[**802.11帧结构、wifi连接过程、加密方式**](http://blog.csdn.net/xinyuan510214/article/details/50570092)

2016-01-23 15:56 3260人阅读 [评论](http://blog.csdn.net/xinyuan510214/article/details/50570092#comments)(0) [收藏](javascript:void(0);) [举报](http://blog.csdn.net/xinyuan510214/article/details/50570092#report)

http://static.blog.csdn.net/images/category_icon.jpg 分类：

WEP/WPA算法（3） http://static.blog.csdn.net/images/arrow_triangle%20_down.jpg WIFI（3） http://static.blog.csdn.net/images/arrow_triangle%20_down.jpg

**[cpp]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. <pre name="code" **class**="cpp">Linux黑客大曝光: 第8章 无线网络
2. 无线网络安全攻防实战进阶
3. 无线网络安全 黑客大曝光 第2版
4. http://zh.wikipedia.org/wiki/IEEE\_802.11
5. http://www.hackingexposedwireless.com/doku.php
6. http://blog.csdn.net/gueter/article/details/4812726
7. http://my.oschina.net/u/994235/blog/220586#OSC\_h2\_6
8. http://h257249.top.sh/simple/?t3.html
9. http://blog.csdn.net/chengwenyao18/article/details/7176090
10. http://www.cnblogs.com/aixin0813/p/3208579.html
11. http://www.cnblogs.com/aixin0813/p/3211752.html
12. http://www.cnblogs.com/aixin0813/p/3214197.html
13. http://www.cnblogs.com/aixin0813/p/3222771.html
14. http://www.cnblogs.com/aixin0813/p/3225266.html

**[cpp]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. 802.11标准简介
2. 2. 802.11协议格式
3. 3. Wi-Fi认证过程
4. 4. 802.11标准中的数据安全加密协议

**1. 802.11标准简介**

IEEE 802.11是现今无线局域网通用的标准，它是由国际电机电子工程学会(IEEE)所定义的无线网络通信的标准。  
其中定义了媒体访问控制层(MAC层)和物理层。物理层定义了工作在2.4GHz的ISM频段上的两种扩频作调制方式和一种红外传输的方式，总数据传输速率设计为2Mbit/s。两个设备可以自行构建临时网络，也可以在基站(Base Station, BS)或者接入点(Access Point，AP)的协调下通信。为了在不同的通讯环境下取得良好的通讯质量，采用CSMA/CA(Carrier Sense Multiple Access／Collision Avoidance)硬件沟通方式  
注意:

802.11和Wi-Fi技术并不是同一个东西。Wi-Fi标准是802.11标准的一个子集，并且是Wi-Fi联盟负责管理

我们知道，802.11协议标准是一个系列标准，经过了一些列的发展演变过程

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **协议** | **发布年份/日期** | **Op.标准频宽** | **实际速度 (标准)** | **实际速度（最大）** | **半径范围（室内）** | **半径范围（室外）** |
| Legacy | 1997 | 2.4-2.5 GHz | 1 Mbit/s | 2 Mbit/s | ? | ? |
| 802.11a | 1999 | 5.15-5.35/5.47-5.725/5.725-5.875 GHz | 25 Mbit/s | 54 Mbit/s | 约30米 | 约45米[[3]](http://zh.wikipedia.org/wiki/IEEE_802.11" \l "cite_note-3" \t "_blank) |
| 802.11b | 1999 | 2.4-2.5 GHz | 6.5 Mbit/s | 11 Mbit/s | 约30米 | 约100米 |
| 802.11g | 2003 | 2.4-2.5 GHz | 25 Mbit/s | 54 Mbit/s | 约30米 | 约100米 |
| 802.11n | 2009 | 2.4 GHz or 5 GHz bands | 300 Mbit/s (20MHz\*4 MIMO) | 600 Mbit/s (40MHz\*4 MIMO) | 约70米 | 约250米 |
| 802.11p | 2009 | 5.86-5.925 GHz | 3 Mbit/s | 27 Mbit/s | 约300米 | 约1000米 |
| 802.11ac | 2011.11 | 5 GHz | 433Mbit/s, 867Mbit/s (80MHz), (160MHz为可选) | 867Mbit/s, 1.73 Gbit/s, 3.47 Gbit/s, 6.93 Gbit/s (8 MIMO, 160MHz) | 约35米[[4]](http://zh.wikipedia.org/wiki/IEEE_802.11" \l "cite_note-4" \t "_blank) |  |

