Wireless Networking Technologies

WLAN, WiFi Mesh and WiMAX

Sridhar Iyer

K R School of Information Technology

IIT Bombay

sri@it.iitb.ac.in

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

Course Outline

- Wireless Networks
  - Difference from wired
  - Mobility
- RF Basics
  - Frequency, modulation
  - Medium access control
- WiFi Overview
  - Basic elements
  - Standards and variants
- WiMaX Overview
  - Basic elements
- Wireless LANs (WiFi)
  - 802.11 standards
  - Mobility support
  - Voice and QoS support
- Mesh and Adhoc Networks
  - Routing and Transport
- Wireless MANs (WiMaX)
  - 802.16 standard
  - Voice and QoS support
- Trends
  - Overlay networks

Wireless Networks

Wireless networks

- Access computing/communication services, on the move
- Wireless WANs
  - Cellular Networks: GSM, GPRS, CDMA
  - Satellite Networks: Iridium
- Wireless LANs
  - WiFi Networks: 802.11
  - Personal Area Networks: Bluetooth
- Wireless MANs
  - WiMaX Networks: 802.16
  - Mesh Networks: Multi-hop WiFi
  - Adhoc Networks: useful when infrastructure not available

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

Mobile communication

- Wireless vs. mobile Examples

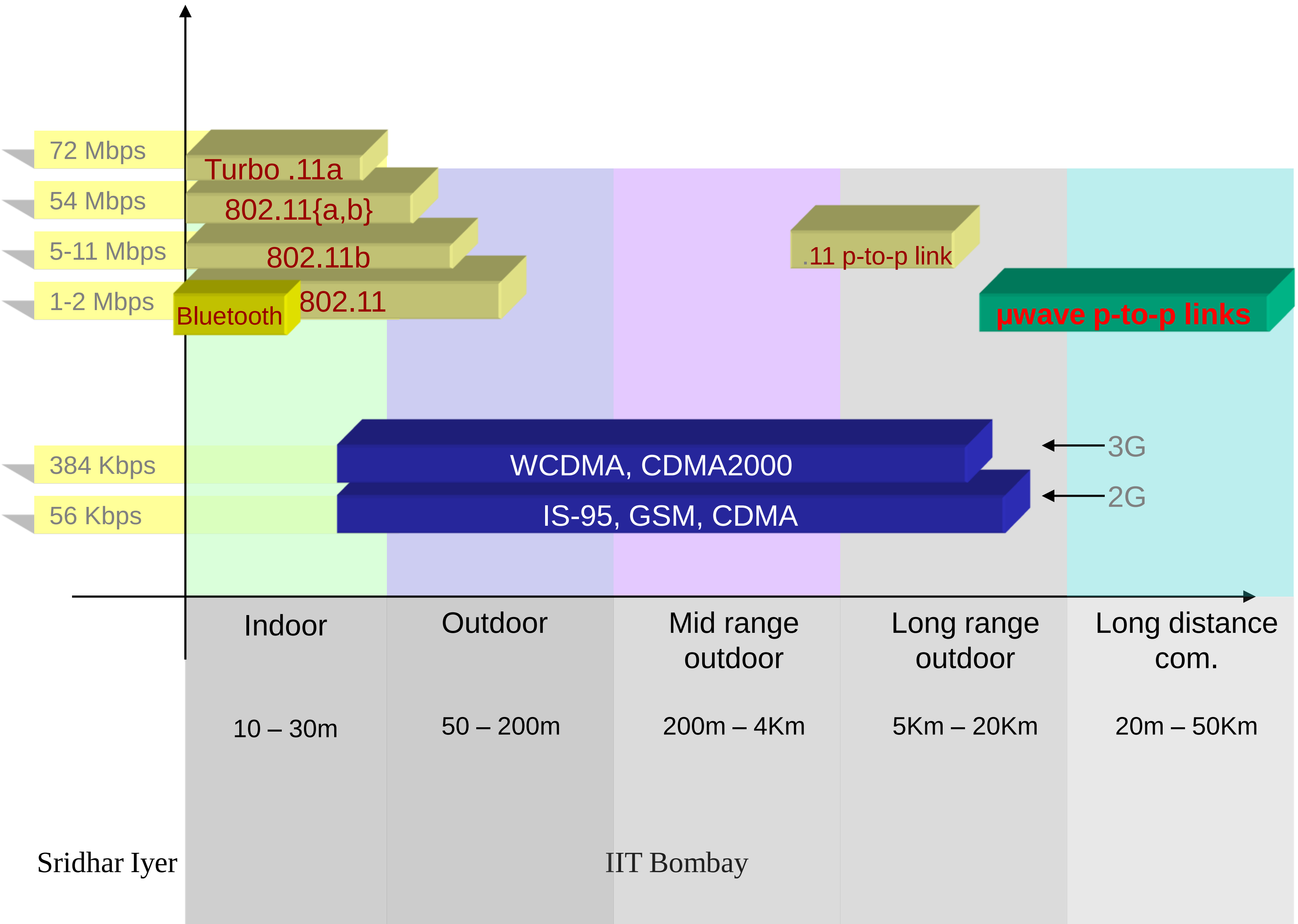
Wireless	Mobile	Examples
✗	✗	stationary computer
✗	✓	laptop in a hotel (portable)
✓	✗	wireless LAN in historic buildings
✓	✓	Personal Digital Assistant (PDA)

- Integration of wireless into existing fixed networks:
  - Local area networks: IEEE 802.11, ETSI (HIPERLAN)
  - Wide area networks: Cellular 3G, IEEE 802.16
  - Internet: Mobile IP extension

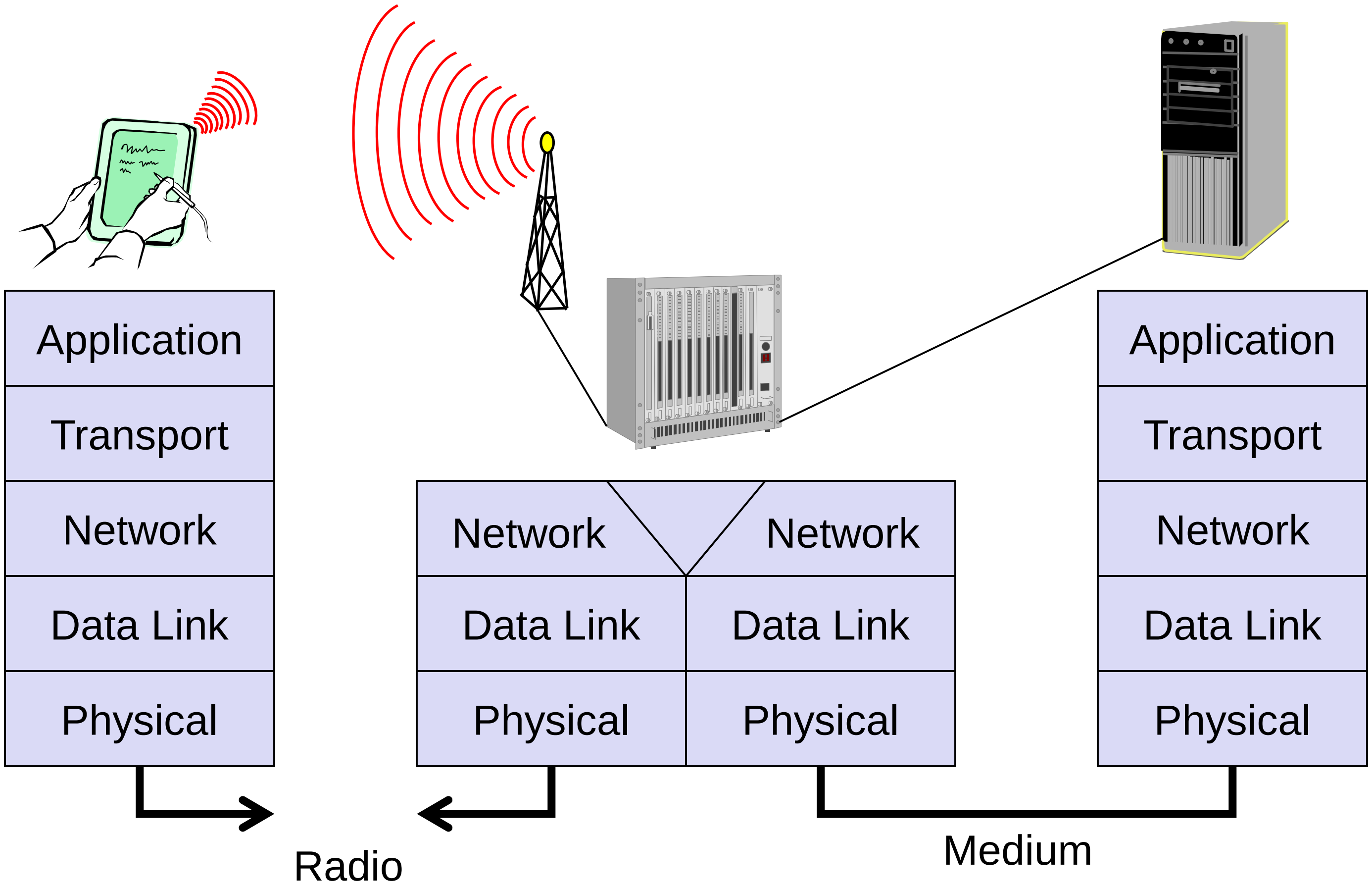
Wireless v/s Wired networks

- 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
  - secure access mechanisms important

Wireless Technology Landscape



Reference model



Effect of mobility on protocol stack

- Application
  - new applications and adaptations
  - service location, multimedia
- Transport
  - congestion and flow control
  - quality of service
- Network
  - addressing and routing
  - device location, hand-over
- Link
  - media access and security
- Physical
  - transmission errors and interference

Perspectives

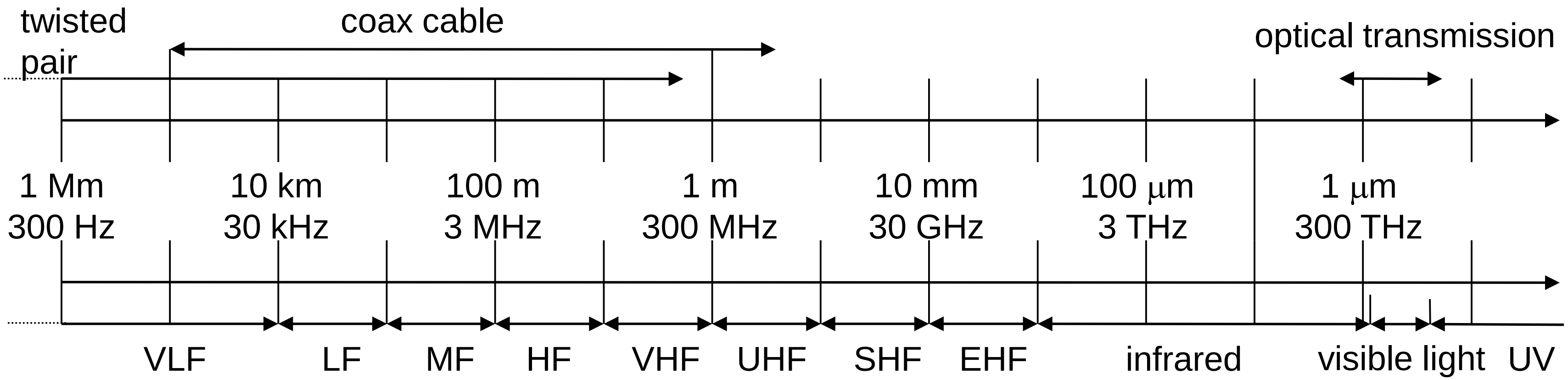
- Network designers: Concerned with cost-effective design
  - Need to ensure that network resources are efficiently utilized and fairly allocated to different users.
- Network users: Concerned with application services
  - Need guarantees that each message sent will be delivered without error within a certain amount of time.
- Network providers: Concerned with system administration
  - Need mechanisms for security, management, fault-tolerance and accounting.

RF Basics

Factors affecting wireless system design

- Frequency allocations
  – What range to operate? May need licenses.
- Multiple access mechanism
  – How do users share the medium without interfering?
- Antennas and propagation
  – What distances? Possible channel errors introduced.
- Signals encoding
  – How to improve the data rate?
- Error correction
  – How to ensure that bandwidth is not wasted?

Frequencies for communication



- VLF = Very Low Frequency
- LF = Low Frequency
- MF = Medium Frequency
- HF = High Frequency
- VHF = Very High Frequency

UHF = Ultra High Frequency
SHF = Super High Frequency
EHF = Extra High Frequency
UV = Ultraviolet Light

- Frequency and wave length: $\lambda = c/f$
- wave length λ, speed of light $c \cong 3 \times 10^8$ m/s, frequency f

Wireless frequency allocation

- Radio frequencies range from 9KHz to 400GHZ (ITU)

- Microwave frequency range
  – 1 GHz to 40 GHz
  – Directional beams possible
  – Suitable for point-to-point transmission
  – Used for satellite communications
- Radio frequency range
  – 30 MHz to 1 GHz
  – Suitable for omnidirectional applications
- Infrared frequency range
  – Roughly, $3x10^{11}$ to $2x10^{14}$ Hz
  – Useful in local point-to-point multipoint applications within confined areas

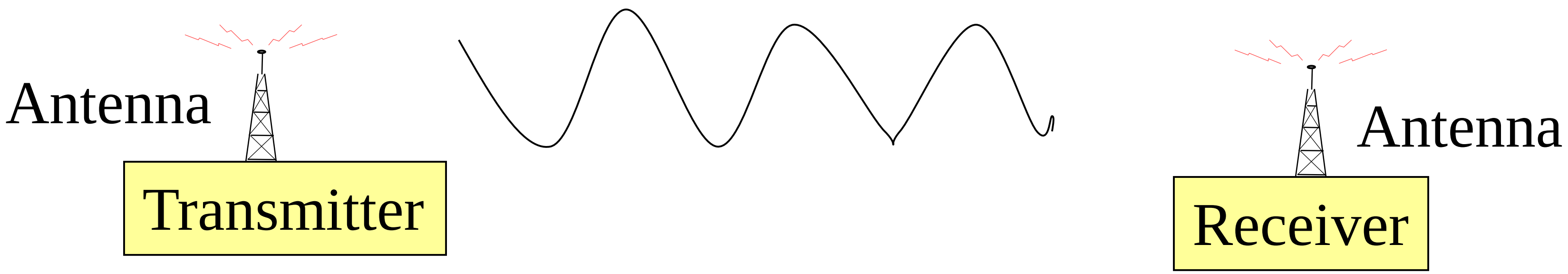
Frequencies for mobile communication

- VHF-/UHF-ranges for mobile radio
  - simple, small antenna for cars
  - deterministic propagation characteristics, reliable connections
- SHF and higher for directed radio links, satellite communication
  - small antenna, focusing
  - large bandwidth available
- Wireless LANs use frequencies in UHF to SHF spectrum
  - some systems planned up to EHF
  - limitations due to absorption by water and oxygen molecules (resonance frequencies)
    - weather dependent fading, signal loss caused by heavy rainfall etc.

Frequency regulations

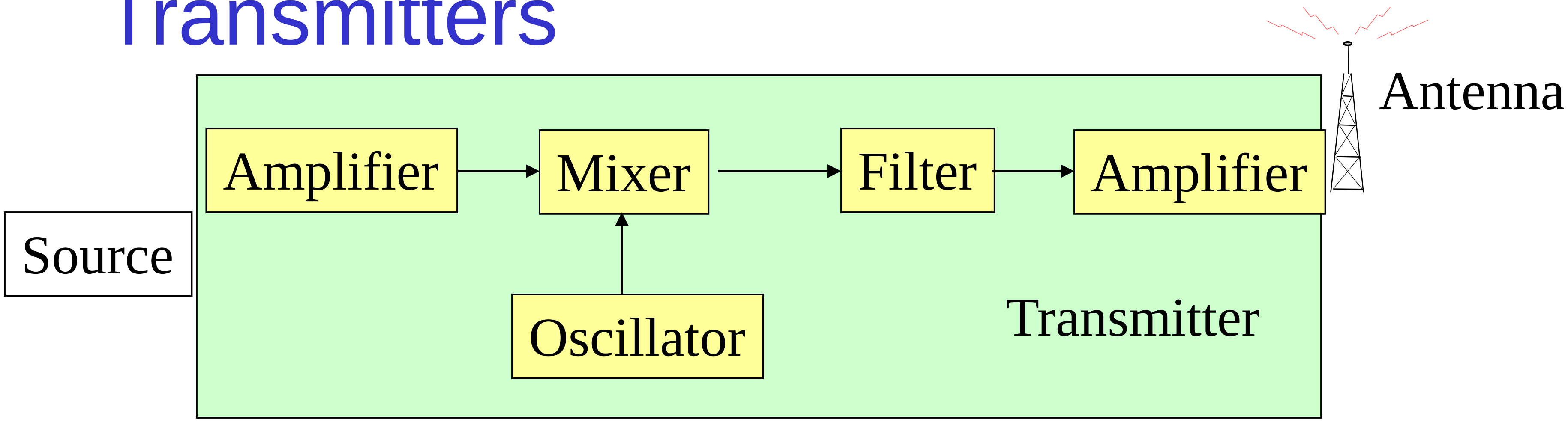
- Frequencies from 9KHz to 300 MHZ in high demand (especially VHF: 30-300MHZ)
- Two unlicensed bands
  - Industrial, Science, and Medicine (ISM): 2.4 GHz
  - Unlicensed National Information Infrastructure (UNII): 5.2 GHz
- Different agencies license and regulate
  - www.fcc.gov - US
  - www.etsi.org - Europe
  - www.wpc.dot.gov.in - India
  - www.itu.org - International co-ordination
- Regional, national, and international issues
- Procedures for military, emergency, air traffic control, etc

Wireless transmission



- Wireless communication systems consist of:
  - Transmitters
  - Antennas: radiates electromagnetic energy into air
  - Receivers
- In some cases, transmitters and receivers are on same device, called transceivers.

Transmitters



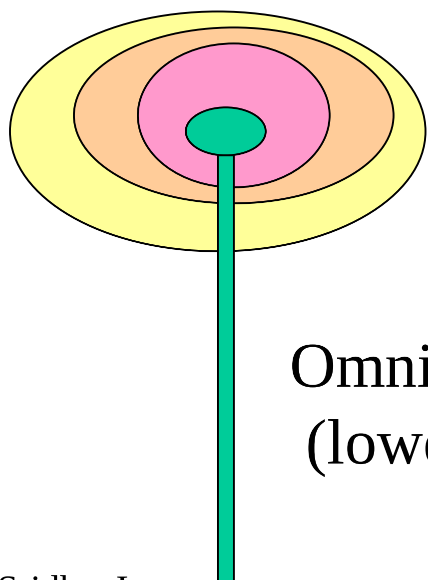
Suppose you want to generate a signal that is sent at 900 MHz and the original source generates a signal at 300 MHz.

- Amplifier - strengthens the initial signal
- Oscillator - creates a carrier wave of 600 MHz
- Mixer - combines signal with oscillator and produces 900 MHz (also does modulation, etc)
- Filter - selects correct frequency
- Amplifier - Strengthens the signal before sending it

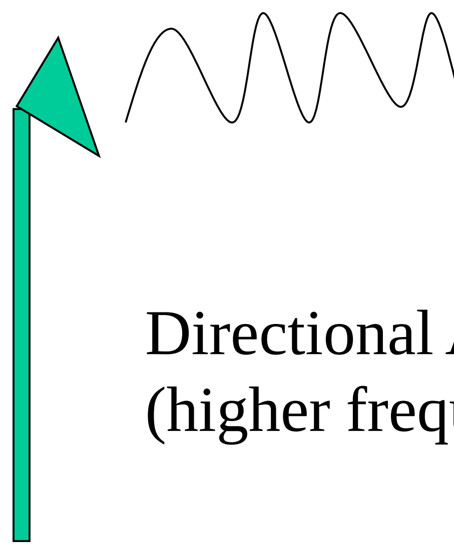
Antennas

Antennas

- An antenna is an electrical conductor or system of conductors to send/receive RF signals
  - Transmission - radiates electromagnetic energy into space
  - Reception - collects electromagnetic energy from space
- In two-way communication, the same antenna can be used for transmission and reception



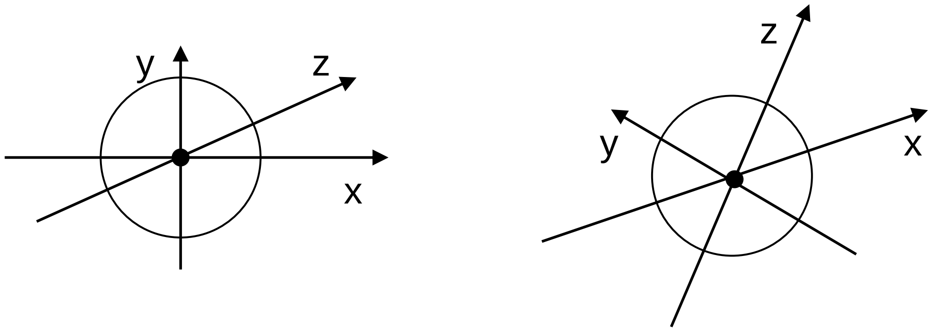
Omnidirectional Antenna
(lower frequency)



Directional Antenna
(higher frequency)

Antennas: isotropic radiator

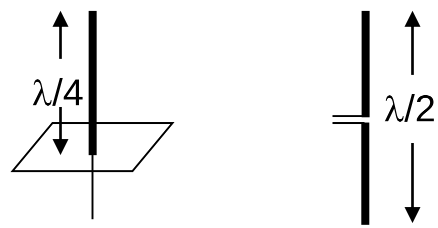
- Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission
- Isotropic radiator: equal radiation in all directions (three dimensional) - only a theoretical reference antenna
- Real antennas always have directive effects (vertically and/or horizontally)
- Radiation pattern: measurement of radiation around an antenna

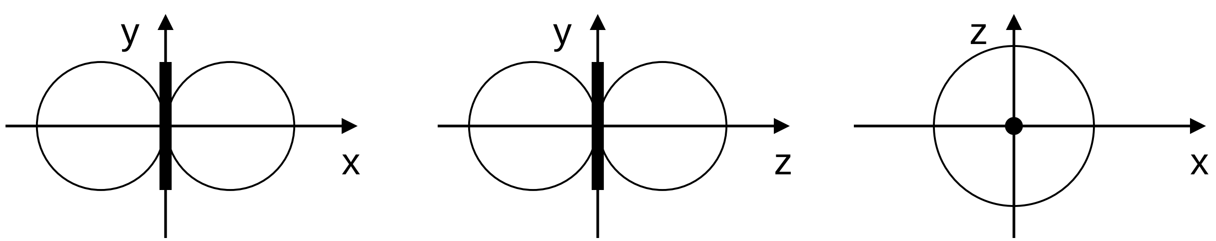


ideal isotropic radiator

Antennas: simple dipoles

- Real antennas are not isotropic radiators
  - dipoles with lengths λ/4 on car roofs or λ/2 (Hertzian dipole)
    ➔ shape of antenna proportional to wavelength
- Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)



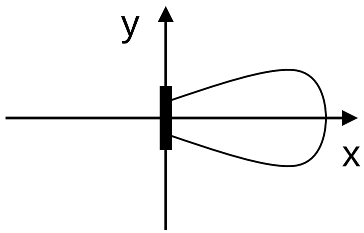


side view (xy-plane) side view (yz-plane) top view (xz-plane)

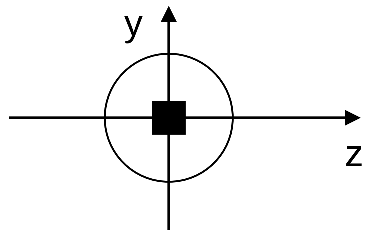
simple dipole

Antennas: directed and sectorized

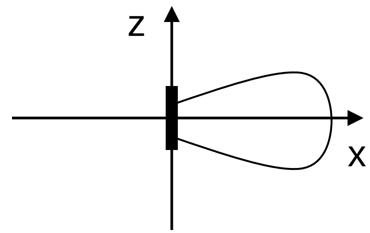
- Often used for microwave connections or base stations for mobile phones (e.g., radio coverage of a valley)



side view (xy-plane)

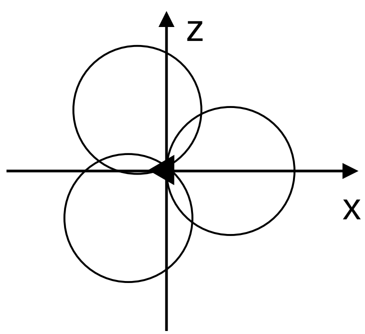


side view (yz-plane)

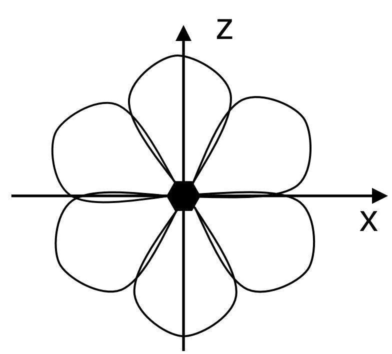


top view (xz-plane)

directed antenna



top view, 3 sector



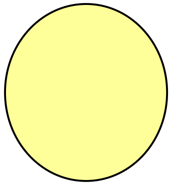
top view, 6 sector

sectorized antenna

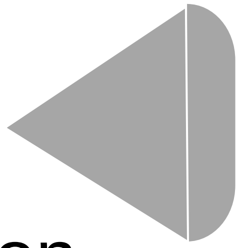
Antenna models

In Omni Mode:

- Nodes receive signals with gain $\mathbf{G^o}$



In Directional Mode:



- Capable of beamforming in specified direction
- Directional Gain $\mathbf{G^d}$ **($\mathbf{G^d > G^o}$)**

Directional communication

Received Power $\propto$ (Transmit power)

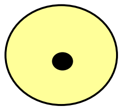
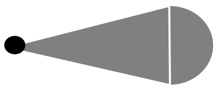
*(Tx Gain) * (Rx Gain)

Directional gain is higher

Directional antennas useful for:

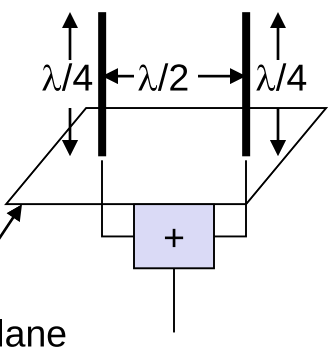
- Increase “range”, keeping transmit power constant
- Reduce transmit power, keeping range comparable with omni mode

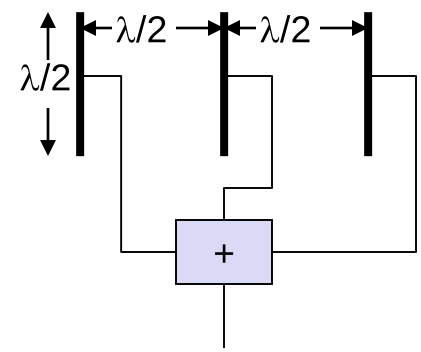
Comparison of omni and directional

Issues	Omni	Directional
Spatial Reuse	Low	High
Connectivity	Low	High
Interference	Omni 	Directional 
Cost & Complexity	Low	High

Antennas: diversity

- Grouping of 2 or more antennas
  - multi-element antenna arrays
- Antenna diversity
  - switched diversity, selection diversity
    - receiver chooses antenna with largest output
  - diversity combining
    - combine output power to produce gain
    - cophasing needed to avoid cancellation





Signal Propagation and Modulation

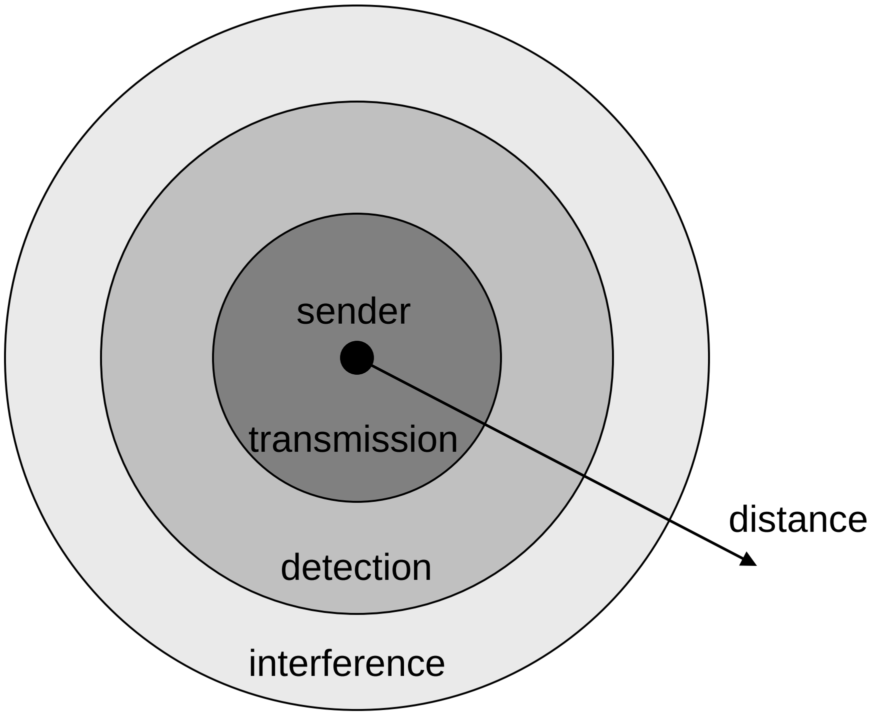
Signals

- physical representation of data
- function of time and location
- signal parameters: parameters representing the value of data
- classification
  - continuous time/discrete time
  - continuous values/discrete values
  - analog signal = continuous time and continuous values
  - digital signal = discrete time and discrete values
- signal parameters of periodic signals:
  period T, frequency f=1/T, amplitude A, phase shift φ
  - sine wave as special periodic signal for a carrier:

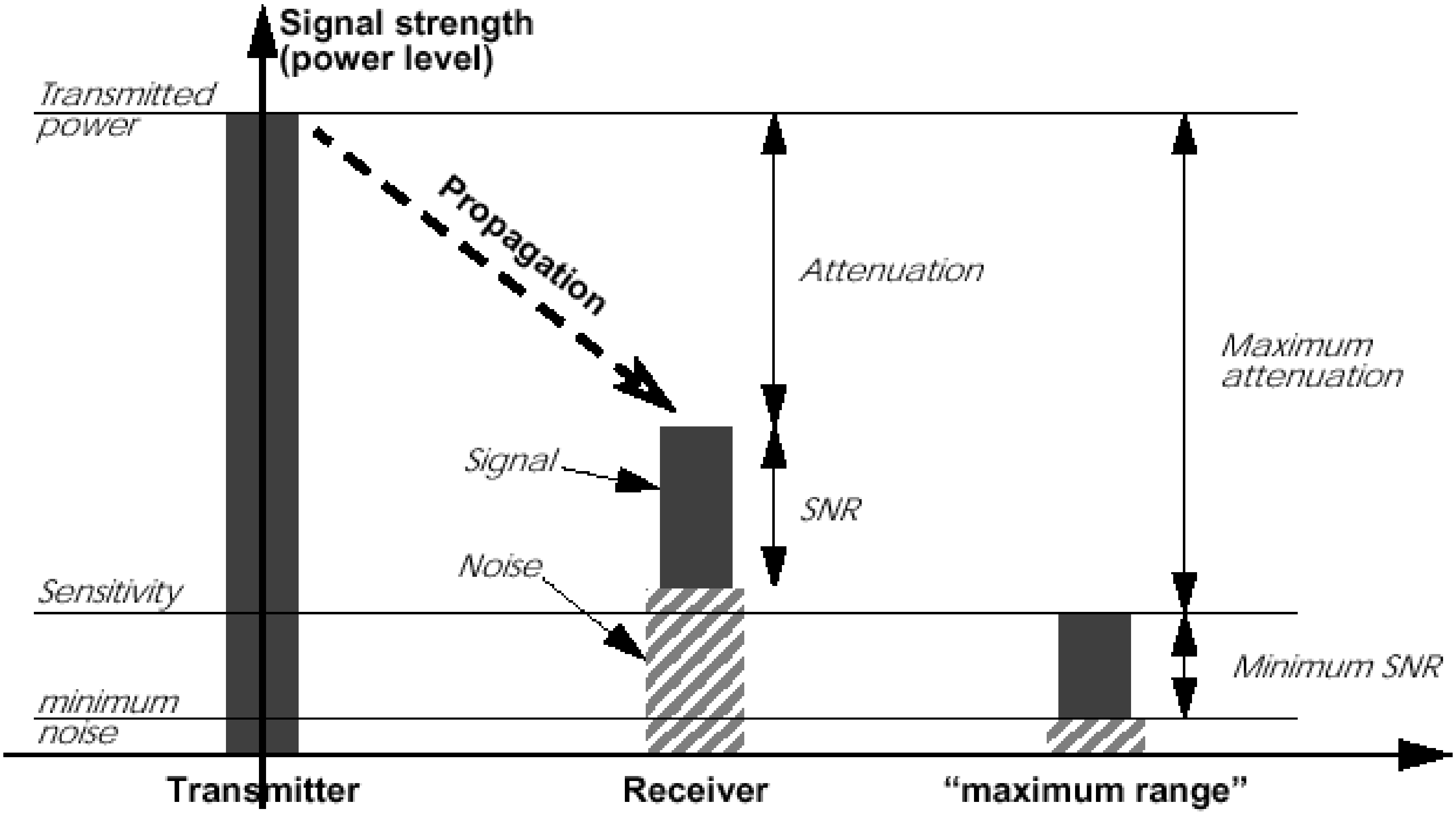
$$s(t) = A_t \sin(2 \pi f_t t + \varphi_t)$$

Signal propagation ranges

- Transmission range
  - communication possible
  - low error rate
- Detection range
  - detection of the signal possible
  - no communication possible
- Interference range
  - signal may not be detected
  - signal adds to the background noise



Attenuation: Propagation & Range

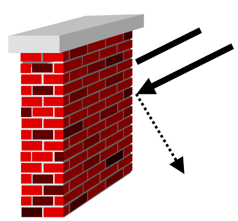


Attenuation

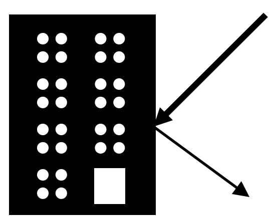
- Strength of signal falls off with distance over transmission medium
- Attenuation factors for unguided media:
  - Received signal must have sufficient strength so that circuitry in the receiver can interpret the signal
  - Signal must maintain a level sufficiently higher than noise to be received without error
  - Attenuation is greater at higher frequencies, causing distortion
- Approach: amplifiers that strengthen higher frequencies

Signal propagation

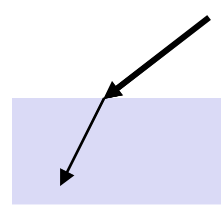
- Propagation in free space always like light (straight line)
- Receiving power proportional to $1/d^2$
  (d = distance between sender and receiver)
- Receiving power additionally influenced by
  - fading (frequency dependent)
  - shadowing
  - reflection at large obstacles
  - refraction depending on the density of a medium
  - scattering at small obstacles
  - diffraction at edges



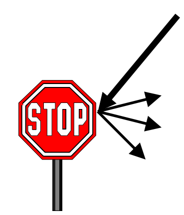
shadowing



reflection



refraction

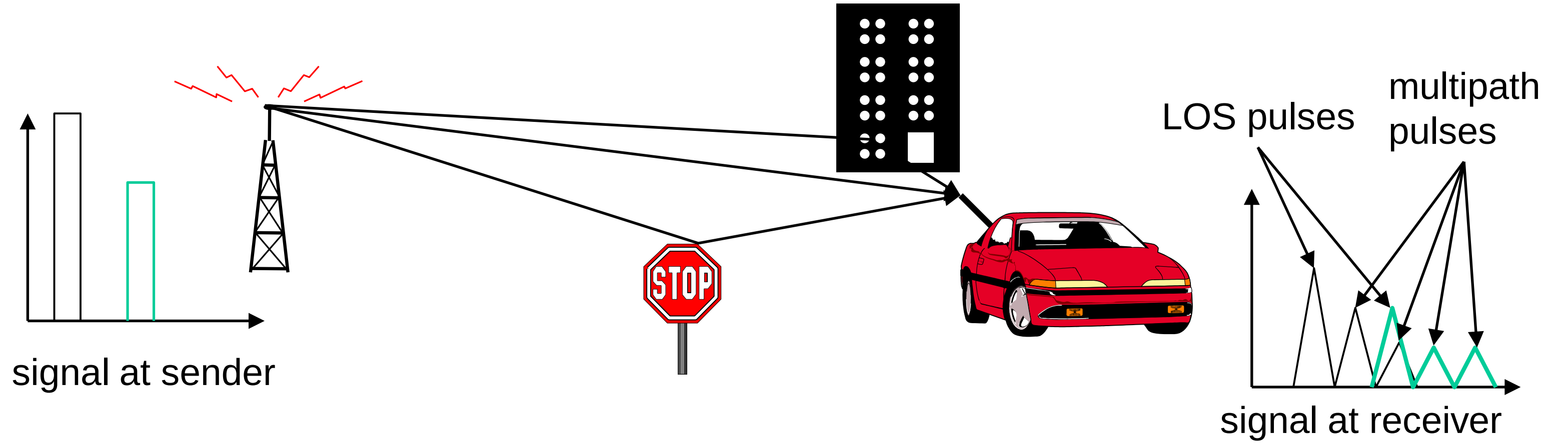


scattering

diffraction

Multipath propagation

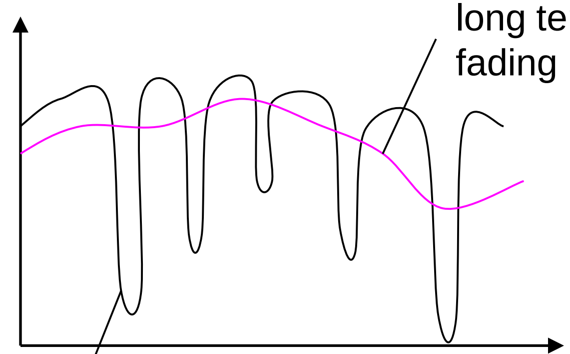
- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction



- Time dispersion: signal is dispersed over time
- ➔ interference with “neighbor” symbols, Inter Symbol Interference (ISI)
- The signal reaches a receiver directly and phase shifted
- ➔ distorted signal depending on the phases of the different parts

Effects of mobility

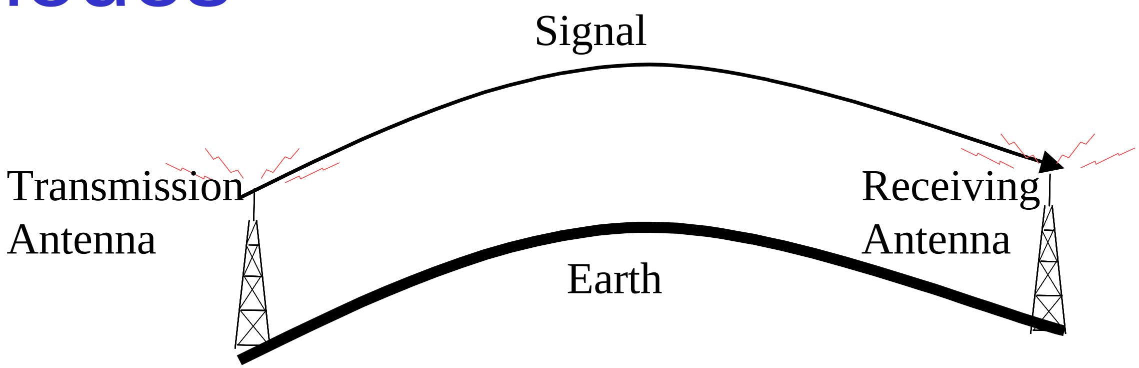
- Channel characteristics change over time and location
  - signal paths change
  - different delay variations of different signal parts
  - different phases of signal parts
- ➔ quick changes in the power received (short term fading)



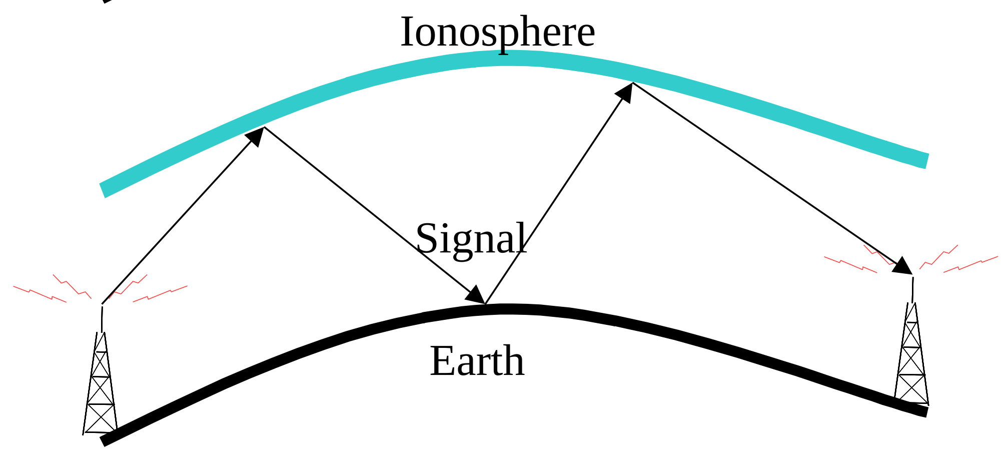
- Additional changes in
  - distance to sender
  - obstacles further away
- ➔ slow changes in the average power received (long term fading)

Propagation modes

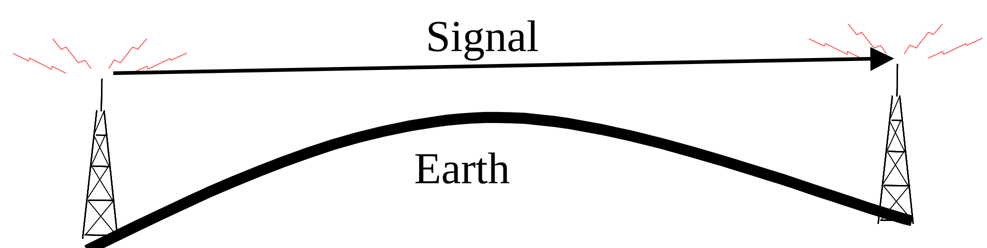
a) Ground Wave Propagation



b) Sky Wave Propagation



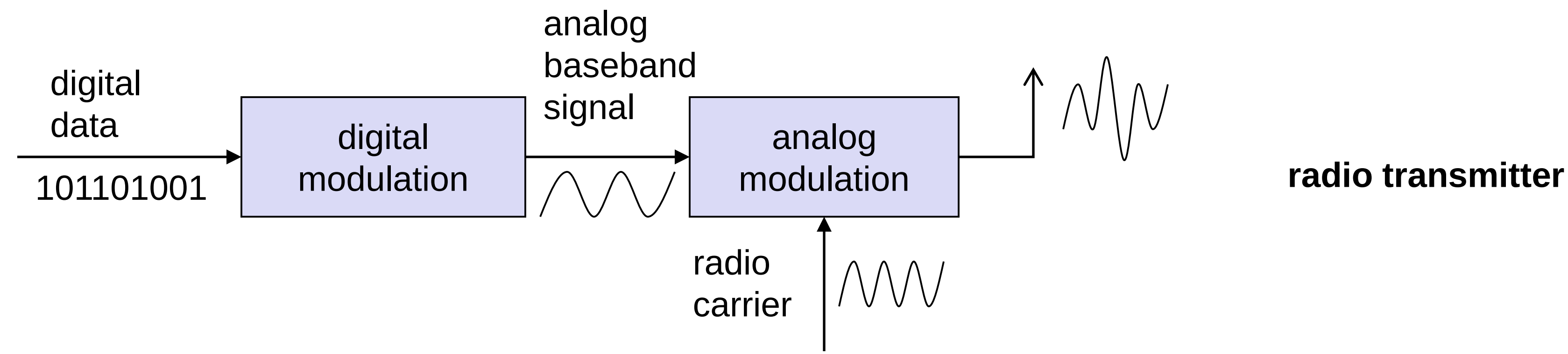
c) Line-of-Sight Propagation

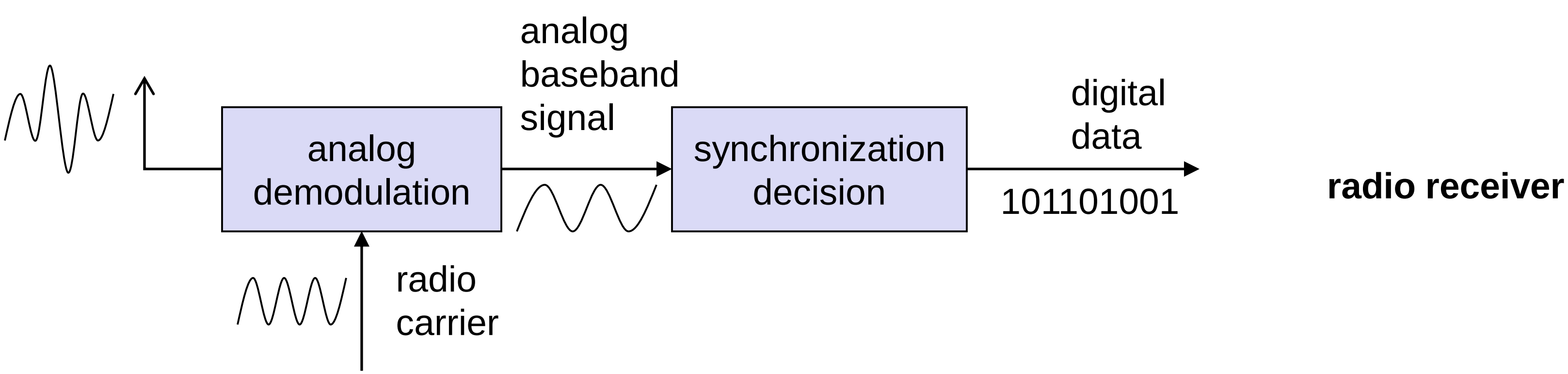


Modulation

- Digital modulation
  - digital data is translated into an analog signal (baseband)
  - ASK, FSK, PSK
  - differences in spectral efficiency, power efficiency, robustness
- Analog modulation
  - shifts center frequency of baseband signal up to the radio carrier
- Motivation
  - smaller antennas (e.g., $\lambda/4$)
  - Frequency Division Multiplexing
  - medium characteristics
- Basic schemes
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
  - Phase Modulation (PM)

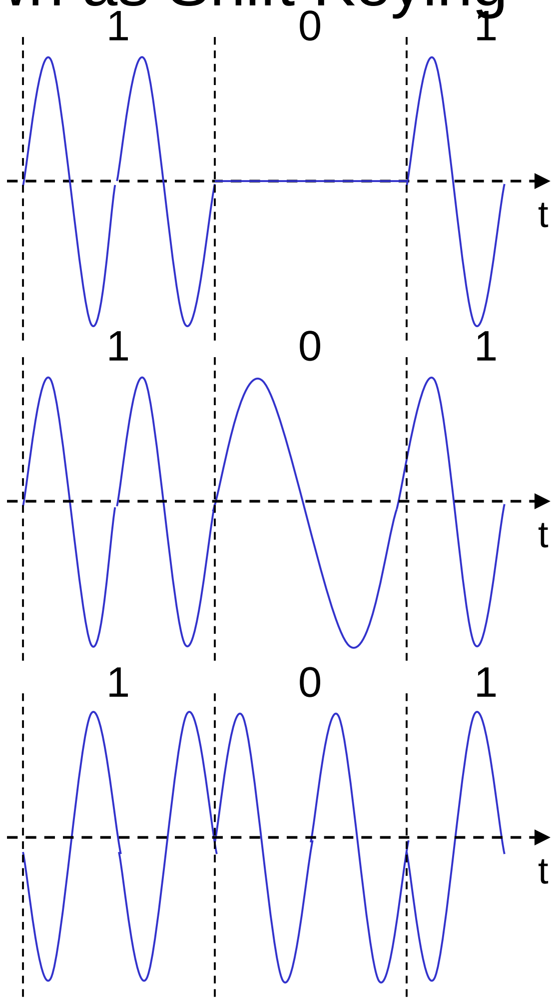
Modulation and demodulation





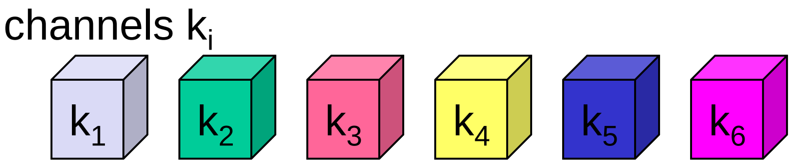
Digital modulation

- Modulation of digital signals known as Shift Keying
- Amplitude Shift Keying (ASK):
  - very simple
  - low bandwidth requirements
  - very susceptible to interference
- Frequency Shift Keying (FSK):
  - needs larger bandwidth
- Phase Shift Keying (PSK):
  - more complex
  - robust against interference
- Many advanced variants

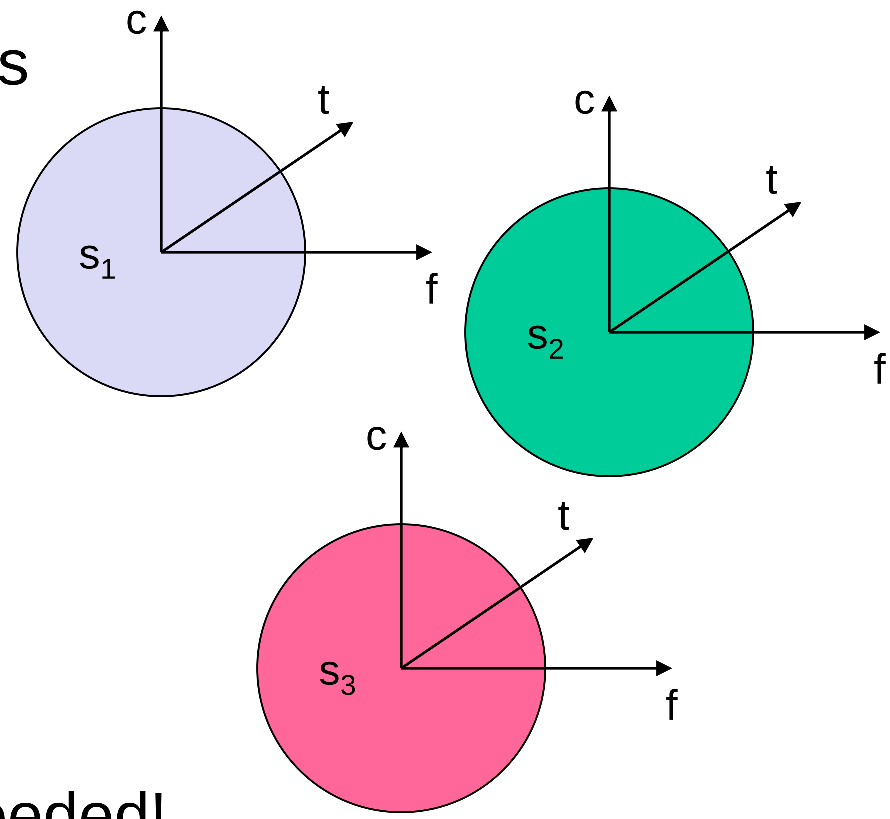


Multiplexing Mechanisms

Multiplexing



- Multiplexing in 4 dimensions
  - space (s_i)
  - time (t)
  - frequency (f)
  - code (c)



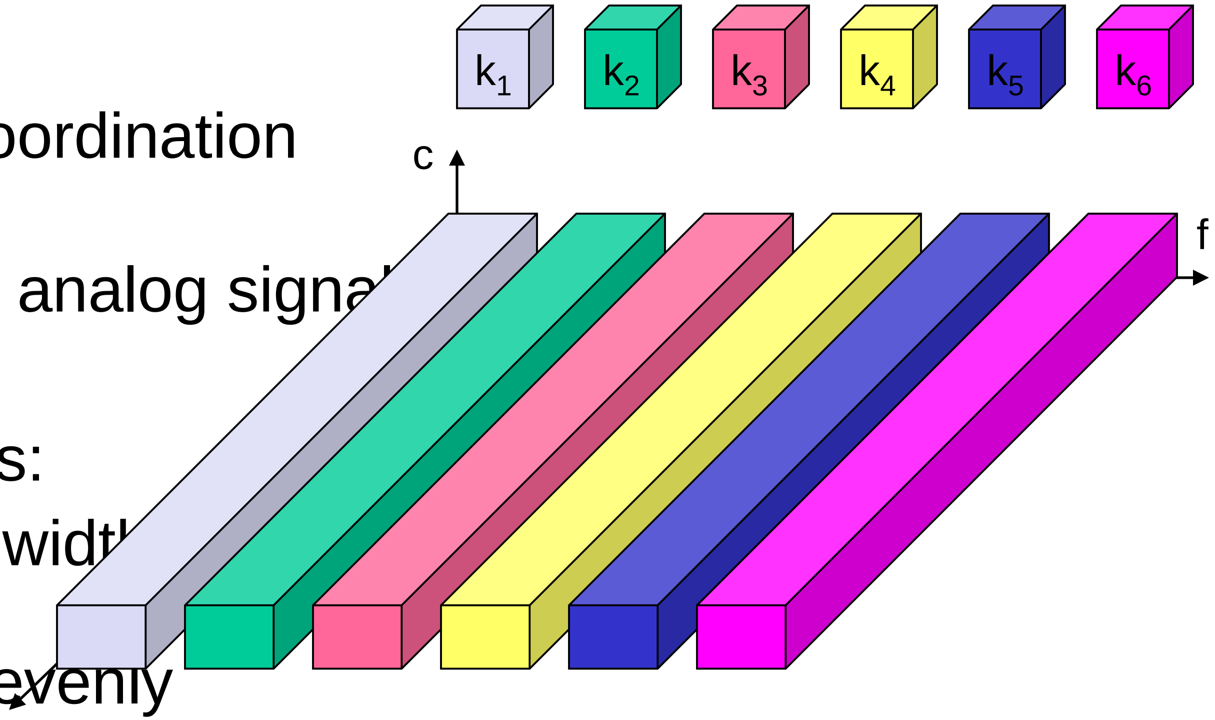
- Goal: multiple use of a shared medium

- Important: guard spaces needed!

Frequency multiplex

- Separation of the whole spectrum into smaller frequency bands
- A channel gets a certain band of the spectrum for the whole time
- Advantages:
- no dynamic coordination necessary
- works also for analog signals

- Disadvantages:
- waste of bandwidth if the traffic is distributed unevenly
- inflexible
- guard spaces

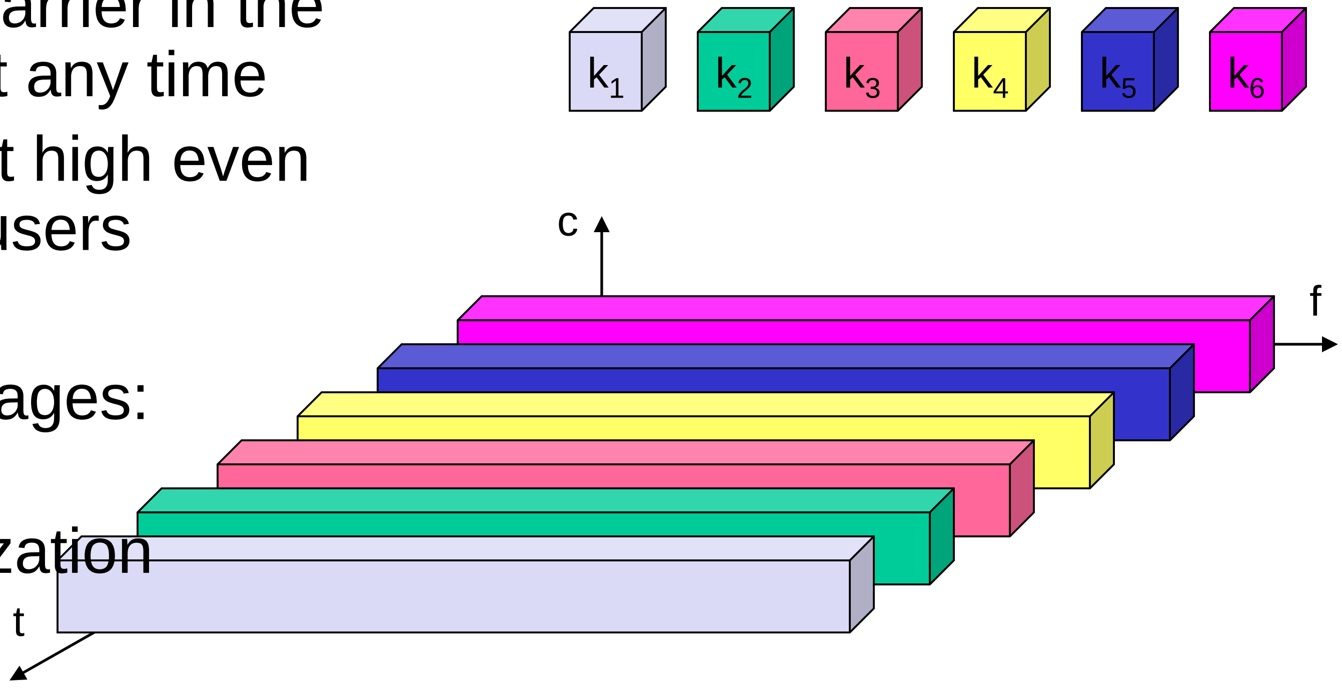


Time multiplex

- A channel gets the whole spectrum for a certain amount of time

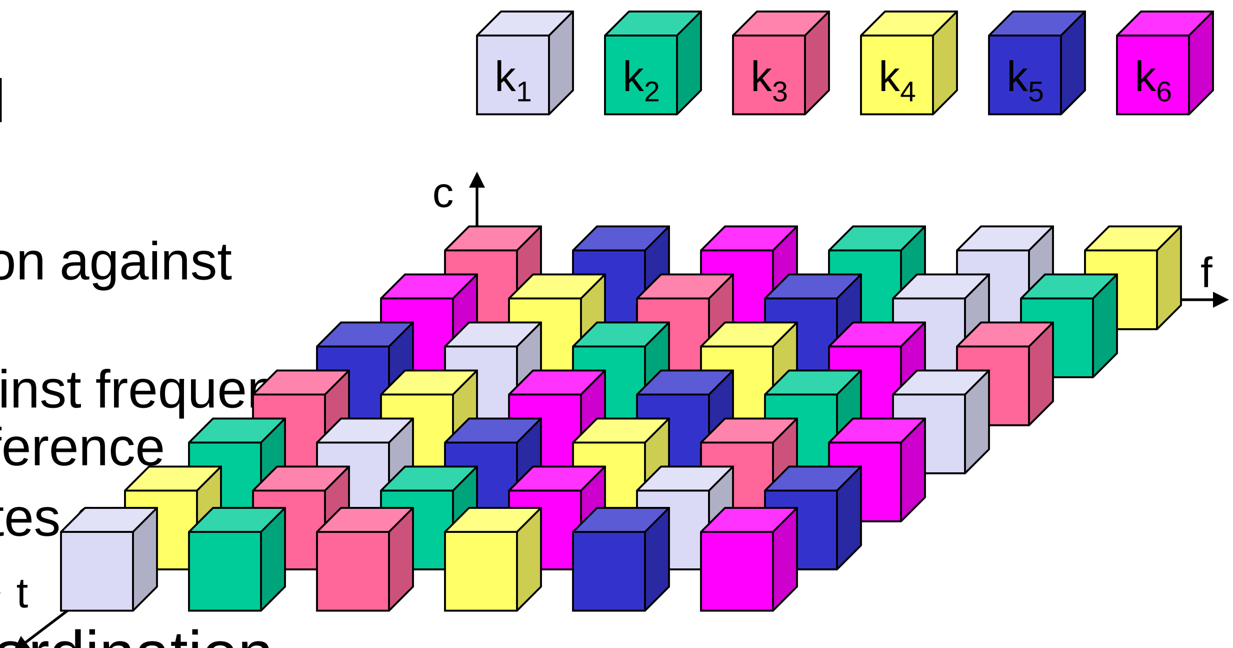
- Advantages:
- only one carrier in the medium at any time
- throughput high even for many users

- Disadvantages:
- precise synchronization necessary



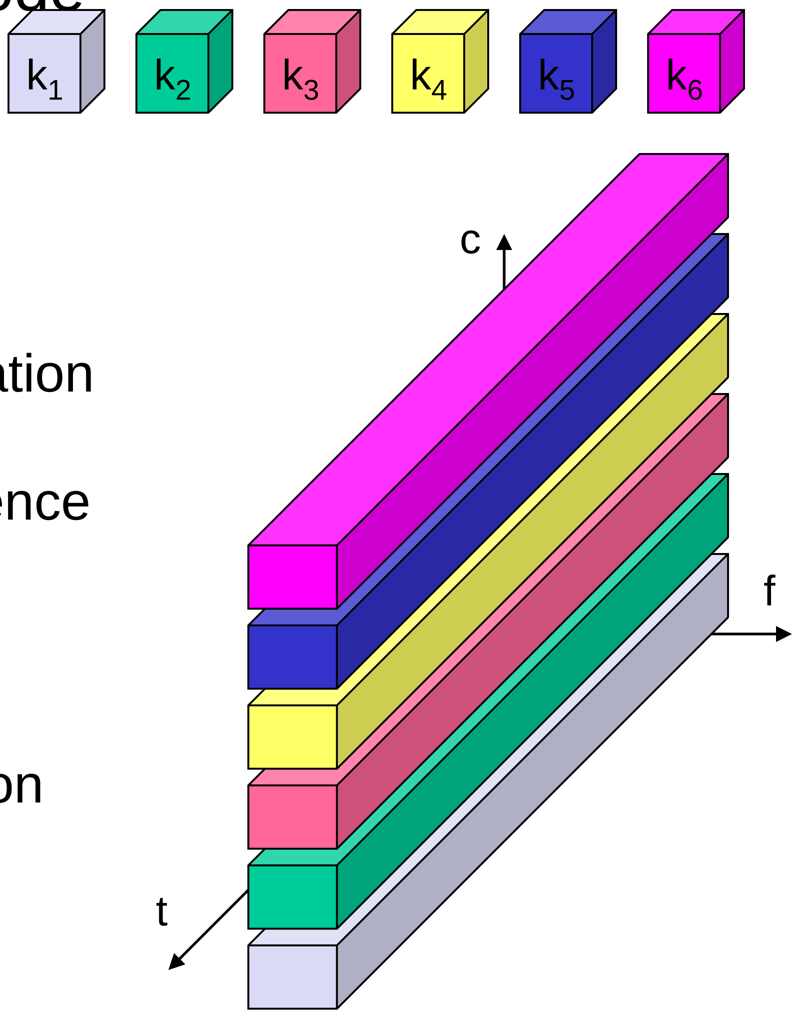
Time and frequency multiplex

- Combination of both methods
- A channel gets a certain frequency band for a certain amount of time
- Example: GSM
- Advantages:
  - better protection against tapping
  - protection against frequen selective interference
  - higher data rates compared to code multiplex
- but: precise coordination required



Code multiplex

- Each channel has a unique code
- All channels use the same spectrum at the same time
- Advantages:
  - bandwidth efficient
  - no coordination and synchronization necessary
  - good protection against interference and tapping
- Disadvantages:
  - lower user data rates
  - more complex signal regeneration
- Implemented using spread spectrum technology



CDMA Example

  - *D* = rate of data signal
  - Break each bit into *k chips*
    - Chips are a user-specific fixed pattern
  - Chip data rate of new channel = *kD*

- If *k*=6 and code is a sequence of 1s and -1s
  - For a '1' bit, A sends code as chip pattern
    - <c1, c2, c3, c4, c5, c6>
  - For a '0' bit, A sends complement of code
    - <-c1, -c2, -c3, -c4, -c5, -c6>
- Receiver knows sender's code and performs electronic decode function

$$S_u(d) = d1 \times c1 + d2 \times c2 + d3 \times c3 + d4 \times c4 + d5 \times c5 + d6 \times c6$$

