

18-452/18-750
Wireless Networks and Applications
Lecture 13: Wireless LANs
802.11 Management

Peter Steenkiste

Spring Semester 2017

<http://www.cs.cmu.edu/~prs/wirelessS17/>

Peter A. Steenkiste, CMU

1

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Peter A. Steenkiste, CMU

2

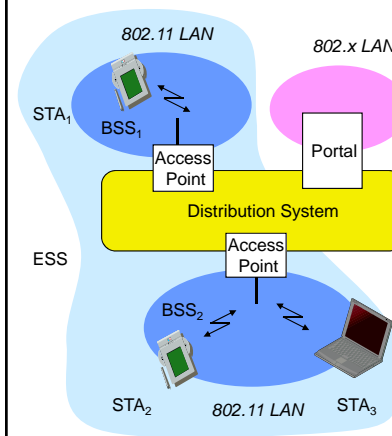
Management and Control Services

- Association management
- Handoff
- Security: authentication and privacy
- Power management
- QoS

Peter A. Steenkiste, CMU

3

802.11: Infrastructure Reminder



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

Peter A. Steenkiste, CMU

4

Service Set Identifier - SSID

- **Mechanism used to segment wireless networks**
 - » Multiple independent wireless networks can coexist in the same location
 - » Effectively the name of the wireless network
- **Each AP is programmed with a SSID that corresponds to its network**
- **Client computer presents correct SSID to access AP**
- **Security Compromises**
 - » AP can be configured to "broadcast" its SSID
 - » Broadcasting can be disabled to improve security
 - » SSID may be shared among users of the wireless segment

Peter A. Steenkiste, CMU

5

Association Management

- **Stations must associate with an AP before they can use the wireless network**
 - » AP must know about them so it can forward packets
 - » Often also must authenticate
- **Association is initiated by the wireless host – involves multiple steps:**
 1. **Scanning:** finding out what access points are available
 2. **Selection:** deciding what AP (or ESS) to use
 3. **Association:** protocol to "sign up" with AP – involves exchange of parameters
 4. **Authentication:** needed to gain access to secure APs – many options possible
- **Disassociation:** station or AP can terminate association

Peter A. Steenkiste, CMU

6

Association Management: Scanning

- **Stations can detect AP using scanning**
- **Passive Scanning:** station simply listens for Beacon and gets info of the BSS
 - » Beacons are sent roughly 10 times per second
 - » Power is saved
- **Active Scanning:** station transmits Probe Request; elicits Probe Response from AP
 - » Saves time + is more thorough
 - » Wait for 10-20 msec for response
- **Scanning all available channels can become very time consuming!**
 - » Especially with passive scanning
 - » Cannot transmit and receive frames during most of that time – not a big problem during initial association

Peter A. Steenkiste, CMU

7

Association Management: Selecting an AP and Joining

- **Selecting a BSS or ESS typically must involve the user**
 - » What networks do you trust? Are you willing to pay?
 - » Can be done automatically based on stated user preferences (e.g., the "automatic" list in Windows)
- **The wireless host selects the AP it will use in an ESS based on vendor-specific algorithm**
 - » Uses the information from the scan
 - » Typically simply joins the AP with the strongest signal
- **Associating with an AP**
 - » Synchronization in Timestamp Field and frequency
 - » Adopt PHY parameters
 - » Other parameters: BSSID, WEP, Beacon Period, etc.

Peter A. Steenkiste, CMU

8

Association Management: Roaming

- **Reassociation:** association is transferred from active AP to a new target AP
 - » Supports mobility in the same ESS – layer 2 roaming
- **Reassociation is initiated by wireless host based on vendor specific algorithms**
 - » Implemented using an Association Request Frame that is sent to the new AP
 - » New AP accepts or rejects the request using an Association Response Frame
- **Coordination between APs is defined in 802.11f**
 - » Allows forwarding of frames in multi-vendor networks
 - » Inter-AP authentication and discovery typically coordinated using a RADIUS server
 - » “Fast roaming” support (802.11r) also streamlines authentication and QoS, e.g. for VoIP

