第4章　网络层

- 教学内容

4.1　IP协议

4.2　认识IP地址

4.3　虚拟局域网（VLAN）

4.4　认识路由器

4.5　路由选择协议

返回

4.1 IP协议

4.1 IP协议

- IP 协议是TCP/IP协议簇的运作核心，位于网络层（即网际层），对上可传输传输层的各种协议报文，对下可将IP数据报通过以太网、FDDI、X.25等各种规范技术来传递。

4.1 IP协议

- IP 协议的两大功能：
  寻址与路由
  分段与重组

4.1 IP协议

- IP 数据报的结构：

4.2 认识IP地址

认识IP地址

- 什么是IP地址
- IP地址的表示方法
- IP地址的结构
- IP地址的分类
- 几种特殊的IP地址形式
- 子网掩码的作用

3.4.1 什么是IP地址（1）

1. TCP/IP协议规定，必须要用一种统一的表示方法来描述节点在网络中的位置，MAC地址无法达到此要求，于是就设计出了IP地址。
2. IP地址的编码取决于网络层协议（IP协议），所以又称为网络地址。目前的版本是IPv4
3. Internet使用TCP/IP协议，所以Internet中的计算机必须要设置IP地址才能通信。
4. 在Internet上，IP地址指定的不是一台计算机，而是计算机到一个网络的连接。因此，具有多个网络连接的Internet设备（如路由器），就应该有多个IP地址。

4.1.1 什么是IP地址（2）

5. IEEE802标准的局域网参考模型规定了物理层和数据链路层的功能；
6. 不同局域网技术的区别主要在物理层和数据链路层（例如传输介质和介质访问控制方法等），当这些不同的局域网需要在网络层互连时，可以借助其他已有的通信网络协议，如IP协议等。
7. 如果局域网使用TCP/IP协议，则该局域网中的计算机也必须配置IP地址才能通信。

3.4.1 什么是IP地址 (3)

8. 当设备从一个网络移到另一个网络时，其IP地址也会发生相应的改变，即IP地址可以提供关于主机所处的网络位置信息。
9. 物理地址(MAC地址)放在数据帧的报头中，IP地址放在分组的报头中；
10. 物理地址是数据链路层使用的地址，而IP地址是网络层使用的地址。
11. 只有网络层的设备（如路由器）才能识别IP地址。

4.2.2 IP地址的表示方法

IP地址的表示方法(1)

- IPv4的地址由32bit（位）二进制数组成；
- 由于二进制使用起来不方便，用户使用“点分十进制”方式表示。用四组十进制数字表示，每组数字取值范围为0～255，数字之间用“.”隔开

例如：

211.69.35.1　　10.0.0.1

4.2.3 IP地址的结构

IP地址的结构(1)

1. IP地址采用层次结构，IPv4由两个标识码（ID）组成，即网络标识和主机标识，又叫网络号和主机号。
2. 网络号用以标识一个特定网络，这个网络中的所有主机都用同一个网络号；
3. 主机号用以标识该网络中具体的节点（如网络上的主机、服务器、路由器等），同一网段内的主机号必须是唯一的。

IP地址的结构(2)

举例：

211 . 69 . 32 . 1

网络号　　主机号

本例中，把IP地址的前三组数字作为网络号，最后一组数字作为主机号

IP地址的结构(3)

举例：

211 . 69 . 32 . 1

211 . 69 . 32 . 3

211 . 69 . 32 . 6

如果把IP地址的前三组数字作为网络号，最后一组数字作为主机号，则本例中的三个IP地址属于同一个网络（网络号相同）。

4.2.4 IP地址的分类

4.1.4 IP地址的分类(2)

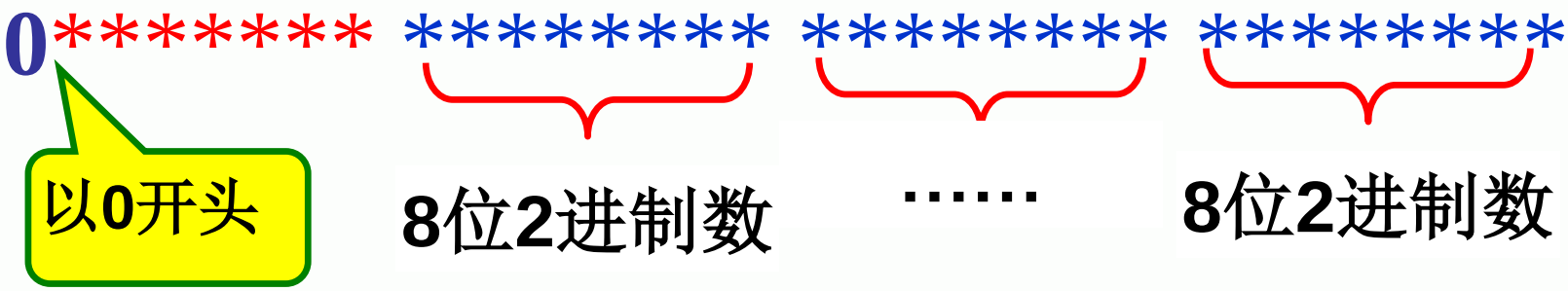
由于网络中包含的计算机有可能不一样多，有的网络可能含有较多的计算机，也有的网络包含较少的计算机，于是人们按照网络规模的大小，把IP地址分为A、B、C、D、E5大类。

A类地址

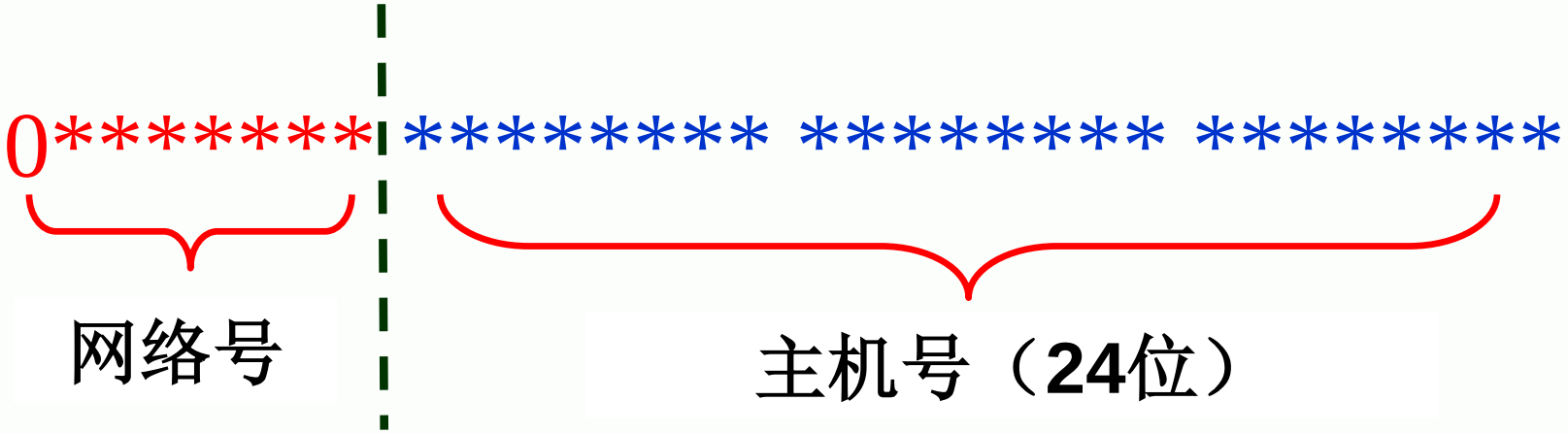
3.4.4.1 A类地址(1)

以32位的二进制表示法来看，A类地址的特点：

- 以0开头
- 第1字节表示网络号
- 第2、3、4字节表示网络中的主机号



3.4.4.1 A类地址(2)



网络号： 有8位，第1位固定为0

主机号： 有24位

3.4.4.1 A类地址(3)

问题1：A类地址中，可以标识多少个网络？

- 由于第1位为0，所以实际网络标识长度为7位，共可标识2^7＝128个网络，但是……
- 网络号为全0，即0000 0000，不能作为网络地址
- 网络号为127，即0111 1111，不能作为网络地址
- A类地址共可标识128－2＝126个网络

3.4.4.1 A类地址(4)

问题2：A类地址第1个字节的实际取值范围是多少？（十进制表示）

- 第1个有效的网络号是0000 0001，十进制是1；
- 最后1个有效的网络号是0111 1110，十进制是126，
- 所以，A类地址第1个字节的实际取值范围是

1～126

例如：61．69．32．1

3.4.4.1 A类地址(5)

问题3：一个A类的网络中，可以有多少个主机？

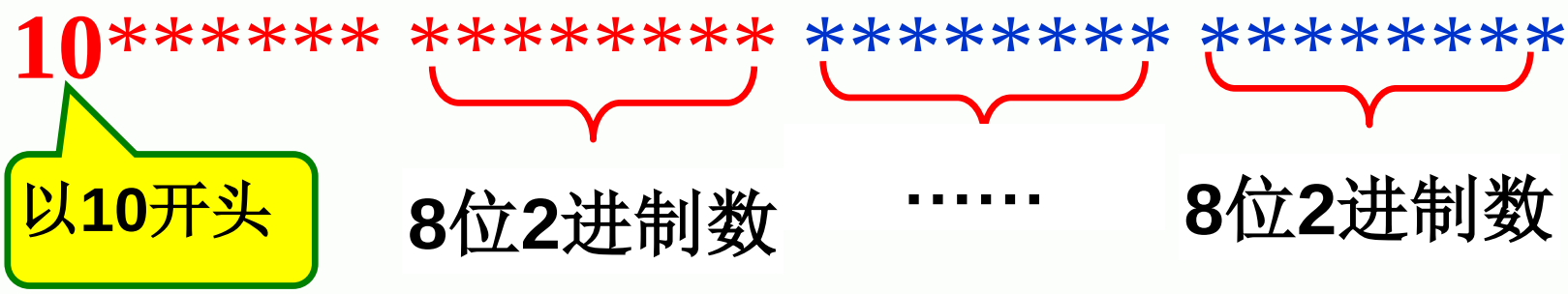
- 由于主机位有24位，所以共可标识2^{24}个主机，但是……
- 主机号为全0，表示本机所在网络的网络号，不能用来表示单个主机；
- 主机号为全1，代表广播地址，不能用来表示单个主机地址
- A类地址的网络，可以有$2^{24}-2$个主机

B类地址

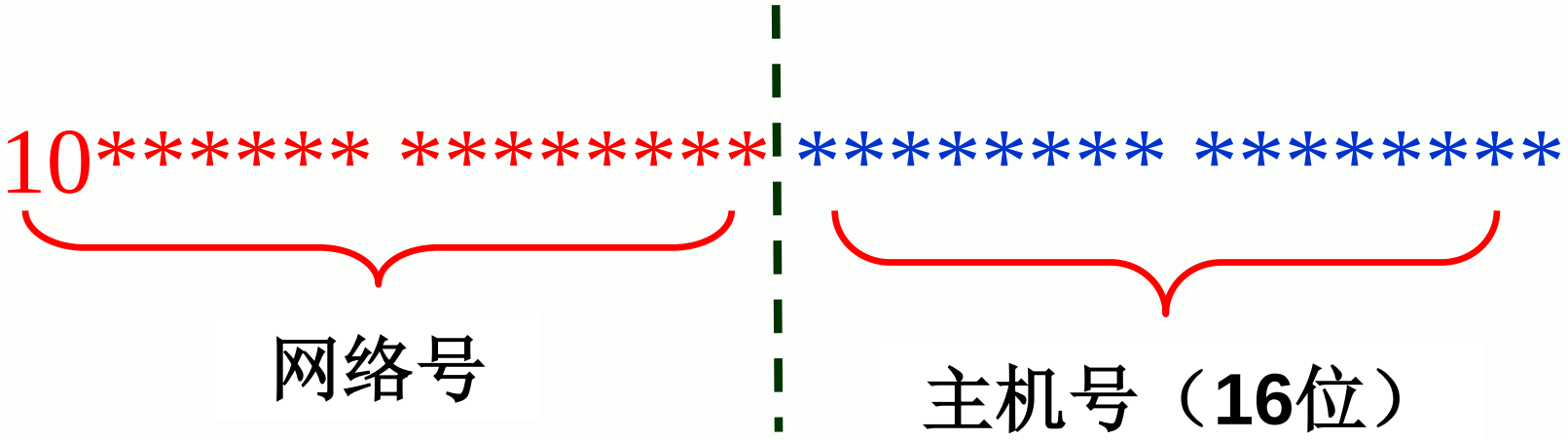
3.4.4.2 B类地址(1)

以32位的二进制表示法来看，A类地址的特点：

- 以10开头
- 第1、2字节表示网络号
- 第3、4字节表示网络中的主机号



3.4.4.2 B类地址(2)



网络号： 有16位，前2位固定为10

主机号： 有16位

3.4.4.2 B类地址(3)

问题1：B类地址中，可以标识多少个网络？

- 由于前2位为10，所以实际网络标识长度为14位，共可标识$2^{14}=16384$个网络

3.4.4.2 B类地址(4)

问题2：B类地址第1个字节的实际取值范围是多少？（十进制表示）

- 从1000 0000～1011 1111
- 十进制表示是128～191；
- 所以，B类地址的网络号的取值范围是

128.0～191.255

3.4.4.2 B类地址(5)

B类地址举例

166.111.0.0 ～ 166.111.255.255

清华大学

3.4.4.2 B类地址(6)

问题3：一个A类的网络中，可以有多少个主机？

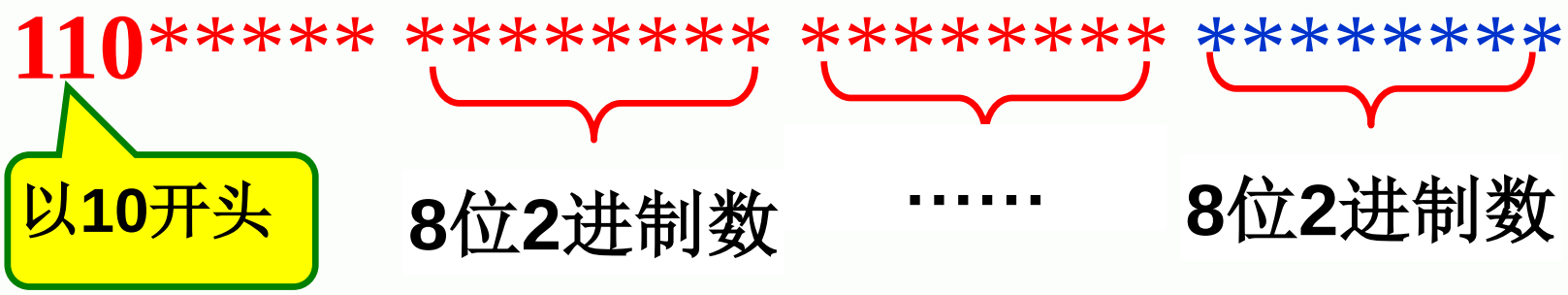
- 由于主机位有16位，所以共可标识2^{16}个主机，但是……
- 主机号为全0，表示本机所在网络的网络号，不能用来表示单个主机；
- 主机号为全1，代表广播地址，不能用来表示单个主机地址
- A类地址的网络，可以有2^{16} －2个主机

C类地址

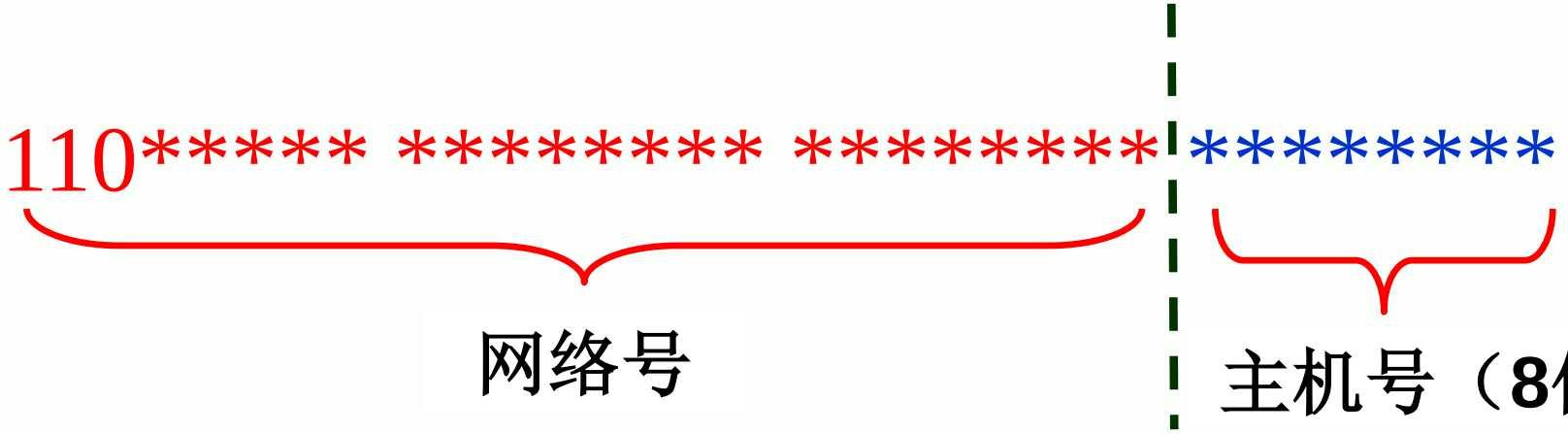
3.4.4.3 C类地址(1)

以32位的二进制表示法来看，A类地址的特点：

- 以110开头
- 第1、2、3字节表示网络号
- 第4个字节表示网络中的主机号



3.4.4.3 C类地址(2)



网络号： 有24位，前3位固定为110

主机号： 有8位

3.4.4.3 C类地址(3)

问题1：C类地址中，可以标识多少个网络？

- 由于前3位为110，所以实际网络标识长度为21位，共可标识2^{21}个网络

3.4.4.3 C类地址(4)

问题2：C类地址第1个字节的实际取值范围是多少？（十进制表示）

- 从1100 0000～1101 1111
- 十进制表示是192～223；
- 所以，C类地址的网络号的取值范围是

192.0.0～223.255.255

3.4.4.3 C类地址(5)

C类地址举例

211.69.32.1

3.4.4.3 C类地址(6)

问题3：一个C类的网络中，可以有多少个主机？

- 由于主机位有8位，所以共可标识2^8＝256个主机，但是……
- 主机号为全0，表示本机所在网络的网络号，不能用来表示单个主机；
- 主机号为全1，代表广播地址，不能用来表示单个主机地址
- 一个C类地址的网络，可以有256-2＝254个主机

D类地址

3.4.4.4 D类地址(1)

组播地址

- 第1个字节以1110开头
- 第1字节的范围是224～239；
- D类地址用以支持组播通信，即可定义一组IP地址对应一个D类地址。
- 不分配给单一主机使用

E类地址

3.4.4.5 E类地址(1)

保留地址

- 第1个字节以1111开头
- 第1字节的范围是大于240；
- 保留，不分配给单一主机使用

总结

- 可以作为普通主机地址进行分配的是A、B、C这3类地址。
- A类地址用于大型网络
- B类地址用于中等规模的网络
- C类地址用于小规模的局域网络

4.2.5 几种特殊的IP地址形式

广播地址

3.4.5.1 广播地址(1)

- TCP/IP规定，主机号全为“1”的IP地址用于广播；
- 例如，192.168.1.255是一个C类的广播地址

网络地址

3.4.5.2 网络地址(1)

- TCP/IP规定，主机号全为“0”的IP地址为网络号；
- 网络号被解释成“本地”网络；
- 例如，173.18.0.0表示“173.18”这个B类网络的网络地址

回送地址

3.4.5.3 回送地址(1)

- A类网络地址的第1段十进制数值为127是一个保留地址，如127.1.11.13，用于网络软件测试以及本地机进程间通信。
- 127开头的地址称为回送地址。

私有地址

3.4.5.4 私有地址(1)

- 在可供分配的主机IP地址资源中，还可以分为共有IP地址和私有IP地址两类。
- 共有地址是连接到公用网络的主机使用的，必须是唯一的，需要统一管理和分配，通常从Internet服务提供者处获得
- A、B、C三类地址中均有部分地址被用作私有地址。私有地址被大量用于企业内部网络中。

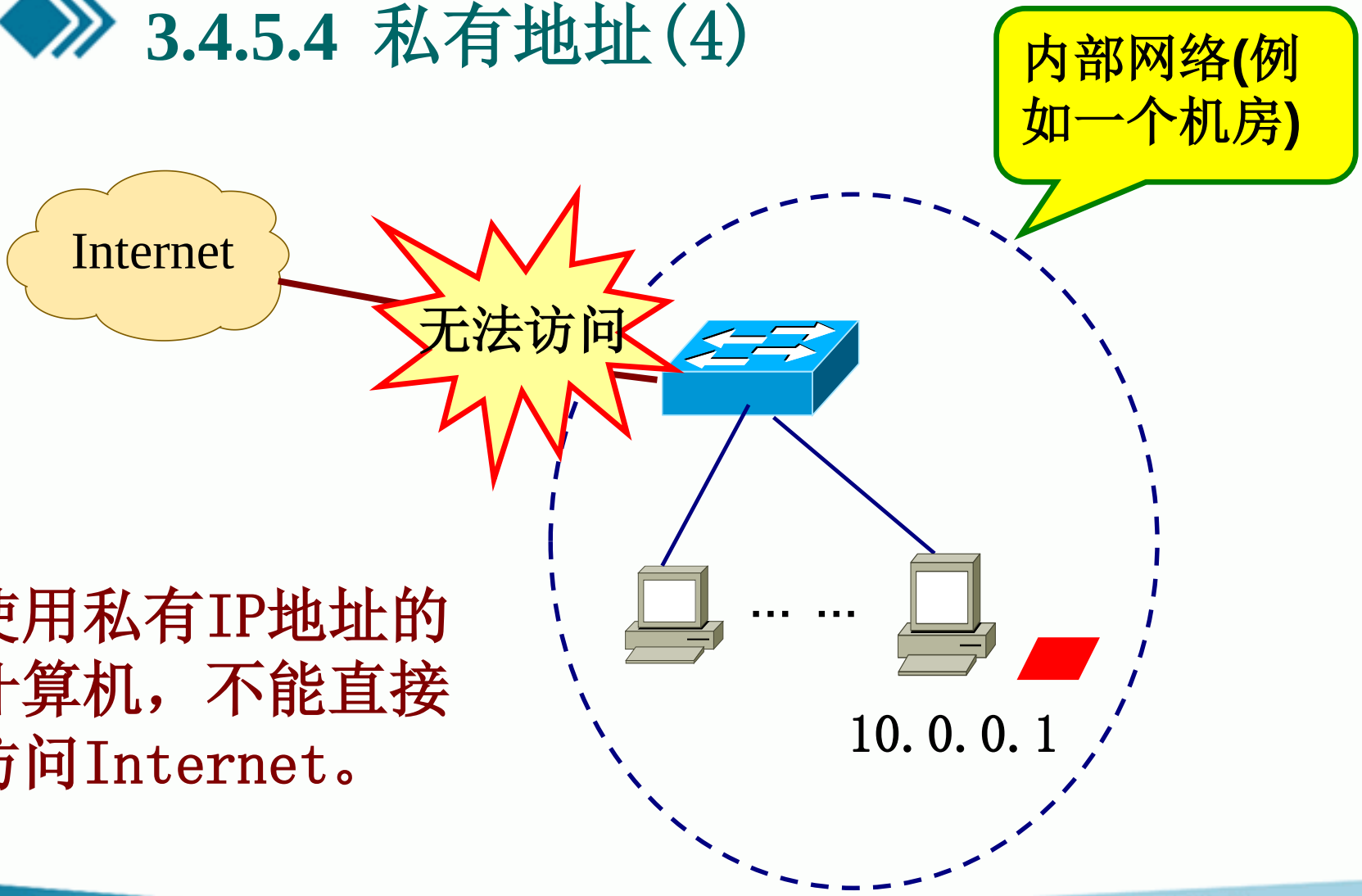
3.4.5.4 私有地址(2)

- 私有网络由于不与外部互连，因而私有网络管理者可能使用随意的IP地址。保留专门的私有地址供其使用，其目的是为了避免以后接入公网时引起地址混乱。
- 在Internet上，私有地址是不能出现的。
- 使用私有地址的私有网络在接入Internet时，要使用地址翻译(NAT)，将私有地址翻译成公用合法地址。

3.4.5.4 私有地址(3)

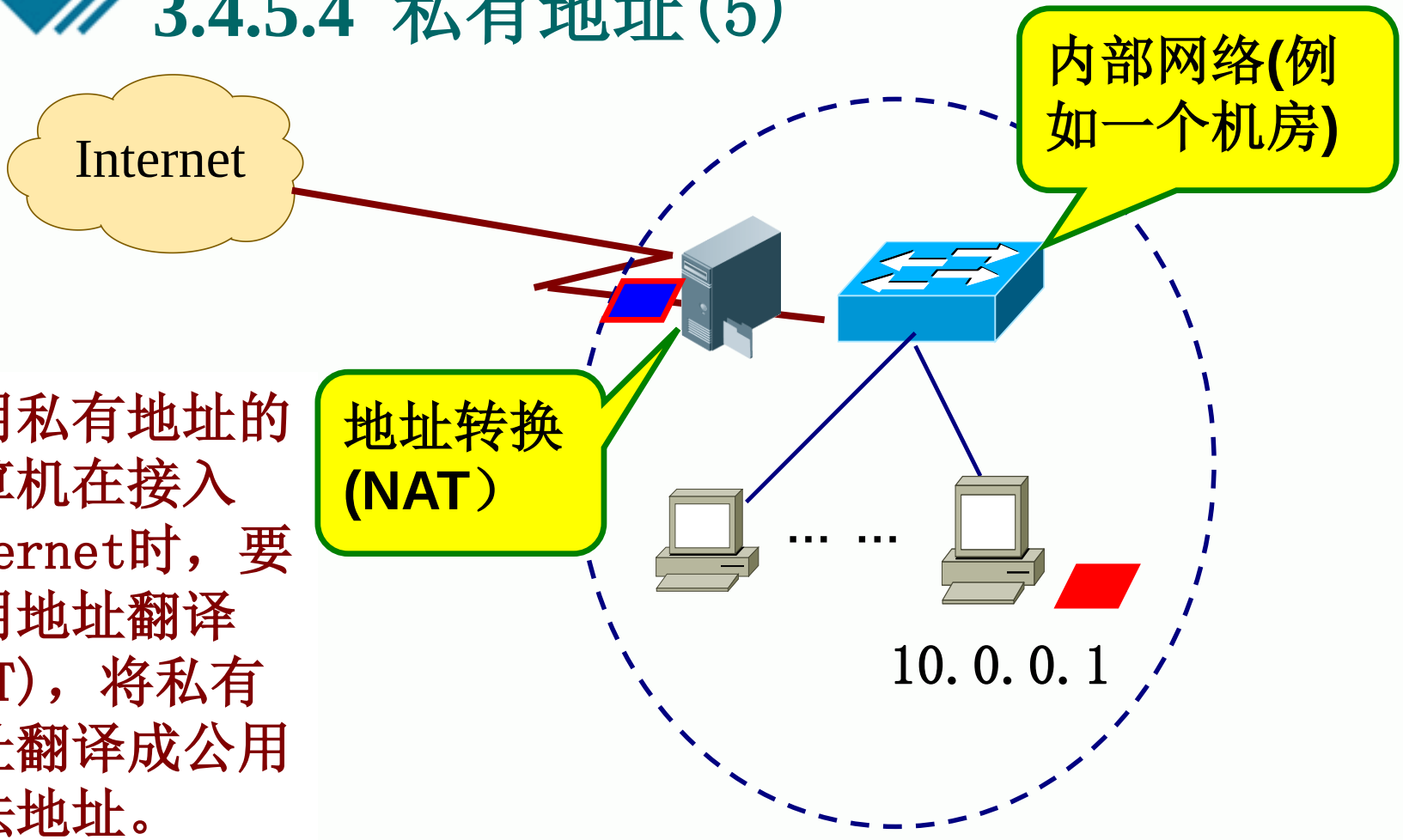
地址类型	私有地址范围	网络个数
A类	10.0.0.0 ~10.255.255.255	1
B类	172.16.0.0 ~ 172.31.255.255	16
C类	192.168.0.0 ~ 192.168.255.255	256

3.4.5.4 私有地址(4)



使用私有IP地址的计算机，不能直接访问Internet。

3.4.5.4 私有地址(5)



使用私有地址的计算机在接入Internet时，要使用地址翻译(NAT)，将私有地址翻译成公用合法地址。

4.2.6 子网掩码的作用

（）

3.4.6　子网掩码的作用

- 引入：

  - 属于同一个网络的两台计算机可以直接通信！（具有相同的网络号）
  - 若不在一个网络中，不能直接通信，必须由路由设备负责接收——转发。

3.4.6　子网掩码的作用

- 子网掩码是一个特殊的32位二进制数，与IP地址配合使用；
- 子网掩码中的“1”表示IP地址的对应位属于网络标识，“0”表示IP地址的对应位属于主机标识。

3.4.6　子网掩码的作用

- **A、B、C三类网络的标准缺省掩码如下**

IP类别	子网掩码位模式
A类	11111111.00000000.00000000.00000000
B类	11111111.11111111.00000000.00000000
C类	11111111.11111111.11111111.00000000

3.4.6　子网掩码的作用

- 子网掩码在应用中也采用点式十进制表示，所以 A、B、C三类网络的标准缺省掩码也可表示如下

IP类别	子网掩码
A类	255.0.0.0
B类	255.255.0.0
C类	255.255.255.0

3.4.6 子网掩码的作用

- 举例

IP地址 ： 211.69.32.1（C类地址）

子网掩码： 255.255.255.0

掩码：11111111 . 11111111 . 11111111 . 00000000

IP ： 11010011 . 01000101 . 00100000 . 00000001

子网掩码中的“1”表示IP地址的对应位属于网络标识，

子网掩码中的“0”表示IP地址的对应位属于主机标识，

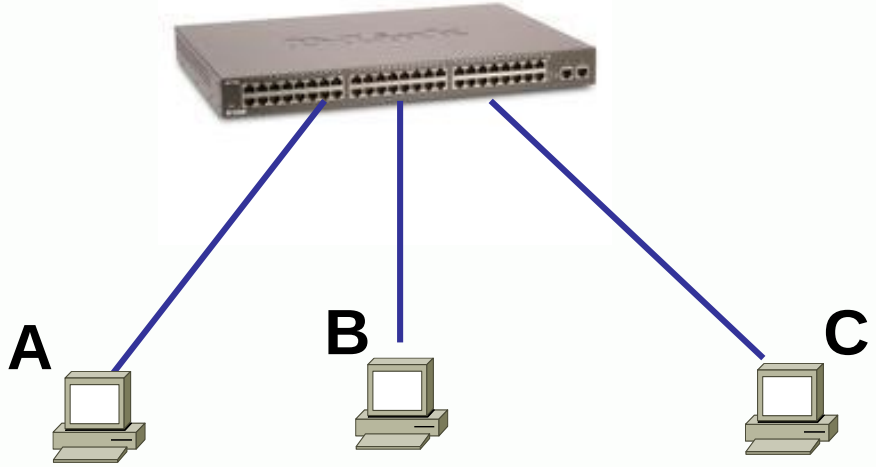
3.4.6　子网掩码的作用

- 归纳
  - 缺省情况下，A类地址的子网掩码是255.0.0.0 ，表示其第1个字节是网络号；
  - 缺省情况下，B类地址的子网掩码是255.255.0.0 ，表示其前2个字节是网络号；
  - 缺省情况下，C类地址的子网掩码是255.255.255.0 ，表示其前3个字节是网络号

