（5）需求 5

现在我们已经保证给正确的计算机发送正确的封装过后的信息了。但是用户级别的体验好不好？难道我每次都要调用 TCP 去打包，然后调用 IP 协议去找路由，自己去发？当然不行，所以我们要建立一个自动收发包、自动寻址的功能。

于是，科学家们又提出了会话层的概念：建立和管理应用程序之间的通信。允许用户在两个实体设备之间建立、维持和终止会话，并支持它们之间的数据交换。例如提供单方向会话或双向同时会话，并管理会话中的发送顺序，以及会话所占用的时间长短。

（6）需求 6

现在我能保证应用程序自动收发包和寻址了。但是要用 Linux 给 Windows 发包，两个系统的语法不一致，就像安装包一样，exe 是不能在 Linux 系统上用的，shell 在 Windows 系统上也是不能直接运行的。于是需要表示层，帮助解决不同系统之间通信的语法问题。

（7）需求 7

现在所有必要条件都准备好了，我们可以写个 Android 程序，web 程序去实现需求。

因为 OSI 模型的层数太多，顺序也不好记忆，于是有人就用 All People Seem To Need Data Processing 来帮助记忆，因为这 7 个单词的首字母和 OSI 模型每一层的首字母是一样的。

1.4　TCP/IP 网络通信协议

通信协议对物联网来说十分常用且关键，无论是近距离无线传输技术还是移动通信技术，都影响着物联网的发展。通信协议是指双方实体完成通信或服务所必须遵循的规则和约定。

我们将物联网协议分为两大类，一类是传输协议，一类是通信协议。传输协议一般负责子网内设备间的组网及通信。通信协议则主要是运行在传统互联网 TCP/IP 协议之上的设备通信协议，负责设备通过互联网进行数据交换及通信。

物联网的通信环境有 Ethernet、Wi-Fi、RFID、NFC（近距离无线通信）、ZigBee、6LoWPAN（IPv6 低速无线版本）、Bluetooth、GSM、GPRS、GPS、3G 和 4G 等网络，而每一种通信应用协议都有一定的适用范围。AMQP、JMS 和 HTTP 都是工作在以太网的协议，CoAP 协议是专门为资源受限设备开发的协议，MQTT 的兼容性则强很多。

1.4.1　TCP/IP 协议

互联网的发展很大程度上要归功于 Vinton Cerf 和 Robert Kahn 这对老搭档。他们在 20

世纪 70 年代设计的 TCP/IP 协议奠定了现代网络的基石，也因此获得了计算机界的最高荣誉——图灵奖。

TCP/IP 的设计非常成功。几十年来，底层的带宽、延时，还有介质都发生了翻天覆地的变化，顶层也多了不少应用，但 TCP/IP 却安如泰山。它不但战胜了国际标准化组织的 OSI 七层模型，而且目前还看不到被其他方案取代的可能。第一代从事 TCP/IP 工作的工程师，到了退休年龄也在做着朝阳产业。OSI 七层模型过于笨重，在实际应用中，市场明显更青睐 TCP/IP 四层模型。

TCP/IP 是一个四层协议系统，如图 1.2 所示。

应用层：Telnet、FTP、E-mail
运输层：TCP、UDP
网络层：IP、ICMP、IGMP
链路层：设备驱动程序及接口卡

图 1.2　TCP/IP 四层协议系统

每一层负责不同的功能。

- 链路层：也称数据链路层或网络接口层。包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。
- 网络层：也称互联网层。处理分组在网络中的活动，例如分组的选路。
- 运输层：也称传输层。主要为两台主机上的应用程序提供端到端的通信。
- 应用层：负责处理特定的应用程序细节。

TCP/IP 协议族具体包含多个协议，如图 1.3 所示。

IP 协议负责数据传输到哪里，而 TCP 协议负责数据的可靠传输。它们在数据传输过程中主要完成以下功能：

（1）由 TCP 协议把数据分成若干数据包，给每个数据包写上序号，以便接收端把数据还原成原来的格式。

（2）IP 协议给每个数据包写上发送主机和接收主机的地址，一旦写上源地址和目的地址，数据包就可以在互联网上传送数据了。IP 协议还具有利用路由算法进行路由选择的功能。

