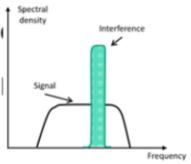
PART III: WIRELESS PROTOCOLS (PHY/MAC LAYER)

Wireless Local Area Network - WLAN

- WLAN is an information system that supports diverse location-independent network service access to portable devices utilizing radio channels
- The communication for WLAN is standardized across industry through IEEE.802.11 family of standards
  - Multiple versions exist a, b, g, h, n….
  - First version appear
- Different modulatio ; are employed across versions including



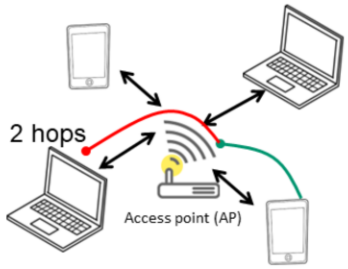
  - FHSS, DSSS, high rate DSSS
  - Orthogonal frequency division multiplexing (OFDM)

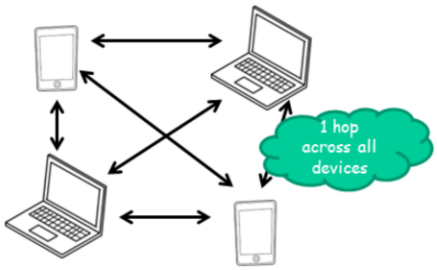
153

- IEEE is the Institute of the Electrical and Electronic Engineers where a division is responsible for developing standards relating to Information and Communication technologies. Standards relating to wireless communications are only a small set of standards developed by IEEE.
- A complete source for WLANs can be found here: M. Gast, *802.11 Wireless Networks: The Definitive Guide*, 2nd Ed., O'Reilly Media Inc., 2005.

Communication within WLANs

- Wireless devices located within a Basic Service Area communicate in two different ways





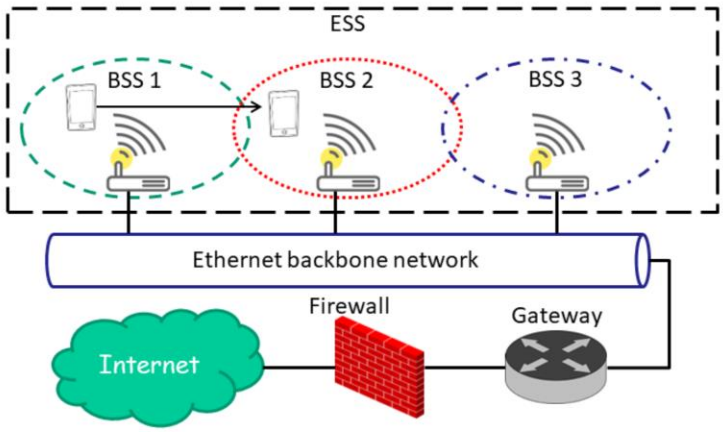
- Infrastructure Basic Service Set (BSS)
  - Communication between two wireless devices (WD) takes two successive hops
    - WD to AP and AP to WD
- Independent Basic Service Set (IBSS)
  - Wireless devices communicate directly
  - Typically involves a small number of devices for a specific task and short period of time

