

IEEE 802.11

Wireless communication is one of the fastest-growing technologies.

The demand for connecting devices without the use of cables is increasing everywhere.

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.



IEEE 802.11

- The **IEEE 802.11 wireless LAN, also known as WiFi.**
- There are several 802.11 standards for wireless LAN technology, including 802.11b, 802.11a, and 802.11g.
- The three 802.11 standards share many characteristics.
- They all use the same medium access protocol, CSMA/CA



SUMMARY OF IEEE 802.11 STANDARDS

Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

Table 6.1 ♦ Summary of IEEE 802.11 standards



IEEE 802.11

- Illustrates the principal components of the 802.11 wireless LAN architecture.
- The fundamental building block of the 802.11 architecture is the **basic service set (BSS)**.
- **A BSS contains one or more wireless stations and a central base station, known as an access point (AP)**
- Each 802.11 wireless station has a 6-byte MAC address that is stored in the firmware of the station's adapter (that is, 802.11 network interface card).
- Each AP also has a MAC address for its wireless interface.



THE 802.11 ARCHITECTURE

- Wireless LANs that deploy APs are often referred to as **infrastructure wireless LANs**, with the “infrastructure” being the APs along with the wired Ethernet infrastructure that interconnects the APs and a router.



THE 802.11 ARCHITECTURE

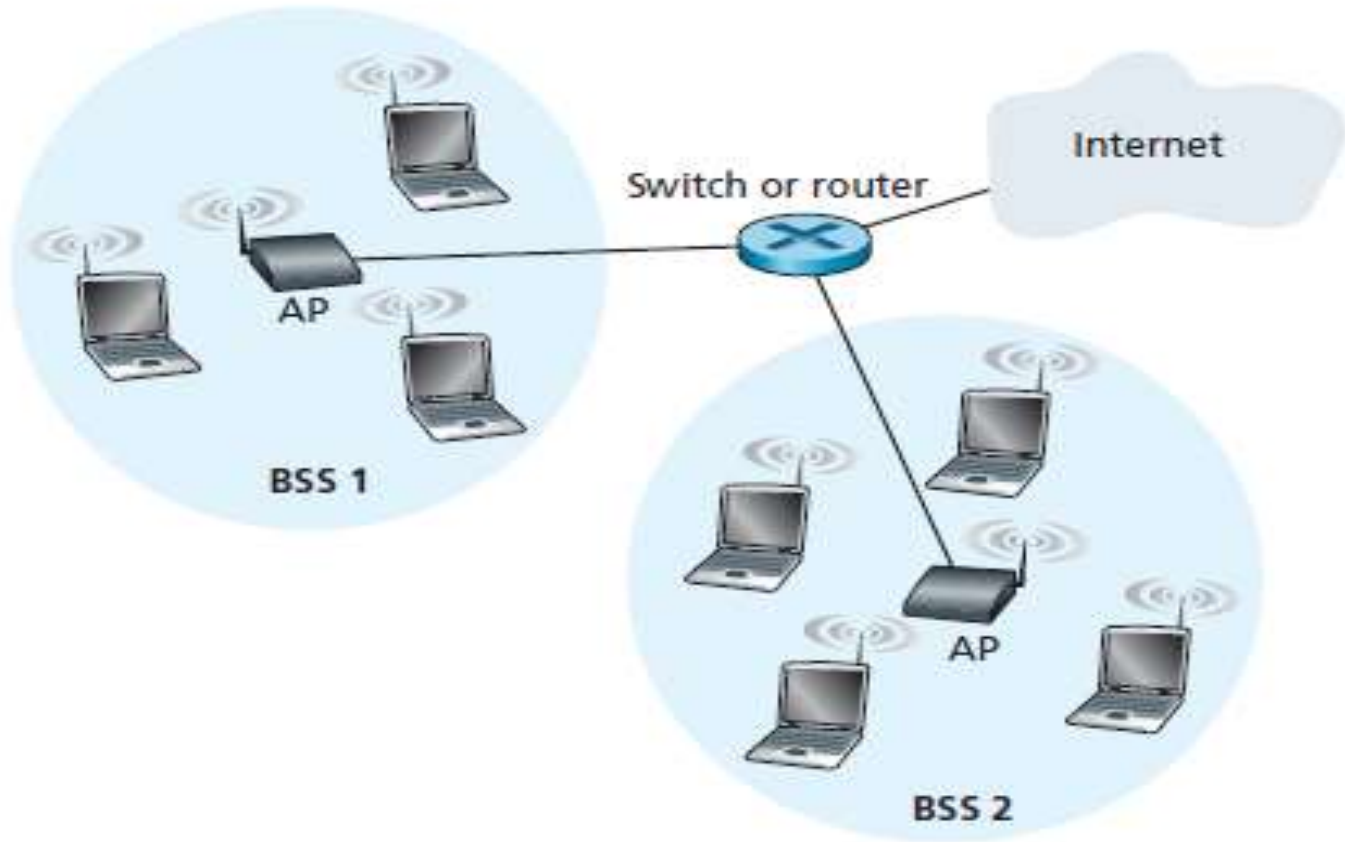


Figure 6.7 ♦ IEEE 802.11 LAN architecture

THE 802.11 ARCHITECTURE


- IEEE 802.11 stations can also group themselves together to form **an ad hoc network—a network with no central control and with no connections to the “outside world.”**
- Here, the network is formed “on the fly,” by mobile devices that have found themselves in proximity to each other, that have a need to communicate, and that find no preexisting network infrastructure in their location





