Addressing Fields

To DS	From DS	Message	Address 1	Address 2	Address 3	Address 4
0	0	station-to-station frames in an IBSS; all mgmt/control frames	DA	SA	BSSID	N/A
0	1	From AP to station	DA	BSSID	SA	N/A
1	0	From station to AP	BSSID	SA	DA	N/A
1	1	From one AP to another in same DS	RA	TA	DA	SA

RA: Receiver Address TA: Transmitter Address

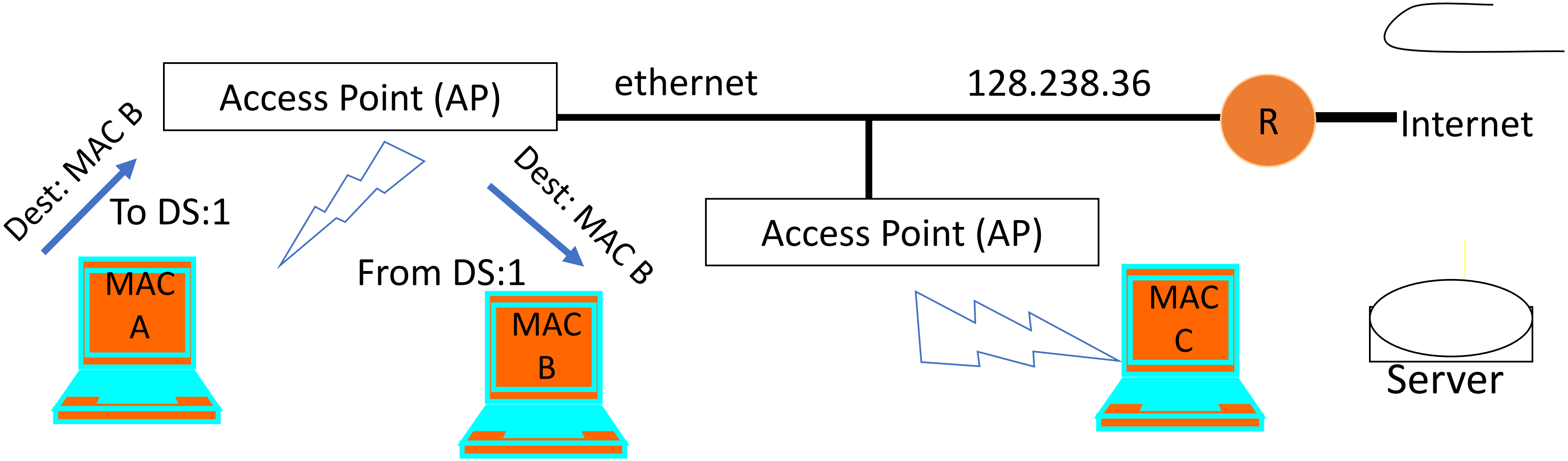
DA: Destination Address SA: Source Address

BSSID: MAC address of AP in an infrastructure BSS

Data Flow Examples

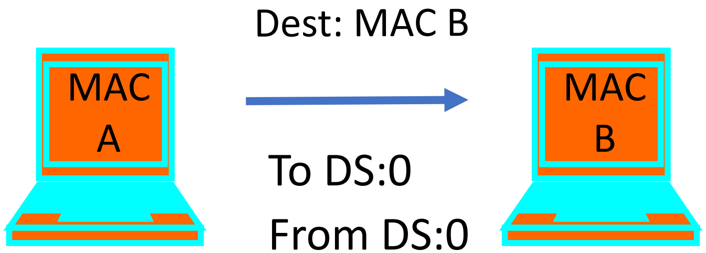
- Case 1: Packet from a station under one AP to another in same AP’s coverage area
- Case 2: Packet between stations in an IBSS
- Case 3: Packet from an 802.11 station to a wired server on the Internet
- Case 4: Packet from an Internet server to an 802.11 station

Case 1: Communication Inside BSS



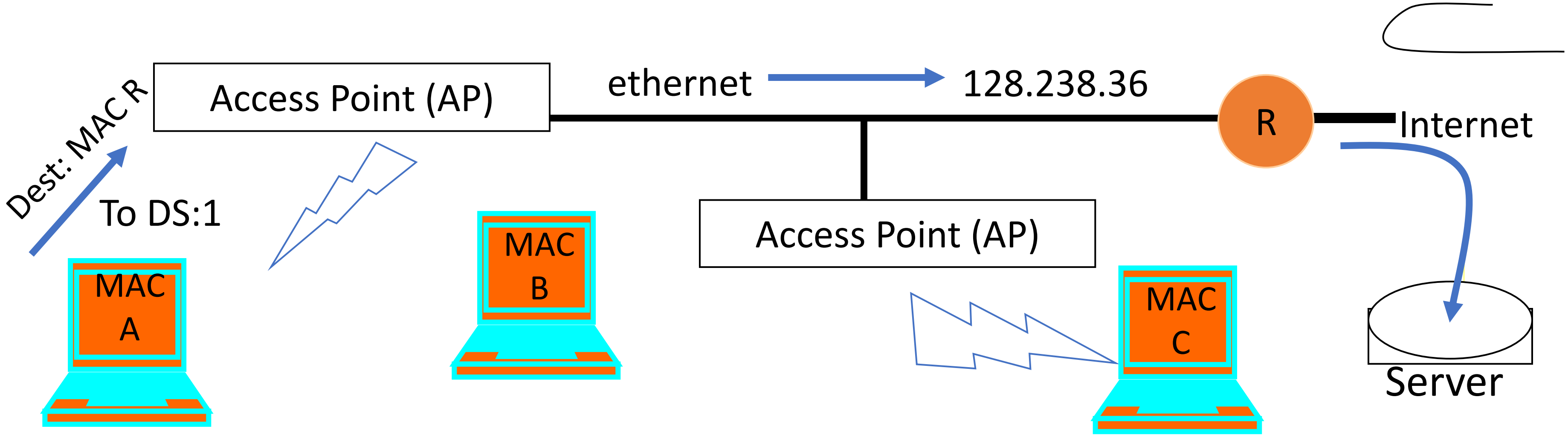
- AP knows which stations are registered with it so it knows when it can send frame directly to the destination

