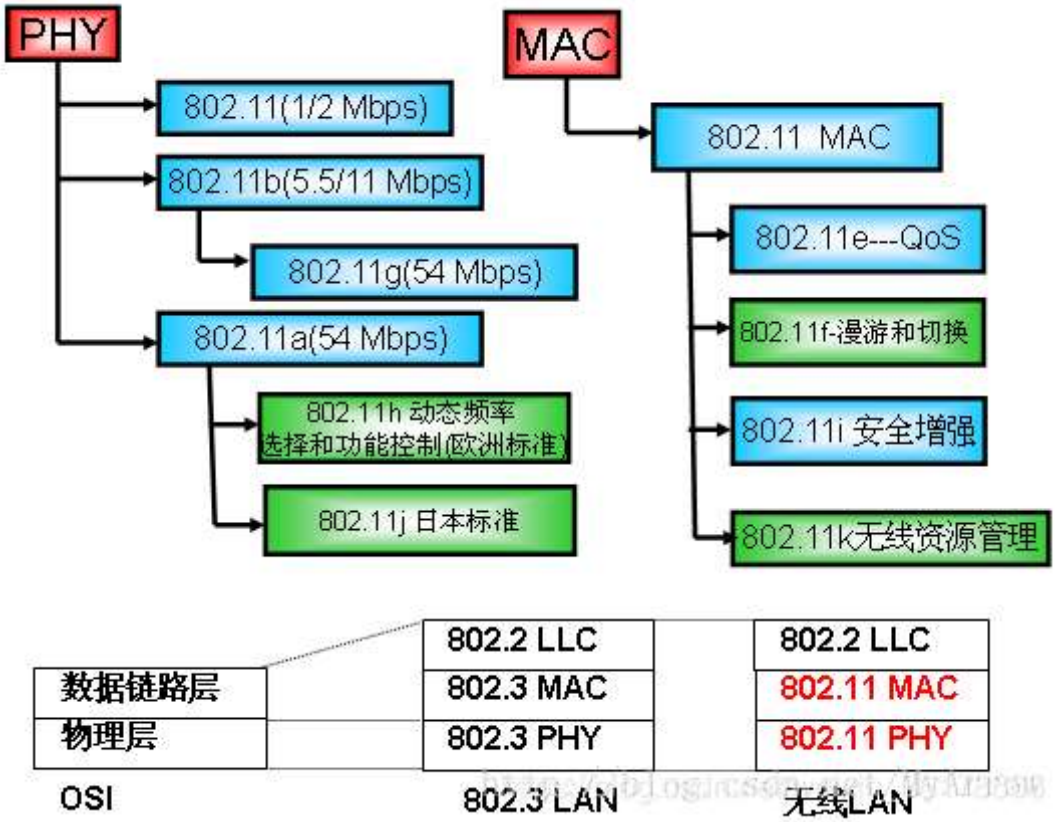
IEEE 802.11协议基础知识整理

Mars.HU
于 2019-06-25 17:29:16 发布 16875 已收藏 142

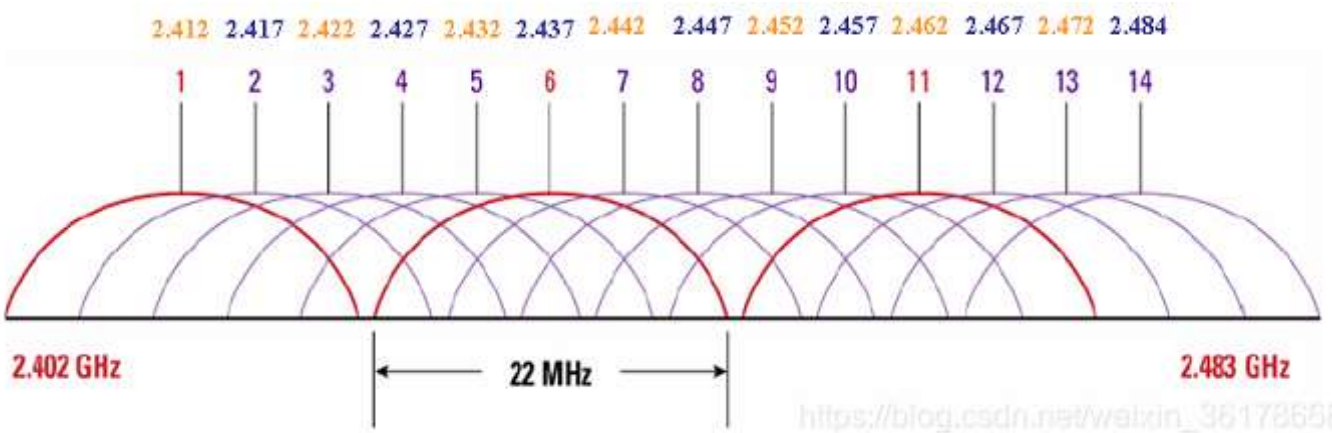
分类专栏： Wireless 文章标签： 802.11 WiFi Wireless

目录

1. IEEE 802.11协议族成员


PHY
802.11(1/2 Mbps)
802.11b(5.5/11 Mbps)
802.11g(54 Mbps)
802.11a(54 Mbps)
802.11h 动态频率选择和功能控制(欧洲标准)
802.11j 日本标准
MAC
802.11 MAC
802.11e---QoS
802.11f-漫游和切换
802.11i 安全增强
802.11k无线资源管理
数据链路层
物理层
802.2 LLC
802.3 MAC
802.3 PHY
802.2 LLC
802.11 MAC
802.11 PHY
OSI
802.3 LAN
无线LAN

