

---

# Indoor WLAN Design

*Part IV: Understanding the 802.11  
Management Operations*

**Kjell Jørgen Hole**  
UiB

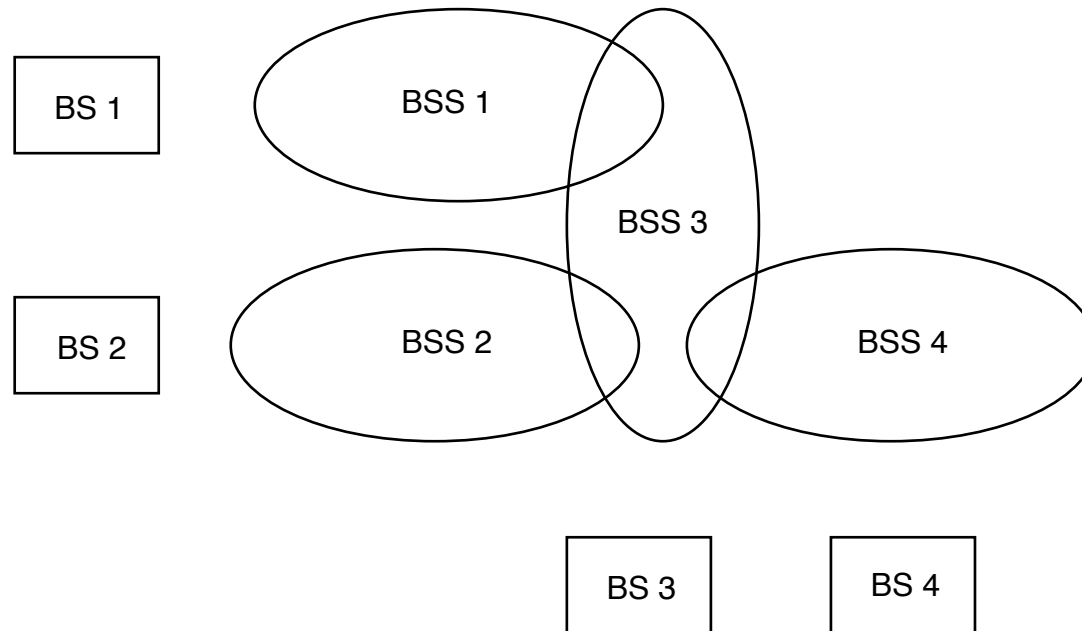
Last updated 22.01.08  
Mail: [Kjell.Hole@ii.uib.no](mailto:Kjell.Hole@ii.uib.no)  
URL: [www.kjhole.com](http://www.kjhole.com)

- Some useful 802.11 definitions describing the network structure
- Management operations:
  1. scanning
  2. authentication
  3. association
  4. power management
  5. spectrum management

**BSS** Basic Service Set. Group of stations that communicate

- **IBSS** *Independent* BSS. Group of MSs communicating directly with each other. Referred to as *ad hoc* BSS or *ad hoc* network
- **Infrastructure BSS** Distinguished by the use of a BS

**ESS** Extended Service Set. Consisting of multiple Infrastructure BSSs connected via a backbone network. All BSs have the same “network name”



# The Distribution System

---

KJhole.com

**DS** Distribution System. Part of ESS. Consists of the backbone network, the communication protocol allowing the BSs to share association information, the bridge engines in the BSs, and the protocols transporting data frames on the backbone

- while 802.11 doesn't specify any particular wired network technology, Ethernet is often used in practice

- DS transports frames
  - ensures that a frame is transported to the right BS and relayed by BS to intended MS
- DS provides mobility by connecting BSs
  - tracks which BS an MS is associated with
  - updates association when an MS moves
  - each BS in an ESS utilizes DS to inform the other BSs of associated MSs

**IAPP** *Inter-Access Point Protocol*. Protocol used to communicate association information between BSs in an ESS. Defined by *802.11f Recommended Practice*