Case 2: Ad Hoc



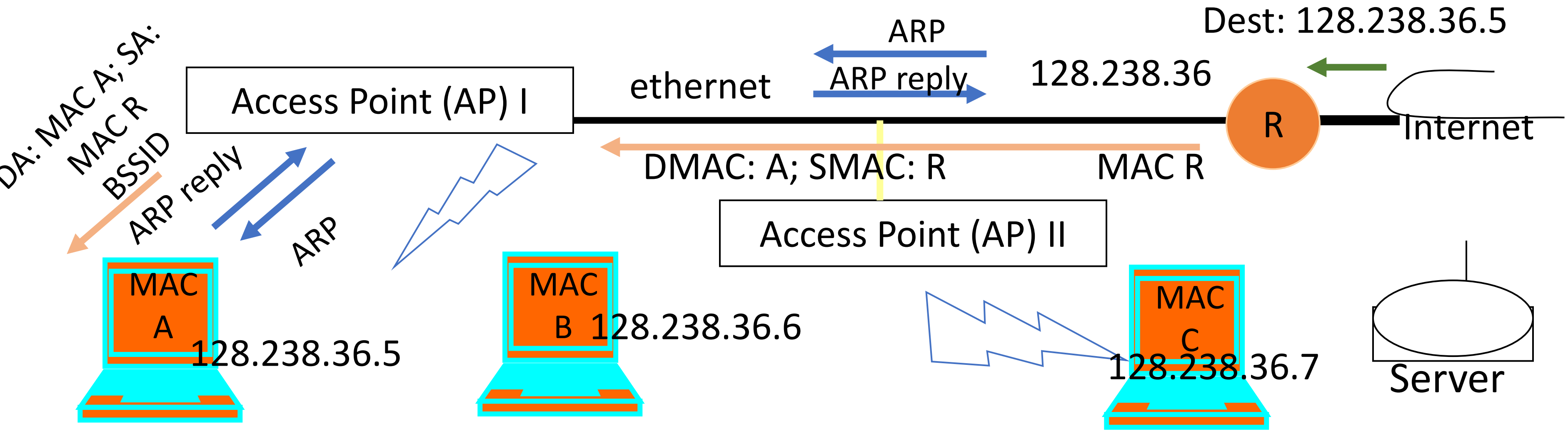
- Direct transmit only in IBSS (Independent BSS), i.e., without AP
- Note:
  - in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B

Case 3: To the Internet



- MAC A determines IP address of the server (using DNS)
- From the IP address, it determines that server is in a different subnet
- Hence it sets MAC R as DA;
  - Address 1: BSSID, Address 2: MAC A; Address 3: DA
- AP will look at the DA address and send it on the ethernet
  - AP is an 802.11 to ethernet bridge
- Router R will relay it to server

Case 4: From Internet to Station



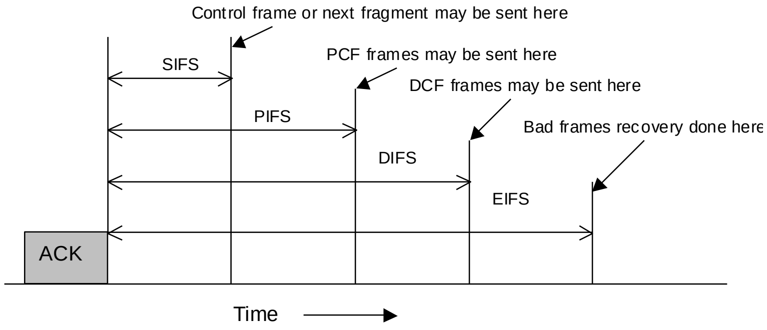
- Packet arrives at router R – uses ARP to resolve destination IP address
  - AP knows nothing about IP addresses, so it will simply broadcast ARP on its wireless link
  - DA = all ones – broadcast address on the ARP
- MAC A host replies with its MAC address (ARP reply)
  - AP passes on reply to router
- Router sends data packet, which the AP simply forwards because it knows that MAC A is registered

Outline

- 802.11 standard
- Physical layer
- MAC
  - ➢DCF
  - PCF
- Advanced MAC functions

MAC Layer

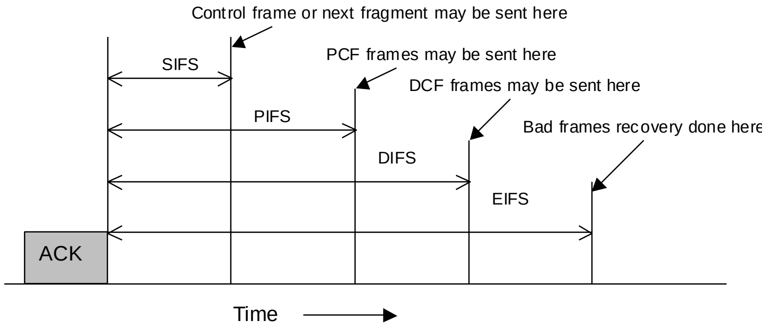
- Asynchronous Data Service (DCF)
  - CSMA/CA
  - RTS/CTS
- Timing-controlled service (PCF)
  - Polling
- Inter-frame spacing (IFS)
  - DIFS (distributed), for the node to start transmitting
  - PIFS (point), used by PCF for network access
  - SIFS (short), between packets of the same flow


Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
DCF frames may be sent here
PIFS
Bad frames recovery done here
DIFS
EIFS
ACK
Time

DCF: Distribution Coordination Function
PCF: Point Coordination Function
DIFS: DCF Inter Frame Spacing
PIFS: PCF Inter Frame Spacing
SIFS: Short Interframe Spacing

Carrier Sense Multiple Access

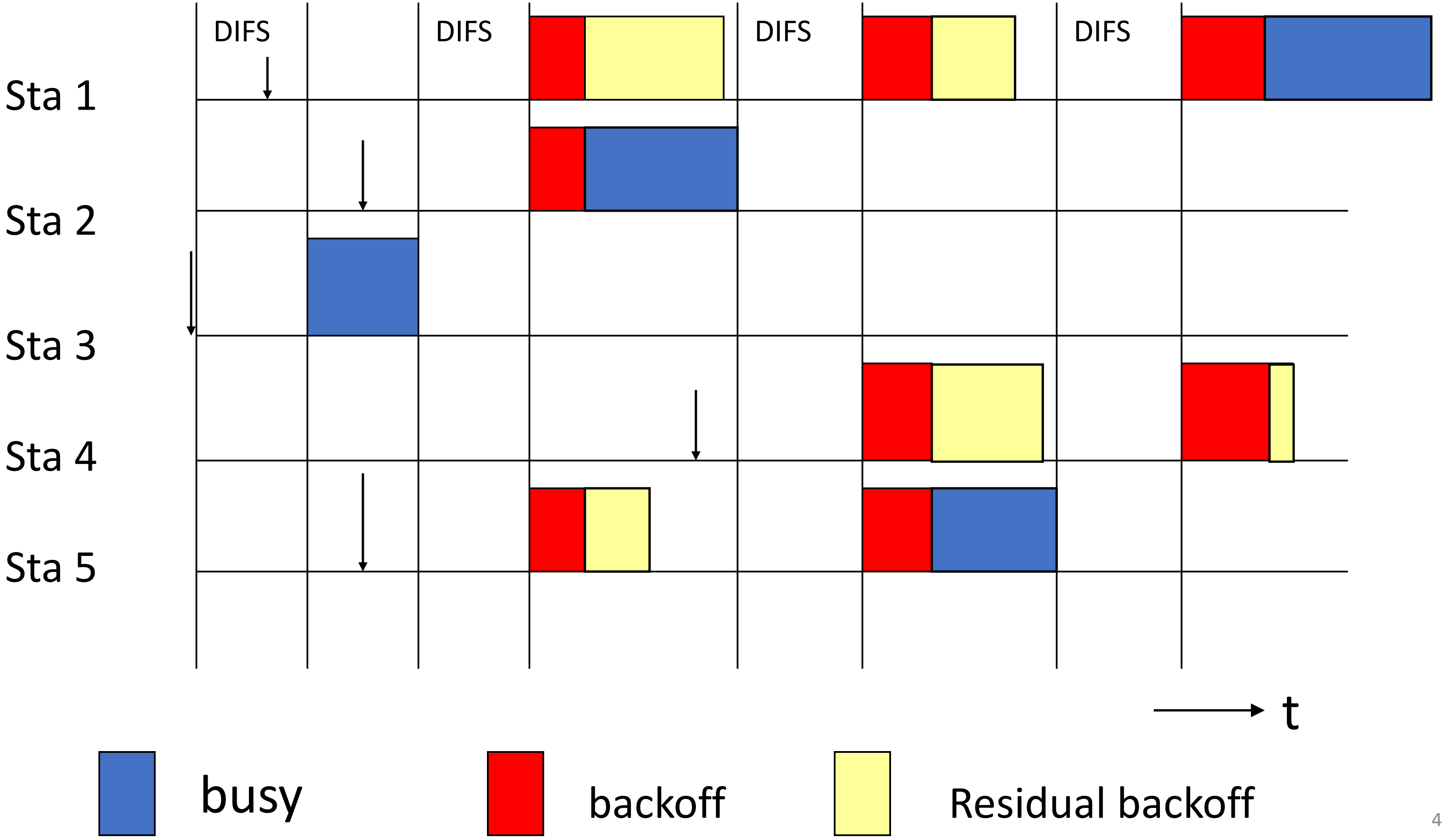
- Before transmitting a packet, sense carrier
- If it is idle, send
  - After waiting for one DCF inter frame spacing (DIFS)
- If it is busy, then
  - Wait for medium to be idle for a DIFS (DCF IFS) period
  - Go through exponential backoff, then send
    - Want to avoid that several stations waiting to transmit automatically collide
- Wait for ACK
  - If there is one, you are done
  - If there isn't one, assume there was a collision, retransmit using exponential backoff


Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
DCF frames may be sent here
PIFS
Bad frames recovery done here
DIFS
EIFS
ACK
Time

Exponential Backoff

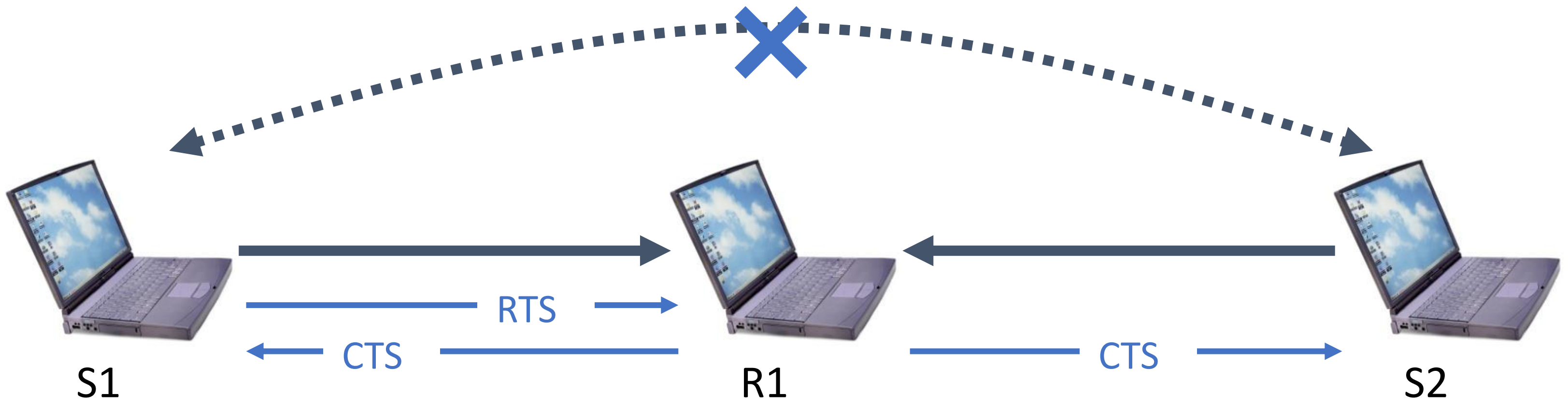
- Force stations to wait for random amount of time to reduce the chance of collision
  - Backoff period increases exponentially after each collision
  - Similar to Ethernet
- If the medium is sensed busy:
  - Wait for medium to be idle for a DIFS (DCF IFS) period
  - Pick random number in contention window (CW) = backoff counter
  - Decrement backoff timer until it reaches 0
    - But freeze counter whenever medium becomes busy
  - When counter reaches 0, transmit frame
  - If two stations have their timers reach 0; collision will occur;
- After every failed retransmission attempt:
  - increase the contention window exponentially
  - 2^i –1 starting with CW_{min} up to CW_{max} e.g., 7, 15, 31$_{, …}$

CSMA/CA


DIFS
DIFS
DIFS
DIFS
Sta 1
Sta 2
Sta 3
Sta 4
Sta 5
t
busy
backoff
Residual backoff

Collision Avoidance

- Difficult to detect collisions in a radio environment
  - While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong
- Why do collisions happen?
  - Near simultaneous transmissions
    - Period of vulnerability: propagation delay
  - Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver

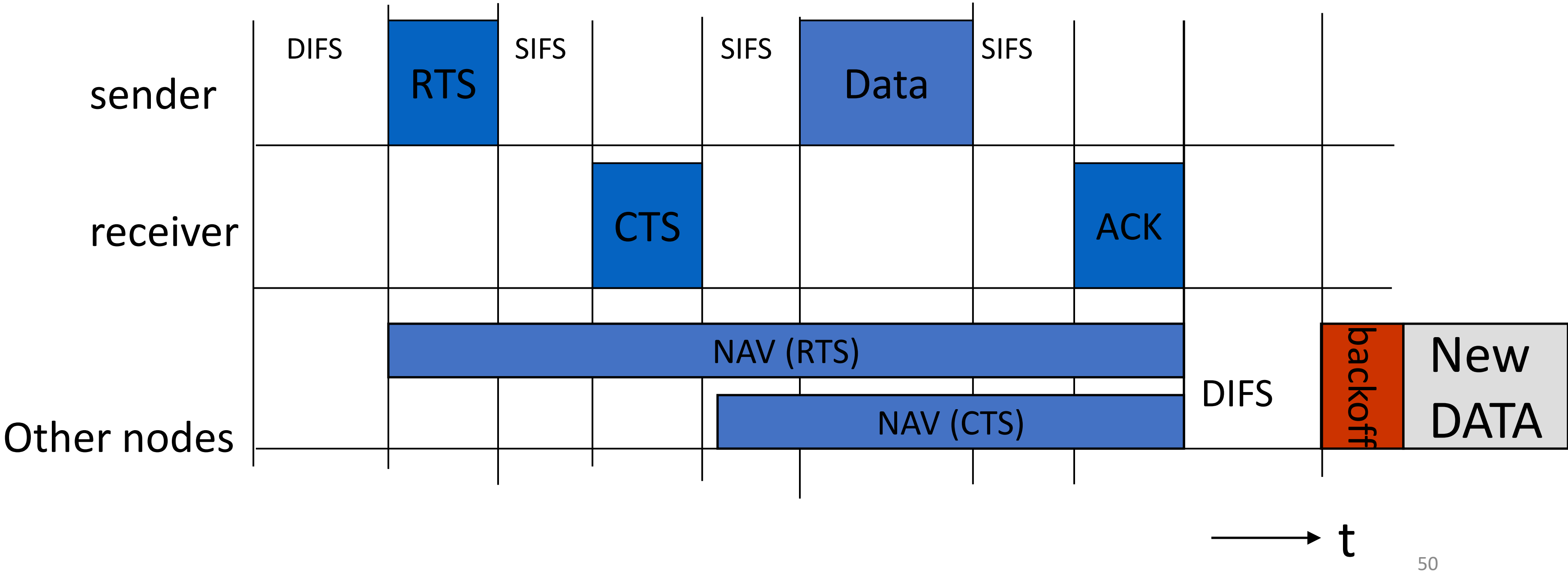


Request-to-Send and Clear-to-Send

- Before sending a packet, a station first sends a RTS.
- The receiving station responds with a CTS.
  - RTS and CTS are smaller than data packets
  - RTS and CTS use shorter IFS to guarantee access
- Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission
  - Based on a Duration ID in the RTS and CTS
- Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)
  - Time that must elapse before a station can sample channel for idle status

