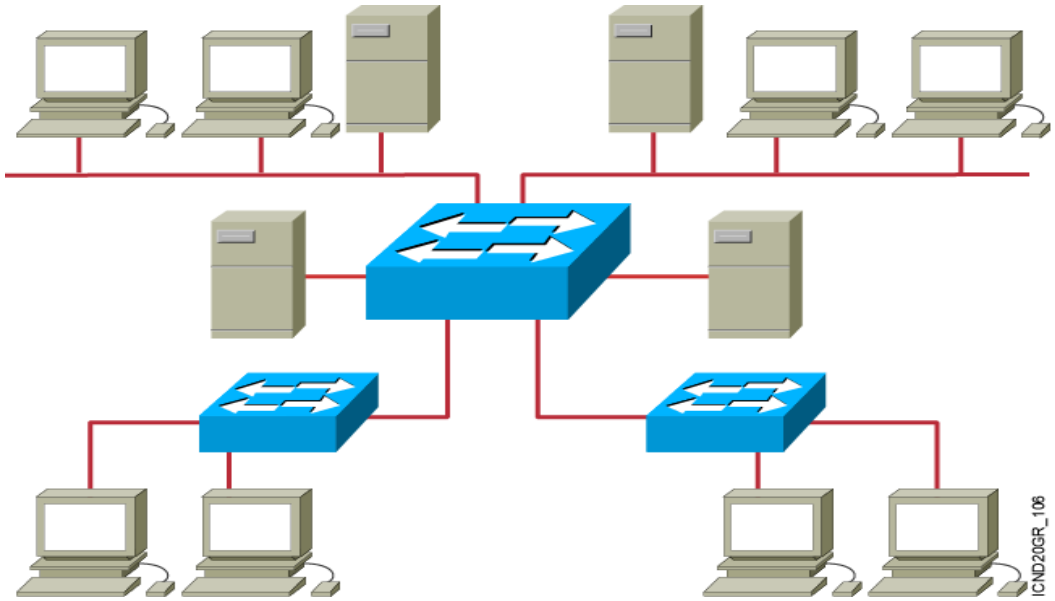
路由与交换技术

内容概要

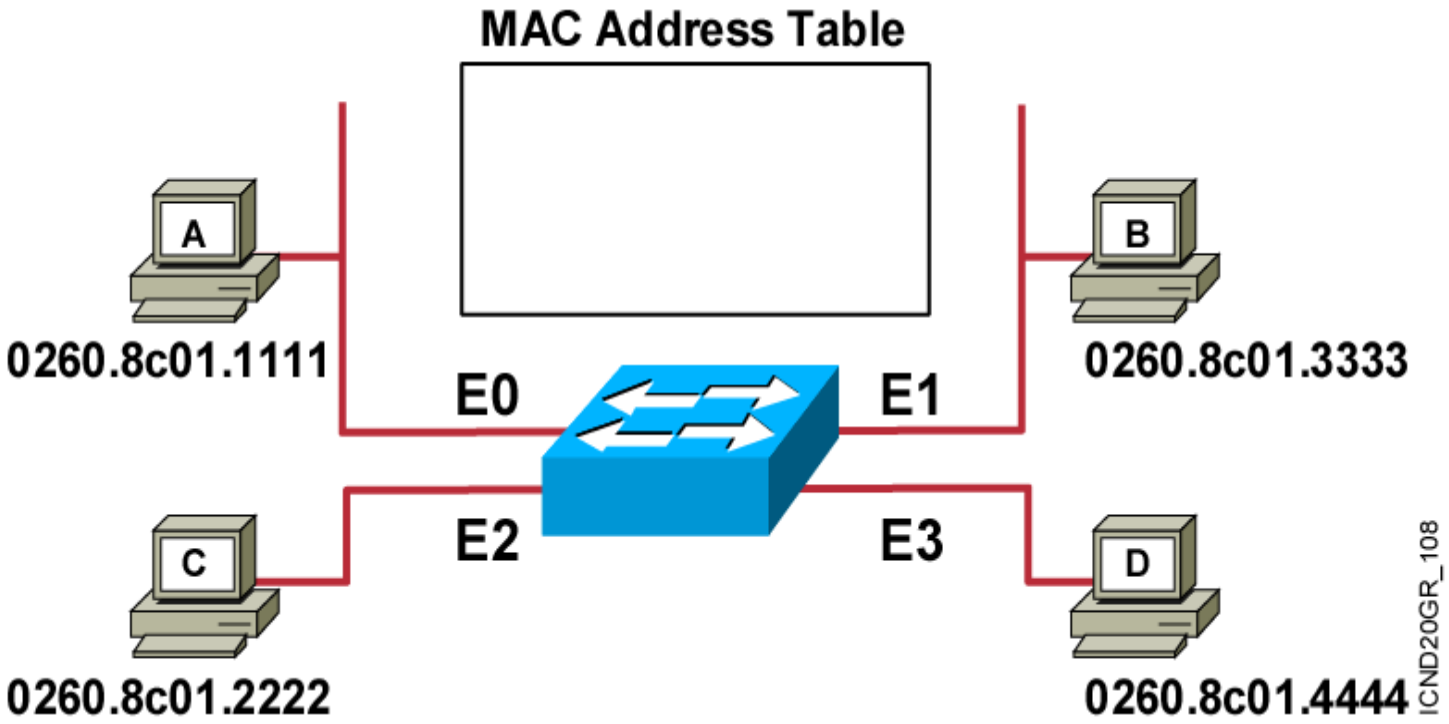
- 二层交换技术
- **VLAN**
- 路由技术
- 多层交换技术
- 网络地址转换（NAT）
- 移动Ad hoc网络路由技术简介

二层交换机的功能



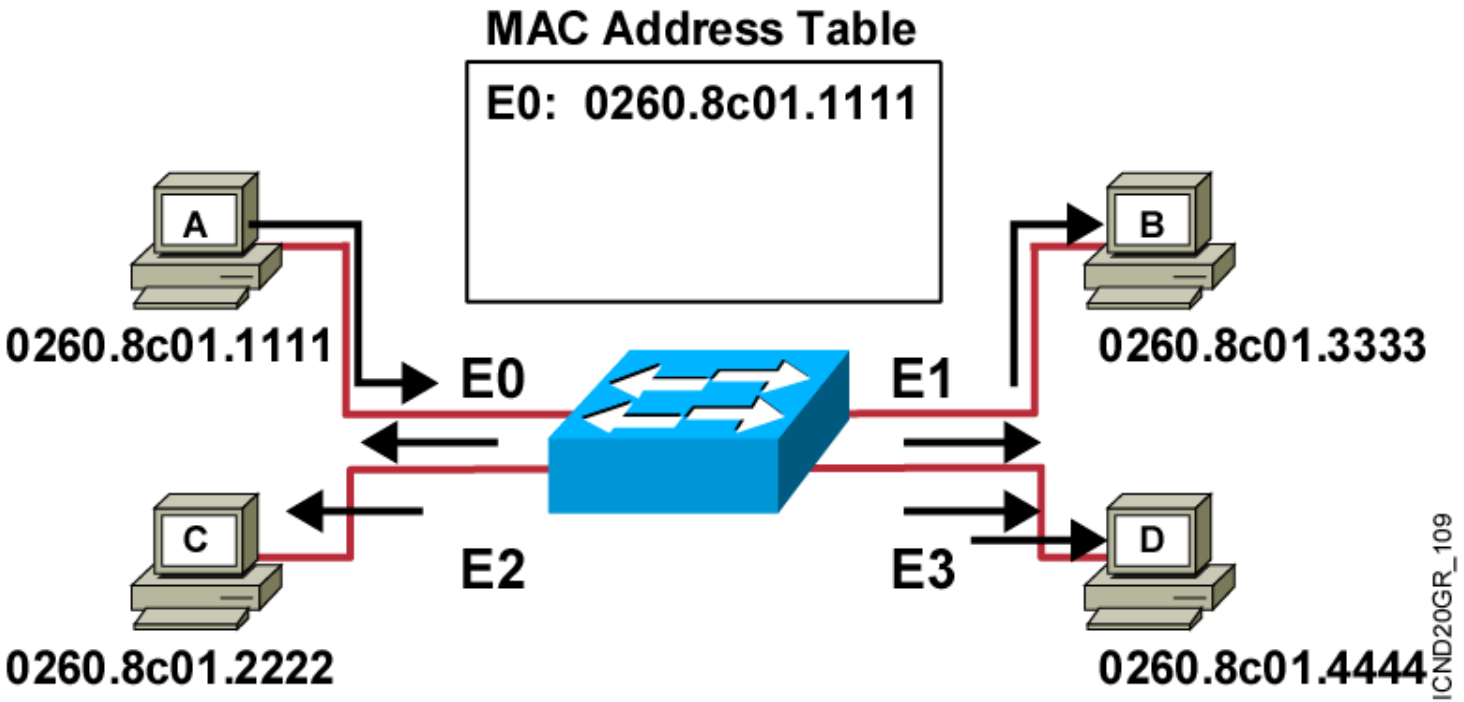
- 地址学习
- 转发/过滤决定
- 避免环路

基本交换原理-mac地址表



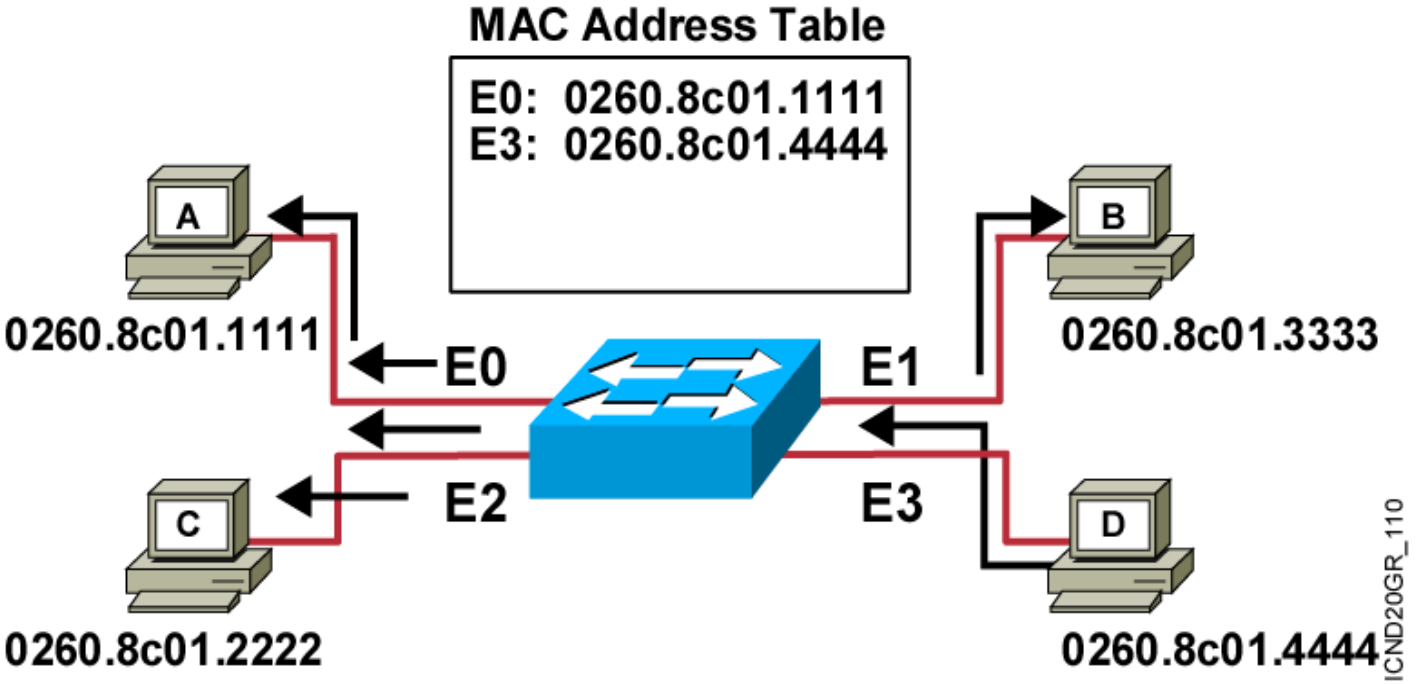
交换机初始化时MAC地址表是空的。

基本交换原理-地址学习



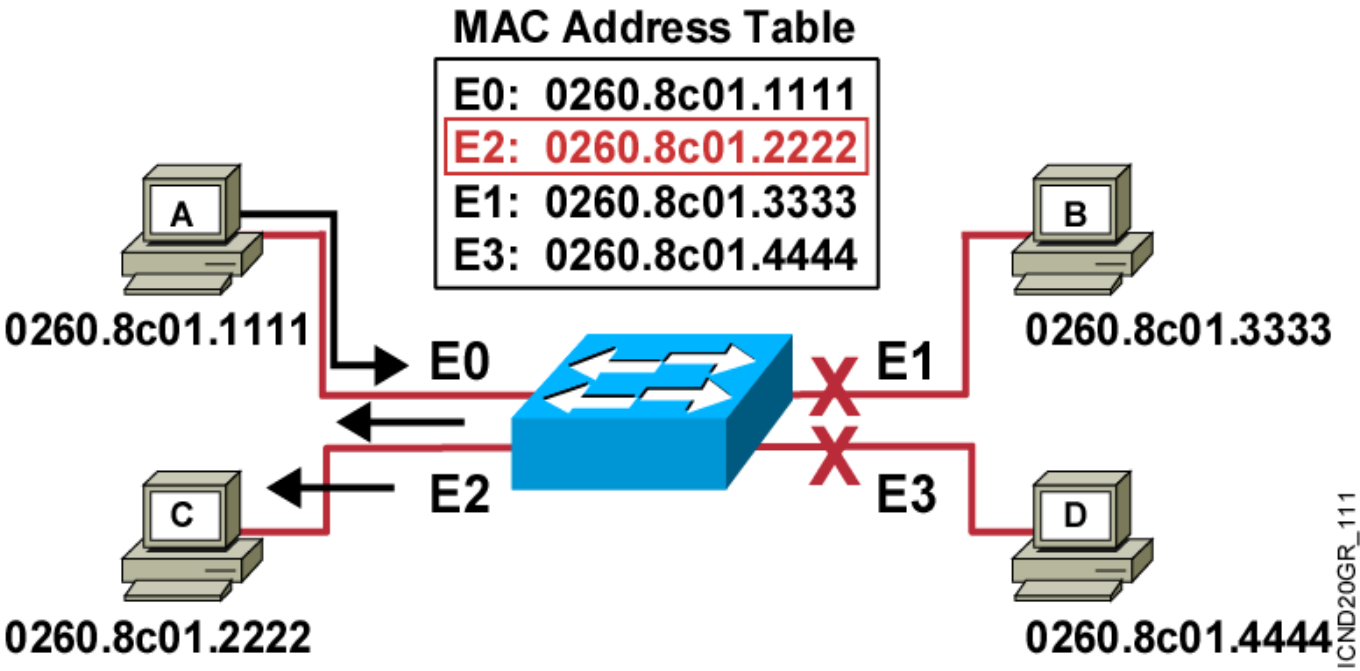
A欲与C进行通讯，不知A的mac地址，先进行ARP广播,交换机会学习到A的MAC地址。

基本交换原理-地址学习（续）



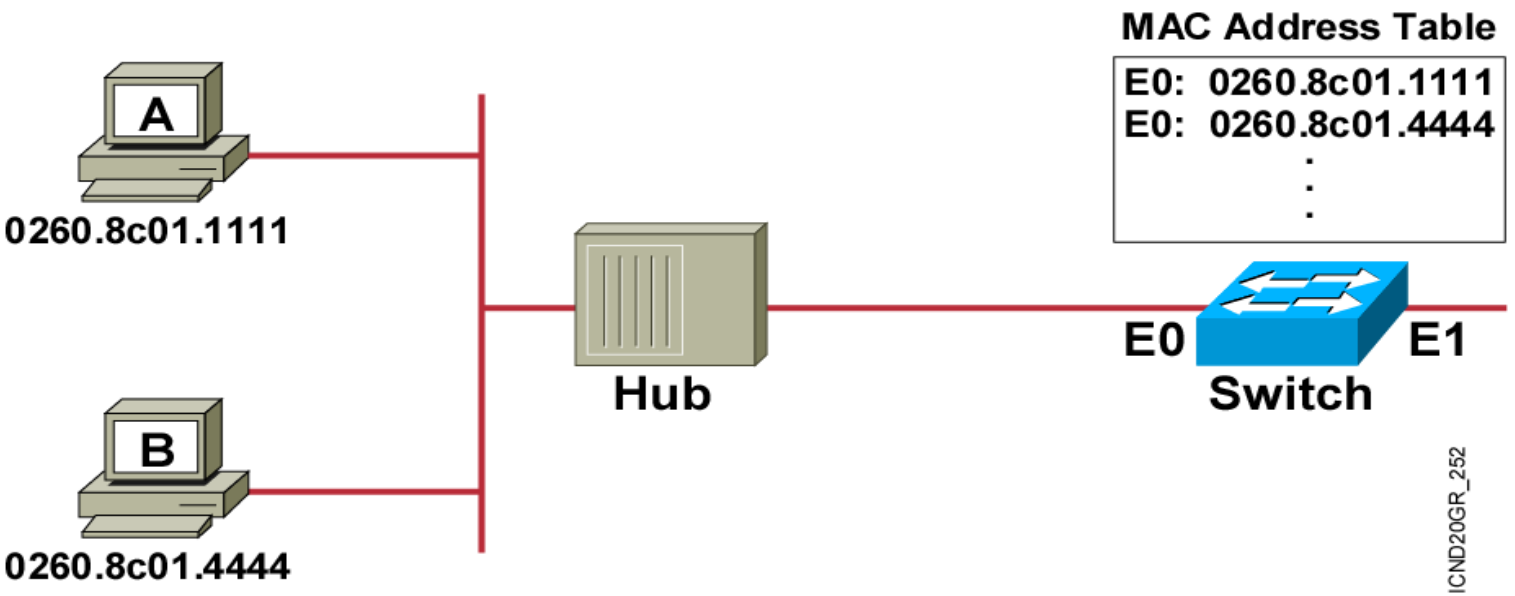
- D已知B的地址且发送数据帧与B通信
- 交换机未知B的地址只有进行广播
- 交换机学习到D的地址

基本交换原理-过滤



- 已知目的地不再广播

基本交换原理-过滤（续）


MAC Address Table
E0: 0260.8c01.1111
E0: 0260.8c01.4444
A
0260.8c01.1111
B
0260.8c01.4444
Hub
E0
E1
Switch
ICND20GR_252

思考：mac地址表攻击

- 攻击方法：

1.交换机MAC地址表溢出

2.MAC地址伪造

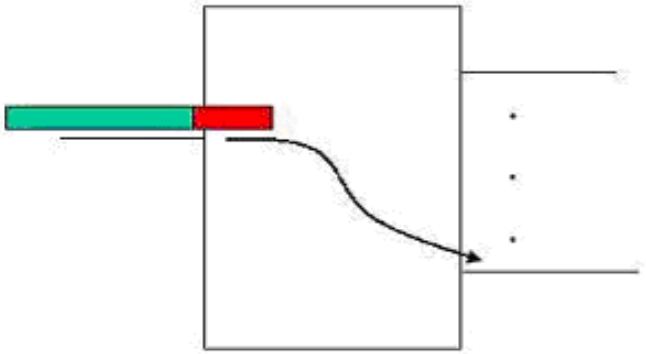
- 解决办法：

1.设置最多可学习到的MAC地址数

2.设置系统MAC地址老化时间

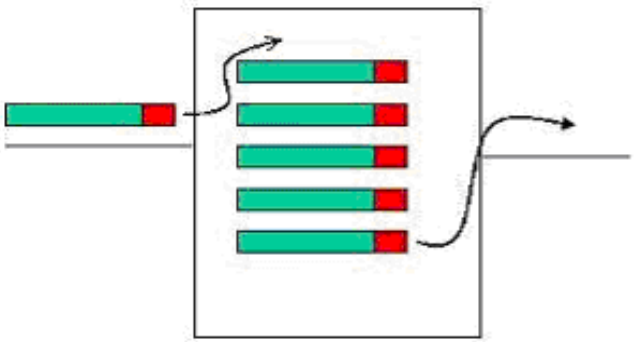
Lan交换机工作方式

- 直通式（Cut Through）方式在输入端口检测到一个数据包后，只检查其包头，取出目的地址，通过内部的地址表确定相应的输出端口，然后把数据包转发到输出端口．这样就完成了交换。因为它只检查数据包的包头（通常只检查14个字节）。



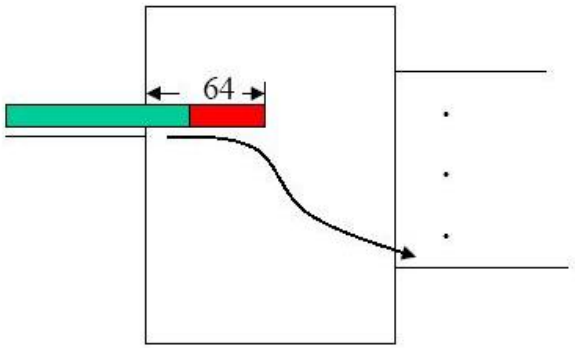
Lan交换机工作方式

- 存储转发（Store and Forward）是计算机网络领域使用得最为广泛的技术之一，在这种工作方式下．交换机的控制器先缓存输入到端口的数据包，然后进行CRC校验，滤掉不正确的帧，确认包正确后，取出目的地址，通过内部的地址表确定相应的输出端口，然后把数据包转发到输出端口。



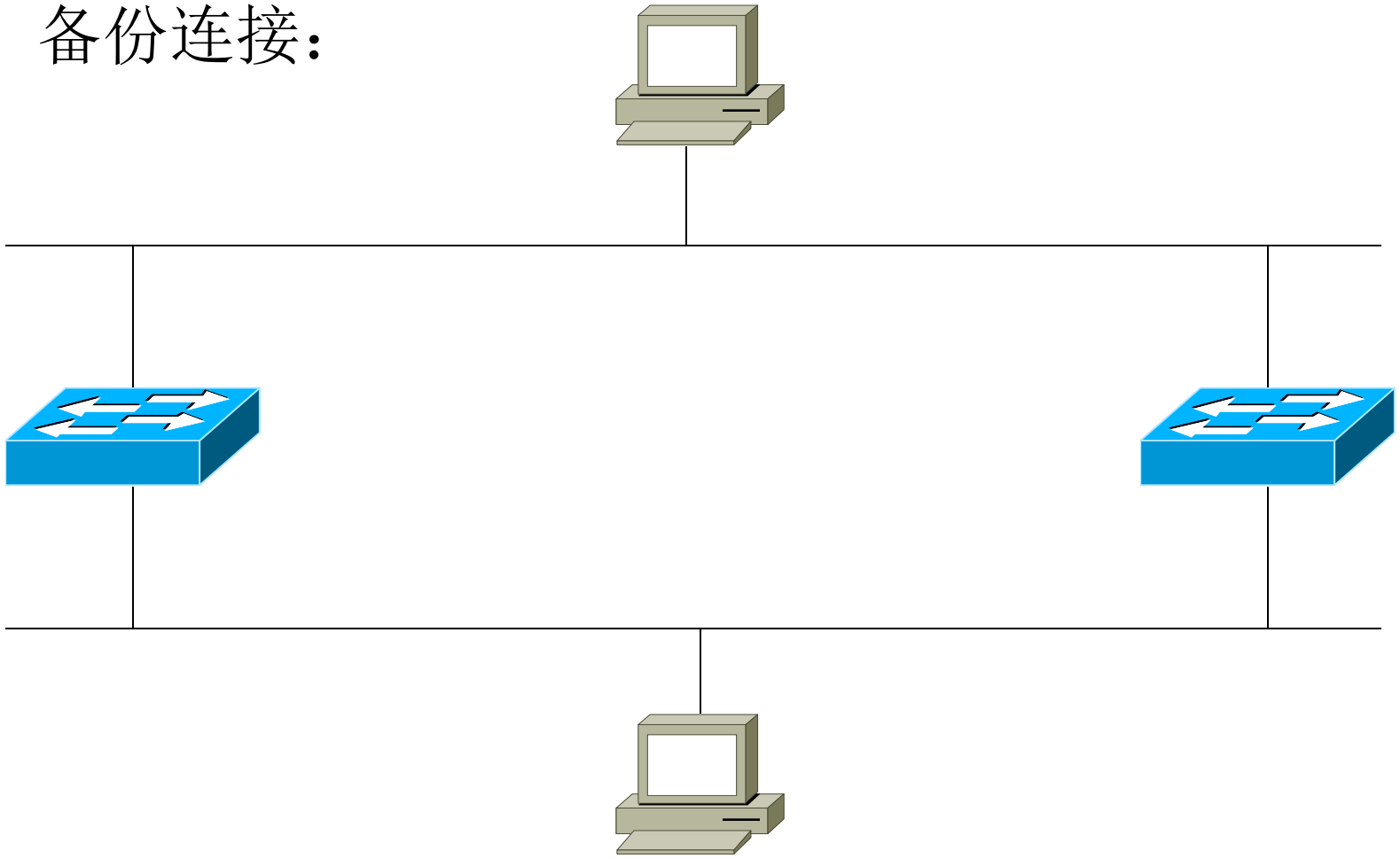
Lan交换机工作方式

- 无碎片直通（Fragment Free Cut Through）是介于直通式和存储转发式之间的一种解决方案，它检查数据包的长度是否够64 Bytes（512bit）如果小于64 Bytes，说明该包是碎片（即在信息发送过程中由于冲突而产生的残缺不全的帧），则丢弃该包，如果大于64 Bytes，则发送该包。该方式的数据处理速度比存储转发方式快，但比直通式慢。