Note

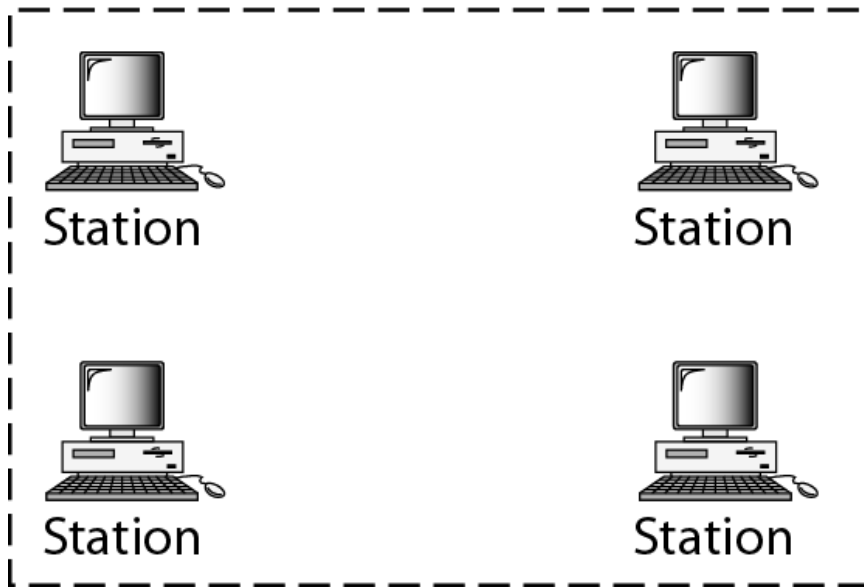
**A BSS without an AP is called an ad hoc network;
a BSS with an AP is called an infrastructure network.**



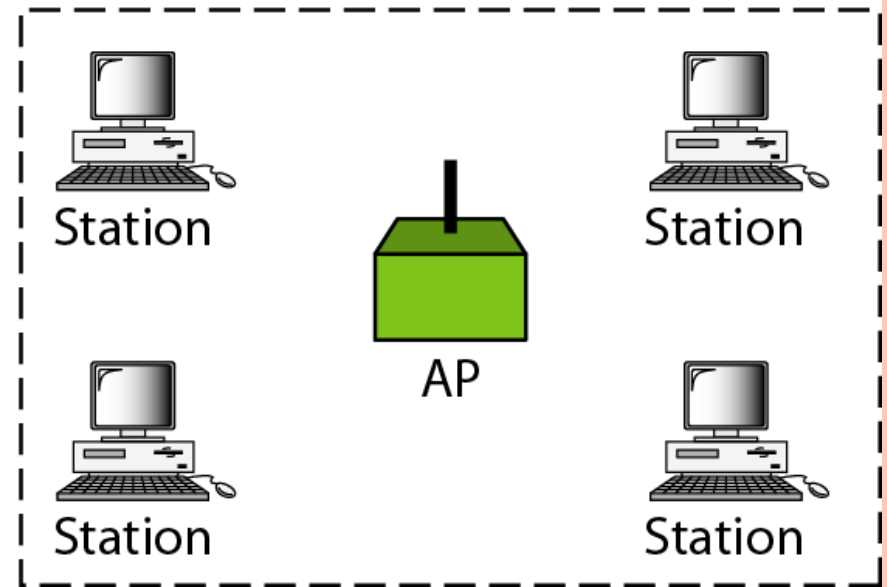
Basic service sets (BSSs)

BSS: Basic service set

AP: Access point



Ad hoc network (BSS without an AP)



Infrastructure (BSS with an AP)

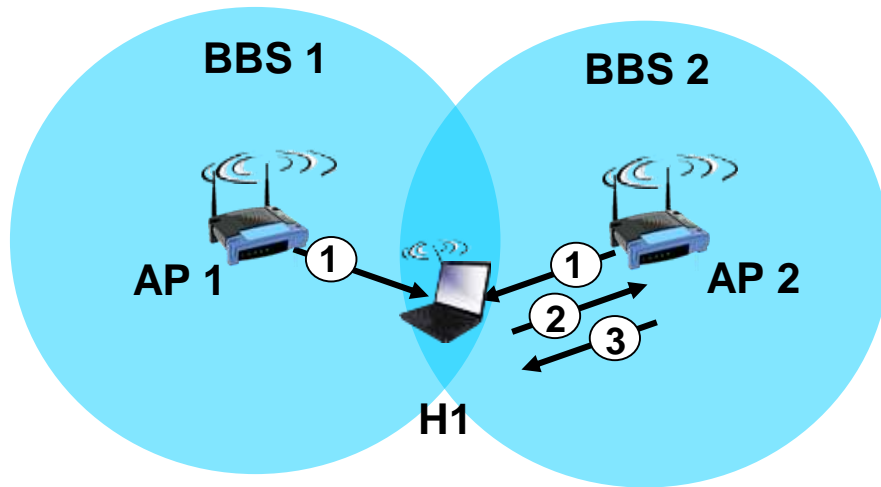


802.11: CHANNELS, ASSOCIATION

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP
- host: must *associate* with an AP
 - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
 - selects AP to associate with
 - may perform authentication
 - will typically run DHCP to get IP address in AP's subnet

