University of Science and Technology

Faculty of Computer Science and Information Technology

Information Technology Department

Computer Networking: Lecture (9)

Instructor: Prof. Dr. Noureldien Abdelrahman Date 16/4/2016

The IEEE 802.11 Frame

Although the 802.11 frame shares many similarities with an Ethernet frame, it also contains a number of fields that are specific to its use for wireless links. The 802.11 frame is shown in Figure 6.13.

The numbers above each of the fields in the frame represent the lengths of the fields in *bytes*; the numbers above each of the subfields in the frame control field represent the lengths of the subfields in *bits*.

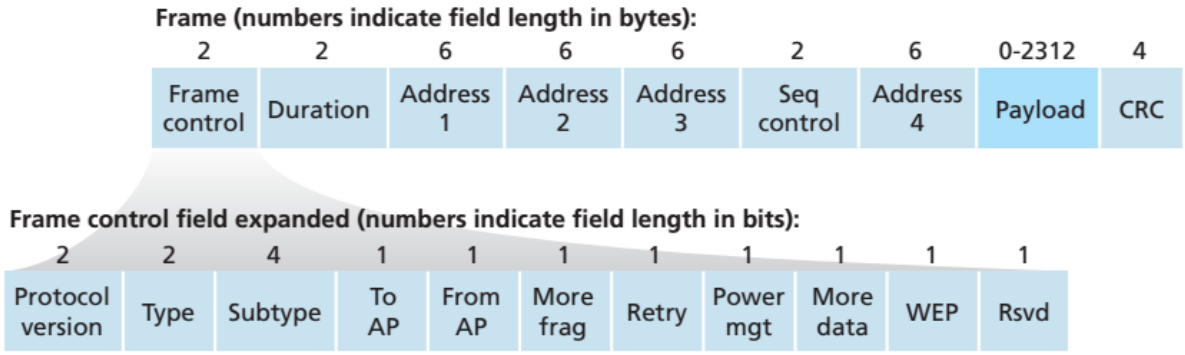

Figure 6.13 ♦ The 802.11 frame

- **Payload and CRC Fields**

At the heart of the frame is the payload, which typically consists **of an IP datagram or an ARP packet.** Although the field is permitted to be as long **as 2,312 bytes, it is typically fewer than 1,500 bytes, holding an IP datagram or an ARP packet**.

As with an Ethernet frame, an 802.11 frame includes a 32-bit cyclic redundancy check (CRC) so that the receiver can detect bit errors in the received frame.

- **Address Fields**

Perhaps the most striking difference in the 802.11 frame is **that *it has four address fields*, each of which can hold a 6-byte MAC address.**

 **But why four address fields?**

 **Don't a source MAC field and destination MAC field suffice, as they do for Ethernet?**

The answer is:

Three address fields are needed for internetworking purposes—specifically, for moving the **network-layer datagram from a wireless station through an AP to a router interface**.

The fourth address field is used when APs forward frames to each other in ad hoc mode.

The 802.11 standard defines these fields as follows:

- 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.

- 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.

- 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.

In figure 6.14, there are two APs, each of which is responsible for a number of wireless stations. Each of the APs has a direct connection to a router, which in turn connects to the global Internet.

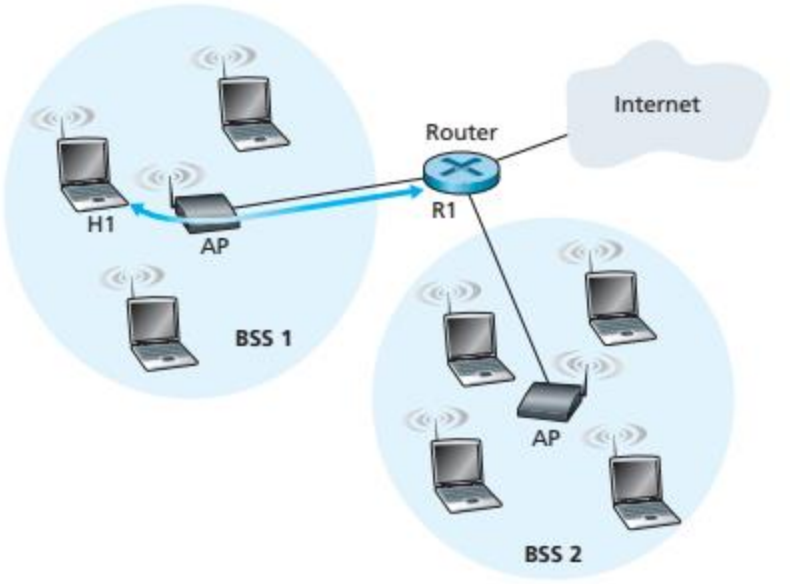

Figure 6.14 ♦ The use of address fields in 802.11 frames: Sending frames between H1 and R1

Consider now moving a datagram from the router interface R1 to the wireless Station H1.

- The router, which knows the IP address of H1 (from the destination address of the datagram), uses ARP to determine the MAC address of H1, just as in an ordinary Ethernet LAN. After obtaining H1's MAC address, router interface R1 encapsulates the datagram within an Ethernet frame. The source address field of this frame contains R1's MAC address, and the destination address field contains H1's MAC address.

- **When the Ethernet frame arrives at the AP, the AP converts the 802.3 Ethernet frame to an 802.11 frame**

before transmitting the frame into the wireless channel. The AP fills **in address 1 and address 2 with H1's MAC address and its own MAC address, respectively**, as described above. For addreSS 3, the AP inserts the MAC address of R1. In this manner, H1 can determine (from address 3) the MAC **address of the router interface that sent the datagram into the subnet.**

Now what happens when the wireless station H1 responds by moving a datagram from H1 to R1.

- H1 **creates an 802.11 frame, filling the fields for address 1 and address 2 with the AP's MAC address and H1's MAC address, respectively, as described above. For address 3, H1 inserts R1's MAC address.**

- When **the AP receives the 802.11 frame, it converts the frame to an Ethernet frame. The source address field for this frame is H1's MAC address, and the destination address field is R1's MAC address.**

Thus, address 3 allows the AP to determine the appropriate destination MAC address when constructing the Ethernet frame.

In summary, address 3 plays a crucial role for internetworking the BSS with a wired LAN.

- **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.

To distinguish between a newly transmitted frame and the retransmission of a previous frame, the sequence number field in the 802.11 frame is used.

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).

As shown in Figure 6.13, the frame control field includes many subfields. **We'll say just a few words about some of the more important s**ubfields:

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.