第3章 IP协议及其安全问题

3.1 IP地址

IP地址是一个32位的二进制地址，它用来唯一地在全世界范围内标识一台主机或一台路由器。因特网上的两台设备不会有相同的IP地址，但一台设备如果有多个网络接口，那么它可以有多个IP地址。

因为一个IP地址有32位，因此总的IP地址数量为2^{32}，即4 294 967 296个。

3.2 IP协议

在TCP/IP协议簇中，网络层包括5个协议：地址解析协议(Address Resolution Protocol，ARP)、反向地址解析协议(Reverse Address Resolution Protocol，RARP)、因特网协议(Internet Protocol，IP)、因特网控制报文协议(Internet Control Message Protocol，ICMP)和因特网群组管理协议(Internet Group Management Protocol，IGMP)，如图3-1所示。

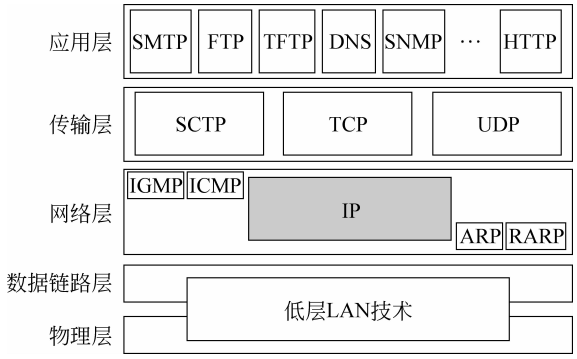


图3-1 TCP/IP层次结构

网络层的主要协议是IP协议，IP协议的主要职责是在全网范围内将IP数据报从源主机送达目的主机，然而IP也需要其他协议所提供的服务。

在IP数据报的传递过程中，IP协议需要ARP确定下一跳路由器的MAC地址，同时需要ICMP来处理传输过程中出现的差错等异常情况。

IP 协议用于单播通信，即将数据报从一个信源端传递到一个信宿端。而因特网上的许多应用（例如视频直播）需要多播传递，即将数据报从一个信源端传递到多个信宿端。这时 IP 协议需要借助 IGMP 完成多播任务。首先学习 IP 数据报的格式。

3.2.1　IP 数据报格式

IP 层的分组被称为 IP 数据报，图 3-2 说明了 IP 数据报的格式。IP 数据报由两部分组成：首部和数据。首部长度为 20～60 字节，它包含进行路由选择和报文传递所必需的信息。

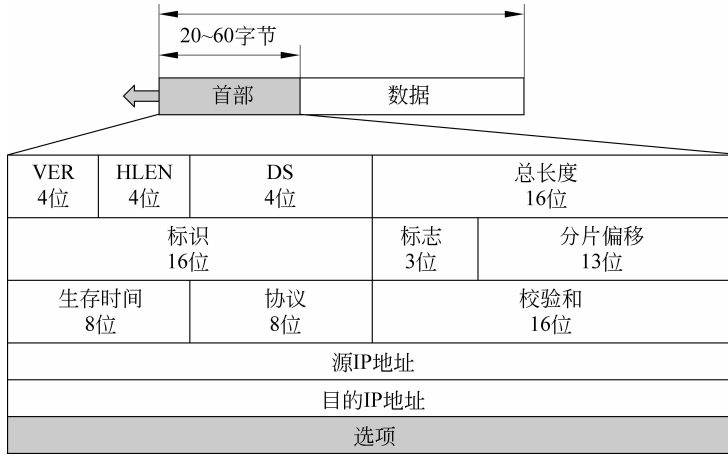


图 3-2　IP 数据报格式

图 3-3 给出的是使用 Sniffer 捕获的一个数据帧，前 14 个字节为数据链路层数据，其后 20 字节（带阴影部分）为网络层数据（即 IP 首部），最后 28 字节为传输层数据（这里是 TCP）。下面通过这个数据帧具体学习 IP 首部的每个字段的含义。

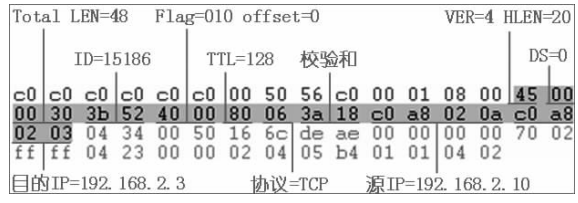


图 3-3　结合具体数据报分析 IP 首部格式

（1）版本（version，VER，4b）：这个字段定义了 IP 协议的版本。IP 首部第 1 个字节的高 4 位定义了版本号，目前的版本是 4（IPv4）。然而不久的将来版本 6（IPv6）可能会完全取代 IPv4 协议。在图 3-3 中第 1 个字节的高 4 位二进制数为 4，说明这个数据报使用的是 IPv4 协议。

（2）首部长度（header length，HLEN，4b）：首字节的低 4 位定义了首部长度，这个字段以 4 字节为单位定义 IP 首部的长度，即将该值乘 4 得到的结果是 IP 首部的长度。上例中首字节的低 4 位为 5，说明 IP 首部长度是 20。

(3) 差分服务(differentiated service,DS,1B)：这个字段定义了服务质量类型。目前在实际应用中,这个字段并未使用。在上例中 DS 为 0。

(4) 总长度(total length,2B)：该字段以字节为单位定义了 IP 数据报的总长度(首部和数据的长度之和)。因为这个字段长度为 2 字节,所以 IP 数据报的总长度限制在 65 535($2^{16}-1$)字节范围之内。在上例中 IP 首部长度为 20 字节、数据长度为 28 字节,因此总长度为 48,用十六进制表示就是 0x 00 30。

(5) 标识、标志和分片偏移在 3.2.2 节介绍。

(6) 生存时间(TTL,1B)：这个字段用来防止无人接收的 IP 数据报在网络中循环传递,造成网络拥塞。当一个信源主机准备发送一个 IP 数据报时,它就在这个数据报的 TTL 字段存储一个数值,这个数值远大于信源和信宿主机之间路由器的个数(例如 Windows 系统主机通常将 TTL 设置为 128)。报文在传递过程中每经过一台路由器,TTL 值就被减 1,如果减 1 后值为 0,路由器就丢弃这个报文,若不为 0 路由器就转发这个报文。上例中 TTL=128。

(7) 协议(1B)：这个字段定义了传输层协议类型。常见传输层协议的对应数值如图 3-4 所示。上例中协议字段值为 6,代表传输层使用的是 TCP。

值	协议
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

图 3-4　传输层协议数值

(8) 校验和(2B)：IP 校验和只对首部进行校验,而不对数据部分校验。这样做有两个原因。第一,传输层协议(TCP 和 UDP)都有自己的校验和机制,可以保证高层数据的完整性,因此 IP 校验和不需要对高层数据进行重复校验。第二,IP 数据报在整个传递过程中会经过多台路由器,每经过一台路由器,IP 首部的某些字段就会发生改变(例如 TTL、分片偏移、标志、总长度),而 IP 数据部分不会改变,因此校验和只包括会发生变化的 IP 首部,如果将数据也包括在内,那么每台路由器必须重新计算整个报文的校验和,这就增加了每台路由器的处理时间,降低了处理效率。

