

第08章 应用层



讲师：韩立刚
51CTO学院金牌讲师
51CTO学院教学顾问
微软最有价值专家MVP
河北师大软件学院讲师
河北地质大学客座教授
计算机图书作者

本章重点

TCP/IPv4协议组

HTTP	FTP	SMTP	POP3	Telnet	DHCP	DNS	TFTP
TCP				UDP			
IPv4						ICMP	IGMP
ARP							
CSMA/CD		X.25	HDLC	Frame Relay		PPP	

本章内容

- 9.1 域名系统DNS
- 9.2 动态主机配置协议DHCP
- 9.3 Telnet协议
- 9.4 远程桌面协议（RDP）
- 9.5 超级文本传输协议HTTP
- 9.6 文件传输协议FTP
- 9.7 发送电子邮件的协议SMTP
- 9.8 接收电子邮件的协议POP3和IMAP

9.1域名系统DNS

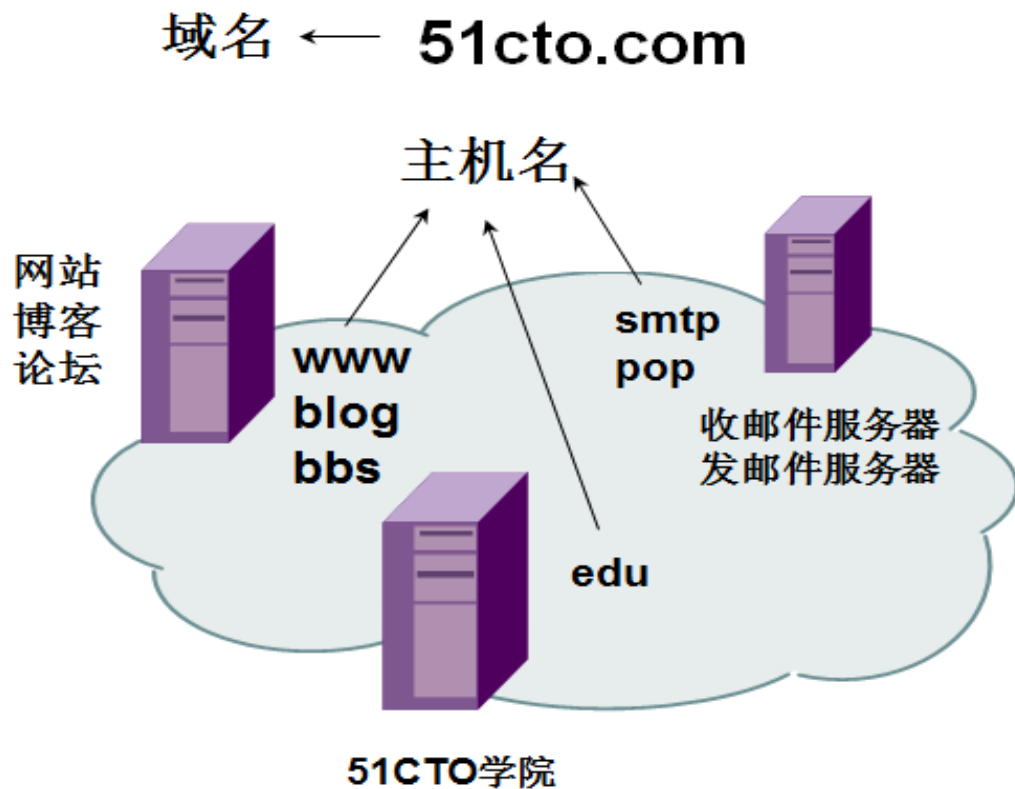
- 9.1.1什么是域名
- 9.1.2域名的结构
- 9.1.3Internet中的域名服务器
- 9.1.4域名解析过程
- 9.1.5实战1：搭建企业内网的DNS服务
- 9.1.6实战2：测试域名解析
- 9.1.7实战3：抓包分析域名解析的过程

9.1.1 什么是域名

- 整个Internet网站和各种服务器数量众多，各个组织的服务器都需要给一个名称，这就很容易重名。如何确保Internet上的服务器名称在整个Internet唯一呢？这就需要Internet上有域名管理认证机构进行统一管理。如果你的公司在互联网上有一组服务器（邮件服务器、FTP服务器、Web服务器等），你需要为你的公司先申请一个域名，也就是向管理认证机构注册一个域名。
- 域名的注册遵循先申请先注册为原则，管理认证机构要确保每一个域名的注册都是独一无二、不可重复的。

9.1.2域名的结构1

- 一个域名下可以有多个主机，域名全球唯一，主机名+域名肯定也是全球唯一的，主机名+域名称为完全限定域名（FQDN）。
- FQDN是Fully Qualified Domain Name的缩写, 含义是完整的域名。例如，一台机器主机名（hostname）是www, 域名后缀（domain）是51cto.com, 那么该主机的FQDN应该是www.51cto.com.。



完全限定域名

↑

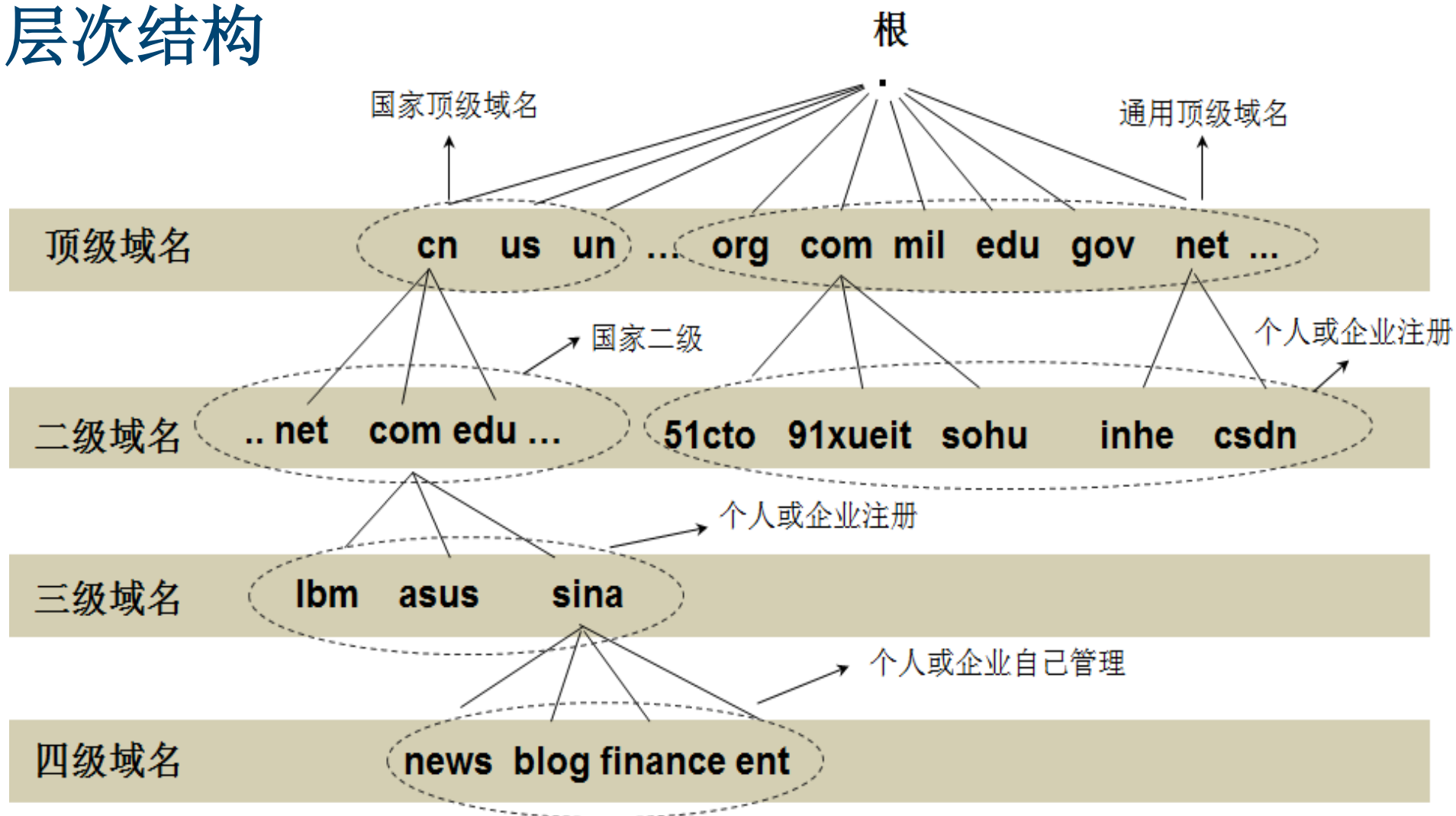
www.51cto.com.
blog.51cto.com.
bbs.51cto.com.
edu.51cto.com.
smtp.51cto.com.
pop.51cto.com.

↓ ↓

主机名 域名

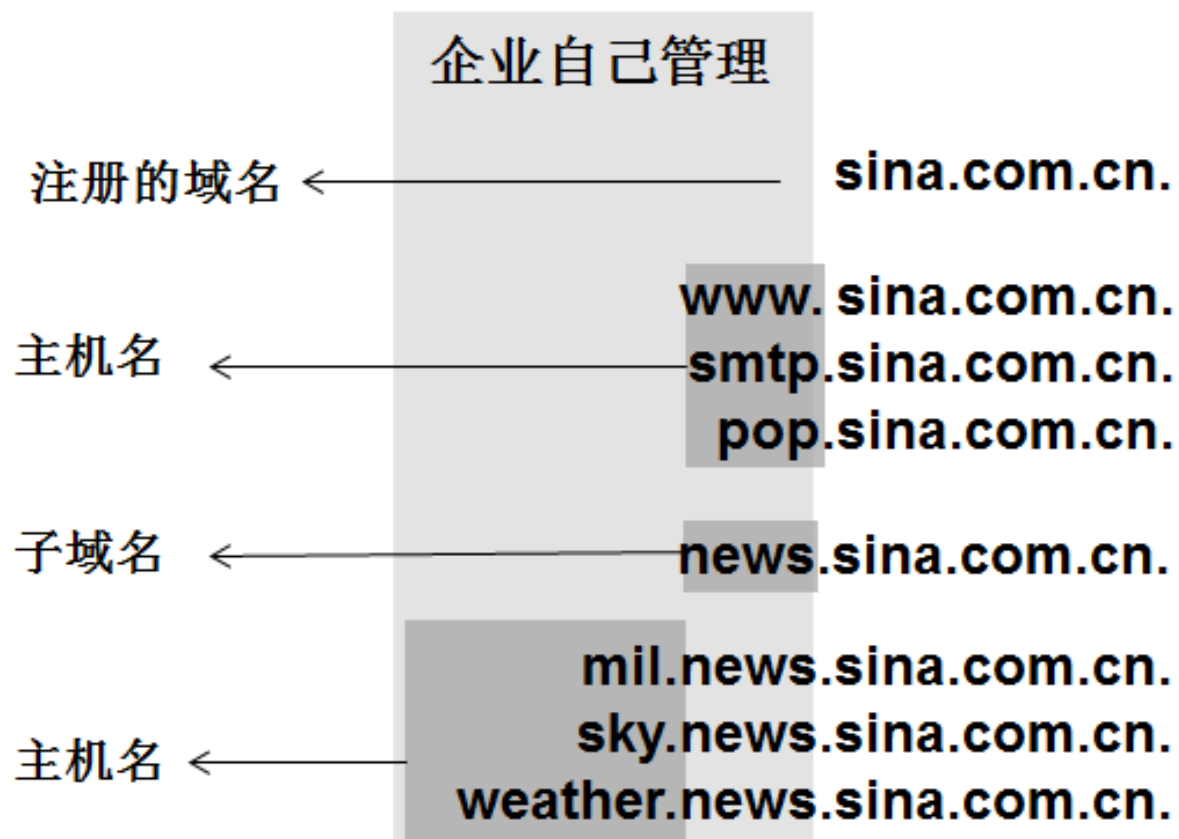
9.1.2域名的结构2

■ 域名的层次结构



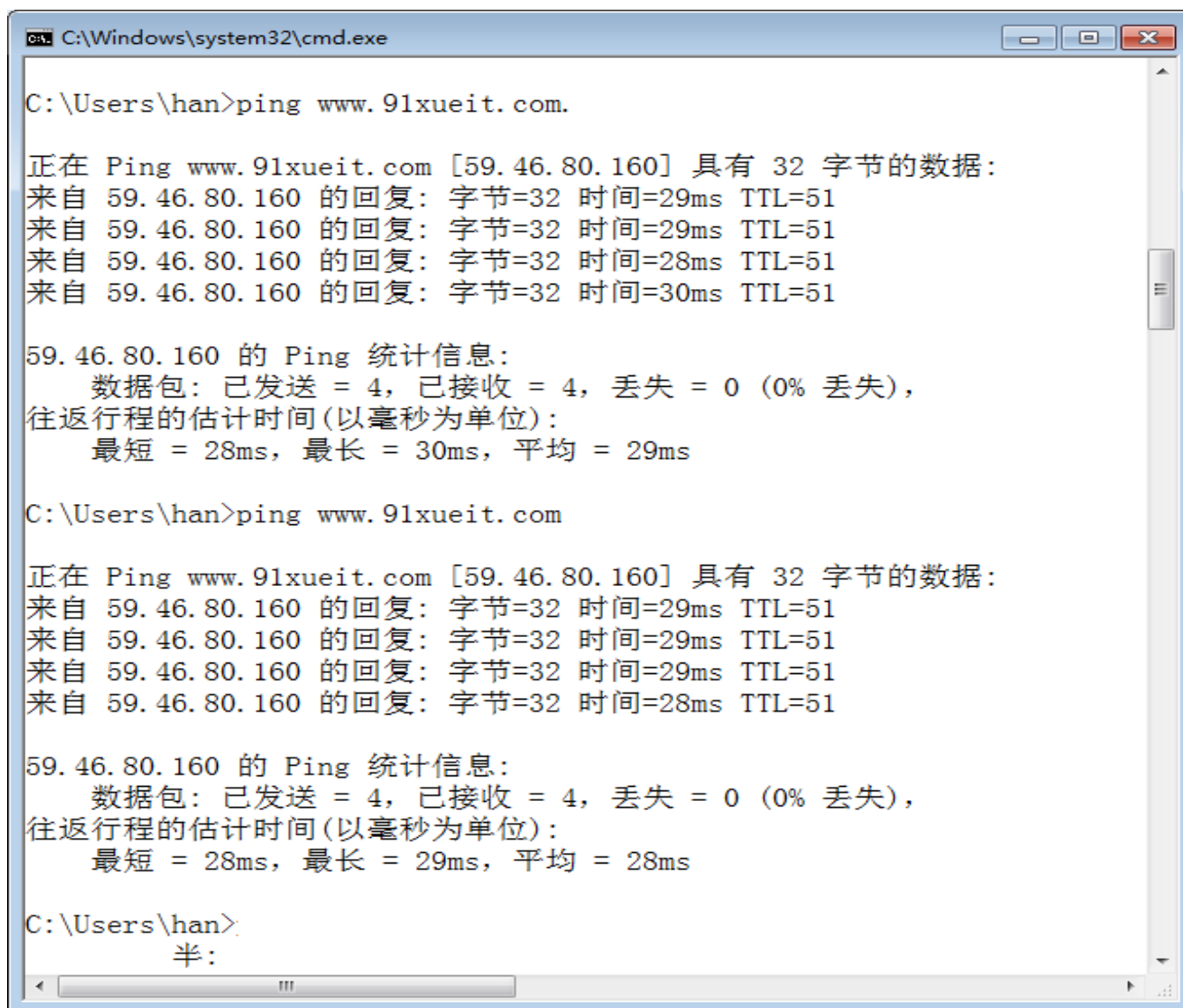
9.1.2域名的结构3

- 企业或个人申请了域名后，可以在该域名下添加多个主机名，也可以根据需要创建子域名，子域名下面，亦可以有多个主机名，



9.1.2域名的结构4

- 所有域名都是以开始，不过我们在使用时，域名最后的经常被省去，如图所示，在命令提示符下ping **www.91xueit.com.**和ping **www.91xueit.com**是一样的。



```
C:\Windows\system32\cmd.exe

C:\Users\han>ping www.91xueit.com.

正在 Ping www.91xueit.com [59.46.80.160] 具有 32 字节的数据:
来自 59.46.80.160 的回复: 字节=32 时间=29ms TTL=51
来自 59.46.80.160 的回复: 字节=32 时间=29ms TTL=51
来自 59.46.80.160 的回复: 字节=32 时间=28ms TTL=51
来自 59.46.80.160 的回复: 字节=32 时间=30ms TTL=51

59.46.80.160 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 28ms, 最长 = 30ms, 平均 = 29ms

C:\Users\han>ping www.91xueit.com

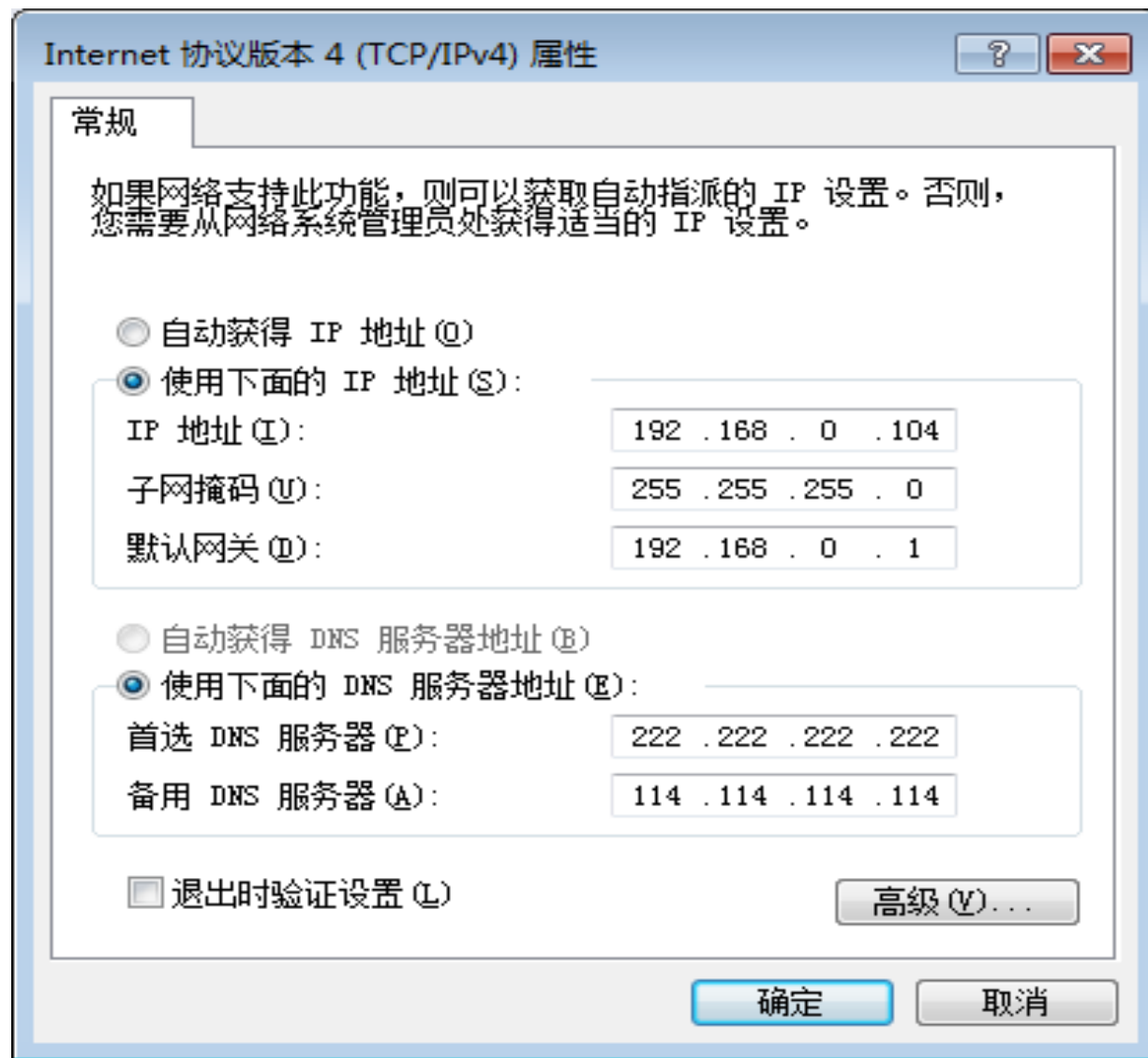
正在 Ping www.91xueit.com [59.46.80.160] 具有 32 字节的数据:
来自 59.46.80.160 的回复: 字节=32 时间=29ms TTL=51
来自 59.46.80.160 的回复: 字节=32 时间=29ms TTL=51
来自 59.46.80.160 的回复: 字节=32 时间=29ms TTL=51
来自 59.46.80.160 的回复: 字节=32 时间=28ms TTL=51

59.46.80.160 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 28ms, 最长 = 29ms, 平均 = 28ms

C:\Users\han>
```

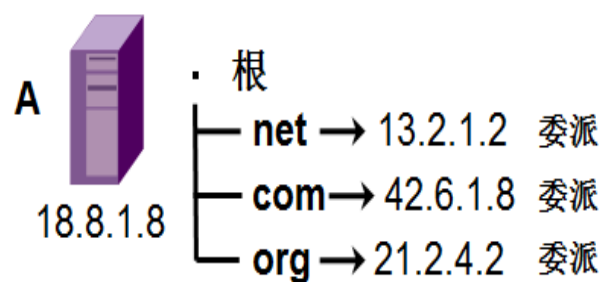
9.1.3 Internet 中的域名服务器

■ 当我们通过域名访问网站或点击网页中的超链接跳转到其他网站，计算机需要将域名解析成 IP 地址才能访问这些网站。DNS 服务器负责域名解析，因此你必须配置计算机使用哪些 DNS 服务器进行域名解析。

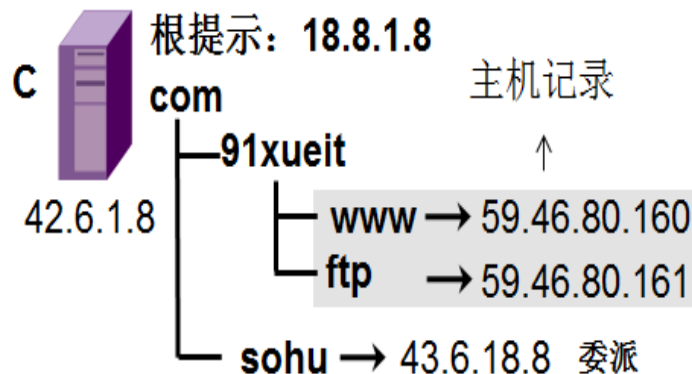
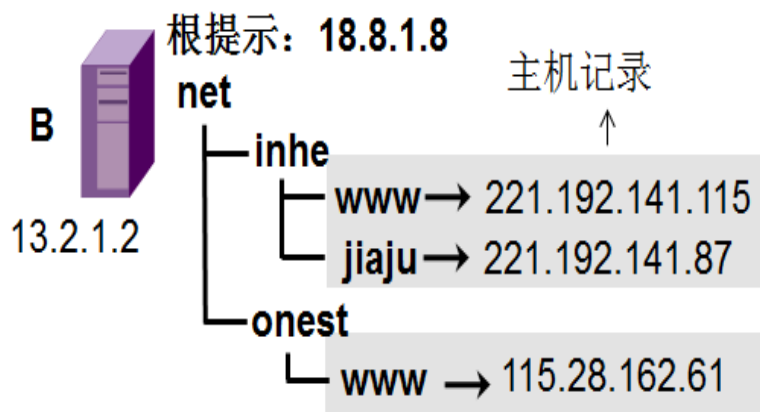


DNS 服务器的 层次

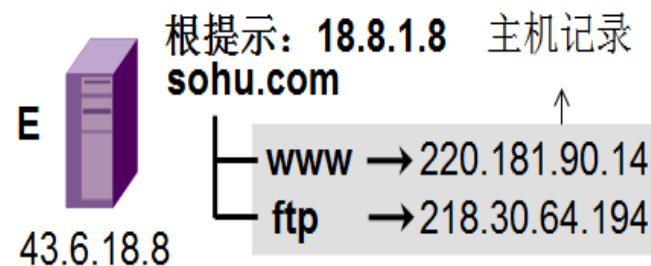
根域名服务器



顶级域名服务器

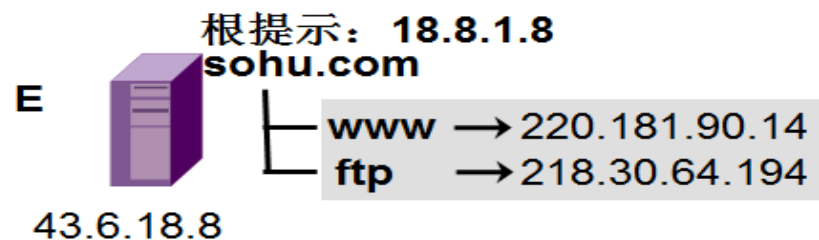
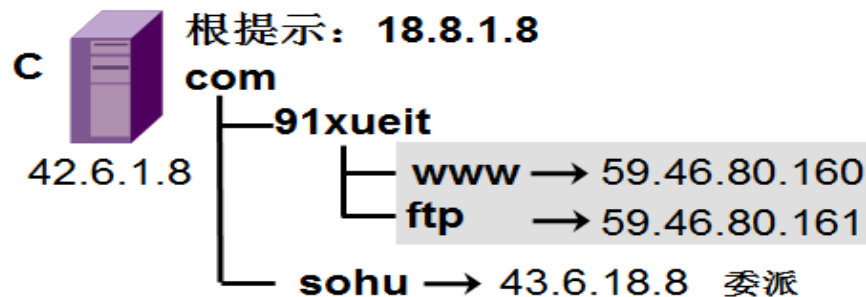
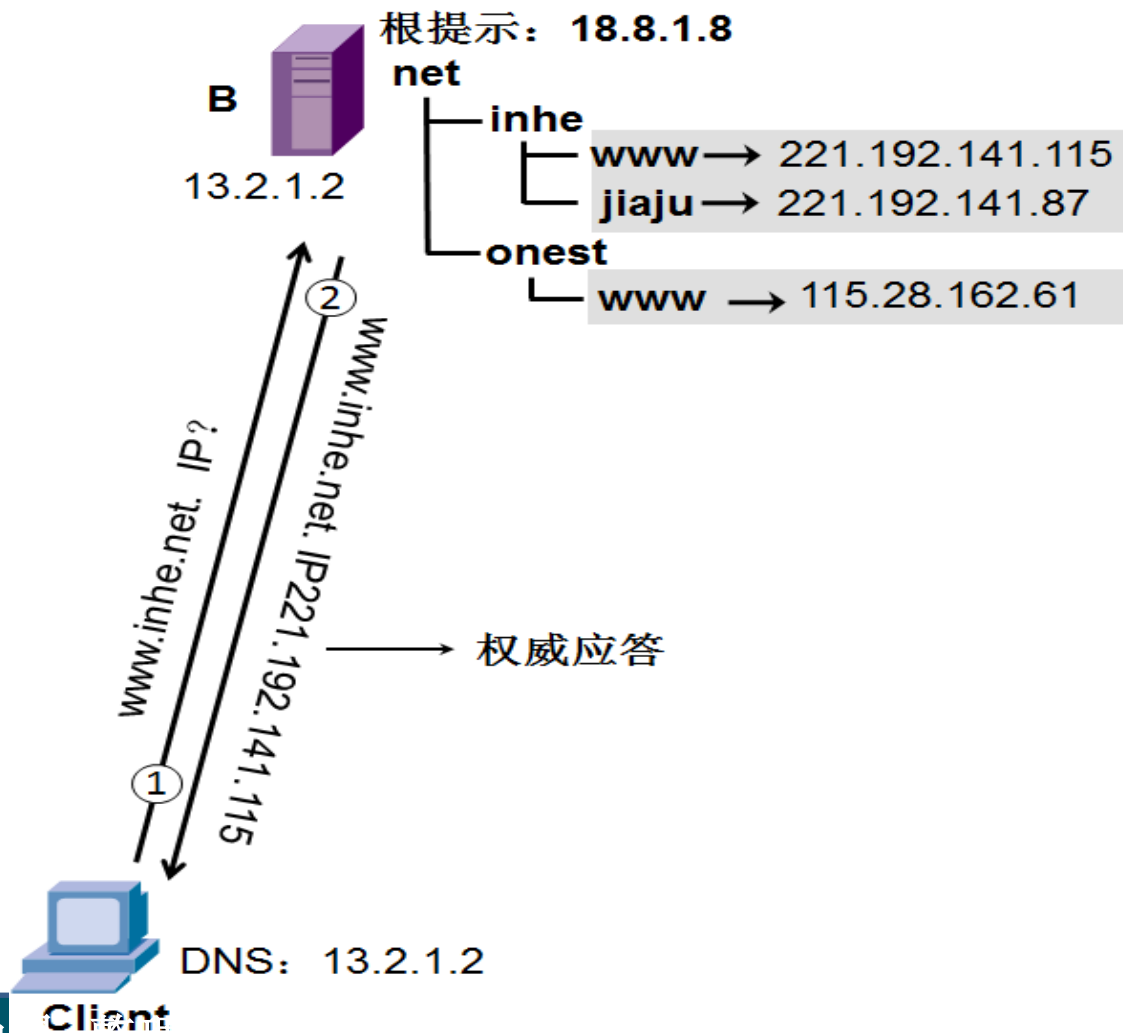
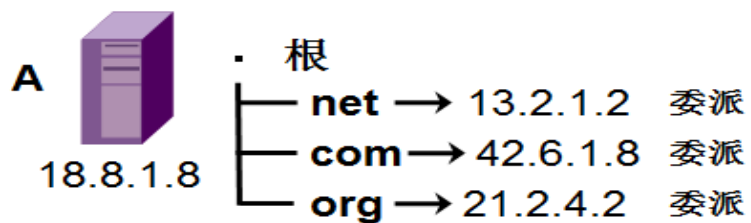