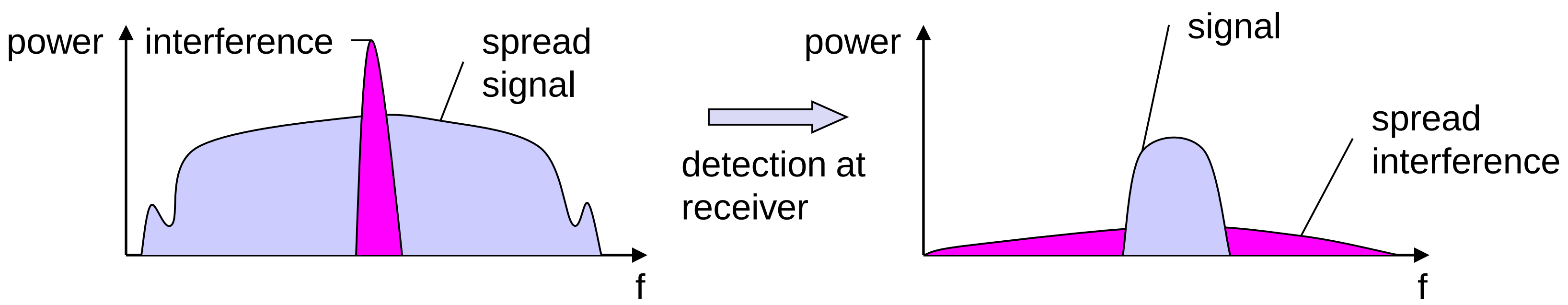
  - <d1, d2, d3, d4, d5, d6> = received chip pattern
  - <c1, c2, c3, c4, c5, c6> = sender's code

CDMA Example

- User A code = <1, –1, –1, 1, –1, 1>
  - To send a 1 bit = <1, –1, –1, 1, –1, 1>
  - To send a 0 bit = <–1, 1, 1, –1, 1, –1>
- User B code = <1, 1, –1, – 1, 1, 1>
  - To send a 1 bit = <1, 1, –1, –1, 1, 1>
- Receiver receiving with A's code
  - (A's code) x (received chip pattern)
    - User A '1' bit: 6 -> 1
    - User A '0' bit: -6 -> 0
    - User B '1' bit: 0 -> unwanted signal ignored

Spread spectrum technology

- Problem of radio transmission: frequency dependent fading can wipe out narrow band signals for duration of the interference
- Solution: spread the narrow band signal into a broad band signal using a special code - protection against narrow band interference



- Side effects:
  - coexistence of several signals without dynamic coordination
  - tap-proof
- Alternatives: Direct Sequence, Frequency Hopping

Spread-spectrum communications

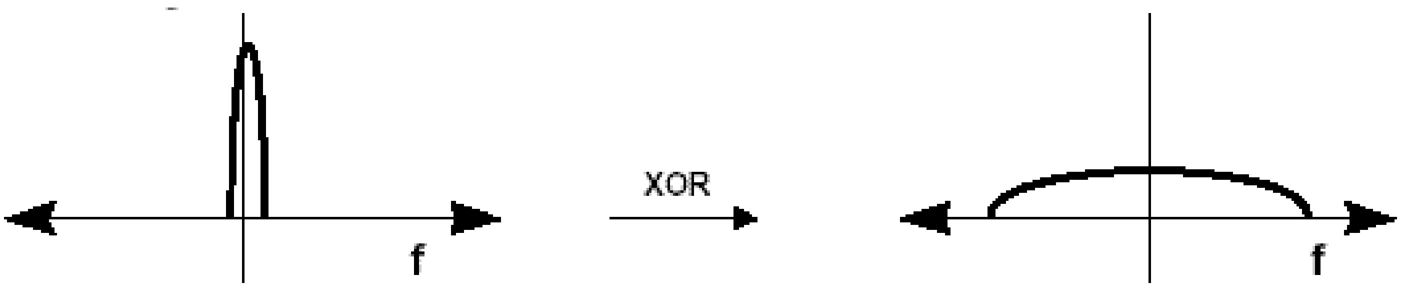


Figure 5a Effect of PN Sequence on Transmit Spectrum

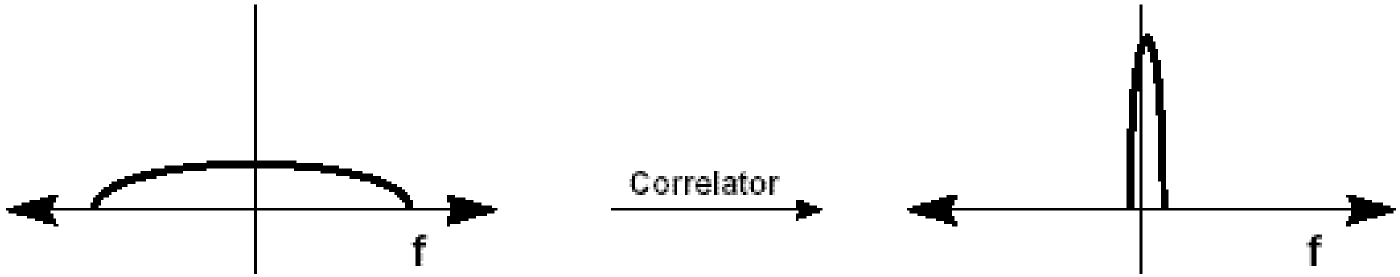
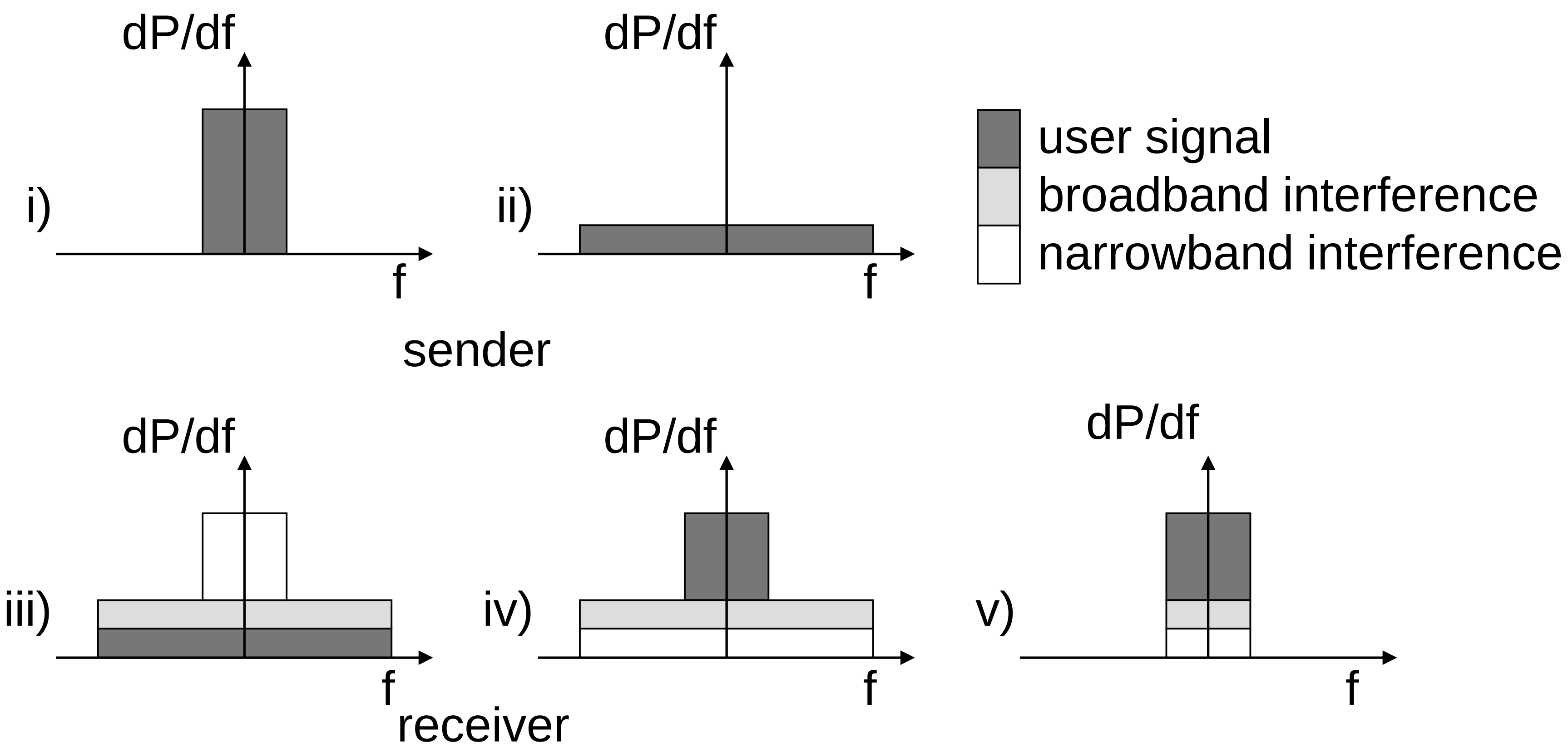


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

Source: Intersil

Effects of spreading and interference



DSSS properties

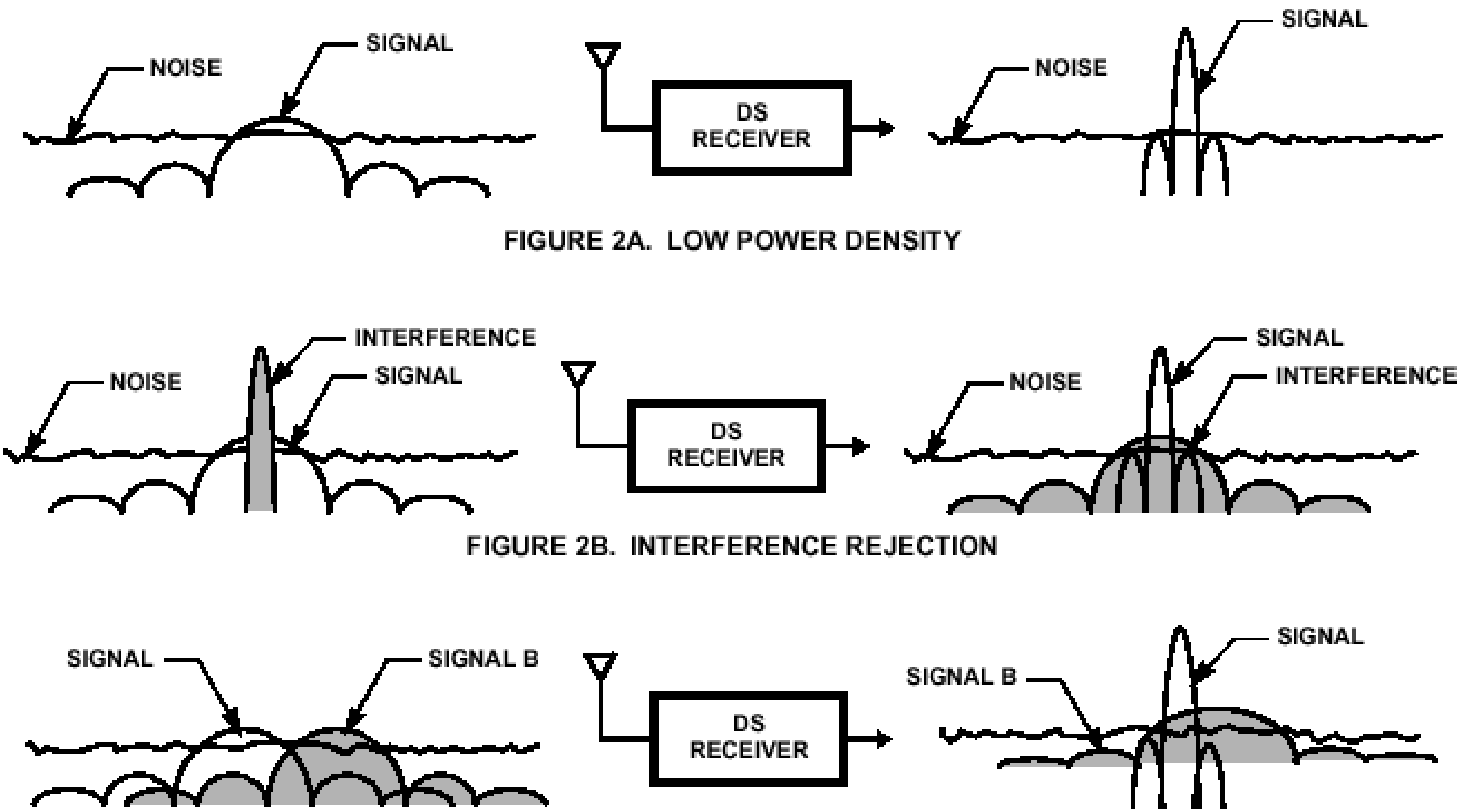


FIGURE 2A. LOW POWER DENSITY

FIGURE 2B. INTERFERENCE REJECTION

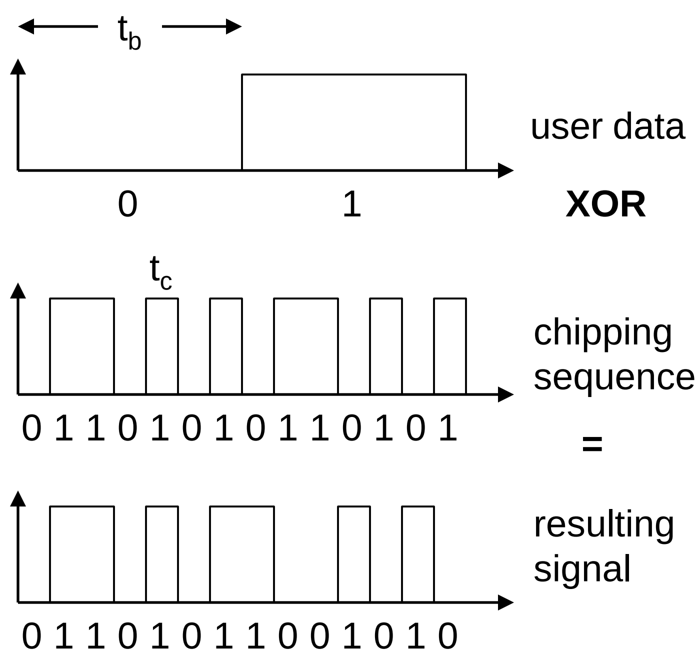
FIGURE 2C. MULTIPLE ACCESS

FIGURE 2. DIRECT SEQUENCE SPREAD SPECTRUM PROPERTIES

Source: Intersil

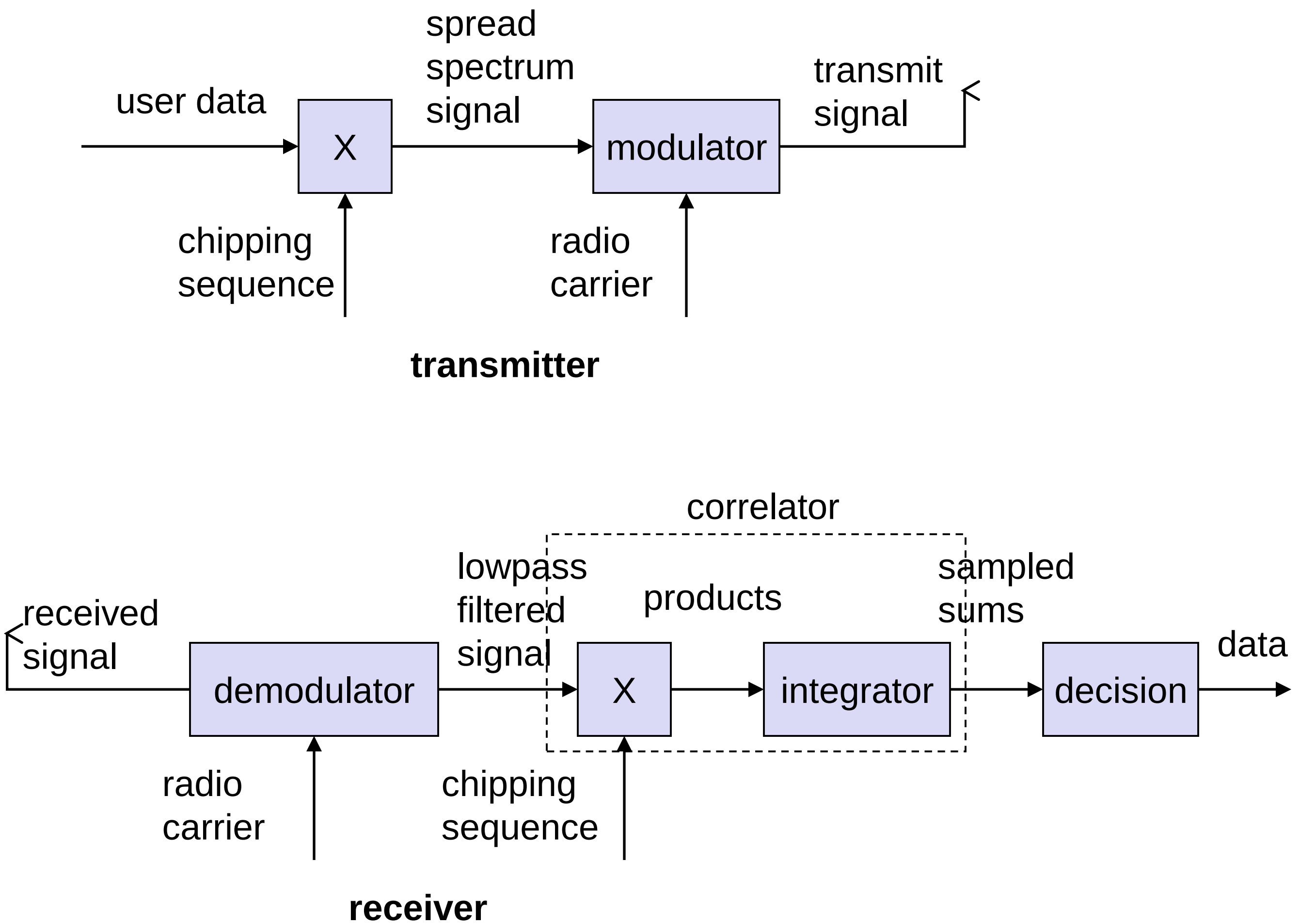
DSSS (Direct Sequence)

- XOR of the signal with pseudo-random number (chipping sequence)
  - many chips per bit (e.g., 128) result in higher bandwidth of the signal
- Advantages
  - reduces frequency selective fading
  - in cellular networks
    - base stations can use the same frequency range
    - several base stations can detect and recover the signal
    - soft handover
- Disadvantages
  - precise power control necessary



t_b: bit period
t_c: chip period

DSSS Transmit/Receive



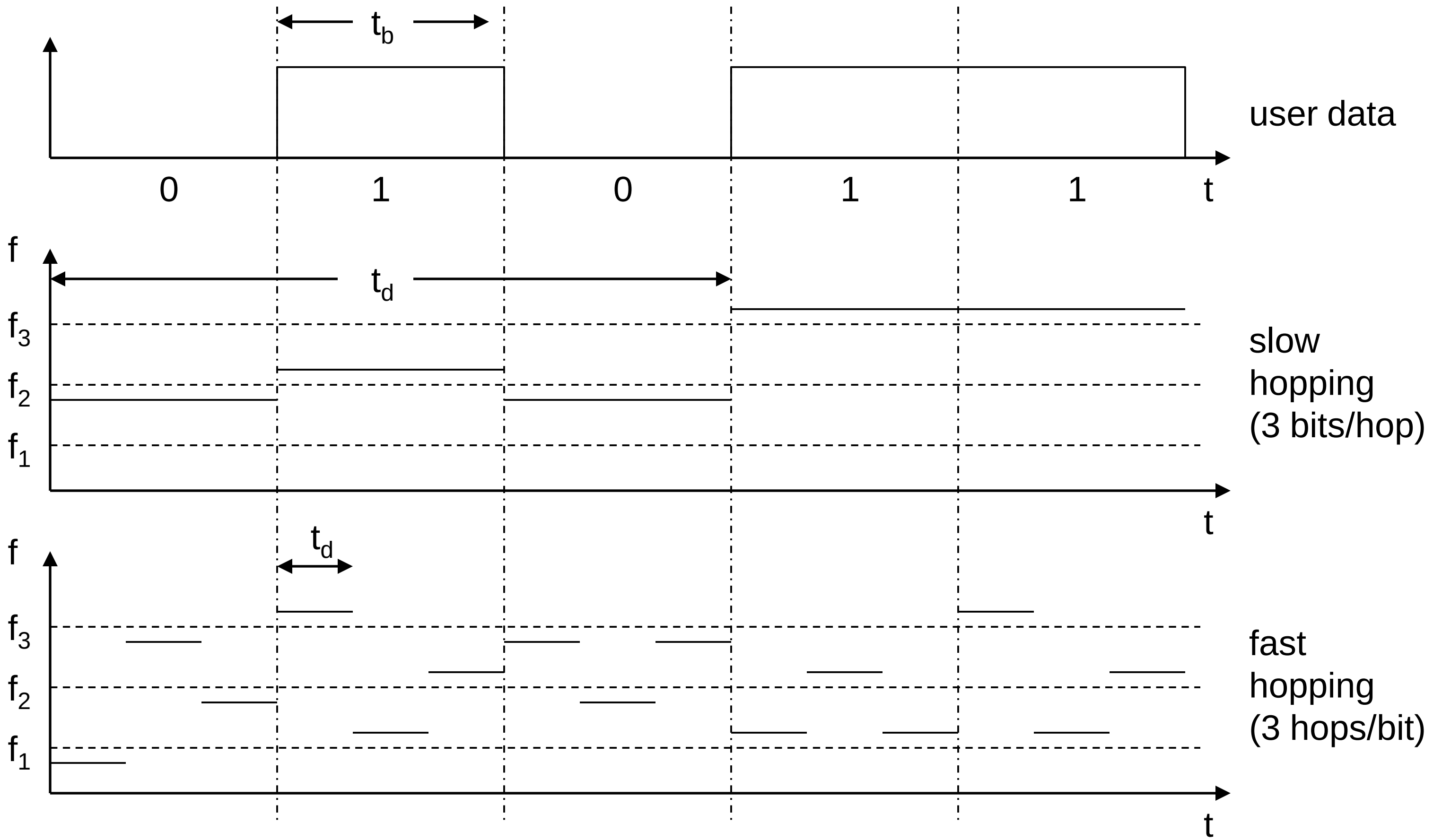
Frequency Hopping Spread Spectrum (FHSS)

- Signal is broadcast over seemingly random series of radio frequencies
- Signal hops from frequency to frequency at fixed intervals
- Channel sequence dictated by spreading code
- Receiver, hopping between frequencies in synchronization with transmitter, picks up message
- Advantages
  – Eavesdroppers hear only unintelligible blips
  – Attempts to jam signal on one frequency succeed only at knocking out a few bits

FHSS (Frequency Hopping)

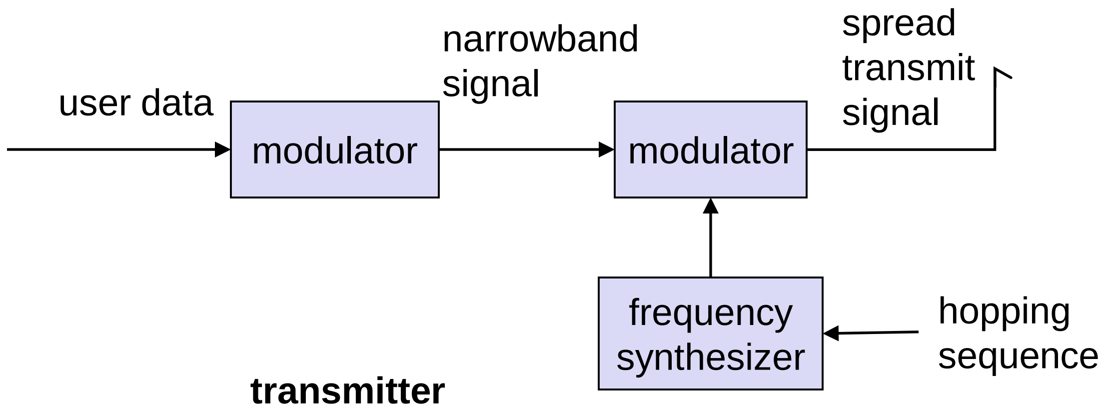
- Discrete changes of carrier frequency
  - sequence of frequency changes determined via pseudo random number sequence
- Two versions
  - Fast Hopping: several frequencies per user bit
  - Slow Hopping: several user bits per frequency
- Advantages
  - frequency selective fading and interference limited to short period
  - simple implementation
  - uses only small portion of spectrum at any time
- Disadvantages
  - not as robust as DSSS
  - simpler to detect

Slow and Fast FHSS

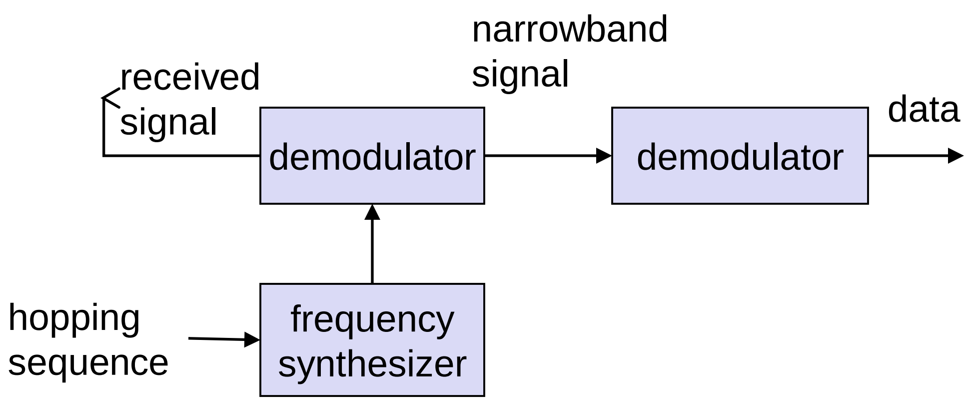


t_b: bit period t_d: dwell time

FHSS Transmit/Receive



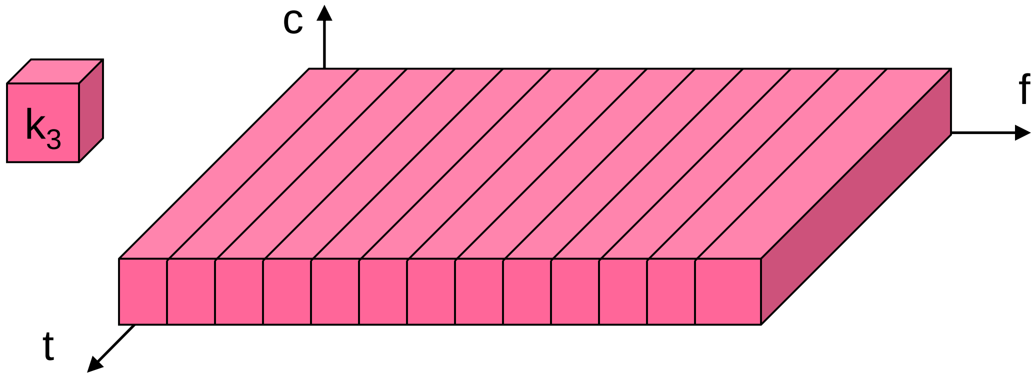
transmitter



receiver

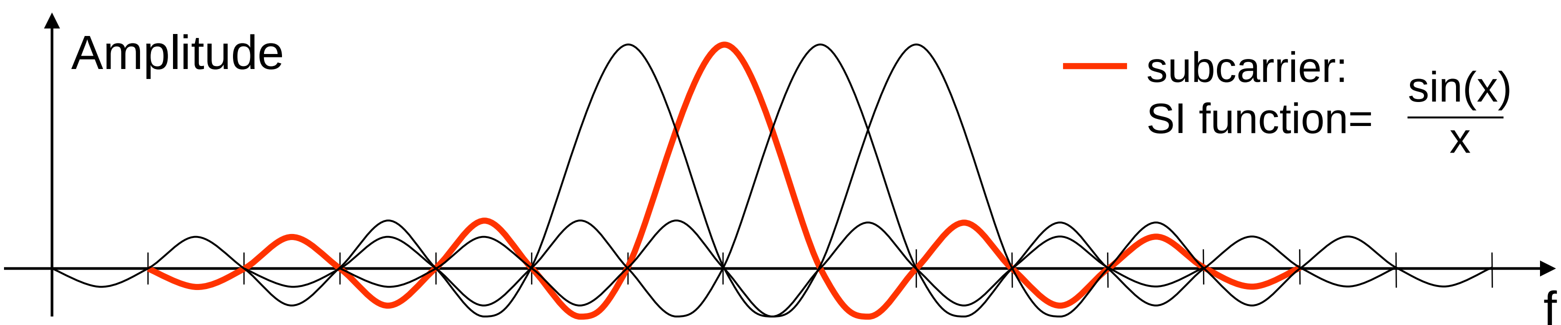
OFDM (Orthogonal Frequency Division)

- Parallel data transmission on several orthogonal subcarriers with lower rate



Maximum of one subcarrier frequency appears exactly at a frequency where all other subcarriers equal zero

- superposition of frequencies in the same frequency range



OFDM

- Properties
  - Lower data rate on each subcarrier ➔ less ISI
  - interference on one frequency results in interference of one subcarrier only
  - no guard space necessary
  - orthogonality allows for signal separation via inverse FFT on receiver side
  - precise synchronization necessary (sender/receiver)
- Advantages
  - no equalizer necessary
  - no expensive filters with sharp edges necessary
  - better spectral efficiency (compared to CDM)
- Application
  - 802.11a, HiperLAN2, ADSL

ALOHA

Stations transmit whenever they have data to send

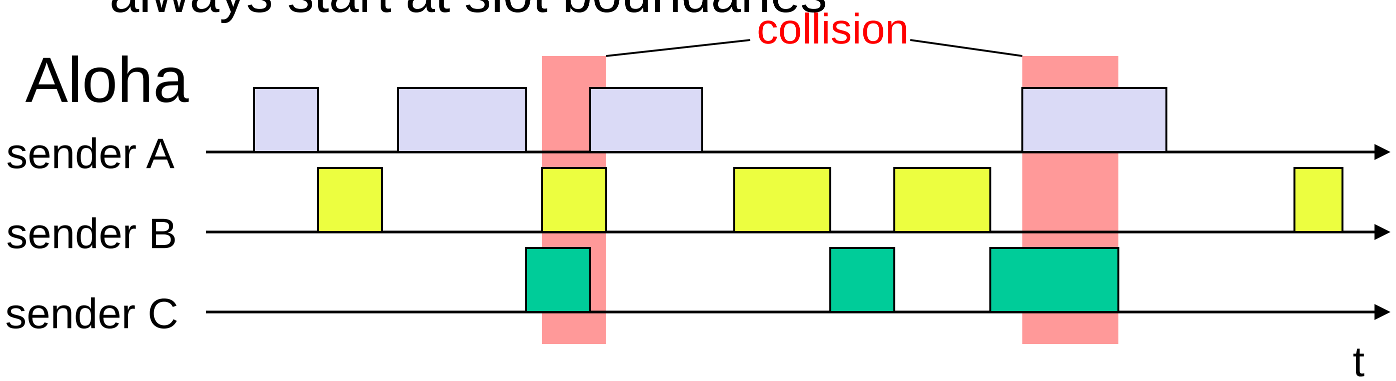
- Detect collision or wait for acknowledgment
- If no acknowledgment (or collision), try again after a random waiting time

Collision: If more than one node transmits at the same time

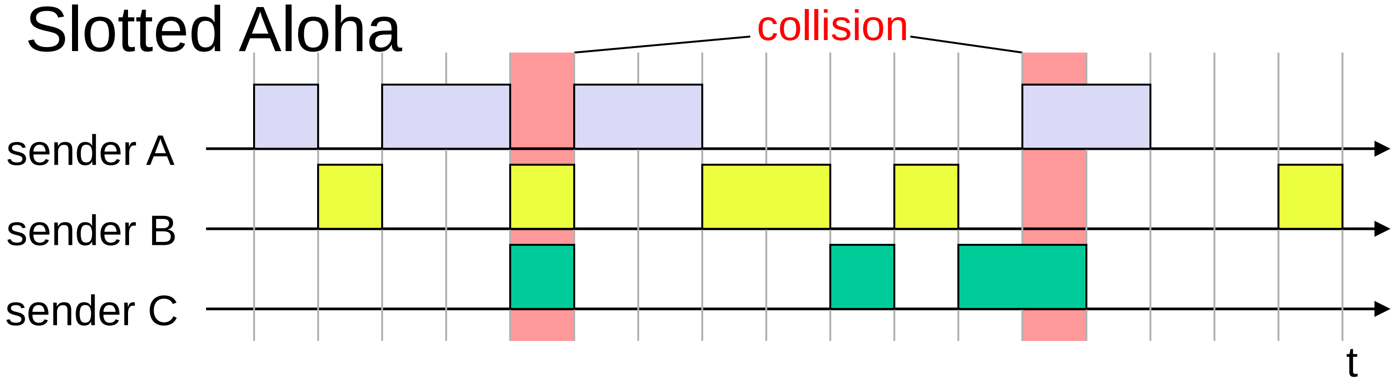
If there is a collision, all nodes have to re-transmit packets

Aloha/slotted Aloha

- Mechanism
  - random, distributed (no central arbiter), time-multiplex
  - Slotted Aloha additionally uses time-slots, sending must always start at slot boundaries
- Aloha



- Slotted Aloha



Slotted Aloha

- Time is divided into slots
  - *slot = one packet transmission time at least*
- Master station generates *synchronization pulses* for time-slots
- Station waits till beginning of slot to transmit

- *Vulnerability Window* reduced from 2T to T; *goodput* doubles

Error control

Bit level error detection/correction

Single-bit, multi-bit or burst errors introduced due to channel noise

- Detected using redundant information sent along with data

- Full Redundancy:
  - Send everything twice
  - Simple but inefficient
- Common Schemes:
  - Parity
  - Cyclic Redundancy Check (CRC)
  - Checksum

Error detection process

- Transmitter
  – For a given frame, an error-detecting code (check bits) is calculated from data bits
  – Check bits are appended to data bits
- Receiver
  – Separates incoming frame into data bits and check bits
  – Calculates check bits from received data bits
  – Compares calculated check bits against received check bits
  – Detected error occurs if mismatch

Frame level error correction

- Problems in transmitting a sequence of frames over a lossy link
  - frame damage, loss, reordering, duplication, insertion
- Solutions:
  - Forward Error Correction (FEC)
    - Use of redundancy for packet level error correction
    - Block Codes, Turbo Codes
  - Automatic Repeat Request (ARQ)
    - Use of acknowledgements and retransmission
    - Stop and Wait; Sliding Window

Block Code (Error Correction)

- Hamming distance – for 2 *n*-bit binary sequences, the number of different bits
  - E.g., v_1=011011; v_2=110001; d(v1, v_2)=3
- For each data block, create a codeword
- Send the codeword
- If the code is invalid, look for data with shortest hamming distance (possibly correct code)

Datablock (k=2)	Codeword (n=5)
00	00000
01	00111
10	11001
11	11110

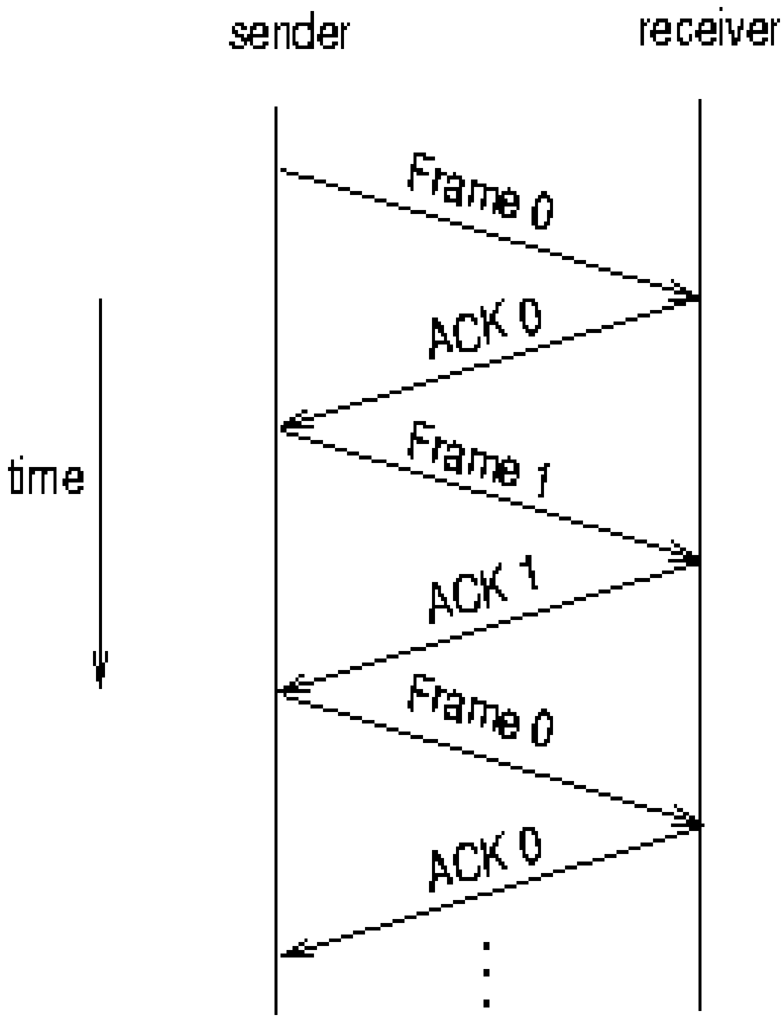
Suppose you receive codeword 00100 (error)

Closest is 00000 (only one bit different)

- Efficient version: Turbo Codes

Stop and Wait ARQ

- Sender waits for ACK (acknowledgement) after transmitting each frame; keeps copy of last frame.
- Receiver sends ACK if received frame is error free.
- Sender retransmits frame if ACKnot received before timer expires.
- Simple to implement but may waste bandwidth.



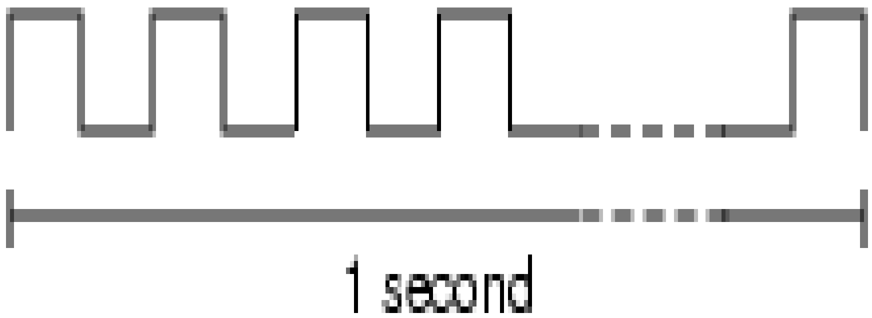
- Efficient Version: Sliding Window

Bandwidth and Delay

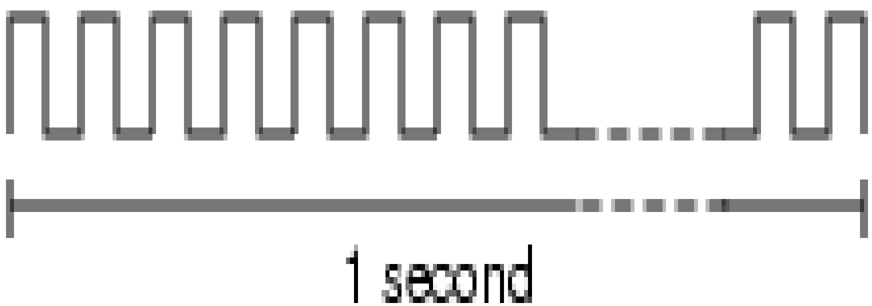
Bandwidth

- Amount of data that can be transmitted per unit time
  - expressed in cycles per second, or Hertz (Hz) for analog devices
  - expressed in bits per second (bps) for digital devices
  - KB = 2^10 bytes; Mbps = 10^6 bps
- Link v/s End-to-End

Bandwidth v/s bit width



1Mbps
(each bit 1 microseconds wide)



2 Mbps
(each bit 0.5 microseconds wide)

Latency (delay)

- Time it takes to send message from point A to point B
  - Latency = Propagation + Transmit + Queue
  - Propagation = Distance / SpeedOfLight
  - Transmit = Size / Bandwidth

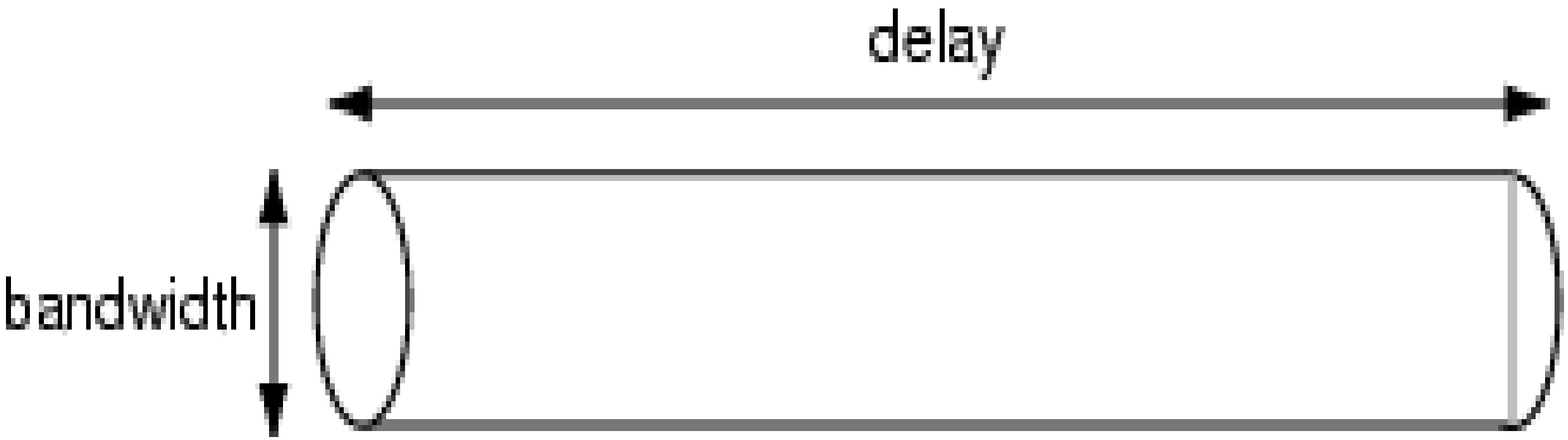
- Queueing not relevant for direct links
- Bandwidth not relevant if Size = 1 bit
- Software overhead can dominate when Distance is small

- RTT: round-trip time

Delay X Bandwidth product

- Relative importance of bandwidth and delay
- Small message: 1ms vs 100ms dominates 1Mbps vs 100Mbps
- Large message: 1Mbps vs 100Mbps dominates 1ms vs 100ms

Delay X Bandwidth product



100ms RTT and 45Mbps Bandwidth = 560 KB of data

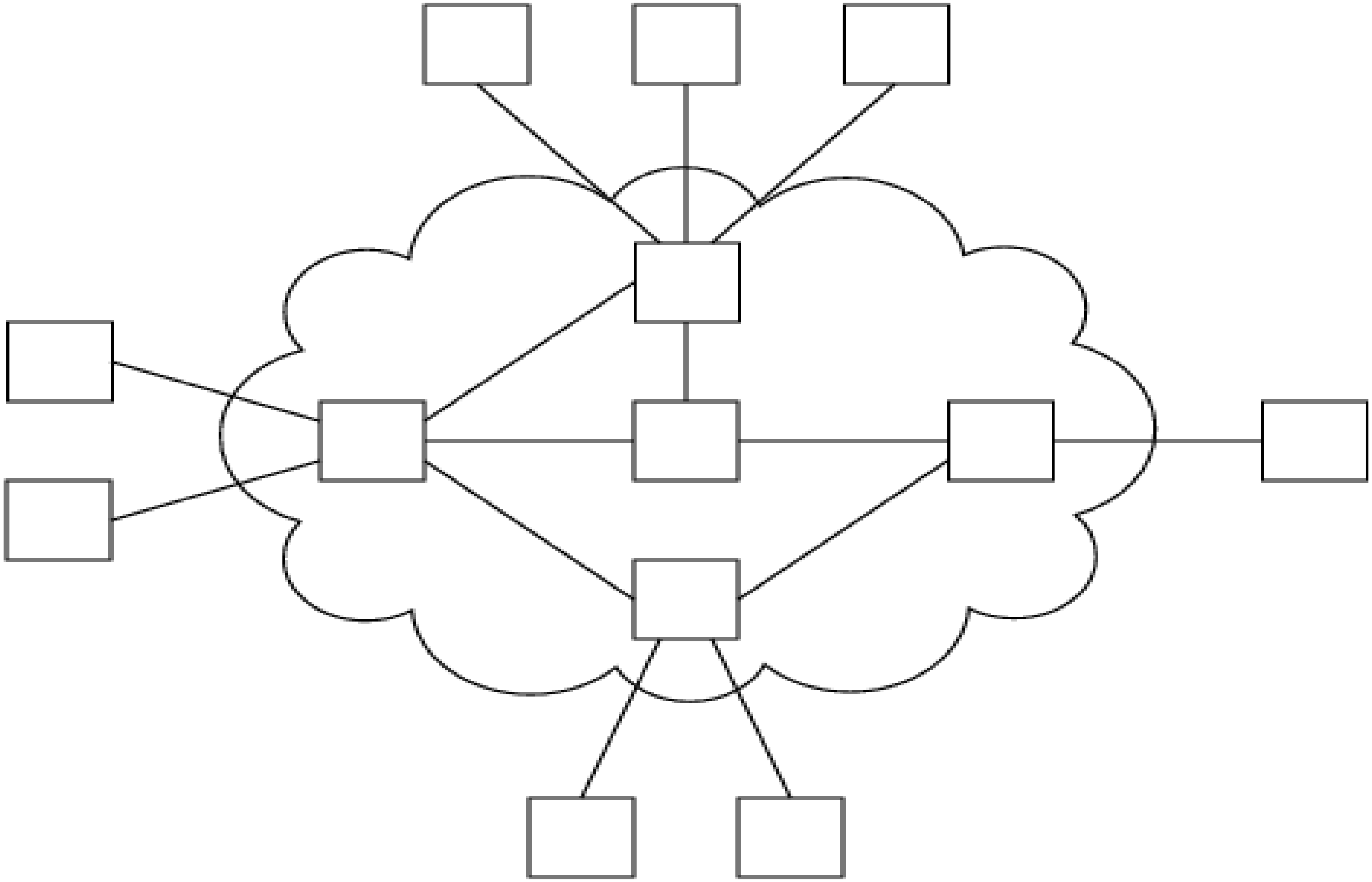
TCP/IP Basics

Interconnection devices

Basic Idea: Transfer data from input to output

- Repeater
  - Amplifies the signal received on input and transmits it on output
- Switch
  - Reads destination address of each packet and forwards appropriately to specific port
  - Layer 3 switches (IP switches) also perform routing functions
- Router
  - decides routes for packets, based on destination address and network topology
  - Exchanges information with other routers to learn network topology

Switched networks



TCP/IP layers

- Physical Layer:
  - Transmitting bits over a channel.
  - Deals with electrical and procedural interface to the transmission medium.

- Data Link Layer:
  - Transform the raw physical layer into a `link' for the higher layer.
  - Deals with framing, error detection, correction and multiple access.

TCP/IP layers (contd.)

- Network Layer:
  - Addressing and routing of packets.
  - Deals with subnetting, route determination.

- Transport Layer:
  - end-to-end connection characteristics.
  - Deals with retransmissions, sequencing and congestion control.

TCP/IP layers (contd.)

- Application Layer:
  - ``application'' protocols.
  - Deals with providing services to users and application developers.
- Protocols are the building blocks of a network architecture.

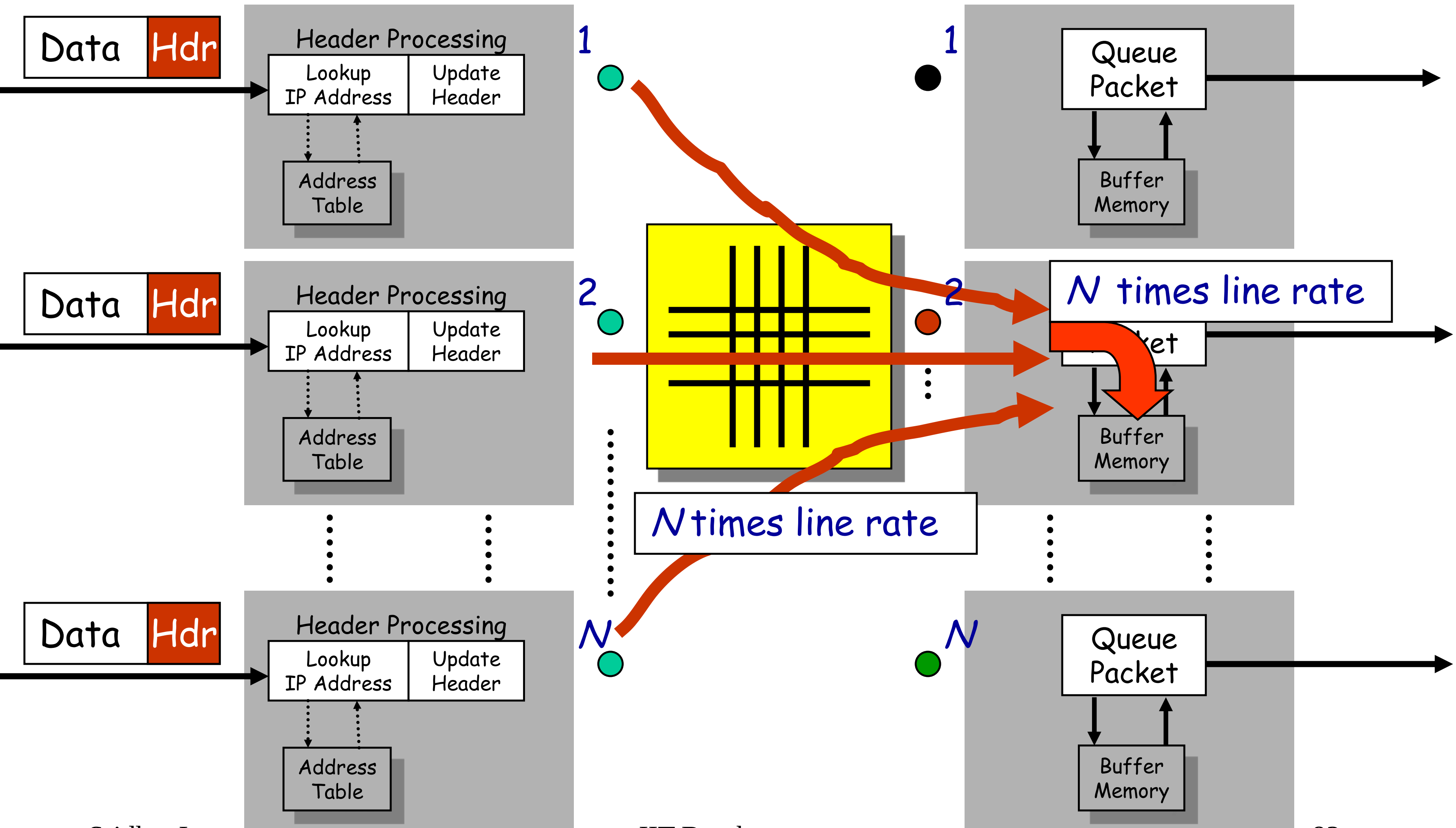
Lower layer services

- Unacknowledged connectionless service
  - No acknowledgements, no connection
  - Error recovery up to higher layers
  - For low error-rate links or voice traffic

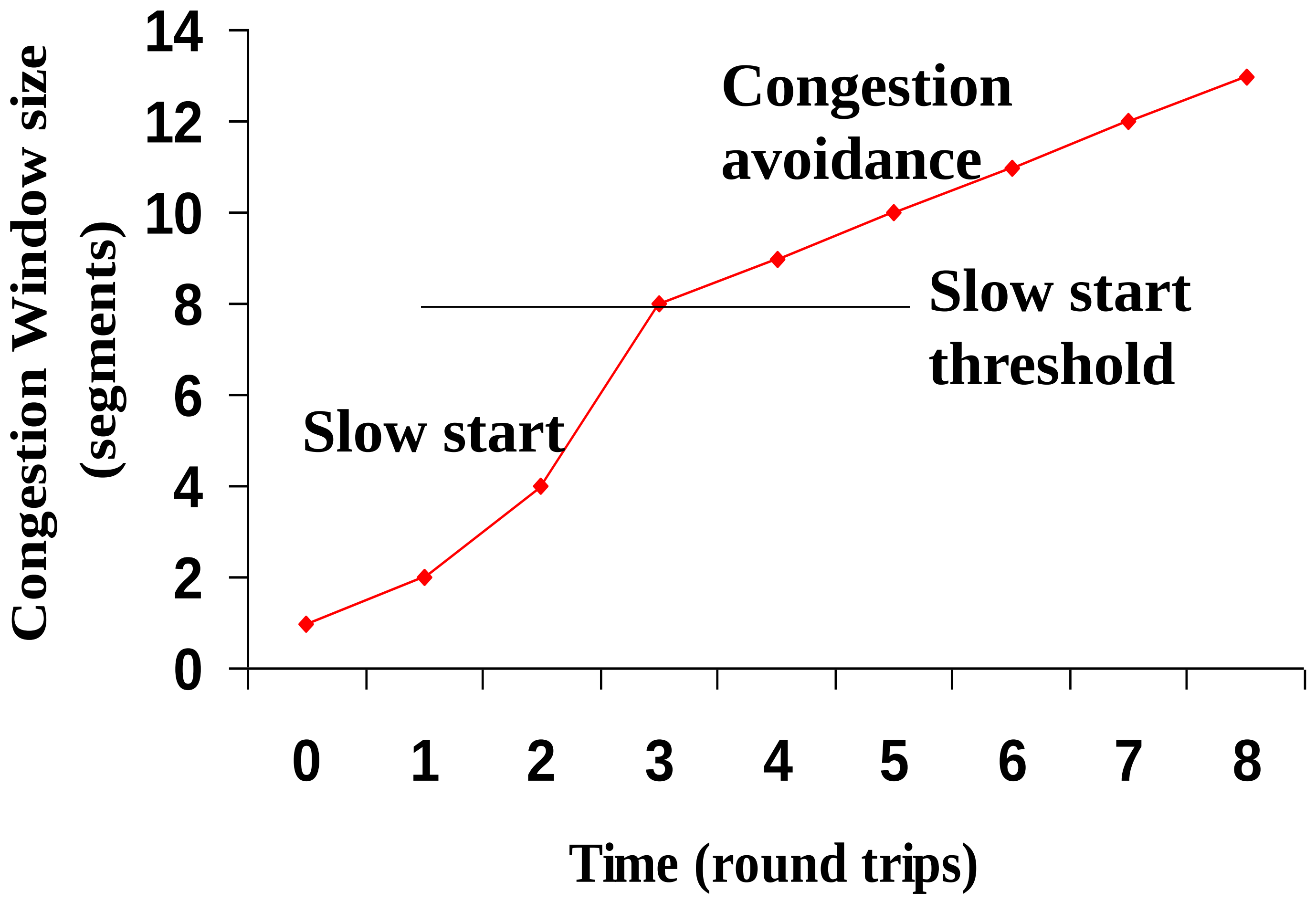
- Acknowledged connectionless service
  - Acknowledgements improve reliability
  - For unreliable channels. e.g.: wireless systems

- Acknowledged connection-oriented service
  - Equivalent of reliable bit-stream; in-order delivery
  - Connection establishment and release
  - Inter-router traffic

Generic router architecture

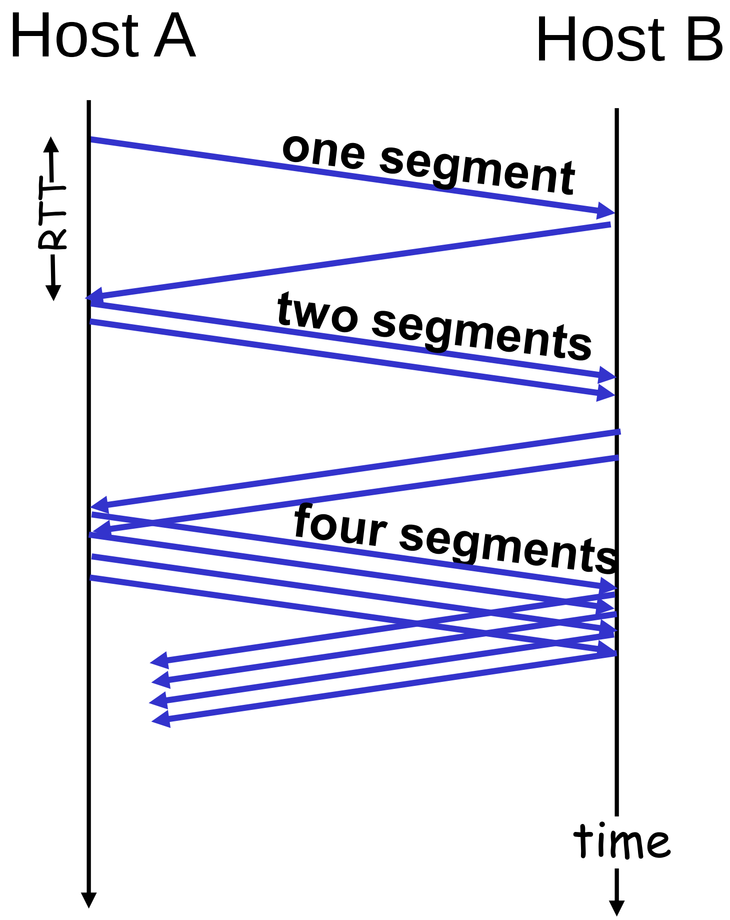


Typical TCP behaviour



Slow start phase

- initialize:
  - Cwnd = 1
- for (each ACK)
  - Cwnd++
- until
  - loss detection OR
  - Cwnd > ssthresh



Congestion avoidance phase

/* Cwnd > threshold */

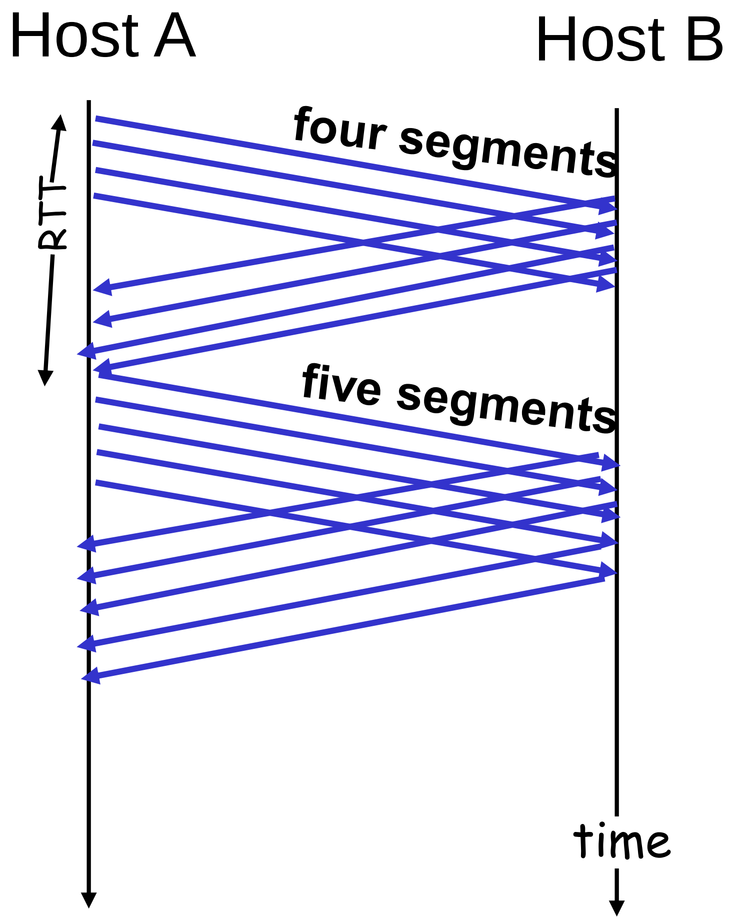
- Until (loss detection) {

  every w ACKs:

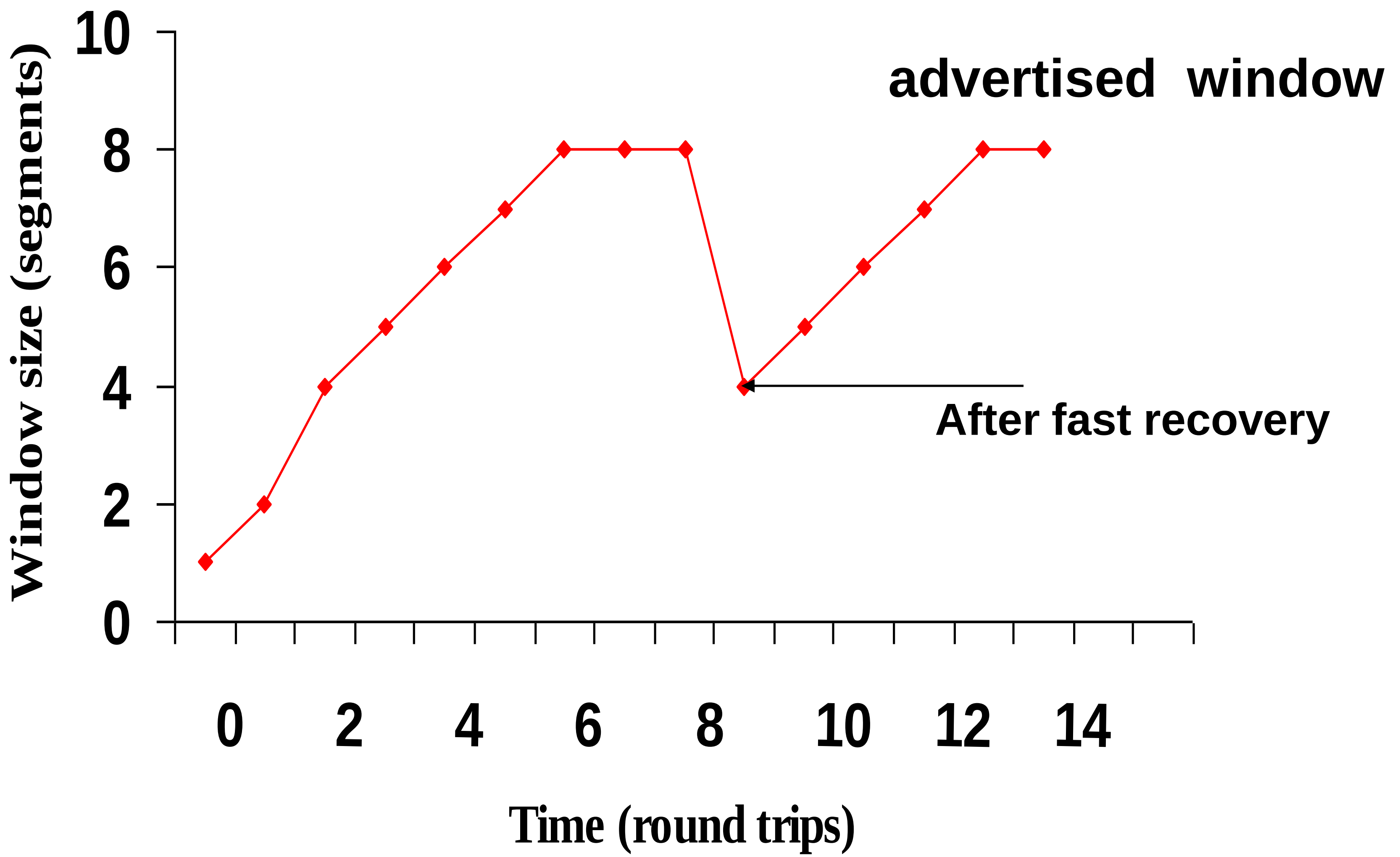
  Cwnd++

  }
- ssthresh = Cwnd/2
- Cwnd = 1
- perform slow start

1



TCP: Fast retransmit and Fast recovery



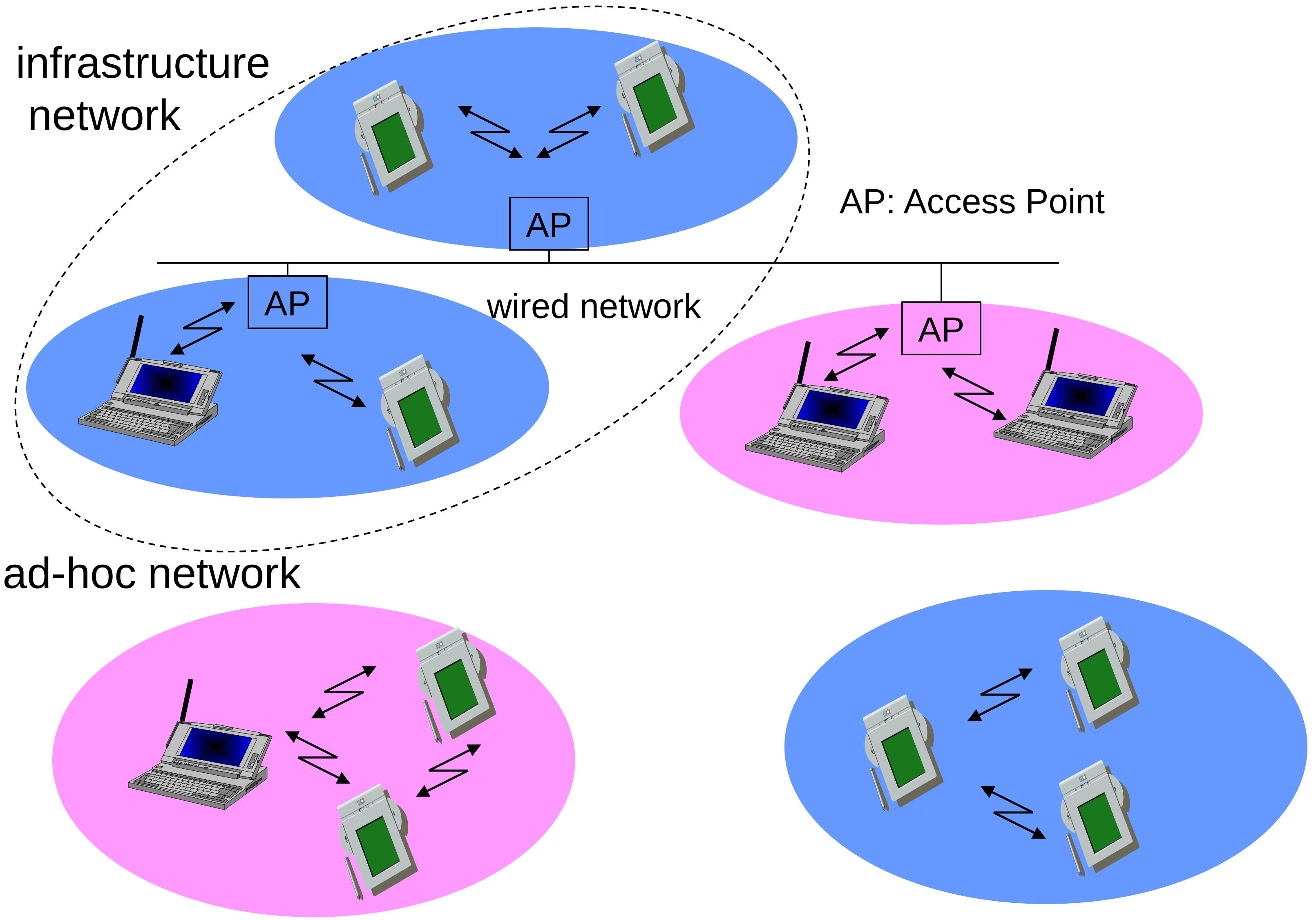
802.11 (WiFi) Overview

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

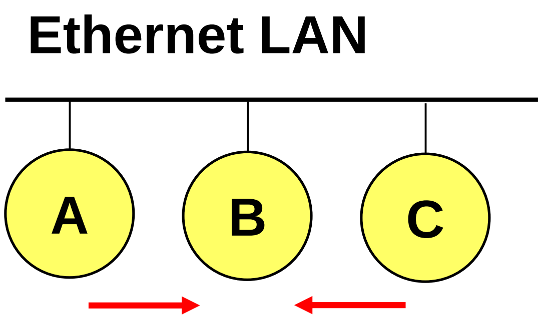
- Infrastructure v/s ad-hoc networks (802.11)

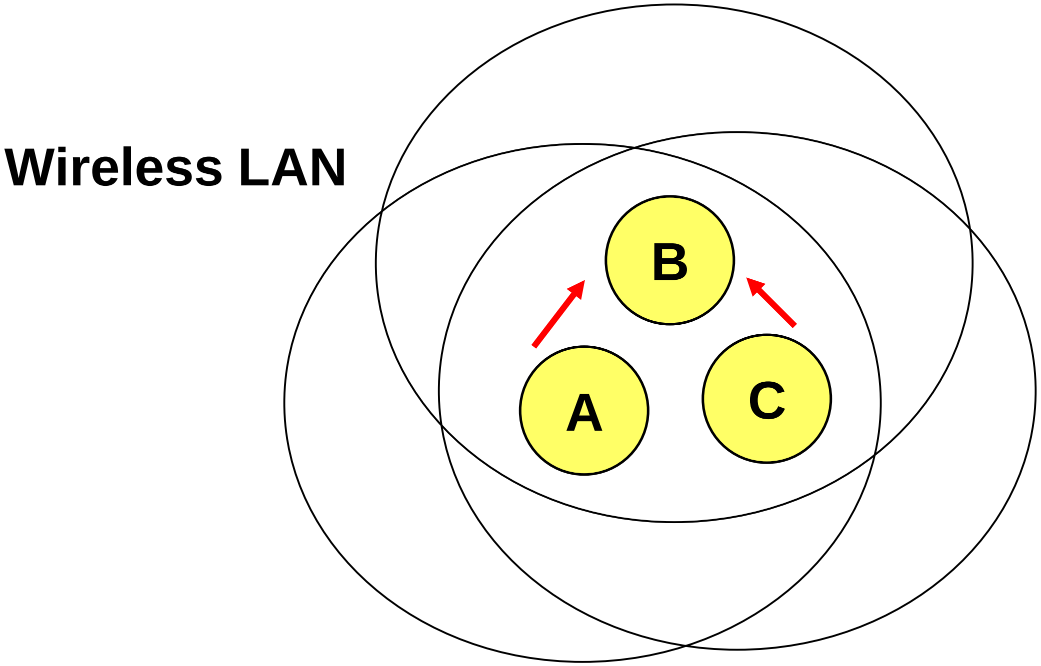
Infrastructure vs. Ad hoc networks



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.

