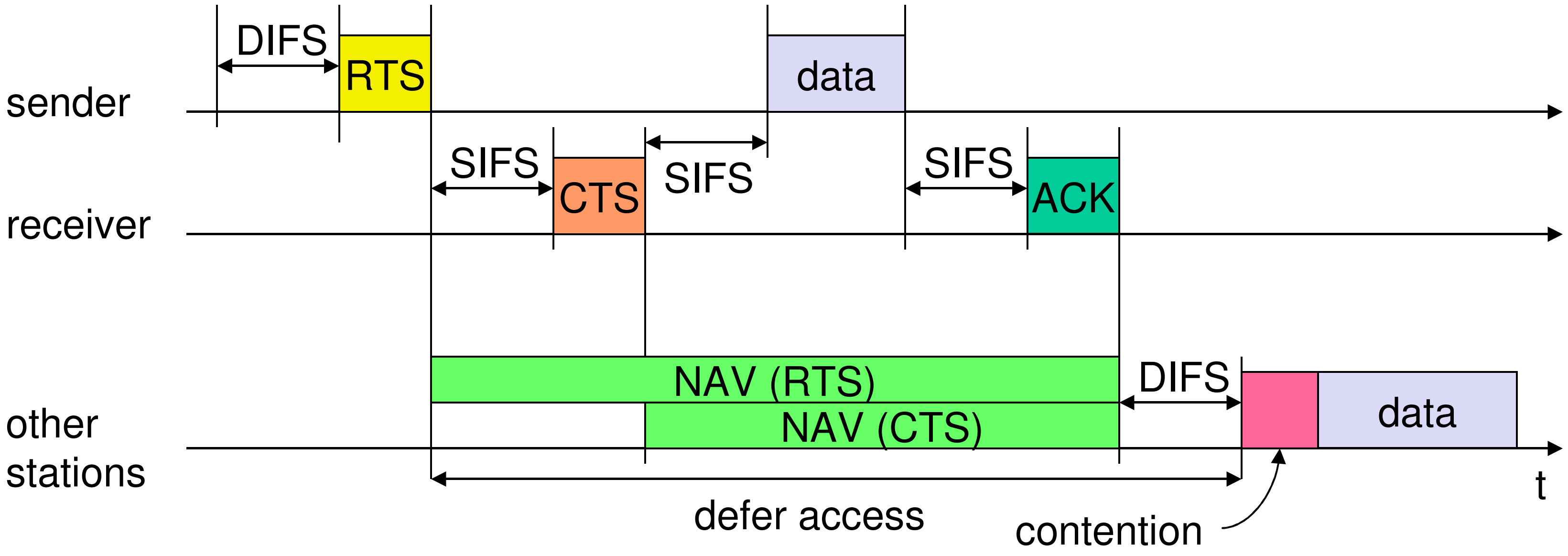
802.11 DCF – basic access

- If medium is free for DIFS time, station sends 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

- If medium is free for DIFS, station can send RTS with reservation parameter (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



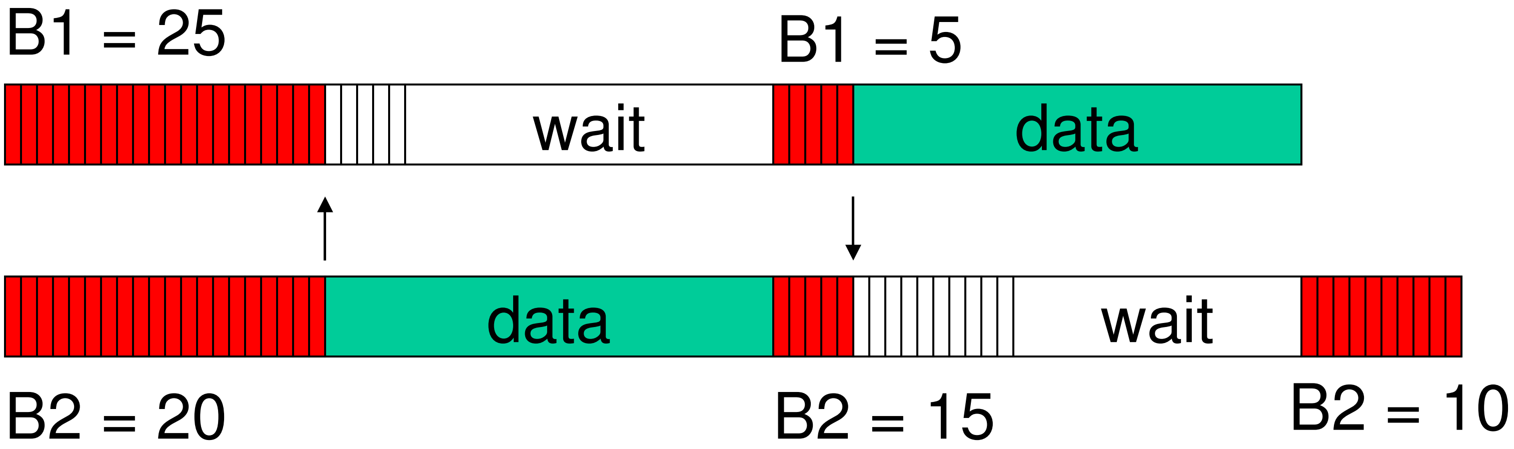
802.11 - Carrier Sensing

- **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 - Collision Avoidance

- If medium is not free during DIFS time..
- Go into Collision Avoidance: Once channel becomes idle, wait for DIFS time plus a randomly chosen backoff time before attempting to transmit
- For DCF the backoff is chosen as follows:
  - When first transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window, nominally 31
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS
  - If collision, then double the cw up to a maximum of 1024
- Time spent counting down backoff intervals is part of MAC overhead

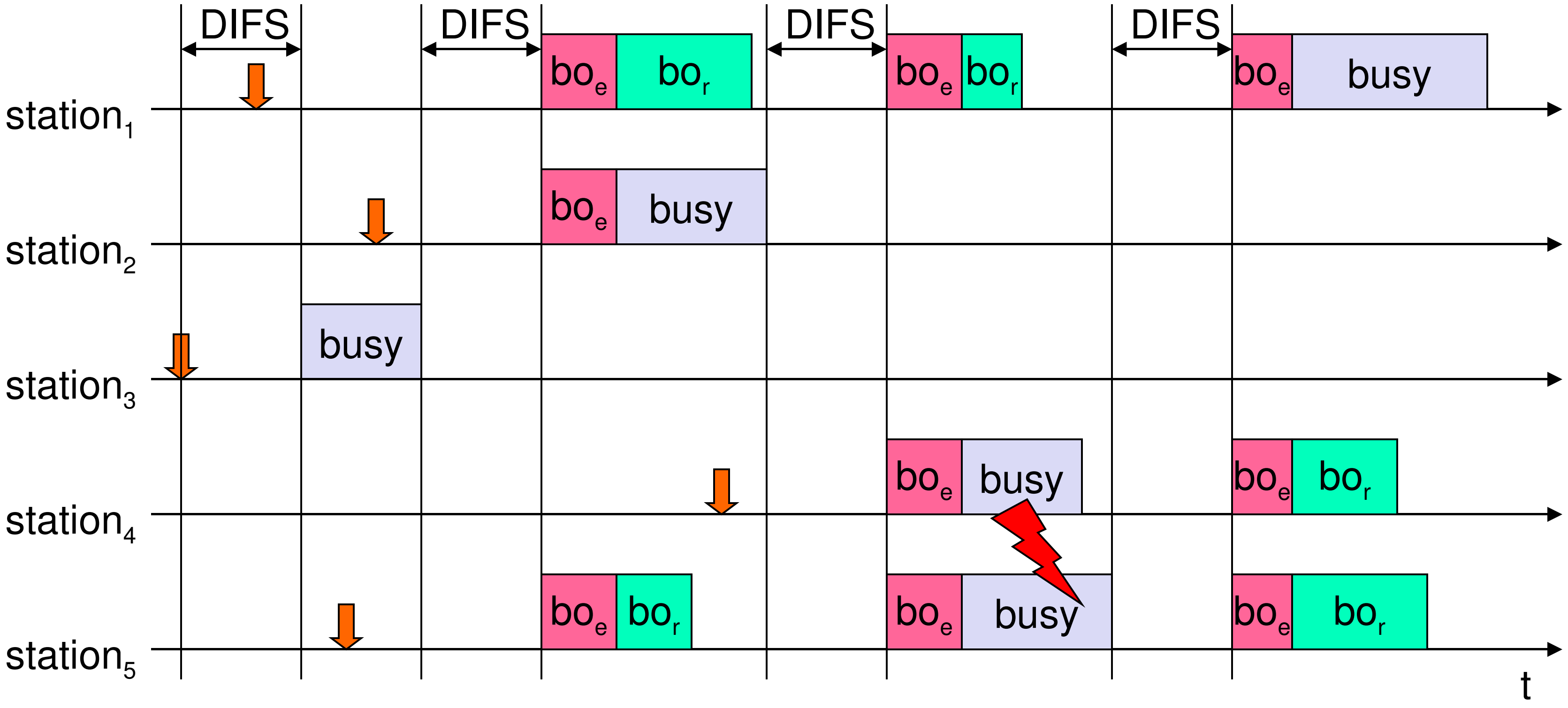
Example - backoff



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

Backoff - more complex example



busy medium not idle (frame, ack etc.)

↓ packet arrival at MAC

bo$_e$ elapsed backoff time

bo$_r$ residual backoff time

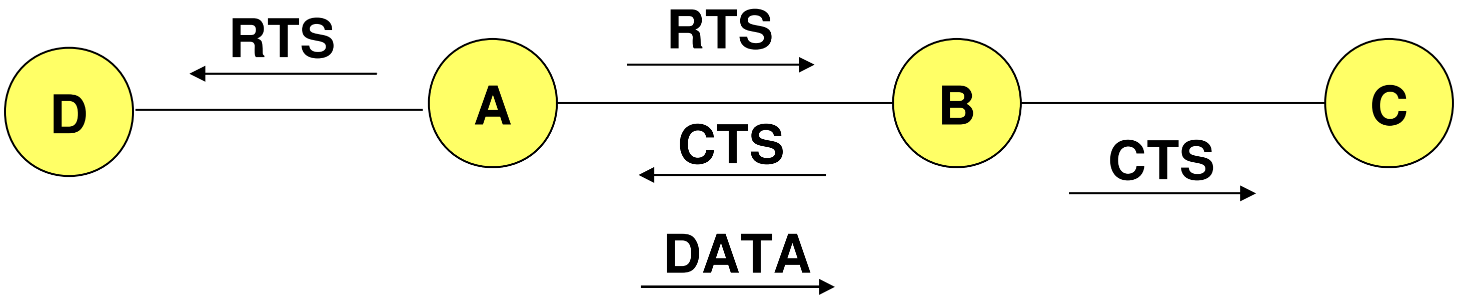
Source: Schiller

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: DIFSTime = SIFSTime + 2xSlotTime