三级域名服务器



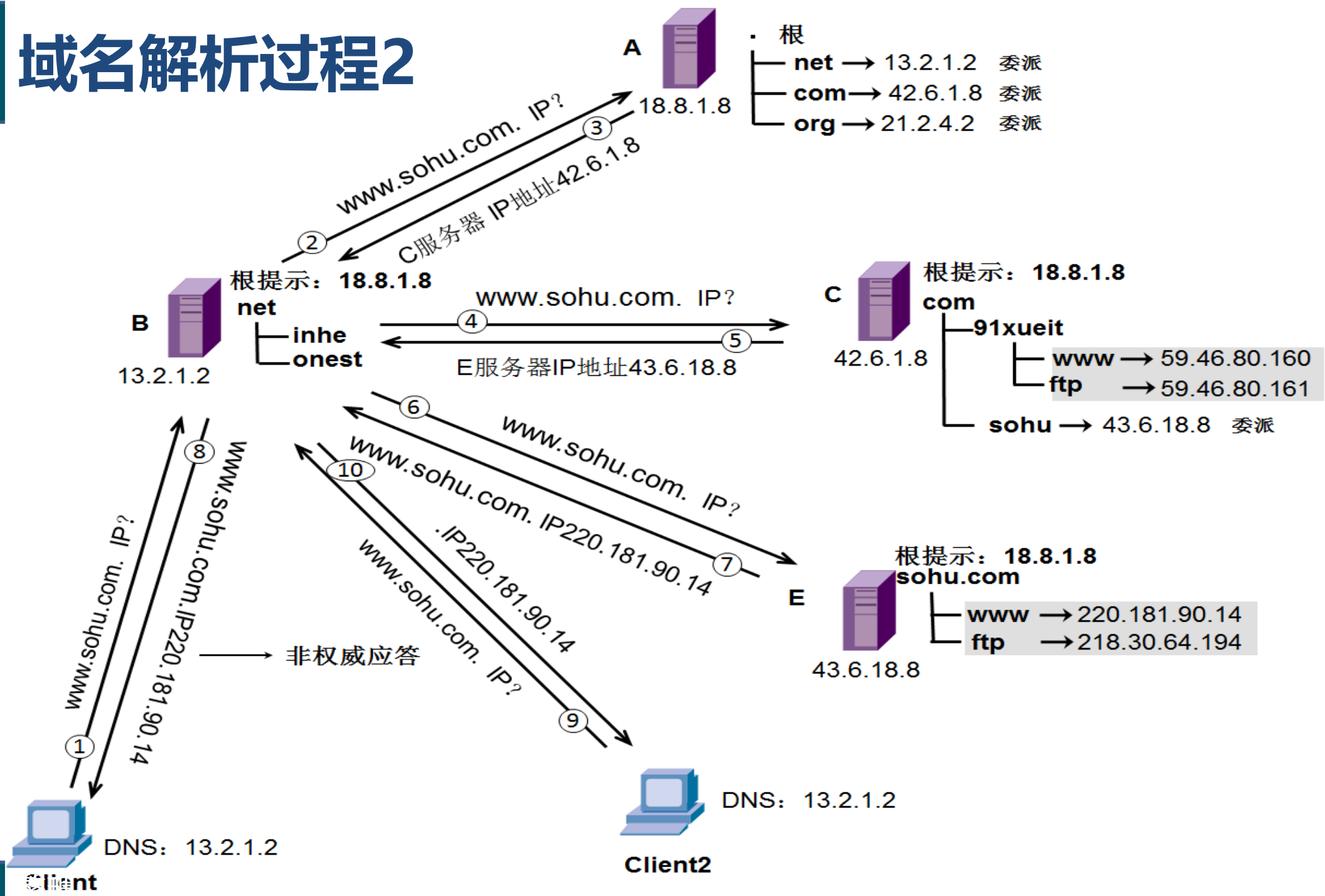
9.1.4

域名解析过程1



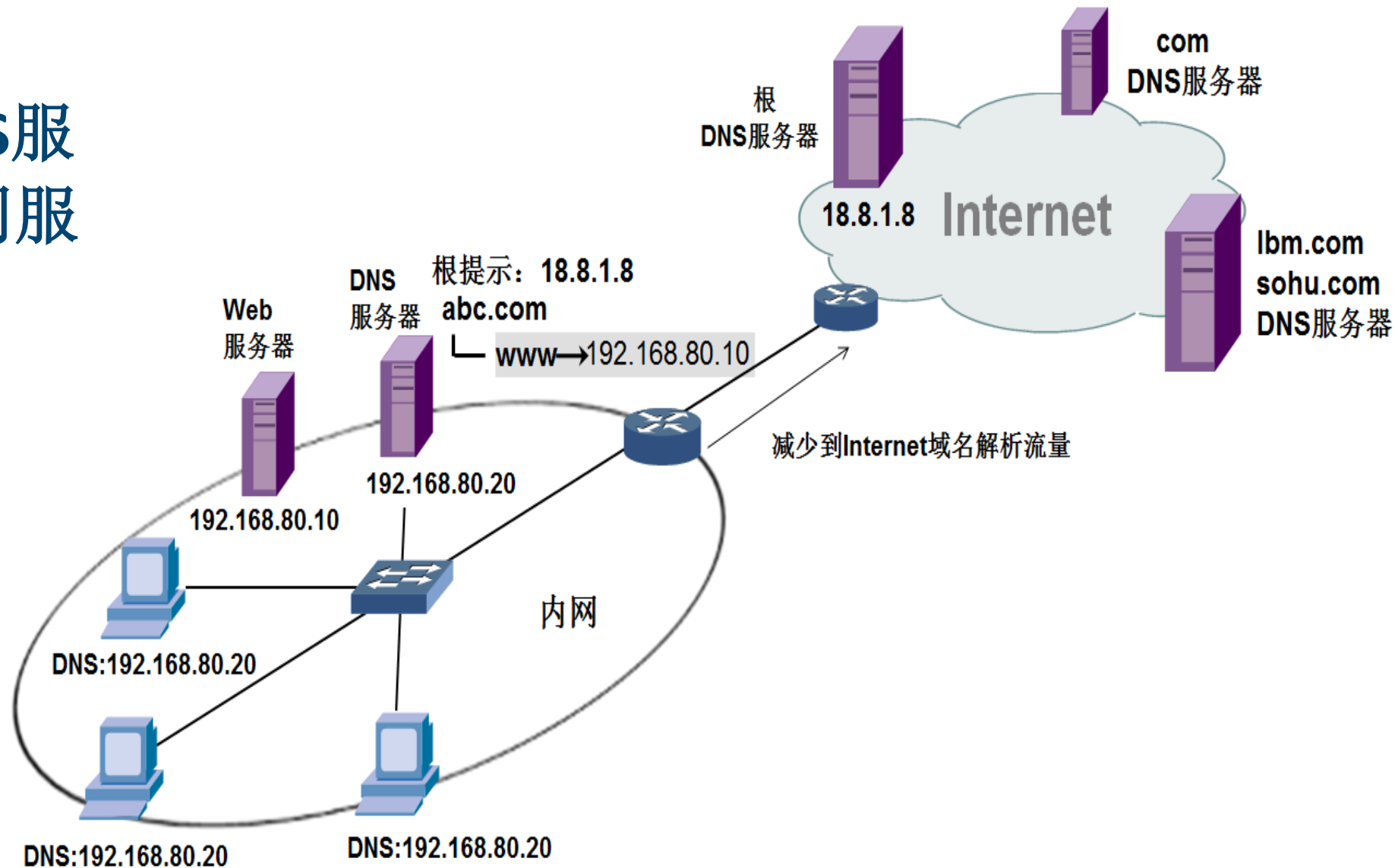
9.1.4

域名解析过程2



9.1.5实战1：搭建企业内网的DNS服务

■搭建内网DNS服务器解析内网服务器域名



9.1.6实战2：测试域名解析

- 使用`ipconfig /displaydns`显示本地缓存的域名解析结果。
- 使用`ipconfig /flushdns`清空缓存的结果。
- 使用`nslookup`命令测试域名解析，在DNS服务器查看缓存的结果。

9.1.7实战3

抓包分析域名解析的过程

WindowXP域名解析请求

DNS服务器转发到根DNS

返回负责的DNS服务器

向负责的DNS服务器转发请求

返回解析的最终结果

向WindowsXP发送解析结果

返回两个负责51cto.com域名解析的DNS服务器域名

负责51cto.com域名解析的全部DNS服务器IP地址

DNS.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Vmware_cc:87:22	Broadcast	ARP	60	who has 192.168.80.20? Tell 192.168.80.111
2	0.00004500	Vmware_14:bf:02	Vmware_cc:87:22	ARP	42	192.168.80.20 is at 00:0c:29:14:bf:02
3	0.00042000	192.168.80.111	192.168.80.20	DNS	73	Standard query 0xbfad A www.51cto.com
4	0.00063200	192.168.80.20	192.43.172.30	DNS	73	Standard query 0x089a A www.51cto.com
5	0.19443100	Vmware_f4:11:93	Broadcast	ARP	60	who has 192.168.80.20? Tell 192.168.80.1
6	0.19446200	Vmware_14:bf:02	Vmware_f4:11:93	ARP	42	192.168.80.20 is at 00:0c:29:14:bf:02
7	0.19470200	192.43.172.30	192.168.80.20	DNS	291	Standard query response 0x089a
8	0.19517000	192.168.80.20	220.249.242.11	DNS	73	Standard query 0x089a A www.51cto.com
9	0.24812700	220.249.242.11	192.168.80.20	DNS	204	Standard query response 0x089a CNAME web.dn
10	0.24835800	192.168.80.20	192.168.80.111	DNS	204	Standard query response 0xbfad CNAME web.dn
11	0.26479700	Vmware_cc:87:22	Broadcast	ARP	60	who has 192.168.80.1? Tell 192.168.80.111

Frame 7: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface 0

Ethernet II, Src: Vmware_f4:11:93 (00:50:56:f4:11:93), Dst: Vmware_14:bf:02 (00:0c:29:14:bf:02)

Internet Protocol Version 4, Src: 192.43.172.30 (192.43.172.30), Dst: 192.168.80.20 (192.168.80.20)

User Datagram Protocol, Src Port: 53 (53), Dst Port: 1030 (1030)

Domain Name System (response)

[Request In: 4]

[Time: 0.194070000 seconds]

Transaction ID: 0x089a

Flags: 0x8000 standard query response, No error

Questions: 1

Answer RRs: 0

Authority RRs: 2

Additional RRs: 11

Queries

www.51cto.com: type A, class IN

Authoritative nameservers

51cto.com: type NS, class IN, ns ns1.dnsv2.com

51cto.com: type NS, class IN, ns ns2.dnsv2.com

Additional records

ns1.dnsv2.com: type A, class IN, addr 111.30.132.180

ns1.dnsv2.com: type A, class IN, addr 115.236.151.178

ns1.dnsv2.com: type A, class IN, addr 125.39.213.168

ns1.dnsv2.com: type A, class IN, addr 14.215.150.11

ns1.dnsv2.com: type A, class IN, addr 180.153.162.151

ns2.dnsv2.com: type A, class IN, addr 111.30.132.180

ns2.dnsv2.com: type A, class IN, addr 122.225.217.193

ns2.dnsv2.com: type A, class IN, addr 180.153.10.167

ns2.dnsv2.com: type A, class IN, addr 182.140.167.167

ns2.dnsv2.com: type A, class IN, addr 183.60.57.177

ns2.dnsv2.com: type A, class IN, addr 220.249.242.11

ns1.dnsv2.com对应的IP地址

ns2.dnsv2.com对应的IP地址

0000 00 0c 29 14 bf 02 00 50 56 f4 11 93 08 00 45 00 ..).....P V.....E.

0010 01 15 ff 0f 00 00 80 11 bd c1 c0 2b ac 1e c0 a8+.....

0020 50 14 00 35 04 06 01 01 84 65 08 9a 80 00 00 01 P..5....e.....

0030 00 00 00 02 00 0b 03 77 77 77 05 35 31 63 74 6fw ww.51cto

0040 03 63 6f 6d 00 00 01 00 01 c0 10 00 02 00 01 00 .com....

0050 02 32 00 00 0c 02 60 73 31 05 64 60 73 76 22 c0

File: "C:\Users\han\Desktop\DNS.pcapng"... Packets: 23 · Displayed: 23 (100.0%) · Load time: 0:00.031 Profile: Default

DNS解析的最终结果

DNS.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Vmware_cc:87:22	Broadcast	ARP	60	who has 192.168.80.20? Tell 192.168.80.20
2	0.00004500	Vmware_14:bf:02	Vmware_cc:87:22	ARP	42	192.168.80.20 is at 00:0c:29:14:b
3	0.00042000	192.168.80.111	192.168.80.20	DNS	73	Standard query 0xbfad A www.51cto.com
4	0.00063200	192.168.80.20	192.43.172.30	DNS	73	Standard query 0x089a A www.51cto.com
5	0.19443100	Vmware_f4:11:93	Broadcast	ARP	60	who has 192.168.80.20? Tell 192.168.80.20
6	0.19446200	Vmware_14:bf:02	Vmware_f4:11:93	ARP	42	192.168.80.20 is at 00:0c:29:14:b
7	0.19470200	192.43.172.30	192.168.80.20	DNS	291	Standard query response 0x089a
8	0.19517000	192.168.80.20	220.249.242.11	DNS	73	Standard query 0x089a A www.51cto.com
9	0.24812700	220.249.242.11	192.168.80.20	DNS	204	Standard query response 0x089a
10	0.24835800	192.168.80.20	192.168.80.111	DNS	204	Standard query response 0xbfad
11	0.26479700	Vmware_cc:87:22	Broadcast	ARP	60	who has 192.168.80.1? Tell 192.168.80.1

Frame 10: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface 0

Ethernet II, Src: Vmware_14:bf:02 (00:0c:29:14:bf:02), Dst: Vmware_cc:87:22 (00:0c:29:cc:87:22)

Internet Protocol Version 4, Src: 192.168.80.20 (192.168.80.20), Dst: 192.168.80.111 (192.168.80.111)

User Datagram Protocol, Src Port: 53 (53), Dst Port: 1025 (1025)

Domain Name System (response)

[Request In: 3]

[Time: 0.247938000 seconds]

Transaction ID: 0xbfad

Flags: 0x8400 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 2

Additional RRs: 0

Queries

- www.51cto.com: type A, class IN
 - Name: www.51cto.com
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Answers

- www.51cto.com: type CNAME, class IN, cname web.dns.51cto.com
- web.dns.51cto.com: type CNAME, class IN, cname gf.dns.51cto.com
- gf.dns.51cto.com: type A, class IN, addr 116.211.167.193 → 解析到的IP地址

Authoritative nameservers

- 51cto.com: type NS, class IN, ns ns2.dnsv2.com
- 51cto.com: type NS, class IN, ns ns1.dnsv2.com

0080 6f 03 63 6f 6d 00 c0 4a 00 01 00 01 00 02 58 o.com. .JX

0090 00 04 74 d3 a7 c1 c0 10 00 02 00 01 00 01 51 80 .t.Q.

00a0 00 0f 03 6e 73 32 05 64 6e 73 76 32 03 63 6f 6d .ns2.d nsv2.com

00b0 00 c0 10 00 02 00 01 00 01 51 80 00 0f 03 6e 73Q.ns

00c0 31 05 64 6e 73 76 32 03 63 6f 6d 00 1. dnsv2. com.

Text item (text), 16 bytes

Packets: 23 · Displayed: 23 (100.0%) · Load tim... Profile: Default

9.2动态主机配置协议DHCP

- 9.2.1静态地址和动态地址应用场景
- 9.2.2DHCP地址租约
- 9.2.3DHCP租约生成过程
- 9.2.4DHCP地址租约更新
- 9.2.5实战1： 安装和配置DHCP服务
- 9.2.6实战2： 查看 刷新 释放租约
- 9.2.7实战3： 跨网段分配IP地址

9.2.1 静态地址和动态地址应用场景

■ 使用静态地址的情况：

- IP地址不经常更改的设备就使用静态地址。比如企业中服务器会单独在一个网段，很少更改IP地址或移动到到其他网段，这些服务器通常使用静态地址，使用静态地址还方便企业员工使用地址访问这些服务器。比如学校机房，都是台式机，很少移动，这些计算机最好也使用静态地址。

■ 使用动态地址的情况：

- 网络中的计算机不固定，就应该使用动态地址。
- 无线设备最好也使用动态地址。
- ADSL拨号上网通常也是使用自动获得IP地址。

9.2.2 DHCP地址租约

■地址以租约的形式提供给客户端



9.2.3 DHCP租约生成过程1

■ DHCP客户端会在以下所列举的几种情况下，从DHCP服务器获取一个新的IP地址。

- 该客户端计算机是第一次从DHCP服务器获取IP地址。
- 该客户端计算机原先所租用的IP地址已经被DHCP服务器收回，而且已经又租给其他计算机了，因此该客户端需要重新从DHCP服务器租用一个新的IP地址。
- 该客户端自己释放原先所租用的IP地址，并要求租用一个新的IP地址。
- 客户端计算机更换了网卡。
- 客户端计算机转移到另一个网段。

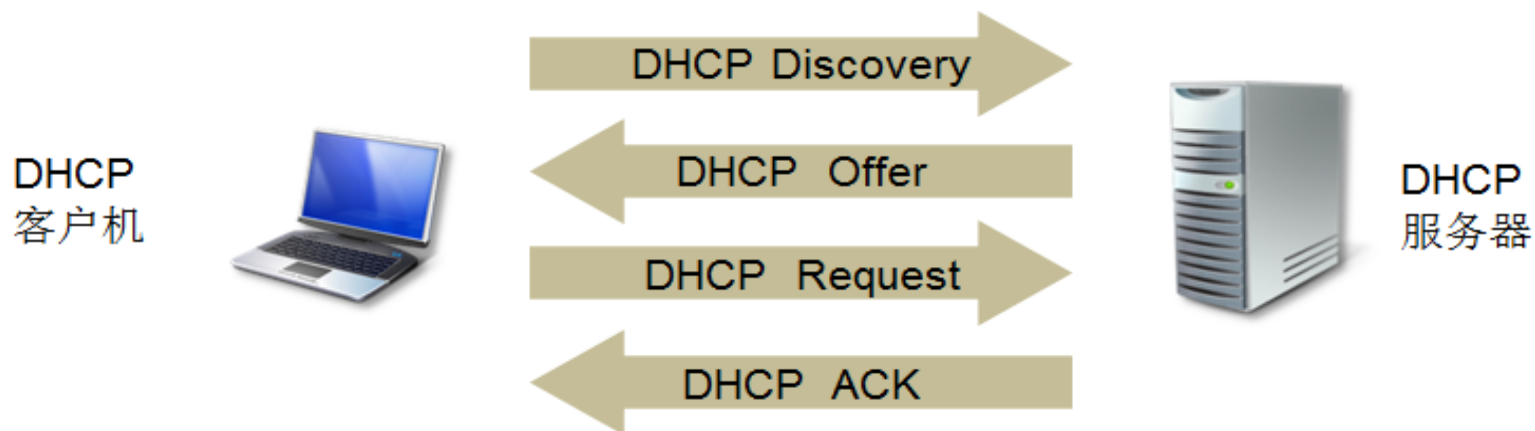
9.2.3 DHCP租约生成过程2

(1) **DHCPDISCOVER** DHCP客户端会先送出DHCPDISCOVER的广播信息到网络，以便寻找一台能够提供IP地址的DHCP服务器。

(2) **DHCPOFFER** 当网络中的DHCP服务器收到DHCP客户端的DHCPDISCOVER信息后，就会从IP地址池中，挑选一个尚未出租的IP地址，然后利用广播的方式传送给DHCP客户端。

(3) **DHCPREQUEST** 当DHCP客户端挑选好第一个收到的DHCPOFFER信息后，它就利用广播的方式，响应一个DHCPREQUEST信息给DHCP服务器。

(4) **DHCPACK** DHCP服务器收到DHCP客户端要求IP地址的DHCPREQUEST信息后，就会利用广播的方式送出DHCPACK确认信息给DHCP客户端。



9.2.4 DHCP地址租约更新-更新时机

- (1) 当租约时间过去一半时，客户机向DHCP服务器发送一个请求，请求更新和延长当前租约。客户机直接向DHCP服务器发请求，最多可重发三次，分别在4、8和16s时。
- (2) 如果某台服务器应答一个DHCP Offer消息，以更新客户机的当前租约，客户机就用服务器提供的信息更新租约并继续工作。
- (3) 如果租约终止而且没有连接到服务器，客户机必须立即停止使用其租约IP地址。然后，客户机执行与它初始启动期间相同的过程来获得新的IP地址租约。

9.2.4 DHCP地址租约更新-更新方法

■方法一：自动更新

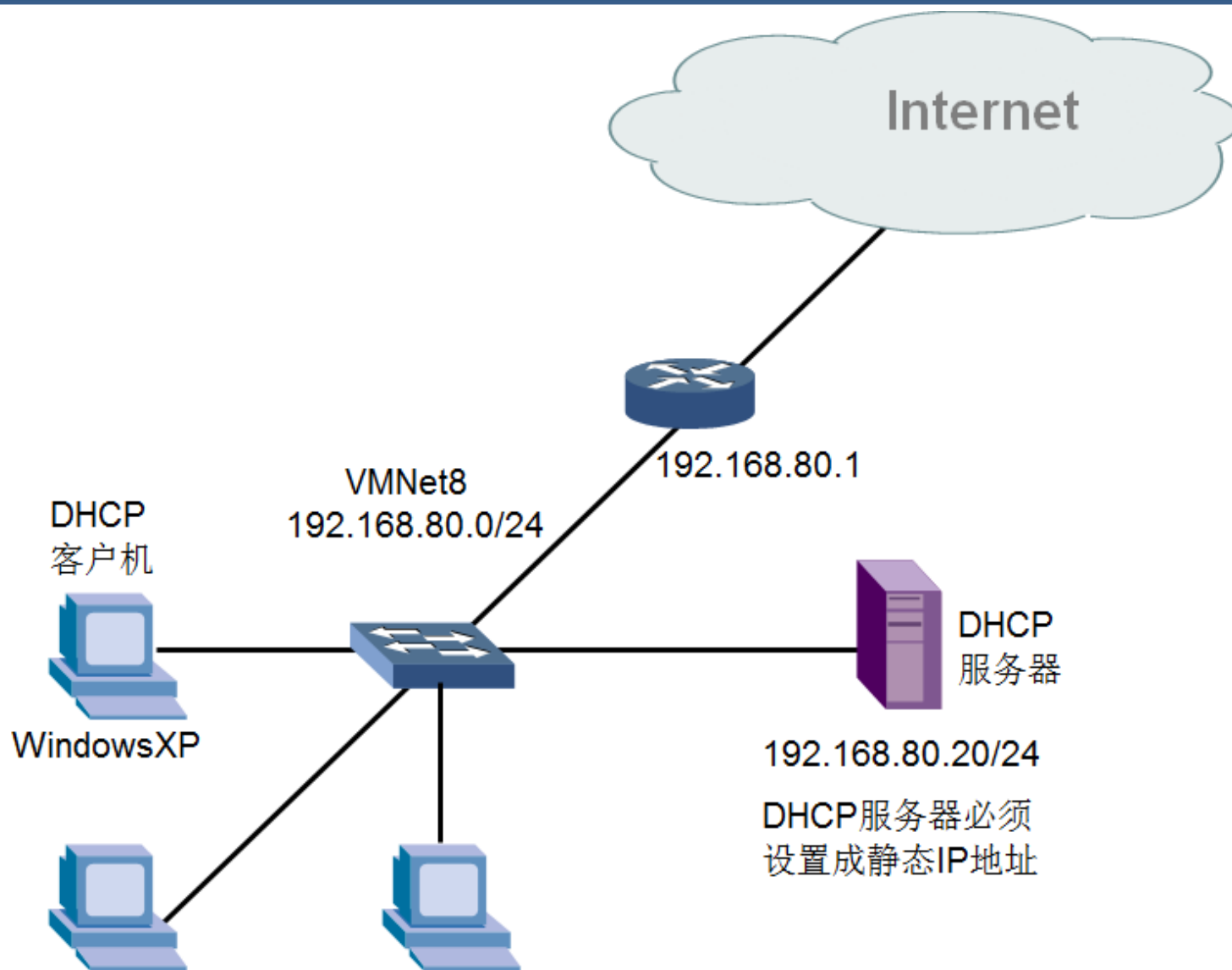
- DHCP服务自动进行租约的更新，也就是前面部分描述的租约更新的过程，当租约期达到租约期限50%时，DHCP客户端将自动开始尝试续租该租约。每次DHCP客户端重新启动的时候也将尝试续租该租约。为了续租其租约，DHCP客户端为它提供租约的DHCP服务器发出一个DHCPREQUEST请求数据包。如果该DHCP服务器可用，它将续租该租约并向DHCP客户端提供一个包含新的租约期和任何需要更新的配置参数值的DHCPACK数据包。当客户端收到该确认数据包后更新自己的配置。如果DHCP服务器不可用，客户端将继续使用现有的配置。

