一般 802.11MAC 帧帧格式

如下图是一般 802.11 MAC 帧帧格式：

2byte	2byte	6byte	6byte	6byte	2byte	6byte	0-2312byte	4byte
Frame control	Duration /ID	Address1	Address2	Address3	Seq-ctl	Address4	Frame body	FCS

一般 802.11MAC 帧

Frame control 字段:所有帧的开头均是长度两个字节的帧控制位，如下图所示。Frame Control 位包括以下次位：

2 bit	2 bit	4 bit	1	1	1	1	1	1	1	1
Protocol	Type	Sub type	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	Protect Frame	Order
0 1	2 3	4 7	8	9	10	11	12	13	14	15

Frame control 字段

Protocol 位

协议版本位由两个 bit 构成，用以显示该帧所使用的 MAC 版本。目前，802.11 MAC 只有一个版本；它的协议编号为 0。到目前为止，802.11 改版尚不需用到新的协议编号。

Type 与 Subtype 位

类型与次类型位用来指定所使用的帧类型。有三类帧类型，控制帧、数据帧和管理帧。数据帧负责在工作站之间传输数据；控制帧负责区域的清空、信道的获取以及载波监听的维护，并于收到数据时予以肯定确认，借此提高工作站之间数据传送的可靠性；管理帧负责监督，主要用来加入或退出无线网络以及处理接入点之间关联。各类帧类型又含有不同种类的子帧类型。下表显示了 type 与 subtype 位跟帧类型的对应关系。

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	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
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

To DS 与 From DS 这两位的含义如下表：

	To DS=0	To DS=1
From DS=0	所有管理帧、控制帧	基础网络中无线工作站所发送的数据帧
From DS=1	基础网络中无线工作站所收到的数据帧	无线桥接器上的数据帧

More fragments 位

如果上层的封包经过 MAC 分段处理，最后一个片段除外，其他片段均会将此 bit 设定为 1 。大型的数据帧以及某些管理帧可能需要加以分段；除此之外的其他帧则会将此 bit 设定为 0 。

Retry 位

有时候可能需要重传帧。任何重传的帧会将此 bit 设定为 1 ，以告知接收端剔除重复的帧。

Power management 位

802.11 网卡通常以 PC Card 的型式出现，主要用于以电池供电的笔记本电脑。为了提高电池的使用时间，通常可以关闭网卡以节省电力。该位用来指出传送端在完成目前的基本帧交换之后是否进入省电模式。1 代表工作站即将进入省电模式，而 0 则代表工作站会一直保持在清醒状态。基站必须行使一系列重要的管理功能，所以不允许进入省电模式，因此基站所传送的帧中，该位必然为 0。

More data 位

为了服务处于省电模式的工作站，基站会将接收的帧加以暂存。基站如果设定该位，即代表至少有一个帧待传给休眠中的工作站。

Protected Frame 位

无线传输本质上就比较容易遭受拦截。如果帧受到链路层安全协议的保护，该位会被设定为 1。

Order 位

帧与帧片段可依序传送。一旦进行“严格依序”传送，该位被设定为 1。

Duration/ID 字段：

含有 16 位，其依据帧类型和子帧类型的不同而取不同的值。取值如下表：

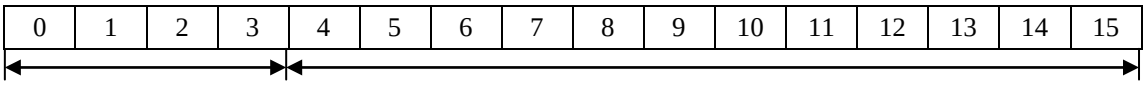
位 0-13	位 14	位 15	作用
0-32767		0	设定 NAV。此数值代表目前所进行的传输预计使用介质多少微秒。工作站必须监视所收到的任何帧头，并据以更新 NAV。任何超出预计使用介质时间的数值均会更新 NAV，同时阻止其他工作站访问介质。
0	0	1	在免竞争期间使用，值为 32768
1-16383	0	1	保留
0	1	1	保留
1-2007	1	1	休眠醒来的工作站会在 PS-Poll 帧中加入连接识别码（association ID，简称 AID），以显示其所隶属的 BSS 。其值介于 1-2,007。
2008-16383	1	1	保留