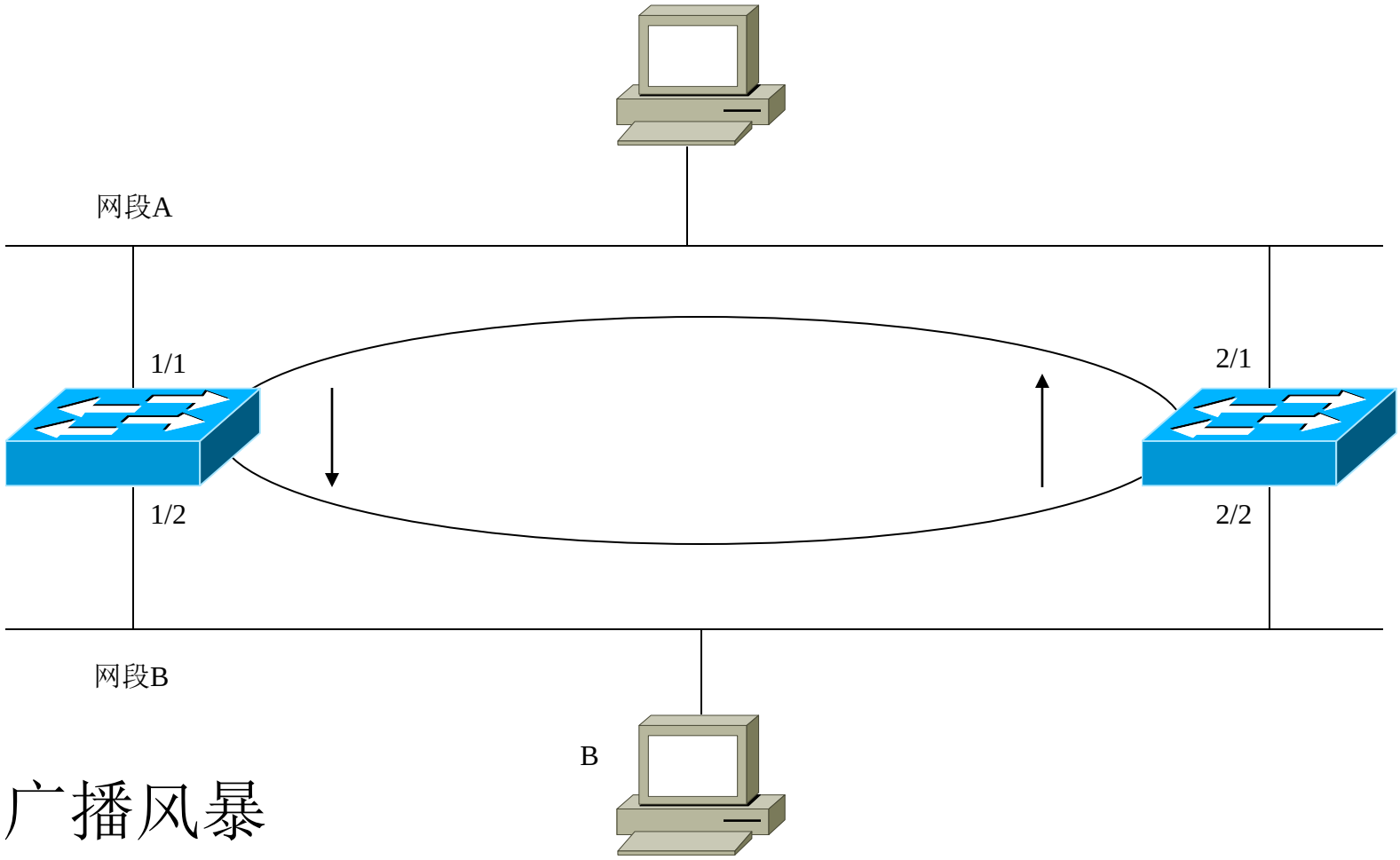


冗余拓扑

备份连接：

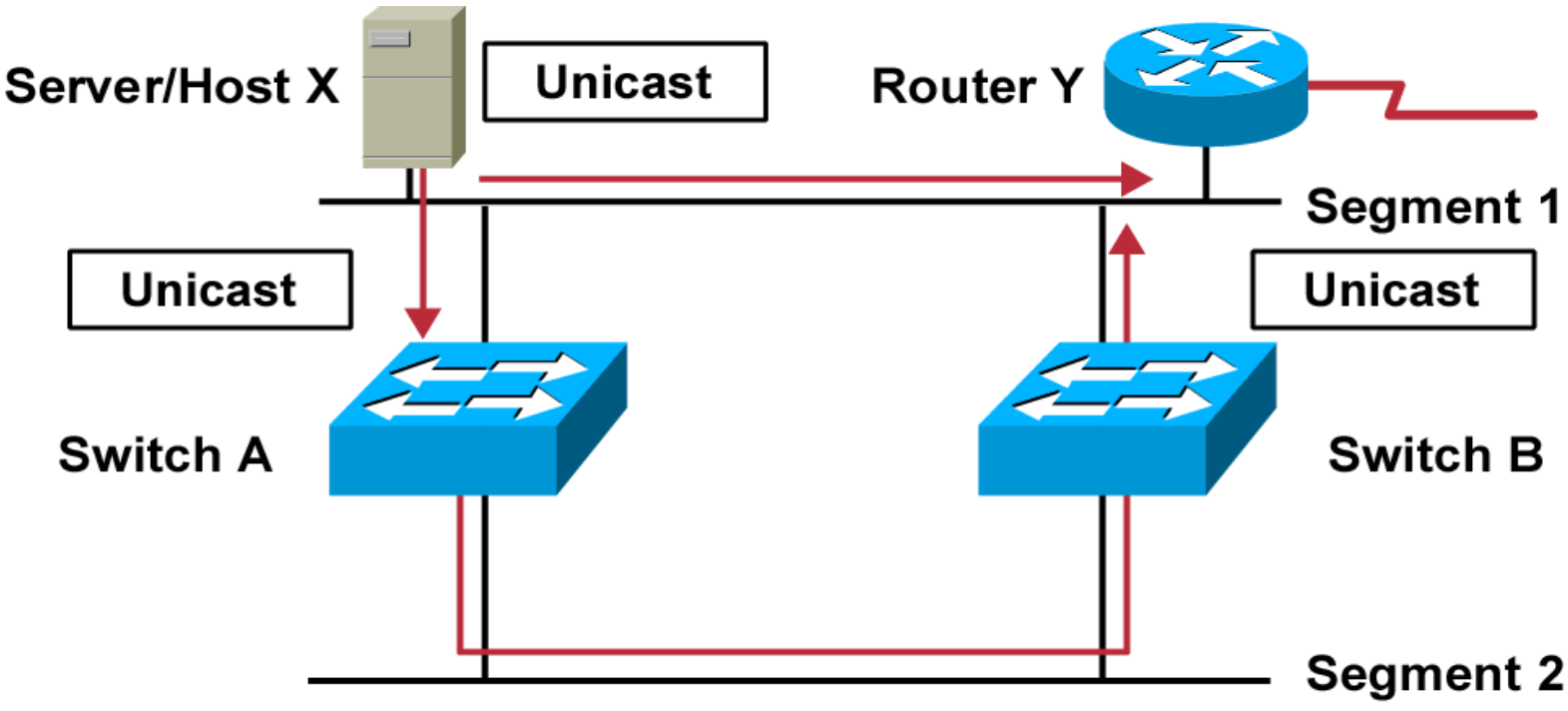


冗余拓扑



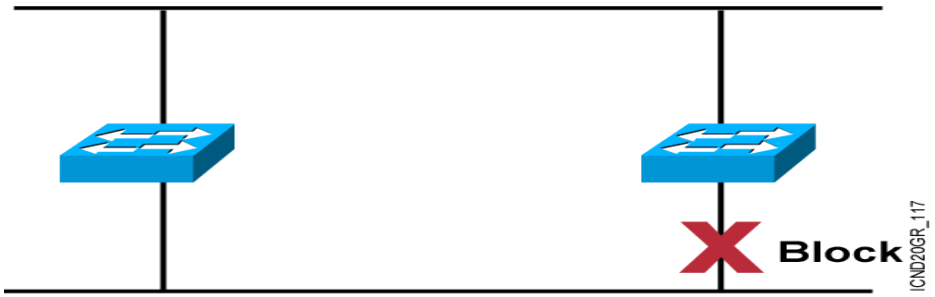
- 广播风暴
- MAC地址表不稳定

冗余拓扑–多帧复制



- 主机X发送单播帧到路由器 Y.
- 交换机A,B没有学习到路由器Y的MAC地址.
- 路由器 Y 将收到两份相同的帧.

生成树协议



- 生成树协议**(Spanning Tree Protocol-STP)**，两个标准：**802.1D**、**802.1w**。
- 生成树协议**(802.1D)**的目的是在保证提供冗余链路的前提下避免产生环路。
- 如何实现？

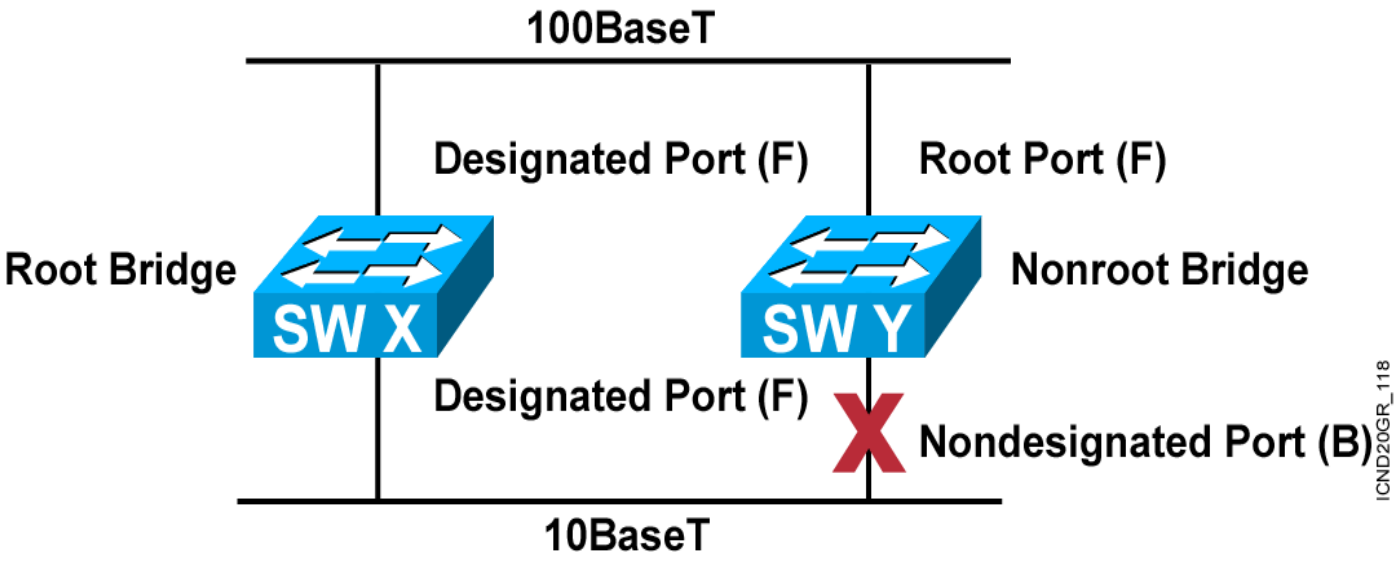
  交换机必须能够相互了解它们之间的连接情况，为了让其他的交换机知道它的存在，每台交换机向网络中发送**BPDU(Bridge protocol data unit)**的数据帧，如果某台交换机能够从两条或多条链路上收到同一台交换机的**BPDU**，则说明它们之间存在着冗余路径，就会产生环路。当存在环路时，交换机则使用生成树算法选择一条链路传递数据，并把某些相关的端口置于阻塞**(Blocking)**状态以将其他的链路虚拟地断开，一旦当前正在使用的链路出现故障，就会把某个阻塞的端口打开以接替原来的链路工作。

生成树协议-术语

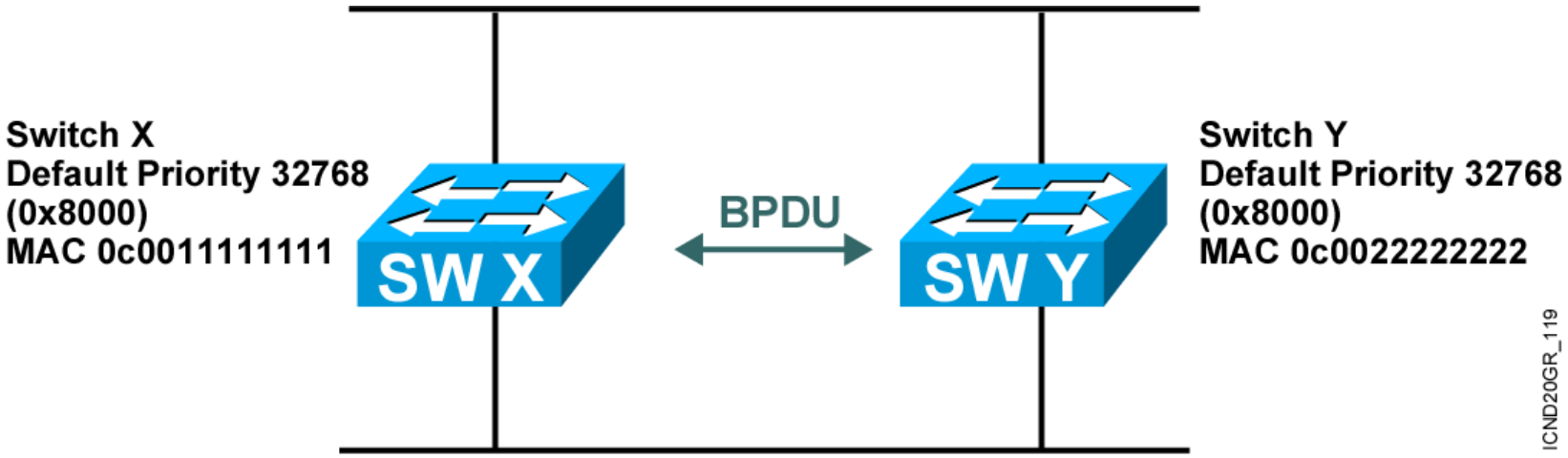
- 根桥：桥ID最低。网络中，所有决定（如哪一个端口要被阻塞，哪一个端口要被置为转发模式）都是根据根桥的判断来做出选择。
- BPDU：交换机之间交换的信息，利用这些信息选出根交换机以及进行网络的后续配置。
- 桥ID：利用它来跟踪网络中的所有交换机。由桥优先级(在所有的Cisco交换机上，默认的优先级为32768)和基本MAC地址的结合来决定的。在网络中，桥ID最低的为根桥。
- 根端口：指直接连到根桥的链路所在的端口，或者到根桥的路径最短的端口。如果有多条链路连接到根桥，就通过检查每条链路的带宽来决定端口的开销，开销最低的端口就成为根端口。
- 指定端口：根端口或者有最低开销的端口就是指定端口，指定端口被标记为转发端口，能够转发帧。
- 端口开销：取决于链路的带宽。
- 非指定端口：将被置为阻塞状态，不能转发帧

生成树协议-执行过程

- 在同一网络内（广播域范围内）选举一台交换机为根桥（**Root)**
- 在每个非根桥的交换机上选举根端口**(Root Port)**
- 在每个网段上选举指定端口
- 落选的端口进入阻塞状态



生成树协议-执行过程-选举根桥



- 根桥：拥有最低的桥ID
- 桥ID由优先级和基本mac地址决定

生成树协议-执行过程-选举根端口、指定端口

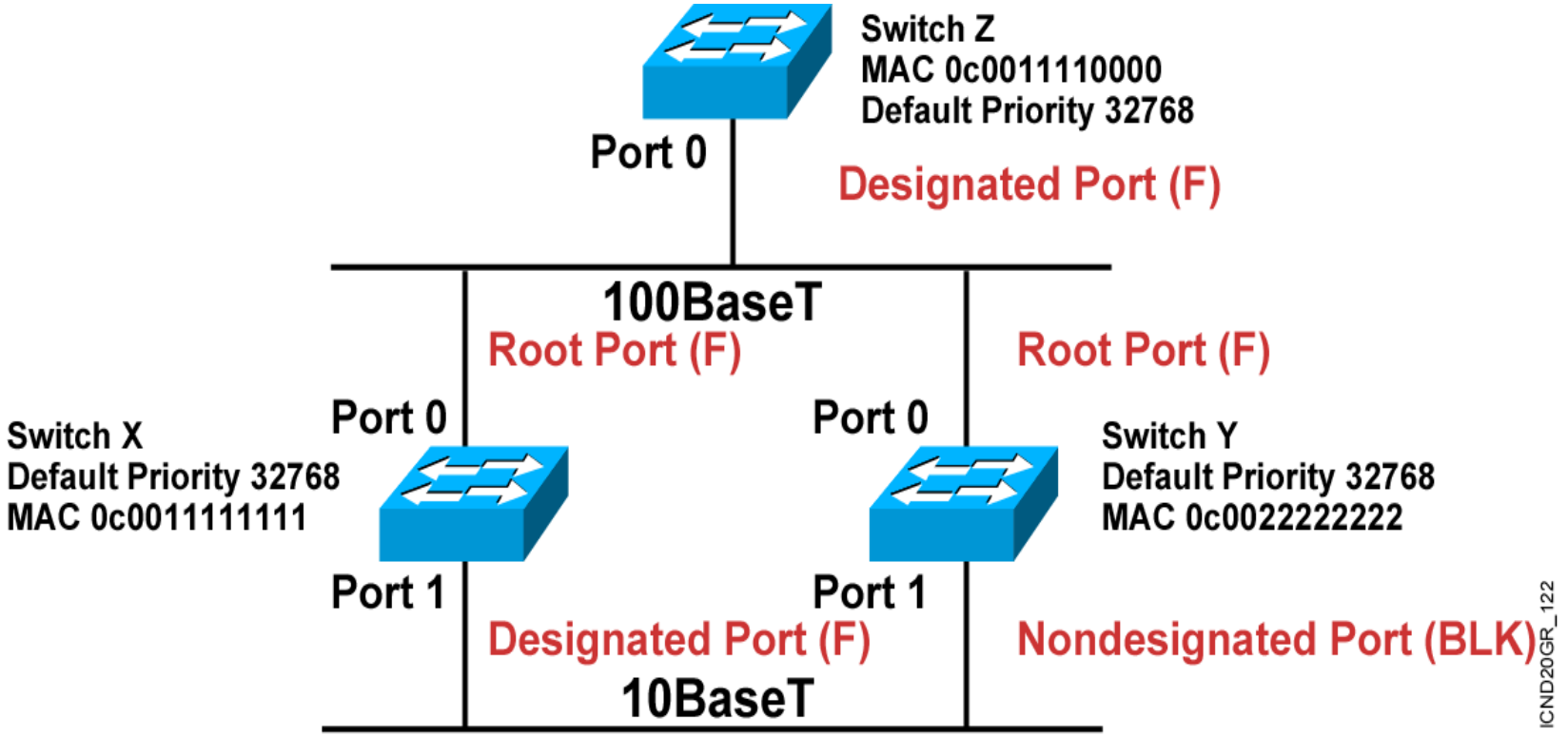
- 选举根端口：比较从各端口到达根桥的路径花费，最小的为根端口
- 选举指定端口：比较网段中各端口到达根桥的路径花费，最小的为指定端口
- 路径花费相同则比较转发根桥BPDU的交换机ID；如ID同，比较端口优先级，如端口优先级同，比较端口ID

Link Speed	Cost (Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

ICND20GR_121

生成树协议-例

- 选举根桥
- 选举根端口
- 选举指定端口



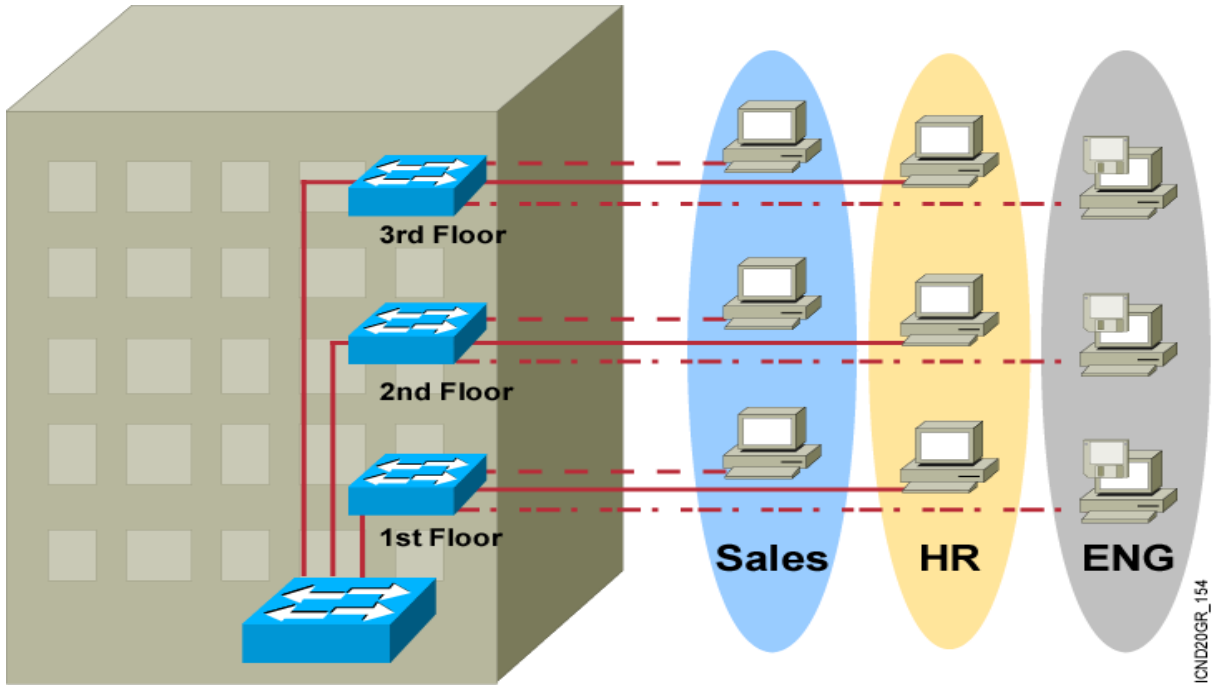
内容概要

- 二层交换技术
- VLAN
- 路由技术
- 多层交换技术
- 网络地址转换（NAT）
- 移动Ad hoc网络路由技术简介

VLAN

- 虚拟网络建立在局域网交换机之上;
- VLAN是一个广播域，是由一些局域网网段构成的与物理位置无关的逻辑组;
- 以软件方式实现对逻辑工作组的划分与管理;
- 一个逻辑工作组的结点可以分布在不同的物理网段上，但它们之间的通信就像在同一个物理网段上一样;
- 一个VLAN就好像是一个孤立的网段，VLAN间不能直接通信，实现VLAN间互联必须借助于路由器(或具有三层交换功能的交换机）。

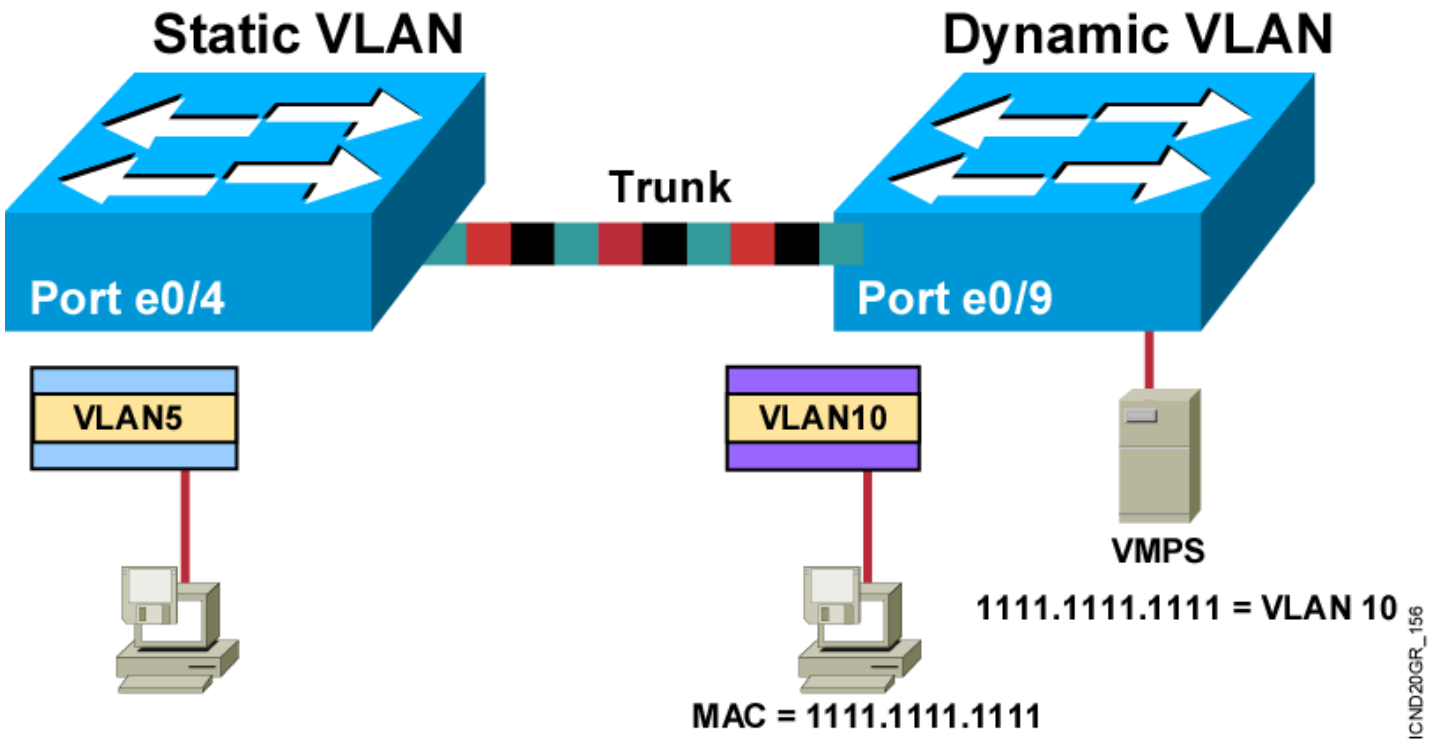
VLAN



- 广播控制
- 安全性
- 灵活性

VLAN分类

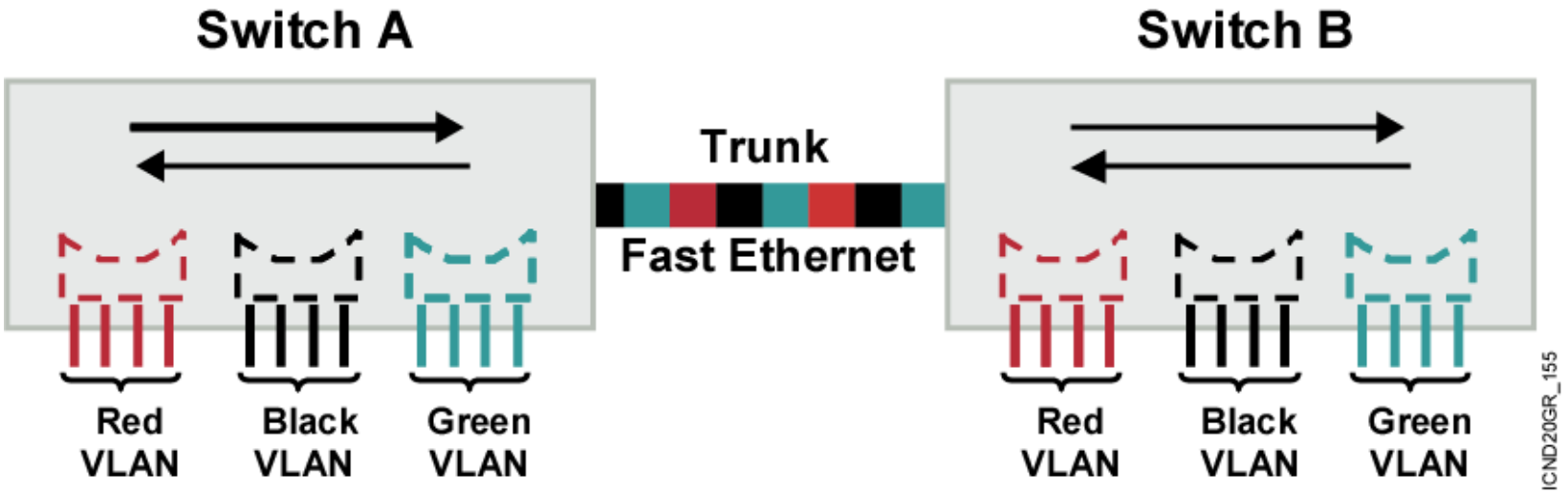
根据使用和管理**VLAN**的不同情况，**VLAN**分为两种：
静态**VLAN**和动态**VLAN**。



VLAN分类（续）

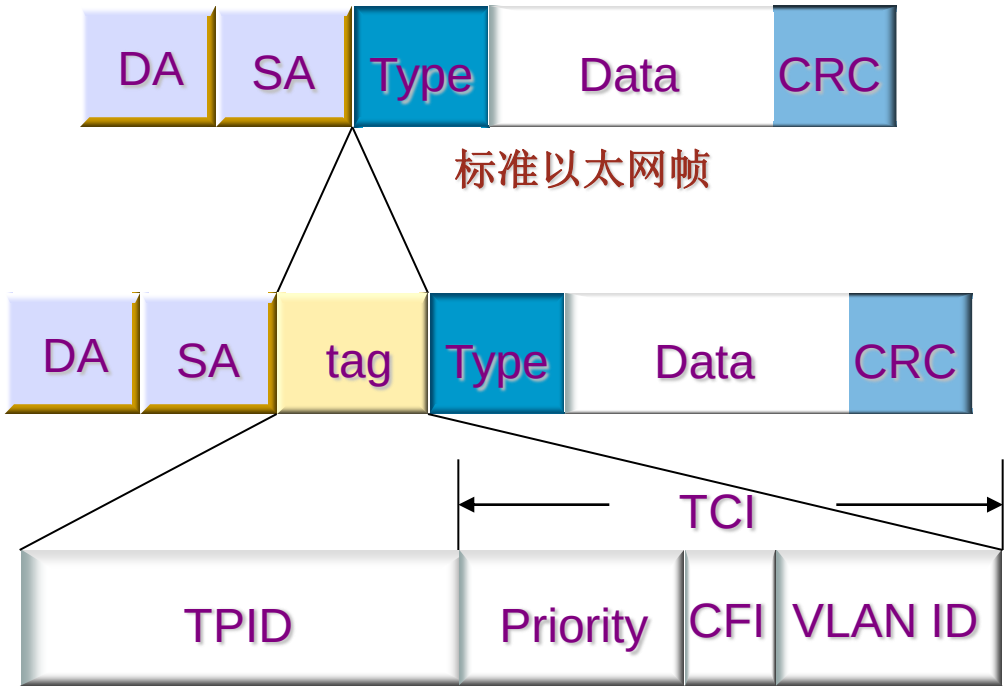
- 静态VLAN，基于瑞口的VLAN，因为用户的主机属于哪个VLAN是根据交换机的端口属于哪个VLAN而定的。网络管理员首先把端口分配到不同的VLAN内，根据规划把用户的主机与相应的端口相连，这样就把用户分配到了对应的VLAN内。
- 动态VLAN。动态VLAN的实现方法有多种，最普通的实现方法是基于MAC地址的动态VLAN。
  - 基于MAC地址的动态VLAN需要一台VMPS(VLAN Management Policy Server)，VMPS可以是一台具有该功能的交换机(如catdyst 5000交换机)或是一台外部服务器，VMPS中维护着MAC地址与VLAN的对应关系表。
  - 需要把交换机的端口设置为支持动态VLAN属性的端口。
  - 当交换机的支持动态VLAN的端口接收到数据帧时，通过使用该数据帧的源MAC地址查询VMPS，从而建立起端口与VLANN的对应关系。