3.4.6　子网掩码的作用

- 举例

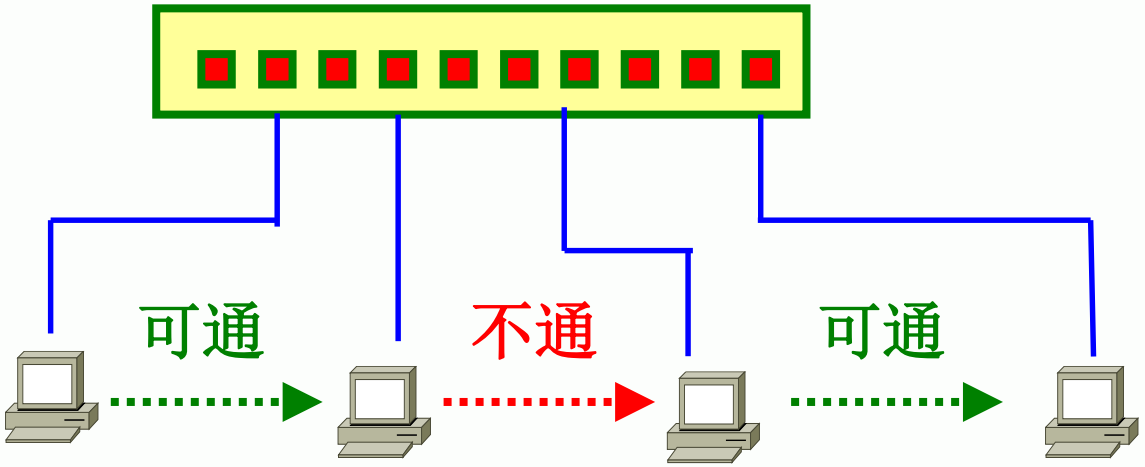
A、B、C三个主机在同一个网络内，可以直接通信。



192.168.1.2　　192.168.1.3　　192.168.1.20

子网掩码：255.255.255.0

➢ 举例



A(2号) B(4号) C(15号) D(18号)

10.0.1.2 10.0.1.4 10.0.2.200 10.0.2.210

子网掩码全是：255.255.255.0

关于子网掩码的扩展

3.4.7 子网掩码的扩展

●默认情况下

- 一个A类地址的网络中，可以有$2^{24}-2$个主机；
  子网掩码： 255.0.0.0
- 一个B类地址的网络中，可以有64000多个主机；
  子网掩码：255.255.0.0
- 一个C类地址的网络中，可以有254个主机；
  子网掩码：255.255.255.0

总结

- 可以作为普通主机地址进行分配的是A、B、C这3类地址。
- A类地址用于大型网络
- B类地址用于中等规模的网络
- C类地址用于小规模的局域网络

3.4.7 子网掩码的扩展

- 问题
  - C类地址的网络，是规模最小的网络吗？

3.4.7 子网掩码的扩展

- 解答

利用子网划分技术，网络管理员可以将一个网络分割成多个小的子网，子网内部可以直接通信，但是子网之间不能直接通信，需要借助路由器才能通信。

3.4.7 子网掩码的扩展

●技术思路

为了创建一个子网地址，网络管理员从主机号“借”位并把它们指定为子网号，从而使主机号的位数进一步缩小。

如何“借”位？

回忆一下子网掩码的作用

- 子网掩码是一个特殊的32位二进制数，与IP地址配合使用；
- 子网掩码中的“1”表示IP地址的对应位属于网络标识，“0”表示IP地址的对应位属于主机标识。

3.4.7 子网掩码的扩展

- 结论

可以利用子网掩码实现从主机号“借”位并把它们指定为子网号，从而实现子网划分。

3.4.7 子网掩码的扩展

子网划分举例

3.4.7 子网掩码的扩展

例1

例1

- IP地址段
  - 10.1.1.1 ~ 10.1.1.255
  - 10.2.1.1 ~ 10.2.1.255
  - 10.3.1.1 ~ 10.3.1.255
  - 10.4.1.1 ~ 10.4.1.255
- 子网掩码：255.0.0.0

根据子网掩码，因为这4个IP地址段的网络号都是10，所以它们属于同一个网络

例1

- IP地址段
  - 10.1.1.1 ~ 10.1.1.255
  - 10.2.1.1 ~ 10.2.1.255
  - 10.3.1.1 ~ 10.3.1.255
  - 10.4.1.1 ~ 10.4.1.255
- 子网掩码：255.255.0.0

根据子网掩码分析，原主机号的前8位被用作网络号，因此这4个IP地址段的网络号不再相同，所以它们表示4个子网。

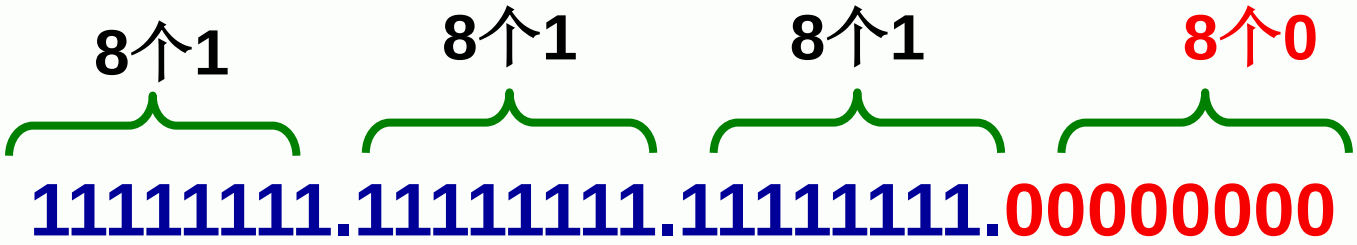
- 10.0.0.3
- 10.0.0.200
- 10.0.1.100

3.4.7 子网掩码的扩展

例2：

将一个C类地址网络划分成两个子网

- IP地址　：10.0.0.*
- 子网掩码：255.255.255.0



这是C类IP地址所用到的子网掩码，其特点：
网络位：24位，主机位：8位，
表示一个可以包含2^8（256)个主机的C类网络。

根据规定：

1. 主机位全为0的IP地址，表示本网络，不能被用作实际主机的IP地址；
2. 主机位全为1的IP地址，表示广播地址，不能被用作实际主机的IP地址；

因此： 在10.0.0.* / 255.255.255.0 这个C类网络中，真正能被用来分配给主机的地址，实际上只有254个， 10.0.0.1 ~ 10.0.0.254

10.0.0.0 ：不能使用，因为它表示“本网络”；

10.0.0.255：不能使用，因为它表示广播；

能否将 10.0.0.1 ~ 10.0.0.254这个地址段，划分成两个子网呢？

10.0.0.1 ~ 10.0.0.254，划分成两个子网

- 子网掩码：255.255.255.0 可以吗？

➢ 子网掩码的设计

8个1　8个1　8个1　1个1＋7个0

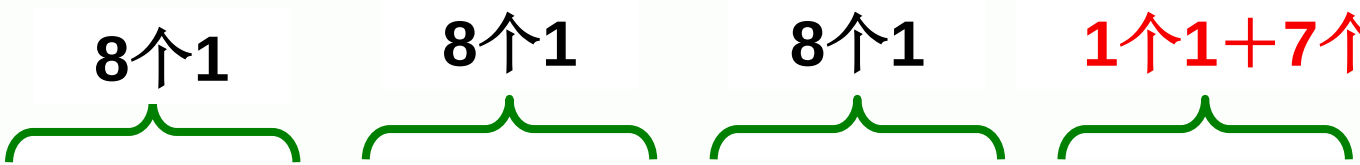
11111111.11111111.11111111.10000000

从原来的主机位中，借1位，用作网络号

➢子网掩码：**255.255.255.128**

子网掩码：255.255.255.128

- 将一个C类网络分成两个子网络



11111111.11111111.11111111.10000000

网络位：增加1位，表示原网络被分成2个子网。

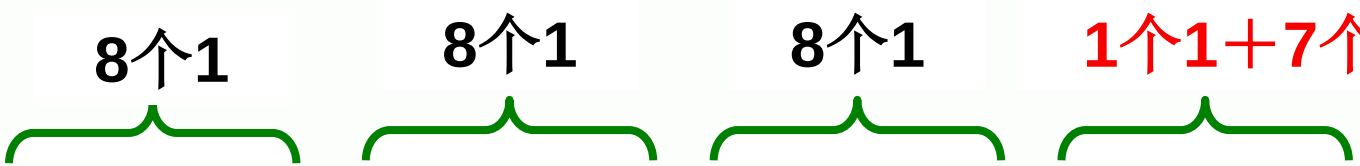
主机位：7位，表示每个子网里可以有2^7个主机

子网1：10.0.0.0 ~ 10.0.0.127

子网2：10.0.0.128 ~ 10.0.0.255

子网掩码：255.255.255.128

- 将一个C类网络分成两个子网络



11111111.11111111.11111111.10000000

00001010.00000000.00000000.01111111

00001010.00000000.00000000.10001000

子网1：10.0.0.0 ~ 10.0.0.127

子网2：10.0.0.128 ~ 10.0.0.255

网络位：增加1位，表示原网络被分成2个子网。

主机位：7位，表示每个子网里可以有2^7个主机

- 举例说明：

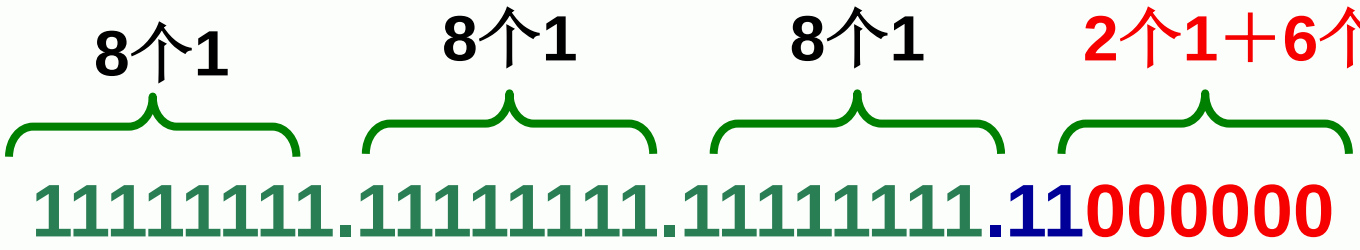
A: 10.0.0.3　　B: 10.0.0.200

- 当子网掩码是255.255.255.0时，A和B属于同一网络；
- 当子网掩码是255.255.255.128时，A和B就分属于不同网络。

以此类推

子网掩码：255.255.255.192

- 将一个C类网络分成4个子网络



网络位：增加2位，表示原网络被分成4个子网。

主机位：6位，表示每个子网里可以有2^6个主机

子网1：10.0.0.0 ~ 10.0.0.63

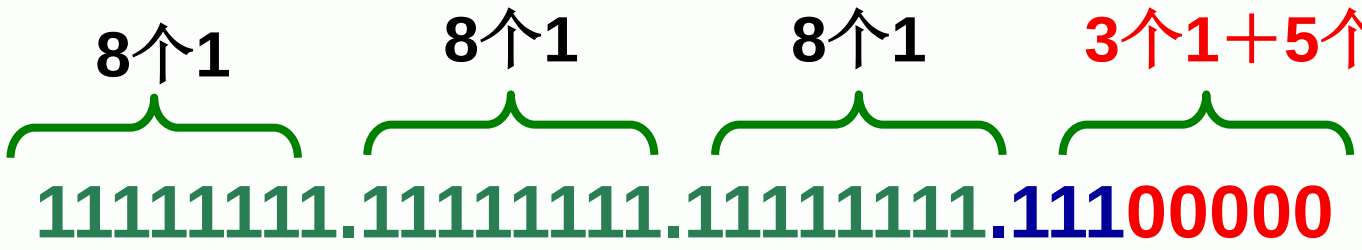
子网2：10.0.0.64 ~ 10.0.0.127

子网3：10.0.0.128 ~ 10.0.0.191

子网4：10.0.0.192 ~ 10.0.0.255

子网掩码：255.255.255.224

- 将一个C类网络分成8个子网络



网络位：增加3位，表示原网络被分成8个子网。

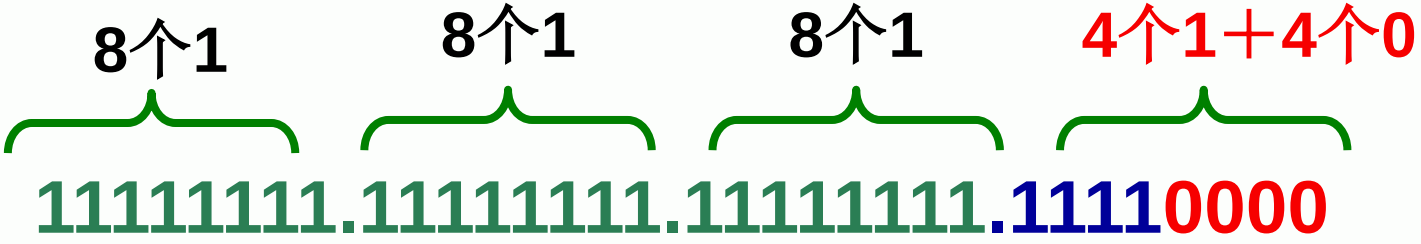
主机位：5位，表示每个子网里可以有2^5个主机

子网1：10.0.0.0 ~ 10.0.0.31

子网2：10.0.0.32 ~ 10.0.0.63 ……

子网掩码：255.255.255.240

- 将一个C类网络分成16个子网络



网络位：增加4位，表示原网络被分成16个子网。

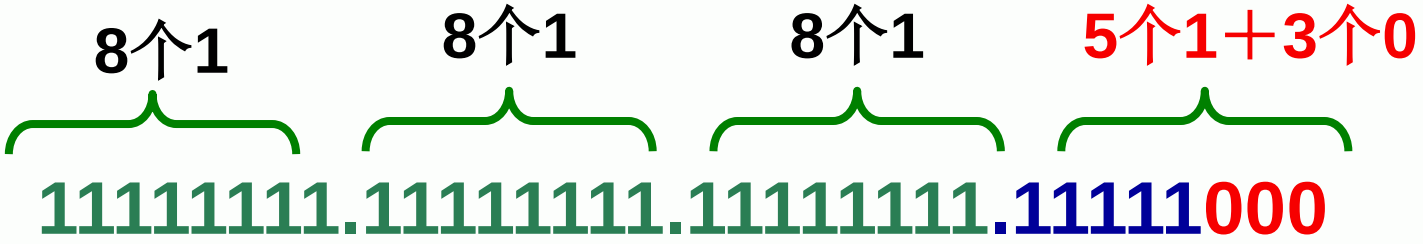
主机位：4位，表示每个子网里可以有2^4个主机

子网1：10.0.0.0 ~ 10.0.0.15

子网2：10.0.0.16 ~ 10.0.0.31 ……

子网掩码：255.255.255.248

- 将一个C类网络分成32个子网络



网络位：增加5位，表示原网络被分成32个子网。

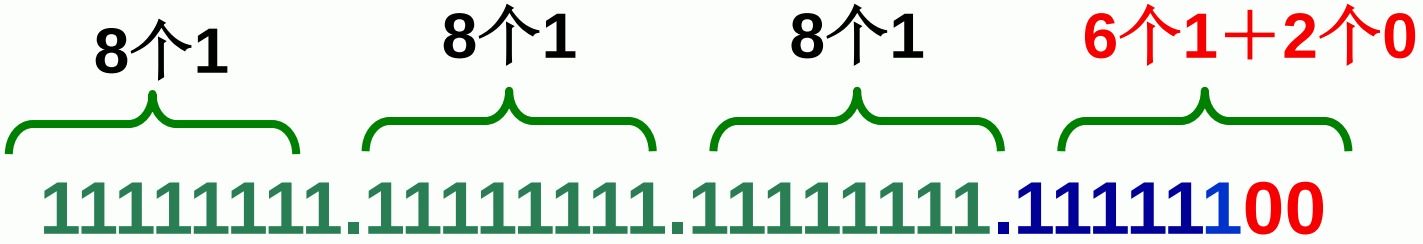
主机位：3位，表示每个子网里可以有2^3个主机

子网1：10.0.0.0 ~ 10.0.0.7

子网2：10.0.0.8 ~ 10.0.0.15 ……

子网掩码：255.255.255.252

- 将一个C类网络分成64个子网络



网络位：增加6位，表示原网络被分成64个子网。

主机位：2位，表示每个子网里可以有2^2个主机

子网1：10.0.0.0 ~ 10.0.0.3

子网2：10.0.0.4 ~ 10.0.0.7 ……

实验4： 利用子网掩码进行子网划分

- 用211.69.32.1 ~ 211.69.32.254 IP地址段为本组的8台计算机分配IP地址；

要求：

1. 8台计算机全部连在一个交换机上；
2. 分成4个子网，每个子网内机器数自定；
3. 画出拓扑图，写出设计方案（包括IP地址和子网掩码的配置）
4. 通过实验验证（利用ping命令）

（1） 同子网内部的通信

（2） 不同子网之间的通信

11111111.11111111.11111111.11000000

如果子网掩码是255.255.192.0，那么下面主机（ ）必须通过路由器才能与主机192.23.144.16通信。

A 192.23.191.21　　B 192.23.127.222

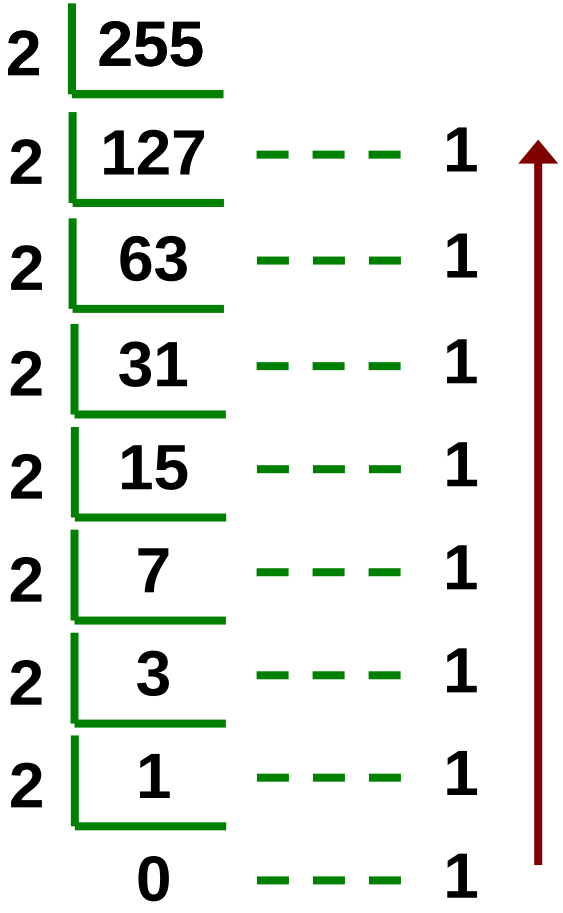
C 192.23.130.33　　D 192.23.148.127

分析：

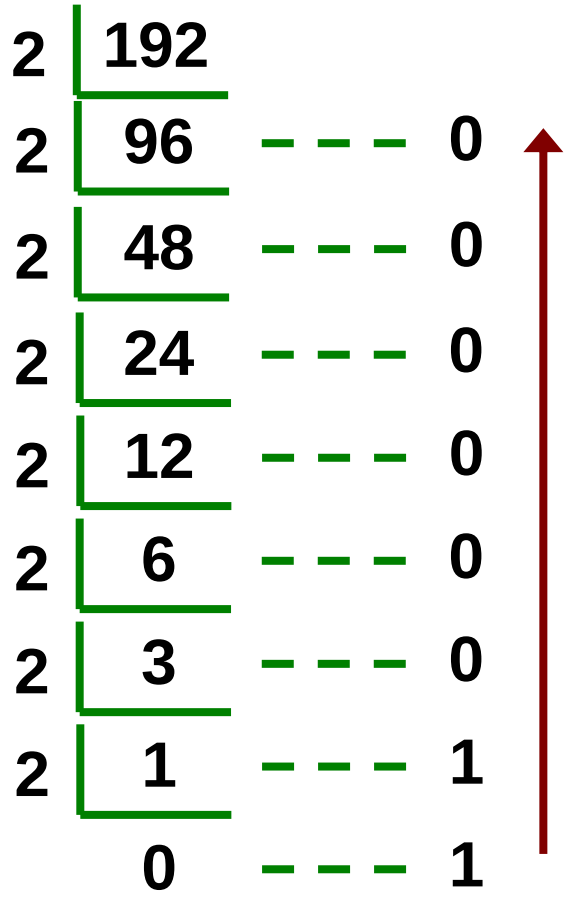
先把子网掩码和IP地址都变成二进制，然后通过子网掩码来分析4个IP地址的网络号和主机号，网络号相同的计算机，属于同一网络。

3.4 设计一个简单的网络 —— 实例3

子网掩码：255.255.192.0的二进制形式



$(255)_{10} = (11111111)_2$



$(192)_{10} = (11000000)_2$

3.4 设计一个简单的网络 —— 实例3

接下来：

根据子网掩码**255.255.192.0**的二进制表现形式，把目标主机和**A、B、C、D**四个答案的**IP**全用二进制表示，然后根据子网掩码判断谁的网络号与目标主机不同。

目标主机： **192.23.144.16**

A 192.23.191.21 **B 192.23.127.222**

C 192.23.130.33 **D 192.23.148.127**

3.4 设计一个简单的网络 —— 实例3

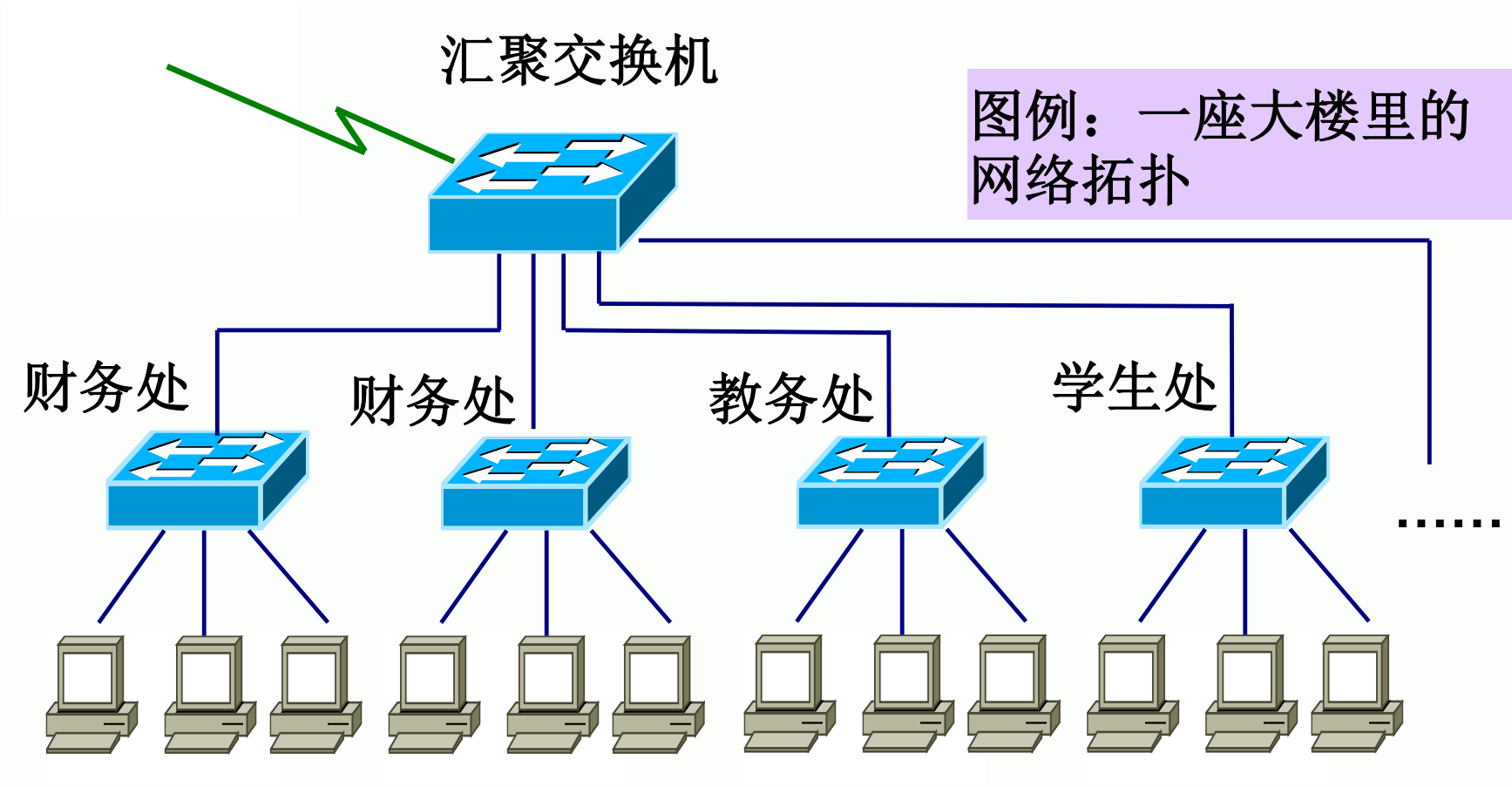
子网掩码	11111111.11111111.11	000000.00000000
目标地址	11000000.00010111.10	010000.00010000
A	11000000.00010111.10	111111.00010101
B	11000000.00010111.01	111111.11011110
C	11000000.00010111.10	000010.00100001
D	11000000.00010111.10	010100.01111111

B的网络号与目标地址的网络号不同，所以B与目标地址不在同一网络。

问题引入

通过交换机的级连，可以把多个交换机汇聚到一个交换机上，从而在物理上形成一个较大的网络。

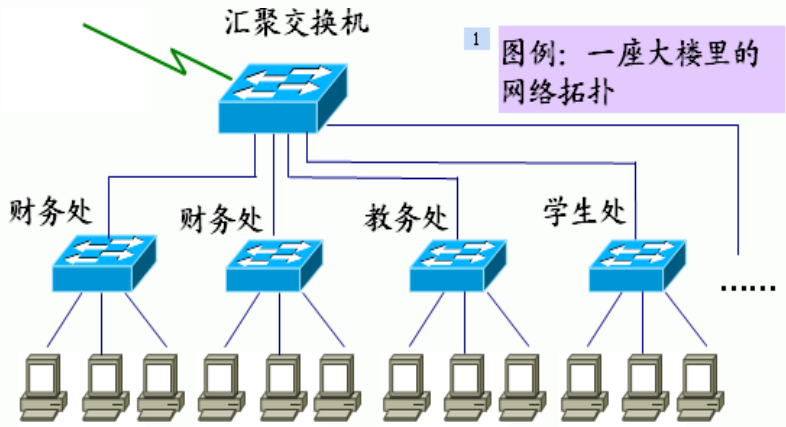
如下图所示



通过交换机的级连，可以把多个交换机汇聚到一个交换机上，从而在物理上形成一个较大的网络

● 网络状况分析

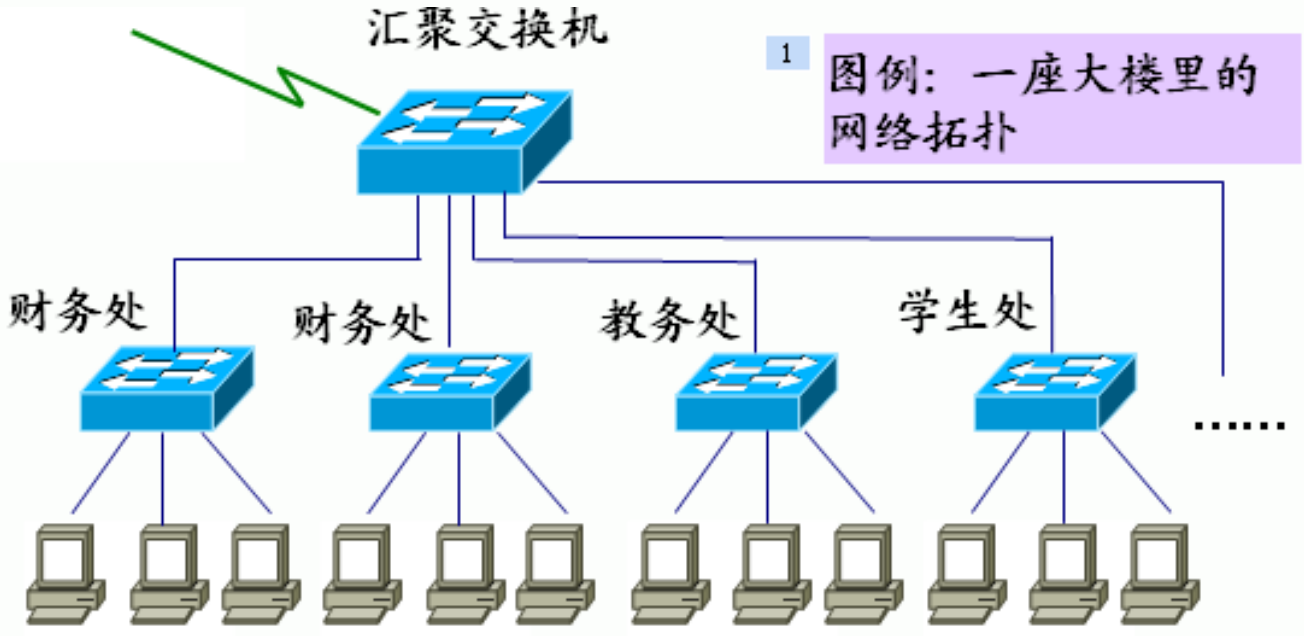
- 这是一座办公楼网络，楼内有近100台计算机上网，分属于不同部门；
- 教务处有30台计算机上网，财务处有18台，学生处有15台，科研处有20台，……；



1 图例：一座大楼里的网络拓扑

- 网管给这座楼内的计算机分配IP地址，从10.0.1.1～10.0.1.200，子网掩码全部是255.255.255.0

● 网络状况分析



- 起初，网络运行的很正常，但是不久，就开始出问题了……

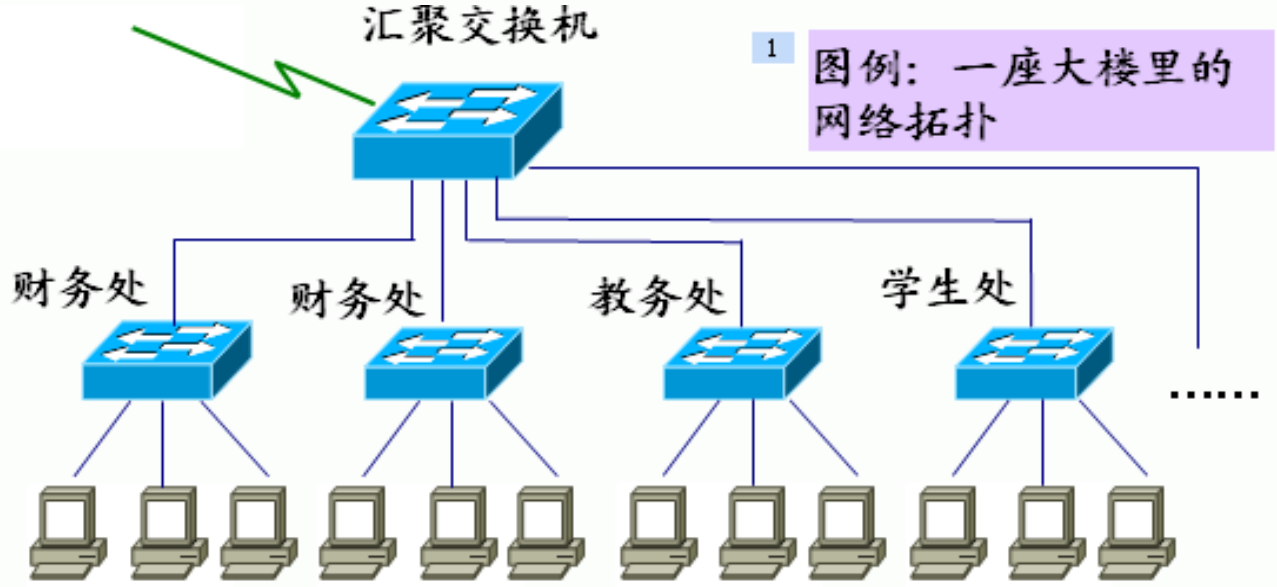
网络状况分析

- 教务处办公室里有一台打印机设置了共享，原本只想让自己科室的计算机使用，但是其他部门的计算机也能利用它来打印；
- 财务处的计算机上共享了一些文件，原本是想方便本科室内部的工作，但却发现其他部门也能访问到这些文件；
- ……

