Assignment 2

1. Consider the following network (Shown in Figure 1) in which there are two IP tunnels set up. R1 forwards any packet destined to LAN D via the tunnel to R4. On the other hand, R2 will forward any packet destined to LAN C via the tunnel to R3.

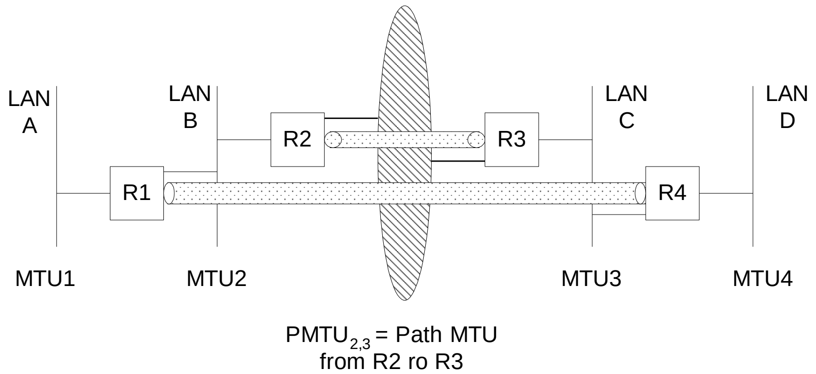


Figure 18

a) In a nested IP tunnel scenario, what is the maximum size of an IP packet that a host on LAN A can send to a host on LAN D without causing IP fragmentation? Express your answer in terms of MTU1-4 and PMTU2,3 and a *min()* function.

a> MTU = IP MTU

ip tunneling 要加 20 bytes 头部

$$\begin{cases} IP\text{-}MTU + 20 \le MTU_{1-4} \\ IP\text{-}MTU + 40 \le PMTU_{2,3} \end{cases}$$

$$\Rightarrow IP\text{-}MTU = \min(MTU_{1-4} - 20,\ PMTU_{2,3} - 40)$$

b) Consider such a case: A host on LAN A sends an IP datagram to a host on LAN D with data of 1500 bytes. Assume that MTU1 =MTU2 = MTU3 = MTU4 = PMTU2,3 = 1500 bytes.

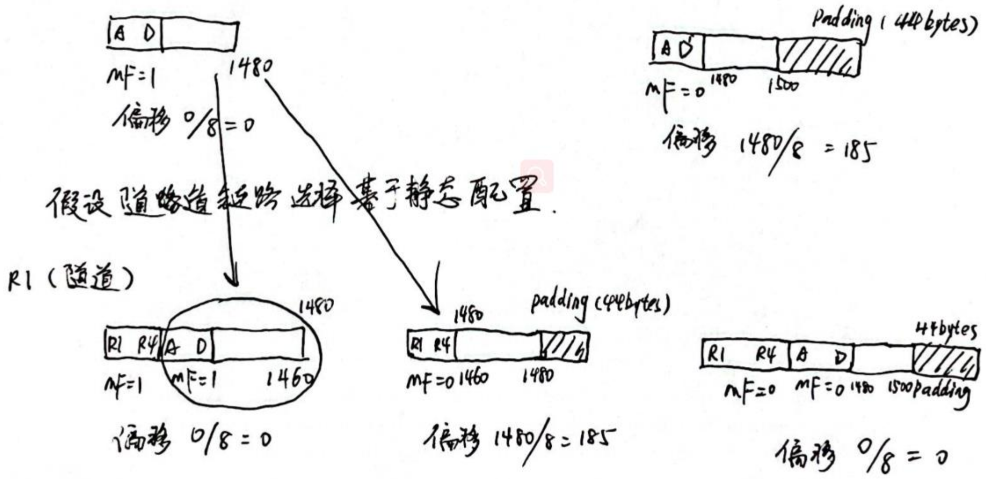
- How many IP packets (IP fragments0) are transmitted in the network between R2 and R3? Why?

