

MOOC_3.4_ICMP协议分析实验

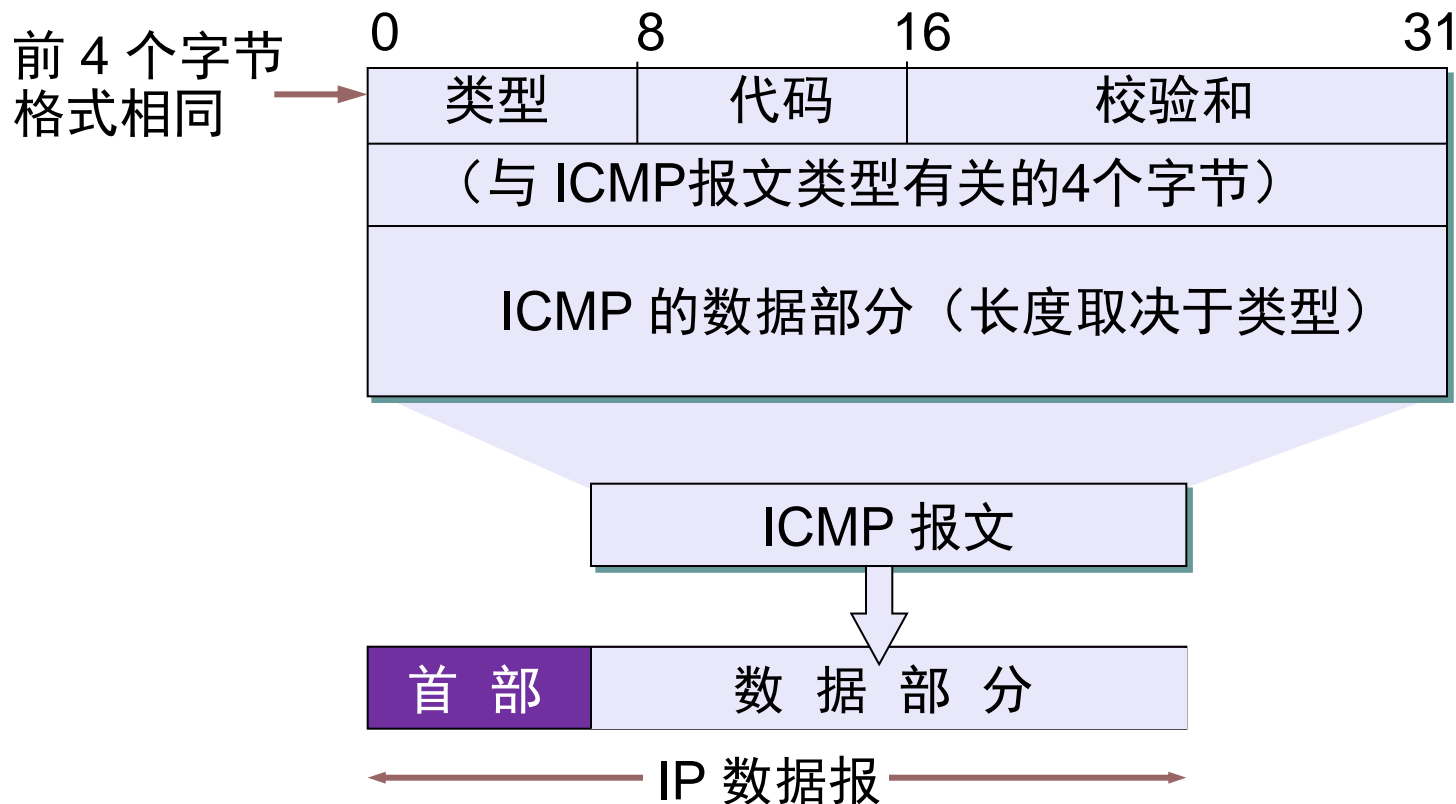
ICMP协议分析实验

- 实验目的
- 实验内容

ICMP协议是做什么的？

IP 报头	ICMP 报头	ICMP 信息
-------	---------	---------

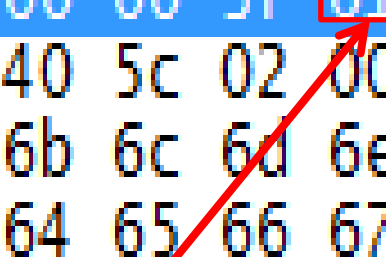
ICMP报文的格式



ICMP报文的格式

0	8	16	31
类型	代码	校验和	
(与 ICMP报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

```
ec a8 6b a0 57 c1 00 e0 fc 48 f6 44 08 00 45 00
00 3c 01 c2 00 00 3f 01 f3 99 c0 a8 03 0a c0 a8
02 0b 08 00 40 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69
```



