CS 439: Wireless Networking
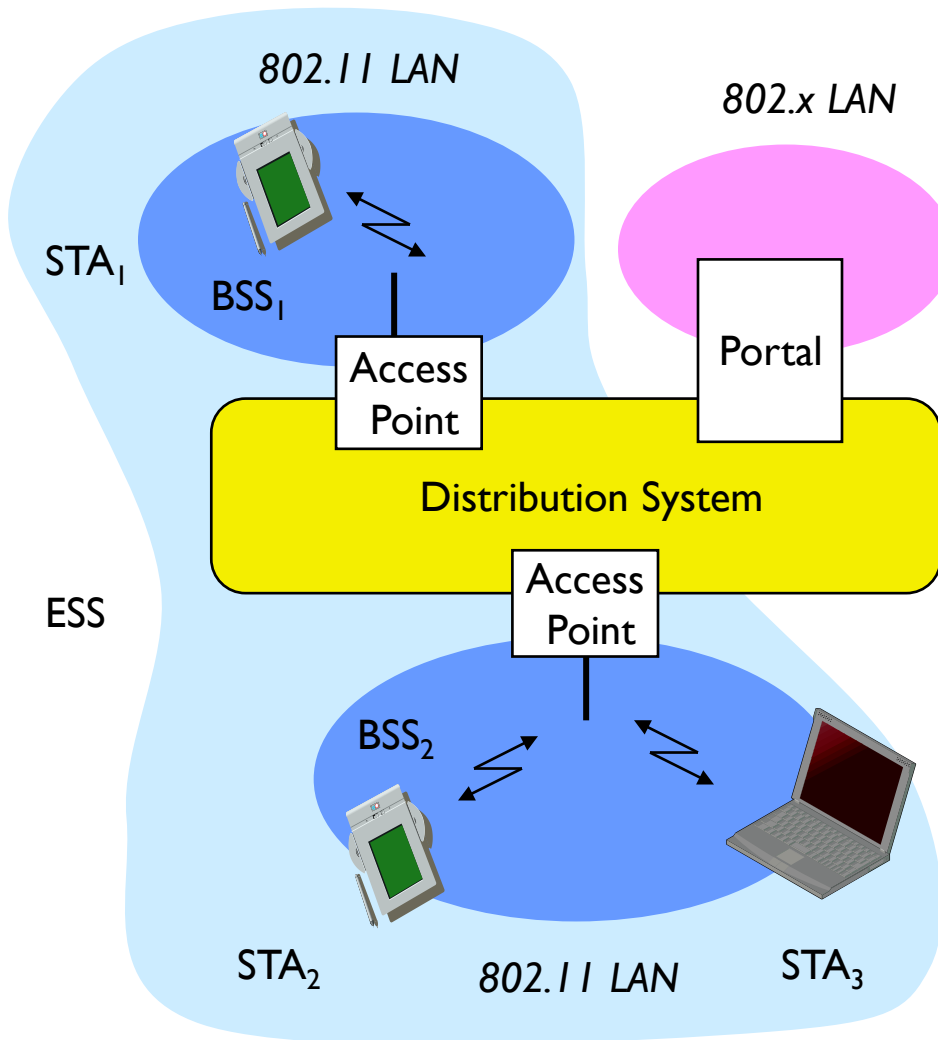
MAC Layer – Management

