第六章 传输层

# TCP 连接的建立

# TCP 连接的建立

采用三次握手建立连接

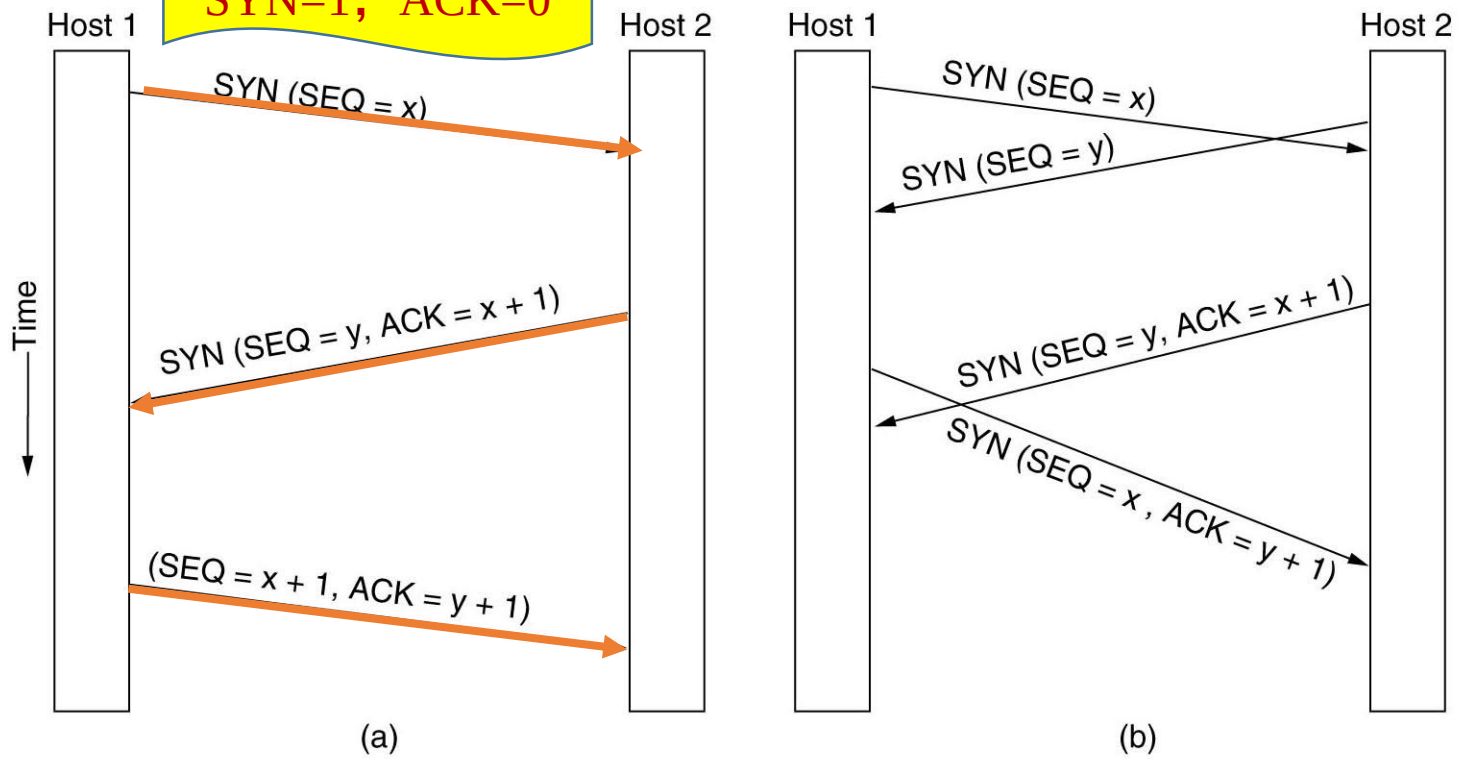
- 一方（server）被动地等待一个进来的连接请求
- 另一方（the client）通过发送连接请求，设置一些参数
- 服务器方回发确认应答
- 应答到达请求方，请求方最后确认，连接建立