VLAN标记技术



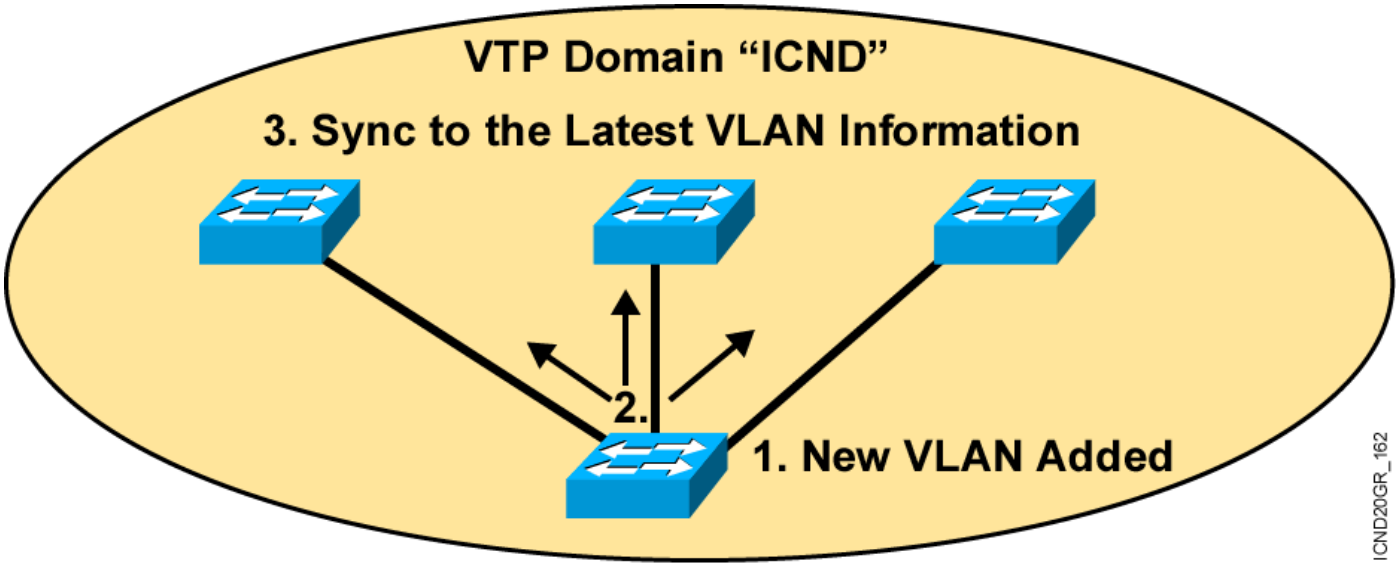
- VLAN可以跨越多台交换机，两个问题，物理通道的问题、区分不同VLAN数据的问题。
- 一个物理通道，但对来自不同VLAN的数据进行标记。这条通道上就承载看多个VLAN的数据，这样的链路称为trunk(干道).
- Trunk链路是通过在交换机上设置trunk端口，并把它们连起来。
- 以太网中两种标记技术：CISCO的ISL(inter-switch link)和IEEE802.1Q

符合IEEE802.1Q标准的以太网帧



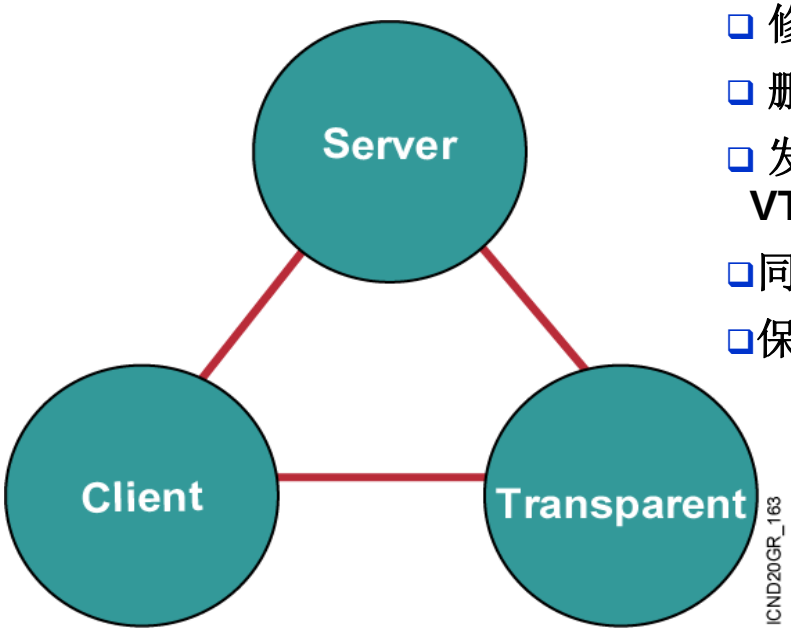
VLAN中继协议

- **VLAN**技术独立于地理位置根据工作组或业务类型组织网络资源。
- 管理的不便（如**VLAN**跨交换机，则该交换机须配置**VLAN**），易生成网络网络规划的不一致。
- 解决办法：**VLAN**中继协议**(VLAN Trunk Protocol)**
- **VTP:**
  - 将添加的**VLAN**动态的报告给**VTP**域中的所有的主机
  - 在网络中所有交换机上实现**vlan**配置的一致性
  - **VTP**信息通过中继（**trunk**）端口在交换机上传送



VLAN中继协议-VTP模式

- 创建 VLANs
- 修改 VLANs
- 删除 VLANs
- 发送/转发通告到整个VTP域
- 同步
- 保存在NVRM中



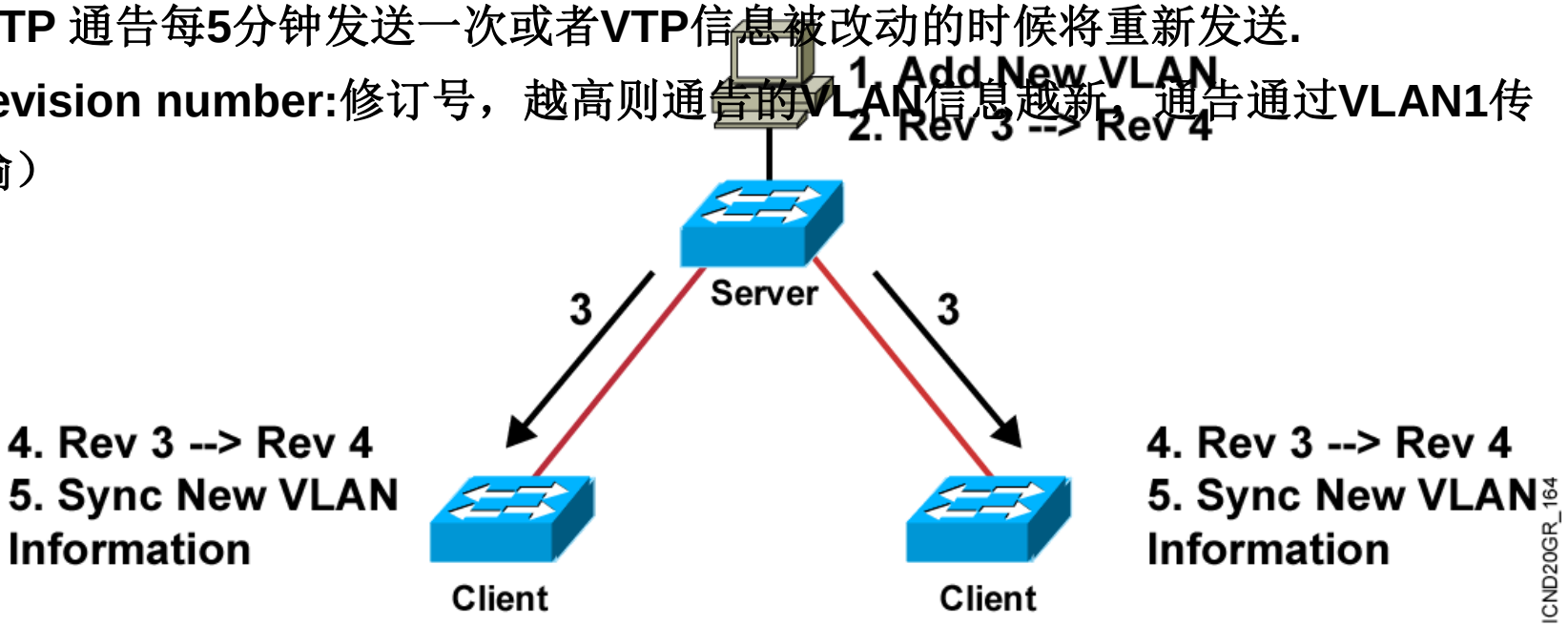
- 发送接收通告
- 同步
- 不保存在NVRM中

- 创建 VLANs
- 修改 VLANs
- 删除 VLANs
- 转发通告
- 不同步
- 保存在NVRM中

VLAN中继协议-VTP操作

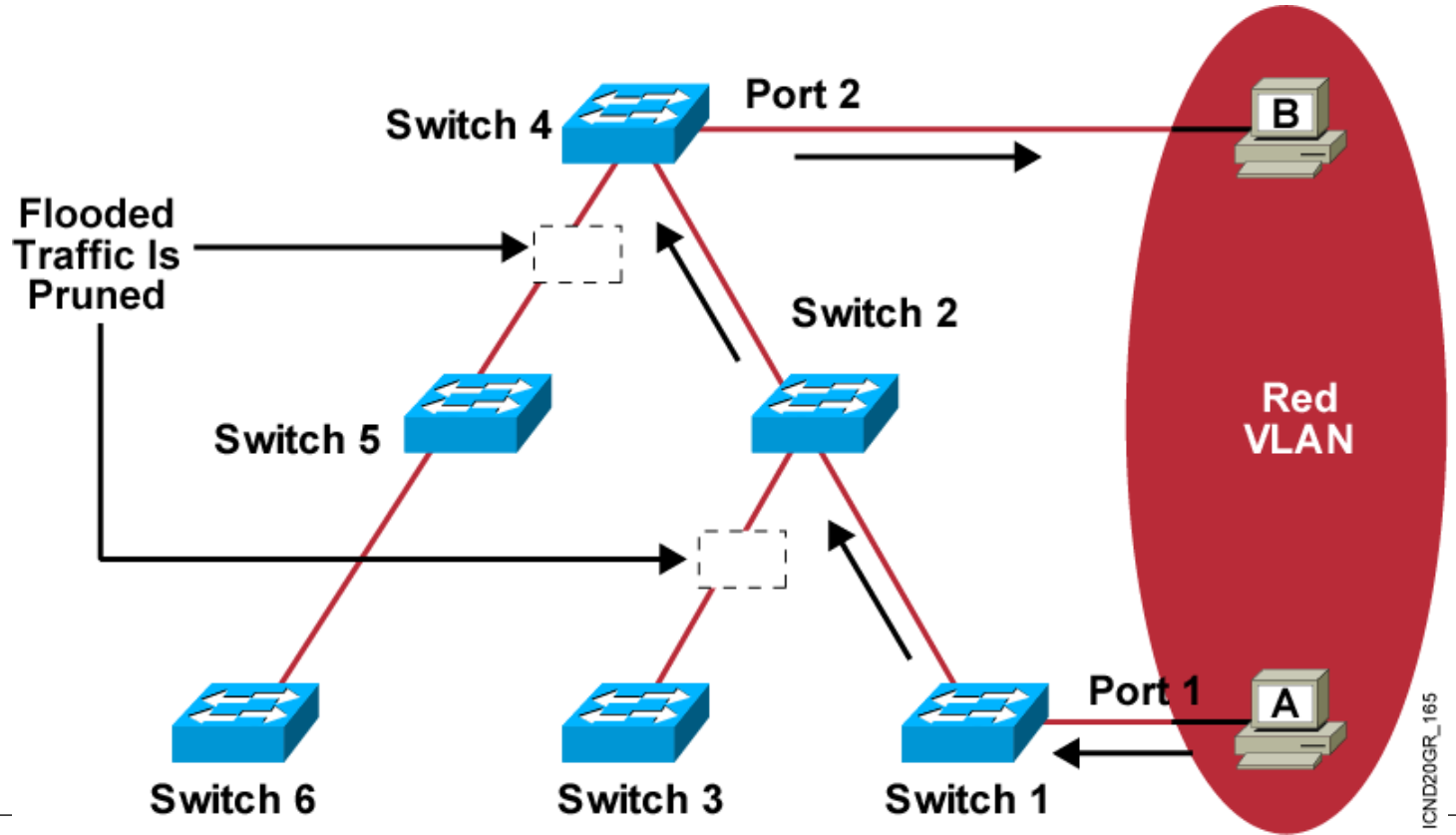
- VTP 通告以组播形式发送.
- VTP 服务端和客户端将同步到最新的修订号.
- VTP 通告每5分钟发送一次或者VTP信息被改动的时候将重新发送.

（revision number:修订号，越高则通告的VLAN信息越新，通告通过VLAN1传输）



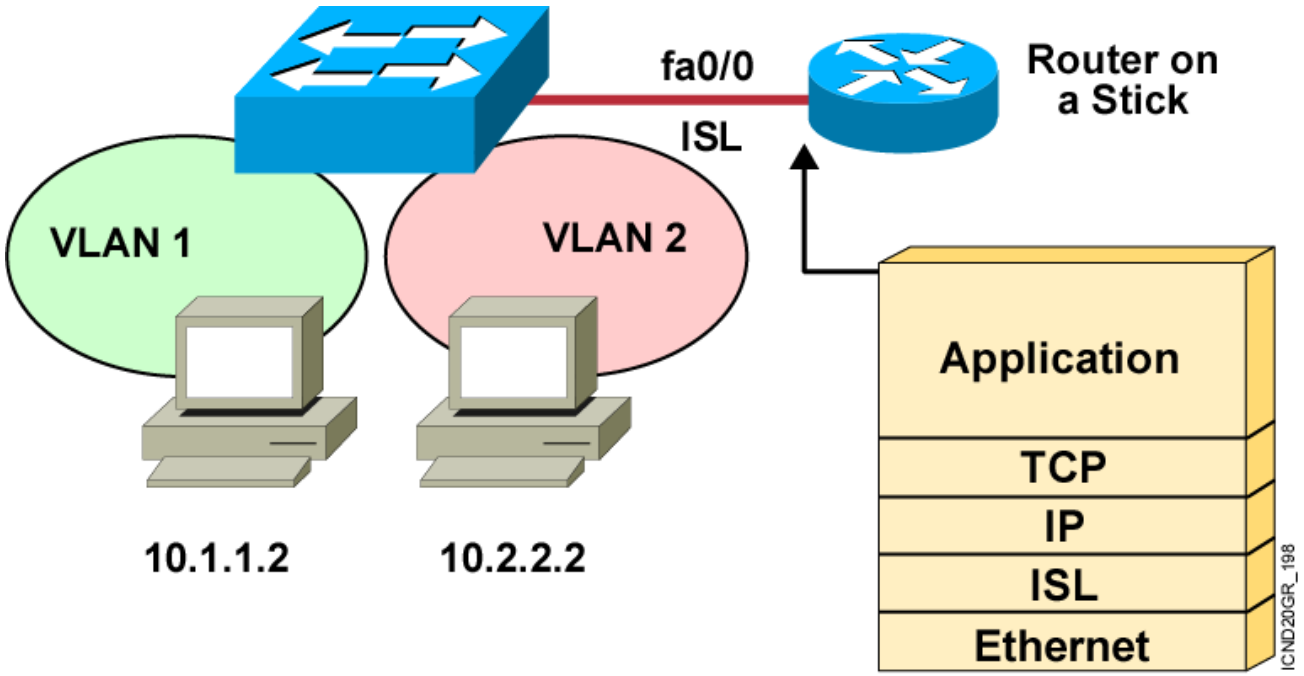
VLAN中继协议-VTP修剪

- 通过减少广播、组播和其他单播包的数量来保留带宽
- 如：A只广播发送到配了red vlan的中继链路上

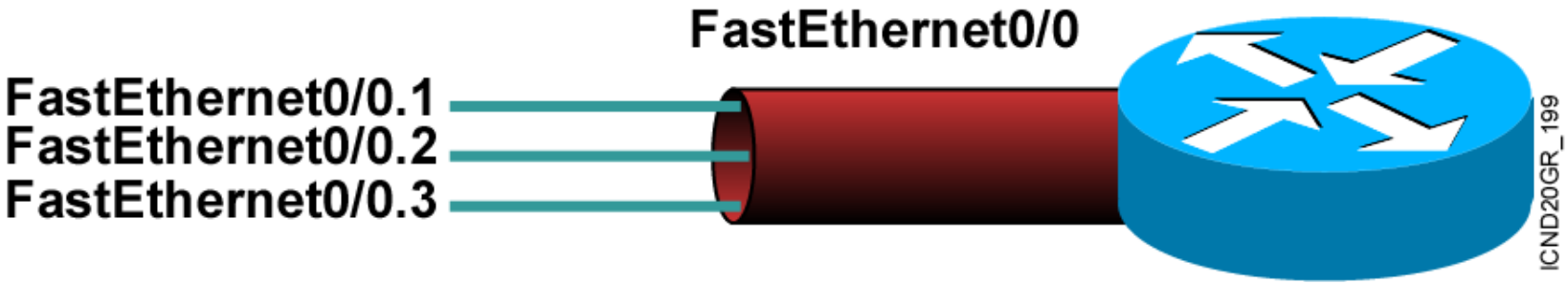


跨VLAN通信

- VLAN间的通信需要路由器作为中间设备
- 如何通信，路由器作为缺省网关，两种办法：外部路由器、使用具有三层交换功能的交换机

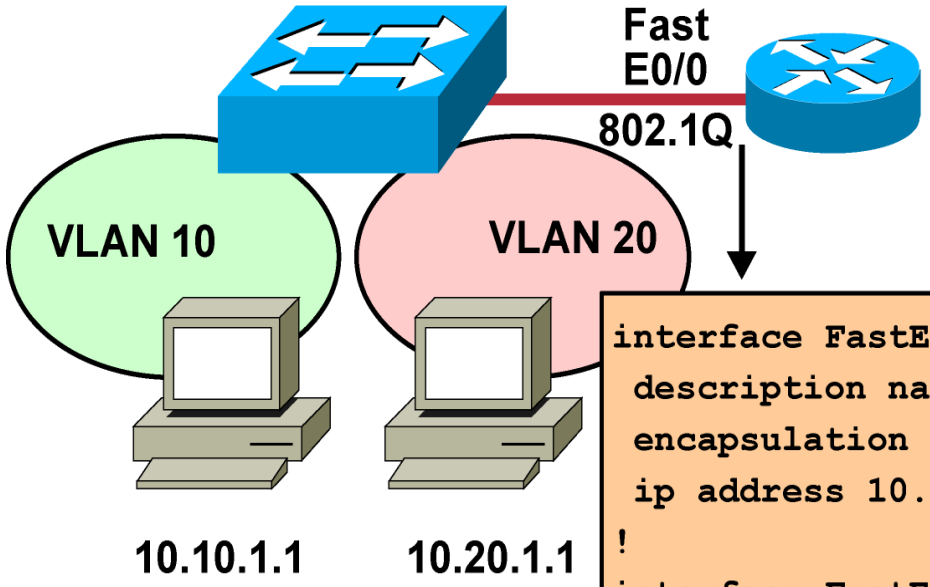


跨VLAN通信-子接口



- 物理接口**FastEthernet 0/0**可被划分成多个子接口。

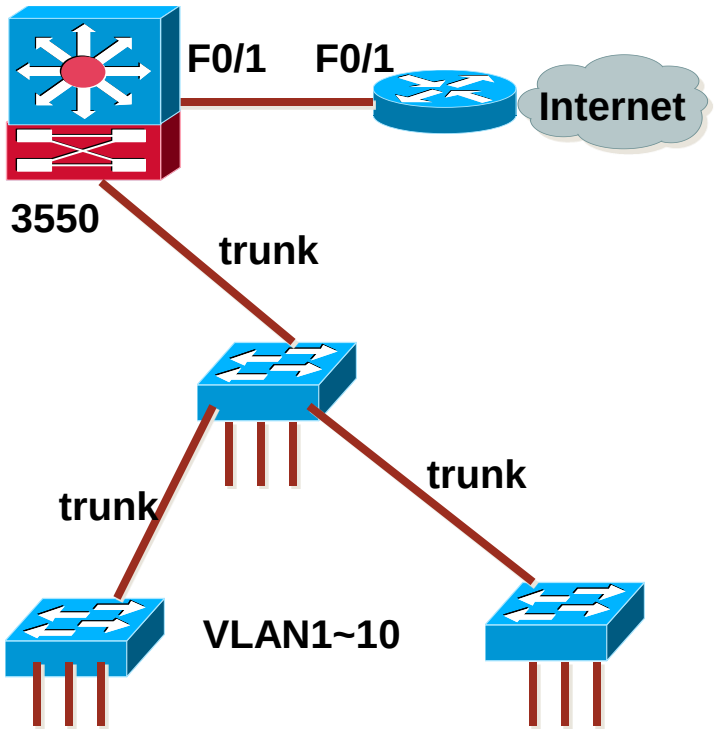
跨VLAN通信-802.1Q TRUNK




```
interface FastEthernet0/0.1
 description native vlan - VLAN 1 is un frame tagged
 encapsulation dot1q 1 native
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.1.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.1.1 255.255.255.0
!
```

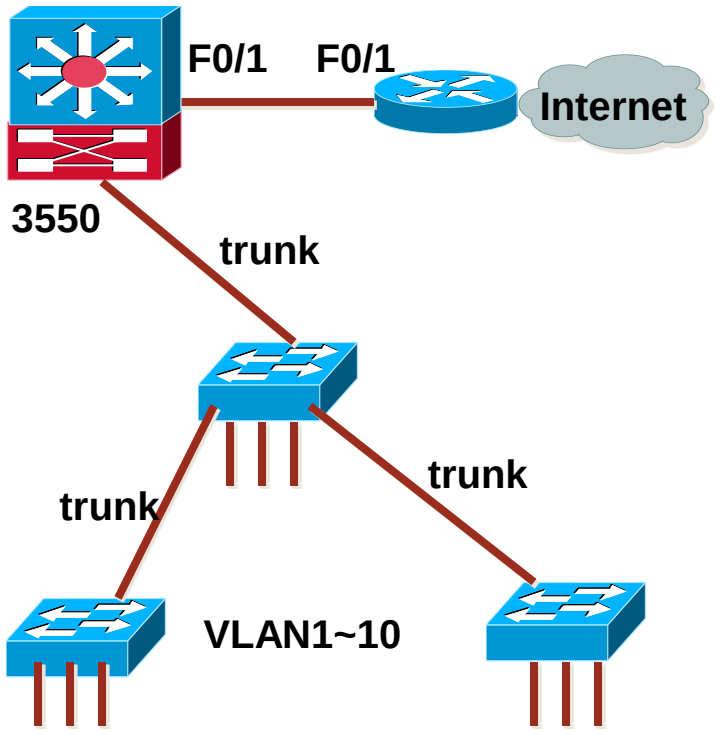
跨VLAN通信-内部路由方法

- 使用一台具有三层交换功能的交换机。
- 2层和三层的功能集成在一起，无需外部路由器
- 虚拟的具有第三层功能的接口与每一个VLAN相连，为跨VLAN的通信提供服务



- **10个VLAN，3550承担VLAN间通信**
- **3550和路由器相连**
- **Valn1~vlan10的地址为：10.10.1.0~10.10.10.0/24**
- **3550的f0/1端口地址：10.10.11.2/24**
- **路由器的f0/1端口地址：10.10.11.1/24**

跨VLAN通信-内部路由方法



3550配置

- 打开IP路由

  Switch3550(config)#ip routing
- **Show vlan命令，确认3550有1~10号vlan**
- 为每个vlan设置虚拟接口，并配置IP地址

  Switch3550(config)#interface Vlan2

  Switch3550(config-if)#ip address 10.10.2.1 255.255.255.0

  Switch3550(config-if)#no shut
- 把f0/1接口设为路由器接口并配置IP地址

  Switch3550(config)#interface Fa 0/1

  Switch3550(config-if)#no switchport

  Switch3550(config-if)#ip address 10.10.11.2 255.255.255.0

  Switch3550(config-if)#no shut
- 为访问Internet设置默认路由

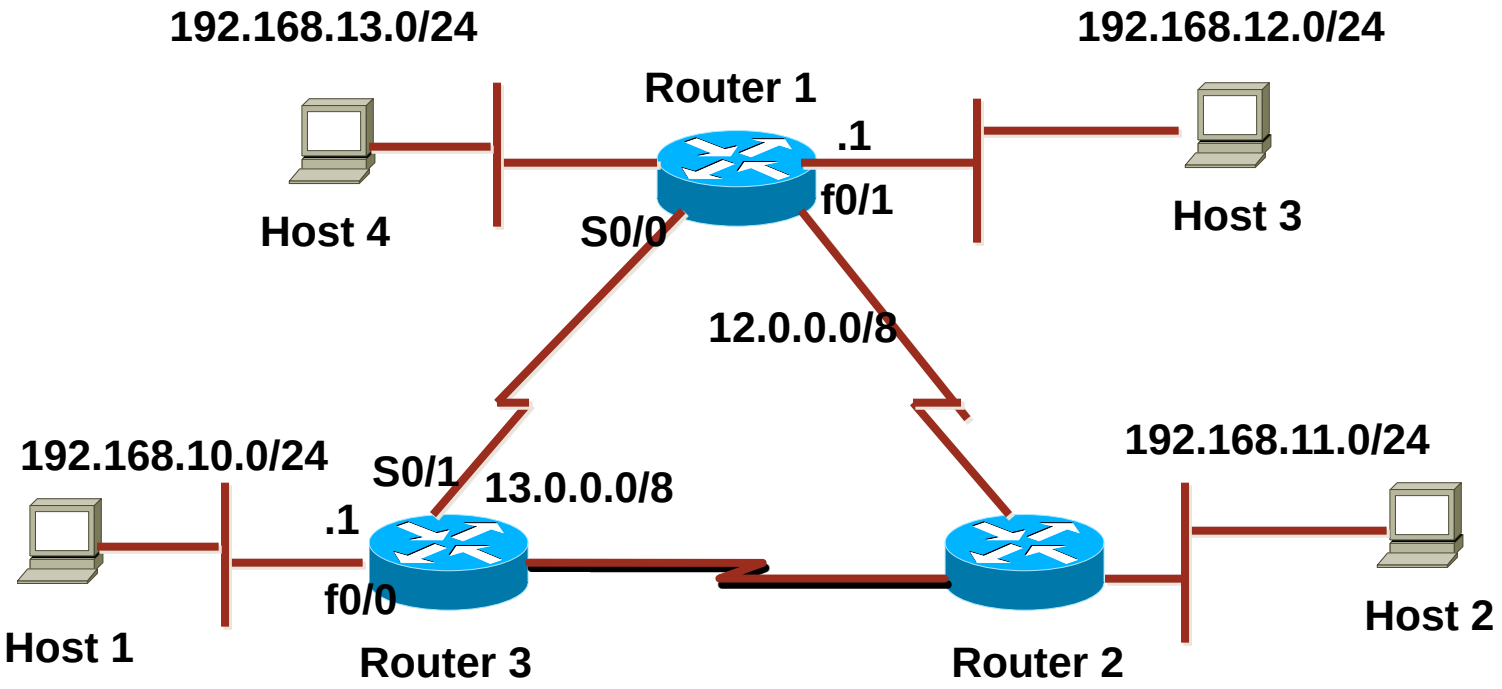
  Switch3550(config)#ip route 0.0.0.0 0.0.0.0 10.10.11.1

