

CS 439: Wireless Networking

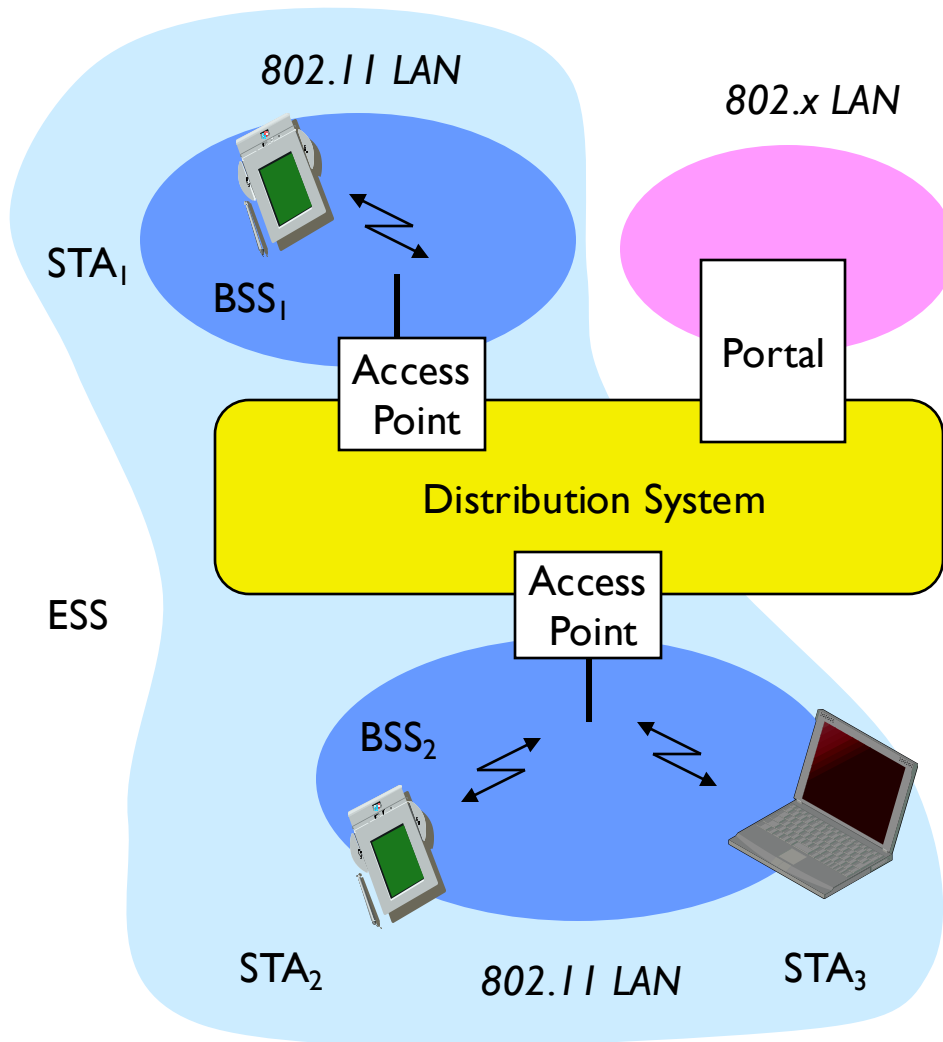
MAC Layer – Management

Management and Control Services

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



802.11: Infrastructure



- ▶ **Station (STA)**
 - ▶ Terminal with access 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

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



Association Management

- ▶ Stations must associate with an AP before using network
 - ▶ AP must know about them so it can forward packets
 - ▶ Often also must authenticate
- ▶ Initiated by the wireless host
 - ▶ Scanning
 - ▶ Finding out what access points are available
 - ▶ Selection
 - ▶ Deciding what AP (or ESS) to use
 - ▶ Association
 - ▶ Protocol to “sign up” with AP – involves exchange of parameters
 - ▶ Authentication
 - ▶ Needed to gain access to secure APs – many options possible
- ▶ Disassociation
 - ▶ Station or AP can terminate association