Peter A. Steenkiste, CMU

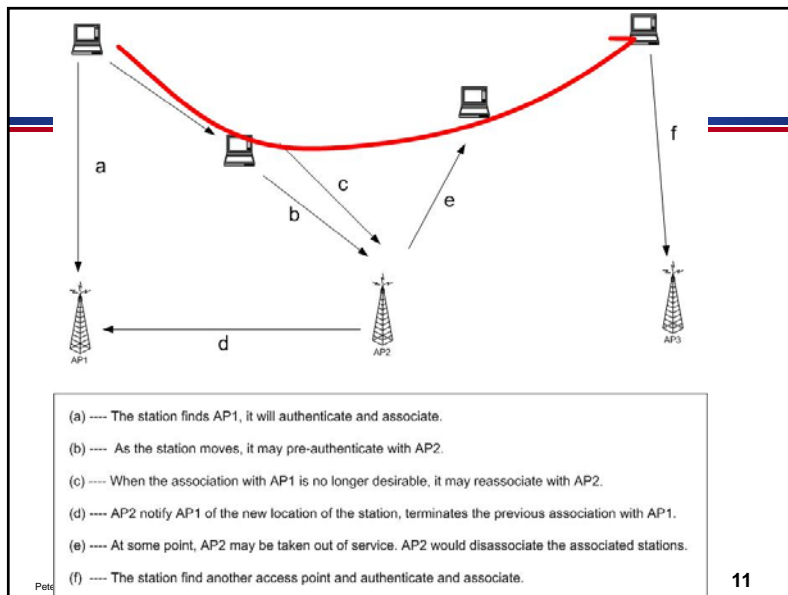
9

Association Management: Reassociation Algorithms

- **Failure driven:** only try to reassociate after connection to current AP is lost
 - » Typically efficient for stationary clients since it not common that the best AP changes during a session
 - » Mostly useful for nomadic clients
 - » Can be very disruptive for mobile devices
- **Proactive reassociation:** periodically try to find an AP with a stronger signal
 - » Tricky part: cannot communicate while scanning other channels
 - » Trick: user power save mode to “hold” messages
 - » Throughput during scanning is still affected though
 - Mostly affects latency sensitive applications

Peter A. Steenkiste, CMU

10



Peter A. Steenkiste, CMU

11

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Peter A. Steenkiste, CMU

12

WLAN Security Requirements

- **Authentication:** only allow authorized stations to associate with and use the AP
- **Confidentiality:** hide the contents of traffic from unauthorized parties
- **Integrity:** make sure traffic contents is not modified while in transit

Peter A. Steenkiste, CMU

13

WLAN Security Exploits

- **Insertion attacks: unauthorized Clients or AP**
 - » Client: reuse MAC or IP address –free service on “secured” APs
 - » AP: impersonate an AP, e.g., use well known name
- **Interception and unauthorized monitoring**
 - » Packet Analysis by “sniffing” – listening to all traffic
- **Brute Force Attacks Against AP Passwords**
 - » Dictionary Attacks Against SSID
- **Encryption Attacks**
 - » Exploit known weaknesses of WEP
- **Misconfigurations, e.g., use default password**
- **Jamming – denial of service**
 - » Cordless phones, baby monitors, leaky microwave oven, etc.

Peter A. Steenkiste, CMU

14

Security in 802.11b

- **WEP: Wired Equivalent Privacy**
 - » Achieve privacy similar to that on LAN through encryption
 - » Intended to provide both privacy and integrity
 - » RC4 and CRC32
 - » Has known vulnerabilities
- **WPA: Wi-Fi Protected Access**
 - » Larger, dynamically changed keys
- **802.1x: port-based authentication for LANs**
 - » Port-based authentication for LANs
- **802.11i (WPA2)**
 - » Builds on WPA
 - » Uses AES for encryption

Peter A. Steenkiste, CMU

15

MAC Filtering

- **Each client is identified by its 802.11 Mac Address**
- **Each AP can be programmed with the set of MAC addresses it accepts (“white list”)**
- **Combine this filtering with the AP’s SSID**
- **Very simple solution**
 - » Some overhead to maintain list of MAC addresses
- **But it is possible to forge MAC addresses ...**
 - » Unauthorized client can “borrow” the MAC address of an authenticated client
 - » Built in firewall will discard unexpected packets

Peter A. Steenkiste, CMU

16

Wired Equivalent Privacy WEP

- Original standard for WiFi security
- Very weak standard: key could be cracked with a couple of hours of computing (much faster today)
 - » Too much information is transmitted in the clear
 - » No protocol for encryption key distribution
 - » Clever optimizations can reduce time to minutes
- All data then becomes vulnerable to interception
 - » WEP typically uses a single shared key for all stations
- The CRC32 check is also vulnerable so that the data could be altered as well
 - » Can make changes without even decrypting!
- 128-bit WEP encryption is recommended

Peter A. Steenkiste, CMU

17

Port-based Authentication

- 802.1x is the IEEE standard for port-based authentication
- Users get a username/password to access the access point
- Was originally defined for switches but extended to APs
- Can be used to bootstrap other security mechanisms
 - » Effectively creating a session

Peter A. Steenkiste, CMU

18

Wi-Fi Protected Access WPA

- Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published
 - » Uses a different Message Integrity Check
 - » Encryption still based on RC4, but uses 176 bit key (48bit IV) and keys are changed periodically
 - » Also frame counter in MIC to prevent replay attacks.
- Can be used with 802.1x authentication (optional)
 - » It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
 - » Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- 802.11i is a “permanent” security fix
 - » Builds on the interim WPA standard (i.e. WPA2)
 - » Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
 - » Better key management and data integrity
 - » Uses 802.1x for authentication.

