Wi-Fi网络介绍

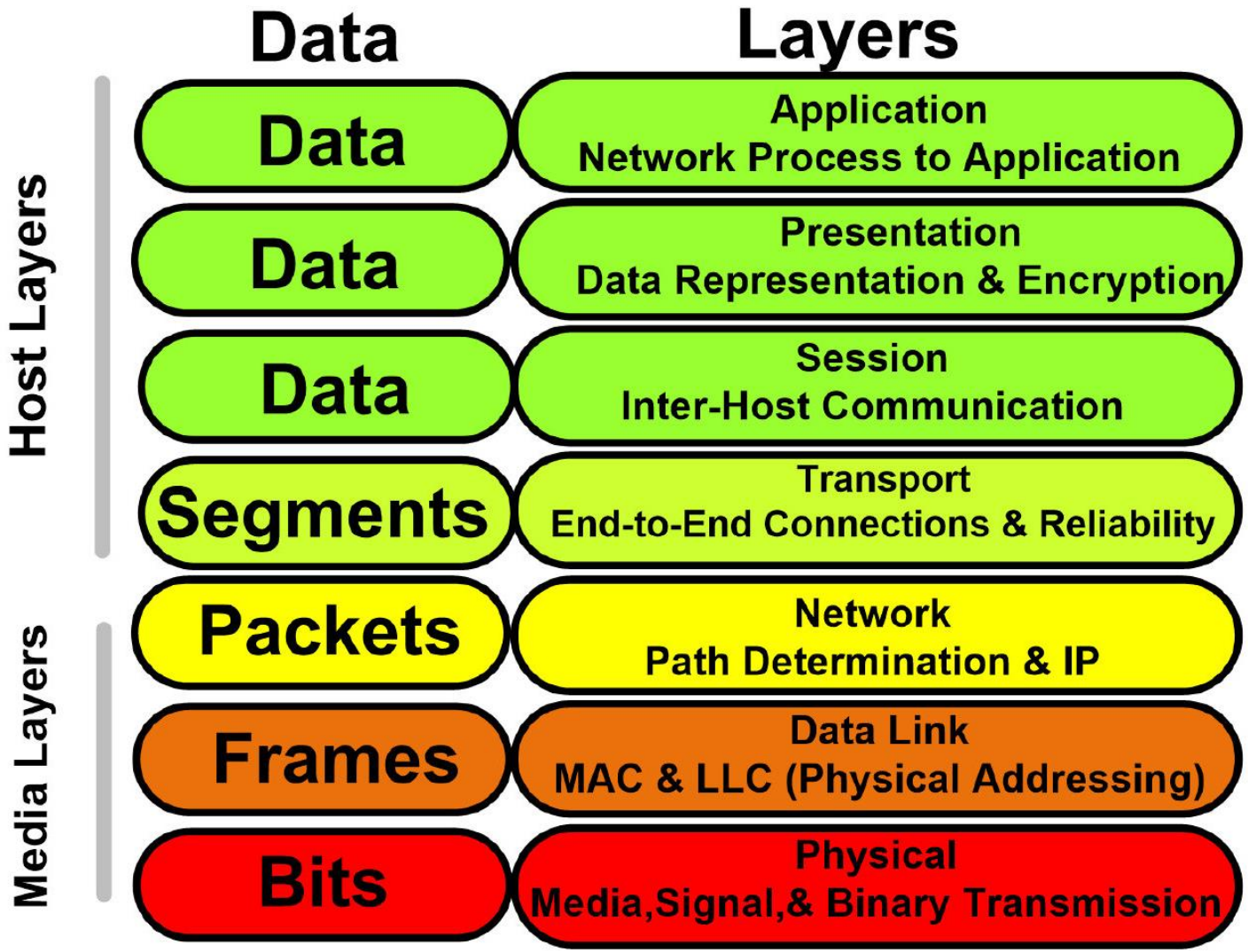
刘煜

西安中心

Wi-Fi

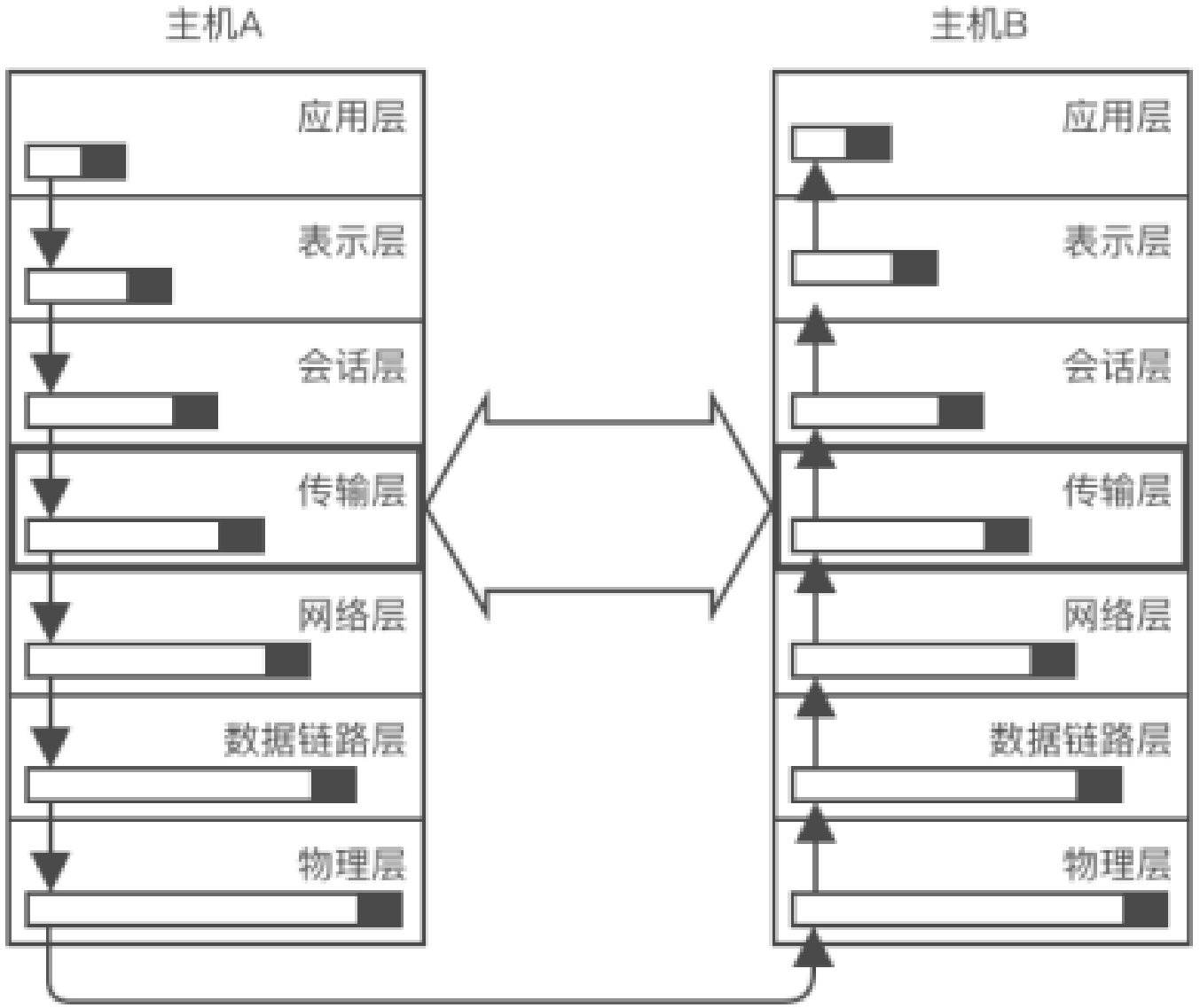
1. Wi-Fi是用来实现无线局域网（WLAN）的一系列无线电技术，基于IEEE 802.11协议族。
2. Wi-Fi是Wi-Fi联盟的认证商标，用于标识基于IEEE 802.11标准可以互相通信的网络设备。

OSI网络模型


Data
Layers
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation & Encryption
Data
Session
Inter-Host Communication
Segments
Transport
End-to-End Connections & Reliability
Packets
Network
Path Determination & IP
Frames
Data Link
MAC & LLC (Physical Addressing)
Bits
Physical