Carrier Sense Multiple Access (CSMA)

- Listen before you speak
- Check whether the medium is active before sending a packet (i.e *carrier sensing*)
- If medium idle, then transmit
- If collision happens, then detect and resolve

- If medium is found busy, transmission follows:
  - 1- persistent
  - P- persistent
  - Non-persistent

Collision detection (CSMA/CD)

- All aforementioned scheme can suffer from collision
- Device can detect collision
  - Listen while transmitting
  - Wait for 2 * propagation delay
- On collision detection wait for random time before retrying
- Binary Exponential Backoff Algorithm
  - Reduces the chances of two waiting stations picking the same random time

Binary Exponential Backoff

1.On detecting 1st collision for packet x

station A chooses a number r between 0 and 1.

wait for r * slot time and transmit.

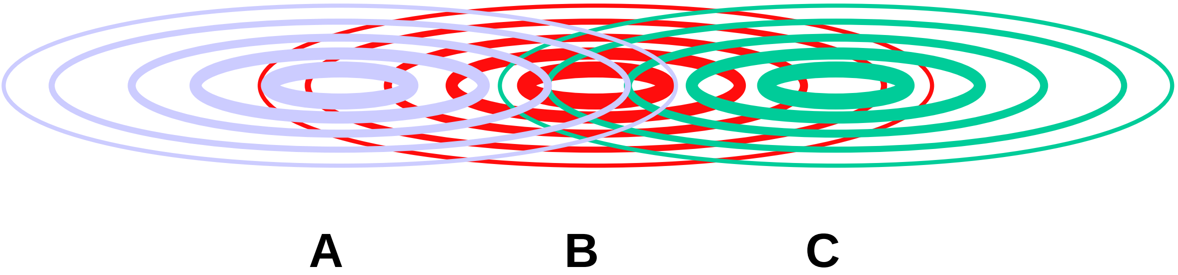
Slot time is taken as 2 * propagation delay

k. On detecting kth collision for packet x

choose r between 0,1,..,(2^k –1)

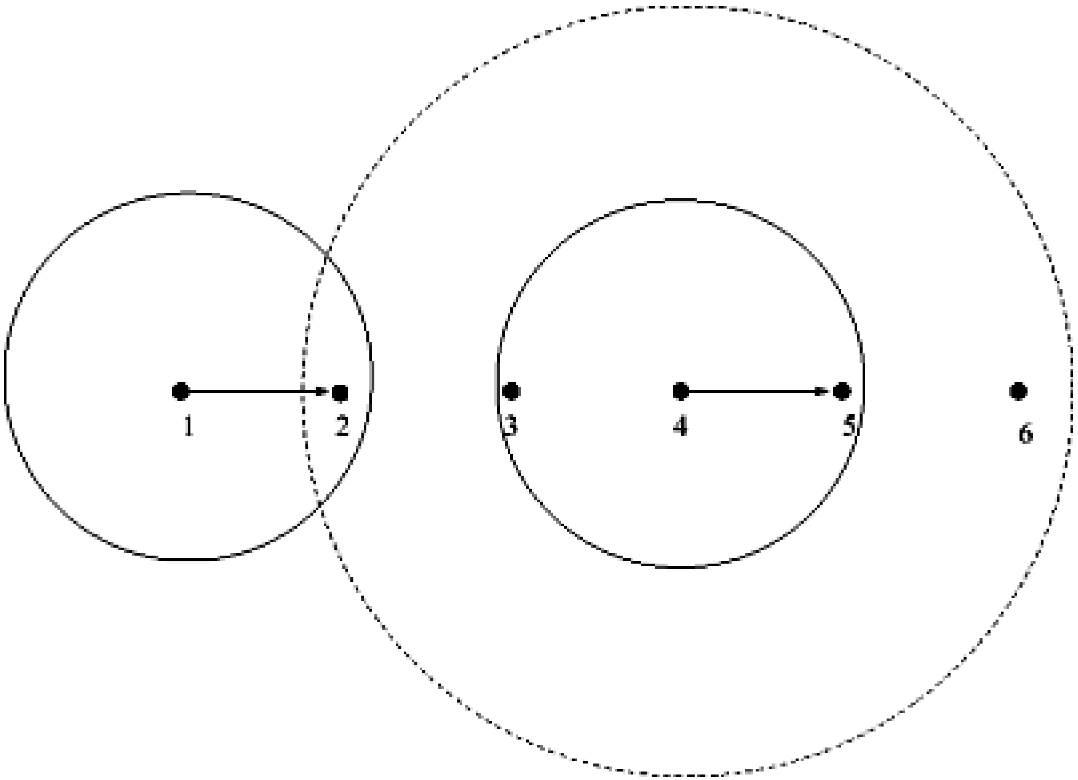
- When value of k becomes high (10), give up.
- Randomization increase with larger window, but delay increases.

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.

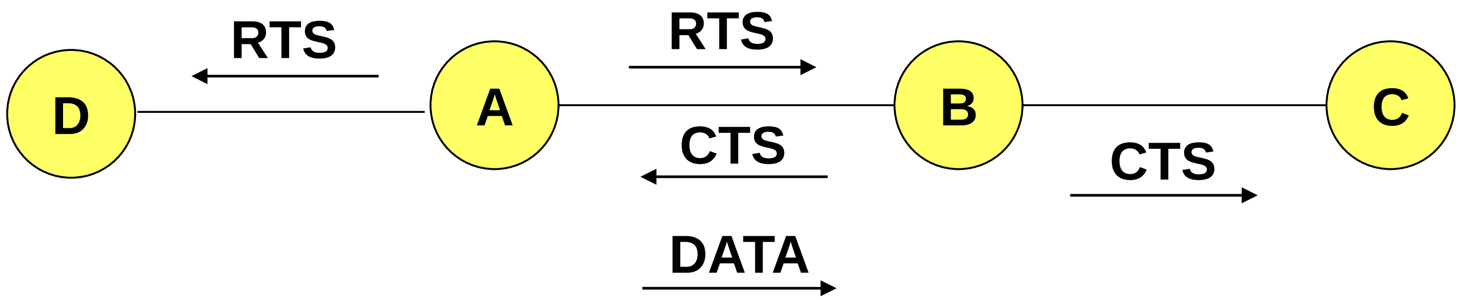
Effect of interference range



Transmission from 1 ⇒ 2 will fail

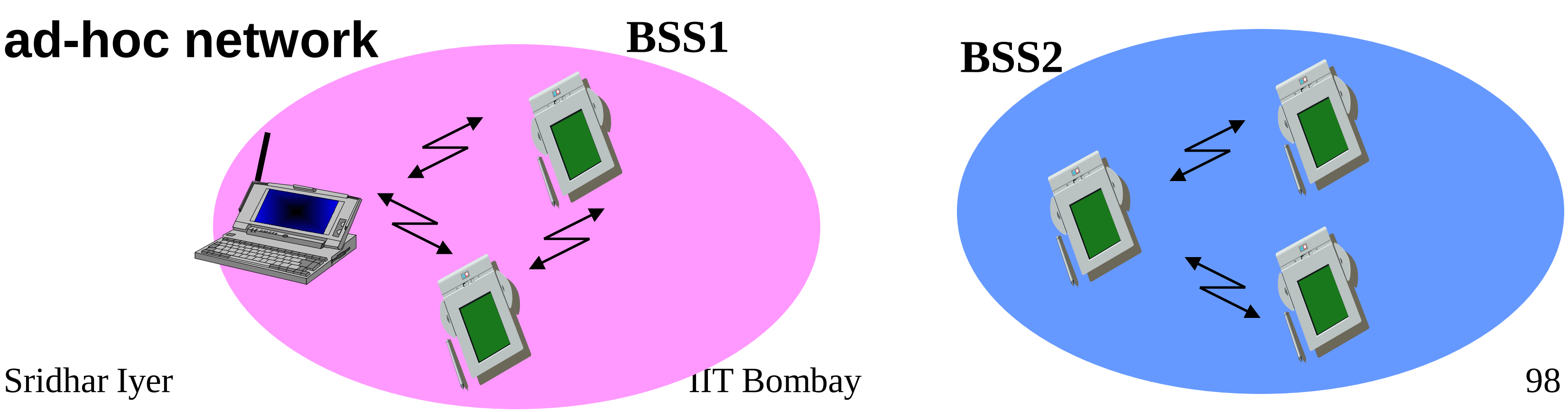
Solution for Hidden Terminals

- 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

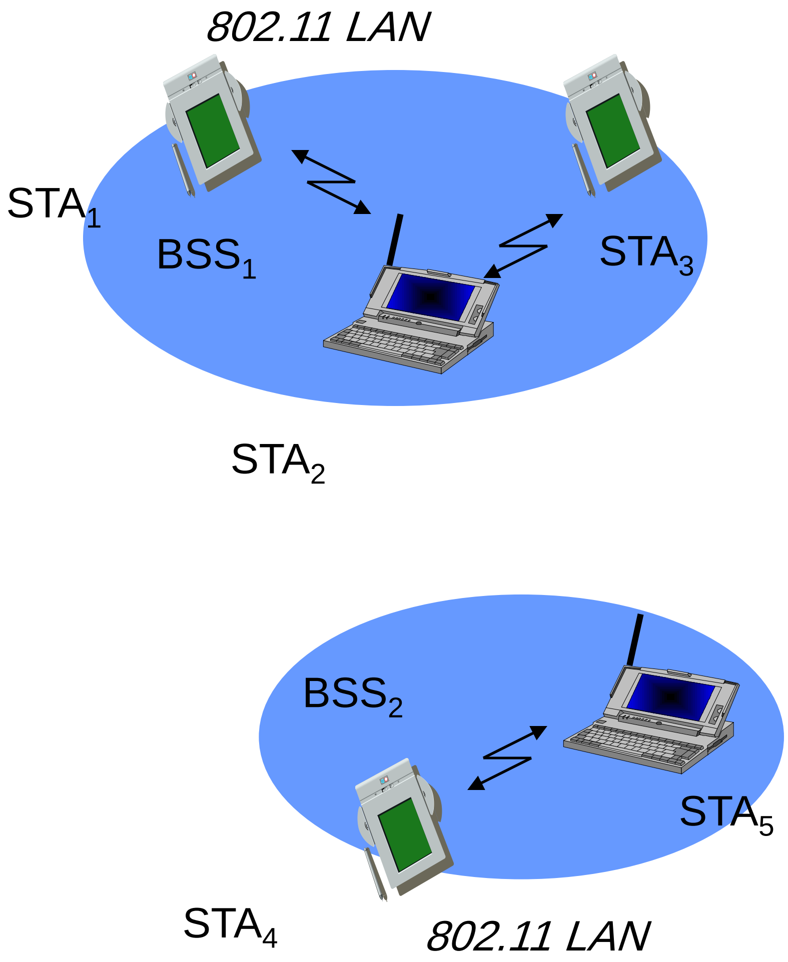


Components of IEEE 802.11 architecture

- 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



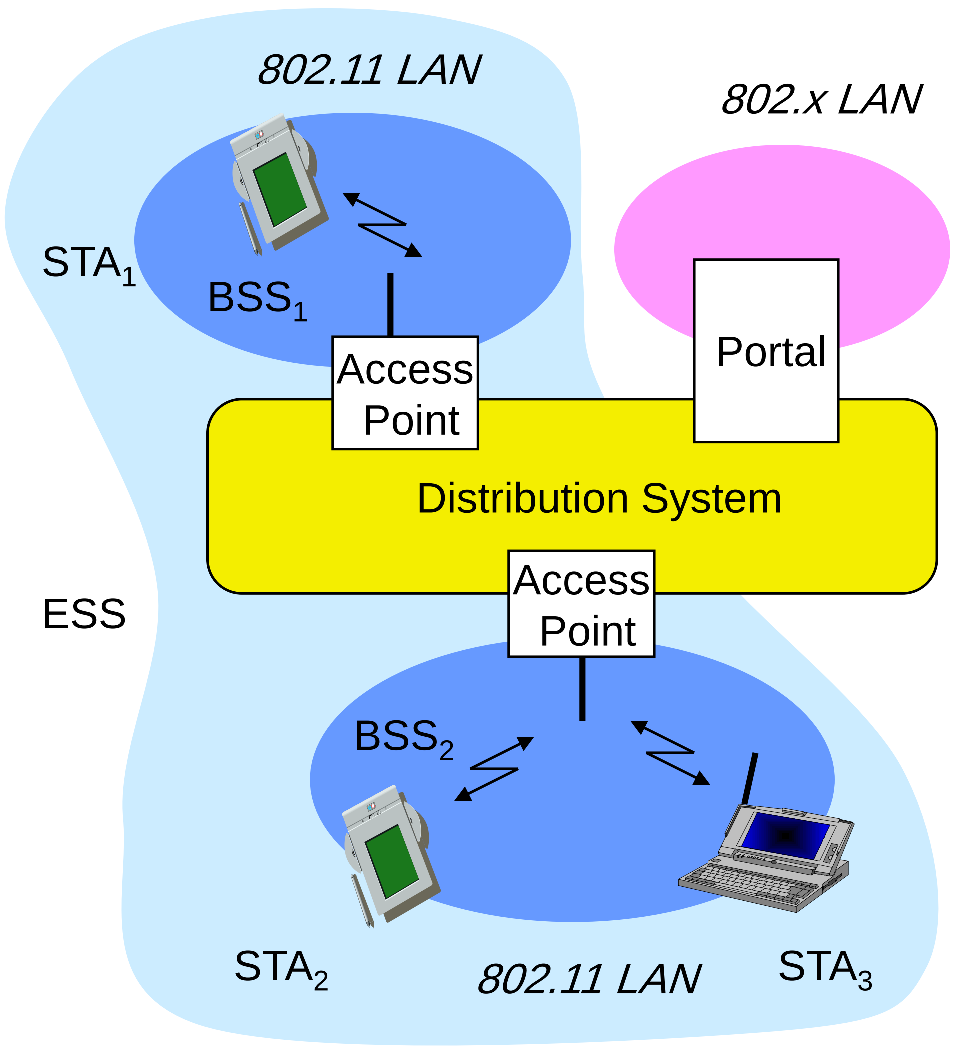
802.11 - ad-hoc network (DCF)



- 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

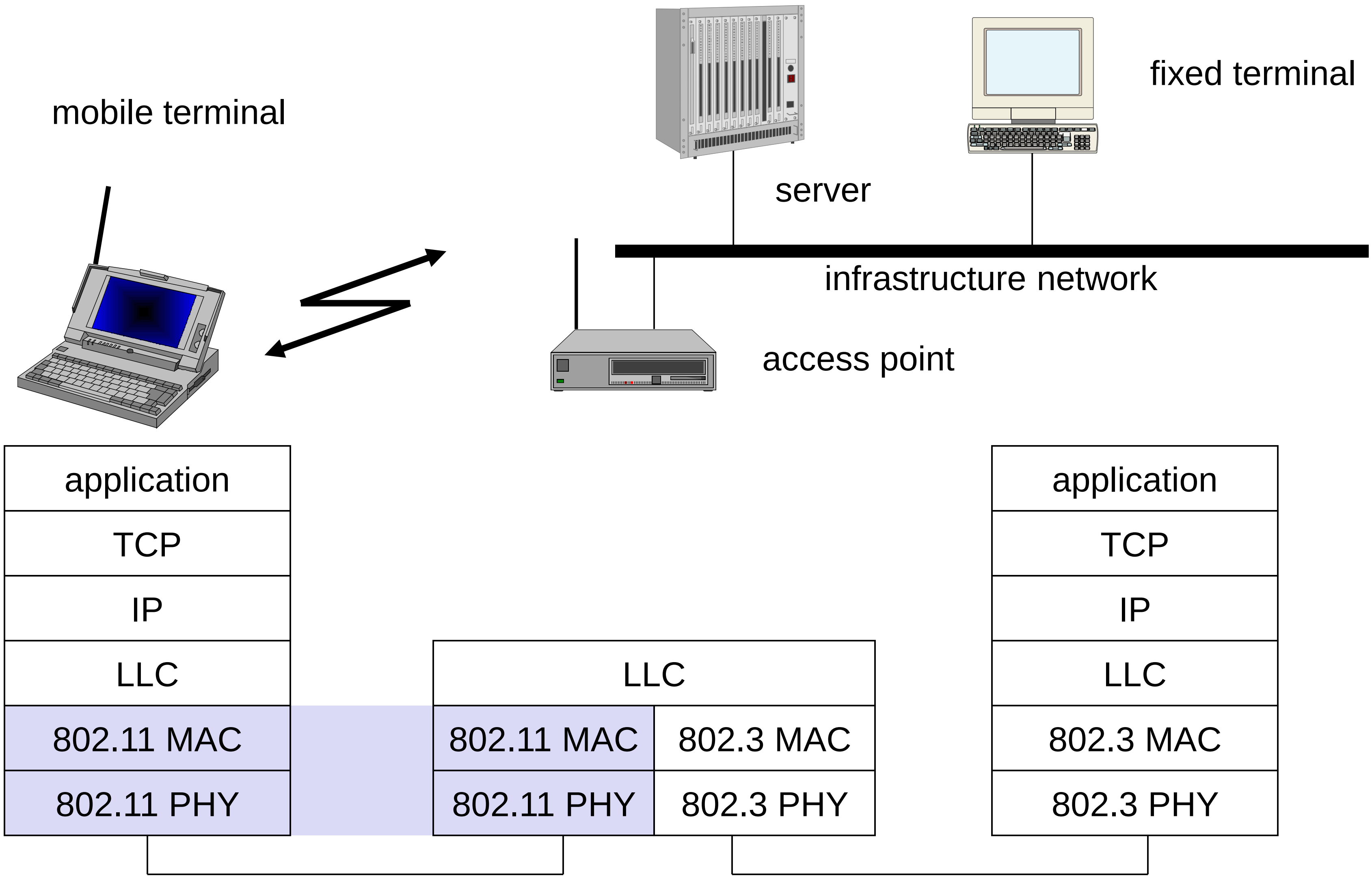
802.11 - infrastructure network (PCF)



- 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

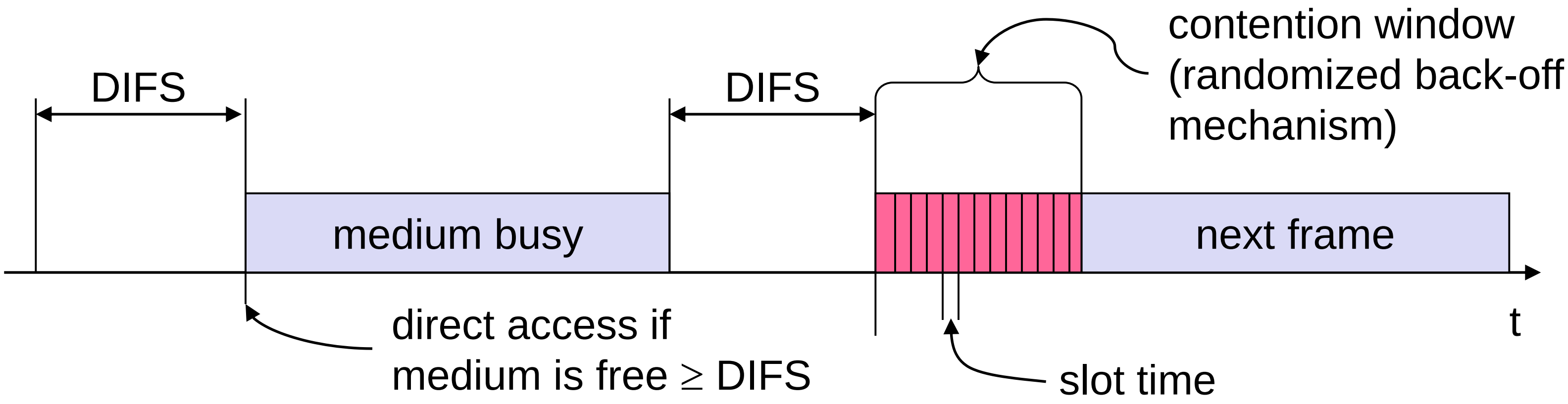
802.11- in the TCP/IP stack



802.11 - MAC layer

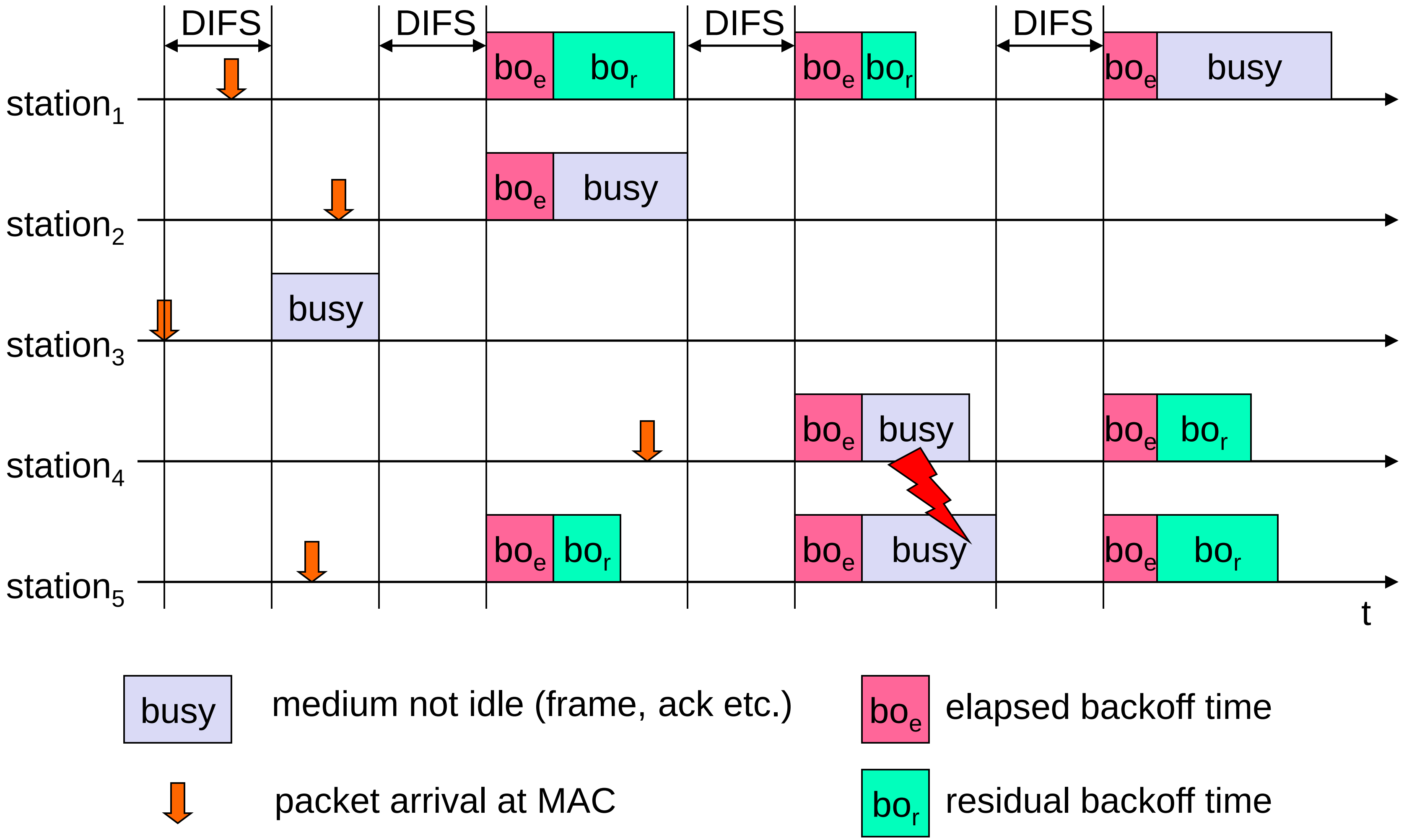
- Traffic services
  - Asynchronous Data Service (mandatory) – DCF
  - Time-Bounded Service (optional) - PCF
- Access methods
  - DCF CSMA/CA (mandatory)
    - collision avoidance via randomized back-off mechanism
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF w/ RTS/CTS (optional)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

802.11 - CSMA/CA



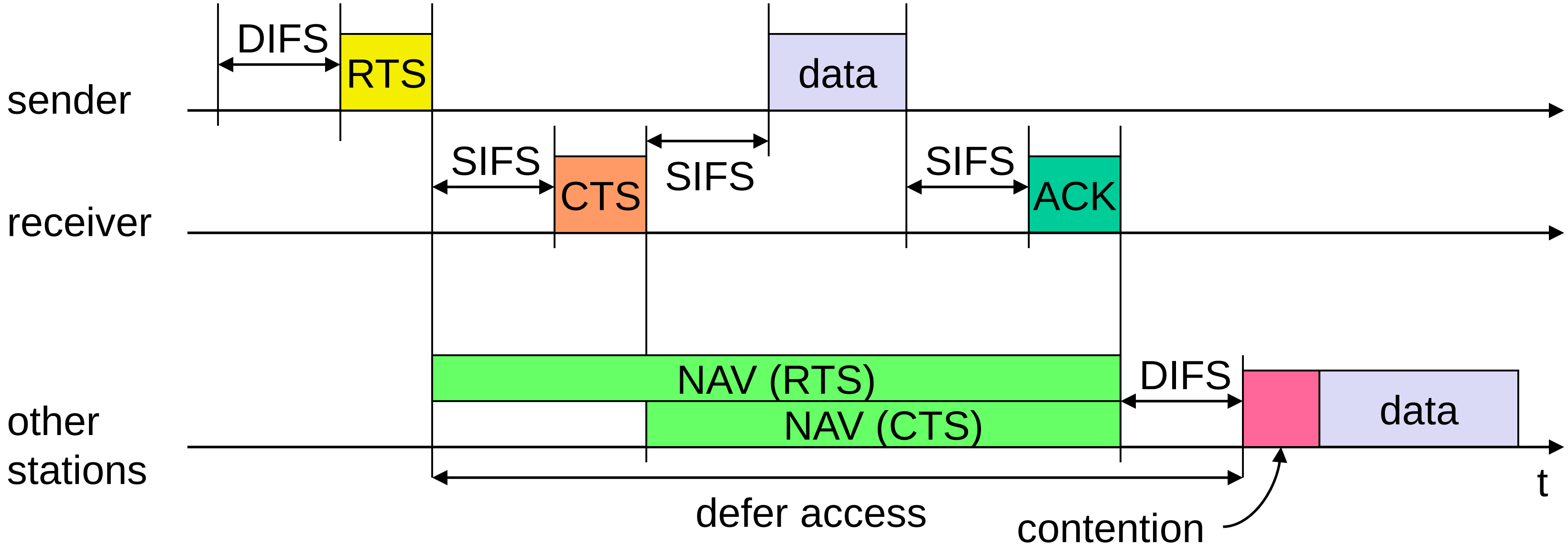
- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, 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

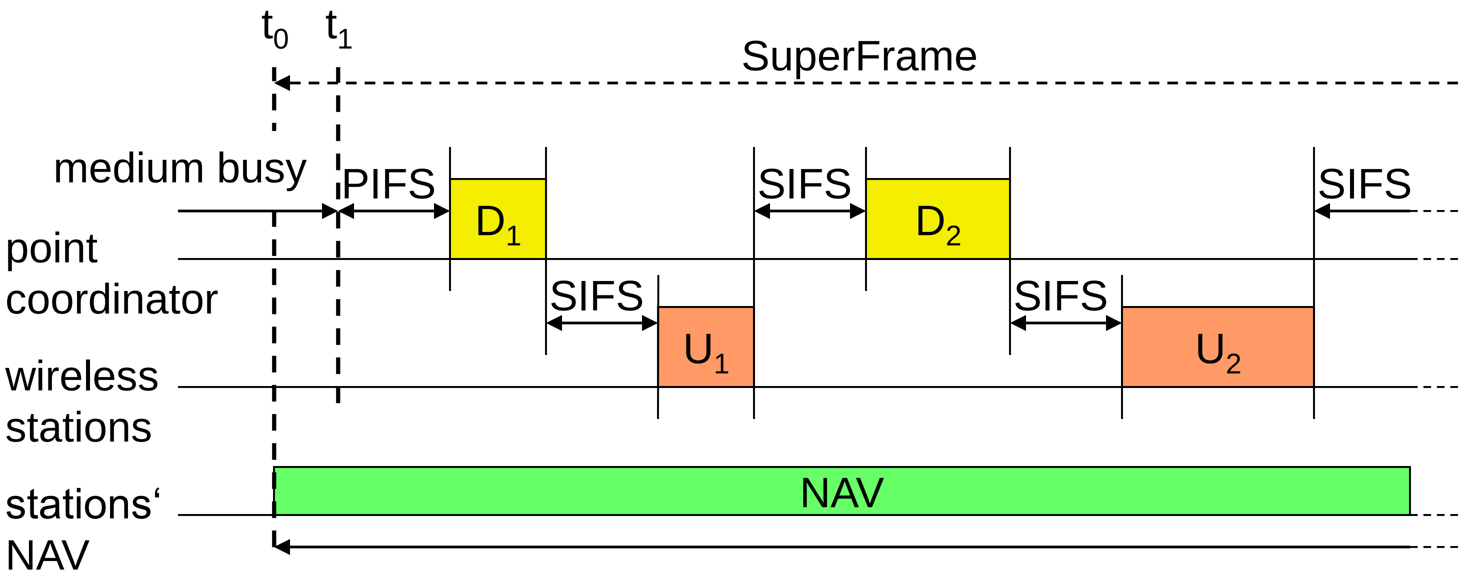


802.11 –RTS/CTS

- 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

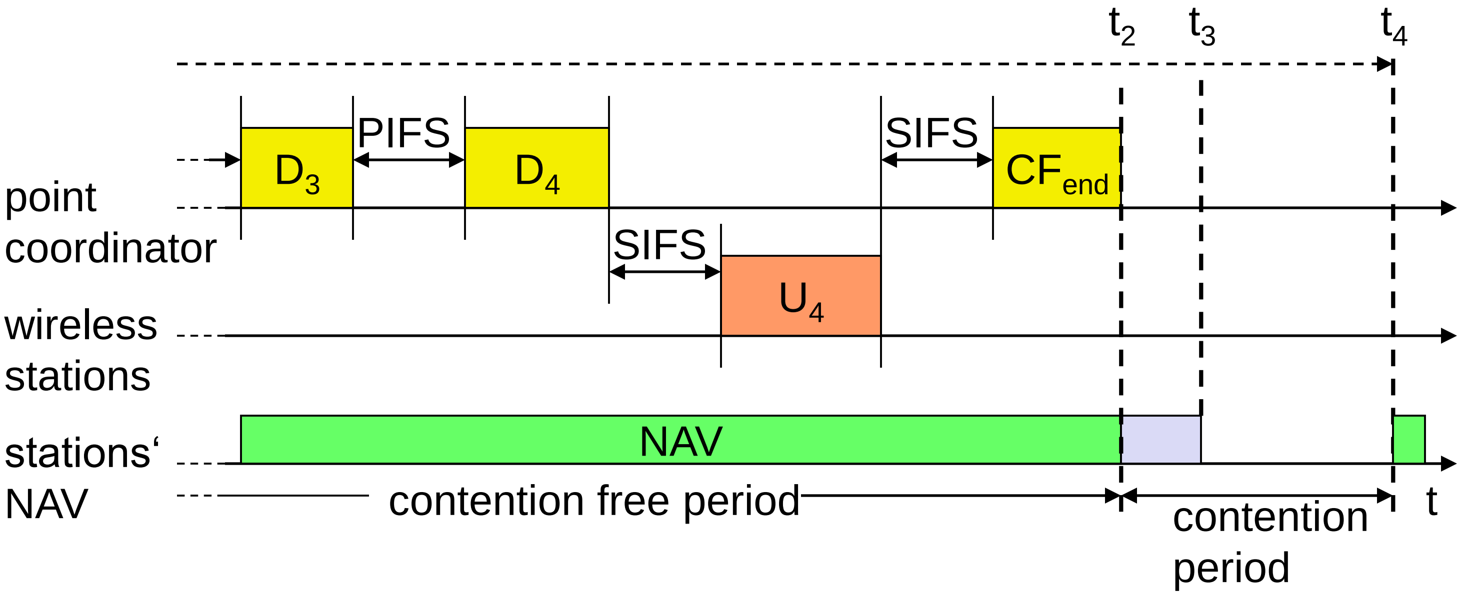


802.11 - PCF I



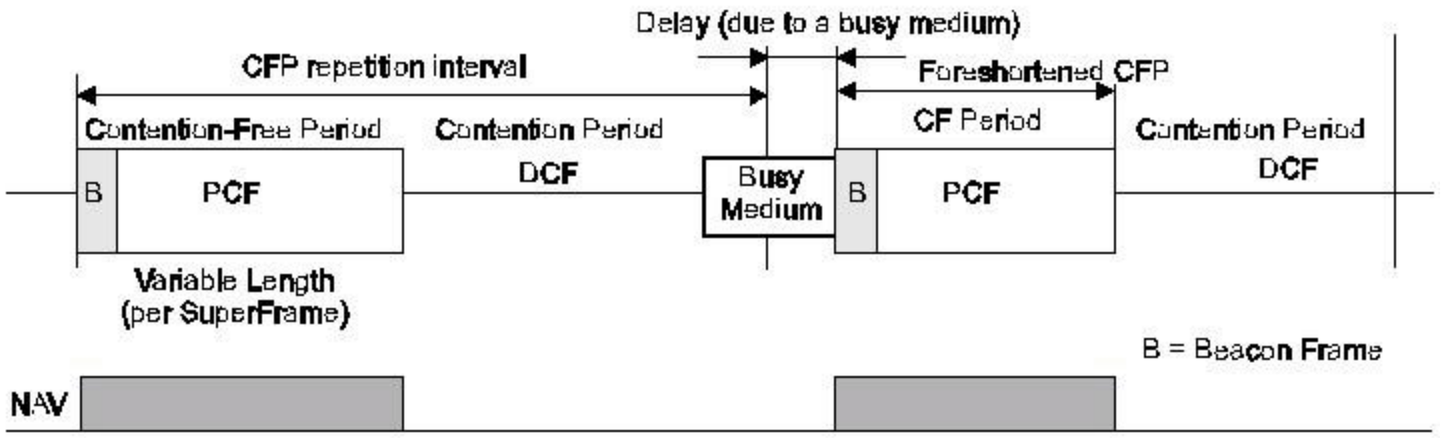
t0
t1
SuperFrame
medium busy
PIFS
SIFS
SIFS
D1
D2
point coordinator
SIFS
SIFS
U1
U2
wireless stations
NAV
stations' NAV

802.11 - PCF II

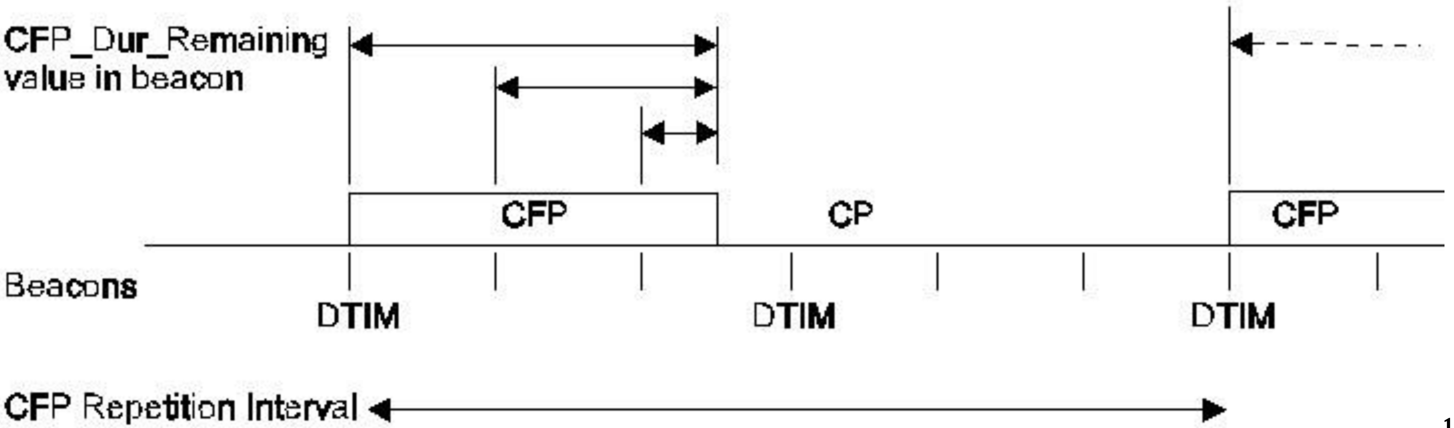


t2
t3
t4
PIFS
SIFS
D3
D4
CFend
point coordinator
SIFS
U4
wireless stations
stations' NAV
NAV
contention free period
contention period
t

CFP structure and Timing



CFP/CP Alternation and Beacon Periods



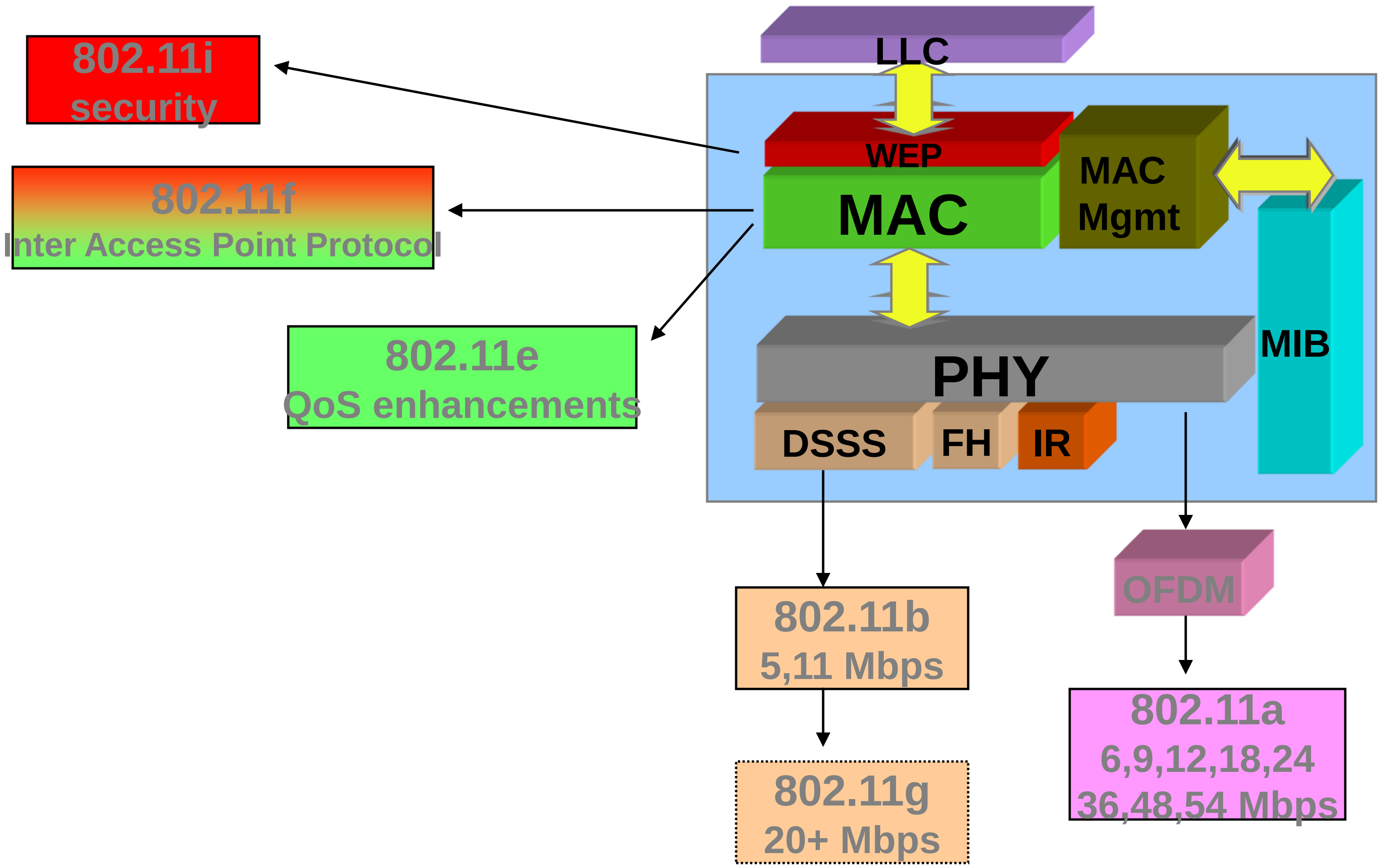
802.11 - MAC management

- 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

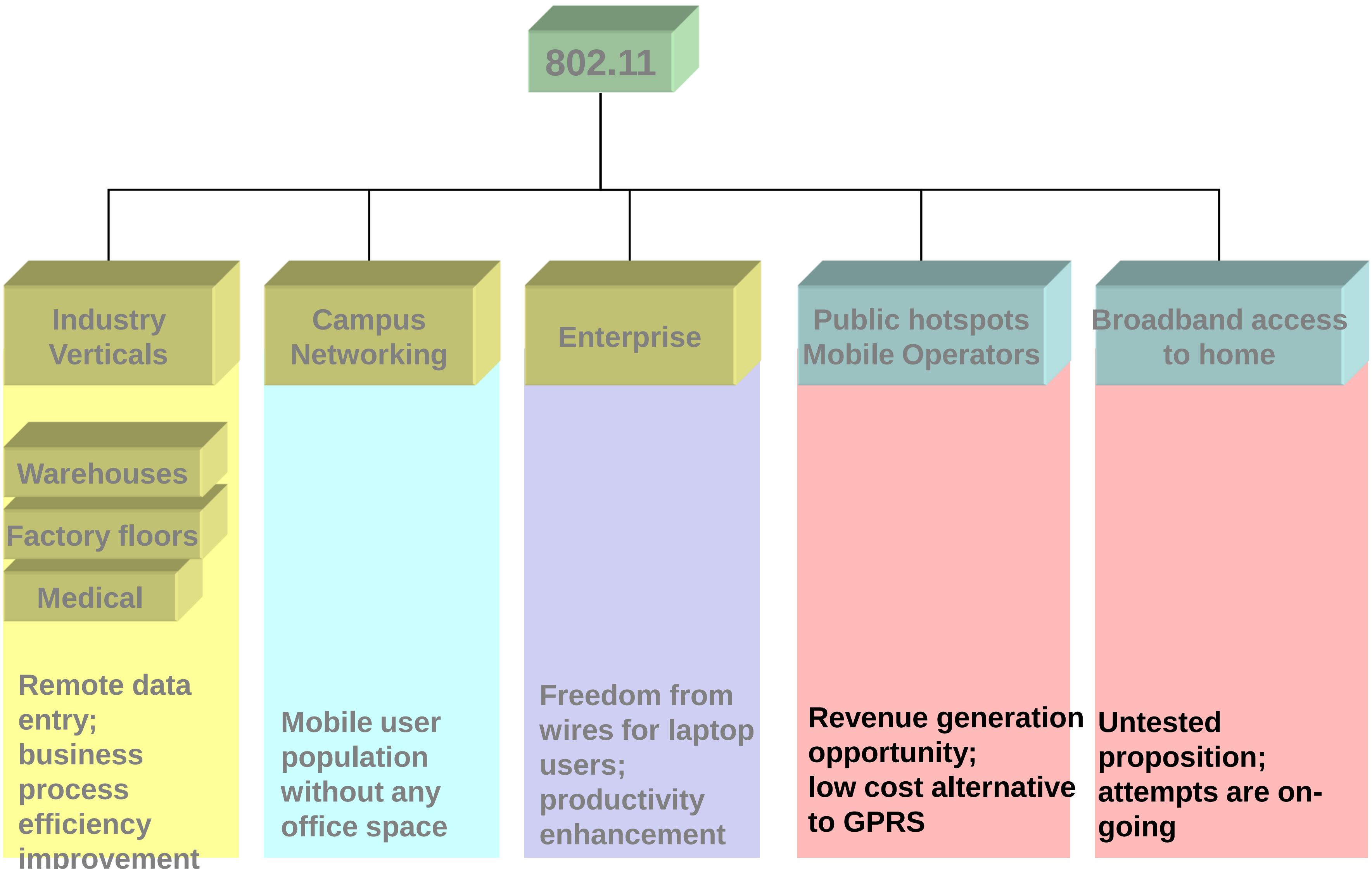
802.11 - Channels, association

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

802.11 variants



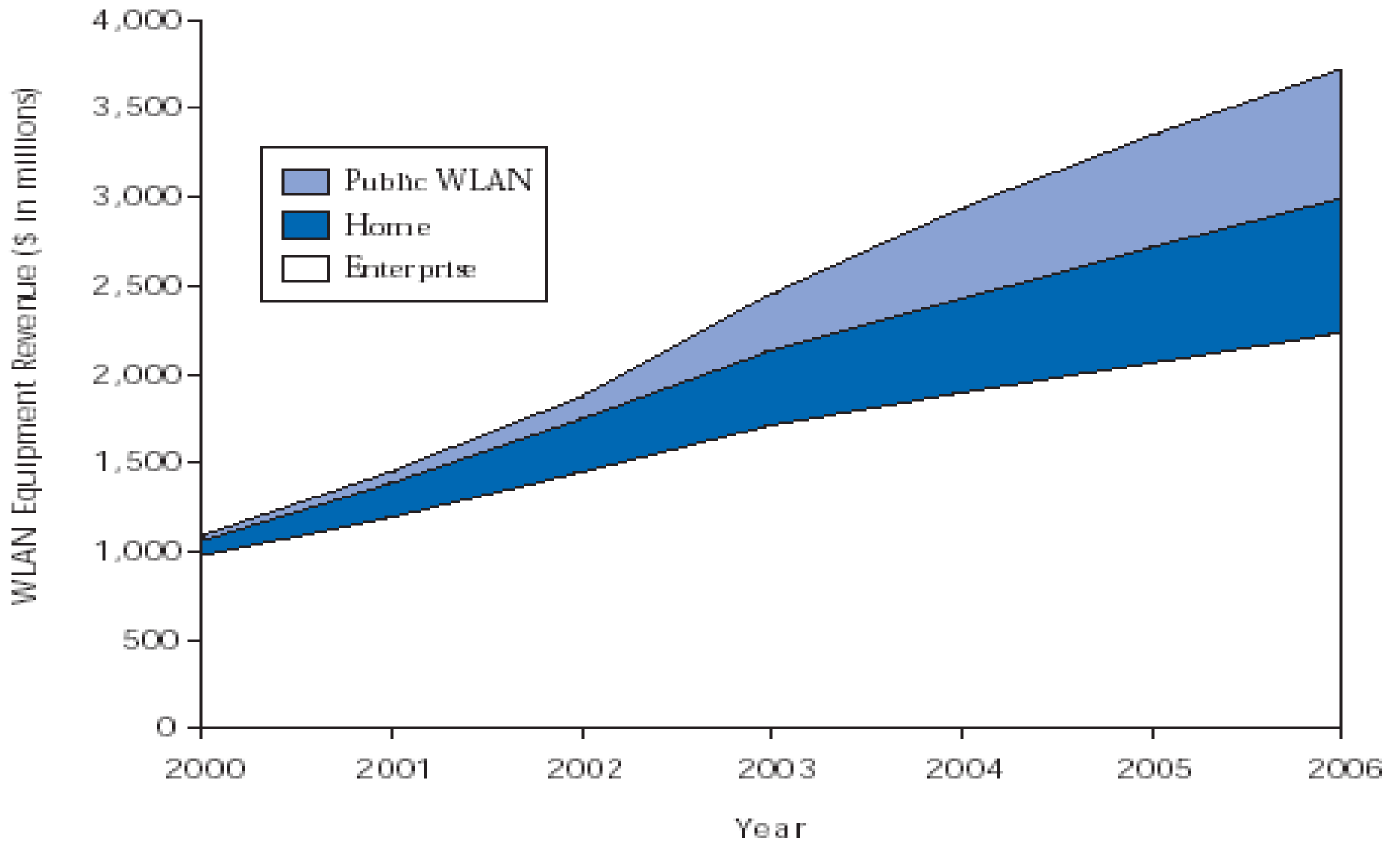
802.11 Market Evolution



Public WLANs

- Provide significantly higher data rates than wide-area wireless networks
- Could take advantages of both WLAN and wide-area radio technologies to create new services and reduce networking costs
- Public WLANs are the first wave of all-IP radio access networks
- New and innovative business models for providing public mobile services

Worldwide WLAN sales



CAGR 2000 – 2006	
Enterprise	13.4%
Home	30.4%
Public WLAN	65.5%

802.16 (WiMaX) Overview

Motivation for 802.16

- Broadband:
  - A transmission facility having a bandwidth sufficient to carry multiple voice, video or data, simultaneously.
  - High-capacity fiber to every user is expensive.

- Broadband Wireless Access:
  - provides “First-mile” network access to buildings.
  - Cost effective and easy deployment.

IEEE 802.16

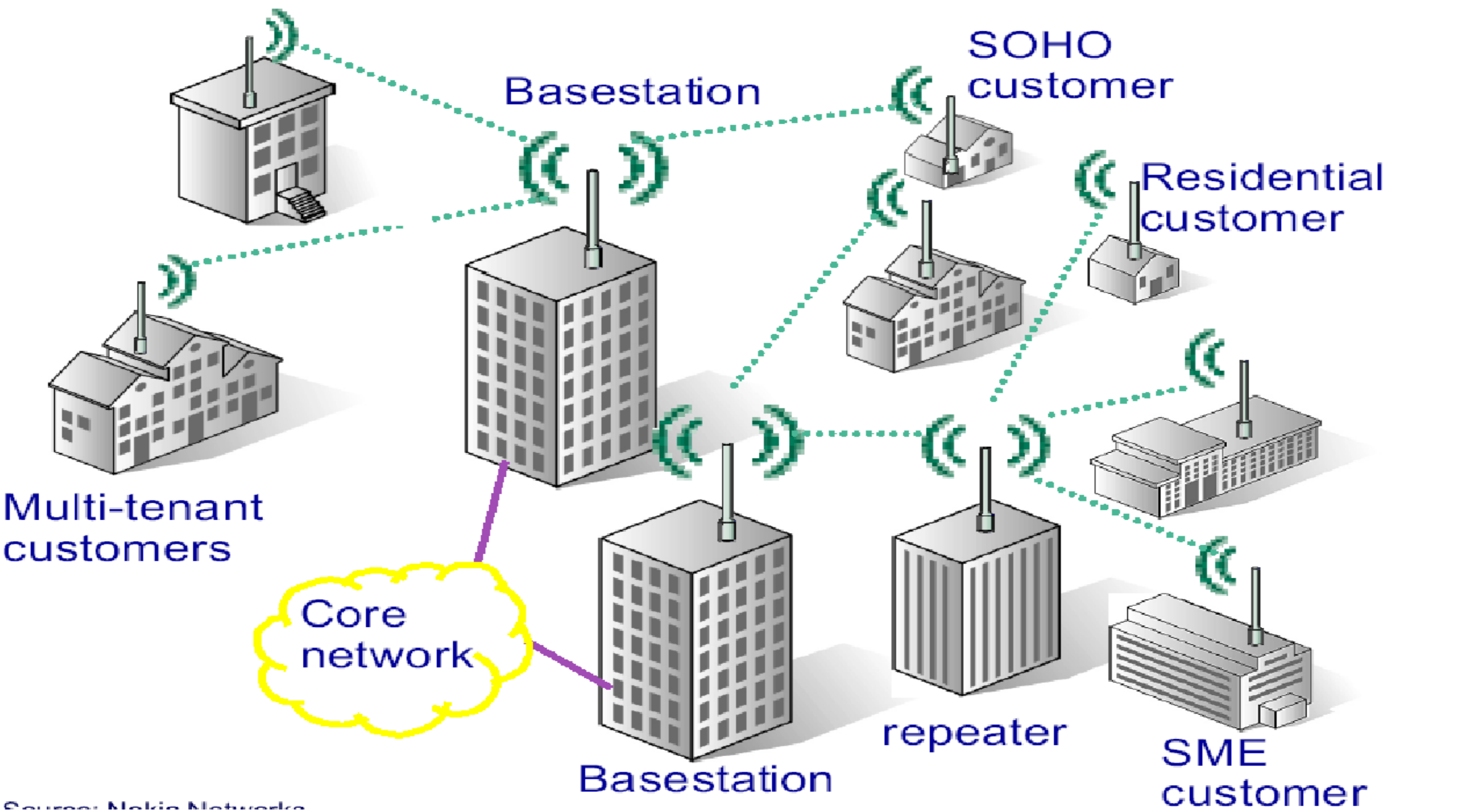
- WirelessMAN air interface
  - for fixed point to multi-point BWA

- Broad bandwidth: 10-66 GHz
  - Channel as wide as 28 MHz and
  - Data rate upto 134 Mbps

- MAC designed for efficient use of spectrum
  - Bandwidth on demand
  - QoS Support

802.16 Architecture

WirelessMAN: Wireless Metropolitan Area Network



Channel model

- Two Channels: Downlink and Uplink
- Supports both Time Division Duplexing and Frequency Division Duplexing

- Base station maps downstream traffic onto time slots with individual subscriber stations allocated time slot serially
- Uplink is shared between a number of subscriber stations by Time Division Multiple Access

Network initialization of SS

- Acquires downlink and uplink channel.
- Perform initial ranging, negotiate basic capabilities.
- Perform registration and authorization.
- Establish IP connectivity and time of day.
- Transfer operational parameters.
- Set up connections.

Bandwidth requests and grants

- Ways
  - Bandwidth request packet.
  - Piggybacking bandwidth request with normal data packet.
- Request can be made during time slot assigned by base station for sending request or data.
- Grant modes
  - Grant per connection.
  - Grant per subscriber station.
- Grant per subscriber station is more efficient and scalable but complex than Grant per connection.

Uplink scheduling services

- Unsolicited grant service
  - Support applications generating constant bit rate traffic periodically.
  - Provides fixed bandwidth at periodic intervals.
- Real-time polling service
  - Supports real-time applications generating variable bit rate traffic periodically.
  - Offers periodic opportunities to request bandwidth.
- Non-real-time polling service
  - Supports non-real-time applications generating variable bit rate traffic regularly.
  - Offers opportunities to request bandwidth regularly.
- Best effort
  - Offers no guarantee.