# TCP 连接的建立

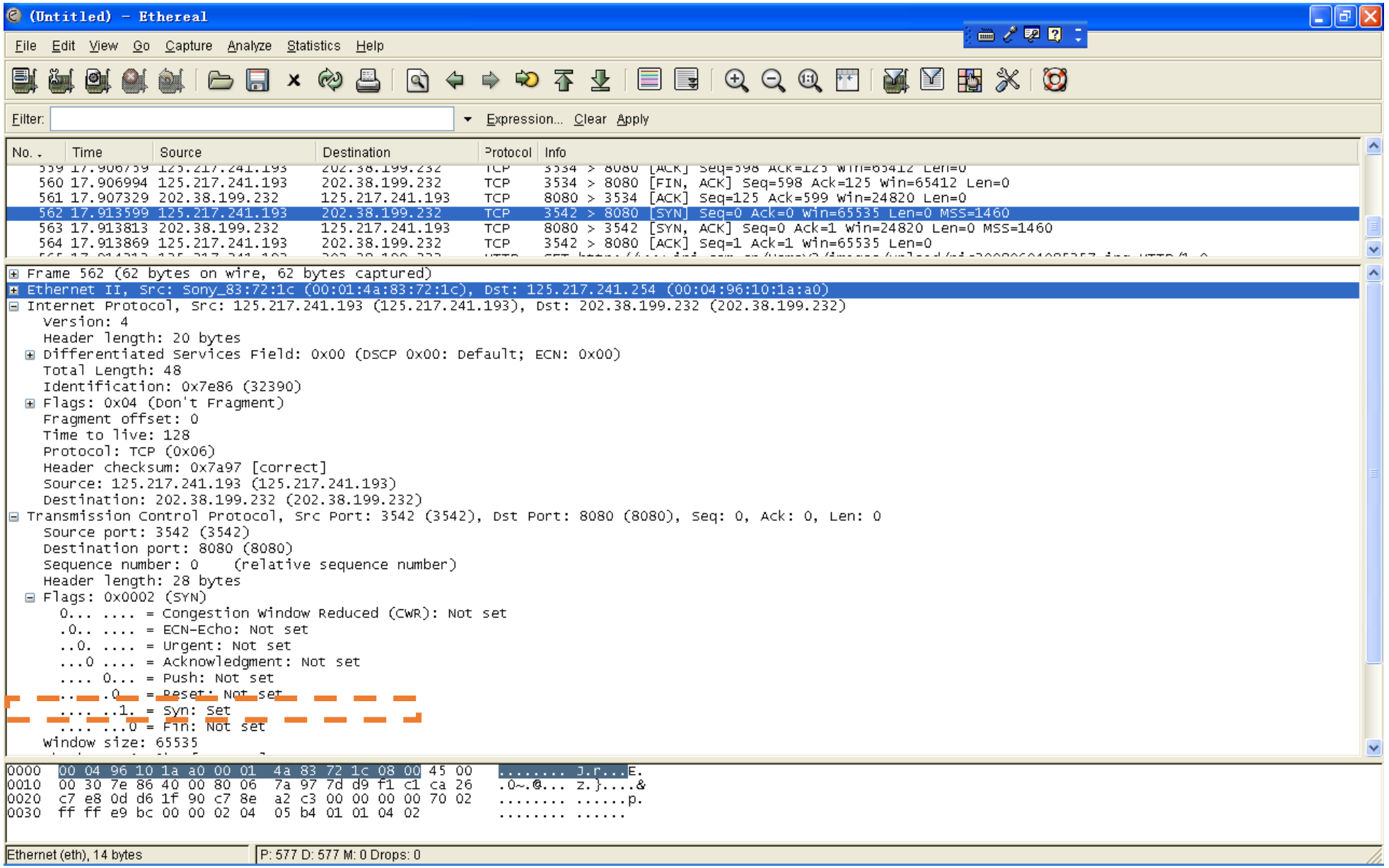
SYN=1，ACK=0

SYN=1，ACK=1

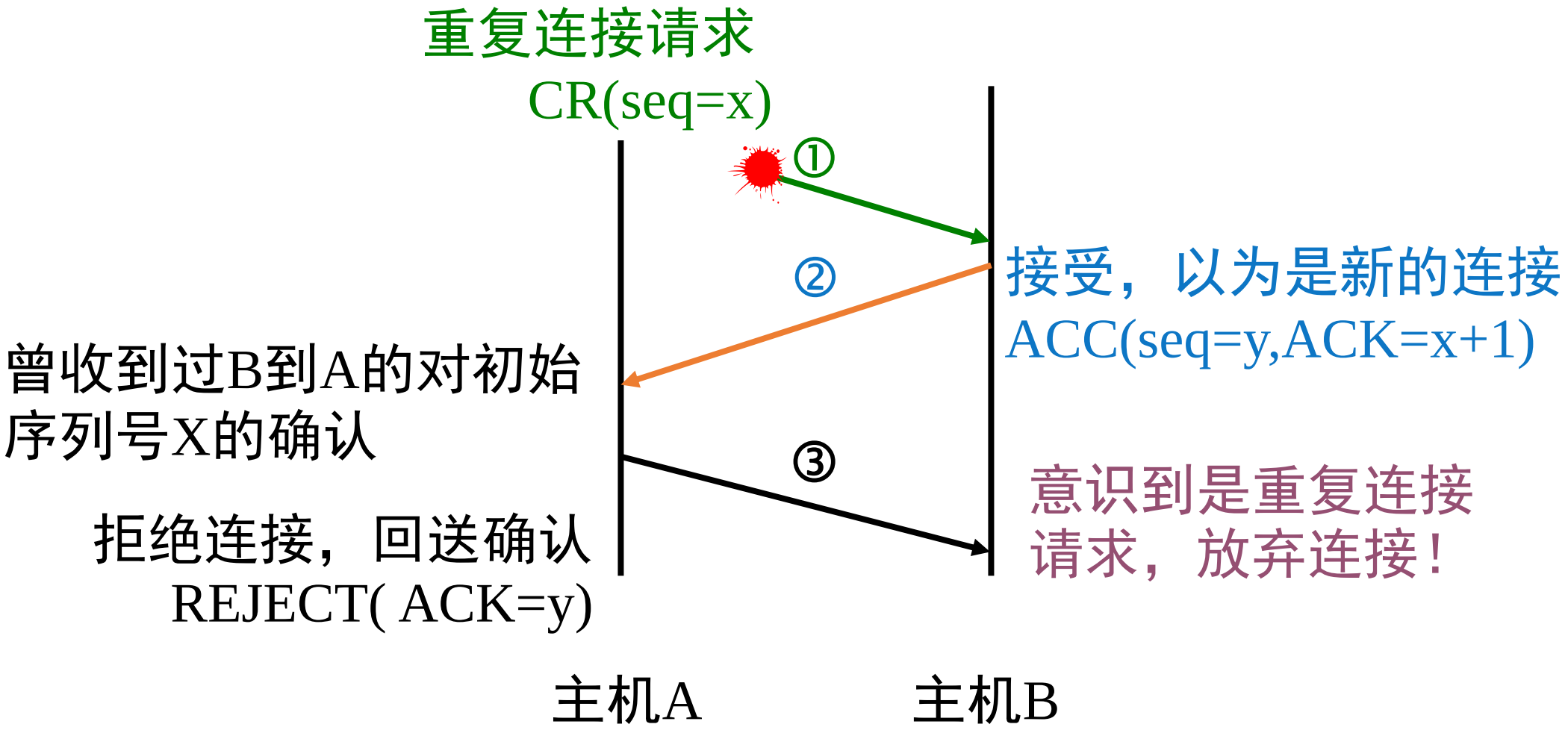
SYN=0，ACK=1



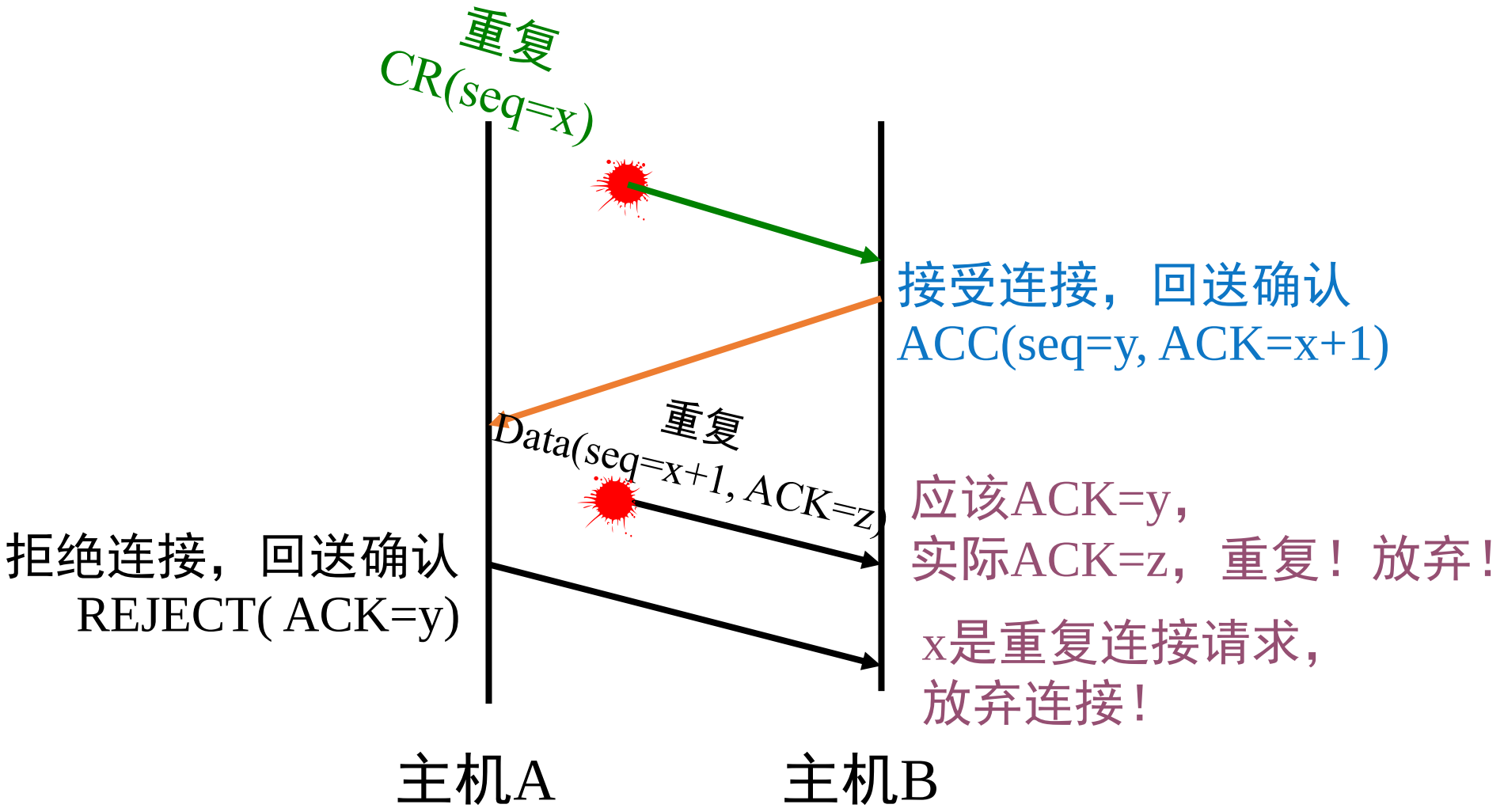
# 三次握手


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
560 17.906994 125.217.241.193 202.38.199.232 TCP 3534 > 8080 [FIN, ACK] Seq=598 Ack=125 Win=65412 Len=0
561 17.907329 202.38.199.232 125.217.241.193 TCP 8080 > 3534 [ACK] Seq=125 Ack=599 Win=24820 Len=0
562 17.913599 125.217.241.193 202.38.199.232 TCP 3542 > 8080 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
563 17.913813 202.38.199.232 125.217.241.193 TCP 8080 > 3542 [SYN, ACK] Seq=0 Ack=1 Win=24820 Len=0 MSS=1460