Peter A. Steenkiste, CMU

19

Authentication in WLAN Hotspots

- Upon association with the AP, only authentication traffic can pass through, as defined by IEEE 802.1x

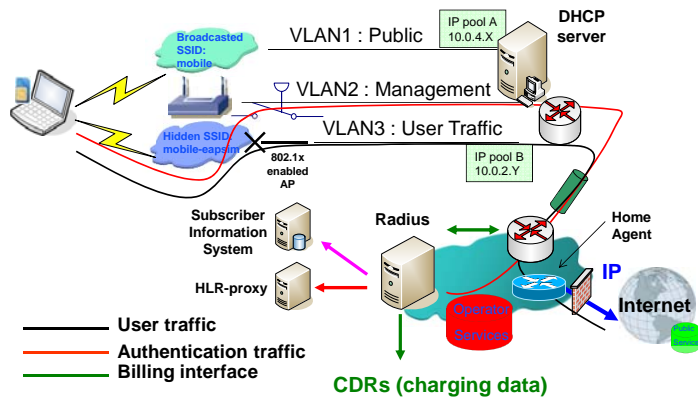


- The protocol used to transport authentication traffic is the Extensible Authentication Protocol (EAP - RFC3748)

Peter A. Steenkiste, CMU

20

Dual SSID Approach



Peter A. Steenkiste, CMU

21

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power management
- 802.11*: b/g/a, h, e, n

Peter A. Steenkiste, CMU

22

Power Management

- Goal is to enhance battery life of the stations
- Idle receive state dominates LAN adapter power consumption over time
- Allow stations to power off their NIC while still maintaining an active session
- Different protocols are used for infrastructure and independent BSS
 - » Our focus is on infrastructure mode

Peter A. Steenkiste, CMU

23

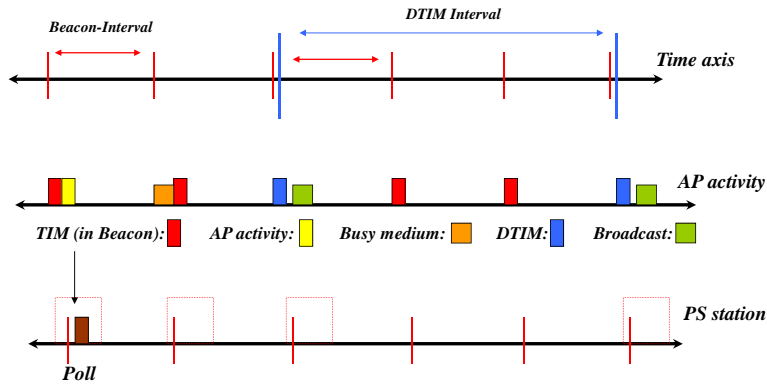
Power Management Approach

- Idle station to go to sleep
- AP keeps track of stations in Power Savings mode and buffers their packets
 - » Traffic Indication Map (TIM) is included in beacons to inform which power-save stations have packets waiting at the AP
- Power Saving stations wake up periodically and listen for beacons
 - » If they have data waiting, they can send a PS-Poll to request that the AP sends their packets
- TSF assures AP and stations are synchronized
 - » Synchronizes clocks of the nodes in the BSS
- Broadcast/multicast frames are also buffered at AP
 - » Sent after beacons that includes Delivery Traffic Indication Map (DTIM)
 - » AP controls DTIM interval

Peter A. Steenkiste, CMU

24

Infrastructure Power Management Operation



Peter A. Steenkiste, CMU

25

Some IEEE 802.11 Standards

- » IEEE 802.11a
 - PHY Standard : 8 channels : up to 54 Mbps : some deployment
- » IEEE 802.11b
 - PHY Standard : 3 channels : up to 11 Mbps : widely deployed.
- » IEEE 802.11d
 - MAC Standard : support for multiple regulatory domains (countries)
- » IEEE 802.11e
 - MAC Standard : QoS support : supported by many vendors
- » IEEE 802.11f
 - Inter-Access Point Protocol : deployed
- » IEEE 802.11g
 - PHY Standard : 3 channels : OFDM and PBCC : widely deployed (as b/g)
- » IEEE 802.11h
 - Suppl. MAC Standard: spectrum managed 802.11a (TPC, DFS): standard
- » IEEE 802.11i
 - Suppl. MAC Standard: Alternative WEP : standard
- » IEEE 802.11n
 - MAC Standard: MIMO : standardization expected late 2008