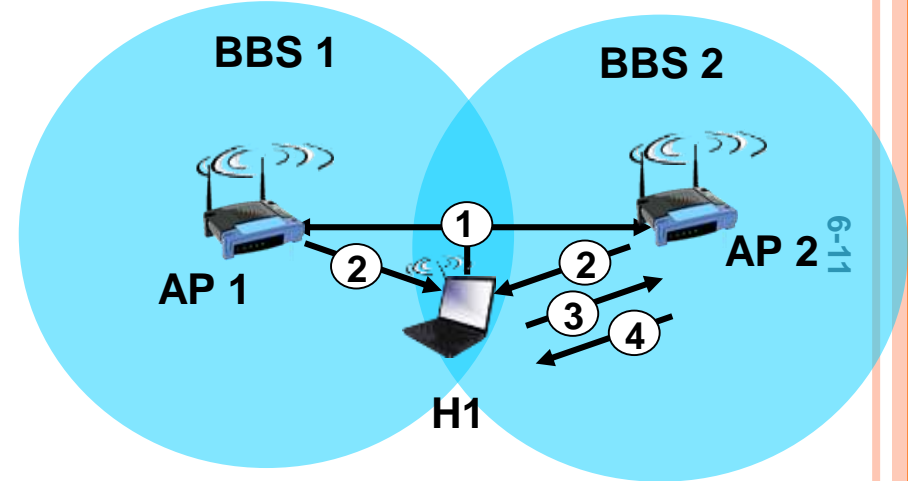


802.11: PASSIVE/ACTIVE SCANNING



passive scanning:

- (1) beacon frames sent from APs
- (2) association Request frame sent: H1 to selected AP
- (3) association Response frame sent from selected AP to H1



active scanning:

- (1) Probe Request frame broadcast from H1
- (2) Probe Response frames sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent from selected AP to H1

THE 802.11 MAC PROTOCOL

- Once a wireless station is associated with an AP, it can start sending and receiving data frames to and from the access point.
- But because multiple stations may want to transmit data frames at the same time over the same channel, **a multiple access protocol is needed to coordinate the transmissions.**
- Here, a **station is either a wireless station or an AP.**



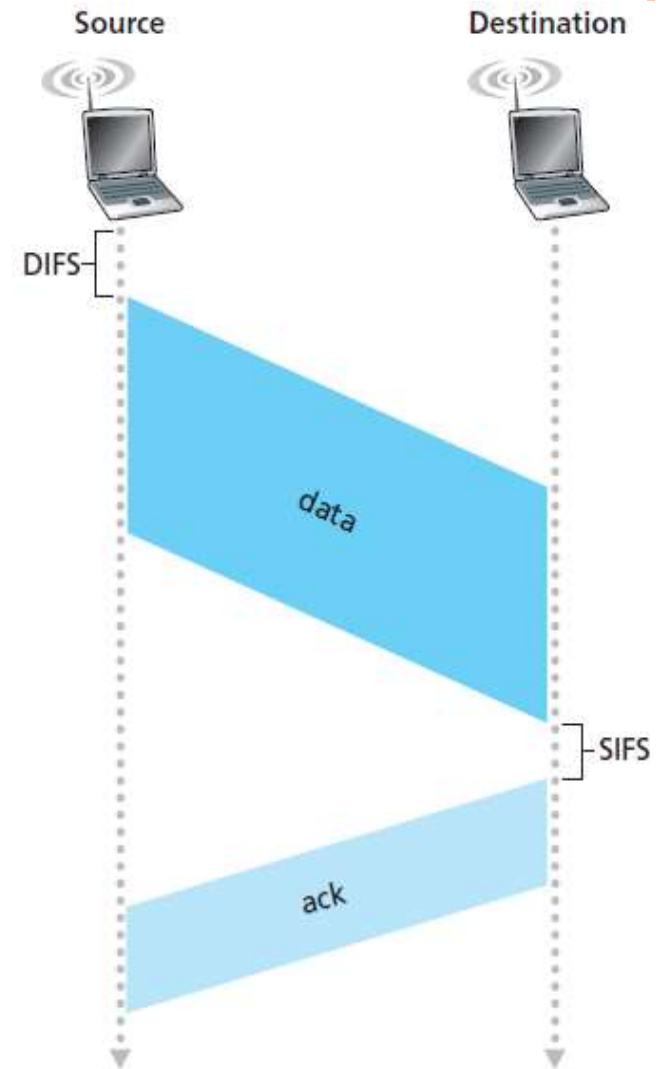
IEEE 802.11: MULTIPLE ACCESS

- avoid collisions: 2⁺ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
 - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
 - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
 - can't sense all collisions in any case: hidden terminal, fading
 - goal: *avoid collisions*: CSMA/C(ollision)A(voidance)



IEEE 802.11 MAC PROTOCOL: CSMA/CA

1. If initially the station senses the channel idle, it transmits its frame after a short period of time known as the **Distributed Inter-frame Space (DIFS)**.
2. Otherwise, the station chooses a random backoff value using binary exponential backoff and counts down this value when the channel is sensed idle. While the channel is sensed busy, the counter value remains frozen.
3. When the counter reaches zero, the station transmits the entire frame and then waits for an acknowledgment.
4. If an acknowledgment is received, the transmitting station knows that its frame has been correctly received at the destination station. If the station has another frame to send, it begins the CSMA/CA protocol at step 2. If the acknowledgment isn't received, the transmitting station reenters the backoff phase in step 2, with the random value chosen from a larger interval.




