第4章
虚拟专用网络(VPN)技术

中国科学技术大学
曾凡平
billzeng@ustc.edu.cn

主要内容

1. 概述
   - VPN的功能和原理
   - VPN的分类
2. 基于第2层隧道协议的PPTP VPN和L2TP VPN
3. 基于第3层隧道协议的IPSec VPN
   - IPSec的组成和工作模式
   - 认证协议AH
   - 封装安全载荷ESP
   - 安全关联与安全策略
4. Windows环境下的VPN

4.1 概述

- VPN（Virtual Private Network）即“**虚拟专用网络**”，是企业网在互联网(或其他公共网络)上的扩展。
- VPN在互联网上开辟一条**安全的隧道**，以保证两个端点（或两个局域网）之间的**安全通信**。
- VPN构建于廉价的互联网之上，可以实现远程主机与局域网(内网)之间的安全通信，也可以实现任何两个局域网之间的安全连接。

- Microsoft Windows和Linux的任何一个版本都可以用作VPN客户端，Windows Server 以及Linux的服务器版本均可以配置为VPN服务器。因此，从经济性和安全性考虑，VPN是企业实现安全通信的一个很好的选择。

4.1.1 VPN的功能和原理

- **VPN的功能是将互联网虚拟成路由器，将物理位置分散的局域网和主机虚拟成一个统一的虚拟企业网。**

- VPN综合利用了隧道技术、加密技术、鉴别技术和密钥管理等技术，在公共网络之上建立一个虚拟的安全通道，实现两个网络或两台主机之间的安全连接。

- 图1所示的是企业使用VPN的两种典型模式。

图1 (a) 远程用户访问企业内网

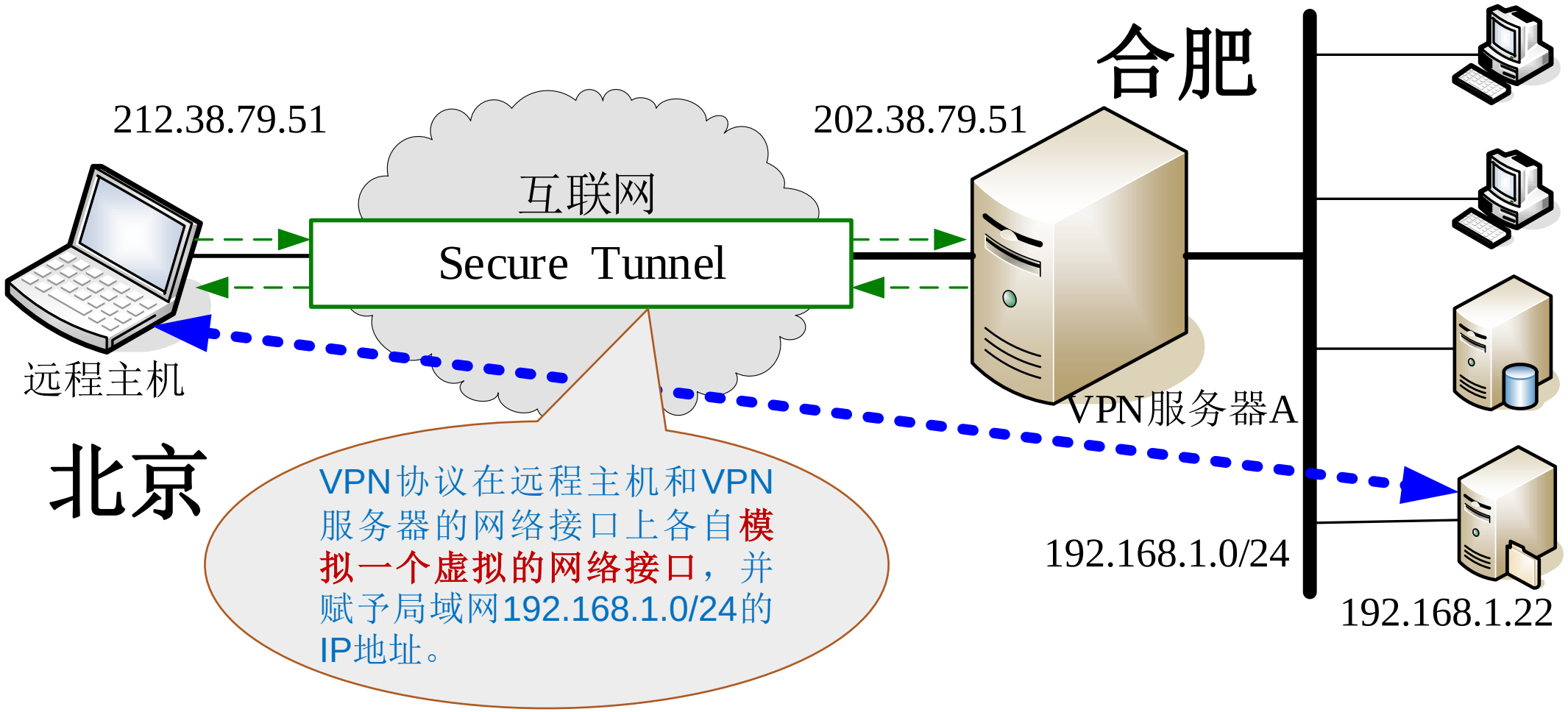


图1 (a) 远程用户访问企业内网

图1(b) 企业分支机构之间的局域网互联

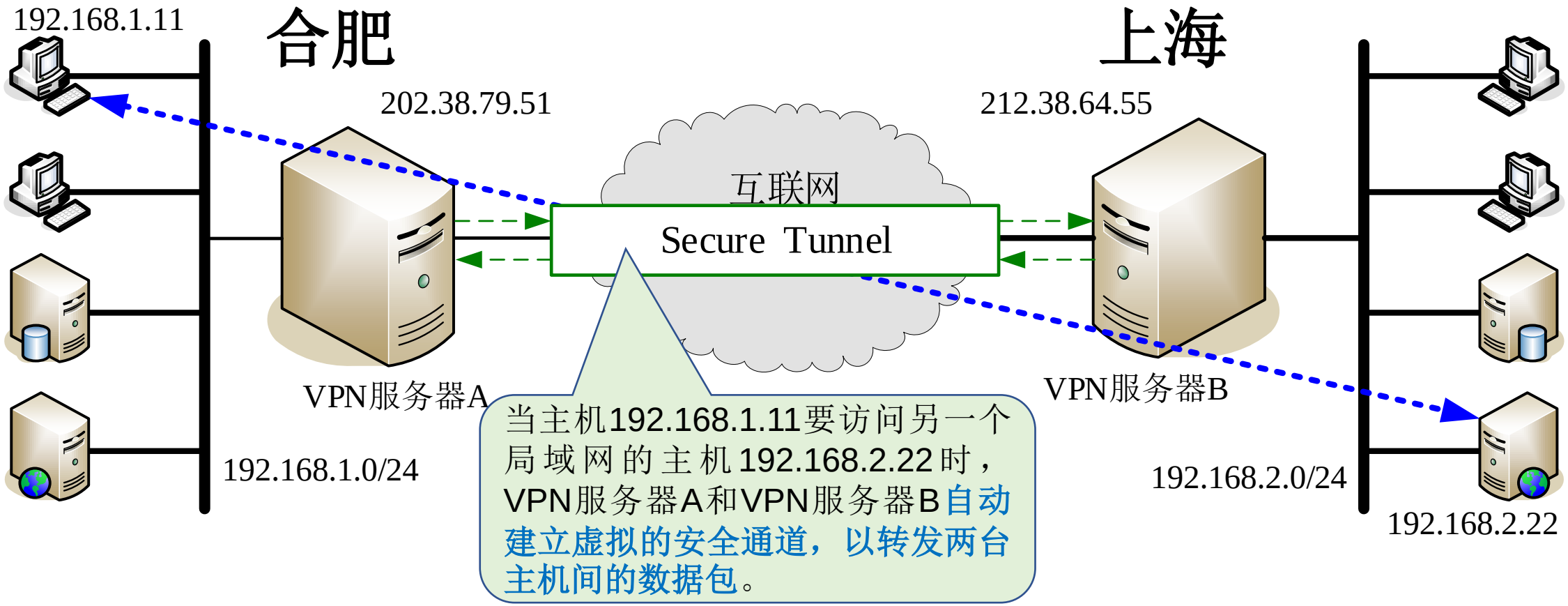


图1(b) 企业分支机构之间的局域网互联

图2 VPN将互联网虚拟成一个路由器

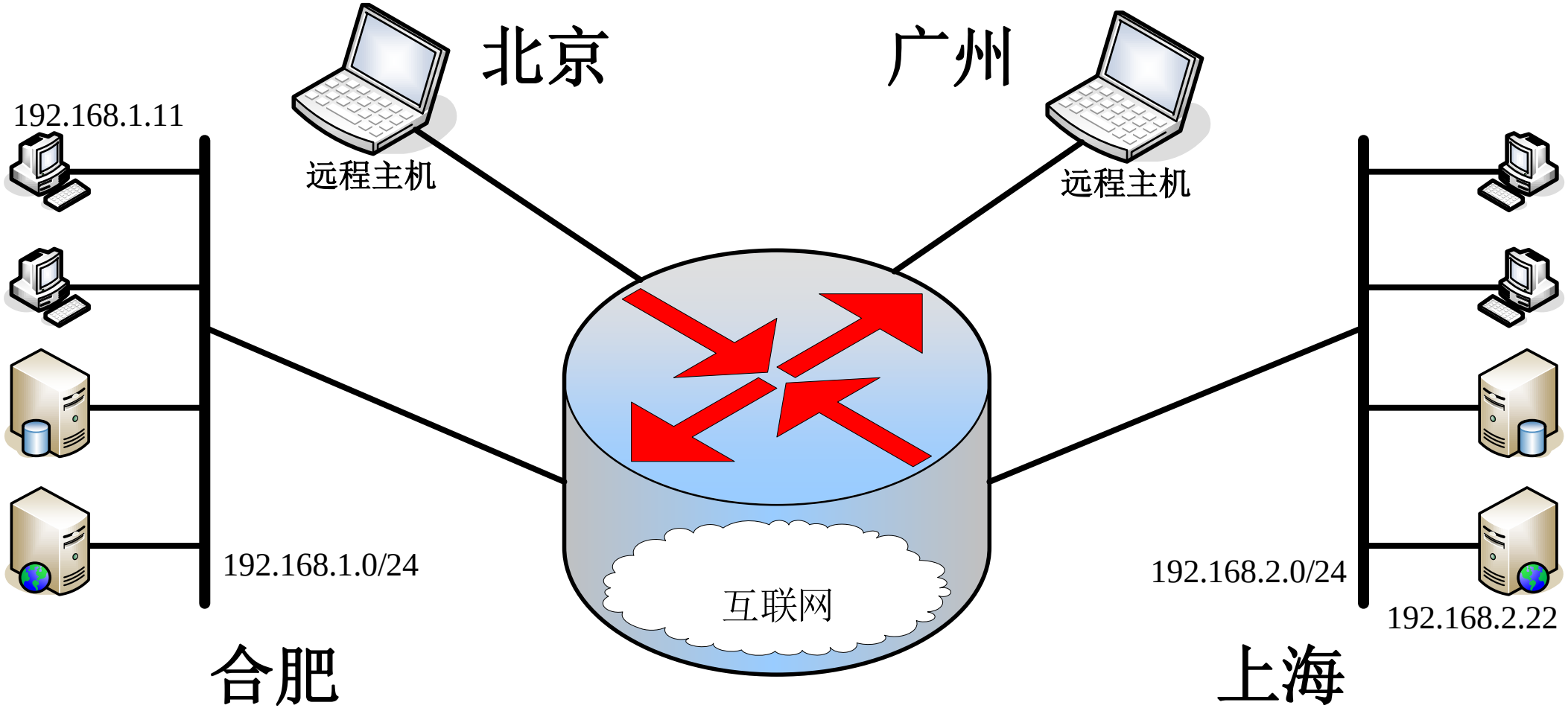


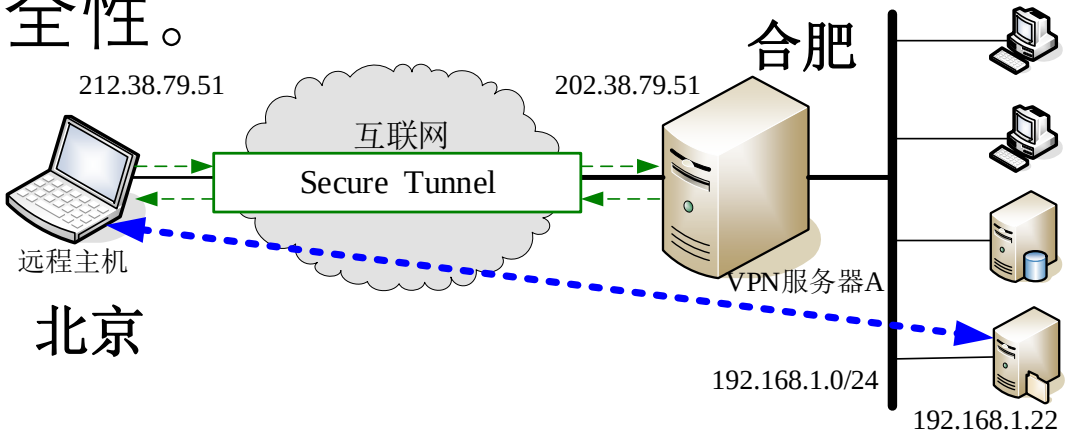
图2 VPN将互联网虚拟成一个路由器

4.1.2 VPN的分类

- 根据应用场合，从应用的观点，VPN可以大致分为二类：远程访问VPN和网关—网关VPN。

(1) 远程访问VPN

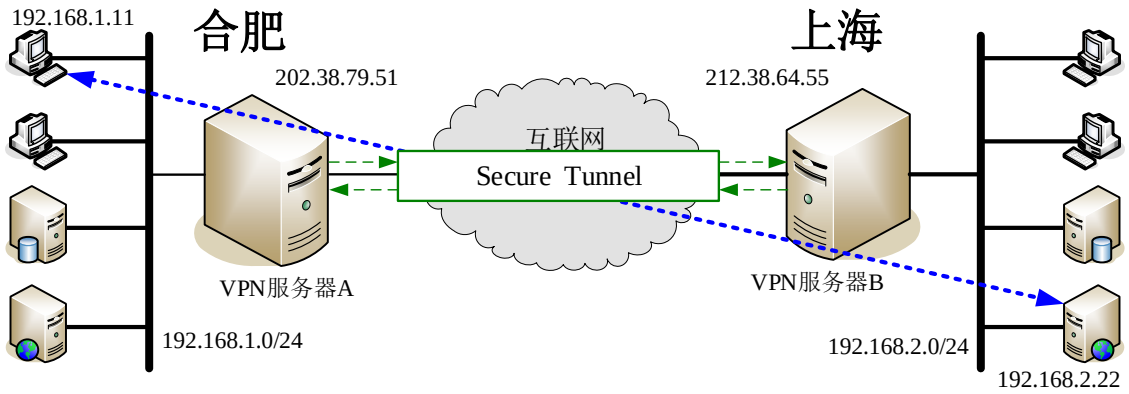
- 它是为企业员工从外地访问企业内网而提供的VPN解决方案，如图1(a)所示。
- 当公司的员工出差到外地需要访问企业内网的机密信息时，为了避免信息传输过程中的泄密，他们的主机首先以VPN客户端的方式连接到企业的远程访问VPN服务器，此后远程主机到内网主机的通信将加密，从而保证了通信的安全性。



从应用的观点分类

(2) 网关—网关VPN

- 也称为**“网络—网络VPN”**，如图1(b)所示。
- 这种方案**通过不安全的互联网实现两个或多个局域网的安全互联**。在每个局域网的出口处设置VPN服务器，当局域网之间需要交换信息时，两个VPN服务器之间建立一条安全的隧道，保证其中的通信安全。
- 这种方式适合企业各分支机构、商业合作伙伴之间的网络互联。



按隧道协议分类

- **隧道协议（Tunneling Protocol）**是一个网络协议的载体。使用隧道的原因是在不兼容的网络上传输数据，或在不安全网络上提供一个安全路径。
- 隧道协议可能使用数据加密技术来保护所传输的数据。

- 隧道协议实现在OSI模型或TCP/IP模型的各层协议栈。根据VPN协议在OSI（7层）模型的实现层次，VPN大致可以分为：
  - 第2层隧道协议
  - 第3层隧道协议
  - 第4层隧道协议
  - 以及基于第2、3层（2.5层）隧道协议(MPLS)之间的VPN。

按隧道协议分类

(1) 第2层隧道协议

- 主要包括点到点隧道协议(PPTP)、第二层转发协议(L2F)、第2层隧道协议(L2TP)。主要用于实现**远程访问VPN**。

(2) 第3层隧道协议

- 主要是IP安全(IPSec)，用于在网络层实现数据包的安全封装。
- IPSec主要用于实现**网关—网关VPN**，也可实现**主机—主机**的安全连接。

(3) 第4层隧道协议(SSL)

- 在传输层上实现数据的安全封装，主要用于保护两台主机的两个进程间的安全通信。安全的Web、安全的电子邮件等均使用了第4层隧道协议。

(4) 基于第2、3层隧道协议

- 也称为2.5层隧道协议，是利用MPLS路由器的标签特性实现的VPN。

隧道协议与OSI分层协议模型

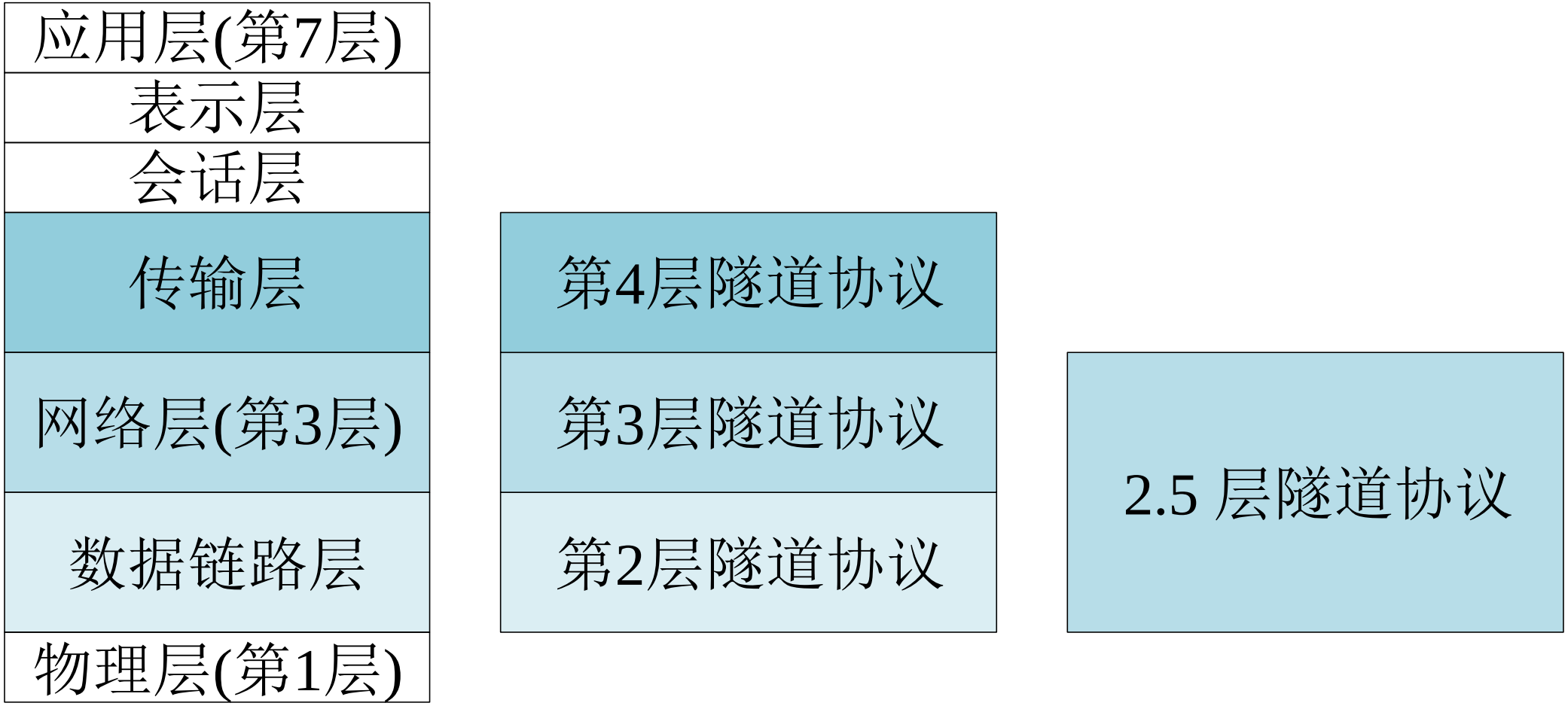


图3 隧道协议与OSI分层协议模型

4.2 基于第2层隧道协议的VPN

- 第2层隧道协议在数据链路层对数据报进行封装，**主要用于远程访问VPN**。
- 目前常用的有点到点隧道协议(PPTP)、第2层转发协议(L2F)、第2层隧道协议(L2TP)。

4.2.1 PPTP VPN

- **点对点隧道协议（Point to Point Tunneling Protocol，缩写为PPTP）**是实现虚拟专用网（VPN）的方式之一。PPTP使用传输控制协议（TCP）创建**控制通道**来传送控制命令，以及利用通用路由封装（GRE）通道（**数据通道**）来封装点对点协议（PPP）数据包以传送数据。

- 这个协议最早由微软等厂商主导开发，但因为它的早期版本加密方式容易被破解，微软已经不再建议老版本的Windows系统使用这个协议。

- **新版本的Windows系统已经对安全进行了增强，安全性能有保障，可以使用**。

PPTP协议

- PPTP的协议规范本身并未描述加密或身份验证的部份，它依靠点对点协议（PPP）来实现这些安全性功能。
- 因为PPTP协议内置在微软Windows家族的各个产品中，在微软点对点协议（PPP）协议堆栈中，提供了各种标准的身份验证与加密机制来支持PPTP。
- 在微软Windows中，它可以搭配PAP、CHAP、MS-CHAP v1/v2或EAP-TLS来进行身份验证。通常也可以搭配微软点对点加密（MPPE）或 IPSec 的加密机制来提高安全性。
- 在Windows或Mac OS平台之外，Linux与FreeBSD等平台也提供开放源代码的版本。