在802.11协议的发展过程中，衍生出了一系列的和安全、加密相关的技术

**[cpp]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. WEP，Wired Equivalent Privacy: 802.11中最早期的加密标准
2. 2. CCMP(CTR with CBC-MAC Protocol): 基于AES的全新加密协议，在IEEE 802.11i中提出
3. 3. WPA(Wi-Fi Protected Access)
4. 4. TKIP(Temporal Key Integrity Protocol)
5. 5. WPA2(Wi-Fi Protected Access 2)

802.11标准将所有的数据包分为3种:

**[cpp]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. 数据: 数据数据包的作用是用来携带更高层次的数据(如IP数据包，ISO7层协议)。
2. 它负责在工作站之间传输数据
3. 2. 管理: 管理数据包控制网络的管理功能
4. 1) 信标帧(Beacons): 在无线设备中，定时依次按指定间隔发送的有规律的无线信号(类似心跳包)，主要用于定位和同步使用
5. 2) 解除认证(Deauthentication)数据包
6. 3) Probe(request and response)
7. 4) Authenticate(request and response)
8. 5) Associate(request and response)
9. 6) Reassociate(request and response)
10. 7) Dissassociate(notify)
11. 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连接的转移事宜
12. 3. 控制: 控制数据包得名于术语"媒体接入控制(Media Access Control, MAC)"，是用来控制对共享媒体(即物理媒介，如光缆)的访问
13. 1) 请求发送(Request To Send，RTS)数据包
14. 2) 清除发送(Clear To Send，CTS)数据包
15. 3) ACK确认(RTS/CTS)
16. 4) PS-Poll: 当一部移动工作站从省电模式中苏醒，便会发送一个 PS-Poll 帧给基站，以取得任何暂存帧
17. 控制帧通常与数据帧搭配使用，负责区域的清空、信道的取得以及载波监听的维护，并于收到数据时予以正面的应答，借此促进工作站间数据传输的可靠性

这些不同类别的数据包被统称为"数据包类型"。

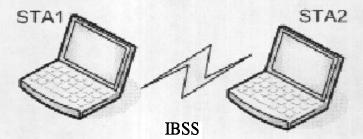
WLAN有以下三种网络拓扑结构:

**[cpp]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

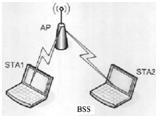
1. 1) 独立基本服务集(Independent BSS, IBSS)网络(也叫ad-hoc网络)
2. 2) 基本服务集(Basic Service Set, BSS)网络
3. 3) 扩展服务集(Extent Service Set, ESS)网络

***1) AD-Hoc网络***



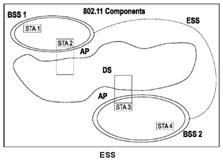
win7自带的AD-Hoc组建功能，可以让我们很方便的在一个小范围内快速组建"局域网"，联网打游戏啥的很方便

***2)* BSS网络**

****

对于个人PC来说，使用最多的所谓"无线Wi-Fi"指的就是BSS网络模式，我们通过AP(Access Point)接入点来接入网络

***3)* ESS网络**

****

其中，ESS中的DS(分布式系统)是一个抽象系统，用来连接不同BSS的通信信道(通过路由服务)，这样就可以消除BSS中STA与STA之间直接传输距离受到物理设备的限制。  
根据拓扑结构可以得出802.11的两类服务：

**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. 站点服务SS(每个STA都要有的服务)
2. 1) 认证(Authentication)
3. 2) 解除认证(Deauthentication)
4. 3) 加密(Privacy)
5. 4) MSDU传递(MSDU delivery)
6. 2. 分布式系统服务DSS(DS特有服务)
7. 1) 关联(Association)
8. 2) 解除关联(Deassociation)
9. 3) 分布(Distribution)
10. 4) 集成(Integration)
11. 5) 重关联(Ressociation)

**2. 802.11协议格式**

我们知道数据链路层是一个很靠近底层的通信协议，它使用Bit来表示信息(也使用Bit来标识数据包的开始和结束)，所以数据链路层的协议格式并没有强制要求一个固定的长度，即802.11协议长度是可变的。不同功能的数据帧长度会不一样。这一特性说明mac802.11数据帧显得更加灵活，然而，也会更加复杂。

mac 802.11的数据帧长度不定主要是由于以下几点决定的

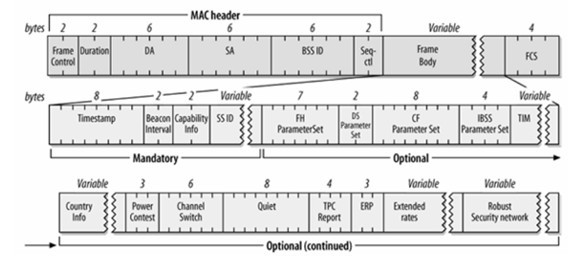
**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