802.11'S LINK-LAYER ACKNOWLEDGMENT SCHEME

- When a station in a wireless LAN sends a frame, the frame may not reach the destination station intact for a variety of reasons.
- To deal with this non-negligible chance of failure, **the 802.11 MAC protocol uses link-layer acknowledgments.**
- when the destination station receives a frame that passes the CRC, it waits a short period of time known as **the Short Inter-frame Spacing (SIFS)** and then sends back an acknowledgment frame.
- If the transmitting station does not receive an acknowledgment within a given amount of time, it assumes that an error has occurred and retransmits the frame, using the CSMA/CA protocol to access the channel.
- If an acknowledgment is not received after some fixed number of retransmissions, the transmitting station gives up and discards the frame.



IEEE 802.11: MULTIPLE ACCESS

- The goal in 802.11 is thus to avoid collisions whenever possible.
 - In 802.11, if the two stations sense the channel busy, they both immediately enter random backoff, hopefully choosing different backoff values.
 - If these values are indeed different, once the channel becomes idle, one of the two stations will begin transmitting before the other, and
 - (if the two stations are not hidden from each other) the “losing station” will hear the “winning station’s” signal, freeze its counter, and refrain from transmitting until the winning station has completed its transmission.
 - In this manner, a costly collision is avoided.
- 

DEALING WITH HIDDEN TERMINALS: RTS AND CTS

- The 802.11 MAC protocol also includes an optional reservation scheme that helps avoid collisions even in the presence of hidden terminals.
- Both of the wireless stations are within range of the AP (whose coverage is shown as a shaded circle) and both have associated with the AP.
- However, due to fading, the signal ranges of wireless stations are limited .
- Each of the wireless stations is hidden from the other, although neither is hidden from the AP.



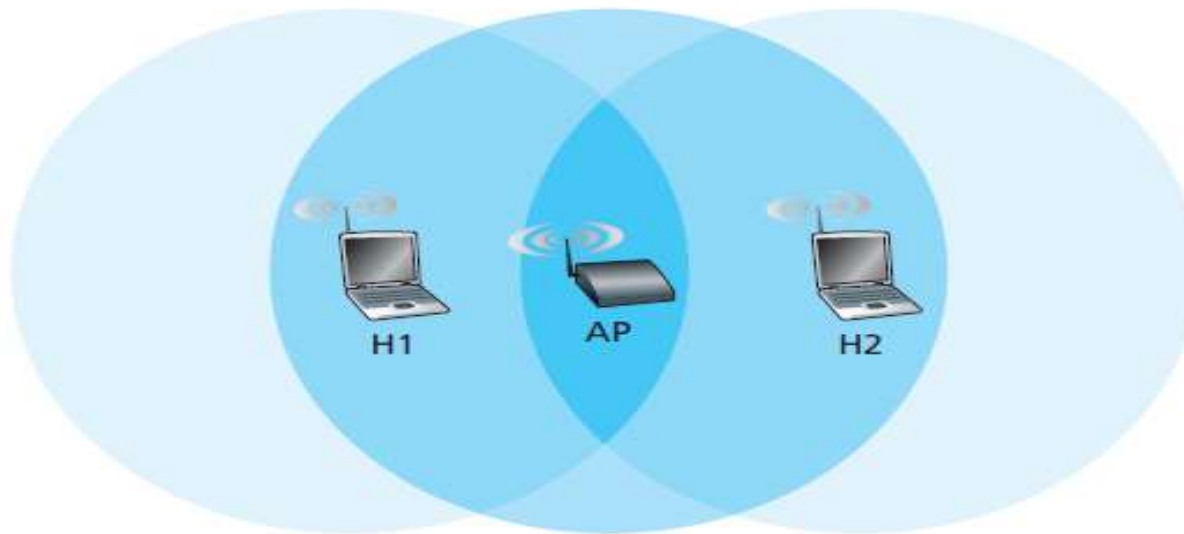


Figure 6.11 ♦ Hidden terminal example: H1 is hidden from H2, and vice versa



DEALING WITH HIDDEN TERMINALS: RTS AND CTS

- Suppose Station H1 is transmitting a frame and halfway through H1's transmission, Station H2 wants to send a frame to the AP.
- H2, not hearing the transmission from H1, will first wait a DIFS interval and then transmit the frame, resulting in a collision.
- The channel will therefore be wasted during the entire period of H1's transmission as well as during H2's transmission.



DEALING WITH HIDDEN TERMINALS: RTS AND CTS

- In order to avoid this problem, the IEEE 802.11 protocol allows a station to use a short **Request to Send (RTS) control frame** and a short **Clear to Send (CTS) control frame** to *reserve access to the channel*.
- *When a sender wants to send a DATA frame*, it can first send an RTS frame to the AP, indicating the total time required to transmit the DATA frame and the acknowledgment (ACK) frame.
- When the AP receives the RTS frame, it responds by broadcasting a CTS frame.
- This CTS frame serves two purposes: It gives the sender explicit permission to send and also instructs the other stations not to send for the reserved duration.