Media,Signal,& Binary Transmission

OSI和快递

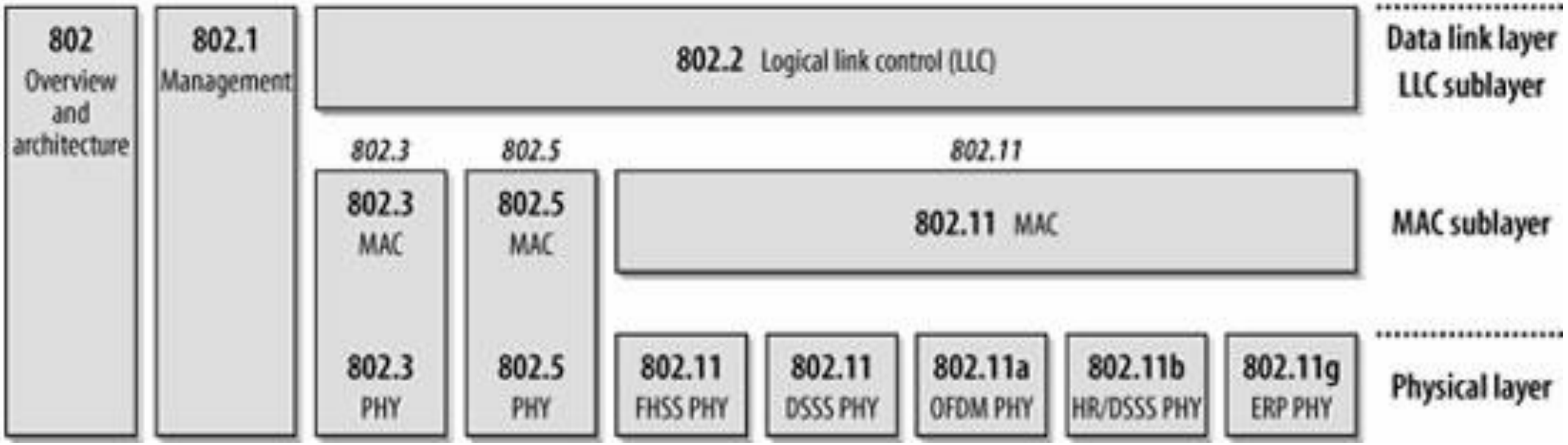

7
经理
写好信件的草稿
阅读讯息
经理
6
助理
修改错字或格式
提醒经理有信收，翻译信的内容
助理
5
秘書
找出收信人的地址，写好信封
打開信件，製作副本
秘書
4
司機
將信件帶到郵局
由郵局拿信回公司
司機
3
排序工人
將信件依收件地區分開
為獨立郵戶排好訊息
排序工人
2
包裝
將郵件包裝好一疊
拆開來自不同地方的包裹
包裝
1
搬運工人（將貨搬上車）
傳遞媒介
搬運工人（將貨搬上車）


主机A
主机B
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

IEEE 802.11 标准

IEEE（电气电子工程师学会）802工作组负责局域网标准的制订，在1997年发布了802.11标准，定义了无线局域网的媒体访问控制层（MAC层）和物理层。 以太网和Wi-Fi采用的协议都属于IEEE 802协议集。其中，以太网使用802.3标准，而Wi-Fi使用802.11标准。