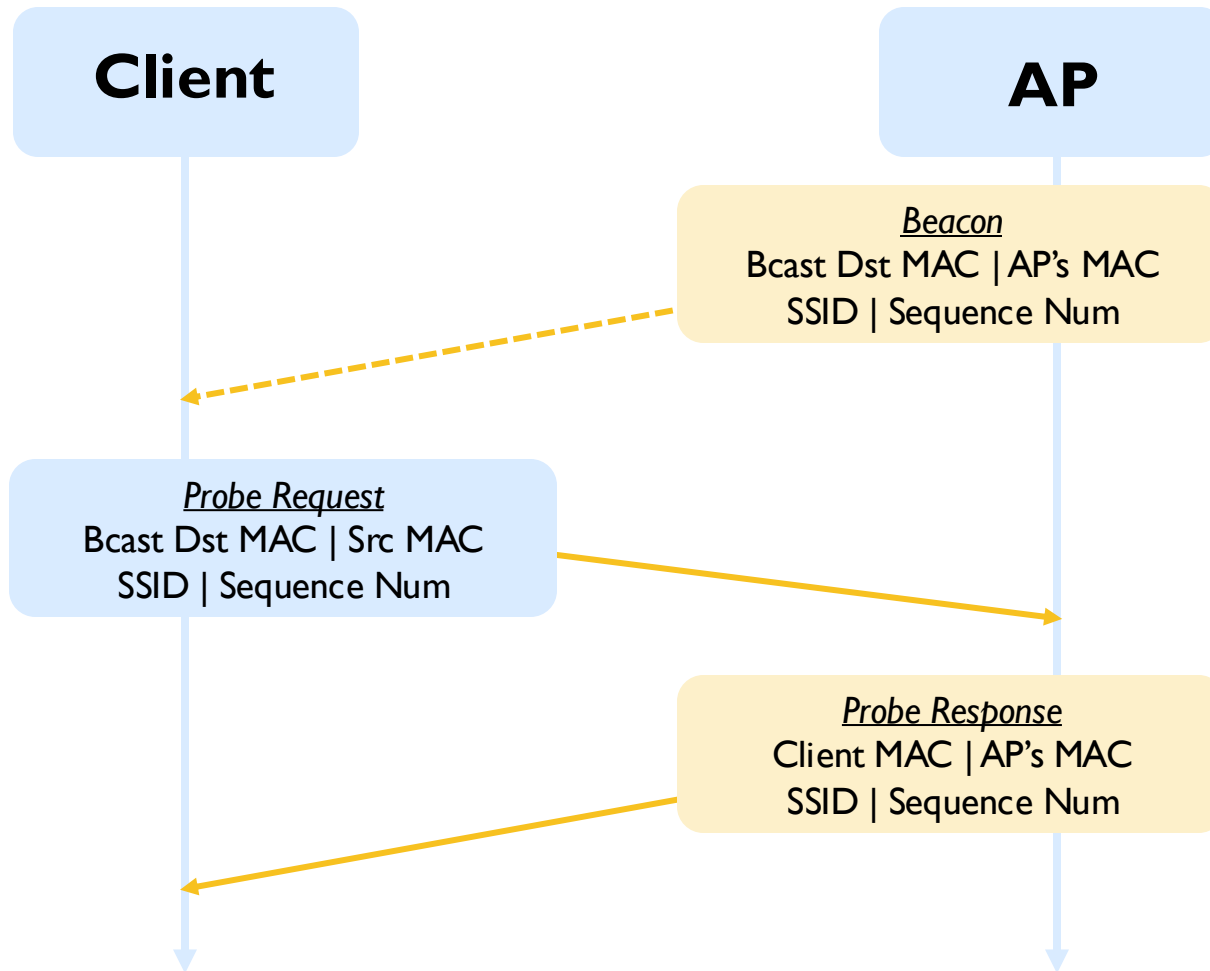


Association Management: Scanning

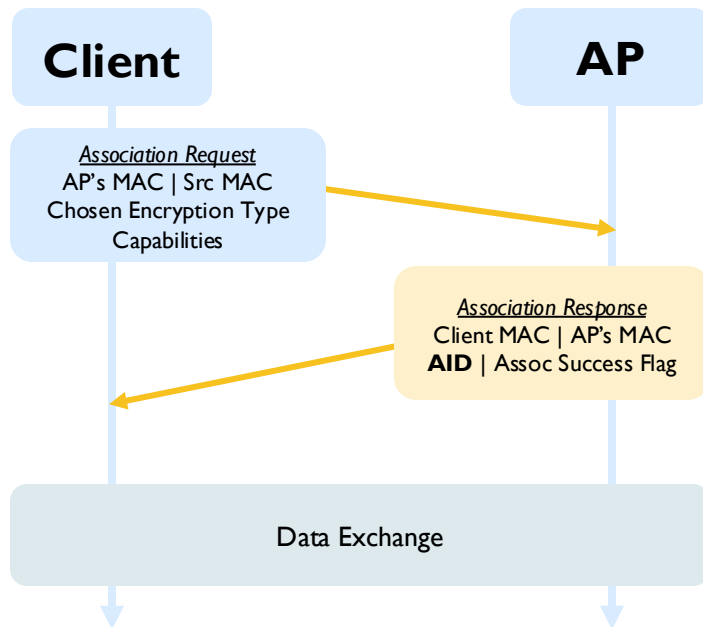
- ▶ Stations can detect AP based by scanning
- ▶ Passive Scanning
 - ▶ Station simply listens for Beacon and gets info of the BSS
 - ▶ Beacons are sent roughly 10 times per second
 - ▶ Power is saved
- ▶ Active Scanning
 - ▶ Station transmits Probe Request; elicits Probe Response from AP
 - ▶ Saves time + 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



802.11 Network Discovery



802.11 Association Process



- ▶ Devices must associate to APs
- ▶ After network discovery
 - ▶ Scan for nearby networks
 - ▶ Find APs' SSIDs and MAC addresses
 - ▶ Ideally choose AP with strongest signal
- ▶ Get IP address from DHCP

Association Management: Selecting an AP and Joining

- ▶ **Selecting a BSS or ESS typically involves 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.



