Alexander T.E.I. of Thessaloniki

School of Technological Applications

Department of Informatics

IEEE 802.11aa: Improvements on Video Transmission over Wireless LANs

B.Sc. Thesis

by

Georgios Savvidis

Thesis Supervisor

Dr. Periklis Chatzimisios
Assistant Professor

Alexander T.E.I. of Thessaloniki

Department of Informatics

P.O. BOX 141
GR - 574 00, Thessaloniki
GREECE

May, 2012

IEEE 802.11aa: Improvements on Video Transmission over Wireless LANs

B.Sc. Thesis

by

Georgios Savvidis

Alexander T.E.I. Of Thessaloniki

Abstract

In the recent years, audio and video applications have started to dominate the Internet. Meanwhile, IEEE 802.11 networks have become a basic feature of mobile devices, the popularity of which is growing fast alongside their technological capacities, providing the end users almost the same capabilities as a Personal Computer. This results in users having performance expectations as defined by their experience with wired video media.

While the current IEEE 802.11 standard provides high enough bandwidth for the needs of video transmission, in addition with specifying mechanisms for a certain level of Quality of Service (QoS), there are still several issues that need to be addressed in order to improve the quality of a multimedia stream. In particular:

- The legacy IEEE 802.11 does not provide mechanisms to ensure that all multicast members successfully receive the transmitted data. In other words the current standard does not provide the means for a reliable multicast/broadcast transmission.
- It is essential to specify a method that mitigates the effects of Overlapping BSS (OBSS) environments in order to offer increased robustness, without the need for centralized management.
- In the case of multiple video transport streams that belong in the same EDCA Access Category, a mechanism is needed to provide prioritization between them.
- In situations with insufficient channel capacity, there needs to be a mechanism that marks the less important information as “discarded”, providing a more graceful video degradation.
- It is also important the applied mechanism for multimedia stream transport to be compatible with the IEEE 802.1AVB protocol suite.

For all the above reasons, various researchers attempted to propose solutions and design techniques until, finally, the IEEE decided to establish a working group, called the Task Group aa (TGaa). This group aims at standardizing MAC layer enhancements for more reliable multicast video transmission, while at the same time ensuring backwards compatibility.

Acknowledgments

This thesis is the result of the past one year of a very interesting and valuable research at the Alexander T.E.I. of Thessaloniki. Through this experience I had the opportunity to put in a well-constructed frame all the relative knowledge that I gained during my B.Sc. studies. However, nothing of this would have come true without the valuable help of some people that I need to thank.

First of all, I would like to specially thank my thesis supervisor, mentor and friend, Dr. Periklis Chatzimisios, Assistant Professor in the Department of Informatics at the Alexander T.E.I. of Thesssaloniki, for assigning to me this particular thesis and giving me the chance to work with and learn a lot of him, for his support and patience and for his guidance in matters that regard the next step of my career.

Part of this work is credited to Kostas Maraslis, PhD candidate in the Department of Telecommunications Science and Technology at the University of Peloponnese, whom I sincerely thank for his kind cooperation and assistance during the whole process of this thesis' implementation.

A deep thank to my old colleague and good friend, Georgios Papadopoulos for generously sharing his knowledge whenever I needed his help.

I would also like to thank my professors Nikolaos Psarras and Stefanos Harhalakis from the Department of Informatics at the Alexander T.E.I. of Thessaloniki, who imparted to me their knowledge in the best possible way and helped me discover my interest in the field of networking.

Finally, this thesis would not have been accomplished without the support of my family and my very close friends who are always next to me.

Georgios Savvidis

Contents

Chapter 1

Theoretical Background

1.1 Introduction to IEEE

The Institute of Electrical and Electronics Engineers (IEEE) was found in 1963 by the merger of the American Institute of Electrical Engineers (AIEE) and the Institute of Radio Engineers (IRE) [1]. IEEE is a non-profit leading organization for technology standards, research and other professional and educational activities in the fields of Electronics, Electrical, Telecommunications, Computer and Biomedical Engineering. As of today, it has more that 400.000 members worldwide.

The IEEE 802 project was requested in December 1979 [1], and its first meeting was held in February 1980. Its object is the development of standards both for wired and wireless Local and Metropolitan Area Networks (LANs/MANs). In the following sub-chapters there will be presented a brief summary of the active IEEE 802 Working Groups (WG) in the wireless zone.

1.2 The IEEE Wireless Zone

In the latest years wireless networks have expanded rapidly and nowadays they play a significant role in business and home communication networks. More and more devices of daily use, such as PDAs, laptops, mobile phones, etc, include wireless network support as a basic feature. The term "wireless network", however, is a very general term, since there are various different types of networks that operate on the wireless medium. IEEE in order to provide high quality support for all these kind of wireless networks, has deployed WGs, where each of them has the responsibility of developing standards for a particular field. Currently, the IEEE 802 project has the following active WGs, for the wireless zone:

- IEEE 802.11 Wireless Local Area Network (WLAN)
- IEEE 802.15 Wireless Personal Area Network (WPAN)
- IEEE 802.16 Wireless Metropolitan Area Network (WMAN)
- IEEE 802.18 Radio Regulatory – Technical Advisory Group (RR-TAG)
- IEEE 802.19 Wireless Coexistence – Technical Advisory Group (WC-TAG)

- IEEE 802.21 Media Independent Handoff (MIH)
- IEEE 802.22 Wireless Regional Area Network (WRAN)

1.2.1 IEEE 802.11 WLAN

The first IEEE 802.11 standard was published in 1997. Since then numerous modifications and enhancements have been made to the original standard, and today it is considered as one of the most significant standardization achievements. The standard has a lot of similarities to the IEEE 802.3 standard, that defines the PHY and MAC layers of wired Ethernet. IEEE 802.11 and its standards family are presented separately in Chapter 2.

1.2.2 IEEE 802.15 WPAN

The IEEE 802.15 WPAN focuses on the development of standards for Personal Area Networks (PANs) or, in other words, for short distance wireless networks. The 802.15 WG includes seven task groups:

- IEEE 802.15.1 Bluetooth specification
- IEEE 802.15.2 Coexistence between IEEE 802.15 and IEEE 802.11
- IEEE 802.15.3 High-rate WPAN
- IEEE 802.15.4 Low-rate WPAN
- IEEE 802.15.5 Mesh Networking
- IEEE 802.15.6 Body Area Network (BAN)
- IEEE 802.15.7 Visible Light Communication (VLC)

IEEE 802.15.1 was published in June 2002. Defining PHY and MAC specifications, 802.15.1 comprises an adaptation of the Bluetooth Specification v1.1. It is also considered an additional resource for Bluetooth devices constructors. For updating the 802.15.1 standard to the Bluetooth v.1.2 specification, the task group 1a (TG1a) was formed [1]. Meanwhile, the IEEE 802.15.2 TG undertook the development of a recommended practice, aiming at facilitating the coexistence of 802.11 and 802.15 networks.

IEEE 802.15.3 is a MAC and PHY standard that provides High-rate (20Mbit/s or greater), among with low power and low cost solutions for the needs of portable consumer digital imaging and multimedia applications, for WPANs [2]. 802.15.3 also provides a certain level of QoS. On the other hand, IEEE 802.15.4 was developed to provide low data rate solutions for WPANs. The emphasis is on very low complexity, among with extremely low power consumption, that would allow battery duration from several months to several years. It is mostly applied to applications such as sensors, remote controls, etc. IEEE 802.15.4 comprises the basis for various specifications, with ZigBee being the most well-known between them. Since neither 802.15.3, nor 802.15.4 define any path selection methods, TG5 was formed to provide the means for mesh networking both for high and low data rate WPANs. The result of this work was the IEEE 802.15.5 standard, which supports both full mesh and partial mesh topologies. There are several advantages of mesh networking, such as the ability to extend the network coverage without increasing the transmit power, the enhanced reliability via route redundancy, easier network configuration and longer device battery life due to fewer retransmissions [3].

In November 2007 the IEEE 802.15 TG6 was formed and began developing a low-power and low-frequency communication standard optimized for devices and operation on, in or around the human body, although it is not limited to humans. It serves a variety of applications including medical, consumer electronics, and entertainment [4]. Finally, 802.15 includes the TG7 the first meeting of which, was held in January 2009. IEEE 802.15.7 is an under-development standard for visible light communications. It based on the idea of “what you see is what you send”, it is aesthetically pleasing and since it operates on the visible light spectrum, it is harmless for the human health. The standard is capable of delivering data rates high enough to support both for indoor and outdoor audio/video multimedia applications.

1.2.3 IEEE 802.16 WMAN

The IEEE 802.16 working group was established in 1999 to develop standards and recommended practices for broadband Wireless MANs. Though its official name is WirelessMAN, it is mostly known as WiMAX (Worldwide Interoperability for Microwave Access). IEEE 802.16 defines four different PHYs [1] supporting channel bandwidths of 1.25 MHz – 20 MHz, in any band in between the range 2 GHz – 66 GHz. It also includes an adaptive modulation scheme that takes advantage of good signal conditions, Multiple-in Multiple-out (MIMO) antennas and Hybrid Automatic Repeat Request (HARQ) for greater error correction performance. The modulation scheme that it uses is Orthogonal Frequency-Division Multiple Access (OFDMA), which is basically a multi-user version of the Orthogonal Frequency-Division Multiplexing (OFDM).

The 802.16 MAC provides a means to encapsulate technologies of the wired medium like Ethernet, Asynchronous Transfer Mode (ATM) and IP on the air interface. It also provides security enhancements, by using both authentication and encryption mechanisms, such as the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). Finally, 802.16 provides a strong QoS support, with 5 QoS classes.

1.2.4 IEEE 802.18 RR-TAG and IEEE 802.19 WC-TAG

IEEE 802.18 and 802.19 are considered Technical Advisory Groups. 802.18 does not develop new standards but, instead it supports the IEEE 802 wireless working groups in radio regulatory matters. Its main purpose is to monitor and to actively participate in ongoing radio regulatory activities worldwide, while it is also the liaison to other standards of mutual interest [5]. It currently supports the following six groups:

- IEEE 802.11 Wireless Local Area Network (WLAN)
- IEEE 802.15 Wireless Personal Area Network (WPAN)
- IEEE 802.16 Wireless Metropolitan Area Network (WMAN)
- IEEE 802.21 Media Independent Handoff (MIH)
- IEEE 802.22 Wireless Regional Area Network (WRAN)

It also supports IEEE 802.20 Mobile Broadband Wireless Access (MBWA) which, however, is in hibernation since March 2011 due to lack of activity.

IEEE 802.19 working group provides technical advise about coexistence to the following working groups [5]:

- IEEE 802.11 Wireless Local Area Network (WLAN)
- IEEE 802.15 Wireless Personal Area Network (WPAN)
- IEEE 802.16 Wireless Metropolitan Area Network (WMAN)
- IEEE 802.22 Wireless Regional Area Network (WRAN)

With 802.19 it is assured that wireless devices operating in one of the above networks, will not cause harmful interference to neighboring networks. To ensure that, sometimes 802.19 is involved in the development of the mentioned standards. Furthermore, since January 2010, the 802.19 working group is developing a standard, the IEEE 802.19.1, that allows wireless networks coexistence in the TV White Spaces.

1.2.5 IEEE 802.21 MIH

IEEE 802.21 standard, which was published in 2008, provides algorithms that enable handover and interoperability both between networks of the same and of different types, that may be either 802 or non-802 networks. Handover is defined by the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP), as “the transfer of a user's connection from one radio channel to another”. Handovers that happen within a single network are known as Horizontal Handovers, while those that are triggers across different networks, are known as Vertical Handovers. 802.21 is mainly used for Vertical Handovers, though it can be used for Horizontal Handovers, as well. Reasons for triggering a handover include [1]:

- Signal quality degradation.
- Stronger signal reception from a neighboring cell.
- The current signal strength has dropped under the minimum acceptable level.
- The current signal quality has dropped under the minimum acceptable level.
- The data traffic in the current cell has become high.

IEEE 802.21 achieves the seamless handover and interoperability between different types of networks, by introducing a new, transparent layer between the layers 2 and 3 in the traditional OSI/ISO model. This transparent layer is responsible for providing the information needed to the upper layers, in order for the handover to be media independent [6]. Practical examples of the use of IEEE 802.21 could be:

- A user wishing to switch from an 802.3 network to an 802.11 one.
- When a mobile phone user connected to a Global System for Mobile Communications (GSM) network enters in range of an 802.11 network, he/she should be able to hand off of the GSM and seamlessly connect to the 802.11.

1.2.6 IEEE 802.22 WRAN

The scope of IEEE 802.22 standard is to enhance the wireless interface, by modifying the MAC and PHY layers, of point-to-multipoint WRANs of 40 km or more, operating in the VHF/UHF TV broadcast bands between 54 MHz and 862 MHz [7]. The purpose of this project was to fulfill the need of broadband wireless network access in areas where the wired infrastructure is too expensive to be deployed. In such areas, the deployment of 802.22 operates in the spectrum that is allocated to the TV broadcast service, but is currently not used. The major prerequisite of the standard was to be able to operate in this spectrum without causing any harmful interference to the incumbent operation both in the VTF and the low UHF TV bands.

The 802.22 working group was formed after the 802.18 study group decided that none of the existing IEEE 802 PHY/MAC combination could achieve this goal without major modifications. The 802.22 project was initially expected to be published in 2010, but it was finally over in July 2011. The working group has two additional task groups, the TG1 and the TG2, which are writing 802.22.1 and 802.22.2, respectively.

The 802.22.1 standard was developed to enhance harmful interference protection for low power licensed devices operating in TV Broadcast Bands. The need of this standard arose when the FCC proposed to allow new license-exempt devices to operate in the same channels as the 802.22. Thus, it was important to protect devices, such as wireless microphones, that were currently using this spectrum, from harmful interference. Finally, 802.22.2 is Recommended Practice, currently under development, that describes the best engineering practices and detailed technical guidance for the installation and deployment of IEEE 802.22 systems [7].

Chapter 2

IEEE 802.11 Standards Family

2.1 The IEEE 802.11 base standard

The initial version of the IEEE 802.11 standard was released in 1997 and specifies two data rates of 1 and 2 Mbit/s. It specifies three alternative physical layer technologies:

- Diffuse Infrared (IR)
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

IEEE 802.11, also defined a Medium Access Control (MAC) sublayer that operates according to a listen-before-talk scheme, known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). A mapping of the defined IEEE 802.11 layers to the OSI reference model is presented in Figure 2.1.

Having published its first 802.11 standard in 1997, the Working Group (WG) received feedback that many products did not provide the degree of compatibility that customers expected. Thus, the need for a certification program came up and led to the foundation of the Wireless Ethernet Compatibility Alliance (WECA) in 1999, which renamed to Wi-Fi Alliance (WFA) in 2003. Wi-Fi certification has become a well-known certification program that has a significant market impact [8].

2.1.1 Infrared (IR)

Infrared light lies between the visible and microwave portions of the electromagnetic spectrum. Infrared light has a range of wavelengths that lies from red light to violet. These wavelengths correspond to a frequency range of approximately 1 to 400 THz (1 THz = 1.000 GHz). Standards regarding IR data transmission are mainly published by the Infrared Data Association (IrDA). The infrared physical layer supports two data rates: 1 and 2 Mbit/s. The specification of two data rates is aimed at allowing [10]:

- A smooth migration to higher data rates
- Asymmetric operation of the BSS

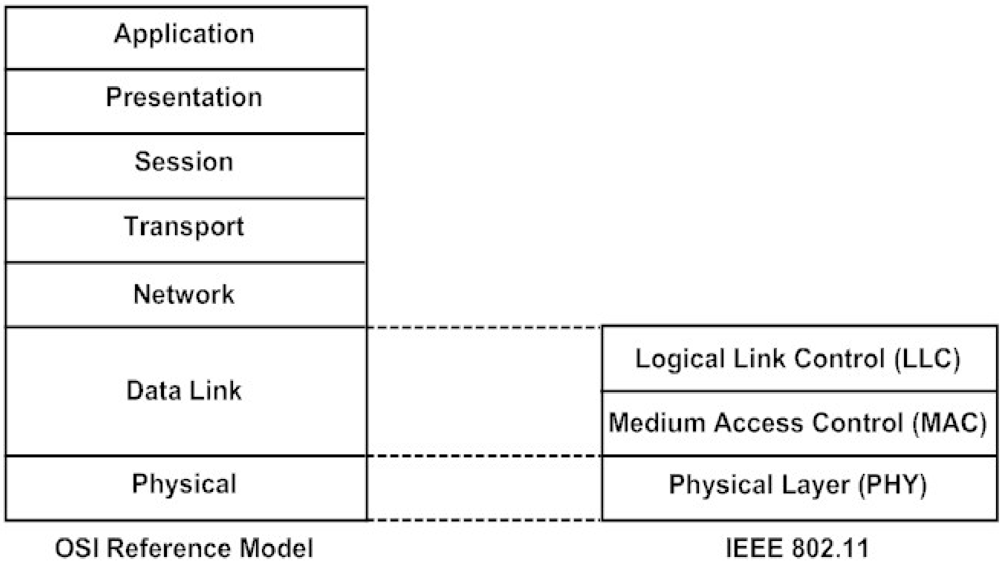


Figure 2.1 IEEE 802.11 standards mapped to the OSI reference model [9]

The modulation method that is adopted for this physical layer is Pulse Position Modulation (PPM) since it is very effective in wireless transmissions. For each of the two data rates specified here, there is a different PPM scheme: 16-PPM for 1 Mbit/s and 4-PPM for 2 Mbit/s. The purpose of this feature is to ensure that the basic pulse is the same at both data rates, which minimizes the additional complexity introduced by the 2 Mbit/s data rates [10]. The use of IR for WLANs is today obsolete, since it has not been adopted by any IEEE 802.11 implementation.

2.1.2 Frequency Hopping Spread Spectrum (FHSS)

FHSS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudo-random sequence known to both transmitter and receiver. In the United States, the FCC requires that at least 75 discrete frequencies must be employed for each transmission channel and that a signal cannot remain on any particular frequency for more than 400 ms. In the IEEE 802.11, the maximum length of a packet is around 30 ms, and the hops are 1 MHz apart from one another. FHSS can be employed for both analog and digital communications, but is currently implemented primarily for digital transmissions. If 75 contiguous frequencies are used, then the bandwidth required for a transmission is 75 times larger than when only one frequency is used – the spectrum is spread over a larger portion of the transmission band (hence “frequency hopping spread spectrum”). The original motivation for developing this technique was a desire to avoid hostile jamming of a radio signal. If a transmission hops to a jammed frequency, the data sent in vain on that frequency are resent after the next hop. For wireless networks, FHSS has a desirable "side effect:" It minimizes the chances that different transmitters on the network will encounter interference from one another; otherwise the network could potentially disable itself.

The IEEE 802.11 FHSS PHY was meant to operate in the 2.4-GHz band at speeds of 1 or 2 Mbit/s. The FHSS system was discarded by the IEEE 802.11b standard after it was found that having two transmission techniques for one standard meant that two kinds of (incompatible) equipment were necessary to implement the standard, and DSSS turned out to be the more reliable technique [11].

2.1.3 Direct Sequence Spread Spectrum (DSSS)

DSSS is one of the most successful data transmission techniques. Beside wireless LANs, it is, also, used in cellular networks (CDMA systems) and Global Positioning Systems (GPS). The idea is to multiply the data being transmitted to a pseudo random binary sequence of a higher bit rate.

DSSS systems spread the signal energy across a relatively wide band by increasing the occupied bandwidth. A DSSS transmitter converts a bit stream into symbol stream where each symbol represents a number of bits depending on the Phase-Shift Keying (PSK) modulation technique. The symbol information is converted into a complex-valued signal, which is fed to the spreader. This spreader multiplies its input signal with a Pseudo Noise (PN) sequence, which is called a chip sequence. The result of this multiplication is a signal with a wider bandwidth. The in-phase and quadrature components of the spreader output signal are fed to a quadrature modulator. The transmitter front-end provides filtering, upmixing and power amplification. The IEEE 802.11 DSSS is based on 11-chips Barker sequence. The 11-chip spreading makes the occupied bandwidth larger and increases the effective bandwidth from 1 MHz to 11 MHz. The IEEE 802.11 standard specifies the following bit rates: 1 Mbit/s with BPSK, 2 Mbit/s with QPSK, 5.5 Mbit/s and 11 Mbit/s with Complementary Code Keying (CCK) [12]. Some of the benefits of DSSS include:

- Resistance to intended and unintended jamming.
- Sharing of a single channel among multiple users.
- Reduced signal/background-noise level hampers interception.
- Determination of relative timing between transmitter and receiver.

2.1.3.1 Complementary Code Keying (CCK)

CCK is a modulation technique that allows for multi-channel operation in the 2.4 GHz band by virtue of using the existing IEEE 802.11 1 Mbit/s and 2 Mbit/s DSSS channelization scheme. In 1999, CCK was adopted to supplement the Baker code in wireless digital networks to achieve data rate higher than 2 Mbit/s at the expense of shorter distance. This is due to the shorter chipping sequence in CCK (8 bits versus 11 bits in Barker code) that means less spreading to obtain higher data rate but more susceptible to narrow-band interference resulting in shorter radio transmission range. Beside shorter chipping sequence, CCK also has more chipping sequences to encode more bits (4 chipping sequences at 5.5 Mbit/s and 64 chipping sequences at 11 Mbit/s) increasing the data rate even further.

2.1.4 Orthogonal Frequency-Division Multiplexing (OFDM)

OFDM is a modulation technique for transmitting large amounts of digital data over a radio wave. It extends the concept of single carrier modulation by using multiple sub-carriers within the same single channel. The total data rate to be sent in the channel is divided between the various sub-carriers. The data do not have to be divided evenly nor do they have to originate from the same information source. Advantages include using separate modulation/demodulation customized to a particular type of data, or sending out banks of dissimilar data that can be best sent using multiple, and possibly different, modulation schemes.

OFDM offers an advantage over single-carrier modulation in terms of narrow-band frequency interference. Since this interference will only affect one of the frequency sub-bands, the other sub-carriers will not be affected by the interference. Since each sub-carrier has a lower information rate, the data symbol periods in a digital system will be longer, adding some additional immunity to impulse noise and reflections. OFDM systems usually require a guard band between modulated sub-carriers to prevent the spectrum of one sub-carrier from interfering with another. These guard bands, however, lower the system’s effective information rate when compared to a single carrier system with similar modulation [13].

OFDM was not supported by the IEEE 802.11 standard until its first amendment, the IEEE 802.11a. Nowadays, OFDM and OFDM-based modulation techniques are used by IEEE 802.11a/g/n, in addition to other 802 family standards, such as IEEE 802.16.

2.2 IEEE 802.11 Amendments

The huge success in the market of the IEEE 802.11 standard, led to its continuous improvement and various revisions of the original standard, driven by a complete alphabet. To avoid confusion with other 802 standards, letters l, o, q and x are not used [8].

2.2.1 IEEE 802.11a

IEEE 802.11a is the first amendment to the original IEEE 802.11 specification, started in September 1997 and finally approved two years later, in September 1999. It added an OFDM physical layer that supports a higher data rate of up to 54 Mbit/s using the 5 GHz band. This high frequency means that IEEE 802.11a signals can achieve a shorter range that the 2.4 GHz signals and, also, they have more difficulties in penetrating walls and other obstructions.

On the other hand, using the 5 GHz band gives IEEE 802.11a a significant advantage, since the 2.4 GHz band is heavily used to the point of being crowded, thus it is prone to conflicts that can cause frequent dropped connections and degradation of service. Even though the IEEE 802.11a standard has a maximum raw data rate of 54 Mbit/s, it yields realistic net achievable throughput in the mid-20 Mbit/s. Finally, the data rate can be reduced to 48, 36, 24, 18, 12, 9 and the 6 Mbit/s (also known as Adaptive Rate Selection), if signal quality becomes an issue.

2.2.2 IEEE 802.11b

IEEE 802.11b was developed at the same time with IEEE 802.11a. Since IEEE 802.11b gained in popularity much faster that IEEE 802.11a did and due to its lower cost, it serves better the home market, whereas IEEE 802.11a is usually found on business networks. IEEE 802.11b supports a bandwidth of up to 11 Mbit/s using a Direct-Sequence Spread Spectrum (DSSS) PHY. It also uses the same CSMA/CA medium control access method defined in the original standard. However, due to the CSMA/CA protocol overhead, in practice the maximum IEEE 802.11b throughput that an application can achieve is about 5.9 Mbit/s using TCP and 7.1 Mbit/s using UDP. IEEE 802.11b uses the 2.4 GHz radio band, same as the original IEEE 802.11 standard. Using this frequency offers lower production costs, but it is more possible to interfere with other devices that operate at the same band, such as microwave ovens, cordless phones etc.

2.2.3 IEEE 802.11d

With the publishing of IEEE 802.11b, the IEEE 802.11 Working Group was beginning to realize the acceptance of its products. However, IEEE 802.11b was defined to operate only in the United States, Canada, Japan, France, Spain, and the portion of Europe operating under ETSI regulations. These six locations were defined in the standard as “regulatory domains”. Outside any of these regulatory domains, a device could not be called compliant with the IEEE 802.11 standard.

To address these regional requirements, the IEEE 802.11 Task Group d (TGd) was formed in June 1999 and the standard was finally released two years later. The solution chosen by TGd was to add a management protocol that would announce certain regulatory and location information. This protocol allows mobile devices to determine whether they are allowed to operate in that location and, if operation was allowed, to configure their radio to comply with the local regulations [14].

2.2.4 IEEE 802.11e

Initially the goal of the IEEE 802.11e project, as approved at the end of March 2000, was to add several enhancements to the IEEE 802.11 standard that would include efficiency improvements, support for Quality of Service, and a higher security level. However, soon enough, the IEEE 802.11 frame encryption algorithm WEP was broken by an attack. The security enhancements were then displaced to a new TG, the TGi. Finally, in 2005, the IEEE 802.11e was approved targeting to provide a set of QoS enhancements through modifications to the MAC layer [8].

In particular, the IEEE 802.11e standard introduced a new coordination function, the Hybrid Coordination Function (HCF), in order to enhance the DCF and PCF access methods and support applications with QoS requirements. Within the HCF, there are two methods of channel access, similar to those defined in the legacy IEEE 802.11 MAC; the HCCA and the EDCA. HCF is further explained in sub-chapter 3.1.3.

IEEE 802.11e also enhanced the MAC layer to support block ACK. The main idea behind this mechanism is that the receiver instead of sending a single ACK for each data frame that has correctly been received, it sends a block ACK after having received multiple frames. This block ACK indicates that the last n frames were received correctly. There are two variations of the block ACK mechanism, the immediate and the delayed block ACK.

After sending a block of frames, the sender transmits a Block ACK Request (BAR) frame, to which the receiver responds with a Block ACK (BA). The difference between immediate and delayed block ACK is that in the first case the BAR solicits an immediate BA response, while with the delayed block ACK the BAR itself needs to be acknowledged, and then the BA is transmitted which in turn needs to be acknowledged [15]. Figure 2.2 demonstrates the operation of both mechanisms.

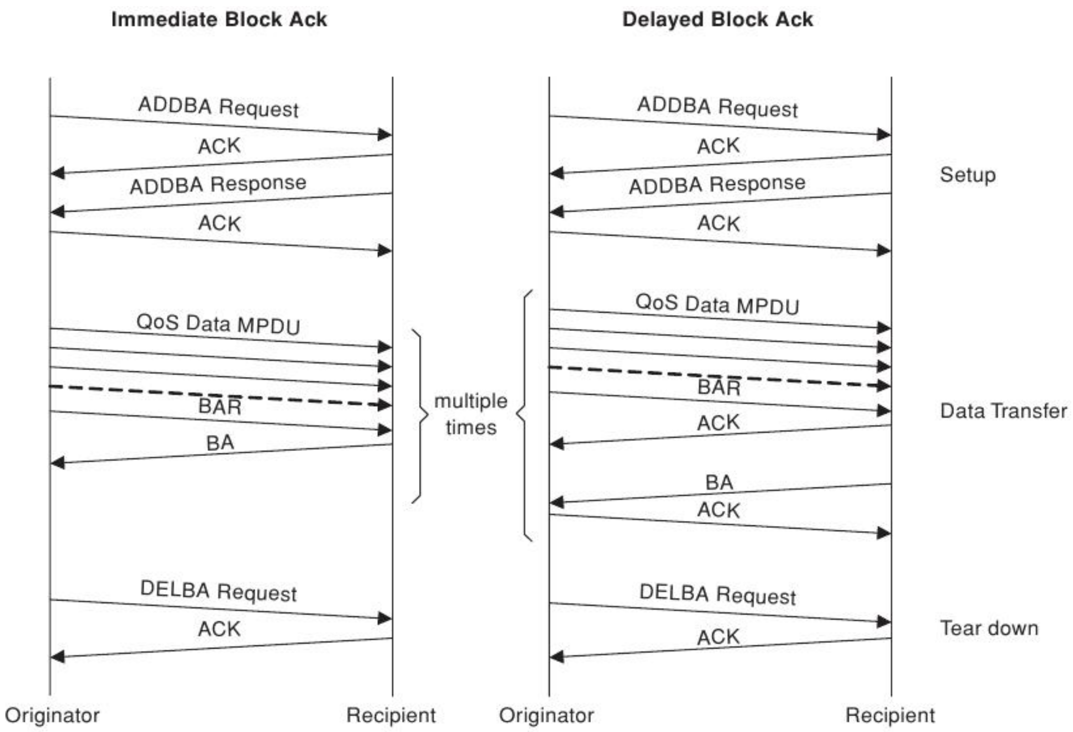


Figure 2.2 Immediate and delayed block ACK sessions [15]

2.2.5 IEEE 802.11f

In 2000, IEEE 802.11 Task Group f (TGf) started to work on a recommended practice for a protocol to be used between IEEE 802.11 APs, the Inter Access Point Protocol (IAPP), today known as IEEE 802.11.1. The goals of IEEE 802.11f are to provide a recommended way for APs to communicate with each other when a mobile station (STA) roams between them, to describe a way for an AP to update the forwarding tables in IEEE 802.1 MAC bridges that may be included in the IEEE 802.11 DS, to establish a format for APs to exchange context information about a station that has roamed, and to enable the distribution of station context information from one AP to neighboring APs. Some of the things that IEEE 802.11f does not define is what an AP should put into the context container in order to communicate with a peer AP or which format should have the information in the context container. This was purposely left for future standardization [14]. IEEE 802.11f was a Trial Use Recommended Practice and the IEEE 802 Executive Committee approved its withdrawal on February 2006.

