第 5 章 接入控制和访问控制

接入控制只允许授权接入网络的用户所使用的终端接入网络，访问控制只允许每一个用户访问授权该用户访问的网络资源，接入控制的核心是身份鉴别，访问控制的核心是身份鉴别和授权。

5.1 身 份 鉴 别

身份鉴别过程是一方向另一方证明自己身份的过程，为了向另一方证明自己的身份，首先需要拥有能够证明自己身份的身份标识信息，同时需要向另一方证明自己确实拥有可以证明自己身份的身份标识信息。

5.1.1 身份鉴别定义和分类

1. 定义

身份鉴别是验证主体的真实身份与其所声称的身份是否符合的过程，主体可以是用户、进程和主机等。现实世界中，人类可以有多种证明自己身份的方式，如出示身份证等有效证件、提供指纹和视网膜等个人特征等。在计算机网络中，可能需要完成两个进程之间，或者两个主机之间的身份鉴别过程，这两个主机或进程可能相距甚远，在这种情况下，两个主体之间无法相互提供证明其身份的物理原件。因此，网络环境下，主体必须有能够证明其身份，且可以通过网络传输的主体身份标识信息。

2. 分类

身份鉴别方式可以分为单向鉴别、双向鉴别和第三方鉴别三种。

1) 单向鉴别

单向鉴别如图 5.1(a)所示，存在主体 A 和主体 B 两个主体，主体 A 需要向主体 B 证明自己的身份，但主体 B 无须向主体 A 证明自己的身份。这种情况下，主体 A 称为示证者，主体 B 称为验证者或鉴别者。

2) 双向鉴别

双向鉴别如图 5.1(b)所示，主体 A 和主体 B 都需要向对方证明自己的身份。

3) 第三方鉴别

第三方鉴别如图 5.1(c)所示，存在可信的第三方，由可信的第三方证明主体的身份标识信息与主体之间的绑定关系，主体 A 和主体 B 利用第三方提供的证明完成向对方证明自己身份的过程。

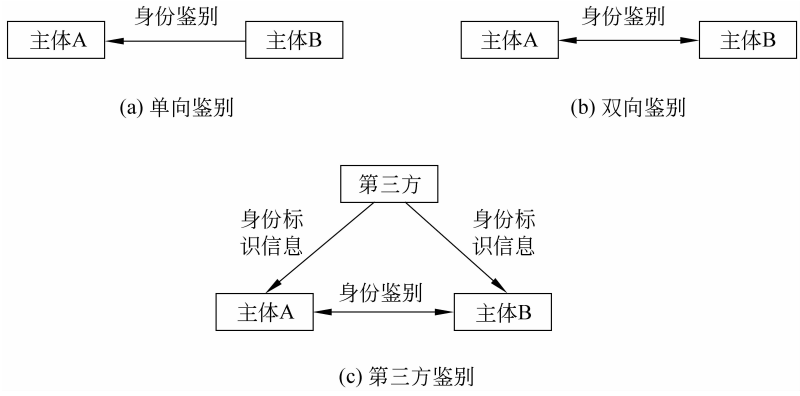

图 5.1 身份鉴别方式

5.1.2 主体身份标识信息

网络环境下，主要用密钥、用户名和口令、证书和私钥作为主体身份标识信息。

1. 密钥

主体拥有某个密钥 x，只要主体能够证明自己知道密钥 x，主体的身份就得到证明。

2. 用户名和口令

这种标识信息主要用于标识用户，为每一个授权用户分配用户名和口令，某个用户只要能够证明自己知道某个授权用户对应的用户名和口令，就能证明该用户是授权用户。

3. 证书和私钥

证书可以证明主体 x 与公钥 PK 之间的绑定关系，如果主体 x 能够证明自己知道与公钥 PK 对应的私钥 SK，就能证明自己是主体 x。

5.1.3 单向鉴别过程

1. 基于共享密钥

基于共享密钥的单向鉴别过程如图 5.2 所示，主体 B 为了能够鉴别主体 A 的身份，一是使得主体 A 和主体 B 有着相同的对称密钥 K，且该对称密钥 K 只有主体 B 和主体 A 知道。二是使得双方使用相同的对称密钥加密解密算法。