PPTP协议

- PPTP是由微软、Ascend Communications（现在属于Alcatel-Lucent集团）、3Com等厂商联合形成的产业联盟开发。1999年7月出版的 **RFC 2637**是第一个正式的PPTP规格书。
- PPTP以通用路由封装（GRE）协议向对方作一般的点对点传输，通过**TCP 1723端口**来发起和管理GRE状态。因为PPTP需要2个网络状态，因此会对穿越防火墙造成困难。很多防火墙不能完整地传递连接，导致无法连接。
- 在Windows或Mac OS平台，通常PPTP可搭配MSCHAP-v2或EAP-TLS进行身份验证，也可配合微软点对点加密（MPPE）进行连接时的加密。

PPTP帧的封装格式

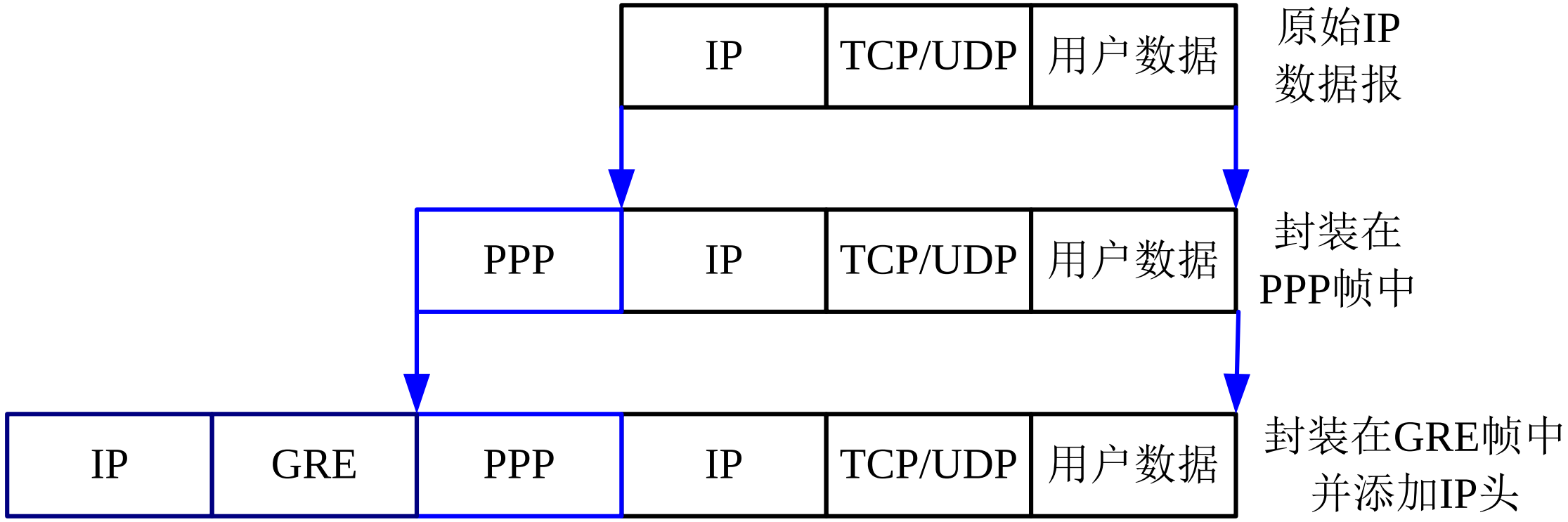


图4 PPTP帧的封装格式

注：GRE协议，IP头中的协议字段为47。

PPTP的实现

- PPTP因为易于设置和使用而流行。自Microsoft Windows 95 OSR2开始的Windows系统包含PPTP客户端，而自Windows NT开始的服务器版本在其**“路由和远程访问服务”**中实现了VPN服务。

- 以往，Linux缺乏完整的PPTP支持，这是因为MPPE是软件专利。
- 但是，自从在2005年10月28日发布的Linux 2.6.14开始，Linux核心提供完整的PPTP支持（包含对MPPE的支持）。

4.2.2 L2TP VPN

- 第二层隧道协议（Layer Two Tunneling Protocol，缩写为L2TP）是一种由RFC 2661定义的数据链路层隧道协议，是一种虚拟隧道协议，通常用于虚拟专用网。
- 互联网工程任务组于1999年8月发布RFC 2661，制定了L2TP协议的标准。
- 2005年，互联网工程任务组发布RFC 3931，制定了该协议标准的新版本——L2TPv3。
- 与L2TP相关的最新RFC为2009年6月发布的RFC 5571。

L2TP协议

- L2TP协议自身不提供加密与可靠性验证的功能，可以和安全协议搭配使用，从而实现数据的加密传输。经常与L2TP协议搭配的加密协议是IPsec，当这两个协议搭配使用时，通常合称L2TP/IPsec。

- L2TP支持包括IP、ATM、帧中继、X.25在内的多种网络。在IP网络中，L2TP协议使用了**UDP 1701**端口。因此，在某种意义上，尽管L2TP协议的确是一个数据链路层协议，但在IP网络中，它又的确是一个会话层协议。

4.2.3 基于第2层隧道协议的VPN实例

用Windows Server实现远程访问VPN

- 基于第2层隧道协议的PPTP VPN用于实现主机到企业内网的远程访问。PPTP VPN由PPTP VPN客户端和PPTP VPN 服务器组成。
- Windows 系统的桌面版本如Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10以及Windows 的服务器版本均包含了PPTP VNP 客户端软件，而Windows 的服务器版本包含了PPTP VPN 服务器软件。
- 在此以Windows Server 2003为例说明PPTP VPN的配置及使用方法。

远程访问VPN的架构

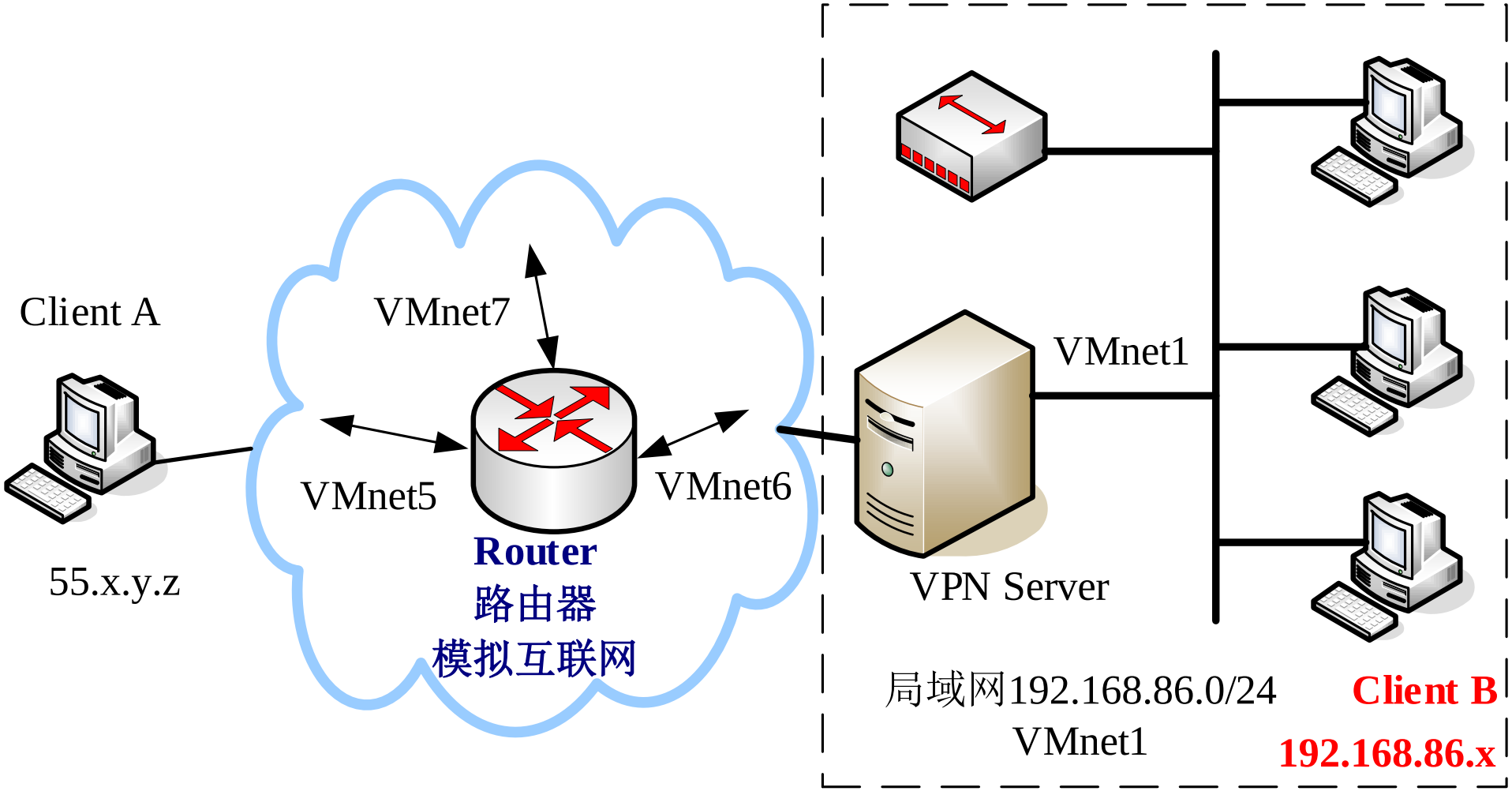
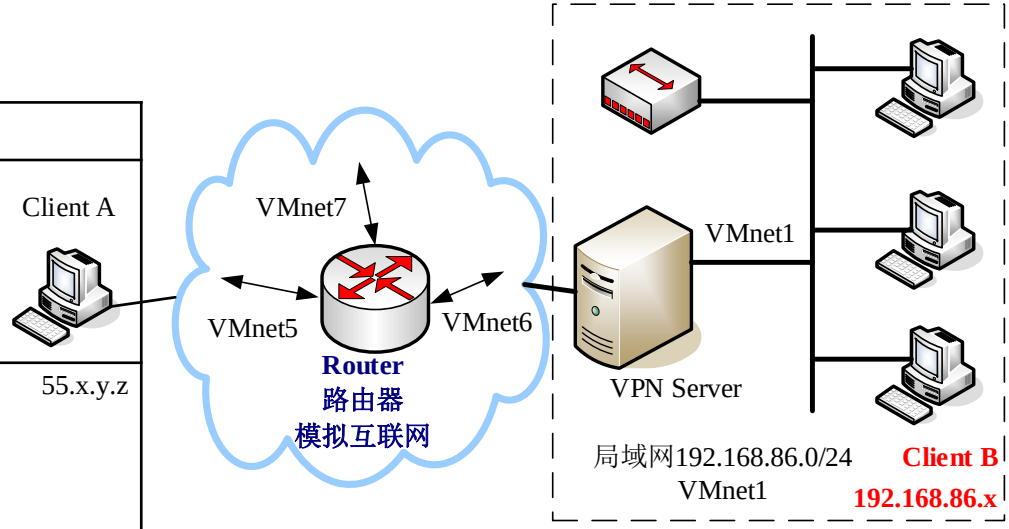


图9 远程访问VPN的架构

表1 虚拟机的配置

机器名	系统及必备软件	虚拟网络	IP地址信息
Client A	Windows 2003	VMnet5	IP: 自动获取 GateWay: **???**
Client B	Windows 2003	VMnet1	IP: 自动获取
VPN Server	Windows Server 2003	VMnet1 VMnet6	IP:自动获取 IP:166.66.66.**203** Subnet Mask: 255.255.0.0 GateWay: **???**
Router	Windows Server 2003 安装了Wireshark软件 http://www.wireshark.org/	VMnet5 VMnet6 VMnet7	IP: 55.55.55.**233** Subnet Mask: 255.0.0.0 IP: 166.66.66.**233** Subnet Mask: 255.255.0.0 IP: 217.77.77.**233** Subnet Mask: 255.255.255.0



准备4个Windows2003虚拟机：
下载VPN实验用的虚拟机，然后复制，更改配置。

2023秋季学期Windows2003虚拟机下载链接：
https://rec.ustc.edu.cn/share/9e308ea0-14e0-11eb-a3ab-2bdddfc577ff
密码：7frl

(1) 配置路由器Router

VMnet5	IP: 55.55.55.233 Subnet Mask: 255.0.0.0
VMnet6	IP: 166.66.66.233 Subnet Mask: 255.255.0.0
VMnet7	IP: 217.77.77.233 Subnet Mask: 255.255.255.0

图10 选用“路由和远程访问”

打开“路由和远程访问”管理界面

图11 “路由和远程访问”管理界面

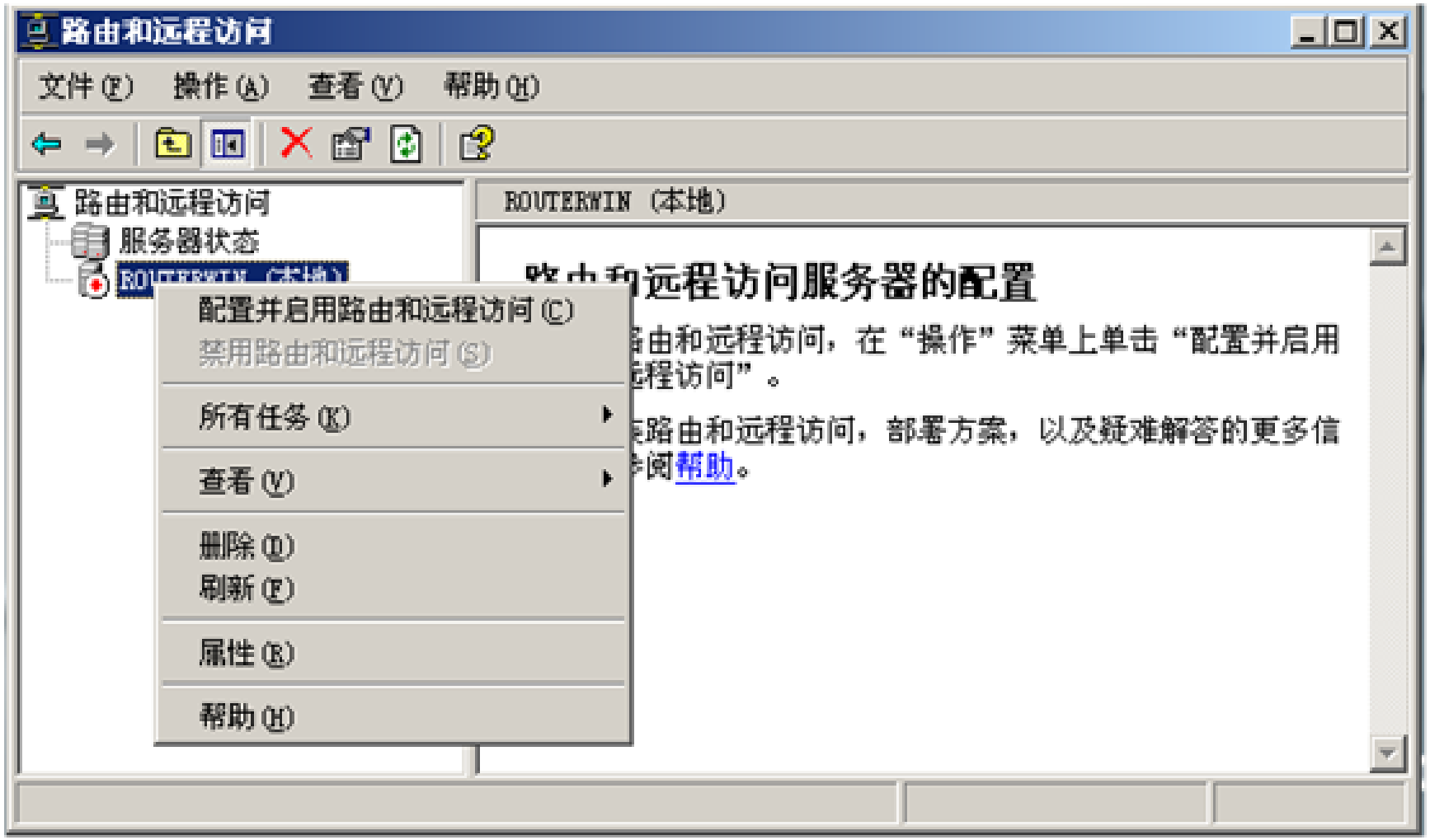


图12 选择“配置并启用路由和远程访问”

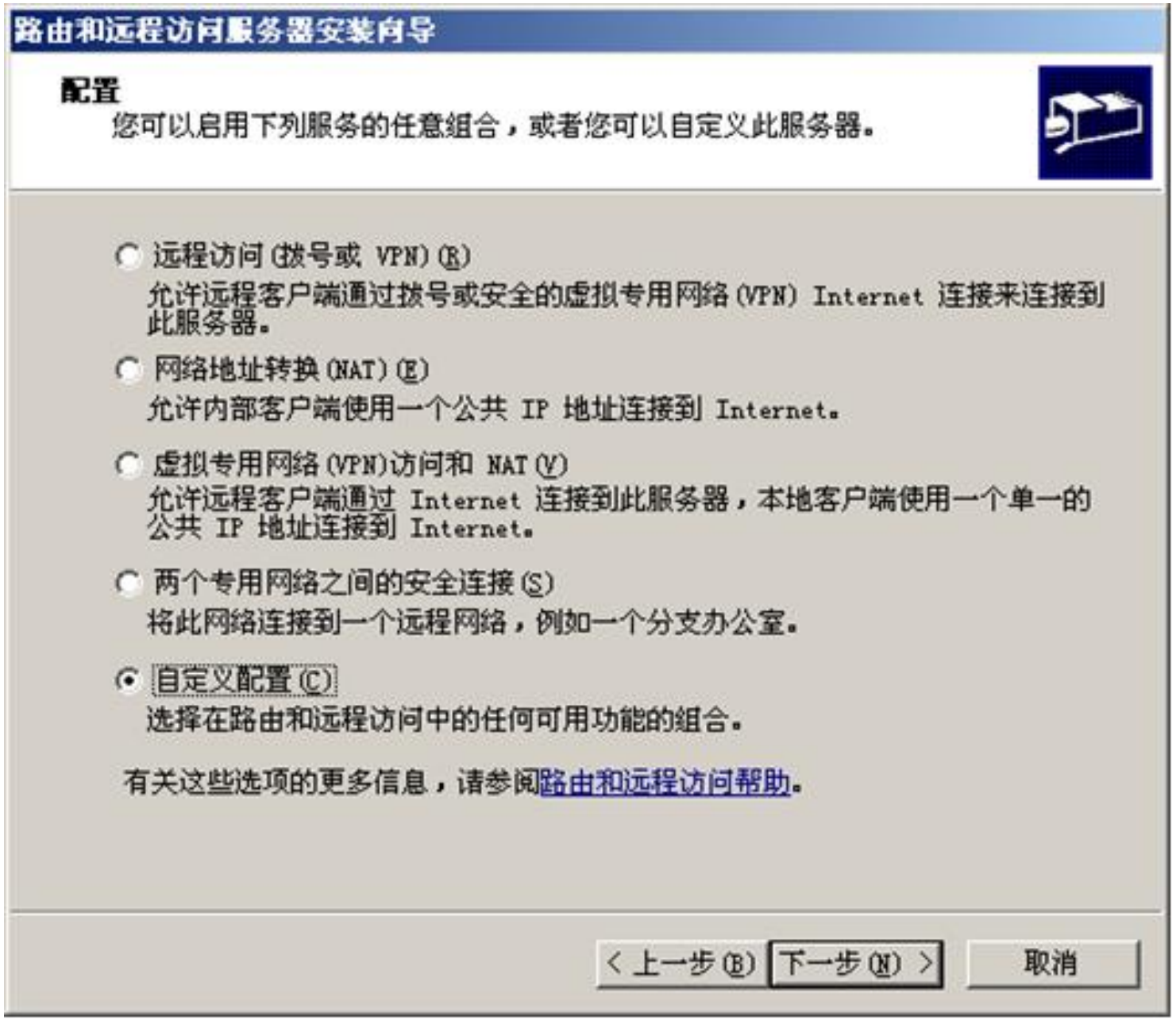


图13 路由和远程访问服务器安装向导

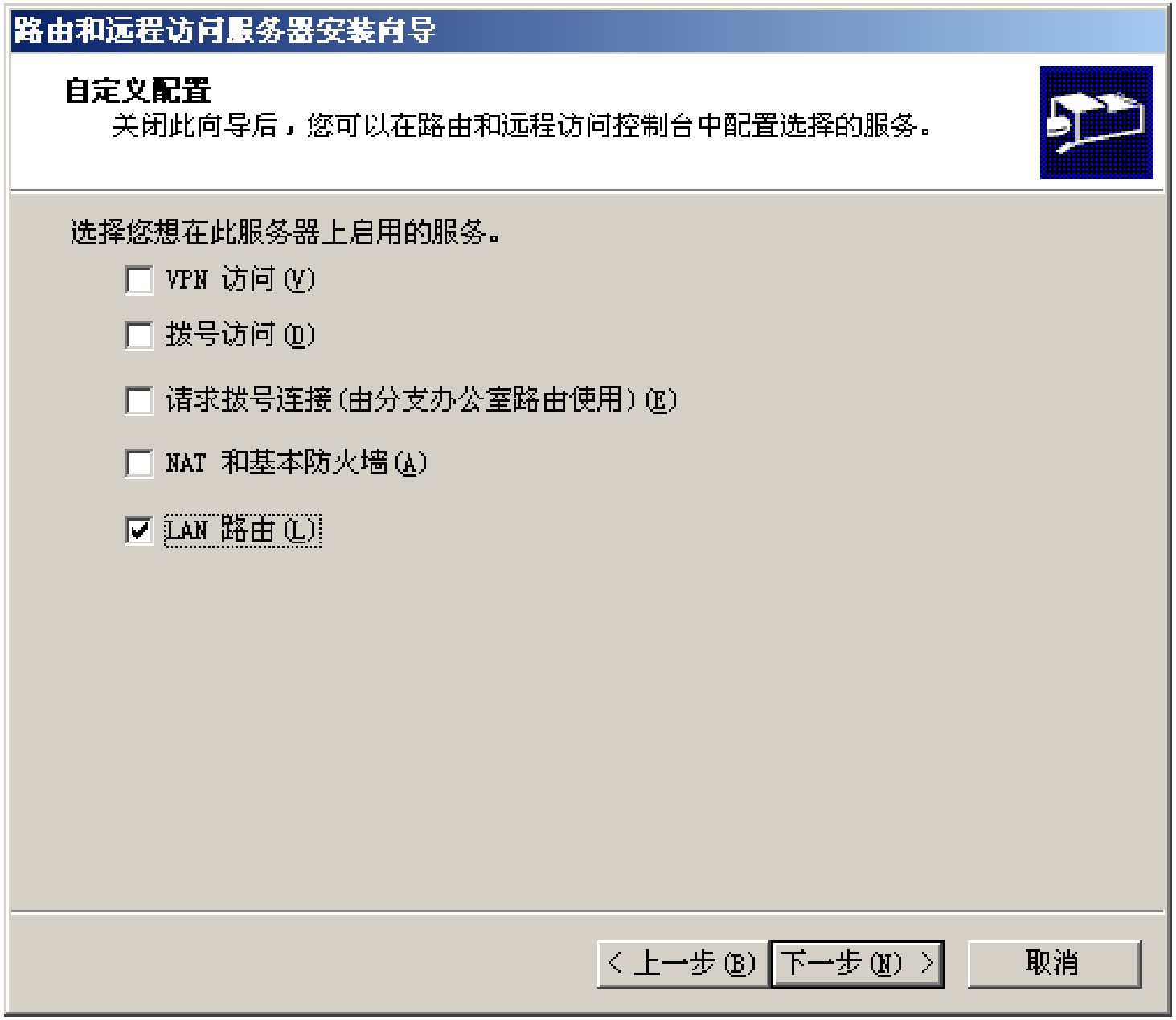

路由和远程访问服务器安装向导
自定义配置
关闭此向导后，您可以在路由和远程访问控制台中配置选择的服务。
选择您想在此服务器上启用的服务。
VPN 访问(V)
拨号访问(D)
请求拨号连接(由分支办公室路由使用)(E)
NAT 和基本防火墙(A)
LAN 路由(L)
< 上一步(B)
下一步(N) >
取消

