第5章

网络安全和监控

5.1 LAN 安全

LAN（Local Area Network，局域网）是指在有限的覆盖范围内将大量 PC 及各种设备互连在一起，实现高速数据传输和资源共享的计算机网络。局域网技术最早诞生于 20 世纪 60 年代的美国，发展过程中出现了许多局域网组网模型，如以太网、令牌环网等。其中，由施乐（Xerox）公司创建，并由 Xerox、Intel 和 DEC 公司联合开发的以太网（Ethernet）技术规范，是当今局域网中最常用的局域网组网标准。随着社会发展和计算机技术的广泛应用，局域网技术已经占据了十分重要的地位。

但是随着局域网使用的普及，局域网安全也受到了严重的威胁，如何防护局域网安全亟待解决。常见的局域网攻击主要发生在第二层，如 MAC 地址泛洪攻击、Telnet 漏洞攻击、CDP 侦察攻击以及 DHCP 相关的攻击等。

5.1.1 交换机端口安全

交换机的端口是连接网络终端设备的重要部分，加强交换机的端口安全是提高整个网络安全的关键。大部分网络攻击行为都采用 MAC 地址或源 IP 欺骗等方法，对网络核心设备进行连续的数据包攻击，最终耗尽网络核心设备系统资源而使系统崩溃。这些攻击行为大多可以通过事前启用交换机的端口安全功能来解决。

默认情况下，交换机的所有端口都是开放的，没有任何安全检查措施，允许到达的所有数据帧通过。因此，对交换机的端口增加安全访问机制，可以有效保护网络的安全，交换机的端口安全主要有以下两个功能。

（1）只允许特定的 MAC 地址的设备接入网络中，防止非法或者未授权的设备接入网络。当数据包的源 MAC 地址不是指定的 MAC 地址时，交换机端口不会转发这些数据包。

（2）通过限制交换机端口接入 MAC 地址的数量，防止因为接入过多的设备导致端口的不安全。默认情况下，交换机每个端口只允许一个 MAC 地址接入。

交换机主要依赖CAM表(包含MAC地址、对应的端口号、端口所属VLAN等信息)来转发数据帧。当数据帧到达交换机端口时,交换机首先提取其源MAC地址并检查CAM表中是否包含该地址。如果包含该MAC地址,交换机将把数据帧转发到该MAC地址所对应的端口上。如果不包含该地址,交换机将把数据帧转发到除收到该数据帧端口外的所有端口,同时将此MAC地址加入CAM表中。MAC泛洪攻击就是利用CAM表的大小有限这一特点,使用攻击工具发送大量无效的源MAC地址的数据帧给交换机,当CAM表被填满后,交换机将接收到的数据帧泛洪到所有端口。

配置交换机端口安全可以防止MAC泛洪攻击。当尝试访问交换机端口的设备违规时,可以采用如下三种处理模式进行惩罚。

(1) 保护(Protect):如果该端口的MAC地址条目超过最大数目或者与所配置的MAC地址不同,那么新的设备就无法接入。此种模式对已经接入的设备没有影响,同时交换机不发送警告信息,也不增加违规计数。

(2) 限制(Restrict):如果该端口的MAC地址条目超过最大数目或者与所配置的MAC地址不同,那么新的设备就无法接入。此种模式对已经接入的设备没有影响,但是交换机会发送警告信息,同时增加违规计数。

(3) 关闭(Shutdown):如果该端口的MAC地址条目超过最大数目或者与所配置的MAC地址不同,那么交换机端口将会关闭,且该端口下的所有设备都无法接入交换机,交换机也会发送警告信息,同时会增加违规计数。

