第 1 章

局域网实验

1.1 局域网基础理论

局域网（Local Area Network，LAN）是指在某一区域内由多台计算机互连成的计算机组，一般是方圆几千米以内。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。

局域网是在一个局部的地理范围内（如一个学校、工厂和机关内），一般是方圆几千米以内，将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网，它可以通过数据通信网或专用数据电路，与远方的局域网、数据库或处理中心相连接，构成一个较大范围的信息处理系统。局域网可以实现文件管理、应用软件共享、打印机共享、扫描仪共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网严格意义上是封闭型的，它可以由办公室内几台甚至上千上万台计算机组成。决定局域网的主要技术要素为：网络拓扑、传输介质与介质访问控制方法。

局域网由网络硬件（包括网络服务器、网络工作站、网络打印机、网卡、网络互连设备等）和网络传输介质，以及网络软件组成。

为了完整地给出 LAN 的定义，必须使用两种方式：一种是功能性定义，另一种是技术性定义。前一种将 LAN 定义为一组台式计算机和其他设备，在物理地址上彼此相隔不远，以允许用户相互通信和共享如打印机和存储设备之类的计算资源的方式互连在一起的系统，这种定义适用于办公环境下的 LAN、工厂和研究机构中使用的 LAN。而后一种将 LAN 定义为由特定类型的传输媒体（如电缆、光缆和无线媒体）和网络适配器（也称为网卡）互连在一起的计算机，并受网络操作系统监控的网络系统。

功能性和技术性定义之间的差别是很明显的，功能性定义强调的是外界行为和服务，技术性定义强调的则是构成 LAN 所需的物质基础和构成的方法。

局域网（LAN）的名字本身就隐含了这种网络地理范围的局域性。由于较小的地理范围的局限性，LAN 通常要比广域网（WAN）具有高得多的传输速率。例如，LAN 的传输速率为 10Mb/s，FDDI 的传输速率为 100Mb/s，而 WAN 的主干线速率国内仅为 64Kb/s 或 2.048Mb/s，最终用户的上限速率通常为 14.4Kb/s。

局域网一般为一个部门或单位所有，建网、维护以及扩展等较容易，系统灵活性高。其主要特点是：

- 覆盖的地理范围较小，只在一个相对独立的局部范围内联，如一座或集中的建筑群内。
- 使用专门铺设的传输介质进行联网，数据传输速率高（10Mb/s～10Gb/s）。
- 通信延迟时间短，可靠性较高（传输的时延一般在几毫秒到几十毫秒之间，其误码率一般为 10^{-11}～10^{-8}）。
- 局域网可以支持多种传输介质（电话线、同轴电缆、光纤、双绞线、红外线、卫星等）。

此外，局域网还有诸如高可靠性、易扩缩和易于管理及安全等多种特性。

1.1.1 局域网分类

局域网的类型很多，若按网络使用的传输介质分类，可分为有线网和无线网；若按网络拓扑结构分类，可分为总线网、星状、环状、树状、混合网等；若按传输介质所使用的访问控制方法分类，又可分为以太网、令牌环网、FDDI 网和无线局域网等。其中，以太网是当前应用最普遍的局域网技术。

1．拓扑结构

局域网通常是分布在一个有限地理范围内的网络系统，一般所涉及的地理范围只有几公里。局域网专用性非常强，具有比较稳定和规范的拓扑结构。常见的局域网拓扑结构如下。

（1）星状

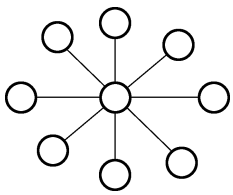

图 1-1 星状拓扑图

这种结构的网络是各工作站以星状方式连接起来的，网中的每一个节点设备都以中防节为中心，通过连接线与中心节点相连，如图 1-1 所示。如果一个工作站需要传输数据，它首先必须通过中心节点。由于在这种结构的网络系统中，中心节点是控制中心，任意两个节点间的通信最多只需两步，所以，传输速度快，并且网络构形简单，建网容易，便于控制和管理。但这种网络系统，网络可靠性低，网络共享能力差，并且一旦中心节点出现故障则导致全网瘫痪。

（2）树状

树状结构网络是天然的分级结构，又被称为分级的集中式网络。其特点是网络成本低，结构比较简单。在网络中，任意两个节点之间不产生回路，每个链路都支持双向传输，并且，网络中节点扩充方便、灵活，寻查链路路径比较简单，如图 1-2 所示。

但在这种结构网络系统中，除叶节点及其相连的链路外，任何一个工作站或链路产生故障会影响整个网络系统的正常运行。

（3）总线网

总线网结构网络是将各个节点设备和一根总线相连，如图 1-3 所示。网络中所有的节点工作站都是通过总线进行信息传输的，作为总线的通信连线可以是同轴电缆、双绞线，也可以是扁平电缆。在总线结构中，作为数据通信必经的总线的负载能量是有限度的，这是由通信媒体本身的物理性能决定的。所以，总线结构网络中工作站节点的个数是有限制的，如果工作站节点的个数超出总线负载能量，就需要延长总线的长度，并加入相当数量的附加转接部件，使总线负载达到容量要求。总线网结构网络简单、灵活，可扩充性能好，所以，进行节点设备的插入与拆卸非常方便。另外，总线结构网络可靠性高、网络节点间响应速度快、共享资源能力强、设备投入量少、成本低、安装使用方便，当某个工作站节

点出现故障时，对整个网络系统影响小。因此，总线结构网络是最普遍使用的一种网络。但是由于所有的工作站通信均通过一条共用的总线，所以，实时性较差。

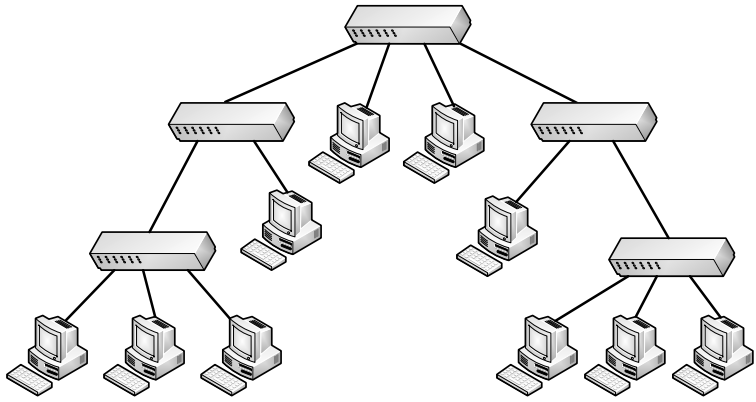

图 1-2　树状拓扑图

（4）环状

环状结构是网络中各节点通过一条首尾相连的通信链路连接起来的一个闭合环状结构网，如图 1-4 所示。环状结构网络的结构也比较简单，系统中各工作站地位相等，系统中通信设备和线路比较节省。

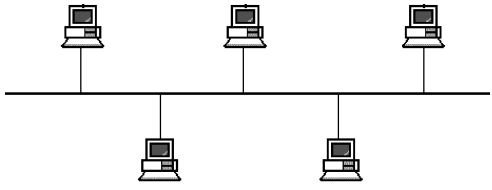

图 1-3　总线网拓扑图

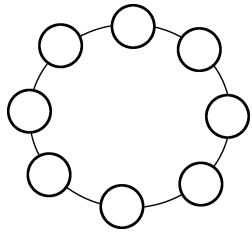

图 1-4　环状拓扑图

在网络中信息设有固定方向单向流动，两个工作站节点之间仅有一条通路，系统中无信道选择问题，某个节点的故障将导致物理瘫痪。环网中，由于环路是封闭的，所以不便于扩充，系统响应延时长，且信息传输效率相对较低。