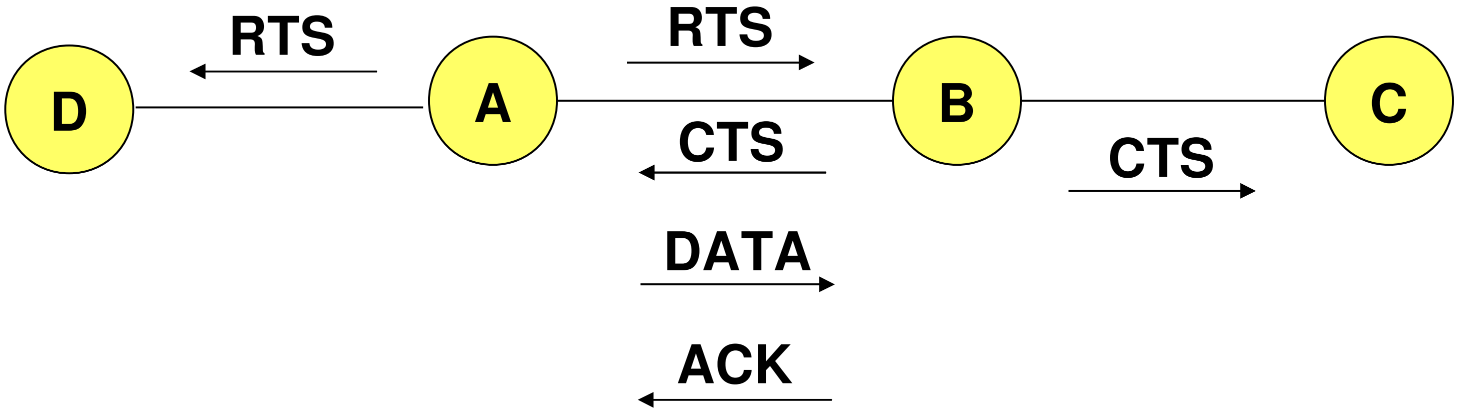
Solution to Hidden/Exposed Terminals

- 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



802.11 - Reliability

- Use 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

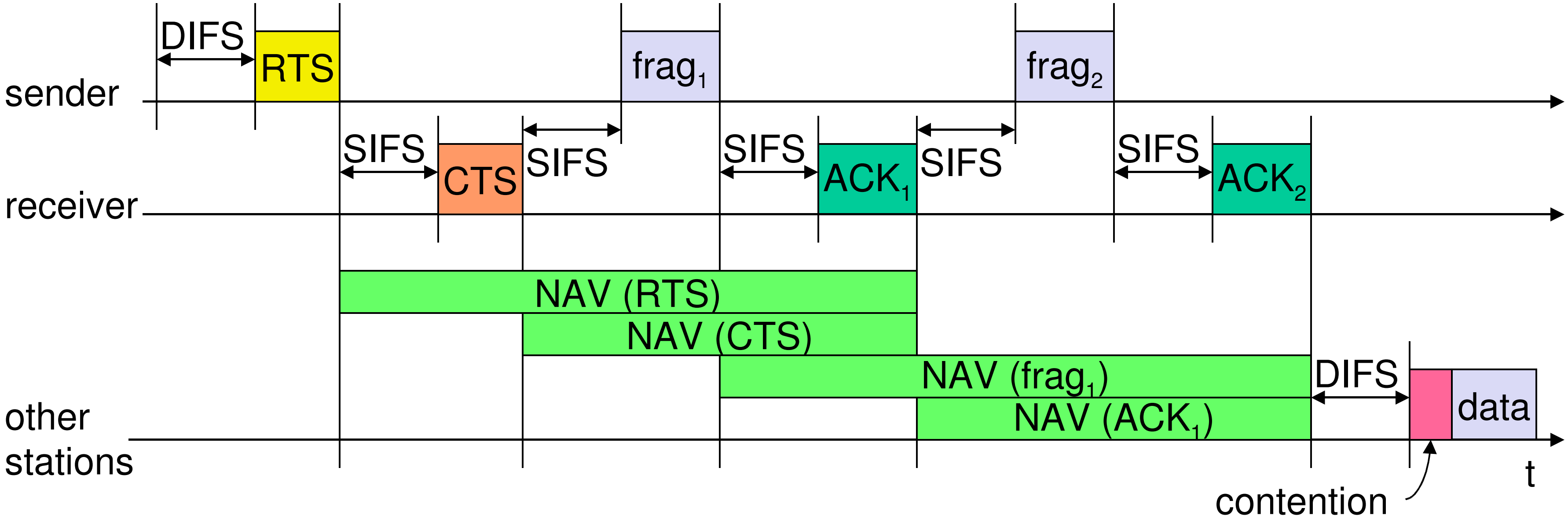


802.11 - Congestion Control

- 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 cwmax =1023)
  - Upon successful completion data transfer, restore cw to cwmin=31

Fragmentation



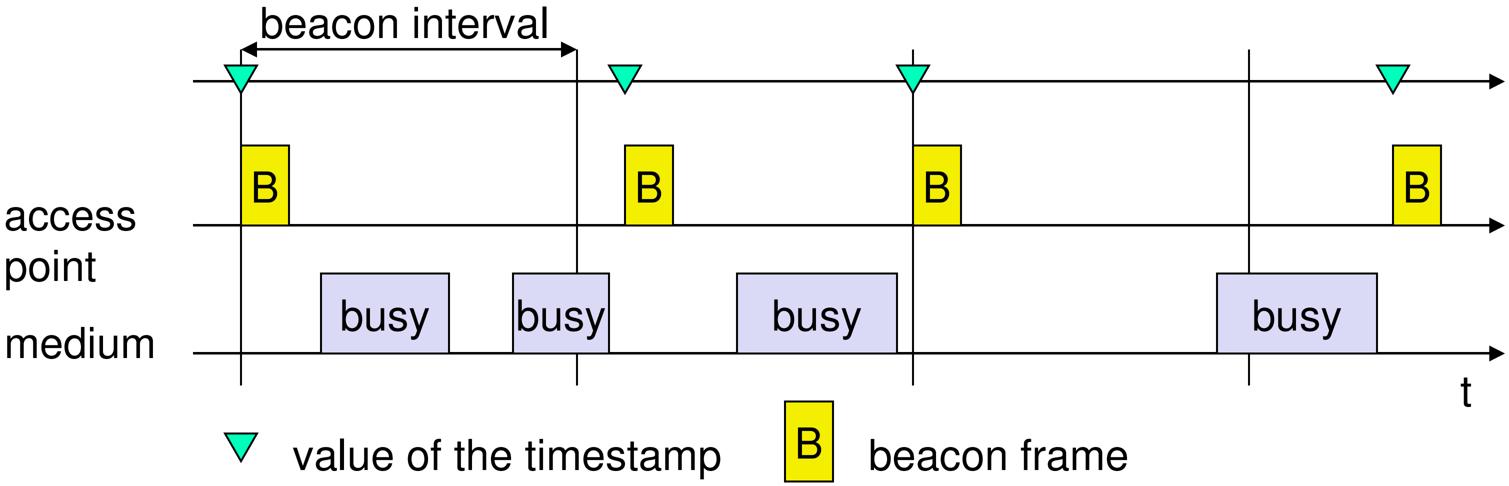
802.11 - MAC management

- 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

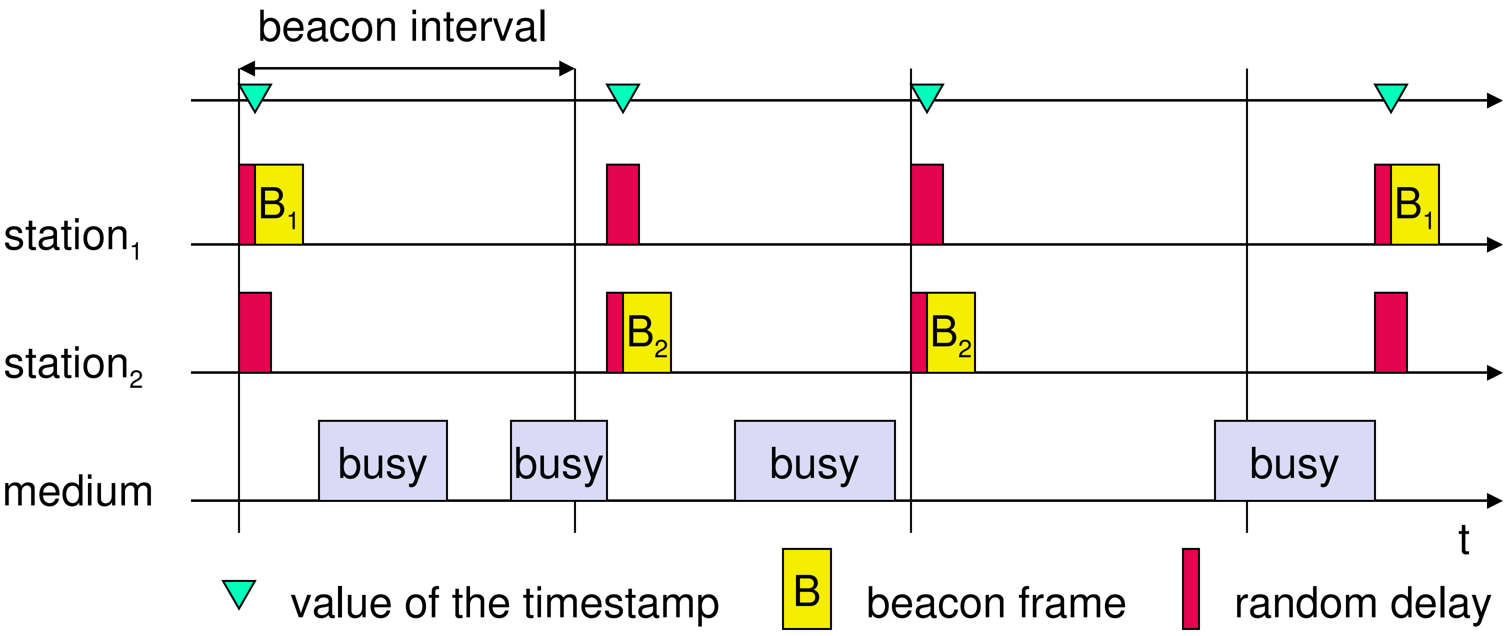
- All STAs within a BSS are synchronized to a common clock
  - Infrastructure mode: AP is the timing master
    - periodically transmits Beacon frames containing Timing Synchronization function (TSF)
    - Receiving stations accepts the timestamp value in TSF
  - Ad hoc mode: TSF implements a distributed 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 mode)



Source: Schiller

Synchronization using a Beacon (ad-hoc mode)



