2021秋计算机网络期末习题课

TA 白欣雨、王澍民

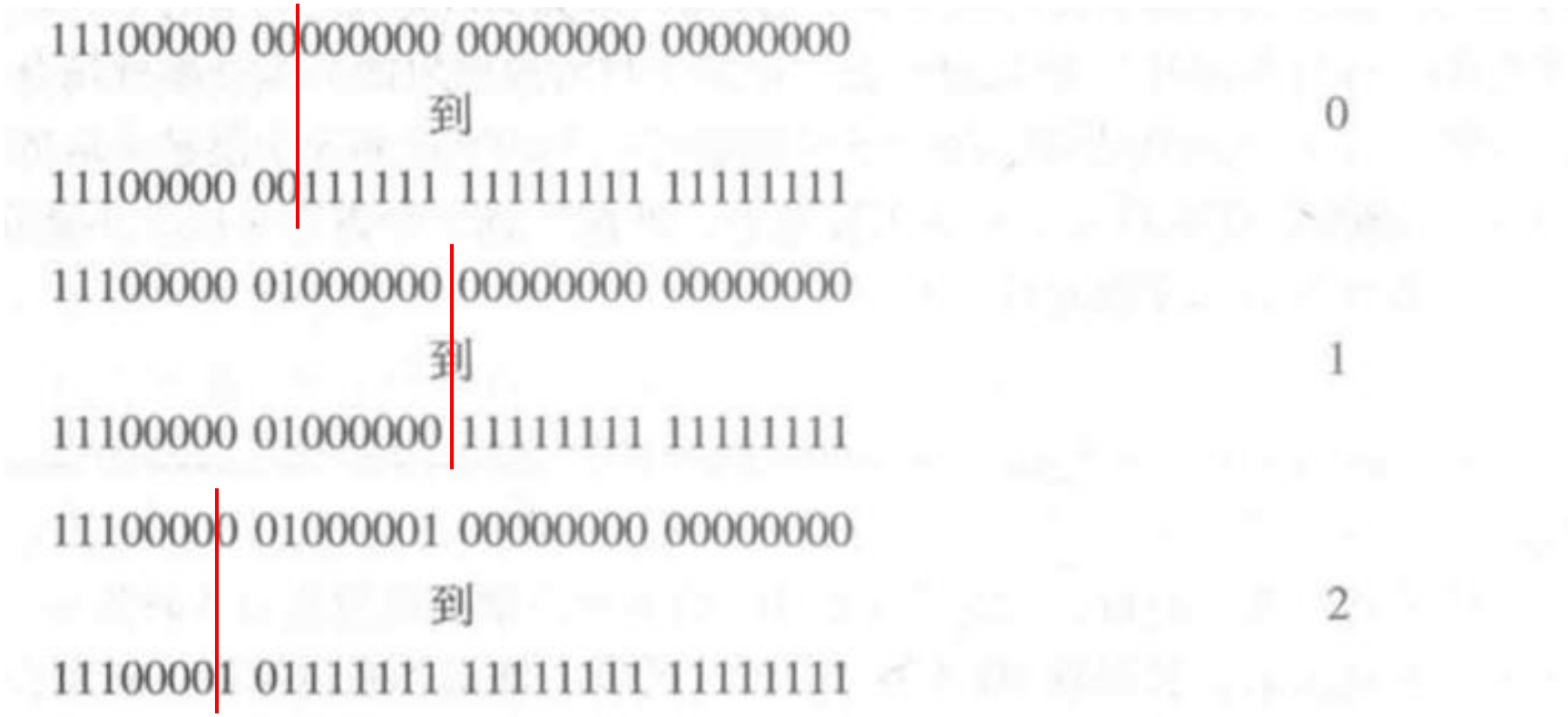
- IP地址的分配问题，子网划分
- IP协议内容
- 数据经过网络层的处理
- 其他相关协议的内容与作用

第四章习题

P5. 考虑使用32比特主机地址的某数据报网络。假定一台路由器具有4条链路，编号为0～3，分组能被转发到如下的各链路接口：

目的地址范围	链路接口
11100000 00000000 00000000 00000000 到 11100000 00111111 11111111 11111111	0
11100000 01000000 00000000 00000000 到 11100000 01000000 11111111 11111111	1
11100000 01000001 00000000 00000000 到 11100001 01111111 11111111 11111111	2
其他	3

第四章习题



- 划分最长的可能前缀，以边界IP地址的第一个不同的位置为界限。
- 检查是否会冲突。
- 题目不要求尽量不要化简，以免出错。

第四章习题

前缀匹配	链路接口
11100000 00	0
11100000 01000000	1
1110000	2
11100001 1	3
其他	3

第四章习题

P12. 考虑图 4-20 中显示的拓扑。（在 12:00 以顺时针开始）标记具有主机的 3 个子网为网络 A、B 和 C，标记没有主机的子网为网络 D、E 和 F。

a. 为这 6 个子网分配网络地址，要满足下列限制：所有地址必须从 214.97.254/23 起分配；子网 A 应当具有足够地址以支持 250 个接口；子网 B 应当具有足够地址以支持 120 个接口；子网 C 应当具有足够地址以支持 120 个接口。当然，子网 D、E 和 F 应当支持两个接口。对于每个子网，分配采用的形式是 *a.b.c.d/x* 或 *a.b.c.d/x ~ e.f.g.h/y*。

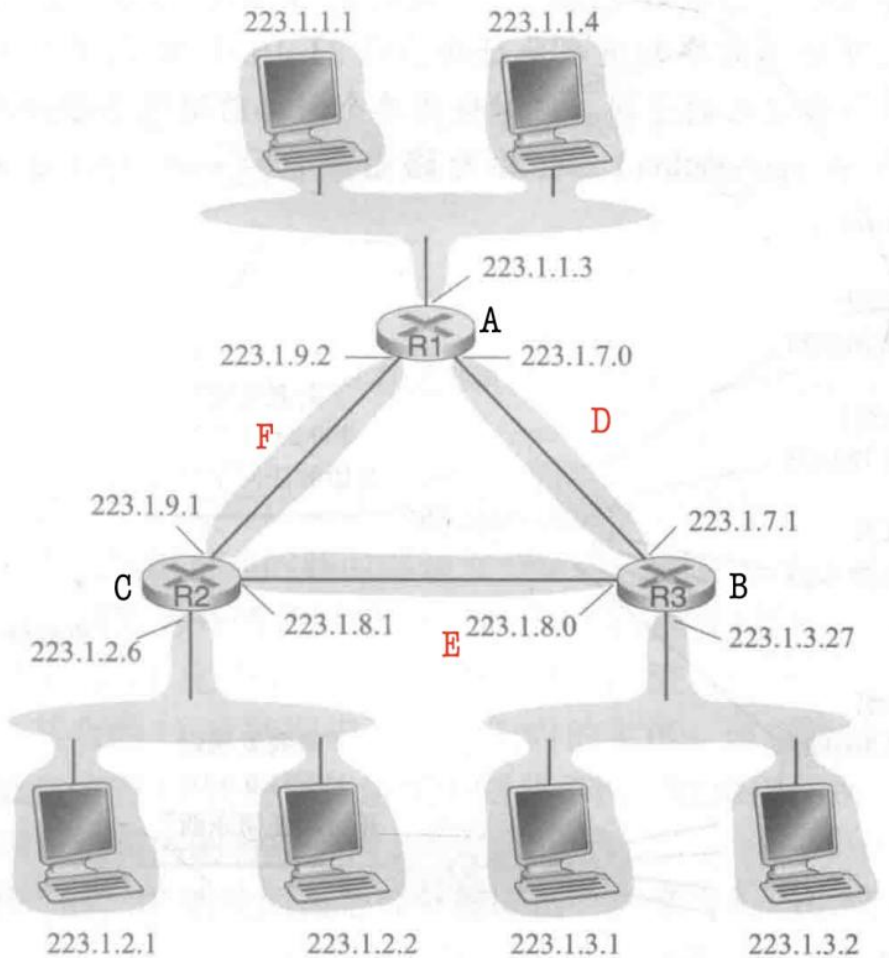
b. 使用你对（a）部分的答案，为这 3 台路由器提供转发表（使用最长前缀匹配）。

通用解法：

1. 确定子网号长度或者主机号的长度。
   - 子网数量决定子网ID的长度，从而决定了子网号的长度，子网数量 $< 2^n$，其中n为子网ID的长度。
   - 主机数量决定了主机号的长度。主机数量 $< 2^n - 2$，其中n为主机号的长度。
2. 根据子网号（网络号+子网ID）的长度确定子网掩码，然后根据子网掩码确定子网号。
3. 根据子网掩码、子网号等信息配置每个路由器上的转发表