2．传输介质所使用的访问控制方法

（1）以太网

以太网（Ethernet）指的是由 Xerox 公司创建并由 Xerox、Intel 和 DEC 公司联合开发的基带局域网规范，是当今现有局域网采用的最通用的通信协议标准，如图 1-5 所示。以太网络使用 CSMA/CD（载波监听多路访问及冲突检测）技术，并以 10Mb/s 的速率运行在多种类型的电缆上。以太网与 IEEE802.3 系列标准相类似。

标准的以太网（10Mb/s）、快速以太网（100Mb/s）和 10G（10Gb/s）以太网。它们都符合 IEEE802.3。

（2）令牌环网

令牌环网（Token-ring Network）常用于 IBM 系统中，其支持的速率为 4Mb/s 和 16Mb/s

两种，如图 1-6 所示。目前 Novell、IBM LAN Server 支持 16Mb/s IEEE802.5 令牌环网技术。在这种网络中，有一种专门的帧称为“令牌”，在环路上持续地传输来确定一个节点何时可以发送数据包。

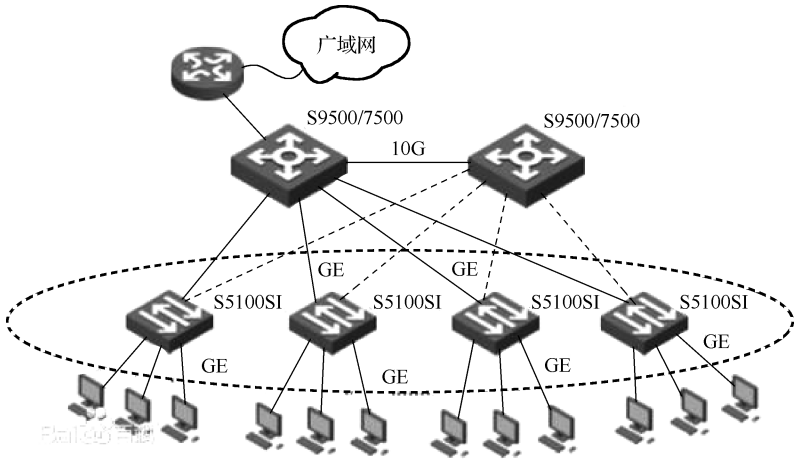

图 1-5　以太网

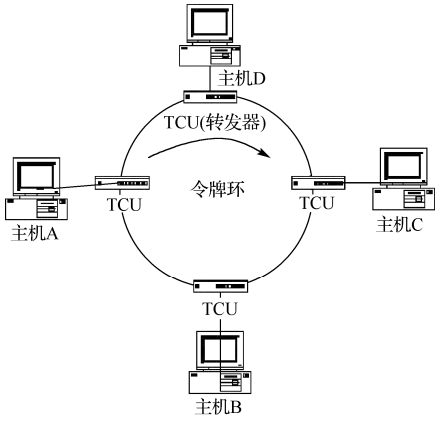

图 1-6　令牌环网

（3）FDDI 网

FDDI（Fiber Distributed Data Interface，光纤分布式数据接口），如图 1-7 所示，它是一项局域网数据传输标准，于 20 世纪 80 年代中期发展起来，它提供的高速数据通信能力要高于当时的以太网（10Mb/s）和令牌网（4Mb/s 或 16Mb/s）的能力。

FDDI 标准由 ANSI X3T9.5 标准委员会制订，为网络高容量输入输出提供了一种访问方法。FDDI 技术同 IBM 的 Token Ring 技术相似，并具有 LAN 和 Token Ring 所缺乏的管理、控制和可靠性措施，FDDI 支持长达 2km 的多模光纤。

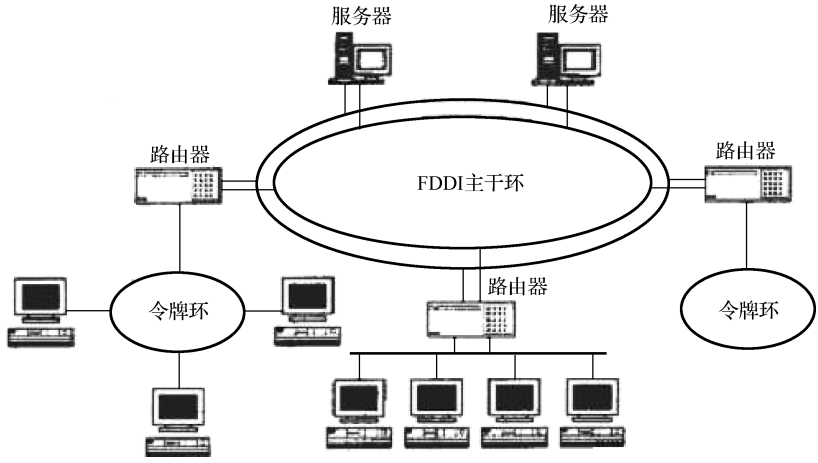

图 1-7　FDDI 网

（4）无线局域网

无线局域网络（Wireless Local Area Networks，WLAN）是相当便利的数据传输系统，如图 1-8 所示，它利用射频（Radio Frequency，RF）的技术，使用电磁波，取代旧式碍手碍脚的双绞铜线（Coaxial）所构成的局域网络，在空中进行通信连接，使得无线局域网络能利用简单的存取架构让用户通过它，达到“信息随身化、便利走天下”的理想境界。

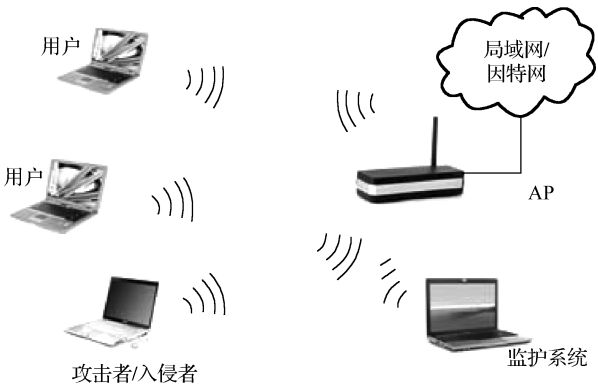

图 1-8　无线局域网

1.1.2　局域网安全

局域网基本上都采用以广播为技术基础的以太网，任何两个节点之间的通信数据包，不仅为这两个节点的网卡所接收，也同时为处在同一以太网上的任何一个节点的网卡所截取，如图 1-9 所示。因此，黑客只要接入以太网上的任一节点进行侦听，就可以捕获发生在这个以太网上的所有数据包，对其进行解包分析，从而窃取关键信息，这就是以太网所固有的安全隐患。事实上，Internet 如 SATAN、ISS、NETCAT 等，都把以太网侦听作为其最基本的手段。

