第五章 网络层

互联网控制协议

ICMP

为什么需要ICMP？

IP分组传送不可靠，可能遭遇各种问题

- 丢包，可能发生拥塞，产生很大延迟、抖动等

ICMP用来向源（通常）报告这些问题或状况

ICMP也常用来测试网络

ICMP - Internet Control Message Protocol

- 用来报告意外的事件或测试互联网
- More ICMP Types：

http://www.iana.org/assignments/icmp-parameters

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ICMP 消息格式

Protocol: 0X01

ICMP头标	ICMP数据

IP报头	IP数据

字节	0	1	2	3	4 … n
	类型	代码	校验和		数据区

ICMP头标

真实的ICMP消息

```
⊟ Internet Protocol Version 4, Src: 220.231.141.193 (220.2
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services
    Total Length: 128
    Identification: 0x3c25
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 47
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x22a2
    Source: 220.231.141.193
    Destination: 192.168.1.1
⊟ Internet Control Message P
    Type: 3 (Destination unr
    Code: 10 (Host administr
    Checksum: 0xe342 [corre
```

```
⊟ Internet Protocol Version 4, Src: 113.67.24.20
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0)
    Total Length: 56
    Identification: 0xab8a (43914)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 119
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x4c1f [correct]
    Source: 113.67.24.203 (113.67.24.203)
    Destination: 192.168.1.101 (192.168.1.101)
⊟ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x7795 [correct]
⊟ Internet Protocol Version 4, Src: 192.168.1.
```

应用 1：ping的工作原理

- 使用ping命令（即调用ping过程）时，将向目的站点发送一个ICMP回声请求报文（包括一些任选的数据），
- 如目的站点接收到该报文，必须向源站点发回一个ICMP回声应答报文，源站点收到应答报文（且其中的任选数据与所发送的相同），则认为目的站点是可达的，否则为不可达。

ICMP 工具 ——ping

测试TCP/IP是否正常工作	ping 127.0.0.1
网络设备是否正确	ping 本机IP地址
检查对外连接的路由器	ping 默认网关IP
检查与某台设备的畅通情况	ping IP
检查DNS设置	如ping www.scut.edu.cn
执行DNS反向查询	ping –a IP地址

```
C:\Documents and Settings\dcampus>ping -a 202.112.17.33
    Pinging orange.gznet.edu.cn [202.112.17.33] with 32 bytes of data:
```

例1（ok）

```
C>ping 172.16.1.20
Pinging 172.16.1.20 with 32 bytes of data:  （正常）
Reply from 172.16.1.20: bytes=32 time<10ms TTL=127
Reply from 172.16.1.20: bytes=32 time<10ms TTL=127
Reply from 172.16.1.20: bytes=32 time<10ms TTL=127
Reply from 172.16.1.20: bytes=32 time<10ms TTL=127
        Ping statistics for 172.16.1.20:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
        Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

例2（have problem）

```
C>ping 172.16.1.20

Pinging 172.16.1.21 with 32 bytes of data:   （有问题）

Request timed out.

Request timed out.

Request timed out.

Request timed out.

        Ping statistics for 172.16.1.21:

