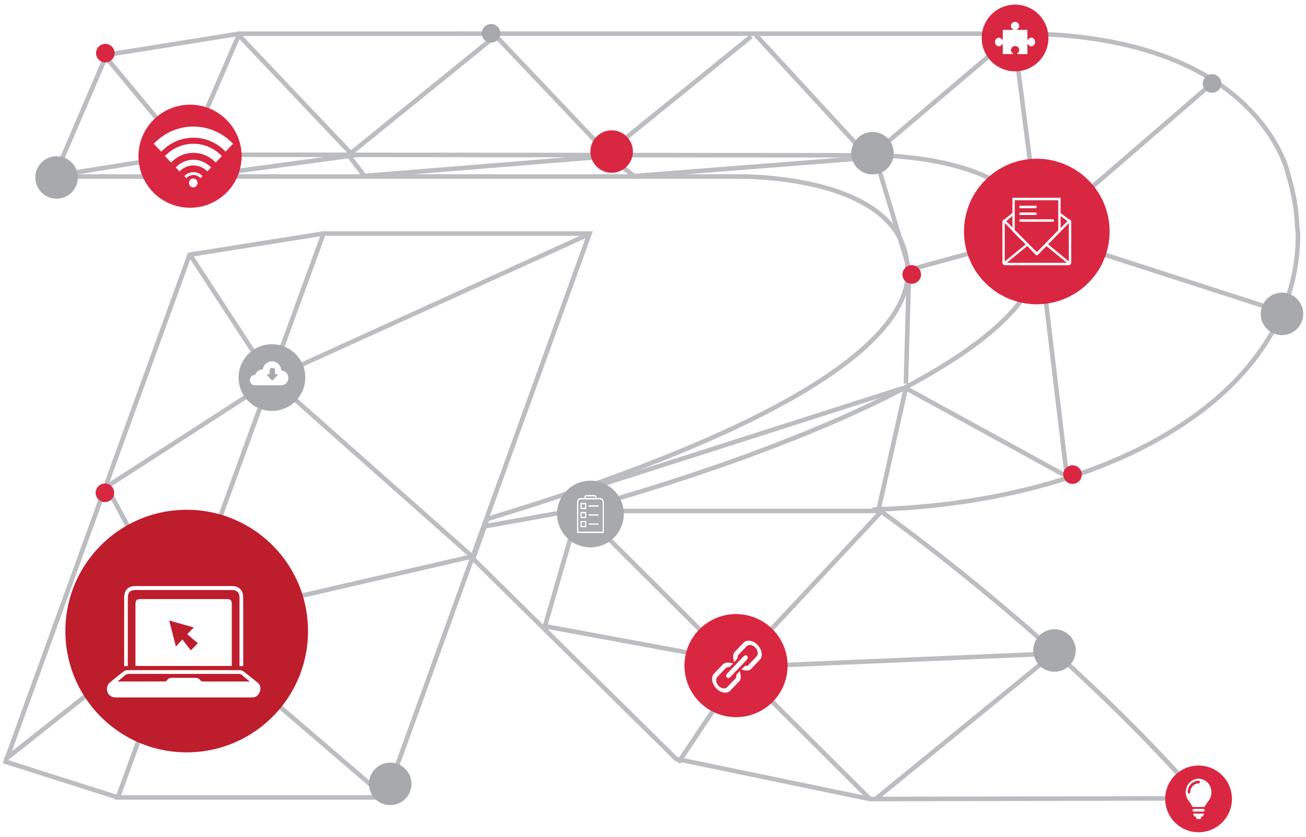
Ruijie Wireless LAN

White Paper



Contents

Introduction 4

Concepts 4

802.11 WLAN Fundamentals 5

IEEE 802 Network Technology Family 5

IEEE 802.11 Network Architecture 6

Wireless Standards 7

Transmission Standards 7

Non-transmission Standards 8

Standard Summary 10

802.11 MAC Frame 11

Basic Format 11

Data Frame 16

Control Frame 17

ACK 19

Management Frame 20

Frame Transmission, Association Status, and Identity Authentication Status 26

802.11 MAC Functions 27

Scanning, Authentication, and Association 27

DCF 29

Fragmentation and Reassembly 35

Retransmission 36

Synchronization 36

Multi-rate Support 38

Energy Saving Management 39

Frame Processing and Bridging 40

802.11n MAC Frame Extension 41

Format Extension 41

HT Control Field 41

Contents

Frame Type Extension.....42
Aggregate MPDU 44

802.11n MAC Function Extension 44
DCF Function 44
A-MSDU 45
A-MPDU 45
Block Acknowledgement.....45
Spatial Multiplexing Power Save 47
Protection Mechanism.....47
Reverse Direction Protocol.....47
Power Saving Multi-Poll.....48
Beamforming 49
Phase Coexistence Operation.....49
Space Time Block Coding 50

Introduction

A Wireless Local Area Network (WLAN) is a network system that applies wireless communication technologies to connect computer devices and implement mutual communication and resource sharing among the computer devices. The nature of WLANs is to connect computers to a network wirelessly rather than by using communication cables, thereby making network building and STA mobility more flexible.

The first milestone in the WLAN history is the release of IEEE 802.11 in June 1997. Though IEEE 802.11 did not bring about network revolution at that time, the "point-to-multipoint access" and "point-to-point relay" work modes proposed in 802.11 provide an efficient and high-speed solution to replace wired networks. It lays a foundation for continuous development of wireless network technologies and substantially contributes to later unified Wi-Fi 802.11b.

The release of 802.11b in September 1999 marks the beginning of the wireless era. From January 9, 2003 on which Intel formally announced to release the wireless mobile technology brand named Intel Centrino Mobile Technology to the current time, IEEE 802.11b has become the unified standard for WLANs. It provides faster and more stable access and features low costs. Therefore, it is widely applied in homes and enterprises. The greatest disadvantage of IEEE 802.11b, however, lies in that it is incapable of transmitting large-capacity data. IEEE 802.11a that provides faster transmission speed emerges accordingly. Nevertheless, IEEE 802.11a serves only as a supplement to 802.11b because of its innate shortcomings. 802.11g that combines 802.11b and 802.11a provides a perfect solution for the WLAN application. Currently, Intel formally launched the 802.11a/b/g WLAN chips on August 26, 2004. 802.11i, providing a supplement in security and authorization, was formally released in 2004. 802.11n improves the WLAN bandwidth surprisingly. 802.11n was released in 2009. WLAN products in the market show that the 802.11n is compatible with 802.11g.

Concepts

WLAN: a Local Area Network (LAN) that applies wireless communication technologies to connect computer devices and implement mutual communication and resource sharing among the computer devices. WLANs are characterized by flexible building, ease of access, support for multiple types of STAs, and flexible STA mobility. Currently, the mainstream data transmission rate can reach up to 54 Mbps.

Wi-Fi: Wireless Fidelity. Wi-Fi authentication is a type of authentication conducted on Wi-Fi-compliant products in the WLAN field. The Wi-Fi standard is formulated and revised by the Wi-Fi Alliance (WFA). Products that pass Wi-Fi authentication can be used in WLANs and can be compatible with other Wi-Fi authenticated products. The common Wi-Fi authentication standards include IEEE 802.11b, IEEE 802.11a, and IEEE 802.11g.

AP: Access Point, used to connect to a wired Ethernet and transmit wireless signals. STAs can communicate with an AP and exchange data with the AP via a wireless network adapter.

STA: devices providing interfaces that comply with the 802.11 MAC and PHY protocols.

WEP: Wired Equivalent Protocol, a security encryption protocol for IEEE 802.11 authentication. When WEP is enabled, data to be transmitted is encrypted, to ensure the security and integrity of data transmission in WLANs.

BSS: Basic Service Set, a basic component of the 802.11 network. Each BSS contains a group of logically associated STAs.

BSSID: Basic Service Set Identifier, an identifier common to the headers of frames from all STAs in the same BSS. This identifier contains 48 bits.

IBSS: Independent Basic Service Set, an 802.11 network without APs. It is also called a temporary or ad hoc network.

DS: Distributed System, a service that connects APs in series. Logically, it includes a wired backbone network and the bridging function.

CF: Contention Free, a service that does not use contention as the media access mode.

CF is a service provided by the Point Coordination Function (PCF).

CFP: Contention-Free Period. 802.11 allows some contention-based media access modes while providing the contention-free service. The media access period controlled by the central mechanism is called contention-free period.

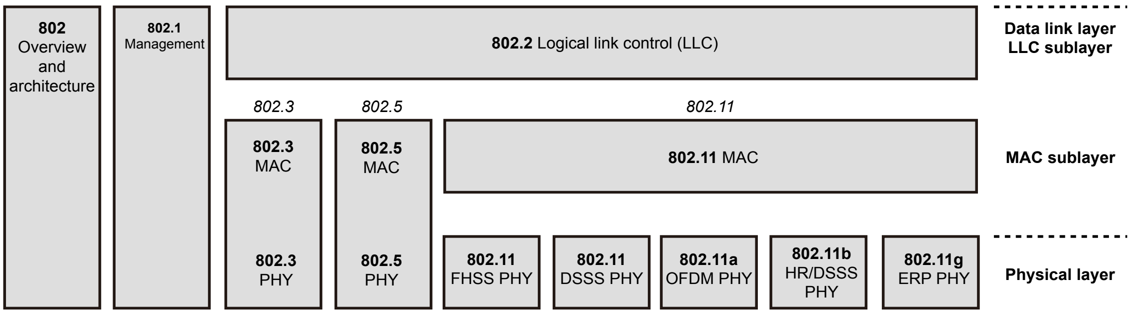
DCF: Distributed Coordination Function, rules for accessing wireless media in the contention-based service of 802.11 networks. In the case of contention, the DCF uses exponential backoff, access delay, and frame acknowledgement as the judgment basis for media access.

PCF: Point Coordination Function, a group of rules provided by APs and used to coordinate all parties' access to the transmission media.

802.11 WLAN Fundamentals

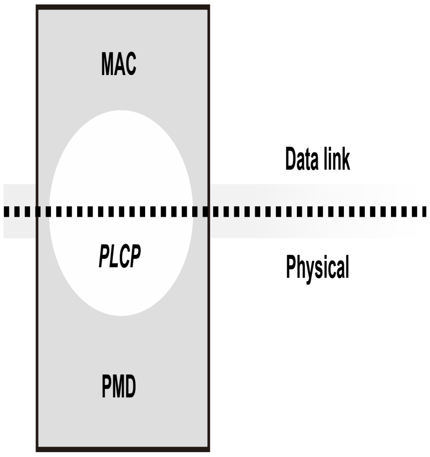
• IEEE 802 Network Technology Family

Figure 1



The 802.11 series standards mainly involve the data link layer and PHY layer.

Figure 2



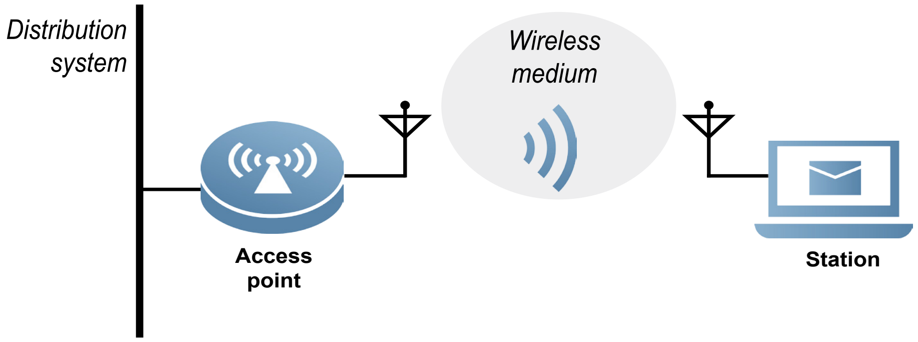
The Data Link Control (DLC) layer of 802.11 is composed of two sublayers: Logic Link Control (LLC) sublayer and Media Access Control (MAC) sublayer. 802.11 uses the LLC layer the same as that of 802.2 and the 48-bit MAC address defined in the 802 protocol, which facilitates the bridging between wired networks and wireless networks. MAC addresses, however, are unique only in WLANs.

The PHY layer of 802.11 consists of two sublayers: Physical Layer Convergence Procedure (PLCP) sublayer and Physical Medium Dependent (PMD) sublayer. The PLCP sublayer converts the MAC Protocol Data Units (MPDUs) of the MAC sublayer into a frame format suitable for transmission over wireless media. The PMD sublayer defines the features of and methods for transmitting and receiving data via the wireless media.

• IEEE 802.11 Network Architecture

802.11 defines two types of devices: One type is STAs, which can be 802.11 PCMCIA cards, PCI cards, or mobile phones. The other type is APs, which serve as a bridge between wireless networks and wired networks. An AP is usually composed of a wireless output interface and a wired network interface (802.3 interface). The bridging software complies with the 802.1d bridge protocol.

Figure 3



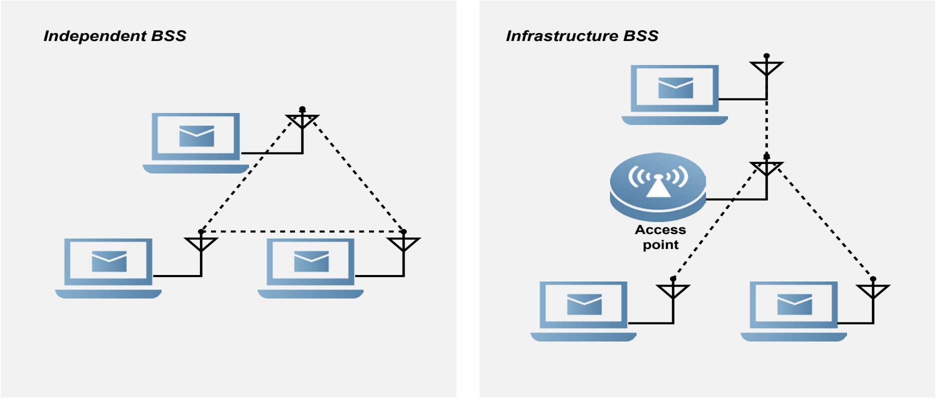
The basic unit of a WLAN is the Basic Service Set (BSS), which provides a coverage area to make sites in the BSS keep connected. The BSS supports two topological structures:

* **Independent Basic Service Set (IBSS): also called as hoc network. It is an independent BSS without hubs. A minimum IBSS contains at least two STAs, which can directly communicate with each other. This operation mode supports flexible networking mechanism and network pre-planning is not required.**

* **Infrastructure BSS: A STA must associate with an AP to obtain network services.**

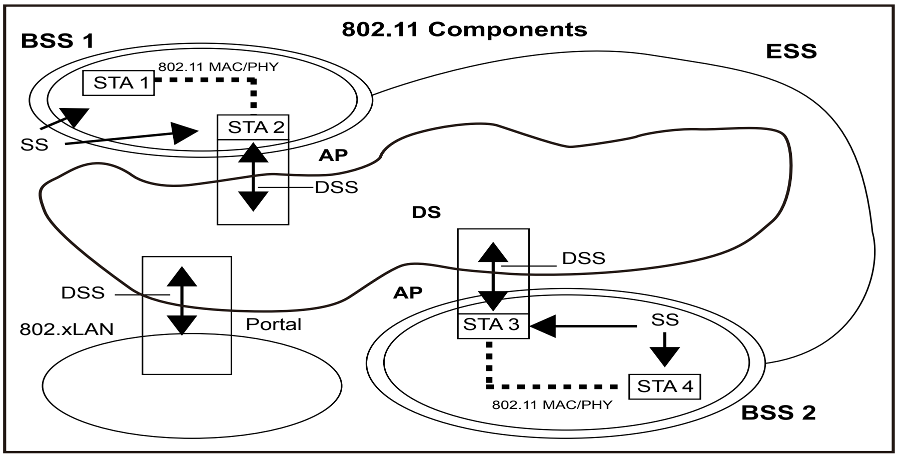
Note: The types of packets vary with the two topological structures.

Figure 4



Multiple BSSs can compose one Extended Service Set (ESS) network. STAs in an ESS network can communicate with each other only through APs. The system that connects multiple APs (BSS component) is called Distributed System (DS).

Figure 5



Wireless Standards

• Transmission Standards

Transmission standards include 802.11 (2 Mbps/2.4 GHz), 802.11a (54 Mbps/5–6 GHz), 802.11b (11 Mbps/2.4 GHz), 802.11g (54 Mbps/2.4 GHz), and 802.11n (500 Mbps/2.4 GHz/5 GHz).

1. 802.11

802.11, released in November 1997, is the 2nd-generation WLAN standard. Relevant products were launched in 1998. This standard adopts the Direct Sequence Spread Spectrum (DSSS) modulation technology, and implements the data transmission rates of 1 Mbps and 2 Mbps by using the Binary Phase Shift Keying (BPSK) and Quadrature Phase Shift Keying (QPSK) technologies respectively. The 1st-generation WLAN refers to the wave regulations released by the Federal Communication Commission (FCC) in 1995 and subsequently released products.

2. 802.11b

802.11b (physical layer specifications for the 2.4 GHz band) was released in 1999 and is the 3rd-generation WLAN standard. 802.11b products adopt the Complementary Code Keying (CCK) modulation technology, and raise the data transmission rates to 5.5 Mbps and 11 Mbps by using the BPSK and QPSK technologies respectively.

3. 802.11a

802.11a (physical layer specifications for the 5 GHz band) was released in 1999 and is the 4th-generation WLAN standard. It adopts a different modulation technology, Orthogonal Frequency Division Multiplexing (OFDM), and increases the data transmission rate to 54 Mbps by using the 64 Quadrature Amplitude Modulation (QAM). 802.11a is applicable to the 5 GHz band. In comparison with 802.11g, 802.11a is disadvantageous in its high costs, poor penetration, and small signal coverage and advantageous in its high bandwidth, immunity to interference, and less hacker attacks.