Address 位

一个 802.11 帧最多可以包含四个地址位。这些位地址位均经过编号，随着帧类型不同，这些位的作用也有所差异。Address 1 代表接收端，Address 2 代表传送端，Address 3 位被接收端拿来过虑地址。比如，在基础网络里，第三个地址位会被接收端用来判定该帧是否属于其所连接网络。

顺序控制位

该位组成如下图，长度为 16 个 bit，用来重组帧片段以及丢弃重复帧。



fragment number　　sequence number

它由 4 个 bit 的 fragment number（片段编号）位以及 12 个 bit 的 sequence number （顺序编号）位所组成。控制帧未使用顺序编号，因此并无顺序控制位。当上层帧交付 MAC 传送时，会被赋予一个 sequence number （顺序编号）。此位的作用是计数已传帧。计数器由 0 起算，MAC 每处理一个上层封包就会累加 1。如果上层封包被切割处理，所有帧片段都会具有相同的顺序编号。如果是重传帧，则顺序编号不会有任何改变。帧片段之间的差异在于 fragment number （片段编号）。第一个片段的编号为 0 。其后每个片段依序累加 1 。重传的片段会保有原来的 sequence number 协助重组。

数据位（Frame Boby）

负责在工作站间传送上层数据。在最初的标准中，802.11 帧最多可以传送 2304 个 bit 构成的上层数据。(实际上必须能够容纳更多的数据，以便将安全性与 QoS 相关信息加入)。

帧检验序列（FCS ）

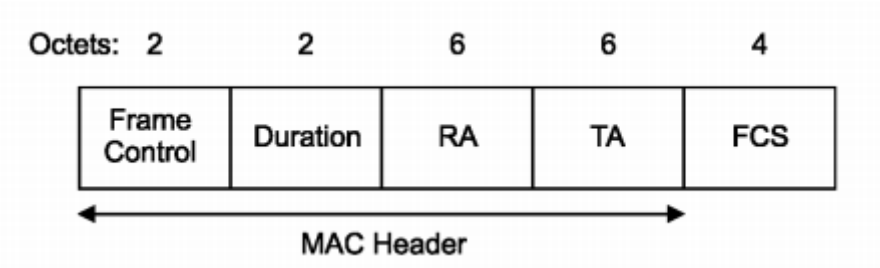
802.11 帧是以帧检验序列（frame check sequence ，简称 FCS ）作为结束。FCS 让工

作站得以检查所收到的帧的完整性。FCS 的计算范围涵盖 MAC 头所有位以及数据位。当帧送至无线介质时，会先计算 FCS ，然后再由无线链路传送出去。接收端随后会为所收到的帧计算 FCS ，然后与记录在帧中的 FCS 做比较。在 802.11 网络上，通过完整性检验的帧需接收端送出应答。接收无误的数据帧必须得到正面应答，否则就必须重传。

常用帧的帧格式

RTS 帧格式：

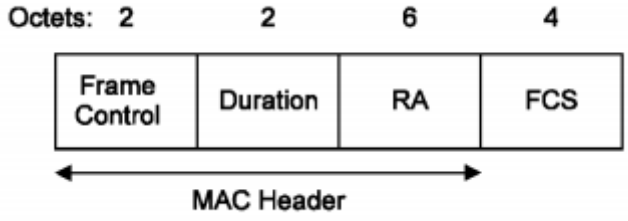
请求发送帧(RTS)有 20 个字节长，它包含有帧控制域、帧交换所需时间长度(duration)/关联号(ID)域、两个地址域和帧校验域。发送这个帧的一个目的是将完成帧交换所需时间长度(duration)信息告知其邻近的 STA，也就是能收到 RTS 的 STA 就用收到的信息更新其 NAV，从而防止了这些 STA 在告知的时间内发送信息，也就避免了冲突的发生。下图定义了 RTS 的格式：



RTS 帧中的 RA 标明的是一个无线媒体上的 STA，该 STA 为即将发送的数据帧或者管理帧的接收者，而且在 RTS 帧中的 RA 必须是某个 STA 的 MAC 地址。TA 标明的是传送 RTS 帧的 STA，它被由 RTS 中的 RA 标识的 STA 用来发送 RTS 的响应帧。在该帧中传送的时间长度(duration)信息是完成一个 4 步骤帧交换(RTS、CTS、DATA、ACK)所需要的时间，它由这些时间构成：传送 1 个 CTS 的时间、传送 1 个数据或者管理帧的时间、传送 1 个对数据或者管理帧应答的时间、以及在 CTS 和数据或者管理帧之间的帧间间隙(SIFS)和在数据或者管理帧和 ACK 之间的帧间间隙(SIFS)时间（一共 3 个 SIFS）。时间长度(duration)是以微秒为单位的。如果计算的时间值不是整数，则取大于该值的最小整数。