当前，局域网安全的解决办法有以下几种。

1．网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听，网络分段可分为物理分段和逻辑分段两种方式。海关的局域网大多采用以交换机为中心、路由器为边界的网络格局，应重点挖掘中心交换机的访问控制功能和三层交换功能，综合应用物理分段与逻辑分段两种方法，来实现对局域网的安全控制。例如，在海关系统中普遍使用的 DEC MultiSwitch900 的入侵检测功能，其实就是一种基于 MAC 地址的访问控制，也就是上述的基于数据链路层的物理分段。

以交换式集线器代替共享式集线器对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包 Unicast Packet）还是会被同一台集线器上的其他用户所侦听。一种很危险的情况是：用户 TELNET 到一台主机上，由于 TELNET 程序本身

缺乏加密功能，用户所键入的每一个字符（包括用户名、密码等重要信息），都将被明文发送，这就给黑客提供了机会。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法侦听。当然，交换式集线器只能控制单播包（Unicast Packet）和多播包（Multicast Packet）。所幸的是，广播包和多播包内的关键信息，要远远少于单播包。

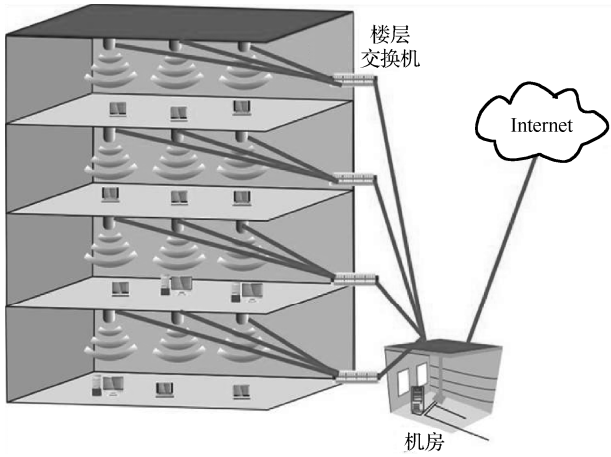

图 1-9　局域网

2．虚拟局域网

为了克服以太网的广播问题，除了上述方法外，还可以运用虚拟局域网（VLAN）技术，将以太网通信变为点到点通信，防止大部分基于网络侦听的入侵。

VLAN 技术主要有三种：基于交换机端口的 VLAN、基于节点 MAC 地址的 VLAN 和基于应用协议的 VLAN。基于端口的 VLAN 虽然稍欠灵活，但却比较成熟，在实际应用中效果显著，广受欢迎。基于 MAC 地址的 VLAN 为移动计算提供了可能性，但同时也潜藏着遭受 MAC 欺诈攻击的隐患。而基于协议的 VLAN，理论上非常理想，但实际应用却尚不成熟。

在集中式网络环境下，用户通常将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许有任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，用户可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内，互不侵扰。

VLAN 内部的连接采用交换实现，而 VLAN 与 VLAN 之间的连接则采用路由实现。大多数的交换机（包括海关内部普遍采用的 DEC MultiSwitch 900）都支持 RIP 和 OSPF 这两种国际标准的路由协议。如果有特殊需要，必须使用其他路由协议（如 Cisco 公司的 EIGRP 或支持 DECnet 的 IS-IS），也可以用外接的多以太网口路由器来代替交换机，实现 VLAN 之间的路由功能。当然，这种情况下，路由转发的效率会有所下降。

无论是交换式集线器还是 VLAN 交换机，都是以交换技术为核心的，它们在控制广播、防止黑客上相当有效，但同时也给一些基于广播原理的入侵监控技术和协议分析技术带来了麻烦。因此，如果局域网内存在这样的入侵监控设备或协议分析设备，就必须选用特殊

的带有 SPAN（Switch Port Analyzer）功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上，提供给接在这一端口上的入侵监控设备或协议分析设备。笔者在厦门海关外部网设计中，就选用了 Cisco 公司的具备 SPAN 功能的 Catalyst 系列交换机，既得到了交换技术的好处，又使原有的 Sniffer 协议分析仪“英雄有用武之地”。

1.1.3　无线局域网

当要把相离较远的节点连接起来时，架设专用通信线路的布线施工难度大、费用高、耗时长，对正在迅速扩大的连网需求形成了严重的瓶颈阻塞。无线局域网 WLAN（Wireless LAN）就是为解决有线网络的以上问题而出现的。在无线局域网 WLAN 发明之前，人们要想通过网络进行联络和通信，必须先用物理线缆-铜绞线组建一个电子运行的通路，为了提高效率和速度，后来又发明了光纤。当网络发展到一定规模后，人们又发现，这种有线网络无论组建、拆装还是在原有基础上进行重新布局和改建，都非常困难，且成本和代价也非常高，于是 WLAN 的组网方式应运而生。

WLAN 是相当便利的数据传输系统，它利用射频（Radio Frequency，RF）的技术，使用电磁波，取代旧式碍手碍脚的双绞铜线（Coaxial）所构成的局域网络，在空中进行通信连接，使得无线局域网络能利用简单的存取架构让用户透过它，达到“信息随身化、便利走天下”的理想境界。

WLAN 最大的优势就是免去或减少了繁杂的网络布线，一般只要安放一个或多个接入点设备就可建立覆盖整个建筑或地区的局域网络，无线用户可以通过传统的 802.11a/b/g 方式接入，也可以使用 802.11n 方式接入无线网络，获得网络资源服务。相比而言，使用 802.11n 方式能够覆盖更大的范围，使无线多媒体应用成为现实。

无线局域网和有线局域网相比优势不言而喻，它可实现移动办公、架设与维护更容易等。在如此巨大的应用与市场面前，无线局域网安全问题就显得尤为重要。人们不禁要问：通过电波进行数据传输的无线局域网的安全性有保障吗?

对于无线局域网的用户提出这样的疑问可以说不无根据，因为无线局域网采用公共的电磁波作为载体，而电磁波能够穿越天花板、玻璃、楼层、砖、墙等物体，因此在一个无线局域网接入点（Access Point，AP）的服务区域中，任何一个无线客户端都可以接收到此接入点的电磁波信号。这样，非授权的客户端也能接收到数据信号。也就是说，由于采用电磁波来传输信号，非授权用户在无线局域网（相对于有线局域网）中窃听或干扰信息就容易得多。所以为了阻止这些非授权用户访问无线局域网络，从无线局域网应用的第一天开始便引入了相应的安全措施。

实际上，无线局域网比大多数有线局域网的安全性更高。无线局域网技术早在第二次世界大战期间便出现了，它源自于军方应用。一直以来，安全性问题在无线局域网设备开发及解决方案设计时，都得到了充分的重视。无线局域网络产品主要采用的是 IEEE（美国电气和电子工程师协会）802.11b 国际标准，大多应用 DSSS（Direct Sequence Spread Spectrum，直接序列扩频）通信技术进行数据传输，该技术能有效防止数据在无线传输过程中丢失、干扰、信息阻塞及破坏等问题。802.11 标准主要应用三项安全技术来保障无线局域网数据传输的安全。第一项为 SSID（Service Set Identifier）技术，该技术可以将一个

无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。第二项为 MAC（Media Access Control）技术，应用这项技术，可在无线局域网的每一个接入点（Access Point）下设置一个许可接入的用户的 MAC 地址清单，MAC 地址不在清单中的用户，接入点将拒绝其接入请求。第三项为 WEP（Wired Equivalent Privacy）加密技术。因为无线局域网络是通过电波进行数据传输的，存在电波泄露导致数据被截听的风险。WEP 安全技术源自于名为 RC4 的 RSA 数据加密技术，以满足用户更高层次的网络安全需求。