内容概要

- 二层交换技术
- VLAN
- 路由技术
- 多层交换技术
- 网络地址转换（NAT）
- 移动Ad hoc网络路由技术简介

路由基本概念

路由是把数据从一个网络转发到另一个网络的过程，
完成这个过程的设备就是路由器



路由技术的构成

通常所说的路由技术其实是由两项最基本的活动组成，即决定最优路径和传输信息单元（也被称为数据包）。

其中，数据包的传输和交换相对较为简单和直接，而路由的确定则更加复杂一些。

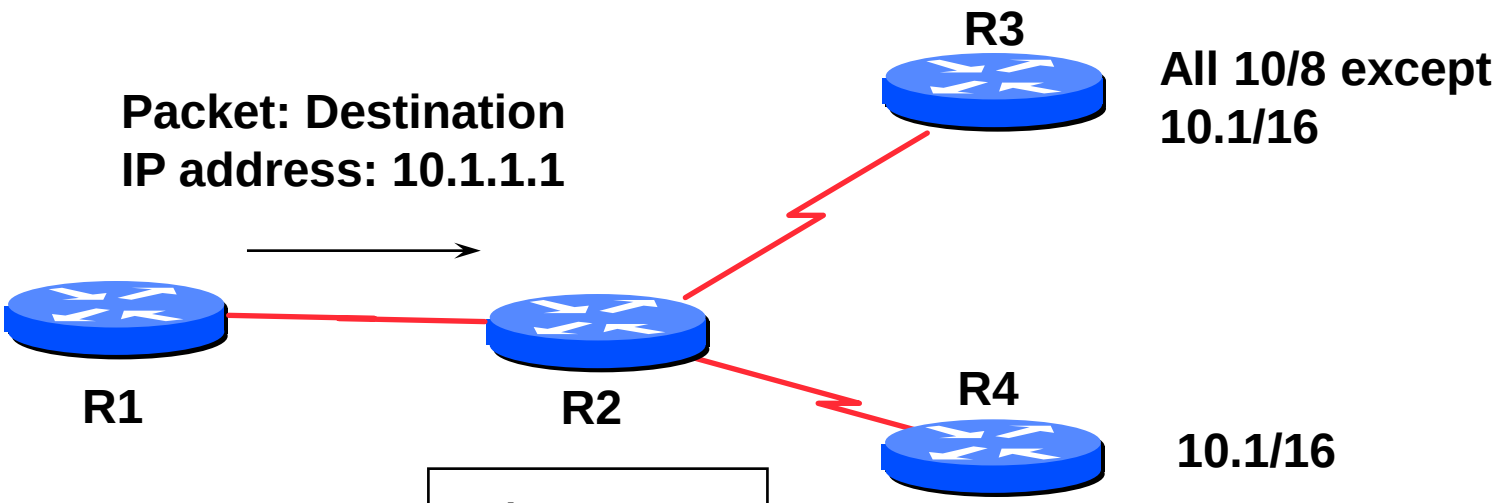
路由器

- 路由器是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读”懂对方的数据，从而构成一个更大的网络。

路由表和目的地址

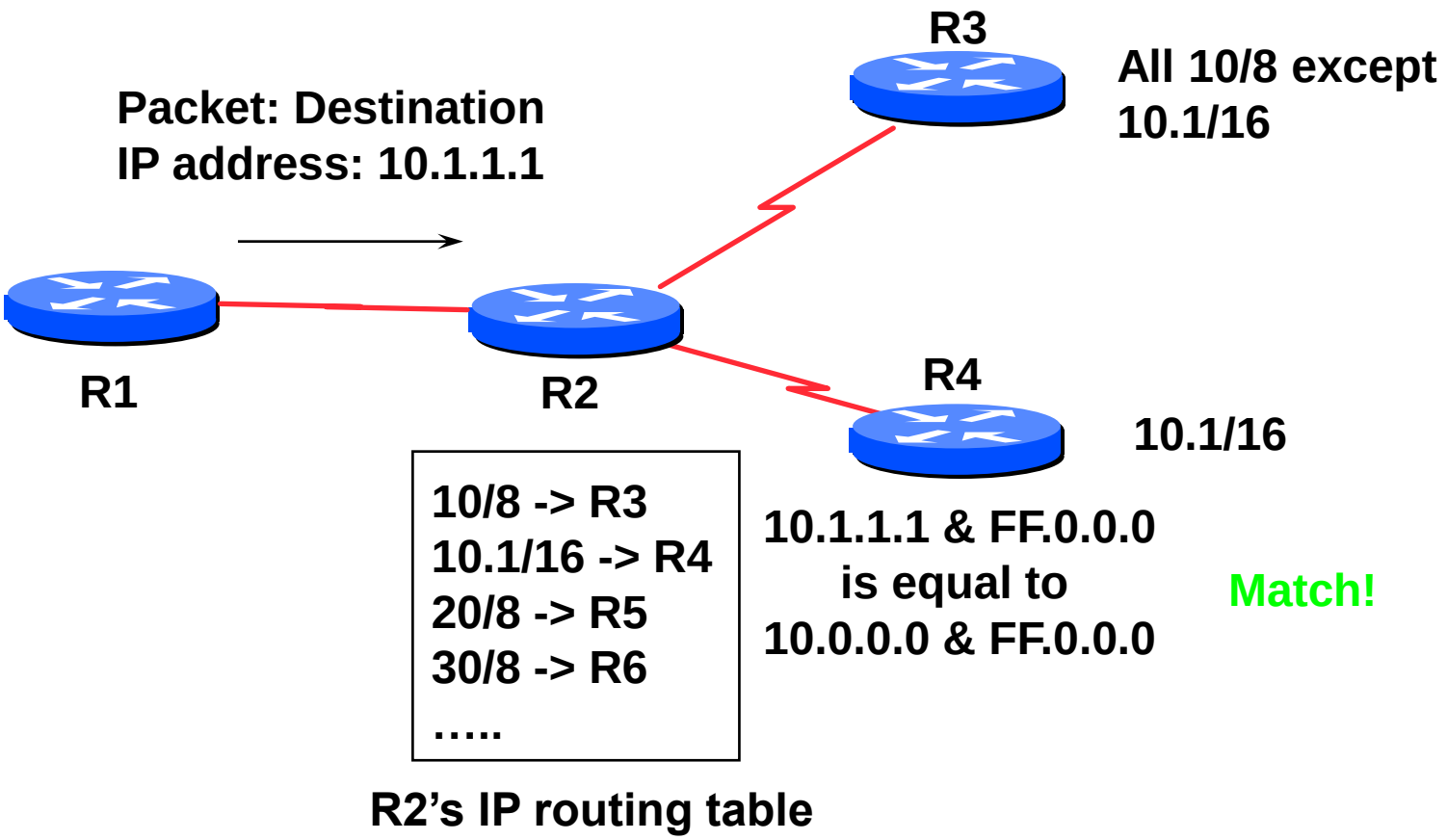
- 路由表保存着目的IP地址和下一个网关地址的映射关系。
- 路由器中共有四种目的地址：
  - 与路由器在同一子网的目的主机或网络地址
  - 路由器中明确定义的目的主机或网络地址
  - 由路由器收到的ICMP重定向消息所确定的目的主机或网络地址
  - 所有其它的目的主机或网络地址

路由表查找：最长匹配

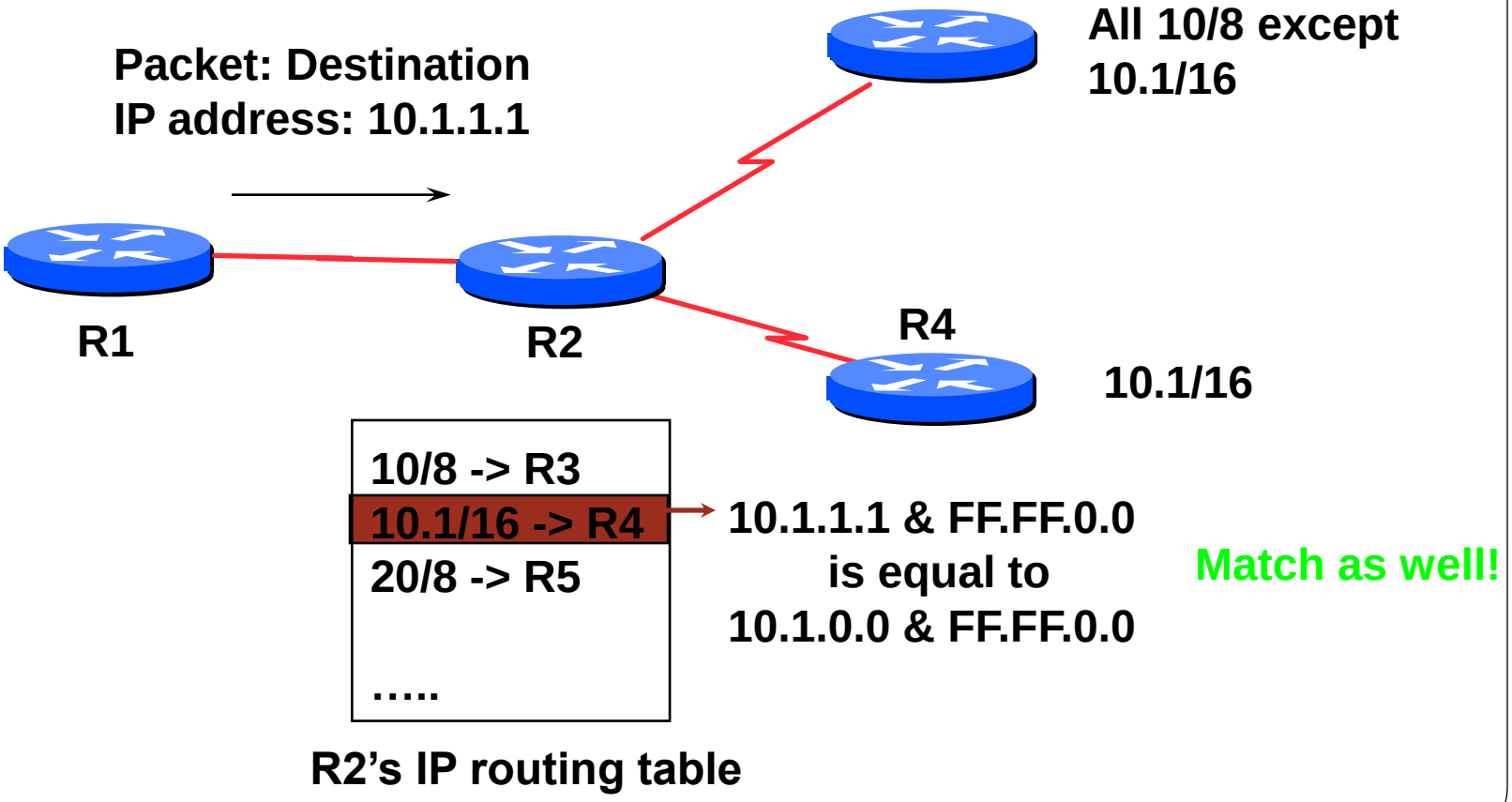


R2’s IP routing table

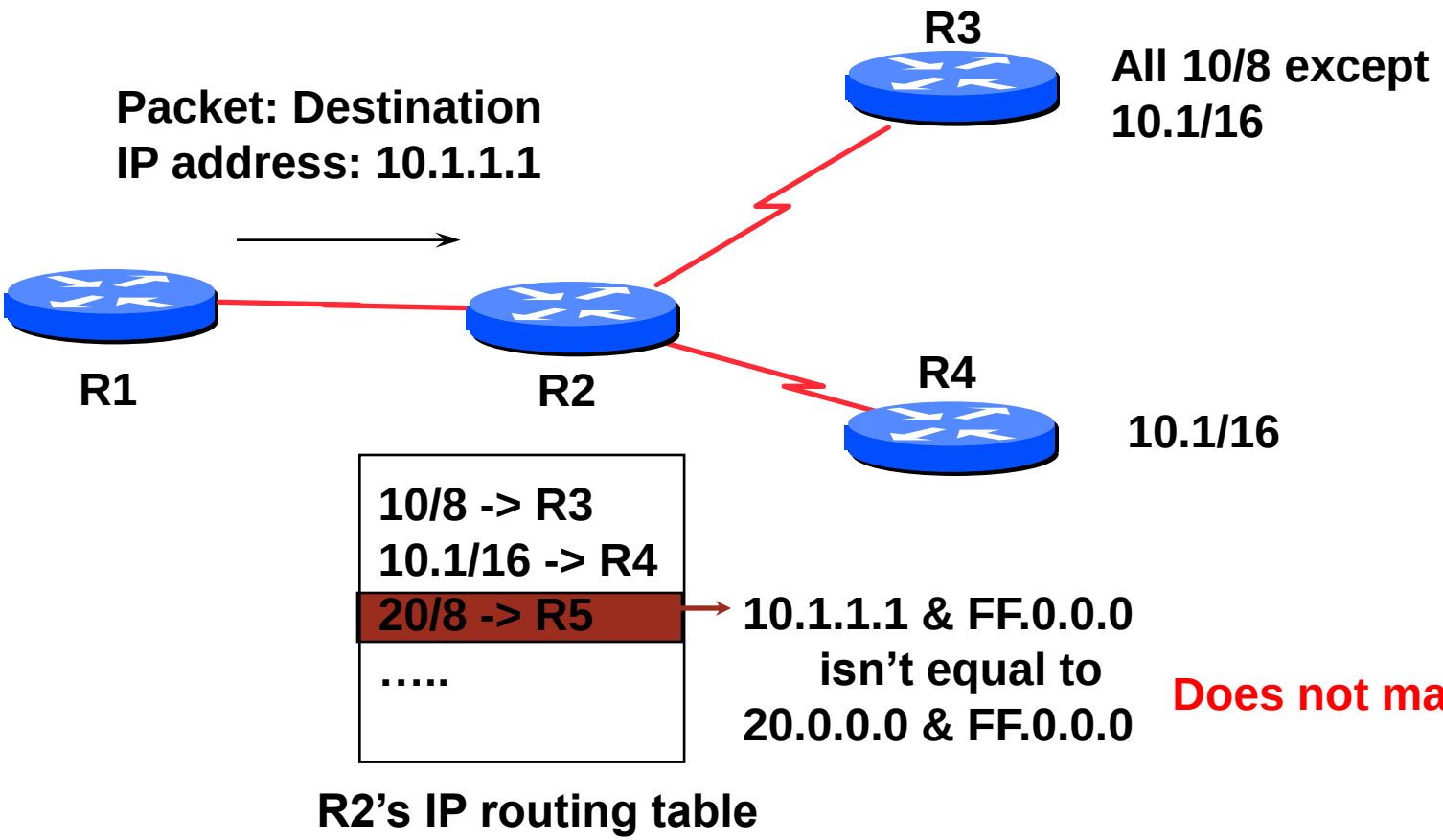
路由表查找：最长匹配


R3
All 10/8 except
10.1/16
Packet: Destination
IP address: 10.1.1.1
R1
R2
R4
10.1/16
10/8 -> R3
10.1/16 -> R4
20/8 -> R5
30/8 -> R6
…..
10.1.1.1 & FF.0.0.0
is equal to
10.0.0.0 & FF.0.0.0
Match!
R2's IP routing table

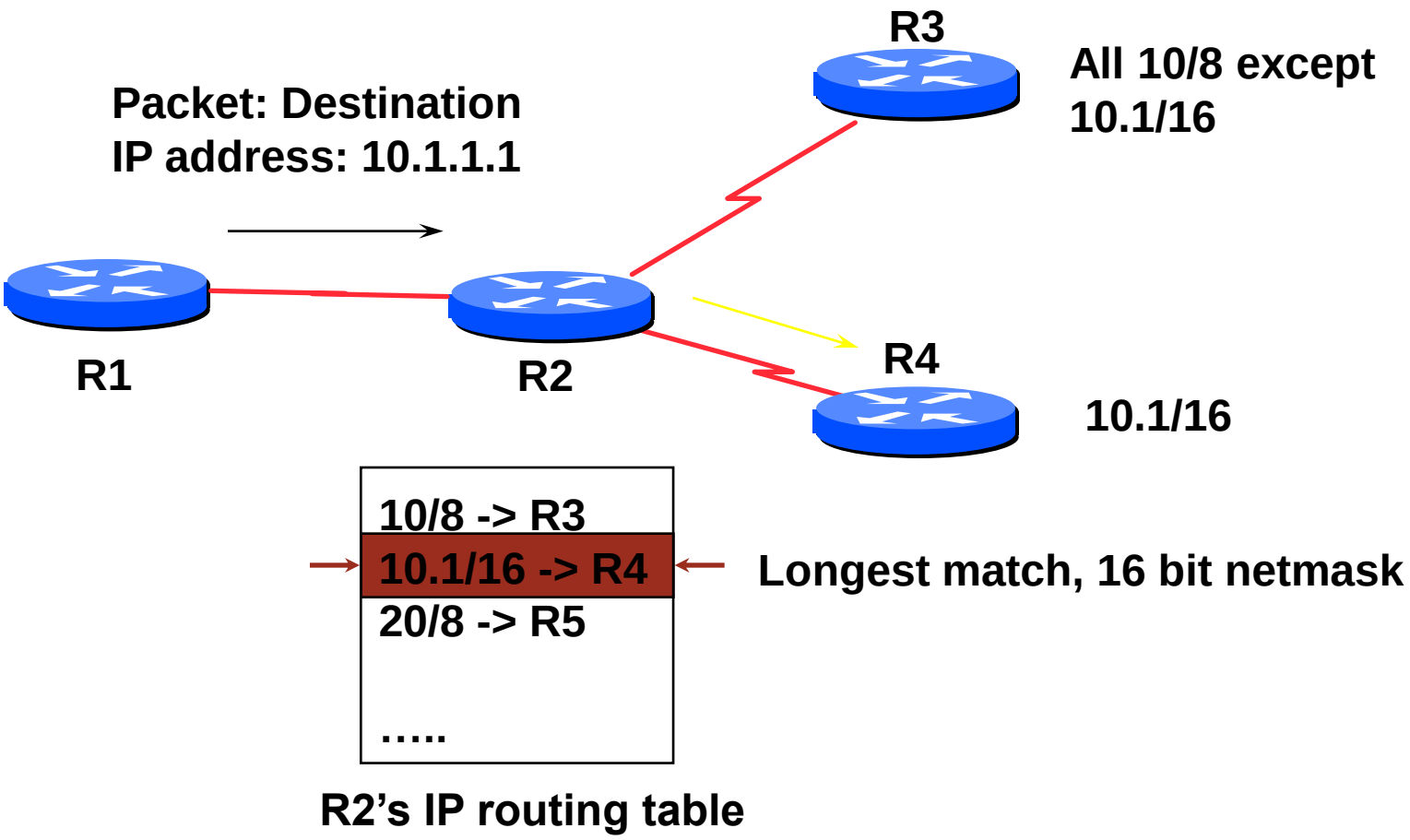
路由表查找：最长匹配


Packet: Destination
IP address: 10.1.1.1
All 10/8 except
10.1/16
R1
R2
R4
10.1/16
10/8 -> R3
10.1/16 -> R4
20/8 -> R5
…..
10.1.1.1 & FF.FF.0.0
is equal to
10.1.0.0 & FF.FF.0.0
Match as well!
R2's IP routing table

路由表查找：最长匹配


R3
All 10/8 except
10.1/16
Packet: Destination
IP address: 10.1.1.1
R1
R2
R4
10.1/16
10/8 -> R3
10.1/16 -> R4
20/8 -> R5
.....
10.1.1.1 & FF.0.0.0
isn't equal to
20.0.0.0 & FF.0.0.0
Does not match!
R2's IP routing table

路由表查找：最长匹配


R3
All 10/8 except
10.1/16
Packet: Destination
IP address: 10.1.1.1
R1
R2
R4
10.1/16
10/8 -> R3
10.1/16 -> R4
20/8 -> R5
.....
Longest match, 16 bit netmask
R2's IP routing table

路由类型

◆ 静态路由

网络管理员必须人工建立路由表，该表必须是一个包含通向所有网络的所有可能的路径的数据库。

◆默认路由

可以转发那些在路由表中没有列出的远端目的网络的数据包到下一跳路由器

◆ 动态路由

路由表能够通过一种特殊的的封包自动维护自己的路径，并能随着网络环境的改变而改变。

静态路由

优点：

- 对于路由器的CPU没有管理性开销
- 在路由器之间没有带宽占用
- 增加了安全性

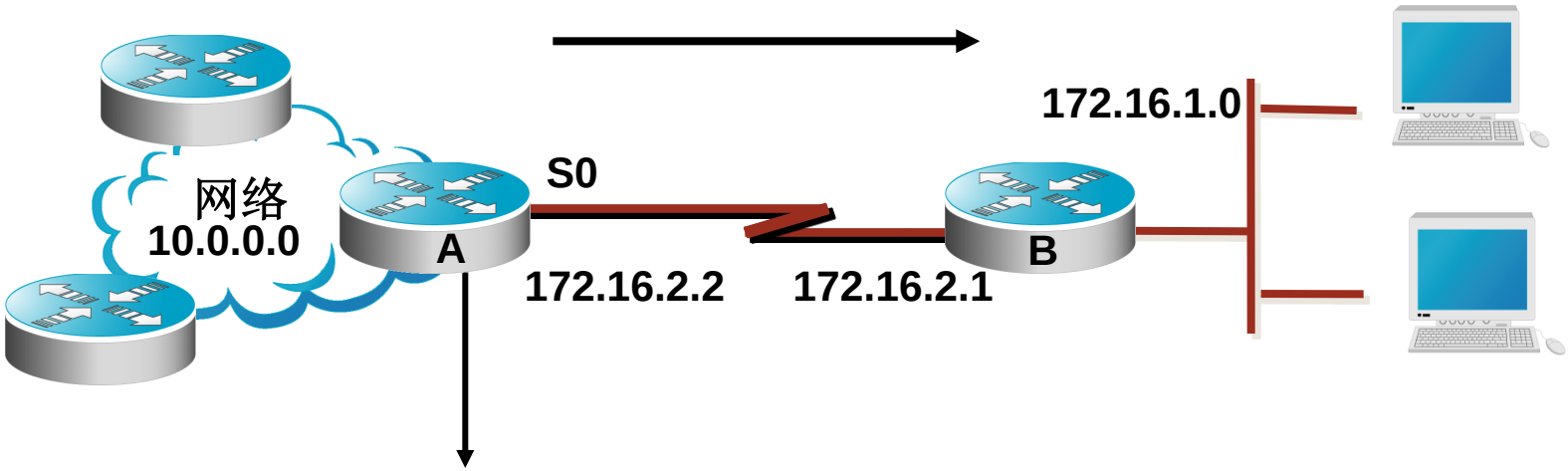
缺点：

- 必须真正地了解所配置的互联网络，以及每台路内器应该如何正确地连接以正确配置这些路由。
- 如果某个网络加入到互联的网络中，必须在所有的路由器上(人工)添加对它的路由。
- 大型网络不可行

静态路由配置命令

- 配置静态路由用命令ip route
- router(config)#ip route [网络编号] [子网掩码] [转发路由器的IP地址/本地接口]

静态路由配置实例



router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1

或

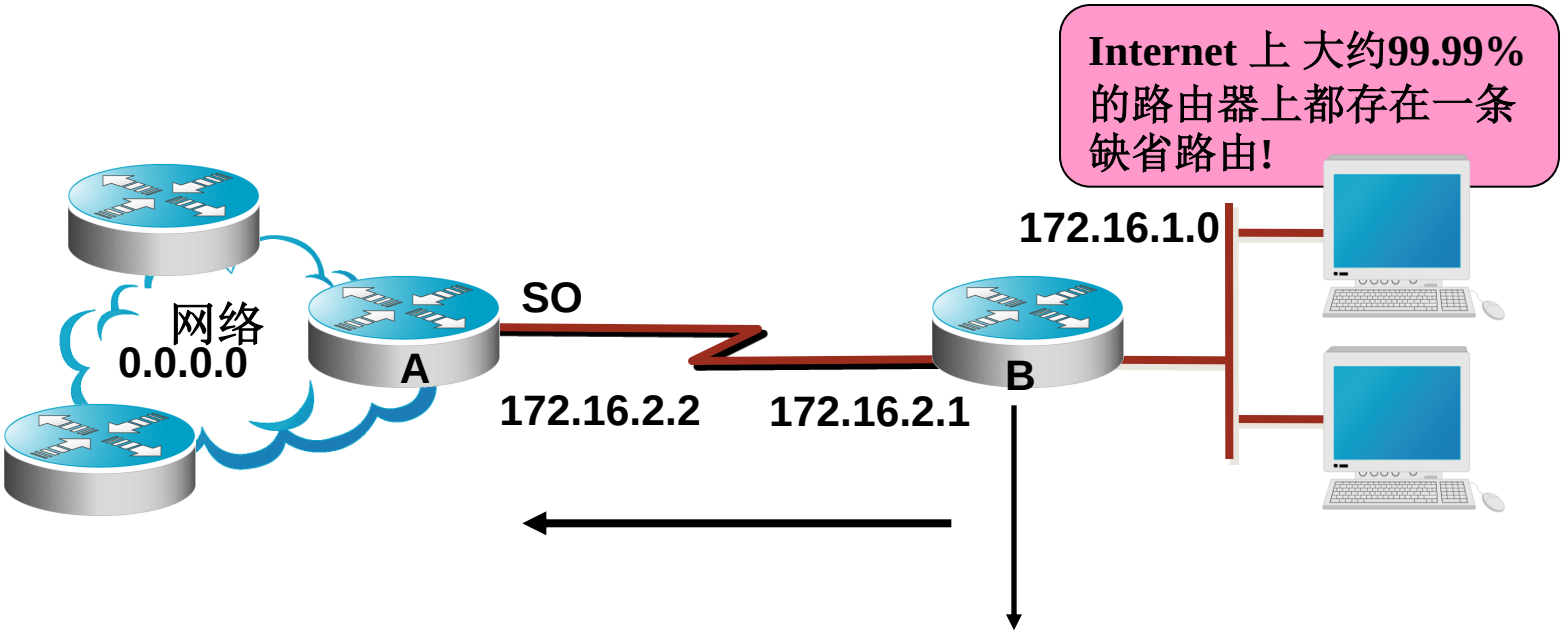
router(config)#ip route 172.16.1.0 255.255.255.0 serial 0

默认路由

- 默认路由可以转发那些在路由表中没有列出的远端目的网络的数据包到下一跳路由器。
- 在存根网络上可以只使用默认路由，即那些与外界只有一个输出连接的网络。
- 默认路由是一个使用通配符来代替网络和子网掩码信息的静态路由。
- **配置缺省路由用如下命令：**

  `router(config)#ip route 0.0.0.0 0.0.0.0 [转发路由器的IP地址/本地接口]`

默认路由配置实例



router(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

动态路由

- **动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。**
- **路由方法：**
  路由器会将自己的已知信息发给相邻路由器。最终每台路由器都会收到网络中所有路由器的信息。然后通过相应算法计算出最终路由。

动态路由协议的分类

- 外部网关协议：在自治系统之间交换路由选择信息的互联网络协议，如BGP。
- 内部网关协议：在自治系统内交换路由选择信息的路由协议，常用的因特网内部网关协议有OSPF、RIP、IGRP,EIGRP 。

路由选择协议基础

管理距离(AD)

- **用来衡量接收来自相邻路由器上路由选择信息的可信度管理距离（0~255），0是最可信赖的，255则意味着不会有业务量通过这个路由。**
- **如路由器接收到两个对于同一远程网络的更新内容，路由器首先AD。带有最低AD值的路由将会被放置在路由表中。**
- **AD相同，则路由协议的度量值(如跳计数或链路的带宽值)将被用做寻找到达远程网络最佳路径的依据，最低度量值的路由将被放置在路由表中。AD相同及度量相同，负载均衡(即它所发送的数据包会平分到每个链路上)。**