DEALING WITH HIDDEN TERMINALS: RTS AND CTS

- Thus, before transmitting a DATA frame, H1 first broadcasts an RTS frame, which is heard by all stations in its circle, including the AP.
- The AP then responds with a CTS frame, which is heard by all stations within its range, including H1 and H2.
- Station H2, having heard the CTS, refrains from transmitting for the time specified in the CTS frame.



RTS AND CTS

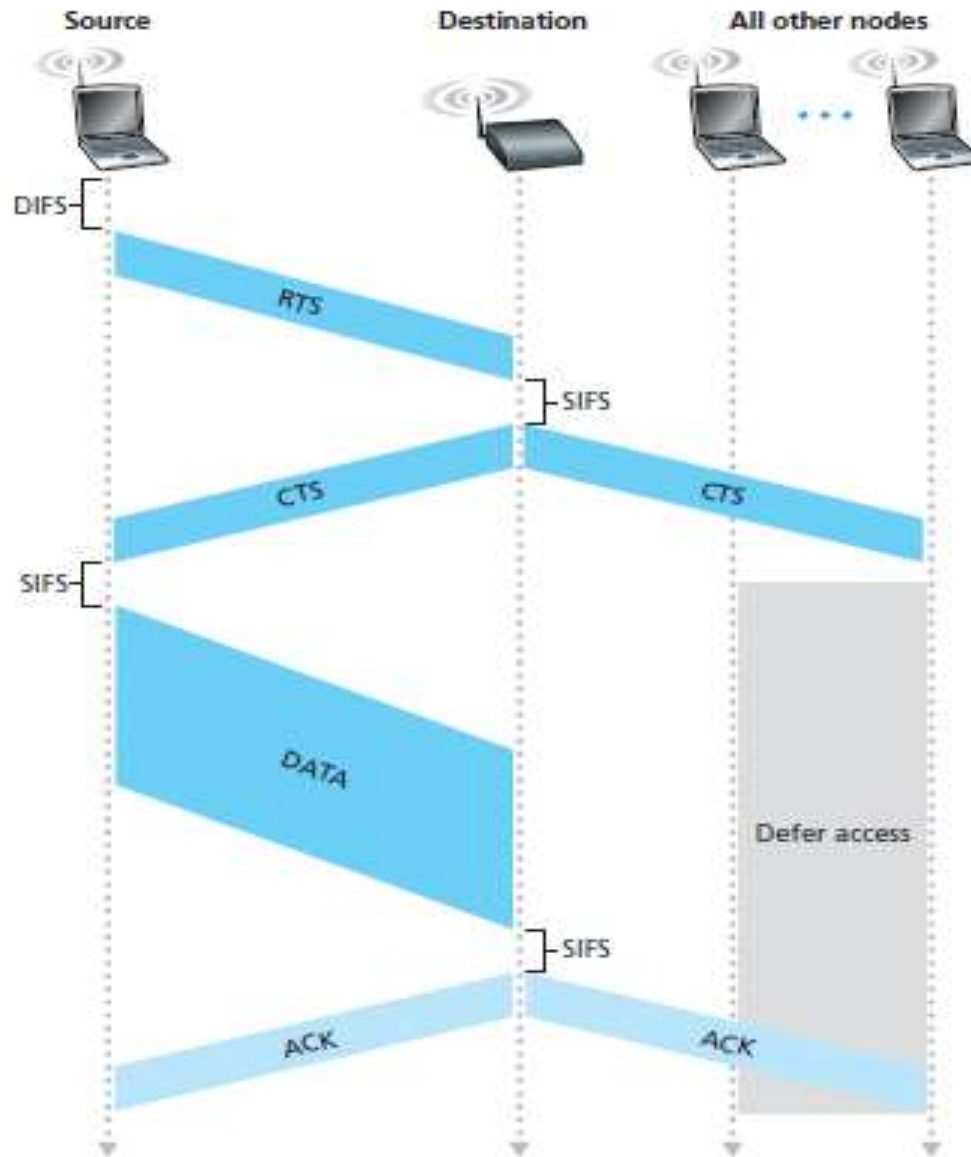


Figure 6.12 • Collision avoidance using the RTS and CTS frames

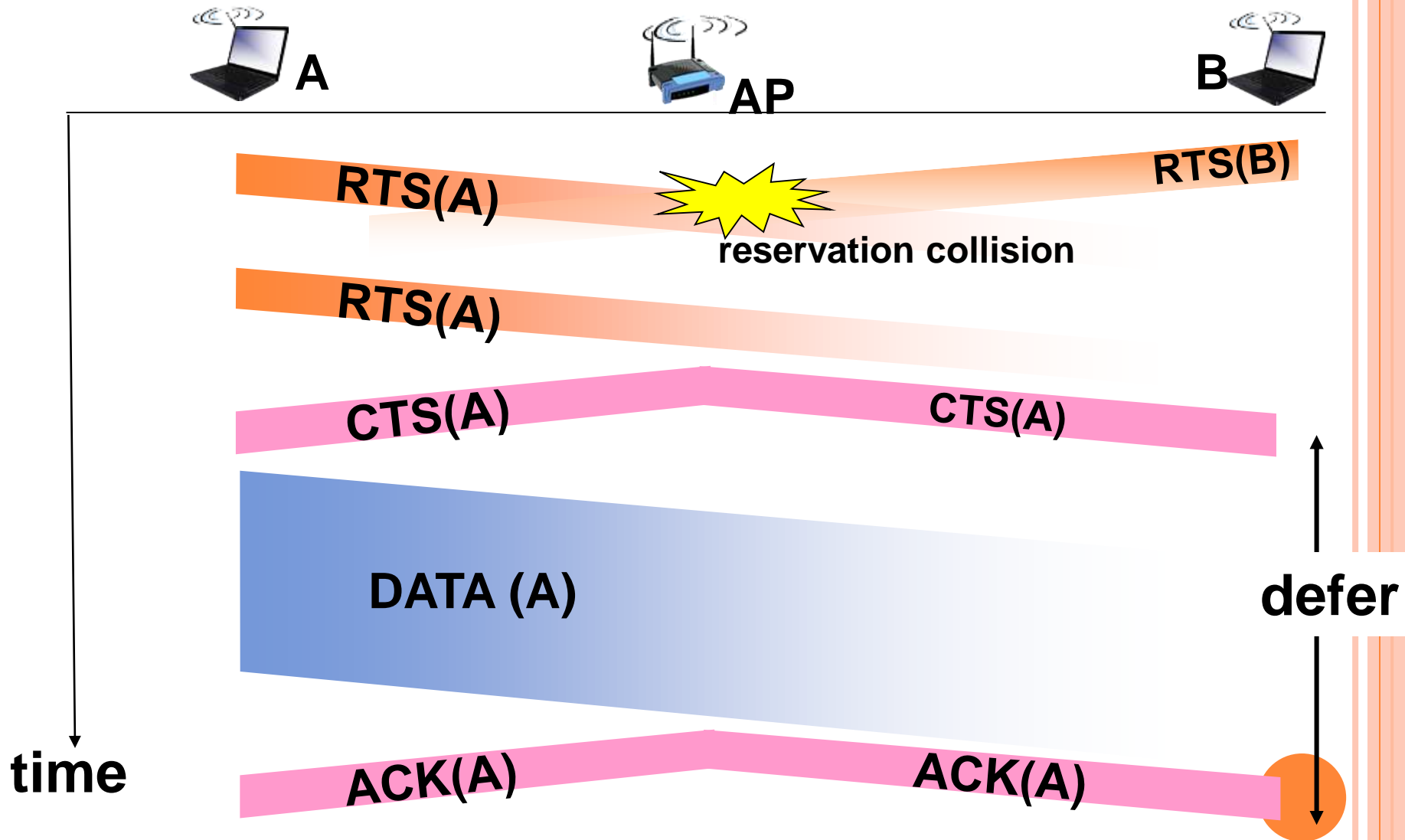


RTS AND CTS

- The use of the RTS and CTS frames can improve performance in two important ways:
 1. The hidden station problem is mitigated, since a long DATA frame is transmitted only after the channel has been reserved.
 2. Because the RTS and CTS frames are short, a collision involving an RTS or CTS frame will last only for the duration of the short RTS or CTS frame. Once the RTS and CTS frames are correctly transmitted, the following DATA and ACK frames should be transmitted without collisions.