上例中 IP 校验和的计算过程如图 3-5 所示。20 字节的 IP 首部按照 16 位等分成 10 段,检验和字段设置为 0,将所有项相加取反得到校验和 0x3a18,将结果插入校验和字段。

(9) 源 IP 地址(4B)：定义了信源 IP 地址,上例信源 IP 地址为 192.168.2.10。

(10) 目的 IP 地址(4B)：定义目的主机地址,上例为 192.168.2.3。

3.2.2　IP 数据报的分片和重组

受物理特性限制,每种类型网络能传输的单个 IP 数据报的最大长度都有一定限制。这个最大数据报长度称为该类型网络的 MTU 值(maximum transfer unit)。图 3-6 给出的是不同类型网络的 MTU 值。

由于不同类型网络能够传输的最大报文长度不同,这就产生了 IP 数据报的分片和重组问题,下面举例说明。在图 3-7 中一个以太网络和一个令牌环网络通过一台路由器连接,主机 H 给主机 A 发送一个大小为 4000 字节的 IP 数据报,路由器在令牌环网接口收到这个报文之后,发现它的长度超过以太网的 MTU 值 1500,因此将其分为三个分片,大小依次为 1400、1400 和 1200 字节。这三个分片通过以太网络最终传输到主机 A,主机 A

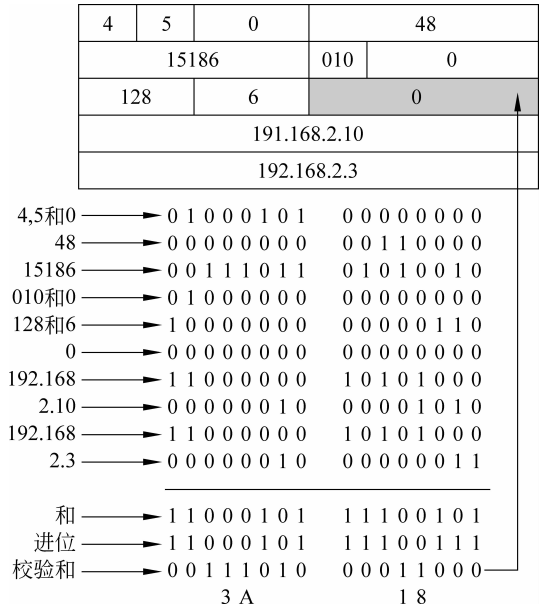


图 3-5　校验和计算示例

再将这三个分片重组为一个 4000 字节的 IP 数据报。在传输过程中路由器负责分片，目的主机 A 负责重组分片。

协议	MTU
超级通道(Hyperchannel)	65 535
令牌环(16Mb/s)	17 914
令牌环(4Mb/s)	4464
FDDI	4352
以太网	1500
X.25	576
PPP	296

图 3-6　不同类型网络的 MTU 值

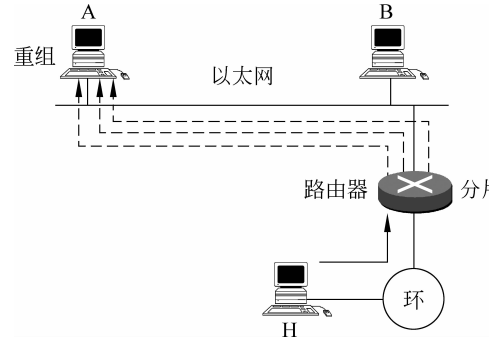


图 3-7　分片和重组机制

在 IP 首部中与分片和重组机制有关的字段是标识、标志和分片偏移。

(1) 标识(2B)：这个字段唯一地定义了一个数据报。数据报被分片时，这个字段被复制到所有分片中。接收端将具有相同标识的分片重组成一个原始报文。

(2) 标志(3b)：这是一个 3 位字段。第一位保留。第二位是“不分片位”，如果该位值为 1，则路由器不能对该数据报进行分片。在上例中如果主机 H 发出的 4000 字节的 IP 数据报的不分片位设置为 1，路由器会直接丢弃这个报文，并向主机 H 发送一个 ICMP 差错报文。如果不分片位值为 0，则路由器可以根据需要对 IP 数据报进行分片。第三位是“还有分片位”，如果其值为 1，则表示当前报文不是最后一个分片，在该数据报之后还有其他分片；如果其值为 0，则意味着这个数据报是最后一个或唯一的分片。

(3) 分片偏移(13b)：表示这个分片的第一个字节在整个数据报中的相对位置。以 8 字节为度量单位。

下面举例说明 IP 数据报的分片和重组机制。原始数据报携带了 4000 字节的数据，路由器为了进行传输，将原始数据报划分为三个分片，原始数据报的标识字段被复制到所有分片当中，如图 3-8 所示。

接收端发现这三个报文具有相同的标识 14 567，于是知道它们属于同一个原始数据报。接下来确定三个分片的次序，分片偏移字段为 0 的是起始分片。第一个分片的长度为 1400 字节，因此第二个分片的偏移字段为 1400/8＝175，如果还有其他分片，可依次确定次序。最后一个分片的“还有分片位”值为 0，据此确定最后一个分片。

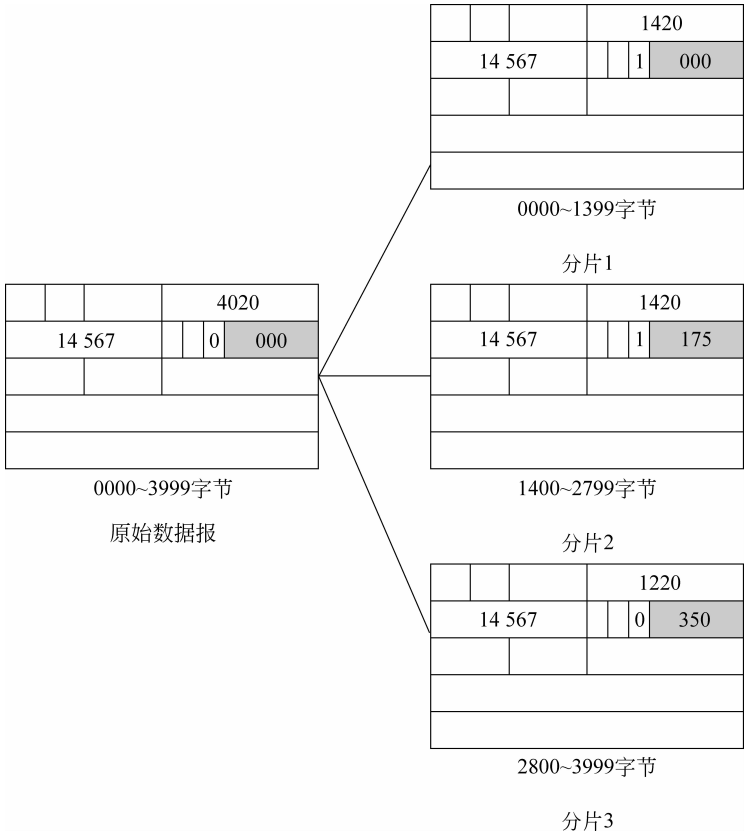


图 3-8　分片举例

训练：捕获、分析 IP 数据报分片。

第一步：启动 Windows XP 虚拟机，配置 IP 地址为 192.168.2.3，子网掩码为 255.255.255.0。本机 IP 地址为 192.168.2.10。