实验5-1:配置交换机端口安全

1. 实验目的

(1) 理解端口安全的实现原理及接口配置方法。

(2) 掌握配置静态端口安全、动态端口安全的方法。

2. 实验拓扑

实验拓扑如图5-1所示。该实验在交换机的f0/1端口配置动态端口安全,在f0/2端口配置静态端口安全(注:一般服务器端配置静态端口安全)。

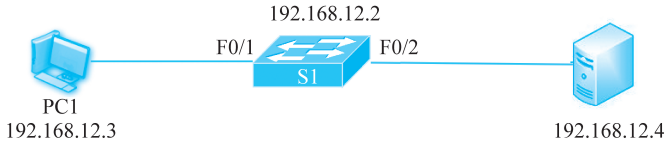

图5-1 交换机端口安全实验拓扑

3. 实验步骤

(1) 配置交换机S1。

```
S1(config)#interface vlan1
//配置交换机交换虚拟接口,对交换机进行远程管理。
S1(config-if)#ip address 192.168.12.2 255.255.255.0
S1(config-if)#no shutdown
S1(config)#ip default-gateway 192.168.12.1
```

```
//配置交换机默认网关。
S1(config)#interface range f0/1-2
S1(config-port-range)#speed-duplex auto
//配置以太网接口双工模式、速率。
S1(config)#interface range f0/3-24,g0/1,…
//禁用其他未使用的端口。
S1(config-port-range)#shutdown
```

（2）配置交换机静态端口安全。

```
S1(config)#interface f0/2
S1(config-if)#switchport port-security
//打开交换机的端口安全功能。
S1(config-if)#switchport port-security maximum 1
//只允许一台设备接入。
S1(config-if)#switchport port-security mac-address 00-00-00-00-00-01
//配置端口允许接入计算机的 MAC 地址,这里应该是服务器的 MAC 地址。
S1(config-if)#switchport port-security violation shutdown
//配置端口安全违规惩罚模式,默认 violation mode 是 shutdown。
```

（3）配置交换机动态端口安全。

```
S1(config)#interface f0/1
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security violation restrict
```

4. 实验调试

（1）用命令“show mac-address-table”在每一步查看交换机的 MAC 地址表变化。

（2）在步骤(2)配置完成后，用命令“show mac-address-table|include f0/2”把服务器的 MAC 地址静态加入 MAC 地址表，在 f0/2 接入其他终端，模拟非法接入，查看交换机信息。

（3）用命令“show port-security(show port-security address)”查看交换机端口安全信息。

5.1.2　DHCP 安全

通过第 4 章的学习，了解了 DHCP 的原理及其工作流程。在局域网内，通常会使用 DHCP 服务器为客户端分配 IP 地址，但是 DHCP 服务器没有验证服务。我们知道，客户端均是以广播的方式来发现 DHCP 服务器，并且只采用第一个响应的服务器提供的服务。

针对 DHCP 的原理，对其进行的攻击主要有以下两种。

（1）中间人攻击：如果在网络中存在一台非授权的 DHCP 服务器，并且它首先应答了客户端的请求，那么客户端最后获得的就可能是具有恶意的 IP 地址和网关等信息，而攻击者就可以使用这些信息实施中间人攻击。

(2) DHCP 耗竭攻击：攻击者会故意地向授权的 DHCP 服务器反复申请 IP 地址，最终导致授权的 DHCP 服务器消耗了地址池中的全部 IP 地址，致使合法的主机无法申请到 IP 地址。

中间人攻击和 DHCP 耗竭攻击通常一起使用，首先使用 DHCP 耗竭攻击耗尽地址池中所有的 IP 地址，然后客户端不得不从非授权的 DHCP 服务器申请到带有恶意的 IP 地址，进行中间人攻击。

DHCP Snooping 是 DHCP 的安全特性，一般作用在交换机上，它可以使网络中的客户端只能从管理员指定的 DHCP 服务器获取 IP 地址，达到屏蔽接入网络中的非法 DHCP 服务器的目的。DHCP Snooping 首先监听并截获交换机端口的 DHCP 响应数据包，然后提取其中的关键信息并生成 DHCP Binding Table 记录表，表中包含客户端主机 MAC 地址、IP 地址、租用期、VLAN ID、交换机端口等。

启用 DHCP Snooping 功能后，交换机上的端口将被设置为信任(Trust)和非信任(Untrust)状态，交换机只转发信任端口的 DHCP Offer/ACK/NAK 报文，当交换机从一个不可信任端口接收到 DHCP 服务器响应的数据包时，交换机会直接将该数据包丢弃，从而阻断非法 DHCP 服务器。一般将连接 DHCP 服务器的端口设置为信任端口，连接客户端的端口设置为非信任端口，这样就可以有效地阻止中间人攻击和 DHCP 耗竭攻击。