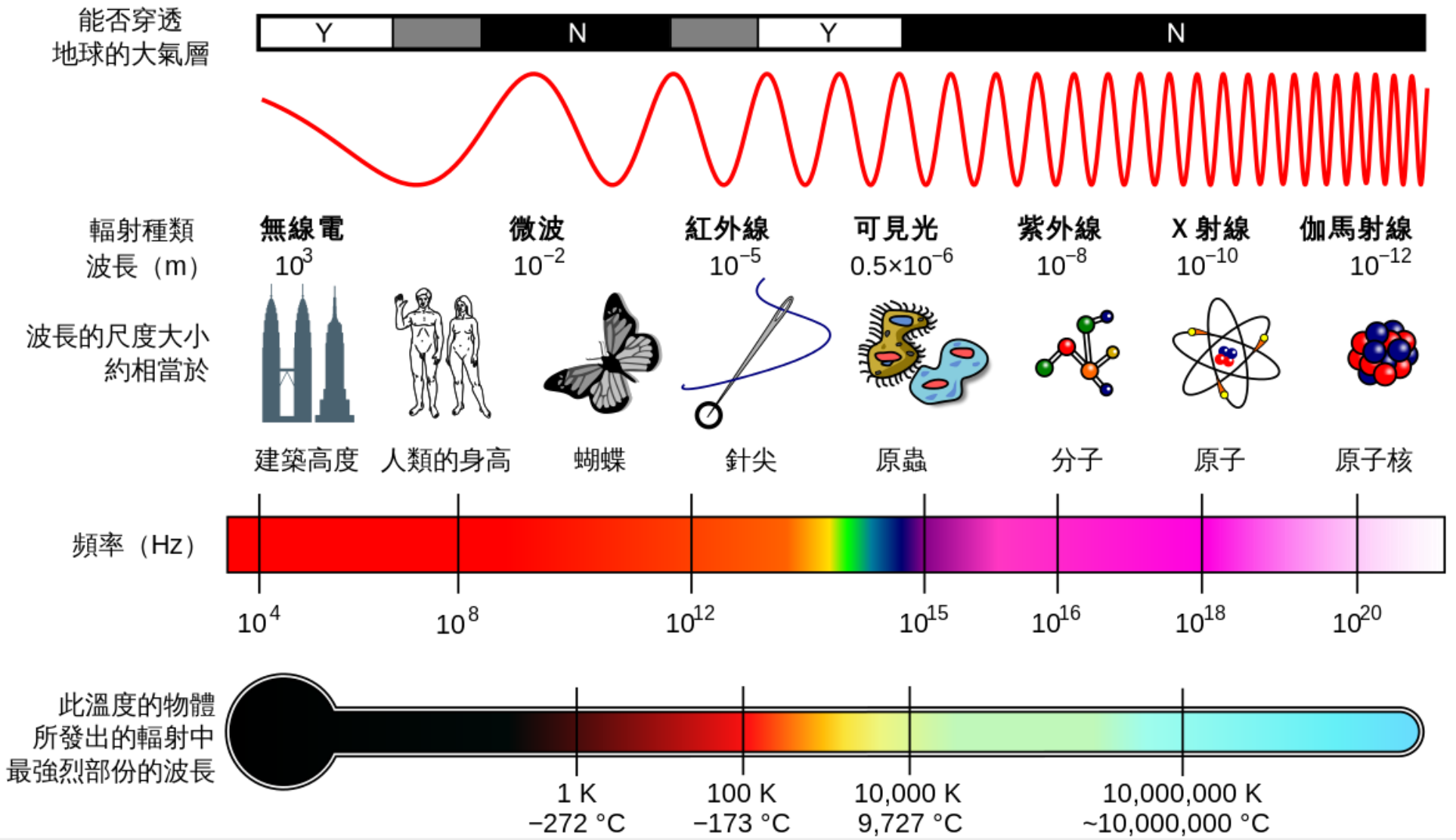
802.11的数据链路层由两个子层构成，逻辑链路控制层LLC(Logic Link Control)和媒体访问控制层MAC(Media Access Control)。 802.11使用和802.3完全相同的LLC子层和48位MAC地址，因此Wi-Fi网络和以太网之间的桥接非常方便。



IEEE 802.11版本

协议(新命名)	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac wave1	802.11ac wave2	802.11ax
					Wi-Fi 4	Wi-Fi 5		Wi-Fi 6
提出时间	1997	1999	1999	2003	2009	2013	2015	2016年7月1.0 2019正式发布
频率范围	2.4GHz	2.4GHz	5GHz	2.4GHz	2.4GHz/ 5GHz	5GHz	5GHz	2.4GHz/5GHz 6GHz待讨论
支持带宽	NA	20MHz	20MHz	20MHz	20/40MHz	20/40/80MHz	20/40/80/160MHz，80+80MHz	20/40/80/160MHz， 80+80MHz
信道（20MHz）	NA	14个	24个	14个	14个/24个	24个	24个	24个
最高阶编码方式	NA	DBPSK/ DQPSK	64QAM	QPSK	64QAM	256QAM	256QAM	1024QAM
最大物理层速率	2Mbps	11Mbps	54Mbps	54Mbps	600Mbps	3.4Gbps	6.9Gbps	9.6Gbps
关键技术		DSSS	DSSS/ OFDM	DSSS/ OFDM	OFDM、 64QAM、4*4 MIMO	OFDM、256QAM、DL MU-MIMO Beamforming		UL/DL OFDMA、 UL/DL 8*8 MU-MIMO、 1024QAM、 空间复用、 Bss-Color、 TWT节能

电磁波谱



ISM频段

ISM频段（Industrial Scientific Medical Band）是各国将无线电波的某一段频段开放给工业，科学和医学机构使用。使用这些频段不需要许可证或费用，只需要遵守一定的发射功率（一般低于1W），并且不要对其它频段造成干扰即可。