2.2.6 IEEE 802.11g

IEEE 802.11g is the third modulation standard for wireless LANs and was finally approved on June 2003. Since IEEE 802.11a is operating in the 5 GHz band, it lacks of backward compatibility with plain IEEE 802.11 devices. This is one of the main reasons that led to the formation of IEEE 802.11g. Basically, IEEE 802.11g attempts to combine the advantages of both 802.11a and 802.11b. It uses the 2.4 GHz band, just like IEEE 802.11b does, but it reaches a maximum raw data rate of 54 Mbit/s using the OFDM modulation scheme, as IEEE 802.11a does.

802.11g received major acceptance and was rapidly adopted by customers even before its ratification, due to the need for higher speeds and reduced manufacturing costs. However, it still suffers from the same interference as IEEE 802.11b, in the already crowded 2.4 GHz range.

2.2.7 IEEE 802.11h

In 1999, the European Union modified its regulations that applied to the radio band used by IEEE 802.11a. The new regulations required that any wireless device or system operating in the 5 GHz band must implement four (4) new functions, in order to protect existing civil and military radar that already operates in the band, as well as to minimize the “hotspot” that might show up in urban areas in radar images of earth satellite systems and also use this band. These four requirements are:

i. The device must be able to detect the presence of radar operations.
ii. The device or system must be able to avoid interfering with radar operations.
iii. The system must be able to uniformly spread its operation across all the channels that may be used in the band.
iv. The system must be able to minimize the overall power output of the system.

To ensure that IEEE 802.11 WLANs operated in a consistent fashion when implementing systems to the new regulations, the IEEE 802.11 Task Group h (TGh) was chartered to write an amendment to the IEEE 802.11 standard. The amendment was ratified by the IEEE in July 2003 [14].

2.2.8 IEEE 802.11i

Late in 1999, several weaknesses of the Wired Equivalent Privacy (WEP) algorithm of the initial IEEE 802.11 standard began to arise. Additionally, its pre-shared keying concept did not allow for integration into enterprise networks, where each device should have its own unique key. Thus, companies required their employees to use Virtual Private Networks (VPNs) and IEEE 802.11 became synonym for insecurity [8].

As mentioned earlier, in 2000 the TGe was approved, aiming to work on both security and QoS enhancements. In May 2001, TGi was split from TGe to focus only on security enhancements. The task for TGi was two-fold [14]:

- To create a new, very secure means of authentication and privacy that would no be vulnerable to the weaknesses of WEP.
- To enhance the security characteristics of the existing WEP.

Meanwhile, the Wi-Fi Alliance (WFA) did not wait for a solution and started its Wi-Fi Protected Access (WPA) certification program. WPA was an intermediate solution to WEP insecurities, that implemented a subset of a draft of IEEE 802.11i. IEEE 802.11i was finally approved in June 2004 and the result of its work were the Robust Security Network (RSN) and the Transition Security Network (TSN).

The WFA refers to their approved, interoperable implementation of the RSN, as WPA2. RSN has been developed to provide very strong encryption and strong per-packet authenticity. It also includes an encryption scheme designed from scratch, that relies on the Advanced Encryption Standard (AES), whereas both WEP and WAP make use of the RC4 stream cipher mechanisms. However, it should to be noted that IEEE 802.11i does not address all of the security problems that plague a WLAN. IEEE 802.11i specifically addresses authentication and confidentiality of data frames but it does not address other shortcomings of IEEE 802.11, such as protection of management frames, prevention of denial of service attacks, or prevention of attacks that may take place in higher layers, e.g., ARP spoofing [14].

Old hardware cannot be upgraded to make use of RSN. Thus, legacy devices would not be able to coexist in the same network with newer ones that make use of RSN. TSN provides a method for legacy equipment that is capable only of WEP encryption to operate together with equipment that provides RSN capabilities, in a mixed environment.

2.2.9 IEEE 802.11j

In August 2002, the Japanese government expanded the frequency band of operation beyond the 5.15-5.25 GHz range, to include both the licensed and unlicensed spectrum from 4.9 GHz to 5.25 GHz, for operating WLANs inside the country. Approved in December 2002 and ratified in September 2004, IEEE 802.11j describes the necessary means to comply with the new Japanese regulatory requirements. and its new applications. The specifications for IEEE 802.11j were defined so that legacy IEEE 802.11a 5 GHz WLANs would require only minimal changes to the PHY hardware and software of the radios [14].

2.2.10 IEEE 802.11k

Approved in December 2002 and ratified in March 2008, IEEE 802.11k is an amendment for radio resource management. It is intended to improve the way traffic is distributed within a network, by defining a series of measurement requests and reports that can be used in layers above the MAC. IEEE 802.11k enables a radio network to collect information regarding other APs and link quality to neighbor stations. It also provides methods to measure interference levels and medium load statistics [16]. In a wireless LAN if there are more than one APs, a station will connect to the one with the strongest signal. However, this can sometimes lead to excessive demand on this AP, while the others remain underutilized. In a network conforming to IEEE 802.11k, if the AP having the strongest signal is loaded to its full capacity, a connected station can switch to one the underutilized APs. Even though the signal may be weaker, the overall throughout is greater because of the more efficient use of network resources. The steps for a station to switch to a new AP are the following:

- The associated AP determines that the station should switch to another AP.
- The AP informs the station to prepare to switch to a new AP.
- The STA requests a list of the nearby APs.
- The AP provides the STA with the requested list.
- The station moves to the best AP based on the reported list.

2.2.11 IEEE 802.11n

IEEE 802.11n amendment defines modifications to both IEEE 802.11 PHY and MAC layer, aiming to a significant increase of the maximum data rate. In particular, IEEE 802.11n can derive a throughput from 100 Mbit/s up to 600 Mbit/s, which is far beyond the maximum throughput of 54 Mbit/s that was supported by then. To achieve that, IEEE 802.11n inherited some new technologies to the existing IEEE 802.11 standard, with the most notable being the so called Multiple-Input Multiple-Output (MIMO). MIMO is a form of “smart antenna” technology. It can use up to four antennas, to resolve more data than possible using a single antenna (Figure 2.3). To provide this, it uses either Spatial Division Multiplexing (SDM), or beam forming.

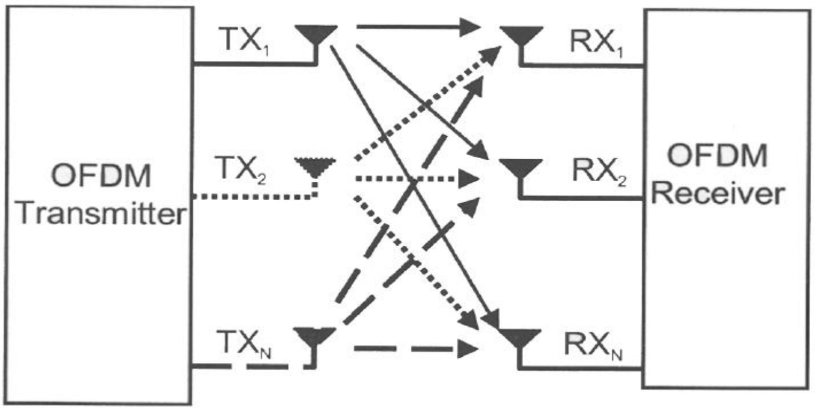


Figure 2.3 MIMO with TXN transmit and RXN receive antennas [14]

MIMO systems offer a number of benefits to WLANs, such as [14]:

- Using several antennas, the signal strength can be significantly improved.
- The interference probability is decreased.
- Higher channel capacity.
- The receiver has the possibility to recover lost or corrupted data using different signal paths.

Another feature of IEEE 802.11n is the usage of optional 40 MHz channels, instead of only 20 MHz channel widths, as it was defined in the previous IEEE 802.11 PHYs. The 40 MHz operation raised many concerns regarding neighbor friendly behavior. Especially for the crowded 2.4 GHz mode, there were concerns that it would severely affect the performance of existing IEEE 802.11 and non-802.11 devices, such as Bluetooth (802.15.1) and ZigBee (802.15.4) [8]. As a consequence, the development of an appropriate compromise was a prerequisite for IEEE 802.11n's ratification, which was finally made six years later, in September 2009. As a result, IEEE 802.11n devices can operate in 40 MHz mode only if they are able to detect 20 MHz-only devices. They can also be enabled to operate in the 5 GHz band or, alternatively, in the 2.4 GHz only if there is knowledge that they will not interfere with other devices.

Finally, IEEE 802.11n introduces enhancements in the MAC layer, too, with the main mechanisms being frame aggregation and block acknowledgment. With frame aggregation multiple data packets from the Network layer (OSI layer 3) are combined in one larger frame for transmission. Frame aggregation achieves better channel utilization from the legacy frame encapsulation mechanism, since there is reduced header overhead, in addition to inter-frame time. IEEE 802.11n supports a two-level aggregation technique. At the top of the MAC there is the MAC Protocol Service Unit (MSDU) aggregation (A-MSDU), which forms a MAC Protocol Data Unit (MPDU). Then, in the second level, at the bottom of the MAC there is the MPDU aggregation (A-MPDU) which forms a PSDU that is passed down to the PHY layer [15].

As mentioned earlier, in sub-chapter 2.2.4, block acknowledgment was initially introduced by the IEEE 802.11e. IEEE 802.11n enhances this mechanism to support frame aggregation and further improve the network efficiency. The resulted mechanisms are referred to as HT-immediate block ACK and HT-delayed block ACK, where HT stands for High Throughput.

2.2.12 IEEE 802.11p

Published in 2010, IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add Wireless Access in Vehicular Environments (WAVE). It describes several modifications brought to the PHY and MAC layers of the original standard in order to support Intelligent Transportation Systems (ITS) applications. ITS basically refers to information being exchanged between high speed vehicles or between vehicles and roadside infrastructure aiming to improve transport outcomes, such as safety, reliability and comfort. IEEE 802.11p operates in 5.855-5.925 GHz band in the United States, and the 5.855-5.905 GHz band in Europe, which was recently harmonized for IEEE 802.11p operation. Its PHY is similar to OFDM-based IEEE 802.11a, with the major difference that IEEE 802.11p operates on 10 MHz wide channels, instead of 20 MHz.

2.2.13 IEEE 802.11r

With the advancements of Wireless LANs, fast roaming support has become one of the most important issues in IEEE 802.11. The TGr was formed in 2004 to address roaming capabilities of real-time applications with an attempt to minimize BSS transition time, while still providing the IEEE 802.11i security and IEEE 802.11e QoS. IEEE 802.11r permits seamless connectivity with a fast and secure handover from one AP to another, within the same mobility domain [17]. With IEEE 802.11r, a station can negotiate security and QoS settings with neighbor APs, while it is still associated to another AP. Thus, if a station loses connectivity with the AP and re-associates to a neighbor AP, the duration of the re-connectivity can be substantially reduced. IEEE 802.11r was finally approved in June 2008.

2.2.14 IEEE 802.11s

IEEE 802.11s is an amendment to the IEEE 802.11 standard for mesh networking. The project got approved in 2004 and in June 2011, the TGs Draft 12.0 closed with 97.2% approval rate. IEEE 802.11s defines a multi-hop framework, where wireless devices can interconnect to create a WLAN mesh network, by serving as wireless routers. Precisely, it defines mechanisms that:

- Determine how to route packets through the mesh.
- Allow access to external networks, such as the Internet.
- Allow stations to access the mesh network.

2.2.15 IEEE 802.11w

IEEE 802.11w is the most recent security related amendment and was released in September 2009. It consists an amend to the IEEE 802.11i, and its objective is to protect against subtle attacks on wireless LAN management frames. For example, it protects against network disruption caused by malicious systems that forge disassociation requests, that appear to be sent by valid equipment. This is achieved by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity and replay protection.

2.2.16 IEEE 802.11y

In 2005 the FCC established a new regulatory regime for systems that operate within the 3.65-3.70 GHz band [8]. IEEE 802.11y, which approved for publication in June 2008, enables high-powered Wi-Fi equipment to operate in the 3.65-3.7 GHz band in the United States. With up to 20 W output power, stations operating at the US 3.65 GHz band can communicate at distances of 5 km or more. IEEE 802.11y adds three new concepts to the IEEE 802.11 base standard:

- Contention Based Protocol (CBP): enhancements to carrier sensing and energy detection mechanisms.

- Extended Channel Switch Announcement (ECSA): a mechanism for an AP to notify the associated stations of its intention to change channels or to change channel bandwidth.
- Dependent Station Enablement (DSE): is the process by which an enabling station grants permission and dictates operational procedures to dependent stations.

Title	Project approval date	Final approval date	Title	Comment
802.11a	16-09-1997	16-09-1999	Higher Speed PHY Extension in the 5GHz Band	54 Mbit/s OFDM PHY in 5 GHz
802.11b	09-12-1997	16-09-1999	Higher Speed PHY Extension in the 2.4 GHz Band	11 Mbit/s DSSS PHY in 2.4 GHz
802.11d	26-06-1999	14-06-2001	Operation in Additional Regulatory Domains	Allows devices to comply with regional requirements
802.11e	30-03-2000	22-09-2005	MAC Enhancements QoS	Support for QoS
802.11f	30-03-2000	12-06-2003	Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation	Released as 802.11.1 and administratively withdrawn on 03-02-2006
802.11g	21-09-2000	12-06-2003	Further Higher Data Rate Extension in the 2.4 GHz Band	54 Mbit/s OFDM PHY in 2.4 GHz
802.11h	07-12-2000	11-09-2003	Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe	In Europe, 5 GHz devices must implement 802.11h
802.11i	30-05-2001	24-06-2004	MAC Security Enhancements	MAC security enhancements, known as WPA and WPA2
802.11j	11-12-2002	23-09-2004	4.9 GHz-5 GHz Operation in Japan	Compliance with Japanese 5 GHz spectrum regulation
802.11k	11-12-2002	31-03-2008	Radio Resource Measurement	Measurements of the wireless channel
802.11n	11-09-2003	11-09-2009	High Throughout	600 Mbit/s MIMO PHY in 2.4 GHz and 5 GHz

802.11p	23-09-2004	15-07-2010	Wireless Access for the Vehicular Environment	Car to car communication, closely related to IEEE 1609
802.11r	13-05-2004	30-06-2008	Fast Roaming	Fast hand-off for moving devices
802.11s	13-05-2004	01-08-2011	Mesh Networking	Transparent multi-hop operation
802.11w	20-03-2005	30-09-2009	Protected Management Frames	Security for management frames
802.11y	16-03-2006	30-06-2008	3650-3700 MHz Operation in USA	Contention-based protocols for FCC band 3.65 GHz in the U.S.

Table 2.1 Published amendments [8]

2.3 Ongoing standardizations

2.3.1 IEEE802.11ac

IEEE 802.11ac is an emerging amendment that aims to push WLAN throughput over the gigabit-per-second barrier and up to 7 Gb/s. The following new technologies are introduced in the IEEE 802.11ac draft standard, among others:

- Multi-user multiple-input multiple-output (MU-MIMO)
- Larger channel bandwidths of 80 and 160 MHz

Most wireless networks have multiple active clients that share the available bandwidth. If this sharing is done in time, then the overall throughput can only be increased by increasing the link rate for all clients. However, many clients may not be able to transmit at the highest IEEE 802.11ac rates. For such clients, MU-MIMO is the solution to get significant network throughput gains. A MU-MIMO capable transmitter can transmit multiple packets simultaneously to multiple clients. In IEEE 802.11ac, a MU-MIMO mode is defined with up to eight spatial streams divided across up to four different clients. Thus, the data rate per client can be up to four times larger, because the MU-MIMO packets can be transmitted at the maximum data rate per client while without MU-MIMO, each client can only be transmitted to about a quarter of the time such that the effective per-user throughput is a quarter of its maximum [18].

IEEE 802.11ac will operate in 80 MHz and 160 MHz channel bandwidths, in addition to the 20 and 40 MHz defined in IEEE 802.11n. IEEE 802.11ac, 2 more bandwidths of 80 and 160

MHz are introduced. The 80 MHz mode uses two adjacent 40 MHz channels with some extra subcarriers to fill the unused tones between two adjacent 40 MHz channels. The 160 MHz mode uses two separate 80 MHz channels without any tone filling in the middle of these two sub-channels. The two 80 MHz channels do not have to be adjacent. This increases the probability of finding a 160 MHz channel at the cost of additional hardware to send and receive in two non-adjacent 80 MHz channels. IEEE 802.11ac only applies to the 5 GHz band, since there is no room in the 2.4 GHz band for the 80 and 160 MHz channels [18]. IEEE 802.11ac also provides backward compatibility with IEEE 802.11a and IEEE 802.11n devices.

2.3.2 IEEE 802.11ad

The objective of IEEE 802.11ad is to define standardized modifications to both IEEE 802.11 PHY and MAC layers, in order to enable operation in the 60 GHz frequency band, capable of very high throughput in short-range data transmissions. 60 GHz band can provide solutions for various applications, such as local file transfer and HD video transfer. The project got approved in December 2008 and is expected to be published by the end of 2012.

2.3.3 IEEE 802.11ae

IEEE 802.11ae is the second amendment for QoS enhancements to the IEEE 802.11 base standard. The project was approved in December 2009 and was finally approved in the first half of 2012. Its goal is to provide QoS management and prioritization of management frames.

2.3.4 IEEE 802.11af

IEEE 802.11af defines mechanisms for operation of WLAN within the TV white space, that is, the TV unused spectrum. The work started in December 2009 and by July 2011, the Draft 1.06 met with 62% approval rate. Some of the advantages of operating the TV white space are:

- Propagation characteristics: In view of the fact that the TV white spaces would use frequencies below 1 GHz, this would allow for greater distances to be achieved.
- Additional bandwidth: One of the advantages of using TV white space is that unused frequencies can be accessed. However, it will be necessary to aggregate several TV channels to provide the bandwidths that Wi-Fi uses on 2.4 and 5 GHz, to achieve the required data throughput rates.

2.3.5 IEEE 802.11ai

IEEE 802.11ai is an amendment approved in December 2010 for fast initial link setup. The project intends to amend the MAC only, thereby providing a fast initial link service to all IEEE 802.11 devices. One way to achieve that, is by reducing the number of messages transmitted per user during set-up, to free airtime and increase the number of users that may simultaneously enter an ESS. The project does not intend to remove any existing mechanisms of IEEE 802.11 but to add additional, coexisting functionality, enabling fast initial link set-up. The project is still in a very early phase and no draft has been released, yet.

2.3.6 IEEE 802.11ah

This amendment defines an OFDM physical layer operating in the license-exempt bands below 1 GHz, excluding the TV white space band. The data rates defined in this amendment optimize the rate vs range performance of the specific channelization in a given band. IEEE 802.11ah adds support for transmission range up to 1 km and data rate higher that 100 kb/s. As IEEE 802.11ai, IEEE 802.11ah is, also, in a very early phase and no draft has been released, yet.

Title	Project approval date	Expected final approval date	Title	Comment
802.11ac	26-09-2008	31-12-2012	Very High Throughout 6 GHz	Enhancements for > 1 Gb/s throughput for operation in bands below 6 GHz
802.11ad	10-12-2008	31-12-2012	Very High Throughout 60 GHz	Enhancements for > 1 Gb/s throughput for operation in 60 GHz band
802.11ae	09-12-2009	31-12-2012	Prioritization of Management Frames	QoS management and prioritization of management frames
802.11af	09-12-2009	31-12-2013	TV White Spaces	WLAN operation within the TV white spaces
802.11ai	08-12-2010	13-12-2014	Fast Initial Link Setup	Provide a fast initial link service to all IEEE 802.11 devices
802.11ah	04-10-2010	31-12-2013	Sub 1 GHz	PHY operation in the bands below 1 GHz

Table 2.2 Amendments in process

Chapter 3

IEEE 802.11 Medium Access Control (MAC) Layer

The Medium Access Control (MAC) is a sublayer of the data link layer specified in the seven-layer OSI model (layer 2). Among other functions, it provides addressing and channel access control mechanisms that make it possible for several stations to communicate on multi-access networks. Similar to the Ethernet MAC, the IEEE 802.11 MAC uses a Carrier Sense Multiple Access (CSMA) scheme to control access to the transmission medium. However, collisions waste valuable transmission capacity, so instead of the collision detection (CSMA/CD) employed by Ethernet, IEEE 802.11 uses Collision Avoidance (CA). Also like Ethernet, IEEE 802.11 uses a distributed access scheme with no centralized controller. That is, each IEEE 802.11 station uses the same method to gain access to the medium [19].

The architecture of the MAC sublayer includes the Distributed Coordination Function (DCF), the Point Coordination Function (PCF), the Hybrid Coordination Function (HCF) and their coexistence in an IEEE 802.11 LAN (Figure 3.1). These functions are further explained in the following sub-chapters.

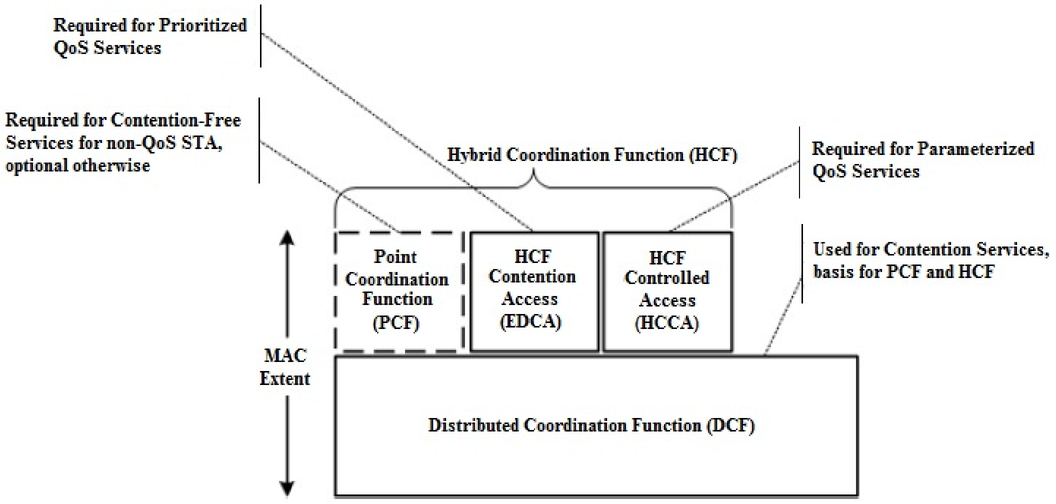

Required for Prioritized QoS Services
Required for Contention-Free Services for non-QoS STA, optional otherwise
Hybrid Coordination Function (HCF)
Required for Parameterized QoS Services
Used for Contention Services, basis for PCF and HCF
Point Coordination Function (PCF)
HCF Contention Access (EDCA)
HCF Controlled Access (HCCA)
MAC Extent
Distributed Coordination Function (DCF)

Figure 3.1 MAC architecture [9]

3.1 Distributed Coordination Function (DCF)

The basic medium access protocol is a DCF that allows for automatic medium sharing between compatible PHYs through the use of CSMA/CA and a random backoff time following a busy medium condition. In addition, all individually addressed traffic uses immediate positive acknowledgement (ACK frame) where retransmission is scheduled by the sender if no ACK is received [9].

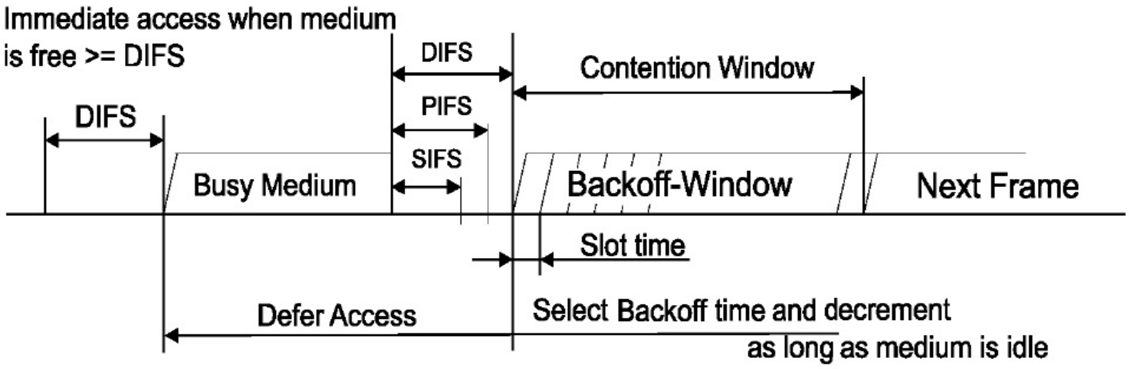

Immediate access when medium is free >= DIFS
DIFS
DIFS
PIFS
SIFS
Contention Window
Busy Medium
Backoff-Window
Next Frame
Slot time
Defer Access
Select Backoff time and decrement as long as medium is idle

Figure 3.2 Distributed Coordination Function [9]

3.1.1 Carrier Sense Multiple Access (CSMA)

CSMA is a probabilistic protocol in which a station listens to the medium before transmitting. If the medium is sensed as “idle”, the station may proceed to the transmission. Otherwise, the medium is sensed as “busy” and the station postpones its transmission. IEEE 802.11 defines two carrier sensing mechanisms to avoid interference in wireless local area networks for the kind of interference originating from within the receiving range of a receiver [21]. The two mechanisms and the function each one uses are summarized in Table 3.1.

Carrier Sensing Mechanism	Function	Description
Physical carrier sensing	Clear Channel Assessment (CCA)	Indicates a busy medium for the current frame
Virtual carrier sensing	Network Allocation Vector (NAV)	Reserves the medium as busy for future frames

Table 3.1 IEEE 802.11 Carrier Sensing Mechanisms

The CCA is composed of two related functions; Carrier Sense (CS) and Energy Detection (ED). The first one refers to the ability of a station to detect and decode incoming Wi-Fi signal preamble, while ED refers to the ability of a station to detect non-Wi-Fi energy level present on the current channel. Such an energy level may be produced by external sources that interfere. Unlike CS which can determine the exact length of the time the medium will be busy with the current frame, ED must sample the medium every slot time to determine if the energy still exists [21]. While CCA itself is implemented at the PHY layer, the primary impact of its performance and complexity is on MAC metrics like throughput and energy efficiency. The channel status is determined by the sensed signal power level in the channel. If the power level is above a predefined threshold, the medium is considered to be busy, otherwise idle.

In addition to CCA determining the medium idle/busy state for the current frame and noise, the NAV allows stations to indicate the amount of time required for transmission of required frames immediately following the current frame. It is important to reserve the medium as busy for these mandatory frames. The importance of NAV virtual carrier sense is to ensure medium reservation for frames critical to the operation of the IEEE 802.11 protocol. Typically these are control frames, but not always. They include IEEE 802.11 acknowledgments, subsequent data and acknowledgment frames as part of a fragment burst, and data and acknowledgment frames following an RTS/CTS exchange [21]. Finally, the medium is determined to be idle only when both the physical and virtual carrier sense mechanisms indicate it to be so [15].

3.1.2 Collision Avoidance (CA), Random Backoff & Contention Window

The purpose of CA is to improve the performance of CSMA by attempting to divide the wireless channel somewhat equally among all transmitting nodes within the collision domain. Every station that wishes to transmit first senses the medium for a fixed duration, called DCF Inter-Frame Space (DIFS). If the medium is idle the station assumes it may take ownership of the medium and begin a frame exchange sequence. If the medium is busy, the stations waits for the medium to go idle, defers for DIFS, and waits for a further random backoff period. If the medium remains idle for the DIFS deferral and the backoff period, the stations assumes that it may take ownership of the medium and begin a frame exchange sequence [21].

The random backoff period provides the CA aspect. When the network is loaded, multiple stations may be waiting for the medium to go idle having accumulated packets to send while the medium was busy. Since each station probabilistically selects a different backoff interval, collisions where more than one stations begin transmission at the same time are unlikely. The length of the backoff period is determined by the following equation:

BackoffTime = Random() x aSlotTime

where:

Random() = Pseudo-random integer drawn from a uniform distribution over the interval [0, CW], where CW (Contention Window) is an integer within the range of values of the PHY characteristics aCWmin and aCWmax, aCWmin ≤ CW ≤ aCWmax. It is important that designers recognize the need for statistical independence among the random number streams among stations.

aSlotTime = The value of the correspondingly named PHY characteristic.

Once CW reaches aCWmax, it shall remain at the value of aCWmax until it (CW) is reset. This improves the stability of the access protocol under high-load conditions [9].