下面从无线局域网安全技术的发展历程来对无线局域网中采用的主要安全技术及发展方向进行介绍。

1．早期技术

（1）无线网卡物理地址（MAC）过滤

每个无线工作站网卡都由唯一的物理地址标示，该物理地址编码方式类似于以太网物理地址，是 48 位。网络管理员可在无线局域网访问点 AP 中手工维护一组允许访问或不允许访问的 MAC 地址列表，以实现物理地址的访问过滤。

如果企业当中的 AP 数量太多，为了实现整个企业当中所有 AP 统一的无线网卡 MAC 地址认证，AP 也支持无线网卡 MAC 地址的集中 Radius 认证。

（2）服务区标识符（SSID）匹配

无线工作站必须出示正确的 SSID，与无线访问点 AP 的 SSID 相同，才能访问 AP；如果出示的 SSID 与 AP 的 SSID 不同，那么 AP 将拒绝它通过本服务区上网。因此可以认为 SSID 是一个简单的口令，从而提供口令认证机制，实现一定的安全性。

在无线局域网接入点 AP 上对此项技术的支持就是可不让 AP 广播其 SSID 号，这样无线工作站端就必须主动提供正确的 SSID 号才能与 AP 进行关联。

（3）有线等效保密（WEP）

有线等效保密（WEP）协议是由 802.11 标准定义的，用于在无线局域网中保护链路层数据。WEP 使用 40 位钥匙，采用 RSA 开发的 RC4 对称加密算法，在链路层加密数据。

WEP 加密采用静态的保密密钥，各 WLAN 终端使用相同的密钥访问无线网络。WEP 也提供认证功能，当加密机制功能启用，客户端要尝试连接上 AP 时，AP 会发出一个 Challenge Packet 给客户端，客户端再利用共享密钥将此值加密后送回存取点以进行认证比对，只有正确无误，才能获准存取网络的资源。40 位 WEP 具有很好的互操作性，所有通过 Wi-Fi 组织认证的产品都可以实现 WEP 互操作。WEP 一般也支持 128 位的钥匙，提供更高等级的安全加密。

2．解决方案

（1）802.11 技术

端口访问控制技术（IEEE 802.1x）和可扩展认证协议（EAP）：该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站与无线访问点 AP 关联后，是否可以使用 AP 的服务要取决于 802.1x 的认证结果。如果认证通过，则 AP 为无线工作站打开这个逻辑端口，否则不允许用户上网。

802.1x 要求无线工作站安装 802.1x 客户端软件，无线访问点要内嵌 802.1x 认证代理，

同时它还作为 Radius 客户端，将用户的认证信息转发给 Radius 服务器。安全功能比较全的 AP 在支持 IEEE802.1x 和 Radius 的集中认证时支持的可扩展认证协议类型有：EAP-MD5&TLS、TTLS 和 PEAP。

（2）无线客户端二层隔离技术

在电信运营商的公众热点场合，为确保不同无线工作站之间的数据流隔离，无线接入点 AP 也可支持其所关联的无线客户端工作站二层数据隔离，确保用户的安全。

无线局域网内的无线用户只要属于同一 VLAN 就可以互连互通，而有线内的用户可以通过交换机的二层隔离功能实现用户间的相互访问。

智能型无线交换网络的无线交换机由于有了一般交换机的 VLAN 的强大功能，所以，对于二层隔离也可以实现，从而隔离无线网络用户的相互访问。

端口隔离的基本原理是在交换机上创建一个端口隔离组，加入同一端口隔离组内的接口之间不能通信。不同隔离组的接口，或者隔离组内接口和未加入隔离组的接口之间可以通信。端口隔离技术提供一种同一 VLAN 内主机禁止互访的基本机制，交换机所做的就是基于 MAC 转发表（二层转发）或路由表（三层转发）判断出接口之后，如果出接口和入接口在同一端口隔离组就丢弃该报文。

（3）VPN-Over-Wireless 技术

已广泛应用于广域网络及远程接入等领域的 VPN（Virtual Private Networking）安全技术也可用于无线局域网。与 IEEE802.11b 标准所采用的安全技术不同，VPN 主要采用 DES、3DES 等技术来保障数据传输的安全。对于安全性要求更高的用户，将现有的 VPN 安全技术与 IEEE802.11b 安全技术结合起来，是较为理想的无线局域网络的安全解决方案之一。

（4）2003 年的技术

在 IEEE802.11i 标准最终确定前，WPA（Wi-Fi Protected Access）技术将成为代替 WEP 的无线安全标准协议，为 IEEE802.11 无线局域网提供更强大的安全性能。WPA 是 IEEE802.11i 的一个子集，其核心就是 IEEE802.1x 和 TKIP。

新一代的加密技术 TKIP 与 WEP 一样基于 RC4 加密算法，且对现有的 WEP 进行了改进。在现有的 WEP 加密引擎中增加了“密钥细分（每发一个包重新生成一个新的密钥）”“消息完整性检查（MIC）”“具有序列功能的初始向量”和“密钥生成和定期更新功能”4 种算法，极大地提高了加密安全强度。TKIP 与当前 Wi-Fi 产品向后兼容，而且可以通过软件进行升级。从 2003 年的下半年开始，Wi-Fi 组织已经开始对支持 WPA 的无线局域网设备进行认证。

3．安全标准

为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容，IEEE802.11 工作组正在开发作为新的安全标准的 IEEE802.11i，并且致力于从长远角度考虑解决 IEEE802.11 无线局域网的安全问题。IEEE802.11i 标准草案中主要包含加密技术：TKIP（Temporal Key Integrity Protocol）和 AES（Advanced Encryption Standard），以及认证协议 IEEE802.1x。

无线局域网总的发展方向是速度会越来越快（已见的是 11Mb/s 的 IEEE802.11b，54Mb/s 的 IEEE802.11g 和 IEEE802.11a 标准），安全性会越来越高。当然无线局域网的各项技术均

处在快速的发展过程当中，但 54Mb/s 的无线局域网规范 IEEE802.11g 及 IEEE802.1x 将是整个无线局域网业的热点。

（1）对无线局域网的安全防护应考虑以下防范点和措施。

安全防范点：①未经授权用户的接入；②网上邻居的攻击；③非法用户截取无线链路中的数据；④非法 AP 的接入；⑤内部未经授权的跨部门使用。

相应措施：使用各种先进的身份认证措施，防止未经授权用户的接入。由于无线信号是在空气中传播的，信号可能会传播到不希望到达的地方，在信号覆盖范围内，非法用户无须任何物理连接就可以获取无线网络的数据，因此，必须从多方面防止非法终端接入以及数据的泄露问题。

（2）利用 MAC 阻止未经授权的接入。每块无线网卡都拥有唯一的一个 MAC 地址，为 AP 设置基于 MAC 地址的 Access Control（访问控制表），确保只有经过注册的设备才能进入网络。使用 802.1x 端口认证技术进行身份认证。使用 802.1x 端口认证技术配合后台的 Radius 认证服务器，对所有接入用户的身份进行严格认证，杜绝未经授权的用户接入网络，盗用数据或进行破坏。