802.16: Summary

- **Higher throughput at longer ranges (**up to 50 km**)**
  - Better bits/second/Hz at longer ranges
- **Scalable system capacity**
  - Easy addition of channels maximizes cell capacity
  - Flexible channel bandwidths accommodate allocations for *both licensed and license-exempt* spectrums
- **Coverage**
  - Standards-based mesh and smart antenna support
  - Adaptive modulation enables tradeoff of bandwidth for range
- **Quality of Service**
  - Grant / request MAC supports voice and video
  - Differentiated service levels: E1/T1 for business, best effort for residential

IEEE 802.16 Standard

	802.16	802.16a/REVd	802.16e
Completed	Dec 2001	802.16a: Jan 2003 802.16REVd: Q3'04	Estimate 2006
Spectrum	10 - 66 GHz	< 11 GHz	< 6 GHz
Channel Conditions	Line of sight only	Non line of sight	Non line of sight
Bit Rate	32 – 134 Mbps at 28MHz channelization	Up to 75 Mbps at 20MHz channelization	Up to 15 Mbps at 5MHz channelization
Modulation	QPSK, 16QAM and 64QAM	OFDM 256 sub-carriersQPSK, 16QAM, 64QAM	Same as 802.16a
Mobility	Fixed	Fixed	Pedestrian mobility – regional roaming
Channel Bandwidths	20, 25 and 28 MHz	Selectable channel bandwidths between 1.25 and 20 MHz	Same as 802.16a with uplink sub-channels to conserve power
Typical Cell Radius	1-3 miles	3 to 5 miles; max range 30 miles based on tower height, antenna gain and power transmit	1-3 miles

802.11 Internals

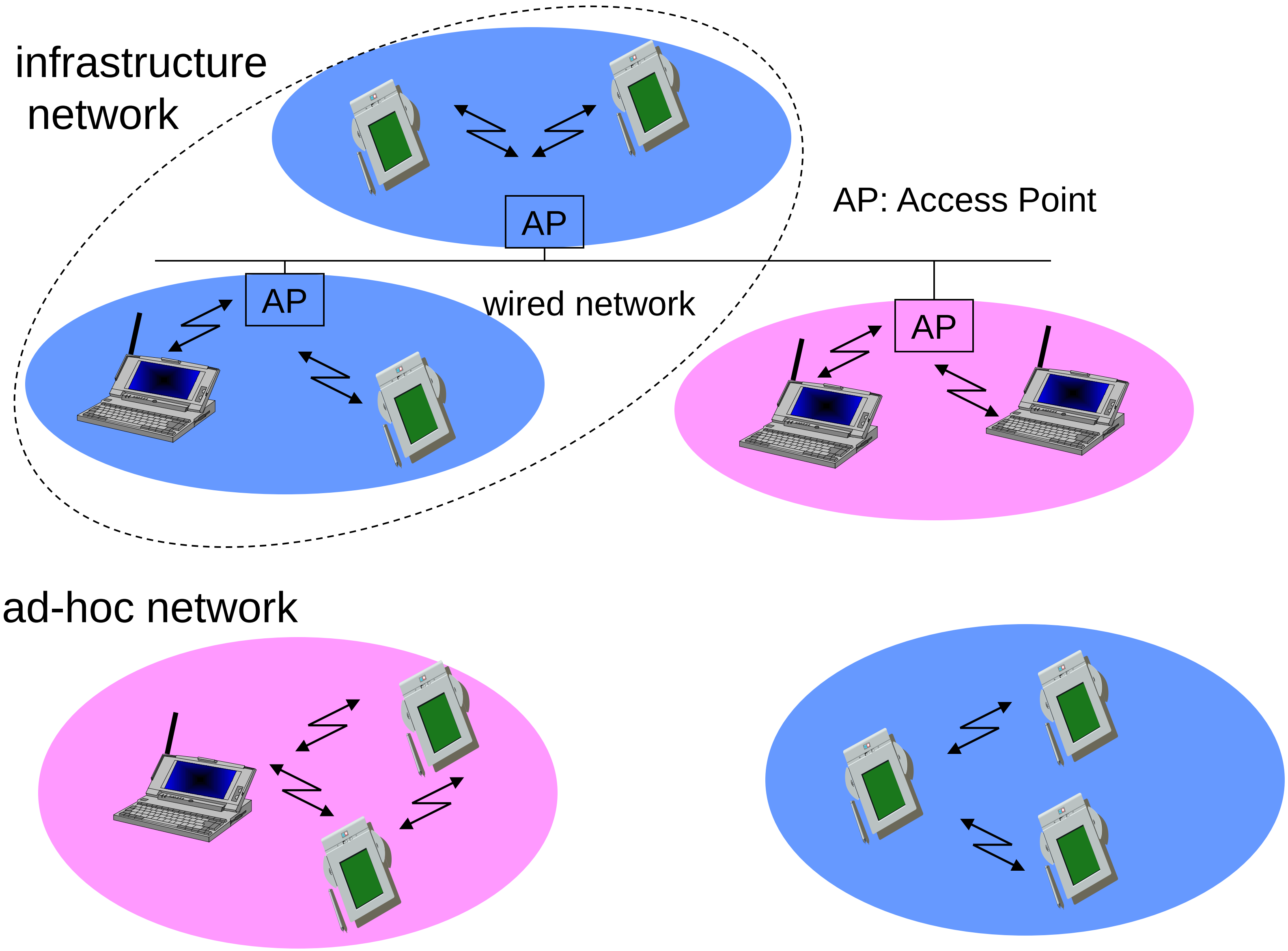
Wireless LANs vs. Wired LANs

- 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

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

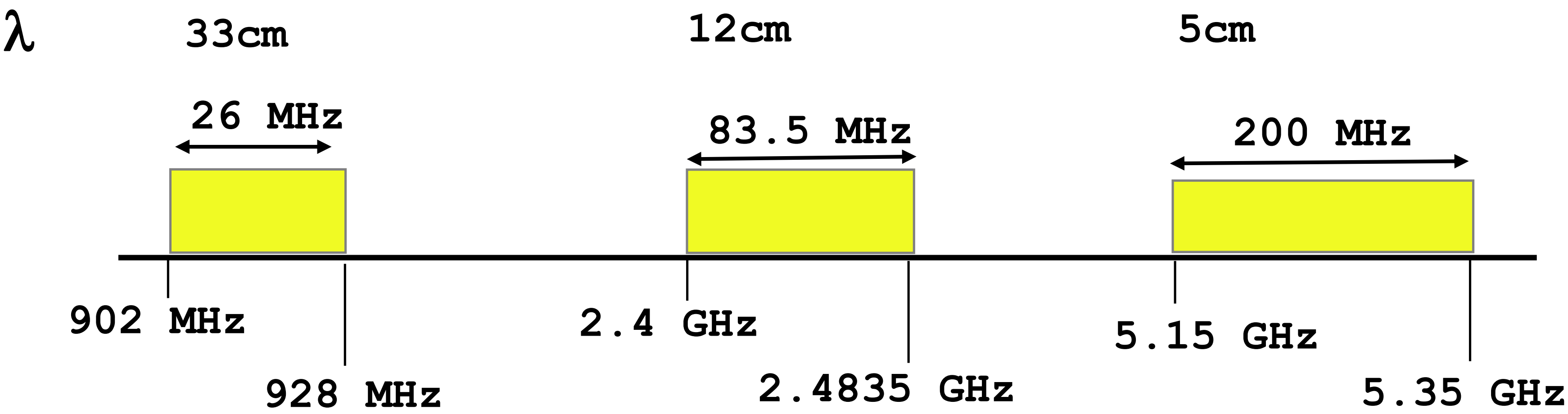
Infrastructure vs. Ad hoc WLANs



Source: Schiller

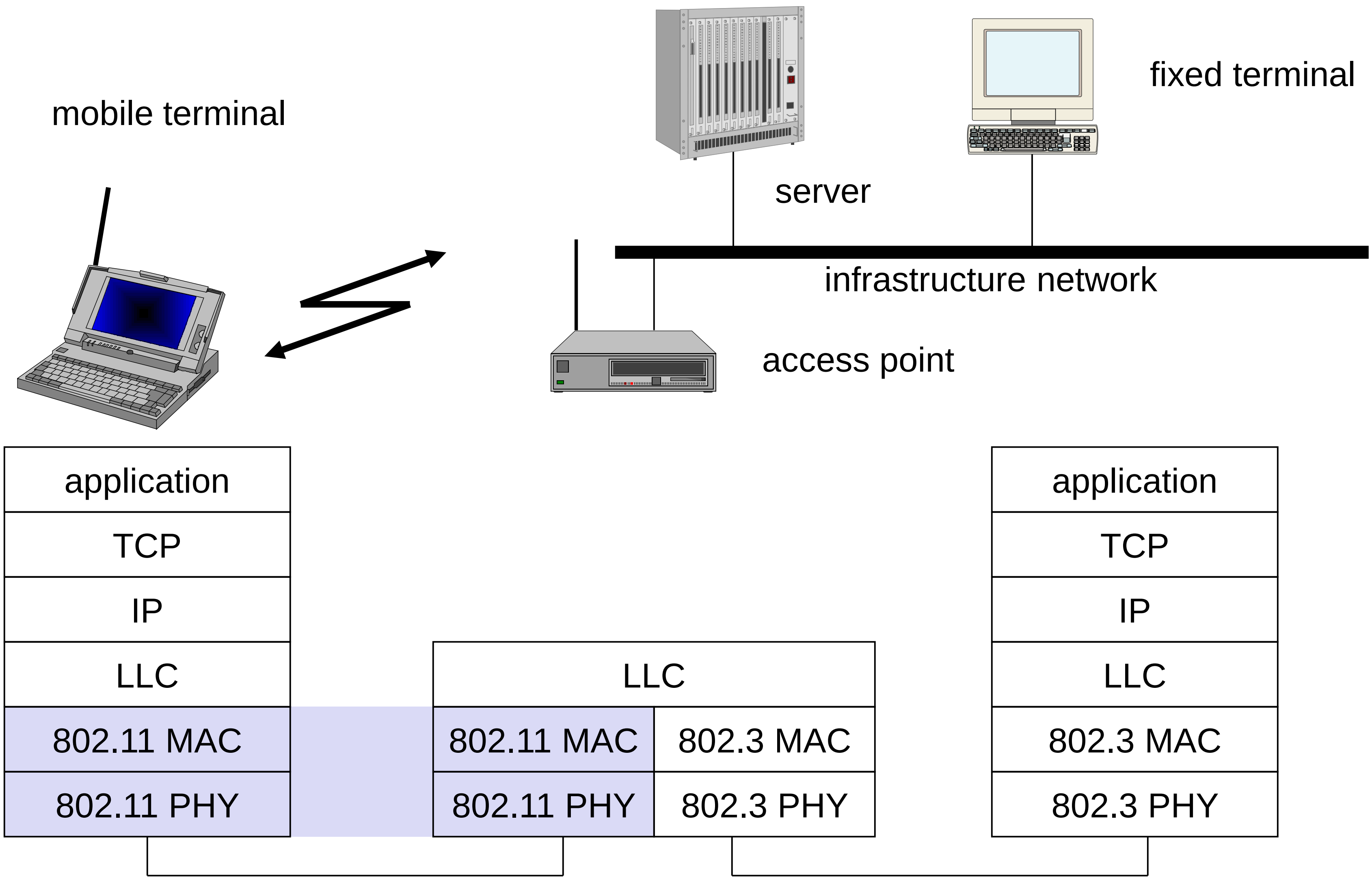
IEEE 802.11

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

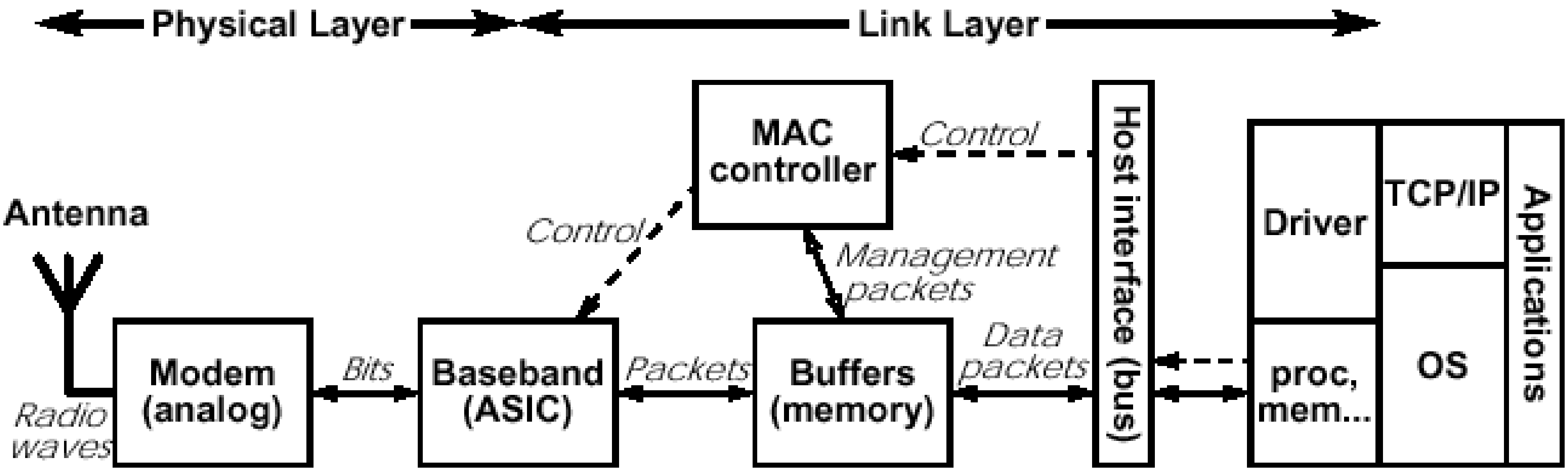


- Standards covers the MAC sublayer and PHY layers
- Three different physical layers in the 2.4 GHz band
  - FHSS, DSSS and IR
- OFDM based Phys layer in the 5 GHz band (802.11a)

802.11- in the TCP/IP stack

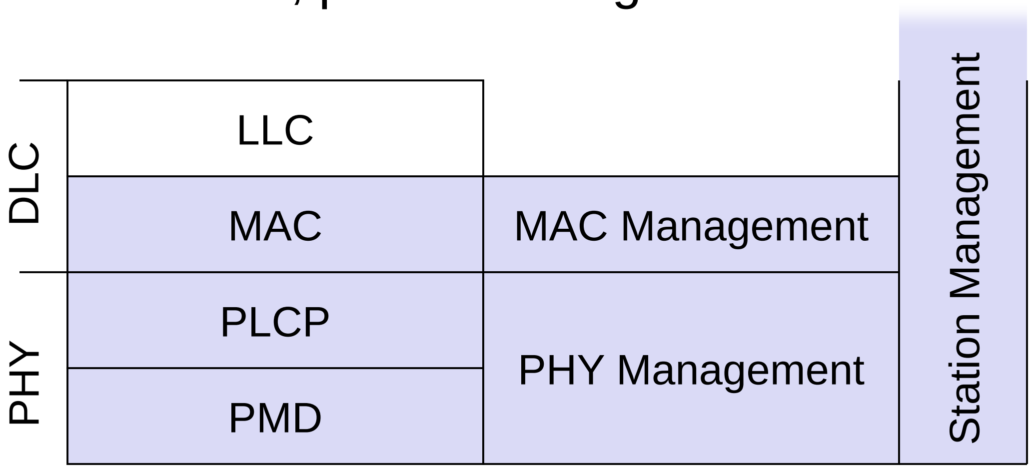


Functional Diagram



802.11 - Layers and functions

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

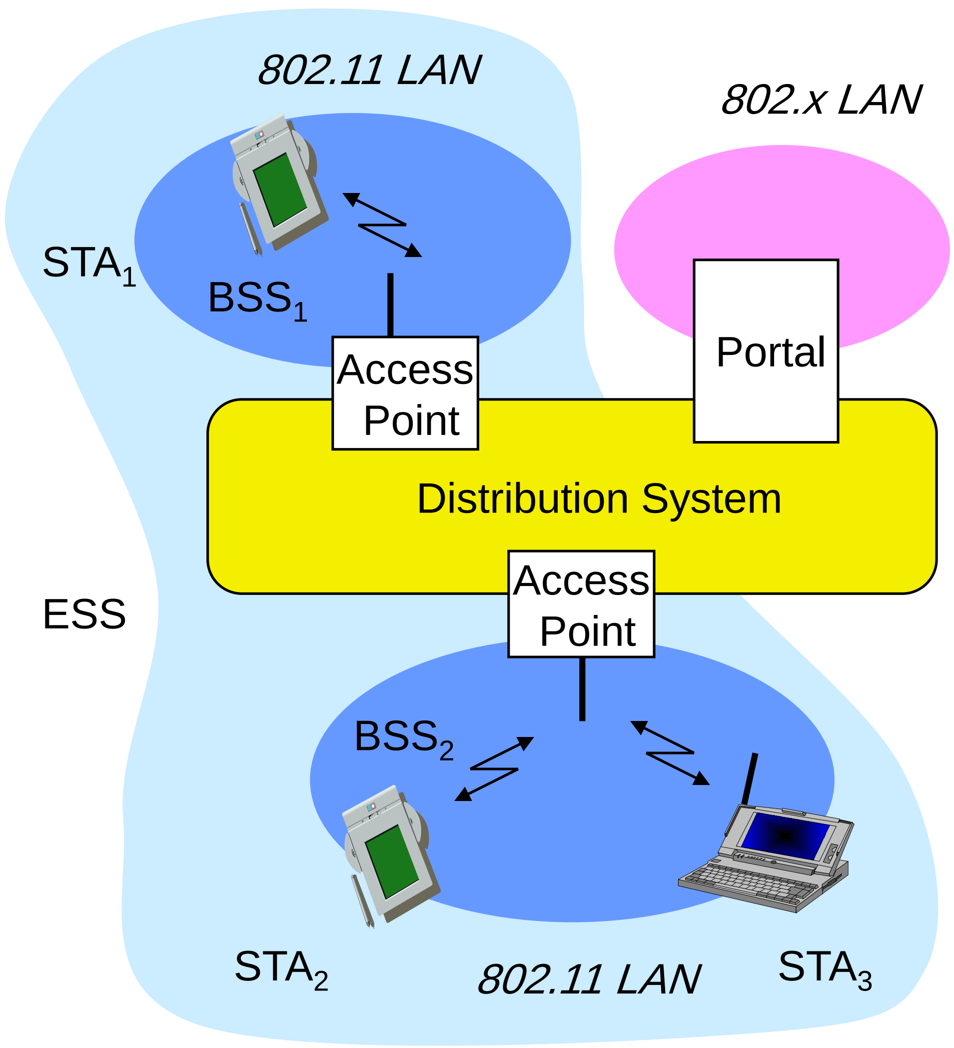


- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding

PHY Management
  - channel selection, MIB

Station Management
  - coordination of all management functions

802.11 - 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

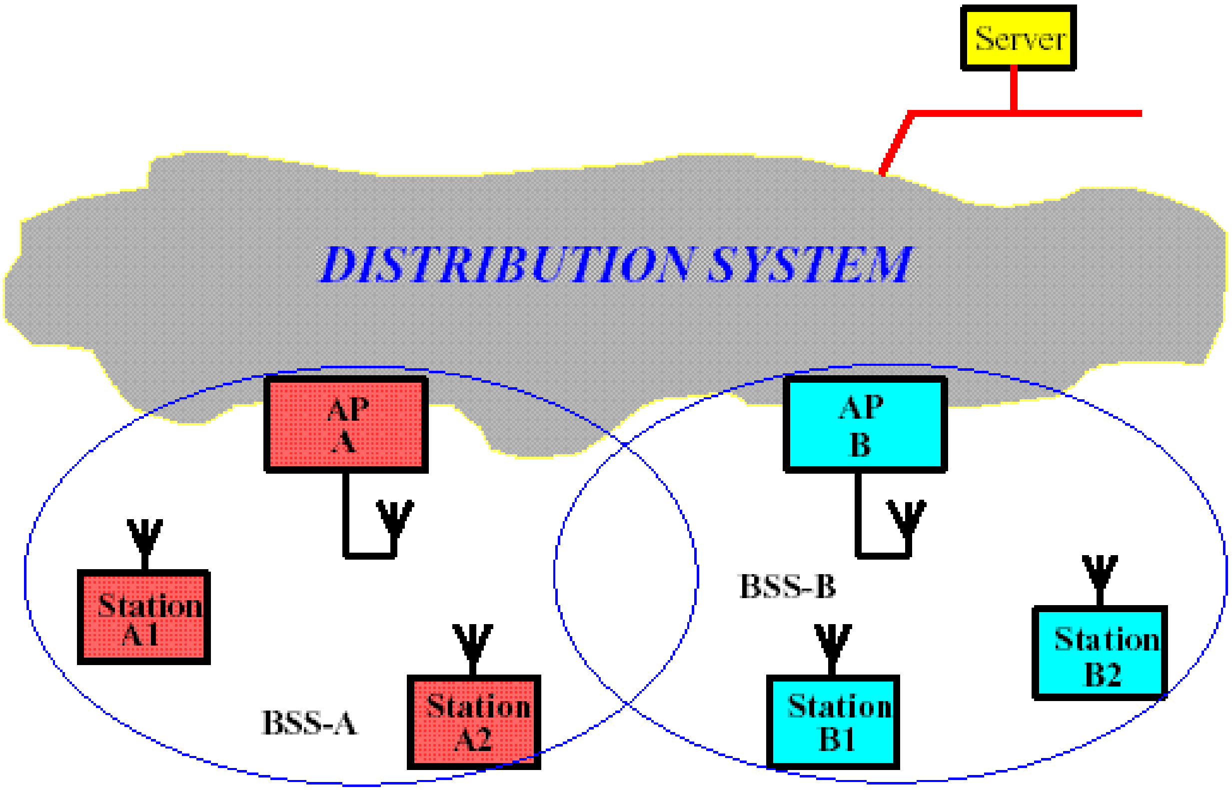


Figure 2 ESS Provides Campus-Wide Coverage

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

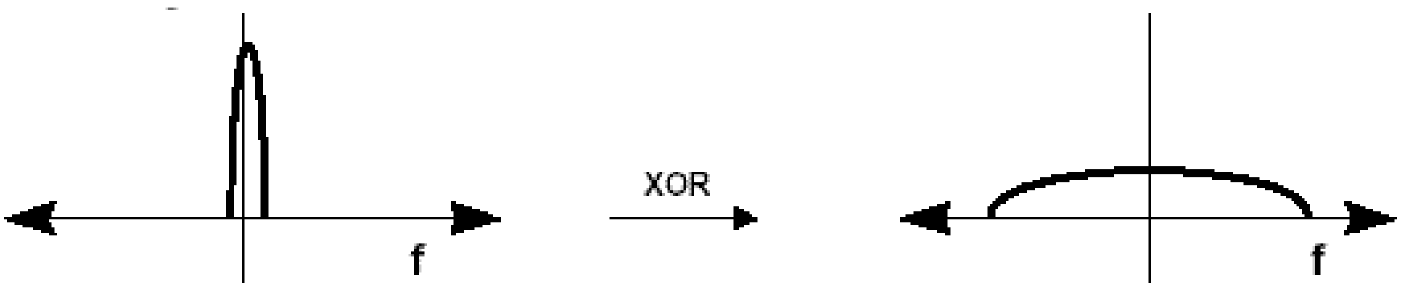


Figure 5a Effect of PN Sequence on Transmit Spectrum

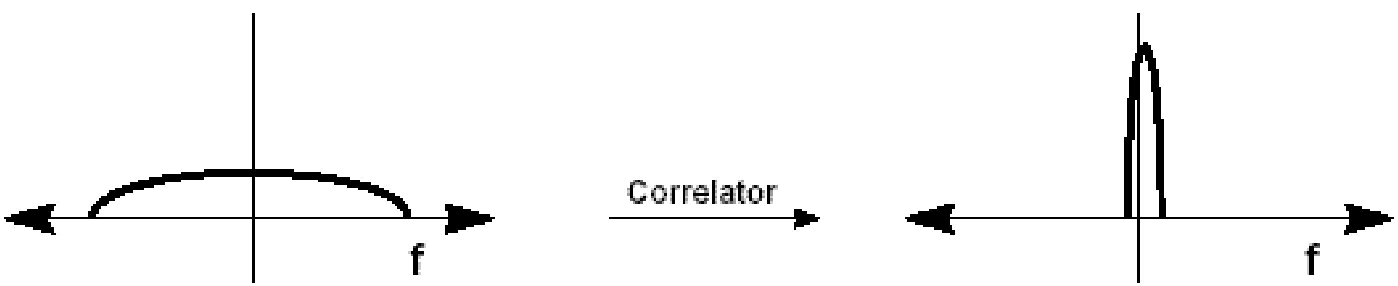
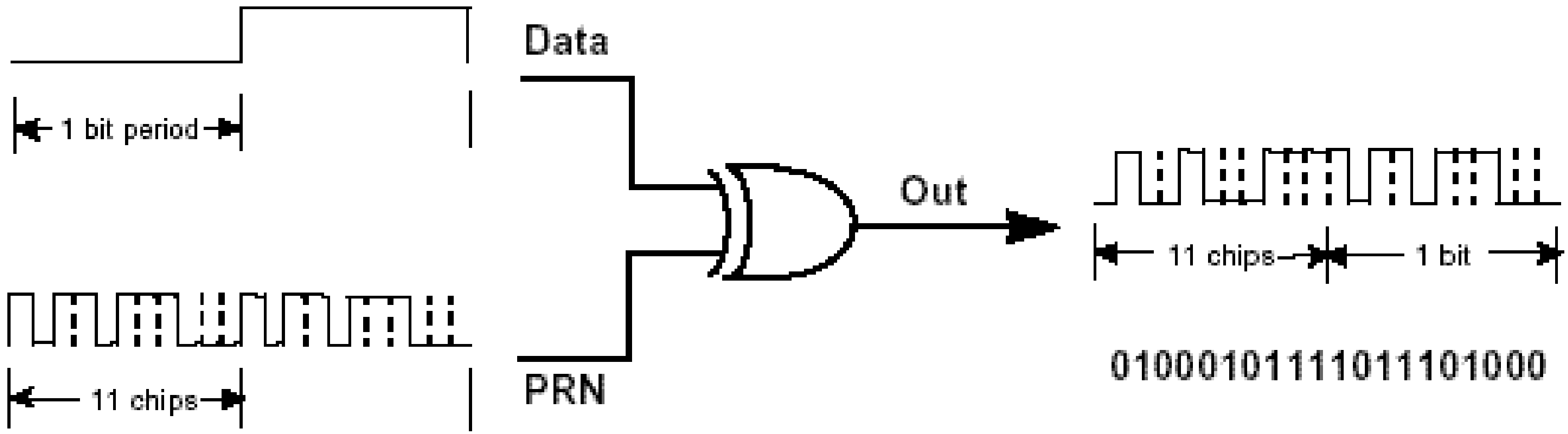


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

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

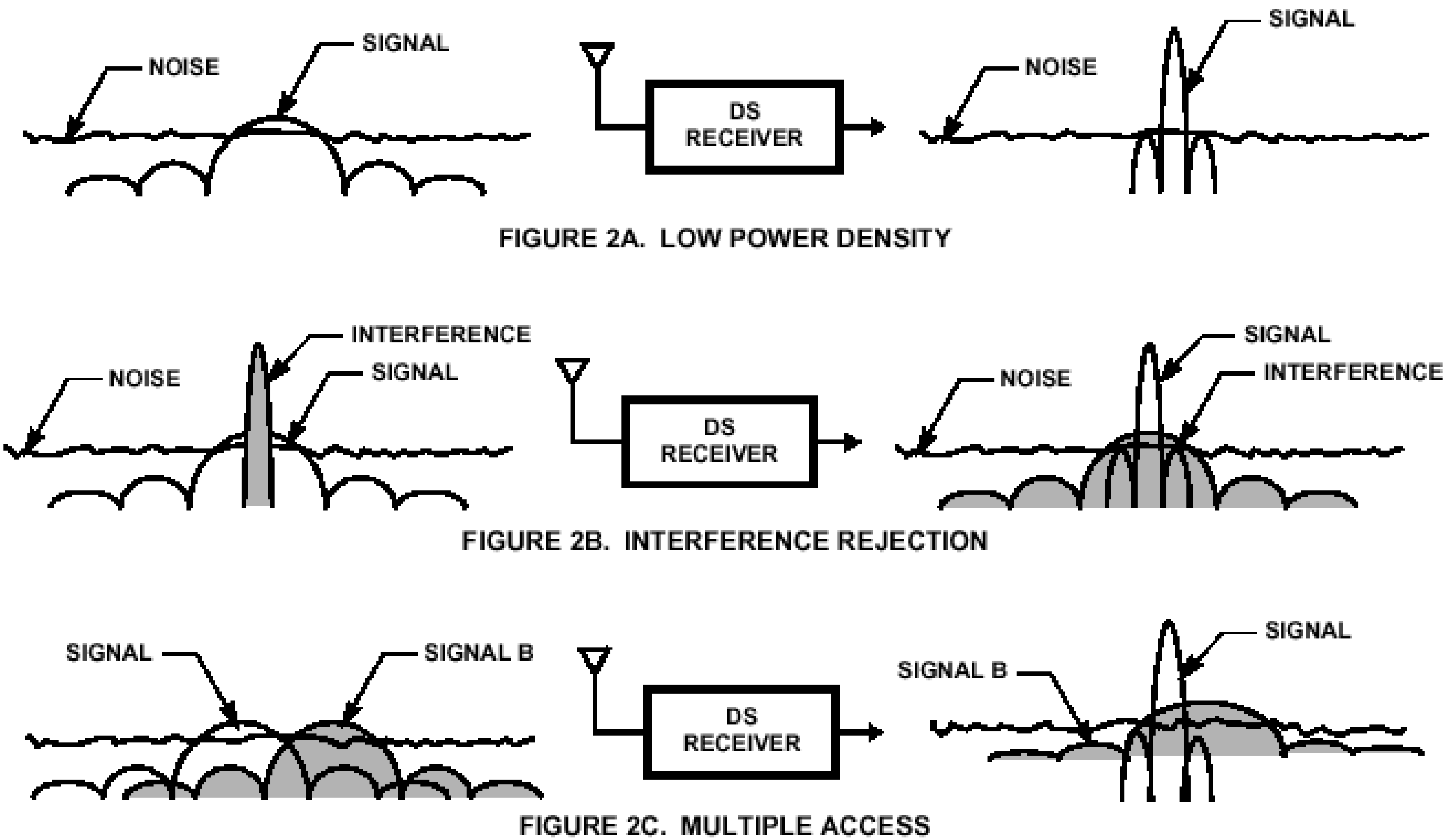


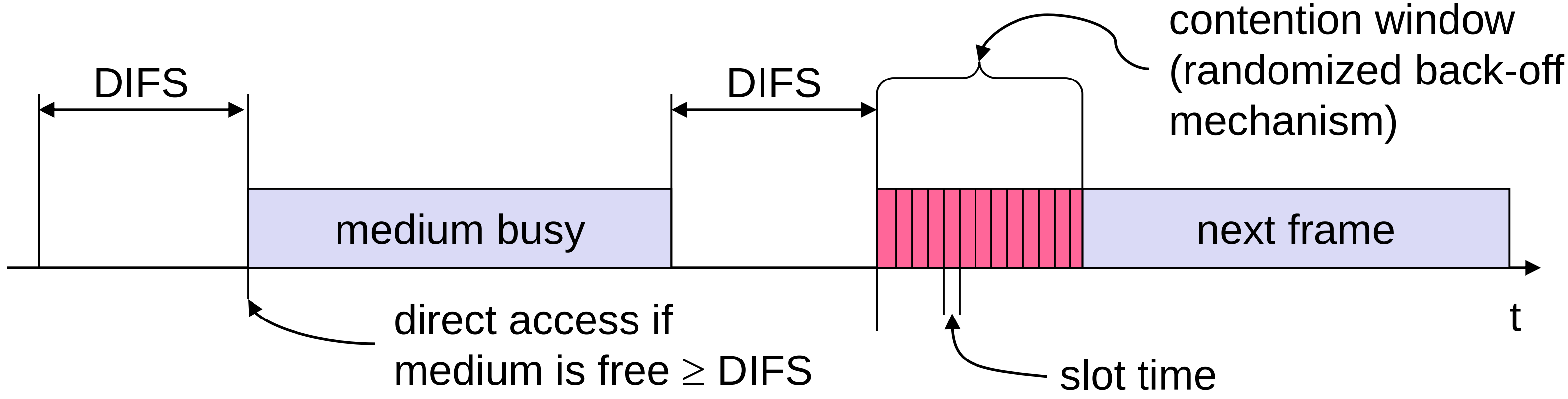
FIGURE 2. DIRECT SEQUENCE SPREAD SPECTRUM PROPERTIES

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

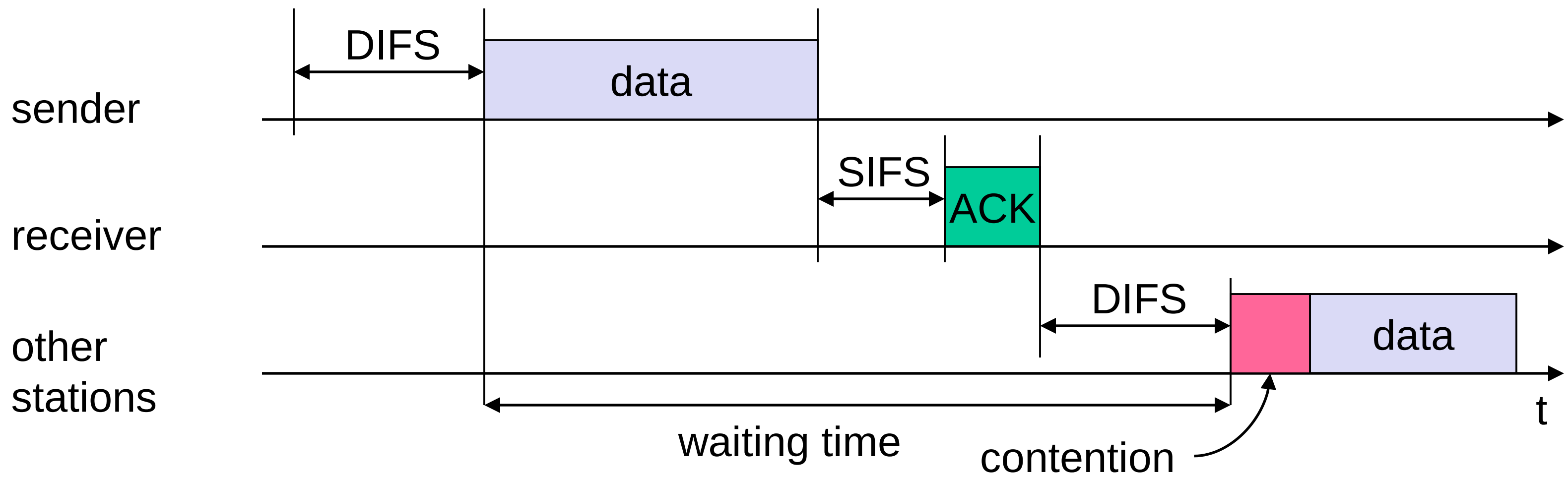
802.11 - CSMA/CA



– 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)

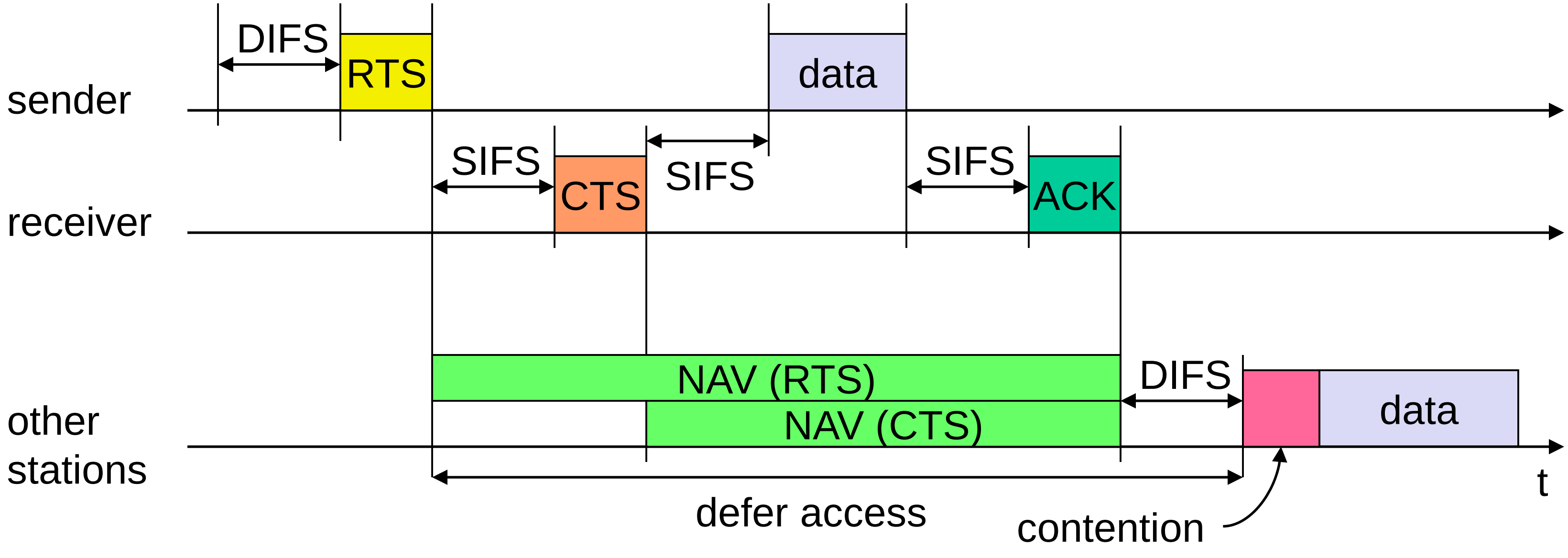
802.11 DCF – basic access

- 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



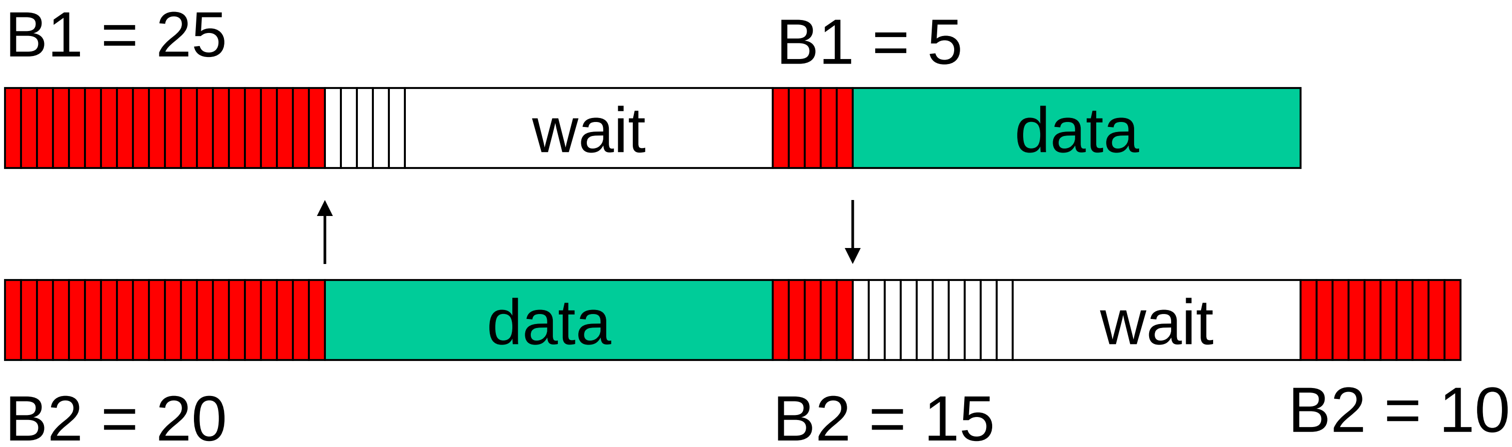
802.11 - Carrier Sensing

- **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

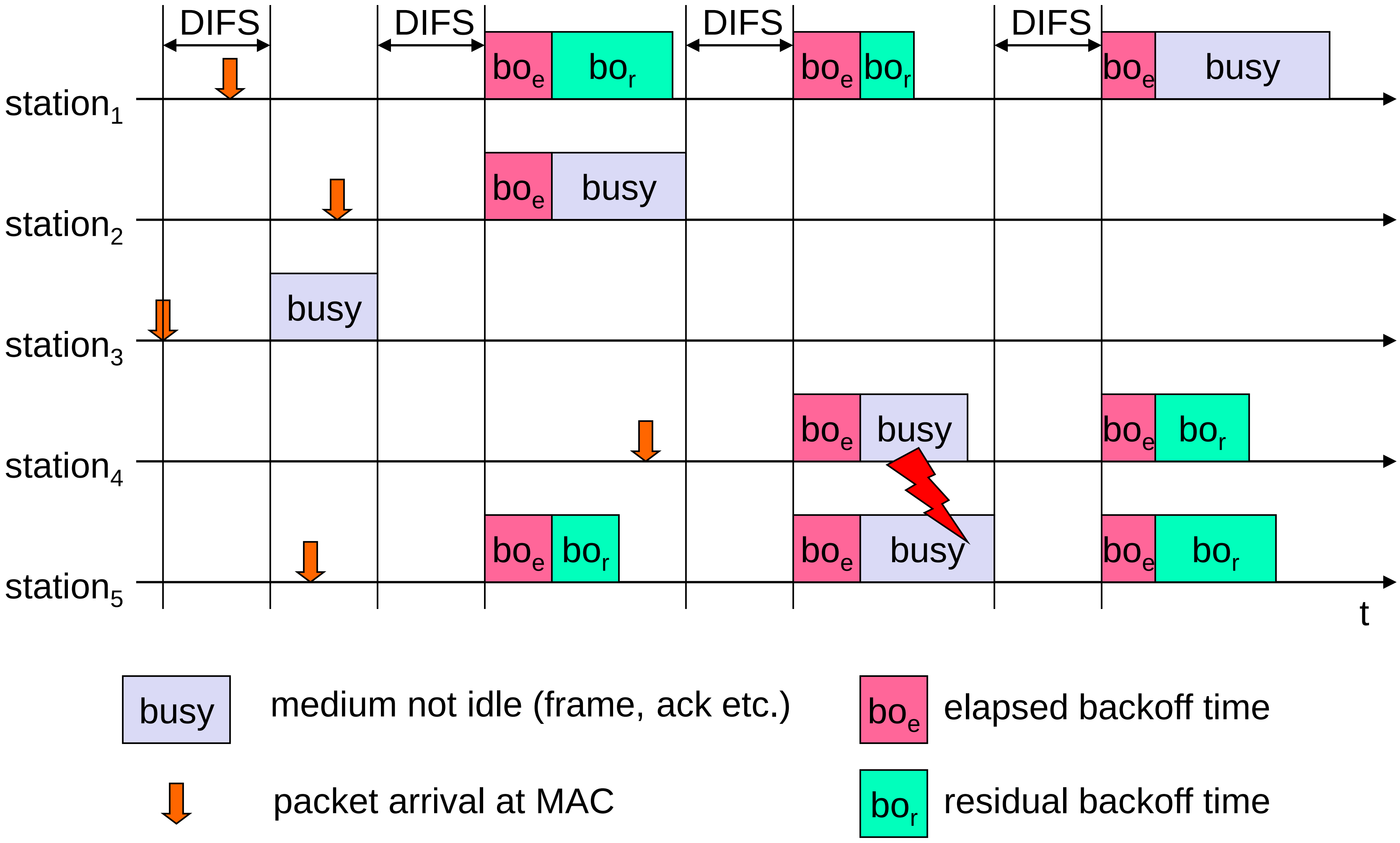
Example - backoff



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

Backoff - more complex example



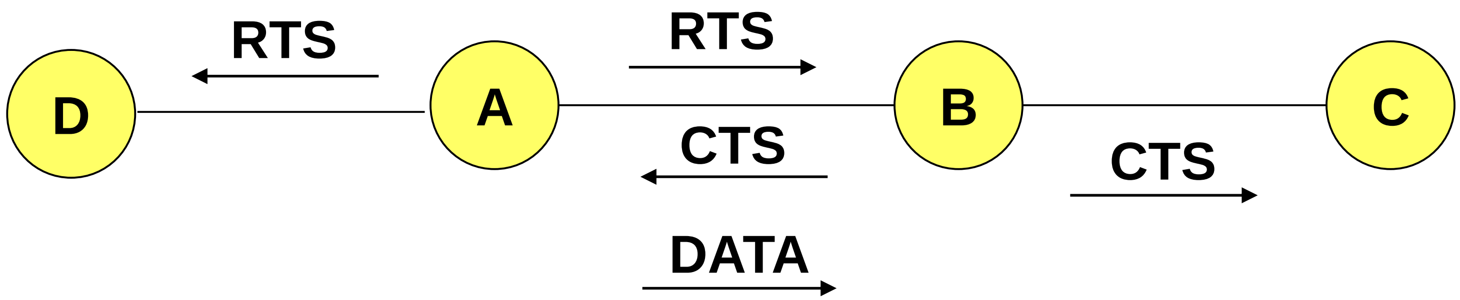
Source: Schiller

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 μs and 20 μs 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

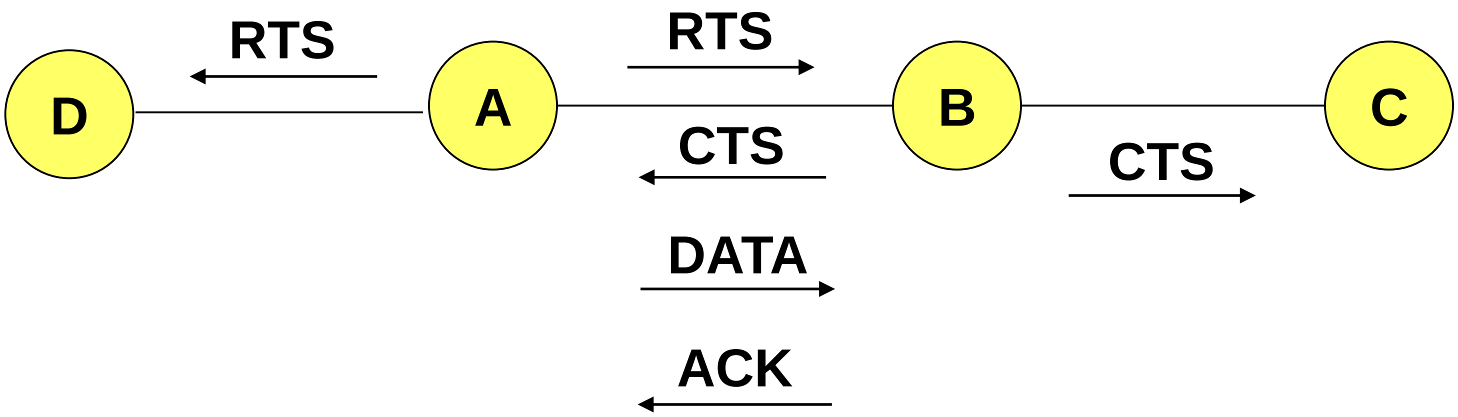
Solution to Hidden Terminals

- 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

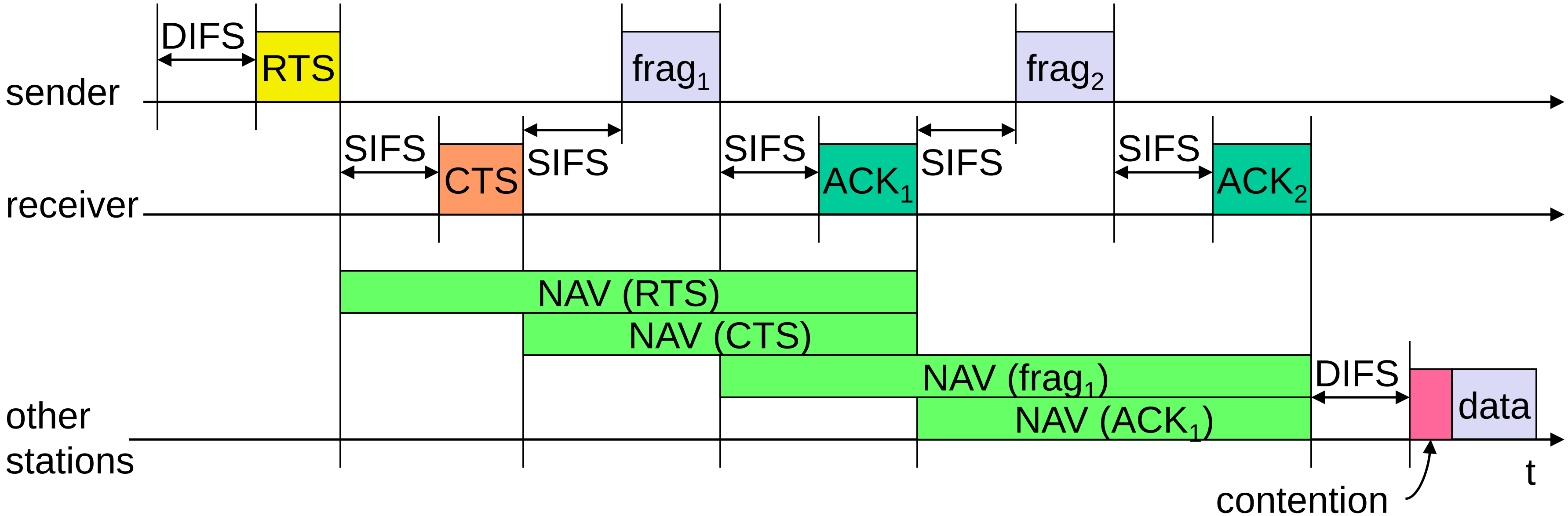


802.11 - Congestion Control

- 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



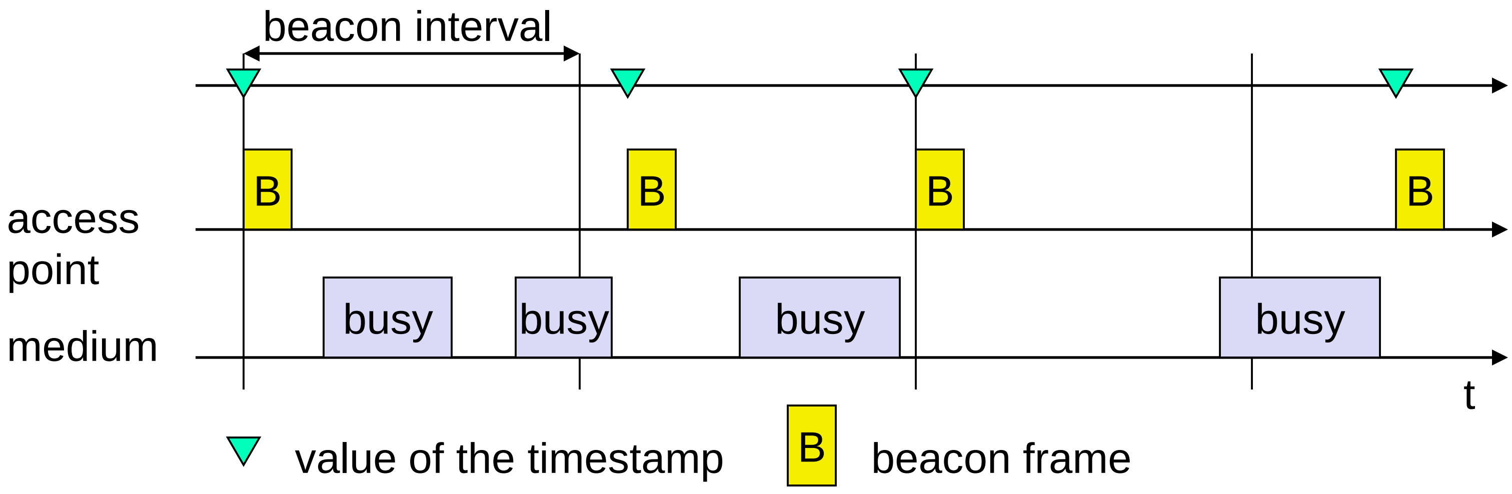
802.11 - MAC management

- 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

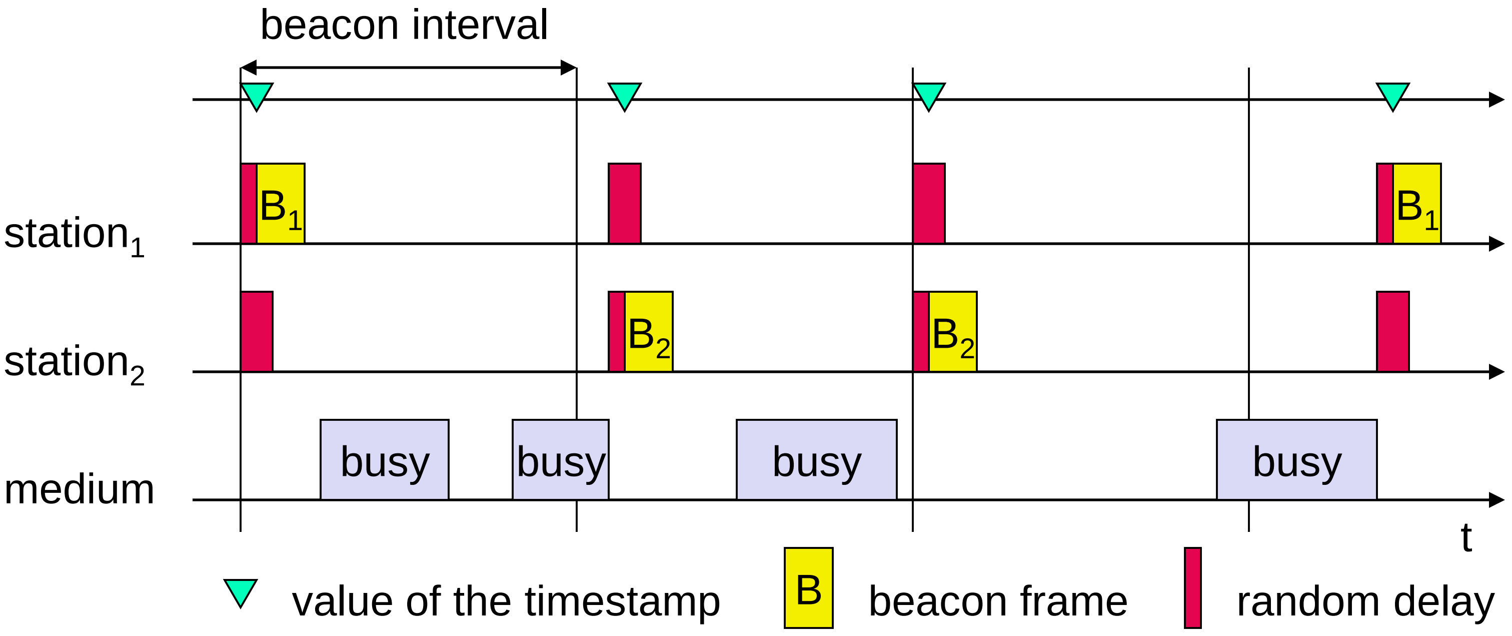
- All STAs within a BSS are synchronized to a common clock
  - Infrastructure mode: AP is the timing master
    - periodically transmits Beacon frames containing Timing Synchronization function (TSF)
    - Receiving stations accepts the timestamp value in TSF
  - Ad hoc mode: TSF implements a distributed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

Synchronization using a Beacon (infrastructure mode)



Source: Schiller

Synchronization using a Beacon (ad-hoc mode)



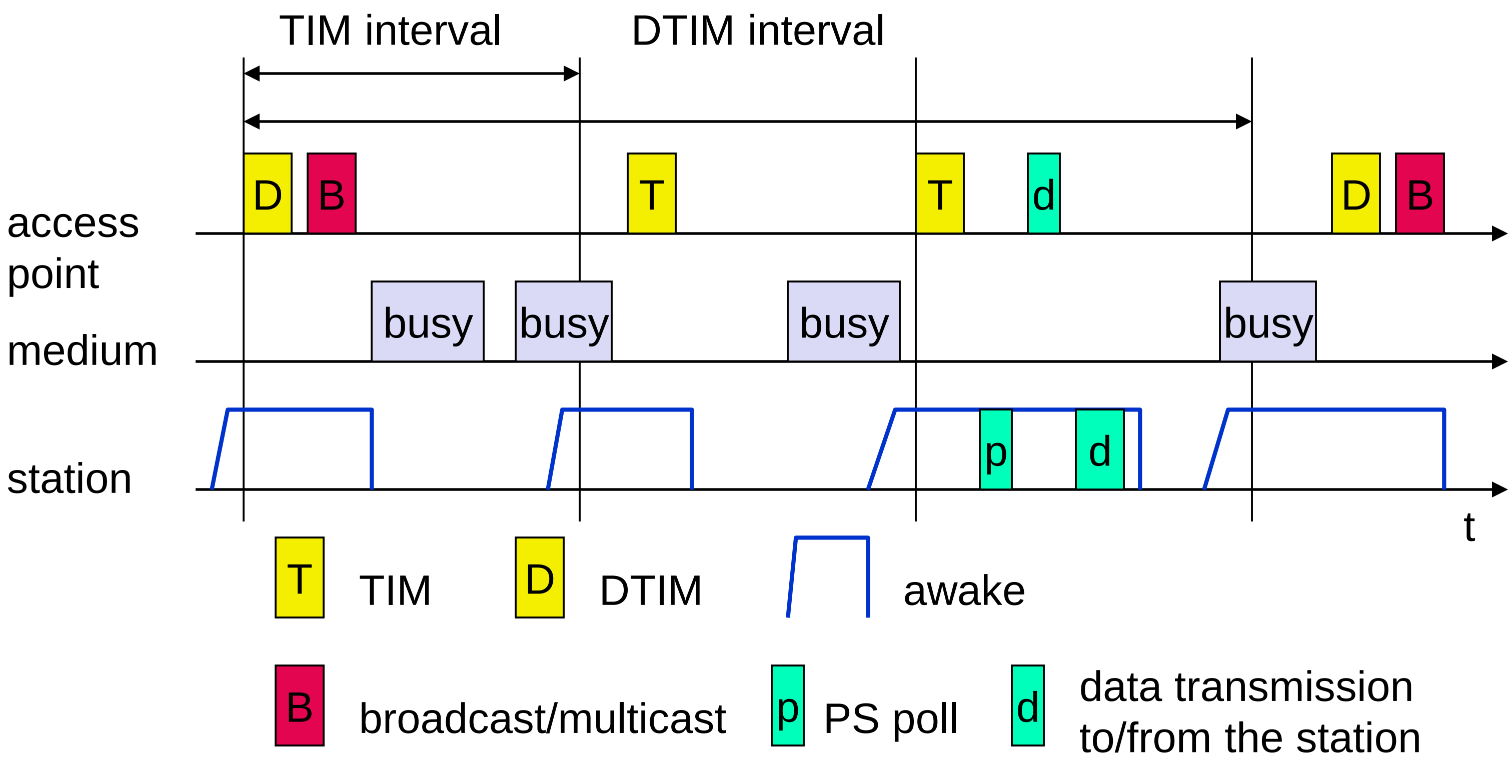
802.11 - Power management

- 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

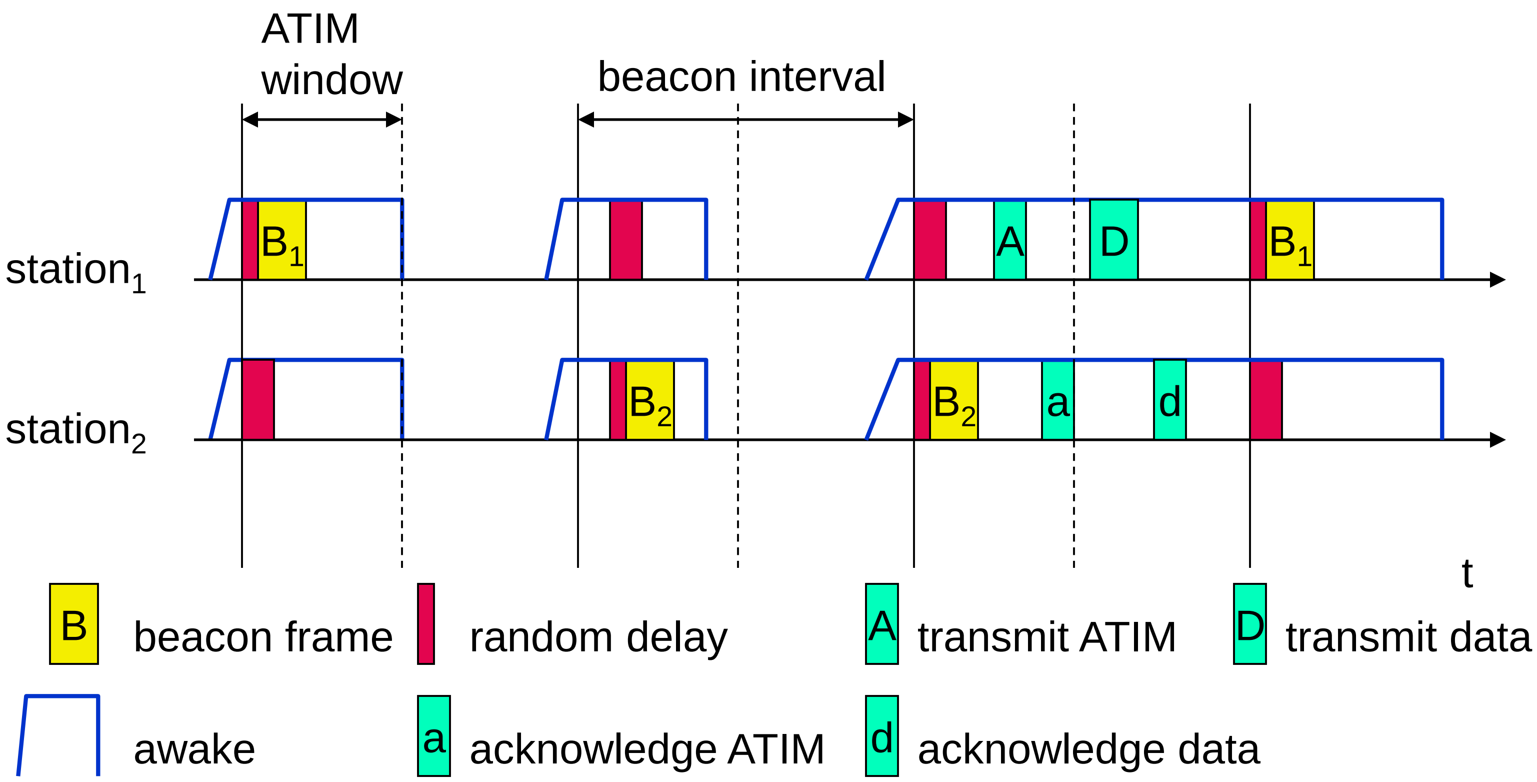
- Power Saving in infrastructure mode
  - Nodes can go into sleep or standby mode
  - An Access Point periodically transmits a beacon indicating which nodes have packets waiting for them
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a node has a packet waiting, then it sends a PS-Poll
    - After waiting for a backoff interval in [0,CWmin]
  - 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)



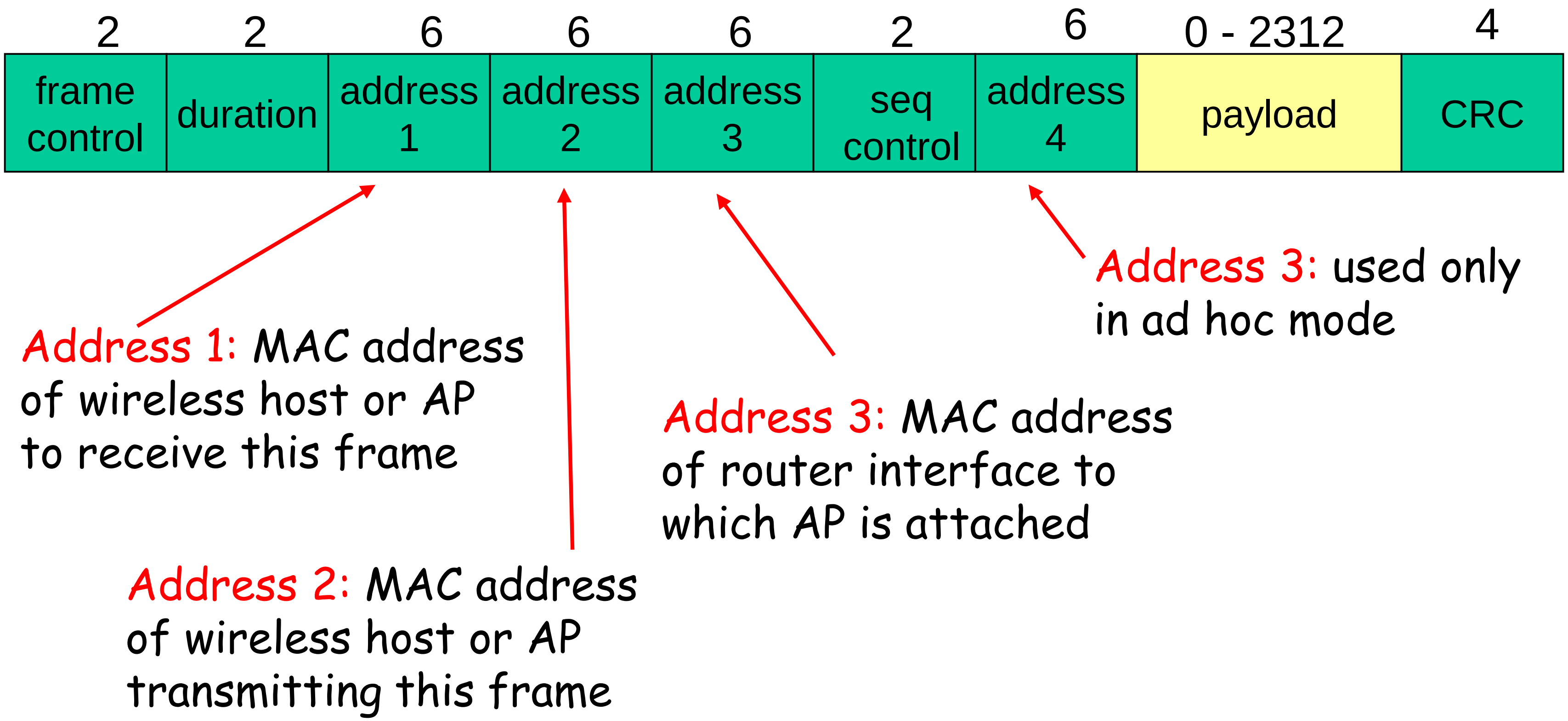
802.11 - Frame format

- 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

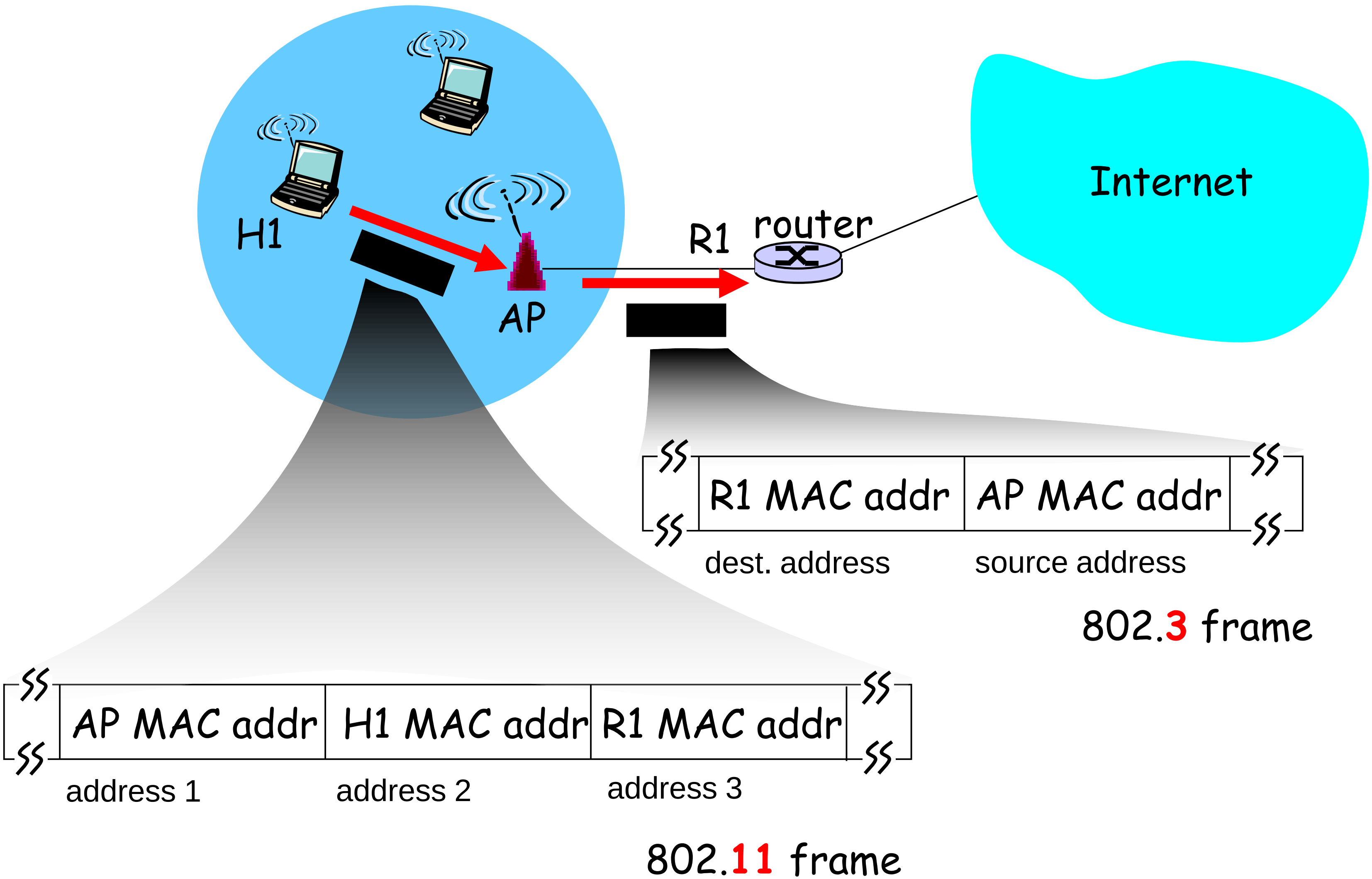
bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