ICMP报文的格式——回送请求与应答

0	8	16	31
类型			
代码			
校验和			
(与ICMP报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

ec a8 6b a0 57 c1 00 e0 fc 48 f6 44 08 00 45 00
00 3c 02 c2 00 00 3f 01 f3 99 c0 a8 03 0a c0 a8
02 0b 08 00 40 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

00 e0 fc 48 f6 44 ec a8 6b a0 57 c1 08 00 45 00
00 3c 02 b5 00 00 40 01 f1 a6 c0 a8 02 0b c0 a8
03 0a 00 00 48 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

ICMP报文的格式——回送请求与应答

0	8	16	31
类型			
代码			
校验和			
(与 ICMP 报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

ec a8 6b a0 57 c1 00 e0 fc 48 f6 44 08 00 45 00
00 3c 01 c7 00 00 3f 01 f3 99 c0 a8 03 0a c0 a8
02 0b 08 00 40 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

00 e0 fc 48 f6 44 ec a8 6b a0 57 c1 08 00 45 00
00 3c 02 b5 00 00 40 01 f1 a6 c0 a8 02 0b c0 a8
03 0a 00 00 48 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

ICMP报文的格式——回送请求与应答

0	8	16	31
类型	代码	校验和	
(与 ICMP 报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

ec a8 6b a0 57 c1 00 e0 fc 48 f6 44 08 00 45 00
00 3c 01 c2 00 00 3f 01 f3 99 c0 a8 03 0a c0 a8
02 0b 08 00 40 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

00 e0 fc 48 f6 44 ec a8 6b a0 57 c1 08 00 45 00
00 3c 02 b5 00 00 40 01 f1 a6 c0 a8 02 0b c0 a8
03 0a 00 00 48 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

ICMP报文的格式——回送请求与应答

0	8	16	31
类型		代码	校验和
标识		序列号	
ICMP 的数据部分（长度取决于类型）			

ec a8 6b a0 57 c1 00 e0 fc 48 f6 44 08 00 45 00
00 3c 01 c2 00 00 3f 01 f3 99 c0 a8 03 0a c0 a8
02 0b 08 00 40 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

00 e0 fc 48 f6 44 ec a8 6b a0 57 c1 08 00 45 00
00 3c 02 b5 00 00 40 01 f1 a6 c0 a8 02 0b c0 a8
03 0a 00 00 48 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69

ICMP报文的格式——回送请求与应答

0	8	16	31
类型	代码	校验和	
标识		序列号	
ICMP 的数据部分（长度取决于类型）			

```
ec a8 6b a0 57 c1 00 e0 fc 48 f6 44 08 00 45 00
00 3c 01 c2 00 00 3f 01 f3 99 c0 a8 03 0a c0 a8
02 0b 08 00 40 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69
```

```
00 e0 fc 48 f6 44 ec a8 6b a0 57 c1 08 00 45 00
00 3c 02 b5 00 00 40 01 f1 a6 c0 a8 03 0b c0 a8
03 0a 00 00 48 5c 02 00 0b 00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
77 61 62 63 64 65 66 67 68 69
```

ping的过程

192.168.2.11
可达吗?