第二步：在本机执行 ping 192.168.2.3 -l 4000 命令。-l 参数指明本机发送的 IP 数据报大小为 4000 字节，这个数值超过以太网的最大报文长度限制 1500，因此在本机将对原始数据报进行分片，以下是使用 Sniffer 捕获到的三个分片。

如图 3-9 所示，第一个分片标识为 15 186，总长度是 1500。IP 数据报首部长度是 20

字节，因此 IP 数据部分长度是 1480 字节，由此可知第二个 IP 数据报的分片偏移字段值为 1480/8＝185，即 0xB9。

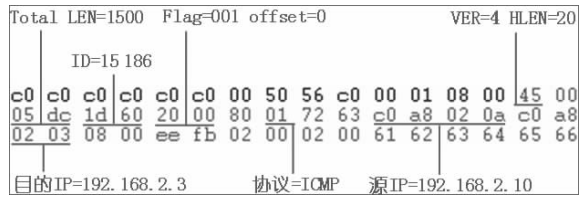


图 3-9　第一个分片

如图 3-10 所示，第二个分片的标识也是 15 186，分片偏移为 0xB9。总长度为 1500 字节。IP 首部长度为 20 字节，因此 IP 数据部分长度为 1480 字节，由此可知第三个 IP 数据报的分片偏移字段值为(1480＋1480)/8＝370，即 0x172。

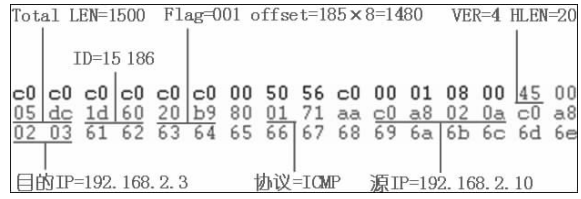


图 3-10　第二个分片

如图 3-11 所示，第三个分片的标识也是 15 186，分片偏移为 0x172。总长度为 1068 字节。IP 首部长度为 20 字节，因此 IP 数据部分长度为 1048 字节。这个数据报的“还有分片位”值为 0，说明这是最后一个分片。

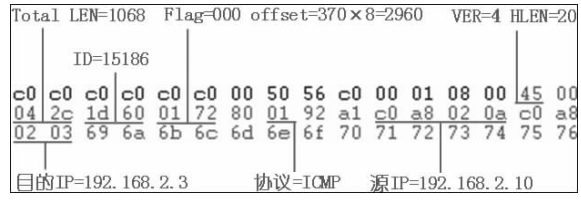


图 3-11　第三个分片

三个分片 IP 数据部分的长度分别为 1480、1480 和 1048 字节，将这三个数值相加得到的结果为 4008，而不是 4000，那么多出的那 8 字节是什么呢？通过 Sniffer 分析第一个分片可知，多出的那 8 字节数据是 ICMP 的首部。

3.3　泪滴攻击

图 3-12 给出的是正常情况下 IP 数据报的分片和重组过程。在发送端 3072 字节的原始数据报被分成三个 1024 字节的分片通过网络传输给接收端，接收端收到这三个分片

之后，根据三个分片的标识、标志和分片偏移字段将这三个分片重新组装成一个原始报文。

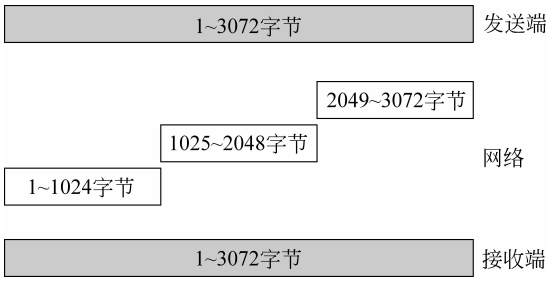


图 3-12　正常情况下的分片过程

泪滴攻击也称为分片攻击。它是入侵者伪造数据报文，向目标主机发送含有重叠偏移的畸形数据分片，当数据分片到达目的主机后，在堆栈中重组时，就会导致重组出错，引起协议栈的崩溃。图 3-13 给出的是泪滴攻击的示意图。

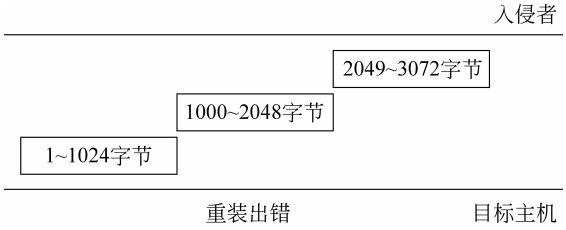


图 3-13　泪滴攻击示意图

攻击者发送三个分片，目标主机收到这三个分片之后，发现它们具有相同的标识字段，因此尝试将它们重组成一个原始报文，但由于第一和第二个数据分片具有重叠部分，因此重组失败。如果这类重叠报文数量庞大，就会引起目标主机协议栈崩溃。

3.4　网络地址转换

3.4.1　专用地址

所有 IPv4 地址加在一起总共有 2^{32} 个，这个数字虽然看起来比较庞大，但随着 Internet 规模的快速增长，IP 地址出现不足。

中国的 IPv4 地址主要是通过几大网络运营商和中国互联网络信息中心申请到的。在我国拥有的 IPv4 地址中，运营商手中仍掌握部分 IPv4 地址可以使用，根据运营商网络和业务的不同情况，有的运营商手中的地址可以支撑未来五六年，有的则只能支撑一两年。

如何解决 IP 地址不足的问题呢？因特网权威机构采用专用地址来解决。IP 地址空间中预留出三块地址用做专用地址，见图 3-14。任何组织机构都可以使用这些专用地

址，而不需要获得因特网权威机构的许可，这就解决了地址不足的问题。

前缀	范围	总数
10/8	10.0.0.0~10.255.255.255	2^{24}
172.16/12	172.16.0.0~172.31.255.255	2^{20}
192.168/16	192.168.0.0~192.168.255.255	2^{16}

