Week 10: Wireless Local Area Network

EE3017/IM2003 Computer Communications

School of Electrical and Electronic Engineering

Prof. Cheng Tee Hiang
Room: S1-B1a-29
Email: ethcheng@ntu.edu.sg
Phone: 6790-4534

Topic Outline
(Updated in January 2020)

Topic Outline

Wireless Local Area Network (WLAN)

- Introduction to WLAN
- IEEE 802.11 Standards
- Network Topology
- MAC Services
- IEEE 802.11 Frame Structure

Recommended reading:
Section 6.3, Pages 562 to 580 of the recommended textbook
(Page numbers are based on 5th or 2010 Edition.)

Learning Objectives

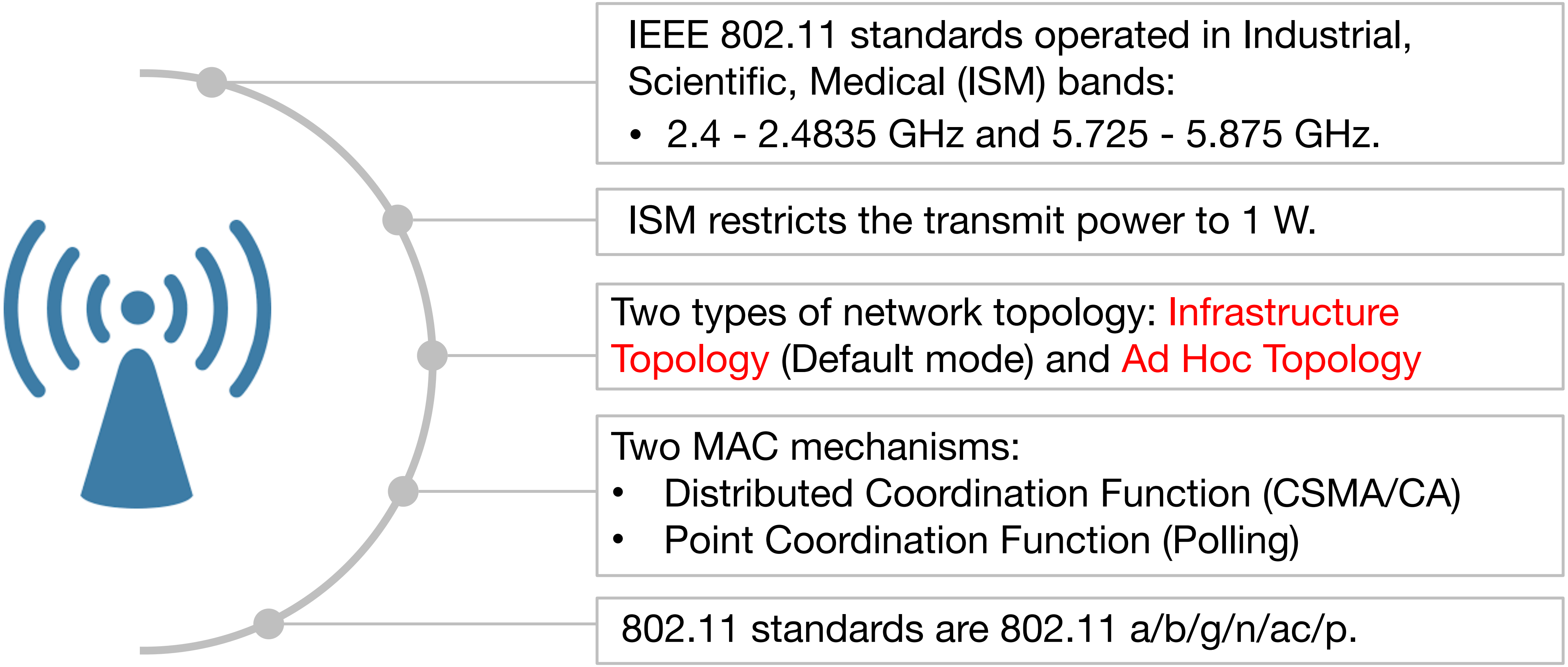
Learning Objectives

By the end of this topic, you should be able to:

- Explain the key differences of major IEEE 802.11 standards.
- Explain the differences between infrastructure topology and ad hoc topology.
- Explain the Distributed Coordination Function; i.e., the CSMA/CA protocol.
- Explain the Point Coordination Function.
- Explain the functions of the various fields in the IEEE 802.11 frames.

Introduction to WLAN

Introduction to WLAN



IEEE 802.11 standards operated in Industrial, Scientific, Medical (ISM) bands:

- 2.4 - 2.4835 GHz and 5.725 - 5.875 GHz.

ISM restricts the transmit power to 1 W.

Two types of network topology: Infrastructure Topology (Default mode) and Ad Hoc Topology

Two MAC mechanisms:

- Distributed Coordination Function (CSMA/CA)
- Point Coordination Function (Polling)

802.11 standards are 802.11 a/b/g/n/ac/p.

802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Notes: Introduction to WLANs

- IEEE 802.11 wireless LAN is also commonly known as Wi-Fi or WiFi. It operates in the Industrial, Scientific, Medical (ISM) band, which limits the maximum transmitter output power, fed into the antenna, to 1 watt (30 dBm).

- Wireless LANs that deploy access points (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.

- IEEE 802.11 stations can also group themselves together to form an ad hoc network – a network with no central control and no connections to the 'outside world'. An ad hoc network might be formed when people with laptops and smart phones get together; for example, in a meeting room, and want to exchange data in the absence of an AP.

We will focus on the infrastructure mode but will also briefly discuss about the ad hoc mode in this module.

Notes: Introduction to WLANs

- IEEE 802.11 supports two medium access control (MAC) protocols; i.e., Distributed Control Function (DCF) based on Carrier-sense Multiple Access/ Collision Avoidance (CSMA/CA) and Point Coordination Function (PCF) but PCF is rarely used in practice.

- DCF is based on CSMA/CA and contention based while PCF is based on polling and non-contention based.

- 802.11a and 802.11b are the earlier standards, 802.11g was standardised in 2003. Dual-mode (802.11a/g) and tri-mode (802.11a/b/g) are also available.

- 802.11n is a new standard which uses multiple-input multiple-output (MIMO) antennas, which allow the data rate to scale up to 600 Mbps. 802.11ac is the newest standard for a 1Gbps WLAN.

- 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE) for Intelligent Transportation Systems (ITS) applications. It uses the licensed ITS band of 5.9 GHz (5.85 - 5.925 GHz).

Infrastructure Topology

Infrastructure Topology

- Wireless stations may act as clients using wireless cards and WLAN access point (AP) acts as a server.

- The AP may connect to the Internet.

- An AP covers an area with a number of wireless stations and collectively they are called the Basic Service Set (BSS).