564 17.913869 125.217.241.193 202.38.199.232 TCP 3542 > 8080 [ACK] Seq=1 Ack=1 Win=65535 Len=0
Frame 562 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Sony_83:72:1c (00:01:4a:83:72:1c), Dst: 125.217.241.254 (00:04:96:10:1a:a0)
Internet Protocol, Src: 125.217.241.193 (125.217.241.193), Dst: 202.38.199.232 (202.38.199.232)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 48
Identification: 0x7e86 (32390)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x7a97 [correct]
Source: 125.217.241.193 (125.217.241.193)
Destination: 202.38.199.232 (202.38.199.232)
Transmission Control Protocol, Src Port: 3542 (3542), Dst Port: 8080 (8080), Seq: 0, Ack: 0, Len: 0
Source port: 3542 (3542)
Destination port: 8080 (8080)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x0002 (SYN)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
.... ...0 = Fin: Not set
Window size: 65535
0000 00 04 96 10 1a a0 00 01 4a 83 72 1c 08 00 45 00 ........ J.r...E.
0010 00 30 7e 86 40 00 80 06 7a 97 7d d9 f1 c1 ca 26 .0~.@... z.}....&
0020 c7 e8 0d d6 1f 90 c7 8e a2 c3 00 00 00 00 70 02 ........ ......p.
0030 ff ff e9 bc 00 00 02 04 05 b4 01 01 04 02 ........ ......
Ethernet (eth), 14 bytes
P: 577 D: 577 M: 0 Drops: 0