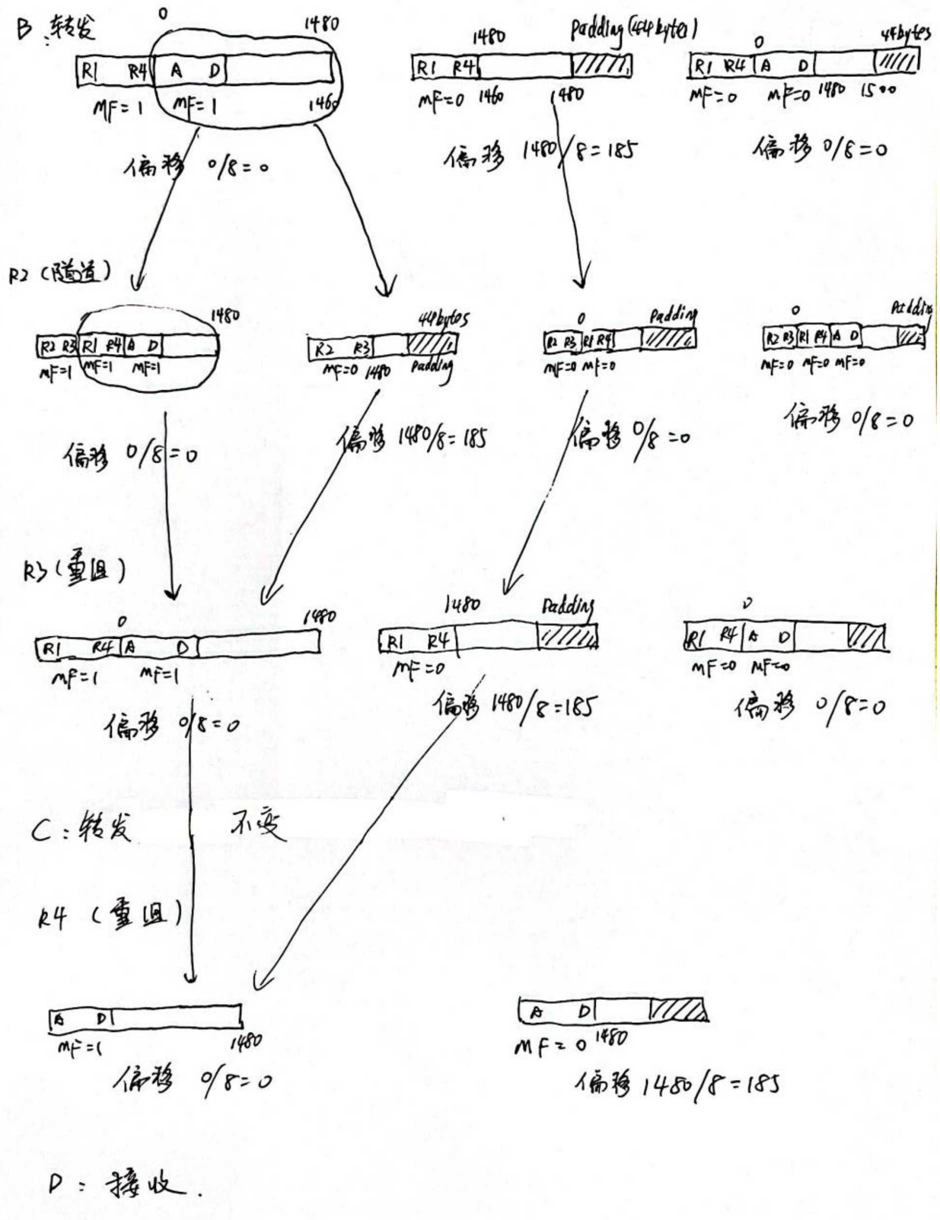
- How many IP header(s) does each fragment have?
- Please write down the FRAGMENT OFFSET and MORE flag in each IP packet.
- If the last fragment is dropped by a router somewhere between R1 and R4 due to TTL being exceeded, an ICMP error message will be sent by the router that drops the packet. Who will receive the ICMP message and why?

b) ip header 20 bytes ; data 1500 bytes

min MTU = 64 bytes

A :





当报文在 R1 和 R2 或者 R3 和 R4 之间丢失时，收到 ICMP 的是 R1，当报文在 R2 至 R3 之间丢失时，收到 ICMP 的是 R2，取决于最外层 IP header 的 source ip.