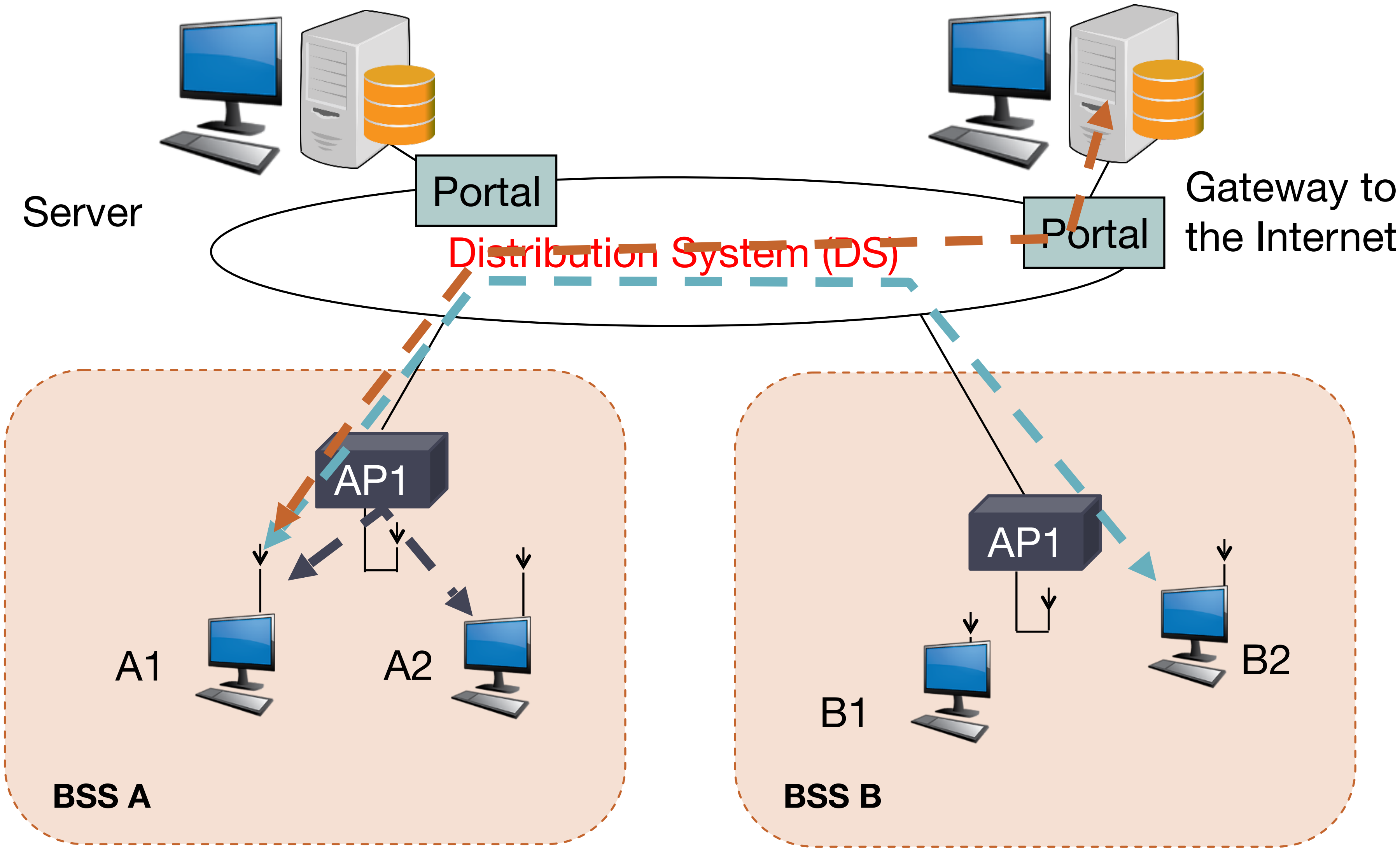
- Wireless stations communicate with each other or Internet through the AP.

- A station sends the message to AP, which then forwards the message to the destination based on the MAC address of the destination.

- Stations and AP use 48-bit MAC address.

- The Service Set Identifier (SSID) and channel number are configured by the administrators.

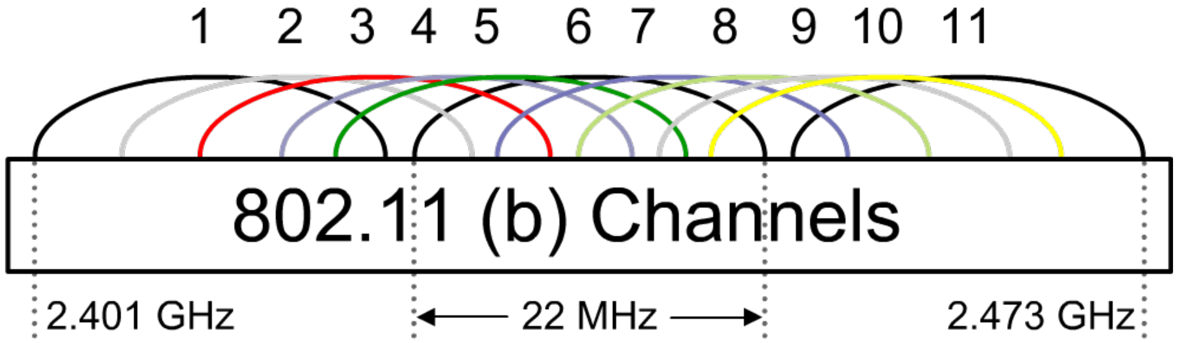
Infrastructure Network



IEEE 802.11 Standards

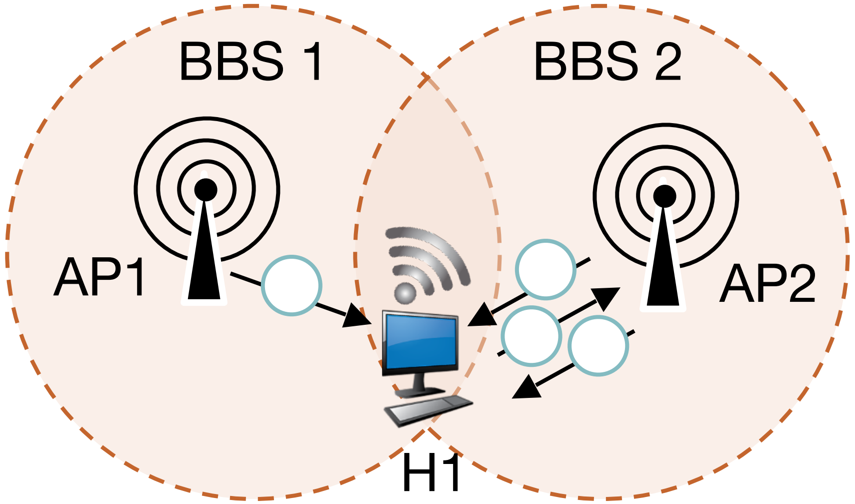
802.11: Channels, association

- E.g., 802.11b: 2.4G Hz - 2.485 GHz 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!



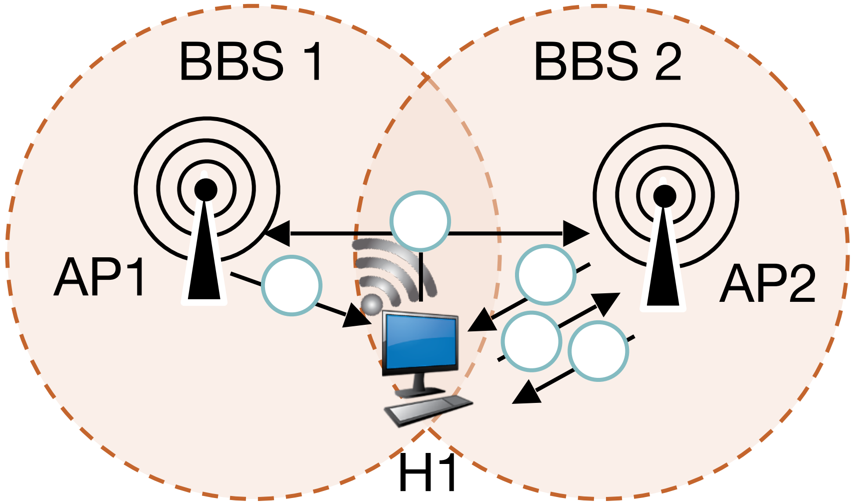
- Host: must associate with an AP
  - Scans channels, listening for beacon frames containing AP’s name (SSID) and MAC address.
  - Selects AP to associate with.
  - May perform authentication.
  - Will typically run DHCP to get IP address in AP’s subnet.