Management and Control Services

▸ Association management

▸ Handoff

▸ Security: authentication and privacy

▸ Power management

▸ QoS

802.11: Infrastructure

802.11 LAN

802.x LAN

STA$_1$

BSS$_1$

Access Point

Portal

Distribution System

ESS

Access Point

BSS$_2$

STA$_2$

802.11 LAN

STA$_3$

▸ 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

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

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

Making Dense Networks work for You

High Density WLANs

FREE
Wi Fi

- **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

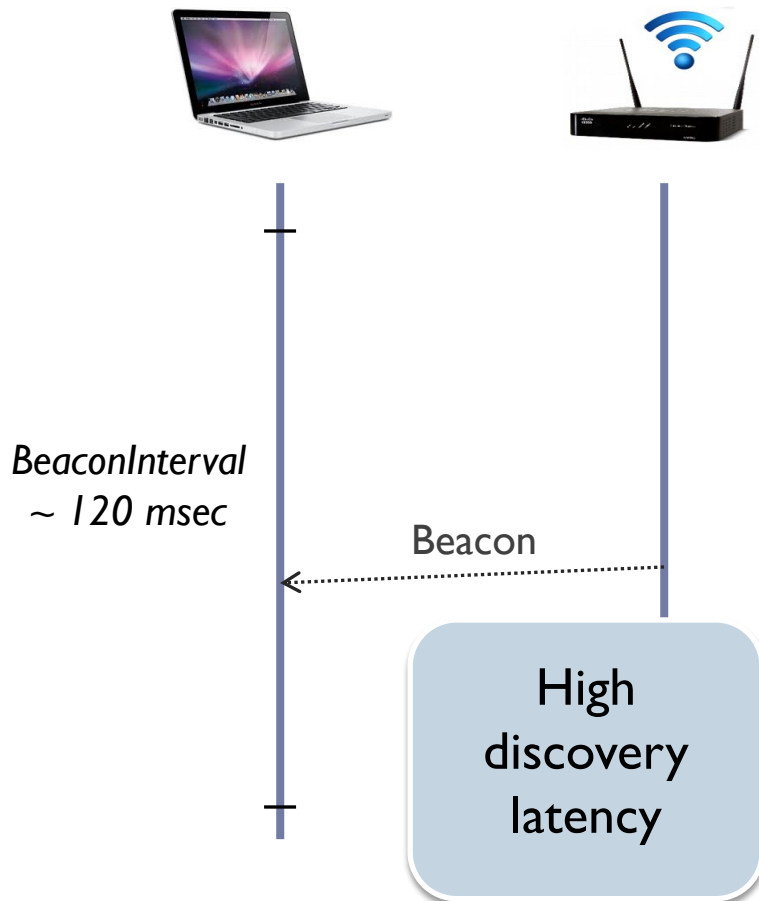# User Traces

Busy Session

- 824 devices
- 2 APs – channel 6 & 11
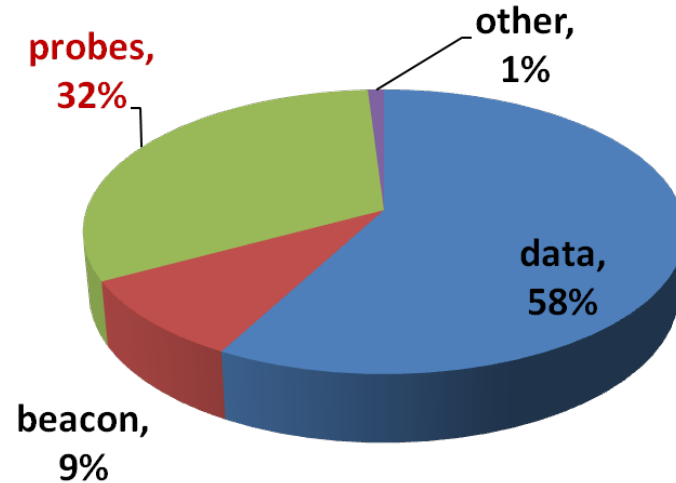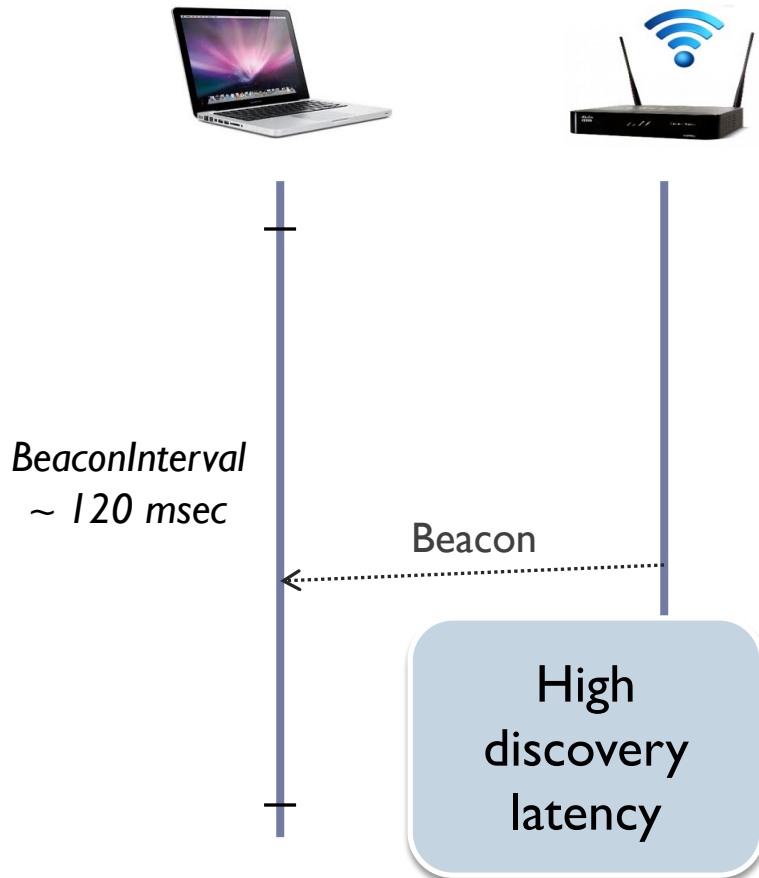