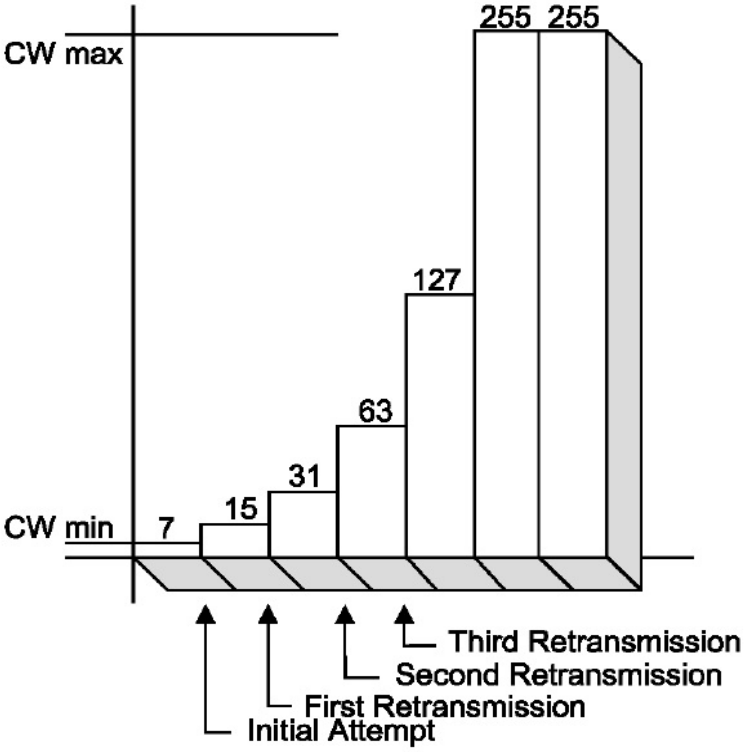


Figure 3.3 CW incrementation example [9]

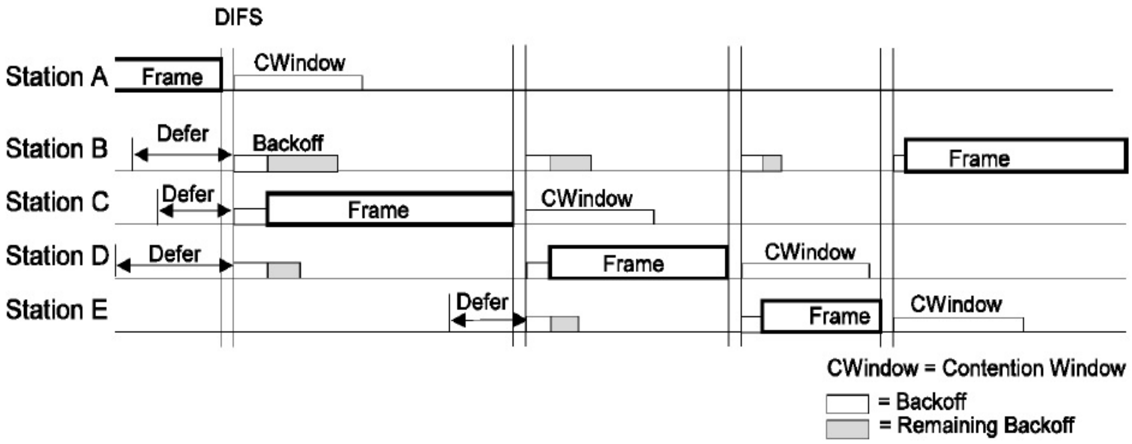


Figure 3.4 Backoff Procedure for DCF [9]

3.1.3 Request to Send/Clear to Send (RTS/CTS) Frame Exchange

CA cannot detect transmissions from hidden nodes. RTS/CTS, on the other hand, helps to solve this problem (the hidden node problem). To protect its transmission a station may begin a sequence with an RTS/CTS exchange. During this sequence a station wishing to transmit sends an RTS frame after it has sensed the medium as idle. The destination station responds to the RTS frame with a CTS frame after a SIFS (Short Interframe Spacing – used for high-priority transmissions) period has elapsed. Upon successful reception of the CTS frame, the transmitting station assumes that the medium is reserved and may start sending the actual data. Any other station that receives an RTS or CTS frame reads the duration field and sets its NAV accordingly, so that it refrains from sending data for the given time. Also, RTS and CTS are short frames which occupy less air time than the data frames and are, thus, less susceptible to collisions.

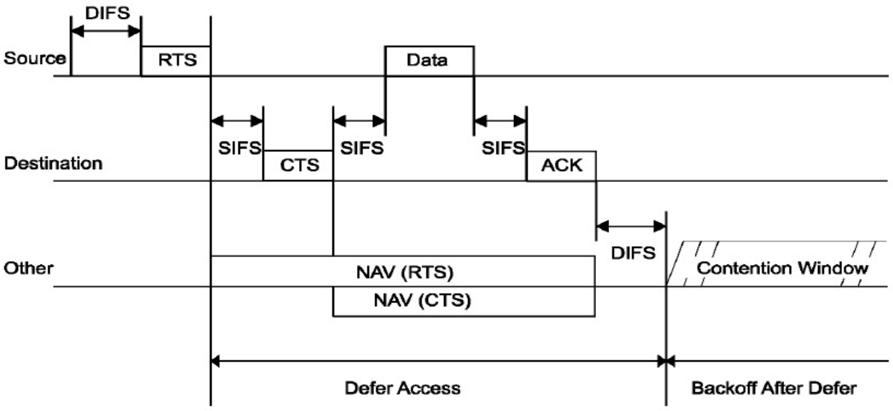


Figure 3.5 RTS/CTS/data/ACK and NAV setting [9]

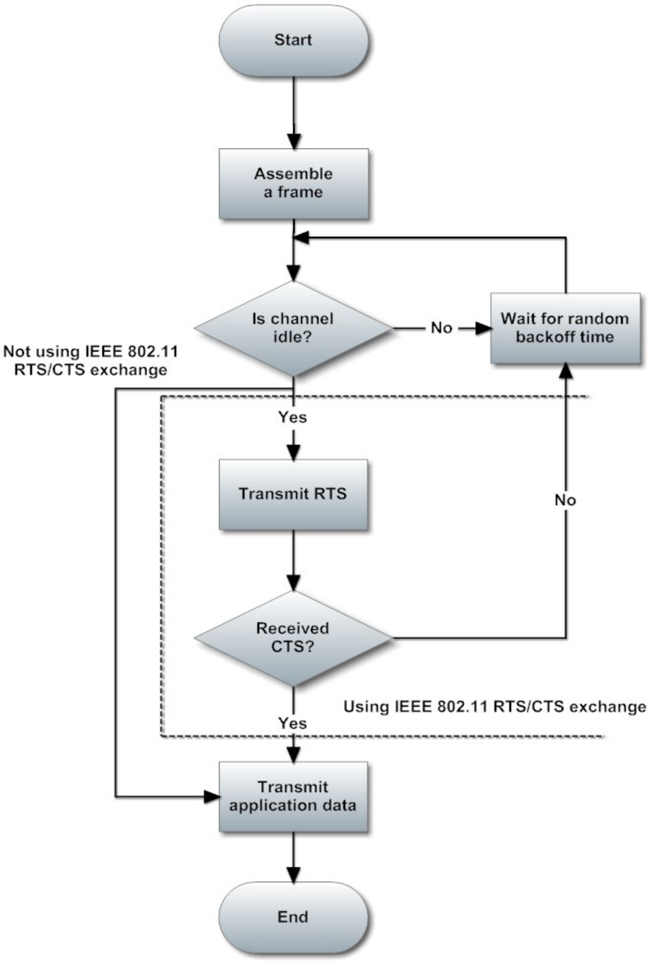

Start
Assemble a frame
Is channel idle?
No
Wait for random backoff time
Not using IEEE 802.11 RTS/CTS exchange
Yes
Transmit RTS
No
Received CTS?
Using IEEE 802.11 RTS/CTS exchange
Yes
Transmit application data
End

Figure 3.6 Simplified algorithm of CSMA/CA

3.2 Point Coordination Function (PCF)

The IEEE 802.11 MAC may also incorporate an optional access method called PCF, which is only employed for infrastructure network configurations. This access method uses a Point Coordinator (PC), which shall operate at the AP of the BSS, to determine which station currently has the right to transmit. The operation utilizes polling, with the PC performing the role of the polling master.

The PCF uses a virtual CS mechanism aided by an access priority mechanism. The PCF shall distribute information within Beacon management frames to gain control of the medium by setting the NAV in stations. In addition, all frame transmissions under the PCF may use an interframe space (IFS) that is smaller than the DIFS for frames transmitted via the DCF. The use of a smaller IFS implies that the point-coordinated traffic shall have priority access to the medium over stations in overlapping BSSs operating under the DCF access method [9].

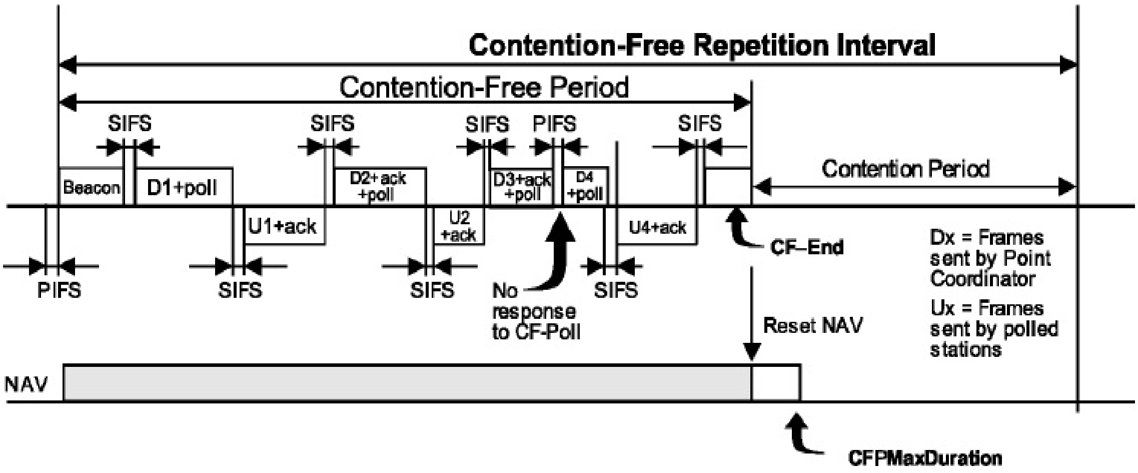


Figure 3.7 Point Coordination Function [9]

3.3 Hybrid Coordination Function (HCF)

The IEEE 802.11e is an approved amendment to the IEEE 802.11 standard that defines a set of Quality of Service (QoS) enhancements for the wireless LAN applications through modifications to the MAC layer. QoS is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. The IEEE 802.11e extends the DCF and PCF, through a new coordination function, namely HCF, that enhances QoS functionality to QoS aware applications. HCF is only usable in QoS network configurations and shall be implemented in all QoS stations. The HCF combines functions from the DCF and PCF with some enhanced, QoS-specific mechanisms and frame subtypes to allow a uniform set of frame exchange sequences to be used for QoS data transfers during both the Contention Period (CP) and the Contention Free Period (CFP). The HCF uses both a contention-based channel access method, called the Enhanced Distributed Channel Access (EDCA) mechanism for contention-based transfer and a controlled channel access, referred to as the HCF Controlled Channel Access (HCCA) mechanism, for contention-free transfer [9].

3.3.1 HCF Contention Based Channel Access (EDCA)

The EDCA mechanism provides differentiated, distributed access to the wireless medium for stations using eight different User Priorities (UPs). The EDCA mechanism defines four access categories (ACs) that provide support for the delivery of traffic with UPs at the stations [9]. The mapping between the UPs and the ACs is demonstrated in Table 3.2.

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	-	AC_BK	Background
	0	BE	AC_BE	Best Effort
↓	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

Table 3.2 UP-to-AC mappings [9]

Every station maintains four transmit queues, one per AC as illustrated in Figure 3.8. For each AC, an enhanced variant of the DCF, called an Enhanced Distributed Channel Access Function (EDCAF), contends for TXOPs using a set of EDCA parameters from the EDCA Parameter Set element received from the associated AP, or from the default values for the parameters if no EDCA Parameter Set element is received.

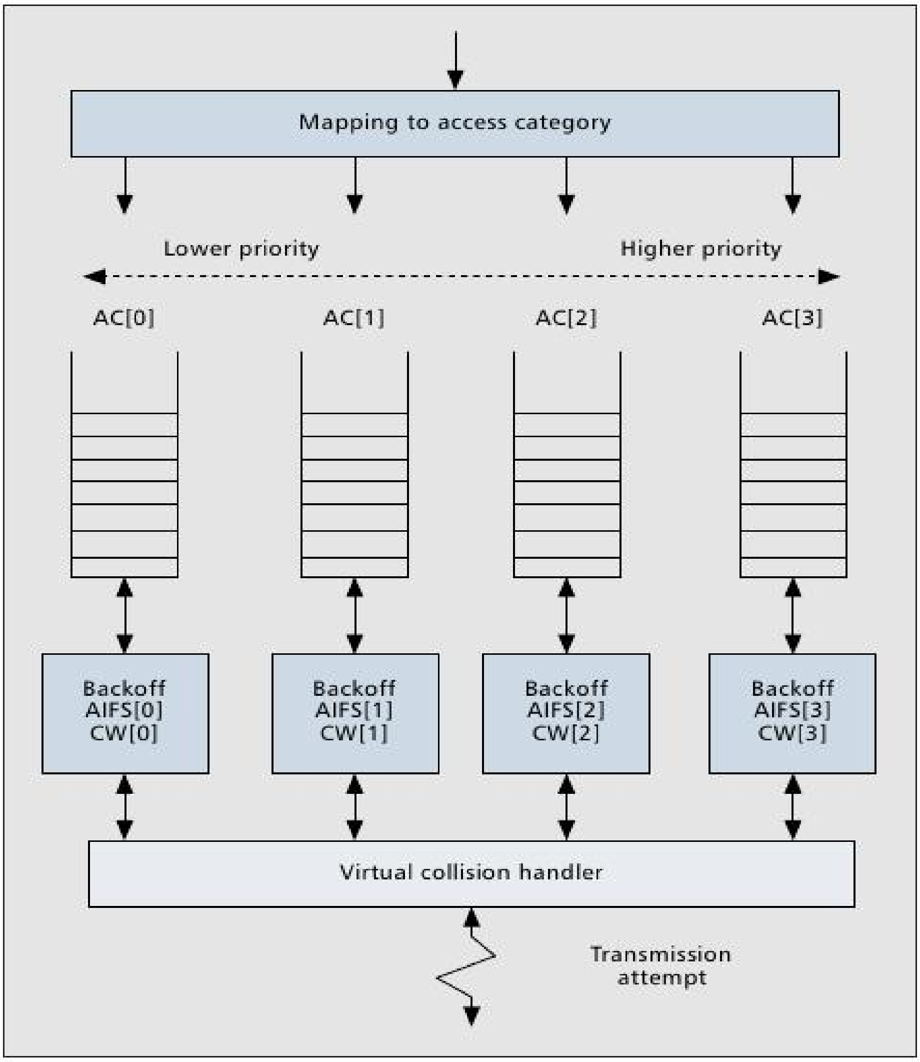


Figure 3.8 Reference implementation model [22]

The EDCA Parameter Set element is used by the AP to establish policy, to change policies when accepting new stations or new traffic, or to adapt to changes in offered load. The EDCA Parameter Set includes the following parameters [22]:

- Minimal CW value for a given AC (CWmin[AC]): CWmin can be different for different ACs. Assigning smaller values of CWmin to high priority classes can ensure that high-priority classes obtain more TXOPs than low-priority ones.
- Maximal CW value for a given AC (CWmax[AC]): Similar to CWmin, CWmax is also on a per AC basis.
- Arbitration Interframe Space (AIFS[AC]): Each AC starts its backoff procedure after the channel is idle for a period of AIFS[AC] instead of DIFS. The AIFS[AC] for a given AC should be equal to an SIFS plus multiple time slots (i.e., AIFS[AC] = sSIFSTime + AIFSM[AC]*aSlotTime). Considering in legacy IEEE 802.11 we have

DIFS = aSIFSTime +2*aSlotTime, AIFSN[AC] is typically set to not less than 2 such that the shortest waiting time is DIFS.

- TXOPlimit[AC]: TXOPs obtained via EDCA are referred as EDCA-TXOPs. During an EDCA-TXOP, a station may be allowed to transmit multiple data frames from the same AC with a SIFS gap between an ACK and the subsequent data frame transmission. TXOPlimit[AC] gives the limit for such a consecutive transmission.
- Virtual collision: If the backoff counters of two or more collocated ACs in one station elapse at the same time, a scheduler inside the station treats the event as a virtual collision. The TXOP is given to the AC with the highest priority among the "colliding" ACs, and the other colliding ACs defer and try again later as if the collision occurred in real medium.

AC	**CWmin**	**CWmax**	**AIFSN**	**TXOP Limit DC-CCK/PBCC PHY**	**TXOP Limit OFDM/CC-OFDM PHY**
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	aCWmax	3	0	0
AC_VI	(aCWmin+1)/2 - 1	aCWmin	2	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4 - 1	(aCWmin+1)/2 -1	2	3.264 ms	1.504 ms

Table 3.3 Default EDCA Parameter Set element parameter values [9]

The QoS AP announces the EDCA Parameter Set element in all Beacon frames occurring within two or more Delivery Traffic Indication Message (DTIM) periods following a change in AC parameters to assure that all stations are able to receive the updated EDCA parameters. Moreover, the EDCA Parameter Set element is included in all Probe Response and (Re)Association Response frames. If no such element is received, the stations shall use the default values for the parameters.

3.3.2 HCF Controlled Channel Access (HCCA)

Unlike EDCA and TXOP, HCCA is an optional enhancement for IEEE 802.11e networks. In fact, few (if any) APs currently available are enabled for HHCA. The HCCA mechanism uses a QoS-aware centralized coordinator, called Hybrid Coordinator (HC), and operates under rules that are different in several significant ways from the PC of the PCF, although it may optionally implement the functionality of a PC. In contrast to PCF, in which the interval between two beacon frames is divided into two periods of CFP and CP, the HCCA allows for CFPs being initiated during a CP. This kind of CFP is called a Controlled Access Phase (CAP) in IEEE 802.11e. A CAP is initiated by the AP whenever it wants to send a frame to a station or receive a frame from a station in a contention-free manner. In fact, the CFP is a CAP, too. The HCF protects the transmissions during each CAP using the virtual CS mechanism. A station may initiate multiple frame exchange sequences during a polled TXOP of sufficient duration to perform more than one such sequence. The use of virtual CS by the HC provides improved protection of the CFP.

HCCA allows for the reservation of TXOPs with the HC. A station based on its requirements requests the HC for TXOPs, both for its own transmissions as well as for transmissions from the AP to itself. The HC either accepts or rejects the request based on an admission control policy. If the request is accepted, the HC schedules TXOPs for both the AP and the station. For transmissions from the station, the HC polls the station based on the parameters supplied by the station at the time of its request. For transmissions to the station, the AP directly obtains TXOPs from the collocated HC and delivers the queued frames to the station, again based on the parameters supplied by the station.

Generally, HCCA is considered to be the most advanced and complex coordination function, allowing QoS to be configured with great precision. QoS-enabled stations have the ability to request specific transmission parameters, such as data rate, jitter, etc. This should allow advanced applications like VoIP and video streaming to work more effectively on a Wi-Fi network.

Chapter 4

Stream Classification Service and Interworking with 802.1AVB

4.1 Stream Classification Service

The Stream Classification Service aims to cover two of the targets within the scope of the IEEE 802.11aa amendment:

- Intra-Access Category prioritization: the need to differentiate between separate streams within the same access category
- Graceful degradation: In situations with insufficient channel capacity, there needs to be a mechanism that marks the less important information as discardable, providing a more graceful video degradation.

As mentioned in sub-chapter 3.1.3.1, the EDCA function in IEEE 802.11e, that provides QoS for video and voice streams, specifies four Access Categories (AC) with different priorities. The differentiation is enforced by configuring the contention parameters used by the station to content for the medium, which are the minimum and maximum size of the Contention Window (CWmin and CWmax), the Arbitration Inter-Frame Space (AIFS) and the maximum size of the Transmission Opportunity (TXOP). Higher priority access categories have a smaller contention window and shorter inter-frame space, increasing the probability of the frame taking hold of the medium.

The problem of the IEEE 802.11e EDCA function in the case of video transmission is that with only four (4) access categories, there is only one category reserved for voice traffic and one for video streams. However, there may be a need for simultaneous transmission of many video streams with different performance restrictions. For example, video conferencing has a smaller tolerance for delay and jitter than streaming video. In the current EDCA scheme, these streams should belong to the same access category and there is no way to give one stream higher priority over the other. Also, the smaller contention window for the video access category means that there is a higher collision probability in the presence of multiple streams that leads to retransmissions and throughput degradation.

4.1.1 Intra-access category prioritization

The target of the IEEE 802.11aa Task Group was to increase the granularity of the EDCA access categories without making major changes to the EDCA function of the IEEE 802.11 standard. To achieve this, it provides an alternate transmit queue for the two highest priority access categories; voice and video. This allows individual streams with different requirements that belong to the same access category to access the medium with different priority. Figure 4.1 shows how the EDCA function operates when intra-access category prioritization is used. The packets for the primary and the alternate queue in each access category are kept in separate buffers. A scheduling function selects a frame between the primary and the alternate queue before it is passed on to the video or voice EDCA function, with a higher probability to select a frame from the queue that has a higher User Priority. Having six queues allows for a better mapping with the 8 user priorities specified in IEEE 802.11, which are identical to the 8 priority tags in 802.1D and therefore enable better interworking of IEEE 802.11 with other networks (Table 4.1). The incoming frames can be classified to an alternate queue either by specifying directly the User Priority or by using the Intra-Access Category Priority element when the Traffic Stream is set-up (Figure 4.2).

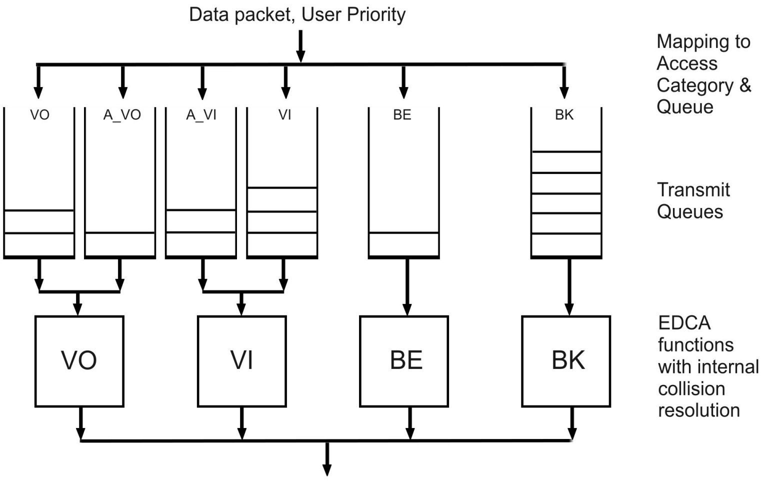

Data packet, User Priority
Mapping to Access Category & Queue
VO
A_VO
A_VI
VI
BE
BK
Transmit Queues
VO
VI
BE
BK
EDCA functions with internal collision resolution

Figure 4.1 EDCA operation with Intra-Access Category Prioritization [9]

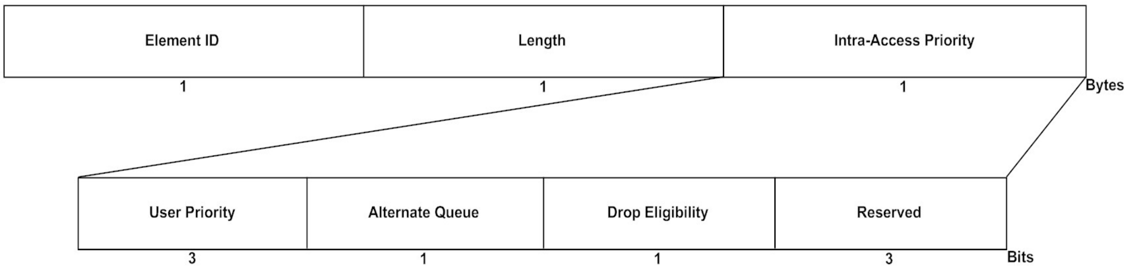


Figure 4.2 Intra-Access Category Priority Element

Priority	UP (Same as 802.1D UP)	802.1D designation	AC	Transmit Queue	Designation (informative)
Lowest	1	BK	AC_BK	BK	Background
	2	-	AC_BK	BK	Background
	0	BE	AC_BE	BE	Best Effort
↓	3	EE	AC_BE	BE	Best Effort
	4	CL	AC_VI	A_VI	Video (alternate)
	5	VI	AC_VI	VI	Video (primary)
Highest	6	VO	AC_VO	VO	Voice (primary)
	7	NC	AC_VO	A_VO	Voice (alternate)

Table 4.1 UP-to-AC mappings with 6 transmitting queues

4.1.2 Graceful degradation

The Intra-Access Category Priority element also includes a Drop Eligibility Indicator (DEI) that is connected to a stream. When a frame with the DEI bit activated is to be transmitted, the retransmission procedure keeps two different drop-eligible retry counters, long and short, that may be shorter than the normal ones. Therefore, in the case of bandwidth shortage a stream that has the DEI bit activated is more likely to reach the maximum number of retransmissions and be discarded. Also, the DEI bit appears in the MAC frame header and this allows the frame to be dropped in the receiving station if it has insufficient resources to process it. The details of when a frame is selected to be dropped are not set in the standard and are left open to the implementation.

4.1.3 Stream Classification Service (SCS)

Stream Classification Service (SCS), introduced by the TGaa, can be used to classify a range of traffic classifications to a particular Intra-Access Category Priority element. The SCS enables the establishment of a classification using layer 2 and/or layer 3 signaling to match incoming unicast MSDUs. Once classified, unicast MSDUs matching the classification are assigned to an access category and are tagged with their drop eligibility. When intra-access category prioritization is enabled, SCS allows MSDUs matching the classification to be assigned to the primary or alternate transmit queues [9]. Using the combination of the primary and alternate queue and the Drop Eligibility Bit, a transport stream that is set up between the station and the AP can achieve better prioritization between other streams.

4.1.4 Related Work

Various attempts have been made in order to provide differentiation mechanisms between traffic flows within the same priority class, thus reduce the contentions between those flows. Therefore, much of this work proposes enhancements to DCF and EDCA.

Some of the proposals consist of dynamic adjustment of the CW size. In [23], the authors try to improve the protocol capacity of IEEE 802.11 networks, by tuning its backoff algorithm. Their purpose is to show that by observing the network status, it is possible to estimate the average backoff window size that maximizes the throughput. With this estimation the optimal value of the CW can be computed, for a given congestion level, without increasing the collisions in an IEEE 802.11 network. [24] proposes a method based on Kalman filter for estimating the number of active hosts to set suitable values for CW. The Kalman filter is an algorithm which operates recursively on streams of noisy input data to produce a statistically optimal estimate of the underlying system state. The authors also enhance this approach with a change detection mechanism that detects network state variations and accordingly feed the Kalman filter. Those solution, however, are hard to be directly used in real wireless environments due to their high complexity.

In [25], the authors proposed a simple adaptive mechanism, called Dynamic Optimization On Range (DOOR) that aims at improving the IEEE 802.11 DCF by integrating system measurement with adjusting parameters, dynamically. The proposed mechanism offers a low algorithm complexity and low system cost and it is, also, applicable in complex wireless networks. This solution, however, cannot be applied to the distributed Ad Hoc mode due to the need of a central control. Qiang Ni et al. in [26] have introduced a method that is based on slow CW decrease, that after a successful transmission the CW size is divided by two, instead of being reset to the minimal value (CWmin). That way the CW value should be kept the same as long as the congestion level is not likely to drop sharply, providing more collision avoidance during congestion periods. This method, however, lacks in monitoring channel load and taking in consideration issues such as the presence of hidden nodes. Thus, it has limited adaptation to network conditions.

[27] proposed an enhanced service differentiation mechanism called Differentiation Service based on Per Queue (DSPQ). DSPQ offers an improved ability to differentiate QoS provisioning between traffic classes, while remaining overall bandwidth efficient. Through adopting traffic conditions at the entrance of MAC AC queues and maintain collision rate for each AC, DSPQ dynamically adjusts to changing conditions, confirming oscillations in throughput and delay. This allows the mechanism to provide strict service differentiation and good flow fairness, while still maintaining a high level of channel utilization. The simulations showed that, indeed, DSPQ improves the goodput and reduces delay and collision rate. Furthermore, since there is no need for a central coordinator, it can also be applicable to QoS control in wireless Ad Hoc networks.

4.2 Interworking with 802.1AVB

4.2.1 IEEE 802.1AVB

IEEE 802.1 is a working group of the IEEE 802 project of the IEEE Standards Association, an organization within IEEE that develops standards in a broad range of industries. The IEEE 802.1 working group is concerned with and develop standards and recommended practices in the following areas: 802 LAN/MAN architecture, internetworking among 802 LANs, MANs and other wide area networks, 802 link security, 802 overall network management, and protocol layers above the MAC and Logical Link Control (LLC) layers [28].

The 802.1 working group has four active task groups: Interworking, Security, Audio/Video Bridging (AVB), and Data Center Bridging (DCB) [28]. In the following pages we will make a presentation of the AVB task group and its interworking with the IEEE 802.11aa task group. The IEEE 802.1 AVB task group is developing a set of standards to allow the transport of high-quality low-latency streaming of time-sensitive audio/video applications over IEEE 802 bridged LANs. Its specific goals include [28]:

- Layer 2 time synchronizing service that is appropriate for the most stringent requirements of consumer electronics applications.
- Definition of an admission control system that allows bridges to guarantee the resources needed for AV streams.

- Enhancement of standard 802.1 bridge frame forwarding rules to support AV streams.
- Establishment of a set of usage-specific profiles using the AV bridging specifications.
- Creation of a standard for AV bridging between specific 802 LAN configurations and “802-like” LANs.

These enhancements are implemented using relatively small extensions to standard Layer 2 MACs and bridges. This allows non-AVB and AVB devices to communicate with each other using standard 802 frames. However, as shown in Figure 4.4, only AVB devices are able to:

- Reserve a portion of network resources through the use of admission control and traffic shaping.
- Send and receive the new timing-based frames.

Currently, AVB consists of the following four active projects:

- IEEE 802.1AS: Timing and Synchronization for Time-Sensitive Applications
- IEEE 802.1Qat: Stream Reservation Protocol
- IEEE 802.1Qav: Forwarding and Queuing for Time-Sensitive Streams
- IEEE 802.1BA: Audio Video Bridging Systems

IEEE 802.1Qat and 802.1Qav are amendments to the base IEEE 802.1Q document, which specifies the operation of “Virtual Bridged Local Area Networks”. Note that a bridged network refers to multiple network segments connected to each other at the data link layer (Layer 2) of the OSI model.