Association Management: Roaming

▶ Reassociation

- ▶ Association is transferred from active AP to a new target AP
 - ▶ Supports mobility in the same ESS – layer 2 roaming
- ▶ 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



High Density WLANs



- ▶ **Stadiums, arenas, and ballparks**
- ▶ **Concert halls and amphitheaters**
- ▶ **Convention center meeting halls**
- ▶ **Lecture halls and auditoriums**
- ▶ **Press areas at public events**
- ▶ **Airport concourses**

High Density Networks



Characteristics of Dense Networks

- More neighbors
- Frequent traffic
- Redundancy

Wireless

- Shared medium
- Limited energy resources

High contention



Dense WLANs



**AP provides good connectivity
when number of devices < 50**



Number of devices > 500

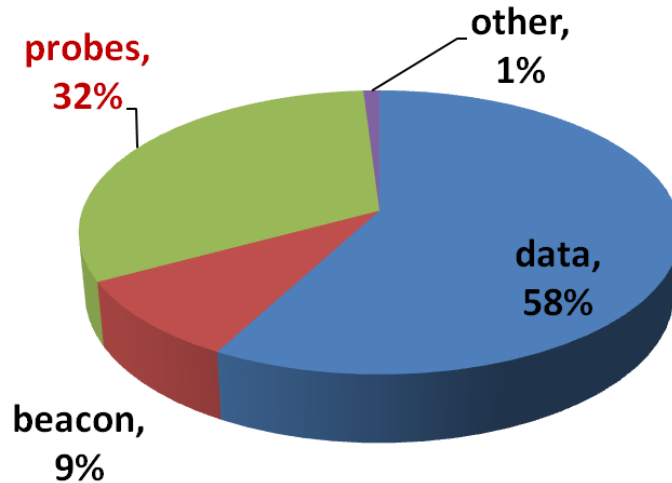
**Co-channel interference limits the
max. number of APs to 3**