（3）这些数据包可以通过不同的传输途径（路由）进行传输，由于路径不同，加上其他的原因，可能出现顺序颠倒、数据丢失、数据失真甚至重复的现象。这些问题都由 TCP 协议来处理，它具有检查和处理错误的功能，必要时还可以请求发送端重发。

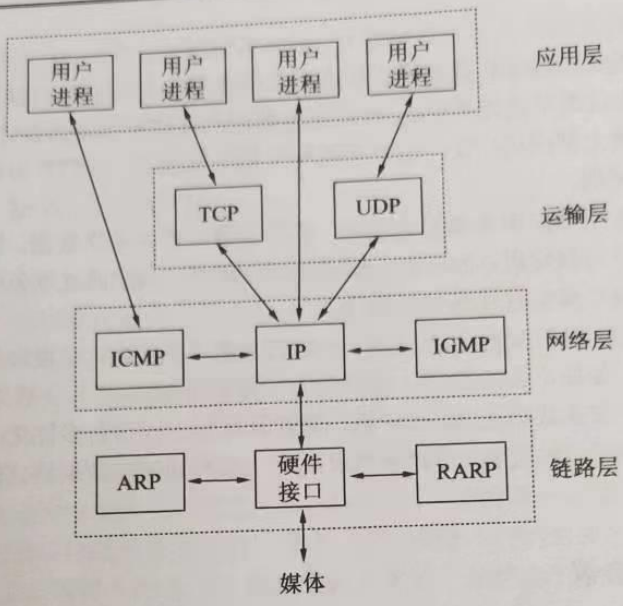


图 1.3　TCP/IP 协议族

TCP/IP 协议族跟 OSI 模型的对比，如图 1.4 所示。

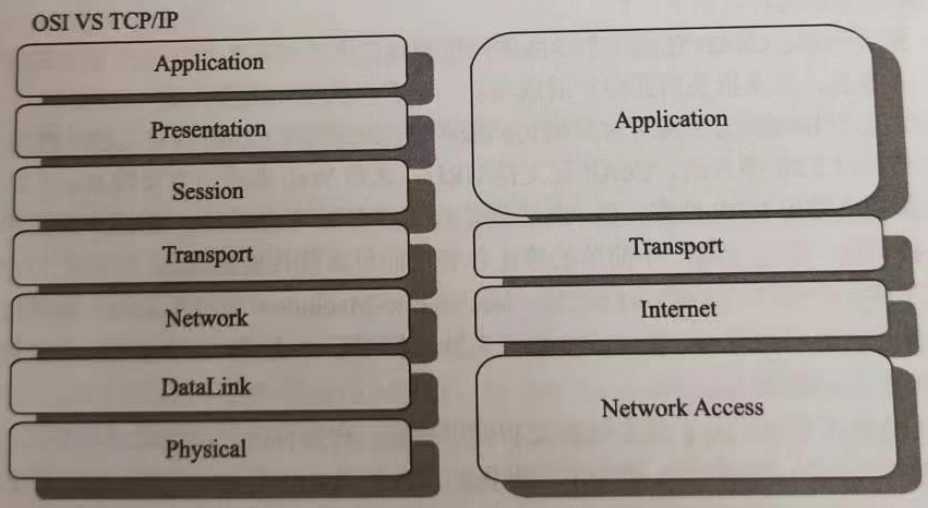


图 1.4　OSI TCP/IP 比较

互联网时代，TCP/IP 协议已经一统江湖，现在的物联网的通信架构也是构建在传统互联网基础架构之上。在当前的互联网通信协议中，HTTP 协议由于开发成本低，开放程度高的优势，几乎占据了大半江山，所以很多厂商在构建物联网系统时也基于 HTTP 协议进行开发。包括 Google 主导的 physic web 项目，都是期望在传统 Web 技术基础上构建物

联网协议标准。

HTTP 协议是典型的 CS 通信模式，由客户端主动发起连接，向服务器请求 XML 或 JSON 数据。该协议最早是为了适用 Web 浏览器的上网浏览场景而设计的，目前在 PC、手机、Pad 等终端上都应用广泛，但并不适用于物联网场景。HTTP 协议在物联网场景中应用有以下三大弊端：