为什么？

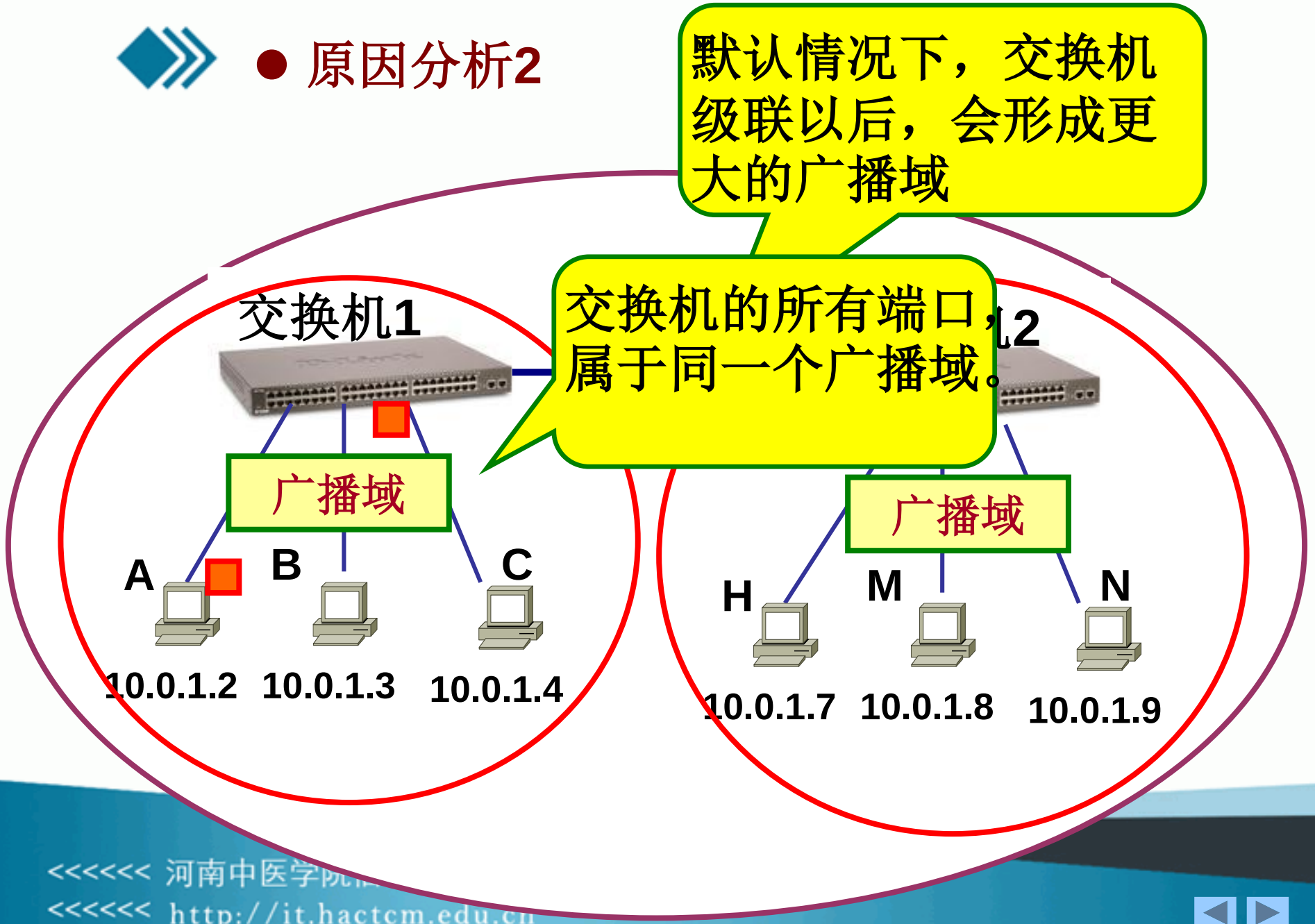
- 不仅如此，楼内用户发现网络经常变得很慢……

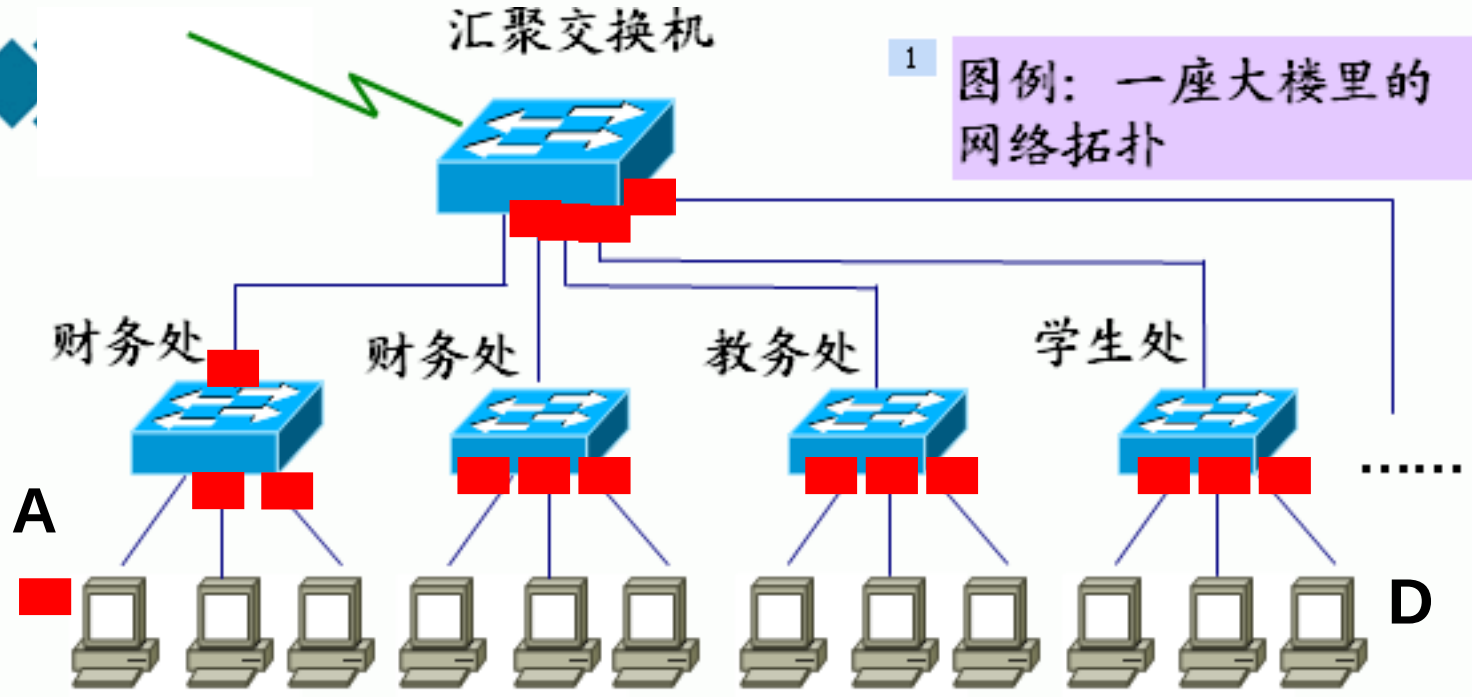
● 原因分析1



通过IP地址和子网掩码分析，整座大楼内的计算机都属于同一个网络，因此相互之间可以直接互访。某台计算机共享的文件或打印机，大家都可以看到。

● 原因分析2

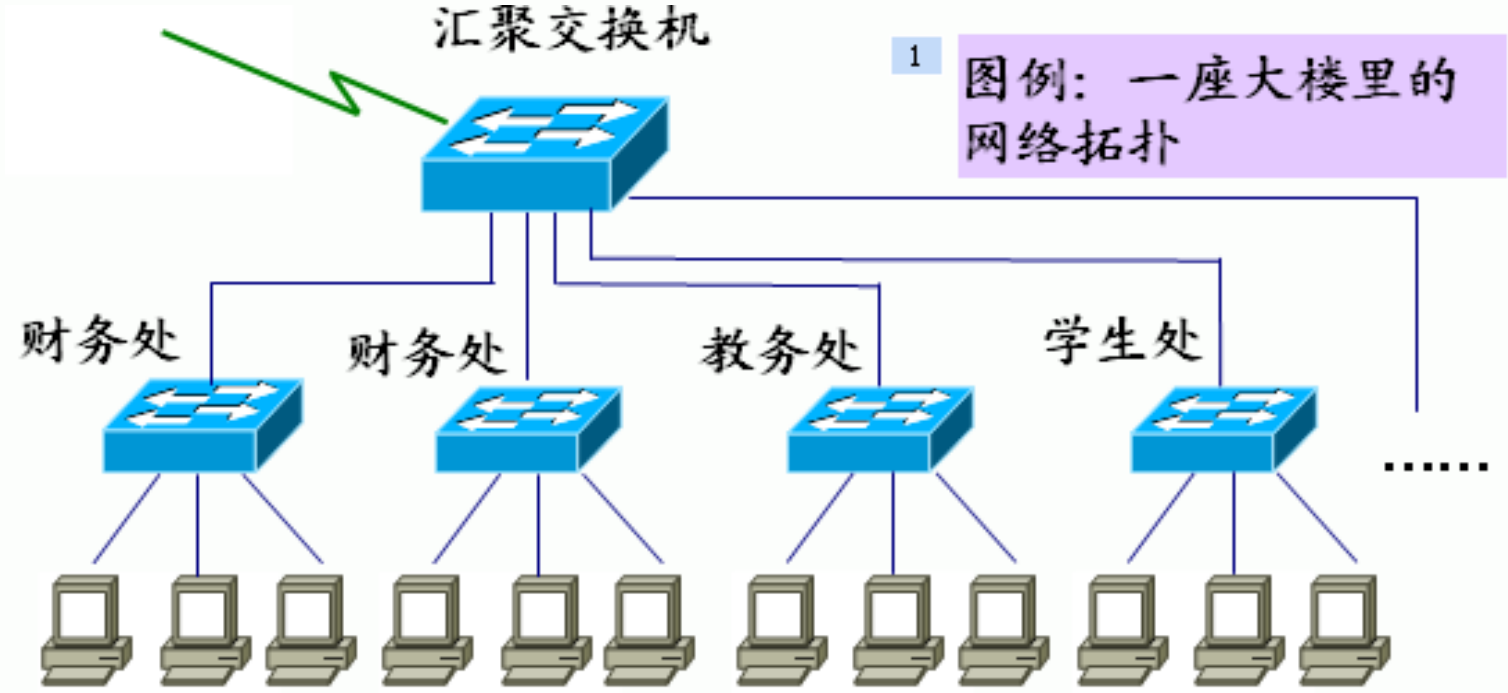

默认情况下，交换机级联以后，会形成更大的广播域
交换机的所有端口，属于同一个广播域。
交换机1
广播域
A
B
C
10.0.1.2
10.0.1.3
10.0.1.4
广播域
H
M
N
10.0.1.7
10.0.1.8
10.0.1.9



A：10.0.1.5　255.255.255.0

D：10.0.1.75　255.255.255.0

A 向D 发信息，但是目前各交换机的MAC地址表中没有D的信息，所以各交换机以广播的形式发送

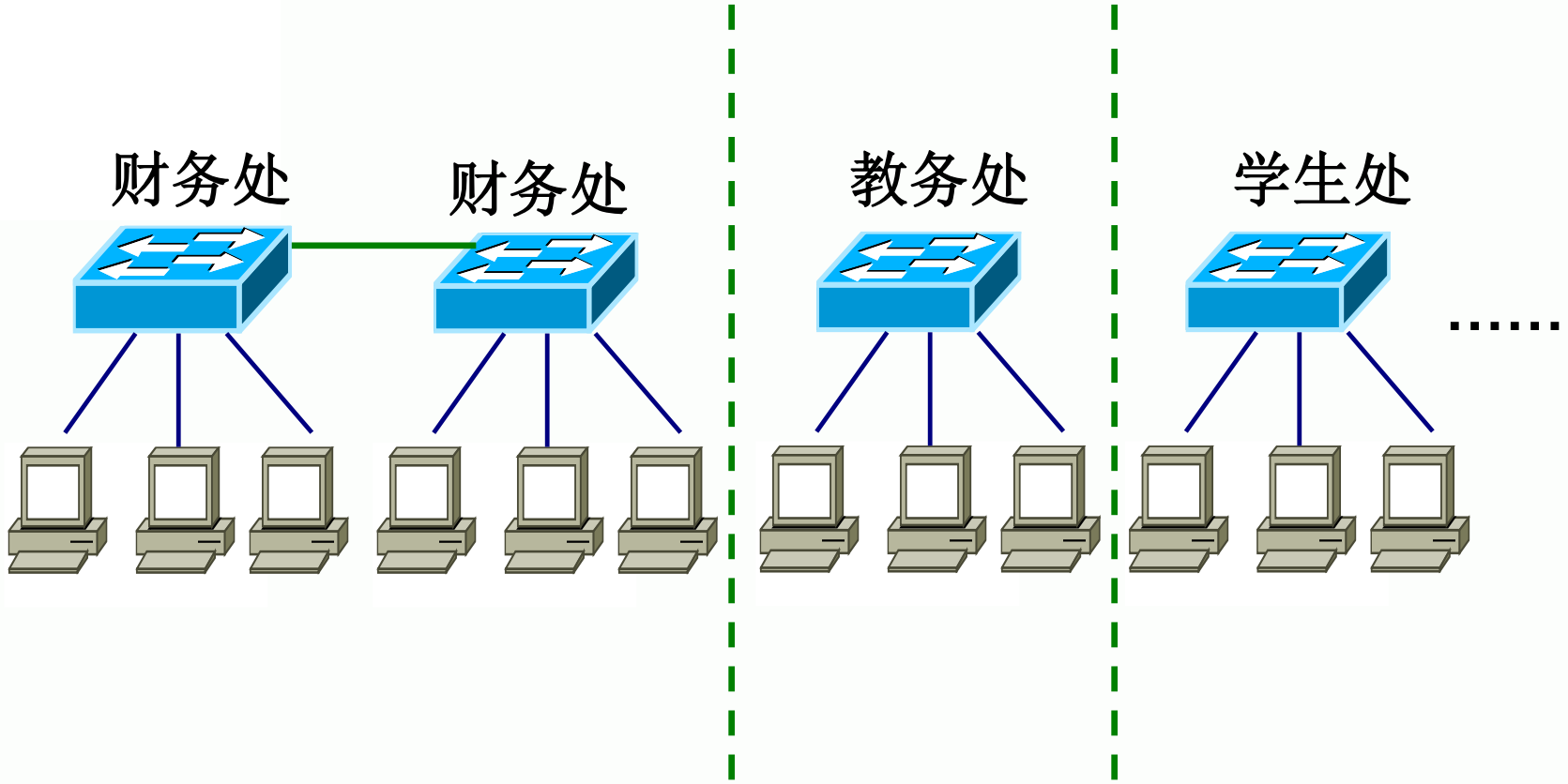


在较大规模的网络中，大量的广播信息很容易引起网络性能的降低，甚至导致整个网络的崩溃。

怎么办？

解决方案1

- 不同部门的交换机之间，不再级联。从物理上把不同部门的网络给隔开。



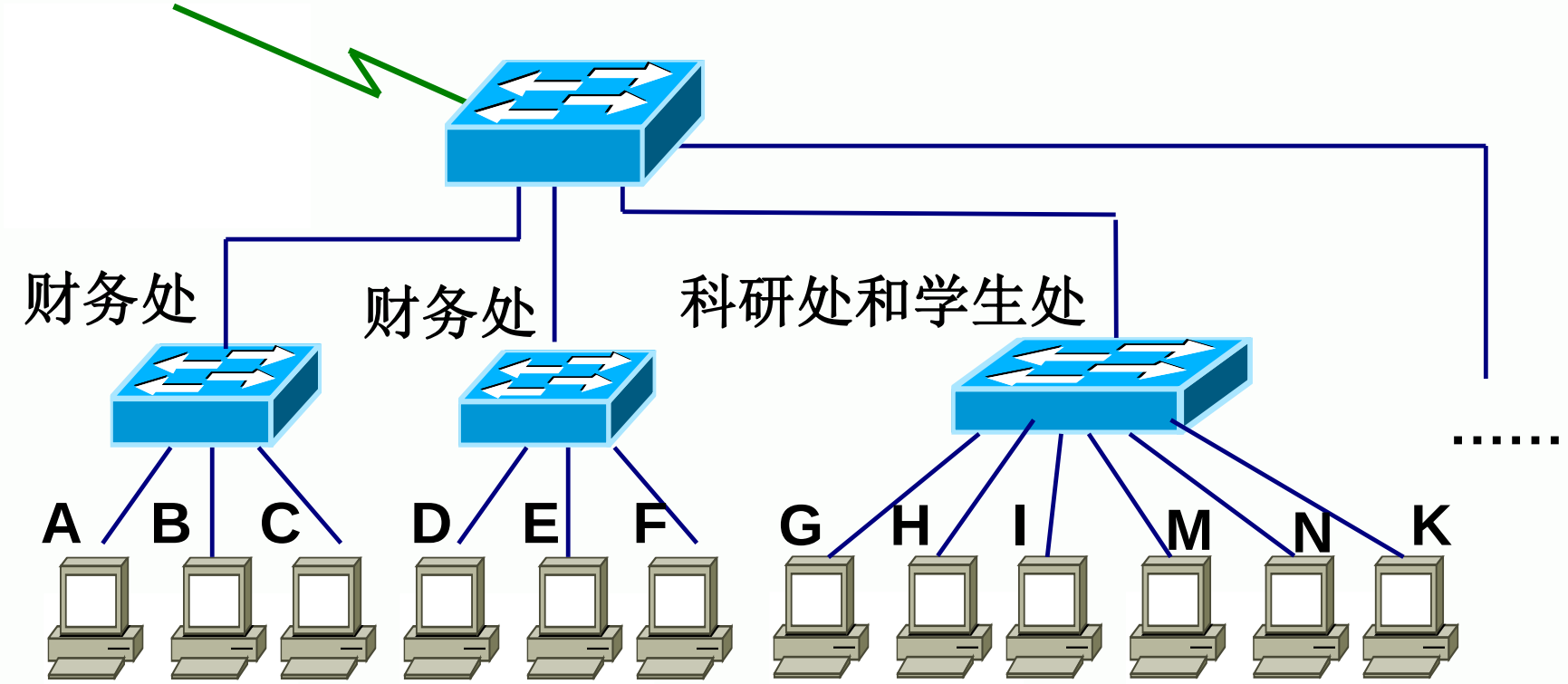
各部门使用独立的交换机

●方案1的分析

- 不同部门之间被彻底分开了；
- 部门之间无法互相访问；
- 有些部门机器较少，但是也要占用一台交换机，总成本提高了。

解决方案2

- 利用子网掩码进行子网划分
- 通过修改各部门机器的IP地址和子网掩码，将各个部门划分到不同的子网中。



A ~ F : 10.0.1.2 ~ 10.0.1.7

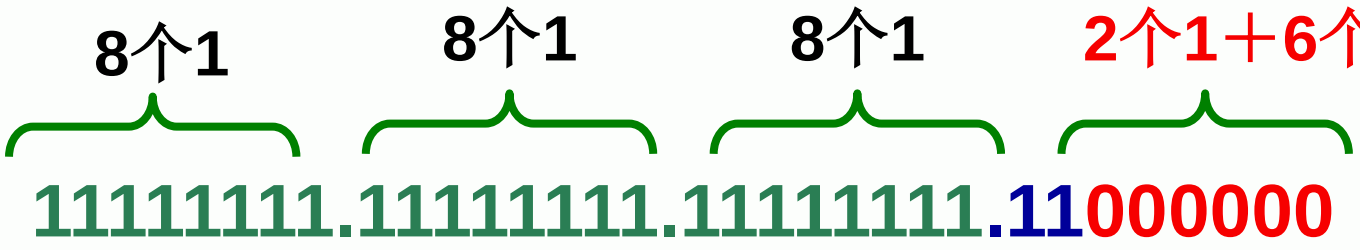
G ~ I : 10.0.1.90 ~ 10.0.1.92

M ~ K : 10.0.1.201 ~ 10.0.1.203

子网掩码： 255.255.255.192

➢ 将一个C类网络分成4个子网络

子网掩码：255.255.255.192



网络位：增加2位，表示原网络被分成4个子网。

主机位：6位，表示每个子网里可以有2^6 -2个主机

子网1：10.0.0.0 ~ 10.0.0.63

子网2：10.0.0.64 ~ 10.0.0.127

子网3：10.0.0.128 ~ 10.0.0.191

子网4：10.0.0.192 ~ 10.0.0.255

子网掩码： 255.255.255.192

	11111111.11111111.11111111.11	000000
10.0.1.2	00001010.00000000.00000001.00	000010
10.0.1.90	00001010.00000000.00000001.01	011010
10.0.1.201	00001010.00000000.00000001.11	001001

根据上面的分析，如果子网掩码是255.255.255.192的话，上面三个IP地址不在同一网络内

●方案2的分析

- 由于不在一个子网，所以各部门之间无法互相访问；
- 机器较少的部门可以和其他部门共用一台交换机，不提高总成本。
- 但是，用户可以自行修改IP地址和子网掩码，不好控制。

●关于上述问题的引申分析

1. 属于同一网络内的计算机，可以直接通信，它们属于同一个广播域；
2. 将不同部门分别连接在相互独立的交换机上，可以有效隔离广播，但成本较高。能否在不过多增加网络成本的前提下，找到一个隔离网络广播域的方法？

●关于上述问题的引申分析

3. 缺省情况下，交换机的所有端口属于同一个广播域；
4. 能否想办法，使同一交换机的端口属于不同[illegible]络管理员
5. 这样，不同部门的网络可以连接在同一交换机上，而且相互之间不在同一个广播域内。即属于不同的子网。

能否把一台交换机当成多台交换机来使用？

把一个交换机分成多个交换机，每个就可以理解成一个虚拟交换机，一台交换机组成的网络称为LAN，那么这种虚拟交换机组成的网络就是虚拟的LAN，简称VLAN。

- 使用VLAN技术，就可以实现前面的构想。

4.3　虚拟局域网(VLAN)

- 4.3.1　什么是VLAN?
- 4.3.2　如何划分VLAN
- 4.3.3　VLAN的优点

4.3.1 什么是VLAN?

VLAN（Virtual Local Area Network）

中文名：虚拟局域网

VLAN是一种将局域网交换机从逻辑上划分成一个个网络段，从而实现虚拟工作组的数据交换技术。

4.3.1 什么是VLAN?

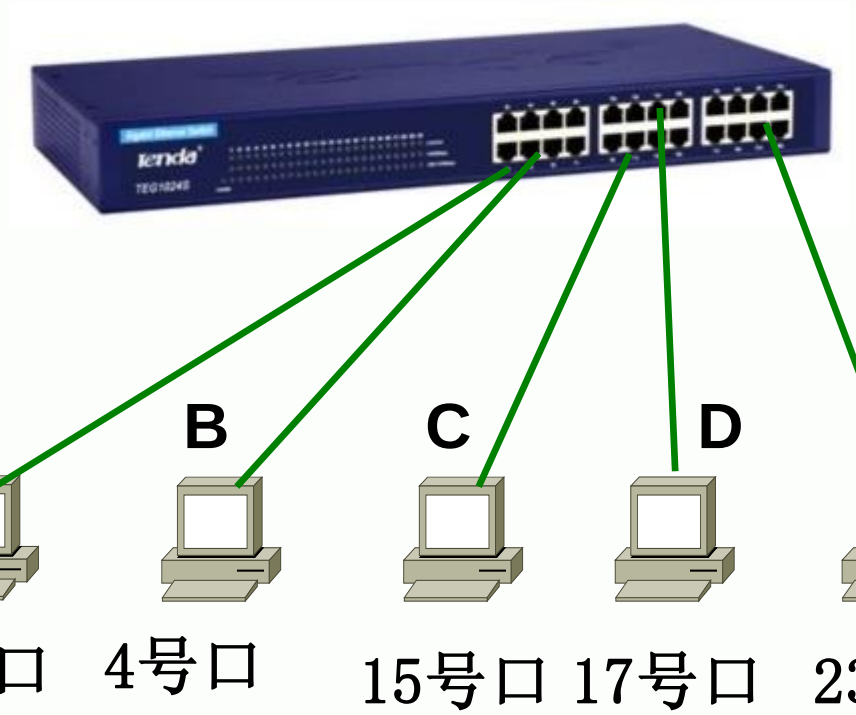
- 在物理网络基础架构上，利用交换机的功能，配置网络的逻辑拓扑结构，即人为的将一个物理的LAN逻辑地划分成不同的广播域（一个站点发送的广播信息，域中的所有站点都能听到）。
- 每一个VLAN都包含一组有着相同需求的计算机。这些计算机不一定属于同一个物理LAN网段。

举例说明

A B C D E

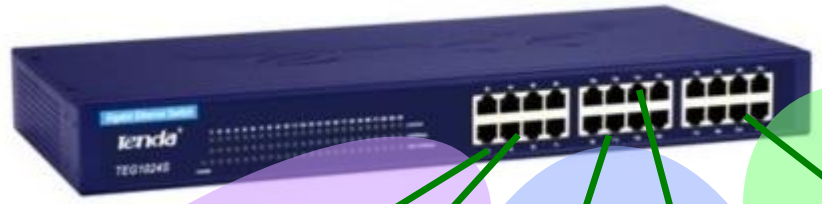
2号口 4号口 15号口 17号口 23号口

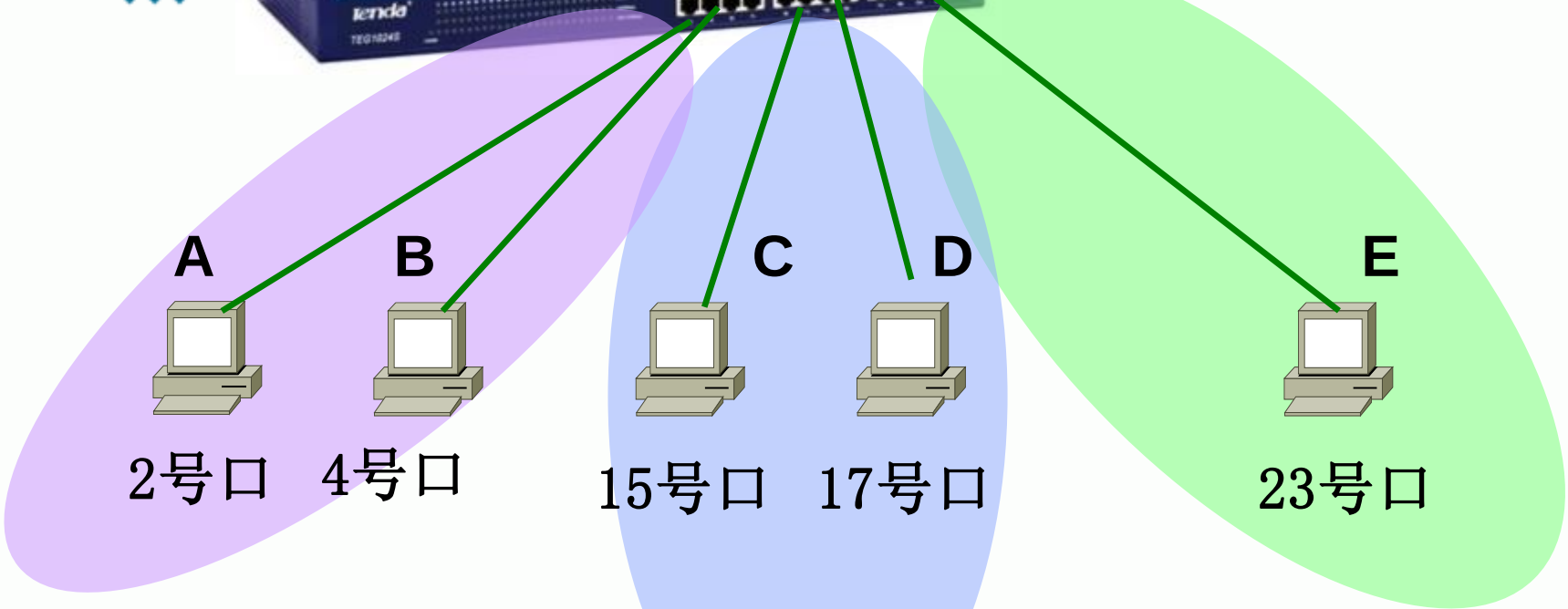
主机 A~E 都连接在一个交换机上，从物理上看，它们属于同一个网络。



例如，将1-10号划分到VLAN1，将11-20号口划分到VLAN2，将21-24划分到VLAN3。

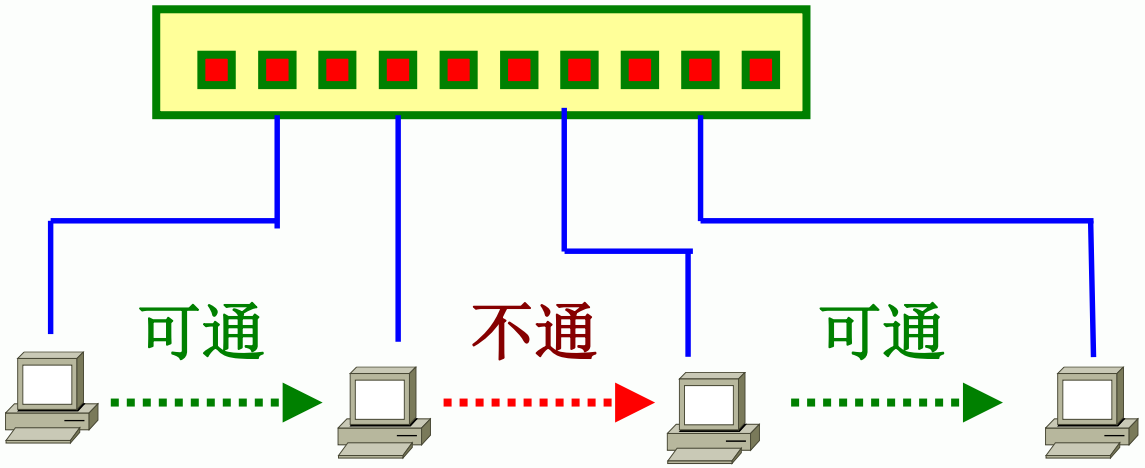
利用交换机的VLAN功能，管理员可以将这个物理的网络逻辑的分割成不同的虚拟局域网(VLAN)。