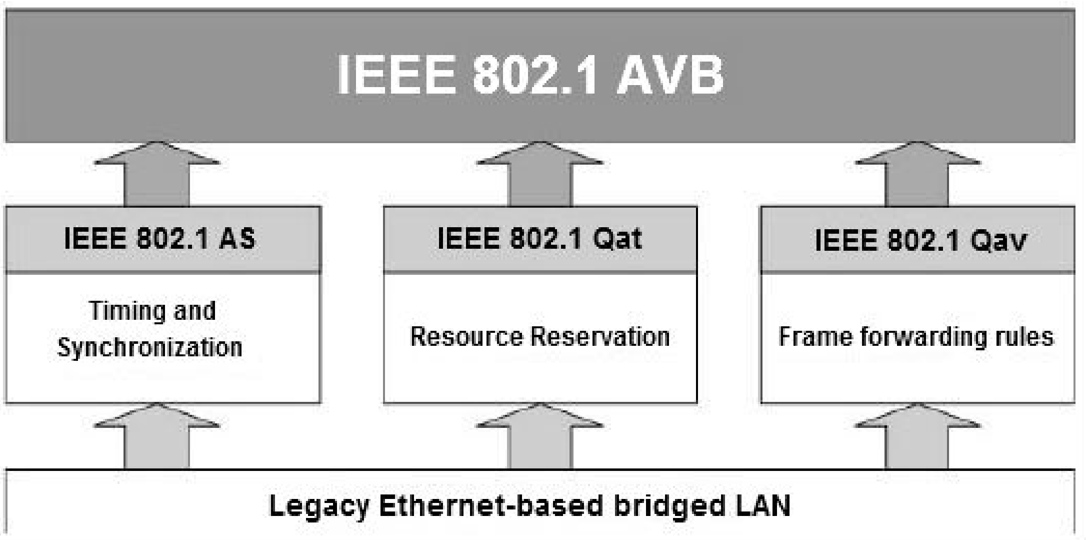


Figure 4.3 Overview of IEEE 802.1 AVB

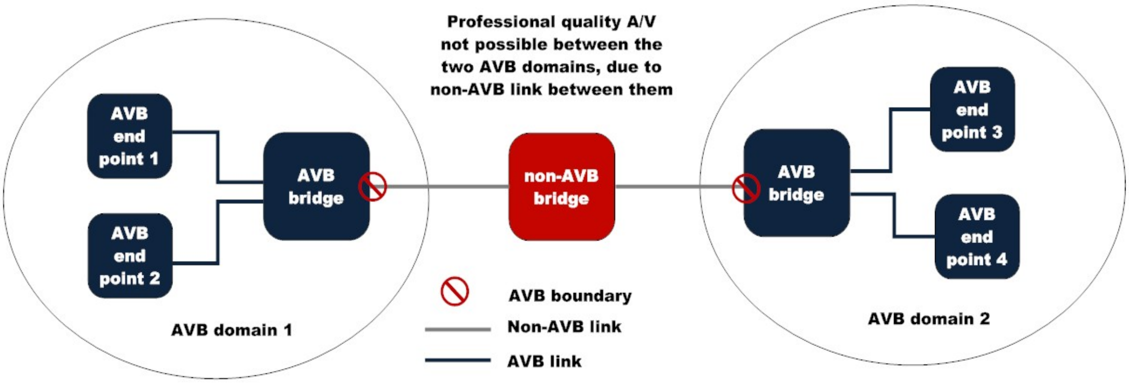


Figure 4.4 AVB Connections

4.2.1.1 IEEE 802.1AS

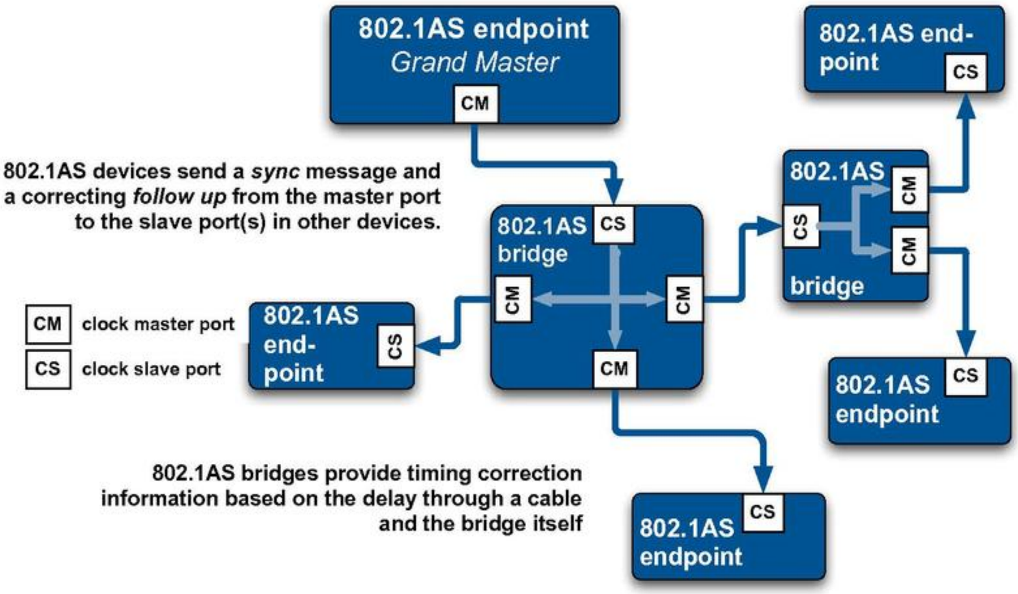
IEEE 802.1AS specifies the transport of timing and precise synchronization in bridged full-duplex IEEE 802.3 and IEEE 802.11 networks. This precise synchronization has two purposes:

i. To allow synchronization of multiple streams.
ii. To provide a common time base for sampling/receiving data streams at a source device and presenting those streams at the destination device with the same relative timing.

A bridge or end station that meets the requirements of IEEE 802.1AS is referred to as a “time-aware” bridge or end station, respectively. IEEE 802.1AS relies on the transfer of timestamps using mechanisms that are medium depended. Specifically, for a full-duplex Ethernet medium, 802.1AS uses a subset of IEEE 1588, a protocol used to define precise timing, referred to as Precision Time Protocol (PTP). For IEEE 802.11 links, 802.1AS uses timing facilities, developed initially for location determination (defined in IEEE 802.11v) [29].

An 802.1AS network timing domain is formed when all devices follow the requirements of the 802.1AS standard and communicate with each other using the IEEE 802.1AS protocol. Within this domain there is a single device, called the “Grand Master”, that provides a master timing signal as demonstrated in Figure 4.5. This device can be either auto-selected or can be specifically assigned. Typically, AVB devices exchange capability information on physical link establishment, so that network synchronization capable devices will start to exchange clock synchronization frames. If there are AVB devices with no such capability, an AVB timing domain boundary is determined (Figure 4.4).

The requirements of IEEE 802.1AS were chosen to provide for low-cost bridges, while still allowing application performance requirements to be met. IEEE 802.1AS has very few user-configurable options, consistent with the goal of AVB networks being plug-and-play [29].



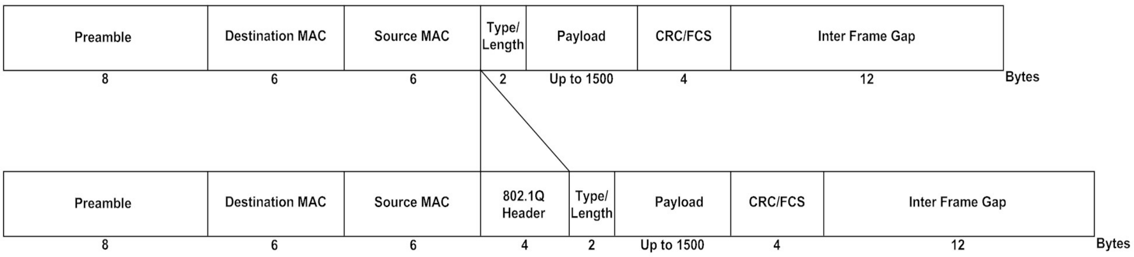
802.1AS devices send a *sync* message and a correcting *follow up* from the master port to the slave port(s) in other devices.

802.1AS bridges provide timing correction information based on the delay through a cable and the bridge itself

Figure 4.5 Clocking hierarchy

4.2.1.2 IEEE 802.1Q

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet work. A VLAN is the mechanism that allows the creation of groups of logically networked devices that act as if they are on their own independent network, even if they share a common infrastructure with other VLANs [30]. The IEEE 802.1Q standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames (Figure 4.6). The standard continues to be actively revised and, as mentioned earlier, two of its revisions (802.1Qat and 802.1Qav) are part of the AVB set of technical standards.



Preamble	Destination MAC	Source MAC	Type/ Length	Payload	CRC/FCS	Inter Frame Gap	
8	6	6	2	Up to 1500	4	12	Bytes

Preamble	Destination MAC	Source MAC	802.1Q Header	Type/ Length	Payload	CRC/FCS	Inter Frame Gap	
8	6	6	4	2	Up to 1500	4	12	Bytes

Figure 4.6 Insertion of 802.1Q Tag in an Ethernet frame

4.2.1.2.1 IEEE 802.1Qat

IEEE 802.1Qat, commonly known as Stream Reservation Protocol (SRP), deals with reservation and maintenance of QoS for a multimedia flow. It deals with up to seven hops between the source and the sink, with up to two of the hops being IEEE 802.11 [31]. IEEE 802.1Qat allows network resources to be reserved for specific traffic that is traversing a LAN. It also provides the necessary QoS by allocating and maintaining buffers within the switches and/or bridges [32]. Those network resources regard both the end nodes of the data stream and the transit nodes along the path. Once the reservation is set up, periodic QoS maintenance reports are monitored to ensure that the required QoS is maintained [31]. An end-to-end signaling mechanism to detect the success or failure of the effort is also provided.

Many vendors and users desire a single network infrastructure to carry various multimedia applications such as digital video, high-fidelity digital audio, and gaming traffic, as well as non-time-sensitive traffic (e.g., data traffic). The application of current IEEE 802 technologies for high quality time sensitive streaming allows users to load their networks unknowingly to the extent that the user experience is negatively impacted. To provide the robust guaranteed QoS capability for streaming applications, the availability of network resources along the entire data path must be assured before transmission takes place [28]. This requires a signaling mechanism, called Multiple Registration Protocol (MRP), to be used between the bridge nodes to complete the resources reservation process.

4.2.1.2.2 IEEE 802.1Qav

IEEE 802.1Qav utilizes methods described in IEEE 802.1Q to separate time-critical and non time-critical traffic into different traffic classes. It mainly focuses on three building blocks: traffic mapping or remapping into classes, shaping, and queue management according to class [33].

Egress port buffers are separated into different queues, each allocated to a specific class. This ensures a separation of low priority traffic from high priority traffic [34]. AV bridges reserve priorities 4 and 5 for video and audio traffic, respectively. To guarantee that the highest priorities are assigned only to the AV streams, it is required that the priority 4 and 5 legacy traffic that enters the AVB cloud have its priorities remapped. An alternative to this solution is to increase the number of queues by two, to provide distinct traffic classes for AV uses of priorities 4 and 5. This approach does not require any change to the number of priorities, as streams are recognizable by the existence of a reservation [33].

Moreover, all egress ports have a credit-based shaping mechanism to prevent bursty behavior [32]. At the extreme, the burst size can be reduced to the nominal frame size, and in this case the frame size becomes fixed and the interval between consecutive frames can be strictly enforced [33]. As for the queue management, IEEE 802.1Qav uses the timing derived from IEEE 802.1AS. Finally, dynamic release of reserved critical traffic class bandwidth is also supported, so lower priority traffic classes without maximum bandwidth allocation can fill those gaps [34].

4.2.1.3 IEEE 802.1BA

The purpose of this standard is to specify defaults and profiles that manufacturers of LAN equipment can use to develop AVB-compatible LAN components, and to enable a person not skilled in networking to build a network, using those components, that does not require configuration to provide transporting time-sensitive audio and/or video data streams. Specifically, this standard satisfies needs such as:

- The selection of default operating parameters, when the performance requirements of AVB over various media prevent the use of some portions of other standards. These parameters must be defined in order to meet the needs of the users of components built to those standards.
- The detection of non-AVB equipment, so that the performance of AVB equipment can be maintained.
- The definition of the configuration parameters of various 802.1 standards, in order to achieve automatic configuration of AVB networks.

4.2.2 IEEE 802.11aa: Interworking with 802.1AVB

The IEEE 802.11aa Task Group worked closely with the AVB Task Group in order to make IEEE 802.11 networks compatible with SRP. Changing the standard to provide for this, required only minor modifications to the MAC layer. The main one was to add a mechanism that allows for an AP to initiate the Transport Stream setup procedure, whereas it was only possible for a Transport Stream to be setup when a station requested it. This was necessary for an IEEE 802.11 network to be able to complete the process of setting up a path between a talker and a listener as described in the IEEE 802.1Qat standard. A Higher Layer Stream ID is included in all the messages exchanged when setting up a stream using the AP initiated setup, which is used to identify the SRP stream.

Also to facilitate the interworking of IEEE 802.11 with SRP networks, it was important to standardize the mapping between the User Priorities in 802.1D with the access categories and transmit queues used by the IEEE 802.11 QoS services, which was done together with the modifications for the SCS service, whether the new alternate queues are used or not.

Chapter 5

Multicast Issues and IEEE 802.11aa

In today's wireless networks most applications make use of unicast mechanisms to send data and voice traffic directly from one point to another. However, there are many instances where multicasting offers many advantages, such as in streaming a video to multiple users in a public hotspot. Multicast transmission allows for the conservation of the bandwidth by reducing unnecessary packet duplication as well as, making use of the inherently broadcast nature of the wireless medium.

However, there are many issues that must be addressed, regarding multicast communication in IEEE 802.11 wireless LANs. A basic one is that of guaranteeing reliability. Though the IEEE 802.11 standard does not include this, various efforts have been made to solve this issue. Some of those proposals are being presented here, classified according to the TCP/IP protocol suite. Although there are some proposals based on the PHY, such as dual tones based on additional RF channels, their implementation is very difficult and inefficient. Thus, in the following sub-chapters only solutions based on layers above the PHY will be presented.

5.1 MAC Layer Solutions

As the wireless medium is inherently unreliable, in the IEEE 802.11 MAC protocol the reliable transmission of data is guaranteed by the feedback mechanism where every transmitted frame is acknowledged by the receiver. This mechanism is not used in multicasting, because receiving acknowledgments from all the receivers would be inefficient, as it incurs a large overhead and raises issues with the scheduling and synchronization of receiving them. Additionally the MAC layer of IEEE 802.11 networks specifies that multicast frames can only be transmitted using the basic access procedure. Therefore, it cannot use the RTS/CTS mechanism to protect the broadcast of the frame, and this leads to more collisions. This means that multicast transmission is unreliable, as the source does not know if the data was not received because of a collision or because of other problems that are common in wireless communications. Also there is no provision in the MAC layer for retransmissions of the data to ensure the reliable receipt. It must be implemented by higher layers, which introduces a large overhead. It would be much more efficient to support reliable multicast transmission in the MAC layer.

Another problem is that the IEEE 802.11 MAC specifies that multicast frames must be transmitted using one of the bit-rates in the Basic Rate Set (BRS), which is a minimum set of bit-rates that must be supported by all stations in a IEEE 802.11 wireless LAN to ensure they can receive control frames. Although it is not necessary, most Access Points today use only the lowest bit-rate for transmitting multicast frames. This leads to lower throughput, which is also worsened by the performance anomaly problem of IEEE 802.11 wireless LANs. This is the phenomenon where one station transmitting in low bit-rate causes a large degradation to the throughput of the whole network, as the low bit-rate transmission occupies the medium for a significant amount of time. For all these reasons, transmitting multicast frames in legacy IEEE 802.11 cannot support a reliable, high rate multicast stream. The problems with multicast in IEEE 802.11 networks have been studied in many previous works. Most of the proposed solutions can be divided in two categories.

5.1.1 Negative Feedback-Based Solutions

The first category is based on negative feedback (NFB-based). Kuri and Kasera [35] presented the Leader-Based Protocol (LBP) for reliable multicast over wireless LANs. According to this protocol, one chosen leader is responsible for sending CTS and ACK frames responding to RTS and data packets, respectively. On erroneous reception of a packet, the leader does not send an ACK, prompting the sender to retransmit the packet. On erroneous reception of a packet at receivers other than the leader, the LBP allows negative acknowledgments (NACKs) from these receivers, which will collide with the leader's ACK and result in destroying the acknowledgment and prompt the retransmission of the packet from the sender.

However, leader-based protocols face several problems that exist in all NFB-based protocols, such as type-unknown for lost packet and frame aggregation support [36]. The first one could happen when collisions or link errors occur. At these situations the group member does not receive the frame correctly, thus cannot acquire information contained in the MAC header, regarding the source and destination address. As a result, it is difficult for the receiver to decide which node the feedback should be sent to. As mentioned, a collision between an ACK and a NACK will lead to a retransmission. However, when frame aggregation is considered, the sender will retransmit the whole aggregated unit even though not all frames in that unit were transmitted unsuccessfully. LBPs have to deal with other major problems as well, such as unnecessary retransmission that happens when some receivers send NACK for an erroneous retransmitted frame that they received, regardless of whether this frame has been received successfully before or not. This result in redundant retransmission. Generally, LBPs could not be considered perfectly reliable as the only leader cannot provide feedback about the rest of the receivers.

5.1.2 Positive Feedback-Based Solutions

The second category is based on positive feedback (PFB-based). Kuri and Kasera [35], also presented the Delayed Feedback-Based Protocol (DBP) which differentiates from LBP mainly in two ways. The first is that MCTS frames are sent by each receiver instead of only the leader. The second difference is that in order to avoid the collisions between NACKs and MCTSs, the receivers will have to wait for a random time before transmit a MCTS. Another issue of DBP is the choice of the right parameter for waiting times.

Tang and Gerla proposed the Broadcast Media Window (BMW) [37] protocol that supports reliable multicast in ad hoc networks. The basic idea in this scheme is to treat each multicast request as multiple unicast requests by transmitting a sequence of frames in each round of transmission to each receiver in turn. When channel contention is high, this protocol becomes inefficient and reverts back to the unreliable delivery of IEEE 802.11. The Batch Mode Multicast MAC (BMMM) proposed by M.T.Sun et al. [38] is based on the BMW protocol but reduces the number of contention phases when the acknowledgments are sent to make it more efficient. At this approach the sender sends RTS frames to each station of the multicast group and waits for CTS replies from each of them (Figure 5.1). Upon successful reception of the CTSs the sender transmits the data frame and then it sends a Request for ACK (RAK) frame to each station individually (Figure 5.2). All the receivers who successfully received the data, reply with an ACK. Upon receipt of ACKs from all the recipients, the transmission is completed. If there were stations that did not reply with ACK, the sender transmits the data frame again, except this time only to subset of stations whose ACKs where not received. Although BMMM is a rather efficient approach to achieve reliable multicast, it still has a very high control traffic overhead (Figure 5.3).

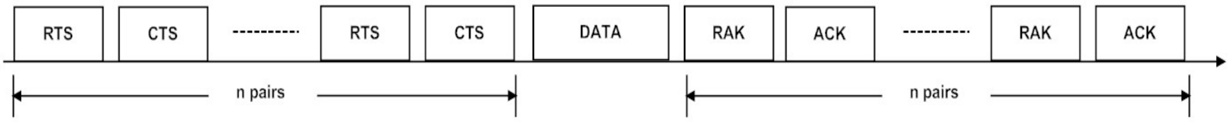


Figure 5.1 Primary idea of BMMM

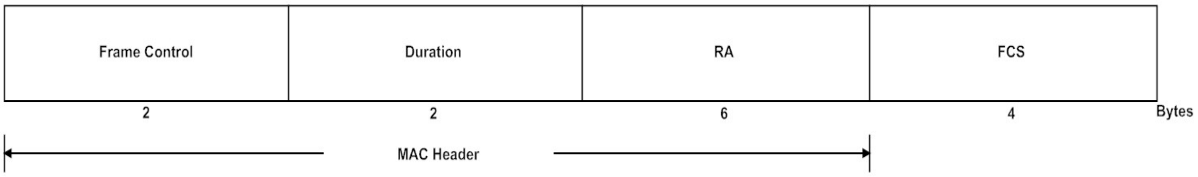


Figure 5.2 RAK frame format

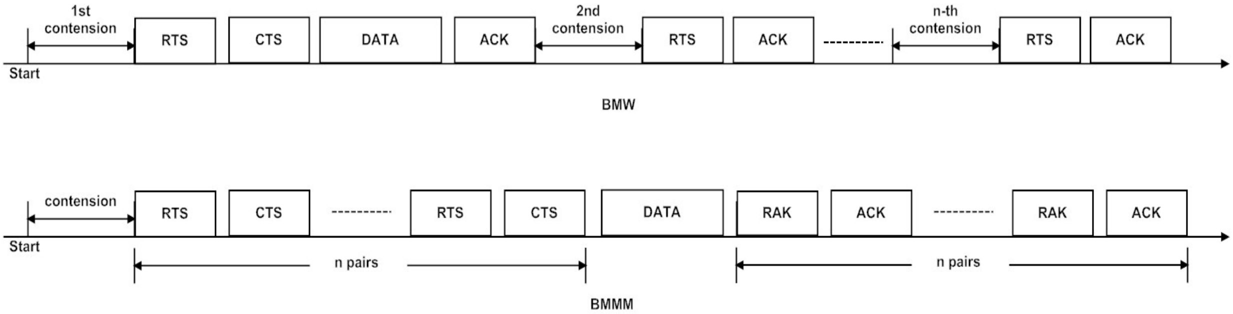


Figure 5.3 BMW vs BMMM

In [36], the Double Piggyback Mode Multicast (DPMM) protocol is presented trying to decrease the control packet overhead and improve the efficiency by embedding the acknowledgment information of a received data frame, in the next CTS frame. Lyakhov et al. [39] proposed the Enhanced Leader Based Protocol (ELBP) that further improves the BMMM protocol by using the BlockAck mechanism from IEEE 802.11e. Another improvement of the BMMM is proposed in [40]. V. Srinivas and L. Ruan presented the Slot Reservation Based (SRB) reliable multicast protocol. The SRB uses the RTS-CTS-DATA-ACK exchange mechanism to ensure reliability. Upon successful association with a station, the AP sends, among others, two parameters called Association ID (AID) and Multicast Association ID (MAID) (Figure 5.4). This helps to establish a schedule of transmissions of the multicast receivers and avoid the collisions that otherwise would be occurred by the simultaneous transmission of the stations' ACKs and CTSs. To ensure efficiency in retransmissions, the SRB uses a modification of the RTS multicast frame that is sent out at the beginning of each retransmission. The RTS frame is appended with bitmap with n bits, where n is the number of the stations in multicast group and each bit corresponds to a station, resulting that way in a one-to-one mapping. In any retransmission phase only the bits that correspond to the participant stations are set to 1. With this mechanism the data are being retransmitted only to those stations from whom the AP did not receive ACK, improving significantly the efficiency and throughput (Figure 5.5) .

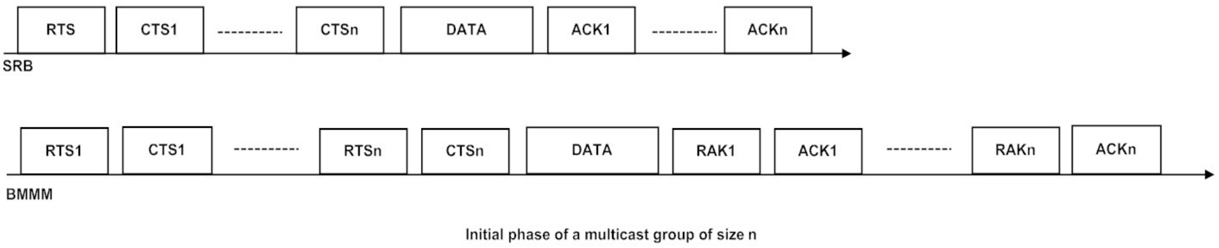


Figure 5.4 Comparison of the initial transmission phase

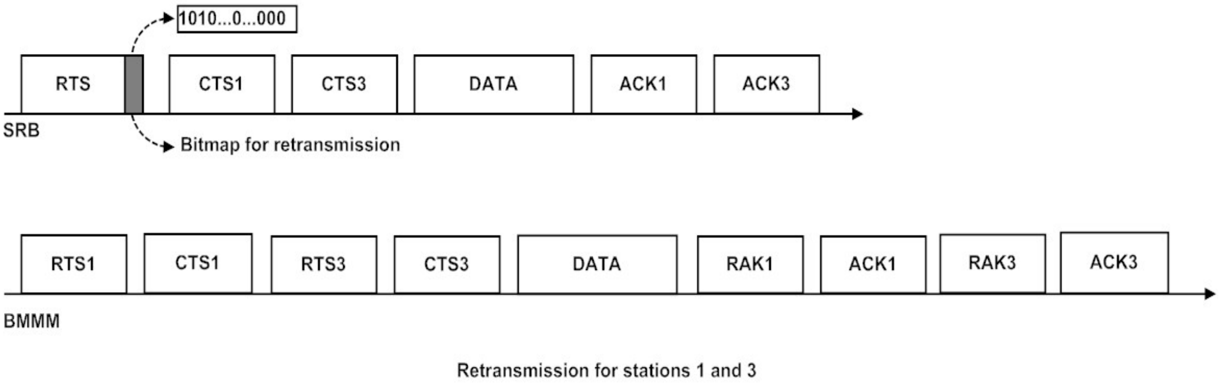


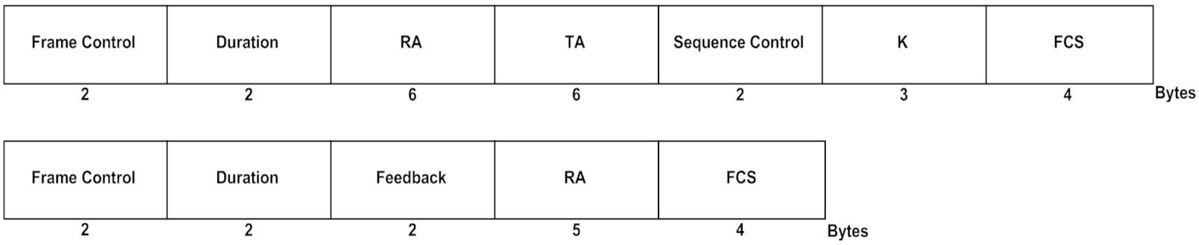
Figure 5.5 Comparison of the retransmission phase

5.2 Network Layer Solutions

Though, most of the proposals for reliable multicast transmission are based on the MAC layer, there are a few others that are applied on the upper layers. For multicast on the network layer, two interesting approaches have been made, the first of which gives a solution for P2P live streaming multicast transmission and the second for video multicast transmission.

In P2P live streaming systems the data are being exchanged between peers by application layer multicast protocols, which in turn usually use unicast transmission in the network layer. This results in a lot of bandwidth waste. To overcome this problem, Wenbin Jiang et al. [42] proposed a wireless multicast agent mechanism (WiMA) that uses IP multicast, reducing that way the network overhead and, thus, being able to support more users. The main idea behind this is to select a multicast agent that acts as a proxy to the other wireless peers. It is also necessary to set one multicast IP address for each channel. The selection of the agent is a process that takes in consideration parameters such as radio signal, network traffic and power of the CPU of the candidate agent. Though this solution does reduce the bandwidth consumption, it does not include an efficient QoS mechanism.

Another attempt for reliable video multicast transmission on IEEE 802.11 WLAN has been done in [43]. There, Maria Samokhina et al. proposed a scheme based on raptor code that is applied right above the MAC layer. According to their proposal, the AP before the transmission of data first determines the expected symbol loss rate by taking in account the channel status, and then using the raptor encoder, encodes the data and generates as many encoded parity symbols, as need to prevent the losses. The IEEE 802.11n Power Save Multi-Poll (PSMP) burst of two rounds is used, for the transmission. During the first round, the AP collects information based on the Singal-to-Noise Ratio (SNR) feedback from the multicast receivers to calculate the raptor symbol loss rate. In case that the SNR is different between the receivers, the AP takes in account the worst SNR value. The receivers send their feedback to the AP by sending Reliable Multicast (RM) and Feedback (FB) frames. These frames are shown in Figure 5.6. Even if one FB frame is not received by the AP, the process starts again. This does not increases significantly the network overhead because the probability that an RM or FB frame fails is much smaller than that of a data frame failure due to their small size. The multicast data transmission takes place during the second round of PSMP burst, where each raptor symbol forms an MSDU (Figure 5.7). The main disadvantage if this proposal is that it only supports video multicast transmission.