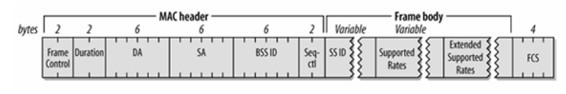
1. 1. mac地址数目不定，根据帧类型不同，mac 802.11的mac地址数会不一样。比如说 ACK帧仅有一个mac地址，而数据帧有3个mac地址，在WDS模式下，帧头有4个mac地址。
2. 2. 802.11的管理帧所携带的信息长度不定，在管理帧中，不仅仅只有一些类似于mac地址，分片标志之类的这些信息，而且另外还会包括一些其它的信息，这些信息有关于安全设置的，有关于物理
3. 通信的，比如说我们的SSID名称就是通过管理帧获得的。AP会根据不同的情况发送包含有不同信息的管理帧。
4. 3. 加密(wep,wpa等)信息，QOS(quality of service)信息，若有加密的数据帧格式和没有加密的数据帧格式还不一样，加密数据帧格式还多了个加密头，用于解密用。然则QOS也是同样道理

***0x1: 管理帧协议格式***

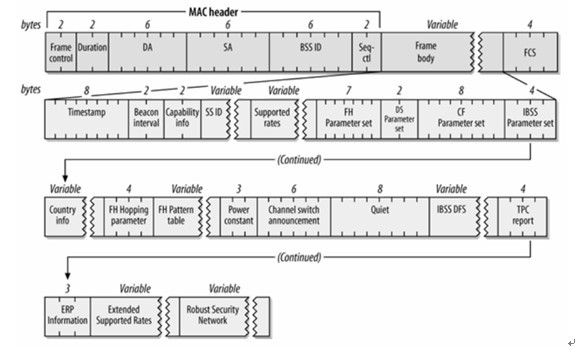
***(Beacon(信标)帧)***

******

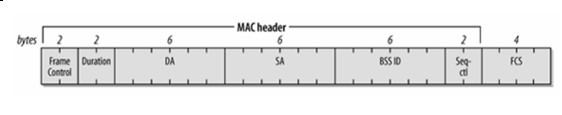
***(Probe Request(探测请求)帧)***



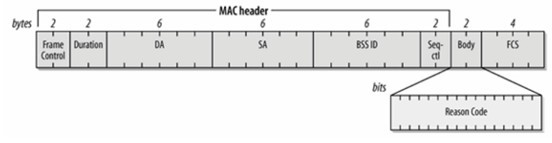
***(Probe Response(探测响应)帧)***



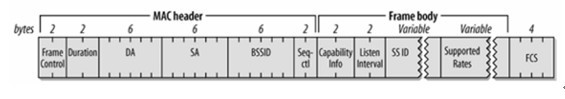
***(ATIM帧)***



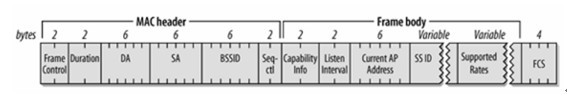
***(Disassociation(解除关联)与Deauthentication(解除认证)帧)***