图14 选择“LAN路由”

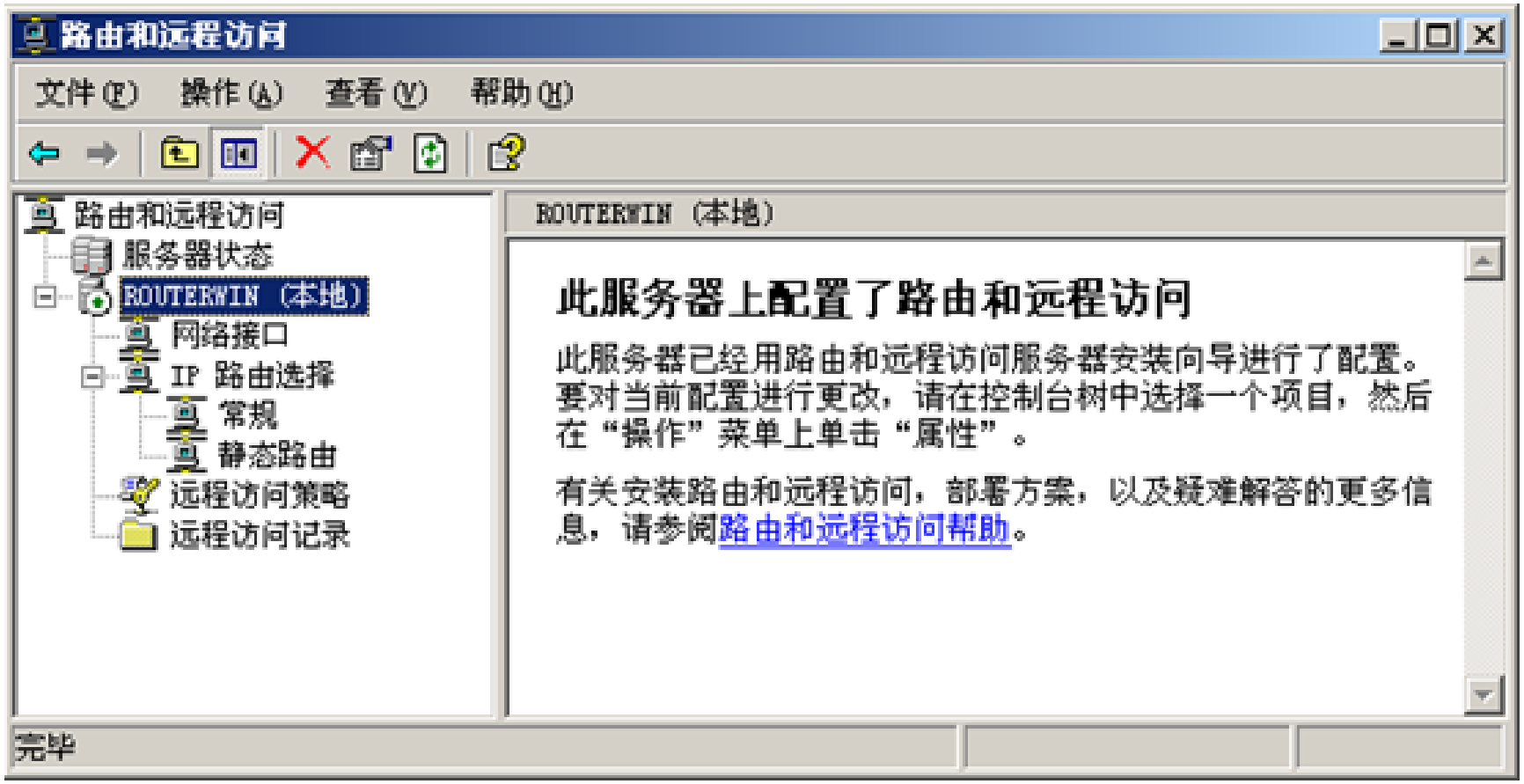


图15 启用“路由和远程访问服务”

对于Windows 2003系统，必须先**禁用防火墙（ICS）**才能配置路由和远程访问服务

图16 禁用防火墙和互联网连接共享

(2) 配置远程访问服务器VPN Server

- 首先按图16所示的方法禁用防火墙和互联网连接共享，然后打开路由和远程访问服务器安装向导，选择“远程访问(拨号或VPN)”（也可选择“虚拟专用网络(VPN)访问和NAT”）。

- 依次按照图17-21所示的步骤配置服务器。

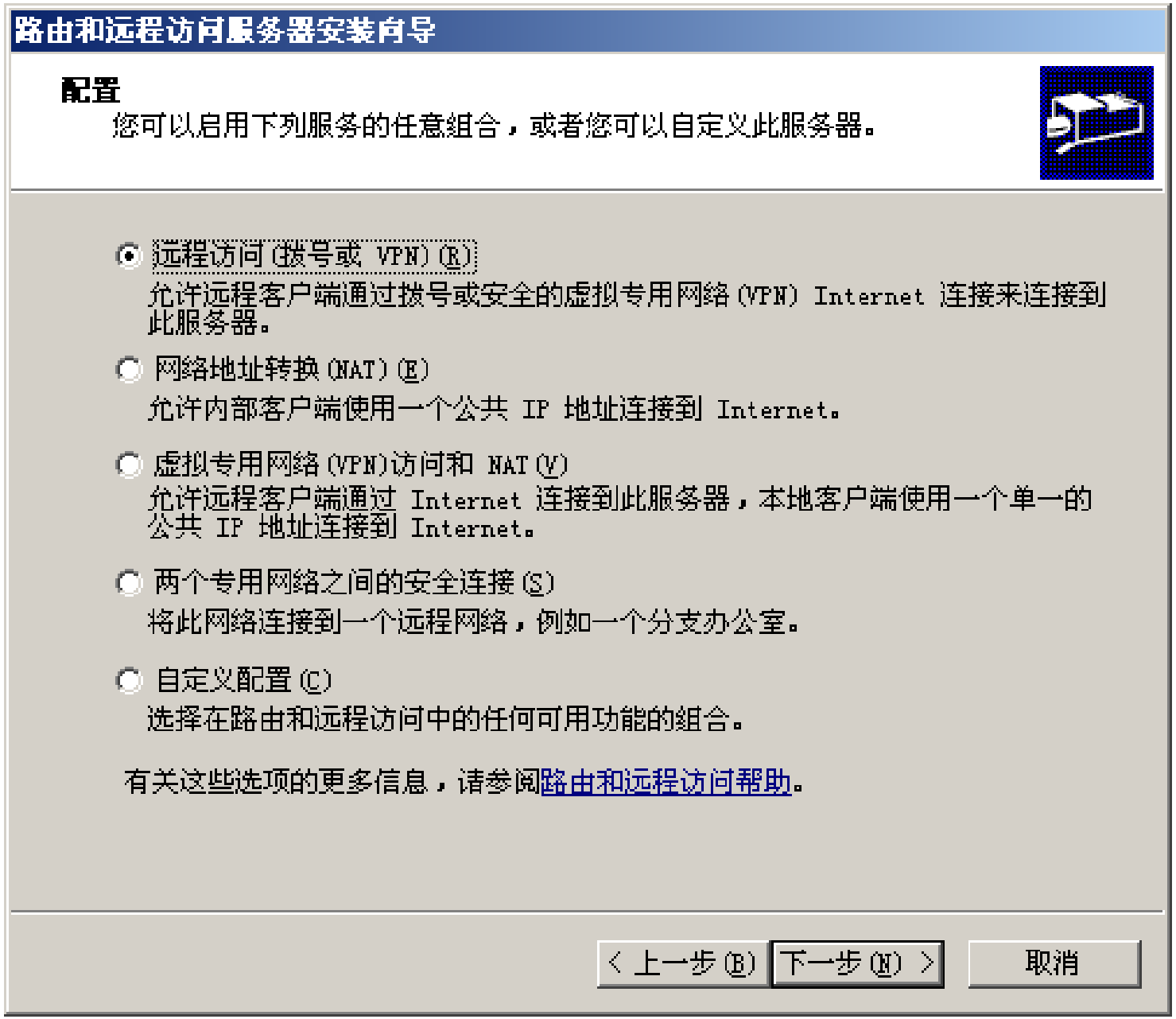


图17 配置为“远程访问(拨号或VPN)”

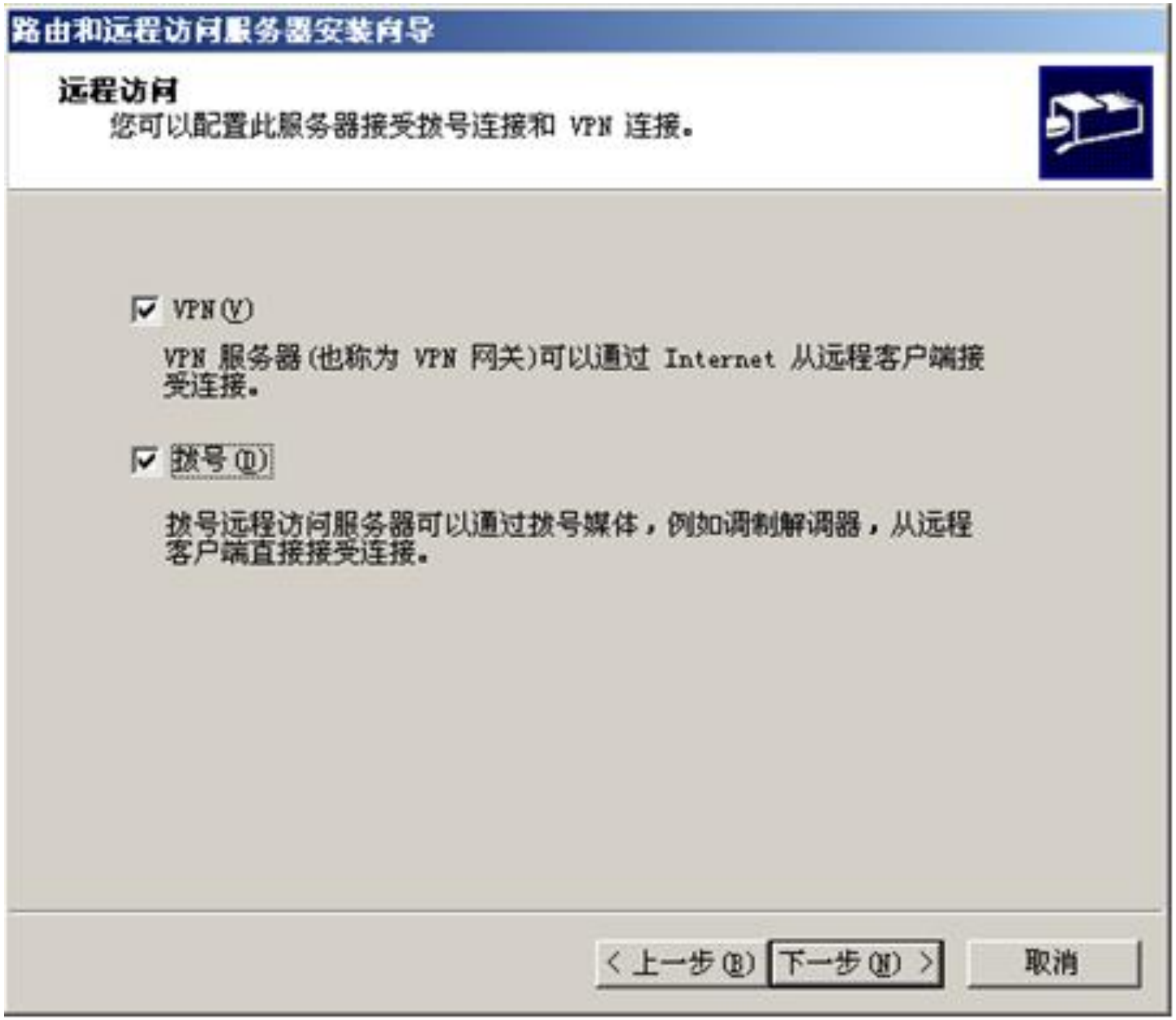
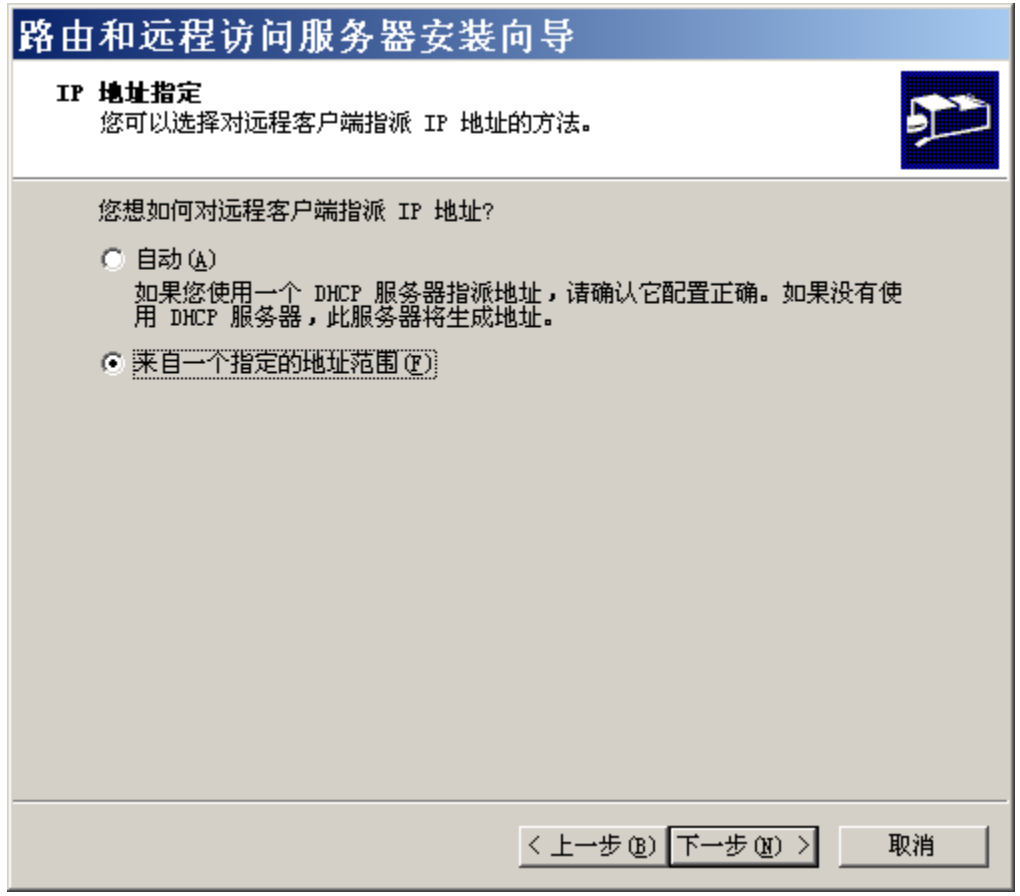
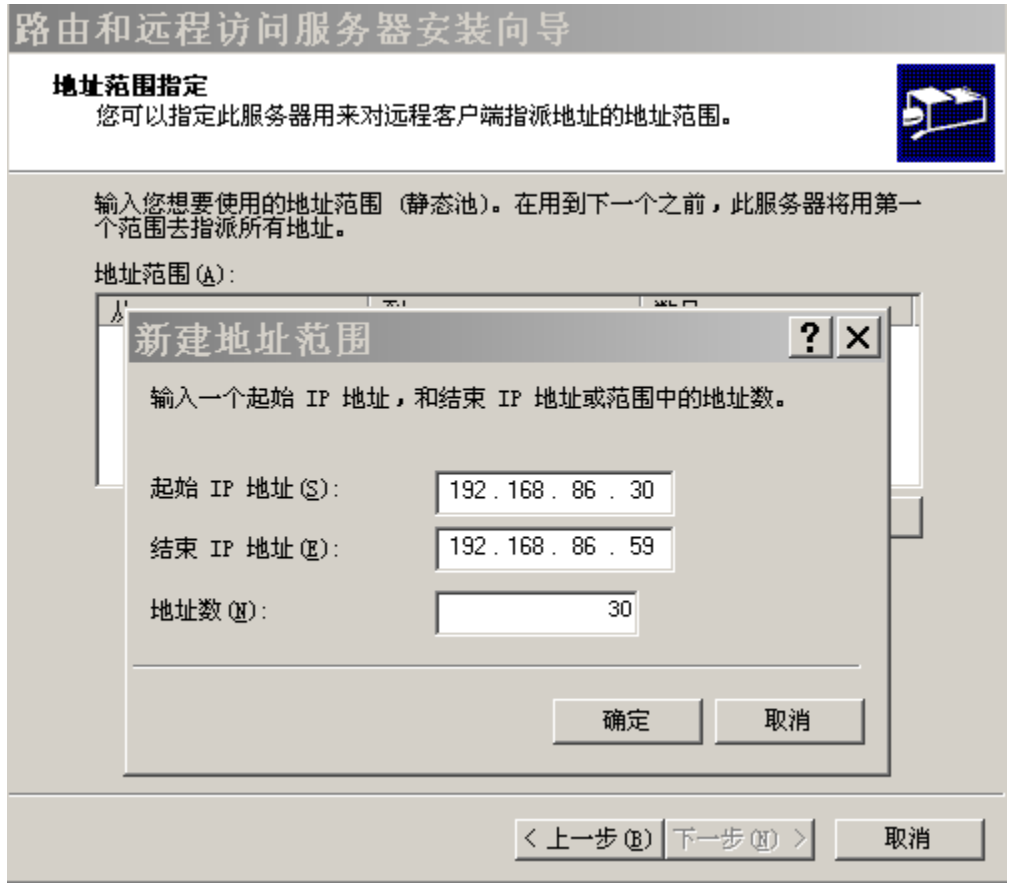

路由和远程访问服务器安装向导
远程访问
您可以配置此服务器接受拨号连接和 VPN 连接。
VPN(V)
VPN 服务器(也称为 VPN 网关)可以通过 Internet 从远程客户端接受连接。
拨号(D)
拨号远程访问服务器可以通过拨号媒体，例如调制解调器，从远程客户端直接接受连接。
< 上一步(B)
下一步(N) >
取消

图18 选择“VPN”

图19 选择连接到Internet的网络接口

设置VPN客户端的IP地址





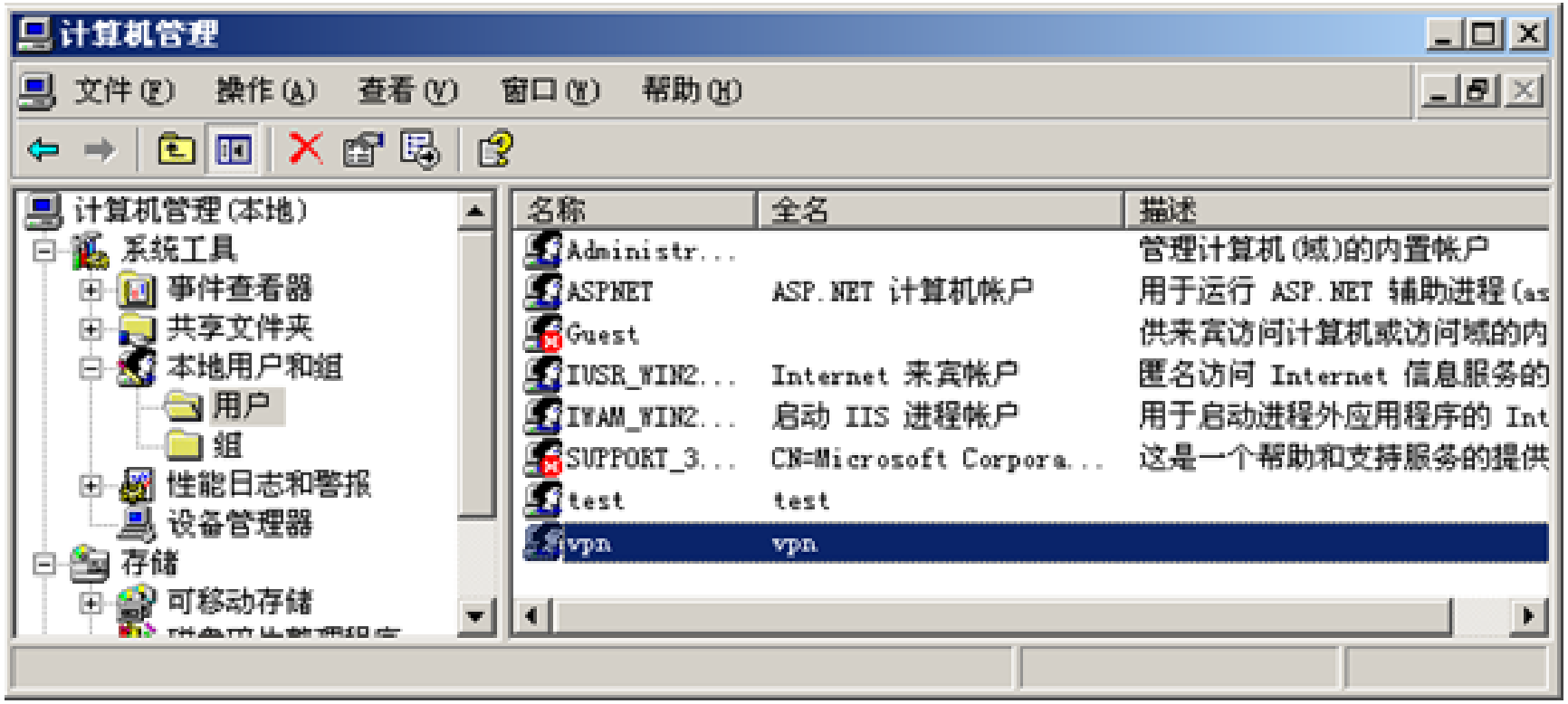


图20 选择待管理的用户(如VPN)