2. 频谱划分



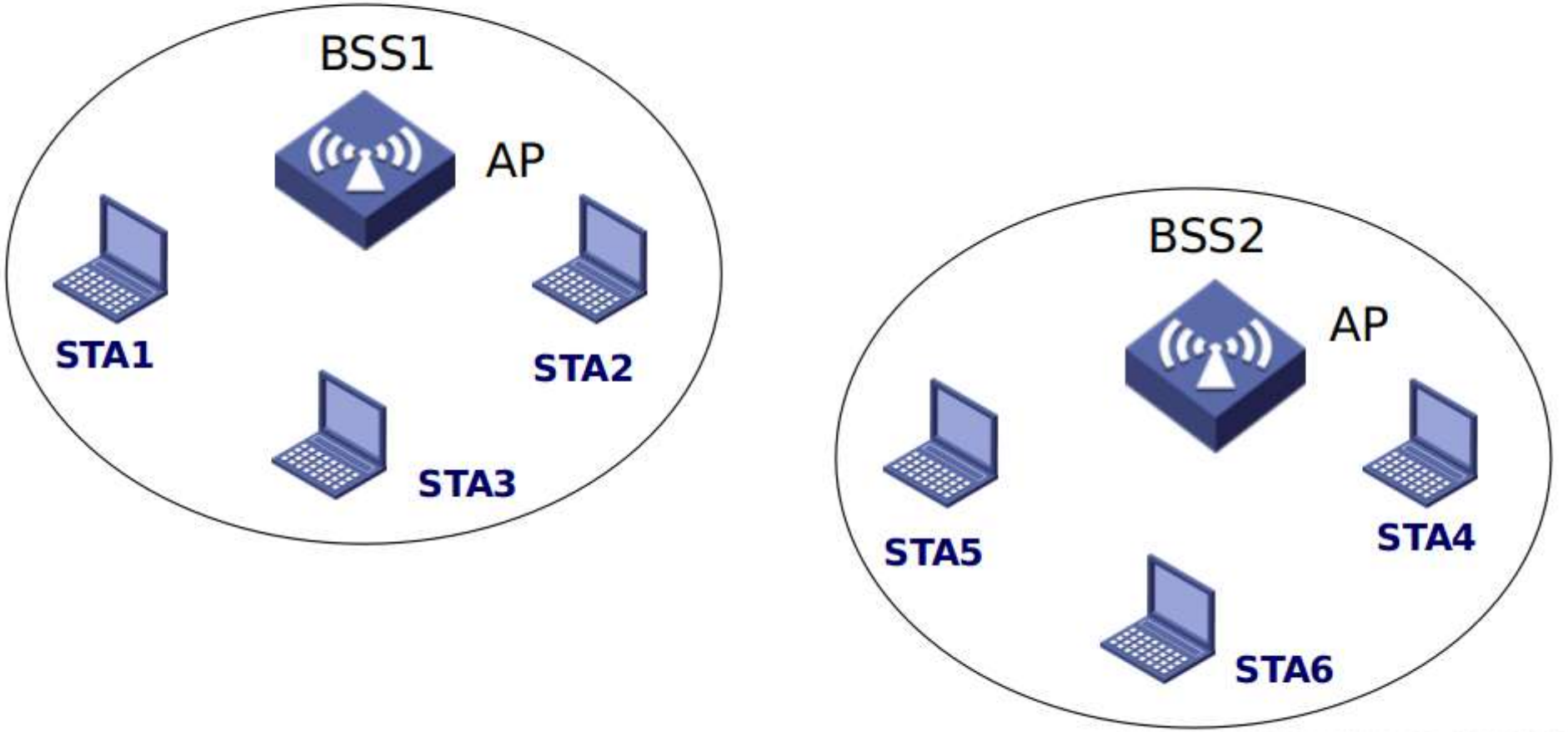
WiFi总共有14个信道，如下图所示：

- IEEE 802.11b/g标准工作在2.4G频段，频率范围为2.400—2.4835GHz，共83.5M带宽
- 划分为14个子信道
- 每个子信道宽度为22MHz
- 相邻信道的中心频点间隔5MHz
- 相邻的多个信道存在频率重叠(如1信道与2、3、4、5信道有频率重叠)
- 整个频段内只有3个（1、6、11）互不干扰信道

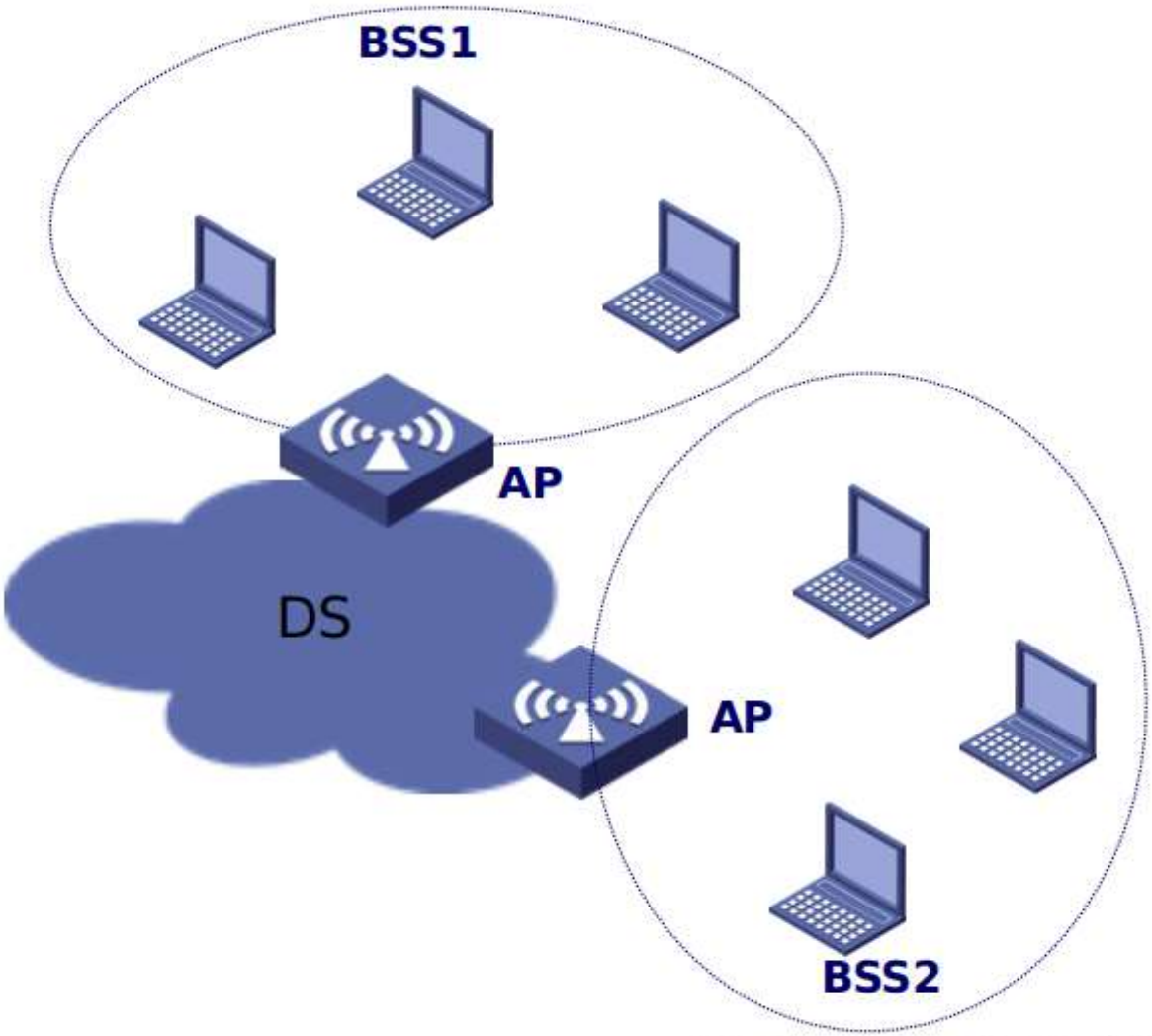
3. 802.11网络的基本元素

3.1 BSS(Basic Service Set)

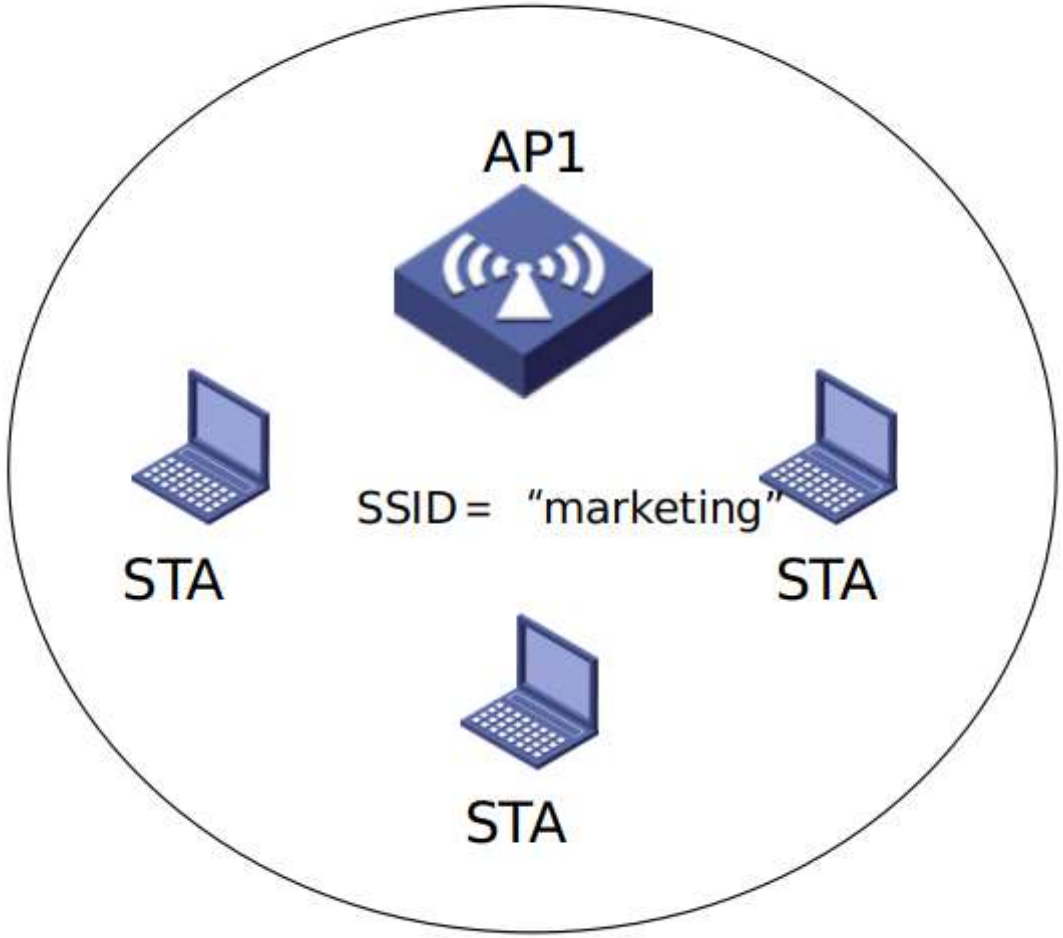
- Stations (STA)：任何的无线终端设备
- AP （Access Point）：一种特殊的STA