4. 802.11g

802.11g was released in 2002 and is the 4th-generation WLAN standard. It is an amendment to 802.11b. It enhances the performance and application of 802.11b-compatible networks by raising the data rate. It is basically the 802.11a modulation solution working in the 2.4 GHz band. To support the interoperability between the 2.4 GHz CCK/DSSS and the OFDM modem, IEEE adopts the protection mechanism based on the Request To Send/Clear To Send (RTS/CTS) signals. The current Wi-Fi solution supports 802.11a, 802.11b, and 802.11g and is called multi-mode 802.11a/b/g.

5. 802.11n

Released in 2009, 802.11n is based on Multiple-Input Multiple-Output (MIMO)-OFDM. This standard can be compatible with existing Wi-Fi equipment in 5 GHz and 2.4 GHz bands in forcible mode, and the transmission rate exceeds 500 Mbps. 802.11n is mainly used in two types of applications: applications that require high-speed data transmission and excellent Quality of Service (QoS); and applications that provide the performance equivalent to wired networks in high-density environments such as large enterprises or communities.

The MIMO can create more "air paths" for data to be transmitted, thereby improving the data throughput in a single channel. It adopts multiple transmit and receive antennas, to enable each path to transmit a group of different data at the same frequency.

This standard adopts the 40 MHz channel in the 5 GHz band and also supports the 20 MHz channel and 2.4 GHz band. The 40 MHz channel is composed of two 20 MHz adjacent channels. 802.11n utilizes the unutilized quadrant band between the two channels to increase the WLAN data transmission rate from 54 Mbps to about 125 Mbps.

Note 1: Comparison between 802.11g and 802.11a

802.11g outperforms 802.11a with the 54 Mbps high speed and downward compatibility with 802.11b. In bandwidth, 802.11a is superior to 802.11g. 802.11a supports 12 non-overlapped channels and the supported bandwidth is 648 Mbps (54 Mbps x 12). 802.11g supports only three non-overlapped channels (Channels 1, 6, and 11), and the supported bandwidth is 162 Mbps (54 Mbps x 3). Likewise, the total bandwidth supported by 802.11b is 33 Mbps (11 Mbps x 3). Therefore, 802.11g supports only three APs in the same area. 802.11g is vulnerable to interference from other APs, microwave ovens, and radio telephones when working in 2.4 GHz band. 802.11g provides a smaller coverage scope than 802.11a.

Actually, the OFDM technology was proposed to be applied in 802.11b in 1999 but the FCC prohibited the application of OFDM in the 2.4 GHz band. The 802.11b had to use the CCK module design. It was not until May 2001 that FCC cancelled the prohibition. Then, OFDM fully displays its capability in 802.11g, and implements high-speed WLAN transmission in the 2.4 GHz band.

Note 2: Current status of 802.11n

The 802.11n proposal is divided into two groups. One is led by Atheros and advocates use of the 40 MHz bandwidth. Intel, Panasonic, Philips, and Sony are supporters of this group, and they call themselves TGnSynch. The other group, called WWiSE group, is led by Airgo and stick to the 20 MHz bandwidth. Broadcom, Conexant, Mitsubishi, Motorola, STMicroelectronics, and Texas Instruments are supporters of this group.

• Non-transmission Standards

1. 802.11e

This standard adds the QoS function at the MAC physical layer, and supports multimedia in existing wireless standards. It helps wireless networks implement the transmission of multimedia services such as voice, audio, and video services.

2. 802.11h

To eliminate mutual interference with other systems, 802.11h introduces two key technologies: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). It prevents 802.11a wireless systems from interfering with the broadband technology used in radar and other similar systems, thereby ensuring smooth wireless communication.

3. 802.11f

802.11f implements roaming among different APs (different equipment providers) in the same network segment. It does not support roaming among different WLAN network segments. 802.11f specifies the communication process and exchanged information among APs during Mobile Terminal (MT) roaming. The Inter-Access Point Protocol (IAPP) defined in 802.11f stipulates the information to be exchanged among APs and between an AP and a RADIUS server at the IP layer. When an MT switches from one BSS to another, the MT sends a "reconnection" request. The new AP obtains the IP address and access key of the old AP from the RADIUS server, and interacts with the old AP to obtain the authentication information, temporary IP address, MAC address, and other information of the MT. The new AP instructs the Layer-2 network device (for example, Ethernet switch) in the DS to modify the forwarding table, so as to complete one roaming process. If the MT moves to the coverage of an AP and sends a "connection" request rather than a "reconnection" request, the AP further broadcasts the MT information in the subnet when it establishes a connection with the MT. Each AP in the subnet checks the MT information with the stored connection information. If an AP has a connection to the MT, the AP deletes the connection. Meanwhile, the AP instructs the Layer-2 network device to modify the forwarding table.

4. 802.11r

802.11r formulated by the IEEE aims at reducing the authentication time required during roaming, so as to support real-time applications such as the voice service. Re-authentication is required in the new 802.11i security protocol. Moreover, authentication is also needed if the Remote Authentication Dial In User Service (RADIUS) server is used. Both will lead to a delay of hundreds of milliseconds during authentication. The delay needs to be controlled within 20 milliseconds during handovers in the voice communication. Therefore, the 802.11r work group is working on a faster algorithm and pre-authentication method to minimize the authentication time. In this way, users do not need re-authentication when associating with a new AP, to prevent call interruption. The problem to be solved by 802.11r is how to ensure that authentication and security policies are not affected while a STA is rapidly handed over from one AP to another.

5. 802.11i

In allusion to the security deficiency in the Wired Equivalent Privacy (WEP) protocol, 802.11i introduces the Temporal Key Integrity Protocol (TKIP) in encryption processing and changes fixed keys to dynamic keys. Though 802.11i still uses the RC4 algorithm, it is more advanced than WEP using fixed keys.

In addition to key management, 802.11i uses the user audit mechanism with the Extensible Authentication Protocol (EAP) as the core. This mechanism audits the IDs of access users through the server, preventing unauthorized access of hackers to a certain extent.

802.11i also defines the Counter-Mode/CBC-MAC Protocol (CCMP) based on the Advanced Encryption Standard (AES) algorithm. Compared with the current Wi-Fi Protected Access (WPA) security standard, the AES provides higher security and supports 128-bit, 192-bit, and 256-bit keys.

6. 802.11k

802.11k (Radio Resource Management) improves operations on APs and STAs as well as the detection of environmental data, thereby boosting the WLAN operation and management efficiency. In general, wireless devices associate with the APs with the strongest transmit signals. As a result, some APs are overloaded while some other APs are underloaded, reducing the overall service quality. 802.11k enables network management software to detect the AP load and make STAs associate with unutilized APs. The unutilized APs can provide a high throughput in spite of their relatively weak signal strength.

802.11k implements various functions related to roaming decision, RF channel knowledge, channel payload, hidden node, STA statistics, beacon, histogram, and TPC. APs or WLAN switches provide site reports for STAs to improve roaming decisions. 802.11k first defines beacon requests. Based on a beacon request, an AP requests a STA to access a specific channel and report other APs' beacons obtained by the AP via listening. The AP collects data, and the AP or WLAN switch analyzes beacon information to find out specific requirements, for example, the service type and encryption type supported by each AP, and the strength of beacon signals received by the STA. Afterwards, the switch or AP generates an AP sequence list, including APs from the one providing the optimal service to the one providing the worst service. This sequence list is called site report. .

Currently, APs and STAs cannot share channel information. When 802.11k is adopted, an AP creates a noise histogram for a STA and the noise histogram displays all non-802.11k energy in the channel of the STA. An AP can also request a related channel payload or the time length for using a channel within the specified time period. Then, the AP or WLAN switch will learn whether the interference or information amount is heavy in a channel, to determine whether to use the channel for WLAN communication.

Hidden nodes refer to STAs or APs that cannot be detected by other STAs or APs. In an 802.11 system, signals are listened before radio signals are transmitted, to prevent conflicts. In a case with hidden nodes, multiple nodes may transmit signals simultaneously, which results in interference and reduces WLAN performance. After 802.11k is adopted, a STA tracks hidden nodes and an AP queries the STAs relative to the hidden nodes. The queried information shows the STAs at the network edge to the AP. Based on the information, the AP can guide STAs to APs that could provide better service for the STAs.

802.11 STA statistics are applicable only to AP statistics or WLAN switch maintenance. The current WLAN tracking items include data packet counting, and statistics on transmitted and received data packets. When 802.11k is used, APs and WLAN switches can query all STAs, to obtain their statistical reports. The WLAN system provides a more comprehensive network performance view based on the data queried by the APs and switches.

Extended TPC application: 802.11h defines TCP to meet requirements for frequency management in the 5 GHz band. When 802.11k is adopted, the TPC application is extended to other management scopes and bands, to reduce interference and power consumption and control the spread scope of radio waves. 802.11k helps network administrators better build WLANs. The improvement in the spread control of radio waves is conductive to network management, implements reliable network access even during user roaming, and ensures smooth network connections. In addition, the WLAN utilization improvement also raises the service efficiency.

7. 802.11s

802.11s connects APs to compose a mesh backbone communications network. It aims to make APs serve as wireless data routers. Not all APs need to be directly connected to a wired LAN. Similar to Internet nodes, 802.11s-compliant APs forward traffic to adjacent APs and conduct a series of multi-hop transmission. This mesh network innately has high reliability because it automatically bypasses faulty nodes and automatically makes adjustments to balance traffic load and optimize the performance.

• Standard Summary

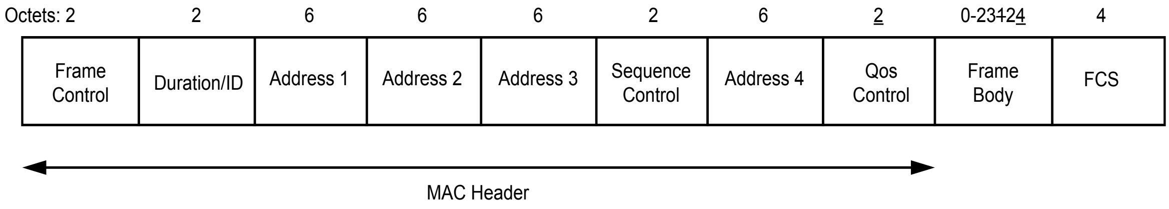
Standard	Description	Release Time
802.11a	Transmission standard: 54 Mbps, 5 GHz	1999
802.11b	Transmission standard: 11 Mbps, 2.4 GHz	1999
802.11d	Multicountry roaming	2001
802.11e	QoS	Summer in 2005
802.11f	AP layer-2 roaming	2003
802.11g	Transmission standard: 54 Mbps, 2.4 GHz	June 2003
802.11h	Dynamic frequency selection and transmission power control	September 2003
802.11i	Security	2004
802.11j	Transmission standard: 4.9 GHz to 5.0 GHz (Japan)	2004
802.11k	Radio resource management	End of 2002

Standard	Description	Release Time
802.11n	Transmission standard: 100 Mbps, 5GHz	2008
802.11r	Fast roaming	2006
802.11s	Extended service set for mesh networking	2006
802.16d	Fixed WMAN	2004
802.16e	Mobile WMAN	Second half of 2005
802.1x	Security authentication	2001

802.11 MAC Frame

• Basic Format

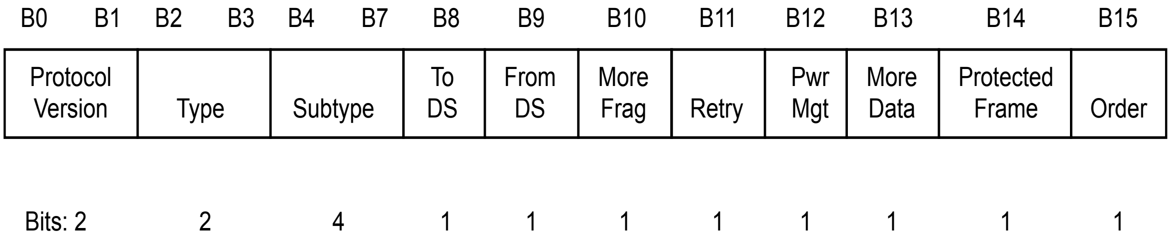
Figure 6



Octets: 2	2	6	6	6	2	6	2	0-23~~1~~24	4
Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Qos Control	Frame Body	FCS

Frame Control Field

Figure 7



B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	Protected Frame	Order
Bits: 2	2	4	1	1	1	1	1	1	1	1

The **Frame Control** field occupies two bytes.

Protocol Version displays the MAC version used by this frame. There is only one version numbered 0 for 802.11 MAC frames.

Type and **Subtype** indicate the frame type.

Type Value (B2 and B3)	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110–1111	Reserved
01	Control	0000-0111	Reserved
01	Control	1000	Block Ack Request (BlockAckReq)
01	Control	1001	Block Ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data

Type Value (B2 and B3)	Type Description	Subtype Value	
10	Data	1001	QoS Data + CF-Ack
10	Data	1010	QoS Data + CF-Poll
10	Data	1011	QoS Data + CF-Ack + CF-Poll
10	Data	1100	QoS Null (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data)
10	Data	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserved	0000–1111	Reserved

The **To DS** and **From DS** bits indicate whether the destination of the frame is a DS.

	To DS=0	To DS=1
From DS=0	All management and control frames Data frames in the IBSS	Data frames sent by STAs in the BSS
From DS=1	Data frames received by STAs in the BSS	Data frames in the wireless bridge

The **More Frag** bit plays a similar role as the **More fragments (MF)** bit in IP. If upper-layer encapsulated packets are fragmented according to the MAC protocol, this bit is set to 1 in all fragments except the last one.

The value **1** of the **Retry** bit indicates that the current frame is a retransmitted frame.

The value **1** of the **Pwr Mgt** bit indicates that a STA enters the Power Save (PS) mode after the current frame is transmitted. The value **0** indicates that the STA keeps staying in the awake state. This bit is always **0** for APs.

More Data indicates whether there is data to be transmitted to a STA in the sleep state. The value **1** indicates yes while the value **0** indicates no.

The value **1** of the **Protected Frame** bit indicates that the current frame is encrypted while the value **0** indicates the opposite.

The value **1** of the **Order** bit indicates the frame is transmitted in strict order.

Duration/ID Field

Figure 8

Bits 0-13	Bit 14	Bit 15	Usage
0-32 767		0	Duration value (in microseconds) within all frames other than PS-Poll frmes transmitted during the CP, and under HCF for frames transmitted during the CFP
0	0	1	Fixed value under point coordination function (PCF) within frames transmitted during the CFP
1-16 383	0	1	Reserved
0	1	1	Reserved
1-2007	1	1	AID in PS-Poll frames
2008-16 383	1	1	Reserved

The **Duration/ID** field has three functions:

When Bit 15 is set to **0**, the **Duration/ID** field is used to set the Network Allocation Vector (NAV), which indicates the estimated duration in microseconds for using media for the current transmission.

When Bit 14 is set to **0** and Bit 15 is set to **1**, the **Duration/ID** field indicates that the frame is transmitted in the contention-free period. Other bits are set to 0.

When both Bit 14 and Bit 15 are set to **1**, the **Duration/ID** field is used for the PS-Poll frame. A STA transmits the PS-Poll frame when it wakes up from the sleep state. Bits 0-13 are set to the Association ID (AID), which indicates the BSS to which the STA belongs.

Address Fields

Figure 9

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	Not used
To AP (infra.)	1	0	BSSID	SA	DA	Not used
From AP (infra.)	0	1	DA	BSSID	SA	Not used
WDS (bridge)	1	1	RA	TA	DA	SA

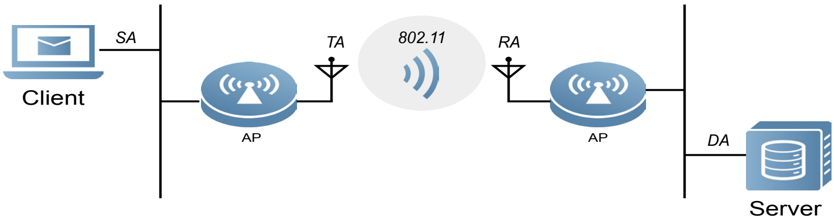
Address 1 indicates the receiver address. The BSSID must be checked when **Address 1** is a broadcast or multicast address. A STA responds only to broadcast or multicast packets from the same BSS as that of the STA.

Address 2 indicates the transmitter address.

Address 3 is used for filtering by APs and DSs.

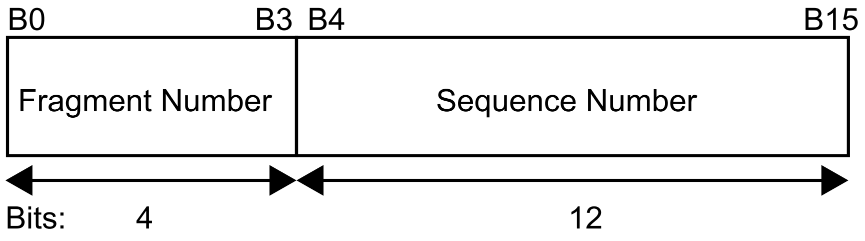
A Wireless Distributed System (WDS) uses four addresses, where RA and TA are AP addresses while SA and DA are STA addresses, as shown in the figure below.

Figure 10



Sequence Control Field

Figure 11



The **Sequence Control** field contains 4-bit **Fragment Number** and 12-bit **Sequence Number**. This field is used to reassemble frame fragments and discard duplicate frames.

QoS Control Field

Figure 12

Applicable frame (sub) types	Bits 0-3	Bit 4	Bits 5-6	Bit 7	Bits 8-15
QoS (+)CF-Poll frames sent by HC	TID	EOSP	Ack Policy	Reserved	TXOP Limit
QoS Data, QoS Null, and QoS Cata+CF-Ack frames sent by HC	TID	EOSP	Ack Policy	Reserved	AP PS Buffer State
QoS data frames sent by non-AP STAs	TID	0	Ack Policy	Reserved	TOXP Duration Requested
	TID	1	Ack Policy	Reserved	Queue Size

The **QoS Control** field is not described in this document.

Frame Body

Frame Body is used to transmit valid payloads among STAs.

The minimum length of **Frame Body** is 0.