图 3-14　专用地址

3.4.2　网络地址转换概述

专用地址虽然解决了 IP 地址不足的问题，但由于任何一个组织机构都可以随意地使用专用地址块，这会导致不同机构的主机采用了相同的 IP 地址，即出现 IP 地址冲突。为了防止这种现象的出现，因特网权威机构规定：专用地址只能使用在机构的内部局域网中，而不能出现在外部的因特网上（即路由器不会向外网转发目的 IP 地址为专用地址的数据报）。这样一来地址冲突的问题解决了，但又导致内部主机无法与外网通信的问题。

为了能让使用专用地址的内部主机与外部因特网通信，在路由器上需要开启 NAT 地址转换功能。图 3-15 说明了 NAT 地址转换过程。内部网络使用 192.168.*.* 的专用地址块，内部网络通过 NAT 路由器与外部因特网连接。IP 地址为 192.168.7.1 的内部主机向外网主机发送一个数据报，报文的源 IP 地址为 192.168.7.1。报文到达路由器之后，路由器将源 IP 地址替换为自己的合法地址 200.24.5.8，之后将其转发给外网，此时数据报的源和目的 IP 地址都是合法 IP，因此可以通过因特网传送到目的主机。

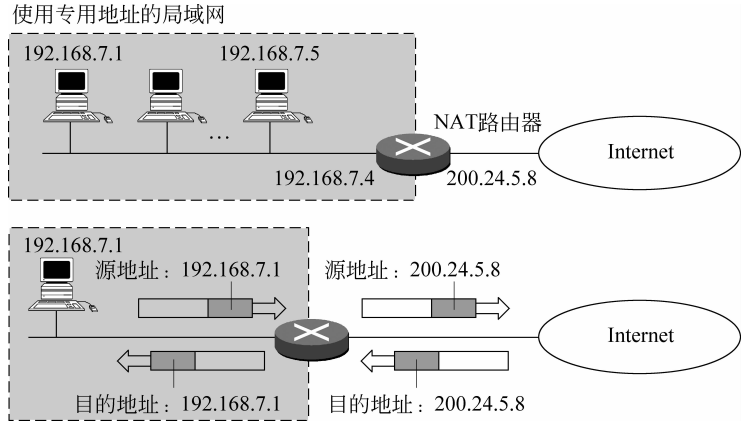


图 3-15　NAT 地址转换过程

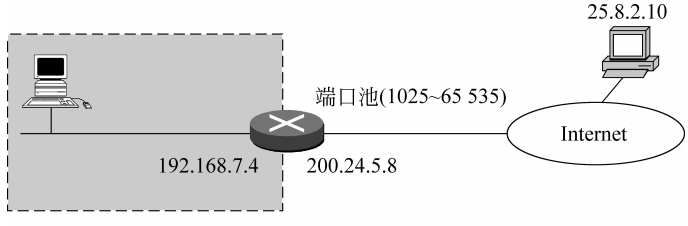
外网返回的数据报到达路由器之后，路由器将目的 IP 地址由 200.24.5.8 替换回 192.168.7.1，然后在内网接口转发，这样一来内部主机实现了与外部主机的通信。

3.4.3　同时使用 IP 地址和端口号

目前路由器广泛采用的 NAT 转换方法是同时使用 IP 地址和端口号的 NAPT 转换

方法，下面结合实例说明。在 NAT 路由器上维护了一个端口池，其中保存了 1025～65 535 共 64 511 个随机端口，同时路由器维护了一个转换表，包括 4 个字段：专用地址、源端口、专用端口和传输层协议字段。如图 3-16 所示，假设路由器接收到一个发给外网的数据报，源 IP 地址为 192.168.7.1、源端口为 2000，目的 IP 为 25.8.2.10、目的端口为 80。路由器从端口池中取出一个空闲端口 1025 分配给这条 TCP 连接，然后在转换表中记录下相应信息，之后将源 IP 地址改为自己的合法 IP 地址 200.24.5.8、源端口改为 1025，再将报文转发给因特网。

因特网返回的数据报到达路由器之后，路由器取出报文的目的端口 1025 到转换表中进行查找，发现存在匹配记录，于是将报文的目的 IP 改为 192.168.7.1、目的端口改为 2000，之后将报文在内网接口转发，这样内、外网主机实现了连通。当这条 TCP 连接不再使用时（例如出现 4 次挥手中断连接报文或 RST 复位报文或连接超时），这条转换记录将被清除，1025 端口被重新放回端口池。



专用地址	源端口号	专用端口	传输层协议
192.168.7.1	2000	1025	TCP

转换表

图 3-16　NAPT 转换

训练：利用 NAPT 实现局域网访问因特网。

第一步：利用 Cisco 模拟器按照图 3-17 组建网络。

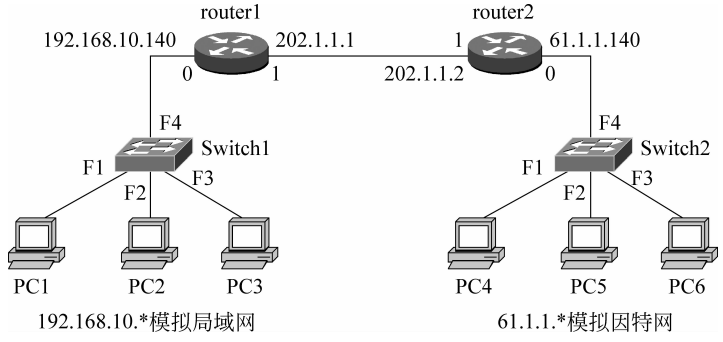


图 3-17　网络拓扑结构

1～3 号主机连接在 Switch1 的 1～3 端口上，Switch1 的 4 端口与 router1 的 0/0 端口连接。4～6 号主机连接在 Switch2 的 1～3 端口，Switch2 的 4 端口与 router2 的 0/0 端口连接。router1 的 0/1 端口和 router2 的 0/1 端口通过一根反序双绞线连接在一起。Switch1 上连接的主机处于 192.168.10.* 网段(模拟使用专用地址的局域网)。Switch2 上连接的主机处于 61.1.1.* 网段(模拟使用全球合法地址的外部 Internet)。

第二步：将 1～3 号主机的 IP 地址改为 192.168.10.*，其中 * 为序号，网关设置为 192.168.10.140。将 4～6 号主机的 IP 地址改为 61.1.1.*。其中 * 为序号，网关设置为 61.1.1.140。

第三步：配置局域网路由器 router1 端口 IP 地址。

```
router >en
router #conf  t
router (config)#interface fastethernet 0/0
router (config-if)#ip address 192.168.10.140 255.255.255.0
router (config-if)#no shutdown
router (config-if)#interface fastethernet 0/1
router (config-if)#ip address 202.1.1.1 255.255.255.0
router (config-if)#no shutdown
router (config-if)#
router #
router #show ip interface brief
Interface                      IP-Address(Pri)      OK?      Status
FastEthernet 0/0               192.168.10.140/24    YES      UP
FastEthernet 0/1               202.1.1.1/24         YES      UP
```