主机A

192.168.3.10

嘿，我收到你了！

192.168.2.11

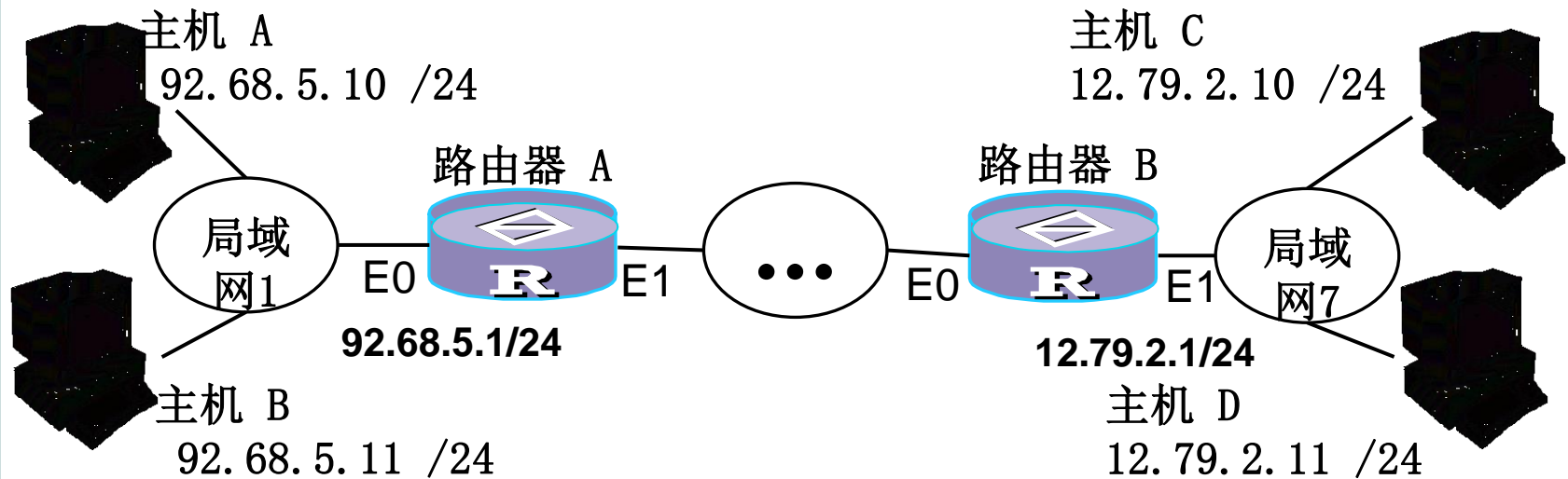
主机B

ICMP Echo Request

ICMP Echo Reply

00	e0	fc	48	f6	44	ec	a8	6b	a0	57	c1	08	00	45	00
00	3c	02	b5	00	00	40	01	f1	a6	c0	a8	02	0b	c0	a8
03	0a	00	00	48	5c	02	00	0b	00	61	62	63	64	65	66
67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76
77	61	62	63	64	65	66	67	68	69						

差错报告报文



ICMP类型域含义

类型	ICMP报文功能	类型	ICMP报文功能
0	回送应答，构成常用的ping命令	13	时戳请求
3	信宿不可达	14	时戳应答
4	信源抑制，用于流控和拥塞控制	15	信息请求（已不用）
5	重定向（改变路由）	16	信息应答（已不用）
8	回送请求，构成常用的ping命令	17	地址掩码请求
11	数据报超时，超过分组生成周期	18	地址掩码应答
12	数据报参数错		

ICMP报文的格式——终点不可达

0	8	16	31
类型	代码	校验和	
(与 ICMP报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

ec a8 6b a0 57 c1 00 e0 fc 07 a3 c0 08 00 45 00
00 38 00 12 00 00 ff 01 36 56 c0 a8 02 01 c0 a8
02 0b 03 01 a7 a2 00 00 00 00 45 00 00 3c 02 a5
00 00 40 01 f1 be c0 a8 02 0b c0 a8 03 02 08 00
47 5c 02 00 04 00

ICMP报文的格式——终点不可达

0	8	16	31
类型	代码	校验和	
(与 ICMP报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

ec a8 6b a0 57 c1 00 e0 fc 07 a3 c0 08 00 45 00
00 38 00 12 00 00 ff 01 36 56 c0 a8 02 01 c0 a8
02 0b 03 01 a7 a2 00 00 00 00 45 00 00 3c 02 a5
00 00 40 01 f1 be c0 a8 02 0b c0 a8 03 02 08 00
47 5c 02 00 04 00

ICMP报文的格式——终点不可达

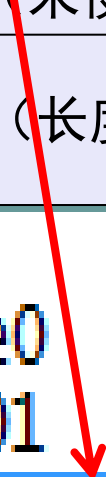
0	8	16	31
类型	代码	校验和	
(与 ICMP报文类型有关的4个字节)			
ICMP 的数据部分 (长度取决于类型)			

ec a8 6b a0 57 c1 00 e0 fc 07 a3 c0 08 00 45 00
00 38 00 12 00 00 ff 01 36 56 c0 a8 02 01 c0 a8
02 0b 03 01 a7 a2 00 00 00 00 45 00 00 3c 02 a5
00 00 40 01 f1 be c0 a8 02 0b c0 a8 03 02 08 00
47 5c 02 00 04 00