■方法二：手动更新

- 如果需要立即更新DHCP配置信息，可以手工对IP地址租约进行续租操作，例如：如果我们希望DHCP客户端立即从DHCP服务器上得到一台新安装的路由器的地址，只需简单地在客户端做续租操作就可以了。
- 直接在客户机上的命令提示符下，执行命令：`Ipconfig /renew`

9.2.5实战1：安装和配置DHCP服务

- 单网段环境下安装DHCP服务器，网络环境如图所示，配置DHCP服务器给本网段计算机分配IP地址。将演示如何配置DHCP作用域，查看DHCP客户端记录的租约和DHCP服务器记录的租约，在DHCP服务器上使用抓包工具捕获生成租约、更新租约、释放租约的数据包。



9.2.6实战2：查看 刷新 释放租约1

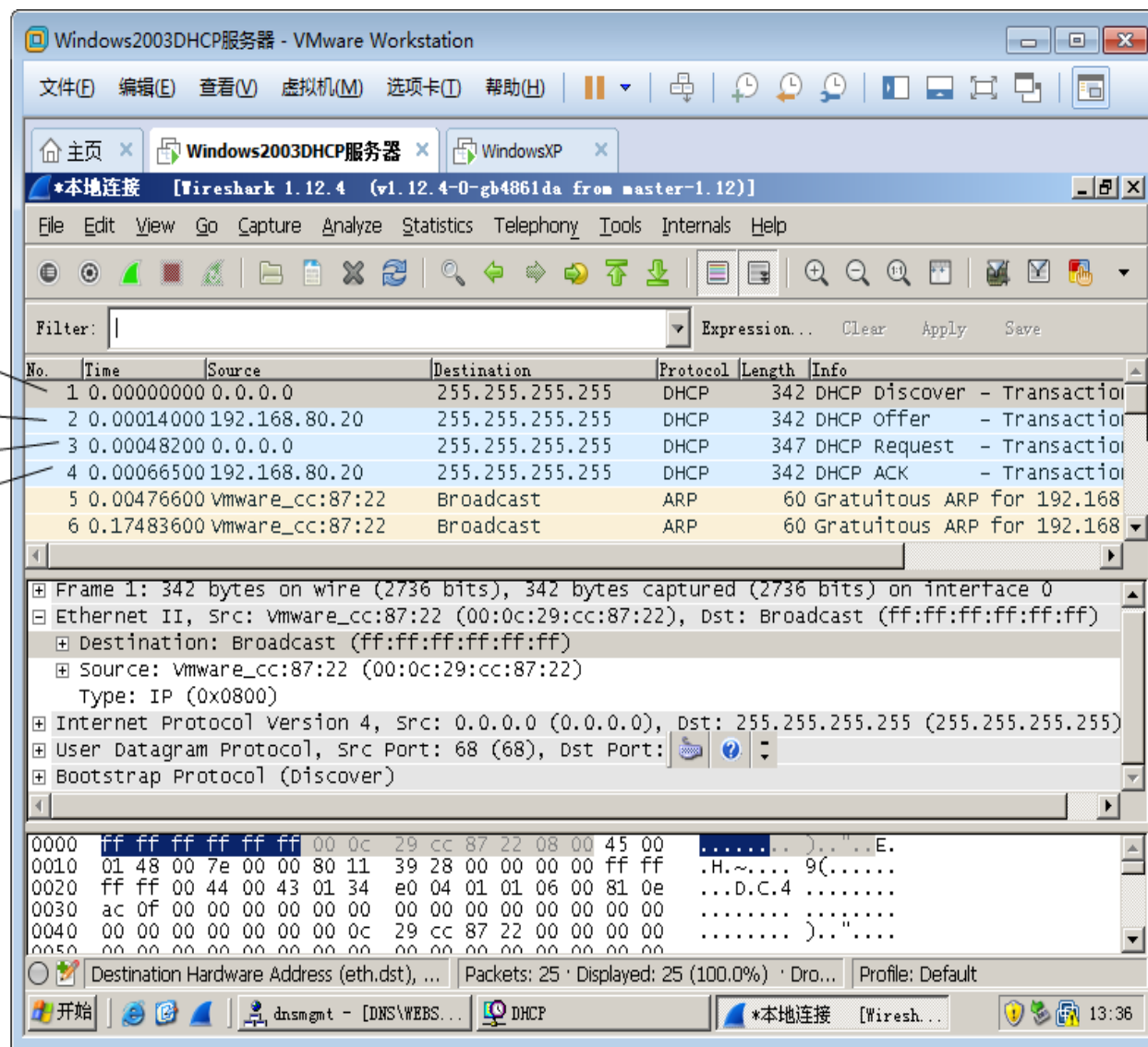
■获DHCP客户端
请求地址的产生的
数据包。

DHCP Discover

DHCP Offer

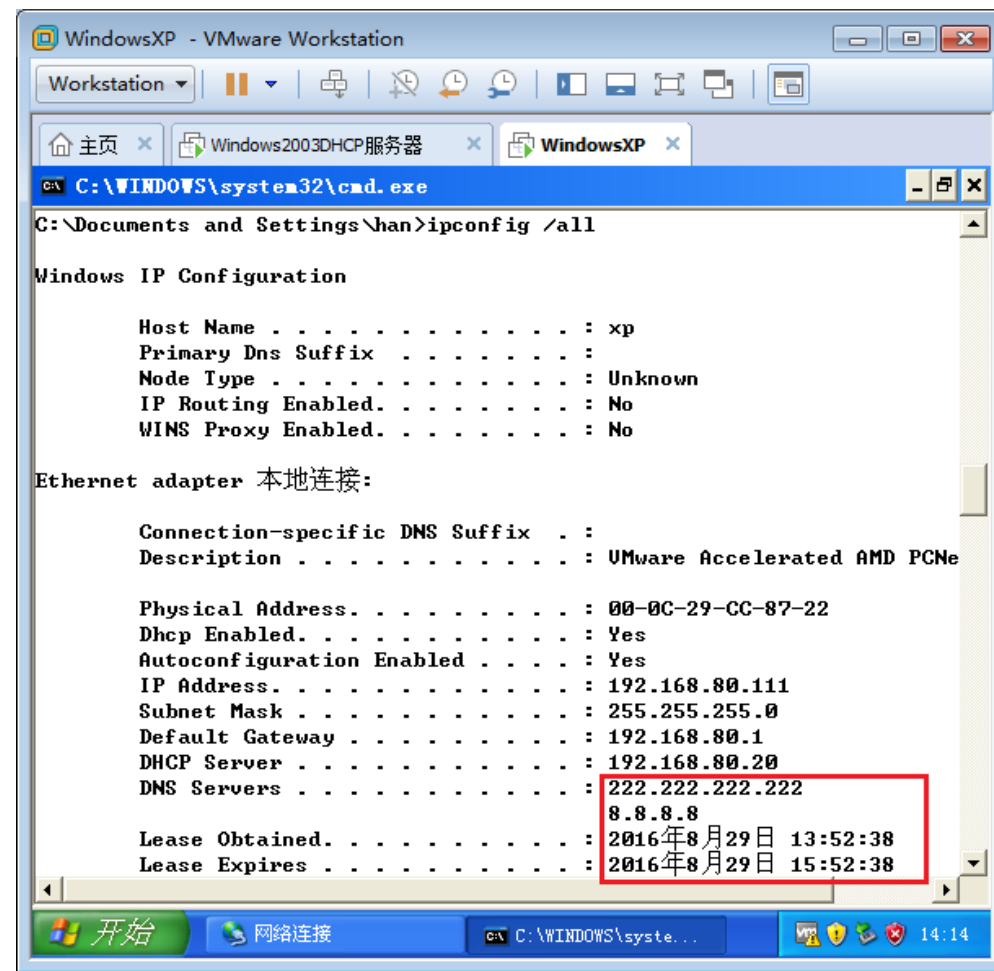
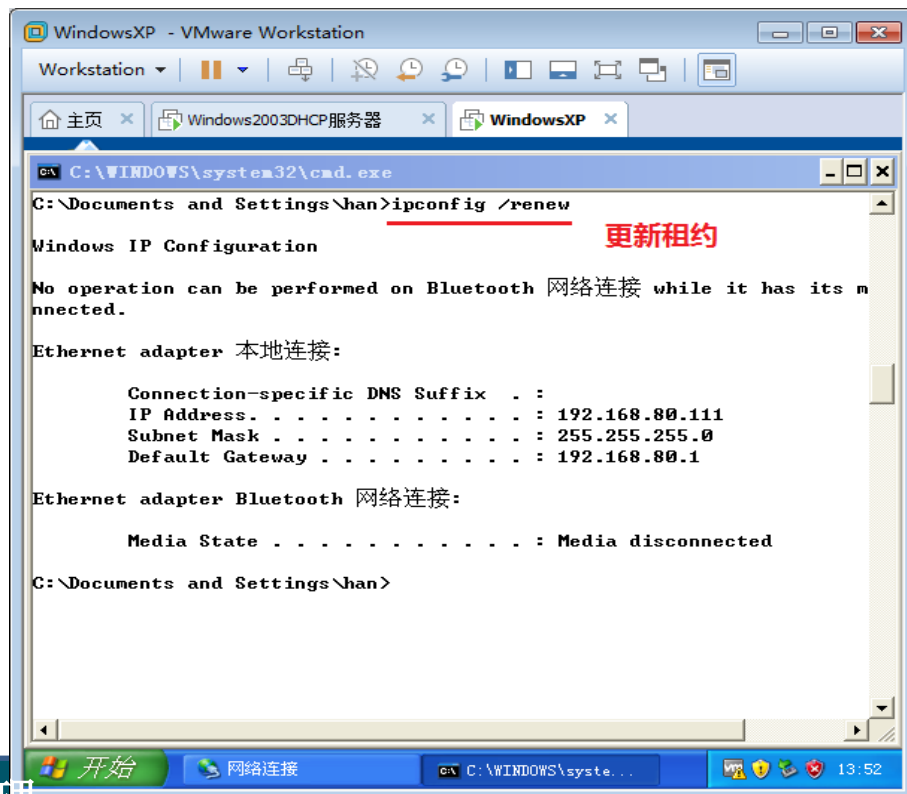
DHCP Request

DHCP ACK



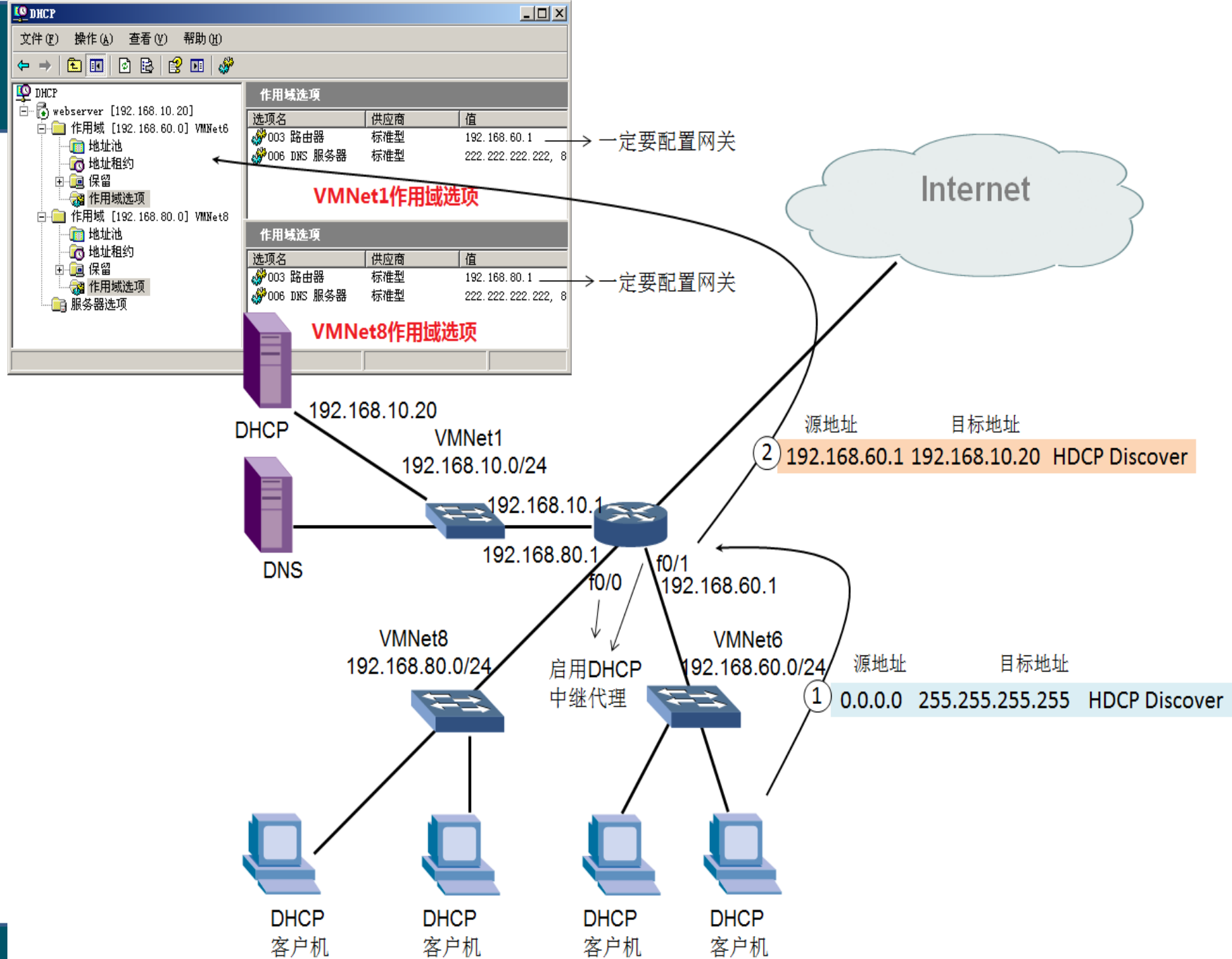
9.2.6实战2：查看 刷新 释放租约1

- `ipconfig /all`可以查看地址租约。
- `ipconfig /release`能够释放租约。
- `ipconfig /renew`更新租约。



9.2.7实战3:

跨网段分配IP地址



9.2.7实战3：跨网段分配IP地址2

■需要在路由器上为VMNet8和VMNet6启用DHCP中继代理，命令如下：

- Router (config) #interface fastEthernet 0/0
- Router (config-if) #ip helper-address 192.168.10.20
- Router (config-if) #exit
- Router (config) #interface fastEthernet 0/1
- Router (config-if) #ip helper-address 192.168.10.20

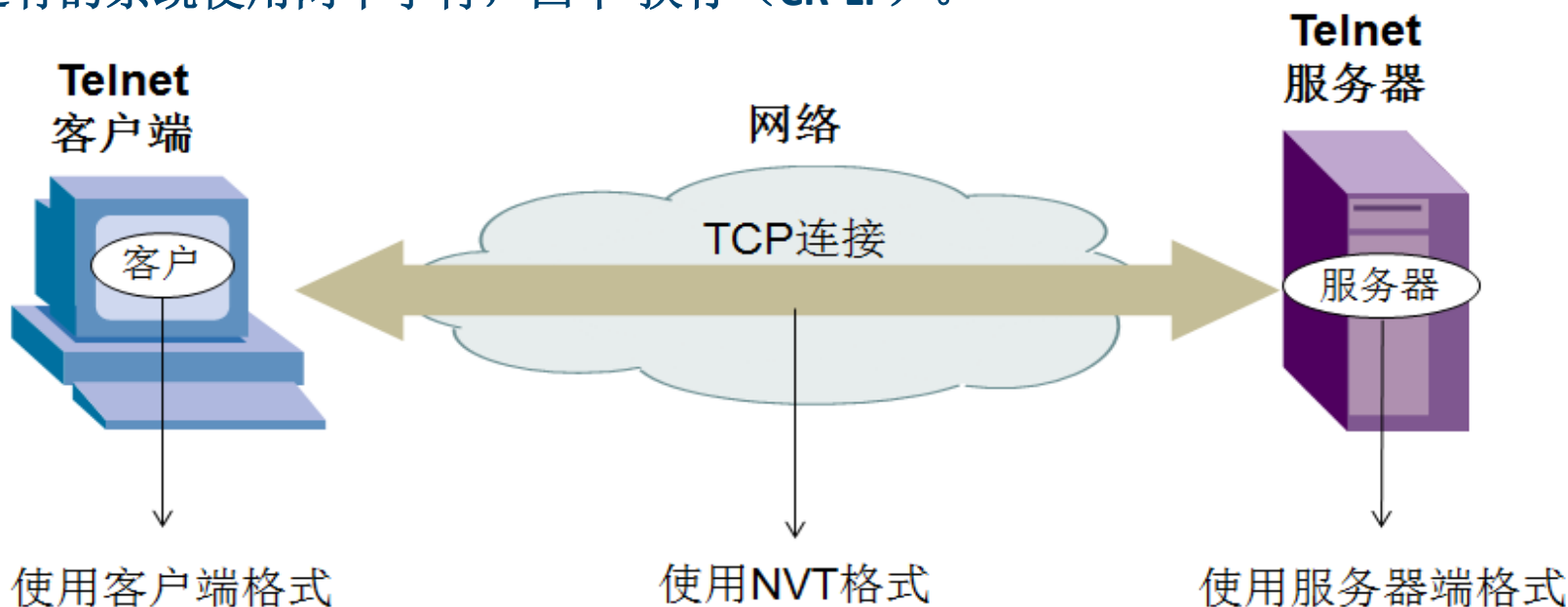
■在接口模式下输入ip helper-address 192.168.10.20，就是告诉路由器，该接口如果收到DHCP Discover广播，就由该接口产生一个DHCP请求包，目标地址是192.168.10.20，源地址是收到该广播包的接口地址。DHCP服务器收到这样的一个DHCP Discover，就知道这是来自哪个网段的请求，就会从相应的作用域选择一个地址提供。

9.3Telnet协议

- TELNET是一个简单的远程终端协议，它也是因特网的正式标准。用户使用telnet客户端就可以连接到远程运行Telnet服务的设备（可以是网络设备比如路由器、交换机，也可以是操作系统，比如Windows或Linux），进行远程管理。
- TELNET能将用户的键盘指令传到远地主机，同时也能将远地主机的输出通过TCP连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上。因此，TELNET又称为终端仿真协议。
- TELNET并不复杂，以前应用得很多。现在由于操作系统（Windows和Linux）功能越来越强，用户已较少使用TELNET了。不过配置Linux服务器和网络设备还是需要TELNET来实现远程管理和配置

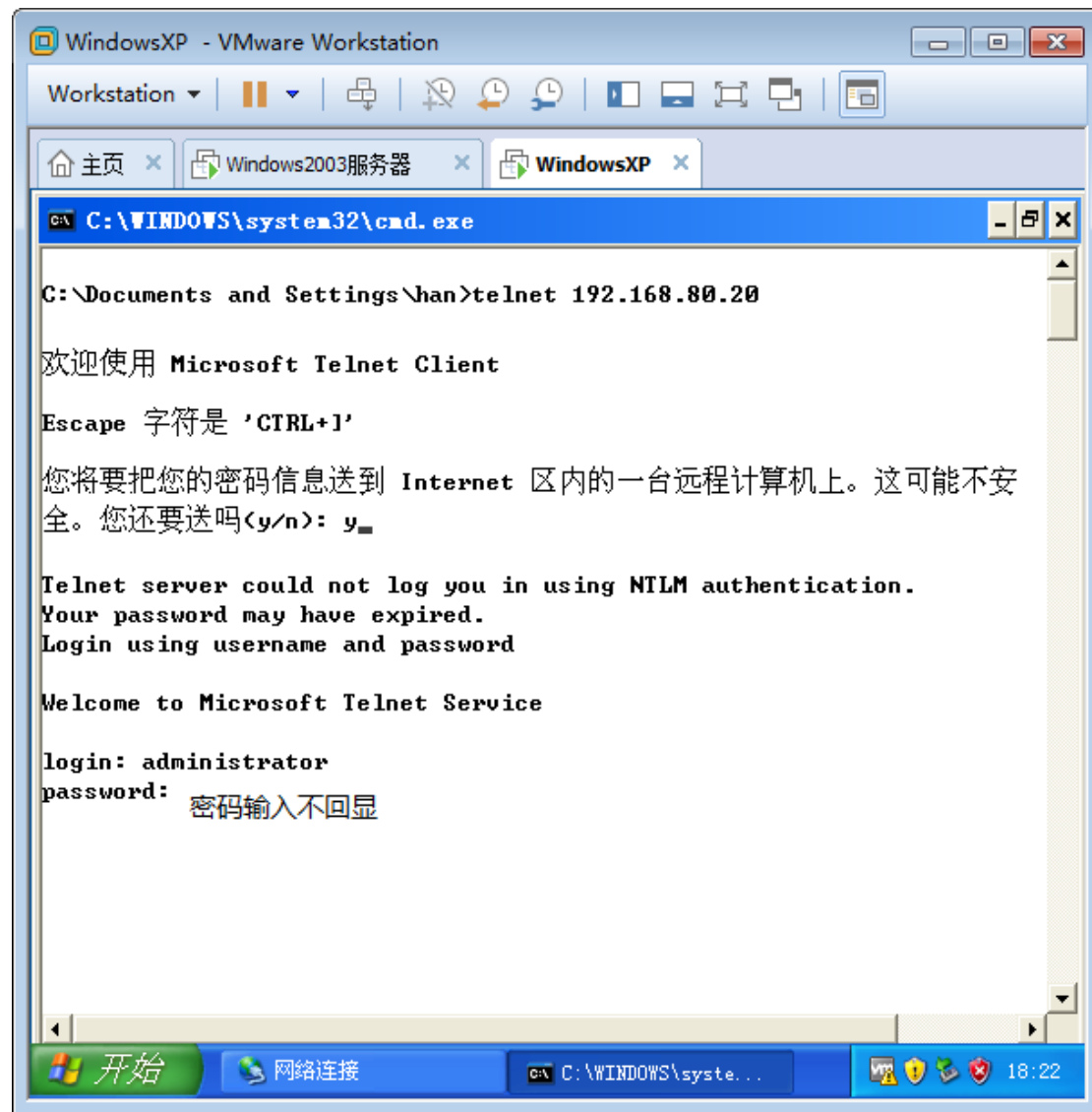
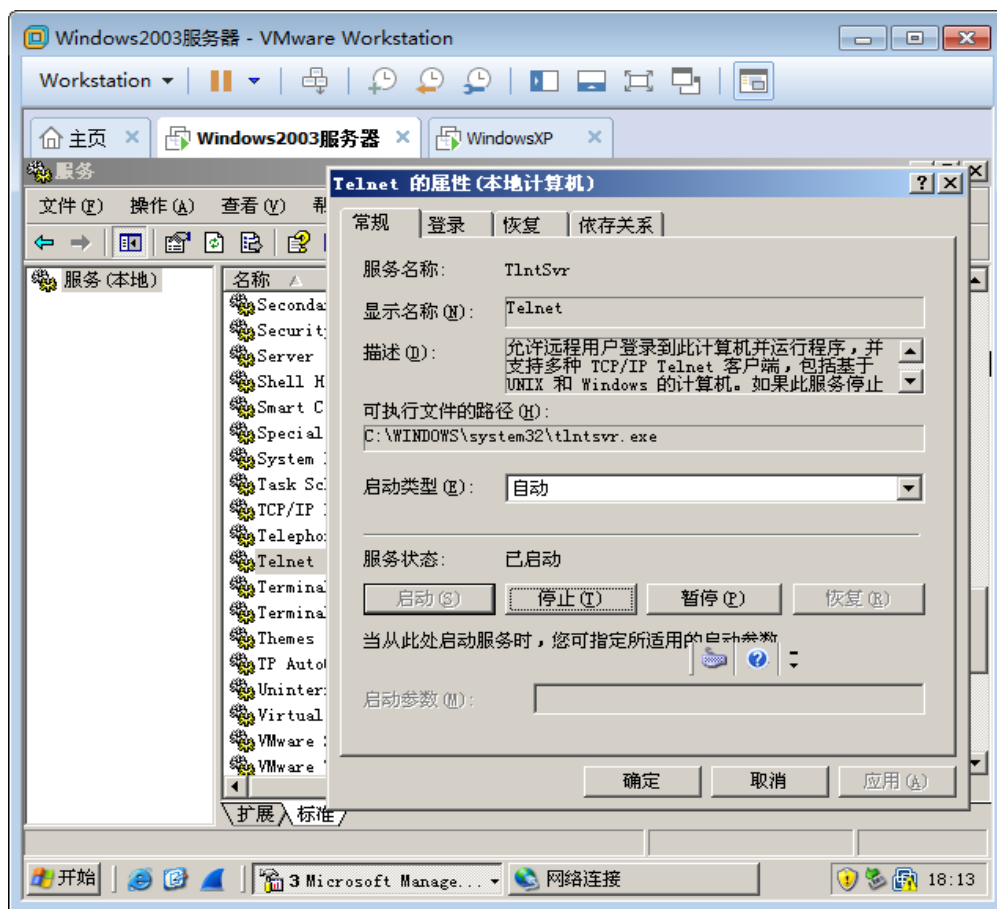
9.3.1 Telnet协议工作方式

- TELNET也使用客户端-服务端方式。在本地系统运行TELNET客户进程，而在远地主机则运行TELNET服务器进程。服务器中的主进程等待新的请求，并产生从属进程来处理每一个连接。
- TELNET能够适应许多计算机和操作系统的差异。例如，对于文本中一行的结束，有的系统使用ASCII码的回车（CR），有的系统使用换行（LF）。还有的系统使用两个字符，回车-换行（CR-LF）。又如，在中断一个程序时，许多系统使用Control-C，但也有系统使用ESC按键。
- TELNET定义了数据和命令应怎样通过网络。这些定义就是所谓的网络虚拟终端NVT（Network Virtual Terminal），还有的系统使用两个字符，回车-换行（CR-LF）。