- Approved June 12, 2003
- Specifies the information to be exchanged between BSs amongst themselves and higher-layer management entities to support the DS functions
- The information exchanges specified for DSs are built on the IETF IP in a manner sufficient to enable the interoperation of DSs containing BSs from different vendors

# Need for Management Operations

---

- The management operations in 802.11 were designed to reduce problems caused by
  - unreliable medium
  - limited battery power
  - lack of physical boundaries
- Operations are carried out between MSs, BSs, and DS
- Operation may vary because MSs have different device drivers

- The following management operations are needed to establish a new wireless link:
  1. scanning
  2. authentication
  3. association
- These operations, as well as power management operations, will be discussed. We concentrate on infrastructure networks

# 1. Scanning

---

**Scanning** The process of identifying existing networks. Many parameters are used in the scanning procedure:

- **BSSType** specifies whether to seek out IBSSs (*ad hoc* networks), infrastructure BSSs, or all networks
- **BSSID** Basic Service Set ID. A 48-bit ID. Determines whether or not an MS scans for a specific network (ID=MAC of BS) or for any network (ID=1) that is willing to allow it to join
- **SSID** Service Set Identity. A text string. Assigned to all BSs in an ESS. Often called the **network name**. MSs wishing to find *any* network should set the SSID equal to the broadcast SSID

# More Scanning Parameters

---

- **ScanType** *Active scanning* uses the transmission of Probe Request frames to identify networks. *Passive scanning* saves battery power by listening for **Beacon frames**
  - Beacon frames are sent out by the BS, typically about 10 times a second
  - Beacon frames advertise the presence of the BS and inform the MSs about the network name and the BS's capabilities (e.g. security support)
- **ChannelList** List of channels an MS will listen on for the existence of a network

## Even More Scanning Parameters

---

KJhole.com

- **ProbeDelay** The delay, in microseconds, before the procedure to probe a channel in active scanning begins. This delay ensures that an empty or lightly loaded channel does not completely block the scan
- **MinChannelTime** and **MaxChannelTime** These values specify the minimum and maximum amount of time that the scan works with any particular channel

- Passive scanning is mandatory, while active scanning is optional
- MS saves battery power because it does not transmit
- MS goes from channel to channel on *ChannelList* and listens for Beacon frames. Records information from Beacons it receives
  - Beacon contains information about BSS needed to start communication
  - the MS may not hear all BSs in its area

# Active Scanning (1)

---

- An MS uses the following procedure for each channel on the *ChannelList*:
  1. Move to the channel and wait for either an indication of an incoming frame or for the *ProbeDelay* timer to expire. If an incoming frame is detected, the channel is in use and can be probed. The timer prevents an empty channel from blocking the entire procedure
  2. Gain access to the medium using the DCF (Distributed Coordination Function) access procedure and send a Probe Request frame