（3）使用先进的加密技术，使得非法用户即使截取无线链路中的数据也无法破译基本的 WEP。加密 WEP 是 IEEE 802.11b 无线局域网的标准网络安全协议。在传输信息时，WEP 可以通过加密无线传输数据来提供类似有线传输的保护。在简便的安装和启动之后，应立即设置 WEP 密钥。

（4）利用对 AP 的合法性验证以及定期进行站点审查，防止非法 AP 的接入。在无线 AP 接入有线集线器的时候，可能会遇到非法 AP 的攻击，非法安装的 AP 会危害无线网络的宝贵资源，因此必须对 AP 的合法性进行验证。AP 支持的 IEEE 802.1x 技术提供了一个客户机和网络相互验证的方法，在此验证过程中不但 AP 需要确认无线用户的合法性，无线终端设备也必须验证 AP 是否为虚假的访问点，然后才能进行通信。通过双向认证，可以有效地防止非法 AP 的接入。对于那些不支持 IEEE 802.1x 的 AP，则需要通过定期的站点审查来防止非法 AP 的接入。在入侵者使用网络之前，通过接收天线找到未被授权的网络。通过物理站点的监测应当尽可能地频繁进行，频繁的监测可增加发现非法配置站点的存在概率。选择小型的手持式检测设备，管理员可以通过手持扫描设备随时到网络的任何位置进行检测。

（5）利用 ESSID、MAC 限制防止未经授权的跨部门使用。

利用 ESSID 进行部门分组，可以有效地避免任意漫游带来的安全问题；MAC 地址限制更能控制连接到各部门 AP 的终端，避免未经授权的用户使用网络资源。

保障整个网络安全是非常重要的，无论是否有无线网段，大多数的局域网都必须要有一定级别的安全措施。而无线网络相对来说比较安全，无线网段即使不能提供比有线网段更多的保护，也至少和它相同。需要注意的是，无线局域网并不是要替代有线局域网，而是有线局域网的替补。使用无线局域网的最终目标不是消除有线设备，而是尽量减少线缆和断线时间，让有线与无线网络很好地配合工作。

下面我们对 WLAN 技术进行介绍。

（1）WLAN 安全技术

无线网络的安全性主要体现在认证和数据加密两个方面。认证用来保证只能由授权用户进行访问，数据加密则保证发送的数据只能被特定的用户所接收。

认证主要有 802.1x 接入认证、PSK 认证、MAC 地址认证等。数据加密主要有 WEP、TKIP 和 CCMP。如果和安全服务器配合使用，无线设备还支持动态控制用户权限、Portal 等安全管理方式。

（2）WLAN 漫游技术

WLAN 漫游技术支持 AC 内漫游、AC 间漫游，并且提供必要的安全性，确保漫游过程中的可靠性和私密性。漫游域不受子网的限制，可以让客户在规划无线网络时，不用考虑以前的有线网络的规划，完全只考虑无线信号的覆盖即可，这种方式大大简化了前期的网络规划，减少了网络规划成本。

此外，设备也支持快速漫游，满足对切换时间要求苛刻的语音业务需求。

（3）WLAN 资源管理

WLAN 资源管理解决了如何为接入点自动配置最佳工作频率和传输功率的关键问题，并且提供了一套实时智能射频管理方案，使无线网络能够自动适应无线射频环境的变化，保持最优的射频资源状态。它采用了分布式方法学习周围环境，进行集中式评估，有效地控制和分配无线资源，降低用户的操作成本。此外，系统还实现了无线接入用户的负载均衡，有效保证该高密度无线网络环境中无线用户的合理接入。

（4）WLAN IDS 技术

WLAN IDS 技术就是为了解决 WLAN 网络的入侵检测实现对 WLAN 服务网络的保护。目前主要包括下面三个特性。

① 非法设备检测：非法设备检测比较适合于大型的 WLAN 网络。通过在已有的 WLAN 网络中部署非法设备检测功能，可以对整个 WLAN 网络中的异常设备进行监视，并且可以根据需要对非法的设备进行防攻击处理。

② 入侵检测：入侵检测主要为了及时发现 WLAN 网络的恶意或者无意的攻击，通过记录信息或者日志方式通知网络管理者。根据入侵检测的结果，可以及时调整网络的配置，清除 WLAN 网络的不安全因素。

③ 无线用户接入控制（黑名单和白名单）：无线用户接入控制根据特定的属性实现对无线客户端接入 WLAN 网络的权限控制。

（5）WLAN QoS 技术

多媒体、语音等业务在无线局域网中的应用，使得原本紧张的无线资源更加捉襟见肘。由于无线网络具有数据传输率低而误码率高的特点，传统有线网络的 QoS 技术无法直接应用在无线局域网中。IEEE 802.11E 标准的引入，再结合有线网络的 QoS，就可以保证端到端的 QoS。端到端的 QoS 解决方案不仅解决了无线接入点和无线用户直接在无线介质上的 QoS，而且可以将无线用户的优先级映射到 AP-AC 间的 CAPWAP 隧道上，保证了 AP-AC 间无线用户的 QoS。

（6）WLAN Mesh 技术

传统 WLAN 网络的骨干网络均采用 Ethernet 技术，各 AP 之间通过有线方式进行互连。Mesh 网络是利用无线连接替代有线连接将多个 AP 连接起来，并最终通过一个 Portal 节点接入有线网络。在 Mesh 网络里，如果要添加或移动设备时，Mesh 网络能够自动发现拓扑变化，并调整通信路由，以获取最有效的传输路径。与传统非 Mesh 网络相比，Mesh 网络具有高性价比、部署快捷、可扩展性强等优点。

1.1.4 虚拟局域网

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN 工作在 OSI 参考模型的第 2 层和第 3 层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点：网络设备的移动、添加和修改的管理开销减少；可以控制广播活动；可提高网络的安全性。

在计算机网络中，一个二层网络可以被划分为多个不同的广播域，一个广播域对应了一个特定的用户组，默认情况下这些不同的广播域是相互隔离的。不同的广播域之间想要通信，需要通过一个或多个路由器。这样的一个广播域就称为 VLAN。

虚拟局域网（Virtual Local Area Network，VLAN）是指在局域网交换机（ATM、LAN、以太网等）里采用网络管理软件所构建的可跨越不同网段、不同网络、不同位置的端到端的逻辑网络。VLAN 是一个在物理网络上根据用途、工作组、应用等来逻辑划分的局域网络，是一个广播域，与用户的物理位置没有关系。VLAN 中的网络用户是通过 LAN 交换机来通信的，一个 VLAN 中的成员看不到另一个 VLAN 中的成员。同一个 VLAN 中的所有成员共同拥有一个 VLAN ID，组成一个虚拟局域网络；同一个 VLAN 中的成员均能收到同一个 VLAN 中的其他成员发来的广播包，但收不到其他 VLAN 中成员发来的广播包；不同 VLAN 成员之间不可直接通信，需要通过路由支持才能通信，而同一 VLAN 中的成员通过 VLAN 交换机可以直接通信，不需路由支持。VLAN 的特性是：控制通信活动，隔离广播数据顺化网络管理，便于工作组优化组合；VLAN 中的成员只要拥有一个 VLAN ID 就可以不受物理位置的限制，随意移动工作站的位置；增加网络的安全性，VLAN 交换机就是一道道屏风，只有具备 VLAN 成员资格的分组数据才能通过，这比用计算机服务器做防火墙要安全得多；网络带宽得到充分利用，网络性能大大提高。