The maximum length of **Frame Body** is the maximum length of the MAC Service Data Unit (MSDU) + Integrity Check Value (ICV) + Initialization Vector (IV). The maximum length of the MSDU is 2304 bytes.The length of ICV + IV is 8 bytes (used for WEP). Therefore, the maximum length of **Frame Body** is 2312 bytes.

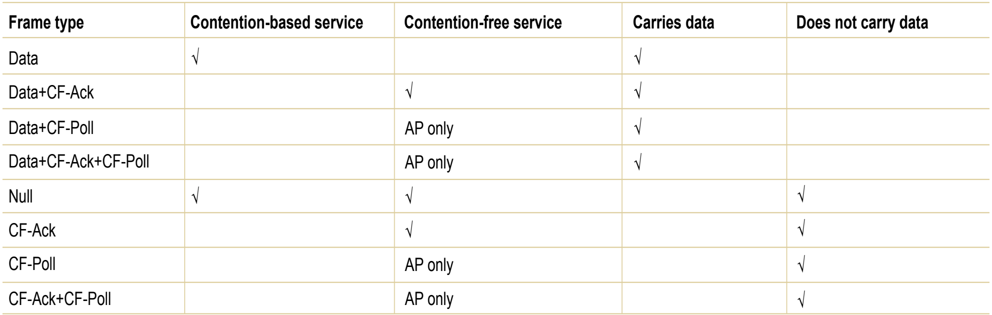
FCS

FCS is used to conduct the Cyclic Redundancy Check (CRC) on frames.

• Data Frame

Types

Figure 13



Frame type	Contention-based service	Contention-free service	Carries data	Does not carry data
Data	√		√	
Data+CF-Ack		√	√	
Data+CF-Poll		AP only	√	
Data+CF-Ack+CF-Poll		AP only	√	
Null	√	√		√
CF-Ack		√		√
CF-Poll		AP only		√
CF-Ack+CF-Poll		AP only		√

Some data frames are used for contention-based services and some other for contention-free services.

Duration Field

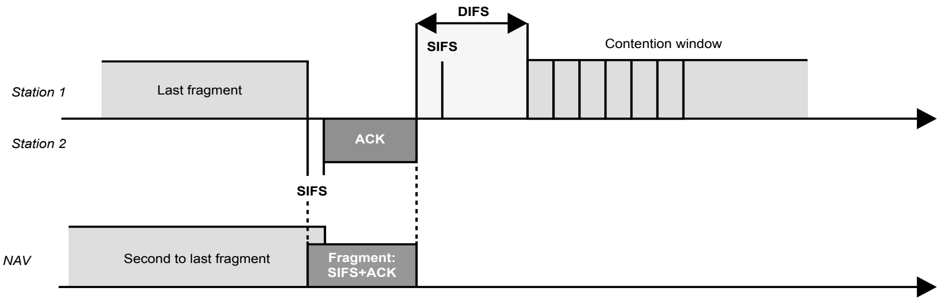
Set the **Duration** field of data frames according to the following rules:

1. **Duration** must be set to 32768 for any frames transmitted inside a CFP.

2. **Duration** must be set to 0 for broadcast or multicast frames.

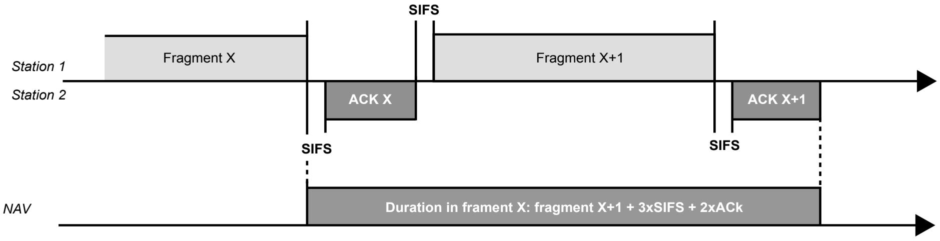
3. If **More Frag** in the **Frame Control** field of a data frame is **0**, it indicates that the frame has no other fragments. The frame is used to make a reservation for media use. In this case, **Duration** is set to one Short Inter-Frame Space (SIFS) plus one ACK.

Figure 14



4. If **More Frag** in the **Frame Control** field of a data frame is **1**, **Duration** is set to two ACKs plus three SIFSs and the time required by the next frame.

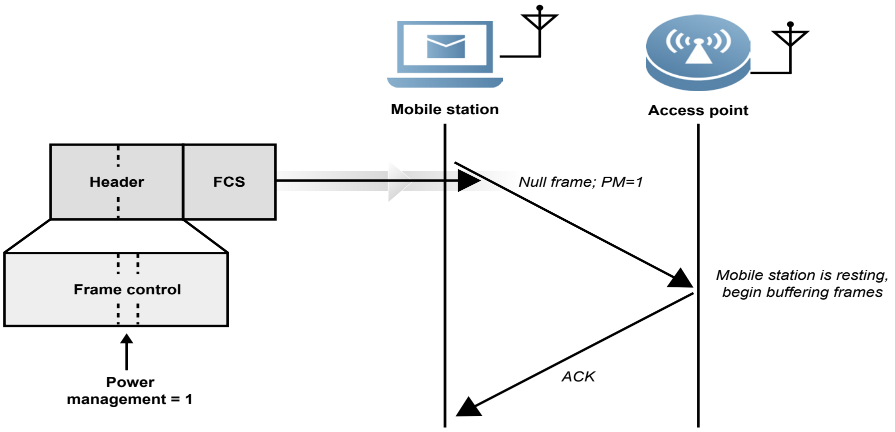
Figure 15



Null Frame

STAs use the Null frame to instruct APs to change the power save state.

Figure 16



• Control Frame

Frame Control Field

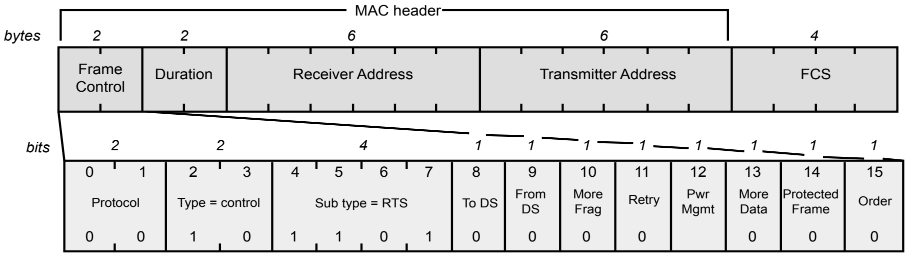
Figure 17

B0										B15
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	Protected Frame	Order
Protocol Version	Control	Subtype	0	0	0	0	Pwr Mgt	0	0	0
Bits : 2	2	4	1	1	1	1	1	1	1	1

The **To DS, From DS, More Frag, Retry, More Data, Protected Frame,** and **Order** bits of control frames must be set to 0.

RTS

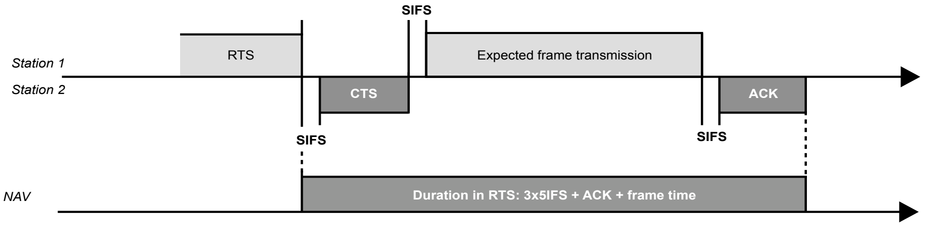
Figure 18



For large frames, the RTS frame is adopted to obtain the media control right, to prevent network performance deterioration caused by retransmission. The frame size is defined using the RTS threshold in the driver. Note that the RTS/CTS mechanism is applicable only to unicast frames, and is not available for multicast and broadcast frames.

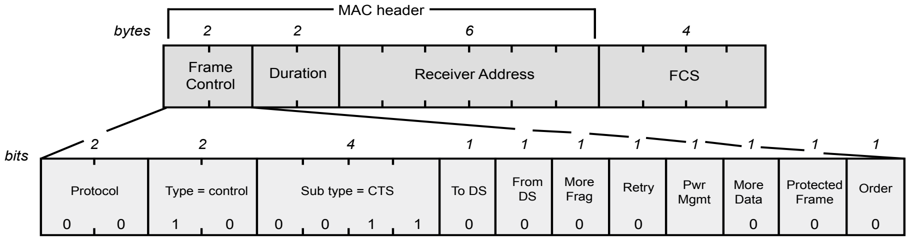
The **Duration** field of the RTS frame is set to three SIFSs, one CTS, ACK, and the time required for transmitting the first frame or frame fragment.

Figure 19


SIFS
Station 1
Station 2
RTS
CTS
Expected frame transmission
ACK
SIFS
SIFS
NAV
Duration in RTS: 3xSIFS + ACK + frame time

CTS

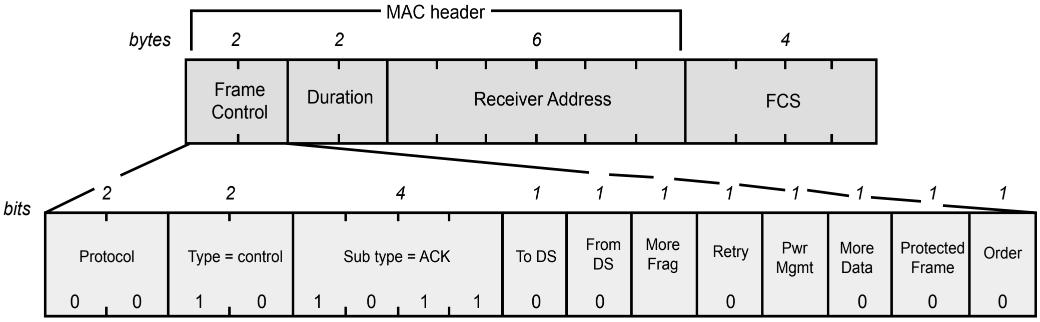
Figure 20



The CTS frame is used only to respond to RTS frames.

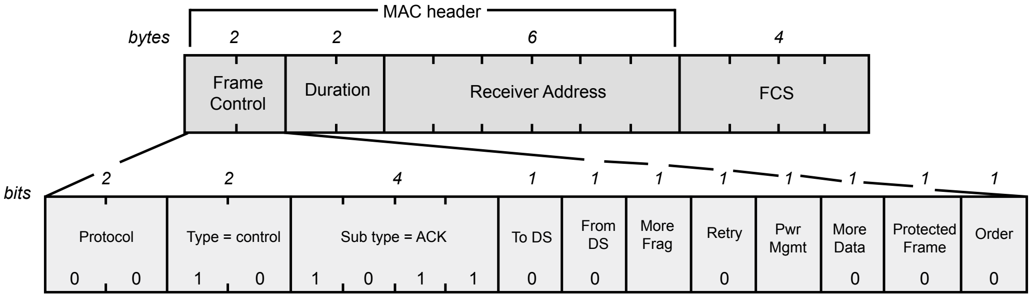
The **Duration** field of the CTS frame is set to the **Duration** value of the RTS frame minus the sum of one SIFS and the time required for transmitting the CTS frame.

Figure 21



- ACK

Figure 22

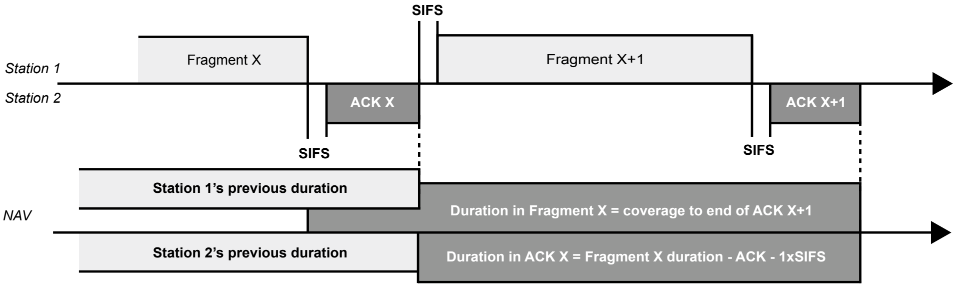


The ACK frame is used to respond to received frames.

If the value of the **More Frag** bit is **0**, it indicates that the data transmission is completed and **Duration** is set to 0.

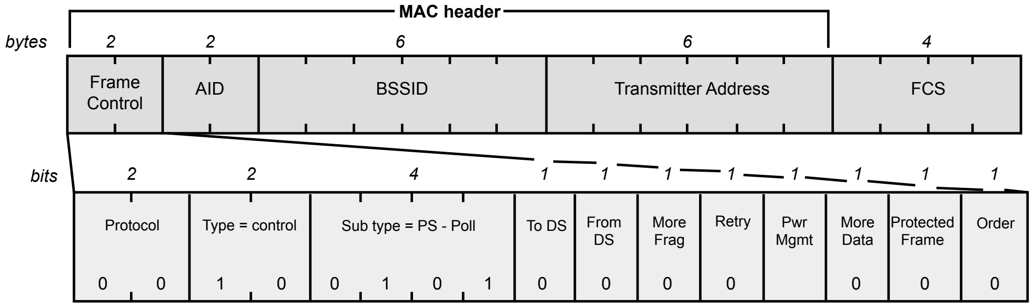
If the value of the **More Frag** bit is **1**, the value of **Duration** is calculated in a way similar to CTS calculation, that is, the Duration value in the received frames minus one SIFS and the time required for transmitting the ACK frame.

Figure 23


SIFS
Station 1
Station 2
Fragment X
Fragment X+1
ACK X
ACK X+1
SIFS
SIFS
Station 1's previous duration
Duration in Fragment X = coverage to end of ACK X+1
NAV
Station 2's previous duration
Duration in ACK X = Fragment X duration - ACK - 1xSIFS

PS-Poll

Figure 24



After waking up from the PS mode, a STA sends a PS-Poll frame to an AP to obtain a buffer frame.

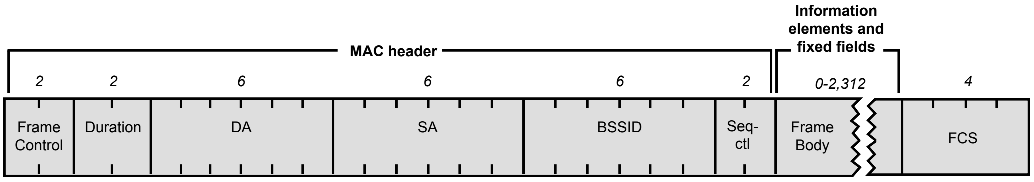
The PS-Poll frame does not contain the **Duration** field. All STAs that receive the PS-Poll frame update the NAV based on the SIFS plus the time required for transmitting the ACK frame, so that their responses will not conflict with the responses from APs.

• Management Frame

Management Frame

The MAC headers of management frames basically share the same structure and are irrelevant to the frame subcategory. Management frames use fixed fields or information elements to exchange information with other systems.

Figure 25



The **Frame Body** field of management frames contains fixed fields and an information element. The length of fixed fields is fixed while the information element is a variable-length data block.

The length and sequence of fixed fields are fixed, and therefore the fixed fields do not need to be defined with a header. Ten fixed fields are defined in the standards:

1. Authentication Algorithm Number

This field is used to distinguish whether the open system identity authentication or shared key identity authentication is adopted.

2. Authentication Transaction Sequence Number

This field is used to track the progress of identity authentication.

3. Beacon Interval

This field specifies the number of time units between Beacon signals.

4. Capability Information

This field advertises the network performance during beacon signal transmission.

5. Current AP Address

This field indicates the MAC address of the currently associated AP, and is used for association and re-association.

6. Listen Interval

This field is used to calculate the sleep time based on Beacon Interval. A STA wakes up periodically based on the listen interval, to listen to messages.

7. Association ID

An AID is assigned to facilitate control and management when a STA is associated with an AP.

8. Timestamp

This field is used to synchronize time of STAs in one BSS.

9. Reason Code

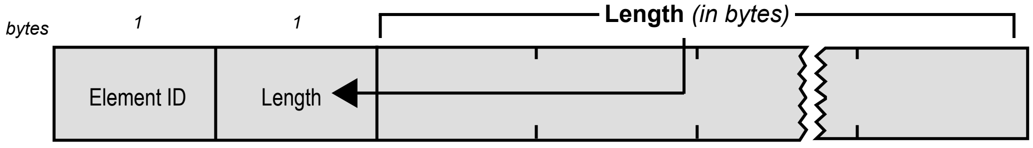
This field shows the reason for cancelling association and identity authentication.

10. Status Code

This field shows whether an operation succeeds or fails.

The information element is a variable-length component in management frames. The information element contains one Element ID, one **Length** field, and one variable-length field.

Figure 26



The table below lists the standard values of **Element ID**.