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

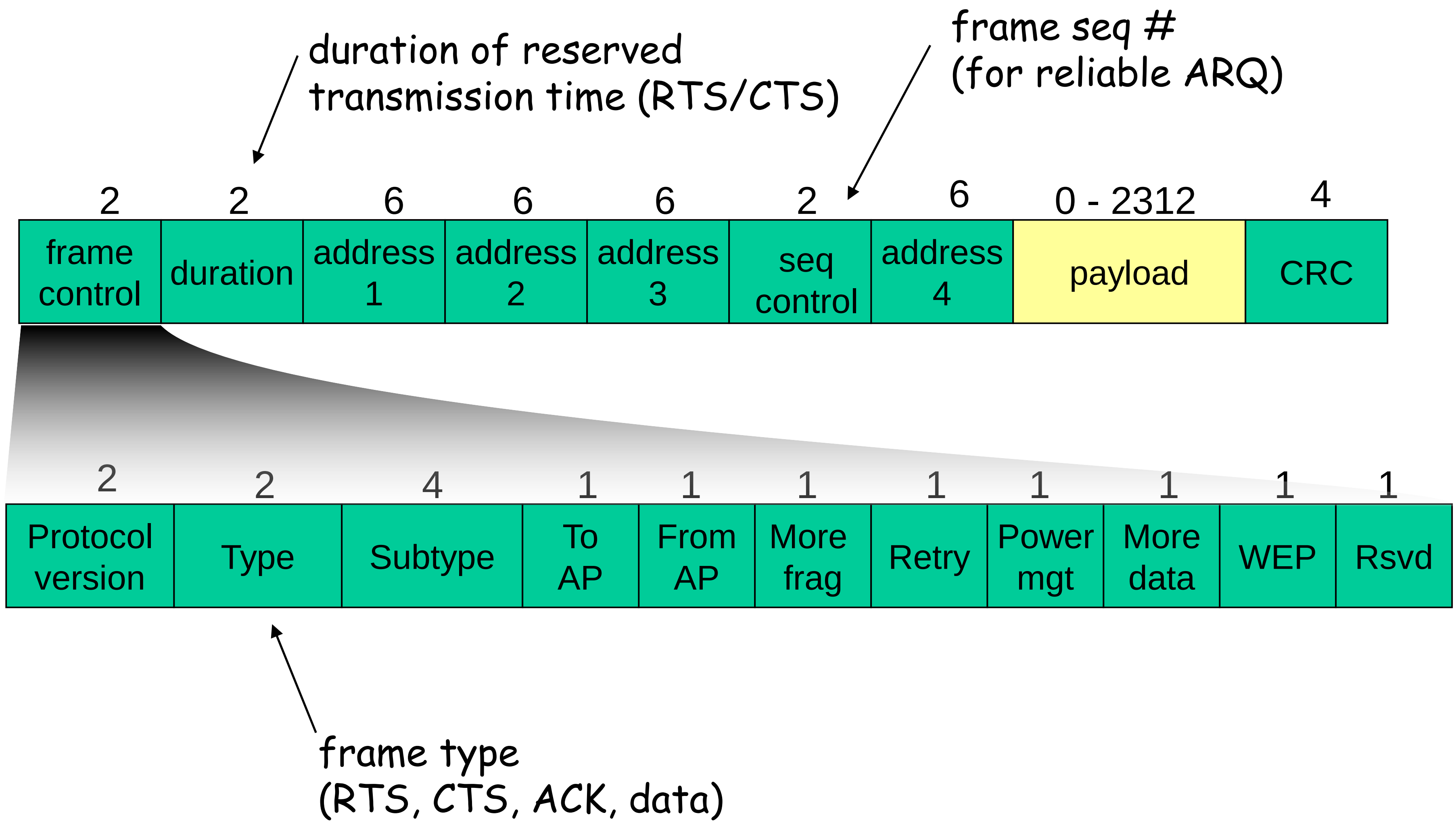
802.11 frame: addressing



802.11 frame: addressing



802.11 frame: more



Types of Frames

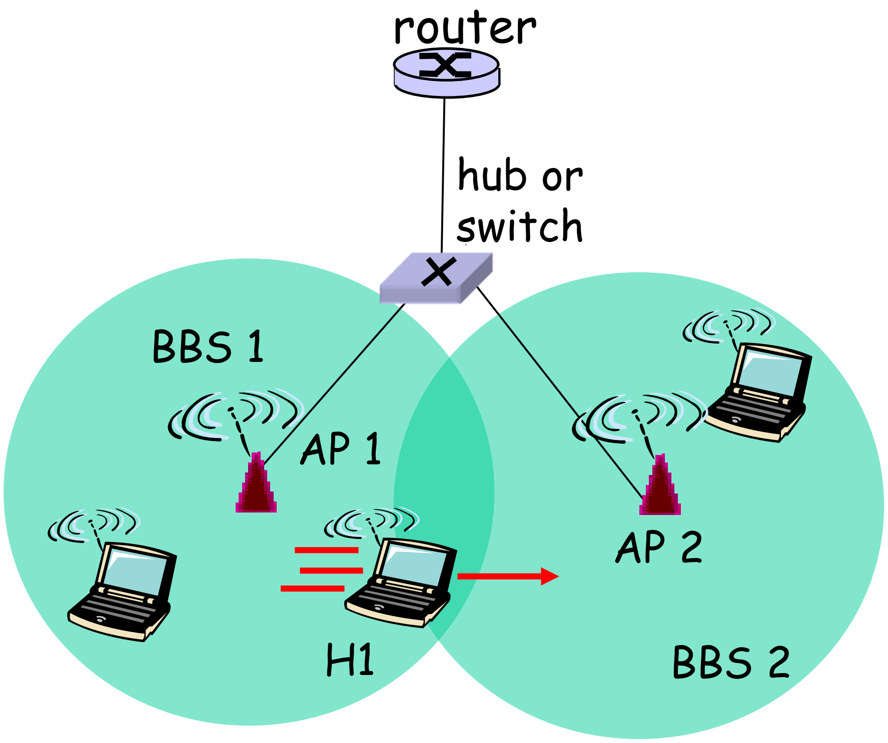
- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
- Management Frames
  - Beacons
  - Probe Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
  - Authentication/Deauthentication
  - ATIM
- Data Frames

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 - Roaming within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning
  - switch will see frame from H1 and “remember” which switch port can be used to reach H1



802.11 - Point Coordination Function

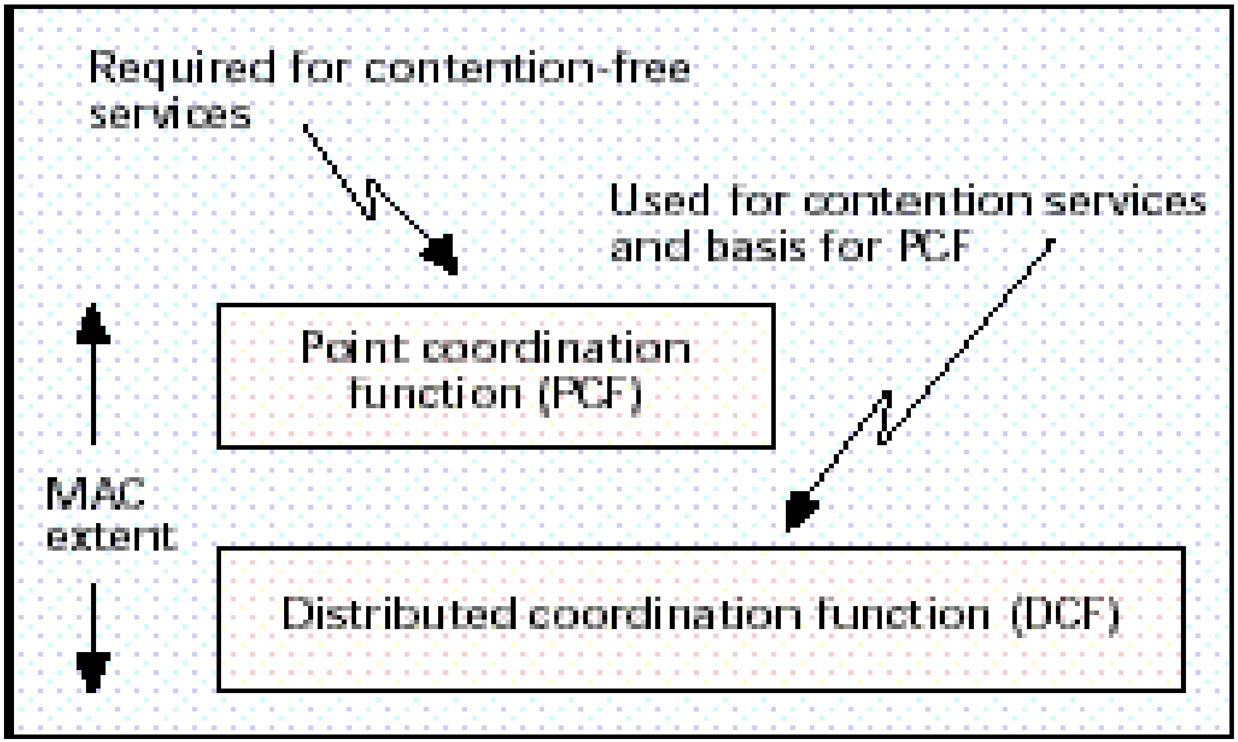
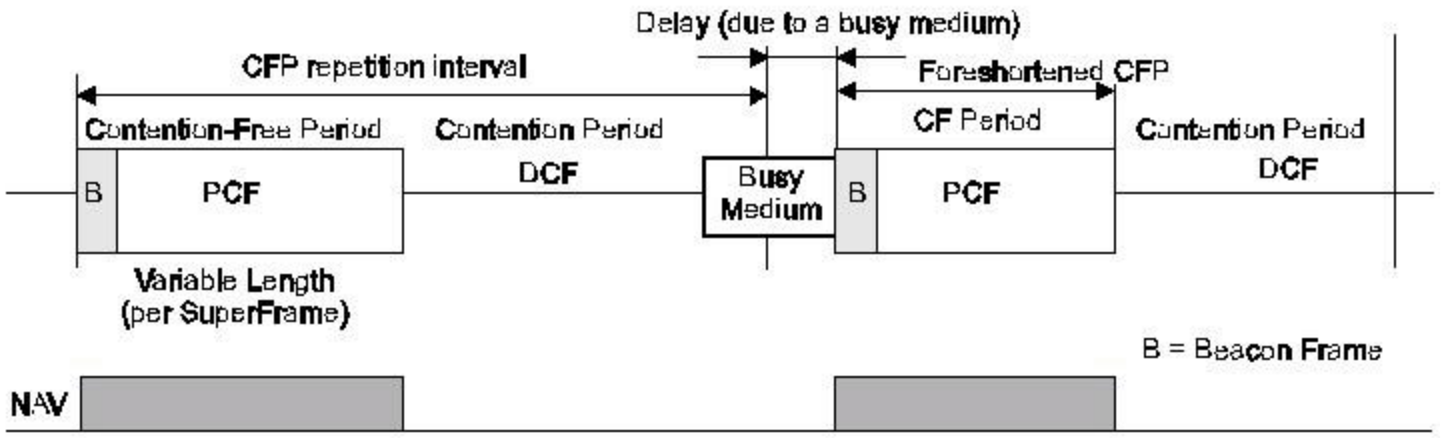


Figure 4. *MAC architecture.*

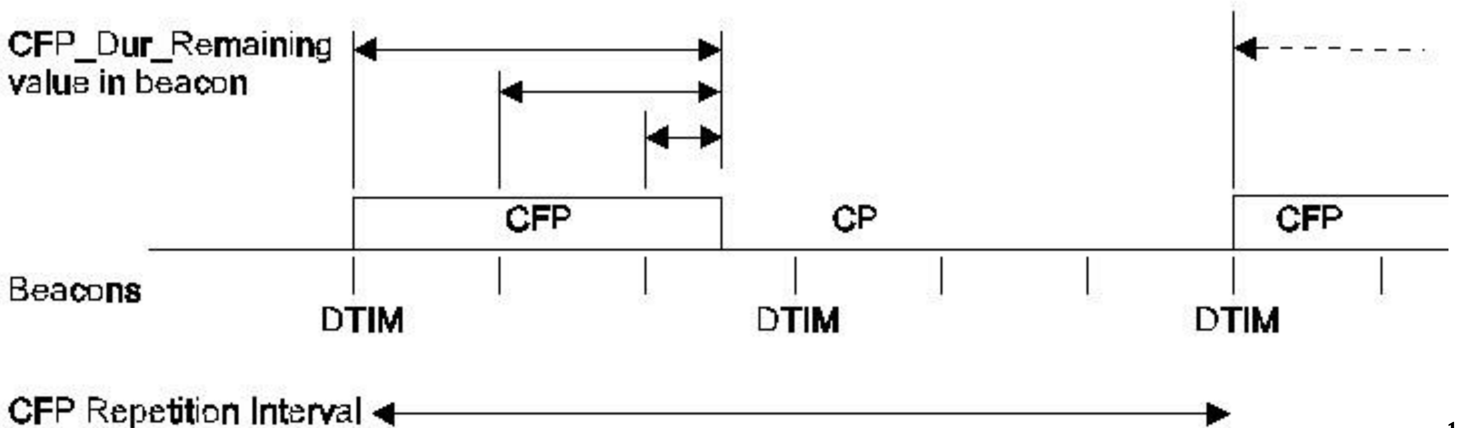
Coexistence of PCF and DCF

- 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

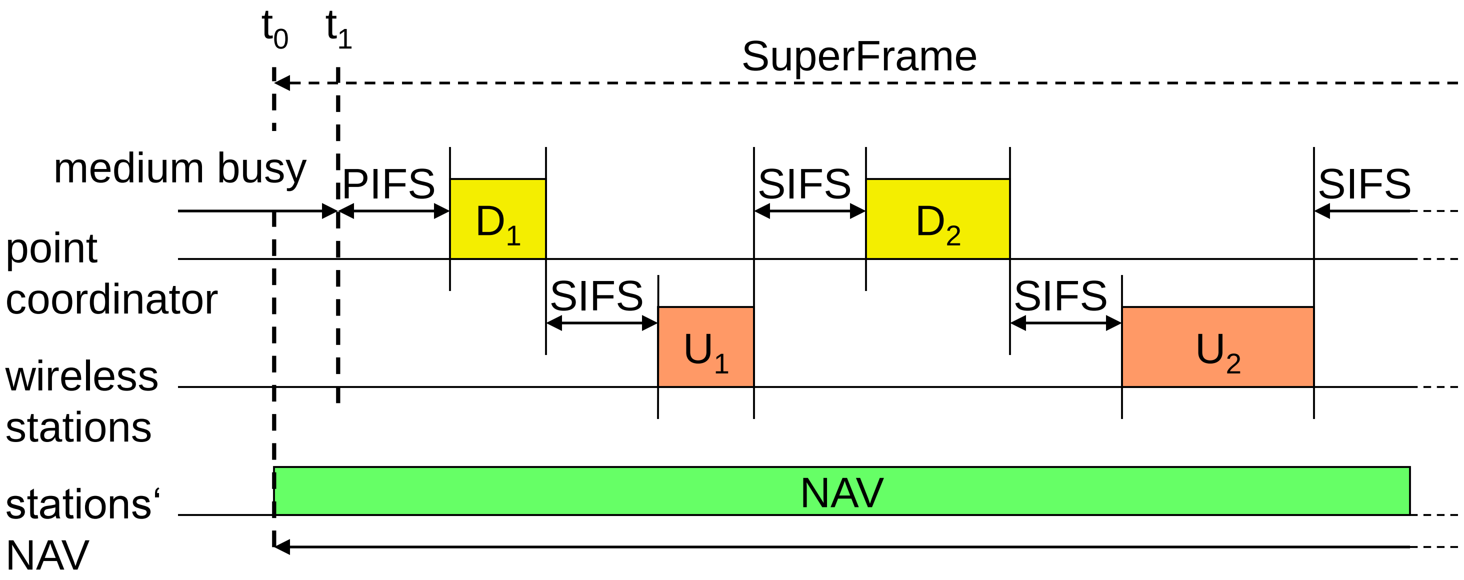
CFP structure and Timing



CFP/CP Alternation and Beacon Periods

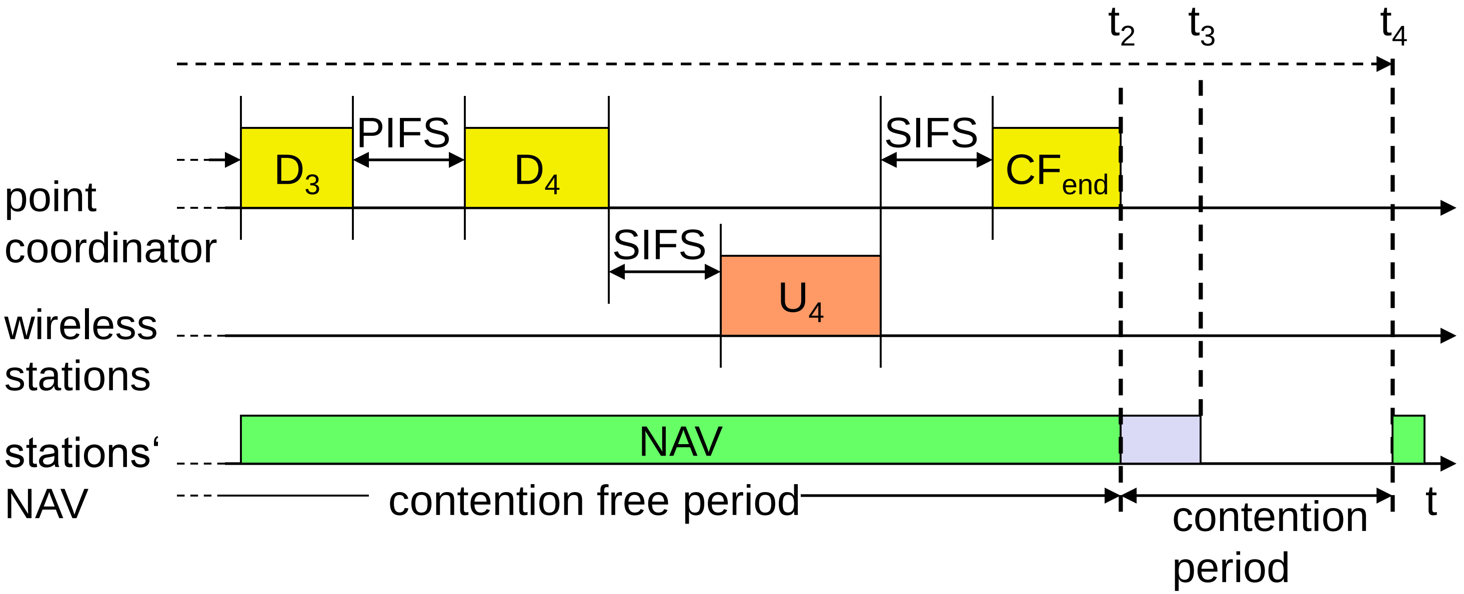


802.11 - PCF I



Source: Schiller

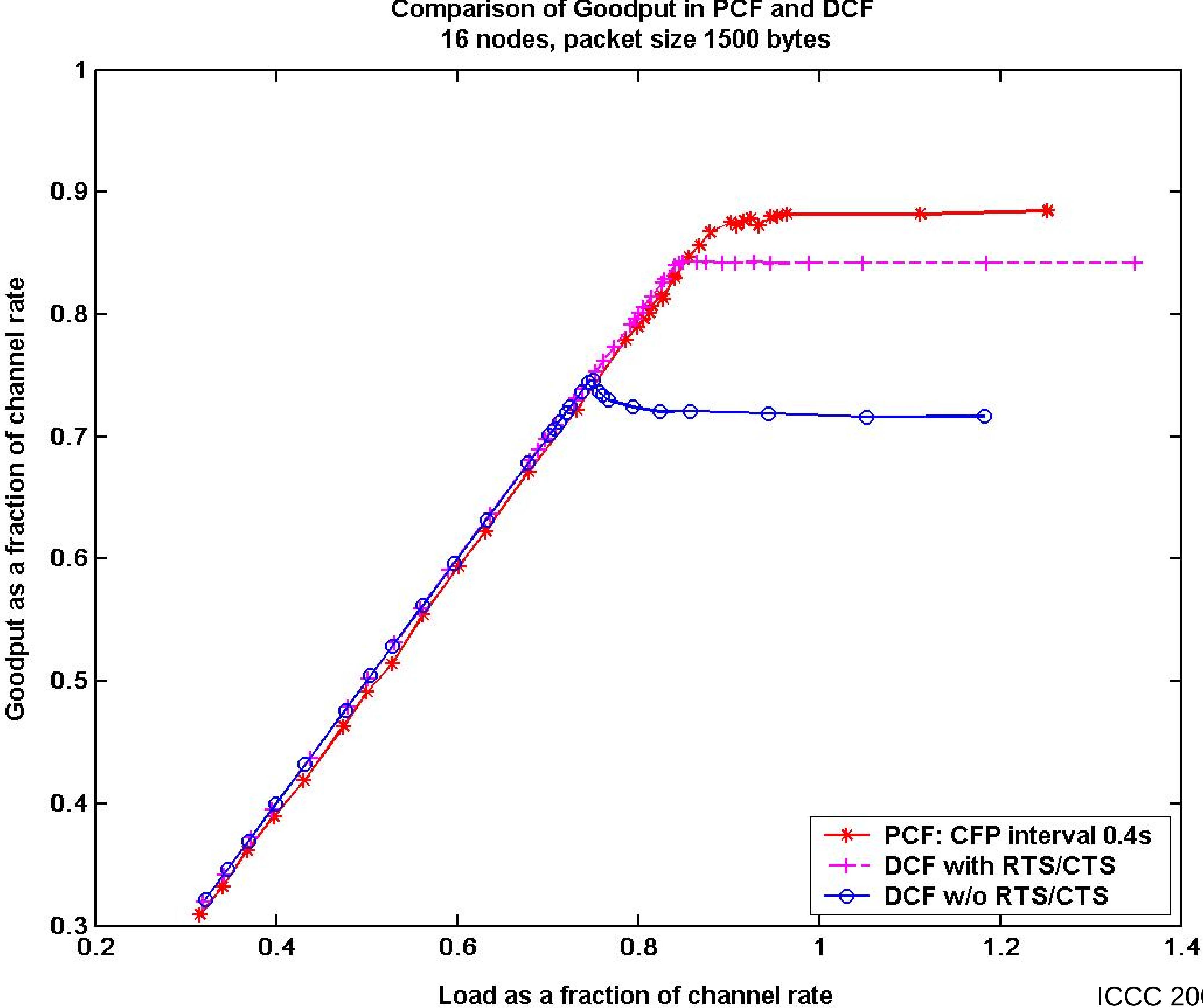
802.11 - PCF II



t2
t3
t4
PIFS
SIFS
D3
D4
CFend
point coordinator
SIFS
U4
wireless stations
NAV
stations' 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
Load 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
PCF: CFP interval 0.4s
DCF with RTS/CTS
DCF w/o RTS/CTS

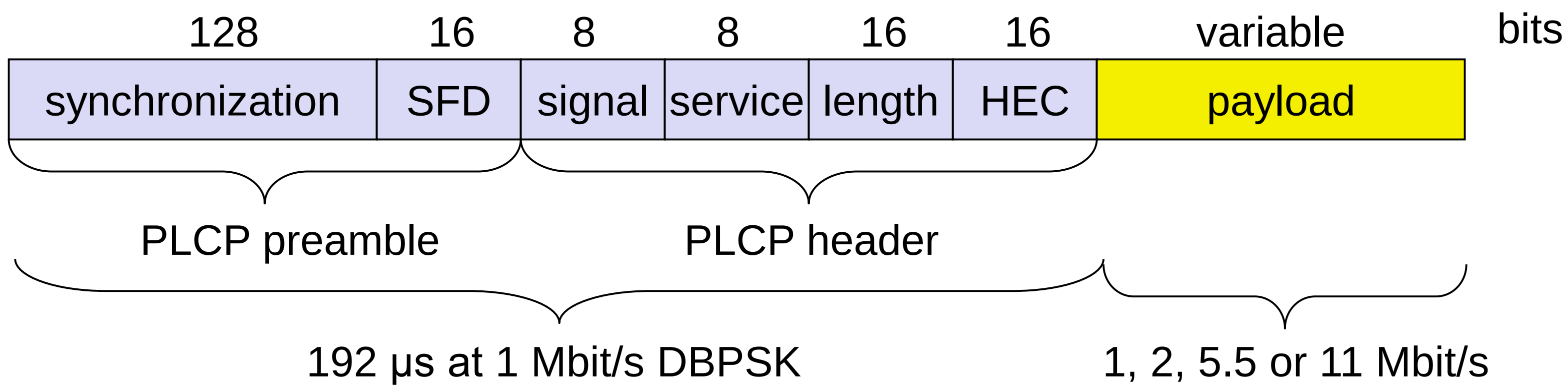
ICCC 2002

WLAN: IEEE 802.11b

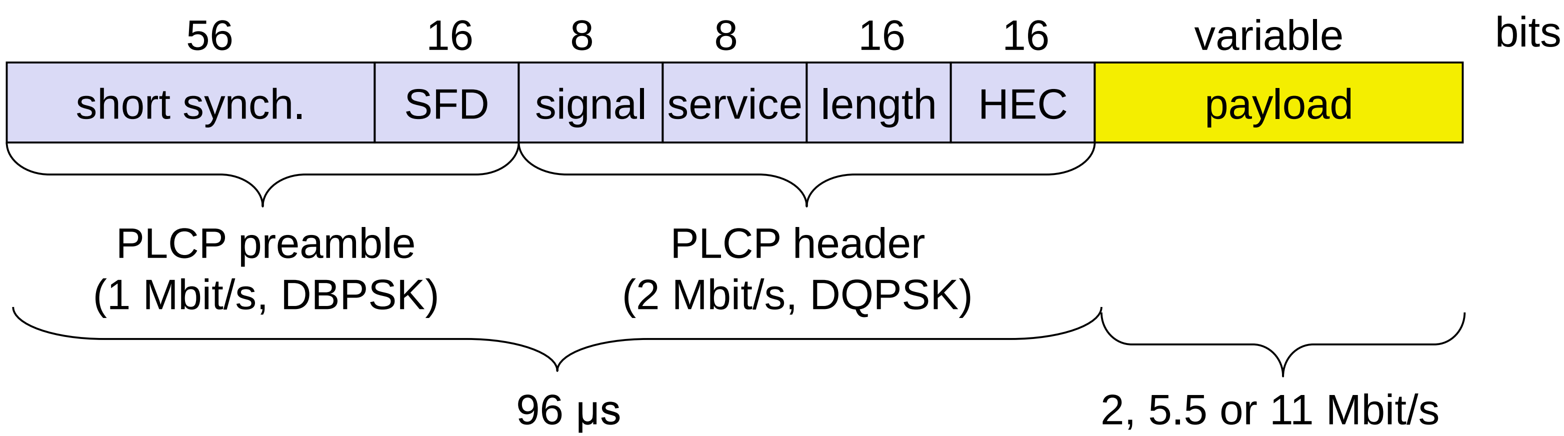
- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Cost
  - 100$ adapter, 250$ base station, dropping
- Availability
  - Many products, many vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11b – PHY frame formats

Long PLCP PPDU format

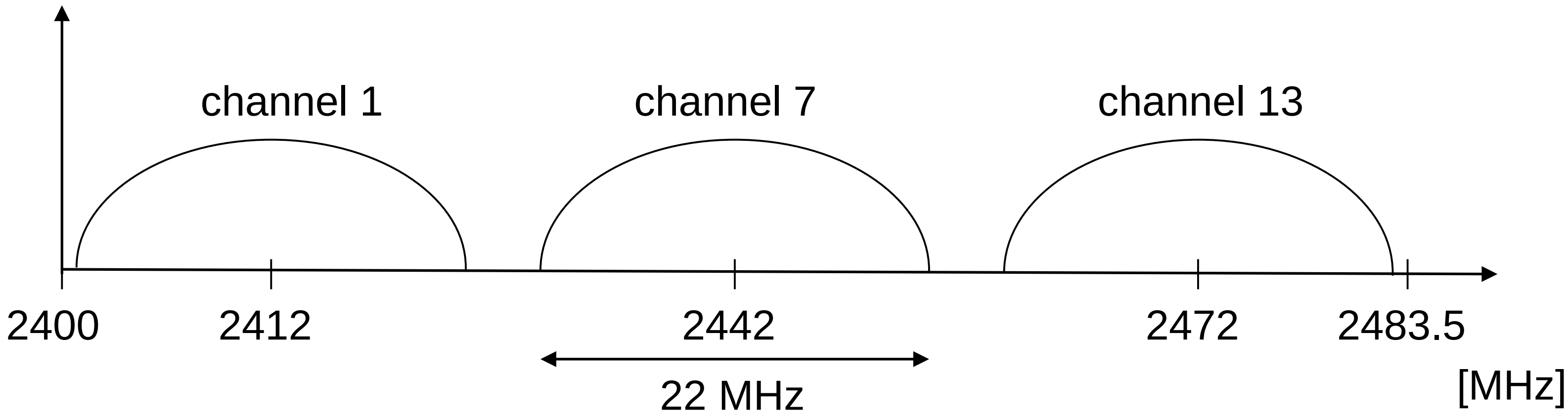


Short PLCP PPDU format (optional)

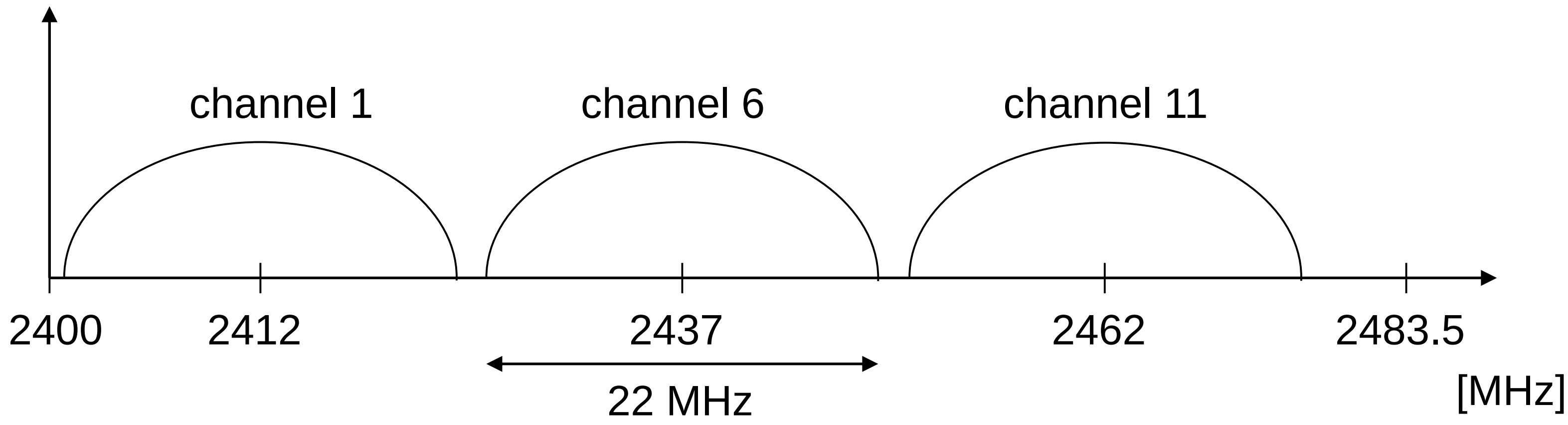


Channel selection (non-overlapping)

Europe (ETSI)



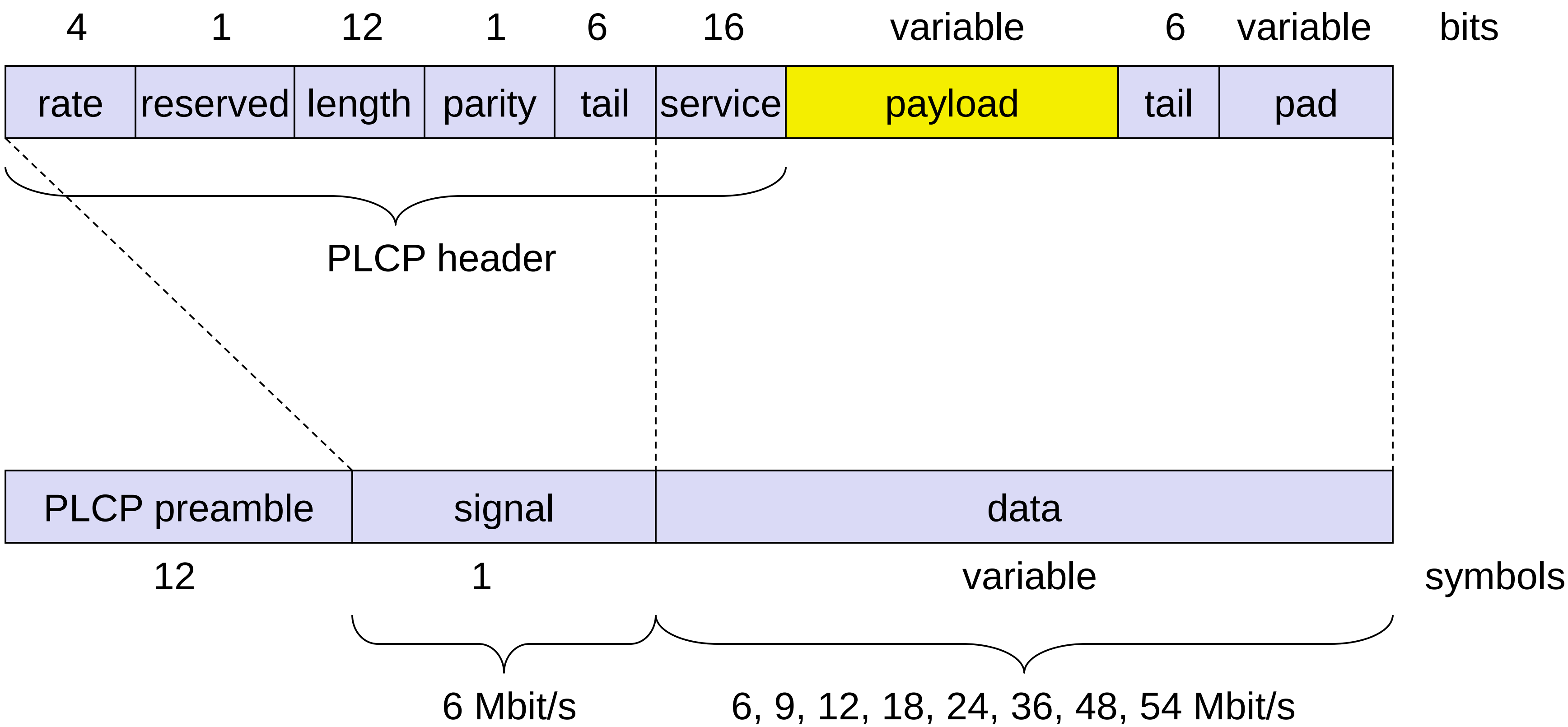
US (FCC)/Canada (IC)



WLAN: IEEE 802.11a

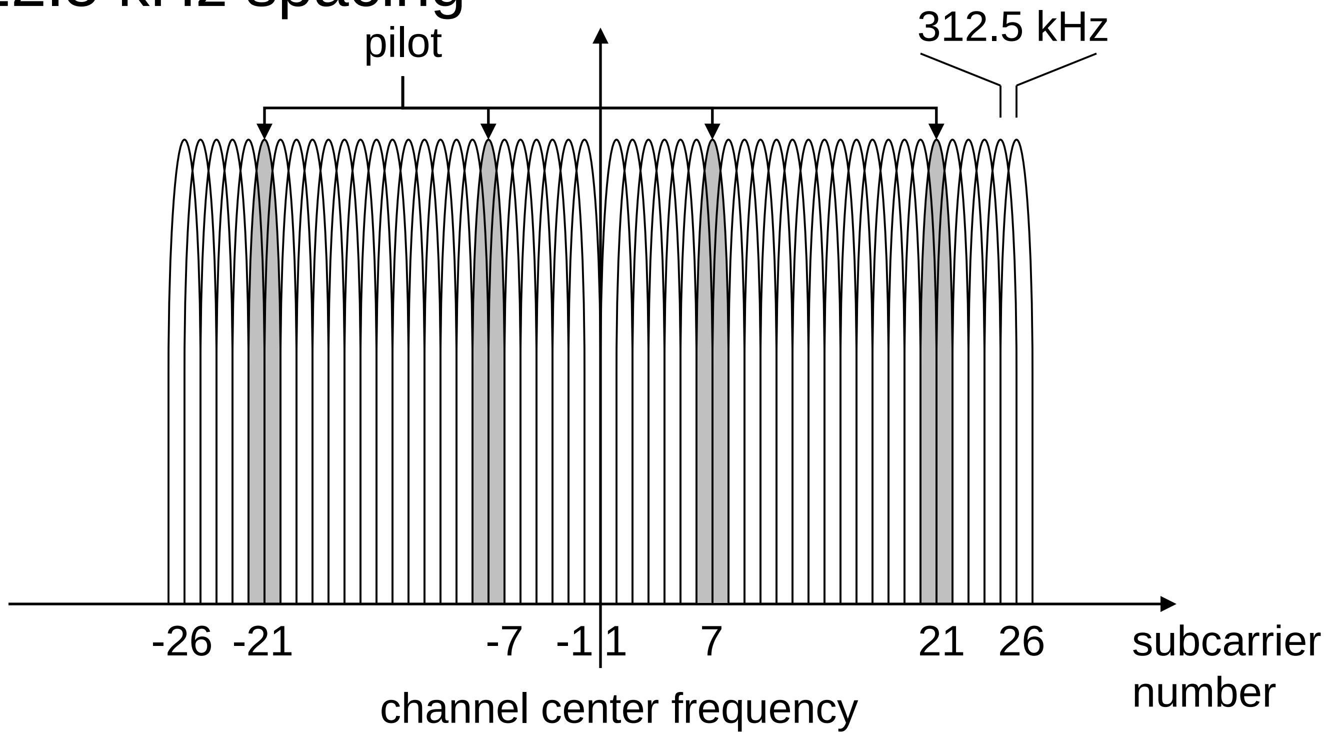
- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Cost
  - 280$ adapter, 500$ base station
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS

IEEE 802.11a – PHY frame format

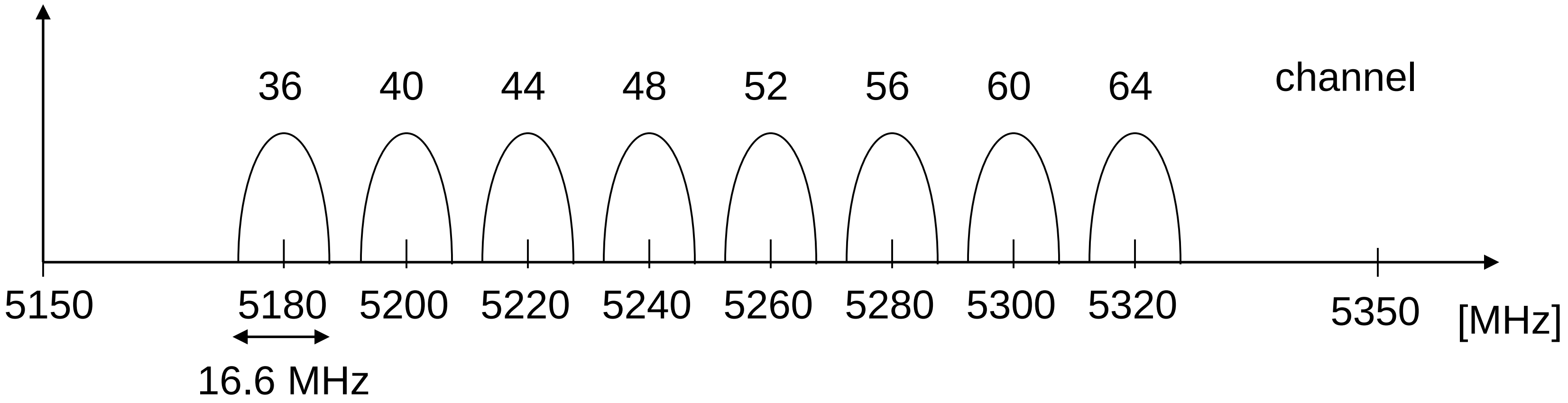


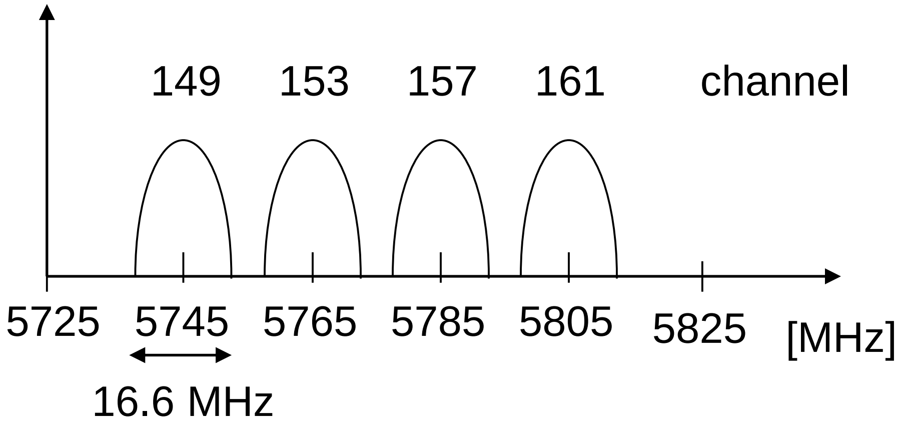
OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers (64 in total)
- 48 data + 4 pilot
- 312.5 kHz spacing



Operating channels for 802.11a





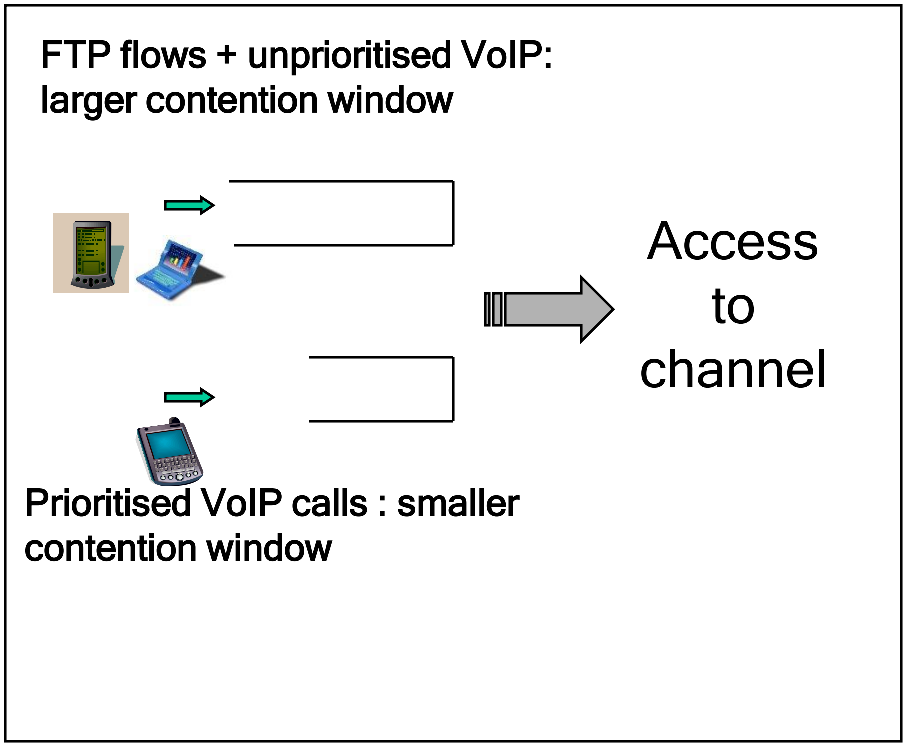
center frequency =
5000 + 5*channel number [MHz]

WLAN: IEEE 802.11e

- 802.11e: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.

- EDCF
  - Contention Window based prioritization
    - Real-time
    - Best effort
  - Virtual collision resolved in favor of higher priority

Extending DCF: EDCF



EDCF improves upon DCF by prioritising traffic

- Each traffic class can have a different contention window
- Different traffic classes to use different interframe spaces, called Arbitration Interframe Space (AIFS)

EDCF contention window parameters

- VoIP (priority): 7-31
- FTP w/o priority: 32-1023
- VoIP w/o priority:32-1023

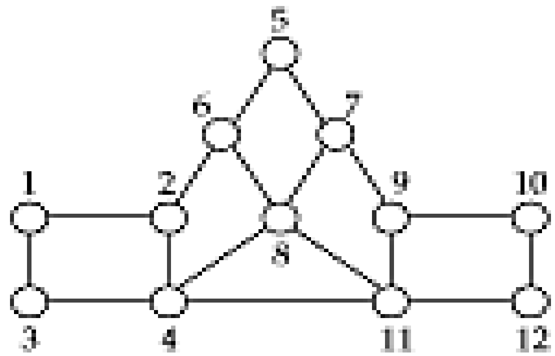
IEEE 802.11 Summary

- 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

Mobile IP

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

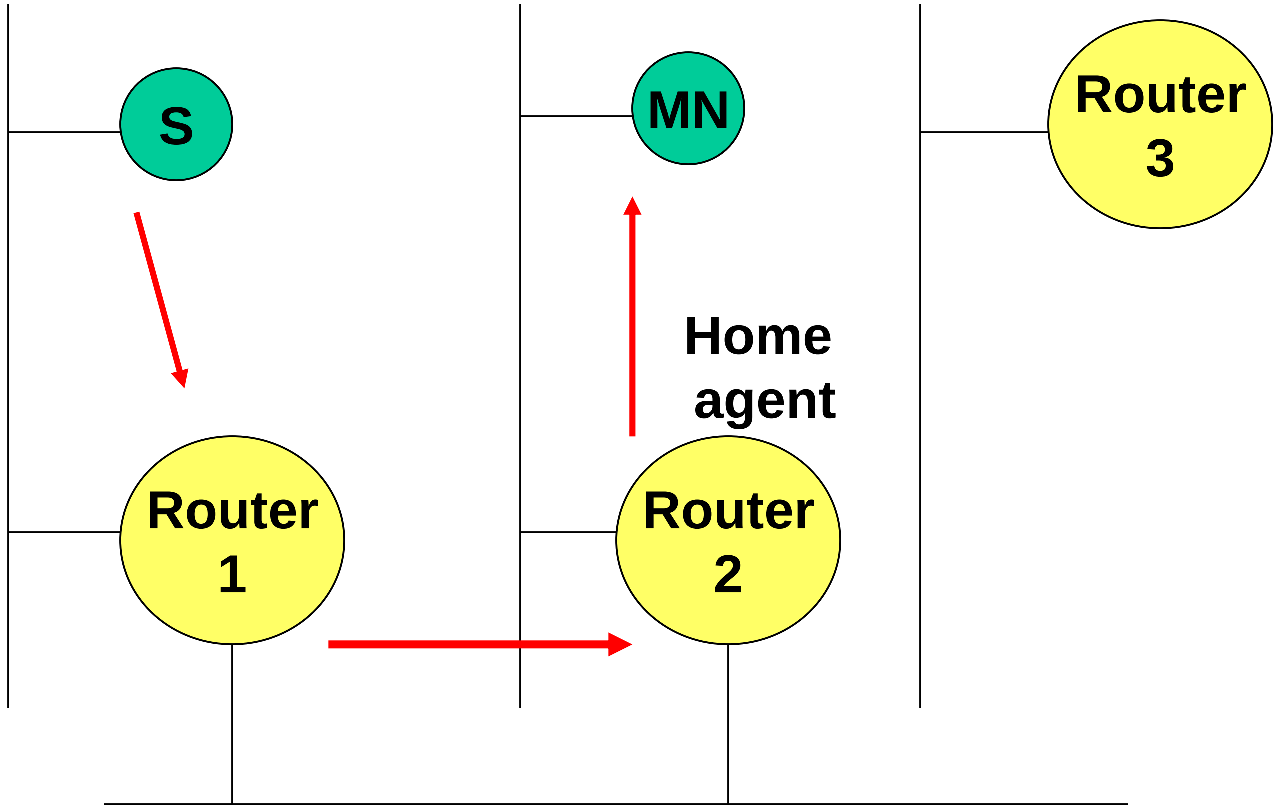
Routing and Mobility

- 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)

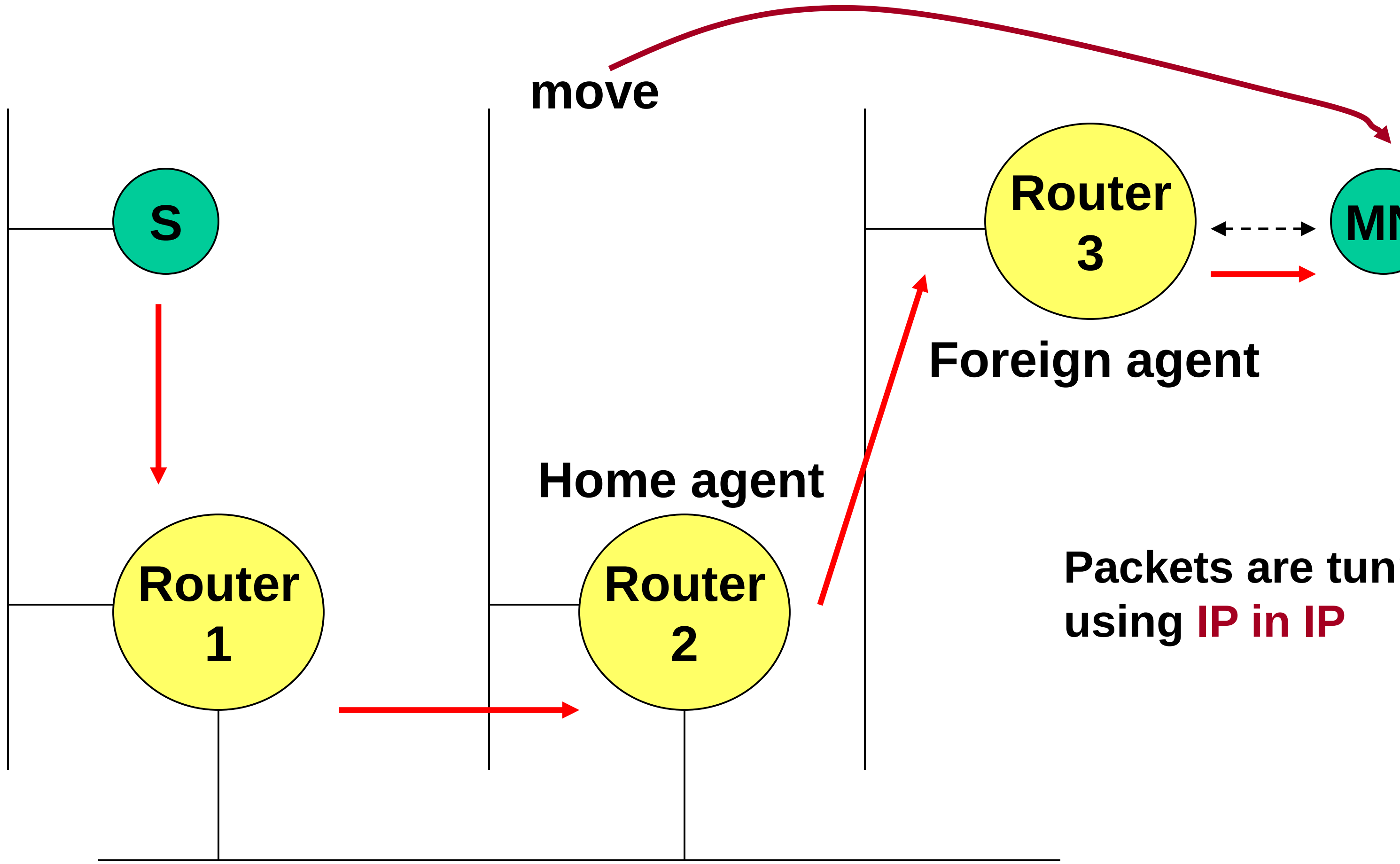
Mobile IP (RFC 3344): Motivation

- 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

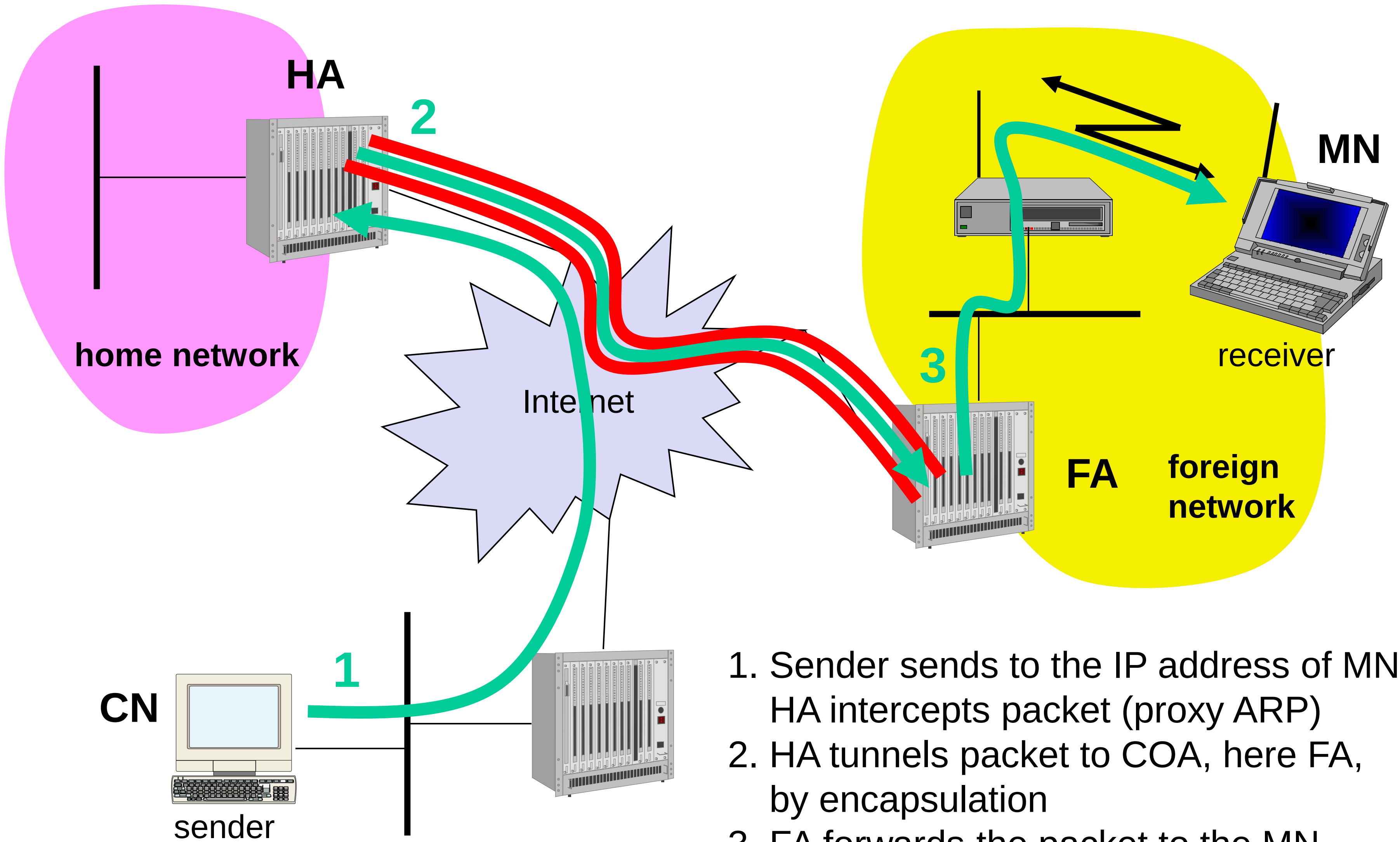


Packets are tunneled using IP in IP

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)

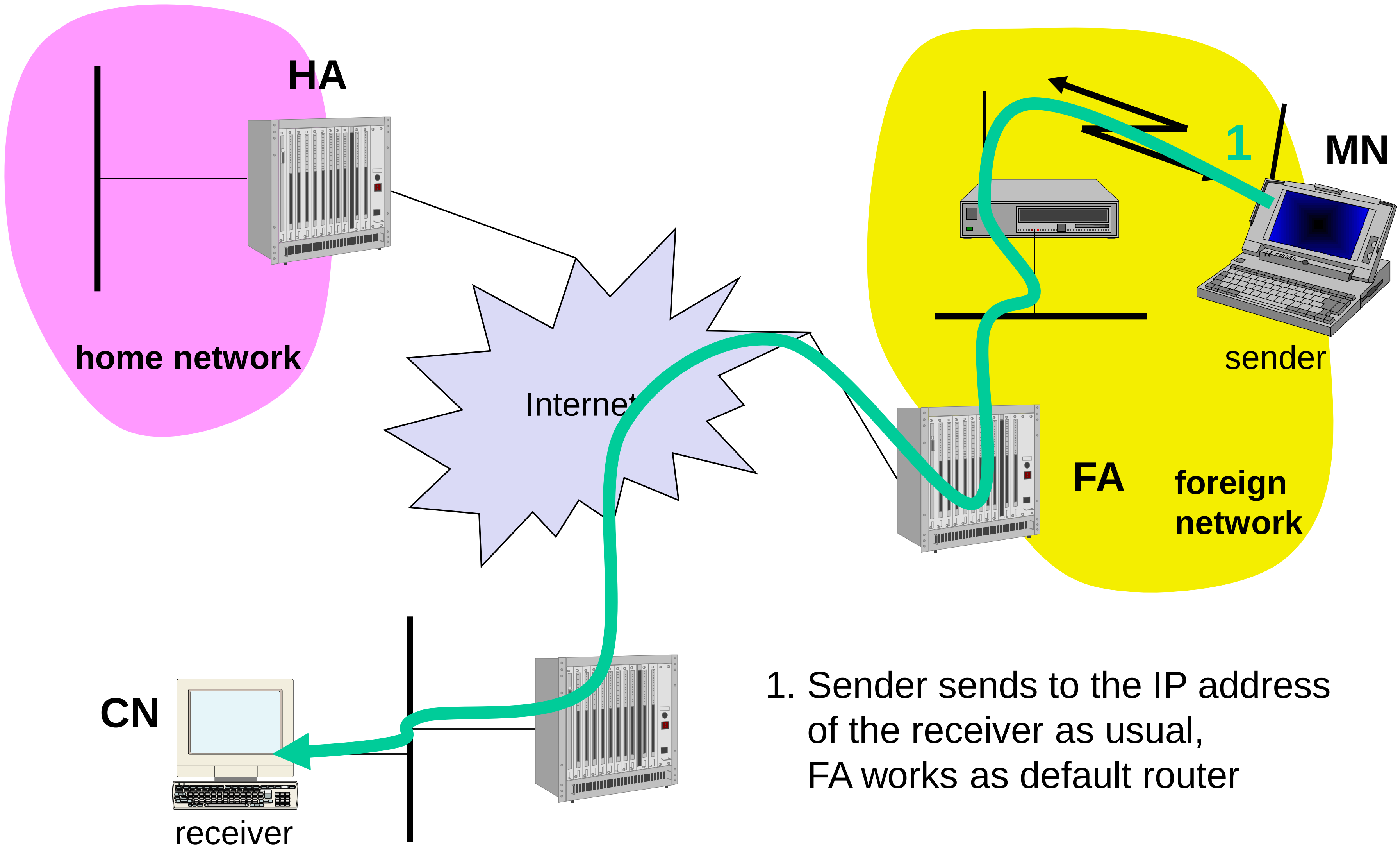
Data transfer to the mobile system



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

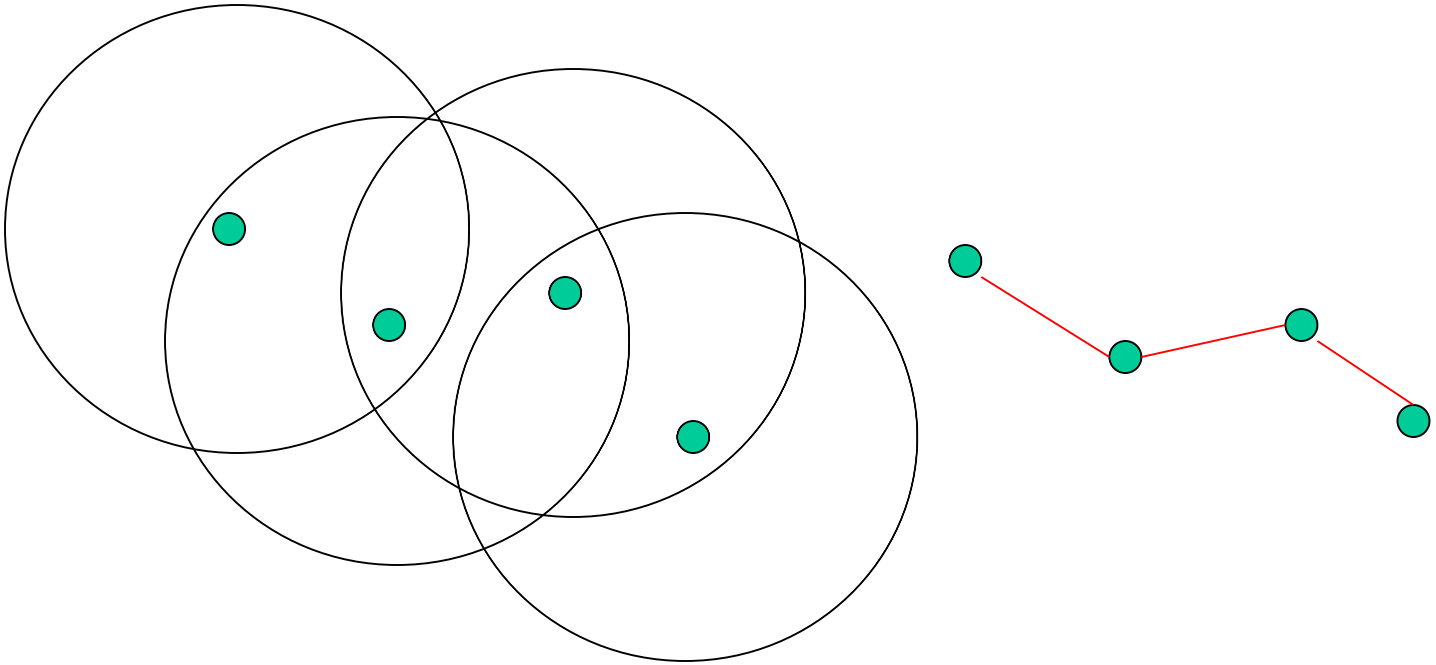
- Reverse Tunneling
  - firewalls permit only “topological correct“ addresses
  - a packet from the MN encapsulated by the FA is now topological correct

- 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

Mesh and Adhoc Networks

Multi-Hop Wireless

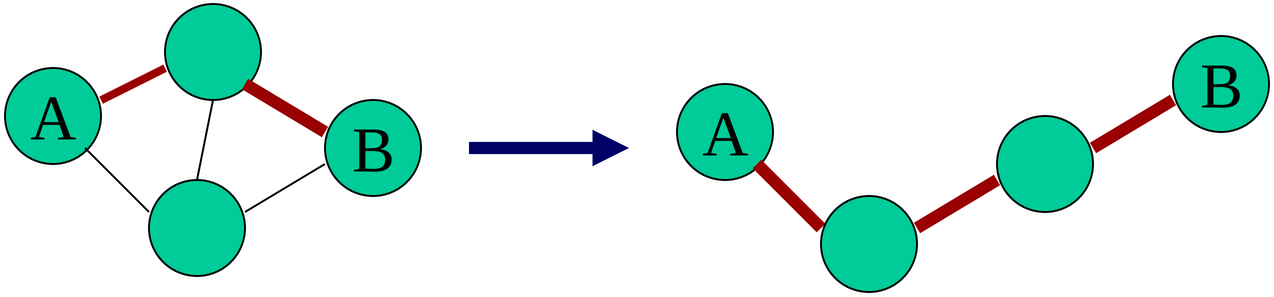
- May need to traverse multiple links to reach destination



- Mobility causes route changes

Mobile Ad Hoc Networks (MANET)

- Host movement frequent
- Topology change frequent



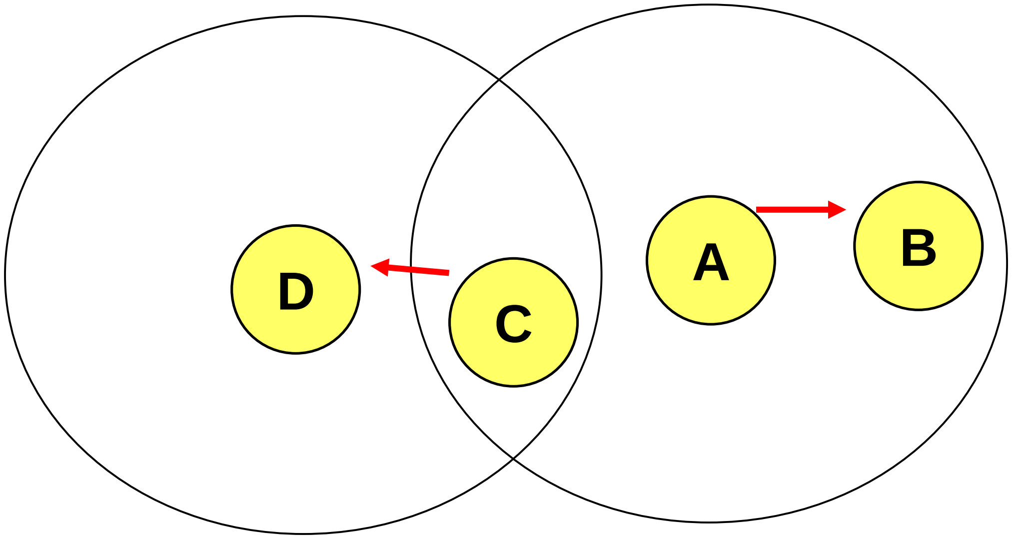
- No cellular infrastructure. Multi-hop wireless links.
- Data must be routed via intermediate nodes.