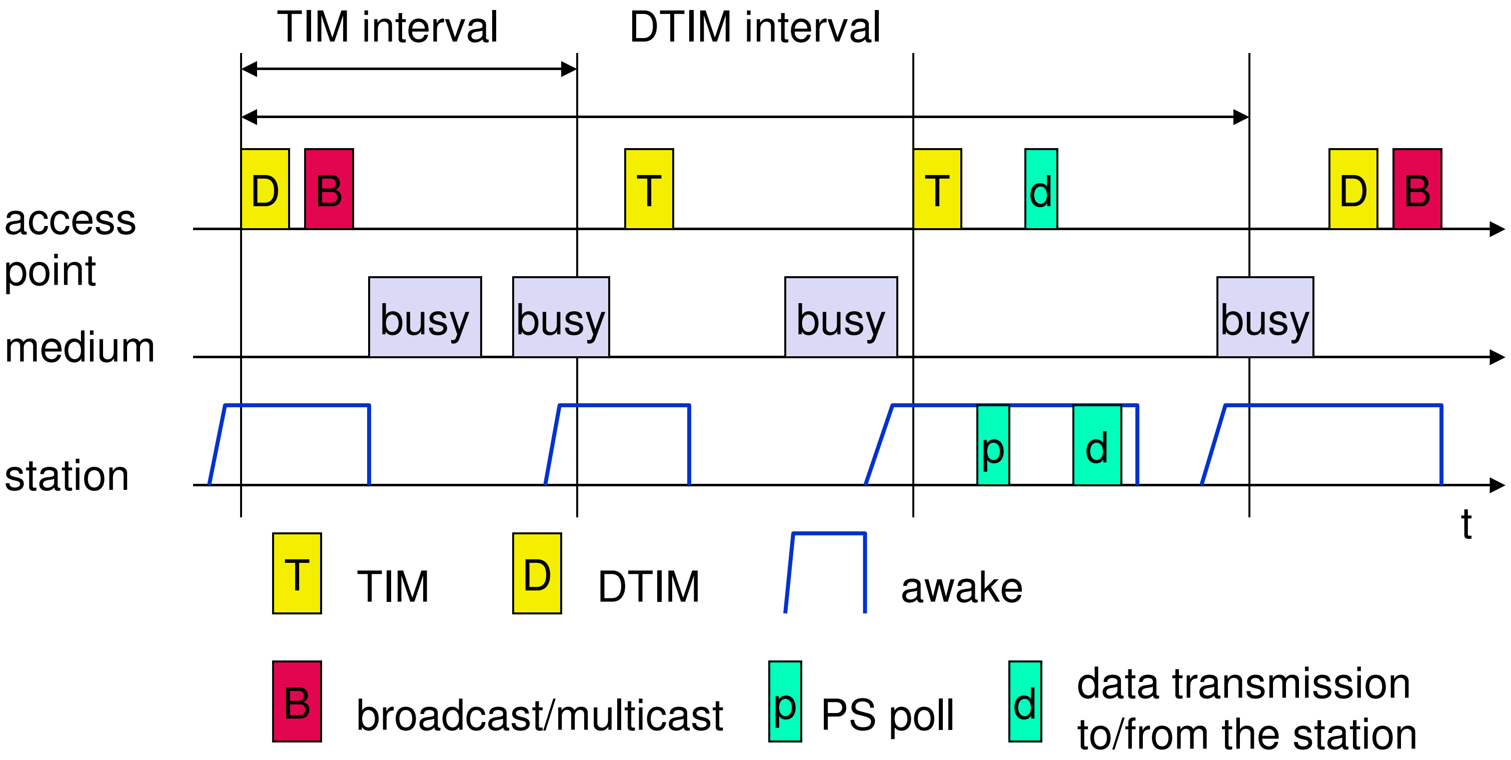
802.11 - Power management

- 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

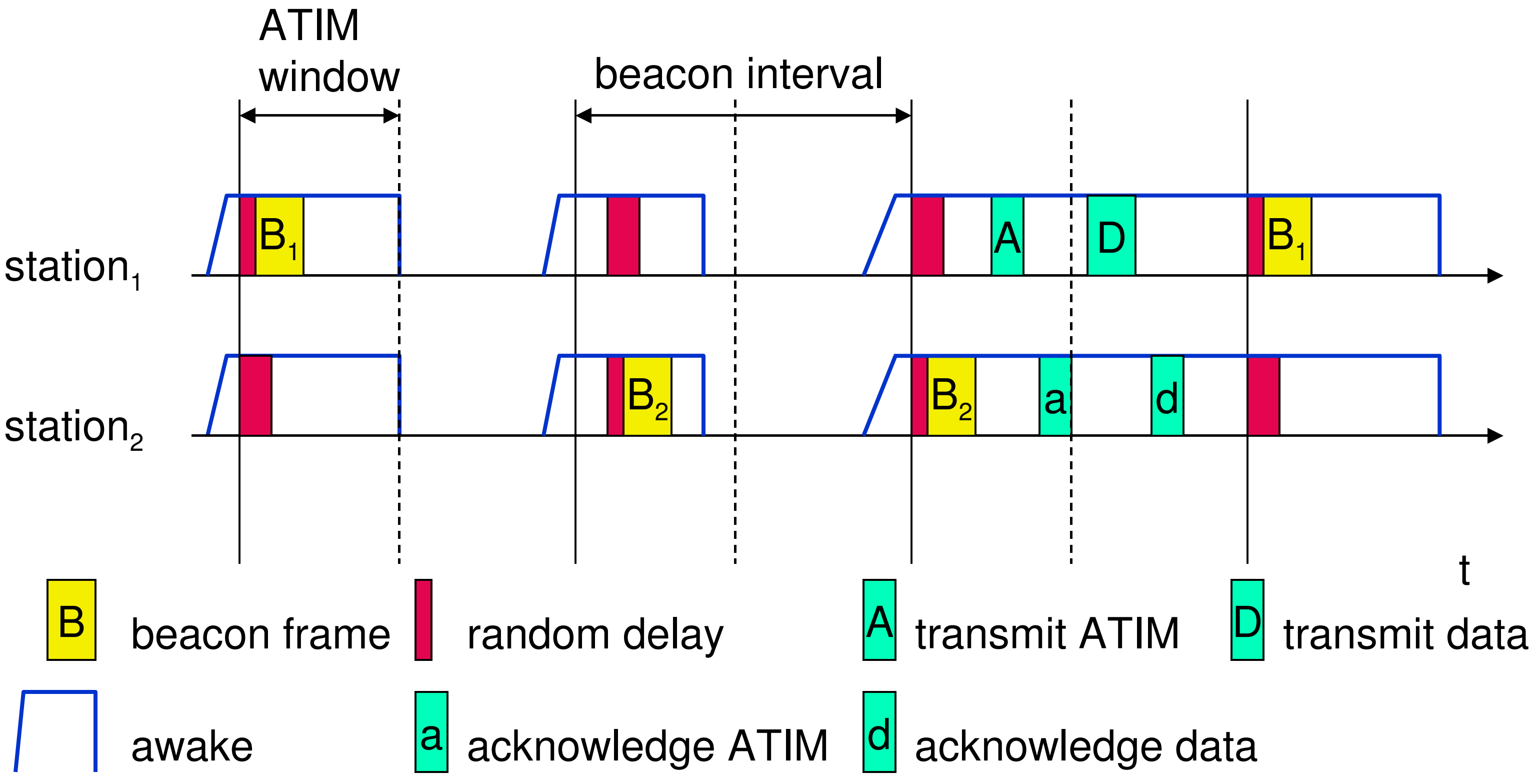
- Power Saving in infrastructure mode
  - Nodes can go into sleep or standby mode
  - An Access Point periodically transmits a beacon indicating which nodes have packets waiting for them
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a node has a packet waiting, then 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)



Source: Schiller

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



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

version, type, fragmentation, security, ...

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

802.11 - Roaming

- Bad connection in Infrastructure mode? Perform:
- scanning of environment
  - listen into the medium for beacon signals or send probes into the medium and wait for an answer
- send Reassociation Request
  - station sends a request to a new AP(s)
- receive Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request and
  - signals 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

802.11-based Wireless LANs
Point Coordination Function (PCF)

802.11 - Point Coordination Function

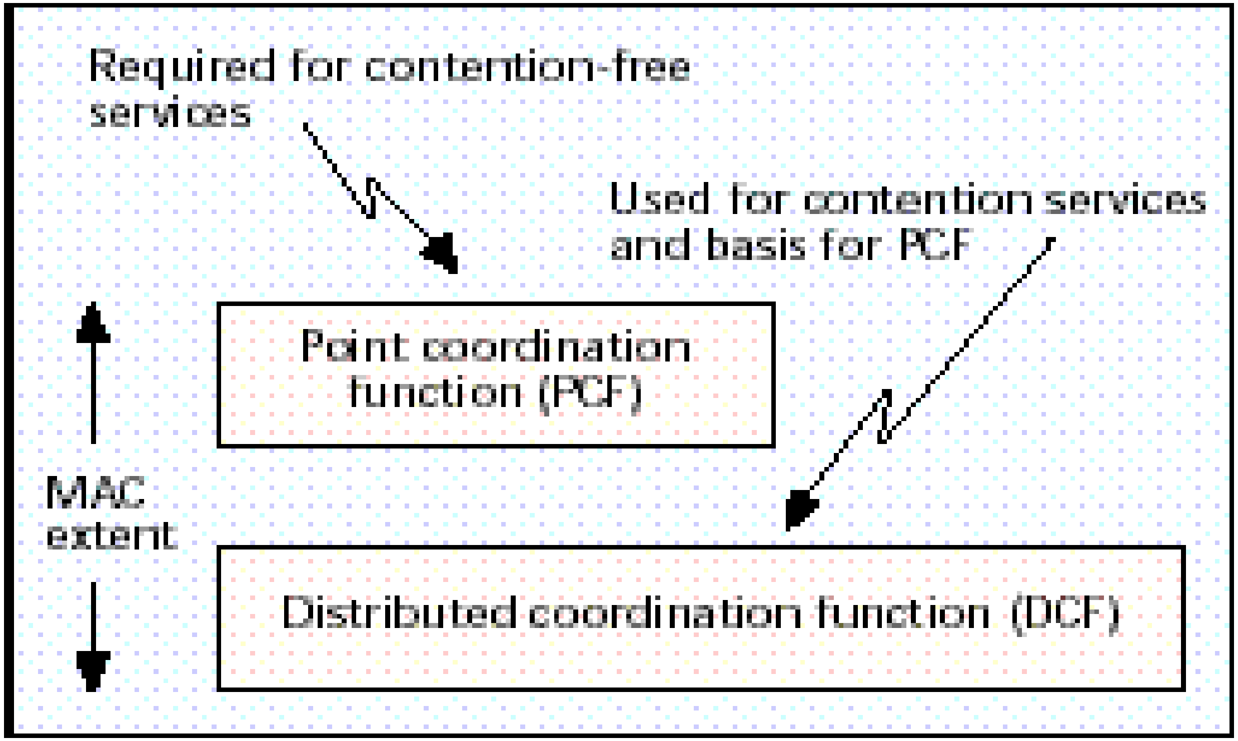
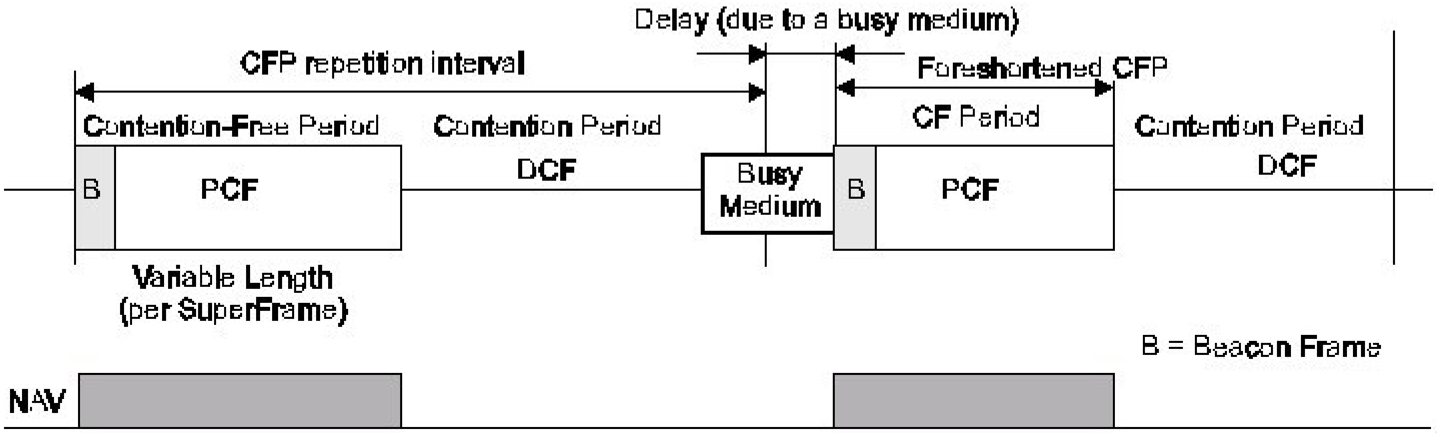