第四步：配置互联网路由器 router2 端口 IP 地址。

```
router>en
router #conf  t
router (config)#interface fastethernet 0/0
router (config-if)#ip address 61.1.1.140 255.255.255.0
router (config-if)#no shutdown
router (config-if)#interface fastethernet 0/1
router (config-if)#ip address 202.1.1.2 255.255.255.0
router (config-if)#no shutdown
router (config-if)#
router #
router #show ip interface brief
Interface                      IP-Address(Pri)      OK?      Status
FastEthernet 0/0               61.1.1.140/24        YES      UP
FastEthernet 0/1               202.1.1.2/24         YES      UP
```

第五步：在局域网路由器 router1 上配置默认路由。

```
router #conf t
```

```
router (config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0/1
router (config)#^z
router #show ip route
Codes: C -connected, S -static, I -IGRP, R -RIP, M -mobile, B -BGP
   D -EIGRP, EX -EIGRP external, O -OSPF, IA -OSPF inter area
  N1 -OSPF NSSA external type 1, N2 -OSPF NSSA external type 2
  E1 -OSPF external type 1, E2 -OSPF external type 2, E -EGP
   i -IS-IS, L1 -IS-IS level-1, L2 -IS-IS level-2, ia -IS-IS inter area
    * -candidate default, U -per-user static route, o -ODR
    P -periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet0/0
C    202.1.1.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 is directly connected, FastEthernet0/1
```

第六步：在局域网路由器 router1 上配置 NAPT 映射。

```
Router#conf t
Router(config)#interface fastethernet 0/0
Router(config-if)#ip nat inside                          //定义 0 端口为内网端口
Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ip nat outside                         //定义 1 端口为外网接口
Router(config-if)#exit
Router(config)#ip nat pool to_internet 202.1.1.3  202.1.1.10 netmask 255.255.255.0
Router(config)#access-list 10 permit 192.168.10.0 0.0.0.255
//定义允许转换的地址
Router(config)#ip nat inside source list 10 pool to_internet overload
```

第七步：在公网 PC4 上开启 Web 服务，在 1～3 号主机访问论坛，在 router1 上查看形成的日志文件。

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 202.1.1.3:1025     192.168.10.1:1025    61.1.1.4:80        61.1.1.4:80
tcp 202.1.1.3:1024     192.168.10.2:1025    61.1.1.1:80        61.1.1.1:80
```

3.4.4 利用静态 NAT 实现因特网主机访问局域网服务器

通过 NAPT 可以实现内网主机与外网的通信，但这种通信必须由内网主机首先发起，这样才会在路由器的转换表中形成转换记录。然而在很多情况下需要在内部网络搭建服务器供外网用户访问，例如，在内网搭建介绍本单位信息的 Web 服务器、提供资源下载服务的 FTP 服务器等，这种情况下通信由外网的客户机首先发起，但由于在转换表中

没有形成转换记录，外网主机将无法访问到内网服务器。为了解决这一问题，目前广泛采用的办法是预先在路由器的转换表中添加一条静态转换记录，将某个全局地址映射为内部服务器使用的专用地址。这样一来，外网用户就可以通过这个全局合法地址访问到内网的服务器。下面通过一个实例来学习这种方法。

训练：利用静态 NAT 实现因特网主机访问局域网服务器。

在 PC3 上开启 Web 服务，模拟在内网组建的 Web 服务器。其 IP 地址是 192.168.10.3，在 router1 上开启静态地址转换，将 192.168.10.3 映射为 202.1.1.5，使外部 Internet 上的主机可以通过 202.1.1.5 访问到内网服务器上搭建的网站。

第一步：为内网服务器配置 IP 地址和网关地址。

第二步：配置局域网路由器 router1 端口 IP 地址(步骤略)。

第三步：配置互联网路由器 router2 端口 IP 地址(步骤略)。

第四步：在 router1 上定义默认路由(步骤略)。

第五步：在 router1 上配置静态内部源地址转换，将 PC3 的 IP 地址 192.168.10.3 映射为地址池中的全球合法 IP 地址 202.1.1.5。

选中 router1

```
router#conf t
router (config)#ip nat inside source static 192.168.10.3 202.1.1.5
```

解释：将 PC3 的专用地址映射为全球合法地址

```
router (config)#interface fastethernet 0/0
router (config-if)#ip nat inside
```

解释：定义内部接口

```
router (config-if)#interface fastethernet 0/1
router (config-if)#ip nat outside
```

解释：定义外部接口

第六步：在 4～6 号主机的 IE 地址栏中输入“http://202.1.1.5/”登录内网服务器。

第七步：登录 router1，查看地址转换结果。