CTS 帧格式：

允许发送帧(CTS)有 14 个字节长，它包含有帧控制域、帧交换所需时间长度(duration)/关联号(ID)域、1 个地址域和帧校验域。发送这个帧的一个目的是将完成帧交换所需时间长度(duration)信息告知其邻近的 STA，也就是能收到 CTS 的 STA 就用收到的信息更新其 NAV，从而防止了这些 STA 在告知的时间内发送信息，也就避免了冲突的发生。下图定义了 CTS 的格式：

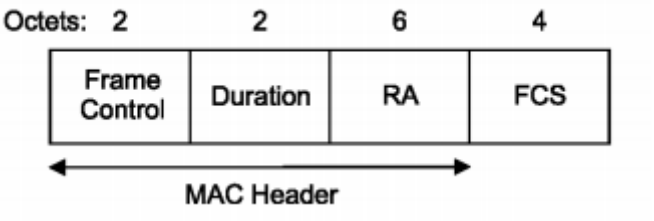


CTS 中的 RA 标识的是接收该 CTS 的某个 STA 的 MAC 地址，在 CTS 中 RA 必须是某个 STA 的 MAC 地址。而 RA 的值是从接收到的 RTS 帧中的 TA 复制过来的，而此 CTS 就

是作为接收到的 RTS 的响应帧。在该帧中传送的时间长度(duration)信息是完成一个 4 步骤帧交换(RTS、CTS、DATA、ACK)所需要的时间，它由这些时间构成：传送 1 个数据或者管理帧的时间、传送 1 个对数据或者管理帧应答的时间、以及在数据或者管理帧和 ACK 之间的帧间间隙(SIFS)时间，也就是将收到的 RTS 帧中的时间长度(duration)减去传送 CTS 时间和 1 个 SIFS 时间。时间长度(duration)是以微秒为单位的。如果计算的时间值不是整数，则取大于该值的最小整数。

ACK 帧格式：

确认(ACK)帧有 14 字节长，它包含有帧控制域、帧交换所需时间长度(duration)/关联号(ID)域、1 个地址域和帧校验域。使用这个帧有两个目的，一是对刚正确接收到的数据、管理帧、PS-Poll 帧的确认。这也就告诉了 ACK 的接收者或者是刚收到的数据、管理帧、PS-Poll 帧的发送者已经正确接收了，那么也就不需要重传刚收到的数据、管理帧、PS-Poll 帧。ACK 帧的第二个目的是在段突发传送过程中，它可以将时间长度(duration)通知给段接收者的邻近 STA，这种情况下 ACK 就扮演了 CTS 的角色。



ACK 帧的 RA 标识的是某个接收该帧的 STA 的 MAC 地址，而且在 ACK 中的 RA 必须是某个 STA 的 MAC 地址，RA 是从刚接收到的数据帧，管理帧或者 PS-Poll 控制帧中的第 2 地址域复制过来的。如果接收到的数据帧或者管理帧中的帧控制域的 More Fragment 位被置为 0，则长度域的值置为 0。如果接收到的数据帧或者管理帧中的帧控制域的 More Fragment 位被置为 1，则长度域的值置将接收到的数据帧或者管理帧的长度域的值减去传送 1 个 ACK 帧的时间和 1 个 SIFS 得到。如果计算出的该值不是整数，则取大于该值的最小整数。