- 必须由设备主动向服务器发送数据，难以主动向设备推送数据。这对于数据采集等场景还可以勉强适用，但是对于频繁的操控场景，只能通过设备定期主动拉取的方式，实现成本和实时性都大打折扣。
- 安全性不高。由于 Web 的不安全性，HTTP 是明文协议，在很多要求高安全性的物联网场景，如果不做很多安全准备工作（如采用 https 等），后果将不堪设想。
- 不同于用户交互终端如 PC、手机，物联网场景中的设备多样化，对于运算和存储资源都十分受限的设备，HTTP 协议实现、XML/JSON 数据格式的解析，都是不可能的任务。

1.4.2 CoAP 协议

CoAP（Constrained Application Protocol，受限应用协议），应用于无线传感网中的协议，是 6LowPAN 协议栈中的应用层协议，适用于资源受限的通信网络。

CoAP 协议的特点如下：

- 报头压缩：CoAP 包含一个紧凑的二进制报头和扩展报头。它只有短短的 4B 本报头，基本报头后面跟扩展选项。一个典型的请求报头为 10～20B。
- 方法和 URIs：为了实现客户端访问服务器上的资源，CoAP 支持 GET、PUT、POST 和 DELETE 等方法。CoAP 还支持 URIs，这是 Web 架构的主要特点。
- 传输层使用 UDP 协议：CoAP 协议是建立在 UDP 协议之上，以减少开销和支持组播功能。它也支持一个简单的停止和等待的可靠性传输机制。
- 支持异步通信：HTTP 对 M2M（Machine-to-Machine）通信不适用，这是由于事务总是由客户端发起。而 CoAP 协议支持异步通信，这对 M2M 通信应用来说是常见的休眠/唤醒机制。
- 支持资源发现：为了自主地发现和使用资源，它支持内置的资源发现格式，用于发现设备上的资源列表，或者用于设备向服务目录公告自己的资源。它支持 RFC5785 中的格式，在 CoAP 中用/.well—known/core 路径表示资源描述。
- 支持缓存：CoAP 协议支持资源描述的缓存，可以优化其性能。

CoAP 协议主要实现：

- libcoap（C 语言实现）；
- Californium（Java 语言实现）。

CoAP 和 6LowPan，分别是应用层协议和网络适配层协议，其目标是解决设备直接连

中，但是它只知道目标主机的 IP 地址，这样就需要地址解析协议（Address Resolution Protocol，ARP）来帮助它找到目标主机的链路层地址，这时路由器就会发送 ARP 请求，在 LAN 中寻找与报文目的 IP 地址对应的 MAC 地址及此主机连接的端口。这样，就完成了 LAN 内的寻址。同时在二层交换机上会有一张 MAC 地址表来帮助以后报文进行 LAN 内的转发。

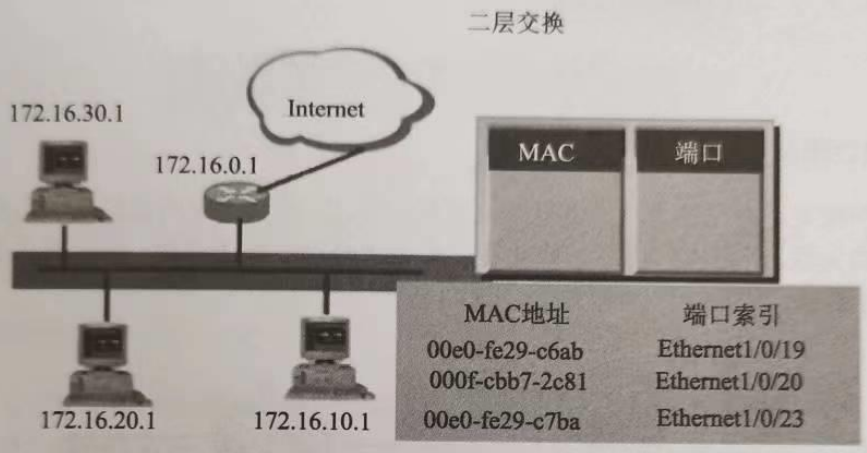


图 2.4　二层交换原理

二层交换的特点总结：

- ARP 解析可以获得对端 MAC 地址；
- 交换机学习 MAC 地址映射。

二层交换的关键数据就是 MAC 表，MAC 表记录了访问指定 MAC 地址的报文需要交换到哪个端口。MAC 是二层交换的核心。

2.7　三层转发——路由器原理

路由器是指用于网络互连的计算机设备，它的主要作用如下：

- 路由（寻径）：学习和维护网络拓扑结构知识的机制，产生和维护路由表。
- 交换/转发：数据在路由器内部移动与处理的过程（从路由器一个接口输入，然后选择合适的接口输出，做帧的解封装与封装，并对包做相应处理）。
- 隔离广播，指定访问规则。
- 异种网络互连。

