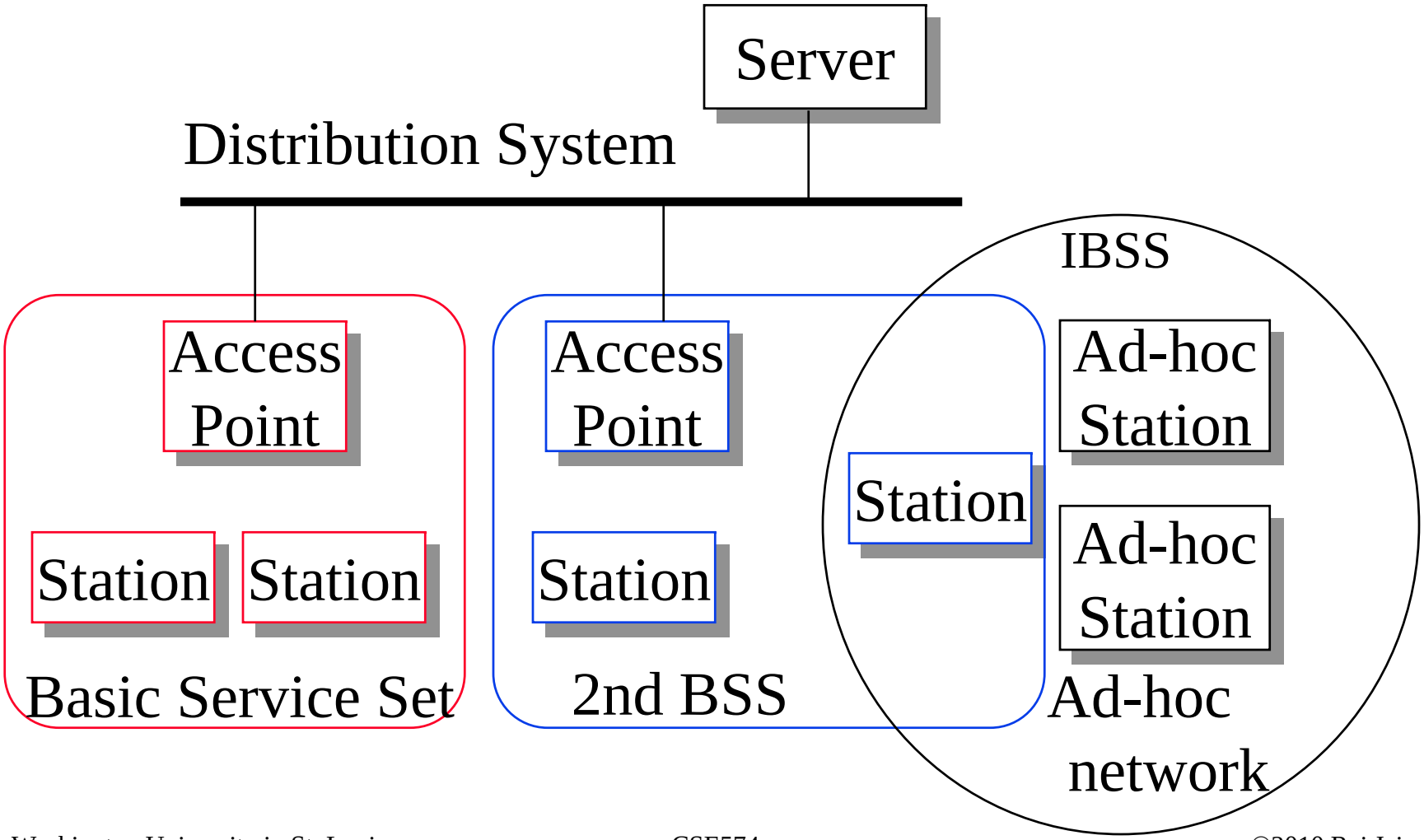
Wireless Local Area Networks (WLANs) Part II

Raj Jain
Professor of CSE
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse574-10/