ICMP报文的格式——终点不可达

0	8	16	31
类型	代码	校验和	
为0（未使用）			
ICMP 的数据部分（长度取决于类型）			

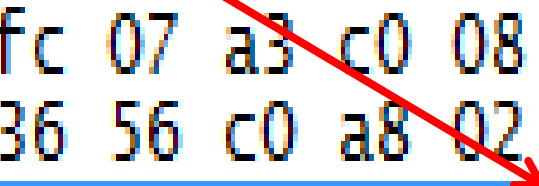
ec a8 6b a0 57 c1 00 e0 fc 07 a3 c0 08 00 45 00
00 38 00 12 00 00 ff 01 36 56 c0 a8 02 01 c0 a8
02 0b 03 01 a7 a2 00 00 00 00 45 00 00 3c 02 a5
00 00 40 01 f1 be c0 a8 02 0b c0 a8 03 02 08 00
47 5c 02 00 04 00



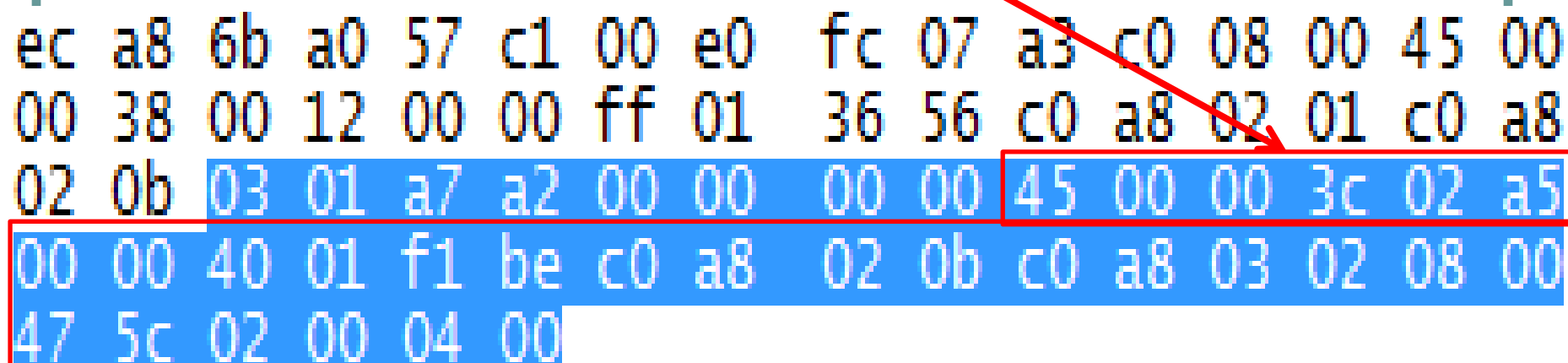
ICMP报文的格式——终点不可达

0	8	16	31
类型	代码	校验和	
为0（未使用）			
ICMP 的数据部分（长度取决于类型）			

ec a8 6b a0 57 c1 00 e0 fc 07 a3 c0 08 00 45 00
00 38 00 12 00 00 ff 01 36 56 c0 a8 02 01 c0 a8
02 0b 03 01 a7 a2 00 00 00 00 45 00 00 3c 02 a5
00 00 40 01 f1 be c0 a8 02 0b c0 a8 03 02 08 00
47 5c 02 00 04 00