实验 5-2：DHCP Snooping

1. 实验目的

(1) 理解 DHCP 攻击的原理。

(2) 理解 DHCP Snooping 的实现原理及接口配置方法。

(3) 掌握 DHCP Snooping 的配置方法。

2. 实验拓扑

实验拓扑如图 5-2 所示。该实验在交换机的 f0/1 端口配置 DHCP 不受信任端口，在 f0/2 端口配置 DHCP 受信端口(服务器开启 DHCP 服务)。

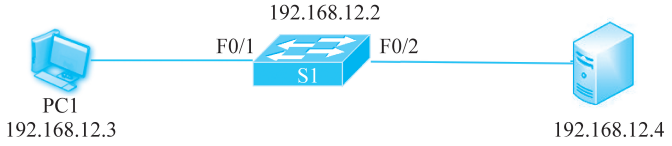

图 5-2　交换机 DHCP Snooping 实验拓扑

3. 实验步骤

(1) 配置交换机 S1。

```
S1(config)#interface vlan 1
//配置交换机交换虚拟接口,对交换机进行远程管理。
S1(config-if)#ip address 192.168.12.2 255.255.255.0
S1(config-if)#no shutdown
S1(config)#ip default-gateway 192.168.12.1
//配置交换机默认网关。
```

```
S1(config)#interface range f0/1-2
S1(Config-Port-Range)#speed-duplex auto
//配置以太网接口双工模式、速率。
S1(config)#interface range f0/3-24,g0/1,…
//禁用其他未使用的端口。
S1(Config-Port-Range)#shutdown
```

（2）全局开启 DHCP Snooping 功能。

```
S1(config)#ip dhcp snooping enable
```

（3）配置交换机 DHCP 的 trust 端口。

```
S1(config)#interface ethernet f0/2
S1(config-if)#ip dhcp snooping trust
```

（4）配置交换机 DHCP 的非 trust 端口，检测到 DHCP 报文后所触发的行为。其他端口已经关闭，不必配置。

```
S1(config)#interface ethernet f0/1
S1(config-if)#ip dhcp snooping action shutdown
```

4. 实验调试

（1）正常情况下，PC1 能够获取 IP。

（2）如果把两个设备互连接口换一下，PC1 接 F0/2，服务器接 F0/1，PC1 不能够获取 IP，在交换机查看发现 F0/1 接口被 shutdown。

（3）一般来说，DHCP 服务器是在其他区域，因此接入交换机上连到汇聚或核心层设备的端口需要配置为 DHCP 信任端口。

（4）可以使用“debug ip dhcp snooping”命令来监控调试信息。

（5）新型号的交换机还支持 ARP inspecting 功能，具体实践中两个功能共同使用，可以防止 DHCP 和 ARP 攻击，效果更好。

5.2　SNMP

简单网络管理协议（Simple Network Management Protocol，SNMP）是应用层协议，用于 IP 网络结点管理。SNMP 可以帮助网络管理员监控和管理网络性能，发现并解决网络问题以及规划网络增长。

SNMP 主要由 3 部分组成，分别是网络管理工作站（Network Management Station，NMS）、SNMP 代理（Agent）和管理信息库（Management Information Base，MIB）。

（1）NMS：指运行 SNMP 管理软件的计算机。可以通过 SNMP 代理 MIB 中读取信息，也可以把命令发送给 SNMP 代理去执行。

（2）Agent：指运行在网络设备上的 SNMP 代理软件。当 Agent 接收到 NMS 的请

求后,可以根据包类型进行读写操作,并生成响应返回给 NMS;当设备发生异常或者状态改变时,Agent 主动发送 Trap 信息给 NMS。

(3) MIB:一种树状数据库,存储与设备和操作信息有关的数据,是管理对象的集合。MIB 管理的对象,就是树的末端结点,每个结点有唯一的标识,即管理信息库对象识别符(Object Identifier,OID)。