# 重复连接请求CR


重复连接请求
CR(seq=x)
①
②
接受，以为是新的连接
ACC(seq=y,ACK=x+1)
曾收到过B到A的对初始序列号X的确认
③
意识到是重复连接请求，放弃连接！
拒绝连接，回送确认
REJECT( ACK=y)
主机A
主机B

# 重复CR与重复ACK

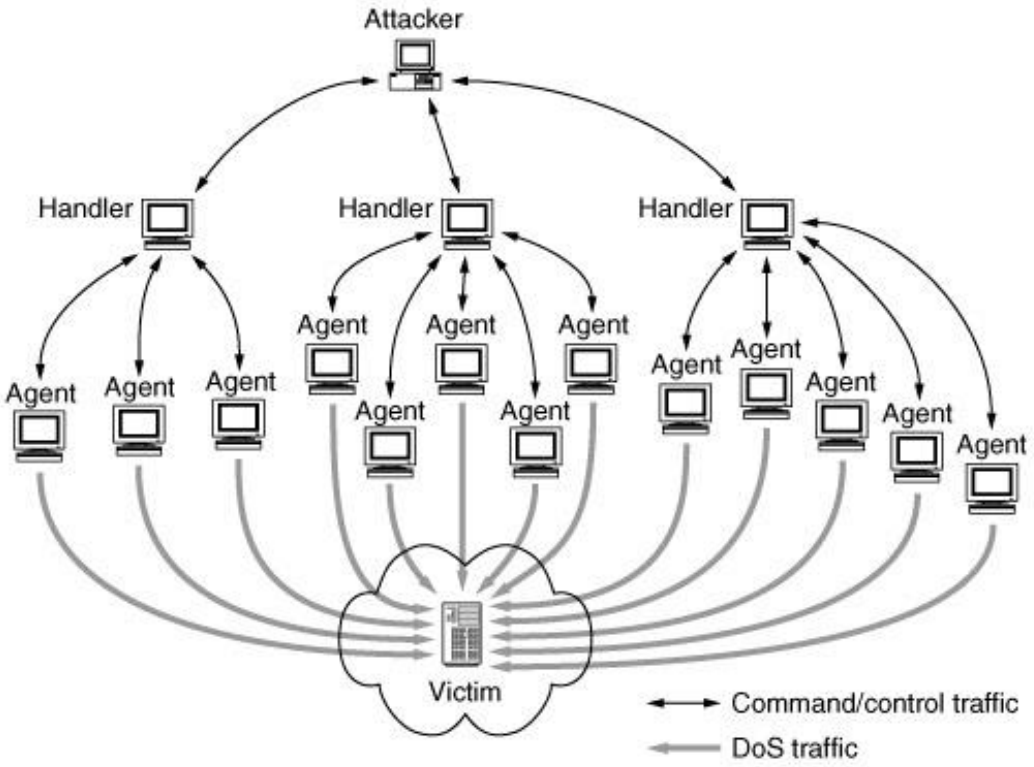

重复
CR(seq=x)
接受连接，回送确认
ACC(seq=y, ACK=x+1)
重复
Data(seq=x+1, ACK=z)
应该ACK=y，
实际ACK=z，重复！放弃！
拒绝连接，回送确认
REJECT( ACK=y)
x是重复连接请求，
放弃连接！
主机A
主机B