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通信介质的数据网络通信技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机实现 LAN 互连虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了虚拟局域网 VLAN（Virtual Local Area Network）技术，这种技术可以把一个 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文被限制在一个 VLAN 内，如图 1-10 所示。

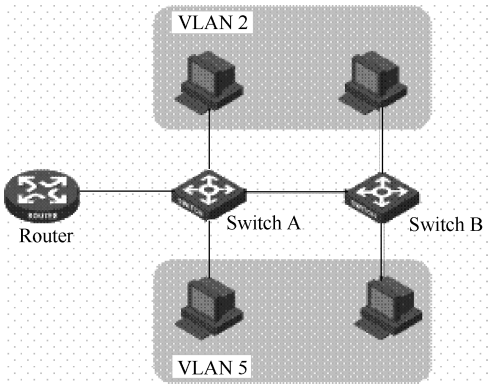

图 1-10 VLAN

VLAN 的划分不受物理位置的限制：不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由器。

VLAN 的优点如下。

① 限制广播域。广播域被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。

② 增强局域网的安全性。VLAN 间的二层报文是相互隔离的，即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信，如果不同 VLAN 要进行通信，则需通过路由器或三层交换机等三层设备。

③ 灵活构建虚拟工作组。用 VLAN 可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。

VLAN 两个相关的端口：Access 端口、Trunk 端口。

- Access 口：字面意思理解就是访问端口，一般用于连接计算机网卡，能且只能属于一个 VLAN（必须属于一个 VLAN）。
- Trunk 口：中继链路的端口，用来透明传输多个 VLAN（就是 Access 口的 VLAN），一般是用来连接 SW 到 SW 或者 SW 到 Router。Trunk 口上可以配置允许哪些 VLAN 通过，哪些不能通过。
- Access 口收到帧时：检查该帧是否有 VLAN 信息，没有就加上自己的 VLAN ID 然后再发送，有的话丢弃该帧。
- Access 口发送帧时：检查该帧 VLAN ID，与自己的 VLAN ID 一致的，剥离 VLAN ID 后发送，不一致的丢弃。
- Trunk 口收到帧时：检查该帧是否有 VLAN 信息，没有就加上 Native VLAN ID 然后发送，有的话检查该 VLAN ID 是否为本 Trunk 口所允许通过的 VLAN ID，是的话原封不动地转发，否则丢弃。
- Trunk 口发送帧时：检查该帧 VLAN ID，与本端口 VLAN ID 一致时，剥离 VLAN 标签转发；与本端口不一致时，在相应的 VLAN 中来进行转发。

VLAN 成员的连接方式分为三种：Access、Trunk 和 Hybrid。

- Access 连接：报文不带 tag 标签，一般用于和 tag-unaware（不支持 802.1Q 封装）设备相连，或者不需要区分不同 VLAN 成员时使用。
- Trunk 连接：在 PVID 所属的 VLAN 不带 tag 标签转发，其他 VLAN 中的报文都必须带 tag 标签，用于 tag-aware（支持 802.1Q 封装）设备相连，一般用于交换机之间的互连。
- Hybrid 连接：可根据需要设置某些 VLAN 报文带 tag，某些报文不带 tag。与 Trunk 连接最大的不同在于，Trunk 连接只有 PVID 所属的 VLAN 不带 tag，其他 VLAN 都必须带 tag，而 Hybrid 连接是可以设置多个 VLAN 不带 tag。
- 实际应用中，根据设置设备端口的 Access、Trunk、Hybrid 属性来实现各种不同的连接方式。端口属性的应用也远远超出了简单的 VLAN 成员互连，用端口属性来实现了一些相对复杂的功能，比如 isolated-user VLAN，组播 VLAN。

为了理解 VLAN 内报文的转发，就必须要知道交换机对于不同 VLAN 报文的 tag/untag 的处理原则。

首先，需要明确的一点就是，在交换机的内部，为了快速高效地处理，报文都是带 tag 转发的。其实，这点很好理解，因为交换机上很可能会配置多个 VLAN，那不同 VLAN 流量区分只有依靠 tag 标签。