SNMP 具有三个常见版本,分别是 SNMPv1、SNMPv2 和 SNMPv3。在 SNMPv3 版本中提供了认证和加密安全机制,增强了安全性。

实验 5-3:SNMP

1. 实验目的

(1) 理解 SNMP 的原理,理解 MIB 工作机制。

(2) 掌握配置 SNMP,通过 SNMP 对交换机或路由器的管理方法。

(3) 了解通过交换机配置 SNMP,服务器安装网络管理软件,从而进行大型网络管理。

2. 实验拓扑

实验拓扑如图 5-3 所示。该实验在交换机的 f0/1 端口连接一台 PC1,PC 上运行 SNMP 测试软件验证配置。

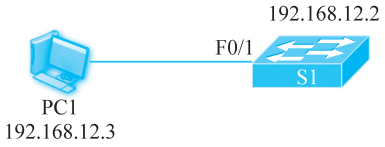

图 5-3 交换机 SNMP 实验拓扑

3. 实验步骤

(1) 配置交换机 S1。

```
S1(config)#interface vlan 1
//配置交换机交换虚拟接口,对交换机进行远程管理。
S1(config-if)#ip address 192.168.12.2 255.255.255.0
S1(config-if)#no shutdown
S1(config)#ip default-gateway 192.168.12.1
//配置交换机默认网关。
S1(config)#interface f0/1
S1(config-if)#speed-duplex auto
//配置以太网接口双工模式、速率。
S1(config)#interface range f0/2-24,g0/1,…
//禁用其他未使用的端口。
S1(Config-Port-Range)#shutdown
```

(2) 打开交换机作为 SNMP 代理服务器功能。

```
S1(config)#snmp-server enable
```

（3）配置交换机 SNMP 团体字符串，用 private 作为团体字符串对交换机进行可读写的访问，也可以使用 public 作为团体字符串对交换机进行只读的访问。

```
S1(config)#snmp-server community rw private
S1(config)#snmp-server community ro public
```

4. 实验调试

（1）在 PC1 上配置 IP 地址为 192.168.12.2，配置 SNMP 软件（本实验使用了 Paessler SNMP Tester 这款免费软件），首先填入要访问的设备 IP 地址，以及团体字符串，单击 Start 按钮开始测试，如图 5-4 所示。

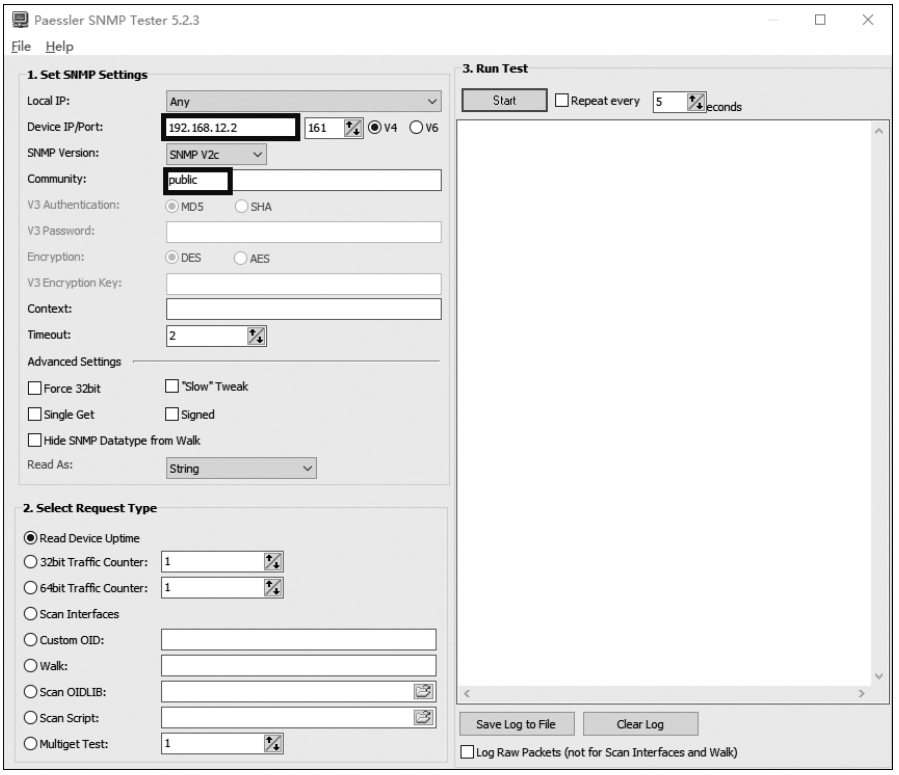

图 5-4　测试

（2）在右侧输入界面查看结果，如图 5-5 所示。

```
SNMP V2c
Uptime
: SNMP Datatype: ASN_TIMETICKS
: -------
: DISMAN-EVENT-MIB::sysUpTimeInstance = 1499545815 ( 173 days )
: SNMP Datatype: SNMP_EXCEPTION_NOSUCHOBJECT
: HOST-RESOURCES-MIB::hrSystemUptime.0 = No such object (SNMP error # 222) ( 0 seconds )
: Done
```