802.11: Passive/Active Scanning



Passive Scanning

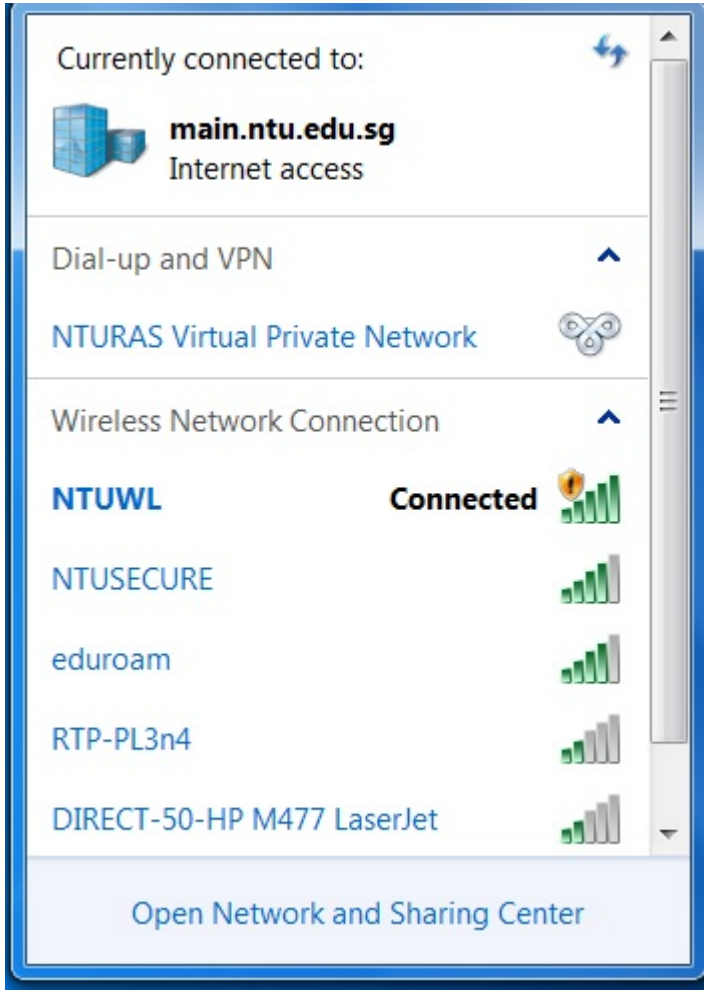
1) Beacon frames sent from APs.
2) Association Request frame sent: H1 to selected AP.
3) Association Response frame sent: selected AP to H1.



Active Scanning

1) Probe Request frame broadcast from H1.
2) Probes response frame sent from APs.
3) Association Request frame sent: H1 to selected AP.
4) Association Response frame sent: selected AP to H1.

Sample Screenshot



Currently connected to:

main.ntu.edu.sg
Internet access

Dial-up and VPN

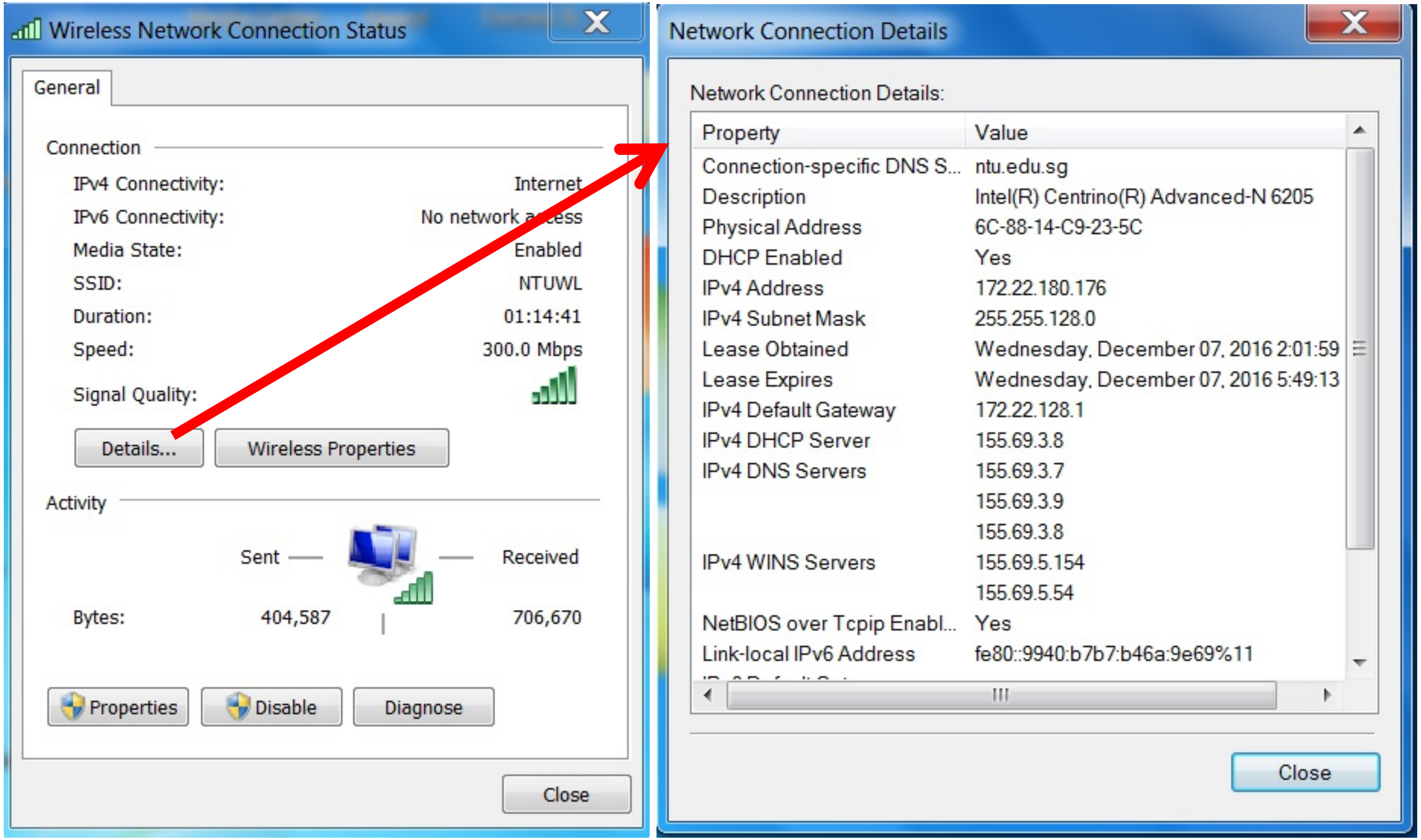
NTURAS Virtual Private Network

Wireless Network Connection

NTUWL	**Connected**
NTUSECURE	
eduroam	
RTP-PL3n4	
DIRECT-50-HP M477 LaserJet	

Open Network and Sharing Center

Sample Screenshot



Connection

IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
SSID: NTUWL
Duration: 01:14:41
Speed: 300.0 Mbps
Signal Quality:

Activity

Sent — Received
Bytes: 404,587 | 706,670

Network Connection Details:

Property	Value
Connection-specific DNS S...	ntu.edu.sg
Description	Intel(R) Centrino(R) Advanced-N 6205
Physical Address	6C-88-14-C9-23-5C
DHCP Enabled	Yes
IPv4 Address	172.22.180.176
IPv4 Subnet Mask	255.255.128.0
Lease Obtained	Wednesday, December 07, 2016 2:01:59
Lease Expires	Wednesday, December 07, 2016 5:49:13
IPv4 Default Gateway	172.22.128.1
IPv4 DHCP Server	155.69.3.8
IPv4 DNS Servers	155.69.3.7 155.69.3.9 155.69.3.8
IPv4 WINS Servers	155.69.5.154 155.69.5.54
NetBIOS over Tcpip Enabl...	Yes
Link-local IPv6 Address	fe80::9940:b7b7:b46a:9e69%11

Notes: Infrastructure mode

- When an AP is installed, the administrator assigns a one or two-word Service Set Identifier (SSID) and a channel number. The SSID serves to identify the AP while the channel number dictates a specific frequency channel among a number of available frequency channels to use. For example, 802.11b operates in the frequency range of 2.4 GHz to 2.485 GHz, and within this 85 MHz band, 11 partially overlapping channels are defined.

- The backbone network, which could be an Ethernet or another LAN technology, that connects various APs is known as the Distributed System (DS).

- The MAC addresses of WLAN network interface cards (NICs) in the AP and wireless stations are 48 bits, the same as those of Ethernet NICs.

- Normally a wireless station is able to receive strong signals from many APs in the vicinity due to the widespread deployment of WLANs. To gain Internet access, the station needs to associate with exactly one of the APs. Association means the station creates a virtual wire between itself and the AP.