默认的管理距离

路由源	默认AD
连接接口	0
静态路由	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120

路由度量

- 跳数（hop count）：分组从源结点到达目的结点经过的路由器的个数。
- 带宽（bandwidth）— 链路的传输速率。
- 延时（delay）— 分组从源结点到达目的结点花费的时间。
- 负载（load）— 通过路由器或线路的单位时间通信量。
- 可靠性（reliability）— 网络链路的可信度（通常指单位时间内链路的失效次数）。
- 开销（overhead）— 传输过程中的耗费，与所使用的链路带宽相关。

距离矢量型路由协议

- RIP和IGRP是距离矢量路由选择协议。
- 数据包每通过一个路由器，称为一跳。使用最少跳数量到达网络的路由被认为是最佳路由。
- 它们发送整个路由表到直接相邻的路由器。
- 路由表信息的更新

若项目中的目的网络不在路由表中，则将该项目添加到路由表中（距离D值加1）。

否则

若下一跳字段给出的路由器地址是同样的，则将收到的项目替换原路由

表中的项目。

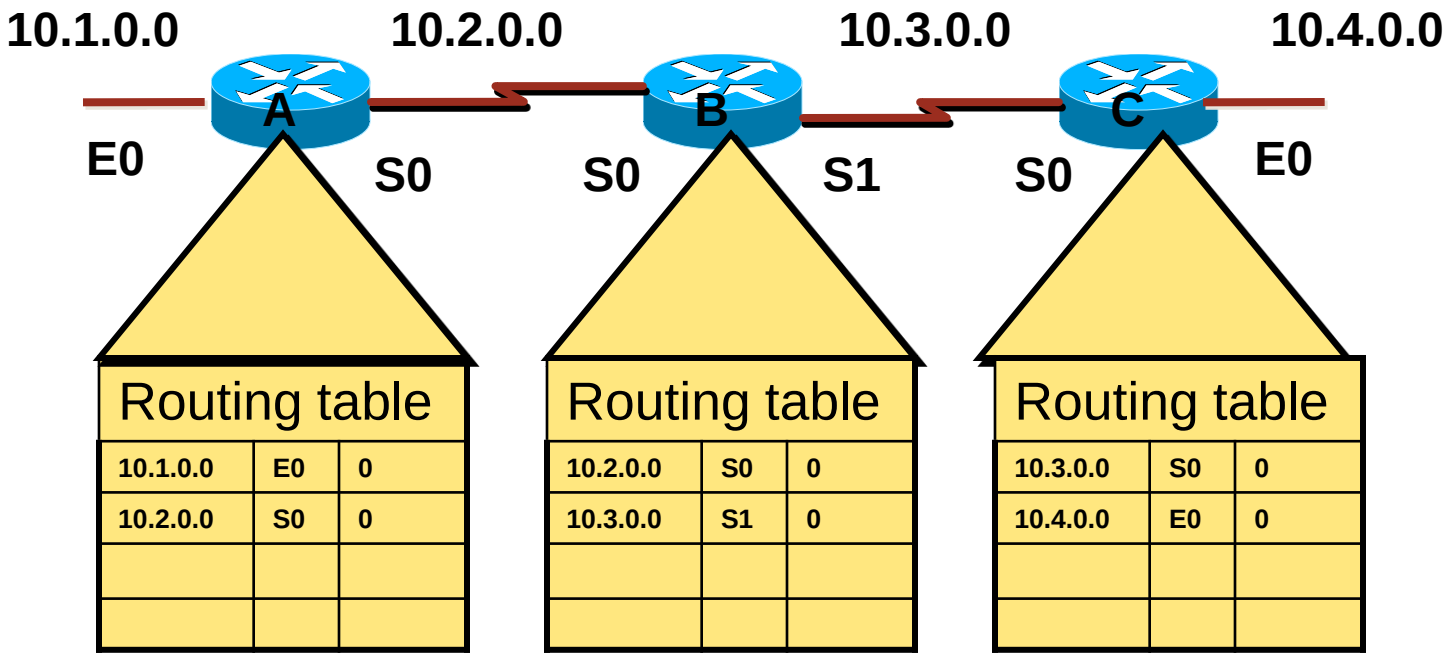
否则

若收到的项目中的距离加1的值小于路由表中的距离值，则进行更新。

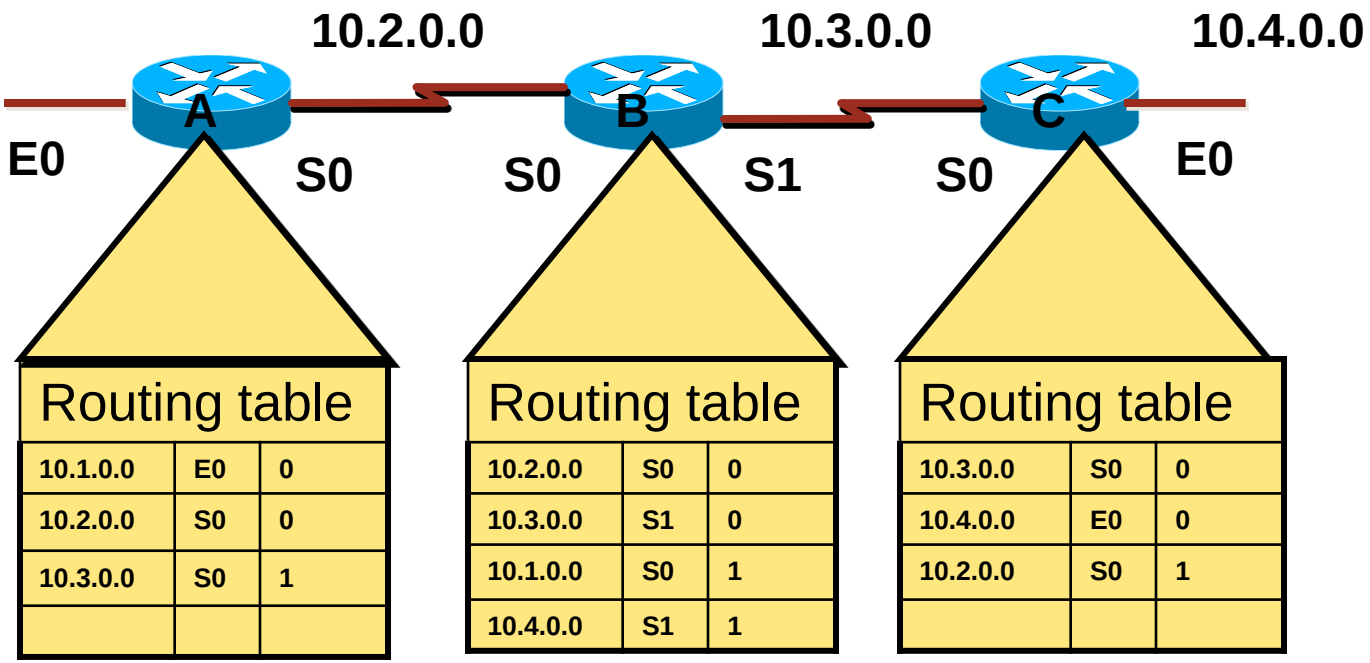
否则，什么也不做。

RIPv1-构建路由表

向谁传送，传送什么，何时传送
路由器不了解网络的确切拓扑信息

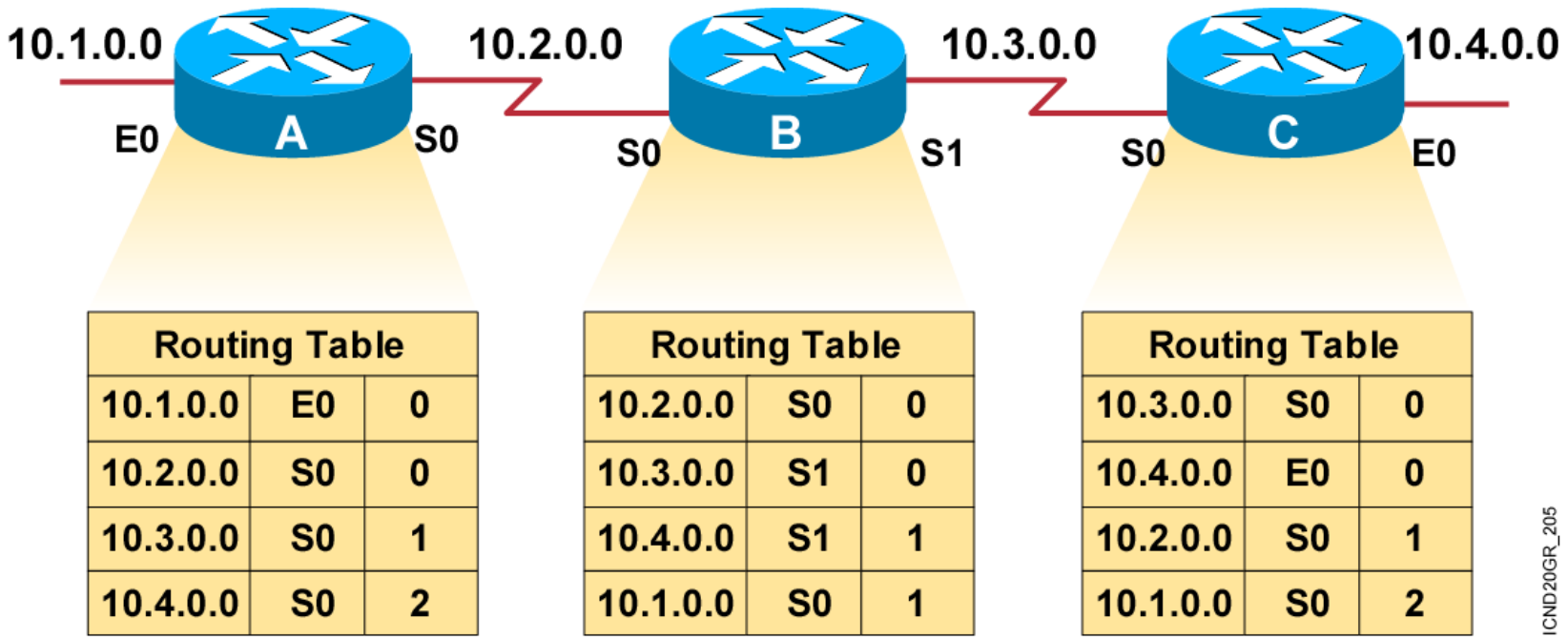


RIPv1-构建路由表


10.2.0.0
10.3.0.0
10.4.0.0
A
B
C
E0
S0
S0
S1
S0
E0
Routing table
10.1.0.0 E0 0
10.2.0.0 S0 0
10.3.0.0 S0 1
Routing table
10.2.0.0 S0 0
10.3.0.0 S1 0
10.1.0.0 S0 1
10.4.0.0 S1 1
Routing table
10.3.0.0 S0 0
10.4.0.0 E0 0
10.2.0.0 S0 1

RIPv1-构建路由表

路由收敛

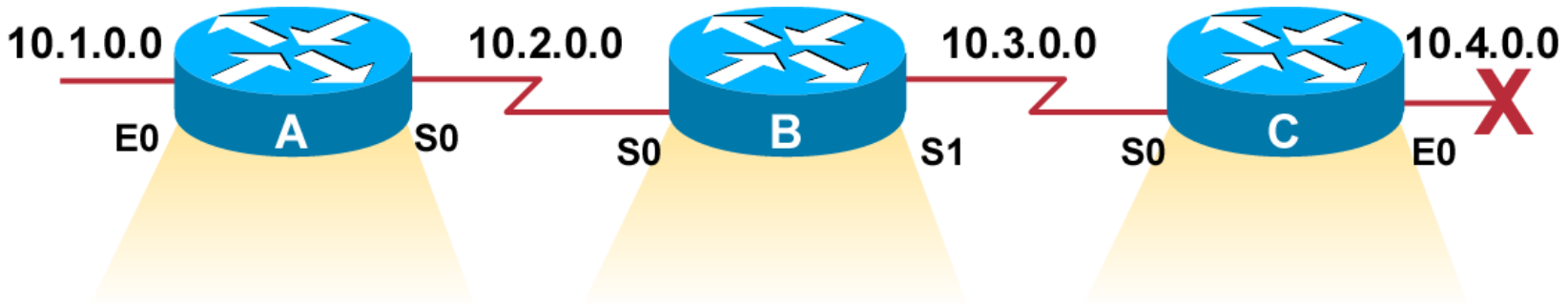


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

路由环路的形成

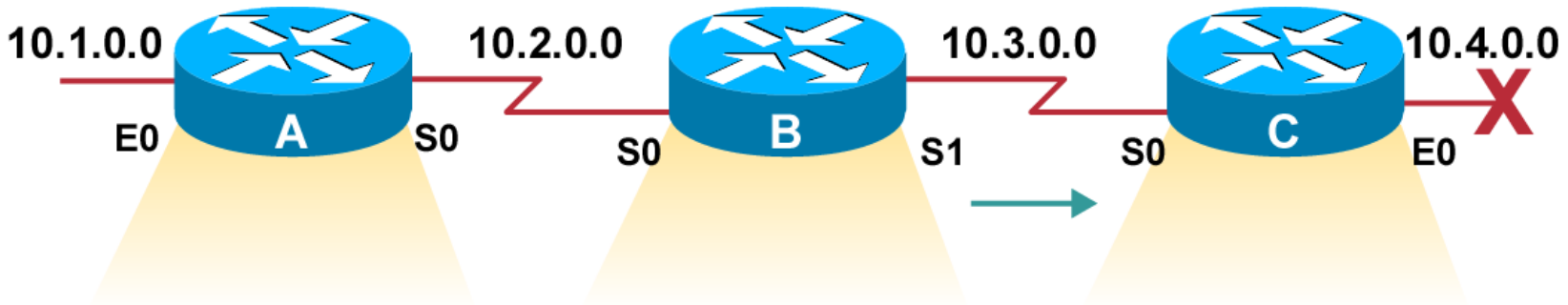


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

路由环路的形成

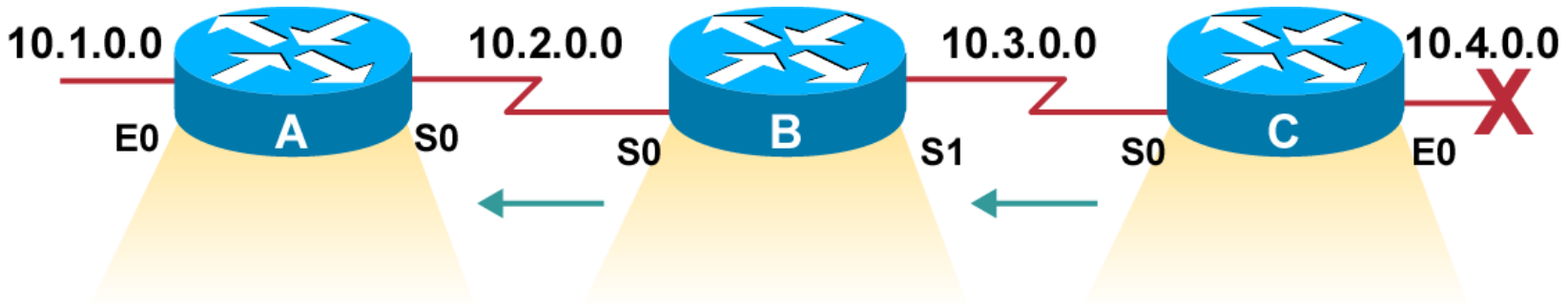


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

路由环路的形成

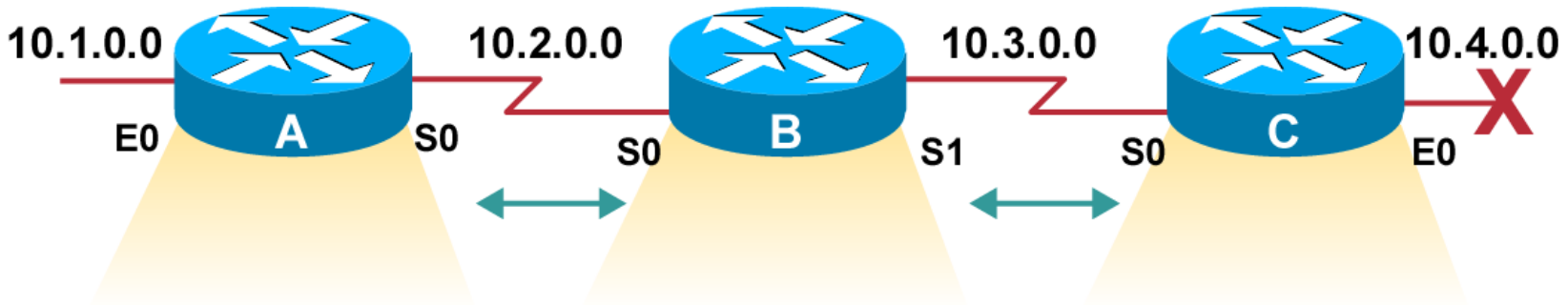


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	4

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	3
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

路由环路的形成

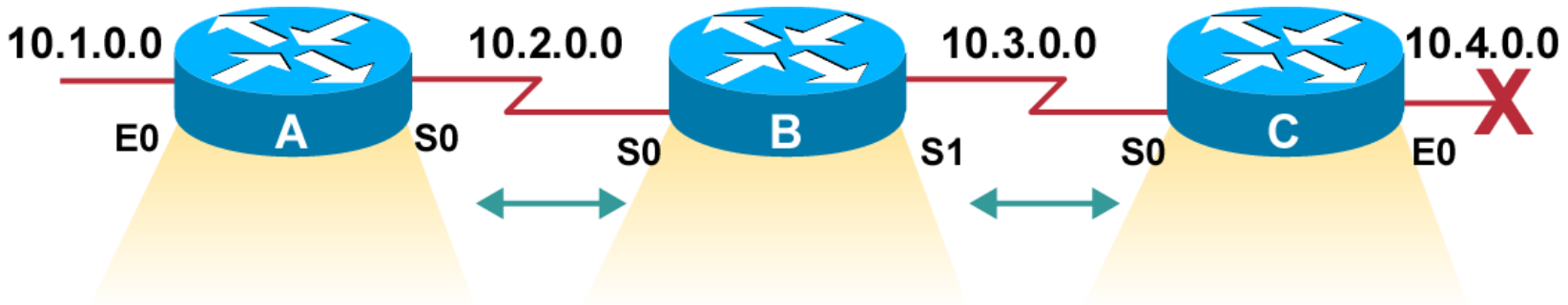


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	6

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	5
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	4
10.2.0.0	S0	1
10.1.0.0	S0	2

路由环路的形成-定义最大跳



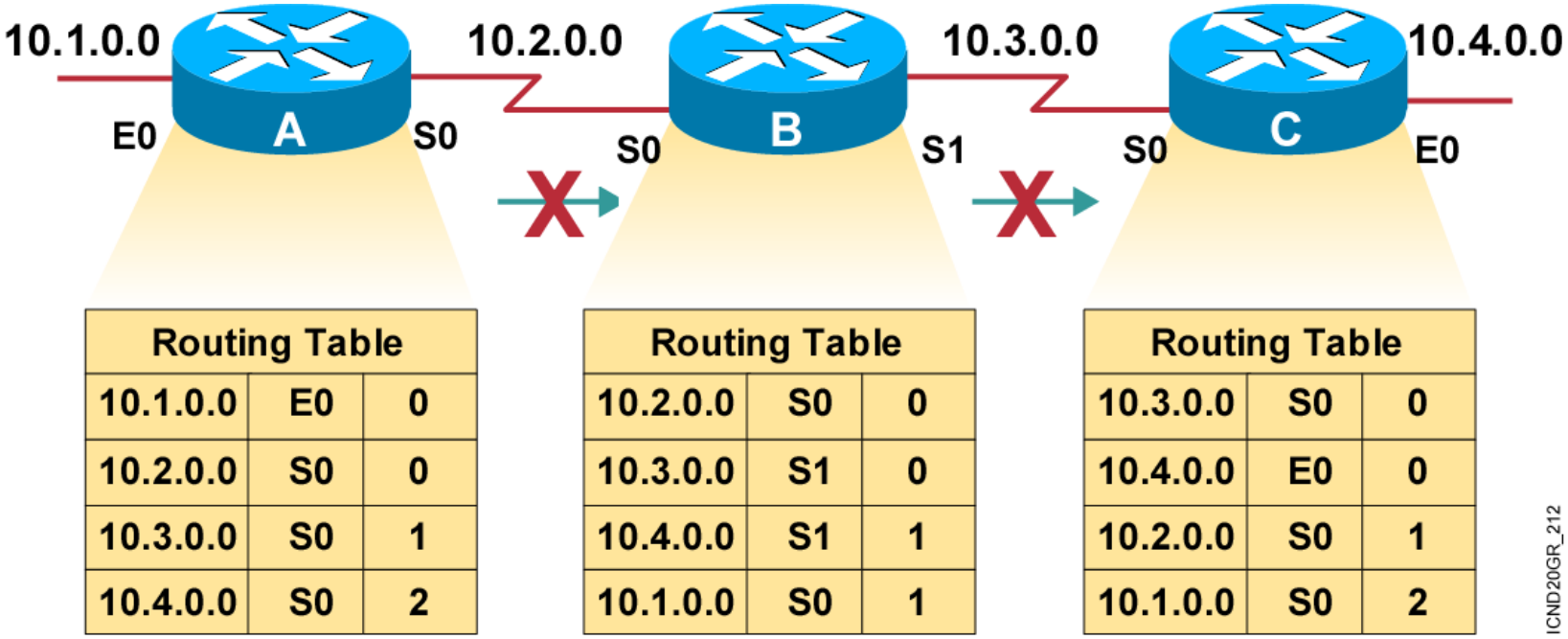
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	16

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	16
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	16
10.2.0.0	S0	1
10.1.0.0	S0	2

解决路由环路的方法：水平分割

- 路由器不会把那些从它的某个接口学到的路由再从同接口通告出去。
- 水平分割默认启动



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

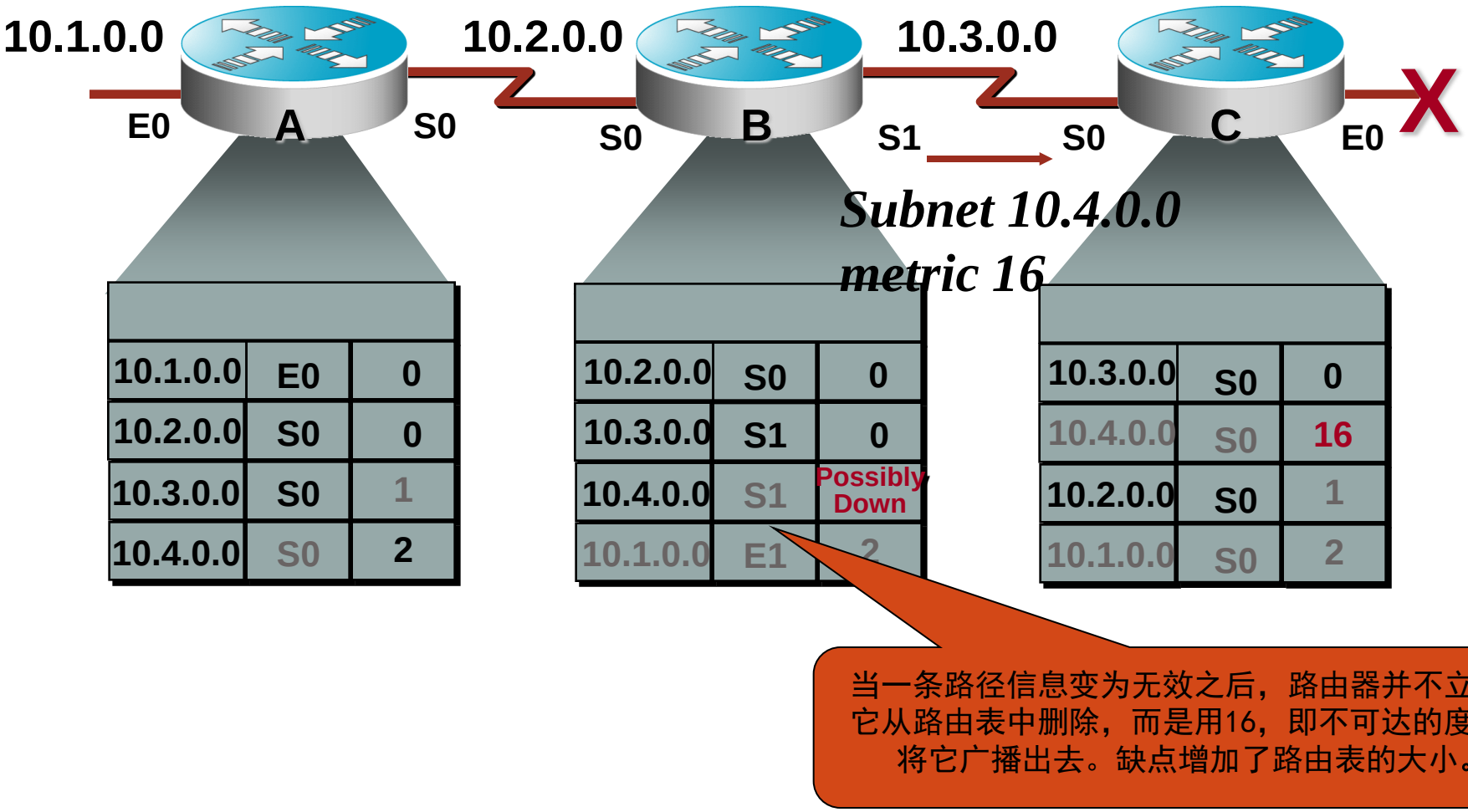
Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

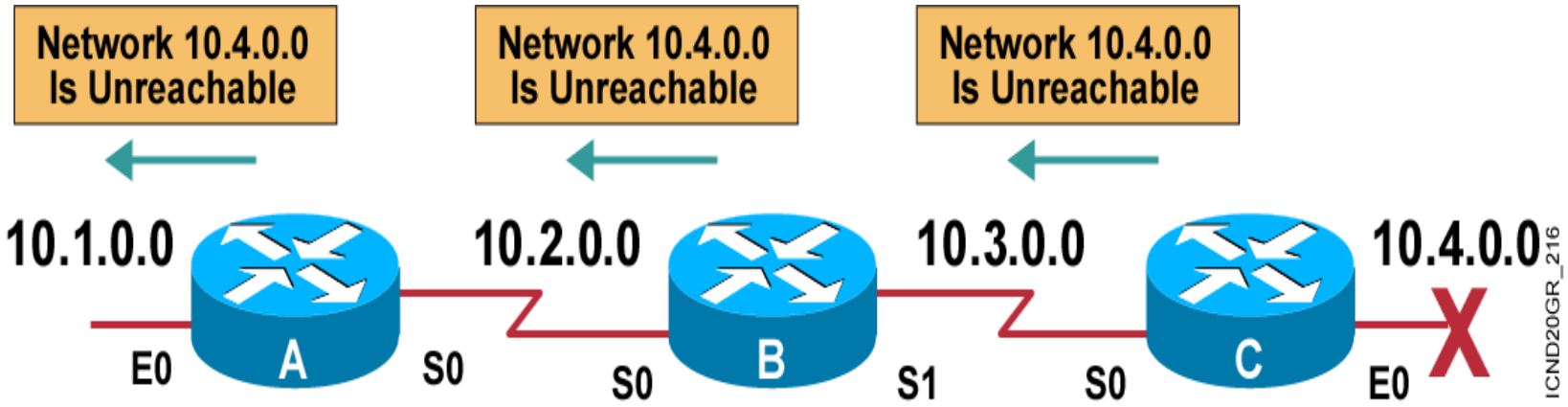
路由中毒与毒性反转

- 路由中毒：是指在路由信息在路由表中失效时，先将度量值变为无穷大，而不是马上从路由表中删掉这条路由信息。(RIP协议中，其度量值变为16，意味着路由不可达)再将其信息发布出去，这样相邻的路由器就得知这条路由已无效了。
- 毒性反转与路由中毒概念是不一样的，它是指收到路由中毒消息的路由器，不遵守水平分割原则将中毒消息转发给所有的相邻路由器，也包括发送中毒信息的源路由器，也就是通告相邻路由器这条路由信息已失效了，主要目的是达到快速收敛的目的。