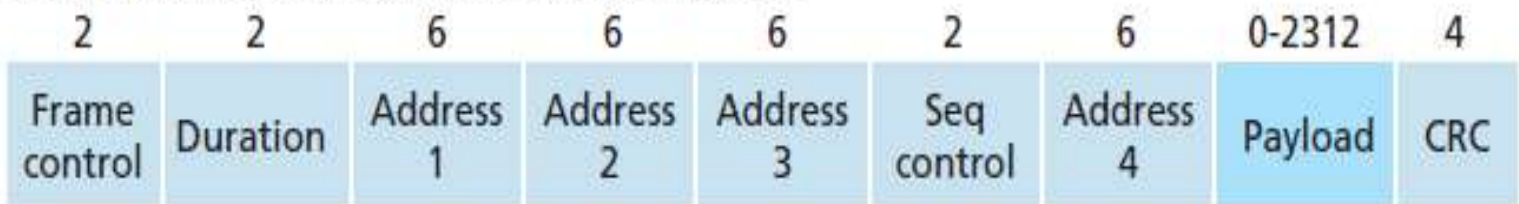


COLLISION AVOIDANCE: RTS-CTS EXCHANGE



THE IEEE 802.11 FRAME

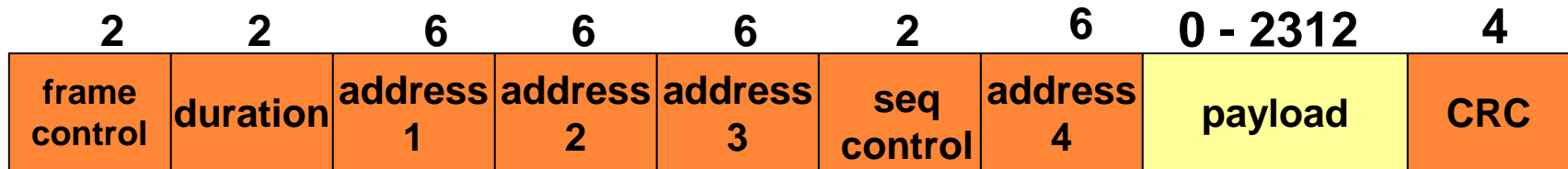
Frame (numbers indicate field length in bytes):



Frame control field expanded (numbers indicate field length in bits):



802.11 | FRAME: ADDRESSING



Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode



THE IEEE 802.11 FRAME: ADDRESS FIELD

- AP → Wireless Station (Add 1: MAC Address of Wireless Station)
- Wireless Station → AP (Add 1: MAC Address of AP)
- **Address 1 is the MAC address of the wireless station that is to receive the frame.**
- Thus if a mobile wireless station transmits the frame, address 1 contains the MAC address of the destination AP.
- Similarly, if an AP transmits the frame, address 1 contains the MAC address of the destination wireless station.