9.3.2实战：telnet管理Windows系统

- 开启telnet服务
- 在客户端telnet服务器



9.3.3实战：telnet管理网络设备

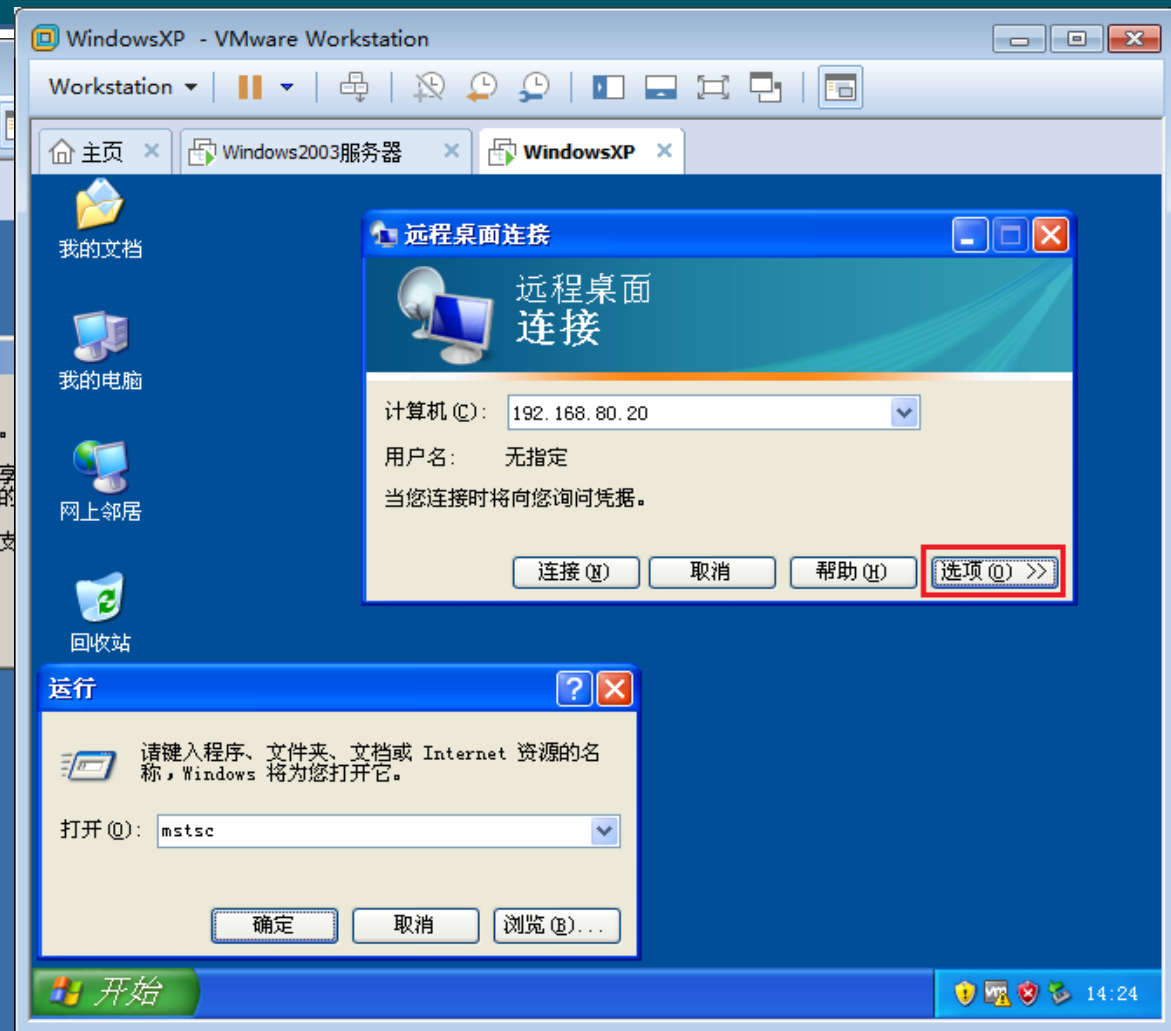
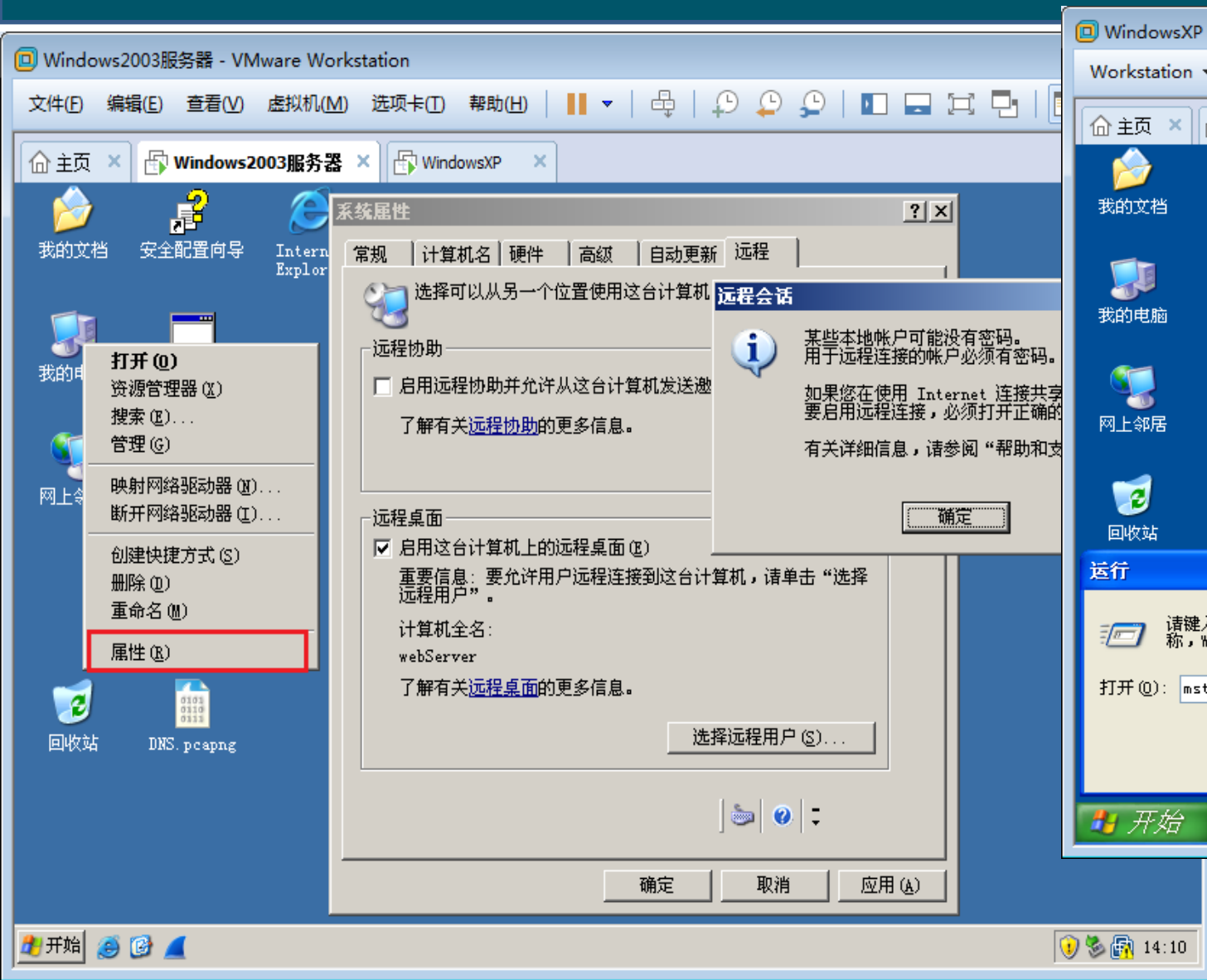
■在R1路由器上配置telnet虚拟接口，设置telnet密码和enable密码。

- Router#config t --进入全局配置模式
- Enter configuration commands, one per line. End with CNTL/Z.
- Router (config) #line vty 0 ? --查看telnet虚拟接口数量
- <1-871> Last Line number
- <cr>
- Router (config) #line vty 0 871 --进入虚拟接口配置模式
- Router (config-line) #password 91xueit --设置telnet连接密码
- Router (config-line) #login --必须登录才能telnet连接
- Router (config-line) #exit --退出telnet虚拟接口
- Router (config) #enable password 51cto --设置enabled密码
- Router (config) #exit

9.4远程桌面协议RDP1

- 现在Windows操作系统很少使用telnet进行远程管理了，更多是使用远程桌面进行远程管理。Windows系统启用远程桌面，客户端使用远程桌面客户端（mstsc）进行连接。它们之间使用RDP协议进行通信，RDP协议默认使用TCP的3389端口。

9.4远程桌面协议RDP2

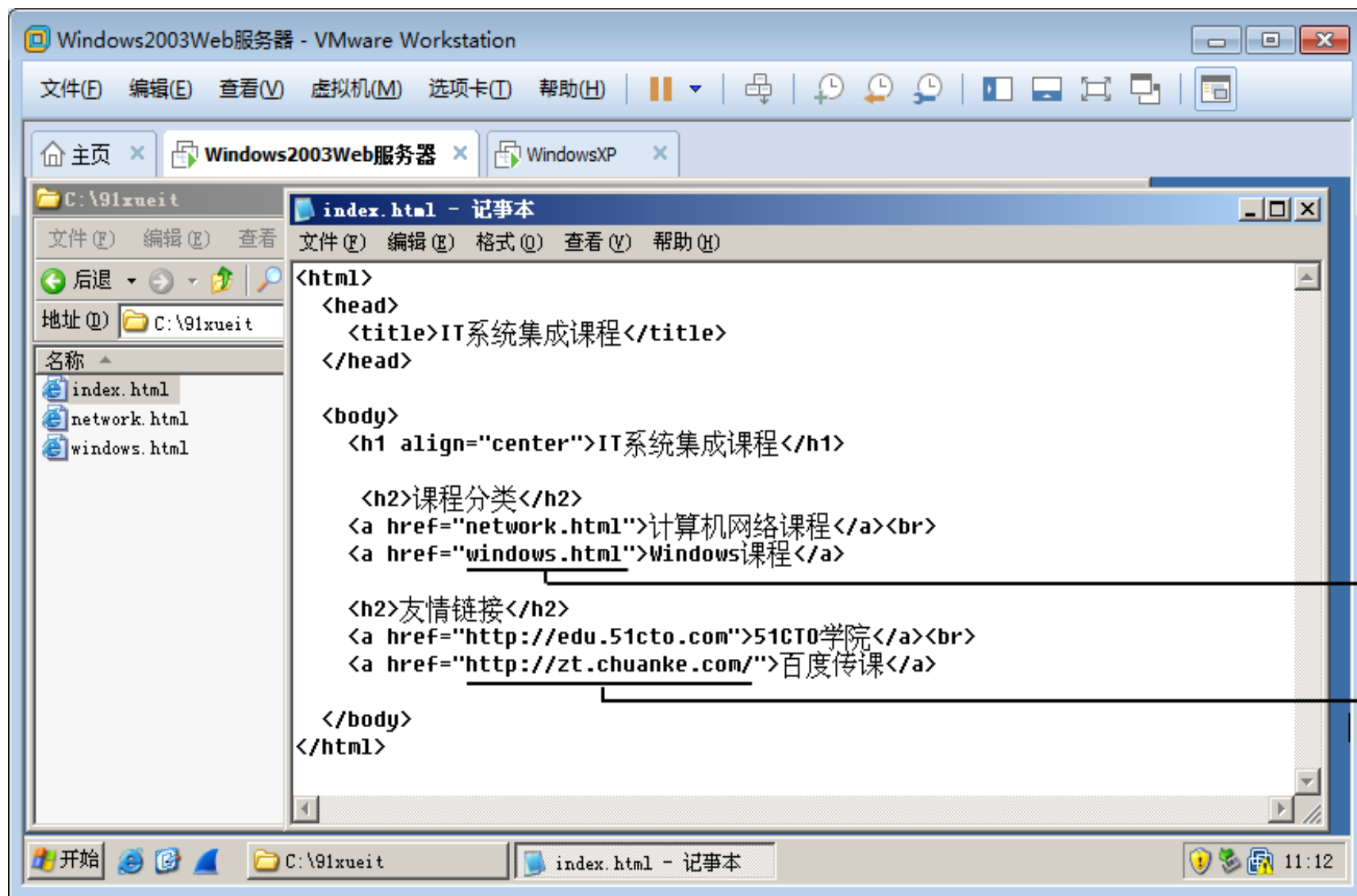


9.5超级文本传输协议HTTP

- 9.5.1创建网页
- 9.5.2统一资源定位符URL
- 9.5.3绝对路径和相对路径
- 9.5.4创建Web站点
- 9.5.5HTTP协议版本
- 9.5.6HTTP请求报文和响应报文
- 9.5.7HTTP响应报文：
- 9.5.8 Cookie
- 9.5.9通过代理服务器访问网站

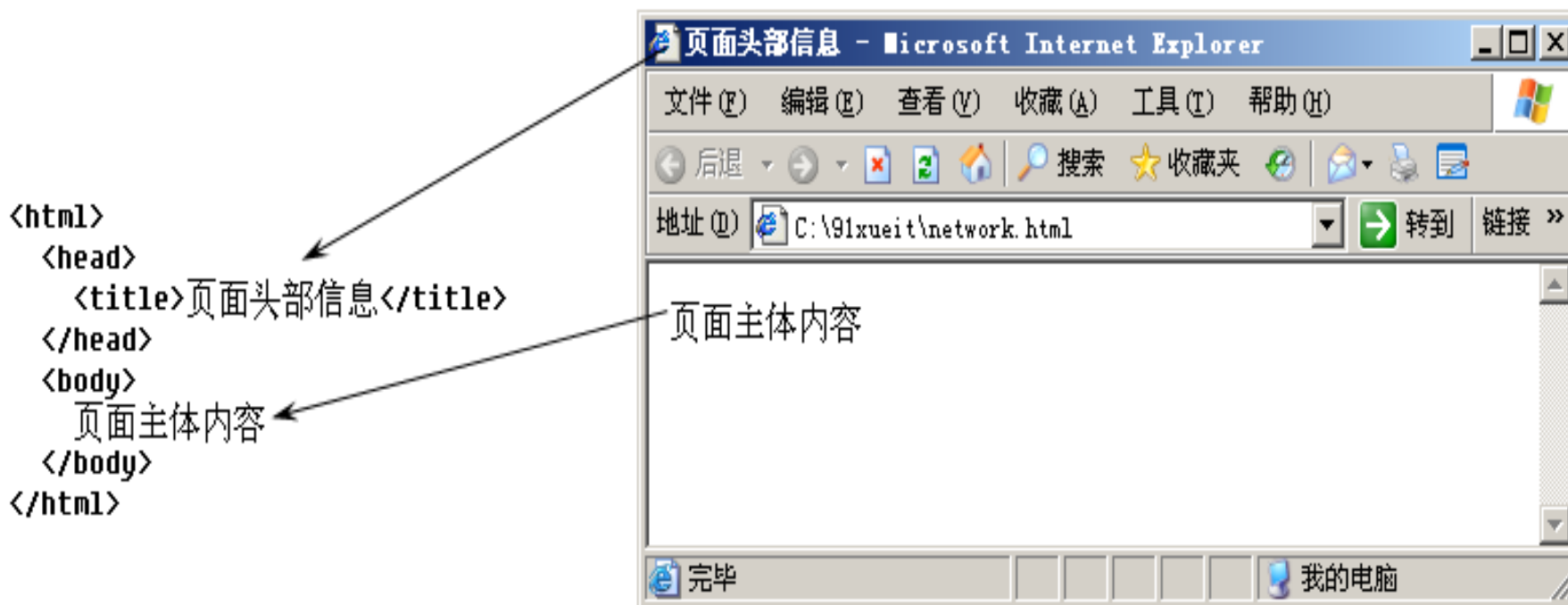
9.5.1 创建网页

- HTTP协议是超
级文本传输协议，
先看看什么是超
级文本。
- 一个网站通常是
由一组网页组成，
其中一个网页是
首页，通过首页
的超链接可以访
问到该网站的其他网页，超链接
也可以链接到其他网站。



HTML文件结构

- HTML文件均以<html>标记开始，以</html>标记结束。
- <head>...</head>标记之间的内容用于描述页面的头部信息，如页面的标题、作者、摘要、关键词、版权、自动刷新等信息。
- 在<body>...</body>标记之间的内容为页面的主体内容。
- HTML文件的整体结构及对应的预览效果如图所示。



9.5.2统一资源定位符URL

- 统一资源定位符URL（Uniform Resource Locator）是用来表示从因特网上得到的资源位置和访问这些资源的方法。URL给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。只要能够对资源定位，系统就可以对资源进行各种操作，如存取、更新、替换和查找其属性。
- URL是与因特网相连的机器上的任何可访问对象的一个指针。由于访问不同对象所使用的协议不同，所以URL还指出读取某个对象时所使用的协议。URL的一般形式由以下四个部分组成：
<协议>://<主机>:<端口>/<路径>

下面是使用得最多的两种URL

■ (1) HTTP的URL的一般格式是:

http://<主机>:<端口>/<路径>

- 如果HTTP使用的是默认端口号是80，通常可省略。若再省略文件的<路径>项，则URL就指到该网站的根目录下的主页（homepage）。
- 更复杂一点的URL是指向网站第二级或第三级目录的网页。
- `http://edu.51cto.com/member/id-2_1.html`

■ (2) FTP的URL的一般格式:

- `ftp://<主机>:<端口>/<路径>`
- 比如北京邮电FTP服务器，`ftp://ftp.bupt.edu.cn`。FTP的URL中还可以包括登录FTP服务器的账户和密码，比如
`ftp://stargate:sg1@61.155.39.141:9921`，其中登录名为stargate，密码为sg1，FTP服务器IP地址61.155.39.141，端口为9921。

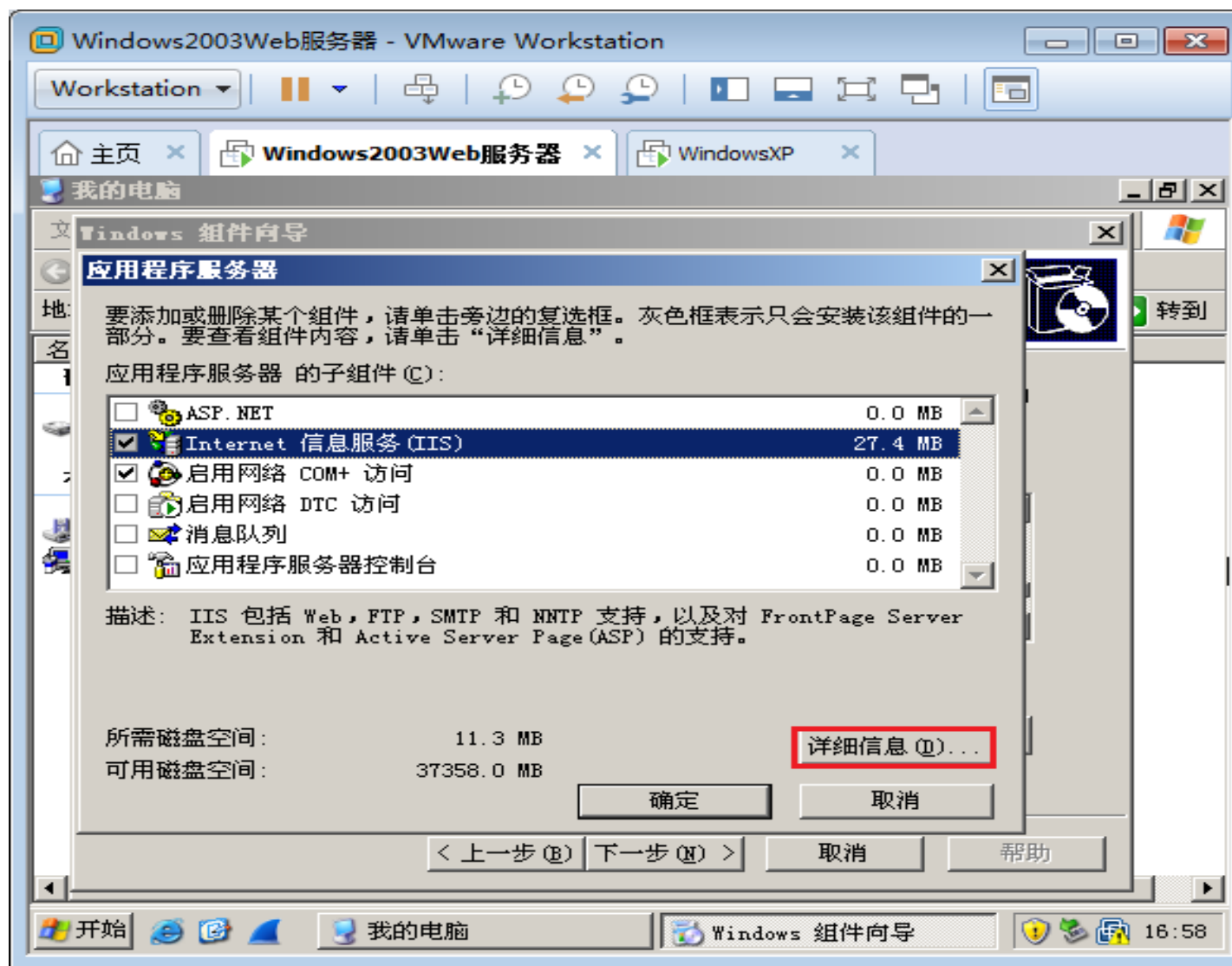
9.5.3绝对路径和相对路径

■在Internet上访问资源时使用URL，网页中的超级链接指向其他网站的资源时也需要使用URL，网页中的超链接如果指向的同一个网站下的其他网页，就可以使用相对路径或根路径。在网页中添加超级链接需要搞明白使用绝对路径、相对路径还是根路径，需要确定当前文档同站点根目录之间的相对路径关系。链接可以分为以下3种：

- 绝对路径，如<http://www.webjx.com>
- 相对路径，如<news/default.htm>
- 根路径，如</website/news/default.htm>

9.5.4创建Web站点

- 将网页通过网站发布出去，网络中的用户才能访问。IIS、Apache、Tomcat都可以搭建Web服务器，IIS服务是Windows操作系统的一个组件，安装后就可以创建Web站点，将编辑好的网页发布出去。
- 在WindowsServer2003上安装IIS服务，创建Web站点。

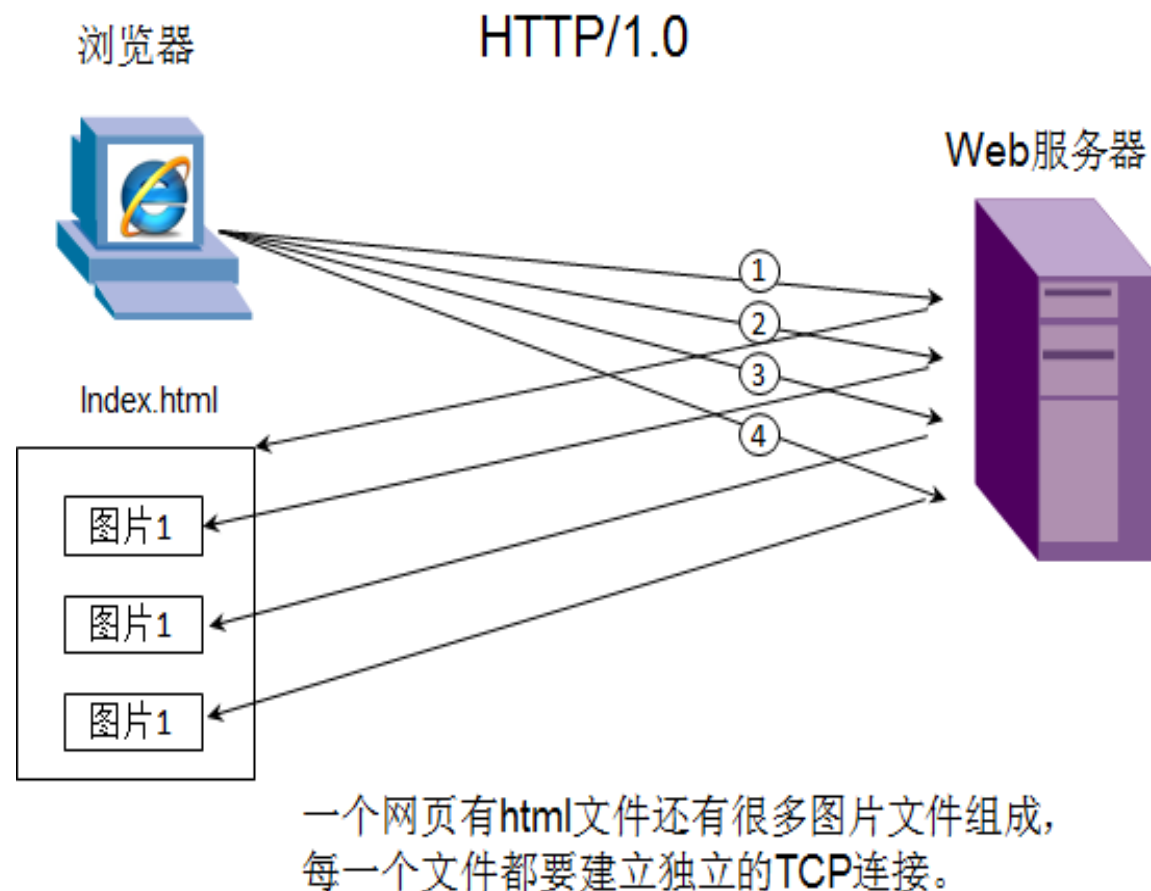


9.5.5 HTTP协议版本

■ 设计HTTP最初的目的是为了提供一种发布和接收HTML页面的方法。HTTP协议有三个版本HTTP/0.9、HTTP/1.0、HTTP/1.1，HTTP2.0 目前HTTP/1.0和1.1被广泛应用。