Moderate Session

- 62 devices
- 1 AP – channel 6
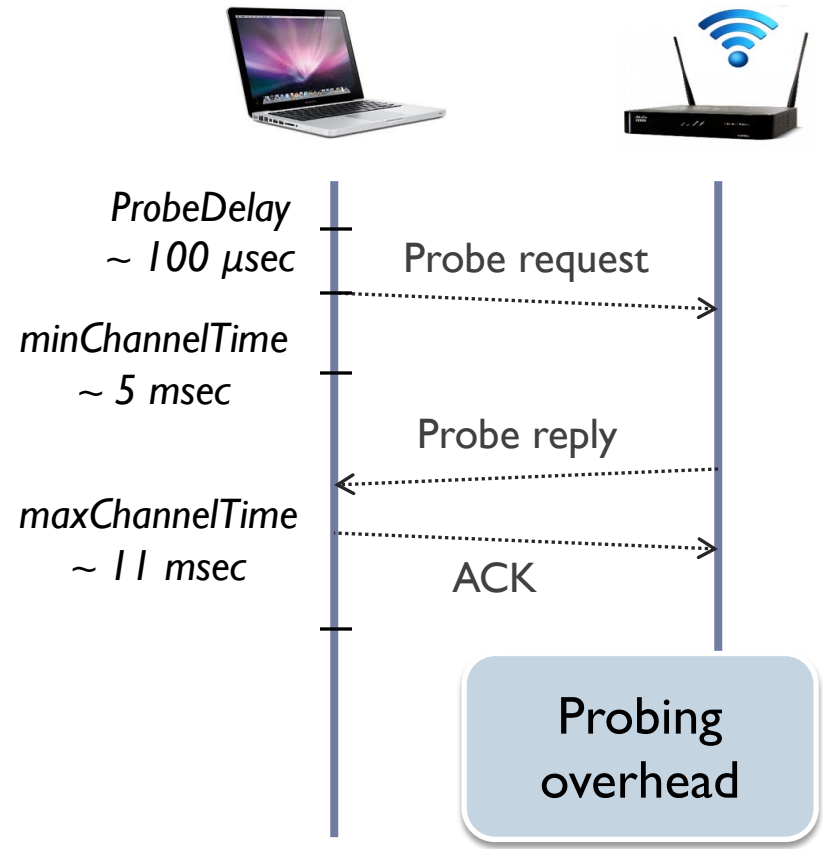
AP Discovery in IEEE standards

Passive Scan

BeaconInterval ~ 120 msec

Beacon

High discovery latency
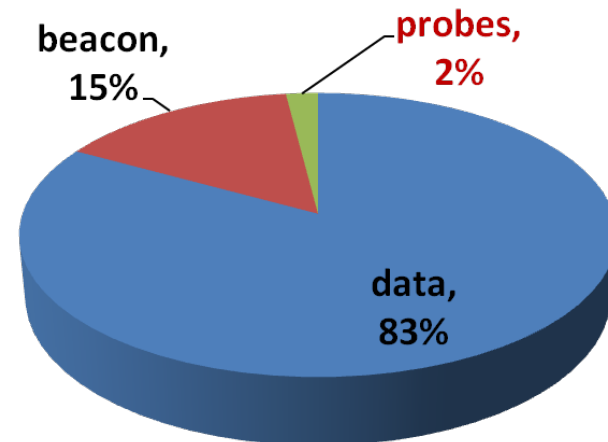
AP Discovery in IEEE standards

Passive Scan

Active Scan

BeaconInterval
~ 120 msec

Beacon

High discovery latency

ProbeDelay
~ 100 µsec

Probe request

minChannelTime
~ 5 msec

Probe reply

maxChannelTime
~ 11 msec

ACK

Probing overhead

AP Discovery in Device Drivers

Hybrid Scan

Passive Scan

Beacon

Targeted Active Scan

Probe request for **IllinoisNet**

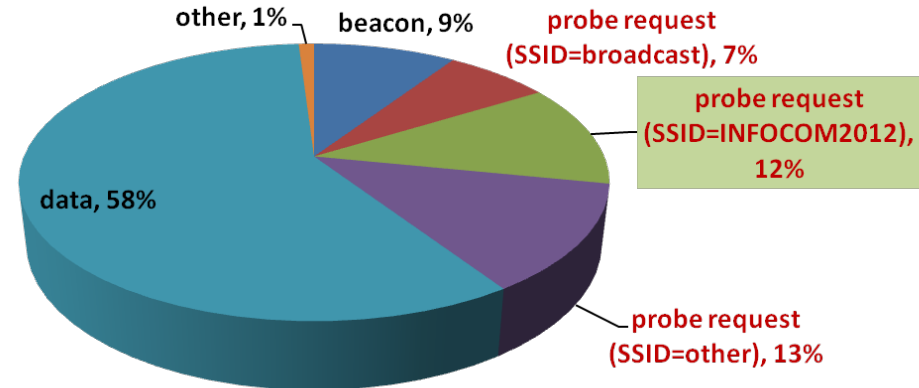Probe request for **Eduroam**

Broadcast Active Scan

Probe request for **ALL**

Probe reply

ACK

other, 1%
beacon, 9%
probe request (SSID=broadcast), 7%
probe request (SSID=INFOCOM2012), 12%
data, 58%
probe request (SSID=other), 13%