- A和B属于同一个VLAN，在同一个广播域内
- C和D属于同一个VLAN，在同一个广播域内
- E属于第3个VLAN，在另一个广播域内

VLAN划分以前达到的效果

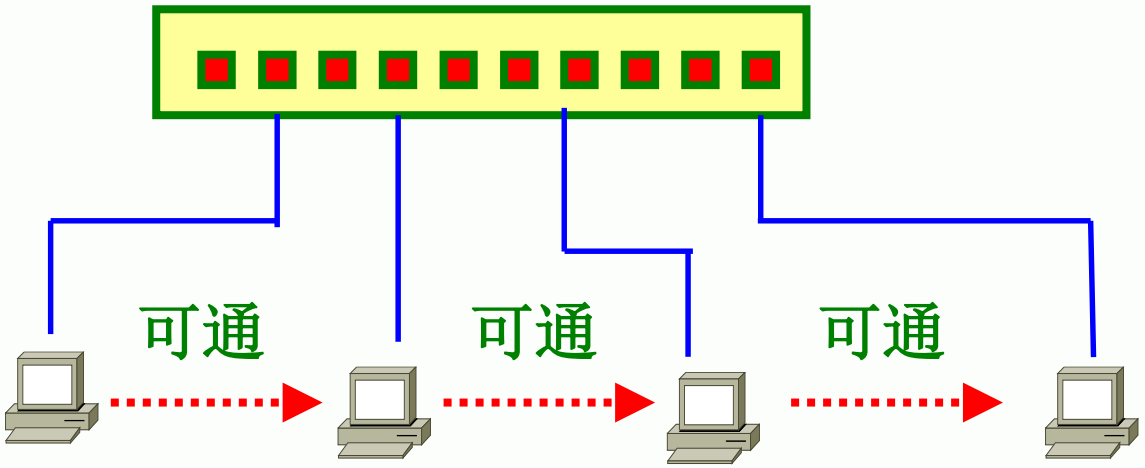


A(2号) B(4号) C(15号) D(17号)

10.0.1.2 10.0.1.4 10.0.1.200 10.0.1.210

子网掩码： 255.255.255.128

VLAN划分以前达到的效果

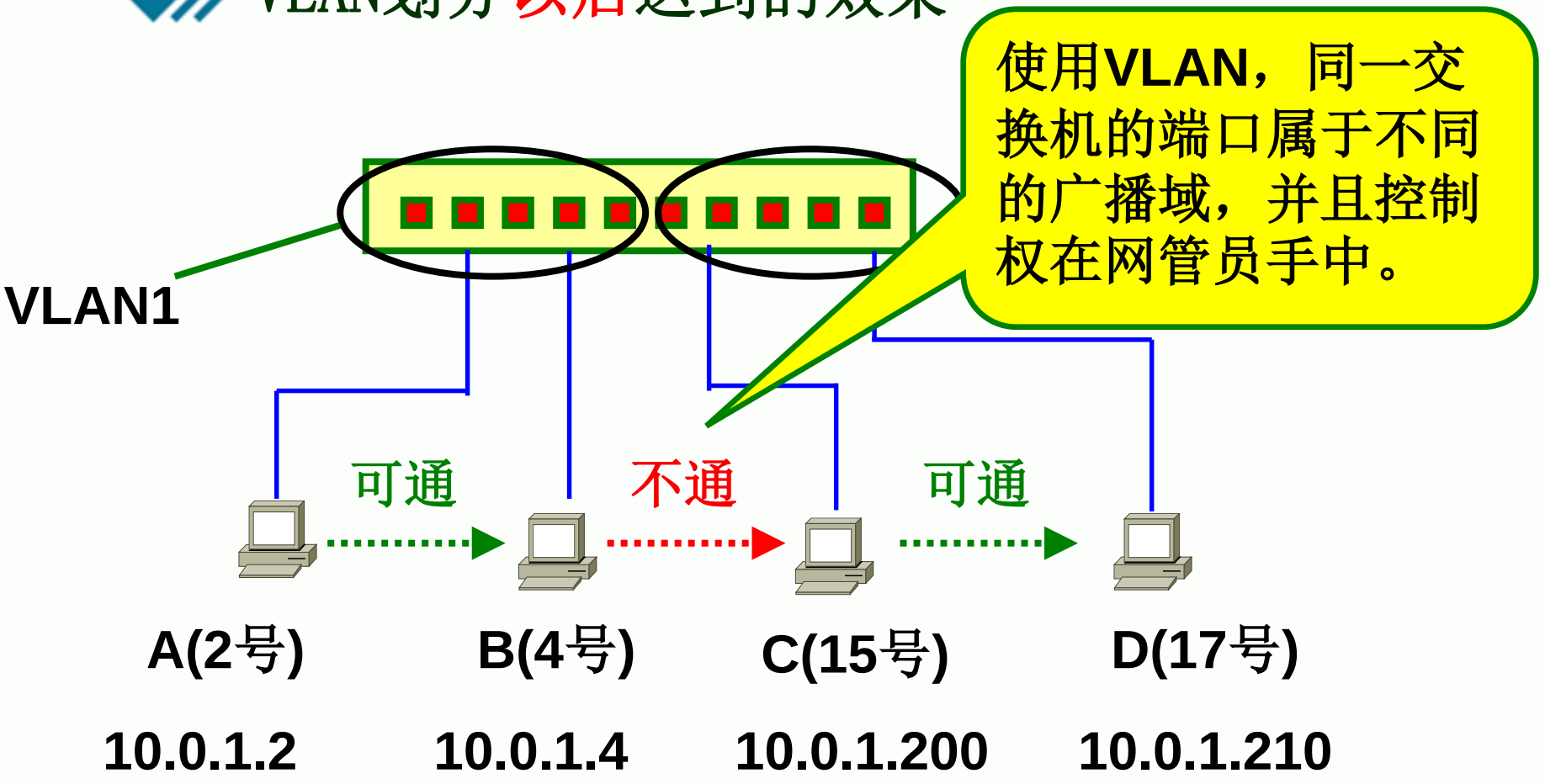


A(2号) B(4号) C(15号) D(18号)

10.0.1.2 10.0.1.4 10.0.1.200 10.0.1.210

子网掩码： 255.255.255.0

VLAN划分以后达到的效果



子网掩码： 255.255.255.0

4.3.2　如何划分VLAN

4.3.2　如何划分VLAN

- 1. 基于交换机端口划分VLAN
- 2. 基于主机MAC地址划分VLAN

常用的有两种方法

4.3.2　如何划分VLAN

- 1、基于交换机端口划分VLAN
  这种方法分为两种划分方式

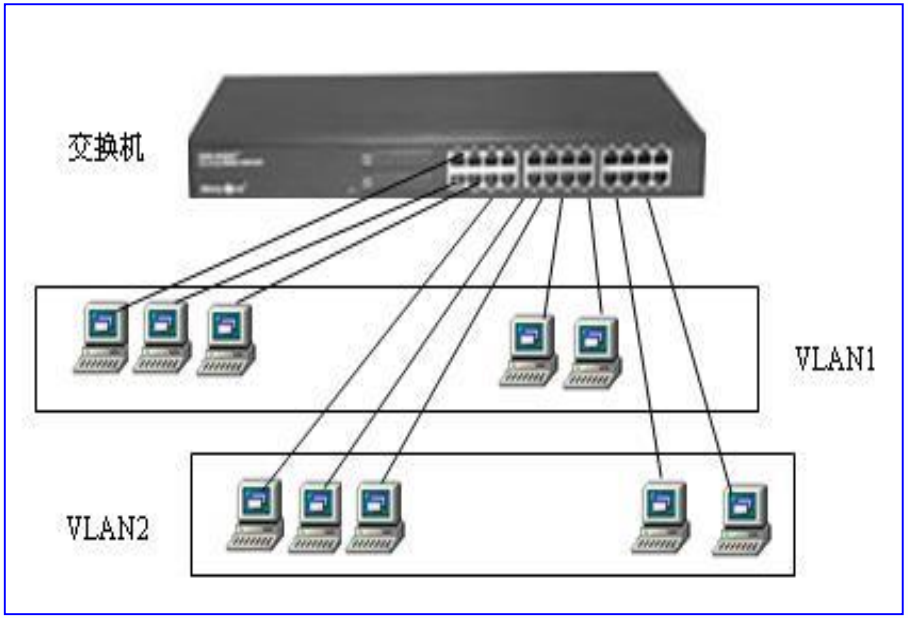
（1）将同一交换机的端口划分成不同的VLAN；

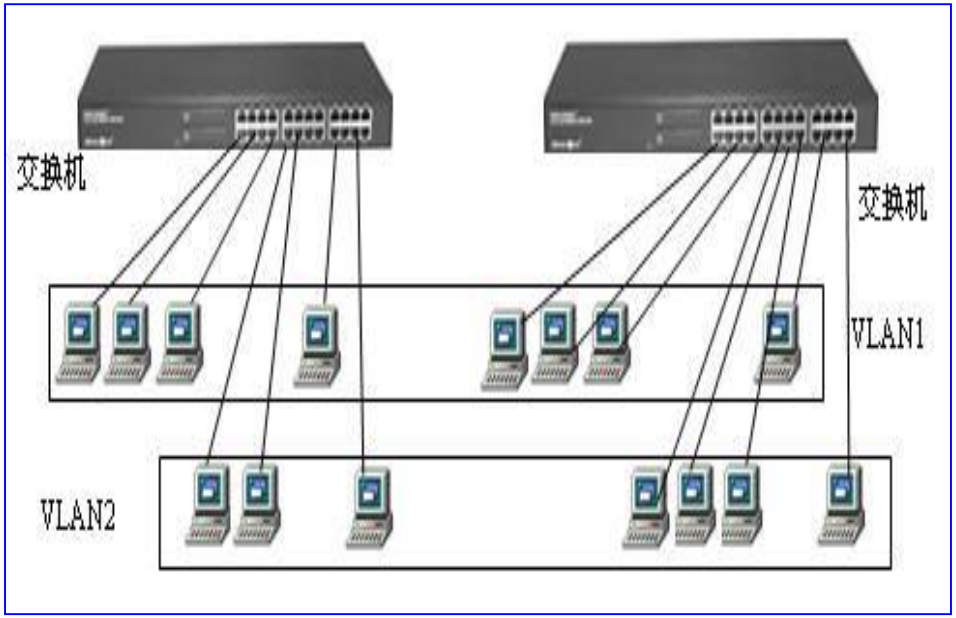
（2）将不同交换机的端口划分成同一个VLAN

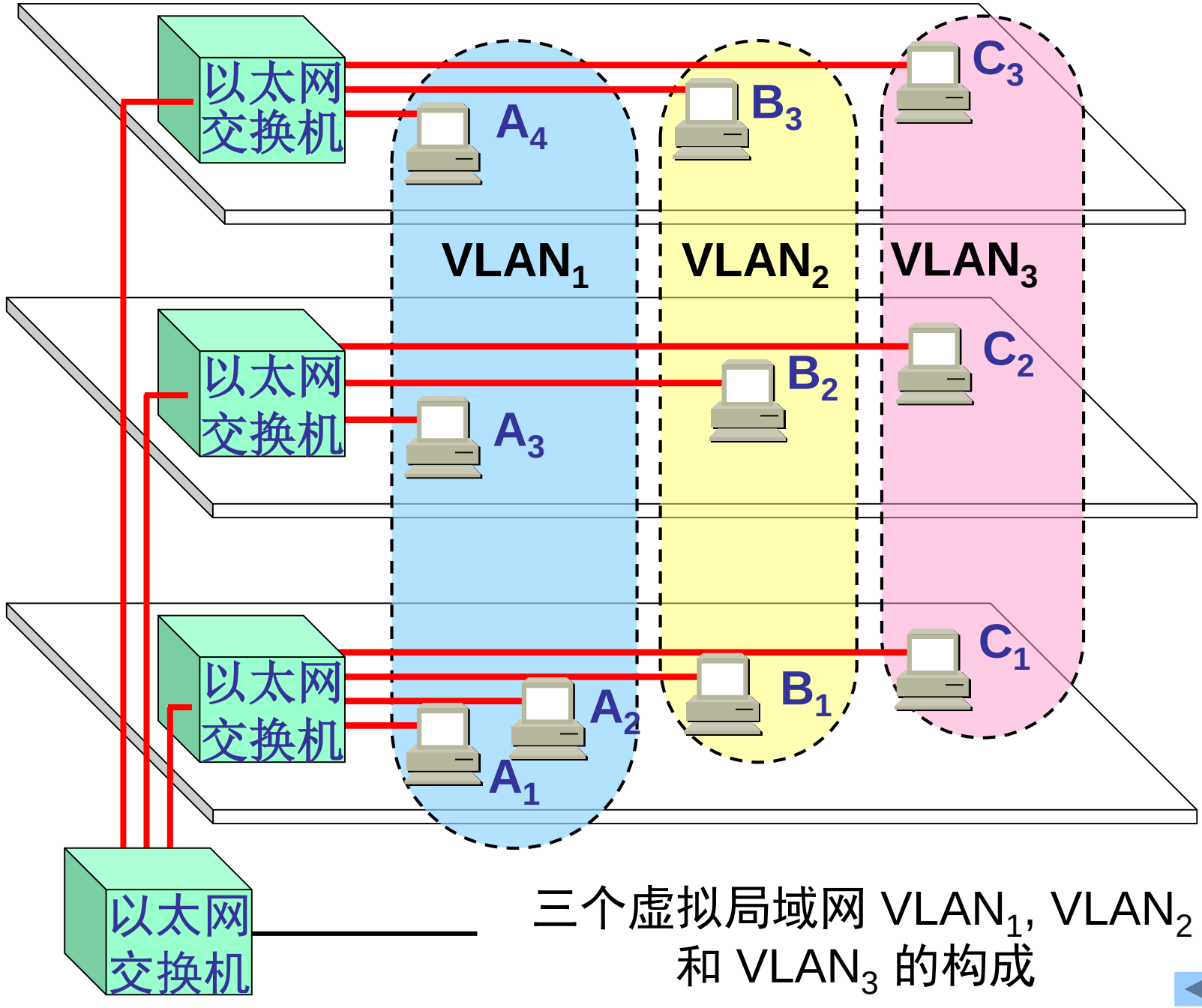
4.3.2 如何划分VLAN

（1）将同一交换机的端口划分成不同的VLAN；

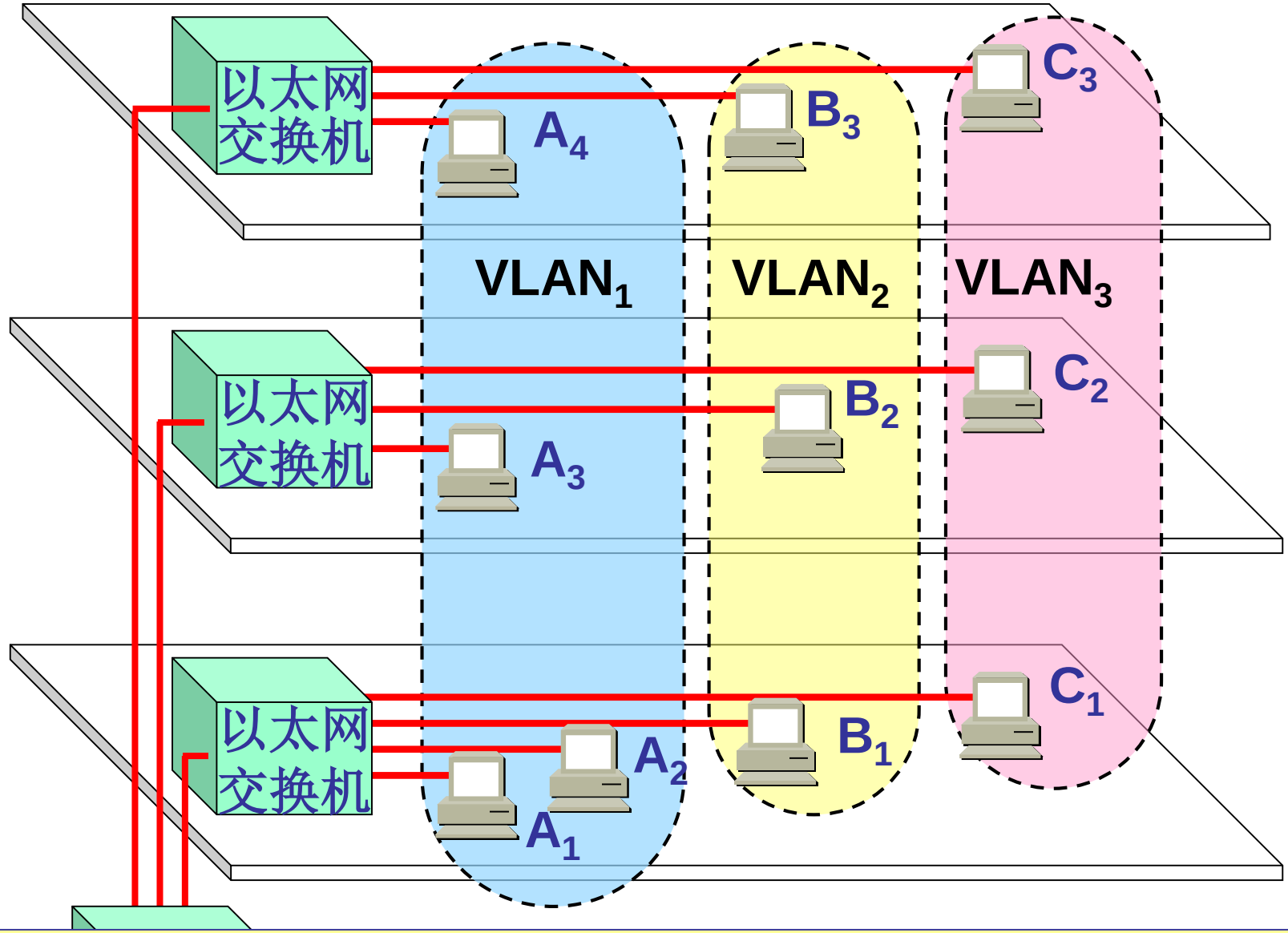
（2）将不同交换机的端口划分成同一个VLAN



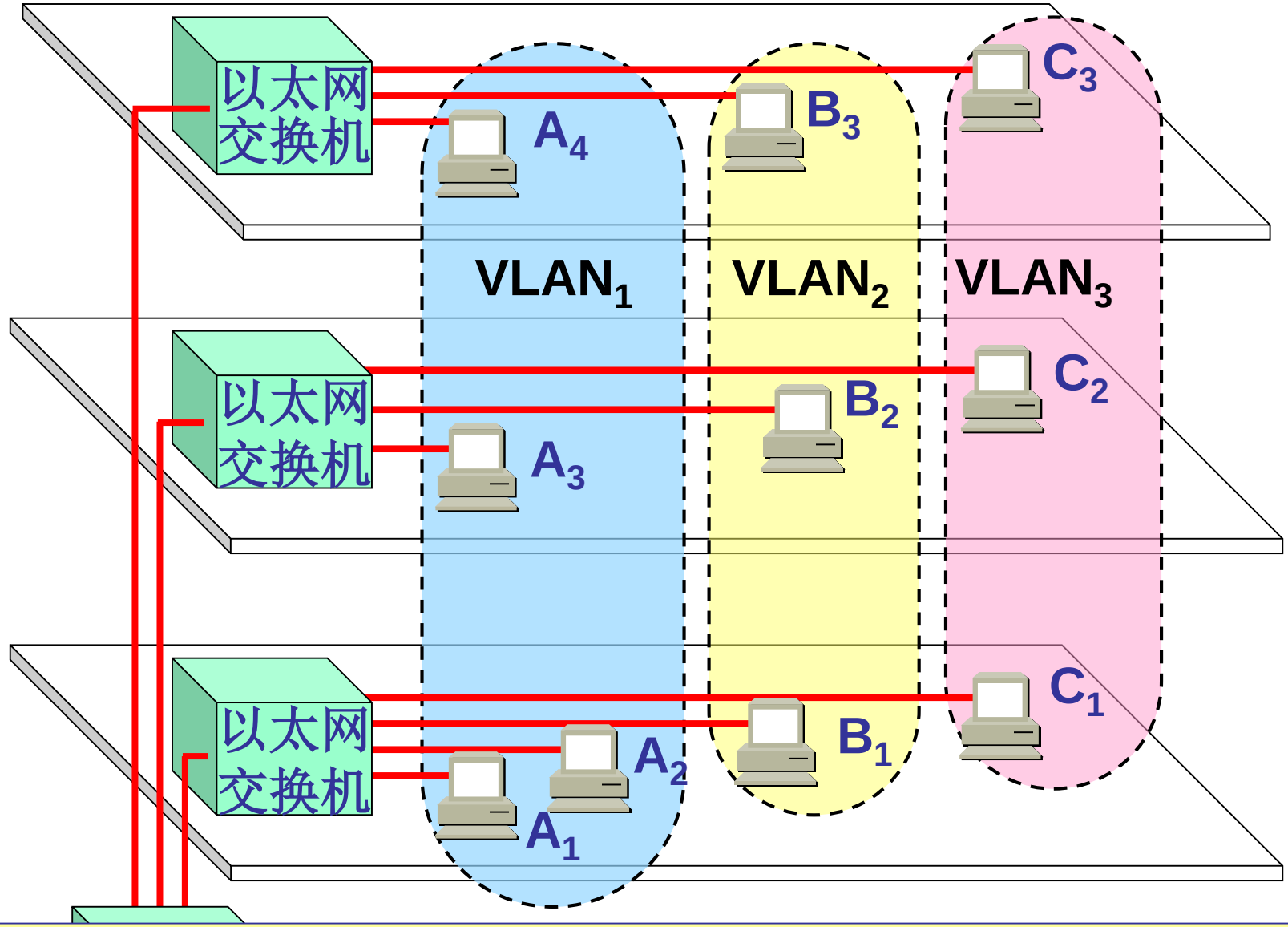




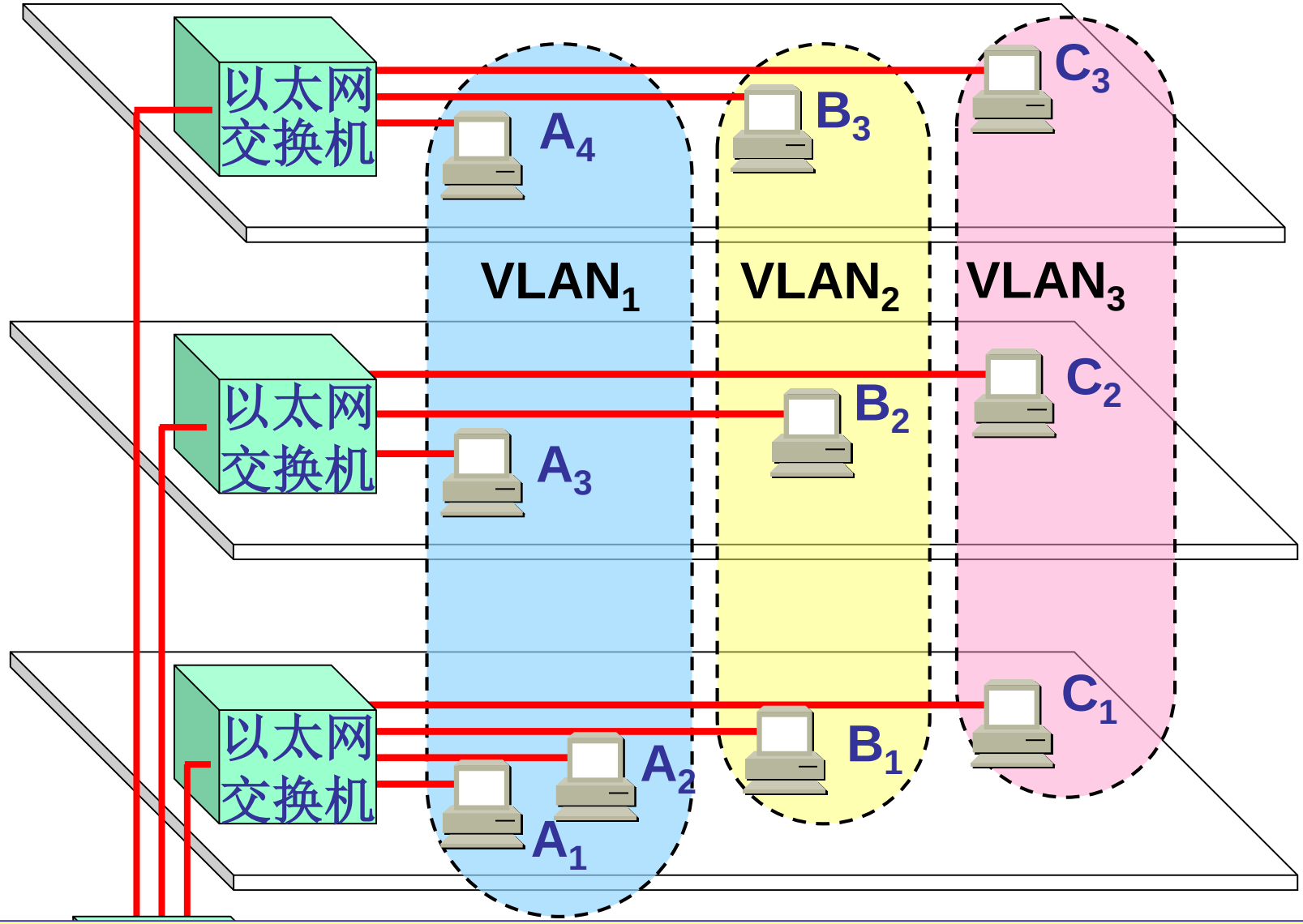
三个虚拟局域网 $VLAN_1$, $VLAN_2$ 和 $VLAN_3$ 的构成



当 B_1 向 $VLAN_2$ 工作组内成员发送数据时，
工作站 B_2 和 B_3 将会收到广播的信息。



B_1 发送数据时，工作站 A_1, A_2 和 C_1 等都不会收到 B_1 发出的广播信息。



虚拟局域网限制了接收广播信息的工作站数，使得网络不会因传播过多的广播信息而引起性能恶化。

4.2.2　如何划分VLAN

1. 基于端口的VLAN

通过将交换机端口设置成不同的VLAN而组建不同的虚拟局域网。

①基于端口的VLAN属于静态VLAN配置，即某个端口固定属于某个VLAN。
②缺点：灵活性不好
③优点：容易配置和维护

4.2.2　如何划分VLAN

- 2、基于机器的MAC地址划分VLAN
  - 这种划分VLAN的方法是根据每个连网主机的MAC地址来配置该主机属于哪个虚拟网。
  - 这种VLAN的划分方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN不用重新配置，因为它是基于用户，而不是基于交换机的端口。这种方法的缺点是初始化时，必须将所有用户的MAC地址进行登记和配置，如果有几百个甚至上千个用户的话，配置是非常麻烦的，另外，若用户更换了机器的网卡，网络管理员必须重新配置VLAN。

4.3.3　VLAN的优点

4.2.3 VLAN的优点

1. VLAN的目的是为了解决以太网的广播问题和安全性而提出的一种协议。
2. 通过将企业网络划分为VLAN，可以控制不必要的数据广播。在共享网络中，一个物理的网段就是一个广播域。而在交换网络中，广播域局限在同一VLAN内，这样可以使网络的拓扑结构变得更加灵活。
3. 不同VLAN之间不能之间通信，因此，VLAN还可以强化网络管理和网络安全，用于控制网络中不同部门、不同站点之间的互相访问。

4.2.3 VLAN的优点

（1）提高管理效率

允许用户工作站从一个地点移动到另一个地点，而无需重新布线。

（2）控制广播数据

在较大规模的网络中，大量的广播信息很容易引起网络性能的降低，甚至导致整个网络的崩溃。

与使用路由器的解决方案相比，VLAN技术具有传输延迟小、价格便宜、维护和管理开销小的优点。

4.2.3 VLAN的优点

（3）增强网络内部的安全性

控制用户访问，控制VLAN的大小和成员，借助网管软件发现非法入侵。

（4）实现虚拟工作组

虚拟工作组是指，企业网络环境下各部门处于各自的VLAN中，即使办公地点不同，部门中的所有成员都可以像处于同一个VLAN上那样进行通信。

- 当某个成员有移动时，如果其工作部门不变，则不用对他的计算机重新配置。
- 如果某个成员调到另一个部门，他可以不改变其工作地点，而只需修改其VLAN成员身份即可。