- IEEE 802.11 Architecture
- Frame Format
- 802.11 Address Fields
- IEEE 802.11 Activities
- IEEE 802.11e QoS
- Power Management
- 802.11n
- IETF Activities related to 802.11

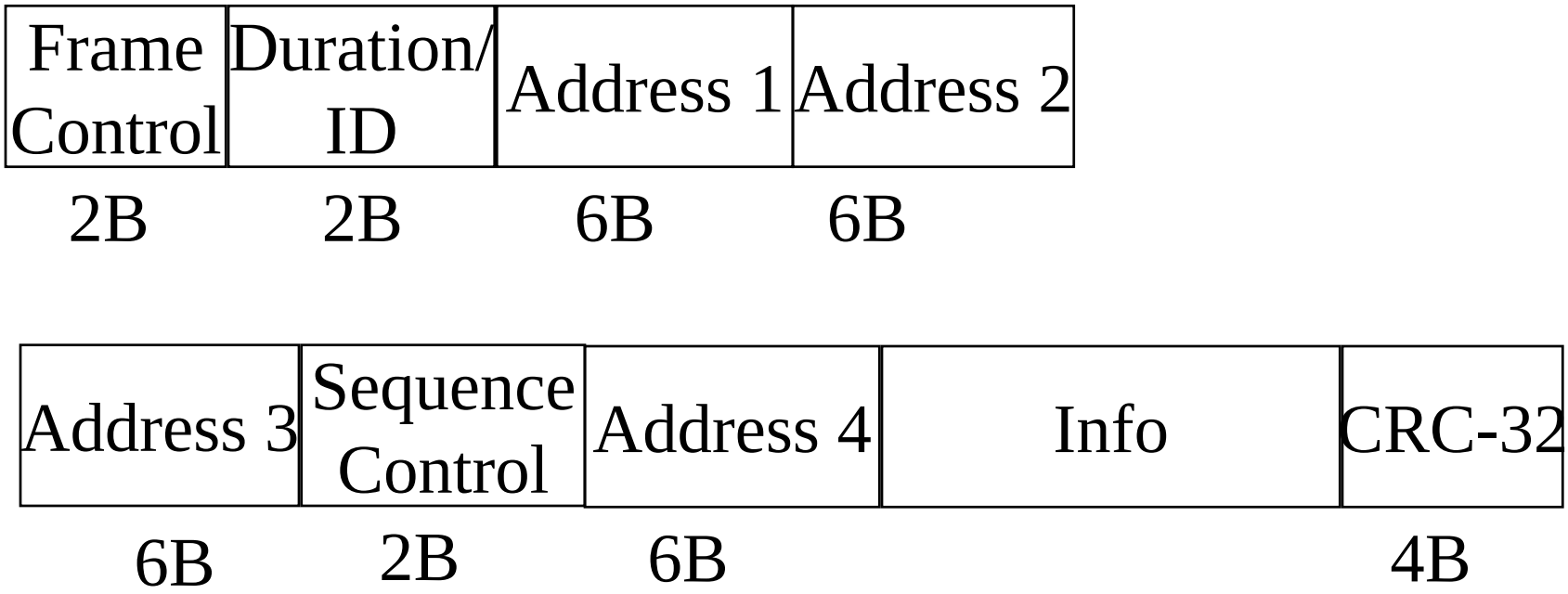
IEEE 802.11 Architecture



IEEE 802.11 Architecture (Cont)

- Basic Service Area (BSA) = Cell
- Each BSA may have several access points (APs)
- Basic Service Set (BSS)
  = Set of stations associated with one AP
- Distribution System (DS) - wired backbone
- Extended Service Area (ESA) = Multiple BSAs interconnected via a distribution system
- Extended Service Set (ESS)
  = Set of stations in an ESA
- Independent Basic Service Set (IBSS): Set of computers in ad-hoc mode. May not be connected to wired backbone.
- Ad-hoc networks coexist and interoperate with infrastructure-based networks

Frame Format



- **Frame Control**: Type of frame (Control, management, or data)
  - Includes whether frame is to or from DS, fragmentation information, and privacy information

MAC Frame Fields

- **Duration/Connection ID**:
  - If used as duration field, indicates time (in μs) channel will be allocated for successful transmission of MAC frame. Includes time until the end of Ack
  - In some control frames, contains association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

802.11 Address Fields

- Address 1: All stations filter on this addr.
- Address 2: Transmitter. BSSID = MAC Adr of AP.
- Address 3: Depends upon to/from
- Address 4: Original source

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

Wireless backbone. DA and SA are also on wireless LAN.

