

第7章 网络层协议

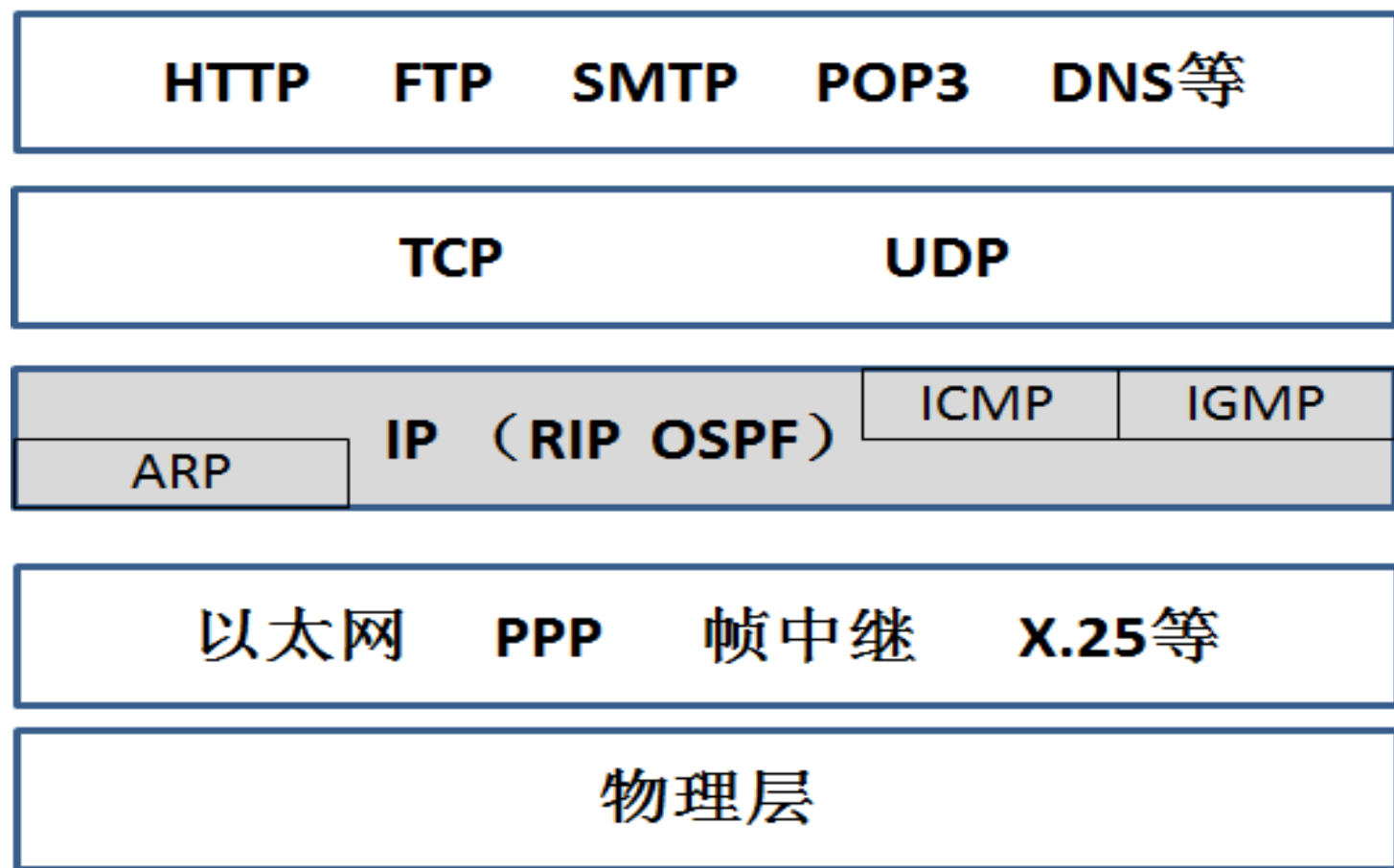


韩老师QQ 458717185
韩老师视频课程学习路线
www.91xueit.com
韩老师博客
<http://91xueit.blog.51cto.com/>

讲师：韩立刚
河北师大软件学院讲师
微软最有价值专家（MVP）
微软企业护航专家（ESS）

2016年11月21日晚录制/

TCP/IP协议栈



本章内容

- 网络层首部
- ICMP协议
- 使用ICMP排除网络故障案例
- ARP协议
- IGMP协议
- 实战：跨网段观看组播视频

7.1网络层首部

- 7.1.1抓包查看网络层首部
- 7.1.2网络层首部格式
- 7.1.3实战：查看协议版本和首部长度
- 7.1.4实战：给数据包设置区分服务字段
- 7.1.5数据分片详解
- 7.1.6实战：捕获并观察数据包分片
- 7.1.7实战：查看和配置链路MTU
- 7.1.8数据包生存时间（TTL）详解
- 7.1.9实战：指定ping命令发送数据包的TTL值
- 7.1.10实战：抓包查看数据包的TTL变化

7.1.1抓包查看网络层首部

版本
首部长度
区分服务
总长度
标识
标志
片偏移
生存时间
协议
首部校验和
源IP地址
目标IP地址

Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1329	9.20318900	59.46.80.160	10.7.10.135	TCP	1514	[TCP segment of a
1330	9.20395800	59.46.80.160	10.7.10.135	TCP	1514	[TCP segment of a
1331	9.20400700	10.7.10.135	59.46.80.160	TCP	54	53113→80 [ACK] Seq
1332	9.20475500	59.46.80.160	10.7.10.135	TCP	1514	[TCP segment of a
1333	9.20475600	59.46.80.160	10.7.10.135	TCP	1514	[TCP segment of a
1334	9.20475700	59.46.80.160	10.7.10.135	TCP	1514	[TCP segment of a
1335	9.20475700	59.46.80.160	10.7.10.135	TCP	1514	[TCP segment of a
1336	9.20482600	10.7.10.135	59.46.80.160	TCP	54	53113→80 [ACK] Seq

Frame 1333: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface

Ethernet II, Src: 50:da:00:ce:11:3c (50:da:00:ce:11:3c), Dst: AsustekC_2e:6e:1e (c8:60:00:2e:6e:1e)

Internet Protocol Version 4, Src: 59.46.80.160 (59.46.80.160), Dst: 10.7.10.135 (10.7.10.135)

Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECT-CE))
Total Length: 1500
Identification: 0x35e6 (13798)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 47
Protocol: TCP (6)
Header checksum: 0x6fda [validation disabled]
Source: 59.46.80.160 (59.46.80.160)
Destination: 10.7.10.135 (10.7.10.135)
[Source GeoIP: unknown]
[Destination GeoIP: unknown]

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 53113 (53113), Seq: 43933

0000 c8 60 00 2e 6e 1e 50 da 00 ce 11 3c 08 00 45 00 . . . n . P . . . < . . E .
0010 05 dc 35 e6 40 00 2f 06 6f da 3b 2e 50 a0 0a 07 . . 5 . @ . / . o . ; . P . . .
0020 0a 87 00 50 cf 79 ac 88 fb 22 5d e4 61 74 50 10 . . . P . y . . . " . j . a t P . .
0030 fa f0 62 eb 00 00 70 65 6e 20 72 75 6e 73 20 66 . . b . . . p e n r u n s f
0040 69 72 73 74 0a 09 09 09 74 68 61 74 2e 5f 64 65 i r s t t h a t . _ d e
0050 6c 61 79 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b l a y (f u n c t i o n () {
0060 0a 09 09 09 2f 2f 20 6a 51 75 65 72 79 20 63 // j q u e r y c
0070 72 65 61 74 65 73 20 61 20 73 70 65 63 69 61 6c r e a t e s a s p e c i a l

Internet Protocol Version 4 (ip), 20 bytes Packets: 5507 · Displayed: 5507... Profile: Default

网络层首部

7.1.2网络层首部格式

- IP数据包首部的格式能够说明IP协议都具有什么功能。
- IP数据包由首部和数据两部分组成。首部的前一部分是固定长度，共20个字节，是所有IP数据包必须有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。

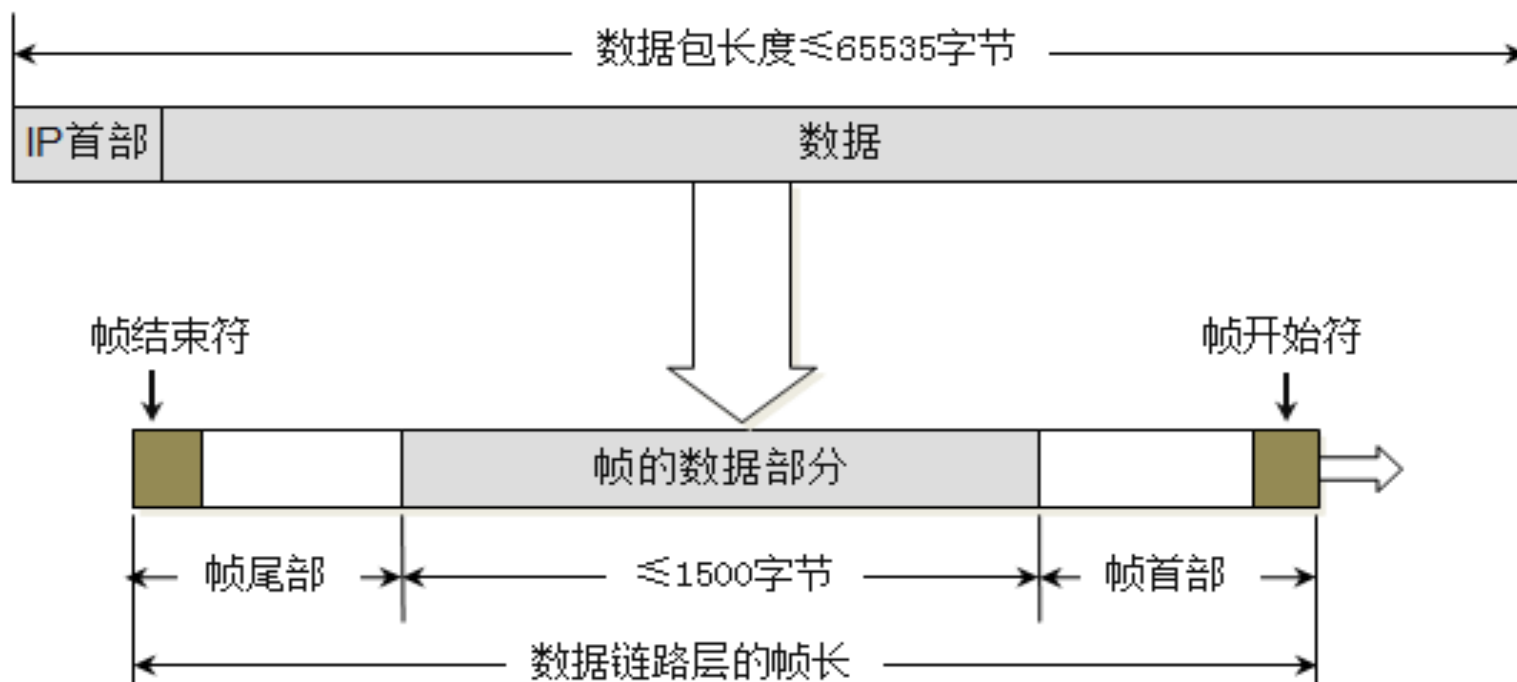


网络层首部固定部分各个字段(1)

- (1) 版本 占4位，指IP协议的版本。IP协议目前有两个版本IPv4和IPv6。通信双方使用的IP协议版本必须一致。目前广泛使用的IP协议版本号为4（即IPv4）。
- (2) 首部长度 占4位，可表示的最大十进制数值是15。请注意，这个字段所表示数的单位是32位二进制数（即4个字节），因此，当IP的首部长度为1111时（即十进制的15），首部长度就达到60字节。
- (3) 区分服务 占8位，配置计算机给特定应用程序的数据包添加一个标志，然后再配置网络中的路由器优先转发这些带标志的数据包，在网络带宽比较紧张的情况下，也能确保这种应用的带宽有保障，这就是区分服务，为这种服务确保服务质量（Quality of Service, QoS）。

网络层首部固定部分各个字段(2)

- (4) 总长度 总长度指IP首部和数据之和的长度，也就是数据包的长度，单位为字节。总长度字段为16位，因此数据包的最大长度为 $2^{16}-1=65535$ 字节。实际上传输这样长的数据包在现实中是极少遇到的。

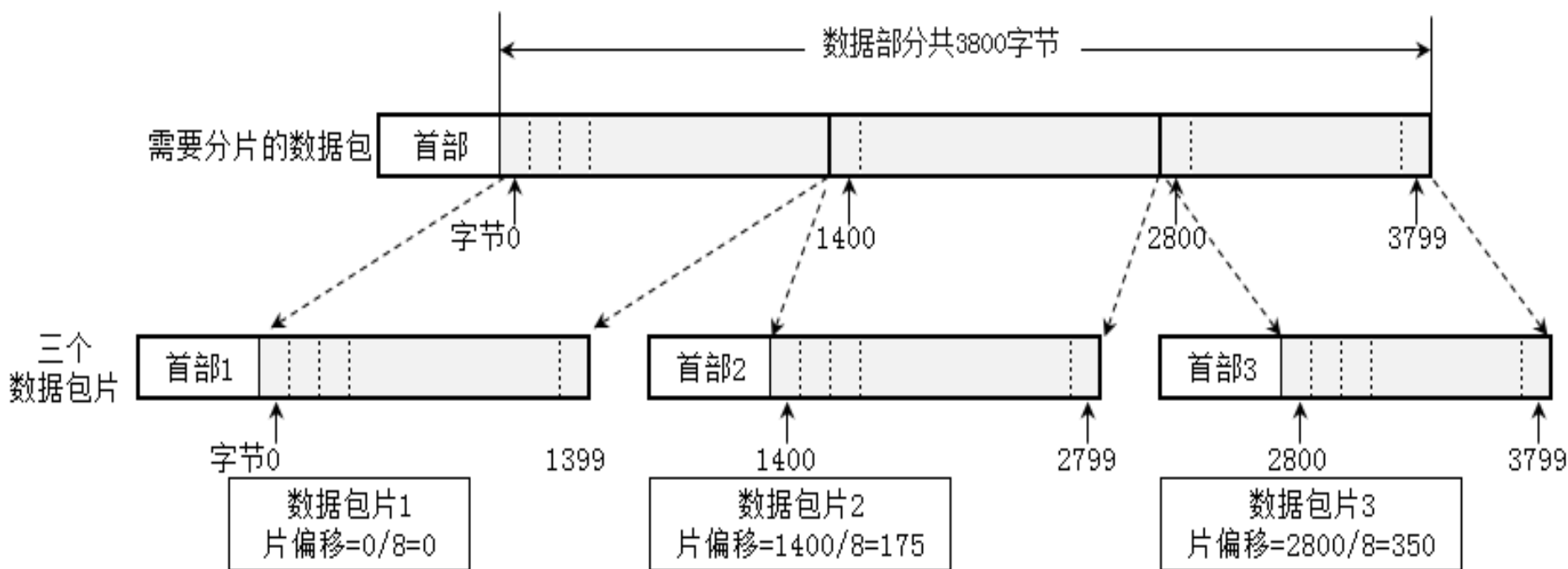


网络层首部固定部分各个字段(3)

- (5) 标识 (identification) 占16位。IP软件在存储器中维持一个计数器，每产生一个数据包，计数器就加1，并将此值赋给标识字段。但这个“标识”并不是序号，因为IP是无连接服务，数据包不存在按序接收的问题。当数据包由于长度超过网络的MTU而必须分片时，同一个数据包被分成多个片，这些片的标识都一样，也就是数据包这个标识字段的值就被复制到所有的数据包分片的标识字段中。相同的标识字段的值使分片后的各数据包片最后能正确地重装成为原来的数据包。
- (6) 标志 (flag) 占3位，但目前只有两位有意义。标志字段中的最低位记为MF (More Fragment) 。MF=1即表示后面“还有分片”的数据包。MF=0表示这已是若干数据包片中的最后一个。标志字段中间的一位记为DF (Don't Fragment) ，意思是“不能分片”。只有当DF=0时才一允许分片。

网络层首部固定部分各个字段(4)

- (7) 片偏移 占13位。片偏移指出：较长的分组在分片后，某片在原分组中的相对位置。也就是说，相对于用户数据字段的起点，该片从何处开始。片偏移以8个字节为偏移单位。这就是说，每个分片的长度一定是8字节（64位）的整数倍。



网络层首部固定部分各个字段(5)

■ (7) 片偏移 示例

	总长度	标识	MF	DF	片偏移
原始数据包	3820	12345	0	0	0
数据包片1	1420	12345	1	0	0
数据包片2	1420	12345	1	0	175
数据包片3	1020	12345	0	0	350

网络层首部固定部分各个字段(6)

- (8) 生存时间 生存时间字段常用的英文缩写是TTL (Time To Live) , 表明是数据包在网络中的寿命。现在TTL字段的功能改为“跳数限制”。
- (9) 协议 占8位, 协议字段指出此数据包携带的数据是使用何种协议, 以便使目的主机的网络层知道应将数据部分上交给哪个处理过程。

协议名	ICMP	IGMP	IP	TCP	EGP	IGP	UDP	IPv6	ESP	OSPF
协议字段值	1	2	4	6	8	9	17	41	50	89

网络层首部固定部分各个字段(7)

- (10) 首部检验和 占16位，这个字段只检验数据报的首部，但不包括数据部分。这是因为数据报每经过一个路由器，路由器都要重新计算一下首部检验和（一些字段，如生存时间、标志、片偏移等都可能发生变化）。不检验数据部分可减少计算的工作量。

7.1.3实战：查看协议版本和首部长度1

正在捕获 本地连接 2

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/> 表达式... +

No.	Time	Source	Destination	Protocol	Length	Info
10	2.033345	192.168.0.20	192.168.0.10	ICMP	74	Echo (ping...
11	3.046965	192.168.0.10	192.168.0.20	ICMP	74	Echo (ping...
12	3.047597	192.168.0.20	192.168.0.10	ICMP	74	Echo (ping...
13	6.939768	2001:2012:1975::606	2001:2012:1975::8	ICMPv6	94	Echo (ping...
14	6.940113	2001:2012:1975::8	2001:2012:1975::606	ICMPv6	94	Echo (ping...
15	7.944670	2001:2012:1975::606	2001:2012:1975::8	ICMPv6	94	Echo (ping...

Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: Vmware_ec:1b:90 (00:0c:29:ec:1b:90), Dst: Vmware_66:8b:ee (00:0c:29:66:8b:ee)

Internet Protocol Version 4, Src: 192.168.0.20, Dst: 192.168.0.10

0100 = Version: 4

.... 0101 = Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x0186 (390)

Flags: 0x00

0000 00 0c 29 66 8b ee 00 0c 29 ec 1b 90 08 00 45 00 ..)f....).....E.

0010 00 3c 01 86 00 00 80 01 b7 cc c0 a8 00 14 c0 a8 .<.....

0020 00 0a 00 00 55 4f 00 01 00 0c 61 62 63 64 65 66U0.. ..abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Version (ip.version), 1 字节 分组: 713 · 已显示: 713 (100.0%) 配置文件: Default

7.1.3实战：查看协议版本和首部长度2

正在捕获 本地连接 2

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/> 表达式...

No.	Time	Source	Destination	Protocol	Length	Info
10	2.033345	192.168.0.20	192.168.0.10	ICMP	74	Echo (ping...
11	3.046965	192.168.0.10	192.168.0.20	ICMP	74	Echo (ping...
12	3.047597	192.168.0.20	192.168.0.10	ICMP	74	Echo (ping...
13	6.939768	2001:2012:1975::606	2001:2012:1975::8	ICMPv6	94	Echo (ping...
14	6.940113	2001:2012:1975::8	2001:2012:1975::606	ICMPv6	94	Echo (ping...
15	7.944670	2001:2012:1975::606	2001:2012:1975::8	ICMPv6	94	Echo (ping...

Frame 13: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0

Ethernet II, Src: Vmware_66:8b:ee (00:0c:29:66:8b:ee), Dst: Vmware_ec:1b:90 (00:0c:29:ec:1b:90)

Internet Protocol Version 6, Src: 2001:2012:1975::606, Dst: 2001:2012:1975::8

0110 = Version: 6

.... 0000 0000 = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000

Payload length: 40

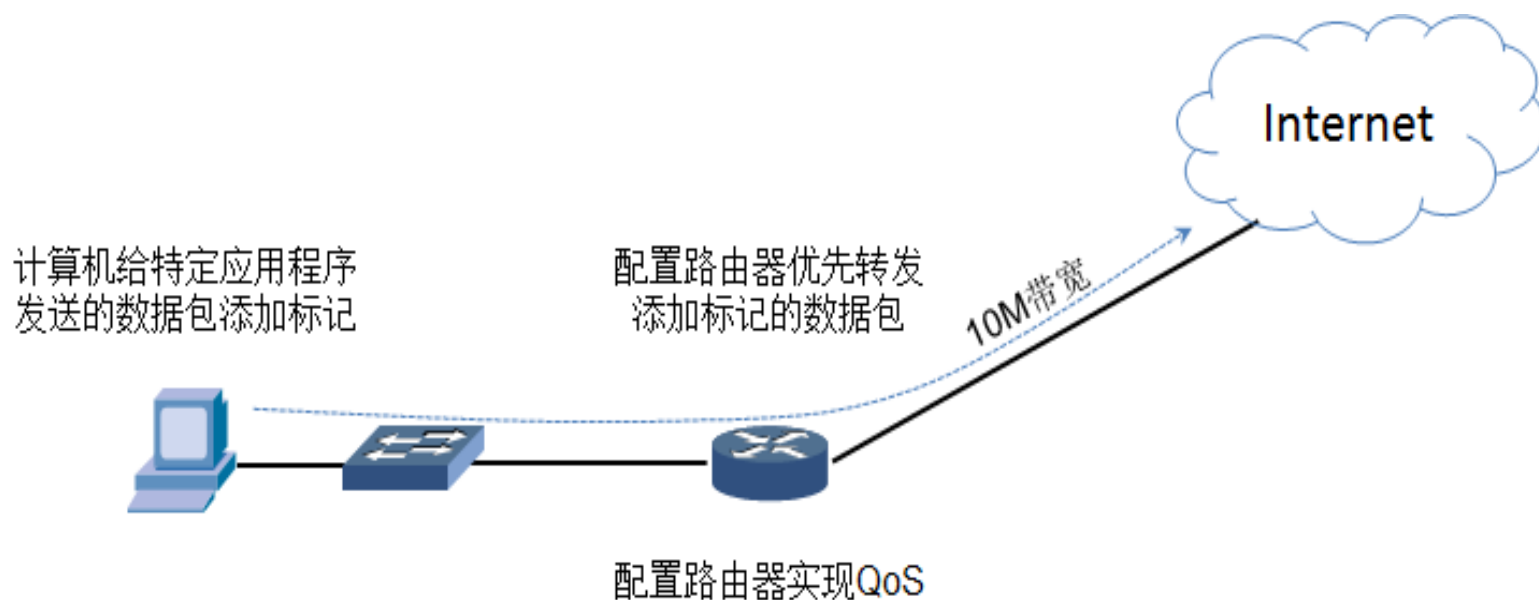
Next header: ICMPv6 (58)

Hex limit: 128

Offset	Hex	ASCII
0000	00 0c 29 ec 1b 90 00 0c 29 66 8b ee 86 dd 60 00	..).)f....
0010	00 00 00 28 3a 80 20 01 20 12 19 75 00 00 00 00	...(:. . .u....
0020	00 00 00 00 06 06 20 01 20 12 19 75 00 00 00 00u....
0030	00 00 00 00 00 08 80 00 1b c6 00 01 00 14 61 62ab
0040	63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72	cdefghij klmnopqr

Version (ipv6.version), 1 字节 | 分组: 713 · 已显示: 713 (100.0%) | 配置文件: Default

7.1.4实战：给数据包设置区分服务字段



7.1.4实战：给数据包设置区分服务字段

Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12))

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
113	4.55201400	120.55.239.108	10.7.10.94	TCP	66	80→58151 [SYN, ACK] Seq=0 Ack=1 w
114	4.55212700	10.7.10.94	120.55.239.108	TCP	54	58151→80 [ACK] Seq=1 Ack=1 win=66
115	4.55651100	10.7.10.94	120.55.239.108	TCP	1498	[TCP segment of a reassembled PDU]
116	4.55651700	10.7.10.94	120.55.239.108	HTTP	381	GET /space?uid=400469 HTTP/1.1
117	4.58544300	203.185.9.210	10.7.10.94	UDP	87	Source port: 8462 Destination po
118	4.58564000	10.7.10.94	203.185.9.210	UDP	85	Source port: 21210 Destination po
119	4.59581100	120.55.239.108	10.7.10.94	TCP	60	80→58151 [ACK] Seq=1 Ack=1445 win
120	4.59581300	120.55.239.108	10.7.10.94	TCP	60	80→58151 [ACK] Seq=1 Ack=1772 win
121	4.64331500	183.61.167.89	10.7.10.94	UDP	75	Source port: 17788 Destination po
122	4.64348600	10.7.10.94	114.113.127.66	UDP	66	Source port: 21210 Destination po
123	4.69052800	fe80::4d71:d92:3508:cff02::1:3		LLMNR	84	Standard query 0x41d7 A wpaad

Frame 116: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0

Ethernet II, Src: AsustekC_2e:6e:1e (c8:60:00:2e:6e:1e), Dst: 50:da:00:ce:11:3c (50:da:00:ce:11:3c)

Internet Protocol Version 4, Src: 10.7.10.94 (10.7.10.94), Dst: 120.55.239.108 (120.55.239.108)

Version: 4
Header Length: 20 bytes

Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

0010 00.. = Differentiated Services Codepoint: Class Selector 1 (0x08)

.... 0000 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)

Total Length: 367
Identification: 0x7707 (30471)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128

0000 50 da 00 ce 11 3c c8 60 00 2e 6e 1e 08 00 45 20 P....<. .n...E
0010 01 6f 77 07 40 00 80 06 00 00 0a 07 0a 5e 78 37 .ow.@... ..^x7
0020 ef 6c e3 27 00 50 29 dd c3 b1 e9 d4 b4 98 50 18 .l.'.P).P.
0030 40 de 7d 6a 00 00 34 34 33 39 30 64 61 37 37 37 @.}j..44 390da777
0040 24 62 26 61 20 22 62 22 24 64 24 20 66 28 65 21 4b6302b2 4d40f8e1

Frame (381 bytes) Reassembled TCP (1771 bytes)

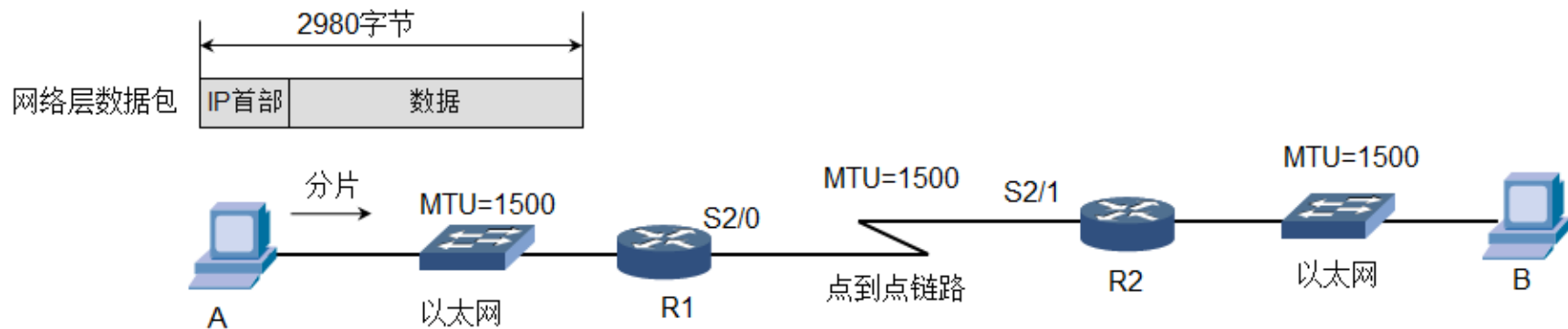
Differentiated Services Codepoint (ip.dsfield...) Packets: 1106 · Displayed: 1106 (100.0%) · Dropped: 0 (0.0%) Profile: Default

7.1.5数据分片详解

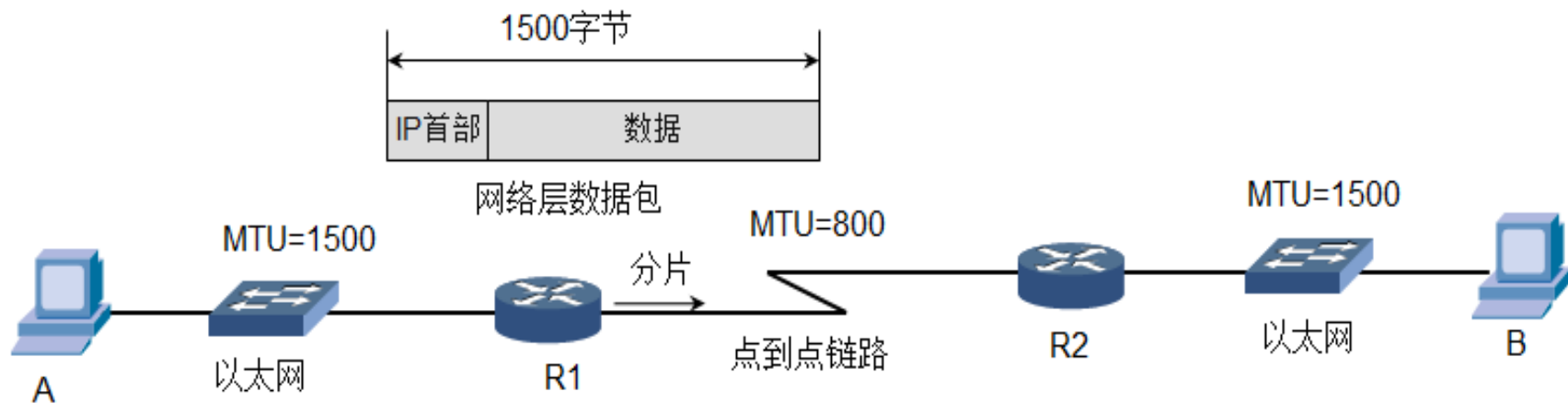
- 在IP层下面的每一种数据链路层都有其特有的帧格式，帧格式也定义了帧中数据字段的最大长度，数据字段最大长度称为最大传送单元MTU（Maximum Transfer Unit）。当一个IP数据包封装成链路层的帧时，此数据包的总长度（即首部加上数据部分）一定不能超过下面的数据链路层的MTU值。例如以太网就规定其MTU值是1500字节。若所传送的数据包长度超过数据链路层的MTU值，就必须把过长的数据包进行分片处理。

7.1.5数据分片详解

■ 在计算机A的数据链路层分片



■ 在R1和R2链路的数据链路层分片



7.1.6实战：捕获并观察数据包分片（1）

■ C:\Users\win7>ping www.cctv.com -l 3500

- 正在 Ping cctv.xdwscache.ourglb0.com [111.11.31.114] 具有 3500 字节的数据:
- 来自 111.11.31.114 的回复: 字节=3500 时间=10ms TTL=128
- 来自 111.11.31.114 的回复: 字节=3500 时间=11ms TTL=128
- 来自 111.11.31.114 的回复: 字节=3500 时间=10ms TTL=128
- 来自 111.11.31.114 的回复: 字节=3500 时间=11ms TTL=128

7.1.6实战：捕获并观察数据包分片（2）

Capturing from 本地连接 [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	192.168.80.21	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
2	3.05608300	192.168.80.21	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
3	3.29770700	192.168.80.100	111.11.31.114	ICMP	74	Echo (ping) request id=
4	3.30505800	111.11.31.114	192.168.80.100	ICMP	74	Echo (ping) reply id=
5	4.30173800	192.168.80.100	111.11.31.114	ICMP	74	Echo (ping) request id=
6	4.31002700	111.11.31.114	192.168.80.100	ICMP	74	Echo (ping) reply id=

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: Vmware_ec:1b:90 (00:0c:29:ec:1b:90), Dst: Vmware_f4:11:93 (00:50:56:f4:11:93)

Internet Protocol Version 4, Src: 192.168.80.100 (192.168.80.100), Dst: 111.11.31.114 (111.11.31.114)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable))

Total Length: 60

Identification: 0x0200 (512)

Flags: 0x00

- 0... .. = Reserved bit: Not set
- .0... .. = Don't fragment: Not set
- ..0. = More fragments: Not set

Fragment offset: 0

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x0000 [validation disabled]

Source: 192.168.80.100 (192.168.80.100)

Destination: 111.11.31.114 (111.11.31.114)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Internet Control Message Protocol

0000 00 50 56 f4 11 93 00 0c 29 ec 1b 90 08 00 45 00 .PV.....).....E.
0010 00 3c 02 00 00 00 80 01 00 00 c0 a8 50 64 6f 0b .<...Pdo.
0020 1f 72 08 00 4d 33 00 01 00 28 61 62 63 64 65 66 .r..M3..(abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Reserved bit (ip.flags.rb), 1 byte

Packets: 49 · Displayed: 49 (100.0%)

Profile: Default

分片标记

32个字节

7.1.6实战：捕获并观察数据包分片（3）

Fragmented 代表后面还有分片

The screenshot shows the Wireshark interface with a packet list table. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The packets are captured on the '本地连接' (Local Connection) interface. The filter is empty. The status bar at the bottom indicates 'Packets: 158 · Displayed: 158 ... Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
19	10.3082800	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
20	10.3083010	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
21	10.3083090	192.168.80.100	111.11.31.114	ICMP	582	Echo (ping) request
22	10.3193380	111.11.31.114	192.168.80.100	IPv4	582	Fragmented IP protocol
23	10.3193440	111.11.31.114	192.168.80.100	IPv4	1514	Fragmented IP protocol
24	10.3193480	111.11.31.114	192.168.80.100	ICMP	1514	Echo (ping) reply
25	11.3370150	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
26	11.3370250	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
27	11.3370350	192.168.80.100	111.11.31.114	ICMP	582	Echo (ping) request
28	11.3474780	111.11.31.114	192.168.80.100	IPv4	582	Fragmented IP protocol
29	11.3474800	111.11.31.114	192.168.80.100	IPv4	1514	Fragmented IP protocol
30	11.3474820	111.11.31.114	192.168.80.100	ICMP	1514	Echo (ping) reply
31	12.3514150	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
32	12.3514310	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
33	12.3514350	192.168.80.100	111.11.31.114	ICMP	582	Echo (ping) request
34	12.3622760	111.11.31.114	192.168.80.100	IPv4	582	Fragmented IP protocol
35	12.3622780	111.11.31.114	192.168.80.100	IPv4	1514	Fragmented IP protocol
36	12.3622800	111.11.31.114	192.168.80.100	ICMP	1514	Echo (ping) reply

第一个分片
第二个分片
分片结束

第一个
ICMP请求
数据包

第二个
ICMP请求
数据包

第三个
ICMP请求
数据包

7.1.6实战：捕获并观察数据包分片（4）

第一个分片 ←

数据包标识517 ←

分片标志为1
后面还有分片 ←

片偏移0字节 ←

The image shows the Wireshark 1.12.4 interface with a packet capture from '本地连接' (Local Connection). The packet list shows four packets. Packet 19 is selected, showing details for an IPv4 packet. The packet is fragmented, with the first fragment (No. 19) having a length of 1514 bytes. The details pane shows the following information:

- Frame 19: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
- Ethernet II, Src: Vmware_ec:1b:90 (00:0c:29:ec:1b:90), Dst: Vmware_f4:11:93 (00:50:56:f4:11:93)
- Internet Protocol Version 4, Src: 192.168.80.100 (192.168.80.100), Dst: 111.11.31.114 (111.11.31.114)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not-ECT))
- Total Length: 1500
- Identification: 0x0205 (517)
- Flags: 0x01 (More Fragments)
 - 0... .. = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ...1. = More fragments: Set
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x0000 [validation disabled]
- Source: 192.168.80.100 (192.168.80.100)
- Destination: 111.11.31.114 (111.11.31.114)

The packet bytes pane shows the raw data of the packet, starting with 0000 00 50 56 f4 11 93 00 0c 29 ec 1b 90 08 00 45 00, which corresponds to the Ethernet II header.