Figure 27

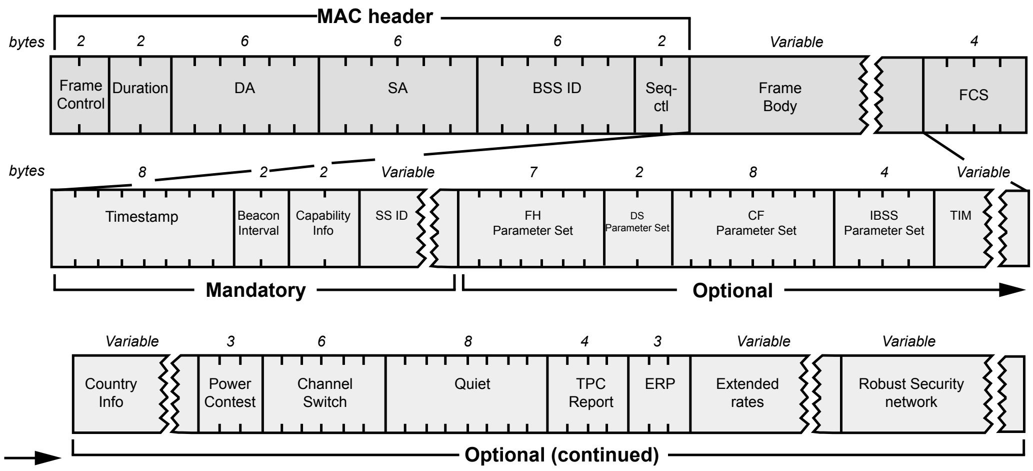
Element ID	Name
0	Service Set Identity (SSD)
1	Supported Rates
2	FH Parameter Set
3	DS Parameter Set
4	CF Parameter Set
5	Traffic Indication Map (TIM)
6	IBSS Parameter Set
7 (802.11d)	Country
8 (802.11d)	Hopping Pattern Parameters
9 (802.11d)	Hopping Pattern Table
10 (802.11d)	Request
11-15	Reserved; unused
16	Challenge text
17-31	Reserved[a] (formerly for challenge text extension, before 802.11 shared key authentication was discontinued)
32 (802.11h)	Power Constraint
33 (802.11h)	Power Capability
34 (802.11h)	Transmit Power Control (TPC) Request
35 (802.11h)	TPC Report
36 (802.11h)	Supported Channels
37 (802.11h)	Channel Switch Announcement
38 (802.11h)	Measurement Request
39 (802.11h)	Measurement Request
40 (802.11h)	Quiet
41 (802.11h)	IBSS DFS
42 (802.11h)	ERP information
43-49	Reserved
48 (802.11i)	Robust Security Network
50 (802.11g)	Extended Supported Rates
32-255	Reserved; unused
211[b]	Wi-Fi Protected Access

[a] 802.11 shared key authentication is no longer recommended, so it is unlikely that these fields will ever be used.

[b] This is used by WPA, and is not an official part 802.11. However, it is widely implemented, so I include it in the table.

Beacon Frame

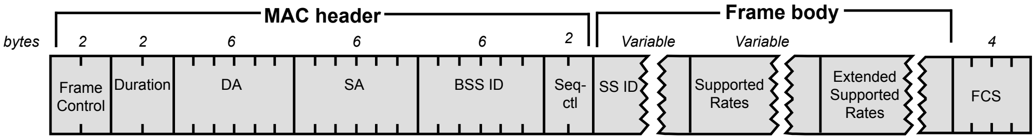
Figure 28



An AP transmits Beacon frames periodically to state the existence of a network. A STA knows the existence of a network based on the Beacon frames, and accordingly adjusts mandatory parameters for accessing the network.

Probe Request Frame

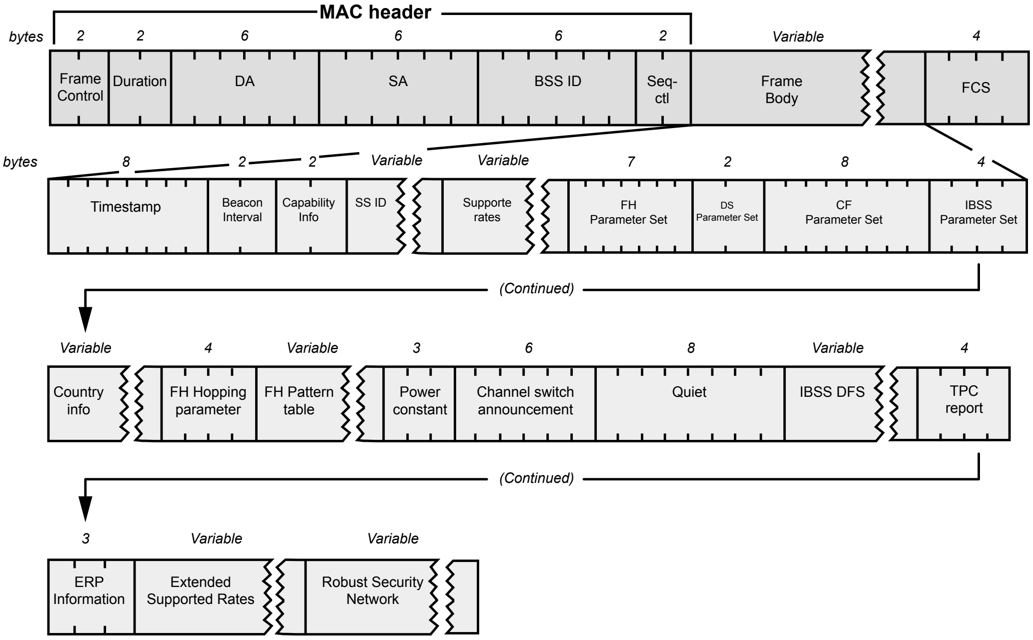
Figure 29



A STA sends a Probe Request to scan 802.11 networks in an area.

Probe Response Frame

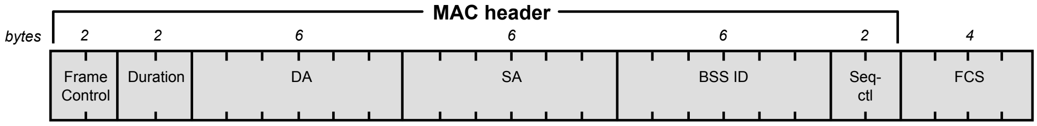
Figure 30



An AP responds to a Probe Request with a Probe Response. A Probe Response contains all parameters in the Beacon frame. The STA adjusts the parameters for accessing the network based on the Probe Response.

ATIM Frame

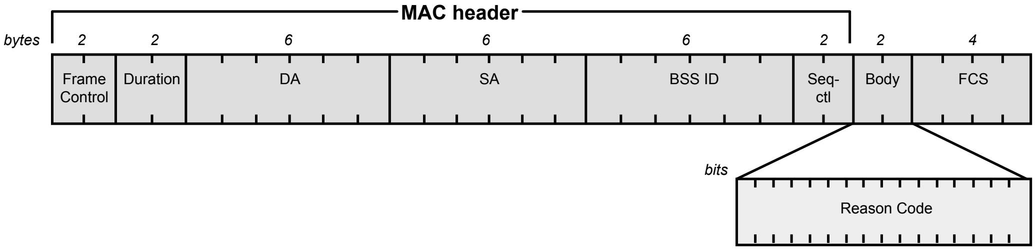
Figure 31



In an IBSS, ATIM frames are used to instruct a STA in the sleep state to receive buffered frames.

Disassociation and Deauthentication Frames

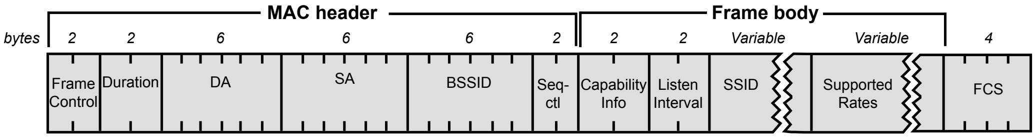
Figure 32



The Disassociation frame is used to cancel association while the Deauthentication frame is used to cancel identity authentication. The **Reason Code** field shows the cancellation reason.

Association Request Frame

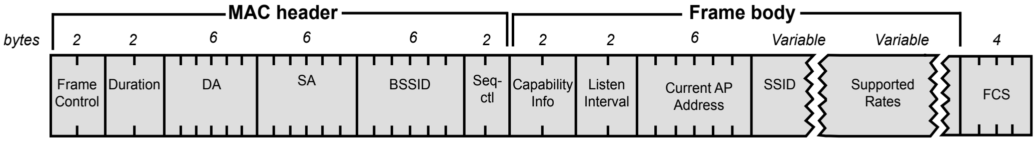
Figure 33



When a STA attempts to access a network, it sends an Association Request to an AP.

Reassociation Request Frame

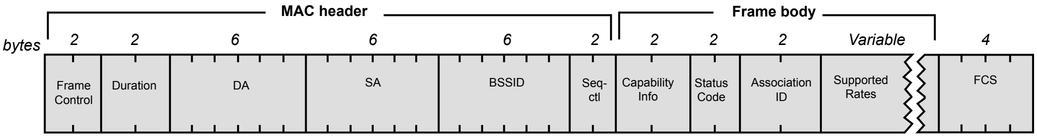
Figure 34



A STA needs reassociation when roaming among different APs.

Association Response and Reassociation Response Frames

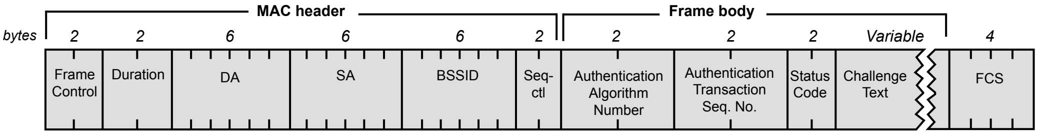
Figure 35



Association Response and Reassociation Response are returned by APs to STAs.

Authentication Frame

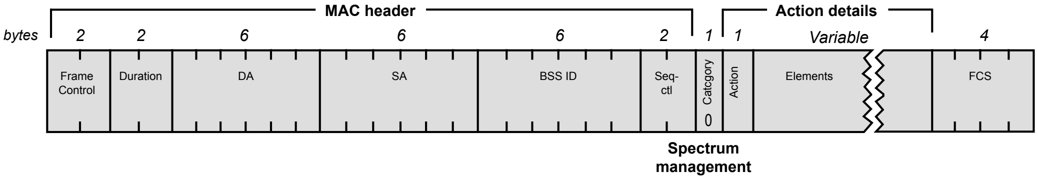
Figure 36



The Authentication frame is used for shared key identity authentication.

Action Frame

Figure 37



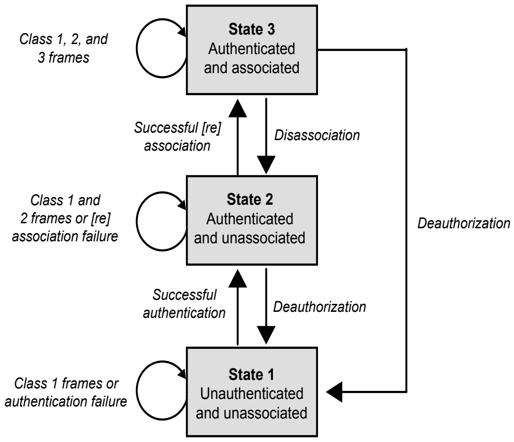
The Action frame is used to request a STA to take necessary actions.

Category indicates the category, for example, **0** indicates spectrum management.

Action details are specified by the **Action** and **Elements** fields.

• Frame Transmission, Association Status, and Identity Authentication Status

Figure 38


Class 1, 2, and 3 frames
State 3
Authenticated and associated
Successful [re] association
Disassociation
Class 1 and 2 frames or [re] association failure
State 2
Authenticated and unassociated
Deauthorization
Successful authentication
Deauthorization
Class 1 frames or authentication failure
State 1
Unauthenticated and unassociated

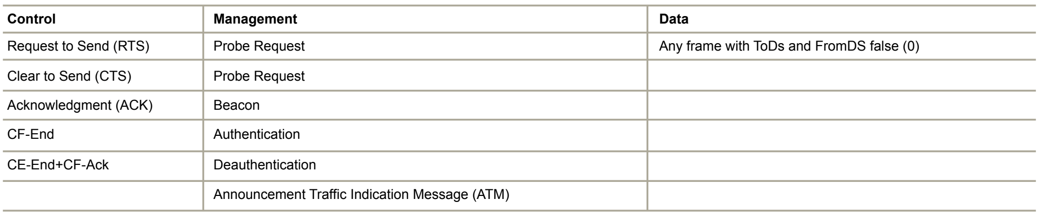
Frames that can be transmitted in 802.11 networks vary with the association status and identity authentication status.

A STA can be in any of the following states in 802.11 networks:

1. Initial state: unauthenticated and unassociated state
2. Authenticated and unassociated state
3. Authenticated and associated state

When a STA is in State 1, it can transmit frames shown in the figure below.

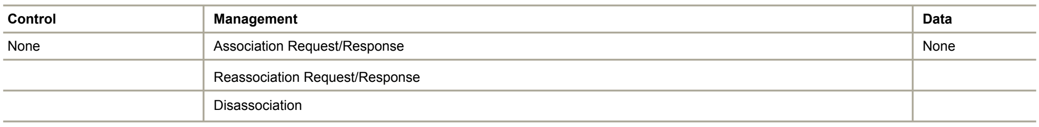
Figure 39



Control	Management	Data
Request to Send (RTS)	Probe Request	Any frame with ToDs and FromDS false (0)
Clear to Send (CTS)	Probe Request	
Acknowledgment (ACK)	Beacon	
CF-End	Authentication	
CE-End+CF-Ack	Deauthentication	
	Announcement Traffic Indication Message (ATM)	

When a STA is in State 2, it can transmit frames shown in the figure below.

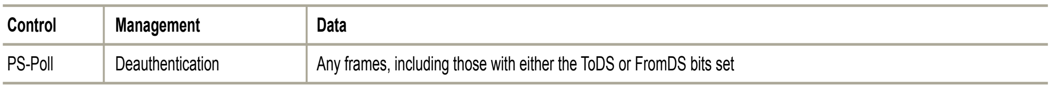
Figure 40



Control	Management	Data
None	Association Request/Response	None
	Reassociation Request/Response	
	Disassociation	

When a STA is in State 3, it can transmit frames shown in the figure below.

Figure 41



Control	Management	Data
PS-Poll	Deauthentication	Any frames, including those with either the ToDS or FromDS bits set

802.11 MAC Functions

• Scanning, Authentication, and Association

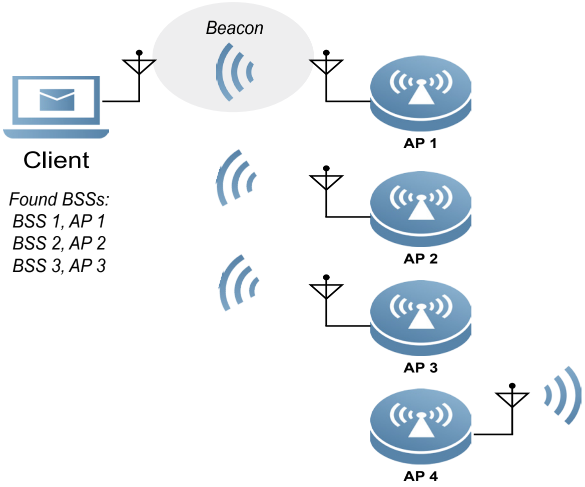
Scanning

In the wireless field, before accessing any compatible WLAN, a STA must identify existing networks in an area, that is, perform scanning. Scanning is intended to discover and access a network.

Scanning includes passive scanning and active scanning.

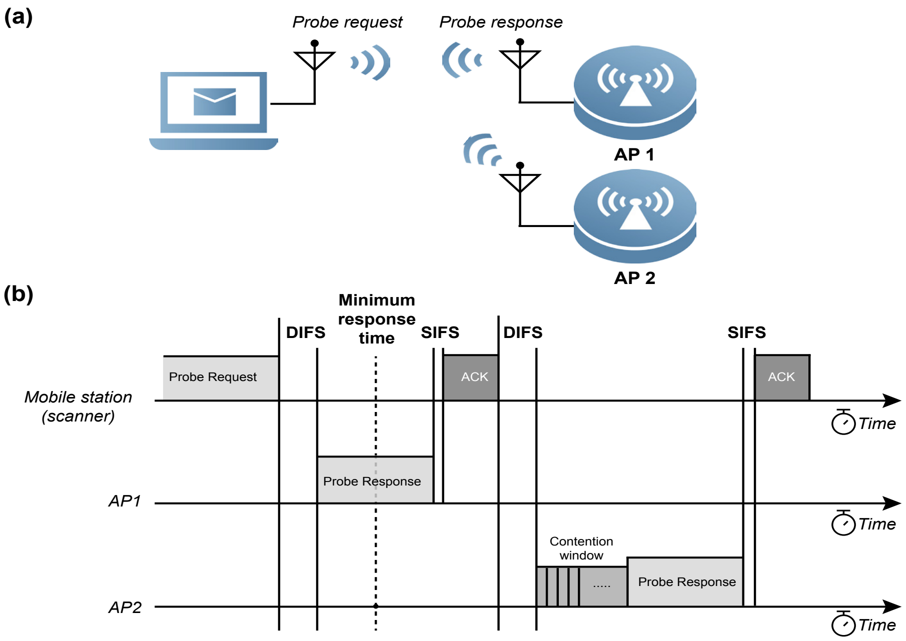
Passive scanning is implemented by listening to the Beacon frames of APs.

Figure 42



In active scanning, a STA sends a Probe Request to request a network response. When a network receives the Probe Request for searching for its ESS, it responds with a Probe Response.

Figure 43



Authentication

WLAN identity authentication includes 802.11 identity authentication and 802.11i identity authentication.

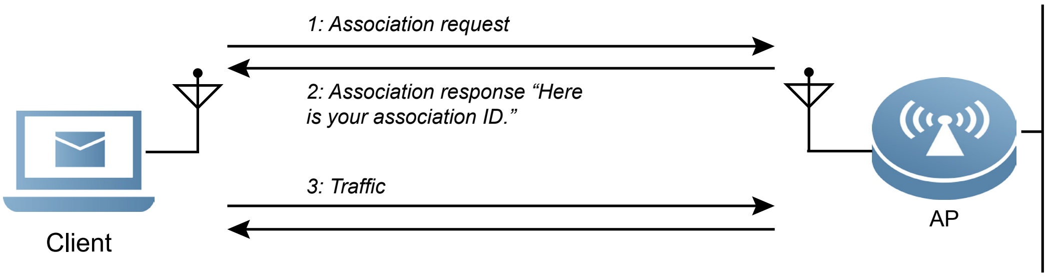
802.11 identity authentication includes open system identity authentication and shared key identity authentication.

802.11i further specifies 802.1x identity authentication.