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

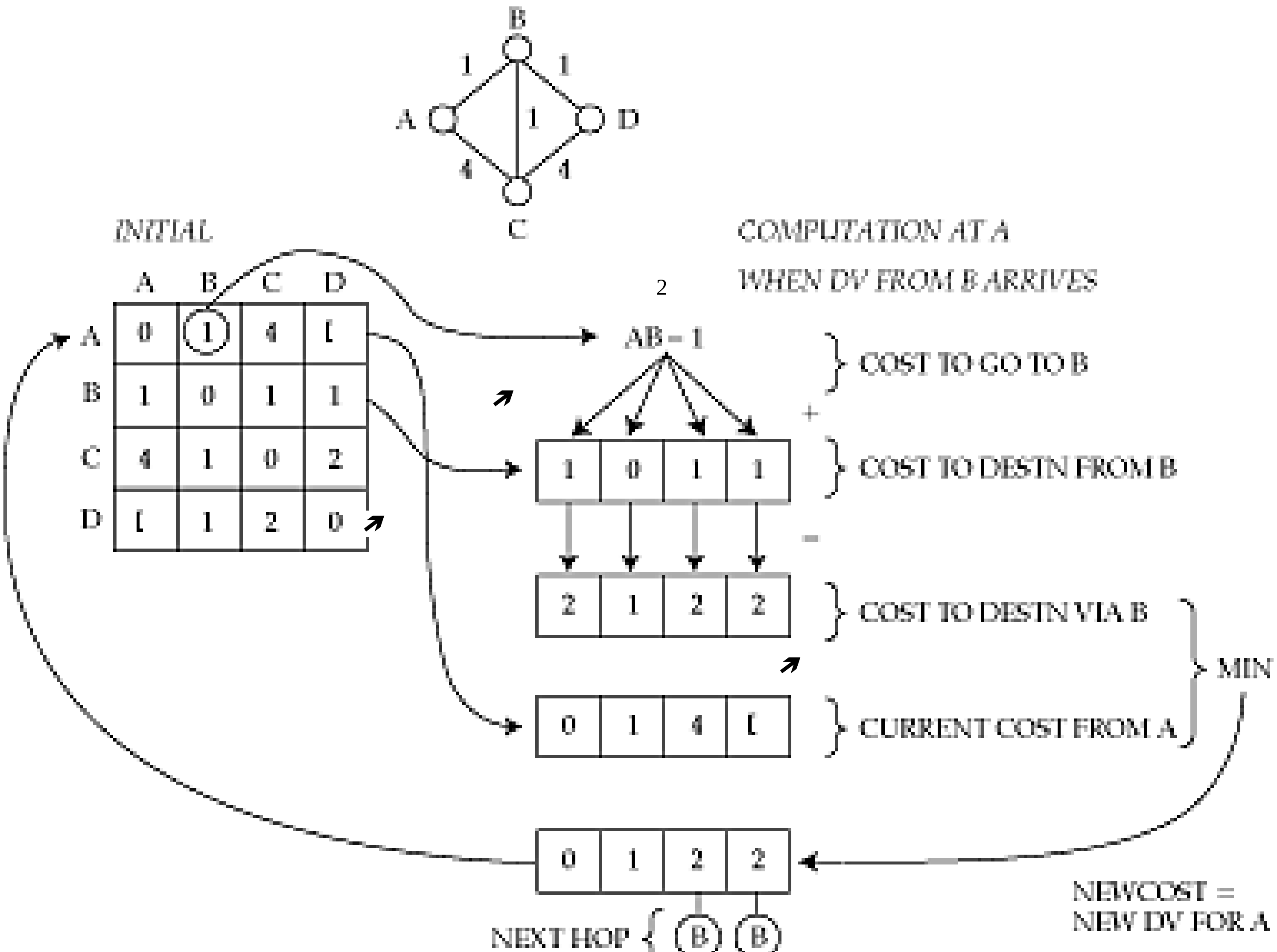
Distance-vector & Link-state Routing

- Both assume router knows
  - address of each neighbor
  - cost of reaching each neighbor
- Both allow a router to determine global routing information by talking to its neighbors

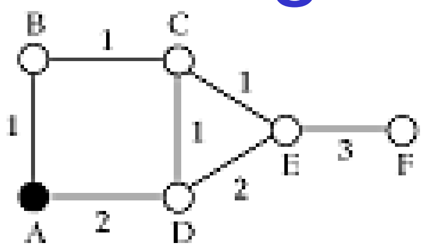
- Distance vector - router knows cost to each destination

- Link state - router knows entire network topology and computes shortest path

Distance Vector Routing: Example

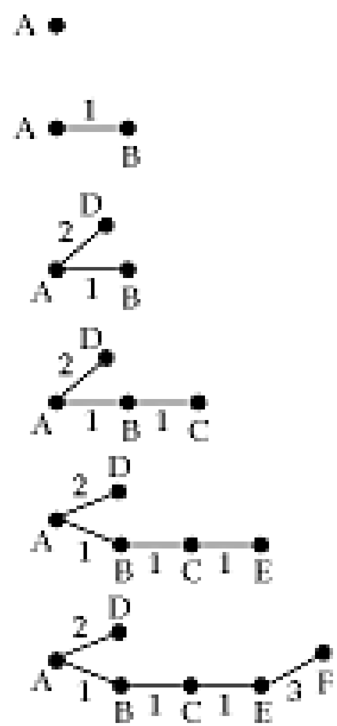


Link State Routing: Example



B(A,1) means B was reached by A, cost 1

PERMANENT	TEMPORARY	COMMENTS
A	B(A,1), D(A,2)	ROOT AND ITS NEIGHBORS
A, B(A,1)	D(A,2), C(B,2)	ADD C(B,2)
A, B(A,1) D(A,2)	E(D,4), C(B,2)	C(D,3) DIDN'T MAKE IT
A, B(A,1) D(A,2), C(B,2)	E(C,3)	E(D,4) TOO LONG
A, B(A,1) D(A,2), C(B,2) E(C,3)	F(E,6)	
A, B(A,1) C(B,2), D(A,2) E(C,3), F(E,6)	NULL	STOP



MANET 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)

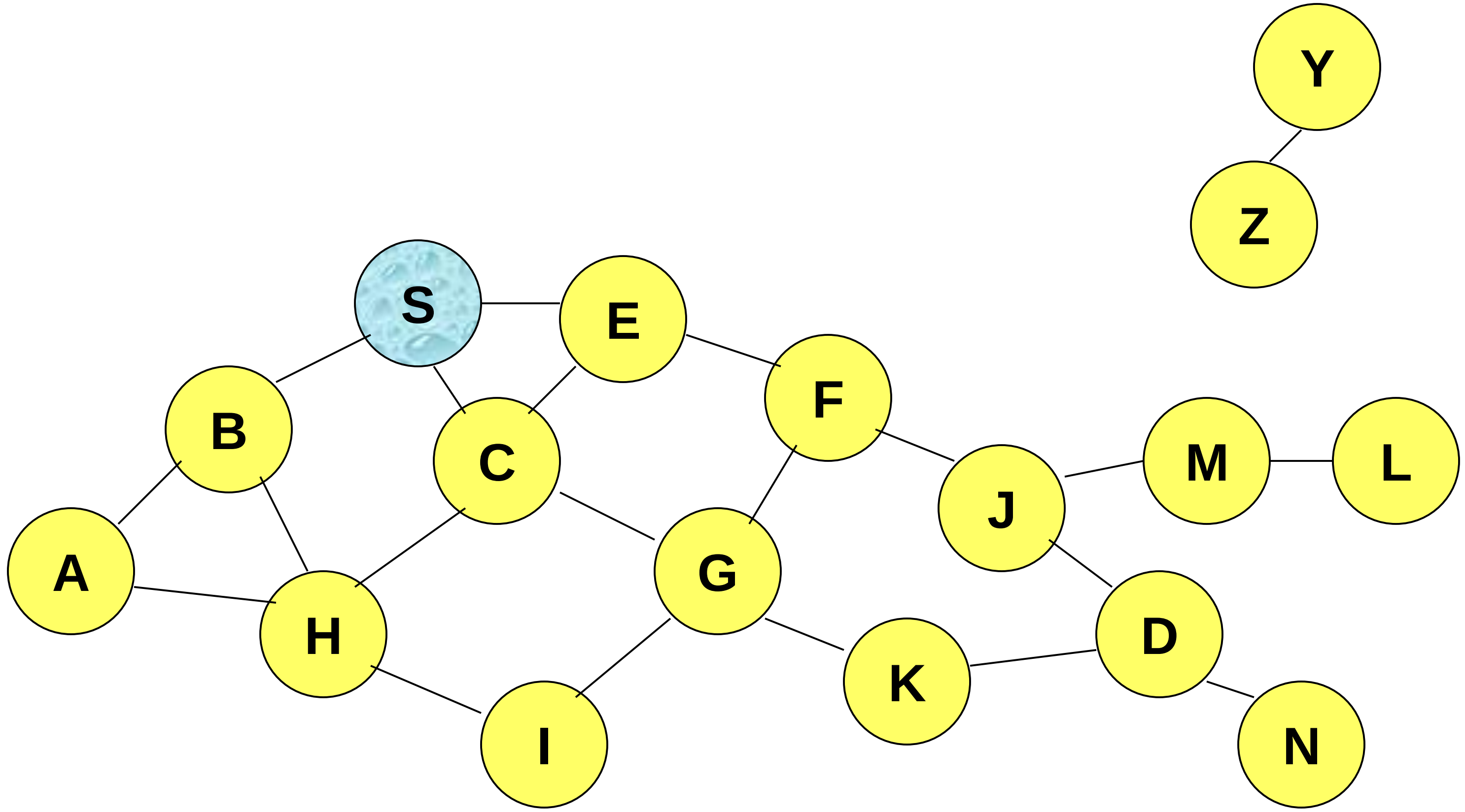
- Reactive protocols
  - Determine route if and when needed
  - Source initiates route discovery
  - Example: DSR (dynamic source routing)

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

Dynamic Source Routing (DSR)

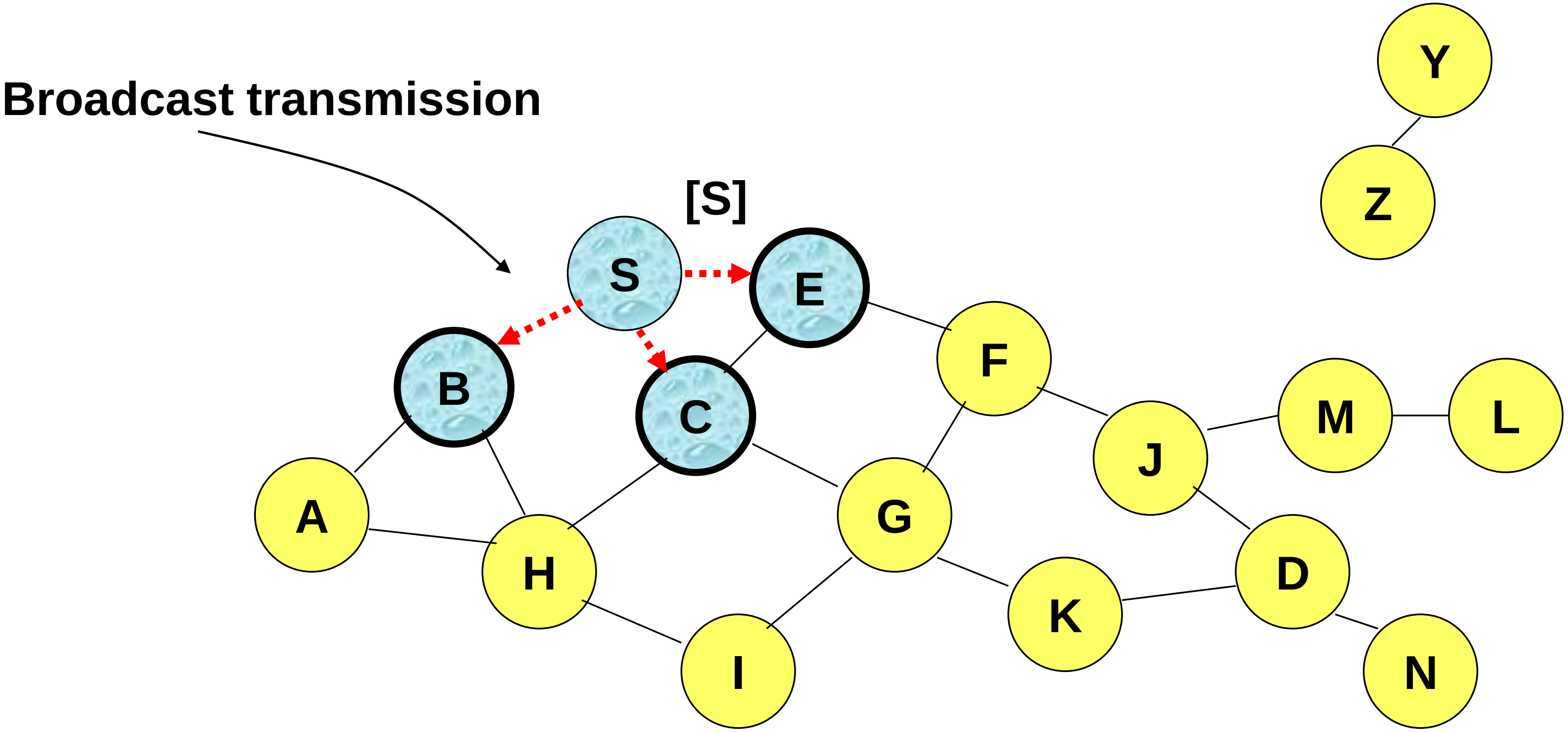
- Route Discovery Phase:
  - Initiated by source node S that wants to send packet to destination node D
  - Route Request (RREQ) floods through the network
  - Each node *appends own identifier* when forwarding RREQ
- Route Reply Phase:
  - D on receiving the first RREQ, sends a Route Reply (RREP)
  - 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

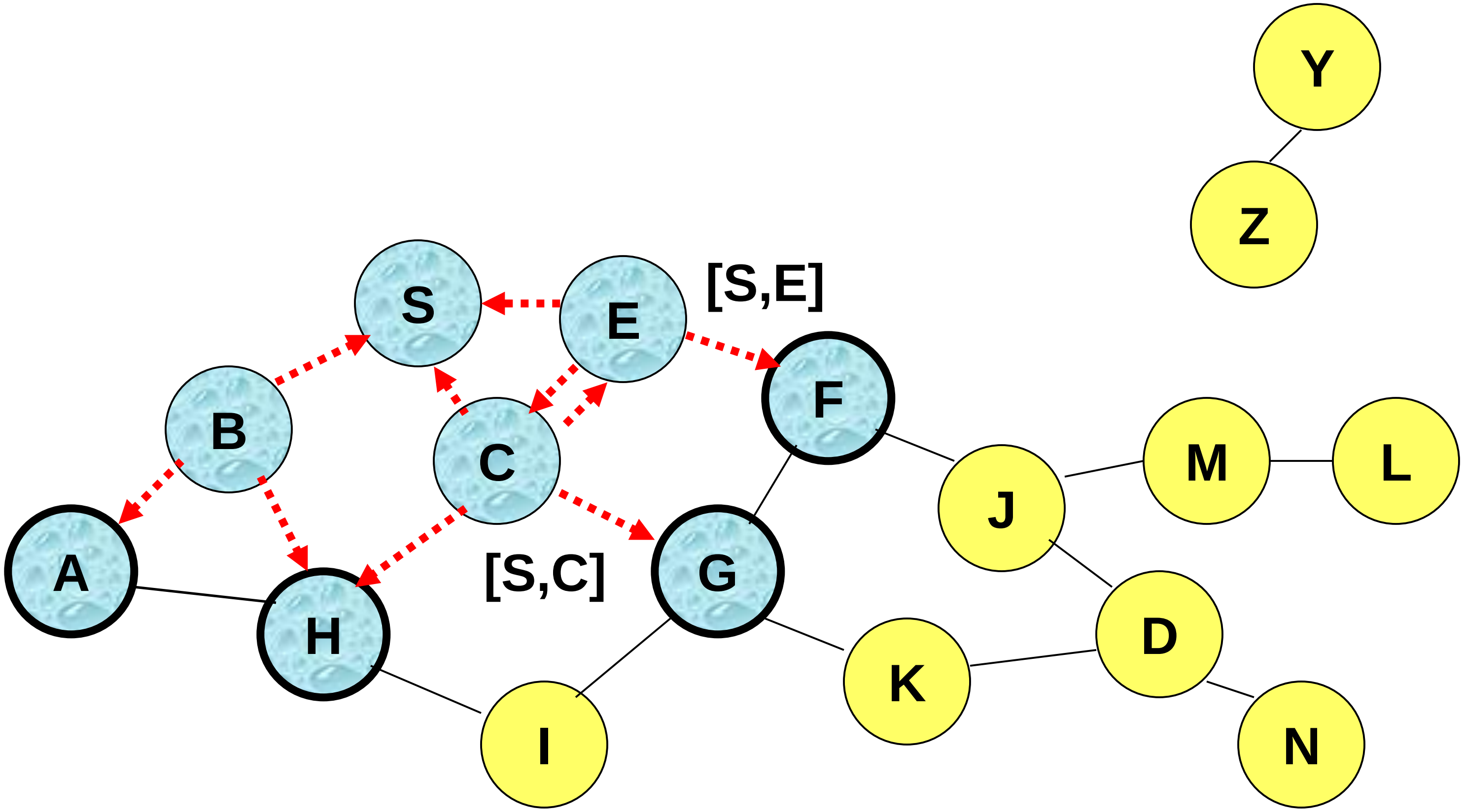
Route discovery in DSR



Represents transmission of RREQ

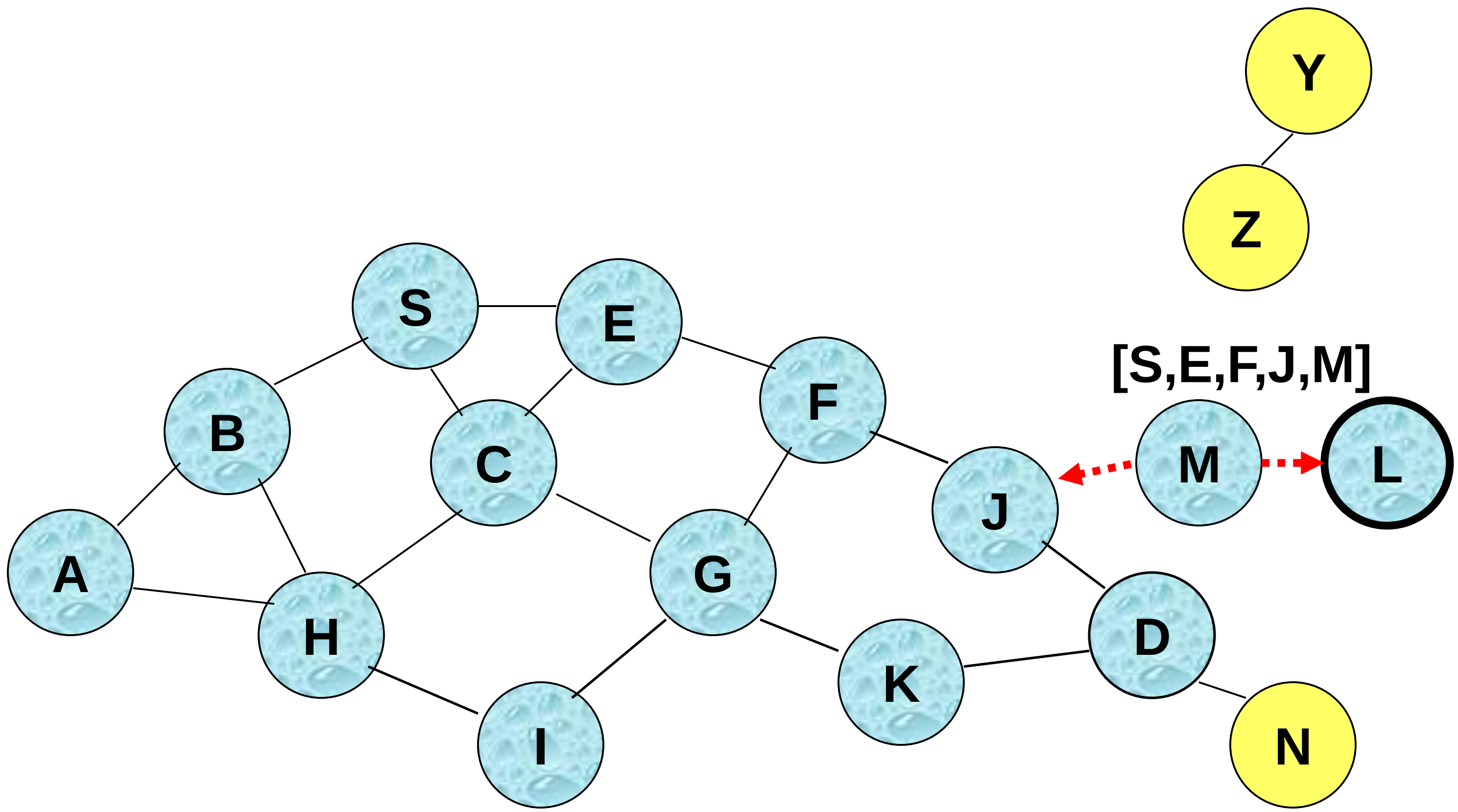
[X,Y] **Represents list of identifiers appended to RREQ**

Route discovery in DSR



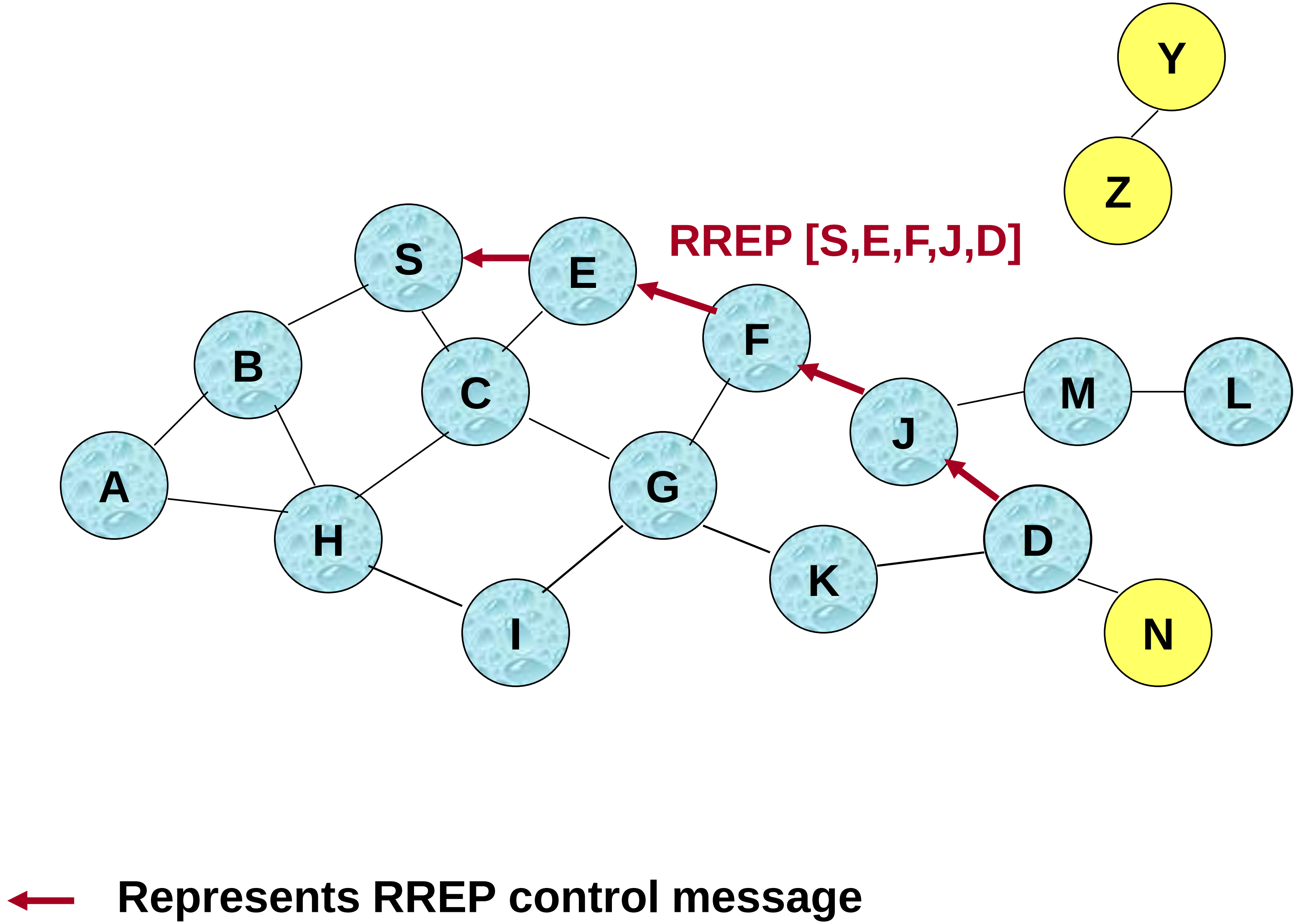
- **Node H receives packet RREQ from two neighbors: potential for collision**

Route discovery in DSR



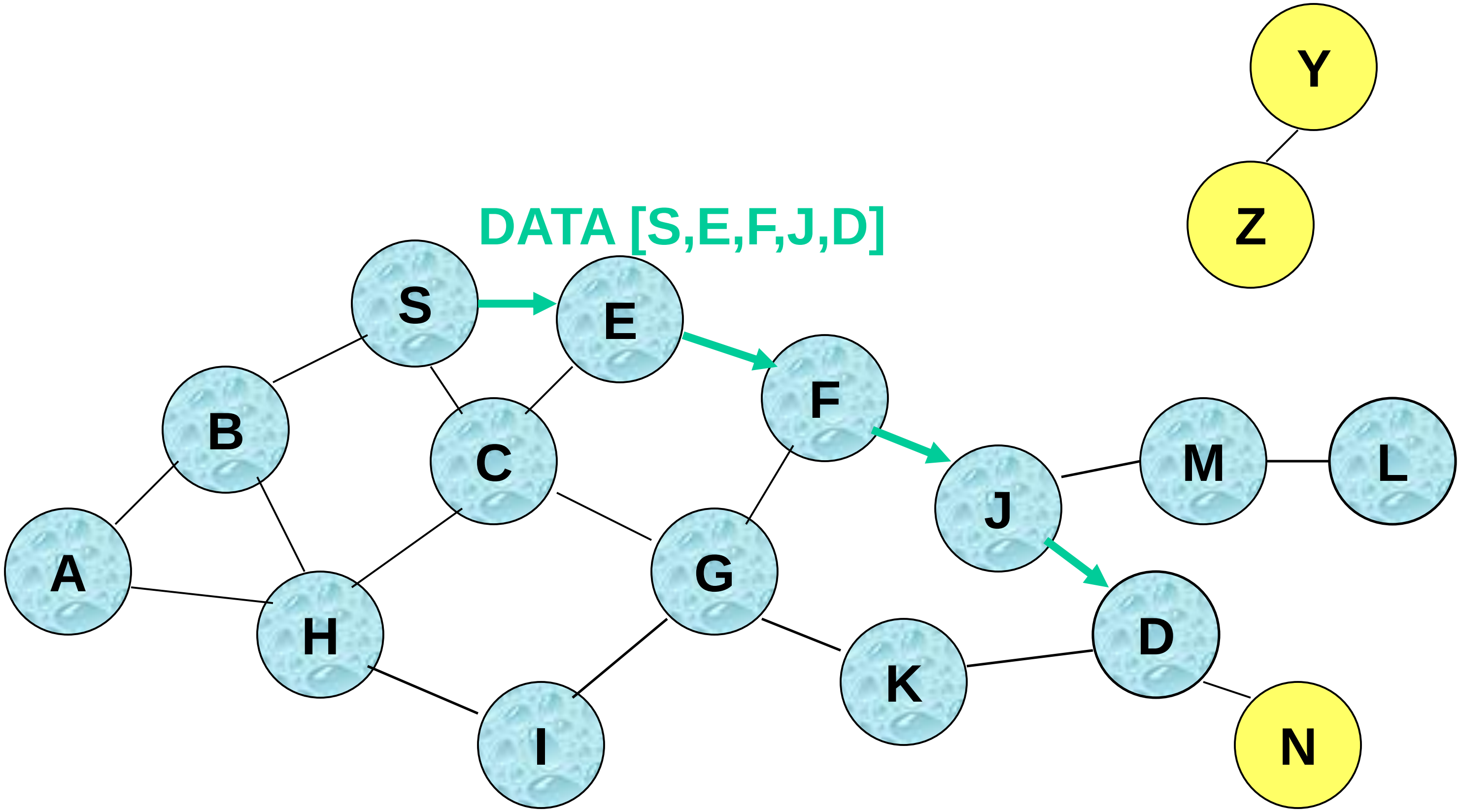
- **Node D does not forward RREQ, because node D is the intended target of the route discovery**

Route reply in DSR



Represents RREP control message

Data delivery in DSR



Packet header size grows with route length

Destination-Sequenced Distance-Vector (DSDV)

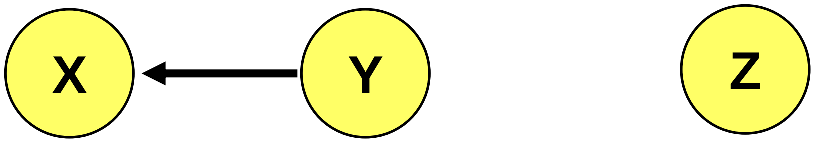
- Each node maintains a routing table which stores
  - next hop, cost metric towards each destination
  - a sequence number that is created by the destination itself
- Each node periodically forwards routing table to neighbors
  - Each node increments and appends its sequence number when sending its local routing table
- Each route is tagged with a sequence number; routes with greater sequence numbers are preferred

DSDV

- Each node advertises a monotonically increasing even sequence number for itself
- When a node decides that a route is broken, it increments the sequence number of the route and advertises it with infinite metric
- Destination advertises new sequence number

DSDV example

- When X receives information from Y about a route to Z
  – Let destination sequence number for Z at X be S(X), S(Y) is sent from Y



  – If S(X) > S(Y), then X ignores the routing information received from Y
  – If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z
  – If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y)

Protocol Trade-offs

- Proactive protocols
  - Always maintain routes
  - Little or no delay for route determination
  - Consume bandwidth to keep routes up-to-date
  - Maintain routes which may never be used
- Reactive protocols
  - Lower overhead since routes are determined on demand
  - Significant delay in route determination
  - Employ flooding (global search)
  - Control traffic may be bursty
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

TCP over wireless

Impact of transmission errors

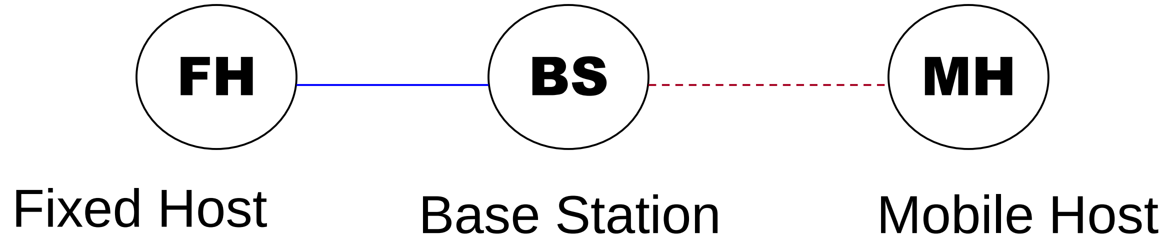
- Wireless channel may have bursty random errors

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

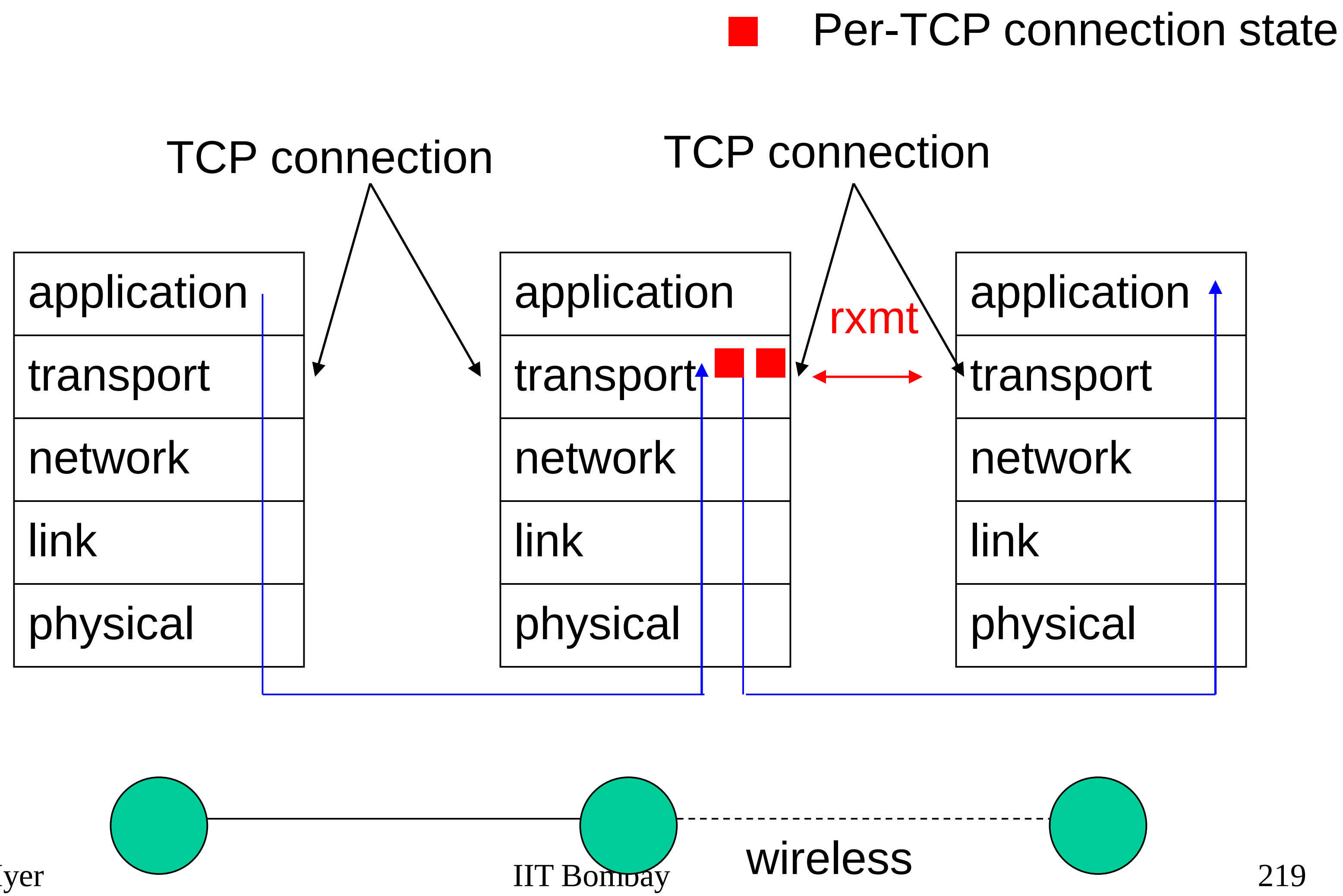
- Unnecessarily reduces congestion window
- Throughput suffers

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



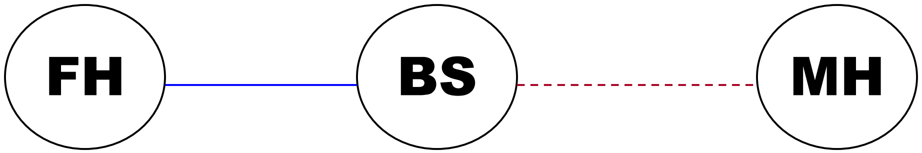
I-TCP: Split connection approach



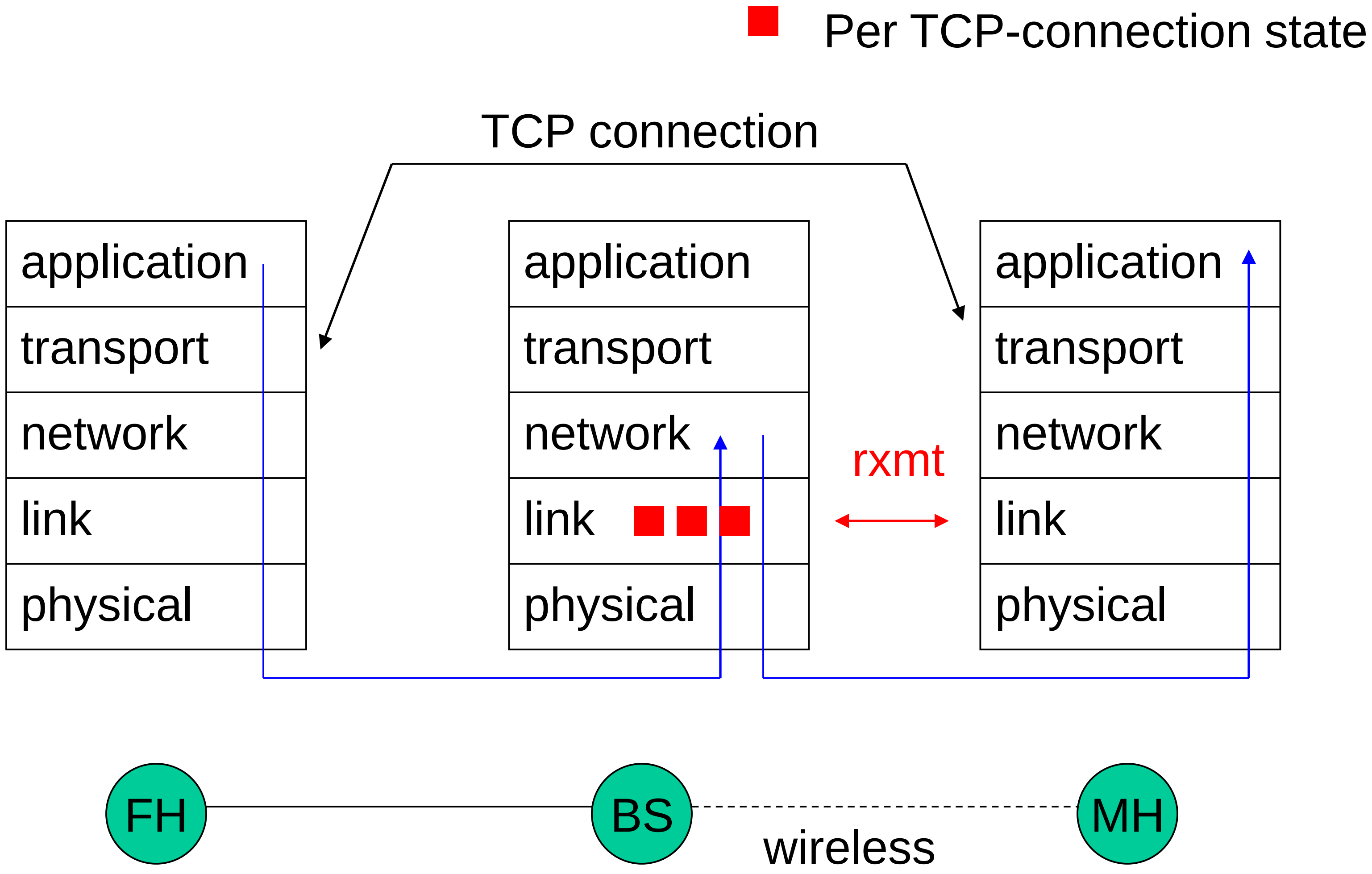
Snoop protocol

- 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

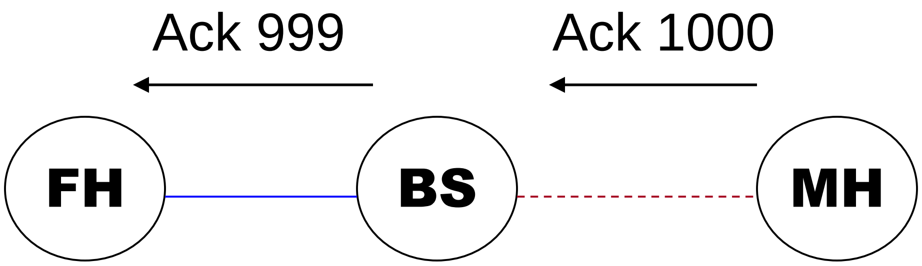


Impact of handoffs

- 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

TCP in MANET

Several factors affect TCP performance in MANET:

- Wireless transmission errors
  - may cause fast retransmit, which results in
    - retransmission of lost packet
    - reduction in congestion window
  - 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

Impact of Multi-hop Wireless Paths

TCP throughput degrades with increase in number of hops

- Packet transmission can occur on at most one hop among three consecutive hops
  - Increasing the number of hops from 1 to 2, 3 results in increased delay, and decreased throughput

- Increasing number of hops beyond 3 allows simultaneous transmissions on more than one link, however, degradation continues due to contention between TCP Data and Acks traveling in opposite directions

- When number of hops is large enough (>6), throughput stabilizes

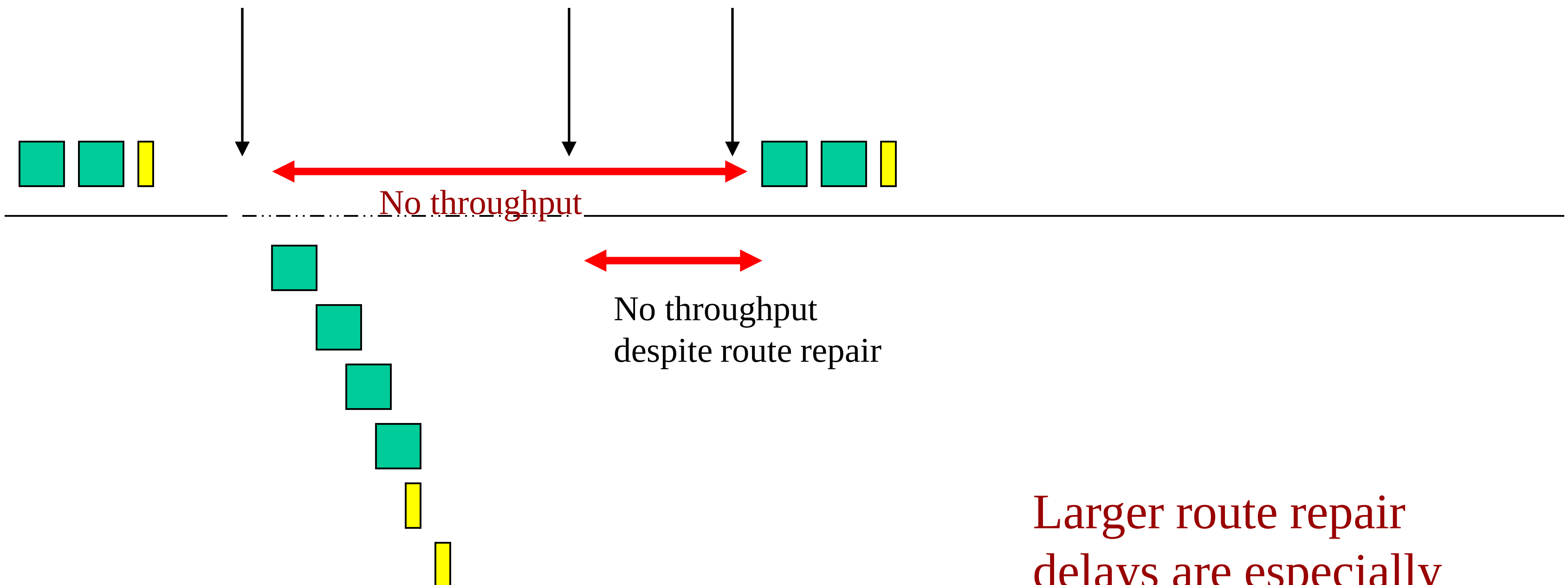
Impact of Node Mobility

TCP throughput degrades with increase in mobility but not always

mobility causes link breakage, resulting in route failure

Route is repaired

TCP sender times out. Starts sending packets again



TCP data and acks en route discarded

Larger route repair delays are especially harmful

WiFi: Management and Security

Network management

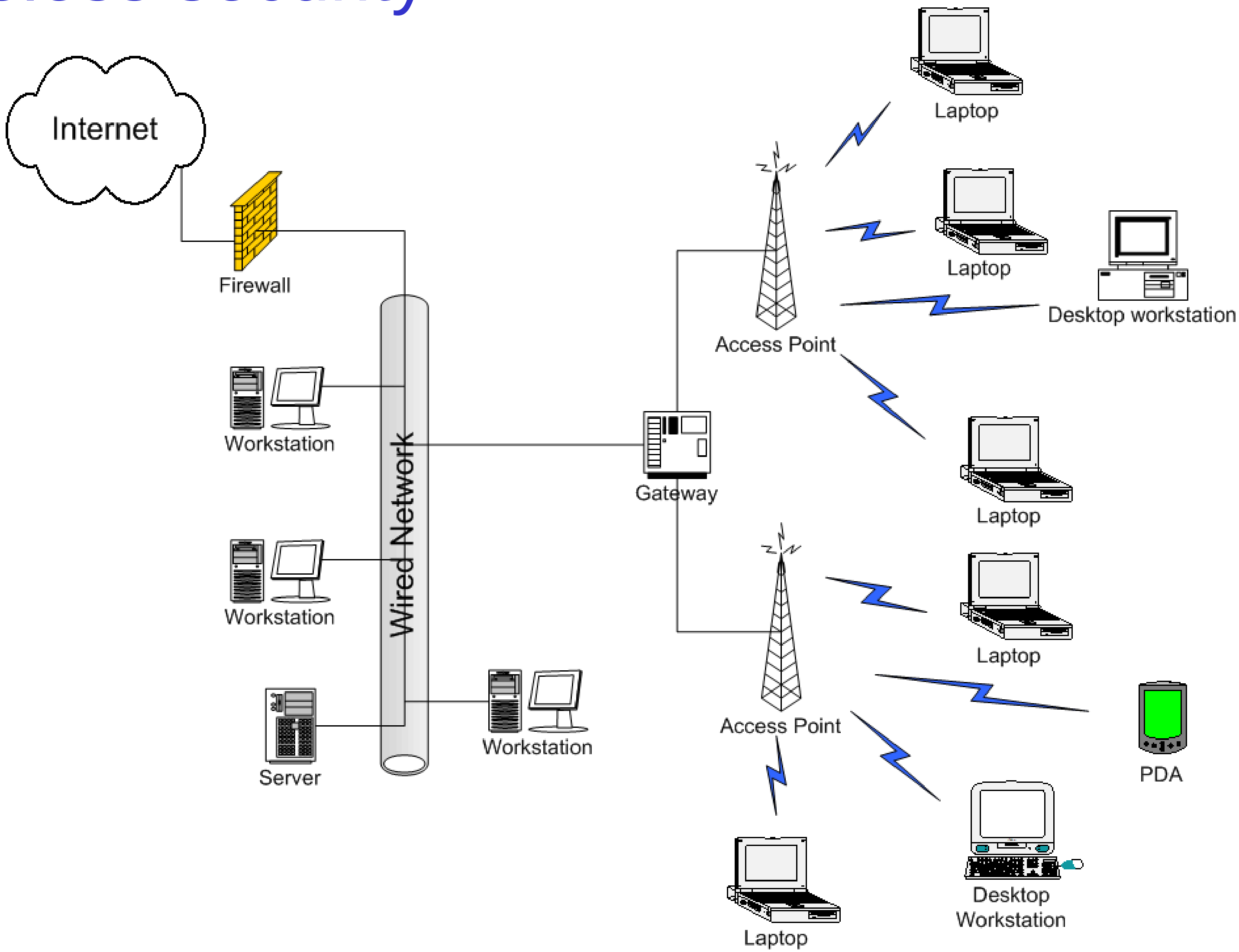
- Five key areas (FCAPS):
  - Fault management
  - Capacity management
  - Accounting(access) management
  - Performance management
  - Security management
- FCAPS at all layers of a stack (network, middleware, apps)

- Security is the main area of concern

Wireless Network Management

- In addition to the wired network issues, wireless network management needs to address some specific issues:
  - Roaming.
  - Persistence of Mobile Units.
  - Lack of SNMP Agents in Mobile Units.
  - Mobile Adhoc Networks.

Wireless security



Threats

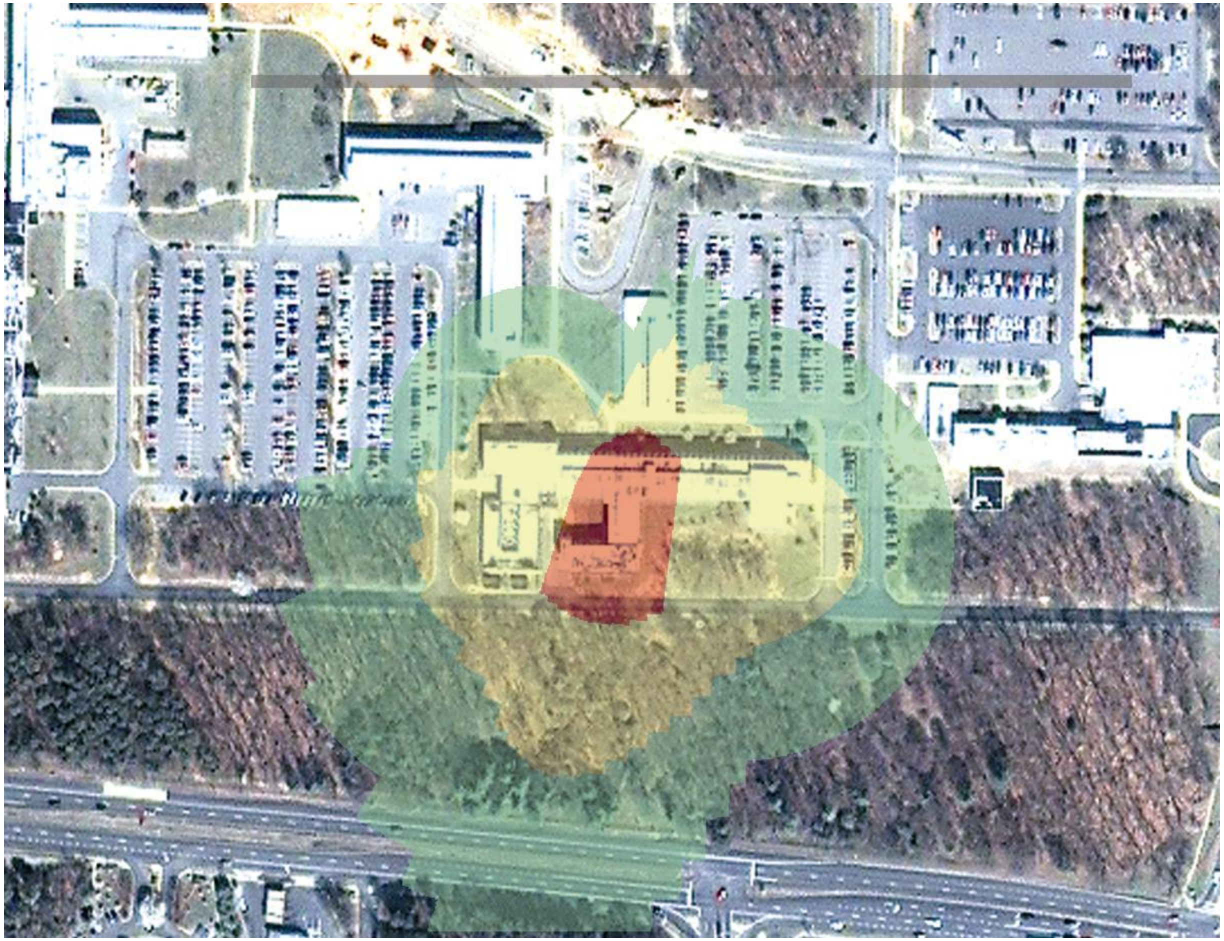
- Disclosure of sensitive/confidential data
- Denial of service (DoS)
- Unauthorized access to wireless-enabled resources
- Potential weakening of existing security measures on connected wired networks and systems

Vulnerabilities

- Wired Equivalent Privacy (WEP) encryption standard is weak
- Radio signals susceptible to jamming and interference
- Protocol vulnerabilities allow
  - Network sessions to be taken over by an intruder
  - Injection of invalid data into network traffic
  - Network reconnaissance
- Default configurations create “open” network

Vulnerabilities - 1

Example: The radio signal from a wireless network can spill over from the building where access points are located to neighboring buildings, parking lots and public roads.

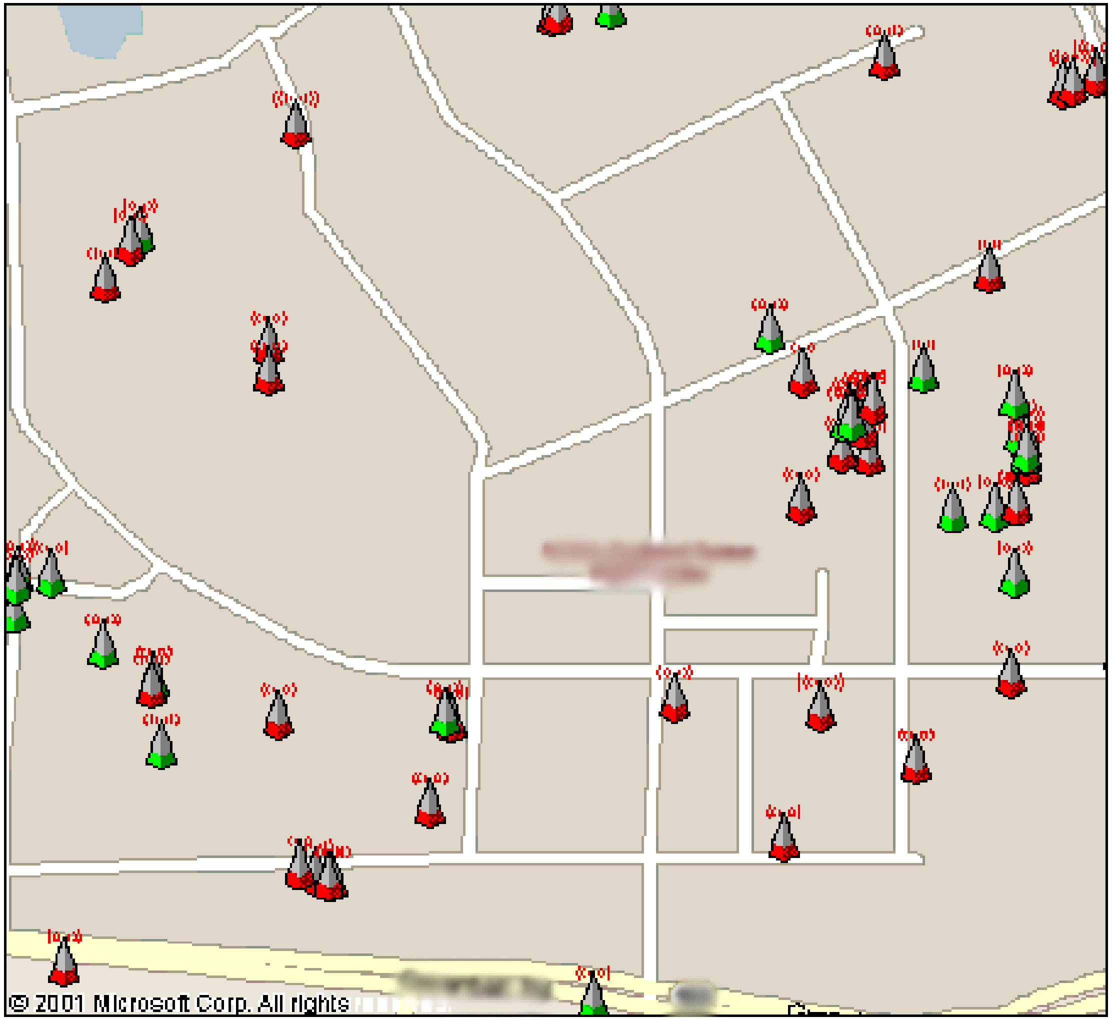


Vulnerabilities - 2

Example: Many wireless networks do not use WEP or other encryption to protect network traffic.