下面从报文入和报文出两个方向来介绍。

（1）报文入方向

在入方向上，交换机的根本任务就是决定该报文是否允许进入该端口，根据入报文的tag/untag 的属性以及端口属性，细分为如下情况。

① 报文为 untag：允许报文进入该端口，并打上 PVID 的 VLAN tag，与端口属性无关。

② 报文为 tag：在这种情况下，需要交换机来判断是否允许该报文进入端口：

Access 端口：PVID 和报文中 tag 标明的 VLAN 一致，接收并处理报文；否则丢弃。

Trunk/Hybrid 端口：如果端口允许 tag 中标明的 VLAN 通过，则接收并处理报文；否则丢弃。

（2）报文出方向

在出方向上，交换机已经完成对报文的转发，其根本任务就是在转发出端口时，是否携带 tag 转发出去，根据出端口属性，细分为如下情况。

① Access 端口：将标签剥掉，不带 tag 转发。

② Trunk 端口：报文所在 VLAN 和 PVID 相同，则报文不带 tag；否则带 tag。

③ Hybrid 端口：报文所在 VLAN 配置为 tag，则报文带 tag；否则不带 tag；

图 1-11 和图 1-12 所示分别为 Trunk 发送和接收示意图。

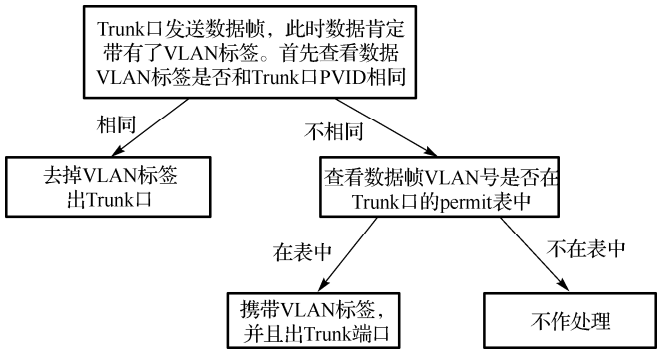

图 1-11 Trunk 发送

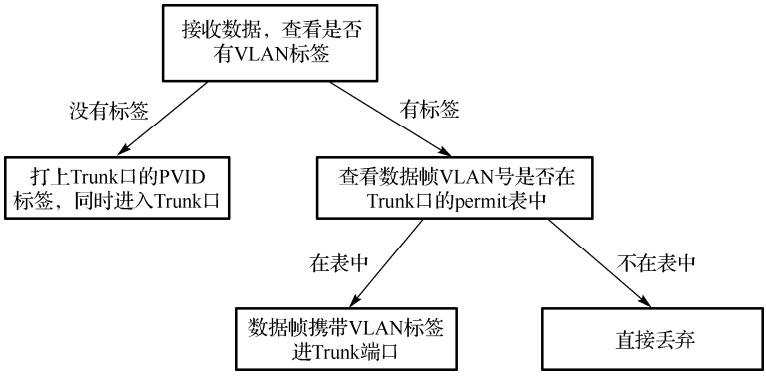

图 1-12 Trunk 接收

图 1-13 和图 1-14 所示分别为 Hgbird 发送和接收示意图。

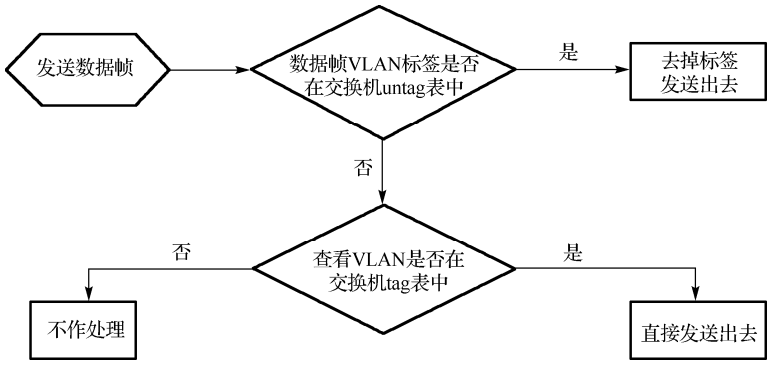

图 1-13　Hybrid 发送

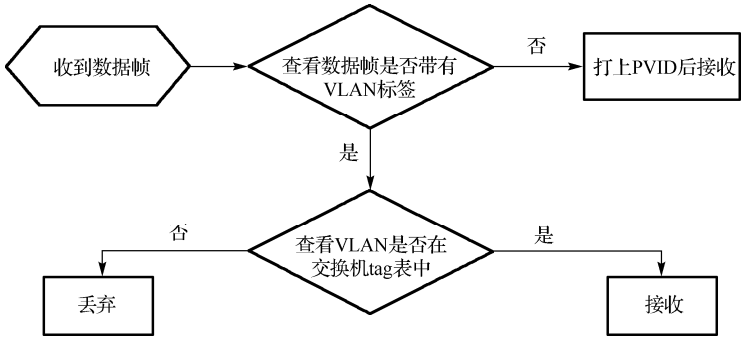

图 1-14　Hybrid 接收

1.1.5　动态主机分配协议 DHCP

DHCP（Dynamic Host Configuration Protocol）是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。它能够动态地向网络中每台设备分配独一无二的 IP 地址，并提供安全、可靠的 TCP/IP 网络配置，确保不发生地址冲突，帮助维护 IP 地址的使用。这些被分配的 IP 地址都是 DHCP 服务器预先保留的一个由多个地址组成的地址集，并且它们一般是一段连续的地址。

DHCP 是 BOOTP 协议的一个扩展，它主要实现允许无盘工作站连接到网络系统并且自动获取一个 IP 地址。DHCP 由两个基本部分组成，分别是把配置的专用信息传达给网络主机和把 IP 地址分配给主机，从而向网络主机提供配置参数。将默认网关、一个 IP 地址、一个 DNS 服务器 IP 地址、子网掩码以及一个 WINS 服务器 IP 地址等提供给每一位网络客户是 DHCP 的主要工作。DHCP 是在对客户/服务器的模式上而存在的，这种模式是将网络地址分配给专门特别指出的主机，再把网络配置的参数给有此需求的网络主机传送过去。将被特指的主机称作成服务器是因为易于被理解，也就是能够给主机进行 DHCP 服务的提供者。对信息进行接收的主机被称作客户。我们将 DHCP 的 IP 地址的分配方式大致分为三种：自动分配、动态分配、手工分配。它们之间的区别在于自动分配给用户机分配的 IP 地址是永久性的；动态分配获取的 IP 地址使用时间受限制；手工分配的意思就是由管理员手工指定一个 IP 地址给用户，而 IP 地址的传送是由 DHCP 服务器来实现的。不同的网络配置也不相同，因此要根据实际情况来选择采用什么样的方法来进行分配。关于准许自动

重用地址方法只有一种，就是动态分配。所以，此种方法对于需要进行临时上网而且 IP 地址的资源也较缺乏者最适用。手工指定方法也有一大优点，那就是管理不希望使用动态 IP 地址的用户十分方便。总之 DHCP 是一种相对集中式的管理方式。

DHCP 协议的消息交互过程为：①客户端广播 DHCPDISCOVER 消息。②网络中的 DHCP 服务器（可能不止一台）收到此消息后，从自己的地址池里取出一个地址，包含在 DHCPOFFER 消息中，发回客户端。③客户端可能会收到多个 DHCPOFFER 消息，从中选择一个服务器，将里面的 IP 地址和服务器标志包含在 DHCPREQUEST 消息中，再次广播发送到所有服务器。值得注意的是，此时客户端收到了 IP 地址，但此 IP 地址在收到服务器的 DHCPACK 消息之前不可用。④服务器收到 DHCPREQUEST 消息后，判断客户端是否选择了自己。如果是，则判断此地址是否可用。如果可用，则将此地址与客户端绑定，并发回 DHCPACK 消息。若此地址已分配给其他客户端，则发回 DHCPACK 消息。⑤一段时间后，客户端下线，向服务器单播发送 DHCPRELEASE 消息。服务器收到此消息后，标记该 IP 地址为可用地址。

DHCP 工作流程如图 1-15 所示。

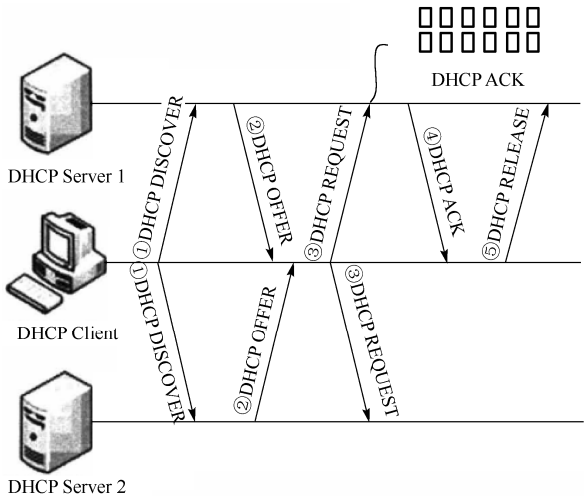

图 1-15　DHCP 工作流程

在使用 TCP/IP 协议的网络上，每一台计算机都拥有唯一的计算机名和 IP 地址。IP 地址（及其子网掩码）使用与鉴别它所连接的主机和子网，当用户将计算机从一个子网移动到另一个子网的时候，一定要改变该计算机的 IP 地址。如采用静态 IP 地址的分配方法将增加网络管理员的负担，而 DHCP 可以让用户将 DHCP 服务器中的 IP 地址数据库中的 IP 地址动态地分配给局域网中的客户机，从而减轻了网络管理员的负担。

动态分配 IP 地址的好处：可以解决 IP 地址不够用的问题；用户不必自己设置 IP 地址、网关地址、DNS 服务器地址等网络属性，不存在盗用 IP 地址的问题。

DHCP 使服务器能够动态地为网络中的其他服务器提供 IP 地址，通过使用 DHCP，就可以不给局域网中除 DHCP、DNS 和 WINS 服务器外的任何服务器设置和维护静态 IP 地址。使用 DHCP 可以大大简化配置客户机的 TCP / IP 的工作，尤其是当某些 TCP / IP 参数改变时，如网络的大规模重建而引起的 IP 地址和子网掩码的更改。

1.1.6　无线 802.11 协议

无线 802.11 协议发展经历了 802.11、802.11b、802.11a、802.11g 和 802.11n 的过程。目前最新的无线协议是 802.11n 协议，但主流且使用最多的还是 802.11a/g 协议。