路由设备的工作流程如图 2.5 所示。

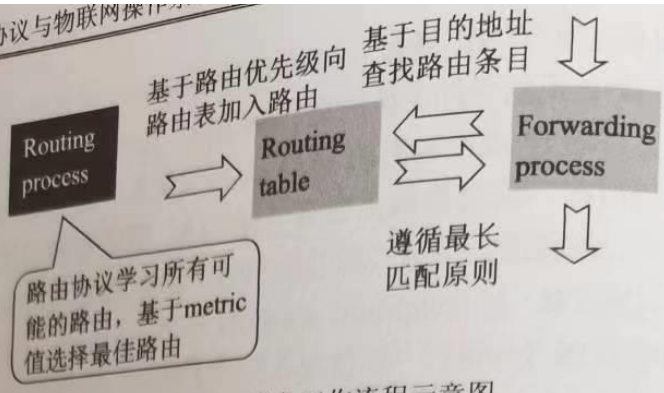
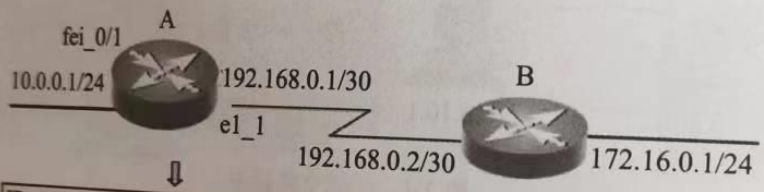


图 2.5　路由设备工作流程示意图

1. 直连路由

当接口配置了网络协议地址并状态正常时，接口上配置的网段地址自动出现在路由表中并与接口关联，并随接口的状态变化在路由表中自动出现或消失。IPv4 路由表结构示意图如图 2.6 所示。



IPv4 Routing Table:

Dest	Mask	Gw	Interface	Owner	pri	metric
10.0.0.0	255.255.255.0	10.0.0.1	fei_0/1	direct	0	0
10.0.0.1	255.255.255.255	10.0.0.1	fei_0/1	address	0	0
192.168.0.0	255.255.255.255	192.168.0.1	e1_1	direct	0	0
192.168.0.1	255.255.255.255	192.168.0.1	e1_1	address	0	0

ZXR10#

图 2.6　IPv4 路由表结构示意图

2. 静态路由

静态路由是一条单向路由，还需要在对方的路由设备上配置一条相反的路由。静态路由示意图如图 2.7 所示。

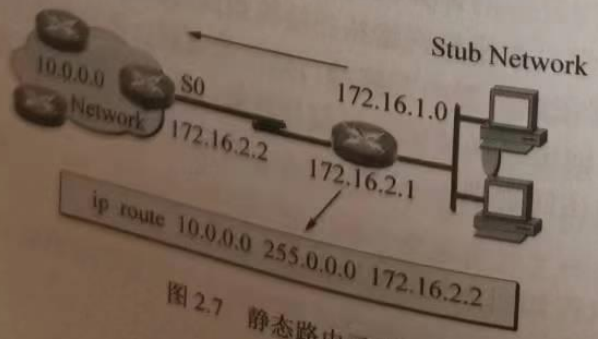


图 2.7　静态路由示意图

默认路由配置示例如图 2.8 所示。

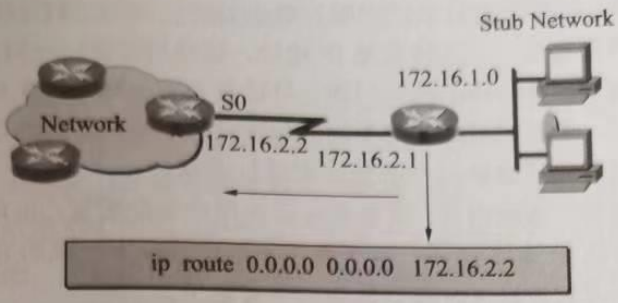


图 2.8　静态路由默认配置

默认配置路由可以配置在只有一条出口的“根状网络”的出口路由设备上，可以访问“未知的”目的网络。

3. 动态路由

动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由机制的运作依赖路由器的两个基本功能：路由器之间适时的路由信息交换，以及对路由表的维护。