Frame Control	Duration	RA	TA	Sequence Control	K	FCS	
2	2	6	6	2	3	4	Bytes

Frame Control	Duration	Feedback	RA	FCS	
2	2	2	5	4	Bytes

Figure 5.6 RM and FB frame formats

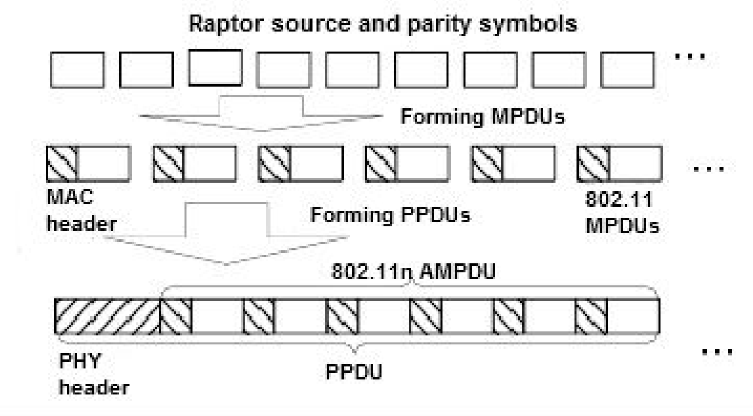


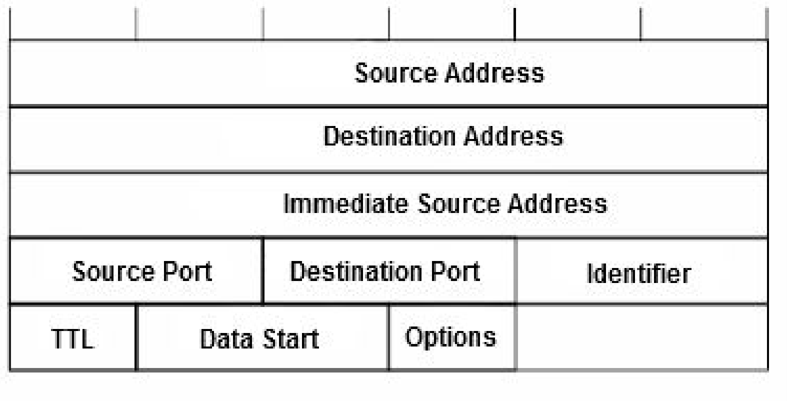
Figure 5.7 An 802.11n A-MPDU based scheme

5.3 Transport Layer Solutions

In [44], H. Fujisawa et al. examined the multicast packet loss due to collisions with TCP packets on IEEE 802.11 WLANs and presented two significant results. First, they proved after simulation that the packet loss rate does not increase as the number of TCP station increases. Actually, they stated that the ratio remains constant if the number of the stations is more than 3. That happens because TCP's flow control, which uses ACKs, prevents the stations from contending. Moreover, they stated that as the multicast transmission rate increases, the packet loss rate decreases. The second result is that the multicast packet losses can be recovered by a FEC technique, the Reed-Solomon (RS) code which shortens the code length to improve error correcting capability.

5.4 Application Layer Solutions

In [45], M. Kappes et al. presented the Application Layer Communicator (ALC), an application-layer approach for ad-hoc networks. The ALC uses MAC/IP multicast without the need to apply an changes to the MAC or IP layer. It also uses UDP as its transport protocol, at which some further headers need to be added as illustrated in Figure 5.8. Where the immediate source address is the MAC address of the last device that forwarded the frame. Each ALC node periodically sends out a list of its neighbors just like in a distance vector routing protocol. By keeping a list of all stations, each node can determine the next hop in an efficient route. This approach does not declare a mechanism that calculates the retransmission timers.



Source Address			
Destination Address			
Immediate Source Address			
Source Port	Destination Port	Identifier	
TTL	Data Start	Options	

Figure 5.8 ALC frame format

R. Chandra et al. proposed in [46] proposed an application layer multicast technique that takes advantage of the multi-access nature of the wireless medium. This mechanism requires a DirCast server, as shown in the figure Figure 5.9. Also, each multicast receiver must have installed a DirCast client software. The idea behind this is that the server sends multicast packets as unicast to a selected station at each AP. The main goal now is to select the appropriate target client. As the AP adjusts the transmission rate based on the client's channel conditions, it is logical that the worst client has to be selected so that all the receivers can decode successfully the received packets. The DirCast re-calculates the data rate that the AP uses every 30 seconds. Moreover, this value is re-evaluated every time a new client joints and whenever the loss rate at any client exceeds the 10%.

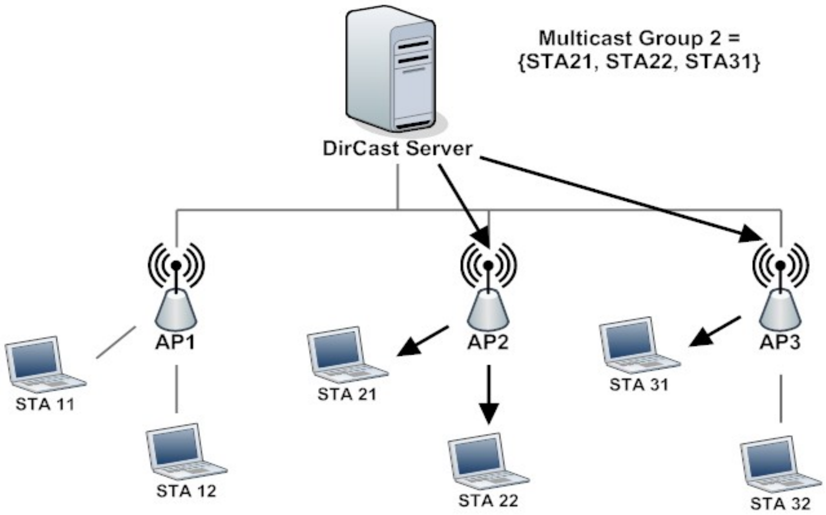


Figure 5.9 DirCast operational overview

C. Bravo and A. Gonzalez [47], proposed a polling-based service to improve the reliability of IEEE 802.11 wireless LANs for multicast data. Here, a Smart Server is required for each AP in a network. A Smart Client mechanism, placed right below the client application, is also required (Figure 5.10). The process starts with the server transmitting the first 8 frames. If one of those is lost, all the others with sequence number greater than this of the lost one, are stored in a buffer until the frame is retransmitted and received successfully or until the buffer is filled up at a certain point where the lost frame is ignored and the all of the waiting frames are sent up to the client application. Once the server has completed the transmission of the frame group, it sends out a poll message asking for the reception status of the frames of that group. The Smart Client, then, set the Bit Array of the poll message depending if it successfully received or not the frames of the group. At the next round the Smart Server after having received the Bit Array, transmits the next group of frames, including those that were not received by the stations, previously.

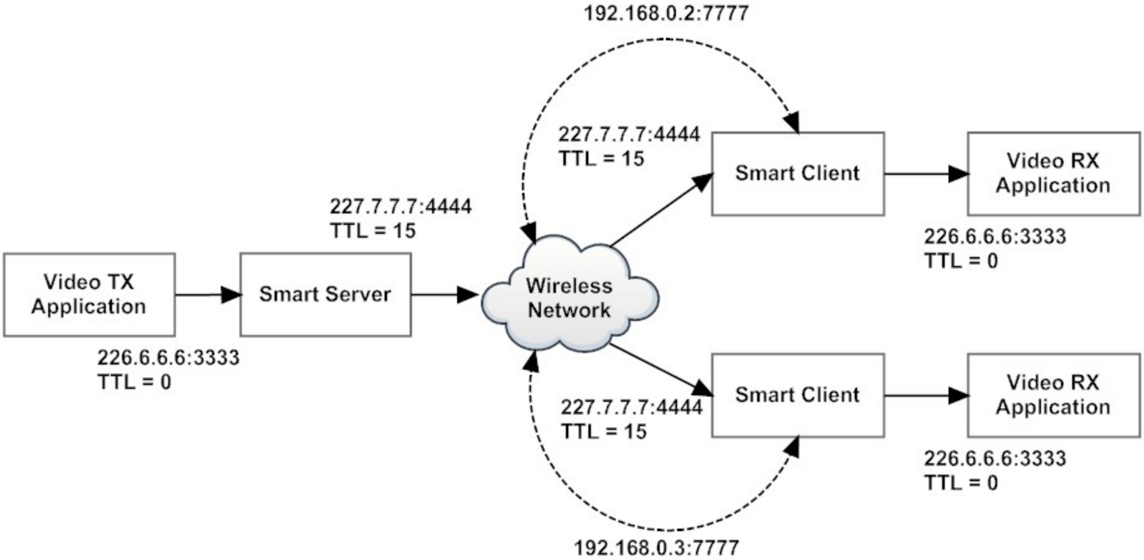


Figure 5.10 GP protocol network diagram

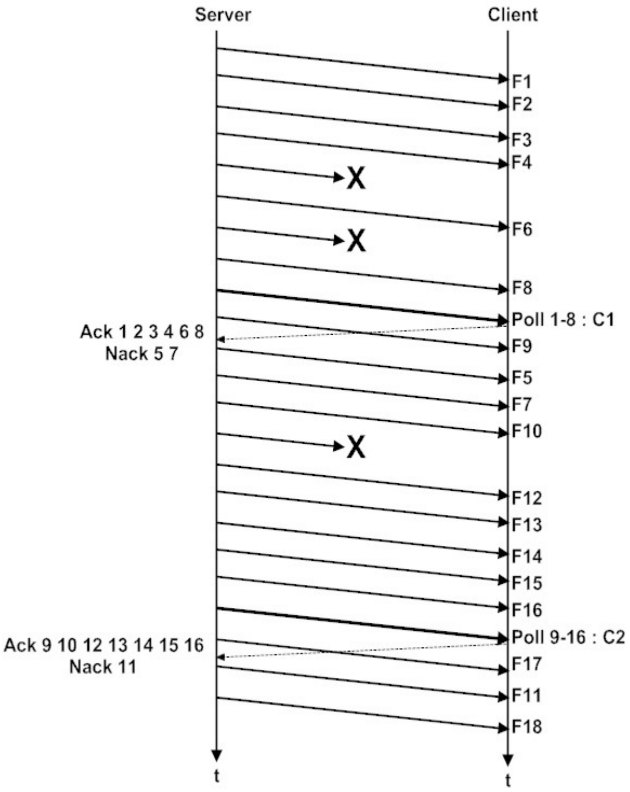


Figure 5.11 GP protocol over time diagram

In [48], a Cooperative Peer-to-peer Repair (CPR) strategy that allows peers in Wireless Wide Area Networks (WWANs) to cooperatively repair lost packets from neighbors watching different views, is presented. To succeed this, the server should transmit dept maps in addition to texture maps, so that a viewer A watching a video can repair a lost frame of viewer B, by synthesizing in B's viewpoint its frames via depth-image based rendering (DIBR). To do so, the two viewers need to be watching the video in different views.

5.5 Cross-Layer Solutions

There have, also, been proposed other solutions that are not based on a single layer, but instead they need cross-layer information to be exchanged. Those solutions can be categorized based on the network topology as centralized, where an AP manages the network traffic, and decentralized, where the network nodes do not rely on any preexisting infrastructure.

5.5.1 Decentralized Networks (Ad-Hoc Networks)

In [49], there has been implemented a scheme that relies on the cooperation of both the MAC and application layer and aims to improve the video quality, thus to minimize the distortion, at all network nodes. To do so, each node consists of a link state monitor at the MAC layer and a video rate controller at the application layer (Figure 5.12). By sending periodic broadcasts, all the nodes are able to collect information regarding their neighbors' link utilization and congestion values. Based on that, an accumulated price is calculated that is being forwarded up to the application layer, where, in turn, the controller uses it to calculate the appropriate video rate. Moreover, the receiving rates may vary between nodes that are accepting the same video, because of the heterogeneity that might be in their link speeds. Thus, rate adaptation needs to be implemented, and this is being accomplished by adopting the Scalable Video Coding (SVC) extensions of the H.264/AVC standard. Although, the experimental results have shown that it is pretty effective, this solution has the strong limitation that it is not applicable on transmissions that carry various data types.

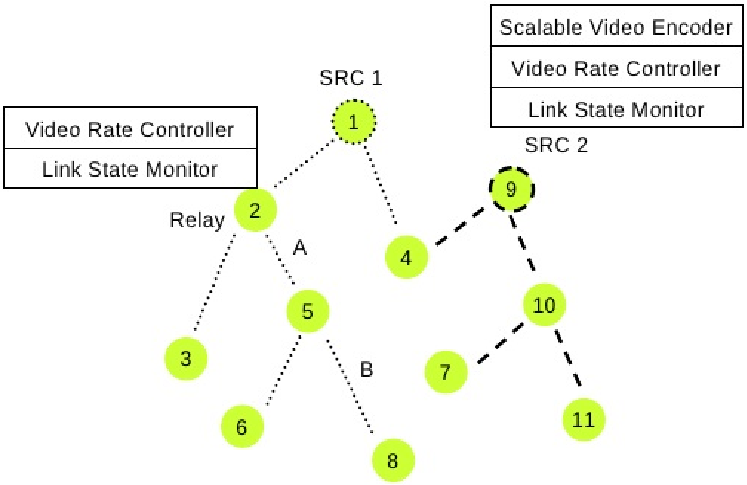


Figure 5.12 Each node consists of two layers

Another interesting attempt to improve multicast transmissions in ad hoc networks has been presented in [50]. Soon Y. Oh et al. proposed the MIMO-Cast protocol, that works in conjunction with Multi Point Relay (MPR) and, basically, consists of two mechanisms. The first is that it builds a multicast tree of all nodes, similarly to the ODMRP protocol, with the difference that only the selected MPR nodes can forward the message. That way, the network overhead is reduced significantly (Figure 5.13). The second mechanism takes care of eliminating completely the problem of the hidden node; as each terminal transmits at different radio weight, selective reception is applied and thus, interference signals are being blocked. Simulation results have shown that MIMO-Cast performs far better than conventional multicast protocols with IEEE 802.11.

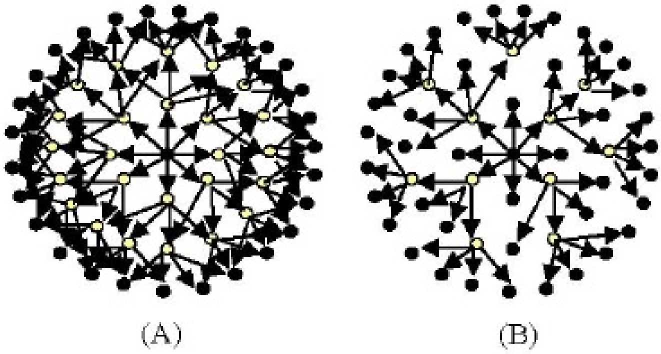
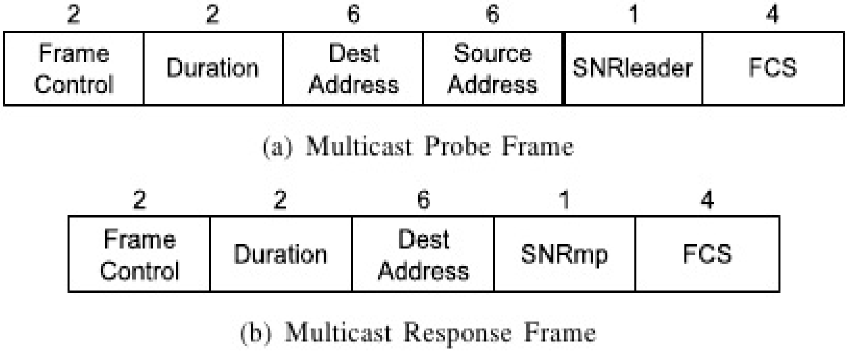


Figure 5.13. Normal flooding (A) vs proposed scheme's flooding (B)

C.C. Hu [51] presented another cross-layer scheme that works with the cooperation of the physical, the MAC and the network layer, as well and aims at bandwidth consumption improvement and data rate selection for multicast transmissions in multi-rate Mobile Ad-Hoc NETworks (MANETs). In the proposed protocol, the hosts monitor the channel's status, that can be either idle or busy. Also, when a node is forwarding data frames, its neighbors are blocked and cannot transmit anything within this period. The goal here, is to calculate the appropriate data rates, based on the number of each forwarder's neighbors, to improve the network performance. That means that there must be selected a tree that consists of forwarders with as fewer neighbors as possible. The tree determination starts from the server by broadcasting a network layer control packet. When a node receives that packet, it responds with another control packet that carries information about the link time with its neighbors, the rest of its bandwidth and the relations with the neighbors that is kept in its MAC layer. The server, then, can determine the best tree and data rates, using this information. If a client detects a change that renders the tree to be considered outdated, then it broadcasts another control packet, so that, the server can update the tree.

5.5.2 Centralized Networks (Access Point-Based Networks)

Jose Villalon et al. [52] introduced the Auto Rate Selection mechanism for Multicast (ARSM), that dynamically adapts to the channel conditions changes and selects the appropriate data rate. This process is done with the collaboration of the PHY and MAC layer. The main idea is that for each multicast group is being selected a leader. First, the AP sends out to the group a Multicast Probe (MP) frame. When the members receive that frame, they calculate the Signal-to-Noise Ratio (SNR) value of the channel. Based on this value, each station estimates the point in time that it will respond to the AP. The station with the lowest SNR value, that is the worst channel, responds first by sending a Multicast Response (MR) frame to the AP. MP and MR frames are represented in Figure 5.14. This node will then be selected as the group leader and will be responsible for acknowledging the received multicast data on behalf all the other members, which, however, may issue NACK frames in case they detect errors in the received frames. The AP in this case retransmits the data.



2	2	6	6	1	4
Frame Control	Duration	Dest Address	Source Address	SNRleader	FCS

(a) Multicast Probe Frame

2	2	6	1	4
Frame Control	Duration	Dest Address	SNRmp	FCS

(b) Multicast Response Frame

Figure 5.14. Control frames formats

Although, this mechanism guarantees reliability, it has the disadvantage that the data rate adaptation is made based on the station with the worst channel conditions, penalizing that way, the rest of the stations that are able to communicate at higher rates. The need of a mechanism that also adapts to this heterogeneity, led the same team to a cross-layer architecture that extends their first approach of ARSM to the application layer, as well [53]. This enhanced version of ARSM, called Hierarchical ARSM (H-ARSM), provides further services that allows the nodes with better channel conditions to take advantage of that, at least at a certain point. The H-ARSM is only implemented for video communications. With this mechanism implemented, the video is decoded into two layers; the base layer, which is supposed to provide the minimum acceptable video quality, and the enhancement layer. The frames that contain the data for the base layer are transmitted to all the members of the multicast group, according to the rules defined by the ARSM. The frames that contain the data for the enhancement layer follow an operation similar to that of the ARSM with a main difference, though. Instead of the leader being the station with the worst channel, now this selection is being made based on the best SNR. So, in this case the station with the best channel conditions has the responsibility of acknowledging the frames with the enhancement layer data, on behalf all the members of the group. Again, the other stations may reply with a NACK upon erroneous reception of the data. The formats of the MP and MR frames are the same as those used by ARSM. The simulation results have shown that in real-time video streaming the quality of the video can be improved significantly. However, in a scenario where exists only one station in the multicast group that can receive data at the high ratio of the enhancement layer, only this station would be able to receive the video in a high quality and the rest of them would have to compromise with the minimum acceptable video quality.

A very similar mechanism to the above, is presented by W.S. Lim, D.W. Kim and Y.J. Suh in [54]. They first presented a MAC-layer protocol for multicast transmissions in IEEE 802.11n WLANs, called Reliable and Efficient Multicast Protocol (REMP) and then they extended it via cross-layer optimization, to support scalable video streaming. This enhanced version of REMP is called Scalable REMP (S-REMP). S-REMP is basically a leader-based protocol, where the leader is the node with the worst channel conditions. Under S-REMP, when the channel condition is stable the AP exchanges control frames only with the leader, whereas when it is dynamic, it exchanges control frames with all the network nodes and based on their feedback, -that is, each node's channel condition- the AP adjusts accordingly the modulation and coding scheme (MCS). S-REMP's goal is to provide high-quality video to the users with high SNR value when the available bandwidth is not enough for the AP to transmit the entire video to all the multicast members. To do so, each A-MPDU is separated into two sub A-MPDUs, when the network overhead becomes heavy. The first sub A-MPDU contains the base layer of the video and is transmitted to every network station with a low MCS, to guarantee the minimum video quality to all, while the second sub A-MPDU that contains the enhanced video layer is transmitted with a higher MCS to avoid packet drops.

To better manage the multicast group, the AP maintains a GroupTable of eleven fields. Group address field and leader address field indicate the multicast group address and leader address, respectively. The address list field contains the addresses of all the receivers, while SNR list field contains their SNR values. The timestamp field keeps the time of the last transmission for the group. Tdelay field stores the last waiting time for channel access. Drop field represents whether one or more data frames where dropped since the last data transmission. This field is set to 1 every time a frame destined for the multicast group is dropped due to overload at the AP's data queue and is reset to 0 for each data transmission. LoadUp and LoadDown fields indicate the network load status and are updated before each data transmission, according to the drop field. K field represents the number of the enhancement layers that are included in the second sub A-MPDU and mAlg2 field is a MCS value for the second sub A-MPDU.

S-REMP has the advantage over H-ARSM [53] that the enhancement layers are not transmitted at a ratio that is based only on the SNR value of the station with the best channel condition. Instead, under S-REMP the MCS selection for such layers, takes in account other parameters such as the K field and the MCS value of the first sub A-MPDU.

O. Alay et al. [55] proposed an alternative solution that is implemented both in the MAC and application layer. The main idea here, is to dynamically adapt the data transmission rate and the Forward Error Correction (FEC), as well, in order to succeed the maximum video quality for all the multicast members. In multicast transmissions, expecting the AP to retransmit the lost frames to all the multicast members, obviously is not a good idea as it may lead to extremely high network overhead. FEC implemented in the application layer, on the other hand, is a good alternative solution for handling erroneously received packets. For this solution to be more effective, CRC-based error detection needs to be implemented at the link layer, so that any corrupted packets would first be removed and then recovered by the application layer's FEC. This solution however adds some overhead at the network since more parity packets are now needed. Moreover, the count of those packets increases as the Packet Error Rate (PER) increases, too. Therefore, it is important to always know the PER of the multicast group, in order not to apply more FEC parity packets than needed. The answer to this issue, is that all the multicast receivers should periodically send PER information to the AP. Using this feedback, the AP adapts the transmission rate and the FEC based on the worst station's PER. From experiments they ran, the authors concluded that using higher transmission rate, thus more FEC information, is more efficient than using lower transmission rate along with weaker FEC. Based on this, they focused on using the higher transmission rate possible together with the appropriate FEC. The rate adaptation method that is adopted in the current thesis, is that the optimal transmission rate is chosen by searching through different rates. The resulting algorithm has two major features.

The first is to switch the transmission rate. When the PER is 0% - 15%, they switch to a higher transmission rate. This means that if, for example, for a rate of 1 Mbit/s the PER was less than 15%, then the next transmission will be at 5.5 Mbit/s. This also means, that the next PER will be less than 40%, which is the worst case scenario. If at any time the PER is more than 40%, then it is considered that the current transmission rate cannot be sustained. In this case, the mechanism switches at the base rate, which is 1 Mbit/s. PER higher than 50% was not studied, since in such a case there was observed frequent network connection lost. The second component of the proposed scheme is to keep the transmission rate stable. This happens in case the PER is more than 15% while transmitting at the base rate. Jumping to the next rate, in this case is not worth as the PER may become higher than the 40%.

While the transmission rate and FEC switch, the video rate switches, as well. It also switches even if the transmission rate remains stable because the FEC is always being adjusted based on the received PER. Basically, the video rate is adapted in the following way; regarding the transmission and FEC rate, the video is pre-encoded in different bit rates, resulting in various versions of the same video. To simplify the system, the authors suggested to create only two different video streams for each transmission rate.

Transmission rate	PER range (%)	Video rate (Mbit/s)
1 Mbit/s	0-25	0.13
	25-40	0.10
5.5 Mbit/s	0-25	0.70
	25-40	0.52
11 Mbit/s	0-20	1.44
	20-40	0.98

Table 5.1 Video rate adaptation based on PER for different transmission rates

The simulation results confirmed that this mechanism improves the network performance when it is about multicast transmission. However, it lacks of an efficient-enough video rate adaptation mechanism and a more accurate FEC prediction method, as currently only the PER of the last transmission is used, instead of a history of the reported PERs. Finally, the proposed solution has not yet been adapted in other environments than the IEEE 802.11b.

5.6 The IEEE 802.11aa Task Group Approach

5.6.1 Group Addressed Transmission Service (GATS)

In order to provide reliable multicast, the IEEE 802.11aa amendment specifies the Group Addressed Transmission Service (GATS) that allows a station to request greater reliability for a group addressed stream. The service, in addition to the legacy No-Ack/No-Retry multicast, comprises the Directed Multicast Service (DMS) and the Groupcast with Retries (GCR). When setting up a stream to a multicast group with the AP, a station can request to use any of these policies. The policy that is used for a particular stream can be changed dynamically later [56].

5.6.1.1 DMS Procedures

This method was first introduced in the IEEE 802.11v amendment for Wireless Network Management. In IEEE 802.11aa, however this method can be used dynamically and switched to the GCR policy. The implementation of DMS is optional for a WiFi Multimedia (WMM) station and mandatory for a robust Audio/Video (AV) streaming station. The DMS converts multicast traffic to unicast frames directed to each of the group recipients in a series. The transmission uses the normal acknowledgment policy and will be retransmitted until it is received correctly. This is obviously the most reliable scheme but it also has the greatest overhead and does not scale well to multicast groups with a large number of members.

5.6.1.2 GCR Procedures

GCR is a flexible service that aims at increasing the reliability of group addressed frames, while providing a better scalability of the DMS. GCR may be provided either by an AP to the associated stations of a BSS, or by a mesh station to the rest of the peer stations in a mesh BSS. The TGaa group specifies that the GCR service uses the same setup, modification and termination procedures as the DMS. GCR is an extension of DMS. In particular:

- A GCR agreement applies to a single group address, whereas a DMS flow is not restricted to a single group address.
- DMS offers multicast-to-unicast conversion only, whereas GCR includes several retransmission policies and delivery methods.

GCR extends the DMS Request and DMS Response elements with the addition of the GCR Request and GCR Response sub-elements respectively, for managing the set up, the modification and the tear down of GCR services between the GCR service provider, that is an AP or a mesh station, and the associated group addressed stations. The GCR service has two delivery methods, regarding group addressed frames:

- Non-GCR Service Period (non-GCR-SP)
- GCR Service Period (GCR-SP)

GCR-SP transmits GCR group addressed frames at intervals that might be smaller than the beacon interval. Compared to non-GCR-SP, GCR-SP might provide lower delay and jitter. Further analysis regarding the functionality of those two delivery methods, is beyond the scope of this thesis.

Moreover, GCR defines two additional retransmission policies for group addressed frames, in addition to the "No-Ack/No-Retry" and DMS mechanisms:

- GCR Unsolicited Retry
- GCR Block Ack

The TGaa also specifies the GCR transmission concealment; a mechanism that prevents group addressed traffic transmitted via either of the above two retransmission policies, from being passed up through the MAC layer of GCR-incapable stations.

5.6.1.2.1 GCR Unsolicited Retry

This mechanism allows the transmission of the multicast frames to be repeated a number of times to increase the probability of correct reception at the stations that are listening to the particular group address. No acknowledgment mechanism is used. The number of retransmissions is not specified in the standard; it depends on the implementation and is subject to applicable frame lifetime and retry limits. Note that the AP or a mesh station may vary the lifetime limit for a group address at any time and may use different lifetime limits for different GCR group addresses. The standard also suggests a protection mechanism to be used to prevent other stations from transmitting at the same time. However, the GCR unsolicited retry uses a backoff algorithm to avoid collisions, regardless of whether or not a protection mechanism is in use. To detect and prevent frame duplications, the receiving stations keep a cache of recently received frames. In general, this method may provide moderate delay, efficiency and reliability but has high scalability, thus it is better suited for groups with large number of members.

5.6.1.2.2 GCR Block Ack

This method extends the Block Ack mechanism specified in IEEE 802.11e for use in multicast transmissions to a group. The AP transmits a number of multicast frames and then requests from one or more of the recipients to acknowledge the receipt of the transmitted frames, by sending a modified Block ACK Request (BAR) control frame. Frames that have not been received correctly by one or more of the receivers can then be scheduled for retransmission. For this mechanism to function, every recipient of a GCR Block Ack agreement shall maintain a block acknowledgment record that includes:

- a bitmap, indexed by sequence number
- a 12-bit unsigned integer starting sequence number

- WinStartR, representing the lowest sequence number position in the bitmap
- a variable WinEndR
- the maximum transmission window size, WinSizeR.

Upon a BAR reception, a station responds with a BlockAck frame containing the above information that the originator will use to determine which frames to retransmit. Although each station shall transmit a BlockAck frame at a delay of SIFS after the BAR reception, the standard suggests a protection mechanism to be implemented in order to avoid collisions.

The choice of the stations from which an acknowledgment will be requested is left to be decided by the implementation, and therefore this method can be used with many leader-based multicast methods and algorithms for selecting a leader. This method can offer a high degree of reliability, scalability and performance, with the trade-off depending on the implementation. However, the current hardware on the market does not allow to ACK multicast or broadcast frames, thus it is not possible to arrange such a mechanism over existing MAC, where packets not requiring acknowledgment are immediately discarded after transmission.

In the beginning stages of the Task Group discussions it was suggested that a scheduled BlockAck mechanism would be used, where the AP would send one modified BlockAck Request with a bitmap specifying the order in which the receivers would answer, and the receivers would send their acknowledgments in the specified order, separated by SIFS time. However this was canceled due to several worries such as the effect of air propagation time, the effect of hidden stations or of a station missing the BlockAck Request. Now only the Polled BlockAck mechanism [57] is specified, where the AP requests an acknowledgment from each receiver separately. This does not require any changes to the BlockAckRequest frame, is easier to handle within hardware and does not cause legacy client compatibility issues.

Table 5.2 summarizes the characteristics of the different policies specified by the Group Addressed Transmission Service. The legacy No-Ack/No-Retry multicast and the three alternative policies are illustrated in Figure 5.15.