 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

应用 2：tracert命令

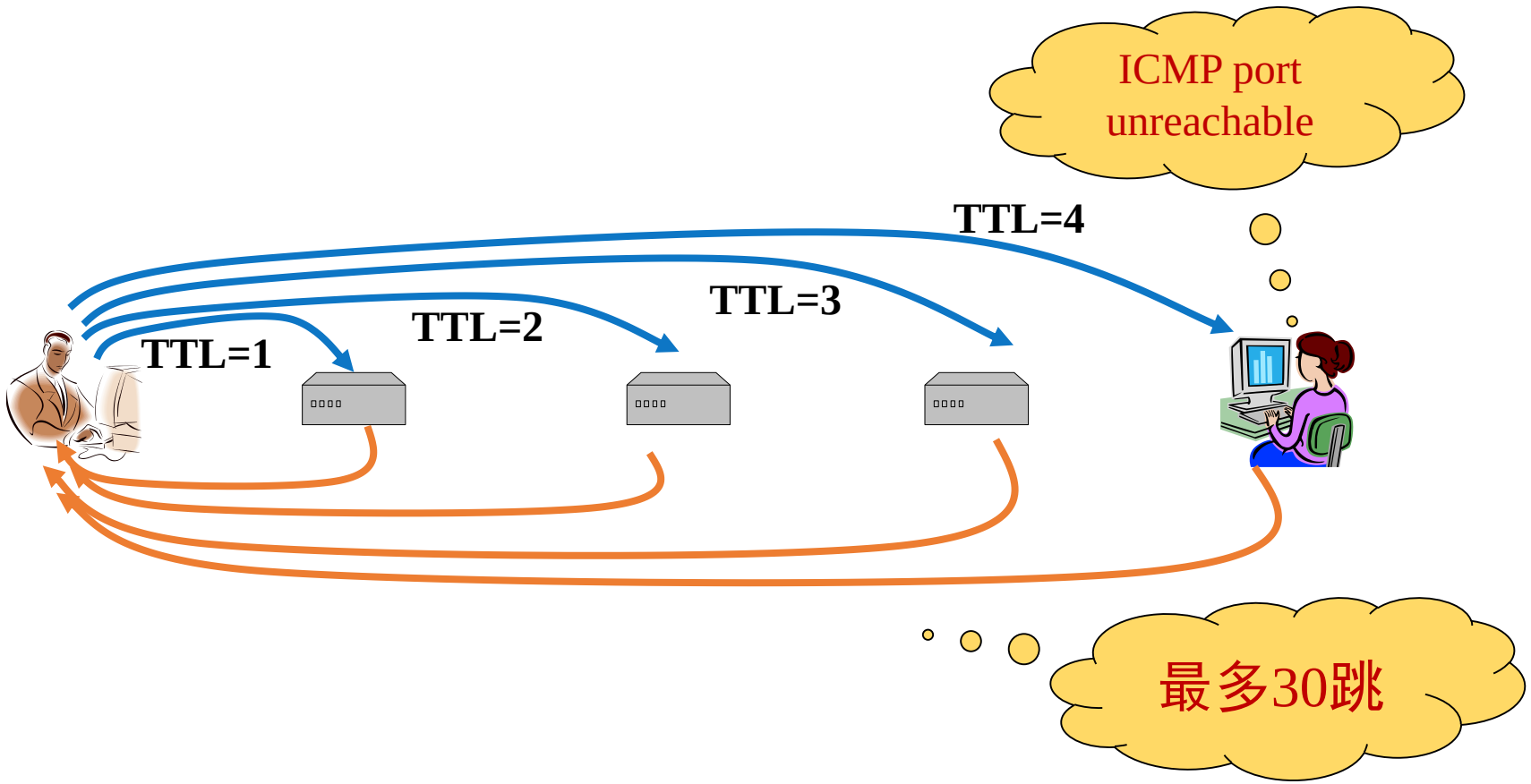
- tracert过程是通过ICMP数据报超时报文来得到一张途经的路由器列表
- 源主机向目的主机发一个IP报文，并置TTL为1，到达第一个路由器时，TTL减1，为0，则该路由器回发一个ICMP数据报超时报文，源主机取出路由器的IP地址即为途经的第一个路由端口地址

应用 2：tracert命令

- 接着源主机再向目的主机发第二个IP报文，并置TTL为2，然后再发第三个、第四个IP数据报，……直至到达目的主机
- 但互联网的运行环境状态是动态的，每次路径的选择有可能不一致，所以，只有在相对较稳定（相对变化缓慢）的网络中，tracert才有意义