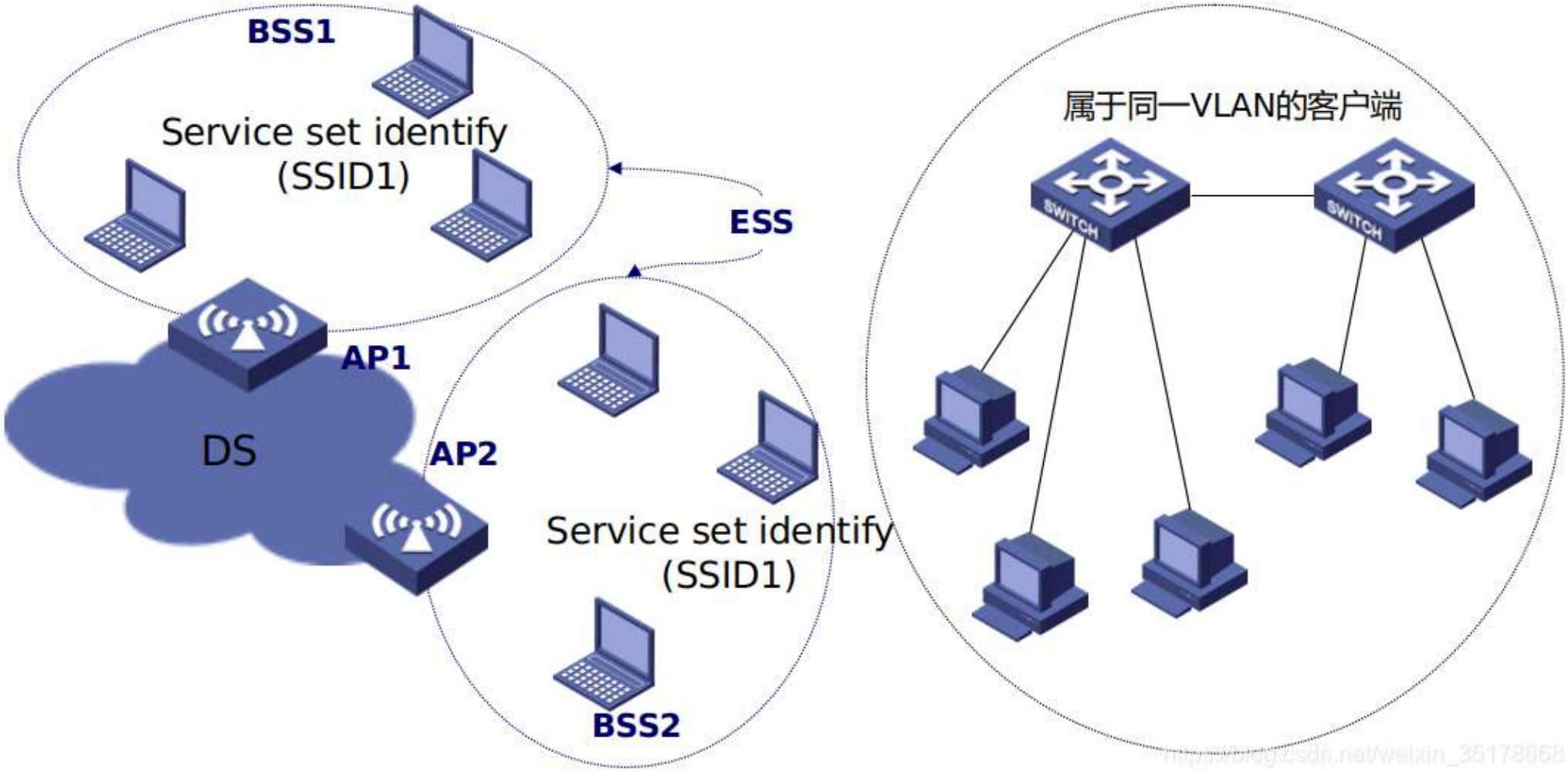
3.2 DS(Distribution System,分布式系统)



3.3 SSID(Service Set ID 服务集识别码)



3.4 ESS(Extended Service Set,采用相同的SSID的多个BSS形成的更大规模的虚拟BSS)



4. 802.11MAC层工作原理

802.11MAC层负责客户端与AP之间的通讯。主要功能包括：扫描、接入、认证、加密、漫游和同步。

4.1 802.11MAC 报文类型

4.1.1 数据帧

用户的数据报文

Type	Subtype	Frametype
10	0000	Data（数据）
10	0001	Data+CF-ACK
10	0010	Data+CF-Poll
10	0011	Data+CF-ACK+CF-Poll
10	0100	Null data（无数据：未传送数据）
10	0101	CF-ACK（未传送数据）
10	0110	CF-Poll（未传送数据）
10	0111	Data+CF-ACK+CF-Poll
10	1000	Qos Data
10	1001	Qos Data + CF-ACK
10	1010	Qos Data + CF-Poll
10	1011	Qos Data + CF-ACK+ CF-Poll
10	1100	QoS Null（未传送数据）
10	1101	QoS CF-ACK（未传送数据）

10	1110	QoS CF-Poll（未传送数据）
10	1111	QoS CF-ACK+ CF-Poll（未传送数据）

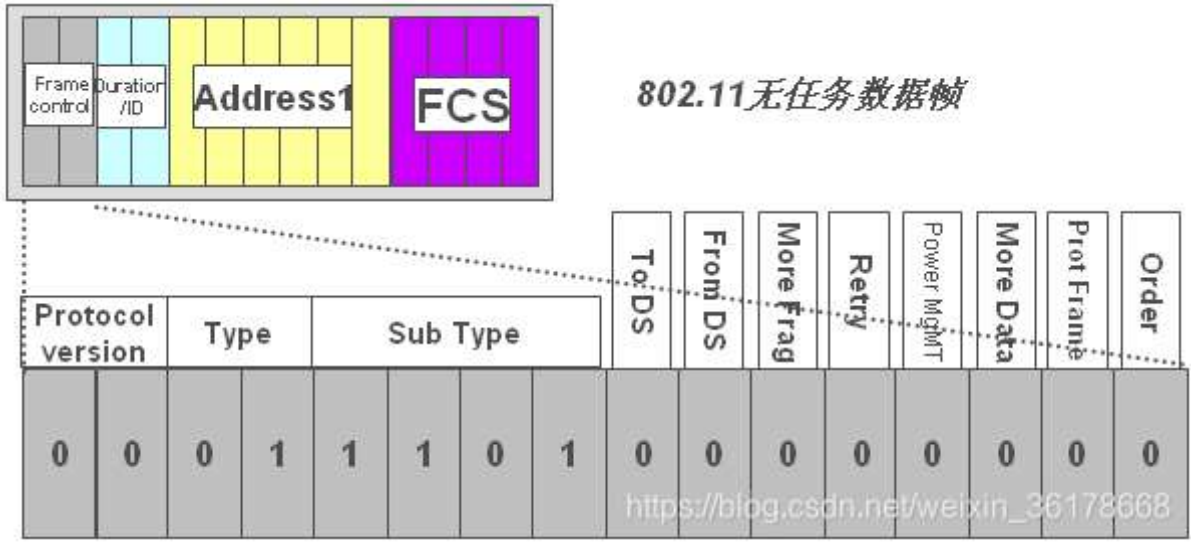
4.1.2 控制帧

协助发送数据帧的控制报文，例如：RTS、CTS、ACK等

Type	Subtype	Frametype
01	1010	Power Save（PS）- Poll（省电 - 轮询）
01	1011	RTS（请求发送，即: Request To Send ，预约信道，帧长20字节）
01	1100	CTS（清除发送，即:Clear To Send ，同意预约，帧长14字节）
01	1101	ACK（确认）
01	1110	CF-End（无竞争周期结束）
01	1111	CF-End（无竞争周期结束）+CF-ACK（无竞争周期确认）