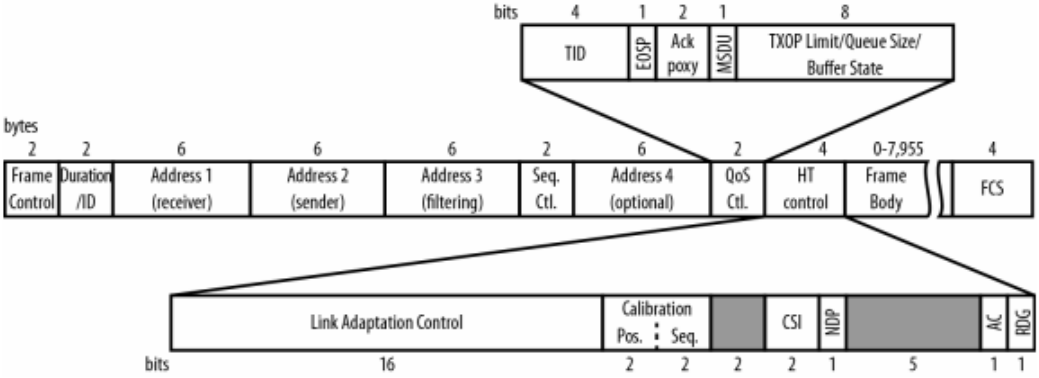
Beacon 帧格式：

信标帧 Beacon 是相当重要的维护机制，主要用来宣告某个网络的存在。定期发送的信标，可让移动工作站得知该网络的存在，从而调整加入该网络所必要的参数。在基础型网络里，接入点必须负责发送 Beacon 帧。Beacon 帧所及范围即为基本服务区域。在基础型网络里，所有沟通都必须通过接入点，因此工作站不能距离太远，占则便无法接收到信标。信标并不全会用到所有位。选择性位只有在用到时才一会出现。下表是 Beacon 帧体各段的含义。

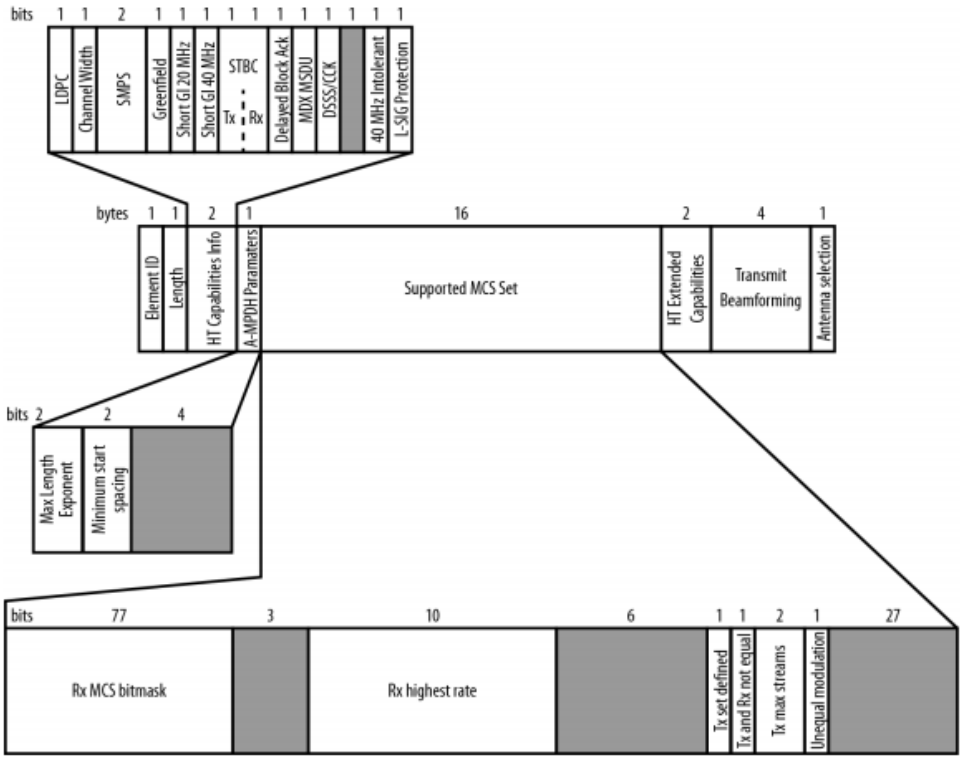
Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	Service Set Identifier (SSID)	
5	Supported rates	
6	Frequency-Hopping (FH) Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using FH PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using Clause 15, Clause 18, and Clause 19 PHYs.
8	CF Parameter Set	The CF Parameter Set information element is present only within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is present only within Beacon frames generated by STAs in an IBSS.
10	Traffic indication map (TIM)	The TIM information element is present only within Beacon frames generated by APs.
11	Country	The Country information element shall be present when dot11MultiDomainCapabilityEnabled is true or dot11SpectrumManagementRequired is true.
12	FH Parameters	FH Parameters as specified in 7.3.2.10 may be included if dot11MultiDomainCapabilityEnabled is true.
13	FH Pattern Table	FH Pattern Table information as specified in 7.3.2.11 may be included if dot11MultiDomainCapabilityEnabled is true.
14	Power Constraint	Power Constraint element shall be present if dot11SpectrumManagementRequired is true.
15	Channel Switch Announcement	Channel Switch Announcement element may be present if dot11SpectrumManagementRequired is true.
16	Quiet	Quiet element may be present if dot11SpectrumManagementRequired is true.
17	IBSS DFS	IBSS DFS element shall be present if dot11SpectrumManagementRequired is true in an IBSS.
18	TPC Report	TPC Report element shall be present if dot11SpectrumManagementRequired is true.
19	ERP Information	The ERP Information element is present within Beacon frames generated by STAs using extended rate PHYs (ERPs) defined in Clause 19 and is optionally present in other cases.
20	Extended Supported Rates	The Extended Supported Rates element is present whenever there are more than eight supported rates, and it is optional otherwise.
21	RSN	The RSN information element shall be present within Beacon frames generated by STAs that have dot11RSNAEnabled set to TRUE.
22	BSS Load	The BSS Load element is present when dot11QosOption-Implemented and dot11QBSSLoadImplemented are both true.
23	EDCA Parameter Set	The EDCA Parameter Set element is present when dot11QosOptionImplemented is true and the QoS Capability element is not present.
24	QoS Capability	The QoS Capability element is present when dot11QosOption-Implemented is true and EDCA Parameter Set element is not present.
Last	Vendor Specific	One or more vendor-specific information elements may appear in this frame. This information element follows all other information elements.