路由协议是运行在路由器上的软件进程，与其他路由器上相同路由协议之间交换路由信息，学习非直连网络的路由信息，并加入路由表，并且在网络拓扑结构变化时能自动调整，维护正确的路由信息。

常见的动态路由协议有以下几个：

- RIP 协议：路由信息协议（RIP）是内部网关协议 IGP 中最先得到广泛使用的协议。RIP 是一种分布式的基于距离向量的路由选择协议，是因特网的标准协议，其最大优点就是实现简单，开销较小。
- OSPF 协议：OSPF（Open Shortest Path First，开放式最短路径优先）是一个内部网关协议（Interior Gateway Protocol，IGP），用于在单一自治系统（Autonomous System，AS）内决策路由。

动态路由工作机制如图 2.9 所示。

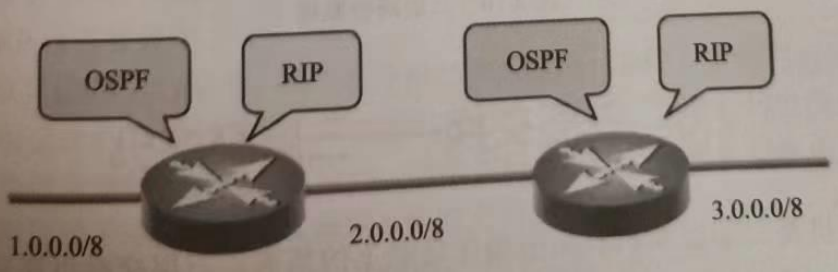


图 2.9　动态路由工作机制

路由转发的核心是路由表。

三层 IP 转发和二层交换有什么区别呢？最主要的区别是它们寻找目的地的关键字不同，二层交换是链路层地址，三层转发是 IP 地址。链路层地址——MAC 地址，通常存在于一个平面地址空间，没有清晰的地址层次，只适合于同一网段内主机的通信。对于不同网络之间的互连通信，考虑到可能使用不同的传输介质，不同的链路层协议，为提供更大的灵活性，通常使用网络层地址——IP 地址来寻址通信。

每个路由器中都有一张路由表，这张表可以由用户手动配置，也可以从动态路由协议中学到。该表的索引是 IP 地址/掩码，每个表项中都存放有下一跳的 IP 地址和出口。有了这张表，路由器接在收到数据包时就能做到心中有数了。

如图 2.10 所示，IP 地址为 192.4.1.1 的主机要访问远端 IP 地址为 192.5.1.1 的主机。数据包需要先在接入路由器上查找路由，一般情况下接入路由器上路由表项都比较简单，对所有网段的地址都指向其直连的上游设备 20.1.1.2.。然后还需在 20.1.1.2 上查找路由表，找到匹配项 192.5.1.0 /24 ：10.1.1.1，就从 10.1.1.2 所在的接口通过 E1 链路将数据包发送出去。在 10.1.1.1 上接收到报文后，检查数据报的目的地址，发现在其直连网段，遂将数据报文正确送到 IP 地址为 192.5.1.1 的主机，从而完成一次完整的转发。