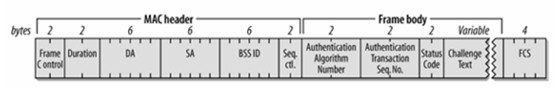
***(Association Request(关联请求)帧)***



***(Reassociation Request(重新关联请求)帧)***



***(Authentication(身份认证)帧)***



**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

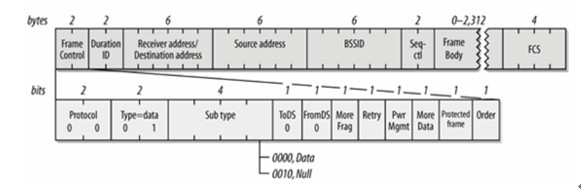
[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. 帧控制结构(Frame Control)
2. 1) Protocol Version: (协议版本)通常为0
3. 2) Type: 帧类型，管理帧: 00
4. 3) Subtype: 进一步判断帧的子类型
5. 3.1) Beacon(信标)帧
6. 3.2) Probe Request(探测请求)帧
7. 3.3) Probe Response(探测响应)帧
8. 3.4) ATIM帧
9. 3.5) Disassociation(解除关联)
10. 3.6) Deauthentication(解除认证)帧
11. 3.7) Association Request(关联请求)帧
12. 3.8) Reassociation Request(重新关联请求)帧
13. 3.9) Authentication(身份认证)帧
14. 4) To DS: 表明该帧是否是BSS向DS发送的帧
15. 5) From DS: 表明该帧是否是DS向BSS发送的帧
16. 6) More Fragment: 用于说明长帧被分段的情况，是否还有其它的帧，如果有则该值设置为1
17. 7) Retry(重传域): 表示该分段是先前传输分段的重发帧。
18. 8) Power Management: 表示传输帧以后，站所采用的电源管理模式
19. 8.1) 为1: STA处于power\_save模式
20. 8.2) 为0: STA处于active模式
21. 9) More Data: 表示有很多帧缓存到站中。即至少还有一个数据帧要发送给STA是设置为1。
22. 10) Protected Frame: 表示根据WEP(Wired Equivalent Privacy)算法对帧主体进行加密。如果帧体部分包含被密钥套处理过的数据，则设置为1，否则设置为0
23. 11) Order(序号域): 在长帧分段传送时，该域设置为1表示接受者应该严格按照顺序处理该帧，否则设置为0
24. 2. Duration/ID(持续时间/标识)
25. 表明该帧和它的确认帧将会占用信道多长时间，Duration 值用于网络分配向量(NAV)计算
26. 3. Address Fields(地址域):
27. 1) Destination Address
28. 2) Source Address
29. 3) BSS ID
30. 4. Sequence Control(序列控制域): 用于过滤重复帧
31. 1) MSDU(MAC Server Data Unit), 12位序列号(Sequence Number)
32. 2) MMSDU(MAC Management Server Data Unit), 4位片段号(Fragment Number)组成
33. 5. Frame Body(Data): 发送或接收的信息。对于不同类型的数据帧来说，这个域的格式差别较大
34. 1) Beacon(信标)帧
35. 1.1) Timestamp(时戳)位: 可用来同步 BSS 中的工作站 BSS 的主计时器会定期发送目前已作用的微秒数。当计数器到达最大值时，便会从头开始计数
36. 1.2) Beacon interval位: AP点每隔一段时间就会发出的Beacon(信标)信号，用来宣布 802.11网络的存在。我们打开无线连接的时候之所以能看到很多Wi-Fi点就是因为它
37. 1.3) Capability information位: 发送Beacon信号的时候，它被用来通知各方，该网络具备哪种性能
38. 1.4) SSID服务集标识(Service Set Identity): 由字节所形成的字串，用来标示所属网络的BSSID，即我们在Wi-Fi连接前看到的接入点名称
39. 1.5) 跳频参数组合(PH Parameter Set): 包含了加入 802.11跳频(frequency-hopping)网络所需要的参数
40. 1.6) 直接序列参数集合(DS Parameter Set): 指明网络所使用的信道数
41. 1.7) 免竞争参数集合(CF Parameter Set): 出现在支持免竞争接入点所发送的 Beacon帧中，并非必须
42. 1.8) IBSS 参数集合(IBSS Parameter Set): 指明ATIM window (数据待传指示通知信息间隔期间)
43. 1.9) TIM数据待传信息(Traffic Indication Map): 指示有哪些工作站需要接收待传数据
44. 1.10) Country: 国家识别码
45. 1.11) 功率限制(Power Constraint): 让网络得以向工作站传达其所允许的最大传输功率
46. 1.12) 信道切换宣告(Channel Switch Announcement): 为了警告网络中的工作站即将变换信道
47. 1.13) 禁声(Quiet): 为了避免与特定的军事雷达技术彼此干扰
48. 1.14) 发射功率控制报告(TPC Report): 指明链路的衰减情况，可以帮助工作站了解该如何调整传输功率
49. 1.15) 扩展物理层(ERP)
50. 1.16) 支持速率(Supported Rates): 无线局域网络支持数种标准速率。当移动工作站试图加入网络，会先检视该网络所使用的数据速率。有些速率是强制性的，每部工作站都必须支持