RTS/CTS: NAV

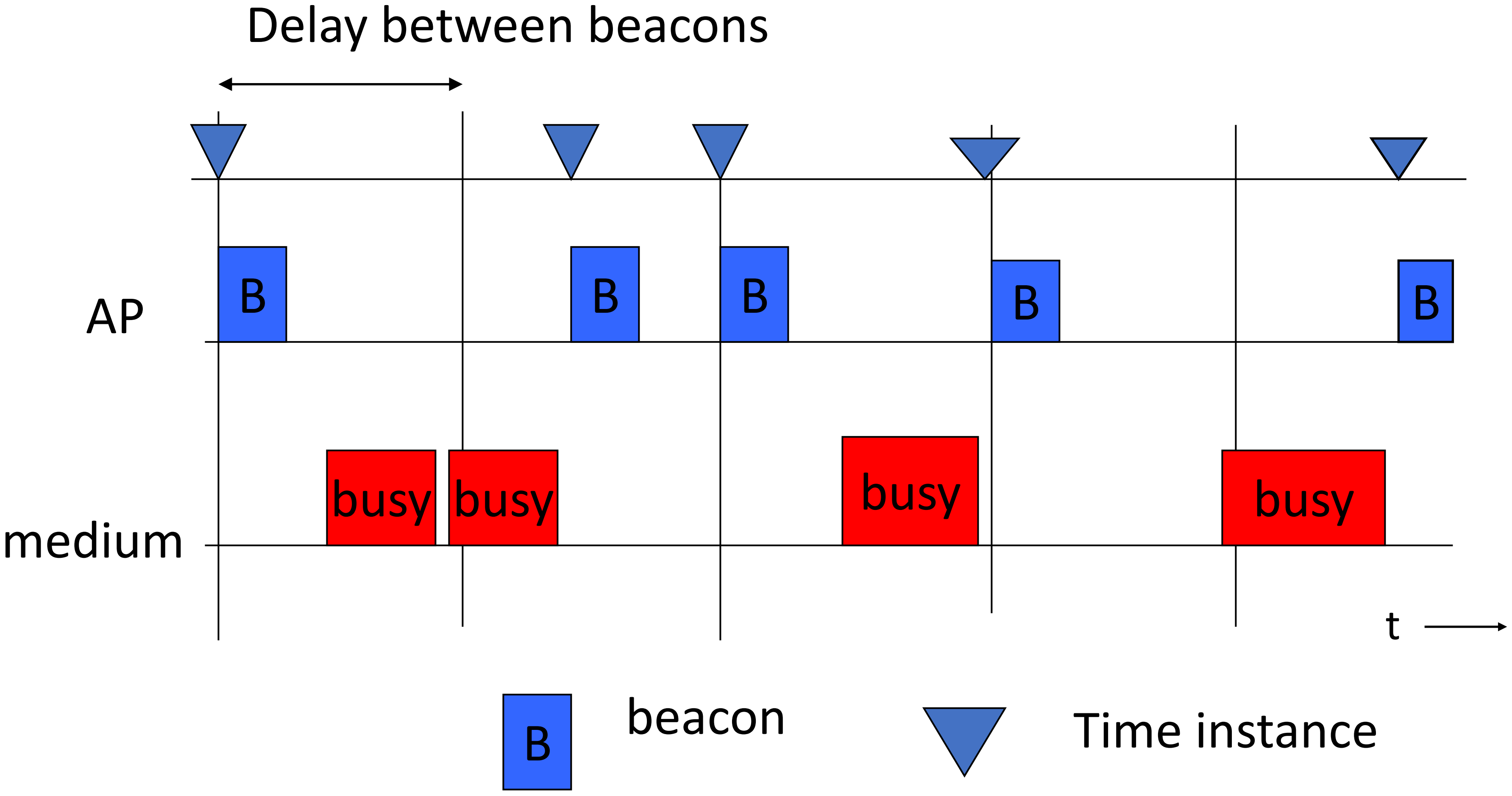
- NAV: Network Allocation Vector
- NAV acts as a distributed (in each node) resource allocation register
- RTS/CTS
  - Not a “major” concern



Synchronization

- Timing synchronization function (TSF)
  - Beacons of the AP are sent in well-defined instants.
  - Content of packet is the exact instant when it goes to the network.
- Used also for power management
  - All clocks of all stations in the BSS are synchronized
    - This allows STA to wake-up to check if packets exist.

Synchronization



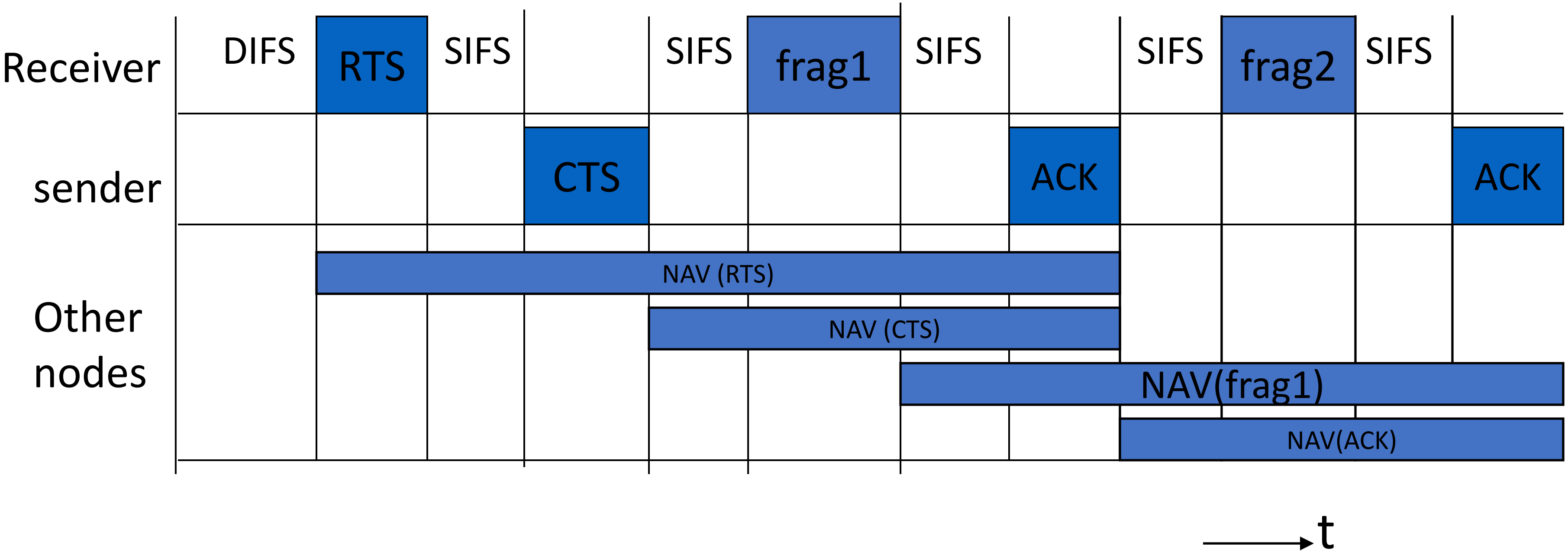
Outline

- 802.11 standard
- Physical layer
- MAC
  - ➢DCF
  - PCF
- Advanced MAC functions