IP 转发的特点总结：

- 报文逐跳转发；
- 报文的转发单位可以是数据包，也可以是数据流。

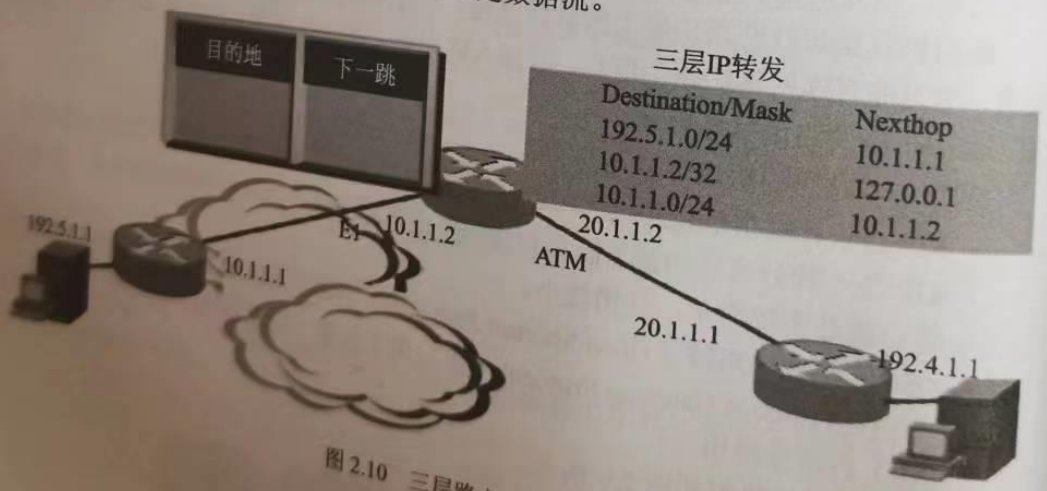


图 2.10 三层路由原理

2.8 三层交换——三层交换机

三层交换机是二层交换机和路由器在功能上的集成，三层交换机在功能上实现了 VLAN 的划分，VLAN 内部的二层交换和 VLAN 间路由的功能。

IEEE 802.11 网络协议定义了基本服务集（basic service set），包含物理组件和服务集合。

3.2.1　Wi-Fi 物理组件

（1）工作站（Station）

构建网络的目的是为了在工作站间传送数据。所谓工作站，是指配备无线网络接口的计算设备。

（2）接入点（Access Point，AP）

IEEE 802.11 网络所使用的帧必须经过转换，方能被传递至其他不同类型的网络上。具备无线至有线的桥接功能的设备称为接入点，接入点的功能不仅于此，但桥接最为重要。接入点既有普通站点的身份，又有接入到分布系统的功能。

（3）无线热点布式系统（Distribution System，DS）

当几个接入点串联以覆盖较大区域时，彼此之间必须相互通信以掌握移动式工作站的行踪。分布式系统属于 802.11 的逻辑组件，负责将帧转送至目的地。

802.11 并没有规范分布式系统的技术细节。大多数商用产品是以桥接引擎（Bridging engine）和分布式系统媒介（Distribution system medium）共同组成分布式系统。分布系统用于连接不同的基本服务单元。分布系统使用的媒介（Medium）逻辑上和基本服务单元使用的媒介是截然分开的，尽管它们物理上可能会是同一个媒介，例如同一个无线频段。

WDS，即无线热点分布系统，它是无线 AP 和无线路由中一个特别的功能，简单来说就是 AP 的中继加桥接功能，它可以实现两个无线设备通信，也可以起到放大信号的作用，而产品的 SSID 也可以不同。这是一个非常实用的功能，比如有三户邻居，每户都有一个支持 WDS 的无线路由器或 AP，这样无线信号就可以在这三户同时覆盖了，使得相互的通信更加方便。但要注意的是，每个品牌的无线路由所支持的 WDS 设备是有限制的（一般可以支持 4～8 个设备），不同品牌的 WDS 功能不一定可以链接成功。

（4）无线媒介（Wireless Medium）

IEEE 802.11 标准以无线媒介在工作站之间传递帧。其所定义的物理层不只一种，IEEE 802.11 最初标准化了两种射频物理层及一种红外线物理层；存在 3 种媒介：站点使用的无线媒介、分布系统使用的媒介，以及和无线局域网集成的其他局域网使用的媒介。物理上它们可能互相重叠。

IEEE 802.11 只负责在站点使用的无线媒介上的寻址（Addressing）。分布系统和其他局域网的寻址不属无线局域网的范围。

3.2.2　Wi-Fi 服务功能

1. 基本服务集（BSS）

基本服务集是 IEEE 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 的其他成员通信。

2. 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，如图 3.2 所示。一个 ESS 网络内部的 STA 可以互相通信，是采用相同 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）。