IEEE 802.11 Activities

- **802.11a**: Higher Speed PHY Extension in the 5 Ghz Band, Published as IEEE Std 802.11a-1999
- **802.11b**: Higher Speed PHY Extension in the 2.5 GHz Band, Published as IEEE Std 802.11b-1999
- **802.11c**: Bridge Operation (Completed. Added to IEEE 802.1D)
- **802.11d**: Global Harmonization (PHYs for other countries. Published as IEEE Std 802.11d-2001)
- **802.11e**: Quality of Service. IEEE Std 802.11e-2005
- **802.11F**: Inter-Access Point Protocol (Withdrawn)
- **802.11h**: Dynamic Frequency Selection and transmit power control to satisfy 5GHz band operation in Europe. Published as IEEE Std 802.11h-2003

IEEE 802.11 Activities (Cont)

- **802.11i**: MAC Enhancements for Enhanced Security. Published as IEEE Std 802.11i-2004
- **802.11j**: 4.9-5 GHz operation in Japan. IEEE Std 802.11j-2004
- **802.11k**: Radio Resource Measurement interface to higher layers. Published as IEEE Std 802.11k-2008.
- **802.11m**: Maintenance. Correct editorial and technical issues in 802.11a/b/d/g/h.
- **802.11n**: Enhancements for higher throughput (100+ Mbps). Approved by Revcom Sept 2009
- **802.11p**: Inter-vehicle and vehicle-road side communication at 5.8GHz. Active. Approval expected Nov 2010
- **802.11r**: Fast Roaming. Started July 2003. Published as IEEE Std 802.11r-2008

IEEE 802.11 Activities (Cont)

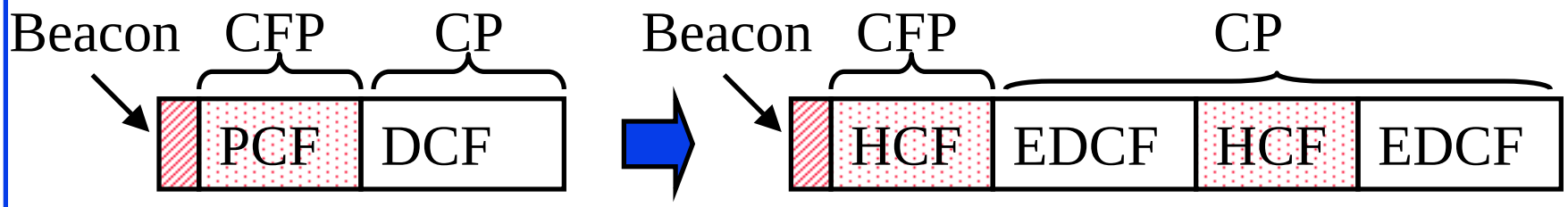
- **802.11s**: ESS Mesh Networks. Active. Expected Jan 2011.
- **802.11T**: Performance Metrics, Active.
- **802.11u**: Inter-working with External Networks. Active. Expected June 2010
- **802.11v**: Wireless Network Management enhancements for interface to upper layers. Extension to 802.11k. Active. Expected June 2010
- **802.11z:** Direct Datalink Setup (DLS) mechanism w Power Save. Active. Expected July 2010
- **802.11aa**, Video Transport Streams, PAR approved 03/27/08, Expected Oct 2011
- **802.11ac**, Very High Throughput <6GHz, PAR approved 09/26/08, Expected Dec 2012
- **802.11ad**, Very High Throughput 60 GHz, PAR approved 12/10/08, Expected Dec 2010

IEEE 802.11 Activities (Cont)