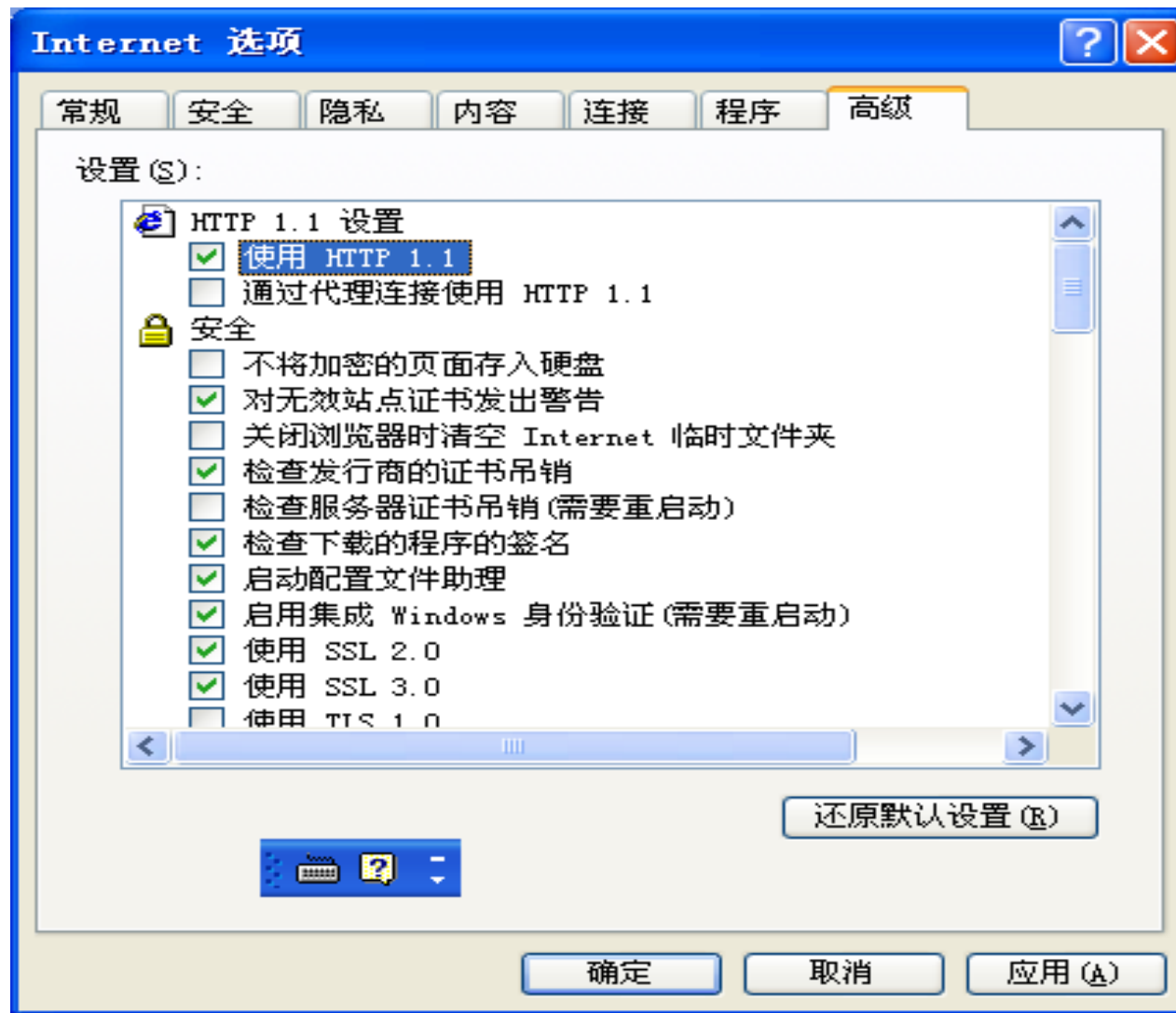
■ HTTP 1.0与HTTP 1.1的比较：

一个WEB站点每天可能要接收到上百万的用户请求，为了提高系统的效率，HTTP 1.0规定浏览器与服务器只保持短暂的连接，浏览器的每次请求都需要与服务器建立一个TCP连接，服务器完成请求处理后立即断开TCP连接，服务器不跟踪每个客户也不记录过去的请求。

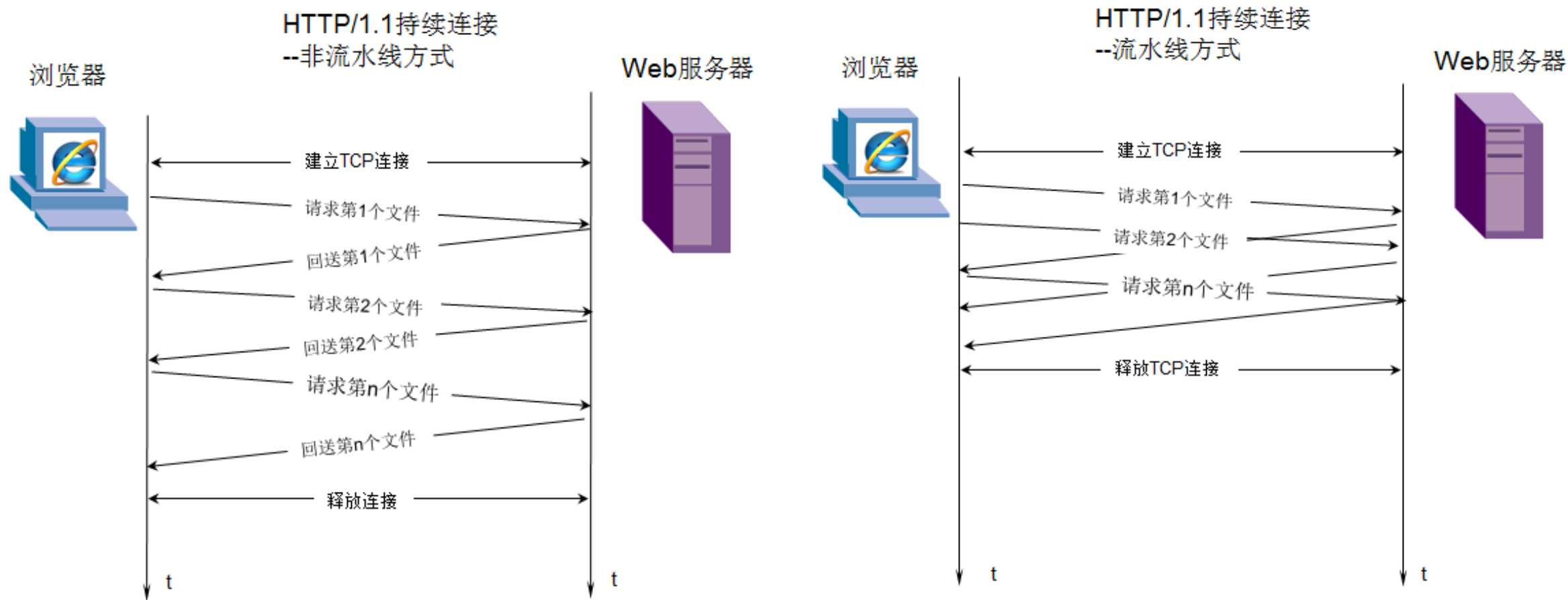


HTTP 1.1支持持续连接

- 为了克服HTTP 1.0的这个缺陷， HTTP 1.1支持持续连接，持续连接就是Web服务器在发送响应后仍然在一段时间内保持这条连接，使同一个客户（浏览器）和该服务器可以继续在这条连接上传送后续的HTTP请求报文和响应报文。



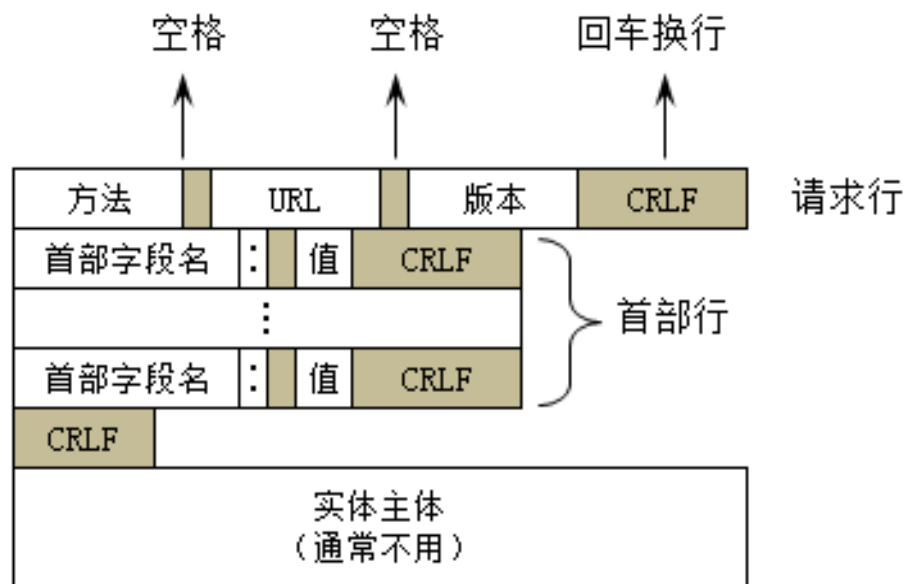
HTTP/1.1协议的持续连接有两种工作方式



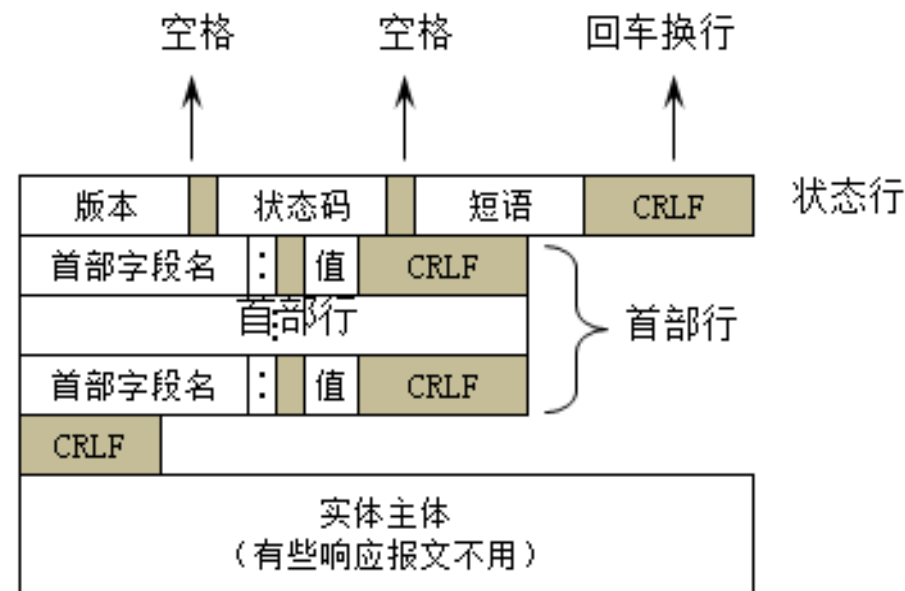
9.5.6 HTTP请求报文和响应报文

■ HTTP有两类报文：

- (1) 请求报文-从客户端向服务器发送请求报文。
- (2) 响应报文-从服务器到客户端的应答。



(a) 请求报文



(b) 响应报文

HTTP请求报文由三个部分组成

- 由于HTTP是面向文本的（**text-oriented**），因此在报文中的每一个字段都是一些**ASCII**码串，因而各个字段的长度都是不确定的。
- HTTP请求报文由三个部分组成。可以看出，这两种报文格式的区别就是开始行不同。
 - 开始行，用于区分是请求报文还是响应报文。在请求报文中的开始行叫做请求行（**Request-Line**），而在响应报文中的开始行叫做状态行（**status-Line**）。在开始行的三个字段之间都以空格分隔开，最后的“**CR**”和“**LF**”分别代表“回车”和“换行”。
 - 首部行，用来说明浏览器、服务器或报文主体的一些信息。首部可以有好几行，但也可以不使用。在每一个首部行中都有首部字段名和它的值，每一行在结束的地方都要有“回车”和“换行”。整个首部行结束时，还有一空行将首部行和后面的实体主体分开。
 - 实体主体（**entity body**），在请求报文中一般都不用这个字段，而在响应报文中也可能没有这个字段。

HTTP请求报文特点和方法

- 先介绍HTTP请求报文最主要的一些主要特点。请求报文的“请求行”只有三个内容，即方法，请求资源的URL，以及HTTP的版本。
- HTTP/1.1协议中共定义了八种方法（有时也叫“动作”）来表明Request-URL指定的资源的不同操作方式：
 - GET：请求获取Request-URL所标识的资源。在浏览器的地址栏中输入网址的方式访问网页时，浏览器采用GET方法向服务器请求网页
 - POST：在Request-URL所标识的资源后附加新的数据。要求被请求服务器接受附在请求后面的数据，常用于提交表单。比如向服务器提交信息、发帖、登录。
 - HEAD：请求获取由Request-URL所标识的资源的响应消息报头。
 - PUT：请求服务器存储一个资源，并用Request-URL作为其标识。
 - DELETE：请求服务器删除Request-URL所标识的资源。
 - TRACE：请求服务器回送收到的请求信息，主要用于测试或诊断。
 - CONNECT：用于代理服务器。
 - OPTIONS：请求查询服务器的性能，或者查询与资源相关的选项和需求。

9.5.7 HTTP 响应报文

■ 状态码（Status-Code）都是三位数字的，分为5大类共33种，例如：

- 1xx表示通知信息的，如请求收到了或正在进行处理。
- 2xx表示成功，如接受或知道了。
- 3xx表示重定向，如要完成请求还必须采取进一步的行动。
- 4xx 表示客户端错误，如请求中有错误的语法或不能完成。
- 5xx表示服务器的差错，如服务器失效无法完成请求。

■ 下面三种状态行在响应报文中是经常见到的。

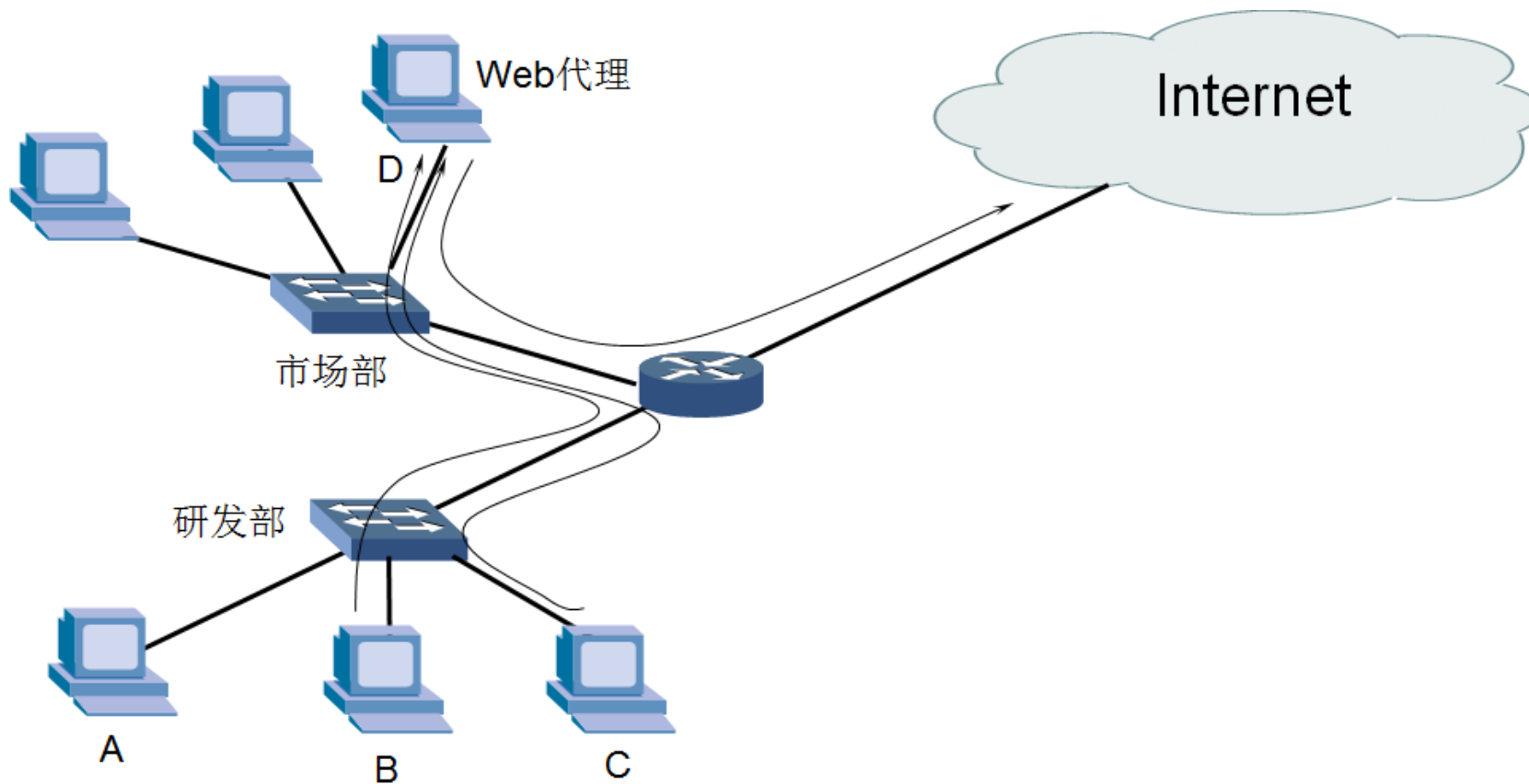
- HTTP/1.1 200 Success （成功）
- HTTP/1.1 202 Accepted （接受）
- HTTP/1.1 400 Bad Request （错误的请求）
- HTTP/1.1 404 Not Found （找不到）

9.5.8 Cookie

- **Cookie**意为“甜饼”，是由W3C组织提出，最早由Netscape社区发展的一种机制。目前**Cookie**已经成为标准，所有的主流浏览器如IE、Netscape、Firefox、Opera等都支持**Cookie**。
- 由于**HTTP**是一种无状态的协议，服务器单从网络连接上无从知道客户身份。怎么办呢？就给客户端们颁发一个通行证吧，每人一个，无论谁访问都必须携带自己通行证。这样服务器就能从通行证上确认客户身份了。这就是**Cookie**的工作原理。
- **Cookie**可以导出导入。

9.5.9通过代理服务器访问网站

- 代理服务器英文全称是（**Proxy Server**），其功能就是代理网络用户去取得网络信息。我们可以配置计算机通过**Web代理服务器**访问**Web**站点，而不直接访问网站。



9.6文件传输协议FTP

■FTP 是File Transfer Protocol（文件传输协议）的英文简称。用于Internet上的控制文件的双向传输。基于不同的操作系统有不同的FTP应用程序，而所有这些应用程序都遵守同一种协议以传输文件。在FTP的使用当中，用户经常遇到两个概念：

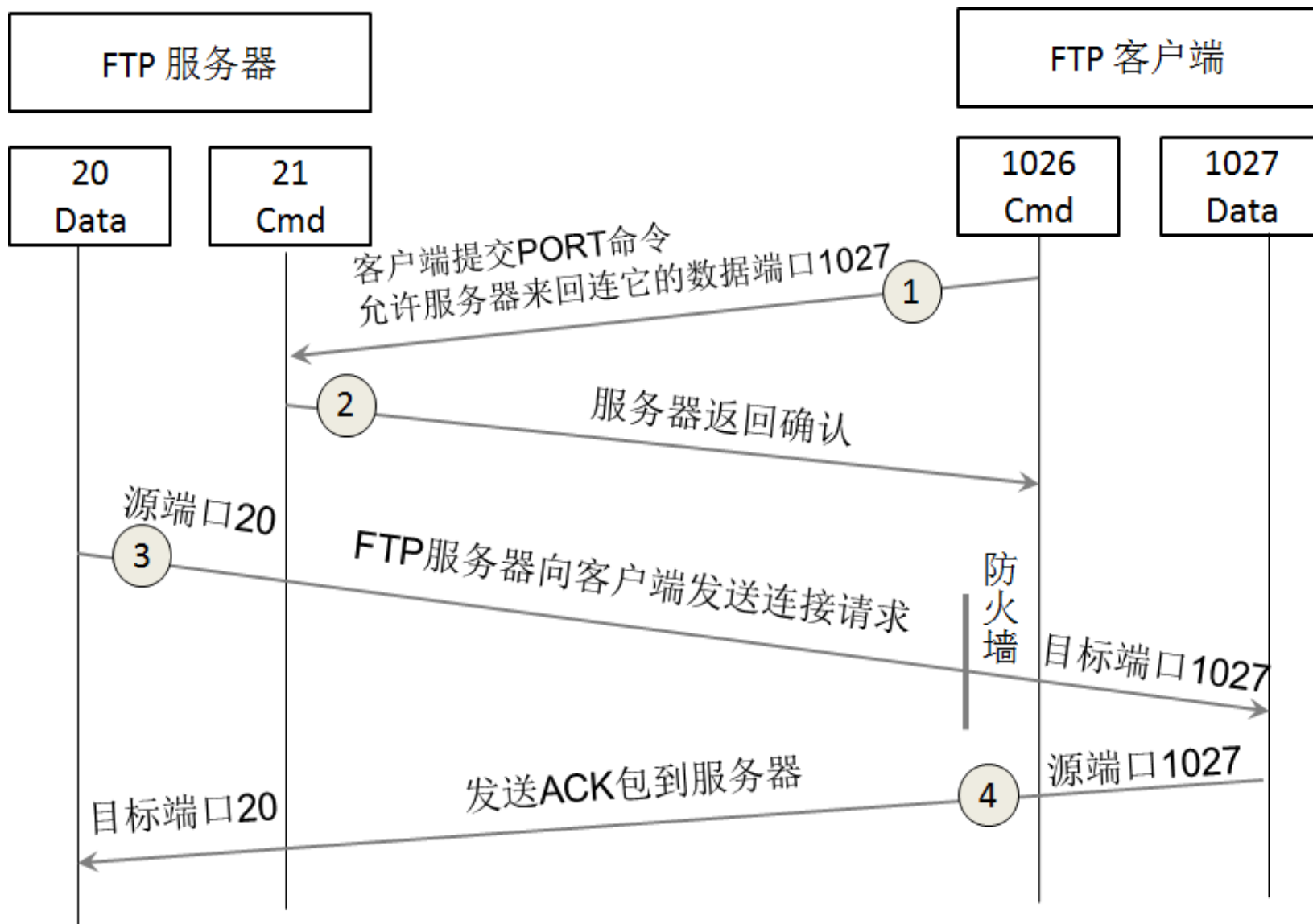
“下载”（Download）和“上传”（Upload）。“下载”文件就是从远程主机拷贝文件至自己的计算机上；“上传”文件就是将文件从自己的计算机中拷贝至远程主机上。用Internet语言来说，用户可通过客户机程序向（从）远程主机上传（下载）文件。

■简单地说，支持FTP协议的服务器就是FTP服务器。

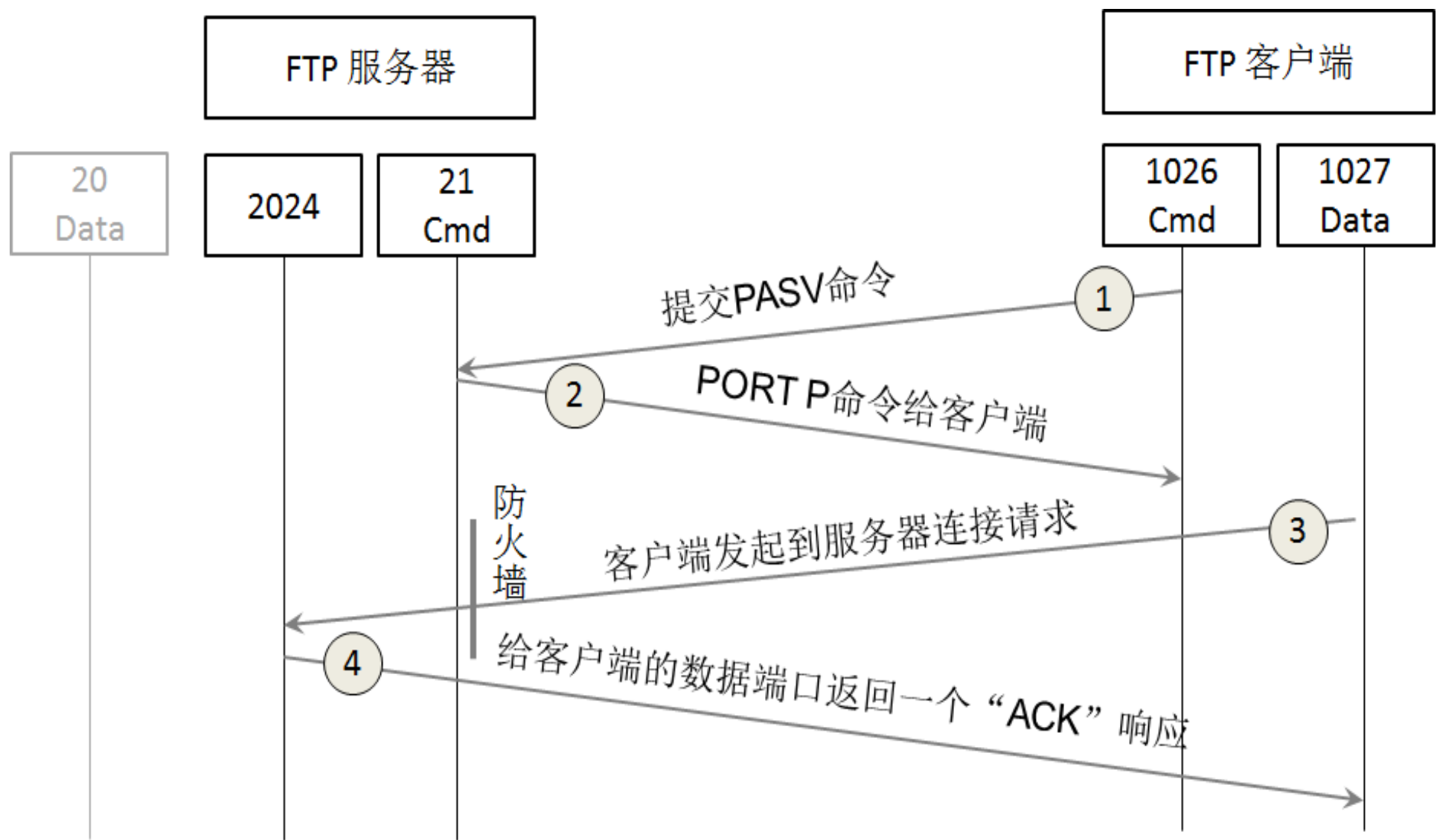
9.6.1 FTP主动模式和被动模式

- **FTP**协议和其他协议不一样的地方就是客户端访问**FTP**服务器需要建立两个**TCP**连接，一个是用来传输**FTP**命令，一个用来传输数据。在**FTP**服务器上需要开放两个端口，一个命令端口（或称为控制端口）和一个数据端口。通常**21**端口是命令端口，**20**端口是数据端口。当混入主动/被动模式的概念时，数据端口就有可能不是**20**了。