7.1.6实战：捕获并观察数据包分片（5）

第二个分片

数据包标识517

分片标志为1
后面还有分片

片偏移1480字节

The image shows the Wireshark 1.12.4 interface with a packet capture on the '本地连接' (Local Area Connection). The packet list shows four packets. Packet 20 is selected, and its details are expanded in the packet details pane. The details pane shows the following information:

- Frame 20: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
- Ethernet II, Src: Vmware_ec:1b:90 (00:0c:29:ec:1b:90), Dst: Vmware_f4:11:93 (00:50:56:f4:11:93)
- Internet Protocol Version 4, Src: 192.168.80.100 (192.168.80.100), Dst: 111.11.31.114 (111.11.31.114)
 - Version: 4
 - Header Length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not-ECT))
 - Total Length: 1500
 - Identification: 0x0205 (517)
 - Flags: 0x01 (More Fragments)
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..1. = More fragments: Set
 - Fragment offset: 1480
 - Time to live: 128
 - Protocol: ICMP (1)

The packet bytes pane shows the raw data of the packet, starting with the Ethernet II header and the IP header.

No.	Time	Source	Destination	Protocol	Length	Info
19	10.3082800	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
20	10.3083010	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
21	10.3083090	192.168.80.100	111.11.31.114	ICMP	582	Echo (ping) request
22	10.3193380	111.11.31.114	192.168.80.100	IPv4	582	Fragmented IP protocol

7.1.6实战：捕获并观察数据包分片（6）

最后一个分片

数据包标识517

分片标志为0

最后一个分片

片偏移2960字节

The image shows the Wireshark 1.12.4 interface. The packet list on the left shows four packets. Packet 21 is selected and highlighted in blue. It is an ICMP Echo (ping) request from 192.168.80.100 to 111.11.31.114. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and ICMP. The IP header shows a total length of 568, identification of 0x0205 (517), and flags of 0x00. The ICMP header shows a fragment offset of 2960 and a time to live of 128. The packet bytes pane at the bottom shows the raw data of the packet, which is a reassembled IPv4 packet of 3508 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
19	10.3082800	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
20	10.3083010	192.168.80.100	111.11.31.114	IPv4	1514	Fragmented IP protocol
21	10.3083090	192.168.80.100	111.11.31.114	ICMP	582	Echo (ping) request
22	10.3193380	111.11.31.114	192.168.80.100	IPv4	582	Fragmented IP protocol

Frame 21: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface
Ethernet II, Src: Vmware_ec:1b:90 (00:0c:29:ec:1b:90), Dst: Vmware_f4:11:93 (00:50:56:f4:11:93)
Internet Protocol Version 4, Src: 192.168.80.100 (192.168.80.100), Dst: 111.11.31.114
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not-ECT))
Total Length: 568
Identification: 0x0205 (517)
Flags: 0x00
0... .. = Reserved bit: Not set
.0.. .. = Don't fragment: Not set
..0. .. = More fragments: Not set
Fragment offset: 2960
Time to live: 128
Protocol: ICMP (1)

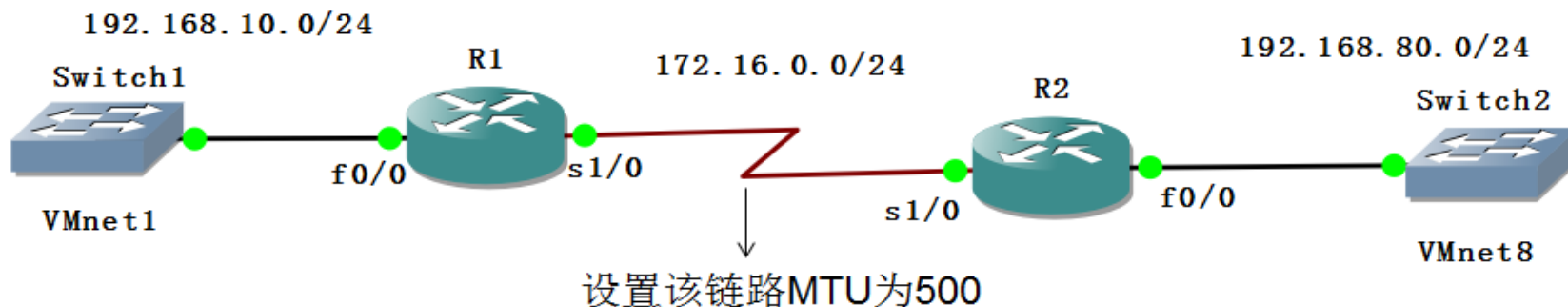
0000 00 50 56 f4 11 93 00 0c 29 ec 1b 90 08 00 45 00 .PV....)....E.
0010 02 38 02 05 01 72 80 01 00 00 c0 a8 50 64 6f 0b .8...r... ..Pdo.
0020 1f 72 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 .rijklnm opgrstuv
0030 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff

Frame (582 bytes) Reassembled IPv4 (3508 bytes)

File: "C:\Users\win7\AppData\Local\Temp..." Packets: 540 · Displayed: 540 ... Profile: Default

7.1.7实战：查看和配置链路MTU（1）

- 可以设置路由器接口的MTU。



- R1#show interfaces serial 1/0
- Serial1/0 is up, line protocol is up
 - Hardware is M4T
 - Internet address is 172.16.0.1/24
 - MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

7.1.7实战：查看和配置链路MTU（2）

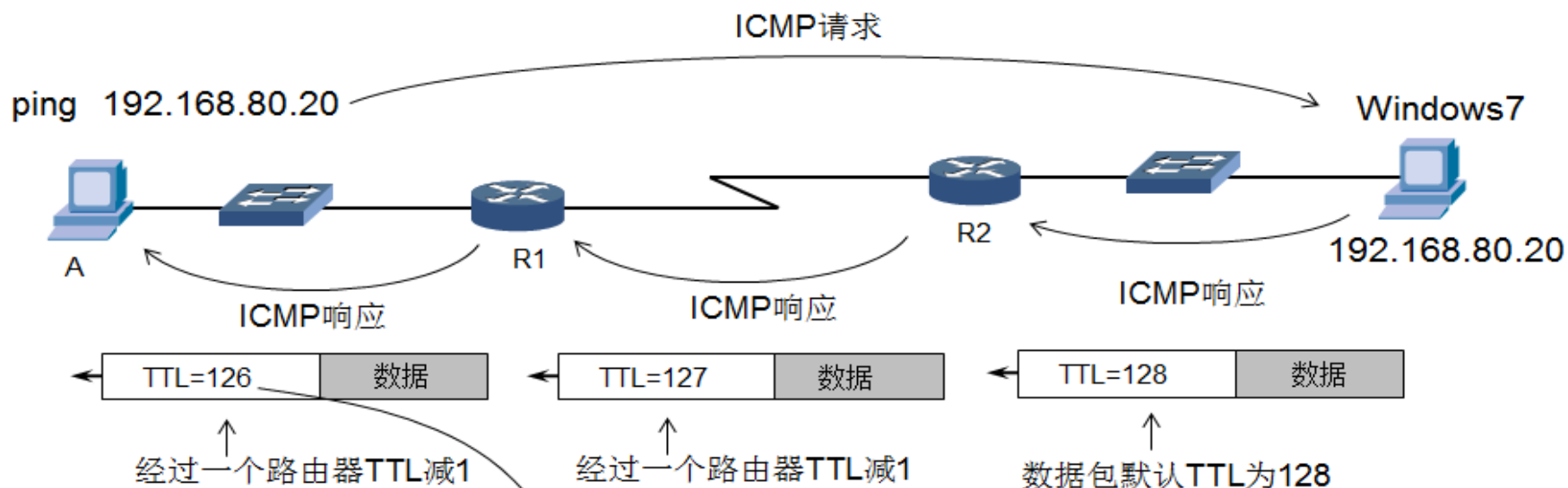
- 设置接口的MTU
- R1(config)#interface serial 1/0
- R1(config-if)#mtu 500

7.1.8数据包生存时间（TTL）详解（1）

- 各种操作系统发送数据包，在网络首部都要给TTL字段赋值，用来限制该数据包能够通过的路由器数量，下面列出一些操作系统发送数据包默认的TTL值。

□ Windows NT 4.0/2000/XP/2003	128
□ MS Windows 95/98/NT 3.51	32
□ Linux	64
□ MacOS/MacTCP 2.0.x	60

7.1.8数据包生存时间 (TTL) 详解 (2)



```
管理员: C:\Windows\system32\cmd.exe
C:\Users\win7B>ping 192.168.80.20

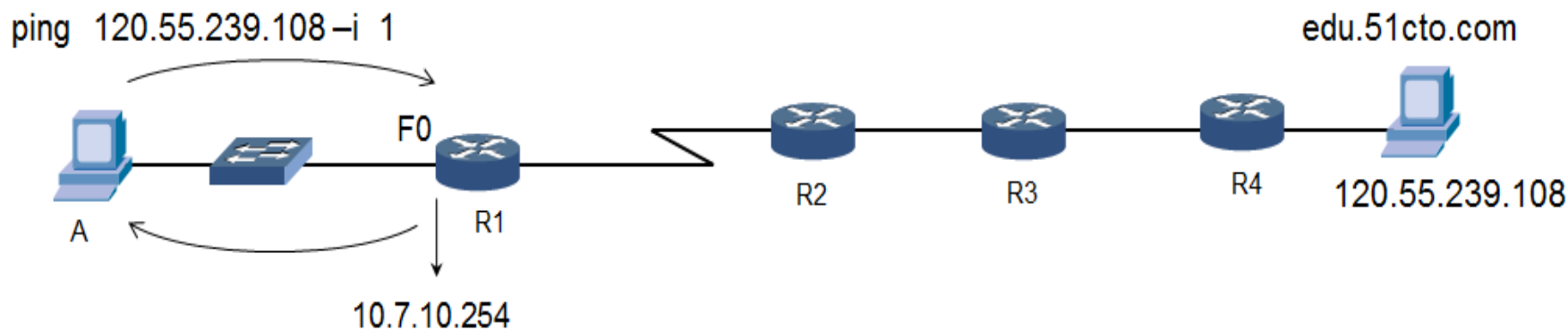
正在 Ping 192.168.80.20 具有 32 字节的数据:
来自 192.168.80.20 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.80.20 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.80.20 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.80.20 的回复: 字节=32 时间<1ms TTL=126

192.168.80.20 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 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\win7B>
```

7.1.9实战：指定ping命令发送数据包的TTL值（1）

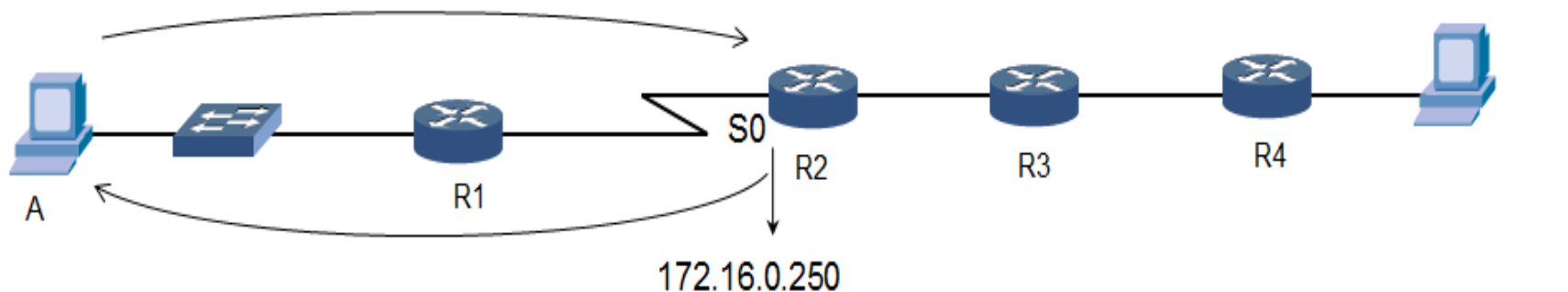
- 虽然操作系统会给发送的数据包指默认的TTL值，但是ping命令允许我们使用参数-i指定发送的ICMP请求数据包的TTL值。
- 一个路由器在转发数据包之前将该数据包的TTL减1，如果减1后TTL变为0，路由器就会丢弃该数据包，然后产生一个ICMP响应数据包给发送者，说明TTL耗尽。通过这种方式，你能够知道到达目标地址经过哪些路由器。



7.1.9实战：指定ping命令发送数据包的TTL值（2）

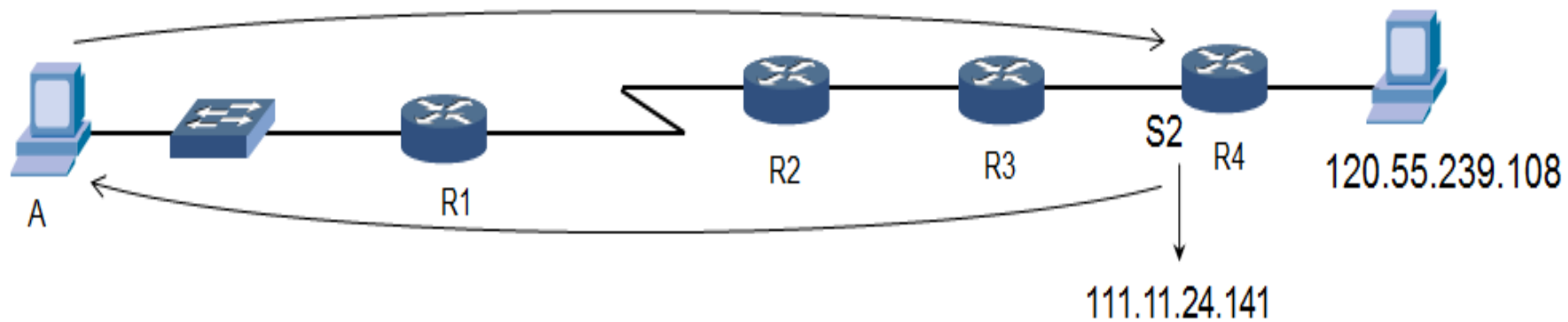
- C:\Users\han>ping edu.51cto.com -i 2
- 正在 Ping yun.dns.51cto.com [120.55.239.108] 具有 32 字节的数据:
- 来自 172.16.0.250 的回复: TTL 传输中过期。
- 来自 172.16.0.250 的回复: TTL 传输中过期。
- 来自 172.16.0.250 的回复: TTL 传输中过期。
- 来自 172.16.0.250 的回复: TTL 传输中过期。

ping 120.55.239.108 -i 2

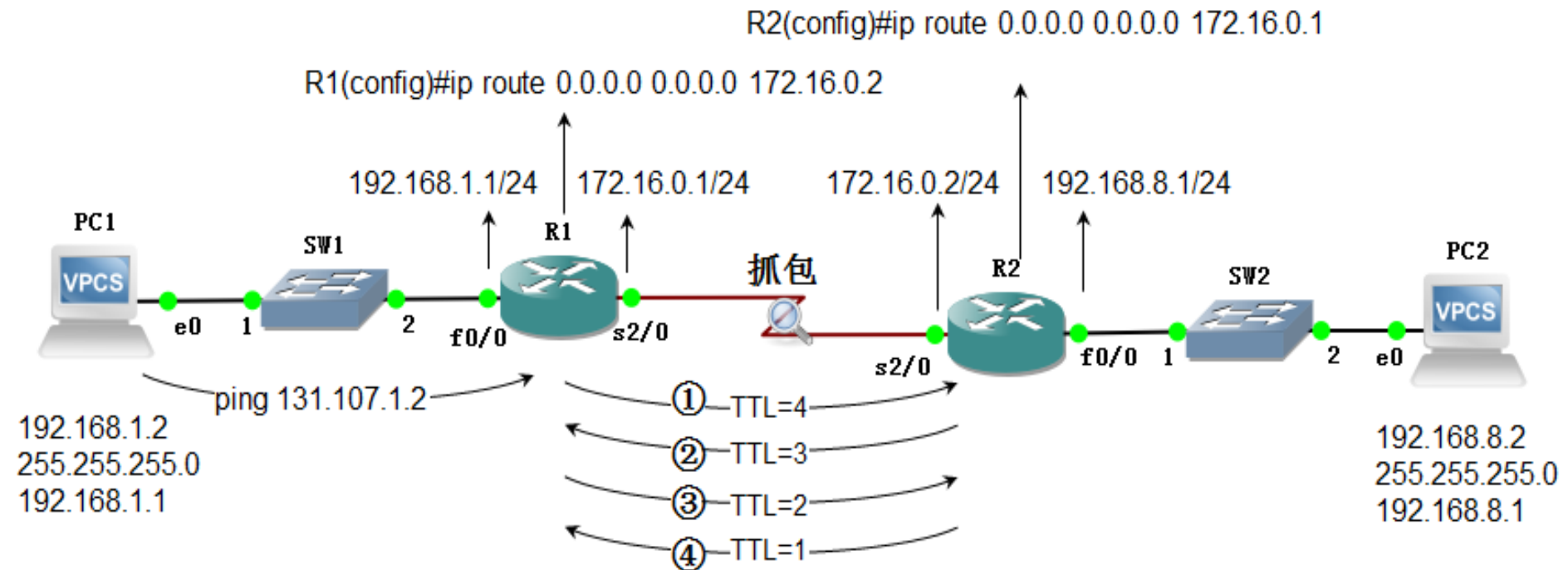


7.1.9实战：指定ping命令发送数据包的TTL值（3）

ping 120.55.239.108 -i 3



7.1.10实战：抓包查看数据包的TTL变化（1）



7.1.10实战：抓包查看数据包的TTL变化（2）

TTL递减

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. A filter bar is present with the text 'Filter:'. The main packet list table shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
249	5.61832100	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=9 (no r
250	5.62532200	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=8 (no r
251	5.62832200	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=7 (no r
252	5.63532200	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=6 (no r
253	5.63832200	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=5 (no r
254	5.67532400	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=4 (no r
255	5.67832500	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=3 (no r
256	5.71532700	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=2 (no r
257	5.71832700	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x45ae, seq=4/1024, ttl=1 (no r
258	5.72532700	172.16.0.2	192.168.1.2	ICMP	60	Time-to-live exceeded (Time to live exceeded in transit
259	6.73838500	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x46ae, seq=5/1280, ttl=63 (no
260	6.74538600	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x46ae, seq=5/1280, ttl=62 (no
261	6.74838600	192.168.1.2	131.107.1.2	ICMP	88	Echo (ping) request id=0x46ae, seq=5/1280, ttl=61 (no

Below the packet list is the packet details pane. It shows the selected packet (No. 257) with the following details:

- Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 131.107.1.2 (131.107.1.2)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 84
- Identification: 0xae43 (44611)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)

At the bottom is the packet bytes pane, showing the raw data in hexadecimal and ASCII.