Association

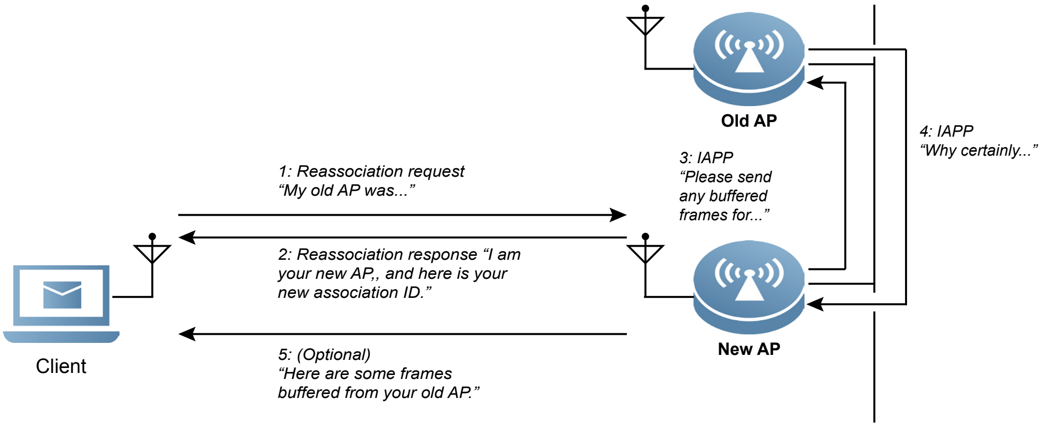
A basic association process includes an Association Request and an Association Response.

Figure 44



Reassociation refers to the process in which the association is transferred from an old AP to a new one.

Figure 45



- DCF

Work Principles

The Distributed Coordination Function (DCF) is the basis of the 802.11 MAC mode. The principal part of DCF is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism.

All STAs in both an IBSS (ad hoc BSS) and an infrastructure BSS (AP BSS) should support the DCF. The DCF uses the CSMA/CA mechanism to properly eliminate possible conflicts among different STAs, so that multiple STAs can share the same transmission media.

The CSMA/CA mechanism requires each STA to conduct Carrier Sense (CS) on a channel before transmitting frames. If finding that the channel is not occupied, a STA can use this channel to transmit frames. Otherwise, the STA needs to defer the frame transmission until the channel is idle.

As specified in IEEE 802.3, in a 802.11 system, after identifying that the channel is idle, a STA does not start transmitting data immediately but waits for a fixed period of time. This period of time is called Inter-Frame Space (IFS).

Different from IEEE 802.3, IEEE 802.11 introduces the priority mechanism in frame transmission. That is, the IFS length varies with the frame priority. Frames with a higher priority have a shorter IFS. An idle channel can be detected for these frames at an earlier time, and there is a higher probability to transmit these frames on the idle channel.

IEEE 802.11 defines four types of IFSs:

1. Short IFS (SIFS): The SIFS can be used in ACK frames, CTS frames, all fragments except the first in the fragment burst, and responses from all STAs to PC-Poll frames in the PCF mechanism.
2. PCF IFS (PIFS): necessary waiting time before frame transmission by a STA in PCF contention-free mode.
3. DCF IFS (DIFS): necessary waiting time before frame transmission by a STA in PCF contention-based mode.
4. Extended IFS (EIFS): necessary waiting time before frame retransmission by a STA. The relationship of the four IFSs is as follows: SIFS < PIFS < DIFS < EIFS.

When detecting that a channel changes from busy to idle, a STA cannot transmit frames immediately but waits for a period of IFS based on the frame priority. The STA can transmit frames only after detecting that the channel keeps idle within this IFS. However, there is still a high probability that frames of the same priority conflict with each other, as STAs will send the frames of the same priority at the same time after waiting for the same IFS and detecting that the channel is idle within this IFS.

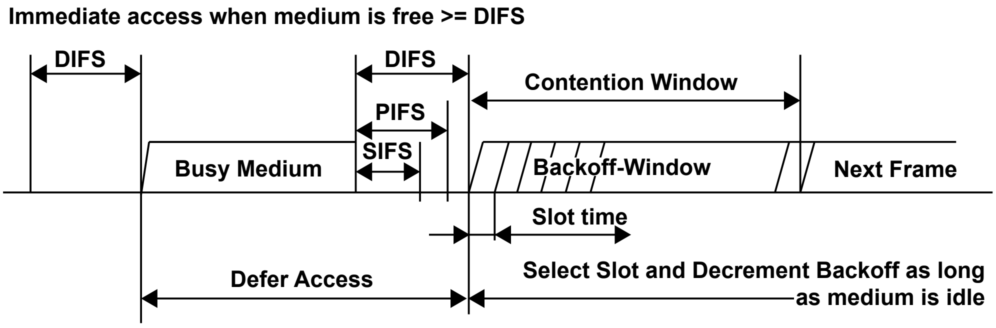
A solution is to enable a STA to wait for another random period of time (that is, backoff time) before transmitting frames. Obviously, the STA with the shortest backoff time has a higher priority of transmitting frames. Other STAs will defer frame transmission when detecting that the channel is busy. The backoff times randomly generated for STAs are different, thereby greatly reducing the frame conflict probability. This is the so-called backoff algorithm, which is similar to the backoff algorithm used in Carrier Sense Multiple Access with Collision Detection (CSMA/CD) of IEEE 802.3.

According to 802.11, the period for each STA to contend for a channel based on the backoff time is called "contention window". The contention window starts from the end of the current shortest IFS. When a STA transmits data and occupies a channel, it indicates that the current contention window ends.

After STAs enter the contention window, the backoff time starts to decrease. Each STA can transmit frames only when the current backoff time decreases to zero. If the current contention window ends, each STA that does not obtain the transmission right freezes the current remaining backoff time until the next contention window arrives. Then, STAs start a new round of channel contention based on their remaining backoff times.

Note that STAs do not need to perform the backoff mechanism after each IFS. Instead, if the STA finds that a detected channel is always idle in the first IFS, the STA can transmit frames immediately. If the STA finds that a channel is busy at the very beginning or within the first IFS, the STA needs to perform the backoff mechanism after each IFS.

Figure 46


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

The backoff time calculation specified in the IEEE 802.11 is as follows: Backoff time = Random()*aSlotTime.

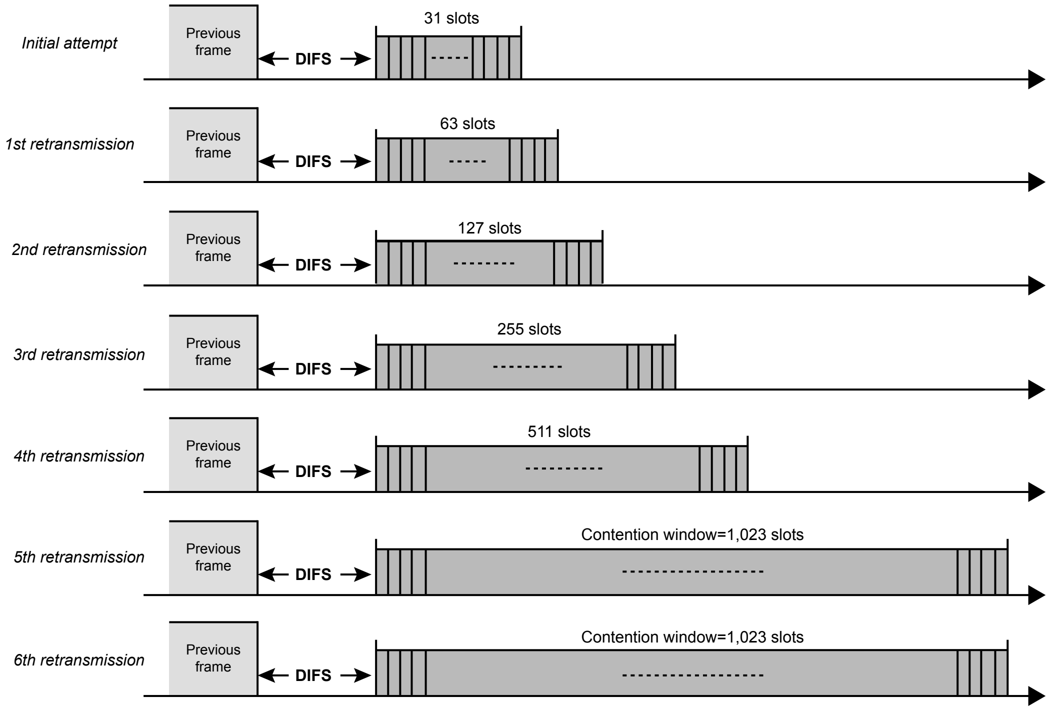
Random() is a random integer in the range of [0,CW] and aCWmin ≤ CW ≤ aCWmax.

The values of aCWmin, aCWmax, and aSlotTime should conform to different 802.11 PHY standards, as listed in the table below.

Standard	aSlotTime	aCWmin	aCWmax
802.11a	9 µs	15	1023
802.11b	20 µs	31	1023
802.11g	9 µs (short) 20 µs (long)	15	1023

The initial value of CW is aCWmin for the transmission of each frame. If a frame is retransmitted, the CW increases with the retransmission count. The value of CW is (aCWmin+1)*2n-1 for each retransmission, where n indicates the retransmission count. When CW increases to aCWmax, the CW value keeps unchanged. When transmission of the next frame starts, the CW value changes back to aCWmin again. The figure below shows an example of the CW value.

Figure 47

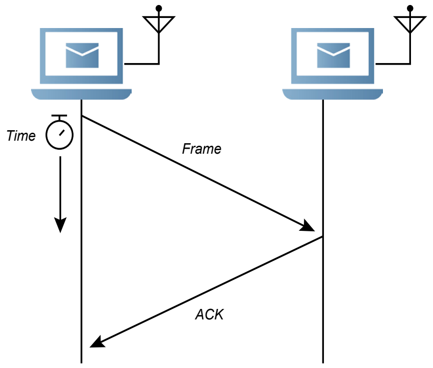


Retransmission and Acknowledgement

In ideal conditions (no transmission delay and infinite signal coverage), the CSMA/CA mechanism can effectively prevent conflicts. In actual applications, not all conflicts can be prevented by the CSMA/CA mechanism. For example, different STAs have the same backoff time. For another example, at different time points, different STAs detect that a channel is idle because of their different physical locations, and as a result, the backoff times of the STAs may decrease to 0 at the same time. Conflicts occur unavoidably in such cases. In addition, "hidden stations" described below also cause conflicts.

802.11 introduces the retransmission mechanism to DCF, to prevent data loss caused by conflicts. The retransmission mechanism is built on the message acknowledgement mechanism. In the transmission of all data frames and management frames, after acknowledging that frames are correctly received, the receiver should send the ACK frame to the transmitter for acknowledgement. If the transmitter fails to receive the ACK frame, it retransmits the frames.

Figure 48



In the CSMA/CA mechanism, a STA cannot detect a conflict during frame transmission due to the absence of the conflict detection mechanism. For this, 802.11 introduces the message acknowledgement mechanism (ACK). When the receiver fails to receive frames correctly in the case of conflict, it does not return the ACK frame for acknowledgement. When the transmitter fails to receive the ACK frame after the ACK timer (ACKtimeout) expires, it automatically retransmits the previous frame. In comparison with the real-time conflict detection mechanism defined in 802.3, the message acknowledgement mechanism of 802.11 implements non-real-time conflict detection.

The message acknowledgement mechanism provides other functions in addition to the non-real-time conflict detection. As previously described, this mechanism can also remedy or prevent frame loss, frame errors, and other exceptions. The transmitter does not need to consider the type of error occurring during transmission. The transmitter retransmits the previous frame provided that it fails to receive a valid ACK frame, regardless of whether the ACK frame is lost or an ACK frame transmission error occurs.

The receiver receives a duplicate frame due to frame retransmission caused by ACK frame transmission error or loss. Therefore, the receiver needs to identify duplicate frames based on the frame header information in the received frames and filters out duplicate frames. Each STA maintains a table, with entries composed of <Address 2, sequence-number, fragment-number>. When a STA receives a valid frame with the Retry bit being 0 (non-duplicate frame), the STA adds the frame content to the table. When the STA receives a valid frame with the Retry bit being 1 (duplicate frame), the STA considers the frame a duplicate and discards it if the frame content matches an entry in the table. If the frame does not match any entry in the table, the STA adds information about the frame to the table as a new entry.

The receiver also needs to respond to the transmitter with the ACK frame when receiving a duplicate frame.

Virtual Carrier Sense

The Physical Carrier Sense (PCS) based on the radio frequency media is costly. To prevent exceptions, 802.11 defines the Virtual Carrier Sense (VCS) mechanism, to assist the PCS mechanism in completing carrier sense.

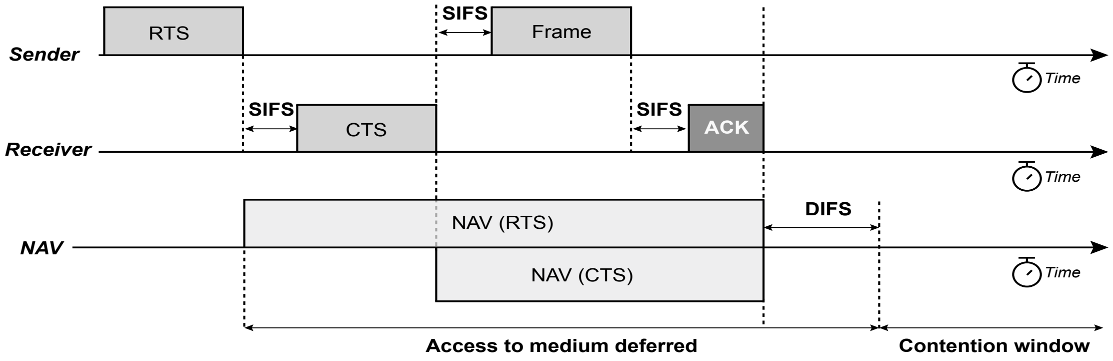
A channel is considered occupied regardless of whether the PCS or VCS detects that the channel is busy. A channel is considered idle only when both the PCS and VCS detect that the channel is idle.

The core of the VCS mechanism is the Network Allocation Vector (NAV). Each STA has a NAV for recording the estimated time of channel occupancy by other STAs. The NAV is actually a counter, whose value decreases with the elapse of time. A STA is always in the waiting state in this process. When the NAV value decreases to 0, the VCS mechanism considers that the channel is idle.

The NAV value comes from the Duration field carried in received frames. When a STA receives a valid frame that is not destined for the STA, if the value of the Duration field carried in the frame is greater than the current NAV value, the STA must use the value of the Duration field to update the NAV record.

The channel occupancy time recorded by the NAV may accumulate continuously. Before the time is reset, a channel remains busy and the STA cannot transmit frames. In this sense, the NAV has the carrier sense function, and can notify a STA whether a channel is busy. Therefore, the NAV is referred to as the VCS mechanism.

Figure 49



All frames involved in the DCF mechanism carry the **Duration** field. The **Duration** field is a channel occupancy time estimated by the transmitter for the transmission of subsequent frames (between the source and target sites). The occupancy time is "predictable" to the transmitter. For example, if the value of the **More Frag** bit in the data frame received by the receiver is **1** during fragment burst, the **Duration** field carried in the ACK frame returned by the receiver can only be an estimated value: the sum of the transmission time of one fragment, transmission time of one ACK frame, and two SIFSs. The time sequence is as follows: SIFS -> DATA -> SIFS -> ACK. The number of fragments to be transmitted subsequently cannot be predicted. Therefore, the "predictable" channel occupancy time is the time required for the transmission and response of the next fragment.

The table below lists the value of the **Duration** field carried in typical frames.

Frame Type	Duration Value		
RTS	SIFS+CTS+SIFS+DATA+SIFS+ACK		
CTS	SIFS+DATA+SIFS+ACK		
DATA	Multicast/Broadcast		0
	Unicast	More Fragment bit = 0	SIFS+ACK
		More Fragment bit = 1	SIFS+ACK+SIFS+DATA+SIFS+ACK
ACK	More Fragment bit = 0		0
	More Fragment bit = 1		SIFS+DATA+SIFS+ACK
Note: DATA here includes data frames and management frames.			

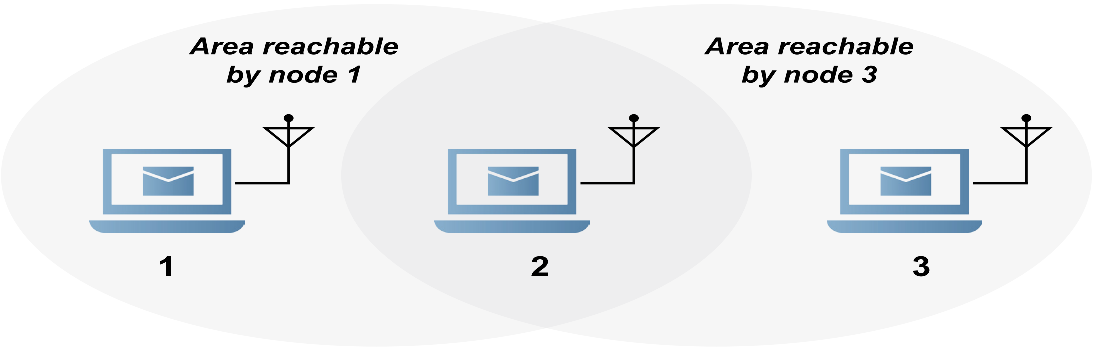
The message acknowledgement mechanism is not adopted for multicast frames and broadcast frames. These frames do not need acknowledgment or occupy channels. Therefore, the value of the Duration field carried in multicast frames and broadcast frames is 0.

Hidden Station

WLANs are complex and one typical problem in WLANs is the hidden station.

In actual applications, the situation shown in the figure below often occurs: Coverage areas of STA 1 and STA 2 overlap and the STAs can communicate with each other; coverage areas of STA 2 and STA 3 overlap and the STAs can communicate with each other. STA 1 and STA 3 cannot receive wireless signals from each other due to weak signal strength, that is, they cannot communicate as they are "hidden" to each other. In this case, when STA 1 and STA 3 both need to transmit data to STA 2, they consider that the channel idle as they cannot receive each other's signals. Consequently, the two STAs transmit data through the channel simultaneously, resulting in a conflict in STA 2, and STA 2 cannot receive data normally, leading to the hidden station problem.