注：某些题要注意特殊的IP地址，比如广播地址，本题未考虑

第四章习题



以R1为例

- 确定主机号长度

对于A	有$2^n \geq 250$，因此可以取n=8	子网ID长度为1
对于D	有$2^n \geq 2$，因此可以取n=1	子网ID长度为8
对于F	有$2^n \geq 2$，因此可以取n=1	子网ID长度为8

- 标准答案把F的主机号长度修改为2，这里不修改也可以。
- 确定子网号

对于A	子网ID长度为1	ID=1
对于D	子网ID长度为8	ID=00000000
对于F	子网ID长度为7	ID=0000001

- 按照第一题的方式来确定最长前缀匹配的转发表

第四章习题

A: 214.97.255/24

D: 214.97.254.0/31

F: 214.97.254.4/30

前缀匹配	链路接口
11010110 01100001 11111111	A
11010110 01100001 11111110 0000000	D
11010110 01100001 11111110 000001	F

第四章习题

P14. 考虑向具有 700 字节 MTU 的一条链路发送一个 2400 字节的数据报。假定初始数据报标有标识号 422。将会生成多少个分片？在生成相关分片的数据报中各个字段的值是多少？

- MTU=IP head + data
- 2400字节的数据报分为20字节的IP head，和2380字节的数据部分；
- 链路部分即为680字节的部分；
- 则要分2400/680=4（向上取整）个片段；
- IP头的偏移部分单位是8字节，所以该字段为680/8=85；
- 标识号表示的是若干个数据报是同一个数据报分段的结果，所以同为422。
- 标志分别为1、 1、 1、 0（表示最后一片）。

第四章补充习题（概念）

1. 下列关于 IP 路由器功能的描述中，正确的是（　）。

I. 运行路由协议，设置路由表

II. 监测到拥塞时，合理丢弃 IP 分组

III. 对收到的 IP 分组头进行差错校验，确保传输的 IP 分组不丢失

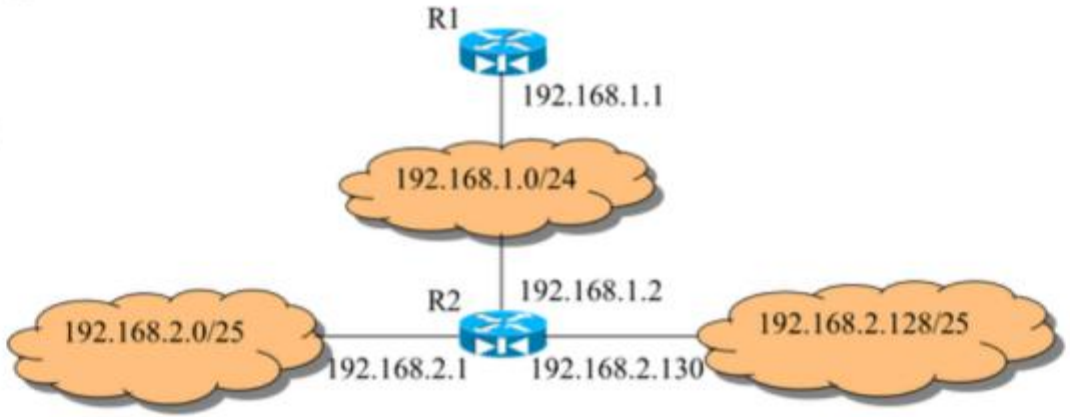
IV. 根据收到的 IP 分组的目的 IP 地址，将其转发到合适的输出线路上

(A) 仅 III、IV　　(B) 仅 I、II、III　　(C) 仅 I、II、IV　　(D) I、II、III、IV

- 路由器的两个功能：路由与转发，所以1和4正确；
- 当路由器监测到拥塞时，会丢弃 IP 分组，并向发出该 IP 分组的源主机发送一个源点抑制的 ICMP 报文，所以2正确；
- 路由器对收到的 IP 分组首部进行差错检验，丢弃有差错首部的报文，但无法保证 IP 分组不丢失，所以3错误。

补充习题（子网）

13. 某网络拓扑如图 1 所示，路由器 R1 只有到达子网 192.168.1.0/24 的路由。为使 R1 可以将 IP 分组正确地路由到图中的所有子网，则在 R1 中需要增加的一条路由（目的网络，子网掩码，下一跳）是（）。



- 需要有到 192.168.2.0/25 和 192.168.2.128/25的路由，写到一个表项内，所以将二者聚合
- IP地址的前 24 位都是相同的，可以聚合成超网 192.168.2.0/24
- 子网掩码为 255.255.255.0
- 路由的下一跳是与 R1 直接相连的 R2 的地址：192.168.1.2

(D) 192.168.2.0　　255.255.255.0　　192.168.1.2

补充习题（其他协议综合）

16. 某校园网有两个局域网，通过路由器 R1、R2 和 R3 互联后接入 Internet，S1 和 S2 为以太网交换机。局域网采用静态 IP 地址配置，路由器部分接口以及各主机的 IP 地址如图 4 所示。

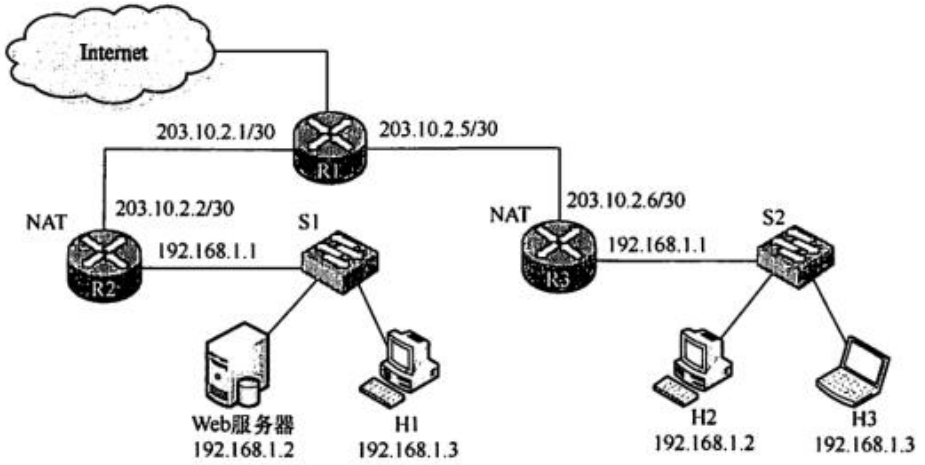


图 4: 第 4 章第 16 题图

假设 NAT 转换表结构为

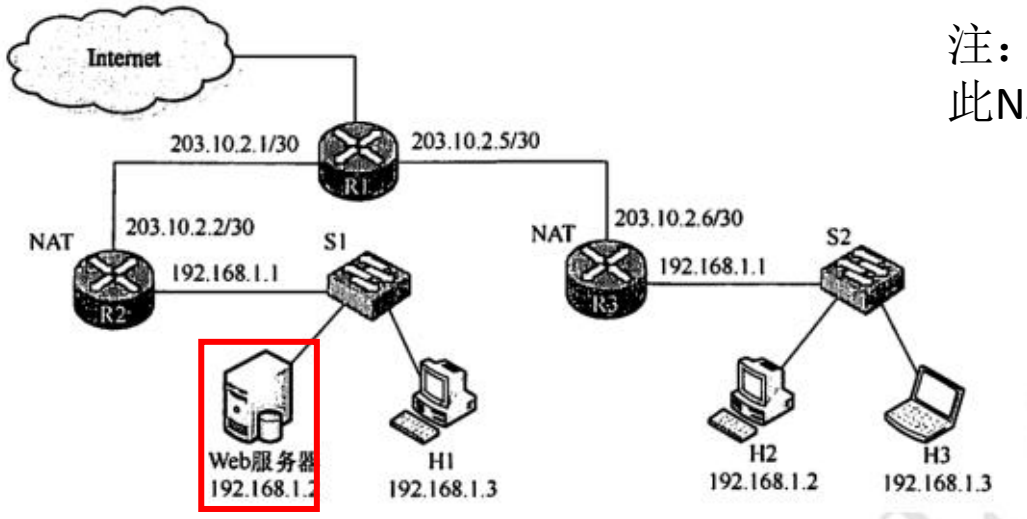
外网		内网	
IP 地址	端口号	IP 地址	端口号

请回答下列问题：

(1) 为使 H2 和 H3 能够访问 Web 服务器 (使用默认端口号)，需要进行什么配置?