Annotations on the image:

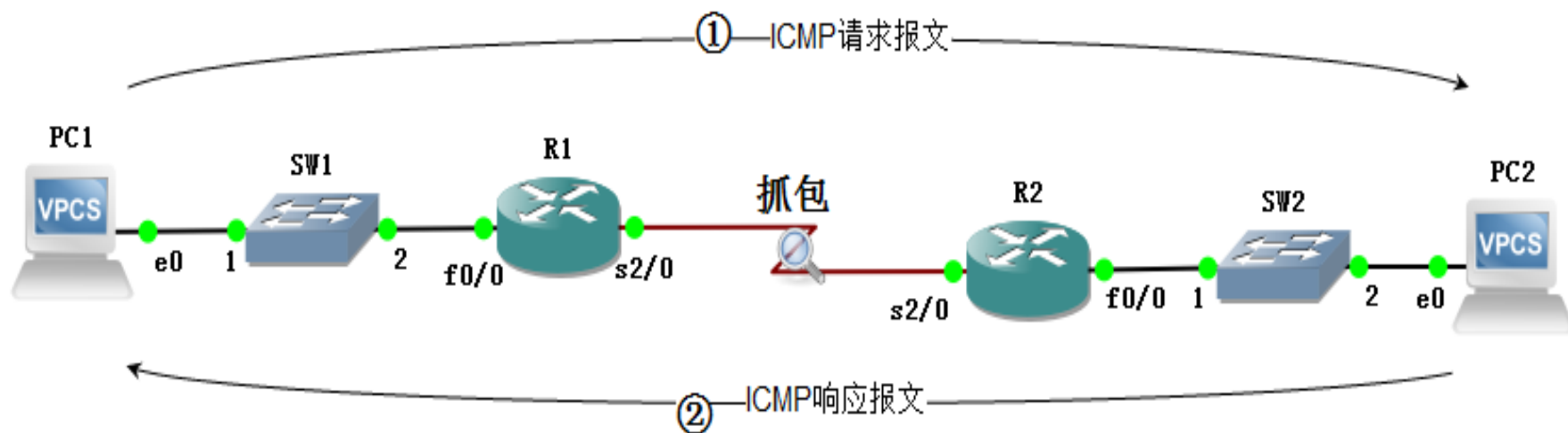
- An arrow points from the text "TTL=1" to the "Time to live: 1" field in the packet details pane.
- An arrow points from the text "报告TTL耗尽" to the packet list entry for No. 258, which shows "Time-to-live exceeded".
- An arrow points from the text "TTL递减" to the "ttl=9" field in the packet list entry for No. 249.

7.2 ICMP协议

- ICMP协议是TCP/IP协议栈中的网络层的一个协议，ICMP是（Internet Control Message Protocol）Internet控制报文协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。
- ICMP报文是在IP数据报内部被传输的，它封装在IP数据报内。ICMP报文通常被IP层或更层协议（TCP或UDP）使用。一些ICMP报文把差错报文返回给用户进程。

7.2.1抓包查看ICMP报文格式

- ICMP报文分为：
 - ICMP请求报文
 - ICMP响应报文
 - ICMP差错报告报文



*Standard input [R1 Serial2/0 to R2 Serial2/0] [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
3	1.74510000	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x524a, seq=1/256
4	1.75810000	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x524a, seq=1/256
5	2.77015800	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x534a, seq=2/512
6	2.78815900	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x534a, seq=2/512
7	3.79621700	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x544a, seq=3/768
8	3.83921900	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x544a, seq=3/768
9	4.85527700	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x554a, seq=4/1024
10	4.87327800	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x554a, seq=4/1024

Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

Cisco HDLC

Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.8.2 (192.168.8.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request) **ICMP请求报文**

Code: 0

Checksum: 0xcdc0 [correct]

Identifier (BE): 21066 (0x524a)

Identifier (LE): 19026 (0x4a52)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Response frame: 4]

Data (56 bytes)

Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f... [Length: 56]

0000 0f 00 08 00 45 00 00 54 4a 52 00 00 3f 01 a7 02E..T JR..?...
0010 c0 a8 01 02 c0 a8 08 02 08 00 cd c0 52 4a 00 01RJ..
0020 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17
0030 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27!"#\$%&'
0040 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-./ 01234567
0050 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-./ 01234567

File: "C:\Users\han\AppData\Local\Temp\... Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (... Profile: Default

ICMP报文类型

ICMP报文代码

校验和

ICMP数据部分

ICMP
报文格式

ICMP响应报文

*Standard input [R1 Serial2/0 to R2 Serial2/0] [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
3	1.74510000	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x524a, seq=1/256, 1
4	1.75810000	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x524a, seq=1/256, 1
5	2.77015800	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x534a, seq=2/512, 1
6	2.78815900	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x534a, seq=2/512, 1
7	3.79621700	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x544a, seq=3/768, 1
8	3.83921900	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x544a, seq=3/768, 1
9	4.85527700	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request id=0x554a, seq=4/1024, 1
10	4.87327800	192.168.8.2	192.168.1.2	ICMP	88	Echo (ping) reply id=0x554a, seq=4/1024, 1

Frame 4: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

Cisco HDLC

Internet Protocol Version 4, Src: 192.168.8.2 (192.168.8.2), Dst: 192.168.1.2 (192.168.1.2)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply) **ICMP响应报文**

Code: 0

Checksum: 0xd5c0 [correct]

Identifier (BE): 21066 (0x524a)

Identifier (LE): 19026 (0x4a52)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Request frame: 3]

[Response time: 13.000 ms]

Data (56 bytes)

Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...

[Length: 56]

0000	0f 00 08 00 45 00 00 54	4a 52 00 00 3f 01 a7 02E..T JR..?...
0010	c0 a8 08 02 c0 a8 01 02	00 00 d5 c0 52 4a 00 01RJ..
0020	08 09 0a 0b 0c 0d 0e 0f	10 11 12 13 14 15 16 17
0030	18 19 1a 1b 1c 1d 1e 1f	20 21 22 23 24 25 26 27 !"#\$%&'
0040	28 29 2a 2b 2c 2d 2e 2f	30 31 32 33 34 35 36 37	()*+,-./ 01234567
0050	38 39 3a 3b 3c 3d 3e 3f		89...~?

File: "C:\Users\han\AppData\Local\Temp\... Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (... Profile: Default

ICMP报文类型和代码

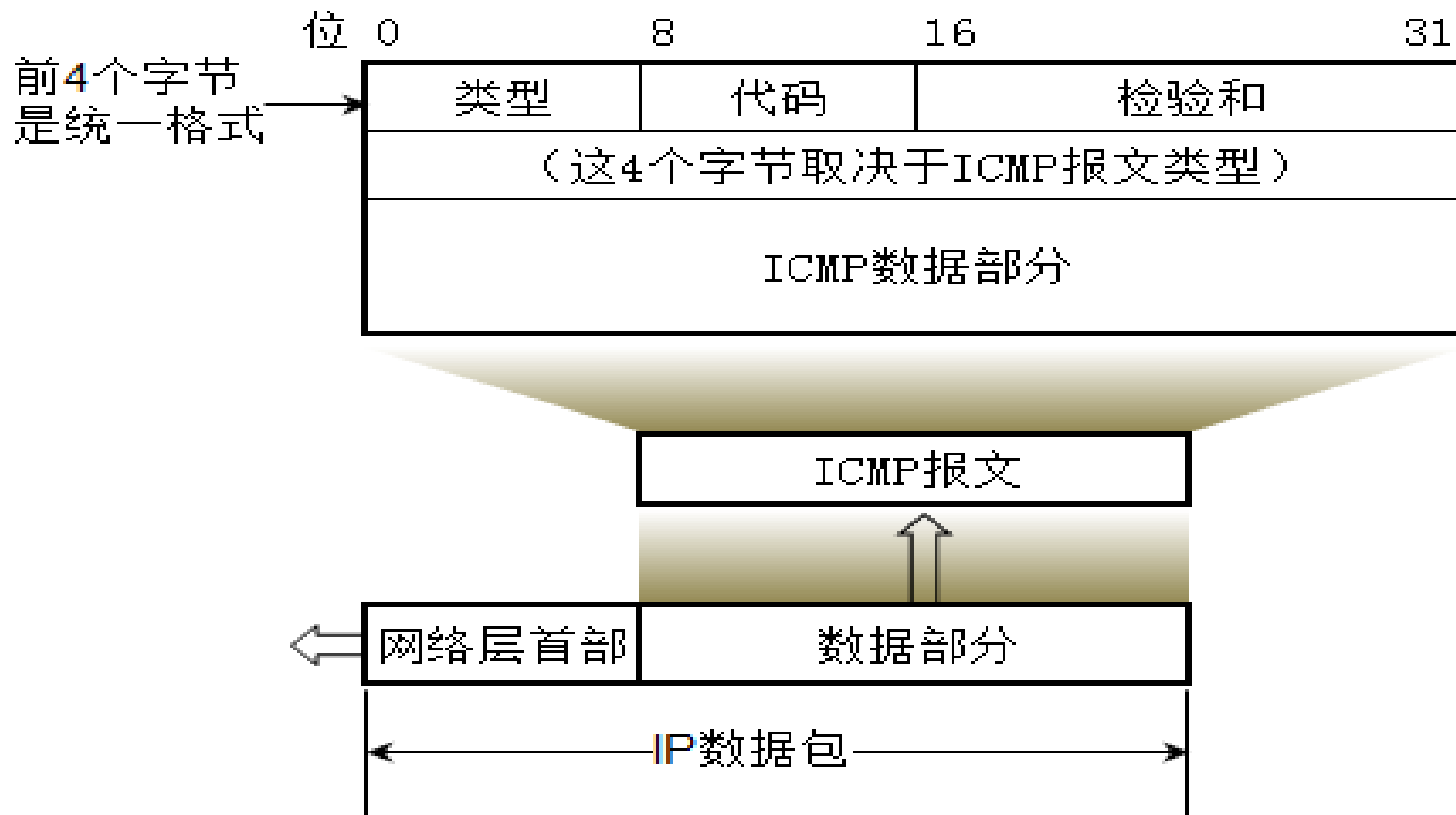
报文种类	类型值	代码	描述
请求报文	8	0	请求回显报文
响应报文	0	0	回显应答报文
差错报告报文	3 (终点不可到达)	0	网络不可达
		1	主机不可达
		2	协议不可达
		3	端口不可达
		4	需要进行分片但设置了不分片
		13	由于路由器过滤，通信被禁止
	4	0	源端被关闭
	5 (改变路由)	0	对网络重定向
		1	对主机重定向
	11	0	传输期间生存时间(TTL)为0
	12 (参数问题)	0	坏的IP首部
		1	缺少必要的选项

ICMP报文类型和代码

- (1) 终点不可到达 当路由器或主机没有到达目标地址的路由时，就丢弃该数据包，给源点发送终点不可到达报文。
- (2) 源点抑制 当路由器或主机由于拥塞而丢弃数据包时，就会向源点发送源点抑制报文，使源点知道应当降低数据包的发送速率。
- (3) 时间超时 当路由器收到生存时间为零的数据报时，除丢弃该数据报外，还要向源点发送时间超过报文。当终点在预先规定的时间内不能收到一个数据报的全部数据报片时，就把已收到的数据报片都丢弃，并向源点发送时间超过报文。
- (4) 参数问题 当路由器或目的主机收到的数据报的首部中有的字段的值不正确时，就丢弃该数据报，并向源点发送参数问题报文。
- (5) 改变路由（重定向） 路由器把改变路由报文发送给主机，让主机知道下次应将数据报发送给另外的路由器（可通过更好的路由）。

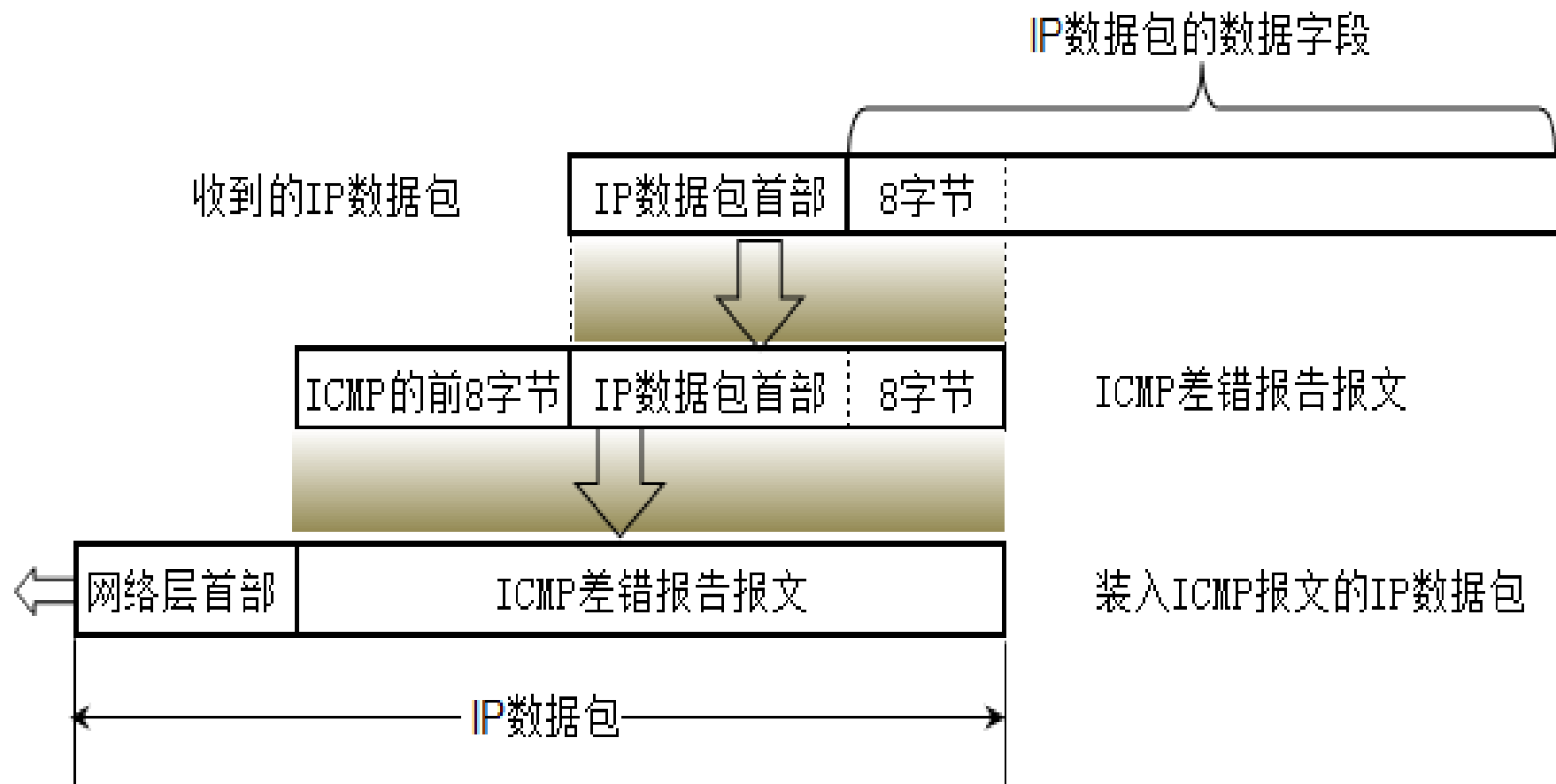
7.2.2 ICMP报文格式 (1)

- ICMP报文的前4个字节是统一的格式，共有三个字段：即类型、代码和检验和。接着4个字节的内容与ICMP的类型有关。

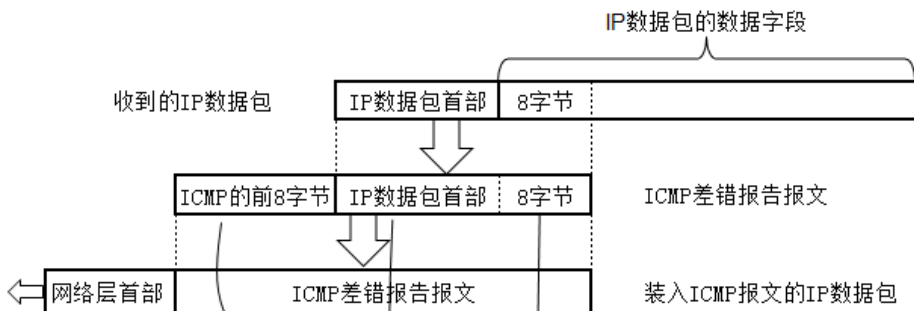


7.2.2 ICMP报文格式 (2)

■ ICMP差错报告报文的数据字段的内容



7.2.3 ICMP差错报告报文-TTL过期



Capturing from Standard input [R1 Serial2/0 to R2 Serial2/0] [Wireshark 1.12.4 ...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear

No.	Time	Source	Destination	Protocol	Length	Info
6	12.1840970	172.16.0.2	192.168.1.2	ICMP	60	Time-to-live exceeded
7	13.1987550	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request
8	13.2087560	172.16.0.2	192.168.1.2	ICMP	60	Time-to-live exceeded
9	14.2188130	192.168.1.2	192.168.8.2	ICMP	88	Echo (ping) request
10	14.2278140	172.16.0.2	192.168.1.2	ICMP	60	Time-to-live exceeded

Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface

Cisco HDLC

Internet Protocol Version 4, Src: 172.16.0.2 (172.16.0.2), Dst: 192.168.1.2 (192.168.1.2)

Internet Control Message Protocol

- Type: 11 (Time-to-live exceeded)
- Code: 0 (Time to live exceeded in transit)
- Checksum: 0xccf3 [correct]

Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.8.2 (192.168.8.2)

- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Total Length: 84)
- Identification: 0xf951 (63825)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x3603 [validation disabled]
- Source: 192.168.1.2 (192.168.1.2)
- Destination: 192.168.8.2 (192.168.8.2)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xce10
- Identifier (BE): 20985 (0x51f9)
- Identifier (LE): 63825 (0xf951)
- Sequence number (BE): 2 (0x0002)
- Sequence number (LE): 512 (0x0200)

0000 0f 00 08 00 45 c0 00 38 00 06 00 00 ff 01 4d 42E..8.....MB

0010 ac 10 00 02 c0 a8 01 02 0b 00 cc f3 00 00 00 006.....