图 5-5　查看结果

从图 5-5 可以看出，本设备已经运行了 173 天。

（3）在软件中更改团体字符串为“private”查看结果。

(4) 在软件中更改 Request Type 选项卡选项,查看结果。

(5) 在交换机配置“snmp-server enable traps”“snmp-server host 192.168.12.2”,PC1 上安装 OpenNMS 软件,通过 PC1 的 Web 浏览器访问 NMS(网络管理软件)服务,来管理交换机。

5.3 VPN

虚拟专用网络(VPN)的功能是在公用网络上建立专用网络,进行加密通信,属于远程访问技术。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。

VPN 隧道协议主要有 3 种:PPTP、L2TP 和 IPSec。其中 PPTP 和 L2TP 工作在 OSI 模型的第二层,又称二层隧道协议;IPSec 是三层隧道协议。

VPN 可通过多种方式实现,常用的有以下 4 种。

(1) VPN 服务器:在大型局域网中,可以通过在网络中心搭建 VPN 服务器的方法实现。

(2) 软件 VPN:可以通过专用的软件实现 VPN。

(3) 硬件 VPN:可以通过专用的硬件实现 VPN。

(4) 集成 VPN:某些硬件设备,如路由器、防火墙等,都含有 VPN 功能。

VPN 数据包的一般处理过程为:首先,受保护主机发送明文信息到 VPN 设备;然后,VPN 设备根据网络管理员设置的规则,对数据进行加密或者直接传输,如果需要加密,VPN 设备将整个数据包加密并进行数据签名,加上新的数据包头重新封装;最后,将封装后的数据包通过隧道在公共网络上传输。


实验 5-4 视频

实验 5-4:VPN 配置

1. 实验目的

(1) 理解虚拟专用网的实现原理、协议和结构。

(2) 掌握利用 PPTP(点对点隧道协议)配置 VPN 的方法。

2. 实验拓扑

在 Windows 2003 Sever 中 VPN 服务称为“路由和远程访问”,默认状态下已经安装,但需要对此服务进行必要的配置使其生效。实验拓扑如图 5-6 所示。

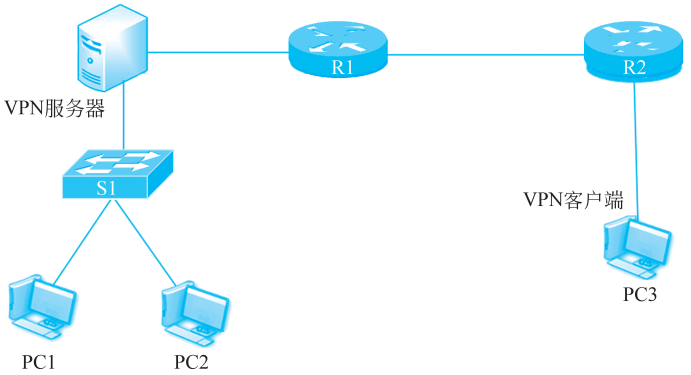

图 5-6 VPN 实验拓扑

3. 实验步骤

(1) VPN 服务器配置。

在服务器端,依次选择“开始”→“所有程序”→“管理工具”→“路由和远程访问”,打开“路由和远程访问”服务窗口,如图 5-7 所示;再在窗口中右击服务器名,在弹出的菜单中选择“配置并启用路由和远程访问”命令,出现“路由和远程访问服务器安装向导”对话框,如图 5-8 所示,单击“下一步”按钮。