- **802.11ae**, QoS Manangement, PAR approved, 12/09/09, Expected June 2012
- **802.11af**, TV Whitespace, PAR approved 12/09/09, Expected Dec 2012
- Reference: http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

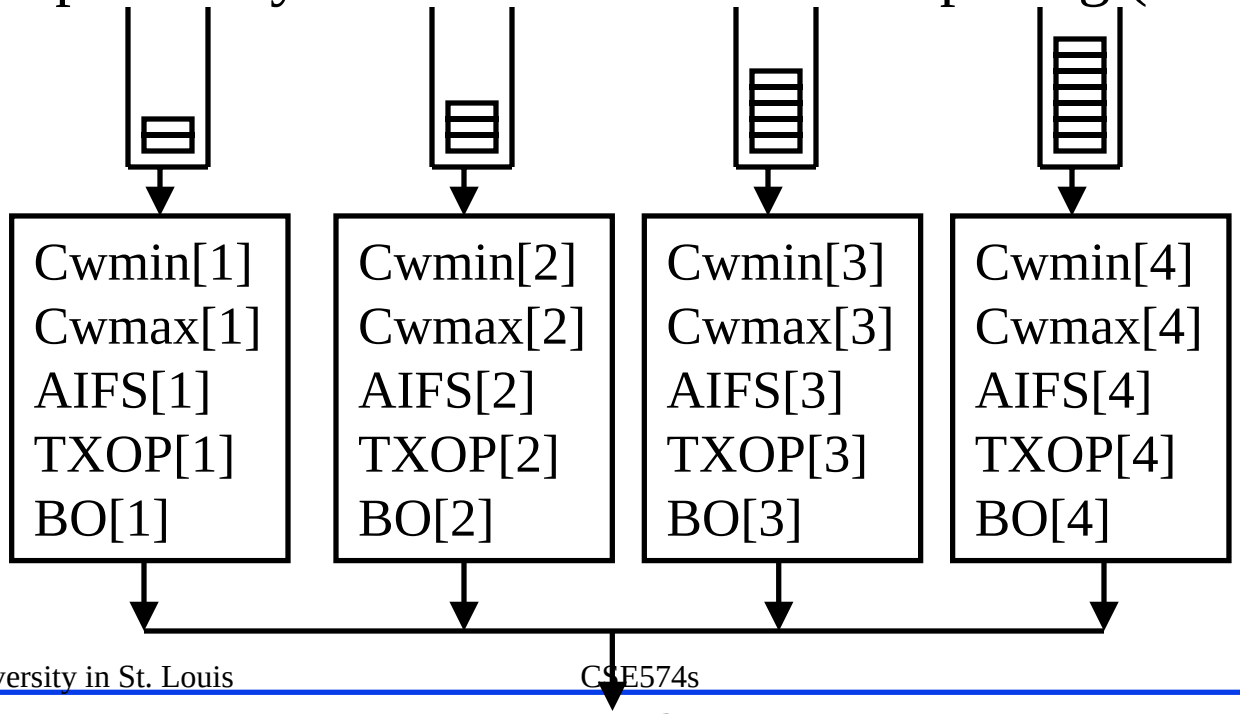
IEEE 802.11e QoS

- Backward compatible:
  $\Rightarrow$ Non-802.11e terminals can receive QoS enabled streams
- New Features:
  1. Hybrid Coordination Function (HCF) w two components
     a. Contention Free Access: Hybrid Polling
     b. Contention-based Access: Enhanced DCF (EDCF)
  2. Direct Link: Traffic sent directly between two stations
  3. Frame bursting and Group Acknowledge
  4. Multiple Priority levels