Figure 50



A conflict is common in 802.11 networks. The 802.11 system can utilize the retransmission mechanism to prevent data loss caused by conflicts. However, different from other conflicts, a conflict caused by hidden stations means that the CS mechanism, basis of the conflict avoidance mechanism, becomes invalid (STA 2 and STA 3 cannot detect each other), indicating that retransmission is blind. Therefore, in the case of hidden stations, the conflict probability is far higher than that in other cases.

It is necessary to know the consequence caused by conflicts arising from the hidden station problem. Even if the CS mechanism fails, the random backoff mechanism is still carried out automatically. The random value range of the backoff time is large. In the 802.11b/g system, the maximum range of the random backoff time used for transmitting the long preamble frame can be [0, 20.46] in milliseconds. In addition, it can be calculated that, without considering the ACK response process, the required transmission time is 0.25 ms (802.11b)/0.05 ms (802.11g) for a 80-byte frame, 0.4 ms (802.11b)/0.08 ms (802.11g) for a 272-byte frame, and 1.9 ms (802.11b)/0.38 ms (802.11g) for a 2346-byte frame. In conclusion, in the case of hidden stations, STAs can utilize the conflict-free period occurring due to the backoff time differences of STAs, to complete transmission of both long and short packets. Obviously, the conflict probability in the transmission of short packets is smaller than that of long packets.

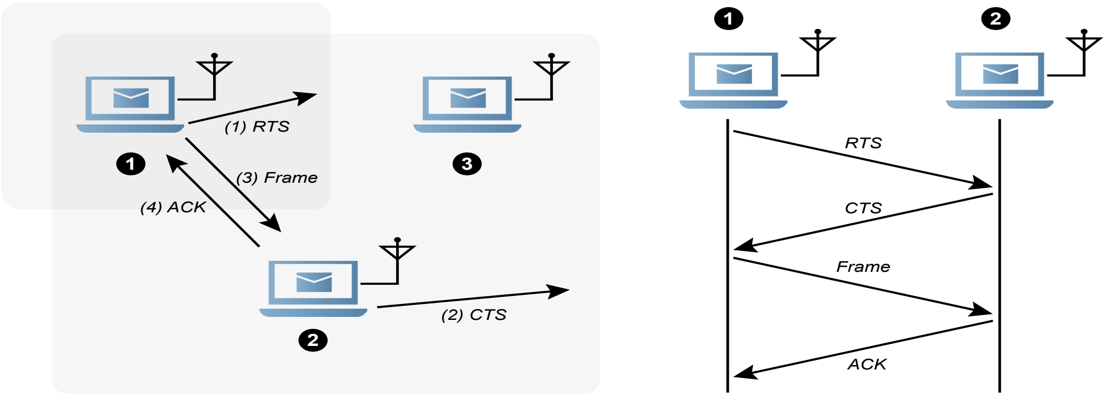
The hidden station problem reveals the limitations of the PCS mechanism and the VCS mechanism is required. In the hidden station example, though STA 1 and STA 3 cannot communicate with each other but they are both within the signal coverage of STA 2, the ACK frame returned by STA 2 can be received by both STA 1 and STA 3 regardless of whether STA 2 receives data frames from STA 1 or STA 3. In this way, based on the value of the Duration field carried in the ACK frame, STA 1 or STA 3 can learn the estimated time of channel occupancy by the other party, and keep waiting in this period of time. With the transmission in progress, the STA in the waiting state updates the NAV value based on the value of the Duration field carried in subsequently received ACK frame, and starts to preempt the channel when the NAV value decreases to 0.

In brief, STA 1 and STA 3 transmit data frames (or management frames), intending to outperform the other party by first receiving the ACK frame returned by the receiver, to complete channel preemption. The VCS mechanism comes into play only after STA 1 or STA 3 successfully preempts a channel. Before that, the channel preemption process of STA 1 or STA 3 is prone to a conflict, which is beyond the capability of the VCS mechanism. As described above, the conflict probability is lower when shorter packets are transmitted in the case of hidden stations. Therefore, 802.11 recommends that one pair of short RTS and CTS frames be used for channel preemption. The lengths of the RTS and CTS frames are 20 bytes and 8 bytes respectively, excluding the frame body. The RTS frame contains the Frame Control, Duration, RA, TA, and FCS fields. The CTS frame does not carry the TA field and its RA field comes from the TA field in the received RTS frame.

When the RTS/CTS channel preemption mechanism is adopted, each STA transmits the RTS frame to the target STA before starting data transmission. If the STA successfully receives the CTS frame returned by the target STA before the CTS timer (CTStimeout) expires, it indicates that the STA preempts the channel successfully and can transmit data. If the STA fails to receive the CTS frame returned by the target STA or receives another frame (indicating that the channel is preempted by another STA) before the CTS timer expires, the STA fails to preempt the channel.

After receiving the CTS frame, the STA transmits subsequent data/management frames with the highest priority (that is, by using the SIFS), to prevent other STAs (which join channel preemption during CTS response and do not receive the complete CTS frame) from preempting the channel.

Figure 51



In general, the RTS/CTS channel preemption mechanism is applicable only to unicast transmission but not multicast or broadcast transmission of data/management frames, because it is obviously unreasonable to wait for multiple CTSs. The multicast and broadcast transmission varies with types of BSSs and varies among BSSs. The table below lists four processes in the multicast transmission and broadcast transmission, and use statuses of the RTS/CTS mechanism and ACK mechanism in each process.

Process	Frame Control Field		RTS/CTS	ACK	Transmission Direction
	Process	Frame Control Field			
A	0	0	No	No	Multicast: STA -> other STAs in the BSS Broadcast: STA -> the other STAs in the BSS
B	1	0	Optional	Yes	STA -> AP
C	0	1	No	No	Multicast: AP -> some STAs in the BSS Broadcast: AP -> all STAs in the BSS
D	1	1	No	No	AP -> other APs in the ESS (wireless)

The multicast and broadcast transmission inside an IBSS conform to Process A.

In the multicast and broadcast transmission inside an independent infrastructure BSS, the source STA performs Process B and then the AP performs Process C.

In the multicast and broadcast transmission inside an ESS composed of multiple BSSs, the source STA first performs Process B, the AP in the same BSS as the source STA subsequently performs Process C and Process D, and then other APs in the ESS perform Process C.

Specially, in an 802.11 LAN, a STA receives a broadcast frame with the source address being the STA’ s own address when the STA is in an infrastructure BSS. Such broadcast packets need to be filtered out in the MAC design.

The RTS/CTS channel preemption mechanism is disadvantageous in waste of channel bandwidth. Therefore, in 802.11, it is recommended that the RTS/CTS mechanism be selectively used for the transmission of frames of different lengths. For short frames with a low conflict probability, the use of the RTS/CTS mechanism may waste more bandwidth than retransmission caused by a conflict. 802.11 neither forcibly requests the application of the RTS/CTS mechanism nor defines the length of frames suitable for the RTS/CTS mechanism, and both can be user-defined. The parameter dot11RTSThreshold is defined in 802.11. The RTS/CTS mechanism needs to be used frames whose length exceeds the value of dot11RTSThreshold. When the value of dot11RTSThreshold is 0, the RTS/CTS mechanism is mandatory. When the value of dot11RTSThreshold is greater than the maximum frame length, the RTS/CTS mechanism is not used.

• Fragmentation and Reassembly

802.11 recommends that an MSDU be divided into several fragments for transmission, to improve the transmission success rate. MSDUs are fragmented based on FragmentationThreshold. Fragmentation can reduce the interference probability and decrease the bandwidth wasted due to retransmission.

The current fragmentation implementation shows that FragmentationThreshold is not intelligently specified by the MAC frame but needs to be manually set. It is a fixed value rather than a dynamic value.

The post-fragmentation transmission is called fragmentation burst, in which SIFS is adopted. The value range of FragmentationThreshold is not specified in the standards.

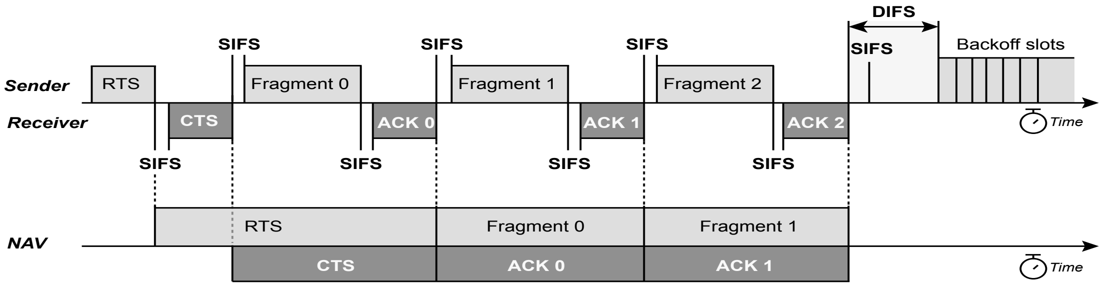
Maximum value: 2346 – 34 – 8 = 2304 bytes (encryption required)

2346 – 34 = 2312 bytes (encryption not required) Minimum value: 256 – 34 = 222 bytes (actual products)

The transmitter marks each fragment with sequence-number and fragment-number. When the receiving ends (More Frag = "0"), reassembly starts.

Note that a STA always has the channel control right during fragmentation burst. The NAV is set to ensure that other STAs do not use the channel during fragmentation burst. As shown in the figure below, each frame fragment reserves the NAV for the next frame.

Figure 52



• Retransmission

The acknowledgement to RTS relies on the CTS response and the acknowledgement to data and management frames relies on the ACK response. After the timer expires, the transmitter starts retransmission if receiving no response.

The transmitter maintains MaxTransmitMsduLifetime for each transmitted MSDU. After MaxTransmitMsduLifetime expires, the transmitter discards all fragments that are not transmitted.

The receiver maintains MaxReceiveMsduLifetime for each received MSDU. After MaxReceiveMsduLifetime expires, the receiver discards all received fragments. Even if fragments of the MSDU are subsequently received, the receiver discards the fragments.

ShortRetryLimit is used to restrict the maximum retransmission count of short frames (frame length ≤ RTSthreshold); LongRetryLimit is used to restrict the maximum retransmission count of long frames (frame length > RTSthreshold).

• Synchronization

Multiple synchronization mechanisms such as carrier synchronization, bit synchronization, and frame synchronization must be used to ensure normal operation of the 802.11 wireless transceiving system. However, the synchronization function defined in 802.11 is not any of the mechanisms above but a mechanism akin to network synchronization. The synchronization function is used for two special applications in the 802.11 system: energy saving management and frequency hopping.

In energy saving management mode, a STA in sleep state needs to wake up periodically to receive data. In frequency hopping mode, each STA needs to switch the frequency simultaneously. The two applications needs a common time reference among STAs. This time reference is stored in the 64-bit Timing Synchronization Function (TSF) timer (in the unit of μs) of each STA. The timer value increases by 1 each time 1 μs passes by. The 64-bit TSF timer is sufficient for a timing span of 100,000 years.

When a STA initiates an association request to a new BSS or waits for associating with an existing BSS, its TSF initial value is 0. When a STA waiting for associating with an existing BSS receives a desired Beacon frame (in passive scanning mode) or receives a returned Probe Response frame (in active scanning mode), the STA uses the value of Timestamp carried in the frame to replace the TSF timer value. After associating with the BSS, the STA receives the Beacon frames from other STAs at an interval of aBeaconPeriod, which can be obtained from the Beacon frame or Probe Request frame. When the value of Timestamp carried in the frame is greater than the TSF timer value, the STA uses the value of Timestamp to update the value of the TSF timer.

In an infrastructure BSS, the Beacon frame is periodically sent by an AP (not in sleep state) at an interval of aBeaconPeriod. In an IBSS, the Beacon frame is periodically sent by all STAs not in the sleep state in the IBSS at an interval of aBeaconPeriod in contention mode. All STAs that fail the contention need to receive the Beacon frame transmitted by the STA that succeeds in the contention. The TSF timer value is updated only when the value of Timestamp carried in the Beacon frame is greater than the TSF timer value.

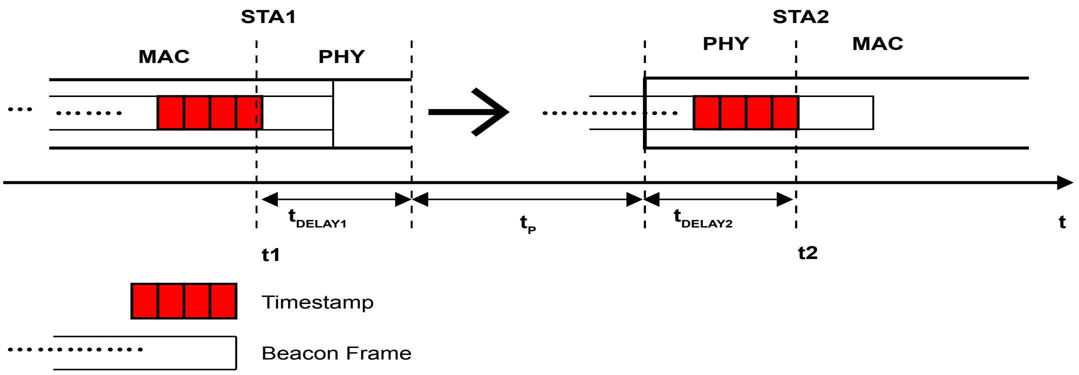
For details about how a STA in the sleep state receives the Beacon frame, see "Energy Saving Management." The critical point is to enable a STA to wake up periodically. Therefore, maintaining synchronization among STAs is crucial.

The synchronization mechanism adopted by 802.11 can only ensure a quasi-synchronous state among STAs. As shown in the figure below, assume that STA 2 receives the Beacon frame from STA 1 to update its own TSF timer. Due to the delay in the transmission path (PHY of STA1 –> Radio channel -> PHY of STA2), when STA 2 receives the Beacon frame, the value of Timestamp carried in the frame is smaller than the current TSF timer value (which increases with the elapse of time) of STA1 by tDELAY1 + tP + tDELAY2.

To solve this problem, according to requirements in 802.11, when the first bit of Timestamp in the Beacon frame reaches the MAC-PHY interface, STA 1 sets the value of Timestamp and the value equals the current TSF timer value of STA1 t1 plus the estimated transmission delay tDELAY1 in the PHY of STA1. After STA 2 extracts the Timestamp value from the received Beacon frame, the STA 2 needs to add the estimated transmission delay tDELAY2 in the PHY of STA 2 to the Timestamp value. Therefore, the TSF timer value to be set by STA 2 is a revised value (t1 + tDELAY1 + tDELAY2), on the condition that the revised value is greater than the current TSF timer value of STA 2.

Therefore, to update the TSF timer value, the revised value of Timestamp must be greater than the current TSF timer value of the STA.

Figure 53



The error in the synchronization mechanism of the 802.11 system mainly comes from the transmission delay tp in the radio channel. The distance among STAs changes dynamically due to WLAN mobility. The dynamic ranging technology can hardly be implemented for STAs. Therefore, the error cannot be revised. In 802.11, the estimated maximum error equals the transmission delay in the radio channel at the transmission rate of 1 Mbps plus 4 μs.

• Multi-rate Support

802.11 defines three types of rates: BSS basic rate set, operational rate set, and mandatory rate.

The BSS basic rate set lists the rates that all STAs associating with the BSS must support. The operational rate set is an extension to the BSS basic rate set. Both communication parties must support the operational rate set so that they can communicate with each other at a rate in the operational rate set. Rates in the two rate sets can be selected by software (or specified by the driver or by users) from the rates that are already implemented by the PHY. No limitation is specified in the standard.

The two types of rate information are carried in the following management frames: Beacon, Probe Request, Probe Response, Association Request, and Association Response. The information element in management frames contains two parameters: Supported Rates and Extended Supported Rates. The Supported Rates parameter can carry only eight rates, and excessive rates are placed in the Extended Supported Rates parameter. For BSS basic rates, the MSB is 1 and operational rate set is 0.

Both communication parties obtain the supported rates of the peer by performing handshakes using management frames. The content of the BSS basic rate set is specified by the AP that builds the infrastructure BSS or the STA that builds the IBSS. After a STA receives a Beacon or Probe Response frame, the STA should not connect to the peer if finding that the STA can support none of the rates in the BSS basic rate set.

Mandatory rates are the rates that must be implemented by various PHYs. They are the requirements on the chip design in the standard.

According to the standard, the relationship among the three types of rates is as follows: Mandatory rates and BSS basic rate set are not subordinate to each other and can have intersection or not. The operational rate set is a supplement to the BSS basic rate set.

	To DS=0	To DS=1
802.11b	DSSS	1, 2
	CCK	5.5, 11
802.11a	OFDM	6, 12, 24
802.11g	ERP-DSSS/CCK (that is, 802.11b)	1, 2, 5.5, 11
	ERP-PBCC (optional)	
	ERP-OFDM (considered as 2.4 GHz of 802.11a)	6, 12, 24
	SSS-OFDM (optional)	

No rate switching algorithm is specified in the standard. However, some rules are defined to ensure the PHY compatibility:

1. All control frames must be transmitted at a rate contained in the BSS basic rate set.
2. Broadcast and multicast frames must be transmitted at a rate in the BSS basic rate regardless of the frame type.
3. Unicast data and management frames can be transmitted at a rate selected via the rate switching algorithm. The source STA must use a rate supported by the target STA to transmit data. In the communication between the same source STA and target STA, the target STA should select a possible maximum rate (which cannot be higher than the transmission rate of the previously received frame) from the BSS basic rate set (or select a mandatory rate if there is no proper rate in the basic rate set), to respond to the source STA with a response frame (such as ACK or CTS). This rule ensures a relatively accurate value of the **Duration/ID** field estimated by the source STA.