(2) 若 H2 主动访问 Web 服务器时，将 HTTP 请求报文封装到 IP 数据报 P 中发送，则 H2 发送的 P 的源 IP 地址和目的 IP 地址分别是什么？经过 R3 转发后，P 的源 IP 地址和目的 IP 地址分别是什么？经过 R2 转发后，P 的源 IP 地址和目的 IP 地址分别是什么？

补充习题（子网）



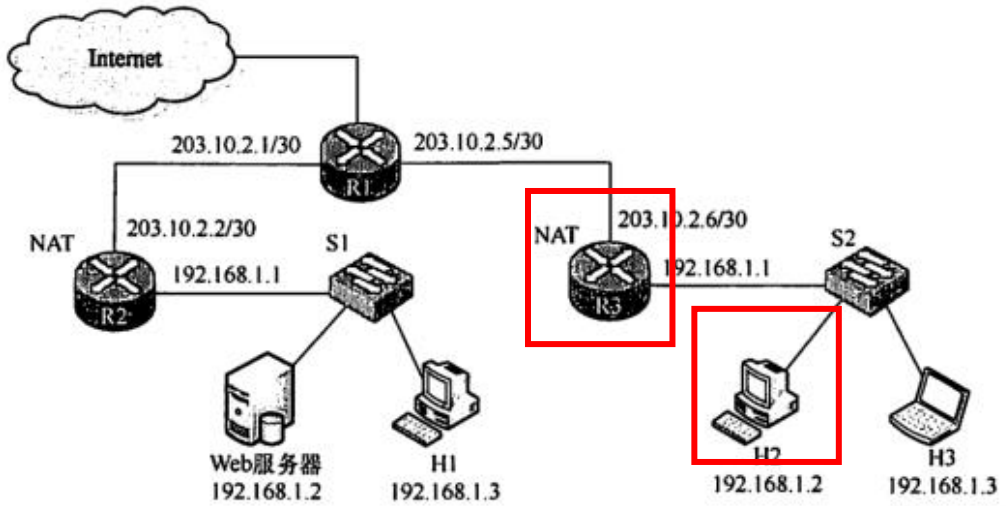
注：NAT转发表是{IP:端口}的映射，因此NAT路由在转发时可以看到端口号。

- 两个子网使用了相同的网段，且路由器开启了 NAT 功能，因此需要配置 NAT 表。
- 路由器 R2 开启 NAT 服务，当路由器 R2 从 WAN 口收到来自 H2 或 H3 发来的数据时，根据 NAT 表发送给 Web 服务器的对应端口。
- 外网 IP 地址应该为路由器的外端 IP地址。内网 IP 地址应该为 Web 服务器的地址， Web 服务器默认端口为 80，因此内网端口号固定为 80，当其他网络的主机访问 Web 服务器时，默认访问的端口应该也是 80，但是访问的目的IP 是路由器的 IP 地址，因此 NAT 表中的外部端口最好也统一为 80。
- R2 的 NAT 表配置如下：

外网		内网	
IP 地址	端口号	IP 地址	端口号
203.10.2.2	80	192.168.1.2	80

补充习题（子网）

(2) 若 H2 主动访问 Web 服务器时，将 HTTP 请求报文封装到 IP 数据报 P 中发送，则 H2 发送的 P 的源 IP 地址和目的 IP 地址分别是什么？经过 R3 转发后，P 的源 IP 地址和目的 IP 地址分别是什么？经过 R2 转发后，P 的源 IP 地址和目的 IP 地址分别是什么？

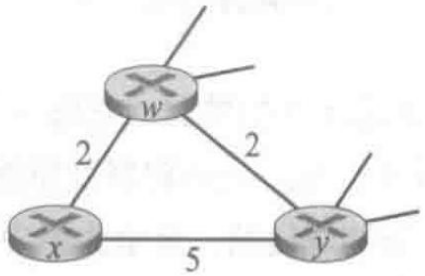


- 启用了 NAT 服务， H2 发送的 P 的源 IP 地址应该是 H2 的内网地址，目的地址应该是 R2 的外网 IP 地址，因此源 IP 地址是 192.168.1.2，目的 IP 地址是 203.10.2.2。
- R3 转发后，将 P 的源IP 地址改为 R3 的外网 IP 地址，目的 IP 地址仍然不变，源 IP 地址是 203.10.2.6，目的 IP 地址是 203.10.2.2。
- R2 转发后，将 P 的目的 IP 地址改为 Web 服务器的内网地址，源地址仍然不变，源 IP 地址是 203.10.2.6，目的 IP 地址
- 注：内网的IP地址对其他的内网不可见

- 路由选择算法
- ICMP 协议

第五章习题

P7. 考虑下图所示的网络段。x 只有两个相连邻居 w 与 y。w 有一条通向目的地 u（没有显示）的最低开销路径，其值为 5，y 有一条通向目的地 u 的最低开销路径，其值为 6。从 w 与 y 到 u（以及 w 与 y 之间）的完整路径未显示出来。网络中所有链路开销皆为正整数值。

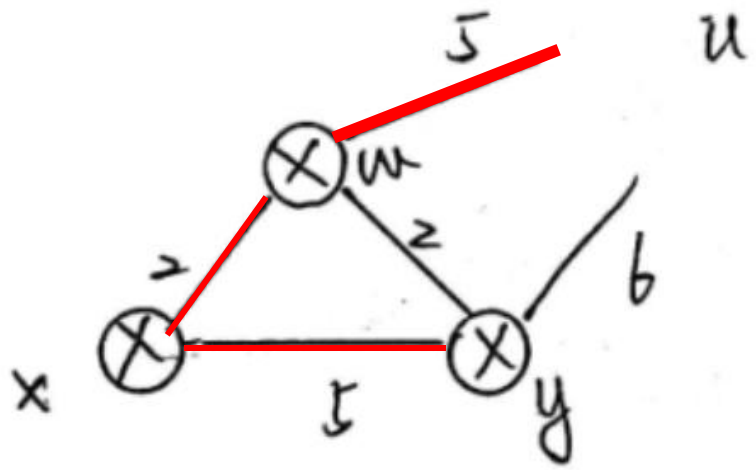


a. 给出 x 对目的地 w、y 和 u 的距离向量。

b. 给出对于 $c(x, w)$ 或 $c(x, y)$ 的链路开销的变化，使得执行了距离向量算法后，x 将通知其邻居有一条通向 u 的新最低开销路径。

c. 给出对 $c(x, w)$ 或 $c(x, y)$ 的链路开销的变化，使得执行了距离向量算法后，x 将不通知其邻居有一条通向 x 的新最低开销路径。

第五章习题



1. 从相邻的 X 路由器接收发送过来的 RIP（Routing Information Protocol） 报文
2. 将该 RIP 报文中的下一跳地址修改为 X，且跳数增加 1
3. 对每个项目执行如下步骤
   a.若原路由表没有 RIP 中的目的网络 N，**直接添加到原路由表中**
   b.若原路由表中有 RIP 中的目的网络 N，但下一跳地址不是 X，**选择跳数少的替换**。如果两者跳数一样，则保留原路由表的项。
   c.若原路由表中有 RIP 中的目的网络 N，且下一跳地址是 X，**使用收到的项替换**
4. 若超过 180s （RIP 默认 180s）还没有收到相邻路由器的更新路由表，则相邻路由器**置为不可达**，跳数为 16

- 最低开销路径改变$(x \to w \to u) \to (x \to y \to u)$

$$c(x,w)+5 > c(x,y)+6$$

$c(x,y)$不变时，$c(x,w) > c(x,y)+6-5=6$

即$c(x,w) > 6$时，路径改变，从$(x \to w \to u)$到$(x \to y \to u)$

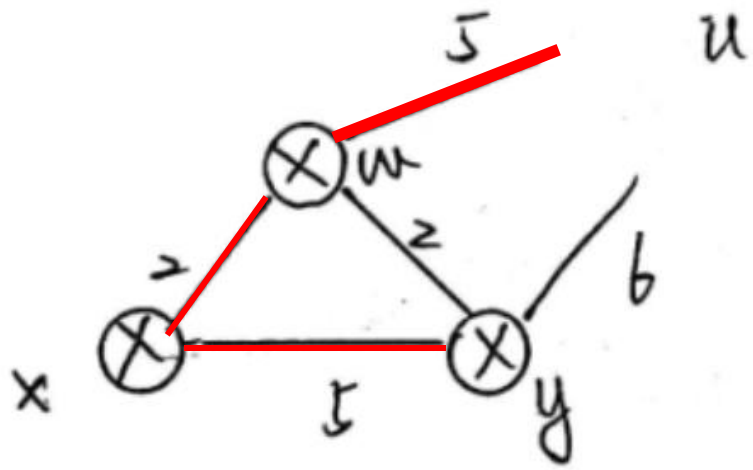
当$c(x,w) \le 6$时，虽然路径不变，但最低开销变化，会通知邻居。

$c(x,w)$不变时，$c(x,y) < c(x,w)+5-6=1$

但是不符合题目的要求，舍去。

即$c(x,y) \ge 1$下的所有变化均不会导致改变，不会通知。

第五章习题



1. 从相邻的 X 路由器接收发送过来的 RIP（Routing Information Protocol） 报文
2. 将该 RIP 报文中的下一跳地址修改为 X，且跳数增加 1
3. 对每个项目执行如下步骤
   a.若原路由表没有 RIP 中的目的网络 N，**直接添加到原路由表中**
   b.若原路由表中有 RIP 中的目的网络 N，但下一跳地址不是 X，**选择跳数少的替换**。如果两者跳数一样，则保留原路由表的项。
   c.若原路由表中有 RIP 中的目的网络 N，且下一跳地址是 X，**使用收到的项替换**
4. 若超过 180s （RIP 默认 180s）还没有收到相邻路由器的更新路由表，则相邻路由器**置为不可达**，跳数为 16