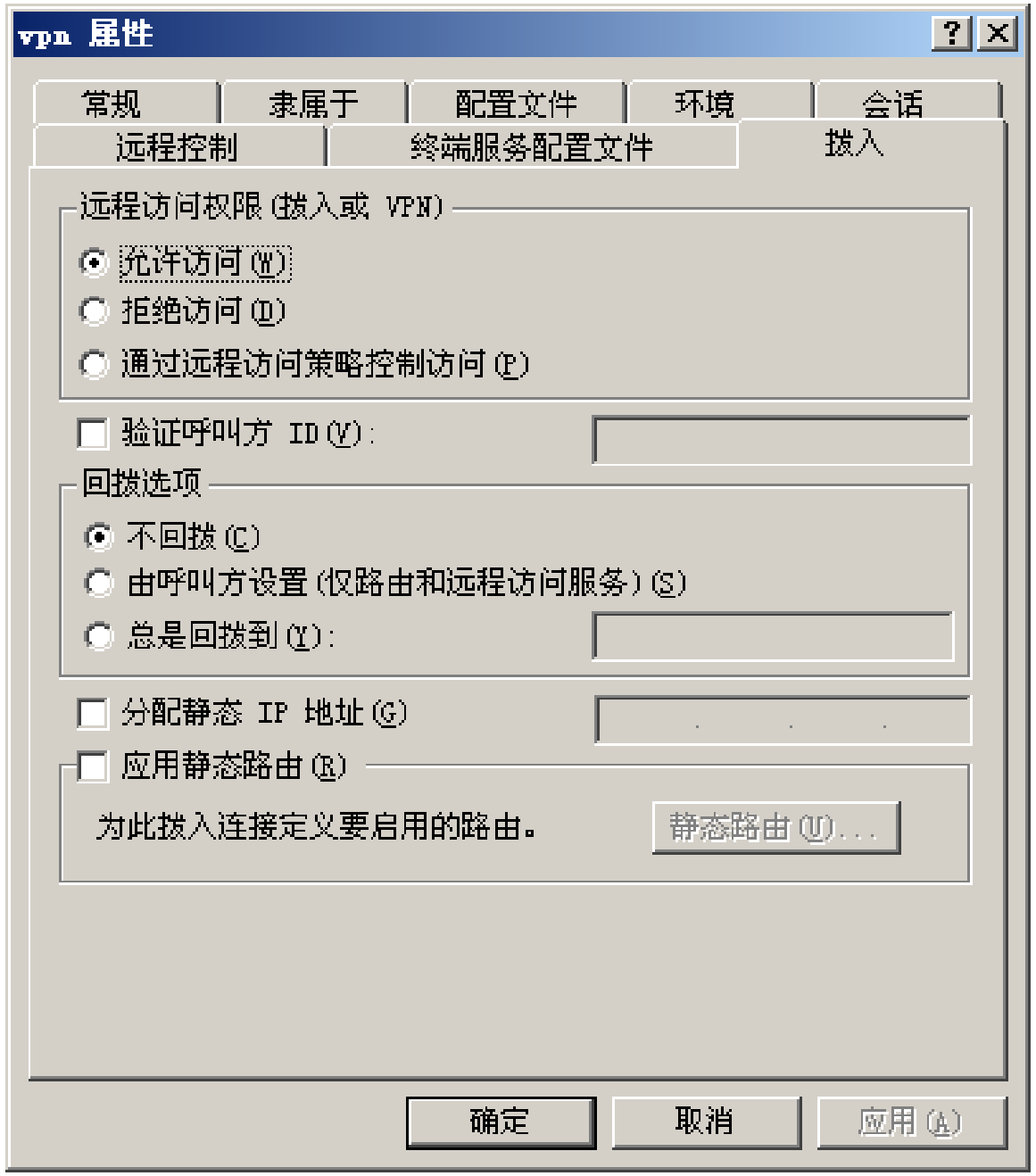

vpn 属性
常规
隶属于
配置文件
环境
会话
远程控制
终端服务配置文件
拨入
远程访问权限(拨入或 VPN)
允许访问(W)
拒绝访问(D)
通过远程访问策略控制访问(P)
验证呼叫方 ID(V):
回拨选项
不回拨(C)
由呼叫方设置(仅路由和远程访问服务)(S)
总是回拨到(Y):
分配静态 IP 地址(G)
应用静态路由(R)
为此拨入连接定义要启用的路由。
静态路由(U)...
确定
取消
应用(A)

图21 选择“允许访问”

查看VPN服务器的IP

- 在VPN服务器的“命令提示符”下运行IPConfig，得到如下输出：
- c:\HKTools>ipconfig

  Ethernet adapter 本地连接 4:

    Connection-specific DNS Suffix . :

    IP Address. . . . . : 166.66.66.**203**

    Subnet Mask . . . . . : 255.255.0.0

    Default Gateway . . . . . : 166.66.66.**???**

  Ethernet adapter 本地连接 3:

    Connection-specific DNS Suffix . :

    IP Address. . . . . : 192.168.86. xxx

    Subnet Mask . . . . . : 255.255.255.0

    Default Gateway . . . . . :

(3) 配置VPN 客户端

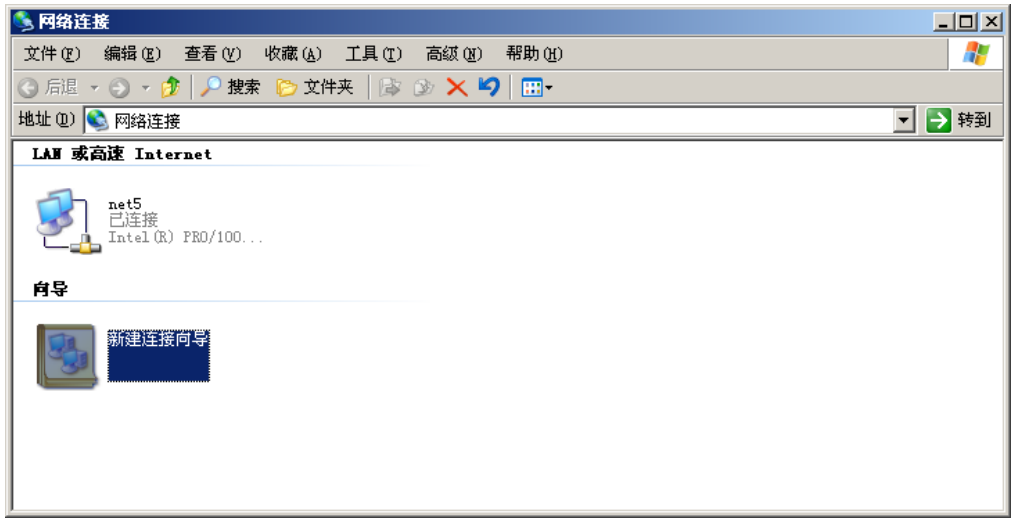


图22 网络连接

- 为了使远程主机通过互联网访问局域网，需要在客户机上配置拨号网络。
- 打开“网络连接”，如图22所示：

- 点击“创建一个新的连接”，打开“新建连接向导”，选择“连接到我的工作场所”，如图23所示。

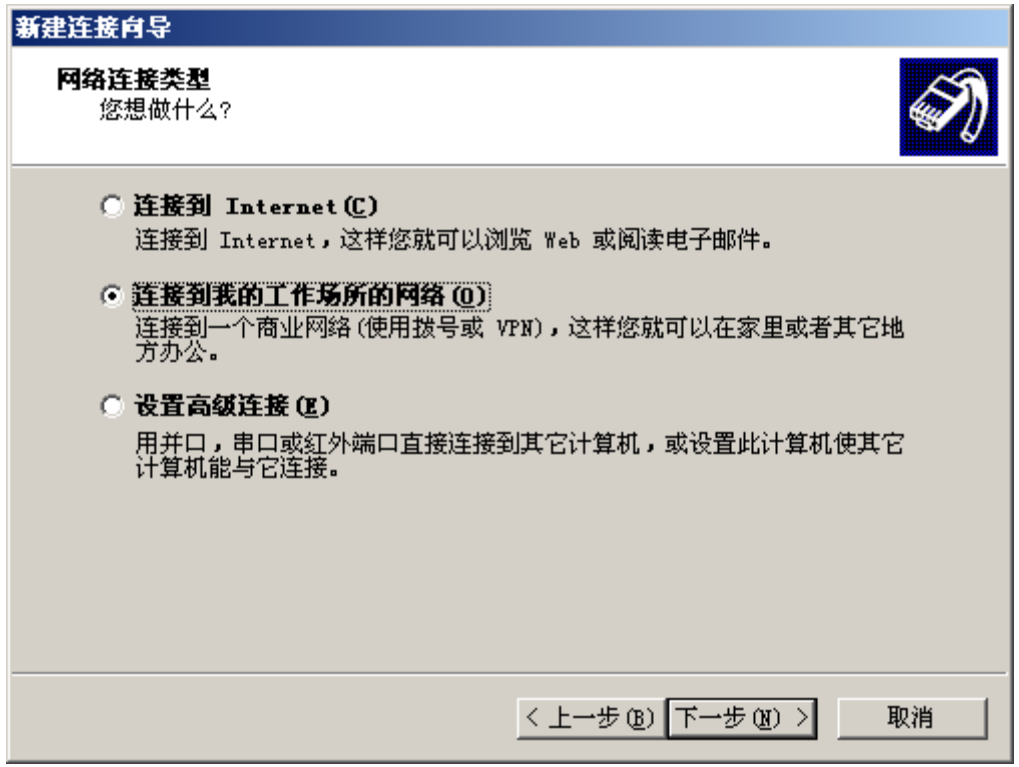


图23 确定网络连接类型

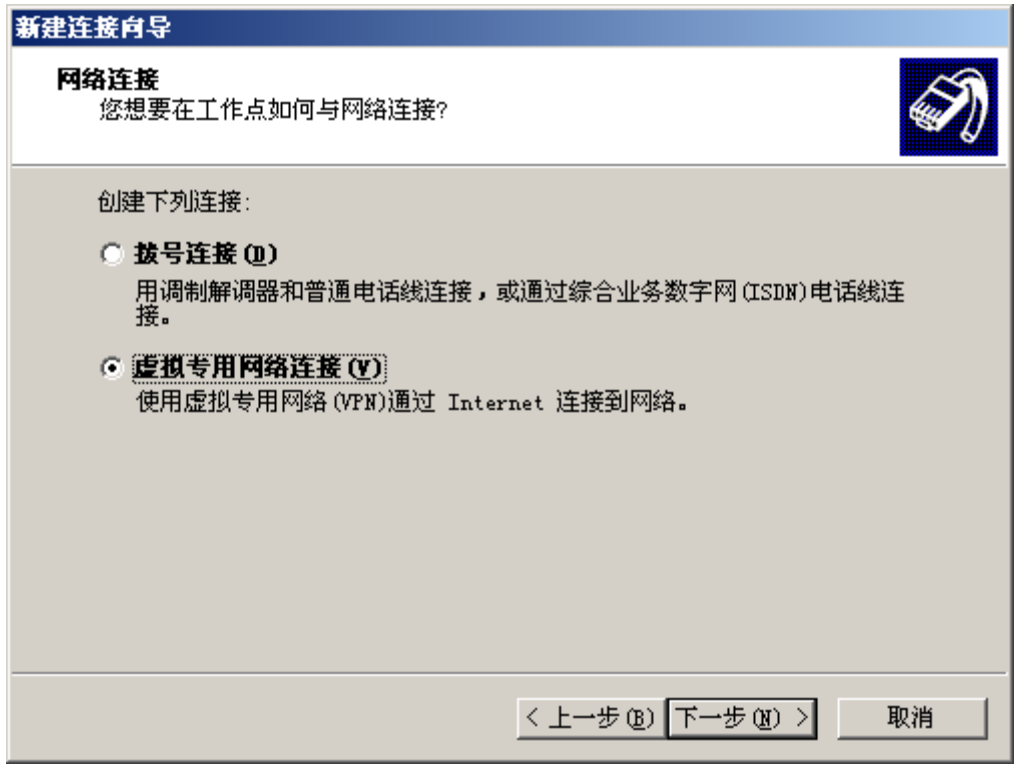

新建连接向导
网络连接
您想要在工作点如何与网络连接?
创建下列连接:
拨号连接(D)
用调制解调器和普通电话线连接，或通过综合业务数字网(ISDN)电话线连接。
虚拟专用网络连接(V)
使用虚拟专用网络(VPN)通过 Internet 连接到网络。
< 上一步(B)
下一步(N) >
取消

图24 选择虚拟专用网

创建一个新的VPN连接

- 点击“下一步”，输入该连接的名称，在此命名为“To-Server”；点击“下一步”，输入远程访问VPN服务器的IP地址，在此输入“166.66.66.xxx”；依次点击“下一步”，在点击“完成”，则完成了VPN客户端的配置。

- 接下来可通过该连接与VPN服务器建立虚拟专用网。
- 打开To-Server，在其中输入VPN服务器中允许拨入的用户名及密码（假设用户名为vpn，密码也为vpn），如图 25所示：

VPN客户端连接到VPN服务器

- 点击“连接”，则可以建立到VPN服务器的虚拟专用网。连接完成后在任务栏可以看到一个新的连接图标。用IPconfig命令可以看到，VPN客户机新建了一个虚拟网络接口。
- 同理，VPN服务器也新建了一个虚拟网络接口。
- 因此，VPN客户机和VPN服务器通过各自的虚拟网络接口建立了一条虚拟通道，就好像VPN客户机位于局域网内部一样，从而可以访问局域网内的主机。

图25 输入拨号的用户名和密码

用IPconfig命令查看到的虚拟网络接口

VPN客户机的虚拟网络接口

C:\work>ipconfig

Windows IP Configuration

Ethernet adapter net5:

Connection-specific DNS Suffix . :

IP Address. . . . . : 55.0.0.15

Subnet Mask . . . . . : 255.0.0.0

Default Gateway . . . . . : 55.55.55.233

PPP adapter To-Server:

Connection-specific DNS Suffix . :

IP Address. . . . . : **192.168.86.31**

Subnet Mask . . . . . : 255.255.255.255

Default Gateway . . . . . : 0.0.0.0

VPN服务器的虚拟网络接口

C:\work>ipconfig

Windows IP Configuration

PPP adapter RAS Server (Dial In) Interface:

Connection-specific DNS Suffix . :

IP Address. . . . . : **192.168.86.30**

Subnet Mask . . . . . : 255.255.255.255

Default Gateway . . . . . :

Ethernet adapter net6:

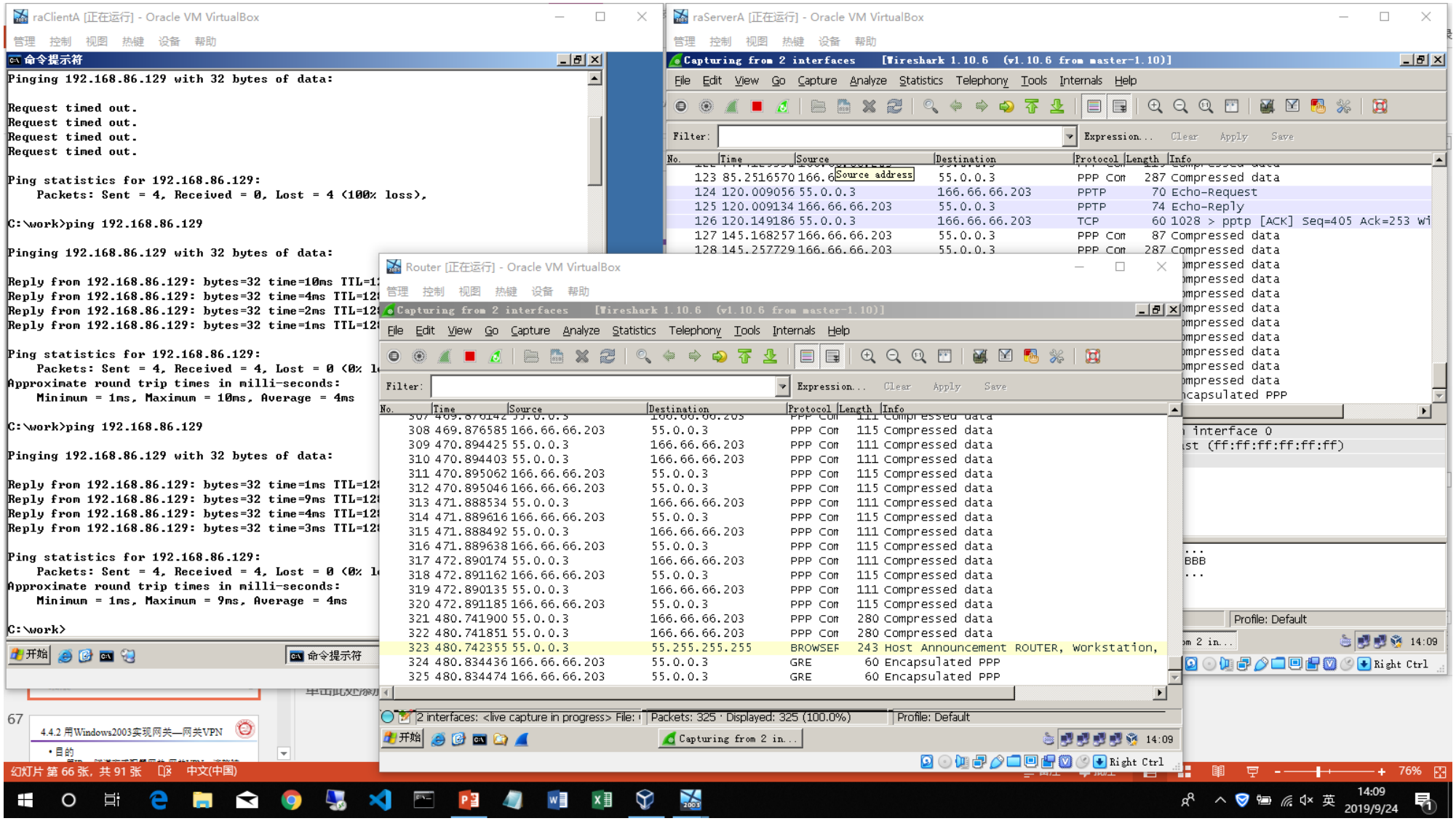
Connection-specific DNS Suffix . :

IP Address. . . . . : 166.66.66.203

Subnet Mask . . . . . : 255.255.0.0

Default Gateway . . . . . :

演示


raClientA [正在运行] - Oracle VM VirtualBox
命令提示符
Pinging 192.168.86.129 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.86.129:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\work>ping 192.168.86.129
Pinging 192.168.86.129 with 32 bytes of data:
Reply from 192.168.86.129: bytes=32 time=10ms TTL=1
Reply from 192.168.86.129: bytes=32 time=4ms TTL=12
Reply from 192.168.86.129: bytes=32 time=2ms TTL=12
Reply from 192.168.86.129: bytes=32 time=1ms TTL=12
Ping statistics for 192.168.86.129:
Packets: Sent = 4, Received = 4, Lost = 0 (0% l
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 10ms, Average = 4ms
C:\work>ping 192.168.86.129
Pinging 192.168.86.129 with 32 bytes of data:
Reply from 192.168.86.129: bytes=32 time=1ms TTL=12
Reply from 192.168.86.129: bytes=32 time=9ms TTL=12
Reply from 192.168.86.129: bytes=32 time=4ms TTL=12
Reply from 192.168.86.129: bytes=32 time=3ms TTL=12
Ping statistics for 192.168.86.129:
Packets: Sent = 4, Received = 4, Lost = 0 (0% l
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 9ms, Average = 4ms
C:\work>
raServerA [正在运行] - Oracle VM VirtualBox
Capturing from 2 interfaces [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
123 85.2516570 166.6 Source address 55.0.0.3 PPP Com 287 Compressed data
124 120.009056 55.0.0.3 166.66.66.203 PPTP 70 Echo-Request
125 120.009134 166.66.66.203 55.0.0.3 PPTP 74 Echo-Reply
126 120.149186 55.0.0.3 166.66.66.203 TCP 60 1028 > pptp [ACK] Seq=405 Ack=253 Wi
127 145.168257 166.66.66.203 55.0.0.3 PPP Com 87 Compressed data
128 145.257729 166.66.66.203 55.0.0.3 PPP Com 287 Compressed data
Router [正在运行] - Oracle VM VirtualBox
Capturing from 2 interfaces [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
308 469.876585 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
309 470.894425 55.0.0.3 166.66.66.203 PPP Com 111 Compressed data
310 470.894403 55.0.0.3 166.66.66.203 PPP Com 111 Compressed data
311 470.895062 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
312 470.895046 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
313 471.888534 55.0.0.3 166.66.66.203 PPP Com 111 Compressed data
314 471.889616 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
315 471.888492 55.0.0.3 166.66.66.203 PPP Com 111 Compressed data
316 471.889638 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
317 472.890174 55.0.0.3 166.66.66.203 PPP Com 111 Compressed data
318 472.891162 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
319 472.890135 55.0.0.3 166.66.66.203 PPP Com 111 Compressed data
320 472.891185 166.66.66.203 55.0.0.3 PPP Com 115 Compressed data
321 480.741900 55.0.0.3 166.66.66.203 PPP Com 280 Compressed data
322 480.741851 55.0.0.3 166.66.66.203 PPP Com 280 Compressed data
323 480.742355 55.0.0.3 55.255.255.255 BROWSER 243 Host Announcement ROUTER, Workstation,
324 480.834436 166.66.66.203 55.0.0.3 GRE 60 Encapsulated PPP
325 480.834474 166.66.66.203 55.0.0.3 GRE 60 Encapsulated PPP
2 interfaces: <live capture in progress> File:
Packets: 325 · Displayed: 325 (100.0%)
Profile: Default
Capturing from 2 in...
Right Ctrl
interface 0
st (ff:ff:ff:ff:ff:ff)
BBB
Profile: Default
Right Ctrl
4.4.2 用Windows2003实现网关—网关VPN
幻灯片 第 66 张，共 91 张
中文(中国)
76%
14:09
2019/9/24