Required for contention-free services
Used for contention services and basis for PCF
Point coordination function (PCF)
MAC extent
Distributed coordination function (DCF)

Figure 4. *MAC architecture.*

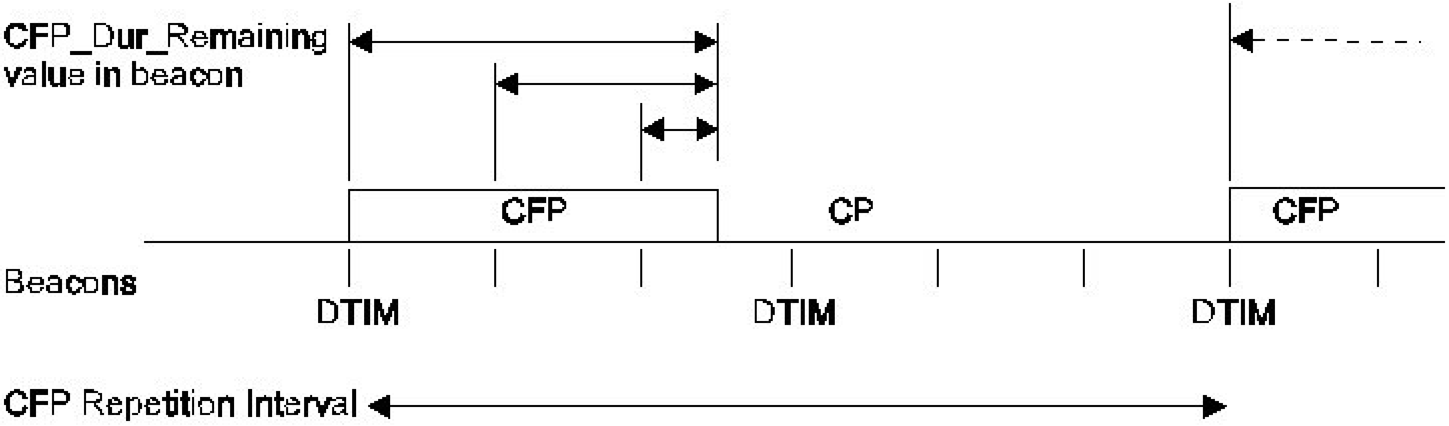
Coexistence of PCF and DCF

- A Point Coordinator (PC) resides in the Access Point and controls frame transfers during a Contention Free Period (CFP)
- A CF-Poll frame is used by the PC to invite a station to send data. Stations are polled from a list maintained by the PC
- The CFP alternates with a Contention Period (CP) in which data transfers happen as per the rules of DCF
- This CP must be large enough to send at least one maximum-sized packet including RTS/CTS/ACK
- CFPs are generated at the CFP repetition rate
- The PC sends Beacons at regular intervals and at the start of each CFP
- The CF-End frame signals the end of the CFP