51. ，有些则是选择性的
52. 1.17) RSN强健安全网络(Robust Security Network)
53. 2) Probe Request(探测请求)帧
54. 2.1) SSID服务集标识(Service Set Identity): 由字节所形成的字串，用来标示所属网络的BSSID，即我们在Wi-Fi连接前看到的接入点名称
55. 2.2) Supported Rate(支持速率)
56. 2.3) 扩展支持速率(Extended Supported Rate)
57. 3) Probe Response(探测响应)帧
58. 3.1) Timestamp(时戳)位: 可用来同步 BSS 中的工作站 BSS 的主计时器会定期发送目前已作用的微秒数。当计数器到达最大值时，便会从头开始计数
59. 3.2) Beacon interval位: AP点每隔一段时间就会发出的Beacon(信标)信号，用来宣布 802.11网络的存在。我们打开无线连接的时候之所以能看到很多Wi-Fi点就是因为它
60. 3.3) Capability information位: 发送Beacon信号的时候，它被用来通知各方，该网络具备哪种性能
61. 3.4) SSID服务集标识(Service Set Identity): 由字节所形成的字串，用来标示所属网络的BSSID，即我们在Wi-Fi连接前看到的接入点名称
62. 3.5) 支持速率(Supported Rates): 无线局域网络支持数种标准速率。当移动工作站试图加入网络，会先检视该网络所使用的数据速率
63. 3.6) 跳频参数组合(PH Parameter Set): 包含了加入 802.11跳频(frequency-hopping)网络所需要的参数
64. 3.7) 直接序列参数集合(DS Parameter Set): 指明网络所使用的信道数
65. 3.8) 免竞争参数集合(CF Parameter Set): 出现在支持免竞争接入点所发送的 Beacon帧中，并非必须
66. 3.9) IBSS 参数集合(IBSS Parameter Set): 指明ATIM window (数据待传指示通知信息间隔期间)
67. 3.10) Country: 国家识别码
68. 3.11) FH Hopping Parameters
69. 3.12) FH Pattern Table
70. 3.13) 功率限制(Power Constraint): 让网络得以向工作站传达其所允许的最大传输功率
71. 3.13) 信道切换宣告(Channel Switch Announcement): 为了警告网络中的工作站即将变换信道
72. 3.14) 禁声(Quiet): 为了避免与特定的军事雷达技术彼此干扰
73. 3.15) IBSS 动态选项(IBSS DFS):在 IBSS 中负责动态选频的工作站可以在管理帧中传递 IBSS DFS 信息元素
74. 3.16) 发射功率控制报告(TPC Report): 指明链路的衰减情况，可以帮助工作站了解该如何调整传输功率
75. 3.17) 扩展物理层(ERP)
76. 3.18) 扩展支持速率(Extended Supported Rate)
77. 3.19) RSN强健安全网络(Robust Security Network)
78. 4) ATIM帧
79. 5) Disassociation(解除关联)
80. 5.1) Beacon Code
81. 6) Deauthentication(解除认证)帧
82. 6.1) Beacon Code
83. 7) Association Request(关联请求)帧
84. 7.1) Capability information位: 发送Beacon信号的时候，它被用来通知各方，该网络具备哪种性能
85. 7.2) Listen interval位: 为了节省电池的电力，工作站可以暂时关闭 802.11网络接口的天线。当工作站处于休眠状态，接入点必须为之暂存帧
86. 7.3) SSID服务集标识(Service Set Identity): 由字节所形成的字串，用来标示所属网络的BSSID，即我们在Wi-Fi连接前看到的接入点名称
87. 7.4) Supported Rate(支持速率)
88. 8) Reassociation Request(重新关联请求)帧
89. 8.1) Capability information位: 发送Beacon信号的时候，它被用来通知各方，该网络具备哪种性能
90. 8.2) Listen interval位: 为了节省电池的电力，工作站可以暂时关闭 802.11网络接口的天线。当工作站处于休眠状态，接入点必须为之暂存帧
91. 8.3) Current AP Address位: 使用Current AP Address(目前接入点的地址)位来表明目前所连接的接入点的 MAC地址
92. 8.4) SSID服务集标识(Service Set Identity): 由字节所形成的字串，用来标示所属网络的BSSID，即我们在Wi-Fi连接前看到的接入点名称
93. 8.5) Supported Rate(支持速率)
94. 9) Authentication(身份认证)帧
95. 9.1) Authentication Algorithm Number: 指明认证程序所使用的认证类型
96. 9.2) Authentication Transaction Sequence Number: 用以追踪身份认证的进度
97. 9.3) Status Code: 状态代码用来表示某项过程成功或失败
98. 9.4) 质询口令(Challenge Text): 802.11所定义的共享密钥身份认证系统。会要求移动工作站必须成功解码一段加密过的质询口令。这段质询口令的发送系通过 Challenge Text
99. (质询口令)信息元素
100. 6. FCS(CRC): 包括32位的循环冗余校验(CRC)，用于检错，注意是检错不是纠错