154

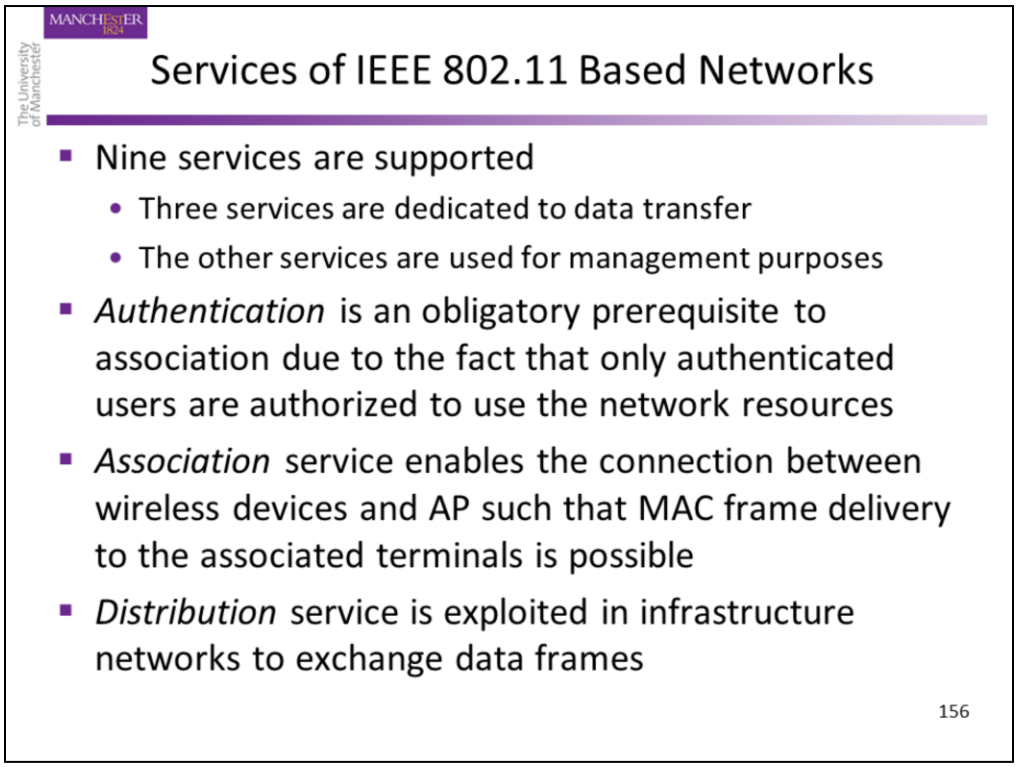
- The usage APs in infrastructure networks exhibits two primary advantages. No restriction is placed on the physical distance between WDs. Alternatively, straight communication between wireless devices would preserve system capacity but at the cost of increased physical and MAC layer complexity.
- The most important functions of an AP are to assist stations in accessing the Internet and help save battery power in associated wireless stations.
- If a mobile device is in a power-saving (PS) mode, the AP buffers those frames destined to reach this device during the period it will be in PS status. When the device exits the PS mode, the AP forwards the cached data frames to the device one by one. Thus, the AP is important in enabling energy savings policies and mechanisms.
- IBSSs are often called *ad hoc* BSSs or simply *ad hoc* networks.

Extended Service Set (ESS)

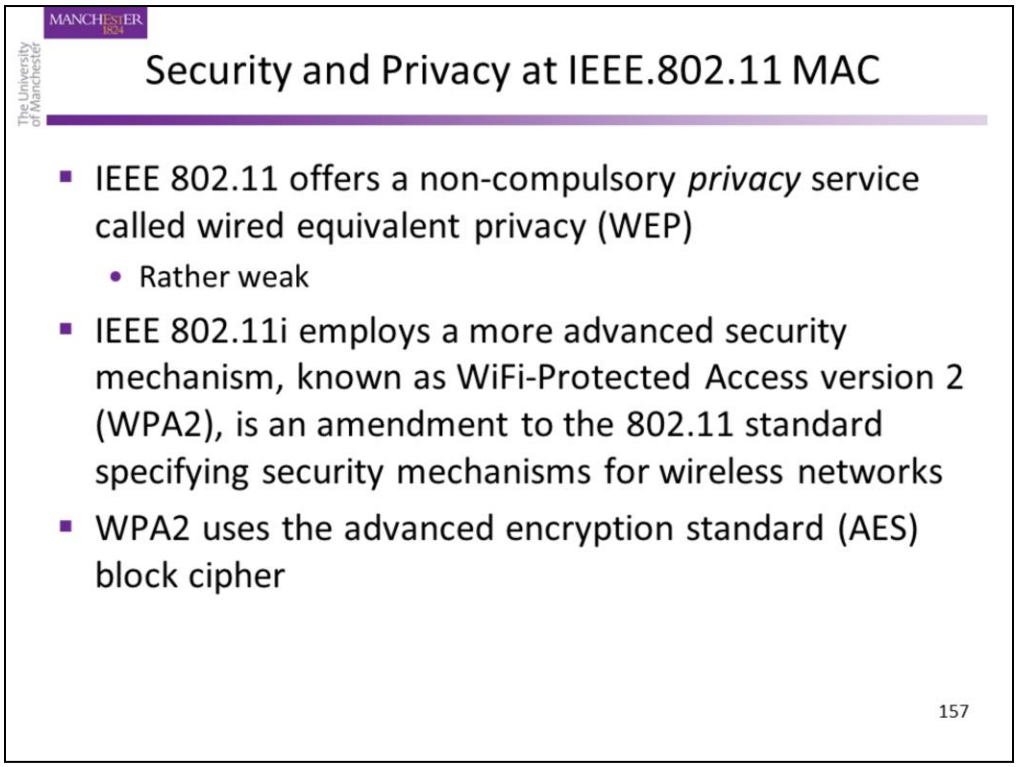
- The idea is to support an arbitrary network size