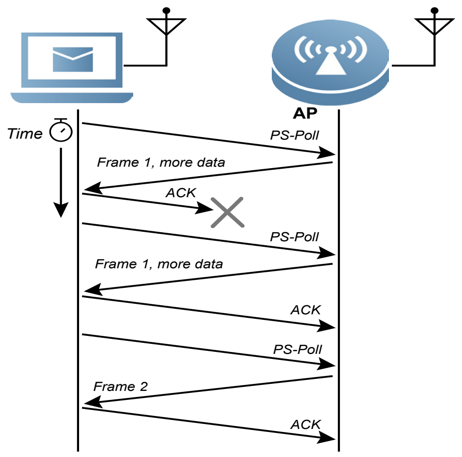
• Energy Saving Management

A STA can determine, based on its requirements, to use the active mode or power save mode for power management. A STA must use the **Power Management** bit in the **Frame Control** field carried in the transmitted frames to notify the coordinator of a mode change. The coordinator needs to store the frames to be transmitted to a STA in PS mode, and transmit them at a specified time. The STAs with to-be-transmitted frames stored in the coordinator are recorded in the Traffic Indication Map (TIM). The coordinator adds the TIM in the Beacon frame each time the Beacon frame is transmitted. A STA in PS mode should wake up periodically to receive the Beacon frame (the wakeup interval is defined by the **aListenInterval** parameter of the STA). After receiving the TIM, the STA automatically analyzes whether the STA has frames stored in the coordinator. Each STA that is associated with the coordinator is assigned an AID. The TIM records, in the form of virtual bitmap, whether a STA has frames stored in the coordinator. For example, if the ith bit is 1, it indicates that the STA with AIDi has frames stored in the coordinator.

AID0 is reserved for broadcast or multicast frames. If the 0th bit is 1, it indicates that broadcast or multicast frames are stored in the coordinator. A STA in PS mode can be a polling or non-polling STA. In the contention period in PCF operation environment or in the DCF operation environment, if a STA in PS mode (polling or non-polling STA) finds that it has a frame stored in the coordinator, the STA transmits a short PS-Poll frame to the coordinator. The coordinator transmits the stored frame destined for the STA (one PS-Poll frame for one stored frame) to the STA as early as possible. The **More Data** field in the PS-Poll frame records whether the STA has other frames stored in the coordinator. If yes, the STA sends another PS-Poll frame to retrieve the second frame. The process repeats until the coordinator transmits all stored frames destined for the STA to the STA.

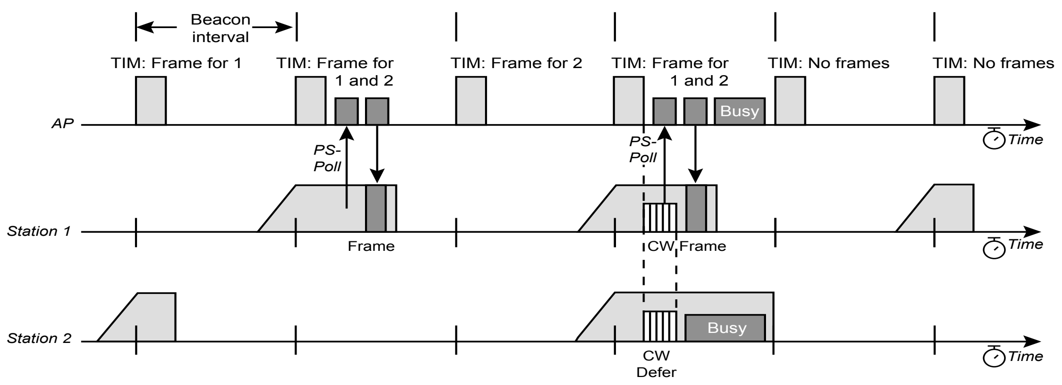
Note that an ACK frame from the receiver must be received before a frame is removed from the buffer.

Figure 54



In addition, if a STA finds from the TIM that other STAs also have frames stored in the coordinator, the STA cannot transmit the PS-Poll frame immediately. Otherwise, other STAs may also transmit the PS-Poll frames, resulting in the PS-Poll frame conflicts. To reduce the conflict probability, the STA needs to delay transmitting the PS-Poll frame for a random period of time. The random delay falls in [0, aCWmin] on average. The STA that transmits the PS-Poll frame must keep staying in the awake state until it receives a corresponding frame or another Beacon frame indicating that the STA has no frame stored in the coordinator (possibly transmitted in the contention-free period).

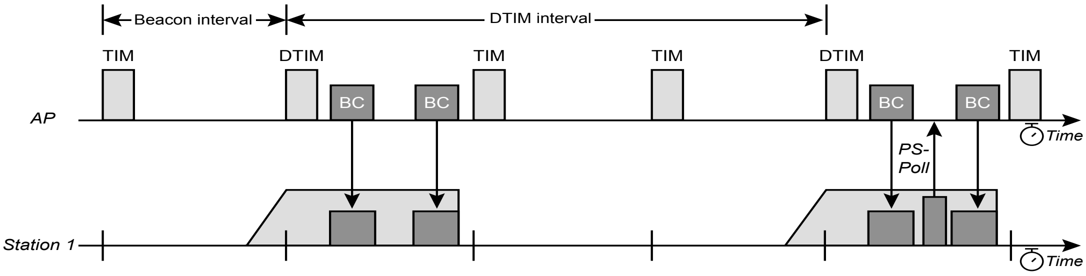
Figure 55



The coordinator processes broadcast or multicast frames differently. If there is a STA in PS mode in a BSS, the coordinator must store to-be-transmitted broadcast or multicast frames, and transmit them only after transmitting the Beacon frame that carries the Delivery TIM (DTIM). The coordinator can transmit multiple Beacon frames that carry the DTIM in one contention-free period. STAs in PS mode wake up to receive Beacon frames only at a specific time. Therefore, transmitting the stored broadcast or multicast frames after the Beacon frame allows the STAs in PS mode to accurately plan the time for receiving the broadcast or multicast frames, thereby preventing frequent power management mode switching caused by the receiving of irregularly transmitted broadcast or multicast frames.

TIMs are classified into TIMs and DTIMs. The coordinator adds a TIM to the Beacon frame every time the Beacon frame is transmitted. Moreover, the coordinator adds a DTIM to the Beacon frame at an interval of **aDTIMPeriod**. The coordinator transmits broadcast or multicast frames after Beacon frames carrying the DTIM and before unicast frames. Whether a STA in PS mode needs to wake up or when the STA wakes up to receive Beacon frames carrying the TIM (or DTIM) depends on the STA itself. If a STA wakes up periodically to receive Beacon frames, it will not miss any frame (including broadcast or multicast frames) transmitted from any other STAs but the modes are frequently switched, which causes power waste. If power saving is the top concern, STAs can wake up at a long interval to receive Beacon frames. In this case, frames transmitted from other STAs may be received late (stored in the coordinator) and the STAs may miss some broadcast or multicast frames.

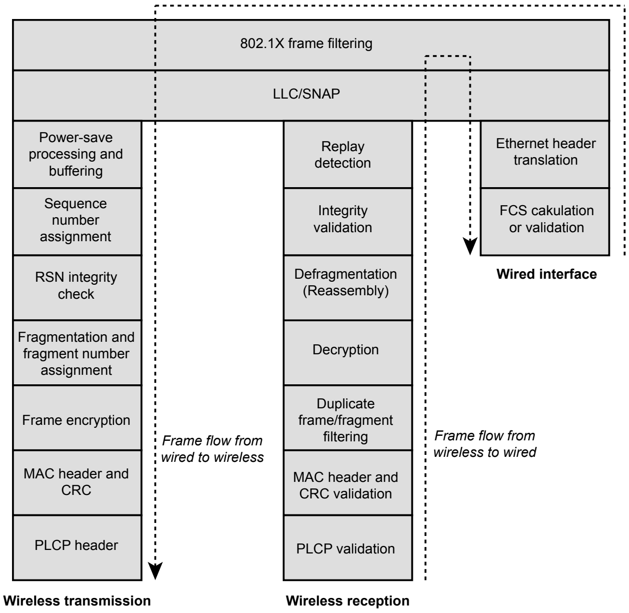
Figure 56



• Frame Processing and Bridging

The core of an AP is a bridge, which transmits frames between wired and wireless media. The figure below shows the transmission of frames in the two media.

Figure 57


802.1X frame filtering
LLC/SNAP
Power-save processing and buffering
Sequence number assignment
RSN integrity check
Fragmentation and fragment number assignment
Frame encryption
MAC header and CRC
PLCP header
Frame flow from wired to wireless
Replay detection
Integrity validation
Defragmentation (Reassembly)
Decryption
Duplicate frame/fragment filtering
MAC header and CRC validation
PLCP validation
Frame flow from wireless to wired
Ethernet header translation
FCS cakulation or validation
Wired interface
Wireless transmission
Wireless reception

802.11n MAC Frame Extension

• Format Extension

Figure 58

Octets: 2	2	6	6	6	2	6	2	4	0-7955	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Qos Control	HT Control	Frame Body	FCS

MAC Header

802.11n extends the 802.11 MAC frame by adding the 4-byte HT Control field.

• HT Control Field

Figure 59

	B0 B15	B16 B17	B18 B19	B20 B21	B22 B23	B24	B25 B29	B30	B31
	Link Adaptation Control	Calibration Position	Calibration Sequence	Reserved	CSI/ Steering	NDP Announcement	Reserved	AC Constraint	RCG/More PPDU
Bits	16	2	2	2	2	1	5	1	1

The **HT Control** field occupies four bytes.

The **Link Adaptation Control** field of the **HT Control** field occupies two bytes.

Figure 60

B0	B1	B2 B5	B6 B8	B9 B15
reserved	TRQ	MAI	MFSI	MFB/ASELC
1	1	4	3	7

The TRQ bit indicates the sounding request. The value 1 of this bit indicates that the receiver is requested to transmit the sounding PPDU, which is mainly used for beamforming.

The MCS Request or Antenna Selection Indication (MAI) is used for the Modulation and Coding Scheme (MCS) request or antenna selection.

The MFB Sequence Identifier (MFSI) is used for the Modulation and Coding Scheme Feedback (MFB).

The MCS Feedback and Antenna Selection Command/Data (MFB/ASELC) indicates the antenna selection command and data if MAI is used for antenna selection. This field provides the recommended MCS feedback in other cases.

The Calibration Position and Calibration Sequence fields are used for calibration control in beamforming.

The CSI/Steering field is used for the beamforming feedback.

The NDP Announcement field is used to notify whether there are Null Data Packets (NDPs) subsequently. The value 1 indicates yes and the value 0 indicates no. The NDP serves as the probe frame of beamforming.

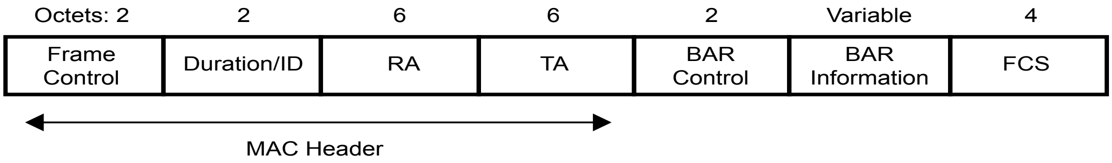
The AC Constraint field indicates whether reverse direction frames (that is, response frames) are identified by the same traffic identifier (TID). The value 1 indicates yes.

The RDG/More PPDU field indicates whether Duration/ID in the reverse direction frame is reserved.

• Frame Type Extension

BlockAckReq Frame

Figure 61

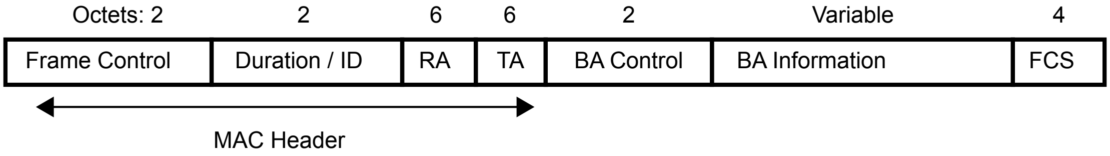


Octets: 2	2	6	6	2	Variable	4
Frame Control	Duration/ID	RA	TA	BAR Control	BAR Information	FCS

The BlockAckReq frame is used as a block acknowledgment request, and its variants include Basic BlockAckReq, Compressed BlockAckReq, or Multi-TID BlockAckReq.

BlockAck Frame

Figure 62

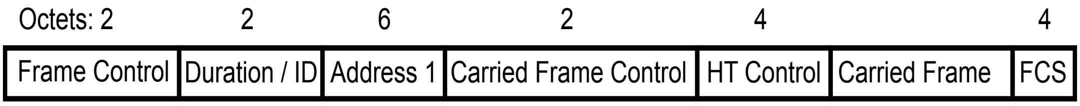


Octets: 2	2	6	6	2	Variable	4
Frame Control	Duration / ID	RA	TA	BA Control	BA Information	FCS

The BlockAck frame is used to respond to multiple frames simultaneously.

Control Wrapper Frame

Figure 63



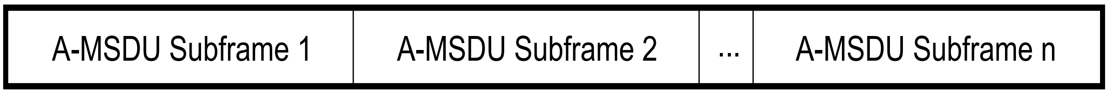
Octets: 2	2	6	2	4		4
Frame Control	Duration / ID	Address 1	Carried Frame Control	HT Control	Carried Frame	FCS

The Control Wrapper frame is used to encapsulate other control frames in a frame format that carries the HT Control field.

Aggregate MSDU Frame

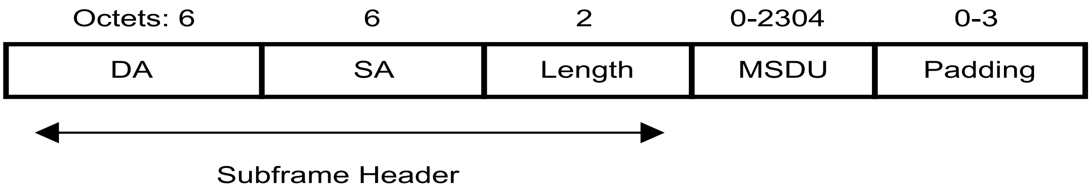
An Aggregate MSDU (A-MSDU) is a large payload composed of multiple A-MSDU subframes. All A-MSDU subframes are 4-byte aligned except the last subframe.

Figure 64



The figure below shows the format of an A-MSDU subframe.

Figure 65



HT Action Frame

The Category field in the HT Action frame is set to 7.

The figure below describes the value of the Action field.

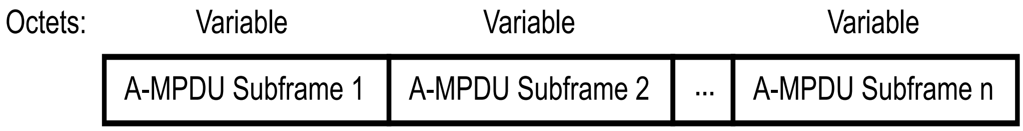
Figure 66

Action field value	Meaning
0	Notify Channel Width
1	SM Power Save
2	PSMP action frame
3	Set PCO Phase
4	MIMO CSI Matrices
5	MIMO Non-compressed Beamforming
6	MIMO Compressed Beamfroming
7	Antenna Selection Indices Feedback
8	HT Infromation Exchange
9-255	Reserved

• Aggregate MPDU

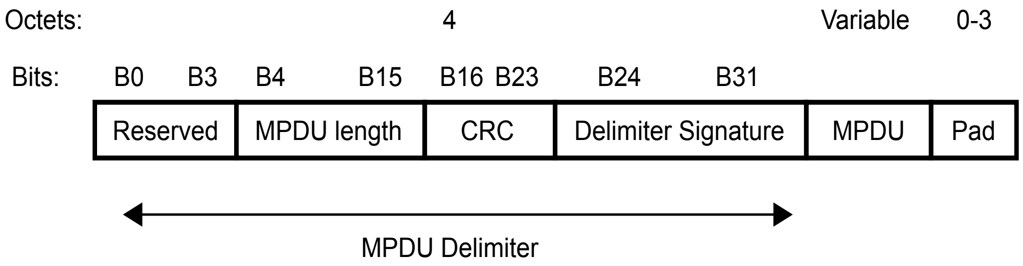
An Aggregate MPDU (A-MPDU) is composed of multiple A-MPDU subframes.

Figure 67



The figure below shows the format of an A-MPDU subframe.

Figure 68



802.11n MAC Function Extension

• DCF Function

RIFS

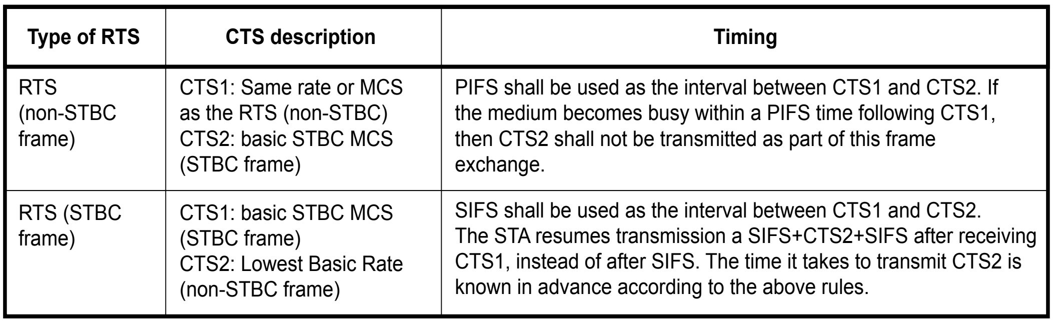
802.11n defines the Reduced Inter-Frame Spacing (RIFS) shorter than the SIFS, to improve performance. After a transmitter transmits multiple frames consecutively but receives no response, it uses the RIFS to replace the SIFS to improve network performance.

The RIFS is applicable only to the MAC frame that carries the HT Control field.

Dual CTS Protection

802.11n provides dual CTS protection to ensure that the Space-Time Block Coding (STBC) properly functions.