Some More MAC Features

- Use of RTS/CTS is controlled by an RTS threshold
  - RTS/CTS is only used for data packets longer than the RTS threshold
  - Pointless to use RTS/CTS for short data packets – high overhead!
- Number of retries is limited by a Retry Counter
  - Short retry counter: for packets shorter than RTS threshold
  - Long retry counter: for packets longer than RTS threshold
- Packets can be fragmented.
  - Each fragment is acknowledged
  - But all fragments are sent in one sequence
  - Sending shorter frames can reduce impact of bit errors
  - Lifetime timer: maximum time for all fragments of frame

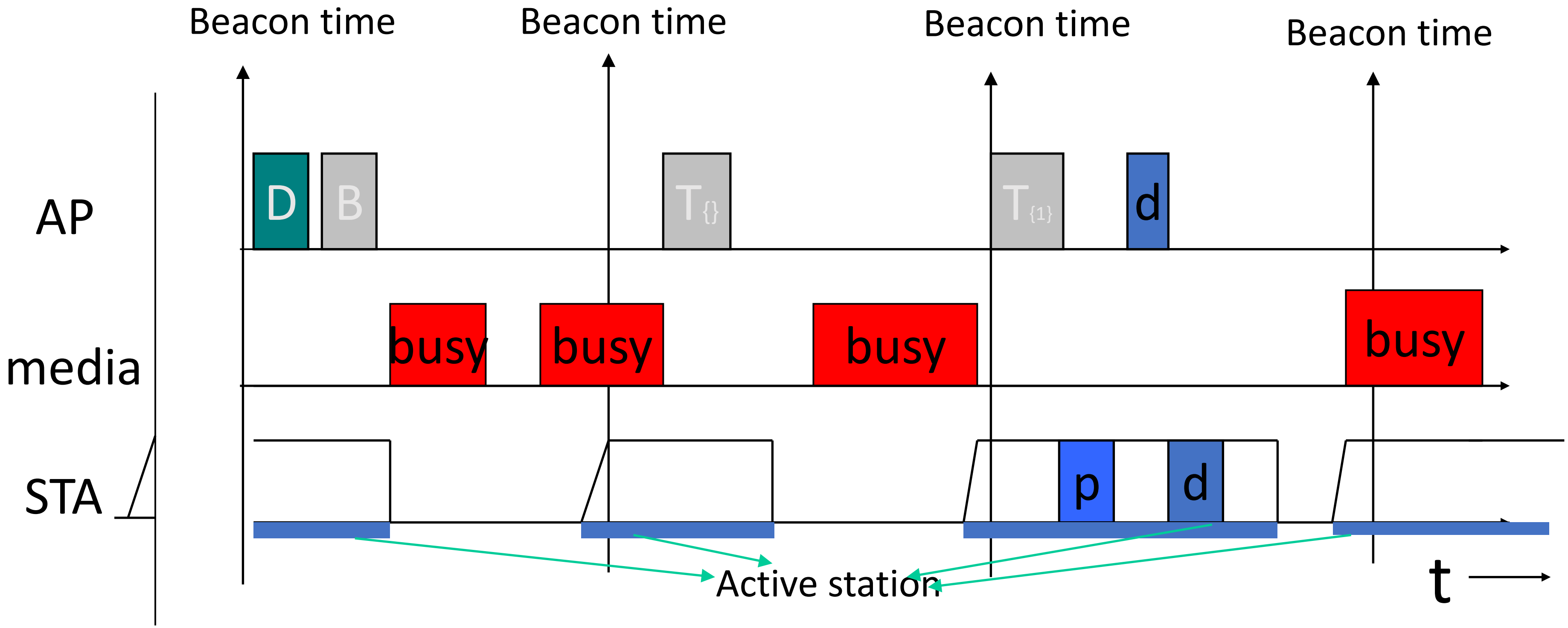
Fragmentation



Power management (infrastructure)

- APs buffer packets to stations in power saving mode
  - APs announce in beacons which packets are waiting with the TIM (traffic indication Map)
  - Broadcast/multicast frames are also buffered at AP
    - Sent after beacons, same common timing period.
    - Uses Delivery Traffic Indication Map (DTIM)
    - AP controls DTIM interval
- STA in power save wake periodically to listen for beacons
  - If it has data pending, send a PS-Poll
  - AP sends buffered data to this PS-poll
- TSF (Timing Synchronization Function) assures AP and stations are synchronized
  - Synchronizes clocks of the nodes in the BSS

Power management



B Broadcast/ multicast

p PS poll

d Transmission to/from STA

How does a station connect to an Access Point?

Control services at MAC

- Synchronization, Roaming and Association
  - Functions to find a network
  - Change APs
  - Search APs.
- Power Management
  - sleep mode without losing packets
  - Power management functions
- MIB: Management information base
- Security: authentication and cypher

SSID

- Mechanism used to segment wireless networks
  - Multiple independent wireless networks can coexist in the same location
- 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: Scanning

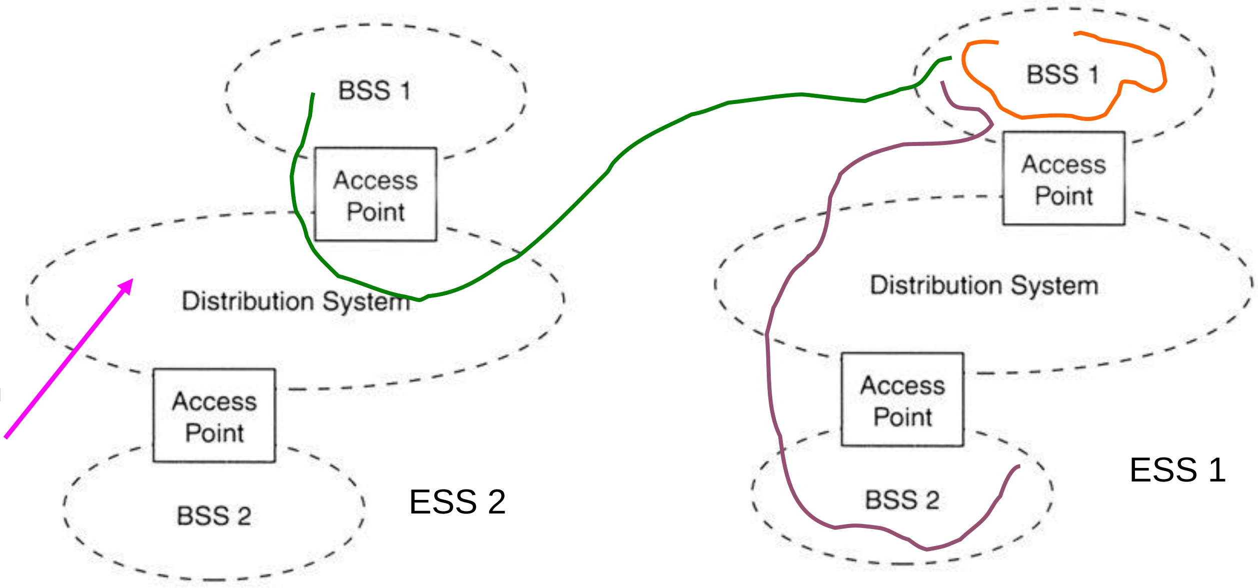
- Scanning is needed to:
  - Find and connect to a networks
  - Find a new AP during roaming
- Passive Scanning:
  - Station simply listens for Beacon and get info of the BSS. Power is saved.
- Active Scanning:
  - Station transmits Probe Request; elicits Probe Response from AP. Saves time.