Notes: Scanning and Association

- The 802.11 standard requires that an AP periodically sends beacon frames, each of which include the AP's SSID and MAC address.
- The wireless station, knowing that APs are sending out beacon frames, scans all the available channels, seeking beacon frames from any APs that may be out there and selects one of the APs for association. The process of scanning channels and listening for beacon frames is known as passive scanning.
- Note that the 802.11 standard does not specify the algorithm for selecting which of the available APs to associate with; that algorithm is left up to the designers of the 802.11 firmware and software. Most implementation allows the human user to intervene by manually selecting the AP to be associated with.
- A wireless station can also perform active scanning by broadcasting a probe frame that will be received by all APs within the station's range. The station can then choose the AP with which to associate from among the responding APs.

Notes: Scanning and Association

- After selecting the AP with which to associate, the wireless host sends an association request frame to the AP, and the AP responds with an association response frame.

- Once associated with an AP, the wireless station will want to join the IP subnet to which the AP belongs. Thus, the host will typically send a Dynamic Host Configuration Protocol (DHCP) discovery message into the subnet via the AP in order to obtain an IP address on the subnet.

- Once the address is obtained, the mobile station (MS) will have access to the Internet.

- Note that in order to create an association with a particular AP the wireless station may be required to authenticate itself to the AP.

- *Several screenshots of the WLAN connection of my laptop are captured and shown. You are encouraged to look at these screenshots and compare with what you have learned.*

Ad Hoc Topology

Ad Hoc Topology

- Provide communication between a number of terminals as an ad hoc, free-style connection, network using peer-to-peer communication.

- No AP is needed.

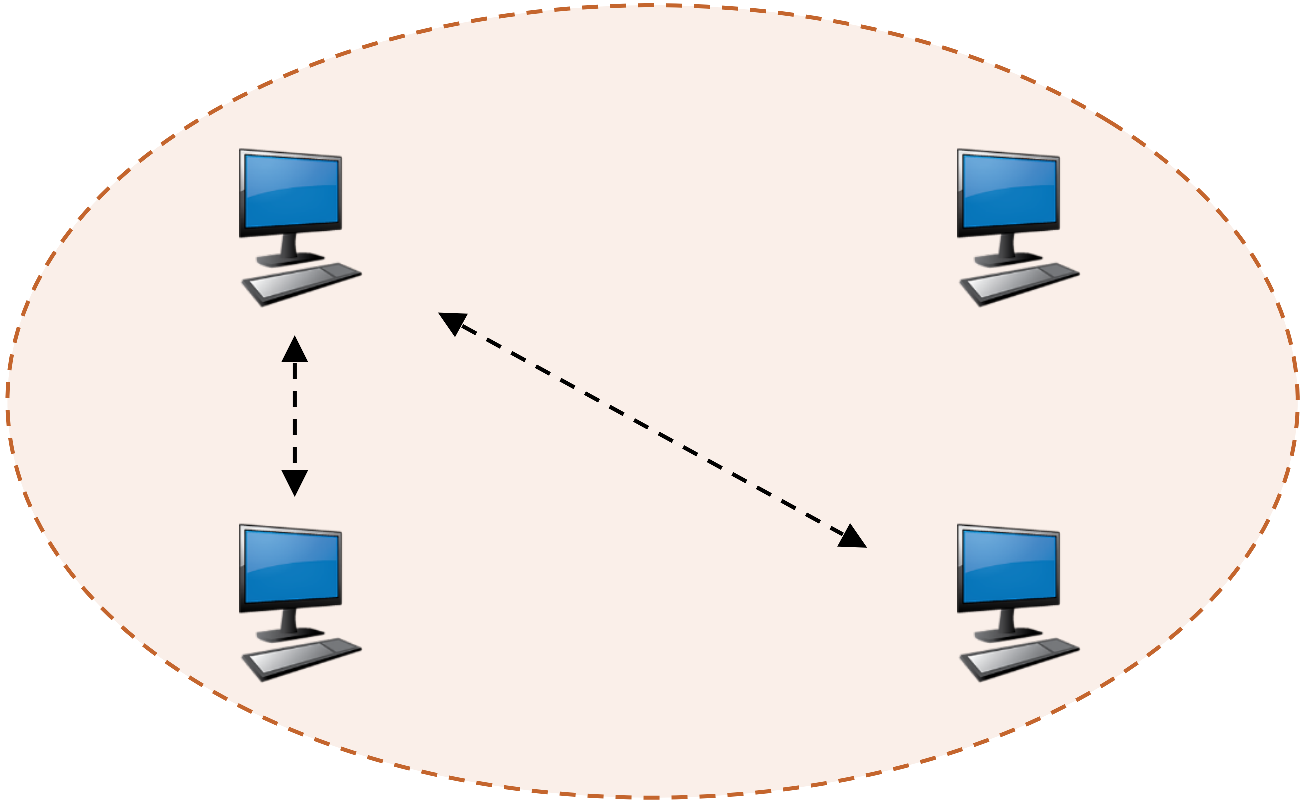
- Wireless stations can directly communicate with each other only within the transmission range.

- All these stations form an independent BSS (IBSS).

Ad Hoc Communications

Temporary association of group of stations

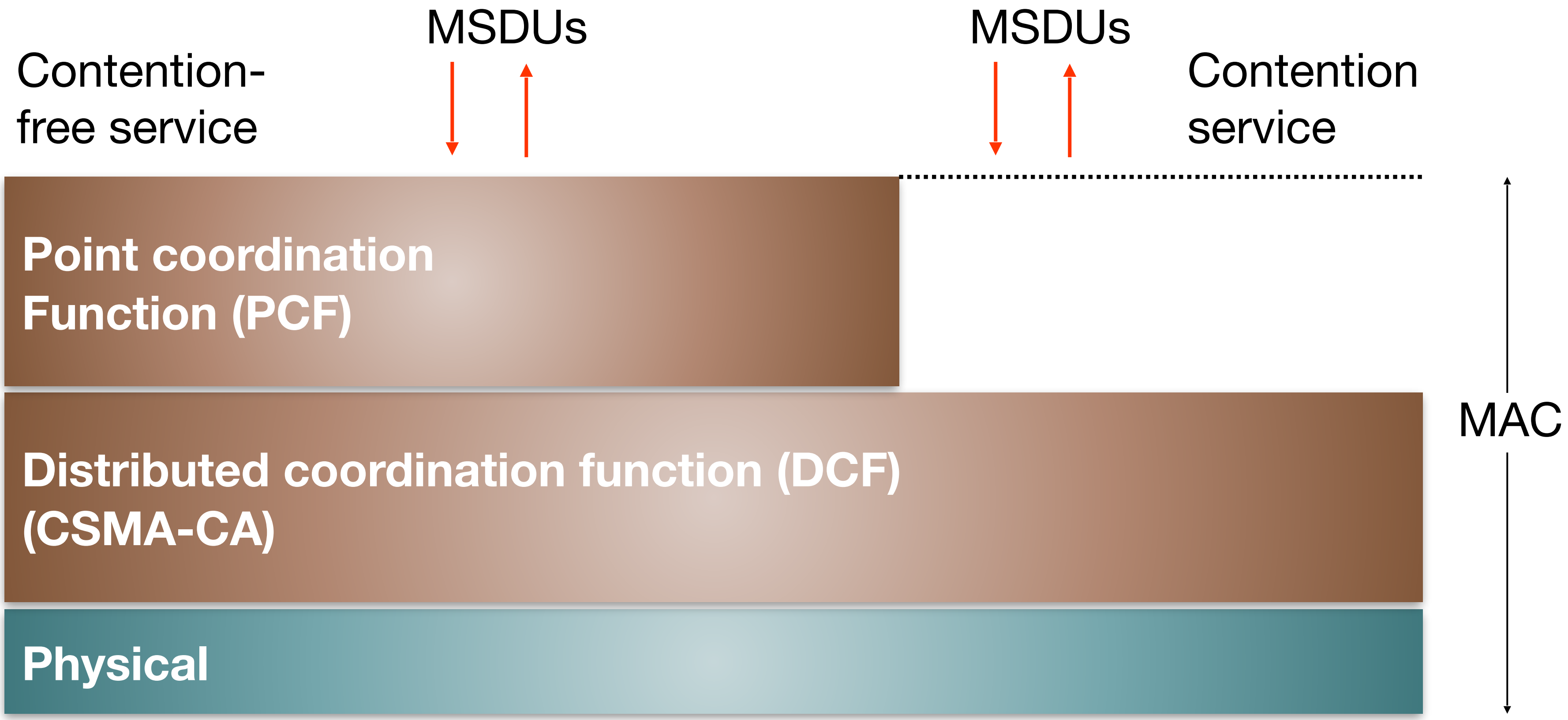
- Within range of each other.
- Need to exchange information.
- E.g. Presentation in meeting, or distributed computer game, or both.