Figure 69



Type of RTS	CTS description	Timing
RTS (non-STBC frame)	CTS1: Same rate or MCS as the RTS (non-STBC) CTS2: basic STBC MCS (STBC frame)	PIFS shall be used as the interval between CTS1 and CTS2. If the medium becomes busy within a PIFS time following CTS1, then CTS2 shall not be transmitted as part of this frame exchange.
RTS (STBC frame)	CTS1: basic STBC MCS (STBC frame) CTS2: Lowest Basic Rate (non-STBC frame)	SIFS shall be used as the interval between CTS1 and CTS2. The STA resumes transmission a SIFS+CTS2+SIFS after receiving CTS1, instead of after SIFS. The time it takes to transmit CTS2 is known in advance according to the above rules.

• A-MSDU

The A-MSDU technology aggregates multiple MSDUs into a large payload. The MSDUs here can be Ethernet packets. When an AP or wireless STA receives packets (MSDUs) from the protocol stack, it adds the Ethernet packet header. MSDUs with Ethernet packet headers are called A-MSDU subframe. Before being transmitted through a radio port, the packets need to be converted into packets in the 802.11 packet format one by one. The A-MSDU technology aims at aggregating multiple A-MSDU subframes and encapsulating them into one 802.11 packet for transmission. In this way, the overheads of the PLCP Preamble, PLCP header, and 802.11MAC header required for the transmission of each 802.11 packet are reduced, the number of response frames is reduced, and the packet transmission efficiency is raised.

• A-MPDU

Different from the A-MSDU technology, the A-MPDU technology aggregates the MPDUs, which are data frames encapsulated via 802.11. The A-MPDU technology transmits several MPDUs at a time. This reduces the overheads of the PLCP Preamble and PLCP header required for the transmission of each 802.11 packet, thereby increasing the system throughput.

• Block Acknowledgement

According to the 802.11 protocol, an ACK frame must be transmitted immediately in response to each received unicast data frame, to ensure the data transmission reliability. After receiving an A-MPDU, the receiver needs to process each MPDU contained in the A-MPDU and transmits a response frame for each MPDU.

The Block Acknowledgement (BA) utilizes one ACK frame to respond to multiple MPDUs, to reduce the number of ACK frames.

1. N-immediate BA

The N-immediate BA simplifies the conventional immediate BA adopted for A-MPDUs. The N-immediate BA mainly involves the following processing:

a) The "normal ACK mechanism" is used for QoS data frames. ACK frames are sent in response to non-aggregate PPDU requests, and BAs are sent in response to aggregate PPDU requests.

b) Block Acknowledgement Requests (BARs) are used to request BA frames.

c) The compressed BA bitmap format is used. Each bit in the BA bitmap field indicates whether the corresponding MPDU is correctly received.

d) The Tx buffer control module of the BA Tx site sets the WinStart and WinSize parameters to deliver the MPDU to be transmitted and release the Tx buffer that buffers relevant BAs from the BA Rx site. The WinStart parameter indicates the start position (sequence number) of a transmission window and the WinSize parameter indicates the number of buffers agreed in the BA.

e) The response to each MPDU is determined based on BA requirements for frames aggregated by the aggregation control module.

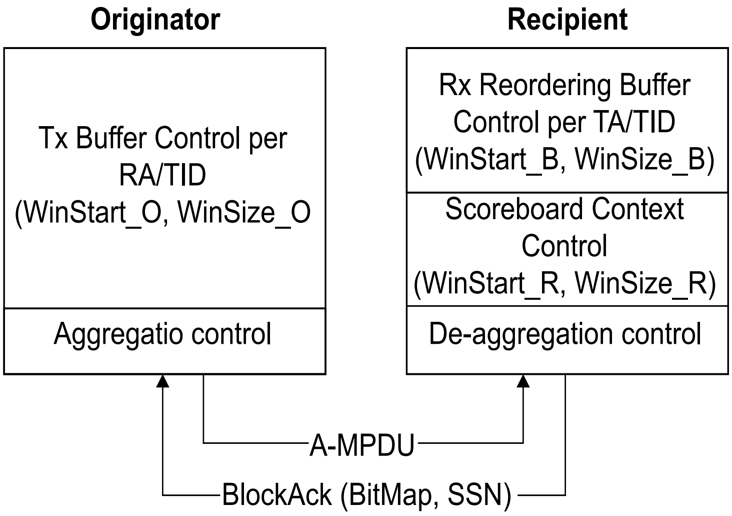
f) The Rx reordering Buffer module of the BA Rx site notifies the upper layer of received MPDUs in sequence based on the Rx SN. The reordering of the module is independent of the scoreboard context control module.

g) The BA Rx site can select standard mode or partial mode for the N-immediate BA. The scoreboard context control module stores different content in standard mode and partial mode, and provides information such as the SSN of BA responses destined for the BA Tx site.

h) The de-aggregation control module splits aggregated frames into single MPDUs.

i) The figure below shows the architecture of the N-immediate BA.

Figure 70


Originator
Recipient
Tx Buffer Control per RA/TID (WinStart_O, WinSize_O
Rx Reordering Buffer Control per TA/TID (WinStart_B, WinSize_B)
Scoreboard Context Control (WinStart_R, WinSize_R)
Aggregatio control
De-aggregation control
A-MPDU
BlockAck (BitMap, SSN)

2. N-delay BA

The N-delay BA is optional. A site identifies whether it supports the N-delay BA function in the HT Capabilities field. A site can use the BA response frame of N-delay BA only when the peer communication object also supports N-delay BA.

The N-delay BA mechanism uses the No-ACK mode for BA/BAR frames that do not need immediate response frames. That is, after a period of time, the transmitter of BA/BAR frames considers that the receiver has received the frames, and no longer waits for responses from the receiver. If the No-ACK response mode is not adopted, responses are expected to be received after a specified period of time for the BA/BAR frames transmitted in the N-delay BA mechanism. Whether the No-ACK mode is adopted can be specified dynamically. The response mode may vary with each PPDU, and may be randomly set for one group of BAR and BA frames.

BA frames for N-delay BARs are delayed for an unspecified period of time prior to transmission. That is, the BA frames can be transmitted within the next Transmit Opportunity (TXOP) obtained by the BA Rx site or the current or next TXOP obtained by the transmission initiator in the reverse direction transmission.

3. MTBA rules

Multi-TID BA (MTBA) rules are a type of response rules generated with the Power Saving Multi-Poll (PSMP) scheme. According to the scheme, MTBA frames are used as responses to data transmitted in the ranges of the Downlink Transmission Time (DTT; an AP transmits data) and the Uplink Transmission Time (UTT; a STA transmits data) of the PSMP sequence group. The ACK policy field in the MPDUs or MTBAR frames can be used to request MTBA responses. Non-AP sites transmit one MTBA frame in the UTT of the current PSMP sequence group, to respond to data received within the DTT. An AP transmits the MTBA frame in the DTT of the next PSMP sequence group, to respond to data received in the current UTT.

When an AP receives an MTBA frame transmitted from a site in the UTT, if the frame indicates that data loss occurs, the AP retransmits the previously transmitted frames in the current or next service interval. If the AP does not receive the expected MTBA frame, it retransmits all frames that are not responded to.

• Spatial Multiplexing Power Save

When the 802.11n service is used, the power capacity problem is exceedingly severe due to the installation of multiple antennas. Therefore, 802.11n adopts the Spatial Multiplexing (SM) power save technology to improve power saving processing. The technical principle is as follows: When no data needs to be forwarded, a STA has only one antenna in the working state and other antennas are in the sleep state, so as to save power. The SM power save technology defines two power management modes: dynamic SM power save and static SM power save.

Dynamic SM power save adopts the RTS frames to activate antennas.

Static SM power save has only one antenna in the receive state.

• Protection Mechanism

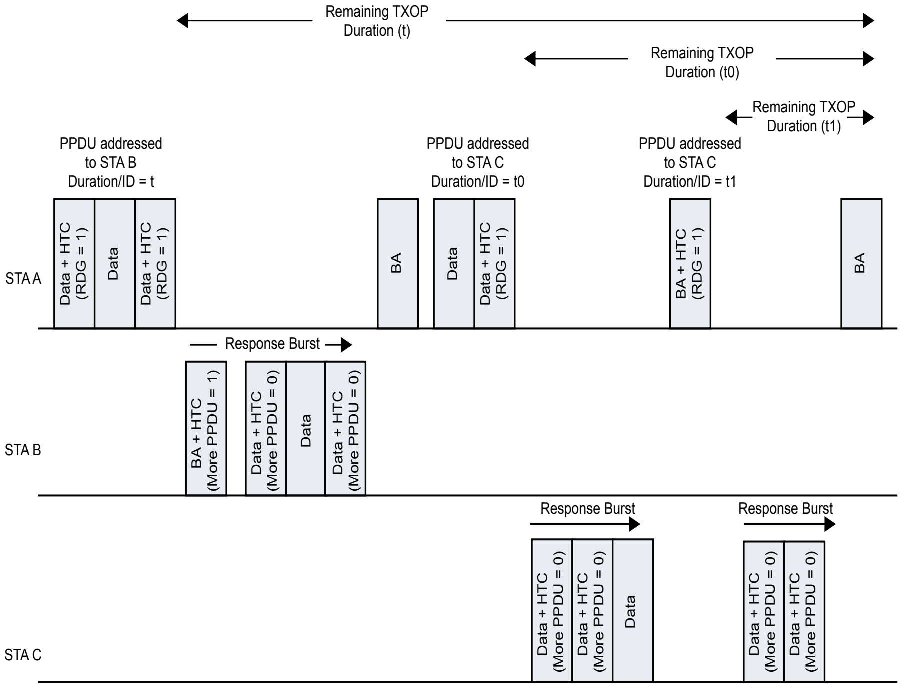
802.11n allows the access of 802.11a/b/g users. It is possible that signals transmitted by 802.11n devices cannot be parsed by 802.11a/b/g devices. As a result, 802.11a/b/g devices directly transmit signals to the air, causing channel conflicts. To solve the problem, the preamble that can be correctly parsed by 802.11a and 802.11b/g devices is added to the header of the to-be-transmitted packet in 802.11n hybrid mode (in which the 802.11a/b/g devices coexist). In this way, 802.11a/b/g devices can detect signals from 802.11n devices. In addition, the conflict avoidance mechanism is enabled to implement interworking between 802.11n devices and 802.11a/b/g devices.

• Reverse Direction Protocol

The reverse direction protocol, proposed in IEEE 802.11n, is an improvement to the common transmission mode. In reverse direction transmission, the initiator can transmit PPDUs during sequence exchange and obtain response PPDUs from a single site (responder). This transmission mode enables a communication site that is occupying a channel at a time point, to transmit frames without delay. The communication site does not need to release the channel and then repeat a series of actions such as the channel contention to transmit frames in the other direction after completing transmission in one direction. From a macro perspective, the reverse direction protocol further reduces some control frames and response frames in common transmission mode and improves the frame transmission efficiency.

The reverse direction protocol supports response frames that contain data frames. A response frame can contain one or more PPDUs. If the RDG field carried in a PPDU from the transmitter indicates that the transmitter supports the reverse direction protocol, after the last PPDU is transmitted, the receiver starts transmitting responses one interval later. Whether the receiver supports the reverse direction protocol is identified in relevant message fields in the both non-tail and tail PPDUs in the responses. Only the responder can transmit data during the response process. Other sites including the initiator are not allowed to transmit data. The responder ensures that the transmission of its PPDUs and the receiving of expected responses are completed in the remaining TXOP duration.

Figure 71


Remaining TXOP Duration (t)
Remaining TXOP Duration (t0)
Remaining TXOP Duration (t1)
PPDU addressed to STA B Duration/ID = t
PPDU addressed to STA C Duration/ID = t0
PPDU addressed to STA C Duration/ID = t1
STA A
Data + HTC (RDG = 1)
Data
Data + HTC (RDG = 1)
BA
Data
Data + HTC (RDG = 1)
BA + HTC (RDG = 1)
BA
Response Burst
STA B
BA + HTC (More PPDU = 1)
Data + HTC (More PPDU = 0)
Data
Data + HTC (More PPDU = 0)
Response Burst
Response Burst
STA C
Data + HTC (More PPDU = 0)
Data + HTC (More PPDU = 0)
Data
Data + HTC (More PPDU = 0)
Data + HTC (More PPDU = 0)

• Power Saving Multi-Poll

The Power Saving Multi-Poll (PSMP) is a new transmission mode proposed in IEEE 802.11n. PSMP frames, as a type of management behavior frames, are broadcasted by APs. The PSMP sequence exchange starts from PSMP frames and covers the DTT state, UTT state, and the interval in between. This transmission mode simplifies the data sending and receiving between a site and an AP and focuses on the mutual transmission between some sites and APs, which saves the power of sites that do not send or receive data.

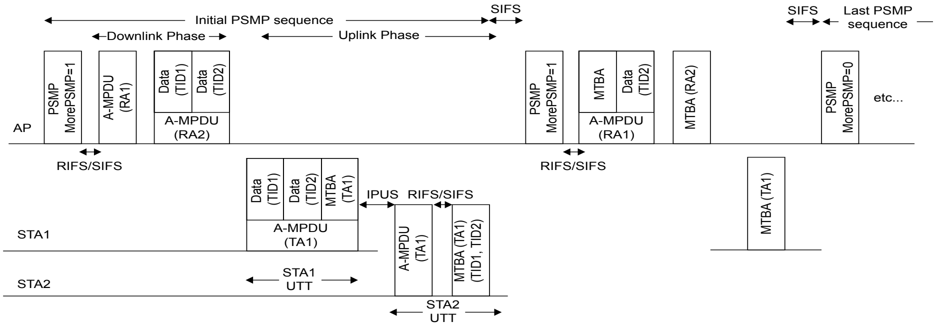
The minimum DTT2UTT delay is the minimum interval between the DTT state and the UTT sate of a site. It represents the minimum time limit of a site for processing MTBAs and data. If this delay cannot be ensured, an AP delays the entire UTT phase. Alternatively, the AP transmits the CTS-to-self frame between the DTT and UTT to meet the minimum DTT2UTT delay, so as to ensure the PSMP implementation.

A PSMP sequence group can be used to transmit unicast, multicast, and broadcast frames. The site that needs to transmit or receive unicast frames should reduce the number of state switching times as many as possible and increase the interval between the DTT and UTT. In a PSMP sequence group, a site should be capable of receiving frames in its scheduled DTT. An AP needs to ensure that all information destined for this site is transmitted in the DTT range. The site starts transmitting data at the beginning of its UTT and does not perform the Clear Channel Assessment (CCA). If a site fails to transmit entire data within the assigned UTT, it still releases the media control right at the end of the assigned UTT as scheduled. The site will obtain the data transmission opportunity in the next multi-phase PSMP.

The TSID set field of PSMP helps a site determine the MPDUs to be transmitted, and MPDUs to be transmitted by a site are not restricted to the TSID set. If an AP does not provide relevant information about transmitted data, the site can determine the data to be transmitted at its discretion.

A site with a determined Service Period (SP) is in the activated sate at the start of the SP. It enters the sleep state after receiving a PSMP frame or after the maximum SP expires. An AP sets the More PSMP field to 0 or transmits the CF-END frame to all sites, to notify that its SP ends.

Figure 72



Based on a requirement, an AP can transmit multiple subsequent PSMPs (sub-MSMPs) to allocate resources and correct errors more accurately. An initial PSMP followed by one or more sub-PSMPs is called a multi-phase PSMP.

An AP can determine the UTT duration of a PSMP sequence group based on the TSPEC frame for associating with a site. To allocate resources efficiently, an AP should be capable of accurately estimating the UTT duration of each site. However, in real-time video and other scenarios, the communication experience bursts, and it is difficult to predict the UTT duration when there is no feedback. To prevent resource waste caused by inaccurate prediction, an AP sets a limit in the UTT duration field of PSMP frames. When a site receives a PSMP frame, it judges whether its data queuing for transmission can be transmitted thoroughly. If the duration assigned by an AP to a site is insufficient, the site transmits some data as scheduled and additionally transmits a receive ready (RR) frame to the AP. At the RR request of the site, the AP assigns proper UTT duration to the site in the subsequent sub-PSMP frame. The multi-phase PSMP can be also used for data retransmission. Frames that fail to be transmitted in the DTT or UTT range can be retransmitted in the subsequent sequence group of sub-PSMP frames.

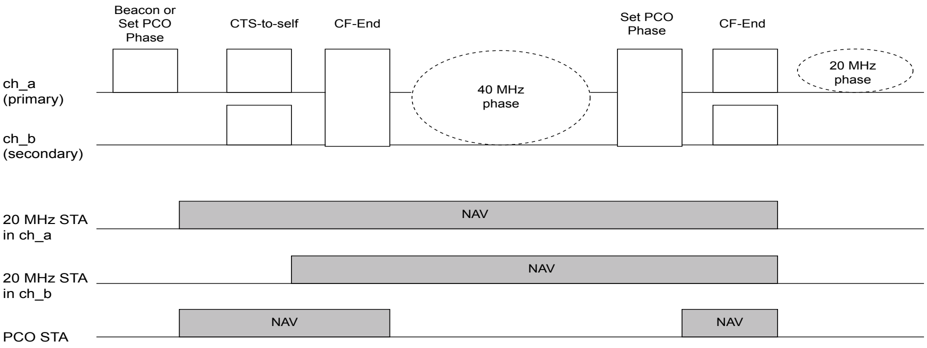
- Beamforming

802.11n devices transmit sounding frames to each other, to test the link performance. Based on information collected via sounding and calibration, 802.11n devices can use beamforming to enable signals to be transmitted along channels of interest, so as to improve the signal quality.

- Phase Coexistence Operation

Phase Coexistence Operation (PCO) is an optional BSS mode. APs that support PCO operate in the 20M and 40M phases alternately. When a STA that supports PCO associates with an AP, an information element can be set to notify the AP that the STA supports PCO. When a STA that does not support PCO associates with an AP that supports PCO, the AP can correctly operate in the 20M or 40M phase.

Figure 73



• Space Time Block Coding

Each spatial flow is generally transmitted by one group of antennas. The antenna quantity may be greater than the number of spatial flows in some cases. The mode in which multiple groups of antennas are used to transmit a single spatial flow is called Space Time Block Coding (STBC).

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**