- 最低开销路径不变（仍然为$x \to w \to u$）

$$c(x,w)+5 \le c(x,y)+6$$

$c(x,y)$不变，$c(x,w) \le 6$时，路径仍为$x \to w \to u$，但若开销变化会通知。

$c(x,w)$不变，$c(x,y) \ge 1$时，路径不改变，不会通知。

第五章习题

P14. 考虑下图所示的网络。假定 AS3 和 AS2 正在运行 OSPF 作为其 AS 内部路由选择协议。假定 AS1 和 AS4 正在运行 RIP 作为其 AS 内部路由选择协议。假定 AS 间路由选择协议使用的是 eBGP 和 iBGP。假定最初在 AS2 和 AS4 之间不存在物理链路。

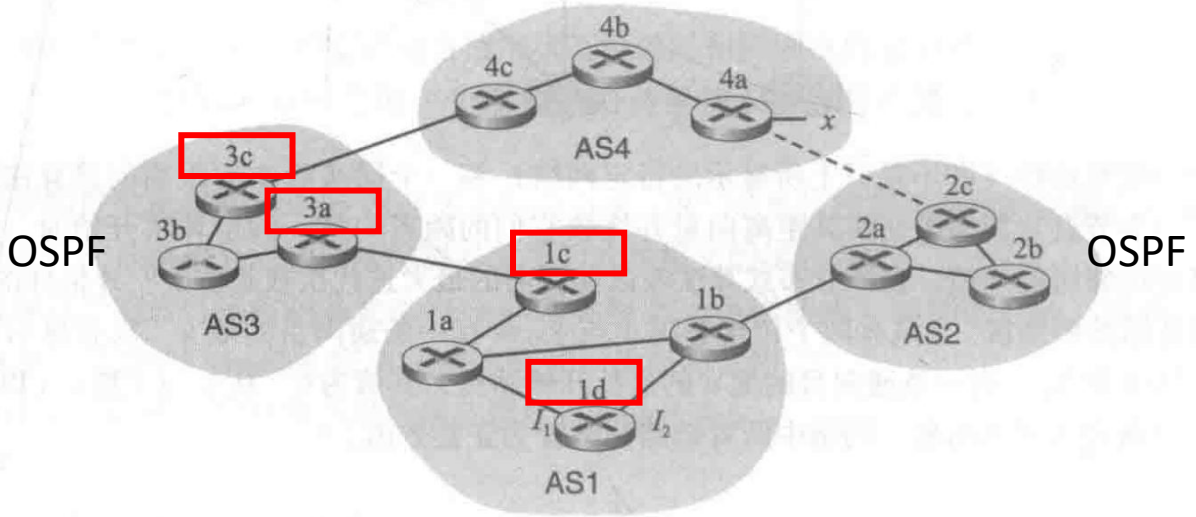
a. 路由器 3c 从下列哪个路由选择协议学习到了前缀 x：OSPF、RIP、eBGP 或 iBGP?

b. 路由器 3a 从哪个路由选择协议学习到了前缀 x?

c. 路由器 1c 从哪个路由选择协议学习到了前缀 x?

d. 路由器 1d 从哪个路由选择协议学习到了前缀 x?

大规模私有网络iBGP，互联网eBGP。

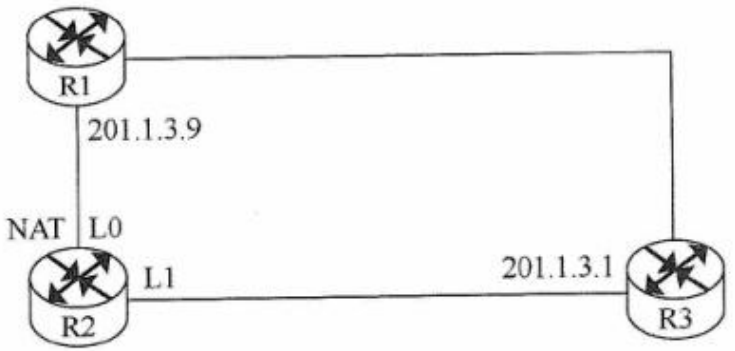


- 3c 从路由器 4c 处学习到前缀 x，所以是eBGP。
- 3a 从路由器 3c 处学习到前缀 x，所以是iBGP。
- 1c 从路由器 3a 处学习到前缀 x，所以是eBGP。
- 1d 从路由器 1c 处学习到前缀 x，所以是iBGP。

第五章补充习题（RIP）

2. 假设图 6 中的 R1、R2、R3 采用 RIP 交换路由信息，且均已收敛。若 R3 检测到网络 201.1.2.0/25 不可达，并向 R2 通告一次新的距离向量，则 R2 更新后，其到达该网络的距离是（ ）。

(A) 2　　(B) 3　　(C) 16　　(D) 17　　跳数



- R3 检测到网络 202.1.2.0/25 不可达，因此将到该网络的距离设置为 16 (表示不可达)
- 当 R2 从 R3 收到路由信息时，因为 R3 到该网络的距离为 16，则 R2 到该网络也不可达
- 但此时记录 R1 可达 (由于 RIP 的特点是“坏消息传得慢”， R1 并未收到 R3 发来的路由信息)， R1 到该网络的距离为 2，再加上从 R2 到 R1 的距离的 1， 所以最终距离为3

第五章补充习题（ICMP）

5. 若路由器 R 因为拥塞丢弃 IP 分组，则此时 R 可向发出该 IP 分组的源主机发送的 ICMP 报文类型是（　）。

(A) 路由重定向　　(B) 目的不可达　　(C) 源点抑制　　(D) 超时

- 源点抑制是指在路由器或主机由于拥塞而丢弃数据报时，向源点发送源点抑制报文，使源点知道应当把数据报的发送速率变慢。

五类差错报告：

1）终点不可达。当路由器或主机不能交付数据报时，就向源点发送终点不可达报文。

2）源点抑制。当路由器或主机由于拥塞而丢弃数据报时，就向源点发送源点抑制报文，使源点知道应当把数据报的发送速率放慢。

3）时间超过。当路由器收到生存时间（TTL）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）。

第六章

P5

考虑5比特生成多项式，G=10011，并假设D的值为1010101010。R的值是什么？

循环冗余校验（CRC）

- CRC是一种多项式编码，它将一个位串看成是某个一元多项式的系数，如1011看成是一元多项式$X^3 + X + 1$的系数
- 信息多项式M(x)：由m个信息比特为系数构成的多项式
- 冗余多项式R(x)：由r个冗余比特为系数构成的多项式
- 码多项式T(x)：在m个信息比特后加上r个冗余比特构成的码字所对应的多项式，表达式为$T(x) = x^r \cdot M(x) + R(x)$
- 生成多项式G(x)：双方确定用来计算R(x)的一个多项式
- 编码方法：$R(x) = x^r \cdot M(x) \div G(x)$ 的余式（减法运算定义为异或操作）
- 检验方法：若$T(x) \div G(x)$的余式为0，判定传输正确
- CRC码检错能力极强，可用硬件实现，是链路层上应用最广泛的检错码