0020 45 00 00 54 f9 51 00 00 01 01 36 03 c0 a8 01 02 E..T.Q...6...

0030 c0 a8 08 02 08 00 ce 10 51 f9 00 02Q...

Internet Control Message Protocol (icmp)... Packets: 3013 Profile: Default

7.2.4 ICMP差错报告报文-目标主机不可到达

The image shows a Wireshark packet capture of an ICMP Destination Unreachable (Host Unreachable) message. The packet list shows a series of ping requests and responses. The selected packet (Frame 5) is an ICMP Destination Unreachable (Host Unreachable) message. The packet details pane shows the following information:

- Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 1 (Host unreachable)
 - Checksum: 0xd4f2 [correct]
- Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 131.107.1.2 (131.107.1.2)
 - Version: 4
 - Header Length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable))
 - Total Length: 84
 - Identification: 0x3422 (13346)
 - Flags: 0x00
 - Fragment offset: 0

The packet bytes pane shows the raw data of the packet, with the ICMP header and data highlighted in blue.

0000 00 50 79 66 68 00 cc 01 1f 54 00 00 08 00 45 00 .Pyfh... .T....E.
0010 00 38 00 03 00 00 ff 01 38 6e c0 a8 01 01 c0 a8 .8..... 8n.....
0020 01 02 03 01 d4 f2 00 00 00 00 45 00 00 54 34 22 ..E...T4"
0030 00 00 3f 01 01 70 c0 a8 01 02 83 6b 01 02 08 00 ..?...p...k...
0040 fd d6 22 34 00 01 .."4..

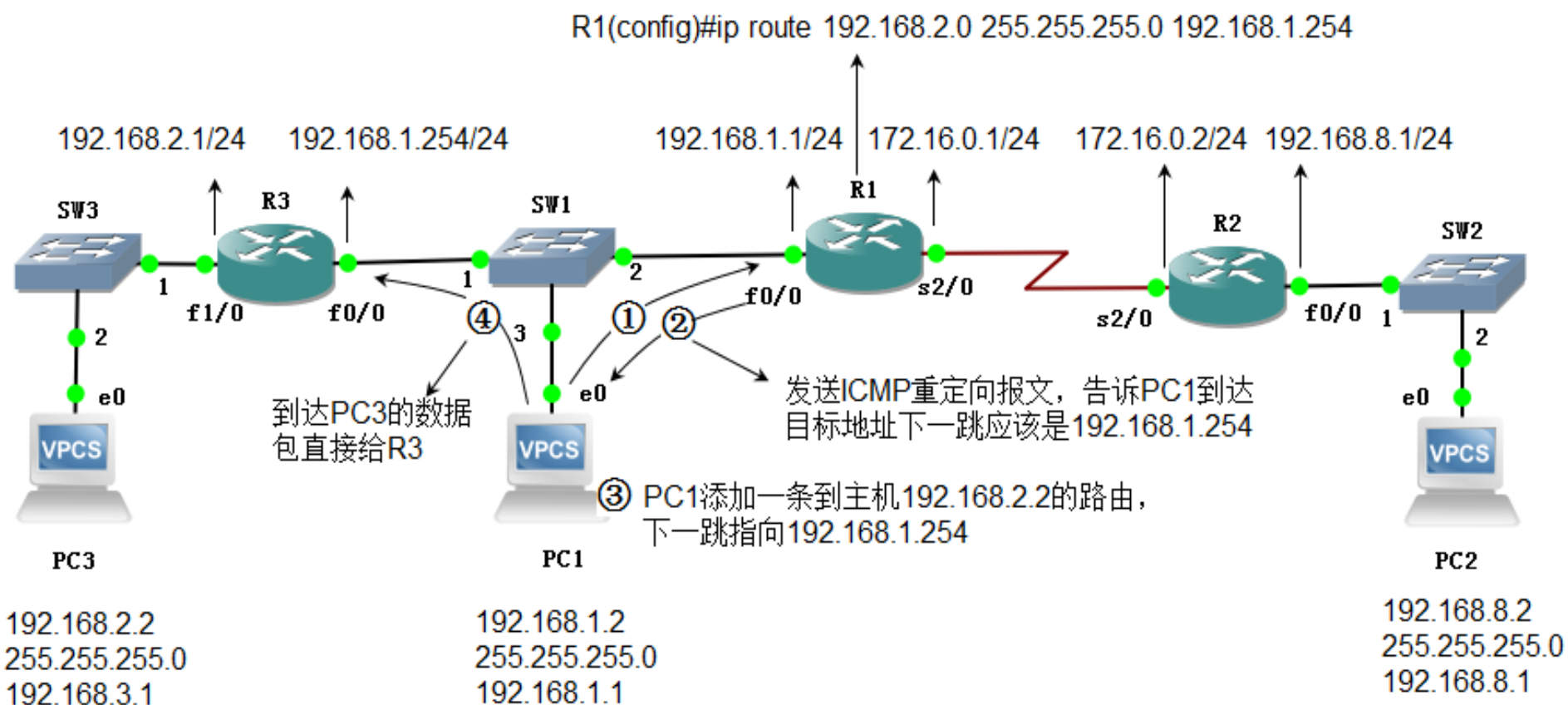
类型

代码

注意观察源地址和目标地址

收到的ICMP请求数据报首部

7.2.5 ICMP差错报告报文-路由重定向 (1)



7.2.5 ICMP差错报告报文-路由重定向 (2)

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 4 is an ICMP Redirect message from 192.168.1.1 to 192.168.1.2. The middle pane shows the detailed view of this packet, highlighting the 'Gateway address: 192.168.1.254' field. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.01400100	cc:01:1f:54:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at cc:01:1f:54:00:00
3	0.01500100	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x103c, seq=1
4	0.04600200	192.168.1.1	192.168.1.2	ICMP	70	Redirect (Redirect for network)
5	0.05600300	cc:01:1f:54:00:00	Broadcast	ARP	60	who has 192.168.1.254? Tell 192.168.1.254
6	0.14800800	Private_66:68:00	Broadcast	ARP	64	who has 192.168.1.254? Tell 192.168.1.254
7	0.15500900	cc:03:3a:c4:00:00	Private_66:68:00	ARP	60	192.168.1.254 is at cc:03:3a:c4:00:00
8	0.15600900	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x103c, seq=1
9	2.15612300	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x123c, seq=2
10	2.20012600	192.168.1.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x123c, seq=2

Packet 4 Details:

- Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
- Ethernet II, Src: cc:01:1f:54:00:00 (cc:01:1f:54:00:00), Dst: Private_66:68:00 (00:50:79:66:68:00)
- Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
- Internet Control Message Protocol
 - Type: 5 (Redirect)
 - Code: 0 (Redirect for network)
 - Checksum: 0x104d [correct]
 - Gateway address: 192.168.1.254 (192.168.1.254)
- Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.2.2 (192.168.2.2)
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x0fcf
 - Identifier (BE): 4156 (0x103c)
 - Identifier (LE): 15376 (0x3c10)
 - Sequence number (BE): 1 (0x0001)

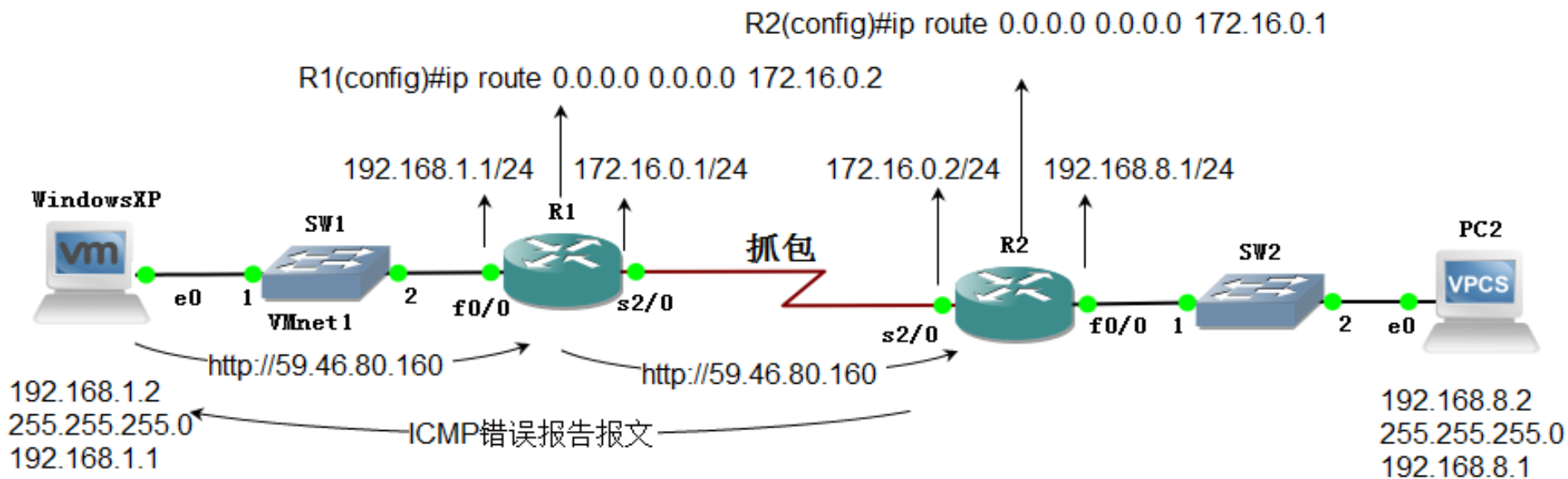
Raw Data:

Offset	Hex	ASCII
0000	00 50 79 66 68 00 cc 01 1f 54 00 00 08 00 45 00	.Pyfh... .T....E.
0010	00 38 00 08 00 00 ff 01 38 69 c0 a8 01 01 c0 a8	.8.....8i.....
0020	01 02 05 00 10 4d c0 a8 01 fe 45 00 00 54 3c 10M...E..T<.
0030	00 00 3f 01 bb 44 c0 a8 01 02 c0 a8 02 02 08 00	...?..D.....
0040	0f cf 10 3c 00 01	...<..

Gateway address (icmp.redir_gw), 4 bytes Packets: 17 · Displayed: 17 (100.0%) · ... Profile: Default

类型
代码
网关

7.2.6 ICMP差错报告报文-给程序返回错误消息



*Standard input [R1 FastEthernet0/0 to SW1 nio_gen_eth:VMware Network Adapter VMnet1] ...

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	cc:01:1f:54:00:00	cc:01:1f:54:00:00	LOOP	60	Reply
2	7.81584200	192.168.1.2	59.46.80.160	TCP	62	1058→80 [SYN] Seq=0 win=65535
3	9.85944500	172.16.0.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to
4	9.98424600	cc:01:1f:54:00:00	cc:01:1f:54:00:00	LOOP	60	Reply
5	10.7954470	192.168.1.2	59.46.80.160	TCP	62	[TCP Retransmission] 1058→80 [
6	13.1042510	172.16.0.2	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to

Frame 3: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

Ethernet II, Src: cc:01:1f:54:00:00 (cc:01:1f:54:00:00), Dst: vmware_cc:87:22 (00:0c:29:cc:87:22)

Internet Protocol Version 4, Src: 172.16.0.2 (172.16.0.2), Dst: 192.168.1.2 (192.168.1.2)

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Checksum: 0x2d0f [correct]

Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 59.46.80.160 (59.46.80.160)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (0x00: Not-ECT, 0x01: ECT(1)))

Total Length: 48

Identification: 0x039d (925)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 1

Protocol: TCP (6)

Header checksum: 0x28b3 [validation disabled]

Source: 192.168.1.2 (192.168.1.2)

Destination: 59.46.80.160 (59.46.80.160)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 1058 (1058), Dst Port: 80 (80)

Source Port: 1058 (1058)

Destination Port: 80 (80)

Sequence number: 1627742841

0000 00 0c 29 cc 87 22 cc 01 1f 54 00 00 08 00 45 c0 ..)..."..T....E.

0010 00 38 00 10 00 00 fe 01 4e 38 ac 10 00 02 c0 a8 .8.....N8.....

0020 01 02 0b 00 2d 0f 00 00 00 00 45 00 00 30 03 9d-...E...0..

0030 40 00 01 06 28 b3 c0 a8 01 02 3b 2e 50 a0 04 22 @...(. ...:..P..

0040 00 50 61 05 62 79 .Pa.by

Destination (ip.dst), 4 bytes

Packets: 10 · Displayed: 10 (1...)

Profile: Default

TCP协议

访问网站的
数据包

ICMP差错
报告报文

第2个数
据包首部

传输层首部
前8个字节

TCP协议
源端口
目标端口

7.3使用ICMP排除网络故障案例

- 7.3.1 使用ping命令诊断网络故障
- 7.3.2使用ping断定哪一段链路出现故障
- 7.3.3使用tracert跟踪数据包路径
- 7.3.4使用pathping跟踪数据包路径

7.3.1 使用ping命令诊断网络故障

Windows XP desktop environment showing network diagnostic tools.

Ethereal (Wireshark) Packet Capture:

Filter: Expression... Clear

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	BOOTP	BOOT R
2	0.000029	0.0.0.0	255.255.255.255	BOOTP	BOOT R
3	0.000058	0.0.0.0	255.255.255.255	BOOTP	BOOT R
4	0.000086	0.0.0.0	255.255.255.255	BOOTP	BOOT R

... Multicast: This is a UNICAST fra
... Locally Administrated Address: T
Type: IP (0x0800)

Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 328
Identification: 0x0208 (520)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: UDP (0x11)
Header checksum: 0xb89d [correct]
Source: 0.0.0.0 (0.0.0.0)
Destination: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Source port: bootpc (68)
Destination port: bootps (67)

0000 ff ff ff ff ff ff 00 01 63 bf e0 40 08 00 45 00 C..@
0010 01 48 02 08 00 00 ff 11 b8 9d 00 00 00 00 ff ff .H.....
0020 ff ff 00 44 00 43 01 34 00 00 01 01 06 00 00 00 ...D.C.4.....
0030 00 00 16 b9 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 01 63 bf e0 40 00 00 00 00 C..@....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 63 82 53 63 0c 0b 57 53 2d 43 C..S...WS-C

File: "F:\MCSE PPT\网络安全\guangbo\关闭生成树广播包" 27 MB 00:00:02

Windows Command Prompt:

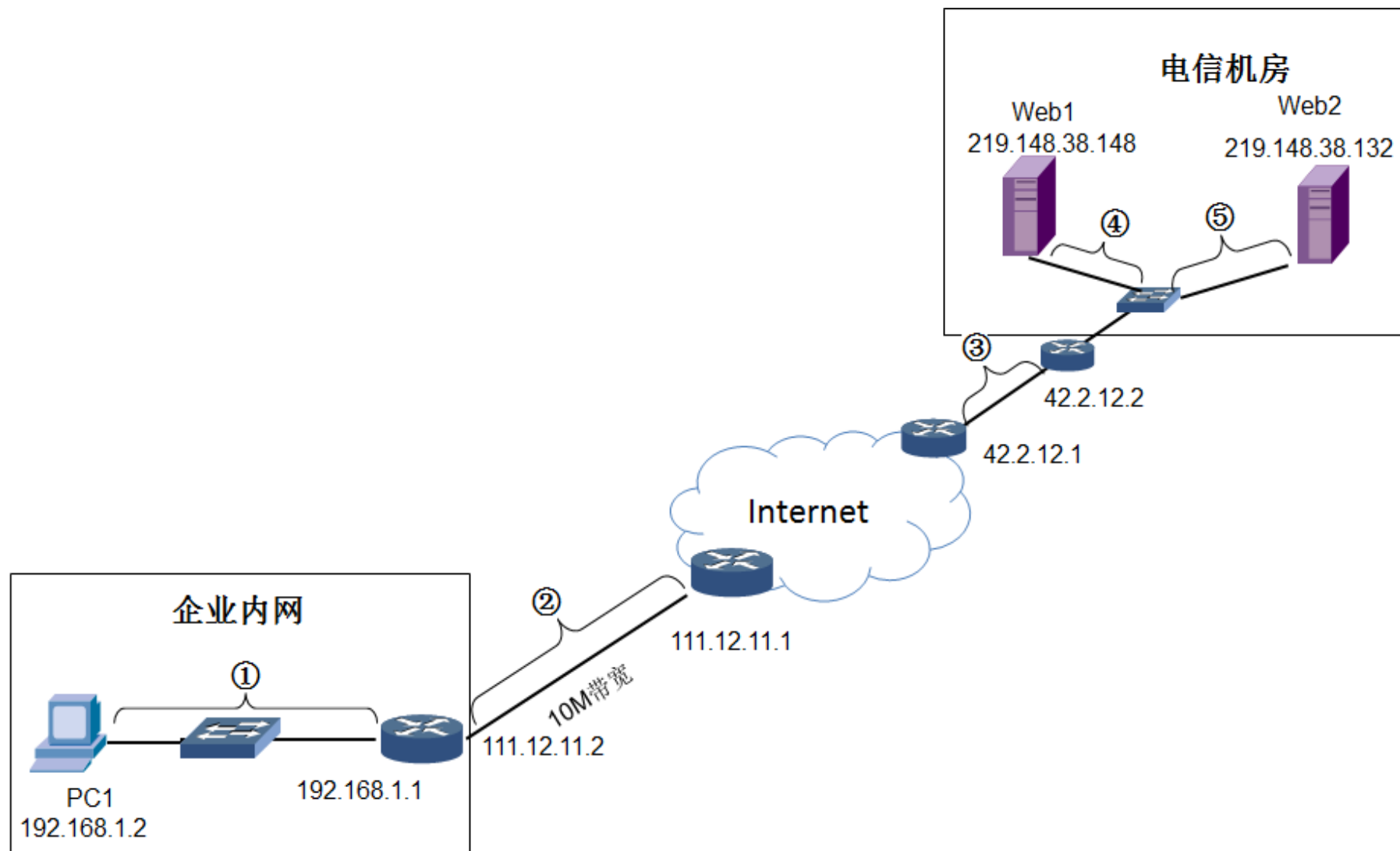
C:\WINDOWS\system32\cmd.exe - ping 192.168.1.222 -t

```
Reply from 192.168.1.222: bytes=32 time=1936ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.222: bytes=32 time=1953ms TTL=255
Request timed out.
Request timed out.
Reply from 192.168.1.222: bytes=32 time=1933ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.222: bytes=32 time=1938ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.222: bytes=32 time=1943ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.222: bytes=32 time=1950ms TTL=255
Request timed out.
```