All APs are overloaded

User Traces

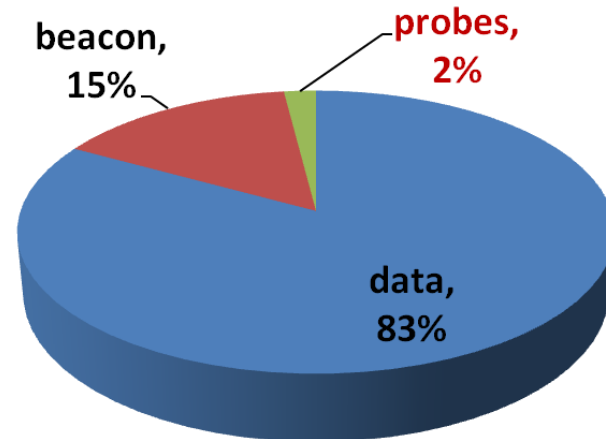
Busy Session

- 824 devices
- 2 APs – channel 6 & 11



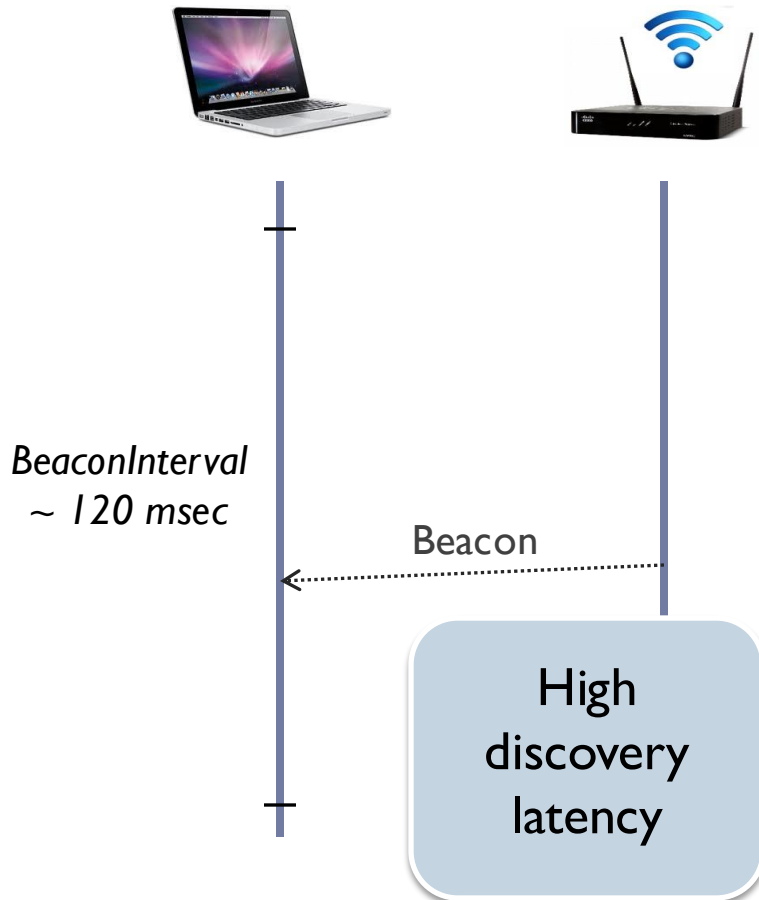
Moderate Session

- 62 devices
- 1 AP – channel 6



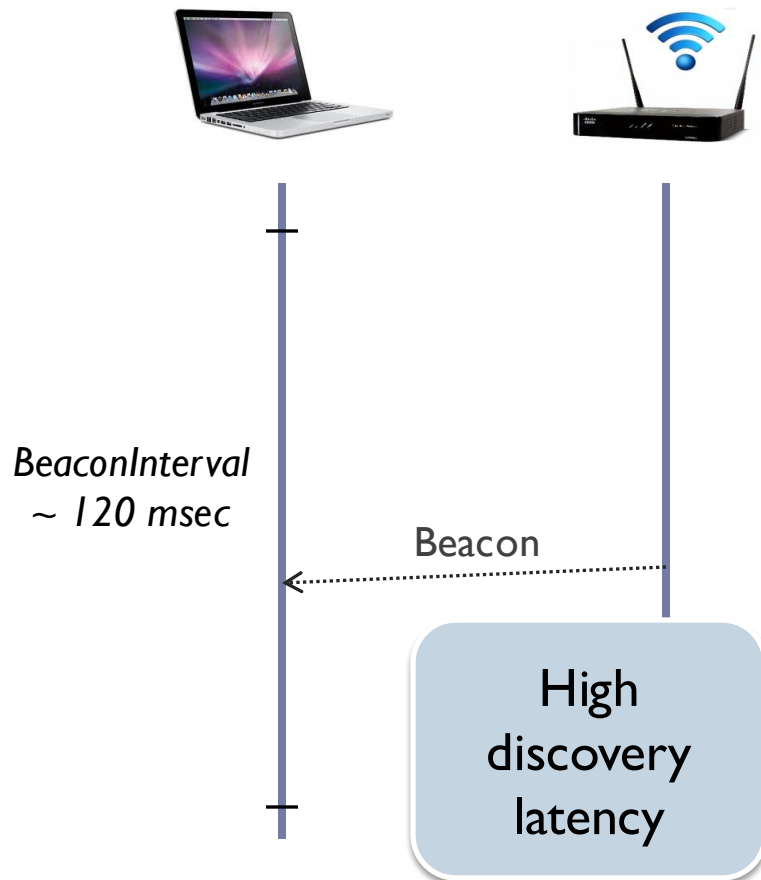
AP Discovery in IEEE standards

Passive Scan

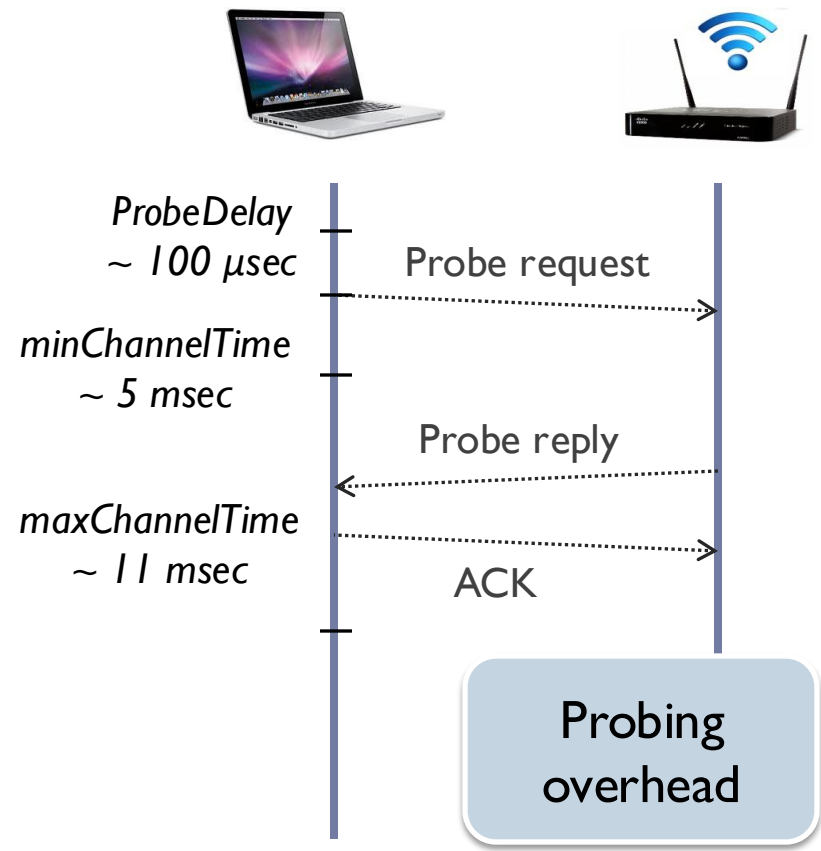


AP Discovery in IEEE standards

Passive Scan



Active Scan



AP Discovery in Device Drivers

Hybrid Scan



Passive Scan

Beacon



Targeted Active Scan

Probe request
for **IllinoisNet**



Probe request
for **Eduroam**



Broadcast Active Scan

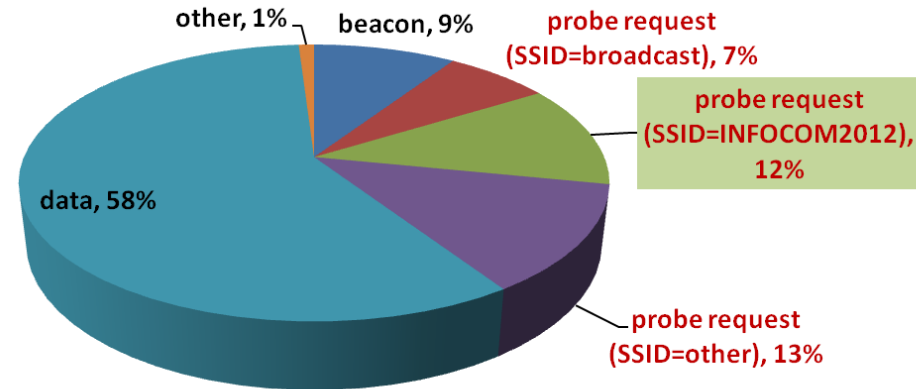
Probe request
for **ALL**



Probe reply



ACK



Busy Traces

Even more
probing overhead

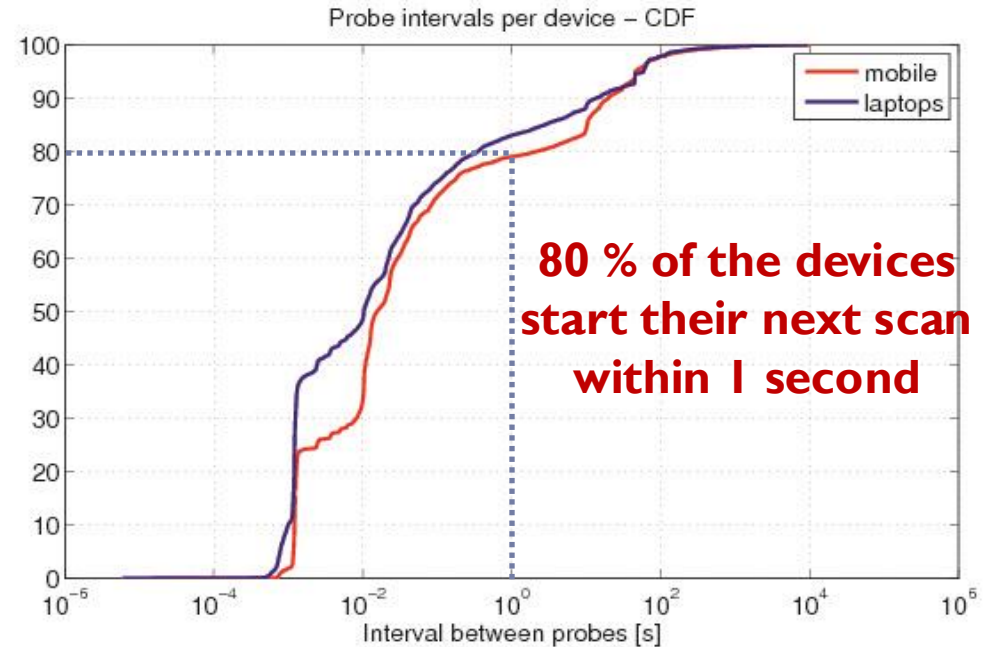
Probe Storms in Busy Traces



Laptops ~ 569