Peter A. Steenkiste, CMU

26

IEEE 802.11 Family

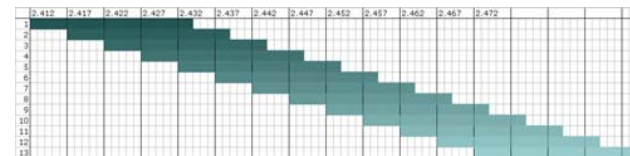
Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	600 Mbps	~50 m

Peter A. Steenkiste, CMU

27

802.11b Channels

- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22MHz
- Significant overlap
- Non-overlapping channels are 1, 6 and 11



Peter A. Steenkiste, CMU

28

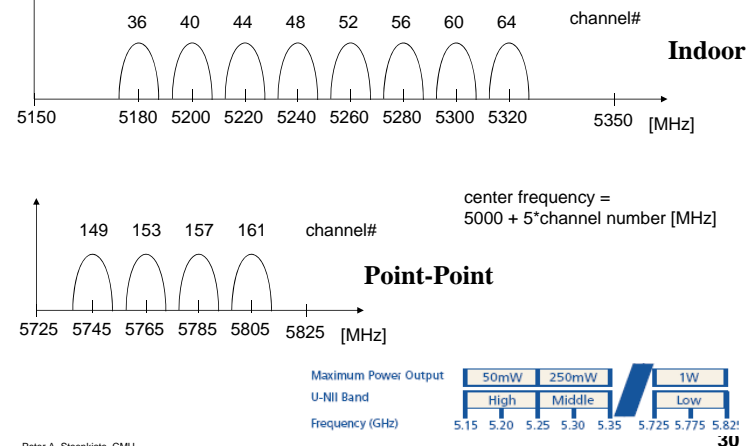
802.11b Physical Layer

- **FHSS (legacy)**
 - » 2 & 4 GFSK
 - » Using one of 78 hop sequences, hop to a new 1MHz channel (out of the total of 79 channels) at least every 400microseconds
- **DSSS (802.11b)**
 - » DBPSK & DQPSK
 - » Uses one of 11 overlapping channels (22 MHz)
 - » 1 and 2 Mbps: multiply the data by an 11-chip spreading code (Barker sequence)
 - » 5.5 and 11 Mbps: uses Complementary Code Keying (CKK) to generate spreading sequences that support the higher data rates
 - Spreading code is calculated based on the data bits

Peter A. Steenkiste, CMU

29

802.11a Physical Channels

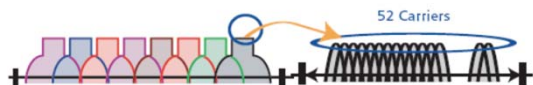


Peter A. Steenkiste, CMU

30

802.11a Modulation

- Use OFDM to divide each physical channel (20 MHz) into 52 subcarriers (20M/64=312.5 KHz each)
 - » 48 data, 4 pilot



- **Adaptive modulation**
 - » BPSK: 6, 9 Mbps
 - » QPSK: 12, 18 Mbps
 - » 16-QAM: 24, 36 Mbps
 - » 64-QAM: 48, 54 Mbps

Peter A. Steenkiste, CMU

31

802.11a Discussion

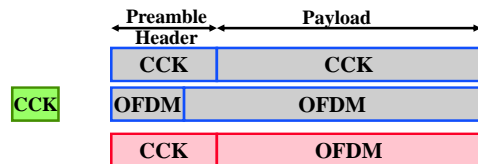
- Uses OFDM in the 5.2 and 5.7 GHz bands
- What are the benefits of 802.11a compared with 802.11b?
 - » Greater bandwidth (up to 54Mb)
 - 54, 48, 36, 24, 18, 12, 9 and 6 Mbs
 - » Less potential interference (5GHz)
 - » More non-overlapping channels
- But does not provide interoperability with 802.11b, as 802.11g does

Peter A. Steenkiste, CMU

32

Going Faster: 802.11g

- 802.11g basically extends of 802.11b for higher rates – effectively 802.11a at 2.4 GHz
 - » Use the same technology DSSS/CCK for old rates (1,2, 5.5, 11)
 - » Uses 802.11a OFDM technology for new rates (6 Mbs and up)
 - » Using OFDM makes it easier to build 802.11a/g cards
- But it creates an interoperability problem since 802.11b cards cannot interpret OFDM signals
 - » Solutions: send CTS using CCK before OFDM packets in hybrid environments, or use (optional) hybrid packet format



Peter A. Steenkiste, CMU

33