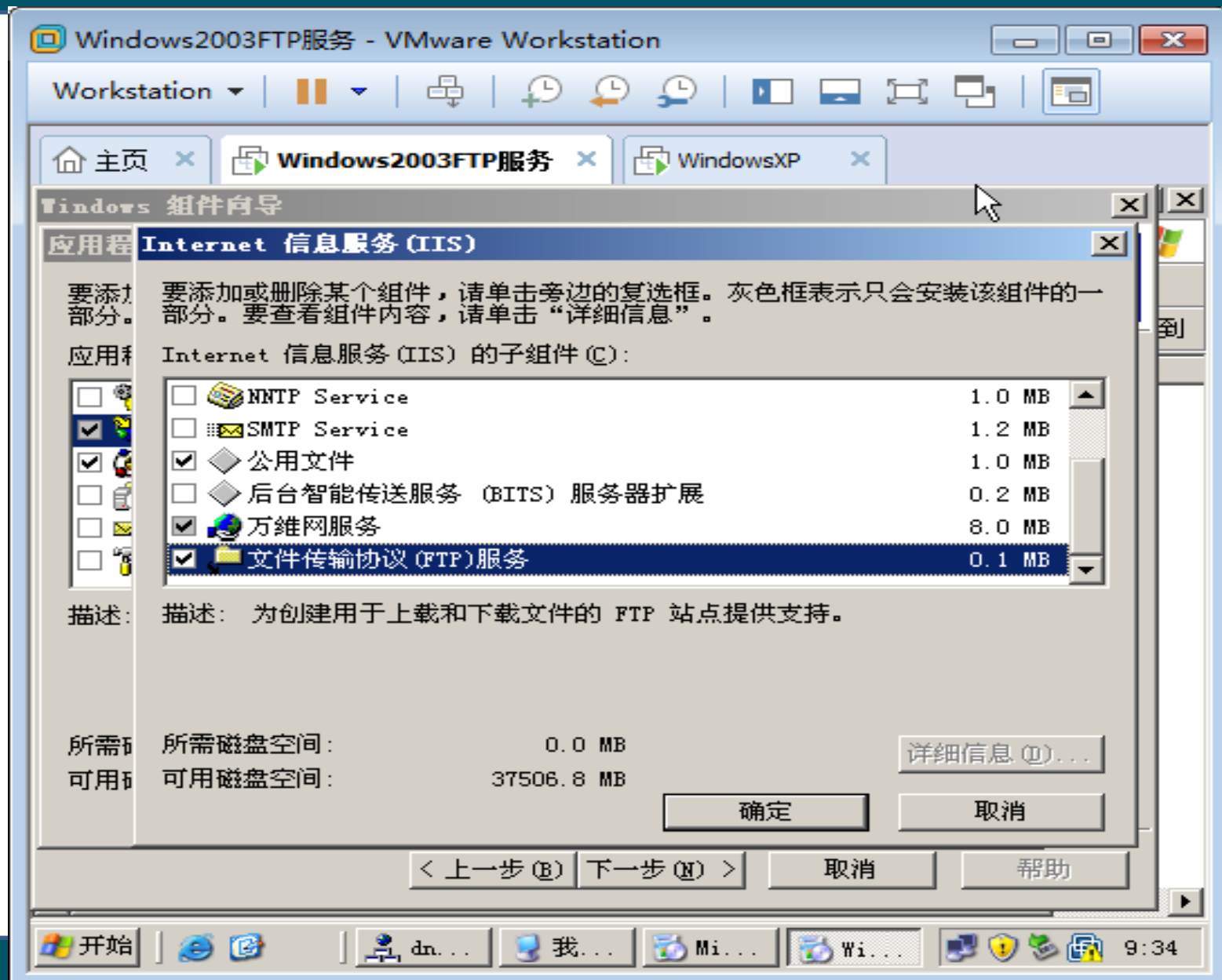
FTP主动模式



被动模式FTP

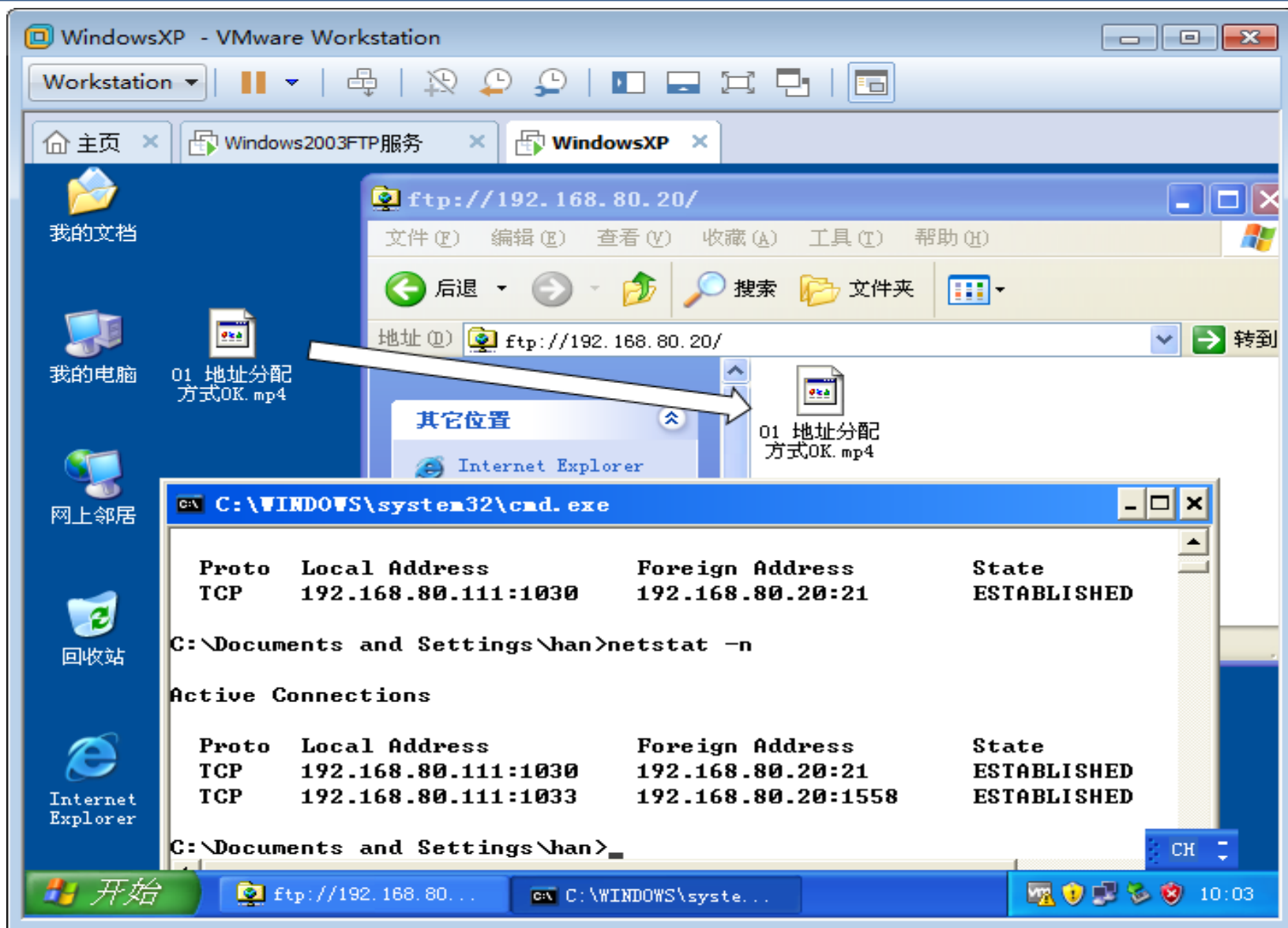


9.6.2 安装和创建FTP站点

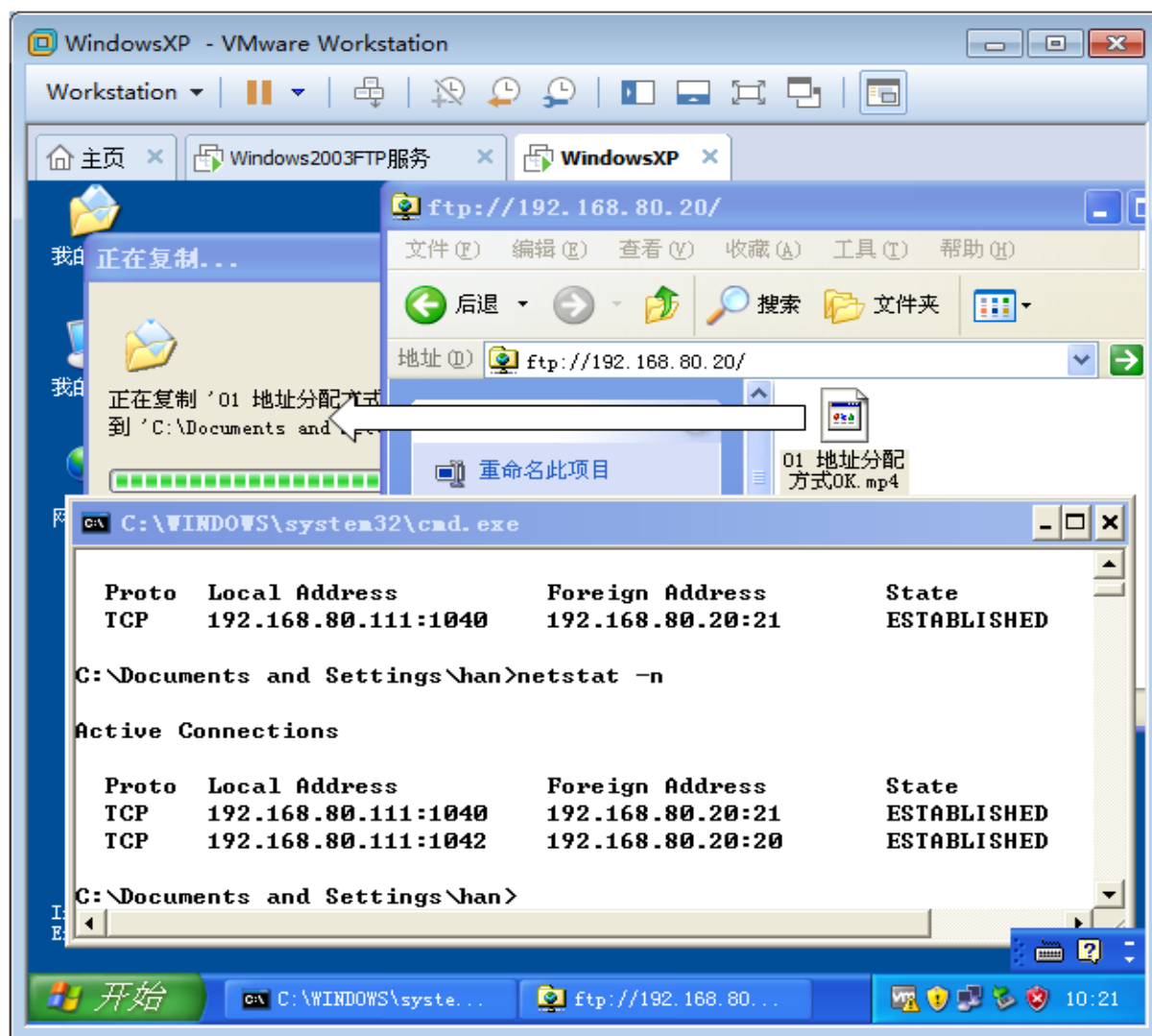
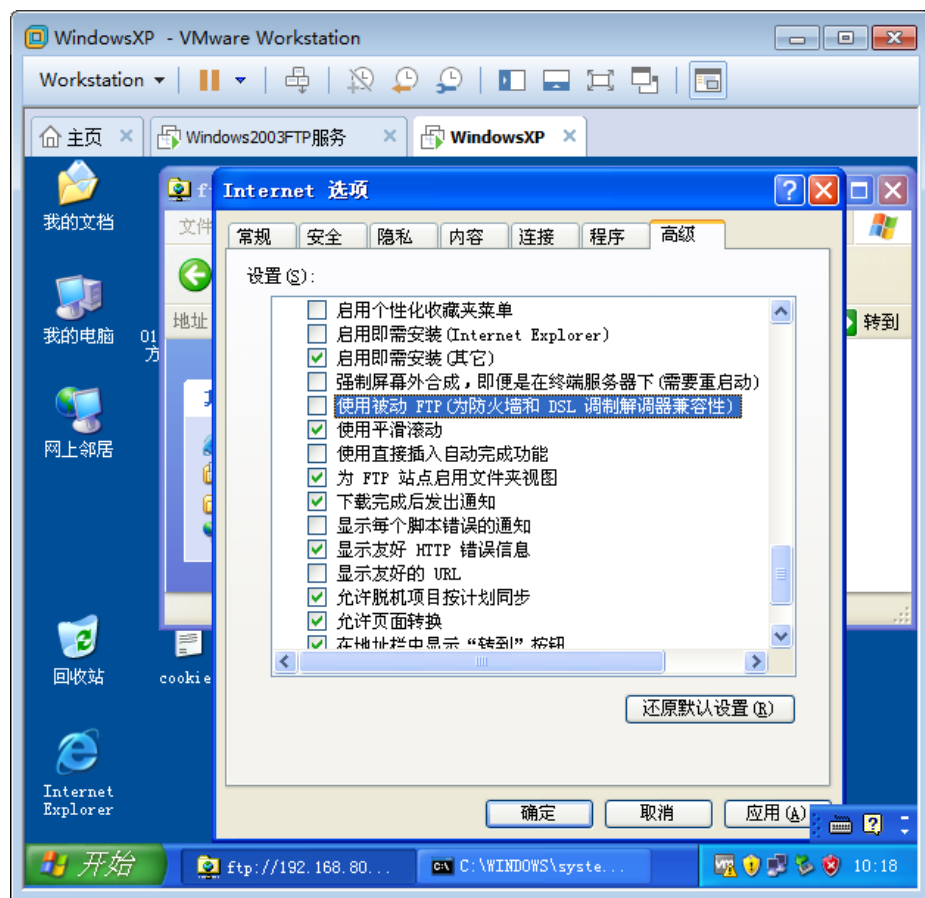


9.6.3访问FTP服务器

■ 被动模式



更改成主动模式



9.6.4 FTP命令访问FTP服务器

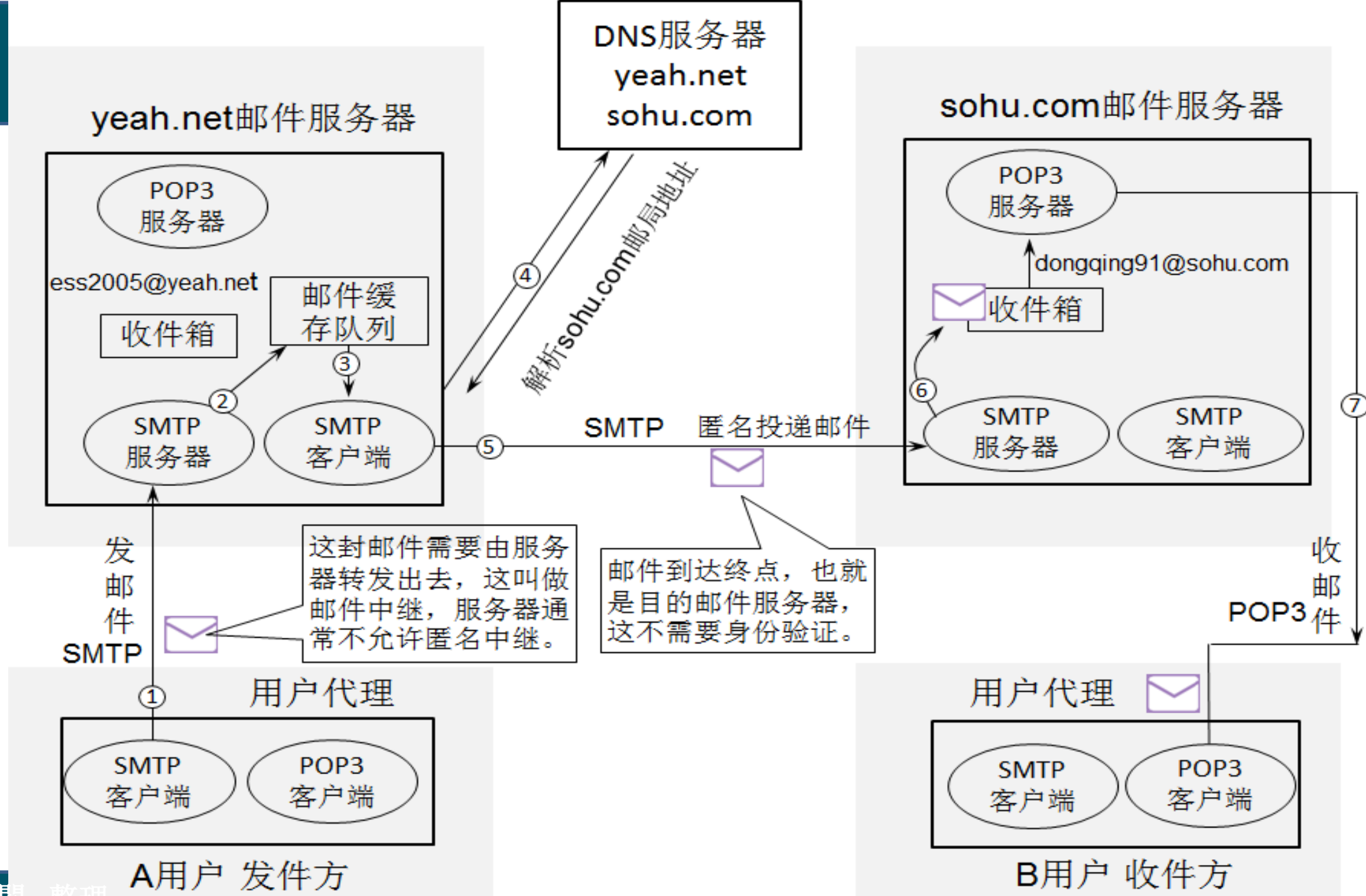
- C:\Documents and Settings\han>ftp
- ftp> open 192.168.80.20 --连接到FTP服务器
- Connected to 192.168.80.20.
- 220 Microsoft FTP Service
- User (192.168.80.20: (none)) : administrator --输入账户
- 331 Password required for administrator.
- Password: --输入密码，不回显输入，不能是空密码
- 230 User administrator logged in.
- ftp> ls --列出FTP服务器上的内容
- 200 PORT command successful.
- 150 Opening ASCII mode data connection for file list.
- 01 地址分配方式OK.mp4 --一个MP4文件
- 226 Transfer complete.

9.7电子邮件

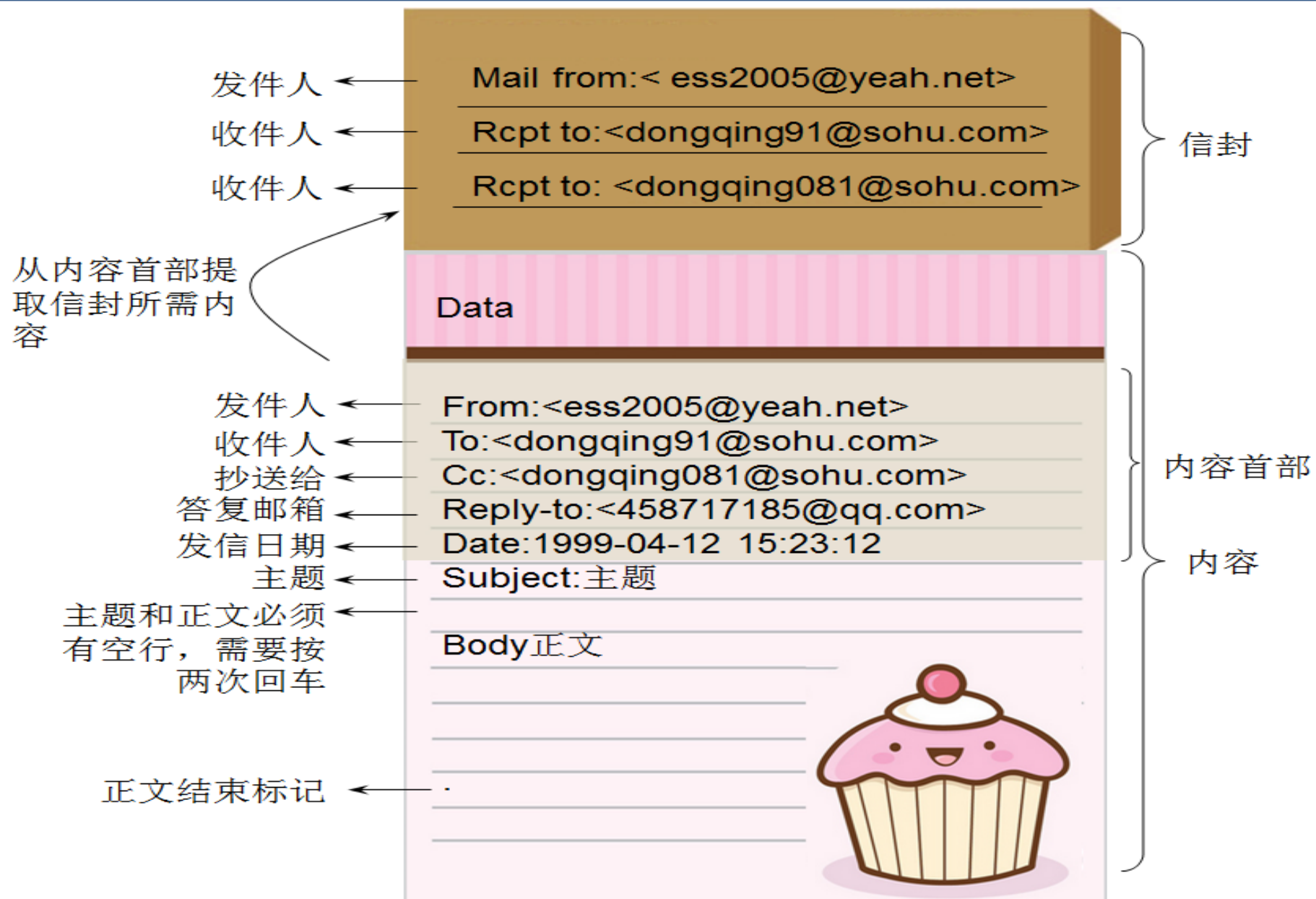
- 9.7.1电子邮件发送和接收过程
- 9.7.2电子邮件信息格式
- 9.7.3SMTP协议
- 9.7.4POP3协议和IMAP协议
- 9.7.5部署企业内部邮件服务器

9.7.1

电子邮件发送和接收过程

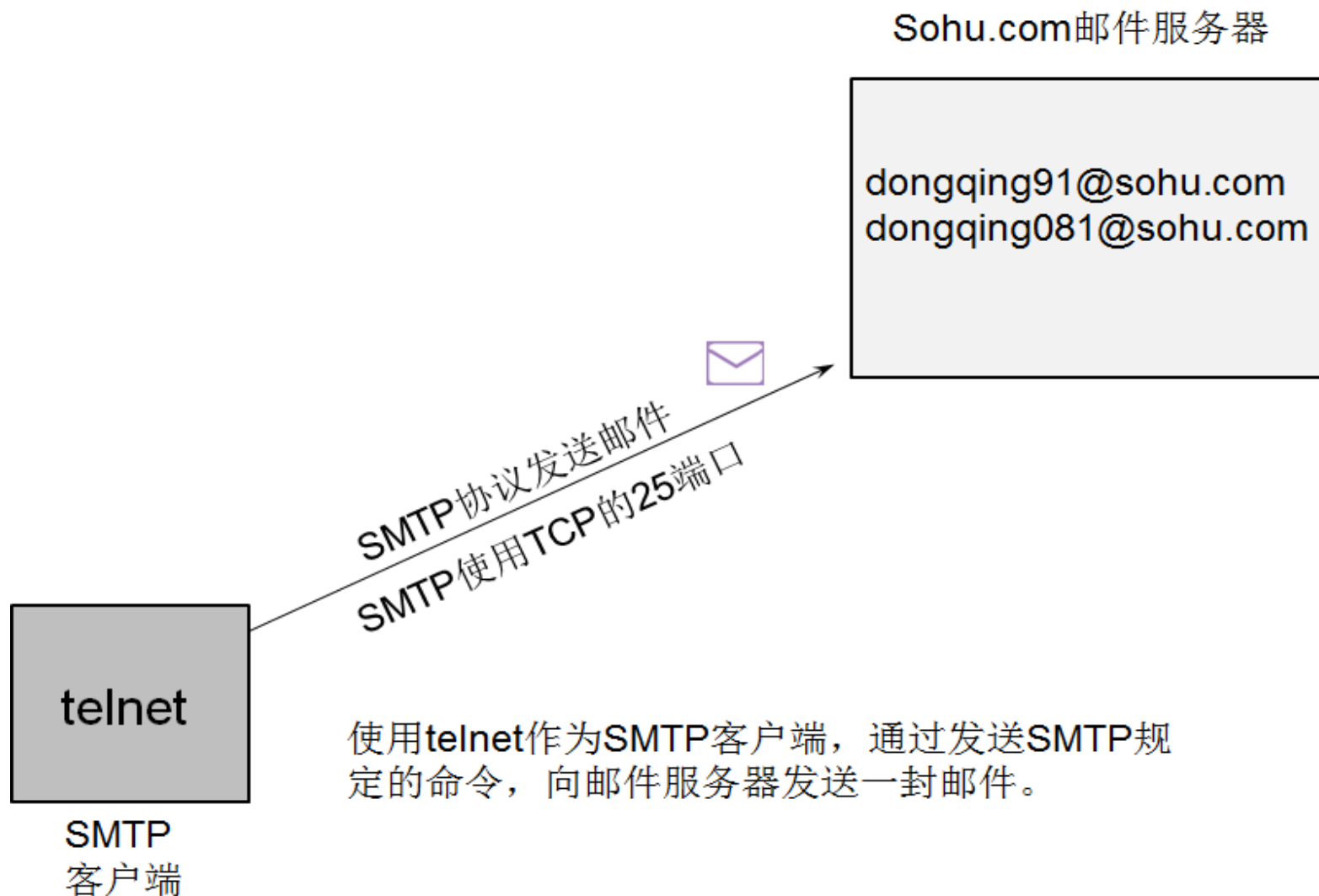


9.7.2电子邮件信息格式



9.7.3 SMTP协议

■SMTP规定了14条命令和21种应答信息。每条命令用4个字母组成，而每一种应答信息一般只有一行信息，由一个3位数字的代码开始，后面附上（也可不附上）很简单的文字说明。



使用nslookup查找某个域名的邮件服务器

将查找类型设置为MX，默认为A
查找sohu.com的邮件服务器

找到三个邮件服务器

将查找类型改回A

解析该域名的IP地址

解析出的IP地址

```
C:\Windows\system32\cmd.exe

C:\Users\han>nslookup
默认服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

> set type=MX
> sohu.com
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
sohu.com      MX preference = 5, mail exchanger = sohumx1.sohu.com
sohu.com      MX preference = 5, mail exchanger = sohumx2.sohu.com
sohu.com      MX preference = 10, mail exchanger = sohumx.h.a.sohu.com

> set type=A
> sohumx2.sohu.com
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
名称:  sohumx2.sohu.com
Address:  123.125.123.1

> quit

C:\Users\han>
```

半:

使用telnet发送一封电子邮件

telnet SMTP 服务器
通知服务器支持旧版SMTP
发件人
误写收件人
查无此人
错写邮箱
格式不对
收件人
收件人
开始写内容
内容首部
主题
必须有空行
正文
正文结束
断开连接

```
C:\Windows\system32\cmd.exe
C:\Users\han>telnet sohumx2.sohu.com 25
220 sohumx4_76.sohu.com ESMTP Postfix
helo Windows7
250 sohumx4_76.sohu.com
mail from:<ess2005@yeah.net>
250 2.1.0 Ok
rcpt to:<dongqing082@sohu.com>
550 5.1.1 <dongqing082@sohu.com>: Recipient address rejected: User unknown
in local recipient table
rcpt to:<dongqing.sohu.com>
504 5.5.2 <dongqing.sohu.com>: Recipient address rejected: need fully-
qualified address
rcpt to:<dongqing91@sohu.com>
250 2.1.5 Ok
rcpt to:<dongqing081@sohu.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
from:<ess2005@yeah.net>
to:<dongqing91@sohu.com>
cc:<dongqing081@sohu.com>
date:1999-04-21 12:23:25
subject:Detail report
Add a Textbox control to the report, just above the text box containing the
Sales Order title, aligned to the left edge.
.
250 2.0.0 Ok: queued as 3sT9Fs4mY4z30PFT
quit
221 2.0.0 Bye
遗失对主机的连接。
C:\Users\han>
```