路由中毒与毒性反转


10.1.0.0
10.2.0.0
10.3.0.0
E0
A
S0
S0
B
S1
S0
C
E0
X
Subnet 10.4.0.0
metric 16
10.1.0.0 E0 0
10.2.0.0 S0 0
10.3.0.0 S0 1
10.4.0.0 S0 2
10.2.0.0 S0 0
10.3.0.0 S1 0
10.4.0.0 S1 Possibly Down
10.1.0.0 E1 2
10.3.0.0 S0 0
10.4.0.0 S0 16
10.2.0.0 S0 1
10.1.0.0 S0 2
当一条路径信息变为无效之后，路由器并不立即将它从路由表中删除，而是用16，即不可达的度量值将它广播出去。缺点增加了路由表的大小。

触发更新



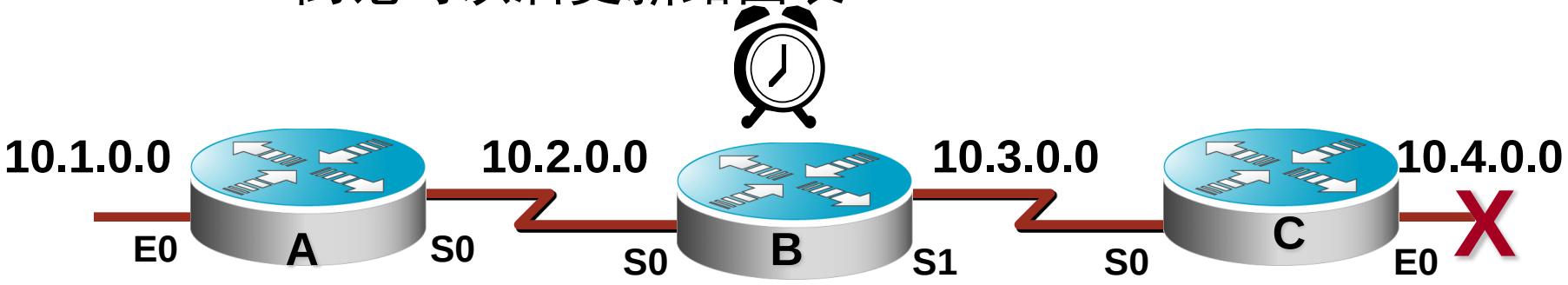
得知网络拓扑结构发生改变，不等待发送周期，立刻通告更新后全部的路由表

RIP定时器

- 路由更新定时器　用于设置定期路由更新的时间间隔(典型位为30秒)，在这个间隔里路由器发送一个自己路由表的完整拷贝到所有相邻的路由器。
- 路由失效定时器 路由器在认定一个路由成为无效路由 之前所需要的时间间隔。如果路由器在这个期间内没有 得到关于某个指定路由的任何更新消息，它将认为这个 路由失效。
- 保持失效定时器　路由信息被抑制的时间
- 路由刷新定时器　设置某个路由为无效路由并从路由表中删除的时间间隔（240秒）

Hold-down倒记时

hold-down倒记时以后更新路由表



等待网络中其它路由器收敛，在该时间内不学习任何与该网络相关的路由信息（RIP缺省180秒），在倒记时其间继续向其它路由器发送毒化信息

配置RIP路由

```
Router(config)#router rip
```

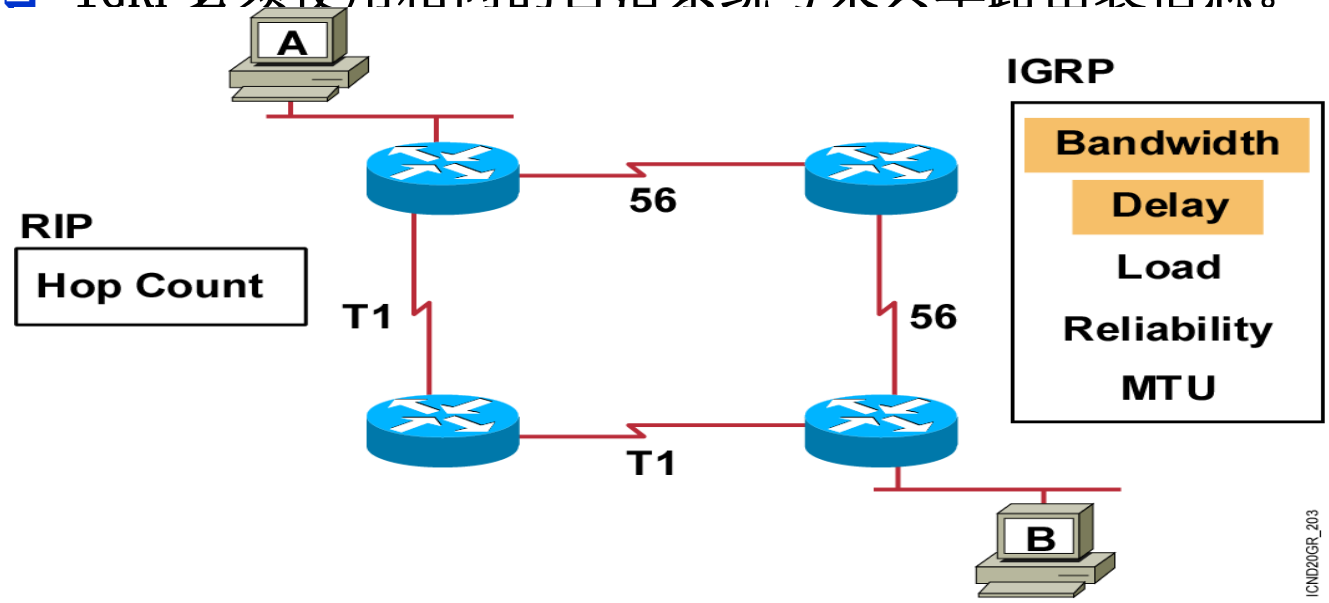
启动**RIP**路由协议

```
Router(config-router)#network network-number
```

路由选择协议要通告哪些网络，并启用相应的接口参与动态路由协议的运行进程

内部网关路由协议（IGRP）

- IGRP，Cisco专用的距离矢量路由选择协议。
- IGRP的最大跳计数值为255，默认时为100。
- IGRP使用了与RIP不同的度量,默认时，使用带宽和线路延迟作为判断到达某个互联网络最佳路由的量度，称为合成度量。可靠性、负载和最大传输单元(MTU)也可以用做度量。
- IGRP必须使用相同的自治系统号来共享路由表信息。



内部网关路由协议（IGRP）

- **配置IGRP路由**

```
Router(config)#router igrp AS号
```

```
Router(config-router)#network network-number
```

IGRP可实现多达6条链路的负载均衡。RIP网络要实现负载均衡必须具有相同的跳计数，而IGRP使用带宽来决定如何实现负载均衡。

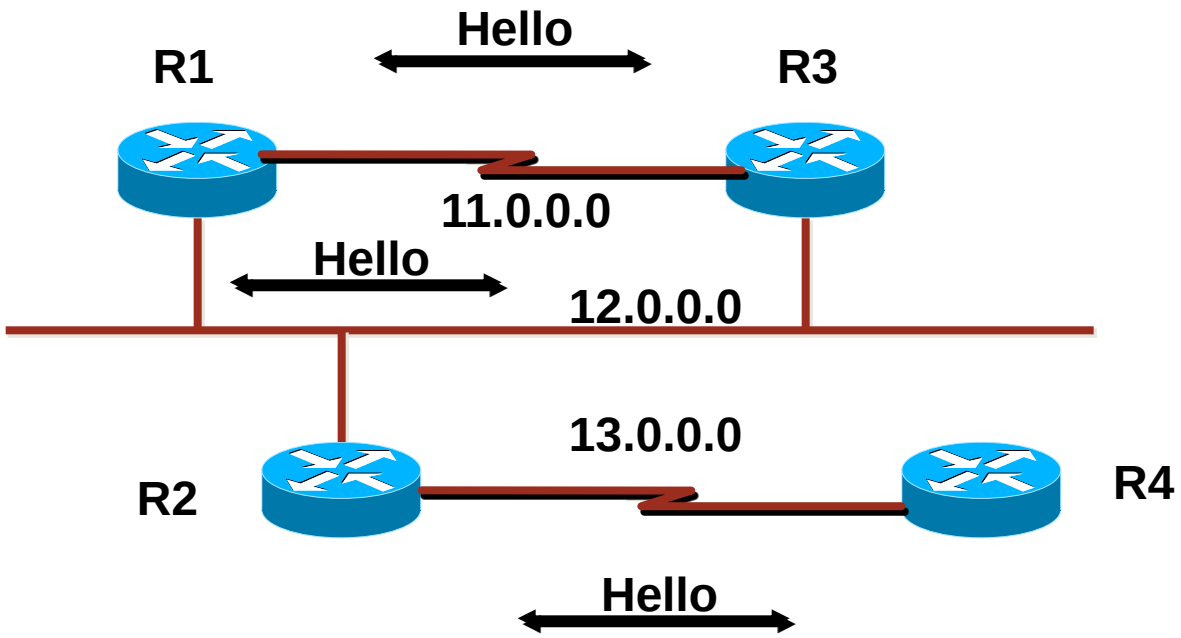
链路状态型路由协议

- 链路状态型路由协议和距离矢量型路由协议相比有以下特点；
- 没有跳数限制。
- 以路径花费值作为选择最佳路径的度量。**Cost**是能够体现带宽的一个参数，所以路由器可以根据链路的实际带宽选择路径而不是跳数。
- 事件触发**(Event triggered)**的更新机制，并非像距离矢量型协议那样更新。
- 增量更新。
- 更新的是链路状态数据库而不是路由表。
- 路由器有一个完整和同步的网络拓扑图，没有环路。
- 需要更多的内存和更大的处理能力。
- 网络初期**LSA**的扩散可能会占用大量的带宽。

链路状态型路由协议

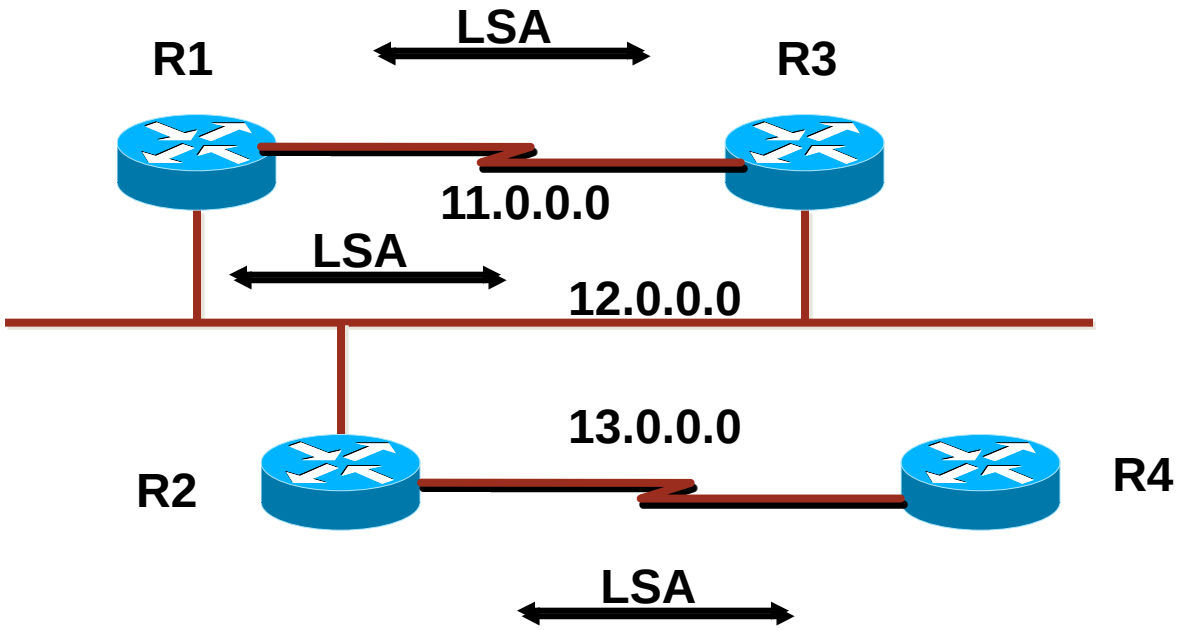
链路状态路由协议的路由表的计算分三个步骤

- 建立邻居关系



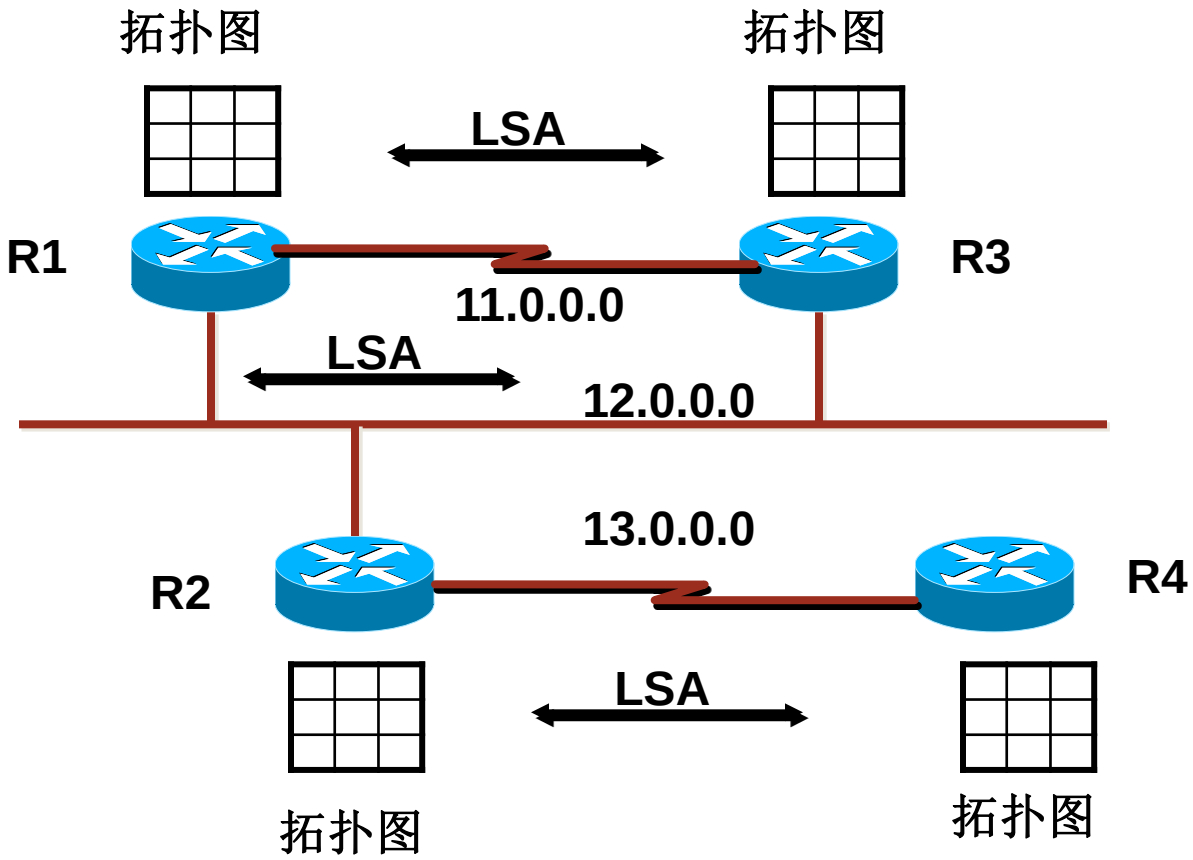
链路状态型路由协议

- 交换链路状态信息　　链路状态广播包**LSA**



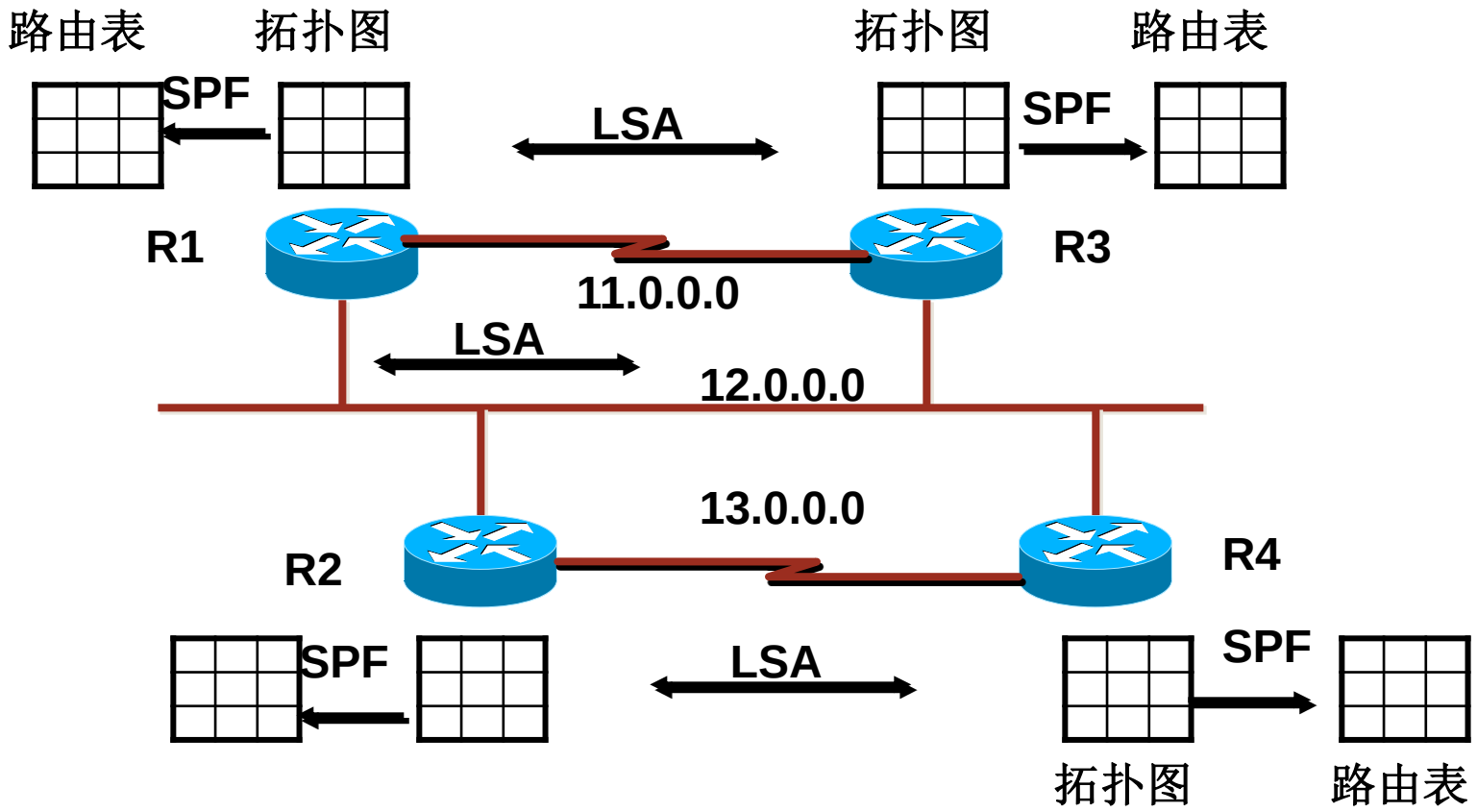
链路状态型路由协议

- 根据链路状态信息，构建拓扑结构（链路状态）数据库



链路状态型路由协议

- 计算路由表



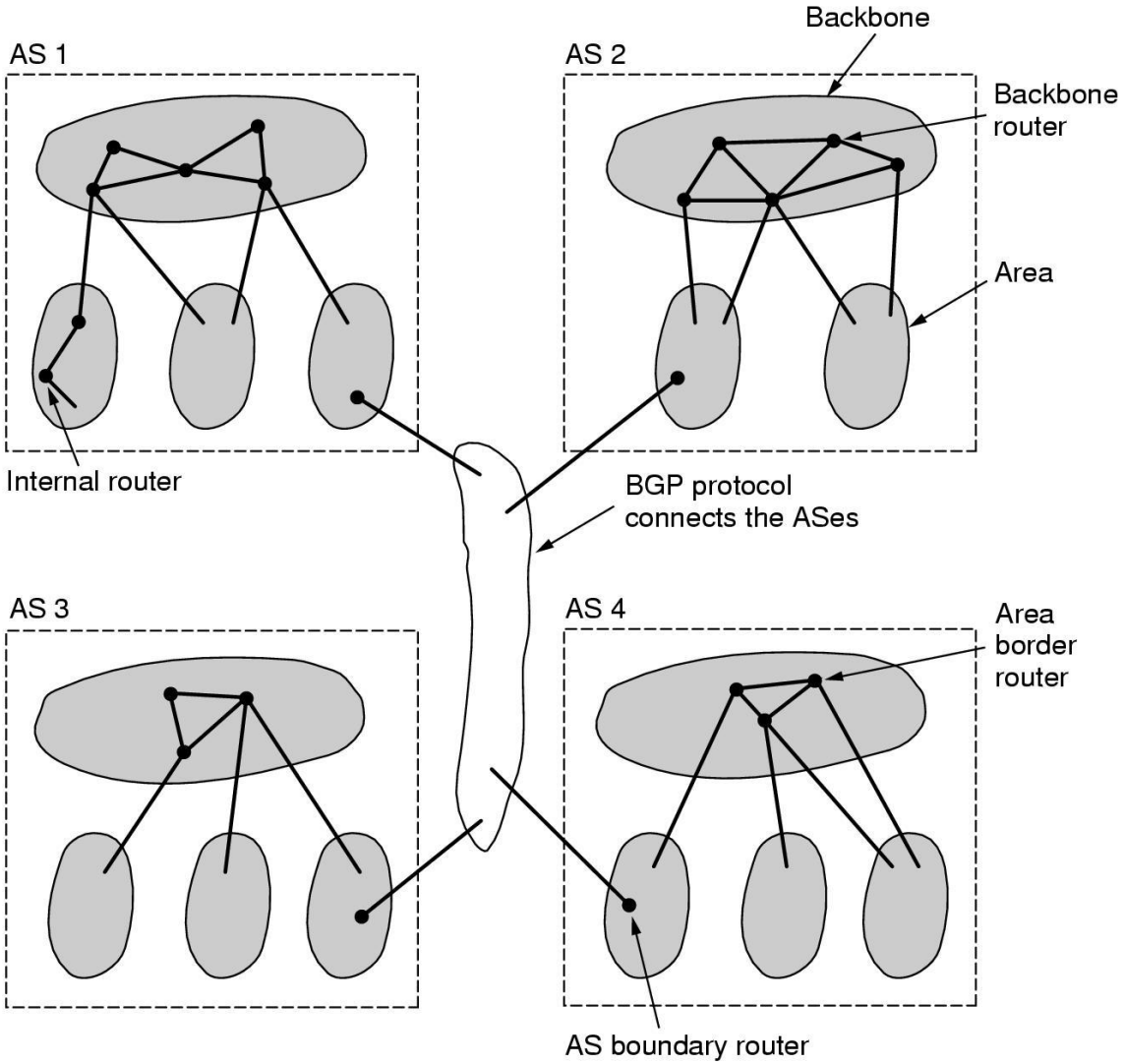
OSPF概述

- 开放式最短路径优先（OSPF）是一种典型的链路状态路由协议。
- OSPF特点：
  - 没有跳数限制，适应大型IP网络的扩展。
  - 路由搜索是基于网络地址以及链路状态度量。
  - 具有自适应特点，根据网络故障情况自动进行调整。收敛时间短。
  - 可以防止通信数据形成环路。

OSPF基本概念

- OSPF将一个自治系统划分为多个区域（Area），以减少每个路由器存储和维护的信息量。每个路由器有所在区域的完整信息。
- 区域用数字标识，区域0为骨干网络，其他所有区域必须连接到区域0。
- 4类路由器：内部路由器，区域边界路由器，主干路由器，AS边界路由器。每个路由器都被分配一个唯一的32位的路由器标识符RID（Route ID）。

OSPF中AS、主干和区域之间的关系



OSPF中的工作原理

- 区域内：利用扩散法，每个路由器将它的邻居和开销信息告诉给本区域中的所有其它路由器，这些信息使每个路由器都能构造出一个本区域的有向图，并计算最短路径。
- 区域间：主干路由器从区域边界路由器处获取信息，计算出每个主干路由器到每个其它路由器的最佳路径。这一信息再传回区域边界路由器，由该路由器在它的区域中进行广播。这样一个要发送区域间分组的路由器就可选择一个去往主干的最佳出口路由器。

OSPF算法描述

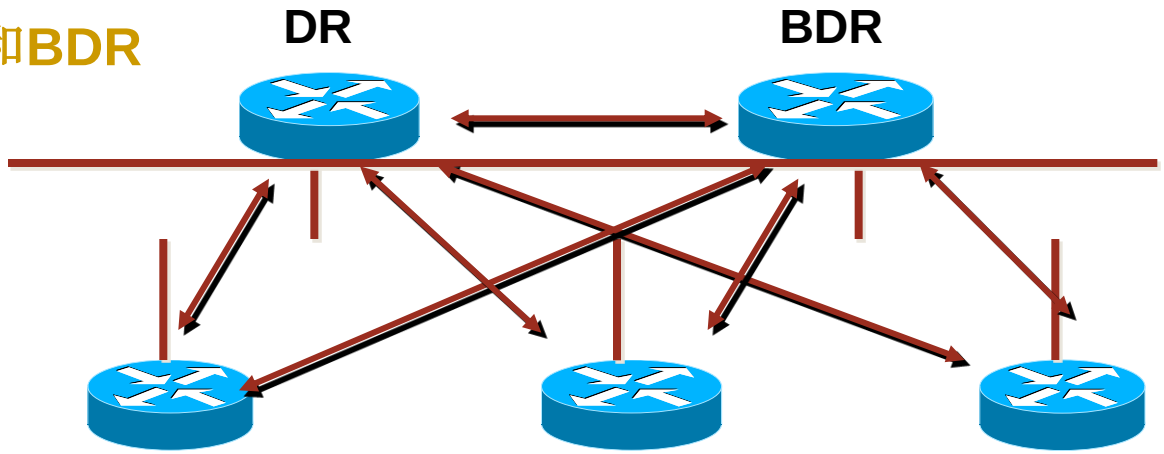
1. 发出Hello 报文
2. 建立邻居关系
3. 在形成邻居关系的邻居间发送LSA
4. 收到从邻居发的LSA的路由器记录到数据库，并发拷贝给路由器其他邻居。
5. 通过LSA泛洪，所有路由器汇形成同样的链路状态数据库。
6. 当数据库完全相同，生成最小生成树。
7. 每一台路由器都从最小生成树中构建自己的路由表

OSPF的五种协议报文

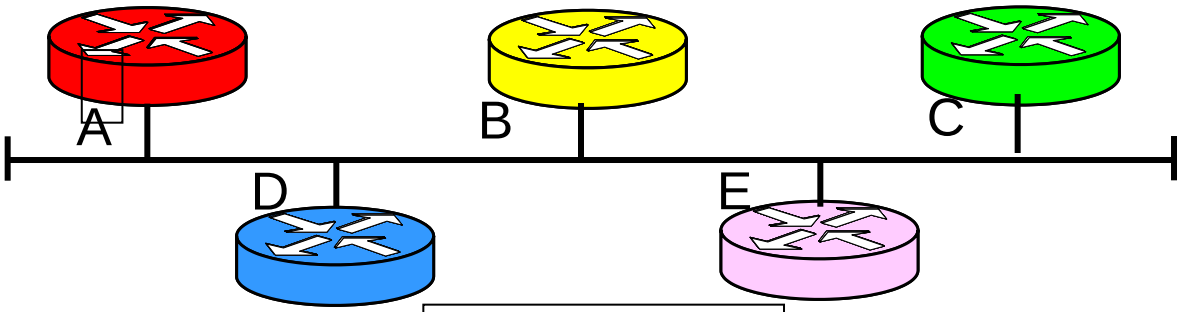
- HELLO报文
  - 用来发现及维持邻居关系，选举DR、BDR。
- DD报文
  - 用来描述本地LSDB的情况。
- LSR报文
  - 向对端请求本端没有或对端更新的LSA。
- LSU报文
  - 向对端路由器发送所需的LSA。
- LSAck报文
  - 收到LSU之后，进行确认。