VPN-Server显示的信息

Capturing from 2 interfaces [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
245	516.171887	192.168.86.129	192.168.86.255	BROWSER	243	Local Master Announcement SERVERA, Workstation, Server, Dialin Server, NT Workst
246	516.171268	166.66.66.203	55.0.0.3	PPP Com	280	Compressed data
247	520.207249	166.66.66.203	55.0.0.3	PPP Com	87	Compressed data
248	540.083795	55.0.0.3	166.66.66.203	PPTP	70	Echo-Request
249	540.083872	166.66.66.203	55.0.0.3	PPTP	74	Echo-Reply
250	540.233342	55.0.0.3	166.66.66.203	TCP	60	1028 > pptp [ACK] Seq=517 Ack=393 Win=63848 Len=0
251	580.342956	55.0.0.3	166.66.66.203	PPP Com	111	Compressed data
252	580.343069	166.66.66.203	55.0.0.3	PPP Com	115	Compressed data
253	581.342269	55.0.0.3	166.66.66.203	PPP Com	111	Compressed data
254	581.342553	166.66.66.203	55.0.0.3	PPP Com	115	Compressed data
255	582.353997	55.0.0.3	166.66.66.203	PPP Com	111	Compressed data
256	582.354422	166.66.66.203	55.0.0.3	PPP Com	115	Compressed data
257	583.355545	55.0.0.3	166.66.66.203	PPP Com	111	Compressed data
258	583.355870	166.66.66.203	55.0.0.3	PPP Com	115	Compressed data
259	600.098548	55.0.0.3	166.66.66.203	PPTP	70	Echo-Request
260	600.098938	166.66.66.203	55.0.0.3	PPTP	74	Echo-Reply
261	600.259995	55.0.0.3	166.66.66.203	TCP	60	1028 > pptp [ACK] Seq=533 Ack=413 Win=63828 Len=0

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_36:72:8a (08:00:27:36:72:8a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 36 72 8a 08 06 00 01   ........ '6r.....
0010  08 00 06 04 00 01 08 00  27 36 72 8a a6 42 42 42   ........ '6r..BBB
0020  00 00 00 00 00 00 a6 42  42 cb 00 00 00 00 00 00   .......B B.......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

2 interfaces: <live capture in progress> File: | Packets: 261 · Displayed: 261 (100.0%) | Profile: Default

开始 命令提示符 Capturing from 2 in... 14:17

4.3 基于第3层隧道协议的IPSec VPN

- 互联网安全协议（Internet Protocol Security，缩写为 IPsec），是通过对IP协议（互联网协议）的分组进行加密和认证来保护IP协议的网络传输协议族（一些相互关联的协议的集合）。

- 第一版IPsec协议在RFC 2401—2409中定义。第二版IPsec协议的标准文档在2005年发布，新的文档定义在RFC 4301—RFC 4309中。

- RFC 4301 Updated by RFC 6040, RFC 7619

IPsec协议工作在OSI 模型的第三层

- IPsec协议工作在OSI 模型的第三层（网络层或TCP/IP模型的IP层），使其在单独使用时适于保护基于TCP或UDP的协议（如安全套接子层（SSL）就不能保护UDP层的通信流）。
- 这就意味着，与传输层或更高层的协议相比，IPsec协议必须处理可靠性和分片的问题，这同时也增加了它的复杂性和处理开销。
- 相对而言，SSL/TLS依靠更高层的TCP（OSI的第四层）来管理可靠性和分片。

4.3.1 IPSec的组成和工作模式

IPSec由一序列的协议组成，其中最重要的协议有三个：

(1) 认证头AH (Authentication Headers)：

- AH为IP数据报实现无连接的完整性和数据源认证功能，并能抵抗重放攻击。

(2) 封装安全有效载荷ESP (Encapsulating Security Payloads)：

- ESP实现保密性、数据源认证、无连接的完整性、抵抗重放攻击的服务(一种形式的部分序列完整性)和有限的网络流的保密性。

(3) 安全联盟SA (Security Associations)：

- 也称为**安全关联**
- SA给出**算法和数据的集合**，以向AH或ESP的操作提供必须的参数。
- 安全联盟和密钥管理协议ISAKMP（Internet Security Association and Key Management Protocol）提供了认证和密钥交换的框架。该框架支持手工配置的预共享密钥以及通过其他方法获得的密钥，这些方法包括：Internet密钥交换（IKE和IKEv2协议）、KINK（Kerberized Internet Negotiation of Keys）、IPSEC KEY DNS记录。

IPSec的工作模式

IPSec有两种工作模式：传输模式和隧道模式。

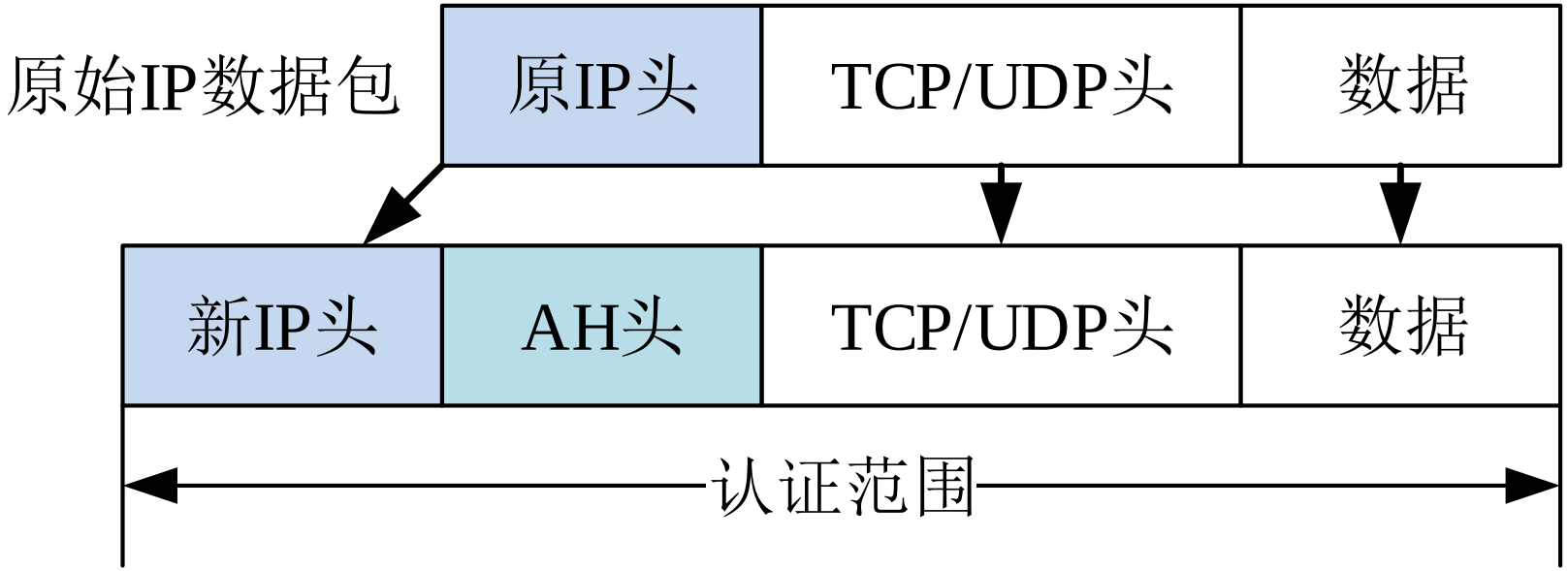
1. 传输模式用于**两台主机之间的连接**，在IP层封装**主机—主机**的分组；

2. 隧道模式用于**两个网关之间的连接**，在IP层封装**网关—网关**的分组，可穿过公共网络（如Internet）实现局域网之间的互联。AH和ESP均支持传输模式和隧道模式，实现认证和（或）加密等安全功能。

4.3.2 认证协议AH

- IP**认证头AH（IP Authentication Header）**定义在RFC4302中，实现IP数据报的认证、完整性和抗重放攻击。
- AH数据报直接封装在IP数据报中，如果IP数据包的**协议字段为51**，表明IP头之后是一个AH头。
- AH和ESP同时保护数据时，在顺序上，AH头在ESP头之后。

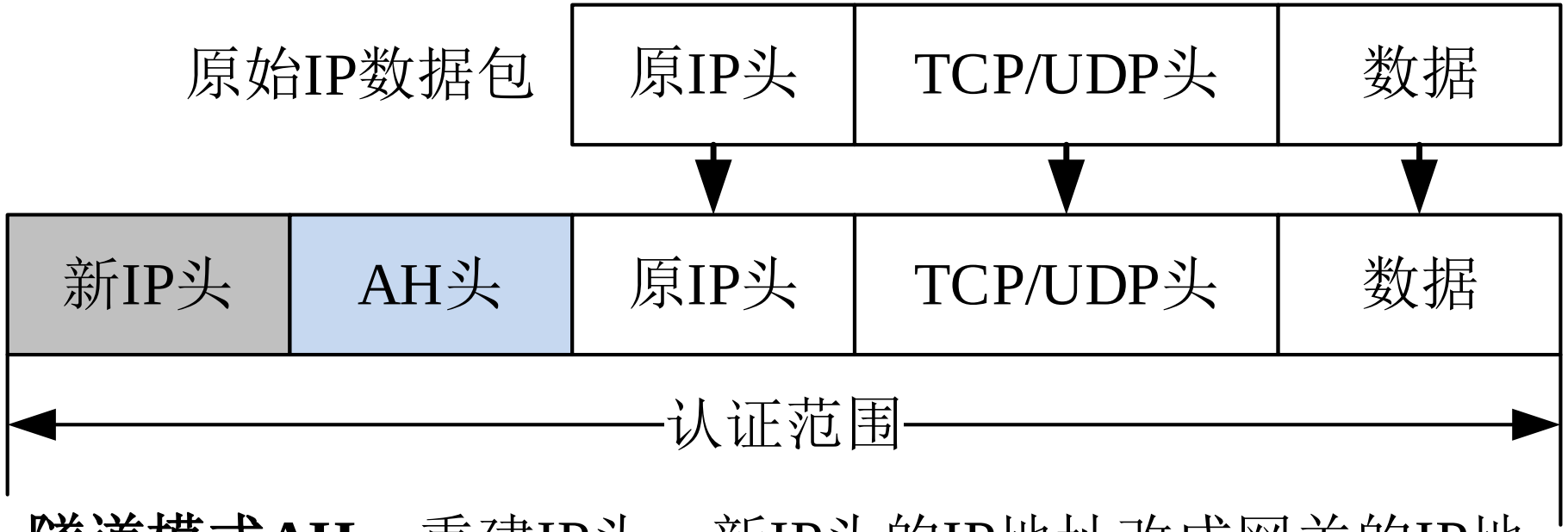
AH的传输模式



传输模式AH：新IP头拷贝自原IP头，将协议字段改为51，原协议字段拷贝到**AH头**的下一个头字段。

图5(a) AH的传输模式

AH的隧道模式



隧道模式AH： 重建IP头，新IP头的IP地址改成网关的IP地址，协议字段为51，**AH头**中的**下一个头为4或41**（对应于IPv6），原始数据包拷贝到AH头之后。

图5(b) AH的隧道模式

AH头的格式

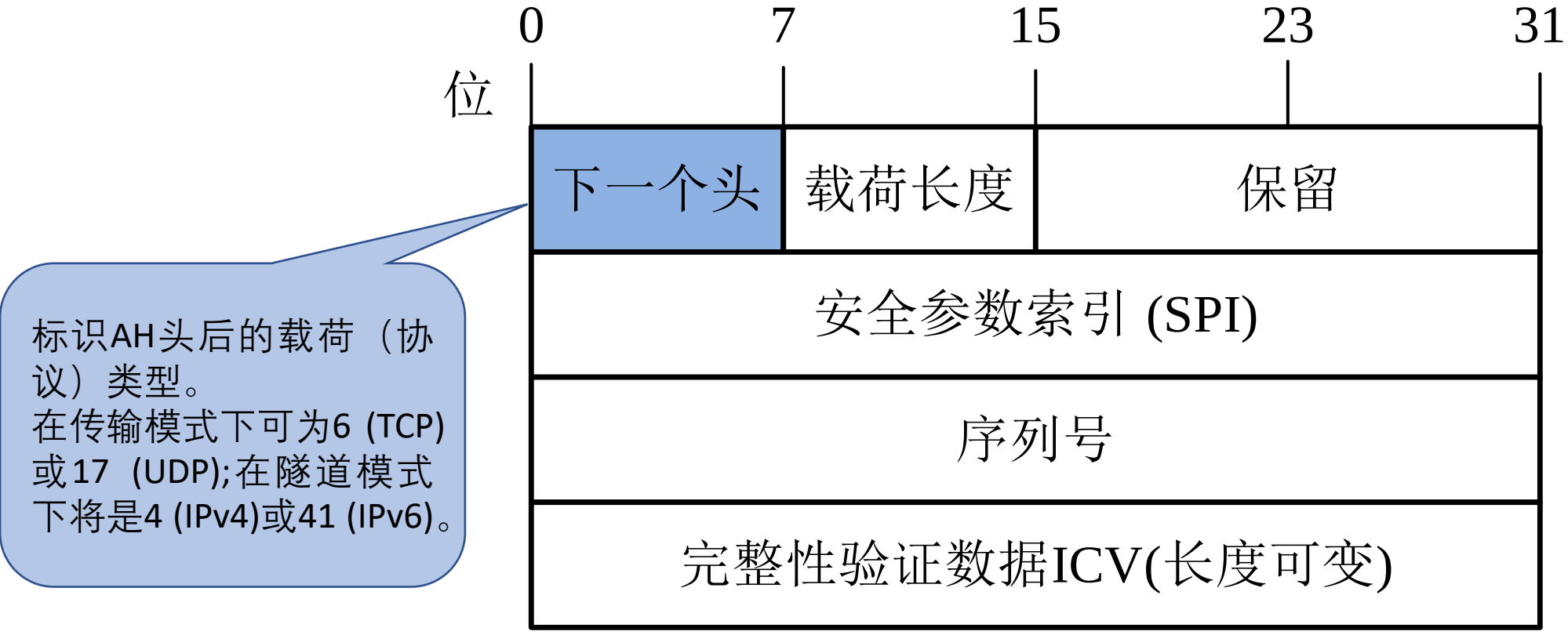


图6 AH头的格式

AH头的格式

① **下一个头(Next Header)**：8-bits，标识AH头后的**载荷（协议）类型**。在传输模式下可为6 (TCP)或17 (UDP);在隧道模式下将是4 (IPv4)或41 (IPv6)。

② 载荷长度(Payload Length)：8-bits，表示AH头本身的长度，以32-bits为单位。

③ 保留(Reserved)：16-bits，保留字段，未使用时必须设为0。

④ 安全参数索引SPI (Security Parameters Index)：32-bits，接收方用于标识对应的安全关联(SA)。

⑤ 序列号(Sequence Number)：32-bits，是一个单向递增的计数器，提供抗重播功能（anti-replay）。

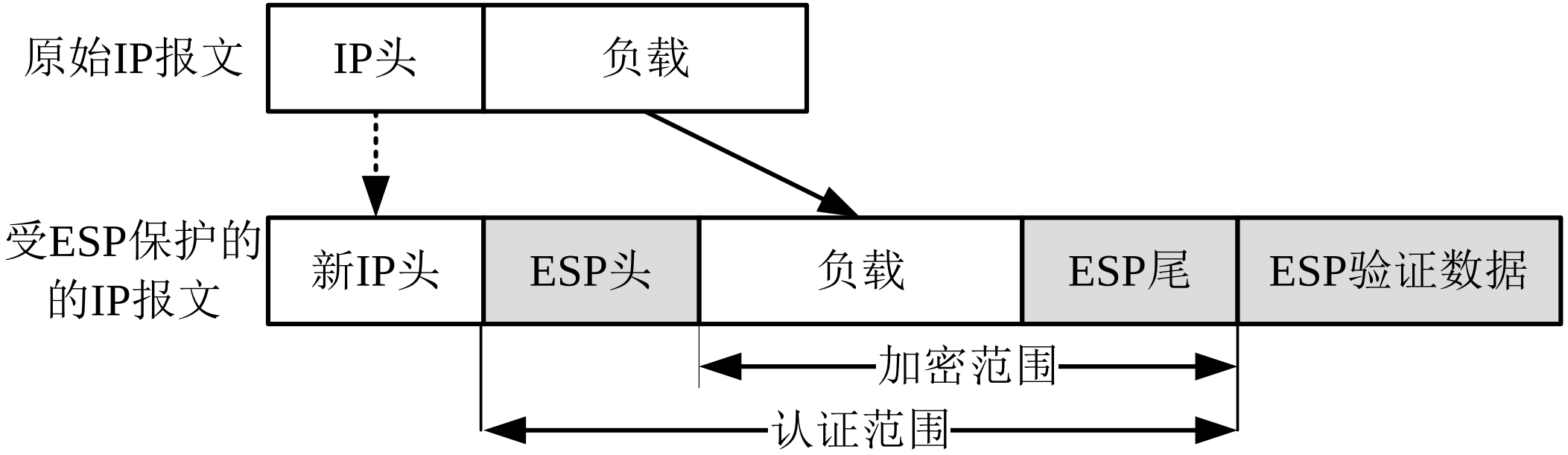
⑥ 完整性验证数据ICV（Integrity Check Value）：这是一个可变长度（必须是32比特的整数倍）的域，长度由具体的验证算法决定。完整性验证数据ICV验证IP数据包的完整性，因此ICV的计算包含了整个IP数据包。

4.3.3 封装安全载荷ESP

- IP封装安全载荷ESP （IP Encapsulating Security Payload）定义在RFC 4303中，实现IP数据报的认证、完整性、抗重放攻击和加密。
- ESP可以实现AH的所有功能，然而由于AH比ESP出现得更早，AH至今未被废弃。
- 与AH协议一样，ESP的数据报也直接封装在IP数据报中，如果IP数据包的**协议字段为50**，表明IP头之后是一个ESP数据报。

- ESP数据报由四部分组成，分别是：**头部**、加密数据（**ESP载荷+ESP尾**）和**ESP验证数据**。

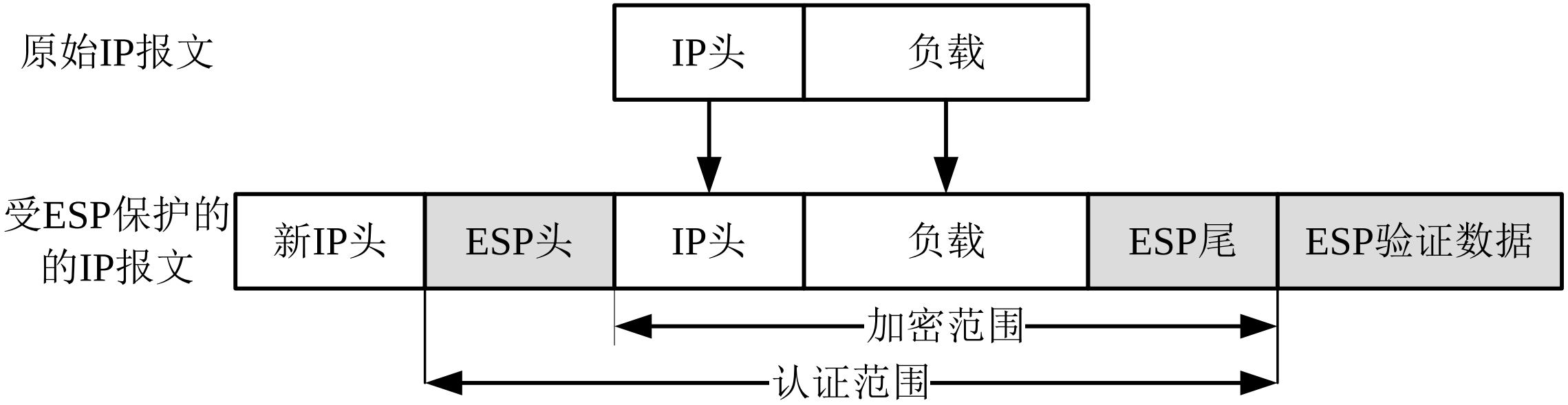
传输模式的ESP



传输模式ESP：新IP头拷贝自原IP头，将协议字段改为50，原协议字段拷贝到ESP尾的下一个头。

图7 (a) 传输模式的ESP

隧道模式的ESP



隧道模式ESP：重建IP头，新IP头的IP地址改成网关的IP地址，协议字段为50，ESP尾中的下一个头为4或41(对于IPv6)，原始数据包和ESP尾加密后拷贝到ESP头之后。