ICMP报文的格式——终点不可达

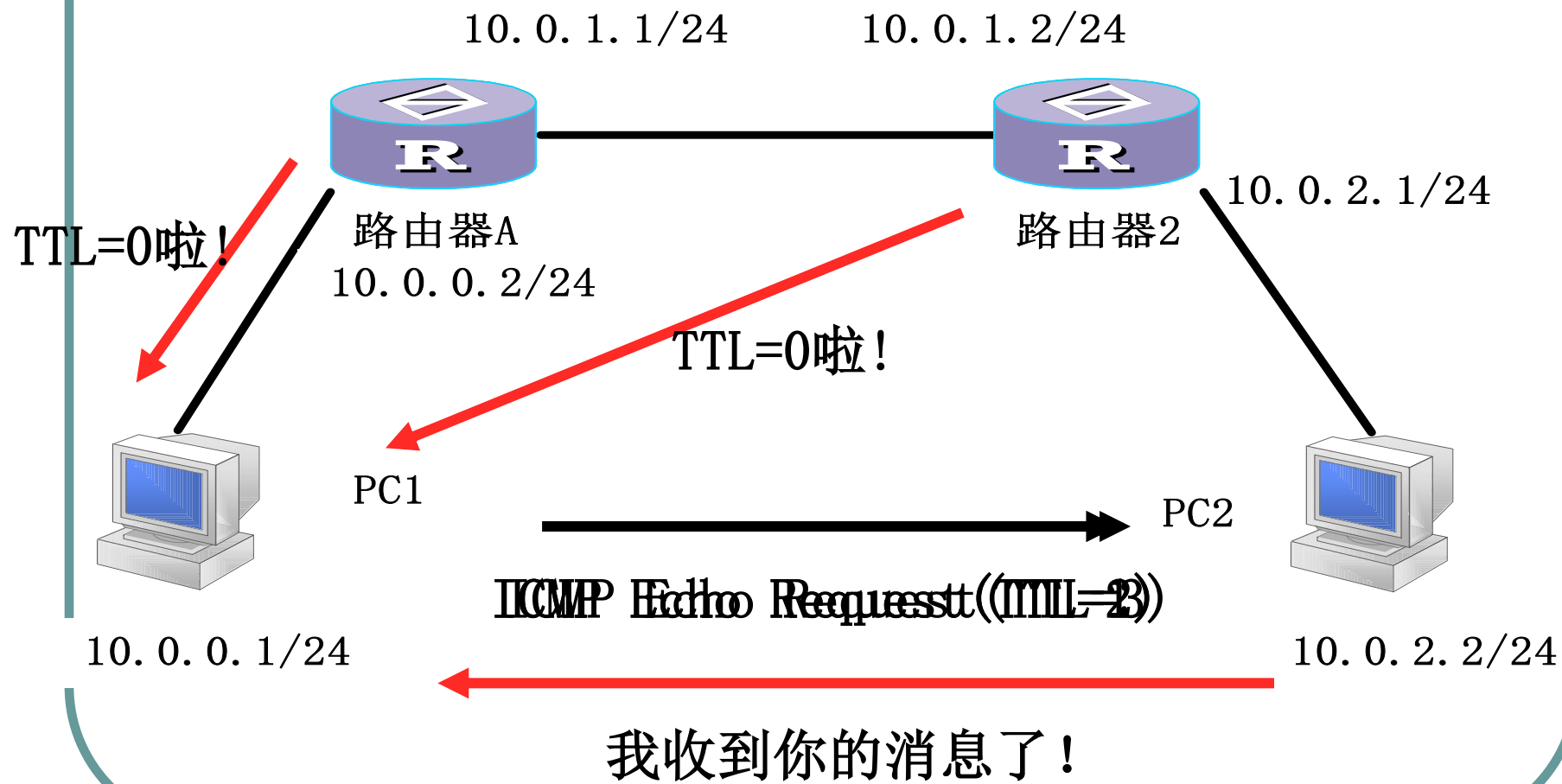


The diagram illustrates the structure of an ICMP Unreachable message. It shows a sequence of hexadecimal bytes. A red arrow points from the title to the 'Destination Address' field, which is highlighted with a red box. The 'Destination Address' field is 32 bytes long, starting with '45' (IP version 4) and '00' (type of service). The 'Next Hop Limit' field is 1 byte long, containing '3c' (60). The 'Checksum' field is 2 bytes long, containing '02' and 'a5'. The 'Data' field is 16 bytes long, starting with '00' and '00' (reserved), followed by '40' and '01' (type and code), and then 'f1', 'be', 'c0', 'a8', '02', '0b', 'c0', 'a8', '03', '02', '08', '00' (source and destination IP addresses).

ec	a8	6b	a0	57	c1	00	e0	fc	07	a3	c0	08	00	45	00
00	38	00	12	00	00	ff	01	36	56	c0	a8	02	01	c0	a8
02	0b	03	01	a7	a2	00	00	00	00	45	00	00	3c	02	a5
00	00	40	01	f1	be	c0	a8	02	0b	c0	a8	03	02	08	00
47	5c	02	00	04	00										

00	e0	fc	07	a3	c0	ec	a8	6b	a0	57	c1	08	00	45	00
00	3c	02	a5	00	00	40	01	f1	be	c0	a8	02	0b	c0	a8
03	02	08	00	47	5c	02	00	04	00	61	62	63	64	65	66
67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76
77	61	62	63	64	65	66	67	68	69						

Tracert的过程



ICMP报文格式和PingTest

ICMP协议实验台

ICMP报文

<-----8bits----->		<-----8bits----->		<-----16bits----->			
类型		代码		校验和			
13		0		0			
标识				序列			
10				01			
数据							
0		0		0		0	
0		0		0		0	
0		0		0		0	

目标地址 10.1.3.10 报文大小 20 发送... 退出