IEEE 802.11n MAC 帧

IEEE 802.11n 数据帧格式相比于传统的 802.11 数据帧变大了。加入了高吞吐量（HT）控制字段和 Qos 控制字段。如下图是 11nMAC 帧格式。帧体部分增加了大约四倍（最大 7955 字节）。



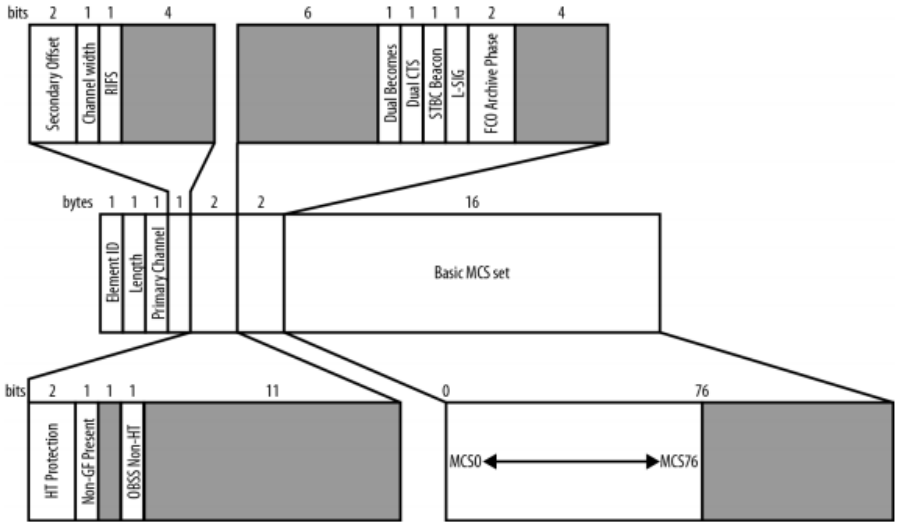
管理帧通过在传统管理帧中插入 HT 信息单元表明它们来自于 11n 网络。下图是 HT 信息单元的格式。



HT 信息单元中 2 字节的 HT Capabilities Info 用于告知信道类型，编码规则，使用 20MHz 还是 40MHz 信道。1 字节 A-MPDU 参数用于声明使用 A-MPDU 聚合。16 字节 Supported MCS Set 包含有大量的数据传输速率信息。2 字节 HT Extended Capabilities 字段描述对扩展功能如 PCO、RD 的支持，不常用。4 字节 Transmit Beamforming Capabilities 字段是对波束赋形的支持。1 字节 Antenna Selection Capabilities 用于天线比射频多的系统中，在现有系统中基本不用。