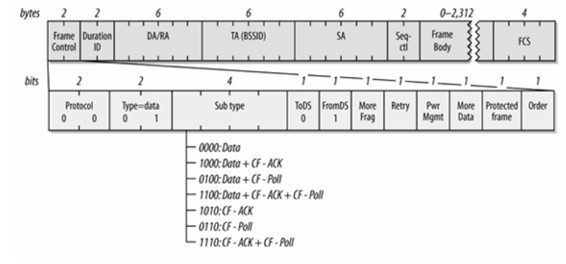
***0x2: 数据帧协议格式***

数据帧的形式取决于网络的形式。帧究竟属于哪种类型，完全取决于subtype(子类型)位，而与其他位是否出现在帧中无关

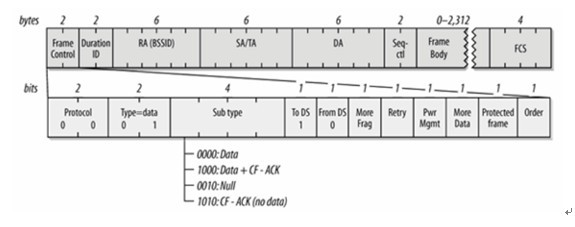
***(IBSS 数据帧的一种)***

******

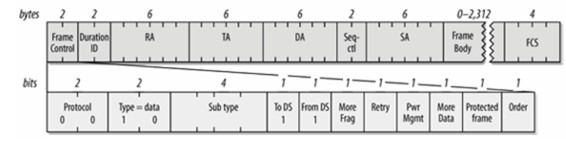
***(接入点发送(From AP)的帧，数据帧的一种)***



***(发送至接入点(To AP)的帧，数据帧的一种)***



***(WDS帧，数据帧的一种)***



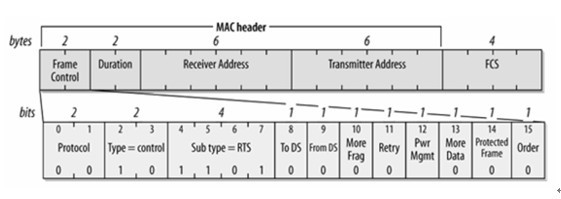
**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

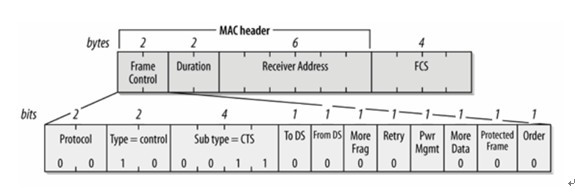
1. 1. 帧控制结构(Frame Control)
2. 1) Protocol Version: (协议版本)通常为0
3. 2) Type: 帧类型，数据帧: 10
4. 3) Subtype: 进一步判断帧的子类型，不同类型的数据帧这个字段的格式是不同的
5. 3.1) IBSS帧
6. 3.1.1) 0000: Data
7. 3.1.2) 0010: Null
8. 3.2) From AP帧
9. 3.2.1) 0000: Data
10. 3.2.2) 1000: Data+CF+ASK
11. 3.2.3) 0100: Data+CF+Poll
12. 3.2.4) 1100: Data+CF+ACK+CF+Poll
13. 3.2.5) 1010: CF+ACK
14. 3.2.6) 0110: CF+Poll
15. 3.2.7) 1110: ACK+CF+Poll
16. 3.3) To AP帧
17. 3.3.1) 0000: Data
18. 3.3.2) 1000: Data+CF+ACK
19. 3.3.3) 0010: Null
20. 3.3.4) 1010: CF+ACK(no data)
21. 3.4) WDS帧
22. null
23. 4) To DS: 表明该帧是否是BSS向DS发送的帧时
24. 4.1) IBSS: 设置为0
25. 4.2) To AP: 设置为1
26. 4.3) From AP: 设置为0
27. 4.4) WDS: 设置为1
28. 5) From DS: 表明该帧是否是DS向BSS发送的帧时
29. 5.1) IBSS: 设置为0
30. 5.2) To AP: 设置为0
31. 5.3) From AP: 设置为1
32. 5.4) WDS: 设置为1
33. 6) More Fragment: 用于说明长帧被分段的情况，是否还有其它的帧，如果有则该值设置为1
34. 7) Retry(重传域): 表示该分段是先前传输分段的重发帧。
35. 8) Power Management: 表示传输帧以后，站所采用的电源管理模式
36. 8.1) 为1: STA处于power\_save模式
37. 8.2) 为0: STA处于active模式
38. 9) More Data: 表示有很多帧缓存到站中。即至少还有一个数据帧要发送给STA是设置为1。
39. 10) Protected Frame: 表示根据WEP(Wired Equivalent Privacy)算法对帧主体进行加密。如果帧体部分包含被密钥套处理过的数据，则设置为1，否则设置为0
40. 11) Order(序号域): 在长帧分段传送时，该域设置为1表示接受者应该严格按照顺序处理该帧，否则设置为0
41. 2. Duration/ID(持续时间/标识)
42. 表明该帧和它的确认帧将会占用信道多长时间，Duration 值用于网络分配向量(NAV)计算
43. 3. Address Fields(地址域):
44. 这个域的具体格式和控制帧的子类型有关，不同的子类型会有一些微小的差别
45. 1) IBSS
46. 1.1) Destination Address
47. 1.2) Source Address
48. 1.3) BSSID
49. 每个BSS都会被赋予一个BSSID，它是一个长度为48个bit的二进制识别码，用来辨识不同的BSS
50. 2) From AP
51. 2.1) Destination Address
52. 2.2) BSSID
53. 2.3) Source Address
54. 3) To AP
55. 3.1) BSSID
56. 3.2) Source Address
57. 3.3) Destination Address
58. 4) WDS
59. 4.1) BSSID
60. 4.2) Source Address
61. 4.3) Destination Address
62. 4. Sequence Control(序列控制域): 用于过滤重复帧
63. 1) MSDU(MAC Server Data Unit), 12位序列号(Sequence Number)
64. 2) MMSDU(MAC Management Server Data Unit), 4位片段号(Fragment Number)组成
65. [SA，只有WDS中的帧有这个字段]
66. 5. Frame Body(Data): 发送或接收的信息。
67. 6. FCS(CRC): 包括32位的循环冗余校验(CRC)，用于检错，注意是检错不是纠错