交换机的重要实验

实验

- VLAN划分实验
  - 登录交换机
  - 基于端口划分VLAN
  - 测试VLAN内部的通信
  - 测试VLAN直接的通信

4.4　认识路由器

返回

4.4 认识路由器

- 4.4.1　路由器的功能
- 4.4.2　路由器的工作原理
- 4.4.3　路由器的组成
- 4.4.4　路由器和交换机的区别

4.4.1 路由器的功能

4.4.1　路由器的功能

问题引入

交换机的“不足”之处

4.4.1　路由器的功能

交换机不能实现不同网络之间的直接通信

4.4.1　路由器的功能

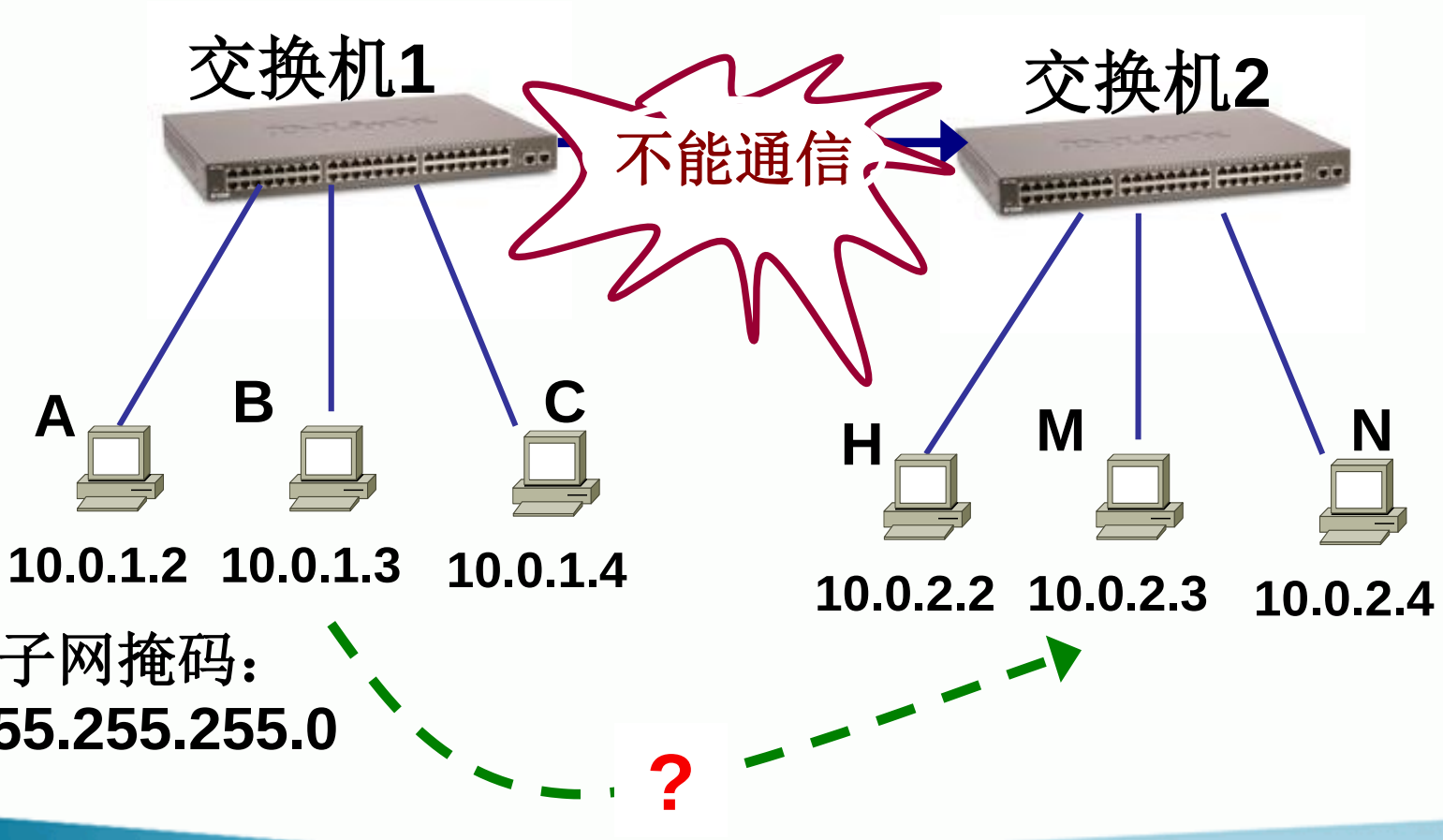
何谓 “不同的网络” ？

4.4.1　路由器的功能

- 回忆一下：
  - 局域网和广域网
  - 以太网和令牌环网 （不同类型）
  - 一个以太网中的两个不同子网（IP地址的网络号不同）
  - 两个VLAN

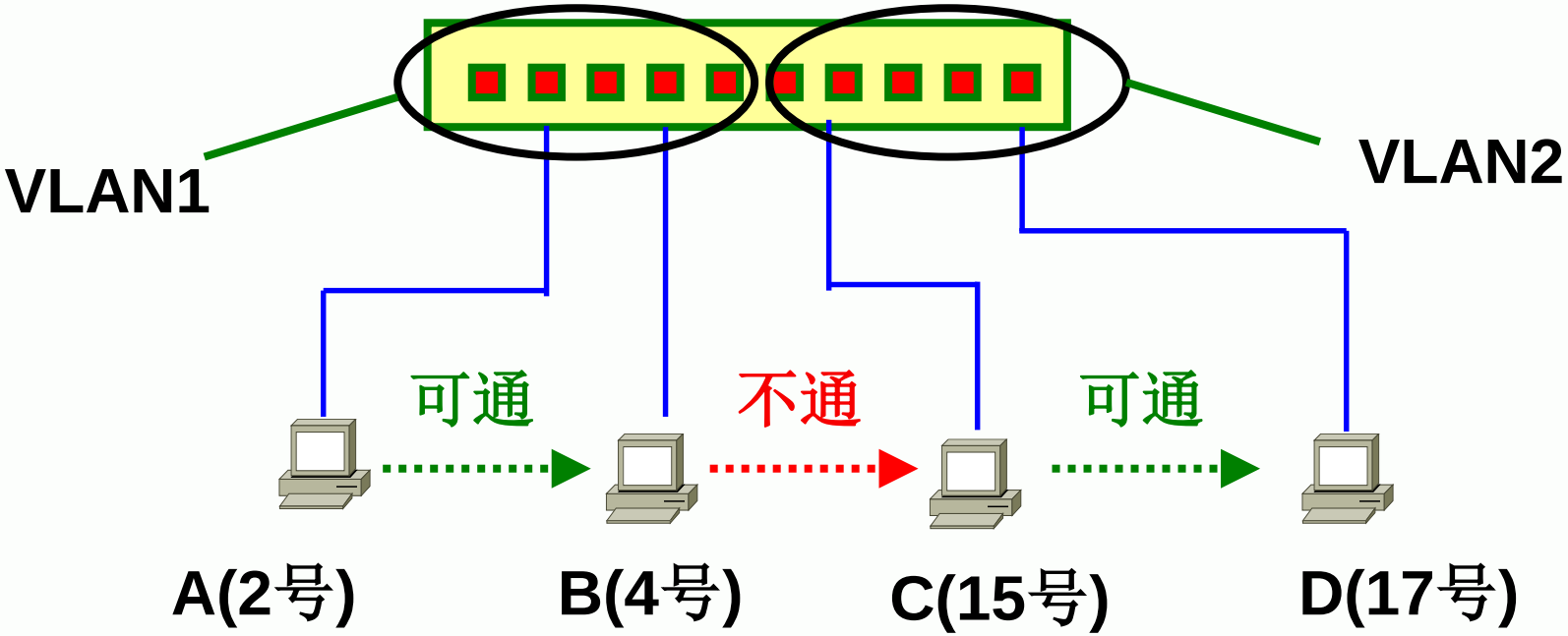
4.4.1 路由器的功能

例1



VLAN划分以后达到的效果

例2



4.4.1　路由器的功能

- 提出问题：

不同网络间通过什么设备进行互连通信？

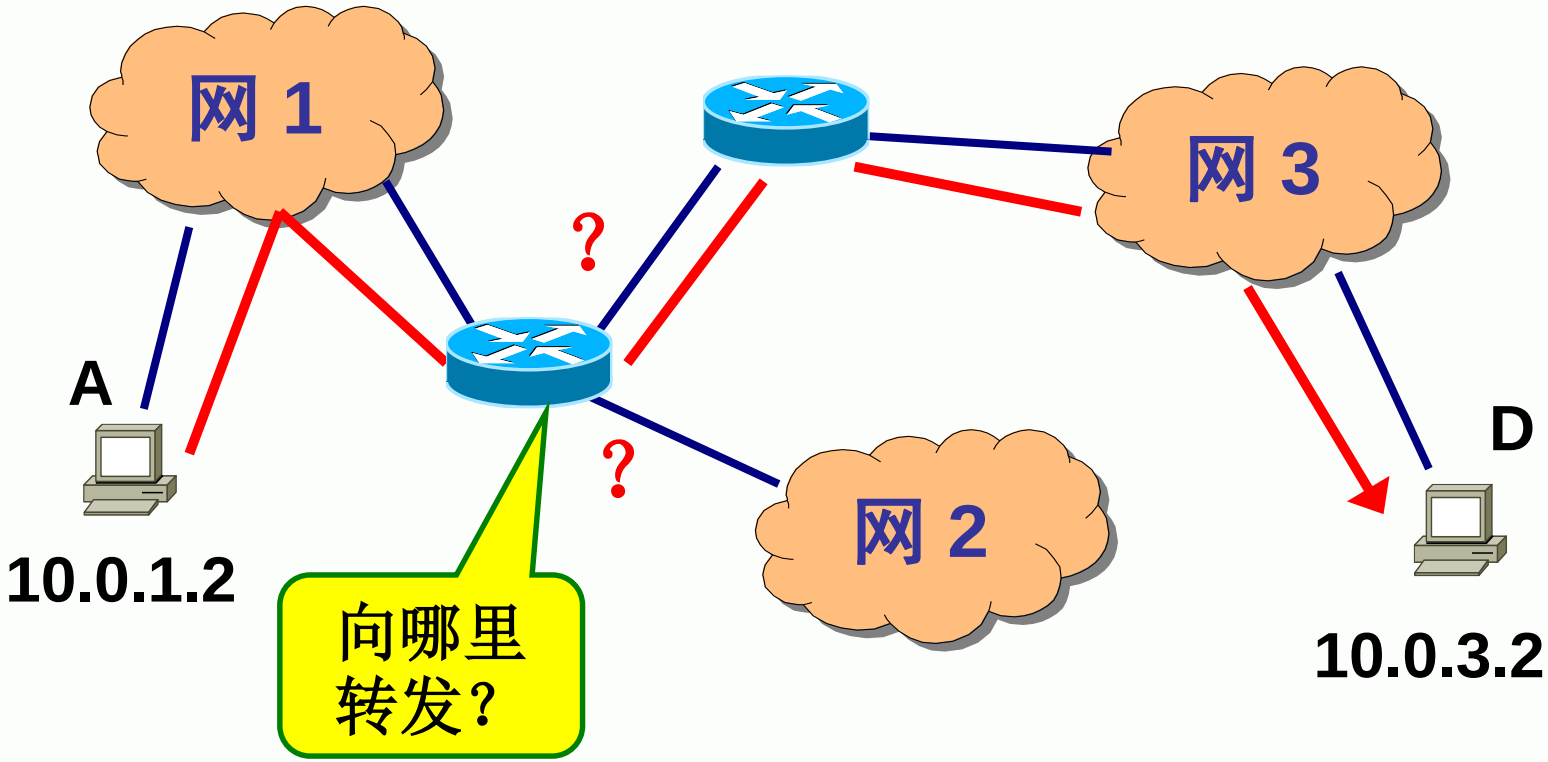
认识路由器

2.4.1 什么是路由器？

- 什么是路由器？

是什么把网络相互连接起来？是路由器。路由器英文名**Router**，是互联网的主要节点设备。路由器通过执行路由选择策略，来决定把收到的数据转发到哪个网络。

2.4.1 什么是路由器？



路由

4.4.1　路由器的功能

- 路由器的功能
  1. 改进网络分段，即可根据实际需求将整个网络分割成不同的子网。
  2. 提供不同类型网络的互联。
  3. 隔离广播风暴。
  4. 支持子网间的信息传输。
  5. 提供安全访问的机制。

4.4.1　路由器的功能

路由器（Router）

- 网络层设备，用于连接多个逻辑上分开的网络。
- 逻辑网络是代表一个单独的网络或者一个子网。
- 路由器具有判断网络地址和选择路径的功能，它能在多网络互联环境中建立灵活的连接，可用于连接数据分组和介质访问方法完全不同的各种子网（即异构型网络）。

4.4.2 路由器的工作原理

2.4.2 路由器的工作原理

- 提出问题？
  - 路由器是如何工作的？

4.4.2　路由器的工作原理

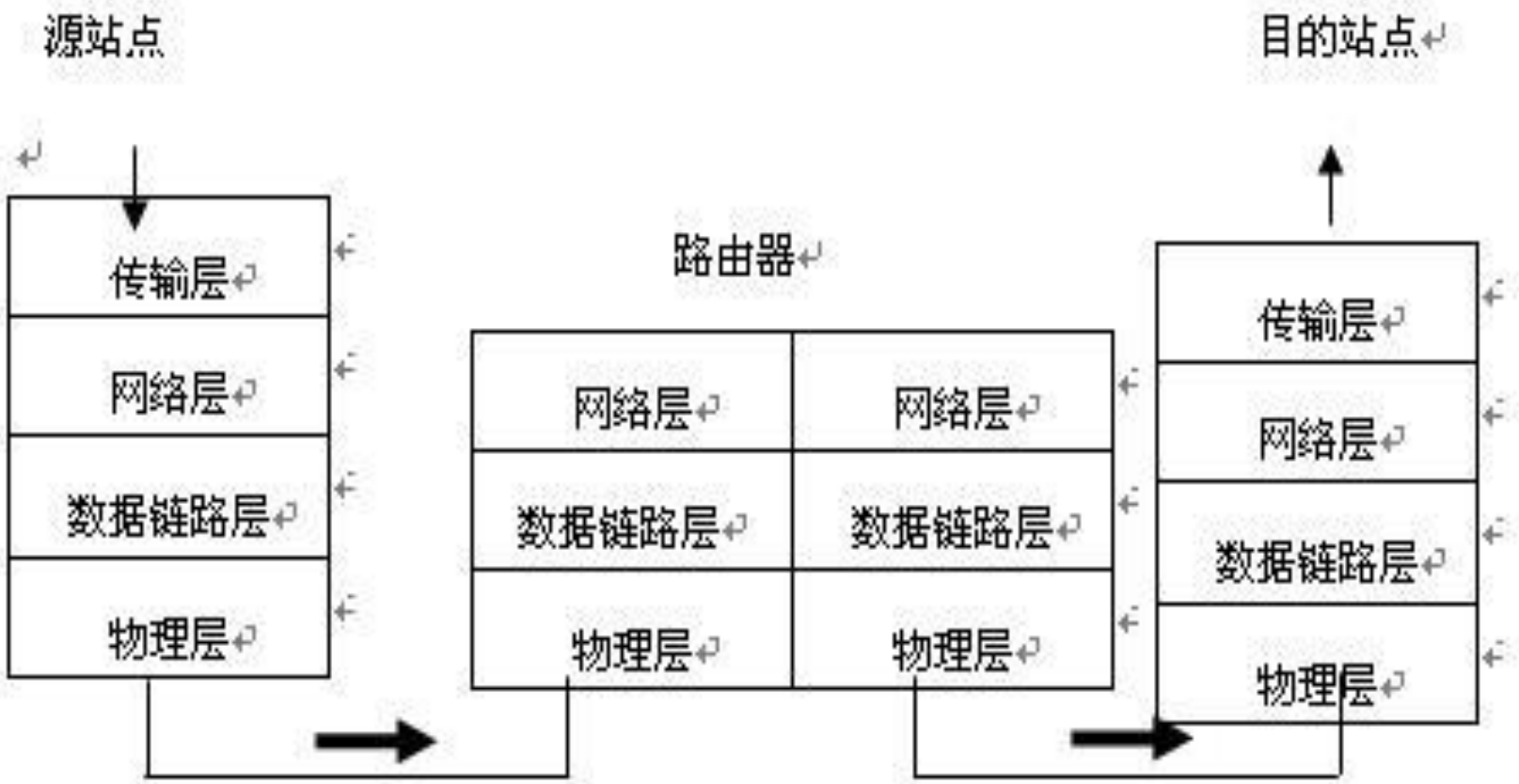
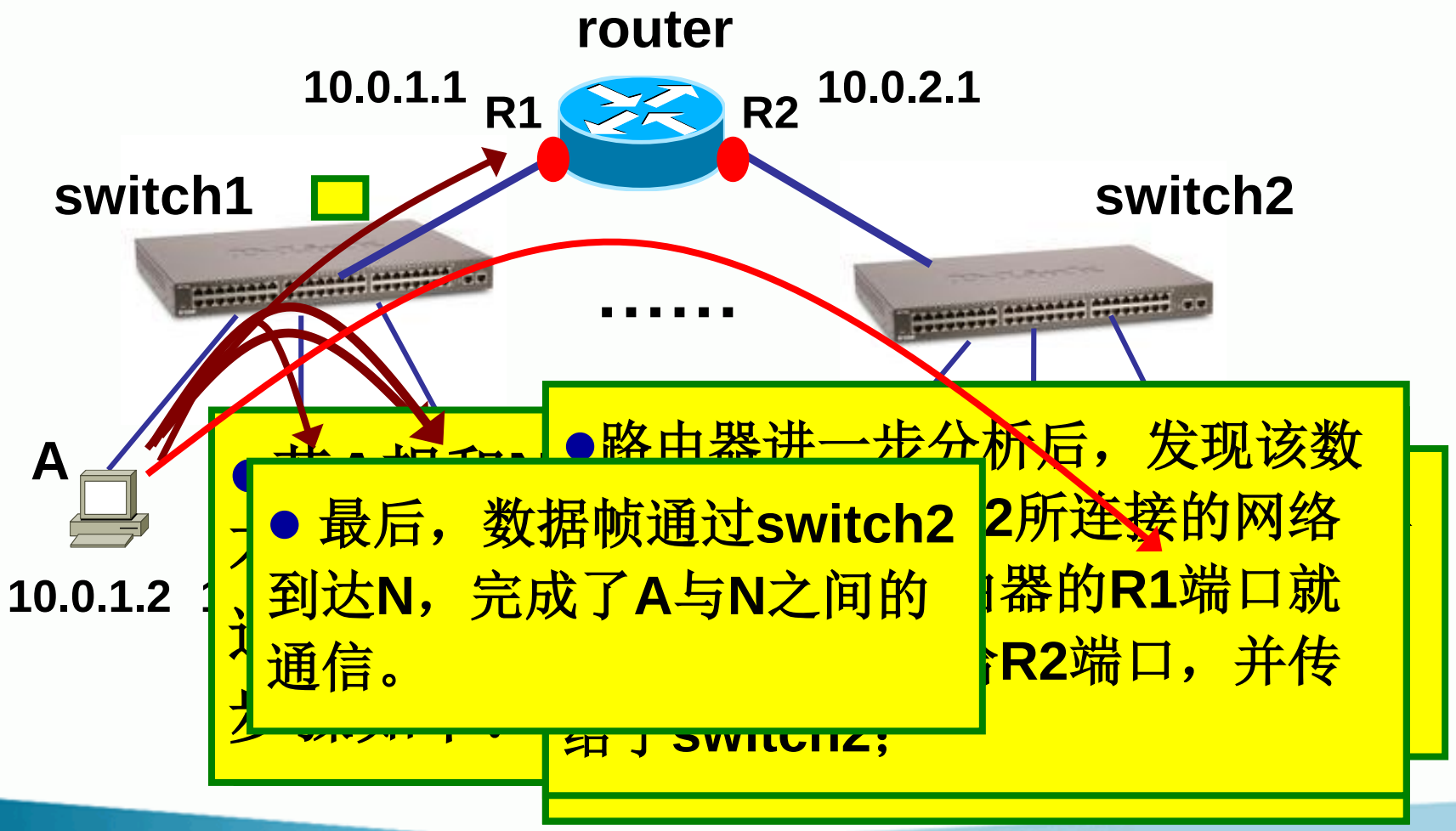


图 4-12　在路由器的体系结构中转发数据的过程

4.4.2 路由器的工作原理



4.4.2　路由器的工作原理

路由器进行路由选择的关键是有一个保存路由信息的数据库：**路由表**，它包含了互联网络中各个子网的地址、到达各子网所经过的路径以及与路径相联系的传输开销等内容。

4.4.2　路由器的工作原理

一个路由器有多个网络接口，当某个接口上收到一个分组时，它就根据目的网络地址到路由表中查找其对应的转发接口。这种根据分组的目的网络地址查找路由表，最终决定分组转发路径的过程称为**路由选择**。

4.4.2　路由器的工作原理

- 当路由器接收到IP数据报时，先取出目的主机的IP地址，再计算出目的主机所在网络的网络地址，然后用网络地址来查找路由表以决定通过哪一个接口转发该IP数据报。
- 作为中间节点的路由器为了选择分组的转发路径，必须了解**网络的拓扑**连接情况。因此，中间路由器只要知道目的网络地址，只有到达目的网络时才会用到主机地址。

4.4.2　路由器的工作原理

路由算法

建立和更新路由表的算法。

互联网中各个网络和它们之间相互连接的情况经常会发生变化，因此路由表中的信息需要及时更新。

动态路由： 在运行过程中由路由器来动态建立和更新路由表；

静态路由： 由网络管理员预先设置好路由表。

4.4.3 路由器的组成

4.4.3 路由器的组成

（1）CPU：中央处理单元，是路由器的控制和运算部件。

（2）RAM/DRAM：内存，用于存储临时的运算结果。如路由表、ARP表、快速交换缓存、缓冲数据包、数据队列、当前配置文件。

（3）Flash Memory：可擦除、可编程的ROM，用于存放路由器的操作系统IOS。

4.4.3 路由器的组成

（4）NVRAM：非易失性RAM，用于存放路由器的配置文件。

（5）ROM：只读存储器，存储了路由器的开机诊断程序、引导程序和特殊版本的IOS软件。

（6）接口：用于网络连接。

Cisco路由器的操作系统称为IOS（Internetwork Operating System，网络互联操作系统）。

4.4.4 路由器与交换机的区别

4.4.4　路由器与交换机的区别

- 提出问题：

　　路由器与交换机都是用于连接的网络设备，它们有什么区别呢？

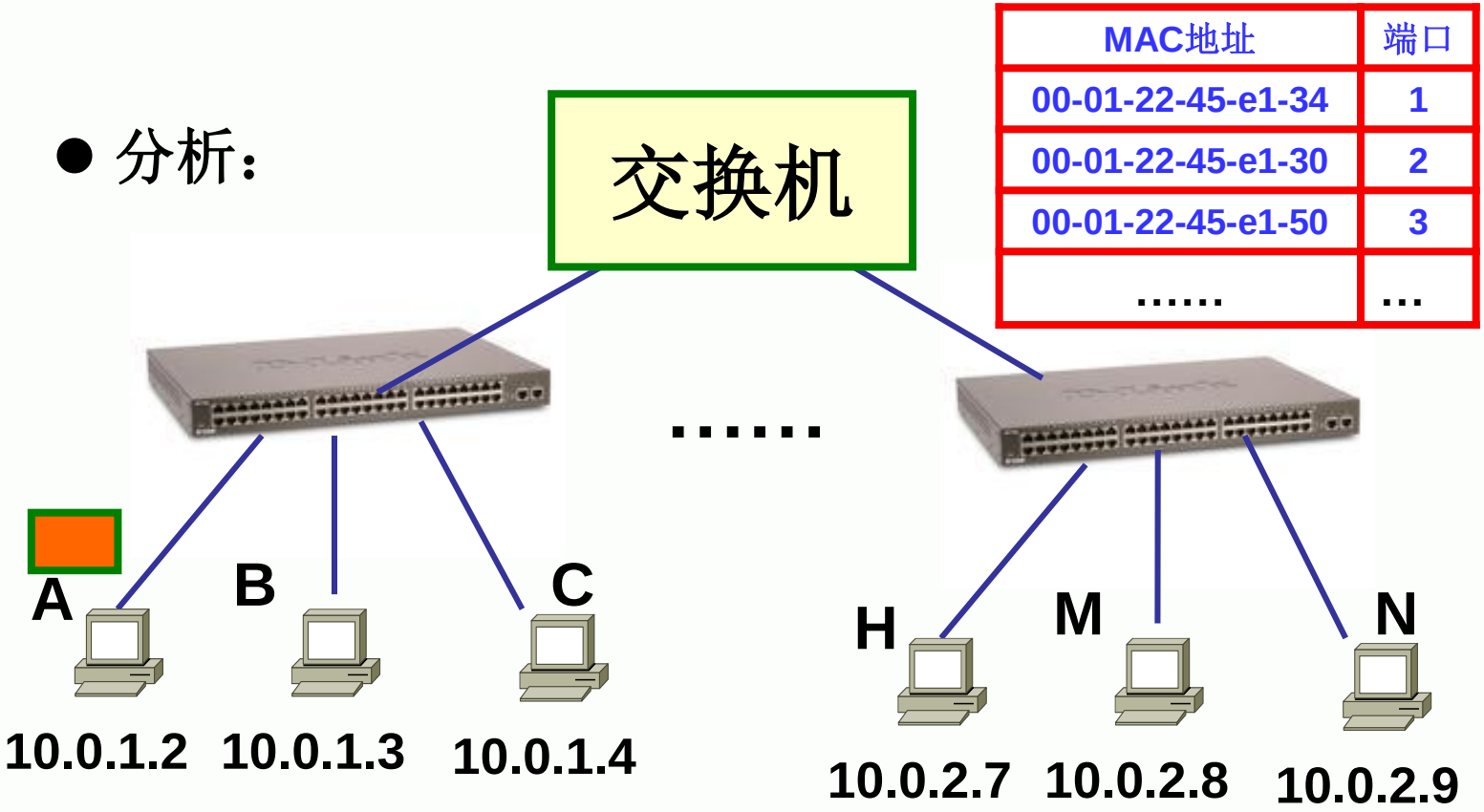
4.4.4　路由器与交换机的区别

- 数据转发所依据的对象不同

交换机是利用物理地址或者说MAC地址来确定转发数据的目的地址。而路由器则是利用不同网络的ID号（即IP地址）来确定数据转发的地址。

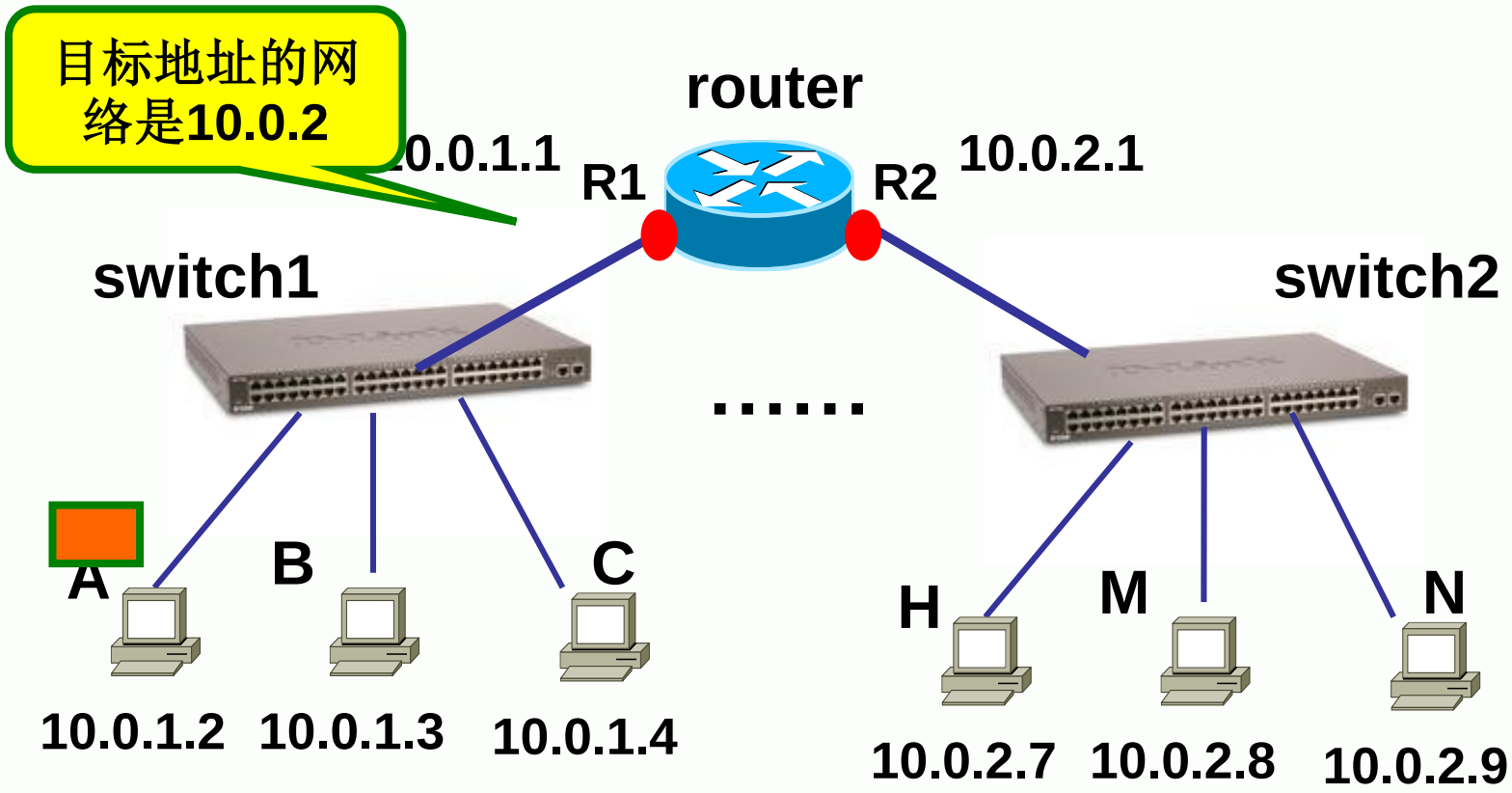
4.4.4 路由器与交换机的区别

- 分析：



子网掩码：255.255.0.0

4.4.4 路由器与交换机的区别



子网掩码：255.255.255.0

4.4.4　路由器与交换机的区别

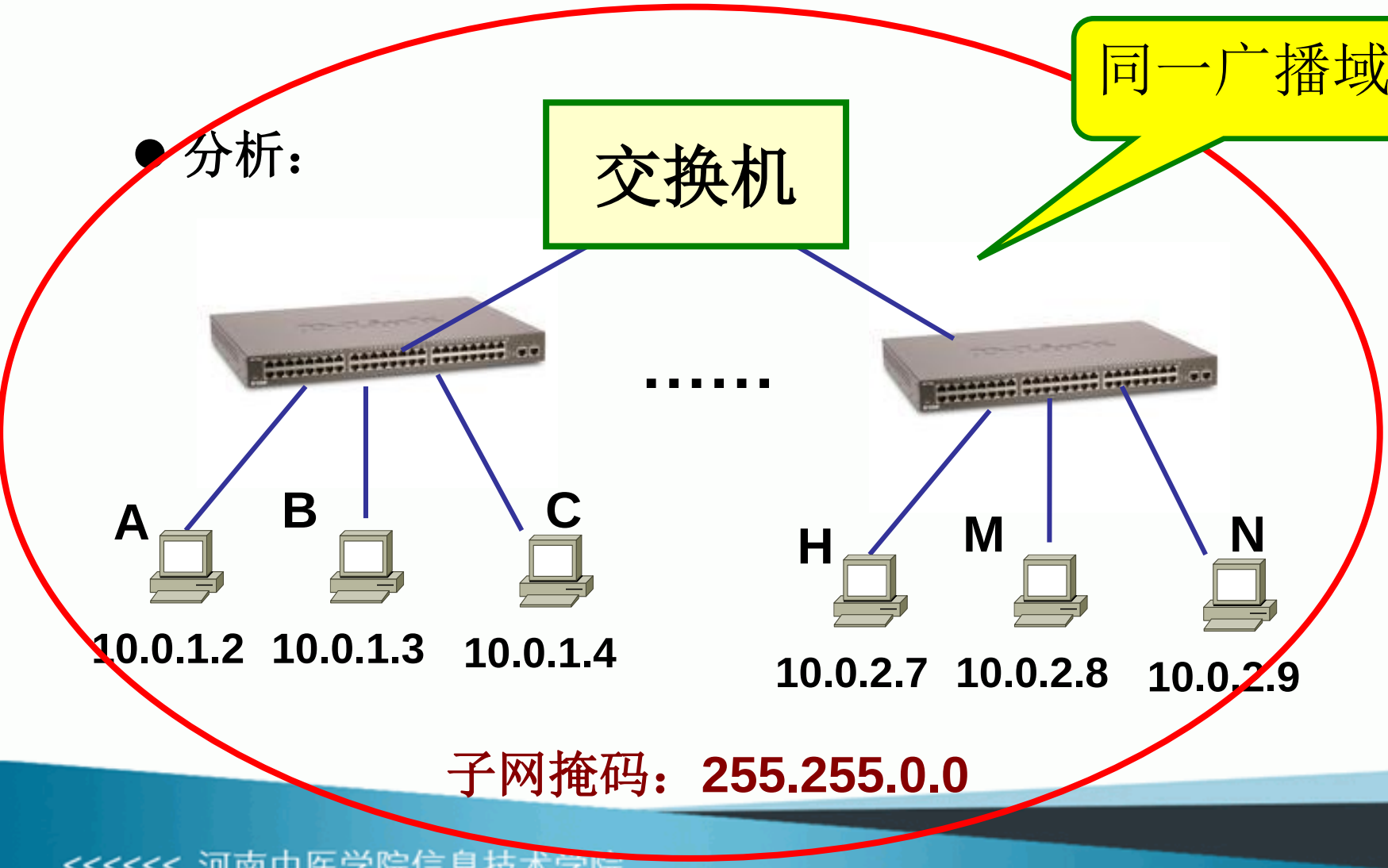
➢分割冲突域与广播域

交换机只能分割冲突域，不能分割广播域；而路由器可以分割广播域。

由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。

4.4.4 路由器与交换机的区别

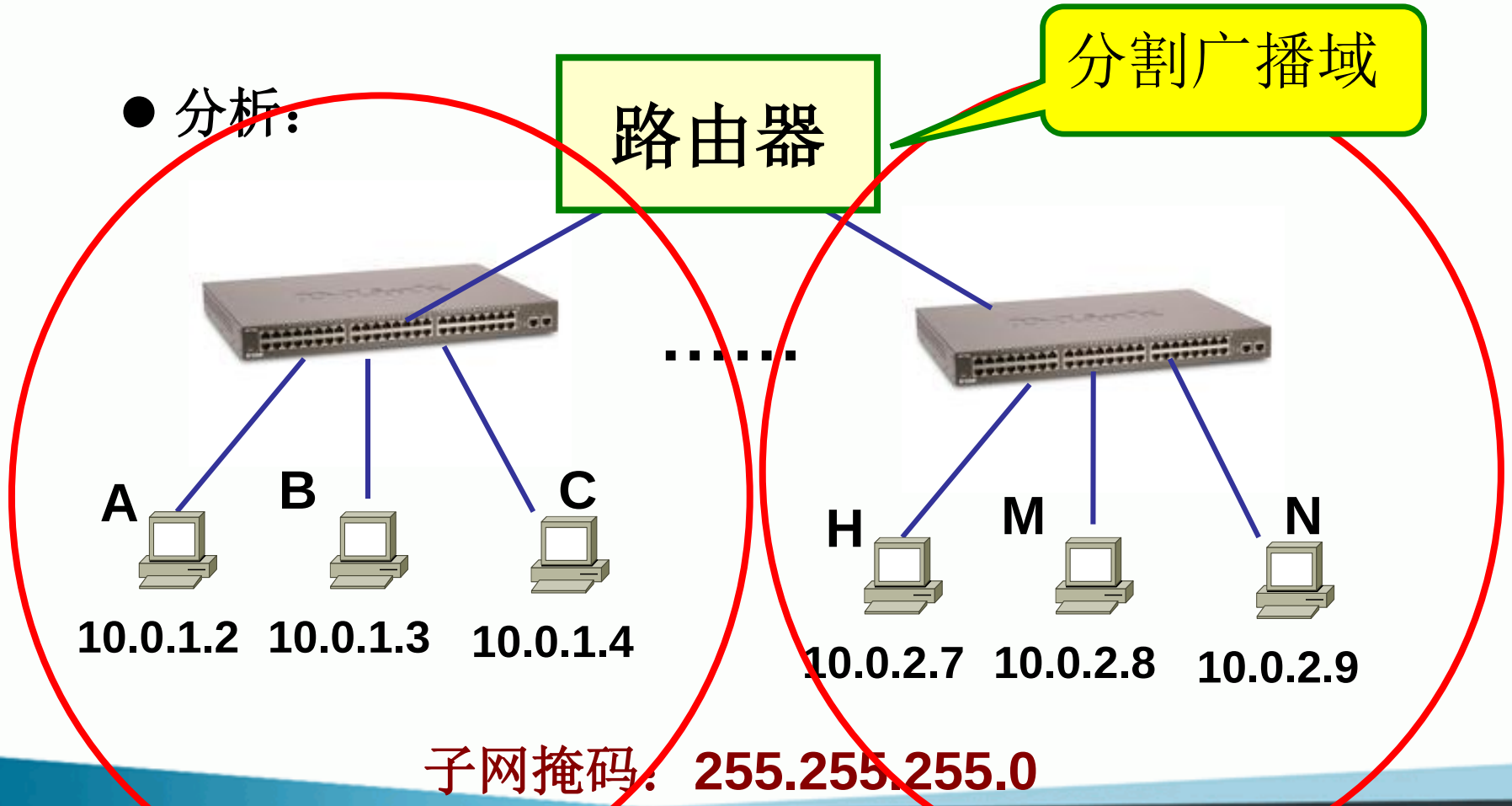
- 分析：



子网掩码：255.255.0.0

4.4.4 路由器与交换机的区别

- 分析：



4.4.4　路由器与交换机的区别

- 在OSI/RM中对应的层次不同
  - 交换机工作在数据链路层。
  - 路由器工作在网络层

4.5　路由基础

4.5.1　路由表
4.5.2　静态路由与动态路由
4.5.3　自治系统AS
4.5.4　IGP与EGP

4.5　路由基础

4.5.1　路由表
4.5.2　静态路由与动态路由
4.5.3　自治系统AS
4.5.4　IGP与EGP

4.5　路由基础

4.5.1　路由表

- 路由动作包括两项基本内容：寻径和转发。
- **寻径**即指路由器使用各种方法获取有关网络的方位信息，这样，每一个路由器才可以成为一个真正意义上的数据转发中继点。
- **寻径的结果**让路由器**形成**了有效的**路由表**，从而变得真正智能起来，并因此提供了路由器指挥数据包转发通路的依据。