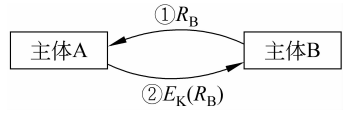

图 5.2 基于共享密钥单向鉴别过程

这种情况下，主体 A 通过向主体 B 证明自己知道对称密钥 K 来证明自己是主体 A。主体 B 产生一个随机数 R_B，并将随机数 R_B 发送给主体 A，主体 A 用对称密钥 K 和加密算法 E 对随机数 R_B 进行加密，生成密文 $E_K(R_B)$，并将密文发送给主体 B。主体 B 用对称密钥 K 和解密算法 D 对密文解密，获得明文，如果明文等于 R_B，即 $D_K(E_K(R_B))=R_B$，表示主体 A 知道对称密钥 K，主体 A 的身份得到证明。

每一次鉴别主体 A 身份时，主体 B 先向主体 A 发送随机数 R_B，这样做的目的是为了防止重放攻击。由于主体 B 每一次鉴别主体 A 身份时，产生不同的随机数，导致主体 A

每一次回送的密文是不同的，使得第三方无法通过截获上一次主体 A 发送给主体 B 的密文来冒充主体 A。

主体 A 向主体 B 发送密文的目的是为了防止截获攻击，即使第三方截获到主体 B 发送的随机数 R_B 和密文 $E_K(R_B)$，也无法通过随机数 R_B 和密文 $E_K(R_B)$ 解析出对称密钥 K，因而无法冒充主体 A。

2. 基于用户名和口令

基于用户名和口令的单向鉴别过程如图 5.3 所示，主体 B 为了能够鉴别主体 A 的身份，需要事先建立注册用户库，注册用户库中存储所有注册用户的用户名和口令，主体 A 证明自己身份的过程就是证明自己是用户名标识的注册用户的过程。主体 A 为了证明自己是用户名标识的注册用户，需要向主体 B 提供用户名和口令，主体 A 提供的用户名和口令必须是注册用户库中某个注册用户对应的用户名和口令。

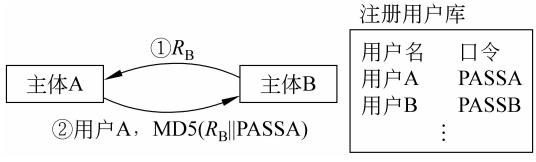

图 5.3　基于用户名和口令的单向鉴别过程

主体 B 产生一个随机数 R_B，并将随机数 R_B 发送给主体 A，主体 A 将随机数 R_B 和自己的口令 PASSA 串接在一起，并对串接结果进行报文摘要运算，然后将用户名用户 A 和报文摘要 MD5(R_B ‖ PASSA)一起发送给主体 B，这里的 MD5 是一种计算报文摘要的算法。主体 B 根据用户名用户 A 检索注册用户库，找到用户名为用户 A 的注册用户，获取其口令 PASSA，将随机数 R_B 和口令 PASSA 串接在一起，并对串接结果进行报文摘要运算。然后将运算结果与主体 A 发送的报文摘要进行比较，如果相等，表明主体 A 是用户名为用户 A 的注册用户，主体 A 的身份得到证明。

由于报文摘要算法的单向性，即使第三方截获到报文摘要 MD5(R_B ‖ PASSA)，也无法推导出口令 PASSA。主体 B 先向主体 A 发送随机数 R_B 的目的是为了防止重放攻击。

3. 基于证书和私钥

基于证书和私钥的单向鉴别过程如图 5.4 所示，主体 B 拥有用于证明公钥 PKA 与主体 A 之间绑定关系的证书，且证书的有效性已经得到验证。主体 A 证明自己身份的过程就是证明自己知道公钥 PKA 对应的私钥 SKA 的过程。