写信封
写内容

9.7.4 POP3协议和IMAP协议

- 邮局协议POP是一个非常简单、功能有限的邮件读取协议。邮局协议POP最初公布于1984年[RFC 918]。经过几次更新，现在使用的是1996年的版本POP3[RFC1939]，它已成为因特网的正式标准。大多数的ISP都支持POP，POP3可简称为POP。
- 另一个读取邮件的协议是网际报文存取协议IMAP，它比POP3复杂得多。IMAP和POP都按客户服务器方式工作，但它们有很大的差别。现在较新的版本是2003年3月修订的版本4，即IMAP4[RFC 3501]，它目前还只是因特网的建议标准。

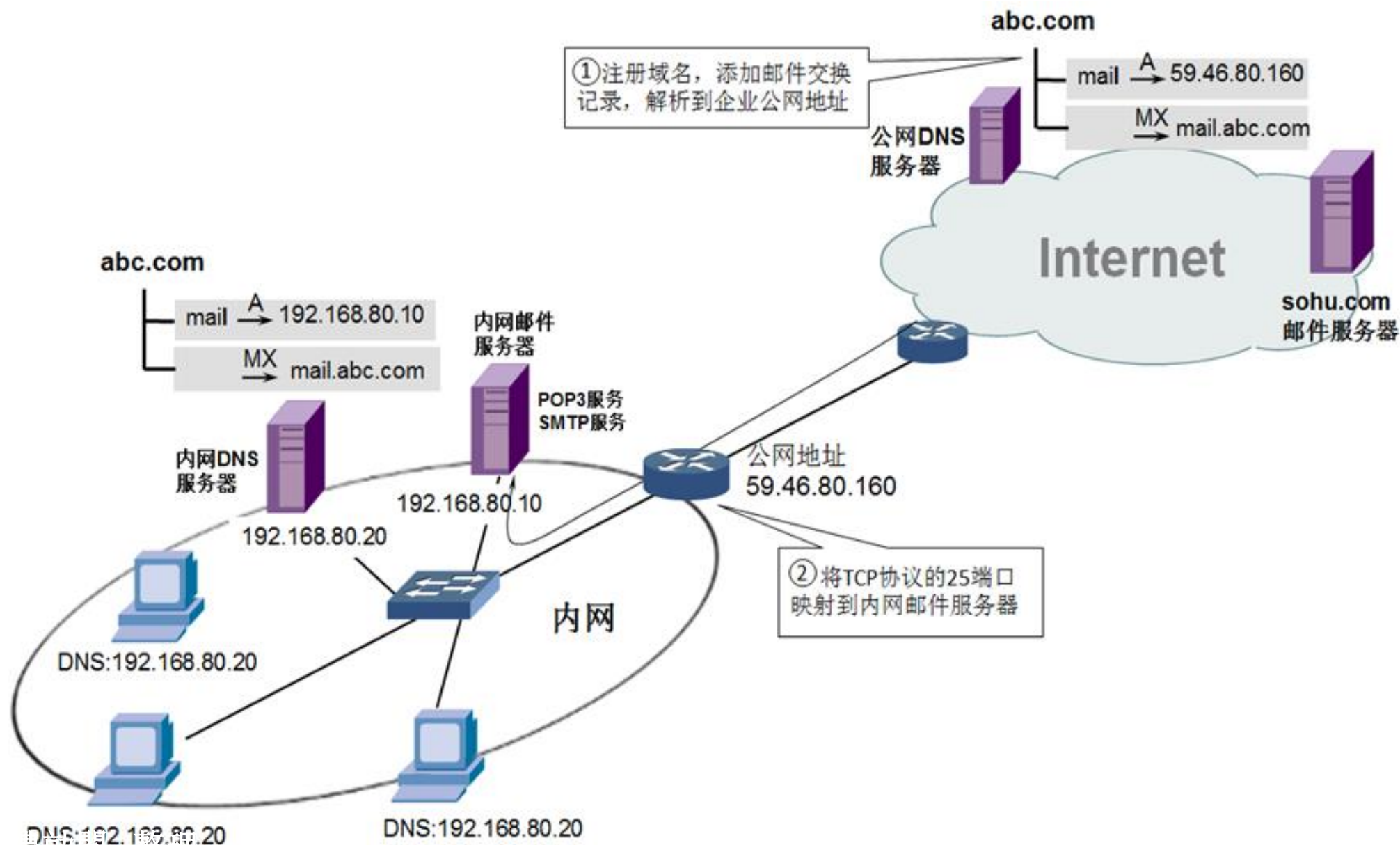
9.7.5部署企业内部邮件服务器1

- 第一种情况：在内网部署一个邮件服务器，实现内网员工之间用户相互发送接收邮件，向Internet发送电子邮件，不需要接收来自Internet的邮件。
 - 这种情况，内网的邮箱后缀可以随便指定，不用考虑和Internet上的域名是否冲突的问题，企业在内网部署了一个邮件服务器，邮箱后缀为abc.com，内网的计算机使用域名mail.abc.com访问内网邮件服务器，因此在内网部署一个DNS服务器，创建abc.com正向查找区，添加主机记录mail，添加邮件交换记录MX，指向mail.abc.com。

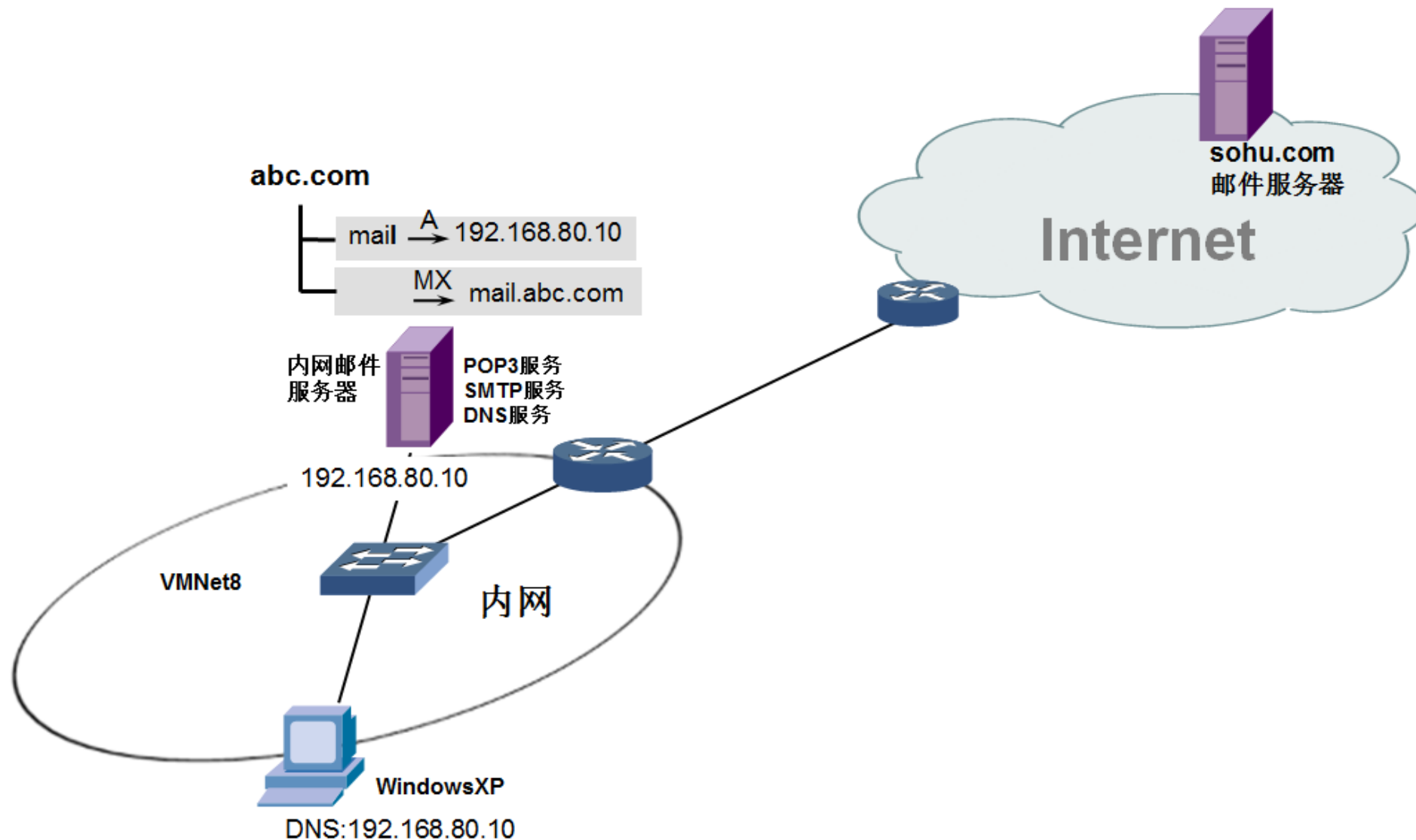
9.7.5部署企业内部邮件服务器2

- 第二种情况：如图所示，在内网部署一个能够向Internet发送邮件，也能够接收来自Internet的邮件的服务器。
- 要想让内网的邮件服务器收到来自Internet的邮件，需要满足两个条件：
 - 第一、需要企业在Internet上注册一个域名（比如是abc.com），添加邮件交换记录（MX记录），指向企业的公网地址。
 - 第二、在企业具有公网地址的网络设备上做端口映射，将TCP的25端口映射到内网的SMTP服务器。这样发给企业公网地址的邮件便能到达内网SMTP服务器。

内网邮件服务器能够接受Internet邮件的条件

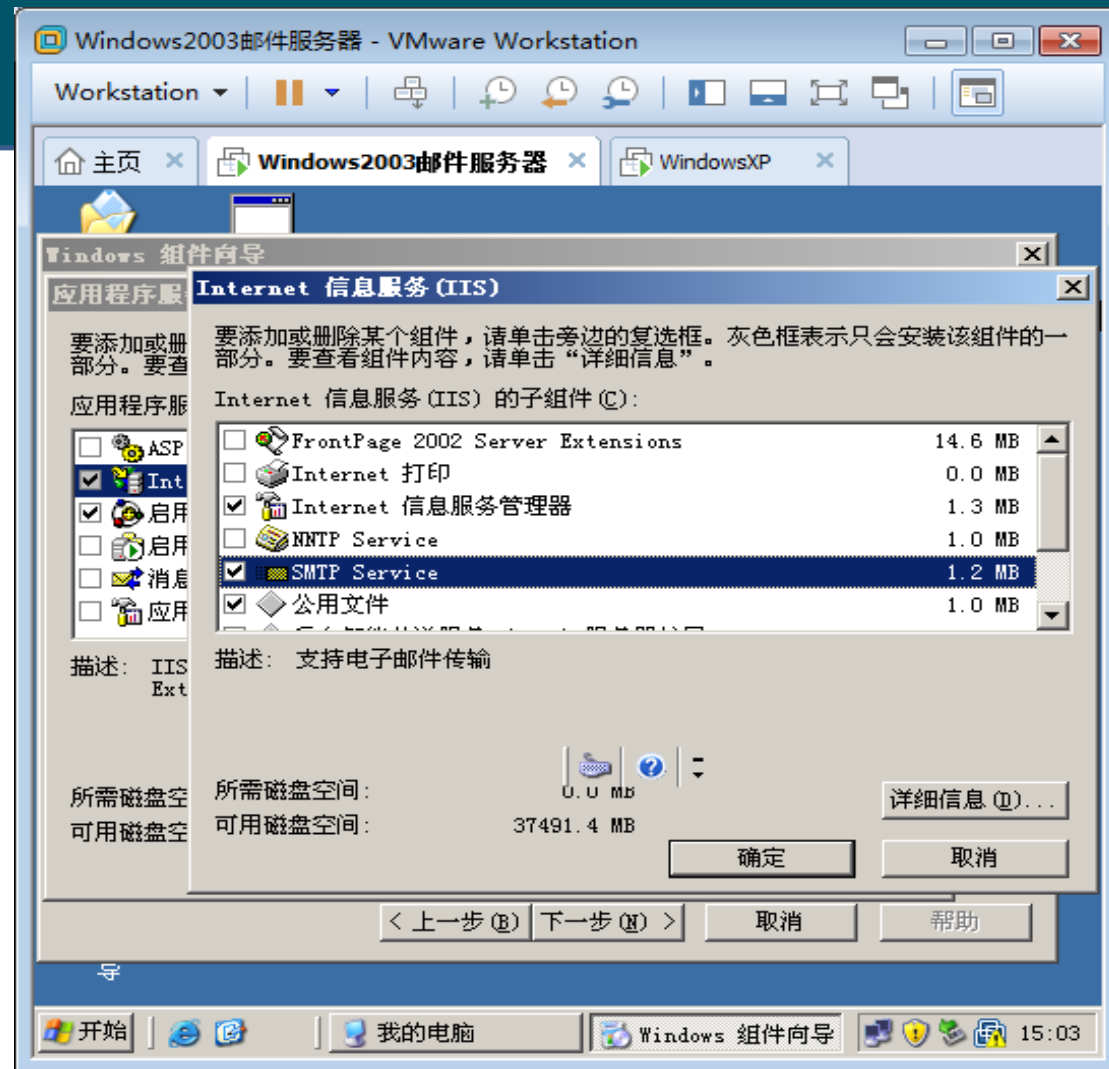
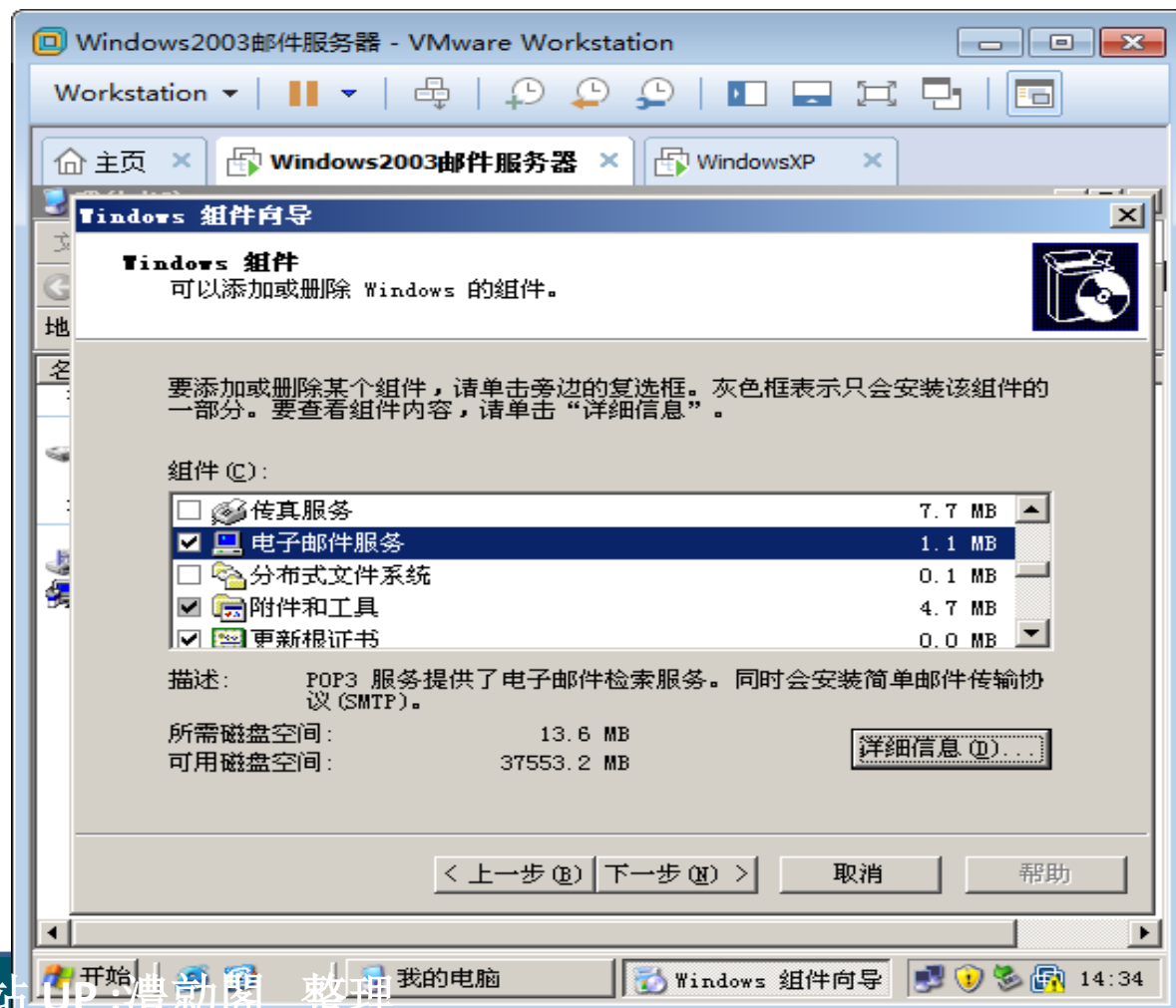


9.8实战：在内网部署邮件服务器向Internet发送邮件



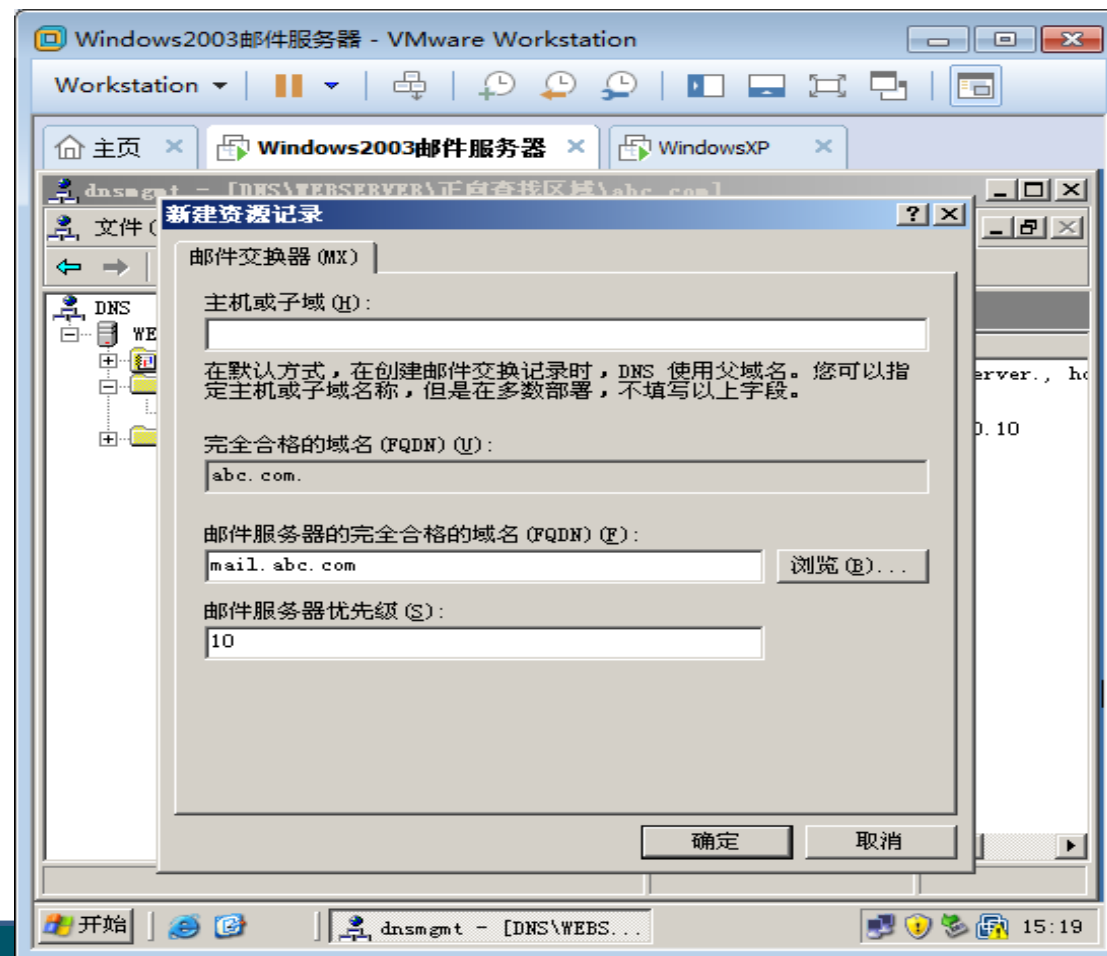
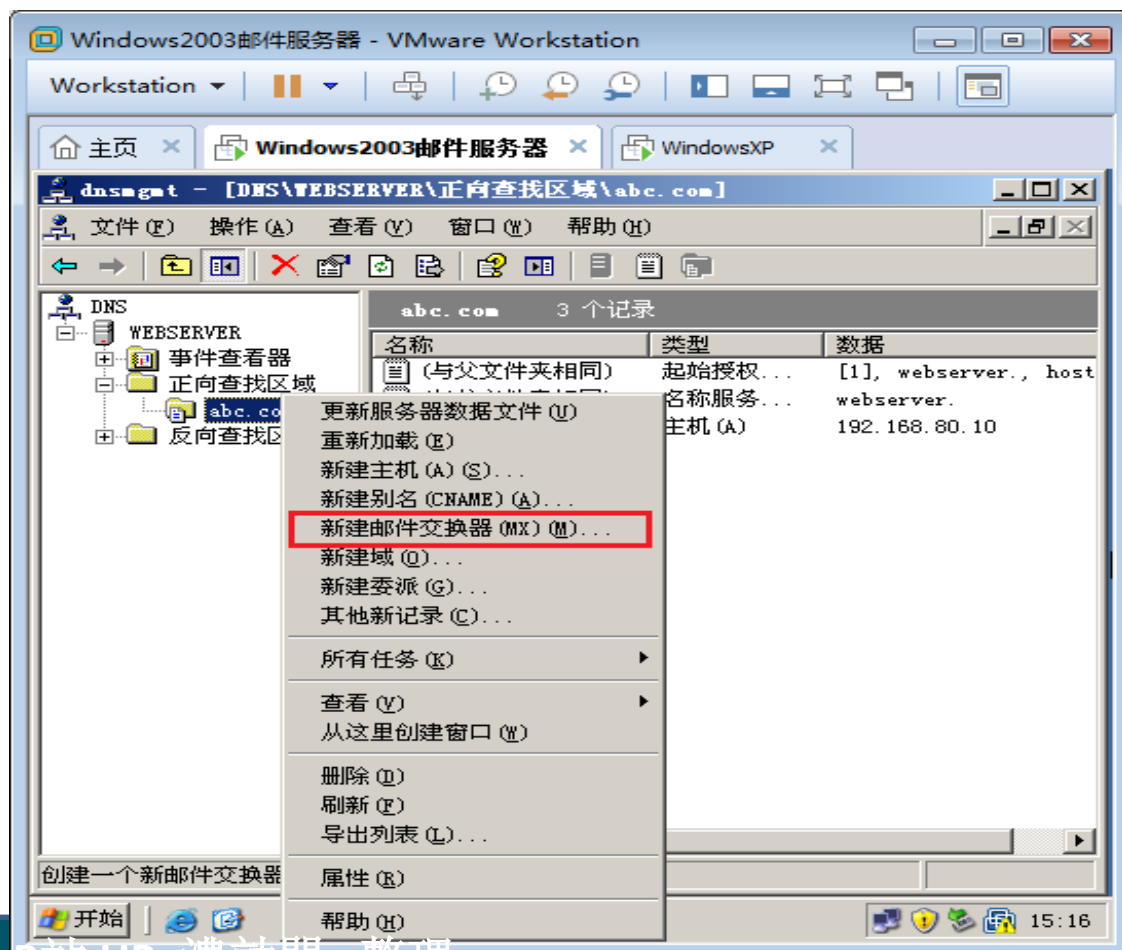
9.8.1 安装邮件服务器