4.5　路由基础

4.5.1　路由表

- 路由动作包括两项基本内容：寻径和转发。
- **寻径**即指路由器使用各种方法获取有关网络的方位信息，这样，每一个路由器才可以成为一个真正意义上的数据转发中继点。
- **寻径的结果**让路由器**形成**了有效的**路由表**，从而变得真正智能起来，并因此提供了路由器指挥数据包转发通路的依据。

4.5.1 路由表

【路由表实例】

```
RA_config#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2


VRF ID: 0

C       10.0.1.0/24         is directly connected, FastEthernet0/0
C       10.1.1.0/24         is directly connected, FastEthernet0/3
RA_config#
```

4.5.1 路由表

【路由表实例】

```
RA_config#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2


VRF ID: 0

C       10.0.1.0/24       is directly connected, FastEthernet0/0
C       10.1.1.0/24       is directly connected, FastEthernet0/1
RA_config#
```

4.5.1　路由表

【路由表实例】

上图中显示的就是一个路由表信息，其中Code：后面的内容表示在接下来的表项中最前面的一列的字母缩写的含义。例如：

C 表示此条路由信息由直连网络的IP地址自动写入路由表。也就是说路由器的f0/0短裤中配置的地址为10.0.1.0网络的某个地址，而f0/3端口配置了10.1.1.0网络中的某个地址。

S 表示此项路由信息是由管理员静态手动添加构成。

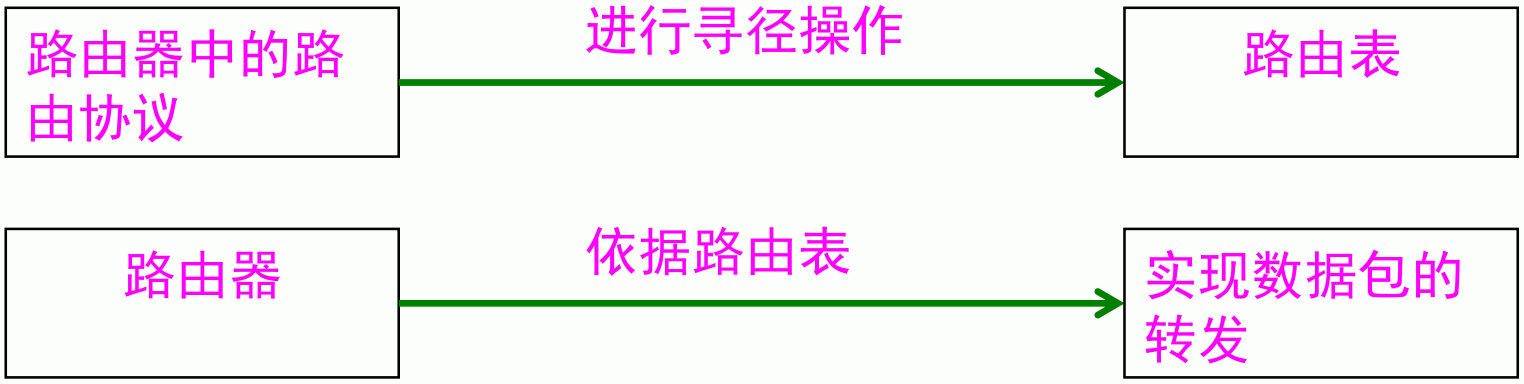
O 表示此项路由信息是通过OSPF路由协议动态学习到的；

R 表示此项路由信息是通过RIP路由协议动态学习到的；

4.5.1 路由表

【寻径与转发的意义】

需要指出的是：路由器的寻径过程与数据的转发过程是完全独立的，换言之，即指路由器转发数据的过程不需要寻径操作的参与，而仅仅使用寻径的结果——路由表而已。通常路由器的寻径过程只用路由协议完成，而路由协议并不直接参与数据包的转发过程。

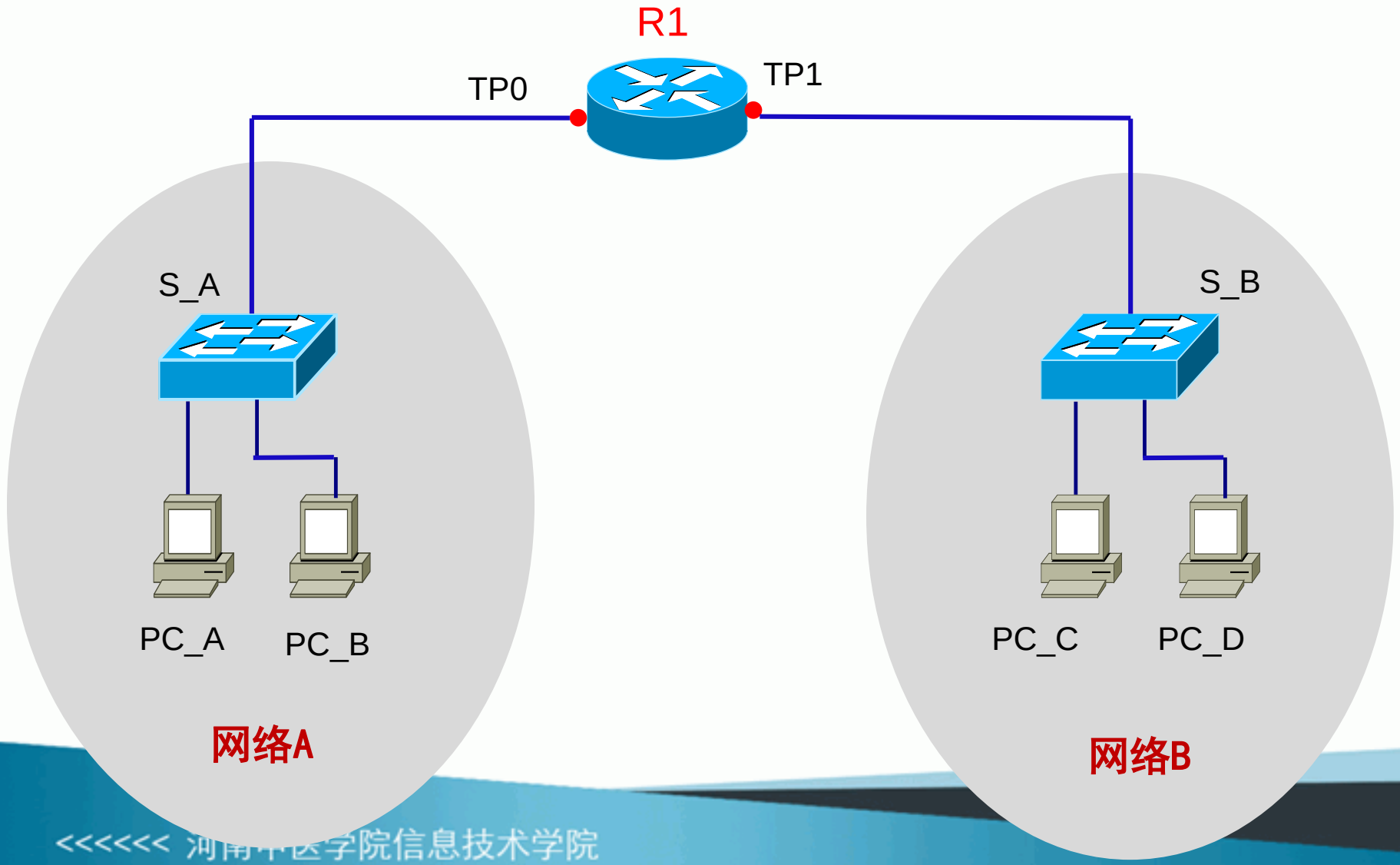


4.5.1 路由表

【何时用到路由协议？】

通常，如果网络中只有一个路由器，不需要使用路由协议，这是因为路由器的每个端口都具有自动学习各自所属网络的功能，其学习的结果被直接写入路由表。这样当数据从一个端口到来，需要到另一个端口所在的网络中去时，路由器从路由表中即可以查询到出口在哪里，完全不需要其他寻径操作的协助；

【看下面的拓扑】


R1
TP0
TP1
S_A
S_B
PC_A
PC_B
PC_C
PC_D
网络A
网络B

4.5.1 路由表

【路由表实例】

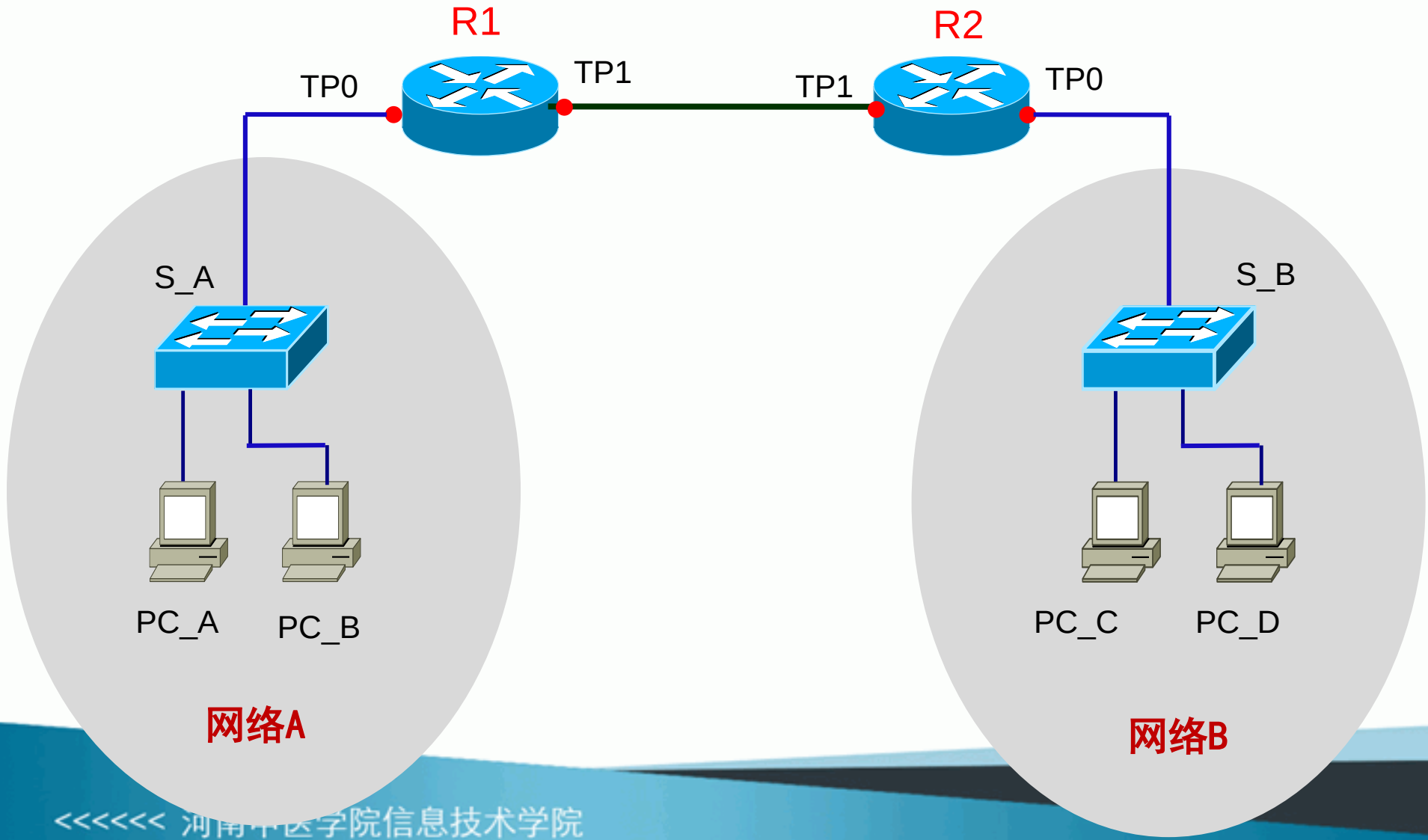
```
RA_config#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2


VRF ID: 0

C       10.0.1.0/24       is directly connected, FastEthernet0/0
C       10.1.1.0/24       is directly connected, FastEthernet0/1
RA_config#
```

4.5.1 路由表

【何时用到路由协议？】

只有当网络中具有多个路由器时，由于路由器之间屏蔽了各自独立连接的网络分段，因此远端的路由器无法通过直连的端口获取所有网络分段的位置信息，这时才有必要为路由器添加必要的对远端网络位置的认知信息。

这时就要用到路由协议。


R1
R2
TP0
TP1
TP1
TP0
S_A
S_B
PC_A
PC_B
PC_C
PC_D
网络A
网络B

```
R1_config#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C       10.0.1.0/24          is directly connected, FastEthernet0/0
C       10.1.1.0/24          is directly connected, FastEthernet0/1
S       192.168.1.0/24       [1,0] via 10.1.1.2(on FastEthernet0/1)
R1_config#
```

4.5　路由基础

4.5.1　路由表

4.5.2　静态路由与动态路由

4.5.3　自治系统AS

4.5.4　IGP与EGP

4.5 路由基础

4.5.2 静态路由与动态路由

根据路由算法能否随网络的通信量和网络拓扑的变化而自动的进行调整，可以将路由策略分为两大类：

- **静态**路由选择策略——即非自适应路由选择，其特点是简单和开销较小，但不能及时适应网络状态的变化。
- **动态**路由选择策略——即自适应路由选择，其特点是能较好地适应网络状态的变化，但实现起来较为复杂，开销也比较大。

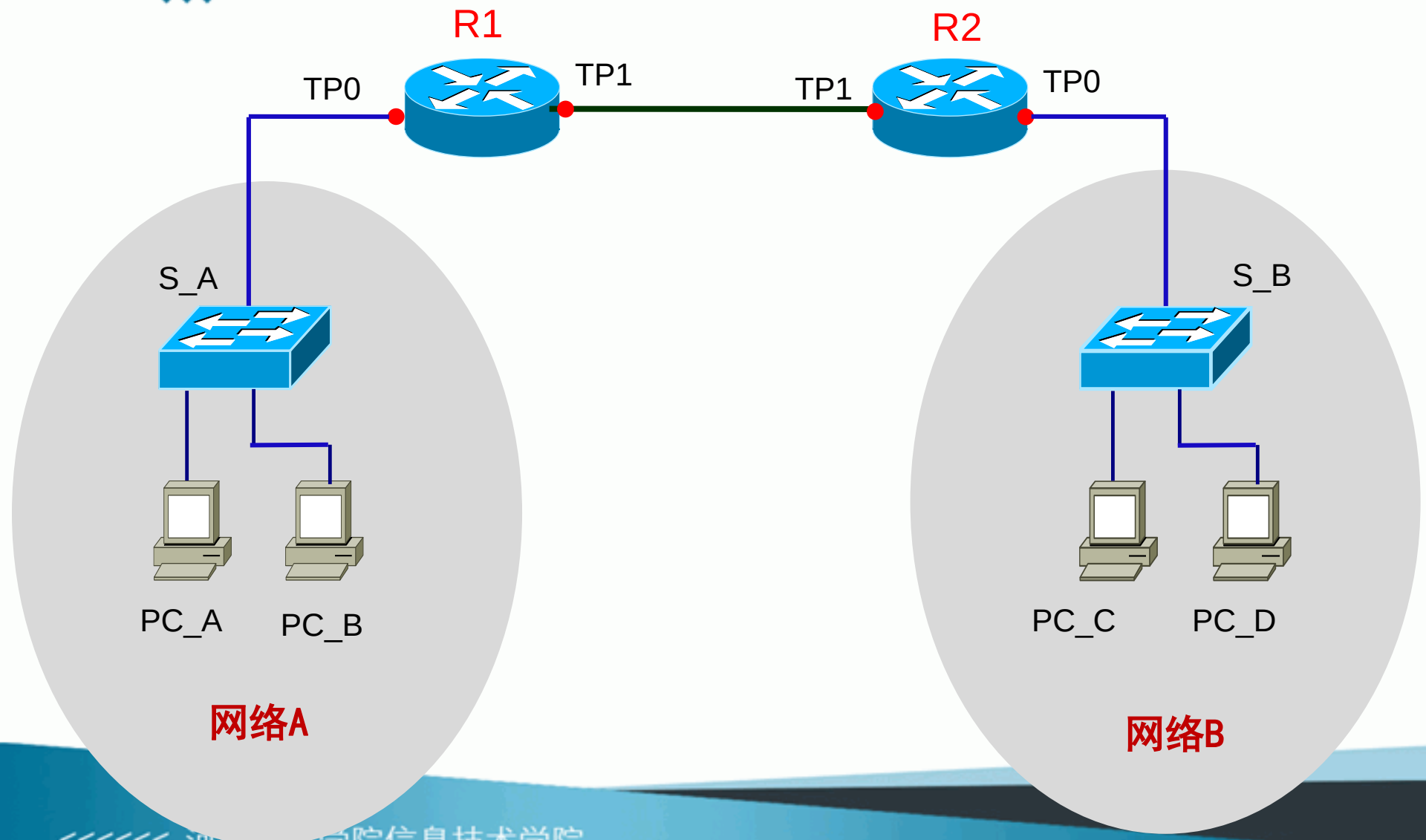
4.5 路由基础

4.5.2 静态路由与动态路由

（1） 静态路由

- 静态路由是在路由器中设置的固定的路由表，除非网络管理员干预，否则静态路由不会发生变化。
- 通常网络管理员根据其对整个网络拓扑结构的认识和管理，为每个路由器规定其到达非直连网络的下一跳及出口。
- 这种设置方法不能对网络的改变做出反应，一般用于网络规模不大、拓扑结构固定的网络中。
- 静态路由的优点是简单、高效、可靠。
- 在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

（2） 静态路由配置举例



（2） 静态路由配置举例

- 步骤1. 配置路由器R1的端口地址

1.1 为TP0端口配置IP地址

```
Router_config#interface fastethernet 0/0
Router_config_f0/0#ip address 10.0.1.1 255.255.255.0
```

1.2 为TP1端口配置IP地址

```
Router_config#interface fastethernet 0/1
Router_config_f0/0#ip  address  10.1.1.1  255.255.255.0
```

（2） 静态路由配置举例

- 步骤2. 配置路由器R2的端口地址

2.1 为TP0端口配置IP地址

```
Router_config#interface fastethernet 0/0
Router_config_f0/0#ip address 192.168.1.1 255.255.255.0
```

2.2 为TP1端口配置IP地址

```
Router_config#interface fastethernet 0/1
Router_config_f0/0#ip  address  10.1.1.2  255.255.255.0
```

（2） 静态路由配置举例

- 步骤3. 配置R1的静态路由

```
R1_config#ip  route  192.168.1.0  255.255.255.0  10.1.1.2
R1_config#
```

//该命令的含义：到达目标网络192.168.1.0，其下一跳地址是10.1.1.2

（2） 静态路由配置举例

- 步骤4. 查看R1的路由表信息

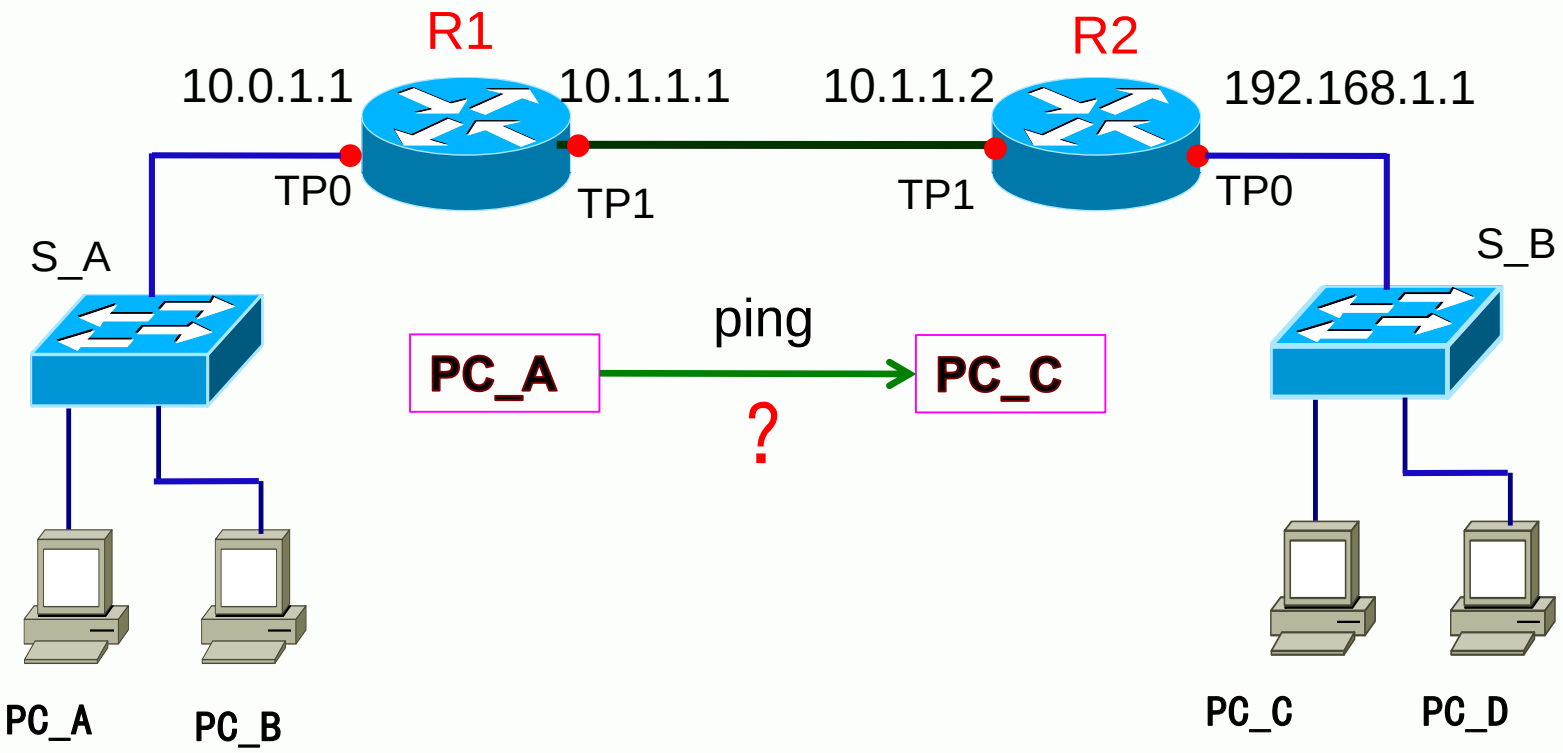
```
C    10.0.1.0/24     is directly connected, FastEthernet0/0
C    10.1.1.0/24     is directly connected, FastEthernet0/3
S    192.168.1.0/24    [1,0] via 10.1.1.2(on FastEthernet0/3)
```

注释：可以看出路由表中多了一条到达192.168.1.0网络的静态路由，用S标志。

```
C    10.1.1.0/24      FastEthernet0/1
C    192.168.1.0/24   FastEthernet0/0
```

R2的路由表

➢ 步骤5.　　测试连通性




```
C 10.0.1.0/24    FastEthernet0/0
C 10.1.1.0/24    FastEthernet0/1
S 192.168.1.0/24   [1,0] via 10.1.1.2(on FastEthernet0/3)
```

R1的路由表

（2） 静态路由配置举例

- 步骤6. 配置R2的静态路由

```
R2_config#ip route 10.0.1.0 255.255.255.0 10.1.1.1
R2_config#
```

该命令的含义：到达目标网络10.0.1.0，其下一跳地址是10.1.1.1

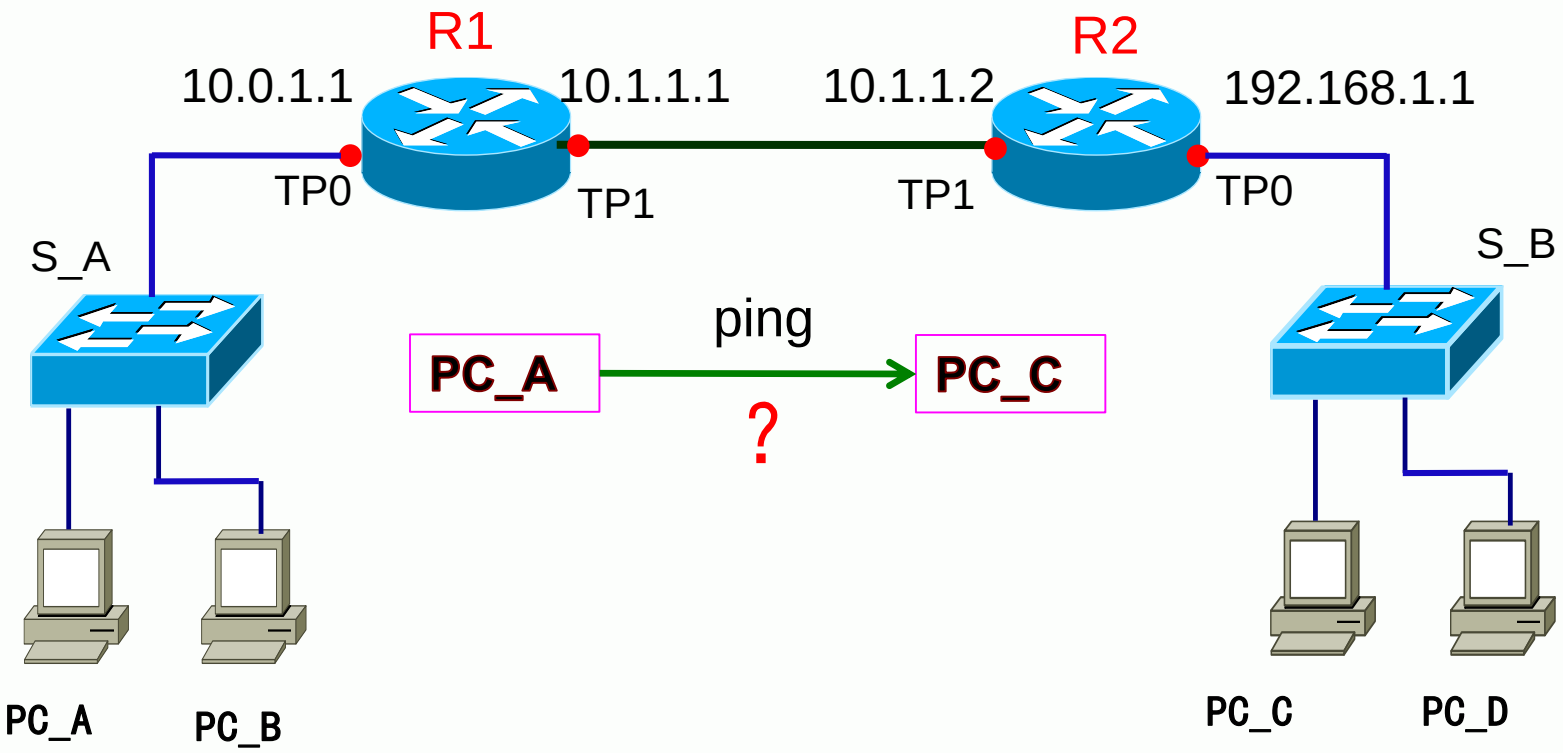
（2） 静态路由配置举例

- 步骤7. 查看R2的路由表信息

```
S    10.0.1.0/24      [1,0] via 10.1.1.1(on FastEthernet0/3)
C    10.1.1.0/24      FastEthernet0/3
C    192.168.1.0/24   FastEthernet0/0
```

```
C    10.1.1.0/24        FastEthernet0/1                R2的路由表
C    192.168.1.0/24     FastEthernet0/0
S    10.0.1.0/24          [1,0] via 10.1.1.1(on FastEthernet0/1)
```

➢ 步骤8.　　测试连通性




```
C 10.0.1.0/24    FastEthernet0/0          R1的路由表
C 10.1.1.0/24    FastEthernet0/1
S 192.168.1.0/24    [1,0] via 10.1.1.2(on FastEthernet0/3)
```