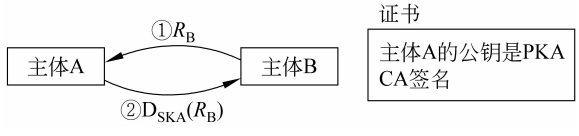

图 5.4　基于证书和私钥的单向鉴别过程

主体 B 产生一个随机数 R_B，并将随机数 R_B 发送给主体 A。主体 A 用私钥 SKA 和解密算法 D 对随机数进行解密运算，得到运算结果 $D_{SKA}(R_B)$，并将运算结果 $D_{SKA}(R_B)$ 回送给主体 B。主体 B 用公钥 PKA 和加密算法 E 对主体 A 发送的运算结果进行加密运

算，如果加密运算结果等于随机数 R_B，即 $E_{PKA}(D_{SKA}(R_B))=R_B$，表明主体 A 知道公钥 PKA 对应的私钥 SKA，主体 A 的身份得到证明。

5.1.4 双向鉴别过程

1. 基于共享密钥

基于共享密钥的双向鉴别过程如图 5.5 所示，主体 A 和主体 B 共同拥有相同的对称密钥 K，且双方使用相同的对称密钥加密解密算法。双向鉴别过程是主体 A 和主体 B 分别向对方证明自己知道共享密钥 K 的过程。

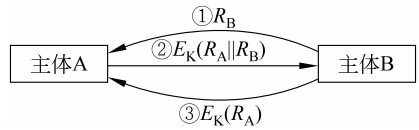

图 5.5 基于共享密钥的双向鉴别过程

主体 B 产生一个随机数 R_B，并将随机数 R_B 发送给主体 A。主体 A 产生一个随机数 R_A，将随机数 R_A 和随机数 R_B 串接在一起，并用对称密钥 K 和加密算法 E 对串接结果 $R_A \| R_B$ 进行加密运算，生成密文 $E_K(R_A \| R_B)$，将密文发送给主体 B。主体 B 用对称密钥 K 和解密算法 D 对密文解密，获得明文，如果从明文中分离出 R_B，即 $D_K(E_K(R_A \| R_B))=R_A \| R_B$，表示主体 A 知道对称密钥 K，主体 A 的身份得到证明。主体 B 从明文中分离出 R_A，用对称密钥 K 和加密算法 E 对 R_A 进行加密运算，生成密文 $E_K(R_A)$，将密文发送给主体 A。主体 A 用对称密钥 K 和解密算法 D 对密文解密，获得明文，如果明文等于 R_A，即 $D_K(E_K(R_A))=R_A$，表示主体 B 知道对称密钥 K，主体 B 的身份得到证明。

2. 基于用户名和口令

基于用户名和口令的双向鉴别过程如图 5.6 所示，主体 A 证明自己身份的过程就是向主体 B 提供有效的用户名和口令的过程。一般情况下，主体 A 对应的口令只有主体 A 和主体 B 知道，如主体 A 是注册用户 A，主体 B 是作为 Internet 服务提供商(Internet Service Provider，ISP)的电信，用户 A 对应的口令 PASSA 只有用户 A 和电信知道，因此，主体 B 为了证明自己是电信，需要向用户 A 证明知道用户 A 的口令 PASSA。

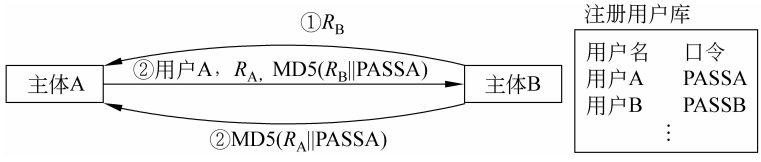

图 5.6 基于用户名和口令的双向鉴别过程

主体 B 产生一个随机数 R_B，并将随机数 R_B 发送给主体 A，主体 A 将随机数 R_B 和自己的口令 PASSA 串接在一起，并对串接结果进行报文摘要运算。主体 A 产生一个随机数 R_A，然后将用户名用户 A、随机数 R_A 和报文摘要 MD5($R_B \| PASSA$)一起发送给主体 B。主体 B 根据用户名用户 A 检索注册用户库，找到用户名为用户 A 的注册用户，获取其口令 PASSA，将随机数 R_B 和口令 PASSA 串接在一起，并对串接结果进行报文摘要运算。然后将运算结果与主体 A 发送的报文摘要进行比较，如果相等，表明主体 A 是用户名为用户 A 的注册用户，主体 A 的身份得到证明。