▲ = Access points using encryption

▲ = Access points without encryption



Vulnerabilities - 3

Example: These packet traces show highly confidential data that can be captured from a wireless network

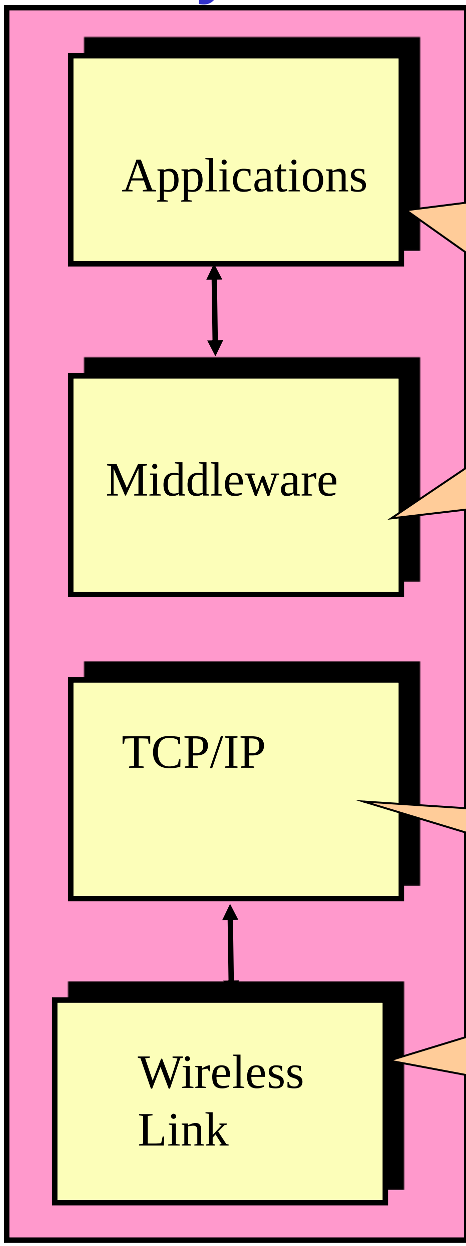
```
12:46:31.535667 192.168.33.20.33755 > 66.93.98.69.21: P [tcp sum ok] 10:30(20)
ack 267 win 6432 <nop,nop,timestamp 59110051 430777478> (DF) [tos 0x10]  (ttl
64, id 16715, len 72)
0x0000       4510 0048 414b 4000 4006 72f6 c0a8 2114  E..HAK@.@.r...!.
0x0010       425d 6245 83db 0015 ebc5 a32c 0a27 b4f2  B]bE.......,.'..
0x0020       8018 1920 8c10 0000 0101 080a 0385 f2a3  ................
0x0030       19ad 2486 5553 4552 2061 646d 696e 6973  ..$.USER.adminis
0x0040       7472 6174 6f72 0d0a                      trator..
```

```
12:46:34.885986 192.168.33.20.33755 > 66.93.98.69.21: P [tcp sum ok] 30:48(18)
ack 313 win 6432 <nop,nop,timestamp 59113401 430777584> (DF) [tos 0x10]  (ttl
64, id 16717, len 70)
0x0000       4510 0046 414d 4000 4006 72f6 c0a8 2114  E..FAM@.@.r...!.
0x0010       425d 6245 83db 0015 ebc5 a340 0a27 b520  B]bE.......@.'..
0x0020       8018 1920 ebd7 0000 0101 080a 0385 ffb9  ................
0x0030       19ad 24f0 5041 5353 2064 6f75 626c 6568  ..$.PASS.doubleh
0x0040       656c 6978 0d0a                           elix..
```

Wireless security technologies

Can use higher level services to compensate for lower layers

Tradeoffs in performance and security



- SET for transaction security
- S/MIME and PGP for secure email
- Java security (sandboxes)
- Database security

- SSL and TLS
- Web security (HTTPS, PICS, HTTP Headers)
- Proxy server security

- IPSEC and wirless VPN
- Mobile IP

- 802.11 security (WEP)
- WLL link security

Security and availability

- The security S is provided at the following levels:
  - Level 0: no security specified
  - Level 1: Authorization and authentication of principals
  - Level 2: Auditing and encryption (Privacy)
  - Level 3: Non-repudiation and delegation

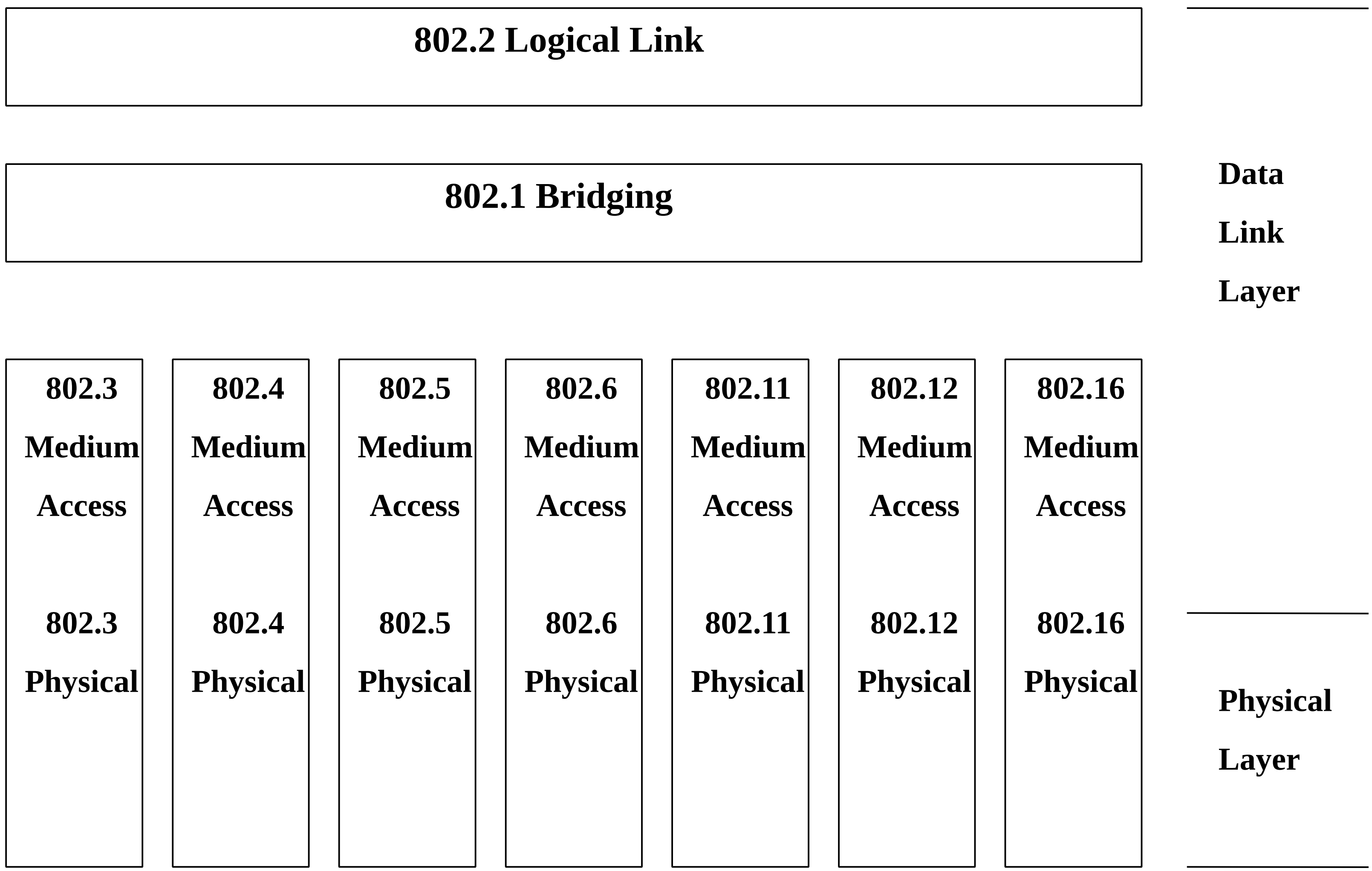
- Availability A can be represented in terms of replications (more replications increase system availability):
  - Level 0: No replication (i.e., only one copy of the resource is used)
  - Level 1: Replication is used to increase availability. The resource is replicated for a fail-safe operation
  - Level 2: FRS (Fragmentation, Redundancy, Scattering) is used. FRS schemes split a resource, replicate it, and scatter it around the network to achieve high availability and intrusion tolerance

Being secure

- Develop wireless network policies
- Conduct risk assessments to determine required level of security
- Limit access to wireless networks through the use of wireless security measures (i.e. 802.11i or WPA)
- Maintain logical separation between wireless and wired networks
- Perform wireless scans to identify wireless networks and applications (on a regular basis)
- Enforce wireless network policies

802.16 internals

IEEE 802 family



IEEE 802.16

- Purpose:
  - to enable rapid worldwide deployment of cost-effective broadband wireless access products
- 802.16:
  - consists of the BS (Base Station) and SSs(Subscriber Stations)
  - All data traffic goes through the BS, and the BS can control the allocation of bandwidth on the radio channel.
  - 802.16 is a Bandwidth on Demand system.
- Standard specifies:
  - The air interface, MAC (Medium Access Control), PHY(Physical layer)

IEEE 802.16

- The spectrum to be used
  - 10 - 66 GHz licensed band
    - Due to the short wavelength
      - Line of sight is required
      - Multipath is negligible
    - Channels 25 or 28 MHz wide are typical
    - Raw data rates in excess of 120 Mbps
  - 2 -11 GHz
    - IEEE Standards Association Project P802.16a
    - Approved as an IEEE standard on Jan 29, 2003

IEEE 802.16 MAC layer function

- Transmission scheduling :
  - Controls up and downlink transmissions so that different QoS can be provided to each user
- Admission control :
  - Ensures that resources to support QoS requirements of a new flow are available
- Link initialization:
  - Scans for a channel, synchronizes the SS with the BS, performs registration, and various security issues.
- Support for integrated voice/data connections:
  - Provide various levels of bandwidth allocation, error rates, delay and jitter

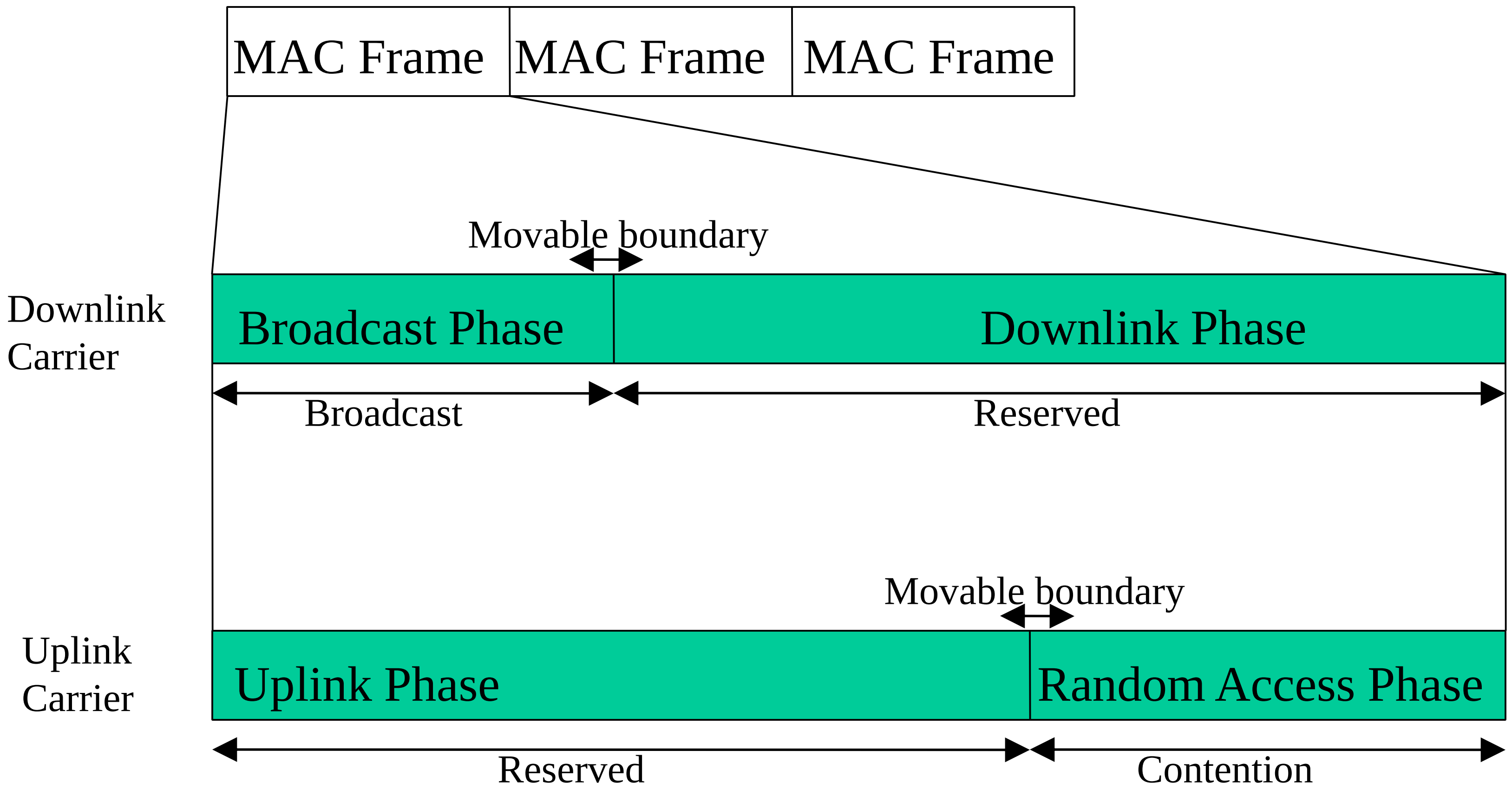
Basic services

- UGS(Unsolicited Grant Service)
  - Supports real-time service flows that generate fixed size data packets on a periodic basis, such as T1/E1 and Voice over IP
  - The BS shall provide fixed size slot at periodic intervals.
- rtPS(Real-Time Polling Service)
  - Supports real-time service flows that generate variable size data packets on a periodic basis, such as MPEG video
- nrtPS(Non-Real-Time Polling Service)
  - Supports non real-time service flows that generate variable size data packets on a regular basis, such as high bandwidth FTP.
- BE(Best Effort service)
  - Provides efficient service to best effort traffic

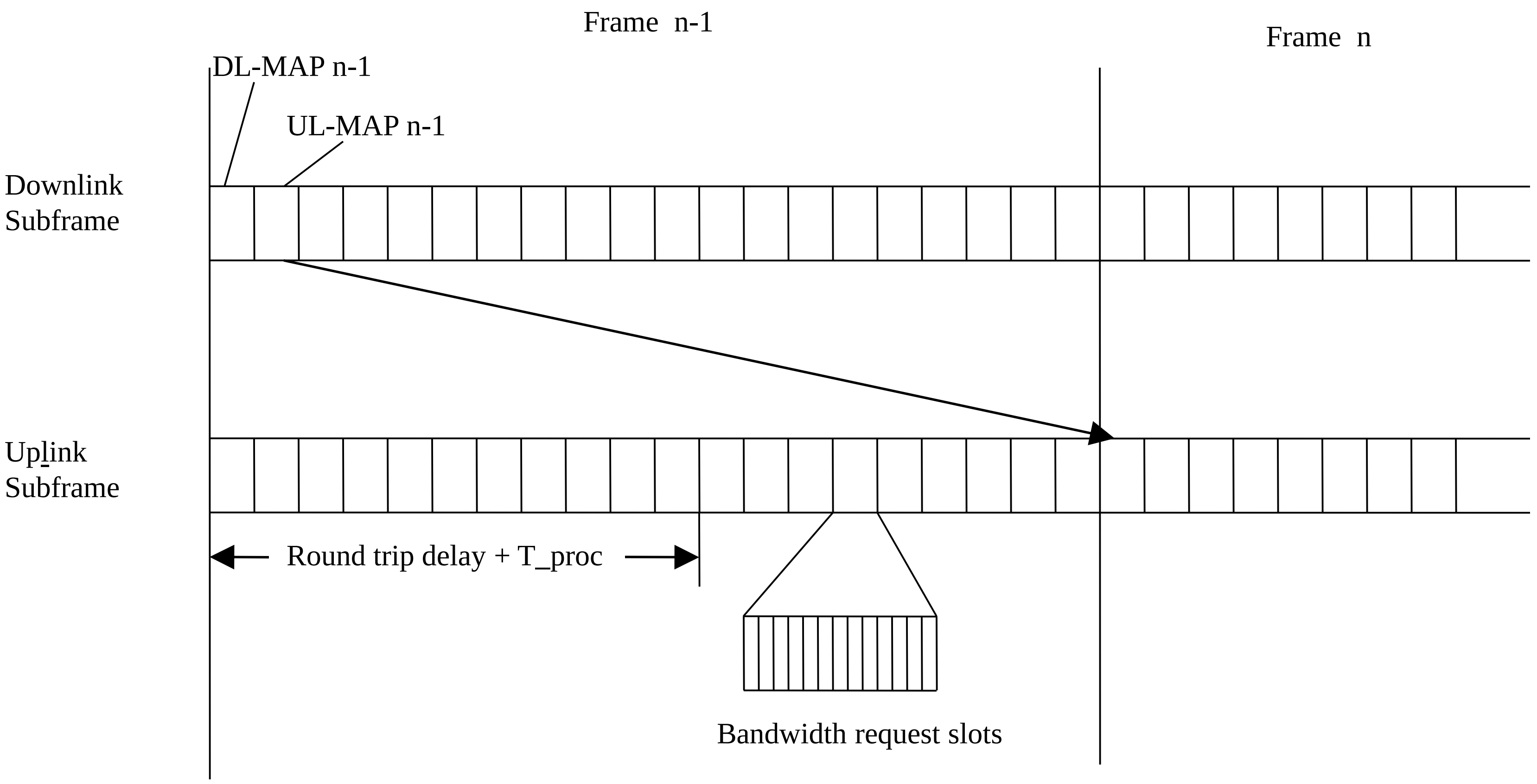
FDD based MAC protocol

- Downlink
  - Broadcast phase : The information about uplink and downlink structure is announced.
  - DL-MAP(Downlink Map)
    - DL-MAP defines the access to the downlink information
  - UL-MAP(Uplink Map)
    - UL-MAP message allocates access to the uplink channel
- Uplink
  - Random access area is primarily used for the initial access but also for the signalling when the terminal has no resources allocated within the uplink phase.

FDD based 802.16 MAC Protocol



Time relevance of PHY and MAC control information

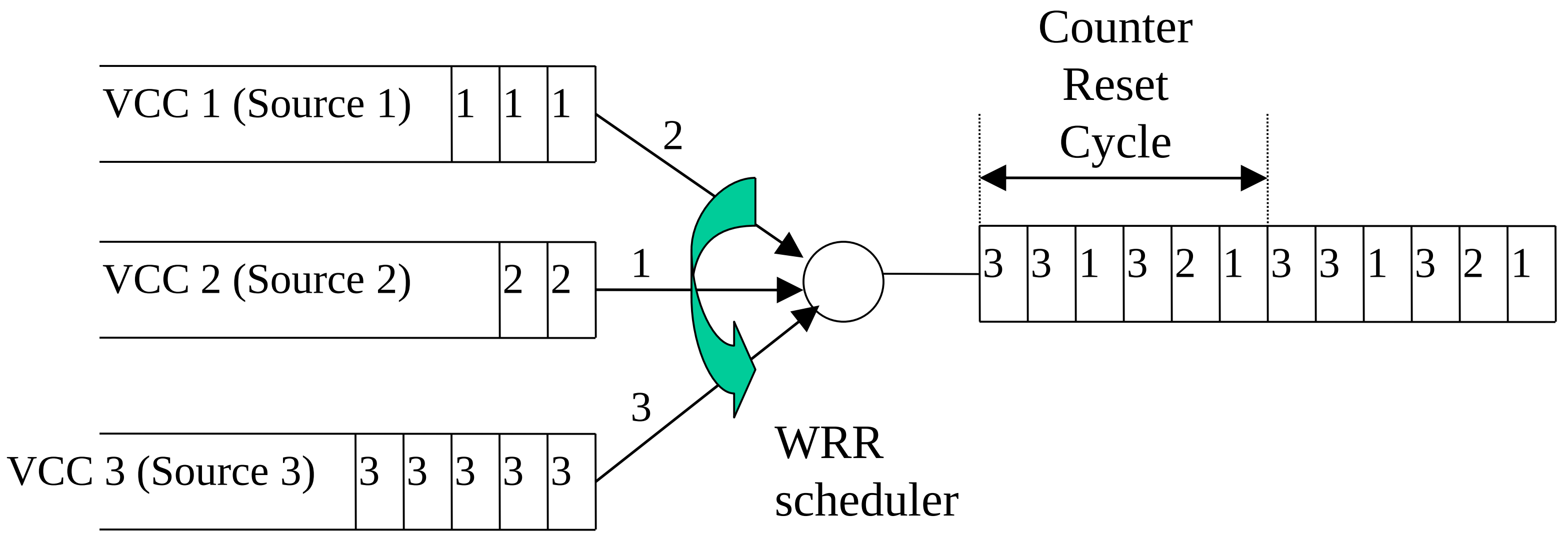


Downlink Scheduling

- Radio resources have to be scheduled according to the QoS(Quality of Service) parameters
- Downlink scheduling:
  - the flows are simply multiplexed
  - the standard scheduling algorithms can be used
    - WRR(Weighted Round Robin)
    - VT(Virtual Time)
    - WFQ(Weighted Fair Queueing)
    - WFFQ(Worst-case Fair weighted Fair Queueing)
    - DRR(Deficit Round Robin)
    - DDRR(Distributed Deficit Round Robin)

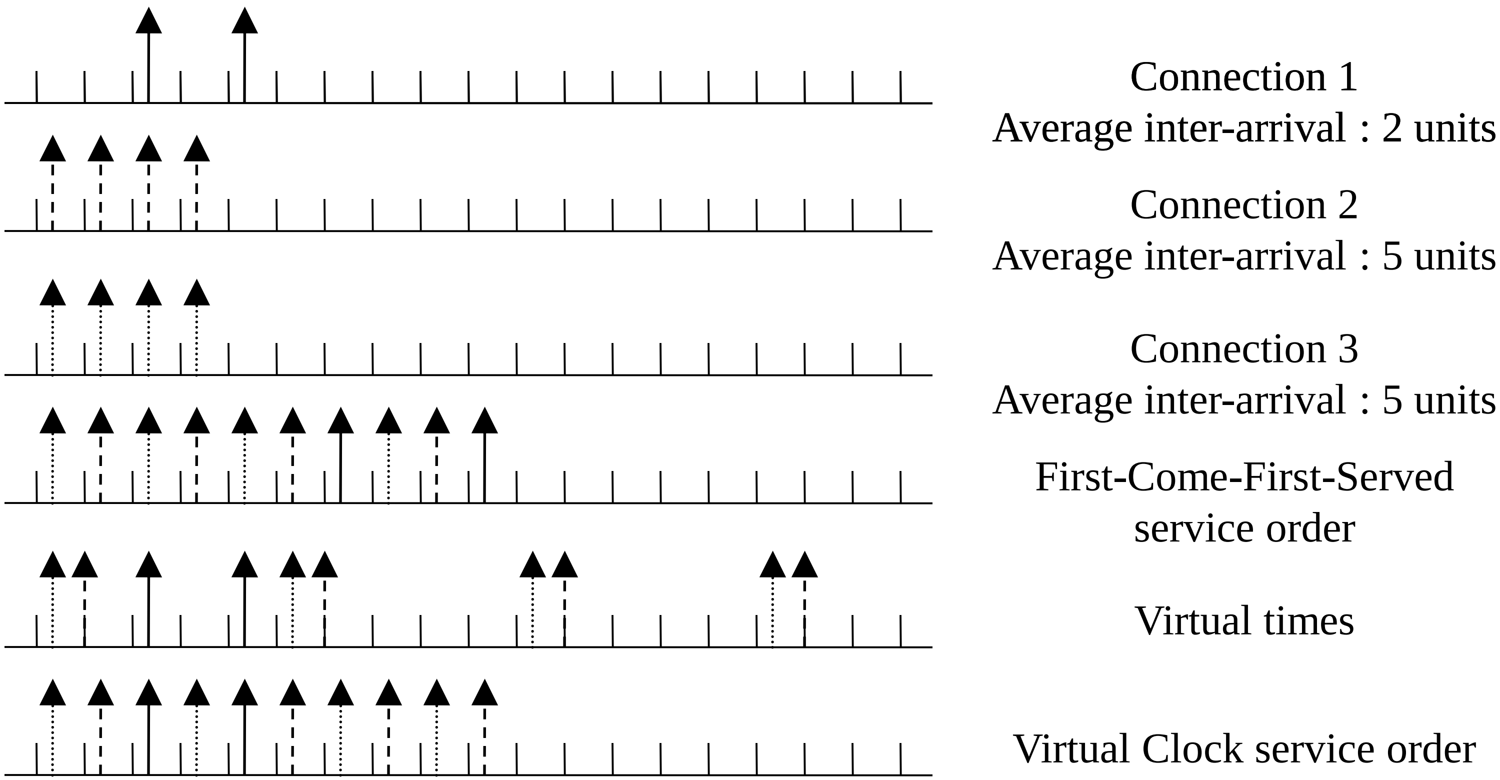
WRR

- It is an extention of round robin scheduling based on the static weight.



VT

- VT : aims to emulate the TDM(Time Division Multiplexing) system
  - connection 1 : reserves 50% of the link bandwidth
  - connection 2, 3 : reserves 20% of the link bandwidth



Uplink Scheduling

Uplink scheduling:

- Responsible for the efficient and fair allocation of the resources(time slots) in the uplink direction
- Uplink carrier :
  - Reserved slots
  - contention slots(random access slots)
- The standard scheduling algorithms can be used

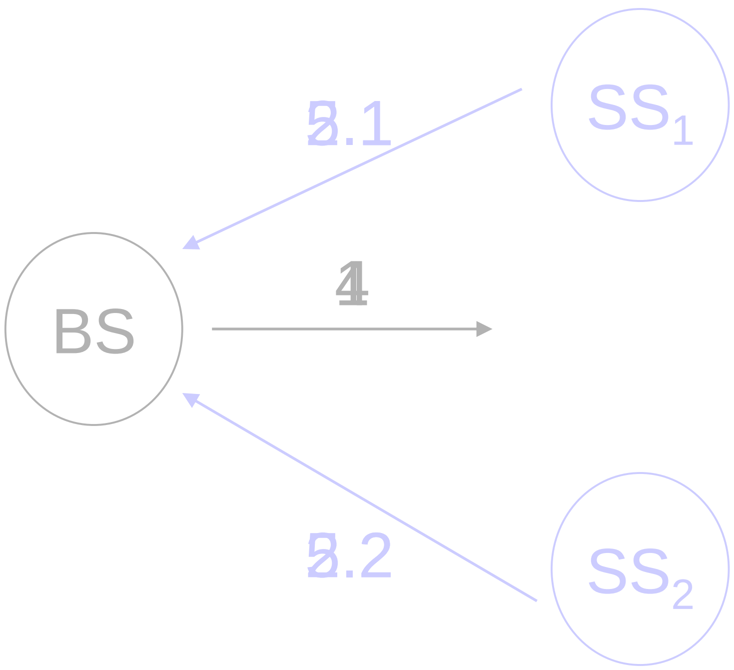
Bandwidth allocation and request mechanisms

- The method by which the SS(Subscriber Station) can get the bandwidth request message to the BS(Base Station)
  - Unicast
    - When an SS is polled individually, no explicit message is transmitted to poll the SS.
    - The SS is allocated, in the UP-MAP(Uplink Map), bandwidth sufficient for a bandwidth request.
  - Multicast
    - Certain CID(Connection Identifier) are reserved for multicast groups and for broadcast messages.
    - An SS belonging to the polled group may request bandwidth during any request interval allocated to that CID in the UP-MAP
  - Broadcast

Bandwidth allocation and request mechanisms

- UGS :
  - The BS provides fixed size bandwidth at periodic intervals to UGS.
  - The SS is prohibited from using any contention opportunities.
  - The BS shall not provide any unicast request opportunities.
- rtPS
  - The BS provides periodic unicast request opportunities.
  - The SS is prohibited from using any contention opportunities.
- nrtPS
  - The BS provides timely unicast request opportunities.
  - The SS is allowed to use contention request opportunities.
- BE
  - The SS is allowed to use contention request opportunities.

Bandwidth Request-Grant Protocol



1: BS allocates bandwidth to SSs for transmitting bandwidth request.

2.1 SS_1 transmits bandwidth requests.

2.2 SS_2 transmits bandwidth requests.

4: BS allocates bandwidth to SSs for transmitting data based on their bandwidth requests. Bandwidth is also allocated for requesting more bandwidth.

5.1 SS_1 transmits data and bandwidth requests.

5.2 SS_2 transmits data and bandwidth requests.

Example

Total Uplink Bytes = 100

2 SS and 1 BS

SS_1 Demands:

UGS = 20

rtPS = 12

nrtPS = 15

BE = 30

SS_2 Demands:

UGS = 10

rtPS = 10

nrtPS = 15

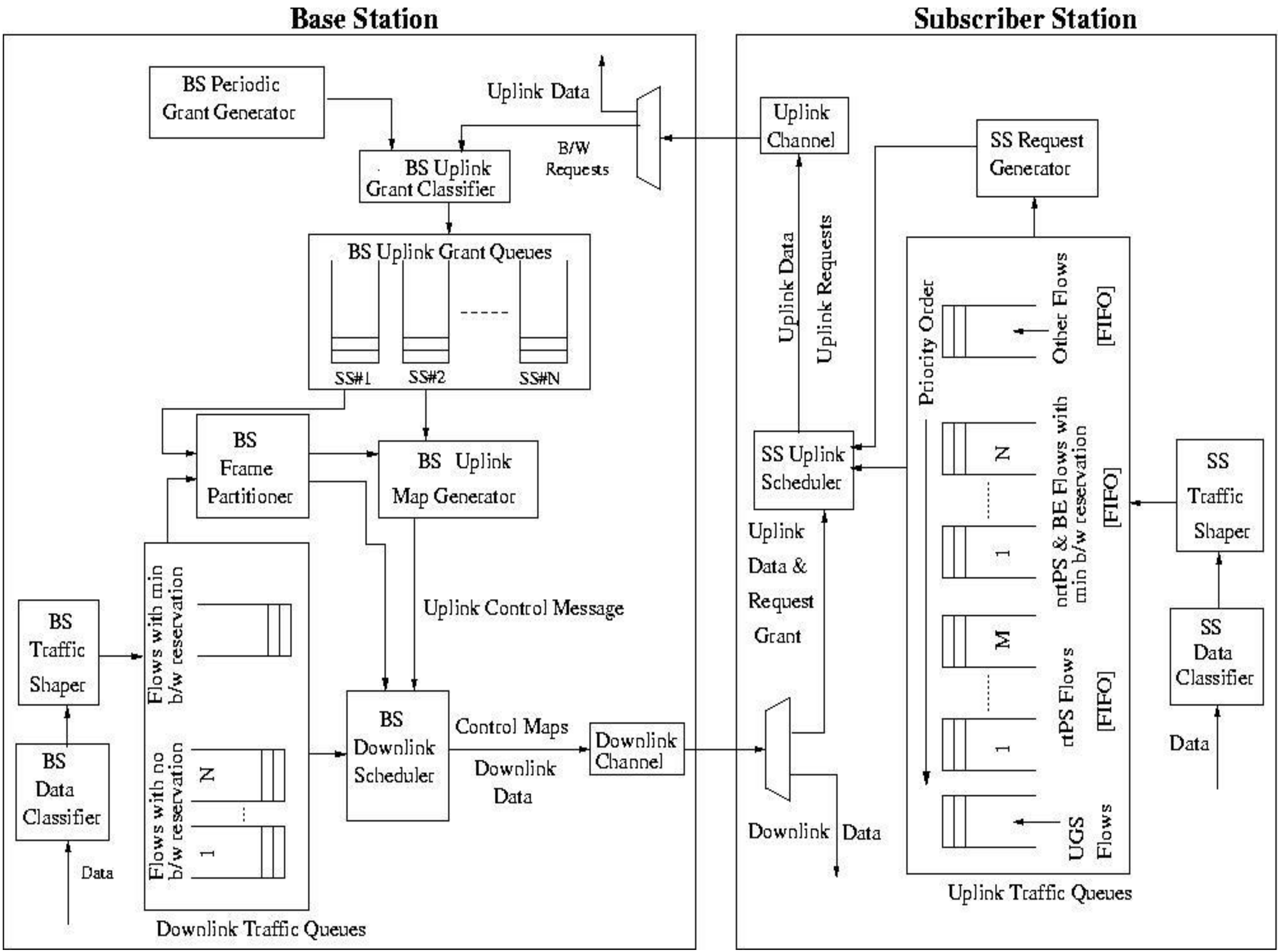
BE = 20

Flows:	UGS	rtPS	nrtPS	BE
1st Round	40	30	20	10
	30	22	20	10
Excess Bytes = 18				
2nd Round	30	22	20+12	10+6
	30	22	32	16
Excess Bytes = 2				
3rd Round	30	22	30	16+2
	30	22	30	18

Total Demand Per Flow:
UGS = 30
rtPS = 22
nrtPS = 30
BE = 50

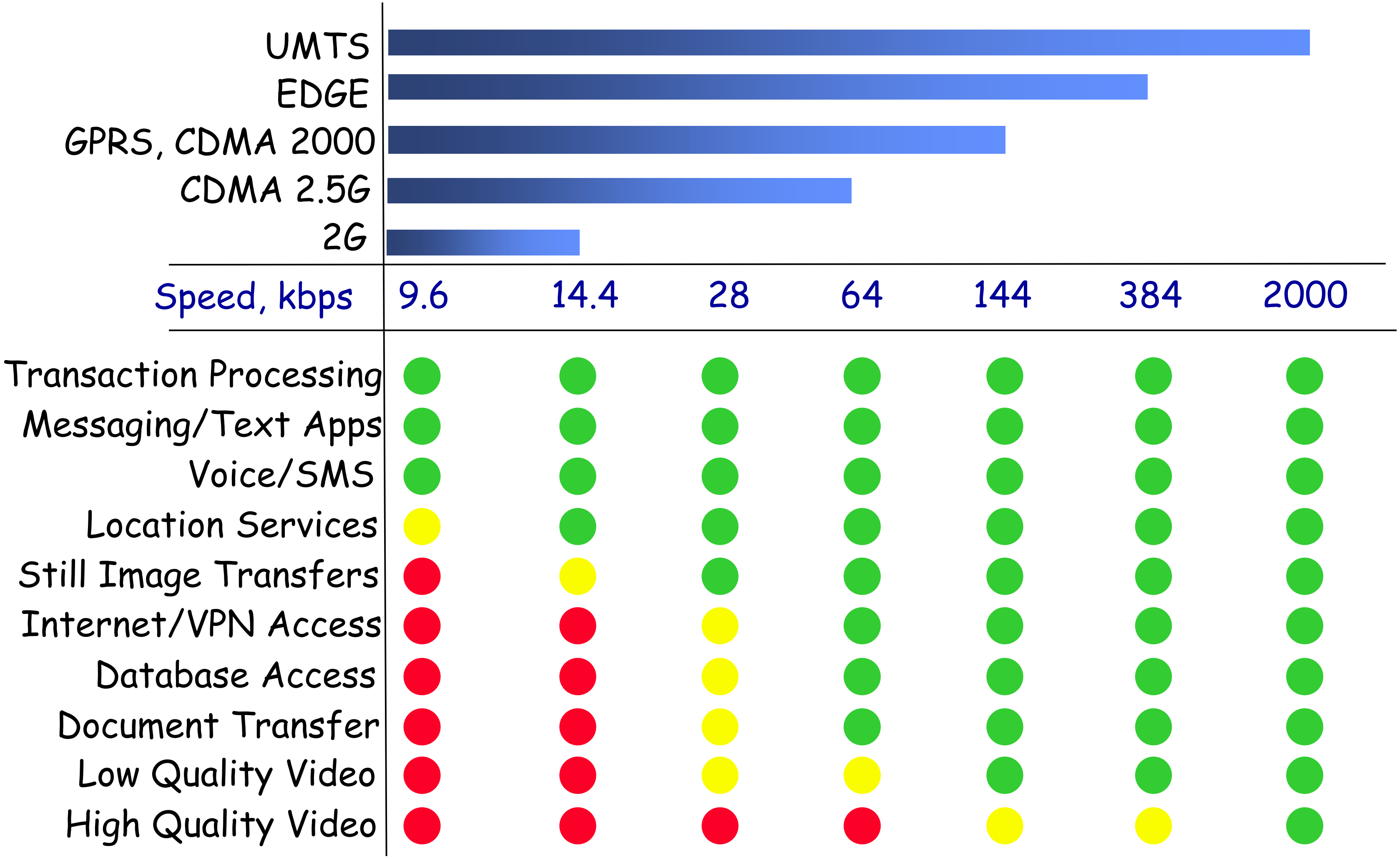
SS_1 Allocation = 20 +12 + 15 + 9 = 56

SS_2 Allocation = 10 +10 + 15 + 9 = 44

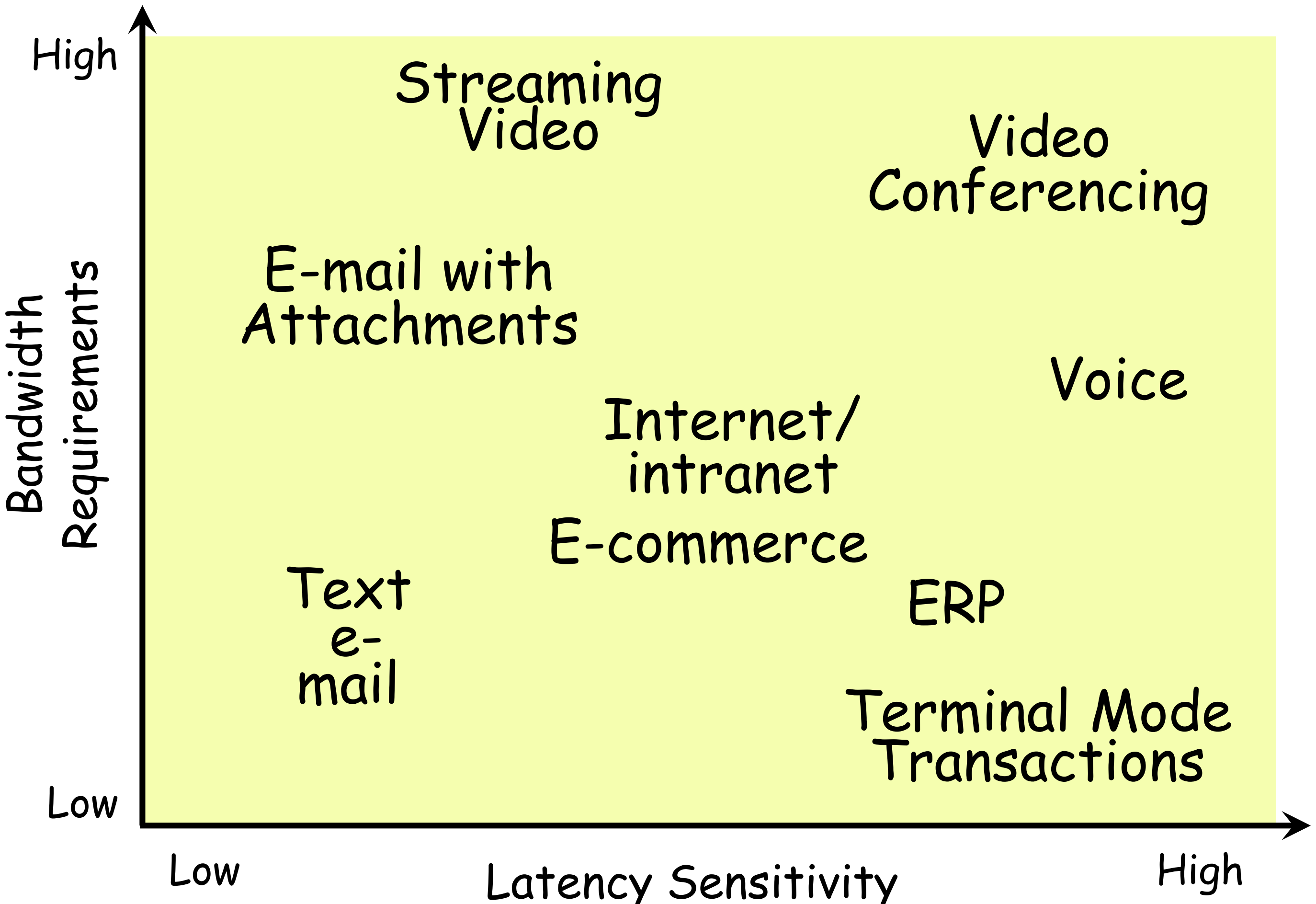

Base Station
Subscriber Station
BS Periodic Grant Generator
Uplink Data
B/W Requests
BS Uplink Grant Classifier
BS Uplink Grant Queues
SS#1
SS#2
SS#N
BS Frame Partitioner
BS Uplink Map Generator
Uplink Control Message
BS Traffic Shaper
BS Data Classifier
Data
Flows with min b/w reservation
Flows with no b/w reservation
N
1
Downlink Traffic Queues
BS Downlink Scheduler
Control Maps
Downlink Data
Downlink Channel
Uplink Channel
SS Request Generator
Uplink Data
Uplink Requests
SS Uplink Scheduler
Uplink Data & Request Grant
Downlink Data
Priority Order
Other Flows
[FIFO]
nrtPS & BE Flows with min b/w reservation
[FIFO]
N
1
M
1
rtPS Flows
[FIFO]
UGS Flows
Uplink Traffic Queues
SS Traffic Shaper
SS Data Classifier
Data

QoS and Voice/Video Applications

Bandwidth and applications



Applications: network requirements



Quality of Service

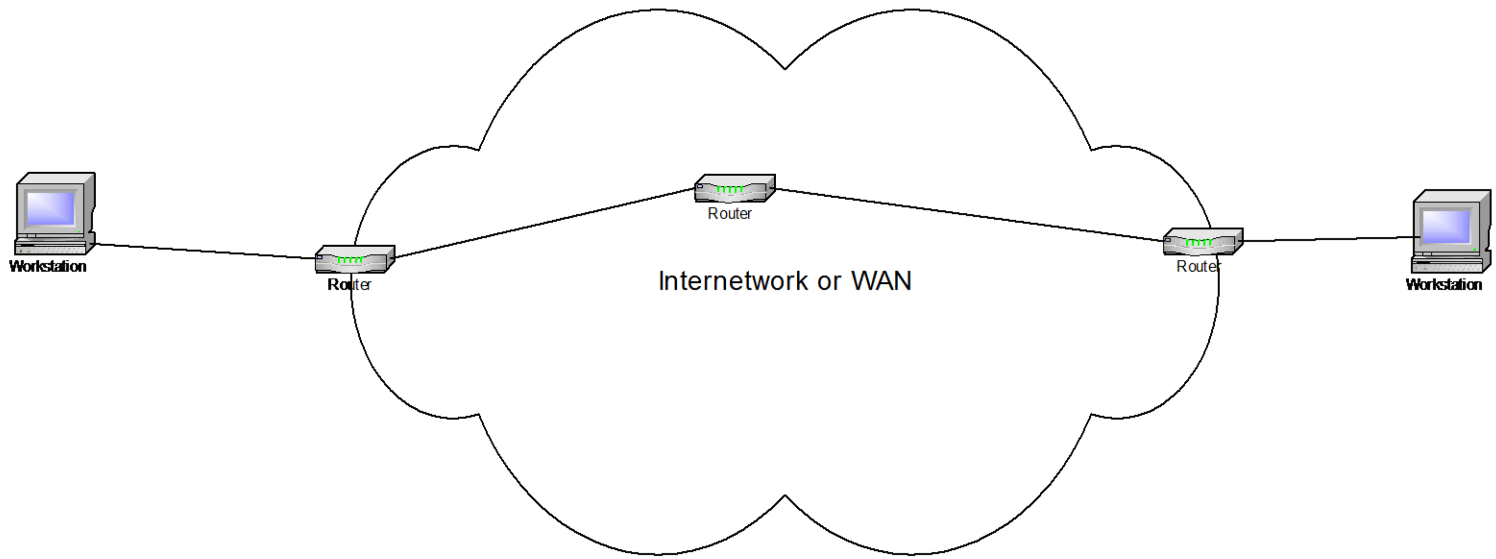
- Network-level QoS
  - Metrics include available b/w, packet loss rates, etc
  - Elements of a Network QoS Architecture
    - QoS specification (traffic classes)
    - Resource management and admission control
    - Service verification and traffic policing
    - Packet forwarding mechanisms (filters, shapers, schedulers)
    - QoS routing
- Application-level QoS
  - How well user expectations are qualitatively satisfied
  - Clear voice, jitter-free video, etc
  - Implemented at application-level:
    - end-to-end protocols (RTP/RTCP)
    - application-specific encodings (FEC)

QoS building blocks

- What kind of premium services?
  - ***Service/SLA design***
- How much resources?
  - ***admission control/provisioning***
- How to ensure network utilization, load balancing?
  - ***QoS routing, traffic engineering***
- How to set aside resources in a distributed manner?
  - ***signaling, provisioning, policy***
- How to deliver services when the traffic actually comes in?
  - ***traffic shaping, classification, scheduling***
- How to monitor quality, account and price these services?
  - ***network management, accounting, billing, pricing***

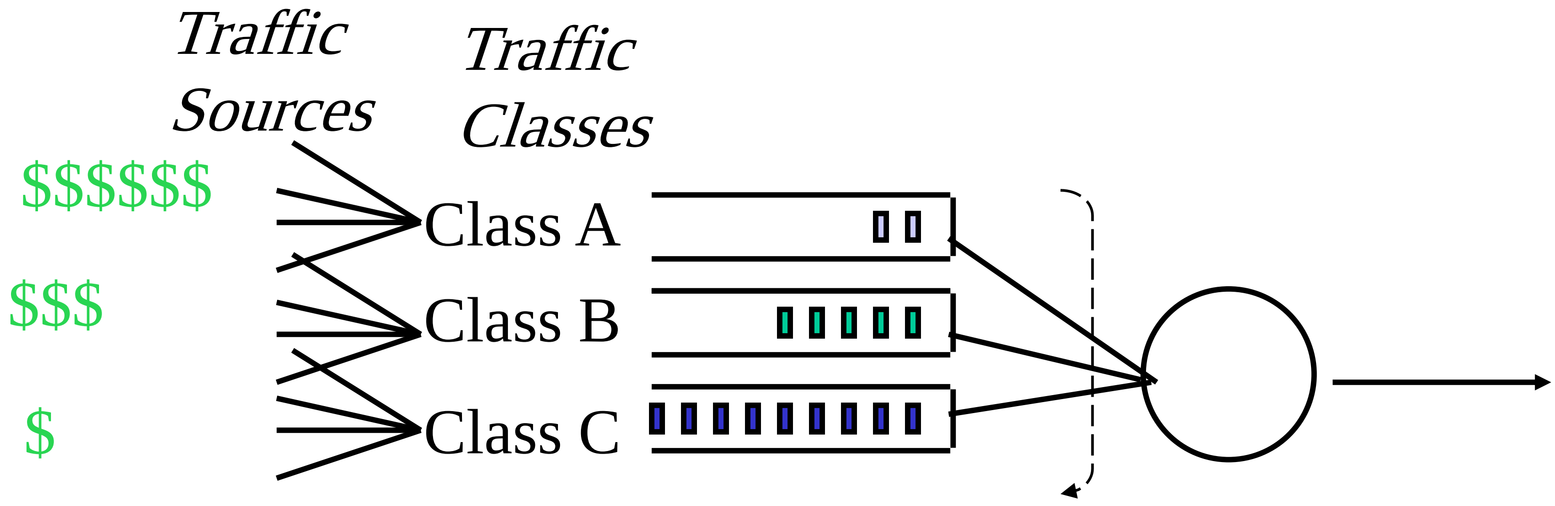
QoS big picture: Control/Data planes

Control Plane: Signaling + Admission Control or
SLA (Contracting) + Provisioning/Traffic Engineering



Data Plane: Traffic conditioning (shaping, policing, marking etc) at the edge +
Traffic Classification + Claiming Reserved Resources (Per-hop Behavior- PHB),
scheduling, buffer management

Services: Queuing/Scheduling



- Extra bits indicate the queue (class) for a packet
- High $$ users get into high priority queues, which are in turn less populated => lower delay and near-zero likelihood of packet drop

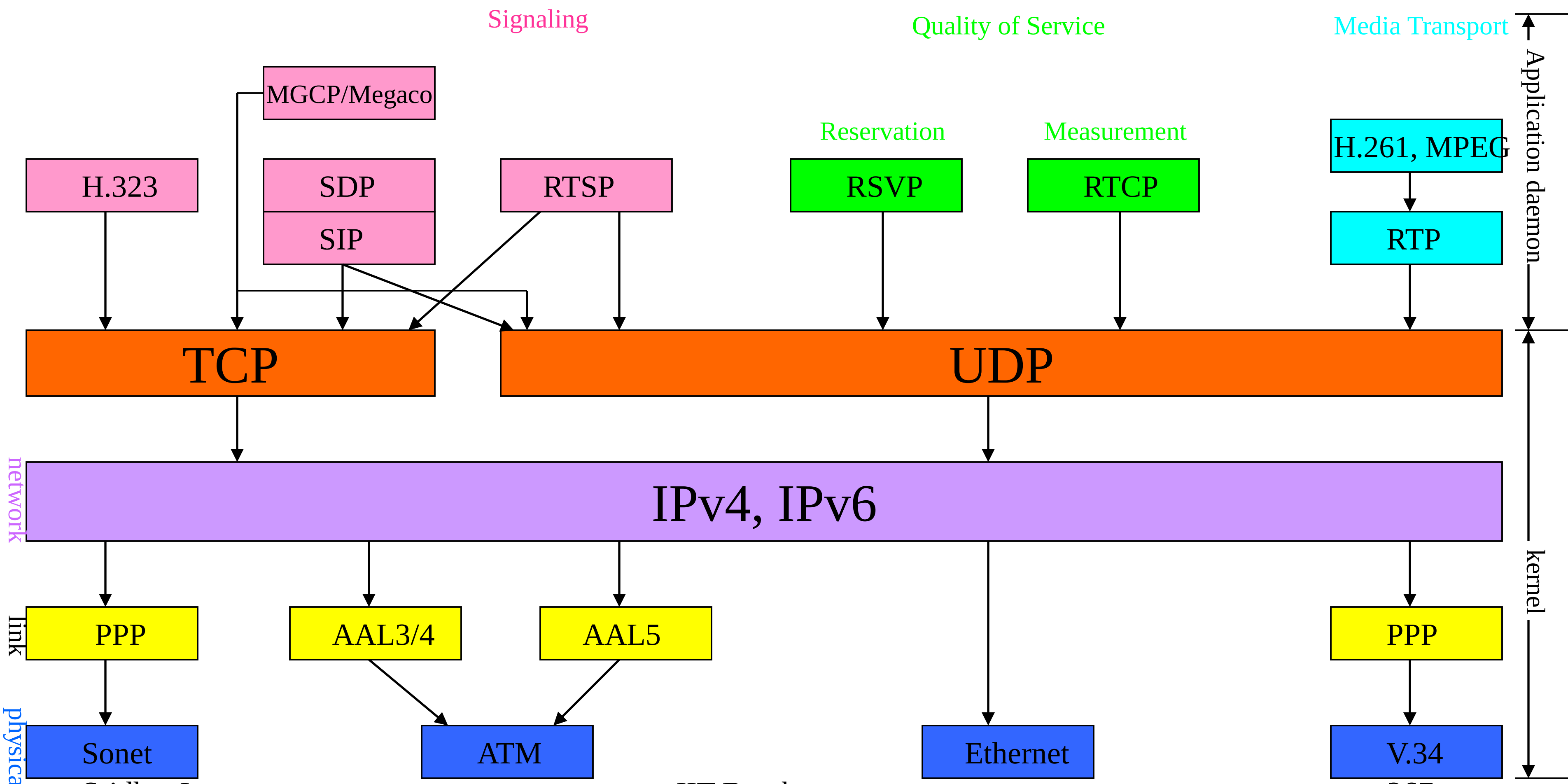
QoS and pricing

- QoS Pricing
  - Multi-class network requires differential pricing
  - Otherwise all users select best service class
- Service provider’s perspective
  - Low cost (implementn, metering, accounting, billing)
  - Encourage efficient resource usage
  - Competitiveness and cost recovery
- User’s perspective
  - Fairness and Stability
  - Transparency and Predictability
  - Controllability

Multimedia applications

- Audio
  - Speech (CELP – type codecs)
  - Music (MP3, WAV, WMA, Real)
- Video (MPEG –1, 2, 4)
- Streaming
  - using HTTP/TCP (MP3)
  - using RTP/UDP (Video)

Multimedia protocol stack



Session Initiation Protocol (SIP)

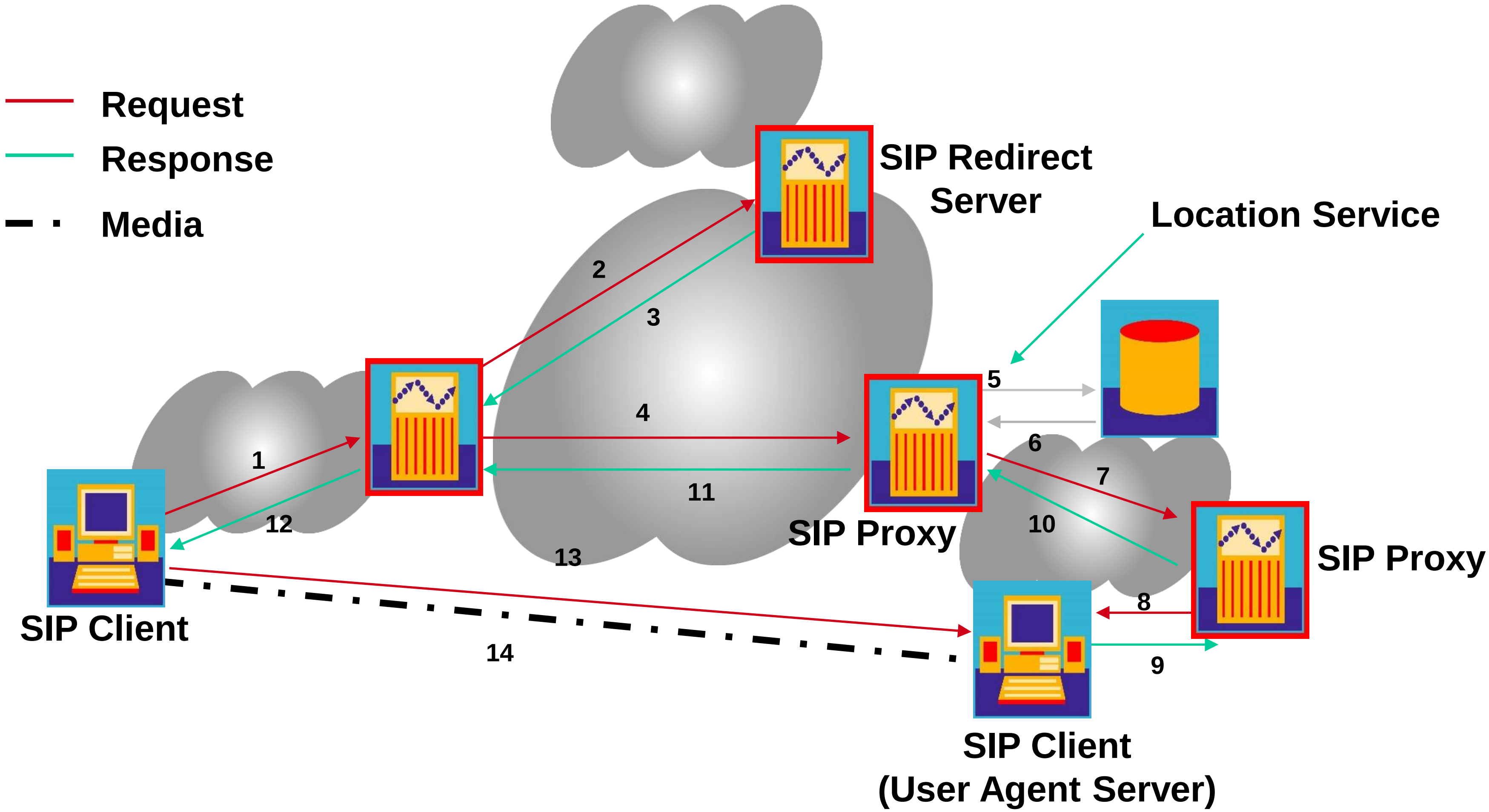
- Invite users to sessions
  - Find the user’s current location
  - match with their capabilities and preferences in order to deliver invitation
- Modify/Terminate sessions

- Session Description Protocol (SDP)
  - Used to specify client capabilities
  - Example (client can support MPEG-1 video codec, and MP3 codecs)

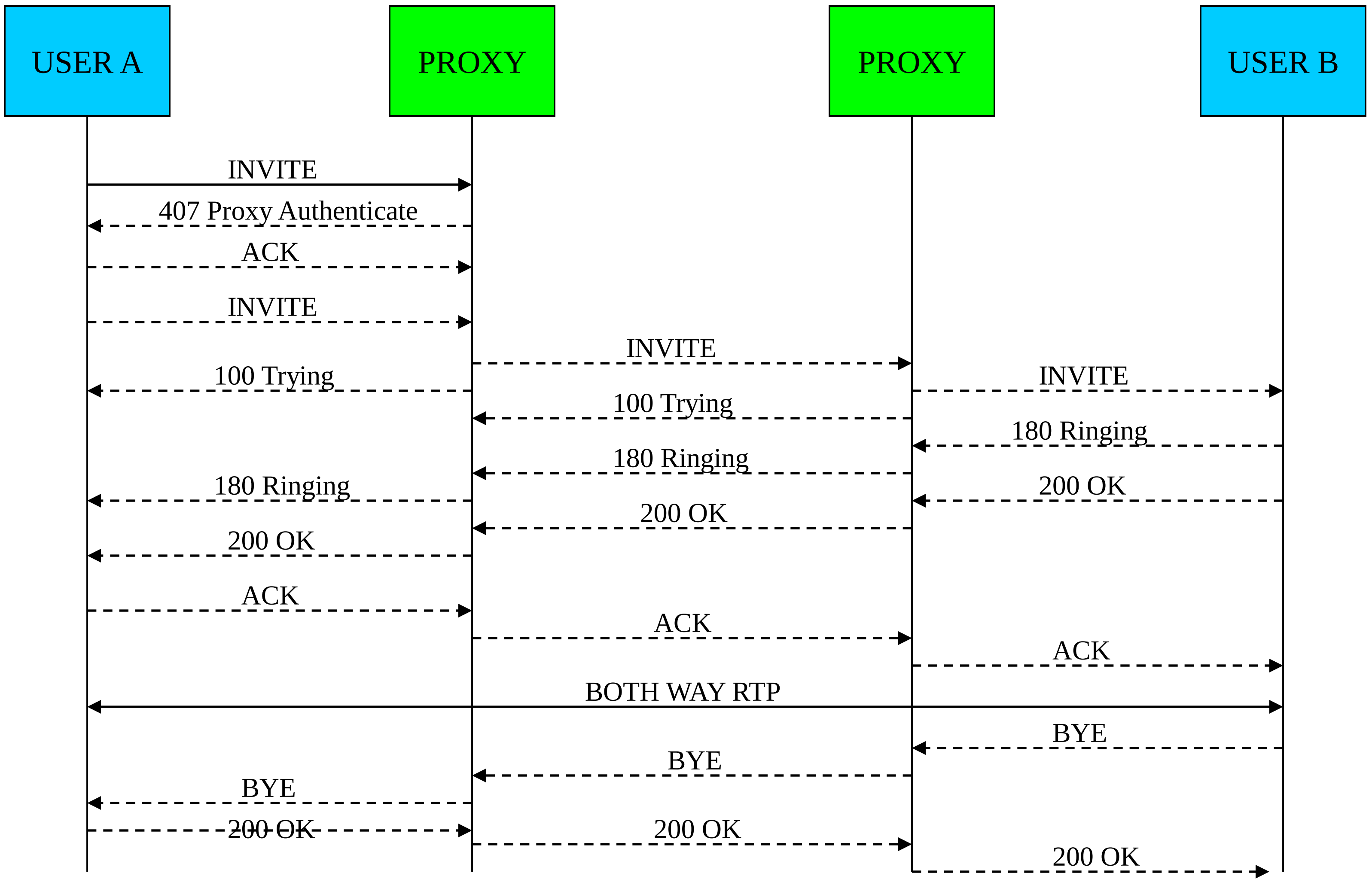
SIP components

- User Agent Client (UAC)
  - End systems; Send SIP requests
- User Agent Server (UAS)
  - Listens for call requests
  - Prompts user or executes program to determine response
- User Agent: UAC plus UAS
- Registrar
  - Receives registrations regarding current user locations
- Redirect Server
  - Redirects users to try other server
- Proxy Server

SIP architecture



SIP call flow example

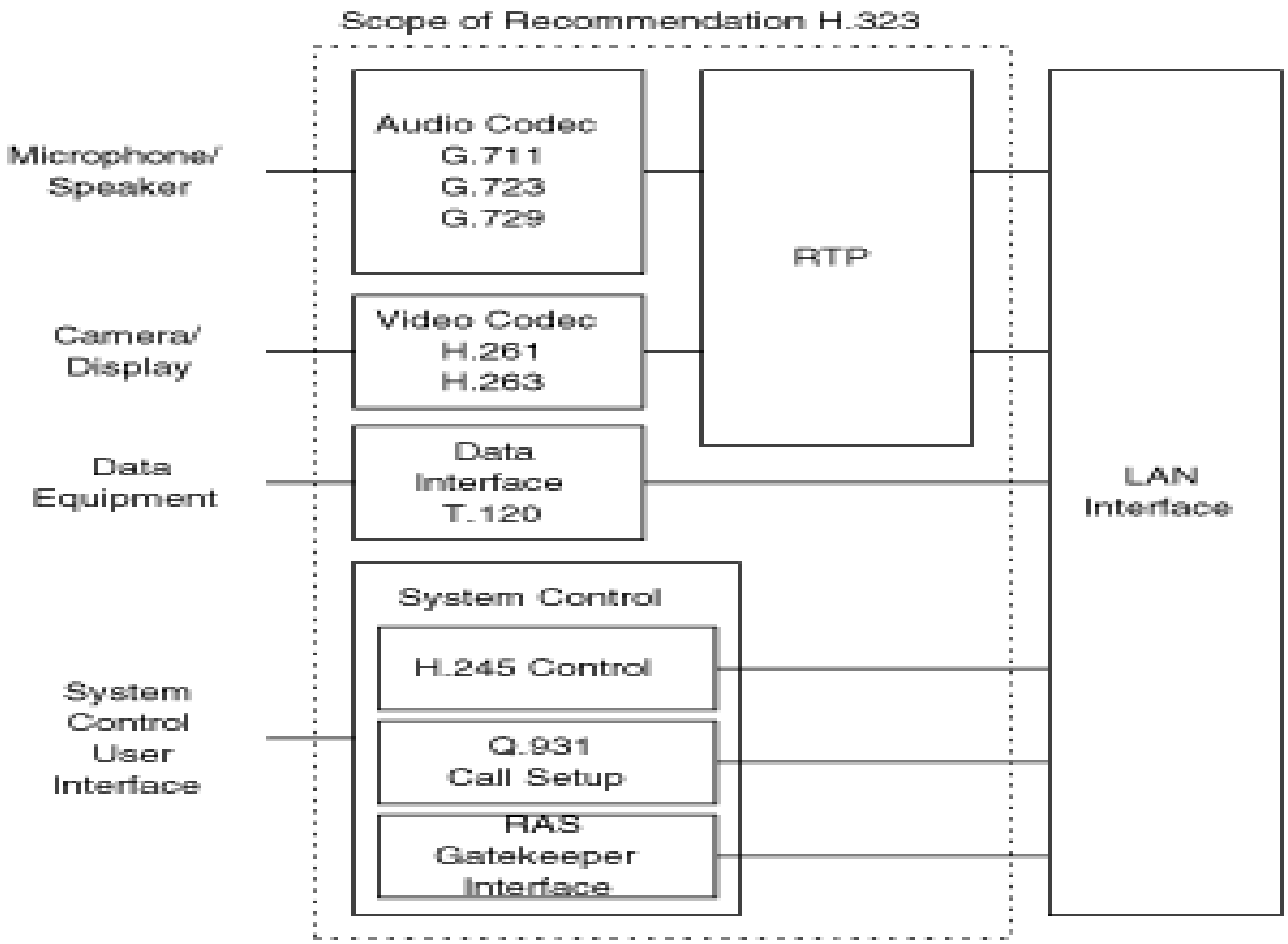


H.323

- H.323 is an ITU standard for multimedia communications over best-effort LANs.
- Part of larger set of standards (H.32X) for videoconferencing over data networks.

- H.323 addresses call control, multimedia management, and bandwidth management as well as interfaces between LANs and other networks.

H.323 architecture



H.323 components

- Terminals:
  - All terminals must support voice; video and data are optional
- Gatekeeper:
  - most important component which provides call control services
- Gateway:
  - an optional element which provides translation functions between H.323 conferencing endpoints (esp for ISDN, PSTN)
- Multipoint Control Unit (MCU):
  - supports conferences between three or more endpoints. Consists of a Multipoint Controller (MC) and Multipoint Processors (MP)

H.323 Gatekeeper

- Address translation
  – H.323 Alias to transport (IP) address
- Admission control
  – Permission to complete call
  – Can apply bandwidth limits
  – Method to control LAN traffic
- Call signaling/management/reporting/logging
- Management of Gateway
  – H.320, H.324, POTS, etc.

H.323 example

1. A sends request to GateKeeper: Can I call B?
2. GK resolves “Bob” to IP address through H.323 registration or external name service
3. GK applies Admission Policy
4. GK replies to A with B’s IP address
5. A sends Setup message to B
6. B checks with GK for authorizing the connection
7. GK acknowledges B to accept call
8. B replies to A and alerts User
9. H.245 connection established

Media transport: RTP

- Transport of real-time data, audio and video
- RTP follows the application level framing (ALF)
  - RTP specifies common application functions
  - Tailored through modifications and/or additions to the headers
- RTP consists of a data and a control part
  - The data part of RTP is a thin protocol
  - The control part of RTP is called RTCP
    - quality-of-service feedback from receivers
    - snchronization support for media streams

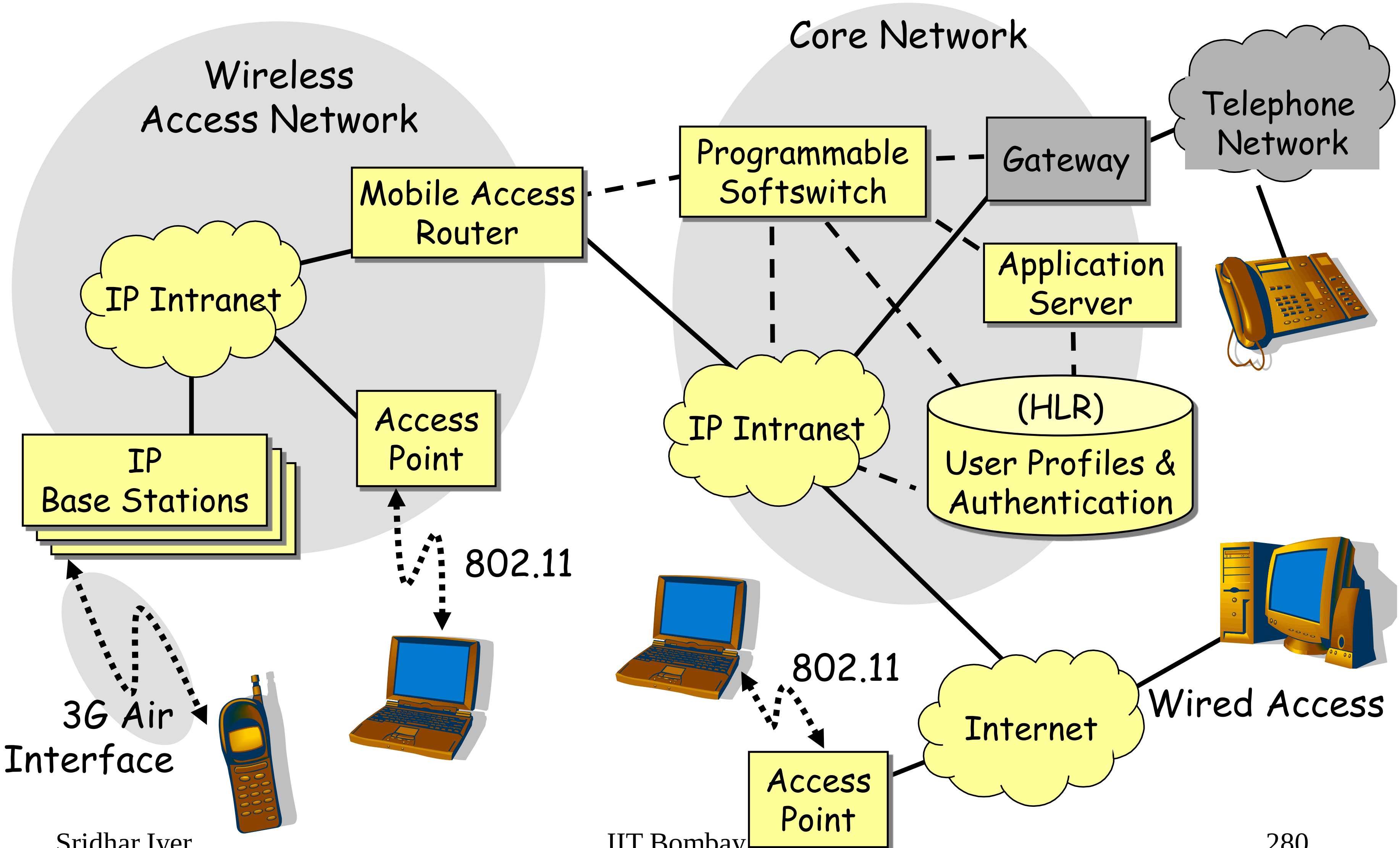
RTP (contd)

- RTP services
  - payload type identification
  - sequence numbering, timestamping
  - delivery monitoring, optional mixing/translation.