Association Management: Scanning, and Joining

- Station must associate with an AP before they can use the network
  - AP must know about them so it can forward packets
- Re-association (roaming): association is transferred
  - Supports mobility in the same ESS
- Disassociation: station or AP can terminate association
- Stations can detect AP based on scanning
- Joining a BSS
  - Synchronization in Timestamp Field and frequency (i.e., channel) :
  - Adopt PHY parameters
  - Other parameters: BSSID, WEP, Beacon Period, etc.

IEEE 802.11 Mobility

- Standard defines the following mobility types:
  - No-transition: no movement or moving within a local BSS
  - BSS-transition: station moves from one BSS in one ESS to another BSS within the same ESS
  - ESS-transition: station moves from a BSS in one ESS to a BSS in a different ESS (continuos roaming not supported)



- Address to destination mapping
- seamless integration of multiple BSS

Roaming

- Roaming: station changes network (BSS)
- STA may go:
  - Outside the coverage area of their AP
  - But still under the coverage area of another AP

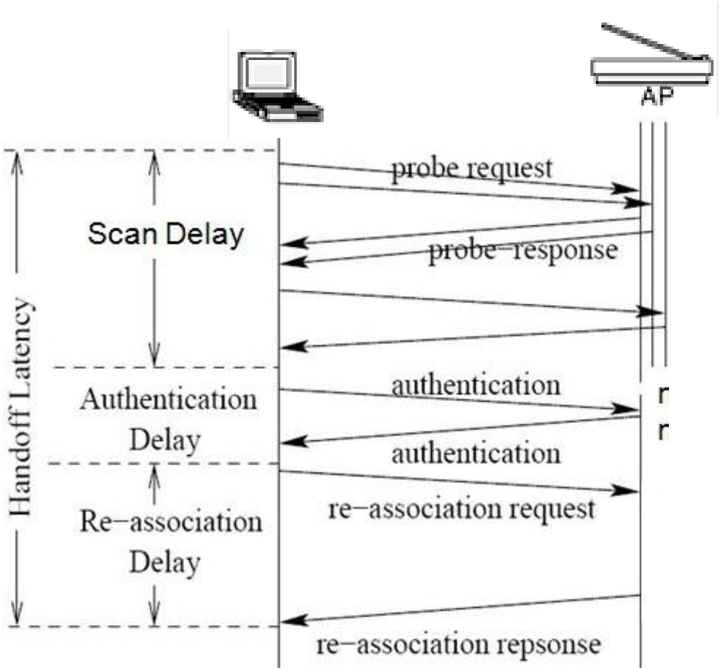
- Reassociate the STA with the new AP allows the communication to continue

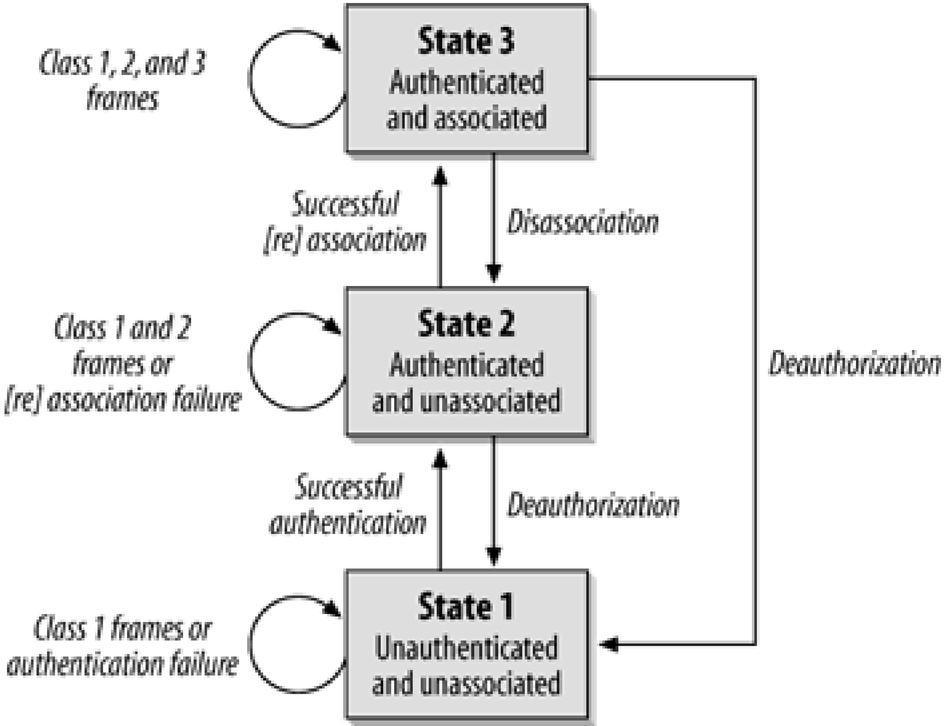
Roaming

- STA decides that the signal with the current AP is bad.
- STA does scanning (act/pas) to find new AP
- STA reassociates with the New AP (NAP)
  - Includes authorization.
- Without positive answer
  - STA does new scan
- With positive answer:
  - STA changed network to the new NAP
  - AP informs the ESS of the new association
  - Information in the distributed system is always updated.

Attachment to a BSS

- The STA finds a BSS/AP through **Scanning/Probing**
- Both **Authentication** as well as **Association**are necessary to enter a BSS




State 3
Authenticated and associated
State 2
Authenticated and unassociated
State 1
Unauthenticated and unassociated
Class 1, 2, and 3 frames
Class 1 and 2 frames or [re] association failure
Class 1 frames or authentication failure
Successful [re] association
Disassociation
Successful authentication
Deauthorization
Deauthorization

Phase 1: Scanning

- The STA searches for APs
  - **Passive Scanning**
    - STA analizes channels looking for ***Beacon*** packets, which are periodically sent by the AP, announcing its presence and SSID
  - **Active Scanning**
    - STA sends ***Probe Request*** packets to all channels in sequence
    - AP's listening in these diferente channels respond with a ***Probe Response***

Phase 2: Authentication

- After finding and selecting an AP, the STA has to authenticate with it. Two main methods:
- Method 1: **Open System Authentication**
  - Default procedure, executed in 2 steps:
    - 1 - STA sends an authentication frame including its identity
    - 2 - AP responds with a frame as a Ack/NAck
- Method 2: **Shared Key Authentication**
  - STA and AP have a shared secret, obtained in some other way
  - 1 – STA sends an initial authentication request
  - 2 – AP replies to the STA with a challenge
  - 3 – STA decyphers the challenge with its own key and sends it to the AP
  - 4 – AP uses its own key to decifer the challenge and compares results

Phase 3: Association

- After authenticated, the STA begins the **association** process, i.e., Exchange roaming and capacity information between STA and AP
- Procedure:
  - 1 – STA sends a **Associate Request** to AP, indicating supported transmission rates and intended association SSID
  - 2 – AP allocates resources and decides if it accepts or rejects the STA
  - 3 – AP sends an **Association Response**, indicating the association identifying and supportted transmission rates, in case the association is accepted
  - 4 (optional) – In case of a handover (transition of the STA between two different APs), the new AP informs the old AP
- Only after associating to the AP, can the STA start to send and receive data

How to extend range in Wi-Fi?