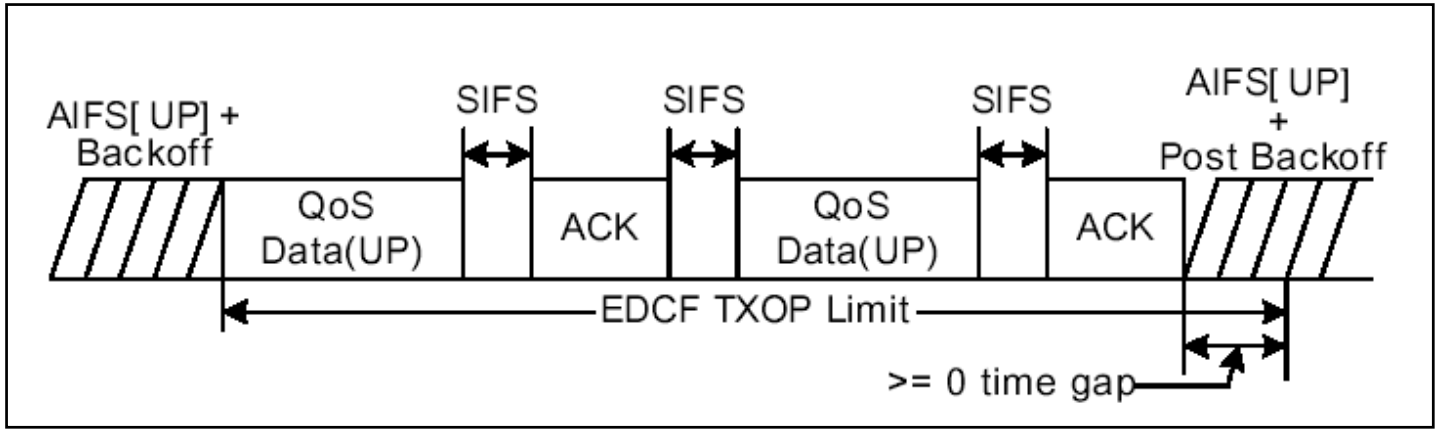
Enhanced DCF

- Up to 8 queues. Each Q gets a different set of four Parameters:
  - CW_{min}/CW_{max}
  - Arbitrated Inter-Frame Spacing (AIFS) = DIFS
  - Transmit Opportunity (TXOP) duration
- DIFS replaced by Arbitrated Inter-frame Spacing (AIFS)



ECDF Bursting

- EDCF parameters announced by access point in beacon frames
- Can not overbook higher priorities ⇒ Need admission control
- EDCF allows multiple frame transmission
- Max time = Transmission Opportunity (TXOP)
- Voice/gaming has high priority but small burst size
- Video/audio has lower priority but large burst size

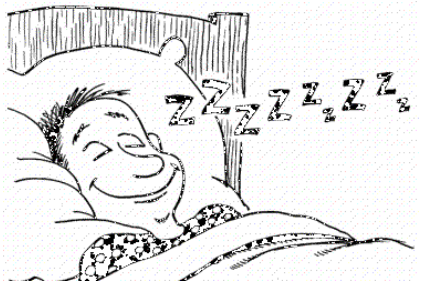


Default EDCA Parameters

Class	CWmin	CWmax	AIFS	TXOP Limit	
				11b	11a/g
Background	aCWmin	aCWmax	7	0	0
Best Effort	aCWmin	aCWmax	3	0	0
Video	(aCWmin+1)/2-1	aCWmin	2	6.016ms	3.008ms
Voice	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264 ms	1.04 ms

- AIFS ⇒ priority order is Voice or video, best effort, background (lowest).
- CWmax ⇒ Voice has higher priority than video
- TXOP
  ⇒ Video is allowed more throughput than voice

Power Management



- Station tells the base station its mode: Power saving (PS) or active
- Mode changed by power mgmt bit in the frame control header.
- All packets destined to stations in PS mode are buffered
- AP broadcasts list of stations with buffered packets in its beacon frames: Traffic Indication Map (TIM)
- SS sends a PS-Poll message to AP, which sends one frame. More bit in the frame header indicates if there are more frames.
- With 802.11e unscheduled Automatic Power Save Delivery (APSD): SS transmits a data or null frame with power saving bit set to 0. AP transmits all buffered frames for SS.
- With Scheduled APSD mode:AP will transmit at pre-negotiated time schedule. No need for polling.
- Hybrid APSD mode: PS-poll for some. Scheduled for other categories