Busy Traces

Even more probing overhead

Probe Storms in Busy Traces

Laptops ~ 569
Avg. Probes ~ 227

Smartphones
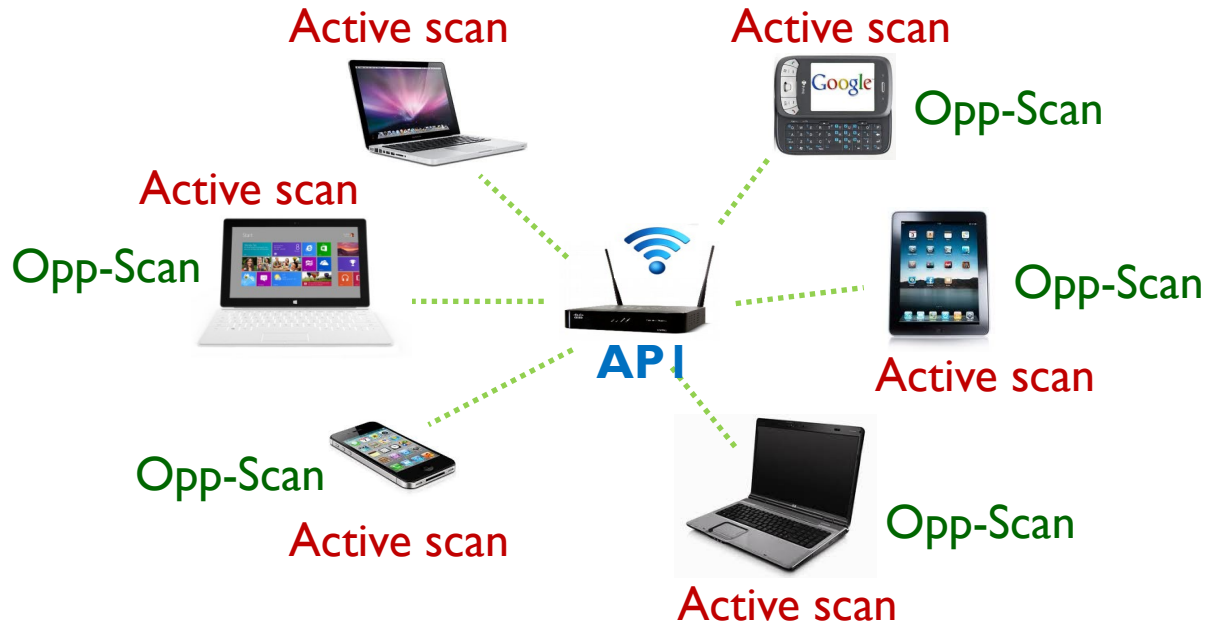*& tablets ~ 255*
Avg. Probes ~ 373

Packet retransmissions

High contention

AP scanning triggered

More probing overhead

ALL devices experience poor channel conditions

Probe intervals per device – CDF

— mobile
— laptops

Interval between probes [s]

80 % of the devices start their next scan within 1 second
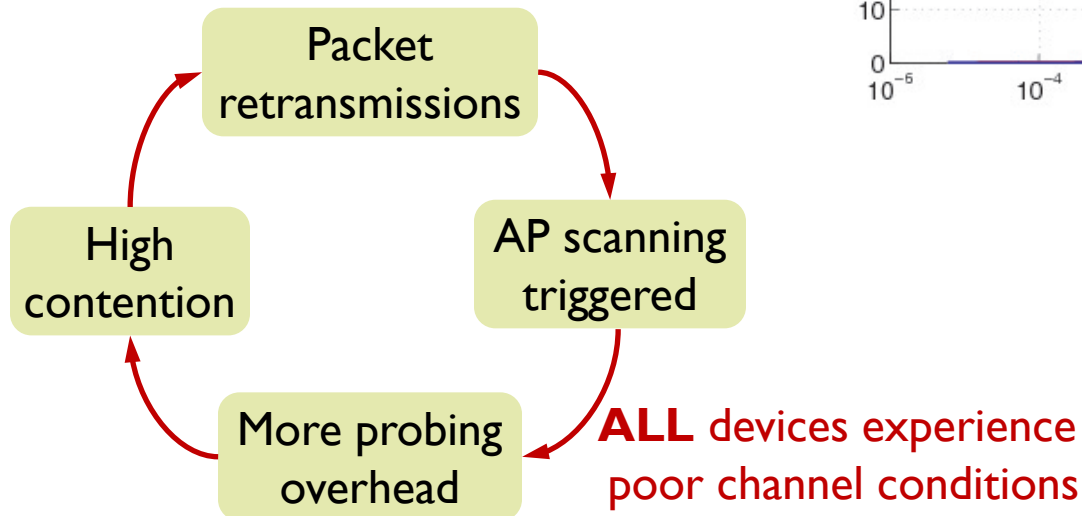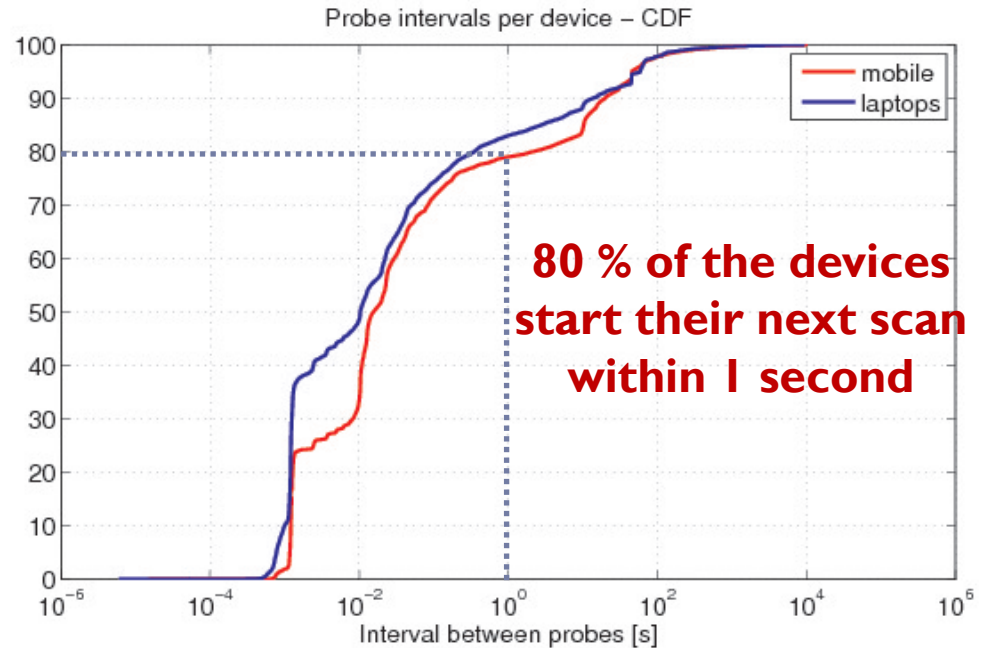
Preventing Probe Storms
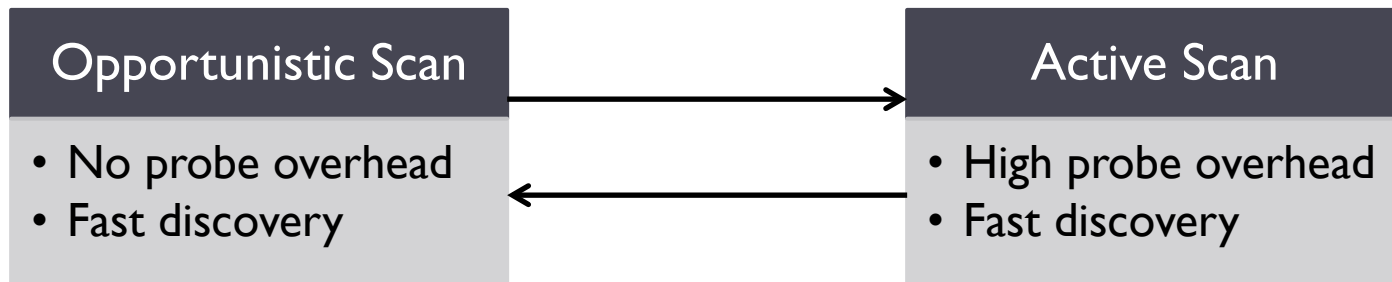
▸ Find a new AP