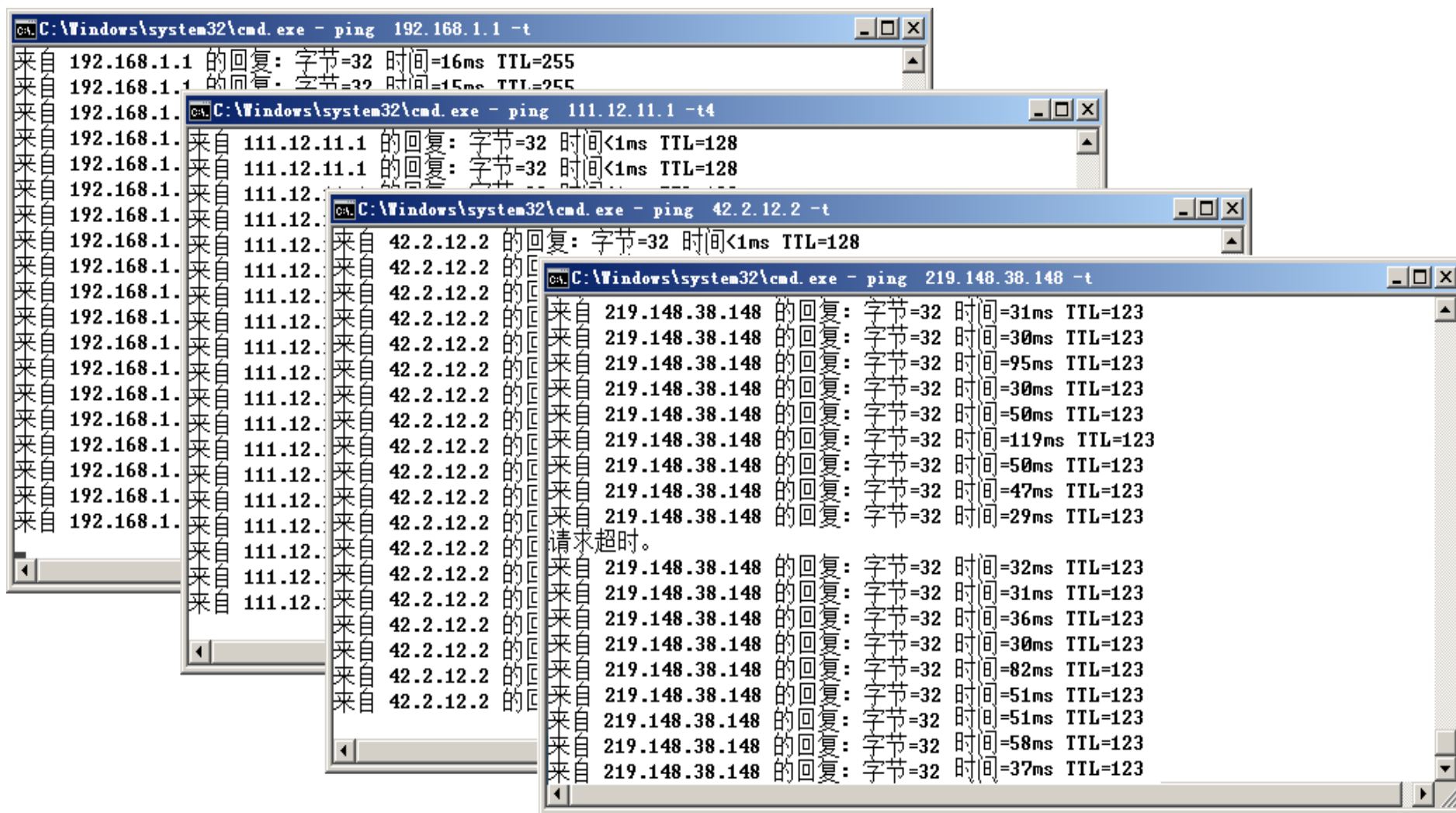
搜狗拼音 半:

P: 82118 D: 82118 M: 0

7.3.2使用ping断定哪一段链路出现故障



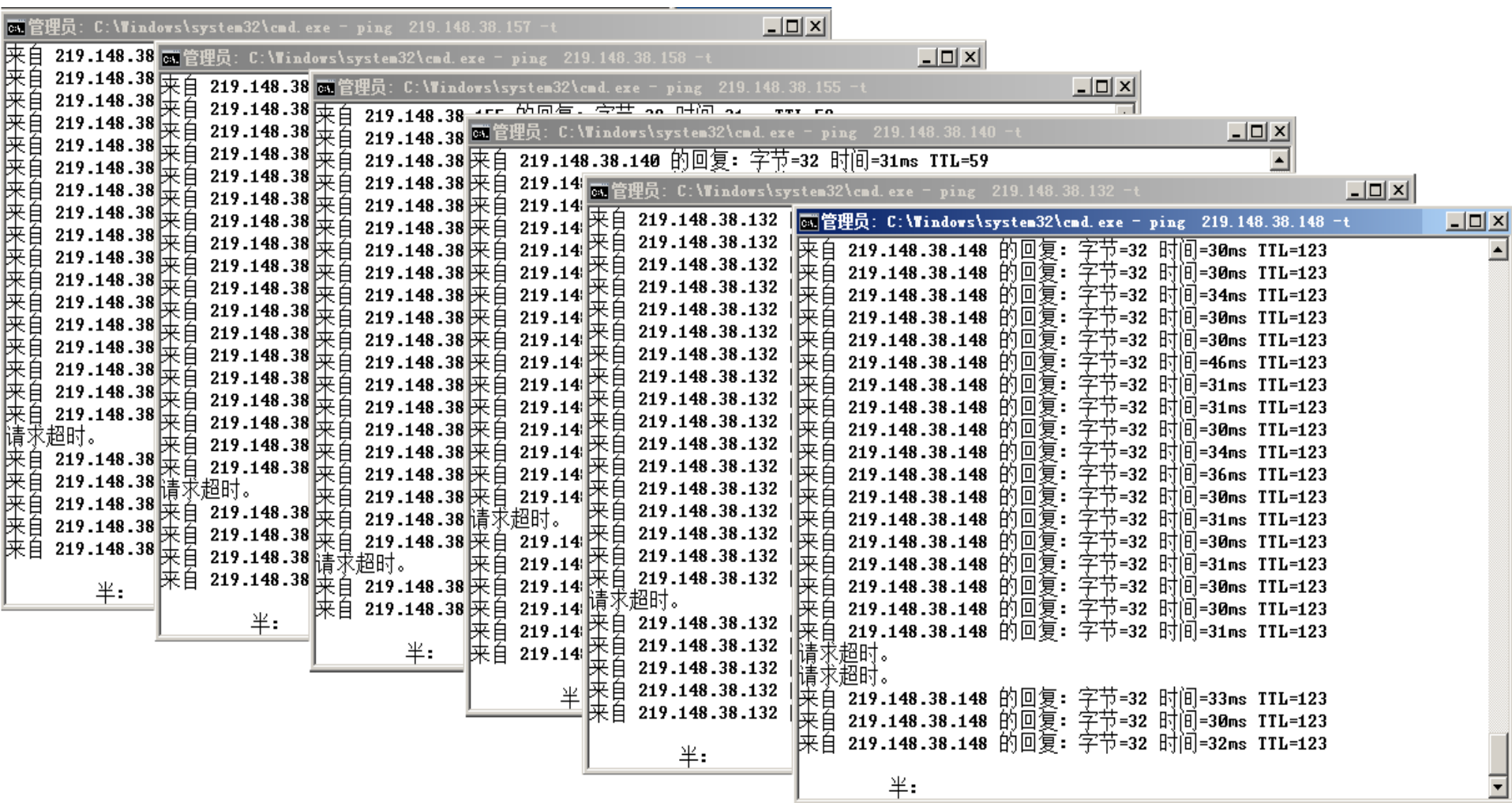
测试哪一段链路丢包



The image displays four overlapping Windows command prompt windows, each showing the results of a continuous ping test to a specific IP address. The windows are titled as follows:

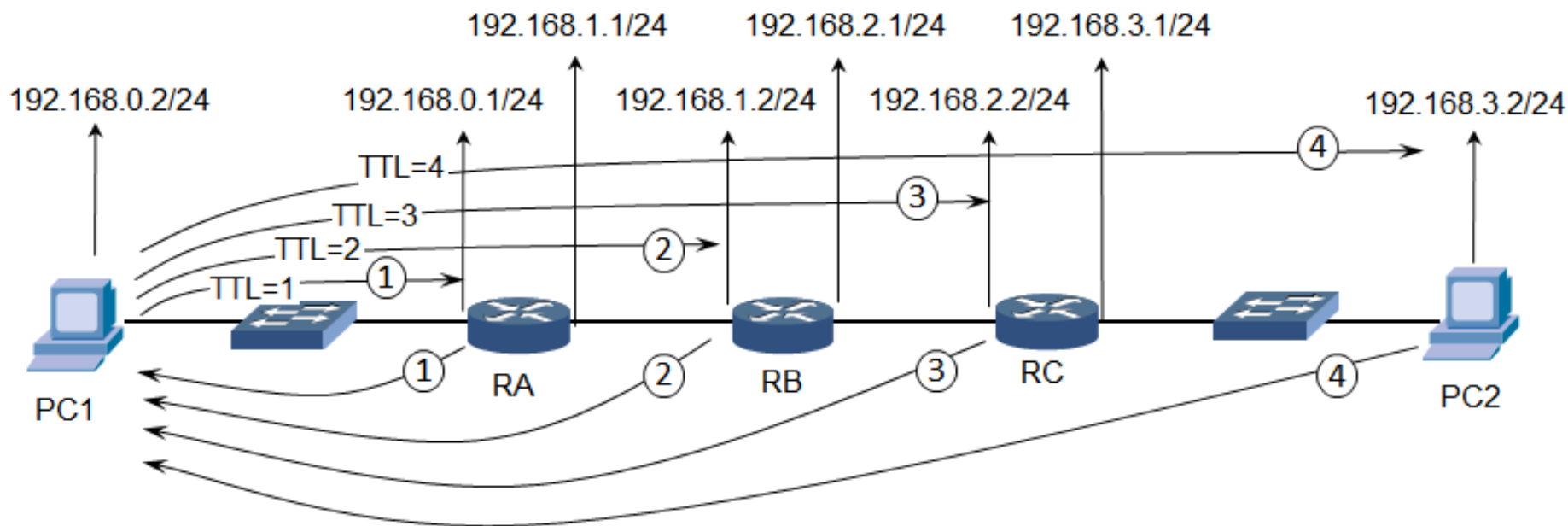
- Window 1 (Top Left):** `C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t`
Output:
192.168.1.1 的回复: 字节=32 时间=16ms TTL=255
192.168.1.1 的回复: 字节=32 时间=15ms TTL=255
- Window 2 (Second from Top Left):** `C:\Windows\system32\cmd.exe - ping 111.12.11.1 -t`
Output:
111.12.11.1 的回复: 字节=32 时间<1ms TTL=128
111.12.11.1 的回复: 字节=32 时间<1ms TTL=128
- Window 3 (Third from Top Left):** `C:\Windows\system32\cmd.exe - ping 42.2.12.2 -t`
Output:
42.2.12.2 的回复: 字节=32 时间<1ms TTL=128
- Window 4 (Bottom Right):** `C:\Windows\system32\cmd.exe - ping 219.148.38.148 -t`
Output:
219.148.38.148 的回复: 字节=32 时间=31ms TTL=123
219.148.38.148 的回复: 字节=32 时间=30ms TTL=123
219.148.38.148 的回复: 字节=32 时间=95ms TTL=123
219.148.38.148 的回复: 字节=32 时间=30ms TTL=123
219.148.38.148 的回复: 字节=32 时间=50ms TTL=123
219.148.38.148 的回复: 字节=32 时间=119ms TTL=123
219.148.38.148 的回复: 字节=32 时间=50ms TTL=123
219.148.38.148 的回复: 字节=32 时间=47ms TTL=123
219.148.38.148 的回复: 字节=32 时间=29ms TTL=123
请求超时。
219.148.38.148 的回复: 字节=32 时间=32ms TTL=123
219.148.38.148 的回复: 字节=32 时间=31ms TTL=123
219.148.38.148 的回复: 字节=32 时间=36ms TTL=123
219.148.38.148 的回复: 字节=32 时间=30ms TTL=123
219.148.38.148 的回复: 字节=32 时间=82ms TTL=123
219.148.38.148 的回复: 字节=32 时间=51ms TTL=123
219.148.38.148 的回复: 字节=32 时间=51ms TTL=123
219.148.38.148 的回复: 字节=32 时间=58ms TTL=123
219.148.38.148 的回复: 字节=32 时间=37ms TTL=123

断定是整个机房堵塞还是服务器网络堵塞



7.3.3使用tracert跟踪数据包路径

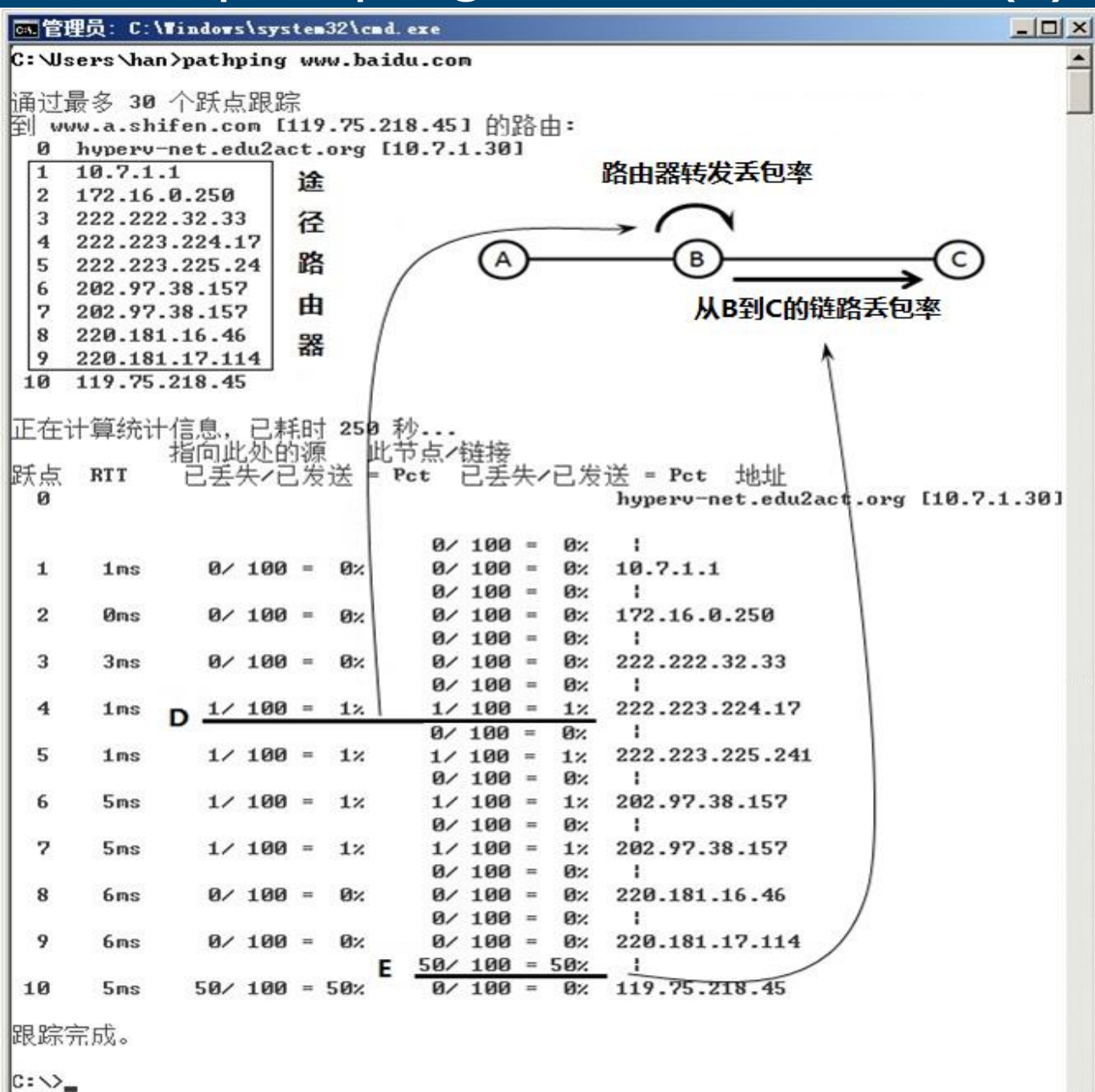
- Ping命令并不能跟踪从源地址到目标地址沿途经过了哪些路由器，Windows操作系统中的tracert命令是路由跟踪实用程序，用于确定IP数据报访问目标地址路径，能够帮助我们发现到达目标网络到底是哪一条链路出现了故障。Tracert 命令就是ping命令的扩展，用IP报文生存时间（TTL）字段和ICMP差错报告报文来确定沿途经过的路由器。
- Tracert工作原理如下图所示。



7.3.4使用pathping跟踪数据包路径(1)