## Active Scanning (2)

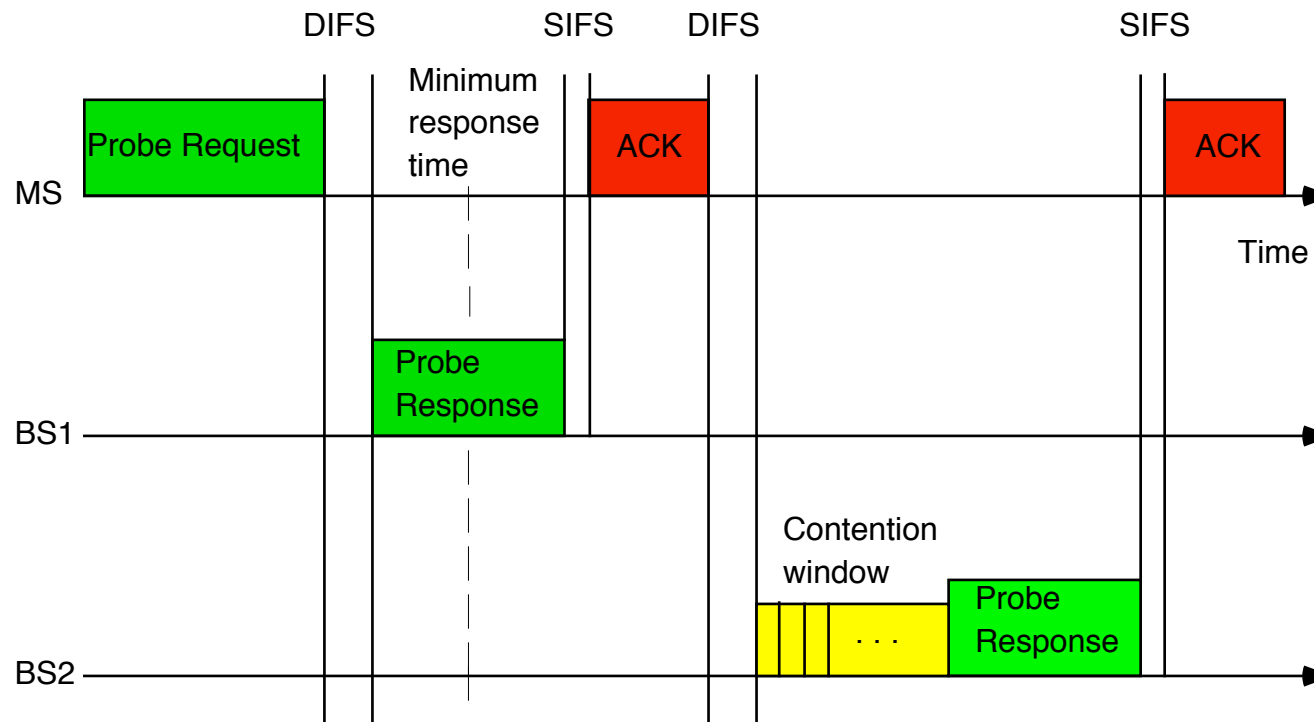
---

KJhole.com

3. Wait for the minimum channel time, *MinChannelTime*, to elapse
  - if the medium was never busy, there is no network. Move to the next channel
  - if the medium was busy during the *MinChannelTime* interval, wait until the maximum time, *MaxChannelTime*, and process any Probe Response frames

# Active Scanning Procedure

KJhole.com



# Active Scanning and SSID

---

- Probe Request frames are used to solicit responses from a network with a given SSID, i.e., network name. It is also possible to use the broadcast SSID to trigger responses from all networks
- The device to transmit the last Beacon frame is responsible for transmitting any Probe Response frames. In an infrastructure network, the BS transmitting the Beacon will also transmit the Probe Response frames
- IBSSs may pass around the responsibility of sending Beacon frames

# Why is Active Scanning Needed?

---

KJhole.com

- It may seem that 10 Beacons a second would be plenty for an MS to find a BS quickly
- However, there are 11 channels and the MS has to go to each channel and wait for 0.1 second to complete a scan
- Furthermore, if the MS is already connected and the signal strength is getting weak, the MS needs to find a new BS quickly to avoid disruption

- A scan report is generated at the conclusion of a scan
- The report lists all BSSs found. Detailed information about each BSS enables an MS to join a selected BSS (not complete list):
  - *Beacon interval*: BS may transmit at its own specific interval
  - *DTIM period*: part of the power-saving mechanism
  - *Timing parameters*: assist in synchronization
  - *BSSBasicRateSet*: data rates MS must support to join network

- An MS can *join* a certain BSS
- Joining is not sufficient to enable network access. Both *authentication* and *association* are also needed
- Choosing which BSS to join is an implementation-specific decision that may involve user intervention
- The user may not specify which BSS to join in an ESS. This is determined by the signal strengths from the different BSSs