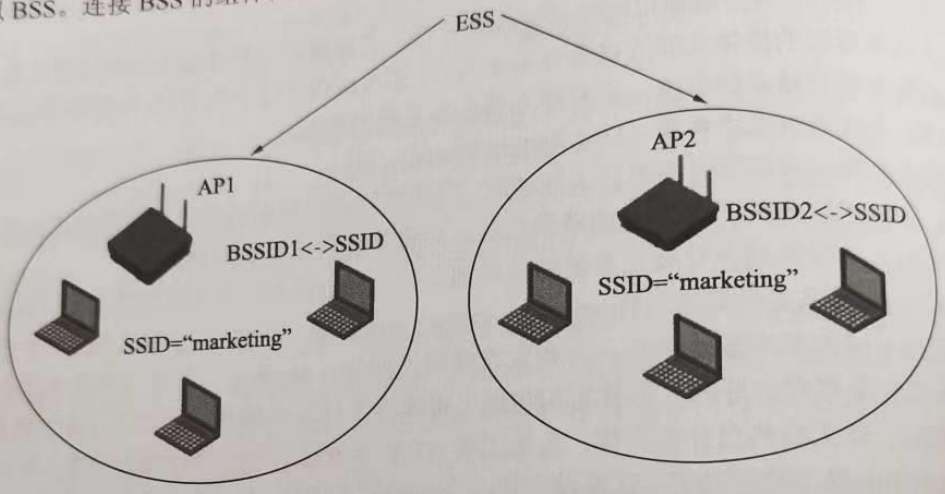


图 3.2 扩展服务集（ESS）网络

3. 服务集的标识（SSID）

服务集的标识SSID(Service Set Identifier)是一个ESS的网络标识(如TP_Link_1201)，通俗地说，SSID 是用户给自己的无线网络所取的名字。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，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，BSSID(MAC) ↔ SSID。

IEEE 802.11 没有具体定义分布系统，只是定义了分布系统应该提供的服务(Service)。整个无线局域网定义了 9 种服务。其中：

- 5 种服务属于分布系统的任务，分别为联接(Association)、结束联接(Diassociation)、分配（Distribution）、集成（Integration）和再联接（Reassociation）。
- 4 种服务属于站点的任务，分别为鉴权(Authentication)、结束鉴权(Deauthentication)、隐私（Privacy）和 MAC 数据传输（MSDU delivery）。

4. 无线接入点AP功能

无线 AP，即 Access Point，也就是无线接入点。简单来说就是无线网络中的无线交换机，它是移动终端用户进入有线网络的接入点，主要用于家庭宽带、企业内部网络部署等，无线覆盖距离为几十米至上百米，目前主要技术为 IEEE 802.11X 系列。一般的无线 AP 还带有接入点客户端模式，也就是说 AP 之间可以进行无线连接，从而可以扩大无线网络的覆盖范围。AP 的主要功能如下：

- 中继：所谓中继就是在两个无线点间把无线信号放大一次，使得远端的客户端可以接受到更强的无线信号。例如在 a 点放置一个 AP，而在 c 点有一个客户端，之间有 120 米的距离，从 a 点到 c 点信号已经削弱很多，于是在中途 60 米处的 b 点放一个 AP 作为中继，这样 c 点的客户端的信号就可以有效地增强，保证了传输速度和稳定性。
- 桥接：桥接就是链接两个端点，实现两个无线 AP 间的数据传输。想要把两个有线局域网连接起来，一般就选择通过 AP 来桥接。例如在 a 点有一个由 15 台计算机组成的有线局域网，b 点有一个由 25 台计算机组成的有线局域网，但是 a、b 两点间的距离很远，超过了 100 米，通过有线连接已不可能，那么怎么把两个局域网连接在一起呢？这就需要在 a 点和 b 点各设置一个 AP，开启 AP 桥接功能，这样 a、b 两点的局域网就可以互相传输数据了。需要提醒的是，没有 WDS 功能的 AP，桥接后两点是没有无线信号覆盖的。
- 主从模式：在这个模式下工作的 AP 会被主 AP 或者无线路由看作是一台无线客户端，比如无线网卡或者是无线模块。这样可以方便网管统一管理子网络，实现一点对多点的连接，AP 的客户端是多点，无线路由或主 AP 是一点。这个功能常被应用在无线局域网和有线局域网的连接中，比如 a 点是一个由 20 台计算机组成的有线局域网，b 点是一个由 15 台计算机组成的无线局域网，b 点已经是有一台无线路由了，如果 a 想接入 b，在 a 点加一个 AP，并开启主从模式，并把 AP 接入 a 点的交换机中，这样所有 a 点的计算机就可以连接 b 点的计算机了。