***0x3: 控制帧协议格式***

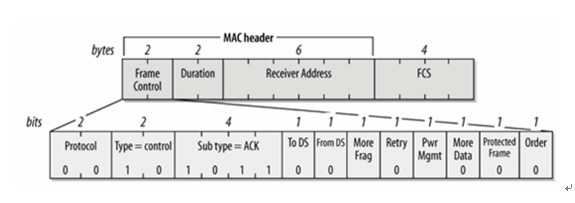
***(RTS帧，控制帧的一种)***



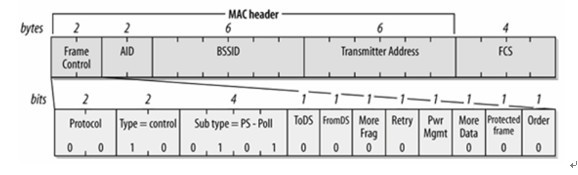
***(CTS帧，控制帧的一种)***



***(ACK帧，控制帧的一种)***



***(PS-Poll帧)***



**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. 帧控制结构(Frame Control)
2. 1) Protocol Version: (协议版本)通常为0
3. 2) Type: 帧类型，控制帧: 01
4. 3) Subtype: 进一步判断帧的子类型:
5. 控制帧
6. 3.1) 请求发送(Request To Send，RTS)数据包
7. 3.2) 清除发送(Clear To Send，CTS)数据包
8. 数据帧
9. 3.3) ACK确认(RTS/CTS)
10. 3.4) PS-Poll: 当一部移动工作站从省电模式中苏醒，便会发送一个 PS-Poll 帧给基站，以取得任何暂存帧
11. 4) To DS: 表明该帧是BSS向DS发送的帧时，该值设置为1
12. 5) From DS: 表明该帧是DS向BSS发送的帧时，该值设置为1
13. 控制帧负责处理无线介质的访问，因此只能够由无线工作站产生。传输系统并不会收送控制帧，因此这两个Bit必然为0
14. 6) More Fragment: 用于说明长帧被分段的情况，是否还有其它的帧，如果有则该值设置为1。
15. 控制帧不可能被切割，这个Bit必然为0
16. 7) Retry(重传域): 表示该分段是先前传输分段的重发帧。
17. 控制帧不像管理或数据帧那样，必须在序列中等候重送，因此这个 Bit必然为0
18. 8) Power Management: 表示传输帧以后，站所采用的电源管理模式
19. 8.1) 为1: STA处于power\_save模式
20. 8.2) 为0: STA处于active模式
21. 9) More Data: 表示有很多帧缓存到站中。即至少还有一个数据帧要发送给STA是设置为1。
22. More Data bit只用于管理数据帧，在控制帧中此Bit必然为0
23. 10) Protected Frame: 表示根据WEP(Wired Equivalent Privacy)算法对帧主体进行加密。如果帧体部分包含被密钥套处理过的数据，则设置为1，否则设置为0。
24. 控制帧不会经过加密。因此对控制帧而言，Protected Frame bit必然为0。
25. 11) Order(序号域): 在长帧分段传送时，该域设置为1表示接受者应该严格按照顺序处理该帧，否则设置为0。
26. 控制帧是基本帧交换程序(atomic frame exchange operation)的组成要件，因此必须依序发送。所以这个Bit必然为0
27. 2. Duration/ID(持续时间/标识)
28. 表明该帧和它的确认帧将会占用信道多长时间，Duration 值用于网络分配向量(NAV)计算。
29. 注意: 在PS-Poll帧中不包含Duration/ID这个字段
30. 3. Address Fields(地址域):
31. 这个域的具体格式和控制帧的子类型有关，不同的子类型会有一些微小的差别
32. 3.1) RTS(请求发送帧)
33. 3.1.1) Receiver Address(接收端地址)
34. 接收大型帧的工作站的地址
35. 3.1.2) Transmitter Address(发送端地址)
36. RTS帧的发送端的地址
37. 3.2) CTS(允许发送)
38. 3.2.1) Receiver Address(接收端地址)
39. 3.3) ACK(应答)
40. 3.3.1) Receiver Address(接收端地址)
41. 3.4) PS-Poll(省电模式一轮询)
42. 3.4.1) AID(连接识别码 association ID)
43. 连接识别码是接入点所指定的一个数值，用以区别各个连接。将此识别码置入帧，可让接入点找出为其(移动工作站)所暂存的帧
44. 3.4.2) BSSID
45. 此位包含发送端目前所在 BSS(AP)的BSSID ，此BSS 建立自目前所连接的AP
46. 3.4.3) Transmitter Address(发送端地址)
47. 此为PS-Poll帧之发送端的 MAC地址
48. 4. FCS(CRC): 包括32位的循环冗余校验(CRC)，用于检错，注意是检错不是纠错