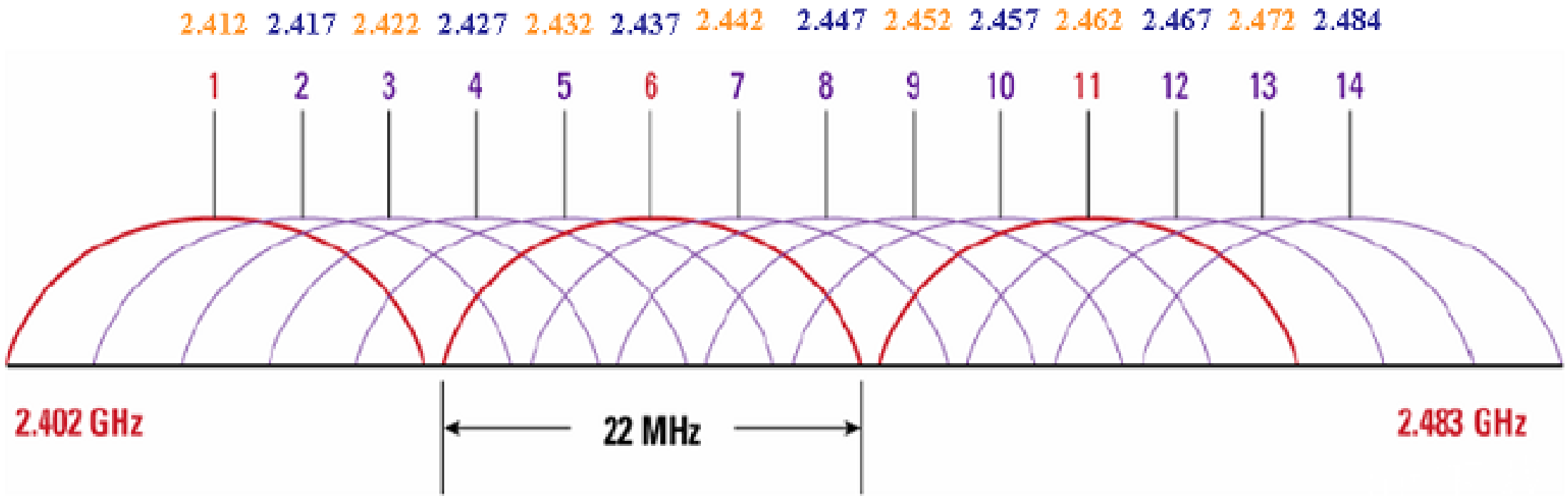
应用：

1. Wi-Fi（2.4G/5G）
2. 蓝牙（2.4G）
3. Zigbee（2.4G/900M）
4. 无线鼠标（2.4G）
5. 遥控玩具（2.4G）
6. 微波炉（2.4G）

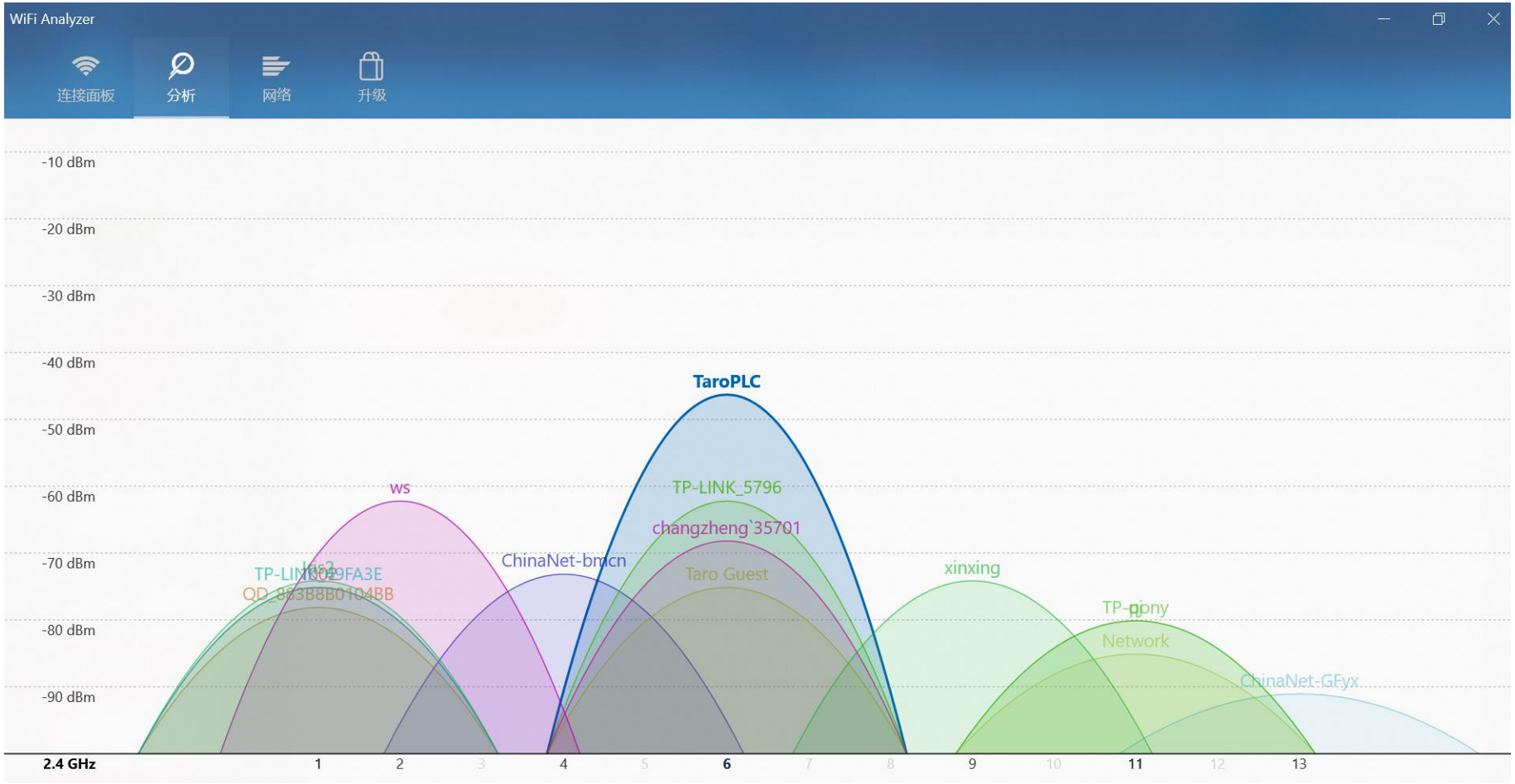
ISM Band Frequencies
6.765 - 6.795 MHz
13.553 - 13.567 MHz
26.957 - 27.283 MHz
40.66 - 40.70 MHz
83.996 - 84.004 MHz
167.992 - 168.008 MHz
433.05 - 434.79 MHz
886 - 906 MHz
2.400 - 2.500 MHz
5.725 - 5.875 MHz
24.0 - 24.25 GHz
61.0 - 61.5 GHz
122 - 123 GHz
244 - 246 GHz