Avg. Probes ~ 227



Smartphones
& tablets ~ 255
Avg. Probes ~ 373



Packet retransmissions

High contention

AP scanning triggered

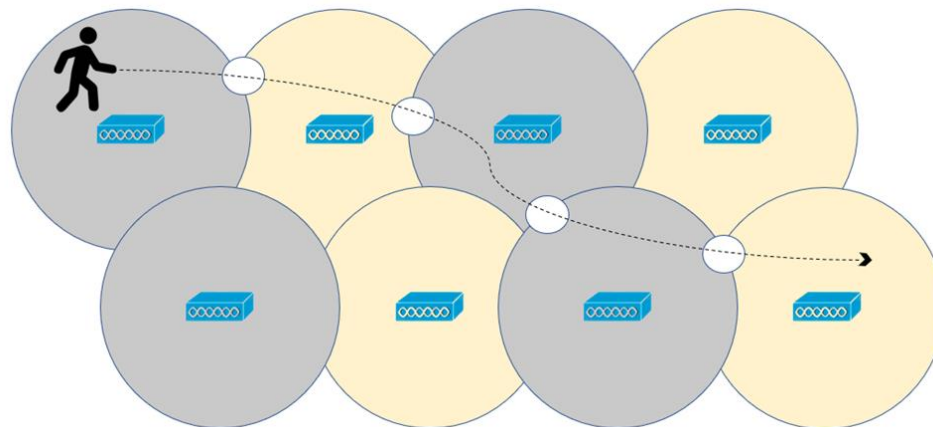
More probing overhead

ALL devices experience poor channel conditions

Association Management: Reassociation Algorithms

► Failure driven

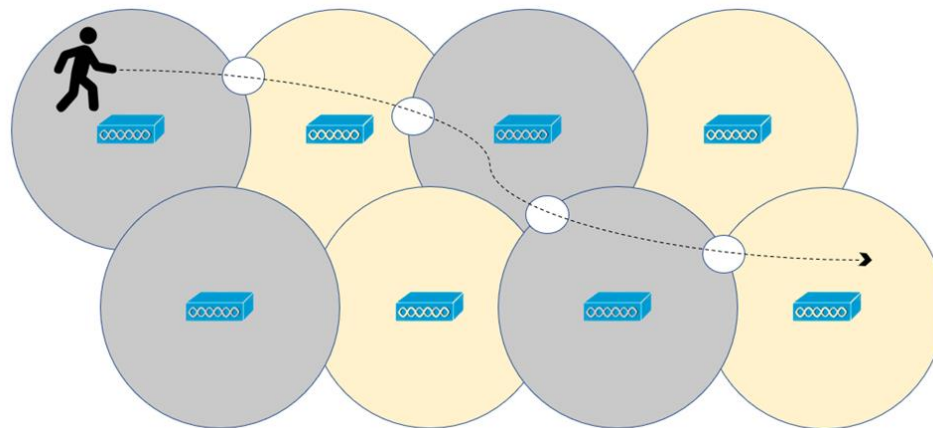
- Only try to reassociate after connection to current AP is lost
 - Low overhead for stationary clients
 - Best AP stable during a session
 - Mostly useful for nomadic clients
 - Can be very disruptive for mobile devices



Association Management: Reassociation Algorithms

▶ Proactive reassociation

- ▶ Periodically try to find an AP with a stronger signal
 - ▶ Cannot communicate while scanning other channels
 - ▶ Trick: user power save mode to “hold” messages
 - ▶ Throughput during scanning is still affected
 - Mostly affects latency sensitive applications



Fast Roaming: Why Basic Reassociation Isn't Enough

- ▶ **The reassociation algorithms just covered still leave a gap in practice**
 - ▶ A client typically only starts looking for a new AP once its current link has already degraded
 - ▶ Scanning, selecting, and reassociating takes long enough to noticeably interrupt a VoIP call or video stream



Fast Roaming: Why Basic Reassociation Isn't Enough

- ▶ Three amendments work together to close that gap
 - ▶ 802.11k: tells the client where to look
 - ▶ 802.11v: lets the network tell the client when and where to roam
 - ▶ 802.11r: makes the actual handoff fast enough to not be noticed
- ▶ Collectively known as the fast/seamless roaming stack - standard in enterprise Wi-Fi today