Multicast Policy	Overhead	Scalability	Complexity	Reliability
Legacy multicast	None	High	Low	Low
DMS	Large	Low	Medium	High
GCR Unsolicited Retry	Small	High	Low	Implementation depended
GCR Block Ack	Implementation depended	Implementation depended	High	Implementation depended

Table 5.2 Characteristics Of Group Addressed Transmission Service Policies

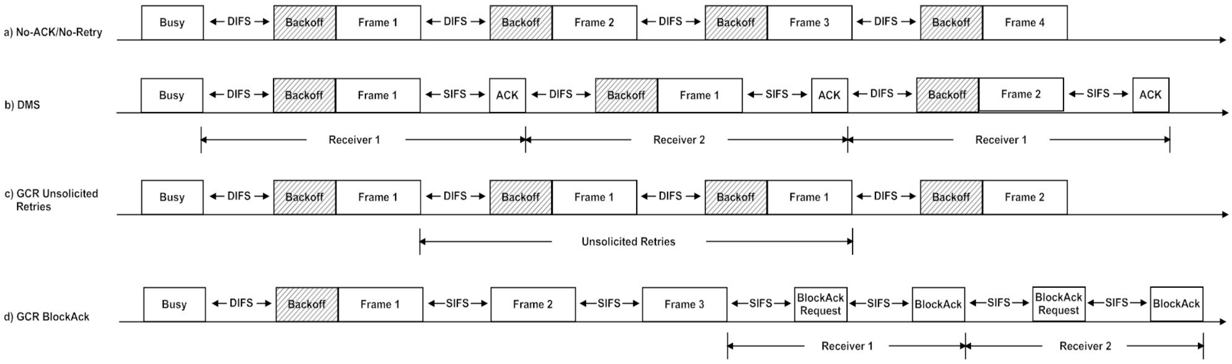


Figure 5.15 Group Address Transmission Service with different policies

5.6.2 Other Solutions

Another proposal that was made to the IEEE 802.11aa Task Group is by Miroll and Li [58], who suggested a leader-based protocol that introduces the idea of feedback cancellation where a Negative ACK (NACK) frame transmitted simultaneously with the leader's ACK frame cancels the acknowledgment at the receiving AP and forces a retransmission (Figure 5.16). This proposal also includes a FEC coding scheme where additional multicast frames are transmitted, to allow the receiver to decode the multicast stream even if some of the frames are corrupted. After discussion, the proposal was not included in the amendment as it required many modifications to the IEEE 802.11 standard.

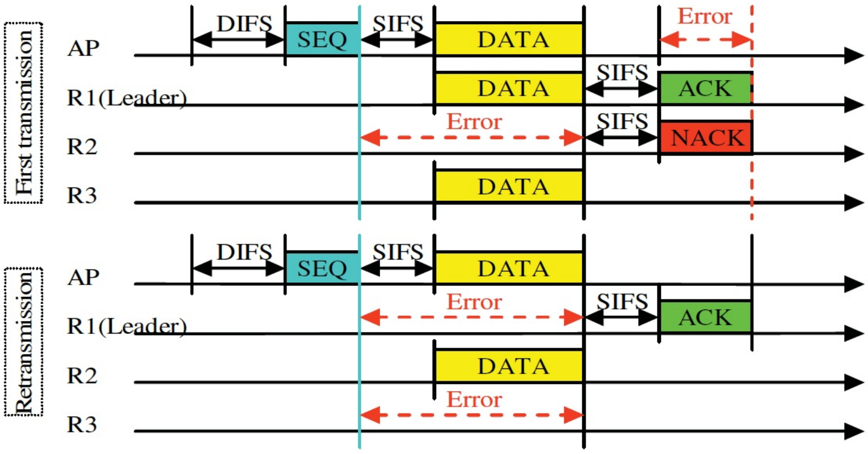


Figure 5.16 The proposed NACK based LBP

In [59], the Multicast Collision Free (MCF) scheme is proposed. This mechanism is based on two steps. First the transmitter sets a multicast flag active to avoid collisions that may arise if other stations attempt to transmit at the same time. Note that this mechanism does not use ACK, so frames will not be retransmitted. In the second step, the transmitter has the multicast flag active and begins the multicast transmission after waiting PIFS making, this way, sure that the medium is idle. Figure 5.17 demonstrates a flow chart of the MCF mechanism, while in Figure 5.18 a comparison between the MCF and the standard channel access, is presented.

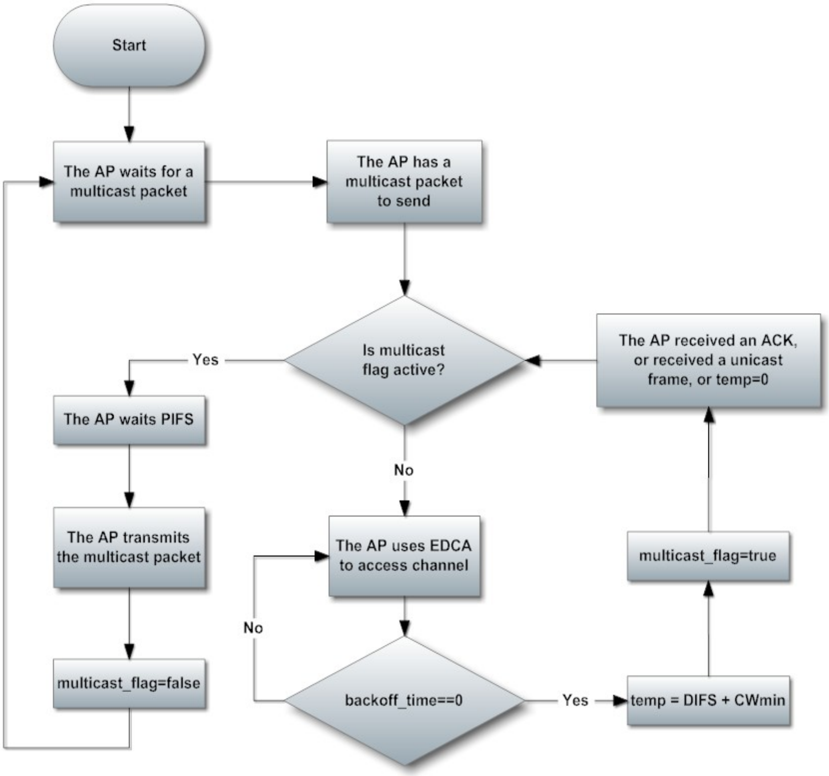
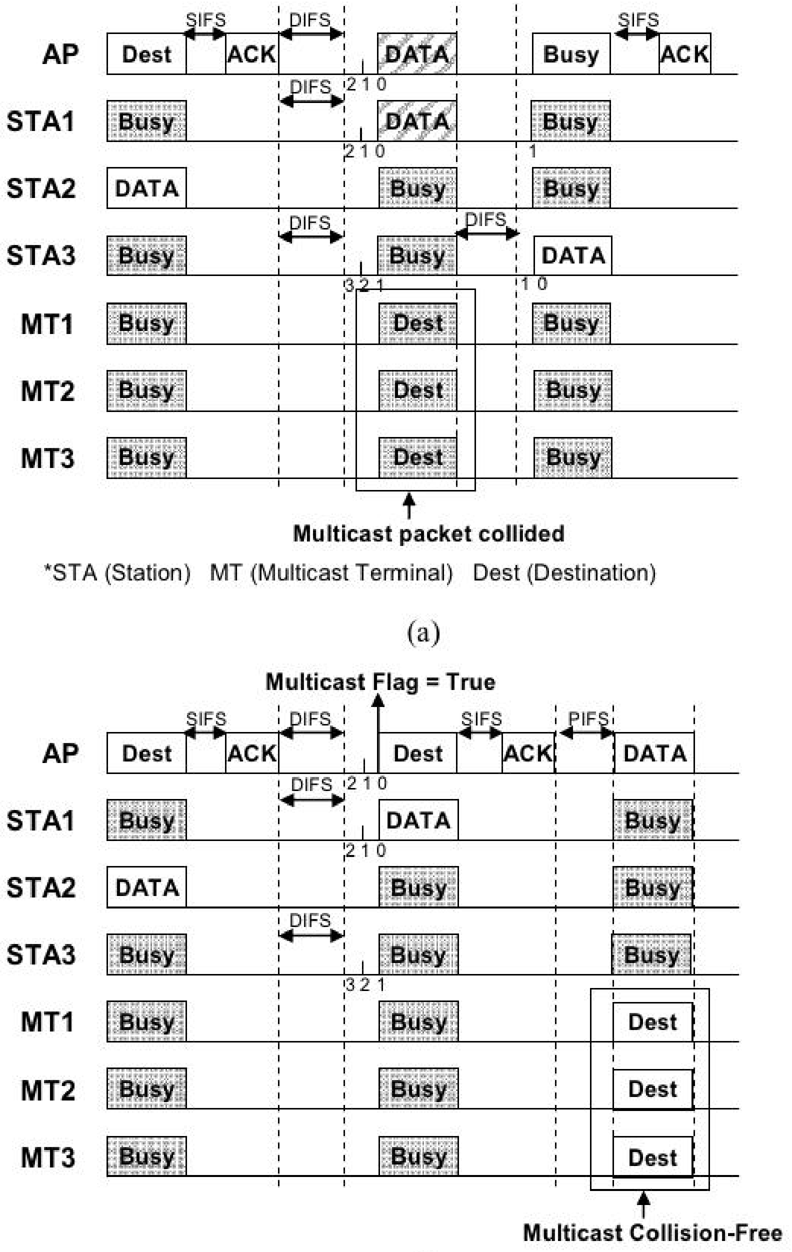

Start
The AP waits for a multicast packet
The AP has a multicast packet to send
Is multicast flag active?
Yes
No
The AP received an ACK, or received a unicast frame, or temp=0
The AP waits PIFS
The AP transmits the multicast packet
multicast_flag=false
The AP uses EDCA to access channel
No
backoff_time==0
Yes
temp = DIFS + CWmin
multicast_flag=true

Figure 5.17 Multicast Collision-Free Mechanism



*STA (Station) MT (Multicast Terminal) Dest (Destination)

(a)

(b)

Figure 5.18 Multicast channel access: (a) Standard, (b) MCF

Chapter 6

Overlapping Basic Service Set (OBSS) Issues and IEEE 802.11aa

6.1 Industrial, Scientific and Medical (ISM) Radio Bands

Industrial, Scientific and Medical (ISM) band is a part of the radio spectrum that can be used by anybody without a license in most countries. In the United States, the 902-928 MHz, 2.4 GHz and 5.7-5.8 GHz bands were initially used for machines that emitted radio frequencies, such as RF welders, industrial heaters and microwave ovens, but not for radio communications [60].

In 1985, the Federal Communications Commission (FCC), a U.S. government agency that regulates interstate and international communications, opened up the ISM bands for wireless LANs and mobile communications. In 1997, FCC added additional bands in the 5 GHz range, known as the Unlicensed National Information Infrastructure (U-NII). Europe's HIPERLAN wireless LANs use the same 5 GHz bands, which are entitled the "Broadband Radio Access Network" [60].

6.1.1 2.4 GHz Wireless Band

The 2.4 GHz band is utilized by the IEEE 802.11 b/g/n standards and is divided into 14 channels, with the last one being used only in Japan and allowed only for IEEE 802.11b. The first 13 channels are spaced 5 GHz apart, with channel 1 being centered on 2.412 GHz and channel 13 on 2.472 GHz (Figure 6.1). The 14th channel, added by Japan, is centered on 2.484 GHz, 12 GHz above the 13th. Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various devices. Each of the channels has signal width of 22 MHz, resulting in only three non-overlapping channels (1, 6, 11) among the first 13. With the latest IEEE 802.11g standard, however, there are four non-overlapping channels (1, 5, 9, 13) among the first 13, since IEEE 802.11g uses 20 MHz signals instead of 22 MHz.

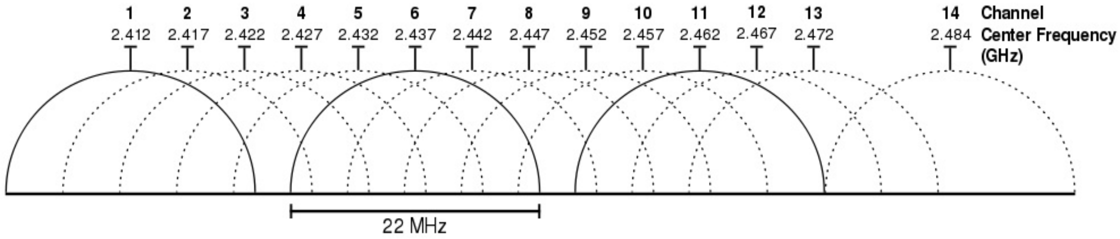


Figure 6.1 Channels of 22 MHz bandwidth in the 2.4 Ghz band

Channel	Center Frequency (MHz)	U.S. (FCC)	Europe (ETSI)	Japan
1	2.412	Yes	Yes	Yes
2	2.417	Yes	Yes	Yes
3	2.422	Yes	Yes	Yes
4	2.427	Yes	Yes	Yes
5	2.432	Yes	Yes	Yes
6	2.437	Yes	Yes	Yes
7	2.442	Yes	Yes	Yes
8	2.447	Yes	Yes	Yes
9	2.452	Yes	Yes	Yes
10	2.457	Yes	Yes	Yes
11	2.462	Yes	Yes	Yes
12	2.467	No	Yes	Yes
13	2.472	No	Yes	Yes
14	2.484	No	No	Only IEEE 802.11b

Table 6.1 WLAN channel frequencies in 2.4 GHz and their availability per region

6.1.2 5 GHz Wireless Band

The 5 GHz band is utilized by the IEEE 802.11 a/n standards and is composed of four frequency bands: 5.150 – 5.250 MHz, 5.250 – 5.350 MHz, 5.470 – 5.725 MHz and 5.725 – 5.850 MHz. As with 2.4 GHz band, not all 5 GHz band channels are available to every region. To be more precise: the 5 GHz band has 24 channels in the U.S. and 19 in Europe with 20 MHz bandwidth each, and a further 11 channels in the U.S. and 9 in Europe with 40 MHz bandwidth each. Operating at the 5 GHz band instead of 2 GHz offers several advantages, such as better penetration, better scatter and larger number of non-overlapping channels that results in less radio congestion.

Channel	Center Frequency (MHz)	U.S. (FCC)	Europe (ETSI)	Japan
34	5.170	No	No	Yes
36	5.180	Yes	Yes	Yes
38	5.190	No	No	Yes
40	5.200	Yes	Yes	Yes
42	5.210	No	No	Yes
44	5.220	Yes	Yes	Yes
46	5.230	No	No	Yes
48	5.240	Yes	Yes	Yes
52	5.260	Yes	Yes	Yes
56	5.280	Yes	Yes	Yes
60	5.300	Yes	Yes	Yes
64	5.320	Yes	Yes	Yes
100	5.500	Yes	Yes	Yes
104	5.520	Yes	Yes	Yes
108	5.540	Yes	Yes	Yes
112	5.560	Yes	Yes	Yes
116	5.580	Yes	Yes	Yes
120	5.600	No	Yes	Yes
124	5.620	No	Yes	Yes
128	5.640	No	Yes	Yes
132	5.660	No	Yes	Yes
136	5.680	Yes	Yes	Yes
140	5.700	Yes	Yes	Yes
149	5.745	Yes	No	No
153	5.765	Yes	No	No
157	5.785	Yes	No	No
161	5.805	Yes	No	No
165	5.825	Yes	No	No

Table 6.2 WLAN channel frequencies in 5 GHz and their availability per region

IEEE 802.11 Standard	2.4 GHz Band	5 GHz Band
802.11a	No	Yes
802.11b	Yes	No
802.11g	No	Yes
802.11n	Yes	Yes

Table 6.3 Radio bands that common IEEE protocols operate in

6.2 The Overlapping BSS Problem

The overlapping BSS problem refers to situations that two or more systems, unrelated to each other, are in close enough proximity to hear each other physically [61]. In other words, the stations or the AP of one BSS are able to receive frames from the other BSS. This is commonly known as the OBSS problem and is generally considered undesirable, because members of the OBSSs that interfere with each other and compete for channel access, may cause increased channel contention level and decreased performance [62]. In particular:

- Due to the doubling of the number of stations, the medium contention level increases dramatically [63].
- Interference makes it difficult for a wireless network to provide robust performance and lead to transient failures [64]. Hence, the stations can not receive the frames correctly [65].
- The expansion of the number of the hidden stations in the overall network system increases the probability of collisions.

Bellow are some of the possible overlapping scenarios.

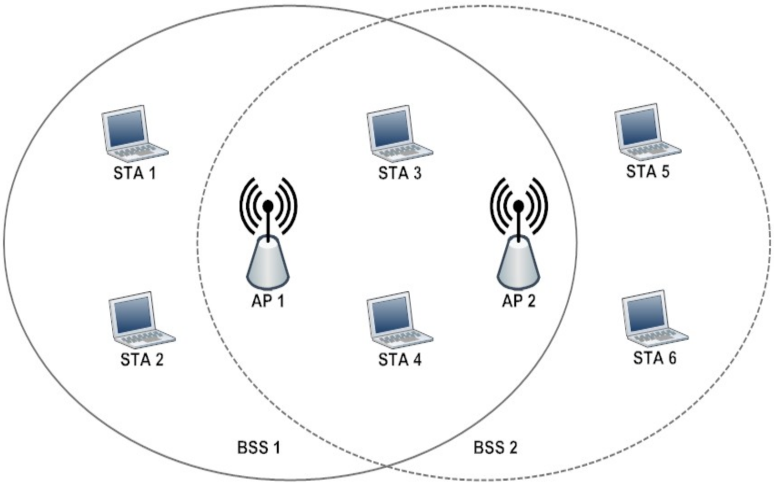


Figure 6.2 Scenario 1: Two OBSSs, APs within range of each other

Scenario 1 denotes an overlapping scenario where APs and some stations both from BSS1 and BSS2 interfere. Additionally, there are some stations from both BSSs, so-called hidden nodes, that increase the collision probability.

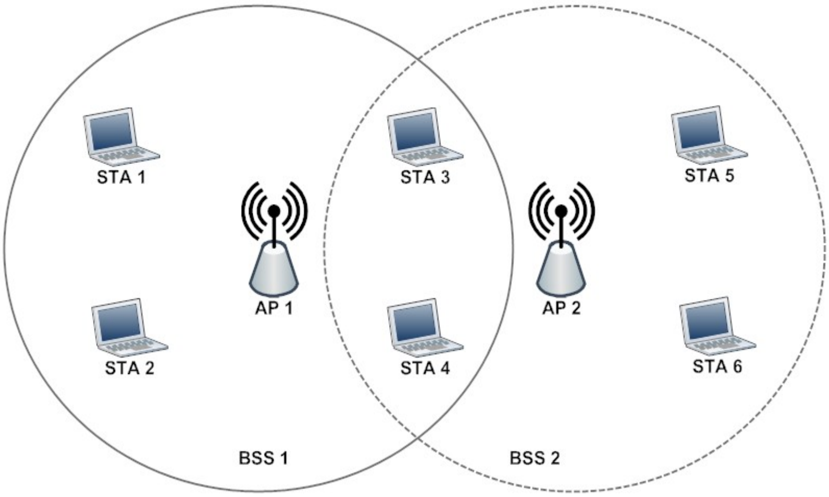


Figure 6.3 Scenario 2: Two OBSSs, APs not within range of each other

Scenario 2 illustrates two BSSs where the APs are not within the range of each other (Hidden APs), thus, the number of collisions may increase.

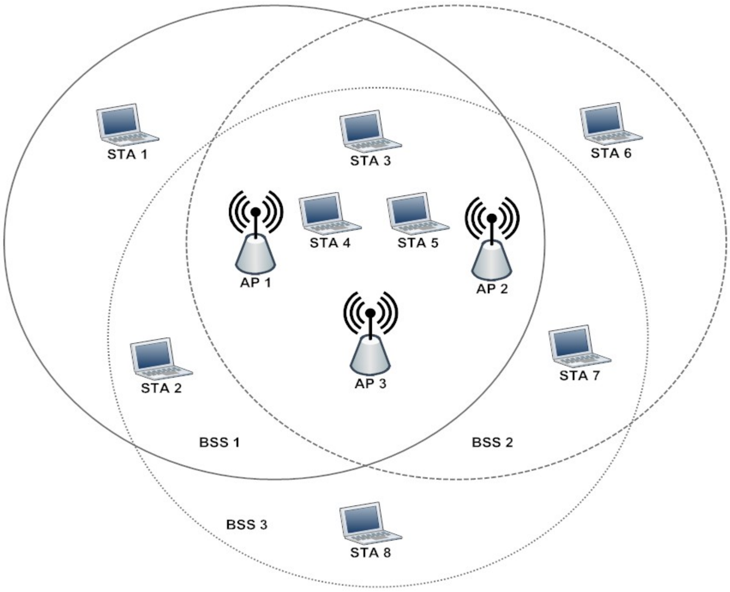


Figure 6.4 Scenario 3: Three OBSSs, APs within range of each other

In scenario 3, an overlapping scenario of three OBSSs is presented, where the AP and some stations of each BSS are within the range of each other, thus they do listen physically to each other. Moreover, there are hidden nodes from each BSS resulting in high collision probability.

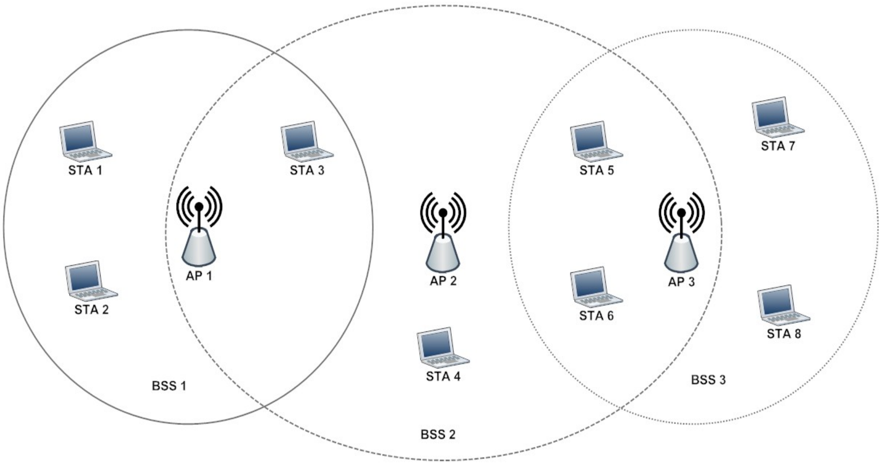


Figure 6.5 Scenario 4: Two OBSSs, one AP within range of two other

Scenario 4 represents the case of "neighborhood capture effect" [66] where there are three BSSs, with one of them being in between the two others which do not hear to each other. As a result, the central BSS suffers from a disproportionate degradation in throughput dependent upon the total traffic in all three BSS. Hence, the two side networks may monopolize the wireless medium, preventing the central one from getting any traffic through.

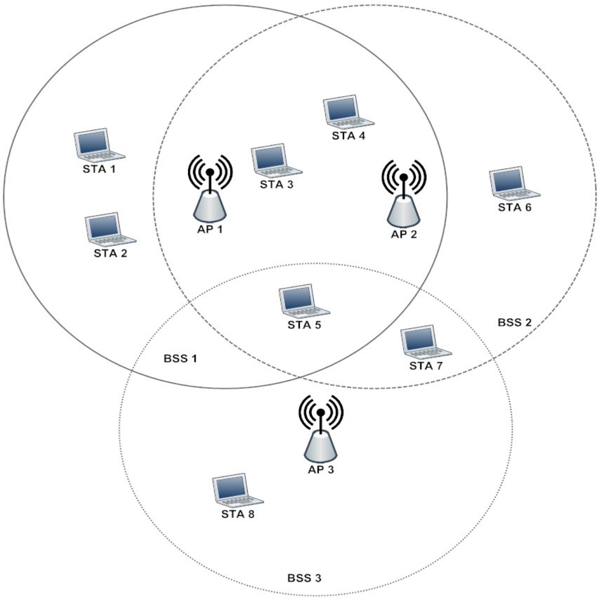


Figure 6.6 Scenario 5: Three OBSSs, two APs within range of each other

Scenario 5 depicts an overlapping scenario very similar to Scenario 3, with the only difference being that just the two out of three APs are within the range of each other.

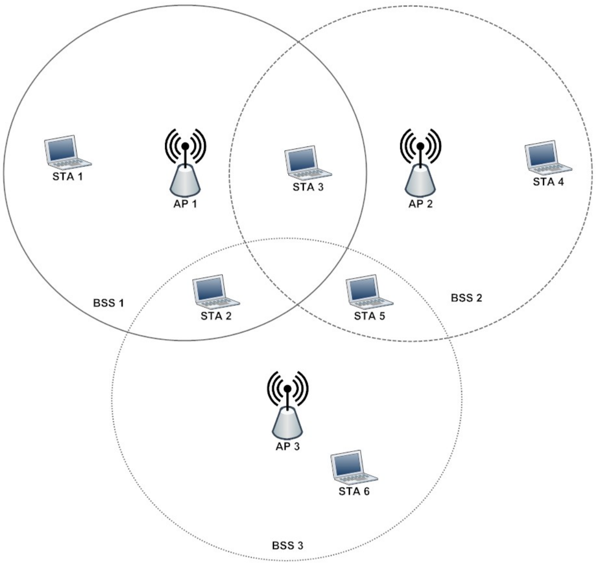


Figure 6.7 Scenario 6: Three OBSSs, APs not within range of each other, shared STAs

Scenario 6 illustrates an overlapping scenario of three OBSSs where the APs are out of range of each other (hidden APs) but there are stations from all three BSSs that overlap. Furthermore, there hidden nodes from each BSS.

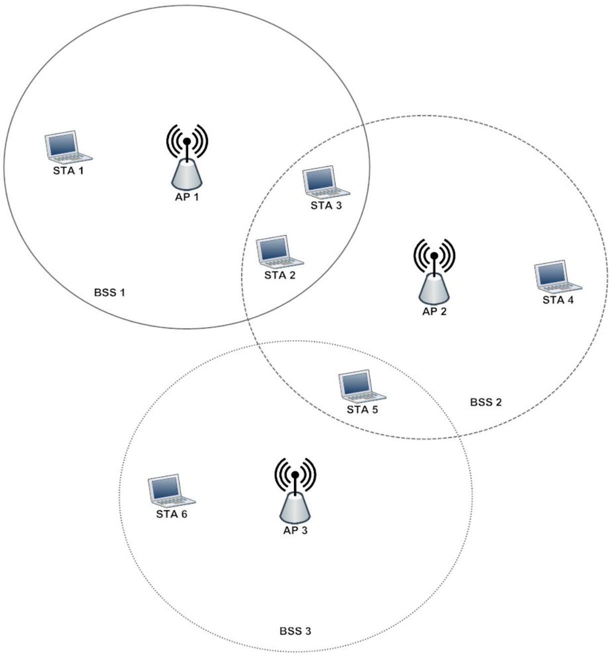


Figure 6.8 Scenario 7: Two OBSSs, APs not within range of each other

Scenario 7 depicts an overlapping scheme similar to the scenario 4 with the “neighborhood capture effect”, where one BSS is in between the other two. In this case, however, APs are not within the range of each other but only some stations of each BSS are overlapping.

6.3 Importance of the OBSS Problem

It is expected that the number of the OBSSs in IEEE 802.11 aa/ac becomes larger than in legacy standards (e.g. IEEE 802.11 a/n) because of both frequency bandwidth extension and increased number of WLAN devices [67]. Furthermore, as mentioned earlier there are cases where a station transmits in a 20 MHz channel, while also there are other cases where 40 MHz channels are being used. 20 MHz frames are transmitted in 20 MHz channel as in normal, while 40 MHz frames are transmitted occupying two adjacent 20 MHz channels. A major issue may arise when 40 MHz stations coexist with 20 MHz stations in the same channel, due to low possibility of having two 20 MHz channels vacant at the same time. Moreover, to acquire both channels for 40 MHz communication, contention probability will increase to double, as the 40 MHz stations will have to content with 20 MHz stations in both channels. On the other hand, 20 MHz stations cannot understand those data sent in 40 MHz, thus they may interfere with 40 MHz communication [68]. A solution to this problem is presented in [68], where Y. Utsunomiya et al. suggested a MAC protocol to realize coexistence between 20 MHz and 40 MHz stations. In the proposed protocol, an AP controls the 20 MHz and 40 MHz stations by setting a MAC level protection mechanism, to them, and divides the time into 20 MHz and 40 MHz periods.

In IEEE 802.11 aa/ac, 80 MHz of channel bandwidth is mandatory, thus there will only five non-overlapping channels; 36-38, 52-64, 100-112, 116-128 and 149-161 plus a sixth, 132-144 with a regulatory change, as it is illustrated in Figure 6.9. In addition, there is the option of 160 MHz of channel bandwidth with only two non-overlapping channels; 36-64 and 100-128. With this in mind, it becomes easily understandable that coexistence of different MHz stations in the same channel, becomes even complicated.

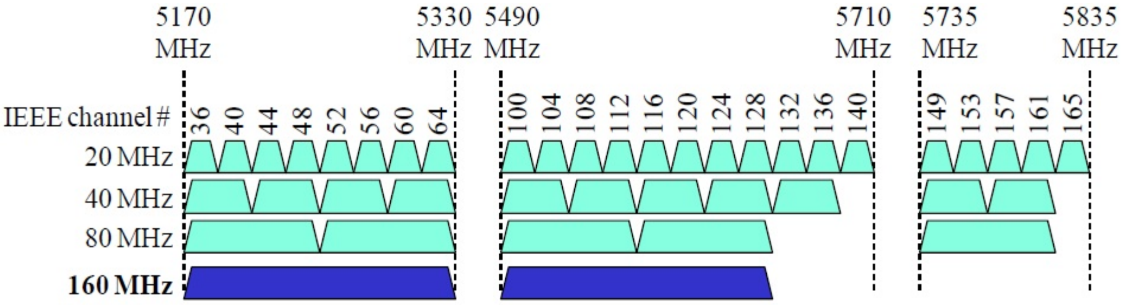
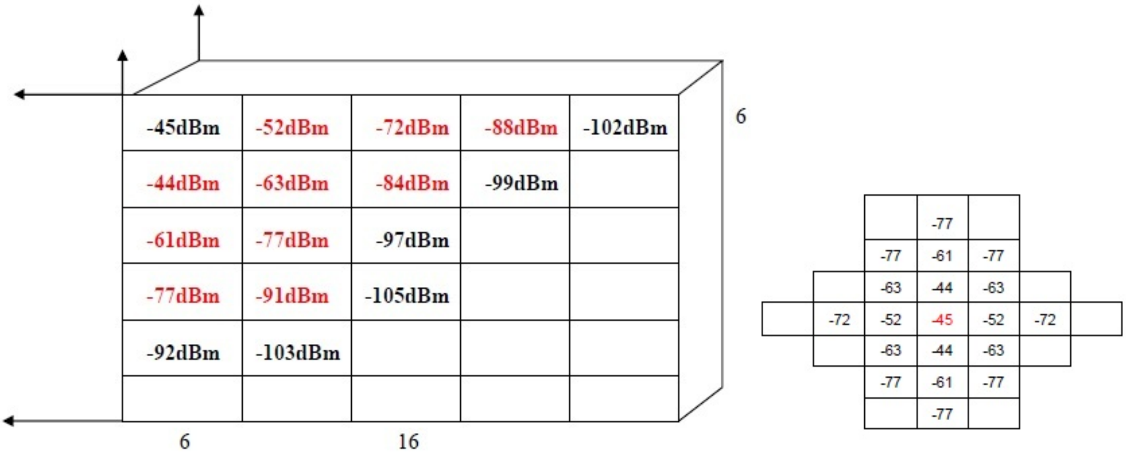


Figure 6.9 The non-overlapping channels in the 5 GHz band [61]

In [69], the authors carried out an analysis of OBSS with the intention of determining the criteria and features that will be used to provide a solution to the OBSS problem. Using empirical propagation formula, they intent to estimate the maximum potential number of overlapping networks for various residential scenarios. Table 6.4 illustrates the their results.