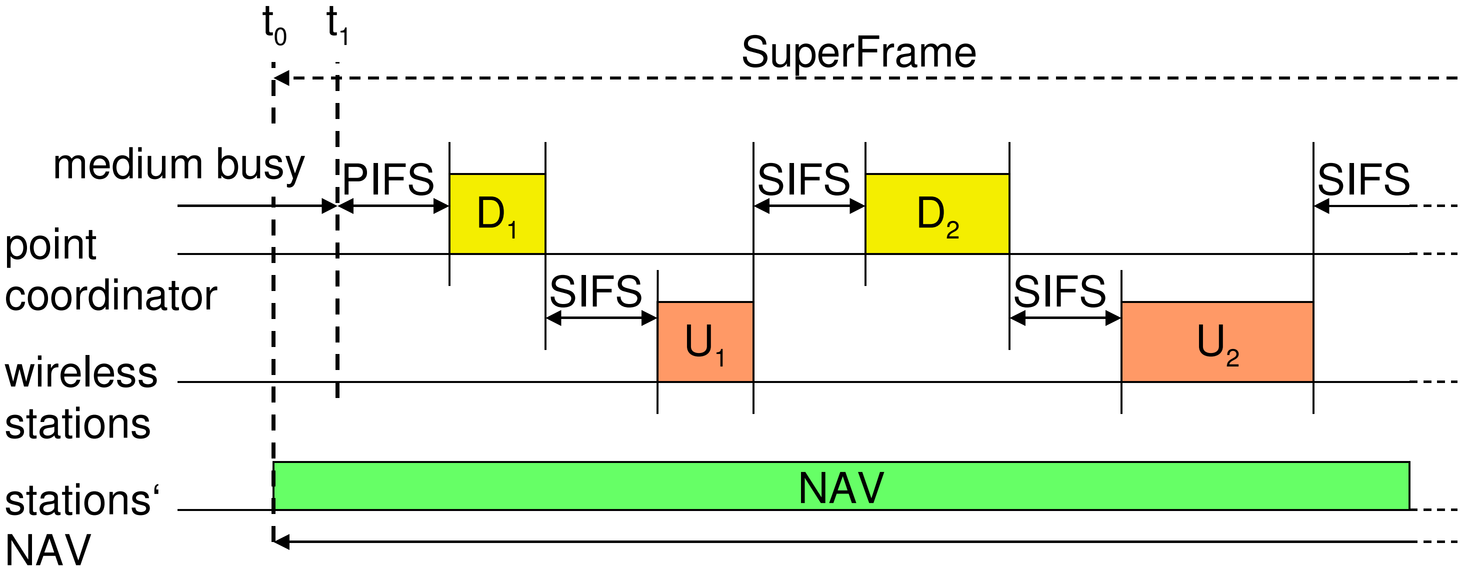
CFP structure and Timing



CFP/CP Alternation and Beacon Periods

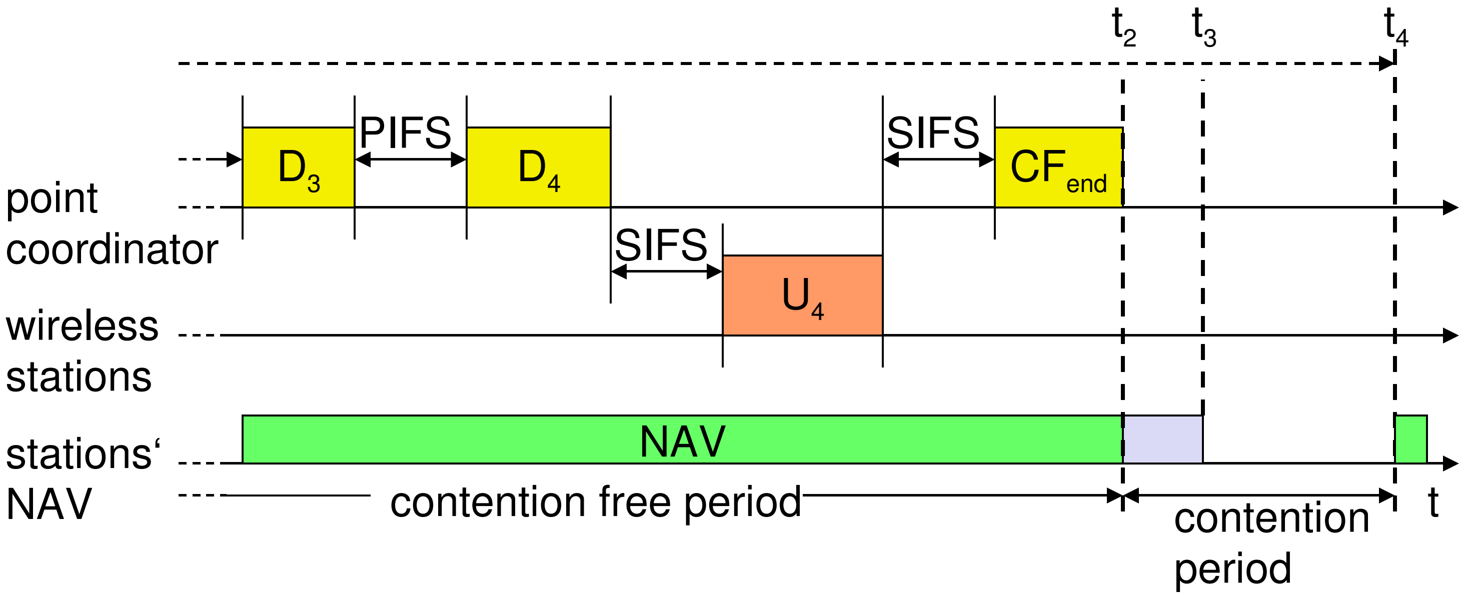


802.11 - PCF I



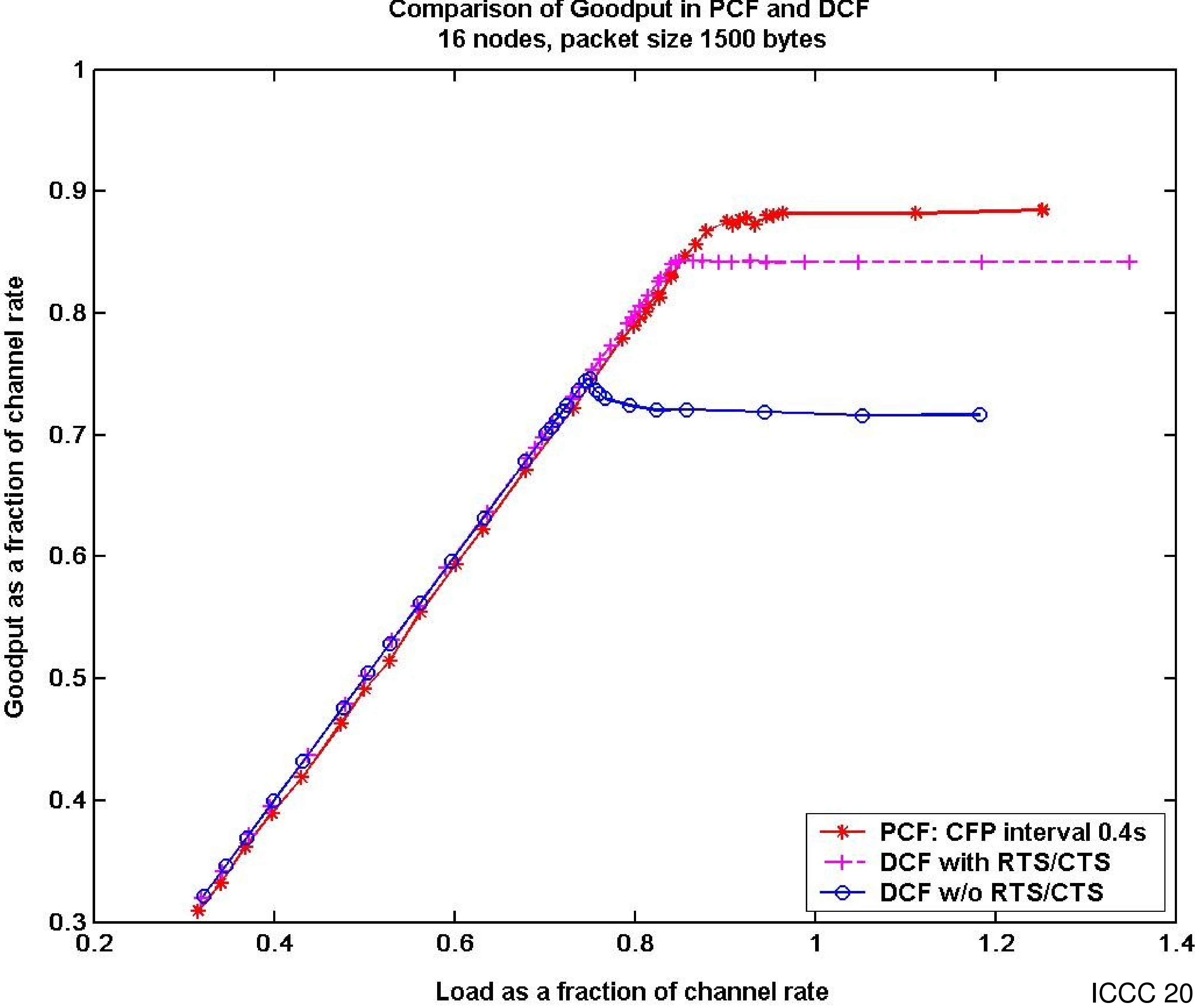
Source: Schiller

802.11 - PCF II


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

Throughput – DCF vs. PCF

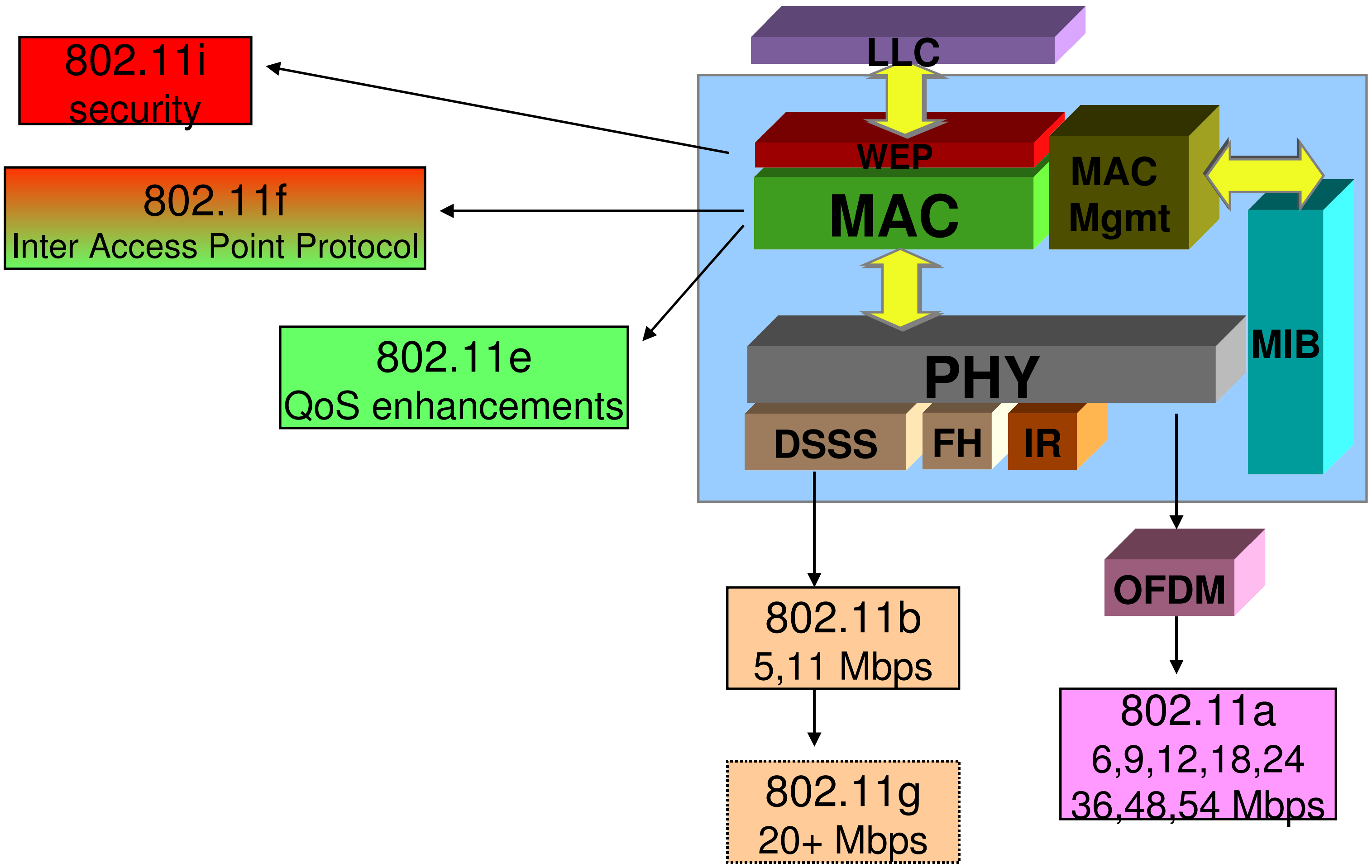
- Overheads to throughput and delay in DCF mode come from losses due to collisions and backoff
- These increase when number of nodes in the network increases
- RTS/CTS frames cost bandwidth but large data packets (>RTS threshold) suffer fewer collisions
- RTC/CTS threshold must depend on number of nodes
- Overhead in PCF modes comes from wasted polls
- Polling mechanisms have large influence on throughput
- Throughput in PCF mode shows up to 20% variation with other configuration parameters – CFP repetition rate
- Saturation throughput of DCF less than PCF in all studies presented here (‘heavy load’ conditions)


Comparison of Goodput in PCF and DCF
16 nodes, packet size 1500 bytes
Goodput as a fraction of channel rate
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.4
0.6
0.8
1
1.2
1.4
Load as a fraction of channel rate
PCF: CFP interval 0.4s
DCF with RTS/CTS
DCF w/o RTS/CTS

IEEE 802.11 Summary

- Infrastructure and ad hoc modes using DCF
- Carrier Sense Multiple Access
- Binary exponential backoff for collision avoidance and congestion control
- Acknowledgements for reliability
- Power save mode for energy conservation
- Time-bound service using PCF
- Signaling packets for avoiding Exposed/Hidden terminal problems, and for reservation
  - Medium is reserved for the duration of the transmission
  - RTS-CTS in DCF
  - Polls in PCF