## 2. Authentication

---

**Identity authentication** is the process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an entity

- Identity authentication happens in two phases:
  - (1) an identifier phase, during which an identifier is selected in some way, and
  - (2) an authentication phase, during which the required level of confidence is established

# Wi-Fi “Authentication”

---

KJhole.com

- Two approaches to “authentication” are specified:
  - **Open-system authentication** The BS accepts an MS without verifying its identity! It may be possible to use MAC address filtering (not part of the 802.11 standard)
  - **Shared-key authentication** Based on WEP (Wired Equivalent Privacy) and requires that both devices implement WEP

# Shared-Key Authentication

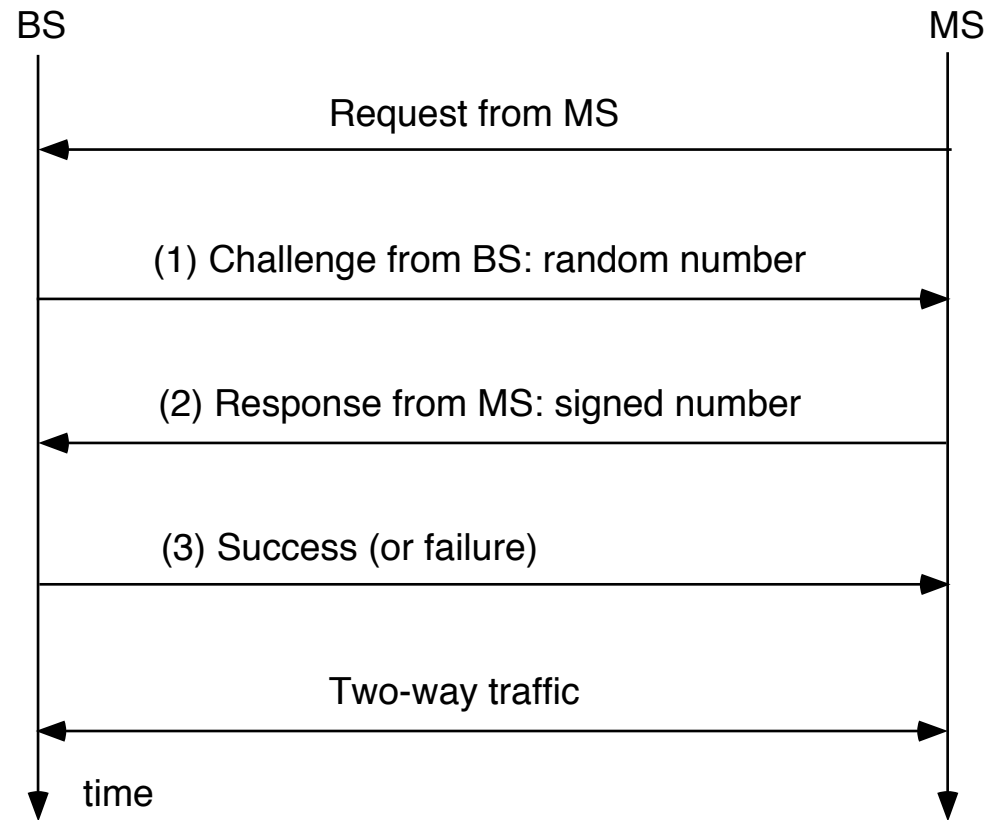
---

The BS uses a “pre-shared” key based challenge-response system to authenticate the MS:

1. The BS sends a random number, i.e. the challenge, to the MS
2. The MS signs this random number using WEP with the “pre-shared” secret key and sends the response back to the BS
3. The BS verifies that the random number has been signed by the correct key by calculating the signature itself and comparing the computed and the received values. Once the BS verifies this, it authenticates the MS

# Shared-Key Authentication Illustration

---



# Why Shared-Key Authentication is Bad (1)

- 802.11 implicitly assumes that BSs are in a privileged position since they are under control of network administrators
- MSs can be authenticated to ensure that only authorized MSs access the network
- MSs can't authenticate the BS