MAC Services

Ethernet: Unreliable, Connectionless

- DCF – Contention-based Access
- PCF – Contention-free Access
- MAC can alternate between Contention Periods (CPs) and Contention-Free Periods (CFPs).


MSDUs
MSDUs
Contention-free service
Contention service
Point coordination Function (PCF)
Distributed coordination function (DCF) (CSMA-CA)
Physical
MAC

Notes: WLAN MAC Services

- Both DCF and PCF are 802.11 medium access types. DCF stands for Distributed Coordination Function and PCF stands for Point Coordination Function.

- DCF is contention-based and is based on the Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol while PCF is non-contention based and operates over the DCF.

- To gain priority over standard contention based services, the PCF allows stations to transmit frames after a shorter interval. The PCF is not widely implemented.

- When the PCF is used, time on the medium is divided into the contention-free period (CFP) and the contention period (CP). Access to the medium during the CFP is controlled by the PCF, while access to the medium during the CP is controlled by the DCF. Basically the PCF will make use of DCF to secure the medium for a period of time and in this time period, use the polling mechanism to grant access to different wireless stations.

DCF
CSMA with Collision Avoidance
(CSMA/CA)

Dealing with Hidden Terminals

Dealing with Hidden Terminals

Notes: Hidden Terminals

- A hidden terminal problem is the problem in which two wireless stations (MSs) are within range of an AP and associated with it but the stations are hidden from each other. This may pose a problem because when one of the stations is transmitting to the AP, the other station will not be aware of the transmission and may also start to transmit; as a result, the AP will not be able to receive the transmissions from both stations correctly.

- In the CSMA/CA protocol, each station is required to use a short Request-to-Send (RTS) control frame to reserve access to the channel for a specific period of time. When the AP receives the RTS frame correctly, it broadcasts a short Clear-to-Send (CTS) control frame. The CTS frame serves two purposes: It gives the requesting station explicit permission to send and also instructs the other stations not to send for the reserved duration.

- After the data frame sent by the station is correctly received by the AP, the AP will broadcast an acknowledgement (ACK) to inform the sender of the reception of the data frame and signals to all the other stations the completion of the sender’s transmission.

Collision Avoidance (CA)

Idea: Allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- Sending station first transmits short RTS frames using CSMA.
  - RTSs may still collide with each other (but they're short).

- Receiving station broadcasts CTS in response to RTS.

- CTS heard by all nodes.
  - Reserves channel for sender, notifying (possibly hidden) stations.
  - Sender transmits data frame.
  - Other stations defer transmissions.

- Avoid hidden station collisions.

! Avoid data frame collisions by using small reservation packets!

Binary Exponential Backoff

- When a station senses that the channel is busy, it waits until the channel becomes idle for DIFS period and then allows the Backoff Time Counter (BTC) to count down -- BTC decrements by one every time a period equal to slot time elapses.

- When the BTC counts down to zero, a wireless station is allowed to start transmission using the RTS-CTS process.

- If the transmission is unsuccessful, BTC is regenerated randomly with the range of backoff values (contention Window or CW) doubling in size, following the binary exponential backoff algorithm.

- The default maximum contention window size (CWmax) is 1023. The CW value will stop doubling when the CWmax is reached.

Binary Exponential Backoff

- Receiving stations of error-free frames send ACK.
  - Sending station interprets non-arrival of ACK within the ACK timeout period as a loss.
  - Executes backoff and then retransmits.

- The CW shall be reset to the minimum contention window size (CWmin) following every successful transmission attempt with acknowledgement received.

- The default value for CWmin depends on the physical layer, it could be 15, 31 or 63.

Example

Assume that CWmax is 1,023 = 2^{10} - 1, and CWmin is 15 = 2^4 - 1, or m = $\log_2$ (15 +1) = 4.

	k = min{m+f, 10}	**Range for BTC = {0, 1, …, 2^k - 1}**
Af a success (f=0)	4	{0, 1, 2, …, 2^4 - 1} or {0, 1, 2, …, 15}
Af 1st failure (f=1)	5	{0, 1, 2, …, 2^5 - 1} or {0, 1, 2, …, 31}
Af 2nd failure (f=2)	6	{0, 1, 2, …, 2^6 - 1} or {0, 1, 2, …, 63}
	:	
Af 5th failure (f=5)	9	{0, 1, 2, …, 2^9 - 1} or {0, 1, 2, …, 511}
Af 6th failure (f=6)	10	{0, 1, 2, …, 2^{10} - 1} or {0, 1, 2, …, 1,023}
Af 7th failure (f=7)	10	{0, 1, 2, …, 2^{10} - 1} or {0, 1, 2, …, 1,023}
:		

Exercise

Assume that CWmin is 31 and CWmax is 1,023. What is the possible range of values the BTC counter after a wireless station failed to transmit a frame in its 3rd attempt?

- $m = \log_2(31+1) = 5$; $f = 3$
- $K = \min(m + f, 10) = 8$
- $2^k - 1 = 255$

Possible range of values for BTC is {0, 1, …, 255}.

A

Exercise

In a wireless network, all stations use the IEEE 802.11 MAC protocol, DIFS = 50 μs and slot time = 20 μs. Assume that, while in the DCF mode of operation, station A generates a random value 18 for its BTC (Backoff Time Counter) at time instant t_0. The carrier sensing mechanism of station A detects the medium to be busy/free in the following sequence:

- Busy for 400 μs from instant t_0.
- Free for 120 μs after the previous busy period.
- Busy for 1000 μs after the previous free period.
- Free for long enough for BTC to expire at some time instant t_1.

Compute the actual time gap between t_1 and t_0.

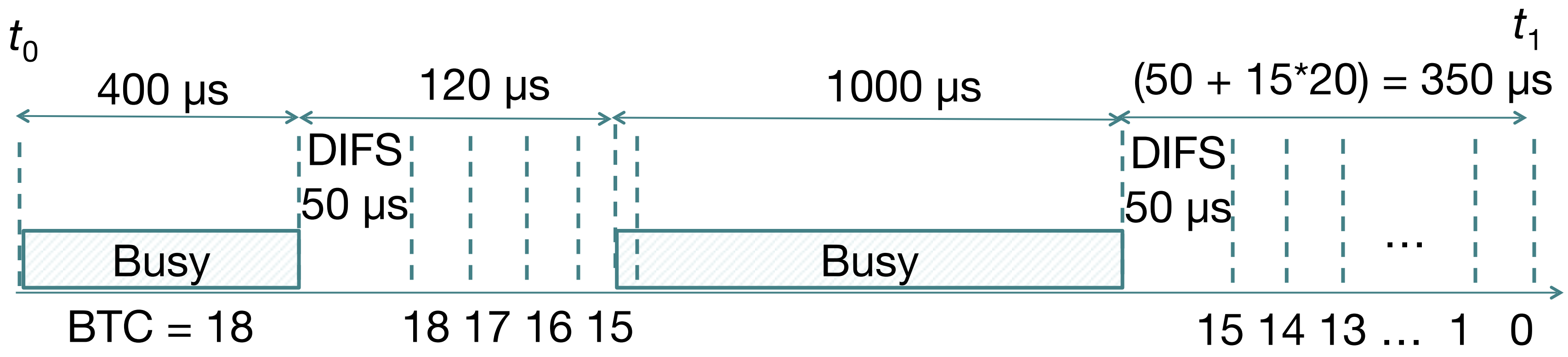
Hint:

○ BTC will not count down when the channel is busy.

○ The channel is only considered idle after it has been inactive for DIFS.