- UDP for multiplexing and checksum services
- RTP does not provide
  - mechanisms to ensure quality-of-service, guarantee delivery or prevent out-of-order delivery or loss

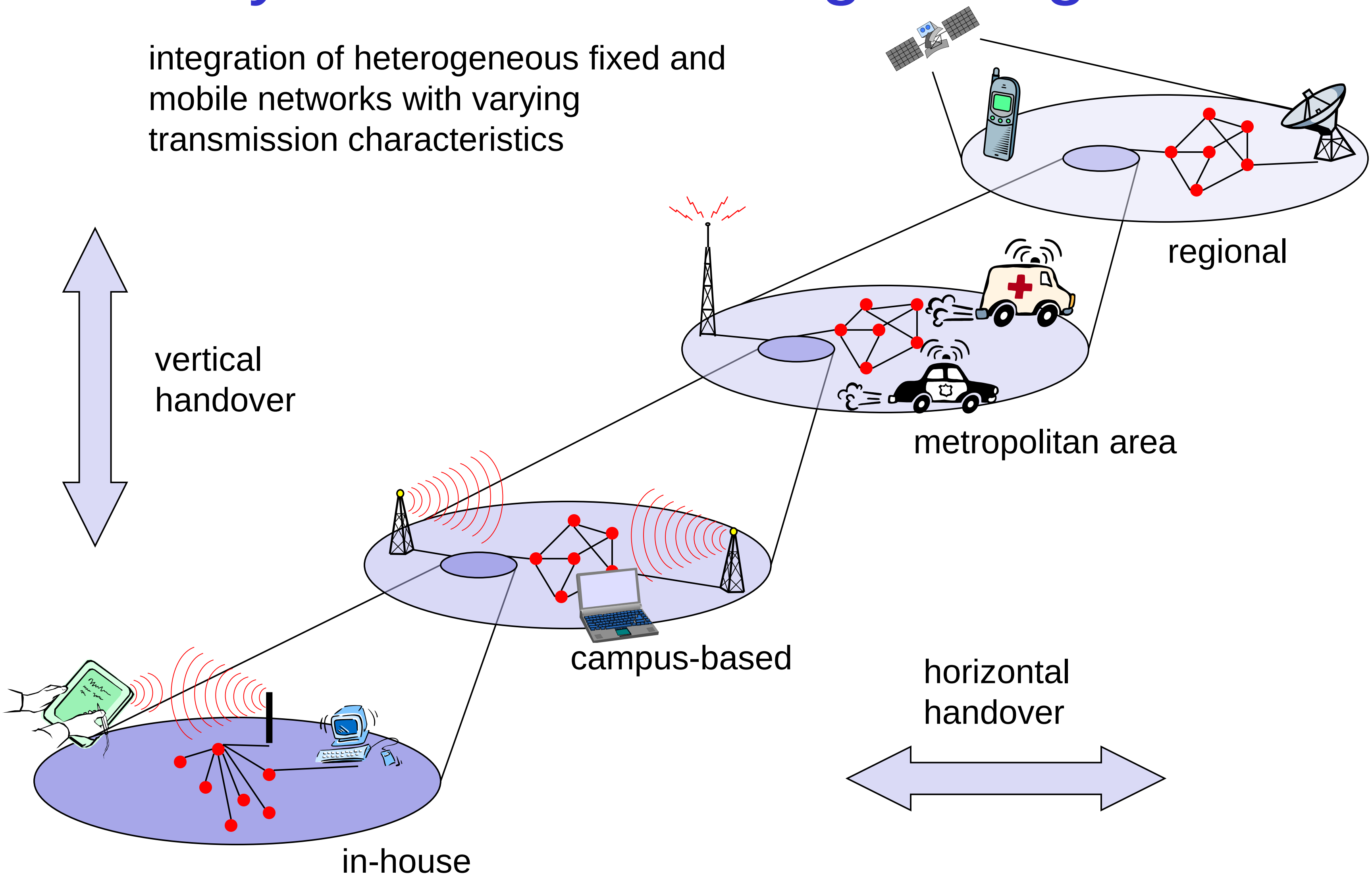
Trends

3G Network Architecture



Overlay Networks - the global goal

integration of heterogeneous fixed and mobile networks with varying transmission characteristics



Future mobile and wireless networks

- Improved radio technology and antennas
  - smart antennas, beam forming, multiple-input multiple-output (MIMO)
    - space division multiplex to increase capacity, benefit from multipath
  - software defined radios (SDR)
    - use of different air interfaces, download new modulation/coding
    - requires a lot of processing power
  - dynamic spectrum allocation
    - spectrum on demand results in higher overall capacity
- Core network convergence
  - IP-based, quality of service, mobile IP
- Ad-hoc technologies
  - spontaneous communication, power saving, redundancy

References

- A.S. Tanenbaum. Computer Networks. Pearson Education, 2003.
- J. Schiller, Mobile Communications, Addison Wesley, 2002.
- Y-B. Lin and I Chlamtac, Wireless and Mobile Network Architectures, Wiley, 2001.

- 802.11 Wireless LAN, IEEE standards, www.ieee.org
- Various RFCs: RFC 2002, 2501, 3150, 3449, www.ietf.org

- Others websites:
  - www.palowireless.com

Thank You

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

Contact Details:

Sridhar Iyer

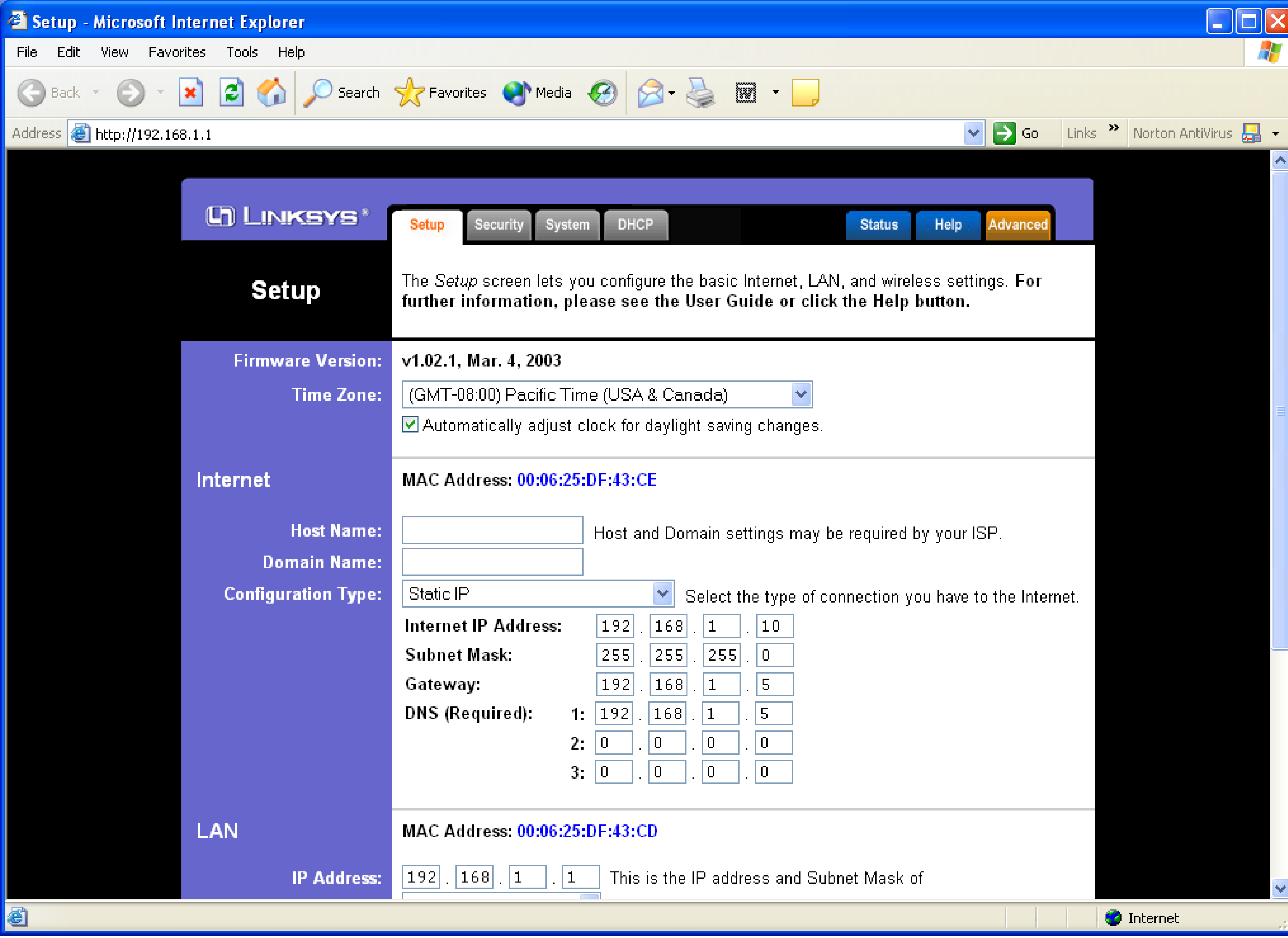
School of Information Technology

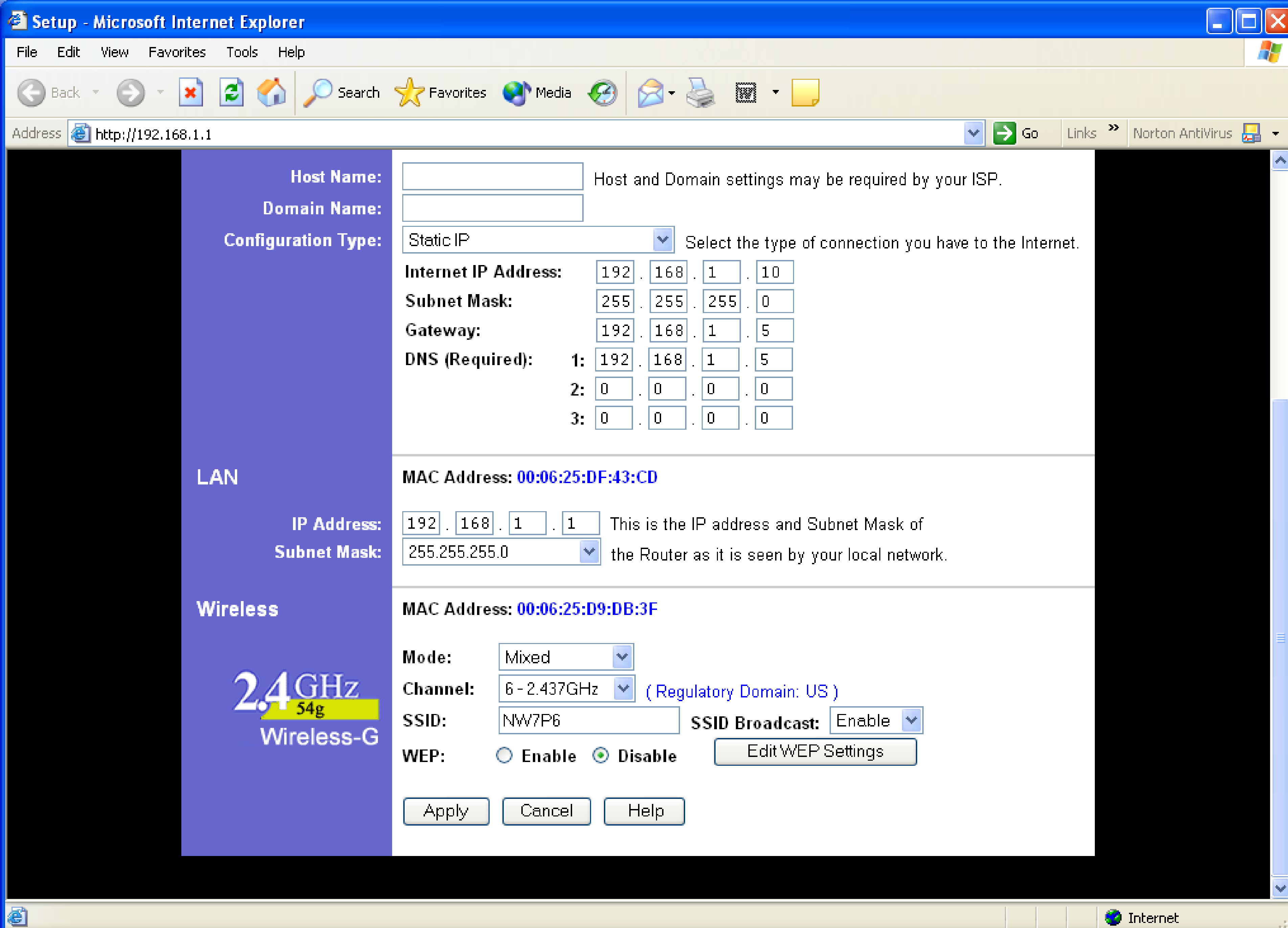
IIT Bombay, Powai, Mumbai 400 076

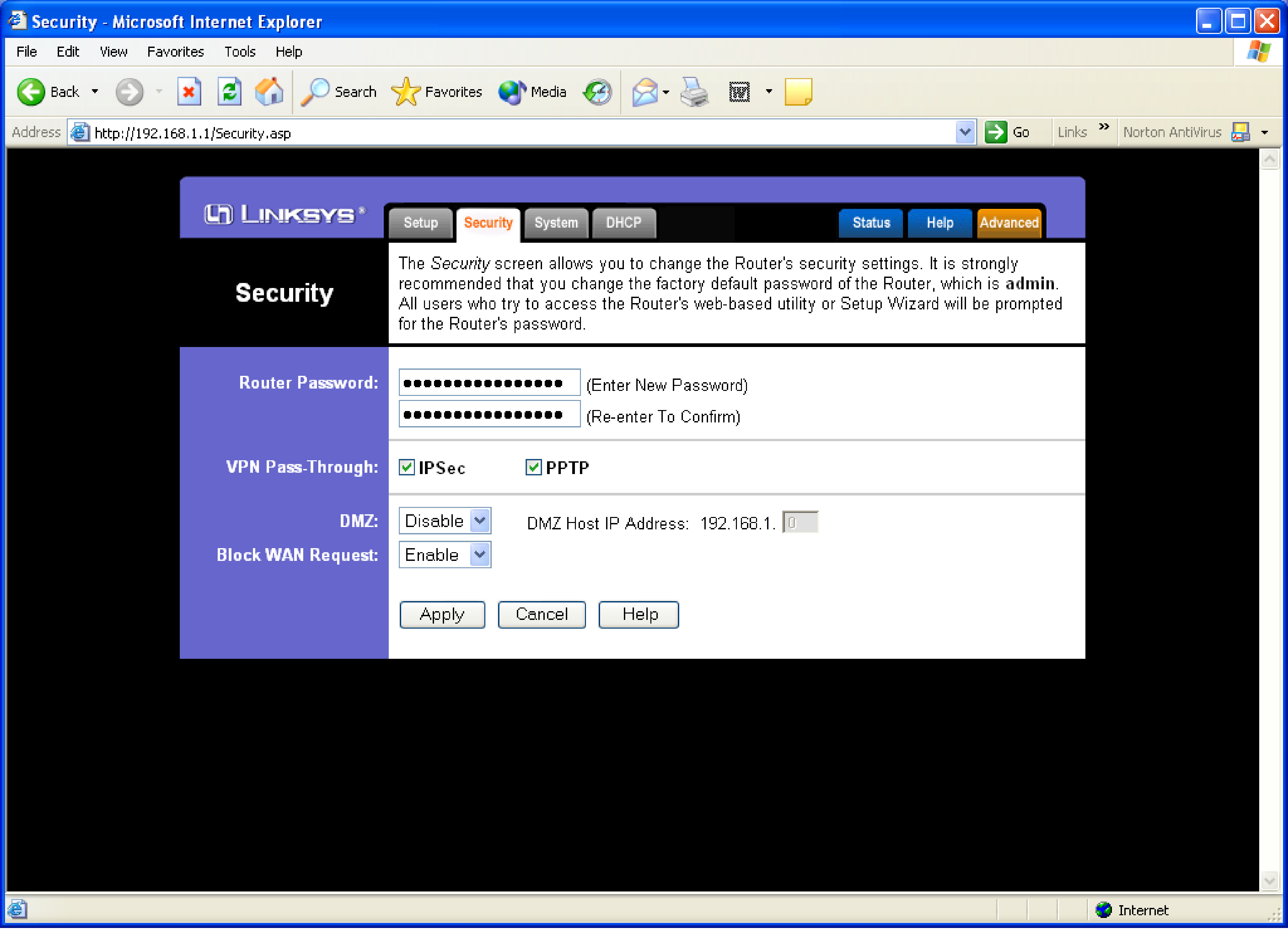
Phone: +91-22-2576-7905

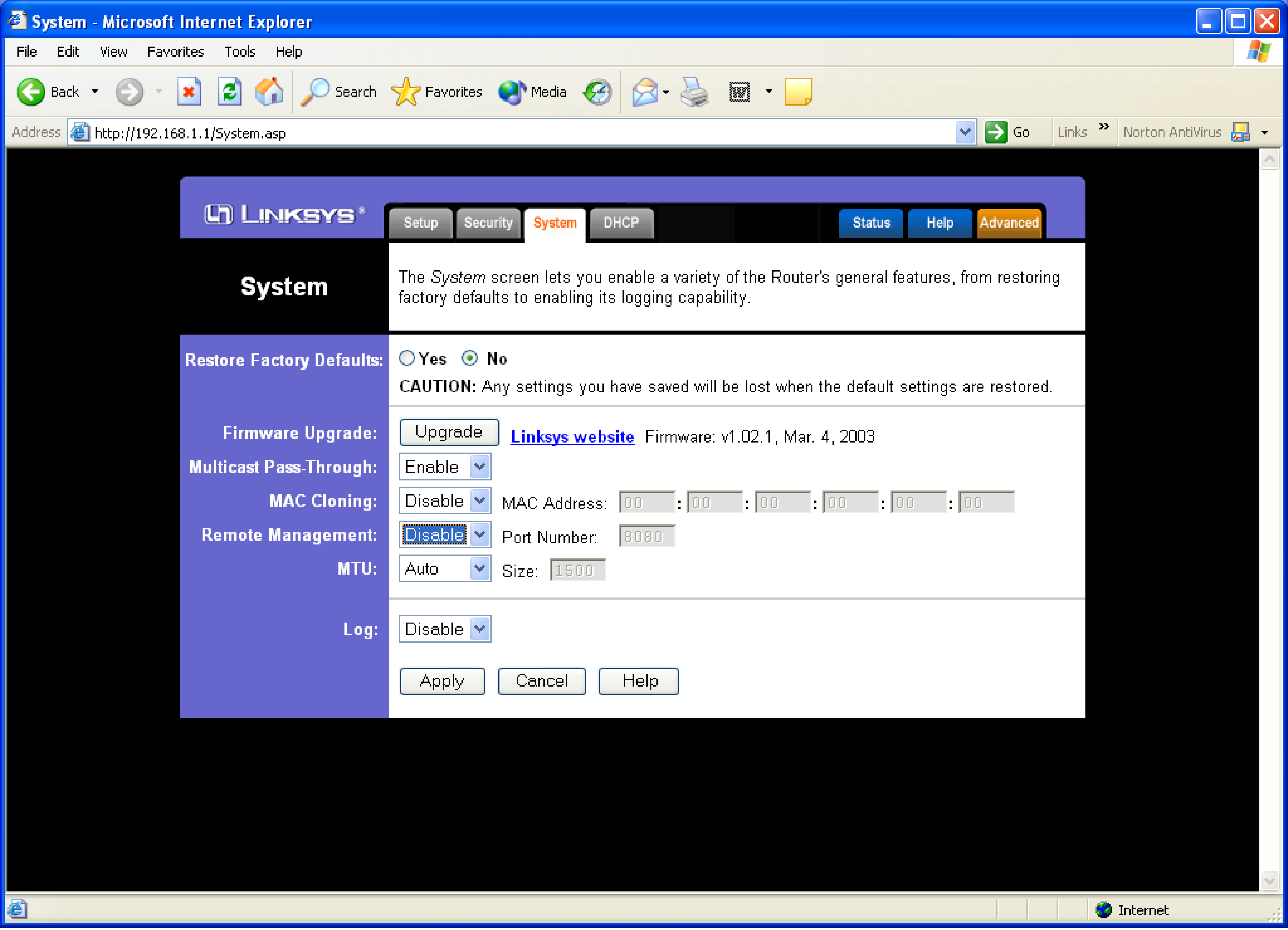
Email: sri@it.iitb.ac.in

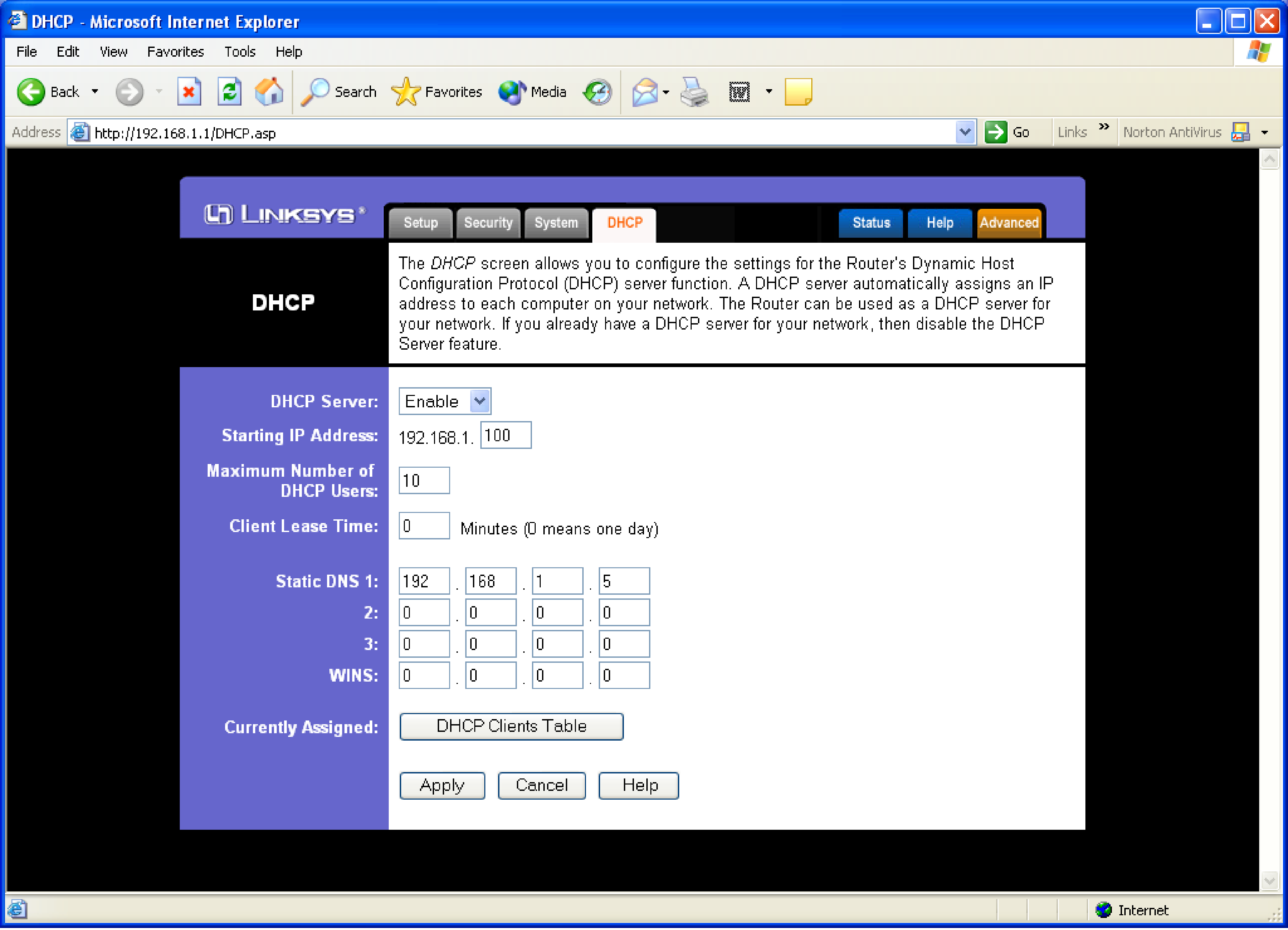
Extra Slides: AP Setup & Site Survey

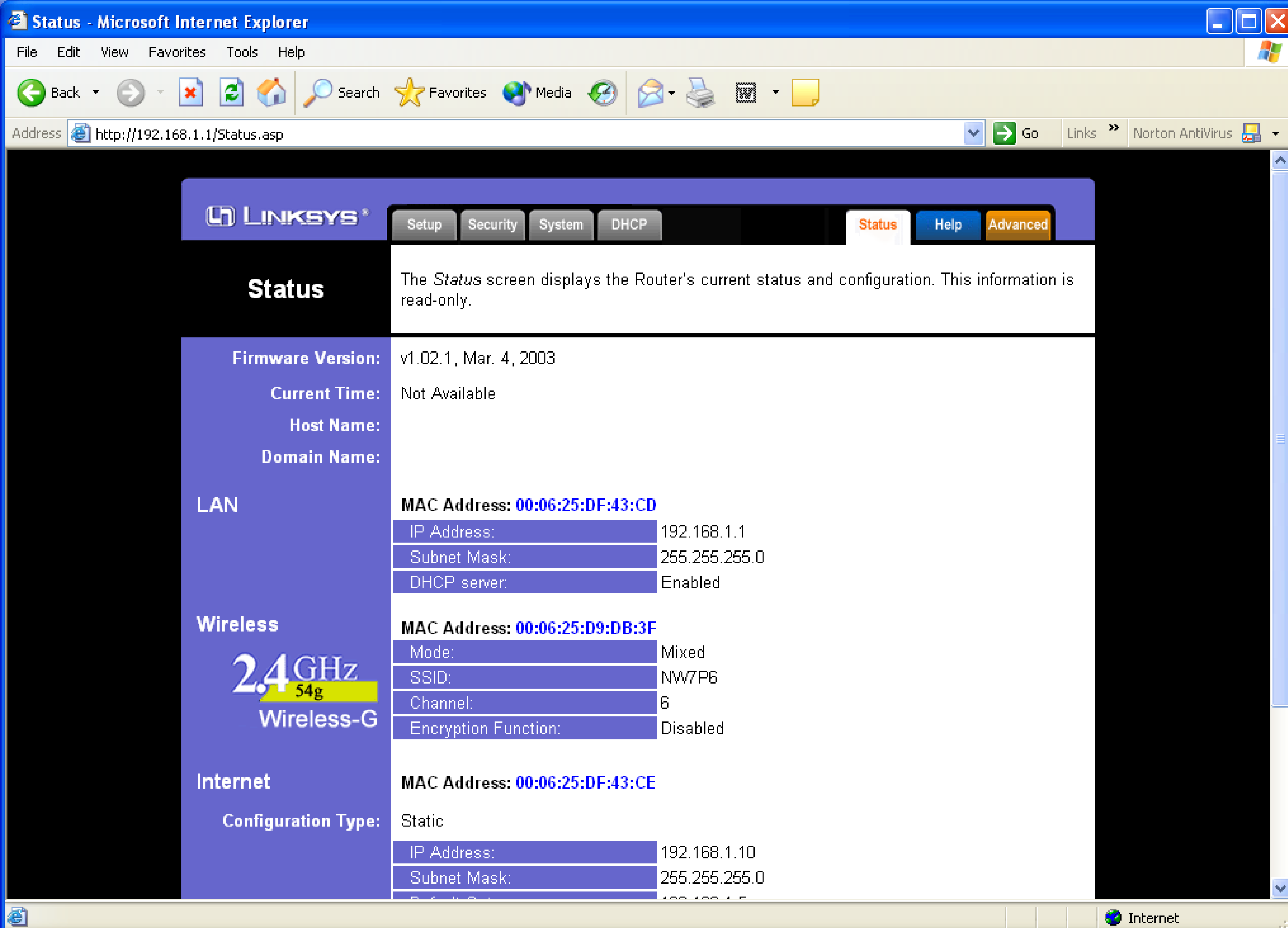

Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1
Go Links Norton AntiVirus
LINKSYS
Setup Security System DHCP Status Help Advanced
Setup
The Setup screen lets you configure the basic Internet, LAN, and wireless settings. For further information, please see the User Guide or click the Help button.
Firmware Version: v1.02.1, Mar. 4, 2003
Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
Automatically adjust clock for daylight saving changes.
Internet
MAC Address: 00:06:25:DF:43:CE
Host Name:
Domain Name:
Host and Domain settings may be required by your ISP.
Configuration Type: Static IP
Select the type of connection you have to the Internet.
Internet IP Address: 192 . 168 . 1 . 10
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 5
DNS (Required): 1: 192 . 168 . 1 . 5
2: 0 . 0 . 0 . 0
3: 0 . 0 . 0 . 0
LAN
MAC Address: 00:06:25:DF:43:CD
IP Address: 192 . 168 . 1 . 1
This is the IP address and Subnet Mask of
Internet

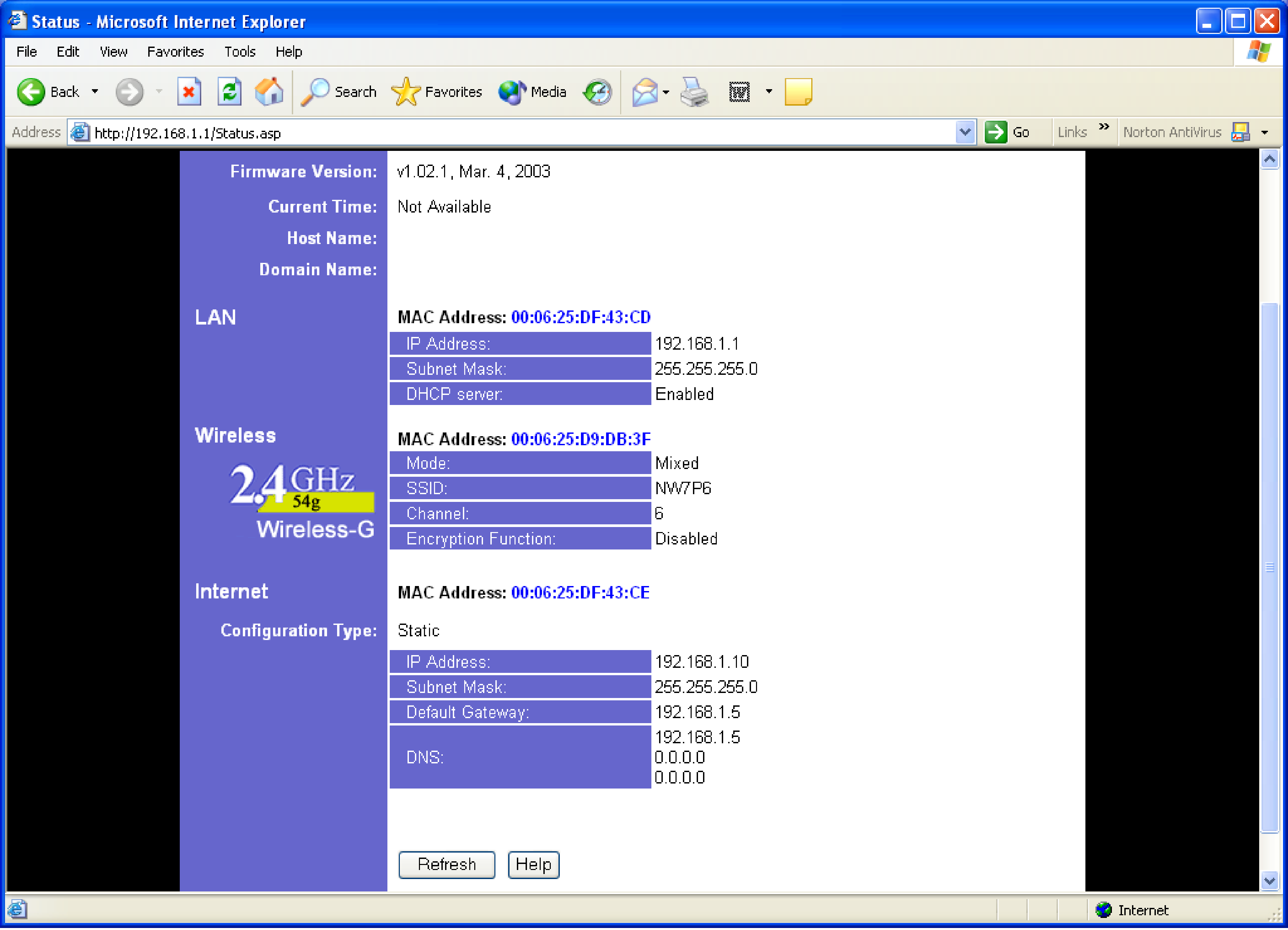

Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1
Go Links Norton AntiVirus
Host Name:
Host and Domain settings may be required by your ISP.
Domain Name:
Configuration Type:
Static IP
Select the type of connection you have to the Internet.
Internet IP Address: 192 . 168 . 1 . 10
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 5
DNS (Required): 1: 192 . 168 . 1 . 5
2: 0 . 0 . 0 . 0
3: 0 . 0 . 0 . 0
LAN
MAC Address: 00:06:25:DF:43:CD
IP Address: 192 . 168 . 1 . 1
This is the IP address and Subnet Mask of
Subnet Mask: 255.255.255.0
the Router as it is seen by your local network.
Wireless
MAC Address: 00:06:25:D9:DB:3F
2.4GHz 54g
Wireless-G
Mode: Mixed
Channel: 6 - 2.437GHz
(Regulatory Domain: US)
SSID: NW7P6
SSID Broadcast: Enable
WEP: Enable Disable
Edit WEP Settings
Apply Cancel Help
Internet

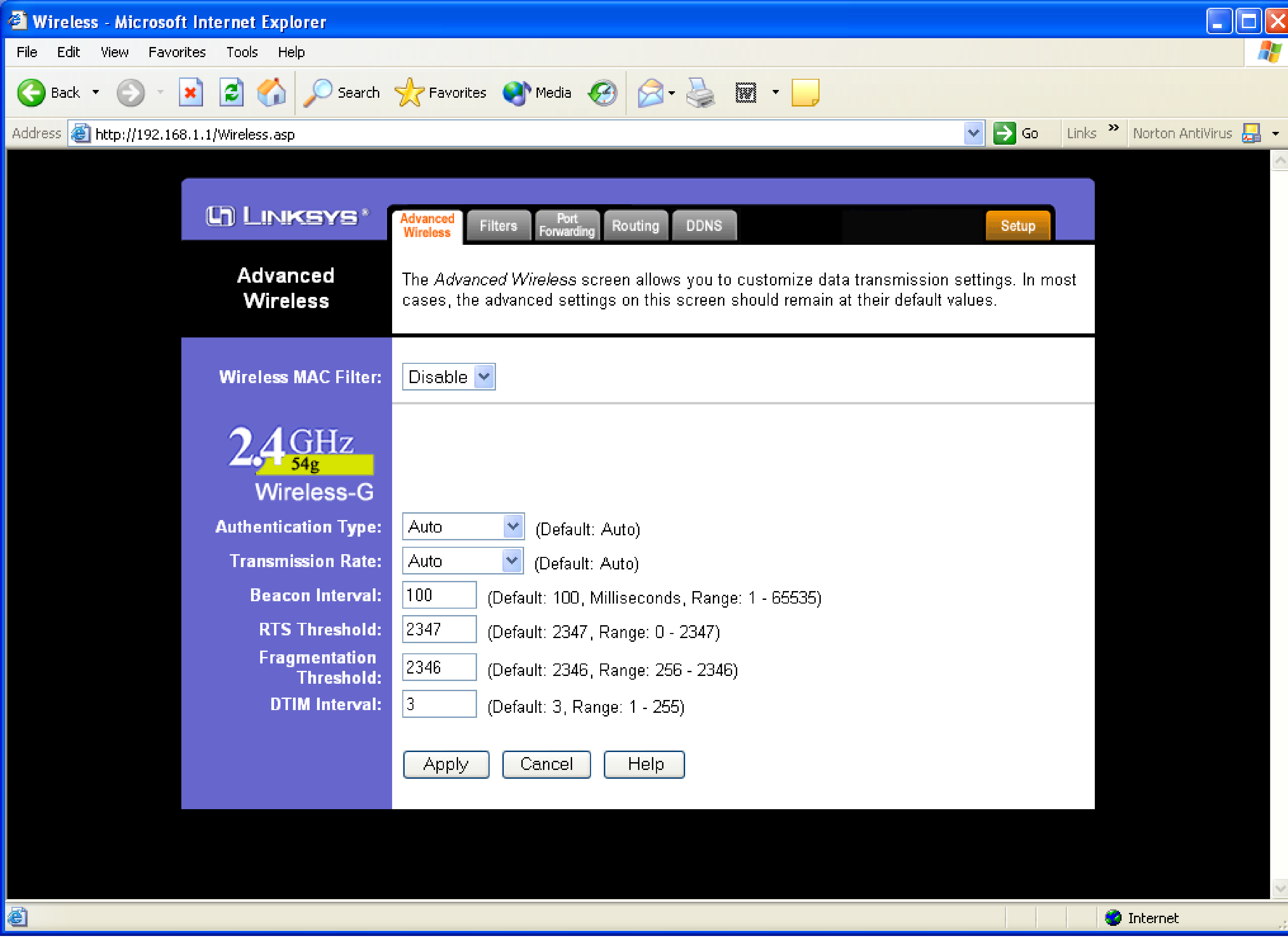

Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/Security.asp
Go Links Norton AntiVirus
LINKSYS
Setup Security System DHCP Status Help Advanced
Security
The Security screen allows you to change the Router's security settings. It is strongly recommended that you change the factory default password of the Router, which is admin. All users who try to access the Router's web-based utility or Setup Wizard will be prompted for the Router's password.
Router Password:
(Enter New Password)
(Re-enter To Confirm)
VPN Pass-Through:
IPSec
PPTP
DMZ:
Disable
DMZ Host IP Address: 192.168.1.
Block WAN Request:
Enable
Apply
Cancel
Help
Internet


System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/System.asp
Go Links Norton AntiVirus
LINKSYS
Setup Security System DHCP Status Help Advanced
System
The System screen lets you enable a variety of the Router's general features, from restoring factory defaults to enabling its logging capability.
Restore Factory Defaults: Yes No
CAUTION: Any settings you have saved will be lost when the default settings are restored.
Firmware Upgrade: Upgrade Linksys website Firmware: v1.02.1, Mar. 4, 2003
Multicast Pass-Through: Enable
MAC Cloning: Disable MAC Address: 00 : 00 : 00 : 00 : 00 : 00
Remote Management: Disable Port Number: 8080
MTU: Auto Size: 1500
Log: Disable
Apply Cancel Help
Internet

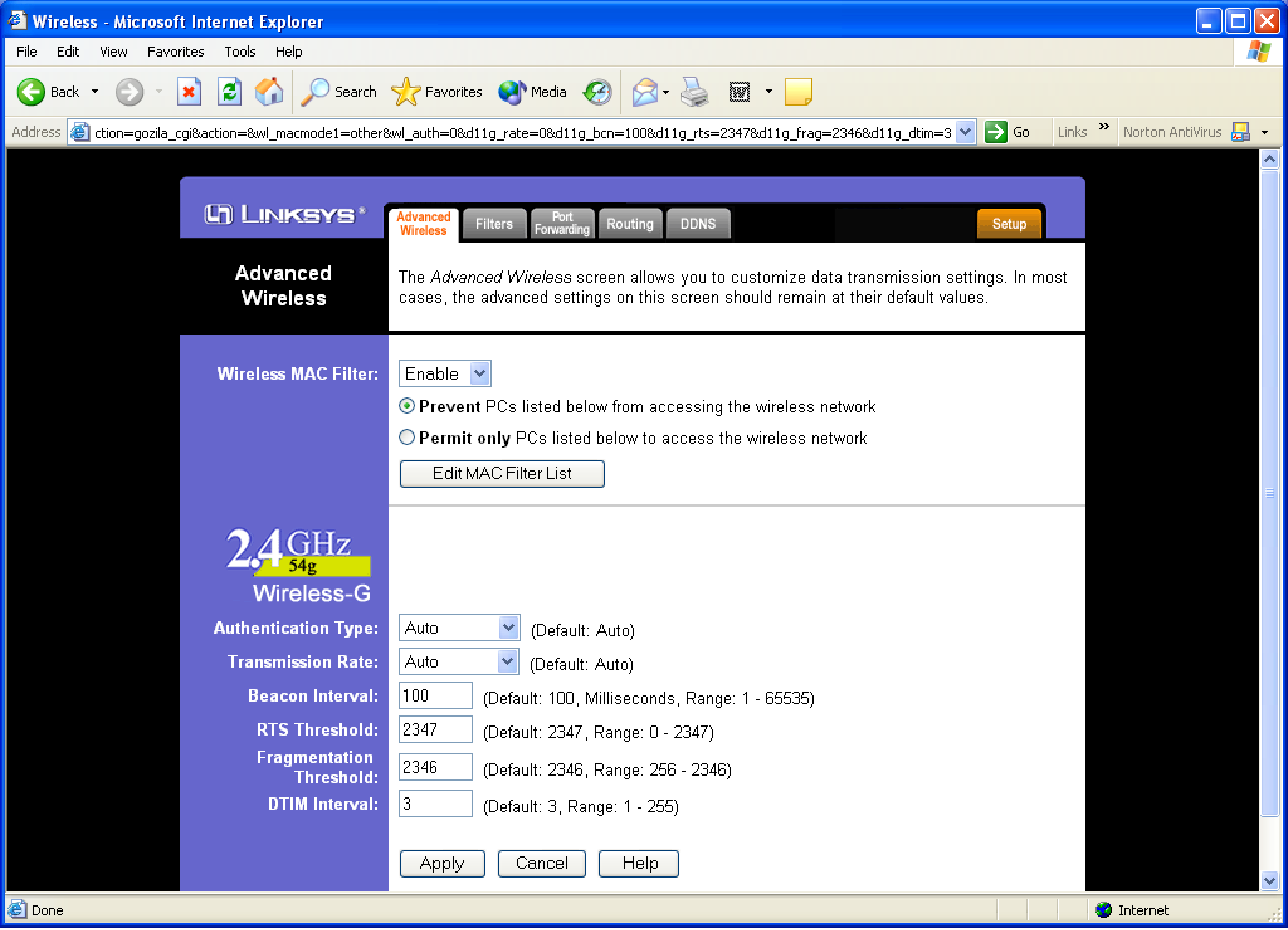

DHCP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/DHCP.asp
Go Links Norton AntiVirus
LINKSYS
Setup Security System DHCP Status Help Advanced
DHCP
The DHCP screen allows you to configure the settings for the Router's Dynamic Host Configuration Protocol (DHCP) server function. A DHCP server automatically assigns an IP address to each computer on your network. The Router can be used as a DHCP server for your network. If you already have a DHCP server for your network, then disable the DHCP Server feature.
DHCP Server: Enable
Starting IP Address: 192.168.1. 100
Maximum Number of DHCP Users: 10
Client Lease Time: 0 Minutes (0 means one day)
Static DNS 1: 192 . 168 . 1 . 5
2: 0 . 0 . 0 . 0
3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0
Currently Assigned: DHCP Clients Table
Apply Cancel Help
Internet

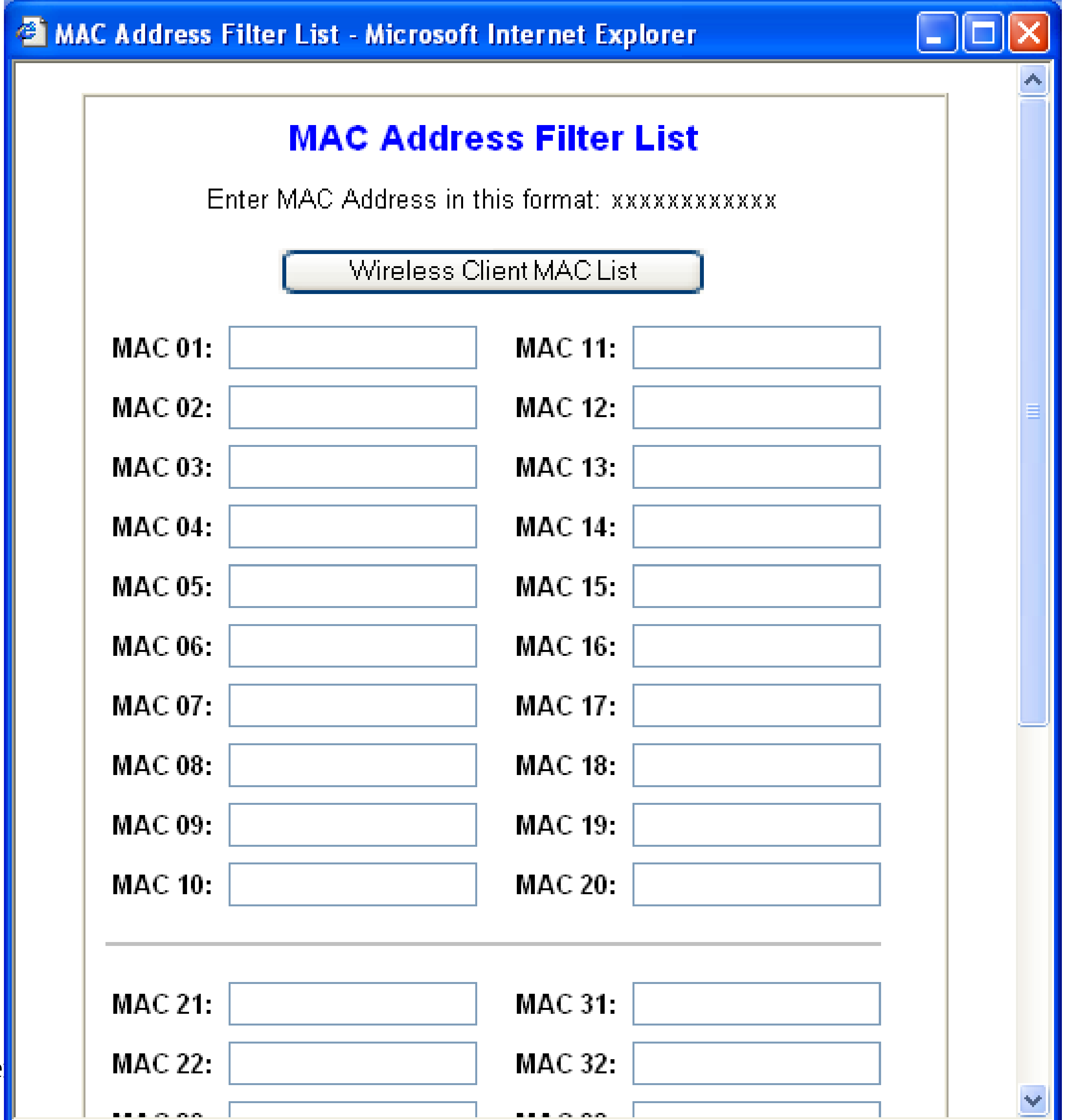

Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/Status.asp
Go Links Norton AntiVirus
LINKSYS
Setup Security System DHCP
Status Help Advanced
Status
The Status screen displays the Router's current status and configuration. This information is read-only.
Firmware Version: v1.02.1, Mar. 4, 2003
Current Time: Not Available
Host Name:
Domain Name:
LAN
MAC Address: 00:06:25:DF:43:CD
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP server: Enabled
Wireless
2.4GHz 54g
Wireless-G
MAC Address: 00:06:25:D9:DB:3F
Mode: Mixed
SSID: NW7P6
Channel: 6
Encryption Function: Disabled
Internet
MAC Address: 00:06:25:DF:43:CE
Configuration Type: Static
IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Internet

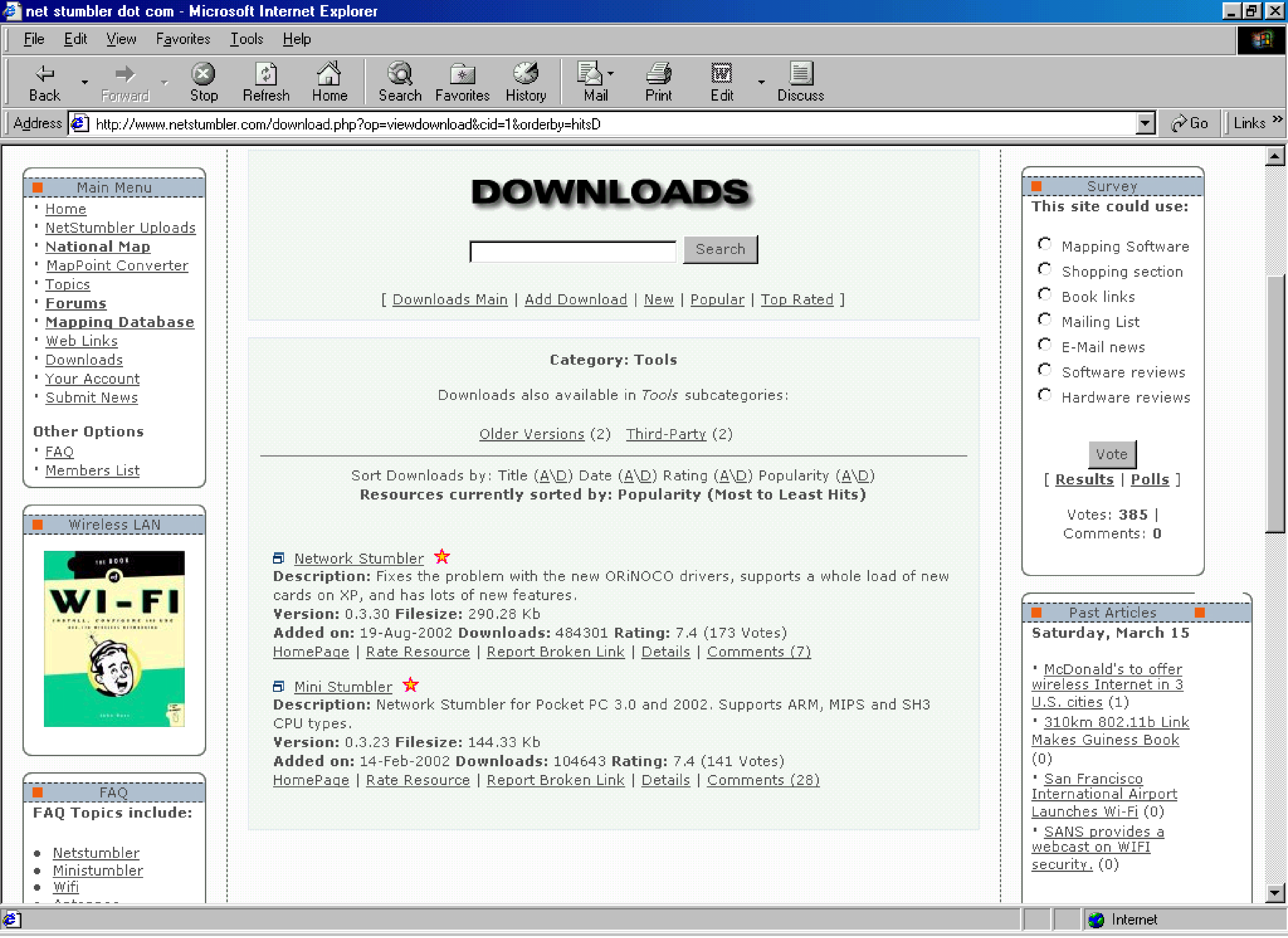

Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.1.1/Status.asp
Go
Links
Norton AntiVirus
Firmware Version: v1.02.1, Mar. 4, 2003
Current Time: Not Available
Host Name:
Domain Name:
LAN
MAC Address: 00:06:25:DF:43:CD
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP server: Enabled
Wireless
2.4GHz
54g
Wireless-G
MAC Address: 00:06:25:D9:DB:3F
Mode: Mixed
SSID: NW7P6
Channel: 6
Encryption Function: Disabled
Internet
MAC Address: 00:06:25:DF:43:CE
Configuration Type: Static
IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.5
DNS: 192.168.1.5
0.0.0.0
0.0.0.0
Refresh
Help
Internet

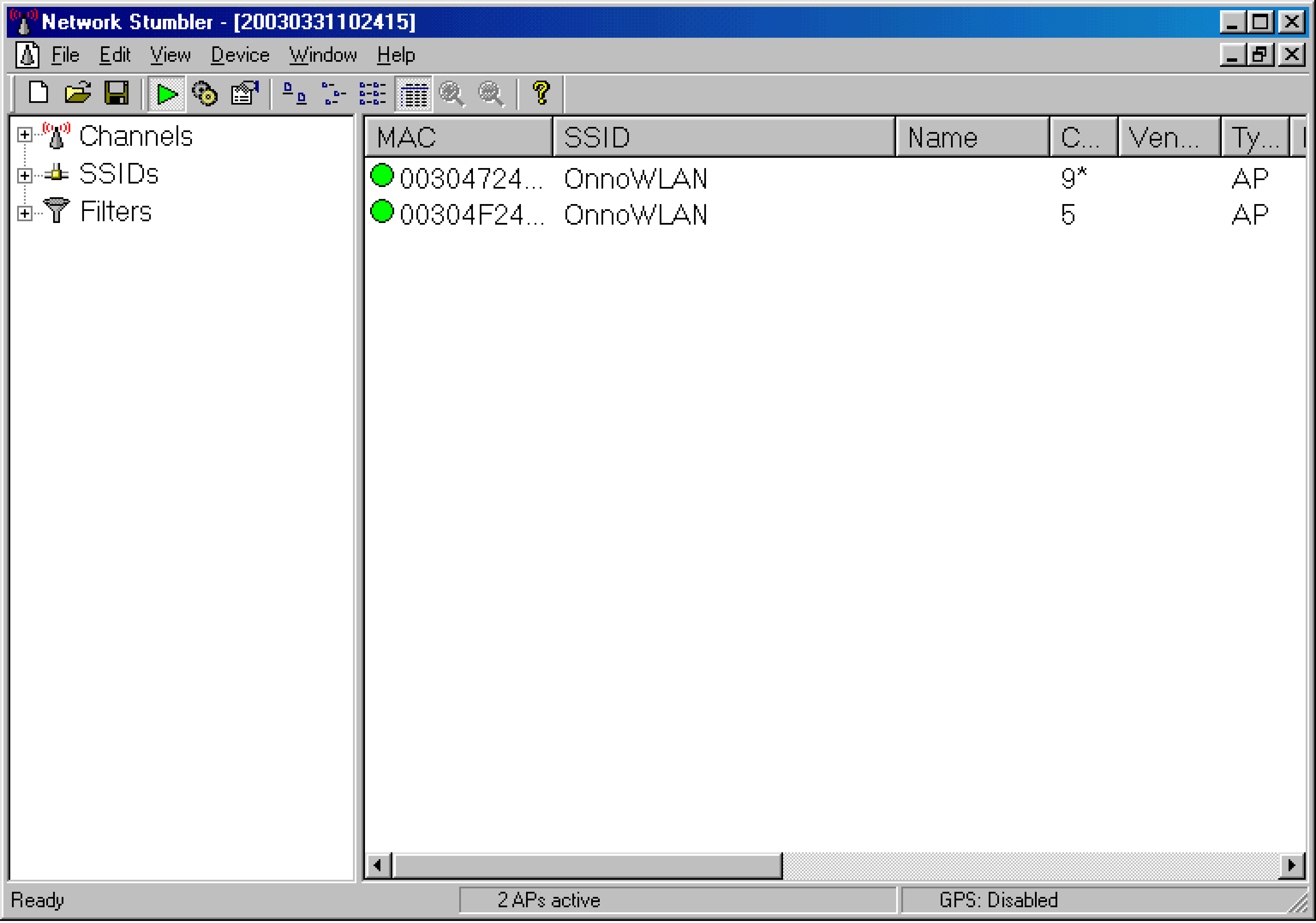


Wireless - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.1.1/Wireless.asp
Go
Links
Norton AntiVirus
LINKSYS
Advanced Wireless
Filters
Port Forwarding
Routing
DDNS
Setup
Advanced Wireless
The Advanced Wireless screen allows you to customize data transmission settings. In most cases, the advanced settings on this screen should remain at their default values.
Wireless MAC Filter:
Disable
2.4GHz
54g
Wireless-G
Authentication Type:
Auto
(Default: Auto)
Transmission Rate:
Auto
(Default: Auto)
Beacon Interval:
100
(Default: 100, Milliseconds, Range: 1 - 65535)
RTS Threshold:
2347
(Default: 2347, Range: 0 - 2347)
Fragmentation Threshold:
2346
(Default: 2346, Range: 256 - 2346)
DTIM Interval:
3
(Default: 3, Range: 1 - 255)
Apply
Cancel
Help
Internet

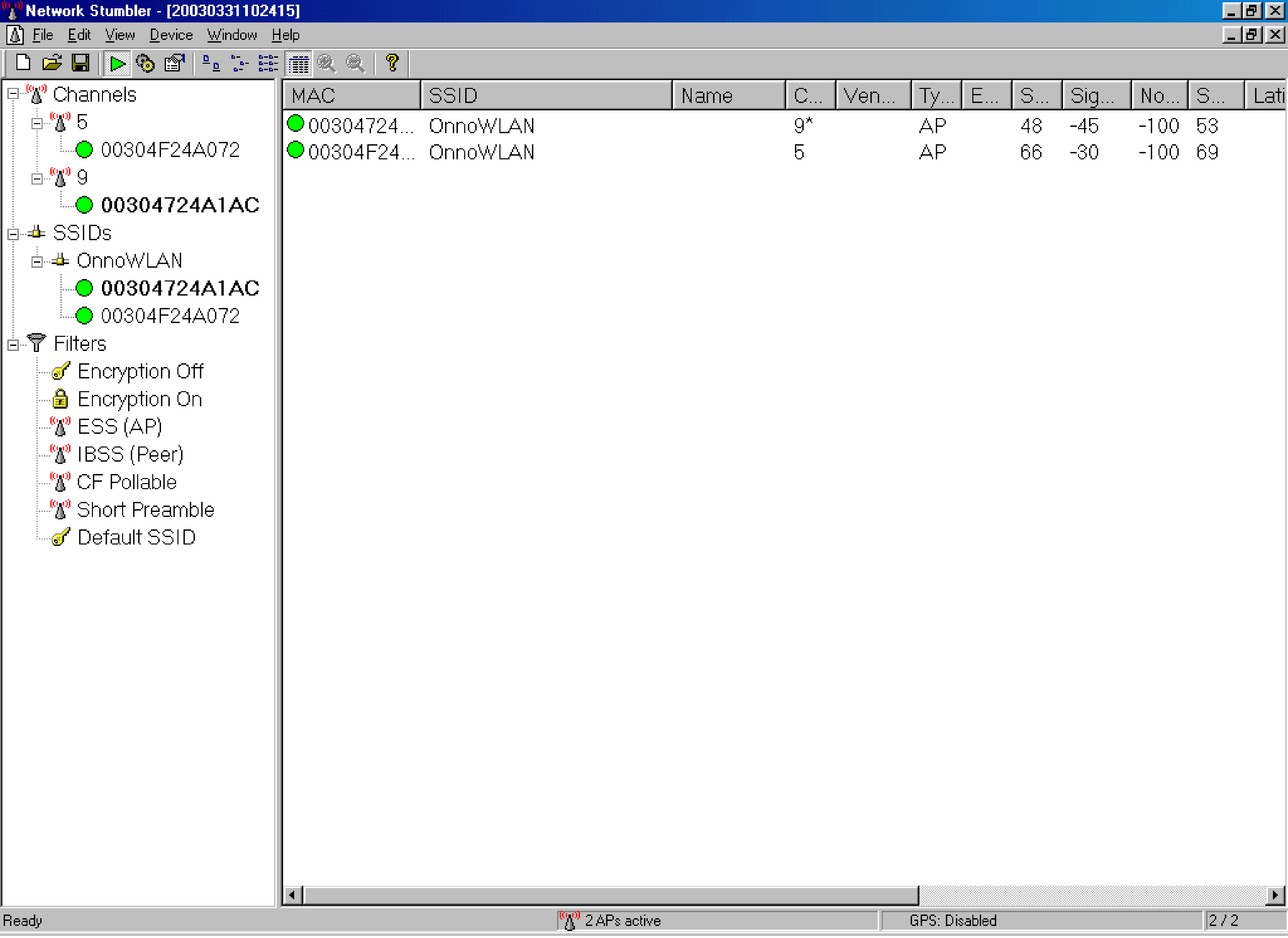

Wireless - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address ction=gozila_cgi&action=&wl_macmode1=other&wl_auth=0&d11g_rate=0&d11g_bcn=100&d11g_rts=2347&d11g_frag=2346&d11g_dtim=3
Go Links Norton AntiVirus
LINKSYS
Advanced Wireless
Filters
Port Forwarding
Routing
DDNS
Setup
Advanced Wireless
The Advanced Wireless screen allows you to customize data transmission settings. In most cases, the advanced settings on this screen should remain at their default values.
Wireless MAC Filter:
Enable
Prevent PCs listed below from accessing the wireless network
Permit only PCs listed below to access the wireless network
Edit MAC Filter List
2.4GHz 54g
Wireless-G
Authentication Type:
Auto
(Default: Auto)
Transmission Rate:
Auto
(Default: Auto)
Beacon Interval:
100
(Default: 100, Milliseconds, Range: 1 - 65535)
RTS Threshold:
2347
(Default: 2347, Range: 0 - 2347)
Fragmentation Threshold:
2346
(Default: 2346, Range: 256 - 2346)
DTIM Interval:
3
(Default: 3, Range: 1 - 255)
Apply
Cancel
Help
Done
Internet


MAC Address Filter List - Microsoft Internet Explorer
MAC Address Filter List
Enter MAC Address in this format: xxxxxxxxxxxx
Wireless Client MAC List
MAC 01:
MAC 02:
MAC 03:
MAC 04:
MAC 05:
MAC 06:
MAC 07:
MAC 08:
MAC 09:
MAC 10:
MAC 11:
MAC 12:
MAC 13:
MAC 14:
MAC 15:
MAC 16:
MAC 17:
MAC 18:
MAC 19:
MAC 20:
MAC 21:
MAC 22:
MAC 31:
MAC 32:


net stumbler dot com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://www.netstumbler.com/download.php?op=viewdownload&cid=1&orderby=hitsD
Go Links
Main Menu
Home
NetStumbler Uploads
National Map
MapPoint Converter
Topics
Forums
Mapping Database
Web Links
Downloads
Your Account
Submit News
Other Options
FAQ
Members List
Wireless LAN
WI-FI
FAQ
FAQ Topics include:
Netstumbler
Ministumbler
Wifi
DOWNLOADS
Search
[Downloads Main | Add Download | New | Popular | Top Rated]
Category: Tools
Downloads also available in Tools subcategories:
Older Versions (2) Third-Party (2)
Sort Downloads by: Title (A\D) Date (A\D) Rating (A\D) Popularity (A\D)
Resources currently sorted by: Popularity (Most to Least Hits)
Network Stumbler
Description: Fixes the problem with the new ORiNOCO drivers, supports a whole load of new cards on XP, and has lots of new features.
Version: 0.3.30 Filesize: 290.28 Kb
Added on: 19-Aug-2002 Downloads: 484301 Rating: 7.4 (173 Votes)
HomePage | Rate Resource | Report Broken Link | Details | Comments (7)
Mini Stumbler
Description: Network Stumbler for Pocket PC 3.0 and 2002. Supports ARM, MIPS and SH3 CPU types.
Version: 0.3.23 Filesize: 144.33 Kb
Added on: 14-Feb-2002 Downloads: 104643 Rating: 7.4 (141 Votes)
HomePage | Rate Resource | Report Broken Link | Details | Comments (28)
Survey
This site could use:
Mapping Software
Shopping section
Book links
Mailing List
E-Mail news
Software reviews
Hardware reviews
Vote
[Results | Polls]
Votes: 385 |
Comments: 0
Past Articles
Saturday, March 15
McDonald's to offer wireless Internet in 3 U.S. cities (1)
310km 802.11b Link Makes Guiness Book (0)
San Francisco International Airport Launches Wi-Fi (0)
SANS provides a webcast on WIFI security. (0)
Internet



Network Stumbler - [20030331102415]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC
SSID
Name
C...
Ven...
Ty...
00304724... OnnoWLAN 9* AP
00304F24... OnnoWLAN 5 AP
Ready
2 APs active
GPS: Disabled


Network Stumbler - [20030331102415]
File Edit View Device Window Help
Channels
5
00304F24A072
9
00304724A1AC
SSIDs
OnnoWLAN
00304724A1AC
00304F24A072
Filters
Encryption Off
Encryption On
ESS (AP)
IBSS (Peer)
CF Pollable
Short Preamble
Default SSID
MAC SSID Name C... Ven... Ty... E... S... Sig... No... S... Lati
00304724... OnnoWLAN 9* AP 48 -45 -100 53
00304F24... OnnoWLAN 5 AP 66 -30 -100 69
Ready
2 APs active
GPS: Disabled
2 / 2