## Why Shared-Key Authentication is Bad (2)

- An attacker can record the challenge (plaintext) from the BS and the response (ciphertext) from the MS to obtain a matching plaintext/ciphertext pair
  - XOR plaintext and ciphertext to recover keystream
- The key used during the challenge-response mechanism is the encryption key
  - this is not acceptable according to security experts
- Shared-key authentication provides no means of verifying that subsequent data frames come from the "authenticated" MS

# What is needed?

---

KJhole.com

- **Mutual authentication:** BS and MS must be able to authenticate each other
- **Method of preserving identity:** Some form of “secret frame token” is needed to verify all data frames from a trusted party
- **Independent authentication keys:** Authentication keys must be independent from encryption keys

## 3. Association

---

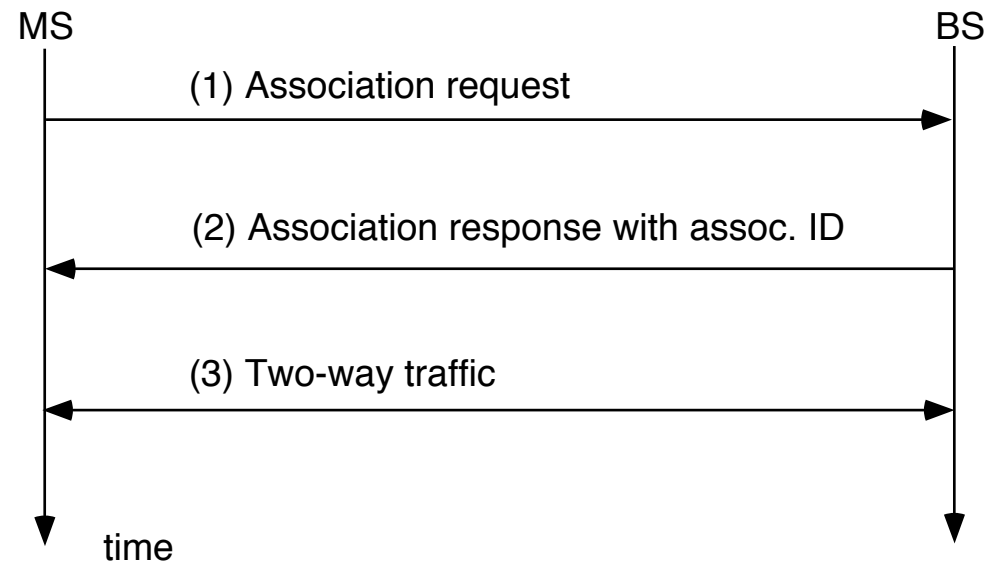
**Association** Recordkeeping procedure that allows the DS to track the positions of the MSs such that frames can be forwarded to the correct BSs

- authentication must be completed before association
- association is restricted to infrastructure networks
- an MS **associates** with a BS to gain full access to the network
- 802.11 does not specify how to determine whether an association should be granted

# Association Procedure

---

KJhole.com



**Reassociation** The process of moving an association from an old BS to a new BS in an ESS

- over the air, the procedure is almost the same as an association
- on the backbone network, BSs may interact with each other to move frames
- the reassociation procedure is initiated when the MS detects that another BS has a stronger signal (decision is product-dependent)
  - needed to support roaming

# Sending Data

---

- Each data frame going from or to an MS has three addresses:
  - a “final” source address
  - a “final” destination address
  - an “intermediate” address
- The “intermediate” address determines which BS the data frame passes through

## 4. Power Management

---

- Most MSs run on batteries. Battery power is a scarce resource and must not be wasted
- Power conservation is achieved by minimizing the time the MS transceiver spends in *active* mode (turned on) and maximizing the time in *power-saving* mode (turned off)
- Greatest savings possible in infrastructure networks. BSs have access to continuous power. They can keep track of MSs' power management states and schedule the traffic accordingly