图7 (b) 隧道模式的ESP

ESP的数据报格式

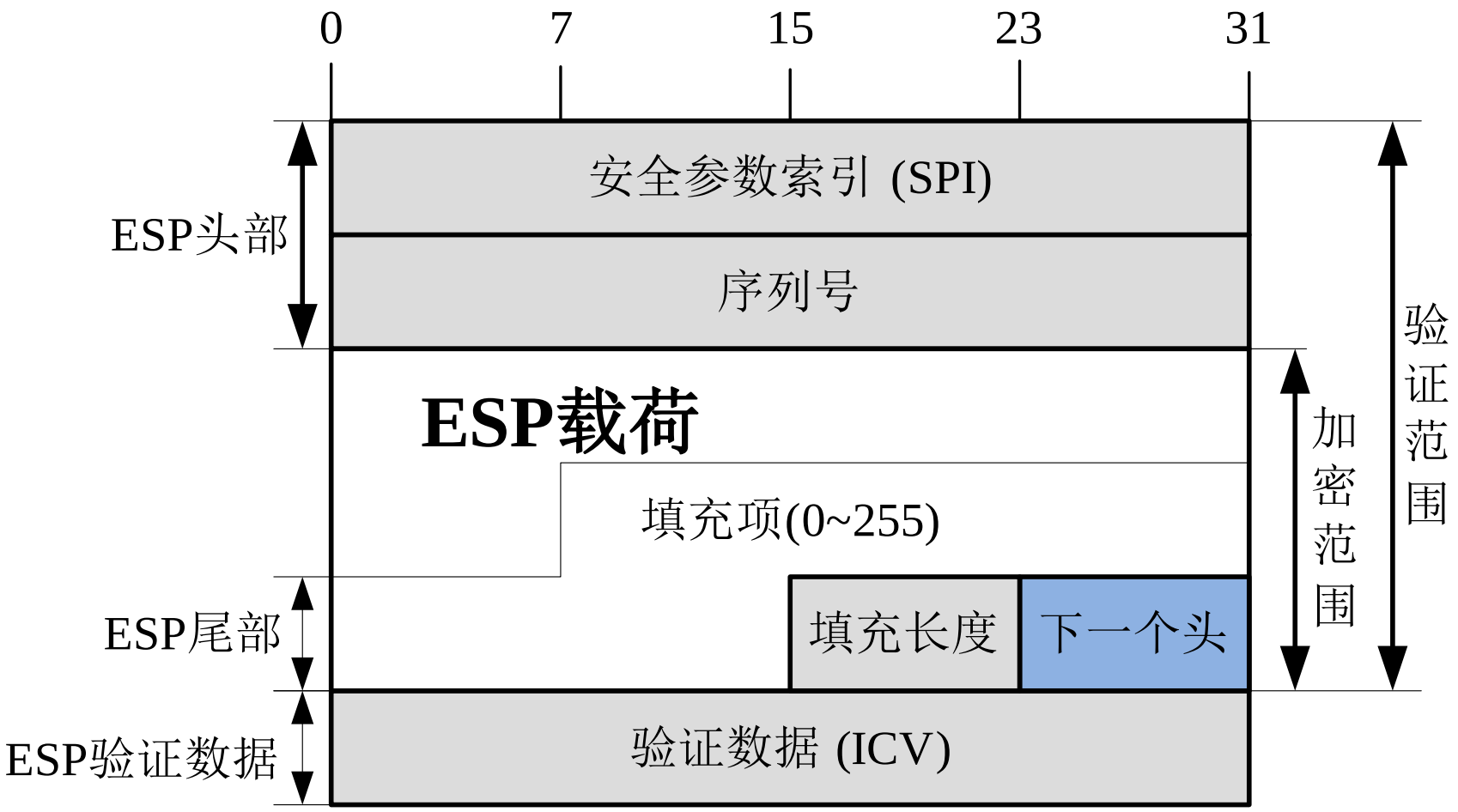


图8 ESP的数据报格式

ESP的数据报格式

- 安全参数索引SPI(32-bits)：在IKE交换过程中由目标主机选定，与IP头之前的目标地址以及协议结合在一起，用来标识用于处理数据包的特定的那个安全关联。SPI经过验证，但并未加密。
- 序列号(32-bits)：它是一个唯一的单向递增的计数器，与AH类似，提供抵抗重播攻击的能力。
- 填充项(0 ~ 255 bytes)：由具体的加密算法决定。
- 填充长度(8-bits)：接收端可以据此恢复载荷数据的真实长度。
- **下一个头**(8-bits)：标识受ESP保护的**载荷的（协议）类型**。在传输模式下拷贝自原IP数据报头中的协议值，可为6 (TCP)或17 (UDP)；在隧道模式下可为4(IPv4)或41 (IPv6)。
- 验证数据(完整性校验值ICV)：一个经过密钥处理的散列值，验证范围包括ESP头部、被保护的数据以及ESP尾部。其长度与具体的验证算法有关，但必须是32bits的整数倍。

4.3.4 安全关联与安全策略

- 在AH和ESP头中有一个32bits的**安全参数索引SPI**，用于标识通信的两端采用的**IPSec安全关联SA**(Security Associations，也称为**安全联盟**)。

- SA保存于通信双方的安全关联数据库中，SA根据安全策略手工或自动创建，安全策略保存在安全策略数据库中。安全关联SA与安全策略定义在RFC 4301中。

(1) 安全关联与安全关联数据库

- **安全关联(SA) 是两个通信实体协商建立起来的一种安全协定，**例如，IPSec协议（AH或ESP）、 IPSec的操作模式（传输模式和隧道模式）、加密算法、验证算法、密钥、密钥的存活时间等。安全关联**SA是单工的**（即**单向**的），输出和输入都需要独立的SA。

- SA是通过IKE密钥管理协议在通信双方之间来协商的，协商完成后，通信双方都会在它们的安全关联数据库(SAD)中存储该SA参数。

安全关联(SA)

一个安全关联由下面三个参数唯一确定：

1. **安全参数索引号(SPI)**：一个与SA相关的位串，由AH和ESP携带，使得接收方能选择合适的SA处理数据包。
2. **IP目的地址**：目前只允许使用单一地址，表示SA的目的地址。
3. **安全协议标识**：标识该SA是AH安全关联或ESP安全关联。

安全关联(SA) 的其他参数

(1) **序列号计数器**：一个32位的值，用于生成AH或ESP头中的序号字段，在数据包的“外出”处理时使用。

(2) **序列号溢出**：用于输出包处理，并在序列号溢出的时候加以设置，安全策略决定了一个SA是否仍可用来处理其余的包。

(3) **抗重放窗口**：用于确定一个入栈的AH或ESP包是否是重放。

(4) **AH信息**：AH认证算法、密钥、密钥生存期和其他AH的相关参数。

(5) **ESP信息**：ESP认证和加密算法、密钥、初始值、密钥生存期和其他ESP的相关参数。

(6) **SA的生存期**：一个SA最长能存在的时间。到时间后，一个SA必须用一个新的 SA替换或终止。

(7) **IPSec协议模式**：隧道、传输、通配符（隧道模式、传输模式均可）。

(8) **路径MTU**：在隧道模式下使用IPSec时，必须维持正确的PMTU信息，以便对这个数据包进行相应的分段。

(2) 安全策略和安全策略数据库SPD

- 安全策略决定了为一个数据包提供的安全服务，它保存在安全策略数据库SPD中。SPD中的每一个安全策略条目由一组IP和上层协议字段值组成，即下面提到的选择符。
- 安全策略数据库(SPD)记录了对IP数据流（根据源IP、目的IP、上层协议以及流入还是流出）采取的安全策略。
- 每一安全策略条目可能对应零条或多条SA条目，通过使用一个或多个选择符来确定某一个SA条目。

IPSec允许的选择符

(1) 目的IP地址：可以是主机地址、地址范围或者通配符。
(2) 源IP地址：可以是主机地址、地址范围或者通配符。
(3) 源/目的端口。
(4) 用户ID：操作系统中的用户标识。
(5) 数据敏感级别。
(6) 传输层协议。
(7) IPSec协议(AH，ESP，AH/ESP)。
(8) 服务类型(TOS)。

4.4 Windows环境下的VPN

- 目前流行的Windows系统各版本均支持远程访问VPN客户端， Windows Server支持远程访问服务及IPSec服务。

- 本节详细介绍**VPN在Windows环境下的配置使用方法**。

4.4.1 用Windows2003实现远程访问VPN

见“4.2.3 基于第2层隧道协议的VPN实例”

4.4.2 用Windows2003实现网关—网关VPN

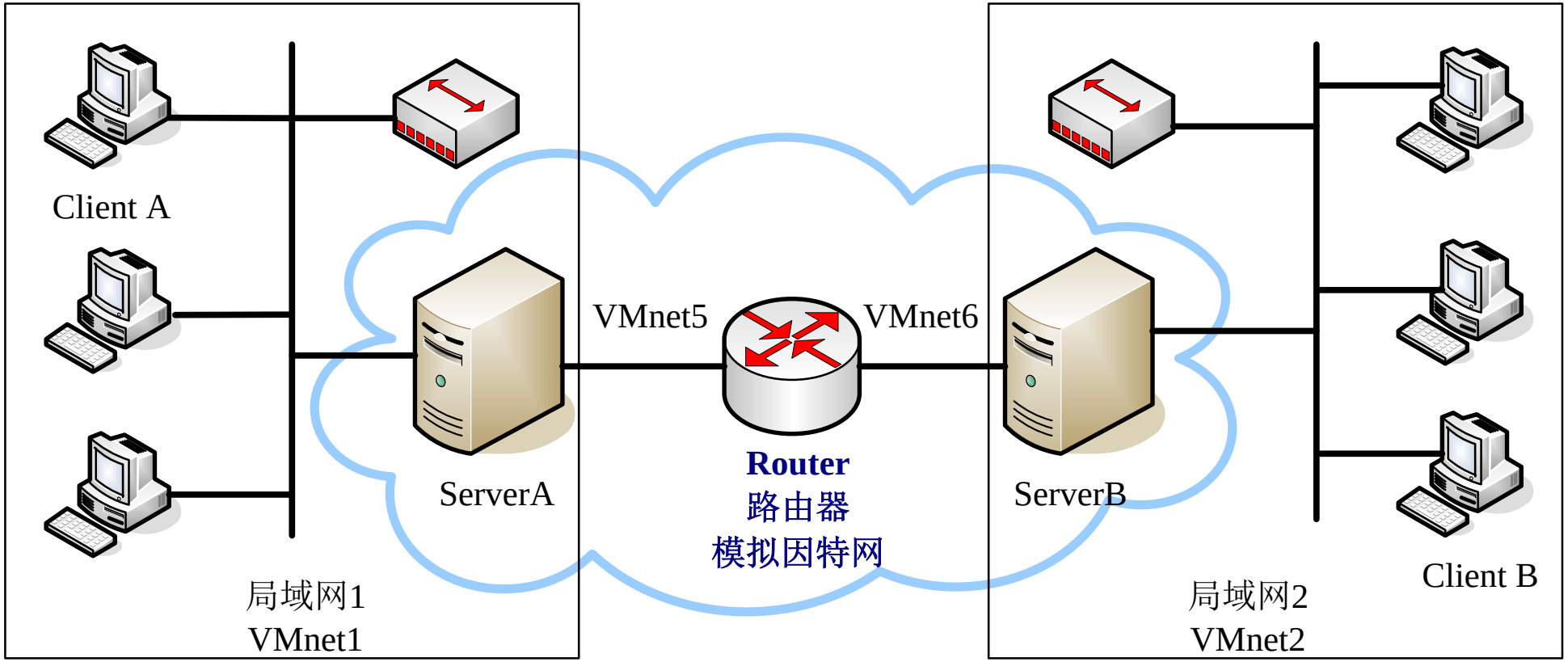
- 目的

  用IPsec隧道方式配置**网关—网关VPN**，连接被Internet隔开的两个局域网(VMnet1和VMnet3)，使之进行安全通信，实现信息的保密性和完整性。

- 设计

  用Vmware或Virtualbox模拟两个局域网和一个广域网（用路由器模拟）。每个局域网含若干台客户机和一台Windows server 2003组成。

  也可以用容器技术（比如docker），搭建出所需的虚拟机。



- 虚拟网卡VMnet1和VMnet2分别模拟两个局域网，VMnet5、VMnet6和Router模拟互联网，ServerA和ServerB模拟互联网上的远程服务器(边界路由器)，建立IPSec隧道以连接两个局域网，并保证通信安全。

机器名	系统及必备软件	虚拟网络	IP地址信息
Client A	Windows Server 2003	VMnet1	IP: 自动获取 Subnet Mask: 255.255.255.0 GateWay: x.x.x.x
Server A	Windows Server 2003	VMnet1 VMnet5	IP: 192.168.86.56 Subnet Mask: 255.255.255.0 GateWay: IP: 55.55.55.56 Subnet Mask: 255.0.0.0 GateWay: x.x.x.x
Router	Windows Server 2003 必须安装Wireshark软件 http://www.wireshark.org/	VMnet5 VMnet6	IP: 55.55.55.55 Subnet Mask: 255.0.0.0 GateWay: IP: 166.66.66.66 Subnet Mask: 255.255.0.0 GateWay:
Server B	Windows Server 2003	VMnet6 VMnet2	IP: 166.66.66.67 Subnet Mask: 255.255.0.0 GateWay: x.x.x.x IP: 172.16.0.67 Subnet Mask: 255.240.0.0 GateWay:
Client B	Windows Server 2003	VMnet2	IP: 自动获取 Subnet Mask: 255.240.0.0 GateWay: x.x.x.x

注：IP地址与演示系统可能有所不同

1.创建ServerA 的IPSec策略

(1) 在管理工具中打开“本地安全策略”--右击“IP安全策略,在本地计算机”—“创建IP安全策略”，如图27所示。

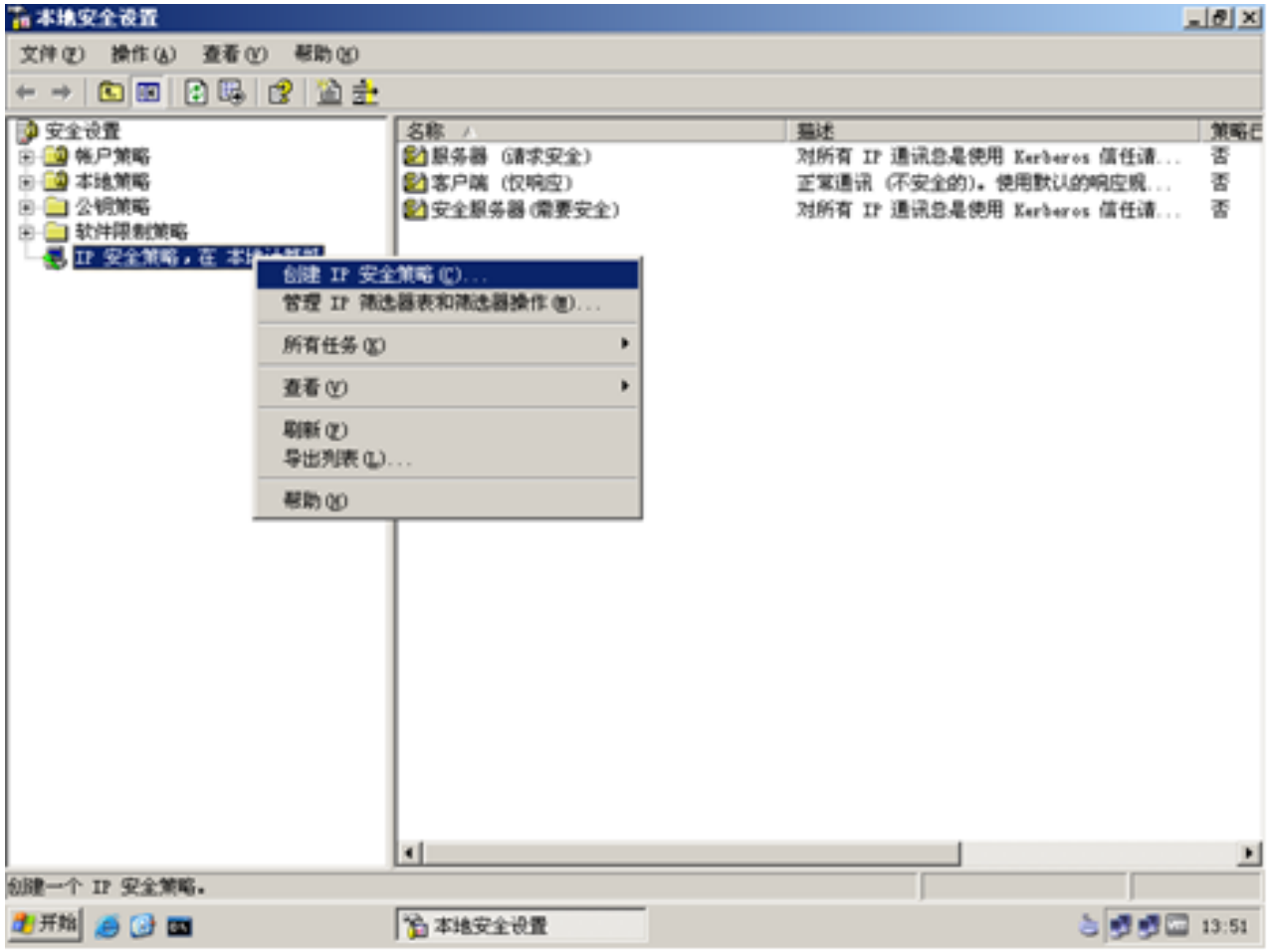


图27 创建IP安全策略

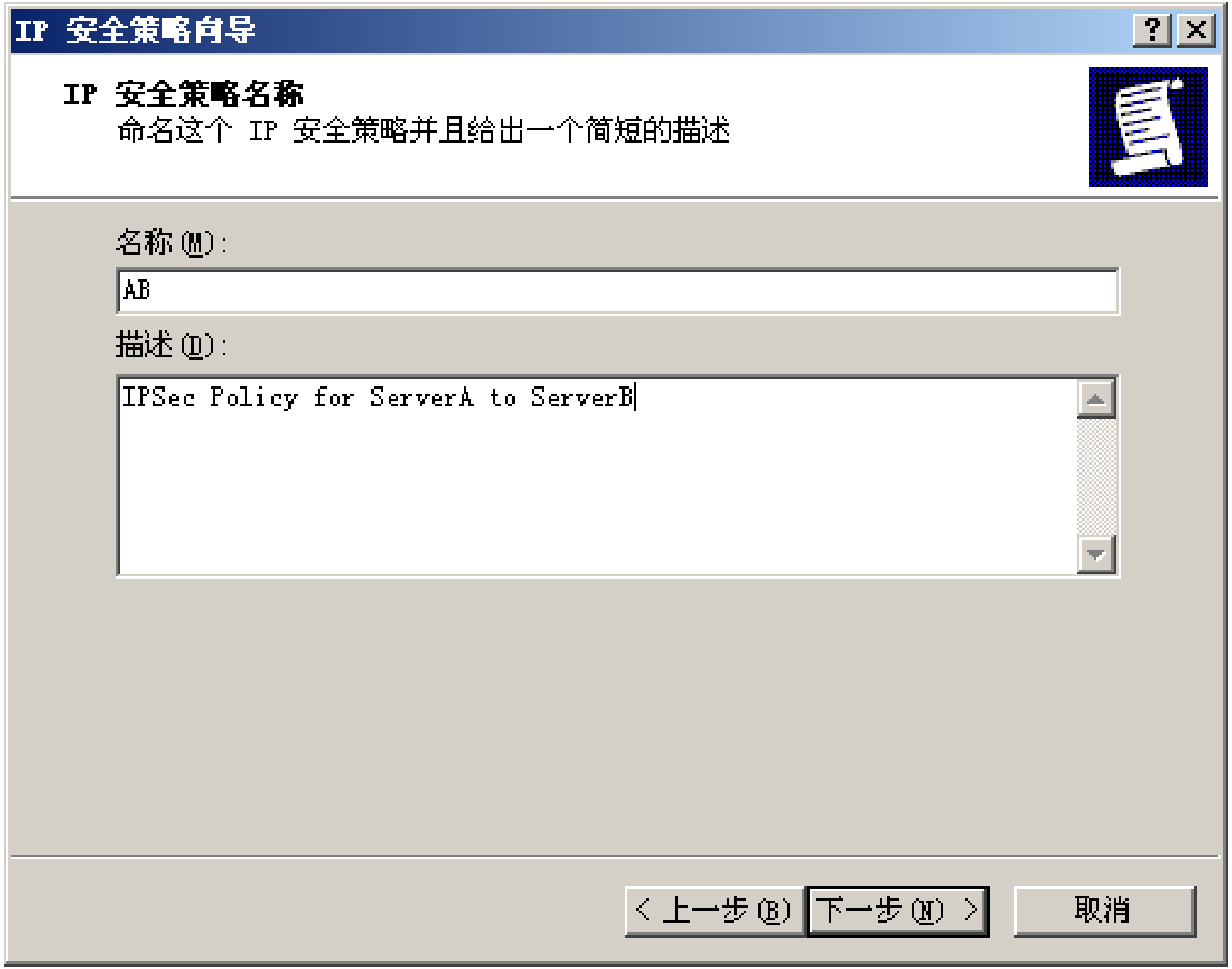


图28 打开“IP安全策略向导”，将该策略命名为”AB”