```
router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  202.1.1.5         192.168.10.3        ---                ---
```

3.5 网络层的安全协议 IPSec

IPSec(IP Security)是由 IETF(Internet Engineering Task Force，因特网工程任务组)设计的用来为 IP 层的分组提供安全的一组协议。IPSec 没有规定使用特定的加密或者鉴别方法，而是提供一个框架和机制，它将加密、鉴别和散列方法的选择权留给用户。

3.5.1 测试开通 IPSec 通道、采用 AH 协议、提供完整性校验

1. 测试环境

实验环境如图 3-18 所示。Windows XP 虚拟机作为 Web 服务器，本机作为客户端，联网方式为 host-only，各个对象的地址信息如图 3-18 所示。

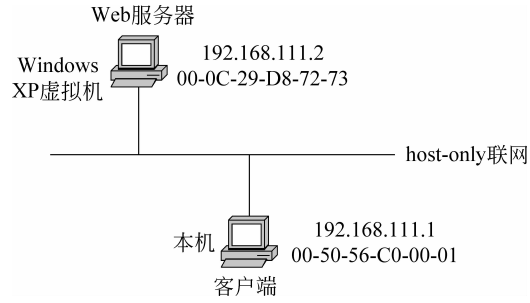


图 3-18 实验环境

2. 测试目的

在本机和 Windows XP 虚拟机上开通 IPSec 通道，选择 AH 协议。使用 Sniffer Pro 捕获客户访问 Web 服务器过程中传输的数据包，通过分析捕获的数据，进一步理解 IPSec 协议的组成、AH 协议的格式和作用。

3. 实验步骤

第一步：开通本机的 IPSec 通道。

在本机控制面板中双击“管理工具”→双击“本地安全策略”→右击“IP 安全策略”，在本地计算机选择创建 IP 安全策略→单击“下一步”按钮→输入新策略名称（例如 AA）→单击“下一步”按钮，直至完成。新添加的 AA 策略如图 3-19 所示。

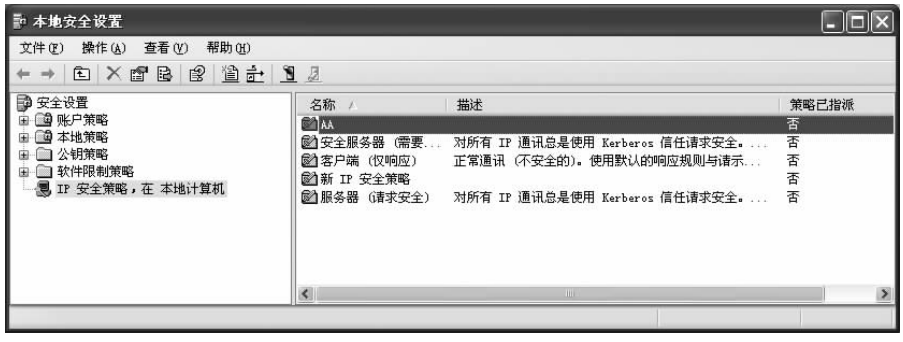


图 3-19 新添加的 AA 策略

右击“AA 策略”→选择“属性”→单击“添加”按钮→在“IP 筛选器”列表中单击“添加”按钮→输入新筛选器名称（如 AA 筛选器）→单击“添加”按钮→源地址和目标地址按如图 3-20 所示进行配置→单击“确定”按钮。

在“IP 筛选器”列表中选中“AA 筛选器”→单击“筛选器操作”标签→单击“添加”按钮→选中“协商安全”→单击“添加”按钮→选择“自定义”→单击“设置”→选中“地址和数据不加密的完整性”，完整性算法选择 MD5→连续两次单击“确定”按钮→在“新筛选器操作属性”对话框中可见新添加的筛选器操作，如图 3-21 所示。

单击“确定”按钮→选中新添加的筛选器操作、单击“身份验证方法”标签→单击“添加”按钮→选中“预共享密钥”→输入共享密钥“86982480”→单击“确定”按钮→选中“预先

图 3-20　设置源和目的 IP 地址

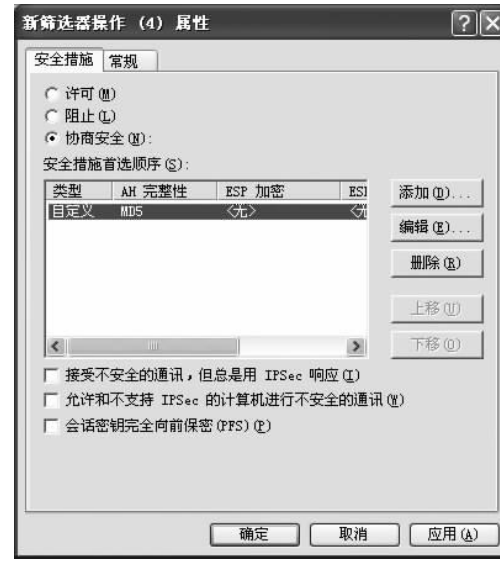


图 3-21　新添加的筛选器操作

共享的密钥”→单击“上移”按钮将其移动到第一的位置(见图 3-22)→单击“应用”按钮→单击“确定”按钮，至此本机端设置完成。

第二步：开通 Windows XP 虚拟机的 IPSec 通道。

开通 Windows XP 虚拟机的 IPSec 通道(步骤同上)，只是源和目的 IP 地址进行了对换，见图 3-23。

图 3-22　设置的预共享密钥

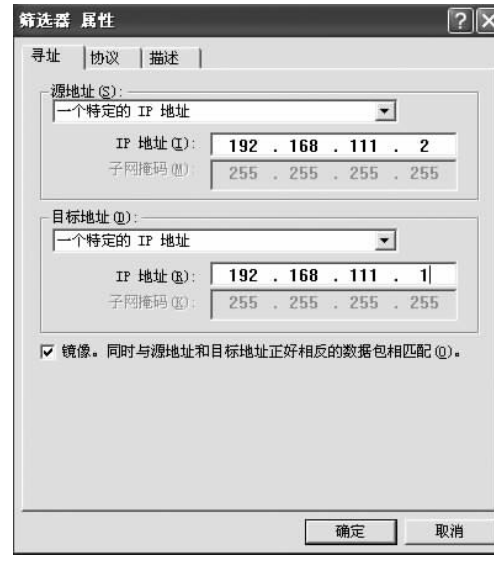


图 3-23　设置源和目的 IP 地址

第三步：在本机和 Windows XP 虚拟机指派安全策略。