Detached Houses	12
Terraced Houses	16
Townhouses	25
Single Layout Apartments	28
Double Layout Apartments	53

Table 6.4 Maximum potential number of APs within range [69]



-45dBm	-52dBm	-72dBm	-88dBm	-102dBm
-44dBm	-63dBm	-84dBm	-99dBm	
-61dBm	-77dBm	-97dBm		
-77dBm	-91dBm	-105dBm		
-92dBm	-103dBm			

			-77			
		-77	-61	-77		
		-63	-44	-63		
	-72	-52	-45	-52	-72	
		-63	-44	-63		
		-77	-61	-77		
			-77			

Figure 6.10 Apartment block single layout [69]

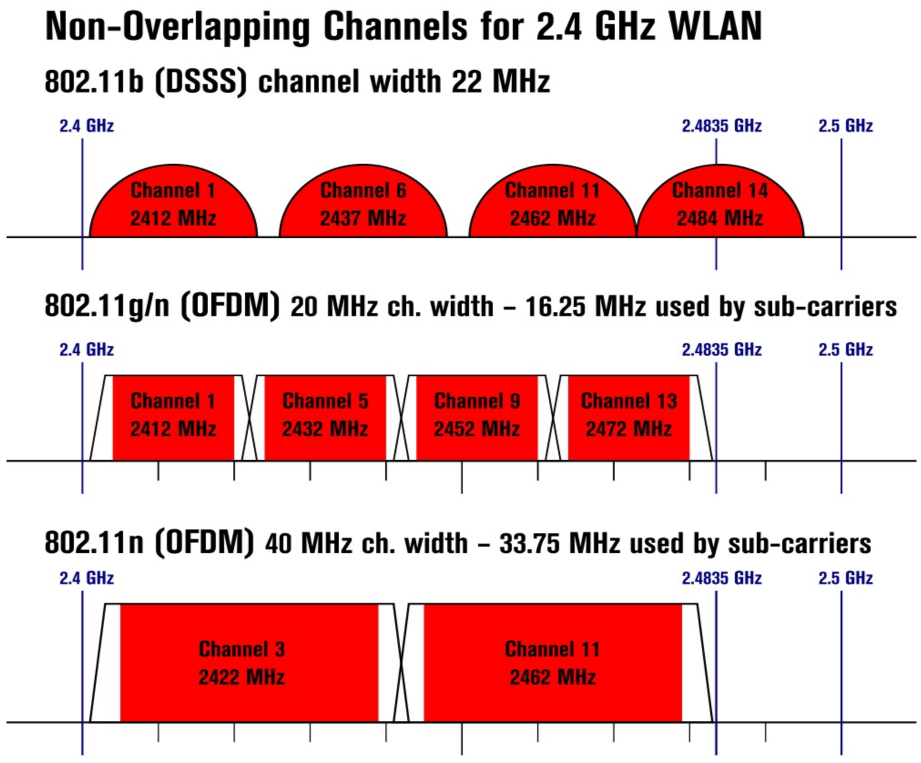


Figure 6.11 Non-overlapping channels in 2.4 GHz band for 20/40 MHz

Since there do not exist non-overlapping channels of 80 MHz bandwidth in the 2.4 GHz band, the IEEE 802.11 aa/ac will operate in the 5 GHz band, a spectrum with less interference. Channel selection can only partially reduce the problem as, even in the 5 GHz band with 19 non-overlapping channels, we could have situations of 2 or 3 overlapping BSSs. When the BSSs are using the legacy channel access (Distributed Coordination Function) or the EDCA function of IEEE 802.11e, the traffic competes fairly between the networks resulting in reduced bandwidth in all of them.

The negative effect on the performance is more severe when the Quality of Service enhancements of IEEE 802.11e are used, as these enhancements break down and cannot support the performance demands of multimedia streams. When one of the BSSs uses EDCA with admission control, the Access Point controls the admission of new streams, based on the information it has about its own BSS, but it has no control and no information about the traffic in the other overlapping networks. Therefore, it cannot guarantee the desired protection to the admitted flows and ensure they are given the agreed Quality of Service. In the case where one of the networks uses the HCCA function, in which the AP schedules traffic during a Contention-Free Period and grants Transmit Opportunities (TXOP) to the stations, this network is able to protect the bandwidth in its own network, reducing the available bandwidth for the rest of the networks. However, when two or more networks use the HCCA function, the AP may not be able to allocate time when it needs to, as it has to obey the TXOPs of other networks. Again, this results in reduced bandwidth for the scheduled protected traffic and no real protection for QoS restraints.

6.4 The IEEE 802.11aa Task Group Approach

The approach that was selected by the IEEE 802.11aa Task Group to manage the Overlapping BSS situation is to provide a decentralized mechanism for neighboring APs to exchange information about the QoS depended traffic load in each BSS. This information can be used for more efficient channel selection and, if it is necessary for BSSs to share a channel, it allows APs to cooperate and work as one bigger QoS-aware network, sharing fairly the wireless medium. This approach is designed to mitigate the effects of overlapping BSSs and provide the means to [70]:

- Advertise QoS load information for channel selection.
- Extend the admission control and scheduled mechanisms to a distributed environment.
- Enable the coordination of scheduled HCCA TXOPs between HCs operating with overlapping BSSs.

6.4.1 QLoad Report Element

The algorithm is based on the exchange of the QLoad Report Element between access points. This Report Element is transmitted with one of the following ways:

- When requested by another AP with a QLoad Request frame. For example, an AP performing the channel selection procedure.

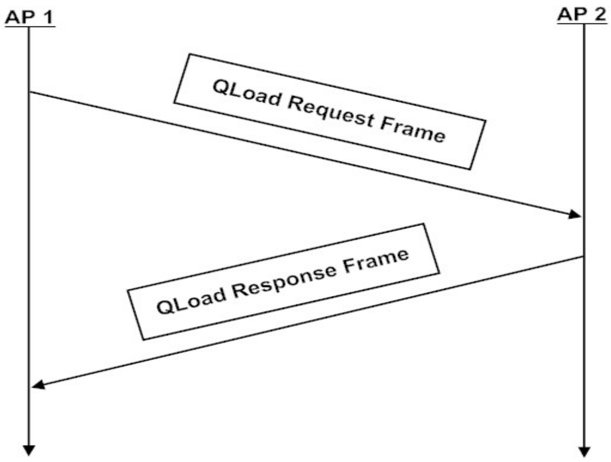


Figure 6.12 QLoad frame transmission, case 1

- Whenever there is a change in the values it includes. For example, when a new QoS stream is accepted.

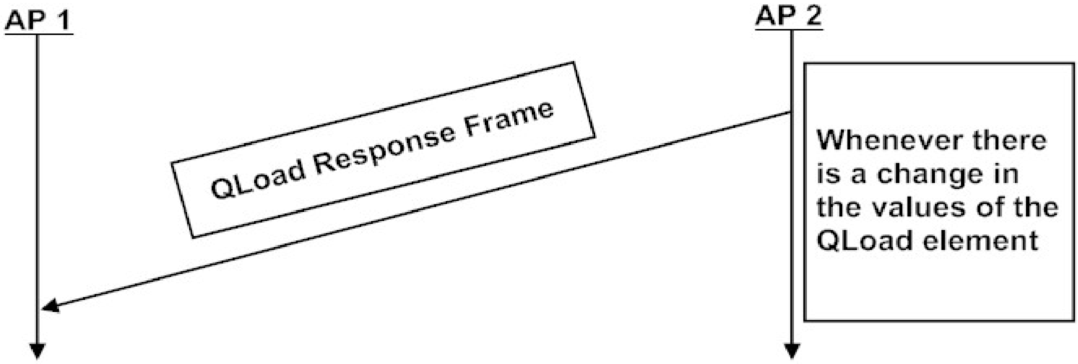

AP 1
AP 2
QLoad Response Frame
Whenever there is a change in the values of the QLoad element

Figure 6.13 QLoad frame transmission, case 2

- Optionally, when the dot11QLoadReportActivated is true, it is included in Beacons every dot11QLoadReportIntervalDTIM.

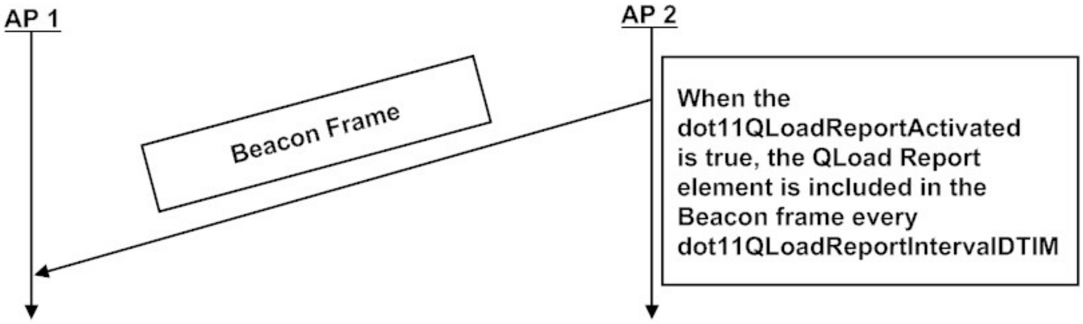

AP 1
AP 2
Beacon Frame
When the dot11QLoadReportActivated is true, the QLoad Report element is included in the Beacon frame every dot11QLoadReportIntervalDTIM

Figure 6.14 QLoad frame transmission, case 3

The Report Element is exchanged directly between APs that are in direct range of each other, as in Figure 6.2. However there is the case that a network overlaps with some stations in one BSS but cannot be seen by the AP as illustrated in Figure 6.4. For these cases the AP can use the neighbor report capability that was defined in IEEE 802.11k amendment. With this, it can request from its associated stations to scan the medium for neighboring APs and send back a Beacon Report, which may contain the QLoad Report Element.

	Element ID	Length	Potential Traffic Self	Allocated Traffic Self	Allocated Traffic Shared	EDCA Access Factor	HCCA Peak	HCCA Access Factor	Overlap	Sharing Policy	Optional Subelements
Octets:	1	1	5	5	5	1	2	1	1	1	Variable

Figure 6.15 QLoad Report Element format

The first three fields have the QLoad field format shown in Figure 6.16. The Mean field is the mean medium time measured in units of 32μs per second for the sum of all the traffic streams, and the standard deviation represents the statistical standard deviation from this mean. The two other fields represent the number of AC_VO and AC_VI streams that are active and can be used for some of the calculations. The way the mean and standard deviation is calculated is included in the informative annex. It is based on the way medium time is calculated in the recommended practices for admission control in the IEEE 802.11-2007 standard, but also adds an overhead factor, based on the number of streams, to estimate the medium overhead caused by the access time (AIFSN, backoff). The mean value for each traffic stream is calculated based on its mean data rate, and the standard deviation is calculated by taking into account the minimum and maximum data rate. When admission control is not used, the AP has to monitor the data rate of QoS streams (those belonging in AC_VI and AC_VO access categories) to calculate the mean and maximum medium time. These values for all the streams are then summed to obtain the total mean and standard deviation.

	Mean	Standard Deviation (Stdev)	Reserved	AC_VO Streams	AC_VI Streams
Bits:	16	14	2	4	4

Figure 6.16. QLoad Field format

6.4.2 Calculating field values

The Potential Traffic Self informs about the total QoS traffic an AP can expect. It is always equal to or greater than the Allocated Traffic Self field. The potential traffic is calculated by keeping an archive of the maximum value of any of the fields (mean, AC_VO streams, AC_VI streams) over a seven day period. Any streams that get rejected by admission control because of overallocation are also added to the value of the potential traffic. The Allocated Traffic Self includes all the QoS traffic an AP has allocated at any given time. It changes every time a new stream is accepted by EDCA admission control or the HCCA hybrid controller, and every time such as stream is deleted. The Allocated Traffic Shared sums the values of all the AP's there is information about, including the self AP. It can be useful to avoid the neighborhood capture effect. This way an AP knows that another AP is over-allocated due to sharing with a neighboring AP that is out of its own range.

The HCCA Peak represents the total TXOP requirements of admitted HCCA traffic streams in time units over one second and the HCCA Access factor is calculated as a fraction of the sum of HCCA Peaks of overlapping networks plus the self network over one second. As this is a sum over many networks, it may have a value greater than one, meaning that the total traffic is greater than the capacity of the wireless medium. Then the EDCA Access factor is calculated by adding the Potential Traffic of all overlapping networks including the self network, and subtracting the HCCA traffic to obtain the EDCA traffic. Like the HCCA Access Factor it is expressed as a fraction possibly greater than one.

The Overlap number represents the number of other APs sharing the same channel that this AP has detected by detecting their Beacons. The sharing policy field shows if the AP currently uses a static or dynamic sharing policy. A static sharing policy means that the medium time of each AP does not change when the allocated traffic changes. In a dynamic sharing policy the medium time of each AP may change as it allocates more traffic. The optional subelements field is reserved for future versions and is not currently used.

The calculation of these fields, the channel selection procedure (sub-chapter 6.4.3) and the sharing schemes (sub-chapter 6.4.4) are included in an informative annex which is intended only as a suggestion and therefore it is not obligatory for an implementation.

6.4.3 Channel Selection

The channel selection procedure is as follows. The AP scans all the available channels for Beacons by other APs and records for each channel the APs that use it, including their QoS capabilities, and if they support the QLoad report, the information about overlaps and QoS traffic. With these information the AP can select a channel in the following order:

- A channel free from any overlaps with other APs
- The channel with the least overlaps with other QoS capable APs
- Depending on whether the AP uses EDCA admission control or a Hybrid Controller, it should select the channel with the least overlaps with APs that use the same transmission mode.
- From these channels, it should select the one that reports the less Overlaps in its QLoad report.
- Finally, it should select the channel that shows the less potential traffic according to the QLoad reports.

More specifically, the recommended method for channel selection can be implemented by adoption of the following procedures [70]:

- Create a list of the available channels. Typically this is the list of channels allowed by regulation in the operating regulatory domain, however this list might be modified by management policy (e.g. removing overlapping channels, avoiding radar detect channels).
- Create an array for each available channel that allows the recording of the QoS AP count, Admission Control Mandatory count, HC count, overlap count and potential load for that channel.
- Step through the list of available channels, listening for beacons for at least dot11OBSSScanPassiveTotalPerChannel TUs per channel.
- Upon completion of the scan of a channel, process the beacons received on that channel, filtered to the set of unique BSSIDs:
    - Using the capabilities signaled in the beacon, modify the QoS AP count, Admission Control Mandatory count, HC count, overlap count and potential load of the channel array for the primary channel indicated in the received beacon.
    - If the AP is using a channel bandwidth that is greater than the channel spacing (e.g. when using the 2.4GHz band or when the overlapping AP allows 40MHz HT PPDUs in its BSS) also update the channel array for channels that are affected by this overlapping BSS. For example a beacon received on channel 2 indicating a 20MHz BSS also affects channels 1, 3 and 4.
- Upon completion of scanning all of the channels, the AP has information on the number of APs and the potential load of each channel, including co-channel BSSs.
- If the channel array indicates that there are channels with no other APs, it is recommended to randomly choose one of these “empty” channels.
- Otherwise, create a list of candidate channels by selecting only the channels with the lowest number of QoS APs. For example if the channel scan procedure indicated that there were two QoS APs on channel 3, three QoS APs on channel 6 and two QoS APs on channel 11, the list of candidate channels would contain 3 and 11.
    - If this list contains one or more channels with non QoS APs, then filter the list for the least number of APs.
    - If this list contains more than one channel, it is recommended to randomly choose one of these channels.

- If this list contains more than one channel and the AP has been configured to use Admission Control Mandatory for AC_VI or AC_VO:
    - Filter the list for the minimum count of QoS AP where the EDCA Parameter Set element is present in the Beacon frame and with Admission Control Mandatory not set for AC_VI or AC_VO.
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with Admission Control Mandatory set for AC_VI or AC_VO and that does not indicate support for QLoad reporting.
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with an HC and that does not indicate support for QLoad reporting.
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with an HC, and that indicate support for QLoad reporting (as indicated by the QLoad Report field equal to 1 in the Extended Capabilities element).
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with Admission Control Mandatory set for AC_VI or AC_VO and that indicates support for QLoad reporting (as indicated by the QLoad Report field equal to 1 in the Extended Capabilities element).
- If this list contains more than one channel and the AP has an HC:
    - Filter the list for the minimum count of QoS AP with an HC and that does not indicate support for QLoad reporting.
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with Admission Control Mandatory set for AC_VI or AC_VO and that does not indicate support for QLoad reporting.
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with an HC, and that indicate support for QLoad reporting (as indicated by the QLoad Report field equal to 1 in the Extended Capabilities element).
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP with Admission Control Mandatory set for AC_VI or AC_VO and that indicates support for QLoad reporting (as indicated by the QLoad Report field equal to 1 in the Extended Capabilities element).
    - If this list contains more than one channel, filter the list for the minimum count of QoS AP where the EDCA Parameter Set element is present in the Beacon frame and with Admission Control Mandatory not set for AC_VI or AC_VO.

- If this list contains more than one channel, filter the list to the set of channels with the minimum overlap count.
- If this list contains more than one channel, filter the list to the set of channels with the minimum potential load.
- From the remaining channels in this list, randomly choose one of these channels.

6.4.4 Sharing in an OBSS situation

If the EDCA Access Factor is greater than one, then there is a potential over-allocation of the WM. APs are advised to avoid this in the Channel selection process but if over-allocation exists, then a sharing scheme is recommended to ensure that each AP has a fair share of the bandwidth, but more importantly, to ensure that any already admitted or scheduled QoS stream are not impaired by the addition of streams from any overlapping BSS. The EDCA Access Factor, HCCA Access Factor and Potential Traffic Self fields in the QLoad Report are provided to enable sharing schemes to be used.

The sharing scheme also protects an AP from the neighborhood effect where it has neighbors that are hidden from each other. A major objective of an OBSS sharing scheme is that if a QoS stream is allocated or scheduled, then it is not compromised by the addition of further streams from any overlapping BSS that would cause the medium to be over-allocated. This is achieved if the APs in overlapping BSSs cooperate [70].

The standard proposes two sharing schemes as examples of static and dynamic sharing policies. The goal of both these schemes is to ensure that the total of QoS traffic admitted by the overlapping networks does not exceed the capacity of the wireless medium. They are also useful to ensure that the overlapping networks share fairly the available resources. Each AP calculates a Maximum Allocation Value, based on the number of overlapping QoS APs, also taking into account non-QoS APs that overlap in order to provide some resources for non-QoS traffic, too.

The first scheme is called Proportional Sharing and it is an example of a static sharing policy. Each AP calculates its maximum allowable traffic based on the EDCA and HCCA access factors. When the AP wants to add a new traffic stream it checks if the sum will exceed its maximum allowable traffic. The second scheme is called On-demand Sharing and is an example of a dynamic sharing policy. The AP adds new streams based on the maximum Allocated Traffic Self value from the overlapping APs.

It is suggested that APs use the On-demand Sharing scheme until they reach the Maximum Allocation Value for any of the overlapping networks, and then use the proportional sharing scheme for any subsequent requests.

6.4.4.1 Proportional Sharing scheme [70]

When using the proportional sharing scheme, the AP examines the sum of the EDCA and HCCA Access Factors in the QLoad Reports from each overlapping BSS, including its own QLoad, and determines the maximum. This maximum value is termed the “combined access factor”.

- If the maximum value from the combined access factor is less than or equal to MAV, the AP is advised to allocate only up to its advertised Potential Traffic Self traffic.
- If the maximum value from the combined access factor is greater than MAV, then the AP is advised to allocate only up to a value of its Potential Traffic Self divided by the combined access factor, multiplies by MAV.

In the proportional sharing scheme, before an AP allocates a new Medium Time or schedules a new TXOP in response to an ADDTS Request, ti checks that this addition does not exceed its sharing limit, as follows:

- If the EDCA Access Factor is less than or equal to MAV, then the AP allocates up to its advertised Potential Traffic Self, with the composite stream (MAX traffic) calculated as:

$$\text{MAXtraffic} = \mu_{tot} + 2\,\sigma_{tot}.$$

- If the EDCA Access Factor is greater than MAV, the AP carries out the following:
  - Calculate the peak traffic value of the Potential Traffic Self, using:

$$\text{Peak} = \mu_{tot} + 2\,\sigma_{tot}.$$

  - Divide this value by the combined access factor and multiply by MAV. This is termed the maximum allowable Potential Traffic Self traffic.
  - Calculate the resulting value of the Allocated Traffic Self if the new TSPEC is accepted, as explained in aa.2.4, and then calculate the resulting peak value using:

$$\text{Peak} = \mu_{tot} + 2\,\sigma_{tot}.$$

- ○ If the resulting peak value, calculated in step 3 is greater than the maximum allowable Potential Traffic Self traffic, then the TS Request is advised to be rejected.
- ○ If the resulting peak value, calculated in step 3 is less than the maximum allowable Potential Traffic Self traffic, and the TS Request is for EDCA admission, then it is advised to be accepted.
- ○ The AP then should check that it is possible to schedule TXOPs using the HCCA TXOP advertisement.

If the new stream is allocated, then the AP updates the appropriate fields in its QLoad element.

6.4.4.2 On-demand Sharing scheme [70]

The On-demand Sharing scheme is as follows:

- Before allocating a new stream, the AP examines the Allocated Traffic Shared values in the QLoad Reports from each overlapping BSS, including its own QLoad, and selects the maximum Allocated Traffic Shared value which has the highest peak value, using:

$$\text{Peak} = \mu_{tot} + 2\ \sigma_{tot}.$$

The AP also notes the number of AC_VI and AC_VO streams in this maximum Allocated Traffic Shared Field.

- The AP adds the requested new stream *(new)* to the selected maximum Allocated Traffic Shared value *(max)* determined in step 1, using:

$$\mu = \mu_{new} + \text{Peak}$$

$$\sigma = \surd\sigma^2{}_{new} + \sigma^2{}_{max}$$

- The AP then calculates the peak value for the new composite stream calculated in step 2, using:

$$\text{Peak} = \mu + 2\sigma$$

- Using the values of the AC_VI and AC_VO streams noted in step 1, plus the stream represented be the new stream, the AP determines the new EDCA Access Factor and then the combined access factor, as described in aa.4.2.2.
- Multiply the peak value calculated in step 3 by the EDCA Access Factor, determined in step 4. This is the new Peak Traffic requirement.
- If this Peak Traffic requirement value calculated in step 5 is greater than MAV, then the AP is advised to refuse to allocate the new stream.
- If the peak value calculated in step 5 is less than or equal to MAV, and the new allocation is for EDCA admission ADDTS, then the AP allocates that new traffic.
- If the peak value calculated in step 4 is less than or equal to MAV, and the new allocation is for HCCA ADDTS, the AP should check if it possible to schedule TXOPs using the HCCA TXOP advertisement.

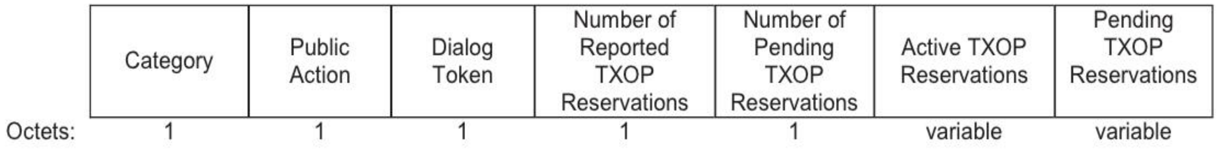
If the new stream is allocated, then the AP updates the appropriate fields in its QLoad element.

6.4.5 HCCA TXOP Negotiation

In order to provide a means of synchronizing the TXOPs between overlapping networks that use HCCA or mixed HCCA and EDCA mode, the IEEE 802.11aa standard provides a set of action frames and information elements that can be exchanged between APs in direct contact to inform each other of their TXOP schedules and allow them to schedule TXOP for newly admitted traffic streams without compromising the schedule of other APs.

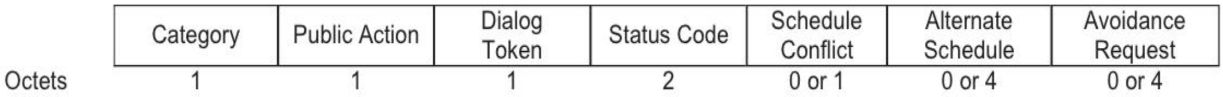
Collaboration candidates are APs that can exchange frames directly without the use of a third station. The AP keeps a table of all its collaboration candidates. Collaboration candidates support both protected and unprotected (public) TXOP negotiation. If peer APs have both protected and unprotected TXOP negotiation activated, then the protected mode is used.

The TXOP schedule coordination is achieved with the use of HCCA TXOP Advertisement and HCCA TXOP Response frames, which are represented in Figure 6.17 and Figure 6.18, respectively. When the AP wants to schedule a TXOP for a new traffic stream, it sends a TXOP advertisement frame to all the APs in the table with its current active TXOP reservations and the proposed new reservation. An HCCA TXOP Count element is also included in the Beacon frame to indicate that an HCCA TXOP schedule has changed.



	Category	Public Action	Dialog Token	Number of Reported TXOP Reservations	Number of Pending TXOP Reservations	Active TXOP Reservations	Pending TXOP Reservations
Octets:	1	1	1	1	1	variable	variable

Figure 6.17 HCCA TXOP Advertisement Frame



	Category	Public Action	Dialog Token	Status Code	Schedule Conflict	Alternate Schedule	Avoidance Request
Octets	1	1	1	2	0 or 1	0 or 4	0 or 4

Figure 6.18 HCCA TXOP Response Frame

An AP shall not send an Add Traffic Stream (ADDTS) Response action frame to the requesting station until one of the following conditions occurs [70]:

- The AP has received an HCCA TXOP Response frame from all the APs to which HCCA TXOP advertisements were sent, with the status field equal to SUCCESS.
- At least two beacon frames have been received from all the APs to which HCCA TXOP advertisements were sent.
- A beacon containing the HCCA TXOP Update Count element is received from all the APs to which HCCA TXOP advertisements were sent.
- A period of three dot11BeaconPeriod TU has elapsed.

If an AP receives another TSPEC request while waiting for one of the above conditions to occur, it shall delay processing this additional TSPEC request until one of the above conditions occurs.

Upon reception of an unprotected HCCA TXOP Advertisement, an AP with dot11PublicTXOPNegotiationActivated set to true, shall discard any entries that correspond to the MAC address of the AP that sent the HCCA TXOP Advertisement and shall prepare a response using the procedures below [70]:

- An AP with dot11ProtectedTXOPNegotiationActivated set to false shall discard any received Protected HCCA TXOP Advertisement frames.
- An AP with dot11ProtectedTXOPNegotiationActivated set to true that does not have an active security association with a peer AP that indicates support for protected HCCA TXOP negotiation shall use the AP PeerKey Protocol and the Authenticated Mesh Peering Exchange (both are defined in the original IEEE 802.11 standard) to

negotiate security parameters and secure the Protected HCCA TXOP Advertisement frames.

Upon reception of a valid Protected HCCA TXOP Advertisement frame, an AP with dot11ProtectedTXOPNegotiationActivated set to true, shall discard any entries that correspond to the MAC address of the AP that sent the HCCA TXOP Advertisement and shall prepare a response using the procedures below [70]:

- If the HCCA TXOP Advertisement frame (either protected or unprotected) has not been discarded due to the procedures above, the AP shall create a new entry for each TXOP reservation in the Active TXOP Reservations field of the (Protected) HCCA TXOP Advertisement frame.
- If the HCCA TXOP Advertisement frame (either protected or unprotected) has not been discarded due to the procedures above, the AP shall inspect its HCCA schedule to check if the TXOP Reservations given in the Pending TXOP Reservations field of the HCCA TXOP Advertisement frame is in conflict with an existing accepted HCCA TXOP, allocated by itself. If there is no conflict, the AP shall send an HCCA TXOP Response frame with the status field set to SUCCESS and create an entry for each TXOP Reservation in the Pending TXOP Reservations field in the HCCA TXOP Advertisement.
- If the HCCA advertisement was sent using an unprotected Public Action frame, the HCCA TXOP Response shall be send using an unprotected Public Action frame, too.
- If the HCCA advertisement was sent using a Protected HCCA TXOP Advertisement frame, the HCCA TXOP Response shall be sent using a Protected HCCA TXOP Response frame.
- If the AP detects that the TXOP given in the (Protected) HCCA TXOP Advertisement frame is in conflict with an existing accepted HCCA TXOP and this AP is not itself in the process of processing an ADDTS request, it shall send a (Protected) HCCA TXOP Response frame with the status field set to TS_SCHEDULE_CONFLICT and the Alternate Schedule field set to a period of time that does not conflict with any currently accepted HCCA TXOPs and the Avoidance Request field absent. The duration sub-field of the Alternate Schedule field should be greater than or equal to the duration sub-field of the schedule field in the (Protected) HCCA TXOP Advertisement frame. The duration sub-field of the Alternate Schedule field may be less than the

duration sub- field of the schedule field in the (Protected) HCCA TXOP Advertisement frame, when there is an insufficient period of time that does not conflict with currently accepted HCCA TXOPs.