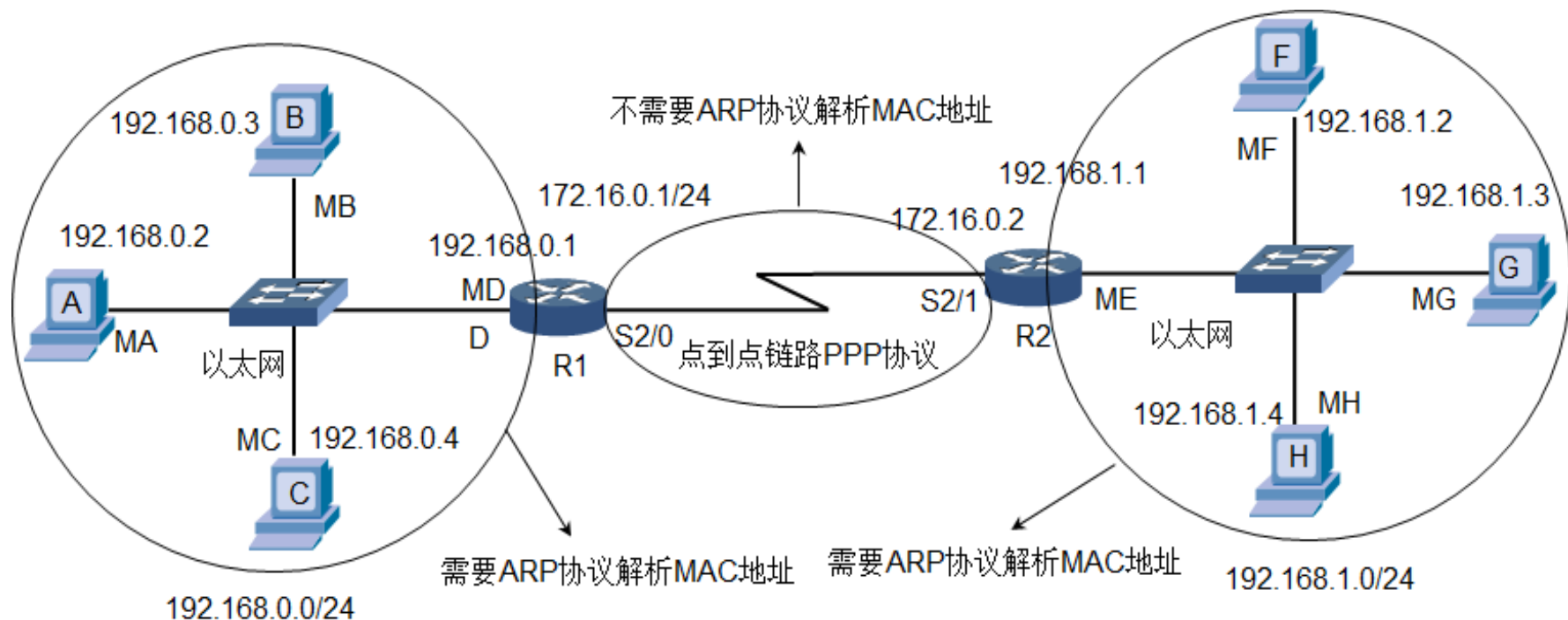
- Pathping是一个基于TCP/IP的命令行工具，该命令不但可以跟踪数据包从源主机到目标主机所经过的路径，还可以统计计算机网络延时以及丢包率，帮助我们解决网络问题，跟踪数据包路径的原理和tracert命令一样。

7.3.4使用pathping跟踪数据包路径(2)



7.4 ARP协议

- ARP协议的作用，将以太网中的计算机的IP地址解析成MAC地址。
- 点到点链路使用PPP协议，不需要ARP协议。

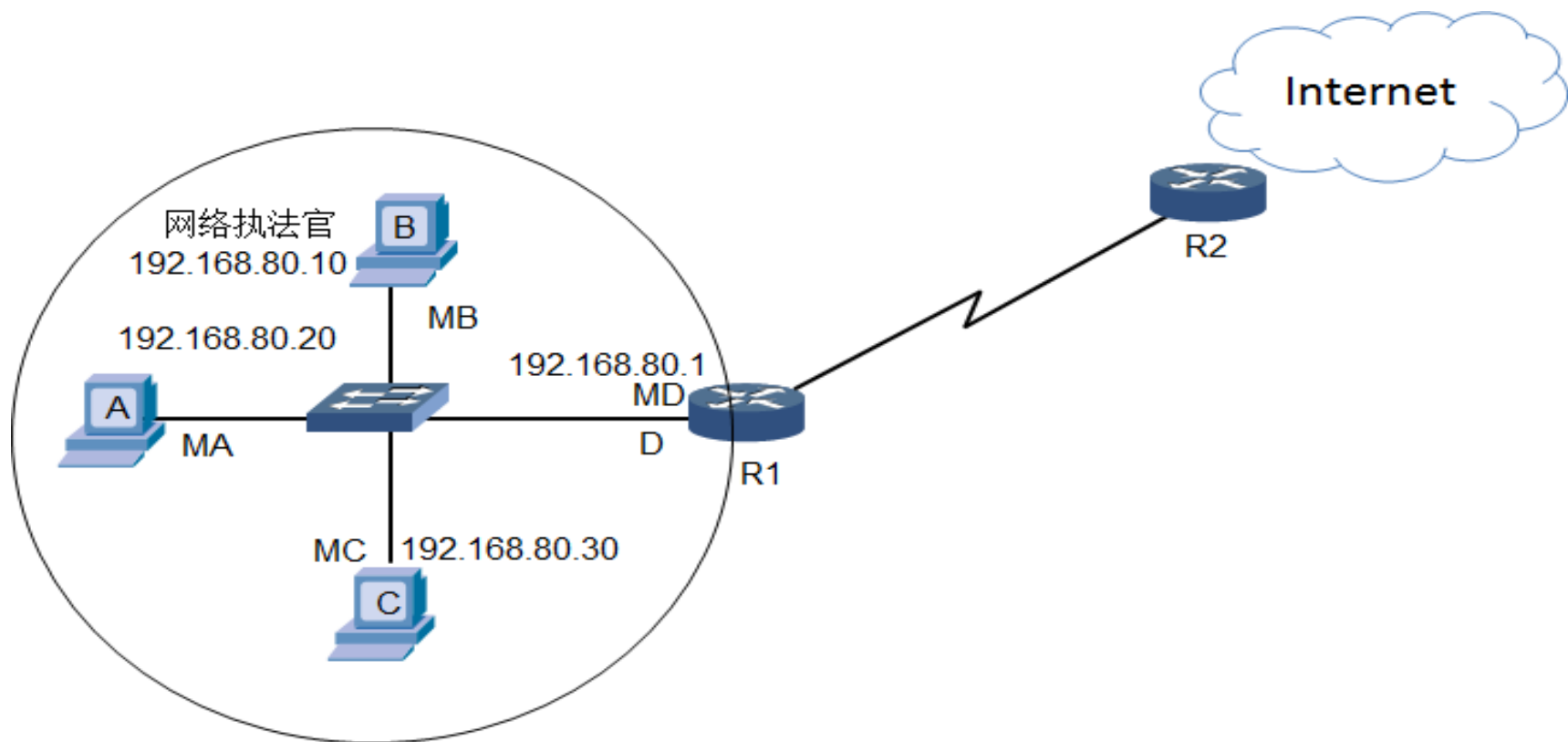


7.4.1 ARP协议的工作过程和安全隐患

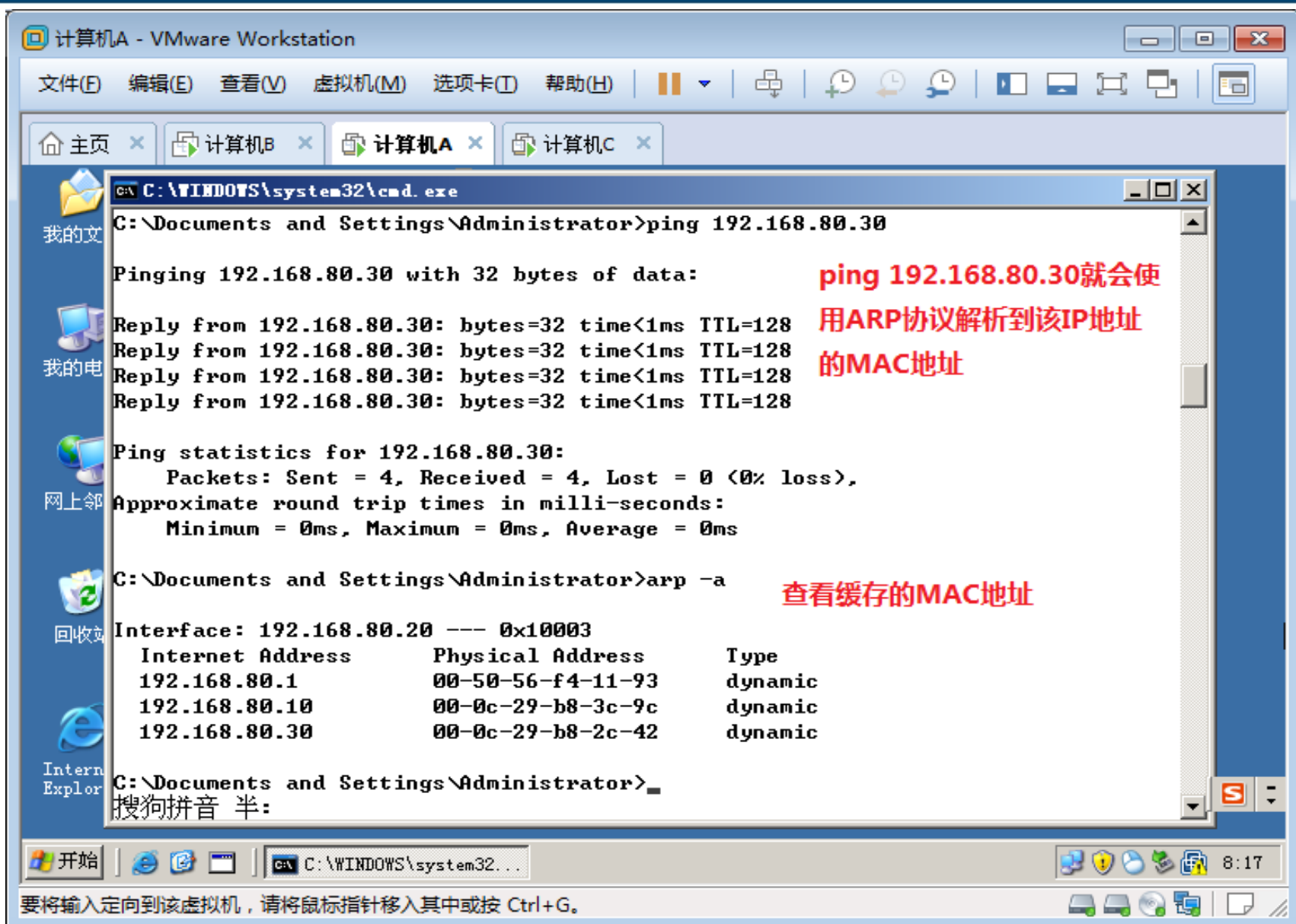
- ARP协议是建立在网络中各个主机互相信任的基础上的，计算机A发送ARP广播帧解析计算机C的MAC地址，同一个网段中的计算机都能够收到这个ARP请求消息，任何一个主机都可以给计算机A发送ARP应答消息，可以告诉计算机A一个错误的MAC地址，计算机A收到ARP应答报文时并不会检测该报文的真实性，就会将其记入本机ARP缓存，这就存在一个安全隐患--ARP欺骗。