# Power Management Infrastructure Networks

---

- A BS knows the current power management modes of all its MSs. It can therefore
  - buffer frames to MSs in power-saving mode
  - send periodic announcements of buffer status to MSs in power-saving mode
- MSs in power-saving mode power up periodically to listen to buffer status reports transmitted in Beacon frames. This requires less power than periodically transmitting polling frames

## 5. Spectrum Management

---

KJhole.com

- The 802.11a standard operates in the 5 GHz frequency band
- European radio regulations mandate the use of
  - Transmit Power Control (**TPC**)
  - Dynamic Frequency Selection (**DFS**)

TPC and DFS were standardized as 802.11h in 2003

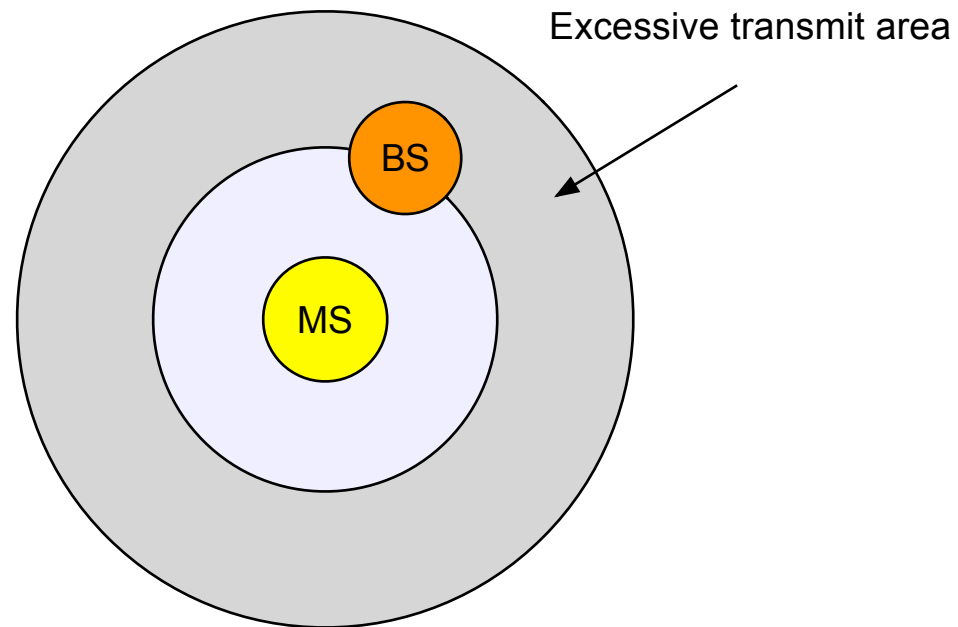
# TPC—Transmit Power Control

---

- TPC ensures that 802.11a radio transmitters stay within regulatory power limits and don't interfere with certain satellite services in Europe
- TPC also limits the range of transmission depending on the distance between a BS and an MS such that little power is “wasted”
  - leads to longer battery life
- TPC limits interference because the transmit power is reduced

# High Power

---



- Before transmission TPC calculates the maximum allowable transmit power based on regulatory constraints and local constraints determined by a network admin
- TPC then attempts to keep the transmit power as low as possible while supporting a good connection between a BS and MS
- Both MS and BS can dynamically adjust the transmission power on a frame-by-frame basis based on the
  - link margin = received power - minimum acceptable power

# DFS—Dynamic Frequency Selection

---

- DFS changes radio channels based on measurements and regulatory requirements
- DFS will periodically test a channel for potential interference from other radio systems, in particular 5 GHz European radar systems
- *Quiet periods*, scheduled by including the Quiet information element in Beacon and Probe Response frames, are used to test radio channels

- An MS must carry out the following steps to gain access to a wireless network:
  - scanning
  - authentication
  - association
- Battery power is a scarce resource. 802.11 supports power conservation