广播型多路访问拓扑下的OSPF

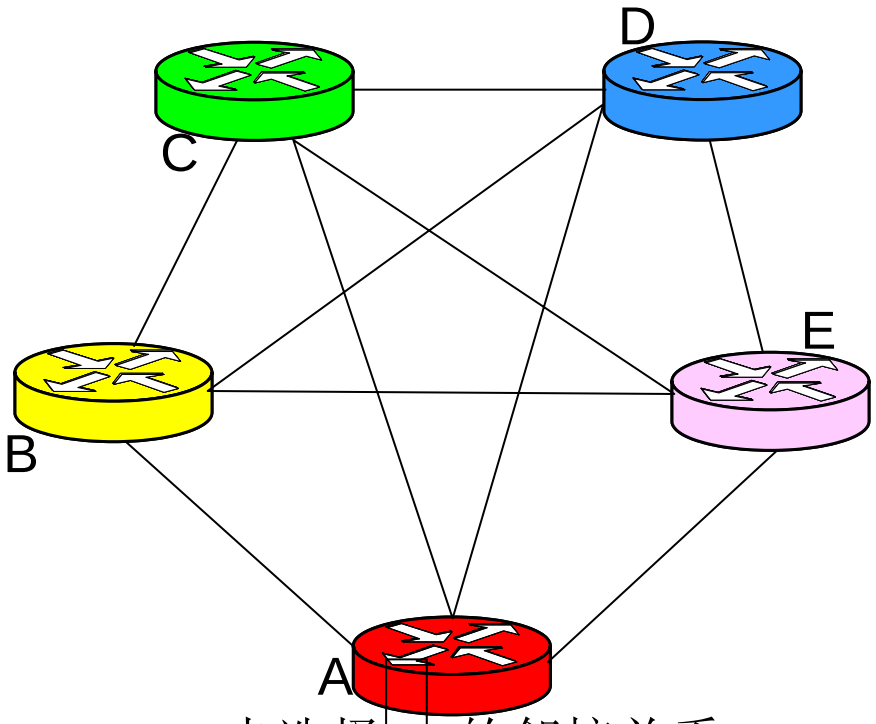
选举DR和BDR



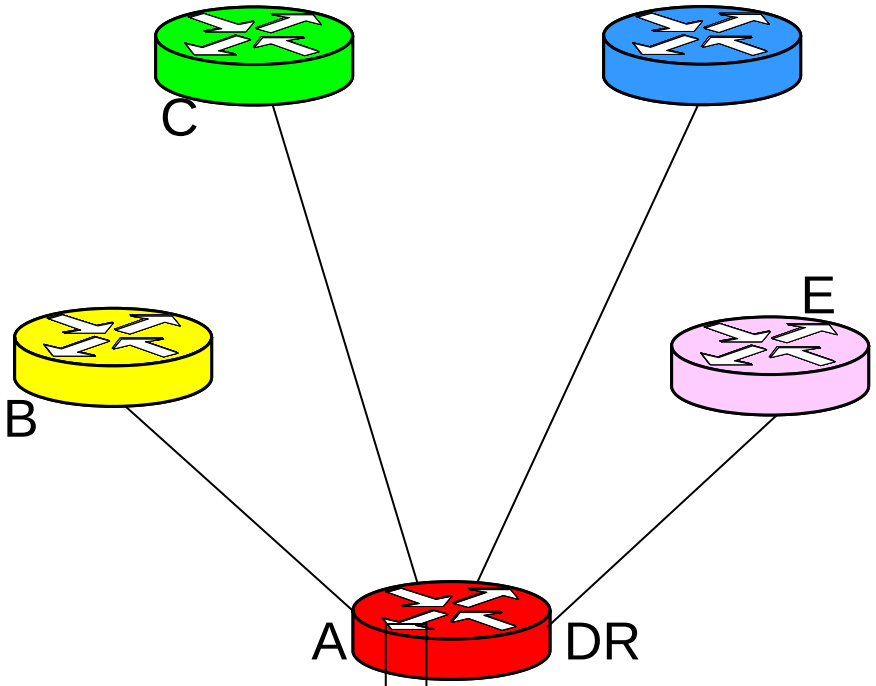
- 指定路由器（DR） 备份指定路由器（BDR）
- 好处：减少路由更新数据流
  管理链路状态同步



网络拓扑结构



未选择DR的邻接关系

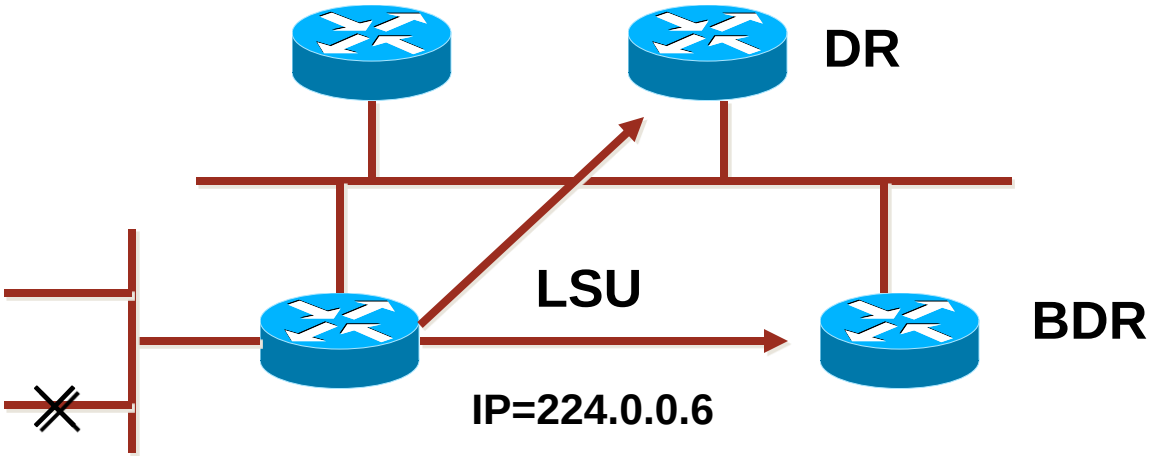


选择DR后的邻接关系

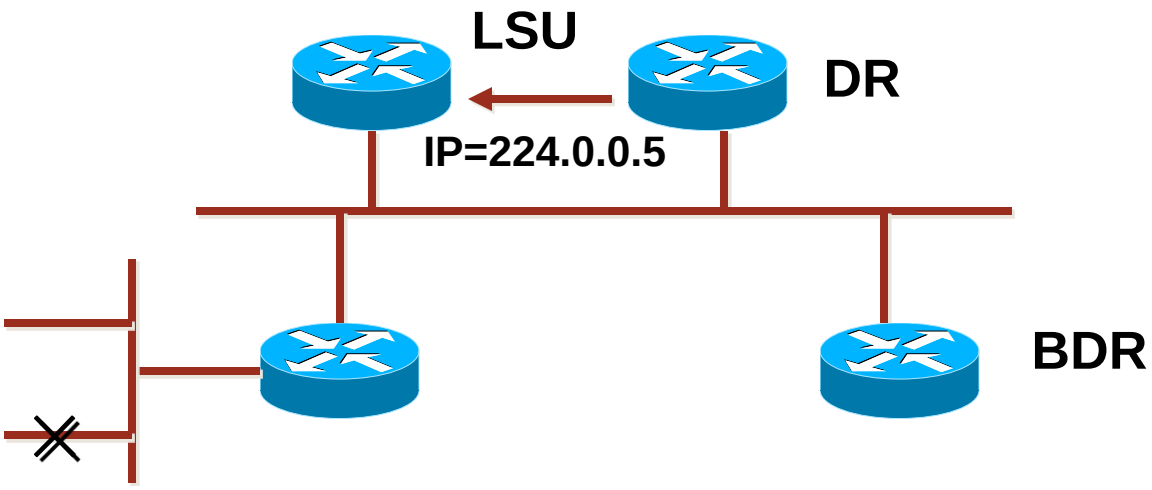
路由信息的维护

路由信息的维护　当链路状态发生变化时，路由器通过扩散**LSA**将变化通告网络中的其它路由器

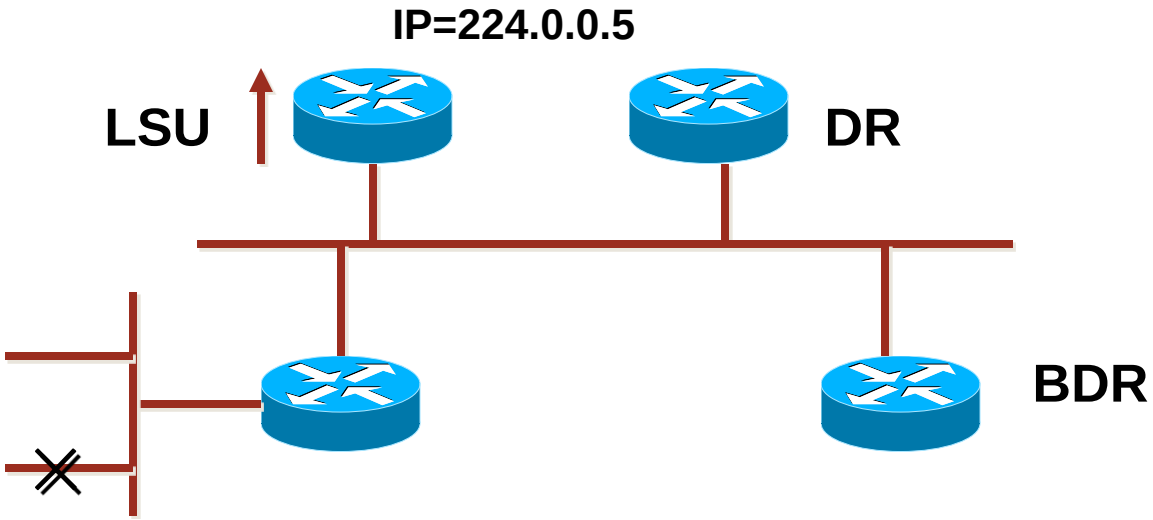
- 更新后的**LSA**条目的**LSU**，使用组播地址**224.0.0.6**（代表**DR**、**BDR**）发出去



- DR通过组播地址224.0.0.5，使用LSU将这一变化扩散到其它路由器



- 如果某个路由器还与另外的网络相联，同样使用地址为**224.0.0.6**的**LSU**向另外网络的**DR**、**BDR**通告。**DR**再向其它的路由器扩散网络发生变化的链路状态信息。



- 当收到更新的**LSA**后路由器更新它的链路状态数据库，然后使用**SPF**算法生成新的路由表。

OSPF与环回接口

- 环回接口是逻辑接口。它们可以用于OSPF的配置和诊断。
- 在路由器上配置环回接口的原因：
  - 路由器上的最高IP地址（激活端口）为此路由器的RID。此RID是用于通告其他路由器以及推选DR和BDR。
  - 如这个接口失效，则在此网络上必须将进行谁是DR和BDR的重新推选（不必要的大处理）
  - 如这个接口是一个状态不稳定的链路(不停地激活 / 失效)，这些路由器将不会实现路由的会聚
- 配置环回接口

```
Router(config) # int loopback 0
Router(config-if) #ip address 172.16.10.1 255.255.255.0
No shut
```

环回接口地址使用私有IP地址

配置OSPF

Router(config)#router ospf *process-id*

定义OSPF为IP路由协议，OSPF使用一个取值于范围1~65535内的数来识别进程的ID。此路由器上的一个取值惟一的数字，在一个指定运行的进程下该路由器分配了一系列的OSPF配置命令。不同的OSPP路由器不需要使用相同的进程ID进行通信。

Router(config-router)#network *address mask* area *area-id*

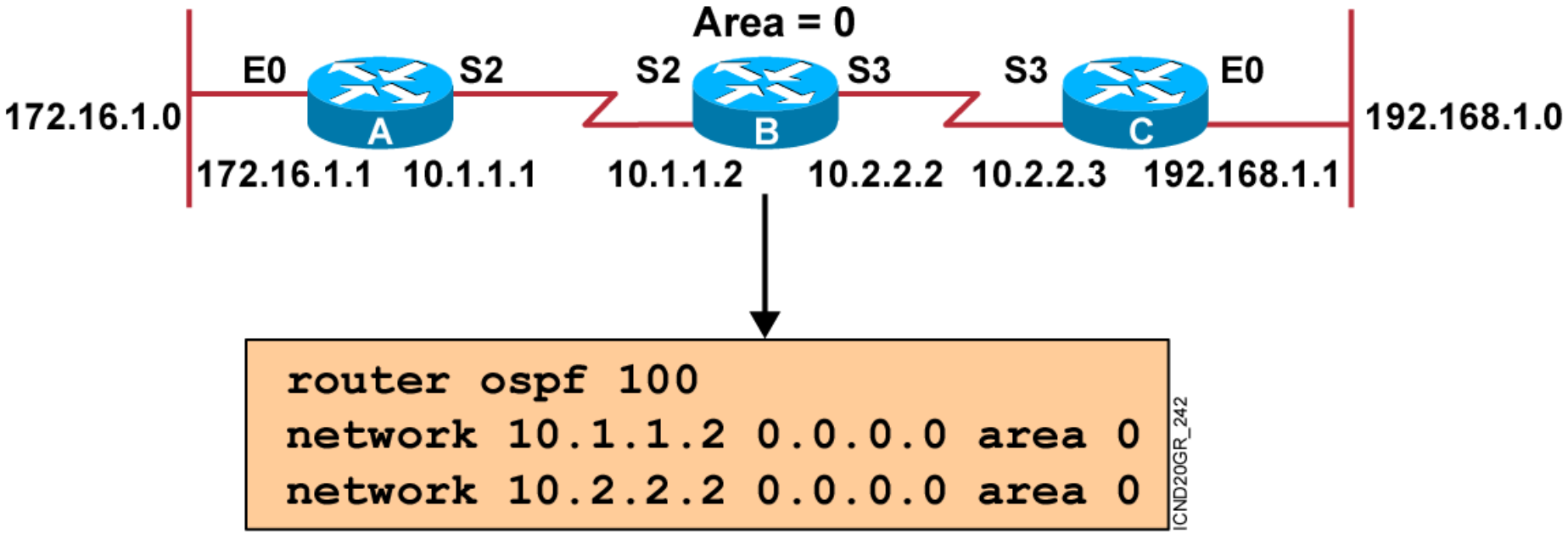
在标识OSPF的进程后，再标识想要进行OSPF通信的接口， 及路由器所在的区域。也就配置了你将要向儿他人通告的网络。

通配符掩码

例：network 1.1.1.1 0.0.0.0 area 0　只指定1.1.1.1接口

network 1.1.0.0 0.0.255.255 area 0　指定1.1.0.0~1.1.255.255范围内的接口

配置OSPF


Area = 0
E0
S2
S2
S3
S3
E0
172.16.1.0
A
B
C
192.168.1.0
172.16.1.1
10.1.1.1
10.1.1.2
10.2.2.2
10.2.2.3
192.168.1.1
router ospf 100
network 10.1.1.2 0.0.0.0 area 0
network 10.2.2.2 0.0.0.0 area 0
ICND20GR_242

BGP协议

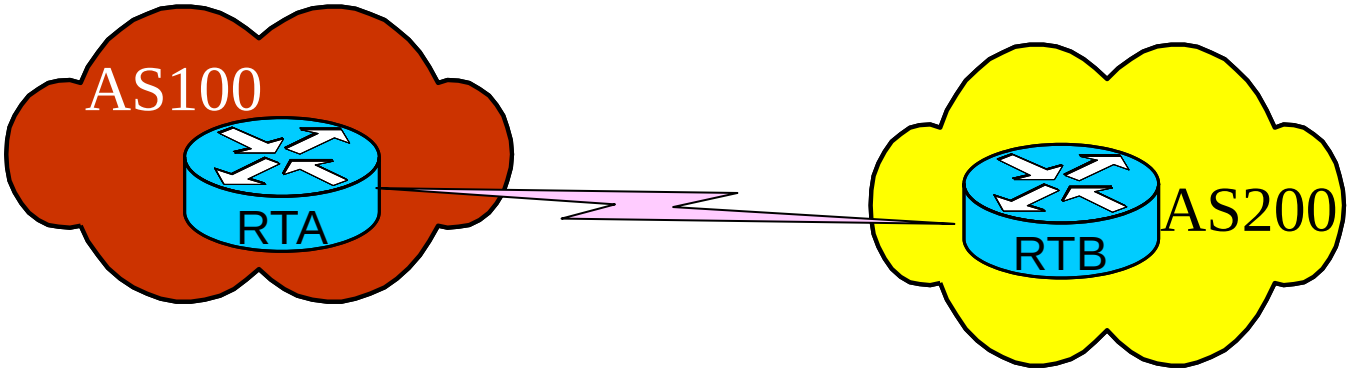
- Border Gateway Protocol，边界网关协议。
- 用来在AS之间传递路由信息。
- 是一种距离矢量的路由协议，从设计上避免了路由环路的出现。
- 支持CIDR（无类别域间选路）。
- 传送TCP协议，端口号：179

BGP的报文种类

BGP的报文种类

- ◆ Open报文
  打招呼，“你好，交个朋友怎么样？”
- ◆ KeepAlive报文
  “我还在呢，别不理我！”
- ◆ Update报文
  “有新消息……”
- ◆ Notification报文
  “拜拜，我不和你玩了！”

BGP协议的工作机制



RTA(config)#router bgp 100

RTA(config-router-bgp)#neighbor 160.10.0.2 remote-as 200

RTB(config)#router bgp 200

RTB(config-router-bgp)#neighbor 160.10.0.1 remote-as 100

基于策略的路由

- 基于策略的路由为网络管理者提供了比传统路由协议对报文的转发和存储更强的控制能力。基于策略的路由比传统路由控制能力更强，使用更灵活，它使网络管理者不仅能够根据目的地址，而且能够根据协议类型、报文大小、应用、IP源地址或者其它的策略来选择转发路径。
- 当数据包经过路由器转发时，路由器根据预先设定的策略对数据包进行匹配，如果匹配到一条策略，就根据该条策略指定的路由进行转发；如果没有匹配到任何策略，就使用路由表中的各项根据目的地址对报文进行路由。

基于协议的策略路由举例

- 当快速以太网接口FE0接收到数据包，如果为telnet流量，就发送到下一跳网关；如果为www流量，其目标网络在路由表中没有匹配项，就发送到接口Fa 0/1。

- interface FastEthernet 0/0
- ip address 192.168.12.6 255.255.255.0
- ip policy route-map pmap //在接口应用策略路由
- access-list 100 permit tcp any eq telnet any gt 1024
- access-list 100 permit tcp any gt 1024 any eq telnet
- access-list 101 permit tcp any eq www any gt 1024
- access-list 101 permit tcp any gt 1024 any eq www
- route-map pmap permit 10　//定义路由图
- match ip address 100　//匹配访问列表中的地址
- set ip next-hop 192.168.34.2　//设置数据包的下一跳IP地址
- route-map pmap permit 20
- match ip address 101
- set default interface FastEthernet 0/1
- 注：以以命令为锐捷路由器的命令

基于源地址的策略路由举例

- 路由器A将192.1.1.1来的所有数据从接口S0发出，而将从192.1.1.2来的所有数据从接口S1发出。

- Interface ethernet0
  ip policy route-map lab1//策略路由应用于E0口
  interface serial0
  ip addr 150.1.1.1 255.255.255.0
  interface serial1
  ip addr 151.1.1.1 255.255.255.0
- access-list 1 permit 192.1.1.1
  access-list 2 permit 192.1.1.2
  route-map lab1 permit 10//定义策略路由图名称：LAB1，10为序号，用来标明被匹配的路由顺序。
  Match ip address 1 //匹配地址为访问列表1
  Set interface serial0 //匹配下一跳为S0
  Route-map lab1 permit 20
  Match ip address 2
  Set interface serial1

  - 注：以以命令为思科路由器的命令

内容概要

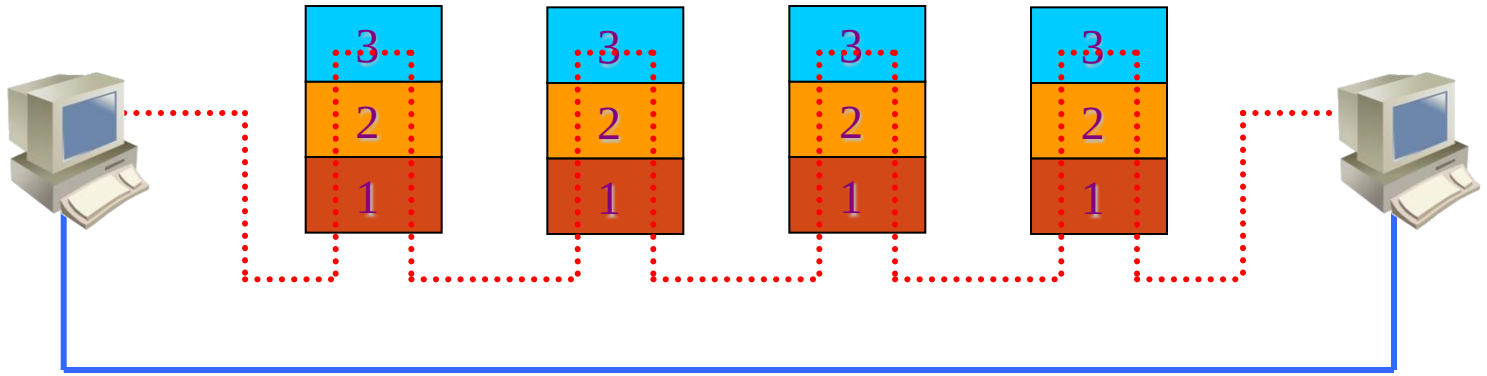
- 二层交换技术
- VLAN
- 路由技术
- 多层交换技术
- 网络地址转换（NAT）
- 移动Ad hoc网络路由技术简介

三层交换技术

通俗地讲，就是将路由与交换合二为一的技术。路由器在对第一个数据流进行路由后，将会产生一个MAC地址与IP地址的映射表，当同样的数据流再次通过时，将根据此映射表直接从二层进行交换而不是再次路由，提供线速性能，从而消除了路由器进行路由选择而造成网络的延迟，提高了数据包转发的效率。采用此技术的交换机我们常称为三层交换机。

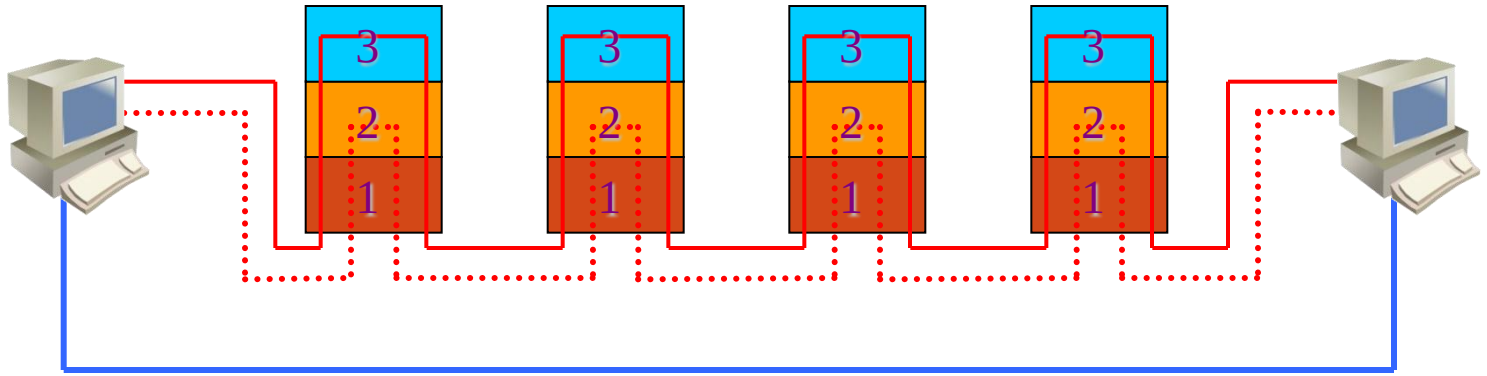
- 二层交换引擎：实现同一网段内的快速二层转发
- 三层路由引擎：实现跨网段的三层路由转发

报文到报文的三层交换技术



- 传统三层技术对每个报文进行处理，并基于第三层地址转发报文。这一方法称为报文到报文（Px P）。

基于流交换的三层交换技术



- 不在三层处理所有报文的的方法称之为流交换（FS）。

第一个报文

后续报文

L3交换机	传统路由器
广域口少，局域网口多	广域网接口广泛
支持的路由协议较少	支持多种路由协议
依靠VLAN隔绝广播	可以隔绝广播
网络号是赋给VLAN的	网络号是赋给端口的
采用硬件，路由速度快	采用软件，路由速度慢

路由器和第三层交换机对数据包交换操作的主要区别在于物理实施。在通用的路由器上，一般由基于微处理器的引擎执行数据包交换；而第三层交换机通过硬件ASIC执行数据包交换。

四层交换技术

- 它决定传输不仅仅依据MAC 地址(第二层网桥)或源/目标IP 地址(第三层路由),而且依据TCP/UDP(第四层) 应用端口号

四层交换的原理

- 具有第四层功能的交换机能够起到与服务器相连接的“虚拟IP”(VIP)前端的作用。
  每台服务器和支持单一或通用应用的服务器组都配置一个VIP 地址。这个VIP 地址被发送出 去并在域名系统上注册。
  在发出一个服务请求时，第四层交换机通过判定TCP 开始，来识别一次会话的开始。然后它利用复杂的算法来确定处理这个请求的最佳服务器。一旦做出这种决定，交换机就将
  会话与一个具体的IP 地址联系在一起，并用该服务器真正的IP 地址来代替服务器上的VIP 地址。

四层交换的几个应用技术

- 包过滤/安全控制
- 服务质量
- 服务器负载均衡
- 主机备用连接
- 统计

七层交换技术

- 第7层交换技术通过逐层解开每一个数据包的每层封装，并识别出应用层的信息，以实现对内容的识别，也叫高层智能交换。
- 提高网络服务水平，完成互联网向智能化的转变。
- 如：根据URL的具体内容的识别交换，带宽管理 等

内容概要

- 二层交换技术
- VLAN
- 路由技术
- 多层交换技术
- 网络地址转换（NAT）
- 移动Ad hoc网络路由技术简介

NAT技术

- 目前不少企事业都已建好了内部局域网，但随着互联网时代的到来，仅搭建局域网已经不能满足众多企业的需要，有更多的用户需要在Internet上发布信息，或进行信息检索，将企业内部局域网接入Internet已经成为众多企业的迫切要求。
- 可用的IP地址越来越少，要想在ISP处申请一个新的IP地址已不是很容易的事了。

NAT的工作原理

（1）客户机将数据包发给运行NAT的路由器。

（2）NAT将数据包中的端口号和专用的IP地址换成它自己的端口号和公用的IP地址，然后将数据包发给外部网络的目的主机，同时记录一个跟踪信息在映像表中，以便向客户机发送回答信息。

（3）外部网络发送回答信息给NAT。

（4）NAT将所收到的数据包的端口号和公用IP地址转换为客户机的端口号和内部网络使用的专用IP地址并转发给客户机。

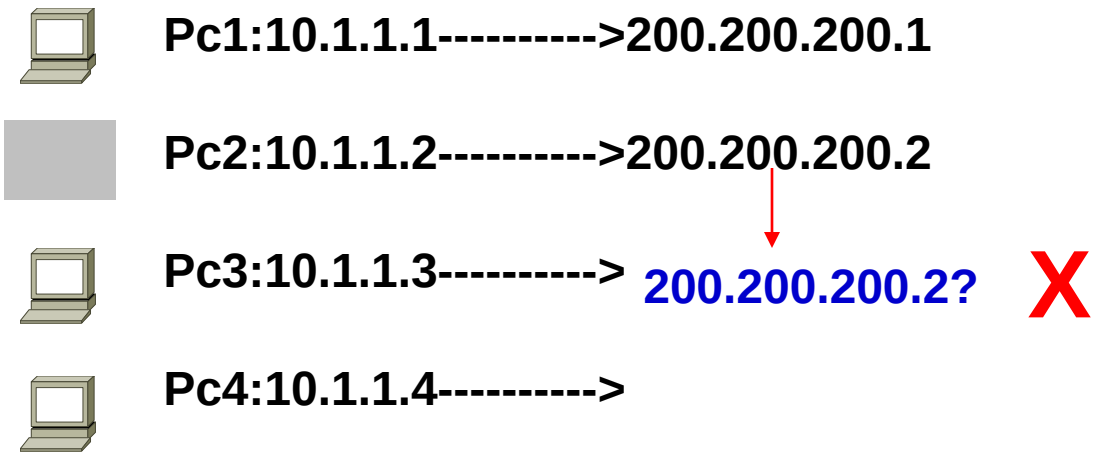
NAT 术语

- 内部本地地址:私有IP，不能直接用于互连网。
- 内部全局地址：用来代替内部本地IP地址的，对外，或在互联网上是合法的的IP地址。
- 地址池：NIC或ISP分配使用的多个地址