Wi-Fi 频谱

2.4Ghz无线WIFI网络设备一般都支持13/14个信道。它们的中心频率虽然不同，但是因为都占据一定的频率范围，所以会有一些相互重叠的情况。当路由器十分密集时，wifi信号之间互相干扰，导致网速变慢。

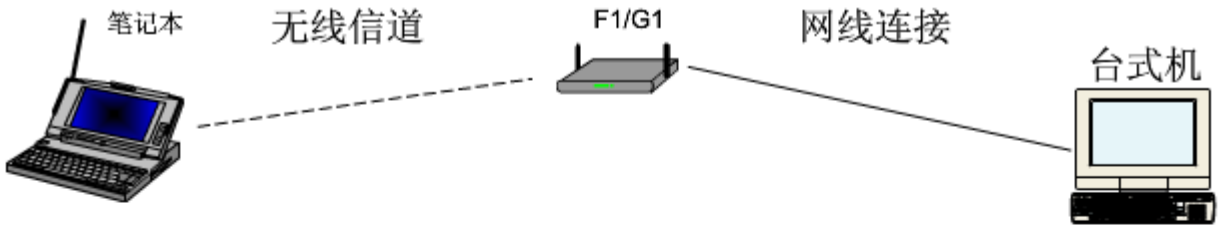


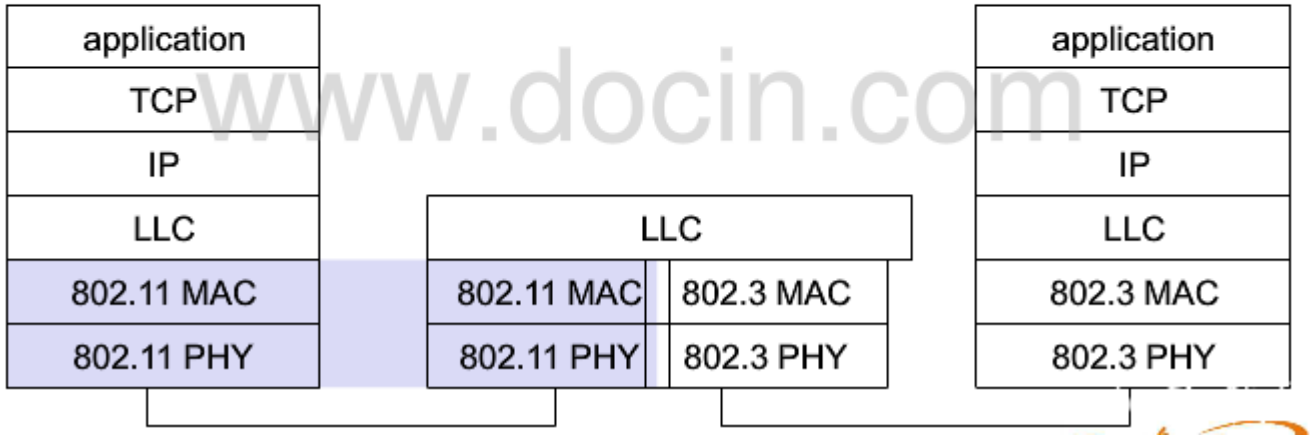
Wi-Fi 信号分析


WiFi Analyzer
连接面板
分析
网络
升级
-10 dBm
-20 dBm
-30 dBm
-40 dBm
-50 dBm
-60 dBm
-70 dBm
-80 dBm
-90 dBm
TaroPLC
TP-LINK_5796
changzheng`35701
Taro Guest
ws
ChinaNet-bmcn
xinxing
TP-
Network
ChinaNet-GFyx
2.4 GHz
1
2
3
4
5
6
7
8
9
10
11
12
13

设备类型

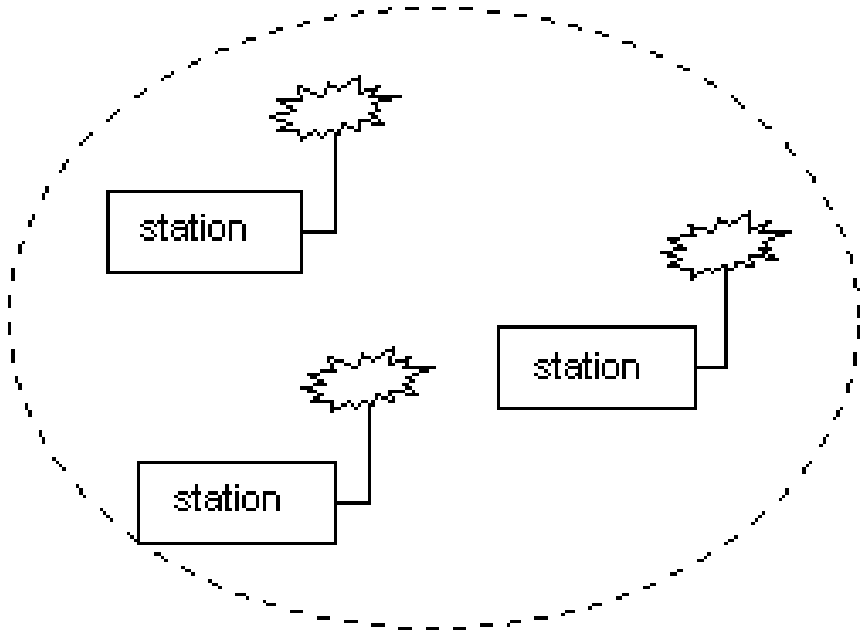
802.11定义了两种类型的设备，一种是无线站（Station，STA），通常是手机或PC机。另一种称为无线接入点(Access Point, AP)，它的作用就像是无线网络的一个无线基站，将多个无线站连接起来，或者将无线站连接到有线网络。