RTS和CTS用于信道预约，CF-End+CF_ACK和ACK用于确认正确接收到帧。

- ACK帧


Frame control
Duration /ID
Address1
FCS
802.11无任务数据帧
Protocol version
Type
Sub Type
To DS
From DS
More Frag
Retry
Power MgMT
More Data
Prot Frame
Order
0 0 0 1 1 1 0 1 0 0 0 0 0 0 0 0
https://blog.csdn.net/weixin_36178668

4.1.3 管理帧

负责STA和AP之间的能力级的交互，认证、关联等管理工作。例如：Beacon、Probe、Association及Authentication等

Type	SubType	FrameType
00	0000	Association request (连接请求)
00	0001	Association response (连接响应)
00	0010	Reassociation request（重连接请求）
00	0011	Reassociation response（重连接联响应）
00	0100	Probe request（探测请求）
00	0101	Probe response（探测响应）
00	1000	Beacon（信标，被动扫描时AP 发出，notify）
00	1001	ATIM（通知传输指示消息）
00	1010	Disassociation（解除连接，notify）
00	1011	Authentication（身份验证）
00	1100	Deauthentication（解除认证，notify）
00	1101～1111	Reserved（保留，未使用）

ATIM：Announcement Traffic Indication Message，ATIM仅在ATIM窗口期间传送，ATIM没有负载。

4.2 用户接入管理过程

STA (工作站）启动初始化、开始正式使用、AP 传送数据帧之前，要经过三个阶段才能接入:

- 扫描(Scaning)
- 认证(Authentication)
- 关联(Association)