7.4.2 ARP欺骗之网络执法官

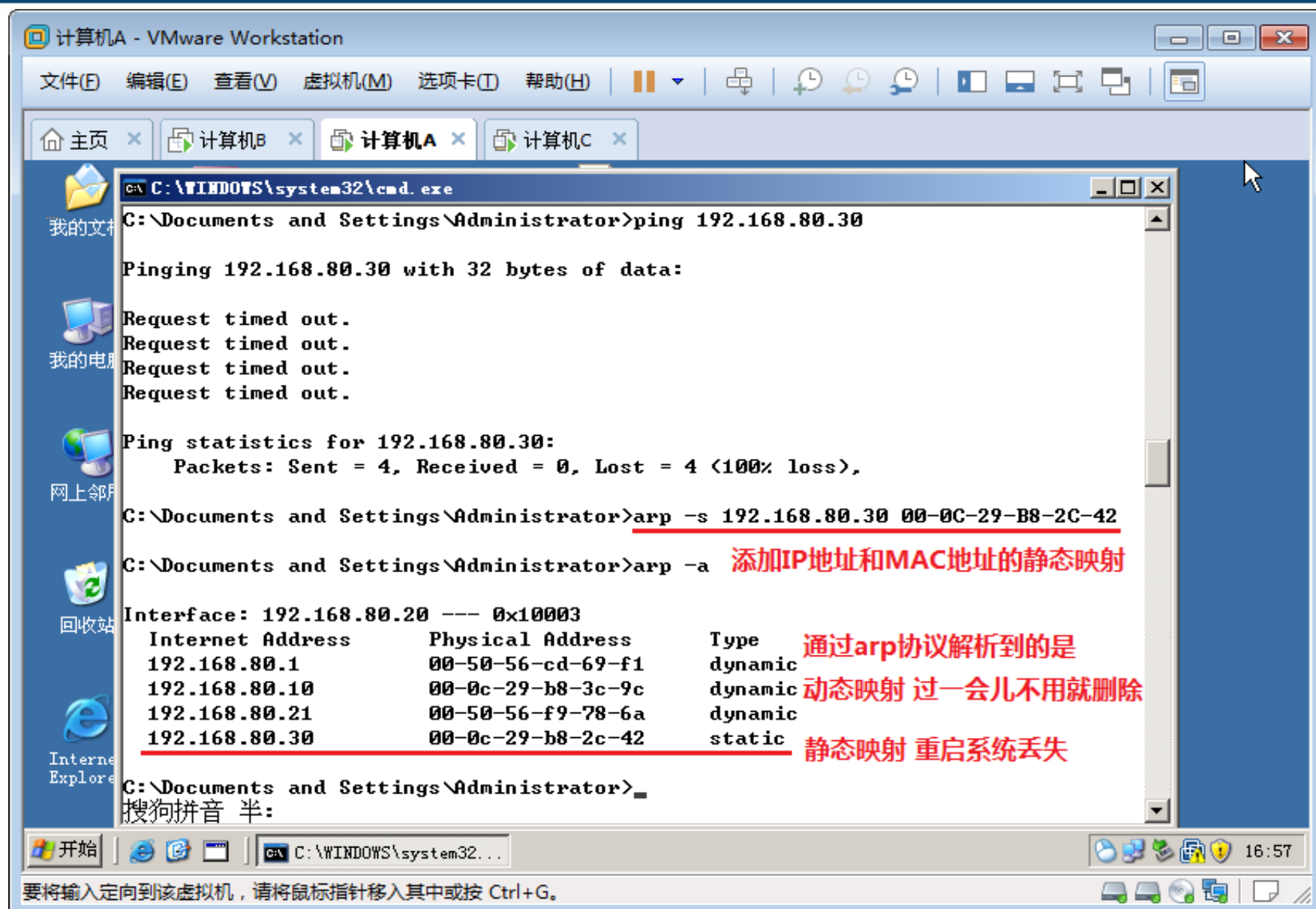
- 网络执法官软件可以控制以太网中的计算机通信



查看解析的MAC地址



7.4.3判断和防止ARP欺骗的方法

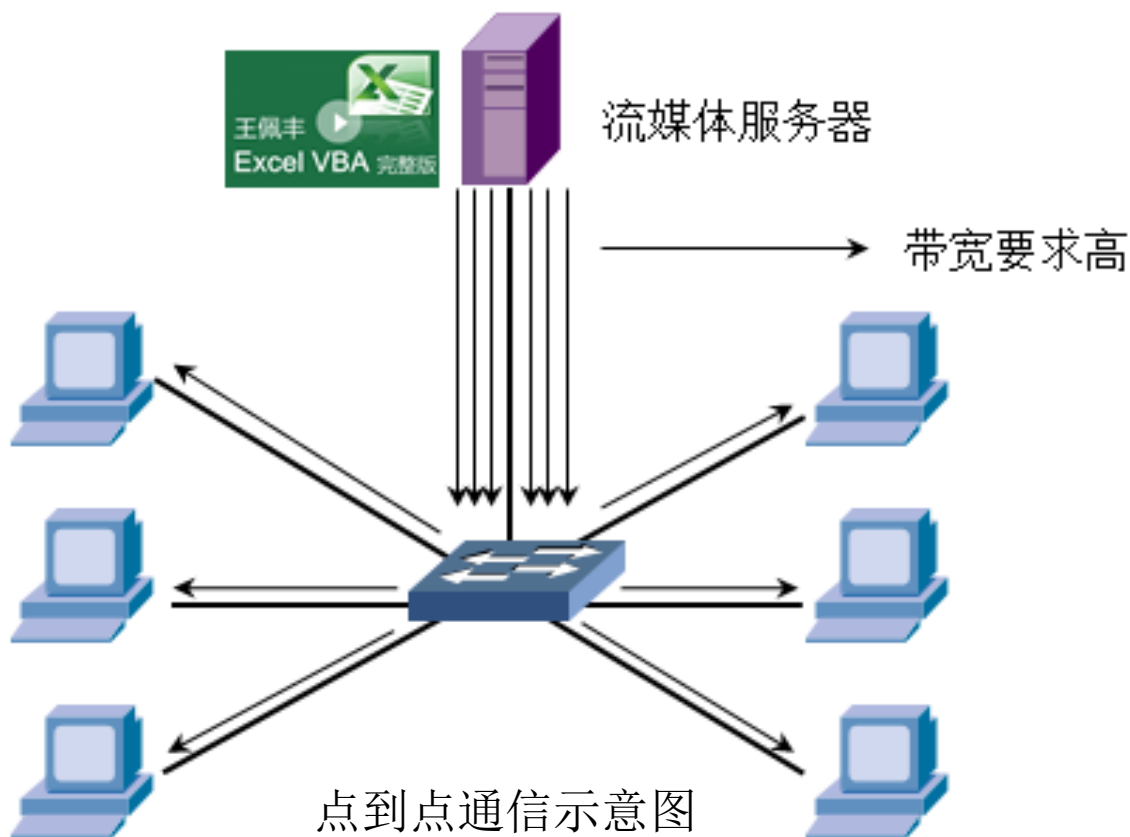


7.5 IGMP协议

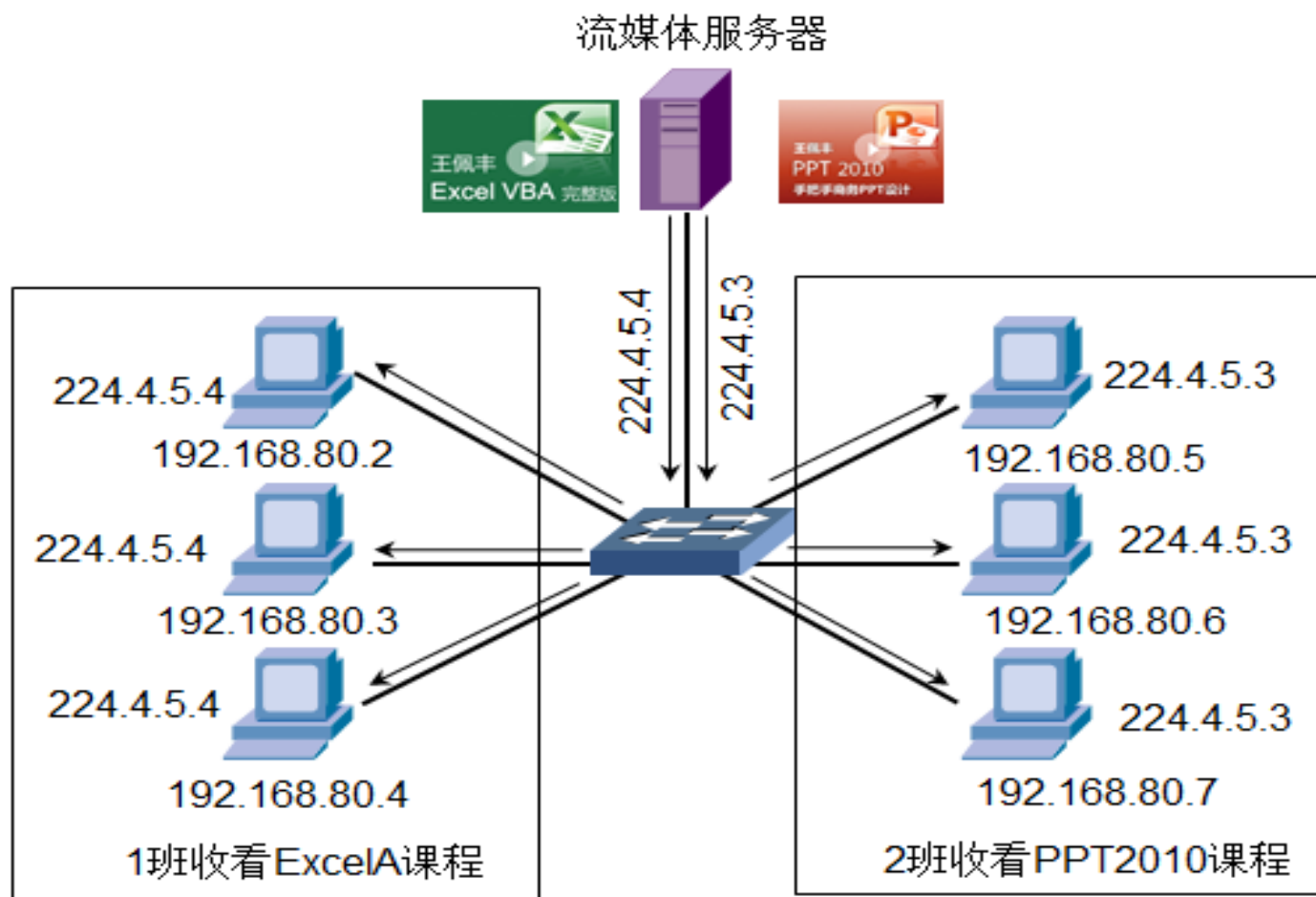
- 7.5.1什么是组播
- 7.5.2组播IP地址
- 7.5.3组播MAC地址
- 7.5.4组播管理协议（IGMP）

7.5.1什么是组播

- Internet 组管理协议称为IGMP协议（Internet Group Management Protocol），是因特网协议家族中的一个组播协议。该协议运行在主机和组播路由器之间，IGMP协议是网络层协议。要想搞明白IGMP协议的作用和用途，先要搞明白什么是组播通信，组播也称为多播。



组播节省网络带宽



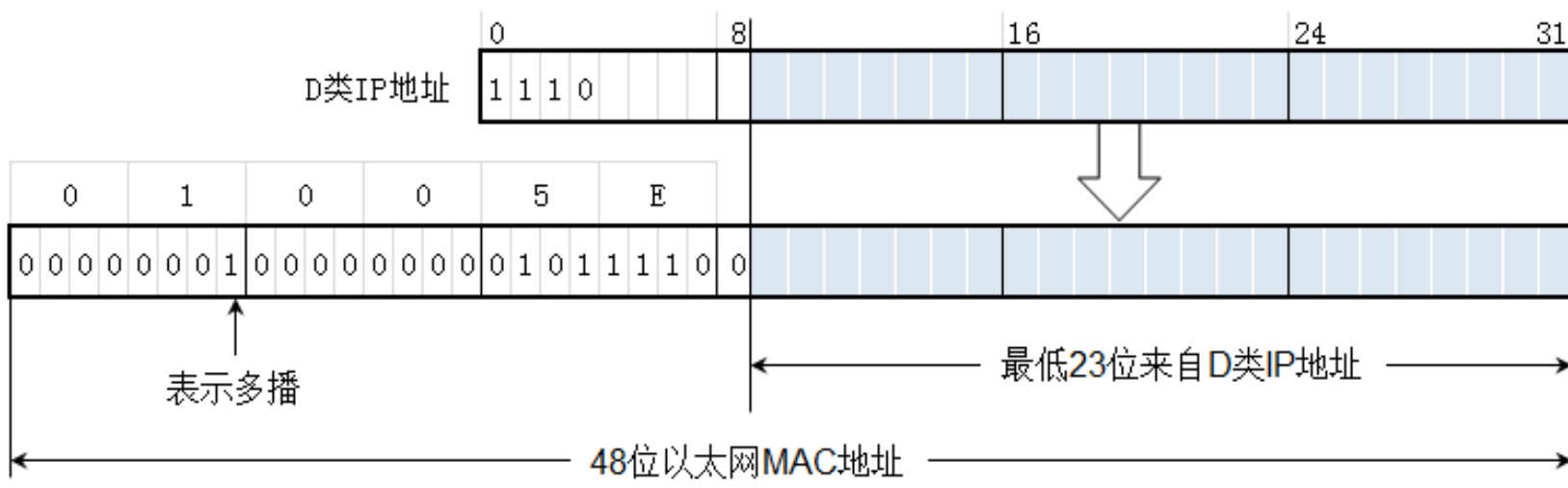
流媒体服务就像电视台，多播地址相当于不同频道。
可以使用两个组播地址向网络中发送两个课程的视频，
网络中的计算机绑定哪个多播地址就能收到哪个视频课程。

7.5.2组播IP地址

- IP地址中的D类地址是组播地址。D类IP地址的前四位是1110，因此D类地址范围是224.0.0.0到239.255.255.255。我们就用每一个D类地址标志一个多播组。
- 多播地址只能用于目的地址，而不能用于源地址。
- D类地址中有一些是不能随意使用的，因为有的地址已经被IANA指派为永久组地址了[RFC3330]。例如：
 - 224.0.0.0基地址（保留）
 - 224.0.0.1在本子网上的所有参加多播的主机和路由器
 - 224.0.0.2在本子网上的所有参加组播的路由器
 - 224.0.0.3未指派
 - 224.0.0.4 DVMRP路由器
 -
 - 224.0.1.0至238.255.255.255全球范围都可使用的组播地址
 - 239.0.0.0至239.255.255.255限制在一个组织的范围

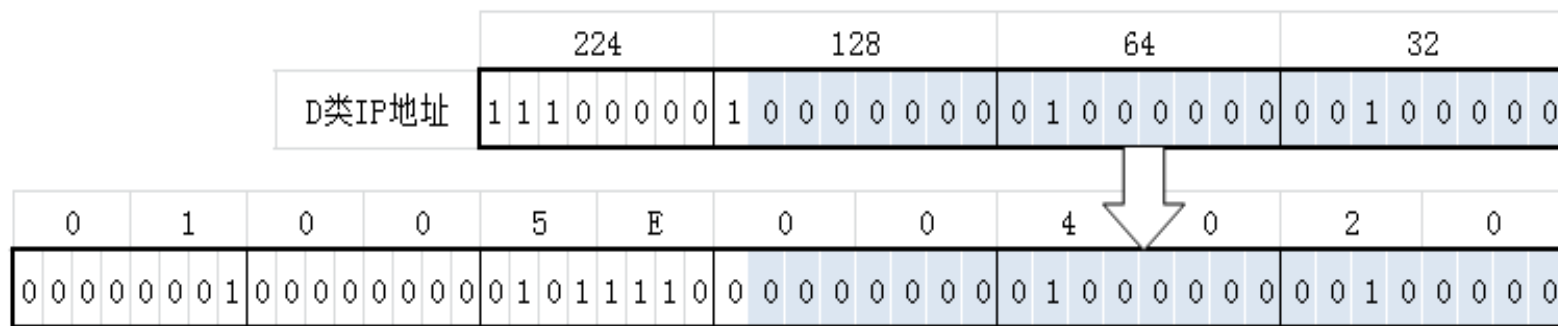
7.5.3组播MAC地址

- 目标地址是组播IP地址的数据包到达以太网，就要使用组播MAC地址封装，组播MAC地址使用组播IP地址构造。
- 为了支持IP 组播，因特网号码指派管理局IANA已经为 Ethernet的MAC地址保留了一个组播地址区间：01-00-5E-00-00-00 到 01-00-5E-7F-FF-FF。如图7-84所示，组播MAC地址48位的MAC地址中的高25位是固定的，为了映射一个IP 多播地址到MAC层的组播地址，IP多播地址的低23位可以直接映射为MAC层组播地址的低23位。

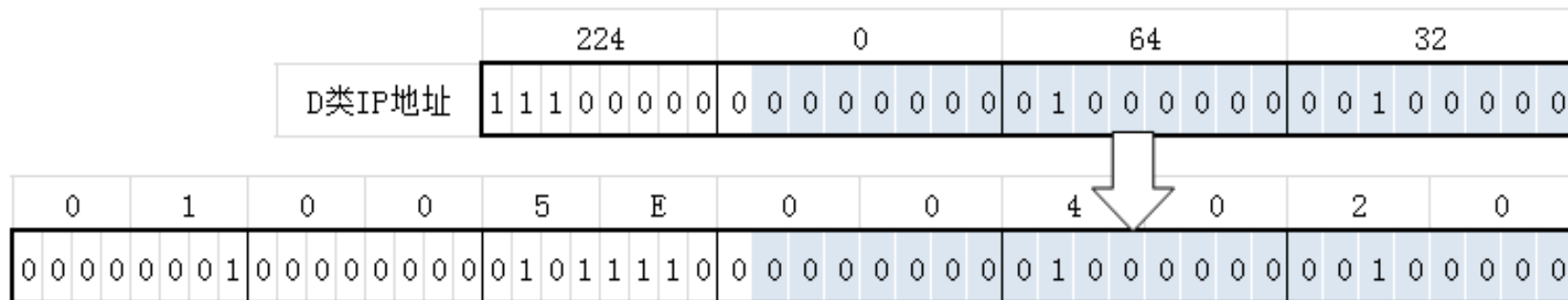


不同的组播IP地址可能构造出相同的多播MAC地址

- 比如组播IP地址224.128.64.32，如图7-85所示，使用上面的方法构造出的MAC地址为01-00-5E-00-40-20。



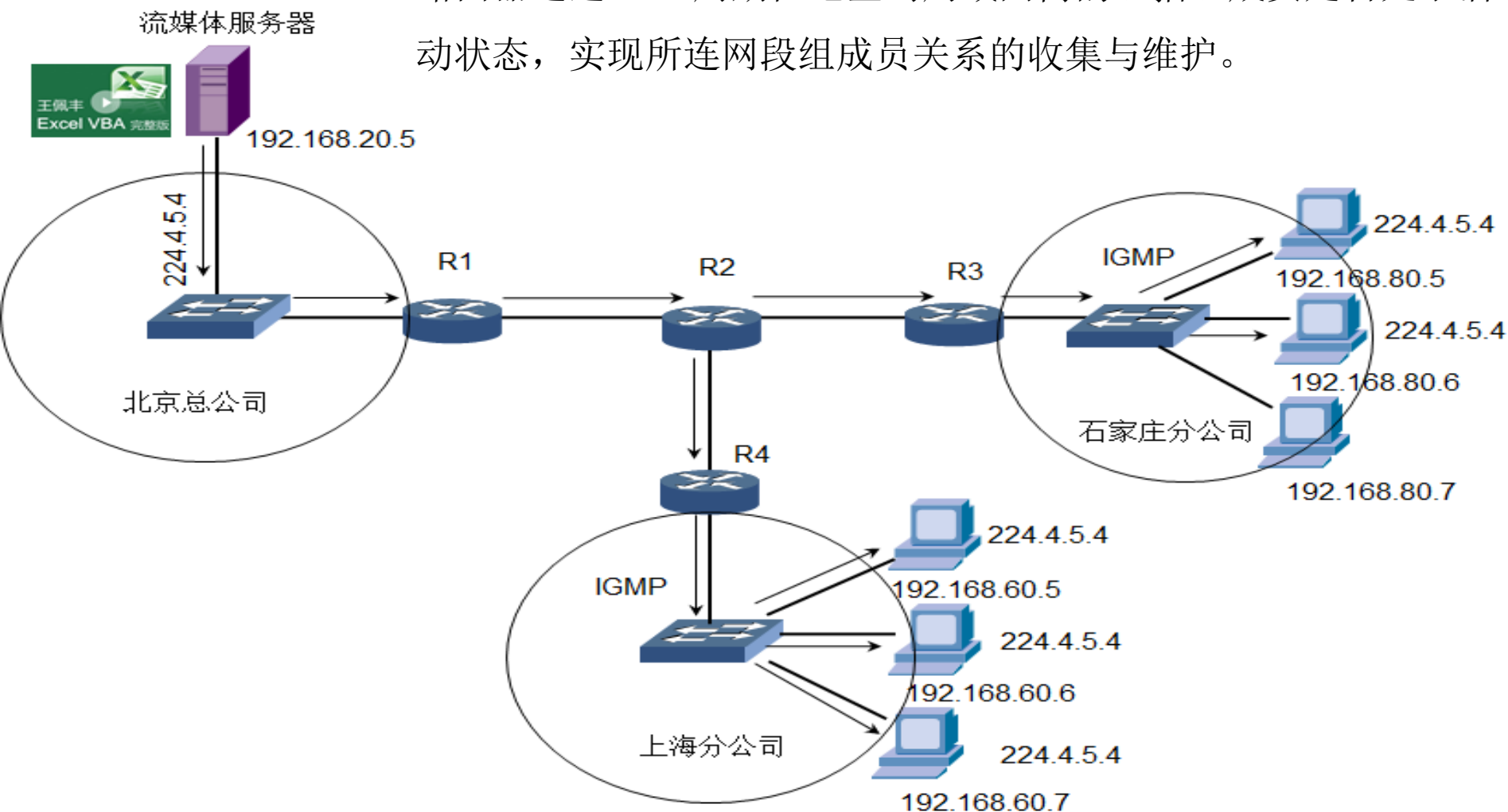
- 组播IP地址224.0.64.32，如下图7-86所示，使用上面的方法构造出的MAC地址也为01-00-5E-00-40-20。



7.5.4组播管理协议 (IGMP)

IGMP实现如下双向的功能:

1. 主机通过IGMP通知路由器希望接收或离开某个特定组播组的信息。
2. 路由器通过IGMP周期性地查询局域网内的组播组成员是否处于活动状态, 实现所连网段组成员关系的收集与维护。



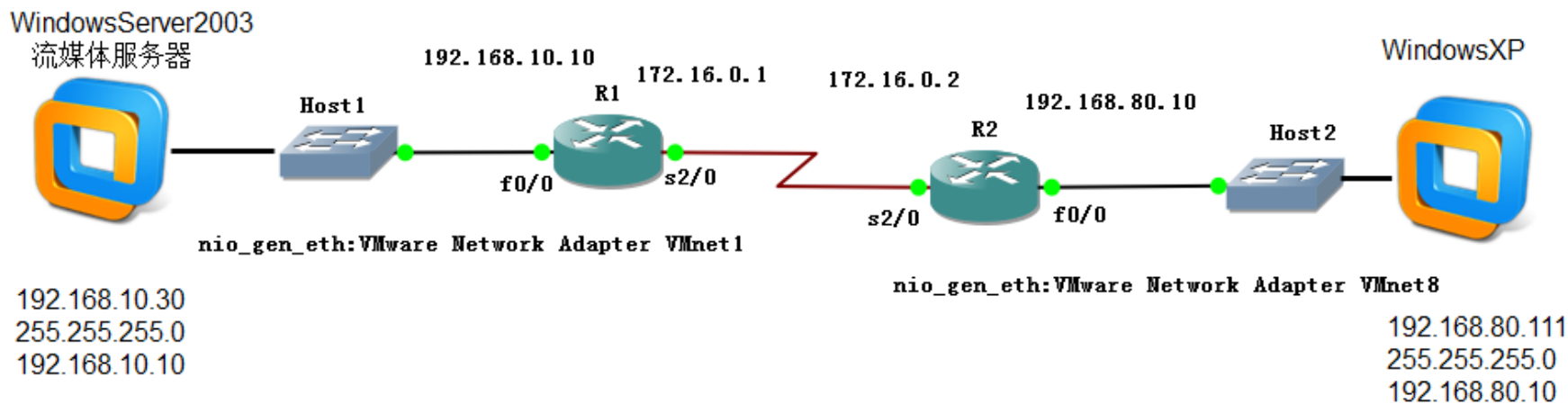
7.6实战：跨网段观看组播视频

■ 7.6.1搭建流媒体服务器

■ 7.6.2点播视频

■ 7.6.3访问多播视频

■ 7.6.4跨网段多播



7.6.4跨网段多播

- R2#debug ip igmp
- *Mar 1 01:04:38.235: IGMP(0): Received Group record for group 239.192.44.166, mode 2 from 192.168.80.111 for 0 sources
- *Mar 1 01:04:38.239: IGMP(0): WAVL Insert group: 239.192.44.166 interface: FastEthernet0/0Successful
- *Mar 1 01:04:38.239: IGMP(0): Switching to EXCLUDE mode for 239.192.44.166 on FastEthernet0/0
- *Mar 1 01:05:06.487: IGMP(0): Send v2 general Query on FastEthernet0/0
- *Mar 1 01:05:16.111: IGMP(0): Received v2 Report on FastEthernet0/0 from 192.168.80.111 for 239.192.44.166
- *Mar 1 01:06:11.115: IGMP(0): Received Leave from 192.168.80.111 (FastEthernet0/0) for 239.192.44.166
- *Mar 1 01:06:11.119: IGMP(0): Send v2 Query on FastEthernet0/0 for group 239.192.44.166