802.11n

- 11n = Next Generation of 802.11
- 4x to 5x faster than 11a/g
  (802.11a/g have 54 Mbps over the air and 25 Mbps to user)
- 64-QAM with 5/6 code rate, 2 spatial streams, 40 MHz channel, 400ns guard interval gives 270 Mbps
- Pre-11n products already available

Belkin


D-Link


Linksys

Major Components of 11n

1. Better OFDM: Higher code rate gives 65 Mbps instead of 54 Mbps
2. Space Division Multiplexing: Up to 4 spatial streams
3. Diversity: More receive antennas than the number of streams. Select the best subset of antennas.
4. Beam Forming: Focus the beam directly on the target antenna
5. MIMO Power Save: Use multiple antennas only when needed
6. Channel Binding: 40 MHz Channels
7. Aggregation: Transmit bursts of multiple data packets
8. Short guard interval (400 ns in place of 800 ns)
9. Reduced Inter-Frame Spacing (2 us)
10. Greenfield Mode: Optionally eliminate support for a/b/g

802.11p: WAVE

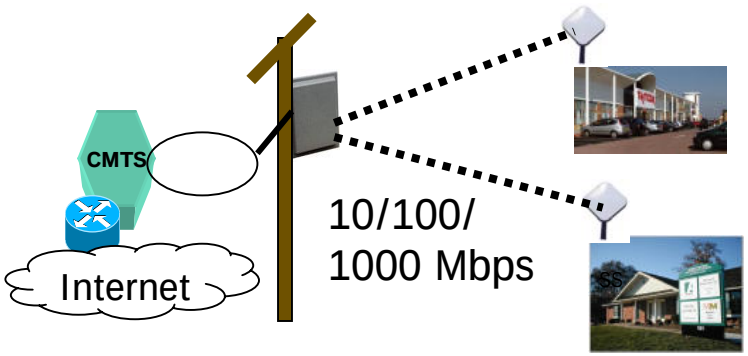
- Wireless Access for Vehicular Environment
- Data exchange between vehicles or between vehicles and road-side infrastructure
- Vehicle safety services, toll collections, commerce transactions
- Up to 1000m at 200 km/h
- Provides lower layers of Dedicated Short Range Communication (DSRC)
- Uses 5 and 10 MHz channels at 5.9 GHz (5.85-5.925 GHz)

802.11r: Fast BSS Transitions

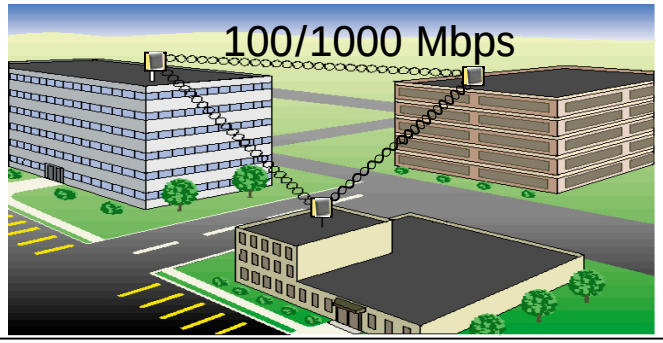
- Important for traffic that needs QoS, e.g., VOIP
- Allows quickly disassociating from one access point and associating with another
- SS can establish QoS and security at the new access point before making a transition