Wi-Fi “extenders”.

- Inexpensive
- They set up a new SSID, and forward all traffic to the original SSID
- Multi-hop configurations are possible
  - Require manual configuration
- Because the original access point and the extender have different SSIDs
  - Many devices will not automatically connect to whichever is closer
  - They prefer to maintain connection with the original SSID until that signal disappears
  - This is, for many mobile users, reason enough to give up on this strategy.

http://intronetworks.cs.luc.edu/current2/mobile/wireless.html

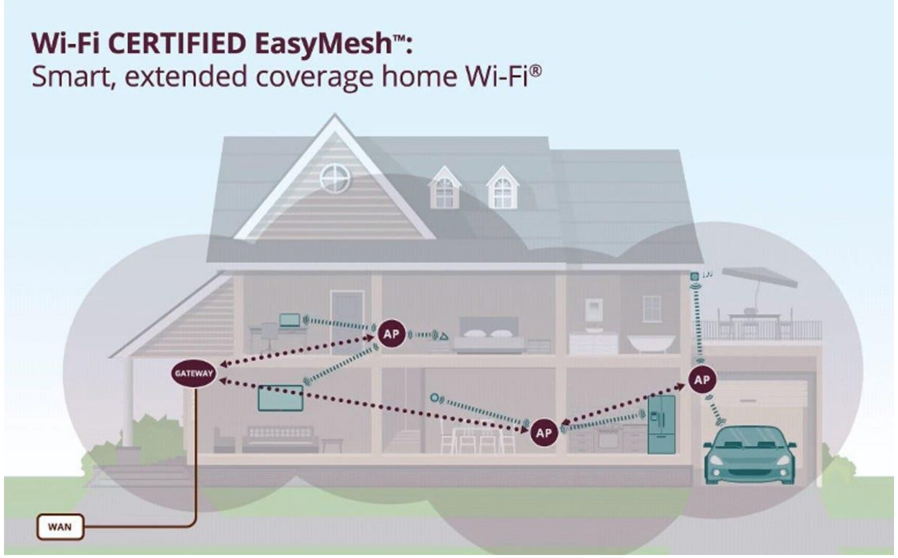
Mesh

- Different standards
  - IEEE 802.11s standard
    - Focuses on the setup of the mesh networks
    - Uses a mandatory routing protocol – Hybrid Wireless Mesh Protocol
    - Mesh Stations can collocate 802.11 AP's and provide access to the mesh network for 802.11 devices
    - A Mesh Gateway interconnects the mesh to other non-802 networks
  - Wi-Fi Alliance standard (a.k.a., "EasyMesh")
    - Focuses on more "easy" setup of mesh WiFi networks
      - incorporates parts of the IEEE 1905.1 standard for home networks, which simplifies initial configuration.
    - Specifies that one access point – the one connected to the Internet – will be a "Multi-AP" Controller
    - the other access points are called Agents.
    - The EasyMesh standard also

http://intronetworks.cs.luc.edu/current2/mobile/wireless.html

Wi-Fi EasyMesh

- WiFi Alliance Certification program that defines multiple access point home and small office Wi-Fi networks that are easy to install and use, self-adapting, and add multi-vendor interoperability.
- This technology brings both consumers and service providers additional flexibility in choosing Wi-Fi EasyMesh devices for home deployment.
- Wi-Fi EasyMesh uses a controller to manage the network, which consists of the controller, plus additional APs, called agents.
- Establishing controllers to manage and coordinate activity among the agents ensures that each AP does not interfere with the other, bringing both expanded, uniform coverage and more efficient service.


Wi-Fi CERTIFIED EasyMesh™:
Smart, extended coverage home Wi-Fi®
GATEWAY
AP
AP
AP
WAN

EasyMesh specification relies on other standards / specification, either by extending them or simply referencing them.

This includes, most notably:

- Building on and extending IEEE Standard 1905.1 to configure Wi-Fi access point interfaces
  - **Discovery**: how nodes are finding each other and identifying the controller
  - **Push-Button Configuration**: to initialize "onboarding" of access points-the process commonly referred to as "meshing"
  - **Backhaul communication**: Communication between the nodes / access points in the mesh network

IEEE 1905.1 standard, Convergent Digital Home Network for Heterogeneous Technologies.

IEEE 1905.1 standard, Convergent Digital Home Network for Heterogeneous Technologies.

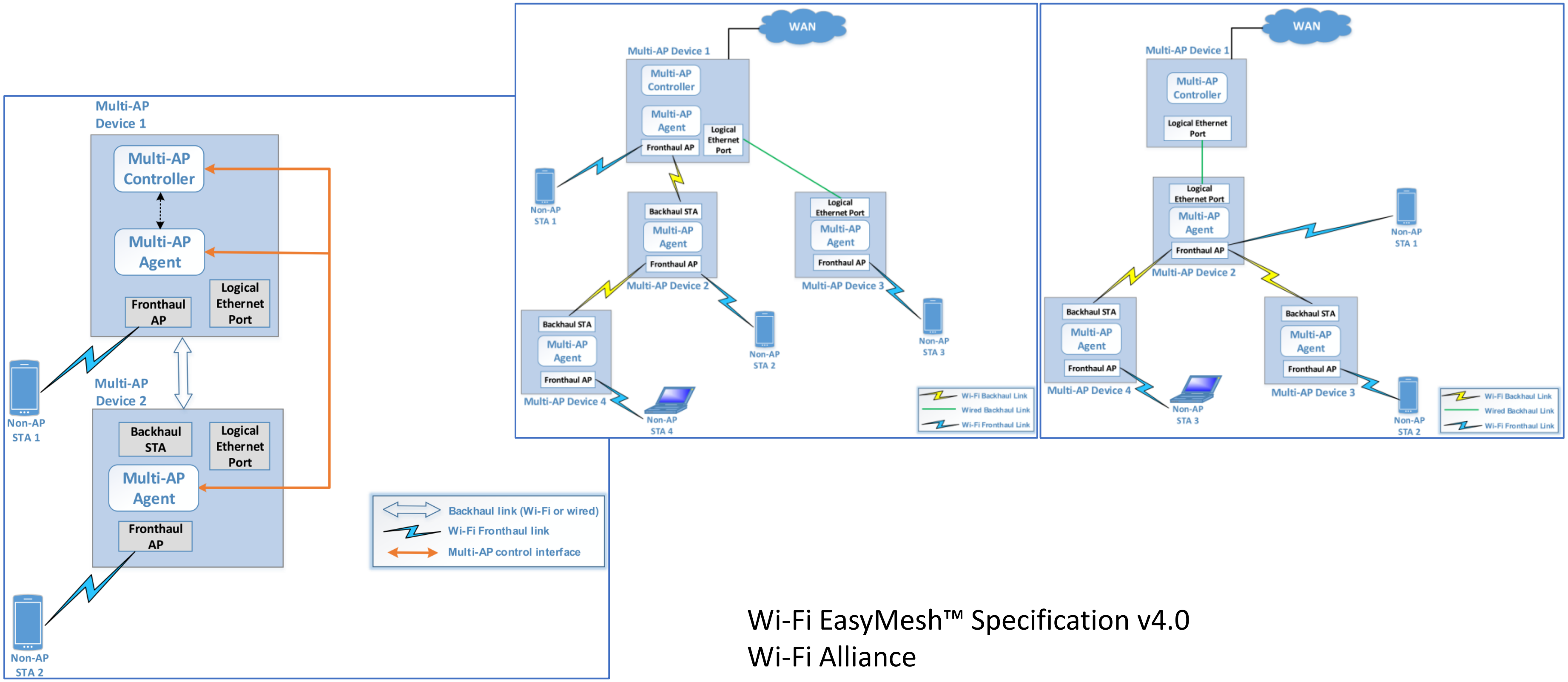
- This technology enables networked devices connected by different network media--say Gigabit Ethernet 2.4Ghz, and 5Ghz Wi-Fi, to operate as if they were connected across a single network. In EasyMesh, the controllers use data from it to configure each agent's AP radios. It also includes mechanisms to configure control-related policies on agents, such as metrics and steering. Additionally, the controller determines the topology of the network of agents, so it can adapt to changing network conditions.