○ BTC will start to count down (decremented by one) every 20 ms (slot time).

Answers



Note that BTC does not count down when the medium is busy. When the medium is sensed to be idle for DIFS, BTC is decreased by one every 20 μs (slot time).

Time gap between t_1 and t_0 = (400+120+1000+350) μs

= 1,870 μs = 1.87 ms

CSMA/CA Protocol

- When a wireless station has a frame to send and the Backoff Time Counter (BTC) is zero, it will monitor the channel and wait for it to be idle.

- When the medium is idle for the duration of DIFS (DCF Interframe Space), the sending station sends an RTS frame (with the MAC addresses of the sender and the intended receiver, and the duration it wishes to transmit) to the AP.

- The sending station needs to receive a CTS frame from the receiving station within CTS timeout interval to be sure that it has successfully reserved the channel. Note that the CTS frame also serves to notify all other stations that the channel has been reserved.

- When the CTS frame has been received completely and correctly, the sending station will wait for SIFS before starting to transmit the data frame.

CSMA/CA Protocol

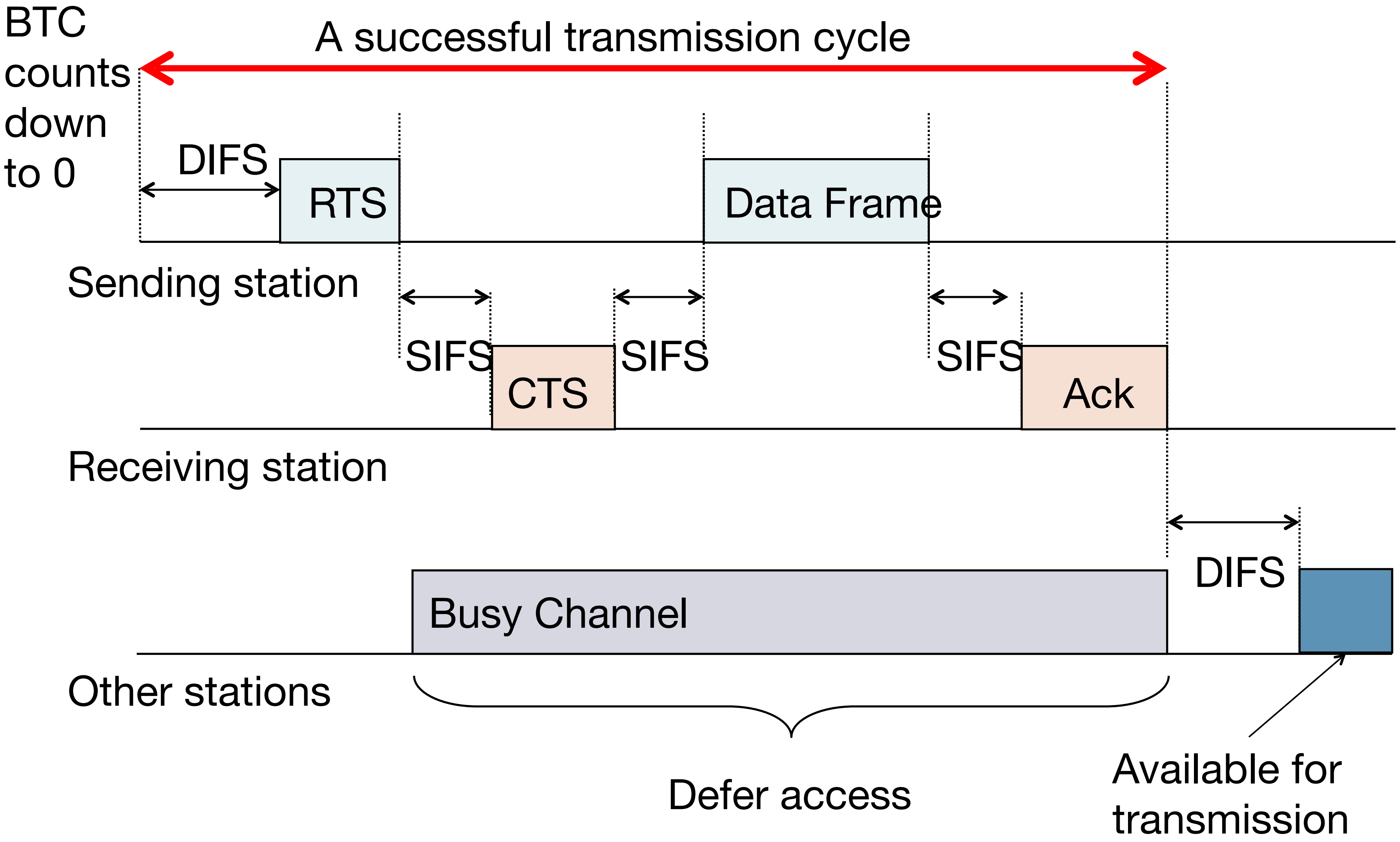
- When the receiving station receives the data frame, it will send an ACK frame to the sending station.

- When the sending station correctly receives the ACK frame within the ACK timeout interval, the transmission is deemed to be successful.

- Regardless of whether the station is successful in transmitting a frame, it will generate a random value based on the exponential backoff algorithm for its Backoff Time Counter (BTC). Only when the BTC counts to zero will the station be allowed to transmit again.

- Note that a Short Interframe Space (IFS) is required to be maintained between the RTS, CTS, Data and ACK frames.

Data Transmission with RTS/CTS

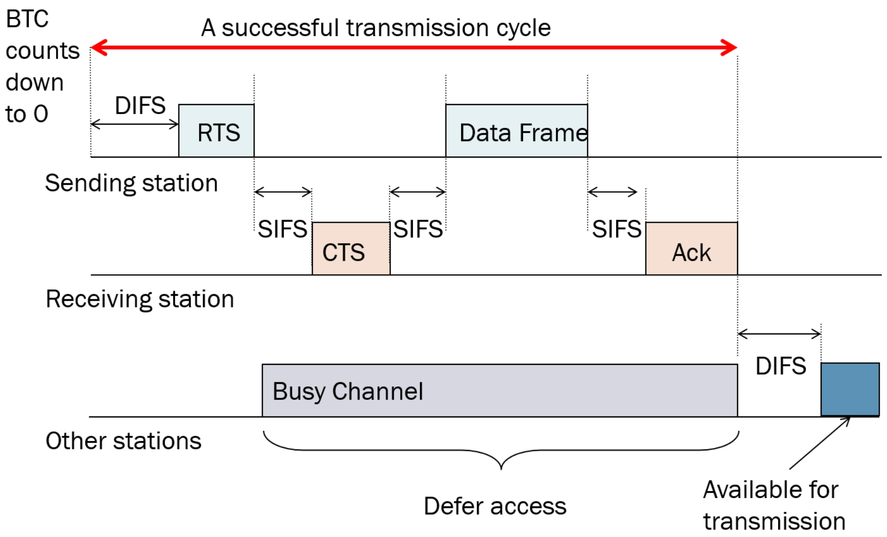


For 802.11b, slot time = 20 μs, DIFS = 50 μs, and SIFS = 10 μs.

Exercise

Suppose an 11 Mbps 802.11b station is configured to always reserve the channel with the RTS/CTS sequence. Suppose this station suddenly wants to transmit 1,000 bytes of data, and all other stations are idle at this time. Ignore the propagation delay and assuming no bit errors, calculate the time required to transmit the frame and receive the acknowledge. You may assume that the length of the RTS, CTS and ACK frames are 20, 14 and 14 bytes, respectively, and that DIFS is 50 μs and SIFS is 20 μs. You may also assume that the header and trailer of IEEE 802.11 frame is 34 bytes long.

Answers



Time required to transmit the frame and receive the ACK, *T*, is

DIFS + RTS + SIFS + CTS + SIFS + FRAME + SIFS + ACK

The time required to transmit the 1,000 bytes data frame is (8272 bits)/ (11 Mbps) = 752.0 usec.