**3. Wi-Fi认证过程**

有了802.11协议的基本格式之后，我们可以使用wireshark进行抓包实验，验证一下我们的理论

**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. ifconfig -a
2. ifconfig wlan1 up
3. airmon-ng start wlan1
4. 启动wireshark，选择mon0网卡(开启了Monotor模式的虚拟网卡

***0x1: 普通无加密连接过程***

***1. AP发送Beacon广播管理帧***

因为AP发送的这个Beacon管理帧数据包是广播地址，所以我们的PCMIA内置网卡、或者USB外界网卡会接收到这个数据包，然后在我们的"无线连接列表"中显示出来

***2. 客户端向承载指定SSID的AP发送Probe Request(探测请求)帧***

当我们点击"连接"的时候，无线网卡就会发送一个Prob数据帧，用来向AP请求连接

***3. AP接入点对客户端的SSID连接请求进行应答***

AP对客户端的连接作出了回应，并表示不接受任何形式的"帧有效负载加密(frame-payload-encryption)"

***4. 客户端对目标AP请求进行身份认证(Authentication)***

***5. AP对客户端的身份认证(Authentication)请求作出回应***

AP回应，表示接收身份认证

***6. 客户端向AP发送连接(Association)请求***

身份认证通过之后，所有的准备工作都做完了，客户端这个时候可以向WLAN AP发起正式的连接请求，请求接入WLAN

***7. AP对连接(Association)请求进行回应***

AP对客户端的连接请求(Association)予以了回应(包括SSID、性能、加密设置等)。至此，Wi-Fi的连接身份认证交互就全部结束了，之后就可以正常进行数据发送了

***8. 客户端向AP请求断开连接(Disassociation)***

当我们点击"断开连接"的时候，网卡会向AP发送一个断开连接的管理数据帧，请求进行断开连接

由此，我们可以发现，基于对数据帧格式的了解，黑客可以发起一些针对协议的攻击

**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. Deanthentication攻击
2. 2. Disassociation攻击

黑客可以利用这种方式加快对WEP/WPS-PSK保护的无线局域网的攻击，迫使客户端重新连接并且产生ARP流量(基于WEP的攻击)、或捕获重新进行WPA连接的四次握手，然后可以对密码进行离线字典或彩虹表破解攻击

***0x2: 基于WEP加密的连接过程***

***0x3: 基于WPA-PSK加密的连接过程***

这两种连接交互过程原理上和无加密方式(开放系统方式)相同，感兴趣的朋友可以使用wireshark进行抓包实验

**4. 802.11标准中的数据安全加密协议**

在IEEE 802.11协议中的加密[**算法**](http://lib.csdn.net/base/datastructure)有如下几个

**[html]** [view plain](http://blog.csdn.net/xinyuan510214/article/details/50570092) [copy](http://blog.csdn.net/xinyuan510214/article/details/50570092)

[print?](http://blog.csdn.net/xinyuan510214/article/details/50570092)

1. 1. WEP，Wired Equivalent Privacy: 802.11中最早期的加密标准
2. http://en.wikipedia.org/wiki/Wired\_Equivalent\_Privacy
4. 2. CCMP(CTR with CBC-MAC Protocol): 基于AES的全新加密协议，在IEEE 802.11i中提出
5. http://en.wikipedia.org/wiki/CCMP
7. 3. WPA(Wi-Fi Protected Access)
8. http://en.wikipedia.org/wiki/WPA
10. 4. TKIP(Temporal Key Integrity Protocol)
11. http://en.wikipedia.org/wiki/Temporal\_Key\_Integrity\_Protocol
13. 5. WPA2(Wi-Fi Protected Access 2)
14. http://en.wikipedia.org/wiki/WPA2

加密算法、以及它们的协议交互过程的，在下一章节进行学习讲解