802.11 current status



802.11i
security

802.11f
Inter Access Point Protocol

802.11e
QoS enhancements

LLC

WEP

MAC

MAC
Mgmt

MIB

PHY

DSSS

FH

IR

OFDM

802.11b
5,11 Mbps

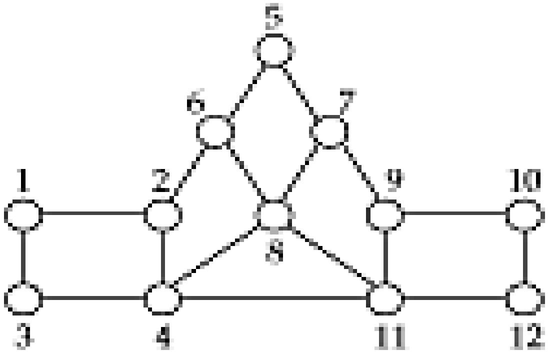
802.11g
20+ Mbps

802.11a
6,9,12,18,24
36,48,54 Mbps

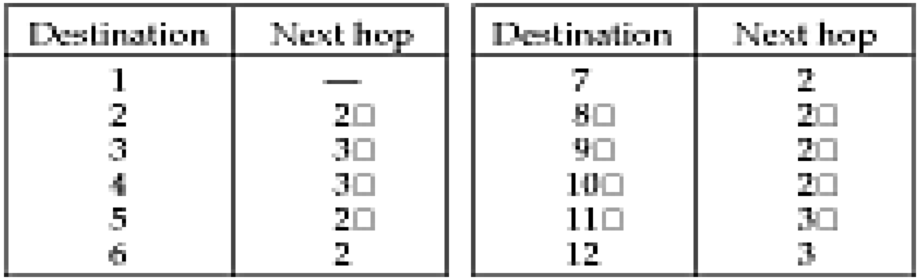
Mobile IP

Traditional Routing

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



ROUTING TABLE AT 1



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

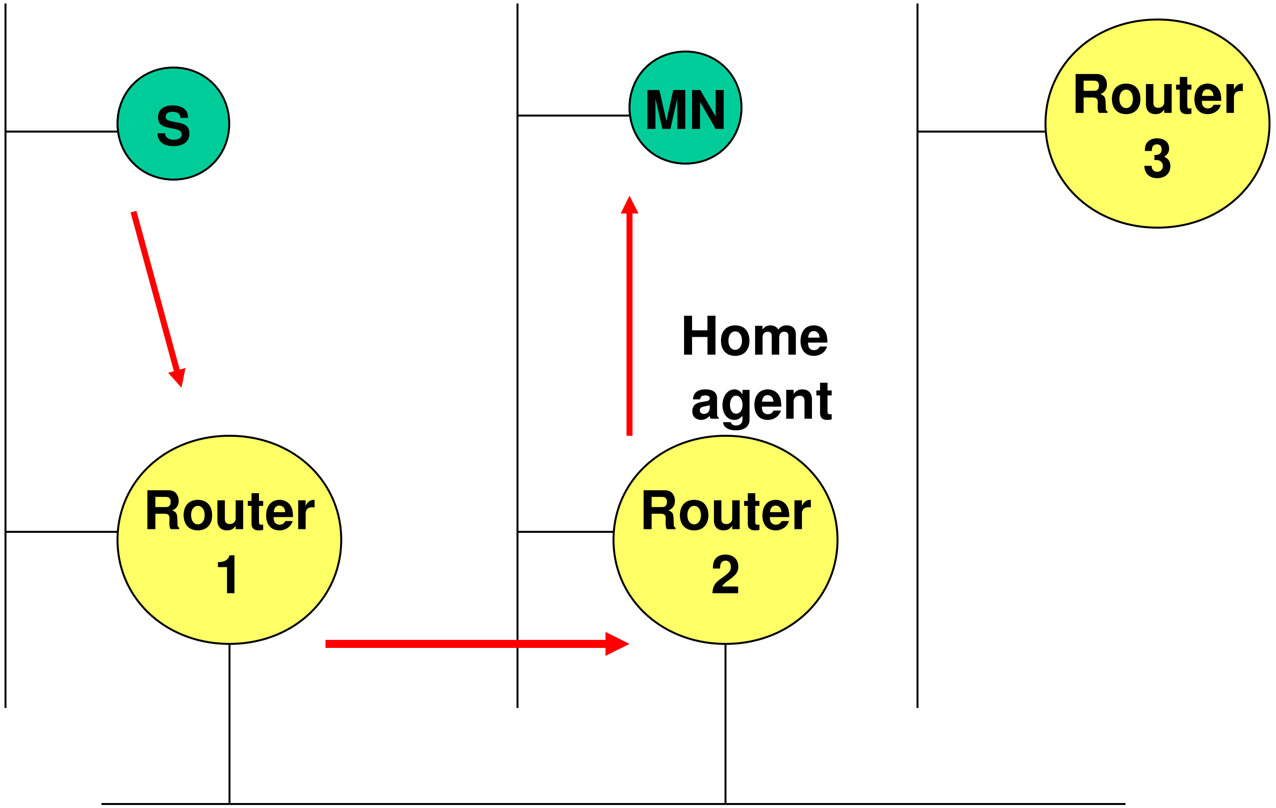
- Issues
  - Frequent route changes
    - amount of data transferred between route changes may be much smaller than traditional networks
  - Route changes may be related to host movement
  - Low bandwidth links

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

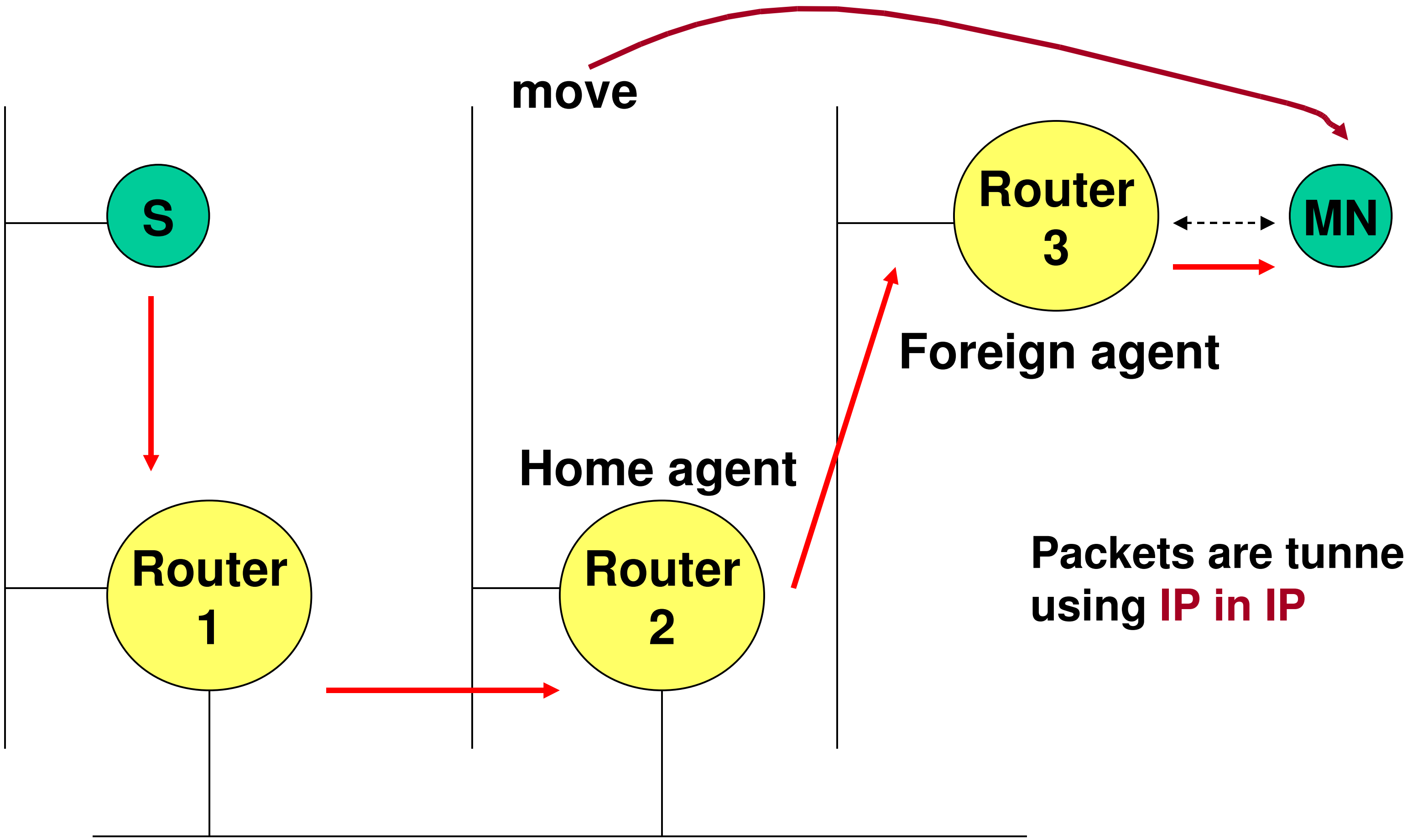
Mobile IP (RFC 3344): Motivation

- 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

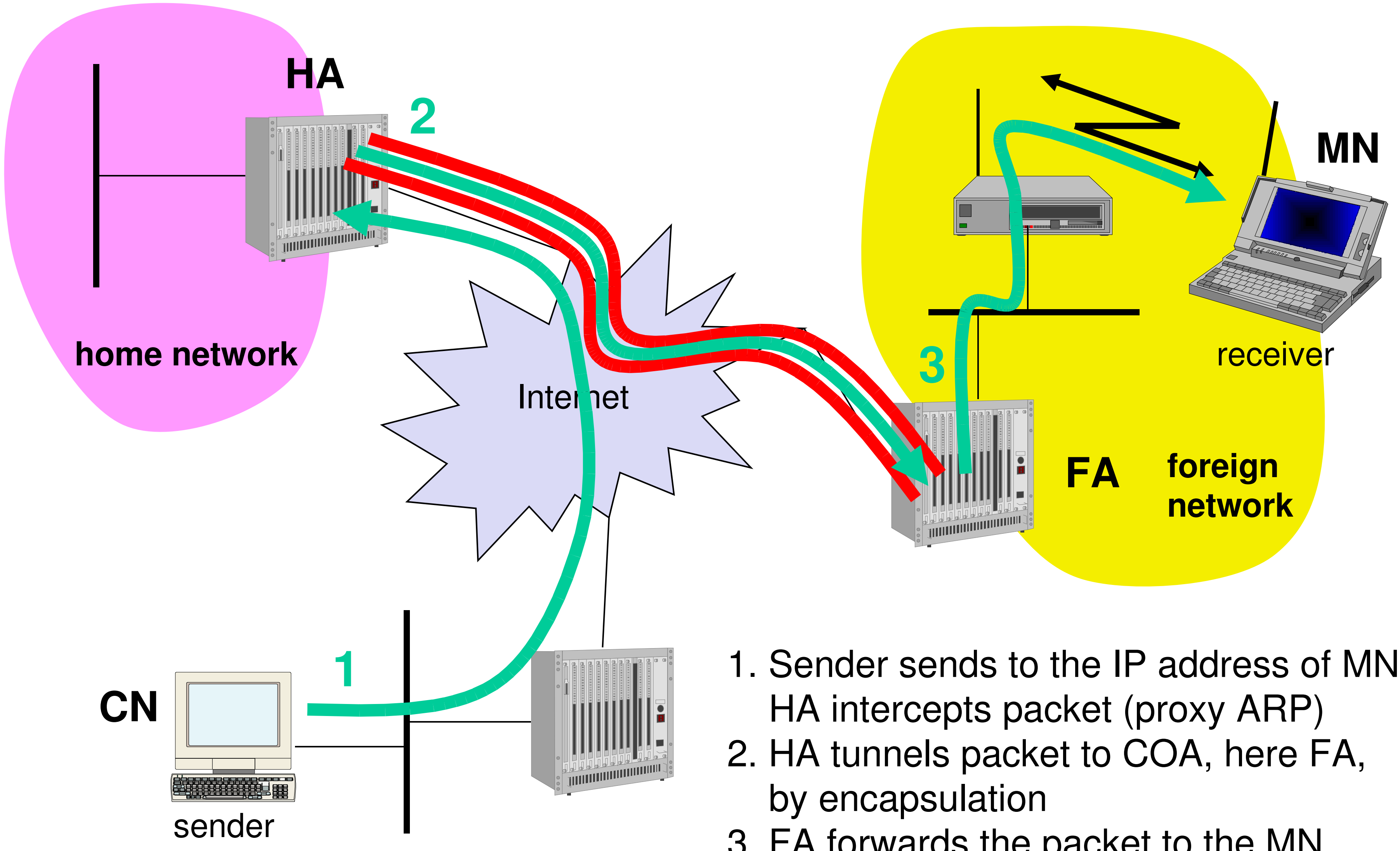


Packets are tunneled using **IP in IP**

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)