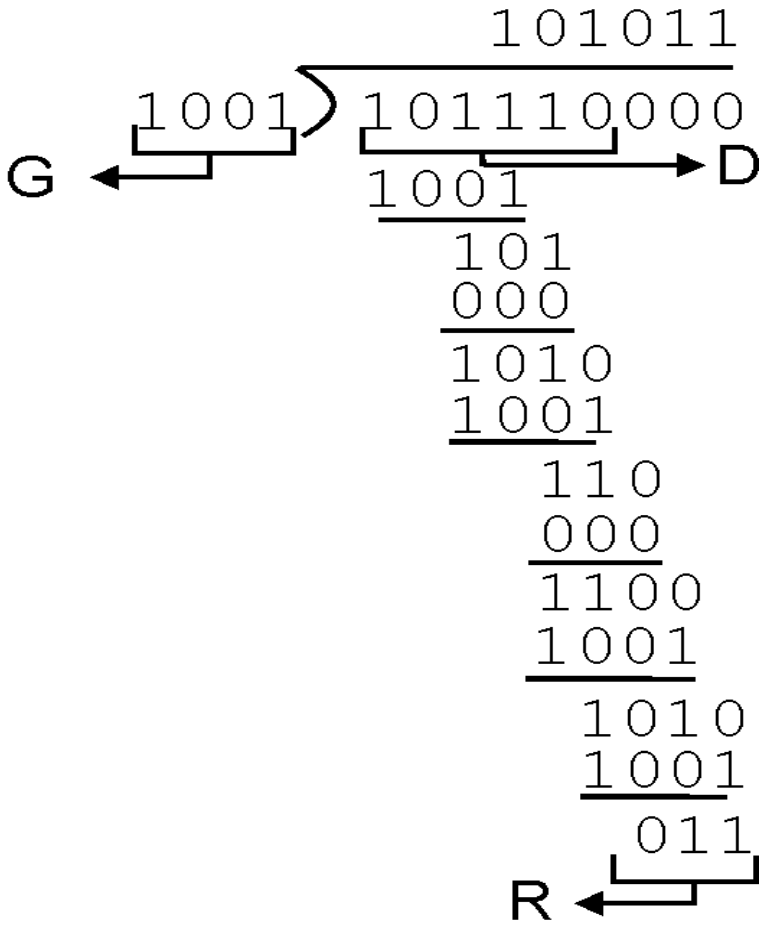
CRC举例

例1：取$G(X) = X^3 + 1$，对信息比特101110计算CRC码。

解答：

- 101110000 ÷ 1001的余式为R=011 (CRC code)
- 码字：101110011

- 注意补0位数：G的位数-1
- 模2运算：按位异或XOR



P5

考虑5比特生成多项式，G=10011，并假设D的值为1010101010。R的值是什么？

1010101010 后加上 4 个 0 进行模 2 除法，得到 10 1101 1100，余数 R = 0100。

P23-P25

P23. 考虑图 6-15。假定所有链路都是 100Mbps。在该网络中的 9 台主机和两台服务器之间，能够取得的最大总聚合吞吐量是多少？你能够假设任何主机或服务器能够向任何其他主机或服务器发送分组。为什么？

P24. 假定在图 6-15 中的 3 台连接各系的交换机用集线器来代替。所有链路是 100Mbps。现在回答习题 P23 中提出的问题。

P25. 假定在图 6-15 中的所有交换机用集线器来代替。所有链路是 100Mbps。现在回答在习题 P23 中提出的问题。

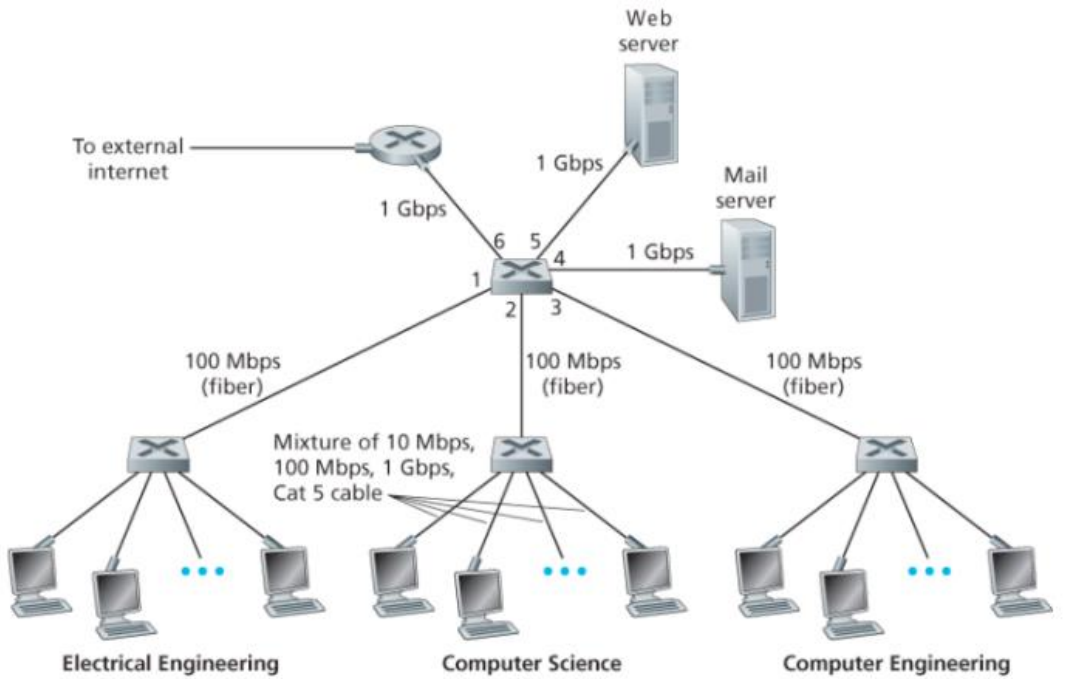
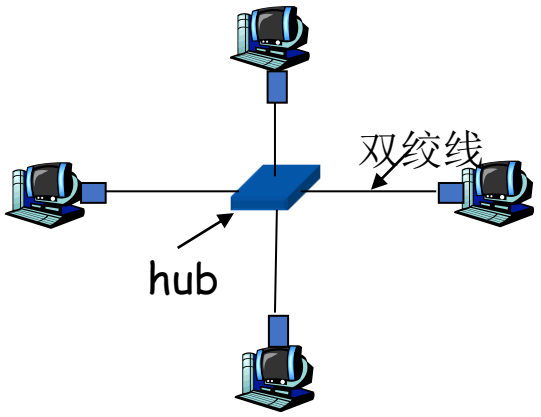


Figure 6.15 An institutional network connected together by four switches

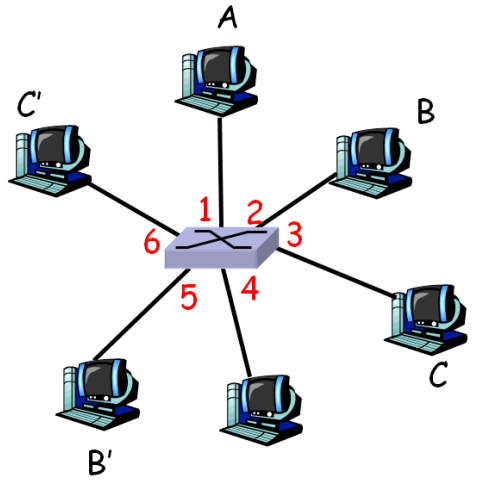
- 冲突域：在以太网中，如果某个 CSMA/CD 网络上的两台计算机在同时通信时会发生冲突，那么这个 CSMA/CD 网络就是一个冲突域。冲突域是在同一个网络上两个比特同时进行传输则会产生冲突;
- 集线器：将接受到的数据以广播的形式发出，它的所有端口为一个冲突域
- 交换机：可以利用物理地址进行选路，可以避免冲突

讨论：共享式以太网和交换式以太网

- 共享式以太网：
  - 集线器的所有端口位于同一个冲突域
  - 任一时刻最多只允许一个主机发送
  - 网络规模（节点数量）与网络性能的矛盾无法解决



- 交换式以太网：
  - 交换机的每个端口为一个冲突域
  - 多对端口可以同时通信
  - 网络的集合带宽=各个端口的带宽之和
  - 从根本上解决了网络规模与网络性能的矛盾



P23

P23. 考虑图 6-15。假定所有链路都是 100Mbps。在该网络中的 9 台主机和两台服务器之间，能够取得的最大总聚合吞吐量是多少？你能够假设任何主机或服务器能够向任何其他主机或服务器发送分组。为什么？

1100Mbps。因为题目假设所有链路都是 100Mbps 并且任意两个端系统都可以发送数据，所以在本地 9 台主机和 2 台服务器共 11 条链路全部满速状态下，总聚合吞吐量可以达到 1100Mbps。