155



- Broadly, management services are responsible for tracking communication among the wireless devices as well as reacting in different circumstances.
- The AP, upon receiving a MAC protocol data unit (MPDU), uses the *distribution* service to forward it to the intended destination device. Therefore, any communication with an AP should use a distribution service to be possible.
- *Integration* is a specific service provided by the distribution system that enables connection with a non-802.11 network. The integration function is not expressed technically by the standard, except in terms of the services it should offer.
- The *association* service plays a vital role in the network services as unassociated wireless terminals are not permitted to obtain any service from the whole system.
- *Reassociation* is generally initiated by a wireless terminal once the signal strength indicates that a different association is necessary. This means that handoff and reassociation requests are never commenced by APs.
- To terminate an existing association, wireless stations may possibly use the so-called *disassociation* service. Upon invocation of disassociation, any mobility information stored in the distribution system corresponding to the requesting station is removed at once.
- If the APs of a distribution system *authenticate* any station, then the system is called an ‘‘open system’’ or an ‘‘open network.’’ Can you think of such examples?
- *Deauthentication* terminates an authenticated relationship between an AP and a wireless station. Essentially, deauthentication terminates any existing association and, consequently, use of network resources from a wireless device.



- IEEE 802.11i architecture contains the following elements: 802.1X for authentication [entailing the use of extensible authentication protocol (EAP) and an authentication server], the robust security network (RSN) for keeping track of associations, and the AES-based counter mode with cipher block-chaining message authentication code protocol (CCMP) to provide confidentiality, integrity, and origin authentication.
- Wireless stations provide the MSDU (MAC Service Data Unit) delivery service, which is responsible for getting the data to the actual recipient.

Access Schemes in IEEE 802.11 MAC

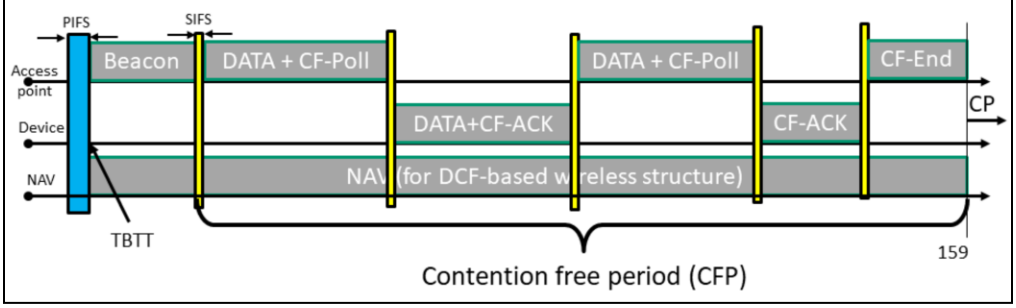
- Distributed Coordination Function (DCF)
  - Applies a listen-before-talk (LBT) approach and multiple-access carrier sense / collision avoidance (CSMA/CA) mechanism
- Point Coordination Function (PCF)
- An 802.11 superframe is composed of a contention-free period (CFP) and a contention period (CP), which alternate periodically in time
  - PCF is used during the CFP interval
  - and DCF is used during the CP interval
- A *beacon* frame generated by the AP initiates a superframe

158

- The *beacon* frames are employed to preserve synchronization of the local timers in the associated stations and to deliver protocol-related parameters.
- The AP transmits these management frames at regular predefined intervals. Each station knows precisely when the subsequent beacon will arrive.
- These time instances are called as target beacon transmission time (TBTT) and are announced in the previous beacon frame.