2. The Distance Vector routing algorithm suffers from the count to infinity problem. One possible solution is Split Horizon. However, it does not solve count-to-infinity in all cases. Please give us an example and explain the reasons. (Hint: consider the example in PPT, page 39).

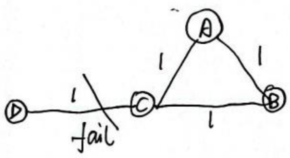
2. Split Horizon.

Never advertise the cost to a neighbor if this neighbor is the next hop on the current path.

即 若 Z的最短路径要通过邻居Y，那么它将告诉Y自己到目的节点的距离是∞.

当涉及到3个或更多节点（不仅仅是两个直接相连的neighbor）的环路时，Split Horizon 技术不能生效.

例：



当C，D 之间的连接断开，将依次发生以下事件.

A 收到来自 C 的 bad news，将选择从 B 到达 D.

A 向C 发送更新报文.

C 向 B 发送更新报文.

这里因为 A，B 无法同时接收到C的更新报文更新 距离向量，时间一定有先后，若 A先于B更新，这就使 A 错误认为可以从 B 到达 C，然后将这个错误的消息通知 C，使C也误以为可以与D相连，同理，B也收到了错误的消息. 但实际 D已经隔离了。

3. A routing protocol developer has proposed a new way of performing "load

balancing" on the network links in OSPF networks. Briefly, for each destination, an OSPF router comes up with two best routes with different next-hop routers, which do not necessarily have equal costs and forward the traffic onto these two routes proportionally. So, for example, if one route has a cost of C1 (route 1) and the other has a cost of C2 (route 2), it will forward C2/(C1+C2)% of the traffic using route 1 and the remaining traffic using route 2. However, another developer has pointed out a serious flaw in this mechanism. What is it? Use a simple example to illustrate it.

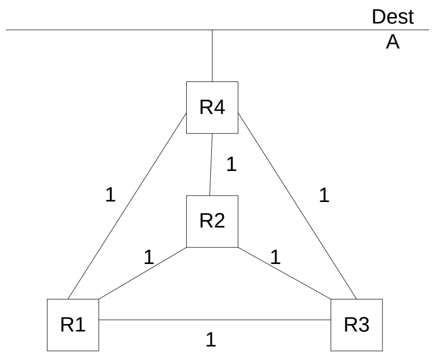


Figure 2

4. In the inter-domain topology shown in Figure 3, each node is an autonomous system (AS). Denote the set of IP addresses inside an AS X by IPx. Consider AS F. F receives some routes from each of its neighboring autonomous systems using BGP.

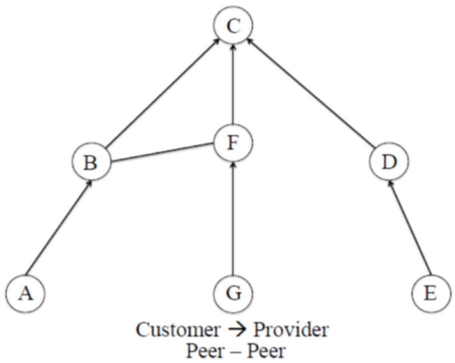


Figure 3

3. 采用这种方法，会有数据包一直在两个路由器间相互转发.

以 R1→R4 的数据包为例.

会有 $\frac{1}{3}$ 的数据流入 R2.

而这些流入 R2 的数据.

又会有 $\frac{1}{3}$ 的数据流回 R1.

从而陷入循环。

a) From each AS given below, which IP addresses (in IPx notation) do F receive advertisements?

Neighber ASs	IP addresses

a> neighbors AS	IP addresses
G	IP_G
B	IP_B IP_A
C	IP_C IP_B IP_A IP_D IP_E IP_F IP_G

b) After processing BGP advertisements received from its neighbors, F updates the routing table entries whose next-hops are routers in neighboring ASs. Then, list the IP addresses (in IPx notation) in these entries. (Hints: F's next hop is the neighboring ASs.)