Time for transmitting RTS frame: (20 x 8 bits)/(11 Mbps) = 14.5 μs

Time for transmitting CTS frame: (14 x 8 bits)/(11 Mbps) = 10.2 μs

Time for transmitting ACK frame: (14 x 8 bits)/(11 Mbps) = 10.2 μs

T = 50 + 14.5 + 20 + 10.2 + 20 + 752.0 + 20 + 10.2 ms = 896.9 μs

PCF - Polling

Point Coordination Function (PCF)

DCF may suffer from delay or jitter if the traffic is heavy because many terminals attempts to send packets and create serious collision.

For real-time applications, voice and multimedia, a strict and tight delay bound is necessary.

PCF is a contention-free access based on polling.

Point Coordination Function (PCF)

PCF provides connection-oriented, contention-free service through polling.

Point coordinator (PC) in AP performs PCF.

Polling table is up to implementer.

Contention free period (CFP)

- Initiated by beacon frame transmitted by PC in AP, which serves to reserve the channel for the CFP.
- During CFP, stations may only transmit to respond to a poll from PC, or to send ACK.

PCF Protocol

1 First, the stations need to register that they want to send data using PCF.

2 The Point Coordinator (PC) within the AP senses the channel.

3 If the channel is free for PCF Intreframe Space (PIFS, 30 μs for 802.11b), the PC sends the beacon frame which contains the contention-free period (CFP).

4 Then, the usual DCF operation will be preempted for a period of CFP.

5 After SIFS, the PC will poll each station on the list for data transmission or reception.

6 Once a station receives a poll, it will send a frame to other station and ACK to a frame from PC.

Note that a period known as Distributed Interframe Space (DIFS) is maintained between the end of CFP and the beginning of CP when DCF takes over the control.

Illustration of PCF

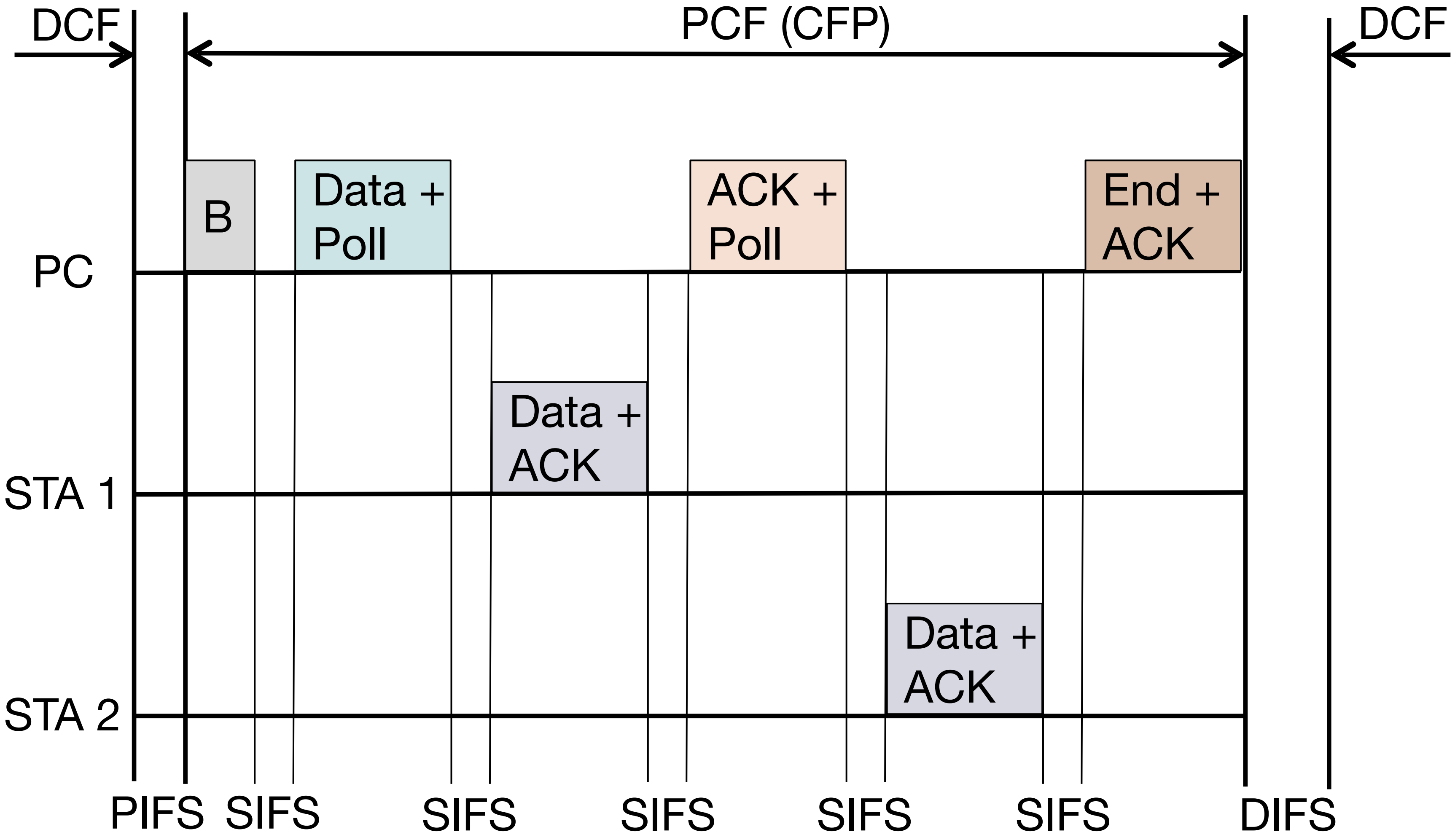


Illustration of PCF

MAC header (bytes)

2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame body	CRC

- MAC Header: 30 bytes
- Frame Body: 0 - 2312 bytes
- CRC: Covers MAC header and frame body
- Address 1: MAC address of the receiving station
- Address 2: MAC address of the transmitting station
- Address 3: e.g. MAC address of the router interface
- Address 4: e.g. used when APs forward frames to each other in ad hoc mode

Address 3 and Address 4 depend on the values of “To DS” bit and “From DS” bit in frame control.