■ 安装POP3和SMTP服务

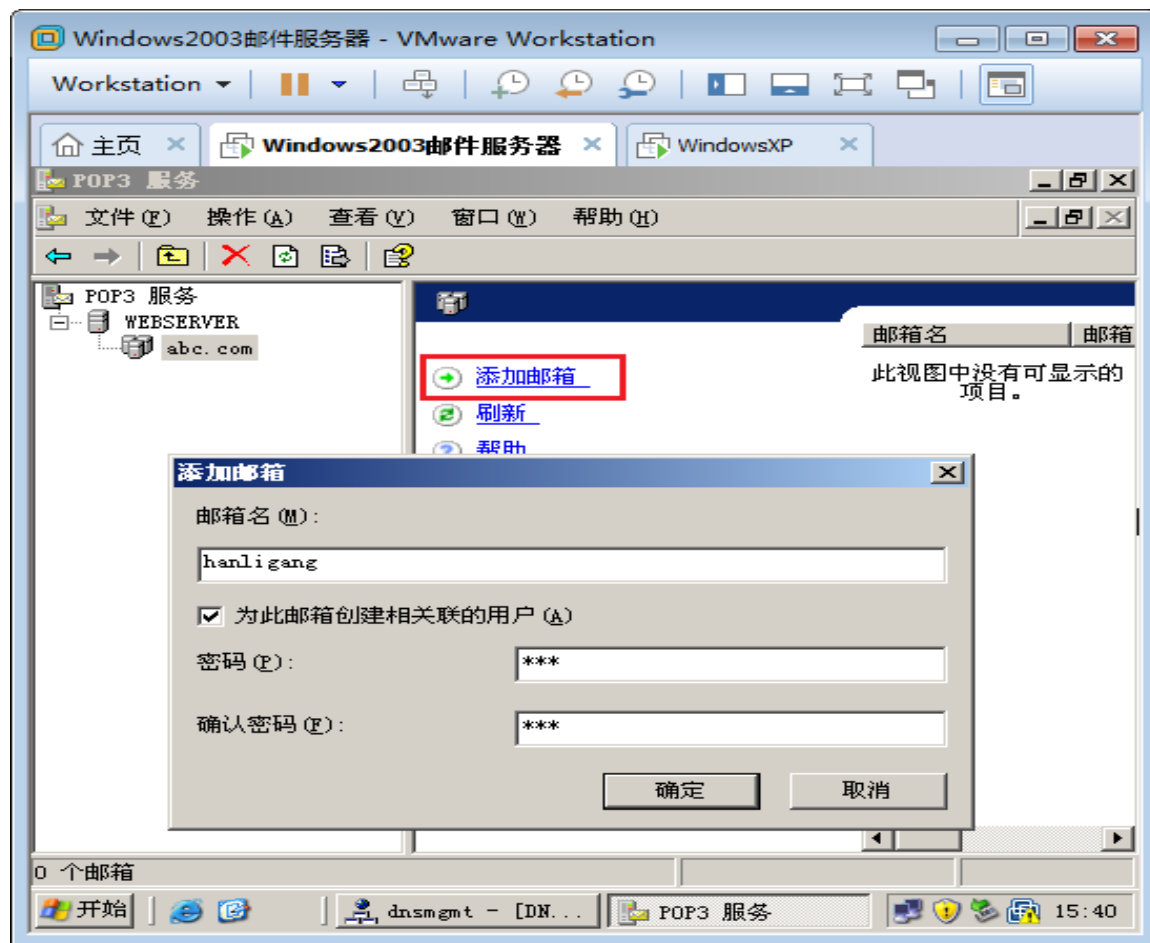
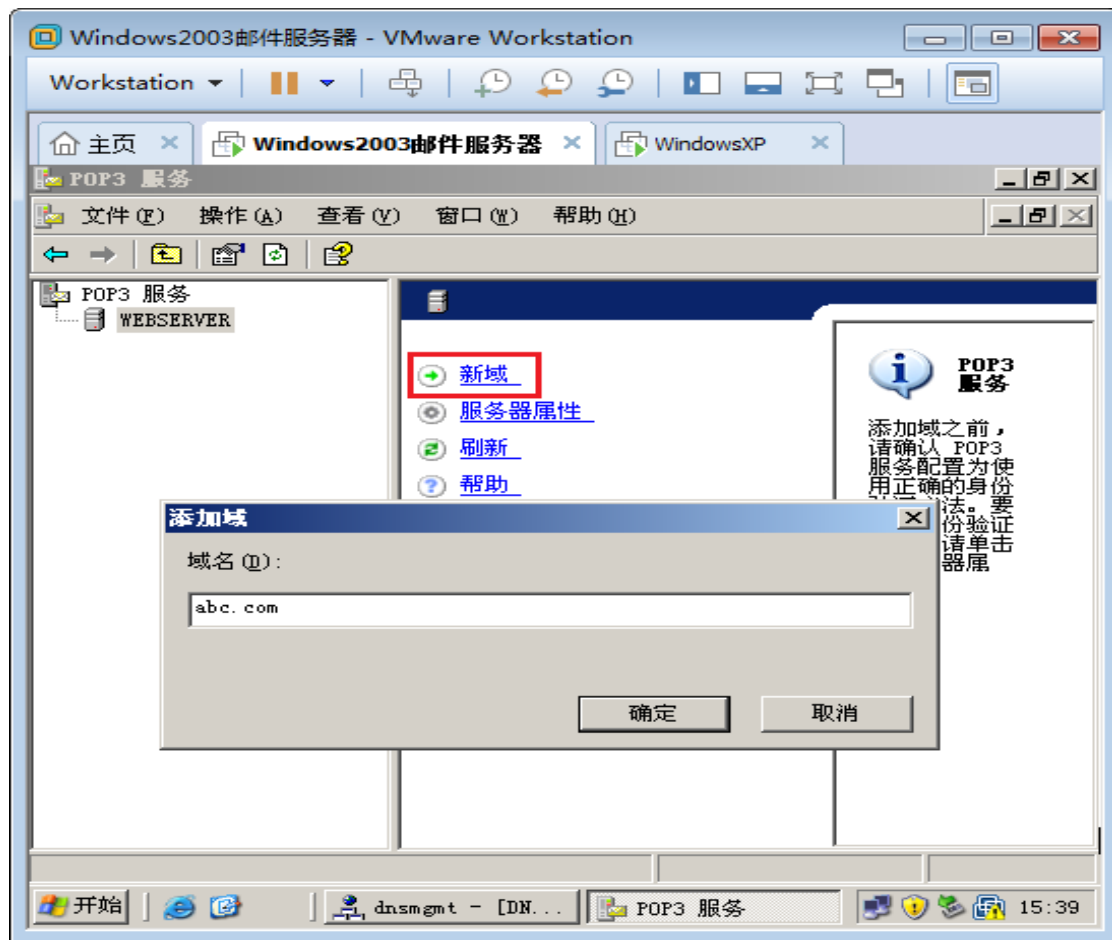


9.8.2在DNS服务器上添加MX记录

- 要想让内网中的计算机通过DNS服务器解析到abc.com邮件服务器，需要在DNS服务器上的abc.com区域添加邮件交换记录（MX记录）。

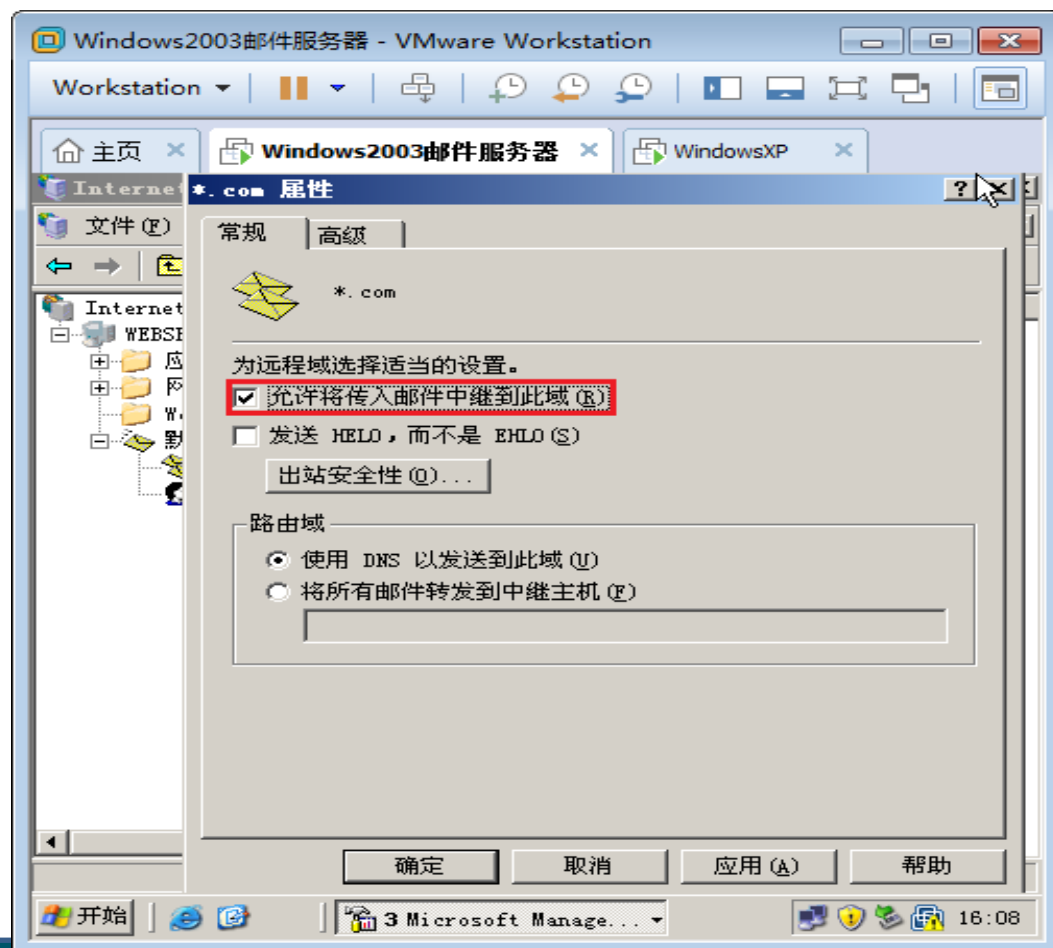
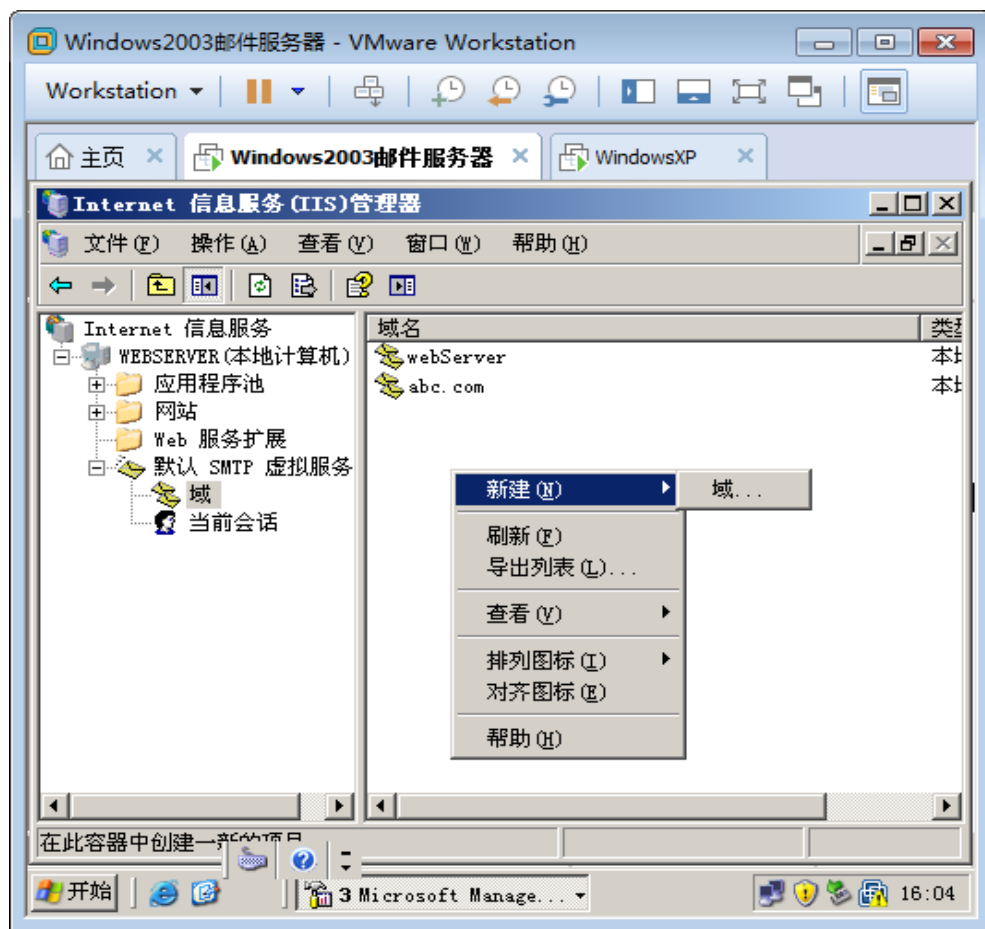


9.8.3为用户创建邮箱

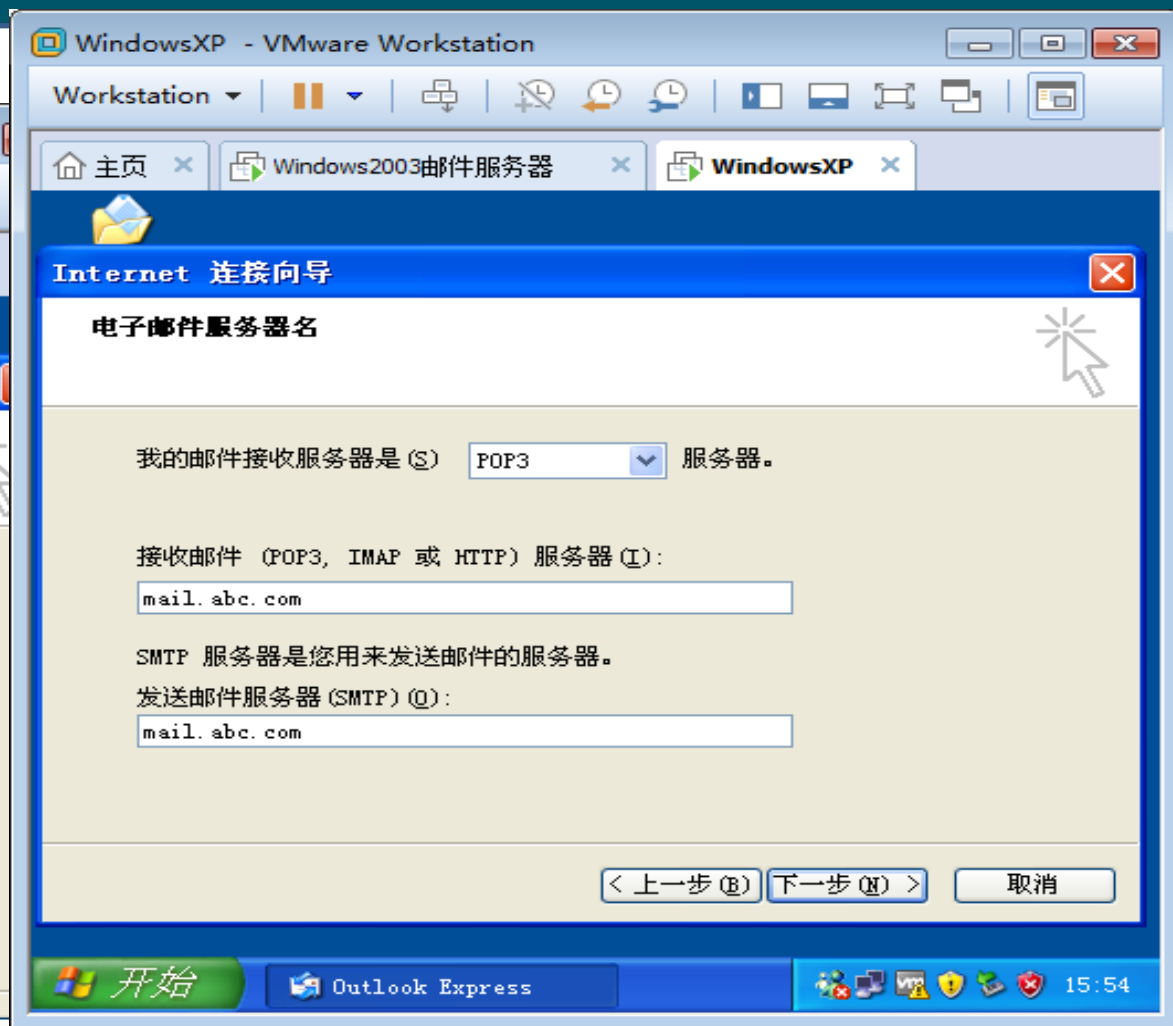
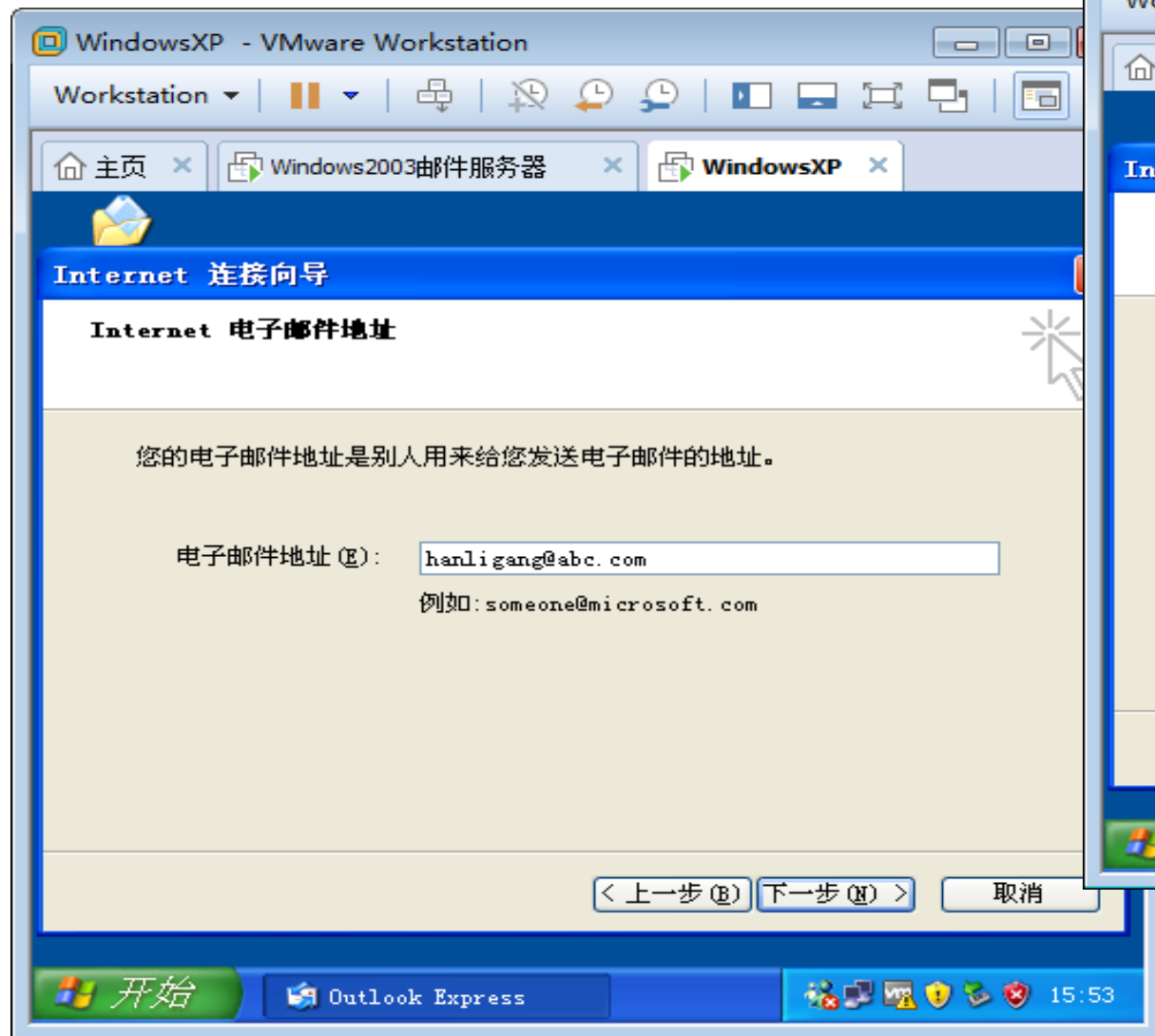


9.8.4配置SMTP服务允许向Internet发送电子邮件

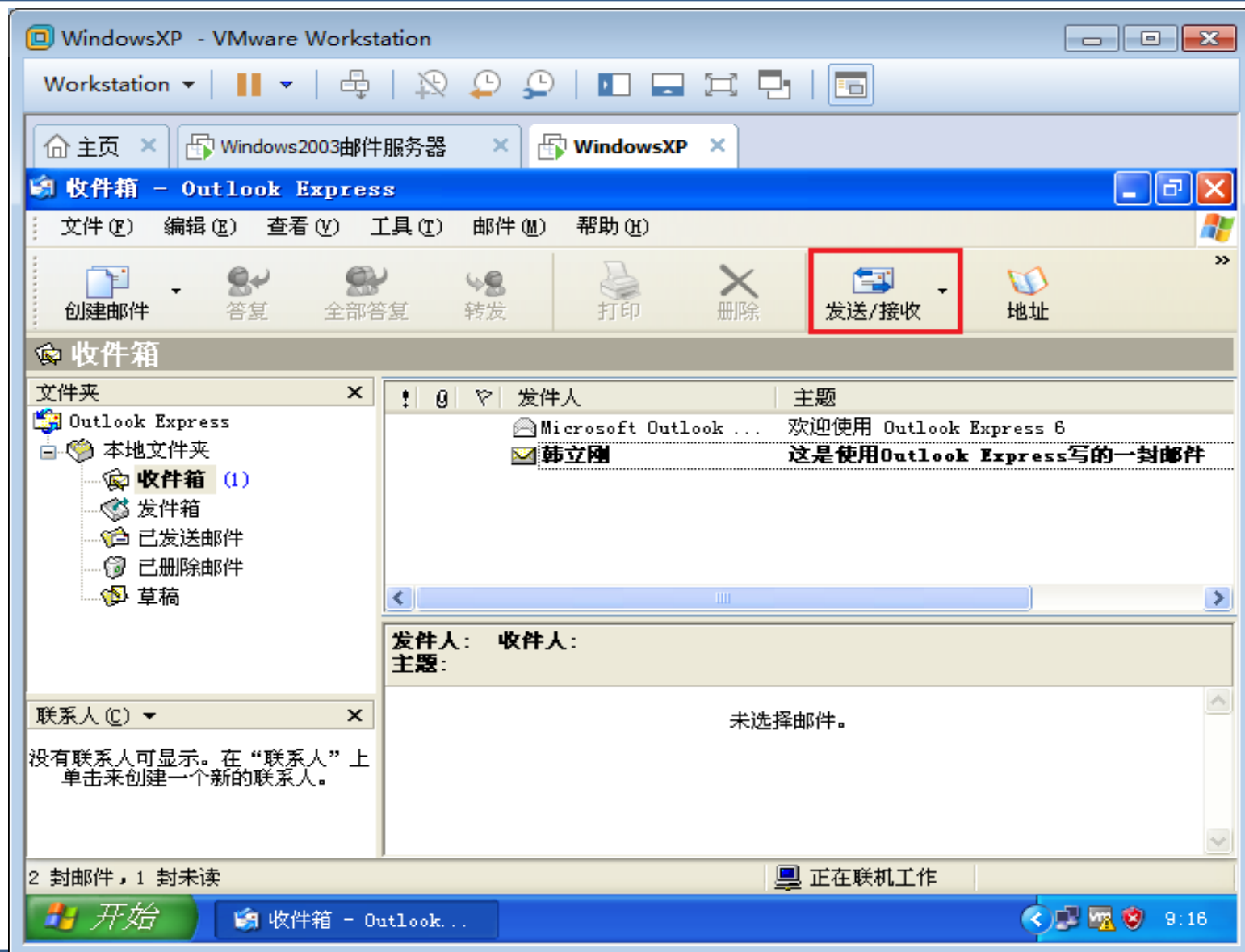
- 在WindowsServer2003上安装了SMTP服务，默认情况下，是不允许向Internet发送电子邮件的，需要配置SMTP服务器，指定可以向远程哪些域名转发电子邮件。



9.8.5配置邮件客户端连接邮件服务器



9.8.6向Internet发送电子邮件



发送电子邮件的数据包

建立TCP连接

发送电子邮件交互过程

命令

参数

SMP.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
18	2.50293400	192.168.80.111	192.168.80.10	TCP	62	1086→25 [SYN] Seq=0 win=65535 Len=0 MSS=1460 S
19	2.50295900	192.168.80.10	192.168.80.111	TCP	62	25→1086 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0
20	2.50318400	192.168.80.111	192.168.80.10	TCP	60	1086→25 [ACK] Seq=1 Ack=1 win=65535 Len=0
21	2.50449900	192.168.80.10	192.168.80.111	SMTP	164	S: 220 webServer Microsoft ESMTP MAIL Service,
22	2.50578600	192.168.80.111	192.168.80.10	SMTP	63	C: HELO xp
23	2.56270600	192.168.80.10	192.168.80.111	SMTP	92	S: 250 webServer Hello [192.168.80.111]
24	2.56366400	192.168.80.111	192.168.80.10	SMTP	86	C: MAIL FROM: <hanligang@abc.com>
25	2.58243800	192.168.80.10	192.168.80.111	SMTP	96	S: 250 2.1.0 hanligang@abc.com...Sender OK
26	2.58302300	192.168.80.111	192.168.80.10	SMTP	86	C: RCPT TO: <dongqing91@sohu.com>
27	2.58319200	192.168.80.10	192.168.80.111	SMTP	86	S: 250 2.1.5 dongqing91@sohu.com
28	2.58363000	192.168.80.111	192.168.80.10	SMTP	84	C: RCPT TO: <hanligang@abc.com>
29	2.58369500	192.168.80.10	192.168.80.111	SMTP	84	S: 250 2.1.5 hanligang@abc.com
30	2.58559100	192.168.80.111	192.168.80.10	SMTP	60	C: DATA
31	2.58630000	192.168.80.10	192.168.80.111	SMTP	100	S: 354 Start mail input; end with <CRLF>.<CRLF>
32	2.58761300	192.168.80.111	192.168.80.10	SMTP	1496	C: DATA fragment, 1442 bytes
33	2.77202100	192.168.80.10	192.168.80.111	TCP	54	25→1086 [ACK] Seq=299 Ack=1552 win=64240 Len=0
34	2.77331600	192.168.80.111	192.168.80.10	IMF	60	from: =?gb2312?B?uqvBorjv?= <hanligang@abc.com>

交互过程

Frame 24: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

Ethernet II, Src: Vmware_cc:87:22 (00:0c:29:cc:87:22), Dst: Vmware_14:bf:02 (00:0c:29:14:bf:02)

Internet Protocol Version 4, Src: 192.168.80.111 (192.168.80.111), Dst: 192.168.80.10 (192.168.80.10)

Transmission Control Protocol, Src Port: 1086 (1086), Dst Port: 25 (25), Seq: 10, Ack: 149, Len: 32

Simple Mail Transfer Protocol

Command Line: MAIL FROM: <hanligang@abc.com>\r\n

Command: MAIL

Request parameter: FROM: <hanligang@abc.com>

0010 00 48 01 52 40 00 80 06 d7 93 c0 a8 50 6f c0 a8 .H.R@... ..Po..

0020 50 0a 04 3e 00 19 b0 c9 d7 ca 0d 26 f9 32 50 18 P..>....&.2P.

0030 ff 6b d9 6b 00 00 4d 41 49 4c 20 46 52 4f 4d 3a .k.k..MAIL FROM:

0040 20 3c 68 61 6e 6c 69 67 61 6e 67 40 61 62 63 2e <hanligang@abc.

0050 63 6f 6d 3e 0d 0a com>..

Command Line (smtp.command_line), 32 ... Packets: 102 · Displayed: 102 (100.0%) · Load time: 0:00.015 Profile: Default

9.9总结1

■通本章给大家介绍了几个常见的应用层协议，我们能够的到什么结论呢？

- 每个应用层协议都是为了解决特定问题、实现特定功能。比如HTTP协议为了能让浏览器请求网页、Web服务器给客户端返回网页，DNS协议为了实现域名解析，FTP协议为了实现文件上传下载，SMTP协议为了实现发送电子邮件，POP3为了实现让电子邮件客户端从服务器下载电子邮件，DHCP协议为了DHCP服务器给计算机分配IP地址。
- 应用层协议就是为了让客户端和服务端能够交换信息提前定义好一些规范。比如客户端需要向服务器发送哪些操作请求（比如HTTP协议定义的访问网站的GET、POST等方法，SMTP协议定义的发送邮件的命令HELO、RCPT TO等），服务器向客户端发送哪些响应（比如网站响应状态代码，SMTP服务器给SMTP客户端返回的状态代码，客户端要能够明白代码代表的意思）。

9.9总结2

■咱们在第一章，讲到协议三要素，语法、语义和同步。那时你可能不好理解这是什么意思，学完本章再来理解协议三要素。

- 请求报文和响应报文格式就是协议的语法。
- 报文中的每个字段不同的值的所代表的意义就是协议的语义。
- 客户端和服务端交互顺序（比如命令执行的顺序）就是协议的同步。



B站 UP : 澧劬閣 整理