主体 B 将随机数 R_A 和用户 A 对应的口令 PASSA 串接在一起，并对串接结果进行报文摘要运算。将报文摘要 MD5($R_A \| PASSA$)发送给主体 A。主体 A 将随机数 R_A 和口令 PASSA 串接在一起，并对串接结果进行报文摘要运算。然后将运算结果与主体 B 发送的报文摘要进行比较，如果相等，表明主体 B 知道用户 A 对应的口令，主体 B 的身份得到证明。

基于用户名和口令的双向鉴别用于防止用户接入伪造的接入点(Access Point，AP)和伪造的 ISP 接入网，以免用户访问 Internet 的信息被伪造的 AP 和伪造的 ISP 截获。

3. 基于证书和私钥

基于证书和私钥的双向鉴别过程如图 5.7 所示，主体 B 拥有用于证明公钥 PKA 与主体 A 之间绑定关系的证书，且证书的有效性已经得到验证。主体 A 证明自己身份的过程就是证明自己知道公钥 PKA 对应的私钥 SKA 的过程。同样，主体 A 拥有用于证明公钥 PKB 与主体 B 之间绑定关系的证书，且证书的有效性已经得到验证。主体 B 证明自己身份的过程就是证明自己知道公钥 PKB 对应的私钥 SKB 的过程。

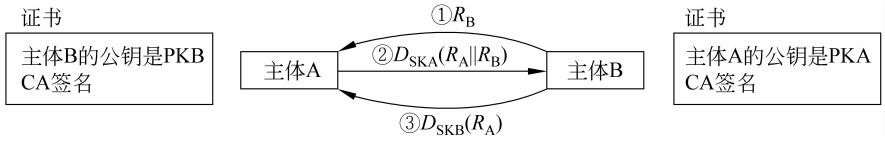

图 5.7　基于证书和私钥的双向鉴别过程

主体 B 产生一个随机数 R_B，并将随机数 R_B 发送给主体 A。主体 A 产生一个随机数 R_A，将随机数 R_A 和随机数 R_B 串接在一起，然后用私钥 SKA 和解密算法 D 对串接结果 $R_A \| R_B$ 进行解密运算，得到运算结果 $D_{SKA}(R_A \| R_B)$，并将运算结果 $D_{SKA}(R_A \| R_B)$回送给主体 B。主体 B 用公钥 PKA 和加密算法 E 对主体 A 发送的运算结果进行加密运算，如果从加密运算结果中分离出随机数 R_B，即 $E_{PKA}(D_{SKA}(R_A \| R_B))=R_A \| R_B$，表明主体 A 知道公钥 PKA 对应的私钥 SKA，主体 A 的身份得到证明。

主体 B 从加密运算结果中分离出随机数 R_A，用私钥 SKB 和解密算法 D 对随机数 R_A 进行解密运算，得到运算结果 $D_{SKB}(R_A)$，并将运算结果 $D_{SKB}(R_A)$发送给主体 A。主体 A 用公钥 PKB 和加密算法 E 对主体 B 发送的运算结果进行加密运算，如果加密运算结果等于随机数 R_A，即 $E_{PKB}(D_{SKB}(R_A))=R_A$，表明主体 B 知道公钥 PKB 对应的私钥 SKB，主体 B 的身份得到证明。

5.1.5　第三方鉴别过程

1. 引出第三方鉴别的原因

基于证书和私钥鉴别过程要求鉴别者必须拥有用于证明公钥与示证者之间绑定关系的证书，且证书的有效性已经得到验证。验证证书的有效性需要提供从鉴别者和示证者共同的信任点开始的证书链。因此，在鉴别者和示证者经常变换的情况下，验证证书有效性的过程将是一个十分复杂的过程。所谓的第三方鉴别就是由权威机构提供与示证者绑定的公钥。且公钥与示证者之间的绑定关系由权威机构予以证明。