HT 操作信息单元被插入由 AP 发送的管理帧如 Beacon 等帧中，来告知客户端设备当前

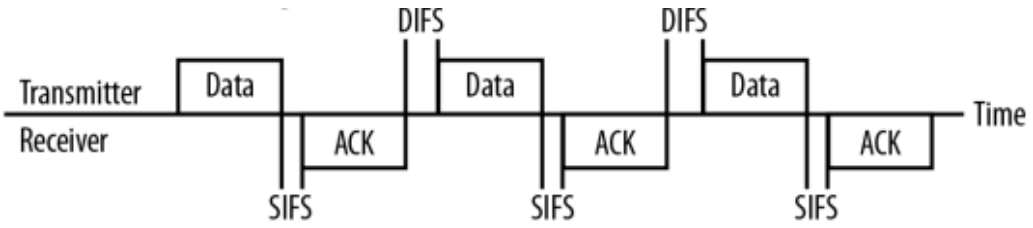
的网络状态。其结构如下图：



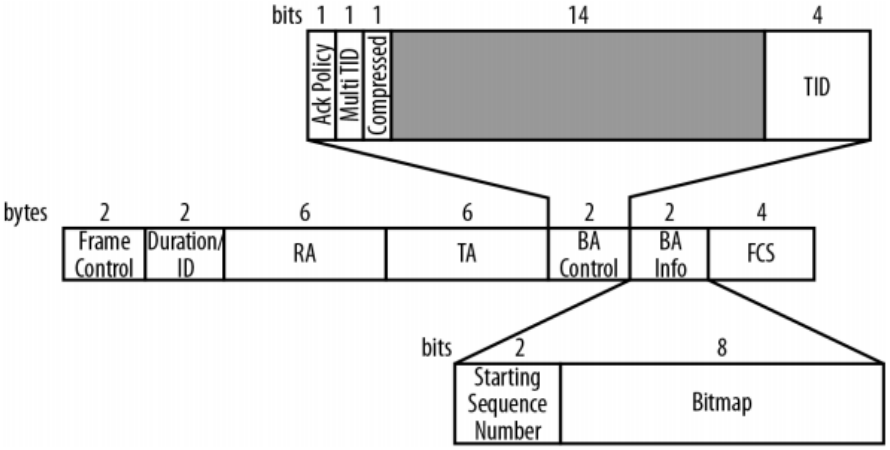
1 字节 Primary Channel 字段用来表明网络操作的主信道。2 位 Secondary Channel Offset，设置成 1 的时候表明次级信道比主信道有一个更高的频率。当次级信道频率低于主信道被设置成 3，没有次级信道时设置成 0。1 位的 Channel width 设置成 1 的时候表示使用的是 20MHz 信道。1 位的 RIFS 设置成 1 允许 RIFS 操作，设置成 0 禁用 RIFS。HT Protection 用来设置避免传统的 11 设备造成的干扰。

11n 块确认帧：

为保证数据传输的可靠性，传统的 802.11 协议规定每收到一个单播数据帧，都必须立即回应以 ACK 帧。如下图所示：

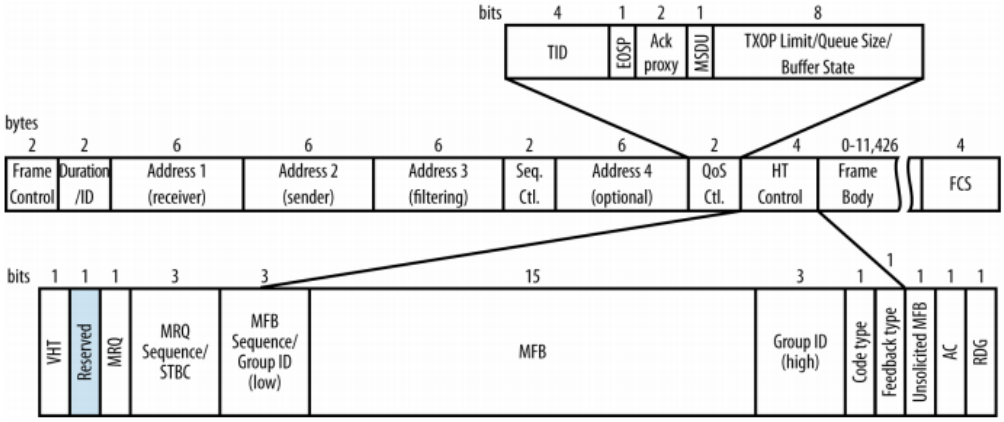


11n 中 A-MPDU 的接收端在收到 A-MPDU 后，需要对其中的每一个 MPDU 进行处理，因此同样针对每一个 MPDU 发送应答帧。Block Acknowledgement 通过使用一个 ACK 帧来完成对多个 MPDU 的应答，以降低这种情况下的 ACK 帧的数量。块确认帧格式如下：