图 5-7　配置并启用路由和远程访问

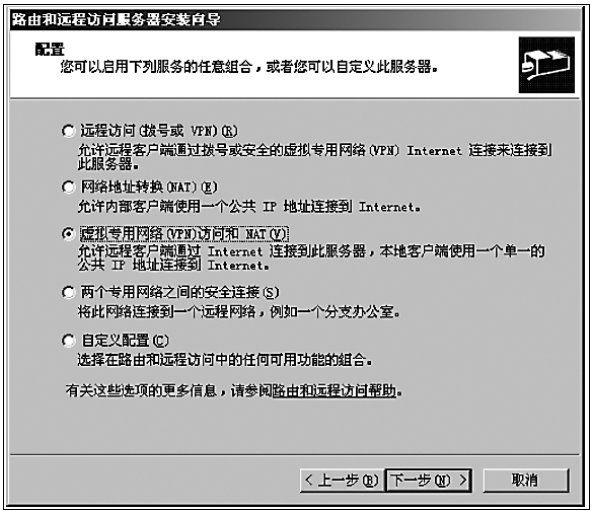

图 5-8　“路由和远程访问服务器安装向导”对话框

在“路由和远程访问服务器安装向导”对话框中,选中“虚拟专用网络(VPN)访问和 NAT(V)”单选按钮,单击“下一步”按钮;然后在 VPN 访问所需协议对话框中选择或添加 VPN 访问所需的协议,如果已经包含所需要的协议,则单击“下一步”按钮,本实验使用的是 TCP/IP。之后,系统对客户端进行配置,一般采用默认值,单击“下一步”按钮。选择通过 VPN 服务器的哪块网卡进行网络连接,并选中指定的网络连接。

下面为 VPN 客户端指定想要使用的网络,在选择客户端 IP 地址指定方式的界面中,选择“来自一个指定的地址范围”单选按钮,如图 5-9 所示。客户端连接到 VPN 服务器时,服务器将为客户端指派一个 IP 地址。如果 VPN 服务器能够连接到网络中的 DHCP 服务器来得到 IP 地址,则选择“自动”方式;如果网络中没有 DHCP 服务器,则由 VPN 服务器指定一个地址范围。为了让客户端和服务器能够在同一个网段,这台服务器将会指派所有第一个范围内的地址。指派的 IP 地址一般为内部网络中的专用 IP 地址。在“地址范围指定”对话框中,输入起始 IP 地址、结束 IP 地址和范围内的 IP 地址数目,如图 5-10 所示。采用 DHCP 动态 IP 的网络速度相对较慢,而使用静态 IP 可减少 IP 地址的解析时间,因此网络速度较快。

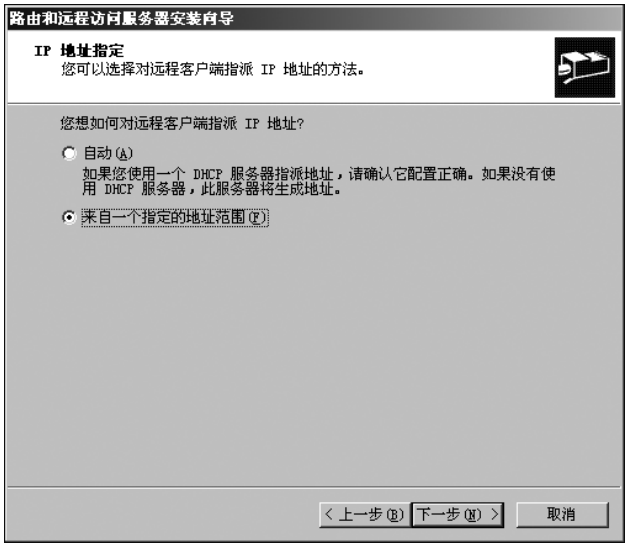

图 5-9 选择地址获取方法

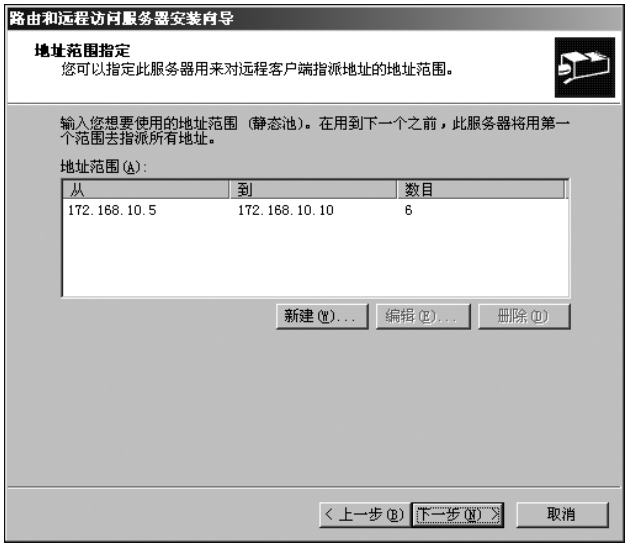

图 5-10 设定地址范围