PCF Operation

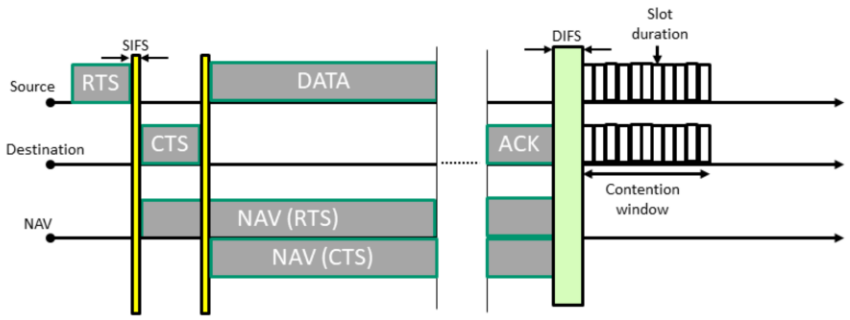
- The point coordinator (PC), which is typically an AP, polls a device to request delivery of a pending frame
- The frame sent to the device is complemented by a poll frame, that is DATA+CF-Poll
- The device acknowledges data reception and send data (MAC frames) should there be any pending frame aimed for the AP/PC



- PIFS: PCF Interframe Space
- SIFS: Short Interframe Space
- TBTT: Target Beacon Transmission Time
- If the PC does not receive a response from a polled station after waiting for one PIFS, it polls the next station or ends the CFP.
- The PCF suffers from several issues where inaccurate beacon frame delay and indefinite data transmission from the polled stations are the most distinct.
- At the TBTT, the PC schedules the beacon as the next frame to be transmitted, but the beacon can only be transmitted when the medium has been determined to be idle for at least one PIFS.
- In IEEE 802.11, wireless stations can start their channel access even if the MAC Service Data Units (MSDU) delivery is not finished before the upcoming TBTT. Depending upon whether the shared medium is idle or busy at the TBTT, a delay of the beacon frame may occur. The time the beacon frame is delayed from the TBTT determines the delay in a time-bounded MSDU transmission added to the CFP. This can influence the QoS introducing unpredictable time delays in each CFP.
- A further problem with the PCF is the unknown transmission duration of polled stations. A station that has been polled by the PC is allowed to deliver an MSDU that may be fragmented and of arbitrary length.

DCF Operation & Timing Diagram

- Listen (poll) the channel if idle for DIFS time and a *backoff* period then transmit
  - DCF interframe space -> DIFS
- Request to Send (RTS) and Clear to Send (CTS) frames contain information about the duration of the data transfer
- ACK frame helps to avoid packet retransmission

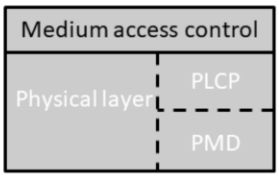


160

- The backoff period is determined through a binary exponential backoff (BEB) mechanism.
- To resolve the status of the radio channel and the use of the wireless medium, the network allocation vector (NAV) both at the physical and MAC (virtual) layer is utilized. The NAV corresponds to the time required for the data transmission/reception including the duration of the ACK frame. This information is provided by the RTS/CTS frames.

IEEE 802.11 Physical Layer

- Two sublayers can be distinguished
  - the PLCP sublayer which receives incoming MSDUs from the MAC layer, adds its own designated header, and then hands them over to the PMD
  - The Physical Medium Dependent (PMD) sublayer is responsible for transmitting every received bit from the PLCP over the wireless medium
- The delivered information must have a preamble, which has a pattern that depends on the modulation technique deployed in the physical layer



161

- PLCP: PHY Layer Convergence Procedure
- Three different modulation schemes were supported by the physical layer of the initial revision of 802.11: frequency-hopping spread spectrum (FHSS), DSSS, and infrared (IR) light.
- Later version, such as 802.11a, 802.11b, and 802.11g were developed which are based on OFDM, high rate (HR)/DSSS, and the extended-rate PHY (ERP), respectively.
- Also, it is noteworthy to mention that 802.11n will be based on multi-input multi-output (MIMO) OFDM.