Next hop	IP addresses

b). 题意是：通过 next hops，在最终的 routing table 可以到达哪些AS.

next hop	ip addresses
B	IP_B, IP_A
C	IP_C, IP_D, IP_E
G	IP_G.

5. Consider the following attack on TCP by an attacker who can observe the packets sent between a server and a client. As a result, the attacker sends only three packets to the server, as depicted in Figure 4.

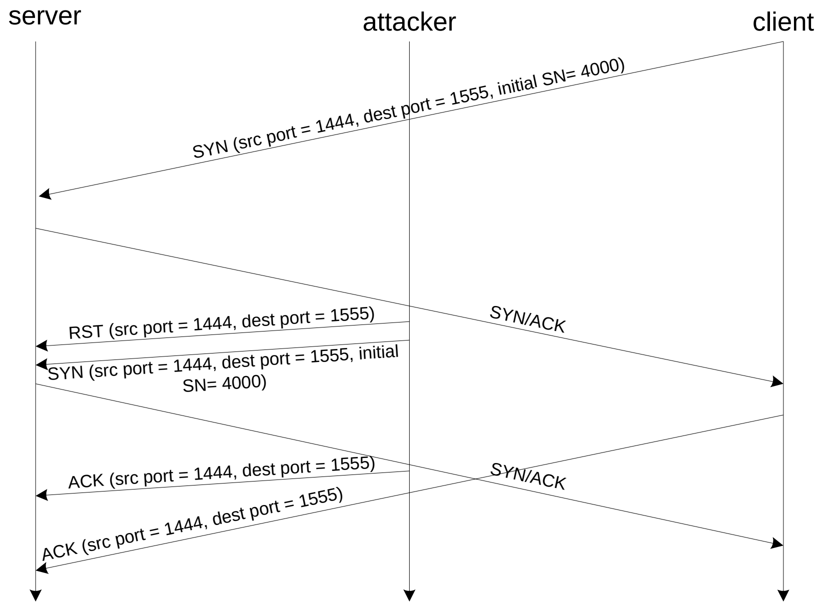


Figure 4

a) Explain the effect of this attack on the TCP connection between the server and client.

a) attacker 伪装成 client，向服务器发送一个具有 RST 位的数据段，服务器收到这样的数据后，认为client 的连接有错误，就会清空缓冲区建立好的连接。此时，attacker 再重新用相同SN与 server 建立连接，达到中间人攻击效果。

b) Explain the effect of this attack on the TCP connection if the attacker sends the second segment in such a pattern:

SYN (src port = 1444, dest port = 1555, initial SN= x), here $x \neq 4000$

b)、 $x \neq 4000$ 时

此时 server 回复的 syn/ack 为

syn (seqNo = y , AckNo = x+1) 其中 $x \neq 4000$

虽然 attacker 重新与 server 建立了连接，

但暴露给了 client，因为 ackNo 不同。

c) Given a receiver window size of 8K, what is the chance that an RST packet with a random sequence number will terminate the connection?

c)． TCP 会话的 SN 为 32 bit，用于跟踪发送的数据量。

8KB = 2^{13} Bytes.

数据包的 SN 有 2^{32} 种可能。

RST 数据包的序号要正好在接收窗口内，共 2^{13} 种可能

$$P_{terminate} = \frac{2^{13}}{2^{32}} = 1/2^{19}$$

d) How many RST packets are needed to span the sequence number space? For example, using 58-byte RST packets on a 10 Mbps link, how long does it take to generate this number of packets?

d). 覆盖接收窗口空间需至少 $\frac{2^{32}}{2^{13}} = 2^{19}$ 个 packet.

RST packet 58 bytes < 64 bytes，使用 min MTU 64 bytes.

$$\frac{2^{19} \times 64 \text{ bytes}}{10 \text{ M bps}} = 3.2s.$$