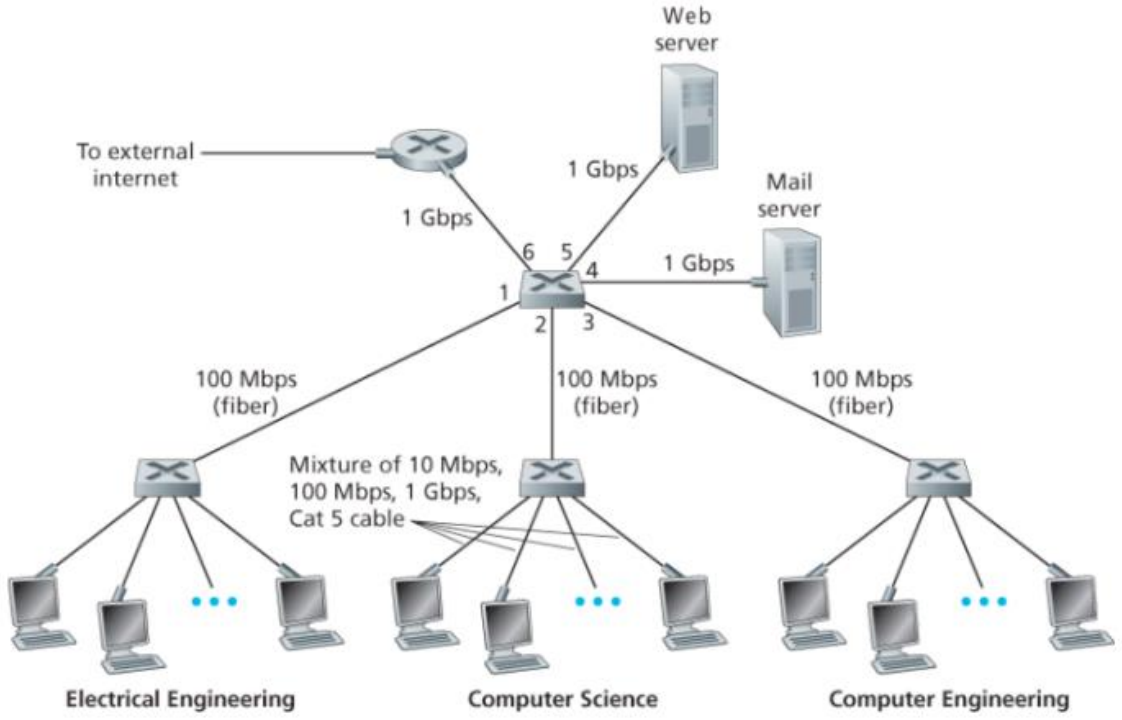


Figure 6.15 An institutional network connected together by four switches

P24

P24. 假定在图 6-15 中的 3 台连接各系的交换机用集线器来代替。所有链路是 100Mbps。现在回答习题 P23 中提出的问题。

500Mbps。因为题目假设把链接部门的交换机改成集线器，这时候各部门的电脑就处在一个冲突域之中（集线器将 收到的数据以广播形式发送，不能同时传输多台设备的数据）只能共享一条 100 Mbps 的带宽，所以任意时刻总共只能有 3 个部门和 2 台服务 器共 5 条链路可以满速运行，总聚合吞吐量 500Mbps .

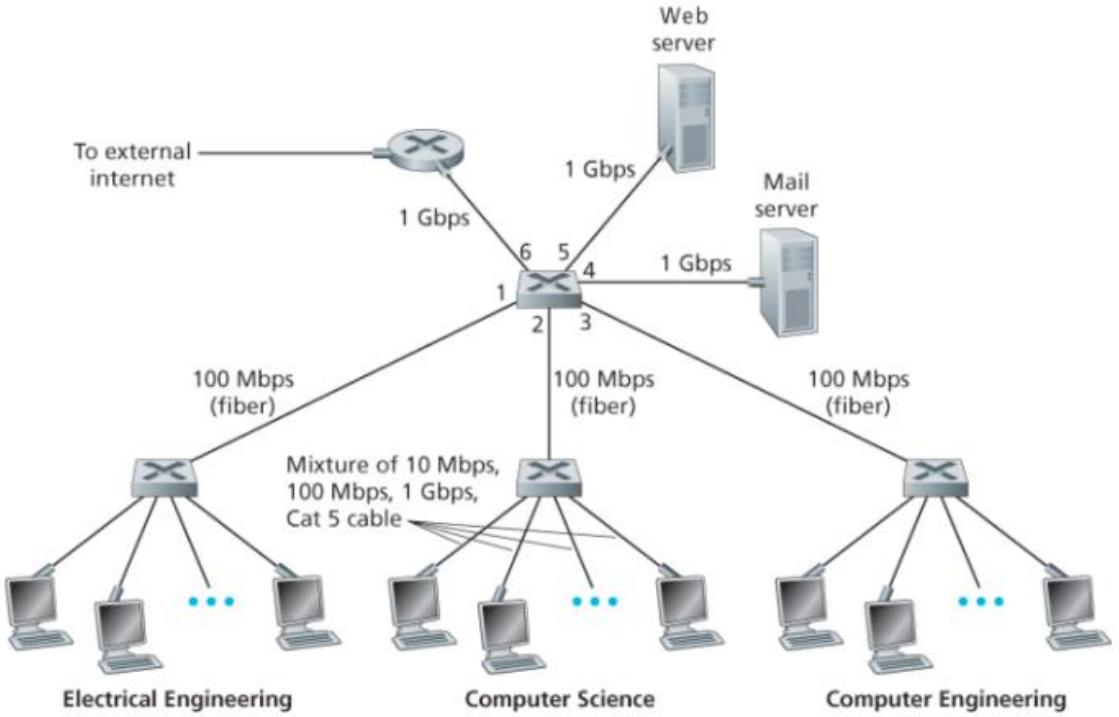


Figure 6.15 An institutional network connected together by four switches

P25

P25. 假定在图 6-15 中的所有交换机用集线器来代替。所有链路是 100Mbps。现在回答在习题 P23 中提出的问题。

100Mbps。所有 11 台端系统全部包含在一个冲突域中，任意时刻都只能有一台设备跑满 100Mbps 的带宽，所以总 聚合吞吐量就是 100Mbps。

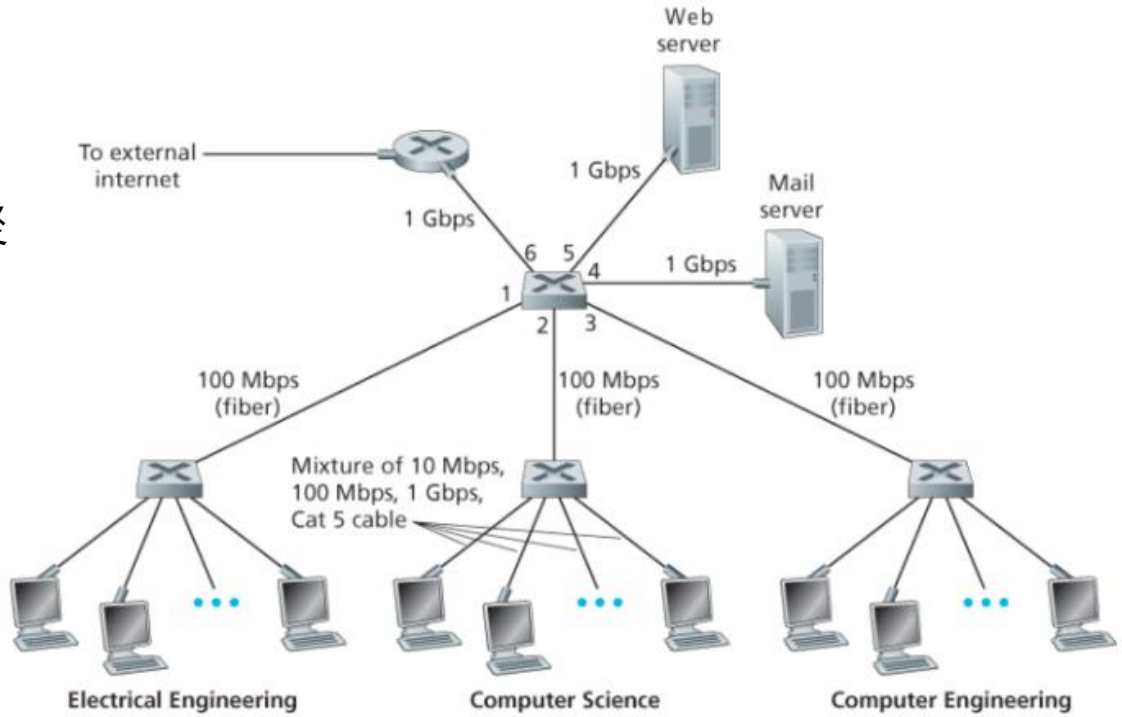


Figure 6.15 An institutional network connected together by four switches

P26

P26. 在某网络中标识为 A 到 F 的 6 个节点以星形与一台交换机连接，考虑在该网络环境中某个正在学习的交换机的运行情况。假定：（i）B 向 E 发送一个帧；（ii）E 向 B 回答一个帧；（iii）A 向 B 发送一个帧；（iv）B 向 A 回答一个帧。该交换机表初始为空。显示在这些事件的前后该交换机表的状态。对于每个事件，指出在其上面转发传输的帧的链路，并简要地评价你的答案。

交换机收到帧的处理过程

- 用帧的目的地址查找转发表（转发决策）：
  - 若目的地址所在端口 = 帧的进入端口，丢弃帧
  - 若目的地址所在端口 ≠ 帧的进入端口，转发帧
  - 若目的地址不在转发表中，扩散帧
- 用帧的源地址查找转发表（更新转发表）：
  - 若找到地址，更新相应表项
  - 若没有找到该地址，添加源地址和进入端口到转发表，设置表项的生存期为最大值

P26

动作	交换机表转发后状态	转发帧的链路	justify 解释（中文版错误翻译为评价）
B-->E	学习 B 的 MAC 地址对应的端口	A, C, D, E, F	交换机表为空，交换机一开始并不知道 B、E 的MAC地址对应的端口，所以记录 B 的 MAC 地址对应端口并直接把收到的数据广播
E-->re-->B	学习 E 的 MAC 地址对应的端口	B	交换机并不知道 E 的MAC地址对应的端口，所以记录 E 的 MAC 地址对应端口并直接转发数据给 B
A-->B	学习 A 的 MAC 地址对应的端口	B	交换机一开始并不知道 A 的MAC地址对应的端口，所以记录 A 的 MAC 地址对应端口并直接转发数据给 B
B-->re-->A	维持原样	A	交换机已经知道 A 的MAC地址对应的端口，直接转发给 A 即可