► Fast Roaming

► Pre-authentication

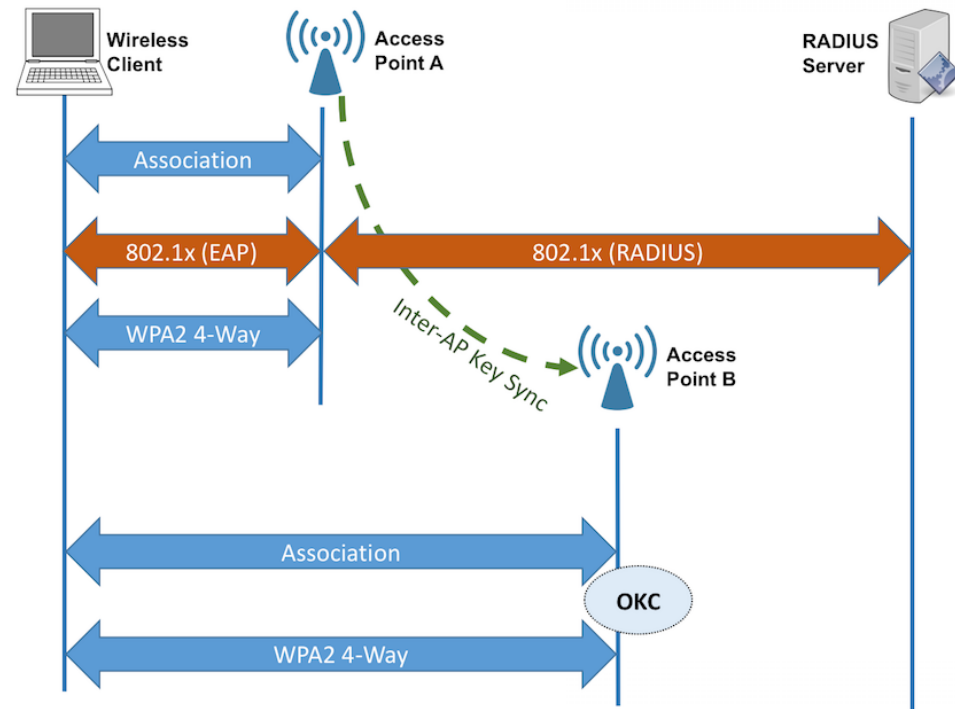
- Authenticate with a new access point before the actual handover
- Reduces time to establish a connection

► Pairwise Master Key (PMK) Caching

- Store and reuse user's connection cryptographic keys
- Faster reauthentication when switching between access points

► Opportunistic Key Caching

- Cache keys for potential future use
- Anticipate handovers and reduce authentication time



IEEE 802.11k: Radio Resource Management

- ▶ Solves the "blind scanning" problem
- ▶ Neighbor Reports
 - ▶ Current AP gives client list of nearby APs on request - channel, BSSID, capabilities
 - ▶ Client can go directly to promising candidates instead of scanning every channel
- ▶ Also standardizes measurement requests
 - ▶ Clients can report link quality, channel load, and noise back to the AP or to each other
 - ▶ Gives the network visibility it needs for 802.11v to make good steering decisions



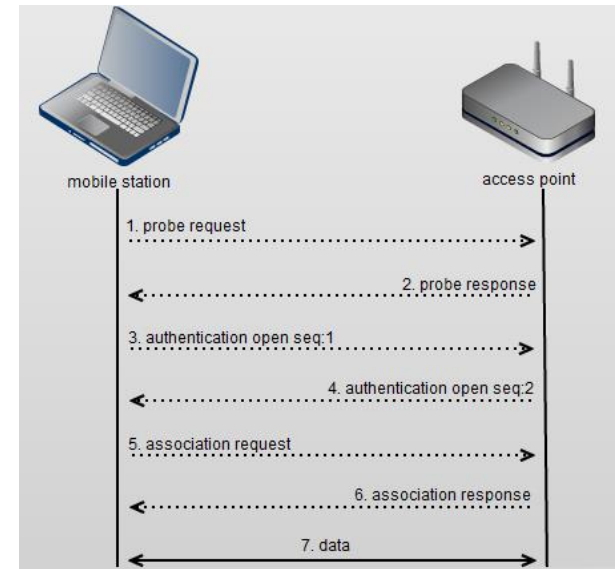
IEEE 802.11v: Wireless Network Management

- ▶ Network actively participates in roaming
- ▶ BSS Transition Management (BTM)
 - ▶ The AP can send a BTM Request suggesting - or in some cases requiring - that a client move to a specific AP
 - ▶ Used for load balancing (nudging clients off a congested AP) and for coverage-based steering
- ▶ Why this matters
 - ▶ Without 802.11v, roaming decisions are entirely client-side - the network has no way to correct a client that's "sticky" on a weak AP



IEEE 802.11r: Fast BSS Transition (FT)

- ▶ Makes the handoff itself fast, once the client knows where it's going
 - ▶ WPA2/WPA3 handoff re-runs full 4-way handshake with the new AP - authentication, key derivation, all before data can flow again
 - ▶ That gap is long enough to drop a VoIP call or stall a video stream