2. 鉴别过程

第三方鉴别过程如图 5.8 所示，公钥管理机构是一个权威机构，由公钥管理机构提供与示证者绑定的公钥，且示证者与公钥之间的绑定关系由公钥管理机构予以证明。每一个主体生成公钥和私钥对，主体拥有私钥，由公钥管理机构管理与每一个主体绑定的公钥，且由公钥管理机构证明主体与公钥之间的绑定关系。每一个主体拥有公钥管理机构的公钥 PK，且 PK 与公钥管理机构之间的绑定关系已经得到证明。

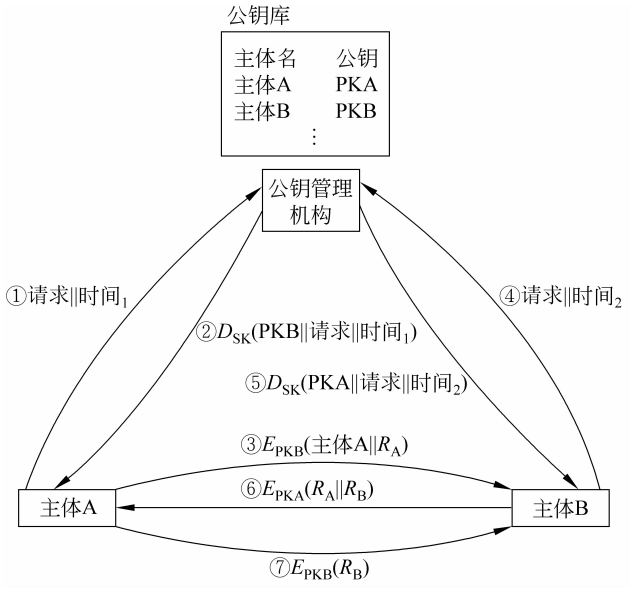

图 5.8 第三方鉴别过程

为了鉴别主体 A 的身份，由公钥管理机构提供与主体 A 绑定的公钥 PKA，且 PKA 与主体 A 之间的绑定关系得到公钥管理机构的证明。主体 A 只要证明自己拥有与 PKA 对应的私钥 SKA，即可证明自己是主体 A。

当主体 A 希望与主体 B 通信时，主体 A 向公钥管理机构发送请求对主体 B 的身份进行鉴别的请求消息，公钥管理机构接收到该请求消息后，根据主体名主体 B 在公钥库中检索到主体 B 对应的公钥 PKB，用公钥管理机构的私钥 SK 和解密算法 D 对主体 B 的公钥 PKB 和请求消息进行解密运算，并将运算结果 D_{SK}(PKB ‖ 请求 ‖ 时间$_1$)发送给主体 A。主体 A 接收到公钥管理机构发送的解密运算结果，用公钥管理机构的公钥 PK 和加密算法 E 对公钥管理机构发送的运算结果进行加密运算，并从加密运算结果(E_{PK}(D_{SK}(PKB ‖ 请求 ‖ 时间$_1$))＝PKB ‖ 请求 ‖ 时间$_1$)中分离出主体 B 的公钥 PKB。主体 A 产生随机数 R_A，将主体名主体 A 和随机数 R_A 串接在一起，用主体 B 的公钥 PKB 和加密算法 E 对串接结果主体 A ‖ R_A 进行加密运算，并将加密运算结果 E_{PKB}(主体 A ‖ R_A)发送给主体 B。主体 B 用自己的私钥 SKB 和解密算法 D 对主体 A 发送的加密运算结果 E_{PKB}(主体 A ‖ R_A)进行解密运算，即 D_{SKB}(E_{PKB}(主体 A ‖ R_A))＝主体 A ‖ R_A。

主体 B 获悉需要与主体 A 通信后，向公钥管理机构发送请求对主体 A 的身份进行鉴别的请求消息，公钥管理机构接收到该请求消息后，根据主体名主体 A 在公钥库中检索