第七章

R7

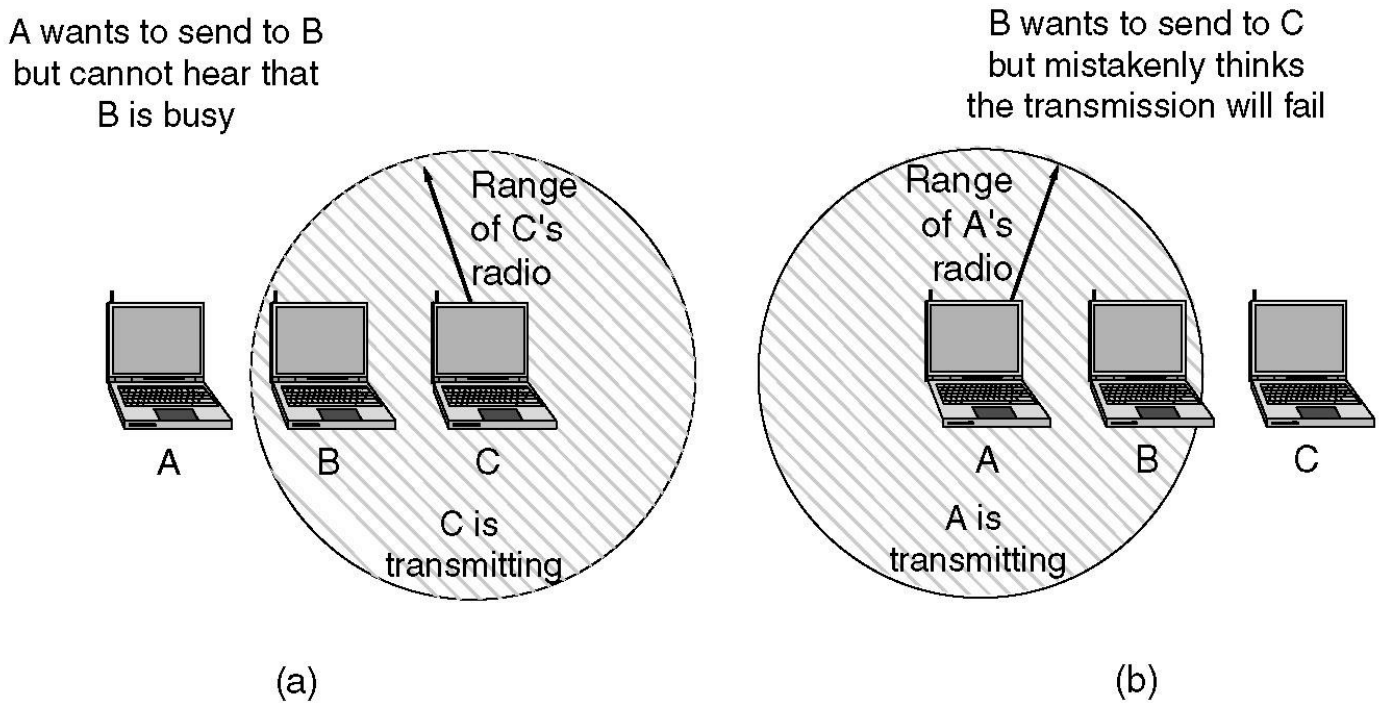
R7. 为什么 802.11 中使用了确认，而有线以太网中却未使用？

无线链路的特性

- 信号衰减: 信号在传播过程中能量逐渐减少（路径损耗）
- 干扰: 受到其它信号源的干扰
- 多径传播: 由于地面或物体的反射作用，信号沿多条不同长度的路径到达接收端

- 以上特性导致无线链路的传输距离受限、误码率很高

无线网络的特性



(a) 隐藏节点问题:

- C正在向B发送
- A监听到信道空闲，A向B发送
- A和C的信号在B冲突

(b) 暴露节点问题:

- B准备向C发送
- B监听到信道忙（A在发送）
- B不发送，但其实B可以发送（A和B的信号不会在C冲突）

CSMA在多跳无线网络中作用受限

- 通过载波侦听，发送节点只能知道其周围是否有节点在发送；但真正影响此次通信的是接收节点周围是否有节点在发送
- 隐藏节点：不在发送节点的通信范围内、但在接收节点通信范围内的活跃节点（发送节点听不到，但影响接收）
- 暴露节点：在发送节点的通信范围内、但不在接收节点通信范围内的活跃节点（发送节点能听到，但不影响接收）

——使用CSMA/CA而非CSMA/CD

R7

R7. 为什么 802.11 中使用了确认，而有线以太网中却未使用？

因为有线以太网使用CSMA/CD进行碰撞检测，在发生碰撞时发送方知情。而802.11使用CSMA/CA进行 碰撞避免，在发生碰撞时发送方不知情，因此需要通过确认信号来判断。

要点：落实到直接关联的协议上、两方都要答到

P6

P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（如果侦听到该信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢？

不使用信道预约机制的CSMA/CA

- 当节点有帧要发送时，侦听信道：
  1）若一开始就侦听到信道空闲，等待DIFS时间后发送帧
  2）否则，选取一个随机回退值，在侦听到信道空闲时递减该值；在此过程中若侦听到信道忙，冻结计数值
  3）当计数值减为0时，发送整个帧并等待确认
  4）若收到确认帧，表明帧发送成功，若还有新的帧要发送，从第2步开始CSMA/CA；若未收到确认，重新进入第2步中的回退阶段，并从一个更大的范围内选取随机回退值
- 可见，如果有k个节点等待发送，它们随机选取的回退值确定了它们的发送顺序

CSMA/CA与CSMA/CD的不同

- CSMA/CA与CSMA/CD最主要的不同：
  - CSMA/CD在发送过程中检测冲突，不使用确认机制
  - CSMA/CA在发送过程中不检测冲突，使用确认机制

- 由此带来的协议处理方面的不同：
  - 在CSMA/CD中，节点侦听到信道空闲时立即发送（不怕冲突，冲突后立即停发，损失不大）
  - 在CSMA/CA中，节点侦听到信道空闲后随机回退（冲突对无线网络损害很大，要尽量避免冲突）

P6

P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（如果侦听到该信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢?

基于公平性的考虑。

如果允许一个站点在完成一次传输立即开始下一次传输，那么某些传输大量长数据的站点可能会长期占 有信道，导致其它站点无法开始传输，这是不公平的。

而要求其先进行随机回退可以避免一个站点长期占用信道，在其回退后的等待期间，其它站点可以获得 信道使用权。

要点：正反面都要答到

第八章

P8

P8. 考虑具有 $p=5$ 和 $q=11$ 的 RSA。

a. n 和 z 是什么?

b. 令 e 为 3。为什么这是一个对 e 的可接受的选择?

c. 求 d 使得 $de=1 \pmod{z}$ 和 $d<160$。

d. 使用密钥 (n, e) 加密报文 $m=8$。令 c 表示对应的密文。显示所有工作。提示：为了简化计算，使用如下事实。

$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

RSA算法：生成密钥

- 选择两个大素数 p 和 q （典型值为大于 10^{100}）
- 计算 $n = p \times q$ 和 $z = (p-1) \times (q-1)$
- 选择一个与 z 互质的数，令其为 d
- 找到一个 e 使满足 $e \times d = 1 \pmod{z}$
- 公开密钥为 (e, n)，私有密钥为 (d, n)

RSA算法：加密和解密

- 加密方法：
  - 将明文看成是一个比特串，将其划分成一个个数据块M，且有$0 \le M < n$
  - 对每个数据块M，计算$C = M^e \pmod n$，C即为M的密文

- 解密方法：
  - 对每个密文块C，计算$M = C^d \pmod n$，M即为要求的明文

RSA算法举例

- 密钥计算：
  - 取p＝3，q＝11
  - 则有n＝33，z＝20
  - 7和20没有公因子，可取d＝7
  - 解方程$7\times e=1 \pmod{20}$，得到e＝3
  - 公钥为（3, 33），私钥为（7, 33）
- 加密：
  - 若明文M＝4，则密文$C=M^e \pmod{n}=4^3 \pmod{33}=31$
- 解密：
  - 计算$M=C^d \pmod{n}=31^7 \pmod{33}=4$，恢复出原文

P8

a.