▸ Cache AP information

▸ Broadcast probe responses

▸ Pre-scan

▸ Fix timeouts

▸ Neighbor pruning

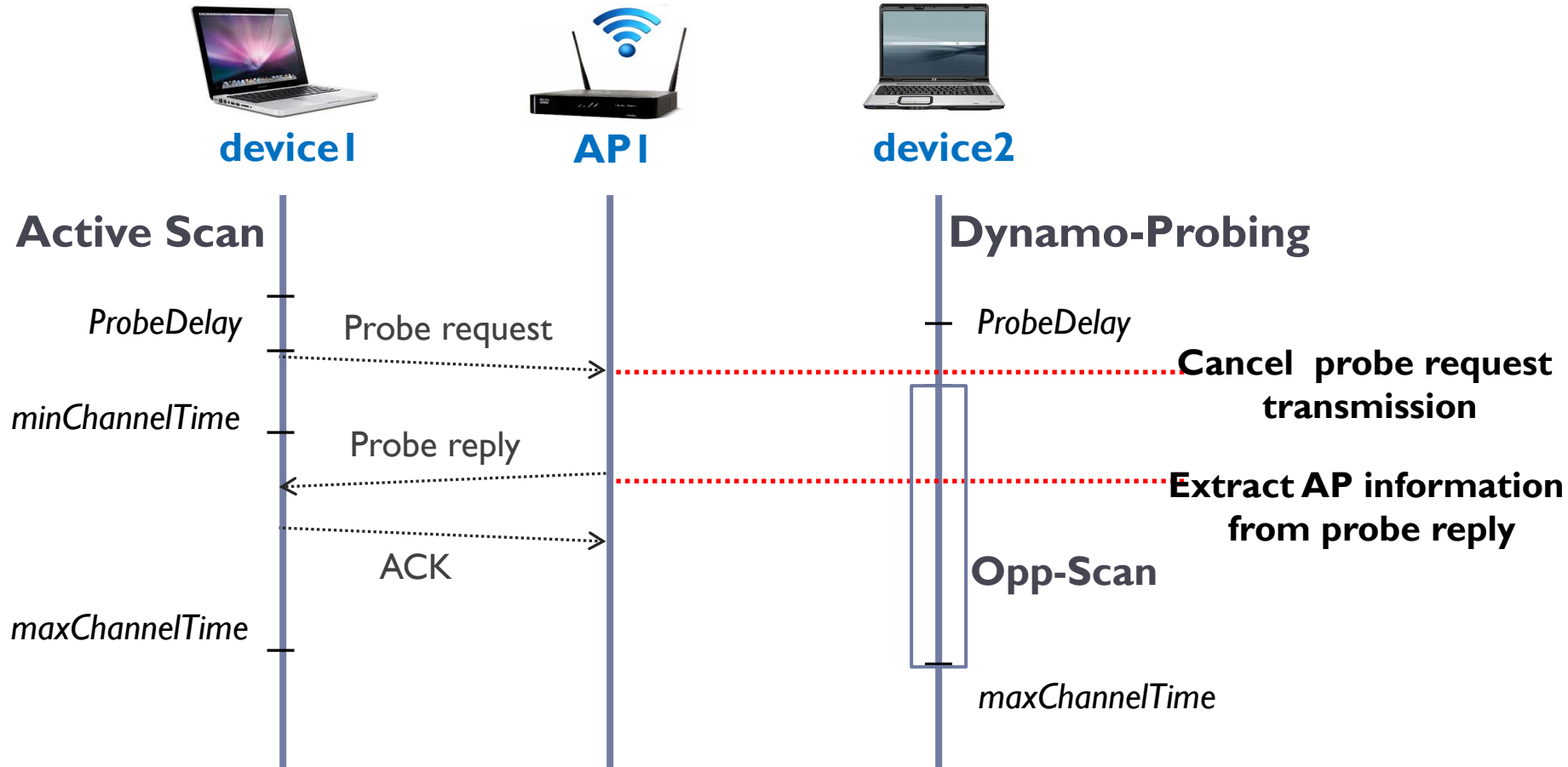# Dynamic Opportunistic Probing

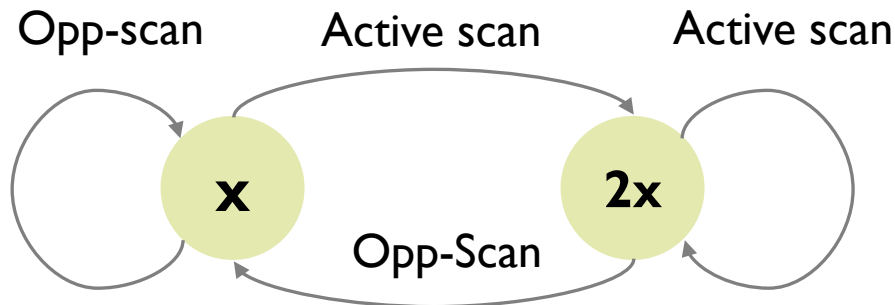Active scan   Active scan

Opp-Scan

Active scan

Opp-Scan

Opp-Scan

API

Active scan

Opp-Scan

Opp-Scan

Active scan

Opp-Scan

Active scan

Active scan

Dynamo-Probing

Opportunistic Scan	Active Scan
• No probe overhead • Fast discovery	• High probe overhead • Fast discovery

Dynamo-Probing

Dynamo-Probing: Mode Switch

Active scan

device1

Opp-Scan

Opp-Scan

Opp-Scan

Opp-Scan

Opp-Scan

device2

AP1

Opp-Scan

Opp-Scan

AP2

Opp-Scan

Opp-Scan

Opp-Scan

device3

Opp-Scan

Opp-Scan

Priority Based:

Opp-scan   Active scan   Active scan
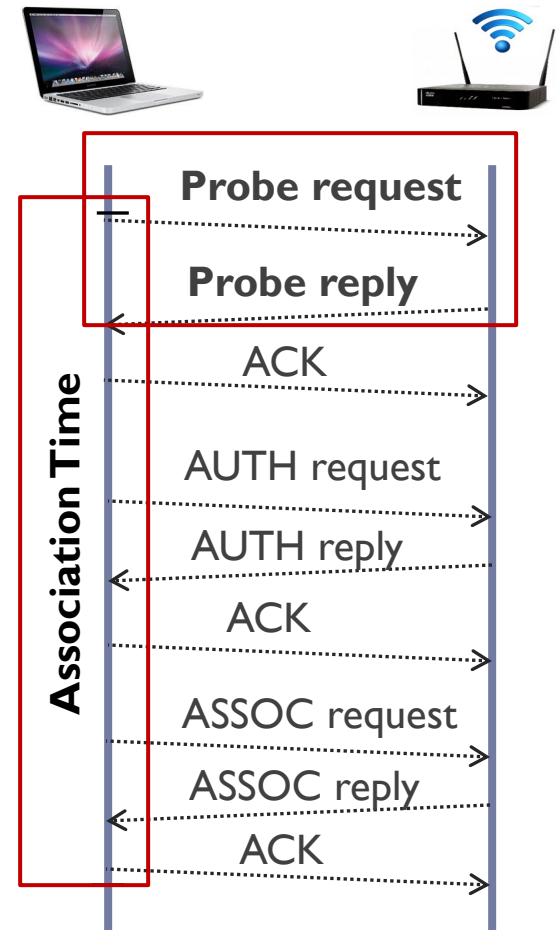
x   **2x**