THE IEEE 802.11 FRAME: ADDRESS FIELD

- AP → Wireless Station (Add 2: MAC Address of AP)
- Wireless Station → AP (Add 2: MAC Address of Wireless Station)
- **Address 2 is the MAC address of the station that transmits the frame.**
- Thus, if a wireless station transmits the frame, that station's MAC address is inserted in the address 2 field.
- Similarly, if an AP transmits the frame, the AP's MAC address is inserted in the address 2 field.



THE IEEE 802.11 FRAME: ADDRESS FIELD

- To understand address 3, recall that the BSS (consisting of the AP and wireless stations) is part of a subnet, and that this subnet connects to other subnets via some router interface.
- Address 3 contains the MAC address of this router interface.



THE IEEE 802.11 FRAME: ADDRESS FIELD

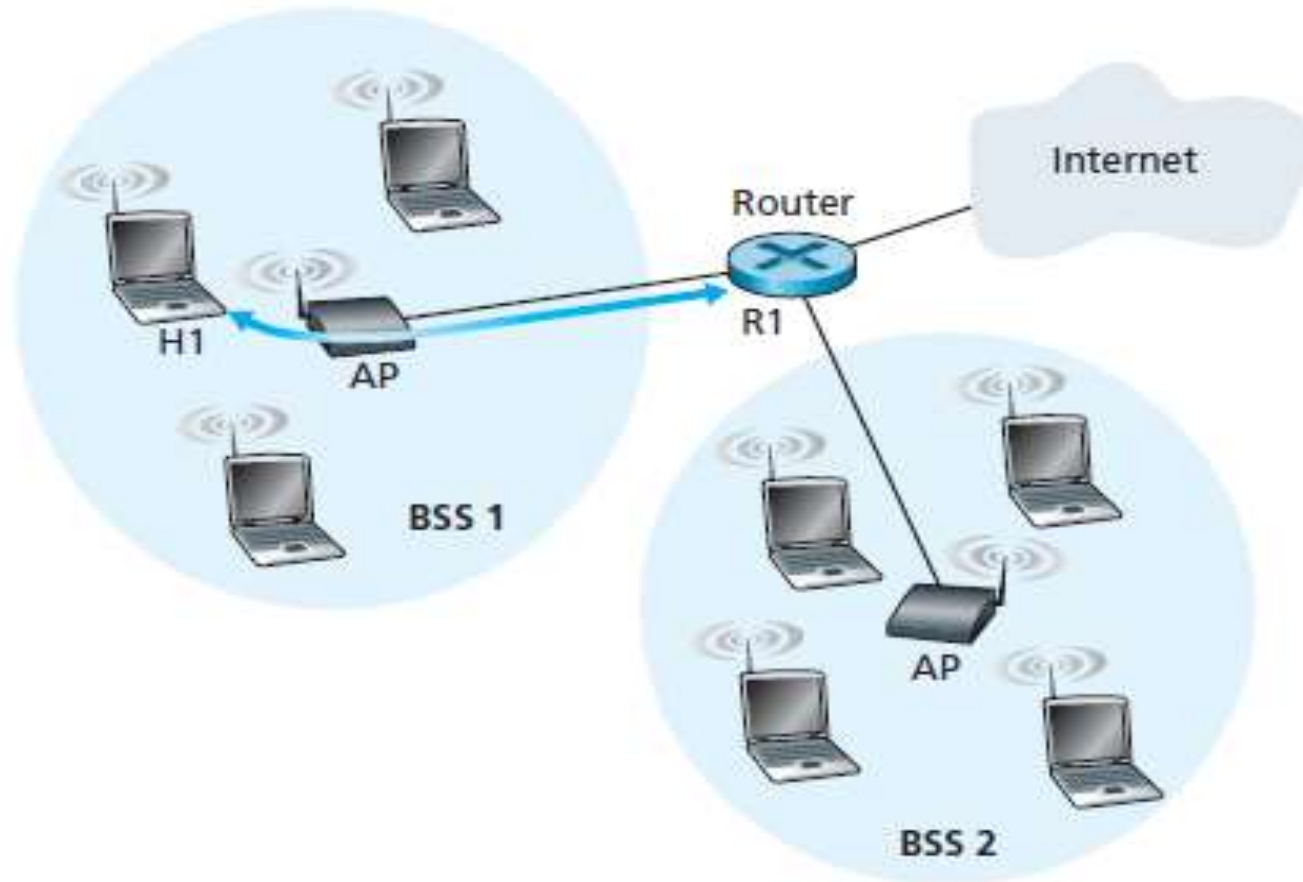


Figure 6.14 ♦ The use of address fields in 802.11 frames: Sending frames between H1 and R1