在本机指派 AA 安全策略，右击 AA→选择“指派”，同样指派 Windows XP 虚拟机上的 BB 安全策略。至此本机和 Windows XP 虚拟机之间的 IPSec 通道开通完成，在这两台主机之间传输的数据都将受到 AH 协议的完整性保护，如图 3-24 和图 3-25 所示。

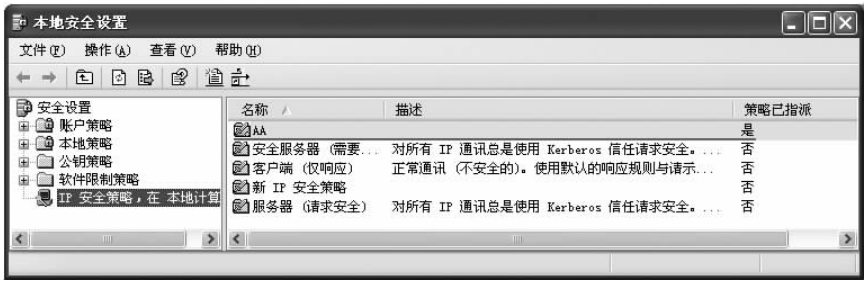


图 3-24　在本机指派 AA 安全策略

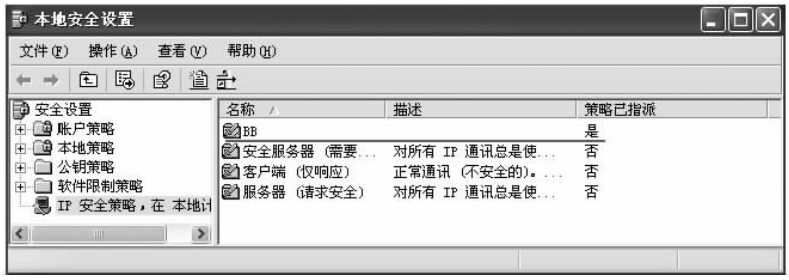


图 3-25　在 Windows XP 虚拟机指派 BB 安全策略

第四步：在本机浏览 Windows XP 虚拟机的网页，同时使用 Sniffer Pro 捕获、分析数据。

使用 Sniffer Pro 捕获的数据包如图 3-26 所示，从中可以清楚看到 IKE 协商过程和 AH 的通信过程。

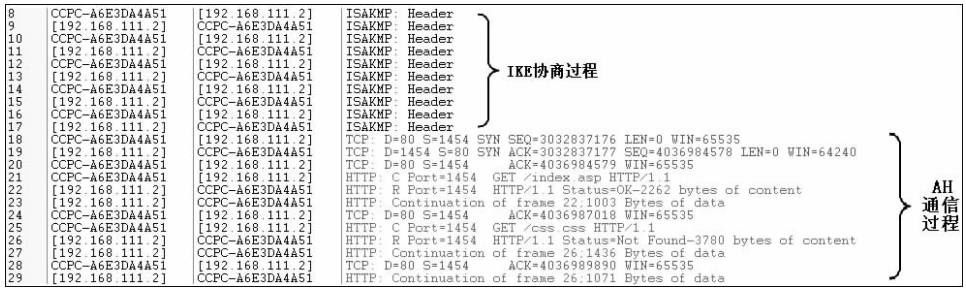


图 3-26　使用 Sniffer Pro 查看到的 IPSec 通信过程

从图 3-26 可以看出，传输的数据包没有进行加密，但具体查看通信数据会发现每个数据包中都加入了一个 AH 首部。图 3-27 为本机发给 Web 服务器的一个数据包，可以看到在 IP 首部后面增加了 24 字节的 AH 首部，各字段含义如图 3-27 所示，其中 12 字节的鉴别数据保证了整个 IP 数据报的完整性。

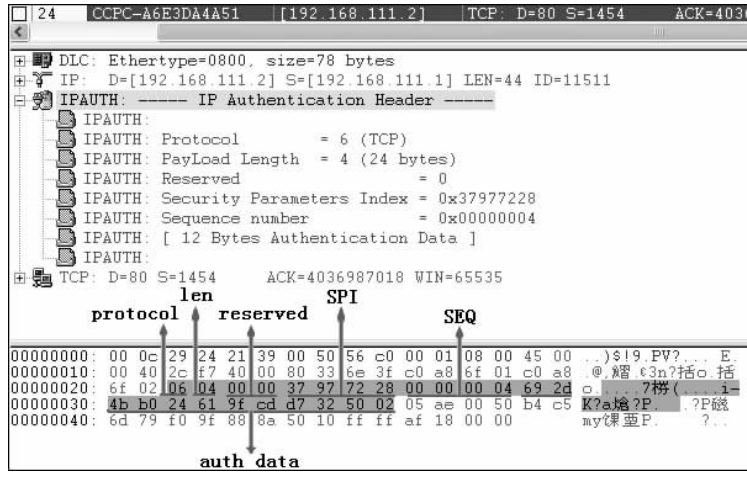


图 3-27　在每个数据包中都加入了一个 AH 首部

3.5.2　测试开通 IPSec 通道、选择 ESP、提供完整性

1. 测试环境

实验环境同 3.5.1 节，这里不再赘述。

2. 测试目的

在上一个实验的基础上修改 IPSec 通道，选择 ESP，提供完整性。使用 Sniffer Pro 捕获客户访问 Web 服务器过程中传输的数据包，通过分析捕获的数据，进一步理解 ESP 的格式和作用。

3. 实验步骤

第一步：修改本机 IPSec 安全策略，选择 ESP，提供完整性。

在本机右击 AA 策略→选择“属性”→选中“AA 筛选器”→单击“筛选器操作”标签→选中之前创建的新筛选器操作→单击“编辑”→再次单击“编辑”→选择“仅保持完整性”→单击“确定”按钮→单击“应用”按钮→单击“确定”按钮→直至关闭窗口，至此本机修改完成。

第二步：修改 Windows XP 虚拟机 IPSec 安全策略，选择 ESP，提供完整性(步骤略)。

第三步：在本机浏览 Windows XP 虚拟机的网页，同时使用 Sniffer Pro 捕获、分析数据。

使用 Sniffer Pro 捕获的数据包如图 3-28 所示，从中可以清楚看到 IKE 协商过程和 ESP 的通信过程。

通过逐一查看 ESP 通信报文可以发现，报文携带的应用层数据没有进行加密，但每个报文都增加了 ESP 首部、ESP 尾部和鉴别数据，用于保证报文的完整性，如图 3-29 所示。

图 3-29 是 Windows XP 虚拟机发给本机的一个数据包，可见其包含 8 字节 ESP 首

部、9 字节 ESP 尾部和 12 字节鉴别数据。在 ESP 首部中 SPI 字段值为 0x5E961238，转换为十进制为 1586893368，SEQ 字段值为 22。在 ESP 尾部中前 7 个字节是填充项，填充数据长度字段为 7，协议字段值为 6 表明传输层采用 TCP。最后 12 字节的鉴别数据用于保证报文的完整性。从图 3-29 可见，HTTP 数据部分以明文方式传递。

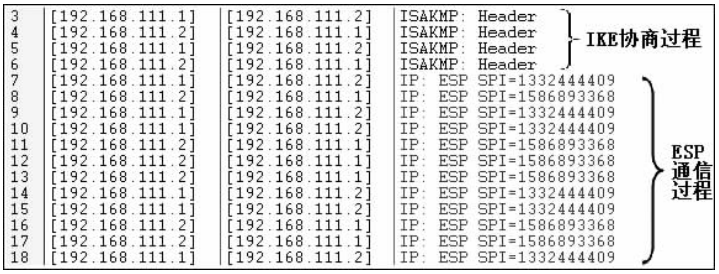


图 3-28　使用 Sniffer Pro 查看到的 IPSec 通信过程