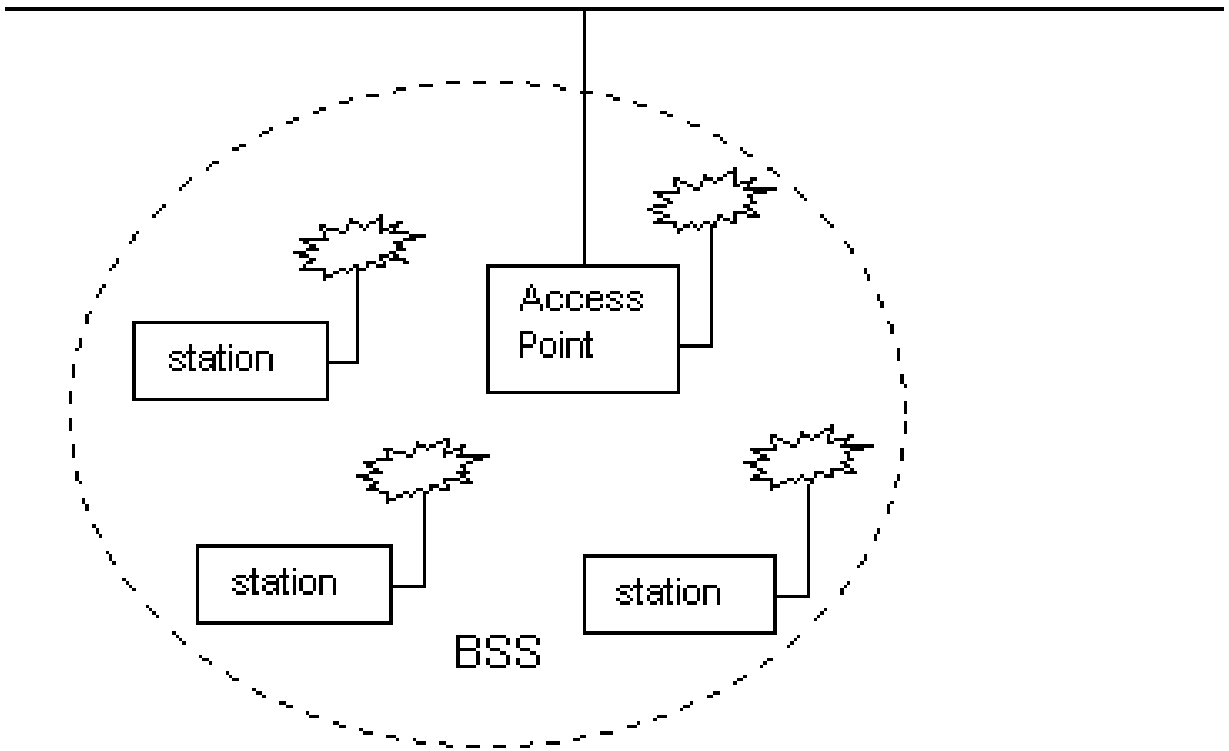


组网方式

Ad-hoc（自组网）

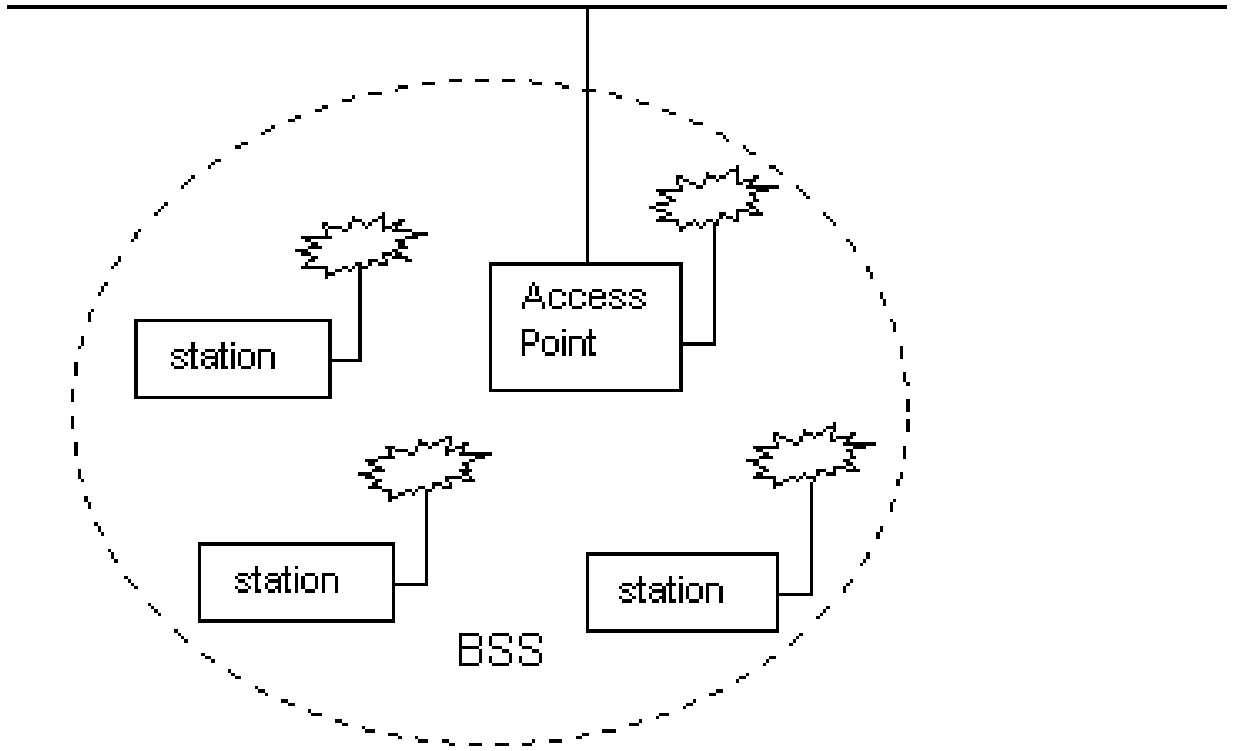


Infrastructure（基础网）



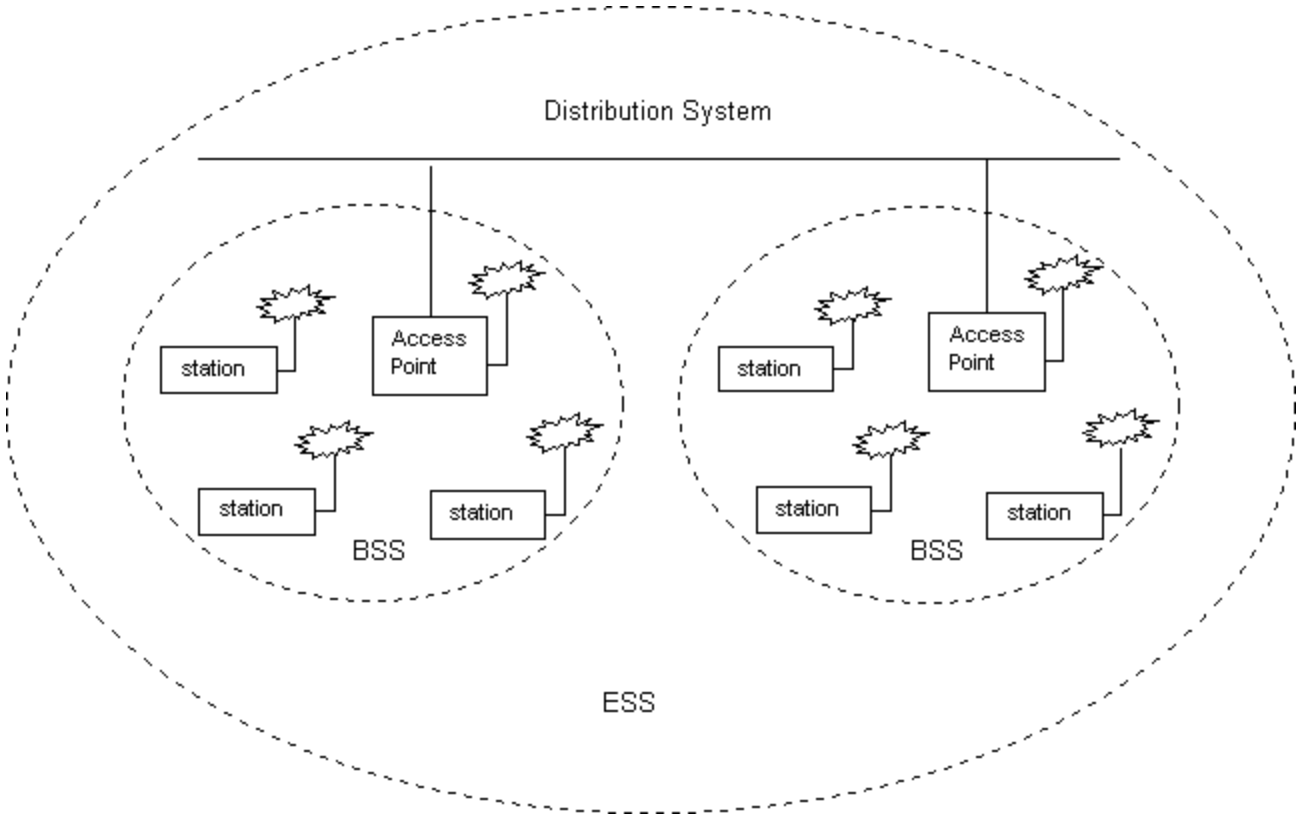
基本服务集（BSS）和BSSID

基本服务集是802.11 LAN的基本组成模块。能互相进行无线通信的STA可以组成一个BSS（Basic Service Set）。如果一个站移出BSS的覆盖范围，它将不能再与BSS的其它成员通信。BSSID是一个BSS的标识，BSSID实际上就是AP的MAC地址，用来标识AP管理的BSS。



扩展服务集（ESS）

多个BSS可以构成一个扩展网络，称为扩展服务集（ESS）网络，一个ESS网络内部的STA可以互相通信，是采用相同的SSID的多个BSS形成的更大规模的虚拟BSS。连接BSS的组件称为分布式系统（Distribution System，DS）。