- If the AP detects that the TXOP given in the (Protected) HCCA TXOP Advertisement frame is in conflict with an in-progress ADDTS request for a HCCA TXOP for which HCCA TXOP Response frames have not been received, it shall send a (Protected) HCCA TXOP Response frame with the status field set to TS_SCHEDULE_CONFLICT with the Alternate Schedule and Avoidance Request fields set according to the following rules:
  - If MIX(MAC_r) < MIX(MAC_i), the Alternate Schedule field is set to a value that does not conflict with any accepted HCCA TXOPs and also does not conflict with the TXOP of the in-progress ADDTS request. The Avoidance Request field is set to the TXOP of the in-progress ADDTS request.
  - If MIX(MAC_r) > MIX(MAC_i), the Alternate Schedule field is set to the value from the TXOP Reservation from the TXOP Advertisement frame. The Avoidance Request field is set to a time period that does not conflict with any accepted HCCA TXOPs nor the TXOP in the Alternate Schedule field and has sufficient duration and service interval to meet the requirements of the in-progress ADDTS request.

Where:

- MAC_r is the MAC address of the AP that received the TXOP Advertisement frame.
- MAC_i is the MAC address of the AP that sent the TXOP Advertisement frame.
- The MIX function takes the 6 octets of a MAC address and computes a 6 octet value:

$$MIX(MAC) = MAC[4] \,||\, MAC[5] \,||\, MAC[0] \,||\, MAC[1] \,||\, MAC[2] \,||\, MAC[3]$$

Case	Status Code	Alternate Schedule Field	Avoidance Request Field
No conflict with existing or in-progress schedules	SUCCESS	Not present	Not present
Conflicts with existing schedule, no ADDTS request in progress	TS_SCHEDULE_CONFLICT	Period of time that does not conflict with any currently accepted HCCA TXOPs	Not present
Conflict in-progress schedules, MIX(MAC$_r$) < MIX(MAC$_i$)	TS_SCHEDULE_CONFLICT	Period of time that does not conflict with any currently accepted HCCA TXOPs nor the in-progress ADDTS request	Schedule of in-progress ADDTS request
Conflict in-progress schedules, MIX(MAC$_r$) > MIX(MAC$_i$)	TS_SCHEDULE_CONFLICT	Same schedule that was in the TXOP Advertisement	Period of time that does not conflict with any currently accepted HCCA TXOPs nor the period given in the Alternate Schedule field

Table 6.5 Contents of the HCCA TXOP Response frame

According to [70], the AP shall also keep a record of the TXOP proposed in the alternate schedule field in a TXOP avoidance record and should avoid scheduling any new HCCA TXOPs in this proposed period until any of the following conditions occurs:

i. A period of dot11HCCATXOPBeaconTimeout multiplied by dot11BeaconPeriod TUs has elapsed.

ii. The AP with dot11PublicTXOPNegotiationActivated set to true receives an unprotected HCCA TXOP Advertisement Public Action frame from the AP to which the unprotected HCCA TXOP Response frame was sent.

iii. The AP with dot11ProtectedTXOPNegotiationActivated set to true receives a Protected HCCA TXOP Advertisement frame from the AP to which the Protected HCCA TXOP Response frame was sent.

Finally, the standard also provides an algorithm for synchronizing the clocks between the collaborating APs so the TXOP reservations can work properly. The APs constantly watch for time drift between them and adjust to synchronize with the slower AP.

6.5 Related Work

The OBSS problem has concerned a lot of researchers who have tried to suggest various solutions. Some of these proposals are categorized and are presented in following sub-chapters. The categorization has been made based on whether the work suggests single channel management or dynamic channel switching. However, some of the proposals cannot be grouped to any of these two categories, thus they are presented separately.

6.5.1 Single channel management

An approach to the OBSS problem is to create a mechanism where the overlapped BSSs are able to manage access in the shared channel, in a way that would be fair and would prevent interference. Schemes that are based on this approach, require from the APs from each overlapped BSS to periodically communicate with each other, in order to cooperatively coordinate their channel access operations. This means that such a scheme is only applicable in an OBSS situation where the APs are in direct range with each other, such as in the topologies described in Figure 6.2 and Figure 6.4.

Bo Han et al. [62], proposed the use of Channel Access Throttling (CAT) in order to manage radio resources for overlapping BSSs. With CAT an AP of each BSS is provided with a coordination mechanism in order to control channel access parameters of its member stations on the fly. With this mechanism, privileged channel access can be supported for a particular BSS at a particular time. This can be achieved, for example, by assigning higher priority channel access parameters to stations associated with this BSS. Furthermore, by tracking how much each BSS has been given privileged channel access, it is possible to achieve proportional partitioning of channel capacity among the overlapped BSSs, thus improve channel utilization. In their scenario, the authors present a simple two-priority-group model which, however, can be extended to more complex models. For instance, a model that allows more than one BSSs to be assigned into the high-priority group, at the same time.

A similar solution is presented in [71]. The author combines two distributed schemes to achieve throughput fairness among overlapped BSSs. The first one uses Dynamic Network

Allocation Vectors (DNAVs) which dynamically adjust the channel interference by temporarily stopping transmissions in some BSSs, while the second scheme uses Forced Hand-Offs (FHO) to force stations, placed within the overlapped area, to hand off. The DNAV is used for each AP to calculate its BSS weighted throughput value and serves to keep throughput fairness among the BSSs. If an AP finds that its own weighted value is higher than the average of all the received weighted throughput values by a certain amount, it increases the NAV duration in its own BSS; otherwise the NAV duration is decreased. Without using NAV to control the inter-BSS interference, BSSs having a lower weighted value can force some associated stations to hand off to neighboring BSSs that have higher weighted throughput value.

In [72], a spectrum sharing concept is proposed that allows BSSs to coexist in a single channel, while providing QoS at the same time. With this scheme the overlapped BSSs multiplex their channel access in the time domain, where each system leaves some channel capacity that can be used as idle period for other systems that may want to compete for medium access. In a way this method can be considered as “TDMA between systems”. However, distributing idle period in a random manner may increase the collisions. Thus, the proposed scheme is implemented in a way that it will occupy the channel in a way keeping idle periods in a regular pattern. Therefore, this scheme can be referred as Regular Channel Access (RCA). RCA is helpful to the OBSSs in two ways: first it allows them to reliably predict the length of the idle periods and their starting offset, and second, it helps each BSS to utilize the idle periods for its own transmissions, reducing to the minimum the collisions caused by orthogonality in time. The simulation results have shown that the proposed solution can achieve a fair throughput sharing, keep the delay of multimedia streams transmission in low levels and reduce the total interference and overhead.

6.5.2 Dynamic channel switching

Another approach to the problem is channel switching after OBSS detection. However, recognizing the existence of OBSS is not as simple as it may sounds. First of all, stations do not always receive frames correctly from OBSSs, thus they may not be able to check the BSSID. This is even worse as the traffic becomes heavier and the transmission rates of frames originating from the OBSSs are higher. Another difficulty is that if the cell radius of the domestic BSS is smaller that that of the OBSS, some stations in the OBSS may transmit frames asynchronously and interfere with transmissions in the domestic BSS. If this interference causes frame errors, the domestic stations may assume that this interference is caused by degradation of channel condition [65].

With that in consideration, [65] proposes a method where stations can detect packets corrupted by interference, even while they receive frames from the domestic BSS. Stations consider two examinations in order to detect interferential packets. The first is to determine whether differential of averaged Received Signal Strength Indicator (RSSI) exceeds threshold. The authors explain that if both the RSSI exceeds two threshold values (one positive and one negative) and the Cyclic Redundancy Check (CRC) indicates that the packet is received incorrectly, then it is decided that interferential packet is detected. The second examination is to determine whether the frame duration derived from header information equals the frame duration as measured by the RSSI. Finally, if a station detects interferential packets with any of the described methods, it reports the existence of another BSS to the AP which, in turn, announces channel switching to all the associated stations in the domestic BSS. Simulation results have shown that this mechanism has a high probability of detecting interferential packets and, also, that throughput can be kept by channel switching.

[64] describes the implementation of a wireless mesh network that supports Dynamic Channel Switching (DCS). Although DCS enables wireless networks to avoid frequency channels with serious interference, it significantly increases the complexity of the networks' routing protocol. The authors integrated the proposed mechanism with fault-tolerant and load-balancing routing to demonstrate that it is still practical to apply DCS to IEEE 802.11-based APs. The resulted wireless mesh network is called “Carlsbad”. The simulation results have shown that despite the additional overhead, DCS can improve the overall throughput of a wireless network, for both TCP and UDP.

6.5.3 Other solutions

In [73], the authors propose an alternative method for nodes in a wireless network to detect and ignore frames received from a BSS, other than the one they are associated with. To achieve that, a new field is added in the Physical Layer Convergence Protocol (PLCP) header (Figure 6.19). This field contains a portion of BSSID, among others, to indicate who must decode this frame. Upon reception of such a frame a node determines whether or not this field is valid and, if it is, the node decodes the succeeding MAC frame. Otherwise, the node drops the MAC frame without decoding it and returns to medium carrier sensing mode. Even though this solution improves the area throughput in an OBSS environment, it does not provide a complete solution since it lacks in several ways. For example, as mentioned earlier, interference caused by OBSS may alter the transmitted data, thus the receiving nodes would not be able to check the BSSID field of the PLCP header. Also, since PLCP is used only by OFDM-based wireless LANs, this solution is limited only to this type of networks.

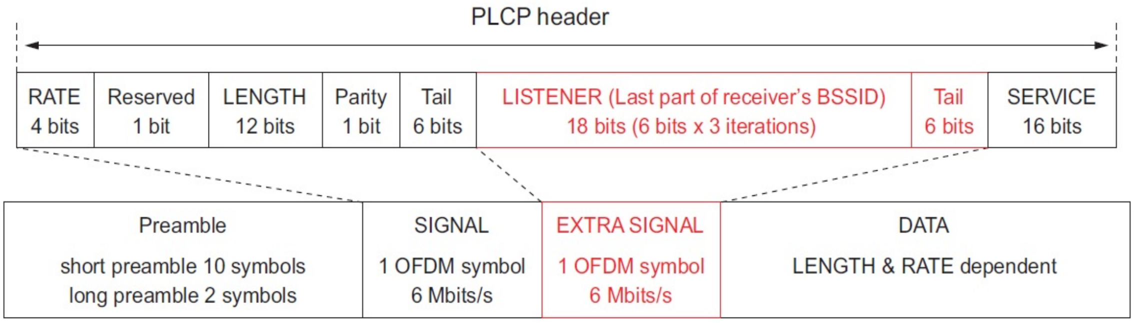


Figure 6.19 PLCP header modification

Chapter 7

Conclusions and Further Research

7.1 Conclusions

The current thesis focused on the research efforts that have been made by the IEEE 802.11aa Task Group and aim at providing improvements for audio/video transmissions over wireless LANs. To succeed this, the TGaa has defined various enhancements on the MAC layer. The latest IEEE 802.11aa draft release, is the Draft 9.0 and was published in January 2012.

Initially, Chapter 1 of the current thesis presented a short description of the IEEE organization and its family of protocols that operate on the wireless medium. A separate, more detailed overview of the IEEE 802.11 protocols was given in Chapter 2, since our objective, which was IEEE 802.11aa, belongs to this group of protocols. Chapter 3 contained a significant part of this thesis which has been devoted in describing the main features and functionality of the current IEEE 802.11 MAC layer, especially since the TGaa focuses on enhancing this particular layer.

Thereafter, the main fields of study of the TGaa were categorized in four groups: the Stream Classification Service, Interworking with 802.1AVB, Multicast and, finally, the OBSS issue. The first two are closely related to each other, thus, they were presented together in Chapter 4, whereas, the efforts about Multicast and the OBSS issues, were presented separately in Chapter 5 and Chapter 6, respectively. Along with the presentation of the TGaa efforts, the thesis also provided related approaches and proposals from individual researchers, who tried to provide solutions on these particular fields, mostly before the formation of the task group. Regarding the multicast issue, the individual proposals were further categorized based on the OSI/ISO reference model layer that they apply on. An extra category has been created, the so called Cross-Layer Solutions, where proposals that rely on more than one layers were presented. Finally, the individual solutions for the OBSS issue were divided in two categories, based on whether they suggest single channel management or dynamic channel switching.

7.2 Further Research

For future work, we are interested in creating an updated summary of the modifications and the enhancements on the MAC layer, as defined in the first oncoming IEEE 802.11aa standard. It would be also interesting to evaluate its performance both in simulation, but mostly in real conditions, and compare the results with those of the performance of legacy IEEE 802.11 protocols.

List of Figures

List of Tables

Bibliography

[1] B.H. Walke, S. Mangold, L. Brlemann, “IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence”, Wiley, January 2007.

[2] “IEEE 802.15 WPAN Task Group 3 (TG3)”, IEEE-802, [Online]. Available: http://www.ieee802.org/15/pub/TG3.html (Last Accessed: April 2012).

[3] “IEEE 802.15 WPAN Task Group 5 (TG5) Mesh Networking”, IEEE-802, [Online]. Available: http://www.ieee802.org/15/pub/TG5.html (Last Accessed: April 2012).

[4] “IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks”, IEEE-802, [Online]. Available: http://www.ieee802.org/15/pub/TG6.html (Last Accessed: April 2012).

[5] “IEEE 802.18 & 802.19”, IEEE-802, [Online]. Available: http://www.ieee802.org/misc-docs/GlobeCom2009/IEEE_802d18_and_d19_Kraemer.pdf (Last Accessed: April 2012).

[6] D.T. Wong, P.Y. Kong, Y.C. Liang, K.C. Chua, “Wireless Broadband Networks”, Wiley, April 2009.

[7] “IEEE 802.22 Working Group on Wireless Regional Area Networks”, IEEE-802, [Online]. Available: http://www.ieee802.org/22/ (Last Accessed: April 2012).

[8] G.R. Hiertz, D. Denteneer , L. Stibor, Y. Zang, X.P. Costa, B. Walke, “The IEEE 802.11 Universe”, IEEE Communications Magazine, vol. 48, issue 1, pp. 62-70, January 2010.

[9] IEEE Standard 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.

[10] R.T. Valadas, A.R. Tavares, A.M. de Oliveira Duarte, A.C. Moreira, C.T. Lomba, “The infrared physical layer of the IEEE 802.11 standard or wireless local area networks”, IEEE Communications Magazine, vol. 36, issue 12, pp. 107-112, December 1998.

[11] “IEEE 802.11 Frequency Hopping Spread Spectrum”, Wireless-Center, [Online]. Available: http://www.wireless-center.net (Last accessed: April 2012).

[12] N.R. Prasad, “IEEE 802.11 system design”, In Proceedings of the IEEE International Conference on Personal Wireless Communications (ICPWC), pp. 490-494, Nieuwegein, Netherlands, 17-20 December 2000.

[13] L. Litwin, M. Pugel, “The principles of OFDM”, www.rfdesign.com, January 2001.

[14] B. O'Hara, A. Petrick, “IEEE 802.11 handbook: a designer's companion”, Wiley-IEEE Press, January 2005.

[15] E. Perahia, R. Stacey, “Next generation Wireless LANs: Throughput, Robustness and Reliability in 802.11n”, Cambridge University Press, 2008.

[16] S. Mangold, L. Berlemann, “IEEE 802.11k: improving confidence in radio resource measurements”, In Proceedings of the IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), vol. 2, pp. 1009-1013, Berne, Switzerland, 11-14 September 2005.

[17] A.A. Tabassam, H. Trsek, S. Heiss, J. Jasperneite, “Fast and seamless handover for secure mobile industrial applications with 802.11r”, In Proceedings of the IEEE 34th Conference on Local Computer Networks (LCN), pp. 750-757, Lemgo, Germany, 20-23 October 2009.

[18] R.V. Nee, “Breaking the gigabit-per-second barrier with 802.11ac”, IEEE Wireless Communications, vol. 18, issue 2, pp. 4, April 2011.

[19] M. Cast, “802.11 Wireless Networks: The Definitive Guide”, O'Reilly Media, April 2005.

[20] F.Y. Hung, I. Marsic, “Effectiveness of Physical and Virtual Carrier Sensing in IEEE 802.11 Wireless Ad Hoc Networks”, In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), pp. 143-147, Kowloon, China, 11-15 March 2007.

[21] A. vonNagy, “Understanding Wi-Fi carrier sense” , [Online]. Available: http://revolutionwifi.blogspot.com/2011/03/understanding-wi-fi-carrier-sense.html (Last accessed: April 2012).

[22] D. Gao, J. Cai, K.N. Ngan, “Admission control in IEEE 802.11e wireless LANs”, IEEE Network, vol. 19, issue 4, pp. 6-13, July-August 2005.

[23] F. Cali, M. Conti, E. Gregori, “Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit”, IEEE/ACM Transactions on Networking, vol. 8, issue 6, pp. 785-799, December 2000.

[24] G. Bianchi, I. Tinnirello, “Kalman filter estimation of the number of competing terminals in an IEEE 802.11 network”, In Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies, INFOCOM, vol. 2, pp. 844-852, 30 March-3 April 2003.

[25] M. Hui, L. Xing, L. Hewu, Z. Peiyun, L. Shixin, Y. Cong, “Dynamic optimization of IEEE 802.11 CSMA/CA based on the number of competing stations”, In Proceedings of the 2004 IEEE International Conference on Communications, vol. 1, pp. 191-195, 20-24 June 2004.

[26] N. Qiang, I. Aad, C. Barakat, T. Turletti, “Modeling and analysis of slow CW decrease for IEEE 802.11 WLAN”, In Proceedings of the 14th IEEE Conference on Personal, Indoor and Mobile Radio Communications (PIMRC), vol.2, pp. 1717-1721, 7-10 September 2003.

[27] L. Wanming, Y. Baoping, L. Xiaoxong, M. Wei, “An enhanced service differentiation mechanism for QoS provisioning in IEEE 802.11e wireless networks”, In Proceedings of the 10th International Conference on Advanced Communication Technology (ICACT), vol. 1, pp. 175-180, Gangwon, South Korea, 17-20 February 2008.

[28] “IEEE 802.1”, IEEE-802, [Online]. Available: http://www.ieee802.org/1/ (Last Accessed: April 2012).

[29] G.M. Garner, R. Hyunsurk, “Synchronization of Audio/Video Bridging Networks Using IEEE 802.1AS”, IEEE Communications Magazine, vol. 49, issue 2, pp. 140-147, February 2011.

[30] “CCNA Exploration: LAN Switching and Wireless”, Cisco Systems, 2007-2009, Chapter 3.

[31] G. Venkatesan, “Multimedia Streaming over 802.11 links”, IEEE Wireless Communications Magazine, vol. 17, issue 2, pp. 4-5, April 2010.

[32] H. Zinner, J. Noebauer, K. Seitz, T. Waas, “A Comparison of Time Synchronization in AVB and FlexRay in-vehicle networks”, In Proceedings of the 9th Workshop on Intelligent Solutions in Embedded Systems (WISES), pp. 67-72, Regensburg, Germany, 7-8 July 2011.

[33] G.M. Garner, G. Feifei, K. den Hollander, J. Kongkyu, K. Byungsuk, L. Byoung-Joon, J. Tae-Chul, J. Jinoo, “IEEE 802.1 AVB and its application in carrier-grade Ethernet”, IEEE Communications Magazine, vol. 45, issue 12, pp. 126-134, December 2007.

[34] M. Jakovljevic, A. Ademaj, “Ethernet protocol services for critical embedded systems applications”, In Proceedings of the IEEE/AIAA 29th Digital Avionics Systems Conference (DASC), pp. 5.B.3-1–5.B.3-10, Salt Lake City, USA, 3-7 October 2010.

[35] J. Kuri, S.K. Kasera, "Reliable multicast in multi-access wireless LANs", In Proceedings of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, vol. 2, pp. 760-767, New York, USA, 21-25 March 1999.

[36] W. Xiaoli, W. Lan, W. Yingjie, Z. Yongsheng, "A reliable and efficient MAC layer multicast protocol in wireless LANs", In Proceedings of the IEEE 69th Vehicular Technology Conference (VTC), pp. 1-5, Barcelona, Spain, 26-29 April 2009.

[37] K. Tang, M. Gerla, "MAC reliable broadcast in ad hoc networks", In Proceedings of the Military Communications Conference (MILCOM). Communications for Network-Centric Operations: Creating the Information Force. IEEE, vol. 2, pp. 1008-1013, 2001.

[38] S. Min-Te, H. Lifei, A. Arora, L, Ten-Hwang, "Reliable MAC layer multicast in IEEE 802.11 wireless networks", In Proceedings of the International Conference on Parallel Processing, pp. 527-536, 18-21 August 2002.

[39] A. Lyakhov, V. Vishnevsky, M. Yakimov, "Multicast QoS support in IEEE 802.11 WLANs", In Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 1-3, Pisa, Italy, 8-11 October 2007.

[40] V. Srinivas, R. Lu, "An Efficient Reliable Multicast Protocol for 802.11-based Wireless LANs", In Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks & Workshops (WoWMoM), pp. 1-6, Kos, Greece, 15-19 June 2009.

[41] S.K.S. Gupta, V. Shankar, S. Lalwani, "Reliable multicast MAC protocol for wireless LANs", In Proceedings of the IEEE International Conference on Communications (ICC), vol. 1, pp. 93-97, 11-15 May 2003.

[42] J. Wenbin, J. Hai, L. Xiaofei, Y. Zhi, "A multicast based bandwidth saving approach for wireless live streaming system", International Journal of Smart Home, Security Engineering Research Support, vol. 2, pp. 65-80, January 2008.

[43] M. Samokhina, K. Moklyuk, S. Choi, J. Heo, "Raptor code-based video multicast over IEEE 802.11 WLAN", Seoul National University, June 2008.

[44] H. Fujisawa, K. Aoki, M. Yamamoto, Y. Fujita, "Estimation of multicast packet loss characteristic due to collision and loss recovery using FEC on distributed infrastructure wireless LANs", In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), vol. 1, pp. 399-404, 21-25 March 2004.

[45] M. Kappes, "An application-layer approach for multihop communication in IEEE 802 11 ad-hoc networks", In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), vol. 3, pp. 1359-1364, 21-25 March 2004.

[46] S. Karanth, T. Moscibroda, V. Navda, J. Padhye, R. Ramjee, L. Ravindranath, "DirCast A practical and efficient Wi-Fi multicast system", In Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP), pp. 161-170, Princeton, USA, 13-16 October 2009.

[47] C. Bravo, A. Gonzalez, "Evaluation and improvement of multicast service in 802 11b", Federico Santa Maria University, 2006.

[48] L. Zhi, G. Cheung, V. Velisavljevic, E. Ekmekcioglu, J. Yusheng, "Joint source-channel coding for WWAN multiview video multicast with cooperative peer-to-peer repair", In Proceedings of the 18th International Packet Video Workshop (PV), pp. 110-117, Hong-Kong, China, 13-14 December 2010.

[49] X. Zhu, T. Schierl, T. Wiegand, B. Girod, "Video Multicast over wireless mesh nerworks with scalable video coding (SVC)", Visual Communications and Image Processing, January 2008.

[50] M. Gerla, P. Zhao, B. Daneshrad, G. Pei, J.H. Kim, "MIMO-Cast: A Cross-Layer ad hoc multicast protocol using MIMO radios", In Proceedings of the IEEE Military Communications Conference (MILCOM), pp. 1-6, Orlando, USA, 29-31 October 2007.

[51] C.C. Hu, "Efficient cross-layer protocol for bandwidth-satisfied multicast in multi-rate MANETs", Wireless Networks, vol. 17, issue 3, April 2011.

[52] J. Villalon, P. Cuenca, L. Orozco-Barbosa, Y. Seok, T. Turletti, "ARSM: a cross-layer auto rate selection multicast mechanism for multi-rate wireless LANs", IET Communications, vol. 1, issue 5, pp. 893-902, October 2007.

[53] J. Villalon, P. Cuenca, L. Orozco-Barbosa, Y. Seok, T. Turletti, "Cross-Layer Architecture for Adaptive Video Multicast Streaming Over Multirate Wireless LANs", EEE Journal on Selected Areas in Communications, vol. 25, issue 4, pp. 699-711, May 2007.

[54] W.S. Lim, D.W. Kim, Y.J. Suh, "Design of Efficient Multicast Protocol for IEEE 802.11n WLANs and Cross-Layer Optimization for Scalable Video Streaming", IEEE Transactions on Mobile Computing, vol. 11, issue 5, pp. 780-792, May 2012.

[55] O. Alay, C. Li, A. Rai, T. Korakis, W. Yao, S. Panwary, "Dynamic Rate and FEC Adaptation for Video Multicast in Multi-rate Wireless Networks", In Proceedings of the 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops (TridentCom), pp. 1-8, Washington, USA, 6-8 April 2009.

[56] K. Maraslis, P. Chatzimisios, A.C. Boucouvalas, "IEEE 802.11aa: Improvements on video transmission over wireless LANs", In Proceedings of the IEEE International Conference on Communications (ICC 2012), Ottawa, Canada, 10-15 June 2012.

[57] R. Suri, B. Hart, "Proposal for Addressing MRG Block Ack related comments", Doc. IEEE 802.11-10/1179r0, September 2009.

[58] J. Miroll, Z. Li, T. Herfet, "Wireless feedback cancellation for leader-based MAC layer multicast protocols: Measurement and simulation results on the feasibility of leader-based MAC protocols using feedback cancellation on the 802.11aa wireless multicast network", In Proceedings of the IEEE 14th International Symposium on Consumer Electronics (ISCE), pp. 1-6, Braunschweig, Germany, 7-10 June 2010.

[59] M.A. Santos, J. Villalon, L. Orozco-Barbosa, "Multicast Collision Free (MCF) mechanism over IEEE 802.11 WLANs", In Proceedings of the 3rd Joint IFIP. Wireless and Mobile Networking Conference (WMNC), pp. 1-6, Budapest, Hungary, 13-15 October 2010.

[60] “ISM band – technical definition”, YourDictionary, [Online], Available: http://computer.yourdictionary.com/ism-band (Last accessed: April 2012).

[61] F. Yue, G. Daqing, A.B. McDonald, Z. Jinyun, “A two-level carrier sensing mechanism for overlapping BSS problem in WLAN”, In Proceedings of the 14th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN), Crete, Greece, 18 September 2005.

[62] H. Bo, J. Lusheng, L. Seungjoon, R.R. Miller, B. Bhattacharjee, “Channel access throttling for overlapping BSS management”, In Proceedings of the IEEE International Conference on Communications (ICC), pp. 1-6, Dresden, Germany, 14-18 June 2009.

[63] K. Heck, “Wireless LAN performance in overlapping cells”, In Proceedings of the 58th IEEE Vehicular Technology Conference (VTC), vol. 5, pp. 2895-2900, 6-9 October 2003.

[64] W. Gang, S. Sathyanarayana, C. Tzi-cker, “Implementation of dynamic channel switching on IEEE 802.11-based wireless mesh networks”, In Proceedings of the 4th Annual International Conference on Wireless Internet (WICON), Maui, USA, 17-19 November 2008.

[65] T. Tandai, K. Toshimitsu, T. Sakamoto, “Interferential packet detection scheme for a solution to overlapping BSS issues in IEEE 802.11 WLANs”, In Proceedings of the IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1-6, Helsinki, Finland, 11-14 September 2006.

[66] D.D. Vergados, D.J. Vergados, “Synchronization of multiple access points in the IEEE 802.11 point coordination functions”, In Proceedings of the IEEE 60th Vehicular Technology Conference, vol. 2, pp. 1073-1077, 26-29 September 2004.

[67] Y. Asai, T. Ichikawa, R. Kudo, K. Ishihara, T. Murakami, Y. Takatori, M. Mizoguchi, “Interference management using beamforming technique in OBSS environment”, Doc. IEEE 802.11-10/0585r2, May 2010.

[68] Y. Utsunomiya, T. Tandai, T. Adachi, M. Takagi, “A MAC protocol for coexistence between 20/40 MHz STAs for high throughput WLAN”, In Proceedings of the IEEE 63th Vehicular Technology Conference (VTC), vol. 3, pp. 1136-1140, Melbourne, Australia, 7-10 May 2006.

[69] G. Smith, “Overlapping BSS analysis of channel requirements”, Doc. IEEE 802.11-08/1470-04-00aa, February 2009.

[70] IEEE P802.11aa/D9.0, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 2: MAC Enhancements for Robust Audio Video Streaming, January 2012.

[71] Z. Dongmei, “Throughput fairness in infrastructure-based IEEE 802.11 mesh networks”, IEEE Transactions on Vehicular Technology, vol. 56, issue 5, pp. 3210-3219, September 2007.

[72] M.M. Siddique, B.L. Wenning, A. Timm-Giel, C. Gorg, M. Muhleisen, “Generic spectrum sharing method applied to IEEE 802.11e WLANs”, In Proceedings of the 6th Advanced International Conference on Telecommunications (AICT), pp. 57-63, Barcelona, Spain, 9-15 May 2010.

[73] K. Yano, S. Tsukamoto, M. Taromaru, M. Ueba, “Area throughput enhancement of OFDM-based wireless LAN in OBSS environment by physical header modification and adaptive array antenna”, In Proceedings of the IEEE 20th International Symposium on Personal, Indoor and Mobile Communications (PIMRC), pp. 3059-3063, Tokyo, Japan, 13-16 September 2009.