无线网络协议只定义了 OSI 架构中物理层和数据链路层（MAC 子层）两层的内容，其他层的内容和有线网络是一样的。

802.11i 是无线安全协议，是总的原则，相当于“宪法”，其内容包括 WPA 和 WPA2 两个部分内容，WPA 相当于“治安处罚管理条例”，而 WPA2 相当于“刑法”，所以 WPA2 是更高级的一种安全方式。PSK 和 802.1x 是两种无线安全认证方式，PSK 是一种个人级别的，相对简单，而 802.1x 是一种企业级别的，较为复杂，但更安全。TKIP 和 CCMP 是两种数据加密算法，在 WPA 和 WPA2 中都可以使用。而 AES 是 CCMP 算法中的核心算法，且目前来看，是最可靠的加密算法。

1.1.7　双绞线

双绞线是综合布线工程中最常用的一种传输介质，有正线和反线两种。

正线，即直通线，（标准 568B），两端线序一样，从左至右线序是：橙白，橙，绿白，蓝，蓝白，绿，棕白，棕。

反线，即交叉线（标准 568A），一端为正线的线序，另一端为从左至右：绿白，绿，橙白，蓝，蓝白，橙，棕白，棕。

双绞线是由一对相互绝缘的金属导线绞合而成的。采用这种方式，不仅可以抵御一部分来自外界的电磁波干扰，也可以降低多对绞线之间的相互干扰。把两根绝缘的导线互相绞在一起，干扰信号作用在这两根相互绞缠在一起的导线上是一致的（这个干扰信号称为共模信号），在接收信号的差分电路中可以将共模信号消除，从而提取出有用信号（差模信号）。

任何材质的绝缘导线绞合在一起都可以叫做双绞线，同一电缆内可以是一对或一对以上双绞线，一般由两根 22～26 号单根铜导线相互缠绕而成，也有使用多根细小铜丝制成单根绝缘线的（这与集肤效应有关），实际使用时，双绞线是由多对双绞线一起包在一个绝缘电缆套管里的。典型的双绞线有一对的，有四对的，也有更多对双绞线放在一个电缆套管里的，这些我们称之为双绞线电缆。双绞线一个扭绞周期的长度，称为节距，节距越小，抗干扰能力越强。

双绞线的作用是使外部干扰在两根导线上产生的噪声（在专业领域里，把无用的信号称为噪声）相同，以便后续的差分电路提取出有用信号，差分电路是一个减法电路，两个输入端同相的信号（共模信号）相互抵消（m–n），反相的信号相当于 x–（–y），得到增强。理论上，在双绞线及差分电路中 m=n，x=y，那么相当于干扰信号被完全消除，有用信号加倍，但在实际运行中是有一定差异的。

双绞线分为屏蔽双绞线（Shielded Twisted Pair，STP）与非屏蔽双绞线（Unshielded Twisted Pair，UTP）。屏蔽双绞线在双绞线与外层绝缘封套之间有一个金属屏蔽层。屏蔽双绞线分为 STP 和 FTP（Foil Twisted-Pair），STP 指每条线都有各自的屏蔽层，而 FTP 只在整个电缆有屏蔽装置，并且两端都正确接地时才起作用。所以要求整个系统是屏蔽器件，包括电缆、信息点、水晶头和配线架等，同时建筑物需要有良好的接地系统。屏蔽层可减

少辐射，防止信息被窃听，也可阻止外部电磁干扰的进入，使屏蔽双绞线比同类的非屏蔽双绞线具有更高的传输速率。非屏蔽双绞线是一种数据传输线，由四对不同颜色的传输线组成，广泛用于以太网路和电话线中。非屏蔽双绞线电缆最早在 1881 年被用于贝尔发明的电话系统中。1900 年美国的电话线网络也主要由 UTP 所组成，由电话公司所拥有。

双绞线常见的有 3 类线、5 类线和超 5 类线，以及最新的 6 类线，前者线径细而后者线径粗。

（1）1 类线（CAT1）：线缆最高频率带宽是 750kHz，用于报警系统，或只适用于语音传输（1 类标准主要用于 20 世纪 80 年代初之前的电话线缆），不用于数据传输。

（2）2 类线（CAT2）：线缆最高频率带宽是 1MHz，用于语音传输和最高传输速率 4Mb/s 的数据传输，常见于使用 4Mb/s 规范令牌传递协议的旧的令牌网。

（3）3 类线（CAT3）：指目前在 ANSI 和 EIA/TIA568 标准中指定的电缆，该电缆的传输频率为 16MHz，最高传输速率为 10Mb/s（10Mb/s），主要应用于语音、10Mb/s 以太网（10BASE-T）和 4Mb/s 令牌环，最大网段长度为 100m，采用 RJ 形式的连接器，目前已淡出市场。

（4）4 类线（CAT4）：该类电缆的传输频率为 20MHz，用于语音传输和最高传输速率 16Mb/s（指的是 16Mb/s 令牌环）的数据传输，主要用于基于令牌的局域网和 10BASE-T/100BASE-T。最大网段长为 100m，采用 RJ 形式的连接器，未被广泛采用。

（5）5 类线（CAT5）：该类电缆增加了绕线密度，外套一种高质量的绝缘材料，线缆最高频率带宽为 100MHz，最高传输率为 100Mb/s，用于语音传输和最高传输速率为 100Mb/s 的数据传输，主要用于 100BASE-T 和 1000BASE-T 网络，最大网段长为 100m，采用 RJ 形式的连接器，这是最常用的以太网电缆。在双绞线电缆内，不同线对具有不同的绞距长度。通常，4 对双绞线绞距周期在 38.1mm 长度内，按逆时针方向扭绞，一对线对的扭绞长度在 12.7mm 以内。

（6）超 5 类线（CAT5e）：超 5 类具有衰减小，串扰少的特点，并且具有更高的衰减与串扰的比值（ACR）和信噪比（SNR）、更小的时延误差，性能得到很大提高。超 5 类线主要用于千兆位以太网（1000Mb/s）。

（7）6 类线（CAT6）：该类电缆的传输频率为 1MHz～250MHz，6 类布线系统在 200MHz 时综合衰减串扰比（PS-ACR）应该有较大的余量，它提供 2 倍于超 5 类的带宽。6 类布线的传输性能远远高于超 5 类标准，最适用于传输速率高于 1Gb/s 的应用。6 类与超 5 类的一个重要的不同点在于：改善了在串扰以及回波损耗方面的性能，对于新一代全双工的高速网络应用而言，优良的回波损耗性能是极重要的。6 类标准中取消了基本链路模型，布线标准采用星状的拓扑结构，要求的布线距离为：永久链路的长度不能超过 90m，信道长度不能超过 100m。

（8）超 6 类或 6A（CAT6A）：此类产品传输带宽介于 6 类和 7 类之间，传输频率为 500MHz，传输速度为 10Gb/s，标准外径 6mm。目前和 7 类产品一样，国家还没有出台正式的检测标准，只是行业中有此类产品，各厂家宣布一个测试值。

（9）7 类线（CAT7）：传输频率为 600MHz，传输速度为 10Gb/s，单线标准外径为 8mm，多芯线标准外径为 6mm，可能用于今后的 10Gb/s 以太网。

通常，计算机网络所使用的是 3 类线和 5 类线，其中 10 BASE-T 使用的是 3 类线，100BASE-T 使用的是 5 类线。