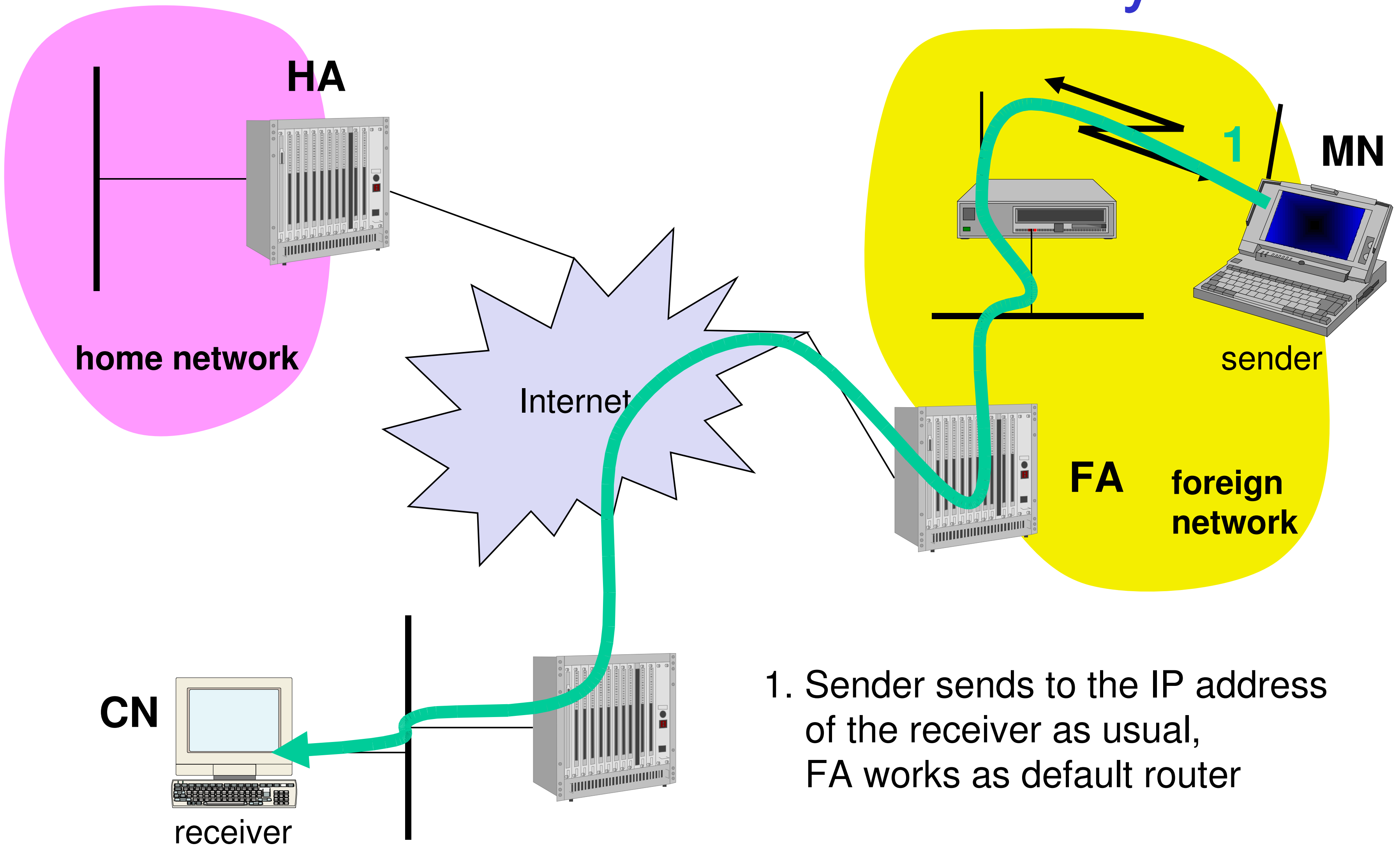
Data transfer to the mobile system



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

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

Agent advertisement

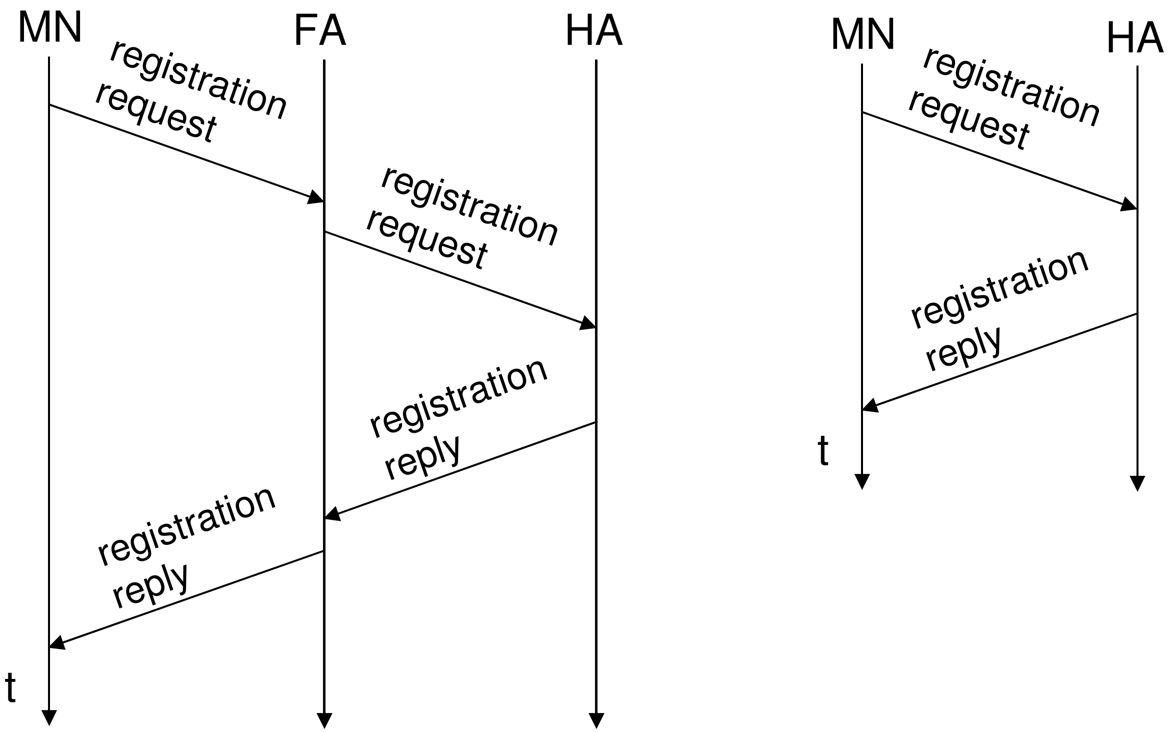
0 7	8 15	16 23	24 31
type	code	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			

. . .

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

. . .

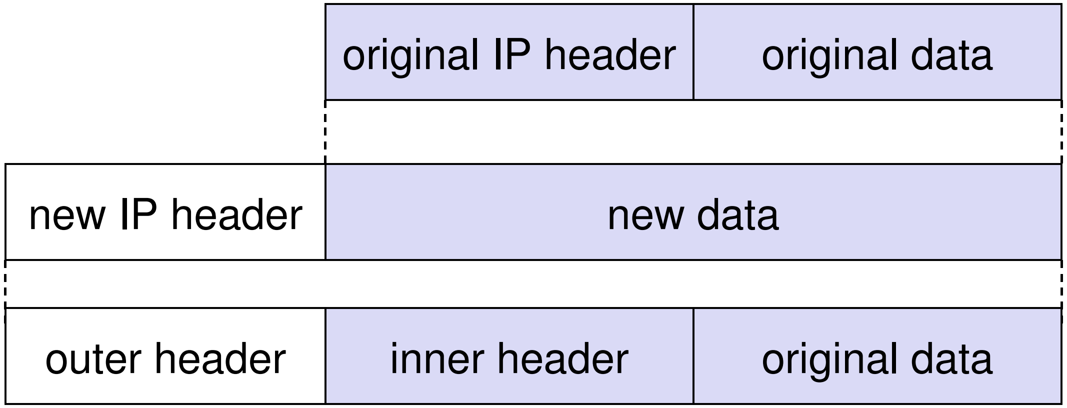
Registration



Registration request

<table>
<tr><td>0 7</td><td colspan="7">8 15</td><td>16 23</td><td>24 31</td></tr>
<tr><td>type</td><td>S</td><td>B</td><td>D</td><td>M</td><td>G</td><td>V</td><td>rsv</td><td colspan="2">lifetime</td></tr>
<tr><td colspan="10">home address</td></tr>
<tr><td colspan="10">home agent</td></tr>
<tr><td colspan="10">COA</td></tr>
<tr><td colspan="10">identification</td></tr>
<tr><td colspan="10">extensions . . .</td></tr>
</table>

Encapsulation



original IP header | original data

new IP header | new data

outer header | inner header | original data

IP-in-IP encapsulation

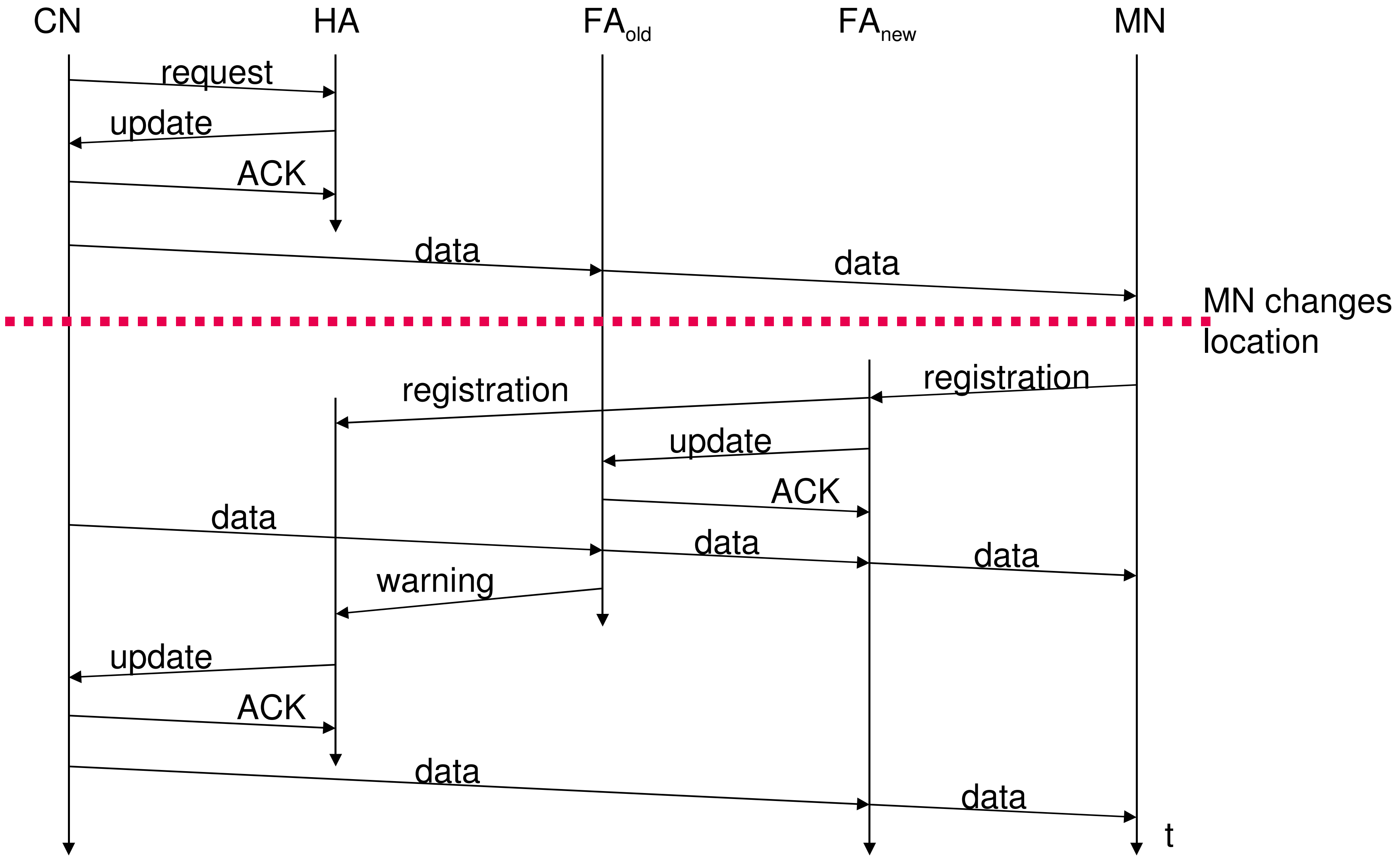
- IP-in-IP-encapsulation (mandatory in RFC 2003)
  - tunnel between HA and COA