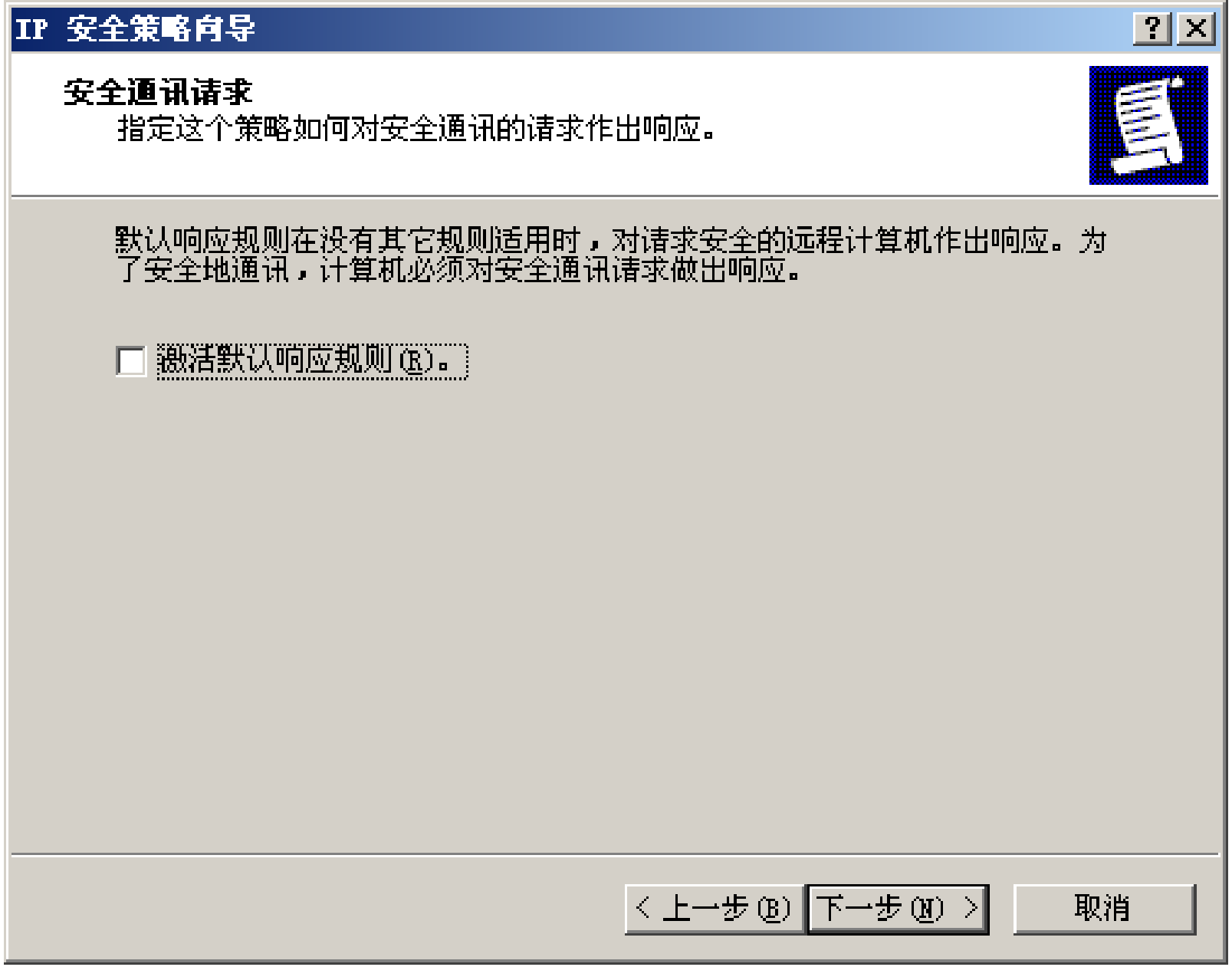


图29 取消“激活默认响应规则”

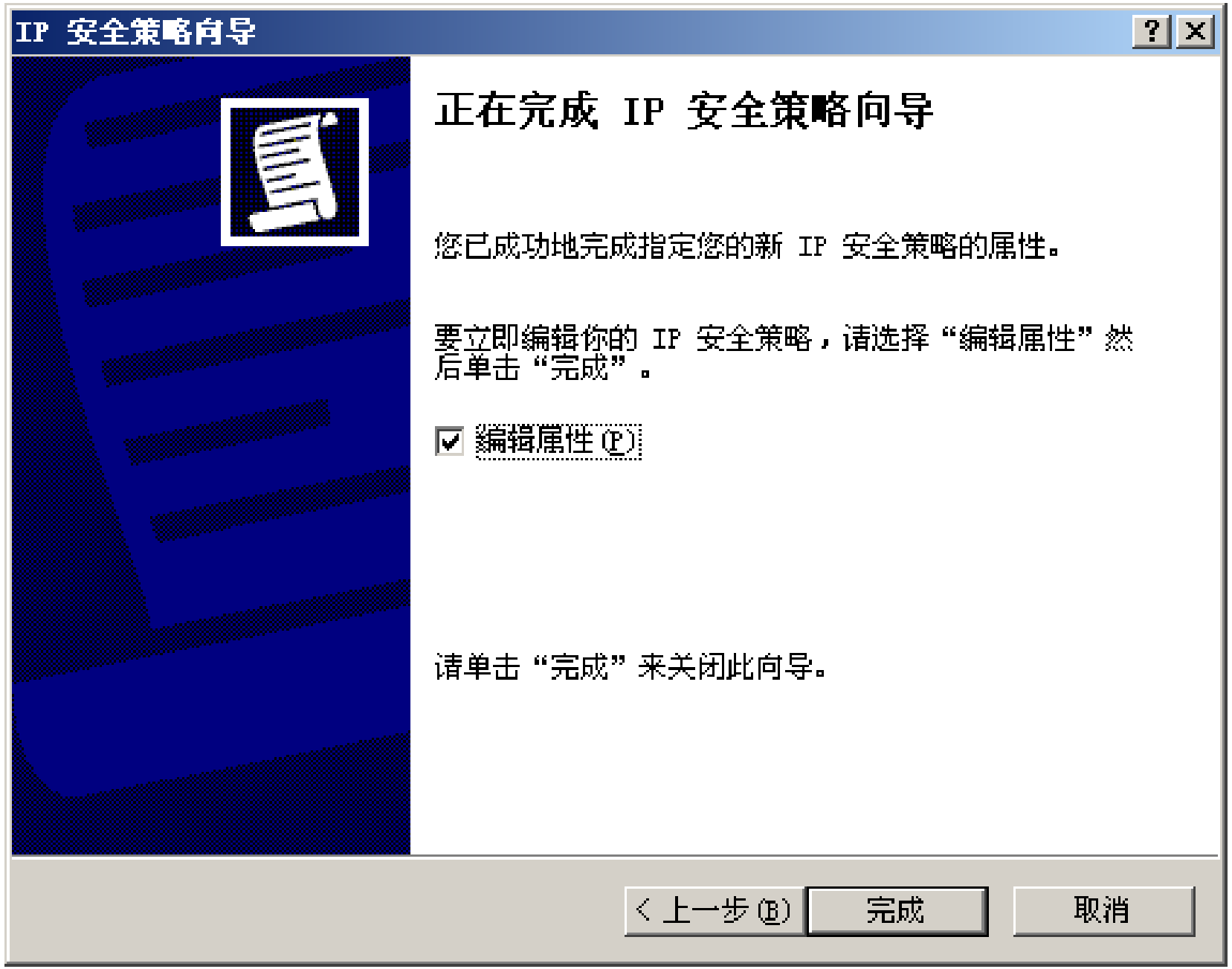

IP 安全策略向导
正在完成 IP 安全策略向导
您已成功地完成指定您的新 IP 安全策略的属性。
要立即编辑你的 IP 安全策略，请选择“编辑属性”然后单击“完成”。
编辑属性(P)
请单击“完成”来关闭此向导。
< 上一步(B)
完成
取消

图30 编辑属性

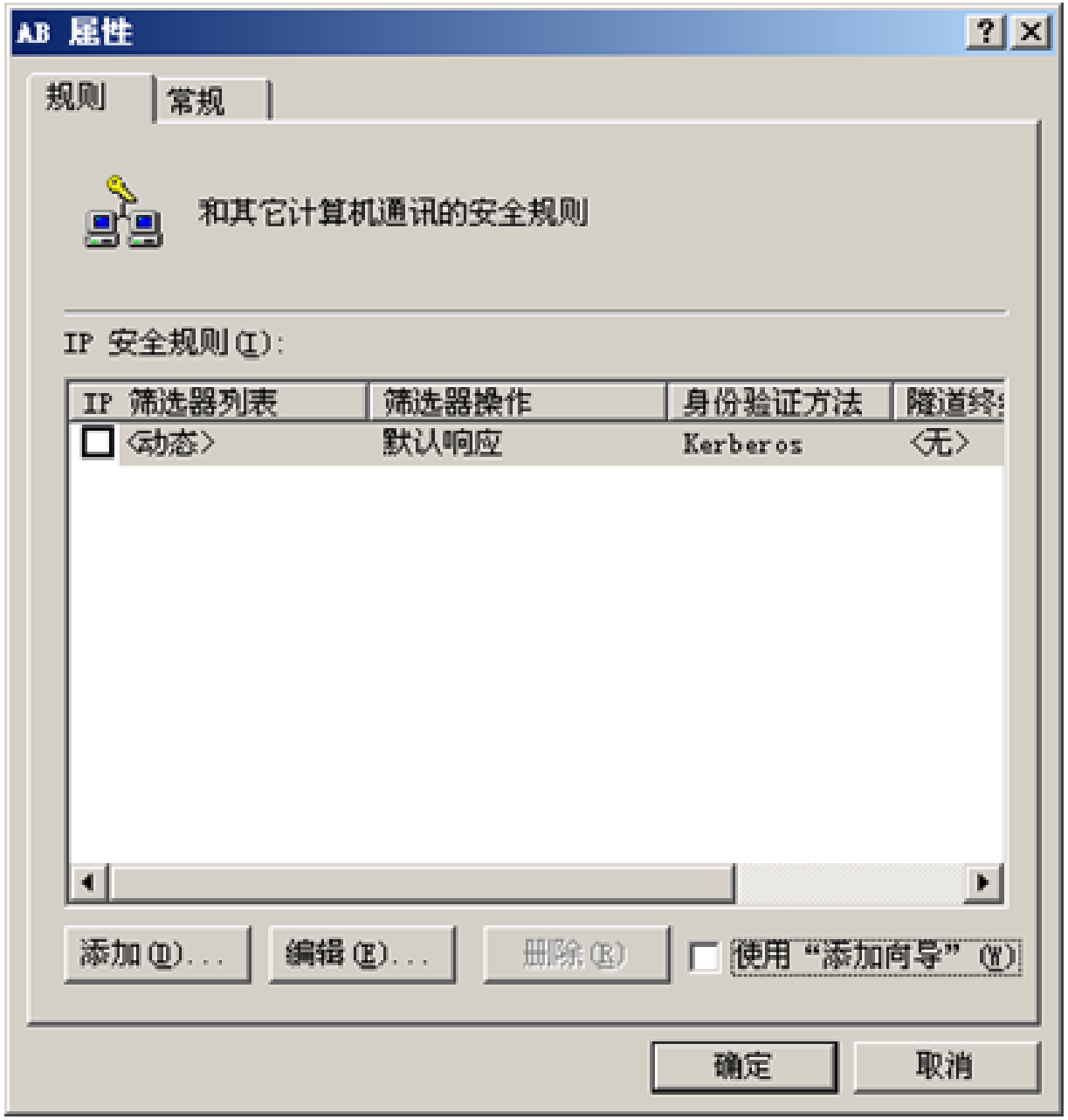


图31 打开“AB属性”编辑界面

(2) 点击“添加(D)...”，打开“新规则 属性”，选择“IP筛选器列表”属性页

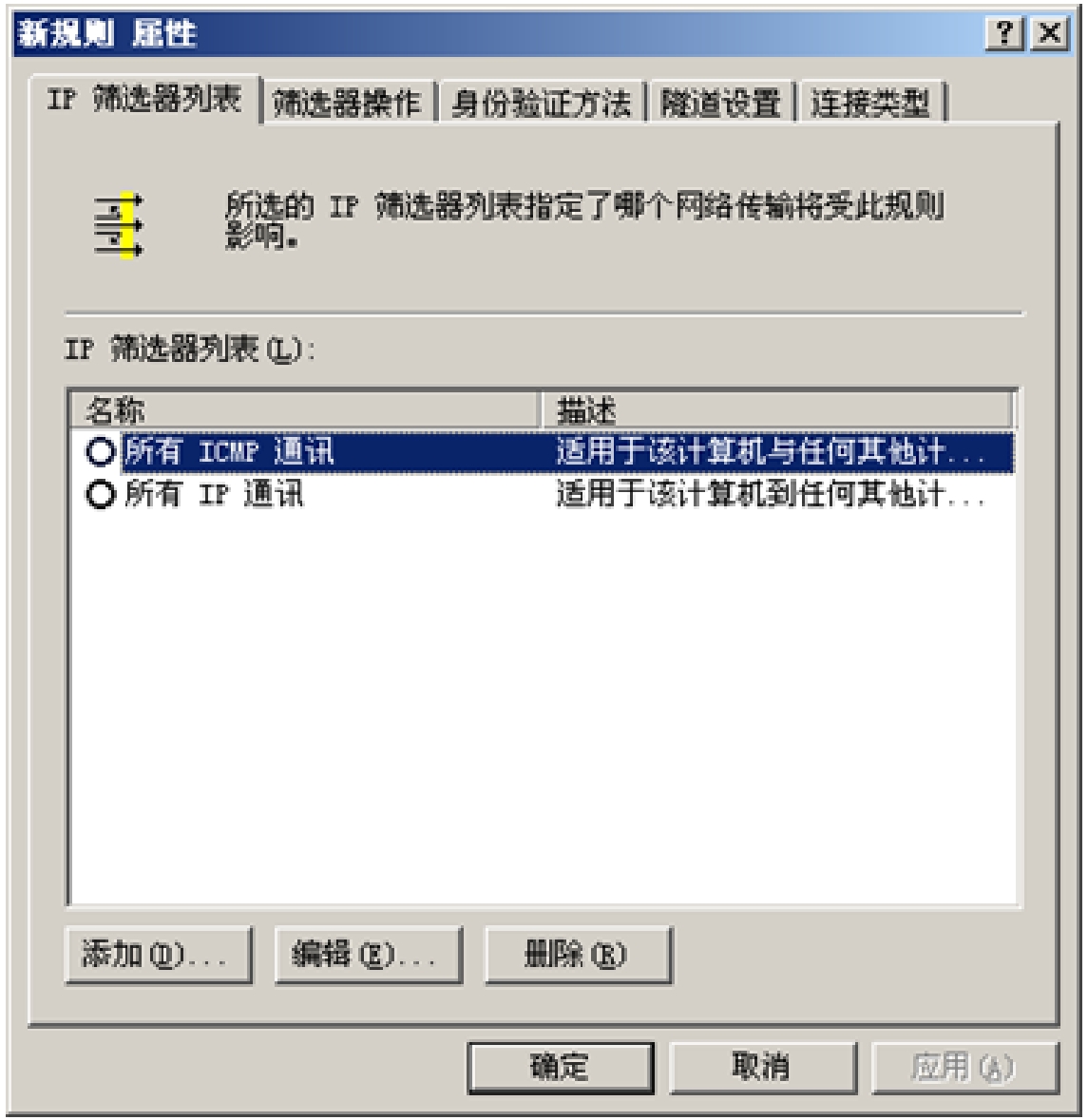


图32 选择“IP筛选器列表”属性页

点击“添加(D)...”，打开“新规则 属性”，选择“IP筛选器列表”属性，命名为“A to B”，不勾选“使用添加向导(W)”

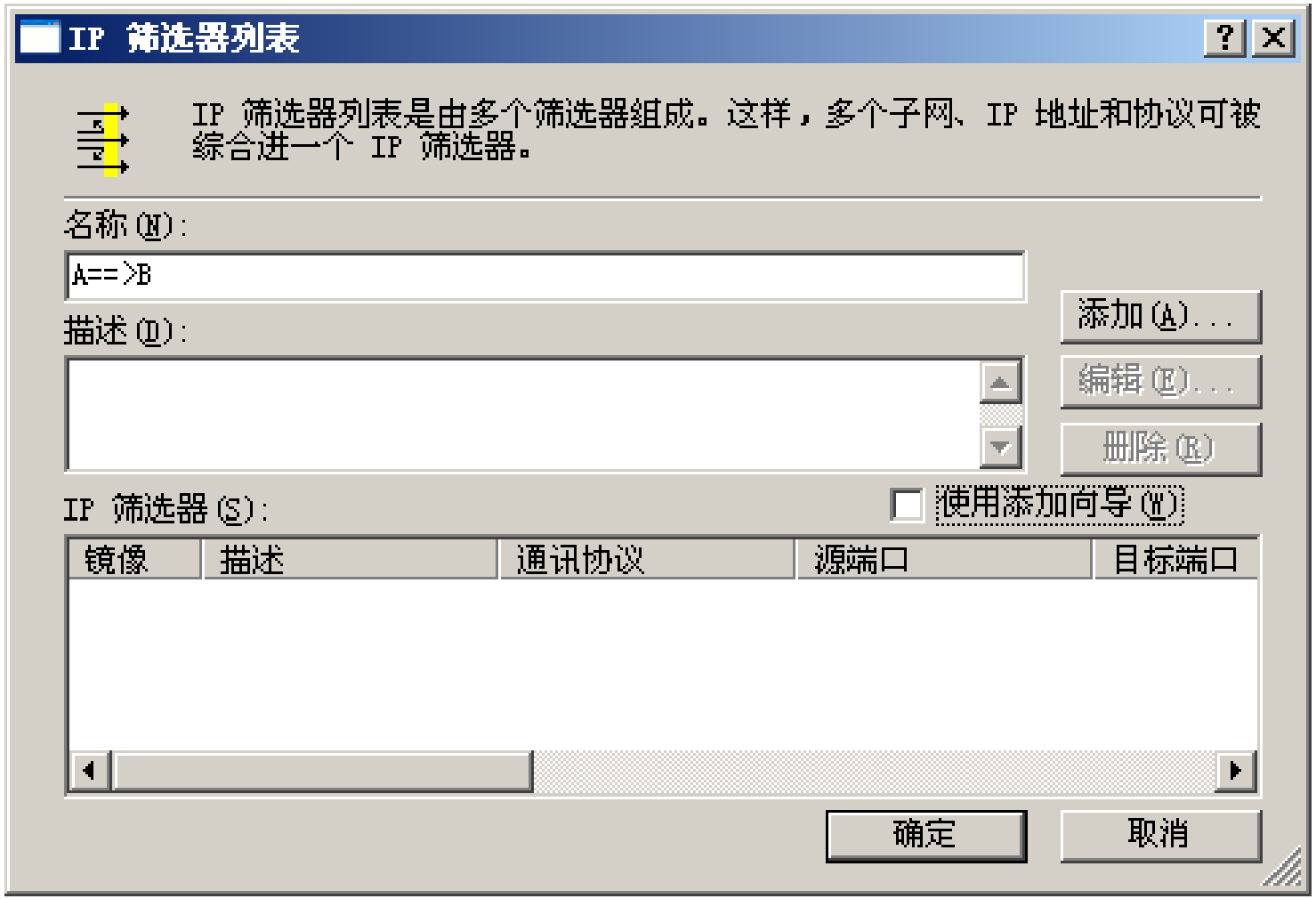


图33

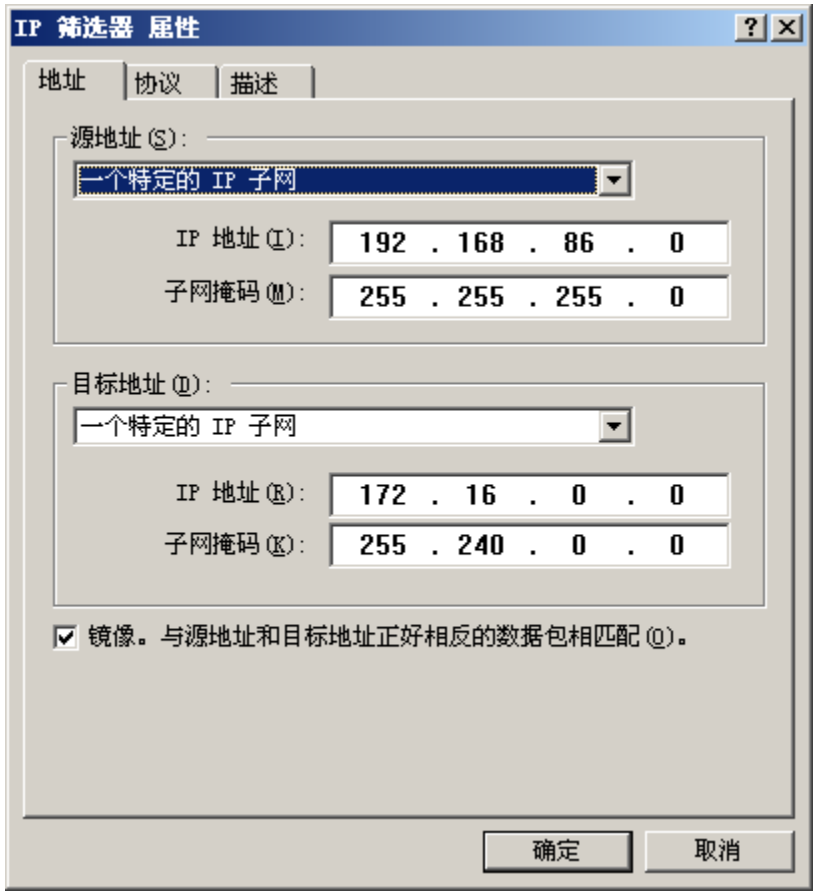


图34

- 点击“添加(A)…”，打开“IP筛选器 属性”，选择“地址”属性页，设置源地址为“一个特定的IP子网”，IP地址为192.168.86.0，子网掩码为255.255.255.0；设置目的地址为“一个特定的IP子网”，IP地址为172.16.0.0，子网掩码为255.240.0.0；不勾选“镜像”。

- 然后选择“协议”属性页，设定为默认值：“任意”。

(3)打开“新规则 属性”，选择“筛选器操作”属性页，不勾选“使用添加向导(W)”。如图35所示。

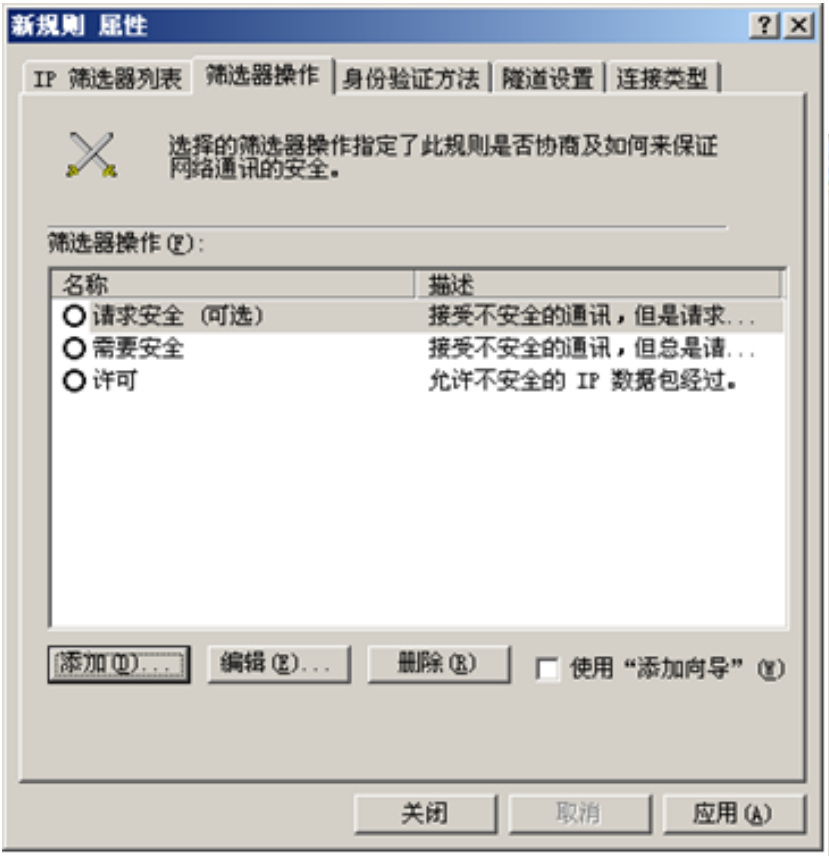


图35

然后点击“添加(D)...”，安全措施为“协商安全”，新增安全措施为“完整性和加密”，如图36所示。

图36

(4) 打开“新规则 属性”，选择“身份验证方法”属性页，点击“添加(D)...”，选择“使用此字符串（**预共享密钥**）”，**设置一个高强度的密钥（此例设为**microsoft），如图37所示