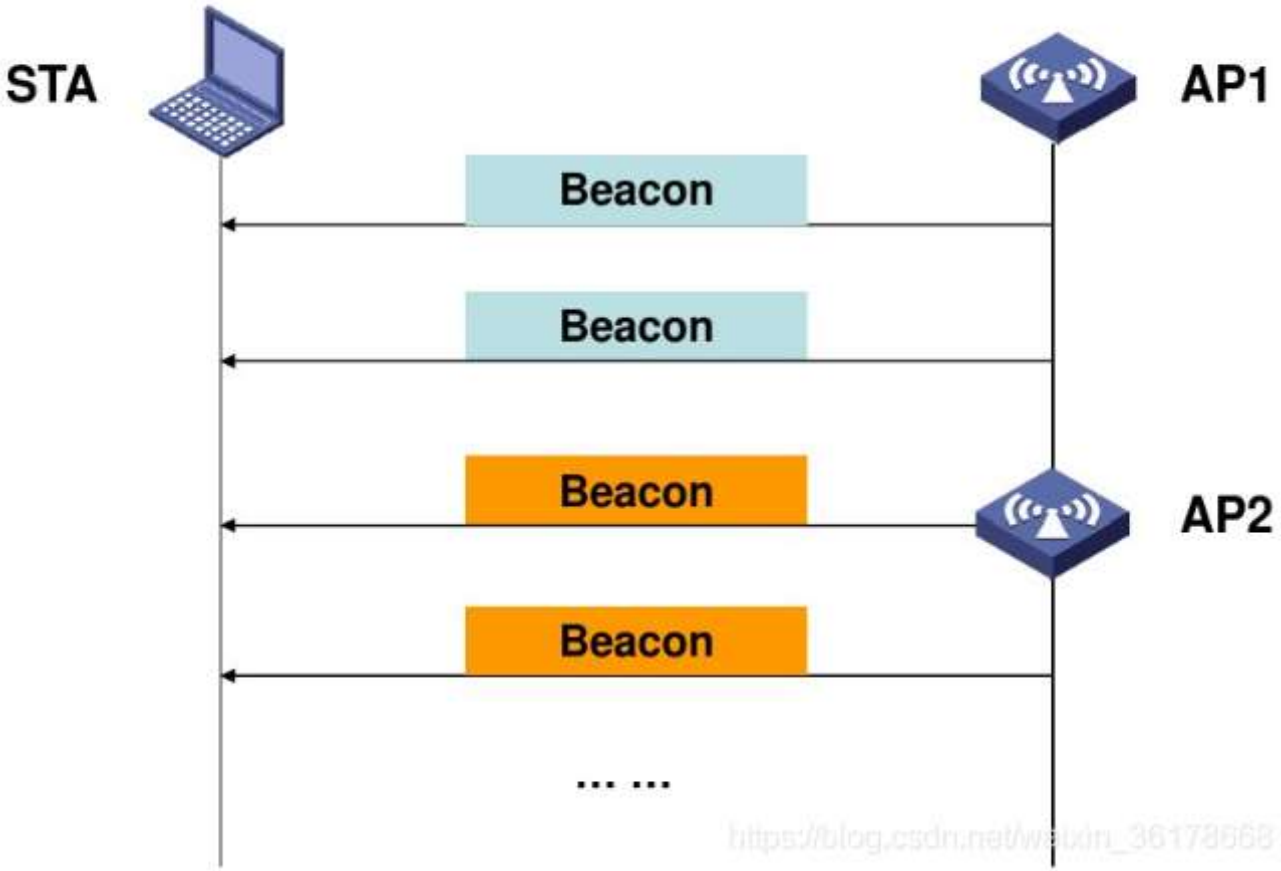
4.2.1 Scaning

802.11MAC 使用Scanning功能来完成Discovery

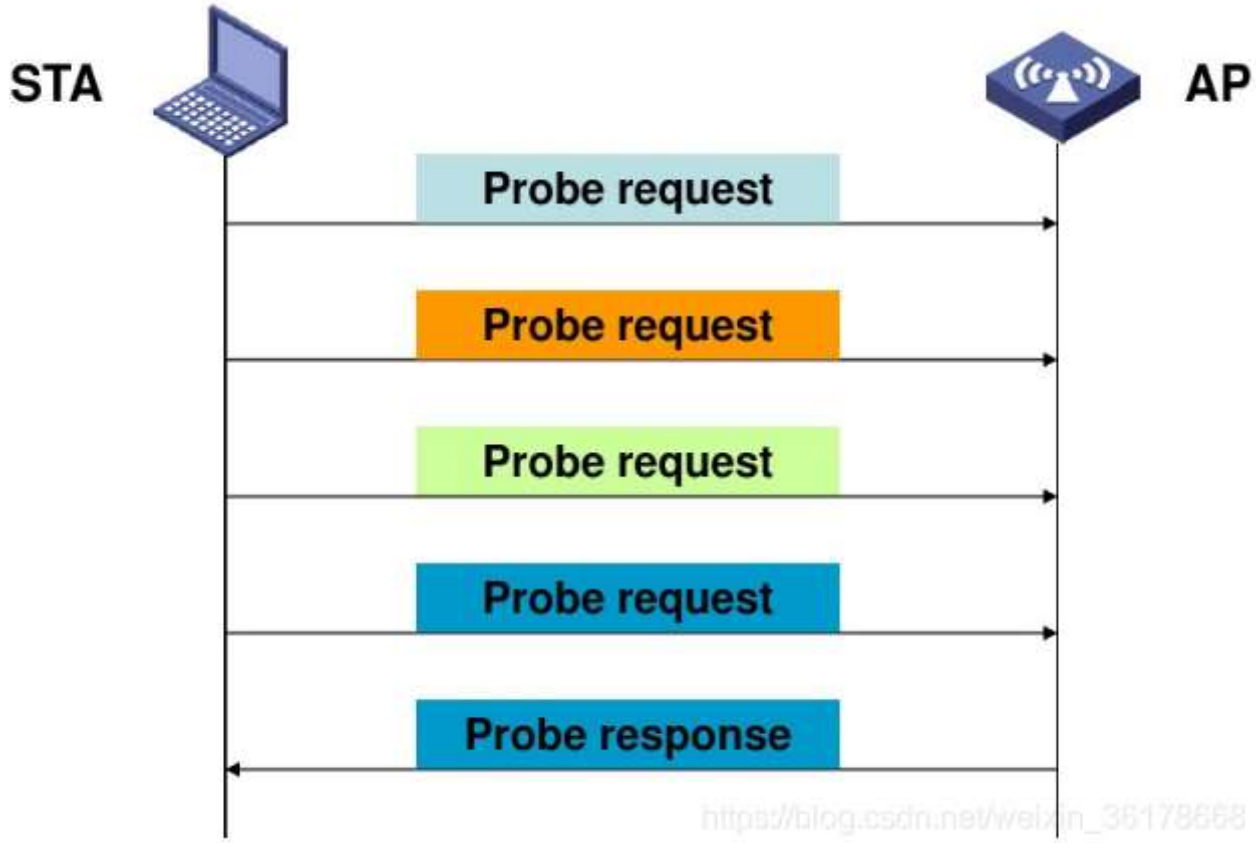
- 寻找和加入一个网络
- 当STA漫游时寻找一个新的AP

Scaning功能的两种方式

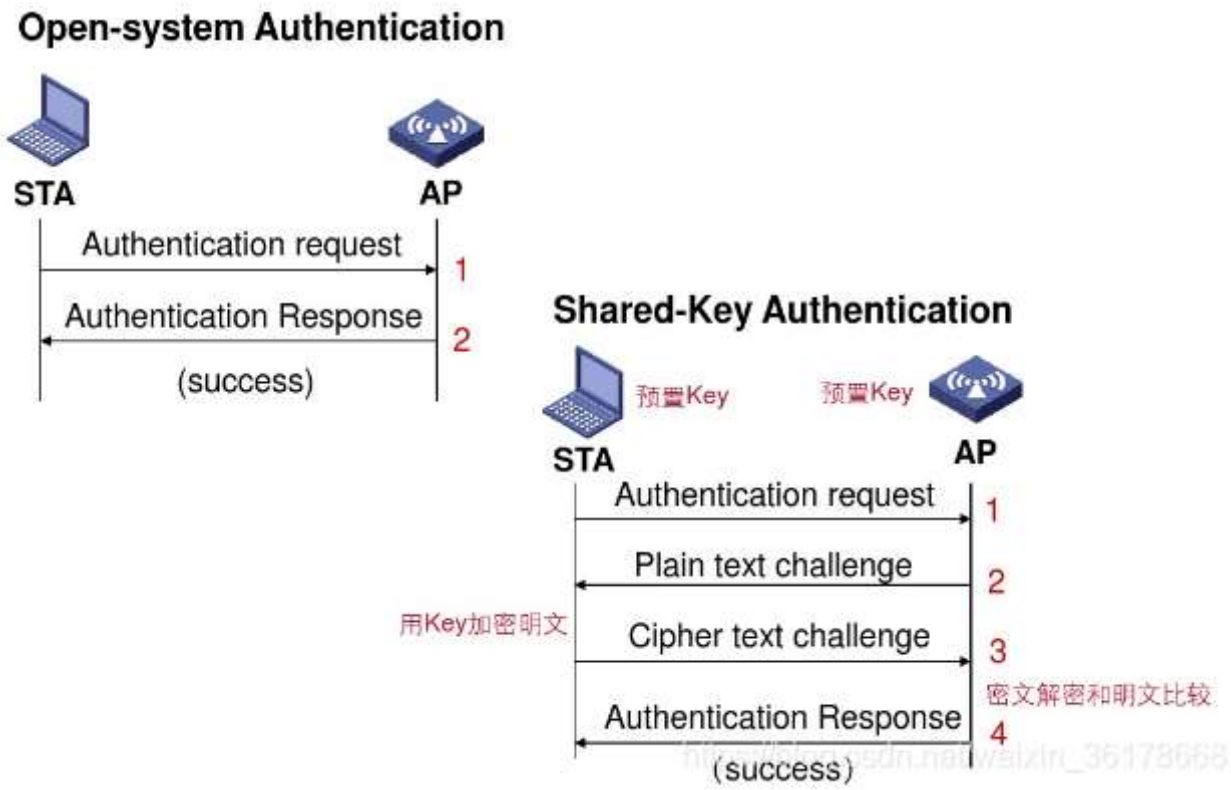
- Passive Scanning
  通过侦听AP定期发送的Beacon帧来发现网络。



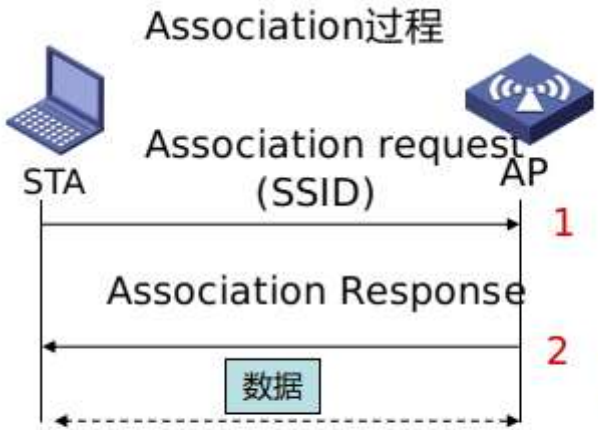
- Active Scanning
  在每个信道上发送Probe request报文，从Probe Response中获取BSS的基本信息。