4.5　路由基础

4.5.2　静态路由与动态路由

（3）　动态路由

- 动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由表的过程。
- 它能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络，引起各路由器重新启动路由算法，并更新各自的路由表以动态地反映网络拓扑变化。
- 动态路由适用于网络规模大，网络拓扑复杂的网络。当然，各种动态路由协议会不同程度地占用网络带宽和CPU资源。

4.5　路由基础

4.5.2　静态路由与动态路由

（3）　动态路由

- 在网络中动态路由通常作为静态路由的补充。
- 当一个分组在路由器中进行寻径时，路由器首先查找静态路由，如果查到则根据相应的静态路由转发分组，否则再查找动态路由。

4.5 路由基础

4.5.1 路由表
4.5.2 静态路由与动态路由
4.5.3 自治系统AS
4.5.4 IGP与EGP

4.5　路由基础

4.5.3　自治系统 AS

（1） 分层次的路由选择协议

因特网采用分层次的路由选择协议：

- 因特网的规模非常大。如果让所有的路由器知道所有的网络应怎样到达，则这种路由表将非常大，处理起来也太花时间。而所有这些路由器之间交换路由信息所需的带宽就会使因特网的通信链路饱和。
- 许多单位不愿意外界了解自己单位网络的布局细节和本部门所采用的路由选择协议（这属于本部门内部的事情），但同时还希望连接到因特网上。
- 为此，因特网将整个互联网划分为许多**较小的自治系统（AS）**。

4.5　路由基础

4.5.3　自治系统 AS

（2）自治系统 AS：　Autonomous System：

- 自治系统 AS 的定义：在单一的技术管理下的一组路由器，而这些路由器使用一种 AS 内部的路由选择协议和共同的度量以确定分组在该 AS 内的路由，同时还使用一种 AS 之间的路由选择协议用以确定分组在 AS之间的路由。
- 例如，一个大的ISP就是一个自治系统。

4.5 路由基础

4.5.1 路由表
4.5.2 静态路由与动态路由
4.5.3 自治系统AS
4.5.4 IGP与EGP

4.5 路由基础

4.5.4 IGP与EGP

- **内部网关协议 IGP**（Interior Gateway Protocol） 即在一个自治系统内部使用的路由选择协议。目前这类路由选择协议使用得最多，如 RIP 和 OSPF 协议。
- **外部网关协议EGP**（External Gateway Protocol） 若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。这样的协议就是外部网关协议 EGP。目前使用的协议是 BGP。

自治系统和
内部网关协议、外部网关协议

自治系统之间的路由选择也叫做域间路由选择(interdomain routing)，在自治系统内部的路由选择叫做域内路由选择(intradomain routing)

4.6　动态路由协议

4.6.1　路由信息协议（RIP）
4.6.2　开放最短路径优先（OSPF）

4.6.1　路由信息协议（RIP）

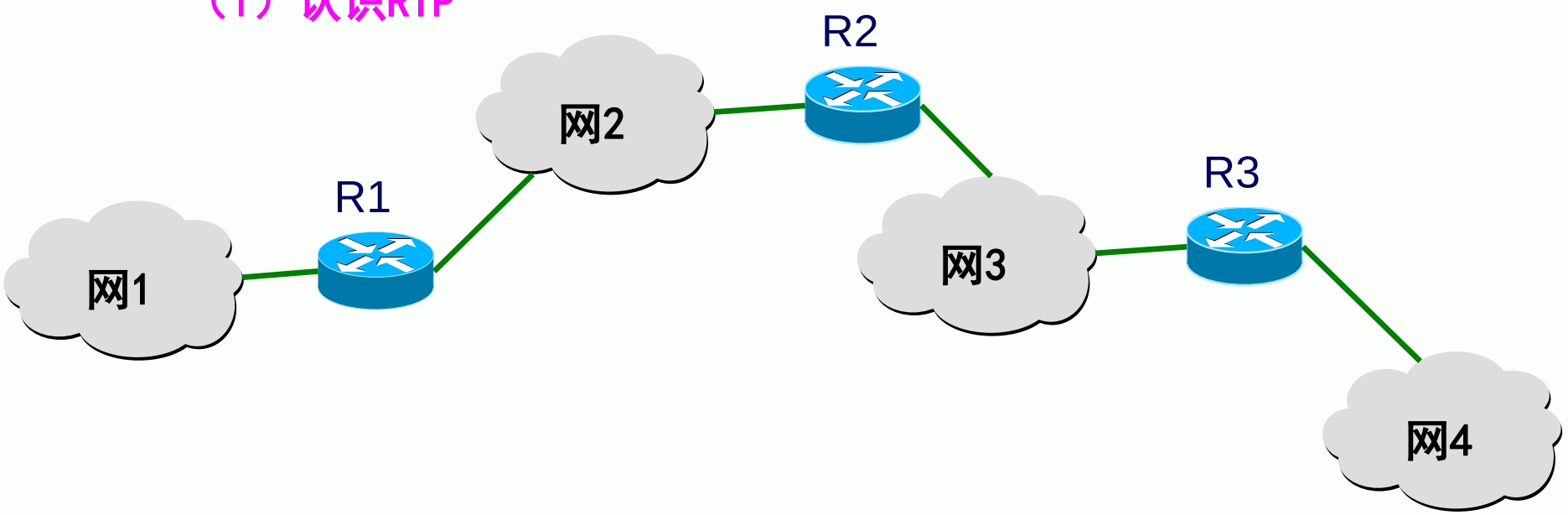
4.6.1 路由信息协议RIP

（1）认识RIP

- 英文全称：Routing Information Protocol
- 路由信息协议 RIP 是内部网关协议 IGP中最先得到广泛使用的协议。
- RIP 是一种分布式的基于距离向量的路由选择协议。
- RIP 协议要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离记录。**（举例）**

4.6.1 路由信息协议RIP

（1）认识RIP



根据RIP 协议，路由器R1——R3的路由表中，都维护了从它自己到网1、网2、网3、网4的距离记录。

4.6.1 路由信息协议RIP

（2）距离和向量的概念-(1)

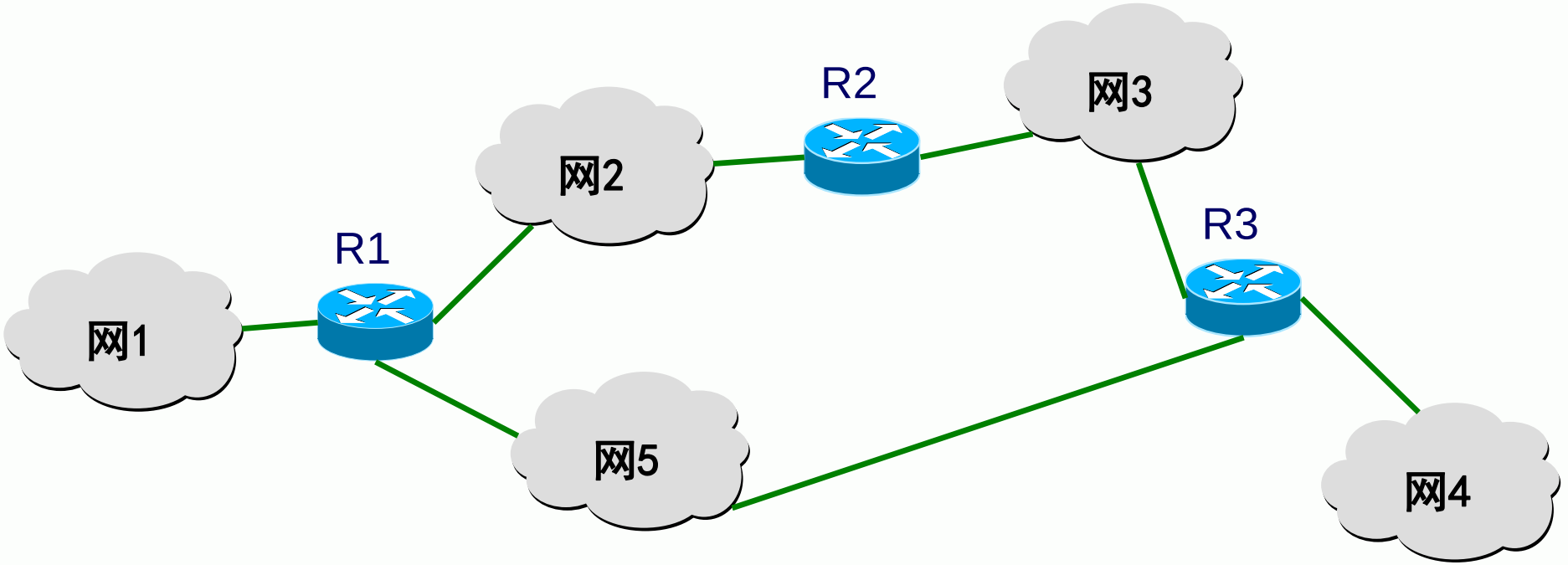
- 距离：指当前路由器到达目标网络的远近度量。
- 向量：从当前路由器到达目标网络的距离值是有方向的，这由其下一跳地址体现。

4.6.1 路由信息协议RIP

（2）距离和向量的概念-(2)

- 我们知道，在一个相对复杂的路由环境中，由于有多个路由器的互联，从一个网络到另一个网络的路径可能就有多个。对于路由器来讲，需要从多个到达同一网络的路径中通过某种算法选择最优的写入到路由表中。
- （例如下图中，从网1到网4就有两条路径）

4.6.1 路由信息协议RIP



从网1到网4有两条路径

R1 —— R2 ——R3

R1 —— R3

4.6.1 路由信息协议RIP

（2）距离和向量的概念-(3)

如何衡量每条路径的好坏呢？

在相同的衡量标准下，度量值最小的路径，就是最优的。

4.6.1 路由信息协议RIP

（3）关于度量值

度量值代表距离。它们用来在寻找路由时确定最优路由。每一种路由算法在产生路由表时，会为每一条通过网络的路径产生一个数值（度量值），最小的值表示最优路径。度量值的计算可以只考虑路径的一个特性，但更复杂的度量值是综合了路径的多个特性产生的。一些常用的度量值有：

4.6.1 路由信息协议RIP

（3）关于度量值

- 跳步数：报文要通过的路由器输出端口的个数。
- Ticks：数据链路的延时（大约1/18每秒）
- 代价：可以是一个任意的值，是根据带宽，费用或其他网络管理者定义的计算方法得到的
- 带宽：数据链路的容量
- 时延：报文从源端传到目的地的时间长短
- 负载：网络资源或链路已被使用的部分的大小。

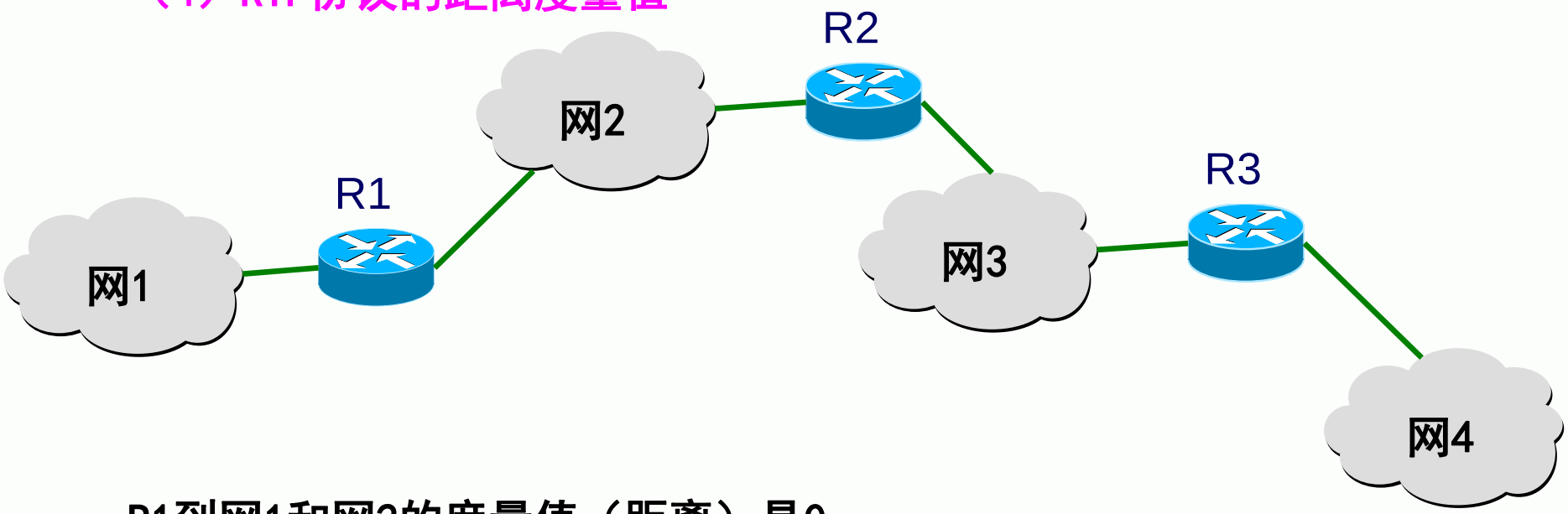
4.6.1 路由信息协议RIP

（4）RIP协议的距离度量值

- RIP 使用“跳步数”作为其度量值。
- RIP认为一个好的路由就是它通过的路由器的数目少，即“距离短”。
- 在RIP中，路由器到与之直接相连网络的跳数为0，通过1个路由器可达的网络的跳数为1，通过2个路由器可达的网络的跳数为2，以此类推。
- “距离”的最大值为16 时即相当于不可达。可见RIP 只适用于小型互联网。

4.6.1 路由信息协议RIP

（4）RIP协议的距离度量值



R1到网1和网2的度量值（距离）是0
R1到网3的度量值（距离）是1
R1到网4的度量值（距离）是2

4.6.1 路由信息协议RIP

（5）路由信息的表示

- 由于路由器通常会有很多个连接不同网络段的端口，因此，路由器判断到达某一个非直接连接的网络段的路径时，通常还要包括出口选择的信息，也就是出端口。通常路由器转发一个数据时，需要明确将这个数据转发给哪个下一跳站点，也就是具体的某节点的IP地址。综合以上所述，路由器对某一个网络的路径信息，通常需要包含如下几项内容：

- 目的网络　度量值　下一跳地址　出端口

S　192.168.1.0/24　[1,0] via 10.1.1.2(on FastEthernet0/1)

R　10.0.1.0/24　[120,1] via 10.1.1.1(on FastEthernet0/0)

4.6.1 路由信息协议RIP

（6）RIP协议的特点 _ 1

- **仅和相邻路由器交换信息**

如果两个路由器之间的通信不需要经过另一个路由器，那么这两个路由器就是相邻的。RIP协议规定，不相邻的路由器不交换信息。

4.6.1 路由信息协议RIP

（6）RIP协议的特点 _ 2

- **路由器交换的信息是当前本路由器所知道的全部信息，即自己的路由表。**

也就是说，交换的信息是：“我到本自治系统中所有网络的（最短）距离，以及到每个网络应经过的下一跳路由器。

4.6.1 路由信息协议RIP

（6）RIP协议的特点 _ 3

- **按固定的时间间隔交换路由信息。**

  例如，每隔30秒，然后路由器根据收到的路由信息更新路由表。

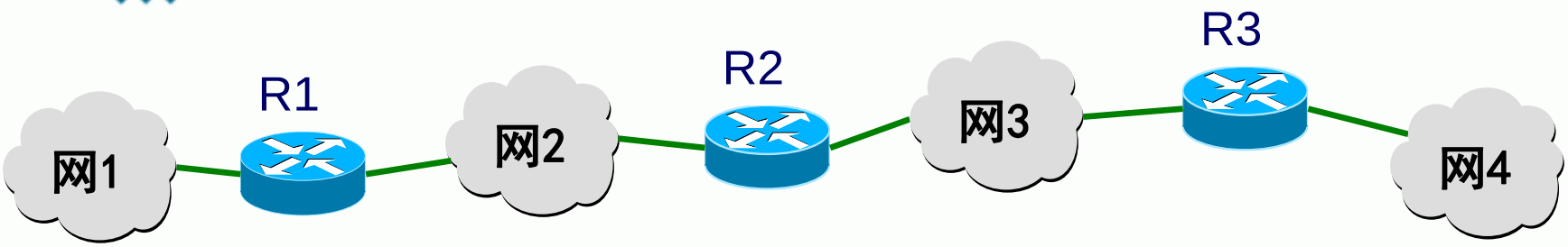
4.6.1 路由信息协议RIP

（7）RIP协议工作过程

- 路由器在刚开始工作时，只知道到直连的网络的距离（此距离定义为0）。
- 接着，每一个路由器也只和数目有限的相邻路由器交换并更新路由信息。
- 但经过若干次的更新后，所有路由器最终都会知道到达本自治系统中任何一个网络的最短距离和下一跳路由器的地址。

【举例说明】

（7）RIP协议工作过程



R1的路由信息

目的	下一跳	跳数
网1	直连	0
网2	直连	0

R2的路由信息

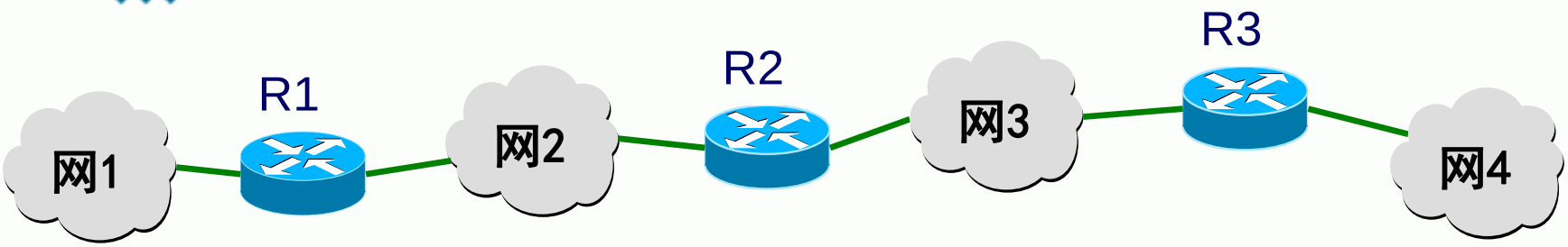
目的	下一跳	跳数
网2	直连	0
网3	直连	0

R3的路由信息

目的	下一跳	跳数
网3	直连	0
网4	直连	0

t0时刻

（7）RIP协议工作过程



R1的路由信息

目的	下一跳	跳数
网1	直连	0
网2	直连	0
网3	R2	1

R2的路由信息

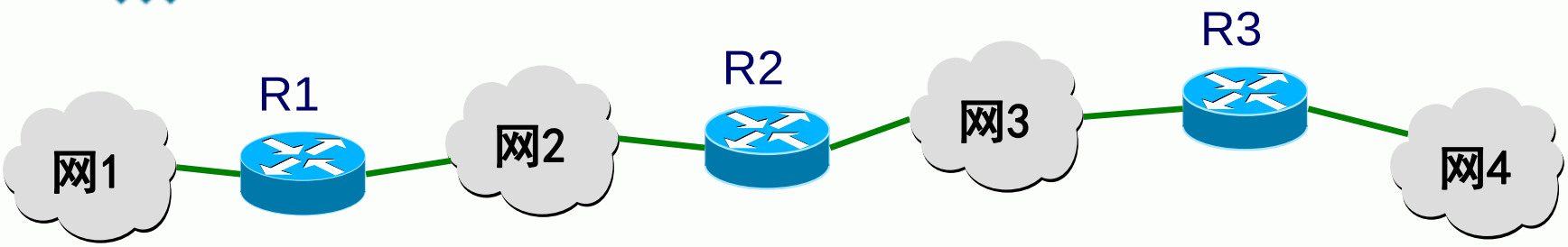
目的	下一跳	跳数
网2	直连	0
网3	直连	0
网1	R1	1
网4	R3	1

R3的路由信息

目的	下一跳	跳数
网3	直连	0
网4	直连	0
网2	R2	1

t1时刻

（7）RIP协议工作过程



R1的路由信息

目的	下一跳	跳数
网1	直连	0
网2	直连	0
网3	R2	1
网4	R2	2

R2的路由信息

目的	下一跳	跳数
网2	直连	0
网3	直连	0
网1	R1	1
网4	R3	1

R3的路由信息

目的	下一跳	跳数
网3	直连	0
网4	直连	0
网2	R2	1
网1	R2	2

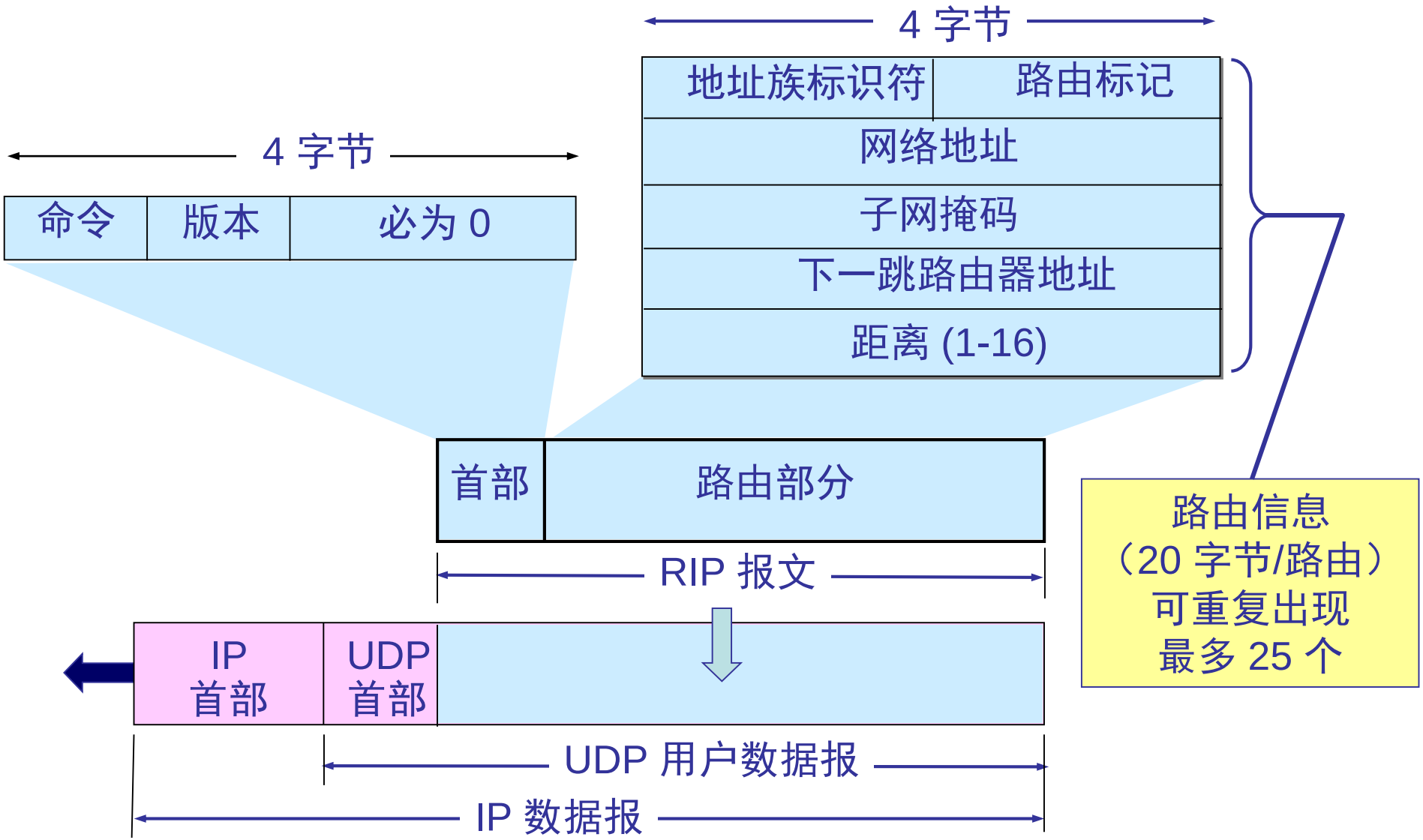
t2时刻

4.6.1 路由信息协议RIP

（8）RIP2 协议的报文格式

- RIP报文由首部和路由部分组成。
- 报文中的路由部分由若干个路由信息组成。每个路由信息需要用20个字节，包括目的网络地址、该网络的子网掩码、下一跳路由器地址以及到此网络的距离。
- 一个RIP报文最多可包括25个路由，因而RIP报文的最大长度是4+20*25=504字节。
- 如超过，必须再用一个RIP报文来传送。

RIP2 协议的报文格式



4.6.1 路由信息协议RIP

（9）距离向量算法

- 路由表中最主要的信息就是：到某个网络的距离（即最短距离），以及应经过的下一跳地址。路由表更新的原则是找出到每个目的网络的最短距离。
- 这种更新算法又称为距离向量算法。

下面是距离向量算法的具体内容

➢ 假设本路由器收到相邻路由器（其地址是X）发送过来的RIP报文：

① 先修改此 RIP 报文中的所有项目：把“下一跳”字段中的地址都改为 X，并把所有的“距离”字段的值加 1。

② 对修改后的 RIP 报文中的每一个项目，重复以下步骤：

if （若项目中的目的网络不在路由表中）

则把该项目加到路由表中。

else if （若本机路由表中到此目的网络的下一跳地址**也是X**）

则用收到的项目替换本机原路由表中的项目。

else if （若收到项目中的距离小于本路由表中的距离）

则进行更新

else （什么也不做）

③ 若 3 分钟还没有收到相邻路由器的更新路由表，则把此相邻路由器记为不可达路由器，即将距离置为16（距离为16表示不可达）。

④ 返回。

4.6.1 路由信息协议RIP

（9）距离向量算法

- RIP协议让互联网中的所有路由器都和自己的相邻路由器不断交换路由信息，并不断更新其路由表，使得从每一个路由器到每一个目的网络的路由都是最短的（即跳数最少）。
- 虽然所有的路由器最终都拥有了整个自治系统的全局路由信息，但由于每一个路由器的位置不同，它们的路由表当然也应当是不同的。

4.6.1 路由信息协议RIP

（10）距离向量算法举例

- 已知路由器R6的路由表（表1），现收到相邻路由器R4发来的路由更新报文，如表2所示，请说明路由器R6的更新结果。

表1

目的	距离	下一跳
网2	3	R4
网3	4	R5

表2

目的	距离	下一跳
网1	3	R1
网2	4	R2
网3	0	直连

（10）距离向量算法举例

① 先修改此 RIP 报文中的所有项目：把“下一跳”字段中的地址都改为 R4，并把所有的“距离”字段的值加 1。

表2

目的	距离	下一跳
网1	3	R1
网2	4	R2
网3	0	直连

更新后的表2

目的	距离	下一跳
网1	4	R4
网2	5	R4
网3	1	R4

（10）距离向量算法举例

② 利用更新后的表2中的路由项目，去更新表1

表1

目的	距离	下一跳
网2	3	R4
网3	4	R5

更新后的表2

目的	距离	下一跳
网1	4	R4
网2	5	R4
网3	1	R4

（10）距离向量算法举例

③ R6的路由表更新后的结果

表1

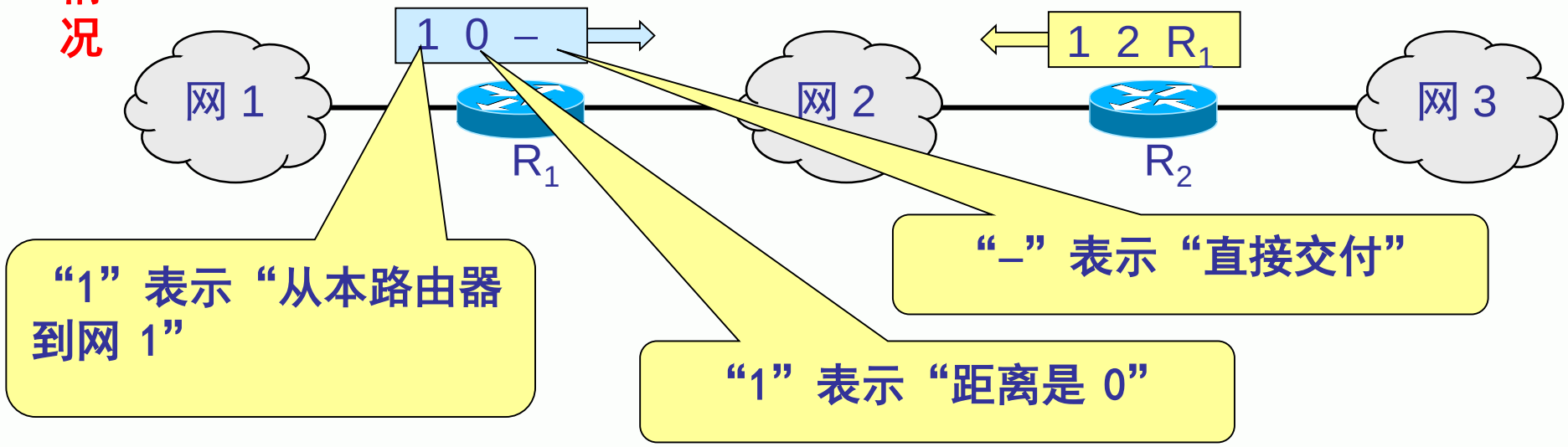
目的	距离	下一跳	说明
网2	5	R4	原有路由，距离进行了更新
网3	4	R5	原有路由，距离和下一跳进行了更新
网1	4	R4	增加一条新路由

4.6.1 路由信息协议RIP

（11）RIP 协议的优缺点

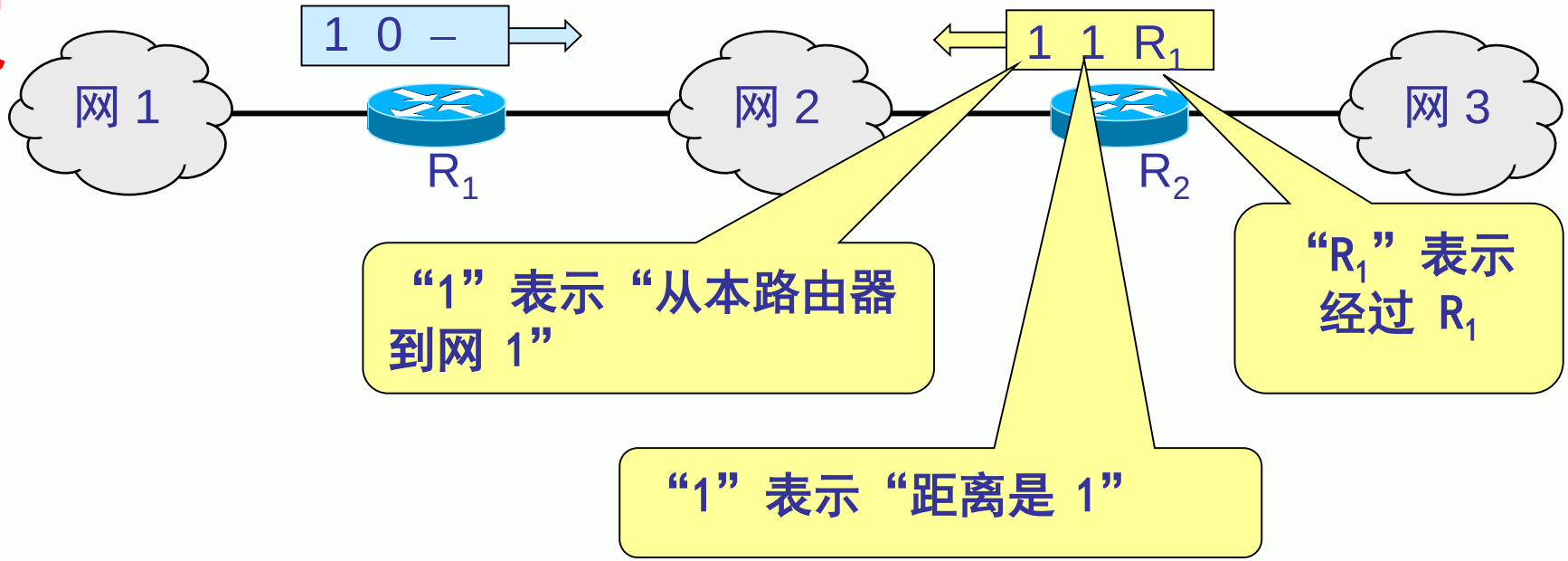
- RIP 存在的一个问题是当网络出现故障时，要经过比较长的时间才能将此信息传送到所有的路由器。
- RIP 协议最大的优点就是实现简单，开销较小。
- RIP 限制了网络的规模，它能使用的最大距离为 15（16 表示不可达）。
- 路由器之间交换的路由信息是路由器中的完整路由表，因而随着网络规模的扩大，开销也就增加。