Supported Multiple Access Physical Layer Techniques

- Frequency Hopping systems transition from one frequency to another in a random pattern, transmitting a short burst at each sub-channel
  - A 2-Mbps FH physical layer is specified
- Direct-sequence systems spread the power out over a wider frequency band using mathematical coding functions
- Two DS structures were specified
  - The initial specification standardized a 2-Mbps physical layer
  - 802.11b added the HR/DSSS physical layer

Frequency Hopping Spread Spectrum

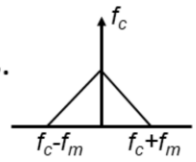
- In FH-based systems, the frequency is time dependent; each frequency is used for a short portion of time, i.e., the so-called dwell time
- If two FH systems want to share the same frequency band, both of them can be configured such that they utilize different hopping sequences so that they do not interfere with each other
- For the duration of each time slot, the aforementioned hopping sequences should be on dissimilar frequency slots

163

- FH is similar to the well-known frequency division multiple access (FDMA). However, in FDMA systems, devices are allocated fixed orthogonal nonoverlapping frequencies (i.e., fixed while totally distinct centre frequencies and bandwidths).
- Beacon frames on FH networks include a timestamp and the so-called FH Parameter Set element. The FH Parameter Set element includes the hop pattern number and a hop index. By receiving a Beacon frame, a station knows everything it needs to synchronize its hopping pattern.
- Adaptive FH (AFH) is more resilient to interference as this scheme can avoid overcrowded frequencies, a strategy used in Bluetooth as we will see later on. Adaptivity is easier to implement with FHSS rather than DSSS.

FH Physical Layer

- In 802.11 FH, the microwave ISM band is partitioned into a series of 1-MHz channels. Approximately 99% of the radio energy is confined to the channel



- Channels are defined by their centre frequencies
  - E.g. f_c = 2.403 GHz
- There are 95 channels with the last channel at 2.495 GHz
- Not all channels are allowed across the globe!
  - US and Europe (excluding Spain and France) allow channels 2-79

164

- The dwell time in 802.11 FH systems is 390 time units, which is about 0.4 s.
- When an 802.11 FH physical layer hops between channels, the hopping process should take no longer than 224 ms.
- The frequency hops are subject to extensive regulation, in terms of both the size of each hop and the rate at which hops must occur.

Direct Sequence Spread Spectrum

- Direct Sequence transmission is an alternative spread-spectrum technique that might be utilized to transmit a narrowband signal over a much wider frequency band
- The DS modulation scheme is accomplished by applying a chipping sequence (CS) to the information bit stream
- Chipping sequences, or the so-called pseudorandom noise (PN) codes, have a much higher rate in comparison to the actual data stream

165

- A *chip* is a binary digit sequence employed by the DS system. These bits are higher level data while the chip signals are binary numbers used in encoding (transmitter side) and decoding (receiver side) procedures.
- For the PN code, IEEE 802.11 adopted an 11-bit Barker word meaning that each bit is encoded using the entire Barker word as a CS.
- Barker words have satisfactory autocorrelation, implying that the correlation function at the receiver operates as expected in a wide range of environments and is relatively tolerant to multipath delay spreads as incurred in multipath fading (attenuating) channels.