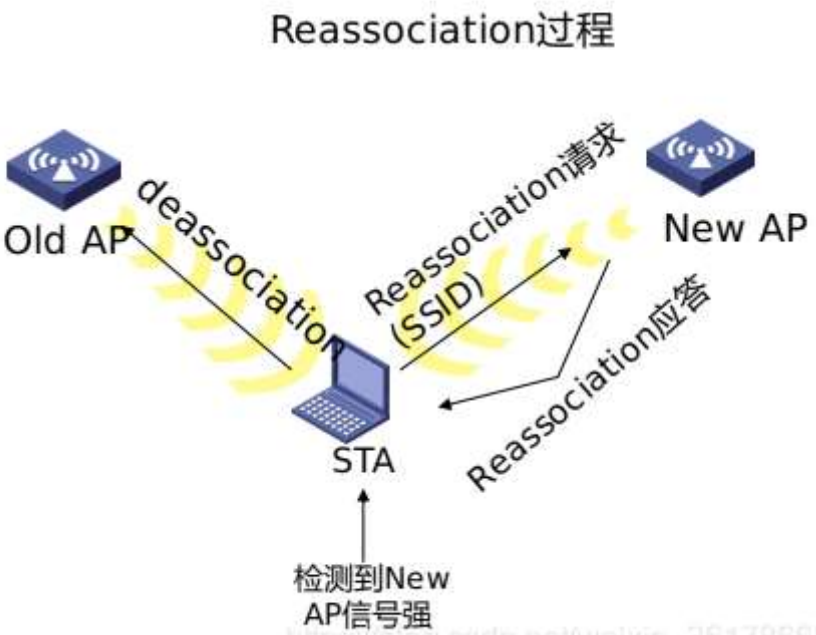


4.2.2 Authentication



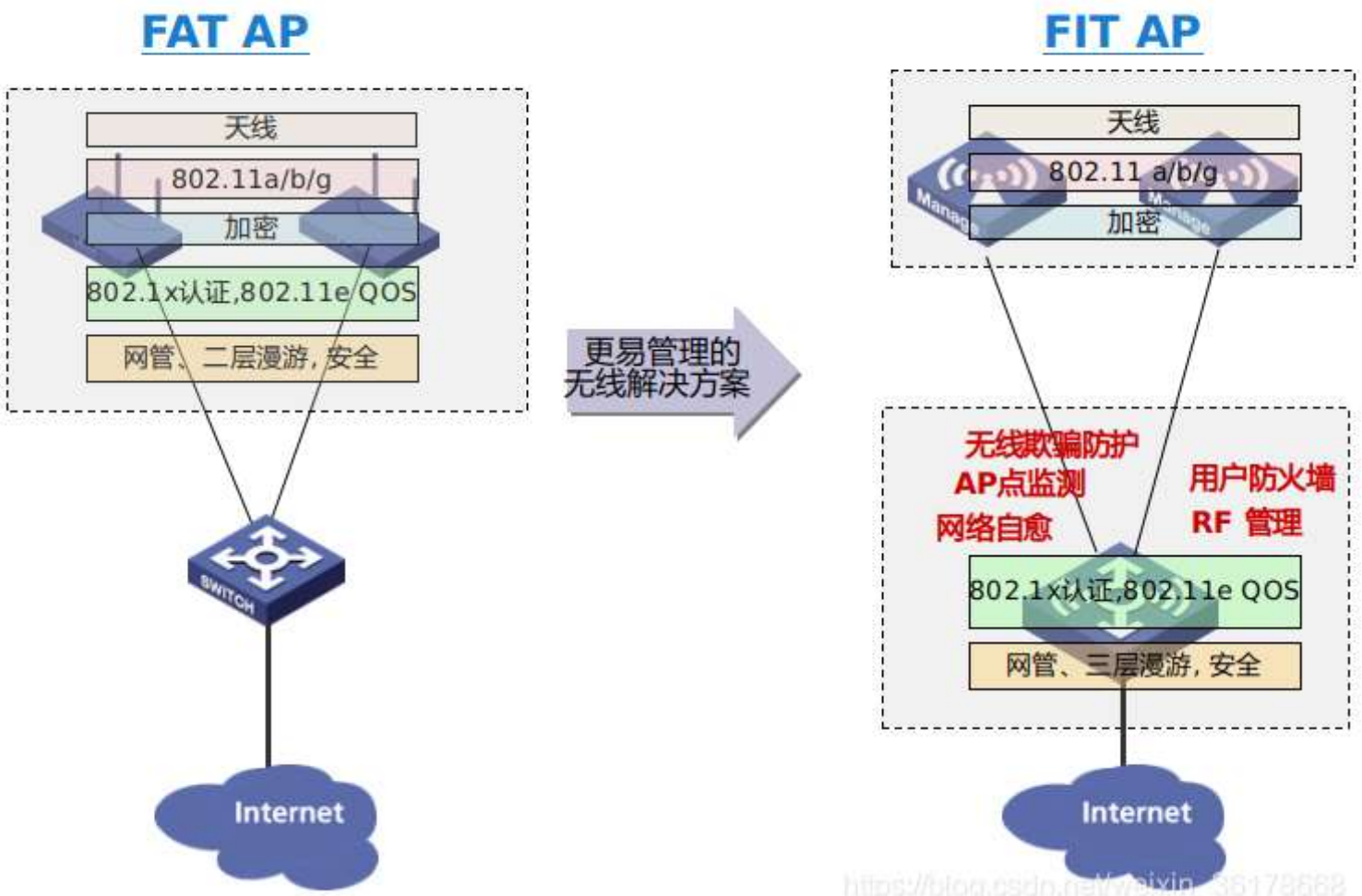
4.2.3 Association


Association过程
STA
AP
Association request
(SSID)
1
Association Response
2
数据

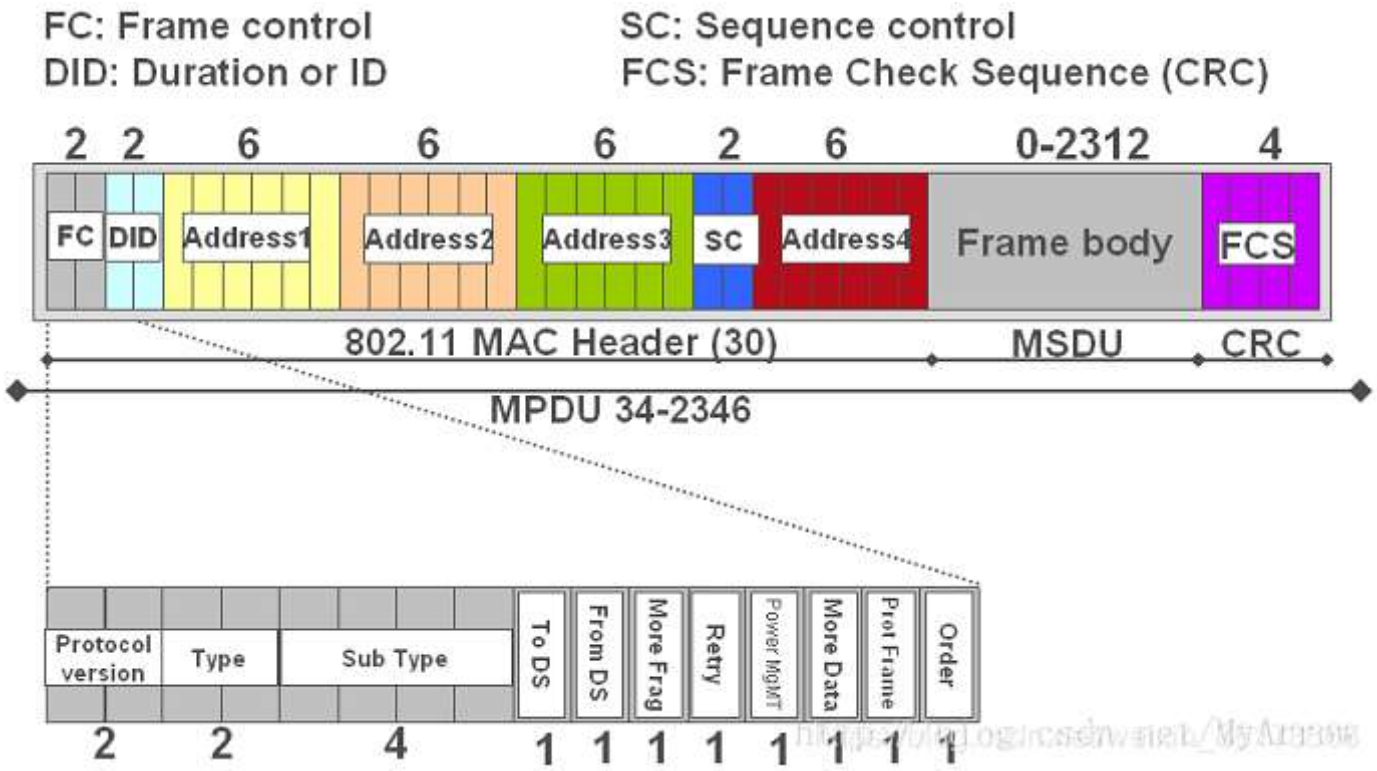

Reassociation过程
Old AP
deassociation
Reassociation请求
(SSID)
New AP
Reassociation应答
STA
检测到New
AP信号强