正常情况



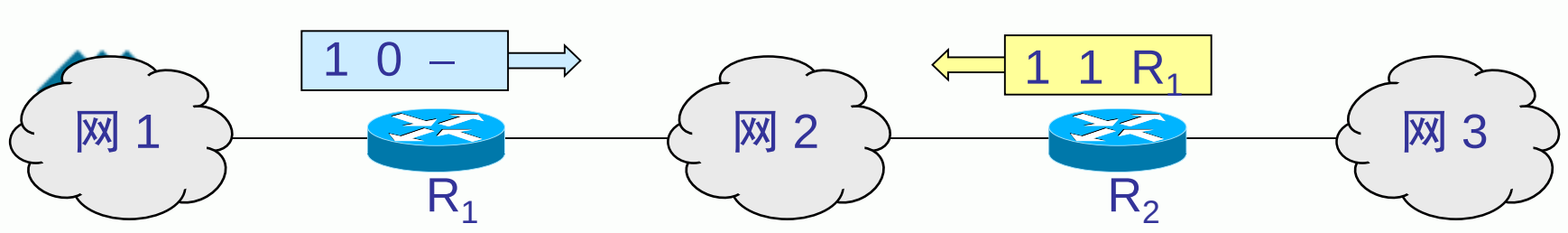
R_1 说：“我到网 1 的距离是 0，是直接交付。”

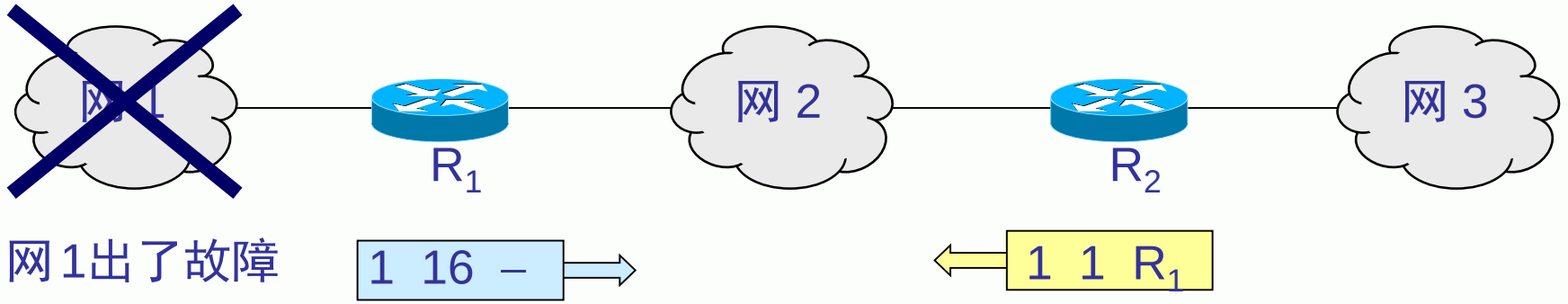
正常情况



R_2 说：“我到网 1 的距离是 1，是经过 R_1。”

正常情况

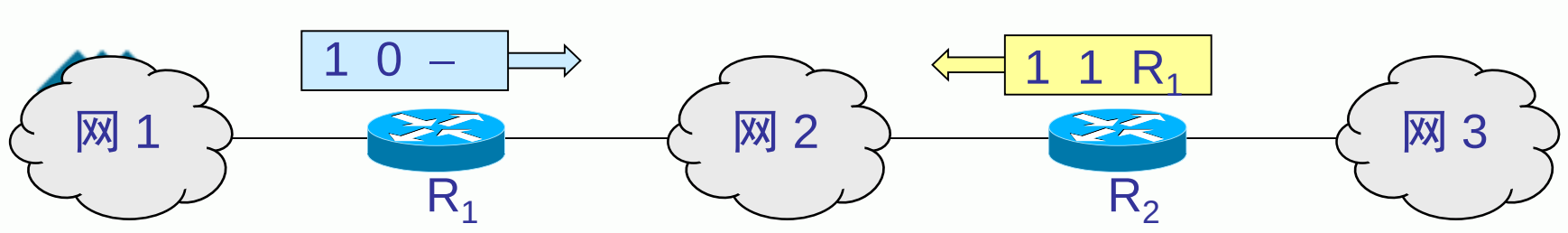


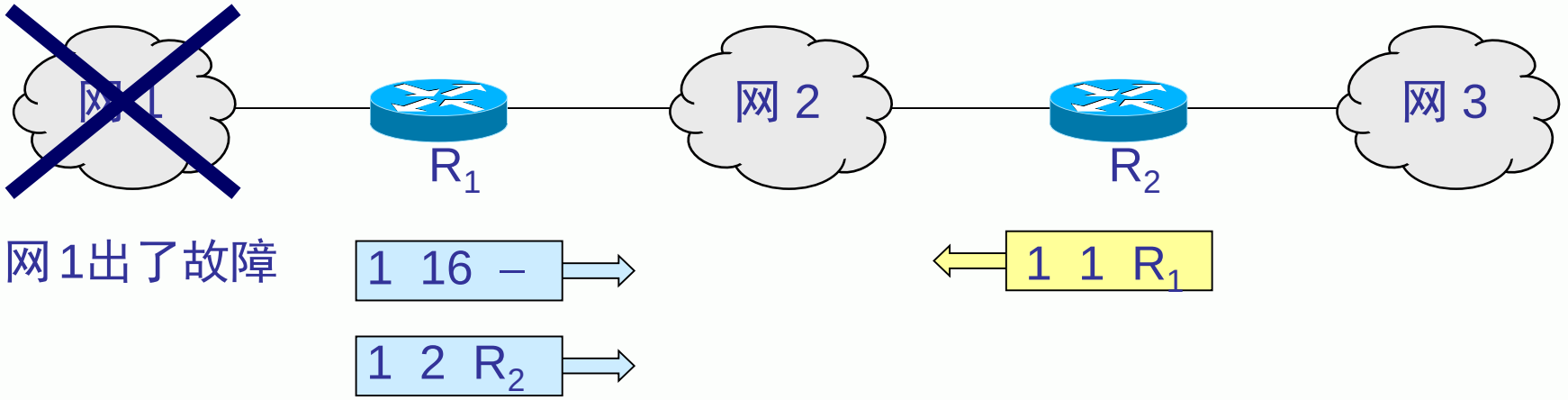


R_1 说：“我到网 1 的距离是 16 （表示无法到达），是直接交付。”

但 R_2 在收到 R_1 的更新报文之前，还发送原来的报文，因为这时 R_2 并不知道 R_1 出了故障。

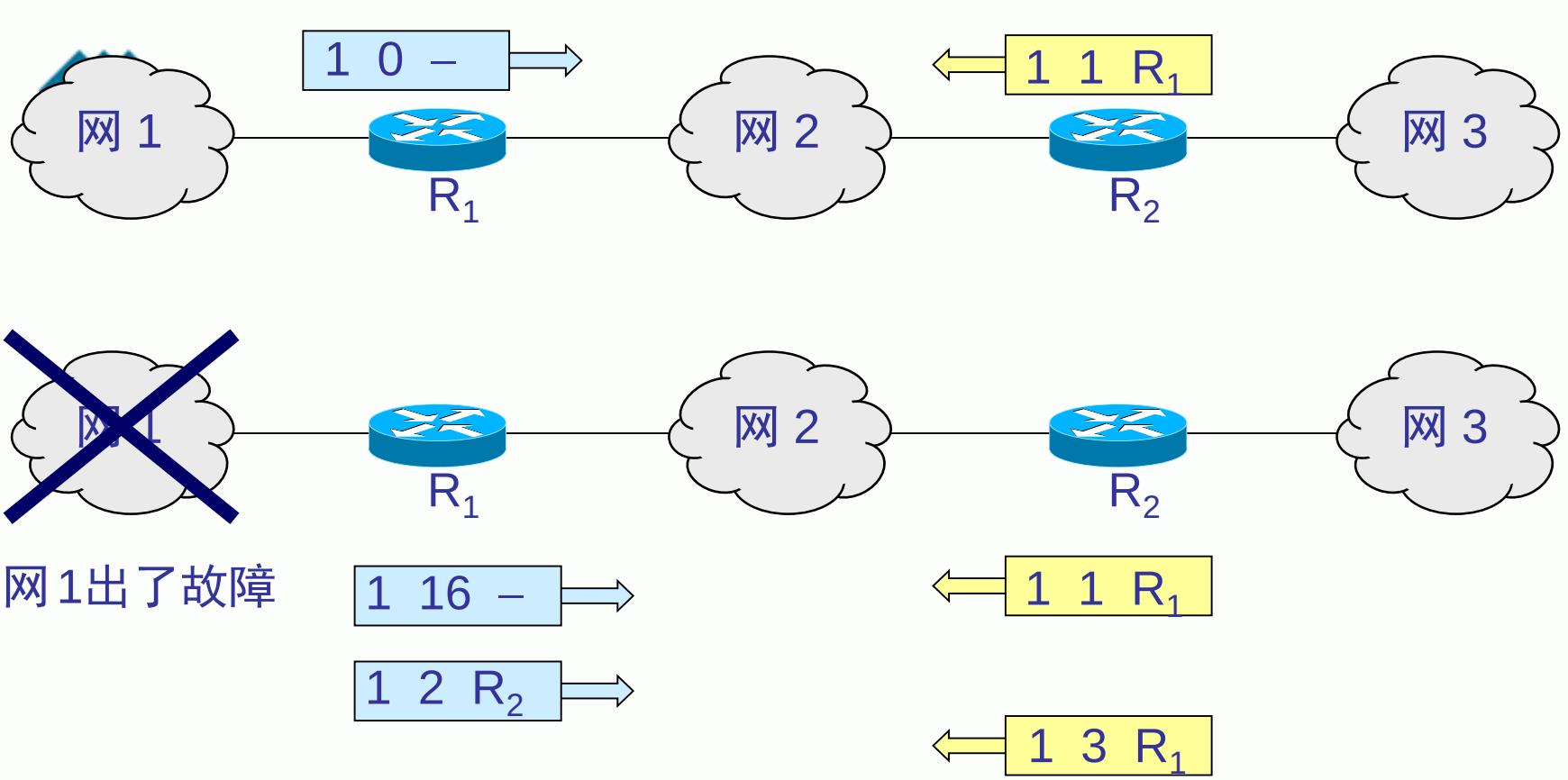
正常情况





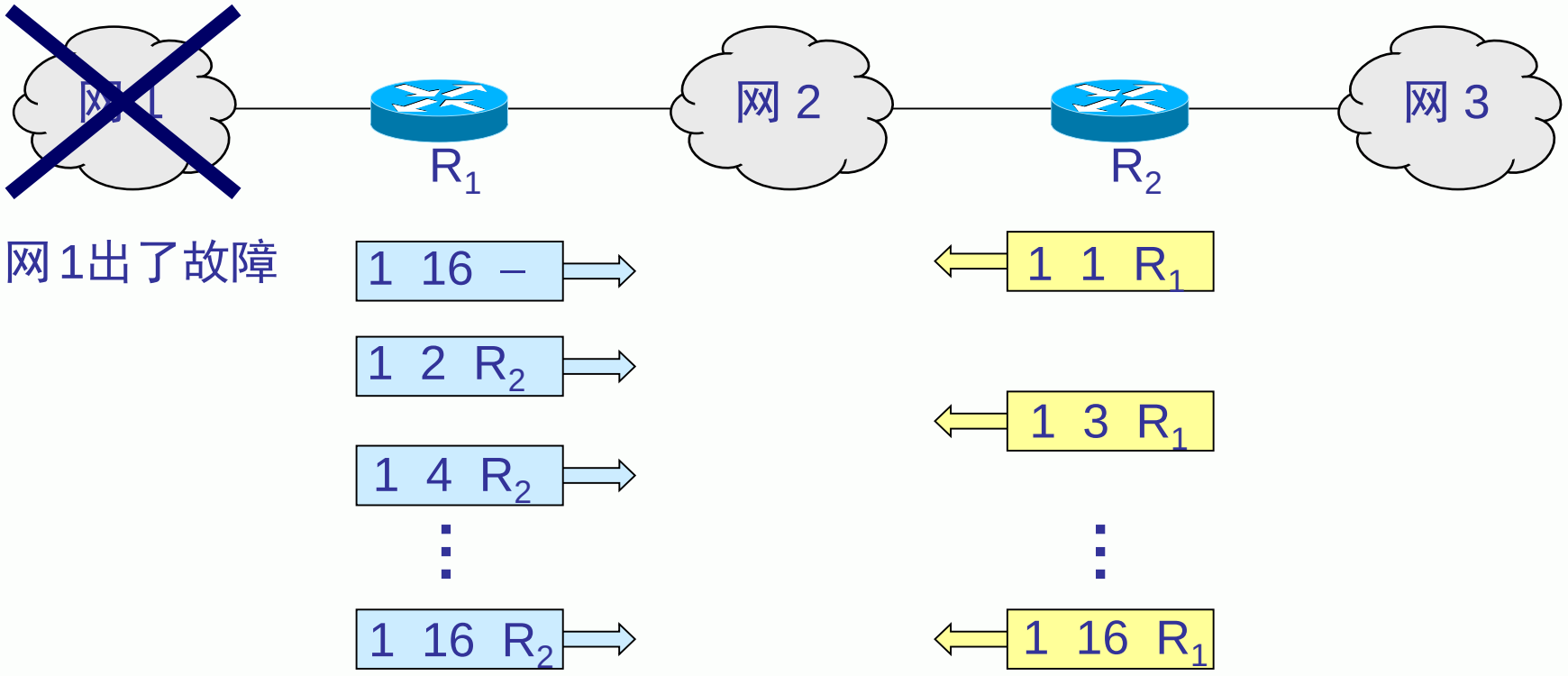
R_1 收到 R_2 的更新报文后，误认为可经过 R_2 到达网1，于是更新自己的路由表，说：“我到网 1 的距离是 2，下一跳经过 R_2”。然后将此更新信息发送给 R_2。

正常情况



R_2 以后又更新自己的路由表为“1，3，R_1”，表明“我到网 1 距离是 3，下一跳经过 R_1”。

这就是好消息传播得快，而坏消息传播得慢。网络出故障的传播时间往往需要较长的时间(例如数分钟)。这是 RIP 的一个主要缺点。



这样不断更新下去，直到 R_1 和 R_2 到网 1 的距离都增大到 16 时，R_1 和 R_2 才知道网 1 是不可达的。

4.6.2　开放最短路径优先（OSPF）

4.6.2 内部网关协议 OSPF (Open Shortest Path First)

（1） OSPF 协议的基本特点

- “开放”表明 OSPF 协议不是受某一家厂商控制，而是公开发表的。
- “最短路径优先”是因为使用了 Dijkstra 提出的最短路径算法SPF
- OSPF 只是一个协议的名字，它并不表示其他的路由选择协议不是“最短路径优先”。
- 是分布式的链路状态协议。

4.6.2 内部网关协议 OSPF

（2）三个要点

- 向本自治系统中所有路由器发送信息，这里使用的方法是洪泛法。
- 发送的信息就是与本路由器相邻的所有路由器的链路状态，但这只是路由器所知道的部分信息。
  - “链路状态”就是说明本路由器都和哪些路由器相邻，以及该链路的“度量”(metric)。
- 只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送此信息。

4.6.2 内部网关协议 OSPF

（3）链路状态数据库

- 由于各路由器之间频繁地交换链路状态信息，因此所有的路由器最终都能建立一个链路状态数据库。
- 这个数据库实际上就是全网的拓扑结构图，它在全网范围内是一致的（这称为链路状态数据库的同步）。
- 相同区域中的每个OSPF路由器都维持一个整个区域的拓扑数据库，并且都是相同的，而且根据拓扑数据库，通过SPF算法以自己作为根节点计算出最短路径树。

4.7 虚拟专用网 VPN 和网络地址转换 NAT

4.7.1 虚拟专用网 VPN

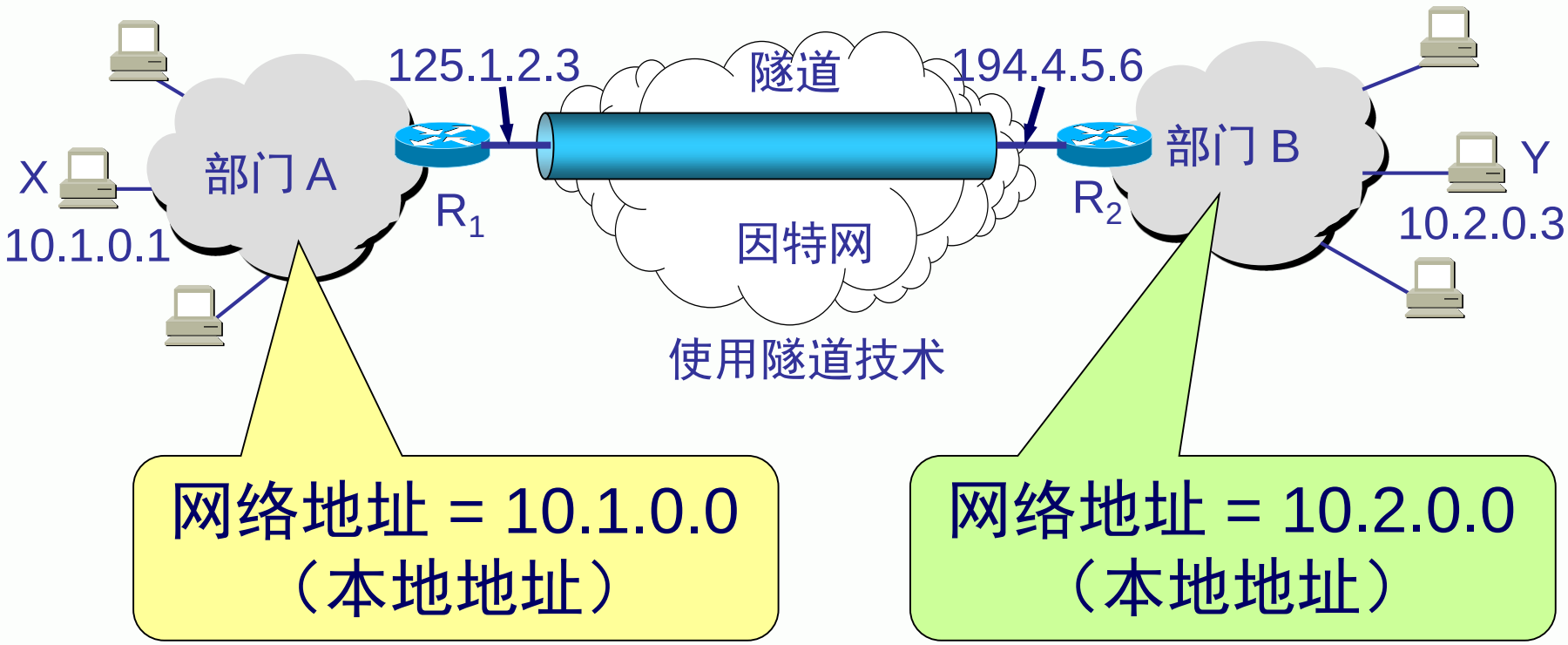
- 本地地址——仅在机构内部使用的 IP 地址，可以由本机构自行分配，而不需要向因特网的管理机构申请。
- 全球地址——全球唯一的IP地址，必须向因特网的管理机构申请。

RFC 1918 指明的专用地址 (private address)

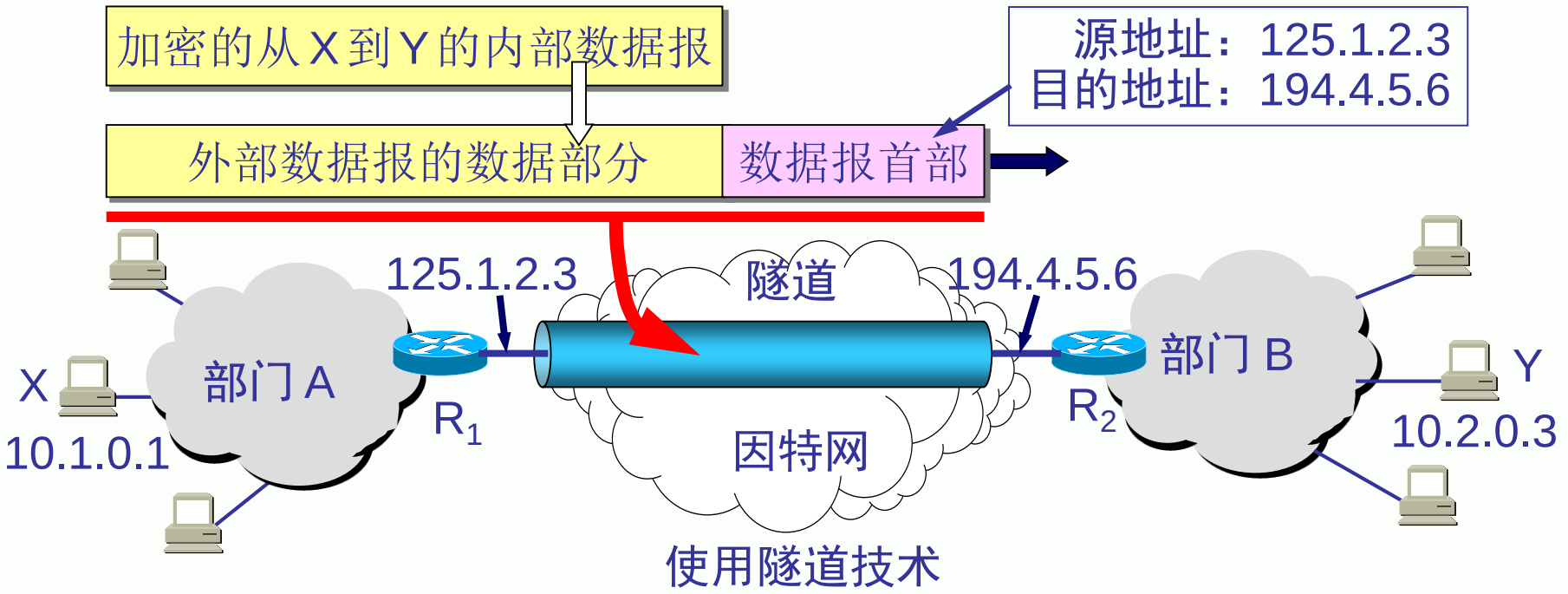
- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 到 172.31.255.255
- 192.168.0.0 到 192.168.255.255
- 这些地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信。
- 专用地址只能用作本地地址而不能用作全球地址。在因特网中的所有路由器对目的地址是专用地址的数据报一律不进行转发。

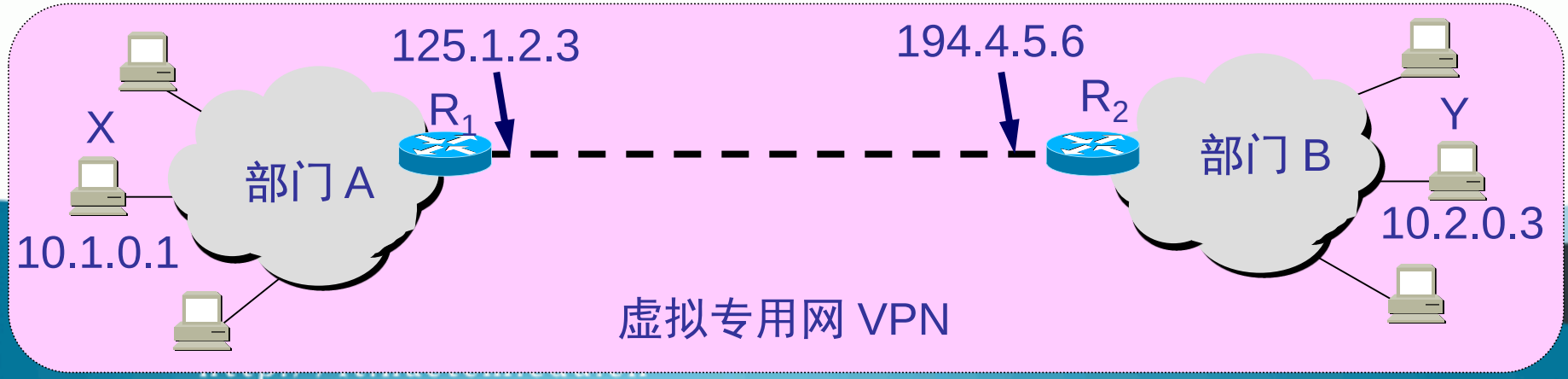
用隧道技术实现虚拟专用网

本地地址　　全球地址　　本地地址



用隧道技术实现虚拟专用网

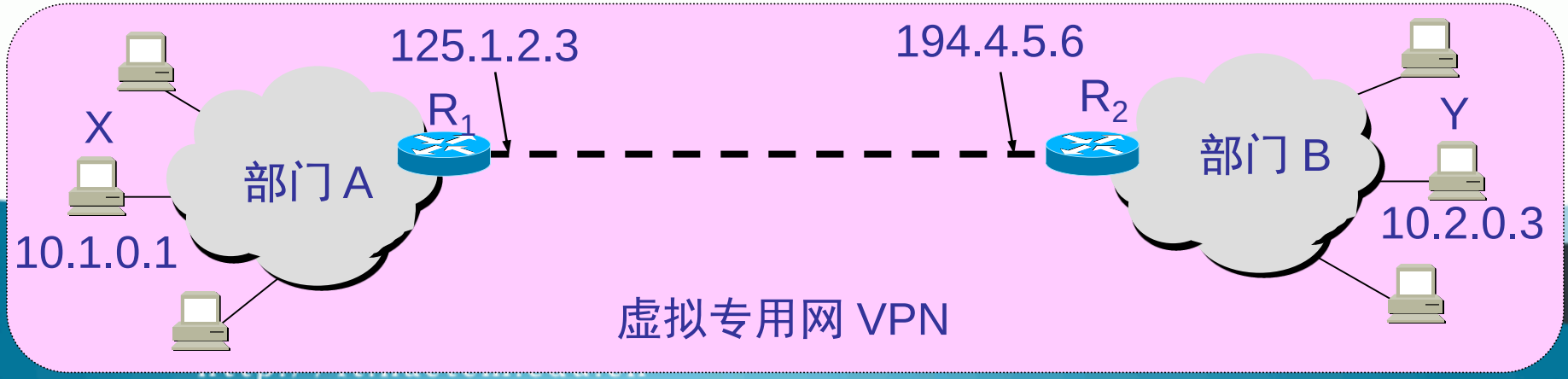




内联网 intranet 和外联网 extranet

（都是基于 TCP/IP 协议）

- 由部门 A 和 B 的内部网络所构成的虚拟专用网 VPN 又称为内联网(intranet)，表示部门 A 和 B 都是在同一个机构的内部。
- 一个机构和某些外部机构共同建立的虚拟专用网 VPN 又称为外联网(extranet)。



远程接入VPN
(remote access VPN)

- 有的公司可能没有分布在不同场所的部门，但有很多流动员工在外地工作。公司需要和他们保持联系，远程接入 VPN 可满足这种需求。
- 在外地工作的员工拨号接入因特网，而驻留在员工 PC 机中的 VPN 软件可在员工的 PC 机和公司的主机之间建立 VPN 隧道，因而外地员工与公司通信的内容是保密的，员工们感到好像就是使用公司内部的本地网络。

4.7.2 网络地址转换 NAT (Network Address Translation)

- 网络地址转换 NAT 方法于1994年提出。
- 需要在专用网连接到因特网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 NAT 路由器，它至少有一个有效的外部全球地址 IP_G。
- 所有使用本地地址的主机在和外界通信时都要在 NAT 路由器上将其本地地址转换成 IP_G 才能和因特网连接。

网络地址转换的过程

- 内部主机 X 用本地地址 IP_X 和因特网上主机 Y 通信所发送的数据报必须经过 NAT 路由器。
- NAT 路由器将数据报的源地址 IP_X 转换成全球地址 IP_G，但目的地址 IP_Y 保持不变，然后发送到因特网。
- NAT 路由器收到主机 Y 发回的数据报时，知道数据报中的源地址是 IP_Y 而目的地址是 IP_G。
- 根据 NAT 转换表，NAT 路由器将目的地址 IP_G 转换为 IP_X，转发给最终的内部主机 X。

英文：administrative distance
缩写：AD
管理距离是指一种路由协议的路由可信度。每一种路由协议按可靠性从高到低，依次分配一个信任等级，这个信任等级就叫管理距离。
对于两种不同的路由协议到一个目的地的路由信息，路由器首先根据管理距离决定相信哪一个协议。
AD值越低，则它的优先级越高。
一个管理距离是一个从0——255的整数值，0是最可信赖的，而255则意味着不会有业务量通过这个路由。
默认情况下：
路由源 AD
直连接口 0
静态路由 1
EIGRP 90
IGRP 100
OSPF 110
RIP 120
ExEIGRP 170
未知 255

度量值代表距离。它们用来在寻找路由时确定最优路由。每一种路由算法在产生路由表时，会为每一条通过网络的路径产生一个数值（度量值），最小的值表示最优路径。度量值的计算可以只考虑路径的一个特性，但更复杂的度量值是综合了路径的多个特性产生的。一些常用的度量值有：
◎跳步数：报文要通过的路由器输出端口的个数。
◎Ticks：数据链路的延时（大约1/18每秒）。
◎代价：可以是一个任意的值，是根据带宽，费用或其他网络管理者定义的计算方法得到的。
◎带宽：数据链路的容量。
◎时延：报文从源端传到目的地的时间长短。
◎负载：网络资源或链路已被使用的部分的大小。
◎可靠性：网络链路的错误比特的比率。
◎最大传输单元（MTU）：在一条路径上所有链接可接受的最大消息长度（单位为字节）。 IGRP使用什么类型的路由度量值？这个度量值由什么组成？
IGRP使用多个路由度量值。它包括如下部分：
◎带宽：源到目的之间最小的带宽值。
◎时延：路径中积累的接口延时。
◎可靠性：源到目的之间最差的可能可靠性，基于链路保持的状态。
◎负载：源到目的之间的链路在最坏情况下的负载，用比特每秒表示。
◎MTU：路径中最小的M T U值。 度量值也称metric值 是在路由选择协议算法完成后得到的一个变量值,例如经过路由器的台数、带宽等。

管理距离是指不同路由来源的可信程度,也就是说在不同协议之间是通过AD来进行选择的.AD数值越小的,则认为越可靠;而度量值是用于同一协议中到达同一目的地的多条路径的比较,比如说,一个拓扑中,所有路由器配置rip,从源到达目的有多条路径,其中一条路径要经过五跳,而另外一条路径则只用三跳,那么路由器就会选择只用三条的那条路径. 而不同的协议可以使用不同的衡量标准作为度量,所以在不同协议之间比较度量值是没有意义的.
不知道我的理解是不是正确?