Opp-Scan

Static:
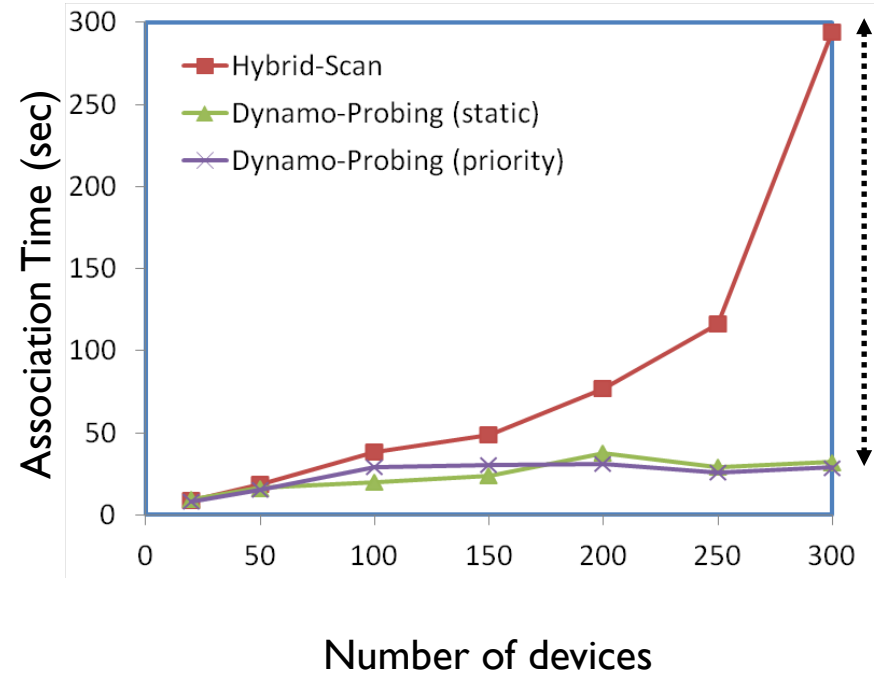**All devices have the same *ProbeDelay* = x**

Evaluation

▸ Dynamo-Probing is an **effective**, **efficient**, **adaptive** and **interoperable** scanning solution

▸ Metric

- ▸ **Effectiveness:** total probes, association time
- ▸ **Efficiency:** throughput, delay, packet drops