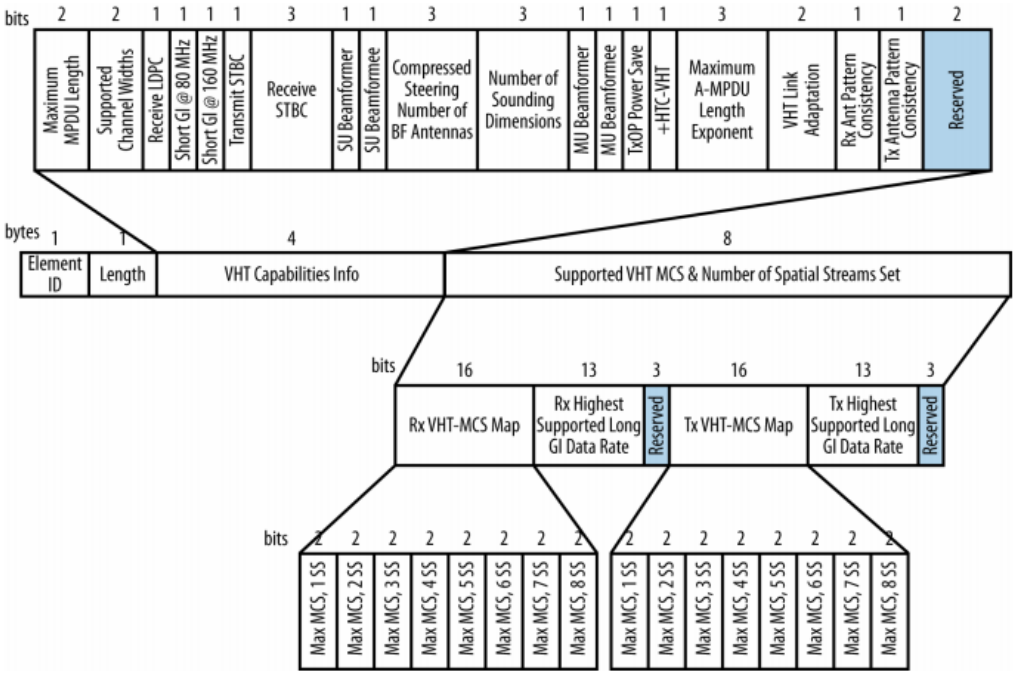


IEEE 802.11ac MAC 帧

802.11ac MAC 帧大部分字段保留给 11a/b/g/n 使用。如下图 11acMAC 数据帧格式，主要有两个变化，一是最大帧体的长度从 11n 的 7000 多字节增加到 11426 字节，增强了聚合来自高层帧的能力。二是重用 11n 中用到的高吞吐量（HT）控制字段，但是使用了新的格式。高吞吐量（HT）控制字段如果以 0 开始，它与 11n 中定义的格式一致；如果以 1 开始，它成为 11ac 中超高吞吐量（VHT）控制字段。11ac MAC 帧格式图给出的是它的定义。



设备要通过发送管理帧表明位于 11ac 网络中，在传统的管理帧中加入 VHT 信息单元。这个信息单元位于探测请求和探测回应管理帧中。VHT 信息单元如下图：



2 位 Maximum MPDU Length 用来表明 11acMAC 帧体的长度。00 表示长度为 3895 字节，01 表示长度为 7991 字节，10 表示长度为 11454 字节，11 保留。2 位 Supported Channel Width 设置位，用来设置支持 20MHz，40MHz，80MHz 操作。13 位 Rx and Tx Highest Supported Data Rate 字段用来表示支持的最大数据速率，以 1Mbps 为单位。比如，一个设备支持最大速率 867Mbps，设置为 0001101100011（十进制为 867）。其他字段在这里没有叙述。