5. Wi-Fi快连（配置）

什么是快连呢？手机（设备 B）已经接入了 AP，而设备 A 是一个信息“孤岛”。手机将 AP 的信息直接发送给设备 A，设备 A 就可以接入 AP 了。

可以这样认为，Wi-Fi 快连就是接入 AP 的手机快速配置设备，是设备 A 接入 AP 的方式。实现原理是：手机通过 UDP 广播，将 AP 的相关信息组帧发出。而 Wi-Fi 模块（设备 A）一直处于 UDP 监听状态。获取到 AP 信息之后，Wi-Fi 模块（设备 A）便可以接入 AP 了。

6. 胖AP与瘦AP

Fat AP 将 WLAN 的物理层、用户数据加密、用户认证、QoS、网络管理、漫游技术

及其他应用层的功能集于一身。Fat AP 无线网络解决方案可由 Fat AP 直接在有线网的基础上构成。Fat AP 设备结构复杂，且难于集中管理。

Fit AP 是一个只有加密、射频功能的 AP，功能单一，不能独立工作。整个 Fit AP 无线网络解决方案由 AC 和 Fit AP 在有线网的基础上构成。

Fit AP 上“零配置”，所有配置都集中到 AC 上。这也促成了 Fit AP 解决方案更加便于集中管理，并由此具有三层漫游、基于用户下发权限等 Fat AP 不具备的功能。

FAT AP 和 FIT AP 比较如图 3.3 所示。

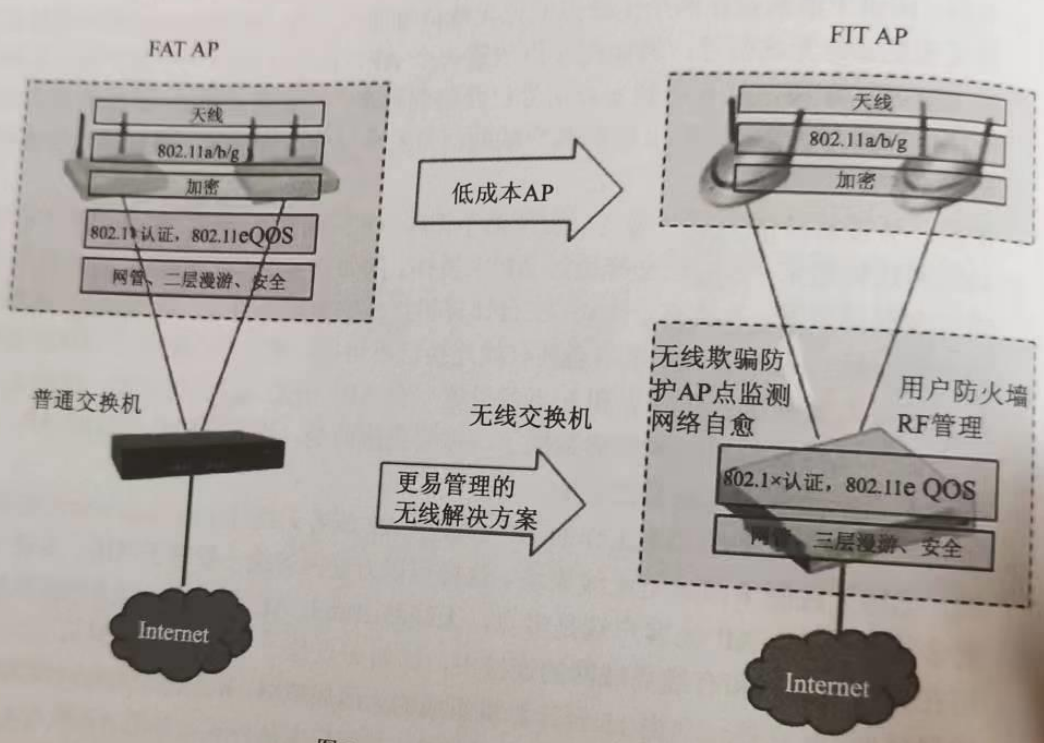


图 3.3　Fat AP 和 Fit AP 比较

3.2.3　Wi-Fi 认证和加密

1. 概念

认证允许只有被认可的用户才能连接到无线网络；加密的目的是提供数据的保密性，完整性，数据在传输过程中不会被篡改。

2. 阶段划分

初级版本：