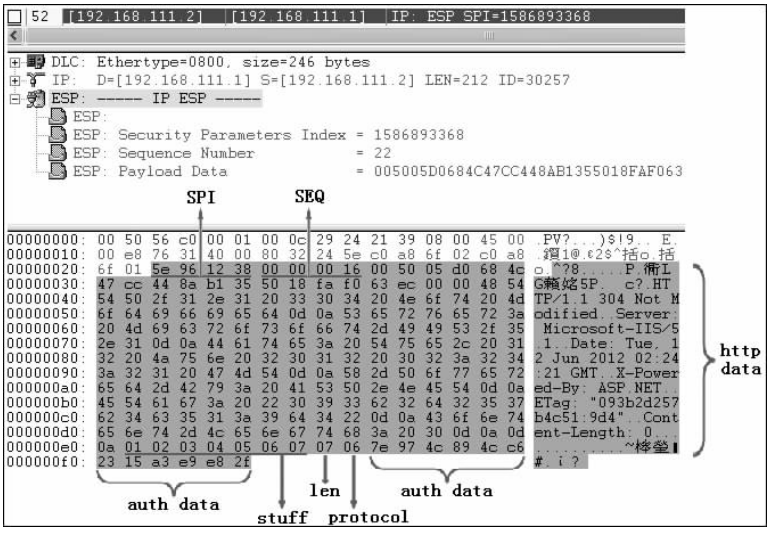


图 3-29　每个报文中都增加了 ESP 首部、ESP 尾部和鉴别数据

3.5.3　测试开通 IPSec 通道、选择 ESP、提供保密性和完整性

1. 测试环境

实验环境同 3.5.1 节，这里不再赘述。

2. 测试目的

在上一个实验的基础上修改 IPSec 通道，选择 ESP，提供保密性和完整性。使用 Sniffer Pro 捕获客户访问 Web 服务器过程中传输的数据包，通过分析捕获的数据，进一步理解 ESP 的格式和作用。

3. 测试步骤

第一步：修改本机 IPSec 安全策略，选择 ESP，提供保密性和完整性。

在本机右击 AA 策略→选择“属性”→选中 AA 筛选器→单击“筛选器操作”标签→选中之前创建的新筛选器操作→单击“编辑”→再次单击“编辑”→选择“加密并保持完整性”→单击“确定”按钮→单击“应用”按钮→单击“确定”按钮→直至关闭窗口，至此本机修改完成。

第二步：修改 Windows XP 虚拟机 IPSec 安全策略，选择 ESP，提供保密性和完整性。步骤略。

第三步：在本机浏览 Windows XP 虚拟机的网页，同时使用 Sniffer Pro 捕获、分析数据。

使用 Sniffer Pro 捕获的数据包如图 3-30 所示，从中可以清楚看到 IKE 协商过程和 ESP 的通信过程。

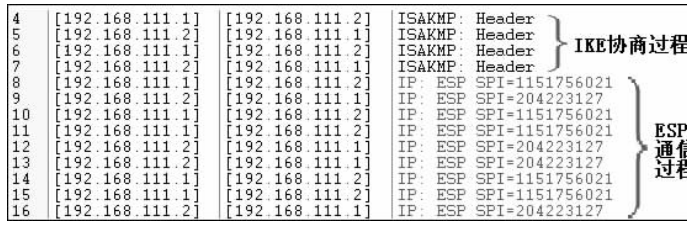


图 3-30　使用 Sniffer Pro 查看到的 IPSec 通信过程

通过逐一查看 ESP 通信报文可以发现，报文携带的应用层数据都进行了加密，图 3-31 是 Web 服务器发送给客户机的一个数据包，可见包含 8 字节的 ESP 首部，应用层数据都进行了加密。

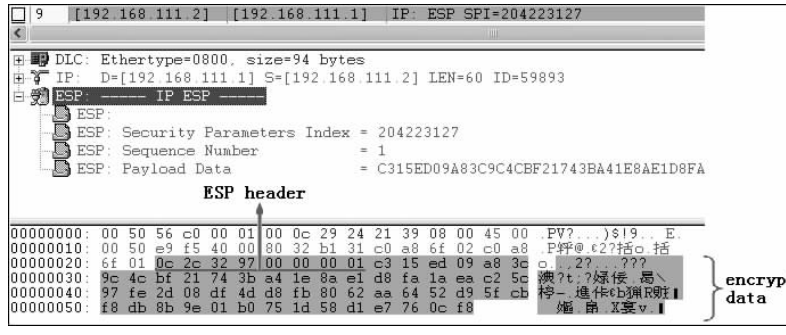


图 3-31　每个报文都进行了加密

思考题

1. IP 数据报在从源主机发送到目的主机的过程中，数据报中的源和目的 IP 地址如

何变化?

2. IP 首部的协议字段起什么作用?
3. 为什么 IP 校验和只涉及首部?
4. IP 首部中的 TTL 字段起什么作用?
5. IP 协议为什么设置分片和重组机制?
6. 网络地址转换(NAT)解决什么问题?
7. NAT 日志的作用是什么?

第 4 章 ARP 及 ARP 欺骗

4.1 地址解析协议 ARP

IP 地址和 MAC 地址都是主机的唯一标识，但 IP 地址在全世界范围内是唯一的，实现全网范围内主机到主机的通信。MAC 地址是在物理网络内唯一的，在全世界范围内不一定是唯一的，它实现了物理网络范围内主机到主机的通信。

因特网是由多个物理网络组成的。一个由源主机产生的 IP 数据报在其最终到达目的主机之前，可能会通过几个不同的物理网络。在 IP 数据报的整个传递过程中源和目的 IP 地址始终不变，而源和目的 MAC 地址在每个物理网络中都会发生变化。

如图 4-1 所示的网络环境标出了每台主机和路由器的接口 IP 及 MAC 地址，现分析主机 1 发送给主机 2 的 IP 数据报的传输过程。该数据报分三阶段传递，即先由主机 1 传给路由器 1，再由路由器 1 转发给路由器 2，最后由路由器 2 转发给主机 2。各个阶段数据报的 IP 及 MAC 地址配置情况如图 4-1 所示。通过分析可以发现，在传输过程中 IP 地址始终不变，实现了全网范围内定位主机，而 MAC 地址在不断发生变化。

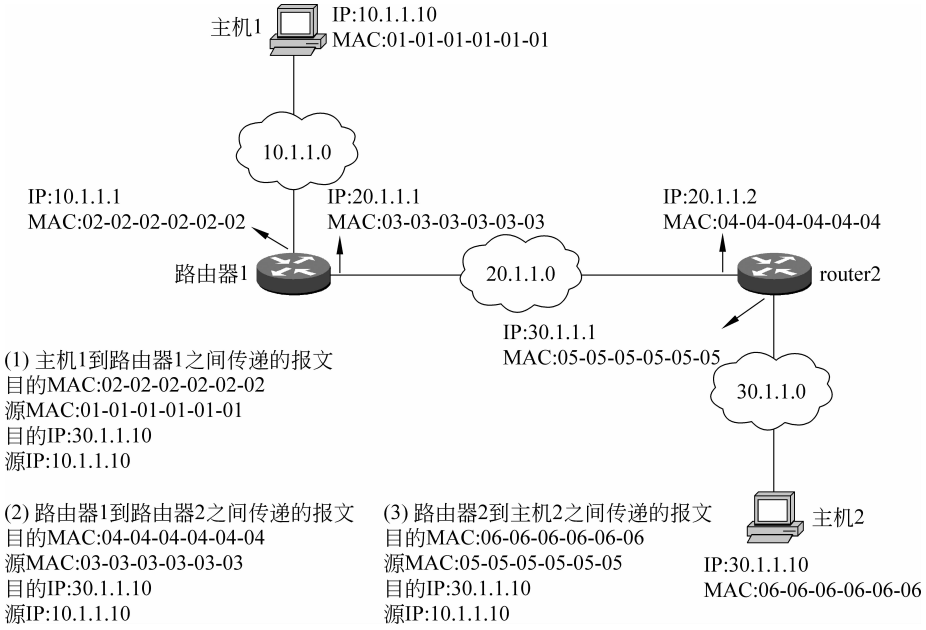


图 4-1　IP 数据报的传递过程