<table>
<tr><td>ver.</td><td>IHL</td><td>TOS</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td><i>IP-in-IP</i></td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5"><b>IP address of HA</b></td></tr>
<tr><td colspan="5"><b>Care-of address COA</b></td></tr>
<tr><td>ver.</td><td>IHL</td><td>TOS</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5"><b>IP address of CN</b></td></tr>
<tr><td colspan="5"><b>IP address of MN</b></td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

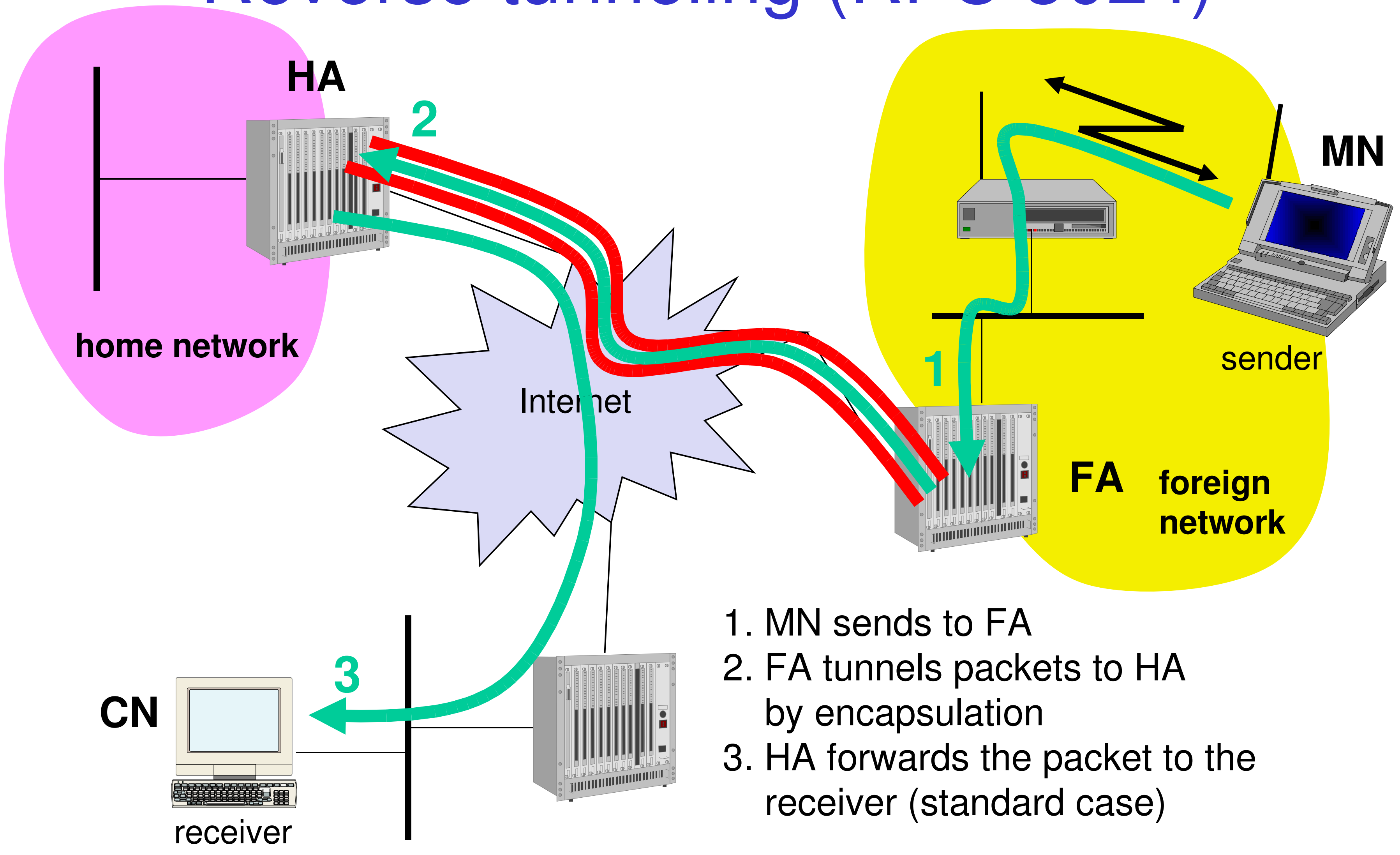
Optimization of packet forwarding

- Triangular Routing
  - sender sends all packets via HA to MN
  - higher latency and network load
- “Solutions”
  - sender learns the current location of MN
  - direct tunneling to this location
  - HA informs a sender about the location of MN
  - big security problems!
- Change of FA
  - packets on-the-fly during the change can be lost
  - new FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
  - this information also enables the old FA to release resources for the MN

Change of foreign agent



Reverse tunneling (RFC 3024)



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

Mobile IP with reverse tunneling

- Router accept often only “topological correct“ addresses (firewall!)
  - a packet from the MN encapsulated by the FA is now topological correct
  - furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is too far away from the receiver)
- Reverse tunneling does not solve
  - problems with *firewalls*, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
  - optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)
- The new standard is backwards compatible
  - the extensions can be implemented easily and cooperate with current implementations without these extensions

Mobile IPv4 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

- Optimizations for triangular routing
- Reverse tunneling

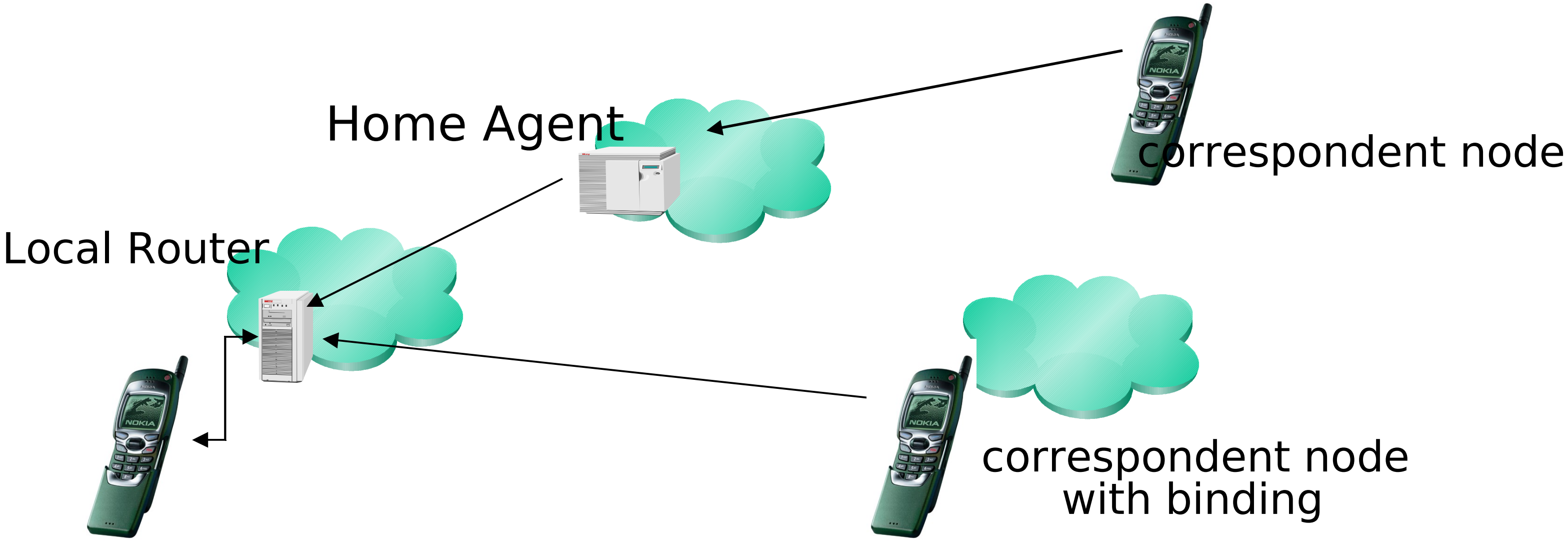
IPv6 Address Architecture

- Unicast address
  - provider-based global address
  - link-local(at least one per interface), site-local
  - IPv4 compatible IPv6 address (IPv6 node)
  - IPv4 mapped IPv6 address (IPv4 node)
- A single interface can have multiple addresses of any type or scope
- Multicast address identifies a group of stations/interfaces (112-bit group ID)
- No Broadcast addresses
  - Broadcast applications in IPv4 will have to be re-written in IPv6

Autoconfiguration

- Plug & Play - a machine when plugged in will automatically discover and register the required parameters for Internet connectivity
- Autoconfiguration includes
  - creating a link-local address
  - verifying its uniqueness on a link
  - determining what information should be autoconfigured, addresses and/or other info
  - In the case of addresses, they may be obtained through stateless or stateful mechanism (DHCPv6), or both

Mobile IPv6 protocol



- Advertisement from local router contains routing prefix
- *Seamless Roaming*: mobile node always uses home address
- Address autoconfiguration for care-of address
- Binding Updates sent to home agent & correspondent nodes
  - (home address, care-of address, binding lifetime)
- Mobile Node "*always on*" by way of home agent

IPv6 and Mobile IPv6 Summary

- Proliferation of wireless devices driving adoption of IPv6
- 340 undecillion addresses
  - (340,282,366,920,938,463,463,374,607,431,768,211,456) total!
- Billions of IP-addressable wireless handsets
- Specially interesting for China which has
  - 8 million IPv4 addresses and 50+ million handsets
- Mobile IP considers the mobility problem as a *routing* problem
  - managing a *binding* – that is, a dynamic tunnel between a care-of address and a home address - Binding updates in IPv6 replace registration requests in IPv4
  - *Of course,*there is a lot more to it than that!
- Mobile IPv6 still hampered by the lack of security solutions
  - IPSec requires deployed PKI (not available yet)