# 注意

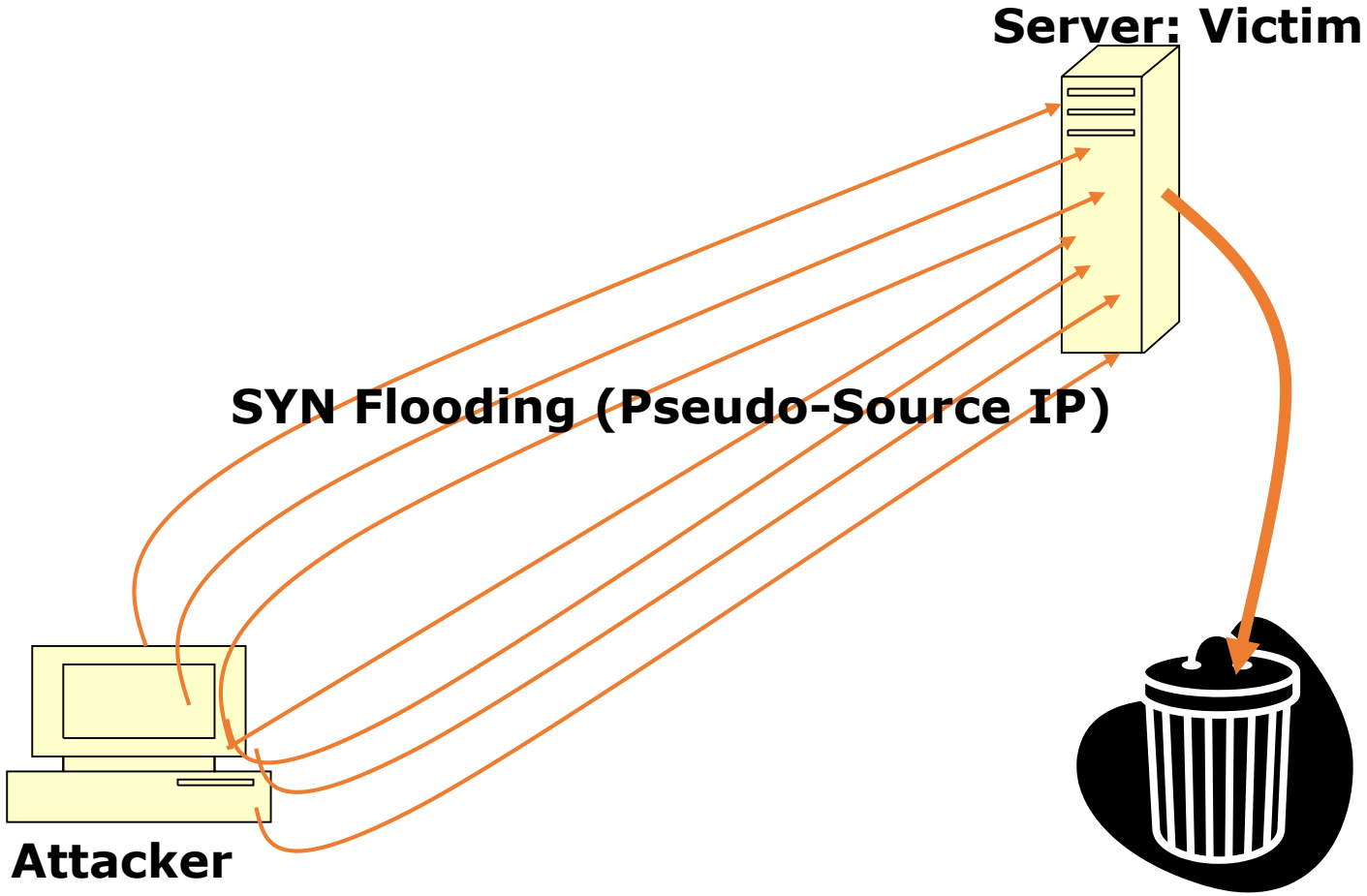
- SYN泛洪导致DoS攻击（伪造源IP）
- 数据传输开始后可能有两个原因导致阻塞
  - 快的机器向慢的机器发送数据
  - 多台机器同时向一台机器发送数据

# 拒绝服务攻击DoS

SYN Flooding can result in DoS (deny of service) attack



# 图示：SYN Flooding



# 小结

- TCP数据段传送之前，一定要建立TCP连接
- 三次握手建立TCP连接
  - 一次：SYN=1，ACK=0
  - 二次：SYN=1，ACK=1
  - 三次：SYN=0，ACK=1
- 三次握手建立连接是一个同步的过程，交换初始序列号，保证后续的每一个字节的可靠传输。

# 思考题

- TCP连接是怎样建立起来的？
- 使用2次握手来建立TCP连接可以吗？
- 为什么TCP连接建立过程又叫同步？
- SYN泛红攻击是怎样产生的？

# 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！