图37

(5) 打开“新规则 属性”，选择“隧道设置”属性页，指定隧道终点的IP地址(Server B的外网IP地址：166.66.66.67)

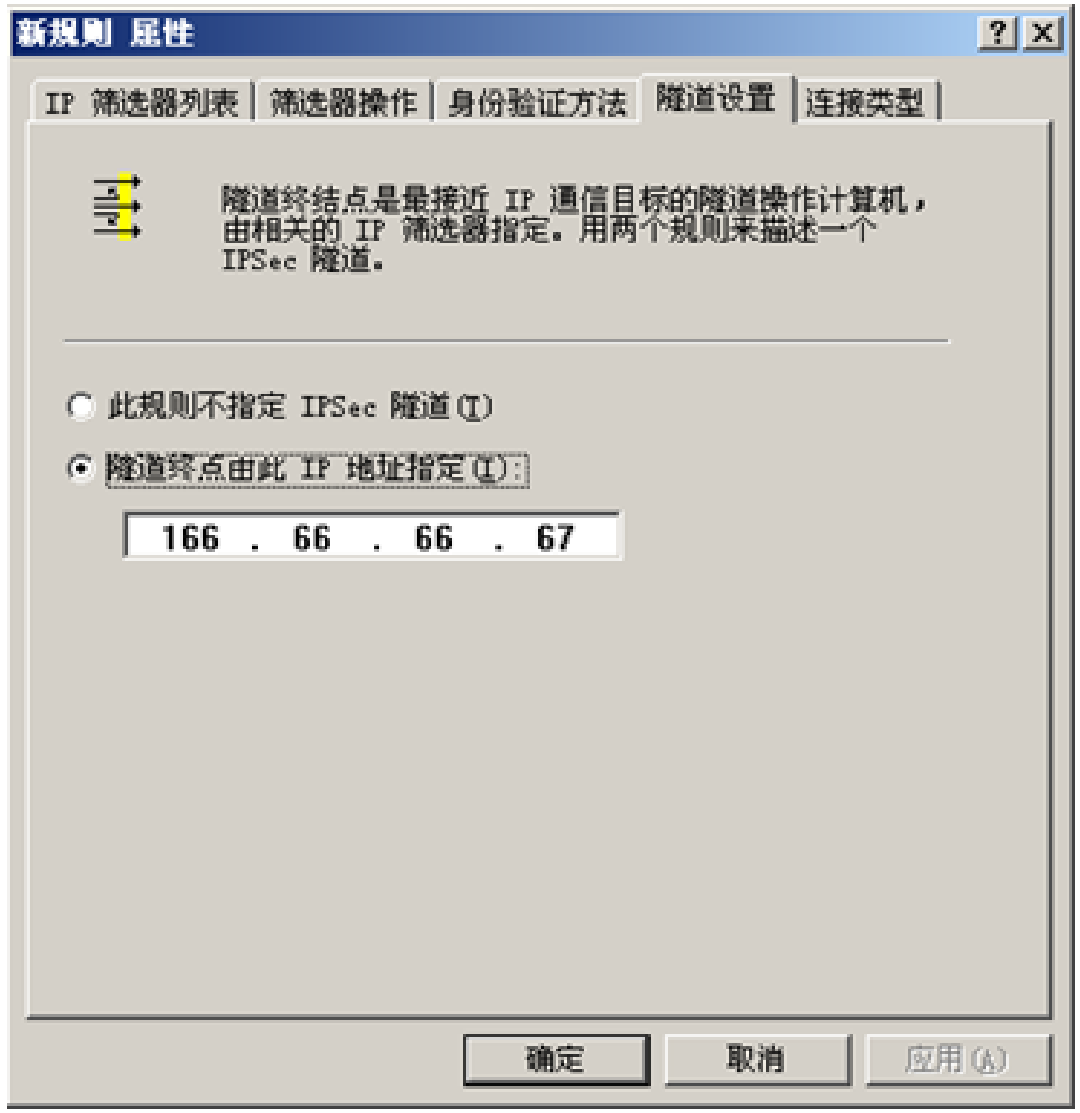


图38

(6) 打开“新规则 属性”，选择“连接类型”属性页，设置为"所有网络连接"，如图39所示

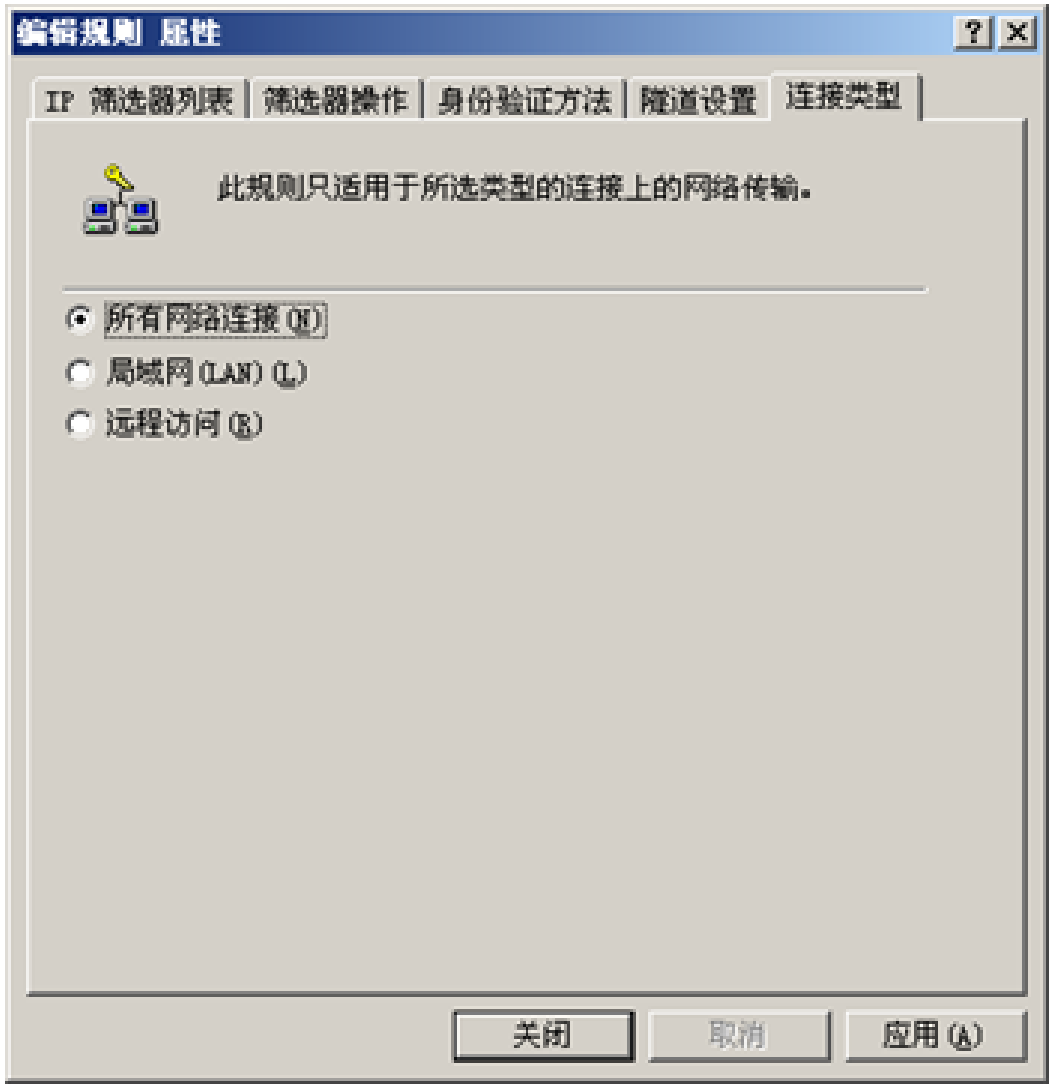


图39

(7) 重复(2)-(6)，创建IP筛选器列表“B to A”

- 设置从ServerB到ServerA的IP策略。将“源子网(IP)”和“目的子网(IP)”互换，隧道终点设置为55.55.55.56。

(8) 在本地安全设置中，右击策略“AB”并指派，如图40所示：

图40

2. 创建ServerB 的IPSec策略

- 按相同的方法步骤，创建ServerB的IP安全策略并指派。

3. 配置远程访问VPN服务器

- 配置Server A和Server B为路由器。在“开始”—“所有程序”—“管理工具”菜单中选择“路由和远程访问”，打开“路由和远程访问”管理界面，选择“配置并启用路由和远程访问”，如图41所示：


路由和远程访问
文件(F) 操作(A) 查看(V) 帮助(H)
路由和远程访问
服务器状态
SERVERA (本地)
SERVERA (本地)
配置并启用路由和远程访问(C)
禁用路由和远程访问(S)
所有任务(K)
查看(V)
删除(D)
刷新(F)
属性(R)
帮助(H)
服务器的配置
访问，在“操作”菜单上单击“配置并启用路由
程访问，部署方案，以及疑难解答的更多信息，

图41

配置为“两个专用网络之间的安全连接”。

如图42所示

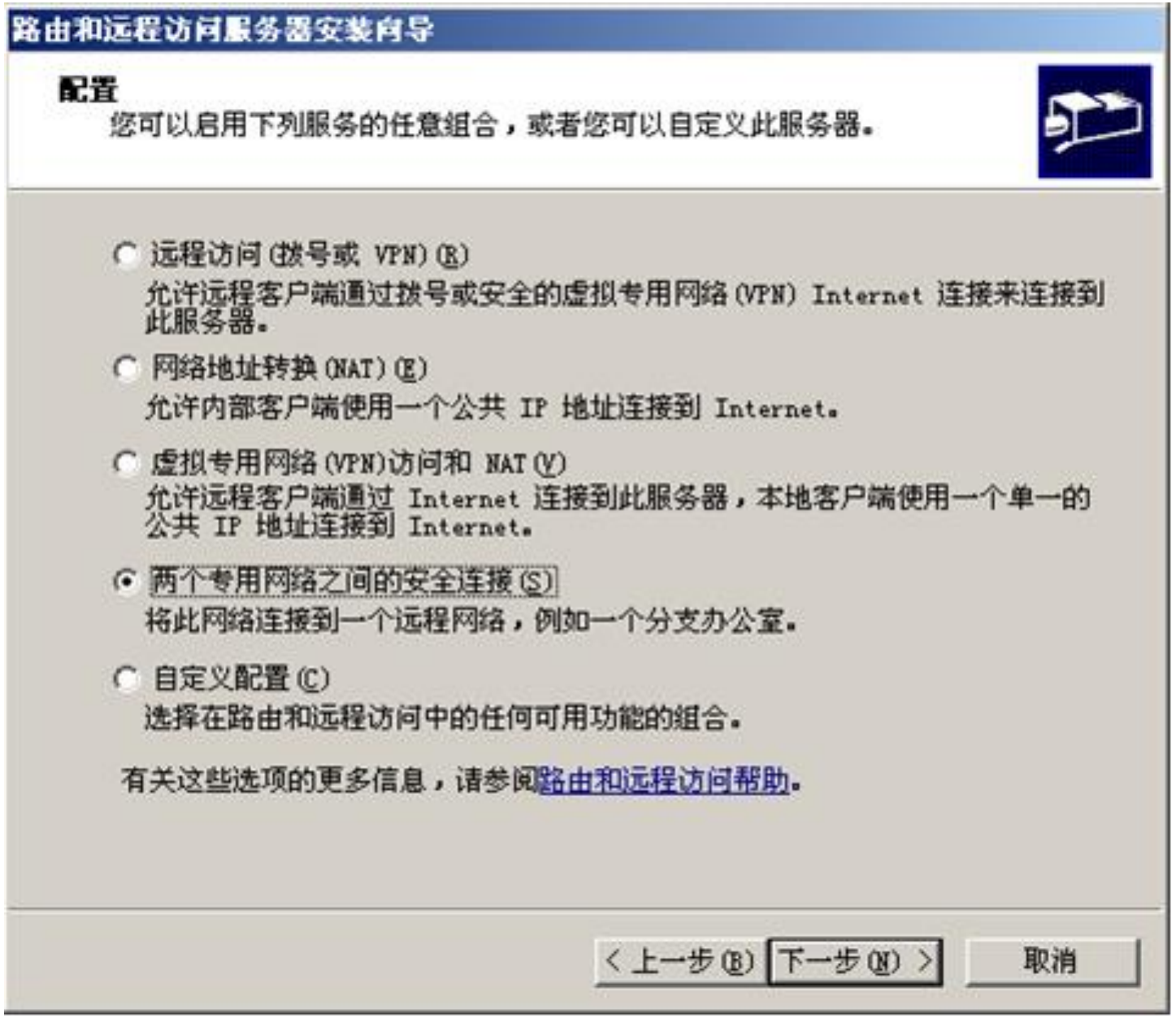


图42

不选择拨号VPN。
如图43所示

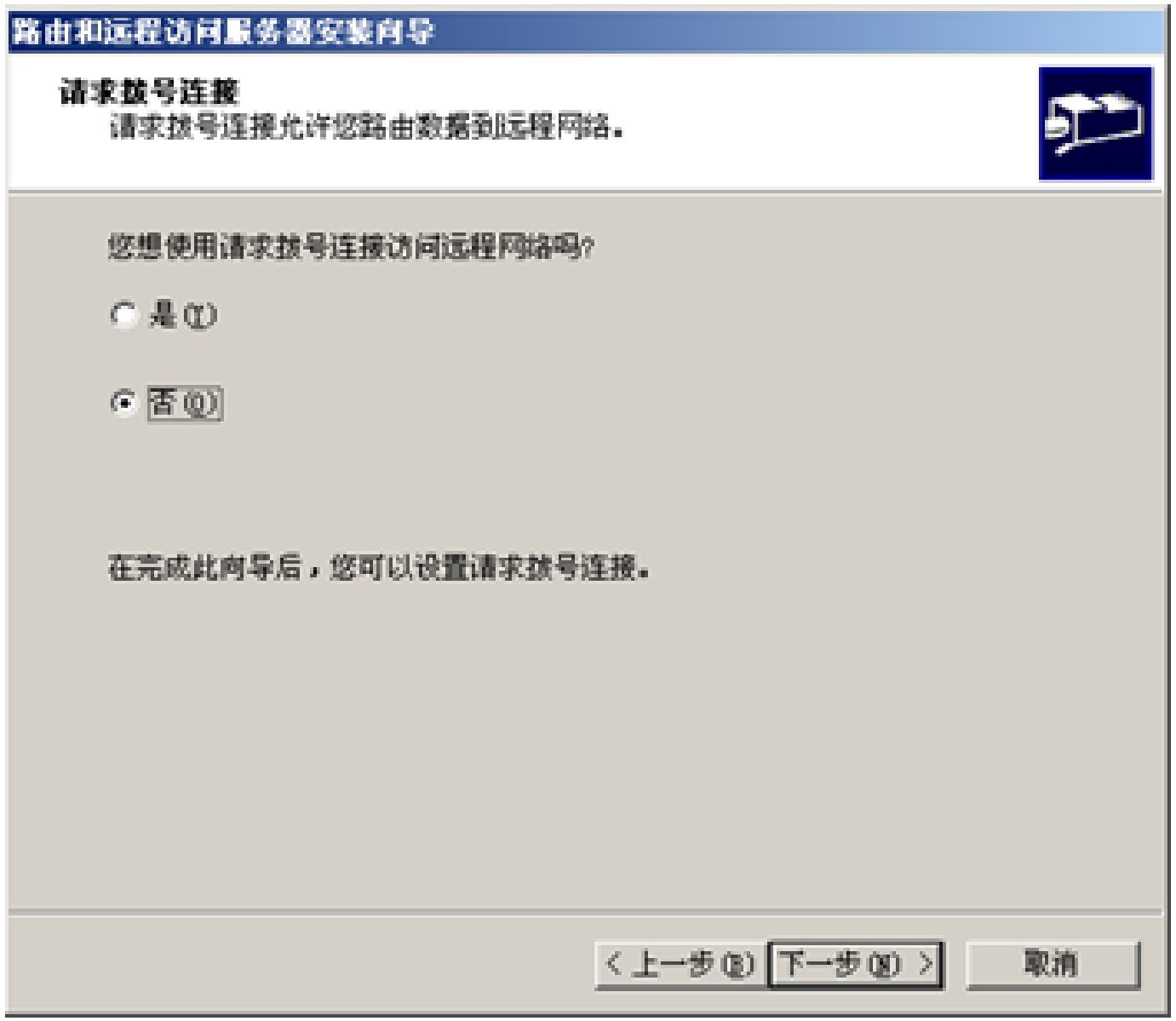


图43

4. ping测试(Client A)

- 在ClientA的cmd中输入ping 172.16.0.67（Client B的IP地址），或者在ClientB的cmd中输入ping 192.168.86.56（Client A的IP地址）。
- 如果两方的IPsec策略没有配置正确，不会ping通。如果正确则说明两个局域网互联互通。

- 在路由器中用wireshark检测到的是ESP数据包，因此实现了数据的安全保密通信。

2个局域网之间的安全通信（IPSec VPN）

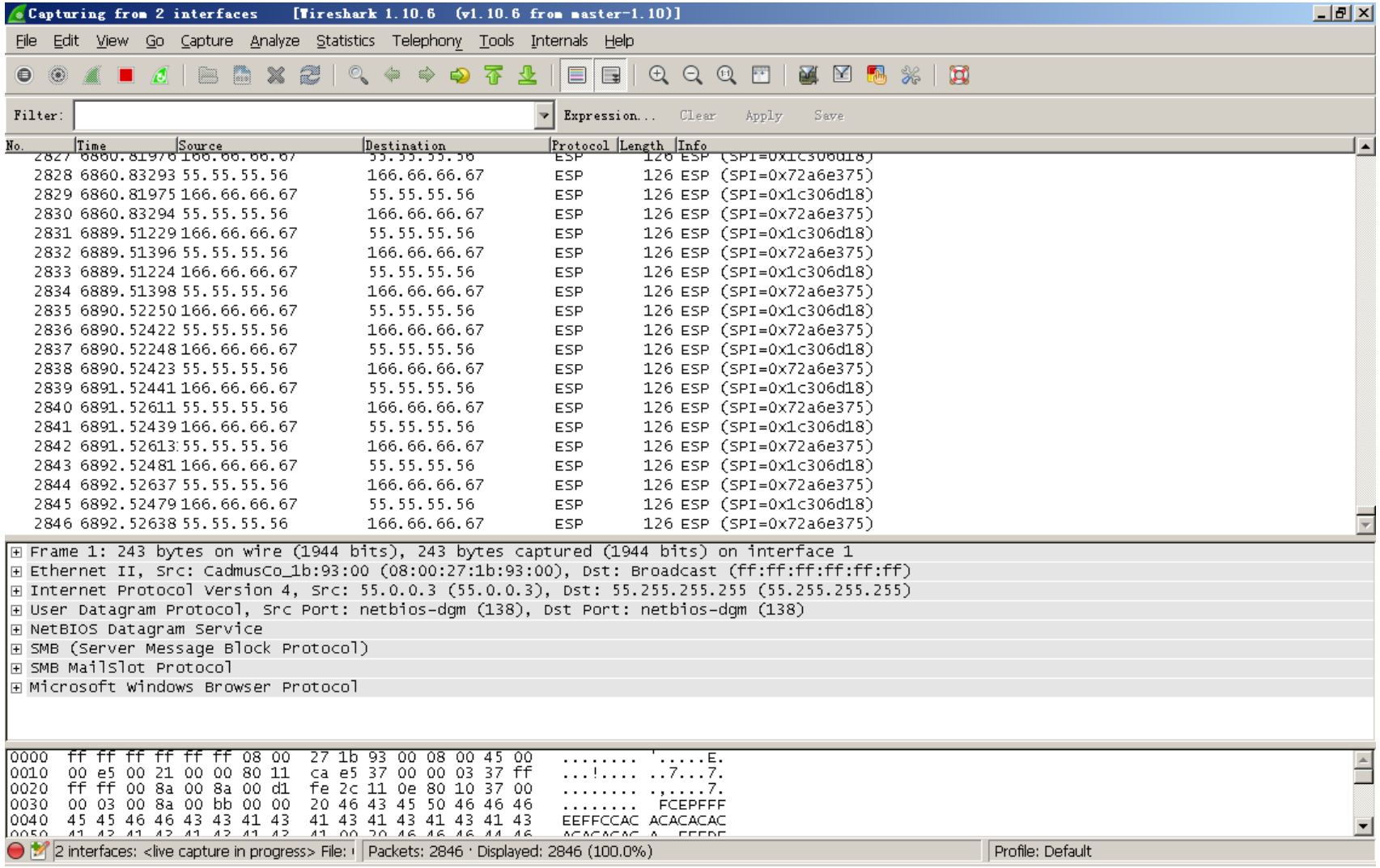


图44

New: Windows Server 2012及后续版本对VPN的支持

- Windows Server 2003的后续版本对VPN提供了支持，**配置方法是相似的**。详见另一个文档:

网络安全04-VPN技术Windows2012VPN实例

谢谢！