- also utilize mechanisms from the new Wi-Fi Alliance Agile Multiband standard. New Agile Multiband certified devices will work better as they're moved from spot to spot with intelligent steering and faster network transitions.

Architecture and components

- **Controller** - every EasyMesh network must have one. The controller can be a unique device or embedded in a device that also has other functionality
- **Agent** - in order for a mesh network to exist, at least two agents must be connected to the controller
- **Device** - any component of a mesh network, whether it contains a controller, an agent, or both

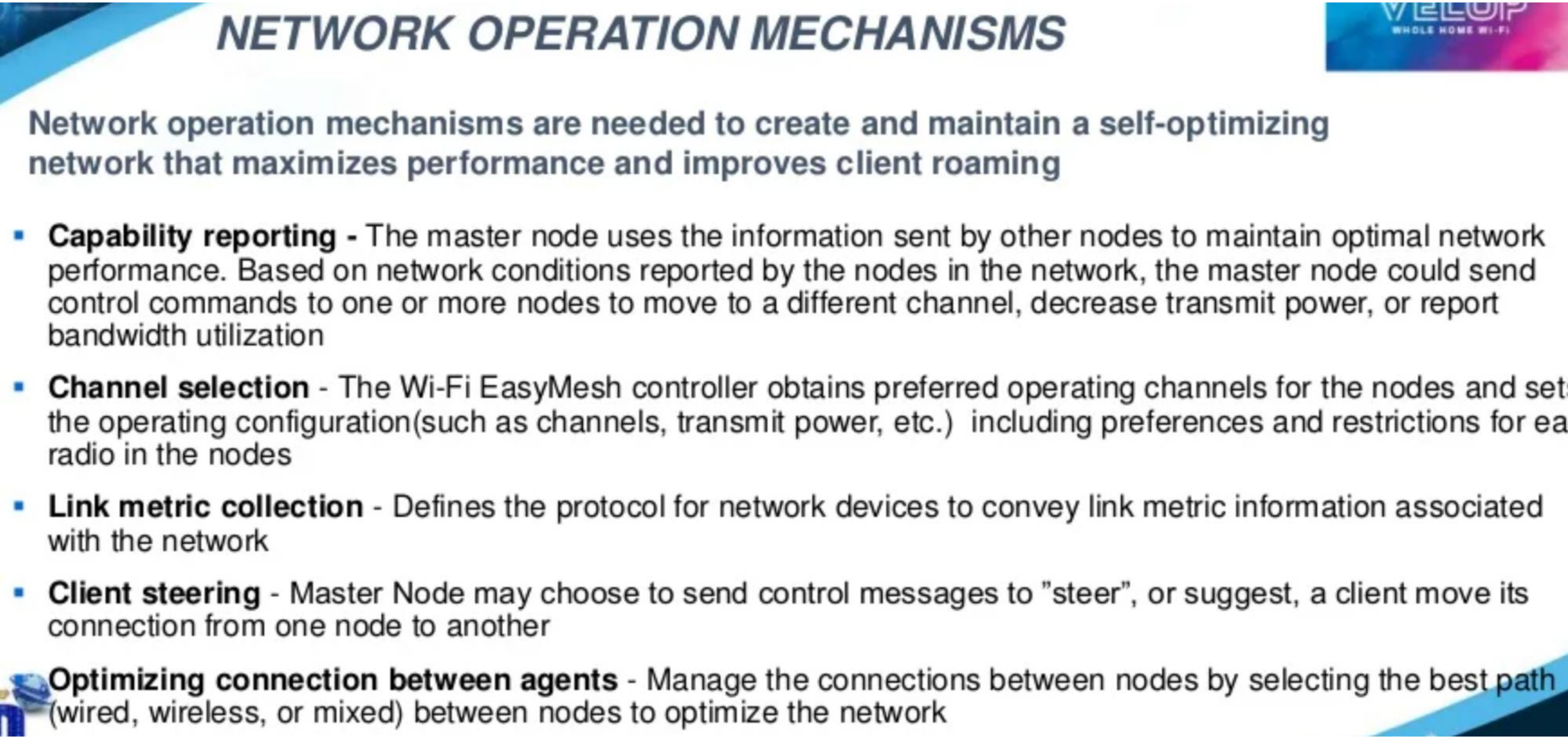
Example deployments



Wi-Fi EasyMesh™ Specification v4.0
Wi-Fi Alliance

- the specification does *not* standardize algorithms or decision-making

- How to do client steering makes up a significant part of the specification, telling manufacturers how to direct a client from one access point to another.
- When a client should be steered is not covered. Therefore, algorithms will still vary (and client roaming mechanisms may of course still interfere).



NETWORK OPERATION MECHANISMS

Network operation mechanisms are needed to create and maintain a self-optimizing network that maximizes performance and improves client roaming

- **Capability reporting -** The master node uses the information sent by other nodes to maintain optimal network performance. Based on network conditions reported by the nodes in the network, the master node could send control commands to one or more nodes to move to a different channel, decrease transmit power, or report bandwidth utilization
- **Channel selection** - The Wi-Fi EasyMesh controller obtains preferred operating channels for the nodes and set the operating configuration(such as channels, transmit power, etc.) including preferences and restrictions for ea radio in the nodes
- **Link metric collection** - Defines the protocol for network devices to convey link metric information associated with the network
- **Client steering** - Master Node may choose to send control messages to ”steer”, or suggest, a client move its connection from one node to another
- **Optimizing connection between agents** - Manage the connections between nodes by selecting the best path (wired, wireless, or mixed) between nodes to optimize the network

https://www.slideshare.net/kanquillano/iecep-agm-2018-wireless-mesh-technology-by-kristian-anquillano