5.AP种类

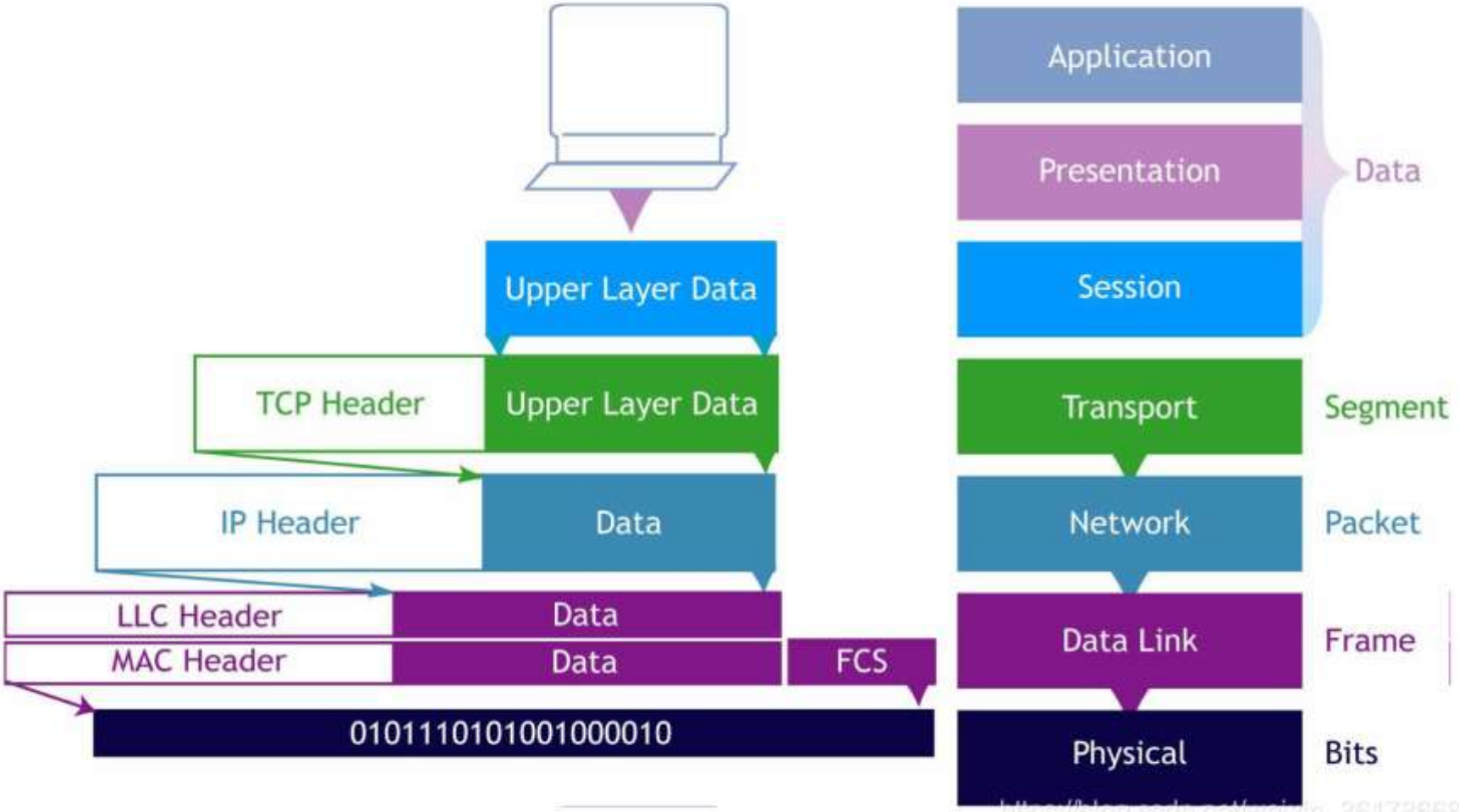
FAT AP和FIT AP比较如下图所示：



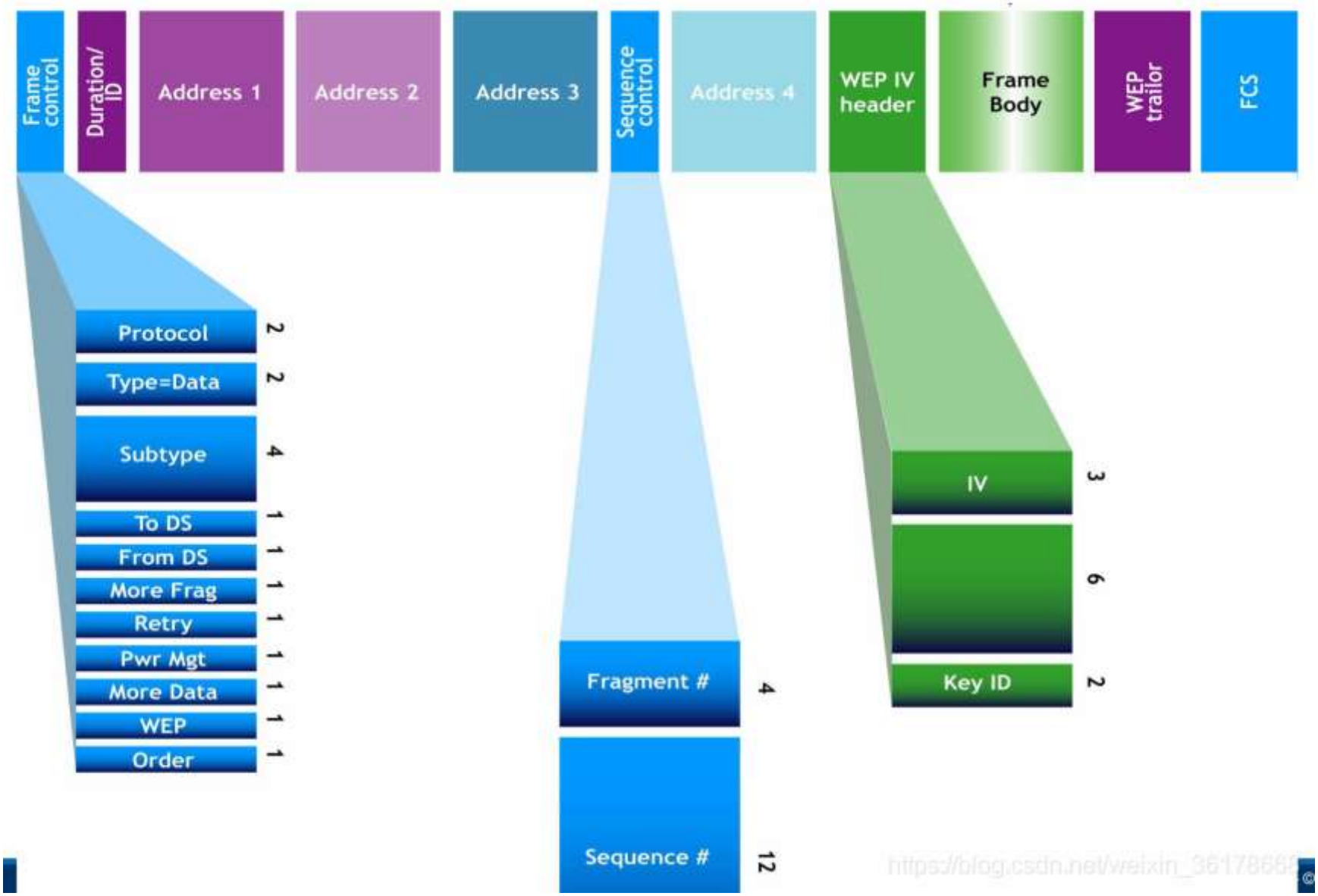
6. 802.11帧格式


FC: Frame control
DID: Duration or ID
SC: Sequence control
FCS: Frame Check Sequence (CRC)
2 2 6 6 6 2 6 0-2312 4
FC
DID
Address1
Address2
Address3
SC
Address4
Frame body
FCS
802.11 MAC Header (30)
MSDU
CRC
MPDU 34-2346
Protocol version
Type
Sub Type
To DS
From DS
More Frag
Retry
Power MgMT
More Data
Prot Frame
Order
2 2 4 1 1 1 1 1 1 1 1