到主体 A 对应的公钥 PKA，用公钥管理机构的私钥 SK 和解密算法 D 对主体 A 的公钥 PKA 和请求消息进行解密运算，并将运算结果 D_{SK}(PKA ‖ 请求 ‖ 时间$_2$)发送给主体 B。主体 B 接收到公钥管理机构发送的解密运算结果，用公钥管理机构的公钥 PK 和加密算法 E 对公钥管理机构发送的运算结果进行加密运算，并从加密运算结果(E_{PK}(D_{SK}(PKA ‖ 请求 ‖ 时间$_1$))＝PKA ‖ 请求 ‖ 时间$_1$)中分离出主体 A 的公钥 PKA。主体 B 产生随机数 R_B，将随机数 R_B 和主体 A 发送的随机数 R_A 串接在一起，用主体 A 的公钥 PKA 和加密算法 E 对串接结果 $R_A \| R_B$ 进行加密运算，并将加密运算结果 $E_{PKA}(R_A \| R_B)$ 发送给主体 A。主体 A 用自己的私钥 SKA 和解密算法 D 对主体 B 发送的加密运算结果 $E_{PKA}(R_A \| R_B)$进行解密运算，即 $D_{SKA}(E_{PKA}(R_A \| R_B))=R_A \| R_B$。如果主体 A 从解密运算结果中分离出随机数 R_A，证明主体 B 拥有公钥 PKB 对应的私钥 SKB，主体 B 的身份得到证明。

主体 A 用主体 B 的公钥 PKB 和加密算法 E 对随机数 R_B 进行加密运算，并将加密运算结果 $E_{PKB}(R_B)$ 发送给主体 B。主体 B 用自己的私钥 SKB 和解密算法 D 对主体 A 发送的加密运算结果 $E_{PKB}(R_B)$进行解密运算，即 $D_{SKB}(E_{PKB}(R_B))=R_B$。如果解密运算结果等于随机数 R_B，证明主体 A 拥有公钥 PKA 对应的私钥 SKA，主体 A 的身份得到证明。

5.2　Internet 接入控制过程

终端接入 Internet 的过程是建立终端与 Internet 中资源之间的传输路径的过程，只有注册用户使用的终端才能接入 Internet，因此，Internet 接入控制过程主要由鉴别使用终端的用户是否是注册用户和允许注册用户使用的终端建立与 Internet 中资源之间的传输路径这两个步骤组成。

5.2.1　终端接入 Internet 需要解决的问题

终端和网络必须完成相关配置后，才能实现终端与网络资源之间的数据交换过程，为了保证只允许授权终端访问网络资源，必须对与授权终端访问网络资源相关的配置过程进行控制。

1. 终端访问网络资源的基本条件

如图 5.9 所示，终端 A 如果需要访问服务器中的资源，终端 A 必须完成以下操作过程。

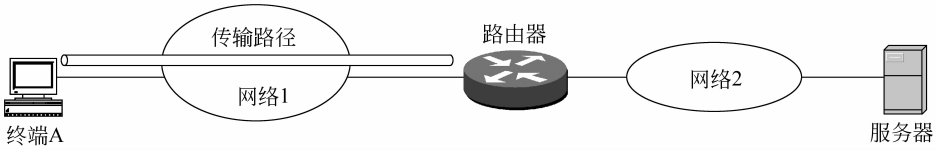

图 5.9　终端访问网络资源过程

(1) 建立终端 A 与路由器之间的传输路径。

终端 A 需要接入网络 1，且建立与路由器之间的传输路径，不同类型的网络有着不同

的建立传输路径的过程。如果网络 1 是公共交换电话网(Public Switched Telephone Network,PSTN),需要通过呼叫连接建立过程建立终端 A 与路由器之间的点对点语音信道。如果网络 1 是以太网,则需要建立终端 A 与路由器之间的交换路径。

(2) 终端 A 完成网络信息配置过程。

建立终端 A 与路由器之间的传输路径后,终端 A 需要完成网络信息配置过程,如 IP 地址、子网掩码、默认网关地址等,终端 A 完成网络信息配置过程后,才能访问网络 2 中的服务器。

(3) 路由器路由表中建立对应路由项。

为实现终端 A 与服务器之间的 IP 分组传输过程,路由器中针对终端 A 的路由项必须将终端 A 的 IP 地址和路由器与终端 A 之间的传输路径绑定在一起,路由器能够将目的 IP 地址为终端 A 的 IP 地址的 IP 分组通过连接路由器与终端 A 之间的传输路径的接口转发出去,该接口可以是物理端口,也可以是逻辑接口。