SEQUENCE NUMBER, DURATION, AND FRAME CONTROL FIELDS

- Recall that in 802.11, whenever a station correctly receives a frame from another station, it sends back an acknowledgment.
- Because acknowledgments can get lost, the sending station may send multiple copies of a given frame.
- The use of sequence numbers allows the receiver to distinguish between a newly transmitted frame and the retransmission of a previous frame.
- The sequence number field in the 802.11 frame thus serves exactly the same purpose here at the link layer



SEQUENCE NUMBER, DURATION, AND FRAME CONTROL FIELDS

- Recall that the 802.11 protocol allows a transmitting station to reserve the channel for a period of time that includes the time to transmit its data frame and the time to transmit an acknowledgment.
- This duration value is included in the frame's duration field (both for data frames and for the RTS and CTS frames).



FRAME CONTROL FIELDS

- The *type and subtype fields* are used to distinguish the association, RTS, CTS, ACK, and data frames.
- The to and from fields are used to define the meanings of the different address fields. (These meanings change depending on whether ad hoc or infrastructure modes are used and, in the case of infrastructure mode, whether a wireless station or an AP is sending the frame.)
- Finally the WEP field indicates whether encryption is being used or not.



BLUETOOTH

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.

A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.



BLUETOOTH ARCHITECTURE

○ Piconet

- Each piconet has one master and up to 7 simultaneous slaves
 - Master : device that initiates a data exchange.
 - Slave : device that responds to the master

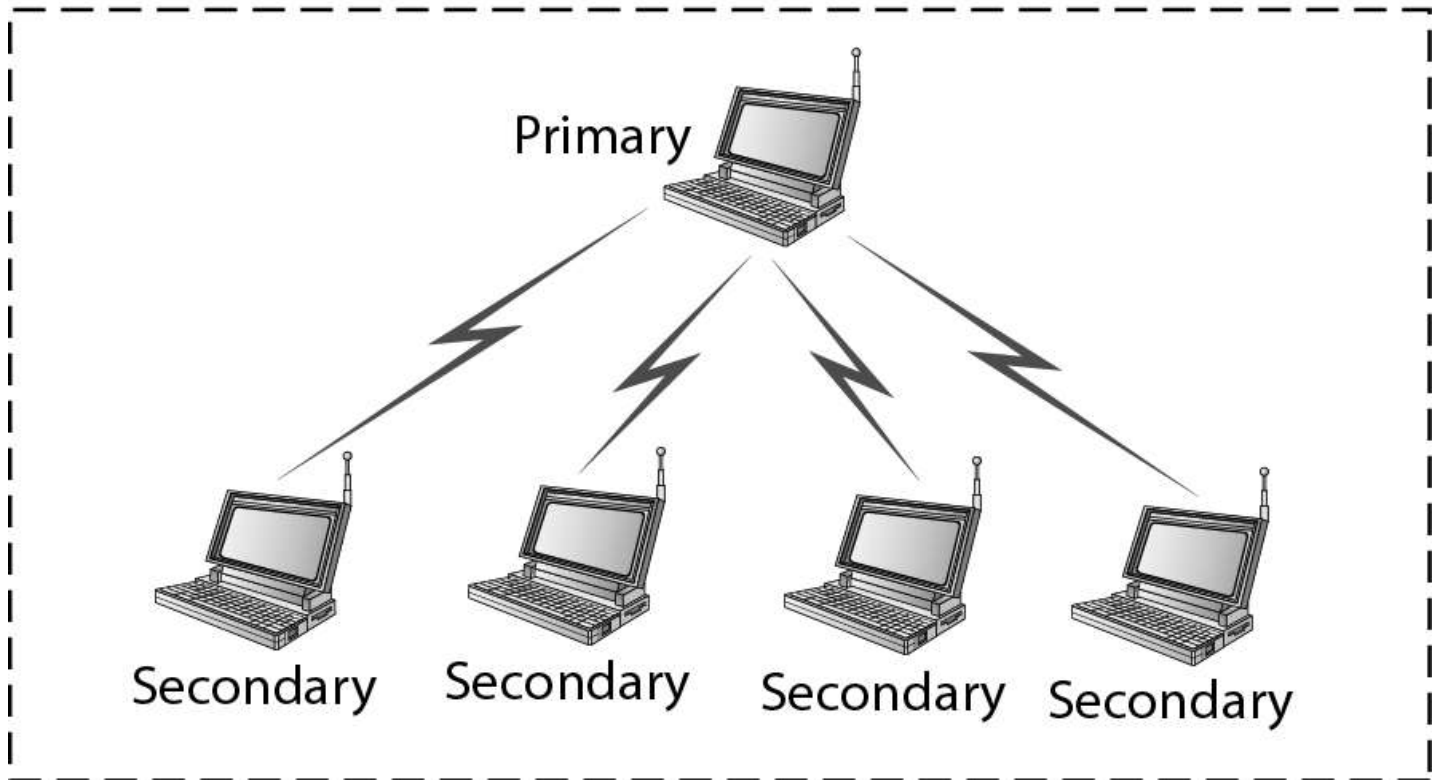
○ Scatternet

- Linking of multiple piconets through the master or slave devices
- Bluetooth devices have point-to-multipoint capability to engage in Scatternet communication.



Piconet

Piconet



Scatternet