$$n = pq = 55$$
$$z = (p-1)\cdot(q-1) = 40$$

b. 因为 $e = 3 < z$，且 e 与 z 互质

c. 可以求得 $d = 27$

d. 加密过程：

$$c = m^e \mod n = 8^3 \mod 55 = 17$$

解密过程：

$$m' = c^d \mod n = 17^{25} \mod 55 = 8$$

$m' = m$，结果正确

（注：d的选取不唯一）

P12

P12. 假定 Alice 和 Bob 共享两个秘密密钥：一个鉴别密钥 S_1 和一个对称加密密钥 S_2。扩充图 8-9，使之提供完整性和机密性。

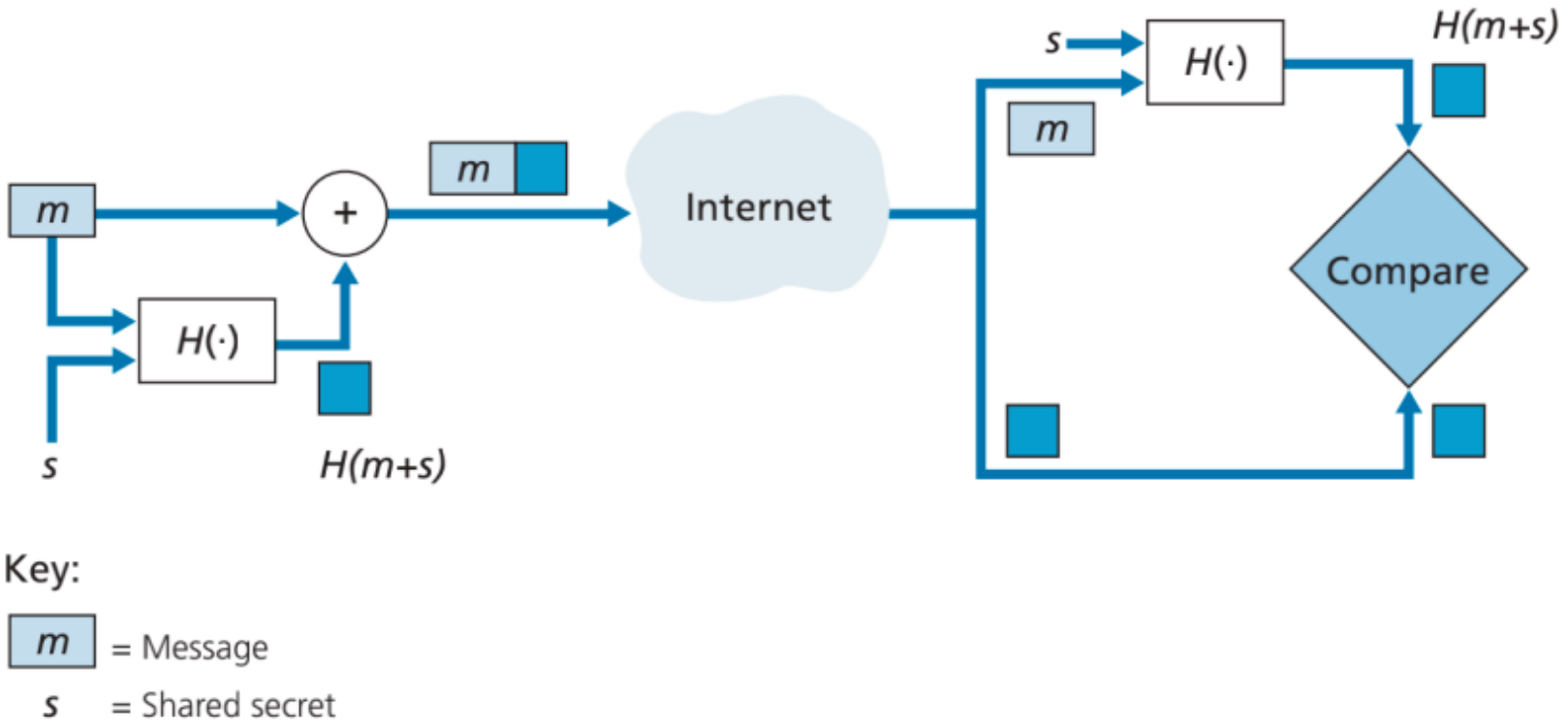


Figure 8.9 ♦ Message authentication code (MAC)

网络中的通信安全

- 机密性:
  - 报文内容的机密性：仅发送方和希望的接收方能够理解报文的内容
  - 通信活动的机密性：通信活动或其特征不被外界察觉
- 端点鉴别：
  - 发送方和接收方都能够证实通信过程中涉及的另一方
- 报文完整性:
  - 报文来自真实的来源，且传输过程中未被修改
- 运行安全性：
  - 网络系统正常运行，网络服务可用

手段

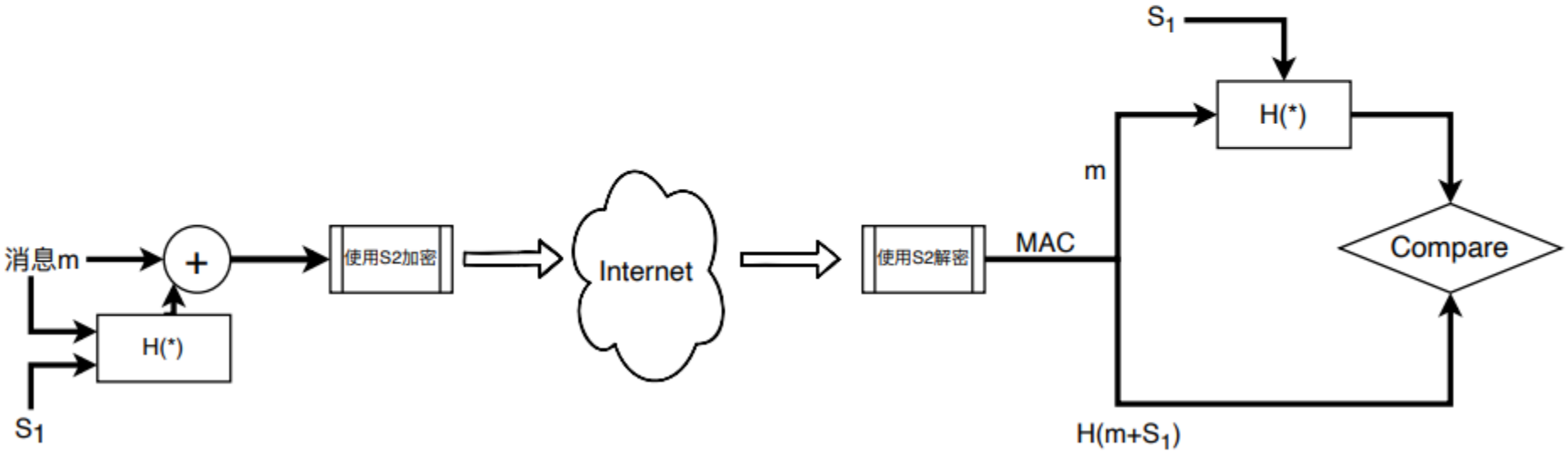
- 加密算法 – 机密性、（报文完整性）
- 报文摘要(数字指纹) – 报文完整性
- 数字签名 – 端点鉴别、（报文完整性）

P12

完整性

这是课本上的图8.9，已经指出了它仅满足而不满足机密性。
现在我们用S_1 和S_2 实现机密性即可

其中，S_1 需要作为图8.9中的Shared Secret，之后我们在用S_2 对MAC进行加解密即可。流程图如下



补充

如果传送的明文信息为 m，散列函数为 H(.)，发送方鉴别用RSA私钥为 (e,n)、公钥为(d,n)，对称加密算法、解密算法、密钥分别为 E(.)、D(.)、K。请给出发送方、接收方保证报文信息机密性和完整性的机制（或过程）。

4. (1)机密性：

发送方：

(2 分)加密：$\mathrm{p} = E_K(\mathrm{m})$

接收方：

(2 分)解密：$m' = D_K(\mathrm{p})$

(2)完整性：

(2 分)发送方：$[H(\mathrm{m})]^e mod\ n$

(2 分)接收方：$[H(\mathrm{m}')]^{\mathrm{d}} mod\ n$(m'为解密后的明文报文)

(2 分)比较上述两个结果是否一致。

说明：公式中的 H(m)代表 H(m)的数值。

关于复习

- 过一遍教材/ppt
- 对照复习提纲掌握好重点内容
- 作业题、小测题
- 某些不可名状的题目

关于考试

- 考试时间: 2022 年 1 月 16 日 (周日) 14:30 ~ 16:30
- 考试地点: 3C101, 3C102 (考场座位表考前会发到课程群)
- 考试形式: 半开卷，不允许使用计算器
- 考试范围: 教材《计算机网络: 自顶向下方法（第七版）》4-8章
- 考试题型: 填空题、选择题、简答题、计算题
- 成绩占比: 期末考试成绩占课程总成绩的25%
- 答题提醒:答案不要写得太乱太分散

期末考试加油

ヾ(◍°∇°◍)ﾉﾞ