2. 终端接入 Internet 的先决条件

如果将图 5.9 中的网络 2 作为 Internet,网络 1 作为接入网络,路由器改为接入控制设备,得出如图 5.10 所示的实现终端 A 接入 Internet 的过程。但开始终端 A 接入 Internet 的过程前,必须完成用户注册,只能由注册用户开始终端 A 接入 Internet 的过程,接入控制设备在确定启动终端 A 接入 Internet 的过程的用户是注册用户的情况下,才允许终端 A 完成接入 Internet 的过程。接入控制设备确定用户是注册用户的过程称为用户身份鉴别过程。因此,终端 A 接入 Internet 的先决条件是由注册用户启动终端 A 接入 Internet 的过程,接入控制设备需要对启动终端 A 接入 Internet 的过程的用户进行身份鉴别过程。

由此得出,如图 5.9 所示的终端访问网络资源过程和如图 5.10 所示的终端接入 Internet 的过程的最大不同在于以下两点。

(1) 终端接入 Internet 前,必须证明使用终端的用户是注册用户;

(2) 在确定使用终端的用户是注册用户的前提下,由接入控制设备对终端分配网络信息,建立将终端的 IP 地址和终端与接入控制设备之间的传输路径绑定在一起的路由项。

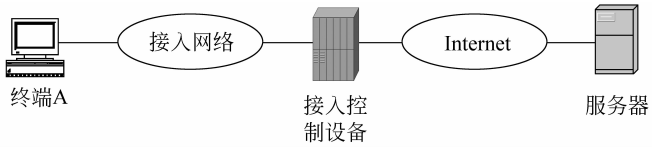

图 5.10 终端接入 Internet 过程

3. 路由器与接入控制设备的区别

图 5.10 中的接入控制设备首先是一个实现接入网络和 Internet 互连的路由器,但除了普通路由器的功能外,还具有以下接入控制功能。

(1) 鉴别终端 A 用户的身份;

(2) 为终端 A 动态分配 IP 地址;

(3) 建立将终端 A 的 IP 地址和终端 A 与接入控制设备之间的传输路径绑定在一起的路由项等。

4. 终端接入 Internet 过程

由于接入 Internet 过程中存在身份鉴别过程,因此,终端 A 完成 Internet 接入过程的操作步骤与图 5.9 中的终端 A 完成网络资源访问过程的操作步骤有所区别。

(1) 建立终端 A 与接入控制设备之间的传输路径。

建立终端 A 与接入控制设备之间的传输路径后,才能进行终端 A 与接入控制设备之间的通信过程。后续操作步骤正常进行的前提是,终端 A 与接入控制设备之间能够正常进行通信过程。不同的接入网络有着不同的建立终端 A 与接入控制设备之间的传输路径的过程,拨号接入、非对称数字用户线路(Asymmetric Digital Subscriber Line,ADSL)接入和以太网接入的主要区别在于建立终端 A 与接入控制设备之间的传输路径的过程。拨号接入方式下,通过终端 A 和接入控制设备之间的呼叫连接建立过程,建立终端 A 和接入控制设备之间的点对点语音信道。以太网接入方式下,由以太网建立终端 A 和接入控制设备之间的交换路径。

(2) 接入控制设备完成身份鉴别过程。

接入控制设备必须能够确定启动终端 A 接入 Internet 的过程的用户是否是注册用户,只有在确定用户是注册用户的前提下,才能进行后续操作步骤。

(3) 动态配置终端 A 的网络信息。

接入控制设备完成用户身份鉴别过程,确定启动终端 A 接入 Internet 的过程的用户是注册用户的情况下,才能对终端 A 配置网络信息。因此,终端 A 是否允许接入 Internet,即配置的网络信息是否有效,取决于使用终端 A 的用户。接入控制设备确定使用终端 A 的用户是注册用户的情况下,维持配置给终端 A 的网络信息有效。一旦确定使用终端 A 的用户不是注册用户,接入控制设备将撤销配置给终端 A 的网络信息。因此,终端 A 的网络信息不是静态不变的。