802.11s Mesh Networks: Applications

MSOs/CLEC/Municipal

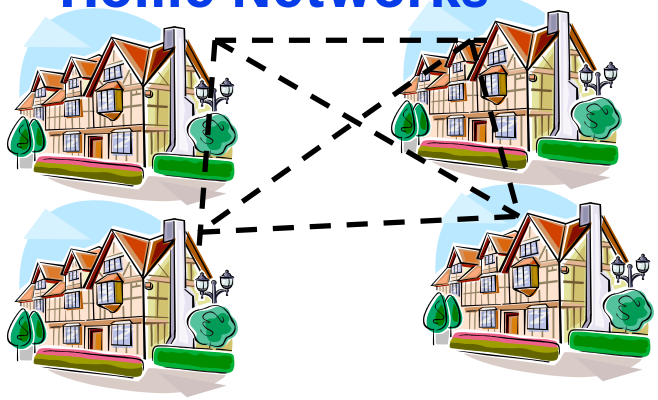


Enterprise Campus



Emergency Response

Home Networks



802.11s: Wireless Mesh Networks

- Security based on 802.11i and push/pull key distribtuion and a mesh KDC (Key distribution center) with fall back to pre-shared keys for small or home networks
- Beacons and Probe/responses to advertise Mesh ID, routing protocol, security capabilities, etc.
- Uses 6-address scheme to accommodate mesh tunneling
- Includes route discovery, route maintenance, route recovery or establishment and mesh routing
- Hybrid wireless mesh protocol (HWMP) for layer 2 routing: combines Tree-based routing and AODV Routing.

802.11T: Wireless Performance Prediction

- Defines test metrics for data, latency sensitive applications and streaming media.
- Throughput and range for data
- Latency, delay jitter, packet loss, admitted calls for latency sensitive applications, e.g., VOIP
- Video quality (throughput, latency, jitter) for streaming media
- Throughput vs path loss, fast BSS transition, receiver sensitivity, association performance

802.11u: Wireless Interworking with External Networks

- Allows network selection: check if the network supports a particular Subscription Service Provider network (SSPN)
- Allows a client multiple credential to select a proper one
- One access point can support multiple SSPNs
- Client can determine inter-working services before association
- Emergency e911 calls

802.11w: Management Frame Protection

- 802.11i does not provide security for management frames, such disassociate, de-authenticate, and broadcast/multicast frames
- Security ⇒ Data integrity, data authenticity, replay protection and data confidentiality
- Without 11w, attacker can forge disassociation
- Broadcast Integrity Protocol (BIP) with AES-128-CMAC (Counter Message Authentication Code)
- Provides replay protection and forgery protection against insider attacks

802.11y Contention Based Protocol

- FCC opened up 3.65-3.7 GHz band for public use in July 2005.
- Mobile SS must receive an enabling signal from an AP before transmitting to avoid interference with FSS and radiolocation services, who are the primary users of 3.65 GHz band
- APs are allowed a peak power of 25W/25MHz
  Mobile clients are allowed 1W/25 MHz
- High power ⇒ Can be used for long range

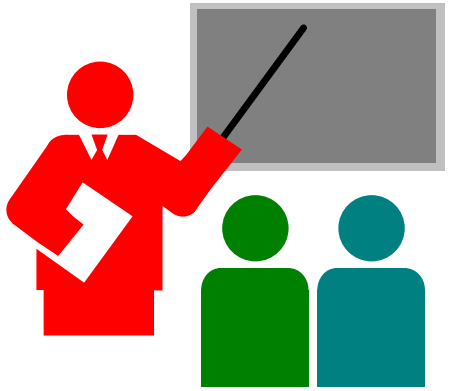
Configuration of APs

- A large number of access points
- Need to configure routing, security, forwarding parameters
- Difficult to reach ⇒ Remote provisioning
- IETF CAPWAP group is working on a common methodology for configuration

References: http://www.ietf.org/dyn/wg/charter/capwap-charter.html

- RFC 3990, "CAPWAP Problem Statement," Feb 2005.
- RFC 4118, "Architecture Taxonomy for CAPWAP," Jun 2005.
- RFC 4564, "Objectives for CAPWAP," July 2006.
- RFC 4565, "Evaluation of Candidate CAPWAP Protocols," July 2006.
- RFC 5415, CAPWAP Protocol Specification, March 2009
- RFC 5416, CAPWAP Protocol Binding for IEEE 802.11, March 2009
- RFC 5417, CAPWAP Access Controller DHCP Option, March 2009
- RFC 5418, CAPWAP Threat Analysis for IEEE 802.11 Deployments, March 2009

Summary



1. 802.11 MAC frames have four 48-bit addresses
2. 802.11e provides better QoS using enhanced DCF and hybrid coordination functions
3. 802.11n improves the throughput by MIMO, channel binding
4. Activities on vehicular communication, fast handover, mesh networks