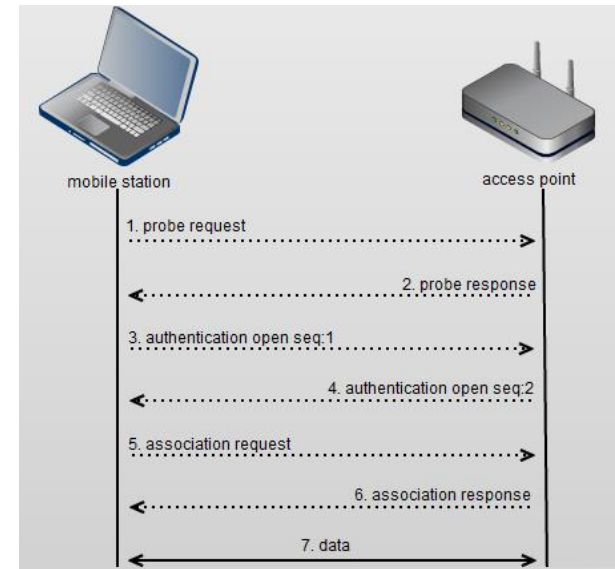
IEEE 802.11r: Fast BSS Transition (FT)

- ▶ **Cryptographic keys**
 - ▶ Pre-computed and cached across APs in the same mobility domain
- ▶ **Over-the-Air FT**
 - ▶ Client authenticates directly with the target AP before switching
- ▶ **Over-the-DS FT**
 - ▶ Client authenticates with the target AP through the current AP first
- ▶ **Either way, the handoff itself becomes a single exchange instead of a full re-authentication**



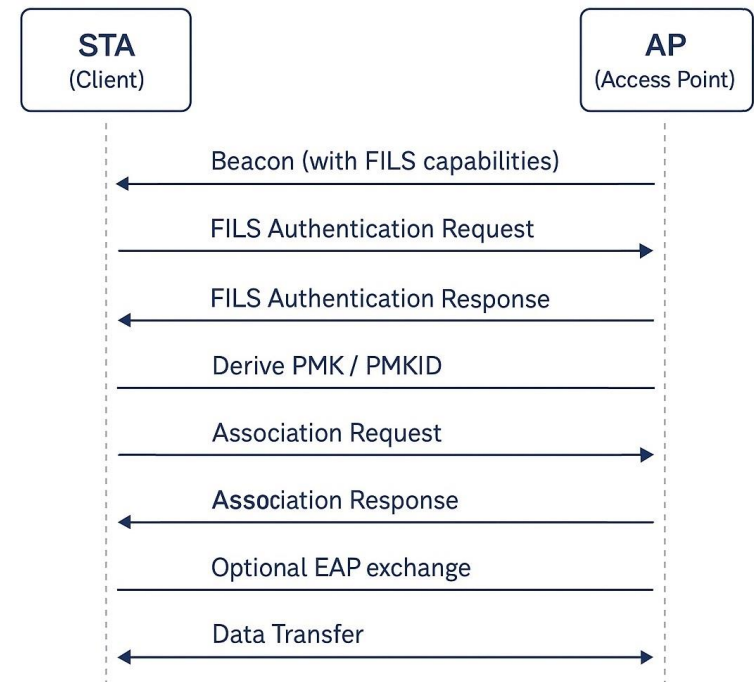
IEEE 802.11ai: Fast Initial Link Setup (FILS)

- ▶ Targets the same latency problem for the very first connection
- ▶ Standard association + authentication (especially with WPA2/WPA3) can take several round trips before a client gets its first data frame through



IEEE 802.11ai: Fast Initial Link Setup (FILS)

- ▶ **FILS approach**
 - ▶ Combines discovery, authentication, and association into a reduced number of frame exchanges
 - ▶ Cuts initial connection time from hundreds of milliseconds to tens of milliseconds
- ▶ Useful anywhere fast handoff matters but the client isn't already associated - dense public Wi-Fi, transit Wi-Fi



DPP and Hotspot 2.0

- ▶ **Wi-Fi Easy Connect (DPP - Device Provisioning Protocol)**
 - ▶ Replaces typing a PSK with scanning a QR code or tapping an NFC tag to onboard a device
 - ▶ No password to leak, no probe-heavy trial-and-error to join a network
- ▶ **802.11u / Hotspot 2.0 (Passpoint)**
 - ▶ Lets a client automatically discover and authenticate to a carrier or roaming-partner network without ever seeing an SSID list
 - ▶ Advertises network type, roaming consortium, and required credentials before association - the client picks the right network on its own
 - ▶ What makes carrier Wi-Fi calling and automatic cellular-to-Wi-Fi offload work seamlessly