6.0 OSI模型

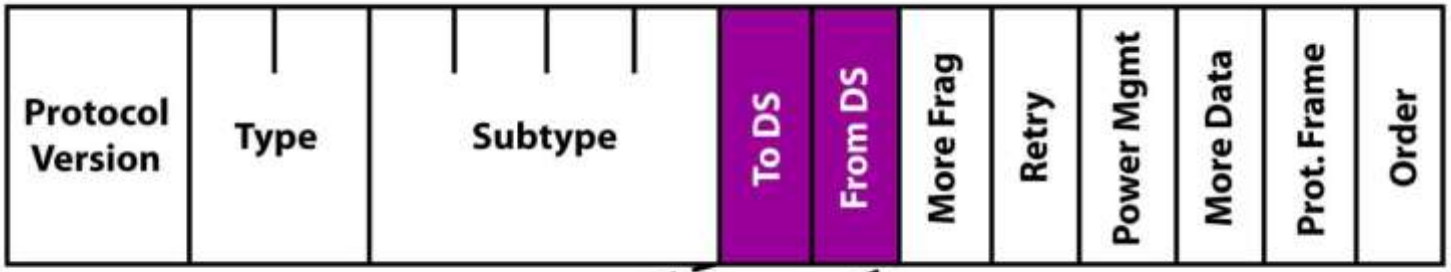


6.1 802.11 MAC Header（MAC头）



6.1.1 Frame Control（帧控制域）

Frame Control Field



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA/DA	TA/SA	BSSID	n/a
0	1	RA/DA	TA/BSSID	SA	n/a
1	0	RA/BSSID	TA/SA	DA	n/a
1	1	RA	TA	DA	SA

- Protocol Version（协议版本）：通常为0；
- Type（类型域）和Subtype（子类型域）：共同指出帧的类型；
- To DS：表明该帧是BSS向DS发送的帧；
- From DS：表明该帧是DS向BSS发送的帧；
- More Frag：用于说明长帧被分段的情况，是否还有其它的帧；
- Retry（重传域）：用于帧的重传，接收STA利用该域消除重传帧；

• Pwr Mgt（能量管理域）：1：STA处于power_save模式；0：处于active模式；
• More Data（更多数据域）：1：至少还有一个数据帧要发送给STA；
• Protected Frame： 1：帧体部分包含被密钥套处理过的数据；否则：0；
• Order（序号域）：1：长帧分段传送采用严格编号方式；否则：0。

6.1.2 Duration/ID（持续时间/标识）

表明该帧和它的确认帧将会占用信道多长时间；对于帧控制域子类型为：Power Save-Poll的帧，该域表示了STA的连接身份（AID, Association Indentification）。

6.1.3 Address（地址域）

Address（地址域）：源地址（SA）、目的地址（DA）、传输工作站地址（TA）、接收工作站地址（RA），SA与DA必不可少，后两个只对跨BSS的通信有用，而目的地址可以为单播地址（Unicast address）、多播地址（Multicast address）、广播地址（Broadcast address）。

6.1.4 Sequence Control（序列控制域）

Sequence Control（序列控制域）：由代表MSDU（MAC Server Data Unit）或者MMSDU（MAC Management Server Data Unit）的12位序列号（Sequence Number）和表示MSDU和MMSDU的每一个片段的编号的4位片段号组成（Fragment Number）。

6.2 Frame Body（帧体部分）

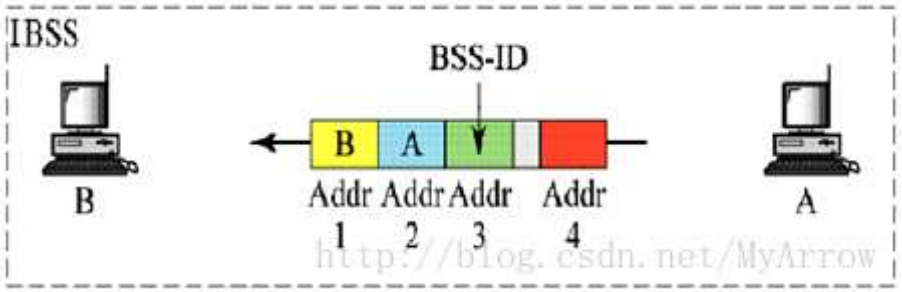
包含信息根据帧的类型有所不同，主要封装的是上层的数据单元，长度为0~2312个字节，可以推出，802.11帧最大长度为：2346个字节；

6.3 FCS（校验域）

包含32位循环冗余码。

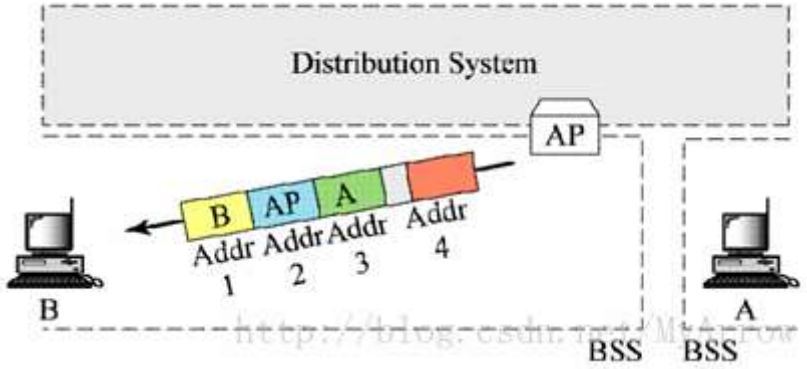
6.4 地址格式

1. 方案一：



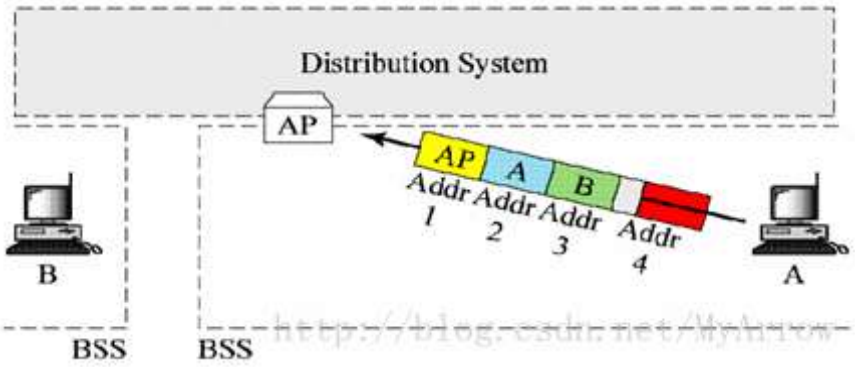
A和B 在同一个IBSS，A->B (Ad hoc无线自组网中的数据帧的地址格式)。

2. 方案二：



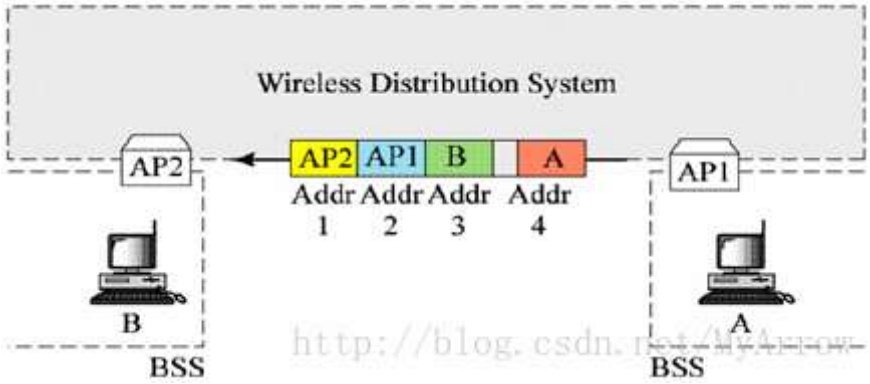
从AP发出的无线数据帧中的地址格式。

3. 方案三：



发到AP的无线数据帧中的地址格式。

4. 方案四：



通过无线分布系统传输的无线数据帧中的地址格式。

7. AP种类

FAT AP和FIT AP比较如下图所示：