▸ Network & Traffic

- ▸ Varying density
- ▸ Simulate Internet traffic

Association Time
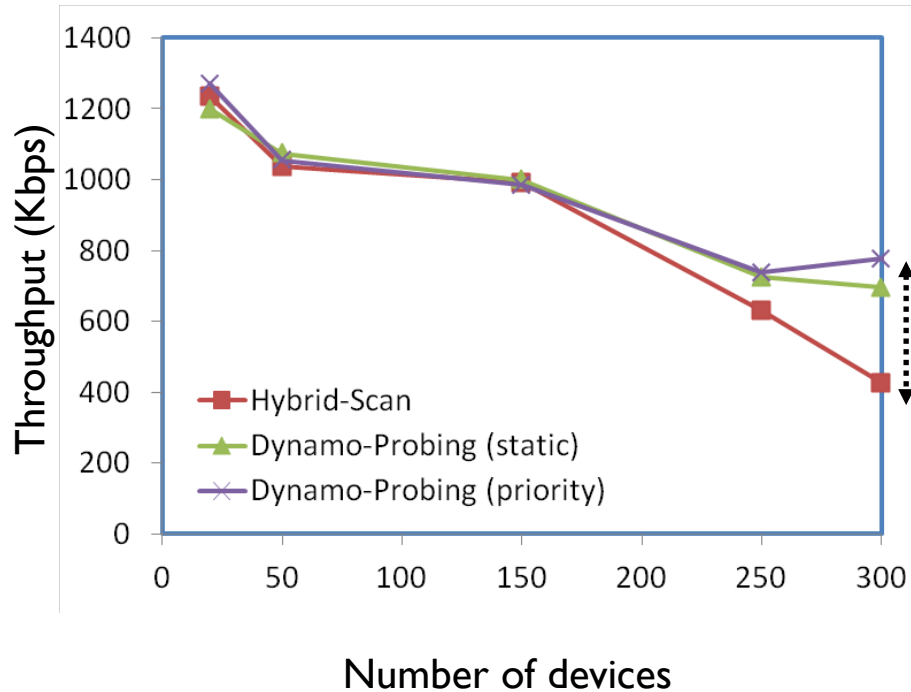
Probe request

Probe reply

ACK

AUTH request

AUTH reply

ACK

ASSOC request

ASSOC reply

ACK

Effectiveness
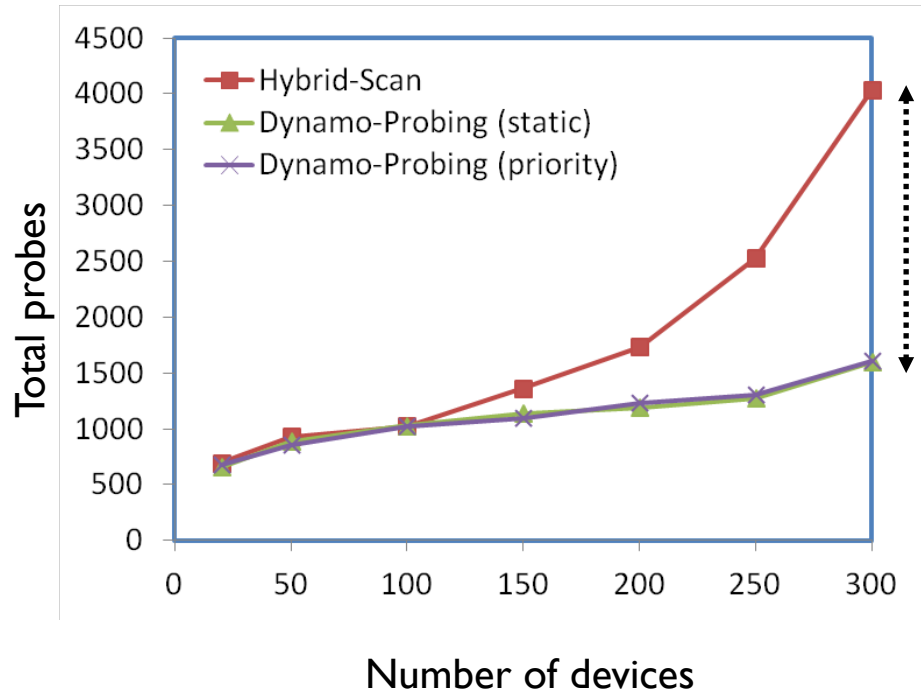
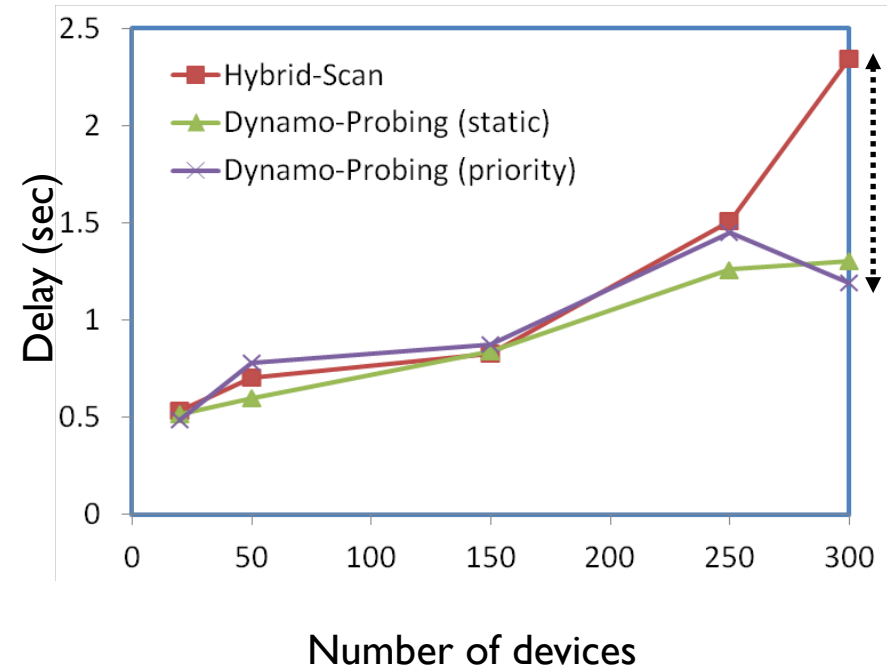**Reduces probing overhead by 59%**   **Reduces discovery latency by 90%**
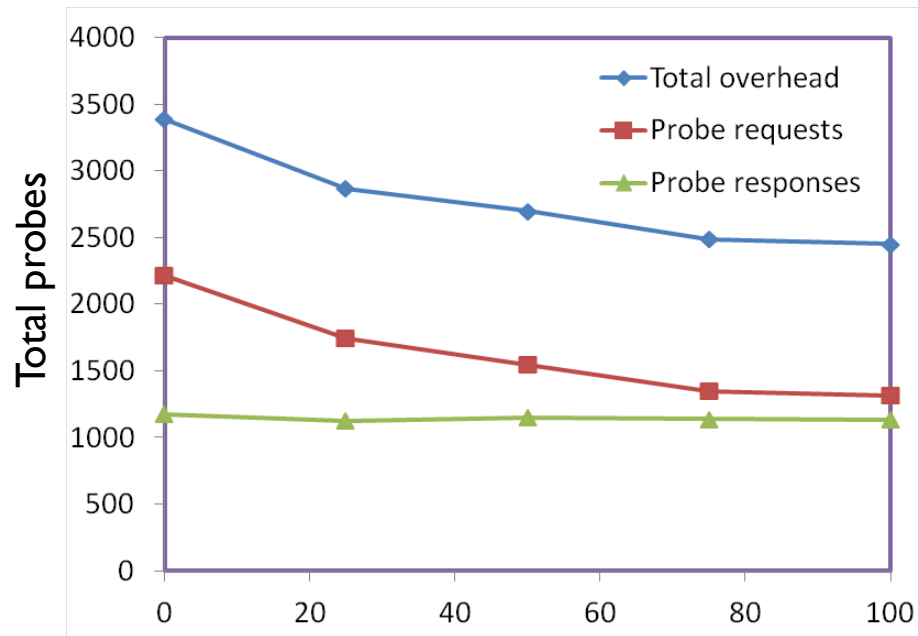
Efficiency

Improves throughput by 82%   **Reduces delay by 50%**

Incremental Deployment

Probing overhead
reduced by 21%
with 25% deployment

Achieves maximum benefit
with only 75% deployment

ALL Hybrid-Scan devices Percentage of Dynamo-Probing devices **ALL Dynamo-Probing devices**

(Network density=250 devices)

Summary

▸ Enables fast AP discovery without overloading the network with streams of probe packets

▸ Adaptive with density and interoperable with legacy devices

▸ Leverages the ***close proximity of devices*** and their ***similar AP fingerprints*** to obtain AP information opportunistically