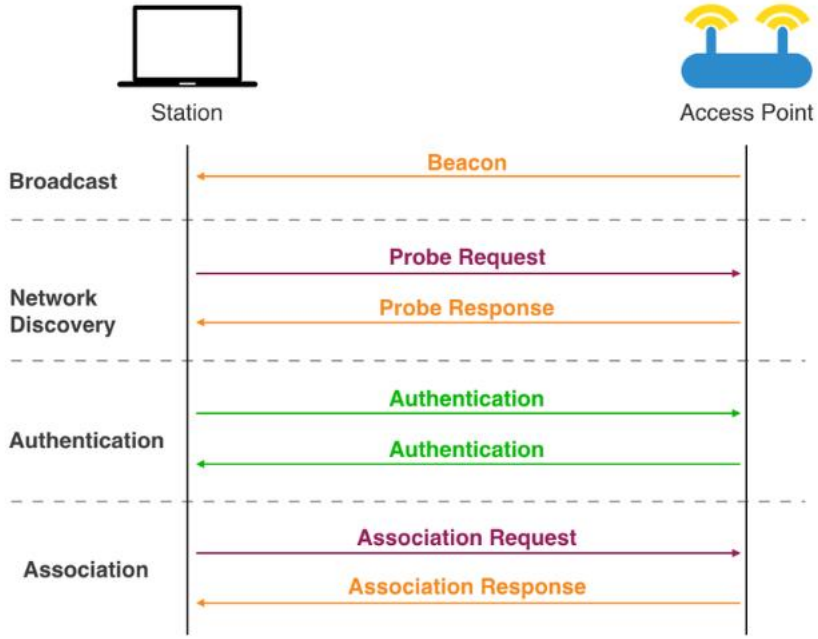
SSID

SSID是一个ESS的网络标识(如:TP_Link_1201)，在同一SS内的所有STA和AP必须具有相同的SSID，否则无法进行通信。在同一个AP内BSSID和SSID一一映射。在一个ESS内SSID是相同的，但对于ESS内的每个AP与之对应的BSSID是不相同的。如果一个AP可以同时支持多个SSID的话，则AP会分配不同的BSSID来对应这些SSID。

Wi-Fi连接过程

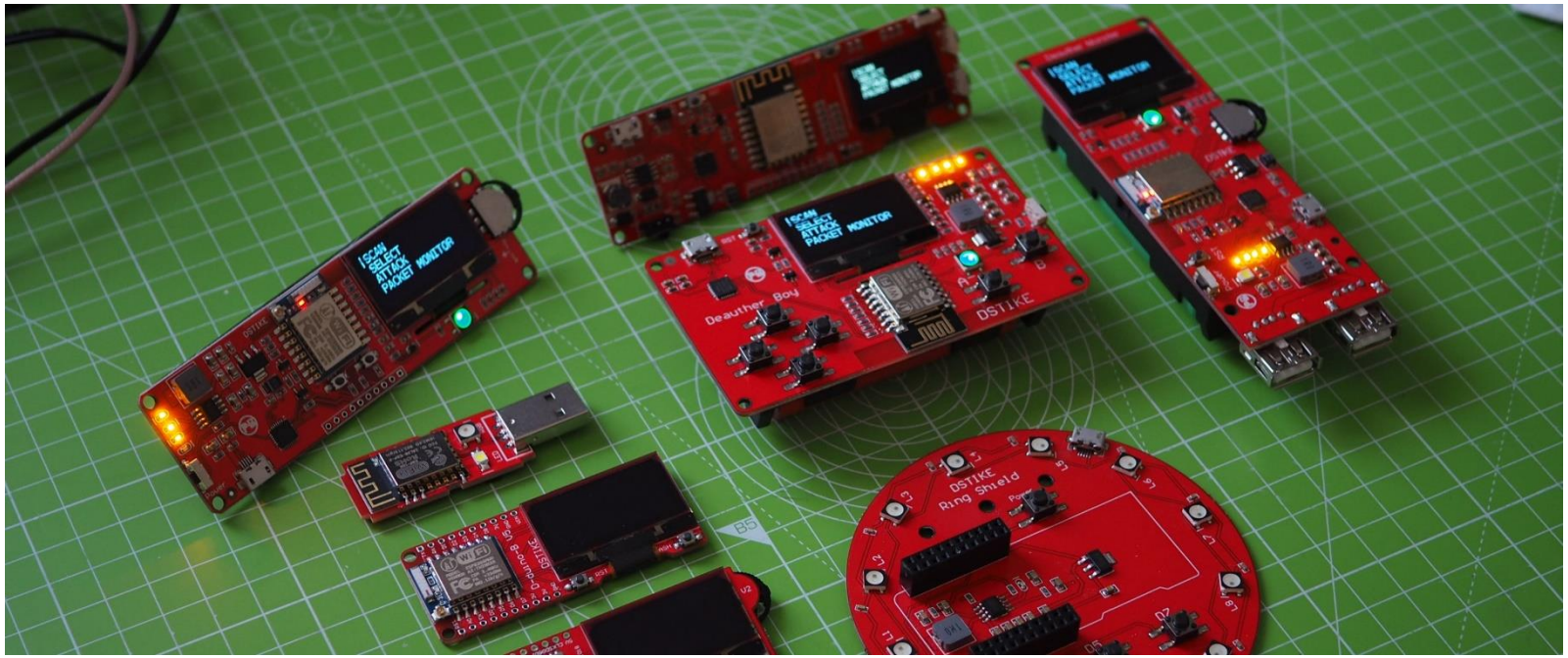
STA(工作站)启动初始化、开始正式使用AP传送数据帧前，要经过三个阶段才能够接入

1. 扫描(Scan)
2. 认证(Authentication)
3. 关联(Association)



Deauthor 攻击

伪造取消认证报文，让已连接AP的设备断开，促使设备重新建立与AP的连接，此时再伪造SSID相同的AP获取设备的Wi-Fi密码。



ESP8266 Deauther https://github.com/spacehuhn/esp8266_deauther

智能硬件的联网方式选择

WiFi的优点：

- 不需要专门的网关设备，即可连接到互联网
- 覆盖范围大，信号好

WiFi的缺点

- 功耗相对较大，不适合使用电池供电
- 星型网络结构，设备数量多了之后会造成AP负载较重
- 配置相对复杂

1) 插电的设备，用WiFi。

2) 电池供电的设备，用BLE，需要配套蓝牙网关使用。

海量视频 贴身学习

超多干货 实时更新

THANKS

谢谢