Illustration of DSSS – Modulation/Spreading

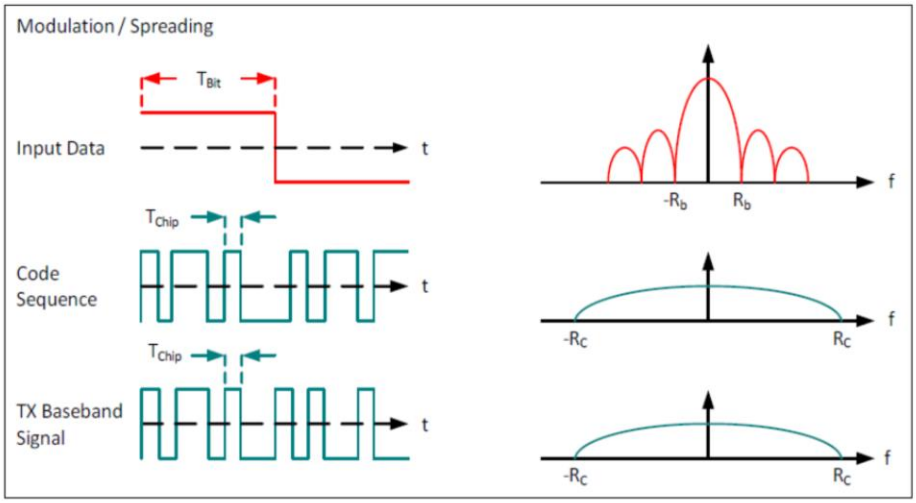
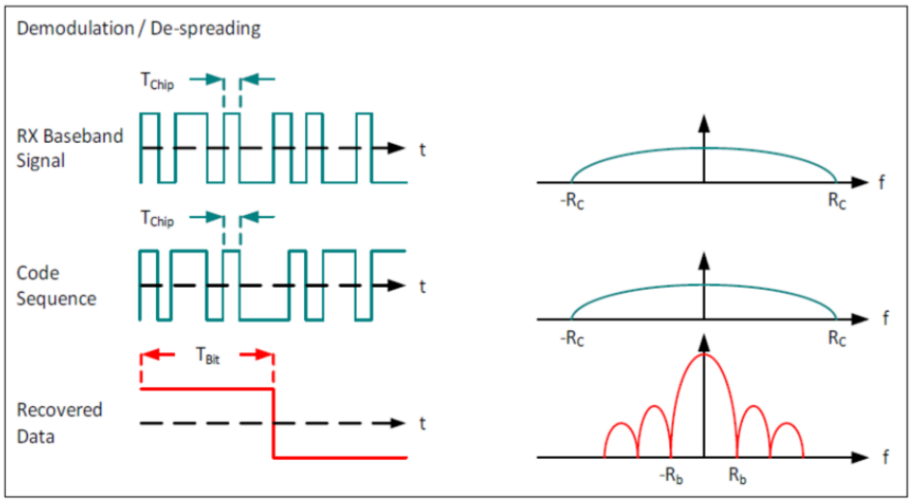


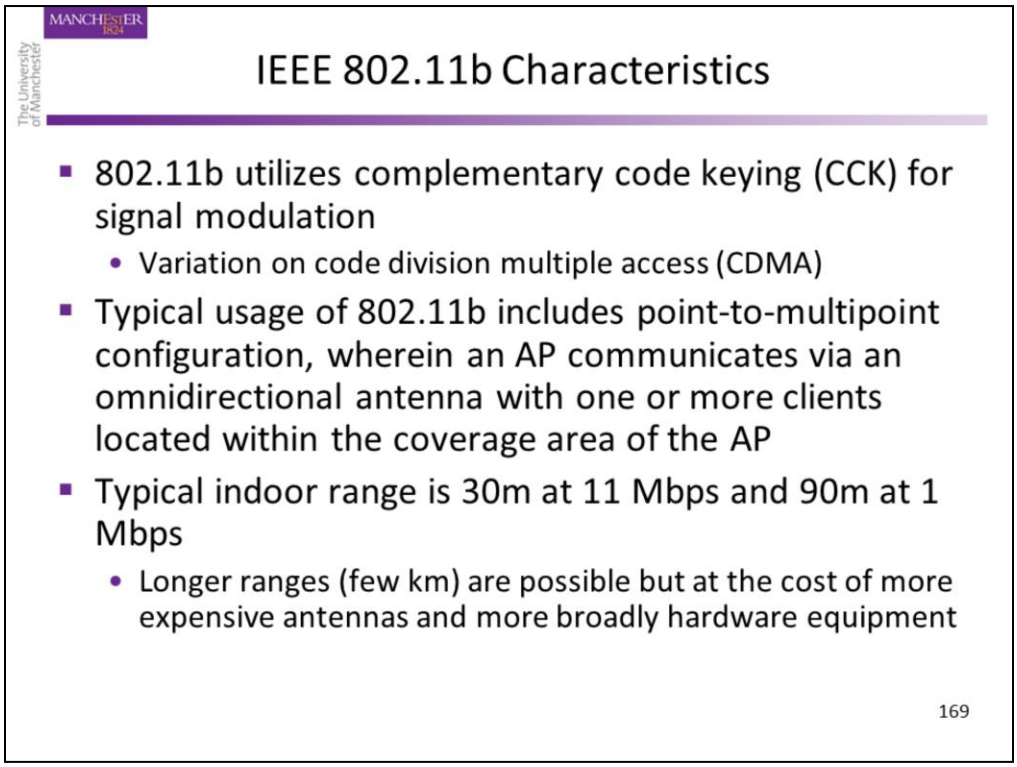
Illustration of DSSS – Demodulation/Despreading