IEEE 802.11 Frame Structure

Address Fields

802.11 MAC Addressing

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	Prot. Frame	Other

Frame Control field

MAC address of AP

Within WLAN

From router

To router

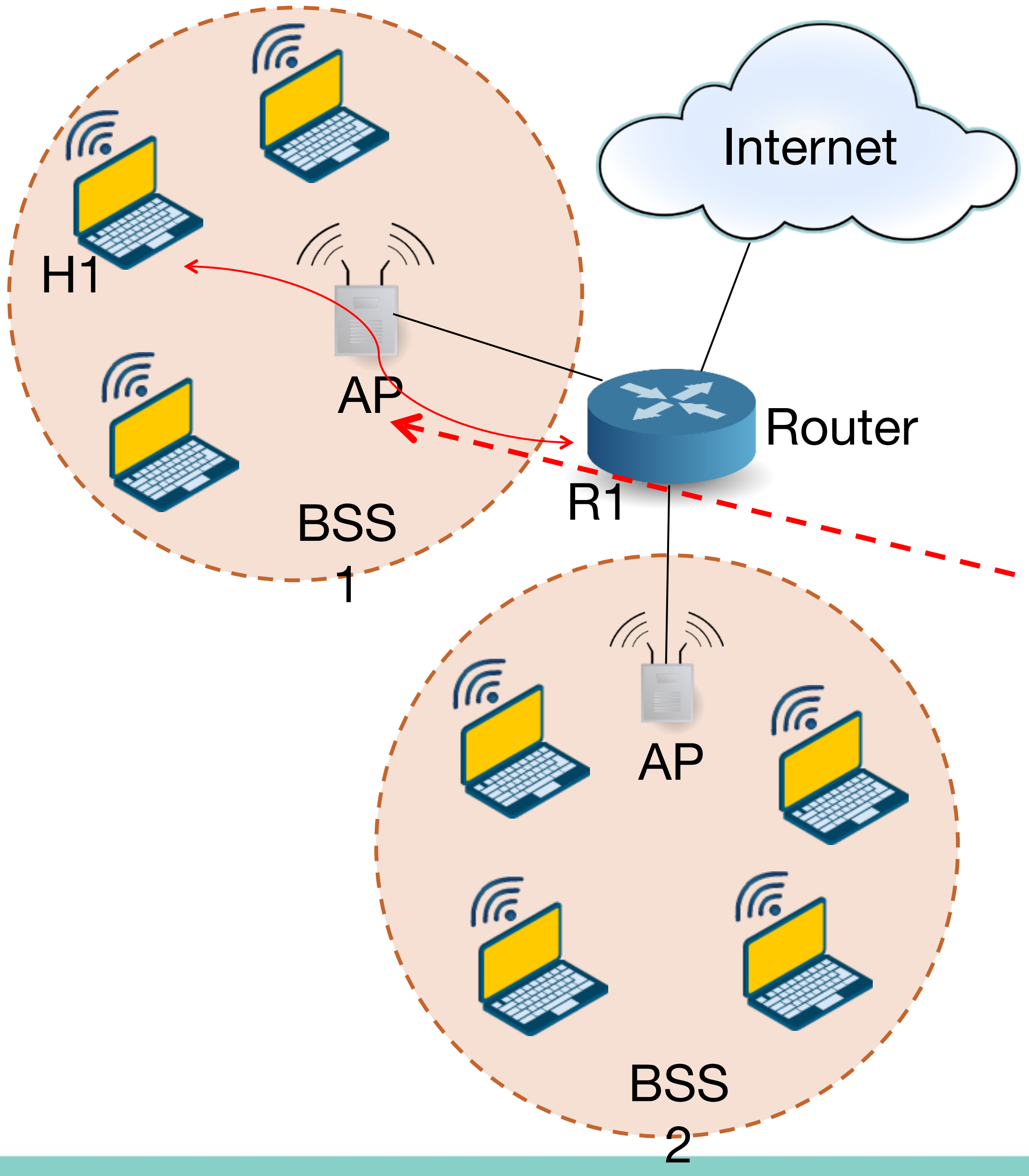
AP to AP in ad hoc mode

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

MAC address of router interface

- SA = MAC address of the original sender (wired or wireless)
- DA = MAC address of the final destination (wired or wireless)
- TA = MAC address of the transmitting 802.11 radio
- RA = MAC address of the receiving 802.11 radio
- BSSID = L2 identifier of the BSS, i.e., MAC address of access point

Example: Use of Address Fields



When a frame is sent from Router to H1 via the AP:

To DS = 0

From DS = 1

Address 1 = H1’s MAC address

Address 2 = AP’s MAC address

Address 3 = Router’s MAC address

Address 4 = Not Applicable

When a frame is sent from H1 to Router via the AP:

To DS = 1

From DS = 0

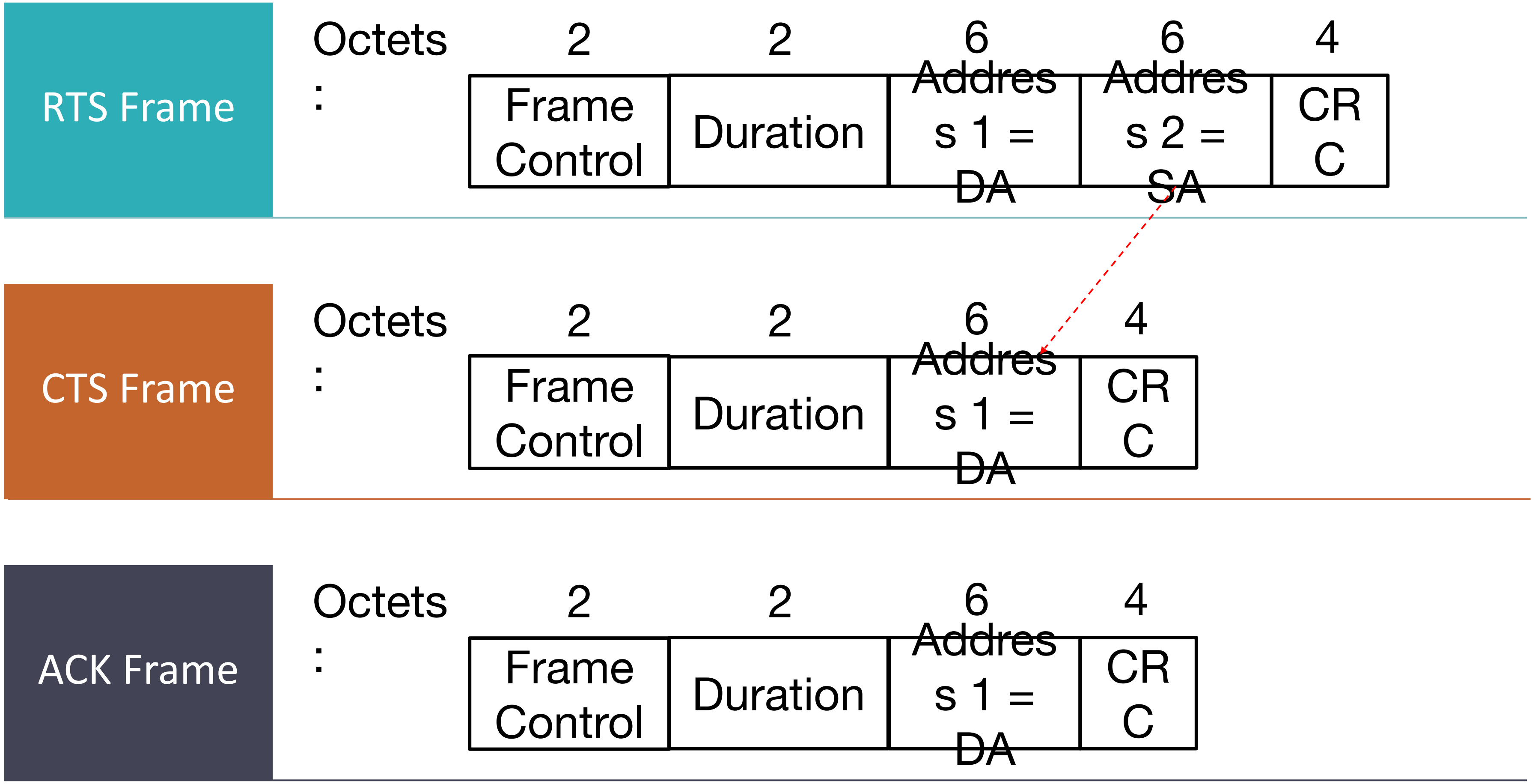
Address 1 = AP’s MAC address

Address 2 = H1’s MAC address

Address 3 = Router’s MAC address

Address 4 = Not Applicable

RTS, CTS and ACK Frames



RTS Frame

Octets:	2	2	6	6	4
	Frame Control	Duration	Address 1 = DA	Address 2 = SA	CRC

CTS Frame

Octets:	2	2	6	4
	Frame Control	Duration	Address 1 = DA	CRC

ACK Frame

Octets:	2	2	6	4
	Frame Control	Duration	Address 1 = DA	CRC

Notes: Address Fields

- 802.11 has four address fields, each of which can hold a 48-bit MAC address.

- 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 or AP that is to receive the frame.

- Address 3 contains the MAC address of the router interface (To DS = 0 and From DS = 1, or To DS = 1 and From DS = 0) or that of the AP (To DS = 0 and From DS = 0).

- Address 4 is used when the APs are connected to each other not via a Distributed System (DS) but via the ad hoc mode.

Summary

Summary

Key points discussed in this topic:

- IEEE 802.11 has a variety of standards that has different specifications and each is differentiated with a letter suffix.
- Wireless LANs that deploy access points (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.
- IEEE 802.11 stations can also group themselves together to form an ad hoc network – a network with no central control and no connections to the ‘outside world’.
- IEEE 802.11 supports two medium access control (MAC) protocols; i.e., Distributed Coordination Function (DCF) based on Carrier-sense Multiple Access/ Collision Avoidance (CSMA/CA) and Point Coordination Function (PCF) but PCF is rarely used in practice.

Summary

Key points discussed in this topic (cont’d):

- DCF based on CSMA/CA is contention based while PCF based on polling is non-contention based.

- 802.11 has four address fields, each of which can hold a 48-bit MAC address.