NAT三种类型

- 1.静态NAT

  静态NAT的特征是内部主机地址被一对一映射到外部主机地址

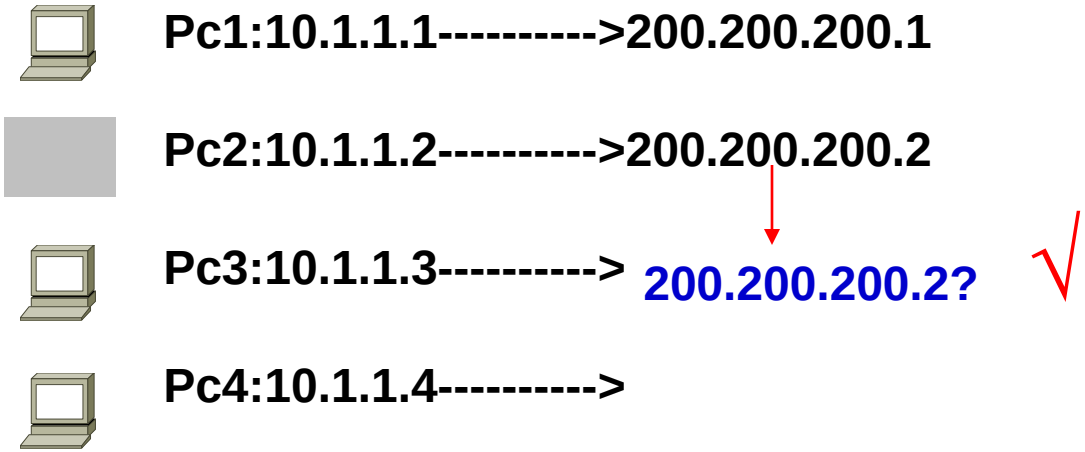


- 多用于服务器。

NAT三种类型

- 2. 动态NAT

  动态NAT的特征是内部主机使用地址池中的公网地址来映射

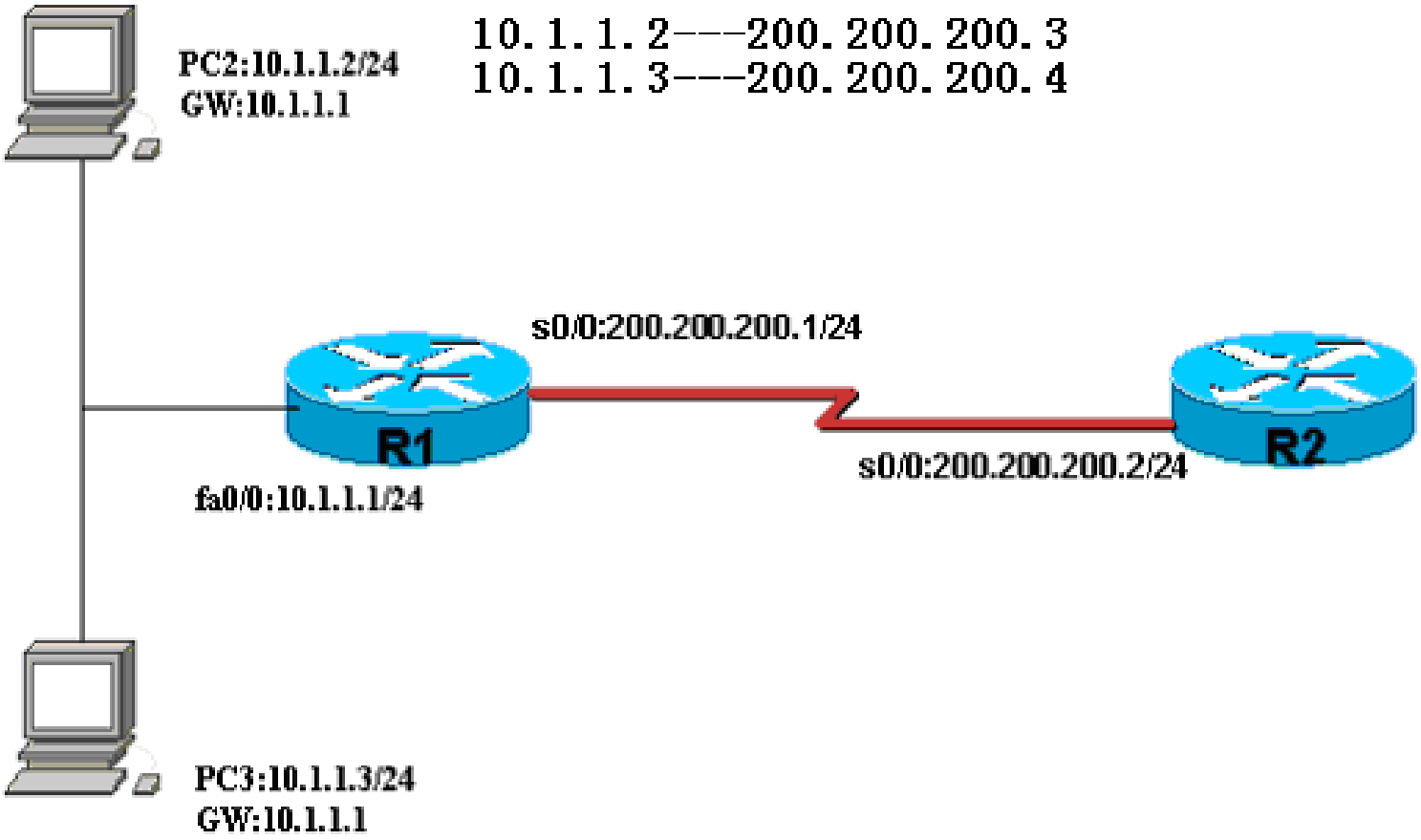


- 多用于网络中工作站。

NAT三种类型

- 3. 端口复用(PAT)
  端口复用的特征是内部多个私有地址通过不同的端口被映射到一个公网地址。

静态NAT配置实例


PC2:10.1.1.2/24
GW:10.1.1.1
10.1.1.2---200.200.200.3
10.1.1.3---200.200.200.4
s0/0:200.200.200.1/24
R1
R2
s0/0:200.200.200.2/24
fa0/0:10.1.1.1/24
PC3:10.1.1.3/24
GW:10.1.1.1

静态NAT配置实例

r1(config)#ip nat inside source static 10.1.1.2 200.200.200.3

r1(config)#ip nat inside source static 10.1.1.3 200.200.200.4

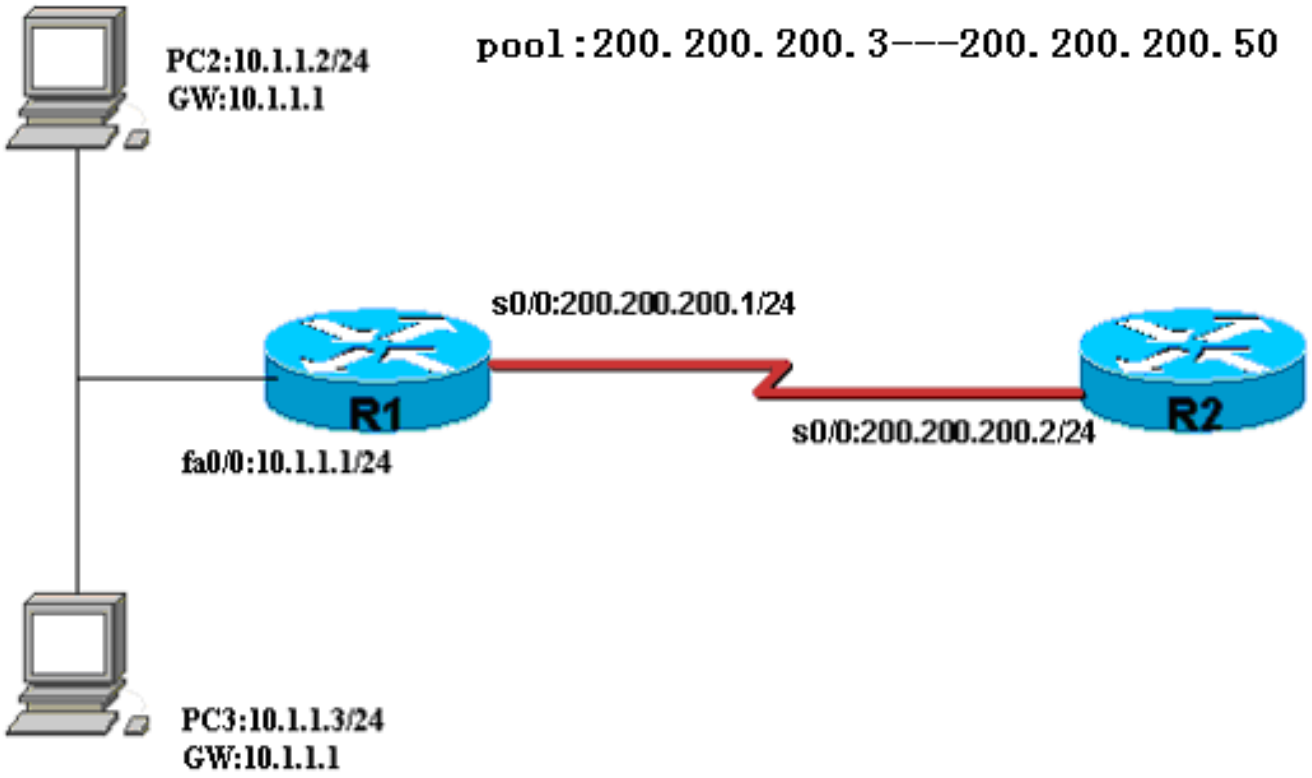
r1(config)#interface f0/0

r1(config-if)#ip nat inside （指定内部接口）

r1(config)#int s0/0

r1(config-if)#ip nat outside （指定外部接口）

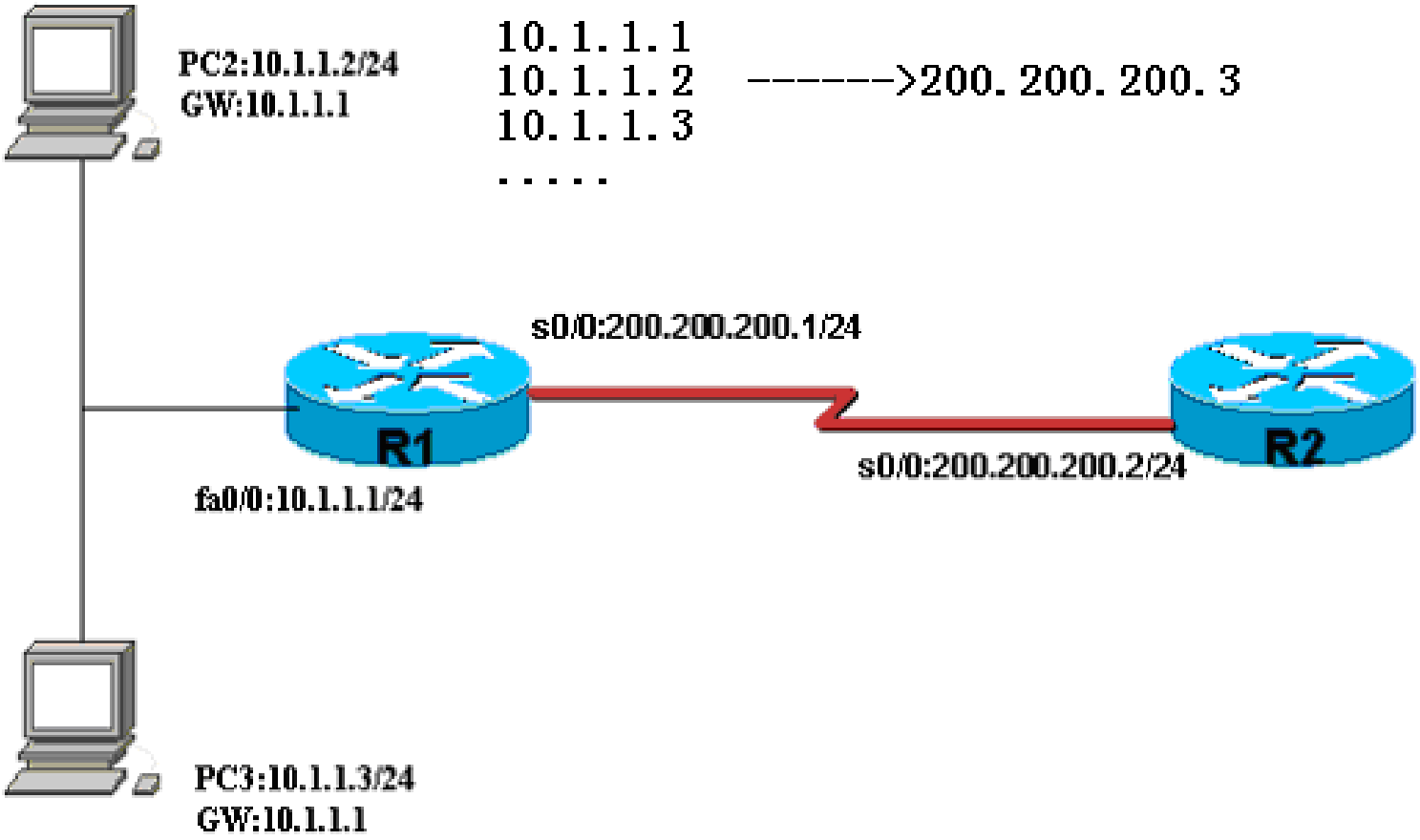
动态NAT配置实例


PC2:10.1.1.2/24
GW:10.1.1.1
pool:200.200.200.3---200.200.200.50
s0/0:200.200.200.1/24
R1
R2
s0/0:200.200.200.2/24
fa0/0:10.1.1.1/24
PC3:10.1.1.3/24
GW:10.1.1.1

动态NAT配置实例

- r1(config)#ip nat pool NAT 200.200.200.3 200.200.200.50 netmask 255.255.255.0
- r1(config)#access-list 1 permit 10.1.1.0 0.0.0.255
- r1(config)#ip nat inside source list 1 pool NAT
- r1(config)#interface f0/0
- r1(config-if)#ip nat inside
- r1(config)#int s0/0
- r1(config-if)#ip nat outside

PAT配置实例


PC2:10.1.1.2/24
GW:10.1.1.1
10.1.1.1
10.1.1.2 ------>200.200.200.3
10.1.1.3
.....
s0/0:200.200.200.1/24
R1
R2
s0/0:200.200.200.2/24
fa0/0:10.1.1.1/24
PC3:10.1.1.3/24
GW:10.1.1.1

PAT配置实例

- r1(config)#ip nat pool NAT 200.200.200.3 200.200.200.50 netmask 255.255.255.0
- r1(config)#access-list 1 permit 10.1.1.0 0.0.0.255
- r1(config)#ip nat inside source list 1 pool NAT overload
- r1(config)#interface f0/0
- r1(config-if)#ip nat inside
- r1(config)#int s0/0
- r1(config-if)#ip nat outside
- r1(config)#ip route 0.0.0.0 0.0.0.0 200.200.200.2

内容概要

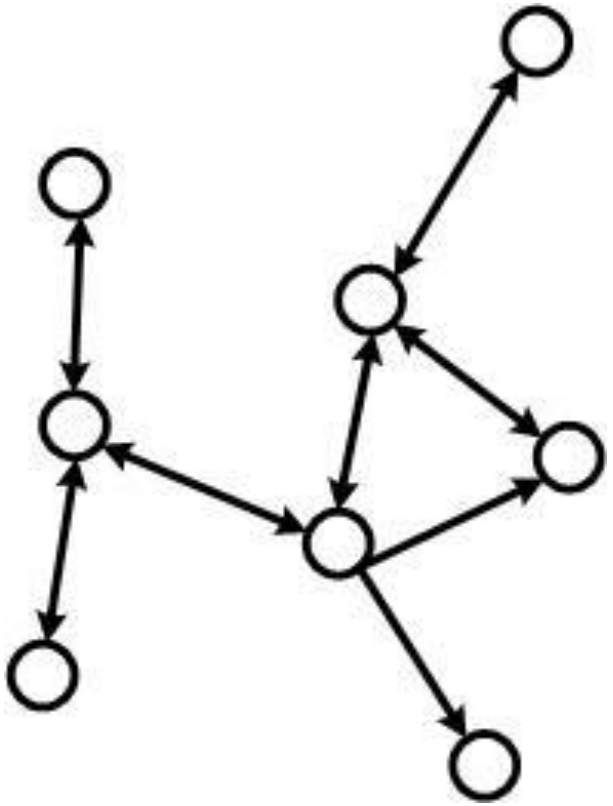
- 二层交换技术
- VLAN
- 路由技术
- 多层交换技术
- 网络地址转换（NAT）
- 移动Ad hoc网络路由技术简介

移动Ad Hoc路由协议

- ，“Ad Hoc”一词来源于拉丁语，意思是“专用的、特定的”，来表示该网为“无固定设施网”或“自组织网”，是一组带有无线收发装置的移动终端组成的一个多跳的临时性自治系统。
- 应用场合：发生地震或水灾后的营救、战场上部队的快速推进、野外科学考查、偏远山区作业、临时组织的会议等

Ad Hoc网络的特点

- 无中心和自组织性
- 多跳路由
- 动态变化的网络拓扑
- 有限的无线传输带宽
- 移动终端的局限性
- 安全性差
- 生存周期短



传统网络路由协议在Ad Hoc网络中存在的问题

- 有限的无线信道带宽
- 很难收敛
- 单向信道的存在
- 移动终端的能源控制

Ad Hoc路由协议分类

Ad Hoc网络路由协议众多，从不同角度可分为以下几种：

- 所处的网络逻辑视图

平面路由协议、分级的路由协议。

- 发现路由的策略

主动路由协议、被动路由协议和混合路由协议。

- 是否有GPS辅助

基于网络拓扑的路由协议、基于位置的路由协议。

平面与分级路由协议的比较

参数	平面路由协议	分级路由协议
算法复杂度	简单	复杂
可扩展性	弱	强
适用范围	小规模网络	大规模网络
健壮性	高	弱
安全性	高	弱

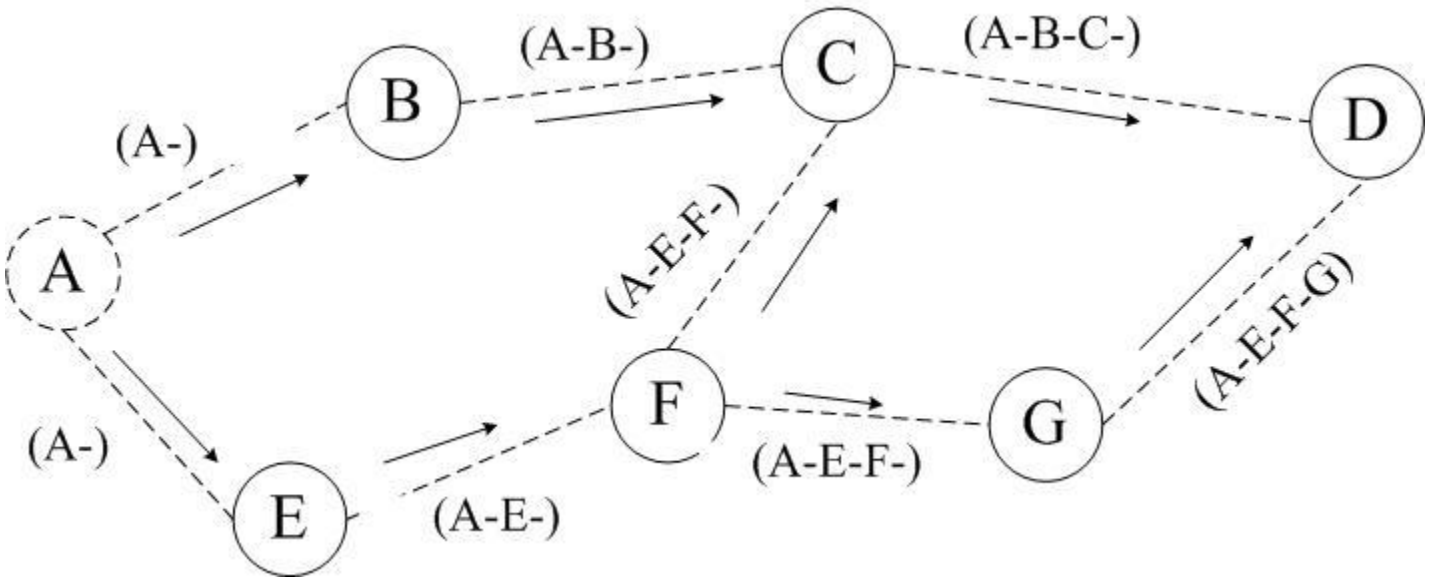
主动与被动路由协议的比较

参数	表驱动方式	按需方式
是否周期更新	是	否
路由获取延迟	低	高
控制负载	高	低
耗电量	高	低
带宽开销	高	低

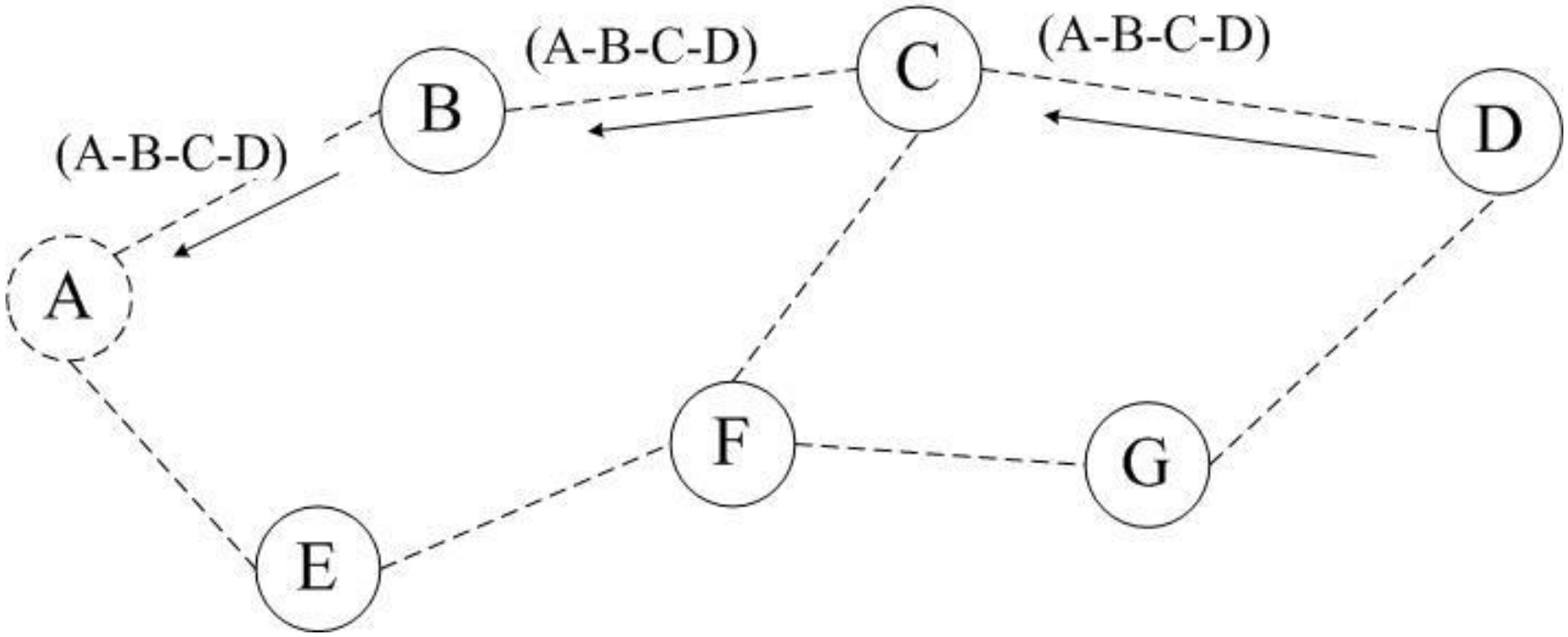
Ad Hoc路由协议举例 ---DSR路由协议

- DSR协议使用了源路由,每一个分组的分组头中包含整条路由的信息, 中间节点不需要维持当前的路由信息
- 主要由路由发现和路由维护两部分组成

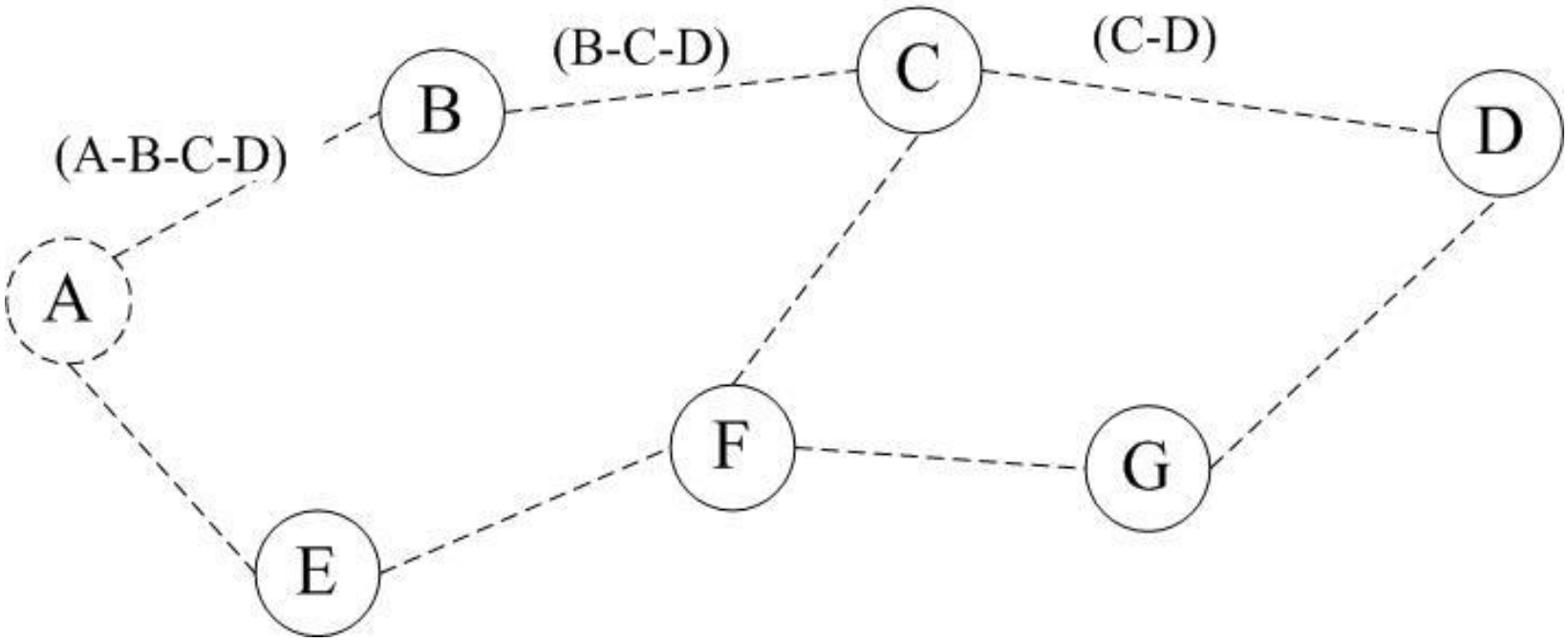
DSR 路由请求过程



DSR路由响应过程



DSR中的路由缓存技术



谢　谢！