Traceroute原理图示

- TTL=1
- TTL=2
- TTL=3
- TTL=4



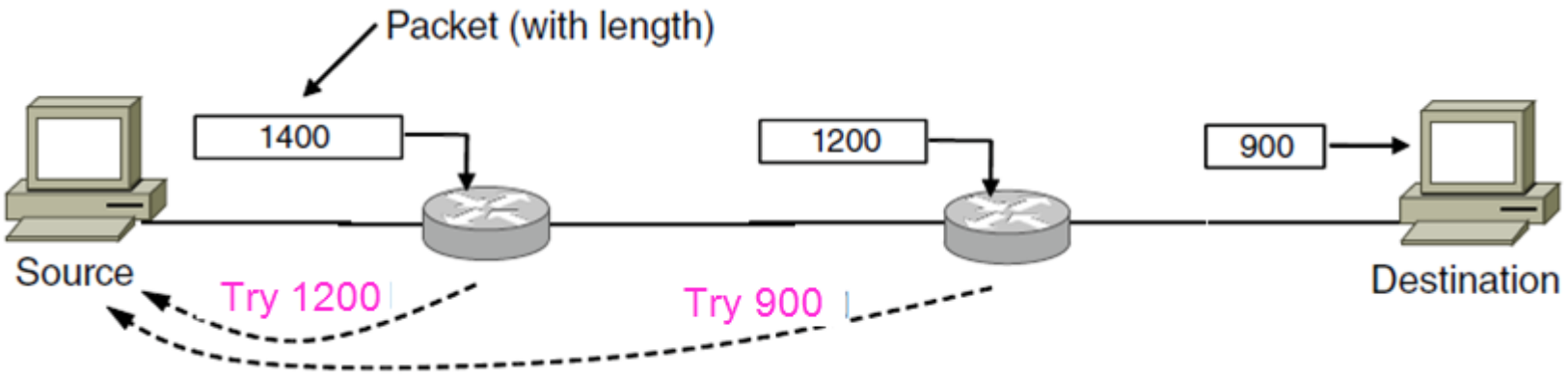
例： Tracert

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\dcampus>tracert www.sina.com.cn

Tracing route to jupiter.sina.com.cn [202.205.3.130]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  scut-bgw5.scut.edu.cn [202.112.18.254
  2    <1 ms    <1 ms    <1 ms  scn-rgw8.gznet.edu.cn [202.112.19.93]
  3     *        *        *     Request timed out.
  4    <1 ms    <1 ms    <1 ms  202.127.216.22
  5     *       37 ms    34 ms  202.127.216.21
  6    34 ms    33 ms    34 ms  cd1.cernet.net [202.112.53.74]
  7    34 ms    34 ms    33 ms  wdc1.cernet.net [202.112.38.82]
  8    34 ms    34 ms    34 ms  202.205.13.249
  9    34 ms    34 ms    34 ms  202.205.13.210
 10    34 ms    34 ms    34 ms  202.205.3.130

Trace complete.
```

应用3：PMTU

- 发数据包，分段标记DF=1，尝试1400，1200，900，直到到达目的机
- 结果：MTU=900



type=3的code

Codes	Description	Reference
0	Net Unreachable	[RFC792]
1	Host Unreachable	[RFC792]
2	Protocol Unreachable	[RFC792]
3	Port Unreachable	[RFC792]
4	Fragmentation Needed and Don't Fragment was Set	[RFC792]
5	Source Route Failed	[RFC792]
6	Destination Network Unknown	[RFC1122]
7	Destination Host Unknown	[RFC1122]
8	Source Host Isolated	[RFC1122]
9	Communication with Destination Network is Administratively Prohibited	[RFC1122]
10	Communication with Destination Host is Administratively Prohibited	[RFC1122]

注意

- 一般来说，ICMP 消息仅送给源机
- ICMP数据传输方式和其他数据传输方式一样，也可能遇到同样的错误，规定：ICMP消息不生成自己的差错报告

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

小结

- ICMP可用来报告网络事件和测试网络
- ICMP消息本身也可能遭遇问题，不报告本身的问题
- ICMP消息封装在IP分组中
- Ping应用原理
- Tracert应用原理

思考题

- 为什么需要ICMP？
- ICMP消息的封装格式是怎样的？
- ICMP应用ping是利用的什么类型的消息？
- ICMP应用tracert是利用的什么类型的消息？

谢谢观看

致谢

本课程课件中的部分素材来自于：（1）清华大学出版社出版的翻译教材《计算机网络》（原著作者：Andrew S. Tanenbaum，David J. Wetherall）；（2）思科网络技术学院教程；（3）网络上搜到的其他资料。在此，对清华大学出版社、思科网络技术学院、人民邮电出版社、以及其它提供本课程引用资料的个人表示衷心的感谢！

对于本课程引用的素材，仅用于课程学习，如有任何问题，请与我们联系！