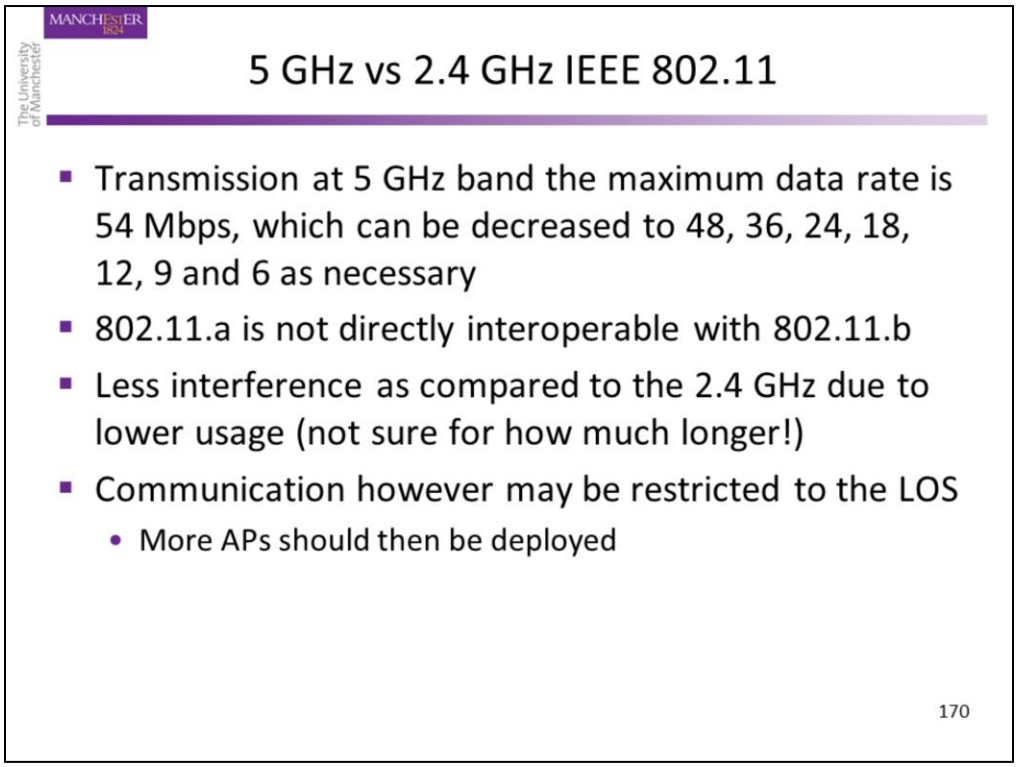
167

DS Physical Layer

- Channels for the 802.11b DS physical layer are much larger than the channels for the FH physical layer
- The DS physical layer has 14 channels in the 2.4-GHz band, each 5 MHz wide
- Channel 1 is placed at 2.412 GHz, channel 2 at 2.417 GHz, up to channel 13 at 2.472 GHz



- The dramatic increase in throughput of 802.11b (compared to the original standard) along with substantial price reductions led to the rapid acceptance of 802.11b as the definitive WLAN technology.



- 802.11a has 12 non-overlapping channels, 8 indoors & 4 point-to-point
- The total bandwidth is 20 MHz with an occupied bandwidth of 16.6 MHz and symbol duration is 4 µsec with a guard internal of 0.8 µsec.
- IEEE 802.11g operates at the 2.4 GHz band and has comparable throughput with the IEEE 802.11a. This version, however, is compatible with the corresponding 802.11b.
- The newer IEEE 802.11n extension can offer data rates of up to 600 Mbps with every possible option activated.