(4) 动态创建终端 A 对应的路由项。

接入控制设备为终端 A 配置 IP 地址后,必须创建用于将终端 A 的 IP 地址和接入控制设备与终端 A 之间的传输路径绑定在一起的路由项。由于终端 A 的 IP 地址不是静态不变的,因此,该路由项也是动态的,在确定使用终端 A 的用户是注册用户的情况下,维持用于将终端 A 的 IP 地址和接入控制设备与终端 A 之间的传输路径绑定在一起的路由项。一旦确定使用终端 A 的用户不是注册用户,接入控制设备将撤销该路由项。

5.2.2　PPP 与接入控制过程

点对点协议(Point to Point Protocol,PPP)既是基于点对点信道的链路层协议,又是接入控制协议。

1. PPP 作为接入控制协议的原因

1) 拨号接入过程

早期的拨号接入过程如图 5.11 所示,终端 A 通过 Modem 连接用户线(俗称电话线),接入控制设备与 PSTN 连接,终端 A 和接入控制设备都分配电话号码,如图 5.11 所

示的终端 A 分配的电话号码 63636767 和接入控制设备分配的电话号码 16300。终端 A 通过呼叫连接建立过程建立与接入控制设备之间的点对点语音信道。

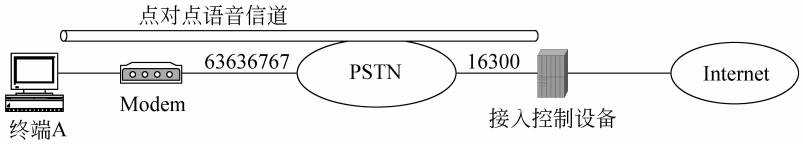

图 5.11　拨号接入过程

2）点对点语音信道与 PPP

接入控制设备完成对终端 A 的接入控制过程中，需要与终端 A 交换信息，如终端 A 的用户身份标识信息、接入控制设备为终端 A 分配的网络信息（IP 地址、子网掩码等）等，由于终端 A 与接入控制设备之间的传输路径是点对点语音信道，因此，需要将终端 A 与接入控制设备之间相互交换的信息封装成适合点对点语音信道传输的帧格式，PPP 帧就是适合点对点语音信道传输的帧格式。因此，接入控制设备完成对终端 A 的接入控制过程中，需要与终端 A 相互传输 PPP 帧。

2. 与接入控制相关的协议

1）PPP 帧结构

与接入控制过程相关的控制协议有鉴别协议、IP 控制协议等，鉴别协议用于鉴别用户身份，IP 控制协议用于为终端动态分配 IP 地址，这些协议对应的协议数据单元（Protocol Data Unit，PDU）成为 PPP 帧中信息字段的内容。PPP 帧中协议字段值给出信息字段中 PDU 所属的协议。封装不同控制协议 PDU 的 PPP 帧格式如图 5.12 所示。

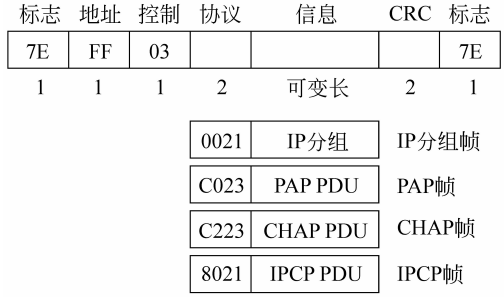

图 5.12　PPP 帧结构

2）用户身份鉴别协议

完成注册后，ISP 为注册用户分配用户名和口令，因此，确定某个用户是否是注册用户的过程就是判断用户能否提供有效的用户名和口令的过程。假定接入控制设备中有着注册用户库，注册用户库中存储了所有注册用户的用户名和口令，在这种情况下，接入控制设备确定某个用户是否是注册用户的过程就是判断用户能否提供注册用户库中存储的用户名和口令的过程。

鉴别用户身份的协议有口令鉴别协议（Password Authentication Protocol，PAP）和挑战握手鉴别协议（Challenge Handshake Authentication Protocol，CHAP）。PAP 完成